



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

UNIDAD DE GESTIÓN DE TECNOLOGÍAS

DEPARTAMENTO DE ELECTRÓNICA Y COMPUTACIÓN

**PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL
TÍTULO DE TECNÓLOGO EN TELEMÁTICA**

AUTOR: MORALES RIVERA JUAN CARLOS

**TEMA: “IMPLEMENTACIÓN DE UNA RED DE VIGILANCIA
CON CÁMARAS DE TECNOLOGÍA IP EN LAS
INSTALACIONES DEL SERVICIO AEROPOLICIAL DE LA
CIUDAD DE QUITO PARA MEJORAR Y OPTIMIZAR LOS
NIVELES DE SEGURIDAD EN EL HANGAR DE LA UNIDAD”**

DIRECTOR: ING. CARLOS ESPÍN HERRERA

LATACUNGA, JUNIO DE 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
UNIDAD DE GESTIÓN DE TECNOLOGÍAS
CARRERA DE TELEMÁTICA

CERTIFICADO DEL DIRECTOR

ING. CARLOS ESPIN HERRERA (DIRECTOR)

CERTIFICA:

Que el trabajo titulado “IMPLEMENTACIÓN DE UNA RED DE VIGILANCIA CON CÁMARAS DE TECNOLOGÍA IP EN LAS INSTALACIONES DEL SERVICIO AEROPOLICIAL DE LA CIUDAD DE QUITO PARA MEJORAR Y OPTIMIZAR LOS NIVELES DE SEGURIDAD EN EL HANGAR DE LA UNIDAD”, realizado por Morales Rivera Juan Carlos, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la UGT, en el Reglamento Estudiantes de la Universidad de las Fuerzas Armadas - ESPE.

El mencionado trabajo consta de un empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (PDF).

Autoriza a Morales Rivera Juan Carlos, entregar el mismo en la biblioteca de la Unidad de Gestión de Tecnologías.

Latacunga, Junio de 2014

ING. CARLOS ESPÍN HERRERA
DIRECTOR

**UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
UNIDAD DE GESTIÓN DE TECNOLOGÍAS
CARRERA DE TELEMÁTICA**

DECLARACIÓN DE RESPONSABILIDAD

MORALES RIVERA JUAN CARLOS

DECLARO QUE:

El proyecto de grado titulado “IMPLEMENTACIÓN DE UNA RED DE VIGILANCIA CON CÁMARAS DE TECNOLOGÍA IP EN LAS INSTALACIONES DEL SERVICIO AEROPOLICIAL DE LA CIUDAD DE QUITO PARA MEJORAR Y OPTIMIZAR LOS NIVELES DE SEGURIDAD EN EL HANGAR DE LA UNIDAD”, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie de las paginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Latacunga, Junio de 2014

Morales Rivera Juan Carlos
CBOP. DE POLICÍA
C.I. 1803008364

**UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
UNIDAD DE GESTIÓN DE TECNOLOGÍAS
CARRERA DE TELEMÁTICA**

AUTORIZACIÓN PUBLICACIÓN

YO, Morales Rivera Juan Carlos

Autorizo a la UNIDAD DE GESTIÓN DE TECNOLOGÍAS DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE, publique en la biblioteca virtual de la institución, “IMPLEMENTACIÓN DE UNA RED DE VIGILANCIA CON CÁMARAS DE TECNOLOGÍA IP EN LAS INSTALACIONES DEL SERVICIO AEROPOLICIAL DE LA CIUDAD DE QUITO PARA MEJORAR Y OPTIMIZAR LOS NIVELES DE SEGURIDAD EN EL HANGAR DE LA UNIDAD”, cuyo contenido, ideas y criterios son de de mi exclusiva responsabilidad y autoría.

Latacunga, Junio de 2014

Morales Rivera Juan Carlos
CBOP. DE POLICÍA
C.I. 1803008364

DEDICATORIA

A Dios

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

A mi esposa Rebeca Gordon a mis hijos Juan Fernando y Juan Sebastián

A ellos que son los seres más maravillosos que la vida me ha dado, a ellos que son la razón para seguir esforzándome día a día; quienes con su apoyo, cariño y comprensión me ayudaron a alcanzar nuevas metas en mi vida profesional y personal.

Por esto y la infinidad de cualidades que me brindan; gracias y los amo.

Juan Carlos Morales Rivera

AGRADECIMIENTO

Agradezco a Dios por la existencia y la vida que me regalo.

Un profundo reconocimiento a mi noble Policía Nacional del Ecuador así como también al Servicio Aeropolicial que me dio la oportunidad de ingresar al Instituto Tecnológico Superior Aeronáutico, brillante oportunidad de superación personal.

Gracias a mis padres Abel Morales y Elorgia Rivera por haber fomentado en mí el deseo de superación y el anhelo de triunfo en la vida; las palabras no bastarían para retribuirles su apoyo incondicional, su comprensión y sus consejos en los momentos difíciles.

Mi gratitud de agradecimiento a todos mis docentes y en especial a mi tutor de tesis Ing. Carlos Espín Herrera, los cuales impartieron sus valiosos conocimientos sin egoísmo alguno.

A todos; espero no defraudarlos y contar siempre con su apoyo sincero e incondicional.

Juan Carlos Morales Rivera

ÍNDICE DE CONTENIDOS

PÁGINAS PRELIMINARES

CERTIFICADO DEL DIRECTOR.....	ii
DECLARACIÓN DE RESPONSABILIDAD.....	iii
AUTORIZACIÓN PUBLICACIÓN.....	iv
DEDICATORIA.....	v
AGRADECIMIENTO.....	vi
ÍNDICE DE CONTENIDOS.....	vii
ÍNDICE DE TABLAS.....	xiv
ÍNDICE DE CUADROS.....	xv
ÍNDICE DE FIGURAS.....	xvi
ÍNDICE DE ANEXOS.....	xix
INTRODUCCIÓN.....	xx
RESUMEN.....	xxii
SUMARY.....	xxiii

CAPÍTULO I

EL TEMA

1.1 Descripción del proyecto.....	1
1.2 Justificación e importancia.....	2
1.3 Objetivos.....	3
1.3.1 Objetivo General.....	3
1.3.2 Objetivos específicos.....	3
1.4 Alcance.....	3

CAPÍTULO II

MARCO TEORICO

2.1 Introducción a los sistemas de vigilancia IP.....	4
---	---

2.2 Vigilancia IP.....	4
2.3 Diferencia entre CCTV y vigilancia IP.....	5
2.4 Digitalización.....	6
2.5 Formato de imagen.....	7
2.6 Resolución.....	11
2.6.1 Resolución de pantalla.....	11
2.6.2 Resoluciones NTSC y PAL.....	12
2.6.3 Resolución VGA.....	13
2.6.4 Resolución MPEG.....	14
2.6.5 Resolución mega pixel.....	14
2.7 Teoría del color.....	15
2.8 Sistemas de televisión.....	17
2.8.1 Sistema NTSC.....	17
2.8.2 Sistema PAL.....	18
2.8.3 Sistema SECAM.....	19
2.9 Circuito cerrado de televisión.....	20
2.9.1 Aplicaciones CCTV.....	21
2.10 Medios de transmisión.....	22
2.11 Medios guiados	22
2.11.1 Pares trenzados.....	23
2.11.1.1 Cable de par trenzado sin blindaje UTP.....	24
2.11.1.2 Cable de par trenzado blindado STP.....	25
2.11.1.3 Categorías de UTP.....	26
2.11.1.4 Consideraciones sobre el cableado de par trenzado.....	27
2.11.2 Cable coaxial.....	27
2.11.2.1 Banda base.....	28
2.11.2.2 Banda ancha.....	29
2.11.2.3 Consideraciones sobre el cable coaxial.....	29
2.11.3 Fibra óptica.....	29
2.11.3.1 Composición del cable de fibra óptica.....	30
2.12 Medios no guiados.....	32
2.13 Transmisión direccional.....	33

2.14 Transmisión omnidireccional.....	33
2.15 Microondas.....	34
2.15.1 Microondas terrestres.....	35
2.15.2 Microondas por satélite.....	36
2.16 Ondas de radio vs microondas.....	37
2.17 Bluetooth.....	37
2.18 Wi-Fi.....	38
2.19 Modos de transmisión.....	39
2.19.1 Paralelo.....	39
2.19.2 Serie.....	40
2.19.2.1 Transmisión asincrónica.....	41
2.19.2.2 Transmisión sincrónica.....	41
2.20 Canal de Comunicación.....	42
2.21 Tipos de comunicación.....	42
2.21.1 Simplex.....	42
2.21.2 Duplex o semi-duplex.....	43
2.21.3 Full duplex.....	43
2.22 Redes IP.....	43
2.23 Topologías de red.....	44
2.23.1 La topología física.....	45
2.23.2 La topología lógica.....	45
2.24 Tipos de topologías.....	45
2.24.1 Topología de bus.....	46
2.24.2 Topología en anillo.....	47
2.24.3 Topología en estrella.....	48
2.24.4 Topología en árbol.....	49
2.24.5 Topología de malla.....	49
2.24.6 Topologías híbridas.....	50
2.24.6.1 En estrella-bus.....	51
2.24.6.2 En estrella-anillo.....	51
2.25 Protocolos de red.....	52
2.25.1 Los protocolos de bajo nivel.....	52

2.25.2 Los protocolos de red.....	52
2.26 Modelo de referencia OSI.....	54
2.27 Capas del modelo OSI.....	55
2.27.1 Capa física.....	55
2.27.2 Capa de enlace.....	56
2.27.3 Capa de red.....	56
2.27.4 Capa de transporte.....	57
2.27.5 Capa de sesión.....	57
2.27.6 Capa de presentación.....	58
2.27.7 Capa de aplicación.....	58
2.28 Direccionamiento IP.....	59
2.29 Clasificación de la direcciones IP	60
2.29.1 Direcciones IP públicas.....	60
2.29.2 Direcciones IP privadas.....	61
2.29.3 Direcciones IP estáticas.....	61
2.29.4 Direcciones IP dinámicas.....	62
2.29.5 El DHCP.....	63
2.30 Tipos de direcciones IP.....	63
2.30.1 Dirección IP clase A.....	64
2.30.2 Dirección IP clase B.....	65
2.30.3 Dirección IP clase C.....	65
2.30.4 Dirección IP clase D.....	66
2.30.5 Dirección IP clase E.....	66
2.31 Video sobre IP.....	67
2.32 Video Broadcast sobre IP.....	68
2.33 Video on Demand (VOD) sobre IP.....	68
2.34 Video conferencia sobre IP.....	69
2.35 Digitalización de video.....	70
2.35.1 Problemas para digitalizar.....	72
2.36 Compresión.....	72
2.37 Formatos de compresión.....	73
2.37.1 Formato MPEG.....	73

2.37.1.1 MPEG-1.....	74
2.37.1.2 MPEG-2.....	75
2.37.1.3 MPEG4.....	75
2.37.2 MJPEG.....	76
2.38 Transmisión de video digital.....	78
2.39 Requerimientos para la transmisión multimedia.....	80
2.39.1 Ancho de banda.....	80
2.39.2 Retraso de transmisión.....	81
2.39.3 Fiabilidad.....	81
2.39.4 Sincronización de canales.....	82
2.39.5 Proceso para la recepción video.....	82
2.40 Aplicaciones de las cámaras IP.....	82

CAPÍTULO III

IMPLEMENTACIÓN DE LA RED DE VIGILANCIA

3.1 Seguridad institucional.....	84
3.2 Descripción del edificio del Servicio Aeropolicial.....	84
3.3 Simbología de las instalaciones.....	85
3.3.1 Bloque A.....	85
3.3.2 Bloque B.....	86
3.3.3 Bloque C.....	86
3.3.4 Bloque D.....	86
3.4 Distribución zonas vulnerables.....	87
3.5 Simbología de zonas vulnerables.....	87
3.6 Distribución y ubicación de las cámara.....	88
3.6.1 Cámara-1.....	89
3.6.2 Cámara-2.....	89
3.6.3 Cámara-3.....	90
3.6.4 Cámara-4.....	90
3.7 Selección de cámaras IP.....	90
3.7.1 Descripción física de la cámara vivotek IP8331.....	91

3.8 Montaje de la cámara.....	92
3.8.1 Conexión general de la cámara.....	92
3.9 Elementos pasivos de la red.....	93
3.9.1 Canaletas.....	93
3.9.2 Toma corriente.....	94
3.9.3 Conectores RJ 45.....	94
3.9.4 Cable UTP.....	94
3.10 Elementos activos de la red.....	95
3.10.1 Descripción física del computador.....	95
3.10.2 Switch.....	95
3.10.3 Regulador de voltaje.....	96
3.11 Topología lógica.....	96
3.11.1 Topología física.....	96
3.11.2 Instalación del software Installation Wizard2.....	97
3.11.3 Configuración del sistema.....	98
3.11.4 Configuración de red.....	99
3.11.5 Configuración de puertos.....	99
3.11.6 Visualización a través del navegador web.....	100
3.11.7 Pantalla principal.....	100
3.11.8 Instalación del software gestor de video ST7501.....	101
3.11.9 Iconos de LiveClient, Playback y Wizar 2.....	102
3.11.10 Asignación de canales al gestor de video.....	102
3.11.11 Ajuste y procedimientos de asignación de canales LiveClient.....	103
3.11.12 Ajustes de visualización de los canales Playback.....	104
3.11.13 Pruebas de funcionalidad.....	104
3.11.14 Visualización de videos en tiempo real y respaldos.....	104
3.11.15 Visualización de eventos-respaldos.....	106
3.11.16 Servicios que proporciona la red de vigilancia.....	106
3.12 Manual.....	107
3.12.1 Descripción del manual de mantenimiento.....	107
3.12.2 Descripción general.....	108
3.13 Estudio económico.....	108

3.13.1 Análisis de costos.....	108
3.13.1.1 Costos primarios.....	108
3.13.1.2 Costos secundarios.....	109
3.13.1.3 Costos total del proyecto.....	109
3.14 Ubicación de la cámara 1.....	112
3.15 Ubicación de la cámara 2.....	113
3.16 Ubicación de la cámara 3.....	114
3.17 Ubicación de la cámara 4.....	115

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones.....	116
4.2 Recomendaciones.....	117

GLOSARIO	118
-----------------------	-----

BIBLIOGRAFÍA	131
---------------------------	-----

ANEXOS	134
---------------------	-----

ÍNDICE DE TABLAS

CAPÍTULO III

Tabla 3.1 Características del computador.....	95
Tabla 3.2 Tabla costos de equipos.....	109
Tabla 3.3 Tabla costos de materiales.....	110
Tabla 3.4 Tabla del total de costos primarios.....	110
Tabla 3.5 Tabla del total de costos secundarios.....	111
Tabla 3. 6 Tabla del total de costos del proyecto.....	111

ÍNDICE DE CUADROS

CAPÍTULO II

Cuadro 2.1 Características sistema NTSC	18
Cuadro 2.2 Características sistema PAL.....	19
Cuadro 2.3 Características sistema SECAM.....	20
Cuadro 2.4 Subsistemas según banda de transmisión.....	20
Cuadro 2.5 Dirección IP y máscara.....	59

ÍNDICE DE FIGURAS

CAPÍTULO II

Figura 2.1 Vigilancia IP.....	5
Figura 2.2 Vigilancia CCTV e IP.....	6
Figura 2.3 Formatos de imagen.....	8
Figura 2.4 Formatos de imagen.....	10
Figura 2.5 Resolución en pixeles por pulgada.....	12
Figura 2.6 Calidad de video.....	14
Figura 2.7 Mezcla aditiva de colores.....	16
Figura 2.8 Mezcla sustractiva de colores.....	16
Figura 2.9 Medios de transmisión.....	22
Figura 2.10 Medios de transmisión.....	23
Figura 2.11 Pares trenzados.....	23
Figura 2.12 Conector RJ 45.....	24
Figura 2.13 Par trenzado UTP.....	25
Figura 2.14 Par trenzado STP.....	25
Figura 2.15 Componentes del Cable coaxial.....	28
Figura 2.16 Fibra óptica.....	30
Figura 2.17 Medios no guiados	32
Figura 2.18 Medio no guiado.....	33
Figura 2.19 Transmisión direccional.....	33
Figura 2.20 Transmisión omnidireccional.....	33
Figura 2.21 Microondas.....	34
Figura 2.22 Enlace de microondas de línea de vista.....	35
Figura 2.23 Microondas por satélite.....	36
Figura 2.24 Satélite geoestacionario.....	37
Figura 2.25 Ondas de radio vs microondas.....	37
Figura 2.26 Identificador de conexión Bluetooth.....	38
Figura 2.27 Identificador de conexión Wi-Fi.....	39
Figura 2.28 Transmisión en paralelo.....	40

Figura 2.29 Transmisión en serie.....	40
Figura 2.30 Formato de un caracter.....	41
Figura 2.31 Comunicación simplex.....	42
Figura 2.32 Comunicación dúplex.....	43
Figura 2.33 Topología bus.....	47
Figura 2.34 Topología anillo.....	48
Figura 2.35 Topología estrella.....	49
Figura 2.36 Topología árbol.....	49
Figura 2.37 Topología malla.....	50
Figura 2.38 Topología híbridas.....	51
Figura 2.39 Modelo OSI.....	55
Figura 2.40 Dirección de 32 bits Clase A.....	65
Figura 2.41 Dirección de 32 bits Clase B.....	65
Figura 2.42 Dirección de 32 bits Clase C.....	66
Figura 2.43 Dirección de 32 bits Clase D.....	66
Figura 2.44 Computador con buenas características.....	71
Figura 2.45 Tarjeta capturadora de video.....	71

CAPÍTULO III

Figura 3.1 Plano de las instalaciones del Servicio Aeropolicial.....	85
Figura 3.2 Plano de las instalaciones del SAP con las zonas vulnerables...87	87
Figura 3.3 Plano de las instalaciones del SAP con las zonas vulnerables y ubicación de las cámaras.....	89
Figura 3.4 Cámara IP 8331.....	91
Figura 3.5 Panel frontal de la cámara IP 8331.....	91
Figura 3.6 Panel posterior de la cámara IP 8331.....	92
Figura 3.7 Conectores de la cámara.....	92
Figura 3.8 Opciones de montaje de la cámara IP.....	92
Figura 3.9 Conexión general de la cámara.....	93
Figura 3.10 Canaleta.....	93
Figura 3.11 Toma corriente.....	94

Figura 3.12 Conector RJ-45.....	94
Figura 3.13 Cable UTP.....	94
Figura 3.14 Switch.....	95
Figura 3.15 Regulador de voltaje.....	96
Figura 3.16 Topología lógica.....	96
Figura 3.17 Topología física.....	97
Figura 3.18 Instalación del software.....	97
Figura 3.19 Icono de la instalación del software Wizard 2.....	97
Figura 3.20 Pantallas de búsqueda de cámaras en la red.....	98
Figura 3.21 Pantalla con direcciones MAC de las cámaras.....	98
Figura 3.22 Pantalla de configuración de la cámara.....	98
Figura 3.23 Pantalla de configuración de la red.....	99
Figura 3.24 Dirección IP para acceder a la visualización.....	100
Figura 3.25 Pantalla de video tiempo real.....	100
Figura 3.26 Pantalla de configuración.....	101
Figura 3.27 Instalación del software gestor de video ST7501.....	102
Figura 3.28 Iconos de LiveClient, Playback y Wizar 2.....	102
Figura 3.29 Instalación del software para asignación de canales.....	103
Figura 3.30 Pantalla de visualización tiempo real.....	103
Figura 3.31 Pantalla de visualización de archivos de video.....	104
Figura 3.32 Visualización de zonas monitoreadas diurna y nocturna.....	105
Figura 3.33 Pantalla de visualización de eventos.....	106
Figura 3.34 Ubicación cámara 1.....	112
Figura 3.35 Ubicación cámara 2.....	113
Figura 3.36 Ubicación cámara 3.....	114
Figura 3.37 Ubicación cámara 4.....	115

ÍNDICE DE ANEXOS**Anexo A**

Anteproyecto.....134

Anexo B

Anexos del anteproyecto.....155

Anexo C

Planos de las instalaciones del Servicio Aeropolicial.....159

Anexo D

Manual básico de mantenimiento de los equipos162

Anexo E

Imágenes de prueba de las zonas vigiladas.....166

INTRODUCCIÓN

La inseguridad ha sido siempre una preocupación mundial; en la que día a día se buscan nuevas soluciones para corregir este problema.

Los países de renta alta son los pioneros en la búsqueda de soluciones; desde evitar faltas menores hasta prevenir y aclarar casos de homicidios o terrorismo.

Con base a la tecnología se han buscado soluciones reales a la inseguridad, es así como surgieron las cámaras de seguridad hace ya más de treinta años (finales de la década de los 70`s)¹, las cuales en sus inicios funcionaban de manera analógica², eran las llamadas cámaras de circuito cerrado; en la medida que el tiempo pasó y surgió lo que hoy es llamada la tecnología digital³, la cual trajo consigo la evolución de las computadoras, el internet y otros.

Es así como se crearon las cámaras IP, estas son videocámaras de vigilancia que tienen la característica de enviar las señales de video (en muchos casos audio) hacia cualquier punto de una red o en cualquier lugar del mundo a través de Internet.

En lo que respecta a seguridad; la situación actual en la que se vive no nos brinda un ambiente confiable, esto no solo es un problema que aqueja a un pequeño grupo de la población ecuatoriana; la inseguridad es un problema latente y una situación que también se debe tener en cuenta en toda institución, empresa y cualquier organización sin importar el rubro a que esta se dedique ya sea comercio, industria o servicio.

La violencia es un fenómeno que está afectando cada vez más la convivencia de los ecuatorianos y se ha convertido en un problema complejo

¹ http://www.axis.com/products/video/about_networkvideo/index.htm

² Analógica: Dicho de un aparato que funciona con señales análogas: forma de onda continua que pasa a través de un medio de comunicación.

³ Digital: Dicho de un aparato que funciona con señales digitales: forma de onda discreta que transmite datos codificados en dos estados como bits 1 y bits 0, los cuales representan el encendido y apagado de los pulsos eléctricos.

que ha puesto en una situación inestable a las políticas de seguridad de los gobiernos de la región.

Las soluciones para la inseguridad se han enfocado mayormente en buscar castigar a los supuestos culpables de los delitos; pero se hace poco en la prevención.

El servicio Aeropolicial de la ciudad de Quito no se escapa de sufrir hechos delincuenciales; principalmente hurtos y está expuesta a la ocurrencia de diferentes delitos.

La seguridad de la unidad se basa en la prestada por el personal de la institución.

El número de personas activas en el Servicio Aeropolicial de la ciudad de Quito actualmente es de 35, esta cantidad varía continuamente.

Estas instalaciones son utilizadas por personal civil y policial en su mayoría; para el desarrollo de las diversas actividades que a cada parte le competen, por lo que a diario es necesario controlar el acceso de personas inescrupulosas a las instalaciones.

Estas personas pueden ser miembros de la unidad o personas ajenas a esta, las cuales pueden acceder con cierto grado de facilidad a los diferentes áreas.

Por lo que se considera que hay una prioridad en la implementación de una red de vigilancia con tecnología IP que garantice la seguridad de las instalaciones del Servicio Aeropolicial de la ciudad de Quito.

RESUMEN

El presente proyecto tiene como finalidad la implementación de la red de video vigilancia con cámaras de tecnología IP para el edificio del Servicio Aeropolicial de la Ciudad de Quito.

Para el desarrollo del presente proyecto se han definido los problemas que presenta el Servicio Aeropolicial de la ciudad de Quito en el ámbito de la seguridad.

Debido a la vulnerabilidad y la falta de seguridad electrónica en la vigilancia del edificio del Aeropolicial.

Se pudo determinar los requerimientos necesarios “Equipos tecnológicos” para la implementación de la red de video vigilancia.

Para la implementación de la red de vigilancia se detallan las técnicas utilizadas en el cumplimiento del mismo; además de la información sobre las tecnologías que pueden ser aplicadas y así poder determinar cuál de ellas se utilizará en la implementación del sistema.

Una vez que finalizó la implementación del sistema de video vigilancia explicando la configuración del software y hardware se realizó las pruebas del mismo para la comprobación del correcto funcionamiento.

También se cita las conclusiones y recomendaciones que surgieron en el desarrollo, ejecución e implementación de la red de video vigilancia.

PALABRAS CLAVES:

- ✓ **VIGILANCIA**
- ✓ **TECNOLOGÍA**
- ✓ **MEJORAR**
- ✓ **OPTIMIZAR**
- ✓ **SEGURIDAD**
- ✓ **UNIDAD**

SUMARY

The present project has as purpose the design and implementation of the net of video surveillance with technology cameras IP for the Aeropolicial Service building Quito City.

For the development of the present project I have been defined the problems that it presents in the Aeropolicial Service of Quito city in the environment of the security.

Due to the vulnerability and the lack electronic surveillance in the Aeropolicial building, I could determine the necessary requirements “technological teams” for the implementation of the net of video surveillance.

For the implementation of the net of surveillance the techniques are detailed used in the execution of the same one, besides the information on the technologies that can be applied and this way to be able to determine which of them it will be used in the implementation of the system.

Once I conclude the implementation of the video system surveillance explaining the configuration of the software and hardware, one carries out the tests of the same one for the confirmation of the correct operation.

One also has the summations and recommendations that arose in the course of the execution and implementation of the net of video surveillance.

KEYWORDS:

- ✓ **MONITORING**
- ✓ **TECHNOLOGY**
- ✓ **IMPROVE**
- ✓ **OPTIMIZE**
- ✓ **SAFETY**
- ✓ **UNIT**

CAPÍTULO I

EL TEMA

1.1 Descripción del proyecto

El Servicio Aeropolicial, es una unidad de la Policía Nacional del Ecuador dedicada a aplicar sus conocimientos en el campo de la aeronáutica; en su hangar se recibe y despacha varios vuelos diariamente en diferentes horarios, además en la unidad laboran decenas de personas entre pilotos, técnicos, personal administrativo y personal de seguridad.

En ese contexto se sitúa la problemática siguiente:

Al recibir a tantas personas en sus instalaciones el sistema de seguridad actual de la unidad no es suficiente para dar cobertura a todas las zonas de las instalaciones por lo que han ocurrido ciertos hechos, tales como los siguientes:

- ✓ Daños en aeronaves.
- ✓ Inadecuado uso de las diferentes herramientas o equipos que se encuentran en el hangar.
- ✓ Posibilidad de que en la unidad ocurran hechos violentos o atentados contra personas o bienes.

Existe facilidad de acceder a las diferentes instalaciones, por lo que da oportunidad a que personas inescrupulosas accedan a esta con la finalidad de cometer algún delito.

La posibilidad de robos o pérdidas de herramientas del hangar como de las bodegas puede ser causa de quebrantos económicas para la unidad y la institución policial.

En caso de ocurrir cualquier problema o evento fuera de orden no existe sistema alguno para comprobar quien o quienes ejecutaron dichas acciones.

Al ser el Servicio Aeropolicial una unidad policial se debe evitar que ocurran incidentes y prevenir que hechos mayores ocurran en las instalaciones.

