ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UN SISTEMA DE VIDEO VIGILANCIA UTILIZANDO Wi-Fi PARA EL CONJUNTO RESIDENCIAL “EL PRADO”

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

ALVAREZ FIGUEROA MAYRA LUCÍA
(mayri_093@hotmail.com)

VALDIVIESO SALAZAR CÉSAR LUIS
(taladrovs@hotmail.com)

DIRECTOR: ING. FABIO GONZÁLEZ
(fabio.gonzalez@epn.edu.ec)

Quito, Mayo 2011

DECLARACIÓN

Nosotros, Mayra Lucía Alvarez Figueroa y César Luis Valdivieso Salazar, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

Mayra Lucía Alvarez Figueroa

César Luis Valdivieso Salazar

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Mayra Lucía Alvarez Figueroa y César Luis Valdivieso Salazar, bajo mi supervisión.

Ing. Fabio González
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Mi agradecimiento a mi madre por todo su apoyo a lo largo de mi carrera y por ser el pilar fundamental de mi vida, a mis hermanos por brindarme su ayuda y apoyo incondicional en cada momento de mi vida.

Quiero dejar constancia de mi gratitud a los profesores que durante mi carrera compartieron sus conocimientos para con mi persona y por ser más que profesores, amigos.

Un agradecimiento especial al Ing. Fabio González director del proyecto, por brindarnos su dedicación y tiempo a nuestro proyecto de titulación.

Al compañero de mi vida y de proyecto César Valdivieso por brindarme su ayuda, amor y apoyo en todo momento.

Mayra Alvarez Figueroa.

DEDICATORIA

Este trabajo está dedicado a mi mami Lcda. Arbita Figueroa por su amor y paciencia ya que sin ella hubiera sido imposible culminar con éxito mi carrera como Tecnóloga en Electrónica y Telecomunicaciones y a mi papi Pablo Alvarez Castillo que desde el cielo nos ha cuidado a lo largo de nuestras vidas.

A mis hermanos Fernando, Pablo y Leydi por su compañía, comprensión, paciencia y apoyo hacia mi persona, a mis sobrinos preciosos Arelis Nahomi, Alexander David y Pablito Alejandro.

Mayra Alvarez Figueroa.

AGRADECIMIENTO

A los diferentes docentes de la Escuela de Formación de Tecnólogos de la Escuela Politécnica Nacional que tuve el placer de conocer durante mi formación profesional y que inculcaron en mí, valores de bien, además de su conocimiento.

De manera especial al Ing. Fabio González quien se dio el tiempo, a pesar de sus múltiples obligaciones, para dirigirnos acertadamente en el desarrollo del presente proyecto.

A mis padres por su esfuerzo y apoyo, quienes nunca han dejado de esforzarse a pesar de las dificultades de la vida y de quienes aprendí a nunca dejarme vencer.

En especial a mi madre quien estuvo siempre a mi lado y a mis hermanas quienes son la inspiración para alcanzar mis objetivos y metas.

A mi compañera Mayra Alvarez por ser mi mano derecha, mi mejor amiga y mi confidente, además de demostrarme con su amor y ternura que el mundo es un lugar hermoso para vivir.

Un agradecimiento especial a mi amigo y tío, el Ing. Milton Salazar quien desde que tengo memoria siempre a estado a mi lado siendo un gran apoyo para mi persona y para mi familia.

César Valdivieso Salazar.

DEDICATORIA

A las personas que siempre confiaron en mí: mis padres, mi familia y mis amigos, en especial a mi madre, la Dra. Rosalía Salazar quien demostró ser la mujer más fuerte que he conocido, por ser un ejemplo a seguir y la mejor mamá del mundo.

Y como les dije a mi madre y mis hermanas María Fernanda y Dianita Carolina cuando empecé esta carrera: - ¡Va por ustedes!!!

César Valdivieso Salazar.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto tiene como objetivo principal aumentar el nivel de seguridad del conjunto residencial “El Prado” y por lo tanto aumentar la calidad de vida de los condóminos del mismo, además de salvaguardar su integridad y sus bienes materiales.

La necesidad de implementar un sistema de video vigilancia surge principalmente por el aumento de la delincuencia en nuestra ciudad, y se opta por un sistema inalámbrico debido al gran tamaño del conjunto y las ventajas que tiene respecto a un sistema cableado.

En el capítulo 1 se presenta los conceptos básicos de cada tema concerniente al proyecto, con el objeto de tener claro el fundamento teórico del presente proyecto.

En el capítulo 2 se detalla los elementos necesarios para el diseño como son: zona de cobertura, ancho de banda, capacidad de almacenamiento, parámetros y requerimientos. Además se seleccionan los equipos necesarios para la implementación del sistema de acuerdo a los parámetros y requerimientos preestablecidos.

En el capítulo 3 se presenta el cálculo teórico del enlace radio-eléctrico usando como datos las especificaciones técnicas de los equipos ya seleccionados y la ubicación de los mismos dentro del conjunto. También se describe la implementación del sistema y la configuración de cada uno de los equipos además de las respectivas pruebas del sistema de video vigilancia en funcionamiento.

En el capítulo 4 se resalta las conclusiones más importantes y las recomendaciones que se obtuvieron como resultado de la implementación del sistema de video vigilancia utilizando Wi-Fi para el conjunto residencial “El Prado”.

Además se adjuntan 3 anexos: Simulación del área de cobertura del sistema de video vigilancia usando el software HeatMapper proporcionado por Ekahau, características técnicas de los equipos y fotografías de la implementación.

PRESENTACIÓN

Los sistemas de video vigilancia nacen con la necesidad de brindar seguridad tanto a las personas como a sus bienes y han ido creciendo y mejorando con el pasar de los años, empezando con los circuitos cerrados de televisión hasta llegar en la actualidad a modernos sistemas de video vigilancia inalámbricos.

La variedad de aplicaciones de video vigilancia permite que éstas se implementen en cualquier campo por complejo que sea, la video vigilancia inalámbrica es líder debido a las ventajas que presenta frente a otros sistemas de video como su instalación, la calidad de las imágenes, video en tiempo real, facilidades de ampliar el sistema, etc.

La tecnología de video IP permite conectarse a Internet de modo que se puede acceder en cualquier momento y desde cualquier lugar a las imágenes de las cámaras.

El audio, el zoom de la imagen, la capacidad de programar la grabación ya sea grabación continua, por horas específicas o por detección de movimiento hace que los sistemas de video vigilancia basada en tecnología IP sean la mejor opción en el mercado.

CAPÍTULO 1. FUNDAMENTOS TEÓRICOS

1.1 ONDAS RADIOELÉCTRICAS

Las ondas radioeléctricas conocidas también como radio frecuencia (RF) son muy utilizadas en sistemas de telecomunicaciones inalámbricas por lo que daremos una breve descripción a continuación.

1.1.1 DEFINICIÓN

Conjunto de ondas electromagnéticas[1] en un rango definido, desde los 3KHz hasta los 3000GHz, del espectro electromagnético. Otra definición: las ondas radioeléctricas son aquellas que pertenecen al espectro radioeléctrico, siendo éste una porción del espectro electromagnético, definido en un rango específico. El espectro radioeléctrico está dividido en 9 bandas de frecuencia, cada una con un rango definido como se muestra en la tabla 1.1.

Tabla 1.1 Espectro Radioeléctrico

NOMBRE	ABREVIATURA INGLESA	FRECUENCIAS	LONGITUD DE ONDA
Muy baja frecuencia (Very low frequency)	VLF	3–30 kHz	100 km – 10 km
Baja frecuencia (Low frequency)	LF	30–300 kHz	10 km – 1 km
Media frecuencia (Medium frequency)	MF	300–3000 kHz	1 km – 100 m
Alta frecuencia (High frequency)	HF	3–30 MHz	100 m – 10 m
Muy alta frecuencia (Very high frequency)	VHF	30–300 MHz	10 m – 1 m
Ultra alta frecuencia (Ultra high frequency)	UHF	300–3000 MHz	1 m – 100 mm
Súper alta frecuencia (Super high frequency)	SHF	3-30 GHz	100 mm – 10 mm
Extra alta frecuencia (Extremely high frequency)	EHF	30-300 GHz	10 mm – 1 mm
> EHF	---	> a 300 GHz	< 1 mm

[1] Una onda electromagnética es la forma de propagación de la radiación electromagnética a través del espacio, no necesitan de un medio material para propagarse, es decir pueden desplazarse por el vacío.

1.1.2 FENÓMENOS DE PROPAGACIÓN

Las ondas electromagnéticas se ven afectadas por varios fenómenos que se deben tomar en cuenta al realizar un radioenlace. A continuación se da una breve descripción de cada uno de ellos.

Atenuación

Pérdida de energía por longitud recorrida, la medida usada para medir la atenuación son los dB, conocida también como ley inversa cuadrática. A mayor distancia mayor atenuación, como se muestra en la figura 1.1.

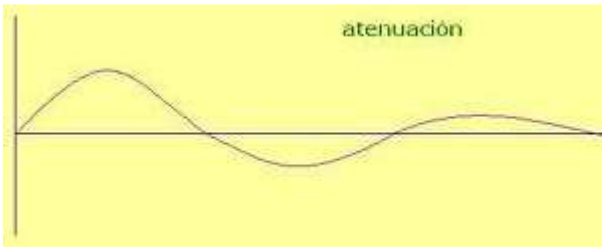


Figura 1.1 Atenuación
Tomada de http://docente.ucol.mx/al021593/RUIDO.htm

Absorción

Pérdida de energía por materiales específicos; los materiales que absorben energía electromagnética naturalmente son: la vegetación y las partículas en el espacio (O_2 y vapor de agua), siendo el principal factor de pérdida de energía el O_2.

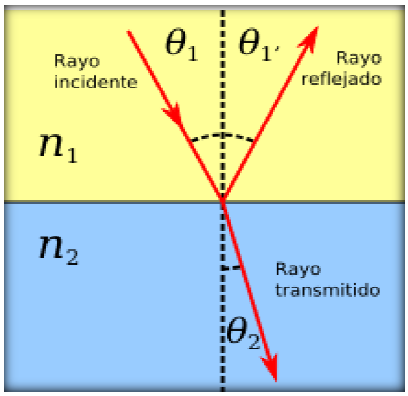
La principal diferencia entre atenuación y absorción es que esta última es pérdida de energía debido a las partículas del medio.

Refracción

Cambio de dirección de un frente de onda[2] al atravesar de un medio de propagación a otro, este fenómeno está definido por la Ley de Snell, se detalla a

[2] Frente de onda: Lugar geométrico en que los puntos del medio son alcanzados en un mismo instante por una determinada onda. Dada una onda propagándose en el espacio o sobre una superficie, los frentes de onda pueden visualizarse como superficies o líneas que se desplazan en el transcurso del tiempo alejándose de la fuente sin tocarse.

continuación en la figura 1.2.



$$n_1 * sen\theta_1 = n_2 * sen\theta_2$$

Figura 1.2 Ley de Snell
Tomada de http://ractually.blogspot.com/2007/04/por-dnde-tiene-que-ir-un-socorrista.html

Reflexión

Es el fenómeno que describe cuando un rayo incide sobre una superficie y éste es reflejado. Rayleigh estableció el "Principio de Rugosidad", este principio describe que una superficie es lisa o rugosa dependiendo de la longitud de onda " " del rayo que va a incidir sobre ella, es decir si un rayo con una gran longitud de onda incide en una superficie "rugosa", la superficie no afectará la dirección del rayo y se considerará una superficie lisa.

Se considera reflexión perfecta cuando el ángulo de incidencia y el ángulo de reflexión son iguales, como se indica en la figura 1.3 a continuación:

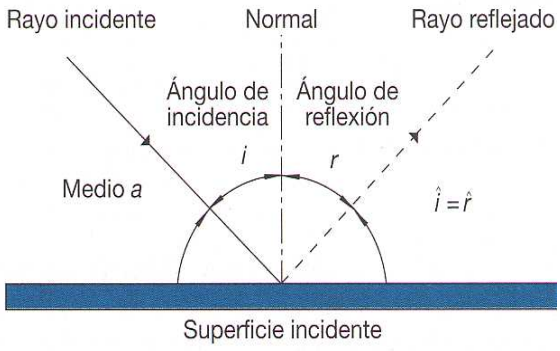


Figura 1.3 Reflexión de un Rayo
Tomada de http://fisicaucidandro.blogspot.com/2009/05/reflexion-y-leyes.html

Difracción

Este fenómeno se basa en el curvado y esparcido de las ondas cuando encuentran un obstáculo o al atravesar una rendija, el principio de Huygens afirma que todo punto de un frente de onda inicial puede considerarse como una fuente de ondas esféricas secundarias que se extienden en todas las direcciones con la misma velocidad, frecuencia y longitud de onda que el frente de onda del que proceden.

Interferencia

Es la diferencia de fase debido al camino recorrido, existen 2 tipos de interferencia: canal adyacente y co-canal.

Interferencia adyacente:

Esta interferencia se da por un mal filtrado en el receptor, ya que recibe frecuencias de otro canal, cercanas a la frecuencia deseada como se indica en la figura 1.4.

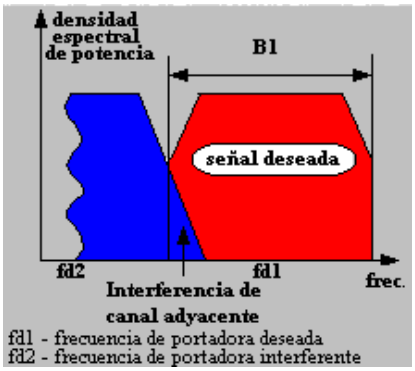


Figura 1.4 Interferencia Adyacente
Tomada de http://www.upv.es/satelite/trabajos/pract_4/radio/interf2.htm

Interferencia co-canal:

Esta interferencia se da debido a que el receptor recibe la resultante proveniente de una suma vectorial donde el primer sumando es la onda directa y el segundo es la onda reflejada, para que la onda reflejada llegue con la misma fase que tiene la onda directa debe haber un número entero de longitudes de onda "λ" entre el transmisor y el receptor.

Existen 2 subtipos: aditiva y sustractiva. Si el número de longitudes de onda “n” es par la interferencia co-canal es aditiva, si “n” es impar la interferencia co-canal es sustractiva, si “n” no es un entero estamos en los intermedios y la resultante será una suma de vectores.

Dispersión

Es un caso especial de reflexión, cuando el frente de onda choca con una superficie heterogénea y existe dispersión de energía, la dispersión generalmente es troposférica.

1.1.3 MECANISMOS DE PROPAGACIÓN

Propagación es el camino que toma la energía para llegar del transmisor al receptor, como se indica en la figura 1.5. Existen 5 mecanismos de propagación que se detallan a continuación.

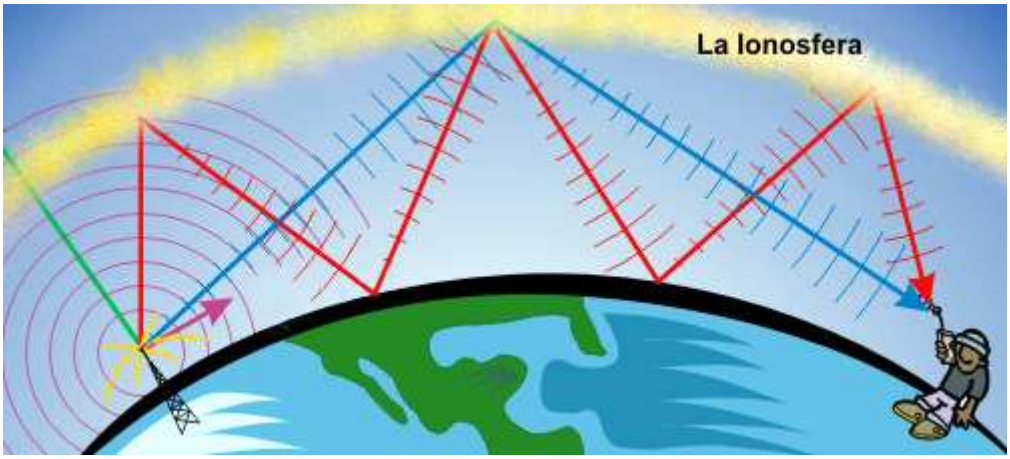


Figura 1.5 Mecanismos de Propagación
Tomada de http://ondascortas.blogspot.com/2010/06/radio-propagacion-ionosferica.html

Onda superficial

Es el camino preferido por las ondas electromagnéticas, como su nombre lo indica las ondas recorren la superficie hasta llegar a su destino, se utiliza este mecanismo hasta una longitud de onda de 100 metros, en la banda VLF la tropósfera se comporta como una guía de onda natural.

Onda directa

Las antenas: transmisora y receptora se pueden ver, es decir tienen línea de vista. Se debe garantizar en las bandas desde la VHF hasta la banda superior a la EHF. El obstáculo natural para este mecanismo es la redondez de la tierra, no existe el rayo directo si no un rayo curvo, la curvatura del rayo depende del índice de refracción de la atmósfera.

Cuando la energía viaja como onda directa se forma un huso entre el transmisor y el receptor llamada Zona de Fresnel, ésta hace que las ondas no se desfasen más de 180º para que la interferencia co-canal no destruya a la onda directa.

Para que exista un radio-enlace en la onda directa, la primera Zona de Fresnel debe considerarse sin obstáculos (hasta el 40%).

Onda reflejada

Se considera onda reflejada cuando la altura de la antena transmisora es hasta 5 longitudes de onda "λ" de la frecuencia con la que estemos trabajando, debido a que si sobrepasa las 5 longitudes de onda "λ" (siendo más estrictos 10 longitudes de onda) la energía de la onda reflejada recorre mucha distancia por lo que es despreciable.

Onda ionosférica

Este tipo de mecanismo de propagación usa como reflector a la ionósfera, la reflexión ionosférica solo se da en la banda HF. El mayor problema que presenta este mecanismo es el desvanecimiento de la señal debido a que la ionósfera se mueve respecto al planeta.

Onda de dispersión

La onda directa se dispersa en todas las direcciones tanto en la ionósfera como en la tropósfera, es un mecanismo muy poco usado porque desperdicia mucha energía y su eficiencia es igual al 1%.

1.2 REDES INALÁMBRICAS

1.2.1 DEFINICIÓN

Red inalámbrica es un término que se utiliza para designar la conexión de equipos inalámbricos sin la necesidad de una conexión física (cables), esta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

1.2.2 TIPOS

Según su área de cobertura:

Wireless Personal Area Network (WPAN)

Tipo de red de cobertura personal, generalmente usado para conectar dispositivos inalámbricos dentro de un domicilio. Las tecnologías usadas son:

- HomeRF
- Bluetooth (IEEE[3] 802.15.1)
- ZigBee (IEEE 802.15.4)

Wireless Local Area Network (WLAN)

Redes que abarcan locales, domicilios, edificios y hasta campus. En las redes de área local podemos encontrar tecnologías inalámbricas basadas en HiperLAN (High Performance Radio LAN), o tecnologías basadas en Wi-Fi (IEEE 802.11).

