ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN CIRCUITO CERRADO DE TELEVISIÓN CON CÁMARAS IP INALÁMBRICAS Y MONITOREO REMOTO, NOTIFICACIÓN DE EVENTUALIDADES MEDIANTE EL USO DE UN SERVIDOR PARA LA GRABACIÓN DE VIDEO BAJO LINUX USANDO ZONEMINDER PARA EL LABORATORIO DE INFORMÁTICA DEL EDIFICIO DE ELÉCTRICA-QUÍMICA.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

JORGE LUIS NOGUERA ROSERO
georgenoguera@hotmail.com

JUAN ANDRÉS VÁSQUEZ PERALVO
juan.vasquez@epn.edu.ec

DIRECTOR: ING. CARLOS HERRERA
carlos.herrera@epn.edu.ec

Quito, julio 2011

DECLARACIÓN

Nosotros, Jorge Luis Noguera Rosero y Juan Andrés Vásquez Peralvo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Jorge Luis Noguera Rosero **Juan Andrés Vásquez Peralvo**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jorge Luis Noguera Rosero y Juan Andrés Vásquez Peralvo, bajo mi supervisión.

_____

ING. CARLOS HERRERA MUÑOZ

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A mi padre DIOS, el cual día a día me llena de bendiciones, de oportunidades para alcanzar mis sueños dándome la valentía y coraje necesario para levantarme en las adversidades permitiéndome luchar por mis metas, sin duda a mi Dios bendito le debo todo lo que soy y lo que llegare a ser.

A mi madre Consuelo Rosero quien hizo un enorme esfuerzo por permitirme culminar mis estudios, ese ser querido que ha sido madre y padre a la vez y que día a día hace lo imposible por darme un mejor estilo de vida, te agradezco por todo lo que me has dado a lo largo de estos maravillosos veinticuatro años que he estado a tu lado, Gracias Mamá.

A mis familiares que con cada palabra de aliento me impulsaron para superarme día a día y llegar a culminar mi meta.

Sin duda la vida universitaria no fue fácil, pero tampoco imposible. A lo largo de esta etapa estudiantil tuve la oportunidad de conocer a personas valiosas mis amigos(as); con los que vivimos momentos inolvidables de alegría, tristezas, éxitos, fracasos, desesperación; cada experiencia vivida es irrepetible, sinceramente gracias por todas sus muestras de cariño y por ese apoyo que fue sumamente importante para culminar mis estudios universitarios.

A mi Director de Tesis, Ing. Carlos Herrera quien con sus conocimientos me guió para realizar el trabajo de grado, sus sabios consejos me ayudarán a enfrentar la vida diaria y laboral. A mi gran amigo y compañero de Tesis, Juanito gracias por brindarme la oportunidad de trabajar juntos, por tu paciencia, tu amistad y por exigirme cada día a entregar mi mejor esfuerzo y a crecer profesionalmente.

A Mogritos por auspiciarnos la impresión de nuestra tesis.

JORGE LUIS NOGUERA ROSERO
Sin derecho a rendirse.

AGRADECIMIENTO

Agradezco de corazón a mis padres, mis hermanos por apoyarme en toda mi carrera estudiantil, a Jorge por estar conmigo en las buenas y en las malas, al Ing. Carlos Herrera por haber contribuido con su guía y conocimiento, además de los concejos que me ha brindado durante mi trabajo en el Laboratorio de Informática.

A todos mis ayudantes y auxiliares del Laboratorio de Informática, por brindarme su apoyo a lo largo de estos maravillosos tres semestres.

A mis amigos que durante nuestra vida universitaria supieron apoyarme tanto académicamente como personalmente.

Al Ing. Carlos Herrera por ser un amigo más que un tutor, guiándome profesionalmente durante este último año.

A Mogritos por auspiciarnos la impresión de nuestra tesis.

A Lorena por haberme apoyado durante los momentos más difíciles de mi vida, gracias de todo corazón mi POLOLITA….

Juan Andrés Vásquez

DEDICATORIA

A todas las personas que a pesar de tener limitaciones físicas, sociales o económicas luchan cada día por ser felices, alcanzar sus sueños y buscan que el mundo sea un mejor lugar para vivir.

A mi mami y a mi ñaña, ustedes son el mejor regalo que me ha dado la vida. Las adoro y las quiero mucho ustedes son mi vida y mucho más…!!!

JORGE LUIS NOGUERA ROSERO

DEDICATORIA

El presente trabajo lo dedico a mis padres que iniciaron desde cero y supieron salir adelante para brindarnos a mis hermanos y a mí la posibilidad de estudiar y superarnos en la vida.

A mis hermanos David, Paulina y Geovanna que desde pequeño me enseñaron que siempre se tiene que luchar por conseguir todo lo que uno añora.

Juan Andrés Vásquez

CONTENIDO

LISTA DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

LISTA DE TABLAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

RESUMEN

El presente Proyecto tiene como objetivo el diseño e implementación de un circuito cerrado de televisión, utilizando cámaras IP inalámbricas y servidores basados en el sistema operativo Linux, para monitorear las actividades realizadas en el Laboratorio de Informática, con el propósito de garantizar la seguridad de los equipos.

El Laboratorio de Informática no cuenta con sistemas de seguridad para proteger la gran cantidad de equipos computacionales y de conectividad de la academia ACIERTE y de la Escuela Politécnica Nacional, es por este motivo que este Proyecto nace como una idea de brindar un monitoreo continuo a estas instalaciones y como la oportunidad de aplicar nuestros conocimientos adquiridos.

A través del monitoreo continuo y remoto las personas encargadas de la administración de la red de datos del Laboratorio de Informática, pueden monitorear desde cualquier lugar con acceso a Internet, las actividades que se desarrollan en este lugar, así como recibir alertas en sus correos electrónicos de las zonas de mayor vulnerabilidad ante un eventual atraco.

El Capítulo I describe el soporte de comunicación de las cámaras inalámbricas IP, su funcionamiento y monitoreo; también se estudia las características del software ZoneMinder, para realizar el control, monitoreo y registro de actividades realizadas en el Laboratorio de Informática.

En el Capítulo II se realiza el diseño del CCTV, el cual comprende el estudio site survey y otros aspectos como el cálculo de ancho de banda, ubicación de los puntos de monitoreo, implementación de los servidores y el desarrollo de una aplicación para el control de las cámaras.

En el Capítulo III se realizan las pruebas de funcionamiento del CCTV, detección de errores y sus respectivas soluciones considerando la información almacenada en el servidor dentro de un periodo determinado.

En el Capítulo IV se realiza un presupuesto referencial de los equipos necesarios que cumplan con las características obtenidas del diseño del CCTV.

En el Capítulo V se indican las conclusiones y recomendaciones que se obtienen al realizar el Proyecto.

Adicionalmente se incluye ocho anexos, tales como: proceso de encapsulamiento de una trama 802.11 g, datasheet de las cámaras utilizadas, del servidor y del router inalámbrico, scripts para la implementación del Firewall, para la aplicación del movimiento de las cámaras, sobrecarga por encapsulamiento, análisis de protocolos utilizando wireshark, y la instalación del sistema operativo CentOS.

PRESENTACIÓN

La video vigilancia se originó como una solución a la necesidad de mantener vigilado a un lugar constantemente y tomó lugar con la aparición de los primeros Circuitos Cerrados de Televisión con cámaras analógicas, en sus inicios la video vigilancia era destinada únicamente a ambientes empresariales, sin embargo con el vertiginoso desarrollo tecnológico y la facilidad de diseño e instalación, este sistema ha llegado a extenderse como una solución de seguridad en hogares, museos, obras de construcción, vigilancia de niños, ancianos, etc.

A través de los años los requerimientos de monitoreo y control de los lugares a ser vigilados se han incrementado, por ejemplo hoy en día es necesario realizar un zoom digital en zonas críticas o que cuenten con sensores de movimiento y muchas de las cámaras analógicas carecen de dichas funcionalidades. Frente a esta necesidad y en conjunto con el auge de la era digital, surge una solución efectiva que es la video vigilancia IP, la misma que es una efectiva solución de seguridad.

La video vigilancia IP desplazó a los sistemas analógicos que además de ser de un precio elevado, no presentan las mismas prestaciones que las cámaras IP, tales como acceso a través de Internet y método de compresión de video.

El software ZoneMinder es una herramienta muy poderosa que permite gestionar el streaming de video recibido, sea por cámaras web, IP o analógicas. Brinda mucha estabilidad y seguridad debido a que trabaja sobre sistemas operativos basados en Linux.

El sistema operativo Linux es uno de los más estables, robustos y rápidos, convirtiéndose en una herramienta ideal para servidores. Linux a diferencia de Windows, es software libre y varias distribuciones son gratuitas lo que permite

hacer modificaciones según las necesidades que se presenten, otra característica es que éste sistema operativo es multiusuario y multitarea.

CAPÍTULO I

1. ESTUDIO TEÓRICO.

En este capítulo se describe el soporte de comunicaciones de las cámaras inalámbricas IP, su funcionamiento y sus componentes. De igual manera se estudia las características del software ZoneMinder que permitan realizar el control, monitoreo y registro de actividades en el Laboratorio de Informática.

1.1 REDES DE DATOS.

1.1.2 INTRODUCCIÓN.

Una red es un conjunto de dispositivos de red interconectados entre sí mediante medios de transmisión alámbricos o inalámbricos; cuyo objetivo es compartir unidades de disco duro, impresoras, documentos, base de datos, archivos, carpetas, etc.; de tal forma que éstos sean accesibles y utilizables desde cualquier equipo informático que esté conectada a dicha red.

1.1.3 CLASIFICACIÓN DE LAS REDES DE DATOS[1].

La clasificación de las redes de datos es muy extensa debido a que se pueden clasificar por:

- Por alcance.
- Por tipo de conexión.
- Por relación funcional.
- Por topología.
- Por la direccionalidad de los datos.

[1] Clasificación de las redes de datos - http://es.wikipedia.org/wiki/Red_de_computadoras.

- Por grado de autentificación.
- Por grado de difusión.
- Por servicio o función.

Considerando el criterio de área de cobertura o alcance las redes se clasifican en LAN, MAN y WAN.

1.1.3.1 Redes de área local (LAN).

Las redes LAN (*Local Area Network - Redes de Área Local)* conectan varios dispositivos en un área geográfica que se extiende desde unos pocos metros hasta algunos kilómetros. Para la transmisión de la información se emplea cable de par trenzado, cable coaxial, fibra óptica, láser, radio y microondas[2].

En la figura 1.1, se indica la topología de una red LAN.

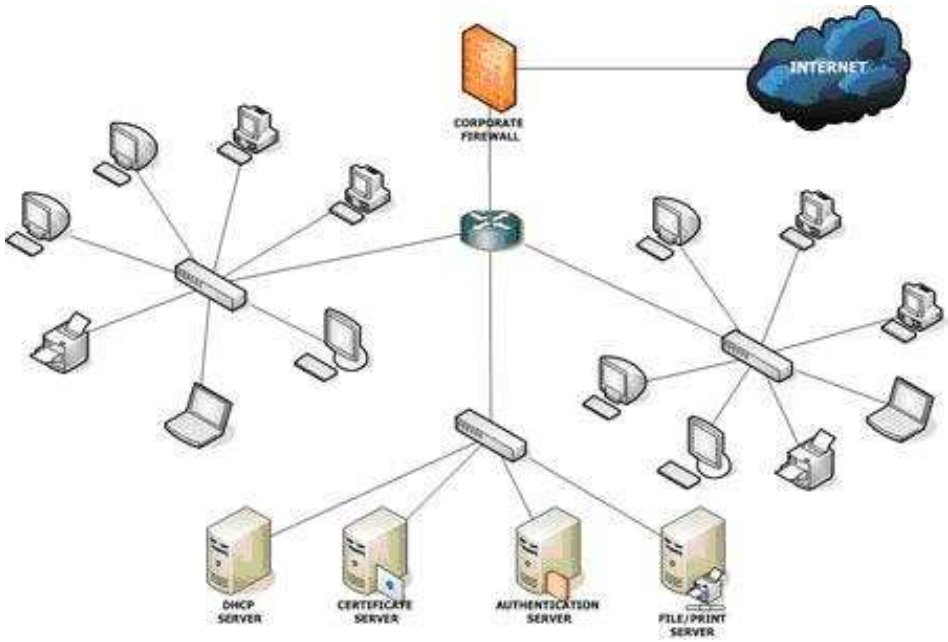


Figura 1. 1 Red de área local[3].

[2] TANEMBAUM, Andrew; "Redes de Computadoras"; 3ra Edición; 1997; Prentice-Hall; Inc.
[3] Red de área local - http://espegizmo.com/2008/01/31/curiosos/30-anos-desde-que-aparecio-la-red-lan/

1.1.3.2 Redes de área metropolitana (MAN).

Las redes MAN (*Metropolitan Area Network - Redes de Área Metropolitana*) se extienden desde una hasta varias decenas de kilómetros, es por ejemplo una red que se extiende por todo una ciudad, o una red que comunica varios edificios distantes entre sí, el medio de transmisión que generalmente se usa es la fibra óptica o se utiliza una infraestructura inalámbrica.

En la figura 1.2, se indica la topología de una red MAN.

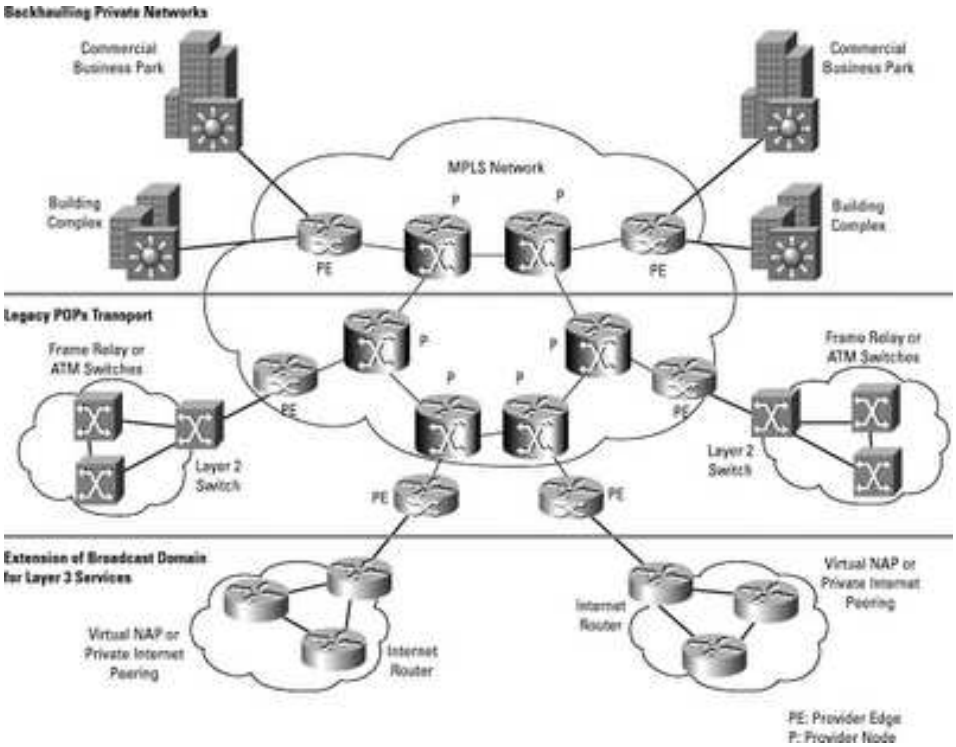


Figura 1. 2 Red de área metropolitana[4].

1.1.3.3 Redes de área extensa (WAN).

Las redes WAN (*Wide Area Network – Redes de Área Extensa)* se extienden sobre un área geográfica amplia, por ejemplo un país, un continente. Para cubrir grandes distancias este tipo de redes emplea diferentes medios de transmisión

[4] Red de área metropolitana. - http://yasshita.blogspot.com/2010/04/redes-lan-man-y-wan.html

como son: microondas, cables de cobre, fibra óptica, enlaces satelitales. El ejemplo más claro de una red WAN es el internet[5].

En la figura 1.3, se indica la topología de una red WAN.

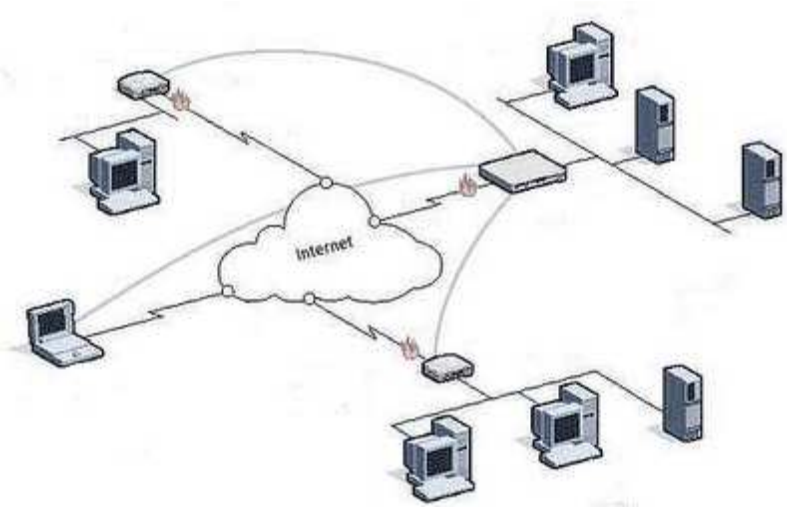


Figura 1. 3 Red de área extendida[6].

1.1.4 REDES DE ÁREA LOCAL INALÁMBRICA (WLAN).

WLAN (*Wireless Local Area Network – Redes de Área Local Inalámbrica*) son redes que emplean ondas de radio, infrarrojos y microondas para conectar dispositivos a una red. En la actualidad las redes de área local inalámbrica son muy conocidas y comúnmente utilizadas debido a la facilidad de instalación y configuración; además presentan ventajas en el campo de movilidad, generan bajos costos, comodidad y escalabilidad. Estas características permiten a los usuarios acceder en tiempo real a información y recursos sin necesidad de estar físicamente conectados a un dispositivo inalámbrico[7].

En la figura 1.4, se indica la topología de una red WLAN.

[5] TANEMBAUM, Andrew; "Redes de Computadoras"; 3ra Edición; 1997; Prentice-Hall; Inc.
[6] Red de área extendida. - http://mariorozenwurcel.com.ar/?p=48
[7] TANEMBAUM, Andrew; "Redes de Computadoras"; 3ra Edición; 1997; Prentice-Hall; Inc.

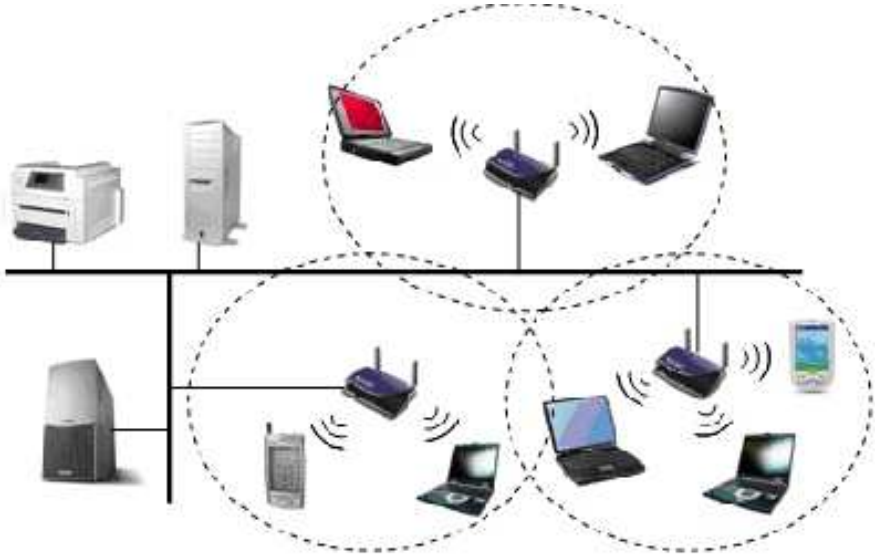


Figura 1. 4 Red de área local inalámbrica[8].

1.1.4.1 Ventajas de las WLAN.

Las ventajas de las WLAN frente a redes cableadas son:

- Movilidad y disponibilidad.
- Escalabilidad.

1.1.4.2 Desventajas de las WLAN.

Las desventajas de las redes de área local inalámbricas son:

- Interferencia.
- Susceptibilidad a obstáculos.
- Pérdida de velocidad en comparación a redes de datos cableadas.
- Seguridad.

[8] Red de área local inalámbrica. - http://www.zero13wireless.net/foro/showthread.php?88-Que-es-el-Wireless-%F3-WLAN

1.1.4.3 Medio físico[9].

Las WLAN a diferencia de las LAN emplean como tecnología de transmisión Radiofrecuencia (RF) e Infrarrojo en lugar de cable; las diferencias entre las dos tecnologías son:

- El cable con su envoltura aislante protege a la información de señales exteriores, por el contrario la señal de RF no está protegida de señales exteriores provocando que éstas se interfieran.

- La transmisión RF está sujeta a los mismos problemas de la tecnología basada en ondas, puede existir superposición de ondas, presencia de señales indeseables, provocando un desvanecimiento en la señal original; por el contrario las LAN emplean un cable como elemento de transmisión, las cuales utilizan una longitud apropiada del cable para mantener la potencia de la señal.

- Las bandas RF se regulan en forma diferente en cada país. La utilización de las WLAN está sujeta a regulaciones adicionales y a conjuntos de estándares que no se aplican a las LAN conectadas por cable.

- Determinadas bandas de RF se eligen de tal forma que no se necesite permiso para poder utilizarlas, debido a que trabajan en la banda ISM (*Industrial, Scientific and Medical - Industrial, Científica y Médica*).

En la tabla 1.1, se indican los canales, la frecuencia central y el ancho de banda correspondiente a las bandas ISM en la frecuencia de 2.4 GHz.

CANAL	FRECUENCIA EN EE.UU. [MHz]	FRECUENCIA EN EUROPA [MHz]
1	2412	NO DISPONIBLE
2	2417	NO DISPONIBLE

[9] TANEMBAUM, Andrew; “Redes de Computadoras”; 3ra Edición; 1997; Prentice-Hall; Inc.

CANAL	FRECUENCIA EN EE.UU. [MHz]	FRECUENCIA EN EUROPA [MHz]
3	2422	2422
4	2427	2427
5	2432	2432
6	2437	2437
7	2442	2442
8	2447	2447
9	2452	2452
10	2457	2457
11	2462	2462

Tabla 1. 1 Banda ISM [10].

1.1.4.4 Componentes de la infraestructura inalámbrica.

1.1.4.4.1 NIC inalámbricas.

Las NIC inalámbricas permiten a las estaciones clientes enviar y recibir señales de RF con el fin de conectarse a los puntos de acceso inalámbricos, los mismos que se conectan a la infraestructura de la red.

En la figura 1.5, se indica una tarjeta de red inalámbrica PCI.

[10] Bandas ISM. - http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/caracteristicas802.htm

Figura 1. 5 Tarjeta de Red Inalámbrica.

1.1.4.4.2 Punto de acceso inalámbrico.

Un punto de acceso inalámbrico es un dispositivo de red, que permite conectar a clientes inalámbricos con una red LAN cableada; para realizar está función convierte los paquetes de datos, desde su formato 802.11 al formato de trama Ethernet 802.3.

En la figura 1.6, se indica un punto de acceso inalámbrico marca Linksys.

Figura 1. 6 Punto de Acceso Inalámbrico[11].

[11] Punto de acceso inalámbrico. – Curriculum de Cisco Módulo 3.

1.1.4.4.3 Router inalámbrico.

El router, es un dispositivo de hardware para interconexión de red de computadoras, opera en la capa tres (nivel de red) del modelo OSI. Un router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos[12].

En la figura 1.7, se indica un router Inalámbrico.

Figura 1. 7 Router Inalámbrico[13].

1.1.4.4.4 Conjunto de Servicios Básicos.

El Conjunto de Servicios Básicos (BSS) es el elemento fundamental en una red de área local inalámbrica y es el conjunto de estaciones que coordinan su acceso

[12] Router Inalámbrico. - http://es.wikipedia.org/wiki/Enrutador
[13] Router Inalámbrico. – Curriculum de Cisco Módulo 3.

al medio. El área de cobertura de un BSS se conoce como Área de Servicios Básicos (BSA).

1.1.4.5 Proceso de autenticación y asociación en una red inalámbrica[14].

1.1.4.5.1 Autenticación.

Es el proceso de identificar el dispositivo y no al usuario, la autenticación se produce en la Capa 2 y es un factor importante en la seguridad, administración y detección de fallas en una WLAN.
Este proceso posee dos mecanismos de autenticación:

1. Autenticación abierta.
2. Autenticación compartida.

1.1.4.5.2 Autenticación abierta.

En este tipo de autenticación, el cliente se identifica directamente con el punto de acceso sin necesidad de ingresar una contraseña.

1.1.4.5.3 Autenticación compartida.

En esta técnica, el cliente envía una solicitud de autenticación al punto de acceso. El punto de acceso luego envía un texto de reto al cliente, quien encripta el mensaje utilizando la clave compartida y vuelve a enviar el texto encriptado al punto de acceso. La autenticación compartida se basa en una clave de privacidad equivalente por cable WEP (Wireless Equivalent Privacy - Equivalente de Privacidad Inalámbrica) compartida entre el cliente y el punto de acceso.

- **WPA.** WPA (*WiFi Protect Acces – Acceso WiFi Protegido*) emplea TKIP (*Temporal Key Integrity Protocol – Integridad de Llave Temporal*) para la gestión de claves dinámicas y el cifrado de datos mejorando las debilidades de

[14] Curriculum CCNA 3 -"Conmutación y conexión Inalámbrica de LAN"

WEP. Clave dinámica se refiere a que la clave cambia constantemente permitiendo que WPA sea considerado como uno de los más altos niveles de seguridad para una red inalámbrica.

- **WPA 2.** WPA2 es la segunda generación de WPA, emplea AES (*Advanced Encryption Standard – Estándar de Codificación Avanzada*) para el cifrado de datos, mejorando las debilidades de WPA. WPA2 se encuentra disponible en los Puntos de Acceso más modernos.

1.1.4.6 Asociación.

Este proceso se realiza después de la autenticación y permite a los clientes usar los servicios del Punto de Acceso para transferir datos. Cuando un nodo desea unirse al BSS necesita obtener información de sincronización desde un Punto de Acceso, para esto emplea un modo de búsqueda activo o un modo de búsqueda pasivo.

1.1.4.6.1 Modo de Búsqueda pasivo.

El Modo de Búsqueda Pasivo consiste en esperar hasta recibir una trama especial de sincronización emitida periódicamente desde el Punto de Acceso llamada Beacon.

1.1.4.6.2 Modo de Búsqueda activo.

El Modo de Búsqueda Activo consiste en enviar tramas de búsqueda llamadas Probe Request y espera recibir desde el Punto de Acceso un Probe Response. Una vez que se ha completado este proceso, el nodo puede intercambiar datos con la red.

1.1.5 CLASIFICACIÓN DE LAS REDES INALÁMBRICAS[15].

Las redes inalámbricas de área local se clasifican en dos tipos:

1. Redes Ad hoc.
2. Redes de Infraestructura.

1.1.5.1 Redes Ad hoc.

Este tipo de redes son formadas por múltiples puntos inalámbricos dentro de un área de cobertura. Las redes Ad hoc no requieren de infraestructura fija y permite que los dispositivos se muevan libremente. Entre las características de las redes Ad hoc se encuentra las topologías dinámicas y la capacidad reducida de ancho de banda.

En la figura 1.8, se muestra la topología de Red Adhoc

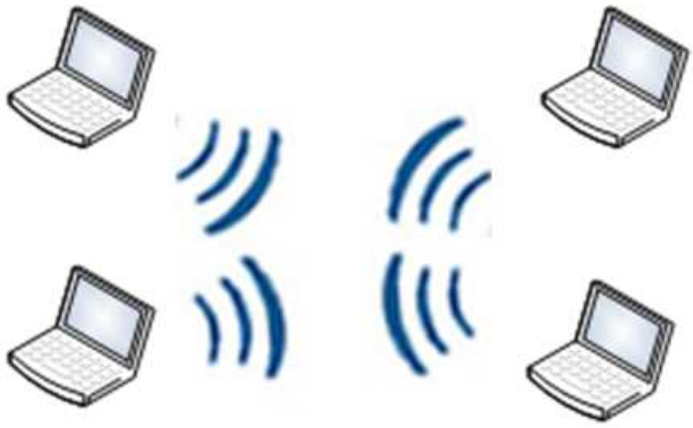


Figura 1. 8 Red Adhoc.

[15] **HIDALGO, Pablo;** "TELEMÁTICA"; EPN, 2010.

1.1.5.2 Redes de infraestructura.

Las redes de infraestructura usan un Punto de Acceso para controlar la asignación del tiempo de transmisión para todas las estaciones y también añade seguridad. En el caso en que un Punto de Acceso no suministre la cobertura necesaria, se puede unir uno o más APs, tal como se muestra en la figura 1.9.

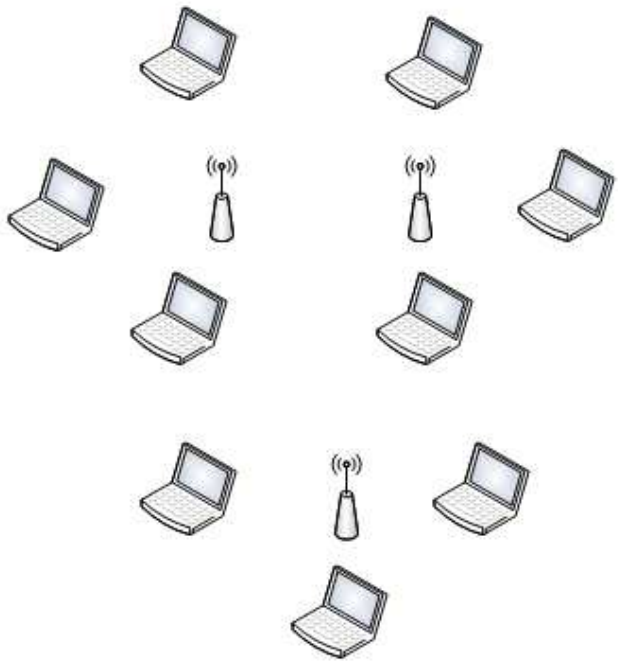


Figura 1. 9 Red de Infraestructura.

1.2 ESTÁNDAR IEEE 802.11[16].

1.2.1 INTRODUCCIÓN.

El Instituto de Ingenieros en Electricidad y Electrónica (IEEE), se encarga de definir los estándares que se utilizan en la electrónica y sistemas computacionales, entre ellos, el que define y gobierna las redes de área local inalámbricas (WLAN).

[16] ESTÁNDAR IEEE 802.11.- http://www.x-net.es/tecnologia/wireless.pdf

Los estándares definidos para las redes de área local inalámbricas son:

1. IEEE 802.11 a.
2. IEEE 802.11 b.
3. IEEE 802.11 g.
4. IEEE 802.11 n.

1.2.2 IEEE 802.11 b.

Esta extensión del estándar 802.11, también conocido como Ethernet Inalámbrico, permite velocidades de 5,5 y 11 Mbps en el espectro de los 2,4 GHz. Emplea el método de acceso CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance - Acceso Múltiple por Detección de Portadora).
En la tabla 1.2, se indican los canales del estándar 802.11 b con sus respectivas frecuencias.

Número de Canal	Frecuencia (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Tabla 1. 2 Canales definidos en el Estándar 802.11b[17].

[17] Canales definidos en el estándar IEEE 802.11 g.- **BERNAL, Iván**; "COMUNICACIONES INALÁMBRICAS", EPN 2010.

1.2.3 IEEE 802.11 g.

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. El IEEE 802.11 g posee los siguientes elementos obligatorios y opcionales:

- El método OFDM (*Orthogonal Frequency Divsion Multiplexing - Multiplexación por División de Frecuencias Ortogonales*) es obligatorio y permite alcanzar altas velocidades en la banda de 2,4 GHz.

- Los sistemas deben ser totalmente compatibles con IEEE 802.11b.

En la 802.11 g hay dos modelos de canales definidos, un modelo americano FCC (*Federal Communications Commission – Comisión Federal de Comunicaciones*) y un modelo ETSI/MKK (modelo Europeo).

La tabla 1.3, indica las asignaciones del estándar 802.11 g.

Número de Canal	FCC (GHz)	ETSI/MKK (GHz)
1	2.412	2.412
2	2.417	2.417
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457
11	2.462	2.462

Número de Canal	FCC (GHz)	ETSI/MKK (GHz)
12	—	2.467
13	—	2.472

Tabla 1. 3 Canales definidos en el Estándar 802.11b/g[18].

1.2.4 IEEE 802.11 a.

El estándar IEEE 802.11 a, se aplica a la banda de los 5 GHz, también conocida como banda UNII (*Unicensed National Information Infraestructure - Infraestructura de Información Nacional sin Licencia*), para la transmisión de datos emplea el método OFDM, ofreciendo una velocidad de hasta 54 Mbps.
Las señales que operan en la banda de los 5 GHz, se atenúan de manera considerable frente a la presencia de obstáculos.
La ventaja que brinda este estándar, es la baja interferencia que pueden sufrir los dispositivos debido a que pocos equipos trabajan en este rango de frecuencias.

1.2.5 IEEE 802.11 n.

El estándar 802.11 n fue propuesto en el año 2007 y es compatible con los estándares 802.11 a/b/g. La velocidad de transmisión puede alcanzar 600 Mbps, emplea tecnología MIMO (Multiple input, Multiple Output) (*Múltiples Entradas, Múltiples salidas*), que permite utilizar varios canales a la vez para enviar y recibir datos. Opera en la banda de los 2,4 GHz y en los 5 GHz.

En la tabla 1.4, se indica un resumen de los estándares con sus principales características.

[18] Canales definidos en el estándar IEEE 802.11 b/g.- **BERNAL, Iván**; "COMUNICACIONES INALÁMBRICAS", EPN 2010.

	802.11ª	802.11b	802.11g		802.11n
BANDA	5.7GHz	2.4GHz	2.4GHz		2.4 GHz y 5 GHz
MODULACIÓN	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
VELOCIDAD DE LOS DATOS	54 Mbps	11 Mbps	11 Mbps	54 Mbps	Posiblemente: 600 Mbps
RANGO	35 m	35 m	35 m		70 m
FECHA DE LANZAMIENTO	Octubre 1999	Octubre 1999	Junio de 2003		Septiembre 2009
VENTAJAS	Menos susceptible a interferencia.	Bajo costo, buen alcance.	Buen alcance, difícil de obstruir.		Buenas velocidades de transferencia de datos, alcance mejorado.
DESVENTAJAS	Costo superior	Lenta, susceptible a interferencia.	Susceptible a interferencia en la banda de 2.4 GHz.		

Tabla 1. 4 Estándares de LAN inalámbricas[19].

1.3 NAT (TRADUCCIÓN DE DIRECCIONES DE RED)[20].

Es un mecanismo utilizado por los routers para traducir direcciones privadas a direcciones públicas o públicas a privadas. El mecanismo de Traducción de Direcciones de Red brinda grandes utilidades, por ejemplo el ahorro de direcciones IP, al permitir que las redes utilicen direcciones IP privadas.

1.3.1 TERMINOLOGÍA.

En NAT se maneja la siguiente terminología:

- Dirección local interna.- Es la dirección IP de un equipo interno, en la mayoría de las veces es una dirección RFC1918 privada.

[19] Estándares de LAN inalámbricas. - Curriculum CCNA 3 -"Conmutación y conexión Inalámbrica de LAN"

[20] NAT.- http://es.scribd.com/doc/17482630/Cisco-CCNA-4-Exploration-Acceso-a-La-Wan-Version-40-Espanol

- Dirección global interna.- Dirección pública válida que se asigna al host interno cuando sale del router NAT.
- Dirección global externa.- Dirección IP asignada a un host en Internet.
- Dirección local externa.- Dirección IP asignada a un host en la red externa.

Existe tres tipos de traducción NAT:

1. Estática.
2. Dinámica.
3. Sobrecarga de NAT.

1.3.1.1 Estática.

Se realiza una asignación uno a uno, en la que una dirección IP privada se traduce a una correspondiente dirección IP pública de forma unívoca. Normalmente se utiliza cuando un dispositivo necesita ser accesible desde fuera de la red privada.

1.3.1.2 Dinámica.

Para la asignación se usa un conjunto de direcciones IP públicas y las asigna según el orden de llegada. Cuando un host con una dirección IP privada solicita acceso a Internet, la traducción NAT dinámica elije una dirección IP del conjunto de direcciones que no esté siendo utilizada por otro host.

1.3.1.3 Sobrecarga de NAT.

Es también conocida como traducción de la dirección del puerto (PAT Port Address Translation). Asigna varias direcciones IP privadas a una única dirección IP pública o a un grupo pequeño de direcciones IP públicas. La sobrecarga de NAT asegura que los clientes utilicen un número de puerto TCP o UDP diferente para cada sesión de cliente con un servidor de Internet.

1.4 CÁMARAS IP[21].

1.4.1 INTRODUCCIÓN.

Las cámaras IP (también conocidas como cámaras de Red) son videocámaras que capturan y transmiten tanto señales de video digitalizadas como señales de audio a través de una red de datos. Las cámaras IP poseen internamente una serie de aplicaciones y funciones como un servidor WEB, servidor FTP, cliente de correos, administración de alarmas, que permiten transmitir y almacenar secuencias de imágenes, las mismas que pueden ser almacenadas en equipos informáticos situados en una LAN o en una WAN, para verificar posteriormente eventos que han sucedido en lugares vigilados.

Para la transmisión de imágenes las cámaras IP, pueden estar conectadas a un Router ADSL para acceder desde el Internet o a un concentrador (HUB, Switch) para acceder desde una Red de Área Local, tal como se indica en la figura 1.10.

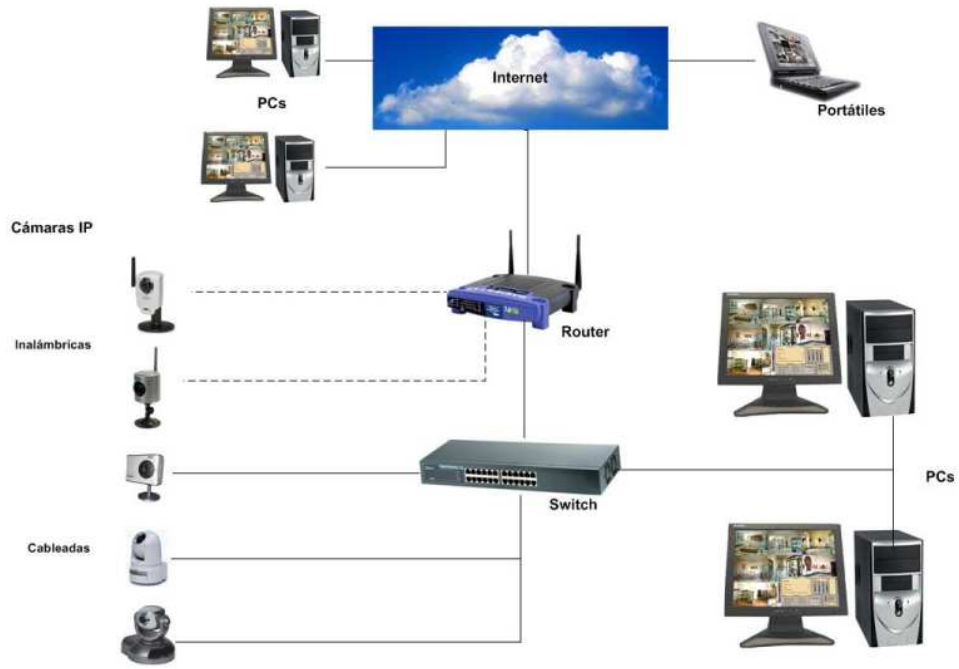


Figura 1. 10 Conexión de una cámara IP a Internet[22].

[21] CAMARAS IP. - http://www.gscssoftware.com/teccamaraip.htm

1.4.2 COMPONENTES INTERNOS DE LAS CÁMARAS IP.

Las cámaras IP poseen los siguientes componentes:

- Cámara de Video.
- Sistema de Compresión de imagen.
- Sistema de Procesamiento.

A continuación se detallan las funciones de cada uno de los principales componentes de las cámaras IP.

1.4.2.1 Cámara de Video.

En esta sección se encuentran elementos tales como: lentes, sensores y el procesador digital de imagen. Inicialmente el lente de la cámara enfoca la imagen, la misma que pasa a través del filtro óptico, el cual remueve luz infrarroja para que los colores sean mostrados correctamente y finalmente el sensor de imagen transforma las ondas de luz en señales eléctricas, para posteriormente ser convertido a señales digitales.

1.4.2.2 Sistema de Compresión de imagen.

Su principal función es comprimir las imágenes captadas por la cámara en formatos que contengan menos datos y pueden ser transmitidos por la red en forma eficiente, estos formatos son el JPEG, MPEG, MPEG4, entre otros.

1.4.2.3 Sistema de Procesamiento.

El sistema de procesamiento se encarga de la gestión de imágenes, del movimiento de la cámara y de la detección del movimiento. Este sistema está formado por Procesadores, Memoria Flash, software de administración y un módulo Ethernet/WiFi que permiten manejar las aplicaciones de red.

---

[22] Conexión de una cámara IP a Internet. - http://segurmatic.com/about/diagrama-camaras-ip-21/

En la figura 1.11, se indican los componentes internos de una cámara IP.

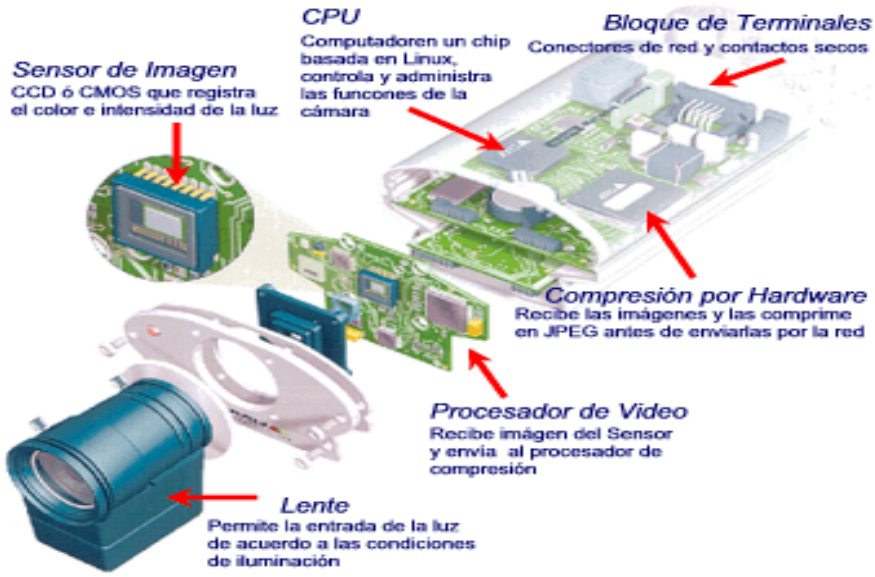


Figura 1. 11 Componentes Internos de una Cámara IP[23].

1.4.3 VENTAJAS Y DESVENTAJAS DE LAS CÁMARAS IP.

Las ventajas y desventajas de las cámaras IP son las siguientes:

- Las cámaras IP ofrecen mayor resolución a un menor costo en comparación con las cámaras de video tradicionales.
- Las cámaras IP permiten tener un acceso remoto a los eventos ocurridos en un determinado lugar.
- Las cámaras IP poseen una gran escalabilidad frente a una ampliación del sistema de seguridad.
- Las cámaras IP gestionan automáticamente el nivel de luz de la imagen, los niveles de color, nitidez y calidad de la imagen.
- Algunas cámaras IP poseen sensores de movimiento.

[23] Componentes Internos de una cámara IP. - http://www.gscssoftware.com/teccamaraip.htm

- Algunas cámaras IP disponen de un filtro de infrarrojos automático, este filtro se coloca delante del CCD (*Charge Coupled Device – Dispositivo de Carga Acoplada*) sólo cuando las condiciones de luz son adecuadas, proporcionándonos de esta manera imágenes en color cuando las condiciones de luz bajan, este filtro se desplaza y la cámara emite la señal en blanco y negro produciendo más luminosidad y de esta manera podemos iluminar la escena con luz infrarroja y ver en total oscuridad.
- Las cámaras IP presentan facilidad de instalación, ya que simplemente se realiza la configuración TCP-IP y se empieza a transmitir el video.
- Las cámaras IP no necesitan de un computador para funcionar.
- Las cámaras IP de diferentes fabricantes no son compatibles entre sí, esto significa que si se desea hacer un remplazo de los componentes físicos o del software de administración de la cámara presentan incompatibilidad entre sí.
- Otra desventaja que presentan las cámaras IP son los retrasos en el streaming de video.
- No existen Normas Internacionales que regulen el estándar de compresión de imágenes de las cámaras IP.
- Al momento de trabajar con altas resoluciones o una gran cantidad de cámaras IP, el consumo de ancho de banda se incrementa, provocando que los equipos de conectividad se encarezcan.

