ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE VIDEO-VIGILANCIA INALÁMBRICO PARA LA CIUDAD DE CAYAMBE

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

JOSÉ LUIS MONTEROS MEJÍA
chelui101@hotmail.com

DIRECTOR: ING. MIGUEL ÁNGEL HINOJOSA RAZA, MSc.
miguel.hinojosa@epn.edu.ec

Quito, Junio 2015

DECLARACIÓN

Yo José Luis Monteros Mejía, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

JOSÉ LUIS MONTEROS MEJÍA

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por José Luis Monteros Mejía, bajo mi supervisión.

Ing. Miguel Hinojosa, MSc.

DIRECTOR

AGRADECIMIENTOS

A Dios por sobre todas las cosas, gracias a él estoy culminando una de las metas más importantes en mi vida.

A mi Virgencita del Quinche, quien se me supo cuidar y proteger todo este tiempo.

A mis padres por su apoyo incondicional y por no perder las esperanzas depositadas en mí.

A mi esposa, quien llego a mi vida para enrumbarme, con sus consejos y apoyo fue un gran baluarte en la consecución de este Proyecto.

A mis hermanas quienes siempre estuvieron pendientes del avance de mi Proyecto.

A mi director de Proyecto de Titulación, el Ing. Miguel Hinojosa, muchísimas gracias por su gran ayuda, paciencia, comprensión y sobre todo por su gran disponibilidad de tiempo.

Y a todas esas personas que de una u otra manera me han brindado su ayuda desinteresadamente. Enumerarlos sería casi imposible. Muchísimas gracias a todos.

DEDICATORIA

Quiero dedicar esta tesis a mi madre, que siempre fue su sueño verme graduado de la mejor universidad del Ecuador, la gloriosa Escuela Politécnica Nacional. Para ti madrecita, ¡Tu sueño está cumplido...!

También quiero dedicar esta tesis a mis hijas, espero que este trabajo sirva de ejemplo y motivación en su vida. Quiero que sepan que los sueños se pueden hacer realidad siempre que se los persiga con ahínco y dedicación, que no existen sueños imposibles de alcanzar, todo lo que uno se propone se lo puede conseguir.

José Luis

CONTENIDO

ÍNDICE DE TABLAS

CAPÍTULO 1. Fundamentos teóricos

CAPÍTULO 2. Análisis de requerimientos

CAPÍTULO 3. Diseño del sistema de video-vigilancia y determinación de costos referenciales

ÍNDICE DE FIGURAS

CAPÍTULO 1. Fundamentos teóricos

CAPÍTULO 2. Análisis de requerimientos

CAPÍTULO 3. Diseño del sistema de video-vigilancia y determinación de costos referenciales

CAPÍTULO 4. Implementación del prototipo del sistema, pruebas y resultados

ÍNDICE DE ANEXOS

PRESENTACIÓN

En los últimos años la inseguridad ha logrado ocupar un gran lugar en la ciudad de Cayambe debido a su crecimiento y al desarrollo presentado en los últimos tiempos. El presente Proyecto de Titulación tiene como objetivo ayudar a reducir el índice delictivo existente en esta ciudad por medio de un sistema de video-vigilancia, el cual, presentará imágenes en tiempo real de lo que sucede en los principales lugares de la ciudad. El sistema de video-vigilancia planteado, puede llegar a ser una gran herramienta para la Policía Comunitaria del lugar, en la realización de sus tareas cotidianas.

Este sistema está diseñado para implementarlo sobre una red inalámbrica de datos en malla (WMN) y de esta manera aprovechar las ventajas que presenta esta tecnología. En el caso de implementación del sistema de video-vigilancia, no sería necesario hacer contratos para el uso de frecuencias, debido a que está desarrollado para operar en la banda de frecuencia libre de 5 GHz.

RESUMEN

El presente proyecto trata del diseño de un sistema de video-vigilancia inalámbrico para el sector urbano de la ciudad de Cayambe, complementado con la implementación de un prototipo, para un mejor entendimiento del funcionamiento y las ventajas que presenta el sistema. A continuación se describirán brevemente el contenido de los capítulos que conforman este Proyecto de Titulación.

En el primer capítulo se hace una introducción a las redes inalámbricas de datos y su clasificación; también se explica lo que son los sistemas de video-vigilancia y los elementos que lo conforman.

En el capítulo dos se describe la situación actual de la ciudad de Cayambe, teniendo en cuenta aspectos como: economía, población y ubicación. Se realiza un análisis de mercado por medio de encuestas y entrevista para poder medir el nivel de aceptación de la población con la posible implementación del sistema.

En el capítulo tres se realiza el diseño del sistema de video-vigilancia, tomando en cuenta aspectos como: tipo de red a utilizar, tráfico generado por el sistema, dimensionamiento del servidor de video, sistema de gestión y administración y se define los lugares para la ubicación de las cámaras de vigilancia. Se presenta además una simulación de la red y el costo referencial en caso de implementación del sistema.

En el capítulo cuatro se presenta la implementación de un prototipo del sistema de video-vigilancia, con el que se pretende realizar pruebas del funcionamiento del sistema. Se presentan los equipos utilizados y las configuraciones realizadas.

Finalmente en el capítulo cinco se presenta las conclusiones y recomendaciones a las que se llegó, durante el desarrollo de este Proyecto de Titulación.

CAPÍTULO 1
FUNDAMENTOS TEÓRICOS

1.1 REDES INALÁMBRICAS [1] [2] [3] [4] [6] [8] [10] [11] [12] [14] [15] [16] [19]

Se conoce como comunicación inalámbrica a aquella que se produce sin el uso de cables de interconexión entre los participantes; por ejemplo, la comunicación mediante un teléfono móvil es inalámbrica, mientras que la comunicación con un teléfono fijo tradicional no lo es. En la actualidad, existen muchas tecnologías que brindan sus servicios mediante comunicaciones inalámbricas.

Las redes inalámbricas cada vez presentan mayores seguridades y mejores velocidades de transmisión, esto acompañado de sus bajos precios de implementación ha generado que rápidamente ocupen un gran lugar en el mercado, siendo esto aprovechado por empresas y personas particulares.

1.1.1 TIPOS DE REDES INALÁMBRICAS

Las redes inalámbricas pueden clasificarse de diferentes maneras dependiendo del criterio al que se atienda. En esta sección se las clasificará de acuerdo a su alcance o cobertura, tal como se muestra en la Figura 1.1.

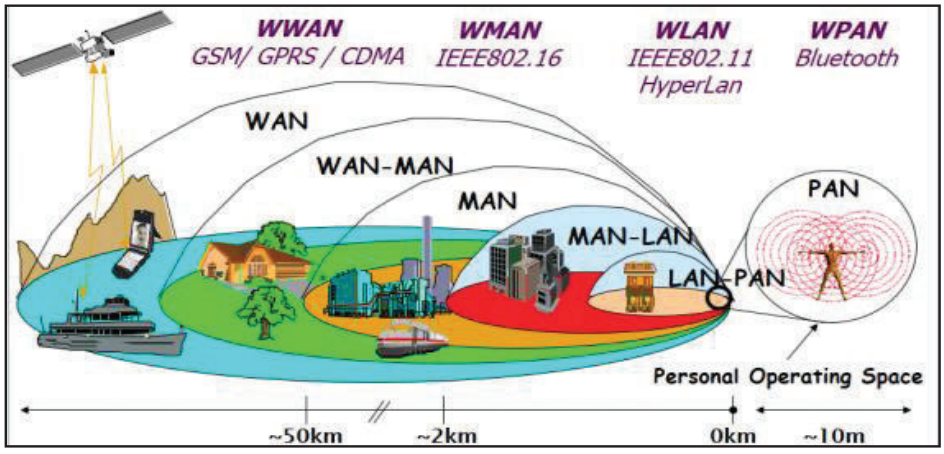


Figura 1.1 Tipos de redes inalámbricas [17]

1.1.1.1 Wireless Body Area Network (WBAN)

Las redes inalámbricas de área corporal son utilizadas en el control de los parámetros vitales del cuerpo y de sus movimientos (ver Figura 1. 2). Son redes que aún se encuentran en su etapa inicial de desarrollo y que tendrán un gran campo de acción, sobre todo en el campo médico ya que permitirán monitorear de manera constante a los pacientes sin que se encuentren conectados por medio de cables.

El funcionamiento de este tipo de redes consiste en la implantación de dispositivos de baja potencia en el cuerpo, estos dispositivos se comunicarán de manera inalámbrica con una estación central o estación base en donde se almacenará los parámetros vitales del paciente. Como ejemplos de este tipo de dispositivos tenemos los auriculares, sensores, micrófonos, etc.

La cobertura de este tipo de redes es de 1 a 2 m. La banda de frecuencia que utiliza para la transmisión de información es la MICS (*Medical Implantable Communication Service),* cuyo intervalo de frecuencia es de 402 a 405 MHz.

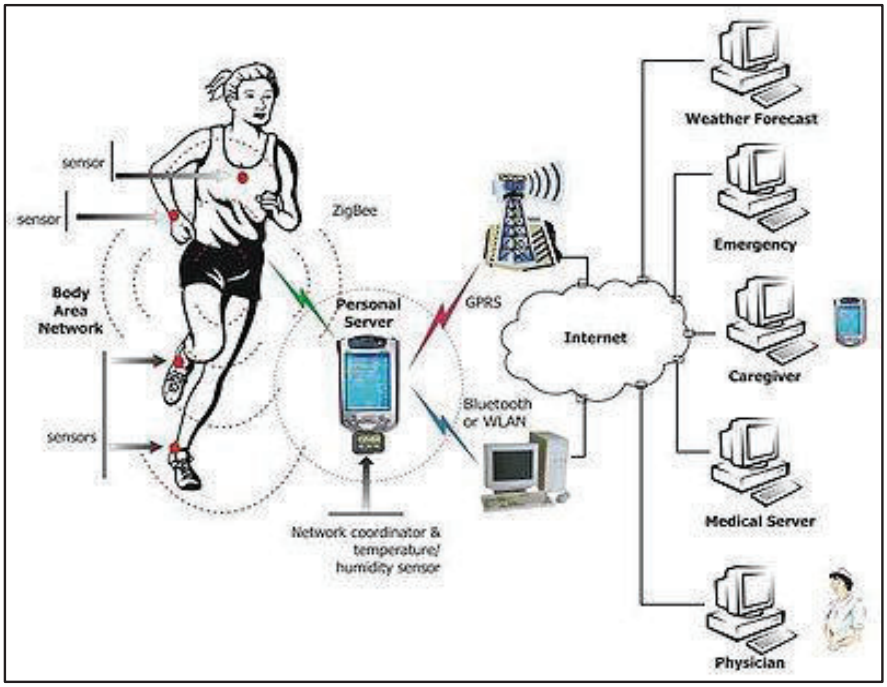


Figura 1.2 Ejemplo de redes WBAN [3]

1.1.1.2 Wireless Personal Area Network (WPAN)

Las redes inalámbricas de área personal se encuentran definidas en el estándar IEEE[1] 802.15 y pueden cubrir distancias inferiores a 10 metros. Estas soluciones están pensadas para la interconexión de dispositivos de usuario, por ejemplo: conectar la impresora con la computadora personal, o con el teléfono celular. Las principales tecnologías que se encuentran en esta categoría se citan a continuación:

- Bluetooth
- Zigbee
- IrDA
- DECT
- WiBree
- UWB

Las WPAN fueron creadas para un uso personal, su mayor utilización está dentro de los hogares, sin embargo hoy en día también se las emplea para el monitoreo de áreas geográficas y en el control de procesos industriales.

1.1.1.2.1 Bluetooth

Es la tecnología más conocida dentro de las WPAN. Está diseñada para dispositivos de bajo consumo que requieren un corto alcance de emisión.

Este tipo de redes posibilitan la transmisión de voz y datos, haciendo empleo de la banda de frecuencia ISM (*Industrial, Scientific and Medical*) de 2.4 GHz. El estándar en el que se encuentra definido es el IEEE 802.15.1.

[1] IEEE.- Institute of Electrical and Electronics Engineers, asociación técnica mundial formada por profesionales de las nuevas tecnologías, dedicados a la estandarización de las mismas.

El principal objetivo de esta tecnología, es el de reemplazar los cables que comunican los dispositivos del hogar por medio de un enlace inalámbrico de corto alcance (ver Figura 1.3).

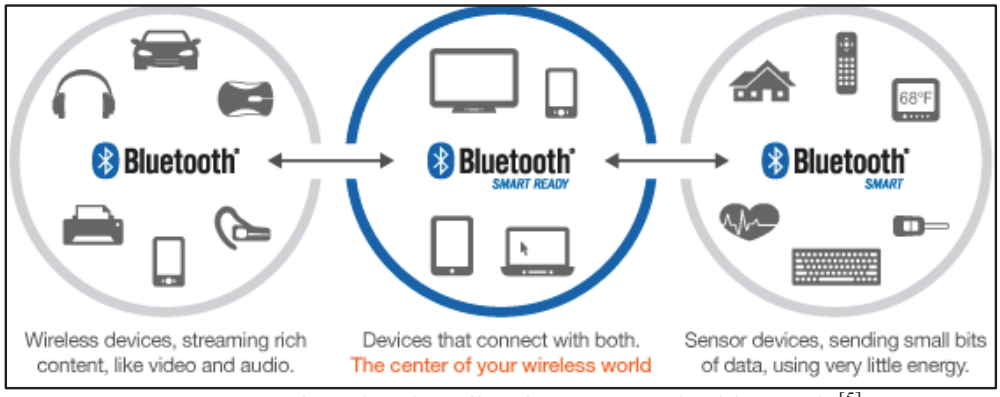


Figura 1.3 Ejemplos de aplicaciones con redes bluetooth [5]

1.1.1.2.2 Zigbee

Zigbee es una tecnología inalámbrica diseñada para hacer frente a las necesidades de redes de bajo costo, sensores inalámbricos de baja potencia y redes de control.

El objetivo principal de esta tecnología son las comunicaciones seguras empleando una baja tasa de envío de datos y bajo consumo de energía. Su desarrollo está basado en el estándar IEEE 802.15.4 y utilizan la banda de frecuencia ISM para la comunicación entre sus dispositivos.

Los campos de aplicación en los cuales se espera tenga éxito son: la automatización de edificios, el cuidado de la salud, la automatización del hogar, energía inteligente, servicios de telecomunicaciones y las compras automáticas.

1.1.1.2.3 IrDA (Infrared Data Association)

Conocida también como infrarrojos. Los sistemas de comunicaciones mediante tecnología infrarroja se basan en la emisión y recepción de haces de luz infrarroja.

La luz infrarroja es un tipo de radiación electromagnética que es invisible para el ojo humano.
Los dispositivos que utilizan esta tecnología poseen emisores/receptores de ondas infrarrojas. Estos dispositivos tienen alcances muy cortos, alrededor de 1 m de distancia, siendo ésta, una de sus principales desventajas.

Entre las principales aplicaciones de esta tecnología, se puede citar, que es muy utilizada para el manejo remoto de los electrodomésticos del hogar (ver Figura 1.4).

Figura 1.4 Ejemplo de aplicaciones con redes Infrarrojas [7]

1.1.1.2.4 DECT (Digital Enhanced Cordless Telecommunications)

El significado de sus siglas en español sería: Telecomunicaciones Inalámbricas Mejoradas Digitalmente. Es un estándar de la ETSI[2] para teléfonos inalámbricos digitales conectados a una base. Trabaja en la banda de frecuencia de 1.9 GHz. Y permite tener alcances de hasta 300 m.

Es un estándar orientado a la transmisión de voz digital. Se utiliza principalmente en sistemas telefónicos del hogar o empresa, donde se puede tener múltiples terminales inalámbricos conectados a una misma base (ver Figura 1.5).

[2] ETSI (European Telecommunications Standards Institute). - Organismo encargado en el desarrollo de normas de aplicación mundial para la Información y Tecnologías de la Comunicación.

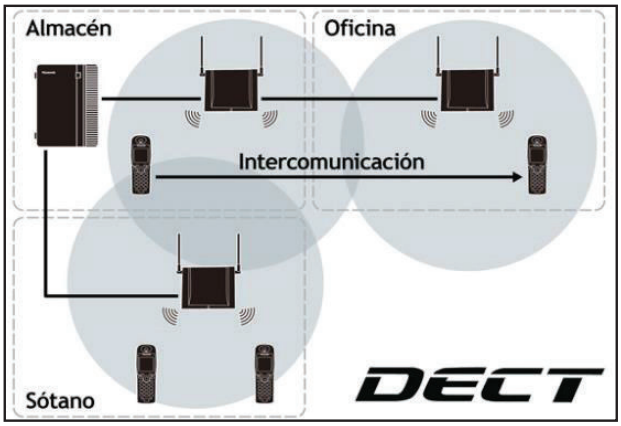


Figura 1.5 Ejemplo de aplicaciones con redes DECT [8]

1.1.1.2.5 Wibree

Es una tecnología digital de radio interoperable para pequeños dispositivos (ver Figura 1.6). Se conoce como la versión de baja potencia de la tecnología Bluetooth.

Esta tecnología ofrece comunicación entre dispositivos móviles o computadores que soporten la tecnología Bluetooth y otros dispositivos más pequeños. Opera en la banda de frecuencia de 2.4 GHz. y soporta una tasa de transferencia de 1 Mbps.

Adicional a esto, está diseñada para que funcione con poca energía.

Figura 1.6 Ejemplo de aplicaciones con redes Wibree [9]

1.1.1.2.6 UWB (Ultra Wide Band)

Permite transmitir grandes paquetes de información (480 Mbps) en distancias cortas (menores a 10m.). Su funcionamiento se basa en la emisión de pulsos de muy corta duración que ocupan un gran ancho de banda instantáneo, por lo que resulta difícil determinar una frecuencia central de RF.

1.1.1.3 Wireless Local Area Network (WLAN)

Las redes de área local inalámbricas fueron pensadas en un principio para crear un entorno de red local en el que todos los dispositivos que se encuentren en un edificio o grupo de edificios puedan comunicarse entre sí.

Este tipo de redes constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones de banda ancha debido a que trabajan en bandas libres y pueden alcanzar una cobertura que se encuentre en el orden de los metros.

Originalmente las WLAN fueron pensadas para las empresas, sin embargo, hoy en día es muy común ver su aplicación en escenarios tanto privados como públicos, escenarios como: zonas industriales, entorno de grandes redes corporativas, campus industriales, hospitales, ciber cafés, hoteles, aeropuertos, medios públicos de transporte, entornos rurales, video-vigilancia, etc.

Entre las principales tecnologías WLAN tenemos:

- Wi-Fi
- HiperLAN

1.1.1.3.1 Wi-Fi

Wi-Fi es un conjunto de estándares para redes inalámbricas que basan su funcionamiento en las especificaciones IEEE 802.11. Mediante el empleo de esta

tecnología se pueden ampliar la cobertura de una red de datos cableada de manera inalámbrica, tal como se muestra en la Figura 1.7.

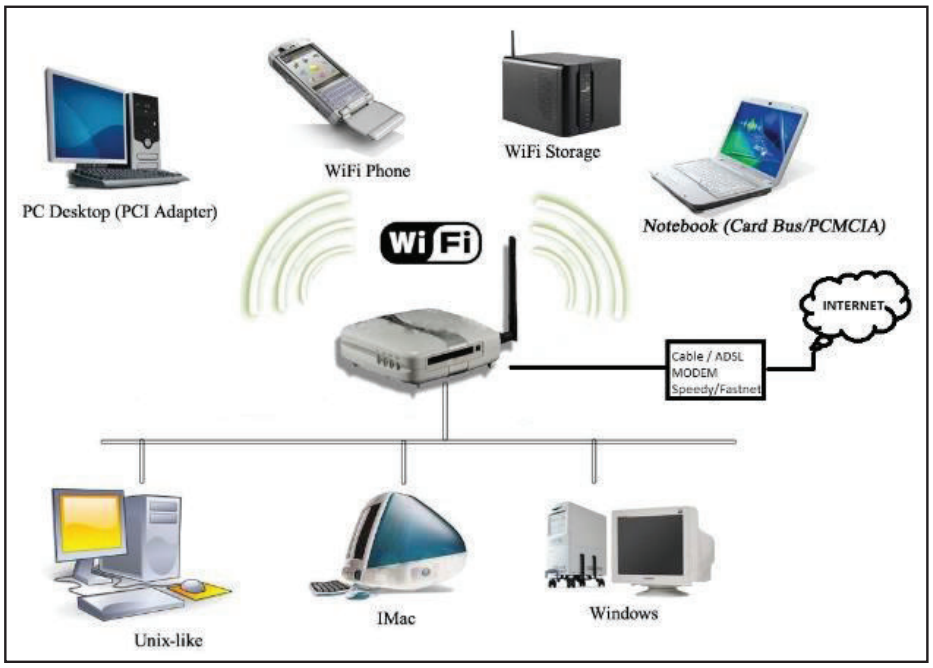


Figura 1.7 Ejemplo de aplicaciones con redes Wi-Fi [13]

Erróneamente se cree que el significado de Wi-Fi es Wireless Fidelity, sin embargo Wi-Fi no es un acrónimo, sus siglas no tienen significado, este nombre surgió como una manera de ser más fácilmente difundida en el mercado.

1.1.1.3.2 HiperLAN (High Performance Radio LAN)

Es un estándar creado por la ETSI en 1997 con el objetivo de desarrollar velocidades de transferencia mayores a los del estándar IEEE 802.11. El objetivo de esta tecnología, es conseguir WLANs de alta capacidad, con calidad de servicio y baja movilidad, en un entorno que no supere los 50 m. (ver Figura 1.8).

Este estándar trabaja en la banda de frecuencia de 5 GHz. y alcanza velocidades de transmisión de datos de 54 Mbps.

HiperLAN es compatible con el estándar IEEE 802.11a.

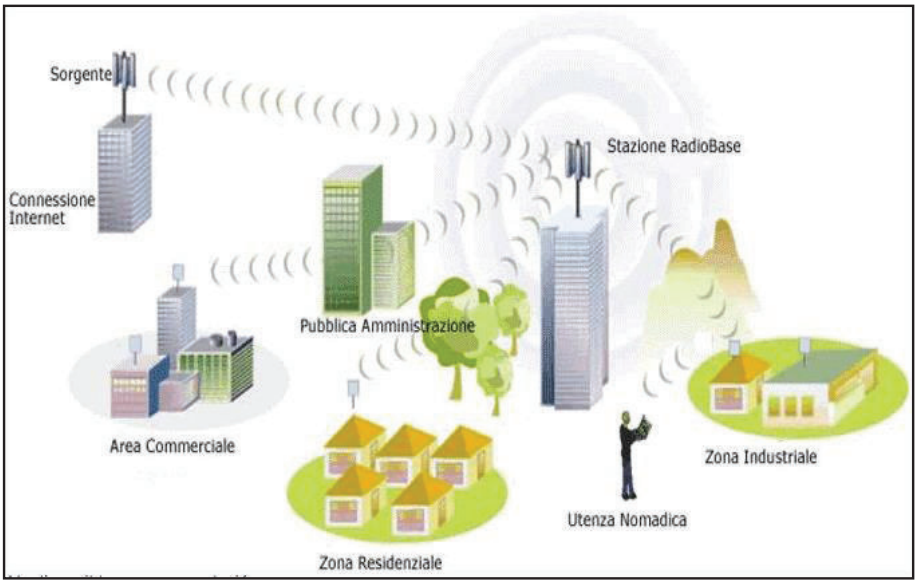


Figura 1.8 Ejemplo de aplicaciones con redes HiperLAN [14]

1.1.1.4 Wireless Metropolitan Area Network (WMAN)

Las redes inalámbricas de área metropolitana fueron creadas pensando en la interconexión de diferentes localidades dentro de un área metropolitana, es muy común tratarlas como redes WLAN extensas o redes WWAN de menor tamaño.

Estas redes pueden alcanzar coberturas que están en el orden de los kilómetros. Entre las principales tecnologías WMAN se tiene:

- WiMax
- WiBro

1.1.1.4.1 WiMax (Worldwide Interoperability for Microwave Access)

Es un estándar de transmisión inalámbrica de datos que se encuentra definida en el estándar IEEE 802.16. Permite la recepción de datos por microondas y retrasmite por ondas de radio. Proporciona accesos concurrentes en áreas de hasta 50 Km de radio. Es compatible con estándares anteriores como el IEEE 802.11 y funciona en un rango de frecuencias que van desde: 2 GHz a 66 GHz (dependiendo de la versión).

La característica principal de una red WiMax es su gran ancho de banda que puede ser aprovechado para el transporte de información, alcanzando velocidades de transmisión de 70 Mbps.

1.1.1.4.2 WiBro (Wireless Broadband Technology)

Es una tecnología de banda ancha de Internet desarrollada por la empresa de Telecomunicaciones Coreana, con la finalidad de proporcionar una solución a Internet de alta velocidad para los consumidores locales, con calidad de servicio.
Esta tecnología se basa en el estándar 802.16e que se conoce comúnmente como WiMax móvil y puede soportar usuarios viajando a una velocidad de 120 Km/h con velocidades de hasta 50 Mbps y un alcance de hasta 5 Km.

1.1.1.5 Wireless Wide Area Network (WWAN)

Las redes inalámbricas de área amplia tienen la particularidad de que su cobertura es la mayor de todas las tecnologías de redes inalámbricas, pueden abarcar áreas geográficas tan extensas como: ciudades o incluso países.

Entre las principales tecnologías WWAN se tiene:

- Redes de telefonía celular
- Redes satelitales

1.1.1.5.1 Redes de telefonía celular

La telefonía celular ha evolucionado muy rápidamente. Al comienzo los teléfonos celulares se los empleaban únicamente para realizar llamadas de voz, ahora se los puede utilizar para navegar en internet, descargar archivos, ver películas, etc. (ver Figura 1.9). Todo esto debido a que cada vez se tiene dispositivos más sofisticados y a la implementación de nuevos estándares tecnológicos.

Figura 1.9 Ejemplo de aplicaciones con redes de telefonía celular [18]

1.1.1.5.2 Redes Satelitales

Son aquellas que necesitan de satélites artificiales para su transmisión. Los satélites enlazan una o más estaciones base para la emisión y recepción de datos (ver Figura 1.10). A estas estaciones se las conoce como estaciones terrestres.

La mayoría de comunicaciones satelitales se realizan en la banda de 2.5 a 22 GHz.

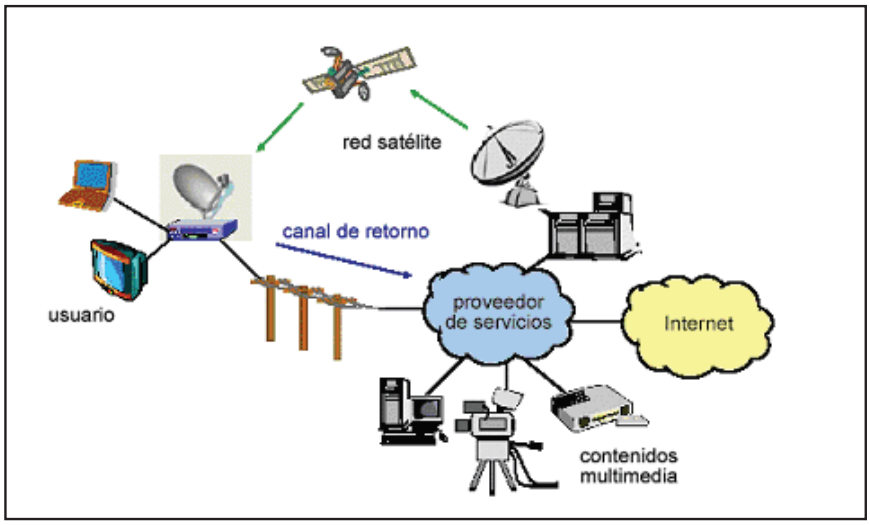


Figura 1.10 Ejemplo de redes satelitales [19]

1.1.2 VENTAJAS DE LAS REDES INALÁMBRICAS

El empleo de redes inalámbricas aporta una serie de ventajas que hacen que sean muy atractivas para los usuarios. Entre las principales ventajas se puede citar las siguientes:

- Facilidad de instalación: debido a que no es necesario tender cables para su conexión, de esta manera no se alteraría el aspecto de inmuebles y edificios.
- Bajo costo de implementación: Al no necesitar tender cables para su conexión, el costo de implementación baja considerablemente si se las compara con sistemas cableados, permitiendo de esta manera estar al alcance de cualquier familia, empresa u organización.
- Flexibilidad: Cualquier dispositivo informático podrá acceder a una red inalámbrica siempre y cuando se encuentre en su zona de cobertura y tenga los permisos de acceso adecuados.
- Movilidad: La tendencia actual es poder intercambiar datos sin estar atado a un cable para poder hacerlo. Las redes de datos inalámbricas permiten el intercambio de información con equipos en movimiento.
- Escalabilidad: Las redes inalámbricas permiten ajustar su tamaño a nuestras necesidades después de haber sido creadas, lo único que se debe hacer es: añadir o quitar puntos de acceso.
- Uso de bandas de frecuencia libres: La mayoría de estándares inalámbricos trabajan en bandas de frecuencia libres lo que abarata los costos de implementación.
- Altas tasas de transmisión: Actualmente las redes inalámbricas alcanzan velocidades de trasmisión de datos que están en el orden de los Gbps.

1.1.3 DESVENTAJAS DE LAS REDES INALÁMBRICAS

Como en toda tecnología, es inevitable que existan desventajas. Entre las principales se pueden citar las siguientes:

- Señales inestables: La señal puede llegar a ser inestable debido a factores externos como el ruido o a condiciones climáticas desfavorables como vientos o lluvia, dando como resultado caídas en la señal.
- Interferencias: Se pueden producir interferencias en la transición de datos cuando equipos de línea blanca destinados para su uso en el hogar o redes de datos cercanas, utilizan la misma banda de frecuencia de los dispositivos que se utilizan para la transmisión de datos en una red.
- Seguridad: Este es uno de los puntos más críticos en redes inalámbricas, sin embargo, con el continuo aparecimiento de nuevas tecnologías, se pueden tener redes inalámbricas cada vez más seguras.

1.2 EL ESPECTRO ELECTROMAGNÉTICO [2] [20]

El espectro electromagnético clasifica al conjunto de ondas existentes de acuerdo a su frecuencia y a la magnitud de su longitud de onda, tal como puede verse en la Figura 1.11. Las ondas de radiofrecuencia (mayor longitud de onda) están compuestas por: las microondas, los rayos infrarrojos, la luz visible y los rayos ultravioleta. Las ondas electromagnéticas (menor longitud de onda) se encuentran compuestas por: rayos x y los rayos gamma.

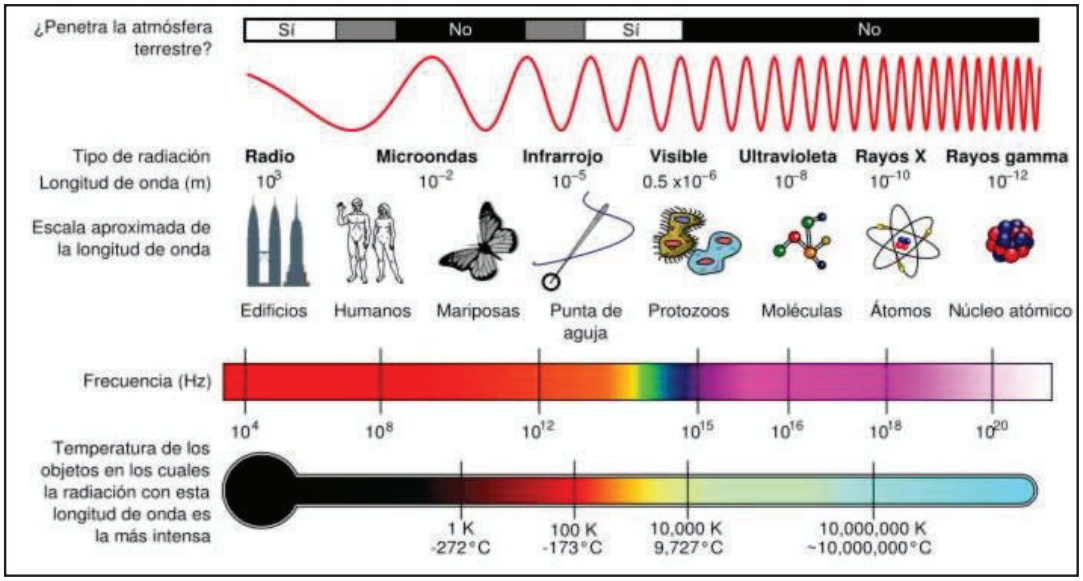


Figura 1.11 Espectro Electromagnético [20]

1.2.1 BANDAS DEL ESPECTRO ELECTROMAGNÉTICO

Se conoce de esta manera a los intervalos de frecuencia que conforman el espectro electromagnético y que están asignados a diferentes usos dentro de las radiocomunicaciones. El uso de las bandas de frecuencia está regulado por la UIT (*Universal Institute of Technology*) y esto puede variar dependiendo de cada país.

Con la finalidad de evitar interferencias y hacer un uso eficiente del espectro electromagnético, se colocan servicios similares en las mismas bandas. Cada banda tiene un plan de frecuencia que determina su uso y compartición (ver Tabla 1.1).

NOMBRE	ABREVIATURA INGLESA	BANDA ITU	FRECUENCIAS	LONGITUD DE ONDA
			Inferior a 3 Hz	>100.000 Km
Extra baja frecuencia	ELF	1	3-30 Hz	100.000-10.000Km
Súper baja frecuencia	SLF	2	30-300 Hz	10.000-1000Km
Ultra baja frecuencia	ULF	3	300-3000 Hz	1000-100 Km
Muy baja frecuencia	VLF	4	3-30 KHz	100-10 Km
Baja frecuencia	LF	5	30-300 KHz	10-1 Km
Mediana frecuencia	MF	6	300-3000 KHz	1 Km-100 m
Alta frecuencia	HF	7	3-30 MHz	100-10 m
Muy alta frecuencia	VHF	8	30-300 MHz	10-1 m
Ultra alta frecuencia	UHF	9	300-3000 MHz	1m - 100 mm
Súper alta frecuencia	SHF	10	3-30 GHz	100-10 mm
Extra alta frecuencia	EHF	11	30-300 GHz	10-1 mm
			Por encima de los 300 GHz	<1 mm

Tabla 1.1 Bandas de frecuencia [20]

A las frecuencias que se encuentran en el rango entre: 1 GHz y 300 GHz se las conoce como microondas. Estas frecuencias abarcan una parte del rango de UHF y todo el rango de SHF y EHF (ver Tabla 1.2).

BANDA	P	L	S	C	X	Ku	K	Ka	Q	U	V	E	W	F	D
INICIO (GHz)	0,2	1	2	4	8	12	18	26,5	30	40	50	60	75	90	110
FINAL (GHz)	1	2	4	8	12	18	26,5	40	50	60	75	90	110	140	170

Tabla 1.2 Bandas de frecuencia de Microondas [20]

1.2.2 BANDA ISM (*Industrial, Scientific, Medical*)

Las bandas ISM se encuentran reservadas internacionalmente por la UIT para un uso no comercial. Su utilización está abierta para todo tipo de público.

En la Figura 1.12 se muestra los rangos de frecuencia que pertenecen a esta banda.

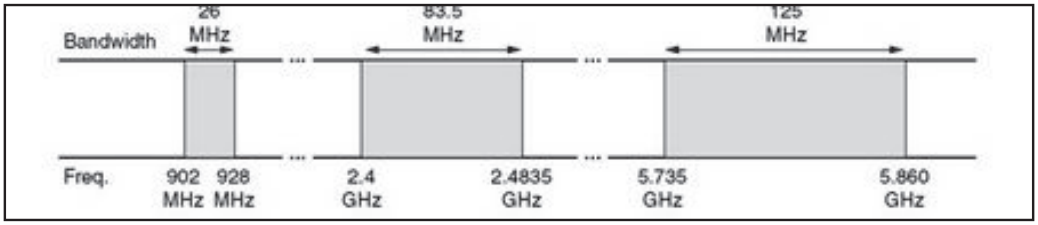


Figura 1.12 Banda ISM [21]

1.3 SISTEMAS DE VIDEO-VIGILANCIA [22] [23] [24] [28] [30] [31] [32] [34] [35] [36] [37]

Los sistemas de video-vigilancia han ido evolucionando de la mano con la tecnología. En un principio se tenían sistemas analógicos en los cuales: la video-vigilancia se podía realizar únicamente de manera local, sin embargo hoy en día es posible hacerla de manera remota, incluso mediante el empleo de teléfonos y demás dispositivos móviles.

Los sistemas de video-vigilancia tienen un gran campo de acción y pueden ser utilizados en aplicaciones como: control del personal de una empresa u oficina, monitoreo del tráfico de una ciudad, vigilancia en entidades bancarias, espionaje, vigilancia de áreas protegidas, supervisión de procesos industriales, etc.

En épocas pasadas estos sistemas eran implementados únicamente por empresas y oficinas. Ahora, gracias a su facilidad de implementación y bajo costo, su utilidad puede ser aprovechada, incluso por personas particulares que requieran vigilar lo que sucede en sus hogares.

En la actualidad se tienen sistemas de video-vigilancia que combinan los beneficios de los sistemas analógicos, con las ventajas que ofrecen las redes basadas en IP[3], comúnmente conocidos como video-vigilancia IP. Mediante el empleo de estos sistemas, se puede obtener una mejor calidad de imágenes, personalizar la grabación de eventos, enviar alertas, incluso se lo puede hacer trabajar de manera conjunta con otros sistemas. Su costo de implementación resulta económico debido a que se puede aprovechar una red de datos previamente instalada.

Los componentes básicos que conforman un sistema de video-vigilancia IP se los puede observar en la Figura 1.13 y se los cita a continuación:

- Cámaras IP.
- Codificador de Video (únicamente cuando es necesario conectar cámaras analógicas al sistema).
- Medios de transmisión.
- Dispositivos de Almacenamiento de video.
- Sistemas de Gestión y Administración de video.

[3] IP.- Internet Protocol, es un protocolo no orientado a conexión usado tanto en el origen, como en el destino, para la comunicación de datos por medio de una red de paquetes conmutados

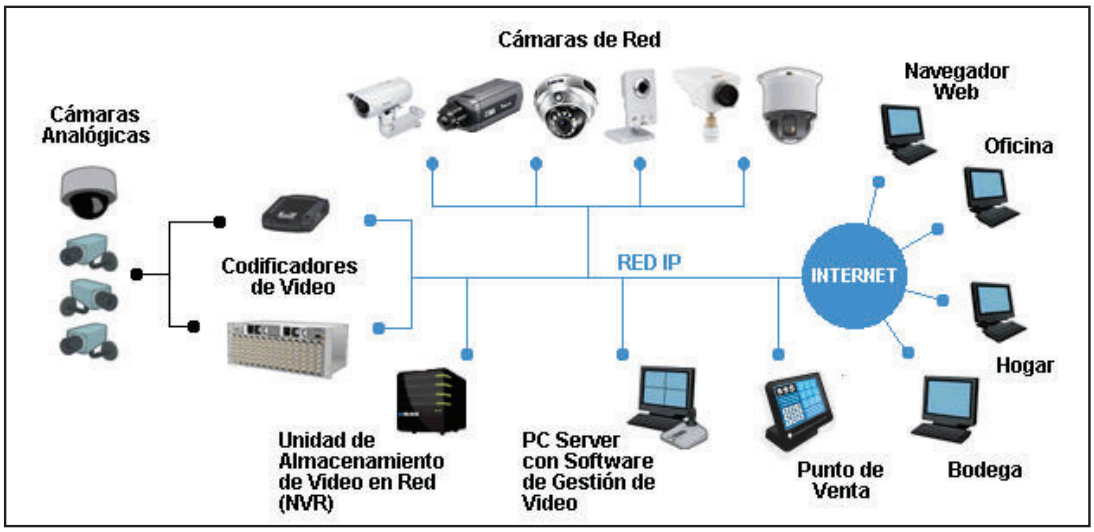


Figura 1.13 Componentes de un sistema de video-vigilancia IP [23]

1.3.1 CÁMARAS IP

Son dispositivos que captan y transmiten señales de audio/video a través de una red de datos basada en IP (alámbrica o inalámbrica), hasta un dispositivo de almacenamiento de video desde el cual se puede gestionar y administrar la información.

Al igual que un computador, a las cámaras IP se les debe asignar una dirección IP para su conexión a la red.

En muchas ocasiones será necesario vigilar lugares donde la iluminación sea escasa, para solucionar este problema, las cámaras modernas incorporan leds, luces infrarrojas o incluso focos térmicos.

A continuación se dará a conocer algunos conceptos que deberán ser tomados en cuenta al momento de elegir una cámara de vigilancia:

- Sensibilidad: Indica la intensidad de luz necesaria para que una cámara pueda funcionar correctamente en condiciones de escasa de iluminación,

su unidad de medida es el Lux. A mayor sensibilidad el valor de Lux será menor. En la Tabla 1.3 se muestra algunos valores de iluminancia.

ILUMINANCIA [LUX]	CONDICIÓN DE ILUMINACIÓN
100,000	Luz solar intensa
10,00	Luz plena de día
500	Luz de oficina
100	Habitación con poca luz

Tabla 1.3 Valores de Iluminancia [23]

- Resolución: Viene dada por la cantidad de pixeles horizontales y verticales que tenga, mientras mayor sea el número de pixeles, mayor resolución tendrá la cámara. Actualmente existen cámaras IP con resolución megapíxel, lo que ha permitido obtener imágenes cada vez más claras y visualización de áreas más grandes. En la Tabla 1.4 se presentan resoluciones megapíxel con sus respectivos formatos de visualización.

FORMATO DE VISUALIZACIÓN	MEGAPÍXELES	PÍXELES
SXGA	1,3	1280x1024
SXGA + (EXGA)	1,4	1400x1050
UXGA	1,9	1600x1200
WUXGA	2,3	1920x1200
QXGA	3,1	2048x1536
WQXGA	4,1	2560x1600
QSXGA	5,2	2560x2048

Tabla 1.4 Resoluciones Megapíxel [23]

- Conmutación: Las cámaras modernas deben funcionar tanto en el día como en la noche, por esta razón, utilizan sistemas que las hacen funcionar a color durante el día y permiten conmutar o cambiar a blanco y negro en la noche, o en lugares con poca iluminación, esto con la finalidad de conseguir mayor sensibilidad y resolución. Simultáneamente, pueden activar iluminación adicional mediante el empleo de luces infrarrojas.

- Compensación de contraluz: La compensación de contraluz evita imágenes oscuras en escenas con poca luz, e imágenes excesivamente claras, cuando la escena tiene mucha luminosidad.
- Ajuste de blancos: La tonalidad de los colores de una imagen depende principalmente del tipo de luz ambiente. Las cámaras necesitan tener una referencia de cuál es el color "blanco", para presentar una tonalidad correcta en el resto de colores.
- Otras Características: Dependiendo del modelo de la cámara, puede incluir características como: entradas de audio, máscaras de privacidad (permite ocultar determinadas áreas de un escena), insertado de texto, contraluz programable por áreas (permite utilizar diferentes tipos de exposiciones para distintos objetos en una escena), ajustes en la escala de colores, etc.

1.3.1.1 Componentes de una cámara IP

Las partes o componentes básicos de una cámara IP se los puede apreciar en la Figura 1.14 y son las siguientes:

- Lente
- Sensor de imagen
- DSP (*Digital Signal Processor*)
- CPU (*Central Processing Unit*)
- Etapa de compresión
- Tarjeta Ethernet

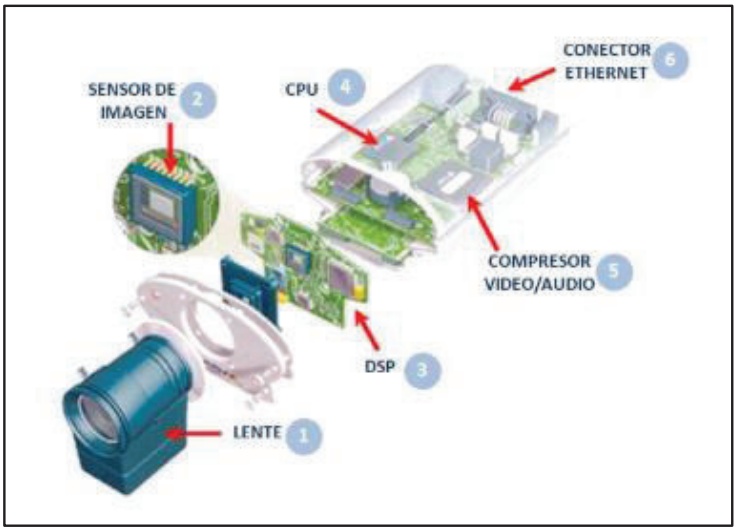


Figura 1.14 Componentes básicos de una cámara IP [24]

1.3.1.1.1 Lente u Objetivo

Las lentes son los ojos de una cámara, éstas determinan la escena que se muestra en un monitor (en función de la distancia focal) y controlan la cantidad de luz que llega al sensor de imagen (Iris).

La distancia focal es la distancia entre el centro de la lente y el sensor de la imagen (ver Figura 1.15). Los rayos de objetos distantes se condensan internamente en la lente, en un punto común en el eje óptico, a ese punto se lo denomina punto focal. Las lentes con una distancia focal pequeña tienen un ángulo de apertura grande, esto permite observar zonas extensas, lo contrario sucede en lentes con distancia focal grande, en donde, se tiene un ángulo de apertura pequeño y esto implica poder visualizar un menor campo de visión. La distancia focal se mide en milímetros, una distancia de 50 mm equivaldría al ángulo de visión humano.

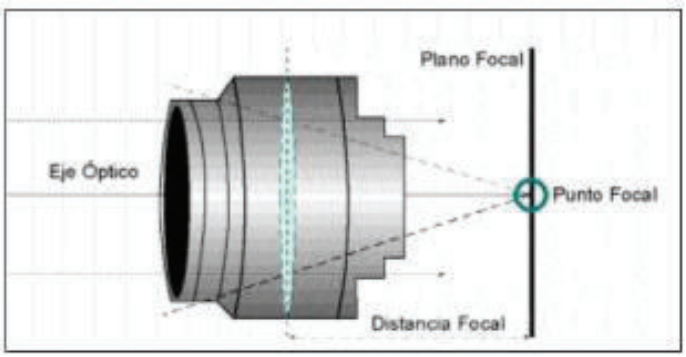


Figura 1.15 Distancia focal de una lente [24]

Según la distancia focal, las lentes pueden se clasificarse en:

- Lentes fijas: Son el tipo más simple de lente. Para encontrar el valor fijo de una lente se requiere de un cálculo preciso. Este cálculo se basa en el tamaño deseado del área de visualización y la distancia a la cámara.
- Lentes vari focales: Conocidas también como lentes de distancia focal variable, estas lentes permiten obtener un ajuste más preciso de la escena. Permiten definir prácticamente cualquier ángulo de visión, lo que aumenta los beneficios de la vigilancia.
- Zoom motorizadas: Se puede ajustar el valor de la distancia focal de manera remota, lo que ofrece una mayor funcionalidad. Una única lente puede ser utilizada para ver una zona amplia y si detecta un intruso, realizar un zoom para capturar detalles faciales.

El Iris controla la cantidad de luz que incide sobre la cara del sensor de imagen. La medida de apertura del iris se determina por el valor de f o f-stops[4]. Un número f-stop menor, producirá por lo general una mejor calidad de imagen. En la Figura 1.16 se puede observar diferentes medidas de aperturas del iris.

[4] F-stop.- Define la cantidad de luz que puede pasar por un lente. Resulta de la relación entre la longitud focal del lente y el diámetro de apertura o diámetro del iris.

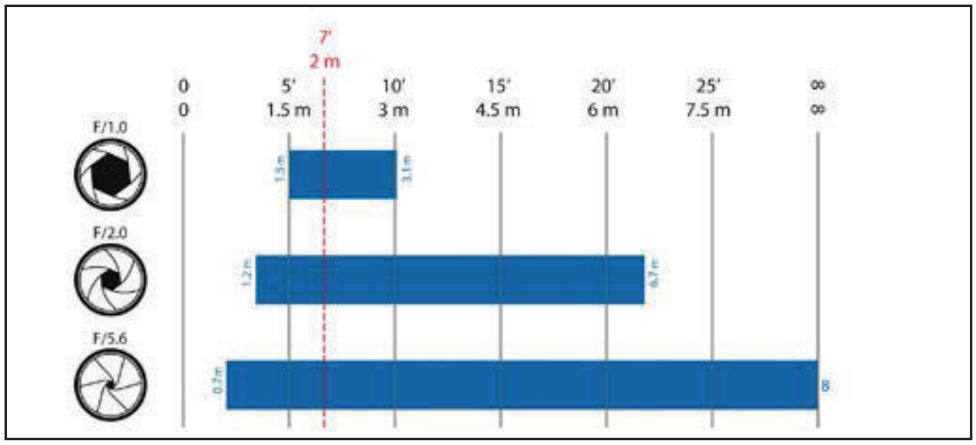


Figura 1.16 Medidas de apertura del Iris [29]

1.3.1.1.2 Sensor de imagen

Cuando la luz atraviesa una lente, ésta se enfoca en el sensor de imagen. Un sensor de imagen tiene como función principal transformar la imagen óptica creada por la lente en una serie de señales eléctricas que darán lugar a la imagen digital. Está compuesto por una matriz de millones de diminutas celdas denominadas fotositos. Dentro de cada una de estas celdas se encuentra un fotodiodo[5].

A cada fotosito le corresponde un elemento de la imagen comúnmente llamado pixel, tal como se puede ver en la Figura 1.17. Cada pixel convierte la energía presente en la luz (fotones) en un número determinado de electrones (carga eléctrica). Mientras más brillante es la luz, más carga eléctrica acumulará.

[5] Fotodiodo.- Componente electrónico que conduce una cantidad de corriente eléctrica en función a la cantidad de luz que lo incide.

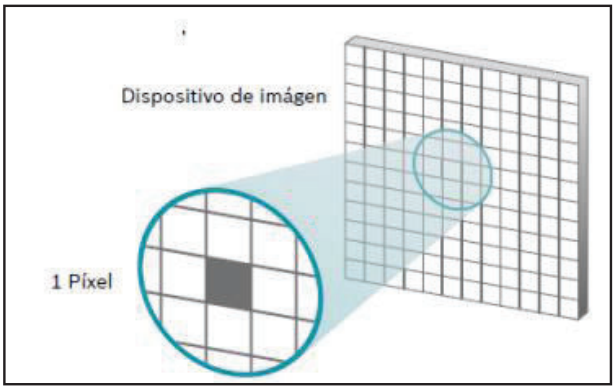


Figura 1.17 Sensor de Imagen [25]

Las principales tecnologías utilizadas para la fabricación de sensores de cámaras digitales son:

- Tecnología CCD (*Charge Coupled Device*): Ofrecen una sensibilidad lumínica ligeramente superior, producen menos ruido, son más caros y consumen más energía que la tecnología CMOS. Esta sensibilidad lumínica se traduce en mejores imágenes con escenas de poca luz.
- Tecnología CMOS (*Complementary Metal Oxide Semiconductor*): Los recientes avances los han acercado más a su competidor la tecnología CCD en términos de calidad de imagen. Son de menor tamaño, consumen menos energía, son más baratos y ofrecen mayores posibilidades de integración con mayores funciones. También ofrecen un menor tiempo de lectura lo que resulta una ventaja cuando se requieren imágenes de alta resolución.