Wireless Metropolitan Area Network (WMAN)

Red de área metropolitana, es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, las tecnologías que se usan son:

- WiMAX (Worldwide Interoperability for Microwave Access) (Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16
- LMDS (Local Multipoint Distribution Service).

[3] IEEE- Institute of Electrical and Electronics Engineers.

Wireless Wide Area Network (WWAN)

Una red de área global abarca el mundo entero, en estas redes encontramos tecnologías como UMTS (Universal Mobile Telecommunications System), utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología GSM (para móviles 2G), también la tecnología digital para móviles GPRS (General Packet Radio Service).

1.2.3 REDES DE ÁREA LOCAL INALÁMBRICAS (WLAN)

1.2.3.1 Definición

Una red de Área Local Inalámbrica es una interconexión de equipos generalmente heterogéneos y que pueden funcionar autónomamente, que usan como medio de transmisión el espacio libre. Se comunican mediante la propagación de ondas electromagnéticas por el espacio libre. Una WLAN provee todas las características y beneficios de las tecnologías tradicionales como Ethernet pero sin las limitaciones de los cables.

Las redes inalámbricas deben dar las mismas prestaciones que las redes cableadas, es decir deben tener la misma calidad de servicio. Las WLAN empezaron utilizando tecnología infrarroja, pero cambiaron al poco tiempo a tecnologías basadas en RF (radio frecuencia), debido a las ventajas tecnológicas.

En la tabla 1.2 se muestra la evolución de las WLAN:

Tabla 1.2 Evolución de las WLAN

VELOCIDAD	860 Kbps	1 a 2 Mbps	11 Mbps	54 Mbps	300 Mbps
TIPO DE RED	Propietarias	Basada en Estándares			
BANDA	900 MHz	2.4GHz		5GHz	
		Borrador IEEE 802.11	802.11	802.11 a y b	802.11g	802.11n
	1986	1990	1994	2000	2006	2010

Las WLAN trabajan en las bandas de frecuencia ISM (Industrial, Scientific and Medical), que no requieren licencia gubernamental en ningún lugar del mundo.

El mecanismo de acceso al medio es CSMA/CA Carrier Sense Multiple Access/ Collision Avoidance (acceso múltiple por detección de portadora evitando las colisiones), es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos.

De esta forma, el resto de equipos de la red sabrán cuándo hay colisiones y en lugar de transmitir la trama cuando el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. La figura 1.6 ilustra el funcionamiento del CSMA/CA:

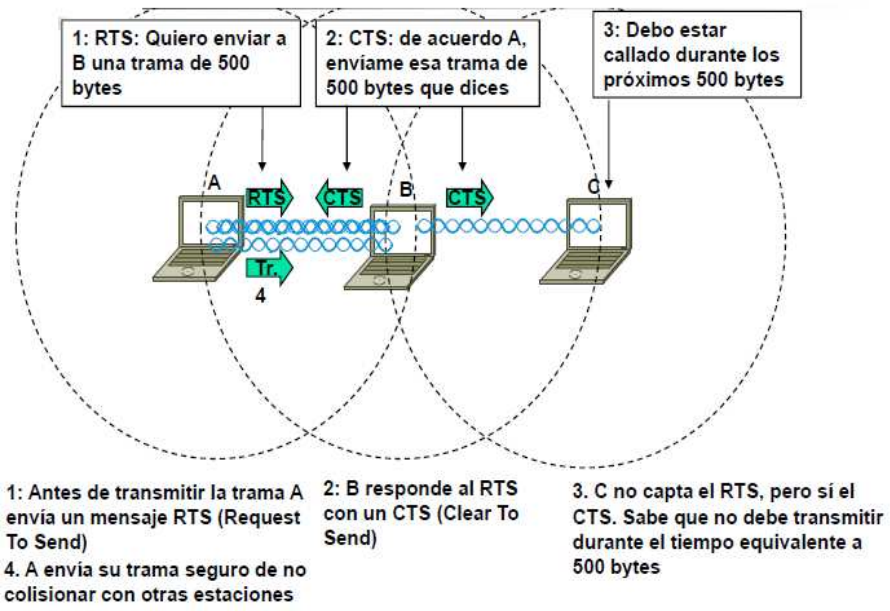


Figura 1.6 Funcionamiento del CSMA/CA
Tomada de http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

1.2.3.2 Terminología usada en los estándares IEEE 802.11

A continuación se muestra una breve descripción de los diferentes términos usados en los estándares IEEE 802.11, estos se detallan en la figura 1.7.

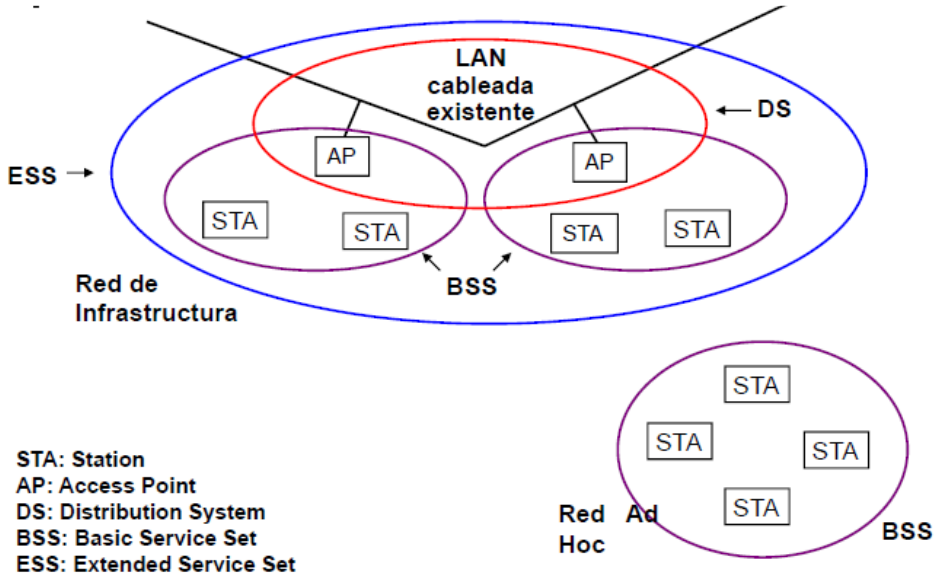


Figura 1.7 Terminología usada en los estándares IEEE 802.11
Tomada de http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

IBSS

Conjunto Básico de Servicio Independiente conocido también como red Ad-Hoc, es un conjunto de estaciones que se reconocen mutuamente según una configuración Peer-to-Peer, no requieren ningún punto de acceso ni tienen acceso a redes externas y el número de equipos que formen parte de ella dependerá del rendimiento que se quiera obtener, como se muestra en la figura 1.8. a continuación:

Figura 1.8 IBSS (Independent Basic Service set)
Tomada de http://www.asisupport.com/newsletter_11_2003.htm

Red de Infraestructura

Requieren de un punto de acceso y se tiene acceso a redes externas; son redes con cierta complejidad e infraestructura que pueden unirse a otras redes cableadas o conectarse a otras infraestructuras inalámbricas.

BSS (Basic Service Set)

Estaciones que se reconocen mediante un único SSID (Service Set Identifier), es decir necesitan un punto de acceso (AP) para unirse a la red.

ESS (Extended Service Set)

Conjunto de varias celdas BSS unidas a través de enlaces cableados o inalámbricos, las celdas pueden pertenecer a la misma o a distintas subredes, como indica la figura 1.9.

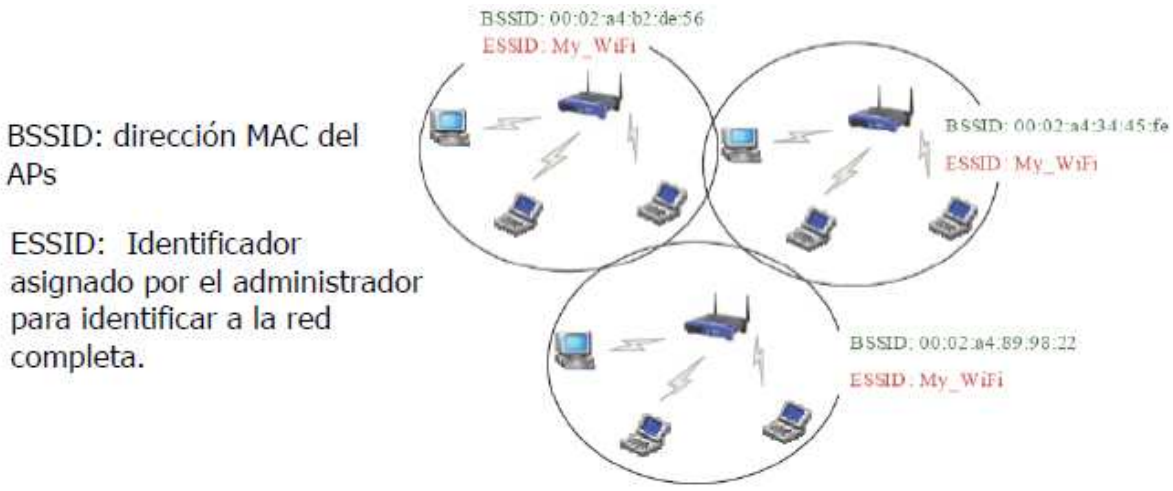


Figura 1.9 ESS (Extended Service Set)
Tomada http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

1.2.3.3 Ventajas y Desventajas

Ventajas

- Movilidad: Los equipos interconectados se pueden mover dentro del área de cobertura sin perder conexión a la red.
- Escalabilidad: Tienen mayor facilidad de crecimiento que las redes cableadas.
- Flexibilidad: Cambiar los equipos de lugar no representa mayor problema.
- Se disminuyen tiempos y costos de instalación.
- Son muy adecuadas en los siguientes escenarios: ambientes con cambios frecuentes, auditorios, sala de reuniones, espacios abiertos, instalaciones temporales, instalaciones en edificaciones antiguas, etc.

Desventajas

- Interferencias y degradación de las señales de RF. Esta desventaja se refiere a los fenómenos de propagación antes descritos.
- Manejo de potencia, velocidad.
- Interoperabilidad de los equipos.
- Seguridad: Al no ser una red cableada cualquier persona que esté dentro del área de cobertura y que tenga un equipo inalámbrico puede detectar la red.
- Afectación a la salud: Existen estudios que refieren que las ondas electromagnéticas causan daño al ser humano, también existen otros estudios que refieren lo contrario.

1.2.3.4 Estándares para WLAN (IEEE 802.11)

El estándar IEEE 802.11 define el uso de dos niveles de la arquitectura OSI[4] (capas física y de enlace), especificando sus normas de funcionamiento en una WLAN. Específicamente tiene normas en la capa física y en la subcapa MAC de la capa enlace, como ilustra la siguiente figura 1.10.

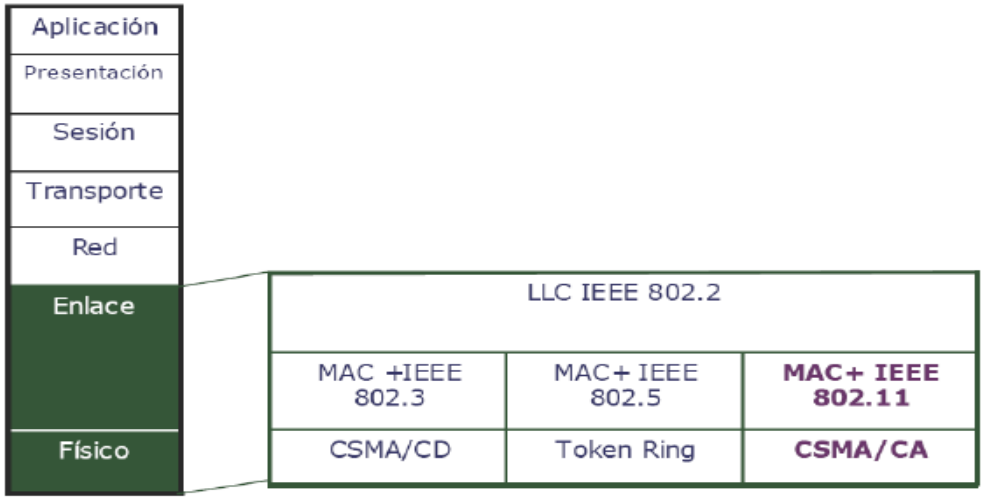


Figura 1.10 IEEE 802.11
Tomada http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

Este estándar se basa en la técnica de Spread Spectrum (espectro ensanchado) donde se utiliza un ancho de banda mayor al necesario para la transmisión ganando inmunidad frente al ruido y permitiendo transmitir bastante información en un pequeño rango de frecuencia, se utilizan por lo general 2 sistemas de codificación: DSSS (Direct-Sequence Spread Spectrum) y OFDM (Orthogonal Frequency-Division Multiplexing). El estándar IEEE 802.11 divide a la banda de 2.4GHz (2400 – 2483,5) en canales de 22MHz que están superpuestos, el número de canales varía de acuerdo a cada país, en Ecuador usamos las regulaciones de la FCC (11 canales de 22MHz), como se detalla en la tabla 1.3 a continuación:

[4] OSI—Open System Interconnection.

Tabla 1.3 Canales Banda 2.4 GHz

CANAL	FRECUENCIA CENTRAL	FCC (AMÉRICA)	ETSI (EUROPA)	MKK (JAPON)
1	2412			
2	2417			
3	2422			
4	2427			
5	2432			
6	2437			
7	2442			
8	2447			
9	2452			
10	2457			
11	2462			
12	2467			
13	2472			
14	2484			

IEEE 802.11a

El estándar 802.11a utiliza los mismos protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza como técnica de codificación OFDM (Orthogonal Frequency Division Multiplexing) con una velocidad máxima de 54 Mbps. 802.11a tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto. Dado que la banda de 2.4 GHz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a, a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso.

IEEE 802.11b

El estándar 802.11b trabaja en la banda de 2.4 GHz y utiliza como técnica de codificación DSSS (Direct Sequence Spread Spectrum) con una velocidad máxima de 11 Mbps. Los códigos de ensanchamiento usados en este estándar son el CCK (Complementary Code Keying) y el Barker Code. Utiliza la técnica DRS (Dynamic Rate Shifting) que permite variar las velocidades entre 1, 2, 5.5, 11 Mbps para compensar problemas de recepción al atravesar diversos materiales o recorrer distintas distancias.

IEEE 802.11g

Es la evolución del estándar 802.11b, este utiliza la banda de 2.4 GHz pero opera a una velocidad teórica máxima de 54 Mbps, que en promedio es de 22.0 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Actualmente existen equipos con especificaciones, con potencias de hasta ½ watio que permite hacer comunicaciones de hasta 50 Km con equipos de radio apropiados.

IEEE 802.11n

Estándar aprobado en Octubre del 2009, la velocidad real de transmisión podría llegar a los 600 Mbps. Utiliza la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento. A continuación se muestra la figura 1.11 resumiendo los estándares IEEE 802.11:

Norma	Banda de frecuencia	Modulación	Alcance	Velocidad máxima	Nº máx. canales sin solap.
802.11 b	2.4 GHz	DSSS	100 m	11 Mbps	3
802.11 a	5 GHz	OFDM	50 m	54 Mbps	12
802.11 g	2.4 GHz	OFDM	100 m	54 Mbps	3
802.11 n	5 GHz 2.4 GHz	OFDM	100 m	300 Mbps	12 3

Norma	Ampliación
802.11 d	Aspectos reglamentarios en países sin normativa vigente sobre 802.11
802.11 e	Define niveles de QoS
802.11 f	IAPP (Inter Access Point Protocol)
802.11 h	Mejora de 11 a en potencia y selección de canal de radio
802.11 i	Mecanismos de seguridad – AES (Advanced Encryption Standard)
802.11 j	Resuelve la adición del canal 4.9 GHz al de 5 GHz para 11 a en Japón

Figura 1.11 Resumen de Estándares IEEE 802.11
Tomada de http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

1.2.3.5 Elementos de una WLAN

Antenas

Una antena es un dispositivo diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa. En otras palabras una antena es un transductor que transforma energía eléctrica en electromagnética y viceversa.

Existe una gran diversidad de tipos de antenas, dependiendo del uso al que van a ser destinadas. En unos casos deben expandir en lo posible la potencia radiada, es decir, no deben ser directivas (ejemplo: una emisora de radio comercial o una estación base de teléfonos móviles), en otras ocasiones deben serlo para canalizar la potencia en una dirección y no interferir a otros servicios (antenas entre estaciones de radioenlaces). Una antena también es la que esta integrada en la tarjeta de red inalámbrica para conectarse a las redes Wi-Fi.

Parámetros de una Antena

Las antenas se caracterizan por una serie de parámetros, los cuales se describen a continuación:

- Diagrama de radiación.- Es la representación gráfica de cómo está distribuida la energía alrededor de una antena.
- Ancho de Banda.- Es el rango de frecuencias en el cual se considera que la antena opera aceptablemente.
- Directividad
    - Omnidireccionales.- Radia igual en todas las direcciones.
    - Isotrópica.- Es una antena teórica con un patrón de radiación uniforme en las 3 dimensiones.
    - Direccionales.- Son aquellas antenas que radian en una dirección determinada como por ejemplo: Yagi, Parabólicas, de Panel, etc.
- Ganancia.- Es una medida de qué tan bien una antena focaliza/dirige la energía de RF en una dirección determinada.
- Eficiencia.- Es la relación entre la potencia radiada y la potencia de transmisión.
- Impedancia de Entrada.- Es la impedancia de la antena en sus terminales. Otra definición: es la relación entre la tensión y la corriente de entrada.
- Anchura de Haz.- Es el ancho medido en grados del lóbulo principal de radiación, medido en los puntos de ½ potencia (-3dB).
- Polarización.- Es la orientación del campo eléctrico radiado por la antena, es la orientación física del elemento de la antena que emite la energía de RF.
- Resistencia de Radiación.- La resistencia de radiación es igual a la relación entre la potencia radiada por la antena y la corriente al cuadrado en el punto de alimentación.
- Diversidad.- Es la operación simultánea de 2 o más sistemas o partes de un sistema en condiciones diferentes, para mejorar la confiabilidad del sistema. Existen dos tipos:
    - Diversidad de espacio (más usada en WLAN)
    - Diversidad de frecuencia

En la figura 1.12 se ilustran una antena parabólica y una tarjeta de red inalámbrica.

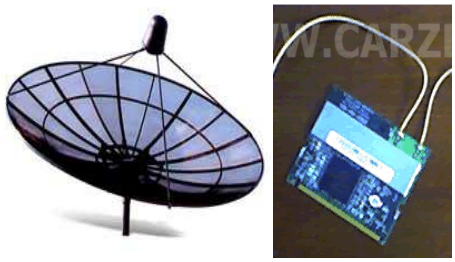


Figura 1.12 Antenas
Tomada de http://www.telali.com.pe/destino/p1.htm

Access Point

Un punto de acceso inalámbrico WAP (Wireless Access Point) o AP es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un AP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Muchos AP`s pueden conectarse entre sí para formar una red aún mayor. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada.

Un único AP puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros. Este o su antena normalmente se colocan en alto pero podrían colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. En la figura 1.13 se muestran algunos AP`s.