1.4.4 APLICACIONES DE LAS CÁMARAS IP.

Las principales aplicaciones de las cámaras IP se encuentran en el monitoreo y vigilancia de propiedades, personas, lugares, maquinaria, zonas turísticas, etc. Estas aplicaciones son ilimitadas y presentan la ventaja de que el video al ser transmitido por la red, puede ser consultado en cualquier lugar del mundo.
A continuación se describen aplicaciones de monitoreo y vigilancia con cámaras IP.

- Monitoreo y vigilancia Urbana y lugares públicos.
- Monitoreo y vigilancia residencial con o sin manejo de alarmas.

- Monitoreo y vigilancia de oficinas, fábricas y negocios.
- Monitoreo y vigilancia de escuelas y hospitales.
- Monitoreo y vigilancia de casinos.
- Monitoreo y vigilancia de Bancos, Casas de Bolsa, Aseguradoras, Casas de Cambio.
- Monitoreo y vigilancia de Obras de Construcción.
- Monitoreo y vigilancia de Museos.
- Monitoreo y vigilancia de Carreteras y vías de comunicación.
- Monitoreo y vigilancia de Equipo y Maquinaria.
- Monitoreo y vigilancia de enfermos, niños, ancianos y mascotas.

1.4.5 MÉTODOS DE COMPRESIÓN DE LAS CÁMARAS IP[24].

Al momento de digitalizar una secuencia de video analógico, se requiere un ancho de banda muy elevado, empleando esta cantidad no es posible transmitir en una LAN, debido a que la mayoría de redes de datos trabajan con equipos que usan la tecnología Fast Ethernet. Existen diferentes técnicas de compresión de video e imágenes que nos permiten superar este inconveniente.
La compresión de video se realiza sobre una serie consecutiva de imágenes, haciendo uso de las similitudes entre imágenes próximas; mientras que la compresión de imágenes se aplica sobre una única imagen individual empleando las similitudes entre píxeles próximos y haciendo uso de las limitaciones del ojo humano.

La efectividad de una técnica de compresión de imágenes viene dada por la relación de compresión, la cual se calcula considerando el tamaño del archivo de la imagen original (sin comprimir) dividido por el tamaño del archivo de imagen resultante (comprimida). A mayor relación de compresión se consume menos ancho de banda, manteniendo un número de imágenes por segundo determinado.

[24] METODOS DE COMRESION DE LAS CÁMARAS IP.- http://www.voxdata.com.ar/voxcompresionvideo.html

Al mismo tiempo, un mayor nivel de compresión implica menor nivel de calidad de imagen para cada imagen individual.

1.4.5.1 Compresión de imágenes M-JPEG.

M-JPEG (*Motion JPEG - JPEG en Movimiento*), es un nombre trivial para aquellos formatos multimedia donde cada fotograma o campo entrelazado de una secuencia de vídeo digital es comprimida por separado como una imagen JPEG. Es frecuentemente usado en dispositivos portátiles tales como cámaras digitales, cámaras IP y cámaras WEB.

JPEG fue desarrollado por el Grupo de Expertos de Fotografía (Joint Photographic Group) y fue estandarizado en los años 80. Este método de compresión emplea la transformada directa del coseno consiguiendo una compresión ajustable a la calidad de la imagen que se desea reconstruir.
Cuando se usa una alta compresión, la imagen resultante sufre alta degradación.

1.4.5.2 Compresión de video MPEG.

MPEG (*Motion Picture Experts Group - Grupo de Expertos en Imágenes Móviles*). En este método de compresión de video, la información se comprime en pequeños paquetes para ser transmitidos fácilmente y posteriormente descomprimidos. MPEG alcanza su alta tasa de compresión almacenando solamente los cambios de un frame al siguiente, en vez de almacenar el frame entero. Con este método de compresión se pierden ciertos datos siendo imperceptible al ojo humano.

1.4.5.3 Compresión de video MPEG 4.

MPEG 4 es un formato de compresión MPEG y fue aprobado en el año 2000. Este algoritmo de compresión de video está basado en la tecnología MPEG 1, MPEG 2 y Apple QuickTime. Al emplear MPEG 4 los archivos resultantes son

pequeños en comparación a los archivos JPEG, de esta manera este algoritmo de compresión es ideal para transmitir video e imágenes a través de un canal limitado.

1.5 DESCRIPCIÓN DEL SOFTWARE ZONEMINDER.

1.5.1 INTRODUCCIÓN[25].

ZoneMinder es un conjunto integrado de aplicaciones que proporcionan una solución completa de vigilancia permitiendo la captura, análisis, registro y seguimiento de streaming de video generado por un dispositivo de video conectado a una computadora que utilice un sistema operativo Linux. Está diseñado para funcionar en distribuciones que soportan la interfaz Video para Linux y ha sido probado con cámaras de video asociadas a tarjetas conversoras analógico digital (BTTV), cámaras USB y cámaras IP.

ZoneMinder está diseñado en torno a una serie de componentes independientes que trabajan únicamente cuando sea necesario limitando de esta manera el consumo innecesario de recursos y maximizando la eficiencia de un computador; incluso si se monitorea un gran número de cámaras, la CPU no se sobrecarga.

Así como Zoneminder es rápido, también es amigable con el usuario ya que cuenta con una interfaz web muy comprensiva escrita en PHP (*Hypertext Preprocessor – Preprocesador Hipertexto)*, la cual permite el control y monitoreo de cámaras con la ayuda de un computador conectada a una red de datos. La interfaz web permite observar eventos capturados por las cámaras, archivar y revisar posteriormente las veces que sean necesarias y eliminarlas si no son de gran utilidad. La interfaz web interactúa de forma directa con los demonios del sistema, para asegurar la cooperación entre ellos. Además Zoneminder puede ser

[25] INTRODUCCION. – www.zoneminder.com

instalado como un servicio, brindando la posibilidad de ejecutarse automáticamente cada vez que se reinicie el servidor.

El núcleo de Zoneminder es la captura y análisis de imágenes, por lo que hay una gran cantidad de parámetros configurables, que nos permite eliminar falsas alarmas generadas por eventos sin trascendencia. Zoneminder permite definir un conjunto de zonas con diferentes tipos de sensibilidad permitiendo la activación de una alarma en caso de movimiento.

Con la ayuda de Zoneminder se puede acceder al circuito cerrado de televisión, ya sea por la intranet o desde internet.

Zoneminder es distribuido bajo licencia GPL (*General Public Licens - Licencia Pública General*). Este programa es software libre, lo cual permite distribuirlo y/o modificarlo sin ningún costo.

En la figura1.12, se indica el logo de Zoneminder.

Figura 1. 12 Logo de ZoneMinder.

1.5.2 CARACTERÍSTICAS DEL SOFTWARE ZONEMINDER[26].

A continuación se describe un conjunto de características específicas del software Zoneminder.

[26] CARACTERÍSTICAS. - http://www.zoneminder.com/documentation

- 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.

1.5.3 REQUERIMIENTOS DEL SOFTWARE ZONEMINDER[27].

1.5.3.1 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.

1.5.3.2 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.

1.5.3.2.1 Requerimientos Mínimos.

- Procesador Pentium III o AMD Atlon.
- Memoria 128 MB.
- Tarjeta de red Ethernet 10 Mbps.
- Tarjeta gráfica 32 MB (para visualizar el video).
- 300 MB de espacio en disco duro.

[27] REQUERIMIENTOS DEL SOFTWARE ZONEMINDER.- http://www.zoneminder.com/wiki/index.php/Documentation

NOTA: Estos requerimientos son para procesar el streaming de un solo dispositivo de video.

1.5.3.2.2 Requerimientos Recomendados.

- Procesador Dual Core o AMD Turion x2.
- Memoria 1GB.
- Tarjeta de red FastEthernet 100 Mbps.
- Tarjeta gráfica 128 MB (para visualizar el video).
- 1 GB de espacio en disco duro.

1.5.4 COMPONENTES DEL SOFTWARE ZONEMINDER[28].

ZoneMinder no es una aplicación independiente, sino que se forma a partir de varios componentes. Estos componentes incluyen ejecutables que hacen el trabajo de procesamiento de video, scripts en PERL que realizan procesos en interfaces externas y scripts en PHP que se utilizan para la ejecución de la interfaz web.

Los principales demonios que ZoneMinder utiliza son:

- ZMC.
- ZMA.
- ZMF.
- ZMS.
- ZMU.

A continuación se realiza una descripción de cada uno de los principales componentes.

[28] COMPONENTES DEL SOFTWARE ZONEMINDER.- http://www.zoneminder.com/wiki/index.php/Documentation

1.5.4.1 Demonios (Archivos PHP).

ZMC.

ZMC es el demonio "Captura" de ZoneMinder. El trabajo de este demonio consiste en monitorear un dispositivo de vídeo y captar cuadros tan rápido como sea posible, funcionando a una velocidad prácticamente constante.

ZMA.

ZMA es el demonio "Análisis" de ZoneMinder. El trabajo de este componente es ir a través de los cuadros capturados y revisarlos para verificar si existe movimiento, lo que podría generar una alarma o evento. Por lo general, se mantiene a la par con el demonio Captura, pero si se encuentra con exceso de procesamiento puede omitir algunas imágenes para no desfasarse.

ZMF.

ZMF es el demonio "Frame de ZoneMinder". Este es un demonio opcional que puede ser ejecutado en conjunto con el demonio Análisis siendo su trabajo grabar los cuadros capturados en el disco de almacenamiento.

ZMS.

ZMS es el demonio "Streaming server de Zoneminder". La interfaz web se enlaza con este demonio para obtener el video en tiempo real o video almacenado. Este se ejecuta cuando se tiene streaming de video producido por una cámara o cuando se monitorea usando la interfaz web; y se detiene una vez concluido el streaming de video o cuando se cierra la página web.

ZMU.

ZMU es el demonio “Utilidad” de Zoneminder; básicamente es una interfaz de línea de comando que permite depurar manualmente errores de Video.

1.5.4.2 Scripts en PERL.

Un Script en PERL es un conjunto de instrucciones que al ser compilados interactúan con el sistema operativo o con el usuario.

Los scripts en PERL que utiliza Zoneminder son:

- Zmpkg.pl.
- Zmdc.pl.
- Zmfilter.pl.
- Zmaudit.pl
- Zmwatch.pl.
- Zmupdate.pl.
- Zmvideo.pl.
- Zmcontrol.pl.

A continuación, se describe los scripts que utiliza ZoneMinder.

zmpkg.pl.

zmpkg.pl es el script de control “Paquete”. Es usado por la interfaz web y por scripts de servicios para controlar la ejecución del sistema como uno solo.

zmdc.pl.

zmdc.pl es el script de control “Demonio”. Es usado por la interfaz web y por el script de control “zmpkg.pl” y mantiene la ejecución de los demonios “captura” y “análisis”.

zmfilter.pl.

zmfilter es el script “Filtro” y controla la ejecución de filtros creados y almacenados, es iniciado y detenido por la interfaz web.

zmaudit.pl.

zmaudit es el script “Auditoría” y es usado para comprobar la coherencia de la base de datos generados por cada uno de los eventos. Tiene también la función de eliminar eventos huérfanos.

zmwatch.pl.

zmwatch.pl es el script “Reloj” su única función es monitorear al demonio “Captura” y reiniciarlo si este se detiene o deja de responder.

zmupdate.pl.

zmupdate.pl es el script “Actualización” y es responsable de comprobar si existen nuevas versiones de ZoneMinder y de otro conjunto de actualizaciones, como por ejemplo parches o scripts para diferentes tipos de cámaras. Este es el único script autorizado a realizar este tipo de acciones.

zmvideo.pl

Este script es usado desde la interfaz web para generar los archivos de video en diferentes tipos de formatos. Este demonio puede ser ejecutado por línea de comandos para depurar errores.

zmcontrol.pl.

zmcontrol.pl. son un conjunto de scripts que son usados para controlar las cámaras tipo Pan/Tilt/Zoom. Cada script convierte un conjunto de comandos que se usan para el control de las cámaras en un protocolo entendible para ellas. Además del control PTZ pueden controlar el brillo, nitidez, focus, etc.

zm.

zm es un script, el cual se encarga de detener, iniciar o reiniciar a Zoneminder.

1.5.4.3 Módulos en PERL[29].

Los módulos en PERL son usados por los scripts PERL para realizar cada una de las funciones ya descritas anteriormente. Estos Módulos tienen extensión .pm.
Los módulos en PERL que ZoneMinder utiliza son:

- ZoneMinder.pm.
- Base.pm.
- Config.pm.
- Debug.pm.
- Database.pm.
- SharedMem.pm.
- ConfigAdmin.pm.

A continuación se describe a cada uno de estos módulos.

ZoneMinder.pm.

Es un módulo que contiene a varios componentes, los cuales son:

[29] MODULOS EN PERL.- http://www.zoneminder.com/wiki/index.php/Documentation

- Base.pm.
- Config.pm.
- Debug.pm.
- Database.pm.
- SharedMem.pm.

Cada uno se describe a continuación.

Base.pm.

Base.pm tiene como función enviar a ZoneMinder.pm la información relacionada a la versión instalada de ZoneMinder.

Config.pm.

Config.pm tiene como función el importar la configuración de ZoneMinder desde una base de datos.

Debug.pm.

Debug.pm contiene funciones de depuración y de error los cuales son usados por los scripts anteriormente mencionados, para generar información de diagnóstico en un formato estándar.

Database.pm.

Database.pm contiene funciones de acceso, modificación a la base de datos que necesita ZoneMinder para el registro de usuarios, configuraciones, registro de eventos, etc.

SharedMem.pm.

SharedMem.pm contiene funciones de acceso estándar a la memoria compartida. Puede ser usado para acceder a uno o a varios Monitores, así como desactivarlos o activarlos.

ConfigAdmin.pm.

ConfigAdmin.pm está especializado en mantener la información acerca de varias opciones de configuración.

1.6 PARÁMETROS DE CONFIGURACIÓN ZONEMINDERN[30].

1.6.1 INTRODUCCIÓN.

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 1.13, se indica la página principal de ZoneMinder.

Figura 1. 13 Página Principal de ZoneMinder.

[30] PARÁMETROS DE CONFIGURACIÓN ZONEMINDER. - http://www.zoneminder.com/wiki/index.php/Documentation

1.6.2 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 1.14.

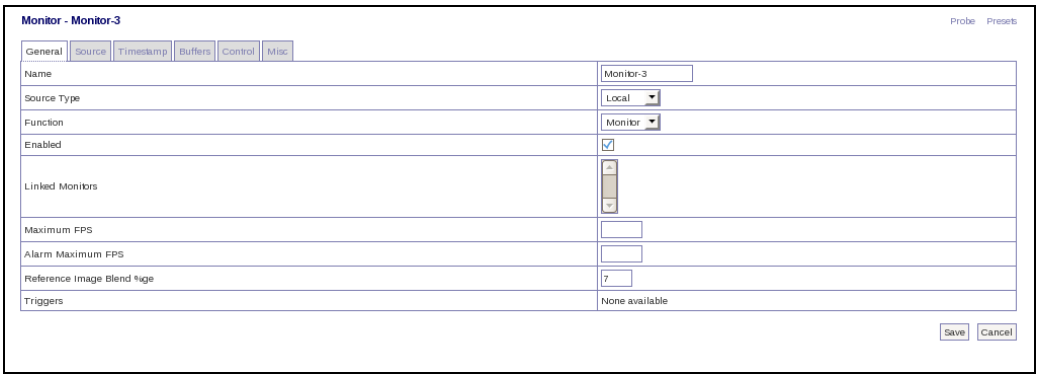


Figura 1. 14 Ventana de configuración para un nuevo monitor.

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.

1.6.2.1 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 serán 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.

1.6.2.2 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 1.15, se indica la ventana generada por la pestaña Fuente cuando se utiliza cámaras Web o cámaras de video analógicas.

Figura 1. 15 Ventana de configuración pestaña Fuente para dispositivos locales.

En la figura 1.16, se indica la ventana de configuración cuando se utiliza cámaras IP.

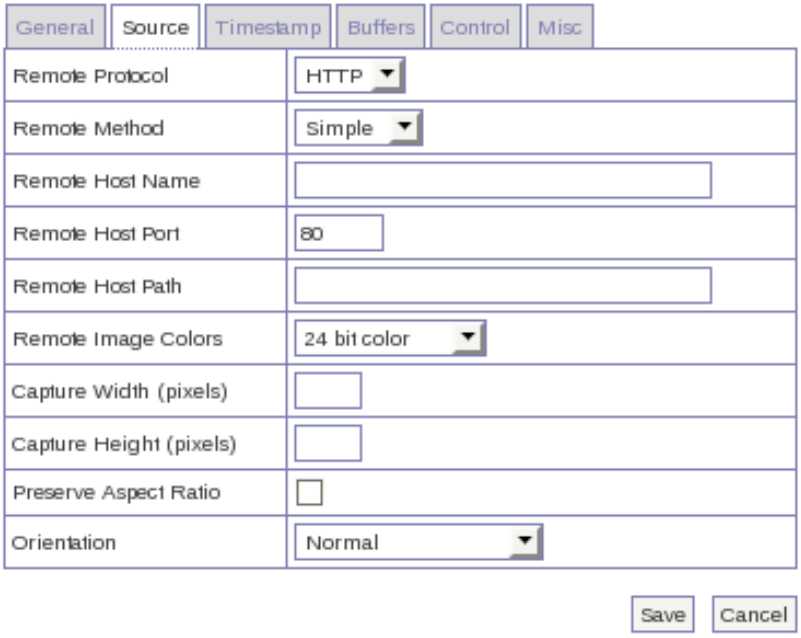


Figura 1. 16 Ventana de configuración pestaña Fuente para Dispositivos Remotos.

- **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.

1.6.2.3 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 1.17, se indica la ventana de configuración Marca de Tiempo.

Figura 1. 17 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.

1.6.2.4 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 1.18, se indica la pestaña Búfer.

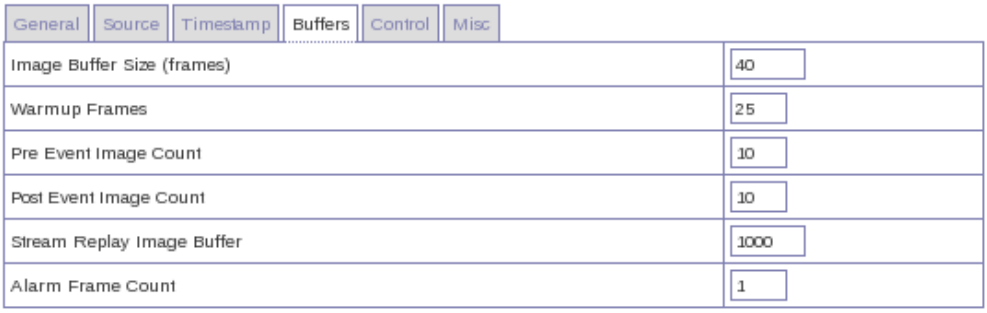


Figura 1. 18 Ventana de configuración de Búfer.

- **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.

1.6.2.5 Pestaña Control.

Las opciones de configuración para esta pestaña permiten determinar controles para manipular remotamente cámaras PTZ. En la figura 1.19, se indica la pestaña control.

Figura 1. 19 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.

1.6.2.6 Pestaña Miscelánea (Misc Tab).

Las opciones de configuración para esta pestaña permiten configurar ciertos aspectos relacionados a los eventos. En la figura 1.20, se indica la pestaña Miscelánea.

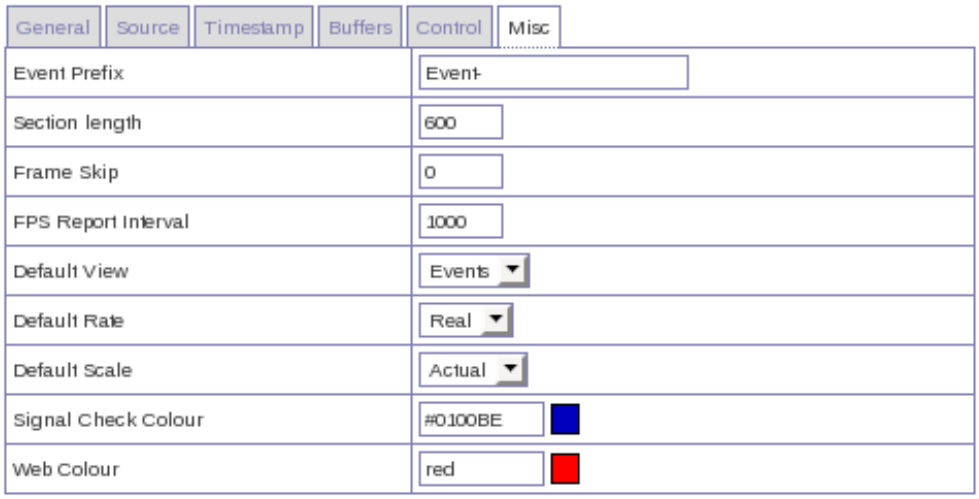


Figura 1. 20 Pestaña de configuración Miscelánea.

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

- **Campo Longitud de Sección (*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.

1.6.3 USUARIOS Y NIVELES DE ACCESO[31].

1.6.3.1 Introducción.

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 1.21, se indica la Pestaña usuarios.

Figura 1. 21 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 1.22.

[31] USUARIOS Y NIVELES DE ACCESOS. - http://www.zoneminder.com/wiki/index.php/Documentation

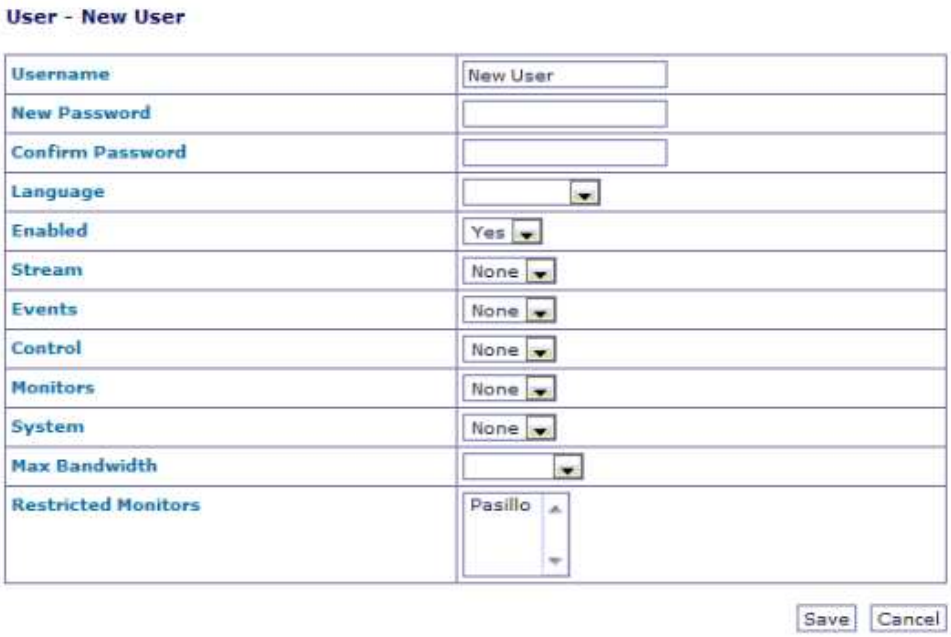


Figura 1. 22 Ventana Usuario Nuevo (*Add New User*).

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.

1.6.4 ZONAS DE VIGILANCIA[32].

1.6.4.1 Introducción.

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 1.23, se indican los campos de configuración de Zonas de Vigilancia.

[32] ZONAS DE VIGILANCIA. - http://www.webtense.es/?p=80

Figura 1. 23 Ventana agregar/editar/eliminar Zona de Vigilancia.

Al agregar o editar una zona de vigilancia se obtendrá lo que se indica en la figura 1.24.

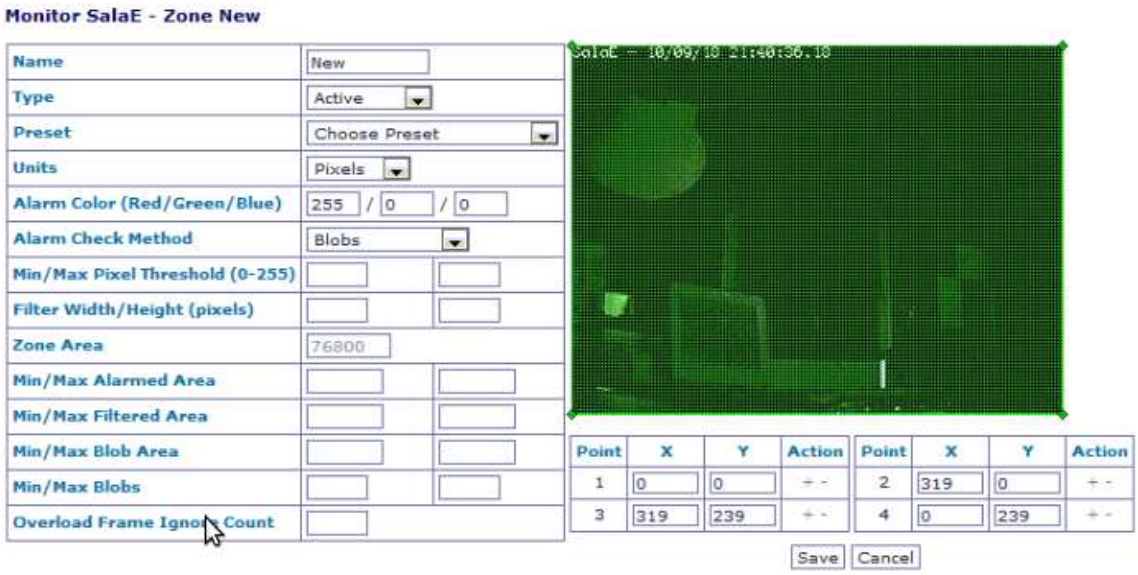


Figura 1. 24 Ventana agregar/editar/eliminar Zona de Vigilancia.

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.

BIBLIOGRAFÍA.

Tutoriales.

HIDALGO, Pablo; "TELEMÁTICA"; EPN, 2010.

TANEMBAUM, Andrew; "Redes de Computadoras"; 3ra Edición; 1997; Prentice-Hall; Inc.

Curriculum CCNA 3 -"Conmutación y conexión Inalámbrica de LAN"

Páginas de Internet.

http://es.wikipedia.org/wiki/Red_de_computadoras.

http://www.wordpress.com/2007/09/21/estandar-y-seguridad-80211/

http://es.wikipedia.org/wiki/Enrutador

http://www.x-net.es/tecnologia/wireless.pdf

http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

http://www.gscssoftware.com/teccamaraip.htm

http://www.voxdata.com.ar/voxcompresionvideo.html

http://www.zoneminder.com

http://www.zoneminder.com/documentation

http://www.zoneminder.com/wiki/index.php/Documentation

http://www.webtense.es/?p=80

CAPÍTULO II

2. DISEÑO E IMPLEMENTACIÓN DEL CIRCUITO CERRADO DE TELEVISIÓN CON CÁMARAS IP.

2.1 INTRODUCCIÓN.

En este capítulo se presenta el diseño e implementación del Circuito Cerrado de Televisión con Cámaras IP, previamente se realiza una descripción de la situación actual del Laboratorio de Informática del Edificio de Eléctrica-Química; es decir, número y distribución de las aulas, área de cada una de ellas y de todo el Laboratorio, capacidad de estudiantes, entre otros; estos parámetros nos permitirán establecer los requerimientos de la red a diseñarse. También se presenta el cálculo del ancho de banda, direccionamiento IP y configuración del Servidor. Para la implementación se emplea equipos de conectividad y servidores proporcionados por el Laboratorio de Informática. Para la selección de cámaras IP se realiza una comparación entre varias alternativas, para finalmente seleccionar las cámaras IP más adecuadas.

2.2 SITUACIÓN ACTUAL DEL LABORATORIO DE INFORMÁTICA.

El Laboratorio de Informática se encuentra ubicado en el sexto piso del edificio de Eléctrica-Química, el ingreso se lo realiza por dos accesos peatonales a los cuales se llega a través de:

- Un pasillo central que se encuentra en el sexto piso.
- Gradas que provienen del séptimo y quinto piso.

En la figura 2.1, se indica la entrada principal al Laboratorio de Informática.

Figura 2. 1 Entrada y Salida Principal al Laboratorio de Informática.

El Laboratorio de Informática posee una gran cantidad de equipos computacionales y de conectividad de la Academia ACIERTE y de la Escuela Politécnica Nacional, actualmente el Laboratorio cuenta con escasos sistemas de vigilancia, por este motivo es necesario monitorear todas las actividades realizadas en el interior del Laboratorio con el propósito de garantizar su

seguridad, de esta manera si existe algún evento inusual tener registrado en video cada una de las actividades.

2.2.1. DESCRIPCIÓN FÍSICA DEL LABORATORIO DE INFORMÁTICA.

El Laboratorio de Informática tiene un área aproximada de 424.53 m^2, se encuentra dividido de la siguiente manera:

- Una entrada principal.
- Una entrada posterior.
- Cinco aulas ubicadas en el sexto piso.
- Un taller de computadores en donde se encuentran los servidores ubicada en el séptimo piso.
- Una cafetería.
- Un pasillo central.
- Baterías sanitarias de Damas.
- Baterías sanitarias de Caballeros.

2.2.1.1. Descripción de las Aulas.

Cada una de las cinco aulas posee 20 computadores y se acostumbra a que cada estudiante trabaje en un computador. Las cinco aulas poseen una distribución similar y una altura idéntica.

En la Sala D donde se ubica el Rack de comunicaciones, el cual tiene una dimensión de 48 Unidades de Rack o 2.14 metros de altura, está formado por diferentes equipos de conectividad como Switch de Acceso y un Switch de Distribución pertenecientes a la Polired, los mismos que sirven para brindar conectividad al edificio de Eléctrica-Química.

En la tabla 2.1, se indica el área en metros cuadrados y la capacidad de estudiantes por cada aula.

Distribución de Aulas	Área [m^2]	Altura [m]	Capacidad de Estudiantes
Sala A	47,53	3,40	20
Sala B	54,70	3,40	20
Sala C	54,24	3,40	20
Sala D	57	3,40	20
Sala E	57,40	3,40	20

Tabla 2. 1 Distribución de las aulas en el Laboratorio de Informática.

2.2.1.2. Descripción de la Entrada Principal y Pasillo Central.

La entrada principal, tiene una extensión de 9 [m]**,** es usado como acceso peatonal y como lugar de descanso antes de ingresar a clases. El número aproximado de auxiliares que realizan prácticas pre-profesionales en el Laboratorio de Informática es 12, los cuales utilizan este espacio en diferentes horarios. Los auxiliares de Laboratorio ayudan a controlar el ingreso y salida por la entrada principal.

El pasillo central atraviesa el Laboratorio de Informática y tiene una extensión de 13 [m].

2.2.1.3. Descripción de la Cafetería.

La cafetería tiene un área de 47.51 [m^2] y una altura de 3,40 [m], es usada para almacenar los equipos de conectividad de la Academia ACIERTE. Los equipos de conectividad son costosos y son usados con fines didácticos por parte de la academia ACIERTE, la seguridad para proteger estos bienes es mínima, por lo cual es necesario incrementar la seguridad.

2.2.2 DESCRIPCIÓN DE LA SEGURIDAD FÍSICA DEL LABORATORIO DE INFORMÁTICA.

El Laboratorio de Informática tiene dos puntos de accesos, el primero es la puerta de ingreso principal, ubicada en el sexto piso, cuyas puertas y las ventanas son protegidas por rejas metálicas. Al segundo punto de acceso se llega desde el quinto y séptimo piso y posee una puerta metálica plegable.

En la figura 2.2, se indica la entrada principal al Laboratorio de Informática.

Figura 2. 2 Entrada Principal al Laboratorio de Informática.

En la figura 2.3, se indica la entrada posterior al Laboratorio de Informática.

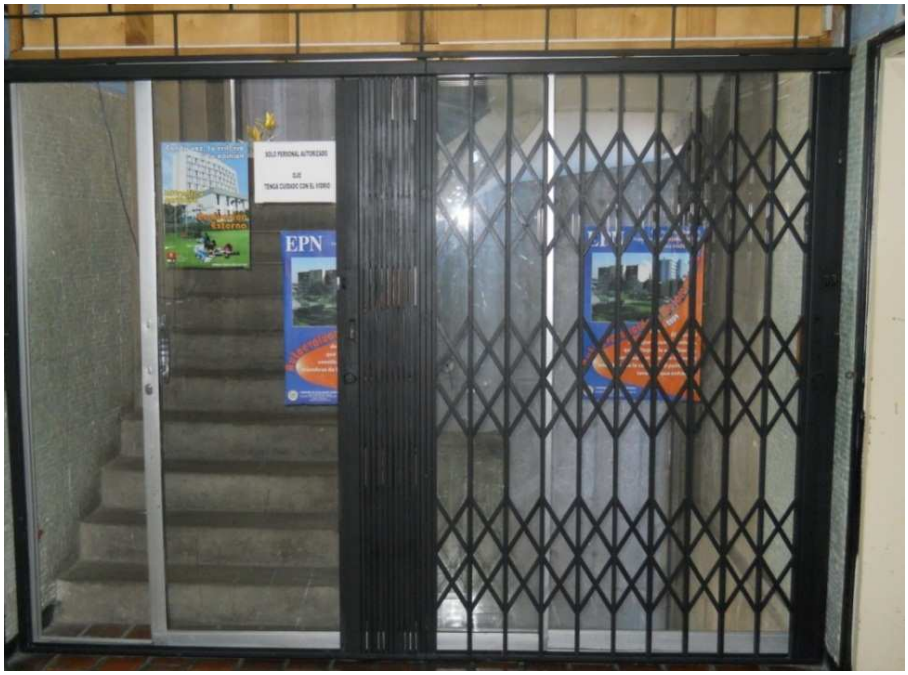


Figura 2. 3 Entrada posterior al Laboratorio de Informática.

2.2.2.1 Características de Seguridad del Laboratorio de Informática.

- El Laboratorio de Informática posee un sistema de seguridad que actualmente no está en funcionamiento.
- La entrada al pasillo central posee un mecanismo para abrir eléctricamente la puerta.
- En el interior del Laboratorio de Informática se cuenta con rejas metálicas que protegen cada una de las 5 aulas y la cafetería.
- No posee guardias de seguridad que vigilen exclusivamente el Laboratorio de Informática.

En la figura 2.4, se indica el interior del Laboratorio de Informática.

Figura 2. 4 Interior del Laboratorio de Informática.

2.2.3 DESCRIPCIÓN DE LA RED DATOS DEL LABORATORIO DE INFORMÁTICA.

El Laboratorio de Informática cuenta con una red de datos y una red inalámbrica que forman parte de la Polired. La red de datos posee una topología estrella extendida, en cada sala existe un Switch de Acceso Catalyst 2950, los mismos que permiten la comunicación entre cada una de las salas del Laboratorio de Informática. Estos switches se conectan a un Switch Catalyst 3560 de distribución ubicado en la Sala D, el cuál se enlaza a un Switch de Core ubicado en el edificio de Química.

El Laboratorio de Informática no posee un cuarto de equipos con las condiciones definidas en los estándares internacionales EIA/TIA (Electronic Industries Alliance / Telecommunications Industry Association - Asociación de Industrial Electrónicas

/ Asociación de las industrias de Telecomunicaciones) y no posee un sistema de backup eléctrico para los servidores, ni para los equipos de conectividad ubicados en la sala A, B, C, E.

La red Inalámbrica posee un router inalámbrico WRT300N que opera en los estándares 802.11 b/g/n. Actualmente la red inalámbrica tiene problemas de interferencia, lo que afecta su rendimiento. Este problema se origina por la presencia de una gran cantidad de redes inalámbricas que operan en los canales 1, 6 y 11.

En la figura 2.5, se indica el diagrama de red del Laboratorio de Informática y su salida hacia la UGI (Unidad de Gestión de Información).

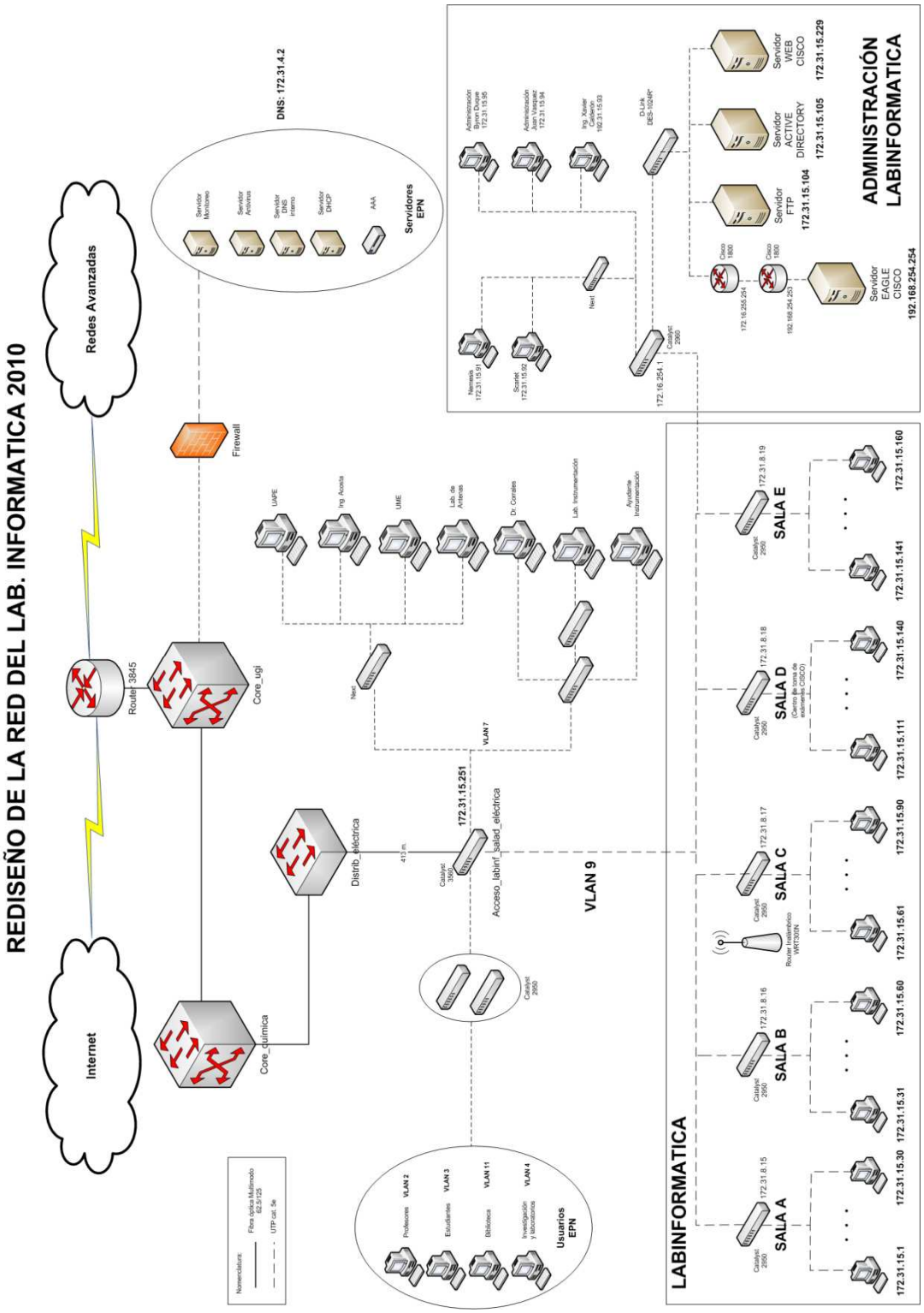


Figura 2. 5 Topología de la Red de Datos del Laboratorio de Informática y su salida hacia la Unidad de Gestión de la Información.

2.3 ESTABLECIMIENTO DE ZONAS DE RIESGO.

En base a la distribución física de las aulas, lugares de ingreso y la ubicación de los equipos de conectividad del Laboratorio de Informática, se estableció las siguientes zonas de riesgo:

- Zona de Riesgo No. 1: Entrada Principal.
- Zona de Riesgo No. 2: Entrada Secundaria.
- Zona de Riesgo No. 3: Cafetería.

Con el monitoreo continuo de estos puntos estratégicos se brindará un mejor control de las personas que ingresan o salen del laboratorio, movimientos inusuales cuando el laboratorio permanezca cerrado, se supervisará los equipos de conectividad evitando que estos dispositivos sean hurtados. Las características que el circuito cerrado de televisión con cámaras IP debe cumplir son:

- El Laboratorio de Informática debe contar con un circuito cerrado de televisión permanente, los 365 días, las 24 horas, que permita el monitoreo de sitios estratégicos como son puntos de ingreso al Laboratorio de Informática y cafetería.

- El circuito cerrado de televisión debe ser instalado en la infraestructura del Laboratorio y debe funcionar independientemente ante cualquier eventualidad, como son: ausencia de energía eléctrica, escasa iluminación e ingreso masivo de estudiantes.

- El servidor de grabación de video debe permitir la grabación y búsqueda de videos previamente almacenados.

- El Punto de Acceso Inalámbrico debe brindar una cobertura adecuada para que las cámaras IP se asocien con normalidad.

2.4 DISEÑO DEL CIRCUITO CERRADO DE TELEVISIÓN CON CÁMARAS IP.

2.4.1. PARÁMETROS DEL CIRCUITO CERRADO DE TELEVISIÓN.

Con el fin de brindar mayor seguridad a la infraestructura y a los usuarios del Laboratorio de Informática, se instala un circuito cerrado de televisión con cámaras IP con capacidad de monitorear las Zonas de Riesgo; enviando notificaciones de eventos inusuales al correo electrónico de la persona encargada del monitoreo.

2.4.2. REQUISITOS DEL CIRCUITO CERRADO DE TELEVISIÓN.

A partir de los parámetros citados anteriormente, se establece los requerimientos del circuito cerrado de televisión:

- Ubicación de cámaras en las Zonas de Riesgo como son entrada principal, entrada posterior y cafetería del Laboratorio de Informática. De este modo se asegura un completo monitoreo de las zonas estratégicas.

- Cámaras que permitan la grabación de actividades en ambientes diurnos y nocturnos.

- Realizar el dimensionamiento del UPS para que proporcione energía en el caso de corte de energía eléctrica.

- Calcular el ancho de banda aproximado y necesario para el óptimo funcionamiento del circuito cerrado de televisión.

- Realizar un direccionamiento IP que permita en un futuro incrementar el número de cámaras IP.

- Realizar el estudio del SiteSurvey para ubicar adecuadamente el Punto de Acceso Inalámbrico.

- Adaptar una sección del Cuarto de Servidores con la seguridad necesaria para la ubicación del servidor.

- Implementar políticas de seguridad para garantizar el manejo adecuado de la información de video almacenada.

En las figuras 2.6, 2.7 y 2.8, se indican las zonas de riesgo definidas para el Laboratorio de Informática.

Figura 2. 6 Zona de Riesgo No 1: Entrada Principal.

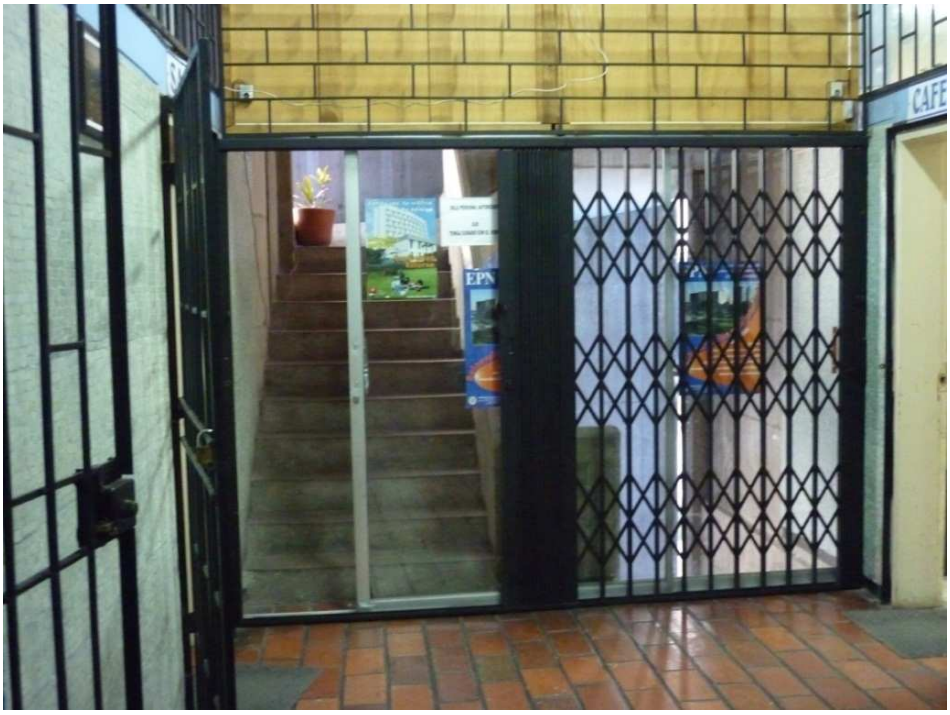


Figura 2. 7 Zona de Riesgo No. 2: Entrada Secundaria.