  Los sensores CMOS megapíxel están mucho más extendidos y son menos caros que los sensores CCD megapíxel.

1.3.1.1.3 Procesador de imagen

En esta etapa, se recibe la imagen digitalizada por parte del sensor, se la procesa y se la envía a la etapa de compresión. Una imagen obtenida por el sensor puede mejorar en su calidad mediante el empleo de diferentes técnicas y parámetros.

1.3.1.1.4 CPU

El CPU de una cámara IP está compuesto por un chip que controla y administra todas las funciones de la cámara y gestiona todos los procesos internos como: el tipo de compresión, el envío de imágenes y la gestión de alarmas y avisos.

1.3.1.1.5 Etapa de Compresión

La compresión de datos resulta imprescindible para la transmisión de imágenes y video a través de una red IP. Si no se hiciera uso de estas técnicas de compresión, las redes se saturarían debido a gran cantidad de información que debería viajar por el canal de trasmisión.

Los métodos de compresión más usados en las cámaras IP son: MJPEG, MPEG-4 y H.264.

- MJPEG.- Conocido también como Motion JPEG (*Joint Photographic Experts Group*), es una secuencia de video digital compuesta por una serie de imágenes JPEG individuales. Cuando se visualizan 16 o más imágenes por segundo el ojo humano lo percibe como video en movimiento.
- MPEG-4.- También conocido como MPEG -4 visual o MPEG -4 Parte 2, es un estándar compatible con aplicaciones de ancho de banda reducido y que requieren imágenes de alta calidad.
- H.264.- Conocido comúnmente como MPEG-4 Parte 10/AVC, es un estándar de nueva generación para la compresión de video digital. Ofrece la mejor resolución de video (menor tamaño) si se lo compara con los métodos antes descritos. Sin comprometer la calidad de una imagen, un codificador H.264 puede reducir el tamaño de un archivo de video digital en más del 80% si se lo compara con MJPEG y hasta en un 50% si se lo compara con MPEG -4.

1.3.1.1.6 Tarjeta Ethernet

Una vez que se ha pasado todas las etapas, la tarjeta Ethernet de una cámara de red es la encargada de ofrecer conectividad a través de una red IP. Gracias a esta tarjeta se puede transmitir o enviar las imágenes/videos capturados.

1.3.1.2 Tipos de cámaras IP

Las cámaras IP pueden ser utilizadas tanto en interiores como en exteriores y pueden ser clasificadas de acuerdo a su funcionalidad, así se tiene:

1.3.1.2.1 Cámaras IP fijas

Este tipo de cámaras una vez montadas disponen de un campo de vista fijo. Pueden ser utilizadas tanto en interiores como en exteriores y se las puede instalar en carcasas diseñadas para su uso.

En la Figura 1.18 se muestra algunos ejemplos de cámaras IP fijas.

Figura 1.18 Cámaras IP fijas [27]

1.3.1.2.2 Cámaras IP domo fijas

Conocidas también como cámaras mini domo, son cámaras que constan básicamente de una cámara de red fija dentro de una pequeña carcasa denominada domo. Entre sus principales ventajas se tiene que pueden ser disimuladas debido a su pequeño tamaño.

En la Figura 1.19 se muestra algunos ejemplos de cámaras IP domo fijas.

Figura 1.19 Cámaras IP domo fijas [27]

1.3.1.2.3 Cámaras IP PTZ (Pant Tilt Zoom)

Son cámaras que pueden moverse de manera horizontal o vertical y que poseen la opción de zoom ajustable de manera manual o automática. Su utilización es para ambientes interiores. Entre los principales beneficios que presentan este tipo de cámaras se pueden citar:

- Estabilidad electrónica de imagen (EIS): Ayuda a reducir el efecto de la vibración (debido al movimiento involuntario de la cámara) en un video.
- Máscara de privacidad: Permite bloquear o enmascarar determinadas áreas en una escena.
- Posiciones predefinidas: Se puede programar escenas predefinidas, una vez hecho esto, el operador puede cambiar de escena de manera muy rápida.
- E-flip: En el caso de que la cámara PTZ sea instalada en el techo de un local o almacén y una persona pase por debajo de la cámara, la funcionalidad E-flip girará la imagen de la persona de manera automática, con el objetivo de que la imagen no aparezca al revés. Esto es transparente para el operador.
- Auto-flip: Generalmente las cámaras PTZ no disponen de un movimiento completo de 360º debido a una parada mecánica que evita que las cámaras puedan hacer un movimiento circular continuo. Con Auto-flip, una cámara PTZ puede girar al instante 180º y seguir realizando un movimiento más allá de su punto cero.

- Autoseguimiento: Es una función de video inteligente en la que una cámara detecta automáticamente el movimiento de una persona o vehículo y lo sigue dentro del área de cobertura de dicha cámara.

En la Figura 1.20 se muestra algunos ejemplos de cámaras IP PTZ.

Figura 1.20 Cámaras IP PTZ [27]

1.3.1.2.4 Cámaras IP domo PTZ

Pueden cubrir una amplia área debido a la mayor flexibilidad que presentan en el movimiento horizontal/vertical y al gran zoom que poseen. El movimiento horizontal de este tipo de cámaras es de 360° y el vertical normalmente es de 180°. Presentan las mismas funcionalidades de una cámara PTZ y son ideales para su uso en exteriores.

En la Figura 1.21 se muestra algunos ejemplos de cámaras IP domo fijas.

Figura 1.21 Cámaras IP domo PTZ [27]

1.3.2 CODIFICADOR DE VIDEO

El codificador de video permite la integración de cámaras analógicas a un sistema de video-vigilancia IP. El codificador de video se conecta a la cámara analógica a través de su cable coaxial y convierte las señales analógicas en secuencias de video digitales para luego ser enviadas a la red por medio de su tarjeta Ethernet. En la Figura 1.22 se muestra un ejemplo de codificador de video.

Figura 1.22 Codificador de video [23]

1.3.3 MEDIOS DE TRANSMISIÓN

En el mercado existen diversas tecnologías de redes de área local (alámbricas e inalámbricas) que permiten aprovechar las ventajas que ofrecen los sistemas de video en red.

1.3.3.1 Red de área local

Una Red de Área Local (LAN), es un grupo de computadores conectados conjuntamente a una determinada área con la finalidad de comunicarse y compartir recursos entre ellos. Los datos se envían en forma de paquetes por medio de diversas tecnologías las que regulan su transmisión. La tecnología LAN más conocida es el protocolo Ethernet, especificado en la norma IEEE 802.3.

El protocolo Ethernet utiliza una topología en estrella en la que los dispositivos (computadores) se conectan a un equipo de red activo como por ejemplo un conmutador. El medio de transmisión físico que se utiliza para la conexión son principalmente el cable par trenzado (distancias de 100 m) y la fibra óptica

(distancias de entre 10 Km y 70 Km). Dependiendo del tipo de cable se pueden tener velocidades de transferencia de datos desde 100 Mbps hasta los 100000 Mbps.

1.3.3.2 Alimentación a través de Ethernet (PoE)

Permite suministrar energía a los dispositivos conectados a una red Ethernet por medio del mismo cable que transmite los datos. Un sistema de video-vigilancia con tecnología PoE (*Power over Ethernet*) permite alimentar a sus cámaras IP desde el cuarto en donde se encuentren sus servidores.

- Estándar 802.3af: El estándar 802.3af fue publicado en el 2003 y para su aplicación emplea cables par trenzado Cat-5 convencionales o de categoría superior. La compatibilidad con dispositivos de red antiguos que no soporten esta tecnología está garantizada debido a que ofrece un mecanismo para identificar automáticamente si un dispositivo es compatible o no con esta tecnología y solo recibe alimentación eléctrica una vez comprobada esta compatibilidad.
- Estándar 802.3at: Conocido también como PoE+, entrega una potencia superior que la de su predecesor.

Ambos estándares establecen una clasificación de acuerdo a la potencia que entregue/reciba un dispositivo y se puede apreciar en la Tabla 1.5.

CLASIFICACIÓN	NIVEL DE ALIMENTACIÓN MÍNIMO EN EQUIPO DE SUMINISTRO ELÉCTRICO	NIVEL DE ALIMENTACIÓN MÁXIMO EMPLEADO POR DISPOSITIVO ALIMENTADO	USO
0	15,4 W	0,44 W - 12,95 W	De forma predeterminada
1	4,0 W	0,44 W - 3,84 W	Opcional
2	7,0 W	3,84 W - 6,49 W	Opcional
3	15,4 W	6,49 W - 12,95 W	Opcional
4	30 W	12,95 W - 25,5 W	Reservado

Tabla 1.5 Clasificación de estándares PoE [31]

En la Tabla 1.5, el nivel máximo de alimentación de un dispositivo alimentado disminuye del entregado por el equipo que suministra la energía debido a las pérdidas de potencia que se generan en el cable par trenzado.

1.3.3.3 Envío de datos a través del Internet

Para poder enviar datos desde un dispositivo conectado a una LAN y otro dispositivo conectado a una LAN diferente, se debe disponer de una vía de comunicación estándar. Esta necesidad dio lugar al desarrollo de un sistema de direcciones IP y de protocolos basados en IP.

Para conectar una red LAN a la Internet se debe establecer una conexión a través de un proveedor de servicios de Internet (ISP). En este punto, aparecen los términos de velocidad de subida y velocidad de bajada, los cuales se describen a continuación:

- Velocidad de Subida.- Representa la velocidad de transferencia a la cual se pueden subir datos desde un dispositivo a la Internet.
- Velocidad de Bajada.- Representa la velocidad de transferencia a la cual se descargan archivos desde la Internet.

1.3.3.4 Direccionamiento IP

Todo dispositivo que requiera comunicarse con otro dispositivo a través de una red basada en el protocolo IP, deberá tener asignada una dirección IP exclusiva.

En la actualidad existen dos versiones de direcciones IP las cuales se citan a continuación:

1.3.3.4.1 Direcciones IPv4

Se representan por cuatro bloques (32 bits en total), cada uno separado por un punto, estos bloques representan a un número de entre 0 a 255. Existen

direcciones IPv4 públicas y privadas. Las direcciones públicas son las que nos asignan los Proveedores de Internet, es decir son las direcciones por las cuales salimos a Internet y las direcciones privadas son aquellas que no están conectadas directamente al Internet. Las direcciones privadas están organizadas por clases, las cuales se citan a continuación:

- Clase A: desde10.0.0.0 hasta 10.255.255.255.
- Clase B: desde172.16.0.0 hasta 172.31.255.255.
- Clase C: desde 192.168.0.0 hasta 192.168.255.255.

1.3.3.4.2 Direcciones IPv6

Se escriben en representación hexadecimal y constan de ocho bloques de 16 bits cada uno (en total 128 bits), subdivididos por dos puntos, por ejemplo: 2001:0da8:65b4:05d3:1315:7c1f:0461:7847. Una de las principales ventajas de utilizar este tipo de direccionamiento es tener la posibilidad de disponer de un gran número de direcciones IP (mayor que IPv4).

1.3.3.5 Puertos

Un número de puerto define un servicio o una aplicación específica. Cuando un equipo envía datos vinculados a una aplicación específica, normalmente añade el número de puerto a la dirección IP, siendo esto transparente para el usuario. Los números de puerto pueden ir desde 0 hasta 65535.

Las aplicaciones por lo general utilizan números de puerto predefinidos por la Autoridad de Números Asignados de Internet (IANA), aunque en la práctica esto se puede cambiar. Por lo general, para un servicio web vía HTTP (*Hyper Text Transfer Protocol*) se asigna el puerto 80.

Para poder acceder a las cámaras de red localizadas en una LAN privada a través del Internet, es necesario adjuntar el número de puerto correspondiente del producto de video en red a la dirección IP pública del enrutador. Pero cuando son

varios los productos de video en red, se debe configurar el enrutador para asociar un número de puerto HTTP exclusivo al puerto HTTP predeterminado y a la dirección IP del producto de video en red. A este proceso se conoce como *"reenvió de puertos"*.

Por medio de la Figura 1.23 se puede comprender de mejor manera el funcionamiento del reenvío de puertos, en donde, el router está programado para remitir las solicitudes que llegan al puerto 8032, hacia una cámara de red con dirección IP privada 192.168.10.13 y número de puerto 80.

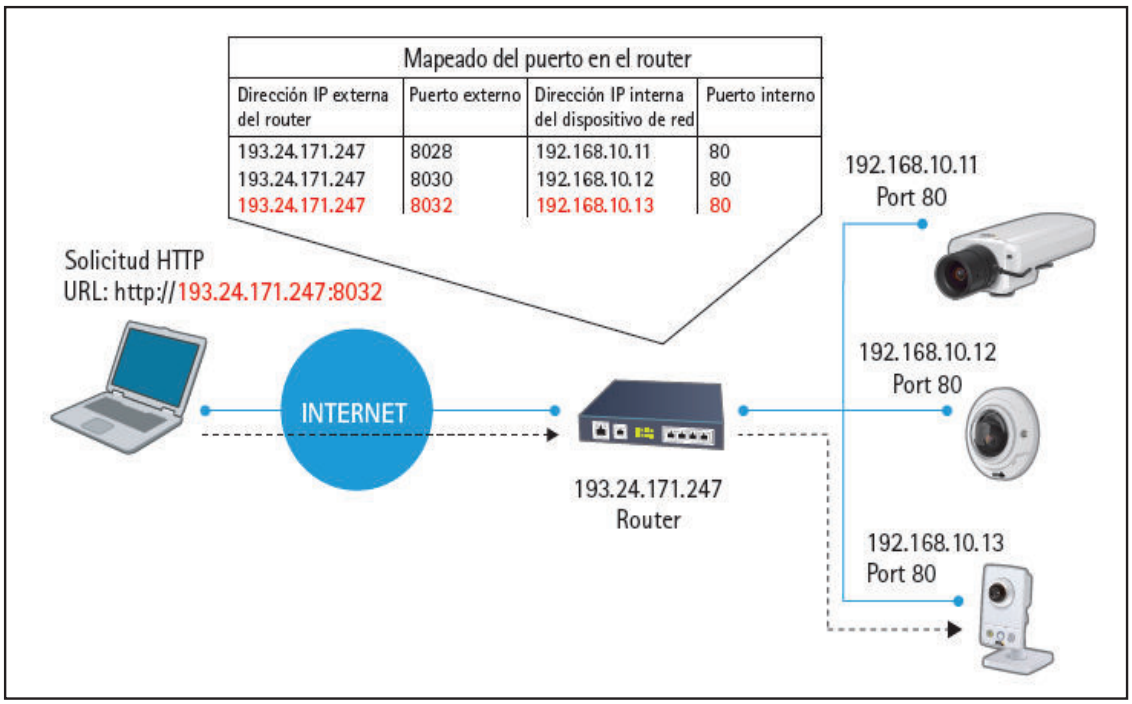


Figura 1.23 Reenvío de Puertos [31]

1.3.3.6 Protocolos de transporte de datos para video en red

Los protocolos basados en IP que se utilizan para él envió de datos son: TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*). Estos protocolos actúan como portadores para muchos otros protocolos. Por ejemplo, el protocolo HTTP se realiza en TCP.

El protocolo TCP proporciona un canal de transmisión fiable basado en conexión, esto asegura que los datos enviados desde un extremo sean recibidos en el otro. Sin embargo, esto puede producir retardos en la red debido a la retransmisión de información (en caso de errores). En general se debe emplear el protocolo TCP cuando la fiabilidad del enlace es preferente sobre la latencia del mismo.

El protocolo UDP es un protocolo no orientado a conexión que no asegura la entrega de los datos enviados, dejando el mecanismo de control y comprobación de errores a la aplicación que lo esté utilizando. No genera retrasos en la entrega de datos debido a que no retrasmite información.

En la Tabla 1.6 se muestra un resumen de los tipos de protocolos de trasmisión y puertos utilizados en aplicaciones de video-vigilancia, así como sus usos.

PROTOCOLO	PROTOCOLO DE TRANSMISIÓN	PUERTO	USO COMÚN	USO DE VIDEO EN RED
FTP (*File Transfer Protocol*)	TCP	21	Transferencia de archivos a través de internet/intranets	Transferencias de imágenes o video procedentes de una cámara de red a un servidor FTP o a una aplicación
SMTP (*Send Mail Transfer Protocol*)	TCP	25	Protocolo para el envío de mensajes de correo electrónico	Una cámara de red puede enviar imágenes o notificaciones de alarma mediante su cliente de correo electrónico integrado
HTTP (*Hyper Text Transfer Protocol*)	TCP	80	Empleado para la búsqueda en web es decir, para recuperar páginas web de servidores web	El modo más común de transferir video desde una cámara de red donde el dispositivo de video en red funciona esencialmente como un servidor web, poniendo el video a disposición del usuario que lo solicita o del servidor de aplicaciones
HTTPS (*Hyper-Text Transfer Protocol over Secure Socket Layer*)	TCP	443	Empleado para acceder a páginas web de forma segura mediante tecnología de cifrado	Transmisión segura de video desde cámaras de red
RTSP (*Real Time Streaming Protocol)*	UDP/TCP	No Definido	Formato de paquete estandarizado RTP para suministrar audio y video a través de Internet empleado con frecuencia en sistemas de transmisión multimedia o videoconferencias	Un modo habitual de transmitir video en red basado en H.264/MPEG y de sincronizar video y audio, ya que RTP proporciona la numeración y el fechado y hora secuencial de paquetes de datos, lo que permite volver a unirlos en el orden correcto. La transmisión se puede realizar mediante unidifusión o multidifusión
RTSP (*Real Time Streaming Protocol*)	TCP	554	Empleado para configurar y controlar sesiones multimedia a través de RTP	

Tabla 1.6 Protocolos y puertos usados normalmente para video en red [31]

1.3.3.7 Seguridad de la red

La información enviada a través de las redes IP debe ser protegida del acceso de personas no autorizadas, para esto, existen distintos niveles de seguridad:

- Autenticación mediante nombre de usuario y contraseña: Es el método más básico para proteger una red basada en IP. Las contraseñas pueden ser cifradas o no. Este método puede ser suficiente en escenarios en donde no se requiera elevados niveles de seguridad.
- Filtrado de direcciones IP: Por lo general los productos de video en red permiten hacer filtrado de direcciones IP. Una configuración habitual en la configuración de las cámaras de red es permitir que únicamente la dirección IP del servidor que almacena el programa de gestión de video pueda acceder a sus imágenes.
- IEEE 802.1X: Habilita un mecanismo de seguridad basado en puertos en la que intervienen el dispositivo solicitante, un dispositivo autenticador y un servidor de autenticación. El estándar IEEE 802.1X evita el secuestro de puertos, llamado también "*port hijacking*" debido a que un dispositivo primero debe autenticarse para que se le permita utilizar el puerto (ver Figura 1.24).

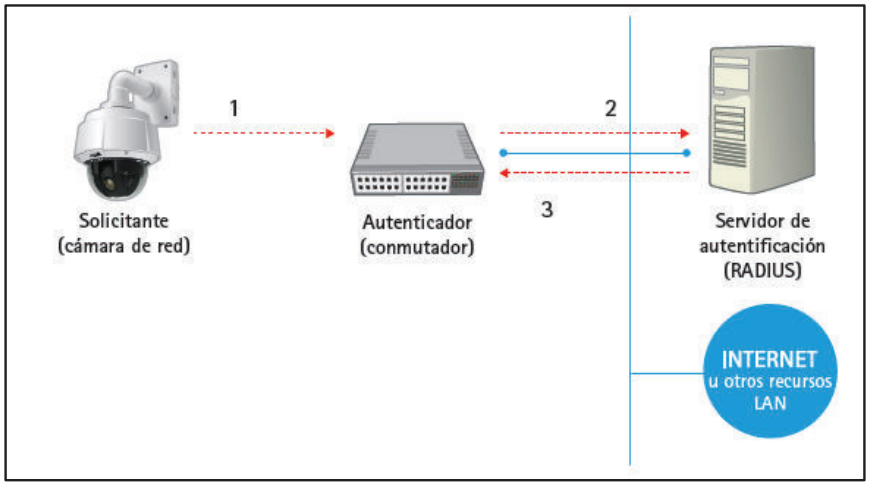


Figura 1.24 Esquema de funcionamiento del protocolo IEEE 802.1X [31]

En la Figura 1.24, la cámara de red solicita acceder a la red y envía una solicitud al conmutador, el mismo que reenvía esta solicitud al servidor de autenticación (RADIUS). Si la autenticación se realiza correctamente, el servidor de autenticación ordena al conmutador abrir el puerto para permitir que la cámara de red pueda transmitir datos a través de la red.

- HTTPS o SSL/TLS: El protocolo HTTPS (*Hyper Text Transfer Protocol Secure*) es un método seguro de comunicación el cual envía HTTP por medio de una conexión SSL (*Secure Socket Layer*) o TLS (*Transport Layer Security*). Esto significa que el HTTP y los datos están cifrados.

  Para habilitar la comunicación sobre HTTPS de un equipo de video, debe instalarse un certificado digital y un par de claves asimétricas, este par de claves las genera el equipo de video. El certificado puede generarlo y firmarlo el propio equipo o una entidad certificadora. En HTTPS, el certificado se lo emplea para autenticación y cifrado de datos.
- VPN (*Virtual Private Network*): Las redes privadas virtuales crean un túnel de comunicación segura entre dos equipos. En este tipo de configuraciones se cifra el paquete original, una vez cifrado, se encapsula en un nuevo paquete que solo muestra las direcciones IP de los equipos de comunicación (routers) a quienes está dirigido.

  La diferencia que se tiene con SSL/TLS, es que éstos, solo cifran los datos reales de un paquete (datos), en cambio, VPN puede cifrar y encapsular el paquete completo y de esta manera crear un túnel seguro, tal como se muestra en la Figura 1.25.

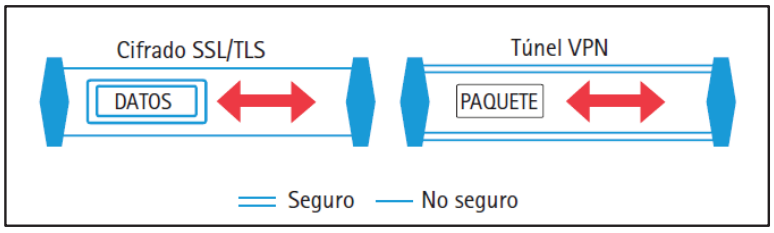


Figura 1.25 Diferencia entre SSL/TLS y VPN [31]

1.3.3.8 Tecnologías Inalámbricas

La tecnología inalámbrica ofrece una manera flexible, rentable y rápida de desplegar cámaras de vigilancia, especialmente en grandes áreas como un centro urbano o campus universitario. También pueden ser de mucha ayuda cuando se necesita instalar un sistema de video-vigilancia en edificios en los que no se puede instalar cables Ethernet.

1.3.3.8.1 Estándares 802.11 WLAN

El estándar más común para redes WLAN es el IEEE 802.11, aunque existen otros estándares y tecnologías patentadas. La ventaja de utilizar los estándares inalámbricos IEEE 802.11 es que trabajan en frecuencias libres, no es necesario el alquiler de frecuencias para su uso, lo que implica que su costo de implementación pueda ser menor si se lo compara con otras tecnologías. Las extensiones más importantes del estándar IEEE 802.11 para productos de video en red son: 802.11a, 802.11b, 802.11g y 802.11n, las cuales se detalla a continuación:

- 802.11a: Opera en la banda de frecuencia de 5 GHz y puede alcanzar una velocidad máxima de 54Mbps por medio de OFDM (*Orthogonal Frequency Division Multiplexing*). Para la interconexión entre equipos mediante este estándar es muy importante la línea de vista entre ellos.
- 802.11b: Opera en la banda de 2.4 GHz. y puede alcanzar una velocidad máxima de transmisión de 11Mbps. Utiliza DSSS (*Direct Sequence Spread Spectrum*) para la transmisión de datos con el método de acceso CSMA/CA (*Carrier Sense Multiple Access* with *Collision Avoidance*). Usualmente es utilizado en configuraciones punto – multipunto.
- 802.11g: Utiliza la banda de frecuencia de 2.4 GHz. y alcanza velocidades de transmisión de 54Mbps. Utiliza OFDM y DSSS como métodos para la transmisión de datos. Es compatible con el estándar IEEE 802.11b y no es necesario que exista línea de vista entre equipos para que puedan conectarse por medio de este estándar.

- 802.11n: Este estándar permite trabajar en las dos bandas de frecuencia libres, la de 2.4 GHz. y la de 5 GHz. Puede alcanzar velocidades de transmisión de 300Mbps. Su mejora respecto a los anteriores estándares, es el uso de varias antenas para transmisión y recepción, a esto se lo conoce como MIMO (*Multiple-input multiple-output*).

En la Tabla 1.7 se presenta un resumen de las características principales de los estándares mencionados.

PARÁMETROS	802.11a	802.11b	802.11g	802.11n
Fecha de Lanzamiento	1999	1999	2003	2007
Frecuencia de Operación	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz 5 GHz
Velocidades de Transmisión	6,9,12,18,24,36,48 y 54 Mbps	1,2,5.5 y 11 Mbps	1,2,5.5,11,18,24,36,48 y 54 Mbps	Cercano a 300 Mbps
Técnica de Modulación	OFDM	DSSS	DSSS OFDM	OFDM
Alcance en Interiores	35 m	38 m	38 m	70 m
Alcance en Exteriores	120 m	140 m	140 m	250 m

Tabla 1.7 Resumen estándares IEEE 802.11 [32]

Al emplear una red inalámbrica se debe tener en cuenta la capacidad de transferencia de la red en el punto de acceso y los requisitos de transferencia de los dispositivos de red. En general el caudal de datos útiles admitido por un estándar IEEE 802.11 es aproximadamente la mitad de la tasa de bits teórica estipulada para el mismo, esto debido a la sobrecarga de la señal y del protocolo.

1.3.3.8.2 Seguridad WLAN.

La naturaleza de las comunicaciones inalámbricas permite que cualquier dispositivo que se encuentre en su área de cobertura puede acceder a ella e interceptar los datos que por ella estén circulando, es por eso, la necesidad de

implementar mecanismos de seguridad que impidan el acceso de dispositivos no autorizados a la red.

- WEP (*Wired Equivalent Privacy*): Fue diseñada para evitar el acceso a la red de personas que no dispusieran de una clave. Este método resulto inseguro debido a deficiencias como: uso de claves cortas y facilidad de reconstrucción de la clave con la intercepción de unos cuantos paquetes de datos.
- Acceso protegido por Wi-Fi: El sistema WPA (*Wi-Fi Protected Access*) y su sucesor WPA2 (*Wi-Fi Protected Access II*) están basados en el estándar IEEE 802.11i y elevan significativamente la seguridad inalámbrica.
  El sistema WPA Personal, también conocido como WPA/WPA2PSK (*Pre-Shared Key*), está diseñado para redes pequeñas, mediante esta técnica, las cámaras de red emplean una clave pre-compartida para la autenticación con el punto de acceso. Existe también el sistema WPA/WPA2-Enterprise, que está diseñado para redes grandes y requiere un servidor de autenticación que utilice el estándar IEEE 802.1X.

Un método para simplificar la configuración WLAN de una cámara de red y la conexión a un punto de acceso, es el empleo de WPS (Wi-Fi Protect Setup), en el que se empareja la cámara de red y el punto de acceso mediante la pulsación del botón WPS en ambos dispositivos, en un plazo de 120 segundos. En ese intervalo de tiempo, los dos dispositivos se descubrirán automáticamente entre si y acordarán una configuración. No todos los productos de video en red soportan este mecanismo.

1.3.3.8.3 Red de Malla Inalámbrica

Conocidas también como WMN (*Wireless Mesh Network*), o WiMesh (*Wireless Mesh*). Una red de malla inalámbrica representa una solución común para sistemas de video-vigilancia en centros urbanos, que podrían estar conformados por varios nodos de conexión, los mismos que sirven para enviar y recibir datos, ofreciendo rutas de conexiones redundantes e individuales (ver Figura 1.26).

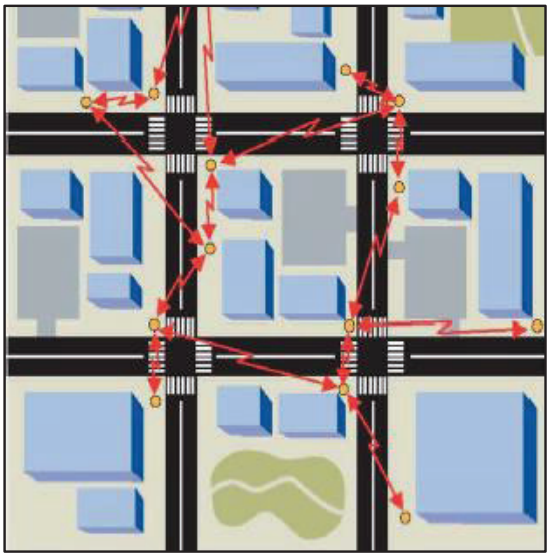


Figura 1.26 Redes malladas inalámbricas [34]

Al utilizar la topología de red en malla los nodos se conectan entre sí permitiendo que se comuniquen entre todos y que puedan llevar mensajes por diferentes caminos, gracias a que poseen mecanismos inteligentes de enrutamiento. Estos nodos son auto-suficientes, es decir, pueden configurarse automáticamente en caso de la caída de alguno de ellos, lo que implica que no sea necesaria una gestión centralizada.

Las WMN mezclan dos topologías de conexión en su funcionamiento, la topología Ad-hoc[6] y la topología infraestructura[7]. Estas redes son relativamente nuevas en el mercado y basan su funcionamiento en el estándar IEEE 802.11s, el cual fue aprobado en junio del 2011 y tienen como objetivo un mejor aprovechamiento de las tecnologías WLAN.

1.3.3.8.4 Elementos de una red WMN

Los elementos que componen una red mesh son los siguientes:

[6] Ad-hoc.- Es un tipo de red inalámbrica descentralizada que no necesita de una infraestructura pre-existente para poder funcionar

[7] Infraestructura.- Es un tipo de red centralizada tipo cliente-servidor

- Nodo Mesh (NM): es el responsable de establecer los caminos de comunicaciones y mantener estas comunicaciones con el resto de nodos de la red.
- Punto de Acceso (AP): permite crear y gestionar la capa de servicio a los clientes.
- Gateway (GT): permite el acceso a una red externa.

En la Figura 1.27 se muestra cada uno de estos elementos.

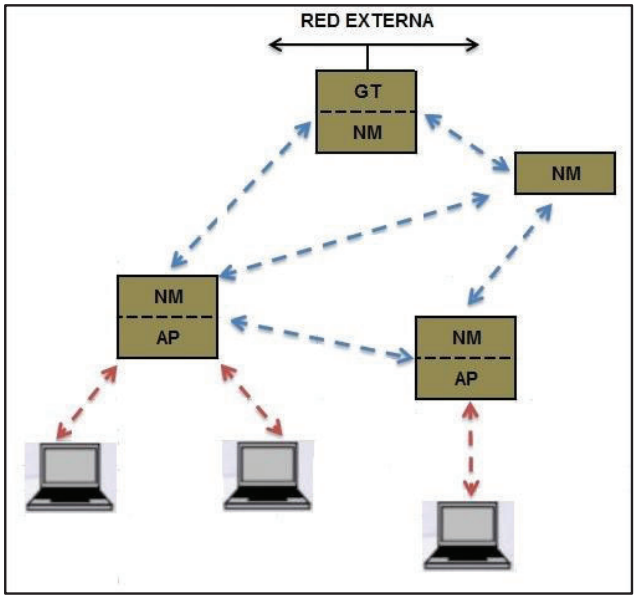


Figura 1.27 Elementos de una red WMN [34]

Los nodos mesh son los elementos principales en este tipo de redes, estos nodos son equipos WLAN que soportan una o múltiples etapas de radio (ver Figura 1.28) y permiten definir las siguientes capas lógicas:

- Capa de servicio (AP): En esta capa se definen los usuarios y sus características de conexión, por ejemplo: encriptación, tipo de protocolo, etc.
- Capa Uplink: Esta capa es la encargada de encaminar el tráfico intramesh en dirección al Gateway.

- Capa Downlink: Esta capa encamina el tráfico intramesh desde el Gateway a los nodos mesh finales.

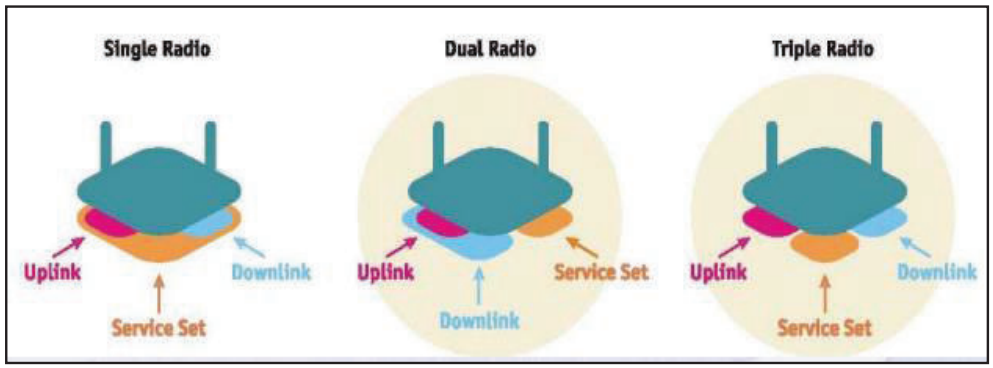


Figura 1.28 Capas lógicas en un nodo mesh con varias etapas de radios [34]

1.3.3.8.5 Características básicas de una red WMN

- Redundancia.- Los equipos que forman la red de backbone se comunican entre sí por medio de algoritmos, usando diversos caminos o rutas, esto permite que la comunicación hacia cualquier destino puede establecerse mediante distintos equipos en la red.
- Itinerancia.- Las redes WMN proporcionan movilidad a los equipos clientes que se encuentren dentro del rango de cobertura de toda la red, esto significa que un equipo cliente pueda asociarse con el siguiente nodo mesh de la red para seguir transmitiendo/enviando información, siendo este intercambio totalmente transparente para el usuario.
- Autoconfiguración y facilidad de despliegue.- Los algoritmos de enrutamiento presentes en los nodos mesh establecen dinámicamente las rutas entre nodos y permiten negociar automáticamente la comunicación con nuevos nodos que se agreguen a la red.
- Autonomía.- Los protocolos de enrutamiento permiten que los nodos mesh se auto-recuperen en caso de caída o uno o más nodos en la red, reconstruyendo dinámicamente sus tablas de enrutamiento.

1.3.3.8.6 Arquitectura de una red WMN

En lo referente a la arquitectura de las redes WMN, éstas se pueden clasificar de las siguientes maneras:

- WMN de Infraestructura.- Los equipos mesh forman la infraestructura necesaria para dar servicio a sus clientes (ver Figura 1.29).

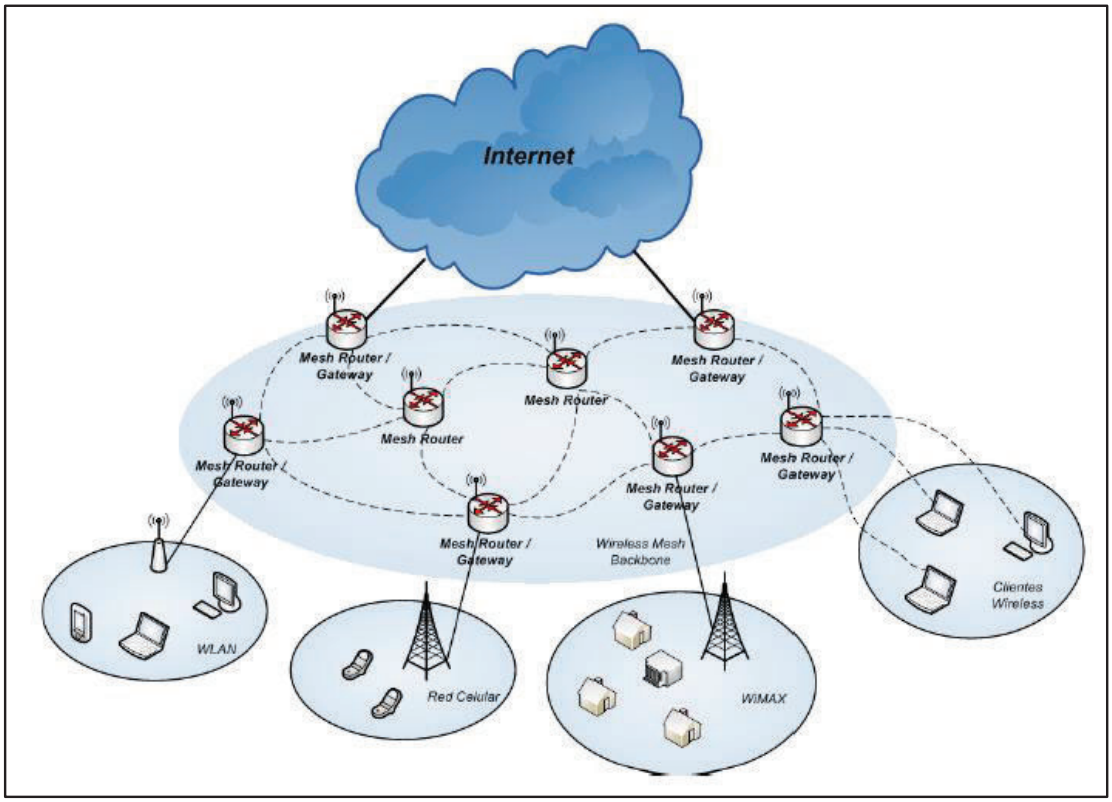


Figura 1.29 Esquema WMN de infraestructura [30]

- WMN Cliente.- Este tipo de infraestructura la conforman los equipos mesh clientes, estos equipos establecen conexiones Ad-hoc o peer to peer con otros equipos clientes de la misma red mesh (ver Figura 1.30).

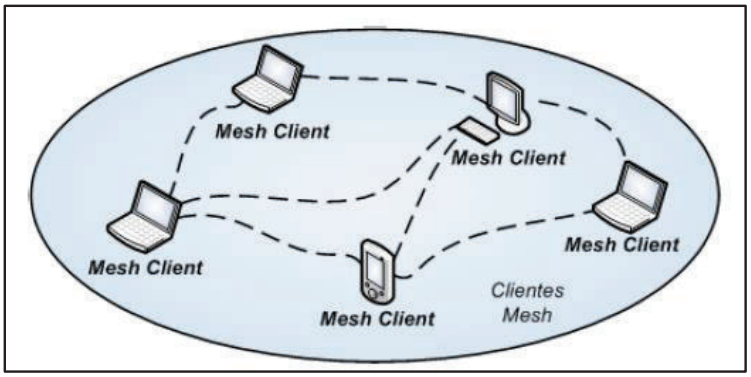


Figura 1.30 Esquema WMN cliente [30]

- WMN Híbridas.- Es la arquitectura resultante de combinar las dos arquitecturas anteriores (ver Figura 1.31).

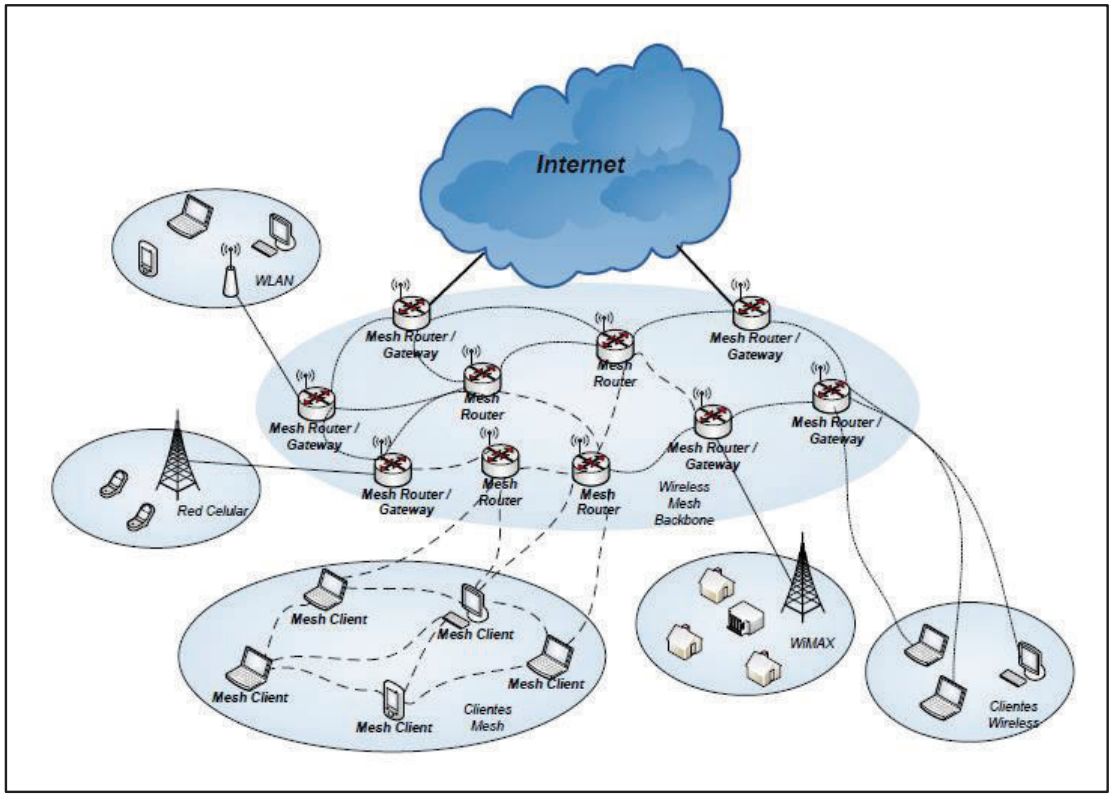


Figura 1.31 Esquema WMN híbrido [30]

1.3.3.8.7 Protocolos de enrutamiento en WMN

Un protocolo o algoritmo de enrutamiento tiene como función principal escoger la mejor ruta o camino para que un datagrama pueda llegar a su destino.

Existen varios protocolos de enrutamiento propietarios que pueden ser usados en redes WMN, sin embargo el estándar IEEE 802.11s define al protocolo HWMP (Hybrid Wireless Mesh) para su enrutamiento.

Entre las principales funciones que debe cumplir un protocolo de enrutamiento se pueden citar las siguientes:

- Cálculo de Rutas: Debe encontrar el mejor camino basado en diferentes criterios de enrutamiento como métricas, calidad del enlace, número de saltos y ancho de banda del medio.
- Manejo de la red troncal: Debe gestionar enlaces a redes externas como por ejemplo la red internet.
- Descubrimiento de frontera: Debe ser capaz de encontrar los límites de la red, generalmente los sitios donde un router se conecta a una red cableada.
- Descubrimiento de nodos: Al usar una red que puede cambiar constantemente, es necesario que el protocolo de enrutamiento sea capaz de descubrir nuevos nodos, así como establecer rutas dinámicas en base a cada descubrimiento.

1.3.3.8.8 HWMP (Hybrid Wireless Mesh Protocol)

Es un protocolo híbrido que tiene un conocimiento parcial de la topología de la red, es decir, conoce únicamente a sus vecinos. Este protocolo debe ser implementado por todos los nodos mesh de una red, sin embargo como ya se mencionó anteriormente, está permitido el uso de protocolos de enrutamiento propietarios.

El protocolo HWMP proporciona un método tanto proactivo como reactivo para la selección de los caminos. La característica reactiva del protocolo se adapta para las estaciones que presentan alta movilidad, mientras que la característica proactiva es una opción más eficiente para una topología de red fija. El hecho de poder usar los dos modos simultáneamente lo convierte en híbrido (ver Figura 1.32).

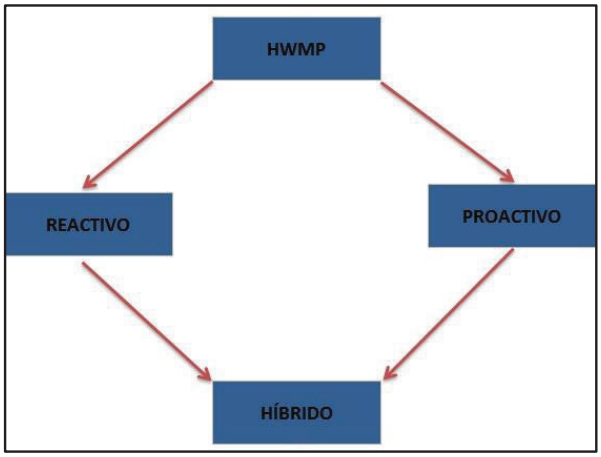


Figura 1. 32 Protocolo de enrutamiento HWMP

1.3.3.8.9 Seguridad en WMN

Las redes mesh se encuentran expuestas a las mismas amenazas que una red cableada u otro tipo de red inalámbrica, por esta razón, es de primordial importancia proteger los datos que se transmiten por un medio no guiado y que resultan susceptibles de ser interceptados.

Como mecanismo de seguridad, el proyecto IEEE 802.11s se basa en la protección entre pares, utiliza EMSA (Efficient Mesh Security Association) para esto. Por lo tanto, la seguridad extremo a extremo debe ser mejorada en las capas superiores.

EMSA utiliza el modelo de autenticación establecido en el estándar IEEE 802.11i, en el cual se incluye la distribución de llaves, la encriptación de las tramas de administración y la autenticación por medio del estándar 802.1x. Sin embargo la

diferencia principal con las redes WLAN tradicionales (un solo salto) es que los puntos de acceso de una WMN deben actuar de dos formas: autenticador y solicitante.

1.3.4 DISPOSITIVOS DE ALMACENAMIENTO DE VIDEO

Los dispositivos o unidades de almacenamiento de video son una parte esencial en un sistema de video-vigilancia. Estos dispositivos permiten monitorear, grabar, administrar y archivar videos e imágenes provenientes de las cámaras de video-vigilancia.

Los dispositivos de almacenamiento de video permiten realizar una configuración específica de la manera de grabar los videos, incluso se puede configurar de manera independiente para cada cámara. Entre las principales formas de grabación se tiene:

- Grabación continua: El dispositivo de almacenamiento graba continuamente y sin interrupciones durante todo el tiempo.
- Grabación programada: Cuando se requiere grabar en ciertas fechas o periodos de tiempo (hora/día/semana).
- Grabación por eventos: El dispositivo empezará a grabar únicamente cuando detecte movimiento o cuando exista un disparo de alarma.
- Grabación por eventos y por tiempo: El dispositivo empezará a grabar cuando existan eventos y éstos, se encuentren dentro de un periodo de tiempo específico.

En los sistemas de video-vigilancia se pueden distinguir tres maneras de almacenamiento de video, las cuales se citan a continuación:

1.3.4.1 Almacenamiento en el mismo dispositivo

Actualmente la mayoría de cámaras IP cuentan con un puerto para colocar una memoria interna, ya sea una tarjeta SD o memorias USB. Estos dispositivos son

capaces de almacenar videos por horas o incluso días (depende de la capacidad de almacenamiento de las tarjetas SD o memorias USB).

Esta forma de almacenamiento resulta útil en situaciones en las que el video no pueda transmitirse a través de una red.

1.3.4.2 Almacenamiento en un PC con software de control

Este tipo de almacenamiento resulta útil en sistemas pequeños en los cuales hay pocas cámaras de video-vigilancia y por tanto, poca carga de videos.

El video proveniente de estas cámaras de vigilancia es almacenado directamente en el disco duro de un computador.

1.3.4.3 Almacenamiento NVR (*Network Video Recorder*)

Un NVR es un sistema de almacenamiento NAS (*Network Attached Storage*) complementado con un software específico de video-vigilancia que funciona independientemente de una computadora. Presenta grandes funcionalidades para la gestión de video en red, las cuales permiten grabar y visualizar las imágenes digitales captadas por las cámaras de video, estas imágenes pueden provenir de una red local o de manera remota.

Este tipo de almacenamiento es recomendado para sistemas grandes debido a que posee un gran disco duro que le permite almacenar grandes volúmenes de video.

1.3.5 SISTEMAS DE ADMINISTRACIÓN Y GESTIÓN DE VIDEO

Un aspecto sumamente importante que se debe tener en cuenta en la implementación de un sistema de video-vigilancia es la gestión de video. La gestión de video se lo realiza por medio de un software específico que puede

correr en múltiples plataformas (Windows, Unix/Linux y Mac OS) y que puede ser gratuito o de pago.

Entre las principales funciones que debe ofrecer un sistema de gestión de video se pueden citar las siguientes:

- Grabación de video.
- Reproducción de video en directo, ya sea de una cámara o de todo el sistema.
- Reproducción y grabación del audio de una escena.
- Gestión de eventos, como la detección de movimientos y alarmas.
- Configuración de las cámaras de red.
- Búsqueda y reproducción de videos previamente guardados.
- Control de acceso a usuarios con diferentes niveles de acceso (Administrador, Operador).
- Aplicaciones de video inteligente, como programar rondas virtuales.
- Mapeo del lugar donde se encuentran las cámaras de vigilancia.
- Envió de alertas.
- Seguridad.

Un programa de gestión de video puede estar implementado de las siguientes maneras:

1.3.5.1 Software implementado en las cámaras de red

Las cámaras de red llevan implementado un software que ofrece las funciones de gestión de video y permite la configuración vía web de manera muy sencilla.

1.3.5.2 Software implementado en un PC

Actualmente, existe una gran variedad de programas que hacen gestión de video. Estos programas pueden ser de licencia libre o de pago y pueden correr en diferentes sistemas operativos. La gran mayoría de proveedores de cámaras de

red ofrecen programas propietarios para la gestión de video, los cuales funcionan únicamente con sus marcas. En la Tabla 1.8 se muestran algunos programas de gestión de video que cumplen con la especificación ONVIF[8].

NOMBRE DEL PROGRAMA	PLATAFORMA	LICENCIA	OBSERVACIONES
Ispy Connect	Windows	Libre y de pago	Libre únicamente para acceso local
Axxon Next	Windows	Libre y de pago	Libre, pero con limitaciones (hasta 1TB de almacenamiento, solo 1 servidor, hasta 16 cámaras)
Xeoma	Linux, MAC y Windows	Libre y de pago	La versión gratuita soporta una única cámara
			La versión de prueba no tiene limitaciones pero no se guardan las configuraciones al salir del programa y se reinicia cada 48 horas
Zondeminder	Linux	Libre	Instalación y configuración compleja
Blue iris	Windows	Pago	Funciona con la gran mayoría de marcas de cámaras de red. La versión de prueba no tiene limitaciones y dura 15 días.