Figura 1.13 Access Point
Tomada de http://arfes.ircfast.com/group/view/kl40615/Driver_Acer_WarpLink_Access_Point.htm

Routers

El “enrutador” en inglés router conocido también como direccionador o encaminador es un dispositivo de hardware para interconexión de red de computadores que opera en la capa tres (capa red) del modelo OSI. Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos. En la figura 1.14 de indican algunos de ellos.

Figura 1.14 Routers
Tomada de http://www.techfuels.com/general-networking/3483-routers.html

Wireless Router

Un router inalámbrico es un dispositivo que realiza las funciones de un router, pero también incluye las funciones de un AP inalámbrico. Es de uso general para permitir el acceso a la Internet o una red sin la necesidad de una conexión cableada. Puede funcionar en una red LAN cableada, una red LAN inalámbrica sola, o una mezcla entre red cableada e inalámbrica. Los Wireless Routers se indican en la figura 1.15 y realizan las siguientes funciones.

- AP (Access Point)
- Switch LAN
- Router
- Proxy server (NAT)
- DHCP Client
- DHCP Server
- Firewall

Figura 1.15 Wireless Router
Tomada de http://narowalonline.com/?p=17881

Switches

Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (capa enlace) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LAN.

Algunos switches se indican en la figura 1.16.

Figura 1.16 Switches
Tomada de http://www.phoenixcontact.es/productos/21718_21733.htm

Adaptadores de red inalámbrica

Adaptador de red inalámbrica o NIC (Network Interface Card) tarjeta de interfaz de red, permite la intercomunicación entre equipos sin la necesidad de cables. Hay diversos tipos de adaptadores de red inalámbrica en función de la topología que se utilice en la red inalámbrica. Los más conocidos son:

- USB
- Mini-PCI
- PCMCIA

En la figura 1.17 se ilustra una PCMCIA.

Figura 1.17 Tarjeta de red inalámbrica PCMCIA
Tomada de http://www.tecnomaniacos.com/shop/?mod=cat&cat_id=12

Cables

Cable Coaxial.- Es utilizado para transportar señales eléctricas, posee dos conductores concéntricos uno central llamado vivo, encargado de llevar la información y uno exterior de aspecto tubular llamado malla o blindaje, que sirve como referencia de tierra.

El conductor central puede estar constituido por un alambre sólido o por varios hilos retorcidos de cobre; mientras que el exterior puede ser una malla trenzada, una lámina enrollada o un tubo corrugado de cobre o aluminio, como se indica en la figura 1.18.

Figura 1.18 Cable Coaxial RG-58/U
Tomada de http://www.afsoncable.com/rg58-cable.htm

Cable de Pares Trenzados.- El cable de pares trenzados es una forma de conexión en la que los aisladores son entrelazados para tener menores interferencias, aumentar la potencia y disminuir la diafonía[5] de los cables adyacentes, se ilustra uno de ellos en la figura 1.19.

[5] Diafonía - Inducción de una señal en otra.

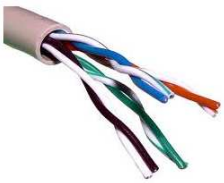


Figura 1.19 Cable de Pares Trenzados
Tomada de http://redesadsi.wordpress.com/clasificacion-de-las-redes/

Existen diversos tipos de pares trenzados a continuación se detalla algunos de ellos:

- UTP → Unshielded Twisted Pair (Cable de Pares Trenzados No Blindado). Se ilustra en la figura 1.20.

Figura 1.20 Cable UTP
Tomada de http://www.videovigilancia.com.mx/ventaonline/index.php?id_categoria=32

- FTP → Foiled Twisted Pair (Cable de Pares Trenzados Apantallado). Se ilustra en la figura 1.21.

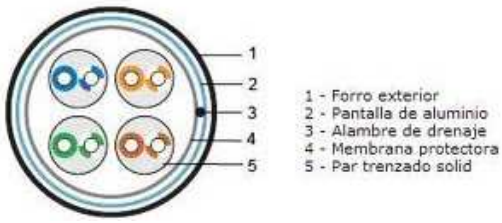


Figura 1.21 Cable FTP
Tomada de http://www.btech.cl/pro.php?id=201224

- STP → Shielded Twisted Pair (Cable de Pares Trenzados Blindado). Se ilustra en la figura 1.22.

Figura 1.22 Cable STP
Tomada de http://www.alfinal.com/Temas/cableadoestructurado.php

- ScTP → Screened Twisted Pair. Se ilustra en la figura 1.23.

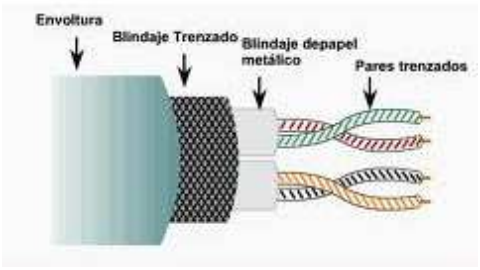


Figura 1.23 Cable ScTP
Tomada de http://www.monografias.com/trabajos30/cableado/cableado.shtml

- SsTP → Screened Shielded Twisted Pair. Se ilustra en la figura 1.24.

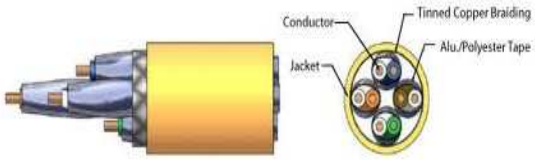


Figura 1.24 Cable SsTP
Tomada de http://www.conexplusnet.com/sstp_cable.html

Conectores

Un conector es un hardware utilizado para unir cables o para conectar un cable a un dispositivo, por ejemplo para conectar un cable de módem a una computadora. La mayoría de los conectores pertenece a uno de los dos tipos existentes: Macho

o Hembra. El conector macho se caracteriza por tener una o más clavijas expuestas; los conectores hembra disponen de uno o más receptáculos diseñados para alojar las clavijas del conector macho.

Conector tipo N

Los conectores tipo N son conectores roscados para cable coaxial, funcionando dentro de especificaciones hasta una frecuencia de 11 GHz. Se adapta a un amplio rango de cables coaxiales, medios y miniatura. Existen en grado comercial, industrial y militar, son de dos tipos: estándar y corrugado.

Conectores N estándar:

- Impedancia: 50 Ω
- Frecuencia: 0 - 11 GHz
- Tensión máxima de pico: 1.500 V
- Relación de onda estacionaria entre 0 y 11 GHz:

Conectores N corrugados:

- Impedancia: 50 Ω
- Pérdidas de retorno:
    - 33 dB (1-2 GHz)
    - 28 dB (2-3 GHz)
- Tensión máxima (RMS): 707 V
- Frecuencia: 0 - 11 GHz

Conector RJ-45

RJ-45 es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado. Los conectores se indican en la figura 1.25.

Figura 1.25 Conectores RJ-45 macho y hembra
Tomada de http://torjaquintero.blogspot.com/2010/04/terminacion-de-cables-utp-y-stp.html

Es utilizado comúnmente con estándares como TIA/EIA-568B (figura 1.26), que define la disposición de los pines. Una aplicación común es su uso en cables de red Ethernet, donde suelen usarse 8 pines (4 pares). Otras aplicaciones incluyen terminaciones de teléfonos (4 pines o 2 pares).

Cableado RJ-45 (T568A/B)

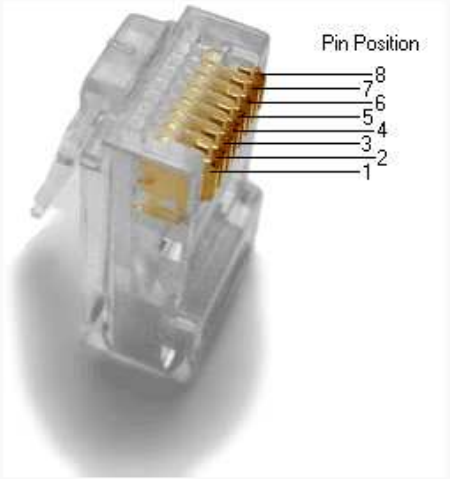
Pin	Color T568A	Color T568B	Pines en conector macho (en conector hembra se invierten)
1	Blanco/Verde (W-G)	Blanco/Naranja (W-O)	
2	Verde (G)	Naranja (O)	
3	Blanco/Naranja (W-O)	Blanco/Verde (W-G)	
4	Azul (BL)	Azul (BL)	
5	Blanco/Azul (W-BL)	Blanco/Azul (W-BL)	
6	Naranja (O)	Verde (G)	
7	Blanco/Marrón (W-BR)	Blanco/Marrón (W-BR)	
8	Marrón (BR)	Marrón (BR)	

Figura 1.26 Estándar T568A Y T568B
Tomada de http://www.consultants-online.co.za/pub/itap_101/html/ch04s05.html

1.2.3.6 Seguridades

Al no ser una red cableada cualquier persona que esté dentro del área de cobertura y que tenga un equipo inalámbrico puede detectar la red.

Los mecanismos de seguridad básica que se usa en las redes WLAN son:

- Bloquear la difusión del SSID (Service Set Identifier)
- No utilizar asignación de IP´s mediante DHCP (Dynamic Host Configuration Protocol)
- Filtros: MAC (Media Access Control), IP y puertos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol)

Filtro MAC

Consiste en programar el punto de acceso a la red para que acepte dispositivos con direcciones MAC específicas, sabiendo que no puede repetirse ninguna MAC en la red. Este mecanismo no es muy confiable ya que gracias al *mac spoofing*[6] es vulnerable.

WEP (Wired Equivalent Protocol)

Es el primer protocolo de cifrado incluido en el estándar IEEE 802.11, proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). El mensaje encriptado C se determina utilizando la siguiente fórmula: C = [M ||ICV (M)] + [RC4 (K ||IV)] donde:

- || es un operador de concatenación y
- + es un operador XOR.

Este protocolo está en desuso debido principalmente a:

- Debilidades del algoritmo RC4 dentro del protocolo WEP debido a la construcción de la clave.
- Los IV`s son demasiado cortos y se permite la reutilización de IV.
- No existe una comprobación de integridad apropiada.

[6] Mac Spoofing.- Son técnicas de suplantación de una dirección MAC por otra distinta.

- Siendo la principal razón que es muy fácil “hackear” una red protegida por WEP.

A continuación en la figura 1.27 se ilustra el Escenario WEP.

Figura 1.27 Escenario WEP
Tomada de http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

WPA/WPA2 (Wi-Fi Protected Access)

WPA.- Mecanismo propuesto por la Wi-Fi Alliance, mejora la codificación de datos usando TKIP (Temporal Key Integrity Protocol) y proporciona autentificación de usuarios (IEEE 802.1X). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado.

Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida ([PSK], Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

WPA2.- Una vez finalizado el nuevo estándar 802.11i se crea el WPA2 basado en este. WPA se podría considerar de "migración”, mientras que WPA2 es la versión certificada del estándar de la IEEE.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

A continuación en la figura 1.28 se ilustra el Escenario WPA.

Figura 1.28 Escenario WPA
Tomada de http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

1.3 DIRECCIONAMIENTO IP

1.3.1 DEFINICIÓN

Una dirección IP es una serie de números asociadas a un dispositivo (generalmente una computadora), con la cual es posible identificarlo dentro de una red configurada específicamente para utilizar este tipo de direcciones (una red configurada con el protocolo IP).

Como Internet es una red basada en el protocolo IP toda computadora o dispositivo conectado a esta, deben ser asociados a una dirección IP. Esta dirección identifica a ese dispositivo unívocamente y puede permanecer invariable en el tiempo o cambiar cada vez que se reconecte a la red. Una dirección IP es estática cuando no varía, y es dirección IP dinámica cuando cambia en cada conexión.

La dirección IP es en un número de 32 bits que en la práctica vemos siempre segmentado en 4 grupos de 8 bits cada uno (xxx.xxx.xxx.xxx). Cada grupo de 8 bits varía de 0-255 y están separados por un punto.

La dirección IP identifica de manera única cada host en su propia red. Dos host de una red no pueden tener la misma dirección IP. Dos equipos pueden tener la misma dirección IP si se encuentran en redes distintas no visibles entre ellas, sin ningún camino posible que las comunique. Cuando accedemos a Internet nuestra

computadora obtiene una dirección IP (pública) única en toda Internet en ese momento. Cada equipo conectado a Internet tiene una dirección IP asignada, que es distinta a todas las demás direcciones IP que están activas en ese momento en todas las redes visibles por la máquina.

Aunque el número de direcciones IP posibles parezca muy elevado, en realidad actualmente hay agotamiento de direcciones IP. Hay que señalar varios conceptos relativos a los tipos de direcciones IP:

- Según el ámbito:
    - Direcciones IP públicas.
    - Direcciones IP privadas (reservadas).
- Según la asignación:
    - Direcciones IP estáticas (fijas).
    - Direcciones IP dinámicas.

Decimos que una dirección IP es pública cuando es visible en todo Internet. Cuando accedemos a Internet desde nuestro equipo obtenemos una dirección IP pública suministrada por el proveedor que nos da conexión a Internet. Nuestro equipo es accesible desde cualquier otro equipo conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

Las direcciones IP privadas se han reservado para los puestos de trabajo de las empresas. Una dirección IP privada sólo es visible en su propia red (LAN) o en otras redes privadas interconectadas por routers. Los equipos con direcciones IP privadas no son visibles desde Internet, sin embargo estos pueden acceder a Internet mediante un dispositivo con una dirección IP pública. Desde Internet sólo es visible el (router, proxy) pero no los equipos con direcciones IP privadas.

Una dirección IP estática es aquella cuyo número es siempre el mismo. Las direcciones IP públicas y estáticas son las que utilizan los servidores de los proveedores de Internet para que siempre estén localizables en la misma dirección. Estas direcciones IP hay que contratarlas a la autoridad correspondiente.

Las direcciones IP dinámicas son aquellas que utilizan un número distinto cada vez que se conecte a Internet. Los proveedores de Internet utilizan direcciones IP dinámicas y públicas para dar acceso a sus clientes. Los proveedores suelen tener más clientes que direcciones IP contratadas, así que cuando un cliente se conecta se le asigna una dirección IP pública dinámica que no esté siendo utilizada en ese momento por otro cliente. Cuando el cliente se desconecta su dirección IP queda libre para otro cliente. Es muy improbable que todos los clientes de un proveedor se conecten simultáneamente.

1.3.2 CLASES DE RED

Hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C. En la actualidad, ICANN reserva las direcciones de clase A para los gobiernos de todo el mundo y las direcciones de clase B para las medianas empresas. Se otorgan direcciones de clase C para todos los demás solicitantes. Cada clase de dirección permite un cierto número de redes y de computadoras dentro de estas redes. A continuación se detalla las clases de red en la tabla 1.4.

Tabla 1.4 Clase de Redes

CLASES DE REDES				
Clase de Red	1er Byte	Máscara	Total de Redes	Computadoras por Red
A	1 a 126	255.0.0.0	126	16 777 214
B	128 a 191	255.255.0.0	16 384	65 534
C	192 a 223	255.255.255.0	2 097 152	254
D	224 a 239	N/A	16	
E	240 a 254	N/A	7	

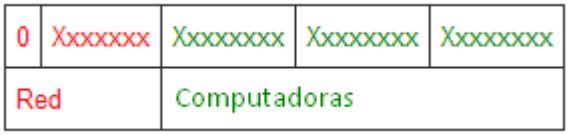
Clase A

En las redes clase A los primeros 8 bits de la dirección son usados para identificar la red, mientras los otros 24 bits son usados para identificar a las computadoras.

Una dirección IP de clase A permite la existencia de 126 redes y 2^{24} – 2 computadoras, esto es 16777214 computadoras por red. Esto pasa porque para

las redes clase A fueron reservadas por la IANA (Internet Assigned Numbers Authority) los IDs "0" y "127". Se indica la clase A en la tabla 1.5.

Tabla 1.5 Clase A

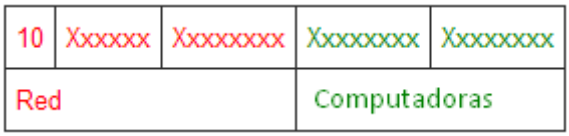


Clase B

En las redes de clase B los primeros dos campos de la dirección es decir 16 bits son usados para identificar la red y los últimos dos campos los restantes 16 bits, identifican las computadoras dentro de estas redes.

Una dirección IP de clase B permite la existencia de 16384 redes y 2^{16} - 2, ó 65534 computadoras por red. El ID de estas redes comienza con "128.0" y va hasta "191.255". Se indica la clase B en la tabla 1.6.

Tabla 1.6 Clase B



Clase C

En las redes de clase C utilizan los tres primeros campos de 8 bits cada uno es decir 24 bits de dirección como identificador de red y sólo el último campo de 8 bits para identificar las computadoras.

Una dirección IP de clase C permite la existencia de 2097152 redes y 2^{16} – 2, es decir 254 computadoras por red. El ID de este tipo de red comienza en "192.0.1" y termina en "223.255.255". Se indica la clase C en la tabla 1.7.

Tabla 1.7 Clase C

En las redes de clase D todos los campos son utilizados para identificar una red y sus direcciones van de "224.0.0.0" hasta "239.255.255.255" y son reservados para los llamados multicast[7].

1.3.3 MÁSCARA DE DIRECCIÓN IP

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Funcionamiento

Básicamente, mediante la máscara de red una computadora (principalmente la puerta de enlace, router) podrá saber si debe enviar los datos dentro o fuera de las redes. Por ejemplo, si el router tiene la dirección IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una dirección IP que empiece por 192.168.1 va para la red local y todo lo que va a otras direcciones IP, para fuera (internet, otra red local mayor).

Supongamos que tenemos un rango de direcciones IP desde 10.0.0.0 hasta 10.255.255.255. Si todas ellas formaran parte de la misma red, su máscara de red sería: 255.0.0.0. También se puede escribir como 10.0.0.0/8

La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y los bits de host usados para crear las subredes. Así, en esta forma de representación (10.0.0.0/8) el 8 sería la cantidad de bits puestos a 1 que contiene la máscara en binario, comenzando desde la izquierda. Para el ejemplo dado (/8), sería 11111111.00000000.00000000.00000000 y en su representación en decimal sería 255.0.0.0.

[7] Multicast.- Es el envío de información a múltiples destinos simultáneamente.

1.4 CÁMARAS IP

1.4.1 DEFINICIÓN

Las cámaras IP, son vídeo cámaras de vigilancia que tienen la particularidad de enviar las señales de video y en muchos casos audio, pudiendo estar conectadas directamente a un Router ADSL, a un concentrador de una Red Local para poder visualizar en directo las imágenes, dentro de una red local (LAN), o a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo.

Las Cámaras IP son un nuevo concepto de seguridad y vigilancia. Una cámara IP es una cámara que emite las imágenes directamente a la red. Debido a su eficiencia y eficacia, se puede utilizar una PC o un servidor estándar para el funcionamiento del software central de monitoreo y de esta manera poder realizar la visualización centralizada. Una cámara de red puede tener una gran variedad de funciones, entre las más importantes tenemos:

- Activación mediante movimiento de la imagen
- Control remoto para mover la cámara y apuntar a una zona
- Programación de una secuencia de movimientos en la propia cámara
- Posibilidad de guardar y emitir los momentos anteriores a un evento.