Figura 2. 8 Zona de Riesgo No. 3: Cafetería.

2.4.3. CÁLCULO DEL ANCHO DE BANDA.

El ancho de banda aproximado y necesario para una cámara IP depende de varios parámetros tal y como se indica en la figura 2.9.

Figura 2. 9 Parámetros que determinan el cálculo aproximado del Ancho de Banda en una cámara IP.

Todos los parámetros indicados en la figura 2.9 permiten obtener un cálculo aproximado del ancho de banda; a continuación se analiza cada uno de estos componentes.

2.4.3.1 Sobrecarga por encapsulamiento.

Este término hace referencia a los bits generados por el encapsulamiento de datos de información por parte de capas superiores. Estos bits generados por cada encapsulamiento corresponden a:

- Direccionamiento.
- Reglas para la transferencia de la información.
- Control de Errores.
- Secuenciamiento de mensajes.
- Control de Flujo.
- Manejo de mensajes de diferente Tamaño.
- Capacidad de Multiplexación.

En la figura 2.10, se indica el encapsulamiento de datos.

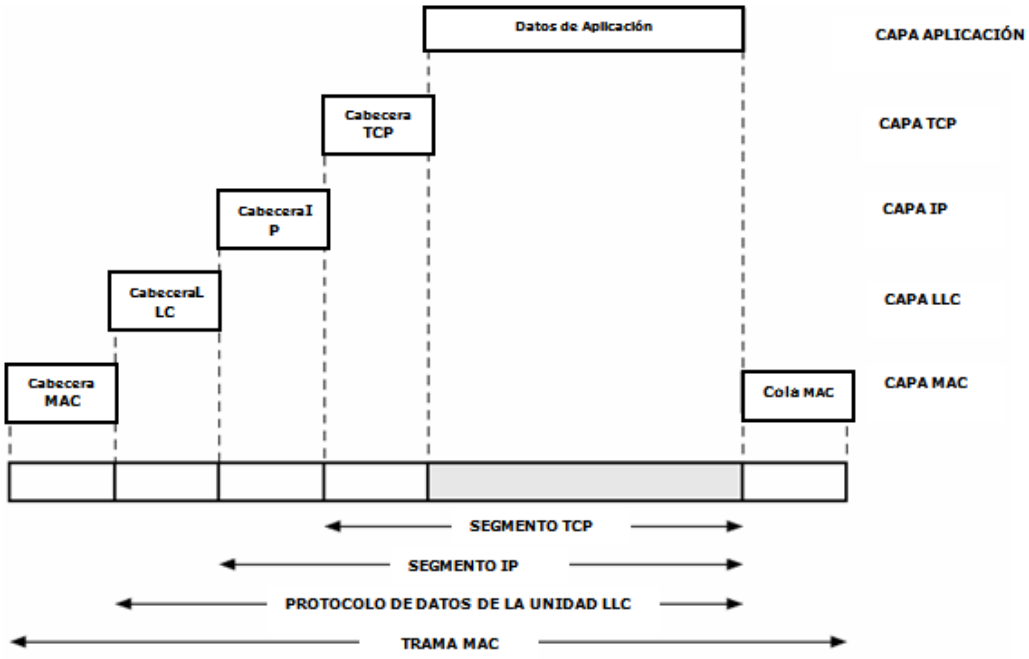


Figura 2. 10 Encapsulamiento de datos[33].

Los datos generados por el encapsulamiento no son bits de información, pero contribuyen al incremento del ancho de banda. Para tener un cálculo aproximado de los bits generados por encapsulamiento de capas, se necesita establecer un escenario.

Debido a que este Proyecto se enfoca en las comunicaciones inalámbricas, se escoge el Estándar IEEE 802.11g para el envío de los datos de información.
El estándar IEEE 802.11g va a trabajar a 54 Mbps; se escoge la mayor velocidad debido a que en estas condiciones se genera más bits por encapsulamiento. El método de seguridad inalámbrica es WPA2, debido a que brinda mayor seguridad en la red inalámbrica.
En el **Anexo A**, se indica el desarrollo del proceso de encapsulamiento de una trama IEEE 802.11 g.
En la figura 2.11, se indica el proceso de encapsulamiento de los datos de información.

[33] W. Stallings; "Wireless Comunications and Networks"; 2nd Edition; Prentice Hall; 2005.

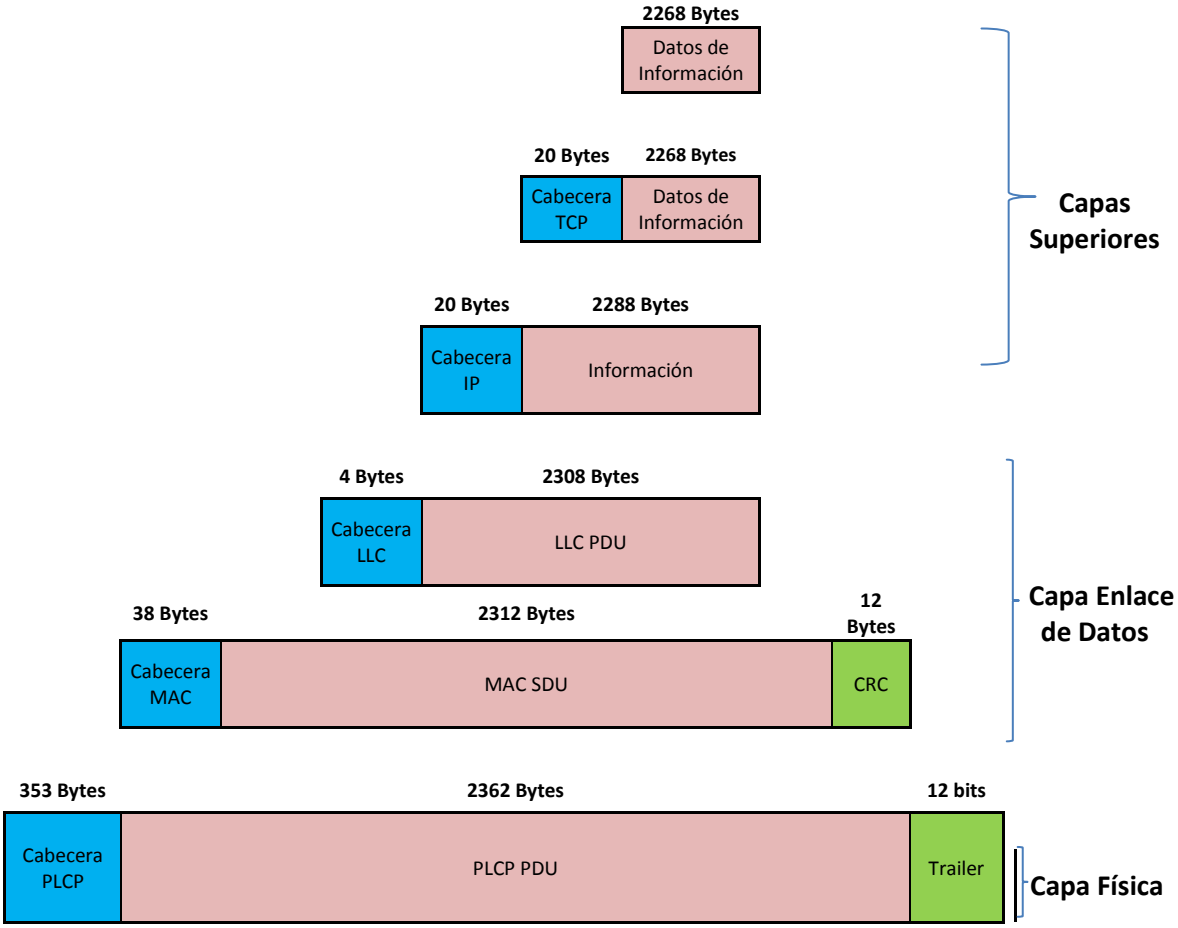


Figura 2. 11 Proceso de encapsulamiento de datos de información.

A partir de la figura 2.11, 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 el PDU de la capa anterior hasta llegar a la capa Física. En la capa física los datos encapsulados son enviados por el medio de transmisión.

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

Con fin didáctico se adjunta la captura de paquetes utilizando un analizador de protocolos en el **Anexo B.**

En las ecuaciones 2.1, 2.2 y 2.3, se calculan la sobrecarga generada por el encapsulamiento de los datos.

$$Sobrecarga\ por\ encapsulamiento = Bits\ totales - Bits\ de\ Información$$

EC. 2.1

$$Sobrecarga\ por\ encapsulamiento = 21732\ bits - 18144\ bits$$

EC. 2.2

$$Sobrecarga\ por\ encapsulamiento = 3588\ bits$$

EC. 2.3

A partir de la ecuación 2.3, se establece que en cada proceso de encapsulamiento se generan 3588 bits o 448.5 Bytes que corresponden al control de flujo, direccionamiento, control de errores, secuenciamiento, multiplexación y reglas para la transferencia de la información. Estos datos no corresponden a bits de información, por lo que esta sobrecarga genera un incremento en el Ancho de Banda.

2.4.3.2 Resolución y métodos de compresión de video.

Los parámetros Resolución y Métodos de compresión de video permiten obtener un nuevo parámetro llamado Tamaño del Cuadro, el cual es medido en Kilobytes.

En la tabla 2.2, se indican los valores de Tamaño del Cuadro en función de la resolución y de la compresión MJPEG.

Resolución	Compresión de video						
	MJPEG-10	MJPEG-20	MJPEG-30	MJPEG-40	MJPEG-50	MJPEG-70	MJPEG-90
320x240 (QVGA)	12 KB	9 KB	8 KB	7 KB	6 KB	5 KB	4 KB
352x240 (CIF NTSC)	13 KB	10 KB	9 KB	8 KB	7 KB	6 KB	4 KB
352x288 (CIF PAL)	15 KB	12 KB	11 KB	9 KB	8 KB	7 KB	5 KB
480X360	26 KB	21 KB	18 KB	16 KB	14 KB	11 KB	9 KB
640X480 (VGA)	46 KB	38 KB	32 KB	28 KB	25 KB	20 KB	16 KB
704x240 (2CIF NTSC)	26 KB	21 KB	18 KB	16 KB	14 KB	11 KB	9 KB
704x288 (2CIF PAL)	31 KB	25 KB	21 KB	19 KB	17 KB	13 KB	10 KB
704x480 (4CIF NTSC)	51 KB	41 KB	36 KB	31 KB	28 KB	22 KB	17 KB
704x576 (4CIF PAL)	61 KB	50 KB	43 KB	38 KB	33 KB	26 KB	21 KB
800x600 (SVGA)	73 KB	59 KB	50 KB	44 KB	40 KB	31 KB	24 KB
1280x720 (HD)	139 KB	113 KB	97 KB	85 KB	76 KB	60 KB	47 KB
1280x960 (1.22 MP)	186 KB	150 KB	129 KB	114 KB	101 KB	80 KB	62 KB

Resolución	Compresión de video						
	MJPEG-10	MJPEG-20	MJPEG-30	MJPEG-40	MJPEG-50	MJPEG-70	MJPEG-90
1280x1024 (1.3 MP)	198 KB	160 KB	138 KB	121 KB	108 KB	86 KB	67 KB
1600x1200 (2MP)	290 KB	235 KB	202 KB	178 KB	158 KB	125 KB	97 KB
1920x1080 (Full HD)	314 KB	253 KB	218 KB	192 KB	171 KB	135 KB	105 KB
2048x1536 (3 MP)	476 KB	384 KB	331 KB	291 KB	259 KB	203 KB	160 KB
2288x1712 (4 MP)	592 KB	479 KB	412 KB	363 KB	323 KB	256 KB	199 KB
2600X1950 (5 MP)	767 KB	619 KB	533 KB	470 KB	418 KB	331 KB	257 KB

Tabla 2. 2 Tamaño del cuadro en función de la resolución y compresión MJPEG[34].

NOTA. La iluminación cumple un factor muy importante para determinar el tamaño del cuadro, pero este parámetro es variable en cada momento, por lo que estos cuadros suponen una iluminación moderada, equivalente a la sección Pasillo central – Baterías Sanitarias[35] (50 lúmenes).

En la tabla 2.3, se indica el tamaño de un cuadro en función de la resolución y compresión MPEG4.

Resolución	Compresión de video					
	MPEG4-10	MPEG4-20	MPEG4-30	MPEG4-50	MPEG4-70	MPEG4-90
320x240 (QVGA)	3 KB	3 KB	2 KB	2 KB	1 KB	1 KB
352x240 (CIF NTSC)	4 KB	3 KB	2 KB	2 KB	1 KB	1 KB
352x288 (CIF PAL)	4 KB	3 KB	3 KB	2 KB	1 KB	1 KB
480X360	7 KB	6 KB	5 KB	3 KB	3 KB	2 KB
640X480 (VGA)	13 KB	10 KB	8 KB	6 KB	5 KB	3 KB
704x240 (2CIF NTSC)	7 KB	6 KB	5 KB	3 KB	2 KB	2 KB
704x288 (2CIF PAL)	9 KB	7 KB	6 KB	4 KB	3 KB	2 KB
704x480 (4CIF NTSC)	14 KB	11 KB	9 KB	7 KB	5 KB	4 KB
704x576 (4CIF PAL)	17 KB	13 KB	11 KB	8 KB	6 KB	4 KB
800x600 (SVGA)	21 KB	16 KB	13 KB	10 KB	7 KB	5 KB
1280x720 (HD)	40 KB	31 KB	25 KB	18 KB	14 KB	10 KB
1280x960 (1.22 MP)	53 KB	41 KB	34 KB	25 KB	18 KB	13 KB

[34] Tamaño de un cuadro en función de la resolución y compresión MJPEG – Software IP Video System Design Tool.
[35] Resource and training kit: Lighting; Australian Greenhouse Office.

Resolución	Compresión de video					
	MPEG4-10	MPEG4-20	MPEG4-30	MPEG4-50	MPEG4-70	MPEG4-90
1280x1024 (1.3 MP)	56 KB	44 KB	30 KB	20 KB	19 KB	14 KB
1600x1200 (2MP)	82 KB	64 KB	53 KB	38 KB	28 KB	21 KB
1920x1080 (Full HD)	89 KB	69 KB	57 KB	41 KB	31 KB	22 KB
2048x1536 (3 MP)	135 KB	105 KB	87 KB	63 KB	46 KB	34 KB
2288x1712 (4 MP)	168 KB	130 KB	108 KB	78 KB	58 KB	42 KB
2600X1950 (5 MP)	218 KB	169 KB	139 KB	101 KB	75 KB	54 KB

Tabla 2. 3 Tamaño de un cuadro en función de resolución y compresión MPEG4.[36]

En la tabla 2.4, se indica el tamaño de un cuadro en función de la resolución y compresión H264.

Resolución	Compresión de video			
	H264-10	H264-20	H264-30	H264-50
320x240 (QVGA)	1 KB	1 KB	1 KB	1 KB
352x240 (CIF NTSC)	1 KB	1 KB	1 KB	1 KB
352x288 (CIF PAL)	1 KB	1 KB	1 KB	1 KB
480X360	3 KB	2 KB	2 KB	2 KB
640X480 (VGA)	5 KB	4 KB	3 KB	3 KB
704x240 (2CIF NTSC)	3 KB	2 KB	2 KB	2 KB
704x288 (2CIF PAL)	3 KB	3 KB	2 KB	2 KB
704x480 (4CIF NTSC)	5 KB	4 KB	3 KB	3 KB
704x576 (4CIF PAL)	6 KB	5 KB	4 KB	4 KB
800x600 (SVGA)	8 KB	6 KB	5 KB	5 KB
1280x720 (HD)	14 KB	11 KB	10 KB	9 KB
1280x960 (1.22 MP)	19 KB	15 KB	13 KB	12 KB
1280x1024 (1.3 MP)	20 KB	16 KB	14 KB	13 KB
1600x1200 (2MP)	30 KB	23 KB	20 KB	19 KB
1920x1080 (Full HD)	32 KB	25 KB	22 KB	21 KB
2048x1536 (3 MP)	49 KB	38 KB	33 KB	31 KB
2288x1712 (4 MP)	60 KB	47 KB	41 KB	39 KB
2600X1950 (5 MP)	78 KB	61 KB	53 KB	50 KB

Tabla 2. 4 Tamaño de un cuadro en función de resolución y compresión H264[37].

[36] Tamaño de un cuadro en función de la resolución y compresión MPEG4 – Software IP Video System Design Tool.

Para realizar un ejemplo de cálculo del ancho de banda, se considera una resolución de 800 x 600 pixeles y que emplee una compresión MJPEG -10. Haciendo referencia a la tabla 2.2, se establece que el tamaño de un cuadro es de 73 KB.

NOTA: Los parámetros resolución y compresión se seleccionaron arbitrariamente.

Con este valor se puede determinar el número aproximado de tramas 802.11 g que se necesitan para trasmitir un cuadro completo. En la ecuación 2.4, se presenta el cálculo necesario para obtener el número aproximado de tramas, esta 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.

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

EC. 2.4

$$\#\ de\ tramas = \frac{73\ [KBytes]}{2268\ [Bytes]} \times \frac{1024\ [Bytes]}{1\ [KByte]}$$

EC. 2.5

$$\#\ de\ tramas = 33\ [Tramas]$$

EC. 2.6

En la ecuación 2.6, se obtuvo un total de 33 tramas; con este valor se procede a calcular la sobrecarga total producida por las cabeceras y los trailers generados en cada encapsulamiento.

En la ecuación 2.7, se indica la sobrecarga total que resulta del producto entre el número de tramas y la sobrecarga total generada por el proceso de encapsulamiento.

$$Sobrecarga\ Total = \#\ de\ tramas\ \times sobrecarga\ total\ por\ encapsulamiento$$

[37] Tamaño de un cuadro en función de la resolución y compresión MPEG1 – Software IP Video System Design Tool.

EC. 2.7

$$Sobrecarga\ Total = 33\ [Tramas] \times 448.5[Bytes] = 14800.5\ [Bytes]$$

EC. 2.8

$$Sobrecarga\ Total = 14800.5\ [Bytes] \times \frac{1\ [KByte]}{1024\ [Bytes]} = 14.45\ [KBytes]$$

EC. 2.9

$$Sobrecarga\ Total = 14.45\ [KBytes]$$

EC. 2.10

Con el tamaño de un cuadro y la sobrecarga que implica el proceso de encapsulamiento, se procede a calcular el tamaño real de un cuadro, tal como se indica en la ecuación 2.12 y 2.13.

$$Tamaño\ Real\ de\ un\ cuadro\ [Bytes] = 73\ KBytes + 14.45\ KBytes$$

EC. 2.11

$$Tamaño\ Real\ de\ un\ cuadro\ [Bytes] = 87.45\ [KBytes]$$

EC. 2.12

$$Tamaño\ Real\ de\ un\ cuadro\ [bits] = 87.45 \times 8\ [bits] = 699.6\ [Kbits]$$

EC. 2.13

Los cuadros por segundo (FPS) son de valor variable que dependen de la luminosidad y movimiento, por lo que se debe hacer el cálculo considerando la peor condición, que en muchas cámaras es de 30 FPS.

En la ecuación 2.14 y 2.15, se realiza un cálculo aproximado del ancho de banda.

$$Ancho\ de\ Banda\ [Mbps] = Tamaño\ Real\ de\ un\ cuadro \times fps\ [Mbps]$$

EC. 2.14

$$Ancho\ de\ Banda\ [Mbps] = 699.6\ \left[\frac{Kbits}{cuadro}\right] \times 30\ \left[\frac{cuadros}{segundo}\right] \times \frac{1\ [Mbit]}{1024\ [Kbits]}$$

EC. 2.15

$$Ancho\ de\ Banda\ [Mbps] = 20.49\ [Mbps]$$

EC. 2.16

El valor encontrado en la Ecuación 2.16, representa el ancho de banda aproximado que consume una cámara IP, empleando una resolución de 800 x 600 pixeles y una compresión MJPEG -10.

2.4.4. ANCHO DE BANDA QUE UTILIZA UN CIRCUITO CERRADO DE TELEVISIÓN.

Para determinar 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.

En la ecuación 2.17, se calcula aproximadamente el ancho de banda q consume un circuito cerrado de televisión.

$$Ancho\ de\ Banda\ [Mbps] = Ancho\ de\ banda\ x\ cada\ cámara\ \times \#\ de\ cámaras$$

EC. 2.17

Esta ecuación no posee valores numéricos, ya que aún no se define el número de cámaras a instalarse.

2.4.5. DIRECCIONAMIENTO IP.

La red del circuito cerrado de televisión trabaja en un ambiente LAN, es por este motivo que se emplea una dirección de red privada, la misma que es:

172.16.0.0

Esta dirección de subred pertenece a una dirección clase B que posee una máscara de 16 bits, además de ser una dirección especificada en el RFC 1918 como dirección privada[38].

Para realizar el direccionamiento se considera el número de Host a ser utilizados. En la tabla 2.5, se indica los Host correspondientes al circuito cerrado de televisión.

HOST
Access Point
Cámara 1
Cámara 2
Cámara 3

Tabla 2. 5 Host del Circuito Cerrado de Televisión.

Adicionalmente se dejan cinco direcciones IP para futuros crecimientos. Estas direcciones IP corresponden a las salas A, B, C, D y E.
Considerando la Tabla 2.5 y el crecimiento de la red se tiene un total de 9 direcciones IP de esta subred. Para determinar cuántos bits se asigna a la porción de host, se emplea la siguiente fórmula:

$$2^N - 2 = Host\ utilizables$$

$$2^N - 2 = 9$$

En donde N representa los bits que identifican la porción de host.

$$2^N = 11$$

Un valor que satisface esta relación matemática es:

$N = 4$.

[38] RFC1918.-http://www.faqs.org/rfcs/rfc1918.html

Considerando que el número de bits que identifican la porción de host es igual a cuatro, se define que la máscara para esta subred es de 28 bits.
La primera dirección de subred es:

172.16.0.0 / 28

Siendo esta dirección la que se utilizará en el presente Proyecto.

En la tabla 2.6, se observa la asignación de direcciones IP.

UBICACIÓN	DISPOSITIVO	DIRECCIÓN IP	MÁSCARA
Pasillo Central	Access Point	172.16.0.1	255.255.255.240
Entrada Principal	Cámara 1	172.16.0.2	255.255.255.240
Entrada Secundaria	Cámara 2	172.16.0.3	255.255.255.240
Cafetería	Cámara 3	172.216.0.4	255.255.255.240
Futuras Cámaras IP	Cámara Extra 1	172.16.0.5	255.255.255.240
Futuras Cámaras IP	Cámara Extra 2	172.16.0.6	255.255.255.240
Futuras Cámaras IP	Cámara Extra 3	172.16.0.7	255.255.255.240
Futuras Cámaras IP	Cámara Extra 4	172.16.0.8	255.255.255.240
Futuras Cámaras IP	Cámara Extra 5	172.16.0.9	255.255.255.240

Tabla 2. 6 Direccionamiento IP.

A partir de la dirección de subred 172.16.0.0 y considerando la tabla 2.6, se observa que existen tres direcciones IP para las cámaras, una para el punto de acceso inalámbrico y cuatro direcciones IP para futuras cámaras.

2.4.6. ANÁLISIS DEL SITE SURVEY.

2.4.6.1. Site Survey.

El SiteSurvey o Evaluación de Sitio permite estudiar y determinar el área de cobertura de la red inalámbrica, también permite obtener información sobre redes inalámbricas existentes, intensidad de señal y en base a estos resultados se determina la ubicación más adecuada para el punto de acceso inalámbrico.
El Estudio de Sitio fue desarrollado mediante el uso de los programas VisiWave y por WirelessMon.

En las figuras 2.12 y 2.13, se indican los logotipos del programa VisiWave y WirelessMon respectivamente.

Figura 2. 12 Logotipo del programa VisiWave[39].

[39] Logotipo del programa VisiWave. - http://www.visiwave.com/

Figura 2. 13 Logotipo del programa WirelessMon[40].

2.4.6.1.1 Site survey pasivo.

En el SiteSurvey Pasivo se detectan las redes inalámbricas que se encuentran en la zona a estudiar.

En la figura 2.14, se indica las redes WiFi que el programa WirelessMon detecta en el Laboratorio de Informática.

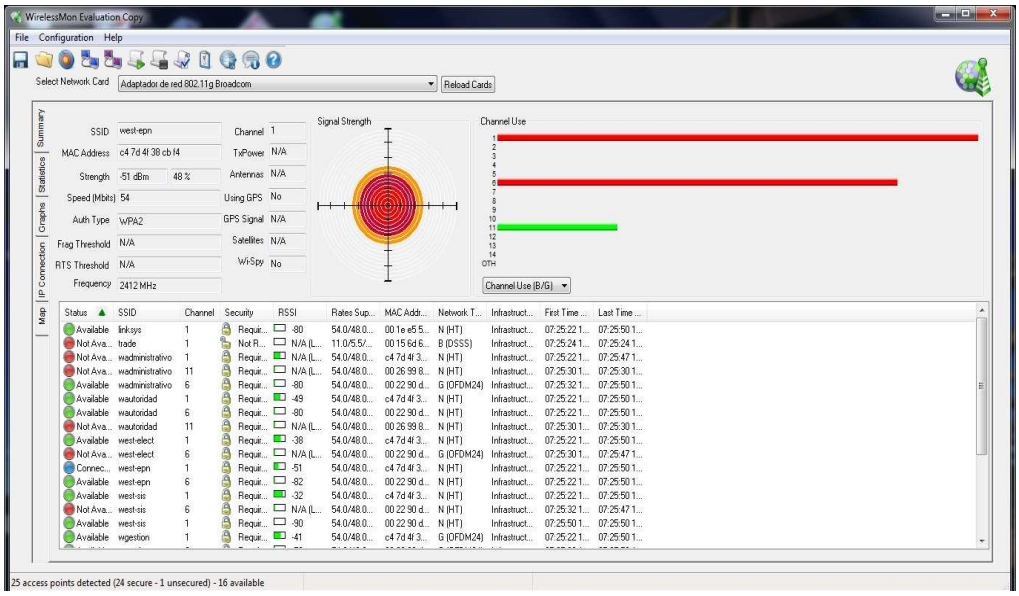


Figura 2. 14 Redes Inalámbricas Detectadas en el Laboratorio de Informática.

A partir de la figura 2.14, se puede apreciar que en el Laboratorio de Informática existen varias redes inalámbricas, muchas con señal muy fuerte y otras con señal prácticamente nula; el canal que se encuentra menos congestionado es el canal 11, por lo que éste canal será el que se va a utilizar para la configuración de los dispositivos inalámbricos para evitar interferencias.

2.4.6.1.2 Site survey activo.

[40] Logotipo del programa WirelessMon. - http://www.wirelessmon.com/

En el Site survey activo, se observa el comportamiento de la red inalámbrica a instalarse con las demás redes existentes en la zona de estudio. En base a los niveles de señal que esta interacción presente, se va a determinar:

- Ubicación del Router Inalámbrico.
- Niveles de Señal en las zonas de riesgo.

2.4.6.2 Zonas a cubrir.

En la figura 2.15, se indica las zonas de riesgo a ser vigiladas por el circuito cerrado de televisión.

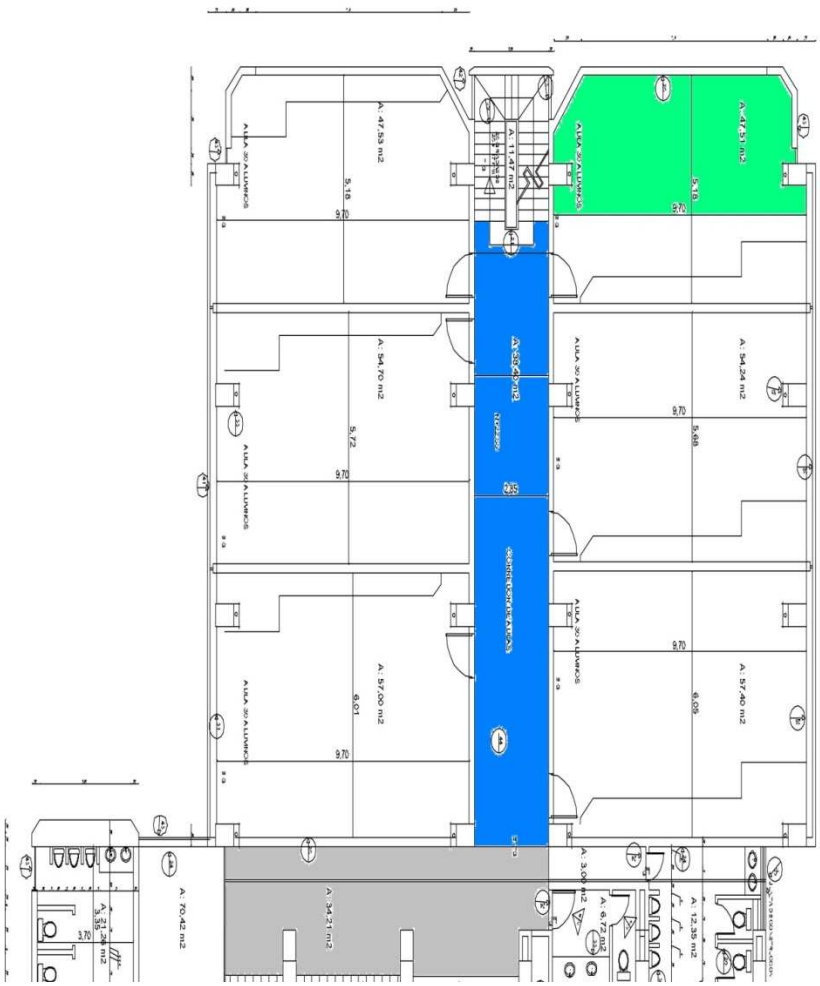


Figura 2. 15 Zonas de riesgo a ser vigiladas.

Zona 1: Entrada Principal

Zona 2: Pasillo Central

Zona 3: Cafetería

2.4.6.3 ESTUDIO DEL SITE SURVEY EN EL LABORATORIO DE INFORMÁTICA.

Con el fin de determinar la mejor ubicación para la instalación del Router Inalámbrico, se realizan pruebas que consisten en ubicarlo en diferentes puntos y en base al software VisiWave analizar los diferentes niveles de potencia en las zonas de riesgo ya establecidas.

Antes de ubicar el router inalámbrico, se debe considerar que la potencia de radiación de este equipo está afectada por diferentes parámetros como son:

- Presencia de metales.
- Presencia de electrodomésticos.
- Potencia de Transmisión del router inalámbrico.
- Tipos de antenas en los equipos inalámbricos.

Para realizar el SiteSurvey activo se empleó un router inalámbrico WRT300N, con una potencia de 125mW. La ubicación del router inalámbrico fue localizada en dos puntos, el primero fue en la mitad del pasillo central y la segunda fue localizada al final del pasillo central, junto a las gradas provenientes del séptimo y quito piso.

Estos puntos fueron seleccionados debido a que poseen una línea de vista directa con las cámaras que se van a instalar.

En la figura 2.16, se indica la ubicación del router inalámbrico en el centro del pasillo.

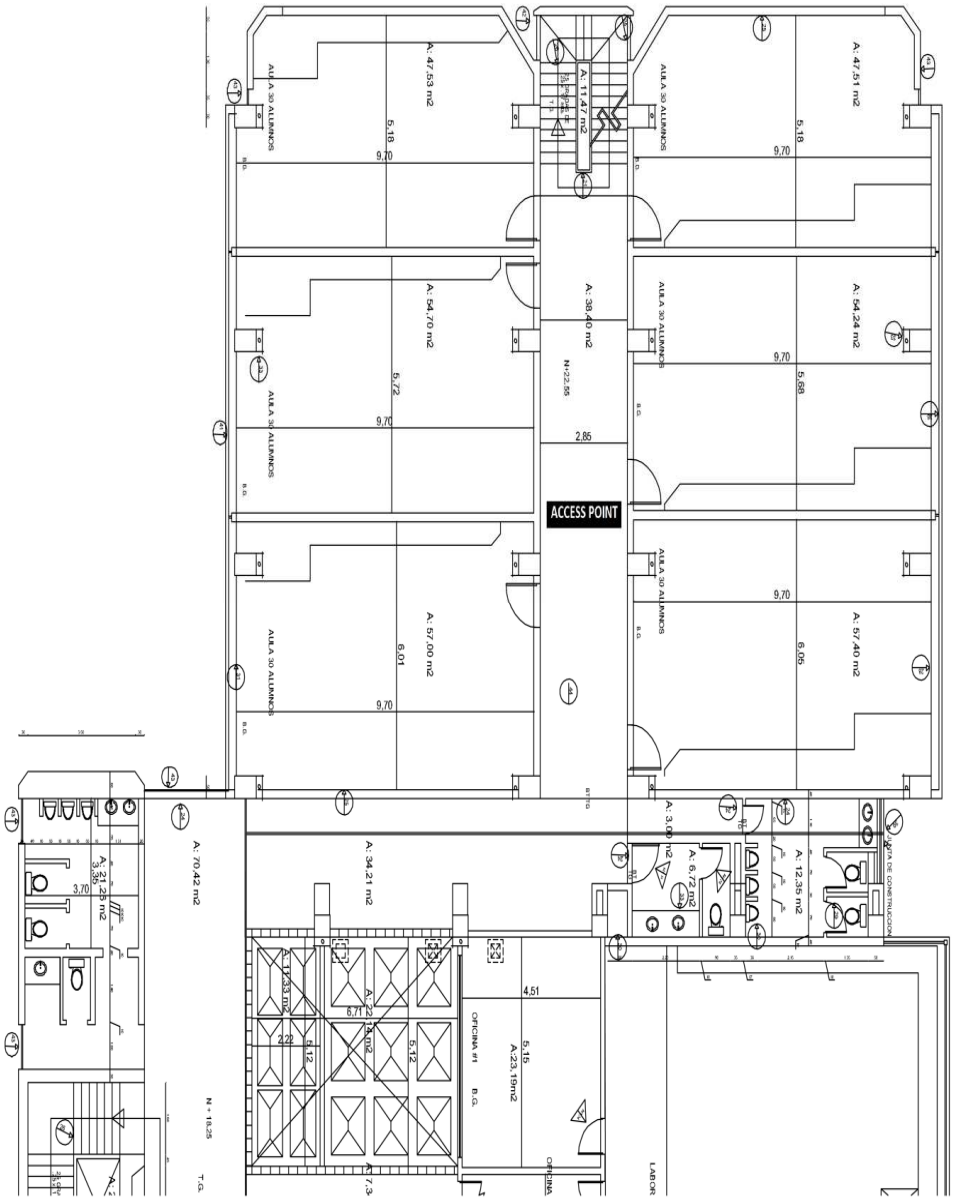


Figura 2. 16 Ubicación del Router Inalámbrico en el centro del pasillo.

En la figura 2.17, se indica la ubicación del router inalámbrico al final del pasillo.

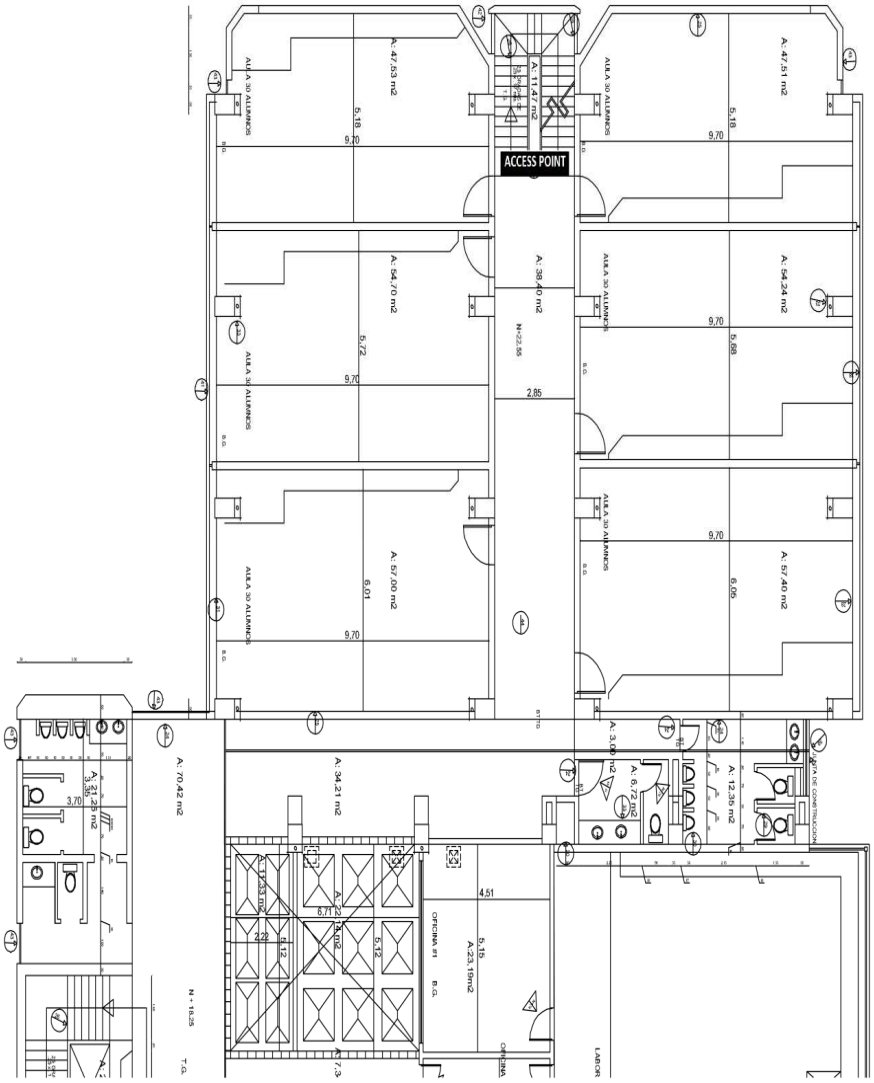


Figura 2. 17 Ubicación del Router Inalámbrico al final del pasillo.

Para realizar el estudio del Site Survey en el Laboratorio de Informática el programa VisiWave emplea los planos arquitectónicos de la zona de estudio.

En la figura 2.18, se indica los resultados del Site Survey realizado en el Laboratorio de Informática cuando el router inalámbrico se ubica en el centro del pasillo central.

Figura 2. 18 Resultados del Site Survey cuando el router inalámbrico se ubica en la mitad del pasillo central.

Los valores de potencia se obtienen al colocar el puntero del ratón sobre el lugar exacto donde se instalará la cámara inalámbrica IP.

Se observa que existen niveles de potencia adecuados para el buen funcionamiento de la red inalámbrica. En la cafetería existe una atenuación considerable de la señal debido a la presencia de columnas y paredes de gran grosor.

Los niveles de potencia que se toman como referencia son los puntos solitarios en negro que se indican en la figura 2.18, debido a que se consideran lugares de posible ubicación de las cámaras IP.

En la tabla 2.7, se indica las zonas críticas y sus respectivos valores de nivel de señal.

Zonas Críticas	Niveles de Señal [dBm]
Entrada Principal	-43 dBm
Pasillo Central	-38dBm
Cafetería	-49dBm

Tabla 2. 7 Zonas Críticas y Niveles de Señal.

En la figura 2.19, se indica los resultados del Site Survey realizado en el Laboratorio de Informática cuando el router inalámbrico se ubica al final del pasillo central junto a las gradas provenientes del séptimo y quinto piso.

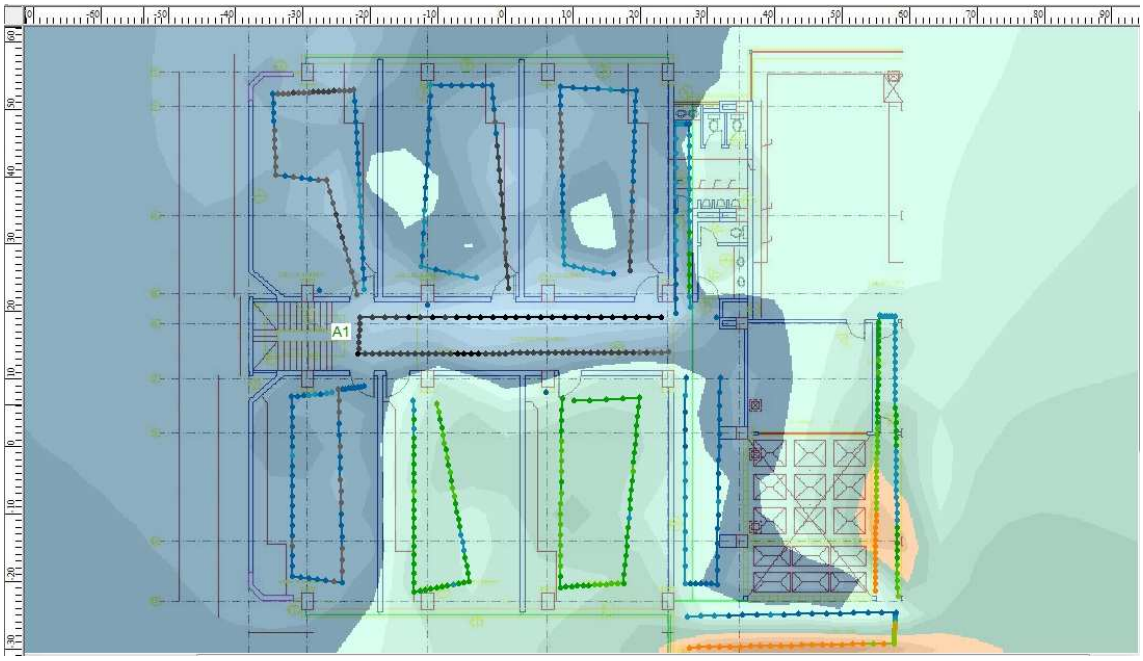


Figura 2. 19 Resultados del Site Survey cuando el router inalámbrico se ubica al final del pasillo central.

Los niveles de señal obtenidos se reducen considerablemente con respecto a los resultados anteriores. En la tabla 2.8, se indica los niveles de señal para cada una de las zonas de riesgo.

Zonas de Riesgo	Niveles de Señal [dBm]
Entrada Principal	-57dBm
Pasillo Central	-56 dBm
Cafetería	-55 dBm

Tabla 2. 8 Zonas de riesgo y Niveles de Señal.

En la Tabla 2.9, se compara los diferentes niveles de señal obtenidos mediante la ubicación del router inalámbrico en dos puntos diferentes.

Zonas de Riesgo	Niveles de Señal [dB] Mitad del Pasillo Central	Niveles de Señal [dB] Final del Pasillo Central
Entrada Principal	-43 dBm	-57dBm
Pasillo Central	-38 dBm	-56 dBm
Cafetería	-49 dBm	-55 dBm

Tabla 2. 9 Zonas de riesgo y comparación de Niveles de Señal.

Los niveles de señal obtenidos con la ubicación del router inalámbrico en la mitad del pasillo central son mayores, es por esta razón que el router se ubicará en la mitad del pasillo central, para asegurar que cada cámara tenga adecuados niveles de señal para su normal funcionamiento.

2.5 SELECCIÓN DE EQUIPOS.

2.5.1. INTRODUCCIÓN.

Con la descripción del lugar y con los requerimientos del software ZoneMinder, se puede determinar los requisitos que deben cumplir las cámaras IP y el servidor.

2.5.2 SELECCIÓN DE CÁMARAS IP.

Una vez realizado el estudio del sitio, considerando el número de cámaras a ser instaladas y las funciones de monitoreo que van a cumplir cada una de ellas, se indica los parámetros que se utilizan para la selección de cámaras IP. Los parámetros que se utilizan para la selección de las cámaras IP se indican en la tabla 2.10.

Parámetro	Requerimientos
Compresión de Video	MJPEG
Resolución (pixeles)	320 x 240
Mínima Iluminación (Lux)	0.5
Visibilidad Nocturna (metros)	5
Ángulo de Visión (º)	51
Cuadros por segundo (fps)	15
Movimiento	Ninguno
Zoom	No

Tabla 2. 10 Requisitos para la selección de las cámaras IP.

Las cámaras que se utilizan para el proceso de selección son:

- TRENDnet TV-IP410.
- FOSCAM FI8918W.
- D-LINK DCS1100.

En la tabla 2.11, se realiza el proceso de selección de la cámara a utilizarse en el CCTV.

Parámetro	TRENDnet TV-IP410	FOSCAM FI8918W	D-LINK DCS1100
Compresión de Video.	SI CUMPLE	SI CUMPLE	SI CUMPLE
Resolución (pixeles).	SI CUMPLE	SI CUMPLE	SI CUMPLE
Mínima Iluminación (Lux).	SI CUMPLE	SI CUMPLE	NO CUMPLE
Visibilidad Nocturna.	NO CUMPLE	SI CUMPLE	SI CUMPLE
Ángulo de Visión (º).	SI CUMPLE	SI CUMPLE	SI CUMPLE
Cuadros por segundo (fps).	SI CUMPLE	SI CUMPLE	SI CUMPLE
Movimiento.	NO CUMPLE	SI CUMPLE	NO CUMPLE
Zoom.	NO CUMPLE	NO CUMPLE	NO CUMPLE

Tabla 2. 11 Selección de las cámaras IP.

A partir de la tabla 2.11, se observa que la cámara FOSCAM FI8918W cumple con la mayoría de los requerimientos previamente establecidos, por lo que esta cámara será utilizada para la implementación del Proyecto.