Tabla 1.8 Programas para la gestión de video

1.3.5.3 Software implementado en un NVR

Un dispositivo NVR lleva preinstalado un programa patentado y diseñado específicamente para la gestión de video. Por lo general, al comprar un NVR se entrega la versión del programa cliente para poder instalarlo en cualquier computador o dispositivo desde donde se quiera tener acceso al sistema de video-vigilancia.

[8] ONVIF (Open Network Video Interface Forum)._ Es un foro abierto y global de la industria fundado en el 2008 por las empresas Axis, Bosch y Sony (Principales fabricantes de cámaras de video IP), el mismo que trabaja para desarrollar un estándar global para productos de seguridad basados en IP. La especificación ONVIF busca garantizar la interoperabilidad entre los productos de video en red de distintos fabricantes.

CAPÍTULO 2
ANÁLISIS DE REQUERIMIENTOS

2.1 ANÁLISIS DEL ENTORNO [1] [8]

La ciudad de Cayambe se encuentra ubicada al noreste de la provincia de Pichincha, a una distancia de 78 Km de la ciudad de Quito (ver Figura 2.1). Cayambe es la cabecera del cantón que lleva su nombre, esta ciudad tiene una superficie de 1.350 km² y cuenta con 39.028 habitantes en el sector urbano y 46.767 en el sector rural, dando como resultado 85.795 habitantes según el último censo realizado en el año 2010.

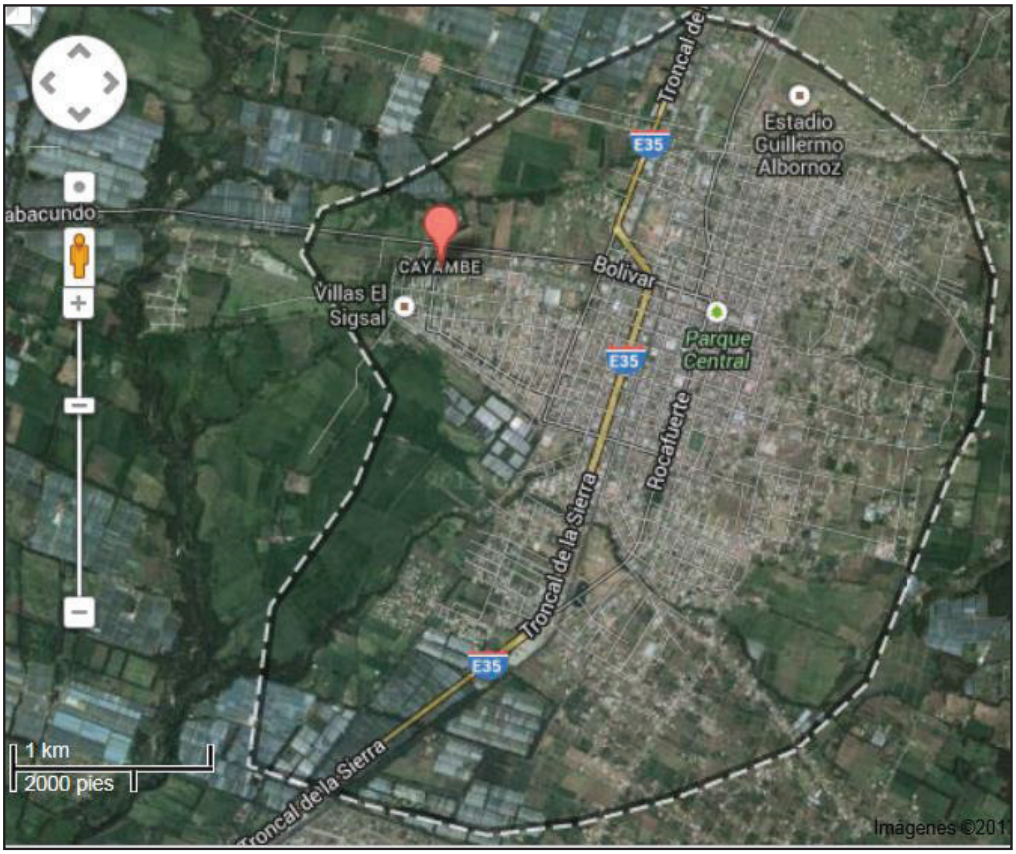


Figura 2.1 Visualización del Cantón Cayambe a través de Google Earth [2]

Se ha tomado en cuenta este cantón para el desarrollo de este proyecto por el gran desarrollo que ha tenido en los últimos años. Esta ciudad ha ido transformándose, empezando desde ser un limitado pueblo hasta lograr convertirse en una ciudad con un gran crecimiento cultural, poblacional y económico (ver Figura 2.2).

Figura 2.2 Parque Central de Cayambe

Una de las principales razones por la cual se ha tenido este progreso es la producción florícola. Cayambe es una de las principales ciudades exportadoras de flores a nivel nacional e internacional, siendo esta una oportunidad de trabajo para personas propias del lugar y también de otros rincones del país, viendo en esta ciudad una oportunidad de progreso.

Otros aspectos que influyen en la economía de esta ciudad son la producción de ganado bovino utilizado en la producción de lácteos y la agricultura en especial la siembra de papas, habas, cebada y trigo, productos típicos del lugar.

La alta tasa poblacional y el desarrollo económico ha traído necesidades de servicios como: vivienda, educación, salud y especialmente seguridad, razón por la cual, se ha pensado en este proyecto.

El sistema de video-vigilancia cubrirá los lugares más vulnerables del sector urbano de la ciudad de Cayambe, de momento no sería necesaria la colocación

de cámaras en el sector rural, ya que la mayor parte de estos sectores son terrenos utilizados para el cultivo y pastoreo de ganado.

El área urbana de la ciudad de Cayambe se puede apreciar en la Figura 2.3 y está delimitada de la siguiente manera:

“ El limite urbano de Cayambe se inicia en la intersección del río Blanco con la prolongación de la quebrada El Poguio en el P1, de coordenadas N1005564-E816948; continua con el cauce del río Blanco aguas arriba hasta el límite nororiente de la propiedad del Señor Nicolás Gonzáles en el P2, de coordenadas N10005778-E819646; sigue en este límite hacia el sur hasta topar el camino que conduce Rosinvar sigue este camino en sentido este hasta el P3 de coordenadas N10005440-E819620 continua hacia el sur bordeando el barrio San Carlos hasta el cruce con la calle Pichincha en P4, de coordenadas N1004830-E819525 continua por la calle Pichincha en sentido sureste bordeando el lindero de las propiedades de los Señores José García y José María Túquerres hasta el cruce con la calle Azuay en el P5, de coordenadas N10004610-E819559; continua por las calles Azuay, Chimborazo Y Santiago en sentido Sur, hasta encontrar la confluencia de las quebradas Yasnán y Chahuarpungo en el P6 de coordenadas N10003530-E 819276; continua descendiendo por el lecho de la quebrada Yasnán hasta el cruce con la línea del Ferrocarril en el P7, de coordenadas N10003991-E817126; siguiendo la línea del ferrocarril en el sentido noroeste, hasta el límite entre la Urbanización EL Sigsal y la plantación florícola de la hacienda la Florida en el P8, de coordenadas N10004398-E817373; continua por el límite norte de la plantación de la hacienda La Florida y el límite sur de la urbanización El Sigsal, hasta el cruce con la quebrada el Poguio en el P9, de coordenadas N10004960-E816480; desde el punto se continua hacia el oeste por el camino existente dentro de la propiedad del Señor Rodrigo Tobar hasta el cruce con el río Granobles, que determina el límite del Cantón Cayambe con el Cantón Pedro Moncayo en el P10, de coordenadas N10004875-E815278, se sigue por el curso ascendente del río Granobles, en dirección norte, hasta el cruce con la carretera Panamericana, en el P11, de coordenadas N10005440-E815374; continua hacia el este de la carretera Panamericana hasta la quebrada el Poguio

en el P13, de coordenadas N10005271-E816806; de este punto cruzamos la Panamericana hacia el norte hasta llegar el P1 de coordenadas N1005564-E816948 " [9]

Figura 2.3 Coordenadas sector urbano del Cantón Cayambe

[9] Reforma a la ordenanza de delimitación urbana Art.1, Año 2006, Gobierno Municipal de Cayambe

2.1.1 BARRIOS UBICADOS EN EL SECTOR URBANO DE CAYAMBE

Los barrios ubicados en el sector urbano de la ciudad de Cayambe que serán objeto de estudio para el desarrollo de este Proyecto, se los enumera en la Tabla 2.1

N.	BARRIO	N.	BARRIO
1	Santa Marianita de Granobles	21	Verde Pamba
2	23 De Julio	22	Bolívar
3	Amazonas	23	La Obrera
4	Santa Laura De Changalá	24	Central
5	Changalá	25	Florida I
6	Sigsal Bajo	26	Florida II
7	Víctor Cartagena	27	1 De Mayo
8	Sandra Pérez	28	Álvarez y Chiriboga
9	El Sigsal	29	La Playa
10	Lucila Cartagena	30	San Pedro
11	La Estación	31	El Obraje
12	Une	32	Bellavista De Cruz Loma
13	Miraflores	33	San Carlos
14	Las Orquídeas	34	Bellavista de Puntiachil
15	Nuevos Horizontes	35	Sur
16	San Ruperto	36	La Cruz
17	Hacienda Primavera	37	Puntiachil
18	Girasoles	38	Chimborazo
19	Sara Jarrín	39	San Nicolás
20	Patarata	40	Don Bosco
		41	4 Esquinas

Tabla 2.1 Barrios sector urbano de Cayambe

En la Figura 2.4 se muestra la ubicación física de los barrios enumerados en la Tabla 2.1

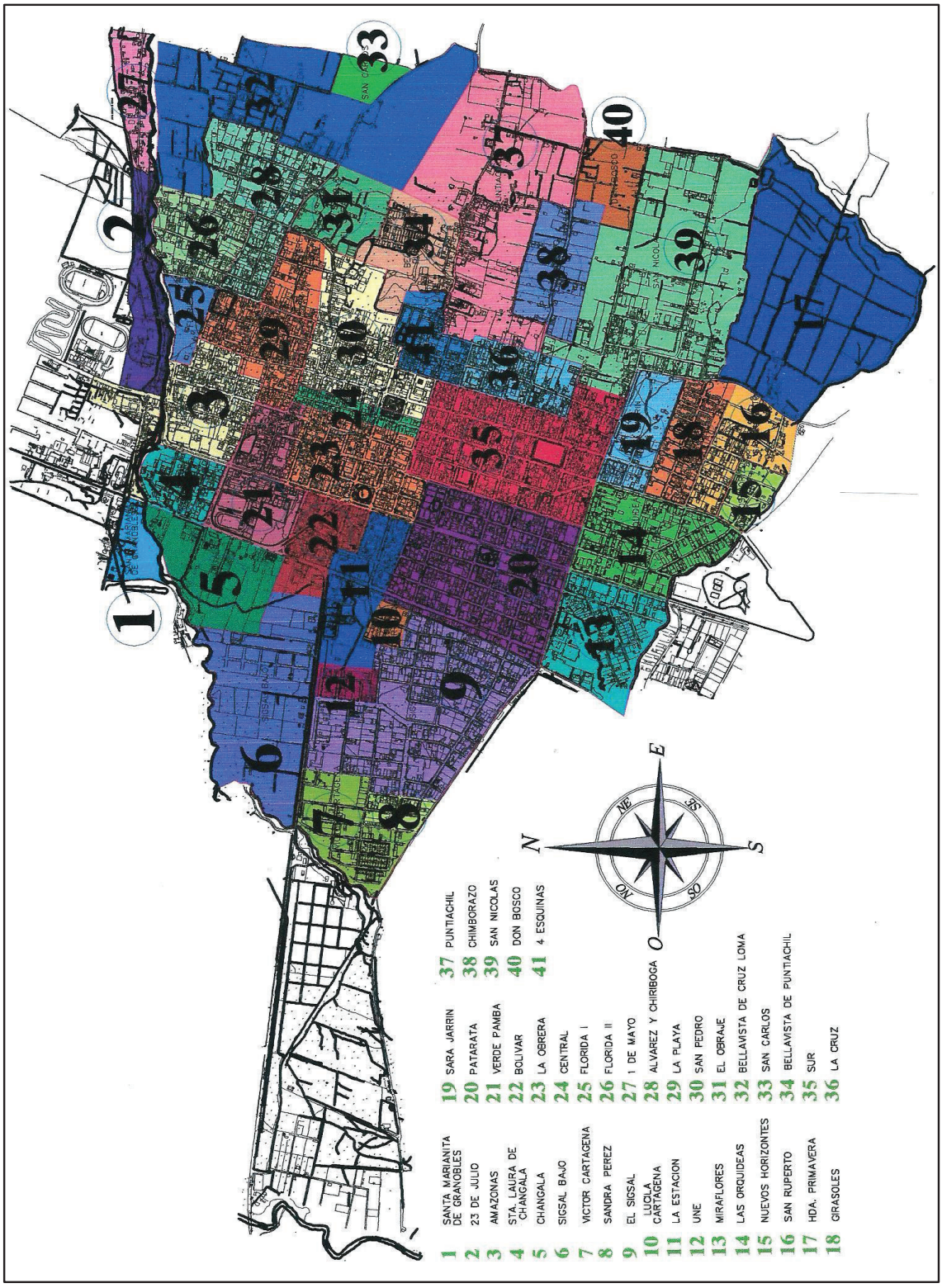


Figura 2.4 Barrios ubicados en el sector urbano del Cantón Cayambe

2.2 INVESTIGACIÓN DEL MERCADO [3] [4] [5] [6] [7]

Para el análisis de la importancia y/o necesidad de la implementación del sistema de video-vigilancia, es necesario adentrarse a la comunidad y conocer los problemas y necesidades que aquejan a los ciudadanos, moradores y visitantes de esta ciudad, en lo que se referente a seguridad. Para esto se ha visto necesario realizar encuestas a moradores del sector y entrevistas a los Agentes del Distrito de Policía de Cayambe y Pedro Moncayo quienes son los encargados de vigilar la seguridad de la ciudad.

De esta manera se obtendrán datos suficientes para poder justificar la posible implementación de este Proyecto de Titulación.

2.2.1 ENCUESTAS

La encuesta es un estudio observacional por medio de la cual el investigador busca obtener datos mediante el empleo de diversas preguntas a una muestra de la población en un cuestionario previamente elaborado. Esta es una herramienta que no puede ser manipulada en su proceso por el investigador si se busca obtener datos verdaderos.

2.2.1.1 Objetivo de la Encuesta

Determinar por medio de un sondeo el grado de aceptación y la necesidad de implementar un sistema de video-vigilancia con el objetivo de prevenir actos delictivos.

La encuesta que se utilizará es del tipo descriptiva[10]. La encuesta consta de ocho preguntas cerradas[11] de esta manera las respuestas serán de mejor entendimiento y será mucho más fácil la tabulación de los datos obtenidos.

---

[10] Encuesta Descriptiva.- Aquellas que buscan o pretenden documentar las actitudes presentes, sin explicar el porqué de una determinada situación.

El modelo de encuesta que se empleó para este análisis se encuentra en el ANEXO A.

2.2.1.2 Cálculo de la Muestra

Para el cálculo del tamaño de la muestra[12] se utilizará la Ecuación 2.1

$$n = \frac{k^2 * p * q * N}{\left(e^2 * (N-1)\right) + k^2\, p\, *\, q}$$

Ecuación 2.1 [4]

Dónde:

N = Tamaño de la población.

e = Error muestral deseado, es la diferencia entre el resultado que se obtendría preguntando a una muestra de la población y el que se obtendría si se preguntara a toda la población.

p = Proporción de individuos en la población que poseen un nivel académico aceptable, cuando no se conoce este dato se emplea el valor de p = q =0.5. [4]

q = Proporción de individuos que no poseen estudios.

$$q = 1-p$$

Ecuación 2.2 [4]

n = Tamaño de la muestra.

k = Constante que depende del nivel de confianza que le asigne. El nivel de confianza indica la probabilidad de que los resultados de la investigación sean

---

[11] Preguntas Cerradas.- Se debe elegir de un grupo de opciones la respuesta que más se aseméjeme a su realidad.

[12] Muestra.- Parte de la población a estudiar que permite representarla.

ciertos, algunos de los valores que se pueden utilizar se encuentran en la Tabla 2.2

K	1,15	1,28	1,44	1,65	1,96	2,00	2,58
NIVEL DE CONFIANZA	75%	80%	85%	90%	95%	96%	99%

Tabla 2.2 Nivel de confianza de k [4]

Los valores de las variables que se utilizarán en el cálculo de la muestra poblacional de la ciudad de Cayambe son los siguientes:

q = 0.5, debido a que se desconoce la porción de individuos que no poseen estudios.
p = 0.5, debido a que se desconoce la porción de individuos que poseen estudios.
e = 5%, debido a que se espera tener un error en la muestra bajo
k = 1.96, debido a que se asigna un nivel de confianza del 95%
N = 39028, tamaño de la población urbana de acuerdo al censo realizado en el 2010.

Desarrollando la Ecuación 2.1 se obtiene:

$$n = \frac{(1.96)^2(0.5)(0.5)(39028)}{\left((0.05)^2(39027)\right) + (1.96)^2(0.5)(0.5)}$$

$$n = \frac{37482.4912}{97.5675 + 0.9604}$$

$$n = \frac{37482.4912}{98.5279}$$

$$n = 380$$

Por lo tanto, será necesario encuestar a 380 personas para obtener datos válidos.

2.2.1.3 Resultados de las Encuestas Efectuadas

Una vez elaborada la encuesta se procedió a efectuar la misma a la población del cantón Cayambe, indistintamente de la raza, género y edad, obteniéndose de esta manera los datos que son presentados a continuación.

Pregunta 1.- ¿Cree usted que el cantón Cayambe es seguro?

En la Tabla 2.3 se presenta el resultado de la pregunta 1 y en la Figura 2.5 se muestra los resultados en forma gráfica.

PREGUNTA 1	PORCENTAJE	CANTIDAD
No	97%	369
Si	3%	11
Total	**100%**	**380**

Tabla 2.3 Resultados pregunta uno

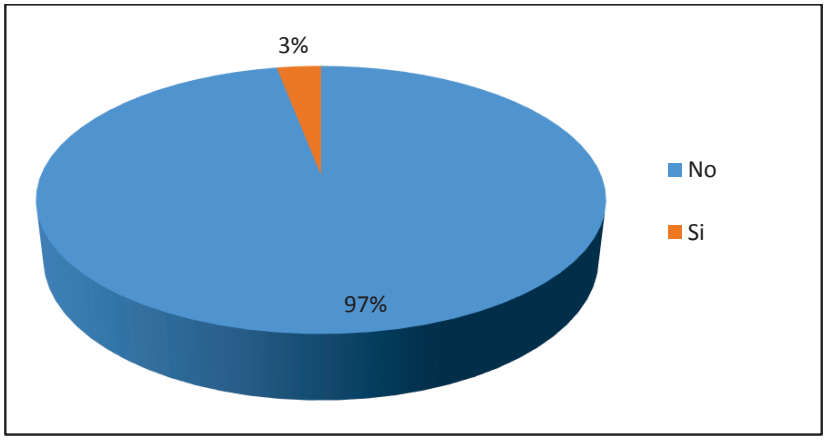


Figura 2.5 Resultados pregunta uno

Pregunta 2.- ¿Ha sufrido usted algún tipo de acto de delincuencia? Si su pregunta es afirmativa, pase a responder las preguntas 3 y 4, caso contrario pase directamente a la Pregunta 5.

En la Tabla 2.4 se presenta el resultado de la pregunta 2 y en la Figura 2.6 se muestra los resultados en forma gráfica.

PREGUNTA 2	PORCENTAJE	CANTIDAD
No	21%	78
Si	79%	302
Total	**100%**	**380**

Tabla 2.4 Resultados pregunta dos

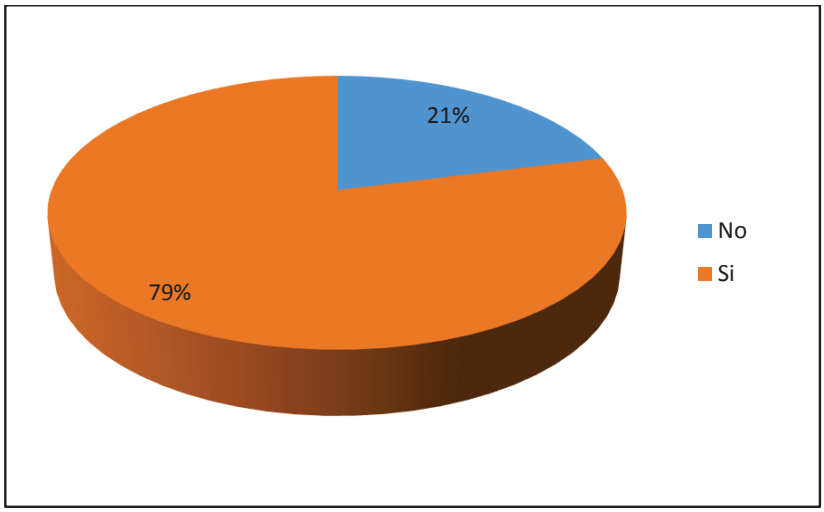


Figura 2.6 Resultados pregunta dos

Pregunta 3.- Mencione ¿Qué tipo de acto delictivo?

En la Tabla 2.5 se presenta el resultado de la pregunta 3 y en la Figura 2.7 se muestra los resultados en forma gráfica.

PREGUNTA 3	PORCENTAJE	CANTIDAD
Asalto	40,40%	122
Hurto	4,60%	14
Estafa	1,00%	3
Robo	53,60%	162
Secuestro	0,30%	1
Total	100%	**302**

Tabla 2.5 Resultados pregunta tres

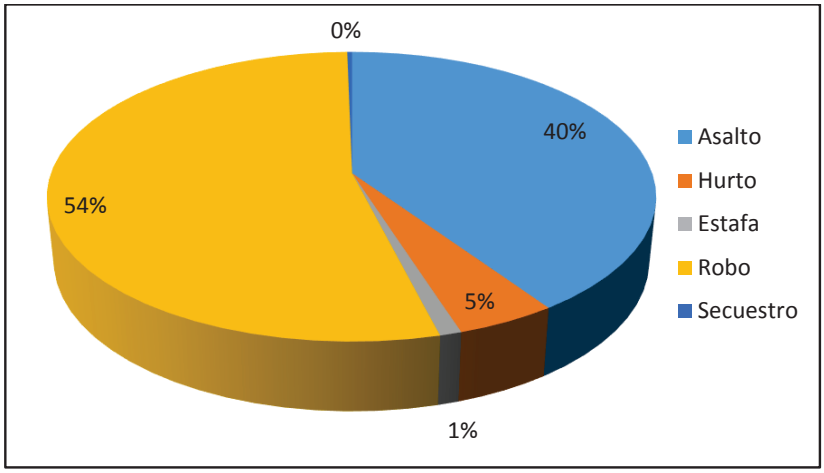


Figura 2.7 Resultados pregunta tres

Pregunta 4.- Mencione ¿En qué lugar o barrio sucedió?

En la Tabla 2.6 se presenta el resultado de la pregunta 4 y en la Figura 2.8 se muestra los resultados en forma gráfica.

PREGUNTA 4	PORCENTAJE	CANTIDAD
1 de Mayo	0,66%	2
Álvarez Chiriboga	16,89%	51
Amazonas	1,32%	4
Central	19,21%	58
Florida	23,51%	71
Fuera del Límite Urbano	7,28%	22
Girasoles	0,33%	1
La Playa	20,86%	63
Miraflores	0,66%	2
Patarata	1,99%	6
San Nicolás	0,99%	3
San Ruperto	0,66%	2
Sigsal	0,99%	3
Sur	4,64%	14
Total	**100%**	**302**

Tabla 2.6 Resultados pregunta cuatro

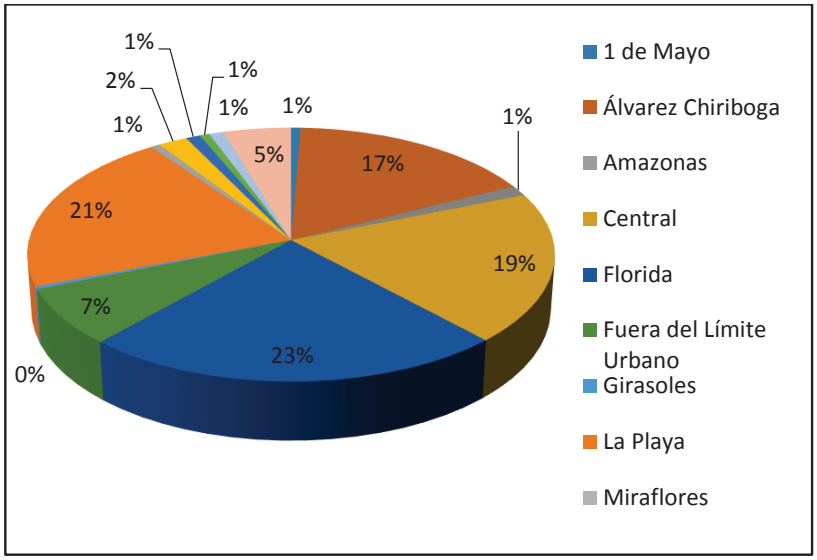


Figura 2.8 Resultados pregunta cuatro

El porcentaje y cantidad correspondiente al parámetro ¨*fuera del límite urbano*", corresponde al cometimiento de actos delictivos en barrios y lugares fuera del perímetro urbano de la ciudad de Cayambe.

Pregunta 5.- ¿Conoce usted qué es un sistema de video-vigilancia?

En la Tabla 2.7 se presenta el resultado de la pregunta 5 y en la Figura 2.9 se muestra los resultados en forma gráfica.

PREGUNTA 5	PORCENTAJE	CANTIDAD
No	40%	151
Si	60%	229
Total	**100%**	**380**

Tabla 2.7 Resultados pregunta cinco

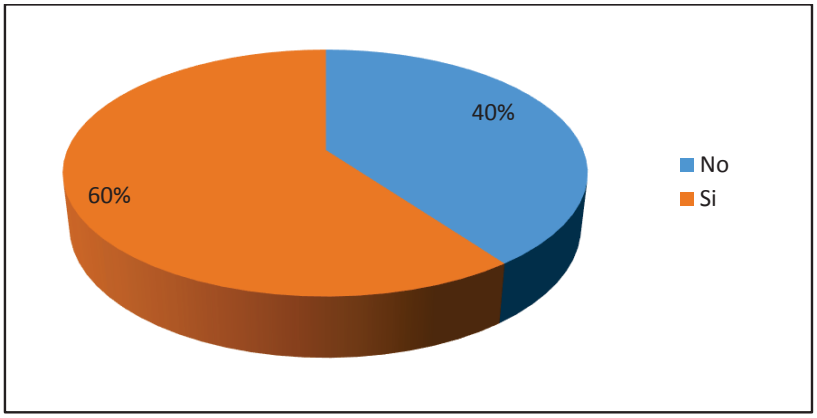


Figura 2.9 Resultados pregunta cinco

Pregunta 6.- ¿Estaría de acuerdo con la instalación de un sistema de video-vigilancia?

En la Tabla 2.8 se presenta el resultado de la pregunta 6 y en la Figura 2.10 se muestra los resultados en forma gráfica.

PREGUNTA 6	PORCENTAJE	CANTIDAD
No	2%	8
Si	98%	372
Total	**100%**	**380**

Tabla 2.8 Resultados pregunta seis

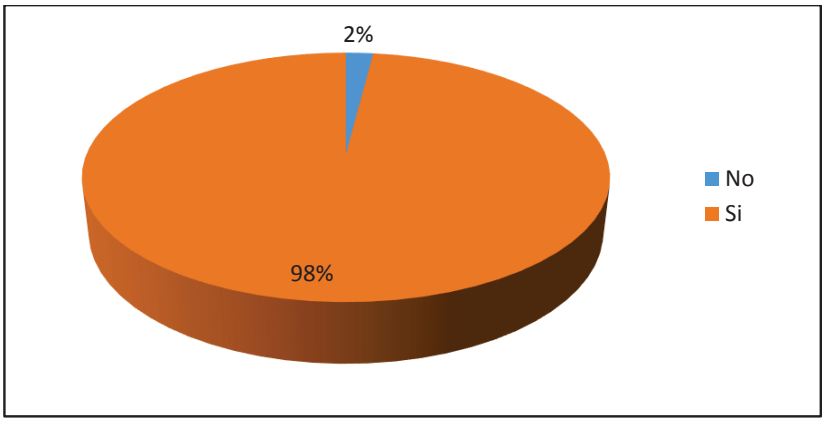


Figura 2.10 Resultados pregunta seis

Pregunta 7.- A su criterio ¿En cuál de estos sitios debería instalarse este sistema de video-vigilancia?

En la Tabla 2.9 se presenta el resultado de la pregunta 7 y en la Figura 2.11 se muestra los resultados en forma gráfica.

PREGUNTA 7	PORCENTAJE	CANTIDAD
Centros Educativos	9,47%	36
Lugares Públicos	3,95%	15
Principales vías públicas	5,79%	22
Todos	78,68%	299
Ningún lugar	2,11%	8
Total	**100,00%**	**380**

Tabla 2.9 Resultados pregunta siete

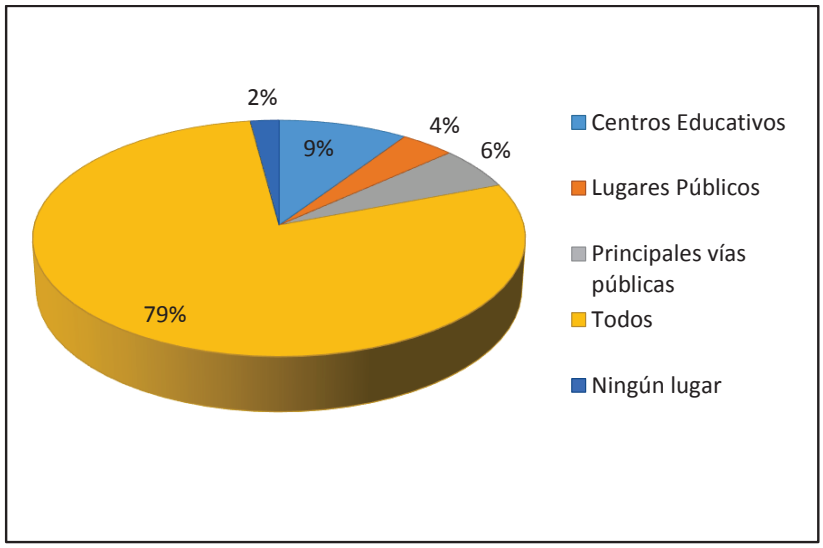


Figura 2.11 Resultados pregunta siete

Pregunta 8.- ¿Cree Usted, que con la ayuda de este sistema disminuya la delincuencia en la ciudad de Cayambe?

En la Tabla 2.10 se presenta el resultado de la pregunta 8 y en la Figura 2.12 se muestra los resultados en forma gráfica.

PREGUNTA 8	PORCENTAJE	CANTIDAD
No	3%	10
Si	97%	370
Total	**100%**	**380**

Tabla 2.10 Resultados pregunta ocho

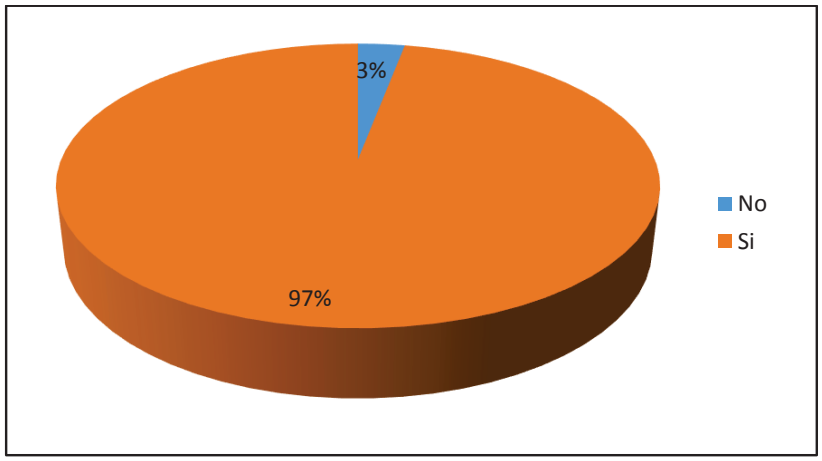


Figura 2.12 Resultados pregunta ocho

2.2.1.4 Conclusiones de la Encuesta

De acuerdo a los resultados obtenidos se puede concluir que más del 90% de la población percibe un nivel de inseguridad muy alto y considera que es necesaria la implementación del sistema de video-vigilancia, con lo cual se justifica el desarrollo del presente Proyecto de Titulación.

2.2.2 ENTREVISTA

Una entrevista es un dialogo establecido entre dos o más personas en las que existe un acuerdo previo acerca del tema, intereses y expectativas de ambos lados.

2.2.2.1 Objetivo de la Entrevista

El objetivo que se persigue con esta entrevista es obtener información acerca de los sitios y lugares que son más vulnerables y mayormente presa de actos delincuenciales. La entrevista se la realizará a los Agentes de la Policía Nacional quienes con su preparación, experiencia y sobre todo, conocedores de la inseguridad que aqueja a la población, serán de gran ayuda en la recolección de estos datos.

2.2.2.2 Desarrollo de la Entrevista

La entrevista es realizada al Teniente Erwin Vladimir Dávila Sánchez, Oficial Operativo, Área de Inteligencia, Policía Comunitaria del Distrito Cayambe y Pedro Moncayo, quien tiene mucha experiencia en el tema Policías Comunitarias y lleva trabajando en la ciudad de Cayambe alrededor de 5 años.

Pregunta 1.- La inseguridad es un problema palpable en las ciudades, ya sean grandes o pequeñas, la inseguridad es causada por muchos factores. ¿Cuáles vienen a ser los factores que inciden en el desarrollo de este problema social?

Respuesta: Lamentablemente la seguridad ya no es un derecho como lo manifiesta la Constitución de la República sino más bien, es un privilegio o un lujo en la actualidad uno de los principales factores que influye en la inseguridad es la alta demanda de población emigrante nacional y extranjera por las gran variedad de florícolas

Pregunta 2.- ¿Cuáles son los cambios o los problemas que ocasiona la inseguridad, y de qué forma han sido las transformaciones que se han vivido en el cantón por este problema?

Respuesta: La inseguridad ha traído una percepción principalmente en la ciudadanía de temor al trasladarse a sus domicilios, de un lugar a otro a diferentes horas del día o en la noche ya que pueden ser objeto de un robo, asalto, una violación, pelea, riña o de un acto violento como ha sucedido. Esto

causa un temor en la sociedad en general de ser víctima de un delito afectando el normal desenvolvimiento de sus actividades.

Pregunta 3.- ¿Cuál es el nivel, datos sobre la inseguridad que ha sufrido en el último año el cantón y sobre qué directrices trabaja en la inseguridad, como asaltos, robos, venta de drogas, etc., a su vez cuál es su nivel de incidencia?

Respuesta: Los principales problemas en la actualidad son: asaltos en carreteras, robos a domicilios, robos a personas y un incremento en homicidios.

En lo referente a directrices nosotros hacemos un análisis y una georreferenciación del delito para en base a esto procedemos realizar estrategias de prevención contra los diferentes tipo de actos delictivos

Cayambe a pesar de ser una ciudad en desarrollo presenta índices bastante grandes referentes a delincuencia en especial con las drogas.

El nivel de datos sobre la inseguridad los podrán analizar minuciosamente y con mayor precisión con el CMI[13]

Pregunta 4.- Se pueden notar lugares específicos en la ciudad, donde esta problemática es más latente, es decir, los barrios y zonas más vulnerables en el sector urbano de la ciudad, ¿cuáles son estas zonas?

Respuesta: Corresponde a barrios como la Florida I y Florida II. Allí hay una alta demanda de vivienda de ciudadanos que vienen de otros lugares del país.

La calle principal Rocafuerte, por el hecho de ser comercial se ha tornado bastante peligrosa sin olvidar el parque central y el mercado.

Pregunta 5.- ¿Qué son los sistemas de prevención, desde cuando se utilizan?

---

[13] CMI.- Cuadro de Mando Integral, Es el sistema empleado por la Policía Nacional para el ataque a la delincuencia, en el cual se toma en cuenta los delitos de mayor incidencia. Los delitos son controlados mensualmente en base a estadísticas y en base a estas estadísticas se aplican estrategias para la prevención, control y solución de estos problemas

Respuesta: Conjunto de medidas con la finalidad de evitar ciertos actos delictivos, aquí en Cayambe hemos tomado ciertas medidas en especial a lo referente a drogas en centros educativos como son campañas de concientización a los estudiantes de las diferentes instituciones.

Y sin olvidar otro problema que aqueja a la ciudanía como son los asaltos y robos es por esto que hemos realizado algunas charlas a los cayambeños y operativos en los lugares de mayor afluencia de personas.

Pregunta 6.- ¿Cómo se emplean estos sistemas de prevención y cuál es el medio de aplicación en Cayambe?

Respuesta: Hemos realizado stand y campañas en la ciudad de Cayambe donde hemos dado medidas de prevención con cierta información adicional para no ser víctimas de la delincuencia.

También ubicamos motos y patrullas en lugares estratégicos de la ciudad, en especial bancos y gasolineras. Realizamos también operativos en discotecas y bares con el fin de prevenir el ingreso de menores de edad, personas con armas y ventas de drogas

Pregunta 7.- El nivel de inseguridad donde se presenta más, ya hablamos de zonas geográficas, se puede delimitar otros escenarios, ya sean horarios (día o noche) y también acercarnos hacia lugares definidos donde pueda o se presente inseguridad.

Respuesta: El nivel de inseguridad está concentrado en sector norte de la ciudad, el parque central y el mercado diario en horas pico de 10:00 a.m. a 1:00p.m. Además según los datos reflejados por el CMI hay un alto nivel de robos los días domingo y lunes.

Pregunta 8.- ¿Cómo se ha presentado la venta ilegal de drogas, desde cuando se tiene estadísticas sobre el tema?

Respuesta: En lo referente a la venta ilegal de drogas desde febrero del año pasado (2012) tenemos decomisos de drogas. En Cayambe tenemos el micro

tráfico de drogas, los expendedores se dan modos para conseguir drogas de otras partes del país en especial de la Concordia.

Pregunta 9.- ¿Cuáles son los sectores vulnerables y cuáles son los lugares donde se dispersa la droga?

Respuesta: Barrios como la Florida I y la Florida II, el sector de los Túneles, el parque Nazacota Puento, el parque Central son los sectores más vulnerables y a lo referente de la dispersión de drogas son discotecas y centros educativos en las que hay una gran afluencia de personas las afueras de estos lugares.

Pregunta 10.- Es verdad que dentro de los centros educativos, también se encuentra este problema, ¿desde cuándo se tiene noción sobre esto y qué medidas se han tomado?

Respuesta: Tenemos noción de esto desde el año anterior (2012), nosotros nos acercamos a estas instituciones junto a autoridades del plantel en vista de la preocupación por el alto consumo de drogas en los estudiantes. Es por eso que la Policía Nacional contribuye realizando capacitaciones y mediante operativos de inteligencia se logró detectar por medio de grabaciones y fotografías a ciertos estudiantes de 14, 15 y 16 años comprando dosis de drogas.

Pregunta 11.- ¿Se han dado denuncias de algún tipo incidentes en paradas de autobuses, cuáles han sido, y de qué grupo social provienen más (hombre o mujeres)?

Respuesta: A lo referente a parada autobuses no hemos reflejado ningún problema, el problema se da más lo que viene a ser el trayecto de los señores transportistas. En donde los delincuentes se hacen pasar por vendedores ambulantes para hacer sus fechorías.

Pregunta 12.- ¿Cuál es el nivel de inseguridad en los centros de diversión nocturna, de qué forma son, a que grupos atañe más (hombre o mujeres)?

Respuesta: Nosotros como otras ciudades no tenemos un lugar específico o un punto de tolerancia para estos centros de diversión donde podríamos trabajar y

apuntar todos los esfuerzos, pero estos centros en la ciudad de Cayambe se encuentran dispersos por toda la ciudad.

Los centros de diversión ocasionan una gran inseguridad para los ciudadanos dentro y fuera de ellos

Pregunta 13.- El sistema de video-vigilancia pretende prevenir la inseguridad pero con la finalidad de que el sistema sea indebidamente manipulado por terceras personas ¿El monitoreo del sistema podría ser ubicado en la Policía Nacional?

Respuesta: Lo que nosotros queremos es una respuesta inmediata o prevenir un delito, en base a esto, podríamos hacer una mini central aquí, ya que contamos con el espacio suficiente para implementar un cuarto especial donde estén ubicados los equipos. Esto sería bastante bueno.

Pregunta 14.- ¿La aplicación de este sistema de video-vigilancia según su experiencia será de ayuda para contrarrestar la delincuencia en Cayambe?

Respuesta: Claro que si nosotros hemos realizado gestiones para la realización de un sistema de video-vigilancia pero hasta ahora no se ha podido agilitar este proceso. Actualmente existen 3 cámaras del sistema ECU 911 aquí, el problema que se tiene con este sistema es que el número de cámaras no abastece y que los monitores se encuentran en la ciudad de Quito por lo que no es de gran ayuda para nosotros.

Existen lugares donde se tienen un gran porcentaje de inseguridad y que deberían tener un sistema de video-vigilancia como este.

2.2.2.3 Conclusiones de la Entrevista

De la entrevista realizada se puede obtener datos que son de mucha importancia para la realización de este proyecto, los cuales se citan a continuación:

- Es innegable el grado de inseguridad que afecta a la ciudad

- Robos, asaltos y venta de drogas son problemas de todos los días
- Existen barrios y lugares que presentan mayor índice delincuencial.
- Las cámaras instaladas del sistema ECU 911 no abastecen y no prestan la funcionalidad que se necesita, debido a que el centro de monitoreo no se encuentra en esta ciudad, limitando así, la capacidad de reacción.
- Es necesario la implementación de un sistema de video-vigilancia que su centro de control se encuentre físicamente en la ciudad.

2.3 REQUERIMIENTOS PARA EL DISEÑO DEL SISTEMA DE VIDEO-VIGILANCIA

De acuerdo a los resultados obtenidos en los numerales precedentes, es necesario contar con un sistema de video-vigilancia que cumpla con los siguientes requerimientos:

- ✓ Video-vigilancia en tiempo real y sin interrupciones.
- ✓ Monitoreo constante las 24 horas del día, los 365 días del año.
- ✓ Almacenamiento de videos por lo menos de tres meses atrás.
- ✓ Acceso remoto a las imágenes desde cualquier lugar
- ✓ Seguridad en la información.
- ✓ Resolución de imágenes de calidad (cámaras de red con resolución en megapíxeles)
- ✓ Grabación de eventos tanto diurnos como nocturnos.

CAPÍTULO 3
DISEÑO DEL SISTEMA DE VIDEO-VIGILANCIA Y DETERMINACIÓN DE COSTOS REFERENCIALES

3.1 INTRODUCCIÓN

En este capítulo se presenta el diseño del sistema de video-vigilancia, los lugares en los cuales serían colocadas las cámaras, esto en función de los resultados de las encuestas y la entrevista presentada en el Capítulo dos. Además se determina el sistema para la gestión y administración y se presenta una comparativa de equipos de los cuales se escogen los que mejor se adapten a las necesidades del sistema.

Adicional a esto, se presenta una simulación de la red con las características de los equipos designados y el costo referencial que implicaría la implementación de este Proyecto.

3.2 DETERMINACIÓN DE LAS ZONAS DE RIESGO

De acuerdo a los resultados de las encuestas realizadas a los moradores de la Ciudad de Cayambe y a la entrevista realizada al Teniente Erwin Vladimir Dávila Sánchez, de la Policía Nacional, presentados en el capítulo dos, se determinan los sectores de mayor vulnerabilidad dentro del perímetro urbano de la ciudad de Cayambe. Estos sectores han sido agrupados de acuerdo al barrio al que pertenecen, tal como lo muestra la Tabla 3.1, en la cual se hace una clasificación de acuerdo a su nivel de inseguridad.

N°	BARRIOS URBANOS	NIVEL DE INSEGURIDAD	N°	BARRIOS URBANOS	NIVEL DE INSEGURIDAD
1	Santa Marianita de Granobles	Bajo	22	Bolívar	Medio
2	23 De Julio	Bajo	23	La Obrera	Medio
3	Amazonas	Medio	24	Central	Alto
4	Santa Laura De Changalá	Medio	25	Florida I	Alto
5	Changalá	Bajo	26	Florida II	Alto
6	Sigsal Bajo	Bajo	27	1 De Mayo	Bajo
7	Víctor Cartagena	Bajo	28	Álvarez y Chiriboga	Alto
8	Sandra Pérez	Bajo	29	La Playa	Alto
9	El Sigsal	Medio	30	San Pedro	Alto
10	Lucila Cartagena	Medio	31	El Obraje	Bajo
11	La Estación	Medio	32	Bellavista De Cruz Loma	Bajo
12	Une	Medio	33	San Carlos	Bajo
13	Miraflores	Medio	34	Bellavista de Puntiachil	Bajo
14	Las Orquídeas	Medio	35	Sur	Medio
15	Nuevos Horizontes	Medio	36	La Cruz	Medio
16	San Ruperto	Medio	37	Puntiachil	Bajo
17	Hacienda Primavera	Bajo	38	Chimborazo	Bajo
18	Girasoles	Medio	39	San Nicolás	Bajo
19	Sara Jarrín	Medio	40	Don Bosco	Bajo
20	Patarata	Medio	41	4 Esquinas	Medio
21	Verde Pamba	Medio			

Tabla 3.1 Nivel de inseguridad en barrios urbanos

Los barrios catalogados con niveles de inseguridad medio, contienen los parques recreacionales, las calles principales, las entidades públicas y privadas y los centros de estudio. En los barrios con un nivel de inseguridad bajo, no será necesario la colocación de cámaras de video-vigilancia. El resto de barrios están catalogados con un nivel de inseguridad alto, debido a que en estos lugares es donde se han cometido la mayoría de actos delictivos.

Para tener una idea de la ubicación de los barrios de acuerdo a la clasificación que se les ha dado en la Tabla 3.1, se presenta la Figura 3.1.

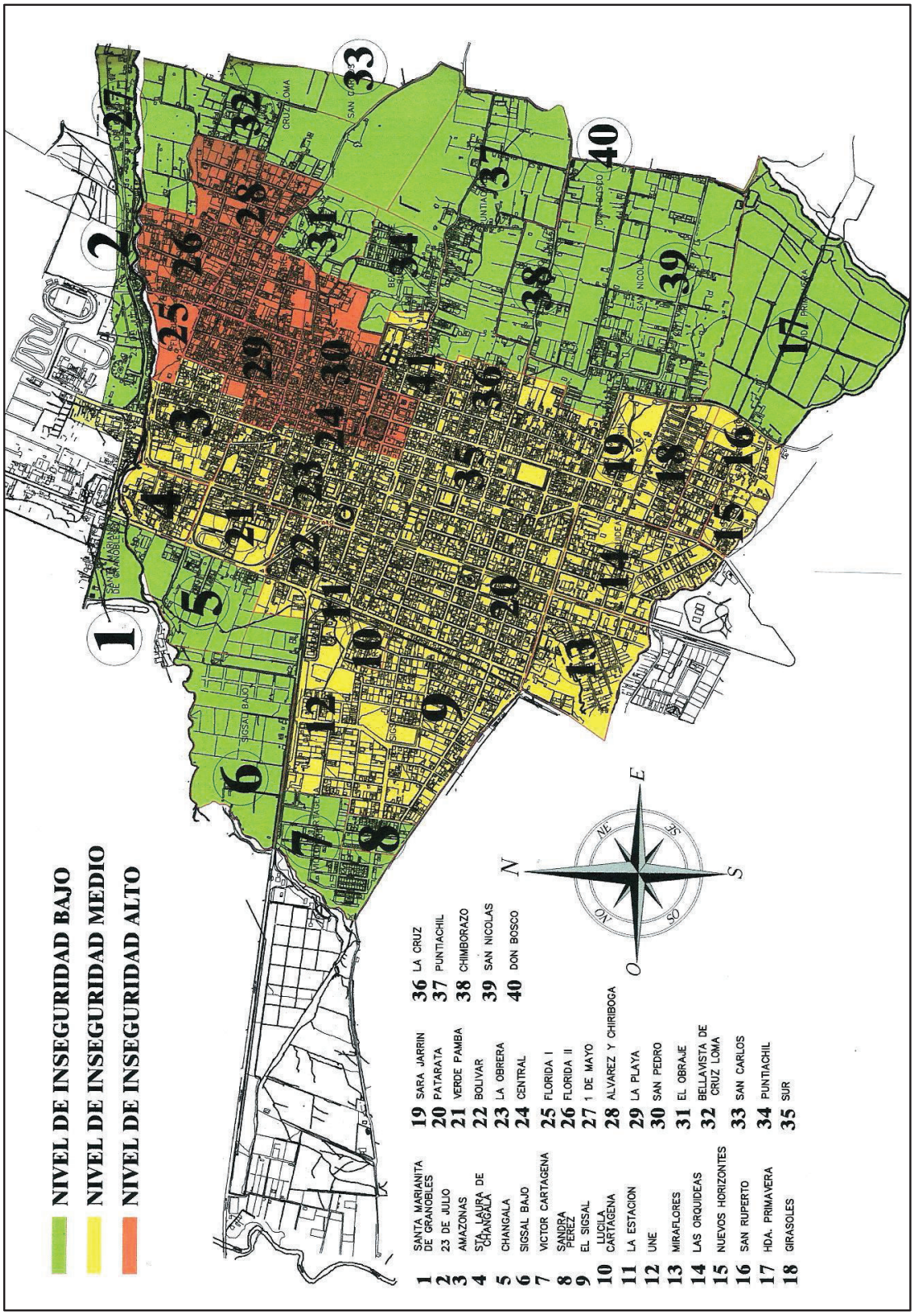


Figura 3.1 Ubicación de barrios de acuerdo a su nivel de inseguridad

3.2.1 UBICACIÓN DE LAS CÁMARAS DE VIGILANCIA

Un sistema de video-vigilancia es un sistema disuasivo, muchos delincuentes al notar la presencia de este tipo de cámaras se abstienen de realizar fechorías, por tal motivo, resulta innecesario colocar cámaras de vigilancia en todas las calles de la ciudad.

Luego de realizar un análisis visual de la ciudad y basándonos en la información de la Tabla 3.1, se ha determinado los lugares en los cuales resultaría adecuado la colocación de cámaras de vigilancia. Para el presente Proyecto se utilizarán cámaras de red del tipo domo PTZ debido a los beneficios que este tipo de cámaras ofrecen.

Por medio del programa Google Earth se ha obtenido las coordenadas de los lugares en donde serían colocadas las cámaras de vigilancia. En la Tabla 3.2 se muestra esta información y en la Figura 3.2 se presenta la ubicación física de estos puntos en la ciudad.