Las cámaras IP permiten ver en tiempo real qué está pasando en un lugar, aunque esté a miles de kilómetros de distancia. Son cámaras de vídeo de gran calidad que tienen incluido un computador a través del que se conectan directamente a una red. Una cámara IP es un dispositivo que contiene:

- Una cámara de vídeo de gran calidad, que capta las imágenes
- Un chip de compresión que prepara las imágenes para ser transmitidas por la red
- Un computador que se conecta por sí mismo a la red.

Una cámara IP, se describe como una cámara y un computador combinados para formar un único dispositivo. Los componentes principales que integran este tipo de cámaras son: un sensor de imagen, uno o más procesadores y la memoria.

Los procesadores se utilizan para el procesamiento de la imagen, la compresión, el análisis de video y para realizar funciones de red. La memoria se utiliza para fines de almacenamiento del software de la cámara y para la grabación local de secuencias de video.

Las cámaras IP pueden configurarse para enviar video a través de una red IP para visualización o grabación, ya sea de forma continua o en horas programadas. Las imágenes pueden ser capturadas con formato: JPEG, MPEG-4, etc., utilizando distintos protocolos de red.

Existe una serie de elementos de la cámara que repercuten en la calidad de la imagen y el campo de visión. Entre estos elementos se tiene:

- La sensibilidad lumínica (medida en luxes) que es el nivel de iluminación más bajo en el que una cámara produce una imagen aceptable. Cuanto más baja es la especificación de lux, mejor es la sensibilidad lumínica de la cámara. Normalmente, es necesario un mínimo de 200 lux para iluminar un objeto de manera que se pueda obtener una imagen de buena calidad. En general, cuanta más luz reciba el objeto, mejor es la imagen.
- El tipo de objetivo, que permite definir el campo de visión, controlar la cantidad de luz y el enfoque.
- El tipo de sensor de imagen que registra la cantidad de luz a la que se expone un objeto y la convierte en un número de electrones. Cuanto más brillante es la luz, más electrones se generan.
- La técnica de barrido, el barrido entrelazado y el barrido progresivo son las dos técnicas disponibles actualmente y muestran la información producida por los sensores de imagen.

En la actualidad existen cámaras IP inalámbricas, que permiten una conexión inalámbrica a la red, siendo esta característica una ventaja en los sistemas de video vigilancia en especial en los siguientes escenarios: ambientes con cambios frecuentes, auditorios, sala de reuniones, espacios abiertos, instalaciones temporales, instalaciones en edificaciones antiguas.

1.4.2 VENTAJAS RESPECTO A CCTV

Acceso Remoto: La observación y grabación de los eventos no tienen que ser necesariamente en el mismo lugar como lo requieren los sistemas CCTV (Circuito Cerrado de Televisión).

Costo reducido: La instalación es mucho más flexible, se elimina el costo de los sistemas de grabación digital de los CCTV ya que las grabaciones se hacen directamente en el disco duro del computador.

Flexibilidad frente a la ampliación del sistema: Los sistemas tradicionales CCTV requieren duplicar los sistemas de monitorización cuando se amplia el sistema, los sistemas que utilizan cámaras IP permiten su ampliación sin necesidad de aumentar los sistemas de monitorización.

CAPÍTULO 2. ELEMENTOS NECESARIOS PARA EL DISEÑO

2.1 ZONA DE COBERTURA DEL SISTEMA DE VIDEO VIGILANCIA

El conjunto residencial “El Prado” tiene aproximadamente 200 metros de largo medidos longitudinalmente, el conjunto cuenta con 52 casas distribuidas en dos hileras, la garita del guardia al inicio del conjunto y una casa comunal al final del mismo como muestra la siguiente figura:

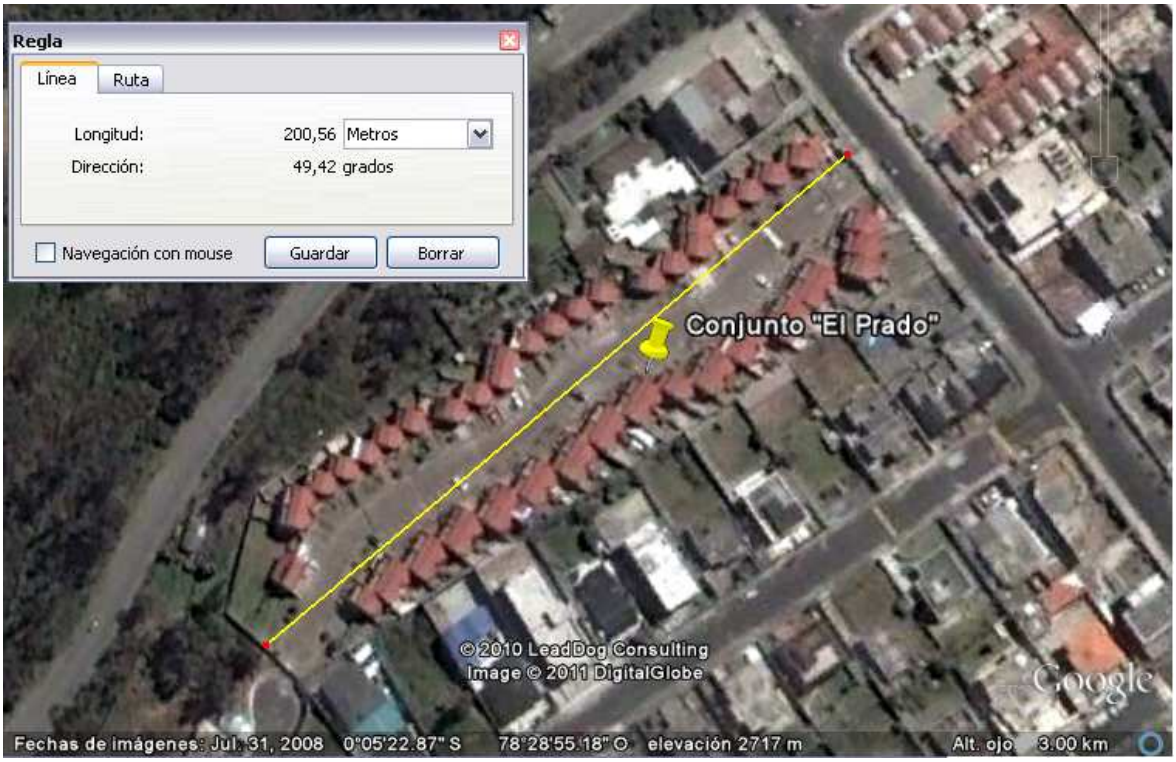


Figura 2.1 Zona de cobertura del sistema de video vigilancia.
Tomada de Google Earth

2.2 ANCHO DE BANDA

A continuación vamos a determinar el ancho de banda teórico necesario es decir, sin formato de compresión y sin tomar en cuenta el tamaño real de bits a transmitirse. Para los cálculos se tomará en cuenta una resolución de 704 x 480 pixeles, 24 bits por pixel (color real) y una frecuencia de 10 imágenes por segundo.

$$I(imagen) = 24\frac{bits}{pixel} \times 337920\ pixeles = 8110080\ \frac{bits}{imagen}$$

$$R = I(imagen) \times frecuencia$$

$$R = 8110080\frac{bits}{imagen} \times 10\ \frac{imagenes}{segundo} = 81{,}1Mbps$$

$$\boldsymbol{AB_{1\ CAMARA} = 81,11Mbps}$$

Para determinar el ancho de banda real es necesario considerar el tamaño real de bits a transmitir, por lo cual se toma de referencia la trama Ethernet y la sobrecarga generada. Los factores que influyen en el cálculo del ancho de banda real para la transmisión de video son:

- El número de imágenes/s,
- La resolución de la imagen,
- El formato de compresión y
- El número de cámaras.

Las técnicas de compresión actualmente más utilizadas son Motion JPEG y MPEG-4. Las técnicas de compresión consisten en reducir y eliminar datos redundantes del video para que la información digital se transmita a través de la red y pueda posteriormente ser procesada.

Por medio de la compresión se puede reducir el tamaño del archivo con una afectación mínima en la calidad de la imagen. A continuación en la tabla 2.1 se muestra algunos valores típicos de compresión de una imagen promedio realizada por una cámara AXIS.

Tabla 2.1 Nivel de Compresión vs. Resolución.[8]

RESOLUCIÓN	NIVEL DE COMPRESIÓN		
	Bajo	**Medio**	**Alto**
PAL 352x288	12 KB	8 KB	4 KB
PAL 704x576	52 KB	34 KB	20 KB
NTSC 352x240	10 KB	7 KB	3 KB
NTSC 704x480	43 KB	28 KB	13 KB

A continuación se presenta el procedimiento para el cálculo del ancho de banda real para una resolución de 704 x 480, con un nivel de compresión medio y en formato M-JPEG. Se siguen los siguientes pasos:

1) Cálculo del número de tramas:

$$\#\ de\ tramas = \frac{Tamaño\ de\ la\ aplicación}{Datos\ útiles\ de\ la\ trama\ Ethernet}$$

$$\#\ de\ tramas = \frac{28KB\ ^{9}}{1460bytes\ ^{10}}$$

$$\#\ de\ tramas = 19{,}17$$

$$\#\ de\ tramas = 19$$

[8] Tomado de http://www.axis.com/files/datasheet/2120/2120_es_ds.pdf
[9] Tomado de la tabla 2.1
[10] Campo de datos de la Trama Ethernet

2) Cálculo de la sobrecarga que produce el paquete transmitido:

$$Sobrecarga\ total = \#\ de\ tramas\ \times Sobrecarga\ trama\ Ethernet$$

$$Sobrecarga\ total = 19\ \times 66\ bytes\ ^{11}$$

$$Sobrecarga\ total = 1254\ bytes$$

3) Cálculo de los datos totales transmitidos:

$$Datos\ totales\ transmitidos = Tamaño\ de\ la\ aplicación + Sobrecarga\ total$$

$$Datos\ totales\ transmitidos = 28\ Kbytes + 1254\ bytes$$

$$Datos\ totales\ transmitidos = 28000\ bytes + 1254\ bytes$$

$$Datos\ totales\ transmitidos = 29254\ bytes = 234{,}032 Kbits = 234032\ bits$$

4) Cálculo del ancho de banda real:

Se usará una frecuencia de 10 imágenes por segundo que es el parámetro admisible para video vigilancia.

$$AB_{1\ CAMARA} = \frac{234{,}032 Kbits}{1\ imagen} \times 10\ \frac{imagenes}{segundo}$$

$$AB_{1\ CAMARA} = 2{,}34 Mbps$$

[11] Sobrecarga real de la Trama Ethernet.

Para que no exista problema en un futuro en cuanto a crecimiento del sistema se calculará un ancho de banda con 6 cámaras:

$$AB_{SISTEMA} = AB_{1\ CAMARA} \times 6\ CAMARAS = 14{,}04Mbps$$

$$\boldsymbol{AB_{SISTEMA} = 14{,}04Mbps}$$

El ancho de banda que se manejará en el sistema será de aproximadamente 14Mbps. Los cálculos aquí presentados se basan en el proyecto de titulación: "Diseño de un Sistema de Vigilancia basado en Tecnología IP para la Protección de los Condominios la Merced de la Ciudad de Ambato", Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Electrónica y Redes de Información, Ing. Lorena Barona, Junio 2010.

2.3 ALMACENAMIENTO

Se tomará en cuenta algunos factores para calcular las necesidades de almacenamiento, los cuales son:

- El número de horas por día en que la cámara estará grabando.
- Tiempo de almacenamiento de los videos.
- Tipo de grabación (detección de movimiento o grabación continua).
- Tipo de compresión y calidad de la imagen.
- El número de cámaras

Se prevé la capacidad de almacenamiento del sistema por el lapso de 7 días (1 semana) y se grabará continuamente. El cálculo se lo realiza para una resolución de 704x480 (NTSC) en formato Motion JPEG, a 10 imágenes por segundo y con un nivel de compresión alto, tamaño de imagen de 13 KB[12]. Para el cálculo de la capacidad de almacenamiento se siguen los siguientes pasos:

[12] Datos referenciales Cámaras AXIS (Tabla 2.1).

1) Se determina la capacidad de almacenamiento por hora.

$$Capacidad\ por\ hora = Tamaño\ de\ imagen\ \times \#de\ imágenes$$

$$Capacidad\ por\ hora = \frac{13\ KB}{imagen} \times \frac{10\ imágenes}{segundo} \times \frac{3600\ seg}{1\ hora}$$

$$Capacidad\ por\ hora = 468\ \frac{MB}{hora}$$

2) Se determina la capacidad por día.

$$Capacidad\ por\ día = \frac{468\ MB}{hora} \times 24\ \frac{horas}{dia}$$

$$Capacidad\ por\ día = 11232\ \frac{MB}{dia}$$

3) Se obtiene la capacidad necesaria para almacenar las grabaciones de una cámara por el lapso de 7 días (1 semana).

$$Capacidad = Capacidad\ por\ día \times \#días\ a\ grabar$$

$$Capacidad\ = 11232\ MB \times 7\ días$$

$$Capacidad = 78624\ MB$$

Para que no exista problema en un futuro en cuanto a crecimiento del sistema se calculará un almacenamiento con 6 cámaras:

La capacidad total del sistema es:

$$Capacidad\ total\ del\ sistema = Capacidad\ de\ una\ cámara \times \#cámaras$$

$$Capacidad\ total\ del\ sistema\ = 78624\ MB \times 6\ cámaras$$

$$Capacidad\ total\ del\ sistema = 471{,}744\ GB$$

Al valor de la capacidad total se debe incrementar un porcentaje del 20% debido al espacio libre que debe tener el disco.

$$Capacidad\ total = 471{,}744\ GB\ \times 1.2$$

$$\boldsymbol{Capacidad\ total = 566{,}093\ GB}$$

Como en el mercado existen discos duros que van desde 128 MB hasta 1.5 TB, utilizaremos un disco estándar de 500 GB y un disco externo de 80 GB.

2.4 PARÁMETROS DEL SISTEMA DE VIDEO VIGILANCIA

El proyecto complementará la necesidad de seguridad de los bienes e integridad de los condóminos del conjunto “El Prado”, por tanto si se llega a cubrir esta necesidad se obtendrán los siguientes beneficios:

- Se podrá acceder en tiempo real a cualquier cámara del sistema desde la central de monitoreo, además se grabará el video proveniente de las cámaras durante un período de tiempo programado con lo que se tendrá un control total del mismo.

- Se procurará la integridad de los condóminos del conjunto y de los bienes materiales del mismo.

El conjunto se encuentra completamente habitado, el status de las personas que viven en dicho conjunto es alto, en consecuencia una instalación que provoque molestias y algún tipo de modificación en las fachadas de las casas no es posible.

Luego del levantamiento de información, en base al criterio de los condóminos, los arrendatarios y nuestro criterio técnico se determina que es necesario diseñar una solución que cumpla con los siguientes parámetros:

- La solución debe permitir la vigilancia de todo el conjunto, además de grabar el respectivo video.

- El sistema de vigilancia debe posibilitar el monitoreo en tiempo real para visitantes y condóminos dentro del conjunto.

- Se tendrá la posibilidad de conectar el sistema de video vigilancia a Internet para aumentar la opción de vigilancia remota a través de cualquier computador conectado a Internet.

- La solución debe permitir un crecimiento fácil y factible del sistema de video vigilancia.

- Las cámaras serán ubicadas estratégicamente de manera que no invadan la privacidad de las personas que habitan en el conjunto.

- El software de la solución debe permitir la visualización y grabación del video en tiempo real.

2.5 REQUERIMIENTOS DEL SISTEMA DE VIDEO VIGILANCIA

A partir de los parámetros antes mencionados y de la situación actual de los condóminos del conjunto residencial “El Prado”, se determina los siguientes requerimientos del sistema:

- El router deberá asignar direcciones IP automáticamente y de preferencia que tenga conexión a Internet.

- El Access Point deberá tener una alta potencia de transmisión (suficiente para cubrir la zona de cobertura) y de preferencia que esté listo para exteriores.

- El Access Point deberá soportar tecnología PoE para facilitar la instalación.

- Se acondicionará un espacio en una sola casa del conjunto para el Access Point y para el router, la cual deberá estar de preferencia en la mitad del conjunto.

- El Access Point será colocado a una altura considerable, para aumentar el alcance de la red y para evitar que personas no autorizadas tengan acceso al equipo.

- Las cámaras deberán ser discretas y de tamaño pequeño.

- Las cámaras deberán soportar tecnología IP, además las cámaras deberán ser inalámbricas y tener una alta sensibilidad de recepción.

- Para la vigilancia se utilizarán cámaras con capacidad de grabación diurna y con poca luz, de preferencia que estén listas para exteriores.

2.6 DIMENSIONAMIENTO DE LOS EQUIPOS

El dimensionamiento de los equipos es de mucha importancia para el rendimiento eficiente de la red inalámbrica. Para determinar las características técnicas de los dispositivos se toma como referencia el ancho de banda, los parámetros y los requerimientos técnicos establecidos.

Del cálculo del ancho de banda real se desprende que el tráfico promedio es de 14 Mbps. Se usará tecnología IEEE 802.11g / 54Mbps, la cual proporcionará confiabilidad en las aplicaciones.

A continuación se presentan las características principales de los equipos a utilizarse.

2.6.1 ROUTER

El router tendrá la función básica de interconectar y asignar direcciones IP dinámicamente a los diferentes dispositivos de la red. Todo router cumple con esta función por lo que el principal criterio de selección de este dispositivo será su posibilidad de conexión a Internet y su precio. El router tendrá las características enlistadas en la tabla 2.2:

Tabla 2.2 Características del Router

CARACTERÍSTICAS DEL ROUTER	
Números de puertos WAN	1 puerto
Números de puertos LAN	Mínimo 1 puerto
Modo de comunicación	Full Dúplex
Gestión de seguridad interna	Username / Password
Gestión de seguridad externa	Firewall
NAT	SI
Protocolos	IP v4

2.6.2 ACCESS POINT

Básicamente el Access Point deberá tener una alta potencia de transmisión además de estar listo para exteriores y que su forma facilite la instalación. El Access Point tendrá las características descritas en la tabla 2.3:

Tabla 2.3 Características del Access Point

CARACTERÍSTICAS DEL ACCESS POINT	
Potencia de transmisión	>18 dBm
Sensibilidad de recepción	Mínimo - 80 dBm
Estándares que soporta	IEEE 802.11g
Seguridad inalámbrica	Mínimo WPA
NAT	SI
Modo Bridge	SI
PoE	SI
Exteriores	SI

La antena del Access Point deberá tener las siguientes características:

- Banda: 2400 – 2483,5 MHz,
- Direccional,
- Ganancia: Mínimo de 5dBi

2.6.3 CÁMARAS IP

Las cámaras IP inalámbricas deberán tener un gran ángulo de visión, además de una alta resolución y una alta sensibilidad de recepción, además de tener un diseño no muy llamativo. De preferencia que estén listas para exteriores. Las cámaras IP inalámbricas tendrán las características descritas en la tabla 2.4:

Tabla 2.4 Características de las cámaras IP.

