UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

PROYECTO SEGURIDAD CCTV

INFORME TÉCNICO POR EXPERIENCIA PROFESIONAL

CALIFICADA PARA OPTAR EL TITULO DE INGENIERO ELECTRÓNICO

PRESENTADO POR

GINO ALEXANDER CARRIL ALVAREZ

LIMA- PERU

2013

AGRADECIMIENTO. Mi agradecimiento a mis padres, a mis hermanos, a mi esposa y a mis hijos por el apoyo incondicional que me dan. También agradezco a la Universidad por darme los conocimientos integrales para enfrentarnos a la vida. Gino Carril

INDICE

CAPÍTULO I. INTRODUCCIÓN

La Universidad Nacional de Tumbes reconoce la necesidad de fortalecer la Seguridad de sus Instalaciones mejorando, el Control y la Vigilancia, con el fin de garantizar en lo posible la Protección de sus Bienes, equipo y personas.

Las medidas adoptadas actualmente para la protección del Campus son básicas careciendo de tecnología para su labor efectiva.

El proyecto aborda la problemática de Seguridad con un enfoque moderno y amplio incorporando la instalación en el Campus de un circuito cerrado de televisión implementado por etapas como pieza básica, que integrado a otros equipos y materiales de última generación, ayudaran a mejorar la calidad de las acciones de control y vigilancia del Campus facilitando al personal encargado de la seguridad un conjunto de medios destinados a optimizar su desempeño y ofrece a las autoridades universitarias el acceso remoto al sistema con el fin de supervisar la marcha del servicio en tiempo real.

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 que sea, la video vigilancia inalámbrica es líder debido a las ventajas que se 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 pueda 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 II. MARCO TEÓRICO

1. ANTECEDENTES

La Universidad Nacional de Tumbes Proyecta la Implementación de un Sistema de Video Vigilancia, para reforzar los servicios de seguridad y control de sus instalaciones, en tiempo real de diferentes puntos al interior del Campus y áreas de influencia externa. Para el desarrollo del presente proyecto, se elaboró una línea base de condiciones de seguridad y Riesgo, información que permite definir de manera general la futura ubicación de las cámaras así como los requisitos técnicos del equipamiento necesario.

Actualmente la Universidad no cuenta con equipos electrónicos de vigilancia, alarmas u otros medios que ayuden en la conservación de sus activos.

Durante el trabajo de campo no se observó la aplicación de normas de control para el ingreso de personas, y vehículos al interior de las instalaciones situación que genera condiciones de riesgo.

Debemos adicionar al panorama descrito las condiciones del entorno vecino:

a) El Campus está localizado dentro de una zona de expansión urbana rodeado por AAHH. con escasa vigilancia policial.

b) De manera general podemos señalar tanto en el ámbito externo como interno se destaca la existencia de condiciones que favorecen la comisión de actos delictivos contrarios a los intereses de la Universidad, las posibilidades de reducir dicha exposición requieren de medios que permitan la observación permanente

delCampus hecho que justifica la incorporación de un sistema de video vigilancia complementario a los procedimientos adoptados para la seguridad del lugar.

2. OBJETIVOS

2.1 Objetivo General.

Dotar a la Universidad de un Sistema integrado de Seguridad y Video Vigilancia para ser implementado por etapas destinado a reducir los niveles de vulnerabilidad y Riesgo Delincuencial de las instalaciones equipos y materiales.

2.2 Objetivos Específicos:

Implementar un sistema de Vigilancia, capaz de operar bajo las condiciones físicas y ambientales adversas imperantes en el lugar.

Disponer la ubicación de las cámaras sustentado en un estudio de línea base de Seguridad..

Reducir la vulnerabilidad de las instalaciones y equipos de la universidad ante la Acción delincuencial y los siniestros.

Permitir a las Autoridades de la universidad realizar la supervisión remota del sistema vía Web, mediante código secreto de acceso.

2.3 SOPORTE TEÓRICO REDES INALAMBRICAS

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 medios de ondas electromagnéticas. La transmisión y recepción se realizan a través de antenas.

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 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)

- MDS (Local Multipoint Distribution Service).

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).

REDES DE ÁREA LOCAL INALÁMBRICAS (WLAN)

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. En la figura 1 se aprecia la evolución de las WLAN teniendo en cuenta su frecuencia, velocidad, tipos de red

Evolución de la WLAN

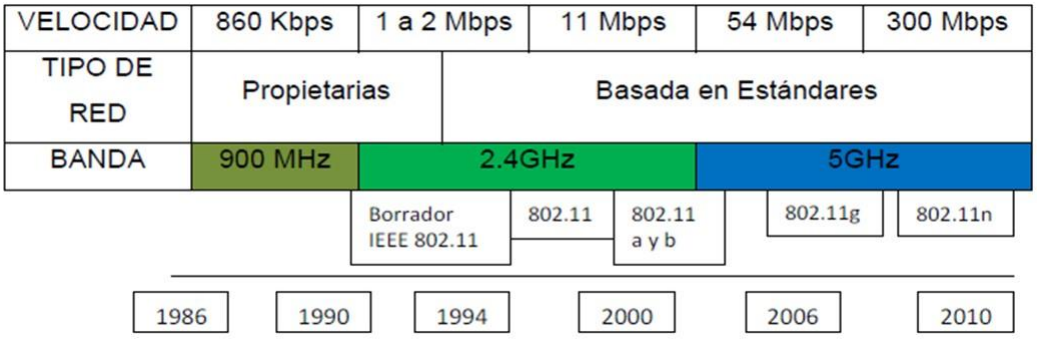


Figura 1 –Evolución de la Wlan

INTRODUCCION A Wi-Fi (802.11)

[La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). **Wi-Fi** (que significa "Fidelidad inalámbrica", a veces incorrectamente abreviado WiFi) es el nombre de la certificación otorgada por la Wi-Fi Alliance, anteriormente WECA (Wireless Ethernet Compatibility Alliance), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11. Por el uso indebido de los términos (y por razones de marketing) el nombre del estándar se confunde con el nombre de la certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11].[3] [En la práctica, Wi-Fi admite ordenadores portátiles, equipos de escritorio, asistentes digitales personales (PDA) o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11 Mbps o superior) dentro de un radio de varias docenas de metros en ambientes cerrados (de 20 a 50 metros en general) o dentro de un radio de cientos de metros al aire libre. El estándar 802.11 establece los niveles inferiores del modelo OSI para las conexiones inalámbricas que utilizan ondas electromagnéticas, como se visualiza en la tabla 1, por ejemplo:

- La capa física (a veces abreviada capa "PHY") ofrece tres tipos de codificación de información.
- La capa de enlace de datos compuesta por dos subcapas: **control de enlace lógico** (**LLC**) y **control de acceso al medio** (**MAC**).