N°	CÁMARAS DE RED TIPO DOMO PTZ		
	LATITUD	LONGITUD	REFERENCIA
1	0° 2'32.89"N	78° 8'45.17"O	Redondel Plaza de Toros
2	0° 2'40.18"N	78° 8'42.86"O	Col. Salesiano y Natalia Jarrín
3	0° 2'53.86"N	78° 8'33.53"O	Puente Rio Blanco
4	0° 2'49.24"N	78° 8'47.57"O	Escuela Samuel Beckett
5	0° 2'26.95"N	78° 8'29.85"O	Policía Comunitaria
6	0° 2'3.50"N	78° 8'43.09"O	Hospital
7	0° 2'39.89"N	78° 8'34.98"O	Parque Nasacota Puento
8	0° 2'47.58"N	78° 8'19.98"O	Escuela Mariana de Jesús
9	0° 2'45.63"N	78° 8'31.00"O	Mercado Dominical
10	0° 2'36.44"N	78° 8'33.37"O	Calle Rocafuerte y Vivar
11	0° 2'26.69"N	78° 8'36.19"O	Parque Central
12	0° 2'20.08"N	78° 8'41.21"O	Escuela Himmelmann
13	0° 2'33.37"N	78° 8'39.85"O	Escuela Crespo Toral
14	0° 2'17.21"N	78° 8'50.55"O	Parque Rubén Rodríguez
15	0° 2'24.99"N	78° 8'39.20"O	Mercado Diario

Tabla 3.2 Ubicación cámaras de vigilancia

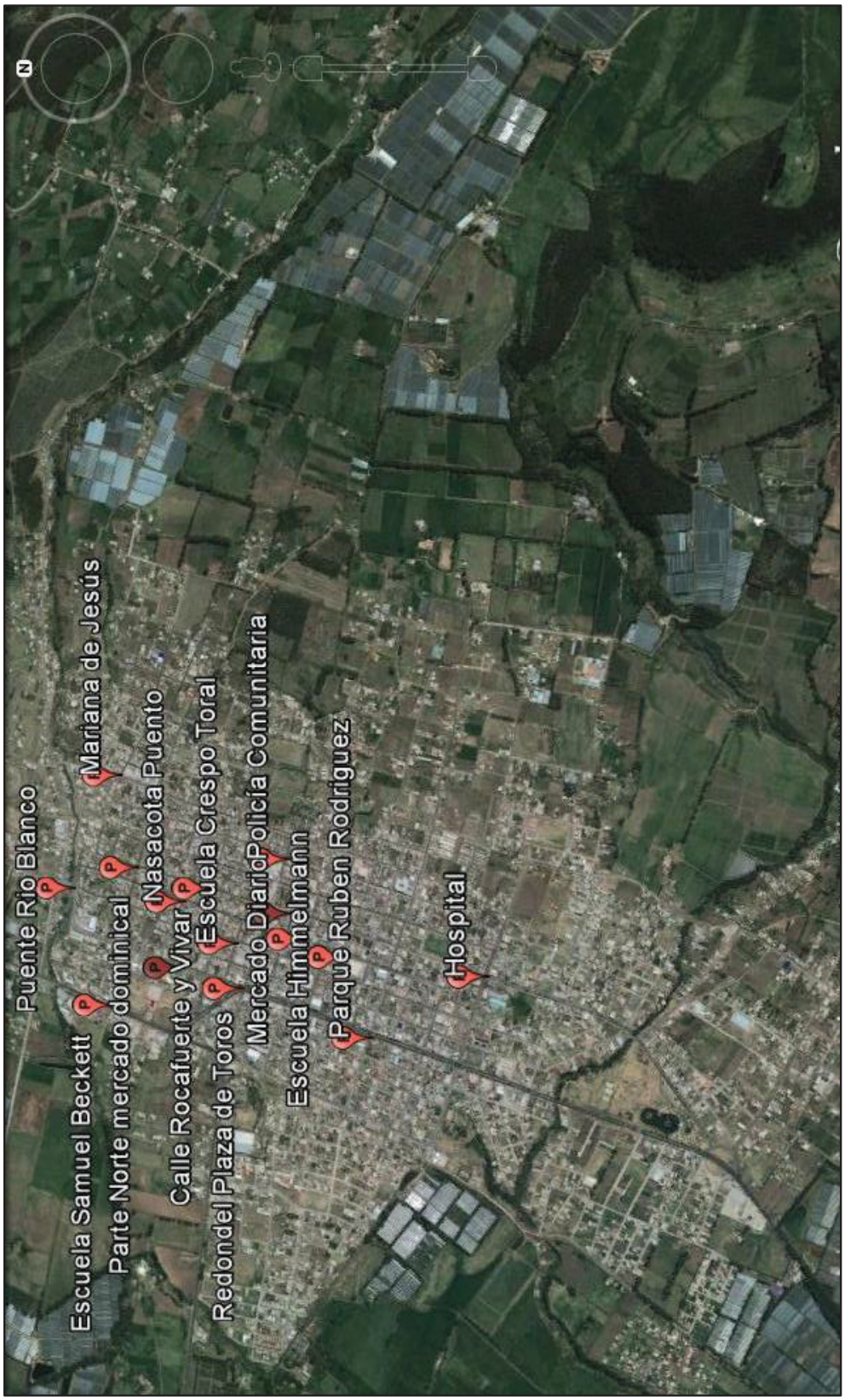


Figura 3.2 Ubicación física de cámaras de vigilancia en la ciudad Cayambe

3.3 BOSQUEJO DEL SISTEMA DE VIDEO-VIGILANCIA A DISEÑARSE

Por medio de la Figura 3.3 se pretende dar una clara idea del esquema de funcionamiento del sistema de video-vigilancia.

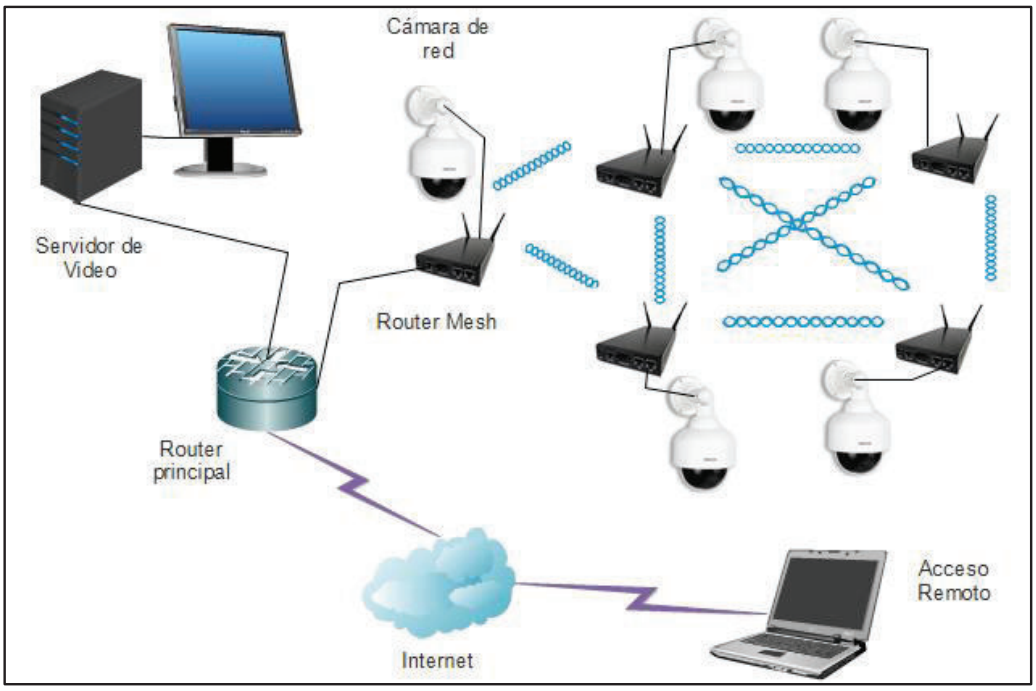


Figura 3.3 Bosquejo del sistema de video-vigilancia

En la Figura 3.3, las cámaras de red se conectan a uno de los puertos Ethernet de los enrutadores mesh, de esta manera, las imágenes y videos capturados se transmitirán de manera inalámbrica hacia el servidor de video.

Para el servidor de video se utilizará un equipo NVR debido a los requerimientos de almacenamiento de información mencionados en el Cap. 2. El equipo NVR también realizará las funciones de gestión y administración del sistema de video-vigilancia.

Para el acceso remoto a las imágenes de las cámaras IP, es necesario la contratación de los servicios de un proveedor de Internet, el mismo que debe proporcionar un equipo enrutador en el cual se pueda configurar un firewall para la seguridad de la red.

3.4 DETERMINACIÓN DE LA RED DE DATOS [1] [29] [31]

De acuerdo al tema de este Proyecto y luego de haber visto en el Cap.1 sobre las tecnologías de transmisión inalámbricas utilizadas en sistemas de video-vigilancia, se tiene claro que la mejor opción para el desarrollo de este Proyecto es emplear una red mallada inalámbrica basada en los estándares IEEE 802.11. De esta manera se podrá garantizar un sistema de video-vigilancia redundante, fiable y seguro.

Para la trasmisión de datos se utilizará el estándar 802.11n operando en la banda de frecuencia libre de 5 GHz, para esto, es necesario recurrir a la normativa oficial de Ecuador en lo concerniente a bandas libres.

En la resolución TEL-560-18 emitida por la CONATEL en el 2010, la banda libre de 5 GHz, va desde 5725 a 5850 MHz. En la Figura 3.4 se muestra la coexistencia entre los canales de 20 y 40 MHz.

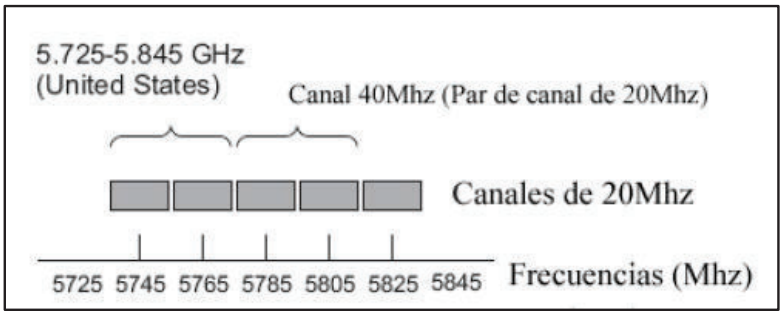


Figura 3.4 Coexistencia de canales en la banda de 5 GHz [29]

Se ha escogido el estándar 802.11n debido a que presenta mayores velocidades de transmisión que los estándares anteriores (802.11 a/b/g) y la banda de 5 GHz,

porque es menos saturada y presenta menos problemas de interferencias que la banda de 2.4 GHz.

La ubicación de los nodos mesh será la misma establecida para las cámaras IP, debido a que los nodos se conectarán directamente a las cámaras y de esta manera, se emula la conexión de cámaras IP inalámbricas.

3.4.1 ESTIMACIÓN DEL TRÁFICO DE RED

La estimación del tráfico de red es un tema muy importante en este diseño, debido a que se necesita garantizar que toda la carga de videos provenientes de las cámaras de vigilancia pueda viajar sin problemas ni retrasos por la red y de esta manera obtener imágenes de buena calidad en tiempo real y sin cortes, por lo tanto, se realizará una estimación del tráfico de red considerando que exista actividad todo el tiempo.

Una vez conocido el número de cámaras que se utilizarán en este Proyecto, por medio de la Ecuación 3.1, se obtendrá el valor del tráfico que generará el sistema de video-vigilancia.

$$Tráfico\ Total\ [Mbps] = Tamaño\ de\ un\ cuadro\left[\frac{KB}{cuadro}\right] * \left[\frac{1MB}{1024\ KB}\right] * \left[\frac{8bits}{1\ Byte}\right] * FPS\left[\frac{cuadro}{segundo}\right] * \%\ Actividad * \#\ Cámaras$$

Ecuación. 3.1 [31]

Donde:

- Tamaño de cuadro = Se obtiene por medio de los valores de compresión y resolución de video, depende de la iluminación de un lugar y su unidad de medida es el KB. De acuerdo a los requerimientos del sistema presentados en el Cap. 2, para este Proyecto se necesitan cámaras IP que

transmitan imágenes de calidad, por lo que se ha pensado en cámaras con una resolución de 3 Megapíxel y que soporten el protocolo H.264.

Por medio de la Tabla 3.3 se obtiene el valor del tamaño de cuadro cuyo valor es de 45 KB.

RESOLUCIÓN	COMPRESIÓN DE VIDEO			
	H264-10 CALIDAD ALTA	H264-20 CALIDAD BUENA	H264-30 CALIDAD MEDIA	H264-50 CALIDAD BAJA
320x240(QVGA)	1KB	1KB	1KB	1KB
352x240(CIF NTSC)	1KB	1KB	1KB	1KB
352x288(CIF PAL)	1KB	1KB	1KB	1KB
480x360	3KB	2KB	1KB	2KB
640x480(VGA)	4KB	3KB	3KB	3KB
704x240(2CIF NTSC)	3KB	2KB	1KB	2KB
704x288(2CIF PAL)	3KB	2KB	2KB	2KB
704x480(4CIF NTSC)	5KB	4KB	3KB	3KB
704x576(4CIF PAL)	6KB	5KB	4KB	4KB
800x600(SVGA)	7KB	5KB	4KB	5KB
1280x720(HD)	13KB	10KB	9KB	9KB
1280x960(1.22MP)	18KB	14KB	11KB	12KB
1280x1024(1.3MP)	19KB	14KB	12KB	12KB
1600x1200(2MP)	27KB	21KB	18KB	19KB
1920x1080(Full HD)	30KB	23KB	19KB	20KB
2048x1536(3MP)	45KB	35KB	29KB	30KB
2288x1712(4MP)	56KB	44KB	36KB	38KB
2600x1950(5MP)	73KB	56KB	46KB	49KB

Tabla 3.3 Tamaño del cuadro para una compresión H.264 [1]

- FPS (*Frames per Second*) = La velocidad de imágenes es un valor variable que depende de la luminosidad del lugar en donde se encuentre ubicada la cámara y del movimiento que ésta tenga. Los fabricantes de cámaras indican en sus características los valores que soportan sus equipos. Valores típicos de FPS son 1, 5, 10, 15, 25 y 30.
  Para el presente diseño se utilizará un valor de 15 FPS, debido a que 15 cuadros por segundo son suficiente para poder analizar lo que sucede en una escena.

- % Actividad = También conocido como *"Motion",* es el porcentaje de actividad de la escena que indica cuanto cambia un cuadro respecto a otro. Se utilizará el valor del 100% (máximo posible)
- # Cámaras = Corresponde al número de cámaras que se emplearan en un sistema de video-vigilancia. En el presente diseño se utilizarán 15 cámaras IP.

Reemplazando los valores en la ecuación se tiene:

$$Tráfico\ Total\ [Mbps] = 45\left[\frac{KB}{cuadro}\right] * \left[\frac{1MB}{1024\ KB}\right] * \left[\frac{8\ bits}{1\ Byte}\right] * 15\left[\frac{cuadro}{segundo}\right] * 100\ \%\ Actividad * 15\ Cámaras$$

$$Tráfico\ Total\ [Mbps] = 79{,}1\ Mbps$$

Cabe recalcar que el valor de tráfico de real dependerá de las características que tengan los equipos a emplear.

3.5 DISEÑO DE RADIOENLACES [2] [27] [28] [30]

Para el diseño de radioenlaces se asumirá las peores condiciones, es decir, se diseñará enlaces punto a punto entre el nodo gateway (cámara 5) y el resto de nodos.

En una red mesh, cada nodo puede comunicarse con otro nodo cercano hasta alcanzar al nodo gateway (por medio de saltos), esto significa que las distancias de enlace planteadas en este diseño serían mucho menor en la práctica.

En la Tabla 3.4 se muestra la distancia entre el nodo gateway y el resto de nodos, así como la capacidad que debería soportar cada enlace.

ENLACE	DISTANCIA [Km]	TRÁFICO DE RED [Mbps]
Cámara 5 - Cámara 1	0,51	5,27
Cámara 5 - Cámara 2	0,57	5,27
Cámara 5 - Cámara 3	0,84	5,27
Cámara 5 - Cámara 4	0,88	5,27
Cámara 5 - Cámara 6	0,83	5,27
Cámara 5 - Cámara 7	0,43	5,27
Cámara 5 - Cámara 8	0,7	5,27
Cámara 5 - Cámara 9	0,58	5,27
Cámara 5 - Cámara 10	0,31	5,27
Cámara 5 - Cámara 11	0,2	5,27
Cámara 5 -Cámara 12	0,41	5,27
Cámara 5 -Cámara 13	0,37	5,27
Cámara 5 -Cámara 14	0,71	5,27
Cámara 5 -Cámara 15	0,29	5,27

Tabla 3.4 Enlaces punto-punto y capacidad de enlace

El valor de 5,27 Mbps resulta de la división del valor del tráfico total del sistema de video-vigilancia obtenido en la sección 3.4.1, para el número de cámaras IP a utilizar (15). Este valor resulta mucho menor a las capacidades de canal que permite manejar el estándar IEEE802.11n.

3.5.1 CÁLCULO DEL PRESUPUESTO DE ENLACE

Es el cálculo de las ganancias y pérdidas que se presentan en una comunicación inalámbrica desde el lado transmisor hasta el lado receptor, teniendo en cuenta las pérdidas que se generan tanto en conectores, cables y espacio libre.

El cálculo del presupuesto de enlace sirve para determinar la vialidad de un enlace, además, es de mucha ayuda para la elección de los equipos que se utilizarán en el mismo.

En el presente diseño, para el cálculo del presupuesto de enlace se asumirá una potencia de transmisión de 20 dBm debido a que la distancia a cubrir entre nodos no supera los 1000 m y una ganancia de antena omnidireccional de 12 dBi. El

valor de la potencia de transmisión cumple con la normativa vigente en el Ecuador (Resolución TEL-560-18 CONATEL 2010), en la cual se establece que la potencia pico máxima que puede ser utilizada por equipos para la transmisión de datos en la banda libre de 5 GHz es de 1000 mW o 30 dBm.

En la Figura 3.5 se muestra los elementos que intervienen en un presupuesto de enlace, más adelante se hablará de éstos elementos.

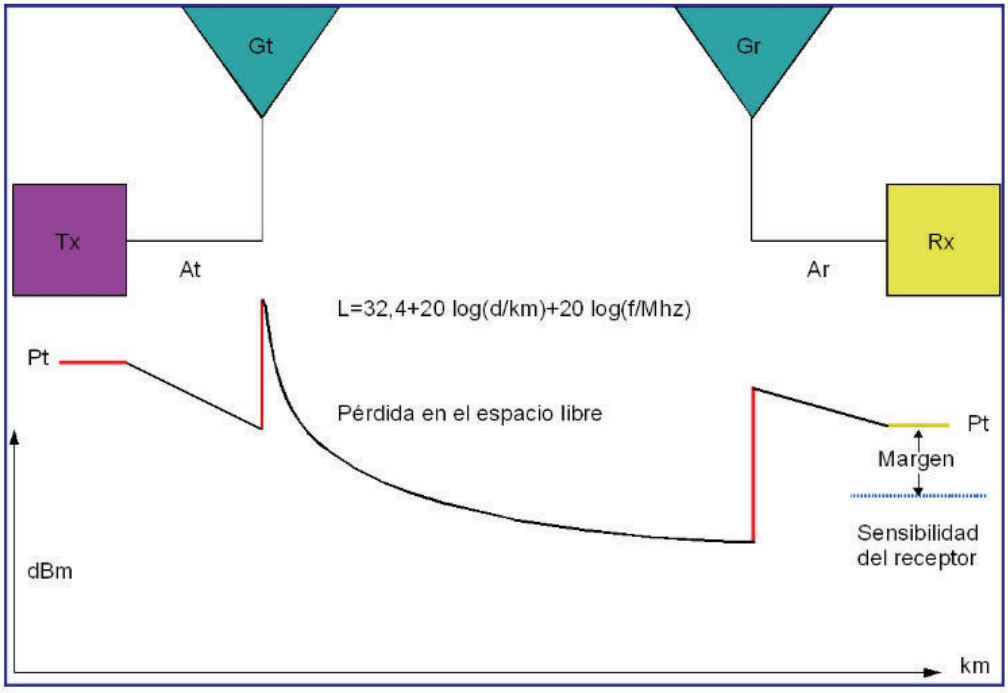


Figura 3.5 Elementos que intervienen en un presupuesto de enlace [30]

3.5.1.1 Pérdidas de propagación en espacio libre

Las ondas de radio pierden energía que se irradia en direcciones diferentes a las que puede captar la antena receptora. Las pérdidas en espacio libre miden la potencia de señal que se pierde en el espacio, ignorando cualquier otro tipo de obstáculo. Su fórmula de cálculo es la establecida en la Ecuación 3.2.

$$L_{FSL}\,[dB] = 20\log(f) + 20\log(d) + 32{,}4$$

Ecuación 3.2 [2]

Donde:

- f = Frecuencia [MHz].
- d = Distancia [Km].

Como ejemplo se presenta el cálculo de pérdidas de propagación desde la cámara 5 hasta la cámara 1.

$$L_{FSL} = 20\log(5745) + 20\log(0{,}51) + 32{,}4$$
$$L_{FSL} = 101{,}73[dB]$$

3.5.1.2 Potencia del receptor

Es la diferencia entre la potencia de transmisión y todas las pérdidas presentes en el enlace, estas pérdidas corresponden a cables de conexión y conectores presentes en el sistema de transmisión/recepción. Para el presente diseño se tomará como referencia el valor de 2 dB por pérdidas en cables y conectores en cada lado del enlace, debido a que la longitud de los cables que unirán las cámaras IP con los enrutadores no superará los 2 m.

Por medio de la Ecuación 3.3 se puede calcular la potencia de recepción.

$$P_{Rx}[dBm] = P_{Tx} + G_{Tx} - L_{Tx} + G_{Rx} - L_{Rx} - L_{FSL}$$

Ecuación 3.3 [2]

Donde:

- G_{Tx} = Ganancia de la antena de transmisión [dBi]
- L_{Tx} = Pérdidas de transmisión [dB]
- G_{Rx} = Ganancia de la antena de recepción [dBi]
- L_{Rx} = Pérdidas de recepción [dB]
- L_{FSL} = Pérdidas de propagación [dB]

Como ejemplo se presenta el cálculo de potencia de recepción en el enlace desde la cámara 5 hasta la cámara 1.

$$P_{Rx} = 20 + 12 - 2 + 12 - 2 - 101{,}73$$
$$P_{Rx} = -61{,}73\ [dBm]$$

3.5.1.3 Margen de desvanecimiento (FM)

Al propagarse una onda electromagnética por la atmósfera terrestre puede tener pérdidas intermitentes en la intensidad de la señal, además de la pérdida normal en la trayectoria. Estas pérdidas se conocen como desvanecimiento y se pueden atribuir a perturbaciones meteorológicas como: lluvia, nieve, granizo, etc.; a una superficie irregular del terreno y a múltiples trayectorias de transmisión.

Por medio de la Ecuación 3.4 se puede calcular el margen de desvanecimiento de una señal.

$$FM = 30\log(d) + 10\log(6 * A * B * f) - 10\log(1 - R) - 70$$

Ecuación 3.4 [2]

Donde:

- d = Distancia [Km]
- f = Frecuencia [MHz]
- A = Factor de rugosidad del terreno, en la Tabla 3.4 se muestran los valores posibles:

TIPO DE RUGOSIDAD	FACTOR
Espejos de agua, ríos muy anchos, etc.	4
Sembrados densos, pastizales, arenales	3
Bosques (la propagación va por encima)	2
Terreno normal	1
Terreno rocoso (muy desparejo)	0,25

Tabla 3.5 Factor de rugosidad del terreno [28]

- B = Factor climático, en la Tabla 3.5 se muestran los valores posibles:

ANÁLISIS CLIMÁTICO ANUAL	FACTOR
Área marina o condiciones de peor mes	1
Áreas cálidas y húmedas	0,5
Áreas mediterráneas de clima normal	0,25
Áreas montañosas de clima seco y fresco	0,125

Tabla 3.6 Factor de análisis climático anual [28]

- R = Confiabilidad de la conexión, se tomará un valor crítico en la disponibilidad del enlace, es decir 99,999%

Como ejemplo se presenta el cálculo del margen de desvanecimiento en el enlace desde la cámara 5 hasta la cámara 1.

$$FM = 30\log(0{,}51) + 10\log(6 * 1 * 0{,}125 * 5745) - 10\log(1 - 0{,}99999) - 70$$
$$FM = 7{,}57$$

3.5.1.4 Umbral de recepción

También conocido como sensibilidad del receptor, es el valor de potencia necesario para mantener una tasa de transferencia determinada en un enlace. Cuanto menor sea este valor, mejor será el equipo, ya que necesitará que le llegue menos potencia para trabajar correctamente (a una velocidad dada).

Por medio de la Ecuación 3.5 se puede calcular el umbral de recepción.

$$UR[dBm] = P_{Rx} - FM$$

Ecuación 3.5 [2]

Donde:

- P_{Rx} = Potencia de recepción [dBm]
- FM = Margen de desvanecimiento

Como ejemplo se presenta el cálculo del umbral de recepción en el enlace desde la cámara 5 hasta la cámara 1.

$$UR = -61{,}73 - 7{,}57$$
$$UR = -69{,}3\ [dBm]$$

3.5.1.5 Margen respecto al umbral

Es la cantidad de señal por encima de la sensibilidad del equipo que debería recibirse para garantizar un enlace estable y de alta calidad. Un margen de 10 a 15 dB garantiza un buen funcionamiento del enlace. Valores superiores a 15 dB proveen enlaces de gran calidad.

Por medio de la Ecuación 3.6 se puede calcular el umbral de recepción.

$$M_U[dB] = P_{Rx} - UR$$

Ecuación 3.6 [28]

Donde:

- P_{Rx} = Potencia de recepción [dBm]
- UR = Umbral de recepción [dBm]

Los valores de Margen respecto al umbral se determinarán una vez se haya elegido a los equipos que se utilizarán en los radioenlaces.

3.5.1.6 Zona de Fresnel

Es la zona de despeje que se debe tener en consideración, además de la vista directa entre antenas transmisoras y receptoras. Lo ideal es que la primera zona de Fresnel no se encuentre obstruida, sin embargo es suficiente despejar el 60% del radio de la primera zona para tener un enlace satisfactorio. En grandes

distancias es necesario tener en cuenta la curvatura de la Tierra. La Figura 3.6 muestra la primera zona de Fresnel en un radio enlace.

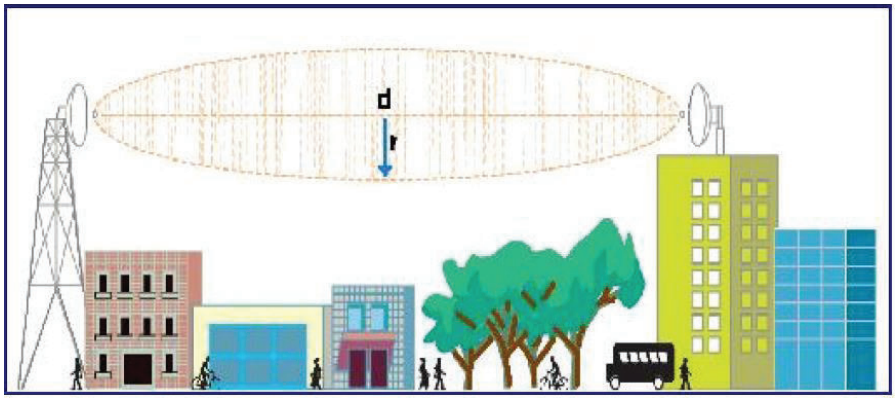


Figura 3.6 Zona de Fresnel [30]

Por medio de la Ecuación 3.7 se puede calcular la primera zona de Fresnel:

$$r = 17{,}32 * \sqrt{\left(\frac{d1 * d2}{d * f}\right)}$$

Ecuación 3.7 [30]

Dónde:

- d1= Distancia al obstáculo desde el transmisor [Km].
- d2= Distancia al obstáculo desde el receptor [Km].
- d = Distancia entre el transmisor y el receptor [Km].
- f = Frecuencia [GHz].
- r = Radio [m].

Los valores de la zona de Fresnel se determinarán más adelante en una simulación con los valores reales de los equipos que se utilizarán en los radioenlaces.

En la Tabla 3.7 se muestran algunos parámetros necesarios para la selección de los equipos que se utilizarán en los radioenlaces (potencia de transmisión y ganancia de las antenas) luego de hacer el presupuesto de enlace entre el nodo gateway (cámara 5) y el resto de nodos. En el caso de los valores de umbral de

recepción, se tomará el menor valor como requerimiento para la selección de equipos.

ENLACE	DISTANCIA [Km]	FRECUENCIA [MHz]	PÉRDIDAS EN ESPACIO LIBRE [dB]	MARGEN DE DESVANECIMIENTO	POTENCIA DE Rx [dBm]	UMBRAL DE RECEPCIÓN [dBm]
Cámara 5 - Cámara 1	0,51	5745	101,74	7,57	-61,74	-69,31
Cámara 5 - Cámara 2	0,57	5745	102,70	9,02	-62,70	-71,72
Cámara 5 - Cámara 3	0,84	5745	106,07	14,07	-66,07	-80,14
Cámara 5 - Cámara 4	0,88	5745	106,48	14,68	-66,48	-81,15
Cámara 5 - Cámara 6	0,83	5745	105,97	13,92	-65,97	-79,88
Cámara 5 - Cámara 7	0,43	5745	100,26	5,35	-60,26	-65,60
Cámara 5 - Cámara 8	0,7	5745	104,49	11,70	-64,49	-76,18
Cámara 5 - Cámara 9	0,58	5745	102,85	9,25	-62,85	-72,10
Cámara 5 - Cámara 10	0,31	5745	97,41	1,08	-57,41	-58,50
Cámara 5 - Cámara 11	0,2	5745	93,61	-4,63	-53,61	-48,98
Cámara 5 -Cámara 12	0,41	5745	99,84	4,73	-59,84	-64,57
Cámara 5 -Cámara 13	0,37	5745	98,95	3,39	-58,95	-62,34
Cámara 5 -Cámara 14	0,71	5745	104,61	11,88	-64,61	-76,49
Cámara 5 -Cámara 15	0,29	5745	96,83	0,22	-56,83	-57,05

Tabla 3.7 Parámetros de los enlaces entre el nodo gateway y el resto de nodos

3.6 DIMENSIONAMIENTO DEL SERVIDOR DE ALMACENAMIENTO DE VIDEO [1] [31]

De acuerdo a los requerimientos del sistema de video-vigilancia, es necesario guardar las grabaciones de video por un tiempo de tres meses, luego de transcurrido este tiempo las grabaciones serán borradas de manera automática, lo que liberaría espacio para nuevas grabaciones. Por tal motivo, es necesario obtener el valor aproximado del espacio en disco duro que se necesitaría esté disponible para poder cumplir con este requerimiento.

La grabación de videos se realizará de manera automática, siempre y cuando existan eventos. Sin embargo se calculará el espacio necesario en disco duro para las peores condiciones, es decir, considerando que esté grabando todo el tiempo y sin interrupciones.

Para poder dimensionar el tamaño en disco duro es necesario conocer previamente la cantidad de tráfico generado por el sistema y a este valor multiplicarlo por el tiempo total de grabación, tal como puede verse en la Ecuación 3.8.

$$Tamaño\ Disco\ Duro[GB] = Tráfico\ total\ [Mbps] * tiempo\ grabación[segundo] * \left[\frac{1\ Byte}{8\ bits}\right] * \left[\frac{1\ GB}{1024\ MB}\right]$$

Ecuación 3.8 [1]

Donde:

- Tráfico total [Mbps]: Para las grabaciones video se calculará un nuevo valor de tráfico total con un valor de 5 FPS, con la finalidad de optimizar recursos.
- Tiempo de grabación: 3 meses ≈ 7257600 segundos.

Reemplazando los valores en la ecuación se tiene:

$$Tamaño\ Disco\ Duro[GB] = 26{,}3\ [Mbps] * 7257600[segundo] * \left[\frac{1\ Byte}{8\ bits}\right] * \left[\frac{1\ GB}{1024\ MB}\right]$$

De acuerdo al resultado obtenido, se necesitará contar con un equipo NVR que disponga de la capacidad de almacenamiento de 22,7 TB

3.7 DIRECCIONAMIENTO IP [1]

El sistema de video-vigilancia se encuentra dentro de una red LAN, por lo tanto, es necesario asignar direcciones de red privadas a los equipos que conforman el sistema.

En este diseño se utilizará la red de clase C: 192.168.0.0/16. Se utilizará también VLSM (*Variable Length Subnet Mask*) para el direccionamiento de los equipos, con la finalidad de ahorrar direcciones y brindar una mayor seguridad al sistema.

En la Figura 3.7 se muestra el diagrama de red a diseñar con sus respectivas subredes, las cuales se detallan en la Tabla 3.8.

SUBRED	DESCRIPCIÓN	# DIRECCIONES
1	Router Principal – Router Mesh	2
2	Router Principal – Servidor de Video	2
3	Red Mesh (Router Mesh – Router Mesh)	15
4	Router Mesh – Cámaras de red	30

Tabla 3.8 Subredes y número de direcciones necesarias

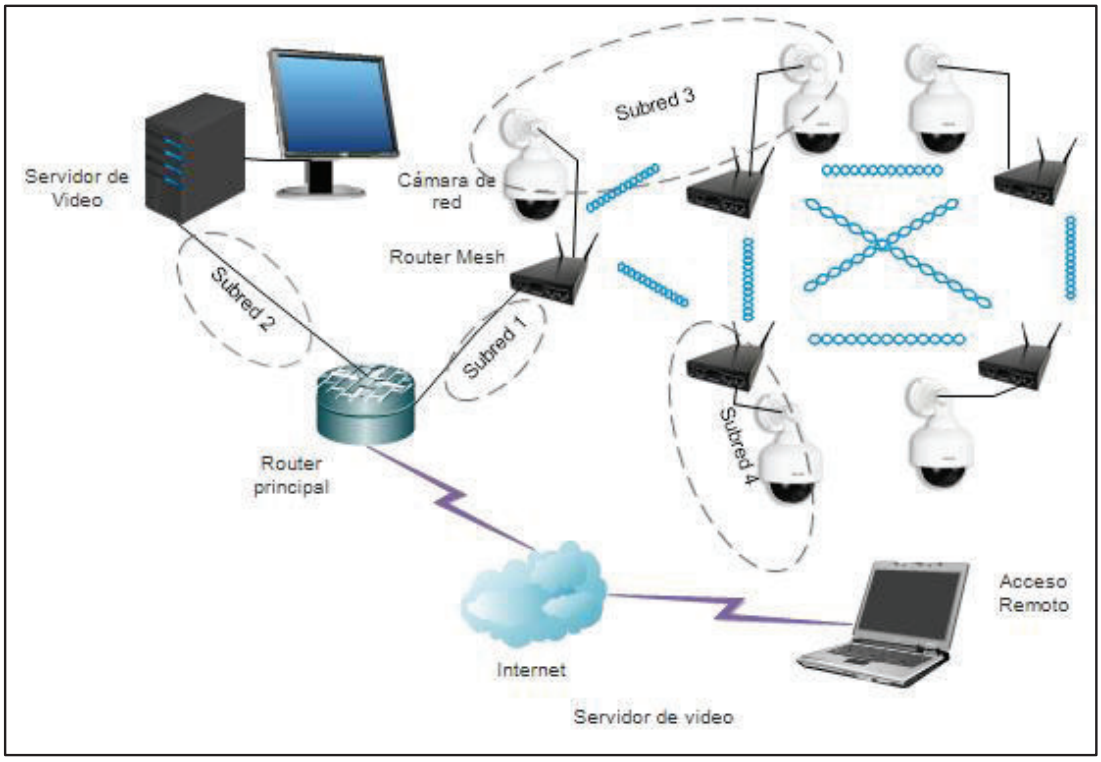


Figura 3.7 Asignación de Subredes en la red

La subred 1 está conformada por el router que proporciona el proveedor del servicio de Internet y el servidor de video, la subred 2 está conformada por el router de internet y un router mesh, la subred 3 está conformada por todos los router mesh y la subred 4 está conformada por cada router mesh y su cámara IP.

En la Tabla 3.9 se muestran las direcciones de cada subred con sus respectivas direcciones de broadcast, números de máscara y números de host válidos.

SUBRED	DESCRIPCIÓN	DIRECCIÓN IP	MÁSCARA	# HOST
4	Dirección de subred	192.168.0.0	255.255.255.224	30
	Primera dirección valida de host	192.168.0.1	255.255.255.224	
	Última dirección valida de host	192.168.0.30	255.255.255.224	
	Dirección de broadcast	192.168.0.31	255.255.255.224	

Tabla 3. 9 Direccionamiento IP de la red del sistema de video-vigilancia

SUBRED	DESCRIPCIÓN	DIRECCIÓN IP	MÁSCARA	# HOST
3	Dirección de subred	192.168.0.32	255.255.255.224	15
	Primera dirección valida de host	192.168.0.33	255.255.255.224	
	Última dirección valida de host	192.168.0.62	255.255.255.224	
	Dirección de broadcast	192.168.0.63	255.255.255.224	
2	Dirección de subred	192.168.0.64	255.255.255.252	2
	Primera dirección valida de host	192.168.0.65	255.255.255.252	
	Última dirección valida de host	192.168.0.66	255.255.255.252	
	Dirección de broadcast	192.168.0.67	255.255.255.252	
1	Dirección de subred	192.168.0.68	255.255.255.252	2
	Primera dirección valida de host	192.168.0.69	255.255.255.252	
	Última dirección valida de host	192.168.0.70	255.255.255.252	
	Dirección de broadcast	192.168.0.71	255.255.255.252	

Tabla 3.9 Direccionamiento IP de la red del sistema de video-vigilancia

3.8 ACCESO REMOTO AL SISTEMA [1]

Para poder acceder remotamente al sistema de video-vigilancia es necesario conectar el sistema al Internet, para esto, es necesario contratar los servicios de un proveedor de internet (ISP). Al momento de contratar el servicio de acceso a Internet se debe tener en cuenta dos factores:

- La velocidad de subida/bajada de la información.
- Tipo de conexión a internet.

La velocidad de subida describe la velocidad de transferencia de datos desde un dispositivo a internet, mientras que la velocidad de bajada describe la velocidad de transferencia de datos desde el internet a un dispositivo. Para el caso particular del sistema de video-vigilancia, es necesario que la velocidad de subida sea mayor o igual a la velocidad de bajada.

En lo referente al tipo de conexión, los ISP proveen el servicio de dirección de red fija o dinámica.

- Una dirección IP fija consiste en que el proveedor de servicios de internet provee una dirección pública al cliente, gracias a esto, la red del cliente se puede encontrar directamente en la Internet.
- Una dirección IP dinámica consiste en que el proveedor de servicios de internet provee una dirección privada al cliente y esta varía cada vez que se reinicia el modem. Para poder conectarse al Internet, el modem tiene que realizar un NAT (Network Address Translation), el cual consiste en intercambiar paquetes entre una dirección privada y una pública.

En la Tabla 3.10 se presentan los requerimientos necesarios para la contratación del servicio de Internet.

REQUERIMIENTOS	
Tipo de conexión	IP fija
Capacidad del enlace	26.3 Mbps
Relación entre velocidad de subida/bajada	1 a 1
Compartición del servicio	1 a 1
Seguridad	Firewall
Última Milla	Fibra Óptica

Tabla 3.10 Requerimientos del servicio de Internet

3.9 ALIMENTACIÓN ELÉCTRICA DEL SISTEMA

En lo que respecta a la alimentación eléctrica del sistema de video-vigilancia, el Gobierno Autónomo Descentralizado Municipal del cantón Cayambe al ser el más interesado en el desarrollo de este Proyecto y al poseer las facilidades administrativas necesarias, puede llegar a un acuerdo con la Empresa Eléctrica Quito (Proveedora de energía eléctrica en Cayambe), en el que se pida alimentar directamente al sistema por medio de tomas de conexión eléctrica debidamente aterradas, así como el uso de los postes transportadores de electricidad para la colocación de los equipos de video. Los equipos de video-vigilancia serían colocados en estructuras metálicas que se colocaran en la parte superior de los postes de electricidad (ver Figura 3.8), esto con la finalidad de evitar el roce con

las líneas de transmisión de energía eléctrica. Los gastos que esto implique sería un tema a tratar entre las partes interesadas, por lo que no se tomará en cuenta estos valores para el cálculo del costo referencial del Proyecto.

Figura 3.8 Ejemplo estructuras metálicas en postes [20]

Con la finalidad de garantizar un monitoreo continuo y sin interrupciones, es necesario el uso de equipos UPS[14] conectados a los equipos. Estas baterías protegerán de picos/caídas de voltajes y alimentarían eléctricamente al sistema en el caso de existir algún corte de energía en la ciudad y de esta manera, el sistema no se vería afectado. Estos equipos UPS serán colocados dentro de gabinetes metálicos para exteriores (ver Figura 3.9).

Figura 3.9 Ejemplo de gabinete metálico [21]

[14] UPS.- Uninterruptible Power Supply, fuente de suministro eléctrico que posee una batería y tiene como objetivo brindar energía eléctrica a un dispositivo, en el caso de haber interrupciones eléctricas.

3.10 SELECCIÓN DE EQUIPOS [3] [4] [5] [6] [7] [8] [9] [10] [11]

En esta sección se presenta una selección de los equipos que conforman el sistema de video-vigilancia, en base a los requerimientos establecidos en el Cap. 2 y al diseño establecido en este Capítulo. El objetivo es elegir los equipos que resulten más idóneos para la posible implementación del sistema.

3.10.1 ENRUTADORES

En la Tabla 3.11 se presentan los requerimientos mínimos que deben cumplir los equipos enrutadores para satisfacer las necesidades del Sistema.

REQUERIMIENTOS	
Estándares	802.11n
Puerto Ethernet	1000 Mbps
Número de Antenas	2
Equipo para exterior	Si
QoS	802.11e
Seguridades	802.11i
WMN	802.11s
Potencia de Transmisión	20 dBm
Umbral de Recepción	<= -81,15 dBm
Ganancia de Antenas	>= 12 dBi Omnidireccional

Tabla 3.11 Requerimientos mínimos Enrutadores

Luego de buscar en el mercado equipos enrutadores que soporten la tecnología de malla inalámbrica, se presentan las siguientes alternativas:

- Motorola[15]: Empresa estadounidense especializada en la electrónica y en las telecomunicaciones con larga trayectoria en el mercado. Esta empresa presenta al mercado el equipo MOTOMESH Duo, el cual, es una solución de última generación para redes mesh inalámbrica de radios duales, diseñado con el objetivo de brindar aplicaciones de gran calidad de datos,

[15] http://es.wikipedia.org/wiki/Motorola

voz y video. El sistema MotoMesh Duo cumple con la norma 802.11e, lo que le permite hacer priorización de voz y video, esto hace que sobre su sistema puedan correr aplicaciones inalámbricas de Voz sobre IP y streaming de video brindando así calidad de servicio. Además de esto, esta solución soporta actualizaciones de software vía aérea, de esta manera se puede agregar nuevas prestaciones y estándares. Su hoja de datos está incluido en el ANEXO B.

- Mikrotik[16]: Empresa Letona fundada en 1995, creada para el desarrollo de routers y sistemas inalámbricos. Esta empresa ha desarrollado unas tarjetas llamadas RouterBoard (similares a las tarjetas madre de las computadoras), las cuales se las puede ir armando dependiendo de las necesidades que se tenga, por ejemplo: se puede tener uno, dos o tres enlaces inalámbricos diferentes en la misma tarjeta, o colocar antenas directivas u omnidireccionales de corto, mediano y largo alcance. Además de esto, disponen de diferentes tipos de carcasas para las RouterBoard, dependiendo de donde va a estar ubicado el equipo (interior o exterior). Mikrotik presenta para este diseño al equipo Routerboard 433GL con su tarjeta para conexiones inalámbricas R52Hn. Su hoja de datos está incluido en el ANEXO B.

Con la finalidad de seleccionar el equipo más idóneo para el sistema se presenta la Tabla 3.12, en la cual se establece una comparación de equipos en base a sus principales características:

CARACTERÍSTICAS	MOTOROLA	MIKROTIK
Marca	Motomesh Duo 4300-49	433GL con R52Hn
Estándares	802.11a/b/g	802.11a/b/g/n

Tabla 3.12 Comparativa entre equipos enrutadores

[16] http://www.mikrotik.com/

CARACTERÍSTICAS	MOTOROLA	MIKROTIK
Número de Antenas	2 omnidireccionales (8dBi para 2.4GHz y 11 dBi para 4.9GHz)	2 Conectores MMCX para antenas directivas u omnidireccionales
Equipo para exterior	Si	Si
QoS	Si	Si
Seguridades	WEP, WPA, WPA2, AES, 802.1X	WEP, WPA, WPA2, AES, 802.1X
WMN	Si	Si
Puertos Ethernet	10/100 Base-T	3 puertos 10/100/1000
Potencia de Transmisión	hasta 35 dBm	Hasta 25 dBm
Sensibilidad de recepción	802.11b: -92dBm a 11Mbps; -100dBm a 1Mbps	802.11b: -93dBm a 11Mbps; -93dBm a 1Mbps
	802.11g: -78dBm a 54Mbps; -95dBm a 6Mbps	802.11g: -81dBm a 54Mbps; -94dBm a 6Mbps
	802.11a: -77dBm a 27Mbps; -93dBm a 3Mbps	802.11a: -80dBm a 54Mbps; -97dBm a 6Mbps
		802.11n(5GHz): -74dBm a 270 Mbps (40MHz, 800Gl); -97dBm a 65 Mbps(20MHz, 800Gl)
Protocolo de transmisión	Hibrido (proactivo/reactivo)	HWMP plus

Tabla 3.12 Comparativa entre equipos enrutadores

Luego de analizar la Tabla 3.12, el equipo seleccionado para la realización de este Proyecto es el equipo de la marca Mikrotik, debido a que cumple con los requisitos mínimos establecidos y además de esto, presenta muy buenas características tecnológicas.

3.10.2 CÁMARAS IP

En la Tabla 3.13 se presentan los requerimientos mínimos que deben cumplir las cámaras de red para satisfacer las necesidades del sistema.

REQUERIMIENTOS	
Compresión de video	H.264
Resolución (pixeles)	1.3 Mp
Mínima iluminación (lux)	0,5
Visibilidad Nocturna	Si
Puerto Ethernet	100 Mbps
Tipo de cámara de red	Domo PTZ para exterior
Cuadros por segundo (fps)	15
Soporte ONVIF	Si
Zoom Óptico	5x
Ambiente exterior	Si

Tabla 3.13 Requerimientos mínimos para cámaras de red

Para la selección de las cámaras de red, se han seleccionado equipos cuyas marcas cumplen con estándar ONVIF y que cuentan con una amplia trayectoria en materia de video-vigilancia.

Las marcas elegidas para participar en el proceso de selección son: Hikvision con su modelo DS-2DE4220-AE y Dahua con su modelo DH-SD6582. Sus hojas de datos se encuentran en el ANEXO C.

Con la finalidad de encontrar el equipo más idóneo para este sistema, se presenta la Tabla 3.14, en la cual se hace una comparación de características entre estos dos equipos:

PARÁMETROS	DAHUA MODELO DH-SD6582	HIKVISION MODELO DS-2DE4220-AE
Compresión de video	H.264	H.264 / MJPEG
Resolución	2 MP	2 MP
Visibilidad nocturna	Si	Si
Max. cuadros por segundo (fps)	30	30
Detección de movimientos	Si	Si
Almacenamiento interno	No	Memoria SD de hasta 64 GB
Zoom	Optical 20x, Digital 12x	Optical 20x, Digital 16x
Mínima iluminación (Lux.)	B/N 0.095, Color 0.5	B/N 0.01, Color 0.05

Tabla 3.14 Comparación de cámaras de vigilancia PTZ

PARÁMETROS	DAHUA MODELO DH-SD6582	HIKVISION MODELO DS-2DE4220-AE
Movimiento PTZ	Pan 360°, Tilf 90°	Pan 360°, Tilf 90°
ONVIF	Si	Si
Puerto Ethernet	Si	100Base-T, 100BaseTX
S/N	≥ 50 dB	≥ 52 dB
PoE	Si, 24V	24 V, 802.3at
IR – CUT	Si	Si
Ambiente Exterior	Si	Si

Tabla 3.14 Comparación de cámaras de vigilancia PTZ

Como resultado de esta comparación, se elige al equipo de la marca Hikvision debido a que cumple con los requisitos mínimos establecidos y además de esto, presenta muy buenas características tecnológicas.

3.10.3 SERVIDORES DE VIDEO

Para el caso del servidor de video, se utilizará un sistema NVR debido a que se necesita almacenar una gran capacidad de información. En la Tabla 3.15 se presentan los requerimientos mínimos que debe tener el equipo NVR para satisfacer las necesidades del Sistema.

REQUERIMIENTOS	
Número de canales	15
Puerto Ethernet	1Gbps
Compresión soportada	H.264
Soporte ONVIF	Si
Programa para gestión y administración de video	Si
Tamaño de disco duro	23 TB

Tabla 3.15 Requerimientos mínimos para equipo NVR

Para la selección del servidor de video, se han elegido a las marcas Toshiba con su modelo NVSPRO32-2U-24T y Hikvision con su modelo DS-9616NI-24TB para participar del proceso de selección. Sus hojas de datos se encuentran en el ANEXO D.

En la Tabla 3.16 se presenta una comparación de características entre estos dos equipos:

PARÁMETROS	TOSHIBA NVSPRO32-2U-24T	HIKVISION DS-9616NI-ST-24TB
Número de Canales	32	16
Tamaño disco	24 TB	24 TB
Interface de red	2, 1 Gbit/s	2, 10/100/1000M
Compresión Soportada	H.264/MJPEG/MPEG-4	H.264/MPEG-4
ONVIF	Si	Si
Sistema de gestión de video	NVSPRO Network Surveillance Server	iVSM
Sistema Operativo	Windows 7 embebido	Hikvision

Tabla 3.16 Comparación entre equipos NVR

Luego de la comparación establecida en la Tabla 3.16, se elige al NVR de la marca Hikvision, modelo DS-9616NI-ST-24TB como servidor del sistema de video-vigilancia, debido a que cuenta con un sistema operativo propio y es menos susceptible de ataques por virus.

3.10.4 ADMINISTRACIÓN Y GESTIÓN DEL SISTEMA

Para la gestión y almacenamiento de video se utilizará el programa de la familia Hikvision, el cual viene embebido en el equipo NVR, modelo DS-9616NI-ST-24TB, el cual permite entre otras cosas:

- Añadir/eliminar cámaras de vigilancia IP de manera intuitiva.
- Configuración personalizada de cámaras de vigilancia IP.
- Múltiples formatos de reproducción de imágenes.
- Acceso remoto a videos.
- Múltiples opciones de grabación.
- Envió de alertas y avisos en caso de pérdida de comunicación con las cámaras de vigilancia.

