ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA WLAN Y CÁMARAS DE SEGURIDAD IP PARA HOSTAL LA CAROLINA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

WILMAN SANTIAGO MALDONADO ERAZO
san_cayo@hotmail.com

DIRECTOR: ING. CÉSAR GALLARDO
cesar.gallardo@epn.edu.ec

Quito, junio de 2009

DECLARACIÓN

Yo, Wilman Santiago Maldonado Erazo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Wilman Santiago Maldonado Erazo

CERTIFICACIÓN

Certifico que el presente trabajo de tesis, fue desarrollado en su totalidad por Wilman Santiago Maldonado Erazo, bajo mi supervisión.

Ing. César Gallardo
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios que es el ser que me da fortaleza, apoyo y sabiduría para culminar con éxito esta etapa estudiantil que me servirá para desarrollarme profesionalmente.

A mis hijos Mateo y Cinthya, que son mi inspiración y los que me impulsan para esforzarme cada día y dar lo mejor de mí.

A mi esposa Cristina por su apoyo incondicional de cada día.

A mi Director de Tesis Ing. César Gallardo que con sus conocimientos y apoyo constante he podido llevar a cabo este proyecto de tesis.

A mis padres que me apoyan en todo momento y me enseñaron que en la vida se consigue todo a base de mucho trabajo y esfuerzo, además de la humildad que debe estar en todo momento.

A la Escuela Politécnica Nacional y en especial a la Escuela de Formación de Tecnólogos, donde encontré la formación personal y profesional.

DEDICATORIA

A Dios que siempre me ha llenado de tranquilidad y bendiciones, para seguir adelante y poder culminar mi carrera con satisfacción.

A mis hijos Mateo y Cinthya que han llegado a mi vida para llenarme cada día de su amor, cariño y es por eso son la razón de mi esfuerzo y dedicación, para poder ser su ejemplo, su fortaleza y hacer de ellos unas personas de bien.

A mi esposa Cristina que ha estado apoyándome siempre y brindándome su amor incondicional siendo el motor para salir adelante.

A mis padres que me han dado su apoyo, pero sobre todo su amor.

RESUMEN

El presente proyecto tiene por objetivo la implementación y configuración de una red inalámbrica WLAN y cámaras de seguridad IP, la misma que garantizará a los clientes de la empresa el fácil y rápido acceso al servicio de Internet en un área de 300 m^2. A su vez las cámaras de vigilancia fortalecerán la seguridad para todos los huéspedes en el cuidado de sus pertenencias. Por consiguiente se ha visto que las alternativas de solución son apropiadas, luego de realizar el análisis correspondiente.

Para el desarrollo del trabajo se ha dividido en cuatro capítulos diferentes:

El primer capítulo trata de la identificación del problema, de las necesidades, objetivos, alcance y meta de la conexión inalámbrica y cámaras de seguridad IP en Hostal La Carolina.

En el segundo capítulo se realiza el estudio teórico de la tecnología de redes inalámbricas, y cámaras de seguridad IP, además la definición de los dispositivos que intervienen en un enlace inalámbrico, y de vigilancia IP: tarjetas, Access Point, antenas, cámaras entre otros. Así como el estudio más profundo de las seguridades sobre ataques y accesos no autorizados a la red.

En el Tercer capítulo se analizan las alternativas de solución que se disponen en el mercado, haciendo hincapié en la tecnología, compatibilidad, precio de los equipos a utilizar.

En el cuarto capítulo se desarrolla la implementación y configuración de la red WLAN y cámaras de seguridad IP, además de las pruebas que dan solución al problema planteado.

Luego de haber implementado el presente proyecto se ha llegado a las conclusiones y recomendaciones las mismas que se detallan al final del documento.

ÍNDICE

CAPÍTULO 1 1
1.1 ANTECEDENTES 1
1.2 OBJETIVOS 2
1.2.1 OBJETIVO GENERAL 2
1.2.2 OBJETIVOS ESPECÍFICOS 2
1.3 JUSTIFICACION ..... - 2 -
1.4 ALCANCE Y META 3
CAPITULO 2 ..... - 4 -
2.1 MARCO REFERENCIAL 4
2.2 ¿QUÉ ES UNA RED? 4
2.3 CARACTERÍSTICAS DE UNA RED DE ÁREA LOCAL 5
2.4 TOPOLOGÍAS DE UNA RED 7
2.4.1 Topología de red en bus 7
2.4.2 Topología en Anillo 8
2.4.3 Topología en Estrella. 9
2.4.4 Topología en Árbol. 10
2.4.5 Topoltogía en Malla: 11
2.4.6 Topología de red celular 12
2.5 ARQUITECTURA DE REDES 13
2.5.1 Modelo de Referencia OSI 13
2.5.1.1 Capa de Aplicación 15
2.5.1.2 Capa de Presentación 15
2.5.1.3 Capa de Sesión 16
2.5.1.4 Capa de Transporte 16
2.5.1.5 Capa de Red 17
2.5.1.6 Capa de Enlace de Datos 17
2.5.1.7 Capa Física 18
2.5.2 ARQUITECTURA DEL MODELO TCP/IP 19
2.5.2.1 Capa de Red Física 20
2.5.2.2 Capa de Enlace de datos 21
2.5.2.3 Capa de Internet 21
2.5.2.3.1 Protocolo IP 21
2.5.2.3.2 Protocolo ARP 22
2.5.2.3.3 Protocolo ICMP 22
2.5.2.4 Capa de Transporte 23
2.5.2.4.1 Protocolo TCP 23
2.5.2.4.2 Protocolo SCTP 24
2.5.2.4.3 Protocolo UDP 24
2.5.2.5 Capa de Aplicación 24
2.5.2.5.1 Servicios TCP/IP estándar 25
2.5.2.5.1.1 FTP y FTP anónimo 25
2.5.2.5.1.2 Telnet 25
2.5.2.5.1.3 TFTP 25
2.5.2.5.2 Servicios de Nombres 26
2.5.2.5.2.1 DNS 26
2.5.2.5.2.2 NIS 26
2.5.2.5.3 Servicio de Directorios 26
2.5.2.5.4 Administración de la red 26

2.5.2.5.5 Protocolos de encaminamiento 27
2.6 MEDIOS DE TRANSMISIÓN 27
2.6.1 Medios guiados 27
2.6.1.1 Cable Coaxial 28
2.6.1.2 Cable Bifilar o Par Trenzado 29
2.6.1.2 Fibra óptica 30
2.6.2 Medios no guiados 31
2.6.2.1 Microondas terrestres 32
2.6.2.2 Microondas por satélite 35
2.6.2.3 Ondas de Radio 37
2.6.2.4 Infrarrojos 38
2.6.2.5 Capacidad del medio 38
2.7 DIRECCIONAMIENTO IPV4 E IPV6 39
2.7.1 Historia del protocolo IP 39
2.7.2 Protocolo IPv4 40
2.7.2.1 Desperdicio de direcciones del protocolo IPv4 41
2.7.2.2 Problemas más importantes sobre el protocolo IPv4: 41
2.7.3 Protocolo IPv6 42
2.7.3.1 Las principales funciones de IPv6 y ventajas con respecto IPv4 42
2.7.3.2 Encabezados de datagramas básicos del protocolo IPv6 43
2.7.3.2.1 Significados de los diferentes campos: 43
2.7.3.3 Notación IPv6 45
2.7.3.4 Autenticación para el protocolo IPv6 46
2.8 MODELO DE REFERENCIA Y ESTÁNDARES 802.11 47
2.8.1 Técnicas de transmisión del estándar 802.11 48
2.8.1.1 DSSS 48
2.8.1.2 FHSS 48
2.8.1.3 OFDM 49
2.8.2 El estándar IEEE802.11 ofrece dos métodos de autenticación 49
2.8.3 Capas del modelo OSI que intervienen en el estándar IEEE 802.11. 49
2.8.3.1 CAPA FÍSICA 49
2.8.3.1 PLCP (Physical Layer Convergence Protocol) 50
2.8.3.2 PMD (Physical Médium Dependet) 51
2.8.3.1.3 PROTOCOLOS IEEE 802.11 DE LA CAPA FÍSICA 51
2.8.3.1.3.1 IEEE 802.11a 52
2.8.3.1.3.2 IEEE 802.11b 53
2.8.3.1.3.3 IEEE 802.11g 54
2.8.3.1.3.4 IEEE 802.11n 56
2.8.3.2 LA CAPA MAC 57
2.8.3.2.1 Mecanismos de Acceso de la capa MAC 57
2.8.3.2.1.1 Protocolos con arbitraje 58
2.8.3.2.1.2 Protocolos de acceso por contienda 58
2.8.3.2.1.2.1 CSMA 58
2.8.3.2.1.2.2 CSMA/CD 59
2.8.3.2.1.2.3 CSMA/CA 59
2.9 ESTUDIO DE LAS REDES INALÁMBRICAS 62
2.9.1 INTRODUCCIÓN 62
2.9.2 HISTORIA 63
2.9.3 VENTAJAS DE WLANS SOBRE LAS REDES ALÁMBRICAS 65
2.9.3.1 Movilidad 65

2.9.3.2 Simplicidad y rapidez en la instalación 65
2.9.3.3 Flexibilidad en la instalación 65
2.9.3.4 Costo de propiedad reducido 66
2.9.3.5 Escalabilidad 66
2.9.4 DESVENTAJAS DE LAS REDES INALÁMBRICAS 66
2.9.4.1 Menor ancho de banda 66
2.9.4.2 Mayor inversión inicial 66
2.9.4.4 Interferencias 67
2.9.5 DIFERENCIAS DE UNA RED INALÁMBRICA FRENTE A UNA RED CABLEADA 68
2.9.6 IDENTIFICACIÓN DE UNA RED INALÁMBRICA 70
2.9.7 CLASIFICACIÓN DE LAS REDES INALÁMBRICAS 70
2.9.7.1 REDES INALÁMBRICAS PERSONALES 70
2.9.7.1.1 INFRARROJOS. 71
2.9.7.1.1.1 Tipos de Infrarrojos 72
2.9.7.1.1.1.1 Modo punto-a-punto ..... - 72 -
2.9.7.1.1.1.2 Modo Cuasi-difuso 73
2.9.7.1.1.1.3 Modo Difuso 73
2.9.7.1.2 Bluetooth 74
2.9.7.1.2.1 USO Y APLICACIONES DE Bluetooth 74
2.9.7.1.2.2 Especificación y características de Bluetooth 76
2.9.8 TIPOS DE REDES INALÁMBRICAS 77
2.9.8.1 Wireless WAN/MAN (Wide Area Network/Metropolitan Area Network) 78
2.9.8.2 Wireless LAN (Local Area Network) 80
2.9.8.2.1 CONEXIÓN PUNTO A PUNTO 82
2.9.8.2.2 CONEXIÓN PUNTO MULTIPUNTO 82
2.9.8.2.3 CONEXIÓN DE REJILLA O MALLA 82
2.9.8.2.4 Wireless PAN (Personal Area Network) 84
2.9.9 TOPOLOGÍAS DE UNA RED INALÁMBRICA 85
2.9.9.1 Redes Ad-Hoc 86
2.9.10 DISPOSITIVOS PARA LA CONEXIÓN DE UNA RED INALÁMBRICA 88
2.9.10.1 ACCESS POINT 88
2.9.10.2 TARJETA DE RED INALÁMBRICA 89
2.9.10.3 ANTENAS Y ACCESORIOS 90
2.9.10.3.1 PoE (Power over Ethernet) 92
2.9.10.3.2 Ventajas que tiene un Sistema de alimentación POE 92
2.9.10.3.3 PIGTAIL 95
2.9.10.3.4 TIPOS DE ANTENAS 95
2.9.10.3.4.1 Antenas Omnidireccionales 95
2.9.10.3.4.1.1 Dipolo (vertical): 96
2.9.10.3.4.1.2 Monopolo vertical de cuarto de onda: 96
2.9.10.3.4.1.3 Colineares 96
2.9.10.3.4.1.4 Guía ondas ranuradas 97
2.9.10.3.4.2 Antenas direccionales 97
2.9.10.3.4.2.1 Dipolo (horizontal): 98
2.9.10.3.4.2.2 Uda-Yagi: sucesión de dipolos 98
2.9.10.3.4.2.3 Panel o 'Patch Antenna' 98
2.9.10.3.4.2.4 Guía-ondas 99
2.9.10.3.5 PARÁMETROS DE UNA ANTENA 99
2.9.10.3.5.1 Resistencia de radiación 99