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red

Capa de enlace de datos (MAC)	802.2
	802.11
Capa física (PHY)	DSSS FHSS Infrarrojo

Estándares de 802.11 - Tabla 1

Cualquier protocolo de nivel superior puede utilizarse en una red inalámbrica Wi-Fi de la misma manera que puede utilizarse en una red Ethernet].[3]

[Los distintos estándares Wi-Fi . Ver tabla 2

Nombre estándar	**Nombre**	Descripción
802.11a	WifiF	El estándar 802.11 (llamado WiFi 5) admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mpbs).
802.11b	Wifi	El estándar 802.11 es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mpbs (6 Mpbs en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres
802.11c	Combinación del 802.11 y el 802.1d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar
802.11d	Internacionalizació	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según
802.11e	Mejora de la	El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la *capa de enlace de datos*. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión
		El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el *protocolo IAPP* que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso
		El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mpbs en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g
802.11h		El estándar *802.11h* tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la *h* de 802.11h) y cumplir con las regulaciones

802.11i		El estándar *802.11i* está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el *AES* (estándar de cifrado avanzado) y
802.11Ir		El estándar *802.11r* se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j		El estándar *802.11j* es para la regulación japonesa lo que el 802.11h es para la regulación europea.

Estándares de WiFi - Tabla 2

También es importante mencionar la existencia de un estándar llamado "*802.11b+*". Éste es un estándar patentado que contiene mejoras con respecto al flujo de datos. Por otro lado, este estándar tiene algunas carencias de interoperabilidad debido a que no es un estándar IEEE.

Rango y flujo de datos

Los estándares 802.11a, 802.11b y 802.11g, llamados "estándares físicos", son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos. Ver tabla 3

Estándar	**Frecuencia**	**Velocidad**	**Rango**
WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2,4 GHz	11 Mbit/s	100 m
WiFi G (802.11b)	2,4 GHz	54 Mbit/s	100 m

Rango de flujo de datos - Tabla 3

802.11a El estándar 802.11 tiene en teoría un flujo de datos máximo de 54 Mbps, cinco veces el del 802.11b y sólo a un rango de treinta metros aproximadamente. El estándar 802.11a se basa en la tecnología llamada OFDM (*multiplexación por división de*

frecuencias ortogonales). Transmite en un rango de frecuencia de 5 GHz y utiliza 8 canales no superpuestos. Es por esto que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de "**banda dual**". Ver tabla 4

Velocidad hipotética (en	**Rang**
54 Mbit/s	10 m
48 Mbit/s	17 m
36 Mbit/s	25 m
24 Mbit/s	30 m
12 Mbit/s	50 m
6 Mbit/s	70 m

802.11a - Tabla 4

802.11b El estándar 802.11b permite un máximo de transferencia de datos de 11 Mbps en un rango de 100 metros aproximadamente en ambientes cerrados y de más de 200 metros al aire libre (o incluso más que eso con el uso de antenas direccionales). Ver tabla 5

Velocidad hipotética	**Rango**	**Rango (al aire libre)**
11 Mbit/s	50 m	200 m
5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

802.11b - Tabla 5

g El estándar 802.11g permite un máximo de transferencia de datos de 54 Mbps en rangos comparables a los del estándar 802.11b. Además, y debido a que el estándar 802.11g utiliza el rango de frecuencia de 2.4 GHz con codificación OFDM, es compatible con los dispositivos 802.11b con excepción de algunos dispositivos más antiguos. Ver tabla 6].[3]

Velocidad	Rango (en ambientes	Rango (al aire
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

802.11g - Tabla 6

Elementos de una WLAN

Antena

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 está 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).

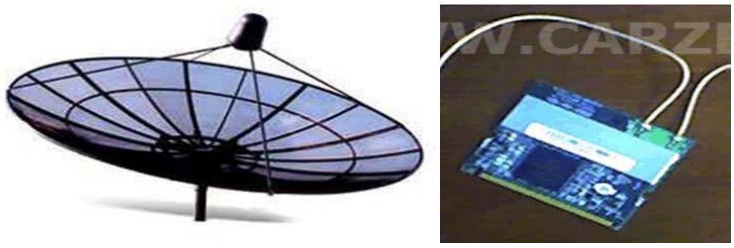
Polarización.- Es la orientación del campo eléctrico radiado por la antena, es la orientación física del elemento de la antena que emite la energía de RF.

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 2 se ilustran una antena parabólica y una tarjeta de red inalámbrica.



[Antena Parabólica – Tarjeta de red]..[7]

Figura 2

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 3 se muestran algunos AP`s.

[Access Point]..[8]

Figura 3

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 4 se indican algunos de ellos.

[Routers]..[9]

Figura 4

Wireless Router

Un router inalámbrico es un dispositivo que realiza las funciones de un router, pero también incluye las funciones de un AP inalámbrico. Puede funcionar en una red LAN cableada, una red LAN inalámbrica sola, o una mezcla entre red cableada e inalámbrica. Los Wireless Routers realizan las siguientes funciones (Ver figura 5):

- AP (Access Point).
- Switch LAN
- Router
- Proxy server
- DHCP Client
- DHCP Server
- Firewal

[Wireless Router]..[10]

Figura 5

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. Ver figura 6.