3.11 SIMULACIÓN DE LA RED DE DATOS DEL SISTEMA DE VIDEO-VIGILANCIA [5] [12] [13] [14] [15] [16] [17] [18]

Por medio del programa Radio Mobile se puede conocer la viabilidad de los enlaces entre enrutadores, teniendo en cuenta aspectos muy importantes como: condiciones climáticas del lugar, condiciones técnicas y topología del terreno.

Radio Mobile es un programa creado para la planificación de radio enlaces, el cual hace uso del modelo de propagación ITM (Irregular Terrain Mode) también conocido como Longley-Rice. Por medio de este programa se puede predecir la atenuación de las señales de radio en enlaces de telecomunicaciones.

A continuación se detallaran los principales pasos seguidos en la simulación de la red:

- Para empezar con la simulación, lo primero que se debe hacer, es obtener la latitud y longitud de la ciudad de Cayambe, para luego, extraer esa parte del mapa al programa Radio Mobile (ver Figura 3.10).

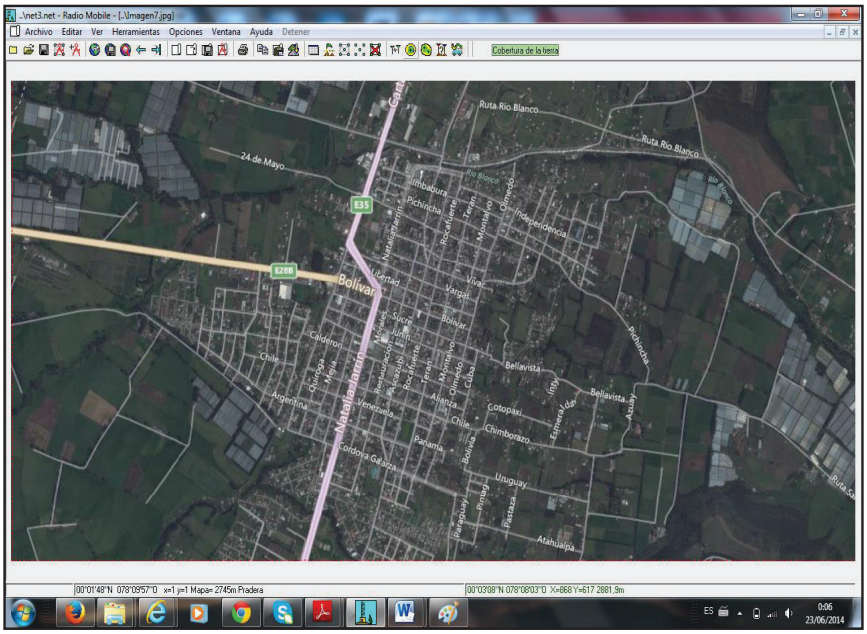


Figura 3.10 Mapa de Cayambe a través de Radio Mobile

- Una vez definida la ubicación de las cámaras de vigilancia, es necesario ubicar estos puntos en el mapa. Esto se lo hace en la ventana **Propiedades de las unidades.** En la Figura 3.11 se puede observar la ubicación física de estos equipos en la ciudad.

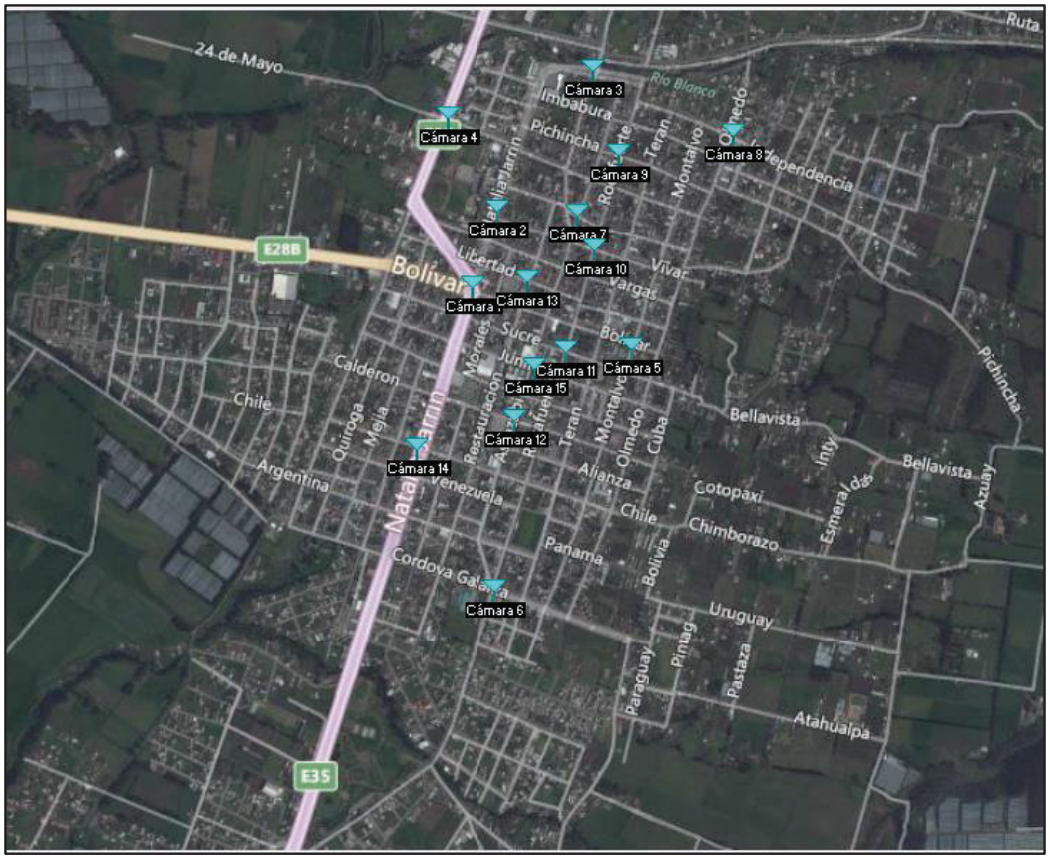


Figura 3.11 Ubicación de cámaras de vigilancia en la ciudad de Cayambe

- La creación de los enlaces se realiza en la ventana **Propiedades de las Redes,** en donde es necesario definir los parámetros de las pestañas: Parámetros, Topología, Miembros y Sistemas.

  En la pestaña Parámetros se debe definir lo siguiente:

  - Nombre de la red: Se puede poner cualquier nombre a la red, en este caso se la llamo: BackhaulVV.

- Frecuencia máxima y mínima: Se colocó el valor de 5735 a 5755 MHz.
- Polarización vertical u horizontal: Se tomó el valor de polarización vertical, debido a que de esta manera se obtiene una mayor cobertura de transmisión (ominidireccional).
- Refractividad de la superficie: Este parámetro tiene que ver con la curvatura que sufrirán las ondas de radio al propagarse por la tierra. El valor de refractividad efectiva de la tierra recomendado para condiciones atmosféricas promedio es de 301 unidades de n (corresponde al valor de curvatura efectiva de la tierra de 4/3 o 1,333).
- Conductividad del suelo y permitividad relativa al suelo: Son valores que se encuentran tabulados y que dependen del tipo del suelo y de la frecuencia de operación. Estos valores se los puede apreciar en la Tabla 3.17.

TIPO DE SUELO	PERMITIVIDAD RELATIVA	CONDUCTIVIDAD [siemens/m]
Tierra promedio	15	0.005
Tierra pobre	4	0.001
Tierra buena	25	0.020
Agua dulce	81	0.010
Agua salada	81	5.000

Tabla 3.17 Permitividad relativa y conductividad del suelo [17]

Para esta simulación se trabajará con los valores de permitividad y conductividad asignados a la tierra promedio.

- Modo estadístico: Determina que es lo que debe ocurrir cuando se establece la comunicación entre los equipos. Radio Mobile permite cuatro modos de operación:

  - Intento: Realiza una transmisión unicast entre estaciones fijas, se envía un único mensaje de intento de conexión.
  - Accidental: Se emplea para evaluar interferencias.

- Móvil: Se utiliza para conexiones en las cuales los equipos están en movimiento.
- Difusión: La trasmisión es del tipo broadcast entre estaciones fijas.

En esta simulación se utilizará como modo estadístico, el modo Difusión, debido a que se quiere simular una red en malla.

Dentro del modo estadístico, también se presentan tipos de variabilidad, los cuales fueron definidos para considerar las variaciones en los niveles de una señal y se los expresa en porcentajes que van desde el 0.1% al 99.9%. Estos tipos de variabilidad son los siguientes:

- Porcentaje de tiempo: Es la fracción de tiempo durante el cual, el campo de fuerzas recibido se espera que sea igual o superior al valor medio de campo calculado por el programa. La variabilidad de tiempo depende de los cambios atmosféricos que puedan suceder en el lugar donde van a implementarse los enlaces. A mayor valor del porcentaje, menor será la variabilidad del tiempo en el lugar.

  Para el caso de esta simulación se trabajará con el valor de 50%.
- Porcentaje de ubicaciones: Similar al anterior con la diferencia que este tiene que ver con la diferencia de trayectos recorridos debido a que la señal que se ve afectada en diferente grado por los perfiles del terreno o por las diferencias ambientales entre ellos. Se trabajará con el valor de 50%.
- Porcentaje de situaciones: Engloba las variables ocultas que no pueden explicarse o que no se han tenido en cuenta de forma explícita en el Proyecto. Se trabajará con el valor de 70%.

- Tipo de clima.- En esta opción se debe escoger el tipo de clima que se presenta en la zona de implementación de las redes. Radio

Mobile permite elegir de entre siete modelos de clima los cuales se citan a continuación:

- Ecuatorial.
- Continental Subtropical.
- Marítimo o Sub-tropical.
- Desierto.
- Continental templado.
- Marítimo o templado sobre la tierra.
- Marítimo o templado sobre el mar.

Para esta simulación se utilizará el clima Ecuatorial por obvias razones.

- Perdidas Adicionales: En esta opción se debe indicar si en el trayecto de la red existen grandes superficies boscosas o entornos urbanos densos, indicando el porcentaje aproximado de este tipo de terreno. Para nuestro caso se elegirá la opción ciudad y se tomará un valor de 10%.

En la Figura 3.12 se puede observar los parámetros configurados:

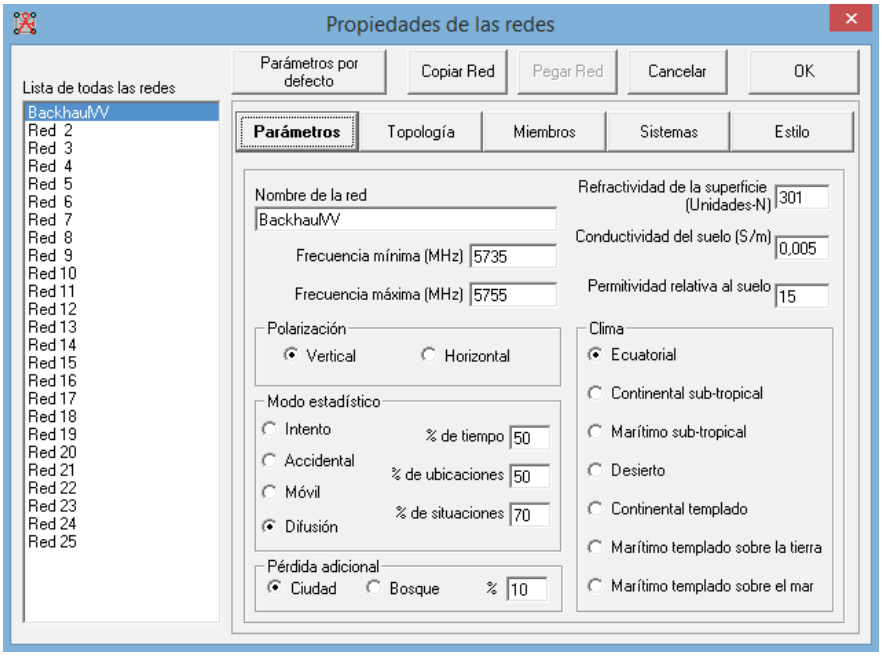


Figura 3.12 Ventana Propiedades de las redes, pestaña Parámetros

En la pestaña Topología se debe elegir el Tipo de Topología de red que se utilizará y se tiene las siguientes alternativas:

- Red de voz (Controlador/Subordinado/Repetidor): En este tipo de red se establece una estructura en la que uno o varios controladores se comunican con sus subordinados, sin que éstos puedan relacionarse entre sí.
- Red de datos, Topología estrella (Master/Esclavo): Se trasmiten datos en redes en las cuales una estación maestra controla a una o varias estaciones esclavas, sin que existan comunicación directa entre estaciones esclavas.
- Red de datos, cluster (Nodo/Terminal): Los nodos que componen la red de datos tienen la propiedad de retransmitir datagramas.

    - Número Máximo de retransmisiones permitidas: En el caso que se elija la opción Red de datos aparecerá esta opción, Si se selecciona el valor de “0” en este apartado, querrá decir que no se permiten retransmisiones.

La opción que más se ajusta a la simulación que se pretende realizar es Red de datos, cluster (Nodo/Terminal). La casilla *"visible"* se la activa cuando se quiere mostrar los enlaces de una red sobre el mapa (ver Figura 3.13).

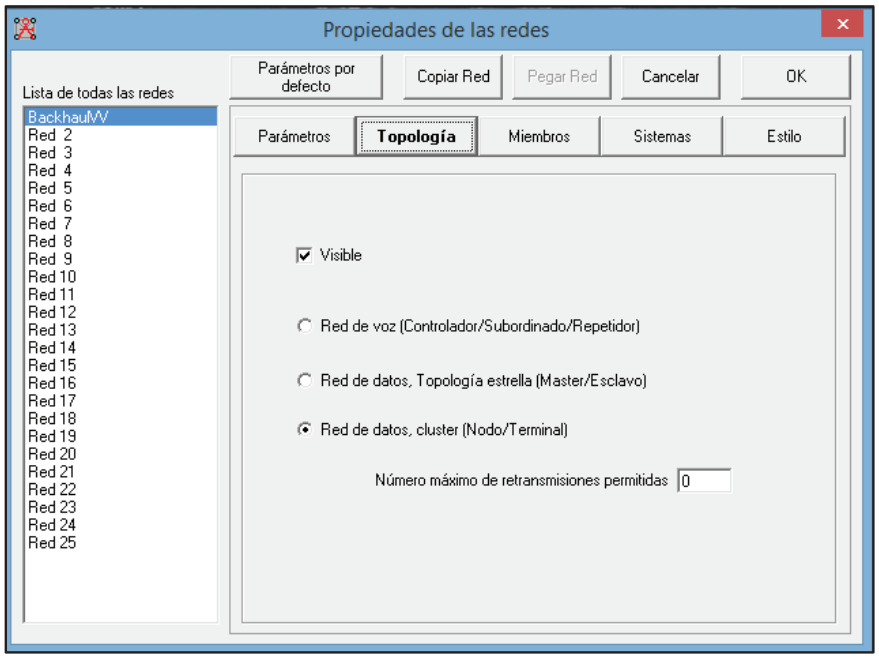


Figura 3.13 Ventana Propiedades de las redes, pestaña Topología

En la pestaña Miembros se debe indicar los equipos y el tipo de antena que se va a utilizar en la red. En el apartado *"Lista de todas las unidades"* se debe elegir los equipos que pertenecen a una red, luego de esto, se debe elegir el tipo de sistema al que pertenecen (será configurado en la siguiente ventana) y el papel que desempeña en la red.

También se debe seleccionar el valor de la altura de una antena, si esta va a ser colocada en un poste o un mástil y la dirección de la misma. Para la presente simulación se ha escogido el valor de 10 m, ya que se espera colocar los enrutadores a esta altura y la dirección de la antena es omnidireccional (ver Figura 3.14).

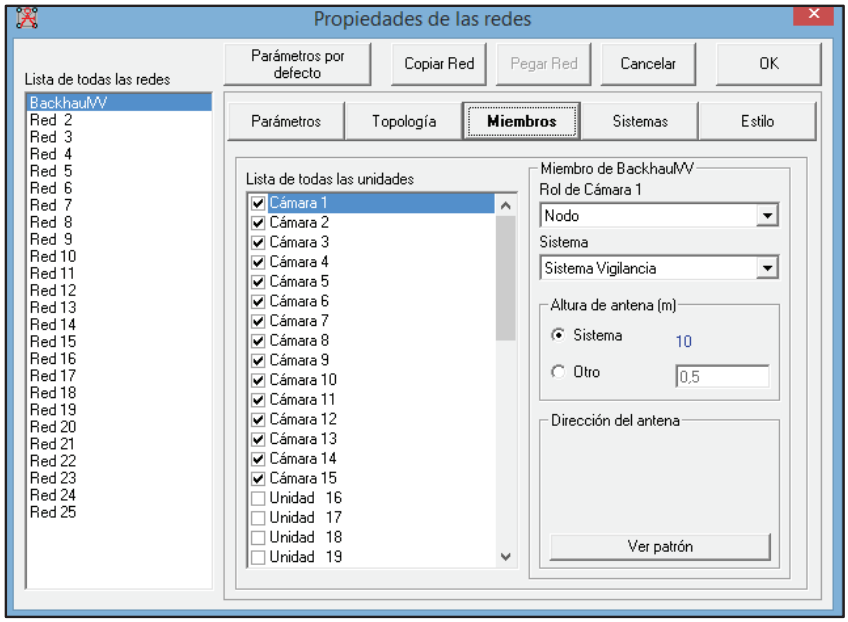


Figura 3.14 Ventana Propiedades de las redes, pestaña Miembros

En el apartado *"Sistemas"* se debe determinar las características de cada una de las estaciones, para esto es necesario recurrir a las hojas de datos de los equipos a utilizar. Radio Mobile engloba todos los equipos que integran una red con el término sistemas.

Los parámetros que se deben ser configurados en este apartado son los siguientes:

- Potencia del transmisor: Es la máxima potencia emitida por el equipo, en nuestro caso, la potencia de las tarjetas R52Hn, trabajando en el estándar IEEE 802.11n en la banda de frecuencia de 5 GHz se tiene 22 dBm.
- Umbral del receptor.- Se refiere a la sensibilidad del equipo receptor, Para nuestro caso el valor de sensibilidad de las tarjetas R52Hn, trabajando con el estándar IEEE 802.11n será de: -92 dBm
- Pérdida de línea.- son pérdidas asociadas a cables y conectores. Se tomará como referencia el valor de 1 dB.
- Tipo de antena.- Para utilizará una antena del tipo omnidireccional.

- Ganancia de la antena.- La ganancia de la antena será de 12 dBi.
- Altura de la Antena.- Se tomó como valor 10 m, ya que la mayoría de casas y edificios en la ciudad de Cayambe no sobrepasan este valor y de esta manera nos aseguramos que exista línea de vista entre todos los enrutadores.
- Perdida Adicional cable.- son pérdidas extras asociadas a la distancia del cable que une a la altura con el equipo transmisor/receptor. Un valor promedio considerado para este tipo de pérdidas es de 0.5 dB por metro. Para la presente simulación se tomó el valor de 0.5 dB.

En la Figura 3.15 se puede observar los parámetros configurados:

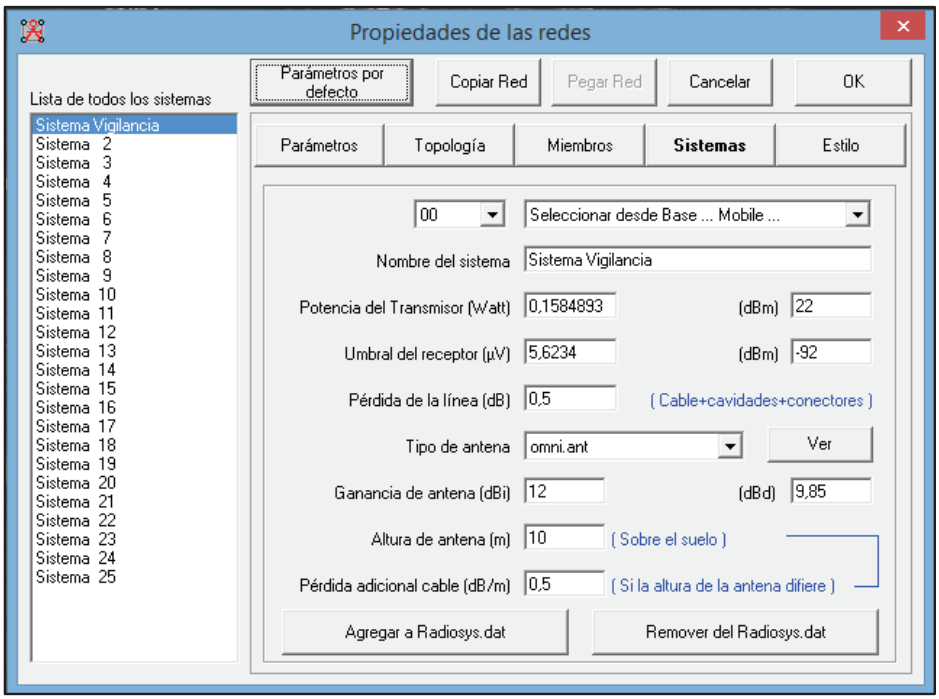


Figura 3.15 Ventana Propiedades de las redes, pestaña Sistemas

En la Figura 3.16 se presenta la conexión entre todos los nodos (malla) en la ciudad de Cayambe, lo que indica que este Proyecto es viable.

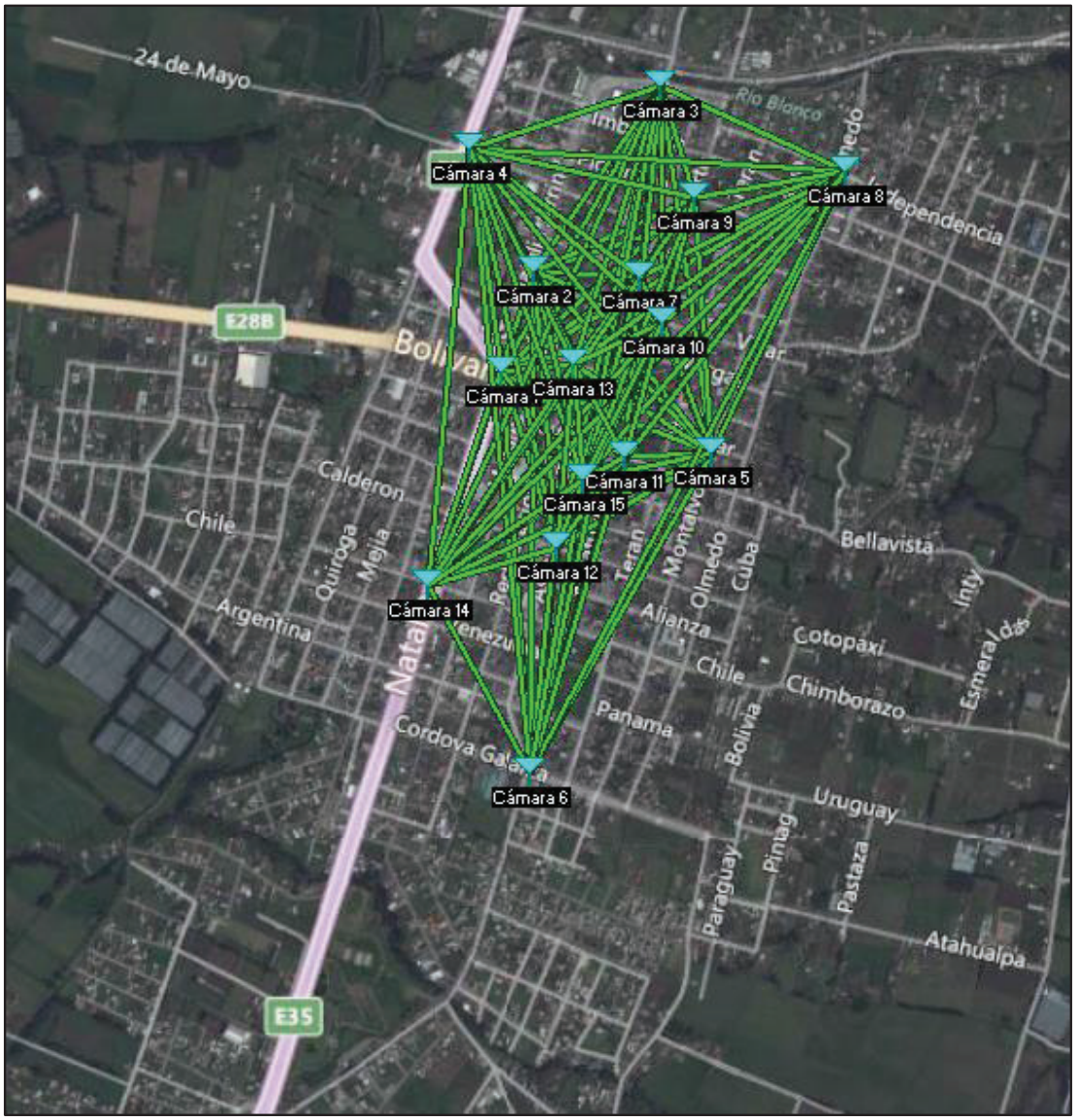


Figura 3.16 Red inalámbrica mallada

3.11.1 ANÁLISIS DE RESULTADOS

3.11.1.1 Enlace cámara 5 – cámara 1

En la Figura 3.17 se muestra la simulación del enlace entre cámara 5 y cámara 1 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

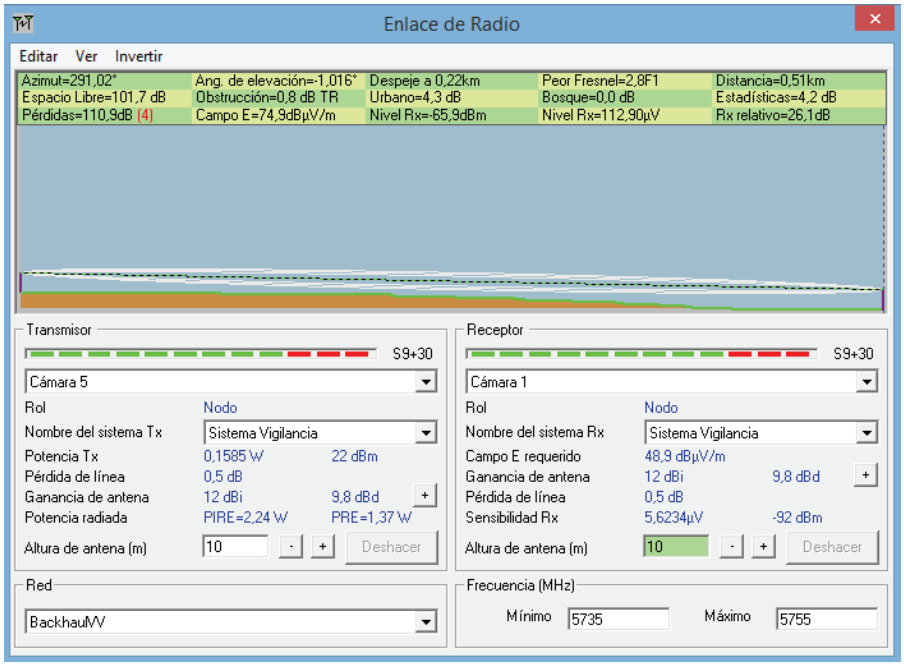


Figura 3.17 Enlace cámara 5 – cámara 1 con características de enlace

En la Figura 3.18 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

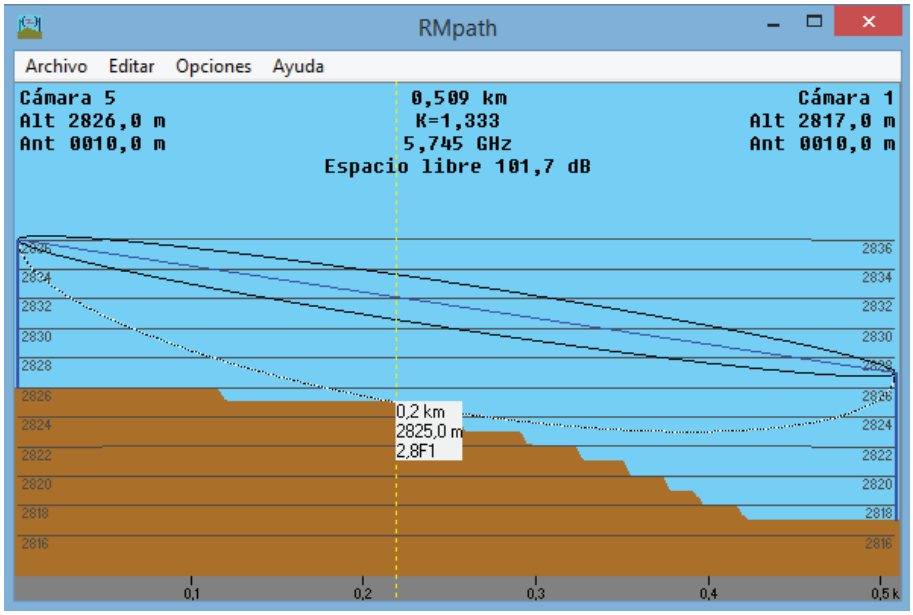


Figura 3.18 Enlace cámara 5 – cámara 1 en base a la zona de Fresnel

En la Figura 3.19 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 26,1 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

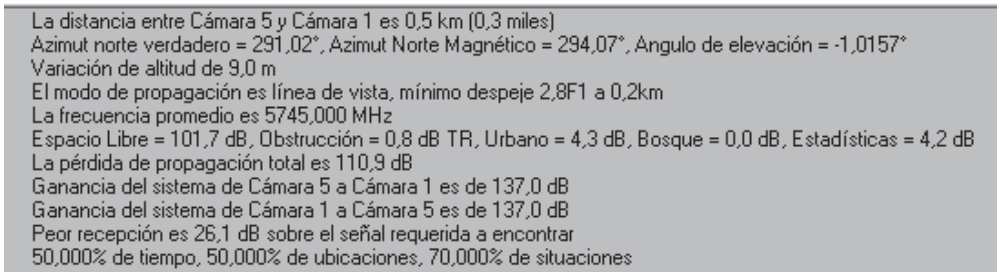


Figura 3.19 Estadísticas del enlace cámara 5 – cámara 1

3.11.1.2 Enlace cámara 5 – cámara 2

En la Figura 3.20 se muestra la simulación del enlace entre cámara 5 y cámara 2 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

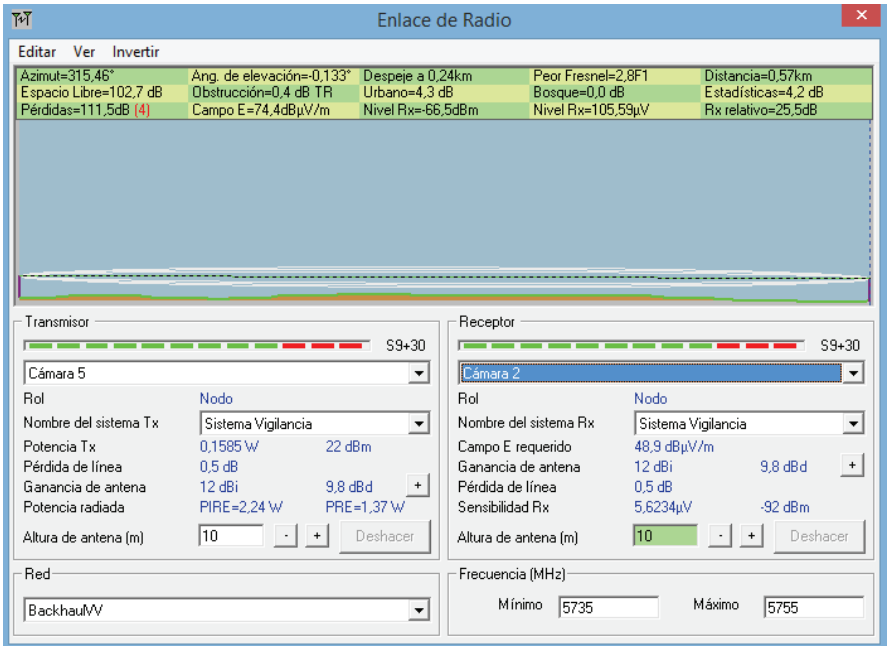


Figura 3.20 Enlace cámara 5 – cámara 2 con características de enlace

En la Figura 3.21 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

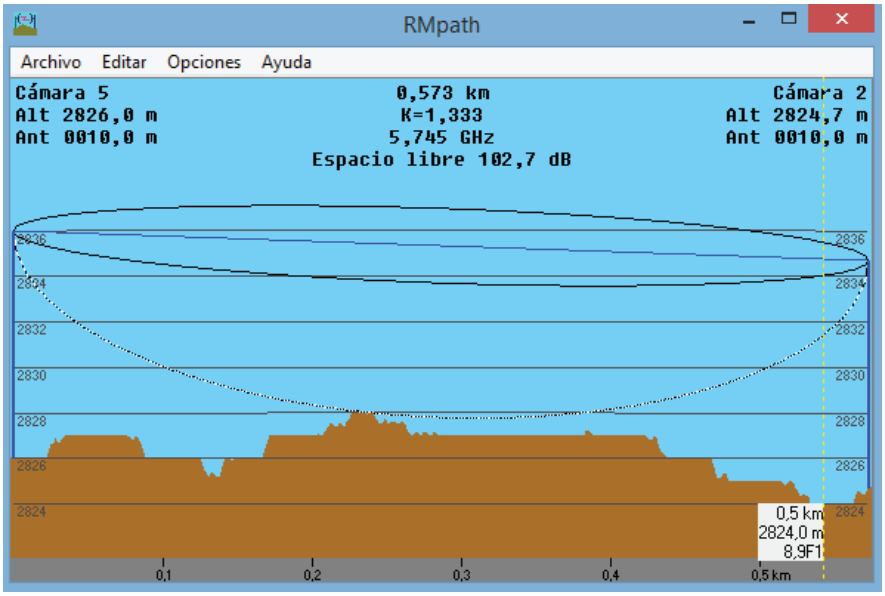


Figura 3.21 Enlace cámara 5 – cámara 2 en base a la zona de Fresnel

En la Figura 3.22 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 25,5 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

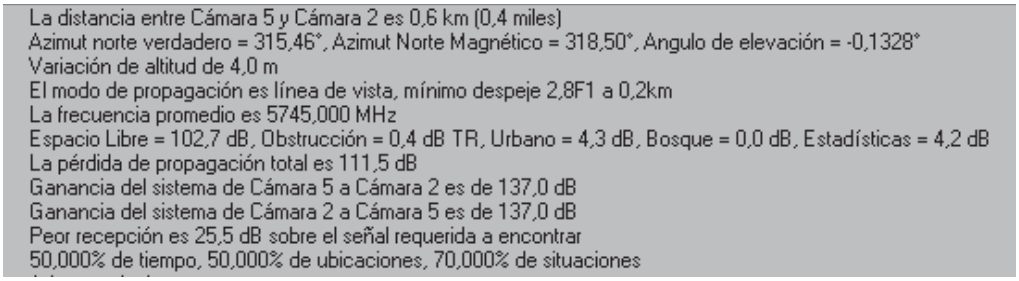


Figura 3.22 Estadísticas del enlace cámara 5 – cámara 2

3.11.1.3 Enlace cámara 5 – cámara 3

En la Figura 3.23 se muestra la simulación del enlace entre cámara 5 y cámara 3 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

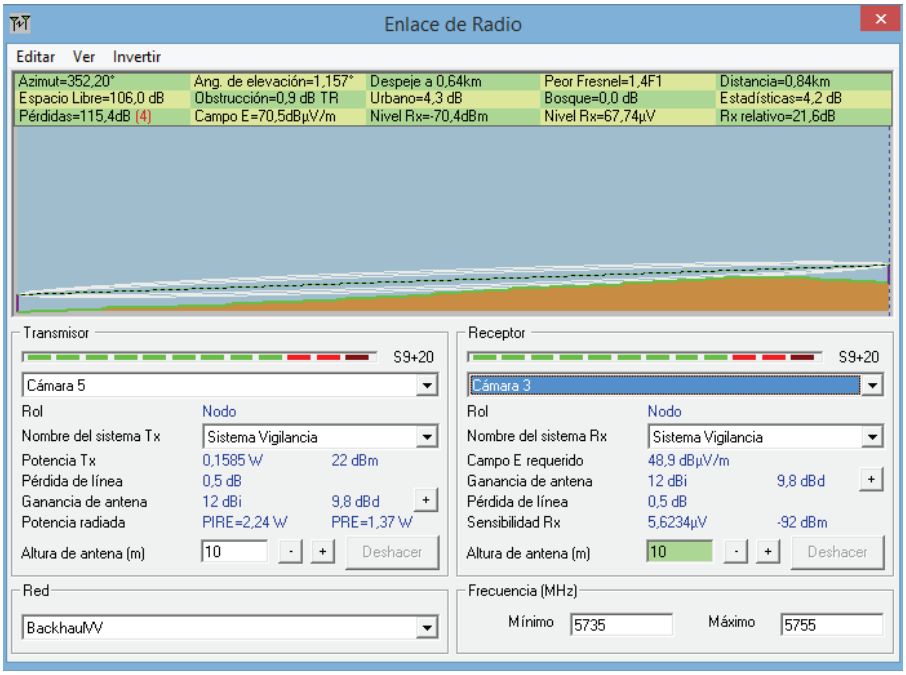


Figura 3.23 Enlace cámara 5 – cámara 3 con características de enlace

En la Figura 3.24 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

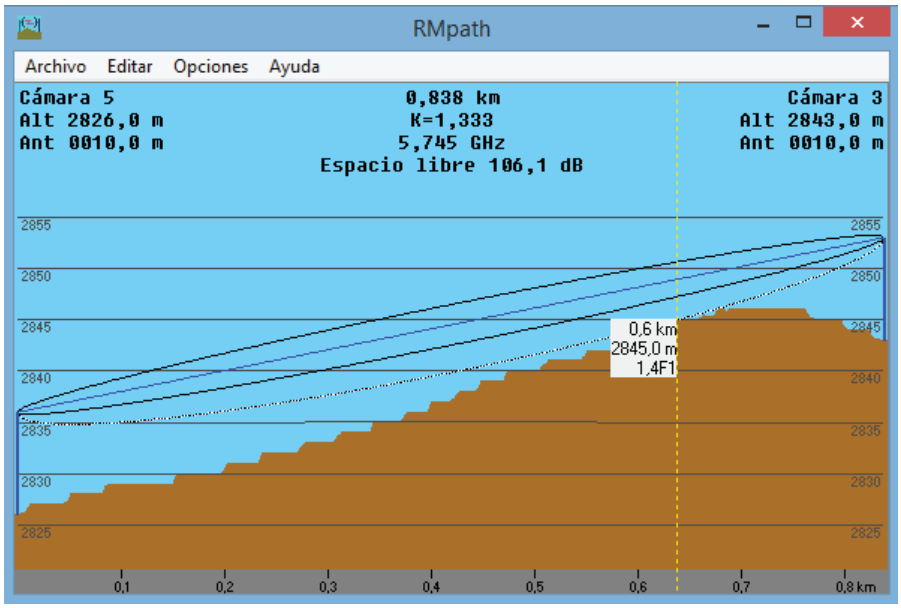


Figura 3.24 Enlace cámara 5 – cámara 3 en base a la zona de Fresnel

En la Figura 3.25 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 21,6 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

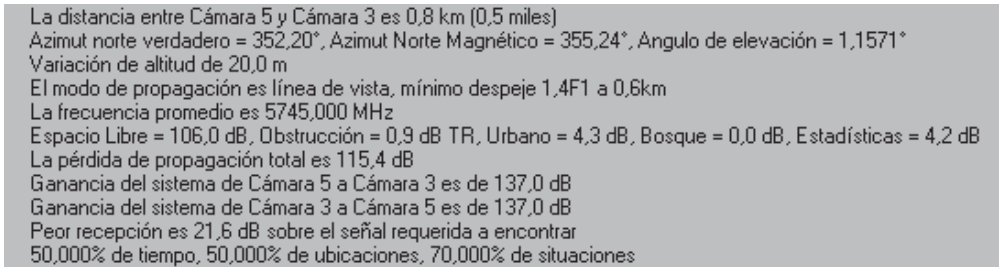


Figura 3.25 Estadísticas del enlace cámara 5 – cámara 3

3.11.1.4 Enlace cámara 5 – cámara 4

En la Figura 3.26 se muestra la simulación del enlace entre cámara 5 y cámara 4 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

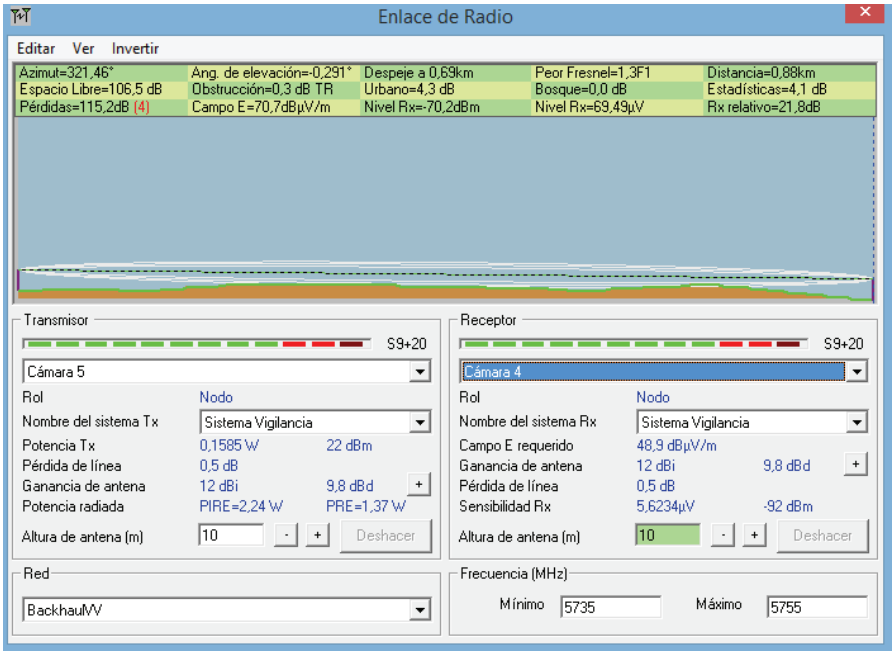


Figura 3.26 Enlace cámara 5 – cámara 4 con características de enlace

En la Figura 3.27 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

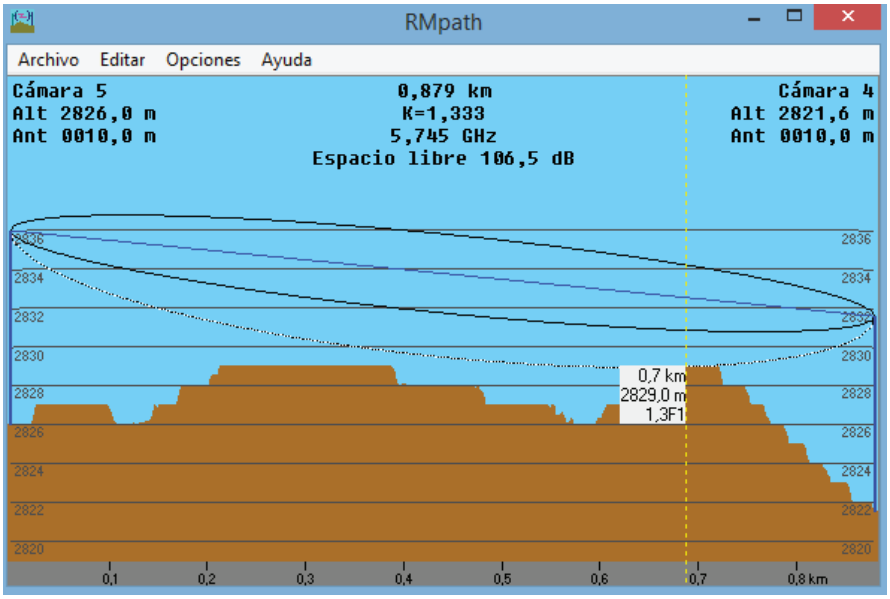


Figura 3.27 Enlace cámara 5 – cámara 4 en base a la zona de Fresnel

En la Figura 3.28 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 21,8 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

La distancia entre Cámara 5 y Cámara 4 es 0,9 km (0,5 miles)
Azimut norte verdadero = 321,46°, Azimut Norte Magnético = 324,51°, Angulo de elevación = -0,2908°
Variación de altitud de 7,4 m
El modo de propagación es línea de vista, mínimo despeje 1,3F1 a 0,7km
La frecuencia promedio es 5745,000 MHz
Espacio Libre = 106,5 dB, Obstrucción = 0,3 dB TR, Urbano = 4,3 dB, Bosque = 0,0 dB, Estadísticas = 4,1 dB
La pérdida de propagación total es 115,2 dB
Ganancia del sistema de Cámara 5 a Cámara 4 es de 137,0 dB
Ganancia del sistema de Cámara 4 a Cámara 5 es de 137,0 dB
Peor recepción es 21,8 dB sobre el señal requerida a encontrar
50,000% de tiempo, 50,000% de ubicaciones, 70,000% de situaciones

Figura 3.28 Estadísticas del enlace cámara 5 – cámara 4

3.11.1.5 Enlace cámara 5 – cámara 6

En la Figura 3.29 se muestra la simulación del enlace entre cámara 5 y cámara 6 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

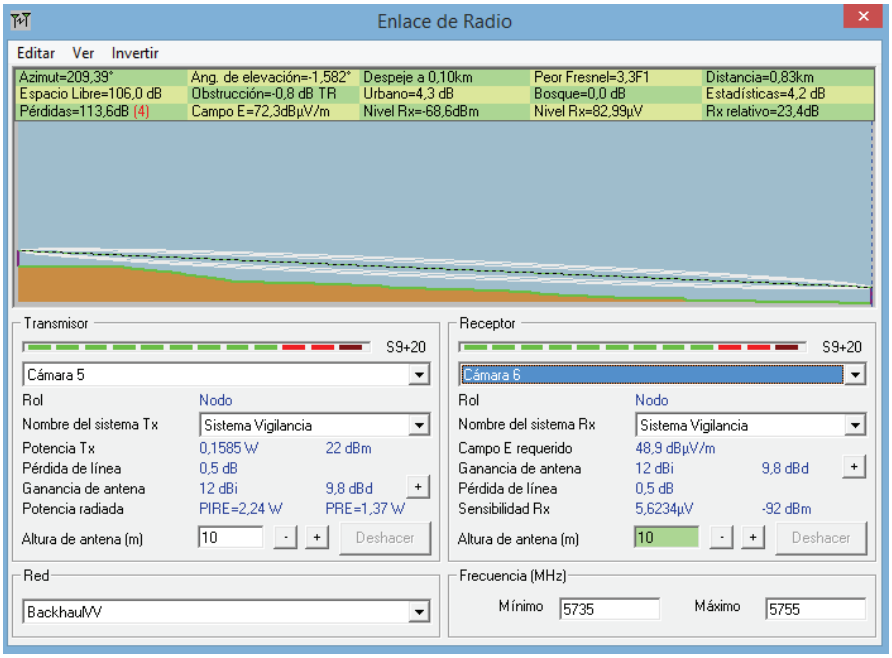


Figura 3.29 Enlace cámara 5 – cámara 6 con características de enlace

En la Figura 3.30 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

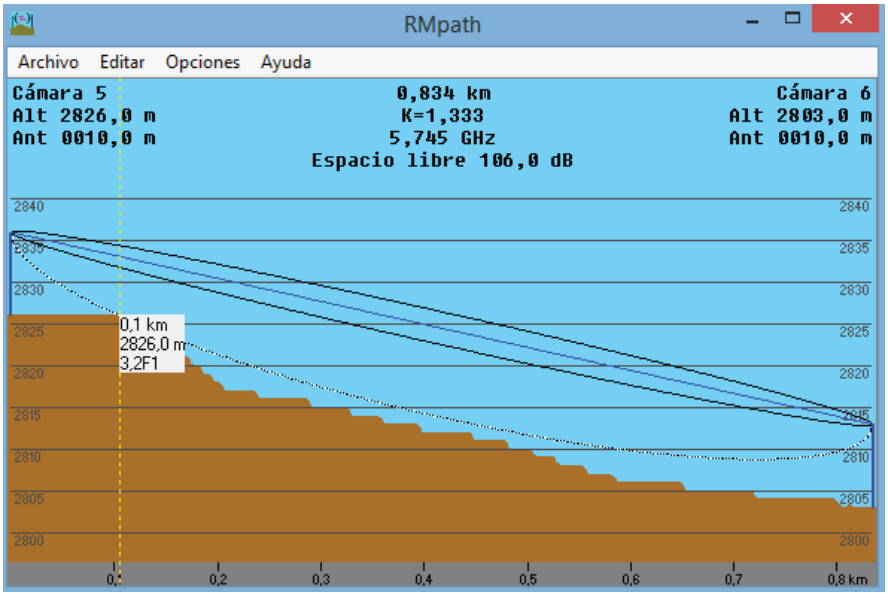


Figura 3.30 Enlace cámara 5 – cámara 6 en base a la zona de Fresnel

En la Figura 3.31 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 23,4 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

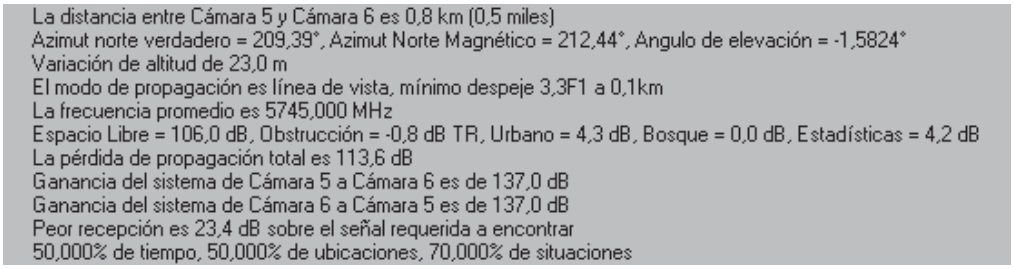


Figura 3.31 Estadísticas del enlace cámara 5 – cámara 6

3.11.1.6 Enlace cámara 5 – cámara 7

En la Figura 3.32 se muestra la simulación del enlace entre cámara 5 y cámara 7 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