2.5.2.1 Cálculo Aproximado del Ancho de Banda usando la cámara IP Foscam FI8918W.

Para establecer los requerimientos de los equipos de interconectividad es necesario saber cuánto ancho de banda se requiere en las peores condiciones para que el CCTV IP funcione sin ningún problema.
En la tabla 2.12, se indican los requerimientos para determinar el ancho de banda aproximado del CCTV.

Número de Cámaras	**3**
Compresión de Video (FOSCAM)	**MJPEG-10**
Resolución del Video (FOSCAM)	**640 x 480 o 320 x 240**

Tabla 2. 12 Requerimientos para determinar el ancho de banda aproximado del Circuito Cerrado de Televisión.

Con estos datos se realiza el cálculo del Ancho de Banda para el CCTV IP del Laboratorio de Informática.

Haciendo referencia al datasheet de la cámara IP Foscam FI8918W, que se encuentra incluido en el **anexo C**, se obtiene las condiciones con las que se genera mayor ancho de banda. Estas condiciones son:

- Resolución Máxima 640 x 480.
- Número máximo de cuadros por segundo: 15.

El tamaño del cuadro se obtiene en base a la tabla 2.2 y el valor es de 46 [KB].

En la ecuación 2.18, se obtienen el número de tramas para él envió de un cuadro en las condiciones establecidas anteriormente.

$$\#\ de\ tramas = \frac{46\ [KBytes]}{2268\ [Bytes]} \times \frac{1024\ [Bytes]}{1\ [KByte]} = 20.77\ [Tramas]$$

EC. 2.18

$$\#\ de\ tramas = 21\ [Tramas]$$

EC. 2.19

En la ecuación 2.20, se calcula aproximadamente la sobrecarga total, la misma que es igual al producto entre el número de tramas y la sobrecarga generada por encapsulamiento.

$$Sobrecarga\ Total = 21\ [Tramas] \times 448.5\ [Bytes]$$

EC. 2.20

$$Sobrecarga\ Total = 9418{,}5\ [Bytes] \times \frac{1\ [KByte]}{1024\ [Bytes]} = 9.19\ [KBytes]$$

EC. 2.21

$$Sobre\ Carga\ Total = 9.19\ [KBytes]$$

EC. 2.22

En la ecuación 2.23 y 2.24, se calcula el tamaño real aproximado de un cuadro transmitido, empleando el estándar IEEE 802.11 g.

$$Tamaño\ Real\ de\ un\ cuadro\ [Bytes] = 46\ KBytes + 9.19\ KBytes = 55.2\ [KBytes]$$

EC. 2.23

$$Tamaño\ Real\ de\ un\ cuadro\ [bits] = 55.2 \times 8\ [bits] = 441.58\ [Kbits]$$

EC. 2.24

En la ecuación 2.25, se obtiene el ancho de banda aproximado que consume una cámara, para encontrar este valor se realiza el producto entre el tamaño real de un cuadro y el número de cuadros enviados en un segundo.

$$Ancho\ de\ Banda\ [Mbps] = 441.58\ [\frac{Kbits}{cuadro}] \times 15\ [\frac{cuadros}{segundo}] \times \frac{1\ [Mbit]}{1024\ [Kbits]} = 6.47\ [Mbps]$$

EC. 2.25

En la ecuación 2.26, se calcula el ancho de banda aproximado que consume el Circuito Cerrado de Televisión, este valor se obtiene del producto del ancho de banda de una cámara por el número total de cámaras.

$$Ancho\ de\ Banda\ CCTV\ [Mbps] = 6.47 \times 3 = 19.41 [Mbps]$$

EC. 2.26

Con el valor encontrado en la ecuación 2.26, se determina que los equipos de conectividad a ser usados bajo estas condiciones deben manejar aproximadamente y en las peores condiciones una cantidad de tráfico máximo de 19.41 [Mbps].

La cámara Foscam FI8918W trabaja con resoluciones de 640 x 480 y 320 x 240, hasta el momento se tiene el valor aproximado de ancho de banda con la resolución más alta, por lo que es conveniente calcular con la resolución más

baja, a fin de comparar los dos valores y tener una idea cuantitativa entre una resolución y otra.

A partir de la ecuación 2.27 hasta la ecuación 2.35, se indica el cálculo del ancho de banda aproximado que consume el Circuito Cerrado de Televisión a una resolución de 320 x 240.

El tamaño del cuadro correspondiente a una resolución de 320 X 240, se obtiene en base a la tabla 2.2. Este valor es igual a de 12 [KB].

En la ecuación 2.27, se obtienen el número de tramas aproximadas y necesarias para él envió de un cuadro en las condiciones establecidas anteriormente.

$$\#\ de\ tramas = \frac{12\ [KBytes]}{2268\ [Bytes]} \times \frac{1024\ [Bytes]}{1\ [KByte]} = 5.41\ [Tramas]$$

EC. 2.27

$$\#\ de\ tramas = \ 6\ [Tramas]$$

EC. 2.28

$$Sobrecarga\ Total = 6\ [Tramas] \times 448.5\ [Bytes]$$

EC. 2.29

$$Sobrecarga\ Total = 2691\ [Bytes] \times \frac{1\ [KByte]}{1024\ [Bytes]} = 2.62\ [KBytes]$$

EC. 2.30

$$Sobre\ Carga\ Total = 2.62\ [KBytes]$$

EC. 2.31

$$Tamaño\ Real\ de\ un\ cuadro\ [Bytes] = 12\ KBytes + 2.62\ KBytes = 14.62\ [KBytes]$$

EC. 2.32

$$Tamaño\ Real\ de\ un\ cuadro\ [bits] = 14.62 \times 8\ [bits] = 116.96\ [Kbits]$$

EC. 2.33

Obteniendo el valor real de un cuadro se procede a calcular el ancho de banda aproximado que consume una cámara IP.

$$Ancho\ de\ Banda\ [Mbps] = 116.96\ [\frac{Kbits}{cuadro}] \times 30\ [\frac{cuadros}{segundo}] \times \frac{1\ [Mbit]}{1024\ [Kbits]} = 3.42\ [Mbps]$$

EC. 2.34

Con el ancho de banda que consume una cámara IP, se procede a calcular el ancho de banda aproximado que consume el circuito cerrado de televisión.

$$Ancho\ de\ Banda\ CCTV\ [Mbps] = 3.42\ \times 3 = 10.26\ [Mbps]$$

EC. 2.35

Este resultado indica que equipos que trabajan en el estándar IEEE 802.11g pueden manejar sin problemas este tráfico, siempre y cuando no existan equipos que operen en el mismo canal, ya que en esta situación se refleja en el rendimiento del equipo inalámbrico.

En la implementación se trabaja con la resolución de 640 x 480, debido a que en esa resolución se obtiene una imagen más clara.

El Laboratorio de Informática cuenta con un router inalámbrico WRT300N que cumple con los requisitos descritos anteriormente y será utilizado para la implementación del Circuito Cerrado de Televisión.

2.5.3 SELECCIÓN DEL SERVIDOR DE VIDEO.

El servidor de video es la parte más importante del CCTV, por lo que se debe utilizar una distribución de Linux bastante estable. En este caso se selecciona CentOS 5.5 como sistema operativo para brindar una mayor confiabilidad.

El Laboratorio de Informática dispone de un servidor HP ProLiant ML110. Las características de este servidor son las siguientes:

- Procesador Core 2 Duo 3.16 GHz.
- Memoria DDR2 3 GB.
- 2 Discos Duros de 250 y 500 GB respectivamente.
- Tarjeta de red 1 Gbps.

En la tabla 2.13, se indica los requerimientos en hardware recomendados por el programa Zoneminder y las características del servidor HP ProLiant ML 110.

Requerimientos recomendados por el programa Zoneminder.	Características del servidor HP ProLiant ML 110.
Procesador Dual Core o AMD Turion x2.	Procesador Core 2 Duo 3.16 Ghz.
Memoria 1 GB.	Memoria DDR2 3 GB.
1 GB de espacio en disco duro.	2 Discos Duros de 250 y 500 GB respectivamente.
Tarjeta de red FastEthernet 100 Mbps.	Tarjeta de red 1 Gbps.

Tabla 2. 13 Requisitos para la selección del Servidor de Video.

NOTA: El datasheet del servidor se encuentra en el Anexo D.

A partir de la tabla 2.13, se observa que las características del servidor HP ProLiant ML110 superan los requerimientos recomendados por el programa ZoneMinder, por lo que este servidor se utiliza para la implementación del Circuito Cerrado de Televisión.

En la figura 2.20, se indica la estructura física del servidor.

Figura 2. 20 Estructura física del servidor.

2.5.3.1 Cálculo de la capacidad aproximada de almacenamiento del disco duro para el servidor *HP Proliant ML110*.

La cantidad de información almacenada en un disco duro depende la cantidad de datos que se guarden en un tiempo determinado.

Conociendo el Ancho de Banda aproximado que genera el Circuito Cerrado de Televisión y considerando que los eventos almacenados se eliminan cada semana, se puede obtener un cálculo aproximado de la cantidad de información que debe ser almacenada en el disco duro.

En la ecuación 2.35, 2.36 y 2.37, se realiza el cálculo aproximado de los datos almacenados cada semana.

$$Almacenamiento[KBytes] = AB\ del\ CCTV \times segundosxsemana$$

EC. 2.35

$$Almacenamiento\ [GBytes] = 19.41\ [Mbps] \times 604800\ [\frac{segundos}{semana}] \times \frac{1}{1024}[\frac{GBits}{MBits}] \times \frac{1}{8}[\frac{Byte}{Bits}]$$

EC. 2.36

$$Almacenamiento\ [GBytes] = 1433\ GBytes$$

EC. 2.37

En base a los cálculos realizados, el disco duro que se necesita para almacenar una semana de grabación de video continuo es de por lo menos 1.5 Terabyte. Este valor es elevado; por este motivo ZoneMinder tiene configurado por defecto la grabación de un cuadro por segundo, con el fin de que el consumo de espacio de disco duro sea mínimo.

El ancho de banda que se encontró en la ecuación 2.26 es de 19.41 Mbps, el mismo que se obtuvo con una transmisión de 15 cuadros por segundo; en este caso se desea calcular el ancho de banda que consume el CCTV considerando la

transmisión de un cuadro por segundo. En la ecuación 2.38 se indica el cálculo aproximado del Ancho de Banda considerando un cuadro por segundo.

$$Ancho\ de\ Banda\ CCTV\ [Mbps] = \frac{19.41[Mbps]}{15} = 1.294\ Mbps$$

EC. 2.38

$$Almacenamiento[KBytes] = AB\ del\ CCTV \times segundosxsemana$$

EC. 2.39

$$Almacenamiento\ [GBytes] = 1.294\ \ [Mbps] \times 604800\ [\frac{segundos}{semana}] \times \frac{1}{1024}[\frac{GBits}{MBits}] \times \frac{1}{8}[\frac{Byte}{Bits}]$$

EC. 2.40

$$Almacenamiento\ [GBytes] = 95.53\ GBytes$$

EC. 2.41

En la ecuación 2.41, se observa que el almacenamiento empleando una transmisión de un cuadro por segundo es igual a 95.53 GBytes, reduciendo el consumo de espacio de disco duro.

2.5.4 SELECCIÓN DE LAS ESTACIONES DE MONITOREO.

Una estación de monitoreo es cualquier computador que tenga acceso al servidor; es decir, un computador que tenga acceso a la red de datos de la Escuela Politécnica Nacional o que tenga acceso a Internet.

2.6 ÁNGULO DE VISIÓN[41].

[41] http://es.wikipedia.org/wiki/%C3%81ngulo_de_visi%C3%B3n

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 2.21 se indica cómo se mide el ángulo de visión de una cámara.

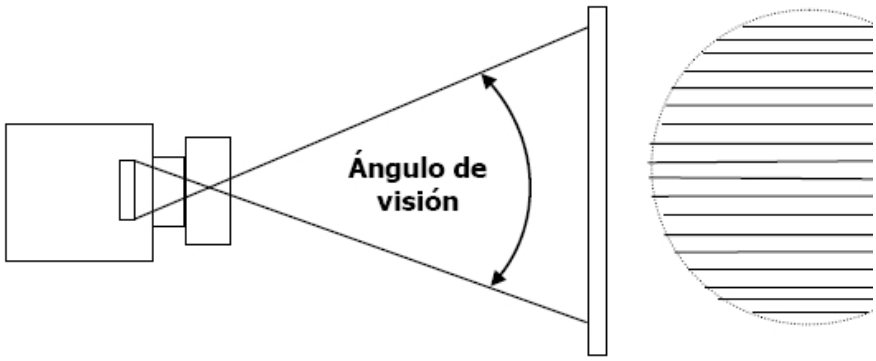


Figura 2. 21 Ángulo de Visión.

El concepto de ángulo de visión es totalmente aplicable en zonas donde la cámara permanece inmóvil o esta no tiene funciones de movimiento; en ciertos lugares es necesario utilizar cámaras que no permanecen estáticas tal es el caso de la cámara IP Foscam que permite movimiento PANEO / CABECEO, en este caso el ángulo de visión varía de tal forma que posee un ángulo de visión superior a 270° siempre y cuando una persona esté operando d icha cámara.

En la figura 2.22, se observa los ángulos de visión correspondiente a PANEO y CABECEO.

Figura 2. 22 Angulo de Movimiento PANEO y CABECEO.

En la figura 2.23, se indican los ángulos de visión de las cámaras instaladas en el Laboratorio de Informática, este ángulo de visión corresponde al momento en que las cámaras no realizan ningún movimiento.

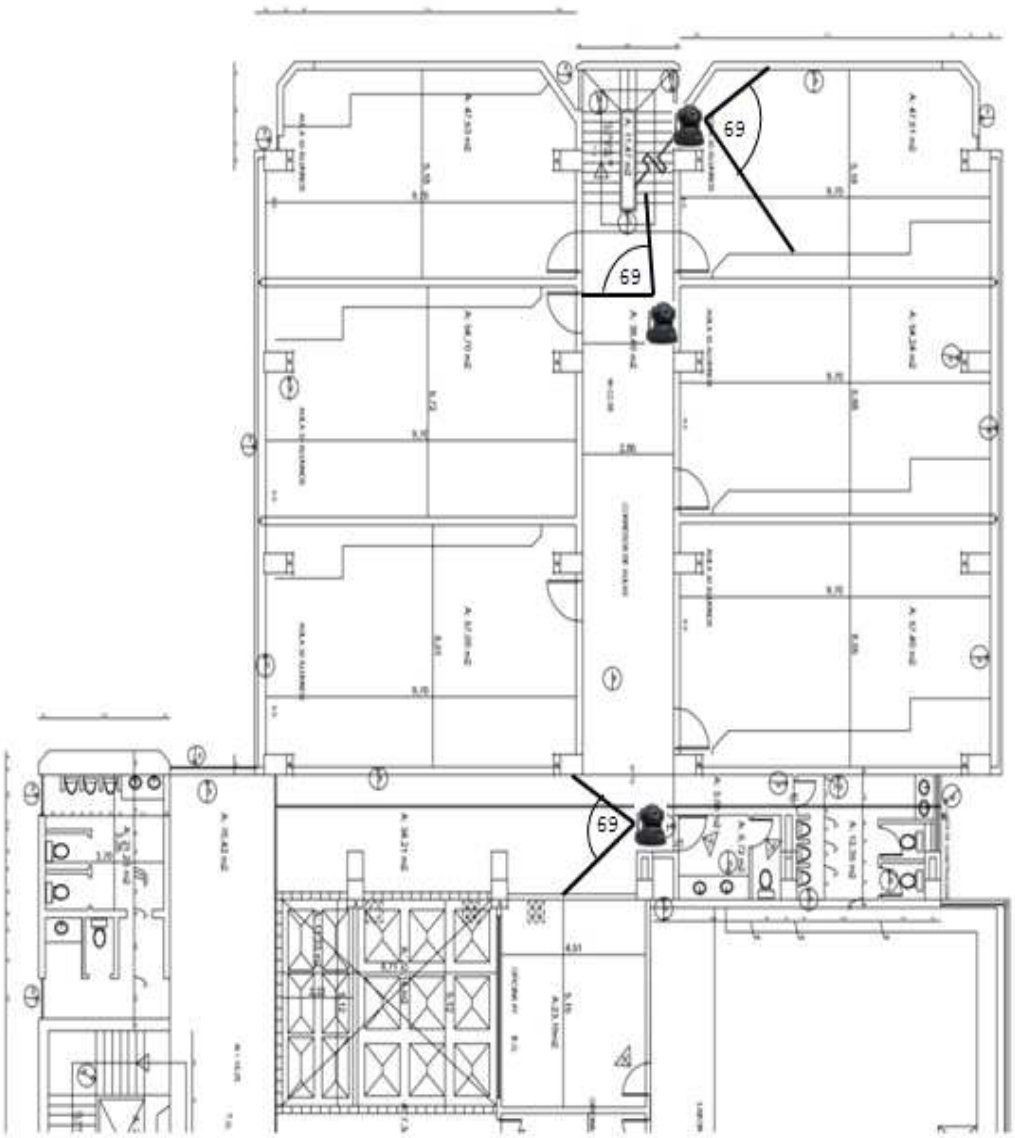


Figura 2. 23 Ángulo de Visión de las Cámaras en cada una de las Zonas de Riesgo.

Al momento de operar con la visión nocturna de las cámaras, la zona de cobertura se ve limitada a 5 metros en cámaras FOSCAM FI8908W y FOSCAM FI8918W.

En la figura 2.24, se observa el alcance de las cámaras al momento de usar la visión nocturna.

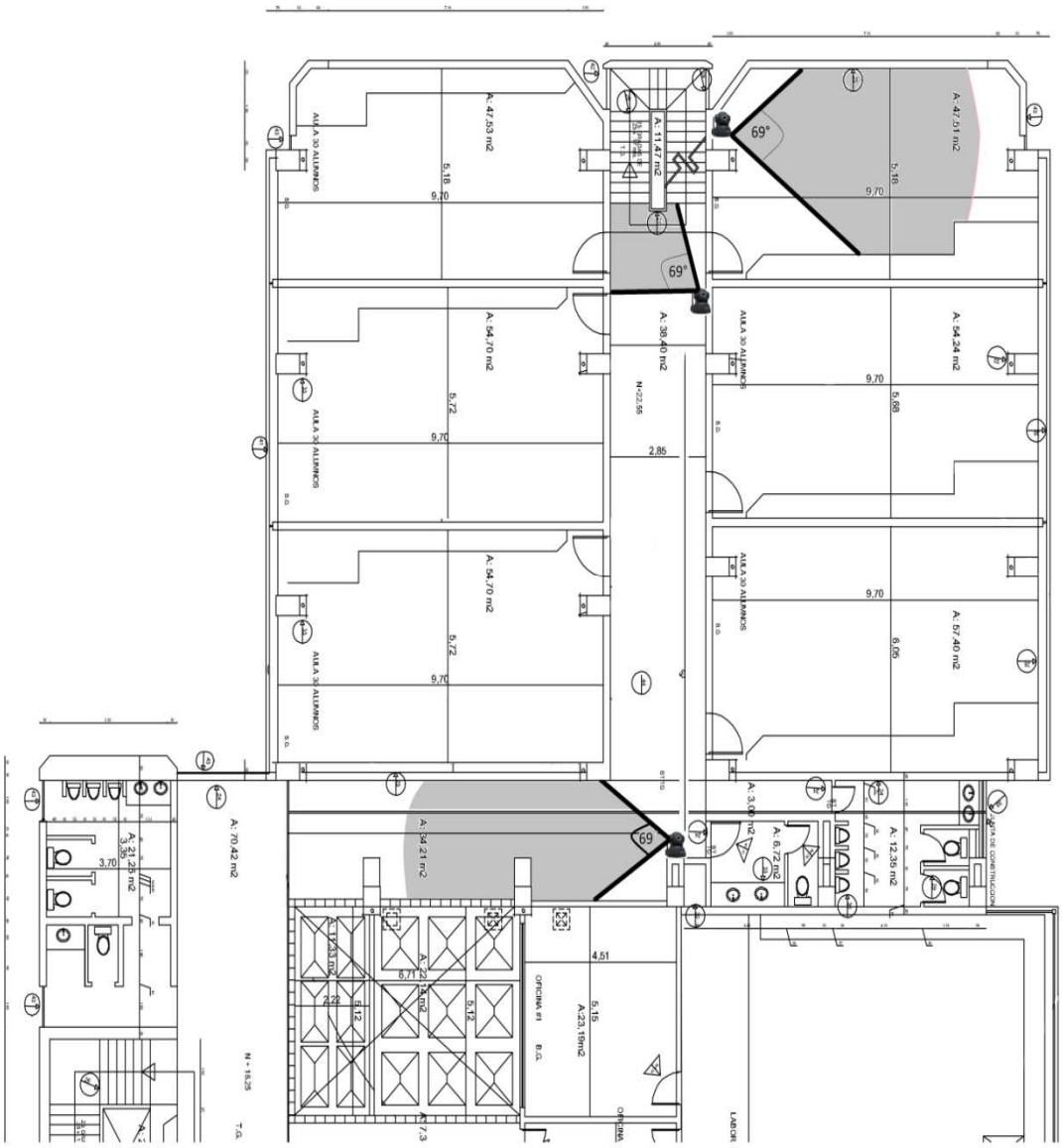


Figura 2. 24 Zonas de Cobertura empleando la visión nocturna.

2.7 INSTALACIÓN DE EQUIPOS.

A continuación, se indica la instalación de los equipos pertenecientes al Circuito Cerrado de Televisión.

La instalación comprende la ubicación y alimentación eléctrica de los equipos. En el caso del router inalámbrico y del servidor es necesario la conexión a los equipos de conectividad.

2.7.1 UPS (SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA).

El Sistema de Alimentación Ininterrumpida, es un equipo o dispositivo capaz de suministrar energía eléctrica frente a alguna interrupción del suministro eléctrico. Adicionalmente estos equipos pueden brindar diferentes opciones como filtrado de la energía entrante, corrección de la forma de onda, corrección de la frecuencia de línea, protección a periféricos de las computadoras o incluso sus partes, como placas de red o módem's, monitoreo de la energía de línea, para optimizar la protección, etc [42].

2.7.1.1 Criterios de selección.

Los UPS son sumamente necesarios para el correcto funcionamiento del CCTV, ya que este debe trabajar continuamente para brindar una cobertura total de seguridad al Laboratorio de Informática, ya sea con la presencia o ausencia de energía eléctrica. Además la presencia de este dispositivo ayuda al buen funcionamiento y a alargar la vida útil de los equipos del CCTV.

Entre los requerimientos que el UPS debe cumplir, encontramos:

- Un UPS que brinde protecciones 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.
- Contar con un UPS que cumpla los requerimientos de potencia del CCTV, para ello es necesario listar a todos los equipos del Circuito Cerrado de Televisión con su respectiva potencia en Watts o en VA.

[42] UPS (Uninterrupted Power System). – http://www.c-mos.com/pdfsproductos/manual_de_ventas_UPS_reducido.pdf

- Considerar el tiempo de respaldo que el UPS brinda a los equipos durante la ausencia de energía eléctrica.

2.7.1.2 Dimensionamiento del UPS.

Un excelente dimensionamiento del UPS permite aprovechar al máximo el grado de autonomía de este equipo, para alcanzar excelentes niveles de eficiencia es aconsejable que el UPS opere entre el 50% y 100% de su capacidad.
Para realizar el dimensionamiento del UPS se procede de la siguiente manera:

1. Listar todos los equipos del CCTV que serán protegidos por el UPS.
2. Registrar los valores de potencia aparente de los dispositivos listados en el paso 1.
3. En el caso en el que la potencia de los dispositivos esté expresada en Watts (potencia real) es necesario convertir a VA, para esto, se procede a dividir por un factor de potencia de 0.7, este valor es estándar para equipos computacionales.
4. Se procede a sumar cada una de las potencias, para encontrar un Subtotal.
5. Al valor encontrado en el paso anterior se multiplica por un factor de seguridad, en el presente proyecto se consideró de un 25%. Este nuevo valor se llama Subtotal_1.
6. Finalmente se procede a sumar Subtotal y Subtotal_1 para encontrar la potencia total del UPS.

En la tabla 2.14, se encuentra detallado los dispositivos del CCTV y sus respectivos valores de potencia.

CANTIDAD	EQUIPOS PROTEGIDOS	VOLTS (V)	AMPERIOS (A)	WATTS (W)	VA
1	Switch 3560 (24 Puertos)	-	-	100,00	142,86
1	Switch 2960 (24 Puertos)	-	-	150,00	214,29
1	Router Inalámbrico WRT 300N	12,00	1,00	8,40	12,00
1	Servidor	-	-	300,00	428,57
3	Cámaras IP	-	-	5,00	7,14
				Sub Total	**804,86**
				Fac. Seguridad 25%	**201,21**
				VA requerido	**1006,07**

Tabla 2. 14 Dimensionamiento del UPS.

Con este valor se procede a seleccionar un UPS que cumpla con esa cantidad de potencia. En el Laboratorio de Informática se encuentra un UPS con una capacidad de 2 KVA, el mismo que cumple con los requerimientos y soporta el valor de potencia requerido.

2.7.2 INSTALACIÓN DE LAS CÁMARAS INALÁMBRICAS IP.

Las cámaras deben estar fuera del alcance de cualquier persona, por este motivo se las ubica a una altura aproximada de 3 metros.

Las conexiones eléctricas de cada cámara deben terminar en la sala D, debido a que en ese lugar se encuentra el UPS.

2.7.2.1 Instalación de la cámara Entrada Principal.

La ubicación de la cámara “Entrada Principal” está en la parte posterior del ingreso principal, de esta manera se tiene completa visibilidad tanto de la entrada, como del pasillo. En la figura 2.25, se indica la ubicación de la cámara “Entrada principal”.

Figura 2. 25 Ubicación de la cámara “Entrada Principal”.

En la figura 2.26, se indica la visión de la cámara “Entrada Principal” durante el día.

Figura 2. 26 Visión de la cámara “Entrada Principal” durante el día.

En la figura 2.27, se indica la visión de la cámara “Entrada Principal” durante la noche.

Figura 2. 27 Visión de la cámara “Entrada Principal” durante la noche.

2.7.2.2 Instalación de la cámara Entrada Posterior.

La ubicación de la cámara “Entrada Posterior” se realizó al final del pasillo central, ubicándola con la vista hacia la entrada proveniente del séptimo y quinto piso. En la figura 2.28, se indica la ubicación de la cámara en la entrada posterior.

Figura 2. 28 Ubicación de la cámara “Entrada Posterior”.

En la figura 2.29, se indica la visión de la cámara “Entrada Posterior” durante el día.

Figura 2. 29 Visión de la cámara “Entrada Posterior” durante el día.

En la figura 2.30, se indica la visión de la cámara “Entrada Posterior” durante la noche.

Figura 2. 30 Visión de la cámara “Entrada Posterior” durante la noche.

2.7.2.3 Instalación de la cámara Cafetería.

La ubicación de la cámara “Cafetería” está en la entrada a la Cafetería, ubicándola con la vista hacia los armarios donde se encuentran los equipos de conectividad de la academia ACIERTE. En la figura 2.31, se indica la ubicación de la cámara “Cafetería”.

Figura 2. 31 Ubicación de la cámara “Cafetería”.

En la figura 2.32, se indica la visión de la cámara “Cafetería” durante el día.

Figura 2. 32 Visión de la cámara “Cafetería” durante el día.

En la figura 2.33, se indica la visión de la cámara “Cafetería” durante la noche.

Figura 2. 33 Visión de la cámara “Cafetería” durante la noche.

2.7.3 INSTALACIÓN DEL ROUTER INALÁMBRICO.

El router Inalámbrico se instala en la mitad del pasillo central como se indica en la figura 2.34

Figura 2. 34 Instalación del router Inalámbrico.

La alimentación eléctrica del router inalámbrico proviene del UPS ubicado en la Sala D.

2.7.4 INSTALACIÓN DEL SERVIDOR.

El servidor se ubicó en el taller de computadoras. En la figura 2.35, se indica la ubicación de servidor.

Figura 2. 35 Instalación del Servidor.

La alimentación eléctrica del servidor proviene del UPS ubicado en la Sala D.

2.8 CONFIGURACIÓN DE EQUIPOS.

2.8.1 CONFIGURACIÓN DEL ROUTER INALÁMBRICO.

En esta sección se presenta la configuración de los parámetros del Router Inalámbrico WRT300N como son: el SSID, dirección IP, canal de trabajo, la seguridad del dispositivo y NAT. Para obtener mayores ventajas y aprovechar los recursos del Router Inalámbrico se reemplaza el IOS existente en el router por un IOS llamado DD-WRT.

DD-WRT es un IOS diseñado para routers inalámbricos marca Linksys, Buffalo, D-Link, TP-Link, entre otros, este IOS es basado en Linux, que permite optimizar

al máximo los recursos del router inalámbrico, las características principales que este programa presenta son:

- Compatibilidad con más de 200 Dispositivos.
- Soporta todos los estándares WLAN actuales (802.11 a/b/g/n).
- Gestión de Ancho de Banda.
- Interfaz de usuario multilingüe, tiene 13 idiomas diferentes.
- Ajuste de potencia de transmisión.
- Soporta diversos sistemas de Hotspot.

2.8.1.1 INSTALACIÓN DEL PROGRAMA DD-WRT[43].

El IOS DD-WRT no tiene costo y se puede descargar desde la página WEB del programa. Antes de proceder con la instalación se debe observar los requerimientos de este software:

- 8 MB de memoria flash.
- 32 MB de memoria RAM.

El Router inalámbrico WRT300N V1.1 cumple con estos requerimientos, por lo que la instalación se desarrolla con total normalidad.

NOTA: El datasheet del router inalámbrico WRT300N se encuentra en el Anexo E.

Para iniciar la configuración el Router Inalámbrico, este equipo debe estar conectado a una PC mediante un cable UTP directo, posteriormente en el campo de dirección IP de un explorador Web se ingresa la dirección IP predeterminada del equipo:

192.168.1.1

A continuación aparece un mensaje indicando que se debe completar el campo nombre y contraseña, tal como se indica en la figura 2.36.

[43] INSTALACIÓN DEL PROGRAMA DD-WRT.- http://www.dd-wrt.com/

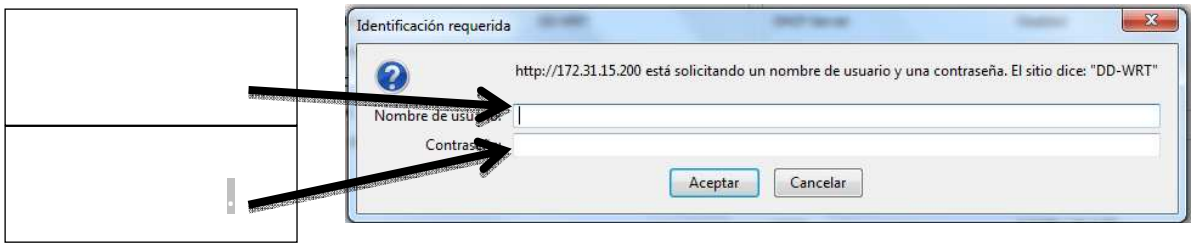


Figura 2. 36 Campo nombre de usuario y contraseña.

2.8.1.2 Configuración de la pestaña Configuraciones Opcionales.

En este campo se configura el nombre del Host y el dominio al que el equipo pertenece tal como se indica en la figura 2.37.

Figura 2. 37 Configuración de la pestaña Configuraciones Opcionales.

2.8.1.3 Configuración de la pestaña Instalación de la WAN.

La configuración de la pestaña WAN consiste en asignar una dirección IP al Router, para que este se conecte a la red de datos del Laboratorio Informática. La dirección IP designada para este dispositivo es 172.31.15.200. En la figura 2.38, se indica la configuración de la pestaña WAN.

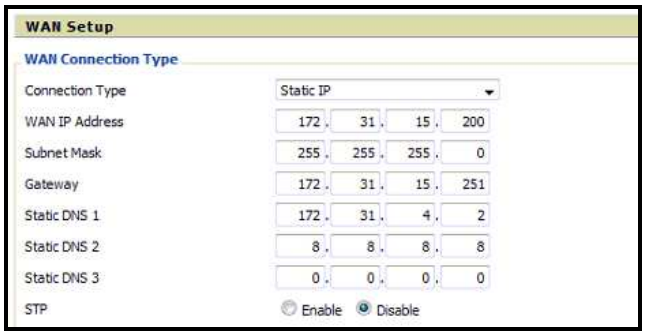


Figura 2. 38 Configuración de la pestaña WAN.

2.8.1.4 Configuración de la pestaña Instalación de Red.

En este campo se configura la dirección IP, la máscara de Red, el Gateway y el DNS local, tal como se indica en la figura 2.39.

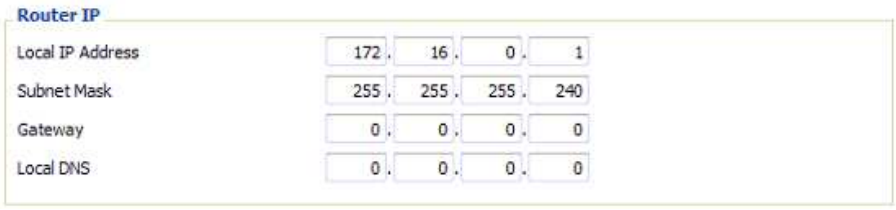


Figura 2. 39 Configuración de la pestaña Instalación de Red.

2.8.1.5 Configuración de la pestaña Seguridad de Red.

El método de seguridad que se va a emplear es el WPA2 Personal y se emplea el protocolo de encripción AES. En la figura 2.40, se indica la pestaña seguridad de red.

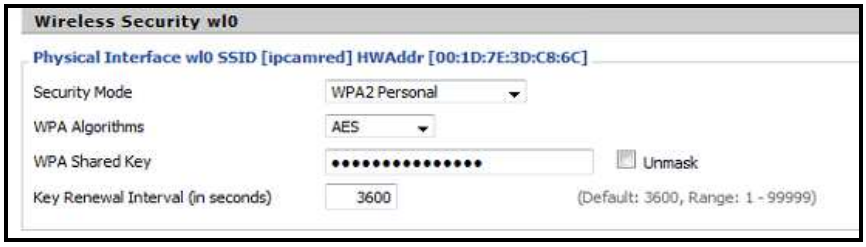


Figura 2. 40 Configuración pestaña seguridad de red.

2.8.1.6 Configuración de las Interfaces Físicas Inalámbricas.

En este campo se configura los siguientes parámetros:

- El SSID, el nombre que se seleccionó fue ipcamred, para hacer referencia a la red de cámaras inalámbricas.
- Modo de operación que se seleccionó es Access Point.
- El estándar en que trabaja es IEEE 802.11G.
- El canal que seleccionó es el 11.

En la figura 2.41, se indica la configuración de la pestaña interfaces físicas inalámbricas.

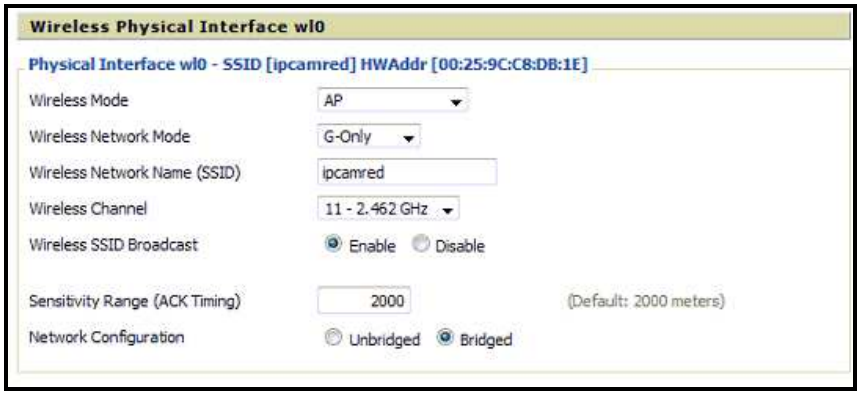


Figura 2. 41 Configuración de la pestaña interfaces físicas inalámbricas.

2.8.1.7 Configuración de NAT en el router inalámbrico.

La configuración del NAT es algo indispensable para obtener el streaming de video de cada una de las cámaras desde una red distinta a la del circuito cerrado de televisión.
En este campo se configura un NAT estático, para ello necesitamos la dirección IP interna, el puerto de entrada y el puerto de salida de cada cámara.

A continuación, se indican los campos de configuración.

- **Aplicación**.- En este campo se escribe un nombre para identificar la aplicación que se está realizando.
- **Desde el Puerto**.- En este campo se escribe el puerto de origen.
- **Protocolo**.- En este campo se escribe el protocolo que se utiliza.
- **Dirección IP**.- En este campo se escribe la dirección IP interna.
- **Puerto Para**.- En este campo se escribe el puerto de destino.

Una vez configurado el NAT, se habilita la pestaña “Habilitado” y finalmente se guarda la configuración.

En la figura 2.42, se indican los campos que se deben completar para llevar a cabo la configuración del NAT.

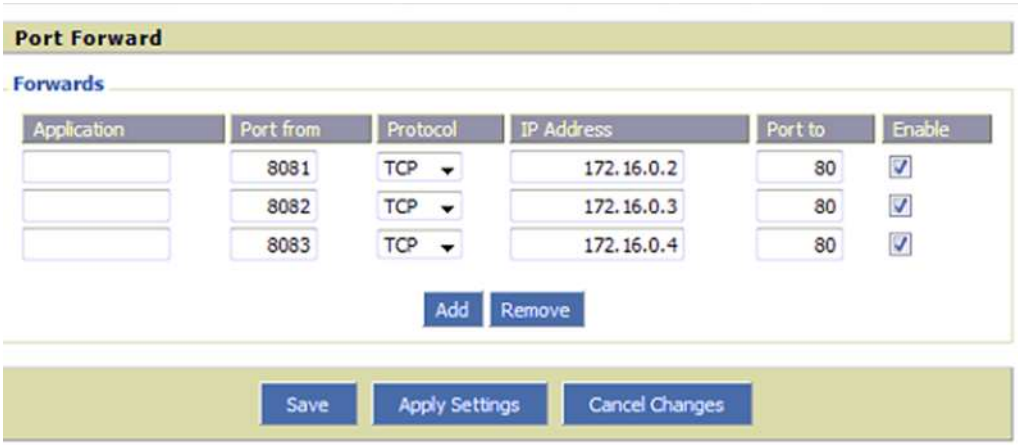


Figura 2. 42 Configuración de NAT en el Router Inalámbrico.

En la tabla 2.15, se indica las configuraciones de NAT realizadas.

Descripción	Dirección IP interna	NAT
Entrada_Principal	172.16.0.2	172.31.15.200:8081
Entrada_Posterior	172.16.0.3	172.31.15.200:8082
Cafetería	172.16.0.4	172.31.15.200:8083

Tabla 2. 15 Configuración de NAT de realizadas.

2.8.2 INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO.

2.8.2.1 Instalación del sistema operativo.

NOTA: La instalación del sistema Operativo CentOS 5.4 se encuentra en el Anexo F.

CentOS por defecto ejecuta varios servicios, los mismos que para el desarrollo del presente Proyecto no interesa que se ejecuten. A continuación, se indica los servicios que ZoneMinder no necesita para su funcionamiento.

- apmd.
- bluetooth.
- cups.
- hidd.
- ip6tables.
- iptables.
- netfs.
- nfslock.
- pcscd.
- portmap.

2.8.2.2 Configuración del sistema operativo.

La configuración del sistema operativo CentOS comprende la instalación y configuración de:

- Servidor WEB Apache.
- Servidor de correo electrónico Postfix.
- Firewall.
- ZoneMinder.

2.8.2.2.1 Instalación y configuración del Servidor WEB Apache.

2.8.2.2.1.1 Configuración del servicio web seguro[44].

Para la configuración de un sitio web con seguridad SSL, es necesario tener instaladas dependencias, las mismas que se obtienen ejecutando la línea de código 2.1:

```
> yum install httpd mod_ssl openssl
```

Línea de Código 2. 1 Instalación servicio de SSL.

Un certificado SSL es una **"firma electrónica que acredita identidad y credenciales".** Cuando se acceda alguna página web segura, se identifica un servidor determinado, o se realiza alguna transacción que implica el ofrecer datos confidenciales a través de la página web segura[45].

En la línea de código 2.2, se realiza la creación de un certificado auto firmado. Este certificado no va a ser firmado por una empresa certificadora, sino que va a ser auto validado.

```
# Se genera la llave privada
openssl genrsa -out ca.key 1024
# Se genera CSR
openssl req -new -key ca.key -out ca.csr
# Se genera una llave autofirmada
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
#Se copia los archivos generados en los lugares adecuados
cp ca.crt /etc/pki/tls/certs
cpca.key /etc/pki/tls/private/ca.key
cpca.csr /etc/pki/tls/private/ca.csr
```

Línea de Código 2. 2 Creación y auto validación de un certificado SSL.

[44] Configuración del sitio web seguro. - http://wiki.centos.org/HowTos/Https
[45] http://www.tecnologiapyme.com/servicios-web/para-que-sirven-los-certificados-ssl

En el archivo de configuración del servicio web con seguridades, se debe buscar la línea SSLCertificateFile para indicar la ubicación de los certificados creados y firmados previamente. En la línea de código 2.3, se ubica y se edita el archivo de configuración.

```
> vi +/SSLCertificateFile /etc/httpd/conf.d/ssl.conf
```

Línea de Código 2. 3 Edición del archivo de configuración ssl.conf.

La edición de este archivo consiste en direccionar las consultas a las ubicaciones de los archivos generados previamente. En la línea de código 2.4, se indica la edición del archivo ssl.conf.

```
<VirtualHost 172.31.15.253:443>
SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/ca.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
<Directory /var/www-ssl/html>
AllowOverride All
</Directory>
DocumentRoot /var/www-ssl/html
ServerName ipcam.server.com
</VirtualHost>
```

Línea de Código 2. 4 Edición del archivo ssl.conf para seguridad SSL.

2.8.2.2.1.2 Configuración de autenticación.[46]

El servidor web apache permite crear un módulo de autenticación usando el protocolo http o https. Existen dos tipos de autenticación, el primero es autenticación Básica y la segunda es autenticación Digest. La autenticación

[46] Configuración de la autenticación..- http://httpd.apache.org/docs/2.0/es/howto/auth.html

Básica consiste en enviar tanto el nombre y la contraseña por texto plano y la autenticación Digest consiste en enviar el nombre y la contraseña encriptados usando MD5 (*Message-Digest Algorithm 5 - Algoritmo de Resumen del Mensaje 5*).

En la configuración del servicio web seguro, se utiliza la autenticación Basic debido a que en la web ya se ha implementado seguridades. La implementación de la autenticación se basa en configurar el archivo ssl.conf, mencionado en la línea de código 2.4 y crear un usuario y una contraseña.

En la línea de código 2.5, se crea un archivo que contiene el nombre de usuario y contraseña encriptados para ser usados en la autenticación y se asignan permisos sobre este al usuario apache.

```
>htpasswd -c /var/www/docs/.htpasswd root
>chown apache.apache  /var/www/docs/.htpasswd
```

Línea de Código 2. 5 Creación y permisos del archivo para la autenticación.

En la línea de código 2.6, se indica la edición del archivo de configuración ssl.conf, esto permite que al momento de ingresar al sitio web se requiera de un usuario y una contraseña.

```
<Directory "/var/www-ssl/html/">
AuthType Basic
AuthName "AccesoRestringido"
AuthUserFile /var/www/docs/.htpasswd
Require user root [username,username]
</Directory>
```

Línea de Código 2. 6 Edición del archivo ssl.conf para autenticación.

2.8.2.2.2 Instalación y configuración del Servidor de correo electrónico Postfix para reenvío de correo. [47]

En principio sería posible instalar un servidor de correo en cualquier equipo conectado a Internet con una dirección IP pública o privada, pero debido al problema del spam, mucho de los servidores de correo de Internet bloquean el correo. Los servidores de correo tales como gmail, hotmail, yahoo entre otros recibirían este correo pero lo detectarían como spam.
Una solución es instalar un servidor de correo que no envíe directamente el correo al servidor destino, sino que utilice el servidor SMTP de gmail para que reenvíe (relay) los mensajes[48]. Se configura un relay de correo debido a que no es necesario recibir correo, solo se necesita enviar.

En la figura 2.43, se indica el proceso de reenvío de correo.