[Switches]..[11]

Figura 6

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

ata de red inalámbrica PCMCIA1.[1]

En la figura 7 se ilustra una PCMCIA.

[Tarj2

Figura 7

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 8:

[Cable Coaxial RG-58/U]..[13]

Figura 8

***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 de los cables adyacentes, se ilustra uno de ellos en la siguiente figura 9:

[Cable de Pares Trenzados]..[14]

Figura 9

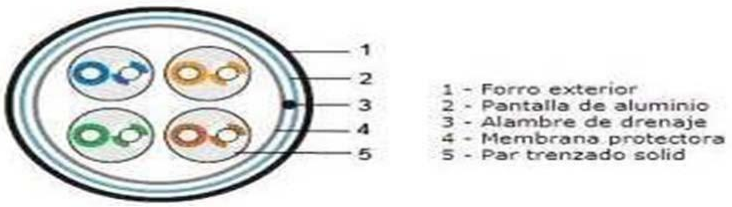
Existen diversos tipos de pares trenzados a continuación se detalla algunos de ellos:

- UTP Unshielded Twisted Pair (Cable de Pares Trenzados No Blindado). Ver tabla 10

[Cable UTP]..[15]

Figura 10

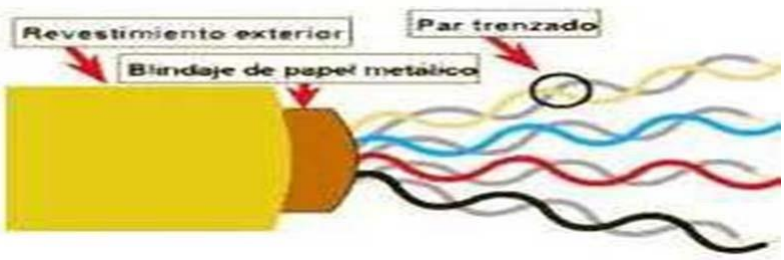
- FTP Foiled Twisted Pair (Cable de Pares Trenzados Apantallado). Ver figura 11



[Cable FTP]..[16]

Figura 11

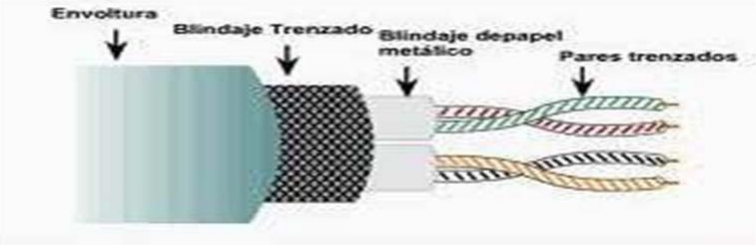
- STP Shielded Twisted Pair (Cable de Pares Trenzados Blindado). Ver figura 12



[Cable STP]..[17]

Figura 12

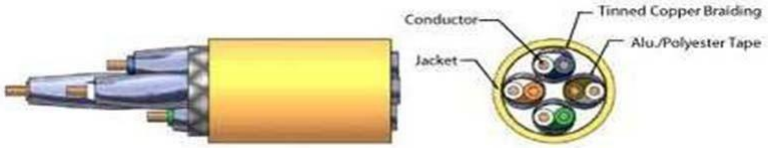
- ScTP Screened Twisted Pair. Se ilustra en la figura 13 :



[Cable ScTP]..[18]

Figura 13

- SsTP Screened Shielded Twisted Pair. Se ilustra en la figura 14:



[Cable SsTP]..[19]

Figura 14

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

Conectores N corrugados:

- Impedancia: 50Ω
- 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. Ver figura 15

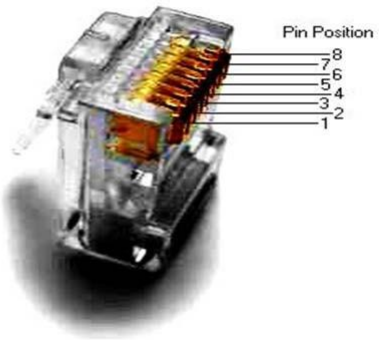
[Conector Macho Conector Hembra]..[20]

Figura 15

Conectores RJ-45 macho y hembra

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). Ver figura 16

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)	

Conectores RJ45 (Diagrama) - [Figura 16]..[21]

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.

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* 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. Siendo la principal razón que es muy fácil "hackear" una red protegida por WEP. A continuación en la figura se ilustra el Escenario WEP.

[Escenario WEP]..[22]

Figura 17

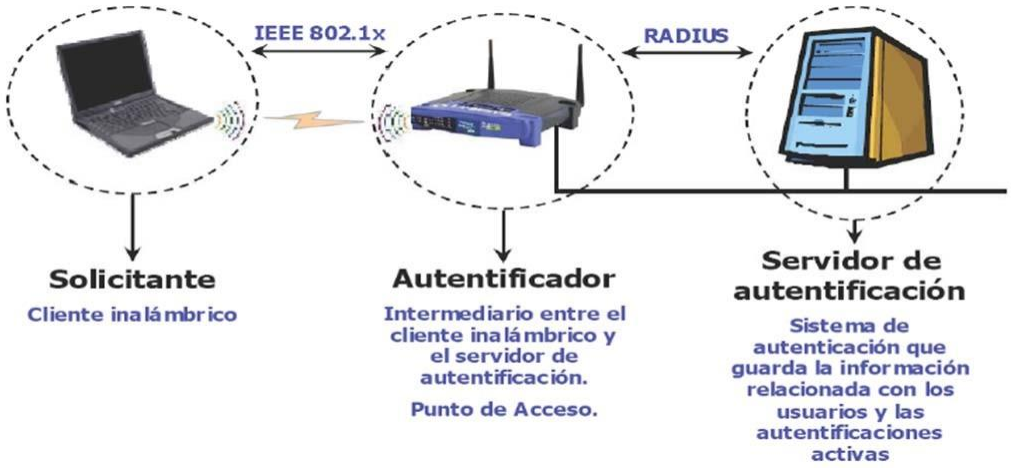
WPA/WPA2 (Wi-Fi Protected Access)

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 se ilustra en la figura 18 el Escenario WPA.