2.9.10.3.5.2 Eficiencia de una antena 99
2.9.10.3.5.3 Impedancia de entrada de una antena 100
2.9.10.3.5.4 Ganancia de una antena 100
2.9.10.3.5.5 Longitud eficaz de la antena 100
2.9.10.3.5.6 Polarización de la antena 101
2.9.10.3.5.7 Ancho de haz de una antena 101
2.9.10.3.5.8 Ancho de banda de la antena 101
2.9.10.3.6 FACTORES QUE INFLUYEN LA CLARIDAD DE LA SEÑAL EN UNA ANTENA 102
2.9.10.3.6.1 Potencia de la señal 102
2.9.10.3.6.2 Distancia 102
2.9.10.3.6.3 Interferencias 102
2.9.10.3.6.4 Línea de visión 103
2.9.10.3.6.5 Transmisión de la señal 103
2.9.10.3.6.6 Enfocar la señal ..... - 104 -
2.9.10.3.6.7 Línea de visión ..... - 105 -
2.9.10.3.6.8 Posición estable de la antena ..... - 106 -
2.9.11 SEGURIDAD PARA LAS REDES INALÁMBRICAS ..... - 106 -
2.9.11.1 MECANISMOS DE SEGURIDAD DE LAS REDES INALÁMBRICAS - 107 -
2.9.11.1.1 CIFRADO WEP (Wired Equivalent Privacy) ..... - 108 -
2.9.11.1.1.1Modo de funcionamiento de WEP ..... - 110 -
2.9.11.1.2 CIFRADO WPA (Wi-Fi Protected Access) ..... - 111 -
2.9.11.1.2.1 IEEE 802.1X. ..... - 112 -
2.9.11.1.2.2 EAP. ..... - 112 -
2.9.11.1.2.3 TKIP ..... - 112 -
2.9.11.1.2.4 MIC ..... - 112 -
2.9.11.1.2.5 Mejoras de WPA respecto a WEP ..... - 112 -
2.9.11.1.2.6 Modos de funcionamiento de WPA ..... - 113 -
2.9.11.1.3 CIFRADO WPA2 (IEEE 802.11i) ..... - 113 -
2.9.11.1.3.1 Características criptográficas de WPA2 ..... - 114 -
2.9.11.1.3.1 Claves temporales de WPA2 115
2.9.11.1.4 AUTENTICACIÓN POR SISTEMA ABIERTO ..... - 117 -
2.9.11.1.5 AUTENTICACIÓN MEDIANTE CLAVE COMPARTIDA ..... - 118 -
2.10 CÁMARA DE SEGURIDAD IP ..... - 119 -
2.10.1 CÁMARAS IP. ..... - 123 -
2.10.1.1 CALIDAD DE IMAGEN. ..... - 124 -
2.10.1.2 FACILIDAD DE INTEGRACIÓN. ..... - 124 -
2.10.1.3 COMPRESIÓN COMPATIBLE CON LOS ESTÁNDARES JPEG, MPEG4 ..... - 124 -
2.10.1.4 Requisitos de sistema para visualización de cámaras vía IP. ..... - 125 -
2.10.1.5 SOFTWARE DE MONITOREO ..... - 125 -
2.10.1.6 FUNCIONALIDAD Y SEGURIDAD DE LAS CÁMARAS DE VIGILANCIA IP. ..... - 126 -
2.10.1.7 MEDIOS DE ALMACENAMIENTO DE LAS CÁMARAS IP ..... - 126 -
2.10.1.8 FORMATOS DE COMPRESIÓN DE VIDEO ..... - 128 -
2.10.1.9 TRANSPORTE DE PAQUETES DE VIDEO ..... - 132 -
2.10.1.10 DIGITALIZACIÓN DE IMÁGENES DE VIDEO ..... - 133 -
2.10.1.11 FALLAS EN LA TRANSMISIÓN. ..... - 134 -
2.10.1.11.1 PÉRDIDA DE PAQUETES. ..... - 134 -

2.10.1.11.2 REORDENAMIENTO DE PAQUETES. ....- 134 -
2.10.1.11.3 Retardo ....- 135 -
2.10.1.11.4 JITTER ....- 136 -
2.10.1.12 POLÍTICAS DE BACKUP ....- 136 -
CAPÍTULO 3 ....- 138 -
3.1 SOLUCIONES PARA REDES INALÁMBRICAS ....- 138 -
3.2 Soluciones 3COM ....- 138 -
3.2.1 Access Point (3COM) ....- 139 -
3.2.2 Tarjeta de red (3COM) ....- 140 -
3.2.2.1 Características y beneficios: ....- 140 -
3.2.3 Antenas (3COM) ....- 141 -
3.2.3.1 Características y ventajas ....- 141 -
3.2.4 Router (3COM) ....- 142 -
3.2.4.1 Características y ventajas ....- 142 -
3.2.4.2 Especificaciones de producto ....- 142 -
3.3 SOLUCIONES LINKSYS ....- 143 -
3.3.1 Access Point (Linksys) ....- 143 -
3.3.1.1 Caracteristicas ....- 144 -
3.3.1.2 Especificaciones ....- 144 -
3.3.2 Tarjeta de red (Linksys) ....- 145 -
3.3.2.1 Características: ....- 145 -
3.3.3 Antena (Linksys) ....- 146 -
3.3.3.1 Especificaciones Técnicas ....- 147 -
3.3.4 Router (Linksys) ....- 147 -
3.3.4.1 Características: ....- 148 -
3.3.5 Cámara de vigilancia IP ....- 148 -
3.3.5.1Características: ....- 149 -
3.4 SOLUCIONES D-LINK ....- 150 -
3.4.1 Switch 8 Puertos ....- 150 -
3.4.1.1 Principales Características y Facilidades ....- 152 -
3.4.2 Tarjeta de red (D-LLINK) ....- 153 -
3.4.2.1 CARACTERÍSTICAS PRINCIPALES ....- 153 -
3.4.3 WIRELESS ROUTER D-Link DI-634M ....- 154 -
3.4.3.1 CARACTERÍSTICAS PRINCIPALES ....- 156 -
3.4.4 Cámara de vigilancia IP DCS 5300 (D-LINK) ....- 157 -
3.4.4 Cámara de vigilancia IP DCS 5300 (D-LINK) ....- 158 -
CAPITULO 4 ....- 161 -
4.1 IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED WLAN, Y CÁMARAS DE SEGURIDAD IP PARA HOSTAL LA CAROLINA ....- 161 -
4.2 FACTORES DE DISEÑO ....- 161 -
4.3 DEFINICIÓN DE EQUIPOS ....- 162 -
4.3.1 ANÁLISIS DE UBICACIÓN DE EQUIPOS PARA LA RED WLAN Y CÁMARAS IP. ....- 162 -
4.3.1.1Recepción ....- 163 -
4.3.1.2 Cocina ....- 163 -
4.3.1.3 Primer, Segundo y tercer piso ....- 163 -
4.4 DISEÑO FÍSICO ....- 164 -
4.5 DISEÑO LÓGICO ....- 166 -
4.6 Conexión de la WLAN con la red cableada: ....- 166 -
4.7 COSTO TOTAL DEL PROYECTO ....- 166 -

4.7.1 Proforma .....- 167 -
4.8 IMPLEMENTACIÓN.....- 167 -
4.8.1 Implementación Tendido de cables.....- 167 -
4.8.2 Implementación de Cámaras y Wireless Router .....- 167 -
4.8.2.1 Ilustración Montaje de equipos .....- 168 -
4.9 CONFIGURACIÓN.....- 169 -
4.9.1 Configuración WIRELESS ROUTER DLINK.....- 169 -
4.9.2 Configuración de la cámara IP.....- 182 -
4.9.3 Configuración de la estación de trabajo .....- 185 -
4.10 PRUEBA DE EQUIPOS .....- 190 -
4.10.1 PRUEBAS DE MONITOREO .....- 190 -
4.10.2 PRUEBAS DE SEÑAL DE RED WLAN.....- 192 -
4.11 CONCLUSIONES Y RECOMENDACIONES .....- 192 -
4.11.1CONCLUSIONES.....- 193 -
4.11.2 RECOMENDACIONES.....- 194 -
4.12 GLOSARIO 196
4.13 BIBLIOGRAFÍA: 206