Por tal razón, en la unidad existe la necesidad de crear una red de vigilancia que permita garantizar la seguridad y salvaguardar los bienes de las

diferentes áreas tales como: aeronaves, recursos informáticos, mobiliario de oficina, entre otros pero principalmente la protección del personal.

El proyecto no solo es importante para proteger a las personas y bienes; sino además como un sistema que elevará el control de parte del comandante de la unidad, puesto que tendrá una herramienta de vigilancia que le permita conocer lo que está ocurriendo o ha ocurrido en el hangar.

Existen muchos factores que considerar para la ejecución del proyecto; tales como: la parte operativa, tecnológica y económica; la cual es principalmente la parte que influye en su implementación o no.

Es por ello que se plantea un proyecto que sirva de base para que en corto plazo pueda ser implementada en las demás unidades Aeropolicial.

1.2 Justificación e importancia

Debido a la vulnerabilidad en la seguridad del Servicio Aeropolicial de la ciudad de Quito y con base a la inseguridad que está presente en todo el Ecuador y sobre todo por la ocurrencia de incidentes en el hangar de la unidad; se hace necesario contar con una red de vigilancia que ayude a mejorar la seguridad de los bienes y principalmente de todas las personas que laboran en la unidad.

Considerando que al tener una red de vigilancia ayudaría y contribuiría en el control y prevención de riesgos laborales en el hangar del Servicio Aeropolicial de la ciudad de Quito, es necesario contar con un instrumento que ofrezca seguridad de calidad hacia todas las personas que utilizan las diferentes instalaciones de la unidad, ya sean personal administrativo, de mantenimiento y seguridad, por lo que la red de vigilancia daría más calidad al ambiente laboral actual.

El presente proyecto está orientado a proveer de un servicio a las instalaciones del Servicio Aeropolicial de la ciudad de Quito, el mismo que cuenta con la aprobación y el apoyo necesario de las autoridades policiales del SAP para su implementación.

Además del beneficio que brinde al mejorar la seguridad, el control y

prevención de riesgos laborales en el hangar del Servicio Aeropolicial de la ciudad de Quito, servirá como proyecto piloto para el resto de unidades.

1.3 Objetivos

1.3.1 Objetivo General

Implementar una red de vigilancia utilizando tecnología de avanzada, con la finalidad de optimizar el nivel de seguridad en el hangar del Servicio Aeropolicial de la ciudad de Quito.

1.3.2 Objetivos específicos

- ✓ Recopilar información sustentable que nos permita la ejecución del proyecto.
- ✓ Realizar un análisis de la situación actual y determinar los requerimientos necesarios para mejorar la seguridad en las áreas vulnerables existentes en el hangar.

1.4 Alcance

El presente trabajo está encaminado a generar beneficios al Servicio Aeropolicial de la ciudad de Quito, ya que proporcionara un alto interés y motivación a todo el personal que se encuentre relacionado con la unidad; poniendo en claro la importancia que genera resguardar los bienes y sobre todo proteger a todo su personal; dando así un adecuado ambiente de trabajo en todas las instalaciones.

CAPÍTULO II

MARCO TEORICO

2.1 Introducción a los Sistemas de Vigilancia IP

El Video IP, también conocido como Video Over IP (del inglés) es uno de los grandes resultados que nos trajo la era digital con la globalización de la información y es el término que se ha utilizado para nombrar la tecnología que sorprendió al mundo al capturar, comprimir y convertir las secuencias de imágenes en movimiento (video) en un flujo de datos que puede ser transmitido por redes de computadoras; también conocidas como Redes IP (LAN / WLAN / WAN / Internet).

El transporte de video por redes de datos ha sido posible hoy día gracias a:

- ✓ Los avances en las técnicas de digitalización y compresión de imágenes.
- ✓ El crecimiento en las redes de datos (IP Networks).
- ✓ El desarrollo y comercialización cada vez mayor de equipos de video digitales que han sido de interés mundial (Satélites, televisión digital por cables, DVD, etc.).

2.2 Vigilancia IP

Una de las grandes aplicaciones que ha encontrado el video IP es sin duda en el campo de los sistemas electrónicos de seguridad y vigilancia, ya que la industria ha desarrollado hardware y software suficientemente potentes y eficientes como para realizar todas las funciones de los sistemas analógicos tradicionales y superarlos ampliamente con la incorporación de funciones inteligentes que eran solo fantasía hasta hace pocos años.

Los sistemas de vigilancia IP, son aquellos en que las imágenes y audio son capturados por las cámaras y micrófonos; se comprimen y transmiten por una red de datos local o internet (LAN / WAN) y pueden ser accedidos desde uno o varios puntos en cualquier lugar del mundo mediante

computadoras convencionales o hardware especialmente diseñado para descomprimir los datos, visualizarlos, analizarlos, grabarlos y hasta generar acciones de manera automática en respuesta a diferentes eventos pre-definidos o a voluntad de un operador.

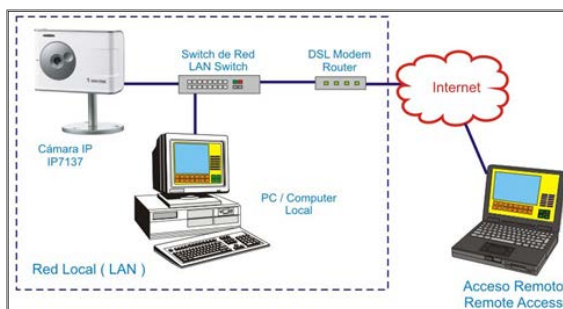


Figura 2.1 Vigilancia IP

Un detalle importante dentro de los sistemas de Vigilancia IP es que no solo involucran video sino también audio y que el audio puede ser bi-direccional, es decir: en una estación de monitoreo se puede escuchar las conversaciones y sonidos generados en los lugares en donde están las cámaras y micrófonos.

El audio bi-direccional puede ser muy útil para disuadir a sospechosos antes que cometan el delito o para coordinar el trabajo de los agentes de seguridad en diferentes posiciones de un objetivo protegido.

Entre los elementos que componen un sistema de vigilancia IP amerita resaltar:

- ✓ Las cámaras IP.
- ✓ Servidores de video.
- ✓ Decodificadores de video IP.
- ✓ Grabadores digitales de red (NVR).
- ✓ Software inteligente para centrales de monitoreo.

2.3 Diferencia entre CCTV y Vigilancia IP

En los sistemas de vigilancia convencionales (CCTV) el video análogo que sale de las cámaras viaja por cable coaxial o UTP hasta el dispositivo de

grabación, distribución, conmutación o visualización según sea el caso, pero en su viaje nunca deja de ser video analógico.

Esto quiere decir por ejemplo, que en cualquier punto entre la cámara y el grabador, se podría literalmente “cortar el cable” para conectarlo a un monitor análogo y ver el video.

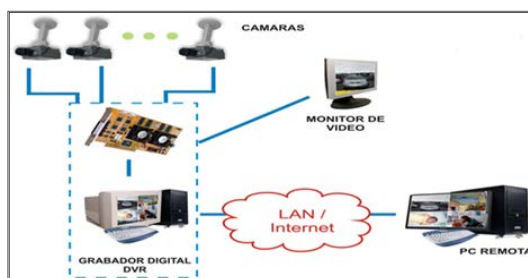


Figura 2.2 Vigilancia CCTV e IP

No se debe confundir el uso de cables de red UTP / STP y balun de video para transportar el video analógico con un sistema IP; pues aunque en este caso se utiliza el mismo tipo de cable, la información que viaja por los cables en un sistema IP es completamente digital o sea datos y se requiere de computadoras o algún hardware especialmente preparado para decodificar ese flujo de información y volverlo a convertir en video.

A diferencia de los sistemas de vídeo analógicos convencionales, la vigilancia IP no requiere de un cableado punto a punto por cada cámara, pues las redes de datos que son su medio de transporte llevan el video, el audio y las señales de control a través de una estructura nódulo-modular, no solo distinta, sino también más eficiente, conveniente y versátil para las instalaciones y futuras expansiones.

2.4 Digitalización

Digitalizar es convertir cualquier señal de entrada continua (analógica), como una imagen o una señal de sonido, en una serie de valores numéricos. Por ejemplo, la imagen que se manda mediante un fax se digitaliza línea a línea mediante el escáner que lleva incorporado, cada línea se convierte en una combinación de ceros y unos que se transmiten por la línea telefónica.

Para esta conversión suelen utilizarse convertidores analógicos digitales. Por extensión también se aplica el término digitalización a la obtención de representaciones digitales de imágenes, sonidos o vídeos.

El tratamiento, transmisión, almacenamiento y recepción de muchos tipos de información por medio de canales de comunicación y por medio de ordenadores exige que esta información esté en un formato compatible con el ordenador, por lo que es necesario convertir esta información en un grupo de números que represente esta información de manera precisa y fiable.

A este proceso se le conoce de manera coloquial como digitalizar, aunque en algunos casos se le conoce como un derivado del nombre del dispositivo que realiza tal función, como en el caso de escanear, por realizarse mediante un escáner.

El proceso de digitalizar o digitalización depende del tipo de información que se trata.

En algunos casos, como por ejemplo una fotografía, se trata de representar el color de cada uno de los puntos de la imagen por una matriz de números de manera que el valor de cada una de las celdas de la matriz lleve la información del color con la precisión adecuada.

En otros casos como es la digitalización del sonido se produce una secuencia de números en que cada uno representa un instante del valor de la señal eléctrica equivalente al sonido.

En todos los procesos de digitalización hay que considerar que la imagen electrónica del documento que se obtiene no contiene más que una pequeña parte de la información que el propio documento contiene aunque para muchos efectos, si se ha realizado con los criterios correctos puede ser suficiente para el propósito seguido.

2.5 Formato de imagen

Para poder intercambiar imágenes entre los diferentes sistemas operativos, existe el formato de imagen, que es la extensión en la que se guarda el archivo de la imagen.

El formato de imagen o de archivo se refiere a la estructura de datos en que se guardará el documento.

Estos formatos también poseen algunas características especiales que permite distinguirlos entre ellos; estas características son: la resolución y la calidad de imagen en contraste con la capacidad de memoria que ocupa. Entre las extensiones más conocidas están: BMP, PSD, GIF, JPEG, JPG, PCX, TIFF.

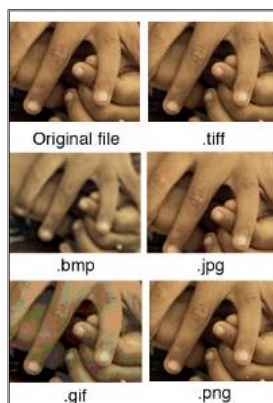


Figura 2.3 Formatos de imagen

TIFF.- El Formato de fichero de información es un formato de archivo usado para almacenar imágenes, como dibujos y fotografías.

Este es un formato popular para imágenes de alta profundidad de color y es apoyado por muchos de manipulación de imágenes, programas como PageMaker, QuarkXPress, Adobe InDesign, Photoshop, Paint Shop Pro.

Tiff es de una calidad de imagen extremadamente alta, proporcionando una excelente compatibilidad con edición e impresión.

Tiff se pueden modificar y volver a guardar, con las imágenes que se utilizan un sinnúmero de veces sin perder los datos de la imagen.

Además, la imagen es extremadamente útil, ya que no requiere un software de post-procesamiento, durante o después de su descarga a partir de una cámara; es un formato flexible y adaptable.

GIF.- El Graphic Interchange Format es un formato de archivo de imagen que fue desarrollado originalmente en 1987 por Unisys utilizando el algoritmo de compresión LZW. Durante años ha sido un formato de imagen estándar

que se utiliza en la web. En 1989, también desarrolló GIF89a permite imágenes animadas. Mientras GIF ha disfrutado de una presencia importante en Internet, en la actualidad está siendo eliminado por la aparición de PNG.

JPG / JPEG.- JPEG es un método de compresión utilizado para imágenes fotográficas.

El nombre JPEG significa Joint Photographic Experts Group, el nombre del comité que redactó la norma. El nivel de compresión puede ser ajustado para permitir seleccionar la configuración deseada entre el tamaño del archivo de imagen y la calidad de la imagen.

Por lo general, JPEG alcanza 10 a 1 de compresión con poca pérdida perceptible en la calidad de imagen.

Además de ser un método de compresión, JPEG es a menudo considerado como un formato de archivo de imagen.

JPEG es el formato de imagen más comúnmente utilizado por las cámaras digitales y otros dispositivos de captura de imágenes fotográficas, también es el formato más común para almacenar y transmitir imágenes fotográficas en Internet.

BMP.- El formato de archivo BMP, es un tipo de formato de archivo de imagen de mapa de bits utilizado para almacenar imágenes digitales, especialmente en los sistemas operativos Microsoft Windows y OS2.

La sencillez del formato de archivo BMP y su amplia familiaridad en Windows y en otros lugares hace que sea un formato muy común que los programas de procesamiento de imágenes de muchos sistemas operativos pueden leer y escribir. Otras razones para su uso generalizado es que está bien documentado y libre de patentes.

Aunque la mayoría de los archivos de imagen BMP tienen un tamaño de archivo relativamente grande debido a la falta de compresión, muchos archivos BMP pueden ser comprimidos considerablemente sin pérdidas con

algoritmos de compresión de datos, tales como ZIP, ya que contienen datos redundantes.

PNG.- El Portable Network Graphics es un formato de imagen de mapa de bits que utiliza compresión sin pérdida de datos similar a la de un archivo GIF.

PNG fue creado para mejorar y reemplazar el formato GIF, ya que no es un formato de archivo de imagen que requiere una licencia de patente.

Fue creado, básicamente, en refutación directa de los requisitos de licencia de Unisys para utilizar el formato GIF.

PNG trabaja con paletas (paletas de colores de 24 bits RGB), escala de grises o RGB. PNG fue diseñado para transferir las imágenes en Internet, no de gráficos profesionales, por lo que no es compatible con otras especificaciones de color como CMYK.

PNG funciona muy bien para los dibujos geométricos o líneas, letras, dibujos animados y otras imágenes con colores planos y bordes bien definidos, tales como imágenes de ordenador.

PNG es en la mayoría de casos superior a GIF, ya que es más reciente, compatible con más colores y está libre de restricciones de patentes.

PNG no se puede utilizar para las animaciones; sin embargo, ofrece una transparencia altamente sofisticada y soporte de color, entre otras características.

En la mayoría de los casos en que las animaciones no son necesarias, lo mejor es usar PNG sobre GIF.



Figura 2.4 Formatos de imagen

Es interesante observar las fortalezas de cada tipo de formato de imagen y las debilidades.

Actualmente a nivel general y sobretodo en el diseño de una página Web los tipos de formato de fichero de imagen más utilizados son JPEG y PNG.

JPEG para el tratamiento y la visualización de imágenes del tipo fotografías, por la calidad de la imagen y por el tamaño de las mismas.

PNG para los iconos, bloques, degradados y gráficos que se utilizan para el diseño de la página Web.

2.6 Resolución

2.6.1 Resolución de pantalla

La resolución de pantalla es el número de píxeles que puede ser mostrado en la pantalla.

Viene dada por el producto del ancho por el alto, medidos ambos en píxeles, con lo que se obtiene una relación, llamada relación de aspecto.

En esta relación de aspecto se puede encontrar una variación, está de acuerdo a la forma del monitor y de la tarjeta gráfica.

Se pueden diferenciar dos tamaños de pantalla diferentes:

Tamaño absoluto.- La anchura y altura de la ventana del monitor, medido generalmente en pulgadas.

Depende del monitor.

Resolución o tamaño relativo.- Viene determinada por el número de píxeles que se muestran en la ventana del monitor, siendo el píxel la unidad mínima de información que se puede presentar en pantalla, de forma generalmente rectangular, depende de la tarjeta gráfica.

La resolución de la imagen es la cantidad de píxeles por unidad de medida que tiene la imagen, de aquí que el término más común para expresar la resolución de imágenes digitales es: píxeles per inch (píxeles por pulgada) (ppi).

La resolución se relaciona directamente con la cantidad de detalles que puede observarse en una imagen es decir cuanto mayor sea la resolución, más detallada y definida es la imagen, como se puede observar en la figura

2.5.

En un mundo digital o analógico es parecida, pero existen algunas diferencias importantes sobre su definición.

En el vídeo analógico, la imagen consiste en líneas, o líneas de TV, ya que la tecnología del vídeo analógico procede de la industria de la televisión.

En un sistema digital, la imagen está formada por píxeles.

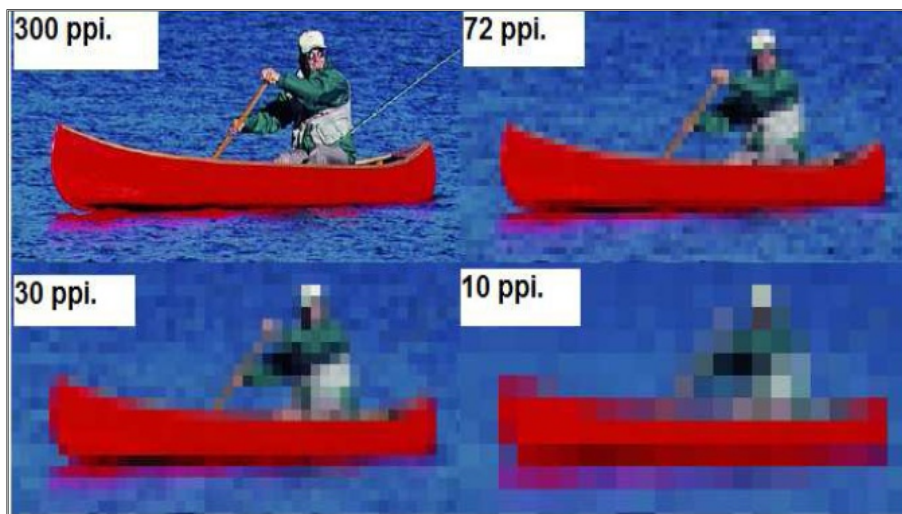


Figura 2.5 Resolución en píxeles por pulgada

2.6.2 Resoluciones NTSC y PAL

En América del Norte y Japón, el estándar NTSC (Comité Nacional de Sistemas de Televisión) es el estándar de vídeo analógico predominante, mientras que en Europa se usa el estándar PAL (Línea de Alternancia de Fase).

Ambos estándares proceden de la industria de la televisión.

NTSC tiene una resolución de 480 líneas horizontales y una velocidad de renovación de 60 campos entrelazados por segundo o 30 imágenes completas por segundo. PAL tiene una resolución de 576 líneas horizontales y una velocidad de renovación de 50 campos entrelazados por segundo o 25 imágenes completas por segundo. La cantidad total de información por segundo es la misma en ambos estándares.

Cuando el vídeo analógico se digitaliza, la cantidad máxima de píxeles que pueden crearse se basará en el número de líneas de TV disponibles para ser digitalizadas.

En NTSC, el tamaño máximo de imágenes digitalizadas es de 720x480 píxeles.

En PAL, el tamaño es de 720x576 píxeles. La resolución más utilizada habitualmente es 4CIF 704x576 PAL / 704x480 NTSC.

2.6.3 Resolución VGA

Con la introducción de las cámaras IP, pueden diseñarse sistemas 100% digitales.

Esto provoca que las limitaciones de NTSC y PAL carezcan de importancia.

Se han introducido algunas resoluciones nuevas procedentes de la industria informática, que proporcionan una mejor flexibilidad y además constituyen estándares universales.

VGA es la abreviatura de Video Graphics Array (Tabla de Gráficos de Vídeo), un sistema de exposición gráficos para PC desarrollado originalmente por IBM.

La resolución se define a 640x480 píxeles, un tamaño muy parecido a NTSC y PAL.

La resolución VGA es normalmente más adecuada para las cámaras IP, ya que el vídeo en la mayoría de los casos se mostrará en pantallas de ordenador, con resoluciones en VGA o múltiplos de VGA. Quarter VGA (QVGA), con una resolución de 320x240 píxeles, también es un formato utilizado habitualmente con un tamaño muy similar a CIF, QVGA en ocasiones se llama SIF (Formato de Intercambio Estándar), que fácilmente se confunde con CIF.

Otras resoluciones basadas en VGA son XVGA (1.024x768 píxeles) y de 1.280x960 píxeles, 4 veces VGA, que ofrecen una resolución mega pixel.

2.6.4 Resolución MPEG

MPEG son las siglas de Moving Picture Experts Group y se pronuncia m-peg. MPEG es un grupo de la ISO y la familia de estándares de compresión y de formatos de archivo de video digital desarrollados por el grupo.

El MPEG produce generalmente vídeos de mejor calidad que otros formatos, como vídeo para Windows, Indeo y QuickTime.

Los algoritmos del MPEG comprimen la información en pequeños paquetes que pueden ser transmitidos fácilmente y después ser descomprimidos.

El MPEG alcanza su alta tasa de compresión almacenando solamente los cambios de un frame al siguiente, en vez de almacenar el frame entero.

La resolución MPEG normalmente significa diferentes resoluciones empleadas.

704x576 pixels (TV PAL)

704x480 pixels (TV NTSC)

720x576 pixels (PAL o D1)

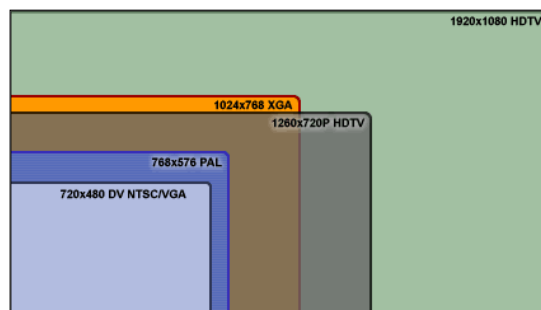


Figura 2.6 Calidad de video

2.6.5 Resolución Mega pixel

Cuanta más alta sea la resolución, más detalles pueden observarse en una imagen.

Esto es una consideración muy importante en las aplicaciones de vigilancia por vídeo, donde una imagen de alta resolución puede permitir la identificación de un delincuente.

La resolución máxima en NTSC y PAL, en cámaras analógicas, después de que la señal de vídeo se haya digitalizado en un DVR o en un servidor de vídeo, es de 400.000 píxeles ($704 \times 576 = 405.504$). 400.000 equivale a 0,4 mega píxeles.

A pesar de que la industria de vigilancia por vídeo ha logrado siempre vivir con estas limitaciones, la nueva tecnología de cámaras IP hace posible hoy en día una resolución mayor.

Un formato mega píxel común es 1.280×1.024 , que ofrece una resolución de 1,3 mega píxeles, 3 veces más que en las cámaras analógicas.

2.7 Teoría del color

El color es la forma en que el ojo traduce los diferentes valores de las longitudes de ondas del espectro electromagnético que se encuentran en el rango de los 380 (violeta) a 780 nanómetros (rojo), las cuales corresponden a la luz visible por el ser humano.

Por debajo de esta medida se encuentra la radiación ultravioleta rayos X, rayos gamma y por arriba los infrarrojos micro ondas, ondas de radio y televisión, los cuales no son visibles por el ojo humano.

Esta pequeña región del espectro es la luz que percibe el ojo humano, la cual permite ver los objetos.

Cada frecuencia dentro de este rango es una diferente sensación, un diferente color del rojo al violeta, que puede percibirse.

La teoría del color es un conjunto de reglas básicas usadas en la mezcla de colores para conseguir el efecto deseado en los campos de la pintura, el diseño gráfico, la fotografía, la imprenta y la televisión; lo cual se logra mediante la combinación de colores ya sean colores-luz o colores-pigmento.

Los sistemas de reproducción del color se dividen en aditivos y sustractivos.

Sistemas Aditivos.- Consisten en partir del negro, es decir ausencia de luz, e ir añadiendo mayor o menor cantidad de luz de tres colores básicos, a partir de los cuales se consigue cualquier otro color, incluyendo la luz blanca.

Los colores básicos necesarios son rojo, verde y azul (RGB).

Éste método de reproducción del color es utilizado en monitores de ordenador y televisiones en color, porque crean los colores añadiendo luces a un fondo negro.

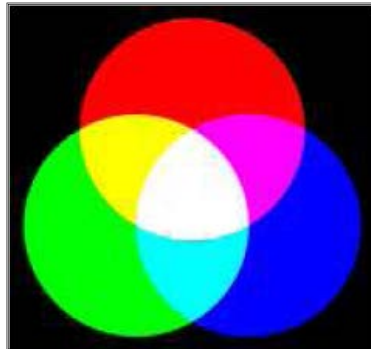


Figura 2.7 Mezcla aditiva de colores

Sistemas Sustractivos.- Este sistema parte de la luz blanca y se suprimen determinadas longitudes de onda.

El color resultante es el de las longitudes no suprimidas. En este sistema, el color blanco se consigue por la ausencia de colorantes.

El sistema sustractivo se denomina también CMY por las iniciales de los colores básicos utilizados; Cyan (un verde azulado), Magenta (rojo violáceo) y Yellow (amarillo).

Éste método de reproducción de color es utilizado en las artes gráficas y en las impresoras.

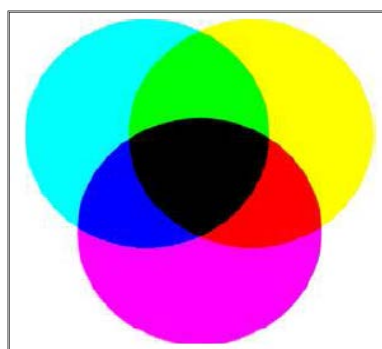


Figura 2.8 Mezcla sustractiva de colores

2.8 Sistemas de televisión

Los Sistemas de televisión son un método de comunicación eléctrica que permite la transmisión y recepción a distancia de señales eléctricas de imágenes visuales transitorias.

En sus inicios, los sistemas de televisión únicamente transmitían y reproducían imágenes en blanco y negro, es decir la información de brillo de la imagen.

Un posterior desarrollo, ha hecho también posible la transmisión del contenido cromático, lo cual se logró mediante la combinación de la información del brillo de la imagen y la información de color.

Con el paso del tiempo, también se modifican los mapas políticos, aparecen nuevos países y algunos cambian sus nombres.

Otros renuevan sus sistemas y características de transmisión a medida que se van modernizando y adaptando a la tendencia de la tecnología y otros aspectos del progreso en esta materia. Algunos países cuentan con un sistema o norma de transmisión de televisión oficial, pero las nuevas compañías de cable que se van incorporando eligen otro sistema distinto.

También sucede el caso típico en que viviendo en un país con un sistema determinado, se reciben señales de televisión en un sistema diferente, como por ejemplo vía satélite, y a veces estos factores agregan confusión acerca de cuál es el sistema que en realidad utilizan determinadas regiones.

2.8.1 Sistema NTSC

El sistema National Television System Committee, en español Comisión Nacional de Sistemas de Televisión conocido por sus siglas NTSC, es un sistema de codificación y transmisión de Televisión a color analógica desarrollada en Estados Unidos en el año 1953.

NTSC se utiliza en Estados Unidos, Canadá, Japón, en la mayoría de los países del continente americano, incluido Ecuador y en varios países asiáticos.