[47] Instalación y configuración del Servidor de correo electrónico Postfix para reenvío de correo.- http://carlton.oriley.net/blog/?p=31
[48] http://albertomolina.wordpress.com/2009/01/04/configurar-postfix-a-traves-de-un-relay-host-autenticado-gmail/

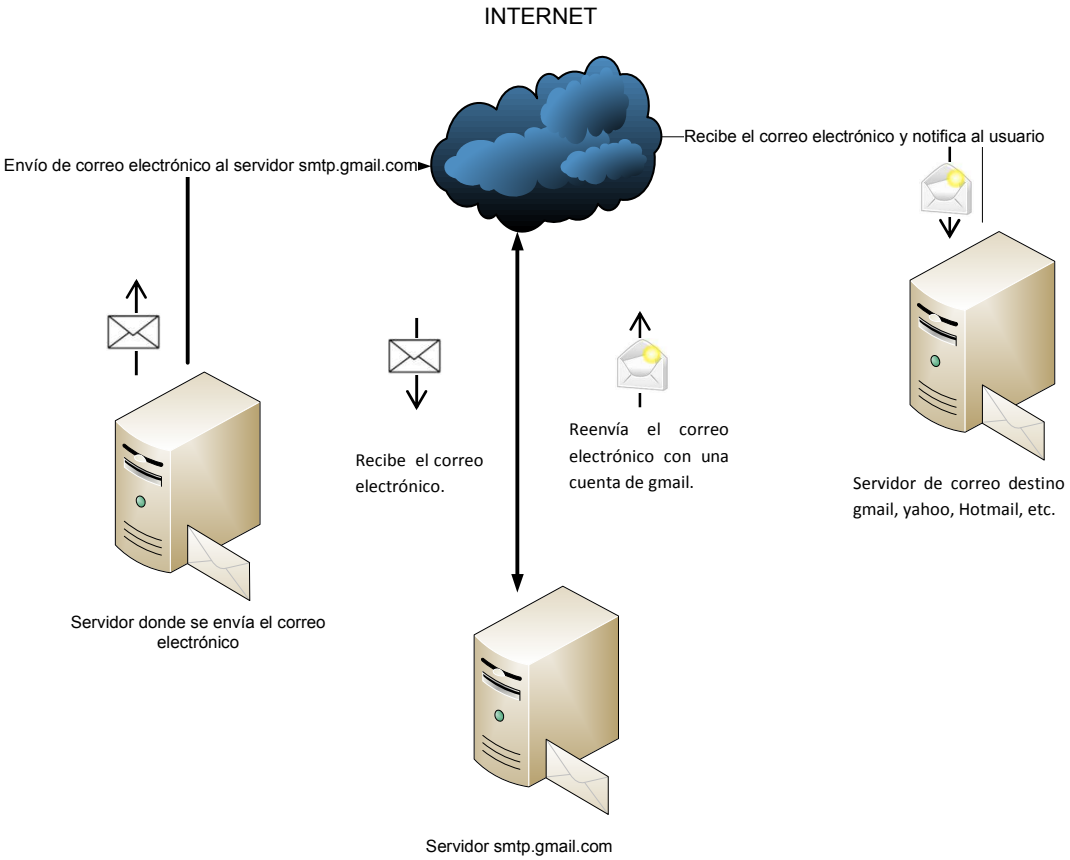


Figura 2. 43 Proceso de reenvío de correo.

A partir de la figura 2.43, se observa que el servidor de correo envía el correo electrónico hasta un servidor SMTP de gmail, desde este sitio se reenvía el correo con una cuenta de gmail hasta el servidor de correo de destino, de esta manera se evita que el correo sea detectado como un spam.

La configuración del servidor de correo se realiza utilizando Postfix como agente de transporte de correo. La instalación de Postfix se indica en la línea de código 2.7.

```
> yum install -y postfix
```

Línea de Código 2. 7 Instalación de Postfix.

Para indicar a Postfix que debe reenviar el correo, se debe editar el archivo main.cf; como se indica en la Línea de Código 2.8.

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

Línea de Código 2. 8 Instalación de Postfix.

Con estas líneas de código se indica que se reenvié todo el correo electrónico saliente del servidor Postfix hacia el servidor SMTP por el puerto 587, indicando que la ubicación del nombre de usuario y contraseña se encuentran en el archivo passwd.

A continuación se debe crear el archivo que contenga el nombre de usuario y contraseña de la cuenta de gmail. En la línea de código 2.9, se indica la creación del archivo passwd.

```
>vim /etc/postfix/sasl/passwd
```

Línea de Código 2. 9 Creación del archivo passwd.

Posteriormente se debe cambiar los permisos del archivo passwd y transformarlo a un fichero indexado de tipo hash como se indica en la Línea de Código 2.10.

```
chmod 600 /etc/postfix/sasl/passwd
postmap /etc/postfix/sasl/passwd
```

Línea de Código 2. 10 Cambio de permisos e indexado tipo hash del archivo passwd.

2.8.2.2.3 Instalación y configuración del Firewall del Servidor.

Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos[49].

En la figura 2.44, se indica el diagrama de red del CCTV incluido el firewall.

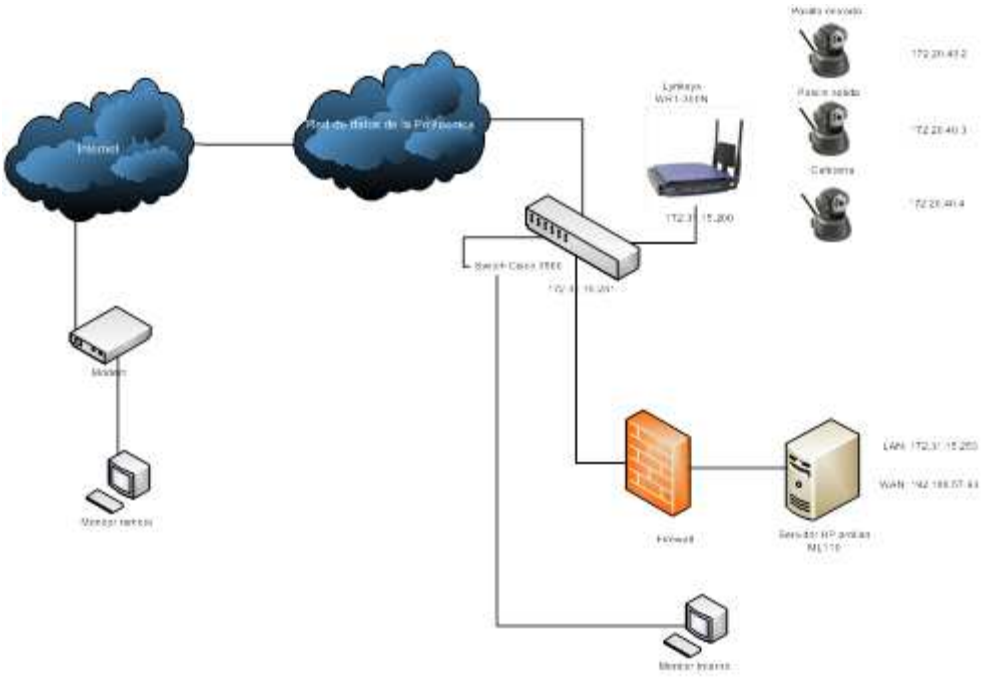


Figura 2. 44 Diagrama de Red del CCTV IP.

El Firewall para el servidor debe permitir únicamente la conexión por ciertos puertos, los mismos que son necesarios para el monitoreo y administración de ZoneMinder. En la tabla 2.16, se indica los puertos necesarios para el funcionamiento del servidor y la función que cumplen.

Puerto	Protocolo	Función en el Servidor
80	TCP	Permite la conexión al Servidor Web.
22	TCP	Permite la administración remota del servidor.

[49] http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

Puerto	Protocolo	Función en el Servidor
443	TCP	Permite conexiones Seguras en el servidor.
587	TCP	Permite conexiones con servidores externos SMTP.
53	UDP	Permite resoluciones de dominio en servidores DNS.
123	UDP	Permite conexiones con servidores NTP.
8081	TCP	Permite conexiones al router inalámbrico.
8082	TCP	Permite conexiones al router inalámbrico.
8083	TCP	Permite conexiones al router inalámbrico.
8084	TCP	Permite conexiones al router inalámbrico.

Tabla 2. 16 Lista de puertos necesarios para el funcionamiento del servidor.

En el presente Proyecto se implementa un firewall en Linux mediante un script, en el cual se permite o se niega el tráfico por protocolos y puertos, además este programa va a trabajar como un demonio que se debe iniciar cada vez que se reinicie el servidor.

NOTA. El script del Firewall se encuentra en el **Anexo G**.

2.8.3 INSTALACIÓN DEL SOFTWARE ZONEMINDER[50].

2.8.3.1 Instalación de dependencias.

ZoneMinder es un programa cuya instalación se realiza por tres métodos diferentes:

1. Instalación desde código fuente.
2. Instalación desde paquetes pre-compilados.
3. Usando un Live CD.

[50] INSTALACIÓN DEL SOFTWARE ZONEMINDER http://www.zoneminder.com/wiki/index.php/Documentation

De los tres métodos de instalación, el que se hace a través del código fuente es el más utilizado, debido a que el proceso de instalación consiste en compilar el código fuente, el cual puede ser ajustado a los requerimientos personales y no se sujeta a una regla fija como es el caso de la instalación a través de paquetes pre-compilados o desde Live CD.

La instalación desde el código fuente necesita varios compiladores, ZoneMinder usa como compilador a PERL siendo este uno de las dependencias fundamentales para la instalación.
ZoneMinder necesita un conjunto de dependencias para su compilación y ejecución, si una de estas dependencias no se encuentra presente, el proceso de compilación e instalación se verá interrumpido hasta que esta sea solucionada.

2.8.3.2 Compilación del Software Zoneminder.

Para definir la configuración de ZoneMinder se debe ejecutar el script de configuración. Por lo que se debe tener en cuenta ciertos parámetros que son incluidos para crear la base de datos. Cada uno de estos parámetros se detalla a continuación.

- Directorio Web donde se va a instalar los archivos PHP, en nuestro caso:

  /var/www-ssl/html/

- Directorio donde se instalarán los archivos CGI, en este caso:

  /var/www-cgi/

- Nombre Host en el cual se crea la base de datos, en este caso:

  localhost

- Nombre de la base de datos que interactúa con ZoneMinder, en este caso:

  zm

- Nombre de Usuario que tiene acceso a la base de datos, en este caso:

  root

- Contraseña del usuario que creó la base de datos.
  CoNtRa$3Ñ@

Para ejecutar el script de configuración, debemos ejecutar la línea de código 2.11 en una terminal dentro de la carpeta que contenga el código fuente de ZoneMinder.

```
>./configure --with-webdir=/var/www-ssl/html --with-cgidir=/var/www/cgi-bin ZM_DB_HOST=localhost, ZM_DB_NAME=zm ZM_DB_USER=root ZM_DB_PASS=CoNtRa$3Ñ@
```

Línea de Código 2. 11 Instrucción para la configuración pre-instalación.

NOTA: La contraseña escrita anteriormente es ficticia por razones de seguridad.

En el momento en que se ejecuta la configuración de ZoneMinder este no se compila, solo se ajusta a las características del host y crea variables. Una vez terminada la configuración se genera un archivo llamado *makefile* que permite la compilación y desempaquetado del software el cual se realiza en la misma carpeta.
Concluida la configuración del servidor se debe continuar con la compilación del software. En la línea de código 2.12, se indica la instrucción para la ejecución del archivo makefile.

```
>make
```

Línea de Código 2. 12 Instrucción para la ejecución del archivo makefile.

Ahora el software está listo para ser copiado en las carpetas correspondientes para su correcta ejecución, para ello se debe ejecutar el comando que se indica en la línea de código 2.13.

```
>make install
```

Línea de Código 2. 13 Instrucción para la instalación del software.

Esta instrucción debe ser ejecutada como súper usuario debido a que necesita permisos para copiar archivos en carpetas del sistema.
Esta rutina de instalación copiará los binarios y scripts a los directorios destinados para la instalación, usualmente se instala en carpeta /usr/local/bin y luego los moverá “ZMS” al área cgi-bin. Luego copiará los archivos PHP al directorio que se ha especificado asegurándose que se tenga los suficientes permisos e instalará módulos PERL de ZoneMinder en los lugares ya especificados por el compilador PERL. También instala una copia del archivo zm.conf (el cual es generado en el proceso de configuración) al área de configuración de su sistema, y finalmente crea un link de zm.PHP a index.PHP para el acceso por la web.

ZoneMinder trabaja con bases de datos absolutamente para todo, desde el registro de los usuarios hasta el registro de los eventos, por lo que se debe crear la base de datos que se especificó en la configuración de ZoneMinder.

En la línea de código 2.14, se presenta la instrucción para ingresar a la base de datos MySQL.

```
>mysql
```

Línea de Código 2. 14 Instrucción para ingresar a la base de datos MySQL.

Dentro del ambiente de MySQL se debe otorgar permisos para su ingreso, que por defecto está deshabilitada. En la línea de código 2.15, se asigna permisos al usuario root para que pueda ingresar a la base de datos con su contraseña.

```
mysql>SET PASSWORD FOR root@localhost=PASSWORD('CoNtRa$3Ñ@');
```

Línea de Código 2. 15 Instrucción para autenticarse para ingresar a la base de datos MySQL.

Crear una base de datos para el uso de ZoneMinder es fundamental, para eso se crea una base de datos llamada zm, este nombre es debido a que en la

configuración se especificó que ZoneMinder trabajará con una base de datos llamada zm. En la línea de código 2.16, se presenta la instrucción para crear una base de datos.

```
mysql>create database zm;
```

Línea de Código 2. 16 Instrucción para crear una base de datos zm.

El usuario con el que ZoneMinder ingrese a la base de datos debe tener permisos, es por este motivo que se ingresa la línea de código 2.17.

```
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on zm.* to root@localhost;
```

Línea de Código 2. 17 Instrucción que asigna permisos para manipular una base de datos zm.

De igual manera el usuario que desee manipular esta base de datos debe autenticarse previamente, para ello se asigna una contraseña para el ingreso tal y como se indica en la línea de código 2.18.

```
mysql>SET PASSWORD FOR root@localhost=PASSWORD('CoNtRa$3Ñ@');
```

Línea de Código 2. 18 Instrucción que asigna una contraseña para el ingreso a la base de datos zm.

Concluida la creación de la base de datos se abandona la consola de MySQL.

```
mysql>exit;
```

Línea de Código 2. 19 Instrucción para salir de la consola de MySQL.

ZoneMinder por defecto trae una plantilla con una base de datos estándar y fundamental para el inicio y ejecución del mismo, por lo que el contenido de esta

base de datos va a ser la entrada estándar de la base de datos zm. En la línea de código 2.20, se indica el comando que se utiliza para disponer del contenido del archivo zm_create.sql como entrada estándar de la base de datos zm.

```
>mysql -u root -p zm<db/zm_create.sql
```

Línea de Código 2. 20 Instrucción para enviar el contenido de la base de datos *zm_create a la base de datos zm.*

ZoneMinder consta de un archivo que permite iniciar, reiniciar o detener todos sus módulos. Este archivo debe ser copiado en la carpeta /etc/init.d/ que contiene a todos los demonios que ejecutan o detienen servicios. Además de esto se tiene que otorgar permisos de ejecución. En la línea de código 2.21, se indica la asignación de permisos de ejecución de este archivo.

```
>chmod +x /etc/init.d/zm
```

Línea de Código 2. 21 Instrucción para asignar permisos de ejecución al archivo zm.

Para que este servicio se ejecute cada vez que se reinicia el sistema, se debe cambiar su nivel de ejecución tal y como se indica en la línea de código 2.22.

```
>chkconfig zm on
```

Línea de Código 2. 22 Instrucción para cambiar el nivel de ejecución al archivo zm.

Para finalizar con la instalación se debe iniciar el servicio de ZoneMinder. En la línea de código 2.23, se indica la instrucción que permite iniciar este servicio.

```
>service zm start
```

Línea de Código 2. 23 Instrucción para iniciar el servicio de ZoneMinder.

Concluida la instalación, se puede ingresar a un explorador de internet y digitar la dirección IP del servidor. En la tabla 2.17, se indican las direcciones IP a las que se puede ingresar al servidor.

Sitio	Dirección IP
Desde la Polired.	172.31.15.253
Fuera de la Polired.	192.188.57.193

Tabla 2. 17 Asignación de direcciones IP al servidor.

2.8.4 CONFIGURACIÓN DE ZONEMINDER[51].

2.8.4.1 Configuración de Monitores.

El principal objetivo del circuito cerrado de televisión es mantener registro de toda actividad generada dentro del campo de visión de cada una de las cámaras, por lo que cada cámara debe grabar permanentemente.
En el capítulo I se indica las opciones de configuración de un monitor, con dichos conocimientos se puede configurar de una forma más orientada cada una de las cámaras.
A continuación se presenta la configuración de la cámara correspondiente a la Entrada principal.

NOTA. Únicamente se realiza la configuración de la cámara correspondiente a la entrada principal, para el resto cámaras el proceso es exactamente el mismo a diferencia de la dirección IP.

En la figura 2.45, se indica la configuración: “Pestaña General” del monitor Entrada_Principal.

[51] Configuración de Zoneminder.- http://www.zoneminder.com/wiki/index.php/Documentation

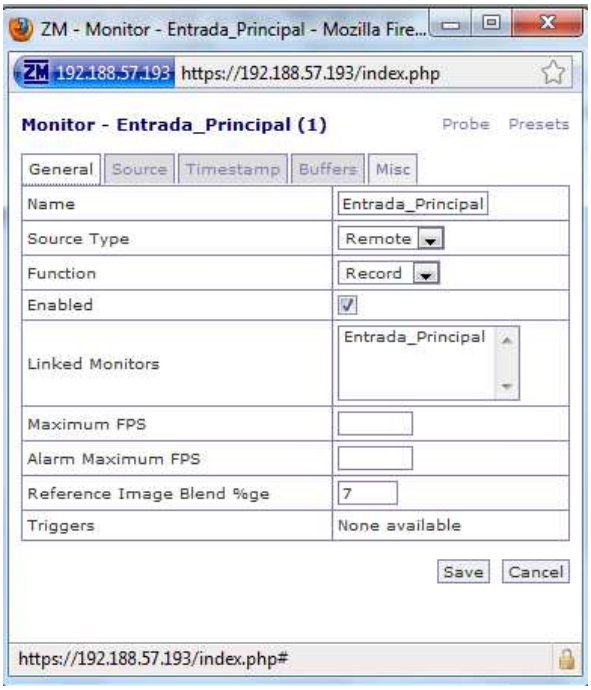


Figura 2. 45 Configuración de Pestaña General del monitor Entrada_Principal.

En la figura 2.46, se indica la configuración: “Pestaña Source” del monitor Entrada_Principal.

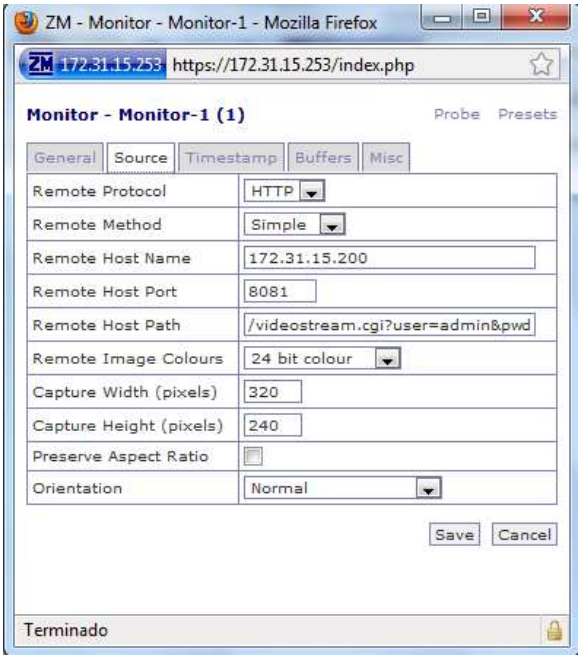


Figura 2. 46 Configuración de Pestaña Source del monitor Entrada_Principal.

Si se realizó correctamente la configuración, se apreciará el streaming de video que se muestra en la figura 2.47.

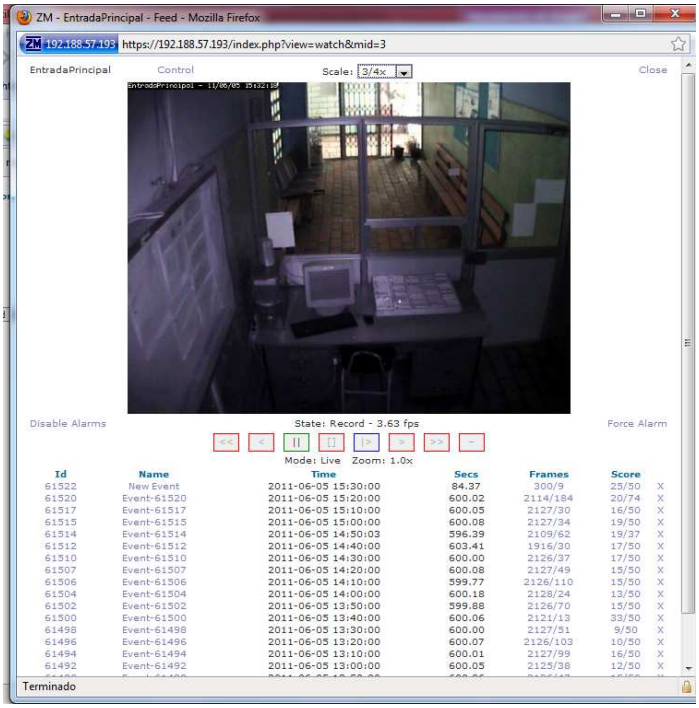


Figura 2. 47 Ventana de un monitor activo.

2.8.4.2 Configuración de Paneo y Cabeceo.

La configuración de paneo y cabeceo (PAN/TILT) de la cámara, se lo hace en base a un script escrito en PERL. La implementación de esta aplicación se realiza a partir de un formato previamente creado por ZoneMinder, que contiene un conjunto de instrucciones que hacen referencias y consultas a varios módulos escritos en PERL. Este script recibe las instrucciones que se seleccionan en la interfaz web y en función de la instrucción seleccionada ejecuta una subrutina, que envía un comando para mover la cámara. Las instrucciones de movimiento de la cámara IP FOSCAM FI8918W son únicas y difieren de otras marcas.

Existen dos maneras de obtener estas instrucciones.

1. Utilizar un sniffer para capturar los paquetes enviados desde el software propio de la cámara.
2. Buscar el set de instrucciones de administración propio de la cámara.

En este caso se obtuvo el set de instrucciones de la cámara y haciendo uso de él, se determinó los comandos correspondientes a todos los controles de la cámara y se presenta en la siguiente tabla 2.18.

Función	Comando
Arriba	decoder_control.cgi?command=2
Abajo	decoder_control.cgi?command=0
Izquierda	decoder_control.cgi?command=6
Derecha	decoder_control.cgi?command=4
Superior Izquierda	decoder_control.cgi?command=93
Superior Derecha	decoder_control.cgi?command=92
Inferior Izquierda	decoder_control.cgi?command=91
Inferior Derecha	decoder_control.cgi?command=90
Detener Movimiento	decoder_control.cgi?command=1
Aumentar Contraste	camera_control.cgi?param=1&value=$ini4
Reducir Contraste	camera_control.cgi?param=1&value=$ini3
Aumentar Brillo	camera_control.cgi?param=2&value=$ini
Reducir Brillo	camera_control.cgi?param=2&value=$ini2
Home	decoder_control.cgi?command=0
Reset	camera_control.cgi?param=2&value=4
Preset 1 (Modo 60 Hz)	camera_control.cgi?param=3&value=0
Preset 2 (Modo 50 Hz)	camera_control.cgi?param=3&value=1
Preset 3 (Modo Outdoor)	camera_control.cgi?param=3&value=2
Preset 4 (Modo Flip)	camera_control.cgi?param=5&value=0

Función	Comando
Preset 5 (Modo Flip + Mirror)	camera_control.cgi?param=5&value=1
Preset 6 (Mirror)	camera_control.cgi?param=5&value=2
Preset 7 (Default)	camera_control.cgi?param=5&value=3
Preset 8 (Movimiento Vertical)	decoder_control.cgi?command=26
Preset 9 (Detener Movimiento Vertical)	decoder_control.cgi?command=27
Preset 10 (Movimiento Horizontal)	decoder_control.cgi?command=28
Preset 11 (Detener Movimiento Horizontal)	decoder_control.cgi?command=29

Tabla 2. 18 Asignación de instrucciones para la cámara IP FI8918W[52] .

En la figura 2.48, se indica el diagrama de flujo resumido correspondiente al script que controla el movimiento de una cámara.

[52] Tabla 2. 21 Asignación de instrucciones para la cámara IP FI8918W.- http://www.notesco.net/download/ipcamcgisdk21.pdf

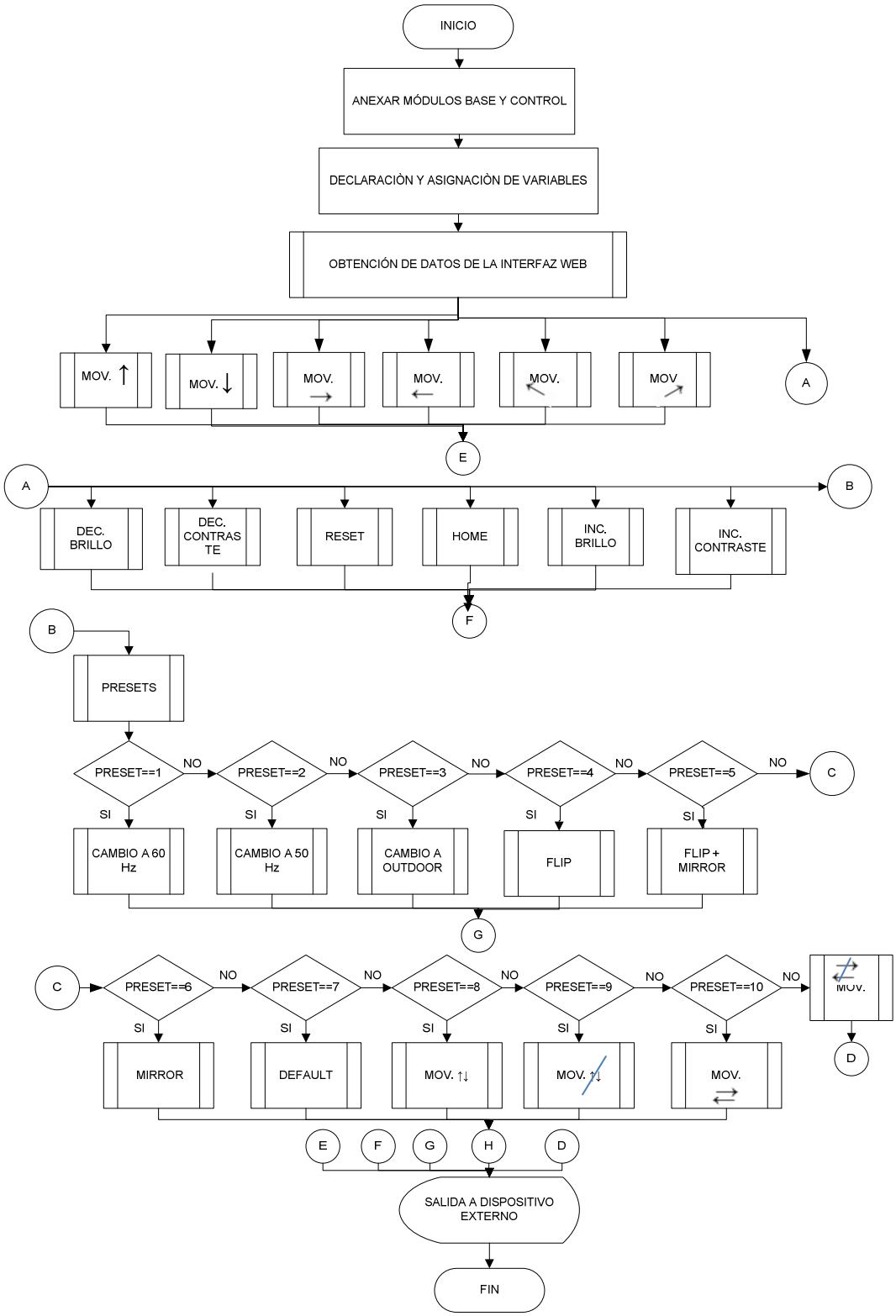


Figura 2. 48 Diagrama de flujo correspondiente al script que controla el movimiento de una cámara inalámbrica IP.

NOTA: El script que controla el movimiento de la cámara se encuentra disponible en el **Anexo H**.

El Script escrito en PERL debe ser copiado en la carpeta con el nombre Foscam F18908W:

/usr/lib/perl5/site_perl/5.8.8/ZoneMinder/Control.

También se debe configurar el movimiento de la cámara en el interfaz web, tal y como se indica en la figura 2.49, en donde se configura la pestaña control.

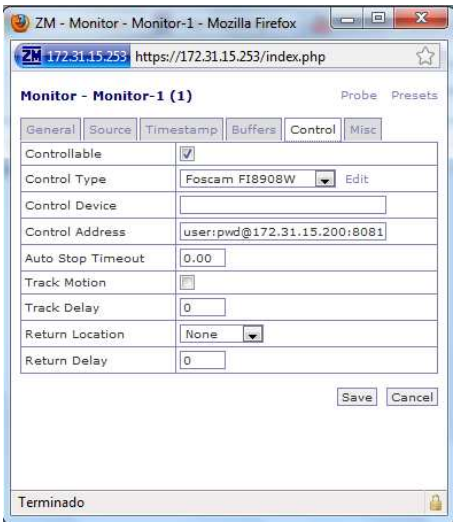


Figura 2. 49 Configuración de la Pestaña de Control.

La edición del campo Control Tipo es fundamental para indicar a ZoneMinder que tipo de funciones de movimiento están permitidas en la cámara y que modelos de cámaras están disponibles.

En la figura 2.50, se configura la pestaña Principal, en donde se indica el nombre del módulo de control, el tipo de cámara y el protocolo que hará referencia al Script creado previamente.

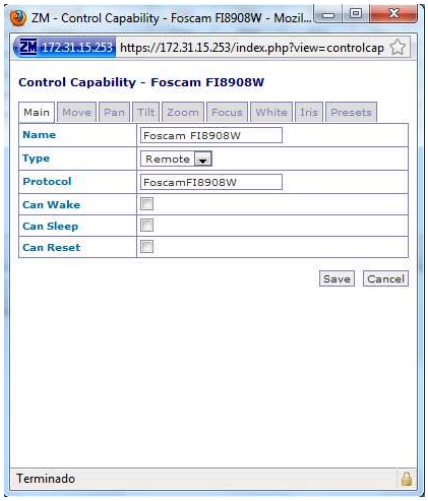


Figura 2. 50 Pestaña de configuración Principal.

En la figura 2.51, se indica la configuración de la pestaña Movimiento, que permite indicar a Zoneminder que la cámara tiene funciones de movimiento diagonal y continuo.

Figura 2. 51 Pestaña de configuración Movimiento.

En la figura 2.52, se indica la pestaña de configuración PANEO, que permite indicar a ZoneMinder que la cámara tiene funciones de movimiento horizontal.

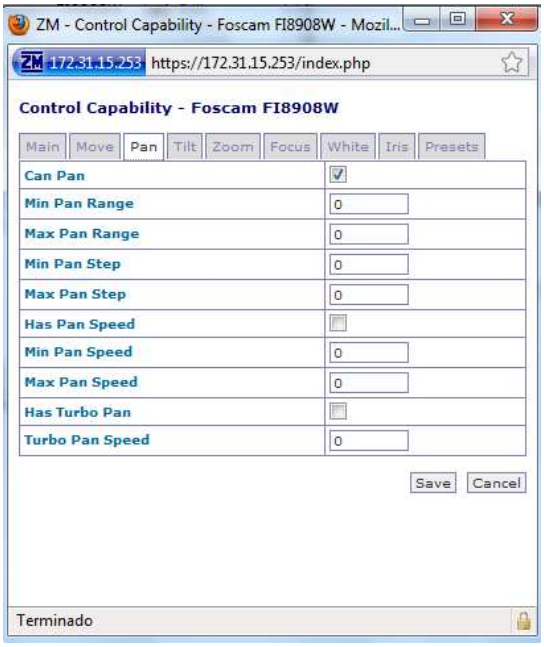


Figura 2. 52 Pestaña de configuración PANEO.

En la figura 2.53, se indica la pestaña de configuración CABECEO, que permite indicar a ZoneMinder que la cámara tiene funciones de movimiento vertical.

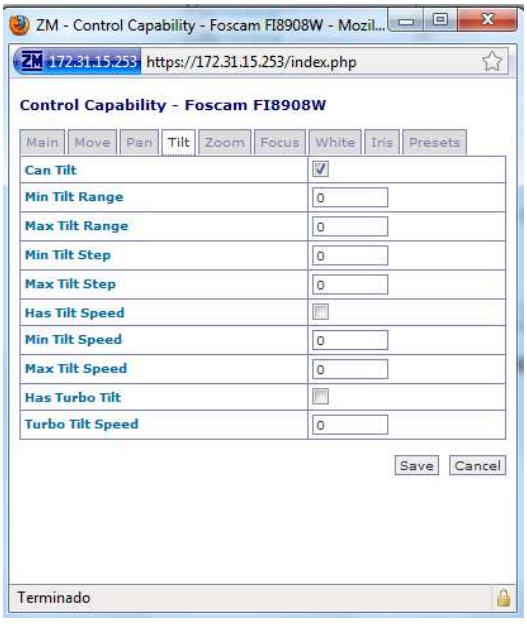


Figura 2. 53 Pestaña de configuración CABECEO.

En las figuras 2.54 y 2.55, se indican las configuraciones de las pestañas White e Iris, las cuales remplazan a las funciones de brillo y contraste propias de la cámara IP.

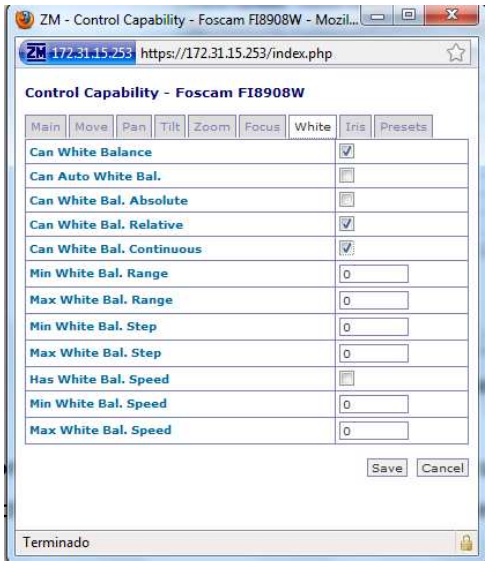


Figura 2. 54 Pestaña de configuración BLANCO.

Figura 2. 55 Pestaña de configuración Iris.

En las figuras 2.56, se indican las configuraciones de la pestaña Presets.

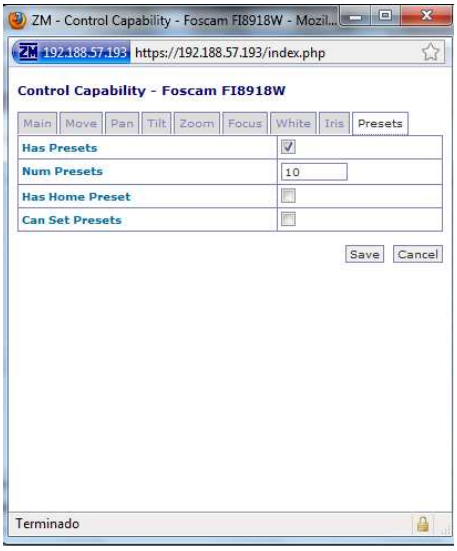


Figura 2. 56 Pestaña de configuración Presets.

Una vez configurado el control de la cámara se puede observar que la interfaz web varía generando una nueva pestaña, que permite controlar el movimiento PAN/TILT de la cámara, además del brillo y contraste tal y como se indica en la figura 2.57.

Figura 2. 57 Ventana de Monitoreo con funciones de Movimiento.

El procedimiento para la configuración del resto de cámaras mantiene el mismo procedimiento.

2.7.4.3 Configuración de envío de correo electrónico cuando se generen eventos.

ZoneMinder brinda la posibilidad de enviar correos electrónicos al usuario cuando exista movimiento inusual en el lugar vigilado, es decir cuando dentro de una zona activa exista movimiento. Por esta razón, el programa ZoneMinder necesita de un servidor de correo electrónico, el cual fue descrito anteriormente.

En la figura 2.58, se indica la pestaña de configuración para el envío de correo electrónico.

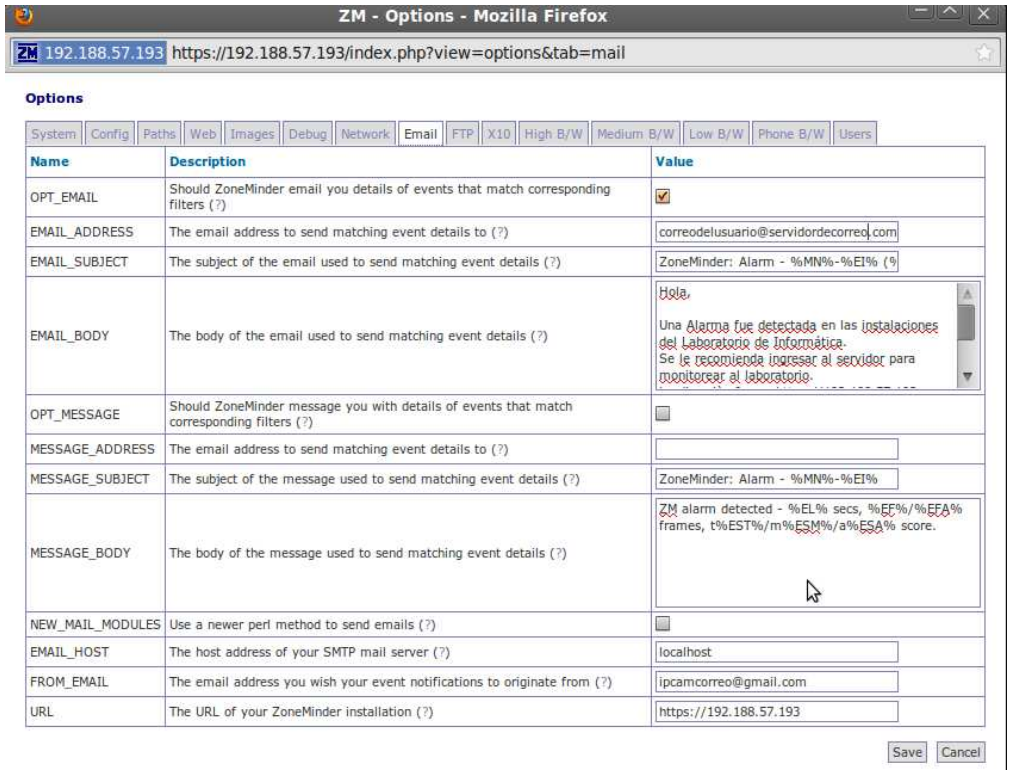


Figura 2. 58 Pestaña de configuración para el envío de correo electrónico.

En la figura 2.58, se observa que existe un campo que se llama “MESSAGE_BODY” o “Cuerpo del Mensaje”, en esta sección se puede apreciar que existe una sección denominada “Valor” en donde existe un conjunto de

wildcards o métodos abreviados, los mismos que permiten invocar información de Zoneminder y del streaming capturado.

En la tabla 2.19, se indica un conjunto de métodos abreviados.

WILDCARDS (MÉTODOS ABREVIADOS)	DESCRIPCIÓN
%EI%	Id del evento.
%EN%	Nombre del evento.
%EC%	Causa del evento.
%ED%	Descripción del evento
%ET%	Tiempo del evento.
%EL%	Duración del evento.
%EF%	Número de cuadros del evento.
%EFA%	Número de cuadros alarmas del evento.
%EST%	Puntuación total.
%ESA%	Puntuación Promedio del Evento.
%ESM%	Máxima Puntuación del Evento.
%EP%	Ruta de Acceso al Evento.
%EPS%	Ruta de Accesos a la Secuencia de Eventos.
%EPI%	Ruta de Acceso a las Imágenes de Eventos.
%EPI1%	Ruta de Acceso a la primera Imagen de un Evento.
%EPIM%	Ruta de Acceso a la primera Imagen de un Evento con el mayor puntaje.
%EI1%	Adjuntar la primera alarma de la imagen del evento.
%EIM%	Adjuntar la primera alarma de la imagen del evento con el mayor puntaje.
%EV%	Adjuntar un evento de video mpeg.
%MN%	Nombre del monitor.
%MET%	Número Total de eventos para el monitor.
%MEH%	Número de eventos para el monitor en la última hora.

WILDCARDS (MÉTODOS ABREVIADOS)	DESCRIPCIÓN
%MED%	Número de eventos para el monitor en el último día.
%MEW%	Número de eventos para el monitor en la última semana.
%MEM%	Número de eventos para el monitor en el último mes.
%MEA%	Número de eventos archivados para el monitor.
%MP%	Camino a la ventana del monitor.
%MPS%	Path to the monitor stream.
%MPI%	Camino a la imagen reciente del monitor.
%FN%	Nombre del filtro actual que coincide.
%FP%	Path del filtro actual que coincide.
%ZP%	Camino a la consola ZoneMinder.

Tabla 2. 19 Métodos Abreviados y su descripción.

2.7.4.4 Calendarización de modos de vigilancia.

La calendarización de los modos de vigilancia en un servidor es de gran utilidad, ya que permite realizar tareas dentro de un período específico, evitando ingresar al servidor para ejecutar dichas actividades manualmente.

El circuito cerrado de televisión del Laboratorio de Informática debe trabajar con un criterio diferente durante el día, la noche, de lunes a viernes, sábados, domingos y feriados.

En la tabla 2.20, se indica un calendario de una semana completa de trabajo en el Laboratorio de Informática, incluyendo el momento cuando se abre las puertas y el momento en el que se suspenden las actividades.

<table>
<tr><th>HORA</th><th>LUNES</th><th>MARTES</th><th>MIÉRCOLES</th><th>JUEVES</th><th>VIERNES</th><th>SÁBADO</th><th>DOMINGO</th></tr>
<tr><td>00H30-01H30</td><td colspan="6" rowspan="6">Sin Atención</td><td rowspan="20">Sin atención</td></tr>
<tr><td>01H30-02H30</td></tr>
<tr><td>02H30-03H30</td></tr>
<tr><td>03H30-04H30</td></tr>
<tr><td>04H30-05H30</td></tr>
<tr><td>05H30-06H30</td></tr>
<tr><td>06H30-07H30</td><td colspan="5" rowspan="14">Atendiendo</td><td rowspan="7">Atendiendo</td></tr>
<tr><td>07H30-08H30</td></tr>
<tr><td>08H30-09H30</td></tr>
<tr><td>09H30-10H30</td></tr>
<tr><td>10H30-11H30</td></tr>
<tr><td>11H30-12H30</td></tr>
<tr><td>12H30-13H30</td></tr>
<tr><td>13H30-14H30</td><td rowspan="7">Sin atención</td></tr>
<tr><td>14H30-15H30</td></tr>
<tr><td>15H30-16H30</td></tr>
<tr><td>16H30-17H30</td></tr>
<tr><td>17H30-18H30</td></tr>
<tr><td>18H30-19H30</td></tr>
<tr><td>19H30-20H30</td></tr>
<tr><td>20H30-21H30</td></tr>
<tr><td>21H30-22H30</td><td colspan="6" rowspan="3">Sin Atención</td></tr>
<tr><td>22H30-23H30</td></tr>
<tr><td>23H30-00H30</td></tr>
</table>

Tabla 2. 20 Horario de atención del Laboratorio de Informática.

La función que va a cumplir cada cámara durante una semana se indica en las tablas 2.21, 2.22 y 2.23.

<table>
<tr><th>HORA</th><th>LUNES</th><th>MARTES</th><th>MIÉRCOLES</th><th>JUEVES</th><th>VIERNES</th><th>SÁBADO</th><th>DOMINGO</th></tr>
<tr><td>00H30-01H30</td><td colspan="5" rowspan="6">Mocord</td><td rowspan="12">Mocord</td></tr>
<tr><td>01H30-02H30</td></tr>
<tr><td>02H30-03H30</td></tr>
<tr><td>03H30-04H30</td></tr>
<tr><td>04H30-05H30</td></tr>
<tr><td>05H30-06H30</td></tr>
<tr><td>06H30-07H30</td><td colspan="4" rowspan="6">Record</td><td rowspan="6">Record</td></tr>
<tr><td>07H30-08H30</td></tr>
<tr><td>08H30-09H30</td></tr>
<tr><td>09H30-10H30</td></tr>
<tr><td>10H30-11H30</td></tr>
</table>

<table>
<tr><th>HORA</th><th>LUNES</th><th>MARTES</th><th>MIÉRCOLES</th><th>JUEVES</th><th>VIERNES</th><th>SÁBADO</th><th>DOMINGO</th></tr>
<tr><td>11H30-12H30</td><td colspan="5" rowspan="8"></td><td rowspan="4"></td><td rowspan="11"></td></tr>
<tr><td>12H30-13H30</td></tr>
<tr><td>13H30-14H30</td></tr>
<tr><td>14H30-15H30</td></tr>
<tr><td>15H30-16H30</td><td rowspan="7">Mocord</td></tr>
<tr><td>16H30-17H30</td></tr>
<tr><td>17H30-18H30</td></tr>
<tr><td>18H30-19H30</td></tr>
<tr><td>19H30-20H30</td></tr>
<tr><td>20H30-21H30</td></tr>
<tr><td>21H30-22H30</td><td colspan="6" rowspan="3">Mocord</td></tr>
<tr><td>22H30-23H30</td></tr>
<tr><td>23H30-00H30</td></tr>
</table>

Tabla 2. 21 Función de monitoreo de la cámara “Entrada_Principal”.