[Escenario WPA]..[23]

Figura 18

DIRECCIONAMIENTO IP

[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.

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. Ver tabla 7

CLASES DE				
Clase de Red	1er Byte	Máscara	Total de	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	

Clases de redes - Tabla 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". Ver tabla 8

Clase A - Tabla 8

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". Ver tabla 9

Clase B - Tabla 9

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". Ver tabla 10

110	Xxxxx	Xxxxxxxx	Xxxxxxxx	Xxxxxxxx
Red				Computadoras

Clase C - Tabla 10

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.

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.]…[24]

CÁMARAS IP

[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.]…[25]

CAPÍTULO III. DESARROLLO DEL PROYECTO

3.1 DESARROLLO DEL PROYECTO

El proyecto se destina a la instalación de un sistema de video vigilancia , que abarque la totalidad del área del campus de la Universidad, el cual se implementará por etapas incluyendo las zonas edificadas, el cerco perimétrico interno, y áreas libres del terreno, señalando la ubicación de cámaras para su instalación progresiva de acuerdo a los módulos que se detallaran más adelante el proyecto incluye además la instalación de otros medios electrónicos de seguridad tales como: Cerco eléctrico, sensores, alarmas locales y a distancia, y el equipamiento básico del personal de seguridad.

3.2 PROCESO DE IMPLEMENTACION DEL PROYECTO

La implementación del Circuito Cerrado de Televisión se deberá iniciar, con un grupo de cámaras en puntos críticos destinadas a brindar cobertura perimétrica y control de acceso al Campus Universitario, además de controlar el área de parque y las vías principales de tránsito peatonal y vehicular.

La implementación requiere ser completada con la señalización del campus y las disposiciones administrativas necesarias para el uso adecuado del sistema.

3.3 ACCESO A LA INFORMACIÓN

La información generada por el sistema de video vigilancia en forma de imágenes es almacenada en un disco duro por periodos de tiempo definido. Además la supervisión

de imágenes se podrá realizar de manera remota accediendo al sistema vía internet, PC o teléfono celular, mediante el empleo de una clave secreta de acceso.

3.4 INGENIERIA DEL PROYECTO

El proyecto considera la Instalación de cámaras de video vigilancia dispuestas en diferentes puntos del Campus universitario con el propósito de mejorar la seguridad del lugar.

El sistema deberá contar con una sala de control ubicada en un ambiente en el edificio del rectorado desde este lugar se tendera una red alámbrica hasta los puntos de cámaras. Complementado con un circuito de alarma sonora y pulsadores de alarma a distancia.

El tendido de la red alámbrica está previsto para la instalación futura de un mayor número de cámaras.

Proceso de implementación del sistema:

1. Trazado y replanteo del plano de ubicación de cámaras y tendido de redes del sistema.
2. Localización de los puntos donde se deberán instalar las cámaras las que podrán ser del tipo fijas o móviles de acuerdo a la necesidad del lugar.
3. Montaje de las cámaras e integración al software.

4. Simulacros y puesta a punto de los equipos.

3.5 COMPONENTES DEL SISTEMA. SALA DE CONTROL

Ambiente de 25 m2 mínimo con electricidad y punto de acceso a Internet.

La sala deberá contener 02 monitores LSD de 39”, Servidor , switcher de acometida para 24 entradas, central de alarma.

El sistema debe permitir el control por Internet.

RED ALAMBRICA

Instalación de cableado de comunicación (coaxial) entre la sala de control y los puntos de cámaras. Dicho cableado será conducido por ductos y de manera aérea apoyada al sistema de postes de iluminación, instalando postes nuevos en los puntos que lo requieran.

Deben estar dotadas de un dispositivo para el registro de las condiciones climáticas y ambientales del lugar.

ALARMA LOCAL SONORA VISUAL (12V)

Del tipo sirena electrónica de tono variado (100W) operado desde diferentes estaciones y central de control de 8 zonas (alámbrico ,pulsadores del tipo botón anti pánico).

ALARMA A DISTANCIA.

La señal de alarma se transmite a través de Internet o línea telefónica dedicada, la señal es registrada en dispositivo instalado en el punto de destino (PNP,CBP) y en la sala de Control del Campus.

CARACTERÍSTICAS MÍNIMAS DE LOS EQUIPOS

Pantalla LCD 39" alta Definición.

Domos de cámaras móviles día y noche mínimo 0,1 Lux y housing para protección de cámaras.

Cámaras fijas día y Noche mínimo 0,1 Lux y housing para protección de cámaras. Software de operación, control, monitoreo, respaldo y grabación.

Equipos de última generación.

Software de Centro de Control que permita conectar Cámaras de Seguridad y controlar sus funciones, así como mover las Cámaras, ver las grabaciones y grabar en equipo remoto.

Búsqueda y Reproducción. Permitir realizar búsqueda y Visualizar tanto en el equipo DVR como remotamente las grabaciones por Fecha/Canal/Archivo horario y cámaras que se deseen.

Acceso remoto vía Web. Permitir visualizar y controlar movimiento remoto de las cámaras, sin Necesidad de instalar software especial.

Extracción y backups (USB o DVD) .Debe considerar la exportación a algunos medios tales como memorias USB, disco Duro USB o DVD.

Visualización de Cámaras

Debe permitir disponer de diferentes presentaciones de Cámaras de Seguridad en pantalla, modo ventana o pantalla completa.:

– 1 cámara – 2 cámaras – 4 cámaras – 8 cámaras

3.6 DISTRIBUCION E INSTALACION DE CAMARAS. Instalación Por Módulos Etapas.

El número de cámaras requeridas para el lugar está relacionado con el Avance constructivo y de ocupación de los espacios. Además del nivel de exposición a posibles Riesgos Identificados tales como. Amenaza de Intrusión, Robos, daños a la propiedad, incendios etc. Para garantizar la efectiva aplicación del sistema las cámaras se instalarían por etapas. Con el fin de Avanzar de manera progresiva de un sistema de Vigilancia Humana, a un Sistema de video Vigilancia.