Cuadro 2.1**Características sistema NTSC**

Parámetros básicos	NTSC-M (Sistema americano)
Líneas/campos	525/60
Frecuencia horizontal	15.734 kHz
Frecuencia vertical	60 Hz
Frecuencia de la portadora de color	3.579545 MHz
Ancho de banda de video	4.2 MHz
Portadora de sonido	4.5 MHz (FM)

Fuente.- http://electronica.ugr.es/~amroldan/asignaturas/curso01-02/tv1/material/guia_tv.htm

2.8.2 Sistema PAL

El Sistema PAL que significa Phase Alternating Line, en español Línea de Fase Alternada, es un sistema de codificación empleado en transmisión de señales de televisión analógica en colores.

Es utilizado en gran parte del mundo, de origen alemán y es utilizado por muchos países africanos, asiáticos, europeos, Oceanía y algunos países sudamericanos.

Su origen se remonta al año 1963, en un intento por mejorar la calidad y reducir los defectos en los tonos del sistema NTSC.

Existen varios formatos del Sistema PAL; éste sistema se usa habitualmente con un formato de vídeo de 625 líneas por cuadro¹⁸ y una tasa de refresco de pantalla de 25 cuadros por segundo, entrelazadas, como ocurre por ejemplo en las variantes PAL-B, G, H, I y N.

Algunos países del Este de Europa que abandonaron el sistema SECAM ahora emplean PAL D o K, adaptaciones para mantener algunos aspectos técnicos de SECAM en PAL.

Cuadro 2.2**Características sistema PAL**

Parámetros básicos	PAL B-G-H	PAL I	PAL D	PAL N	PAL M
Líneas/campos	625/50	625/50	625/50	625/50	525/60
Frecuencia horizontal	15.625 kHz	15.625 kHz	15.625 kHz	15.625 kHz	15.734 kHz
Frecuencia vertical	50 Hz	50 Hz	50 Hz	50 Hz	60 Hz
Frecuencia de la portadora de color	4.43361 MHz	4.43361 MHz.	4.43361 MHz.	3.58205 MHz.	3.57561 MHz.
Ancho de banda de video	5.0 MHz	5.5 MHz.	6.0 MHz.	4.2 MHz.	4.2 MHz.
Portadora de sonido	5.5 MHz. (FM)	6.0 MHz.	6.5 MHz.	4.5 MHz.	4.5 MHz.

Fuente.- http://electronica.ugr.es/~amroldan/asignaturas/curso0102/tv1/material/guia_tv.htm

2.8.3 Sistema SECAM

SECAM proviene de las siglas en francés Séquentiel Couleur à Mémoire, que significa color secuencial con memoria.

Es un sistema para la codificación de televisión en color analógica utilizado por primera vez en Francia, es la primera norma europea de televisión en color.

Igual que los demás sistemas utilizados para la transmisión de televisión en color en el mundo el SECAM es una norma compatible, lo que significa que los televisores monocromos B/N preexistentes a su introducción son aptos para visualizar, en blanco y negro, correctamente los programas que han sido codificados en el sistema SECAM.

Cuadro 2.3**Características sistema SECAM**

Parámetros básicos	SECAM B-G-H	SECAM D-K-K1-L
Líneas/campos	625/50	625/50
Frecuencia horizontal	15.625 kHz.	15.625 kHz.
Frecuencia vertical	50 Hz.	50 Hz.
Ancho de banda de video	5.0 MHz	6.0 MHz.
Portadora de sonido	5.5 MHz (AM)	6.5 MHz (AM)

Fuente.- http://electronica.ugr.es/~amroldan/asignaturas/curso0102/tv1/material/guia_tv.htm

Los siguientes subsistemas se utilizan generalmente para la transmisión en las siguientes bandas de frecuencia.

Cuadro 2.4**Subsistemas según banda de transmisión**

B	G	H	I	D	N	M	K	K1	L
VHF	UHF	UHF	VHF / UHF	VHF	VHF / UHF	VHF / UHF	UHF	VHF / UHF	VHF / UHF

Fuente.- http://electronica.ugr.es/~amroldan/asignaturas/curso0102/tv1/material/guia_tv.htm

2.9 Circuito cerrado de televisión

El Circuito Cerrado de Televisión cuyas siglas es CCTV, proviene del inglés: Closed Circuit Television, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

El circuito puede estar compuesto por una o más cámaras de vigilancia conectadas a uno o varios monitores o televisores.

Aunque en la actualidad éstas cámaras también pueden ser conectadas a la red y a otros componentes como dispositivos de video u ordenadores.

En la moderna arquitectura de control de los edificios actuales, la incorporación del circuito cerrado de televisión CCTV) es indispensable.

Los proyectos incluyen cámaras de funcionamiento nocturno y diurno, internas, externas y de iluminación y captación infrarroja para zonas de seguridad crítica, en color y en blanco y negro.

Entre las distintas cámaras y la imagen a presentar al operador se proponen una variedad de posibilidades dependiendo de la arquitectura del edificio, de la zonificación del mismo y de las posibilidades de control.

Estos últimos equipamientos incluyen: Mecanismos de control de posición de cámara (pan-tilt), controles de aproximación (zoom), controladores de señal (switches), grabadores de señal, particionadores de imagen (quad).

Todos estos procesos se pueden hoy controlar mediante el software aplicado, e incluso utilizar las redes instaladas más comunes como las Ethernet, fibras ópticas e incluso la red telefónica del edificio para transmitir las señales de vídeo.

Los sistemas de CCTV están conformados básicamente por una serie de cámaras de tecnología CCD o ICCD fijas o con movimiento, ocultas o discretas y sus respectivos monitores. Para la mejor gestión o manejo de las cámaras hacia los monitores se utilizan las matrices de vídeo, que son sistemas capaces de direccionar a través de microprocesadores las entradas (cámaras) hacia las salidas (monitores), con las matrices de vídeo se pueden programar las secuencias de cámaras en un monitor.

También los sistemas modernos de CCTV permiten digitalizar las imágenes y comprimirlas para así poder mostrar en un solo Monitor toda la información requerida estos sistemas son los llamados "Multiplexores DIGIQUAD", con los sistemas de videograbación TIMELAPSE se pueden grabar en tiempo real todas las cámaras comprimidas, y así tener una mejor secuencia de los hechos.

2.9.1 Aplicaciones CCTV

Antes se utilizaban este tipo de sistemas únicamente en el

campo de la seguridad, para disuadir o detectar robos, hoy en día, no sólo se utiliza en este campo, sino también para otros propósitos específicos como pueden ser los de la medicina, la educación o la lucha contra eventos antisociales.

Un sistema de CCTV puede ser instalado en los hogares, bancos, casinos, centros comerciales, vías de circulación, aeropuertos, áreas e instalaciones públicas, entre otros.

2.10 Medios de transmisión

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos.

Distinguimos dos tipos de medios:

- ✓ Guiados
- ✓ No guiados

En ambos casos la transmisión se realiza por medio de ondas electromagnéticas.

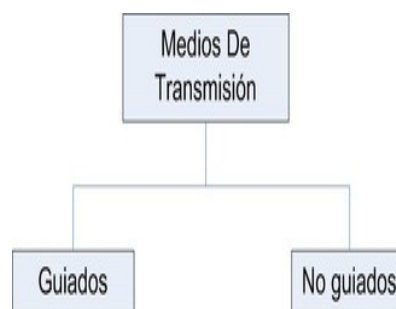


Figura 2.9 Medios de transmisión

2.11 Medios guiados

Conducen (guían) las ondas a través de un camino físico, estos medios son el cable coaxial, la fibra óptica y el par trenzado.

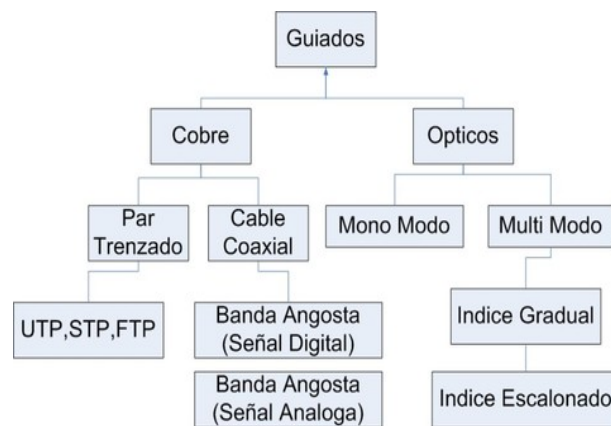


Figura 2.10 Medios de transmisión

2.11.1 Pares trenzados

Este consiste en dos alambres de cobre aislados, en general de 1mm de espesor. Los alambres se entrelazan en forma helicoidal, como en una molécula de DNA. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor.

Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre; en muchos casos pueden obtenerse transmisiones de varios megabits, en distancias de pocos kilómetros.

Debido a su adecuado comportamiento y bajo costo, los pares trenzados se utilizan ampliamente y es probable que se presencia permanezca por muchos años.

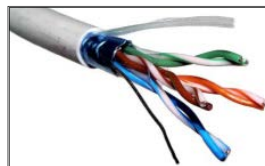


Figura 2.11 Pares trenzados

Existen dos tipos de par trenzado:

- ✓ Protegido: Shielded Twisted Pair (STP)
- ✓ No protegido: Unshielded Twisted Pair (UTP)

Las aplicaciones principales en las que se hace uso de cables de par trenzado son:

Bucle de abonado.- Es el último tramo de cable existente entre el teléfono de un abonado y la central a la que se encuentra conectado. Este cable suele ser UTP Cat.3 y en la actualidad es uno de los medios más utilizados para transporte de banda ancha, debido a que es una infraestructura que está implantada en el 100% de las ciudades.

Redes LAN.- En este caso se emplea UTP Cat.5, Cat.6 o Cat.7 para transmisión de datos, consiguiendo velocidades de varios centenares de Mbps.

Un ejemplo de este uso lo constituyen las redes 10/100/1000BASE-T.

Para conectar el cable UTP a los distintos dispositivos de red se usan unos conectores especiales, denominados RJ-45.

El conector RJ45 (RJ significa Registered Jack) es uno de los conectores principales utilizados con tarjetas de red Ethernet, que transmite información a través de cables de par trenzado.

Por este motivo, a veces se le denomina puerto Ethernet.

El conector RJ-45 es utilizado para enlazar redes de telefonía.

Podemos encontrar en diferentes formatos según nuestras necesidades.

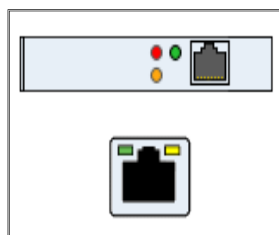


Figura 2.12 Conector RJ 45

2.11.1.1 Cable de par trenzado sin blindaje UTP

El cable de par trenzado sin blindaje es el tipo más frecuente de medio de comunicación que se usa actualmente, tiene una amplia difusión en telefonía

y en redes LAN.

Está formado por dos hilos, cada uno de los cuales está recubierto de material aislante; como Teflón o PVC, debido a que el primero genera poco humo en incendios.

Se distinguen dos tipos de recubrimiento:

El rígido (para cableado vertical y horizontal) y flexible (para patch cord).

Posee 4 pares: blanco azul-azul, blanco naranja- naranja, blanco verde-verde, blanco café-café.

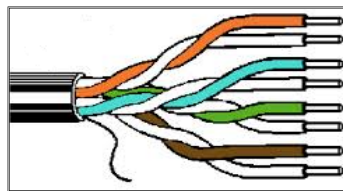


Figura 2.13 Par trenzado UTP

2.11.1.2 Cable de par trenzado blindado STP

El cable de par trenzado blindado combina las técnicas de blindaje, cancelación y trenzado de cables. Tiene una funda de metal o un recubrimiento de malla entrelazada que envuelve cada par de hilos aislados; lo que hace que tenga mayor protección que el UTP, protegiéndolo contra interferencias y ruido eléctrico, haciendo que sea difícil de instalar.

Es utilizado generalmente dentro de centros de informática por su capacidad y sus buenas características contra las radiaciones electromagnéticas.

La pantalla del STP, para que sea más eficaz, requiere una configuración de interconexión con tierra.

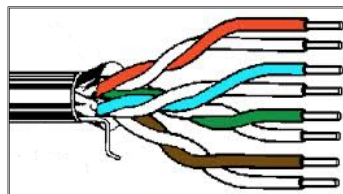


Figura 2.14 Par trenzado STP

2.11.1.3 Categorías de UTP

La especificación 568A Commercial Building Wiring Standard de la Asociación de Industrias Electrónicas e Industrias de la Telecomunicación (EIA/TIA) especifica el tipo de cable UTP que se utilizará en cada situación y construcción.

Dependiendo de la velocidad de transmisión ha sido dividida en diferentes categorías:

Categoría 1.- Hilo telefónico trenzado de calidad de voz (Cable de teléfono) no adecuado para las transmisiones de datos. Las características de transmisión del medio están especificadas hasta una frecuencia superior a 1MHz.

Categoría 2.- Cable par trenzado sin apantallar, datos a 4 Mbps (LocalTalk). Las características de transmisión del medio están especificadas hasta una frecuencia superior de 4 MHz., este cable consta de 4 pares trenzados de hilo de cobre.

Categoría 3.- Velocidad de transmisión típica de 10 Mbps (Ethernet), con este tipo de cables se implementa las redes Ethernet 10BaseT. Las características de transmisión del medio están especificadas hasta una frecuencia superior de 16 MHz., este cable consta de cuatro pares trenzados de hilo de cobre con tres entrelazados por pie.

Categoría 4.- La velocidad de transmisión llega hasta 20 Mbps. (Token Ring). Las características de transmisión del medio están especificadas hasta una frecuencia superior de 20 MHz., este cable consta de 4 pares trenzados de hilo de cobre.

Categoría 5.- Es una mejora de la categoría 4, puede transmitir datos hasta 100Mbps (Fast Ethernet) y las características de transmisión del medio

están especificadas hasta una frecuencia superior de 100 MHz., este cable consta de cuatro pares trenzados de hilo de cobre.

Categoría 6.- Es una mejora de la categoría anterior, puede transmitir datos hasta 1Gbps y las características de transmisión del medio están especificadas hasta una frecuencia superior a 250 MHz.

Categoría 7.- Es una mejor de la categoría 6, puede transmitir datos hasta 10 Gbps y las características de transmisión del medio están especificadas hasta una frecuencia superior a 600 MHz.

2.11.1.4 Consideraciones sobre el cableado de par trenzado

El cable de par trenzado se utiliza si:

- ✓ La LAN tiene una limitación de presupuesto.
- ✓ Se desea una instalación relativamente sencilla, donde las conexiones de los equipos sean simples.

No se utiliza el cable de par trenzado si:

- ✓ La LAN necesita un gran nivel de seguridad y se debe estar absolutamente seguro de la integridad de los datos.
- ✓ Los datos se deben transmitir a largas distancias y a altas velocidades.

2.11.2 Cable coaxial

El cable coaxial consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante.

Este material aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector.

La construcción del cable coaxial produce una buena combinación y un gran

ancho de banda y una excelente inmunidad al ruido.

El ancho de banda que se puede obtener depende de la longitud del cable; para cables de 1km, por ejemplo, es factible obtener velocidades de datos de hasta 10Mbps, y en cables de longitudes menores, es posible obtener velocidades superiores.

Se pueden utilizar cables con mayor longitud, pero se obtienen velocidades muy bajas. Los cables coaxiales se emplean ampliamente en redes de área local y para transmisiones de larga distancia del sistema telefónico.

Para su conexión se utilizan conectores BNC simples y en T.

En una red al final del cable principal de red se deben instalar resistencias especiales, resistores, para evitar la reflexión de las ondas de señal.

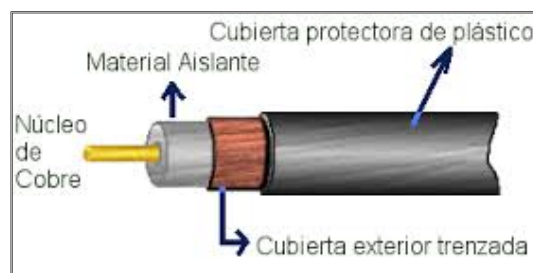


Figura 2.15 Componentes del Cable coaxial

2.11.2.1 Banda base (Baseband)

Es de bajo costo, tiene mayor inmunidad al ruido que el cable de pares y es usado en redes locales como:

10BASE-5.- Coaxial grueso, 5 segmentos c/u de 500 mts, 100 estaciones por segmento.

10BASE-2.- Coaxial delgado, 5 segmentos, c/u de 200 mts, 30 estaciones por segmento.

Se utiliza para transmisión digital, operando en modo halfduplex.

Está compuesto por un núcleo de cobre, aislante y malla conductora.

Tiene 50 ohmios y con cables de 1 km se alcanzan 10 Mbps.

Existen dos tipos de cable coaxial banda base: coaxial grueso (Thick) y coaxial fino (Thin).

2.11.2.2 Banda ancha (Broadband)

Es utilizado para infraestructura de TV por cable, para la transmisión de datos con el acceso a internet y también permite aplicaciones en tiempo real. Se conoce como la red HFC (Hybrid Fiber Coaxial).

Tiene un alcance de 5 Km, un ancho de banda de 300-450 Mhz y un tamaño de canal de TV de 6 Mhz. Es posible alcanzar hasta 150 Mbps, pero necesita amplificadores intermedios que conviertan el canal en unidireccional.

Broadband se utiliza para transmisión analógica y aunque cada canal es half duplex, con 2 se obtiene full duplex.

2.11.2.3 Consideraciones sobre el cable coaxial

En la actualidad es difícil que tenga que tomar una decisión sobre cable coaxial, no obstante, considere las siguientes características del cable coaxial.

Utilice el cable coaxial si necesita un medio que pueda:

- ✓ Transmitir voz, vídeo y datos.
- ✓ Transmitir datos a distancias mayores de lo que es posible con un cableado menos caro.
- ✓ Ofrecer una tecnología familiar con una seguridad de los datos aceptable.

2.11.3 Fibra Óptica

Es el medio de transmisión más novedoso dentro de los guiados y su uso se está masificando en todo el mundo reemplazando el par trenzado y el cable coaxial en casi todos los campos.

En este medio los datos se transmiten mediante una haz confinado de naturaleza óptica, de ahí su nombre, es mucho más caro y difícil de manejar pero sus ventajas sobre los otros medios lo convierten muchas veces en una muy buena elección al momento de observar rendimiento y calidad de transmisión.

Físicamente un cable de fibra óptica está constituido por un núcleo formado por una o varias fibras o hebras muy finas de cristal o plástico; un revestimiento de cristal o plástico con propiedades ópticas diferentes a las del núcleo, cada fibra viene rodeada de su propio revestimiento y una cubierta plástica para protegerla de humedades y el entorno.

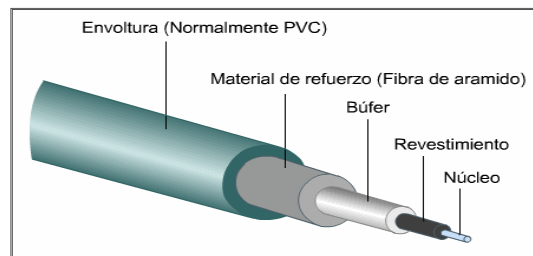


Figura 2.16 Fibra óptica

En el cable de fibra óptica las señales que se transportan son señales digitales de datos en forma de pulsos modulados de luz.

Esta es una forma relativamente segura de enviar datos debido a que, a diferencia de los cables de cobre que llevan los datos en forma de señales electrónicas, los cables de fibra óptica transportan impulsos no eléctricos.

Esto significa que el cable de fibra óptica no se puede pinchar y sus datos no se pueden robar.

El cable de fibra óptica es apropiado para transmitir datos a velocidades muy altas y con grandes capacidades debido a la carencia de atenuación de la señal y a su pureza.

2.11.3.1 Composición del cable de fibra óptica

Una fibra óptica consta de un cilindro de vidrio extremadamente delgado, denominado núcleo, recubierto por una capa de vidrio concéntrica, conocida

como revestimiento.

Las fibras a veces son de plástico. El plástico es más fácil de instalar, pero no puede llevar los pulsos de luz a distancias tan grandes como el vidrio.

Debido a que los hilos de vidrio pasan las señales en una sola dirección, un cable consta de dos hilos en envolturas separadas.

Un hilo transmite y el otro recibe.

Una capa de plástico de refuerzo alrededor de cada hilo de vidrio y las fibras Kevlar ofrece solidez.

En el conector de fibra óptica, las fibras de Kevlar se colocan entre los dos cables. Al igual que sus homólogos (par trenzado y coaxial), los cables de fibra óptica se encierran en un revestimiento de plástico para su protección.

Las transmisiones del cable de fibra óptica no están sujetas a intermodulaciones eléctricas y son extremadamente rápidas, comúnmente transmiten a unos 100 Mbps, con velocidades demostradas de hasta 1 gigabit por segundo (Gbps). Pueden transportar una señal (el pulso de luz) varios kilómetros.

Consideraciones sobre el cable de fibra óptica

El cable de fibra óptica se utiliza si:

- ✓ Necesita transmitir datos a velocidades muy altas y a grandes distancias en un medio muy seguro.

El cable de fibra óptica no se utiliza si:

- ✓ Tiene un presupuesto limitado.
- ✓ No tiene el suficiente conocimiento para instalar y conectar los dispositivos de forma apropiada.

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta.

El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo.

Alrededor de este conglomerado está la cubierta constituida de material plástico o similar que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad.

Permite un gran número de canales y velocidades muy altas, superiores al GHz. Tienen un Bc enorme (50Ghz máx., 2Ghz típico), Rmax enorme (2Gbps máx.), pequeño tamaño y peso, y una atenuación pequeña.

Es inmune a ruidos e interferencias y son difíciles de acceder. Tienen como inconvenientes el precio alto, la manipulación complicada, el encarecimiento de los costos de mano de obra y tendido.

Es un medio muy apropiado para largas distancias e incluso últimamente para LAN.

2.12 Medios no guiados

Son aquellos que no confinan las señales mediante ningún tipo de cable; estas señales se propagan libremente a través del medio, entre los más importantes se encuentran el aire y el vacío.



Figura 2.17 Medios no guiados

Los medios no guiados o sin cable han tenido gran acogida al ser un buen medio de cubrir grandes distancias y hacia cualquier dirección, su mayor logro se dio desde la conquista espacial a través de los satélites y su tecnología no para de cambiar.

Tanto la transmisión como la recepción de información se llevan a cabo mediante antenas.

A la hora de transmitir, la antena irradia energía electromagnética en el medio y en el momento de la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

La configuración para las transmisiones no guiadas puede ser direccional y omnidireccional.

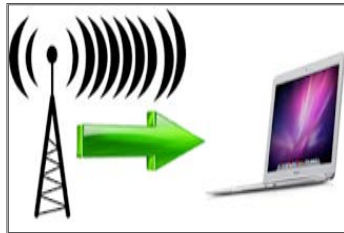


Figura 2.18 Medio no guiado (Transmisor-receptor)

2.13 Transmisión direccional

La energía emitida se concentra en un haz, para lo cual se requiere que la antena receptora y transmisora estén alineadas.

Cuanto mayor sea la frecuencia de transmisión, es más factible confinar la energía en una dirección.



Figura 2.19 Transmisión direccional

2.14 Transmisión omnidireccional

La antena transmisora emite en todas las direcciones espaciales y la receptora recibe igualmente en toda dirección.



Figura 2.20 Transmisión omnidireccional

2.15 Microondas

Son un tipo de onda electromagnética situada en el intervalo del milímetro al metro y cuya propagación puede efectuarse por el interior de tubos metálicos.

Se usa el espacio aéreo como medio físico.

Consiste en una antena tipo plato y circuitos que interconectan con la terminal del usuario.

- ✓ La información es digital.
- ✓ Se transmite en ondas de radio de corta longitud.
- ✓ Dirección de múltiples canales a múltiples estaciones.
- ✓ Pueden establecer enlaces punto a punto.

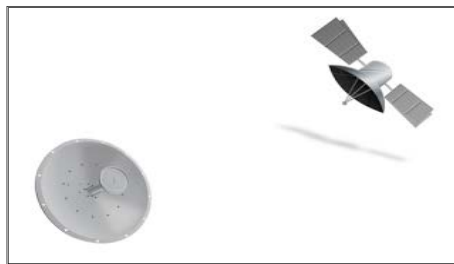


Figura 2.21 Microondas

Características

- ✓ Ancho de banda: entre 300 a 3.000 MHz.
- ✓ Algunos canales de banda superior, entre 3'5 GHz y 26 GHz.
- ✓ Es usado como enlace entre una empresa y un centro que funcione como centro de conmutación del operador, o como un enlace entre redes LAN.
- ✓ Para la comunicación de microondas terrestres se deben usar antenas parabólicas.
- ✓ Estas deben estar alineadas o tener visión directa entre ellas.
- ✓ Entre mayor sea la altura mayor el alcance.
- ✓ Pérdidas de datos, interferencias.
- ✓ Sensible a las condiciones atmosféricas.

2.15.1 Microondas terrestres

Radioenlace que provee conectividad entre dos sitios en línea. Se usa un equipo de radio con frecuencias de portadora por encima de 1 GHz.

La forma de onda emitida puede ser analógica convencionalmente en FM o digital.

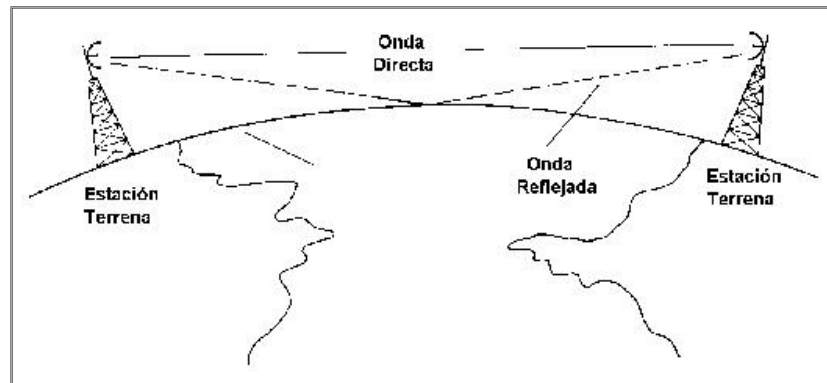


Figura 2.22 Enlace de microondas de línea de vista

Las principales aplicaciones de un sistema de microondas terrestre son:

- ✓ Telefonía básica (canales telefónicos).
- ✓ Telégrafo/Télex/Facsímile.
- ✓ Telefonía Celular (entre troncales).
- ✓ Canales de Televisión.
- ✓ Video.
- ✓ Datos.

Componentes

- ✓ Una antena con una corta y flexible guía de onda.
- ✓ Una unidad externa de RF (Radio Frecuencia).
- ✓ Una unidad interna de RF.

Características

- ✓ Frecuencia utilizadas entre los 12 GHz, 18 y 23 GHz.
- ✓ Conectan dos localidades entre 1 y 15 millas de distancia.
- ✓ El equipo de microondas que opera entre 2 y 6 GHz puede transmitir a distancias entre 20 y 30 millas.