ÍNDICE DE FIGURAS

FIGURA 2.1: TOPOLOGÍA EN ANILLO 8
FIGURA 2.2: TOPOLOGÍA EN ANILLO 9
FIGURA 2.3: TOPOLOGÍA EN ESTRELLA..... - 10 -
FIGURA 2.4: TOPOLOGÍA EN ÁRBOL ..... - 10 -
FIGURA 2.5: TOPOLOGÍA EN MALLA..... - 11 -
FIGURA 2.6: TOPOLOGÍA DE RED CELULAR 12
FIGURA 2.7: ¿POR QUÉ UN MODELO DE RED DIVIDIDO EN CAPAS?..... 14
FIGURA 2.8: LAS 7 CAPAS DEL MODELO OSI..... 14
FIGURA 2.9: CABLE COAXIAL..... 28
FIGURA 2.10: PAR TRENZADO SIN BLINDAJE (UTP) ..... - 30 -
FIGURA 2.11: FIBRA ÓPTICA ..... - 31 -
FIGURA 2.12: MICROONDA TERRESTRE 33
FIGURA 2.13: DIFUSIÓN DE TV 36
FIGURA 2.14: REDES PRIVADAS..... 37
FIGURA 2.15: TRAMA DEL NIVEL FÍSICO DE 802.11B 54
FIGURA 2.16: MECANISMO DE INTERCAMBIO DE MENSAJES..... - 60 -
FIGURA 2.17: COMPARATIVA DISTANCIA/VELOCIDAD DE TIPOS DE REDES 78
FIGURA 2.18: WIRELESS WAN/MAN ..... - 80 -
FIGURA 2.19: ENLACE WLAN (WIRELESS LOCAL AREA NETWORK) ..... - 81 -
FIGURA 2.20: CONEXIÓN PUNTO A PUNTO..... - 83 -
FIGURA 2.21: CONEXIÓN PUNTO A MULTIPUNTO 83
FIGURA 2.22: CONEXIÓN TIPO MALLA 84
FIGURA 2.23: WIRELESS PAN (PERSONAL AREA NETWORK) 85
FIGURA 2.24: RED AD-HOC 86
FIGURA 2.25: ACCESS POINT D-LINK DWL-G700AP..... 88
FIGURA 2.26: TARJETA DE RED INALÁMBRICA..... 89
FIGURA 2.27: TARJETA DE RED INALÁMBRICA..... 90
FIGURA 2.28: TARJETA DE RED PARA LAPTOP ..... - 90 -
FIGURA 2.29: ANTENAS ..... - 91 -
FIGURA 2.30: DISPOSITIVO POE COMERCIAL ..... - 92 -
FIGURA 2.31: ESQUEMA POE TÍPICO..... 94
FIGURA 2.32: OTRA FORMA DE CONEXIÓN DE UN POE..... 94
FIGURA 2.33: ANTENA MONOPOLO 96
FIGURA 2.34: ANTENA DIRECCIONAL..... 99
FIGURA 2.35: ANTENA DIRECCIONAL..... - 99 -
FIGURA 2.36: LÍNEA DE VISIÓN DE UNA ANTENA..... - 106 -
FIGURA 2.37: ALGORITMO DE ENCRIPTACIÓN WEP ..... - 111 -
FIGURA2.38: VIDEO ANALÓGICO CCTV ..... - 120 -
FIGURA 2.39: VIDEO IP DIGITAL CCTV ..... - 122 -
FIGURA 2.40: TÉCNICAS DE COMPRESIÓN DE VIDEO ..... - 131 -
FIGURA 2.41: CODIFICACIÓN DE FUENTE DE VIDEO ..... - 133 -
FIGURA 3.1: AIRCONNECT A 11 MBPS DE 3COM ..... - 139 -
FIGURA 3.2: 11MBPS WIRELESS LAN PC CARD CON ANTENNA X-JACK..... - 140 -
FIGURA 3.3: 3COM® 6/8DBI DUAL-BAND OMNI ANTENNA ..... - 141 -
FIGURA 3.4: 3COM® OFFICECONNECT® REMOTE 812 ADSL ROUTER..... - 142 -
FIGURA 3.5: PUNTO DE ACCESO LINKSYS WAP54G 54 MBPS..... - 144 -
FIGURA 3.6: LINKSYS 54MBPS/2.4GHZ PCI CON CHIP BROADCOM..... - 145 -
FIGURA 3.7: ANTENA HGA7S LARGO ALCANCE PARA CONEXIONES R-SMA ..... - 146 -
FIGURA 3.8: ROUTER WRT54G2 LINKSYS..... - 147 -

FIGURA 3.9: WVC54GC COMPACT WIRELESS-G INTERNET VIDEO CAMERA .... - 149 -
FIGURA 3.11: DWA-510 WIRELESS G PCI ADAPTER 54MBPS ..... - 153 -
FIGURA 3.13: WIRELESS ROUTER D-LINK DI-634M ..... - 156 -
FIGURA 3.14: DCS-5300 SECURITY CAM IP ..... - 157 -
FIGURA 3.15: DCS-2100 SECURITY CAM IP ..... - 159 -
FIGURA 4.1: LISTA DE INFORMACIÓN DE ESTADO CONEXIÓN A INTERNET ..... - 169 -
FIGURA 4.2: LISTA DE INFORMACIÓN DE ESTADO CONEXIÓN WIRELESS ..... - 169 -
FIGURA 4.3: LISTA DE INFORMACIÓN DE ESTADO CONFIGURACIÓN DE LA RED..... - 170 -
FIGURA 4.4: CONFIGURACIÓN DE TIEMPO Y FECHA ..... - 171 -
FIGURA 4.5: CONTROL DE ACCESO URL ..... - 172 -
FIGURA 4.6: ACCESO A SERVIDORES O FTP ..... - 172 -
FIGURA 4.7: CONTROL DE PUERTOS EN EL FIREWALL..... - 173 -
FIGURA 4.8: DIRECCIONAMIENTO MAC ..... - 173 -
FIGURA 4.9: ACTIVACION DE FIREWALL ..... - 174 -
FIGURA 4.10: RADIO DE TRANSMISIÓN DE LA RED ..... - 174 -
FIGURA 4.11: VELOCIDAD Y CONEXIÓN DE RED ..... - 175 -
FIGURA 4.12: RUTAS PARA ACCEDER ..... - 175 -
FIGURA 4.13: ASIGNACIÓN DE USUARIOS..... - 176 -
FIGURA 4.14: CONFIRMACIÓN DE CAMBIOS ..... - 176 -
FIGURA 4.15: FIRMAR ACTUALIZACIÓN ..... - 177 -
FIGURA 4.16: ASIGNACIÓN DE IPS DINÁMICAS..... - 177 -
FIGURA 4.17: TIEMPO DE TRABAJO ..... - 178 -
FIGURA 4.18: RESPALDO EN DISCO..... - 178 -
FIGURA 4.19: ESTADO DE RED..... - 179 -
FIGURA 4.20: VISTA DE CAMBIOS ..... - 179 -
FIGURA 4.21: TRAFICO DE PAQUETES ..... - 180 -
FIGURA 4.22: VISTA DE DIRECCIONES ..... - 180 -
FIGURA 4.23: VISTA DE CONEXIÓN INALÁMBRICA ..... - 181 -
FIGURA 4.24: MENÚ DE SOPORTE ..... - 181 -
FIGURA 4.25: DIRECCIONAMIENTO DE RED..... - 182 -
FIGURA 4.26: PERSONALIZAR CÁMARA ..... - 182 -
FIGURA 4.27: CONFIGURACIÓN DE AUDIO Y VIDEO ..... - 183 -
FIGURA 4.30: TIEMPO DE RETARDO..... - 184 -
FIGURA 4.31: APLICAR CAMBIOS..... - 185 -
FIGURA 4.32: CONFIGURACIÓN DE RED ..... - 185 -
FIGURA 4.33: LISTA DE COMPROBACIÓN PARA CREAR UNA RED ..... - 186 -
FIGURA 4.34: MÉTODO DE CONEXIÓN..... - 186 -
FIGURA 4.35: DESCRIPCIÓN Y NOMBRE ..... - 187 -
FIGURA 4.36: NOMBRE DE LA RED..... - 187 -
FIGURA 4.37: COMPARTIR ARCHIVOS E IMPRESORAS..... - 188 -
FIGURA 4.38: APLICAR CONFIGURACIÓN DE RED..... - 188 -
FIGURA 4.39: RETARDO PARA OBTENCIÓN DE RED ..... - 189 -
FIGURA 4.40: ESTADO DE RED..... - 189 -
FIGURA 4.41: DETALLES DE CONEXIÓN DE RED ..... - 190 -
FIGURA 4.42: ILUSTRACIÓN DE CÁMARAS..... - 191 -

ÍNDICE DE TABLAS

TABLA 2.1: CAPAS Y PROTOCOLOS DEL MODELO OSI ..... - 19 -
TABLA 2.2: PILA DE PROTOCOLO TCP/IP ..... - 20 -
TABLA 2.3: ANCHO DE BANDA QUE CUBRE LAS MICROONDAS..... - 34 -
TABLA 2.4: PROBLEMAS DE INTERFERENCIA ENTRE EMISIONES ..... - 34 -
TABLA 2.5: LAS FRECUENCIAS ASCENDENTE Y DESCENDENTE SON DISTINTAS ..... - 35 -
TABLA 2.6: DATAGRAMA IPV6 ..... - 43 -
TABLA 2.7: INDICADORES DE CANALES DE IEEE802.11A ..... - 53 -
TABLA 2.8: IDENTIFICADORES DE CANALES DE IEEE802.11B Y IEEE 802.11G ... - 55 -
TABLA 2.9: CLASIFICACIÓN DE LOS DISPOSITIVOS BLUETOOTH ..... - 75 -
TABLA 2.10: ANCHO DE BANDA DE BLUETHOOT..... - 75 -
TABLA 2.11: COMO WPA2 ABORDA EL PUNTO DÉBIL DE WEP ..... - 114 -
TABLA 3.1: CARACTERÍSTICAS DE ACCESS POINT 3COM ..... - 139 -
TABLA 3.2: CARACTERÍSTICAS DE LAS POSIBLES SOLUCIONES ..... - 159 -
TABLA 4.1: UBICACIÓN DE CÁMARAS (REFERENCIA) ..... - 162 -
TABLA 4.2: LISTA DE PRECIOS..... - 167 -
TABLA 4.3: PRUEBAS DE SEÑAL INALÁMBRICA..... - 192 -

CAPÍTULO 1

1.1 ANTECEDENTES

Hostal la Carolina se encuentra ubicada en la calle Italia y Vancouver (Quito – Ecuador). Es una empresa dedicada al alquiler de habitaciones, cuenta con una gran gama de clientes con capacidad de setenta personas, en su mayoría son ejecutivos que vienen de diferentes ciudades del país y también del extranjero, para aquellos que viajan por motivos de trabajo es una herramienta muy importante el servicio de Internet. En la actualidad el servicio que brinda el área de sistemas es una red alámbrica con cuatro puntos de red en una sala de estar.

Por otro lado, en los últimos meses se han recibido quejas por parte de algunos huéspedes, sobre la pérdida de objetos de valor en las habitaciones como relojes, celulares, cámaras, etc.

En vista de la falta de más puntos de acceso a Internet, que inclusive podrían estar en las habitaciones, y de la falta de control de la seguridad en el hotel se propone:

- Implementar y configurar la tecnología de acceso inalámbrico WLAN, ya que ésta es móvil y elimina la necesidad de usar cables y, establece nuevas aplicaciones, añadiendo flexibilidad a la red y lo más importante, incrementa la productividad y eficiencia en el servicio de Internet.
- Implementar y configurar cámaras de vigilancia IP, estas son parte de un sistema de vigilancia y seguridad. Gracias a la llegada de las cámaras IP es posible, hoy, hacer seguimiento de personas que atraviesan un punto de entrada, y de esta forma fortalecer la seguridad.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

- Diseñar, implementar y configurar una red inalámbrica WLAN, como una red de cámaras de seguridad IP en Hostal La Carolina, la misma que garantizará a los clientes de la empresa el fácil y rápido acceso al servicio de Internet. A su vez las cámaras de vigilancia fortalecerá la seguridad para todos los huéspedes en el cuidado de sus pertenencias.

1.2.2 OBJETIVOS ESPECIFICOS

- Identificar el problema y determinar las alternativas de solución.
- Investigar los aspectos teóricos y prácticos de la tecnología (WLAN) y video vigilancia IP.
- Analizar el mercado y seleccionar la mejor alternativa de solución.
- Analizar la compatibilidad que debe existir entre los equipos que forman parte de la estructura de la red WLAN y cámaras de seguridad IP.
- Analizar la estructura física y los aspectos de conexión para el funcionamiento de la red WLAN y cámaras de vigilancia IP.
- Establecer los requerimientos de software y hardware que se necesitan para el funcionamiento de la red WLAN y cámaras de seguridad IP.
- Implementar y configurar la red inalámbrica (WLAN) y la de cámaras de seguridad IP.

1.3 JUSTIFICACIÓN

El fácil acceso al servicio de Internet en cualquier parte, dentro del hostal, dará un realce al servicio y a la comodidad del cliente, así también se podrá tener una vigilancia de quien ingresa a las habitaciones por medio de las cámaras.