Las cámaras se instalaran en espacios Abiertos definidos como Exteriores. E interiores para lugares Cerrados o de acceso restringido.

Para definir la correcta ubicación de las cámaras se aplican diferentes criterios de valoración de los lugares a vigilar destacando:

- Lugares peligrosos. Tales como; Vías de Accesos, Muro perimétricos, Patios Estacionamientos
- Lugares con Contenido valioso; Libros, Documentos Computadoras etc.
- Lugares con contenido peligroso; Insumos químicos, Combustibles etc.

Datos generales

El proyecto considera la instalación de cámaras Analógicas y digitales trabajando en red Alámbrica. Todas las cámaras estarán provistas de lentes para trabajar en condiciones de escasa iluminación (0.1 Lux) Filtro de Corte IR, Compresión H.264.CMOS (Para utilización en ambientes de luz cambiante.

Las cámaras estarán provistas de Carcasas herméticas para protegerlas de las inclemencias del clima así como de seguros anti vandálicos.

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.

CAPÍTULO IV. CÁLCULOS DE INGENIERÍA

ZONA DE COBERTURA DEL SISTEMA DE VIDEO VIGILANCIA

La Universidad tiene desde una de las Facultades hacia el otro extremo aproximadamente 200 metros de largo como muestra la siguiente figura 19:

Zona de cobertura del sistema de video vigilancia.

Tomada de Google Earth

Figura 19

ANCHO DE BANDA

El ancho de banda teórico a utilizar, sin formato de compresión y sin tomar en cuenta el tamaño real de bits a transmitirse. 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.

1 $! (\text{Imágenes}) = 24 \frac{\text{bits}}{\text{pixel}} \text{ X } 337920 \text{ pixeles} = 8110080 \frac{\text{bits}}{\text{Imagen}}$

2 $R =! (\text{imagen}) \text{ X frecuencia}$

3 $R = 8110080 \frac{\text{bits}}{\text{Imagen}} \text{ X } 10 \frac{\text{Imágenes}}{\text{Segundo}} = 81{,}1\text{Mbps}$

4 $AB_{1 \text{ cámara}} = 81, 11\text{Mbps}$

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.
- El número de cámaras.

Las técnicas de compresión actualmente más utilizadas son Motion JPEG y MPEG- 4.

Por medio de la compresión se puede reducir el tamaño del archivo con una afectación mínima en la calidad de la imagen. A continuación se muestra en la tabla

11 algunos valores típicos de compresión de una imagen promedio realizada por una cámara AXIS.

Nivel de Compresión vs. Resolución.

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

DATOS REFERENCIALES DE LA CAMARA AXIS

Nivel de Compresión vs. Resolución - **Tabla 11**

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:

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:

5 $$\#\text{ de tramas} = \frac{\text{Tamaño de la aplicación}}{\text{Datos útiles de la trama Ethernet}}$$

6 $$\#\text{ de tramas} = \frac{28KB}{1460bytes}$$

7 $$\#\ \text{de tramas} = 19{,}63$$

8 $$\#\ \text{de tramas} = 19$$

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

9 $$\text{Sobrecarga total} = \#\ \text{de tramas} \times \text{Sobrecarga trama Ethernet}$$

10 $$\text{Sobrecarga total} = 19 \times 66\ \text{bytes}$$

11 $$\text{Sobrecarga total} = 1254\ \text{bytes}$$

3) Cálculo de los datos totales transmitidos:

12 $$\text{Datos totales transmitidos} = \text{Tamaño de la aplicación} + \text{Sobrecarga total}$$

13 $$\text{Datos totales transmitidos} = 28\ \text{Kbytes} + 1254\ \text{bytes}$$

14 $$\text{Datos totales transmitidos} = 28000\ \text{bytes} + 1254\ \text{bytes}$$

15 $$\text{Datos totales transmitidos} = 29254\ \text{bytes} = 234{,}032\text{Kbits} = 234032\ \text{bits}$$

4) Cálculo del ancho de banda real:

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

16 $$AB_{1\ CAMARA} = \frac{234{,}032\text{Kbits}}{1\ \text{imagen}} \times 10\ \frac{\text{imágenes}}{\text{segundo}}$$

17 $$AB_{1\ CAMARA} = 2{,}34\ Mbps$$

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

10 $$AB\ SISTEMA = AB_{1\ CAMARA} \times 6\ CAMARAS = 14{,}04\ Mbps$$

11 $$AB\ SISTEMA = 14{,}04\ Mbps$$

El ancho de banda que se manejará en el sistema será de aproximadamente 14 Mbps.

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.(Datos tomados de la tabla de Nivel de Compresión vs. Resolución) Para el cálculo de la Capacidad de almacenamiento se siguen los siguientes pasos:

1. Se determina la capacidad de almacenamiento por hora.

Capacidad por hora = Tamaño de imagen X # de imágenes

12 $$\text{Capacidad por hora} = \frac{13\ KB}{imagen} \times \frac{10\ imágenes}{segundo} \times \frac{3600\ seg}{1\ hora}$$

21 $$\text{Capacidad por hora} = 468\ \frac{MB}{hora}$$

2. Se determina la capacidad por día.

22 $$\text{Capacidad por día} = \frac{468}{\frac{MB}{hora}} \times 24\ \frac{horas}{dia}$$

23 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 X #días a grabar

24 Capacidad = 11232 MB X 7 días

25 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:

26 Capacidad total del sistema = Capacidad de una cámara X # cámaras Capacidad total del

sistema = 78624 MB X 6 cámaras

27 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 X 1.2

28 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.