<table>
<tr><th>HORA</th><th>LUNES</th><th>MARTES</th><th>MIÉRCOLES</th><th>JUEVES</th><th>VIERNES</th><th>SÁBADO</th><th>DOMINGO</th></tr>
<tr><td>00H30-01H30</td><td colspan="6" rowspan="6">Mocord</td><td rowspan="19">Mocord</td></tr>
<tr><td>01H30-02H30</td></tr>
<tr><td>02H30-03H30</td></tr>
<tr><td>03H30-04H30</td></tr>
<tr><td>04H30-05H30</td></tr>
<tr><td>05H30-06H30</td></tr>
<tr><td>06H30-07H30</td><td colspan="5" rowspan="13">Record</td><td rowspan="6">Record</td></tr>
<tr><td>07H30-08H30</td></tr>
<tr><td>08H30-09H30</td></tr>
<tr><td>09H30-10H30</td></tr>
<tr><td>10H30-11H30</td></tr>
<tr><td>11H30-12H30</td></tr>
<tr><td>12H30-13H30</td></tr>
<tr><td>13H30-14H30</td></tr>
<tr><td>14H30-15H30</td></tr>
<tr><td>15H30-16H30</td><td rowspan="7">Mocord</td></tr>
<tr><td>16H30-17H30</td></tr>
<tr><td>17H30-18H30</td></tr>
<tr><td>18H30-19H30</td></tr>
<tr><td>19H30-20H30</td></tr>
<tr><td>20H30-21H30</td></tr>
<tr><td>21H30-22H30</td><td colspan="6" rowspan="3">Mocord</td></tr>
<tr><td>22H30-23H30</td></tr>
<tr><td>23H30-00H30</td></tr>
</table>

Tabla 2. 22 Función de monitoreo de la cámara “Entrada_Posterior”.

<table>
<tr><th>HORA</th><th>LUNES</th><th>MARTES</th><th>MIÉRCOLES</th><th>JUEVES</th><th>VIERNES</th><th>SÁBADO</th><th>DOMINGO</th></tr>
<tr><td>00H30-01H30</td><td colspan="6" rowspan="6">Modect</td><td rowspan="24">Modect</td></tr>
<tr><td>01H30-02H30</td></tr>
<tr><td>02H30-03H30</td></tr>
<tr><td>03H30-04H30</td></tr>
<tr><td>04H30-05H30</td></tr>
<tr><td>05H30-06H30</td></tr>
<tr><td>06H30-07H30</td><td colspan="5" rowspan="12">Record</td><td rowspan="6">Record</td></tr>
<tr><td>07H30-08H30</td></tr>
<tr><td>08H30-09H30</td></tr>
<tr><td>09H30-10H30</td></tr>
<tr><td>10H30-11H30</td></tr>
<tr><td>11H30-12H30</td></tr>
<tr><td>12H30-13H30</td></tr>
<tr><td>13H30-14H30</td></tr>
<tr><td>14H30-15H30</td></tr>
<tr><td>15H30-16H30</td><td rowspan="6">Modect</td></tr>
<tr><td>16H30-17H30</td></tr>
<tr><td>17H30-18H30</td></tr>
<tr><td>18H30-19H30</td></tr>
<tr><td>19H30-20H30</td></tr>
<tr><td>20H30-21H30</td></tr>
<tr><td>21H30-22H30</td><td colspan="6" rowspan="3">Modect</td></tr>
<tr><td>22H30-23H30</td></tr>
<tr><td>23H30-00H30</td></tr>
</table>

Tabla 2. 23 Función de monitoreo de la cámara “Cafetería”.

Los modos de monitoreo son de dos tipos uno para cuando el Laboratorio de Informática brinde atención al público de lunes a sábado y otro cuando sea domingos y feriados.

Como se describió en el capítulo I, el módulo que se encarga de almacenar y ejecutar las zonas de vigilancia es zmpkg.pl. Para ejecutar este módulo de manera programada es necesario utilizar el archivo crontab.

El crontab, es un archivo en donde se puede configurar tareas para que se ejecuten automáticamente en el sistema, por ejemplo descargar un archivo de

respaldo diariamente, o borrar ciertos archivos periódicamente, ejecutar scripts, etc.

En la línea de código 2.24, se indica el comando que permite invocar al archivo crontab.

```
> crontab -e
```

Línea de Código 2. 24 Llamada del archivo crontab.

En el momento en el que se ejecuta el archivo crontab se ingresa las líneas de comando que nos permite ejecutar ZoneMinder en diferentes modos.

En la línea de código 2.25, se indica el contenido del archivo crontab.

```
#Todas las semanas.
30 06 * * 1-6 /usr/local/bin/zmpkg.pl En_el_dia_LV
30 21 * * 1-5 /usr/local/bin/zmpkg.pl En_la_Noche_LV
30 15 * * 6 /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 * * 7 /usr/local/bin/zmpkg.pl En_la_Noche_LV
#Feriados
0 0 1 1 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 1 5 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 24 5 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 10 8 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 9 10 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 2 11 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 3 11 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
 0 0 6 12 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
0 0 24-31 12 * /usr/local/bin/zmpkg.pl En_la_Noche_LV
```

Línea de Código 2. 25 Edición del archivo crontab para calendarizar el monitoreo.

2.7.4.5 Configuración de filtros.

Un filtro en ZoneMinder permite ejecutar tareas programadas que no se pueden realizar con crontab o resulta muy complicado. Las tareas que se pueden realizar configurando un filtro pueden ser varias, como borrar el disco duro cuando esté lleno de eventos antiguos, permitir el envío de correo electrónico, eliminar eventos de corta duración etc.

Para mejorar el funcionamiento del circuito cerrado de televisión del Laboratorio de Informática se necesitan configurar dos filtros:

1. Filtro para eliminar eventos antiguos y no almacenados cuando el disco duro esté a un 95 % de su capacidad máxima, debido a que si el disco duro se llena puede causar problemas en el inicio del sistema operativo.
2. Filtro para enviar correos electrónicos únicamente cuando la importancia del evento sea en promedio mayor a 10 puntos. Se selecciona este valor, ya que eventos cuya puntuación promedio sea menor a 10 puntos generan falsas alarmas. Este valor resultó ser el más óptimo después de realizar varias pruebas.

En la figura 2.59, se indica la configuración para eliminar eventos antiguos y no almacenados.

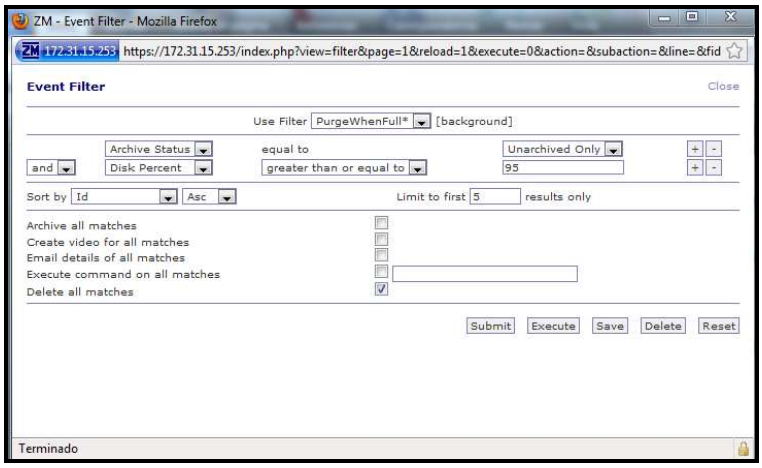


Figura 2. 59 Configuración del filtro Eliminar eventos antiguos y no almacenados.

En la figura 2.60, se presenta la configuración para el envío de correos electrónicos cuya puntuación promedio sobre cien es mayor a diez puntos.

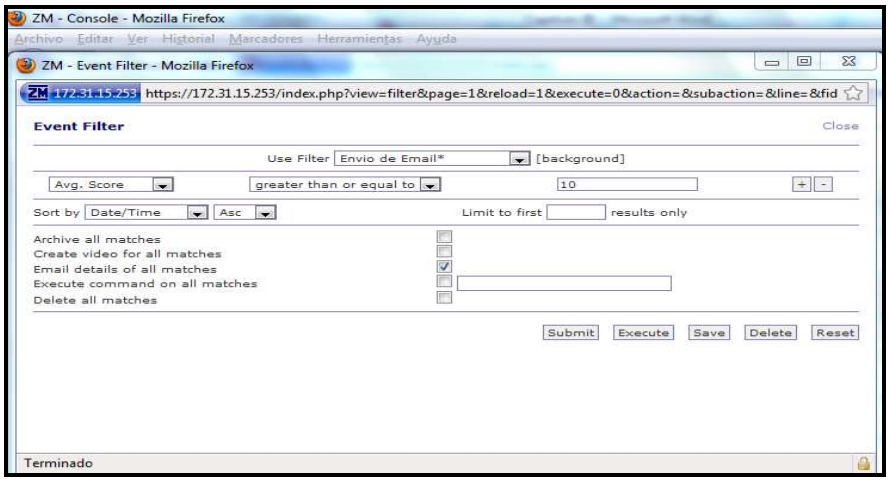


Figura 2. 60 Configuración del filtro para el envío de correo electrónico.

2.7.4.6 Configuración de zonas.

Como se estudió en el Capítulo I, la definición de una zona permite monitorear una área en especial donde existe un alto riesgo de ingreso de intrusos o personas mal intencionadas, creando eventos que pueden ser informados al personal encargado mediante él envió de un correo electrónico, un mensaje de texto al celular o incluso una llamada a un teléfono celular o fijo.

2.7.4.6.1 Configuración de zonas en la cafetería.

En la cafetería se encuentra los equipos de la academia ACIERTE, por tal motivo se debe crear una zona “activa” que detecte cualquier tipo de movimiento.
En la figura 2.61, se indica la cafetería vista desde la cámara IP.

Figura 2. 61 Imagen de la Cafetería desde la cámara IP.

En este lugar durante el día existen fluctuaciones de luz generados por el sol, por tal motivo si en un determinado instante se genera una variación de luz esta podría ser interpretada como un movimiento y generaría una falsa alarma. Para superar este inconveniente se hace uso de una zona “exclusiva”, la misma que al ser ubicada en un sitio donde se generen fluctuaciones de luz, omite la activación de falsas alarmas.

Para la configuración de la sensibilidad se emplea una configuración por defecto “Best, hight sensitivity”, aunque necesita mayor procesamiento brinda mayor seguridad para la detección de movimiento.

En la figura 2.62, se indica las zonas configuradas para el monitor de la cafetería.

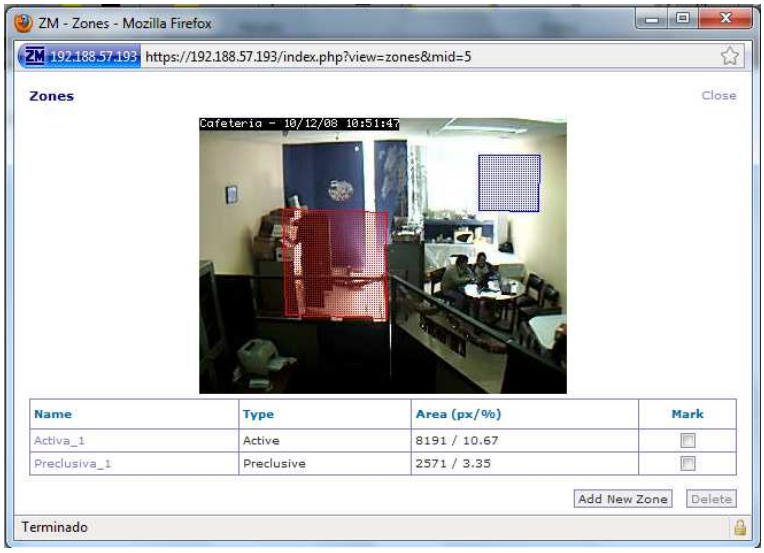


Figura 2. 62 Zonas configuradas en la cafetería.

2.7.4.6.2 Configuración de zonas en la entrada principal.

En la entrada principal ingresan una gran cantidad de personas durante los días laborables; sin embargo durante los días no laborables y en las noches se convierte en un punto altamente vulnerable, por el cual pueden ingresar personas no autorizadas. En la figura 2.63, se indica la imagen de la entrada principal vista desde una cámara IP.

Figura 2. 63 Imagen de la entrada principal vista desde una cámara IP.

Al igual que en la cafetería, en la entrada principal existen fluctuaciones de luz, por lo que se configura una zona exclusiva para evitar falsas alarmas.
Para la configuración de la sensibilidad se utiliza una configuración por defecto “Best, hight sensitivity”.

En la figura 2.64, se indica las zonas configuradas para el monitor de la entrada principal.

Figura 2. 64 Zonas configuradas en la entrada principal.

2.7.4.6.3 Configuración de zonas en la entrada posterior.

La entrada posterior permite la entrada y salida únicamente del personal y es el punto de mayor vulnerabilidad debido a que nadie controla su acceso.

En la figura 2.65, se indica la imagen de la entrada posterior vista desde una cámara IP.

Figura 2. 65 Imagen de la entrada posterior vista desde una cámara IP.

Los sitios a cubrir en esta zona son fundamentalmente las entradas provenientes del sexto y séptimo piso, las mismas que son cubiertas con una zona activa. En este sitio también existen fluctuaciones de luz durante el día, así que es necesario el uso de una zona exclusiva.

Para la configuración de la sensibilidad se utiliza una configuración por defecto “Best, hight sensitivity”.

En la figura 2.66, se indica las zonas configuradas para el monitor de la entrada posterior.

Figura 2. 66 Zonas configuradas en la entrada posterior.

BIBLIOGRAFÍA.

Tutoriales.

W. Stallings; “Wireless Comunications and Networks”; 2nd Edition; Prentice Hall; 2005.

Software IP Video System Design Tool.

Páginas de Internet.

http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

http://www.visiwave.com

http://www.wirelessmon.com/

http://www.c-mos.com/pdfsproductos/manual_de_ventas_UPS_reducido.pdf

eventos.stymapp.com.ar/download/informe4.pdf

http://wiki.centos.org/HowTos/Https

http://httpd.apache.org/docs/2.0/es/howto/auth.html

http://www.zoneminder.com/documentation

http://www.tecnologiapyme.com/servicios-web/para-que-sirven-los-certificados-ssl

http://carlton.oriley.net/blog/?p=31

http://albertomolina.wordpress.com/2009/01/04/configurar-postfix-a-traves-de-un-relay-host-autenticado-gmail/

http://www.notesco.net/download/ipcamcgisdk21.pdf

http://www.1acentosserver.com/centos_apache_web_server/Centos_Authentication_in_Apache.php

CAPÍTULO III

3. PRUEBAS DE FUNCIONAMIENTO.

3.1 INTRODUCCIÓN.

En este capítulo se realizan pruebas de funcionamiento del circuito cerrado de televisión del Laboratorio de Informática en un período de tiempo específico. Estas actividades consisten en analizar durante el día, la noche y fines de semana, diferentes parámetros tales como: detección de movimiento, notificación de eventualidades al correo electrónico, movimiento de las cámaras, verificación del streaming almacenado, visualización de las cámaras y ancho de banda que consume el CCTV.

Una vez concluidas las pruebas de funcionamiento, se hace una recopilación de la información obtenida y se definen los problemas del funcionamiento del CCTV. Finalmente, esta información en conjunto con el análisis del streaming de video almacenado, los eventos generados y los logs almacenados, permiten determinar las soluciones a los problemas encontrados.

3.2 PRUEBAS DEL CCTV.

Las pruebas que se realizan para comprobar el correcto funcionamiento del CCTV son:

- Detección de movimiento y notificación de eventualidades al correo electrónico.
- Movimiento de las cámaras.
- Verificación del streaming almacenado.

- Visualización del streaming de video de cada una de las cámaras.
- Ancho de banda que consume el CCTV.

3.2.1 DETECCIÓN DE MOVIMIENTO Y NOTIFICACIÓN DE EVENTUALIDADES AL CORREO ELECTRÓNICO.

Esta prueba consiste en verificar la funcionalidad de la detección de movimiento en cada una de las cámaras del CCTV.
Para comprobar su correcto funcionamiento, se requiere que usuarios ingresen en horas en el que la detección de movimiento se encuentre habilitada.

El ingreso a la Escuela Politécnica Nacional está permitido entre las 6:30 AM a 9:30 PM, en este horario la detección de movimiento del CCTV está deshabilitada; por tal motivo para realizar esta prueba se cambia momentáneamente el horario de detección de movimiento.

A continuación, se realizan las pruebas en cada cámara del CCTV.

3.2.1.1 Detección de movimiento en la cámara de la entrada principal.

En la figura 3.1, se indica un acceso no autorizado que se registra en la cámara ubicada en la entrada principal.

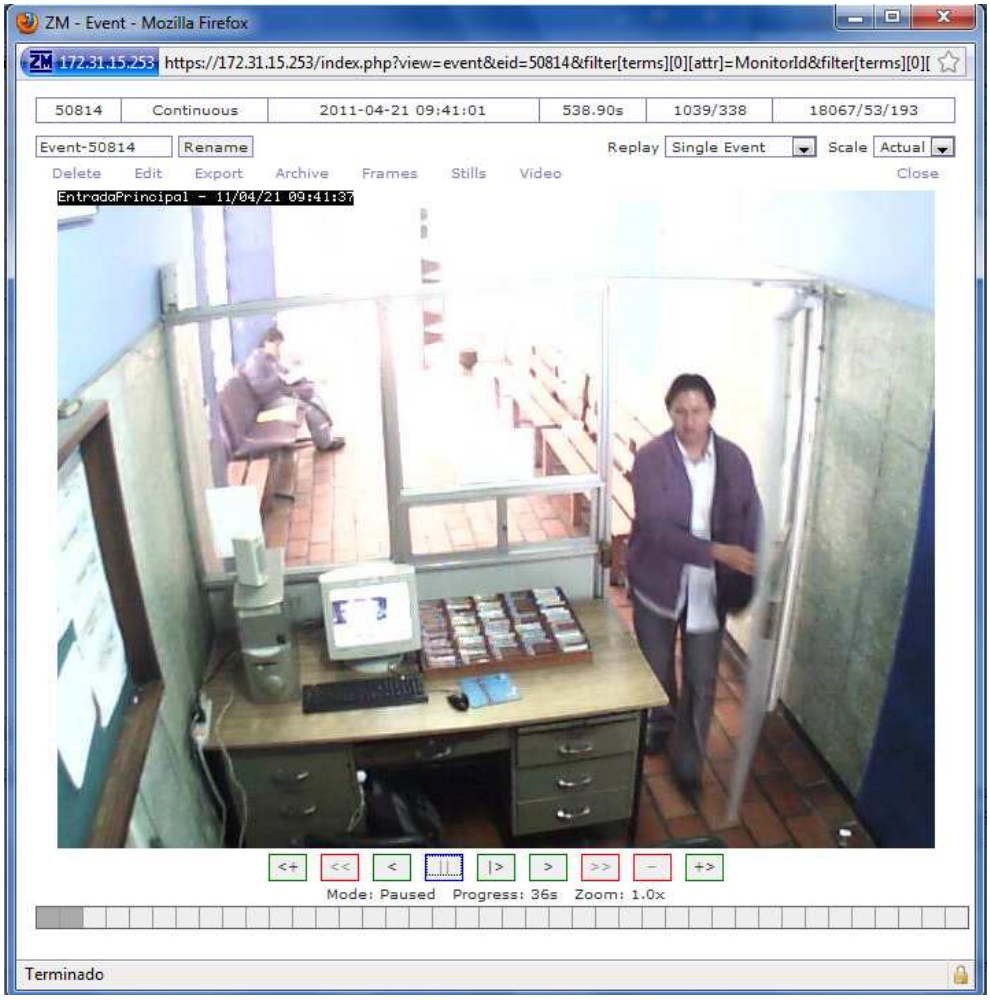


Figura 3. 1 Acceso no autorizado en la entrada principal.

Al momento de generarse una alarma, en la pestaña línea de tiempo del programa Zoneminder se crea un evento alarma representado con un pico en la línea de tiempo.

En la figura 3.2, se indica un evento alarma representado en la línea de tiempo.

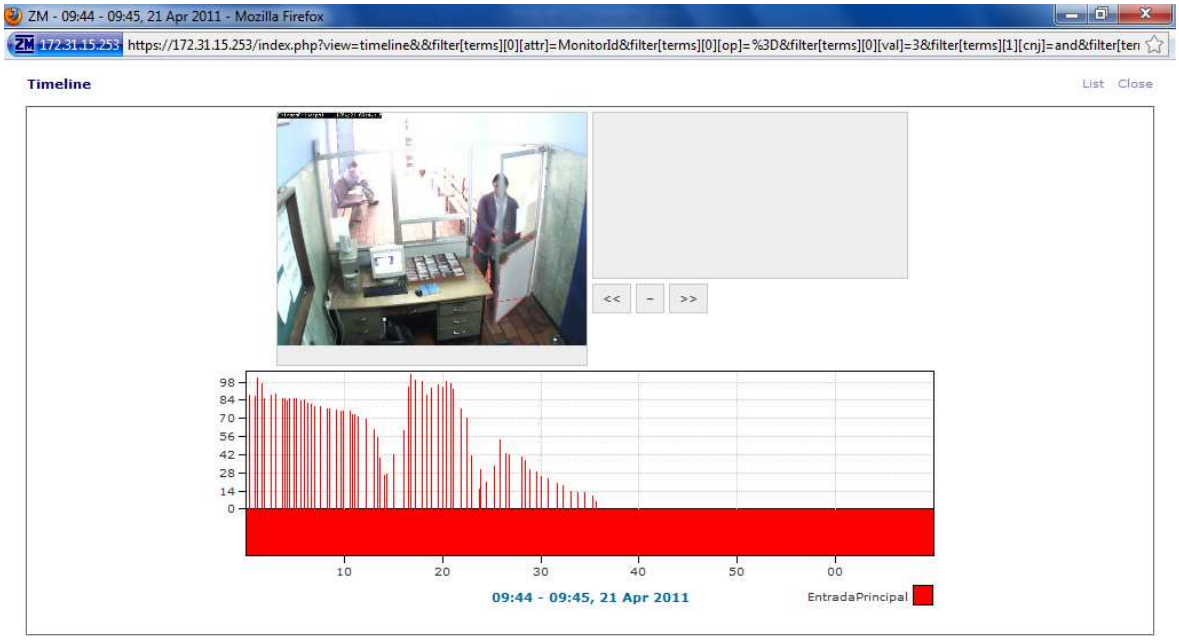


Figura 3. 2 Evento alarma representado en la línea de tiempo.

En el caso de detectar una alarma, la notificación de esta eventualidad se envía al correo electrónico. En la figura 3.3, se observa la notificación de una eventualidad en el correo electrónico.

Figura 3. 3 Notificación de una eventualidad en el correo electrónico.

3.2.1.2 Detección de movimiento en la cámara de la entrada posterior.

En la figura 3.4, se indica un acceso no autorizado que se registra en la cámara ubicada en la entrada posterior.

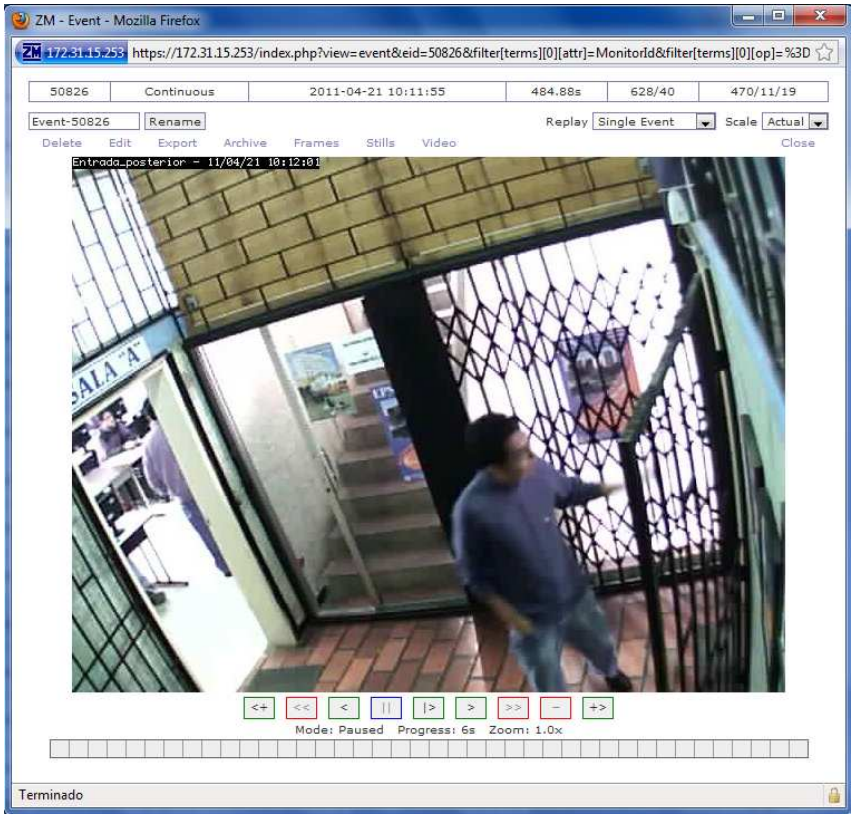


Figura 3. 4 Acceso no autorizado en la entrada posterior.

Al momento de generarse una alarma, en la pestaña línea de tiempo del programa Zoneminder se crea un evento alarma representado con un pico en la línea de tiempo.

En la figura 3.5, se indica un evento alarma representado en la línea de tiempo.

Figura 3. 5 Evento alarma representado en la línea de tiempo.

En el caso de detectar una alarma, la notificación de esta eventualidad se envía al correo electrónico.

En la figura 3.6, se observa la notificación de una eventualidad en el correo electrónico.

Figura 3. 6 Notificación de una eventualidad en el correo electrónico.

3.2.1.3 Detección de movimiento en la cámara de la Cafetería.

En la figura 3.7, se indica un acceso no autorizado que se registra en la cámara ubicada en la cafetería.

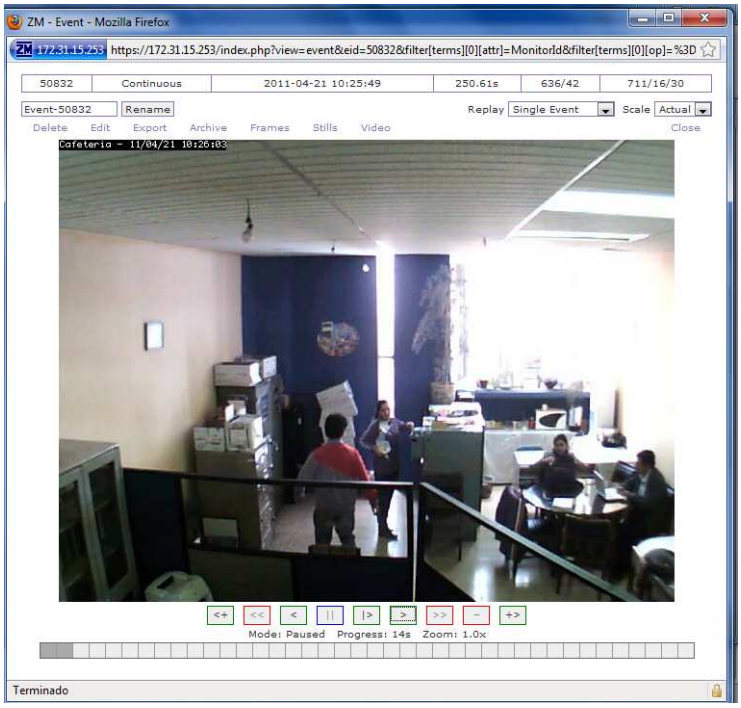


Figura 3. 7 Acceso no autorizado en la Cafetería.

Al momento de generarse una alarma, en la pestaña línea de tiempo del programa Zoneminder se crea un evento alarma representado con un pico en la línea de tiempo.

En la figura 3.8, se indica un evento alarma representado en la línea de tiempo.

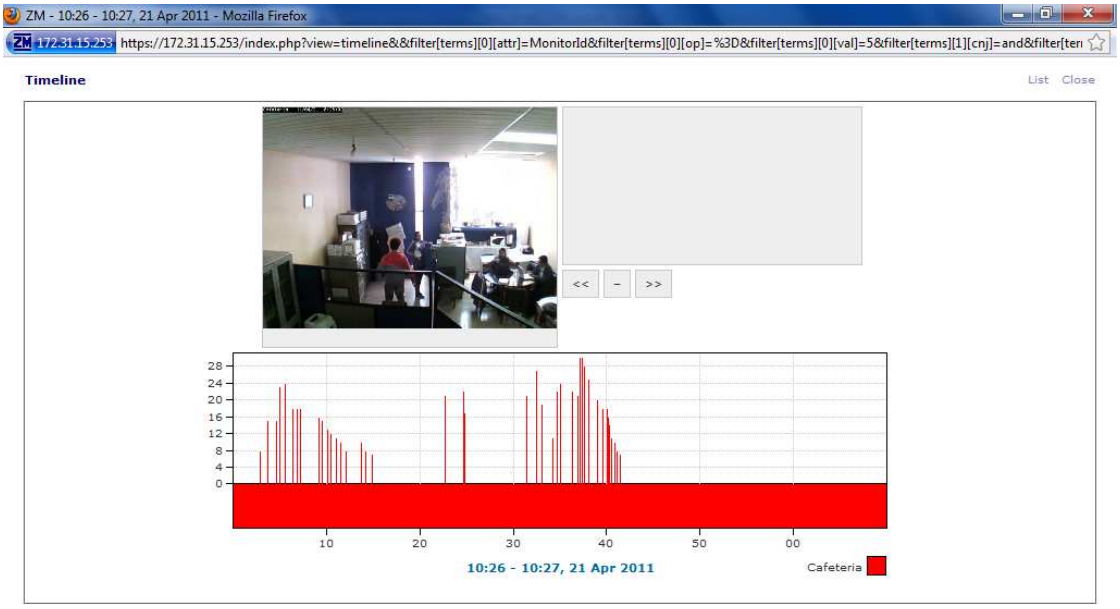


Figura 3. 8 Notificación de una eventualidad en el correo electrónico.

En el caso de detectar una alarma, la notificación de esta eventualidad se envía al correo electrónico. En la figura 3.9, se observa la notificación de una eventualidad en el correo electrónico.

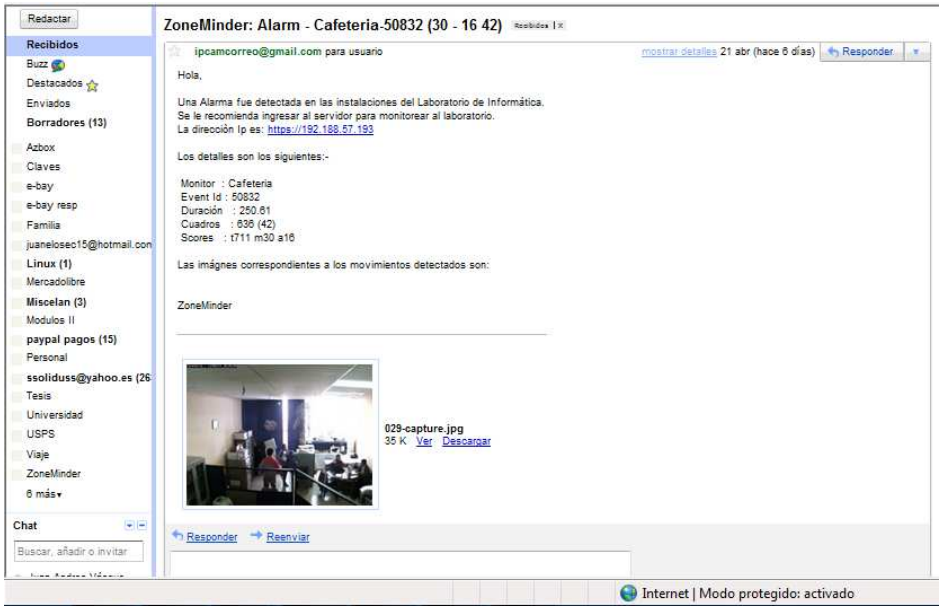


Figura 3. 9 Notificación de una eventualidad en el correo electrónico.

3.2.2 MOVIMIENTO DE LAS CÁMARAS.

Esta prueba de funcionamiento consiste en verificar el correcto desempeño de las opciones de movimiento de cada una de las cámaras IP del CCTV.

En la figura 3.10, se indica un mosaico con cada uno de los movimientos generados en la cámara de la entrada principal.

Figura 3. 10 Mosaico de imágenes con los movimientos generados en la cámara de la entrada principal.

En la figura 3.11, se indica un mosaico con cada uno de los movimientos generados en la cámara de la entrada posterior.

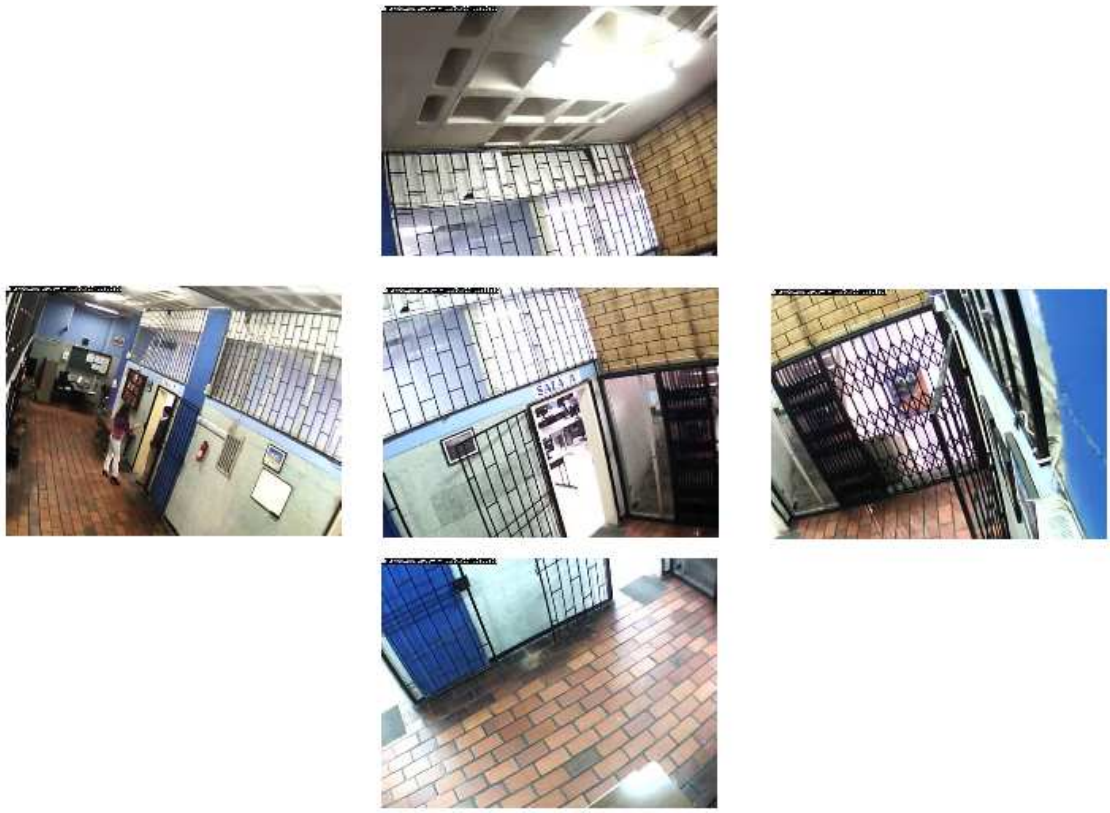


Figura 3. 11 Mosaico de imágenes con los movimientos generados en la cámara de la entrada posterior.

En la figura 3.12, se indica un mosaico con cada uno de los movimientos generados en la cámara de la cafetería.

Figura 3. 12 Mosaico de imágenes generadas con los movimientos generados en la cámara de la Cafetería.

Una vez concluido el monitoreo de las cámaras y en el caso en el que la visión de las cámaras apunten a un lugar distinto al del lugar de origen, éstas no van a cubrir las zonas de vigilancias establecidas, provocando errores en la detección de alarmas, tal como se indican en la figura 3.13.

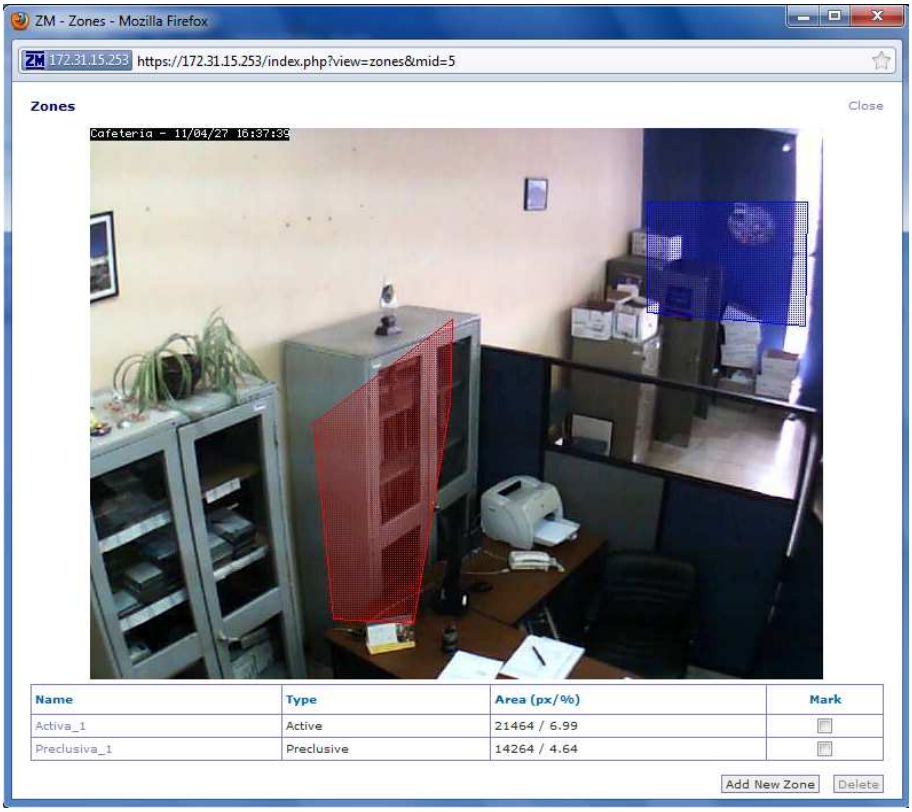


Figura 3. 13 Visibilidad errónea de las zonas de vigilancia.

3.2.3 VERIFICACIÓN DEL STREAMING DE VIDEO ALMACENADO.

En esta prueba de funcionamiento se realiza la verificación del streaming de video almacenado de cada uno de las tres cámaras en el disco duro del servidor.

En la figura 3.14, se indica el streaming de video almacenado de la cámara de la entrada principal.

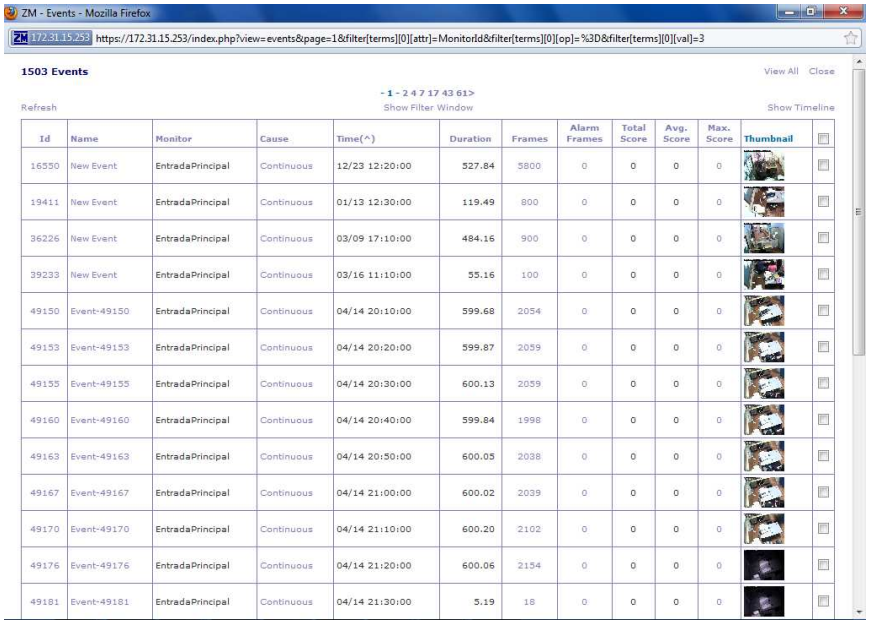


Figura 3. 14 Streaming de video almacenado de la cámara de la entrada principal.

.

En la figura 3.15, se indica el streaming de video almacenado de la cámara de la entrada posterior.

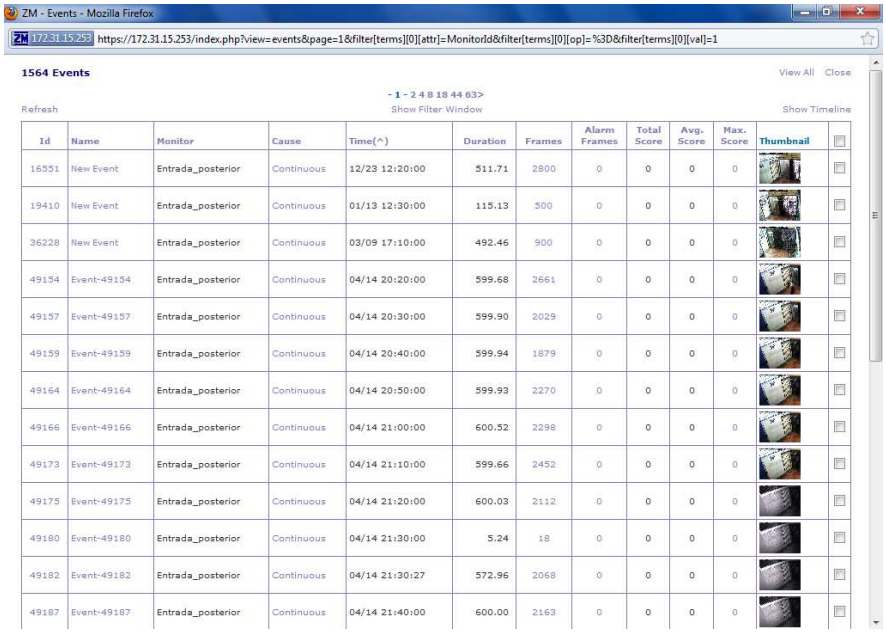


Figura 3. 15 Streaming de video almacenado de la cámara de la entrada posterior.

En la figura 3.16, se indica el streaming de video almacenado de la cámara de la cafetería.

Id	Name	Monitor	Cause	Time(^)	Duration	Frames	Alarm Frames	Total Score	Avg. Score	Max. Score	Thumbnail
16548	New Event	Cafeteria	Continuous	12/23 12:00:00	535.39	2300	0	0	0	0	
39206	New Event	Cafeteria	Continuous	03/16 09:50:00	5121.78	500	0	0	0	0	
49152	Event-49152	Cafeteria	Continuous	04/14 20:20:00	1199.99	2296	0	0	0	0	
49158	Event-49158	Cafeteria	Continuous	04/14 20:40:00	599.98	3437	0	0	0	0	
49162	Event-49162	Cafeteria	Continuous	04/14 20:50:00	600.06	5170	0	0	0	0	
49168	Event-49168	Cafeteria	Continuous	04/14 21:00:00	599.99	4653	0	0	0	0	
49171	Event-49171	Cafeteria	Continuous	04/14 21:10:00	599.99	2966	0	0	0	0	
49174	Event-49174	Cafeteria	Continuous	04/14 21:20:00	600.03	2100	0	0	0	0	
49179	Event-49179	Cafeteria	Continuous	04/14 21:30:00	5.26	18	0	0	0	0	
49183	Event-49183	Cafeteria	Continuous	04/14 21:30:27	572.80	2030	0	0	0	0	
49186	Event-49186	Cafeteria	Continuous	04/14 21:40:00	599.95	2127	0	0	0	0	
49189	Event-49189	Cafeteria	Continuous	04/14 21:50:00	600.04	2127	0	0	0	0	
49192	Event-49192	Cafeteria	Continuous	04/14 22:00:00	600.00	2124	0	0	0	0	

Figura 3. 16 Streaming de video almacenado de la cámara de la Cafetería.

A partir de la figuras 3.14, 3.15 y 3.16, se comprueba que el filtro creado para eliminar eventos antiguos, funciona correctamente debido a que por cada elemento nuevo almacenado se elimina un evento antiguo.

3.2.4 VISUALIZACIÓN DE LOS MONITORES DURANTE UN PERÍODO DE TIEMPO EN ZONEMINDER.

En esta prueba de funcionamiento se verifica que cada una de las cámaras del CCTV se encuentra monitoreando y grabando permanentemente. Para ello se verifican los “logs” generados por Zoneminder, los mismos que nos informan sobre el funcionamiento erróneo del CCTV.