1.4 ALCANCE Y META

Implementar y configurar la red WLAN y cámaras de seguridad IP, las mismas que darán servicio de Internet dentro de la empresa en una área de 300 m^2, y en todos los pisos (planta baja, primer, segundo, y tercer piso), también debe ser posible el acceso a Internet desde el interior de las habitaciones. Además las cámaras de seguridad IP serán instaladas en los lugares más vulnerables al robo como pasillos, restaurant, recepción y sala de estar.

CAPÍTULO 2

2.1 MARCO REFERENCIAL

A mediados de los 70 diversos fabricantes desarrollaron sus propios sistemas de redes locales. Es en 1980 cuando Xerox, en cooperación con Digital Equipment Corporation e Intel, desarrolla y publica las especificaciones del primer sistema comercial de red denominado Ethernet. En 1986 IBM introdujo la red TokenRing. La mayor parte del mercado utiliza hoy día la tecnología del tipo Ethernet. [1]

En 1982 aparecen los ordenadores personales, siendo hoy una herramienta común de trabajo. Esta difusión del ordenador ha impuesto la necesidad de compartir información, programas, recursos, acceder a otros sistemas informáticos dentro de la empresa y conectarse con bases de datos situadas físicamente en otros ordenadores, etc. En la actualidad, una adecuada interconexión entre los usuarios y procesos de una empresa u organización, puede constituir una clara ventaja competitiva. La reducción de costes de periféricos, o la facilidad para compartir y transmitir información son los puntos claves en que se apoya la creciente utilización de redes.

2.2 ¿QUÉ ES UNA RED?

Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas, etc.

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

---

[1] http://comunidad.uach.mx/marana/materias/sir/material/El%20modelo%20OSI.doc

Cada dispositivo activo conectado a la red se denomina *nodo*. Un dispositivo activo es aquel que interviene en la comunicación de forma autónoma, sin estar controlado por otro dispositivo. Por ejemplo, determinadas impresoras son autónomas y pueden dar servicio en una red sin conectarse a un ordenador que las maneje; estas impresoras son nodos de la red.

Dependiendo del territorio que abarca una red se clasifican en:

- LAN: Local Área Network. Está constituida por un conjunto de ordenadores independientes interconectados entre sí, pueden comunicarse y compartir recursos. Abarcan una zona no demasiado grande, un edificio o un campus.
- WAN: Wide Area Network, comprenden regiones más extensas que las LAN e incluso pueden abarcar varios países.

También un conjunto de redes puede conectarse entre sí dando lugar a una red mayor.

2.3 CARACTERÍSTICAS DE UNA RED DE ÁREA LOCAL

Los ordenadores conectados a una red local pueden ser grandes ordenadores u ordenadores personales, con sus distintos tipos de periféricos. Aunque hay muchos tipos de redes locales entre ellas hay unas características comunes: [2]

- Un medio de comunicación común a través del cual todos los dispositivos pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo. Las redes locales están contenidas en una reducida área física: un edificio, un campus, etc.
- Una velocidad de transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo. El equipo de la red local

[2] http://comunidad.uach.mx/marana/materias/sir/material/El%20modelo%20OSI.doc

puede transmitir datos a la velocidad máxima a la que puedan comunicarse las estaciones de la red, suele ser de un Mb por segundo.

- Una distancia entre estaciones relativamente corta, entre unos metros y varios kilómetros.
- La posibilidad de utilización de cables de conexión normales.
- Todos los dispositivos pueden comunicarse con el resto y algunos de ellos pueden funcionar independientemente.
- Un sistema fiable, con un índice de errores muy bajo. Las redes locales disponen normalmente de su propio sistema de detección y corrección de errores de transmisión.
- Flexibilidad, el usuario administra y controla su propio sistema.

Los dos tipos básicos de dispositivos que pueden conectarse a una red local son las estaciones de trabajo y los servidores:
-Una estación de trabajo es un ordenador desde donde el usuario puede acceder a los recursos de la red.

-Un servidor es un ordenador que permite a otros ordenadores que accedan a los recursos de que dispone. Estos servidores pueden ser:

- dedicados: son usados únicamente para ofrecer sus recursos a otros nodos
- no dedicados: pueden trabajar simultáneamente como servidor y estación de trabajo.

Existe un tipo de servidor un poco especial que se tratará por separado, es el servidor de comunicaciones. Este servidor permite que cualquiera de los equipos de una red se comunique con dispositivos o sistemas externos. A su vez, se dividirá en dos grandes grupos: bridges y Gateway.

De forma general, en una red, al nodo que pide un servicio o inicia una comunicación, se le denomina *cliente*. Al nodo que responde a la petición se le denomina *servidor*.

2.4 TOPOLOGÍAS DE UNA RED

Se denomina topología de red a la forma geométrica en que están distribuidas las estaciones de trabajo y los cables que la conectan. Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, y el objeto de la topologías es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo, facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de datos, permitir un mejor control de la red y permitir de forma eficiente el aumento del número de ordenadores en la red.[3]

Las formas más habituales que se puede encontrar en estas redes informáticas son las siguientes:

2.4.1 Topología de red en bus

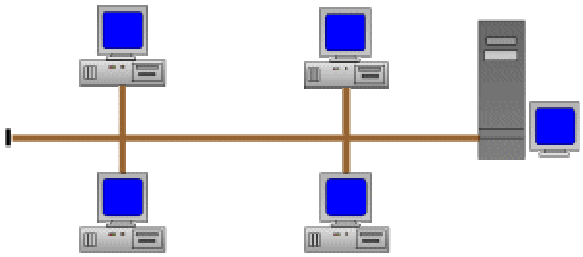
En ella todas las estaciones comparten el mismo canal de comunicaciones, toda la información circula por ese canal y cada una de ellas recoge la información que le corresponde.[4]

El cableado en bus presenta menos problemas logísticos, puesto que no se acumulan montones de cables en torno al nodo central, como ocurriría en una disposición en estrella. Pero, por contra, tiene la desventaja de que un fallo en una parte del cableado detendría el sistema, total o parcialmente, en función del lugar en que se produzca. Es además muy difícil encontrar y diagnosticar las averías que se producen en esta topología.

[3] http://www.ordenadores-y-portatiles.com/topologias-de-red.html

[4] http://html.rincondelvago.com/topologias.html

Figura 2.1: Topología en anillo



Fuente: http://html.rincondelvago.com/topologias.html

2.4.2 Topología en Anillo

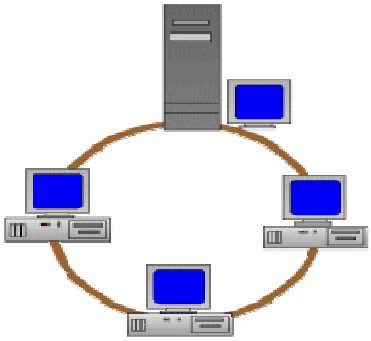
El anillo, como su propio nombre indica, consiste en conectar linealmente entre sí todos los ordenadores, en un bucle cerrado. La información se transfiere en un solo sentido a través del anillo, mediante un paquete especial de datos, llamado testigo, que se transmite de un nodo a otro, hasta alcanzar el nodo destino.

El cableado de la red en anillo es el más complejo de los tres enumerados, debido por una parte al mayor coste del cable, así como a la necesidad de emplear unos dispositivos denominados Unidades de Acceso Multiestación (MAU) para implementar físicamente el anillo.

A la hora de tratar con fallos y averías, la red en anillo presenta la ventaja de poder derivar partes de la red mediante los MAU's, aislando dichas partes defectuosas del resto de la red mientras se determina el problema. Un fallo, pues, en una parte del cableado de una red en anillo, no debe detener toda la red. La adición de nuevas estaciones no supone una complicación excesiva, puesto que una vez más los MAU's aíslan las partes a añadir hasta que se hallan listas, no siendo necesario detener toda la red para añadir nuevas estaciones.

Dos buenos ejemplos de red en anillo serían Token-Ring y FDDI (fibra óptica)

Figura 2.2: Topología en anillo



Fuente: http://html.rincondelvago.com/topologias.html

2.4.3 Topología en Estrella.

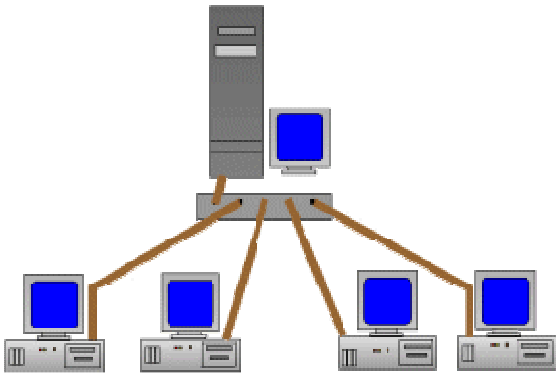
Esta topología se caracteriza por existir en ella un punto central, o más propiamente nodo central, al cual se conectan todos los equipos, de un modo muy similar a los radios de una rueda.

De esta disposición se deduce el inconveniente de esta topología, y es que la máxima vulnerabilidad se encuentra precisamente en el nodo central, ya que si este falla, toda la red fallaría. Este posible fallo en el nodo central, aunque posible, es bastante improbable, debido a la gran seguridad que suele poseer dicho nodo. Sin embargo presenta como principal ventaja una gran modularidad, lo que permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red.

Para aumentar el número de estaciones, o nodos, de la red en estrella no es necesario interrumpir, ni siquiera parcialmente la actividad de la red, realizándose la operación casi inmediatamente.

La topología en estrella es empleada en redes Ethernet y ArcNet.

Figura 2.3: topología en estrella

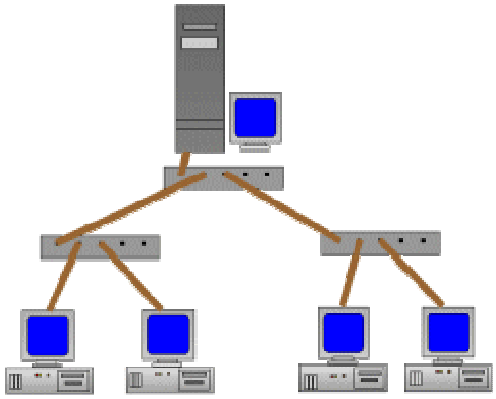


Fuente: http://html.rincondelvago.com/topologias.html

2.4.4 Topología en Árbol.

La topología en árbol es una generalización de la topología en bus. Esta topología comienza en un punto denominado cabezal o raíz (headend). Uno ó más cables pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse. En una topología en árbol no se deben formar ciclos.

Figura 2.4: Topología en árbol



Fuente: http://html.rincondelvago.com/topologias.html

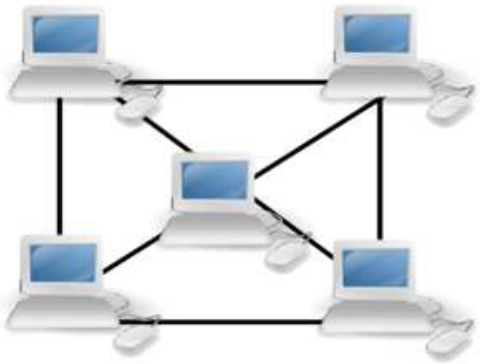
Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.

2.4.5 Topología en Malla:

En la topología malla, cada computador se conecta a otro casi directamente.