PARÁMETROS DEL SISTEMA DE VIDEO VIGILANCIA

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 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.

Las cámaras serán ubicadas estratégicamente de manera que no invadan la privacidad de las personas que habitan en el conjunto. El software debe permitir la visualización y grabación del video en tiempo real.

CÁLCULOS TEÓRICOS DEL ENLACE RADIO-ELÉCTRICO

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

Margen = Potencia de Transmisión [dBm] – **Pérdidas en el cable TX** [dB] + Ganancia de Antena TX [dBi] - **pérdida en la trayectoria del Espacio Abierto** [dB] + Ganancia de Antena RX [dBi]- **Pérdida de Cable RX** [dB] - **Sensibilidad del receptor** [dBm]

$$P_{Tx} - 0C_{Tx} + G_{Tx} - FSL + G_{Rx} - 0C_{Rx} - margen = Sensibilidad_{Rx}$$

33 $24\ dBm - 0 + 10dBi - FSL + 1.5dBi - 0 - 15dBm = -72dBm$

34 $24dBm + 10dBi - FSL + 1.5dBi - 15dBm = -72dBm$

35 $FSL = 92,5dB$

36 $FSL = 20\log_{10} f(MHz) + 20\log_{10} D(Km) + 32,45\ [dB]$

37 $92,5dB = 20\log_{10}(2417) + 20\log_{10} D + 32,45$

38 $\log_{10} D = -0,3807766$

39 $D = 0,416124[Km]$

40 $D = 416.12[m]$

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.

CAPÍTULO V. REFERENCIAS

REFERENCIAS

1. **http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica.**
2. **http://es.wikipedia.org/wiki/Wi_fi.**
3. **http://es.kioskea.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi.**
4. **https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP.**
5. **http://www.axis.com/es/products/video/about_networkvideo/bandwidth.htm.**
6. **http://www.google.com.pe/url?sa=t&rct=j&q=calculos%20de%20radioenlace**
7. **http://www.telali.com.pe/destino/antena.gif**
8. **http://arfes.ircfast.com/group/view/kl40615/Driver_Acer_WarpLink_Access_Point**
9. **http://www.techfuels.com/general-networking/3483-routers.html**
10. **http://narowalonline.com/?p=17881**
11. **http://www.phoenixcontact.es/productos/21718_21733.htm**
12. **http://www.tecnomaniacos.com/shop/?mod=cat&cat_id=12**
13. **http://www.afsoncable.com/rg58-cable.htm**
14. **http://redesadsi.wordpress.com/clasificacion-de-las-redes/**
15. **http://www.videovigilancia.com.mx/ventaonline/index.php?id_categoria=32**
16. **http://www.btech.cl/pro.php?id=201224**
17. **http://www.alfinal.com/Temas/cableadoestructurado.php**
18. **http://www.monografias.com/trabajos30/cableado/cableado.shtml**
19. **http://www.conexplusnet.com/sstp_cable.html**
20. **http://torjaquintero.blogspot.com/2010/04/terminacion-de-cables-utp-y-stp.html**
21. **http://www.consultants-online.co.za/pub/itap_101/html/ch04s05.html**
22. **http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf**
23. **http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf**
24. **http://es.kioskea.net/contents/267-direccion-ip**
25. **http://es.wikipedia.org/wiki/C%C3%A1mara_IP**

GLOSARIO

802.11

802.11, o IEEE 802.11, es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN). 802.11 se compone de distintas normas que operan a diferentes frecuencias, con distintas velocidades y capacidades.

AES (Advanced Encryption Standard).

Algoritmo de encriptación del gobierno de EE.UU, basado en el algoritmo Rijndael, método de encriptación simétrica con clave de 128 bits desarrollada por los belgas Joan Daemen y Vincent Rijmen.

Access Point (AP, Punto de Acceso).

Estación base o "base station" que conecta una red cableada con uno o más dispositivos wireless.

Existen muchos tipos de Access Point en el mercado, con diferentes capacidades: bridge, hubs, gateway, router, y las diferencias entre ellos muchas veces no están claras, porque las características de uno se pueden incluir en otro. Por ejemplo, un router puede hacer bridge, y un hub puede hacer switch.

Además, los Access Points pueden mejorar las características de la WLAN, permitiendo a un cliente realizar roaming entre distintos AP de la misma red, o compartiendo una conexión a Internet entre los clientes wireless.

Ad-Hoc, modo.

Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to- peer. Dado que no existe un dispositivo central, las señales pueden ocasionar mayores interferencias reduciendo las prestaciones de la red.

Ancho de banda (Bandwidth).

Fragmento del espectro radioeléctrico que ocupa toda señal de información.

Asociación, servicio de.

Servicio del protocolo 802.11 que asocia un cliente wireless a un Punto de Acceso.

Autentificación.

Proceso de identificación de un equipo o usuario. El estándard 802.11 define dos métodos de autentificación: open system y shared key.

Bluetooth.

Tecnología desarrollada para la interconexión de portátiles, PDAs, teléfonos móviles y similares a corta distancia (menos de 10 metros) con una velocidad máxima de 11Mbps a la frecuencia ISM de 2'4 GHz.

Bridge.

Dispositivo que conecta dos segmentos de red que emplean el mismo protocolo de red (por ejemplo, IP) pero con distintos medios físicos (por ejemplo, 802.11 y 10baseT).

BSSID, Basic Service Set Identification.

Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo Ad-Hoc.

Clave de encriptación.

Conjunto de carácter se utilizan para encriptar y desencriptar la información que se quiere mantener en privado. El tipo de clave y la forma de emplearla depende del algoritmo de encriptación que se utilice.

Cliente, o dispositivo cliente.

Cualquier equipo conectado a una red y que solicita servicios (ficheros, impresión, etc) de otro miembro de la red. En el caso de las WLAN, se suele emplear para referirse a los adaptadores

que proporcionan conectividad a través de la red inalámbrica, como tarjetas PCMCIA, PCI o USB, que permiten al equipo acceder a la red.