A tener en cuenta.- El clima y el terreno son los mayores factores a considerar antes de instalar un sistema de microondas.

No se recomienda instalar sistemas en lugares donde no llueva mucho; en este caso deben usarse radios con frecuencias bajas.

Las consideraciones en terreno incluyen la ausencia de montañas o grandes cuerpos de agua las cuales pueden ocasionar reflexiones de multi-trayectorias.

2.15.2 Microondas por satélite

Se utilizan para:

- ✓ Difusión de televisión.
- ✓ Transmisión telefónica a larga distancia.
- ✓ Redes privadas.



Figura 2.23 Microondas por satélite

Su principal función es la de amplificar la señal, corregirla y retransmitirla a una o más antenas ubicadas en la tierra.

- ✓ Retransmiten información.
- ✓ Se usan como enlace entre receptores terrestres (estaciones base).
- ✓ El satélite funciona como un espejo sobre el cual la señal rebota.
- ✓ Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.

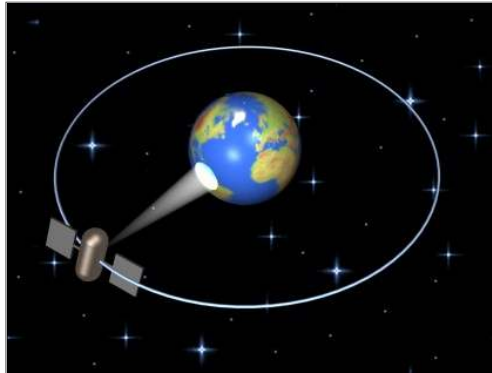


Figura 2.24 Satélite geoestacionario

2.16 Ondas de radio vs Microondas

- ✓ Las ondas de radio son omnidireccionales.
- ✓ Las ondas de radio, al poder reflejarse en el mar u otros objetos, pueden aparecer múltiples señales "hermanas".



Figura 2.25 Ondas de radio VS Microondas

- ✓ Las microondas son unidireccionales.
- ✓ Las microondas son más sensibles a la atenuación producida por la lluvia.

2.17 Bluetooth

Se utiliza principalmente en un gran número de productos como teléfonos, impresoras, módems y auriculares. Su uso es adecuado cuando puede haber dos o más dispositivos en un área reducida sin grandes necesidades de ancho de banda, su uso más común está integrado en teléfonos y PDA bien sea por medio de unos auriculares Bluetooth o en transferencia de ficheros.

Tiene la ventaja de simplificar el descubrimiento y configuración de los dispositivos, ya que éstos pueden indicar a otros los servicios que ofrecen, lo que redundaría en la accesibilidad de los mismos sin un control explícito de direcciones de red, permisos y otros aspectos típicos de redes tradicionales.

- ✓ Redes inalámbricas de área personal (WPAN).
- ✓ Posibilita la transmisión de voz y datos entre dispositivos.
- ✓ Utiliza un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.
- ✓ Facilita las comunicaciones entre equipos móviles y fijos.
- ✓ Elimina cables y conectores.
- ✓ Ofrece la posibilidad de crear pequeñas redes inalámbricas.
- ✓ Facilita la sincronización de datos entre equipos personales.



Figura 2.26 Identificador de conexión Bluetooth

Los dispositivos Bluetooth se componen fundamentalmente, de dos partes muy importantes:

- 1.- Un dispositivo de radio encargado de transmitir y modular la señal.
- 2.- Un controlador digital compuesto por un procesador de señales digitales, una CPU y de los diferentes interfaces con el dispositivo anfitrión.

2.18 Wi-Fi

Es un sistema de envío de datos sobre redes de computadores que utilizan ondas de radio en lugar de cables, este sistema está presente en:

- ✓ Ordenadores personales
- ✓ Consolas de videojuegos
- ✓ Smartphone
- ✓ Reproductores de audio digital.



Figura 2.27 Identificador de conexión WiFi

Estos dispositivos pueden conectarse a internet a través de un punto de acceso de red inalámbrica.

Dicho punto de acceso tiene un alcance de unos 20 metros (65 pies) en interiores y al aire libre una distancia mayor.

Pueden cubrir grandes áreas la superposición con múltiples puntos de acceso.

Wi-Fi es similar a la red Ethernet tradicional y como tal el establecimiento de comunicación necesita una configuración previa.

Utiliza el mismo espectro de frecuencia que Bluetooth con una potencia de salida mayor que lleva a conexiones más sólidas. A veces se denomina a Wi-Fi la Ethernet sin cables, aunque esta descripción no es muy precisa.

Se adecua mejor para redes de propósito general; permite conexiones más rápidas, un rango de distancias mayor y mejores mecanismos de seguridad.

Puede compararse la eficiencia de varios protocolos de transmisión inalámbrica, como Bluetooth y Wi-Fi, por medio de la capacidad espacial bits por segundo y metro cuadrado.

2.19 Modos de transmisión

La comunicación en los medios informáticos se realiza de dos maneras: en paralelo y en serie.

2.19.1 Paralelo

Todos los bits se transmiten simultáneamente, existiendo luego un tiempo antes de la transmisión del siguiente bloque.

Este tipo de transmisión tiene lugar en el interior de una máquina o entre máquinas cuando la distancia es muy corta.

La principal ventaja de este modo de transmitir datos es la velocidad de transmisión y la mayor desventaja es el costo.

También puede llegar a considerarse una transmisión en paralelo, aunque se realice sobre una sola línea, al caso de multiplexación de datos, donde los diferentes datos se encuentran intercalados durante la transmisión.

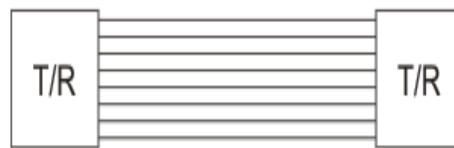


Figura 2.28 Transmisión en paralelo

2.19.2 Serie

En este caso los n bits que componen un mensaje se transmiten uno detrás de otro por la misma línea.

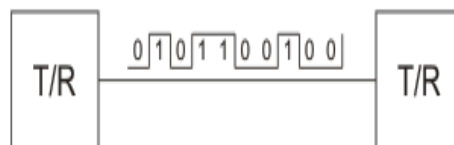


Figura 2.29 Transmisión en serie

A la salida de una máquina los datos en paralelo se convierten los datos en serie, los mismos se transmiten y luego en el receptor tiene lugar el proceso inverso, volviéndose a obtener los datos en paralelo.

La secuencia de bits transmitidos es por orden de peso creciente y generalmente el último bit es de paridad. Un aspecto fundamental de la transmisión en serie es el sincronismo, entendiéndose como tal al procedimiento mediante el cual transmisor y receptor reconocen los ceros y unos de los bits de igual forma.

El sincronismo puede tenerse a nivel de bit, de byte o de bloque, donde en cada caso se identifica el inicio y finalización de los mismos.

Dentro de la transmisión serie existen dos formas:

2.19.2.1 Transmisión asincrónica

Es también conocida como Star/stop, requiere de una señal que identifique el inicio del carácter y a la misma se la denomina bit de arranque. También se requiere de otra señal denominada señal de parada que indica la finalización del carácter o bloque.

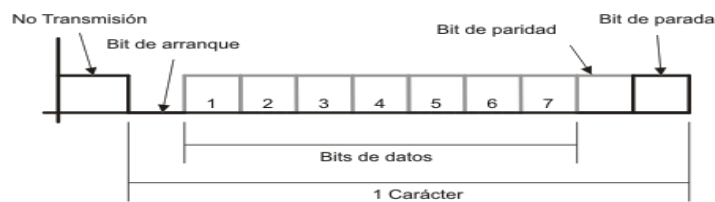


Figura 2.30 Formato de un caracter

Generalmente cuando no hay transmisión, una línea se encuentra en un nivel alto.

Tanto el transmisor como el receptor, saben cuál es la cantidad de bits que componen el carácter.

Los bits de parada son una manera de fijar qué delimita la cantidad de bits del carácter y cuando se transmite un conjunto de caracteres, luego de los bits de parada existe un bit de arranque entre los distintos caracteres.

A pesar de ser una forma comúnmente utilizada, la desventaja de la transmisión asincrónica es su bajo rendimiento, puesto que como en el caso del ejemplo, el carácter tiene 7 bits pero para efectuar la transmisión se requieren 10, o sea que del total de bits transmitidos solo el 70% pertenecen a datos.

2.19.2.2 Transmisión sincrónica

En este tipo de transmisión es necesario que el transmisor y el receptor utilicen la misma frecuencia de clock en ese caso la transmisión se efectúa en bloques, debiéndose definir dos grupos de bits denominados delimitadores, mediante los cuales se indica el inicio y el fin de cada bloque.

Este método es más efectivo por que el flujo de información ocurre en forma uniforme, con lo cual es posible lograr velocidades de transmisión más altas. Para lograr el sincronismo, el transmisor envía una señal de inicio de transmisión mediante la cual se activa el clock del receptor; a partir de dicho instante transmisor y receptor se encuentran sincronizados.

Otra forma de lograr el sincronismo es mediante la utilización de códigos auto sincronizantes los cuales permiten identificar el inicio y el fin de cada bit.

2.20 Canal de Comunicación

Se denomina así al recurso físico que hay que establecer entre varios medios de transmisión para establecer la comunicación.

Al canal de comunicación también se lo denomina vínculo o enlace.

2.21 Tipos de comunicación

En los canales de comunicación existen tres tipos de transmisión.

2.21.1 Simplex

En este caso el transmisor y el receptor están perfectamente definidos y la comunicación es unidireccional. Con esta fórmula es difícil la corrección de errores causados por deficiencias de línea.

Ej. La señal de televisión, radiodifusión.

Este tipo de comunicaciones los receptores no necesitan enviar ningún tipo de dato al transmisor.



Figura 2.31 Comunicación simplex

2.21.2 Duplex o Semi-duplex

En este caso ambos extremos del sistema de comunicación cumplen funciones de transmisor y receptor y los datos se desplazan en ambos sentidos pero no simultáneamente. Este método también se denomina en dos sentidos alternos.

Ej. El walkie - talkie.

Este tipo de comunicación se utiliza habitualmente en la interacción entre terminales y un computador central.



Figura 2.32 Comunicación duplex

2.21.3 Full Duplex

El sistema es similar al duplex, pero los datos se desplazan en ambos sentidos simultáneamente.

Para ello ambos transmisores poseen diferentes frecuencias de transmisión o dos caminos de comunicación separados, es decir, que las dos estaciones simultáneamente pueden enviar y recibir datos y así pueden corregir los errores

de manera instantánea y permanente.

Ej. El teléfono.

Para el intercambio de datos entre computadores este tipo de comunicaciones son más eficientes que las transmisiones semi-duplex.

2.22 Redes IP

Desde que el ser humano tiene capacidad de comunicarse ha desarrollado mecanismos y sistemas que les permiten establecer esta

comunicación a distancias superiores de las alcanzadas por sus propios medios.

En la era de la información, las redes de comunicación tienen una gran importancia en la sociedad, ya que permiten compartir de manera universal la información y además han permitido que diferentes sectores, como por ejemplo telecomunicaciones, datos, radio y televisión se fusionen en uno solo.

Las redes de computadores actuales están compuestas por una variedad de dispositivos, técnicas y sistemas de comunicación.

2.23 Topologías de RED

El término topología se emplea para referirse a la disposición geométrica de las estaciones de una red y los cables que las conectan y al trayecto seguido por las señales a través de la conexión física.

La topología de la red es pues, la disposición de los diferentes componentes de una red y la forma que adopta el flujo de información.

Las topologías fueron ideadas para establecer un orden que evitase el caos que se produciría si las estaciones de una red fuesen colocadas de forma aleatoria.

La topología tiene por objetivo hallar cómo todos los usuarios pueden conectarse a todos los recursos de red de la manera más económica y eficaz; al mismo tiempo, capacita a la red para satisfacer las demandas de los usuarios con un tiempo de espera lo más reducido posible.

Para determinar qué topología resulta más adecuada para una red concreta se tienen en cuenta numerosos parámetros y variables, como el número de máquinas que se van a interconectar, el tipo de acceso al medio físico deseado.

Dentro del concepto de topología se pueden diferenciar dos aspectos:

- ✓ Topología física.
- ✓ Topología lógica.

2.23.1 La topología física

Se refiere a la disposición física de las máquinas, los dispositivos de red y el cableado.

Dentro de la topología física se pueden diferenciar dos tipos de conexiones:

- ✓ Punto a punto.
- ✓ Multipunto.

En las conexiones punto a punto existen varias conexiones entre parejas de estaciones adyacentes, sin estaciones intermedias.

Las conexiones multipunto cuentan con un único canal de transmisión, compartido por todas las estaciones de la red.

Cualquier dato o conjunto de datos que envíe una estación es recibido por todas las demás estaciones.

2.23.2 La topología lógica

Se refiere al trayecto seguido por las señales a través de la topología física, es decir, la manera en que las estaciones se comunican a través del medio físico.

Las estaciones se pueden comunicar entre sí directa o indirectamente, siguiendo un trayecto que viene determinado por las condiciones de cada momento.

2.24 Tipos de topologías

La topología de una red local es la distribución física en la cual se encuentran dispuestos los ordenadores que la componen.

Hay que tener en cuenta un número de factores para determinar qué topología es la más apropiada para una situación dada.

Existen varios tipos:

- ✓ Bus

- ✓ Anillo
- ✓ Estrella
- ✓ Árbol
- ✓ Malla
- ✓ Híbridas
- ✓ Híbridas Estrella-Bus
- ✓ Híbridas estrella-Anillo

2.24.1 Topología de Bus

En una topología de bus todos los equipos de una red están unidos a un cable continuo o segmento que los conecta en línea recta.

En esta topología en línea recta el paquete se transmite a todos los adaptadores de red en ese segmento.

Debido a la forma de transmisión de las señales eléctricas a través de este cable, sus extremos deben estar terminados por dispositivos de hardware denominados terminadores que actúan como límites de la señal y definen el segmento.

Si se produce una rotura en cualquier parte del cable o si un extremo no está terminado, la señal balanceará hacia adelante y hacia atrás a través de la red y la comunicación se detendrá.

El número de equipos presentes en un bus también afecta al rendimiento de la red; cuantos más equipos haya en el bus, mayor será el número de equipos esperando para insertar datos en el bus y en consecuencia la red irá más lenta.

Además, debido al modo en que los equipos se comunican en una topología de bus, puede producirse mucho ruido.

Ruido es el tráfico generado en la red cuando los equipos intentan comunicarse entre sí simultáneamente.

Un incremento del número de equipos produce un aumento del ruido y la correspondiente reducción de la eficacia de la red.

Consideraciones sobre el cable:

Los dos extremos del cable deben tener terminadores.

Todos los adaptadores de red reciben el paquete de datos.

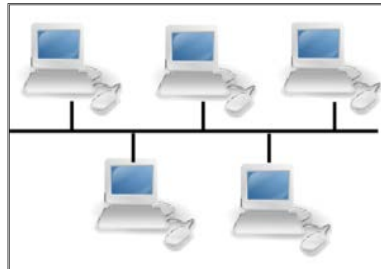


Figura 2.33 Topología bus

2.24.2 Topología en Anillo

En una topología en anillo los equipos están conectados con un cable de forma circular; a diferencia de la topología de bus no hay extremos con terminaciones.

Las señales viajan alrededor del bucle en una dirección y pasan a través de cada equipo que actúa como repetidor para amplificar la señal y enviarla al siguiente equipo.

A mayor escala en una topología en anillo, múltiples LAN pueden conectarse entre sí utilizando el cable coaxial o el cable de fibra óptica.

La ventaja de una topología en anillo es que cada equipo actúa como repetidor, regenerando la señal y enviándola al siguiente equipo, conservando la potencia de la señal.

El método de transmisión de datos alrededor del anillo se denomina paso de testigo (token passing).

Paso de testigo.- Es una serie especial de bits que contiene información de control, la posesión del testigo permite a un dispositivo de red transmitir datos a la red.

Cada red tiene un único testigo.

El equipo emisor retira el testigo del anillo y envía los datos solicitados alrededor del anillo.

Cada equipo pasa los datos hasta que el paquete llega el equipo cuya dirección coincide con la de los datos, el equipo receptor envía un mensaje al equipo emisor indicando que se han recibido los datos.

Tras la verificación, el equipo emisor crea un nuevo testigo y lo libera a la red.

La ventaja de una topología en anillo es que puede gestionar mejor entornos con mucho tráfico que las redes con bus.

Además, hay mucho menos impacto del ruido en las topologías en anillo.

El inconveniente de una topología en anillo es que los equipos sólo pueden enviar los datos de uno en uno en un único Token Ring.

La topología en anillo son normalmente más caras que las tecnologías de bus.

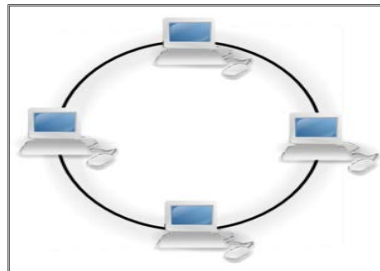


Figura 2.34 Topología anillo

2.24.3 Topología en Estrella

En una topología en estrella los segmentos de cable de cada equipo en la red están conectados a un componente centralizado o concentrador.

Un concentrador es un dispositivo que conecta varios equipos juntos.

En una topología en estrella las señales se transmiten desde el equipo a través del concentrador a todos los equipos de la red.

A mayor escala, múltiples LAN pueden estar conectadas entre sí en una topología en estrella.

Una ventaja de la topología en estrella es que si uno de sus equipos falla, únicamente este equipo es incapaz de enviar o recibir datos el resto de la red funciona normalmente.

El inconveniente de utilizar esta topología es que debido a que cada equipo está conectado a un concentrador, si éste falla, fallará toda la red. Además, en una topología en estrella el ruido se crea en la red.

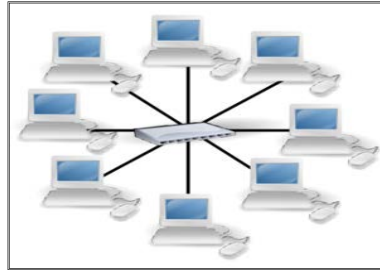


Figura 2.35 Topología estrella

2.24.4 Topología en Árbol

En una topología en árbol, los nodos están colocados en forma de árbol. Desde una visión topológica la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión.



Figura 2.36 Topología árbol

2.24.5 Topología de Malla

En una topología de malla cada equipo está conectado a cada uno del

resto de equipos por un cable distinto.

Esta configuración proporciona rutas redundantes a través de la red de forma que si un cable falla; otro transporta el tráfico y la red sigue funcionando.

A mayor escala, múltiples redes LAN pueden estar en estrella conectadas entre sí en una topología de malla utilizando red telefónica conmutada, un cable coaxial o el cable de fibra óptica.

Una de las ventajas de las topologías de malla es su capacidad de respaldo al proporcionar múltiples rutas a través de la red.

Debido a que las rutas redundantes requieren más cable del que se necesita en otras topologías, una topología de malla puede resultar cara.

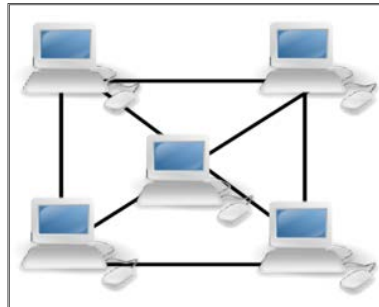


Figura 2.37 Topología malla

2.24.6 Topologías Híbridas

En una topología híbrida se combinan dos o más topologías para formar un diseño de red completo.

Raras veces se diseñan las redes utilizando un solo tipo de topología.

Por ejemplo, es posible que desee combinar una topología en estrella con una topología de bus para beneficiarse de las ventajas de ambas.

Importante.- En una topología híbrida, si un solo equipo falla, no afecta al resto de la red.

Normalmente se utilizan dos tipos de topología híbridas:

- ✓ Topología en estrella-bus
- ✓ Topología en estrella-anillo.

2.24.6.1 En estrella-bus

En una topología en estrella-bus, varias redes de topología en estrella están conectadas a una conexión en bus.

Cuando una configuración en estrella está llena, podemos añadir una segunda en estrella y utilizar una conexión en bus para conectar las dos topologías en estrella.

En una topología en estrella-bus, si un equipo falla, no afectará al resto de la red.

Sin embargo, si falla el componente central o concentrador que une todos los equipos en estrella, todos los equipos adjuntos al componente fallarán y serán incapaces de comunicarse.

2.24.6.2 En estrella-anillo

En la topología en estrella-anillo, los equipos están conectados a un componente central al igual que en una red en estrella, sin embargo estos componentes están enlazados para formar una red en anillo.

Al igual que la topología en estrella-bus, si un equipo falla, no afecta al resto de la red.

Utilizando el paso de testigo, cada equipo de la topología en estrella-anillo tiene las mismas oportunidades de comunicación, esto permite un mayor tráfico de red entre segmentos que en una topología en estrella-bus.

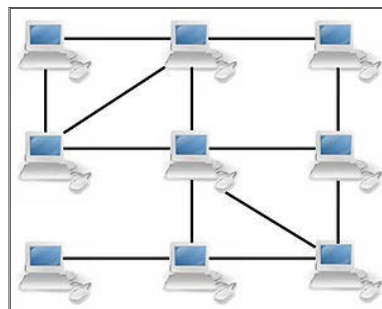


Figura 2.38 Topología híbridas

2.25 Protocolos de RED

Así como nosotros tenemos un lenguaje y unas formas estándar para comunicarnos, las redes también tienen una forma estándar de comunicarse y es a esto lo que llamamos protocolo.

Podemos definir un protocolo como el conjunto de normas que regulan la comunicación (establecimiento, mantenimiento y cancelación) entre los distintos componentes de una red informática.

Existen dos tipos de protocolos:

- ✓ Protocolos de bajo nivel.
- ✓ Protocolos de red.

2.25.1 Los protocolos de bajo nivel

Los protocolos de bajo nivel controlan el acceso al medio físico, lo que se conoce como MAC (Media Access Control) y además parte del nivel de transmisión de datos, ya que se encargan también de las señales de temporización de la transmisión.

Sobre todos los protocolos de bajo nivel MAC, se asientan los protocolos de control lógico del enlace o LLC (Logical Link Control), definidos en el estándar IEEE 802.2.

2.25.2 Los protocolos de red

Organizan la información (controles y datos) para su transmisión por el medio físico a través de los protocolos de bajo nivel. Veamos algunos de ellos:

IPX.- Es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell NetWare.

Es un protocolo orientado a paquetes y no orientado a conexión (esto es, no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino).

SPX.- Actúa sobre IPX para asegurar la entrega de los paquetes.

NetBIOS.- Es un programa que permite que se comuniquen aplicaciones en diferentes ordenadores dentro de una LAN.

Desarrollado originalmente para las redes de ordenadores personales IBM, fue adoptado posteriormente por Microsoft.

NetBIOS se usa en redes con topologías Ethernet y token ring.

No permite por sí mismo un mecanismo de enrutamiento por lo que no es adecuado para redes de área extensa (MAN), en las que se deberá usar otro protocolo para el transporte de los datos (por ejemplo, el TCP).

NetBIOS puede actuar como protocolo orientado a conexión o no (en sus modos respectivos sesión y datagrama). En el modo sesión dos ordenadores establecen una conexión para establecer una conversación entre los mismos.

Mientras que en el modo datagrama cada mensaje se envía independientemente.

Una de las desventajas de NetBIOS es que no proporciona un marco estándar o formato de datos para la transmisión.

NetBEUI.- Es una versión mejorada de NetBIOS que sí permite el formato o arreglo de la información en una transmisión de datos. También desarrollado por IBM y adoptado después por Microsoft, es actualmente el protocolo predominante en las redes Windows NT, LAN Manager y Windows para trabajo en grupo.

Aunque NetBEUI es la mejor elección como protocolo para la comunicación dentro de una LAN, el problema es que no soporta el enrutamiento de mensajes hacia otras redes, que deberá hacerse a través de otros protocolos (IPX o TCP/IP). Un método usual es instalar tanto NetBEUI como

TCP/IP en cada estación de trabajo y configurar el servidor para usar NetBEUI para la comunicación dentro de la LAN y TCP/IP para la comunicación hacia afuera de la LAN.

AppleTalk.- Es el protocolo de comunicación para ordenadores Apple Macintosh y viene incluido en su sistema operativo, de tal forma que el usuario no necesita configurarlo. Existen tres variantes de este protocolo:

- ✓ **LocalTalk.-** La comunicación se realiza a través de los puertos serie de las
- ✓ estaciones. La velocidad de transmisión es pequeña pero sirve por ejemplo para compartir impresoras.
- ✓ **Ethertalk.-** Es la versión para Ethernet. Esto aumenta la velocidad y facilita aplicaciones como por ejemplo la transferencia de archivos.
- ✓ **TokenTalk.-** Es la versión de Appletalk para redes Tokenring.

2.26 Modelo de referencia OSI

Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO creó el modelo de referencia OSI para lograr una estandarización internacional de los protocolos.

Este modelo se ocupa de la interconexión de sistemas abiertos a la comunicación y está dividido en 7 capas, entendiéndose por capa una entidad que realiza de por sí una función específica.

Los principios que se aplicaron para su división en capas son:

- 1.- Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
- 2.- Cada capa debe realizar una función bien definida.
- 3- La función de capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.
- 4.- Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
- 5.- La cantidad de capas debe ser suficientes para no tener que agrupar

funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

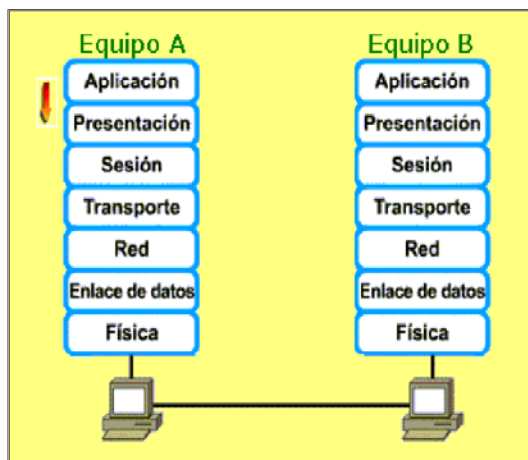


Figura 2.39 Modelo OSI

2.27 Capas del modelo OSI

2.27.1 Capa Física

Es la que se encarga de la topología de la red y de las conexiones globales de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.

Definir las características materiales (componentes y conectores mecánicos) y características eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

Transmitir el flujo de bits a través del medio.

Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.

Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

2.27.2 Capa de Enlace

Esta capa se ocupa del direccionamiento físico, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo.

Es uno de los aspectos más importantes que revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular la forma de la conexión entre computadoras así determinando el paso de tramas (trama = unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes), verificando su integridad y corrigiendo errores, por lo cual es importante mantener una excelente adecuación al medio físico los más usados son el cable UTP, par trenzado o de 8 hilos, con el medio de red que re-direcciona las conexiones mediante un router.

Dadas estas situaciones cabe recalcar que el dispositivo que usa la capa de enlace es el switch que se encarga de recibir los datos del router y enviar cada uno de estos a sus respectivos destinatarios (servidor -> computador cliente o algún otro dispositivo que reciba información como celulares, tabletas y diferentes dispositivos con acceso a la red).