CARACTERÍSTICAS DE LAS CÁMARAS IP	
Estándares	802.3, 802.11g
Mínima Resolución	640 x 480 pixeles
Detección de Movimiento	SI
RF (EIRP) en dBm	15 dBm
Sensibilidad de recepción en dBm	-70 dBm
Ganancia de antena	1.3 dBi
Seguridad Wi-Fi	WEP, WPA, Wi-Fi Protected Access 2 (WPA2)
Campo de visión	Mínimo > 60 grados
Formato de compresión	Mínimo 2

2.6.4 CENTRAL DE MONITOREO

La central de monitoreo será una computadora que tenga la posibilidad de conectarse a una red inalámbrica y ya que el servidor de video será la misma, necesitará un disco duro mínimo de 500 GB (se desprende del cálculo de almacenamiento). La central de monitoreo tendrá las características descritas en la tabla 2.5:

Tabla 2.5 Características central de monitoreo

CARACTERÍSTICAS CENTRAL DE MONITOREO	
Sistema Operativo	Windows XP sp3
Tipo de procesador	Amd Turion 64
Velocidad Procesador	2 GHz
Memoria RAM	1 GB
Capacidad Disco Duro	500 GB
Tarjeta de red inalámbrica	802.11 g
Tarjeta Gráfica	256 MB
Monitor	14”

2.7 SELECCIÓN DE EQUIPOS

Para la selección de los equipos del sistema de video vigilancia se tomará en cuenta las características establecidas en el dimensionamiento de los equipos, a esto se adiciona el precio, la facilidad de instalación y el período de garantía en marcas diferentes para cada equipo.

2.7.1 ROUTER

En la tabla 2.6 se enlista las características principales de dos equipos: Router EchoLife HG520c y un Router D-Link DSL-500B.

Tabla 2.6 Comparación de los routers.

MARCA	ECHOLIFE	D-LINK
Modelo	HG520c	DSL-500B
Puertos	1 Puerto WAN	1 Puerto WAN
	4 Puertos LAN	1 Puerto LAN
Modo de comunicación	Full dúplex	Full dúplex
Normas	ITU G.992.1 (G.dmt) ITU G.994.1 (G.hs) ANSI T1.413, ITU G.992.3 (G.dmt.bis) ITU G.992.5	ITU G.992.1 (G.dmt) ITU G.992.2 (G.lite) ITU G.992.3 ITU G.994.1 (G.hs) ITU G.992.5 ANSI T1.413
Velocidades DSL	Hasta 24Mbps downstream y hasta 3.5Mbps de upstream	Hasta 24Mbps downstream y hasta 1024Kbps de upstream
Garantía	1 año	1 año
Precio	$ 40	$ 60
Gestión de seguridad interna	Username / Password	Username / Password
Gestión de seguridad externa	Firewall	Firewall
Protocolos	PPPoE, PPPoA, RFC2684 (IPoA), RFC2684B (IPoE).	PPP (RFC 1661) PPPoA (RFC 2364) PPPoE (RFC 2516)

Los 2 equipos tienen similares características y éstas cumplen con las mínimas establecidas, se escoge el router EchoLife HG520c ya que este equipo está incluido en el plan de Internet de CNT por lo que este equipo tendrá costo de 0 dólares en la implementación.

2.7.2 ACCESS POINT

En la tabla 2.7 se enlista las características principales de dos equipos: NanoStation2 by Ubiquiti Network y un Cisco Aironet 1300.

Tabla 2.7 Comparación de los Access Point.

MARCA	UBIQUITI	CISCO
Modelo	NanoStation2	Aironet 1300
Memoria	16MB SDRAM, 4MB FLASH	8MB FLASH
Potencia de transmisión	26 dBm ± 2 dBm	20 dBm
Sensibilidad de recepción	-97 dBm ± 2 Dbm	-81 dBm
Banda de frecuencia	2,4GHz	2,4GHz
Estándares que soporta	IEEE 802.11b IEEE 802.11g	IEEE 802.11g
Gestión de seguridad interna	Username / Password	Username / Password
Ancho de Banda	25 Mbps +	28 Mbps
Seguridad inalámbrica	WEP/WPA/WPA2	802.11i/802.1x/ WPA TKIP
Mac (ACL)	SI	---
NAT	SI	SI
Modo Bridge	SI	SI
PoE	SI	NO
Exteriores	SI	SI
Garantía	1 año	1 año
Precio	$120	$897 a $963

Facilidad de instalación	SI	SI
Antena interna	Si	Si
Ganancia de antena	10 dBi	13 dBi
Tipo de antena	Direccional	Direccional

Los 2 equipos cumplen con las características mínimas establecidas, se escoge la NanoStation2 por tener mayor potencia de transmisión y mayor ganancia de antena, además del factor dinero y la facilidad de configuración. Se muestra el diagrama de radiación de la antena interna del equipo NanoStation2 en la figura 2.2.

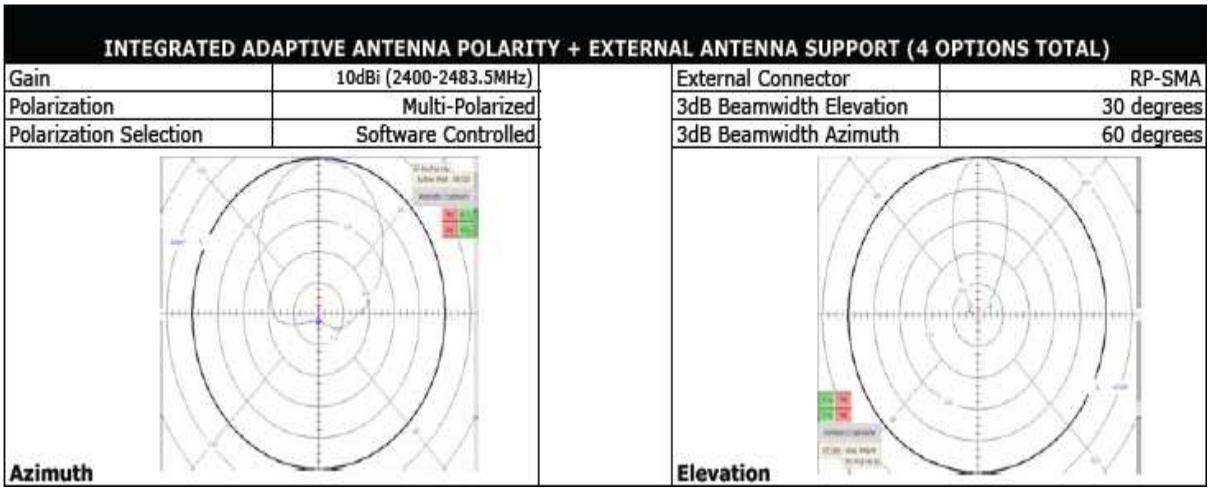


Figura 2.2 Diagrama de radiación de la antena interna NanoStation2
Tomada de www.ubnt.com

2.7.3 CÁMARAS IP

En la tabla 2.8 se enlista las características principales de tres equipos:

- Linksys WVC80N
- D-Link DCS-6620G
- AXIS 211W

Tabla 2.8 Comparación de las cámaras IP.

MARCA	LINKSYS BY CISCO	D-LINK	AXIS
Modelo	WVC80N	DCS-6620g	211W
Estándares	IEEE 802.3u, 802.3, 802.11g, 802.11b, borrador 802.11n	IEEE 802.3u, 802.3, 802.11g	802.11g, 802.11b
Resolución	640 x 480 pixeles	352 x 240 @ 30fps / 704 x 480 @ 10fps	640 x 480 hasta 160 x 120 píxeles a través de API.
Detección de Movimiento	SI	SI	SI
RF (EIRP) en dBm	802.11b: 18 dBm (típico) @ 11Mbps 802.11g: 16 dBm (típico) @ 54Mbps 802.11n:15dBm (normal) a 65Mbps (HT20), 135Mbps (HT40)	802.11g: 15 dBm +/- 2 dB @ 54Mbps	14 a 17 dBm medida sin ganancia de antena
Sensibilidad de recepción en dBm	802.11b:-87dBm (típico) @ 11Mbps 802.11g:-72dBm (típico) @ 54Mbps 802.11n:-70dBm (típico) @ MCS7,-65dBm (típico) @ MCS7	-----	-90 dBm a 1Mbps
Ganancia de antena	1.5 dBi	2 dBi	1.5 dBi
Seguridad Wi-Fi	WEP, WPA, Wi-Fi Protected Access 2 (WPA2)	WPA-PSK Y WPA-TKIP	WEP, WPA, Wi-Fi Protected Access 2 (WPA2), 802.1x.
Campo de visión	61,2 grados	5 a 65 grados	27 a 67 grados horizontal
Formato de compresión	MPEG-4 parte 2 y MJPEG	MPEG-4 y MJPEG	MJPEG MPEG-4 Parte 2 con estimación del movimiento

Movilidad	NO	Si (Pan/Tilt)	NO
Tamaño	90 x 120 x 37 mm	107 x 107 x 135 mm	44 x 88 x 200 mm
Exterior	NO	NO	SI (El paquete viene con carcasa incluida)
Garantía	1 año	1 año	1 año
Precio	$190	$1,313.10 a $1,670.62	$ 699

Los 3 equipos cumplen con las características mínimas establecidas, se escoge la WVC80N debido a su precio, sus características de radio frecuencia (sensibilidad de recepción y potencia de transmisión) y el soporte técnico de esta marca es más accesible. Cabe recalcar que ninguna de las cámaras comparadas están listas para exteriores debido a su alto precio.

2.7.4 CENTRAL DE MONITOREO

En la tabla 2.9 se enlista las características principales de tres equipos:

Acer 4520, Sony VPCEA 35FL y una Dell 14R-CIBL.

Tabla 2.9 Comparación de las centrales de monitoreo.

Marca	**Acer**	**Sony**	**Dell**
Modelo	Aspire 4520	VPCE A 35FL	14R-CI5BL
Sistema Operativo	Windows XP sp3	Windows 7 HP	Windows 7 HP
Tipo de procesador	Amd Turion 64	Intel core i3	Intel core i5
Velocidad Procesador	2.2 GHz	2.4 GHz	2.53 GHz
Memoria RAM	1 GB	3 GB	4 GB
Capacidad Disco Duro	500 GB	500 GB	500 GB
Tarjeta de red inalámbrica	802.11 b/g	802.11 b/g	802.11 b/g
Monitor	14”	14”	14”
Garantía	1 año	1 año	1 año
Precio	$ 660	$ 1030.40	$ 1106.56

Los tres equipos cumplen con los requerimientos necesarios para el sistema, se eligió la primera opción debido a que la tarjeta de red inalámbrica en estos modelos tiene mayor sensibilidad respecto a otros, además de que su costo en el mercado es menor.

Cabe recalcar que se puede usar cualquier computadora que cumpla con las mínimas características establecidas y no necesariamente una portátil, ya que en el mercado se encuentran adaptadores inalámbricos USB y PCI que pueden adaptarse sin problema al sistema de video vigilancia.

CAPÍTULO 3. DISEÑO Y PRUEBAS DEL SISTEMA

3.1 INTRODUCCIÓN

En el presente capítulo se presenta el diseño, la implementación y las pruebas respectivas del sistema de video vigilancia utilizando Wi-Fi para el conjunto residencial “El Prado”.

El capítulo abarca los cálculos teóricos del enlace radio-eléctrico con los datos técnicos específicos de los equipos seleccionados en el capítulo anterior, además de su ubicación dentro del conjunto y el detalle de la configuración de cada uno de los equipos.

En el capítulo anterior se eligieron los equipos que cumplen con los parámetros y requerimientos del sistema, por lo que en este capítulo se determina la mejor ubicación de los equipos y se realiza la implementación del sistema de video vigilancia.

Como punto inicial tenemos la gran necesidad de aumentar la seguridad de los condóminos, para lo cual se ubican los equipos en lugares estratégicos sin que estos interfieran en las actividades cotidianas de los condóminos y sin invadir la privacidad de cada uno de ellos.

Las principales ventajas de implementar un sistema inalámbrico respecto a un cableado en el conjunto residencial “El Prado” son:

- Escalabilidad: Tiene mayor facilidad de crecimiento que un sistema de cableado estructurado.

- Flexibilidad: Existe la posibilidad de cambiar de lugar los equipos, sin causar mayores problemas.

- Se disminuyen tiempos y costos de instalación.

3.2 CÁLCULOS TEÓRICOS DEL ENLACE RADIO-ELÉCTRICO

A continuación se desarrolla el cálculo teórico, con los datos técnicos específicos de los equipos seleccionados en el capitulo anterior, para determinar la distancia teórica (alcance) de la red inalámbrica. Cabe recalcar que se usa la menor sensibilidad de recepción de los equipos, en este caso de las cámaras IP inalámbricas.

$$P_{Tx} - \propto_{Tx} + G_{Tx} - FSL + G_{Rx} - \propto_{Rx} - margen \geq Sensibilidad_{Rx}$$

$$24\ dBm - 0 + 10dBi - FSL + 1.5dBi - 0 - 15dBm \geq -72dBm$$

$$24dBm + 10dBi - FSL + 1.5dBi - 15dBm = -72dBm$$

$$FSL = 92{,}5dB$$

$$FSL = 20\log_{10} f(MHz) + 20\log_{10} D(Km) + 32{,}45\ [dB]$$

$$92{,}5dB = 20\log_{10}(2417) + 20\log_{10} D + 32{,}45$$

$$log_{10} D = -0{,}3807766$$

$$D = 0{,}416124[Km]$$

$$\boldsymbol{D = 416.12[m]}$$

Siendo la zona de cobertura aproximadamente 200 metros, se concluye que los equipos seleccionados son los adecuados ya que cubren la zona de cobertura del sistema de video vigilancia.

3.3 UBICACIÓN DE LOS EQUIPOS

Una vez demostrado teóricamente que los equipos seleccionados son los adecuados para cubrir los parámetros y requerimientos del sistema, y que estos cubren la zona de cobertura procedemos a ubicar los equipos en el conjunto.

El Access Point se colocará en la mitad del conjunto para que la señal radio-eléctrica cubra la zona del mismo en su totalidad, el lugar elegido presenta facilidades de instalación y una visión total del conjunto.

El Access Point se colocará en la fachada de una casa del conjunto, se escogió esta casa ya que desde el punto donde se colocará el Access Point se tiene las siguientes ventajas:

- Está en la mitad del conjunto,
- Línea de vista directa a la casa comunal y a la garita del guardia (inicio y fin del conjunto),
- La casa tiene conexión a Internet.

Por el momento se colocará una sola cámara en el conjunto debido a que el cliente quiere probar el sistema de video vigilancia solo con una cámara para posteriormente estudiar la posibilidad de colocar más cámaras en el conjunto.

Ya que los cálculos teóricos demuestran que las cámaras pueden colocarse en cualquier parte del conjunto, el criterio para la ubicación de estas será:

- Porcentaje de visión que cubre del conjunto,
- Línea de vista directa con el Access Point,
- Parte del conjunto que el guardia no visualiza.

La cámara se colocará en el punto más alejado del conjunto, esto es en la casa comunal, esta cámara cubrirá las fachadas de las casas que se encuentran al final del conjunto.

La central de monitoreo se ubicará en la garita, ya que el guardia es el encargado de la seguridad del conjunto.

3.4 IMPLEMENTACIÓN

El sistema de video vigilancia implementado en el conjunto tiene un radio aproximado de 100 metros medidos desde la mitad del conjunto en donde se colocó el punto de acceso, la cámara IP inalámbrica se encuentra colocada a la misma distancia al final del conjunto, mientras que la central de monitoreo se encuentra a 77 metros aproximadamente del punto de acceso como se ilustra en la figura 3.1.

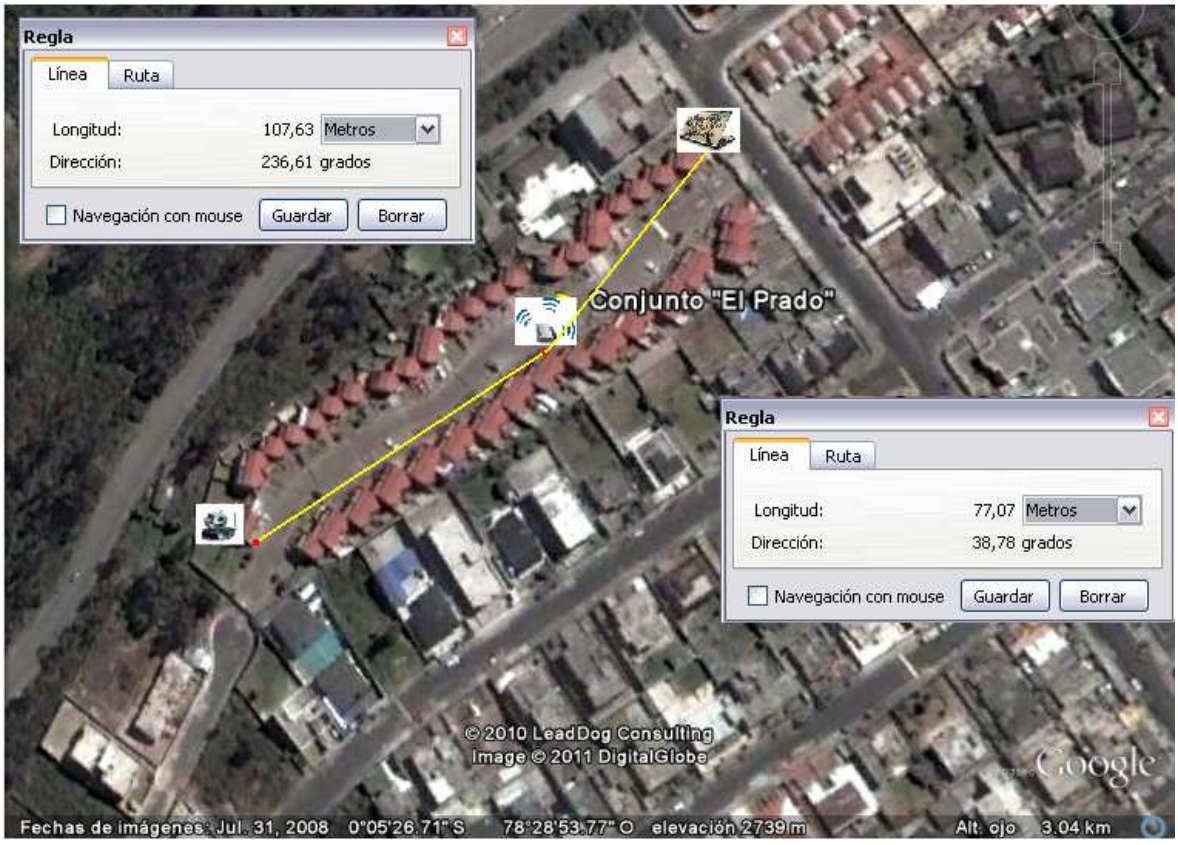


Figura 3.1 Sistema de video vigilancia implementado en el conjunto residencial "El Prado".
Tomada de Google Earth

La central de monitoreo se encuentra en la garita del guardia, el monitoreo se lo realiza mediante una portátil que esta enganchada a la red inalámbrica del sistema de video vigilancia, utilizando el software propio de las cámaras o un software proporcionado por Linksys by Cisco. El almacenamiento se lo realiza en la central de monitoreo, para la grabación de video se usa el software proporcionado por Linksys.