Decibelios, dB.

Unidad logarítmica empleada habitualmente para la medida de potencias. Se calcula multiplicando por diez el resultado del logaritmo en base 10 de la potencia (en watios): $10 * \log_{10}(W)$. También puede usarse como medida relativa de ganancia o pérdida de potencia entre dos dispositivos.

Decibelios isotrópicos, dBi.

Valor relativo, en decibelios, de la ganancia de una antena respecto a la antena isotrópica. Cuanto mayor sea este valor, más directividad tiene la antena y más cerrado será su ángulo de emisión.

DHCP, Dynamic Host Configuration Protocol.

Protocolo para la configuración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan parámetros de configuración.

Dipolo, antena.

Antena de baja ganancia (2.2 dBi) compuesta por dos elementos, normalmente internos, cuyo tamaño total es la mitad de la longitud de onde de la señal que trata.

Directividad.

Capacidad de una antena para concentrar la emisión en una determinada región del espacio. Cuanto más directiva sea la antena, se obtiene un mayor alcance a costa de un área de menor cobertura.

Diversidad.

Un equipo puede utilizar varias antenas distintas para mejorar la calidad en la recepción de la señal, al aprovechar las mejores características de cada una para cada situación.

DSSS, Direct Sequence Spread Spectrum.

Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en el uso de bits de redundancia.

Espectro radioeléctrico.

El espectro radioeléctrico es toda la escala de frecuencias de las ondas electromagnéticas. Considerado como un dominio de uso público, su división y utilización esta regularizado internacionalmente.

ESSID, Extended Service Set Identification.

Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

Ethernet.

Ethernet es el nombre común del estándard IEEE 802.3, que define las redes locales con cable coaxial o par trenzado de cobre.

Existen distintas versiones, desde la original 10Base5 (cable coaxial con 10 Mbps hasta 500 metros), pasando por la 10Base2 (coaxial, 10Mbps, 200m), 10BaseT (par trenzado, 10 Mbps, 100m) y 100BaseT (trenzado, 100Mbps, 100m) conocida como Fast Ethernet, el más utilizado hoy en día en redes locales.

ETSI, European Telecommunications Standard Institute http://www.etsi.org.

Organización europea sin ánimo de lucro para el desarrollo de estándares de telecomunicación, agrupa 699 miembros de 55 países .

FCC, Federal Communication Commision http://www.fcc.gov.

Agencia gubernamental de los EE.UU. para la regularización de las comunicaciones por radio, televisión, cable y satélite.

FHSS, Frequency Hopping Spread Spectrum.

Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en cambios sincronizados entre emisor y receptor de la frecuencia empleada.

Firewall.

Sistema de seguridad que previene el acceso no autorizado a la red, restringiendo la información que entra o sale de la red. Puede ser un equipo o un software instalado en una máquina de uso general.

Gateway.

Dispositivo que conecta a distintas redes entre sí, gestionando la información entre ellas.

Hot Spot.

También conocidos como lugares de acceso público, un Hot Spot es un lugar donde se puede acceder a una red wireless pública, ya sea gratuita o de pago. Pueden estar en cyber-cafes, aeropuertos, centros de convenciones, hoteles, y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados.

Hub.

Dispositivo de red multipuerto para la interconexión de equipos via Eterhnet o wireless. Los concentradores mediante cables alcanzan mayores velocidades que los concentradores wireless (Access Points), pero éstos suelen dar cobertura a un mayor número de clientes que los primeros.

Hz, Hertzios.

Unidad internacional para la frecuencia, equivalente a un ciclo por segundo. Un megahertzio (MHz) es un millón de hertzios; un gigahertzio (GHz) son mil millones de hertzios.

Infraestructura, modo.

El modo de infraestructura es una topología de red inalámbrica en la que se requiere un Punto de Acceso. A diferencia del modo Ad-Hoc, toda la información pasa a través del Punto de Acceso, quien puede además proporcionar la conectividad con una red cableada y controlar el acceso a la propia red wireless.

IEEE, Institute of Electrical and Electronics Engineers (http://www.ieee.org).

Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones. Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

IP, dirección.

Un número de 32 bits que identifica a un equipo a nivel de protocolo de red en el modelo ISO. Se compone de dos partes: la dirección de red, común a todos los equipos de la red, y la dirección del equipo, única en dicha red.

ISM, Industrial, Scientific and Medical band.

Bandas de frecuencias reservadas originalmente para uso no comercial con fines industriales, científicos y médicos. Posteriormente, se empezaron a usar para sistemas de comunicación tolerantes a fallos que no necesitaran licencias para la emisión de ondas.

b y 802.11g operan en la ISM de los 2'4 GHz, así como otros dispositivos como teléfonos inalámbricos y hornos microondas, por ejemplo.

ISO, modelo de red.

La ISO, International Standards Organization (http://www.iso.org), desarrolló un modelo para describir a las entidades que participan en una red. Este modelo, denominado Open System Interconnection (OSI), se divide en 7 capas o niveles, que son:

1. Físico.
2. Enlace.
3. Red.

4. Transporte.
5. Sesión.
6. Presentación.
7. Aplicación.

Con esta normalización de niveles y sus interfaces de comunicación, se puede modificar un nivel sin alterar el resto de capas. El protocolo 802.11 tiene dos partes, una denominada PHY que abarca el nivel físico, y otra llamada MAC, que se corresponde con la parte inferior del segundo nivel del modelo OSI.

Isotrópica, antena.

Modelo teórico de antena consistente en un único punto del espacio que emite homogéneamente en todas las direcciones. Se utiliza como modelo de referencia para el resto de las antenas.

MAC (Media Access Control), dirección.

En las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel

2) en el modelo ISO. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí.

Modulación.

Técnicas de tratamiento de la señal que consiste en combinar la señal de información con una señal portadora, para obtener algún beneficio de calidad, eficiencia o aprovechamiento del ancho de banda.

Multitrayecto (multipath).