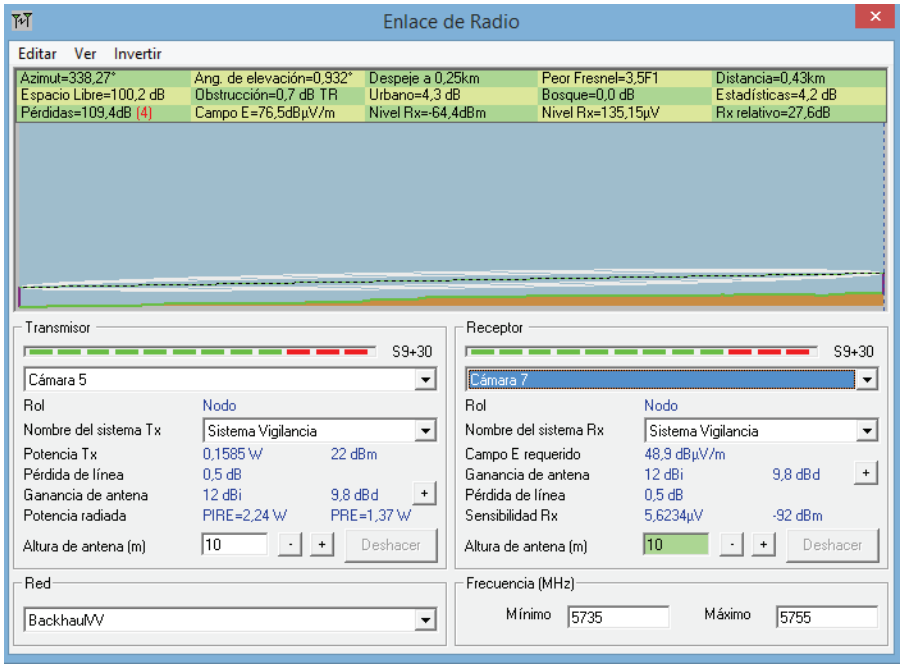


Figura 3.32 Enlace cámara 5 – cámara 7 con características de enlace

En la Figura 3.33 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

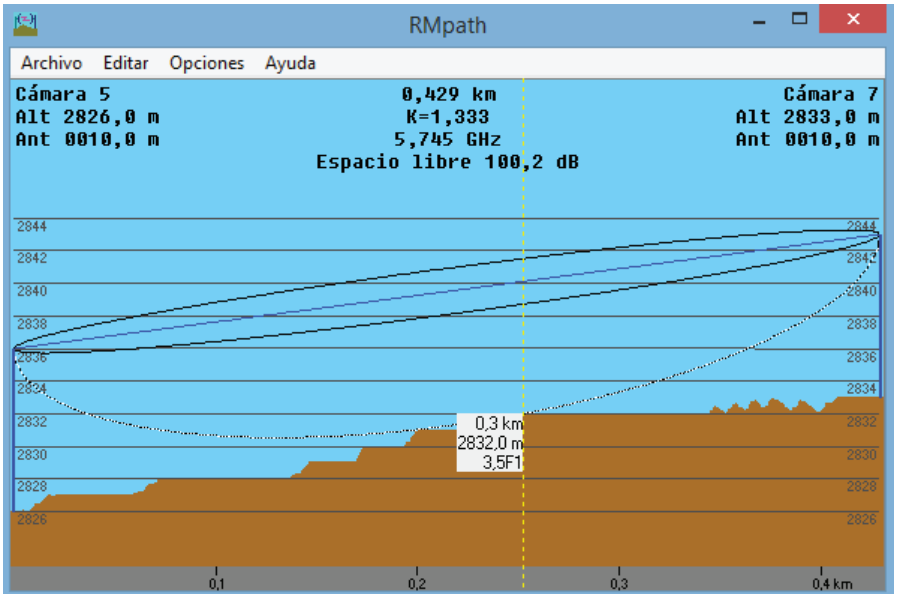


Figura 3.33 Enlace cámara 5 – cámara 7 en base a la zona de Fresnel

En la Figura 3.34 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 27,6 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

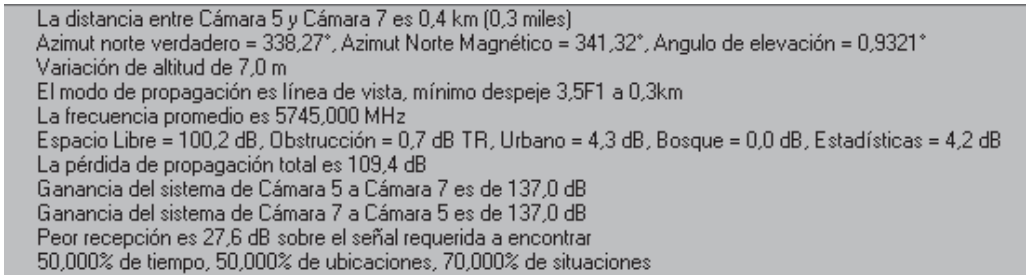


Figura 3.34 Estadísticas del enlace cámara 5 – cámara 7

3.11.1.7 Enlace cámara 5 – cámara 8

En la Figura 3.35 se muestra la simulación del enlace entre cámara 5 y cámara 8 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

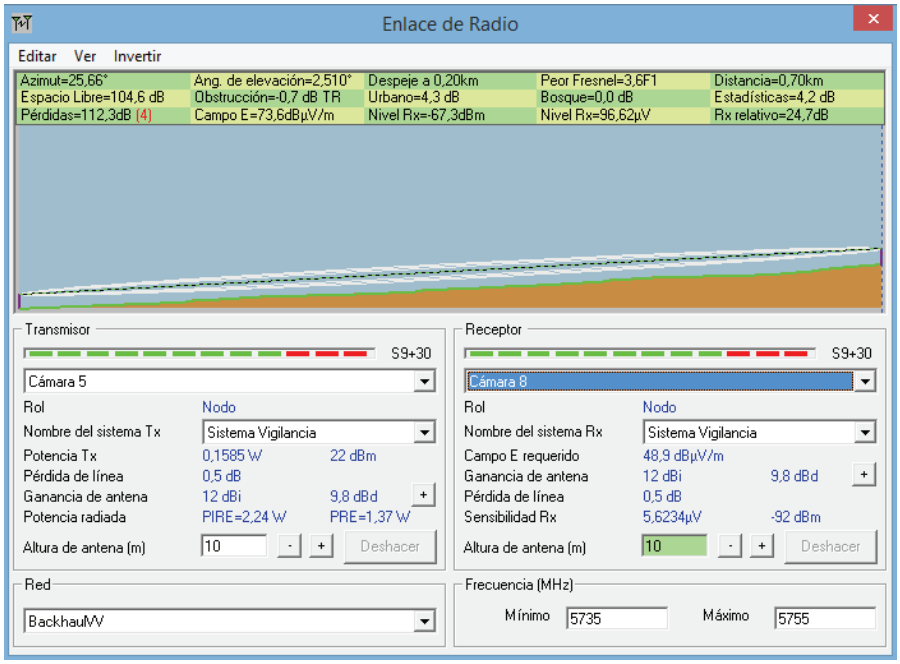


Figura 3.35 Enlace cámara 5 – cámara 8 con características de enlace

En la Figura 3.36 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

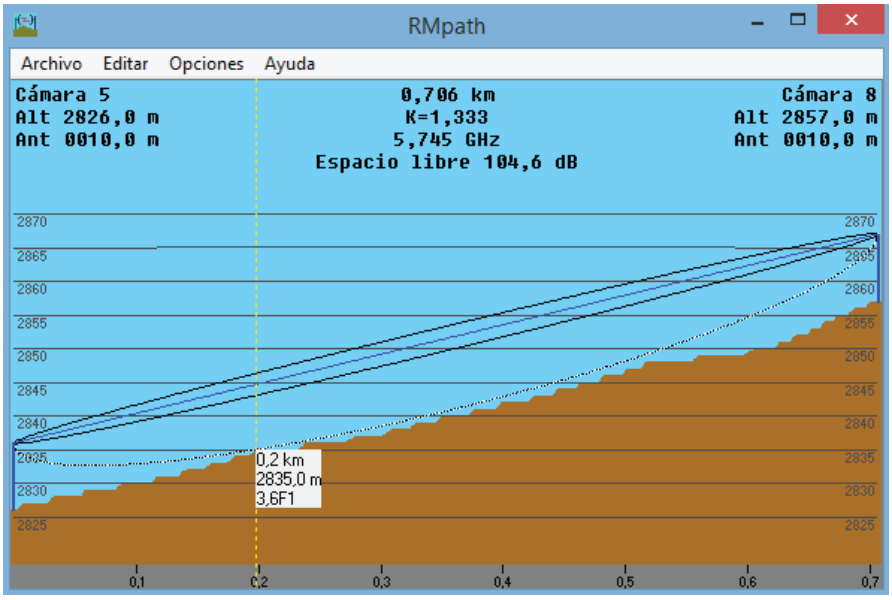


Figura 3.36 Enlace cámara 5 – cámara 8 en base a la zona de Fresnel

En la Figura 3.37 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 24,7 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

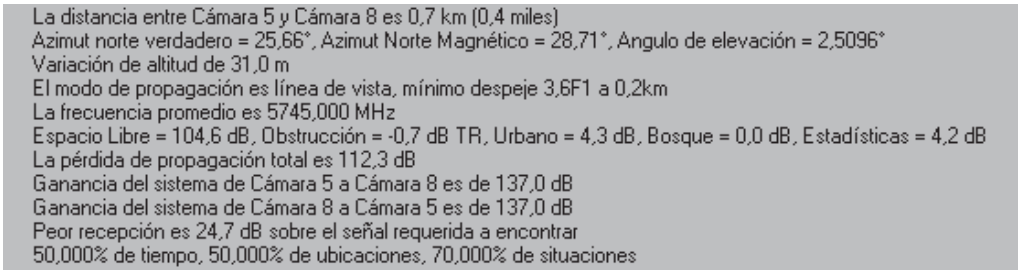


Figura 3.37 Estadísticas del enlace cámara 5 – cámara 8

3.11.1.8 Enlace cámara 5 – cámara 9

En la Figura 3.38 se muestra la simulación del enlace entre cámara 5 y cámara 9 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

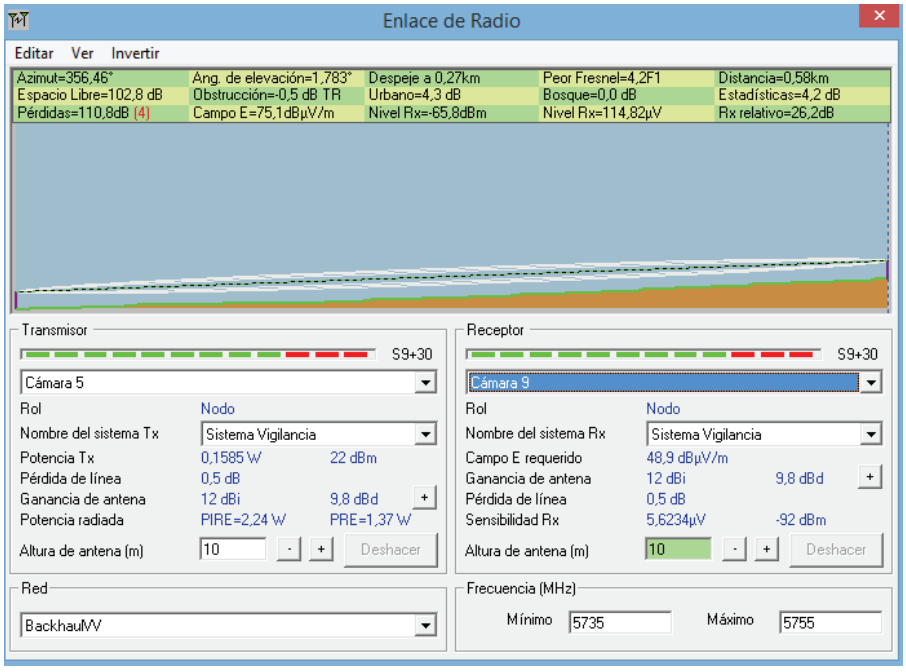


Figura 3.38 Enlace cámara 5 – cámara 9 con características de enlace

En la Figura 3.39 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

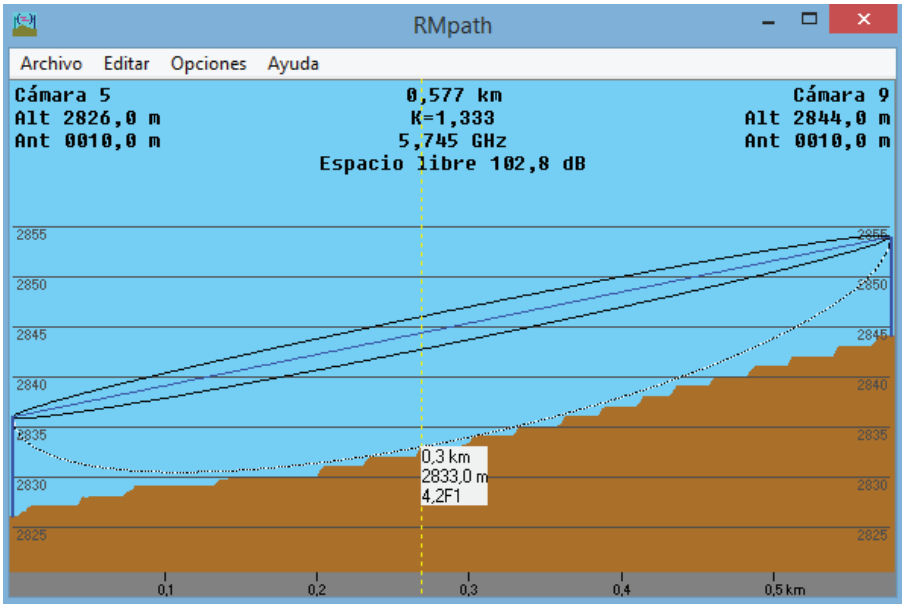


Figura 3.39 Enlace cámara 5 – cámara 9 en base a la zona de Fresnel

En la Figura 3.40 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 26,2 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

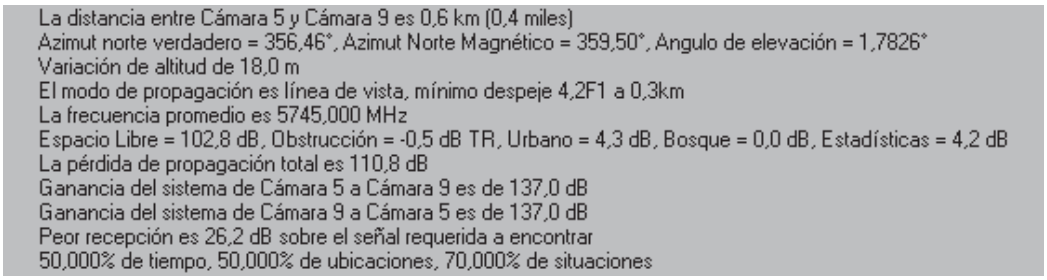


Figura 3.40 Estadísticas del enlace cámara 5 – cámara 9

3.11.1.9 Enlace cámara 5 – cámara 10

En la Figura 3.41 se muestra la simulación del enlace entre cámara 5 y cámara 10 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

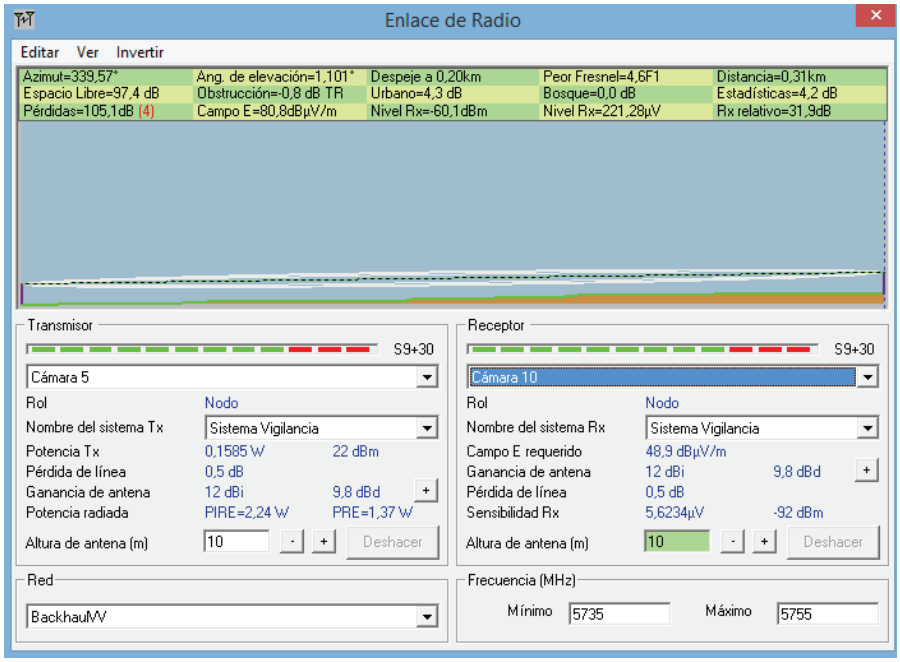


Figura 3.41 Enlace cámara 5 – cámara 10 con características de enlace

En la Figura 3.42 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

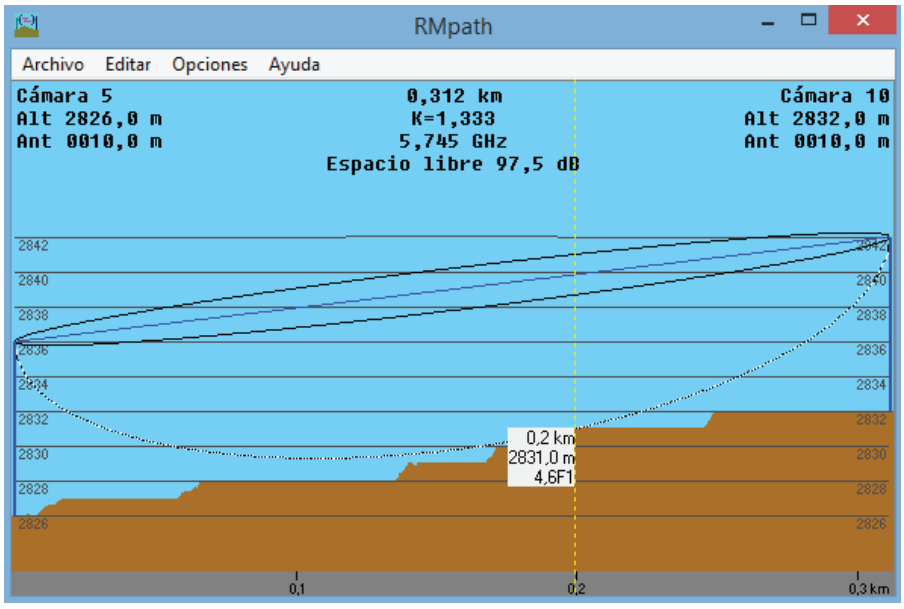


Figura 3.42 Enlace cámara 5 – cámara 10 en base a la zona de Fresnel

En la Figura 3.43 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 31,9 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

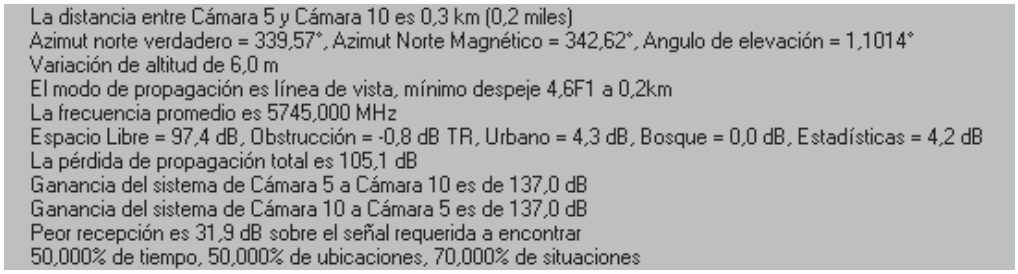


Figura 3.43 Estadísticas del enlace cámara 5 – cámara 10

3.11.1.10 Enlace cámara 5 – cámara 11

En la Figura 3.44 se muestra la simulación del enlace entre cámara 5 y cámara 11 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

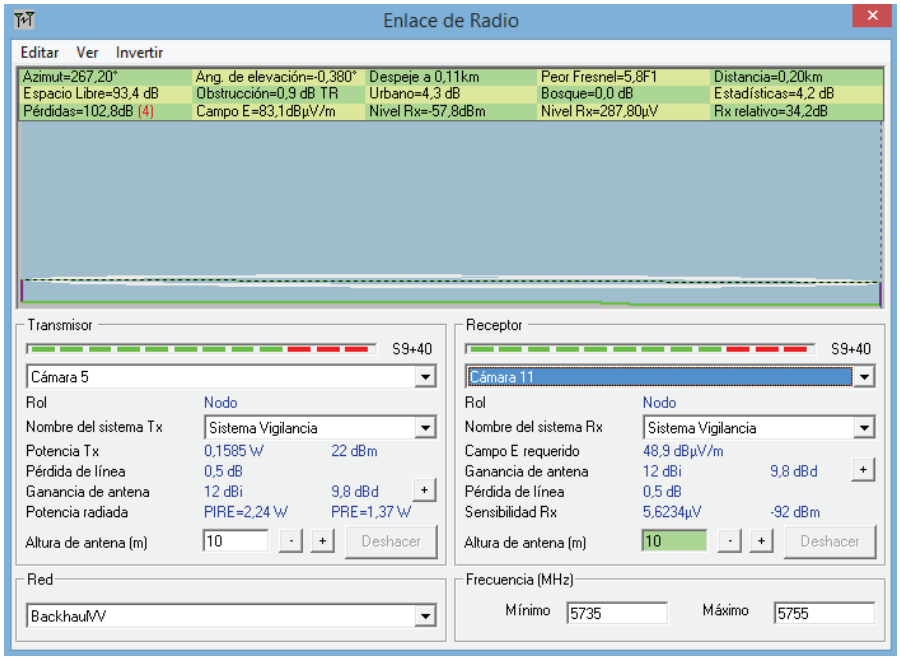


Figura 3.44 Enlace cámara 5 – cámara 11 con características de enlace

En la Figura 3.45 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

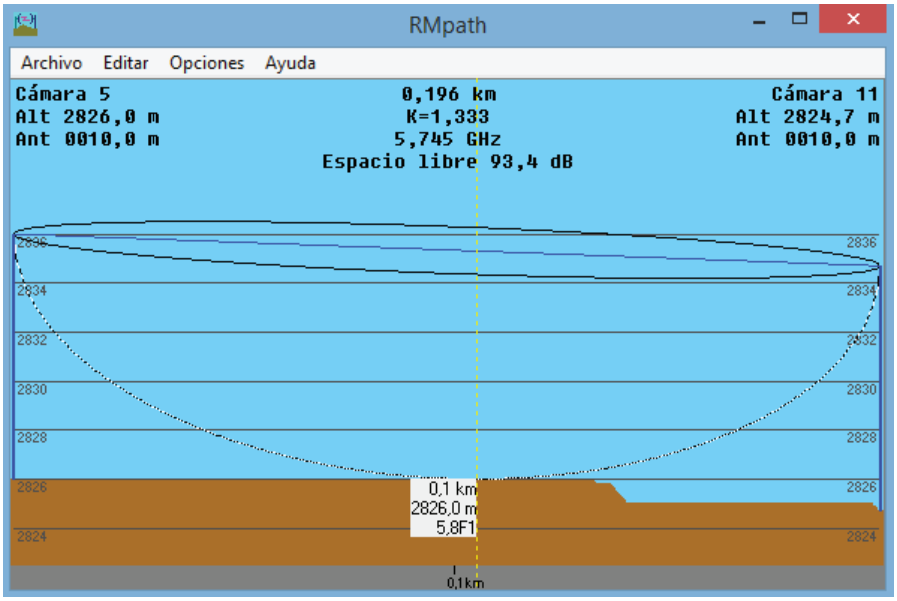


Figura 3.45 Enlace cámara 5 – cámara 11 en base a la zona de Fresnel

En la Figura 3.46 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 34,2 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

La distancia entre Cámara 5 y Cámara 11 es 0,2 km (0,1 miles)
Azimut norte verdadero = 267,20°, Azimut Norte Magnético = 270,25°, Angulo de elevación = -0,3799°
Variación de altitud de 1,3 m
El modo de propagación es línea de vista, mínimo despeje 5,8F1 a 0,1km
La frecuencia promedio es 5745,000 MHz
Espacio Libre = 93,4 dB, Obstrucción = 0,9 dB TR, Urbano = 4,3 dB, Bosque = 0,0 dB, Estadísticas = 4,2 dB
La pérdida de propagación total es 102,8 dB
Ganancia del sistema de Cámara 5 a Cámara 11 es de 137,0 dB
Ganancia del sistema de Cámara 11 a Cámara 5 es de 137,0 dB
Peor recepción es 34,2 dB sobre el señal requerida a encontrar
50,000% de tiempo, 50,000% de ubicaciones, 70,000% de situaciones

Figura 3.46 Estadísticas del enlace cámara 5 – cámara 11

3.11.1.11 Enlace cámara 5 – cámara 12

En la Figura 3.47 se muestra la simulación del enlace entre cámara 5 y cámara 12 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

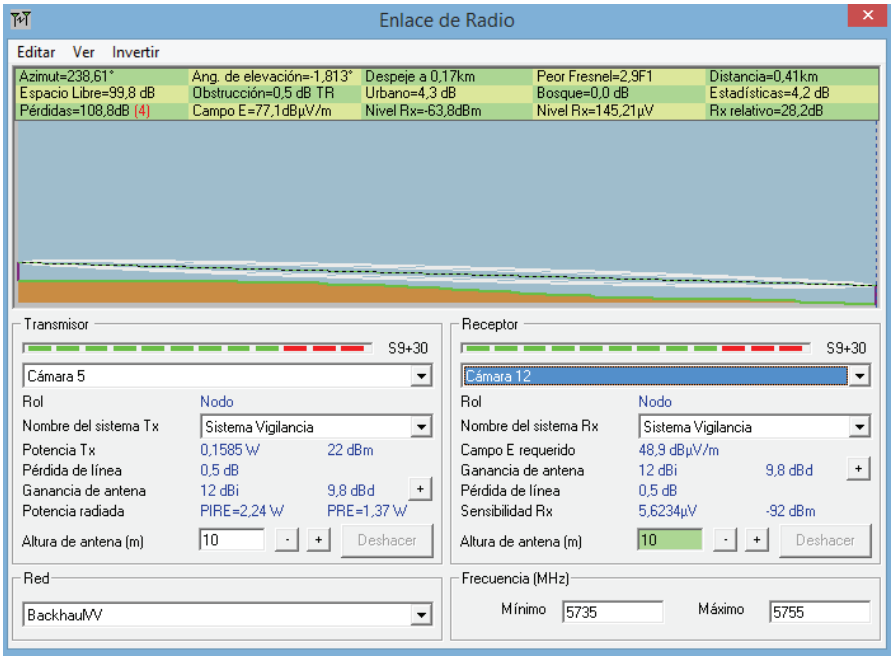


Figura 3.47 Enlace cámara 5 – cámara 12 con características de enlace

En la Figura 3.48 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

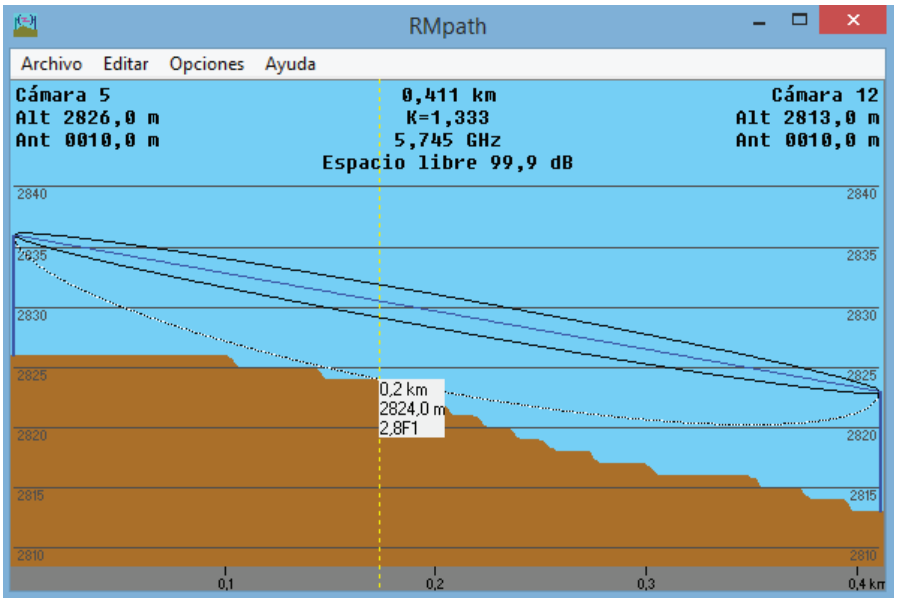


Figura 3.48 Enlace cámara 5 – cámara 12 en base a la zona de Fresnel

En la Figura 3.49 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 28,2 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

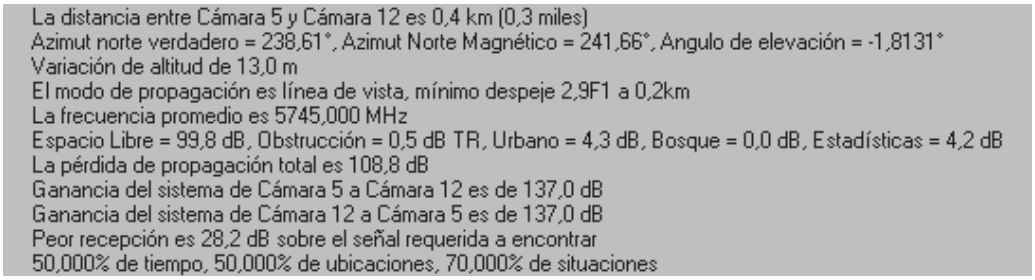


Figura 3.49 Estadísticas del enlace cámara 5 – cámara 12

3.11.1.12 Enlace cámara 5 – cámara 13

En la Figura 3.50 se muestra la simulación del enlace entre cámara 5 y cámara 13 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

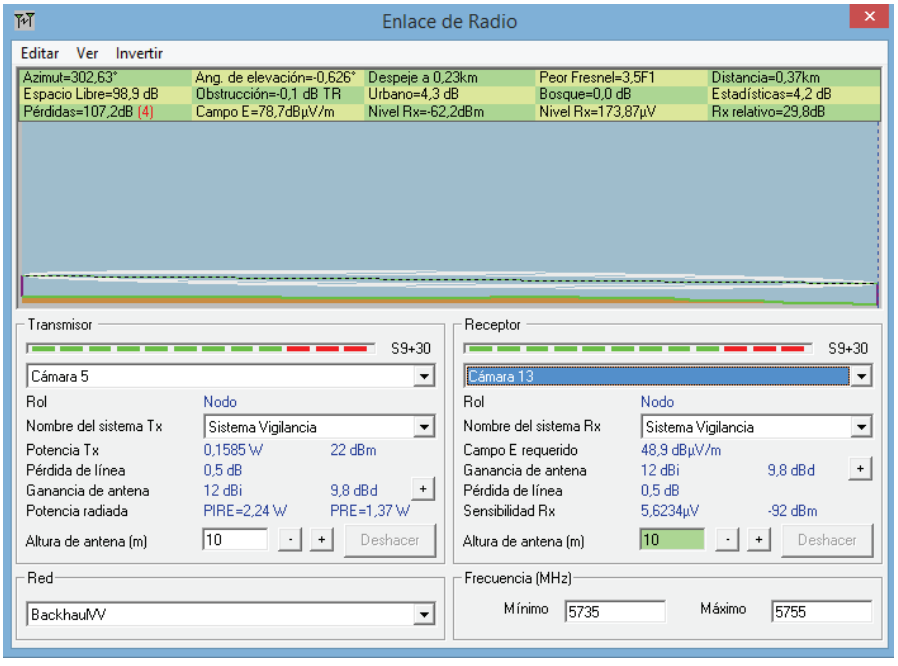


Figura 3.50 Enlace cámara 5 – cámara 13 con características de enlace

En la Figura 3.51 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

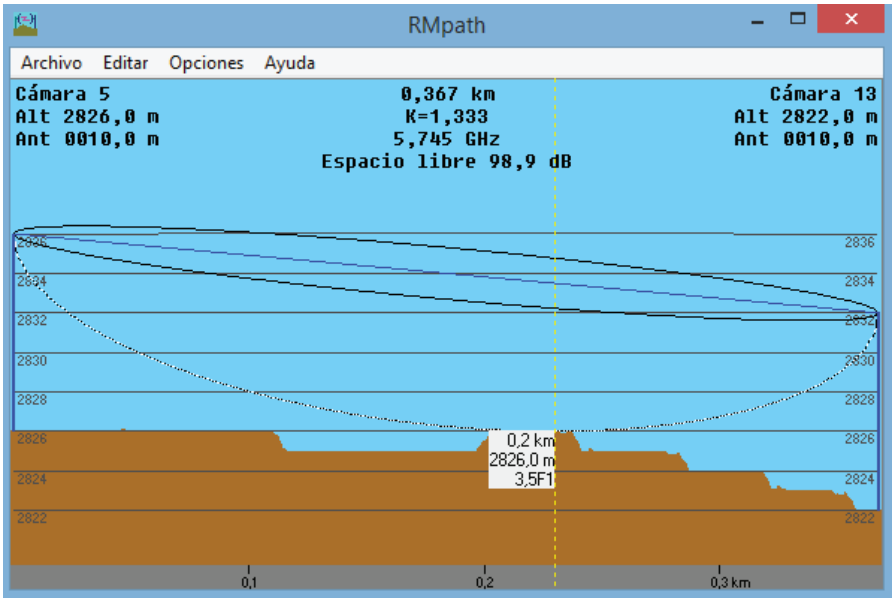


Figura 3.51 Enlace cámara 5 – cámara 13 en base a la zona de Fresnel

En la Figura 3.52 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 29,8 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

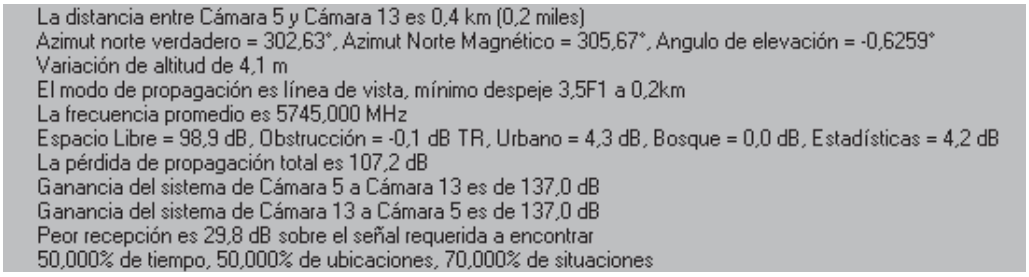


Figura 3.52 Estadísticas del enlace cámara 5 – cámara 13

3.11.1.13 Enlace cámara 5 – cámara 14

En la Figura 3.53 se muestra la simulación del enlace entre cámara 5 y cámara 14 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

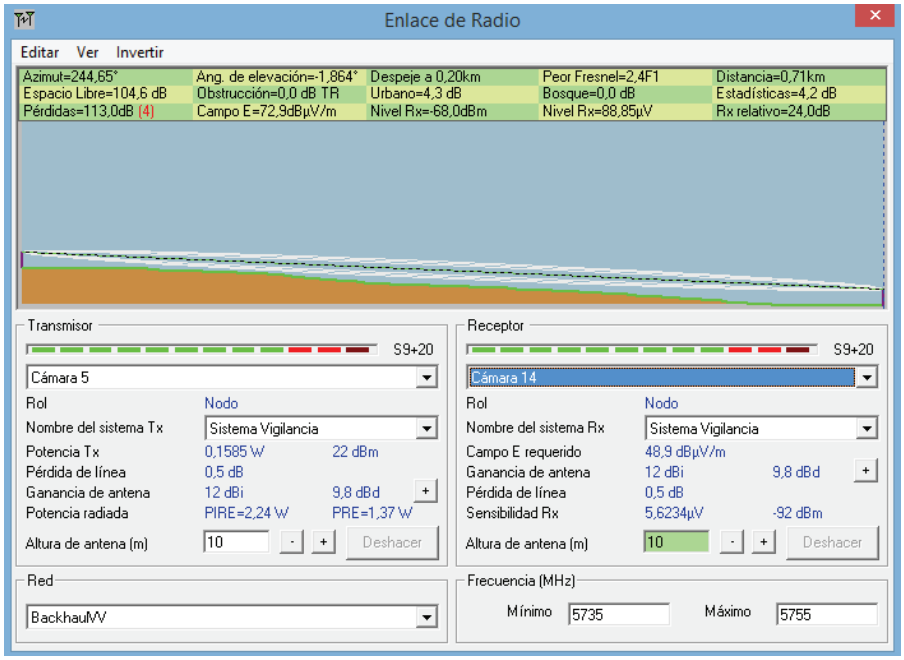


Figura 3.53 Enlace cámara 5 – cámara 14 con características de enlace

En la Figura 3.54 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

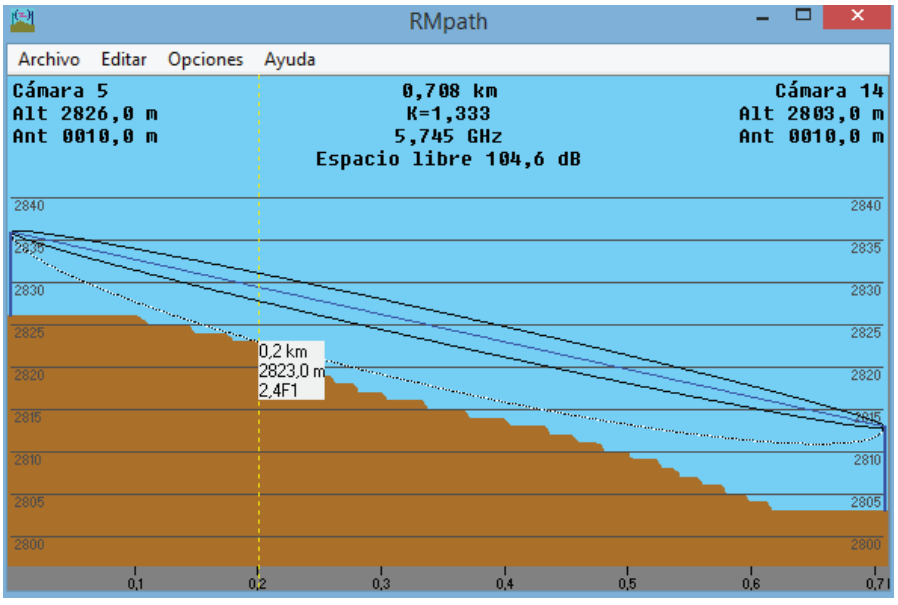


Figura 3.54 Enlace cámara 5 – cámara 14 en base a la zona de Fresnel

En la Figura 3.55 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 24 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

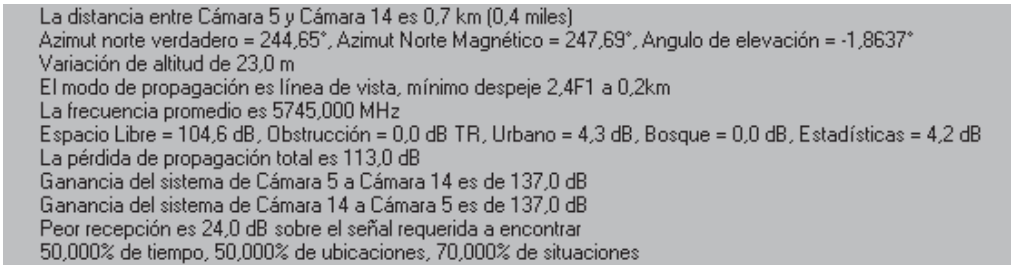


Figura 3.55 Estadísticas del enlace cámara 5 – cámara 14

3.11.1.14 Enlace cámara 5 – cámara 15

En la Figura 3.56 se muestra la simulación del enlace entre cámara 5 y cámara 15 con todos los parámetros ingresados para el enlace. Se puede destacar que se tiene un claro despeje de la línea de vista entre los dos puntos.

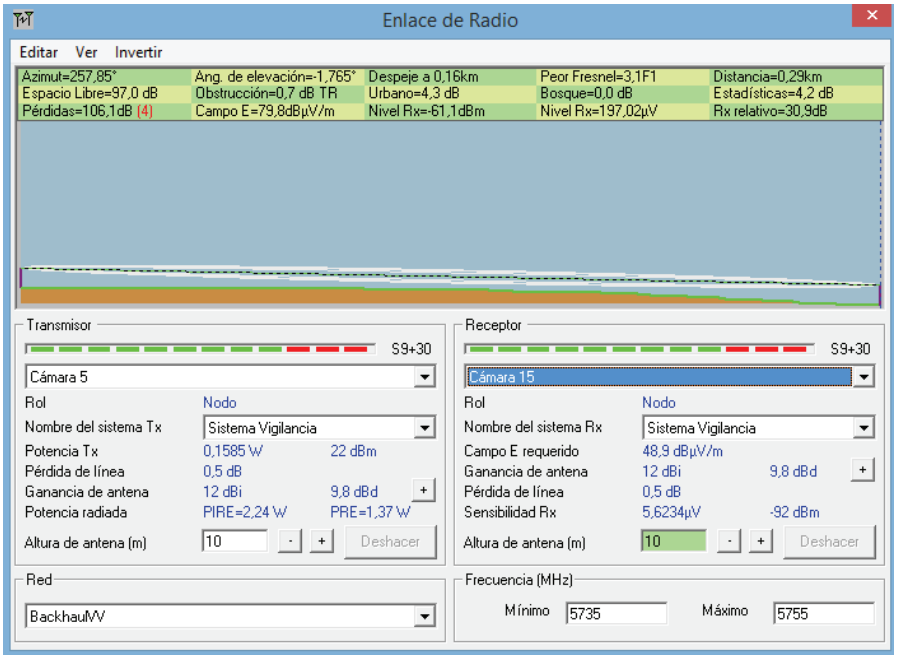


Figura 3.56 Enlace cámara 5 – cámara 15 con características de enlace

En la Figura 3.57 se presenta una mejor visualización de la peor zona de Fresnel con respecto al perfil topográfico de la zona.

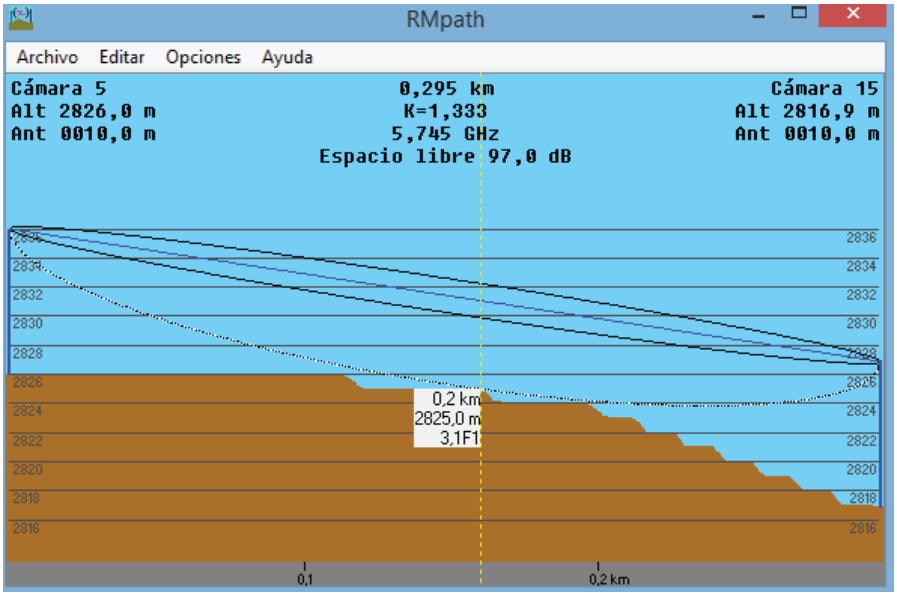


Figura 3.57 Enlace cámara 5 – cámara 15 en base a la zona de Fresnel

En la Figura 3.58 se presenta las estadísticas del enlace, en donde, se puede apreciar que la peor recepción de la señal es de 30,9 dB sobre la señal que se espera recibir (Margen respecto al Umbral), lo que garantiza la vialidad del enlace.

La distancia entre Cámara 5 y Cámara 15 es 0,3 km (0,2 miles)
Azimut norte verdadero = 257,85°, Azimut Norte Magnético = 260,90°, Angulo de elevación = -1,7651°
Variación de altitud de 9,1 m
El modo de propagación es línea de vista, mínimo despeje 3,1F1 a 0,2km
La frecuencia promedio es 5745,000 MHz
Espacio Libre = 97,0 dB, Obstrucción = 0,7 dB TR, Urbano = 4,3 dB, Bosque = 0,0 dB, Estadísticas = 4,2 dB
La pérdida de propagación total es 106,1 dB
Ganancia del sistema de Cámara 5 a Cámara 15 es de 137,0 dB
Ganancia del sistema de Cámara 15 a Cámara 5 es de 137,0 dB
Peor recepción es 30,9 dB sobre el señal requerida a encontrar
50,000% de tiempo, 50,000% de ubicaciones, 70,000% de situaciones

Figura 3.58 Estadísticas del enlace cámara 5 – cámara 15

3.12 COSTOS REFERENCIALES DEL SISTEMA [6] [7] [8] [9] [10] [11] [19] [22] [23] [24] [25] [26]

Un parámetro muy importante a la hora de poner en marcha un Proyecto, es conocer el costo que implicaría la implementación del mismo. Por tal razón, en esta sección se presenta el costo referencial que implicaría la implementación del sistema de video-vigilancia en la ciudad de Cayambe.

En el costo referencial se encuentra incluido el precio de los diferentes equipos de video, así como el de la mano de obra necesaria para la puesta en marcha de este sistema. El precio de los programas necesarios para la administración y gestión del sistema no será tomado en cuenta debido a que estos programas vienen incluidos en la compra de los equipos.

3.12.1 EQUIPOS PARA SISTEMA DE VIDEO-VIGILANCIA

En la Tabla 3.18 se presentan los equipos necesarios para el funcionamiento del sistema de video-vigilancia con sus respectivos costos.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO ($)	PRECIO ENVÍO ($)	PRECIO TOTAL ($)
Servidor de video Hikvision DS-9616NI-ST-24TB	1	7216	0	7216
RouterBoard 433 GL	15	111,55	0	1673,25
Mini slot Board 52Hn	15	42,98	0	644,7
Conector MMCX to N female	30	4,29	6,99	338,4
Antena Onmidireccional TerraWave 12 dBi	30	124,74	0	3742,2
Cámaras Hikvision modelo DS-2DE4220-AE	15	599	0	8985
Case Outdoor CAOTU	15	89	0	1335
Total				**23934,55**

Tabla 3.18 Costo equipos para sistema de video-vigilancia

Los precios han sido sacados de páginas de venta como Ebay y Amazon (en la bibliografía se encuentran las direcciones electrónicas de todas estas páginas) debido a que no se pudo encontrar estos productos en el mercado ecuatoriano. En la Tabla 3.18 consta el precio de los equipos así como el costo de envío.

3.12.2 SERVICIO DE INTERNET

Para tener acceso al sistema de manera remota es necesario tener salida al internet. Sin embargo, en este diseño no es prioridad tener un acceso remoto en tiempo real al sistema. Por esta razón, las velocidades de conexión pueden ser mucho menor a las requeridas en la sección 3.8, lo que si se debe tener presente es que la salida a internet sea por fibra, de este modo, cuando se requiera ampliar las velocidades de conexión se lo pueda hacer de manera instantánea. En función de esto, se ha seleccionado a la empresa Telconet para que sea la proveedora del servicio de Internet debido a que cuentan con la infraestructura necesaria para brindar su servicio en la ciudad de Cayambe (ver Tabla 3.19).

ESPECIFICACIONES	TELCONET
Tipo de Conexión	IP fija
Velocidad de conexión	1 Mbps, Simétrica
Compartición del servicio	1 a 1
Seguridad	Firewall
Última milla	Fibra óptica
Costo ($)	160 / mes

Tabla 3.19 Costo servicio de Internet

3.12.3 ALIMENTACIÓN ELÉCTRICA

Como se mencionó anteriormente, es necesario conectar los equipos de video a equipos UPS, de esta manera, se puede tener vigilancia aun cuando el suministro de energía eléctrica sea suspendido, debido a cortes o daños en el sistema eléctrico de la ciudad. Por tal razón se presenta al equipo CORNELL modelo B-5243A el cual permite alimentar los equipos y sus características principales se muestran en la Tabla 3.20. Su hoja de datos se encuentra en el ANEXO E. Cabe

recalcar que este equipo es para ambiente interior, por tal razón es necesario colocarlo dentro de un gabinete metálico para exteriores.

ESPECIFICACIONES	CORNELL BATTERY BACKUP MODELO B5243A	GABINETE ALLIED MOULDED MODELO AMU1860LF
Voltaje de Entrada	115 AC/ 60 Hz	N/A
Voltaje de Salida	12/24 DC	N/A
Horas de reserva	7AH	N/A
Dimensiones	16"*12"*5"	18"*16,3*10,1
Costo ($)	50	205,55
Costo envío ($)	29	0
Costo unitario ($)	79	205,55
Costo Total ($)	1185	3083,25

Tabla 3.20 Costo alimentación eléctrica

Los precios han sido sacados de páginas de venta como Ebay y Amazon (en la bibliografía se encuentran las direcciones electrónicas de todas estas páginas) debido a que no se pudo encontrar estos productos en el mercado ecuatoriano. En la Tabla 3.20 consta las características, el precio de los equipos y el costo de envío.

3.12.4 MANO DE OBRA

En la Tabla 3.21 se presenta el costo de la mano de obra necesaria para la instalación, configuración y puesta en marcha del sistema de video-vigilancia con sus respectivos costos.

DESCRIPCIÓN	# DE PERSONAS	COSTO POR DÍA	# DÍAS	TOTAL ($)
Mano de Obra	5	50	4	1000

Tabla 3.21 Costo mano de obra

3.12.5 COSTO TOTAL DEL PROYECTO

En la Tabla 3.22 se presenta el costo total que implicaría la implementación del sistema de video-vigilancia en la ciudad de Cayambe

DESCRIPCIÓN	COSTOS ($)
Equipos para sistema de video-vigilancia	23934,55
Servicio de Internet	160
Alimentación eléctrica	4268,25
Mano de Obra	1000
Total	**29362,8**

Tabla 3.22 Costo referencial total del Proyecto

El valor obtenido en la Tabla 3.22 es únicamente referencial. Al obtener un valor que sobrepasa los $ 20000, es necesario traer estos productos a través de una empresa importadora que tenga los permisos necesarios para hacerlo. El costo de importación dependerá del precio y peso de los equipos, este costo no ha sido tomado en cuenta debido a que no fue posible realizar la cotización de éstos equipos con ninguna empresa.