3.4.1 CONFIGURACIÓN DE LOS EQUIPOS

El sistema de video vigilancia esta diseñado como una red de infraestructura siendo el punto de acceso la NanoStation2, el dispositivo EchoLife HG520c trabajando como router y la cámara WVC80N como estación, a continuación se ilustra en la figura 3.2.

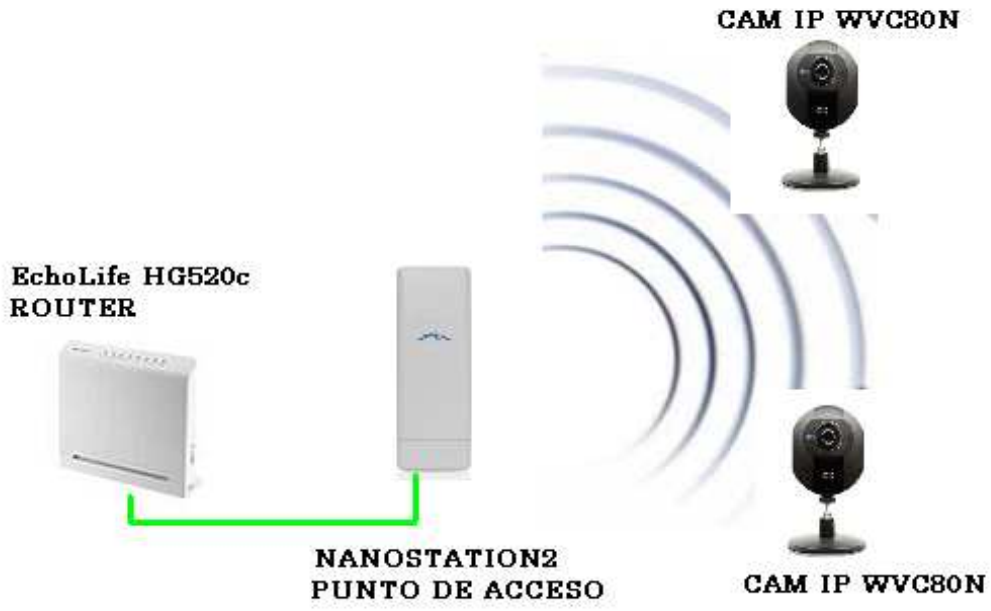


Figura 3.2 Red de Infraestructura

A continuación se muestra paso a paso la configuración de cada equipo para la formación del sistema de video vigilancia:

3.4.1.1 EchoLife HG520c

Este router wireless es proporcionado por la CNT con el plan de Internet y viene configurado de fábrica, simplemente nos cercioramos que asigna direcciones IP de forma dinámica. Su dirección IP por defecto es la 192.168.1.1, el usuario y la clave para ingresar a la configuración es instalador y .coorporación respectivamente como se muestra en la figura 3.3.

Figura 3.3 Usuario y contraseña para el router EchoLife HG520c

3.4.1.2 NanoStation2

Este equipo viene por defecto como estación para sistemas WISP, en este proyecto trabajará como punto de acceso. Para poder ingresar a la configuración del equipo tenemos que colocar direcciones IP estáticas que estén en el rango de trabajo del equipo en la tarjeta de área local como se muestra en la figura 3.4.

Figura 3.4 Direcciones IP estáticas colocadas en la tarjeta de red alámbrica.

La dirección IP por defecto del equipo es la 192.168.1.20, colocamos esta dirección en el browser de nuestro explorador de Internet, aparece una ventana que nos pide usuario y password que por defecto son *ubnt* y *ubnt* como muestra la figura 3.5.

Figura 3.5 Usuario y contraseña de la NanoStation2.

A continuación aparece la página principal de la configuración de la NanoSation2 donde muestra los valores por defecto, en la parte superior están las diferentes pestañas como: Main, Link Setup, Network, Advanced, Services, System.

Para que nuestro equipo trabaje como punto de acceso vamos a la pestaña *Link Setup,* luego en *Wireless Mode* (por defecto está en *Estación*) seleccionamos la opción *Punto de Acceso*, en la siguiente opción *SSID* colocamos el nombre de la red inalámbrica en este caso *CJTO. EL PRADO*.

Para que los cambios queden guardados damos click en *Change* y luego en *Apply*, el procedimiento aquí descrito está ilustrado en la figura 3.6.

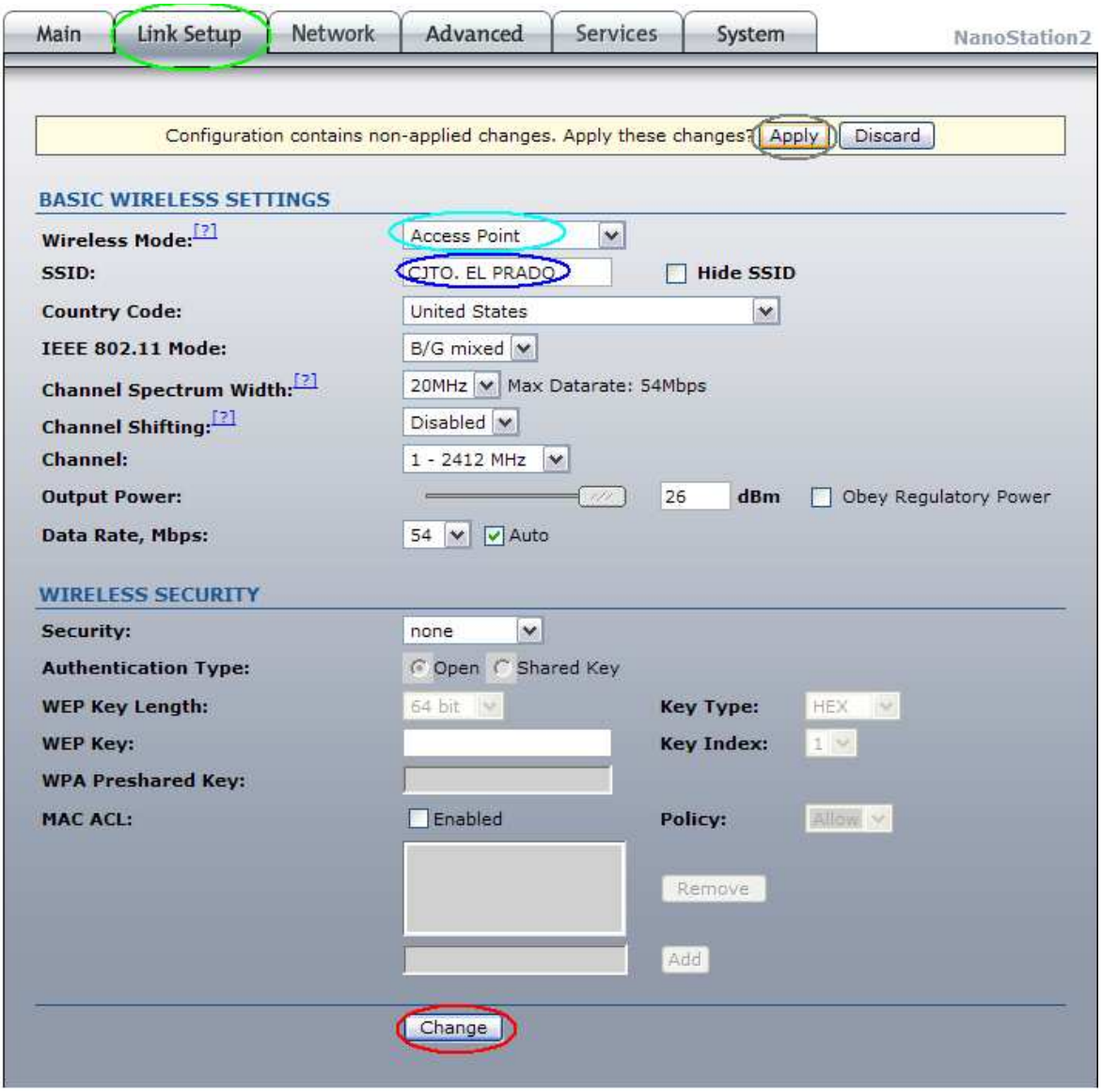


Figura 3.6 Configuración NanoStation2 como punto de acceso.

Luego de que terminen de aplicarse los cambios vamos a la pestaña Network, en Network Settings en la opción Bridge IP Address colocamos por *DHCP*, para que los cambios queden guardados damos click en *Change* y luego en *Apply* como muestra la siguiente figura 3.7.

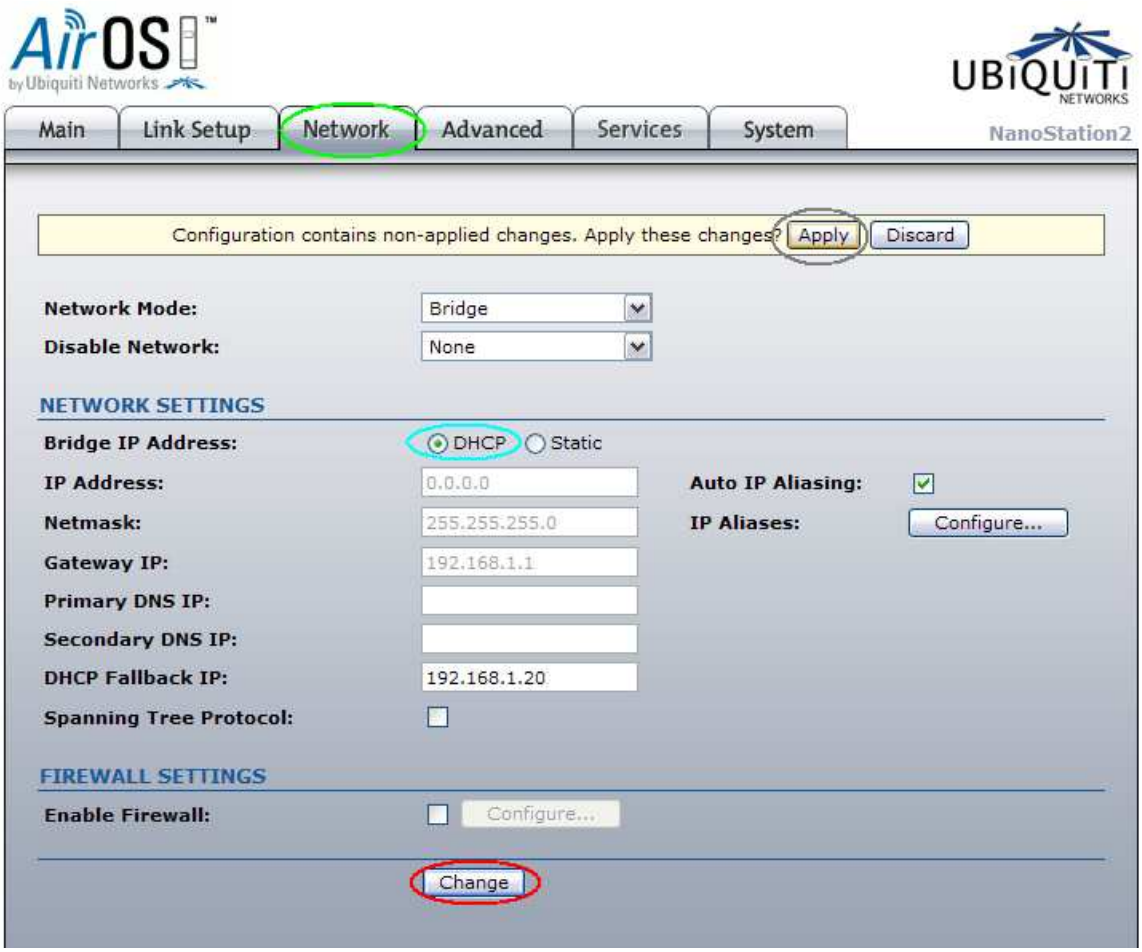


Figura 3.7 Configuración NanoStation2 en modo Bridge.

En este punto nuestra NanoStation2 está configurada como punto de acceso, todas las seguridades de la red se tomarán en un capítulo más adelante.

3.4.1.3 Cámara WVC80N

La configuración de la cámara se realiza mediante un CD de configuración que es proporcionado por Linksys by Cisco, no se la puede configurar de otra manera, no tiene una dirección IP fija por defecto y la dirección IP de la cámara se asigna automáticamente mediante un router.

Para la configuración de la cámara se siguen algunos pasos, de los cuales vamos a describir los más importantes a continuación:

- Primeramente iniciamos la configuración en “Start Setup”.
- Se acepta el contrato de la licencia del software proporcionado por Linksys by Cisco.
- “Setup Wizard” escanea la red y verifica la existencia de otras cámaras en el sistema.
- Conectamos el adaptador de energía y el cable UTP (que vienen incluidos) a los pórticos de energía de la cámara y del router respectivamente como se observa en la figura 3.8.

Figura 3.8 Conexiones de la cámara al router.

- “Setup Wizard” se encarga de encontrar la cámara dentro de la red, este proceso toma pocos minutos.
- Después de detectada la cámara se coloca un Username y un Password para posibles cambios de la configuración en el futuro.
- Se coloca un nombre a la cámara para poder identificarla dentro de la red.

Configuración inalámbrica.

- Se empieza escogiendo la red inalámbrica a la que se va a conectar y se coloca la clave de dicha red.
- Nuevamente el “Setup Wizard” termina la configuración de la cámara, se desconecta los cables de la cámara (de energía y UTP).

- Esperamos 30 segundos y conectamos solamente el adaptador de energía, a partir de este momento la cámara esta lista para su funcionamiento como se muestra en la figura 3.9.

Figura 3.9 Cámara lista para su funcionamiento.

3.4.2 SEGURIDAD DE LA RED INALÁMBRICA

La red inalámbrica denominada “CJTO. EL PRADO” tiene algunas seguridades básicas para evitar intrusiones no autorizadas a la red, a continuación se detallan dichas seguridades.

3.4.2.1 Deshabilitar la difusión del SSID

Esta seguridad permite que solo los que conozcan la existencia de la red y el nombre exacto de la misma puedan ingresar a esta o por lo menos tratar. De esta manera la red esta oculta a terceras personas y nos brinda un buen nivel de seguridad. Para lograr esto simplemente en la configuración del punto de acceso (NanoStation2) se selecciona *Hide SSID* como se muestra en la figura 3.10.

Figura 3.10 Deshabilitar la difusión del SSID.

3.4.2.2 WPA2

Siendo el ultimo mecanismo de seguridad Wi-Fi (por ende más confiable y desarrollado), y ya que la cámara WVC80N soporta este mecanismo, lo implementamos. Para implementar este mecanismo de seguridad nuevamente en el punto de acceso configuramos dicha opción.

En *WIRELESS SECURITY* en la opción *Security* elegimos *WPA2* y en *WPA Preshared Key* colocamos una clave como se muestra en la figura 3.11.

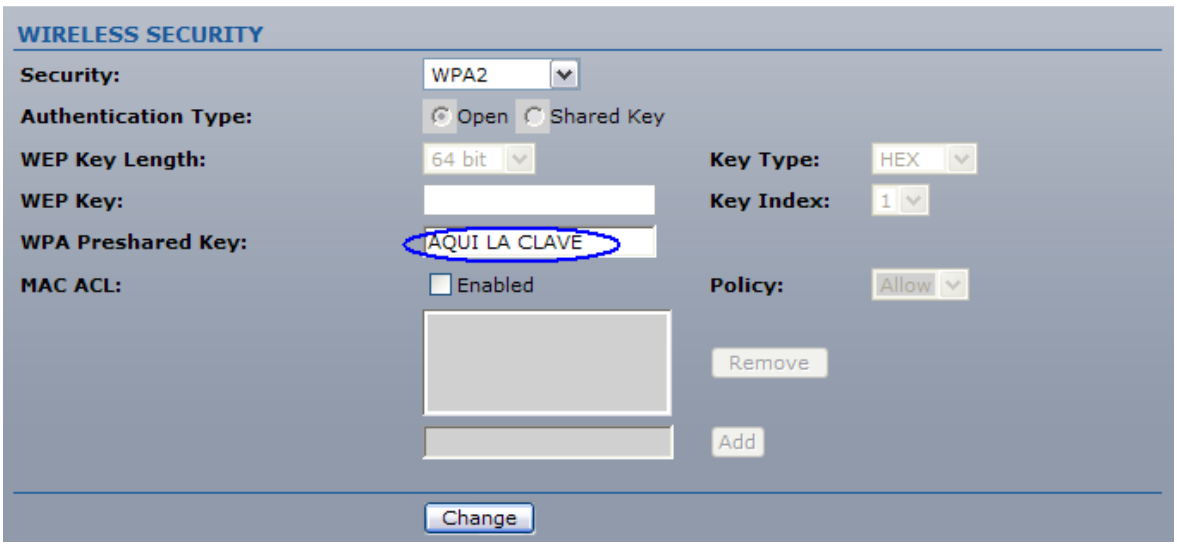


Figura 3.11 Habilitar WPA2.

3.4.2.3 Filtro MAC

En *WIRELESS SECURITY* en la opción MAC ACL programamos el punto de acceso para que acepte dispositivos con direcciones MAC específicas. Simplemente habilitamos la opción MAC ACL y añadimos a la tabla las direcciones MAC de los equipos que se van a poder conectar a la red como muestra la figura 3.12.

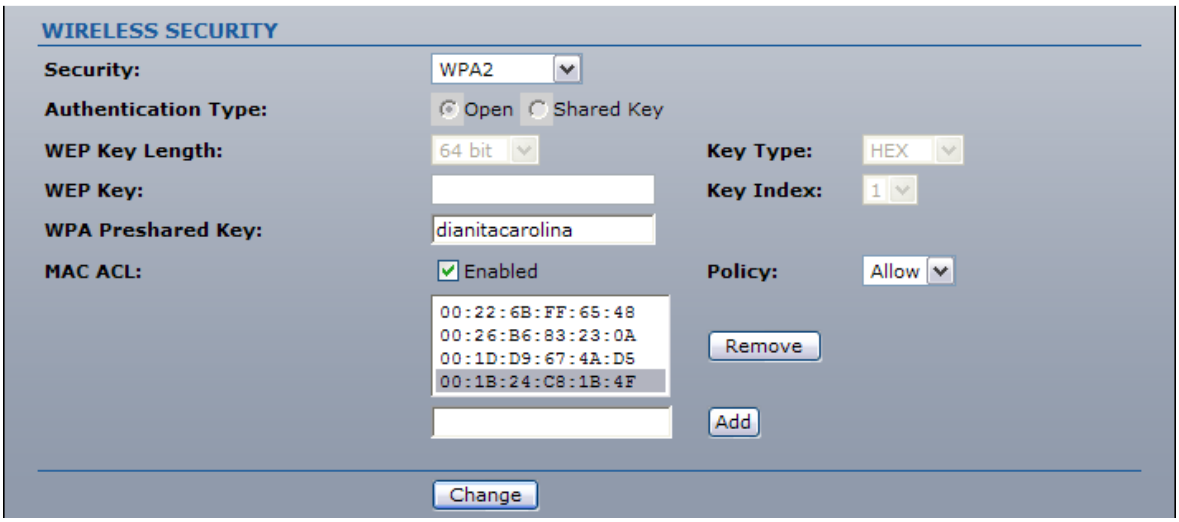


Figura 3.12 Configuración de un Filtro MAC.