Fenómeno que ocurre cuando una señal rebota en las superficies y alcanza el destino final por varios caminos, con efecto positivo o negativo sobre la potencia de señal recibida difíciles de controlar.

Network name, nombre de red.

Identificador de la red para su diferenciación del resto de las redes. Durante el proceso de instalación y configuración de dispositivos wireless, se requiere introducir un nombre de red o SSID para poder acceder a la red en cuestión.

Parabólica, antena.

Antena en forma de disco curvado. Este tipo de antena ofrece la directividad más alta, lo que las hace ideales para enlaces punto a punto a larga distancias.

Omnidireccional, antena.

Antena que proporciona una cobertura total en un plano (360 grados) determinado.

Open System, autentificación.

Método de autentificación por defecto del estándard 802.11, en la que no se realiza ningún proceso de comprobación de identidad; simplemente, se declaran, por lo que no ofrece ninguna seguridad ni control de acceso.

PHY.

Nombre abreviado del nivel más bajo del modelo ISO, el nivel físico, que describe el medio físico en el que se transmite la información de la red.

En el caso de las redes inalámbricas, las normas 802.11 definen el nivel PHY que utilizan, el aire libre, y los parámetros empleados como la velocidad de transmisión, tipo de modulación, algoritmos de sincronización emisor/receptor, etc.

Roaming.

Nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

Router.

Dispositivo de red que traslada los paquetes de una red a otra.

Basándose en las tablas y protocolos de enrutamiento y en el origen y destino, un router decide hacia dónde enviar un paquete de información.

Sensibilidad.

Potencia mínima de señal que el receptor puede transformar correctamente en datos.

Shared Key, autentificación.

Proceso de autentificación por clave secreta. Habitualmente, todos los dispositivos de la red comparten la misma clave.

Spread Spectrum, espectro disperso.

Técnica de trasmisión consistente en dispersar la información en una banda de frecuencia mayor de la estrictamente necesaria, con el objetivo de obtener beneficios como una mayor tolerancia a la interferencias.

SSID, Service Set Identification.

Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.

Dependiendo de si la red wireless funciona en modo Ad-Hoc o en modo Infraestructura, el SSID se denomina ESSID o BSSID.

TKIP, Temporal Key Integrity Protocol.

Algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes wireless. Sus principales características son la renovación automática de la clave de encriptación de los mensajes y un vector de inicialización de 48 bits, lo que elimina el problema del protocolo WEP.

UNII, Unlicensed National Information Infraestructure.

Banda de frecuencia en los 5 GHz reservada por la FCC para las comunicaciones wireless según el estándard 802.11a. No existe una regularización internacional común sobre los aspectos de esta banda y los dispositivos que operan en ella.

Velocidad de transmisión (Throughput)

Capacidad de transmisión de un medio de comunicación en cualquier momento, se suele medir en bits por segundo (bps). Depende de múltiples factores, como la ocupación de la red,

los tipos de dispositivos empleados, etc, y en el caso de redes wireless, se añaden los problemas de propagación de microondas a través de la que se transmite la información.

VPN, Virtual Private Network.

Herramienta de seguridad que permite mantener en privado una comunicación a través de una red pública. Puede ofrecer otros servicios como autentificación de los extremos involucrados, integridad, etc.

War chalking.

Proceso de realizar marcas en las superficies (paredes, suelo, señales de tráfico, etc) para indicar la existencia de redes wireless y alguna de sus características (velocidad, seguridad, caudal, etc).

War driving.

Localización y posible intrusión en redes wireless de forma no autorizada. Sólo se necesita un portátil, un adaptador wireless, el software adecuado y un medio de transporte.

WEP, Wired Equivalent Privacy.

Algoritmo de seguridad, de uso opcional, definido en el estándard 802.11. Basado en el algoritmo criptográfico RC4, utiliza una clave simétrica que debe configurarse en todos los equipos que participan en la red. Emplea claves de 40 y 104 bits, con un vector de inicialización de 24 bits. Se ha demostrado su vulnerabilidad y que su clave es fácilmente obtenible con software de libre distribución a partir de cierta cantidad de tráfico recogido de la red.

Wi-Fi, Wireless Fidelity.

Nombre dado al protocolo 802.11b. Los dispositivos certificados como Wi-Fi son interoperables entre sí, como garantía para el usuario.

Wi-Fi Alliance, también llamada Wireless Ethernet Compability Alliance (WECA) (http://www.wi- fi.org).

Asociación internacional formada en 1999 para certificar la interoperatibilidad de los dispositivos wireless basados en el estándard 802.11, con el objetivo de promover la utilización de dicha tecnología.

WPA, Wi-Fi Protected Access.

Protocolo de seguridad desarrollado por la WECA para mejorar la seguridad de la información en las redes wireless y permitir la autentificación de usuario, puntos débiles del WEP.

PREGUNTAS ADICIONALES

POR QUÉ SE CONSIDERA LA INSTALACIÓN DE CAMARAS ANALOGICAS Y DIGITALES Y NO SOLO DIGITALES

El proyecto contempla la instalación de cámaras Analógicas por: El costo

El ancho de banda a usar.

POR QUÉ CONSIDERA LA INSTALACIÓN DE 6 CÁMARAS Y NO 8, 10 MAS

Se considera la instalación de 6 cámaras y/o más cámaras (pág. 37) para asignar en el sistema el espacio requerido de dicha información.

En el sistema se agrupa 6 cámaras al disco en mención y tratar de no saturar dicho servidor.

QUÉ PERSPECTIVAS DE MEJORA PODRÍA PLANTEAR A SU PROYECTO EN FUTURAS APLICACIONES

La demanda de un sistema de seguridad es útil ya que el nivel de inseguridad que se vive en el país hace posible tener una mayor vigilancia a nuestros locales.

Los sistemas de seguridad también nos ayudan al campo tecnológico a verificar que está pasando con nuestros equipos (prevención de accidentes)

En el campo medico se puede usar para visualizar al paciente cuando está presentando.