Dada esta situación se determina como el medio que se encarga de la corrección de errores, manejo de tramas, protocolización de datos (se llaman protocolos a las reglas que debe seguir cualquier capa del modelo OSI).

2.27.3 Capa de Red

Se encarga de identificar el enrutamiento existente entre una o más redes.

Las unidades de información se denominan paquetes y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

Enrutables.- Viajan con los paquetes (IP, IPX, APPLETALK).

Enrutamiento.- Permiten seleccionar las rutas (RIP, IGRP, EIGRP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente.

Los dispositivos que facilitan tal tarea se denominan encaminadores o enrutadores, aunque es más frecuente encontrarlo con el nombre en inglés routers.

Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne.

Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

2.27.4 Capa de Transporte

Capa encargada de efectuar el transporte de los datos que se encuentran dentro del paquete de la máquina origen a la de destino, independizándolo del tipo de red física que esté utilizando. La PDU de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión.

Trabajan por lo tanto con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP: Puerto (191.16.200.54:80).

2.27.5 Capa de Sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda

efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

2.27.6 Capa de Presentación

El objetivo es encargarse de la representación de la información de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma.

En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Esta capa también permite cifrar los datos y comprimirlos; por lo tanto, podría decirse que esta capa actúa como un traductor.

2.27.7 Capa de Aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros.

Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación; suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

2.28 Direccionamiento IP

Una dirección IP es un número de identificación de un ordenador o de una red subred; depende de la máscara que se utiliza.

Dirección IP es una secuencia de unos y ceros de 32 bits expresada en cuatro octetos (4 byte) separados por puntos.

Para hacer más comprensible se denomina en decimal como cuatro números separados por puntos.

En binario 10101100.00011000.00000111.00101011

En decimal 172. 24. 7. 43

Una dirección IP consta de dos partes.

La primera parte identifica dirección de la red y la segunda sirve para identificar los equipos en la red.

Para saber que rango de bits corresponde para cada parte se utiliza la máscara.

Máscara es combinación de 32 bits expresados en cuatro octetos (4 byte) separados por puntos. Es utilizada para describir cuál es la porción de una dirección IP que se refiere a la red o subred y cuál es la que se refiere al host.

La máscara se utiliza para extraer información de red o subred de la dirección IP.

Cuadro 2.5

Dirección IP y máscara

Dirección IP			
192	168	15	43
11000000	10101000	1111	101011
Máscara			
255	255	255	0
11111111	11111111	11111111	0
Dirección de red			Dirección de host

Fuente.- http://www.marbit.es/index_ip.html

La dirección IP es el identificador de cada host dentro de su red de redes, cada host conectado a una red, tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host.

En el caso de internet, no puede haber dos ordenadores con dos direcciones IP públicas iguales, pero si podríamos tener dos ordenadores con la misma dirección IP, siempre y cuando pertenezcan a redes independientes entre sí y sin que exista ningún camino posible que las comunique.

2.29 Clasificación de la direcciones IP

Las IP son un elemento fundamental de cualquier red informática, tanto de Internet como de redes privadas.

Así tenemos IP fija y dinámica o entre IP pública y privada.

Las IP públicas y privadas no son diferentes en sí mismas, como tampoco lo son las IP fijas y dinámicas, pero pueden tener una especie de apellido.

Tienen una forma y una función muy parecidas pero se utilizan en casos distintos.

2.29.1 Direcciones IP públicas

Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet.

Algunos ejemplos son: los servidores que alojan sitios web como Google, los router o modems que dan a acceso a Internet, otros elementos de hardware que forman parte de su infraestructura, etc.

Las IP públicas son siempre únicas. No se pueden repetir.

Dos equipos con IP de ese tipo pueden conectarse directamente entre sí.

Ejemplo, un router con un servidor web. O dos servidores web entre sí.

Son visibles en todo internet, un computador con una IP pública es accesible (visible) desde cualquier otro computador conectado a internet.

Para conectarse a internet es necesario tener una dirección IP pública.

2.29.2 Direcciones IP privadas

Se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada. En general, en redes que no sean la propia Internet y utilicen su mismo protocolo (el mismo "idioma" de comunicación).

Las IP privadas están en cierto modo aisladas de las públicas.

Se reservan para ellas determinados rangos de direcciones, estos son:

Para IPv4

De 10.0.0.0 a 10.255.255.255

Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers.

Se utilizan en las empresas para los puestos de trabajo.

Los computadores con direcciones IP privadas pueden salir a internet por medio de un router o proxy que tenga una IP pública, sin embargo desde internet no se puede acceder a computadores con direcciones IP privadas.

2.29.3 Direcciones IP estáticas

Su nombre se debe a que no cambia, como ya habrás imaginado. El equipo o dispositivo al que se le asigna tiene siempre la misma. Ya sea en Internet (IP fija pública) o en una red doméstica o empresarial (IP fija privada).

Se utilizan sobre todo en casos donde es importante la estabilidad.

Para hacer más rápidas o permanentes las conexiones, evitar fallos o interrupciones de un servicio cualquiera, tener un control exclusivo de una cierta IP, etc.

Son de uso común por ejemplo en proveedores de telefonía y vídeo por Internet (VoIP) como Skype. También en servidores y servicios de alojamiento web. O en sistemas de redes privadas virtuales (VPN) al estilo de LogMeIn o TeamViewer, que permiten el acceso seguro y a distancia a un PC.

Es raro que un usuario particular tenga una IP fija pública. En general suele implicar un coste adicional y no las ofrecen todos los proveedores de acceso a Internet (ISP).

Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP.

Las direcciones IP públicas estáticas son las que utilizan los servidores de internet con objeto de que estén siempre localizables por los usuarios de internet.

2.29.4 Direcciones IP dinámicas

Las IP de este tipo son variables, un equipo o dispositivo puede tener una IP en un cierto momento y una distinta en otro.

No hay una norma fija sobre la frecuencia con que pueden cambiar.

A veces se mantienen iguales durante mucho tiempo, mientras que otras cambian a menudo.

Muchos proveedores de Internet asignan IP dinámicas a sus clientes. Si uno de ellos se desconecta de Internet y ya "no necesita" su IP, el proveedor puede reutilizarla asignándosela a otro cliente que se conecte.

La reutilización de IP optimiza recursos y abarata costos.

Imagina a tu IP como un hotel. Tiene un número limitado de habitaciones (IP). Es mejor usar una misma habitación (una misma IP) para varios clientes que mantener la habitación cerrada (la IP sin usar) a la espera de que vuelva un cliente específico.

En redes privadas también suelen usarse las IP dinámicas. Entre otras cosas porque eso facilita mucho su configuración y ampliarlas con nuevos equipos o dispositivos.

Un host que se conecte a la red mediante IP dinámica cada vez lo hará con una dirección IP distinta.

Los proveedores de internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP disponibles y es muy improbable que todos los clientes se conecten simultáneamente internet.

2.29.5 El DHCP

Las IP dinámicas pueden ser públicas o privadas, ambas se asignan mediante lo que se llama DHCP.

Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Cuando un equipo se conecta a internet u otra red, el DHCP le atribuye una IP única (que no tenga ningún otro equipo).

Si el equipo se desconecta, el DHCP libera su IP, queda disponible para otro equipo o para reasignársela al anterior si vuelve a conectarse.

El proceso del DHCP es automático. Evita configurar a mano todos los dispositivos de la red uno a uno, u otros nuevos que se añadan a ella. Basta una configuración previa muy sencilla del denominado servidor DHCP.

Él es quien asigna las IP a los equipos, dispositivos o adaptadores de red (los clientes DHCP).

Los proveedores de Internet usan el DHCP para atribuir IP dinámicas públicas a sus clientes. Así pueden conectarse con ellas a Internet. De modo similar, un router doméstico o empresarial atribuye IP dinámicas privadas a los equipos que forman la red. Eso les permite conectarse entre sí.

2.30 Tipos de direcciones IP

El TCP/IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada.

Únicamente el NIC asigna las direcciones IP, aunque si una red no está conectada a internet, dicha red puede determinar su propio sistema de numeración.

Conceptualmente, cada dirección está compuesta por un par (RED (netid), y Dir. Local (hostid)) en donde se identifica la red y el host dentro de la red.

La clase se identifica mediante las primeras secuencias de bits, a partir de los 3 primeros bits de orden más alto.

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red.

Los cuatro formatos, Clase A hasta Clase D, aunque últimamente se han añadido la Clase E para un futuro, más ciertas direcciones especiales.

Cuando se cancela el identificador de host, es decir cuando los bits reservados para los equipos de la red se reemplazan por ceros (Ej. 194.28.12.0), se obtiene lo que se llama dirección de red.

Esta dirección no se puede asignar a ninguno de los equipos de la red.

Red por defecto (default).- La dirección IP de 0.0.0.0 se utiliza para la red por defecto.

Broadcast.- Los mensajes que se dirigen a todas las computadoras en una red se envían como broadcast estos mensajes utilizan siempre la dirección IP 255.255.255.255.

Loopback.- Por último la siguiente dirección IP es la interna de tu PC, conocida como local host o dirección de loopback, en todos los equipos es la misma: 127.0.0.1.

Se utiliza comúnmente para localizar averías y pruebas de la red.

2.30.1 Dirección IP Clase A

Las direcciones de clase A corresponden a redes muy grandes con muchas máquinas, tales como las de una gran compañía internacional.

Las direcciones en decimal son 0.1.0.0 hasta la 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

En redes de la clase A, el valor del bit en el primer octeto es siempre 0.

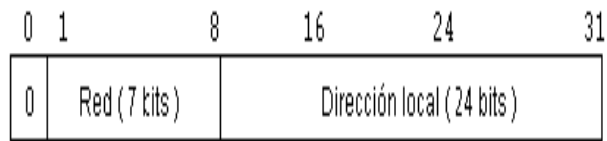


Figura 2.40 Dirección de 32 bits Clase A

2.30.2 Dirección IP Clase B

Las direcciones de Clase B sirven para redes de tamaño intermedio.

Un buen ejemplo es un campus grande de la universidad y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0.

Las direcciones de la clase B también incluyen el segundo octeto como parte del identificador neto.

Esto significa que hay 16,384 (2¹⁴) redes de la clase B con 65,534 (2¹⁶ - 2) host posibles cada uno para un total de 1, 073, 741,824 (2²⁰) direcciones únicas del IP.

Las redes de la clase B tienen un primer bit con valor de 1, segundo bit con valor de 0 en el primer octeto.

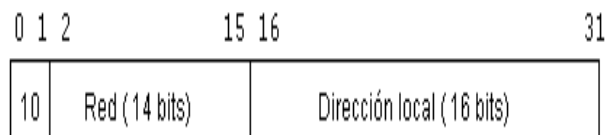


Figura 2.41 Dirección de 32 bits Clase B

2.30.3 Dirección IP Clase C

Las direcciones de la clase C se utilizan comúnmente para los negocios pequeños a mediados de tamaño, tienen sólo 8 bits para la dirección local o (host) y 21 bits para red.

Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, las direcciones de la clase C también incluyen a segundos y terceros octetos como parte del identificador neto.

Esto significa que hay 2, 097,152 (2²¹) redes de la clase C con 254 (2⁸ -2) host posibles cada uno para un total de 536, 870,912 (2²⁹) direcciones únicas del IP.

Las redes de la clase C tienen un primer bit con valor de 1, segundo bit con valor de 1 y de un tercer bit con valor de 0 en el primer octeto.

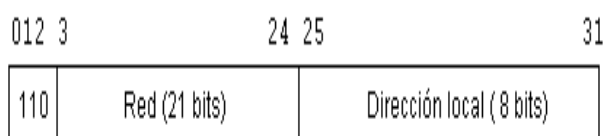


Figura 2.42 Dirección de 32 bits Clase C

2.30.4 Dirección IP Clase D

Utilizado para los multicast, la clase D es levemente diferente de las primeras tres clases.

El rango es desde 224.0.0.0 hasta 239.255.235.255, los otros 28 bits se utilizan para identificar el grupo de computadoras al que el mensaje del multicast está dirigido.

La clase D totaliza 1/16ava (2⁶, 435,456 o 2²⁸) de las direcciones disponibles del IP. Tiene un primer bit con valor de 1, segundo bit con valor de 1, tercer bit con valor de 1 y cuarto bit con valor de 0.



Figura 2.43 Dirección de 32 bits Clase D

2.30.5 Dirección IP Clase E

La clase E se utiliza para propósitos experimentales solamente, (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el

247.255.255.255, los otros 28 bits se utilizan para identificar el grupo de computadoras que el mensaje del multicast está dirigido.

La clase E totaliza 1/16ava (268, 435,456 o 228) de las direcciones disponibles del IP.

Tiene un primer bit con valor de 1, segundo bit con valor de 1, tercer bit con valor de 1 y cuarto bit con valor de 1.

2.31 Video sobre IP

Las señales de vídeo tradicionales se basan en tecnología analógica.

Para su transporte se requieren costosos circuitos de transmisión; afortunadamente, vivimos ahora en un mundo digital.

Gracias a los avances en técnicas de compresión, podemos transportar ahora las señales compuestas de vídeo y audio sobre circuitos de redes típicas de LAN y WAN, e incluso sobre internet. Vídeo sobre IP o IP Streaming Video son las tecnologías más recientes que permiten que las señales de vídeo sean capturadas, digitalizadas, secuenciadas y administradas sobre redes IP.

El primer paso es la captura del contenido de vídeo; lo cual puede realizarse de diferentes maneras. El contenido es procesado, comprimido, almacenado y editado en un servidor de vídeo. El contenido puede ser en vivo (capturado y procesado en tiempo real) o pre registrado y almacenado. Estas transmisiones pueden luego ser enviadas a través de la red a una o varias estaciones para visualizarse en forma individual o simultáneamente. La estación de visualización requerirá de un hardware o software de visualización o, en algunos casos, de ambos.

Las aplicaciones emergentes proporcionan el visualizador y el vídeo sobre Java sin ninguna aplicación especial en la estación terminal.

Las presentaciones de vídeo pueden agruparse en tres categorías:

- ✓ Video Broadcasting.
- ✓ Video on Demand.

✓ Videoconferencia.

De las tres, solo la videoconferencia es full duplex, las otras son esencialmente transmisiones unidireccionales.

Estas transmisiones de vídeo sobre IP son escalables, costo eficientes y muy flexibles; estas nuevas herramientas de negocio integran oficinas distintas en una sola empresa y se están expandiendo rápidamente.

2.32 Video Broadcast sobre IP

Video broadcast sobre IP es una transmisión unidireccional de red de un archivo con contenido de vídeo.

Esta tecnología está siendo implementada en ambientes corporativos como un medio de distribuir capacitación, presentaciones, minutas de reuniones y discursos; también está siendo utilizada por universidades, centros de educación técnica o educación continua, emisoras, proveedores de webcast, solo por nombrar algunos.

Hay tres factores para determinar cuánto ancho de banda requerirá esta tecnología: el número de usuarios, su ancho de banda al servidor y la longitud de la presentación o vídeo.

Video broadcast se considera típicamente como una tubería abierta.

2.33 Video on Demand (VOD) sobre IP

Generalmente, VOD permite a un usuario pedir una determinada secuencia de vídeo almacenada en un servidor. Esta tecnología difiere de Video broadcast en que el usuario tiene las opciones de parar, iniciar, adelantar o regresar el vídeo ya que el servicio es interactivo.

VOD tiene también otra característica en la que generalmente se acompaña del uso de datos para la visualización y la tarificación de los servicios o tiempo de vídeo, aunque VOD se puede usar para visualización en tiempo real, generalmente se utiliza para archivos almacenados de vídeo.

Esta tecnología se usa para e-learning, capacitación, mercadeo, entretenimiento, broadcasting y otras áreas donde el usuario final requiere visualizar los archivos con base en su propio itinerario y no en el horario del proveedor de vídeos.

Una aplicación típica de VOD sobre una red IP, contiene los siguientes elementos:

- ✓ El servidor de vídeo (puede ser un servidor de archivos o un cluster de servidores)
- ✓ El servidor controlador de aplicaciones el cual inicia la transmisión (puede estar incluido en un servidor de archivos)
- ✓ Un punto terminal con un convertidor para responder a la petición de visualización y control de reproducción
- ✓ Software de administración y/o software de tarificación
- ✓ PC o dispositivo de red para registrar/convertir los archivos de vídeo.

2.34 Videoconferencia sobre IP

Videoconferencia (VC) es una combinación de transmisiones full duplex de audio y vídeo los cuales permiten a usuarios ubicados en distintos lugares verse y oírse el uno al otro tal como si estuvieran en una conversación cara a cara.

Se utiliza una cámara en cada uno de los puntos terminales para capturar y enviar las señales de vídeo.

Se usan micrófonos en cada punto terminal para capturar y transmitir la voz la cual es luego reproducida en altoparlantes.

Las comunicaciones son en tiempo real y generalmente no se almacenan.

Estos servicios pueden usarse para diversas aplicaciones incluyendo comunicaciones corporativas, telemedicina, telehealth, capacitación, e-learning, tele-conmutación y servicio a usuarios.

La videoconferencia puede ser punto a punto (un usuario a un usuario), o multipunto (varios usuarios participando en la misma sesión).

Los usuarios pueden posteriormente ser visualizados en ventanas separadas.

La videoconferencia ha introducido un nuevo concepto en comunicaciones por medio de la colaboración. Un tablero electrónico puede ser incluido en la conferencia permitiendo a los usuarios escribir notas en el mismo tablero y/o visualizar las presentaciones y notas de los otros mientras se conversa.

2.35 Digitalización de video

Digitalizar un video es transformar las imágenes y audio a un formato binario como una secuencia de fotos con sonido en pistas separadas.

Cuando digitalizamos podemos hacerlo en forma secuencial o sólo segmentos deseados del video para luego visualizarlos en cualquier máquina PC con instalación básica de Windows usando el componente multimedia Windows Media Player.

Los soportes analógicos pueden ser digitalizados, así se consigue conservar las imágenes durante más tiempo sin que se degraden.

Para transformar el vídeo analógico en vídeo digital se necesitan los siguientes dispositivos:

1.- Un ordenador con un procesador.- Capacidad en el disco duro y memoria RAM. Cuanta más rápido sea el procesador y mayor la memoria RAM más fácil será la captura y la posterior edición del vídeo digital.

La memoria en el disco duro es imprescindible para el almacenaje del vídeo digitalizado.

Es muy importante tener configurado el sistema operativo de modo que permita capturar vídeo.



Figura 2.44 Computador con buenas características

2.- Un dispositivo reproductor de vídeo analógico.- Los soportes analógicos deben ser reproducidos bien en una vídeo cámara o en un aparato reproductor conectado al ordenador.

3.- Una tarjeta de vídeo.- Esta permitirá al ordenador reproducir las imágenes una vez digitalizadas.



Figura 2.45 Tarjeta capturadora de video

4.- Una tarjeta de captura.- También son conocidas como sintonizadoras.

Existen varios tipos de tarjetas; las que sólo capturan y también sintonizan tv, las que capturan y ofrecen salida de vídeo y las tarjetas específicas para edición. Los precios entre unas y otras varían considerablemente y los problemas que pueden dar también.

Algunas tarjetas de vídeo llevan incorporados los sistemas de captura.

5.- Software para captura y edición de vídeo.- Son programas específicos que permiten configurar las distintas opciones de captura elegidas por el usuario.

2.35.1 Problemas para digitalizar

El proceso de digitalizar vídeo analógico no está exento de problemas. Se recomienda tener un buen equipo, con suficiente potencia y capacidad, correctamente configurado y preparado. No escatimar en la calidad del software y el hardware minimiza las dificultades, evita problemas y si valoramos nuestro tiempo resulta rentable.

2.36 Compresión

La técnica de compresión de vídeo consiste de tres pasos fundamentalmente, primero el pre procesamiento de la fuente de vídeo de entrada, paso en el cual se realiza el filtrado de la señal de entrada para remover componentes no útiles y el ruido que pudiera haber en esta.

El segundo paso es la conversión de la señal a un formato intermedio común (CIF), y por último el paso de la compresión.

Las imágenes comprimidas son transmitidas a través de la línea de transmisión digital y se hacen llegar al receptor donde son reconvertidas al formato común CIF y son desplegadas después de haber pasado por la etapa de post-procesamiento.

Mediante la compresión de la imagen se elimina información redundante, se ayuda de la redundancia espacial y temporal.

La redundancia temporal es reducida primero usando similitudes entre sucesivas imágenes, usando información de las imágenes ya enviadas, cuando se usa esta técnica, sólo es necesario enviar la diferencia entre las imágenes, es decir las zonas de la imagen que han variado entre dos fotogramas consecutivos, lo que elimina la necesidad de transmitir la imagen completa.

La compresión espacial se vale de las similitudes entre píxeles adyacentes en zonas de la imagen lisas y de las frecuencias espaciales dominantes en zonas de color muy variado.

El método para eliminar las redundancias en el dominio del tiempo puede ser eliminado mediante el método de codificación de intercuadros, que también incluye los métodos de compensación/estimación del movimiento, el cual compensa el movimiento a través de la estimación del mismo.

En el otro extremo, las redundancias en el dominio espacio es llamado codificación intracuos, la cual puede ser dividida en codificación por predicción y codificación de la transformada usando la transformada del coseno.

La transformada del coseno o DCT es una implementación específica de la transformada de Fourier donde la imagen es transformada de su representación espacial a su frecuencia equivalente.

Cada elemento de la imagen se representa por ciertos coeficientes de frecuencia. Las zonas con colores similares se representan con coeficientes de baja frecuencia y las imágenes con mucho detalle con coeficientes de alta frecuencia.

La información resultante son 64 coeficientes DCT.

El DCT reordena toda la información y la prepara para la cuantización.

El proceso de cuantización es la parte del algoritmo que causa pérdidas.

La cuantización asigna un número de bits específico a cada coeficiente de frecuencias y entonces comprime los datos asignando unos cuantos bits a los coeficientes de alta frecuencia sin que lo note el observador.

Los parámetros de la cuantización son optimizados, pero el proceso aún deteriora la calidad del vídeo. Generalmente se acepta que un factor de compresión de 2:1 (aproximadamente 10Mb/seg), se pueden apreciar visualmente algunas pérdidas en la integridad del vídeo.

2.37 Formatos de compresión

2.37.1 Formato MPEG

MPEG es un estándar internacional, definido por un comité llamado MPEG formado por la ISO, para la representación codificada y comprimida

de imágenes en movimiento y audio asociado, orientado a medios de almacenamiento digital.

El algoritmo que utiliza además de comprimir imágenes estáticas compara los fotogramas presentes con los anteriores y los futuros para almacenar sólo las partes que cambian, la señal incluye sonido en calidad digital.

El inconveniente de este sistema es que debido a su alta complejidad necesita apoyarse en hardware específico.

MPEG aplica la compresión temporal y la espacial.

En primer lugar se aplica una transformada de coseno discreta, seguida de una cuantización para finalmente comprimir mediante un algoritmo RLE.

Los bloques de imagen y los de predicción de errores tienen una gran redundancia espacial, que se reduce gracias a la transformación de los bloques desde el dominio del espacio al dominio de frecuencia.

MPEG requiere una intensiva computación para su codificación, aunque se consiguen ratios desde 50:1 hasta 200:1

Existen diferentes opciones dependiendo del uso:

2.37.1.1 MPEG-1

Guarda una imagen, la compara con la siguiente y almacena sólo las diferencias.

Se alcanzan así grados de compresión muy elevados.

Define tres tipos de fotogramas:

- ✓ Fotogramas o Intra-fotogramas, son los fotogramas normales o de imagen fija, proporcionando una compresión moderada, en JPEG.
- ✓ Fotogramas P o Predichos, son imágenes predichas a partir de la inmediatamente anterior. Se alcanza una tasa de compresión muy superior.
- ✓ Fotogramas B o bidireccionales, se calculan en base a los fotogramas inmediatamente anterior y posterior. Consigue el mayor grado de compresión a costa de un mayor tiempo de cálculo.

2.37.1.2 MPEG-2

Con una calidad superior al MPEG-1, MPEG-2 fue universalmente aceptado para transmitir vídeo digital comprimido con velocidades mayores de 1Mb/s aproximadamente.

Con MPEG-2 pueden conseguirse elevados ratios de hasta 100:1, dependiendo de las características del propio vídeo.

MPEG-2 normalmente define dos sistemas de capas, el flujo de programa y el flujo de transporte.

Se usa uno u otro pero no los dos a la vez. El flujo de programa funcionalmente es similar al sistema MPEG-1.

La técnica de encapsulamiento y multiplexación de la capa de compresión produce paquetes grandes y de varios tamaños.

Los paquetes grandes producen errores aislados e incrementan los requerimientos de buffering en el receptor/decodificador para demultiplexar los flujos de bits.

En contraposición el flujo de transporte consiste en paquetes fijos de 188 bytes lo que decremanta el nivel de errores ocultos y los requerimientos del buffering receptor.

Los estándares MPEG fueron desarrollados para ser independientes de la red específica para proporcionar un punto de interoperabilidad en entornos de red heterogéneos.

2.37.1.3 MPEG4

Es un estándar relativamente nuevo orientado inicialmente a las video - conferencias y para Internet.

El objetivo es crear un contexto audiovisual en el cual existen unas primitivas llamadas AVO (objetos audiovisuales).

Se definen métodos para codificar estas primitivas que podrían clasificarse en texto y gráficos.

La comunicación con los datos de cada primitiva se realiza mediante uno o varios "elementary streams" o flujos de datos cuya característica principal es la calidad de servicio requerida para la transmisión.

Ha sido especialmente diseñado para distribuir videos con elevados ratios de compresión, sobre redes con bajo ancho de banda manteniendo una excelente calidad para usuarios con buen ancho de banda.

Ofrece un ancho rango de velocidades desde usuarios con modems de 10kbps a usuarios con anchos de banda de 10Mbps.

Es rápido codificando el vídeo de alta calidad para contenidos en tiempo real y bajo demanda.

En soluciones como vídeo bajo demanda los datos codificados en el formato MPEG tienen que ser transmitidos sobre redes de comunicaciones.

Puesto que el ancho de banda del medio de transmisión es limitado, para mantener una constante velocidad de salida debe hacerse una negociación entre la velocidad y la calidad de la imagen.

De esto se encargan los algoritmos de cuantización, los cuales seleccionan diferentes tablas de cuantización para diferentes tipos de imágenes durante la codificación de datos.

Una solución simple es codificar los datos originales dinámicamente en el servidor, pero necesita grandes recursos.

Una alternativa es almacenar los ficheros codificados en MPEG en el servidor y adaptativamente recodificarlo en base a las velocidades disponibles.

El objetivo es recodificar y codificar los ficheros MPEG dinámica y eficientemente en un flujo de bits constante.

2.37.2 MJPEG

Motion-JPEG es una versión extendida del algoritmo JPEG que comprime imágenes.

Básicamente consiste en tratar al vídeo como una secuencia de imágenes estáticas independientes a las que se aplica el proceso de compresión del algoritmo JPEG una y otra vez para cada imagen de la secuencia de vídeo.