CAPÍTULO 4
IMPLEMENTACIÓN DEL PROTOTIPO DEL SISTEMA, PRUEBAS Y RESULTADOS

En este capítulo se presenta el desarrollo de un prototipo del sistema de video-vigilancia, el mismo que servirá para realizar las pruebas de funcionamiento del sistema. Se procederá a documentar los principales procedimientos, configuraciones de los equipos y a registrar los resultados obtenidos.

4.1 PROTOTIPO DEL SISTEMA DE VIDEO-VIGILANCIA [1] [2] [3] [4] [5] [6] [7] [8]

El prototipo del sistema se basa en la implementación de un sistema de video-vigilancia de bajo nivel, el cual tiene como objetivo, reflejar el funcionamiento y la utilidad del sistema. En la Figura 4.1 se presenta el prototipo del sistema a implementar.

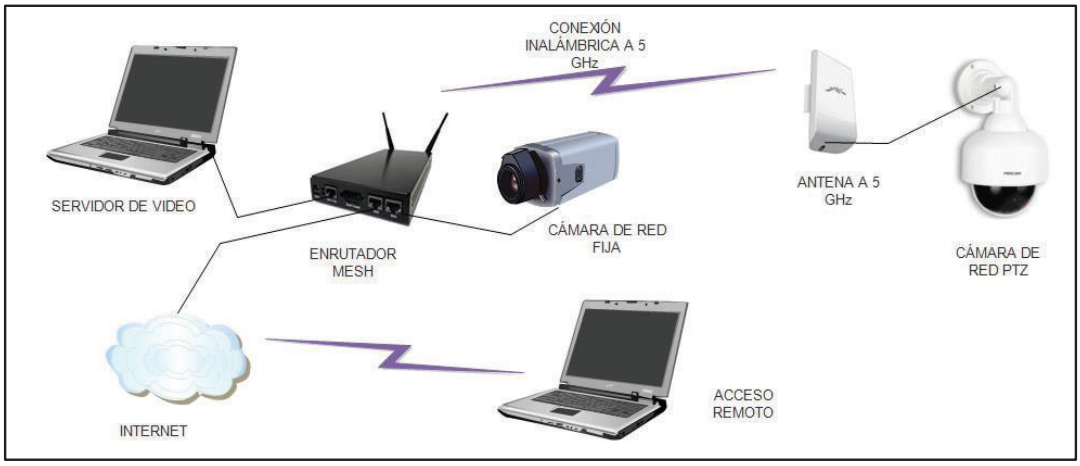


Figura 4.1 Diagrama prototipo sistema de video-vigilancia

En la Figura 4.1 el equipo enrutador mesh tiene 3 puertos Ethernet, los cuales se utilizarán de la siguiente manera:

- Ether1, puerto WAN (Internet).
- Ether2, puerto LAN (Servidor de video).
- Ether3, puerto LAN (Cámara de red fija).

Adicional a esto, el equipo enrutador irradia una señal a 5 GHz por medio de la cual se conectará la cámara de red PTZ al servidor de video. Para el caso del acceso remoto es necesario contar con un punto de red que permita acceder al sistema por medio de la Internet.

Los equipos a utilizar en el prototipo son los siguientes:

- Dos cámaras de red.
- Un router mesh Mikrotik 433UL con dos antenas de ganancia 5 dBi c/u.
- Un punto de acceso Ubiquiti Nano loco 5.
- Un computador, el cual hará las funciones de servidor de video y de administrador del sistema.
- Un computador para el acceso remoto al sistema.

4.1.1 CONFIGURACIÓN DEL ENRUTADOR MIKROTIK

Para la configuración del equipo Mikrotik es necesario descargar e instalar el programa **Winbox**, el cual es gratuito y se lo puede conseguir en la página oficial de Mikrotik. Este programa puede ejecutarse en entornos Linux, Windows y MacOS. Permite acceder a las múltiples configuraciones de los equipos Mikrotik desde un computador por medio de un entorno gráfico (ver Figura 4.2).

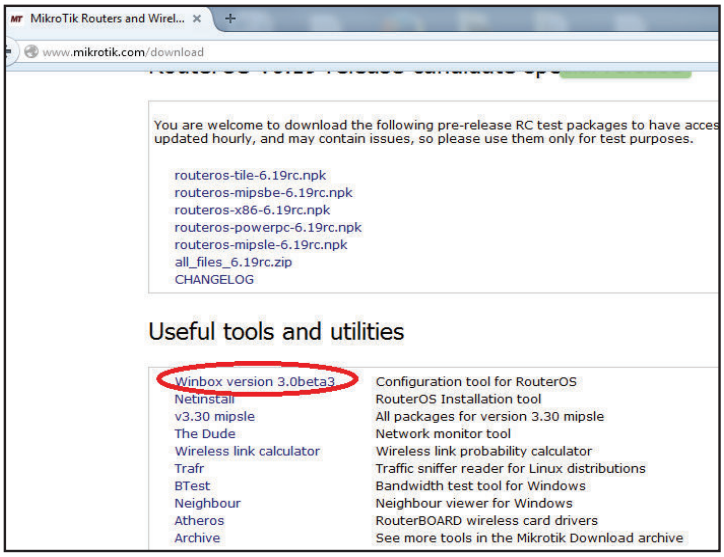


Figura 4.2 Descarga software Winbox [2]

Una vez descargado e instalado el programa Winbox se puede acceder al equipo Mikrotik y observar las interfaces que tiene el equipo.

4.1.1.1 Identificación del Equipo

Se le asigna un nombre al equipo con la finalidad de poder identificar a cada enrutador de manera individual. De acuerdo a la simulación presentada en la Cap. 3, el equipo que se va a configurar es el que se conecta con el servidor de video (NVR), denominado **enrutador 5**. Para identificar al equipo se debe hacer lo siguiente:

- Click en la opción **System**, se desplegará un menú de opciones.
- Click en la opción **Identity**, aparecerá una ventana.
- Se coloca el nombre del equipo, en este caso **Enrutador 5.**
- Click en **Apply** y luego en **Ok.**

En la Figura 4.3 se muestra la configuración de la identificación del equipo.

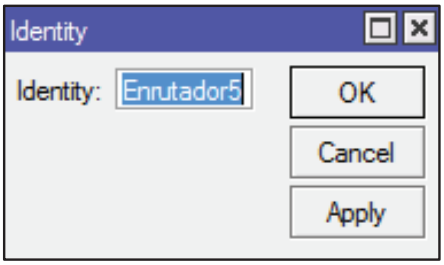


Figura 4.3 Identificando equipo Mikrotik

4.1.1.2 Configuración de las interfaces Ethernet

El equipo Mikrotik tiene 3 interfaces Ethernet, las cuales se van a renombrar para poder identificarlas más fácilmente:

- Ether1 cambia a WAN1.
- Ether2 cambia a NVR2.
- Ether3 cambia a LAN3.

La interface WAN1 se utilizará para conectar el sistema a la Internet y de esta manera permitir un acceso remoto, para esto, se debe configurar la interfaz como DHCP[17] cliente, de esta manera se obtendrán los valores necesarios de Gateway[18] y DNS[19] para conectarse a la red de manera automáticamente.

Para configurar a la interfaz WAN1 como DHCP cliente se deben seguir los siguientes pasos:

- Click en la opción **IP**, se desplegará un menú de opciones.
- Click en la opción **DHCP client**, aparecerá una ventana.
- Click en la opción **New DHCP client**, aparecerá una ventana.

---

[17] DHCP.- Dynamic Host Configuration Protocol, es un protocolo que permite a los clientes de una red puedan obtener parámetros para una configuración automática.

[18] Default Gateway.- Puerta de enlace por defecto.- es la ruta que se le asigna a un equipo para que éste envié cualquier paquete que no se conozca su dirección destino.

[19] DNS.- Domain Name System.- es un sistema de nomenclatura jerárquica para equipos conectados en un red que tiene como función traducir nombres inteligibles en identificadores binarios.

- Se escoge el tipo de interfaz que trabajará como DHCP cliente, en este caso la WAN1.
- Click en la opción **Apply** y luego en **Ok.**

En la Figura 4.4 se muestra la configuración de la interfaz WAN1 como DHCP cliente.

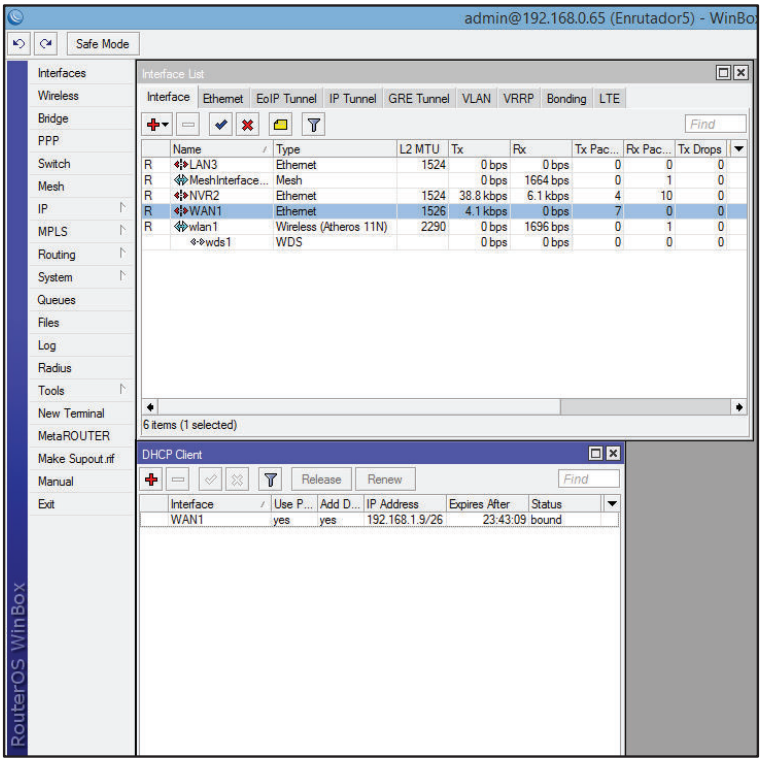


Figura 4.4 Configurando la interfaz WAN1 como DHCP cliente

La interface NVR2 será la que conecte el equipo Mikrotik con el servidor de video, por lo tanto, se le asignará la dirección IP correspondiente. Para asignar la dirección IP se deben seguir los siguientes pasos:

- Click en la opción **IP**, se desplegará un menú de opciones.
- Click en la opción **Addresses**, aparecerá una ventana.
- Click en la opción **New Addresss**, aparecerá una ventana.
- Se asigna la dirección IP 192.168.0.65/30.
- Se selecciona el tipo de interfaz, en este caso NVR2.

- Click en la opción **Apply** y luego en **Ok**.

En la Figura 4.5 se muestra la configuración de la interfaz para la conexión con el servidor de video.

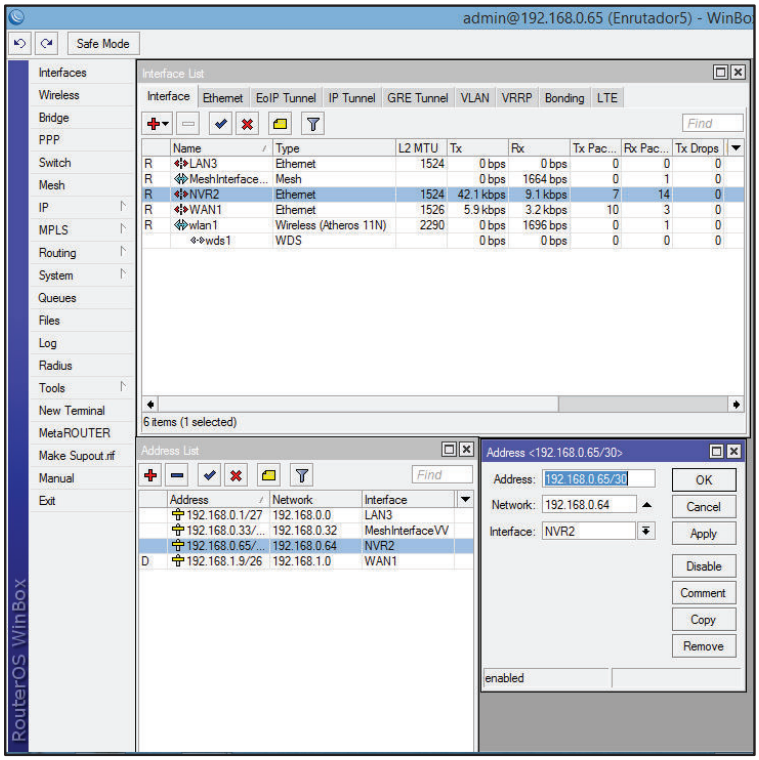


Figura 4.5 Configuración interfaz NVR2

La interface LAN3 será la que conecte el equipo Mikrotik con la cámara de red, por lo tanto, se le asignará la dirección IP correspondiente. Para asignar la dirección IP se deben seguir los siguientes pasos:

- Click en la opción **IP**, se desplegará un menú de opciones.
- Click en la opción **Addresses**, aparecerá una ventana.
- Click en la opción **New Addresss**, aparecerá una ventana.
- Se asigna la dirección IP 192.168.0.1/27.
- Se selecciona el tipo de interfaz, en este caso LAN3.
- Click en la opción **Apply** y luego en **Ok.**

En la Figura 4.6 se muestra la configuración de la interfaz LAN3.

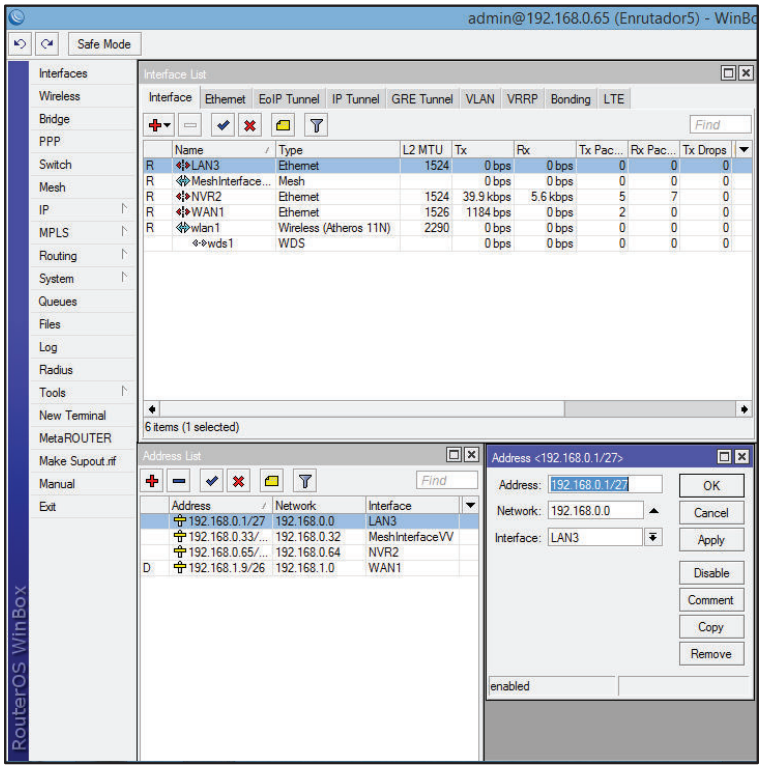


Figura 4.6 Configuración interfaz LAN3

4.1.1.3 Configuración de la interfaz Mesh

Para la configuración inalámbrica Mesh se deben seguir los siguientes pasos:

- Click en la opción **Mesh**, aparecerá una ventana.
- Click en la opción **New Interface**, aparecerá una ventana en la cual se pondrá el nombre de la interfaz que servirá para que puedan verse las dos tarjetas inalámbricas, en este caso se llamará MeshInterfaceVV.
- Click en la opción **Apply** y luego en **Ok.**
- Click en la opción **Ports** de la misma ventana **New Interface.**
- Click en la opción **New Mesh Port**, se selecciona la interfaz inalámbrica que se empleará, en este caso la **wlan1.**
- Click en la opción **Apply** y luego en **Ok.**

- Luego se le asigna una dirección IP, en este caso 192.168.0.33/27.

En la Figura 4.7 se muestra la configuración de la interfaz inalámbrica mesh.

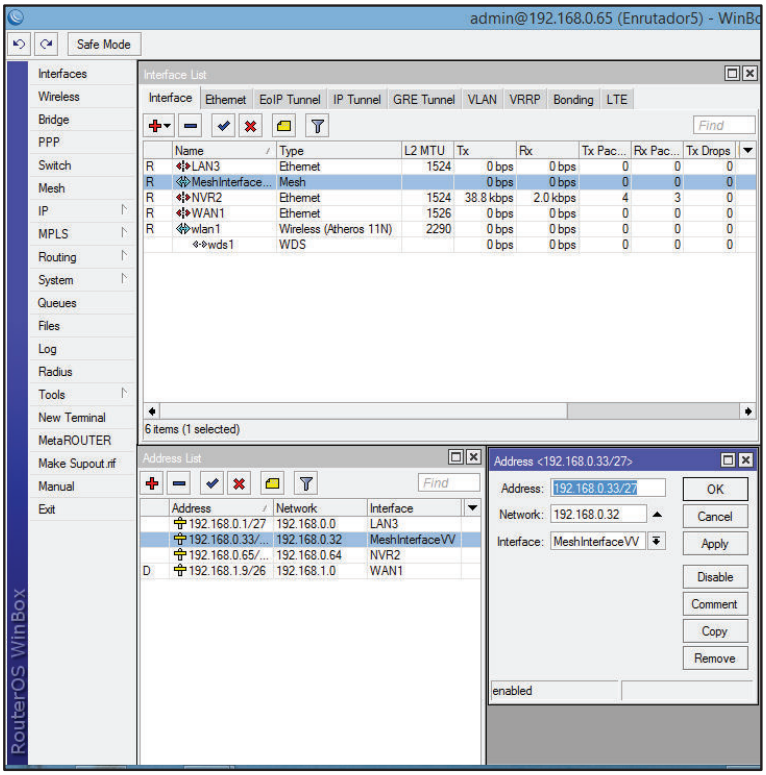


Figura 4.7 Configuración de la interfaz mesh

4.1.1.4 Configuración de la red inalámbrica

Para la configuración de la interfaz inalámbrica, se siguen los siguientes pasos:

- Click en la opción **Wireless**, aparecerá una ventana en la que se muestran las interfaces inalámbricas disponibles, en este caso wlan1.
- Dar doble click sobre la interface wlan1, aparecerá una ventana de configuración de la interface.
- Dar click sobre la pestaña **Wireless** y se eligen los siguientes parámetros:

  Mode: ap bridge

  Band: 5GHz-A/N

  Channel Width: 20 Mhz

Frequency: 5805

SSID: BackhaulVV

Wireless Protocol: any

- Dar click sobre la pestaña **WDS** y se elegir los siguientes parámetros:

  WDS Mode: static mesh

  WDS Default Bridge: MeshInterface

- Click en la opción **Apply** y luego en **Ok.**
- Para establecer una clave de red, en la ventana **Wireless Tables** dar click en **Security Profiles.**
- Dar click en New y crear un perfil de seguridad que luego deberá ser anclado a la red inalámbrica.

En la Figura 4.8 se muestra la configuración de la interfaz inalámbrica WLAN.

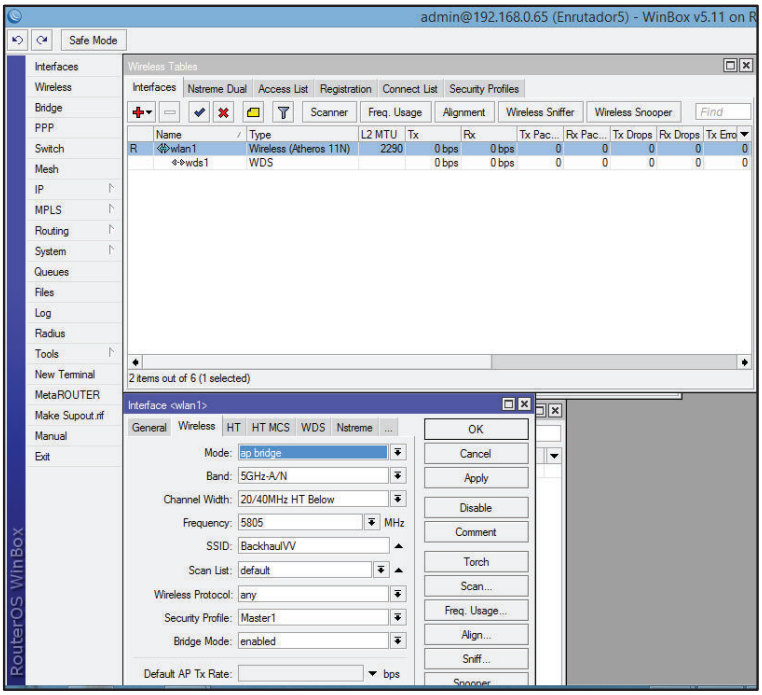


Figura 4.8 Configuración interfaz inalámbrica wlan1

En la Figura 4.9 se muestra la configuración de las seguridades con las que contará la red inalámbrica mesh.

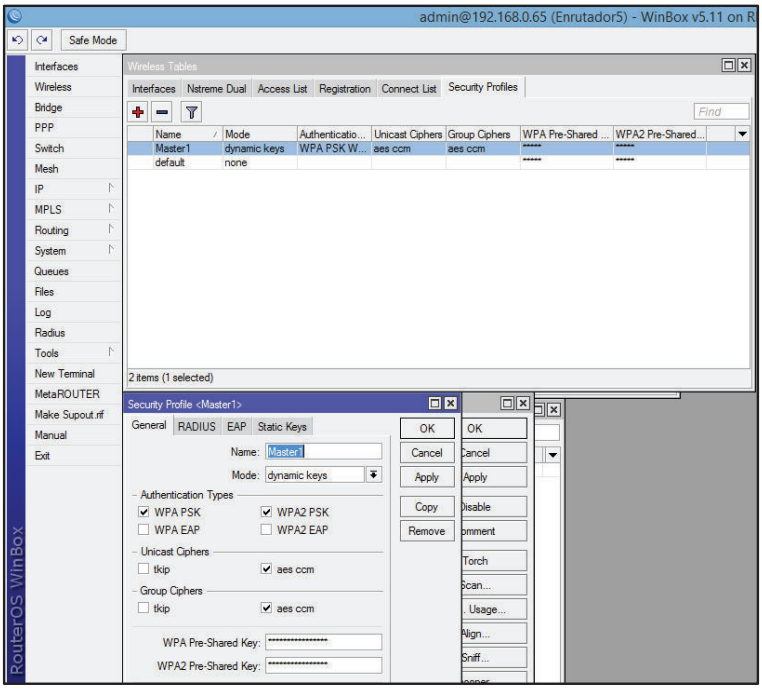


Figura 4.9 Configuración clave de seguridad red inalámbrica

Al utilizar el modo WDS static mesh es necesario colocar la dirección MAC del equipo vecino de manera manual, en este caso se colocará la dirección MAC del equipo nanostation loco M5. Esto se lo hace debido a que son equipos de diferentes marcas y podría generar problemas de comunicación.

Para ingresar la dirección MAC del equipo nanostation se siguen los siguientes pasos:

- En la ventana **WirelessTables**, se selecciona la interfaz **wlan1.**
- Se da click en el icono  y se selecciona **WDS**, aparecerá una nueva ventana en la que se colocará la dirección MAC del equipo nanostation loco M5.
- Click en la opción **Apply** y luego en **Ok.**

En la Figura 4.10 se muestra la configuración de la interfaz inalámbrica WLAN1 como WDS estático.

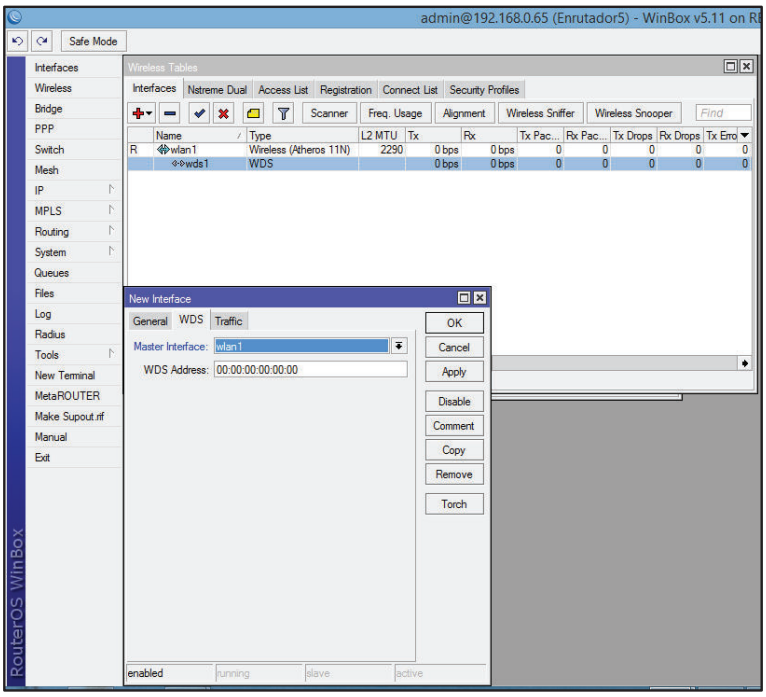


Figura 4.10 Configuración WDS estático en wlan1

4.1.2 CONFIGURACIÓN DEL EQUIPO NANO LOCO M5

Al no contar con otro equipo enrutador Mikrotik para conectar la cámara PTZ al servidor de video, se ha utilizado un equipo nano loco M5 para suplir esta tarea.

El equipo nano loco no tiene la funcionalidad de un enrutador mesh, sin embargo, para fines demostrativos, se lo utilizará para conectar la cámara PTZ al servidor de video de manera inalámbrica. Para esto, se deben seguir los siguientes pasos:

- Ingresar a la configuración del equipo vía web.
- Una vez dentro, en la pestaña **Wireless** se elige el modo **Station.**
- Se selecciona la red a la cual se va a conectar, en este caso la red BackhaulVV.
- Se ingresa la contraseña de la red y se conecta automáticamente.
- En la pestaña **Network** se elige el modo de funcionamiento **Bridge.**
- En la parte de **Management Network Settings** se elige la opción de Administración de dirección IP como **Static.**

- Se ingresa la dirección IP del equipo.
- Se hace click en la opción **Chance** y luego en **Apply.**

En la Figura 4.11 se muestra la configuración del equipo Nanostation Loco M5.

Figura 4.11 Configuración equipo Nanostation Loco M5

4.1.3 CONFIGURACIÓN DE LAS CÁMARAS IP

Para la configuración de las cámaras de red es necesario ingresar los valores de dirección IP, Mascara de red, Puerta de enlace y servidor DNS en función del enrutador al que están conectados. Para el caso de la cámara de red fija, se conectará al puerto Ethernet LAN3 del equipo Mikrotik y en el caso de la cámara de red PTZ se conectará al puerto Ethernet del equipo nanostation loco M5.

4.1.4 CONFIGURACIÓN DEL SERVIDOR DE VIDEO

Como se había dicho anteriormente, al no contar con un equipo NVR, se simulara el funcionamiento de este equipo mediante un computador denominado servidor de video, en el cual se instalará un programa que permita cumplir esta tarea.

El programa que se ha elegido es el Blue Iris, el cual se lo puede descargar de su página oficial. Este es un programa con licencia, sin embargo, permite ejecutar una versión demo del mismo la cual cuenta con todas las funcionalidades del programa licenciado, pero por quince días únicamente. Soporta la especificación ONVIF lo que garantiza que podrá ser conectado a la mayoría de cámaras de red existentes en el mercado y aparte de esto, es un programa muy intuitivo que presenta muy buenas características a la hora de gestionar el sistema de video-vigilancia.

Para configurar nuestro servidor de video se debe hacer lo siguiente:

- Click en la ventana de **Opciones.**
- Click en **Servidor Web.**
- Por default el programa viene configurado para utilizar el puerto 80, sin embargo, se puede poner cualquier puerto.
- Se coloca la dirección privada del servidor y la dirección pública de salida al Internet.

En la Figura 4.12 se muestra la configuración del servidor de video (Blue Iris).

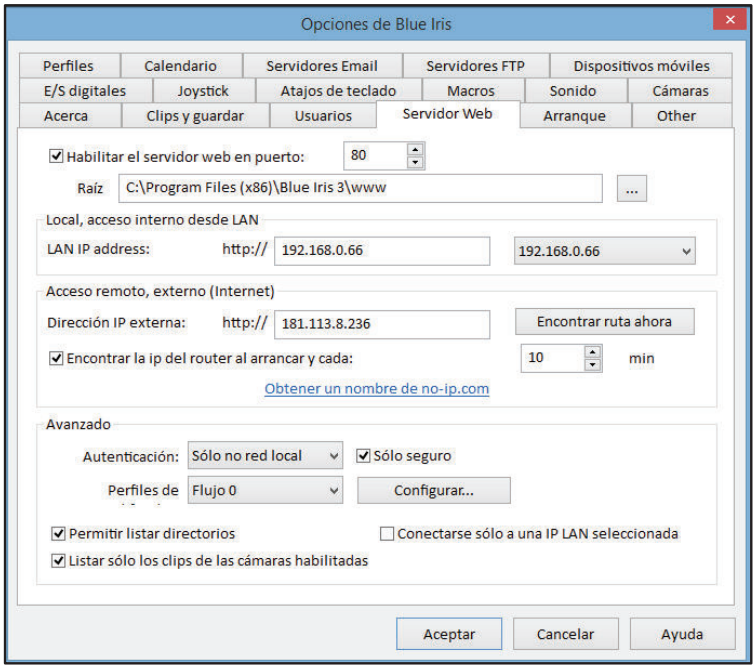


Figura 4.12 Configuración Servidor de Video

Para configurar las grabaciones de video, se debe hacer lo siguiente:

- Click en la ventana de **Opciones.**
- Click en **Clips y Guardar.**
- Se puede elegir el tiempo de grabación, así como el tiempo que permanecerá almacena la información en el disco duro.

En la Figura 4.13 se muestra la configuración del tiempo de grabación y el lugar donde se van a guardar los videos.

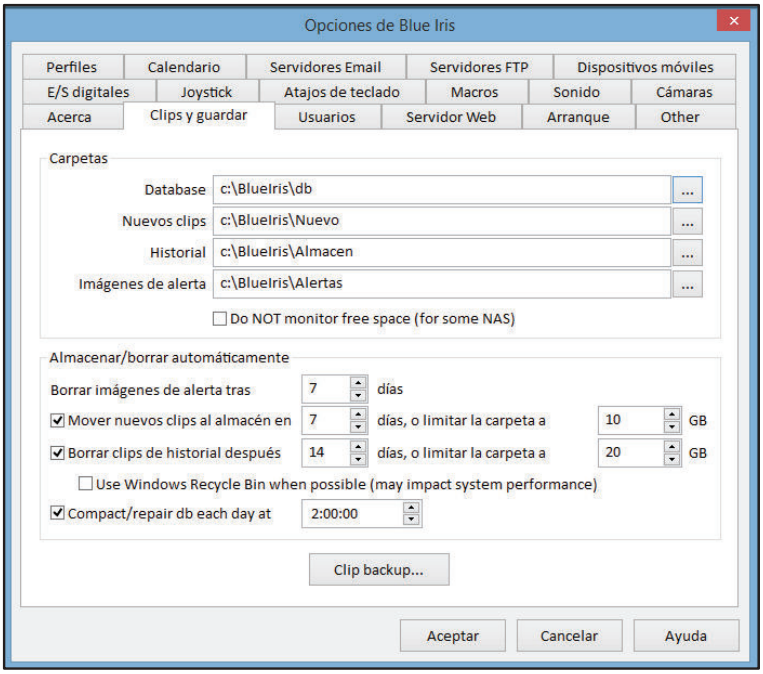


Figura 4.13 Configuración grabaciones de video

4.1.5 CONFIGURACIÓN DEL SISTEMA DE ADMINISTRACIÓN Y GESTIÓN

La administración y gestión del video se lo hará desde el equipo servidor de video, por medio del programa Blue Iris. Para poder acceder a las imágenes de las cámaras de red, es necesario adicionar las cámaras a este programa, para esto, se debe realizar lo siguiente:

- Ejecutar el programa Blue iris.

- Click en la opción **Propiedades de la Cámara** y aparecerá una nueva ventana.
- Click en la opción **Video** y luego en **Configurar Red IP.**
- Elegir el modelo de la cámara y colocar la dirección IP de la cámara y su número de puerto.
- Colocar el nombre de usuario y contraseña de la cámara de video-vigilancia.

En las Figura 4.14 y 4.15 se muestra la configuración y adición de cámaras IP al servidor de video.

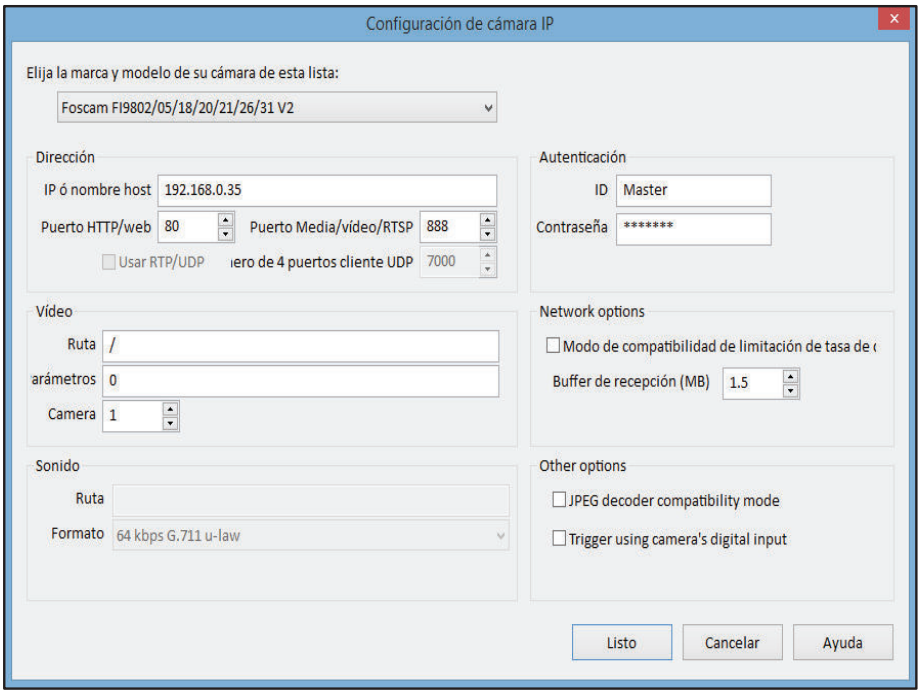


Figura 4.14 Colocando dirección IP y puerto de la cámara de video-vigilancia

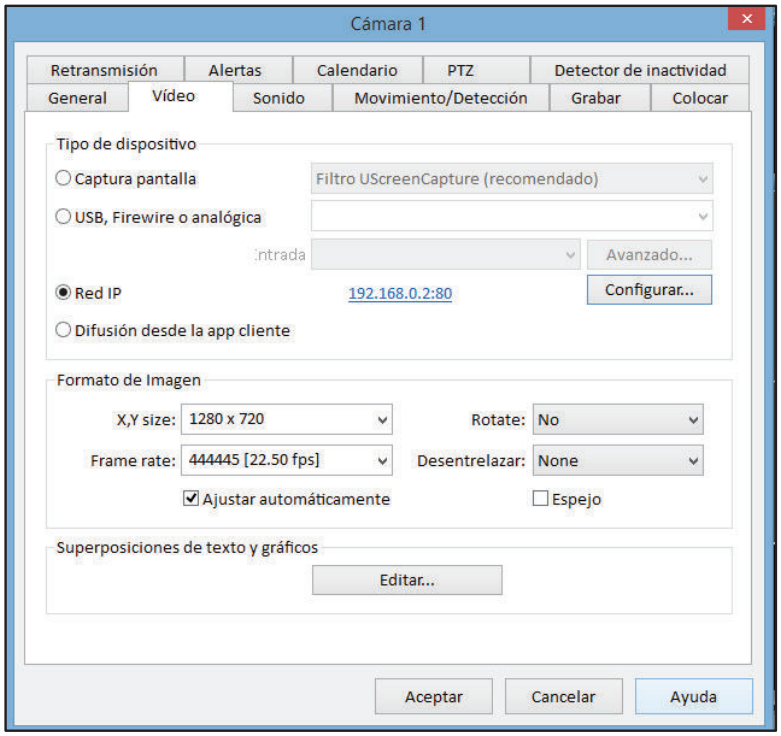


Figura 4.15 Configurando propiedades de la cámara de video-vigilancia

Para crear usuarios que administren el sistema se debe hacer lo siguiente:

- Click en la ventana de **Opciones.**
- Click en la ventana de **Usuarios.**
- Click en **Añadir.**
- Se procede a crear usuarios con distintos niveles de acceso.

En la Figura 4.16 se muestra la configuración de usuarios con distintos niveles de acceso en el servidor de video.

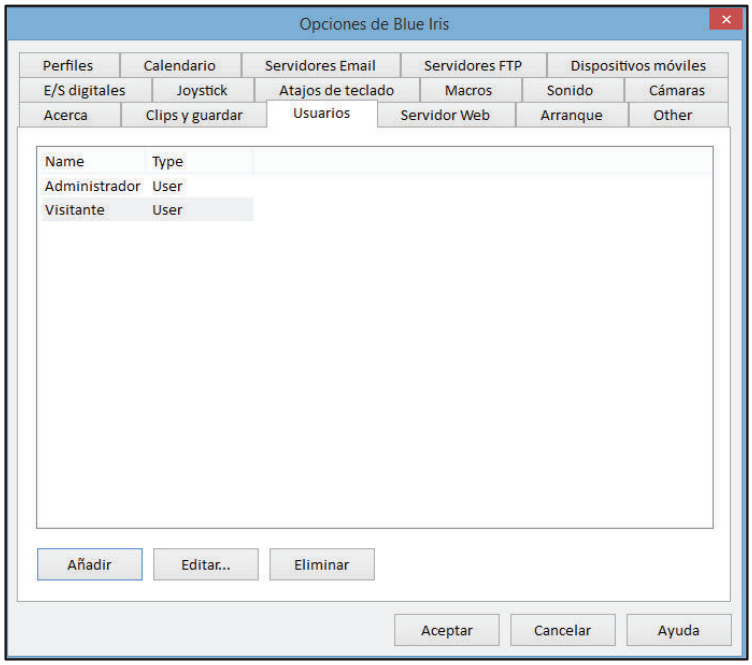


Figura 4.16 Configuración usuarios en el servidor de video

4.1.6 CONFIGURACIÓN DEL ACCESO REMOTO

Para el acceso remoto se debe contar con el servicio de internet por parte de un proveedor. En esta implementación se ha utilizado el servicio de la Corporación Nacional de Telecomunicaciones, tarifa residencial Fast Boy 2, el cual tiene una velocidad de subida de 0.5 Mbps y una velocidad de bajada de 2 Mbps.

Adicional a esto, se debe configurar el router proporcionado por la CNT para que permita acceder remotamente a las imágenes de las cámaras. Para esto se debe habilitar el protocolo HTTP, asignando un puerto en la opción NAT, para esto:

1.- Se dirige a la opción de **Avanzados.**
2.- Se da click en la opción **NAT.**
3.- Se hace click en la opción **Asignación de Puertos.**
4.- Se selecciona la Aplicación, en este caso **Web Server HTTP.**
5.- Se selecciona el protocolo de comunicación que se utilizará, en este caso **TCP.**
6.- Se selecciona el puerto de inicio externo, en este caso 80.

7.- Se selecciona el puerto de fin externo, en este caso 80.

8.- Se coloca la dirección IP del dispositivo al que se va acceder, en este caso la dirección IP del servidor de video.

9.- Se coloca el número de puerto que en el que está habilitado el servicio, en este caso es el 80.

10.- Se da click en la opción **Submit** para que se guarde los cambios.

En la Figura 4.17 se muestra la configuración del router de la CNT para que permita el acceso remoto al servidor de video.

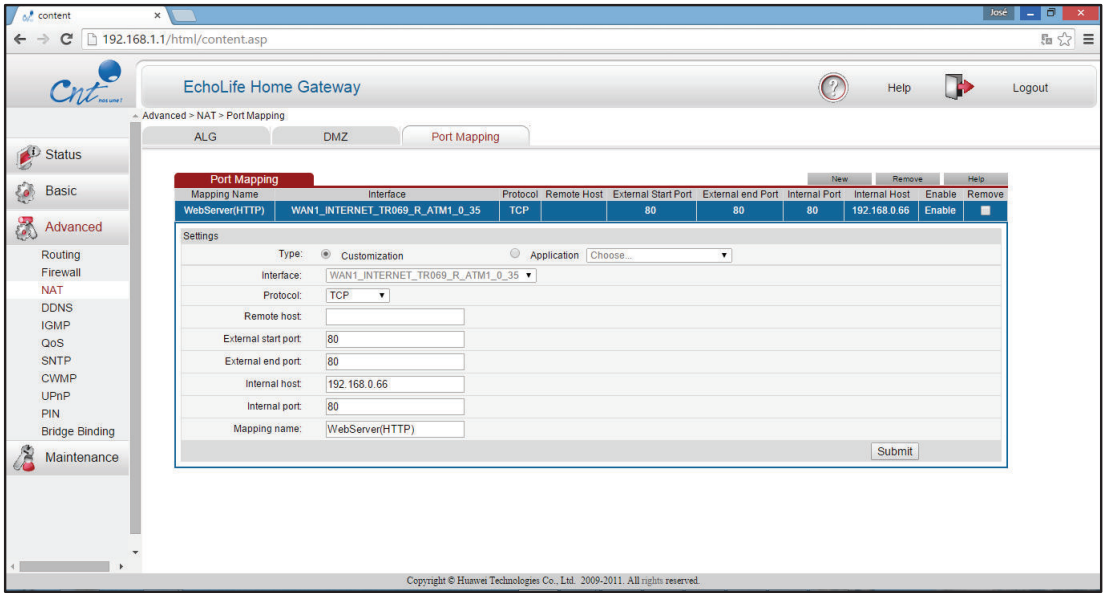


Figura 4.17 Mapeado de puertos en router de acceso a internet

En la Figura 4.18 se muestra la pantalla que aparece cuando se accede remotamente al sistema. En esta pantalla es necesario autenticarse para poder acceder al sistema.

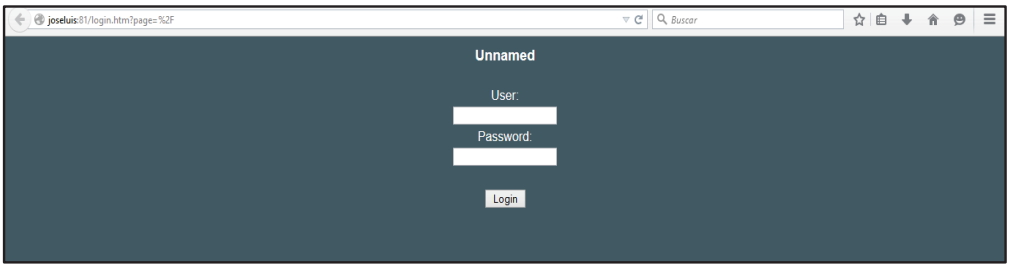


Figura 4.18 Accediendo remotamente al sistema

4.1.7 PRUEBAS Y RESULTADOS

Se comprueba el funcionamiento del prototipo implementado mediante el acceso a las imágenes de la cámara de video-vigilancia y verificando que las grabaciones se almacenen en el disco duro del computador que hace de servidor de video.

En la Figura 4.19 se muestra el funcionamiento del sistema de video-vigilancia.

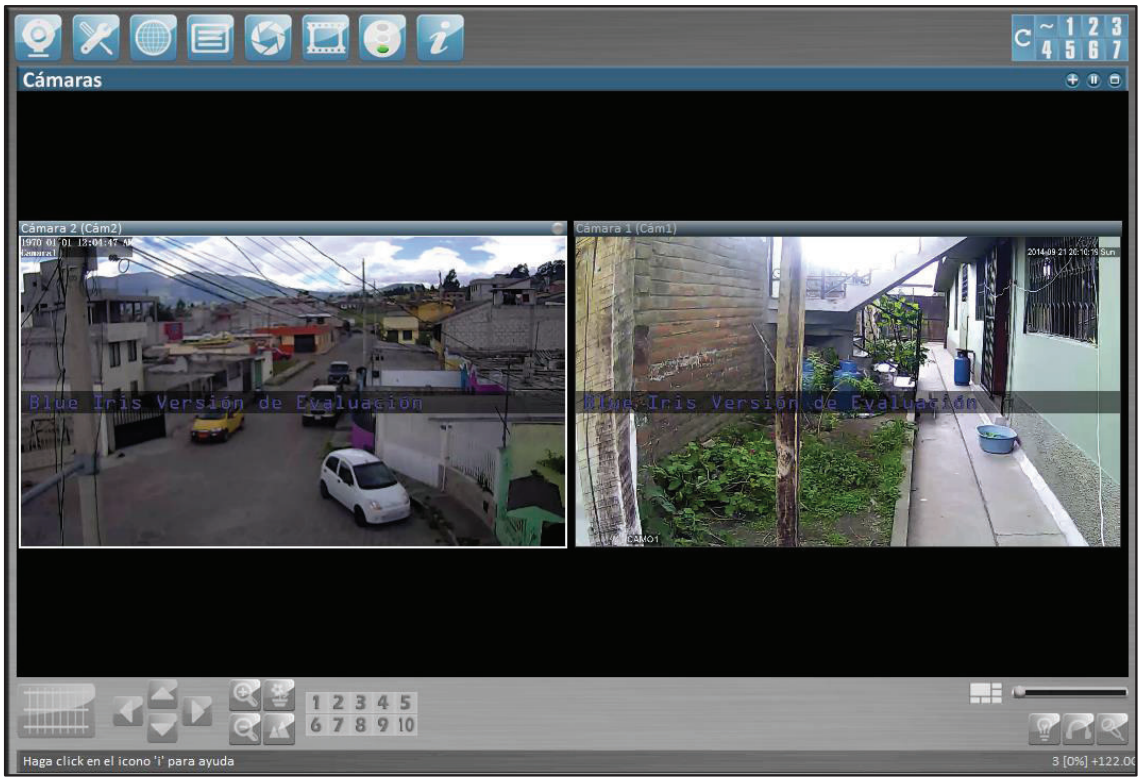


Figura 4.19 Video-vigilancia con el prototipo

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

En este capítulo se dar a conocer las conclusiones a las que se ha podido llegar luego del diseño de un sistema de Video-vigilancia acorde a los requerimientos de la ciudad y también se citaran algunas recomendaciones que serán útiles en la implementación de Proyectos similares.

5.1 CONCLUSIONES

- Un sistema de video-vigilancia no garantiza terminar con el problema de la delincuencia, un sistema de video-vigilancia permite persuadir delincuentes al no cometimiento de actos delictivos y en el caso de que éstos se produzcan, poder identificar a los malhechores. Sin embargo, no se debe pensar que con la colocación de cámaras en la ciudad ya no existirá delincuencia. La mejor manera de evitar que sucedan actos delictivos es la prevención.

- Las redes inalámbricas en malla, basadas en los estándares 802.11x, son una tecnología que aprovecha los beneficios de las redes inalámbricas no licenciadas y que permiten tener mayores alcances y coberturas. Esta tecnología es poco conocida en nuestro país, sin embargo, está siendo muy utilizada en otros países como Colombia, Argentina y España, en donde se la utiliza en actividades como redes comunitarias y sistemas de video-vigilancia.

- Las cámaras de vigilancia fueron ubicadas en lugares donde el índice delictivo es mayor, sin embargo, en caso de necesitar cambiarlas de ubicación, se lo podrá hacer sin mayores inconvenientes. Esta es una de las ventajas de utilizar una red de datos mallada inalámbrica.

- En el caso de implementarse este Proyecto, la tasa de transmisión del sistema será mucho menor que la calculada en el Cap. 3, debido a que, este cálculo fue realizado para las peores condiciones y con cámaras de mayor pixelaje, por lo que es lógico esperar un menor tamaño de almacenamiento de información en el servidor de video.

- La implementación de un sistema de este tipo es beneficioso tanto para la población como para la Policía Comunitaria, ya que se contaría con una nueva herramienta para frenar los actos delictivos. Herramienta que si se la compara con sistemas como el ECU911 es mucho más económica y puede llegar a ofrecer los mismos beneficios.

- Los equipos Mikrotik seleccionados en este diseño, se los puede armar a conveniencia en función de las necesidades que se pretendan cubrir. Esta característica los hace únicos en el mercado. Ofrecen beneficios que llegan a superar marcas muy conocidas como Cisco, Motorola y por un precio mucho menor inferior.

- El uso de sistemas para la gestión y administración permite tener un control más riguroso del mismo y ayuda a evaluar el desempeño de un sistema de una mejor manera.

- En el diseño de este Proyecto no fueron consideradas las cámaras de vigilancia inalámbricas debido a que éstas presentan menores ventajas que las cámaras de red cableadas. Las cámaras de red seleccionadas transmiten su información de manera inalámbrica por medio de los equipos enrutadores conectados a ellas.

- El sistema de video-vigilancia planteado, se encuentra limitado a crecer indefinidamente debido a la capacidad de transmisión de información que permite la red de datos inalámbrica. Sin embargo, para el número de cámaras de vigilancia que se necesitan colocar en la ciudad, teóricamente es posible la transmisión de la información.

- El programa Blue Iris utilizado para la gestión y administración del prototipo del sistema de video-vigilancia, permite tener una mejor idea del funcionamiento de un sistema de gestión y administración de video, ya que permite alertar las caídas de señal de las cámaras, enviar alertas vía correo, realizar la grabación de eventos programados e incluso una vigilancia programada de zonas por horas o días.

- El prototipo implementado en este proyecto tiene sus limitaciones. Por el mismo hecho de no utilizar los equipos seleccionados para el sistema y al ser desarrollarlo a una menor escala, no se está reproduciendo el sistema en las condiciones reales. Por tal razón, aunque en el prototipo se obtenga un buen funcionamiento del sistema, no se podría garantizar que en caso de implementación del sistema de video-vigilancia en las condiciones reales funcione de la misma manera.

- El desarrollo teórico de un proyecto es sencillo si se compara con la implementación del mismo, es en este punto donde surgen los problemas que deberán ser superados mediante la investigación y la perseverancia. Implementar el prototipo del sistema de video-vigilancia fue de gran ayuda para poder relacionar la parte teórica con la práctica.

- Uno de los objetivos planteados al desarrollar este Proyecto de Titulación, era elaborar un presupuesto referencial de hardware y software analizando dos alternativas, esto se hizo parcialmente, debido a que se presentaron equipos y fueron seleccionaron los que aparte de cumplir con los requerimientos del sistema, presentaron mejores características y se elaboró el presupuesto en base a estos equipos. De los equipos que no fueron seleccionados, no se presentó su presupuesto porque no se los va a utilizar en el presente Proyecto.