3.5 PRUEBAS DEL SISTEMA

Todos los equipos: EchoLife HG520c (00:26:b6:83:23:01), NanoStation2 (00:15:6d:8a:2e:22) y la cámara IP inalámbrica WVC80N (00:22:6b:ff:65:48) se asocian correctamente a la red inalámbrica (Figura 3.13), la cámara IP responde al comando ping como se muestra en la figura 3.14 y 3.15. Los parámetros de la red funcionan correctamente.

Figura 3.13 Tabla arp –a de la red inalámbrica.

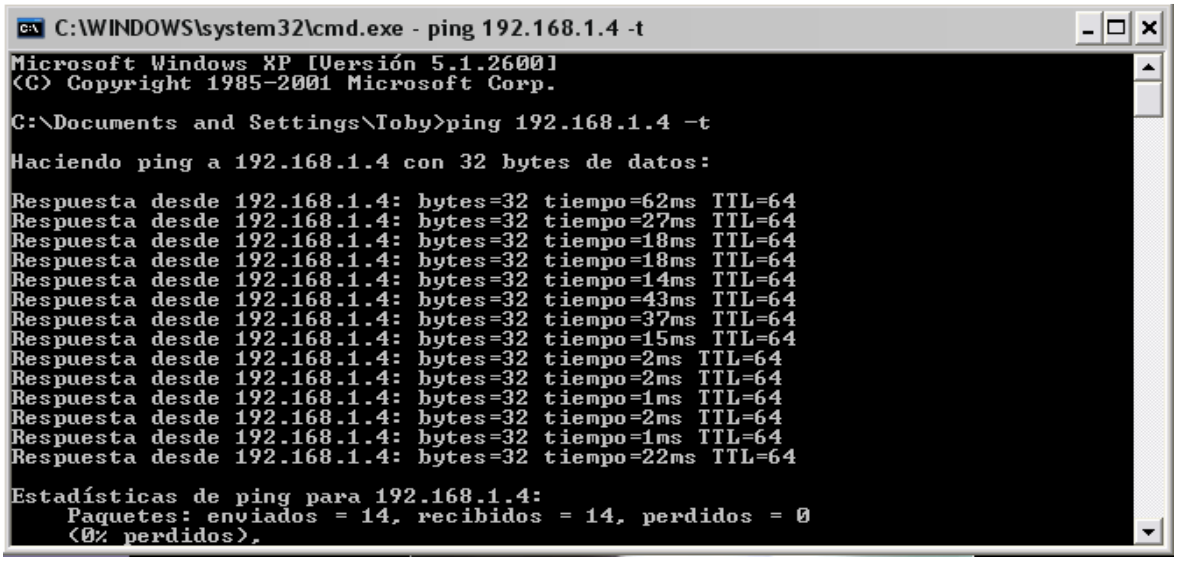


Figura 3.14 Ping a la cámara IP desde la garita del guardia/192.168.1.4

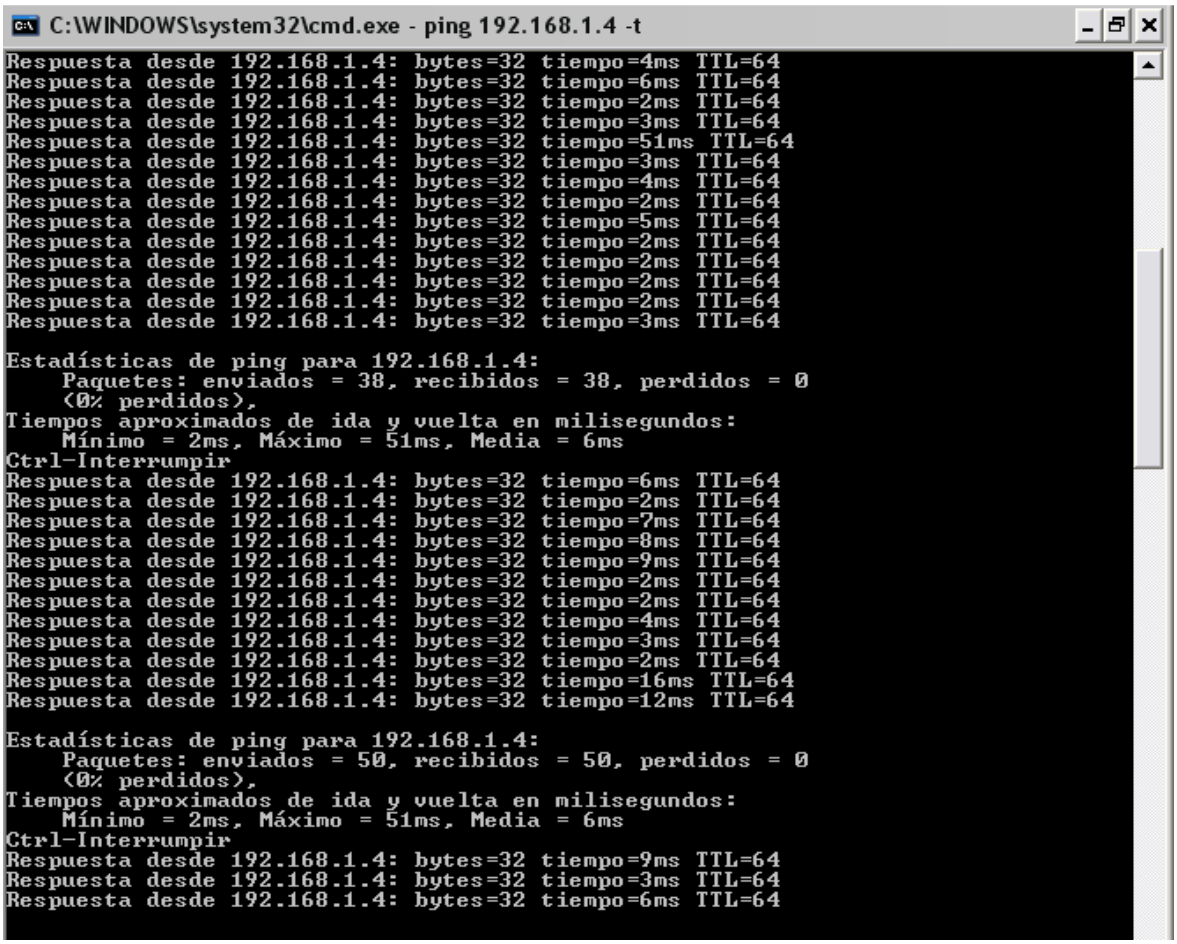


Figura 3.15 Ping extendido a la cámara IP desde la garita del guardia

La respuesta del ping extendido nos da una media de 6ms y 0% de pérdidas, por lo que se concluye que el sistema funciona correctamente.

El sistema de video vigilancia inalámbrico funciona adecuadamente, a continuación se muestran capturas de imagen del sistema de video vigilancia en funcionamiento (Figura 3.16, 3.17 y 3.18):

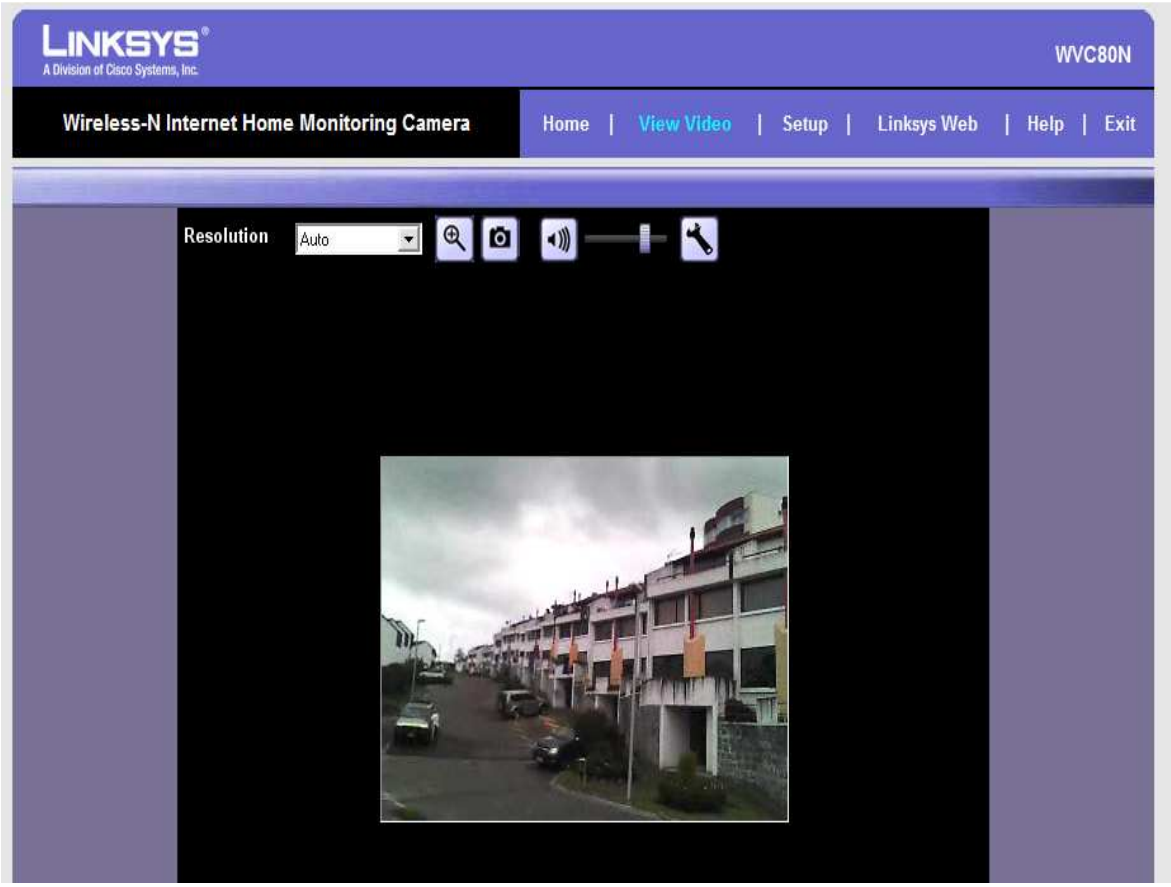


Figura 3.16 Captura del video en tiempo real utilizando Internet Explorer

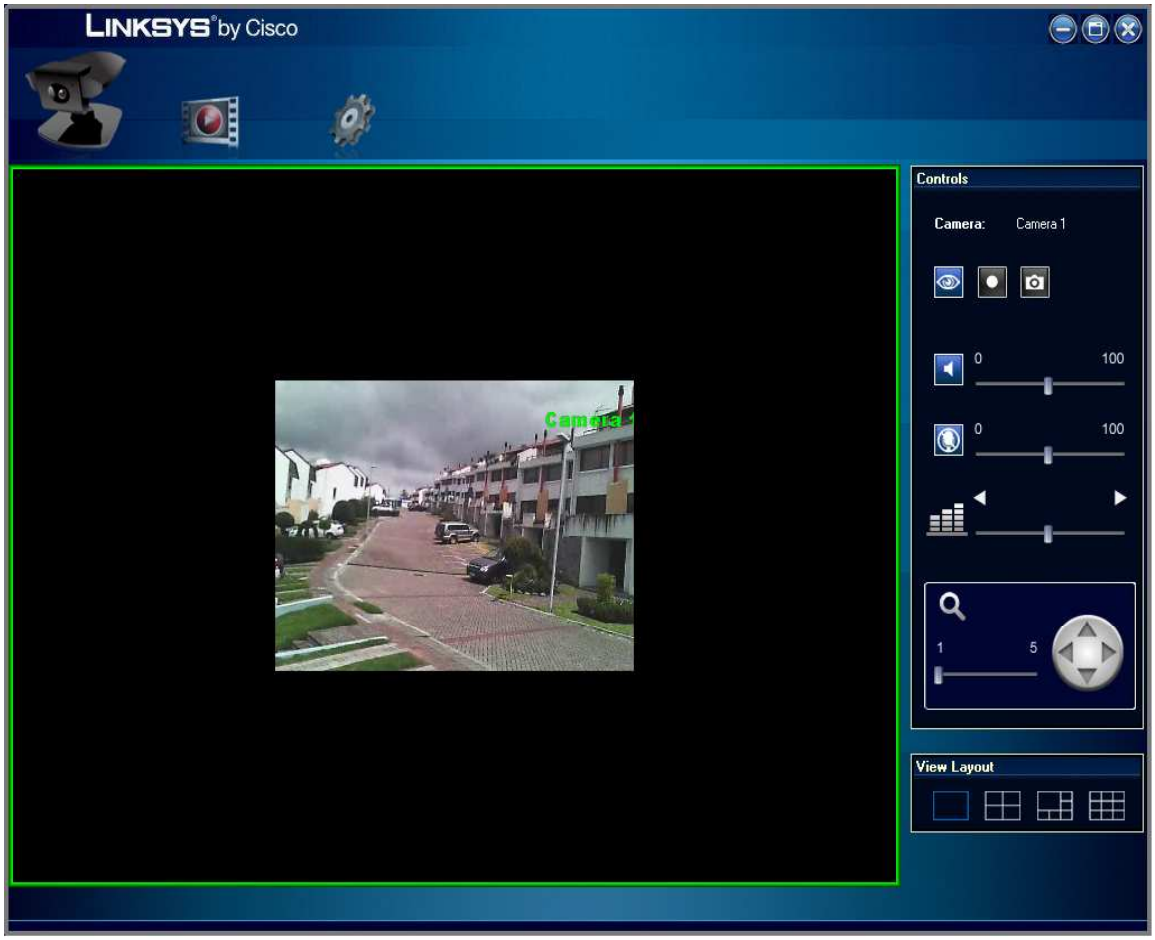


Figura 3.17 Captura del video en tiempo real utilizando el software proporcionado por Linksys.

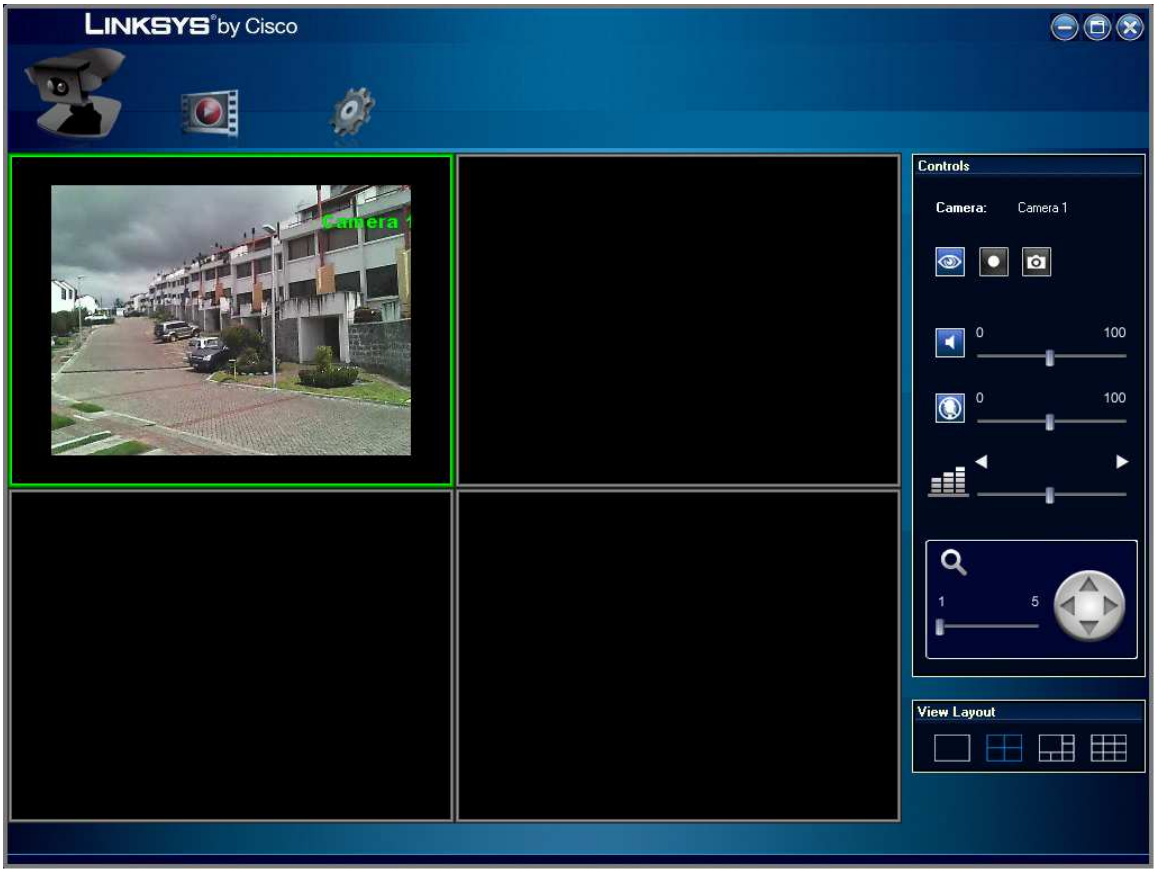


Figura 3.18 Captura del video en tiempo real utilizando el software proporcionado por Linksys.

La tasa de transferencia (Throughtput) del sistema de video vigilancia en la parte WLAN es en promedio de 850 Kbps, este dato se lo obtiene de una herramienta de análisis del equipo NanoStation2 denominada “Show Throughtput”. Esta herramienta visual nos muestra en tiempo real la tasa de transferencia del sistema con una gráfica como se ilustra en la figura 3.19:

Figura 3.19 Tasa de transferencia del sistema de video vigilancia.

CAPÍTULO 4 CONCLUSIONES Y RECOMENDACIONES

En el presente capítulo se presentan las conclusiones y recomendaciones, resultados del desarrollo de la implementación de un sistema de video vigilancia utilizando Wi-Fi, para el conjunto residencial “El Prado”.

4.1 CONCLUSIONES

- Se concluye que el uso de un sistema Wi-Fi es preciso en un espacio abierto de gran tamaño tomando en cuenta todas las ventajas que tiene un sistema inalámbrico respecto a un sistema cableado.

- Podemos concluir que el uso del equipo NanoStation2 mejora la eficiencia del sistema, ya que al tener una mayor potencia de transmisión respecto a otros Access Point consultados y al estar lista para exteriores, el nivel de señal radioeléctrica en el conjunto es excelente.

- Para complementar la anterior, se concluye que el equipo NanoStation2 es excelente para cualquier aplicación Wi-Fi ya que además de lo descrito anteriormente posee una interfaz gráfica bastante intuitiva y fácil de configurar.