Existen cuatro modos de operación para el JPEG: secuencial, progresiva, sin pérdida y jerárquica.

Normalmente se utiliza el modo secuencial.

La ventaja es que se puede realizar en tiempo real e incluso con poca inversión en hardware.

El inconveniente de este sistema es que no se puede considerar como un estándar de vídeo pues ni siquiera incluye la señal de audio.

Otro problema es que el índice de compresión no es muy grande.

JPEG utiliza una técnica de compresión espacial, la intracuadros o DCT.

El sistema JPEG solamente utiliza la compresión espacial al estar diseñado para comprimir imágenes individuales.

Motion-JPEG es el método elegido para las aplicaciones donde se envía la misma información a todos los usuarios.

Muchas aplicaciones actuales como el vídeo requieren que los mismos datos de un servidor sean distribuidos a múltiples clientes.

Si varios clientes solicitan los mismos datos y esta información fuera enviado una vez por cada cliente, estaríamos malgastando el ancho de banda ya que estaríamos transmitiendo la misma información varias veces por el mismo tramo de red y el número de clientes estaría limitado por el ancho de banda disponible.

La solución es IP multicast, soporta eficientemente este tipo de transmisión permitiendo al servidor enviar una sola copia de la información a múltiples clientes quienes deseen recibir la información.

Otros formatos como el MPEG-7 y el MPEG-21 están en la actualidad en pleno desarrollo.

Con ellos se pretende generar potentes bases de datos capaces de gestionar e introducir técnicas de acceso condicional a contenidos multimedia.

Actualmente este formato se ha hecho muy popular en Internet aunque tan solo se esté utilizando una mínima parte de su potencial teniendo en cuenta los elevados factores de compresión que es capaz de soportar con unos resultados visuales muy satisfactorios.

Uno de los codecs que basa su compresión en algunos de los parámetros definidos en el estándar es el conocido DivX en este caso se considera toda la imagen como un único objeto rectangular.

2.38 Transmisión de video digital

La transmisión digital y la distribución de información audiovisual permiten la comunicación multimedia sobre las redes que soportan la comunicación de datos, brindando la posibilidad de enviar imágenes en movimiento a lugares remotos.

Pero no es todo tan bonito a la hora de transmitirlo por red, debido a que nos encontramos con sucesos como lentitud entre la reproducción de imágenes, errores de transmisión o pérdidas de datos.

Existen dos formas de transmisión de datos, analógica y digital.

Una de las características del vídeo es que está compuesto por señales analógicas, con lo que se pueden dar las dos formas de transmisión.

En los últimos años la transmisión de datos se ha volcado hacia el mundo digital ya que supone una serie de ventajas frente a la transmisión analógica.

Al verse la información reducida a un flujo de bits, se consigue una mayor protección contra posibles fallos ya que se pueden introducir mecanismos de detección de errores, se elimina el problema de las interferencias, podemos disminuir el efecto del ruido en los canales de comunicación, conseguir codificaciones más óptimas y encriptado, mezclar con otros tipos de información a través de un mismo canal, y poder manipular los datos con ordenadores para comprimirlos.

Además si queremos difundir el vídeo por vías digitales tendremos que digitalizarlo, con lo que debe ser capturado en su formato analógico y

almacenado digitalmente logrando así que sea menos propenso a degradarse durante la transmisión.

Existen dos tipos de redes de comunicación, de conmutación de circuitos y de conmutación de paquetes.

En la conmutación de circuitos, donde la comunicación está permanentemente establecida durante toda la sesión, un determinado ancho de banda es asignado para la conexión, y el tiempo de descarga del vídeo puede predecirse, pero tienen la desventaja de que las sesiones son punto a punto y limitan la capacidad de usuarios.

En la conmutación de paquetes pueden acomodarse más fácilmente las conferencias multipunto.

Aquí el ancho de banda está compartido pero es variable, lo que supone una importante mejora puesto que, si el bit rate (o número de bits por segundo) es fijo la calidad de la imagen variará dependiendo del contenido de los fotogramas.

Debe de cumplirse que el ancho de banda, la resolución, y la compresión de audio sean idénticos para cada cliente que recibe el vídeo lo que dificulta la configuración del sistema.

El vídeo es muy sensible al retardo de la red, ya que puede provocar cortes en las secuencias.

La pérdida de alguna información en el vídeo sin comprimir no es muy relevante, ya que al perderse un fotograma, el siguiente fotograma proporciona la suficiente información para poder interpretar la secuencia.

En cambio el vídeo comprimido es mucho más sensible a errores de transmisión ya que las técnicas de compresión que se valen de la redundancia espacial y temporal pueden perder la información de esta redundancia y los efectos de la falta de datos pueden propagarse en los próximos fotogramas.

Es por eso que actualmente la comunicación con vídeo vía Internet no prometen una elevada fiabilidad de transmisión.

Algunas técnicas de compresión compensan esta sensibilidad a la pérdida de datos enviando la información completa sobre un fotograma cada cierto tiempo, incluso si los datos del fotograma no han cambiado.

Esta técnica también es útil para los sistemas de múltiples clientes, para que los usuarios que acaban de conectarse, reciban las imágenes completas.

Nos podemos preguntar cuál es la tecnología de red adecuada para las aplicaciones de vídeo, pero siempre dependeremos del entorno en el que trabajemos.

Pero la solución para resolver el cuello de botella del ancho de banda del vídeo no está en un solo tipo de red sino en una infraestructura de red flexible que pueda manejar e integrar diferentes redes y que deje paso también a futuras redes sin cambiar el hardware.

También debe ser capaz de negociar las variables de ancho de banda, resolución, número de fotogramas por segundo y algoritmo de compresión de audio. Así que se necesita un nodo que permita la interconectividad entre todas las redes.

Es el MCU (unidad de control multipunto) cada red RDSI, IP, ATM usa protocolos específicos que definen la naturaleza de las ráfagas de vídeo.

2.39 Requerimientos para la transmisión multimedia

Se suele denominar tráfico multimedia aquel compuesto por vídeo y audio, aunque formalmente se refiere a cualquier medio que se puede transmitir.

En general los requerimientos para la transmisión de audio y vídeo son tratados y sobresalen los siguientes puntos.

2.39.1 Ancho de banda

El tráfico multimedia maneja grandes volúmenes de información; un CD-ROM, que son 72 minutos de sonido estéreo, requiere 648 Mbytes y una película de 90 minutos ocuparía 120 Gbytes, ambos sin comprimir.

La información de vídeo actualmente se trata casi exclusivamente de forma comprimida.

El ancho de banda dependerá por tanto del tipo de compresión y de la calidad con que se desee transmitir.

2.39.2 Retraso de transmisión

Estos requerimientos son más estrictos que los de ancho de banda.

La experiencia con los sistemas de conferencia multimedia y los estándares ITU sugieren un retraso máximo de 150 ms en las aplicaciones de vídeo interactivas y en telefonía este retraso es más exigente (<25ms) para evitar el eco.

En función del retraso se pueden distinguir los siguientes tipos de tráfico:

Asíncrono.- Retraso de transmisión sin restricciones.

Síncrono.- El retraso de transmisión está acotado para cada mensaje.

Isócrono.- El retraso de transmisión es constante para cada mensaje

2.39.3 Fiabilidad

Las redes tradicionales proporcionan comunicación fiable entre emisor y receptor. Los protocolos de transmisión tienen sistemas de control de errores y de reenvío de paquetes que aseguran que esta fiabilidad es transparente a los niveles superiores.

Para la transmisión en tiempo real esta gestión de errores puede ser negativa, debido al retraso que produciría la retransmisión de un paquete de nuevo.

Para evitar este problema se plantea que el tratamiento y gestión de los errores sea a niveles superiores.

Las prestaciones de una transmisión multimedia, puede ser medida en dos dimensiones: latencia y fidelidad.

La latencia puede ser vital para aplicaciones interactivas como conferencias mientras que la transmisión de una película no lo es.

La fidelidad de la transmisión es variable.

Hay aplicaciones que no toleran ninguna variación en la fidelidad de la imagen como podrían ser la transmisión de imágenes médicas y otras en que esta variación solo produce una cierta distorsión tolerable como la transmisión de películas o música.

2.39.4 Sincronización de canales

Cuando audio, vídeo y otros datos vienen por distintos canales se necesitan mecanismos para la sincronización de los distintos flujos en el destino.

Esto se puede conseguir usando una combinación de asignación de tiempos y almacenamiento antes de visualización.

Esto en general no afecta a la red y es un problema del destino.

2.39.5 Proceso para la recepción de video

El proceso de decodificación es básicamente el inverso del proceso de codificación. La compresión del audio está descrita por tres parámetros: ratio de muestreo (numero de muestras por segundo), bits por muestra (numero de bits para representar cada valor), y número de canales (mono o estéreo).

Los estándares de vídeo digital más conocidos son: MPEG, Quicktime, AVI, MOV, real vídeo, ASF y para vídeo analógico: NTSC, PAL, SECAM.

2.40 Aplicaciones de las cámaras IP

Las áreas en donde se están utilizando éstos sistemas con mucho éxito

son:

Educación.- Por seguridad en la supervisión remota de patios, aulas y vestíbulos de escuelas.

Transportes.- Vigilancia remota de centrales de autobuses, estaciones de ferrocarril, carreteras, aeropuertos.

Instituciones Financieras.- Para las aplicaciones de seguridad tradicionales.

Oficinas.- Para vigilancia de la integridad del personal y oficinas, control de acceso o monitoreo de equipo técnico e informático, cafeterías, estacionamientos de empleados.

Tiendas.- Para seguridad, elaborando imágenes/video de manera remota para la vigilancia y supervisión de personal y/o clientes.

Industria Manufacturera.- Supervisando de líneas de producción, procesos industriales, almacenes, departamentos de mensajería y correos.

Seguridad Pública.- Seguridad en las áreas públicas.

Turismo.- Como medio publicitario ya que todas las personas que van a emprender un viaje de placer o negocios le gusta saber detalles como clima, instalaciones hoteleras.

Estas son algunas de las aplicaciones cámaras IP con mas demanda.

CAPÍTULO III

IMPLEMENTACIÓN DE LA RED DE VIGILANCIA

3.1 Seguridad institucional

La seguridad actual del edificio del Servicio Aeropolicial se compone de un personal de 3 policías, que se encargan de vigilar, controlar, custodiar las instalaciones y los recursos de la unidad.

Se encuentran ubicados en el ingreso principal de las instalaciones del Servicio Aeropolicial.

Es evidente que el personal de guardia no es suficiente para dar cobertura a las instalaciones de una mejor manera, ya que debido al cansancio acumulado puede mermar las capacidades y el estado de alerta en algunos momentos.

El edificio tiene un acceso desde la avenida Amazonas, cuenta con 3 policías que controlan el acceso, los cuales permanecen en diferentes horarios. Se encargan de verificar la entrada y salida del personal policial y civil que laboran en la unidad.

Los lugares más vulnerables en las noches en cuanto a la seguridad es el hangar ya que ahí se encuentran las aeronaves, 2 surtidores de combustible y bodegas de repuestos, herramientas y demás materiales.

Las instalaciones de la unidad cuentan con un parqueadero principal, siendo este un punto vulnerable por encontrarse en los exteriores del edificio.

3.2 Descripción del edificio del Servicio Aeropolicial

Las instalaciones del Servicio Aeropolicial se encuentra ubicado en la Av. Amazonas y Rio Topo cabecera sur del parque Bicentenario; antiguo aeropuerto Mariscal Sucre.

La infraestructura consta de 4 bloques establecidos por un edificio de 3 pisos

construido en hormigón, anexo al sur tenemos una infraestructura de un piso construido en hormigón, al norte tenemos una infraestructura de 1 y 2 pisos de construcción mixta hormigón y estructura metálica, en el centro tenemos el hangar construido en estructura metálica, al frente del edificio está el acceso a la unidad y parqueadero.

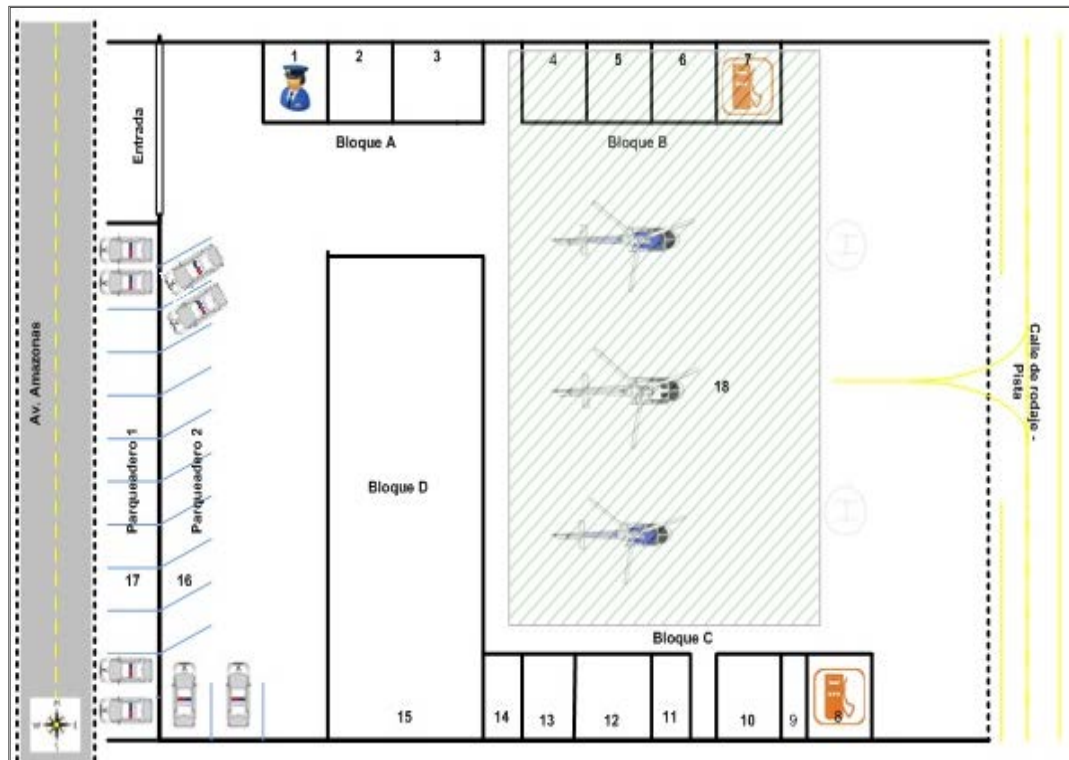


Figura 3.1 Plano de las instalaciones del Servicio Aeropolicial

3.3 Simbología de las instalaciones

3.3.1 Bloque A

El bloque A está conformado por 2 plantas o pisos:

Primera planta

- 1.- Garita de guardia
- 2.- Oficina
- 3.- Oficina

Segunda planta

- 1.- Dormitorio

2.- Oficina

3.3.2 Bloque B

El bloque B está conformado por:

- 4.- Bodega 1
- 5.- Bodega 2
- 6.- Bodega 3
- 7.- Surtidor de combustible 1

3.3.3 Bloque C

El bloque C está conformado por:

- 8.- Surtidor de combustible 2
- 9.- Rastrillo y repuestos de aviación
- 10.- Bodega 5
- 11.- Simulador de vuelo
- 12.- Aula
- 13.- Oficina
- 14.- SS.HH

3.3.4 Bloque D

El bloque D está conformado por:

Primera planta

- 15.- Área administrativa

Segunda planta

- 15.- Dormitorios

Tercera planta

- 15.- Casino

Parqueaderos y hangar

- 16.-Parqueadero Interno
- 17.- Parqueadero externo
- 18.- Hangar

3.4 Distribución de las instalaciones con ubicaciones de zonas vulnerables

En base a los datos recabados en las entrevistas, se han detallado las siguientes zonas propensas a sufrir delitos u otro tipo de hecho delincuenciales.

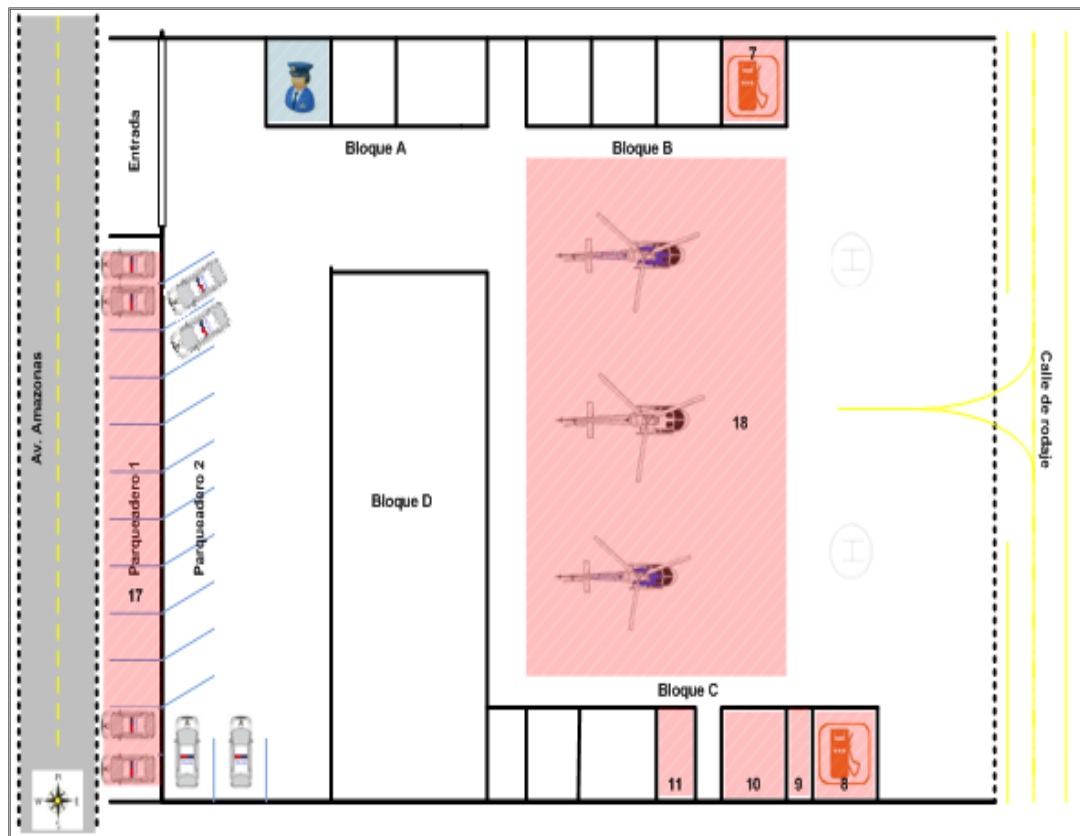


Figura 3.2 Plano de las instalaciones del SAP con las zonas vulnerables

3.5 Simbología de zonas vulnerables

7.- Surtidor de combustible 1.- En este punto hay un surtidor de

combustible para aviación de tipo AVGAS, debiendo ser manipulado con las debidas precauciones.

8.- Surtidor de combustible 2.- Aquí tenemos un surtidor de combustible de aviación de tipo JP1.

9.- Rastrillo y repuestos aeronáuticos.- En esta área se custodia el armamento del personal policial, así como también repuestos y componentes de las diferentes aeronaves.

10.- Cuarto de herramientas.- En esta zona existen materiales y equipo necesario utilizados en el trabajo diario del mantenimiento de las aeronaves.

11.- Simulador de vuelo.- Aquí funciona un simulador de vuelo, el mismo que está conformado por equipos de alta tecnología.

17.- Parqueadero externo.- Aquí se ubican vehículos del personal a más de los pertenecientes a la unidad.

18.- Hangar.- En esta área están las aeronaves en donde pernoctan ya sea en las noches o en mantenimiento, además de que en el día son desplazados hasta el helipuerto desde donde decolan.

En las zonas antes indicadas labora personal policial y civil a más de la afluencia de personas ajenas a la unidad por lo que es necesario llevar un control de las personas que hacen uso de estas áreas.

Aquí se debe tener una buena seguridad debido a la cantidad de materiales que pueden ser sustraídos y equipos tecnológicos de alto valor económico.

3.6 Distribución y ubicación de las cámaras

Para definir las ubicaciones de las cámaras de vigilancia se han tomado en cuenta la distribución de zonas vulnerables.

No necesariamente se han ubicado las cámaras en cada zona, se han elegido puntos estratégicos, desde los cuales se puede tener ángulos de visión de las entradas y/o salidas de cada zona.

El número de cámaras para la implementación son 4, distribuidas de la siguiente manera:

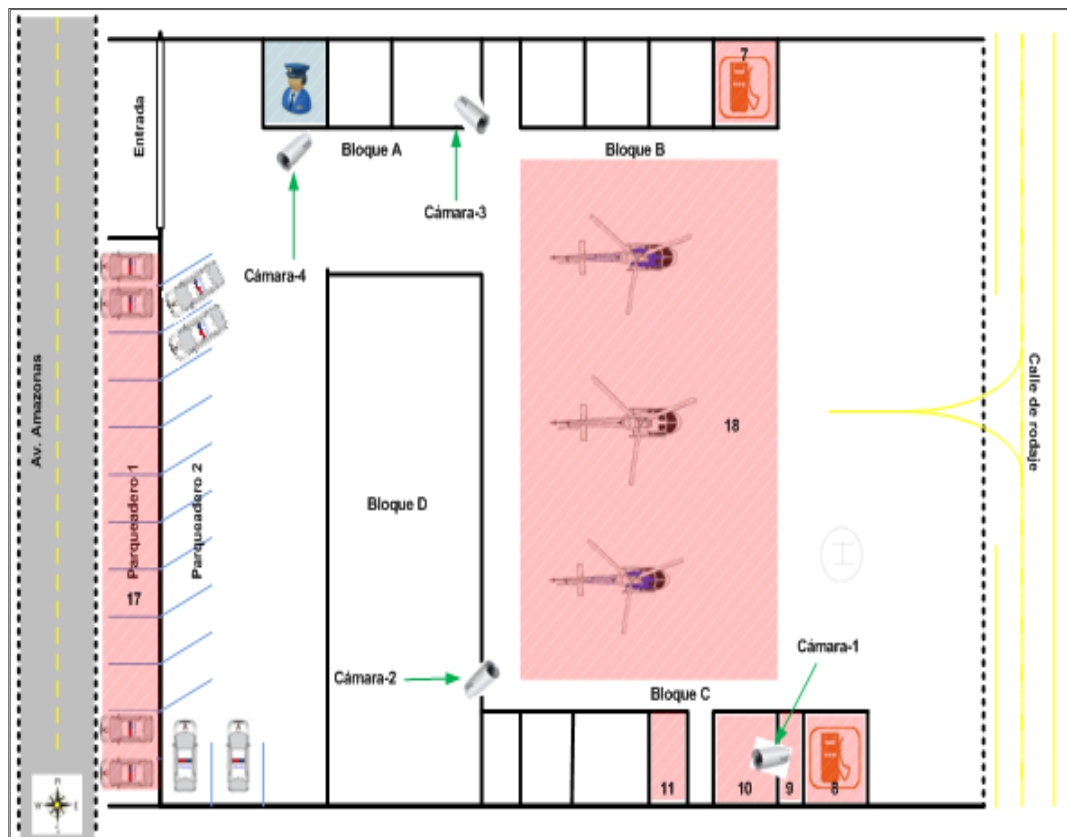


Figura 3.3 Plano de las instalaciones del SAP con las zonas vulnerables y ubicación de las cámaras

3.6.1 Cámara-1

Visualiza el ingreso y parte interna de las zonas 9, 10 y 11.

3.6.2 Cámara-2

Visualiza las zonas 18 y 7.

3.6.3 Cámara-3

Visualiza las zonas 18 y 8 además se puede monitorear el ingreso a las zonas 9,10 y 11.

3.6.4 Cámara-4

Visualiza las zonas 16 y 17.

3.7 Selección de cámaras IP

Los requisitos en los que nos hemos basado para la elección de la cámara han sido:

- ✓ Que pueda trabajar con IP estática.
- ✓ Que sea para exterior y tipo "Domo" para colocar en techo ó pared.
- ✓ Que lleve algún sistema que nos permita ver de noche.
- ✓ Que nos permita visualizar video a través de un PC.
- ✓ Que tenga una gran relación calidad/precio.

Una vez analizado los requerimientos y para el efecto de este proyecto se adquirió las cámaras de tecnología IP marca VIVOTEK en el modelo IP8331 cuyas características se detallan a continuación:

- ✓ Sensor CMOS 1/4" en resolución VGA
- ✓ Lentes de banda dual para la función diurna y nocturna
- ✓ Iluminadores IR integrados, efectivos hasta 10 metros
- ✓ Compresión en tiempo real de H.264, MPEG-4 y
- ✓ MJPEG (Codec Triple)
- ✓ Streams duales simultáneos
- ✓ Carcasa impermeable clasificación IP66



Figura 3.4 Cámara IP 8331

3.7.1 Descripción física de la cámara Vivotek IP8331

La cámara de red tipo bala Vivotek IP8331 tiene una carcasa de clasificación IP66 resistente a la intemperie, la cámara está blindada contra duras condiciones, como lluvia o polvo y proporciona una solución todo en uno sin la necesidad de accesorios adicionales.

Mediante la integración de componentes para la funcionalidad día y noche, como un lente de doble banda e iluminadores IR incorporados con un alcance de hasta 10 metros, la cámara es capaz de lograr un rendimiento superior en un diseño compacto.

La IP8331 soporta también detección de bloqueos, que puede detectar eventos en la cámara tales como bloqueo, redirección y pintura con spray, lo que es una solución inteligente a la posible obstrucción de la cámara.

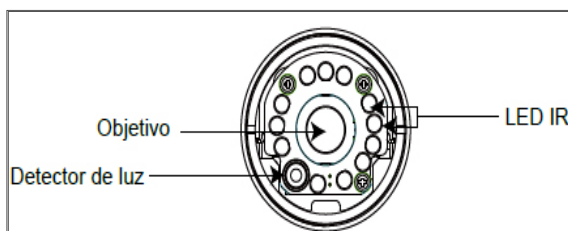


Figura 3.5 Panel frontal de la cámara IP 8331

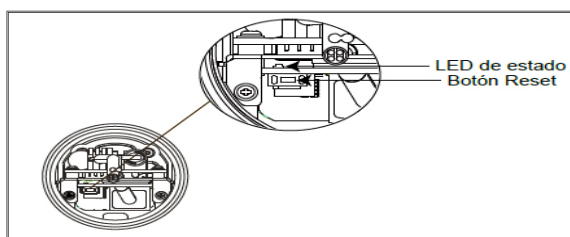


Figura 3.6 Panel posterior de la cámara IP 8331

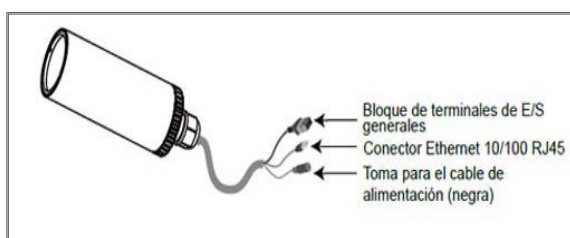


Figura 3.7 Conectores de la cámara

3.8 Montaje de la cámara

Empezaremos por la instalación física de la cámara que es muy sencilla, todo esto una vez que se eligió la zonas que queremos vigilar teniendo en cuenta el lugar más adecuado para nuestras necesidades.