En la comprobación de las funciones de monitoreo y grabación se presenta un problema recurrente, siendo esta la suspensión del envió del streaming de video por parte de las cámaras hacia el servidor.

Para observar la suspensión de envío de streaming de video en la interfaz web de Zoneminder, es necesario ingresar a la pantalla principal del programa y en la columna Source se marca con color rojo la dirección IP correspondiente a la cámara que suspende el envío del streaming de video. En la figura 3.17, se indica la suspensión del streaming de video.

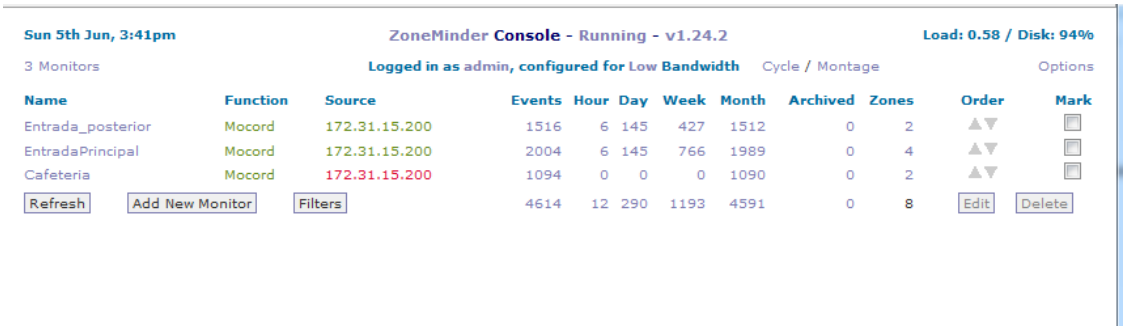


Figura 3. 17 Suspensión del streaming de video.

En la figura 3.18, se indica la visualización de la suspensión del streaming de video en una cámara IP.

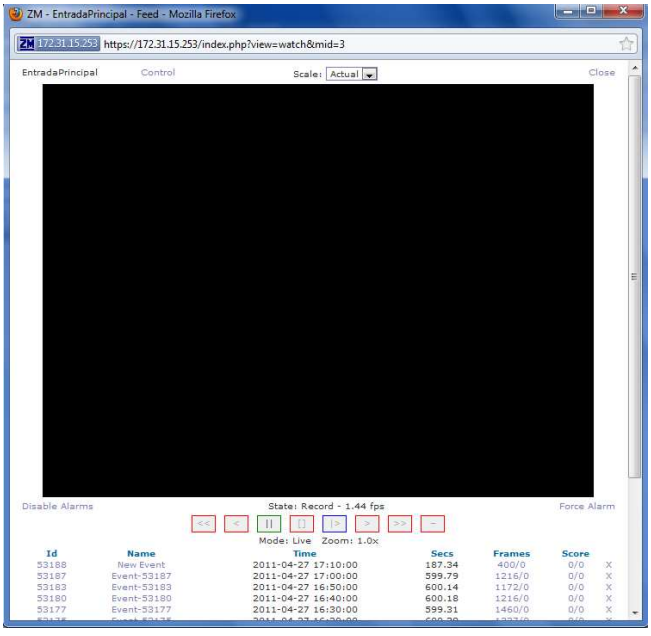


Figura 3. 18 Visualización de la suspensión del streaming de video en una cámara inalámbrica IP.

3.2.4.1 Visualización de los monitores durante el día.

Por facilidad, el horario que se seleccionó para comprobar el funcionamiento del CCTV durante el día fue entre 10 AM y 12 PM.

En la tabla 3.1, se indica el estado de funcionamiento de cada una de las cámaras IP durante horas de la mañana.

ESTADO DE LAS CÁMARAS			
INTERVALO DE TIEMPO	**ENTRADA PRINCIPAL**	**ENTRADA POSTERIOR**	**CAFETERÍA**
10:00 – 10:10	Correcto	Correcto	Correcto
10:10 – 10:20	Correcto	Correcto	Correcto
10:30 – 10:40	Incorrecto	Correcto	Incorrecto
10:40 – 10:50	Correcto	Incorrecto	Correcto
10:50 – 11:00	Correcto	Correcto	Correcto
11:00 – 11:10	Incorrecto	Correcto	Correcto
11:10 – 11:20	Correcto	Correcto	Correcto
11:20 – 11:30	Correcto	Correcto	Incorrecto
11:30 – 11:40	Correcto	Incorrecto	Correcto
11:40 – 11:50	Incorrecto	Correcto	Correcto
11:50 – 12:00	Correcto	Correcto	Correcto

Tabla 3. 1 Estado de funcionamiento de las cámaras IP.

En la tabla 3.2, se indica el estado de funcionamiento de cada una de las cámaras IP durante horas de la tarde.

ESTADO DE LAS CÁMARAS			
INTERVALO DE TIEMPO	**ENTRADA PRINCIPAL**	**ENTRADA POSTERIOR**	**CAFETERÍA**
14:00 – 14:10	Correcto	Correcto	Correcto
14:10 – 14:20	Correcto	Correcto	Correcto
14:30 – 14:40	Incorrecto	Correcto	Correcto
14:40 – 14:50	Correcto	Correcto	Incorrecto
14:50 – 15:00	Correcto	Correcto	Correcto
15:00 – 15:10	Incorrecto	Incorrecto	Correcto
15:10 – 15:20	Correcto	Correcto	Correcto
15:20 – 15:30	Correcto	Correcto	Correcto
15:30 – 15:40	Correcto	Correcto	Correcto
15:40 – 15:50	Incorrecto	Correcto	Correcto
15:50 – 16:00	Correcto	Correcto	Incorrecto

Tabla 3. 2 Estado de funcionamiento de las cámaras IP.

3.2.4.2 Visualización de los monitores durante la noche.

El horario por facilidad que se escogió para comprobar el funcionamiento del CCTV durante la noche fue entre 19:00 Y 21:00.

En la tabla 3.3, se indica el estado de funcionamiento de cada una de las cámaras IP durante horas de la noche.

ESTADO DE LAS CÁMARAS			
INTERVALO DE TIEMPO	**ENTRADA PRINCIPAL**	**ENTRADA POSTERIOR**	**CAFETERÍA**
19:00 – 19:10	Correcto	Correcto	Correcto

ESTADO DE LAS CÁMARAS			
INTERVALO DE TIEMPO	**ENTRADA PRINCIPAL**	**ENTRADA POSTERIOR**	**CAFETERÍA**
19:10 – 19:20	Correcto	Correcto	Correcto
19:30 – 19:40	Correcto	Incorrecto	Correcto
19:40 – 19:50	Correcto	Correcto	Correcto
19:50 – 20:00	Correcto	Correcto	Correcto
20:00 – 20:10	Correcto	Incorrecto	Correcto
20:10 – 20:20	Correcto	Correcto	Correcto
20:20 – 20:30	Correcto	Correcto	Correcto
20:30 – 20:40	Incorrecto	Correcto	Correcto
20:40 – 20:50	Correcto	Correcto	Correcto
20:50 – 21:00	Correcto	Correcto	Correcto

Tabla 3. 3 Estado de funcionamiento de las cámaras IP.

3.2.5 PROBLEMAS ENCONTRADOS EN EL FUNCIONAMIENTO DEL CCTV.

A continuación se presentan los problemas de funcionamiento del CCTV, que se determinaron a partir de las pruebas de funcionamiento realizadas.

- Desplazamiento de las zonas de vigilancia.
- Suspensión del envío del streaming de video.

3.3 SOLUCIÓN A PROBLEMAS DE FUNCIONAMIENTO DEL CCTV.

A continuación se detallan las posibles soluciones a los problemas de funcionamiento del CCTV.

3.3.1 SOLUCIÓN AL DESPLAZAMIENTO DE LAS ZONAS DE VIGILANCIA.

Con el fin de dar una solución a este inconveniente, se va implementar un Script que permita volver a ubicar a cada una de las cámaras IP en su posición original, el mismo que se indica en la línea de código 3.1.

```
#Entrada Principal
28 21 * * 1-5 /usr/local/bin/zmcontrol.pl --id=1 --command=presetHome
28 15 * * 6 /usr/local/bin/zmcontrol.pl --id=1 --command=presetHome
#Entrada Posterior
28 21 * * 1-5 /usr/local/bin/zmcontrol.pl --id=2 --command=presetHome
28 15 * * 6 /usr/local/bin/zmcontrol.pl --id=2 --command=presetHome
#Cafeteria
28 21 * * 1-5 /usr/local/bin/zmcontrol.pl --id=3 --command=presetHome
28 15 * * 6 /usr/local/bin/zmcontrol.pl --id=3 --command=presetHome
```

Línea de Código 3. 1 Script para ubicar las cámaras IP en su posición original.

Una vez implementado este código y copiado al archivo crontab, se supera el problema del desplazamiento de las zonas de vigilancia. En la figura 3.19, se indica la visualización de las cámaras del CCTV sin desplazamiento de las zonas de vigilancia. Es importante conocer, que las cámaras regresan a la posición central una vez al día. De lunes a viernes las cámaras regresan a su posición original a las 21:28 Horas, dos minutos antes de activarse el modo Mocord en cada cámara, en cambio los días sábados las cámaras regresan a su posición original a las 15:28 horas, dos minutos antes de activarse el modo Mocord en cada cámara.

Figura 3. 19 Visualización de las cámaras del CCTV sin desplazamiento de las zonas de vigilancia.

3.3.2 SOLUCIÓN A LA SUSPENSIÓN DEL ENVÍO DEL STREAMING DE VIDEO.

La suspensión del streaming de video se produce por dos razones principales:

- El rendimiento del router inalámbrico se reduce, debido a que no trabaja a la velocidad definida en el estándar, mermando la capacidad de manejar datos.
- Existe gran cantidad de clientes alrededor y dentro del Laboratorio de Informática que compiten por la ocupación del canal.

Para brindar solución al problema de suspensión del envió del streaming de video se planta una posible solución, la misma que consiste en reducir el número de cuadros por segundo.

3.3.2.1 Reducción del número de cuadros por segundo.

En el presente Proyecto, en la configuración se disminuyó el número de frames a un valor de 2, este valor es suficiente para la detección de movimiento y permitió obtener un claro streaming de video. La reducción del número de cuadros por segundo permite que el ancho de banda que necesita el CCTV disminuya, evitando una suspensión en el envío del streaming de video.

Para hacer este cambio en el programa Zoneminder, se debe ingresar al menú principal, posteriormente se presiona en el campo de “dirección IP” de la cámara, a la cual se desea modificar el número de cuadros por segundo, a continuación aparece un nuevo menú en el cuál se selecciona la pestaña “Source” y en la opción “Remote Host Path” se cambian los parámetros de cuadros por segundo.

En la figura 3.20, se indica la opción Remote Host Path perteneciente al menú Source.

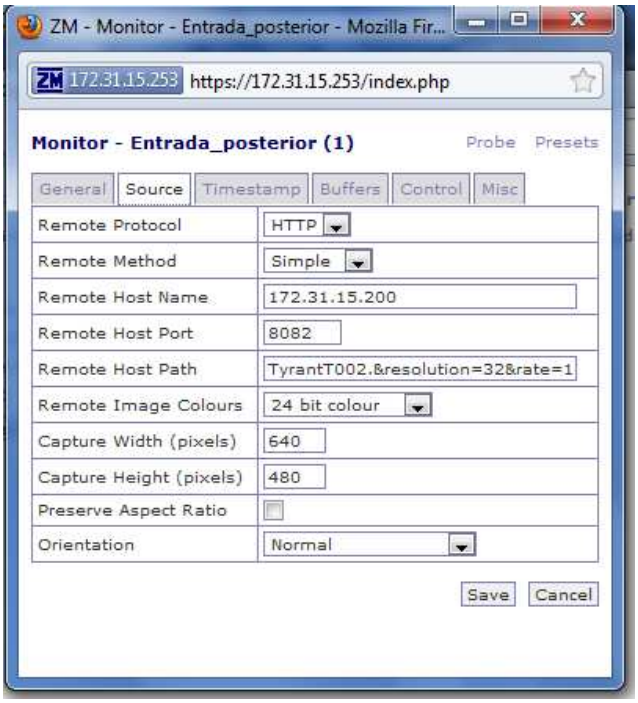


Figura 3. 20 Modificación del campo remote host path.

En la línea de código 3.2, se indica las modificaciones a realizarse en el campo Remote Host Path.

Campo Frames

/videostream.cgi?user=**User**&pwd=**contraseña**&resolution=**resolución**&rate=**frames**

Línea de Código 3. 2 Modificaciones en el campo Remote Host Past.

A partir de la línea de código 3.2, se indica que el campo “frames” corresponde a cuantos frames por segundo va enviar la cámara.

En la tabla 3.4, se indica el parámetro “Frames” que se debe ingresar para obtener el número de frames deseados.

Parámetro “Frames”	Fps
0	Max
1	20
3	15
6	10
11	5
12	4
13	3
14	2
15	1
17	1/2 segundos
19	1/3 segundos
21	1/4 segundos
23	1/5 segundos

Tabla 3. 4 FPS según parámetro rate.

Realizando las modificaciones antes mencionadas se reduce en gran cantidad las suspensiones de streaming de video, sin embargo por periodos cortos de tiempo el problema vuelve a suscitarse. Este inconveniente se debe a que los

dispositivos inalámbricos para poder transmitir información, deben competir por acceder al canal, en este caso las cámaras IP no son las únicas que compiten por acceder, por el contrario existen varias redes inalámbricas que trabajan en el mismo canal, aunque no se encuentran asociadas a la red inalámbrica del CCTV, van a competir por acceder.

Una vez concluida estas modificaciones se obtiene un mejor funcionamiento del circuito cerrado de televisión del Laboratorio de Informática, de esta manera se asegura que el presente Proyecto permita:

- Monitoreo continuo y remoto de las zonas de riesgo del Laboratorio de Informática.
- Detección y notificación de eventos.
- Funcionalidad del CCTV durante las 24 horas del día.

CAPÍTULO IV

4. DESCRIPCIÓN DE COSTOS.

4.1 INTRODUCCIÓN.

En este capítulo se realiza un presupuesto referencial de los equipos y recursos necesarios para la instalación, operación y mantenimiento del Circuito Cerrado de Televisión. El presupuesto aquí establecido determina el monto a ser invertido para la implementación del Proyecto, este presupuesto considera los costos de los materiales empleados y de los equipos necesarios.

4.2 PRESUPUESTO DE INSTALACIÓN.

El Circuito Cerrado de Televisión, requiere elementos de software y hardware para un correcto funcionamiento.
En la Tabla 4.1, se presentan los equipos necesarios para el funcionamiento del CCTV.

DESCRIPCIÓN	CANTIDAD
Software para Administración de Cámaras.	1
Software para Administración de Router Inalámbrico	1
Servidor HP PROLIANT ml110	1
Dirección IP Pública	1
Equipos de conectividad	2
Cámaras IP	4
Material Eléctrico	Varios

Tabla 4. 1 Elementos necesarios para el funcionamiento del CCTV.

A continuación, se describen los costos de los elementos antes mencionados.

4.2.1 COSTOS DE EQUIPOS ACTIVOS DE LA RED.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO [USD]	VALOR TOTAL [USD]
Servidor HP PROLIANT ML 110	1	1.046,96	1.046,96
Switch Cisco Catalyst	1	150,14	150,14
Router Inalámbrico	1	75	75
UPS	1	631	631
COSTOS DE EQUIPOS ACTIVOS DE LA RED			**1.903,10**

Tabla 4. 2 Costos de Equipos Activos de la Red.

4.2.2 COSTOS CÁMARAS IP.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO [USD]	VALOR TOTAL [USD]
CÁMARA IP FOSCAM F18908W	2	100	200
CÁMARA IP FOSCAM F18918W	1	100	100
COSTOS DE CÁMARAS IP			**300**

Tabla 4. 3 Costos de Cámaras IP.

4.2.3 COSTOS DE MATERIAL ELÉCTRICO.

DESCRIPCIÓN	CANTIDAD [Metros]	PRECIO UNITARIO [USD]	VALOR TOTAL [USD]
CABLE ELÉCTRICO #16 AWG	50	0.79	39.5
ENCHUFLES	8	0.20	1.60
COSTOS DE MATERIAL ELÉCTRICO			**41.1**

Tabla 4. 4 Costos de Material Eléctrico.

4.2.4 COSTOS DE MATERIAL DE RED.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO [USD]	VALOR TOTAL [USD]
CABLE UTP CAT. 5E	25 (Metros)	1.00	25.00
Conectores RJ-45	2 (Unidades)	0.05	0.10
Canaleta Plástica Decorativa 32 X 12	5 (Unidades)	2.01	10.05
COSTOS DE MATERIAL DE RED			**35.15**

Tabla 4. 5 Costos de Material de Red.

4.3 COSTO TOTAL DEL PROYECTO.

Una vez descrito los costos necesarios para el funcionamiento del CCTV, se procede a realizar el costo total del proyecto, el mismo que indica el monto necesario para la implementación del CCTV.

DESCRIPCION	COSTOS [USD]
Costos de equipos activos de la red.	1903.10
Costos cámaras IP.	300
Costos de material eléctrico.	41.1
Costos de material de red.	35.15
Costo de diseño del CCTV.	385.00
COSTO TOTAL DEL PROYECTO	**$2664,35**

Tabla 4. 6 Costo total del Proyecto.

El Costo Total del proyecto asciende a 2664,35 dólares, los mismos que servirán para la implementación, operación y mantenimiento del CCTV.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones y recomendaciones producto del diseño e implementación del circuito cerrado de televisión usando cámaras IP inalámbricas para el Laboratorio de Informática.

5.1 CONCLUSIONES.

- Para la implementación del CCTV para el Laboratorio de Informática se empleó cámaras IP FOSCAM, las mismas que manejan los estándares inalámbricos IEEE 802.11 b y IEEE 802.11 g, el principal inconveniente que existe con estos estándares es el hecho de que son altamente susceptibles a la interferencia existente, la misma que es originada por la presencia de otras redes inalámbricas en el Laboratorio de Informática.

- El software de monitoreo que se utiliza en el CCTV es ZoneMinder, el mismo que es de distribución gratuita; este software permite capturar, analizar, llevar un registro y un seguimiento del streaming de video capturado por las cámaras, posee una interfaz amigable con el usuario permitiendo realizar un monitoreo sin contra tiempos.

- Mediante la implementación del CCTV con cámaras IP en el Laboratorio de Informática, se logró brindar el servicio de monitoreo remoto y notificación de eventualidades en caso de producirse alarmas en las zonas de vigilancia establecidas en dichas instalaciones, de esta manera se aumentó los niveles de seguridad para proteger los equipos computacionales y de conectividad existentes en el Laboratorio de Informática.

- El objetivo de realizar una comunicación inalámbrica con cámaras IP fue cumplido, pero el rendimiento de esta comunicación es inestable en un ambiente como el del Laboratorio de Informática, debido a que existe una gran cantidad de fuentes de interferencia tales como: rejas metálicas, presencia de otras redes inalámbricas que operan en el mismo canal, muros y columnas de gran grosor y presencia de objetos metálicos que rodean al router inalámbrico.

- En el diseño del CCTV se consideró diferentes criterios como son: ubicación actual de los equipos de conectividad de la academia ACIERTE, lugares de ingreso y de salida de estudiantes, horarios de atención y distribución física de las aulas, permitiendo de esta manera brindar una cobertura total de los puntos de mayor vulnerabilidad.

- El servidor Apache implementado en el CCTV, necesita tener los permisos necesarios para poder acceder a archivos tales como la aplicación java Cambazola o al directorio de grabación de eventos, etc.

- El acceso al servidor del CCTV consta de dos autenticaciones, la primera que permite el acceso al servidor apache y la otra que permite el acceso a la aplicación ZoneMinder, ambas utilizan el protocolo SSH para el cifrado de los datos de intercambio entre el cliente y el servidor.

- La eficiencia del servidor del CCTV, no va a depender de si tiene o no una tarjeta gráfica potente, debido a que el servidor únicamente procesa datos que provienen desde las cámaras; la tarjeta gráfica ayuda a los equipos clientes, debido a que en éstos se visualiza la imagen.

- El servidor de grabación de video implementado en el presente Proyecto, permite buscar y observar eventos inusuales que ocurrieron con anterioridad, de esta manera en el caso de existir un atraco se procede a buscar en estos registros.

- Las pruebas de funcionamiento del CCTV y la información almacenada en el servidor de video, permitieron entender el comportamiento del CCTV y solucionar diversos problemas.

- El ancho de banda que consume el circuito cerrado de televisión, depende de varios factores tales como el método de compresión, resolución, cuadros por segundo, número de cámaras y luminosidad de la zona vigilada.

- La eficiencia del router inalámbrico del CCTV, se ve afectado fuertemente por las interferencias, reduciendo de tal manera la velocidad con la que va a procesar los datos provenientes de las cámaras, lo que provoca una reducción en los cuadros que envía la cámara, incluso suspendiendo momentáneamente el streaming de video.

- La iluminación del Laboratorio de Informática tiene un efecto considerable en el ancho de banda que consume cada cámara, debido a que en ambientes con mayor iluminación se requiere un mayor consumo de ancho de banda y lo contrario en ambientes oscuros.

- El presupuesto referencial del presente Proyecto es relativamente bajo en comparación a proyectos similares, las principales diferencias radican en el hecho de que en este Proyecto no se tuvo que pagar por una licencia de software para los servidores ni para el software de administración de cámaras, en determinados proyectos en donde se paga por estas licencias el costo total del proyecto sube abruptamente.

5.2 RECOMENDACIONES.

- El diseño e implementación del CCTV con cámaras IP y monitoreo remoto para el Laboratorio de Informática, con sus diferentes consideraciones y criterios debe ser una guía para futuras aplicaciones afines al presente Proyecto y no como una regla específica.

- En el caso de aumentar el número de cámaras en el Laboratorio de Informática, se recomienda comprar cámaras con una mejor compresión o que trabajen en el estándar IEEE 802.11 n. De esta manera el router inalámbrico no se satura con los datos enviados por las cámaras.

- Para aumentar el rango de visión nocturna de las cámaras del CCTV en el Laboratorio de Informática, se recomienda adquirir led's infrarrojos de mayor potencia, para que la iluminación se extienda algunos metros más.

- Se recomienda adaptar una sección del taller de computadoras para el uso exclusivo del servidor HP Proliant ML 110 y del UPS, este área debe contar con la ventilación necesaria para controlar la temperatura de estos equipos, de esta forma se prolongara la vida útil de los mismos; adicionalmente es necesario implementar las seguridades físicas necesarias para salvaguardar a estos equipos.

- Se debe realizar un mantenimiento técnico al UPS del CCTV, este mantenimiento debe llevarse a cabo cada año, en esta actividad se debe realizar pruebas de eficiencia y revisar los aislamientos en la entrada y salida del UPS.

- La administración de la información de video almacenada debe ser manejada con total seriedad, con fines de seguridad y no como una forma de inmiscuirse en las actividades diarias de otras personas.

- Es recomendable almacenar la información de video en diferentes lugares y no únicamente en el directorio eventos, ya que si este directorio o el disco duro donde se graba esta información sufre un daño, se perderá la información permanentemente.

- Es recomendable hacer un sistema de redundancia para el almacenamiento de la información del Circuito Cerrado de Televisión; un arreglo Raid 5 ayuda a cumplir esta función.

GLOSARIO

Infrarrojo: Las ondas infrarrojas tienen longitudes de onda más largas que la luz visible, pero más cortas que las microondas. Estas ondas se encuentran en los 820 nanómetros.

Microondas: Microondas son ondas electromagnéticas cuyo rango de frecuencias está comprendido entre 300 MHZ y 300 GHZ.

Movilidad: El usuario dispone de conexión a la red desde cualquier lugar de la oficina, esté donde esté y aunque se mueva.

Disponibilidad: La disponibilidad de la red es el porcentaje de tiempo que el servicio es ofrecido a un lugar dado con la calidad requerida.

Escalabilidad: Es la propiedad anhelada de una red, sistema, o proceso, que muestra su destreza para operar el incremento continuo de trabajo con fluidez, o muestra la preparación que tiene para crecer manteniendo su calidad en todos los servicios

WEP: Mecanismo opcional de seguridad definido dentro del estándar 802.11 diseñado para hacer que la integridad del enlace del dispositivo inalámbrico sea equivalente a la de un cable.

AES: (Advanced Encryption Standard). Es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

TKIP: Es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua.

Beacon: Tramas usadas para publicar la presencia por ejemplo la presencia de dispositivos inalámbricos.

Topologías dinámicas de red: La topología de la red puede cambiar arbitrariamente

MIMO. (Multiples Entradas Multiples Salidas). Se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores.

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

PTZ.- Son las siglas de Pan, Tilt, Zoom que hace referencia al movimiento horizontal, vertical y acercamiento.

MySQL.- Es un sistema de gestión de base de datos relacional, multihilo y multiusuario.

X.10.- Es un protocolo de comunicaciones para el control remoto de dispositivos eléctricos.

xHTML.- Acrónimo en inglés de eXtensible Hypertext Markup Language, es el lenguaje de marcado pensado para sustituir a HTML como estándar para las páginas web.

FFmpeg.- Es una colección de software libre que puede grabar, convertir y hace streaming de audio y vídeo.

Regexp.- Regular expression.

Bit.- Bit es el acrónimo de Binary digit. (dígito binario). Un bit es un dígito del sistema de numeración binario.

Voltio.- Es la unidad derivada del SI para el potencial eléctrico, fuerza electromotriz y el voltaje.

Amperio.- Es la unidad de intensidad de corriente eléctrica.

Watt.- Es la unidad de potencia del Sistema Internacional de Unidades**.**

Estrella Extendida. La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella.

UGI. Unidad de gestión de la Información.

SiteSurvey.- es el proceso de identificar y detectar las diferentes redes wireless que se encuentran en la cercanía del lugar de implementación, permite seleccionar el lugar estratégico para instalar los equipos de manera que asegura que los usuarios tengan cobertura.

PLCP.- Protocolo de convergencia de capa física.

MPDU.- MAC Protocol Data Unit.

Tamaño del Frame.- Es la cantidad de información medida en bytes que ocupa un cuadro de imagen.

QVGA.- Es un término usado para referirse a una pantalla de ordenador con una resolución de 320x240 píxeles.

CIF.- El CommonIntermediateFormat, más conocido por su acrónimo CIF es un formato definido en la
recomendación H.261 de la ITU, que utiliza para compatibilizar los diversos formatos de vídeo digital.

Dirección IP.- Es un conjunto de 32 bits divididos en cuatro octetos que permiten identificar a dispositivos en una red.

H264.-Es un codec de alta calidad y de alta compresión basado en mpeg4.

dBm.- Deci Belios mili Watios.

Centos.- Community ENTerpriseOperating System.

libjpeg Librerías JPEG.

SIGLAS

LAN Redes de Área Local (Local Area Network).

MAN Redes de Área Metropolitana (Metropolitan Area Network).

WAN Redes de Área Extensa (Wide Area Network).

ISM Industrial, científica y Médica (Industrial, Scientific and Medical).

BSS Conjunto de Servicios Básicos.

BSA Área de Servicios Básicos.

WEP Equivalente de Privacidad Inalámbrica (Wireless Equivalent Privacy).

WPA Acceso WiFi Protegido (WiFi Protect Acces).

TKIP Integridad de Llave Temporal (Temporal Key Integrity Protocol)

AES Estándar de Codificación Avanzada (Advanced Encryption Standard).

IEEE Instituto de Ingenieros en Electricidad y Electrónica (Institute of Electrical and Electronics Engineers).

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

OFDM Multiplexación por División de Frecuencias Ortogonales (Orthogonal Frequency Divsion Multiplexing).

FCC Comisión Federal de Comunicaciones (Federal Communications Commission).

ETSI/MKK. Comisión Europea reguladora de las comunicaciones.

CCD Dispositivo de Carga Acoplada (Charge Coupled Device).

JPEG Grupo de Expertos en Fotografía (Joint Photographic Experts Group).

M-JPEG JPEG en Movimiento (Motion JPEG).

MPEG Grupo de Expertos en Imágenes Móviles (Motion Picture Experts Group).

PHP Preprocesador Hipertexto (Hypertext Preprocessor).

GPL Licencia Pública General (General Public Licens).

PTZ (Pan Tilt Zoom).

ACIERTE Academia de Certificaciones Internacionales en Redes y Tecnologías de Información.

FPS Cuadros por segundo. (Frame Per Second).

FTP Protocolo de Transferencia de Archivos (File Transfer Protocol).

Xhtml Lenguaje Extensible de Marcado de Hipertexto (eXtensible Hypertext Markup Language).

HTTP Protocolo de Transferencia de Hipertexto (HyperText Transfer Protocol).

RTSP Protocolo de Flujo de Datos en Tiempo Real (Real Time Streaming Protocol).

URL Localizador de Recurso Uniforme (Uniform Resource Locator).

EIA/TIA Asociación de Industrias Electrónicas / Asociación de las Industrias de Telecomunicaciones (Electronic Industries Alliance / Telecommunications Industry Association).

UGI Unidad de Gestión de Información.

MD5 Algoritmo de Resumen del Mensaje 5 (Message-Digest Algorithm 5).

PDU Protocolo de Unidad de Datos (Protocol Data Unit).

SDU Servicio de Datos de Unidad (Service Data Unit).

PLCP Procedimiento de Convergencia de Capa Física (Physical Layer Convergence Procedure).

TCP Protocolo de Control de Transmisión (Transmition Control Protocol).

IP Protocolo de Internet (Internet Protocol).

VLSM Mascara de Subred Variable (Variable Length Subnet Mask).

ANEXOS

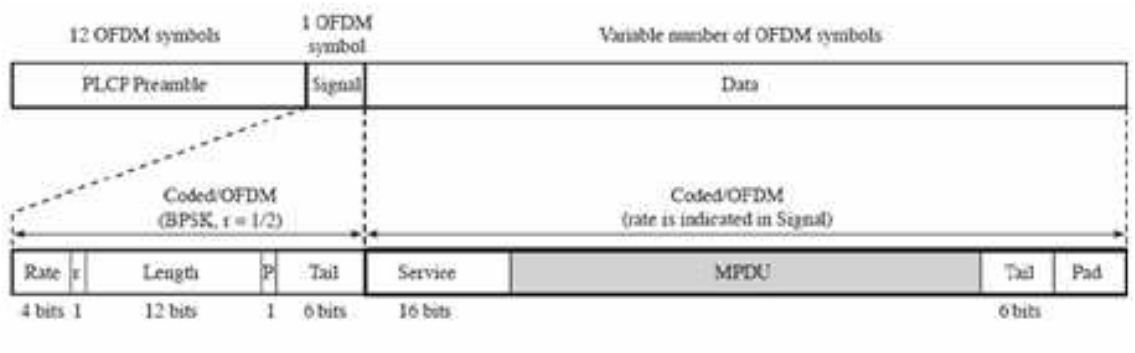
ANEXO A

PROCESO DE ENCAPSULAMIENTO DE UNA TRAMA 802.11 g.

ENCAPSULAMIENTO POR CAPA FÍSICA.

El proceso de encapsulamiento en capa física tiene como objetivo el transmitir las MAC PDU utilizando en este caso el método de transmisión OFDM.

A continuación se presenta la estructura de la trama de capa física (OFDM PLCP).



Dónde:

Campo Rate: Especifica la velocidad con la cual se transmite el campo data.

r: Reservado para un futuro.

Length: Número de octetos en el PDU MAC.

P: Bit de paridad par para los campos Rate, r, y Length,

Tail: Consiste de 6 ceros adheridos al símbolo para llevar al codificador convolucional al estado cero.

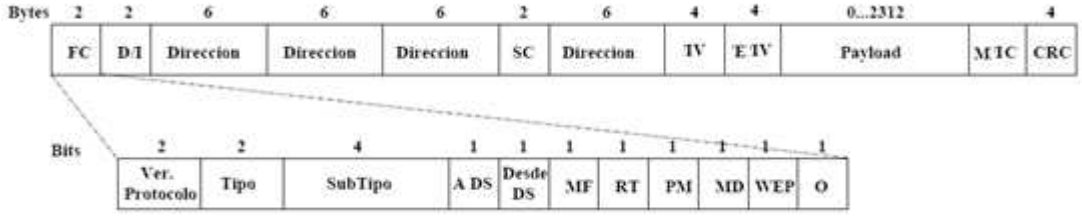
Pad: Numero de bits para hacer que el campo data sea múltiplo de un símbolo OFDM en este caso 6 bits.

1 OFDM symbol = 216 bits

MPDU=2362 bytes

Al sumar todos cada uno de los campos se obtiene un total de: **21732 bits o 2716,5 Bytes.**

ENCAPSULAMIENTO CAPA ENLACE DE DATOS SUBCAPA MAC.



FC: Frame control, indica el tipo de trama y la información de control.

D/I: Indica el tiempo en microsegundos que se tiene destinado para la transmisión de la trama.

Direction: Direcciones destino, origen y reserva.

SC: Secuencia de control, ayuda a desfragmentar y a eliminar tramas duplicadas.

IV: Vector de inicialización, sirve como punto de inicio para la generación de un stream de llaves.

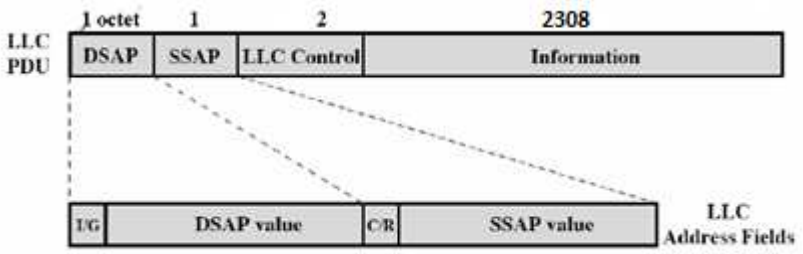
EIV: Vector de inicialización extendido, ayuda a mejorar la seguridad de las llaves generadas en el IV

MIC: Código de Integridad del mensaje, es un algoritmo de encripción llamado Michael.

MIC=8 bytes.

Al sumar todos los campos se obtiene el total de bytes por encapsulamiento de capa enlace de datos subcapa MAC = 2362 bytes.

Encapsulamiento Capa enlace de datos subcapa LLC.



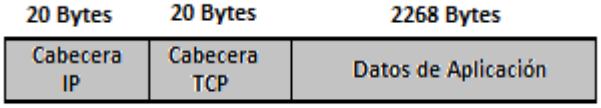
DSAP: Proporciona la dirección de punto de acceso al servicio en el destino.

SSAP: Proporciona la dirección de punto de acceso al servicio en el origen.

Al sumar todos estos campos se obtiene un total de bytes por encapsulamiento en la subcapa LLC de 2312 bytes.

ENCAPSULAMIENTO CAPAS SUPERIORES.

El encapsulamiento por capas superiores se toma en cuenta la cabecera TCP e IP.



Al sumar todos estos campos se obtiene un total de bytes por encapsulamiento por capas superiores de 2308 bytes.

Los datos correspondientes a la aplicación o bytes de datos son de 2268 Bytes.

ANEXO B

TRÁFICO DE DATOS CAPTURADOS UTILIZANDO UN SOFTWARE ANALIZADOR DE TRÁFICO.

El tráfico de datos que cursan por un canal de comunicaciones se lo realiza utilizando un software analizador de protocolos, en este caso se utiliza **Wireshark.**

Wireshark es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

En este caso se necesita observan los protocolos que cursan desde el router inalámbrico al servidor HP Proliant ML110, tal y como se indica en la siguiente figura B1.

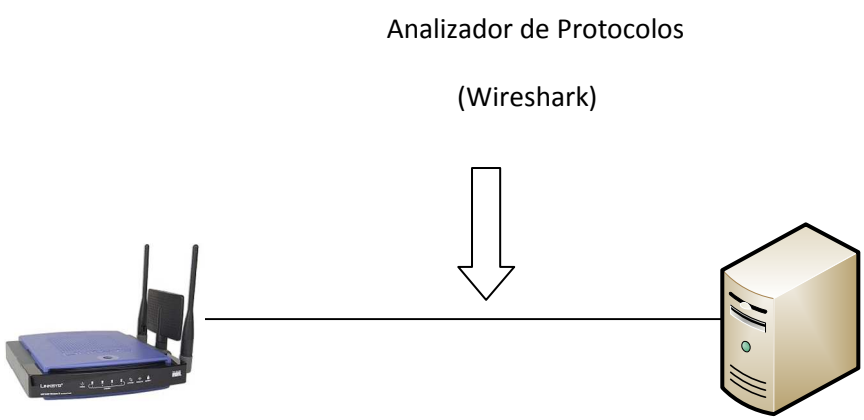


Figura B1. Esquema a analizar el Tráfico de datos.

En la figura B2, se indica la ventana principal, en la cual se indica el tráfico que se dirige desde el Router inalámbrico hacia el servidor HP ProLiant ML110.

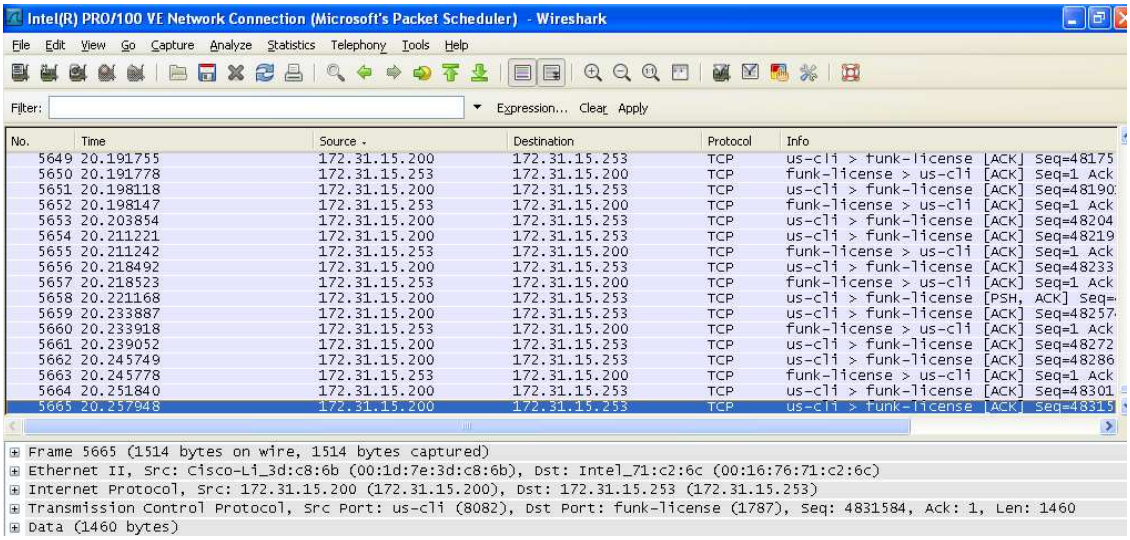
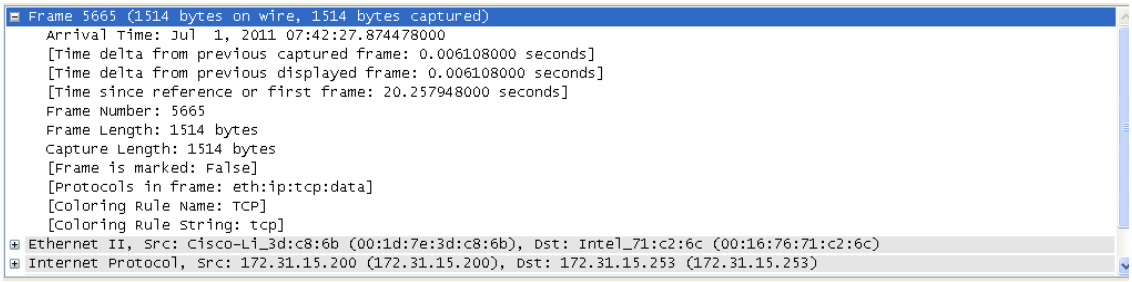


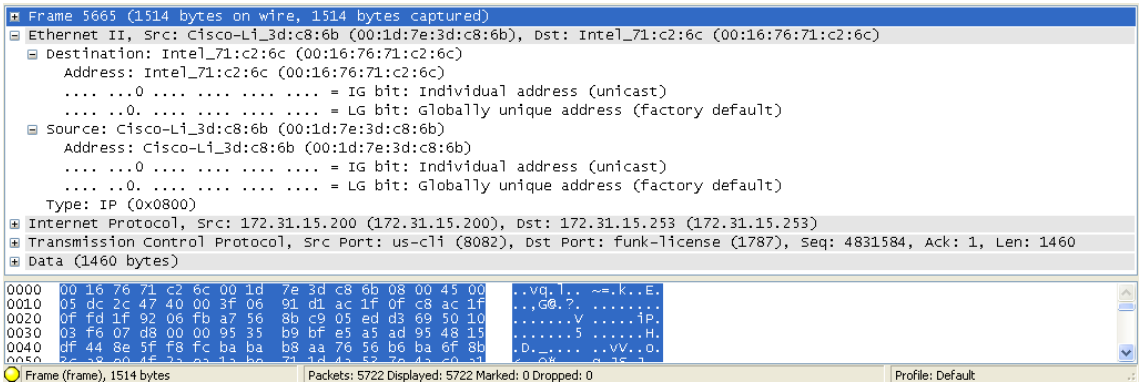
Figura B2. Ventana Principal de Wireshark con tráfico capturado.

Si se selecciona una trama capturada se puede observar lo siguiente:

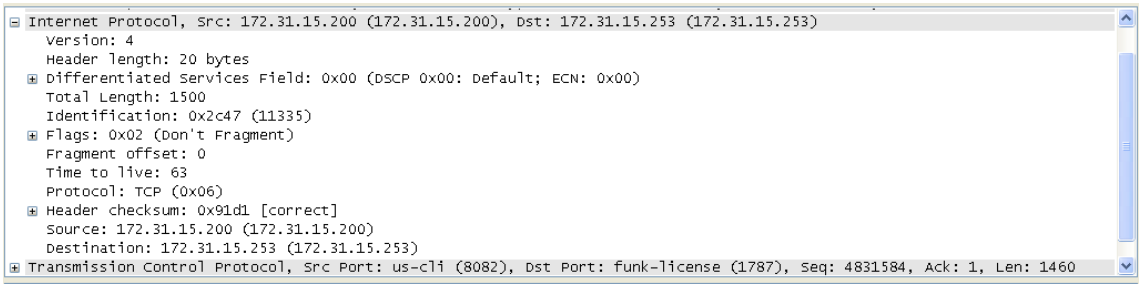
Tamaño de la trama: 1514 bytes



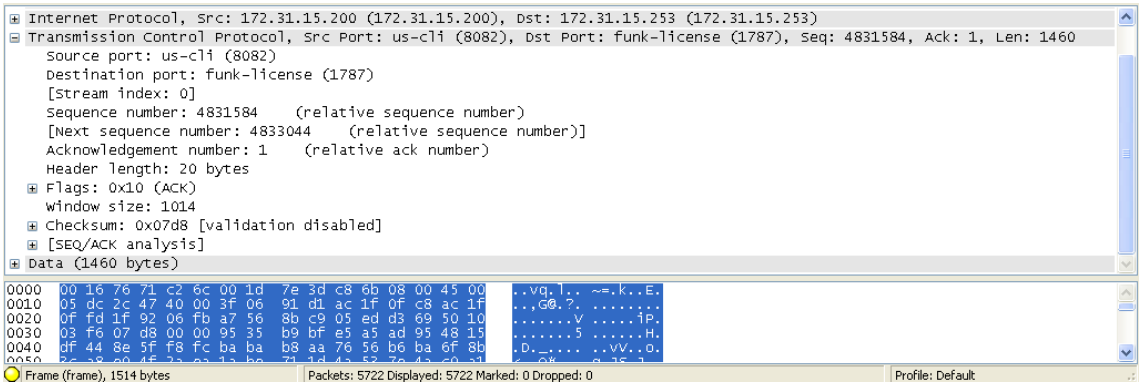
Protocolo de capa Física: Ethernet II.



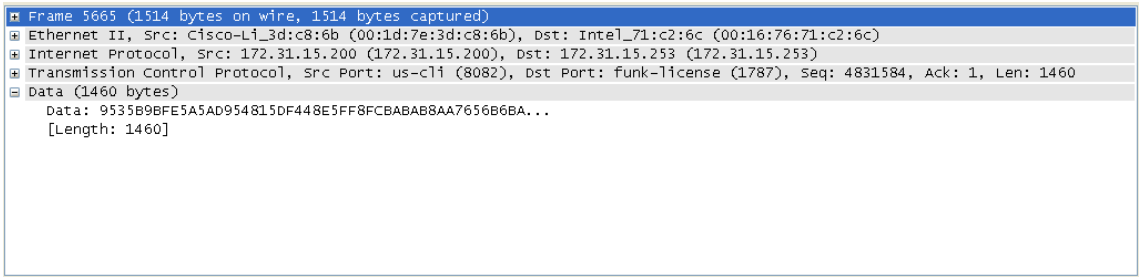
Protocolo IP.



Protocolo TCP.