- Se concluye que para ampliaciones a futuro del sistema de video vigilancia no habría mayores problemas, ya que los sistemas Wi-Fi presentan una gran facilidad de escalabilidad.

- Los sistemas de video vigilancia desde su aparición no han dejado de$ expandirse, esto ha permitido garantizar una vigilancia continua de zonas estratégicas de un barrio, ciudad, centros comerciales, etc.

- Podemos concluir que siempre que se realice un enlace radioeléctrico se debe considerar un rango de 10 a 15 dbm entre la potencia de recepción y la sensibilidad de recepción debido principalmente a los fenómenos que se podrían suscitar en el medio de transmisión ya sea: climáticos, físicos o de otra índole.

- Se concluye que al realizar un enlace radioeléctrico Wi-Fi (bandas ISM) se debe tomar en cuenta que siempre existe la posibilidad de interferencia debido a un radioenlace en la misma frecuencia.

- Podemos concluir que la principal ventaja de este sistema de video vigilancia respecto a un CCTV es la facilidad de conexión a Internet para poder ver el video en tiempo real desde cualquier parte del mundo.

- Se concluye que los equipos implementados en el sistema de video vigilancia Wi-Fi fueron escogidos tomando en cuenta los parámetros técnicos que se acoplen al sistema y el precio de estos.

- Se concluye que mientras mayor ángulo de visión tengan las cámaras, el número necesario para cubrir el conjunto en su totalidad será menor.

- Podemos concluir que el sistema de video vigilancia ayuda a mejorar el nivel de seguridad del conjunto residencial “El Prado”, por ende mejora la calidad de vida de los condóminos del mismo.

4.2 RECOMENDACIONES

- Se recomienda en primer lugar estudiar el sitio donde se va a implementar el sistema para ubicar puntos estratégicos donde colocar las cámaras y el AP.

- Se recomienda utilizar un AP de más cobertura de la que se va a implementar en el conjunto ya que por diversos obstáculos, esta cobertura se reduce.

- Se recomienda que antes de comprar los equipos se analicen todas las opciones, desde el precio, parámetros técnicos hasta la facilidad de instalación.

- Se recomienda que siempre que se trabaje en alturas se tomen las precauciones pertinentes para evitar accidentes.

- Se recomienda conectar los equipos (en especial el AP) a un cortapicos y/o un regulador de voltaje para evitar daños en los equipos ya sea por sobrecarga eléctrica o por descarga atmosférica.

- Se recomienda antes de configurar la cámara instruirse sobre su manejo para evitar problemas al momento de la configuración de los equipos.

- Se recomienda primeramente configurar la red inalámbrica ya que para la configuración de la cámara necesitamos engancharla a dicha red.

BIBLIOGRAFÍA

Referencias Bibliográficas

- Limehouse Book Sprint Team. “Redes Inalámbricas en Países de Desarrollo”. Segunda edición. Junio 2007.
- Barona, Lorena. “Diseño de un Sistema de Vigilancia basado en Tecnología IP para la Protección de los Condominios la Merced de la Ciudad de Ambato”. Escuela Politécnica Nacional. Facultad de Ingeniería Eléctrica y Electrónica. Electrónica y Redes de Información. Junio 2010.
- Apuntes de WLAN.
- Apuntes de Redes de Computadores.
- Apuntes de Propagación y Antenas.

Direcciones Electrónicas

- http://www.ubnt.com
- http://www.linksysbycisco.com
- http://www.alegsa.com.ar/Dic/direccion%20IP.php
- http://es.wikipedia.org/wiki/Difracci%C3%B3n
- http://es.wikipedia.org/wiki/Zona_de_Fresnel
- http://es.wikipedia.org/wiki/IEEE_802.11
- http://es.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance
- http://www.info-ip.net/ip/Clases-de-direcciones-IP.php
- http://es.kioskea.net/contents/internet/ip.php3
- http://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico
- http://es.wikipedia.org/wiki/Conmutador
- http://www.monografias.com/trabajos17/conectores/conectores.shtml
- http://es.wikipedia.org/wiki/RJ-45

- http://www.mailxmail.com/curso-que-son-redes/direcciones-ip-mascaras-red
- http://es.wikipedia.org/wiki/C%C3%A1mara_IP
- http://www.alegsa.com.ar/Dic/direccion%20IP.php
- http://es.wikipedia.org/wiki/Difracci%C3%B3n
- http://es.wikipedia.org/wiki/Zona_de_Fresnel
- http://es.wikipedia.org/wiki/IEEE_802.11
- http://es.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA2
- http://es.wikipedia.org/wiki/Wired_Equivalent_Privacy
- http://www.lsb.es/imagenes/camarasip.pdf
- http://www.lsb.es/camaras_ip.htm
- http://homestore.cisco.com/en-us/cameras/linskys-WVC80-wirelessn_stcVVproductId84737621VVcatId552009VVviewprod.htm
- http://www.dlink.com/products/?pid=411
- http://www.axis.com/files/datasheet/ds_211w_29838_es_0709_lo.pdf
- http://es.wikipedia.org/wiki/M%C3%A1scara_de_red
- http://www.nextag.com/cisco-aironet-1300/products-html
- http://www.shopbot.com.au/pp-d-link-dcs-6620g-price-25331.html
- http://www.networkwebcams.com/product_info.php?products_id=598

ANEXOS

ANEXO A

SIMULACIÓN DE LA COBERTURA DEL SISTEMA DE VIDEO VIGILANCIA

CTWIFI (Open)
akchot (WEP)
VALDMIESO (WP
PAULINA (WPA)
PUNTONET ESMIL
condado (Open)
RAMOS (WPA)
CJTO. EL PRADO (WPA2)
Conjunto "El Prado"
PUNTONET CONDADO (Open)
dlink (Open)
VILLAS C Y D (Open)
MOLINO (Open)
PUNTONET CONDADO
WIFI-ZONA3 (Open)
NA080810 (WEP)
Vicente (WPA)
796074 (WPA)
Red de Casa (WPA2)
jc_om (WEP)

ANEXO B

CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS

ROUTER HG520c

Figura 2.1 Router HG520c
http://www.huaweidevice.com/worldwide/faq.do?method=searchProduct&directoryId=50&pId=2938

Especificaciones técnicas

Normas	Normas ADSL	• ITU G.992.1 (G.dmt) Anexo A • ITU G.994.1 (G.hs) • ANSI TI.413, Versión 2
	Normas ADSL2	ITU G.992.3 (G.dmt.bis) Anexo A
	Normas ADSL2+	ITU G.992.5 Anexo A
	Normas WLAN	802.11b y 802.11g
Velocidades de transmisión DSL	G.dmt T1.413	• Velocidad downlink máxima: 8Mbit/s • Velocidad uplink máxima: 896 kbit/s
	G.992.5 (ADSL2+)	• Velocidad downlink máxima: 24Mbit/s • Velocidad uplink máxima: 1024 kbit/s
Velocidades	802.11b	1Mbit/s; 2Mbit/s; 5,5Mbit/s; 11Mbit/s.

de transmisión inalámbrica	802.11g	1Mbit/s; 2Mbit/s; 5,5Mbit/s; 6Mbit/s; 11Mbit/s; 12Mbit/s; 18Mbit/s; 24Mbit/s; 36Mbit/s; 48Mbit/s; 54Mbit/s.

Información medioambiental

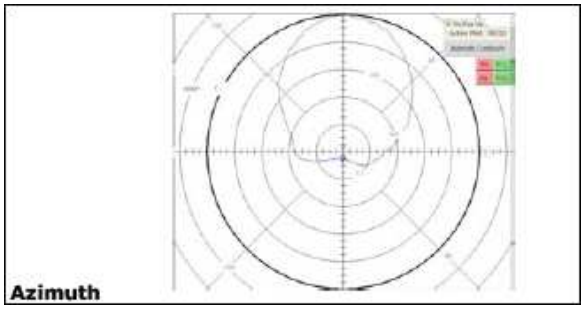
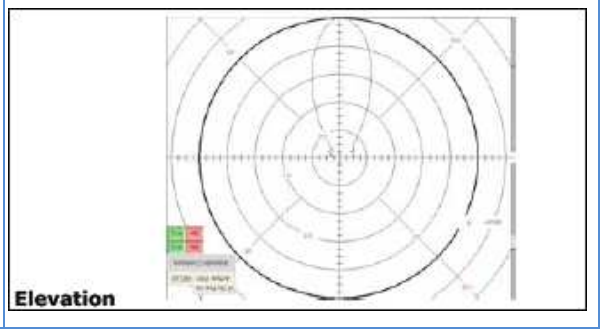
Fuente de Alimentación	12VCC; 0,5A
Consumo de energía	< 6W
Temperatura Ambiente de operación	0ºC a 45ºC
Humedad relativa para funcionamiento de equipo	5% a 95% (sin condensación)
Dimensiones (largo-ancho-profundidad)	164mm-142mm-49mm
Peso	300 gramos aproximadamente

NANOSTATION2 BY UBIQUITI NETWORKS

Figura 2.2 Nanostation2
Tomado de http://www.ubnt.com/nanostation

Especificaciones técnicas

Antena	Integrada 10 dBi

Información de Memoria	16 MB SDRAM, 4 MB flash
Interface de red Ethernet	1 x 10/100 BASE-TX
Estándares Wireless	FCC Part 15.247, IC RS210
Certificación RoHS	Sí
Potencia de Tx	26 dBm ± 2 DBm
Sensibilidad de Recepción	-97 dBm ± 2 DBm
LEDs	Indicadores de ganancia
Rango en Exteriores	Hasta 15 Km
Ancho de Banda TCP/IP	25 Mbps +
Polarización	Multipolarización
Elevación de Ancho de Haz 3 Db	30º
Azimuth	60º
	

Información medioambiental

Máximo Consumo	4 Watts
Fuente	12 V, 1 A
Método de Alimentación	POE
Temperatura de Operación	-20 a 70 º C
Humedad Soportada	5 a 95% condensación
Peso	0.4 Kg
Tamaño	26,4 x 8 x 3 cm
Cubierta	Caja de plástico

WIRELESS-N CAMERA LINKSYS BY CISCO WVC80N

Figura 2.3 Wireless-n Camera WVC80N
Tomado de http://www.linksysbycisco.com/EU/es/products/WRT160N

Especificaciones técnicas

Estándares	IEEE 802.3u, 802.3, 802.11g, 802.11b, borrador 802.11n
Puertos	Ethernet, Energía
Botones	Power, Reset, Wi-Fi Protected Setup
LEDs	Power, Wi-Fi Protected Setup
Tipo de cableado	CAT5
Número de antenas	1
Antena desmontable	No
Máxima Resolución	640 x 480 pixeles
Detección de Movimiento	Sí
Micrófono Incorporado	Sí
Modulaciones	802.11b: CCK / QPSK, BPSK 802.11g: OFDM / BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM / BPSK, QPSK, 16-QAM, 64-QAM

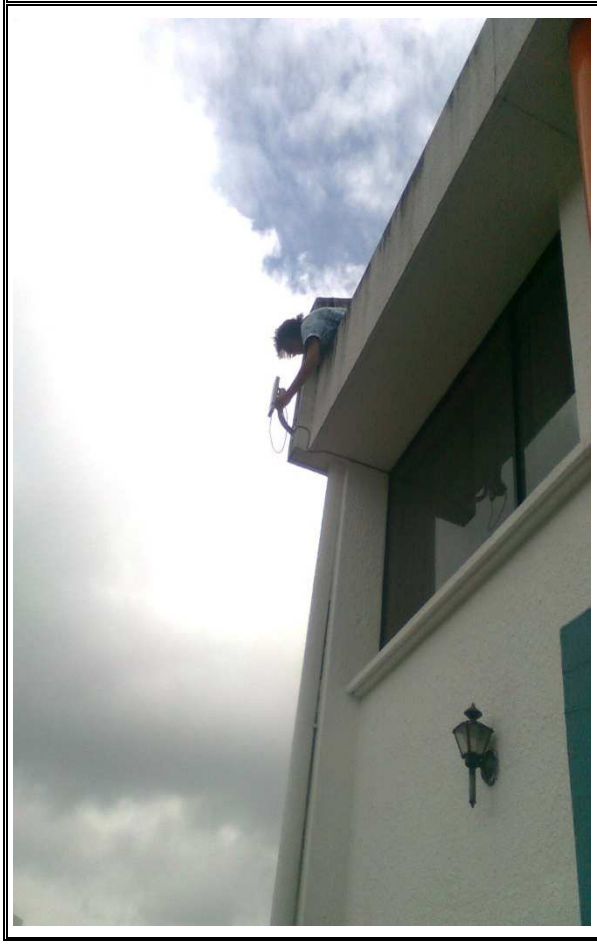
RF (EIRP) en dBm	802.11b: 18 dBm (típico) @ 11Mbps 802.11g: 16 dBm (típico) @ 54Mbps 802.11n:15dBm (normal) a 65Mbps (HT20), 135Mbps (HT40)
Sensibilidad de recepción en dBm	802.11b:-87dBm (típico) @ 11Mbps 802.11g:-72dBm (típico) @ 54Mbps 802.11n:-70dBm (típico) @ MCS7,-65dBm (típico) @ MCS7
Ganancia de antena	1.5 dBi
UPnP able / cert	UPnP Publicidad
Seguridad Wi-Fi	WEP, WPA, Wi-Fi Protected Access 2 (WPA2)
Clave de seguridad de Bits	Hasta 128-bit de encriptación
Requisitos de SO	Windows XP, Vista, Vista 64-bit Edition con las últimas actualizaciones, o Mac OS X 10.4 o superior (para Asistente para la instalación solamente)
Efectivo Focus	50cm a ilimitado
Sensibilidad	6.0V/Lux-sec
Campo de visión	61,2 grados
Formato de compresión	MPEG-4 parte 2 y MJPEG
Registro de Formato de archivo	ASF, AVI
Brillo	Auto / Manual Ajuste

Información medioambiental

Dimensiones	90 x 120 x 37 mm
Peso	130 gr
Alimentación	5V, 1 A
Certificación	FCC, UL/cUL, ICES-003, RSS210, Wi-Fi (IEEE 802.11b/g), WPA2, Wi-Fi Protected Setup
Temperatura de Operación	32 a 95º F – 0 a 35º C
Temperatura de Almacenamiento	-13 a 167º F - -25 a 75º C
Humedad de Operación	0% a 90%

ANEXO C

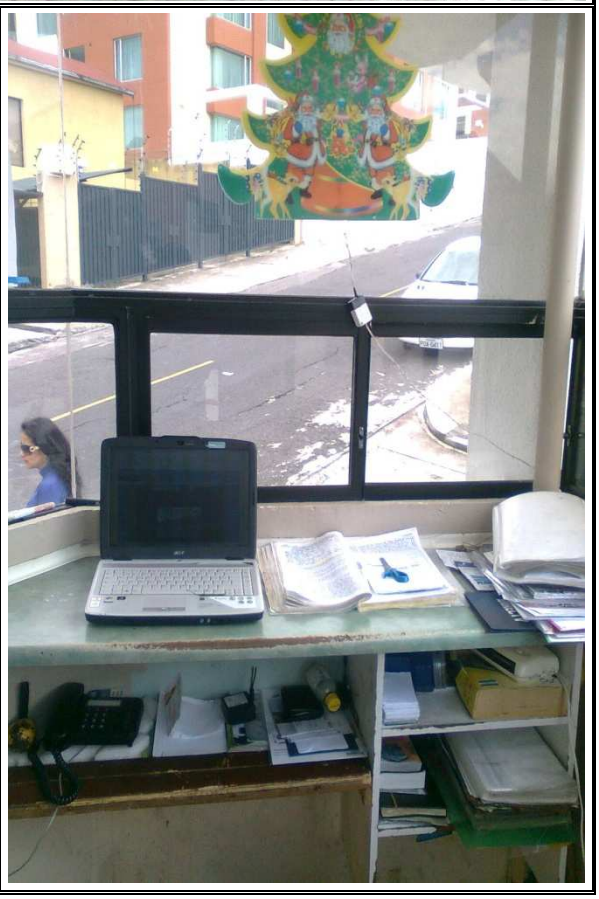
FOTOGRAFÍAS DE LA IMPLEMENTACIÓN




F-4


CISCO


El Prado
CONJUNTO
RESIDENCIAL



GLOSARIO

WPAN: Wireless Personal Area Network

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WiMAX: Worldwide Interoperability for Microwave Access

IEEE: Institute of Electrical and Electronics Engineers

LMDS: Local Multipoint Distribution Service

WWAN: Wireless Wide Area Network

UMTS: Universal Mobile Telecommunications System

GSM: Sistema Global para las Comunicaciones Móviles (*Groupe Spécial Mobile)*

GPRS: General Packet Radio Service

ISM: Industrial, Scientific and Medical

CSMA/CA: Carrier Sense Multiple Access/ Collision Avoidance

IBSS: Independent Basic Service Set

BSS: Basic Service Set

SSID: Service Set Identifier

ESS: Extended Service Set

OSI: Open Systems Interconnection

MAC: Media Access Control

MAC ACL: Media Access Control Acknowledgment

DSSS: Direct Sequence Spread Spectrum

OFDM: Orthogonal Frequency Division Multiplexing

FCC: Federal Communications Commission

ETSI: European Telecommunications Standards Institute

CCK: Complementary Code Keying

DRS: Dynamic Rate Shifting

MIMO: Multiple Input – Multiple Output

Wi-Fi: Wireless Fidelity

WAP: Wireless Access Point

NAT: Network Address Translation

DHCP: Dynamic Host Configuration Protocol

NIC: Network Interface Card

PCI: Peripheral Component Interconnect

PCMCIA: Personal Computer Memory Card International Association

UTP: Unshielded Twisted Pair

FTP: Foiled Twisted Pair

STP: Shielded Twisted Pair

ScTP: Screened Twisted Pair

SsTP: Screened Shielded Twisted Pair

RMS: Root Mean Square

RJ: Registered Jack

TIA: Telecommunications Industry Association

EIA: Electronic Industry Association

IP: Internet Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

WEP: Wired Equivalent Protocol

RC4: Rivest Cipher 4

WPA: Wi-Fi Protected Access

TKIP: Temporal Key Integrity Protocol

PSK: Pre-Shared Key

ICANN: Internet Corporation for Assigned Names and Numbers

IANA: Internet Assigned Numbers Authority

ADSL: Asymmetric Digital Subscriber Line

JPEG: Joint Photographic Experts Group

MPEG-4: Moving Picture Experts Group

M-JPEG: Motion - Joint Photographic Experts Group

CCTV: Circuito Cerrado de Televisión

PAL: Phase Alternating Line

NTSC: National Television System Committee

PoE: Power over Ethernet

EIRP: Equivalent Isotropic Radiated Power

ITU: International Telecommunication Union

ANSI: American National Standards Institute

PPP: Point-to-Point Protocol

PPPoE: Point-to-Point Protocol over Ethernet

PPPoA: Point-to-Point over ATM

ATM: Asynchronous Transfer Mode

RFC: Request for Comments

USB: Universal Serial Bus

UL: Underwriters Laboratories

RSS: Radio Standards Specification

ASF: Advanced Systems Format

AVI: Audio Video Interleave