Tenemos dos opciones para montarla, tanto en techo como pared.

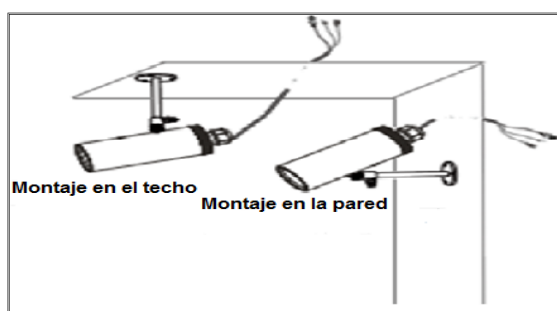


Figura 3.8 Opciones de montaje de la cámara IP

3.8.1 Conexión general de la cámara

Hay varias formas de cómo conectar la cámara a Internet para poder acceder a ella desde cualquier lugar del mundo.

A continuación realizaremos la conexión básica.

Conectaremos la cámara mediante un cable Ethernet al switch o directamente al router, conectaremos el adaptador jack de la fuente de la alimentación a la cámara, antes de enchufar la fuente de alimentación a la red eléctrica.

Así evitaremos accidentes eléctricos como se muestra en la figura.

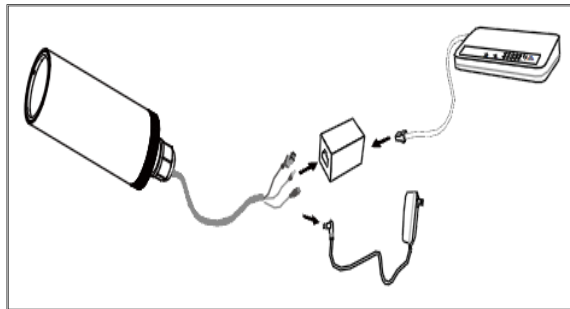


Figura 3.9 Conexión general de la cámara

Ya tenemos nuestra cámara orientada hacia el lugar que queremos vigilar e instalada físicamente y sólo nos queda configurarla y examinar las opciones de vigilancia que nos ofrece este modelo.

3.9 Elementos pasivos de la red

3.9.1 Canaletas

Una canaleta es un ducto adherido a la pared o piso por medio del cual pasara el cable (del tipo que sea). Existen de diversos materiales, pero si es para piso te recomiendo la metálica.



Figura 3.10 Canaleta

3.9.2 Toma corriente

Punto de un sistema eléctrico desde el que se puede alimentar un aparato eléctrico.



Figura 3.11 Toma corriente

3.9.3 Conectores RJ 45

El RJ45 es un conector usado para conectar redes de cable estructurado ethernet y otros dispositivos a redes de área local (LAN).



Figura 3.12 Conector RJ-45

3.9.4 Cable UTP

El cable UTP es una clase de cable que no se encuentra blindado y que suele emplearse en las telecomunicaciones.



Figura 3.13 Cable UTP

3.10 Elementos activos de la red

3.10.1 Descripción física del computador

Para el monitoreo de la red de vigilancia se ha seleccionado el equipo que a continuación se detalla:

Tabla 3.1

Características del computador

Detalle	Descripción
Sistema Operativo	Windows 7
Tipo de sistema	Sistema operativo de 32 bits
Procesador	Intel Core I7
Velocidad	3.40 GHz
Memoria	Instalada 4GB
Disco Duro	500 GB
Monitor LCD	19 Pulgadas

Elaborado por: Juan Carlos Morales

3.10.2 Switch

Un switch o conmutador es un dispositivo de interconexión de redes informáticas.



Figura 3.14 Switch

3.10.3 Regulador de voltaje

Es un dispositivo que tiene varios enchufes, se encarga de proteger contra altas y bajas de voltaje.



Figura 3.15 Regulador de voltaje

3.11 Topología Lógica

La red de vigilancia del Servicio Aeropolicial tendrá una tecnología Ethernet.

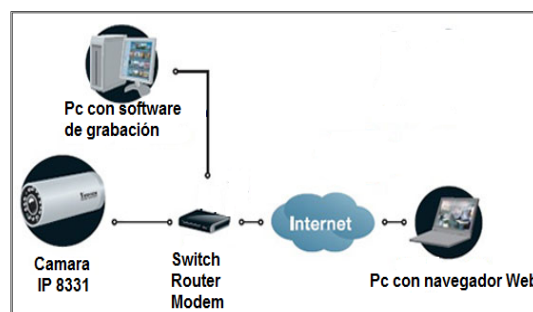


Figura 3.16 Topología lógica

3.11.1 Topología Física

Se utilizará la topología en estrella para estructurar la red de vigilancia del servicio Aeropolicial.

Esta topología nos permite una fiabilidad de cada segmento, resulta ventajoso que la red de vigilancia IP tenga sus propios conmutadores conectados a una red.

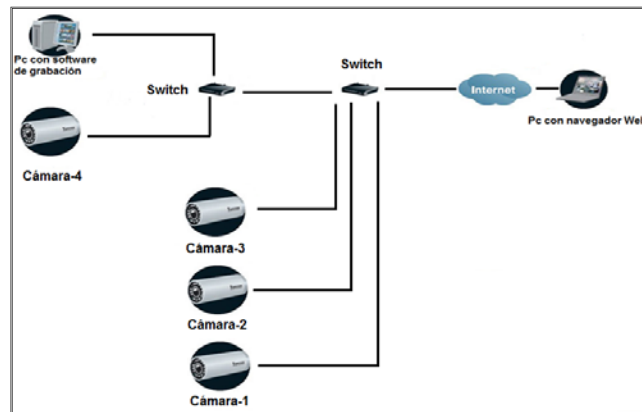


Figura 3.17 Topología física

3.11.2 Instalación del software Installation Wizard 2

Primeramente insertamos en CD del software en la unidad lectora de discos del CPU el cual será utilizado como servidor, seguido ejecutamos “Installation Wizard 2”.



Figura 3.18 Instalación del software

Mostrando en el escritorio del monitor el siguiente icono:



Figura 3.19 Icono de la instalación del software wizard 2

El programa realizara un análisis de su entorno de red, buscando

receptores de video, servidores de video o las cámaras de red vivotek situadas en la misma red local, una vez analizada la red damos un doble clic sobre el icono para continuar con la configuración.

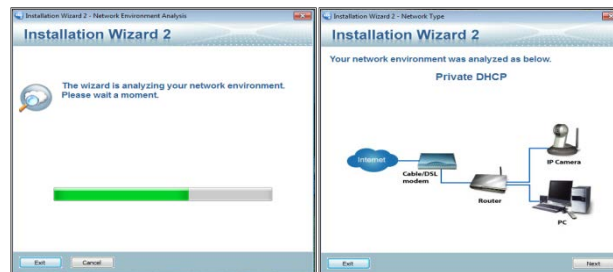


Figura 3.20 Pantallas de búsqueda de cámaras en la red

Tras una búsqueda aparecerá la ventana del instalador principal con las direcciones MAC de todas las cámaras conectadas, lo que debe coincidir con la impresa en la etiqueta.

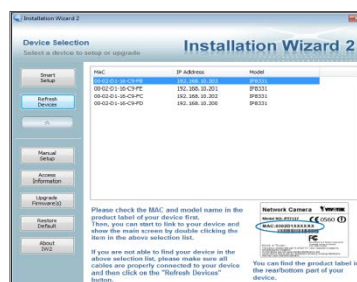


Figura 3.21 Pantalla con direcciones MAC de las cámaras

3.11.3 Configuración del sistema

Aquí daremos el nombre a la cámara, contraseña de acceso de administrador (root) y configuración de la fecha y la hora.

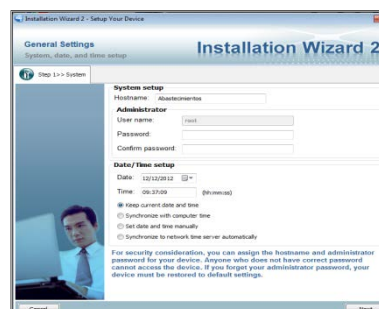


Figura 3.22 Pantalla de configuración de la cámara

3.11.4 Configuración de red

En este apartado debemos asignar una dirección IP a la cámara para que se encuentre asignada dentro del rango de nuestra red, además de la máscara de subred y la puerta de enlace que será la misma que la IP del router.

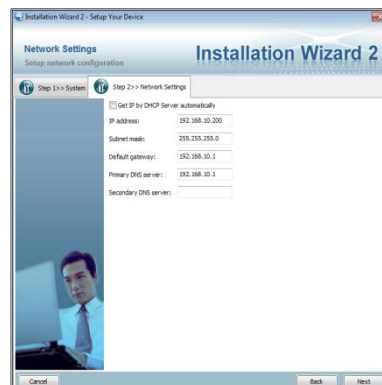


Figura 3.23 Pantalla de configuración de la red

3.11.5 Configuración de puertos

Ahora configuraremos los puertos manualmente. Por defecto el “puerto http” es el 8080 y resulta aconsejable cambiarlo por otro para que no surjan conflictos con el navegador Internet Explorer ya que también utiliza este puerto 80.

Esto sería en el caso de que la cámara la vamos a querer visualizar alguna vez desde otra red externa que no sea la nuestra; como por ejemplo, el comandante de la unidad desea vigilar a través de las cámaras el desarrollo de las actividades de la unidad desde cualquier otro lugar del mundo.

Para ello, pongamos un ejemplo:

Si nuestra IP que le hemos asignado a la cámara es la 192.168.10.32

El puerto que podemos poner por ejemplo es el 8054, con esto podemos acceder de una red que no sea la propia en la que se encuentra la cámara.

Una vez hecho todo esto para acceder a la cámara y visualizarla deberíamos escribir en el navegador de Internet algo así como:

http://192.168.10.32:8054

↑.....↑

Dirección IP privada puerto para acceder desde la propia red.

3.11.6 Visualización a través del navegador web

Para visualizar el modo gráfico de la cámara abrimos el navegador “Internet Explorer, Mozilla, Google Chrome”, y en la barra de direcciones digitamos la dirección IP de nuestra cámara.



Figura 3.24 Dirección IP para acceder a la visualización

Una vez accedido al navegador web se visualiza el vídeo en directo proveniente de la cámara, como se muestra a continuación.



Figura 3.25 Pantalla de video tiempo real

3.11.7 Pantalla principal

Está compuesto de lo siguiente secciones:

1.- Logo.- Logotipo de la unidad y con un clic accedemos para visitar la página Web del Servicio Aeronaval.

2.- Zona de mando de cámara.- minimiza o maximiza la pantalla de la cámara.

3.- Zona de configuración – Menú.- Aquí podemos dar una configuración general a la cámara.

4.- Ventana y botones de control de video.- Esta zona nos permite visualizar el video en tiempo real las 24 horas.

5.- Nombre de la cámara.- Muestra el nombre de la cámara el mismo que se le puso según la zona que está siendo monitoreada.

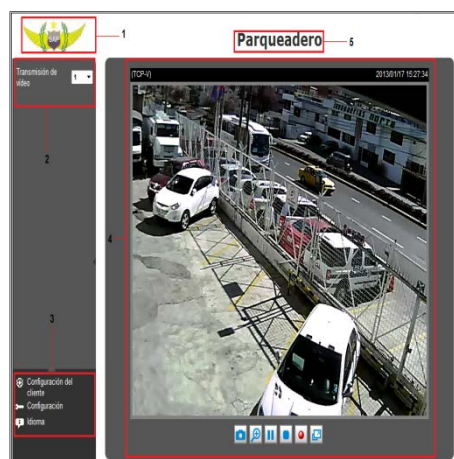


Figura 3.26 Pantalla de configuración

Este proceso se realiza en todas las cámaras que están conectadas a nuestra red de vigilancia, para finalmente instalar el software de grabación y visualización de 32 canales ST7501, que viene en el CD con el fin de tener un despliegue de todas las cámaras en una sola pantalla.

3.11.8 Instalación del software gestor de video ST7501

Primeramente insertamos en CD del software en la unidad lectora de

discos del CPU el cual será utilizado como servidor, en donde ejecutaremos LiveClient y Playback.



Figura 3.27 Instalación del software gestor de video ST7501

3.11.9 Iconos de LiveClient, Playback y Wizard 2

Estos iconos son mostrados en el escritorio del monitor en donde se encuentra el software.



Figura 3.28 Iconos de LiveClient, Playback y Wizard 2

3.11.10 Asignación de canales al gestor de video

En el escritorio de la pantalla mostrara los iconos LiveClient y Playback a los cuales se accederá ingresando usuario y contraseña.



Figura 3.29 Instalación del software para asignación de canales

3.11.11 Ajuste y procedimientos de asignación de canales LiveClient

En este apartado configuramos las cámaras que serán visualizadas en tiempo real, como también configuramos el tipo de video que será archivado en el equipo que esta designado como servidor.

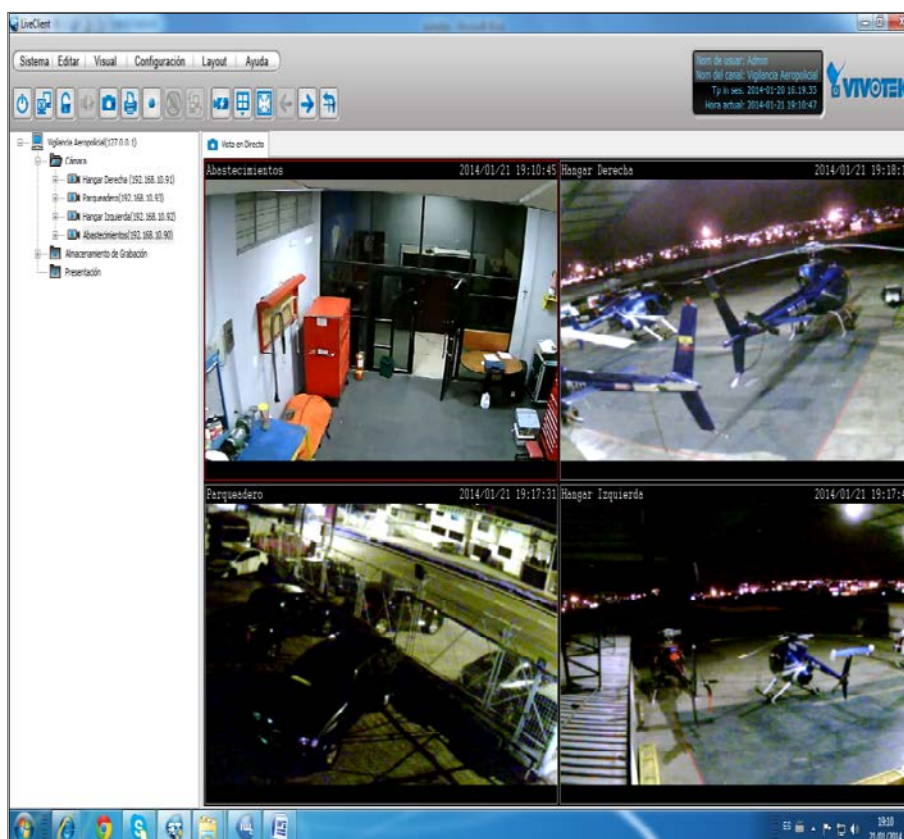


Figura 3.30 Pantalla de visualización tiempo real

3.11.12 Ajustes de visualización de los canales Playback

Para la visualización de los eventos ingresamos en este apartado en donde estarán los archivos de los videos y que se podrá reproducir todas a la vez o individualmente.

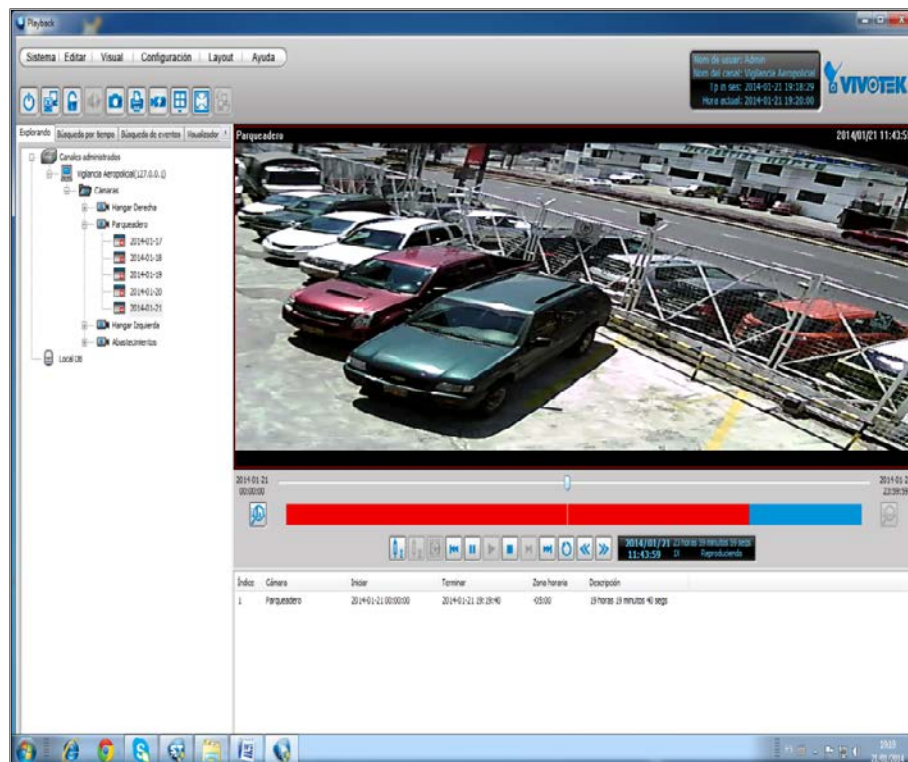


Figura 3.31 Pantalla de visualización de archivos de video

3.11.13 Pruebas de funcionalidad

Para constatar la conectividad de las cámaras ingresamos al cmd, en donde realizamos un ping ingresamos cada una de las direcciones IP.

3.11.14 Visualización de videos en tiempo real y respaldos

Estos datos están disponibles en el computador que esta como servidor de eventos y a la vez muestra en tiempo real las zonas vigiladas.

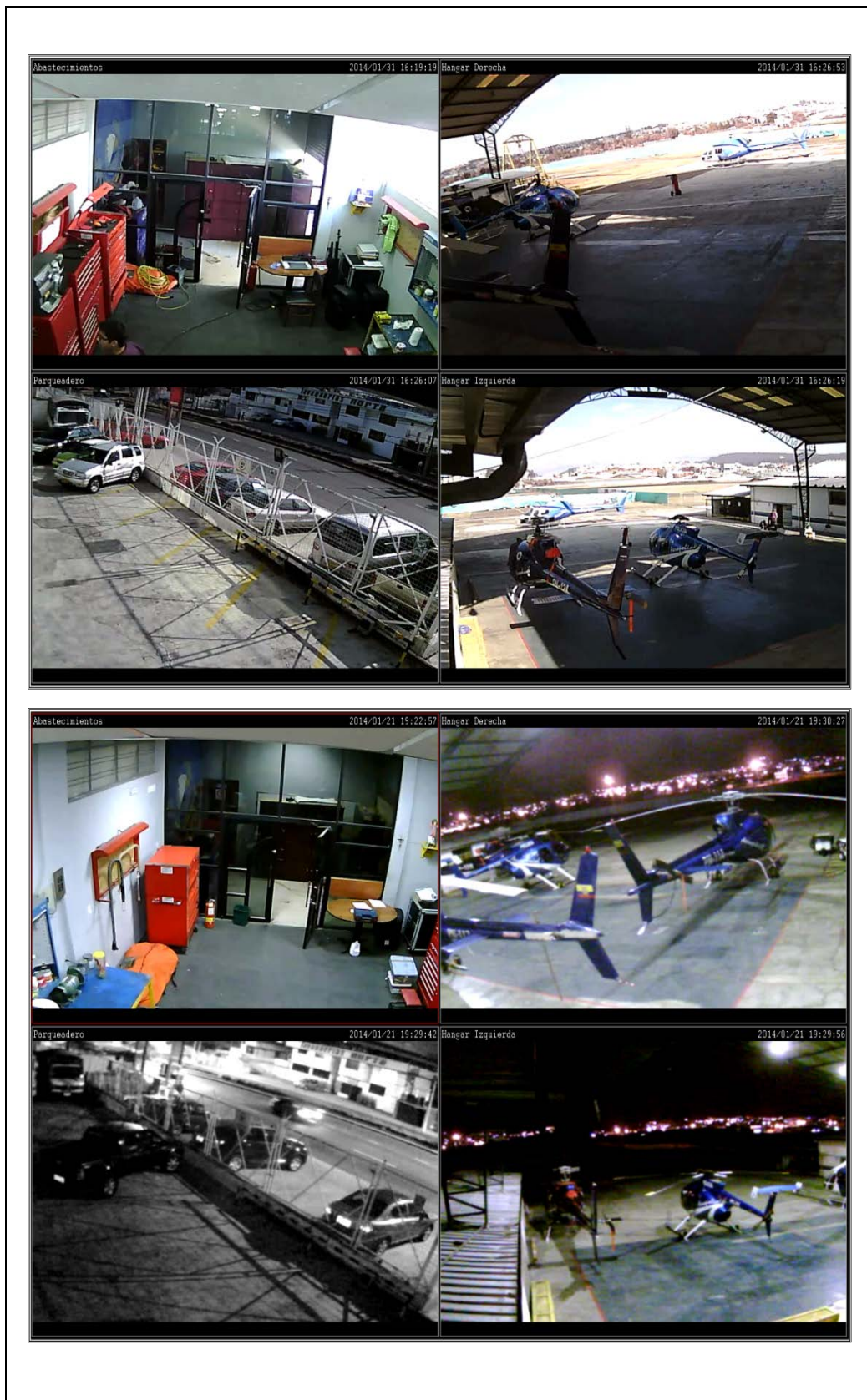


Figura 3.32 Visualización de zonas monitoreadas diurna y nocturna

3.11.15 Visualización de eventos-respaldos

Estos datos están alojados en el computador que esta como servidor en donde se visualiza los eventos de los días anteriores. (Cinco días)

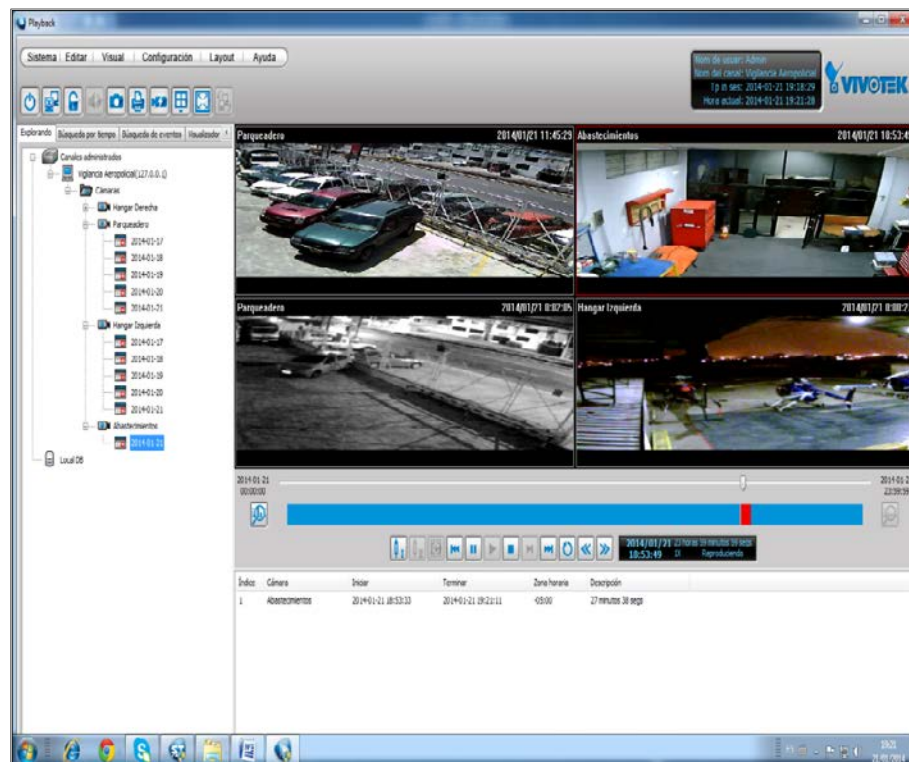


Figura 3.33 Pantalla de visualización de eventos

3.11.16 Servicios que proporciona la red de vigilancia

El sistema de vigilancia tiene las siguientes características o servicios:

- ✓ Monitoreo en tiempo real: se visualiza en el mismo instante las señales provenientes de las cámaras instaladas en las diversas áreas.
 - ✓ Grabación controlada de eventos o constante: el sistema permite grabar las imágenes provenientes de todas las cámaras de manera constante o controlada específicamente para cada una.
- Se debe guardar la información importante y la información que

no se necesite se debe desechar o eliminar.

- ✓ Búsqueda en tiempo real: búsqueda de imágenes grabadas por fecha, hora y cámara.
- ✓ Monitoreo en pantallas múltiples: simultáneamente permite dividir la pantalla y mostrar las señales de todas las cámaras en el mismo monitor.
- ✓ Fácil uso con una interface de usuario amigable: la interfaz del sistema es fácil de utilizar y no requiere mayor destreza de parte de los usuarios.
- ✓ Imágenes digitales de alta resolución (sin degradación). Las cámaras permiten una alta resolución de las imágenes.
- ✓ Bajos costos en manejo, operación y mantenimiento: la red es fácil de administrar; su sistema es fácil de operar y sobre todo el mantenimiento es de poco costo.
- ✓ Niveles de protección de contraseñas: el sistema permite el control de acceso a la red, a los archivos y a las señales provenientes de las cámaras; para lo cual cuenta con un sistema de contraseñas de usuarios.

3.12 Manual

3.12.1 Descripción del manual de mantenimiento

Este manual servirá de ayuda al momento de manipular los equipos de la red de vigilancia y a la vez dar el respectivo mantenimiento preventivo para tener un buen funcionamiento, de esta manera alargar la vida útil de todos los equipos tecnológicos.

El siguiente manual de buen uso de los equipos de la red de vigilancia está dividido en 5 secciones:

- ✓ Objetivo
- ✓ Alcance
- ✓ Precauciones

- ✓ Mantenimiento
- ✓ Procedimiento

3.12.2 Descripción General

En el manual se encontrara los pasos básicos a seguir para realizar un mantenimiento preventivo empleando normas de seguridad y conservación de los equipos.

Las normas que se deben tomar no están por demás advertirlas, tomando en cuenta que los equipos no son de gran tamaño, pero con ello evitamos incidentes o accidentes al momento de la manipulación.

VER ANEXO D

3.13 Estudio Económico

El estudio costo beneficio es un factor importante y necesario porque permite determinar el precio real en la implementación de la red de vigilancia.