Idealmente cada computadora se conecta con todas las demás como se ve en el diagrama. [5]

Figura 2.5: Topología en Malla



Fuente:http://www.unicrom.com/cmp_topologia_redes_estrella_malla.asp

La topología malla se utiliza en redes pequeñas y no es utilizada frecuentemente debido a que es muy costosa.
Una forma más práctica y más económica de hacer esta conexión es utilizar algunos computadores como conmutadores que permiten interconectar grupos de otros computadores. Si un computador falla, la magnitud del problema depende de si es un computador conmutador o no.

[5] http://www.unicrom.com/cmp_topologia_redes_estrella_malla.asp

2.4.6 Topología de red celular

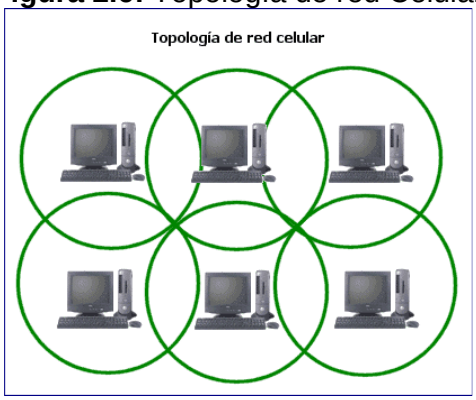
La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.[6]

La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; si lo hay ondas electromagnéticas.

La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.

Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

Figura 2.6: Topología de red Celular



Fuente: http://mx.geocities.com/alfonsoaraujocardenas/topologias.html

[6]http://mx.geocities.com/alfonsoaraujocardenas/topologias.html

2.5 ARQUITECTURA DE REDES

2.5.1 Modelo de Referencia OSI

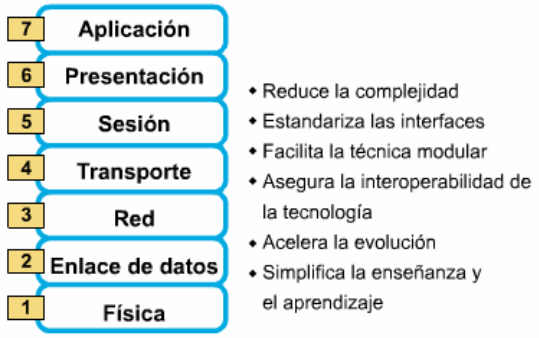
El modelo de Interconexión de Sistemas Abiertos (OSI), es conocido porque ofrece una explicación sencilla de la relación entre los complejos componentes de hardware y de protocolo de red. En el modelo OSI, la capa inferior corresponde al hardware y las capas sucesivas al software que usa la red.

Se puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Figura 2.7: ¿Por qué un modelo de red dividido en capas?



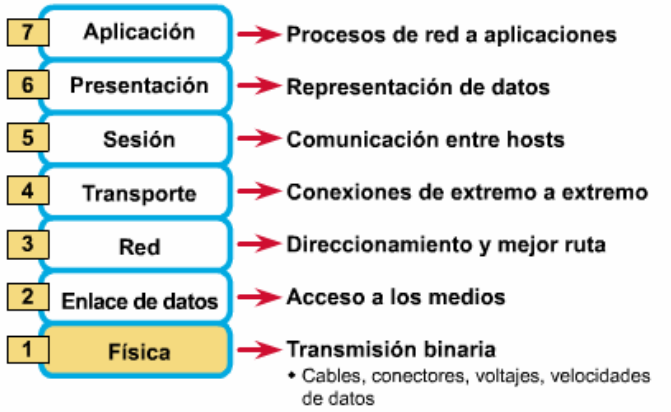
Fuente:http://comunidad.uach.mx/marana/materias/sir/material/El%20modelo%20OSI.doc:

Las siete capas del modelo de referencia *OSI* son:

Capa 7: La capa de aplicación
Capa 6: La capa de presentación
Capa 5: La capa de sesión
Capa 4: La capa de transporte
Capa 3: La capa de red
Capa 2: La capa de enlace de datos
Capa 1: La capa física

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, presentamos una breve descripción de cada capa del modelo de referencia OSI tal como aparece en la figura.

FIGURA 2.8: Las 7 capas del modelo OSI



Fuente: http://comunidad.uach.mx/marana/materias/sir/material/El%20modelo%20OSI.doc

2.5.1.1 Capa de Aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. [7]

La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Ejemplos de protocolos utilizados por los programas de esta capa son **HTTP**, **SMTP**, **POP**, **IMAP** etc.

2.5.1.2 Capa de Presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común. [8]

Actualmente el panorama ha cambiado; solo existe una opción para el formato de datos, a pesar de lo cual, el protocolo OSI sigue negociando un esquema de codificación (el único disponible). En Internet, el único servicio que utiliza esta capa es TELNET, que precisamente es un servicio de acceso a servidores desde terminales remotos. En este caso, la capa de presentación es la que se encarga de configurar el terminal para conectar a un servidor de características particulares.

---

[7] http://zator.com/Hardware/H12_2.htm

[8] http://zator.com/Hardware/H12_2.htm

2.5.1.3 Capa de Sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

2.5.1.4 Capa de Transporte

La capa de transporte segmenta los datos originados en el host emisor y los re ensamblan en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

Un ejemplo típico de protocolo usado en esta capa es **TCP** ("Transport Control Protocol"), otro protocolo que se utiliza es el **UDP** ("Universal Datagram Protocol") utilizada también en Internet por algunos programas de aplicación.

2.5.1.5 Capa de Red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada ("Routing"), pero no se ocupa para nada de los errores o pérdidas de paquetes. Por ejemplo, define la estructura de direcciones y rutas de Internet. A este nivel se utilizan dos tipos de paquetes: Paquetes de datos y Paquetes de actualización de ruta.

Como consecuencia esta capa puede considerarse subdividida en dos:

- **Transporte**. Encargada de encapsular los datos a transmitir (de usuario). Utiliza los paquetes de datos. En esta categoría se encuentra el protocolo **IP** ("Internet Protocol")
- **Conmutación** ("Switching"): Esta parte es la encargada de intercambiar información de conectividad específica de la red (su actividad es raramente percibida por el usuario). Los routers son dispositivos que trabajan en este nivel y se benefician de estos paquetes de actualización de ruta. En esta categoría se encuentra el protocolo **ICMP** ("Internet Control Message Protocol"), responsable de generar mensajes cuando ocurren errores en la transmisión y de un modo especial de eco que puede comprobarse mediante PING.

Los protocolos más frecuentemente utilizados en esta capa son dos: X.25 e IP.

2.5.1.6 Capa de Enlace de Datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Para esto agrupa la información a transmitir en bloques ("Frames"), e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el

receptor. Si algún datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío. El protocolo PPP es ejemplo de esta capa.

La capa de enlace puede considerarse dividida en dos subcapas:

- **Control lógico de enlace LLC** ("Logical Link Control") define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.
- **Control de acceso al medio MAC** ("Medium Access Control"). Esta subcapa actúa como controladora del hardware subyacente (el adaptador de red). De hecho el controlador de la tarjeta de red es denominado a veces "MAC driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección MAC ("MAC address"). Su principal tarea (que le proporciona el nombre -control de acceso-) consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte. El mecanismo **CSMA/CD** ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es un típico ejemplo de esta subcapa.

2.5.1.7 Capa Física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, además de la velocidad de transmisión, si esta es uni o bidireccional (simplex, duplex o flull-duplex). Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física. [9]

Como resumen de los cometidos de esta capa, podemos decir que se encarga de transformar un paquete de información binaria ("Frame") en una sucesión de

---

[9] http://zator.com/Hardware/H12_2.htm

impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); electromagnéticos (transmisión Wireless) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace (ver a continuación).

Por ejemplo: Este nivel define las medidas del cable coaxial Ethernet y de los conectores BNC utilizados. Otro ejemplo de estándares relativos a esta capa son RS-232 para comunicaciones serie y X.21.

Tabla 2.1: Capas y protocolos del Modelo OSI

Capa	Nombre	Protocolos comunes
7	Aplicación	SSH, Telnet, FTP
6	Presentación	HTTP, SMTP, SNMP
5	Sesión	RPC, named pipes, NETBIOS
4	Transporte	TCP, UDP
3	Red	IP
2	Enlace de Datos	Ethernet
1	Física	Cat-5

Fuente: http://www.tech-faq.com/lang/es/osi-model.shtml

2.5.2 ARQUITECTURA DEL MODELO TCP/IP

El modelo OSI describe las comunicaciones de red ideales con una familia de protocolos. TCP/IP no se corresponde directamente con este modelo. TCP/IP combina varias capas OSI en una única capa, o no utiliza determinadas capas. La tabla siguiente muestra las capas de la implementación de Solaris de TCP/IP. La tabla enumera las capas desde la capa superior (aplicación) hasta la capa inferior (red física).

Tabla 2.2: Pila de protocolo TCP/IP

Nº de capa de referencia OSI	**Equivalente de capa OSI**	**Capa TCP/IP**	***Ejemplos de protocolos TCP/IP***
5,6,7	Aplicación, sesión, presentación	Aplicación	*NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.*
4	Transporte	Transporte	*TCP, UDP, SCTP*
3	Red	Internet	*IPv4, IPv6, ARP, ICMP*
2	Vínculo de datos	Vínculo de datos	*PPP, IEEE 802.2*
1	Física	Red física	*Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros.*

Fuente: http://docs.sun.com/app/docs/doc/820-2981/ipov-10?l=es&a=view

La tabla muestra las capas de protocolo TCP/IP y los equivalentes del modelo OSI. También se muestran ejemplos de los protocolos disponibles en cada nivel de la pila del protocolo TCP/IP. Cada sistema que participa en una transacción de comunicación ejecuta una única implementación de la pila del protocolo.

2.5.2.1 Capa de Red Física

La capa de red física especifica las características del hardware que se utilizará para la red. Por ejemplo, la capa de red física especifica las características físicas del medio de comunicaciones. La capa física de TCP/IP describe los estándares de hardware como IEEE 802.3, la especificación del medio de red Ethernet, y RS-232, la especificación para los conectores estándar. [10]

[10] http://docs.sun.com/app/docs/doc/820-2981/ipov-10?l=es&a=view

2.5.2.2 Capa de Enlace de datos

La capa de vínculo de datos identifica el tipo de protocolo de red del paquete, en este caso TCP/IP. La capa de vínculo de datos proporciona también control de errores y estructuras. Algunos ejemplos de protocolos de capa de vínculo de datos son las estructuras Ethernet IEEE 802.2 y Protocolo punto a punto (PPP).

2.5.2.3 Capa de Internet

La capa de Internet, también conocida como capa de red o capa IP, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

2.5.2.3.1 Protocolo IP

El protocolo IP y sus protocolos de encaminamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

Direcciones IP: Las convenciones de direcciones IP forman parte del protocolo IP. Cómo diseñar un esquema de direcciones IPv4 introduce las direcciones IPv4 y Descripción general de las direcciones IPv6 las direcciones IPv6.

Comunicaciones de host a host: El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.

Formato de paquetes: El protocolo IP agrupa paquetes en unidades conocidas como datagramas. Puede ver una descripción completa de los datagramas en Capa de Internet: preparación de los paquetes para la entrega.

Fragmentación: Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original.

El sistema operativo Solaris admite los formatos de direcciones IPv4 e IPv6, que se describen en este capítulo. Para evitar confusiones con el uso del Protocolo de Internet, se utiliza una de las convenciones siguientes:

Cuando se utiliza el término "IP" en una descripción, ésta se aplica tanto a IPv4 como a IPv6.