Tamaño de la trama correspondiente a datos.


Frame 5665 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: Cisco-Li_3d:c8:6b (00:1d:7e:3d:c8:6b), Dst: Intel_71:c2:6c (00:16:76:71:c2:6c)
Internet Protocol, Src: 172.31.15.200 (172.31.15.200), Dst: 172.31.15.253 (172.31.15.253)
Transmission Control Protocol, Src Port: us-cli (8082), Dst Port: funk-license (1787), Seq: 4831584, Ack: 1, Len: 1460
Data (1460 bytes)
Data: 9535B9BFE5A5AD954815DF448E5FF8FCBABAB8AA7656B6BA...
[Length: 1460]

ANEXO C

DATASHEET CÁMARA IP FOSCAM FI8908W

Model: FI8918/FI8918W

IP Wireless / Wired Camera

NIGHT VISION & REMOTE PAN / TILT ROTATE/ TWO WAY AUDIO

User Manual

Color: Black

Color: White

1 WELCOME

IPCAM is an integrated wireless IP Camera solution. It combines a high quality digital video Camera with network connectivity and a powerful web server to bring clear to your desktop from anywhere on your local network or over the Internet.
The basic function of IPCAM is transmitting remote video on the IP network. The high quality video image can be transmitted with 30fps speed on the LAN/WAN by using MJPEG hardware compression technology.
The IPCAM is based on the TCP/IP standard. There is a WEB server inside which could support Internet Explore. Therefore the management and maintenance of your device become more simply by using network to achieve the remote configuration, start-up and upgrade firmware.
You can use this IPCAM to monitor some special places such as your home and your office. Also controlling the IPCAM and managing image are simple by clicking the website through the network.

1.1 Features

- Powerful high-speed video protocol processor
- High-sensitivity 1/4" CMOS sensor
- 300K Pixels
- IR night vision (Range: 8m)
- Pan 300 degree, tilt 120 degree
- Optimized MJPEG video compression for transmission
- Multi-level users' management and passwords definition
- Embedded Web Server for users to visit by IE
- Wi-Fi compliant with wireless standards IEEE 802.11b/g
- Supporting Dynamic IP (DDNS) and UPnP LAN and Internet (ADSL,Cable Modem)
- Giving alarm in cause of motion detection
- Supporting image snapshot
- Support multiple network protocols: HTTP/TCP/IP/UDP/STMP/DDNS/SNTP/DHCP/FTP
- Support WEP/WPA/WPA2 encryption

1.2 Packing List

Untie the pack and check the items contained against the following list:

- IPCAM×1
- Wi-Fi Antenna×1 (only available for wireless model)
- DC Power Supply×1
- Quick Installation Guide×1
- CD×1（Include IPCAM user manual、IP camera tool）
- Network Cable×1
- Mounting bracket×1(option)

NOTE: Please Contact us immediately in the case of any damaged or short of contents.

1.3 Product views

1.3.1 Front View

Figure 1.1

Infrared LED: 11 IR LEDs
LENS: CMOS sensor with fixed focus lens. (3.6mm)
WIFI Antenna: Wireless Antenna
Microphone: Build-in microphone
Speaker: Build-in speaker

1.3.2 Back View

Figure 1.2

LAN: RJ-45/10-100 Base T
Power: DC 5V/2A Power supply
Network Light: The LED will blink when plug the power
Power Light: If the power adapter works well, the light will turn on
Audio Input: The jack is used to plug external microphone
Audio Output: The jack is used to plug external speaker

4.2 Default Parameters

Default network Parameters
IP address: dynamic obtain
Subnet mask: 255.255.255.0
Gateway: dynamic obtain
DHCP: Disabled
DDNS: Disabled
Username and password
Default administrator username: **admin**
Default administrator password: No password

4.3 Specifications

ITEMS		FI8918/FI8918W
Image Sensor	Image Sensor	1/4" Color CMOS Sensor
	Display Resolution	640 x 480 Pixels(300k Pixels)
	Lens	f: 3.6mm, F:2.4 (IR Lens)
	Min. Illumination	0.5Lux
Lens	Lens Type	Glass Lens
	Viewing Angle	67Degree
Video	Image Compression	MJPEG
	Image Frame Rate	15fps(VGA),30fps(QVGA)
	Resolution	640 x 480(VGA), 320 x 240(QVGA)
	Flip Mirror Images	Vertical / Horizontal
	Light Frequency	50Hz, 60Hz or Outdoor
	Video Parameters	Brightness, Contrast
Communication	Ethernet	One 10/100Mbps RJ-45
	Supported Protocol	HTTP,FTP,TCP/IP,UDP,SMTP,DHCP,PPPoE,DDNS,UPnP,GPRS
	Wireless Standard	IEEE 802.11b/g
	Data Rate	802.11b: 11Mbps(Max.) 802.11g: 54Mbps(Max.)
	Wireless Security	WEP & WPA & WPA2 Encryption
	Infrared Light	11 IR LEDs, Night visibility up to 8 meters
	Dimension	110(L) x100(W) x106mm(H)
	Gross Weight	768g (Color Box Size:200X124X169mm)
	Net Weight	418g (accessories included)
Power	Power Supply	DC 5V/2.0A (EU,US,AU adapter or other types optional)
	Power Consumption	5 Watts (Max.)
Environment	Operate Temper.	0° ~ 55°C (14°F ~ 122°F)
	Operating Humidity	20% ~ 85% non-condensing
	Storage Temper.	-10°C ~ 60° (14°F ~ 140°F)

	Storage Humidity	0% ~ 90% non-condensing
PC Requirements	CPU	2.0GHZ or above
	Memory Size	256MB or above
	Display Card	64M or above
	Supported OS	Microsoft Windows 2000/XP/Vista/Windows7
	Browser	IE 6.0, IE7.0, IE8.0 firefox,goolge chrome,safari or other standard browsers
Certification	CE,FCC	
Warranty	Limited 1-year warranty	

5 OBTAINING TECHNICAL SUPPORT

While we hope your experience with the IPCAM network camera is enjoyable and easy to use, you may experience some issues or have questions that this User's Guide has not answered. Please contact your reseller and ask for help first, if they could not resolve your issue, please contact our company.

ANEXO D

DATASHEET HP PROLIANT ML110

HP ProLiant ML110 Generation 5 Server

Data sheet

Can you meet your computing challenges?

Keeping a small business up and running requires a server that is affordable, reliable, and easy to maintain. When you have limited IT resources, you can't assume that you will have staff onsite to handle day-to-day server-related tasks. You need a server that is easy to manage, even from a distance.

How do you meet these needs? Look to the compact and powerful, HP ProLiant ML110 Generation 5 (G5) Server. It delivers true server reliability and functionality for small businesses, branch offices, and remote locations—for the price of a typical desktop computer.

Right size and right features—at the right price

Versatile and easy to use, the ML110 G5 server is designed to be practical and affordable. It delivers all the entry-level server features that small businesses typically need, along with today's latest technology innovations.

Some new features of the ML110 G5 server include Intel® Xeon®, Core™2 Duo, Pentium®, or Celeron® processor, four hard disk drive bays, and an optional HP Lights-Out 100c Remote Management Card that is ideal for remote sites or second offices.

The HP ProLiant ML110 G5 Server is an efficiently-sized server that is ideal for small offices, first networks, and remote sites.

Key features and benefits

Proven HP dependability and support

- Through some rigorous and thorough testing within the industry, HP has built a reputation of dependability. This allows you to deploy the ML110 G5 server with confidence.
- The ML110 G5 server incorporates ProLiant quality that starts with design and is enhanced in manufacturing. Thanks to tireless work on system testing and process control, only the most dependable products reach your environment.

Expandable to grow with changing business needs

- This powerful yet simple platform provides all the relevant server features in an easy-to-use and easy-to-afford package.
- Practical features—such as Intel Xeon 3000 Series, Core 2 Duo, Pentium or Celeron processor, DDR II ECC memory, PCI-Express slots, serial port, and multiple USB 2.0 ports—deliver off-the-shelf functionality with the expandability to grow with your business.
- The ML110 G5 server is designed specifically for businesses that require an easy-to-configure, easy-to-use platform. All major components are designed to be removed or installed with little effort. When growth becomes necessary for a small business network, the ML110 G5 server is easily reconfigurable.
- Companies with remote locations or trusted advisors can take advantage of the optional HP Lights-Out 100c Remote Management Card to decrease server and company downtime, and to increase productivity.

A true server at a desktop price

- The ML110 G5 server incorporates many features that are ideal for small- and medium-size businesses and remote-site locations.
- The design provides a simplified server with the right features at the right price for a small business.
- ProLiant 100 Series servers have tailored features to reflect the usage needs of small businesses and branch offices.

Ideal environments

Ideal applications

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

Remote site or branch offices of small- to medium-size businesses

- Entry-level, single processor server solution for budget-conscious businesses
- Optional, industry-standard remote manageability to manage remote locations
- A variety of service options for tailored support solutions

Small businesses running light applications

- The ML110 G5 server delivers peace of mind through practical design and strenuous testing, helping to deliver dependable performance
- Growth and adaptability are achieved through memory, HDD, and PCI card expandability, giving the ML110 G5 server the headroom to grow with your business
- Small businesses can depend on HP to provide the products and support needed to handle their day-to-day server tasks in a smooth and efficient manner

HP Services

When technology works, business works

The challenge of virtually every IT organization is similar—to develop and maintain an agile, efficient server infrastructure that delivers the service levels your business needs.

HP Technology Services offers a comprehensive portfolio of HP Care Pack Services to help design, deploy, manage, and support your IT environment, enabling cost-effective upgrades to standard warranty with easy-to-buy and easy-to-use support packages.

Minimum recommended HP Care Pack offerings

- 3-year, next business day response onsite, 9-hour x 5-day coverage, hardware support
- Hardware installation only

Enhanced service-level Care Pack offerings

- 3-year same business day, 4-hour response onsite 13-hour x 5-day coverage, hardware support
- Hardware installation plus operating system installation and startup

Benefit from HP Care Pack Services that help you

- Reduce deployment time and manage ProLiant server solutions smoothly and efficiently
- Increase uptime and performance of servers' availability to your business
- Detect, diagnose, and repair problems to quickly save time, money, and resources

For more information, visit
www.hp.com/services/proliantservices or
www.hp.com/go/proliant/carepack

HP ProLiant ML110 Generation 5 Server

Processor and memory	
Number of processors	1
Maximum number of cores	4
Processors supported	Quad-Core Intel Xeon processor: X3370, 3.00 GHz, 1333 MHz X3360, 2.83 GHz, 1333 MHz X3350, 2.66 GHz, 1333 MHz X3220, 2.40 GHz, 1066 MHz X3210, 2.13 GHz, 1066 MHz Dual-Core Intel Core 2 Processor: E7400, 2.80 GHz, 1066 MHz Dual-Core Intel Xeon Processor: E3120, 3.16 GHz, 1333 MHz E3110, 3.00 GHz , 1333 MHz Dual-Core Intel Pentium Processor: E2160, 1.80 GHz, 800 MHz Single-Core Intel Celeron Processor: 440, 2.00 GHz, 800 MHz
Processor cores	Single, dual, and quad core
Cache	12 MB Level 2 cache (Xeon X3370, X3360) 8 MB Level 2 cache (Xeon 3200 Series) 6 MB Level 2 cache (Xeon X3350, E3120, E3110) 3 MB Level 2 cache (Core2 Series) 1 MB Level 2 cache (Pentium Series) 512 KB Level 2 cache (Celeron Series)
Maximum processor speed	3.16 GHz
Multi-processor	N/A
Maximum front-side bus speed	1333 MHz
Memory type	PC2-6400 unbuffered DDR2 ECC 800 MHz
Standard memory	1 GB
Maximum memory	8 GB
Advanced memory protection	N/A
Storage	
Storage type	Non-hot plug 3.5-inch SAS Non-hot plug 3.5-inch SATA
Drives supported	Up to 4: Non-hot plug LFF SAS 15K 450/300/146 GB Non-hot plug LFF SATA 7.2K 1 TB/500 GB/250 GB/160 GB
Maximum internal Storage	1.8 TB SAS; 4.0 TB SATA
Maximum internal drives	4
Removable media bays	2
Expansion slots	4 total: 3 PCI Express (1x8 and 2x1) 1 3.3 V PCI
Storage controller	SATA Models: Integrated 6 ports SATA controller with embedded RAID (4 ports available for Hard Disks) SAS Models: HP SC40Ge Host Bus Adapter with RAID 0, 1 support, RO

Operating system	
OS choices	Microsoft® Windows® Server 2003 R2 Microsoft Windows Small Business Server 2003 Microsoft Windows Server 2008 Microsoft Windows Small Business Server 2008 Microsoft Windows Essential Business Server 2008 Red Hat Enterprise Linux SUSE Linux Enterprise Server Netware
For additional information, please visit www.hp.com/go/ossupport	

Deployment	
Form factor	Tower with Rack Mount Option Kit
Rack height	4U
Networking	Embedded NC105i Express Gigabit Ethernet Server Adapter
Remote management	Standard IPMI 2.0 reporting Lights-Out 100c Remote Management Card (optional)
Warranty (parts/labor/onsite)	Standard: 1-year/1-year/1-year Asia Pacific (excluding Japan): 3-year/1-year/1-year

Financial services

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

Affordability, reliability, and simplicity make HP ProLiant ML110 G5 server ideal for your growing business. To understand how the ML100 G5 server is well-suited for small offices, first networks, and remote sites, visit: www.hp.com/servers/proliantml110

ANEXO E

DATASHEET ROUTER INALÁMBRICO LINKSYS WRT300N

LINKSYS®
A Division of Cisco Systems, Inc.

Start a Wireless Network With Up To 4X the Range and 12X the Speed!

The Wireless-N Broadband Router is really three devices in one box. First, there's the Wireless Access Point, which lets you connect to the network without wires. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices together. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

The Access Point built into the Router uses the very latest wireless networking technology, Wireless-N (draft 802.11n). By overlaying the signals of multiple radios, Wireless-N's "Multiple In, Multiple Out" (MIMO) technology multiplies the effective data rate. Unlike ordinary wireless networking technologies that are confused by signal reflections, MIMO actually uses these reflections to increase the range and reduce "dead spots" in the wireless coverage area. The robust signal travels farther, maintaining wireless connections up to 4 times farther than standard Wireless-G.

With Wireless-N, the farther away you are, the more speed advantage you get. It works great with standard Wireless-G and -B equipment, but when both ends of the wireless link are Wireless-N, the router can increase the throughput even more by using twice as much radio band, yielding speeds up to 12 times as fast as standard Wireless-G. But unlike other speed-enhanced technologies, Wireless-N can dynamically enable this double-speed mode for Wireless-N devices, while still connecting to other wireless devices at their respective fastest speeds. In congested areas, the "good neighbor" mode ensures that the Router checks for other wireless devices in the area before gobbling up the radio band.

To help protect your data and privacy, the Router can encode all wireless transmissions with industrial-strength 256-bit encryption. It can serve as your network's DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, and supports VPN pass-through. Configuration is a snap with the web browser-based configuration utility.

The incredible speed of Wireless-N makes it ideal for media-centric applications like streaming video, gaming, and Voice over IP telephony, and gives you plenty of headroom to run multiple media-intense data streams through the network at the same time, with no degradation in performance. With the Linksys Wireless-N Broadband Router at the center of your home or office network, you can share a high-speed Internet connection, files, printers, and multi-player games, and run media-intensive applications at faster than 10/100 wired network speeds, without the hassle of stringing wires!

Internet-sharing Router and 4-port Switch, with a built-in speed and range enhanced Wireless Access Point	MIMO technology uses multiple radios to create a robust signal that travels up to 4 times farther and reduces dead spots	Up to 12 times faster than Wireless-G, but also works great with Wireless-G and -B devices	Wireless signals are protected by up to 256-bit encryption, and your network is protected from Internet attacks by a powerful SPI firewall

Wireless-N

WIRELESS

Broadband Router

Product Data

Cisco Systems

Model WRT300N

Wireless-N

Broadband Router

Features

- Complies with IEEE draft 802.11n standards
- Blazing fast wireless speeds for high bandwidth applications such as video streaming or file sharing
- Unsurpassed wireless security with 256-bit encryption
- Expanded wireless coverage. Up to 4X the range of 802.11g products
- All LAN ports support auto-crossover (MDI/MDI-X)—No need for crossover cables
- Device can be placed vertically or horizontally

Specifications

Model	WRT300N
Standards	Draft 802.11n, 802.11g, 802.11b, 802.3, 802.3u
Ports	Power, Internet, Ethernet
Button	Reset
Cabling Type	CAT5
LEDs	Power, Internet, Ethernet (1-4), Wireless
Number of Antennas	3
Transmit Power	17 dBm
Antenna Gain	2 dBi
UPnP able/cert	able
Security Features	Up to 256-bit wireless encryption
Security Key Bits	64, 128, 256

Environmental

Dimensions	7.40" x 1.57" x 6.93" (188 x 40 x 176 mm)
Weight	18.60 oz. (0.527 kg)
Power	12 V, 1 A
Certification	FCC, CE, IC-03
Operating Temp.	0° C to 40° C (32° F to 104° F)
Storage Temp.	-20° C to 70° C (-4° F to 158° F)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Linksys
A Division of Cisco Systems, Inc.
121 Theory
Irvine, CA 92617 USA

E-mail: sales@linksys.com
support@linksys.com

Web: http://www.linksys.com

Linksys products are available in more than 50 countries, supported by 12 Linksys Regional Offices throughout the world. For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.

Minimum Requirements

- Internet Explorer 5.5 or Firefox 1.0
- CD-ROM Drive
- Windows 2000 or XP
- Network Adapter

Package Contents

- Wireless-N Broadband Router
- Setup CD-ROM with Norton Internet Security
- User Guide on CD-ROM
- Ethernet Network Cable
- Power Adapter

ANEXO F

INSTALACIÓN DEL SISTEMA OPRATIVO CENTOS 5.5

INSTALCIÓN DE CENTOS 5.4

La instalación de CentOS 5.4 se lo realiza utilizando un DVD e insertandolo en el lector de DVD's del servidor mientras se ejecuta la secuencia de bios.

Una vez que el computador identifica que el lector de DVD's contiene un disco ejecutable, se carga la pantalla de bienvenida del Sistema Operativo Centos 5.4 tal y como se muestra en la figura D.1.

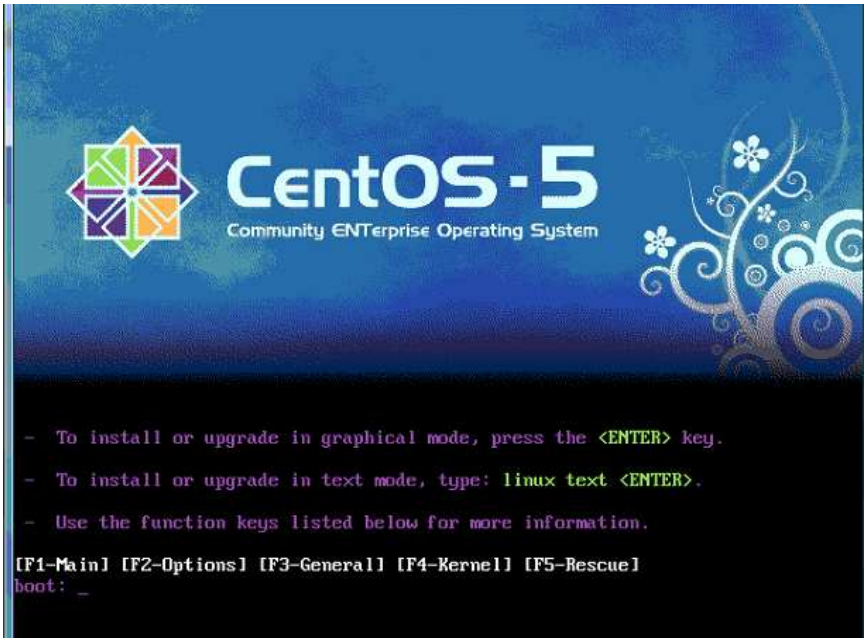


Figura D.1 Pantalla de bienvenida del sistema operativo Centos 5.4.

La instalación se realiza utilizando la interfaz gráfica, por lo que se presiona la tecla "enter" para continuar.

Para evitar errores en la instalación, Centos 5.4 tiene una opción que permite comprobar si el disco tiene errores tal y como se muestra en la figura D.2. En este caso se obvia la comprobación del disco.

Figura D.2 Pantalla de comprobación de DVD.

En la figura D.3, se indica la pantalla de inicio de instalación del Sistema Operativo Centos 5.4.

Figura D.3 Pantalla de inicio de instalación.

El idioma con el que se instala el sistema operativo es en inglés, debido a que la ayuda que posee el sistema operativo tiene errores en la traducción al español.

En la figura D.4 se indica la pantalla de configuración de idioma.

Figura D.4 Pantalla de configuración de idioma.

La distribución del teclado que se utiliza para la instalación y configuración del sistema operativo es Español tal y como se indica en la figura D.5

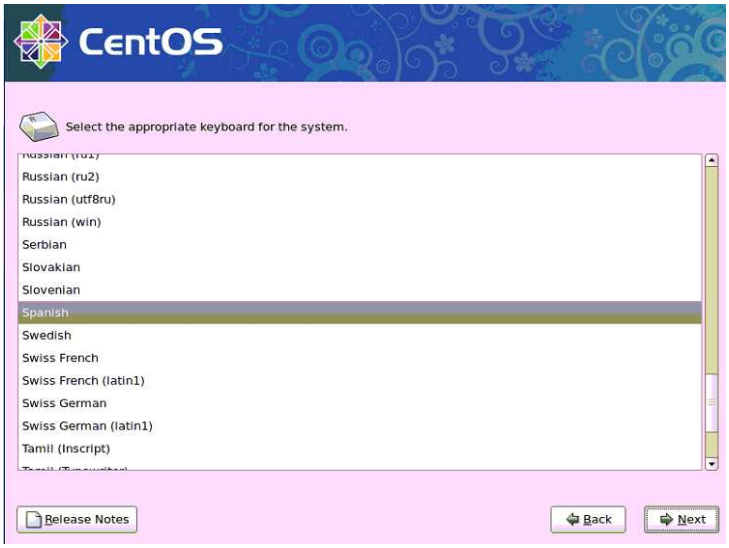


Figura D.5 Pantalla de configuración de la distribución del teclado.

La tabla de particiones que se maneja tiene q ser personalizada, por lo que se escoge la opción crear particiones personalizadas, tal y como se muestra en la figura D.6.

Figura D.6 Pantalla de configuración de particiones y gestión de discos.

En el servidor se instaló dos discos duros; el primero tiene una capacidad de 250 GB y el segundo tiene una capacidad de 500 GB.
Para el correcto funcionamiento de Centos 5.4, es necesario trabajar con al menos 2 particiones:

Swap.- Es el área de intercambio o el espacio en disco duro donde se transfieren las imágenes de procesos que se encuentren en memora RAM, para de esta manera liberar espacio en la memoria.
/.- En esta partición se instala el sistema operativo.

Es recomendable instalar más de una partición, por ejemplo una partición dedicada a /var, al /etc y /usr; pero en este caso lo que interesa es tener en una partición o disco duro separado para las grabaciones de video.
La tabla de particiones a configurar se indica en la tabla D.1.

Sda	
Partición	Tamaño en GB
SWAP	2
/	248
Sdb	
/eventos	500

Tabla D.1 Tabla de particiones.

En la figura D.7 se indica las particiones creadas en los dos discos duros.

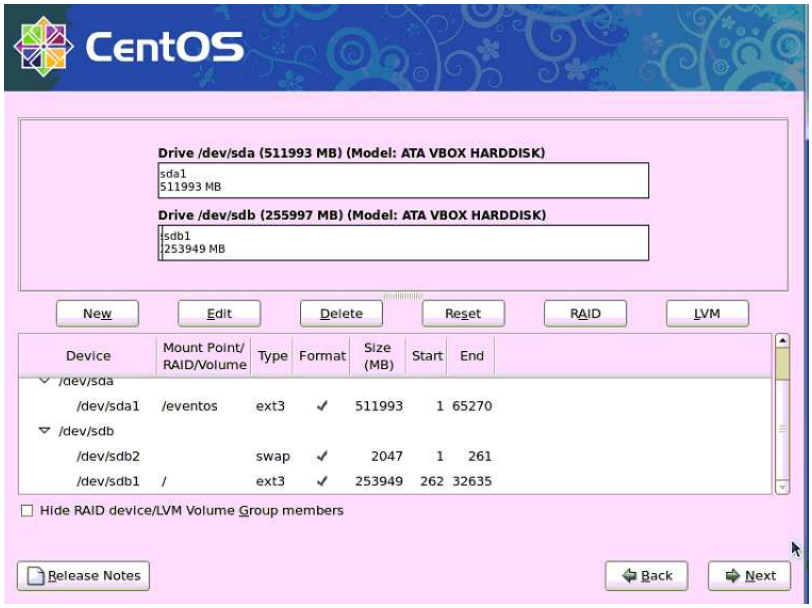


Tabla D.7 Pantalla de particiones creadas en los disco duros.

La instalación de “GRUB” permite gestionar varios sistemas operativos instalados en las diferentes particiones y escoger cual se inicia. En este caso se deja que se escriba en el MBR, tal y como se indica en la figura D.8

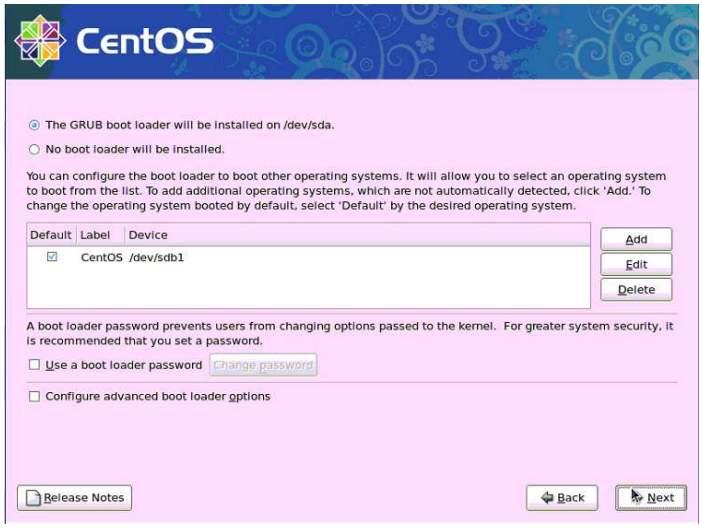


Figura D.8 Pantalla de instalación del GRUB.

En la siguiente ventana de configuración se configura la dirección IP de servidor, máscara de red, puerta de salida, DNS y nombre de host. En la figura D.9, D.10 y D.11 se indica las configuraciones realizadas.

Figura D.9 Pantalla de configuración de dispositivos de red.

Figura D.10 Pantalla de configuración de dirección IP.

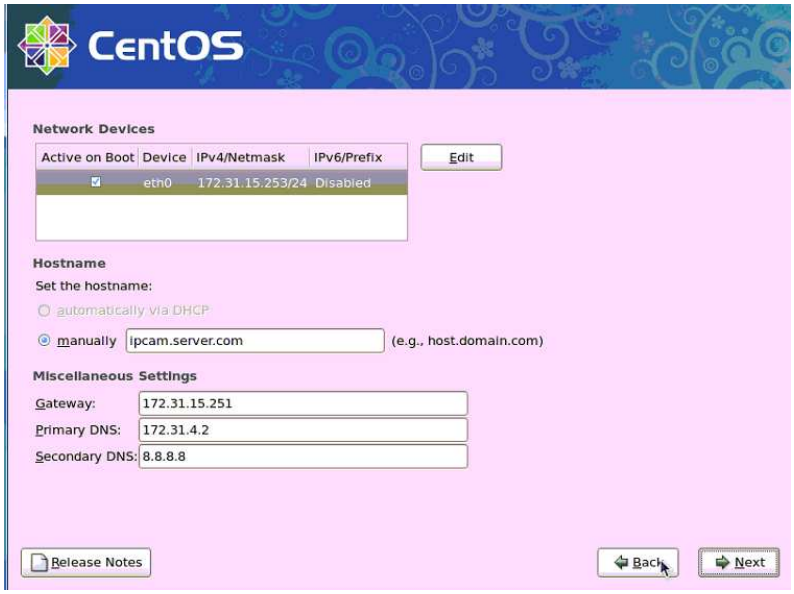


Figura D.11 Pantalla de configuración Dispositivos de red.

En la figura D.12 se configura la zona horaria donde se encuentra el servidor, en este caso se coloca a Guayaquil, Ecuador como referencia.

Figura D.12 Pantalla de configuración de Zona Horaria.

Para la gestión de Centos 5.4 es primordial ingresar una contraseña, tal y como se indica en la figura D.13.

Figura D.13 Pantalla de configuración de password de súper usuario.

El último paso es configurar lo que se necesita instalar. Centos 5.4 tiene una gran cantidad de aplicaciones pero muchos de estos son innecesarios. En la figura

D.14 se indica los ambientes de escritorio a instalarse en este caso se utiliza GNOME, debido a que es un ambiente gráfico que no consume mucha memoria para su ejecución.

Figura D.14 Pantalla de instalación de ambientes de escritorio.

En la pestaña Aplicaciones se deshabilita juegos y entretenimiento, productividad y oficina, video y sonido, tal y como se muestra en la figura D.15.

Figura D.15 Pantalla de instalación de Aplicaciones.

En la pestaña desarrollo se selecciona todo, debido que al realizar la instalación de ZoneMinder es necesario el uso de compiladores, tal y como se indica en la figura D.16.

Figura D.16 Pantalla de instalación de desarrollo.

La pestaña servers se deja deshabilitada, debido a que durante la configuración del sistema operativo se instala las versiones más actuales de los servidores, tal y como se indica en la figura D.17.

Figura D.17 Pantalla de instalación de servidores.

En la figura D.20 se indica la pestaña sistema base y se escoge herramientas administrativas y herramientas del sistema.

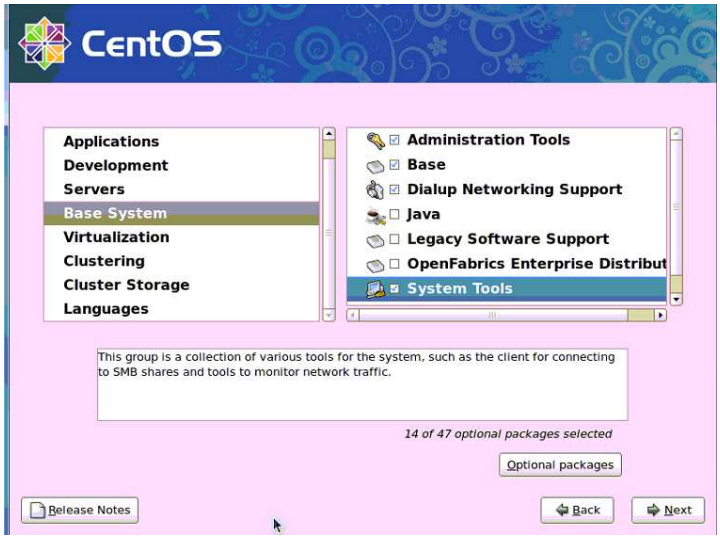


Figura D.20 Pantalla de configuración de sistema base.

En la figura D.21, se indica el paso final de la instalación del sistema Operativo Centos 5.4.

Figura D.21 Pantalla previa a la instalación del sistema operativo Centros 5.4.

ANEXO G

SCRIPT PARA IMPLEMENTACIÓN DEL FIREWALL

```
#!/bin/sh
case "$1" in
start)
#====================================================================
====
#====================================================================
====
                #Firewall
#====================================================================
====
#====================================================================
====

#Inicio de un script que nos permite la implementación de un Firewall

#====================================================================
====
#Mostramos en pantalla la aplicación de las reglas de firewall
echo -n Aplicando Reglas de Firewall...
#====================================================================
====

#====================================================================
====
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
#====================================================================
====

#====================================================================
====
## Se establece la  politica por defecto: DROP o negamos todo tipo de
conexion
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#====================================================================
====
#====================================================================
====
#Se empieza a permitir y abrir puertos

# Operar en localhost sin limitaciones
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
#====================================================================
====
#====================================================================
====
# Al host le permitimos todo
iptables -A INPUT -s 172.31.15.253 -j ACCEPT
```

```
iptables -A OUTPUT -d 172.31.15.253 -j ACCEPT
#================================================================
====

#================================================================
====
#Abrimos los puertos necesarios para que el servidor trabaje sin
problemas
# Abrimos el puerto 80 para conexiones al servidor web
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 80 -m state --state
RELATED,ESTABLISHED -j ACCEPT
#================================================================
====

#================================================================
====
# Permitimos que el servidor pueda conectarse al puerto 80 de otras
hosts
iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state
RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
#================================================================
====

#================================================================
====
# Abrimos el puerto 443 para conexiones al servidor web seguro
iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 443 -m state --state
RELATED,ESTABLISHED -j ACCEPT
#================================================================
====

#================================================================
====
# Abrimos el puerto 443 para conexiones al puerto 443 de otras hosts
iptables -A INPUT -p tcp -m tcp --sport 443 -m state --state
RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
#================================================================
====

#================================================================
====
# Abrimos el puerto  para conexiones al servidor smtp de gmail
#iptables -A INPUT -p tcp -m tcp --dport 587 -j ACCEPT
#iptables -A OUTPUT -p tcp -m tcp --sport 587 -m state --state
RELATED,ESTABLISHED -j ACCEPT
#================================================================
====

#================================================================
====
# Abrimos el puerto para conexiones al puerto 587 de otras hosts
iptables -A INPUT -p tcp -m tcp --sport 587 -m state --state
RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --dport 587 -j ACCEPT
#================================================================
====

#================================================================
====
# Reglas necesarias para conexiones a las cámaras. Se permiten
conexiones entrantes YA establecidas
iptables -A INPUT -p tcp -m tcp --sport 8081:8084 -m state --state
ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p tcp -m tcp --dport 8081:8084 -m state --state
NEW,RELATED,ESTABLISHED -j ACCEPT
#================================================================
====

#================================================================
====
# Permitimos la consulta a un primer DNS
iptables -A INPUT -s 172.31.4.2 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d 172.31.4.2 -p udp -m udp --dport 53 -j ACCEPT
#================================================================
====

#================================================================
====
# Permitimos la consulta a un segundo DNS
iptables -A INPUT -s 8.8.8.8 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d 8.8.8.8 -p udp -m udp --dport 53 -j ACCEPT
#================================================================
====

#================================================================
====
# Permitimos consultar el reloj de hora.rediris.es (un pentium166)
para sincronizarse
iptables -A INPUT -s 130.206.3.166 -p udp -m udp --dport 123 -j
ACCEPT
iptables -A OUTPUT -d 130.206.3.166 -p udp -m udp --sport 123 -j
ACCEPT
#================================================================
====

#================================================================
====
# Abrimos el puerto 22 para conexiones ssl
iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 22 -m state --state
RELATED,ESTABLISHED -j ACCEPT
#================================================================
====

#================================================================
====
# Abrimos el puerto 22 para conexiones ssl de otros hosts
iptables -A INPUT -p tcp -m tcp --sport 22 -m state --state
RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT
#=================================================================
====

#=================================================================
====
echo " ..............OK "
;;
stop)
# Borramos todas las reglas:
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

;;

*)
exit 1
;;
esac

exit 0
```

ANEXO H

SCRIPT CONTROL DE MOVIMIENTO DE LA CÁMARA IP FOSCAM FI8908W

```
# ============================================================
#
# ============================================================
#
# This module contains the implementation of the Foscam FI8908W IP
camera control
# protocol
#
#============================================================
#Define al archivo FoscamFI8908w.pm como un modulo de PERl para no
ingresar
#el path completo del compilador
package ZoneMinder::Control::FoscamFI8908W;
#============================================================

#============================================================
#Indica la version del compilador
use 5.006;
#============================================================

#============================================================
#Definimos la directiva strict
use strict;
#============================================================

#============================================================
#Definimos la directiva warnings
use warnings;
#============================================================

#============================================================
#Invocamos al modulo ZoneMinder y ejecutamos subrutina Base y Control
require ZoneMinder::Base;
require ZoneMinder::Control;
#============================================================
#============================================================
# Heredamos contenidos
our @ISA = qw(ZoneMinder::Control);
#============================================================
#Heredamos contenidos
our $VERSION = $ZoneMinder::Base::VERSION;

# ============================================================
#
# Foscam FI8908W IP Control Protocol
#
# ============================================================
#Usamos todas las variables contenidas dentro de la subrutina Debug y
config
# del modulo ZoneMinder
use ZoneMinder::Debug qw(:all);
use ZoneMinder::Config qw(:all);
# ============================================================

#Usamos todas la variable contenida dentro de la subrutina HiRes
```

```
# del modulo Time
use Time::HiRes qw( usleep );
# ============================================================
#Definimos variables iniciales
# ============================================================

 my $ini = 4;
 my $ini2 = 4;
 my $ini3 = 100;
 my $ini4 = 100;
# ============================================================
#Formato proporcionado por ZoneMinder para el manejo de las camaras
PTZ
# ============================================================

sub new
{

my $class = shift;
my $id = shift;
my $self = ZoneMinder::Control->new( $id );
my $logindetails = "";
bless( $self, $class );
srand( time() );
return $self;

}

our $AUTOLOAD;

sub AUTOLOAD
{
my $self = shift;
my $class = ref($self) || croak( "$self not object" );
my $name = $AUTOLOAD;
$name =~ s/.*://;
if ( exists($self->{$name}) )
{
return( $self->{$name} );
}
Fatal( "Can't access $name member of object of class $class" );
}
our $stop_command;

sub open
{
my $self = shift;

$self->loadMonitor();

use LWP::UserAgent;
$self->{ua} = LWP::UserAgent->new;
$self->{ua}->agent( "ZoneMinder Control Agent/".ZM_VERSION );

$self->{state} = 'open';
}
```

```
sub close
{
my $self = shift;
$self->{state} = 'closed';
}

sub printMsg
{
my $self = shift;
my $msg = shift;
my $msg_len = length($msg);

Debug( $msg."[".$msg_len."]" );
}

sub sendCmd
{
my $self = shift;
my $cmd = shift;
my $result = undef;
printMsg( $cmd, "Tx" );

my $req = HTTP::Request->new( GET=>"http://".$self->{Monitor}-
>{ControlAddress}."/$cmd" );
my $res = $self->{ua}->request($req);

if ( $res->is_success )
{
$result = !undef;
}
else
{
Error( "Error check failed:'".$res->status_line()."'" );
}

return( $result );
}

# ============================================================
#Subrutina que permite enviar reiniciar la camara
sub reset
{
#Seteamos el valor de la variable self
my $self = shift;
#Se hace referencia a la subrutina Camera Reset
Debug( "Camera Reset" );
#Se almacena en la variable cmd
 my $cmd = "camera_control.cgi?param=2&value=4";
#Se almacena el resultado de la subrutina SendCmd en la variable
self.
 $self->sendCmd( $cmd );

}
# ============================================================

# ============================================================
#subrutina de movimiento hacia arriba
```

```
sub moveConDown
{
my $self = shift;
Debug( "Move Down" );
my $cmd = "decoder_control.cgi?command=0";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );
}
# ============================================================

# ============================================================

#Subrutina de movimiento hacia abajo
sub moveConUp
{
my $self = shift;
Debug( "Move Up" );
my $cmd = "decoder_control.cgi?command=2";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );

}
# ============================================================

# ============================================================
#Subrutina de Movimiento hacia la Izquierda
sub moveConLeft
{
my $self = shift;
Debug( "Move Left" );
my $cmd = "decoder_control.cgi?command=4";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );

}
# ============================================================

# ============================================================

#Subrutina del Movimiento hacia la derecha
sub moveConRight
{
my $self = shift;
Debug( "Move Right" );
my $cmd = "decoder_control.cgi?command=6";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );

}
```

```
# ============================================================

# ============================================================

#Subrutina del Movimiento Superior Derecha

sub moveConUpRight
{
my $self = shift;
Debug( "Move Diagonally Up Right" );
my $cmd = "decoder_control.cgi?command=91";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );

}
# ============================================================

# ============================================================

#Subrutina del Movimiento Inferior Derecha
sub moveConDownRight
{
my $self = shift;
Debug( "Move Diagonally Down Right" );
my $cmd = "decoder_control.cgi?command=93";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );
}
# ============================================================

# ============================================================

#Subrutina del Movimiento Superior Izquierda

sub moveConUpLeft
{
my $self = shift;
Debug( "Move Diagonally Up Left" );
my $cmd = "decoder_control.cgi?command=90";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );
}
# ============================================================

# ============================================================

#Subrutina del Movimiento Inferior Izquierda

sub moveConDownLeft
{
my $self = shift;
```

```
Debug( "Move Diagonally Down Left" );
my $cmd = "decoder_control.cgi?command=92";
$self->sendCmd( $cmd );
sleep(1);
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );
}
# ============================================================

# ============================================================

#Subrutina Deter Movimiento

sub moveStop
{
my $self = shift;
Debug( "Move Stop" );
my $cmd = "decoder_control.cgi?command=1";
$self->sendCmd( $cmd );
}
# ============================================================

# ============================================================

#Subrutina Establecer posicion origen
sub presetHome
{
my $self = shift;
Debug( "Home Preset" );
my $cmd = "decoder_control.cgi?command=25";
$self->sendCmd( $cmd );
}
# ============================================================

# ============================================================

#Subrutina Incrementar Brillo


sub focusRelFar
{

    my $self = shift;
    my $params = shift;
    Debug( "Focus Far" );
    $ini = $ini -1;
    my $cmd = "camera_control.cgi?param=2&value=$ini";
    $self->sendCmd( $cmd );
    $ini2= $ini;
}
# ============================================================

# ============================================================

#Subrutina Reducir Brillo
```

```
sub focusRelNear
{

 my $self = shift;
    my $params = shift;
    $ini2 = $ini2 + 1;
    Debug( "Focus Near" );
    my $cmd = "camera_control.cgi?param=2&value=$ini2";
    $self->sendCmd( $cmd );
    $ini=$ini2;
}
# ============================================================

# ============================================================

#Subrutina Reducir Contraste


sub irisRelClose
{

    my $self = shift;
    my $params = shift;
    Debug( "Iris Close" );
    $ini3 = $ini3 -10;
    my $cmd = "camera_control.cgi?param=1&value=$ini3";
    $self->sendCmd( $cmd );
    $ini4= $ini3;
}
# ============================================================

# ============================================================

#Subrutina Incrementar Contraste


sub irisRelOpen
{

 my $self = shift;
    my $params = shift;
    $ini4 = $ini4 + 10;
    Debug( "Iris Open" );
    my $cmd = "camera_control.cgi?param=1&value=$ini4";
    $self->sendCmd( $cmd );
    $ini3=$ini4;

}
# ============================================================

# ============================================================

#Subrutina Presets presentes


sub presetGoto
{
```

```
my $self = shift;
my $params = shift;
#Seteamos el valor de preset en 0
my $preset = 0;
#Se obtiene el valor del preset selecionado
my $preset = $self->getParam( $params, 'preset' );
    #Se ejecuta la subrutina para los presets
Debug( "Goto Preset $preset" );
#Condicional para la vision de 60 Hz.
if ($preset == 1)

{
    my $cmd = "camera_control.cgi?param=3&value=0";
    $self->sendCmd( $cmd );
}
#Condicional para la vision de 60 Hz.
elsif ($preset == 2)

    {
            my $cmd = "camera_control.cgi?param=3&value=1";
            $self->sendCmd( $cmd );
    }

#Condicional para la vision en exteriores
 elsif ($preset == 3)

    {
            my $cmd = "camera_control.cgi?param=3&value=2";
            $self->sendCmd( $cmd );
    }

#Condicional para vision flip
elsif ($preset == 4)

    {
            my $cmd = "camera_control.cgi?param=5&value=0";
            $self->sendCmd( $cmd );
    }

#Condicional para vision Flip y Mirror
    elsif ($preset == 5)

    {
            my $cmd = "camera_control.cgi?param=5&value=1";
            $self->sendCmd( $cmd );
    }

#Condicional para vision Mirror
    elsif ($preset == 6)

    {
            my $cmd = "camera_control.cgi?param=5&value=2";
            $self->sendCmd( $cmd );
    }
#Condicional para vision por Default
elsif ($preset == 7)
```

```
        {
                my $cmd = "camera_control.cgi?param=5&value=3";
                $self->sendCmd( $cmd );
        }


    #Condicional para movimiento continuo Vertical
    elsif ($preset == 8)

    {
        my $cmd = "decoder_control.cgi?command=26";
                $self->sendCmd( $cmd );
    }

    #Condicional para detener el movimiento continuo Vertical
    elsif ($preset == 9)

        {
                my $cmd = "decoder_control.cgi?command=27";
                $self->sendCmd( $cmd );
        }

    #Condicional para movimiento horizontal continuo
        elsif ($preset == 10)

        {
                my $cmd = "decoder_control.cgi?command=28";
                $self->sendCmd( $cmd );
        }

    #Condicional para detener el movimiento continuo Horizontal
    elsif ($preset == 11)

        {
                my $cmd = "decoder_control.cgi?command=29";
                $self->sendCmd( $cmd );
        }

}

1;

__END__
#FIN
```