Una vez terminada la implementación se detalla con precisión los valores económicos empleados en equipos y materiales.

3.13.1 Análisis de Costos

En la elaboración e implementación del proyecto se realizaron los siguientes gastos, siendo todos de importancia, considerando el siguiente orden.

3.13.1.1 Costos Primarios

En los costos primarios tenemos:

- ✓ Costos equipos
- ✓ Costos materiales

3.13.1.2 Costos Secundarios

En los costos secundarios tenemos:

- ✓ Derechos de grado
- ✓ Elaboración de textos

3.13.1.3 Costos Total del proyecto

En el valor total empleado en el desarrollo del proyecto tenemos:

- ✓ Costos primarios
- ✓ Costos Secundarios

Valores de equipos.

Tabla 3.2

Tabla costos de equipos

Nombre	Cantidad	Característica	Valor Unitario USD	Valor Total USD
Monitor	1	HP	200,00	200,00
CPU	1	HP	750,00	750,00
Teclado	1	HP	25,00	25,00
Mouse	1	HP	10,00	10,00
Cámara IP 8331	4	VIVOTEK	350,00	1400,00
Switch 8 Puertos	1	TRENDnet	25,00	25,00
Switch 5 Puertos	1	TRENDnet	17,00	17,00
Regulador de voltaje	1	AVRPRO	35,00	35,00
TOTAL				2462,00

Elaborado por: Juan Carlos Morales

Valores de materiales.

Tabla 3.3

Tabla costos de materiales

Nombre	Material	Cantidad	Característica	Valor Unitario USD	Valor Total USD
Tomacorriente	Plástico	5	Triple	2,50	12,50
Conector	Plástico	50	RJ-45	0,20	10,00
Capuchón de conector	Caucho	50	RJ-45	0,17	8,50
Enchufe	Plástico	5	110 V	0,80	4,00
Alambre gemelo	Caucho	150 m	2x16	0,55	82,50
Brocas	Acero, Cemento	4	11/64"	1,50	6,00
Tornillos	Acero	70	3/4x4 RG	0,05	3,50
Taco Fijer	Plástico	70	F4	0,02	1,40
Cable UTP	Caucho	400 M	Categoría 5E	0,75	300,00
Canaletas	Plástico	100		0,85	85,00
TOTAL					513,40

Elaborado por: Juan Carlos Morales

Total de valores empleados en costos primarios.

Tabla 3.4

Tabla del total de costos de primarios

Nº	Detalle	Valor en USD
1	Costos de Materiales	513,40
2	Costos de Equipos	2462,00
TOTAL		2975,40

Elaborado por: Juan Carlos Morales

Valores de derechos de grado y elaboración de textos.

Tabla 3.5

Tabla del total de costos secundarios

Nº	Detalle	Valor en USD
1	Derechos de Grado	300
2	Elaboración de textos	250
TOTAL		550

Elaborado por: Juan Carlos Morales

Valores de derechos de grado y elaboración de textos.

Tabla 3. 6

Tabla del total de costos del proyecto

Nº	Detalle	Valor en USD
1	Gastos Primarios	2975,40
2	Gastos Secundarios	550,00
TOTAL		3525,40

Elaborado por: Juan Carlos Morales

3.14 Ubicación de la cámara 1

Esta cámara de vigilancia es para la bodega, rastrillo y simulador de vuelo.



Figura 3.34 Ubicación cámara 1

3.15 Ubicación de la cámara 2

Esta cámara monitoreara el hangar desde el lado derecho.



Figura 3.35 Ubicación cámara 2

3.16 Ubicación de la cámara 3

Esta cámara monitoreara el hangar desde el lado izquierdo, bombas de combustible y puerta de acceso a las bodegas.



Figura 3.36 Ubicación cámara 3

3.17 Ubicación de la cámara 4

Esta cámara monitoreará los parqueaderos interno y principalmente el externo.



Figura 3.37 Ubicación cámara 4

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- ✓ Con el apoyo del Servicio Aeropolicial fue posible la adquisición de los equipos necesarios para implementación de la red de vigilancia utilizando cámaras de tecnología IP.
- ✓ La cámara **IP de VIVOTEK** fue elegida por su resistencia, característica propia de la cámara ya que esta puede soportar las inclemencias del tiempo tales como la lluvia, polvo evitando así el uso de accesorios adicionales.
- ✓ Al elegir el cuarto de monitoreo se determinó que el lugar más adecuado es la garita o prevención ya que allí se encuentra el personal de guardia lo que permitirá un monitoreo continuo de las instalaciones, además por su ubicación permitirá tomar acciones de forma oportuna ante cualquier eventualidad.
- ✓ La red de vigilancia implementada es un complemento a la guardia, por ello necesita el monitoreo del personal de seguridad ya que no garantiza la no ocurrencia de hechos delictivos u otro tipo, porque esto dependerá de factores físicos, humanos y de cobertura de la cámara IP en las diferentes zonas.
- ✓ Gracias a la accesibilidad remota permite que cualquier usuario autorizado que disponga del servicio de internet, pueda acceder a la red de vigilancia en cualquier momento y así pueda visualizar imágenes y/o en vídeo en tiempo real, archivos grabados o realizar configuraciones de las cámaras IP.
- ✓ Con la implementación de la presente red de vigilancia se posee un sistema de seguridad escalable, confiable y de gran capacidad en el caso de que las necesidades futuras así lo requieran, debido a que el sistema puede ampliarse añadiendo más cámaras de red y aumentando la capacidad de almacenamiento.

4.2 Recomendaciones

- ✓ Con el fin de mejorar la vigilancia en las instalaciones del Servicio Aeropolicial de Quito es preciso seguir implementando medios y equipos tecnológicos que brinden apoyo al personal de guardia.
- ✓ El período de almacenamiento configurado en el servidor es de 5 días por lo que se recomienda sacar respaldos de los eventos más importantes de éste período para su posterior análisis.
- ✓ Una vez finalizada la fase de instalación se debe realizar un cronograma de mantenimiento preventivo periódico de los equipos y componentes que forman parte del sistema de seguridad al menos cada 6 meses con el fin de garantizar su pleno funcionamiento, cabe mencionar que el servicio de mantenimiento debe constar de: limpieza de cámaras, limpieza física del Servidor o PC, limpieza de discos duros, chequeo de funcionamiento global y organización de las bases de datos.
- ✓ Si presenta alguna falla en el funcionamiento de una o más cámaras IP se recomienda al administrador observar todas las especificaciones y normas técnicas dadas por el fabricante.
- ✓ Se debe tomar en cuenta que el software ST7501 utilizado para la gestión de video por ser una versión libre permite un número limitado de 32 canales de visualización y grabación simultáneo, de los cuales 4 canales ya fueron ocupados, si se requiere una ampliación de la red de cámaras es necesario adquirir la licencia del software.
- ✓ Es necesario que el administrador de la red de vigilancia IP instruya al personal policial en la operación del sistema de seguridad con el fin de evitar daños no intencionados.

GLOSARIO

A

RLE.- La compresión RLE o Run-length encoding es una forma muy simple de compresión de datos en la que secuencias de datos con el mismo valor consecutivas son almacenadas como un único valor más su recuento.

AMPS.- Sistema Telefónico Móvil Avanzado.

APPLETALK.- Protocolo de comunicación para ordenadores Apple Macintosh.

ASF.- De Advanced Streaming Format (o ASF, posteriormente renombrado a Advanced Systems Format) es un formato contenedor digital propiedad de Microsoft, diseñado especialmente para el streaming.

AVI.- De Audio Video Interleave, es un formato contenedor de audio y video lanzado por Microsoft en 1992.

AVO.- Objetos audiovisuales.

B

B/N.- blanco y negro.

BALUN DE VIDEO.- De Balanced-Unbalanced Lines Transformer, se denomina balun a un dispositivo adaptador de impedancias que convierte líneas de transmisión no balanceadas en líneas balanceadas (se transmite la misma información por dos cables o par de cables, al mismo tiempo y con polaridades opuestas). La inversa también es cierta: el balun es un dispositivo reversible.

BANDAS ISM.- De Industrial Scientific and Medical, son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (Wi-Fi) o WPAN (Bluetooth).

BGP.- De Border Gateway Protocol, es un protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

BI-DIRECCIONAL.- Que envía y recibe o transmite y emite es un término utilizado

en las telecomunicaciones para definir a un sistema que es capaz de mantener una comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea.

BMP.- Un archivo BMP es un archivo de mapa de bits, es decir, un archivo de imagen de gráficos, con píxeles almacenados en forma de tabla de puntos que administra los colores como colores reales o usando una paleta indexada.

BROADCAST.- Difusión en español, es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

BUFFERING.- Cuando quiero ver un video, aparece la palabra buffering.Cuál es el significado en español.

C

CABLE STP.- STP, acrónimo de Shielded Twisted Pair (Par Trenzado Apantallado).

Es similar al cable UTP, con la diferencia que cada par tiene una pantalla protectora, además de tener una lamina externa de aluminio o de cobre trenzado alrededor del conjunto de pares, diseñada para reducir la absorción del ruido eléctrico. Este cable es más costoso y difícil de manipular que el UTP. Se emplea en redes de ordenadores como Ethernet o Token Ring.

CABLE UTP.- UTP, acrónimo de unshielded twisted pair o par trenzado sin apantallar.

Son cables de pares trenzados sin apantallar que se utilizan para diferentes tecnologías de red local. Son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.

CCD o ICCD.- Dispositivo de Cargas Acopladas o Interconectadas, que permite no sólo recibir una señal óptica, sino amplificarla.

CCTV.- Circuito Cerrado de Televisión cuyas siglas es CCTV, proviene del inglés Closed Circuit Television

CDM.- Acceso Múltiple por División de Código

CMY.- Cyan (un verde azulado), Magenta (rojo violáceo) y Yellow (amarillo).

CMYK.- El modelo CMYK (acrónimo de Cyan, Magenta, Yellow y Key) es un modelo de color sustractivo que se utiliza en la impresión en colores. Es la versión moderna y más precisa del ya obsoleto modelo de color RYB, que se utiliza aún en pintura y bellas artes. Permite representar una gama de color más amplia que este último, y tiene una mejor adaptación a los medios industriales.

CODECS.- Códec es la abreviatura de codificador-decodificador. Describe una especificación desarrollada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos (stream) o una señal. Los códecs pueden codificar el flujo o la señal (a menudo para la transmisión, el almacenaje o el cifrado) y recuperarlo o descifrarlo del mismo modo para la reproducción o la manipulación en un formato más apropiado para estas operaciones.

Los códecs son usados a menudo en videoconferencias y emisiones de medios de comunicación.

COMPRESIÓN LZW.- Lempel-Ziv-Welch. Método de compresión sin pérdidas de calidad que nos permite reducir el tamaño de un archivo TIFF a la mitad aproximadamente.

COMPRESIÓN ZIP.- Es un formato de compresión sin pérdida, muy utilizado para la compresión de datos como documentos, imágenes o programas.

CONECTORES BNC.- De Bayonet Neill-Concelman, es un tipo de conector, de rápida conexión/desconexión, utilizado para cable coaxial.

CUANTIZACIÓN.- El proceso de cuantificación es uno de los pasos que se sigue para lograr la digitalización de una señal analógica.

Básicamente, la cuantificación lo que hace es convertir una sucesión de muestras de amplitud continua en una sucesión de valores discretos preestablecidos según el código utilizado.

D

DATAGRAMA.- Los datagramas IP son las unidades principales de información de Internet. Los términos trama, mensaje, paquete de red y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

DCT.- La transformada de coseno discreta (DCT del inglés Discrete Cosine

Transform) es una transformada basada en la Transformada de Fourier discreta, pero utilizando únicamente números reales.

DHCP.- De Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica del Host.

DIRECCIÓN IP.- Es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

DVR.- (vídeo grabador digital)

Es un dispositivo que le permite grabar y ver programas cuando es conveniente para usted sin el uso de un video o disco. Puede grabar un solo programa de TV o una serie con sólo apretar un botón. Puede pausarlo, pasar hacia atrás o pasar hacia adelante la TV en vivo usando su control remoto.

E

EIGRP.- Enhanced Interior Gateway Protocol, es un protocolo de

enrutamiento interior desarrollado por Cisco Systems.

Su diseño, configuración y administración se orienta hacia su implementación en redes grandes y complejas; EIGRP es llamado Protocolo de Enrutamiento Híbrido por presentar características de un protocolo de enrutamiento Estado-Enlace y Vector Distancia.

El formato no especifica cómo debe ser codificado en vez de eso sólo especifica la estructura del flujo de video/audio.

F

FRAME.- Un frame, fotograma o cuadro es una imagen particular dentro de una sucesión de imágenes que componen una animación. La continua sucesión de estos fotogramas producen a la vista la sensación de movimiento, fenómeno dado por las pequeñas diferencias que hay entre cada uno de ellos.

FRECUENCIA DE CLOCK.- La frecuencia de reloj indica la velocidad a la que un ordenador realiza sus operaciones más básicas, como sumar dos números o transferir el valor de un registro a otro.

G

GIF.- Graphic Interchange Format, es un formato sin pérdida de calidad para imágenes con hasta 256 colores, limitados por una paleta restringida a este número de colores. Por ese motivo, con imágenes con más de 256 colores (profundidad de color superior a 8), la imagen debe adaptarse reduciendo sus

colores, produciendo la consecuente pérdida de calidad.

GSM.- Sistema Global para las Comunicaciones Móviles.

H

HAZ DE LUZ.- Región del espacio que ocupa una corriente unidireccional

de radiación electromagnética o grupo de ondas emitidas, o sea un rayo de luz

HFC.- Hybrid Fibre Coaxial (Fibra híbrida coaxial).

En Telecomunicaciones, es un término que define una red que incorpora tanto fibra óptica como cable coaxial para crear una red de banda ancha

HUB O SWITCH.- Dispositivo que crea la red. Para que 2 o más equipos estén conectados a la misma red, primero tienen que estarlo físicamente ya sea mediante cable o Wifi para que puedan intercambiar datos entre ellos.

I

IBM.- International Business Machines o IBM, conocida coloquialmente como el Gigante Azul, es una empresa que fabrica y comercializa hardware, software y servicios relacionados con la informática.

IEEE.- Instituto de Ingenieros Eléctricos y Electrónicos.

Se trata de una asociación sin ánimo de lucro radicada en Estados Unidos, aunque de ámbito internacional.

INTERNET.- Interconexión de redes informáticas que permite a los ordenadores o

IP.- Protocolo de Internet.

IPX.- Internetwork Packet Exchange o IPX en español (intercambio de paquetes interred) es un protocolo de la capa de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

ISO.- Organización Internacional de Normalización.

J - L

JPEG.- De Joint Photographic Experts Group, Grupo Conjunto de Expertos en Fotografía es el nombre de un comité de expertos que creó un estándar de compresión y codificación de archivos e imágenes fijas.

LAN.- De Local Área Network. Red de Área Local son redes de propiedad

privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud.

LOOPBACK.- Esta dirección se suele utilizar cuando una transmisión de datos tiene como destino el propio host. También en tareas de diagnóstico de conectividad y validez del protocolo de comunicación.

LZW.- (Lempel-Ziv-Welch) es un algoritmo de compresión sin pérdida desarrollado por Terry Welch en 1984 como una versión mejorada del algoritmo LZ78 desarrollado por Abraham Lempel y Jacob Ziv.

M

MCU.- Acrónimo de Multipoint Control Unit (Unidad de control multipunto)

MODELO OSI.- Open Systems Interconnection - Interconexión de Sistemas Abiertos) Norma universal para protocolos de comunicación lanzado en 1984. Fue propuesto por ISO y divide las tareas de la red en siete niveles.

MODELO TCP/IP.- Es el estándar histórico y técnico de la Internet, modelo que sirve y ha servido de desarrollo para la Internet.

MOV.- Es un formato de multimedios en este caso de video *.mpeg *.mov *.flv son las extensiones que el sistema operativo usa para saber de qué archivo se trata y con qué programa abrirlo.

MPEG.- Grupo de Expertos en Imágenes en movimiento el MPEG1 es el formato de video que utilizan los VCD (vcd o películas piratas en cd), y el MPEG2 es calidad DVD. En si es sólo el formato de video para lectoras de DVD.

MULTICAST.- Multidifusión (inglés multicast) es el envío de la información en múltiples redes a múltiples destinos simultáneamente.

N

NETBEUI.- (NetBIOS Extended User Interface, en español Interfaz extendida de usuario de NetBIOS), es un protocolo de nivel de red sin encaminamiento y bastante sencillo utilizado como una de las capas en las

primeras redes de Microsoft. NetBIOS sobre NetBEUI es utilizado por muchos sistemas operativos desarrollados en 1990, como LAN Manager, LAN Server, Windows 3.x, Windows 95 y Windows NT.

NETBIOS.- Network Basic Input/Output System, NetBIOS permite comunicación orientada a conexión (TCP) o no orientada a conexión (UDP). Soporta tanto broadcast como multicast, además de 4 tipos de servicios diferentes: Servicios Generales, Servicio de Nombres, Servicio de Sesión y Servicio de Datagramas.

NIC.- Centro de Información de Red, NIC proviene de la abreviatura del término inglés Network Information Center, y es un organismo encargado de asignar las direcciones IP a los ordenadores que se conectan a la red global, así como también controlar y asignar los dominios de cada país.

NTSC.- Llamado así por las siglas de National Television System Committee, (en español Comisión Nacional de Sistema de Televisión)¹ es el sistema de televisión analógico que se ha empleado en América del Norte, América Central, la mayor parte de América del Sur y Japón entre otros. Un derivado del NTSC es el sistema PAL que se emplea en Europa y algunos países de Sudamérica como Argentina, Uruguay y Brasil. NVR .- Grabadores Digitales de Red / Network Video Recorders

O

OSPF.- De las siglas de Open Shortest Path First (El camino más corto primero), un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), para calcular la ruta más idónea.

P

PAINT SHOP PRO.- Paint Shop Pro (PSP) es un editor de gráficos rasterizados y editor de gráficos vectoriales para PC que funciona sobre el sistema operativo Microsoft Windows.

PAL.- De la sigla de Phase Alternating Line (Línea de fase alternada). Es

el nombre con el que se designa al sistema de codificación utilizado en la transmisión de señales de televisión analógica en color en la mayor parte del mundo. Se utiliza en la mayoría de los países africanos, asiáticos y europeos, además de Australia y algunos países americanos.

PCX.- De (PiCture eXchange) es un formato de imagen digital que usa la forma

simple de la codificación run-length (un tipo de compresión sin pérdidas).

PDA.- Sigla de la expresión inglesa Personal Digital Assistant, 'asistente digital personal', agenda electrónica que incluye muchas de las funciones de una computadora portátil.

PDU.- Las Unidades de Datos de Protocolo, también llamadas PDU, se utilizan para el intercambio de datos entre unidades disparejas, dentro de una capa del modelo OSI.

PNG.- Portable Network Graphics PNG siglas en inglés (Gráficos de Red Portátiles, pronunciadas "ping") es un formato gráfico basado en un algoritmo de compresión sin pérdida para bitmaps no sujeto a patentes. Este formato fue desarrollado en buena parte para solventar las deficiencias del formato GIF y permite almacenar imágenes con una mayor profundidad de contraste y otros importantes datos.

Por otro lado también son un formato es decir la forma en que estarán almacenados los bit y como los interpretara el programa que los abre esto es a dos partes el archivo (formato mpeg, mov, flv) y por el otros lado el programa con un codec para que pueda usarlos.

PPI.- Píxeles por pulgada (PPP), en inglés pixels per inch (PPI), es una medida de resolución de vídeo relacionada al tamaño del monitor en pulgadas (inch) y del número total de píxeles en la dirección horizontal y en la dirección vertical.

Q - R

QUARKXPRESS.- Es un programa de autoedición para ordenadores Mac OS X y Windows.

RDSI.- Red Digital de Servicios Integrados (RDSI o ISDN en inglés), red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

RGB.- En inglés Red, Green, Blue, en español rojo, verde y azul, es la composición del color en términos de la intensidad de los colores primarios de la luz.

RIP.- En español Ripear, es el proceso de copiar los datos de audio y vídeo de un dispositivo multimedia, (como un CD, DVD, o HD DVD), a un disco duro

RJ-45.- (registered jack 45) es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). 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.

S

SAP.- Servicio Aeropolicial.

SECAM.- De Séquentiel Couleur à Mémoire, en francés, "Color secuencial con memoria". Es un sistema para la codificación de televisión en color analógica utilizado por primera vez en Francia.

SEGMENTO O DATAGRAMA.- Un datagrama es un fragmento de paquete (análogo a un telegrama) que es enviado con la suficiente información para que la red pueda simplemente encaminar el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ETD destino.

SPX.- Son las siglas en inglés de Sequenced Packet Exchange (Intercambio de Paquetes Secuenciados). Es un protocolo de la Capa de transporte

responsable de actuar sobre el protocolo IPX para asegurar la entrega de los paquetes.

T

TCP.- Protocolo de Control de Transmisión.

TDMA.- La multiplexación por división de tiempo (Time Division Multiple Access o TDM) es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión. El Acceso múltiple por división de tiempo (TDMA) es una de las técnicas de TDM más difundidas.

TIFF.- (Tagged Image File Format) es un formato de archivo informático para imágenes.

Un aspecto muy práctico del formato TIFF es que permite almacenar más de una imagen en el mismo archivo.

Un mito que ha de desterrarse es la idea de que el formato TIFF no permite comprimir las imágenes.

TOKEN PASSING.- Es un Protocolo y también se le conoce como protocolo de paso de testigo es un método de acceso al medio determinístico que se utiliza en diferentes redes que disponen de un anillo lógico: token Ring o Token Bus.

TOKEN RING.- Token Ring es una arquitectura de red desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado token que viaja alrededor del anillo.

TOKEN BUS.- Token Bus es un protocolo para redes de área local con similitudes a Token Ring, pero en vez de estar destinado a topologías en anillo está diseñado para topologías en bus.

Es un protocolo de acceso al medio en el cual los nodos están conectados a un bus o canal para comunicarse con el resto. En todo momento hay un

testigo (token) que los nodos de la red se van pasando, y únicamente el nodo que tiene el testigo tiene permiso para transmitir. El bus principal consiste en un cable coaxial.

U, V

VIOLÁCEO.- Color como el de la violeta; es el séptimo color del espectro solar.

UPS.- Sistema de alimentación ininterrumpida.

VGA.- es la abreviatura de Video Graphics Array (Tabla de Gráficos de Vídeo).

W

WAN.- Una red de área amplia, o WAN, por las siglas de (wide area network en inglés), es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales, llamadas LAN, por lo que sus miembros no están todos en una misma ubicación física.

WLAN.- Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local area network), es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Estas redes van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central.

WLL.- El bucle local inalámbrico (Wireless local loop (WLL), radio in the loop (RITL), fixed-radio access (FRA) o fixed-wireless access (FWA) en inglés), es el uso de un enlace de comunicaciones inalámbricas como la conexión de "última milla" para ofrecer servicios de telefonía (POTS) e Internet de banda ancha a los usuarios. Se trata principalmente del uso de frecuencias

licenciadas, descartándose las llamadas "bandas libres" debido a la carencia de garantías, por tratarse de frecuencias de uso compartido, con el correspondiente riesgo de saturación e indisponibilidad de la red.

Z

Zoom.- Óptica en la que podemos escoger diferentes distancias focales, puede ser de accionamiento mecánico (habitual en las ópticas zoom de los equipos reflex) o electrónico (en la mayoría de los modelos compactos).

BIBLIOGRAFÍA

- ✓ Telecomunicaciones y telemática; autor Álvaro Torres Nieto, Rubén Darío Sánchez, editorial Escuela Colombiana de Ingeniería, 3ra edición 2007.
- ✓ Comunicaciones y redes de computadoras; autor William Stallings, editorial Pearson Prentice Hall, 7ma edición 2004.
- ✓ Redes y conectividad; autor y editorial Editorial Macro.
- ✓ Comunicaciones y redes de computadoras; autor William Stallings, editorial Prentice Hall 2000.
- ✓ Microsoft fundamentos de redes-plus; autor Microsoft Corporation, 1ra edición 2000 McGraw-Hill.
- ✓ Redes de comunicación, conceptos fundamentales y arquitectura básica; autor Alberto Leon Garcia, editorial McGraw-Hill 1ra edición 2002.
- ✓ Teleinformática y Redes de computadoras; coordinado por Antonio Alabua, editorial Alfa y Omega, 2da edición.

NET GRAFÍA

- ✓ <http://spanish.howtsetupwebcam.com/news-categories/network-cameras-reviews-manuals-drivers-software>
[en línea]
- ✓ <http://www.gscssoftware.com/teccamaraip.htm>
[en línea]
- ✓ <http://www.voxdata.com.ar/voxseguip.html>
[en línea]
- ✓ http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/protocol1.htm
[en línea]
- ✓ <http://usuarios.multimania.es/janjo/janjo1.html>
[en línea]

- ✓ http://es.wikipedia.org/wiki/Cableado_estructurado
[en línea]
- ✓ http://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf
[en línea]
- ✓ http://www.gmtvaritec.com/portal/index.php?option=com_content&view=article&id=91&Itemid=55
[en línea]
- ✓ <http://www.seguridadporinternet.com/>
[en línea]
- ✓ http://www.camarasip.cl/que_es_una_camara_ip.htm
[en línea]
- ✓ <http://www.sitiosargentina.com.ar/notas/2009/junio/camara-ip.htm>
[en línea]
- ✓ <http://www.ite.educacion.es/formacion/materiales/84/cd/curso/anexo3.htm>
[en línea]
- ✓ http://www.midisec.com/index.php?option=com_content&view=article&id=64:introduccion-a-sistemas-vigilancia-ip&catid=42:introduccion-a-las-tecnologias&Itemid=67
[en línea]
- ✓ <http://www.ite.educacion.es/formacion/materiales/107/cd/imagen/imagen0105.html>
[en línea]
- ✓ http://electronica.ugr.es/~amroldan/asignaturas/curso01-02/tv1/material/guia_tv.htm
[en línea]
- ✓ <http://www.draokon.com/blog/tipos-formatos-imagen-donde-es-mejor-utilizarlos>
[en línea]
- ✓ <http://aitorlarumbe.com/2012/07/tutorialmezcla-aditiva-rgb-y-mezcla-sustractiva-cmyk/>

[en línea]

- ✓ <http://es.kioskea.net/contents/187-conector-rj45>

[en línea]

- ✓ <http://www.textoscientificos.com/redes/comunicaciones/modos>

[en línea]

- ✓ http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/modelo_osi.htm

[en línea]

- ✓ <http://mediosdetransmisionnoguiados.blogspot.com/>

[en línea]

- ✓ <http://www.eduteka.org/VideoDigitalCamara.php>

[en línea]

- ✓ http://www.marbit.es/index_ip.html

[en línea]

- ✓ <http://www.fotonostra.com/digital/digitalizarvideo.htm>

[en línea]

- ✓ <http://mediosdetransmisionnoguiados.blogspot.com/>

[en línea]

- ✓ http://www.tvc.mx/tienda/catalog/product_info.php?products_id=2651

[en línea]