Cuando se utiliza el término "IPv4" en una descripción, ésta sólo se aplica a IPv4.

Cuando se utiliza el término "IPv6" en una descripción, ésta sólo se aplica a IPv6.

2.5.2.3.2 Protocolo ARP

El protocolo de resolución de direcciones (ARP) se encuentra conceptualmente entre el vínculo de datos y las capas de Internet. ARP ayuda al protocolo IP a dirigir los datagramas al sistema receptor adecuado asignando direcciones Ethernet (de 48 bits de longitud) a direcciones IP conocidas (de 32 bits de longitud). [11]

2.5.2.3.3 Protocolo ICMP

El protocolo de mensajes de control de Internet (ICMP) detecta y registra las condiciones de error de la red. ICMP registra:

Paquetes soltados: Paquetes que llegan demasiado rápido para poder procesarse.

Fallo de conectividad: No se puede alcanzar un sistema de destino.

Redirección: Redirige un sistema de envío para utilizar otro encaminador.

[11] http://docs.sun.com/app/docs/doc/820-2981/ipov-10?l=es&a=view

2.5.2.4 Capa de Transporte

La capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Este tipo de comunicación se conoce como transmisión de punto a punto. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP), el Protocolo de datagramas de usuario (UDP) y el Protocolo de transmisión para el control de flujo (SCTP). Los protocolos TCP y SCTP proporcionan un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable.

2.5.2.4.1 Protocolo TCP

TCP permite a las aplicaciones comunicarse entre sí como si estuvieran conectadas físicamente. TCP envía los datos en un formato que se transmite carácter por carácter, en lugar de transmitirse por paquetes discretos. Esta transmisión consiste en lo siguiente:

- Punto de partida, que abre la conexión.
- Transmisión completa en orden de bytes.
- Punto de fin, que cierra la conexión.

TCP conecta un encabezado a los datos transmitidos. Este encabezado contiene múltiples parámetros que ayudan a los procesos del sistema transmisor a conectarse a sus procesos correspondientes en el sistema receptor.

TCP confirma que un paquete ha alcanzado su destino estableciendo una conexión de punto a punto entre los hosts de envío y recepción.

2.5.2.4.2 Protocolo SCTP

SCTP es un protocolo de capa de transporte fiable orientado a la conexión que ofrece los mismos servicios a las aplicaciones que TCP. Además, SCTP admite conexiones entre sistema que tienen más de una dirección, o de host múltiple. La conexión SCTP entre el sistema transmisor y receptor se denomina asociación. Los datos de la asociación se organizan en bloques. Dado que el protocolo SCTP admite varios hosts, determinadas aplicaciones, en especial las que se utilizan en el sector de las telecomunicaciones, necesitan ejecutar SCTP en lugar de TCP.

2.5.2.4.3 Protocolo UDP

UDP proporciona un servicio de entrega de datagramas. UDP no verifica las conexiones entre los hosts transmisores y receptores. Dado que el protocolo UDP elimina los procesos de establecimiento y verificación de las conexiones, resulta ideal para las aplicaciones que envían pequeñas cantidades de datos.

2.5.2.5 Capa de Aplicación

La capa de aplicación define las aplicaciones de red y los servicios de Internet estándar que puede utilizar un usuario. Estos servicios utilizan la capa de transporte para enviar y recibir datos. Existen varios protocolos de capa de aplicación. En la lista siguiente se incluyen ejemplos de protocolos de capa de aplicación:

- Servicios TCP/IP estándar como los comandos ftp, tftp y telnet.
- Servicios de nombres, como NIS o el sistema de nombre de dominio (DNS).
- Protocolo simple de administración de red (SNMP), que permite administrar la red.
- Protocolo RDISC (Router Discovery Server) y protocolos RIP (Routing Information Protocol).

2.5.2.5.1 Servicios TCP/IP estándar

2.5.2.5.1.1 FTP y FTP anónimo

El Protocolo de transferencia de archivos (FTP) transfiere archivos a una red remota y desde ella. El protocolo incluye el comando ftp y el daemon in.ftpd. FTP permite a un usuario especificar el nombre del host remoto y las opciones de comandos de transferencia de archivos en la línea de comandos del host local. El daemon in.ftpd del host remoto administra las solicitudes del host local. A diferencia de rcp, ftp funciona aunque el equipo remoto no ejecute un sistema operativo basado en UNIX. Para realizar una conexión ftp, el usuario debe iniciar sesión en un sistema remoto, aunque éste se haya configurado para permitir FTP anónimo. [12]

2.5.2.5.1.2 Telnet

El protocolo Telnet permite la comunicación entre los terminales y los procesos orientados a los terminales de una red que ejecuta TCP/IP. Este protocolo se implementa como programa telnet en los sistemas locales y como daemon in.telnetd en los equipos remotos. Telnet proporciona una interfaz de usuario a través de la cual se pueden comunicar dos hosts carácter por carácter o línea por línea. Telnet incluye un conjunto de comandos que se documentan de forma detallada en la página del comando man telnet (1).

2.5.2.5.1.3 TFTP

El protocolo de transferencia de archivos trivial (tftp) ofrece funciones similares a ftp, pero no establece la conexión interactiva de ftp. Como consecuencia, los usuarios no pueden ver el contenido de un directorio ni cambiar directorios. Los usuarios deben conocer el nombre completo del archivo que se va a copiar.

---

[12] http://docs.sun.com/app/docs/doc/820-2981/ipov-10?l=es&a=view

2.5.2.5.2 Servicios de Nombres

2.5.2.5.2.1 DNS

El sistema de nombre de dominio (DNS) es el servicio de nombres que proporciona Internet para las redes TCP/IP. DNS proporciona nombres de host al servicio de direcciones IP. También actúa como base de datos para la administración del correo.

2.5.2.5.2.2 NIS

El Servicio de información de la red (NIS) se desarrolló independientemente de DNS y tiene un enfoque ligeramente distinto. Mientras que DNS trata de facilitar la comunicación con el uso de nombres de equipos en lugar de direcciones IP numéricas, NIS se centra en facilitar la administración de la red al proporcionar control centralizado sobre distintos tipos de información de red. NIS almacena información sobre los nombres de equipo y las direcciones, los usuarios, la red y los servicios de red. La información de espacio de nombres NIS se almacena en asignaciones NIS.

2.5.2.5.3 Servicio de Directorios

El sistema operativo Solaris admite LDAP (Protocolo ligero de acceso a directorios) junto con el servidor de directorios Sun ONE (Sun Open Net Environment), así como otros servidores de directorios LDAP. La diferencia entre un servicio de nombres y un servicio de directorios radica en la extensión de las funciones. Un servicio de directorios proporciona las mismas funciones que un servicio de nombres, pero además cuenta con funciones adicionales.

2.5.2.5.4 Administración de la red

El Protocolo simple de administración de red (SNMP) permite ver la distribución de la red y el estado de los equipos clave. SNMP también permite obtener estadísticas de red complejas del software basado en una interfaz gráfica de usuario (GUI). Muchas compañías ofrecen paquetes de administración de red que implementan SNMP. [13]

[13] http://docs.sun.com/app/docs/doc/820-2981/ipov-10?l=es&a=view

2.5.2.5.5 Protocolos de encaminamiento

Los protocolos RIP y RDISC son dos protocolos de encaminamiento disponibles para las redes TCP/IP. Para ver una lista completa de los protocolos de encaminamiento disponibles para el sistema operativo Solaris 10.

2.6 MEDIOS DE TRANSMISIÓN

El medio de transmisión constituye el soporte por el cual a través de ellos el emisor y receptor pueden comunicarse en un sistema de transmisión de datos. Existen dos tipos de medios: guiados y no guiados. En ambos casos la transmisión se realiza por medio de ondas electromagnéticas. Los medios guiados conducen (guían) las ondas a través de un camino físico, ejemplos de estos medios son: cable coaxial, cable bifilar o par trenzado y el cable de fibra óptica. [14]

2.6.1 Medios guiados

La naturaleza del medio junto con la de la señal que se transmite a través de él constituye los factores determinantes de las características y la calidad de la transmisión. En el caso de medios guiados es el propio medio el que determina principalmente las limitaciones de la transmisión: velocidad de transmisión de los datos, ancho de banda que puede soportar y espaciado entre repetidores. Sin embargo, al utilizar medios no guiados resulta más determinante en la transmisión el espectro de frecuencia de la señal producida por la antena que el propio medio de transmisión, estas usan ondas de radio, microondas o infrarrojos, estos medios son más lentos que el cable o la fibra óptica.

Cualquier medio físico o no, que pueda transportar información en forma de señales electromagnéticas se puede utilizar en redes locales como medio de transmisión.

[14] http://nuestrowiki.wikispaces.com/Medios+de+transmision?f=print

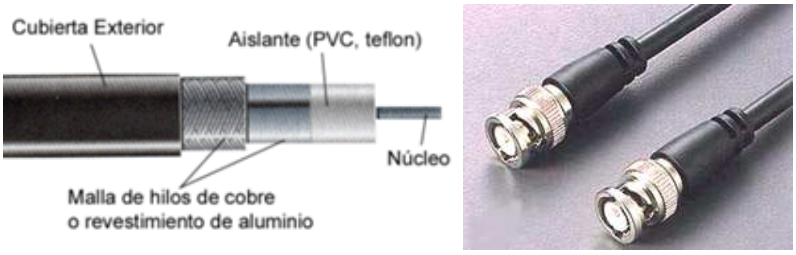
Las líneas de transmisión son la espina dorsal de la red, por ellas se transmite la información entre los distintos nodos. Para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: la banda base y la banda ancha.

Los diferentes tipos de red: Ethernet, TokenRing, FDDI, etc. pueden utilizar distintos tipos de cable y protocolos de comunicación.

2.6.1.1 Cable Coaxial

Hasta hace poco, era el medio de transmisión más común en las redes locales. El cable coaxial consiste en dos conductores concéntricos, separados por un dieléctrico y protegido del exterior por un aislante (similar al de las antenas de TV).

Figura 2.9: Cable Coaxial



Fuente:
http://www.eveliux.com/mx/index.php?option=com_content&task=view&id=21&Itemid=26

Existen distintos tipos de cable coaxial, según las redes o las necesidades de mayor protección o distancia. Este tipo de cable sólo lo utilizan las redes Ethernet.

Tipos de cable coaxial:

- cable *Thick* o cable grueso: es más voluminoso, caro y difícil de instalar, pero permite conectar un mayor número de nodos y alcanzar mayores distancias.
- cable *Thin* o cable fino, también conocido como *cheapernet* por ser más económico y fácil de instalar. Sólo se utiliza para redes con un número reducido de nodos.

Ambos tipos de cable pueden ser usados simultáneamente en una red. La velocidad de transmisión de la señal por ambos es de 10 Mb.

Ventajas del cable coaxial:

- La protección de las señales contra interferencias eléctricas debida a otros equipos, fotocopiadoras, motores, luces fluorescentes, etc.
- Puede cubrir distancias relativamente grandes, entre 185 y 1500 metros dependiendo del tipo de cable usado.