- En caso de existir problemas de retardo y/o interrupciones en la transmisión del video, esto puede deberse a la presencia de otras redes en

el sector. Para eliminar este problema, se puede utilizar programas como el “InSSIDER” para encontrar todas las redes que están provocando interferencias y los canales de frecuencia que están saturados. Cuando se desarrolló este Proyecto, la banda libre de 5 GHz estaba muy poco ocupada.

5.2 RECOMENDACIONES

- El personal encargado de la supervisión del sistema de Video-vigilancia debe ser entrenado y capacitado para efectuar esta tarea, con esto se logrará disminuir el cometimiento de errores al efectuar una mala manipulación del sistema. También es recomendable llevar una documentación formal, en la cual se indique cambios o ampliaciones que el sistema pudiera sufrir.

- Para la implementación del prototipo de pruebas, se recomienda ir configurando los equipos uno a uno, verificando que vaya existiendo conexión entre ellos, de esta manera se disminuirá considerablemente los posibles errores que pudieran presentarse.

- En el caso de accesos de usuarios al sistema, es recomendable asignar nombres de usuarios y contraseñas con distintos niveles de acceso, de esta manera, se podrá evitar el uso incorrecto del sistema y en el caso de existir algún tipo de sabotaje, saber que usuario accedió, la hora de acceso y que fue lo que hizo.

- Instalar los complementos o plugins necesarios en el navegador desde el cual se quiera acceder al sistema de video-vigilancia, ya que puede darse el caso de que se tenga conexión con el sistema pero que no despliegue las imágenes de las cámaras, tal como sucedió en la implementación del prototipo, en el que fue necesario instalar el complemento plugins.xpi en el programa Firefox para poder visualizar las imágenes del sistema.

- Aunque el sistema de video-vigilancia permite asignar direcciones IP dinámicas a los equipos, es recomendable asignar direcciones IP fijas a éstos, de esta manera se podrá identificar de una manera mucho más rápida cuando un equipo presenta algún tipo de fallo, o incluso si se quiere hacer algún cambio en la configuración del equipo, poder acceder mucho más rápido a éste y no perder tiempo buscando la dirección IP que tiene asignado.

- Un tema primordial y más aún en redes inalámbricas es la seguridad. Se debe considerar utilizar la mayor cantidad de seguridades posibles para que la red no sea víctima de ataques.

- Es recomendable que los equipos de seguridad cumplan con estándares internacionales como ONVIF, de esta manera, en caso que querer agrandar el sistema, garantizar la compatibilidad de equipos de diferentes marcas.

- El factor costo/beneficio es muy importante en la implementación de todo proyecto, sin embargo, se debe tener en cuenta que el tratar de ahorrar dinero en equipos de marcas no conocidas, puede llegar a provocar que un Proyecto fracase debido a la mala calidad de los mismos, por lo tanto, es recomendable asesorarse bien acerca de que empresas tienen mayor trayectoria y en qué tipo de producto.

- Es importante destacar que en caso de que se requiera aumentar la capacidad de transmisión de la red inalámbrica, se podría pensar en actualizar el firmware de los equipos Mikrotik para que trabajen con nuevas tecnologías como la 802.11ac.

- En caso de existir una saturación de la capacidad del canal inalámbrico, se puede pensar en configurar una nueva red inalámbrica para que trabaje de manera simultánea con la red principal, en la misma frecuencia pero en

diferente canal, para esto, es necesario aumentar una nueva tarjeta R52Hn al Routerboard RB433GL y una nueva antena.

REFERENCIAS BIBLIOGRÁFICAS

CAPÍTULO 1. Fundamentos teóricos

Documentos, Libros y Publicaciones

[1] Ph. D. Iván Bernal, Comunicaciones Inalámbricas, 2009

[2] Camargo Olivares José Luis, Modelo de Cobertura para Redes Inalámbricas de Interiores, 2009

[23] Negocios de Seguridad, Video en Red, Número 59, RNDS, 2011

[24] Martí Martí Silvia, Diseño de un Sistema de Televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia, 2013

[30] Espiga Alejandro, Selección de Portal en redes malladas utilizando aprendizaje estadístico, 2012

[31] Guía Técnica para vídeo en red, Axis Communications, www.axis.com

[32] Velasco Santamaría Daniel Alejandro, Estudio y Diseño de una red de video vigilancia local y remota, utilizando cámaras de vigilancia para el monitoreo de seguridad, alerta de intrusión y almacenamiento de video, para la planta de producción de la empresa Romery, 2013

[35] Fornés Rumbao Francisco, Simulador de redes WMN para el despliegue de unidades SAR en áreas de crisis, 2014

[36] Moreano Viteri Roberto; Gody Vaca Alejandro, Red inalámbrica tipo malla (WMN) bajo el estándar 802.11 para la Universidad internacional Sek, 2011

Direcciones Electrónicas

[3] http://es.wikipedia.org/wiki/Body_Area_Network

[4] http://es.wikipedia.org/wiki/Bluetooth

[5] http://www.bluetooth.com/Pages/Bluetooth-Brand.aspx

[6] http://es.wikipedia.org/wiki/ZigBee

[7]http://www.blogdelg.es/lg-optimus-g-pro-infrarrojos-quick-remote-colaboracion-erlantz-plaza-eandroid/

[8] http://telefonosinalambricos.info/tecnologia-inalambrica-dect/

[9] http://faqhard.ru/hard/spr/2/11.php

[10] http://en.wikipedia.org/wiki/Ultra-wideband

[11] http://es.wikipedia.org/wiki/HomeRF
[12] https://pabloserrano.wordpress.com/2006/07/03/wi-fi-no-significa-wireless-fidelity/
[13] http://fullofknowledgefullthings.blogspot.com/2014/08/how-wifi-works.html
[14] http://www.ecured.cu/index.php/HiperLAN
[15] http://es.wikipedia.org/wiki/WiMAX
[16] http://www.tech-faq.com/wibro.html
[17] http://www.aiturrih.com/portfolio-view/wwan/
[18] http://identidadgeek.com/redes-sociales-en-los-moviles/2013/07/aplicaciones/
[19]http://aec3c1eg320121.wikispaces.com/%C2%BFQUE+SON+REDES+SATELITALES%3F
[20] http://es.wikipedia.org/wiki/Espectro_electromagn%C3%A9tico
[21]http://efagundes.com/openclass_networking/index.php/transmissao-sem-fio/ism-industrial-scientific-medical/
[22] http://es.wikipedia.org/wiki/V%C3%ADdeovigilancia_IP
[25]http://www.grupolinuxcolombia.com.co/uploads/8/4/3/8/8438227/principios_basicos_de_cctv__1.pdf
[26] http://www.axis.com/es/products/video/about_networkvideo/resolution.htm
[27] http://www.axis.com/es/products/video/camera/about_cameras/types.htm
[28] http://www.gremioseguridad.com/redes.html
[29] http://www.axis.com/es/products/video/camera/about_cameras/lens.htm
[33] http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica_mallada
[34]https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0CEAQFjAH&url=http%3A%2F%2Fwww.aslan.es%2Ffiles%2F381-187-Archivo%2FIIC.pdf%3Fdownload%3D1&ei=4bOYU6WnIs62yATh04D4CQ&usg=AFQjCNEpHYFNkoLQZ7vOB1jnf-BXQapAVQ

CAPÍTULO 2. Análisis de requerimientos

Documentos, Libros y Publicaciones

[6]Loor Espinoza Tito Alejandro, López Castro Johnny Santiago, Rediseño de las redes de condominios El Batán y conjunto residencial Brasilia II para brindar servicios de intranet por el proveedor “STARNET SERVICIOS INFORMÁTICOS”, 2009

Direcciones Electrónicas

[1]http://www.inec.gob.ec/cpv/index.php?option=com_content&view=article&id=167&Itemid=3&lang=es

[2] http://maps.google.com.ec/maps?hl=es&tab=wl

[3] http://es.wikipedia.org/wiki/Encuesta

[4] http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.html

[5] http://es.wikipedia.org/wiki/Entrevista_period%C3%ADstica

Otros

[7] Policía Comunitaria del Distrito Cayambe y Pedro Moncayo

[8] Gobierno Autónomo Descentralizado Municipal del Cantón Cayambe

CAPÍTULO 3. Diseño del sistema de video-vigilancia y determinación de costos referenciales

Documentos, Libros y Publicaciones

[1] Velasco Santamaría Daniel Alejandro; Estudio y Diseño de una red de video vigilancia local y remota, utilizando cámaras de vigilancia para el monitoreo de seguridad, alerta de intrusión y almacenamiento de video, para la planta de producción de la empresa Romery, 2013.

[2] Rivera Pastrano Luis Oswaldo, Zapata Vásquez Cristian Fernando; Diseño de una red de acceso para brindar servicios triple play con tecnología GPON y WIMAX en el cantón Pedro Vicente Maldonado para la empresa Saturno TV, 2012.

[5] Mier González Dennise Giocelyn, Velásquez Duran Santiago David; Análisis y Diseño de un modelo de implementación de una Red Mesh con calidad de servicio, ruteo y seguridades, mediante el uso de equipos Mikrotik, tomando como referencia la red inalámbrica de la Universidad Politécnica Salesiana, sede sur, Campus Sur, 2013.

[27] Redes inalámbricas en los países en desarrollo, cuarta edición, 2013.

[28] Ing. Paúl Camino, Diseño de radio enlaces, 2015.

[29] Loayza Loayza Carlita Vanessa, Espinoza Tapia Belén Elizabeth; Estudio del rendimiento del estándar 802.11n en la comparación con dispositivos con el estándar 802.11b/g en la transmisión de datos, 2010.

Direcciones Electrónicas

[3] http://www.sistelec.es/pdf/WI4_MotoMesh_Duo_Brochure.pdf

[4] http://www.telequismo.com/2012/02/siguiendo-con-la-seccion-de-analisis-de.html

[6]http://www.amazon.com/HIKVISION-USA-Hikvision-Ds-9616Ni-St-24Tb-16-Channel/dp/B00I872QUY/ref=sr_1_58?ie=UTF8&qid=1428593509&sr=8-58&keywords=nvr+24+tb

[7]http://www.amazon.com/Toshiba-Surveillix-NVSPRO-NVSPRO32-2U-24T-rack-mountable/dp/B00VQQ1U5G/ref=sr_1_1?ie=UTF8&qid=1428595361&sr=8-1&keywords=NVSPRO32-2U-24T

[8]http://www.ebay.com/itm/NEW-Hikvision-2MP-1080P-Full-HD-Real-time-WDR-Outdoor-Mini-IP-PTZ-Speed-Dome-PoE/361193343459?_trksid=p2047675.c100009.m1982&_trkparms=aid%3D777000%26algo%3DABA.MBE%26ao%3D1%26asc%3D29266%26meid%3D4fda612b23944ac591f40c4a289dc5c2%26pid%3D100009%26rk%3D1%26rkt%3D1%26mehot%3Dlo%26sd%3D261526073755

[9]http://www.ebay.com/itm/Dahua-2-Megapixel-1080P-HD-SDI-Pan-Tilt-Zoom-PTZ-Camera-20x-16x-24v-IP67-D-WDR-/131028046571?pt=LH_DefaultDomain_0&hash=item1e81e152eb

[10]http://www.amazon.com/Mikrotik-CA-OTU-daughterboards-insulator/dp/B00DZSVO9U/ref=sr_1_1?ie=UTF8&qid=1428891815&sr=8-1&keywords=CAOtu

[11]http://www.amazon.com/TerraWave-5-7-5-85Ghz-12Dbi-Omni-Antenna/dp/B007956AW6/ref=sr_1_71?s=electronics&ie=UTF8&qid=1428638223&sr=1-71&keywords=omni+antenna+12+dbi

[12] http://mum.mikrotik.com/presentations/EC13/bajana.pdf

[13] https://upcommons.upc.edu/pfc/bitstream/2099.1/6989/17/Anexo%2016.pdf

[14]http://www3.fi.mdp.edu.ar/electronica/catedras/mediosdetransmision/files/ManualRadioMobile.pdf

[15] http://www.ipellejero.es/radiomobile/RM_07.php

[16] http://bibing.us.es/proyectos/abreproy/12046/fichero/3_Capitulo3.pdf

[17] http://bibing.us.es/proyectos/abreproy/11901/fichero/capitulo7.pdf

[19] http://www.telconet.net/servicios/internetdedicado

[20]http://agenciasanluis.com/notas/2012/12/03/licitan-la-compra-de-60-camaras-de-video-vigilancia/
[21]http://www.rcwireless.com/catalog/product_info.php?products_id=64&osCsid=9f71b200e73ea67d71968ede8c75344f
[22]http://www.ebay.com/itm/CORNELL-BATTERY-BACKUP-POWER-SUPPLY-B5243A-/261770138719?pt=LH_DefaultDomain_0&hash=item3cf2b7545f
[23]http://www.amazon.com/Allied-Moulded-AMU1860LF-Ultraline-Fiberglass/dp/B00CR90F8E/ref=pd_sim_sbs_hi_7?ie=UTF8&refRID=0PKPG0CQK6E1MBNJ9JYJ
[24]http://www.amazon.com/Mikrotik-R52Hn-802-11a-MiniPCI-connectors/dp/B00DZUO81Y/ref=pd_bxgy_p_text_y
[25]http://www.amazon.com/Mikrotik-RB433GL-RouterBOARD-miniPCI-RouterOS/dp/B00DYZX5O6/ref=sr_1_1?s=electronics&ie=UTF8&qid=1428891651&sr=1-1&keywords=433gl
[26]http://www.amazon.com/Mikrotik-AC-MMCX-ACMMCX-MMCX-Nfemale-pigtail/dp/B00D84L0IG/ref=pd_sim_sbs_p_1?ie=UTF8&refRID=0PHM4FMXR30FXCTQWDWG
[30]http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/06_es_calculo-de-radioenlace_guia_v02.pdf
[31] http://www.gremioseguridad.com/redes.html

Otros

[18] Resolución –TEL-560-18 CONATEL, 2010

CAPÍTULO 4. Implementación del prototipo del sistema, pruebas y resultados

Direcciones Electrónicas

[1] http://www.mikrotik.com/download
[2] http://www.cnt.gob.ec/internet/plan/fast-boy/
[3] http://es.wikipedia.org/wiki/DNS_din%C3%A1mico
[4] http://es.wikipedia.org/wiki/Universal_Plug_and_Play
[5] http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

[6] http://es.wikipedia.org/wiki/Network_Address_Translation

[7] http://es.wikipedia.org/wiki/Puerta_de_enlace

[8] http://es.wikipedia.org/wiki/Wireless_Distribution_System

ANEXOS

ANEXO A._ Modelo de encuesta

Encuesta

Fecha: _____

Género: Masculino ☐ Femenino ☐

Edad: 14-17 ☐ 18-25 ☐ 26-50 ☐ Mayor de 51 ☐

Objetivo General: Determinar por medio de un sondeo el grado de aceptación y la necesidad de implementación de un sistema de video-vigilancia en la ciudad de Cayambe con el objetivo de prevenir actos delictivos.

Instrucciones: Marque con una X según su criterio

1.- ¿Usted cree que el cantón Cayambe es seguro?

Si ☐
No ☐

2.- ¿Ha sufrido usted algún tipo de acto de delincuencia? Si su pregunta es afirmativa, pase a responder las preguntas 3 y 4, caso contrario pase directamente a la Pregunta 5

Si ☐
No ☐

3.- Mencione ¿Qué tipo de acto delictivo?

Robo ☐ Hurto ☐
Asalto ☐ Estafa ☐

Otros: _____

4.- Mencione ¿En qué lugar o barrio sucedió?

#	BARRIO	#	BARRIO	#	BARRIO	#	BARRIO
1	Santa Marianita de Granobles	12	Une	23	La Obrera	34	Bellavista de Puntiachil
2	23 De Julio	13	Miraflores	24	Central	35	Sur
3	Amazonas	14	Las Orquídeas	25	Florida I	36	La Cruz
4	Santa Laura De Changalá	15	Nuevos Horizontes	26	Florida II	37	Puntiachil
5	Changalá	16	San Ruperto	27	1 De Mayo	38	Chimborazo
6	Sigsal Bajo	17	Hacienda	28	Álvarez y	39	San Nicolás

			Primavera		Chiriboga		
7	Víctor Cartagena	18	Girasoles	29	La Playa	40	Don Bosco
8	Sandra Pérez	19	Sara Jarrín	30	San Pedro	41	4 Esquinas
9	El Sigsal	20	Patarata	31	El Obraje		
10	Lucila Cartagena	21	Verde Pamba	32	Bellavista De Cruz Loma		
11	La Estación	22	Bolívar	33	San Carlos		

Otros: _____

5.- ¿Conoce usted qué es un sistema de video-vigilancia?

Si ☐
No ☐

6.- ¿Estaría de acuerdo con la instalación de un sistema de video-vigilancia?

Si ☐
No ☐

7.- A su criterio ¿En cuál de estos sitios debería instalarse este sistema de video-vigilancia?

Lugares públicos ☐ Principales vías públicas ☐
Centros educativos ☐ Todos ☐

8.- ¿Cree Usted, que con la ayuda de este sistema disminuya la delincuencia en la ciudad de Cayambe?

Si ☐
No ☐

ANEXO B._ Hoja de datos, equipos sistema de video-vigilancia, enrutadores

Motorola Motomesh Duo

SPECIFICATION SHEET

wi4 Mesh

MOTOMESH™ Duo

Two Radio Meshed WiFi Network with 4.9GHz for Public Safety

MOTOMESH Product Advantage

The MOTOMESH product series makes wireless cities a reality with robust and future-proof wireless broadband technologies. Whether providing wireless access to a campus, business, neighborhood or city, MOTOMESH delivers real-time data to your first responders, residents, employees, and customers, enabling vital wireless broadband applications.

Dual Mesh Operation

Public safety agencies require data traffic that is separate and secure from public access. MOTOMESH Duo operates as a dual mesh, with the licensed 4.9GHz system providing client access to first responders, as well as meshed backhaul to create a private and secure network. Furthermore, Duo's 10MHz and 20MHz channel support for 4.9GHz allows channel flexibility within the Public Safety Network. The 2.4GHz system provides meshed radio links, and client access to business and residential users, keeping the two systems separated.

Proven Mesh Routing

MOTOMESH Duo leverages MeshConnex routing technology, using real-time congestion management and link control to automatically select the best data route on a per-request basis. This dramatically reduces hop latency, to better deliver real-time voice and multimedia services. Today, MeshConnex powers large-scale Motorola mesh networks of more than 1,000 nodes.

Carrier-Class Security

MOTOMESH Duo supports complete, end-to-end security. It provides WEP, WPA and WPA2 encryption on client access. Motorola's own SecureMesh ensures the highest data security within the meshed WiFi network. Finally, users can create access lists that can block particular clients from accessing the network.

Compact Form Factor

The small profile, light weight form factor, and slim-line aesthetics increase mounting location flexibility and community acceptance.

Advanced Network Management

MOTOMESH Duo utilizes Motorola's One Point Wireless Manager to manage and visualize a multitude of capabilities for small to large networks and all of these capabilities are controllable from a single suite of software. By completing one profile, a large number of devices can be configured easily, reducing the time required to provision individual devices and complete on-going adjustments. Once the network is up and running, the Wireless Manager is a flexible and powerful tool that monitors the health of the network's components for quick detection and resolution of problems that can impact network performance and user satisfaction.

Flexible & Adaptable Gateways

Every MOTOMESH Duo unit is capable of being an Intelligent Access Point (IAP) or Mesh Wireless Router (MWR), reducing the cost of storing excess inventory and simplifying deployment. Additionally, gateway nodes immediately adapt to backhaul loss by becoming wireless routers, routing traffic to an alternate gateway in the network. This automatic, self-healing ability minimizes service interruptions and ensures continuous connectivity.

Quality of Service (QoS)

Delay-sensitive applications like video and voice services require different data priorities. MOTOMESH Duo supports IEEE 802.11e based traffic prioritization. It constantly monitors node congestion, and automatically tunes its QoS parameters to optimize route selections to support latency sensitive applications.

Motorola, Your End-to-End Solution Provider

Motorola's wireless broadband portfolio offers an array of access and backhaul technologies for complete end-to-end wireless initiatives. Motorola's Fixed Point-to-Multipoint and Point-to-Point solutions provide reliable, high-capacity Internet backhaul links to Motorola's mesh networks. MeshPlanner and MeshScanner enable detailed network planning and optimization capabilities. Additionally, Motorola's ecosystem of applications offers a wide range of validated solutions to garner multiple benefits from your wireless network.

Software Highlights

The MOTOMESH Duo solution offers a multitude of software features for enhancing your network experience. With Peer-to-Peer Communication Blocking ISPs (Internet Service Providers) now have an effective way to manage billing applications and client tracking scenarios. With the combination of Duo's VLAN support and standard 802.11e QoS, ISPs can create differentiated services that will allow them to offer tiered packages. Finally, historical, comprehensive statistics are now available for future reference and review.

MOTOwi4

SPECIFICATION SHEET

MOTOMESH Duo
Two Radio Meshed WiFi Network
with 4.9GHz for Public Safety

Benefits
- Best-in-class radio performance
- Reliable coverage
- Best-in-class throughput
- Robust security

MOTOwi4
MOTOMESH Duo is part of the MOTOwi4 family of broadband access technologies, a comprehensive platform of wireless broadband solutions, applications and services. Designed to complement and complete wireless networks, MOTOwi4 solutions address a broad range of applications across municipal, enterprise, and operator segments. The comprehensive MOTOwi4 portfolio creates a true end-to-end ecosystem of complementary products, services and solutions that provide high speed connectivity enabling a broad range of applications in fixed, nomadic, portable or mobile environments. Working together, wi4 Mesh solutions combined with other MOTOwi4 access technologies deliver ubiquitous, metro-wide (community-wide, campus-wide) wireless broadband coverage.

Why Motorola
Motorola is uniquely positioned to address the wireless broadband market through the MOTOwi4 vision. Motorola has aligned its business units and roadmaps to provide a comprehensive, end-to-end solution covering all aspects of the broadband wireless access deployment. With our deep and extensive patent portfolio, over a decade of R&D investment, and our experience as a global supplier of broadband wireless access solutions, Motorola is primed to deliver its best in class wireless networks. Motorola is committed to leading the industry with end-to-end wi4 Mesh solutions addressing the full scope of the operator's deployment needs including access, core, devices, network management and services.

MOTOMESH DUO • 4300-49 RADIO CHARACTERISTICS	
IEEE 802.11b/g Radio (20MHz Channel)	2.400 to 2.483GHz
IEEE 802.11a Radio (10MHz Channel)	4.940 to 4.990GHz
RF Modulation	CCK (802.11b), OFDM (802.11a/g)
Transmit Power (Maximum)	35dBm EIRP (802.11b/g), 34 dBm EIRP (802.11a) • Settable in 1dB increments
Receive Sensitivity	802.11b: -92dBm @ 11 Mbps to -100dBm @ 1 Mbps 802.11g: -78dBm @ 54 Mbps to -95dBm @ 6 Mbps 802.11a: -77dBm @ 27 Mbps to -93dBm @ 3 Mbps
Antenna Type	N-Type • Two (2) omnidirectional: 9dBi for 2.4GHz and 11dbi for 4.9GHz
ROUTING	
Technology	MeshConnex routing with Layer 1 situational-awareness
Protocol	Patented, Layer 2, hybrid proactive/reactive routing
NETWORK	
Network Management Software	EMS on Linux OS via SNMPv1, SNMPv2c or secure SNMPv3 Web Interface via HTTPS (SSL) 802.11 and MOTOMESH MIBs
Network Interface	Weatherized 10/100 Base-T Ethernet (RJ-45) port with surge suppression
Network Segmentation	16 VAPs (Multiple SSIDs with VLAN mapping)
Quality of Service (QoS)	802.11e, weighted fair queuing and IP precedence bits (ToS) supported via DSCP
SECURITY	
Client Encryption Support	WEP, WPA (TKIP) and WPA2 (AES, 802.11i)
Intra-Mesh Encryption	SecureMesh with AES
Authentication	802.1X (Infrastructure/Client) and MAC address hardware authentication
TCP/IP Filtering	Broadcast storm and port filtering
POWER	
Power Input	90-264 VAC (with +/- 20% variation at 47-63Hz) or Optional 10.8-14VDC (2.5A Max)
Power Connector	Weatherized NEMA 5-15 power cord • 12 ft (3.66m)
Power Consumption	15W to 30W (with PoE device)
Power over Ethernet (PoE)	Support for Canopy PoE, or 802.3af Standard PoE device
PHYSICAL	
Dimensions	9" x 6" x 3.5" (23.1cm x 15.2cm x 8.9cm) • 189in³ (3097cm³)
Weight	4.5 lbs (2.04kg)
Packaging	Outdoor, all-weather enclosure (NEMA 4 / IP54)
Mounting	3" (7.62cm) diameter post mounting
ENVIRONMENTAL & REGULATORY	
Temperature Range	-30 to 60 °C (-22 to 140 °F)
Humidity	0 to 95%, non-condensing at 50 °C (122 °F)
Regulatory Certifications	FCC Part 15 & 90, CE, MET Mark / CSA / UL, RoHS / CMM / WEEE, Industry Canada
AVAILABLE OPTIONS & ACCESSORIES	
Mounting	Lamp post mount bracket assembly
Antennas	4 or 6dBi omnidirectional for 2.4GHz
Power Plug Adapters	AC photo cell adapter and US, EU, and AU Power Plug Adapters
Power Over Ethernet (PoE) Adapters	Canopy Connect or IEEE 802.3af PoE

ONE YEAR PARTS & LABOR WARRANTY

MOTOROLA

Motorola, Inc. www.motorola.com/mesh

Mikrotik Routerboard RB433GL

Product specifications

Details	
Product code	RB433GL
CPU nominal frequency	680 MHz
CPU core count	1
Size of RAM	128 MB
Architecture	AR7161
10/100 Ethernet ports	0
10/100/1000 Ethernet ports	3
MiniPCI slots	3
MiniPCI-e slots	0
Number of USB ports	1
Power Jack	1
802.3af support	No
Supported input voltage	8 V - 28 V
PoE in	Yes
PoE out	No
Voltage Monitor	Yes
CPU temperature monitor	No
PCB temperature monitor	No
Dimensions	105 mm x 154 mm,
Operating System	RouterOS
Operating temperature range	-40°C .. +70°C tested
License level	5
Antenna gain DBI	No
Current Monitor	No
CPU	AR7161-BC1A
SFP ports	0
SFP+ ports	0
USB slot type	USB type A
Number of chains	0
Serial port	None
Suggested price	$139.00

Performance test results

RB433GL		AR7161 1G all port test					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none	58.0	704.4	171.9	704.1	187.3	95.9

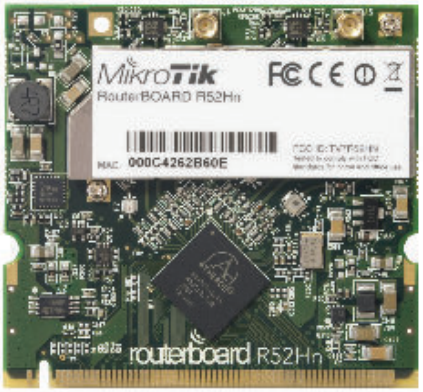
Bridging	25 bridge filter rules	58.5	710.4	84.5	346.1	86.4	44.2
Routing	none	59.7	725.0	136.1	557.5	147.0	75.3
Routing	25 simple queues	55.2	670.3	117.7	482.1	137.0	70.1
Routing	25 ip filter rules	54.7	664.3	59.4	243.3	59.2	30.3

1. All tests are done with Xena Networks specialized test equipment (XenaBay),and done according to RFC2544 (Xena2544)
2. Max throughput is determined with 30+ second attempts with 0,1% packet loss tolerance in 64, 512, 1518 byte packet sizes
3. Values in Italic indicate that max throughput was reached without maxing out CPU, but because board interface configuration was maxed out
4. Test results show device maximum performance, and are reached using mentioned hardware and software configuration, different configurations most likely will result in lower results

Mikrotik Routerboard R52HN

RouterBOARD R52Hn

802.11a/b/g/n dual band miniPCI card



- Dual band IEEE 802.11a/b/g/n standard
- Output Power of up to 25dBm @ a/g/n Band
- Support for up to 2x2 MIMO with spatial multiplexing
- Four times the throughput of 802.11a/g
- Atheros AR9220, chipset
- High Performance (up to 300Mbps physical data rates and 200Mbps of actual user throughput) with Low Power Consumption
- 2 X MMCX Antenna Connector (J4 - Chain 0)
- Modulations:
  OFDM: BPSK, QPSK, 16 QAM, 64QAM
  DSSS: DBPSK, DQPSK, CCK
- Operating temperatures: -50°C to +60°C
- Idle power consumption 0.4W
- Max power consumption 7W
- MiniPCI IIIA+ design (3mm longer than MiniPCI IIIA)
- 1.5mm heatsink, 3mm RF shield thickness
- ±10KV ESD protection on RF ports

RouterBOARD R52Hn miniPCI network adapter provides leading 802.11a/b/g/n performance in both 2GHz and 5GHz bands, supporting up to 300Mbps physical data rates and up to 200Mbps of actual user throughput on both the uplink and downlink. 802.11n in your Wireless device provides higher efficiency for everyday activities such as local network file transfers, Internet browsing, and media streaming. R52Hn has a high power transmitter, bringing you even more range.

802.11b	RX Sensitivity	TX Power
1Mbit	-93	24
11Mbit	-93	24
802.11g		
6Mbit	-94	25
54Mbit	-81	22
802.11n 2.4GHz		
MCS0 20MHz	-94	25
MCS0 40MHz	-92	24
MCS7 20MHz	-78	21
MCS7 40MHz	-75	20

802.11a	RX Sensitivity	TX Power
6Mbit	-97	25
54Mbit	-80	21
802.11n 5GHz		
MCS0 20MHz	-97	24
MCS0 40MHz	-92	22
MCS7 20MHz	-77	18
MCS7 40MHz	-74	17

Data Rates

802.11b	
	11Mbps; 5.5Mbps; 2Mbps; 1Mbps
802.11a/g	
	54Mbps; 48Mbps; 36Mbps; 24Mbps; 18Mbps; 12Mbps; 9Mbps; 6Mbps
802.11n	
20MHz	1Nss: 65Mbps @ 800GI, 72.2Mbps @ 400GI (Max.) 2Nss: 130Mbps @ 800GI, 144.4Mbps @ 400GI (Max.)
40MHz	1Nss: 135Mbps @ 800GI, 150Mbps @ 400GI (Max.) 2Nss: 270Mbps @ 800GI, 300Mbps @ 400GI (Max.)

Antena TerraWave modelo T58120O10006

Product Description

5.7 to 5.85 GHz 12 dBi fiberglass omnidirectional antenna with N-style jack connector TerraWave's 12 dBi fiberglass omnidirectional antenna is designed for 5.7-5.85 GHz wireless local area networks. It features a UV stable, vented radome that provides ultimate sustainability against extreme weather conditions such as high temperature, strong winds and rain. It can be mast or wall mounted. Narrative: TerraWave's 12 dBi fiberglass omnidirectional antenna is designed for 5.7-5.85 GHz wireless local area networks. It features a UV stable, vented radome that provides ultimate sustainability against extreme weather conditions such as high temperature, strong winds and rain. It can be mast or wall mounted. Specific Frequency (MHz): 5700-5850 Maximum Power (Watts): 100 Polarization: Vertical Horizontal Beamwidth (Deg): 360 Vertical Beamwidth (Deg): 7 VSWR: 1.5:1 Size (L x W x H): 21.7 Lightning Protection: Sold Separately Weight (lb): 1.1 Type of Jumper Included: None Type of Hardware Included: Yes Rated Wind Velocity (RWV, MPH): 135

ANEXO C._ Hojas de datos, equipos sistema de video-vigilancia, cámaras IP

Cámara Hikvision modelo DS-2DE4220-AE

HIKVISION

Compact-sized

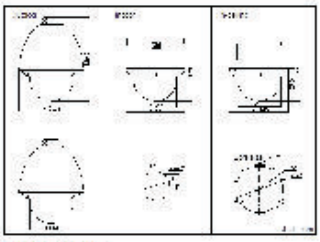
DS-2DE4220 series

2MP Network PTZ Dome Camera

Key features

- 1/2.8" Progressive Scan CMOS
- 1080P Full HD real-time resolution
- 20X Optical zoom, 16X digital zoom
- True Day/Night, D WDR , 3D DNR
- Privacy Mask, Alarm input/output
- 3D intelligent positioning
- PoE+/ PoE / 24VAC power supply
- Compact-sized design

Dimensions



Accessories

Available models

DS-2DE4220-AE, 24VAC/PoE+, outdoor
DS-2DE4220-AE3, 24VAC/PoE, indoor

	DS-2DE4220-AE / DS-2DE4220-AE3
Camera	
Image sensor	1/2.8" Progressive Scan CMOS
Effective pixel	1920(H) ×1080(V)
Min. illumination	Color: 0.05Lux @ (F1.6, AGC On), B/W: 0.01Lux @ (F1.6, AGC On)
White balance	Auto/Manual/ATW/Indoor/Outdoor/Daylight lamp/Sodium lamp
AGC	Auto / Manual
S / N ratio	≥ 52dB
Digital noise reduction	3D DNR
Backlight compensation	BLC
Wide dynamic range	Digital WDR
Defog	Support
Shutter speed	1/1 ~ 1/10,000s
Day & Night	IR Cut Filter
Digital zoom	16X
Focus mode	Auto / Semiautomatic / Manual
Privacy Mask	2 privacy masks programmable
Lens	
Focal length	4.7-94mm, 20x
Zoom speed	Approx.3s (Optical Wide-Tele)
Angle of view	58.3 ~ 3.2 degree (Wide-Tele)
Min. working distance	10 ~1000mm (Wide-Tele)
Aperture range	F1.6 ~ F8.5
Pan and Tilt	
Pan / Tilt range	Pan: 360° endless; Tilt: -2° ~ 90°(Auto Flip)
Pan / Tilt speed	Pan manual speed: 0.1° ~ 160°/s, Pan preset speed: 160°/s Tilt manual speed: 0.1° ~ 120°/s, Tilt preset speed: 120°/s
Proportional zoom	Rotation speed can be adjusted automatically according to zoom multiples
Number of preset	256
Patrol	8 patrols, up to 32 presets per patrol
Park action	Pattern/Pan scan/Tilt scan/Frame scan/Panorama scan/Random scan
Power-off memory	Support
PTZ position display	On / off
Preset freezing	Support
Local Video and Audio	
Alarm input / output	1 input 0-5v DC) / 1 relay output, alarm response actions configurable
Audio input / output	1 mic/Line in, 2-2.4V[p-p]; output impedance: 1KΩ, ±10% / 1 output, Line level, impedance: 600Ω
Network	
Ethernet	10Base-T / 100Base-TX, RJ45 connector
Max. image resolution	1920×1080
Frame rate	50Hz: 25 fps (1920×1080); 25 fps (1280×720); 60Hz: 30 fps (1920×1080); 30 fps (1280×720)
Image compression	H.264/MJPEG
SVC	Support
ROI encoding	Support 2 areas with adjustable levels
Audio compression	G.711u /G.711a /G.726 /MP3L2
Protocols	IPv4/IPv6, HTTP, HTTPS, 802.1X, QoS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP, PPPoE
Simultaneous live view	Up to 6
Streams	Dual streams
SD memory card	Built-in micro SD card slot, up to 64GB, support edge recording
User/Host Level	Up to 32 users, 3 Levels: Administrator, Operator, User
Security measures	User authentication (ID and PW), Host authentication (MAC address), IP address filtering
Integration	
Application programming	Open-ended API, support Onvif, PSIA and CGI
Web Browser	IE 7+, Chrome 18+, Firefox 5.0+, Safari 5.02+
General	
Power	-AE: 24VAC/PoE+(802.3at), Max:18W; -AE3: 24VAC/PoE(802.3af), Max:12W
Working temperature	-AE: -30°C ~ 65°C (-22°F ~ 149°F) ; -AE3: -10°C ~ 50°C (14°F ~ 122°F)
Humidity	90% or less
Protection level	IP66 (outdoor),TVS 4,000V lightning protection, surge protection and voltage transient protection
Dimensions	Φ179.4×289.5mm (Φ7.06"×9.43")(outdoor) Φ165×179.5mm(Φ6.50"×7.07") (ceiling) Φ165×168mm(Φ6.50"×6.61") (in-ceiling)
Weight	Approx. 2Kg (4.41lbs)
Mount option (for outdoor model)	Long-arm wall mount: DS-1601ZJ; Short-arm mount: DS-1618ZJ Pendent mount: DS-1661ZJ(20cm) or DS-1662ZJ(50cm)

NOTE: Indoor models support ceiling and in-ceiling mount.

www.hikvision.com

Cámara Dahua modelo DH-SD6582

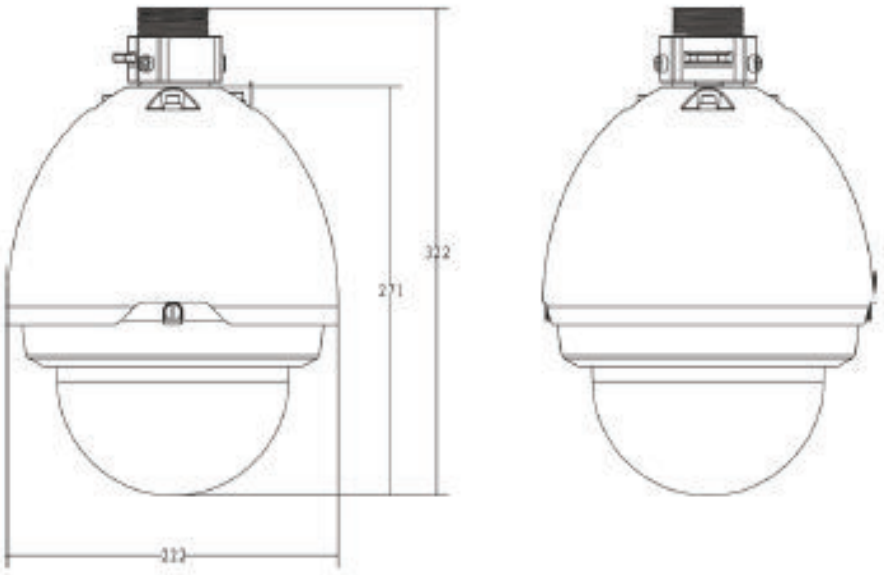
DH-SD6582/6582A-HS

Features

- 1/3" 2.0 Megapixel progressive scan Exmor CMOS
- 4.7mm ~ 94.0mm(20x)optical zoom
- Standard HD-SDI high definition digital interface (SMPT274/292)
- 25/30fps@1080p
- WDR(DWDR), Day/Night(ICR), DNR (2D&3D),Auto iris, Auto focus, AWB, AGC,BLC
- Max 400°/s pan speed, 360° endless pan rotation
- Up to 255 presets, 5 auto scan, 8 tour, 5 pattern
- Built-in 7/2 alarm in/out
- Support intelligent 3D positioning with DH-SD protocol
- IP67, easy installation

DH-SD6582/6582A-HS

Dimensions (mm)



DH-SD6582/6582A-HS

Technical Specifications

Model	HD-SD6582-HS	HD-SD6582A-HS
Camera		
Image Sensor	1/3" Exmor CMOS	
Effective Pixels	1944(H) x 1092(V), 2 Megapixels	
Scanning System	Progressive	
Electronic Shutter Speed	1/1 ~ 1/10,000s	1/1 ~ 1/30,000s
Min. Illumination	Color: 0.5 lux@F1.6 B/W: 0.095 lux@F1.6	Color: 0.05Lux@F1.6 B/W: 0.005Lux@F1.6
S/N Ratio	More than 50dB	
Video Output	BNC(1.0Vp-p/75Ω), PAL / NTSC	
Resolution	1080p(25/30fps), 1080i(50/60fps), 720p(25/30/50/60fps)	1080p(25/30fps), 720p(25/30fps)
HD-SDI Video Output	1ch HD-SDI high -definition video (SMPTE 292M standard)	
Camera Features		
Day/Night	Auto(ICR) / Color / B/W	
Backlight Compensation	BLC / HLC / WDR	BLC / HLC / DWDR (Digital WDR)
White Balance	Auto, ATW, Indoor, Outdoor, Manual	
Gain Control	Auto / Manual	
Noise Reduction	2D / 3D	
Privacy Masking	Up to 24 areas	
Digital Zoom	12x	16x
Lens		
Focal Length	4.7mm ~ 94.0mm(20x Optical zoom)	
Max Aperture	F1.6 ~ F3.5	
Focus Control	Auto / Manual	
Angle of View	H: 58.2° ~ 2.9°	H: 55.4° ~ 2.9°
Close Focus Distance	10mm ~ 800mm	10mm ~ 1000mm
PTZ		
Pan/Tilt Range	Pan: 0° ~ 360° endless; Tilt: -2° ~ 90°, auto flip 180°	
Manual Control Speed	Pan: 0.1° ~ 300°/s; Tilt: 0.1° ~250°/s	
Preset Speed	Pan: 400°/s; Tilt: 300°/s	
Preset	80(DH-SD), 255(Pelco-P/D)	
PTZ Mode	5 Pattern, 8 Tour, Auto Pan, Auto Scan	
Speed Setup	Human-oriented focal length/ speed adaptation	
Power up Action	Auto restore to previous PTZ and lens status after power failure	
Idle Motion	Activate Preset/Pan/Scan/Tour/Pattern if there is no command in the specified period	
Time Task	Auto activation of Preset/Pan/Scan/Tour/Pattern by preset-time	
Protocol	DH-SD, Pelco-P/D (Auto recognition)	
Auxiliary Interface		

DH-SD6582/6582A-HS

RS485	1 port
Alarm	7/2 channel In/Out
General	
Power Supply	AC 24V/3A (±10%)
Power Consumption	12W, 25W(Heater on)
Working Environment	-40°C ~ 60°C / Less than 90% RH
Protection Level	IP67, IK10 optional
Dimensions	Φ222(mm) x 322(mm)
Weight	5.0kg

Dahua Technology Co., Ltd.
1187 BinAn Road, Binjiang District, Hangzhou, China
Tel: +86-571-87688883
Fax: +86-571-87688815
Email:overseas@dahuatech.com
www.dahuatech.com

ANEXO D._ Hojas de datos, equipos sistema de video-vigilancia, NVRs

NVR Toshiba modelo NVSPRO32-2U-24T

TOSHIBA
Leading Innovation

NVSPRO

High Performance Network Video Servers

High-Density Storage for Enterprise Networks

Toshiba NVSPRO servers are designed for high-performance, large storage applications. With capacities up to 24TB and 48TB, Intel Core i7 processors, and dual Gigabit Ethernet ports, the NVSPRO is capable of handling demanding high-megapixel, enterprise-class deployments. Available in either 2U or 4U rackmount chassis, the NVSPRO offers superior performance and high storage density in space-saving form factors.

- 8 or 16 removable hard drives for storage up to 24TB or 48TB
- Intel Core i7 Processor
- Dual Gigabit Ethernet ports
- Includes 8 IP licenses expandable to 64
- 2U or 4U rackmount sizes
- Supports over 150 IP camera models
- Free Surveillix VMS software
- RAID5 option available

ONVIF intel CORE i7 inside Windows 7

NVSPRO

High Performance Network Video Servers

TOSHIBA
Leading Innovation

SERIES OVERVIEW		
Image compression	H.264, MPEG4, MJPEG	
Max Number of Channels	8 included, Expandable up to 64 (data rate dependent)	
Video Outputs	HDMI x 1, DVI x 1 (simultaneous output)	
Audio	1 audio jack input, Up to 64 IP camera audio input, 1 audio out	
STORAGE		
Storage Capacity	Up to 24TB (2U)	Up to 48TB (4U)
Critical Recording Archive	DVD/RW, eSATA x 1	
FRAME RATES		
Throughput	Up to 90 Mbs (non-RAID5 configuration) Up to 260 Mbps (RAID5 configuration)	
INPUTS/OUTPUTS		
PTZ Controls Protocols	Supported Network Cameras [1]	
LAN	2 x 100/1000 Gigabit Ethernet	
USB	8 x USB2.0, 2 x USB3.0	
OTHER		
Remote Connection	TCP/IP, UDP, Internet, LAN, WAN	
Password Control	User defined access level	
Power Interruption Recovery	Automatic restart and resume	
SYSTEM		
CPU	Intel Core i7	
RAM	4GB	
Operating System	Windows 7 Embedded	
DIMENSIONS		
Dimensions (h x w x d)	3.5" x 17.25" x 26.25" (2U)	6.9" x 16.95" x 26.25" (4U)
Weight	48 lbs w/o HDD	59 lbs w/o HDD
POWER		
Power Input	AC 100-240V (50Hz/60Hz)[2]	
Power Consumption	340 watts typical	
INCLUDED ACCESSORIES		
Accessories	Rackmount ears, keyboard and mouse	
WARRANTY		
Limited Warranty	3 years, 1 year advance replacement	

PART NUMBERS
NVSPRO8-2U-2T
NVSPRO8-2U-4T
NVSPRO8-2U-8T
NVSPRO8-2U-12T
NVSPRO8-2U-15T
NVSPRO8-2U-18T
NVSPRO8-2U-21T
NVSPRO8-2U-24T
NVSPRO8-4U-30T
NVSPRO8-4U-36T
NVSPRO8-4U-42T
NVSPRO8-4U-48T

RAID5 PART NUMBERS
RAID5-2TA
RAID5-4TA
RAID5-8TA
RAID5-12TA
RAID5-15TA
RAID5-18TA
RAID5-21TA
RAID5-24TA
RAID5-30TA
RAID5-36TA
RAID5-42TA
RAID5-48TA

1. For supported device list, visit our Integration page: www.toshibasecurity.com/integration
2. 2U chassis cannot have a redundant power supply.

2U Chassis

4U Chassis

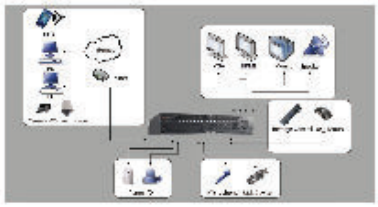
Toshiba America Information Systems, Inc.
Surveillance & IP Video Products, Imaging Systems Division
9740 Irvine Boulevard, Irvine, California 92618
1-877-855-1349 • www.toshibasecurity.com

NVSPRO 12/2012

NVR Hikvision modelo DS-9616NI-st-24TB

HIKVISION

DS-9616NI-ST High-end Embedded NVR



Key features

- Third-party network cameras supported
- Up to 5 Megapixels resolution recording
- HDMI and VGA output at up to 1920×1080P resolution
- Up to 8 SATA interfaces
- HDD quota and group management
- Dual gigabit network interfaces

Rear Panel of DS-9616NI-ST

1. Video out
2. Audio out
3. Line in
4. RS-232 serial interface
5. VGA interface
6. HDMI interface
7. eSATA interface
8. LAN1, LAN2 network interface
9. Termination switch
10. RS-485 serial interface, keyboard interface, alarm in, alarm out
11. GND
12. 100~240 VAC power input
13. Power switch

Specifications

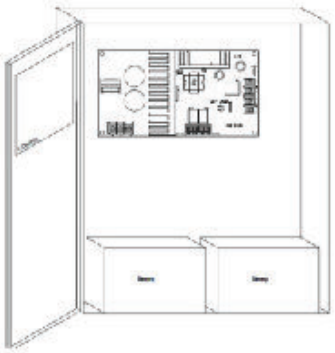
	DS-9616NI-ST
Video / Audio input	
IP video input	16-ch
Voice talk input	1-ch, BNC (2.0 Vp-p, 1 kΩ)
Video / Audio output	
Recording resolution	5MP / 3MP / 1080P / UXGA / 720P / VGA / 4CIF / DCIF / 2CIF / CIF / QCIF
CVBS output	1-ch, BNC (1.0 Vp-p, 75 Ω) Resolution: 704 × 576 (PAL); 704 × 480 (NTSC)
HDMI output	1-ch, resolution: 1920 × 1080P / 60Hz, 1920×1080P / 50Hz, 1600 × 1200 / 60Hz, 1280 × 1024 / 60Hz, 1280 × 720 / 60Hz, 1024 × 768 / 60Hz
VGA output	1-ch, resolution: 1920 × 1080P / 60Hz, 1600 × 1200 / 60Hz, 1280 × 1024 / 60Hz, 1280 × 720 / 60Hz, 1024 × 768 / 60Hz
Audio output	2-ch, BNC (Linear, 600 Ω)
Playback resolution	5MP / 3MP / 1080P / UXGA / 720P / VGA / 4CIF / DCIF / 2CIF / CIF / QCIF
Synchronous playback	16-ch
Hard disk	
SATA	Up to 8 SATA interfaces
eSATA	1 eSATA interface
Capacity	Up to 4TB capacity for each disk
External interface	
Network interface	2, 10M / 100M / 1000M self-adaptive Ethernet interface
Network bandwidth	Up to 40Mbps input, 40Mbps output, up to 128 network streams
Serial interfaces	RS-232, RS-485, RS-485 keyboard
USB interface	2 x USB2.0
Alarm in	16
Alarm out	4
General	
Power supply	100~240 VAC, 6.3A, 50~60Hz
Consumption	< 40W
Working temperature	-10°C ~ +55°C (14 °F ~ 131 °F)
Working humidity	10% ~ 90%
Chassis	19-inch rack-mounted 2U chassis
Dimensions (W x D x H)	445 × 470 × 90 mm (17.52" ×18.5"× 3.54")
Weight	< 8 kg (17.64 lb) (without hard disk or DVD-R/W)

ANEXO E._ Hojas de datos, equipos UPS

CORNELL modelo B5243A

Power Supply Battery Backup, 12 or 24 Volt

B-5243A



System Quote

The Cornell B-5243A is UL listed for fire alarm, burglar alarm, access control applications and hospital signaling - nurse call equipment.

Part Price B-5243A

- Rated Output: 4 amps continuous supply current at 12 VDC and 3 amps continuous supply current at 24 VDC.
- Power: 115VAC/60Hz, 1.45 amp. 4 amps continuous supply current at 12VDC(switch closed), 3 amps continuous supply current at 24 VDC (switch open).
- Circuit Protection: Short circuit and thermal overload protection.
- Termination: Screw terminals.
- Exterior: Grey, baked enamel finish.
- Dimensions:16" H x 12" W x 5" D
- Mounting: Slotted keyholes make it suitable for vertical wall or rack mounting.Unit comes complete with power supply, enclosure, cam locks, battery leads and (2) 12 Volt batteries.

Indicator LED Diagnostics:

Red-DC	Green-AC	Status
On	On	Normal Operating condition
On	Off	Loss of AC
Off	On	No DC output
Off	Off	Loss of AC Discharge. No DC output

Engineering Specifications:

The contractor shall furnish and install the CORNELL Power Supply/Battery Back-up providing 12 VDC 4 amps or 24 VDC 3 amps continuous supply current for use with 12 or 24 VDC products and other general purpose applications. Set the B-5243A to the desired DC output voltage by setting SW1 to the appropriate position. The power supply shall operate at 115 Volts AC 60 Hz.

Get Help with System Design/Installation