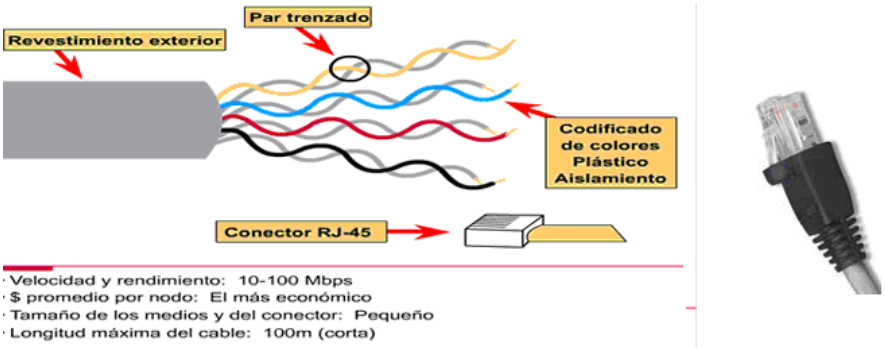
2.6.1.2 Cable Bifilar o Par Trenzado

El par trenzado consta como mínimo de dos conductores aislados trenzados entre ellos y protegidos con una cubierta aislante. Un cable de este tipo habitualmente contiene 1, 2 ó 4 pares, es decir: 2, 4 u 8 hilos.

Los cables trenzados o bifilares constituyen el sistema de cableado usado en todo el mundo para telefonía. Es una tecnología bien conocida. El cable es bastante barato y fácil de instalar y las conexiones son fiables. Sus ventajas mayores son por tanto su disponibilidad y bajo coste.

En cuanto a las desventajas están la gran atenuación de la señal a medida que aumenta la distancia y que son muy susceptibles a interferencias eléctricas. Por este motivo en lugar de usar cable bifilar paralelo se utiliza trenzado y para evitar las interferencias, el conjunto de pares se apantalla con un conductor que hace de malla. Esto eleva el coste del cable en sí, pero su instalación y conexionado continúa siendo más barato que en el caso de cables coaxiales. Tanto la red Ethernet como la TokenRing pueden usar este tipo de cable.

Figura 2.10: Par trenzado sin blindaje (UTP)



Fuente: http://www.eveliux.com/mx/index.php?option=com_content&task=view&id=21&Itemid=26

2.6.1.2 Fibra óptica

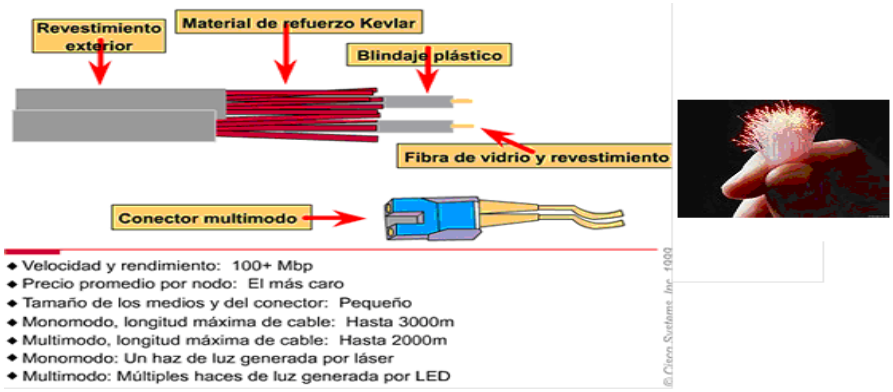
Es el medio de transmisión más moderno y avanzado. Utilizado cada vez más para formar la "espina dorsal" de grandes redes. Las señales de datos se transmiten a través de impulsos luminosos y pueden recorrer grandes distancias (del orden de kilómetros) sin que se tenga que amplificar la señal. [15]

Por su naturaleza, este tipo de señal y cableado es inmune a las interferencias electromagnéticas y por su gran ancho de banda (velocidad de transferencia), permite transmitir grandes volúmenes de información a alta velocidad.

Estas ventajas hacen de la fibra óptica la elección idónea para redes de alta velocidad a grandes distancias, con flujos de datos considerables, así como en instalaciones en que la seguridad de la información sea un factor relevante.

[15] http://www.eveliux.com/mx/index.php?option=com_content&task=view&id=21&Itemid=26

Figura 2.11: Fibra óptica



Fuente: http://www.slide.com/r/IHikAbJ0vj8UmWGLS6GOxQHbxGUOX7xt?cy=ls&view=large

Como inconveniente está, que es el soporte físico más caro. De nuevo, no debido al coste del cable en sí, sino por el precio de los conectores, el equipo requerido para enviar y detectar las ondas luminosas y la necesidad de disponer de técnicos cualificados para realizar la instalación y mantenimiento del sistema de cableado. [16]

2.6.2 Medios no guiados

Proporcionan un soporte para que las ondas se transmitan, pero no las dirigen; como ejemplo el aire y el vacío.

Los medios de transmisión no guiados son los que no confinan las señales mediante ningún tipo de cable, sino que las señales se propagan libremente a través del medio. Entre los medios más importantes se encuentran el aire y el vacío.[17]

Tanto la transmisión como la recepción de información se lleva a cabo mediante antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio. Por el contrario en 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.

---

[16] http://www.eveliux.com/mx/index.php?option=com_content&task=view&id=21&Itemid=26

[17] http://es.wikipedia.org/wiki/Medio_de_transmisi%C3%B3n

En la direccional, la antena transmisora emite la energía electromagnética concentrándola en un haz, por lo que las antenas emisora y receptora deben estar alineadas.

En la omnidireccional, la radiación se hace de manera dispersa, emitiendo en todas direcciones pudiendo la señal ser recibida por varias antenas. Generalmente, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

La transmisión de datos a través de medios no guiados, añade problemas adicionales provocados por la reflexión que sufre la señal en los distintos obstáculos existentes en el medio. Resultando más importante el espectro de frecuencias de la señal transmitida que el propio medio de transmisión en si mismo.

Según el rango de frecuencias de trabajo, las transmisiones no guiadas se pueden clasificar en tres tipos: radio, microondas y luz (infrarrojos/láser).[18]

Microondas: 2 GHz - 40 GHz. Muy direccionales. Pueden ser terrestres o por satélite.

Ondas radio: 30 MHz - 1 GHz. Omnidireccionales.

Infrarrojos: $3 \cdot 10^{11}$ - 200THz.

La zona del espectro de las microondas está dividida de la siguiente manera:

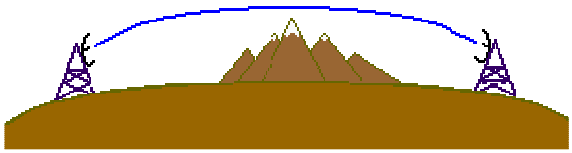
2.6.2.1 Microondas terrestres.

La antena típica de este tipo de microondas es parabólica y tiene unos tres metros de diámetro; el haz es muy estrecho por lo que las antenas, receptora y emisora deben estar muy bien alineadas. A cuanta mayor altura se sitúen las antenas, mayor la facilidad para esquivar obstáculos. La distancia que cubre un único radioenlace de microondas viene dada por la expresión:

---

18 http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

Figura 2.12: Microonda terrestre



$$d = 7.14 \cdot (k \cdot h)^{1/2}.$$

Fuente:

http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

h = altura de la antena (m)

k = 1 si no consideramos los efectos de la gravedad. Generalmente se toma k = 3/4.

Para cubrir distancias mayores se usan radioenlaces concatenados.

Aplicaciones:

La *transmisión a larga distancia*, ya que requiere menos repetidores que el cable coaxial, aunque por contra necesita que las antenas estén alineadas. El uso de microondas es frecuente en aplicaciones de TV y voz.

En *enlaces punto-a-punto sobre distancias cortas*, como circuitos cerrados de televisión, interconexión de redes locales y transmisión entre edificios.

Las microondas cubren una parte importante del espectro, de los 2 a los 40 GHz; el ancho de banda potencial y la velocidad de transmisión aumentan con la frecuencia, por lo que sus prestaciones son muy buenas y tienen múltiples aplicaciones como la transmisión de vídeo y de voz.

Tabla 2.3: Ancho de banda que cubre las microondas

Banda (GHz)	Ancho de Banda (MHz)	Régimen de transmisión (Mbps)
2	7	12
6	30	90
11	40	90
18	220	274

Fuente:

http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

El problema fundamental de este tipo de comunicación es la atenuación, que dependerá de la longitud de onda que estemos utilizando, así como de las condiciones meteorológicas: por ejemplo a partir de los 10 MHz aumenta mucho la atenuación a causa de la lluvia. La expresión general de la atenuación con la distancia es:

$$L\ (dB)=10\log\ (4\pi d/\lambda)^2$$

Además se dan problemas de interferencia entre unas y otras emisiones, por lo que es necesario regular las bandas.

Tabla 2.4: Problemas de interferencia entre emisiones

4-6 (GHz)	Transmisión a larga distancia
12 GHz	Directos
22 GHz	Televisión por cable

Fuente:

http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

Las principales aplicaciones de un sistema de microondas terrestre son las siguientes:[19]

- Telefonía básica (canales telefónicos)
- Datos
- Telégrafo / Télex / Facsímile
- Canales de Televisión.
- Vídeo
- Telefónica Celular

2.6.2.2 Microondas por satélite

El satélite se comporta como una estación repetidora que recoge la señal de algún transmisor en tierra y la retransmite difundiéndola entre una o varias estaciones terrestres receptoras, pudiendo regenerar dicha señal o limitarse a repetirla. Las frecuencias ascendente y descendente son distintas: fasc < fdesc. Para evitar interferencias entre satélites está normalizada una separación entre ellos de un mínimo de 3º (en la banda de la 12/14Ghz) o 4º(4/6GHz).

Tabla 2.5: Las frecuencias ascendente y descendente son distintas

Ascendente (GHz)	Descendente (GHz)	Ancho de banda (MHz)
4	6	500
12	14	500
19	29	2.500

Fuente:
http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

[19] http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

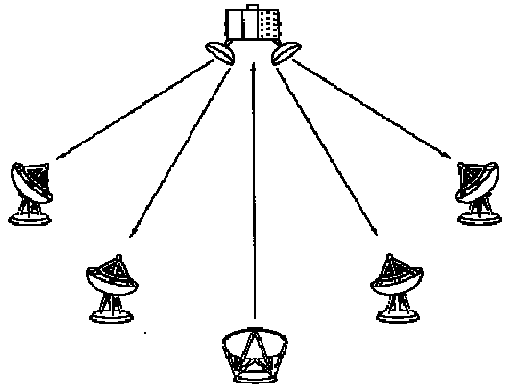
El rango de frecuencias óptimo para la transmisión comprende 1-10 GHz. Por debajo de 1 GHz aparecen problemas debidos al ruido solar, galáctico y atmosférico.

Por encima de 10 GHz, predominan la absorción atmosférica así como la atenuación debida a la lluvia. Cada satélite opera en una banda de frecuencia determinada conocida como *Transpondedor.*

Entre las aplicaciones figuran tanto enlaces punto-punto entre estaciones terrestres distantes como la difusión:

Difusión de TV: el carácter multidestino de los satélites los hace especialmente adecuados para la difusión, en particular de TV, aplicación para la que están siendo ampliamente utilizados.

Figura 2.13: Difusión de TV

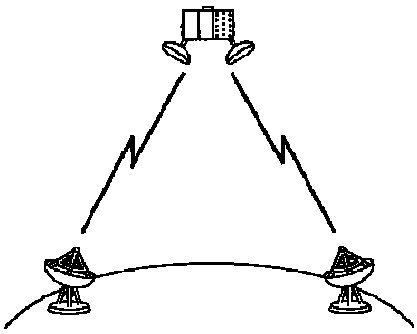


Fuente:
http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

Telefonía: los satélites proporcionan enlaces punto-a-punto entre centrales telefónicas en las redes públicas de telefonía. Es el medio óptimo para enlaces internacionales con un alto grado de utilización, y tecnológica y económicamente es competitivo con otros tipos de enlaces internacionales.

Redes privadas: la capacidad del canal de comunicaciones es dividido en diferentes canales de menor capacidad que se alquilan a empresas privadas que establecen su propia red sin necesidad de poner un satélite en órbita.

Figura 2.14: Redes privadas



Fuente:
http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

Un problema importante que surge en la transmisión de microondas vía satélite es el retardo debido a las largas distancias que recorren las ondas (aprox. 0.25 segundos) lo que dificulta el control de errores y flujo.

2.6.2.3 Ondas de Radio

Se caracterizan por ser omnidireccionales, por lo que no necesitaremos antenas parabólicas. Utilizarán la banda comprendida entre 30 MHz - 1GHz, para transmitir señales FM, TV (UHF, VHF), datos... [20]

Este rango de frecuencias es el más adecuado para transmisiones simultáneas (difusión,...). Las perturbaciones que sufriremos en este tipo de comunicaciones son provocadas por las reflexiones que se producen tanto en la tierra como en el mar, debidas a interferencias multitrayecto.

La distancia cubierta por el enlace vendrá dada por:

$d = 7.14 \cdot (k \cdot h)^{1/2}$.
h = altura de la antena (m)
k = 1 si no consideramos los efectos de la gravedad. Generalmente se toma k = 3/4.

Para cubrir distancias mayores se usan más radioenlaces concatenados.

[20] http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

De igual forma la atenuación:

$L(dB)=10\log(4\pi d/\lambda)^2$

2.6.2.4 Infrarrojos

Características fundamentales: [21]

- Reflexión directa.
- Utilización de transductores que modulan la luz infrarroja no coherente. Deberán estar alineados o tener una reflexión directa.
- No pueden atravesar obstáculos.
- Rapidez en la instalación, ya que no es necesario tener ningún permiso.
- Imposibilidad de establecer enlaces en medios abiertos debido al cambio de las condiciones climatológicas, que pueden actuar a modo de obstáculos.

2.6.2.5 Capacidad del medio

Ancho de banda para los medios de transmisión

El método de transmisión hace relación a la capacidad del medio para transmitir información. El ancho de banda nos indica la capacidad máxima del medio. [22]

Ancho de banda: es la diferencia entre la frecuencia más alta y más baja de una determinada onda. El término ancho de banda hace referencia a la capacidad del medio de transmisión, cuanto mayor es el ancho de banda, más rápida es la transferencia de datos.

---

[21] http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm

[22] http://www.unav.es/cti/manuales/Redes_Internet/#6

Por encima del ancho de banda las señales crean una perturbación en el medio que interfiere con las señales sucesivas. En función de la capacidad del medio, se habla de transmisión en banda base o transmisión en banda ancha.

Banda base: Las redes en banda base generalmente trabajan con mayor velocidad de transmisión que las redes de banda ancha, aunque la capacidad de estas últimas de transmitir por varios canales simultáneamente pueden hacer que el flujo total de datos sea prácticamente el mismo en ambos sistemas.

La transmisión de banda base utiliza señales digitales sobre una frecuencia. Utiliza toda la capacidad del canal de comunicaciones para transmitir una única señal de datos.

2.7 DIRECCIONAMIENTO IPV4 E IPV6

2.7.1 Historia del protocolo IP

Los días del protocolo IP en su formato actual (IPv4) están contados. A partir de la mitad de la década de los 90, las universidades, las industrias de alta tecnología y el gobierno comenzaron a utilizar Internet en gran medida, pero son las empresas comerciales las que se interesan cada vez más en Internet, que será utilizada por una gran cantidad de individuos y sistemas, todos con diferentes necesidades. [23]

Por ejemplo, con la inminente convergencia de las industrias informáticas, de redes, audiovisuales y de entretenimiento, dentro de poco todos los televisores se transformarán en equipos para acceder a Internet, lo cual permitirá que miles de millones de personas disfruten, por ejemplo, de videos a la carta, telecompras o comercio electrónico. En estas circunstancias, IPv6 (también denominado IPng por *IP* próxima generación) debe ofrecer mayor flexibilidad y eficacia para resolver una amplia gama de nuevos problemas, y nunca deben faltarle direcciones.

[23] http://es.kioskea.net/internet/ipv6.php3

Los principales objetivos de este nuevo protocolo son:

- Admitir miles de millones de equipos, superando las limitaciones de espacio para las direcciones IP actuales. [24]
- Reducir el tamaño de las tablas de enrutamiento.
- Simplificar el protocolo para permitir que los routers enruten datagramas de manera más rápida.
- Brindar mejor seguridad (autenticación y confidencialidad) que la proporcionada por el protocolo IP actual.
- Prestar más atención al tipo de servicio y, particularmente, a los servicios asociados con el tráfico en tiempo real.
- Facilitar la difusión a destinos múltiples, permitiendo especificar el tamaño;
- Permitir la movilidad de un equipo sin cambiar su dirección.
- Permitir el futuro desarrollo del protocolo.
- Posibilitar la coexistencia pacífica del protocolo antiguo con el nuevo.

2.7.2 Protocolo IPv4

IPv4 es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

Una dirección IP se representa mediante un número binario de 32 bits (IPv4). Las *direcciones IP* se expresan como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal máximo de cada octeto es 255 (el número binario de 8 bits más alto es 11111111, y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255 en total). Salvo algunas excepciones. Los ceros iníciales, si los hubiera, se pueden obviar.

Ejemplo de representación de dirección IPv4: *164.12.123.65*

[24] http://es.kioskea.net/internet/ipv6.php3

2.7.2.1 Desperdicio de direcciones del protocolo IPv4

El desperdicio de direcciones IPv4 se debe a varios factores.

Uno de los principales es que inicialmente no se consideró el enorme crecimiento que iba a tener Internet; se asignaron bloques de direcciones grandes (de 16,71 millones de direcciones) a países, e incluso a empresas.[25]

Otro motivo de desperdicio es que en la mayoría de las redes, exceptuando las más pequeñas, resulta conveniente dividir la red en subredes. Dentro de cada subred, la primera y la última dirección no son utilizables; de todos modos no siempre se utilizan todas las direcciones restantes. Por ejemplo, si en una subred se quieren acomodar 80 hosts, se necesita una subred de 128 direcciones (se tiene que redondear a la siguiente potencia de base 2); en este ejemplo, las 48 direcciones restantes ya no se utilizan.

Esta limitación ayudó a estimular el impulso hacia IPv6, que está actualmente en las primeras fases de implementación, y se espera que termine reemplazando a IPv4.[26]

2.7.2.2 Problemas más importantes sobre el protocolo IPv4:

- Campo de direcciones de 32 bits: se están terminando las direcciones IP.
- Calidad de servicio: si bien el datagrama de Ipv4 tiene un campo de type of service (TOS), no está implementado.

[25] http://es.wikipedia.org/wiki/IPv4
[26] http://www.andy21.com/ip/ip.html

2.7.3 Protocolo IPv6

El protocolo IPv6 responde razonablemente a los objetivos fijados. Conserva las mejores funciones de IPv4, mientras que elimina o minimiza las peores y agrega nuevas cuando es necesario.

En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos de Internet, incluyendo TCP, UDP, ICMP, IGMP, OSPF, BGP y DNS. A veces se requieren modificaciones mínimas (particularmente, cuando se trabaja con direcciones extensas).

2.7.3.1 Las principales funciones de IPv6 y ventajas con respecto IPv4

La principal innovación de IPv6 es el uso de direcciones más extensas que con IPv4. [27]

Están codificadas con 16 bytes y esto permite que se resuelva el problema que hizo que IPv6 esté a la orden del día: brindar un conjunto prácticamente ilimitado de direcciones de Internet.

IPv4 puede admitir *2^32=4,29.10^9* direcciones mientras que IPv6 puede admitir *2^128=3,4.10^38* direcciones.

La mejora más importante de IPv6 es la simplificación de los encabezados de los datagramas. El encabezado del datagrama IPv6 básico contiene sólo 7 campos (a diferencia de los 14 de IPv4). Este cambio permite que los routers procesen datagramas de manera más rápida y mejore la velocidad en general.

La tercera mejora consiste en ofrecer mayor flexibilidad respecto de las opciones. Este cambio es esencial en el nuevo encabezado, ya que los campos obligatorios de la versión anterior ahora son opcionales. Además, la manera en la que las opciones están representadas es distinta, dado que permite que los routers simplemente ignoren las opciones que no están destinadas a ellos. Esta función agiliza los tiempos de procesamiento de datagramas.

[27] http://es.kioskea.net/internet/ipv6.php3

Además, IPv6 brinda más seguridad.

La autenticación y confidencialidad constituyen las funciones de seguridad más importantes del protocolo IPv6.

Finalmente, se ha prestado más atención que antes a los tipos de servicios. Si bien el campo Type of services (Tipo de servicios) en el datagrama IPv4 se utiliza pocas veces, el esperado aumento del tráfico multimedia en el futuro demanda que se le otorgue mayor importancia.

2.7.3.2 Encabezados de datagramas básicos del protocolo IPv6

A continuación se indica cómo se ve un datagrama IPv6:

Tabla 2.6: Datagrama IPV6

<---------- 32 bits ---------->

Version (Versión)	Traffic class (Clase de tráfico)	Flow label (Etiqueta de flujo)
Payload length (Longitud de carga útil)	Next header (Siguiente encabezado)	Hop limit (Límite de saltos)
Source IP address (Dirección IP de origen)		
Destination IP address (Dirección IP de destino)		
Data (Datos)		

Fuente: http://es.kioskea.net/internet/ipv6.php3

2.7.3.2.1 Significados de los diferentes campos:

- **El campo Version** (Versión) siempre es equivalente a 4 bits para IPv6. Durante el período de transición de IPv4 a IPv6, los routers deberán fijarse en este campo para saber qué tipo de datagrama están enrutando.
- **El campo Traffic Class** (Clase de tráfico) (codificado con 8 bits) se utiliza para distinguir las fuentes que deben beneficiarse del control de flujo de otras. Se asignan prioridades de 0 a 7 a fuentes que pueden disminuir su velocidad en caso de congestión. Se asignan valores de 8 a 15 al tráfico en tiempo real (datos de audio y video incluidos) en donde la velocidad es constante.

Esta distinción en los flujos permite que los routers reaccionen mejor en caso de congestión. En cada grupo de prioridad, el nivel de prioridad más bajo se relaciona con los datagramas de menor importancia.

- **El campo Flow label** (Etiqueta de flujo) contiene un número único escogido por la fuente que intenta facilitar el trabajo de los routers y permitir la implementación de funciones de calidad de servicio como RSVP (*Resource reSerVation setup Protocol [Protocolo de reserva de recursos]*). Este indicador puede considerarse como un marcador de un contexto en el router. El router puede entonces llevar a cabo procesamientos particulares: escoger una ruta, procesar información en "tiempo real", etc.

  El campo de etiqueta de flujo puede llenarse con un valor aleatorio, que se utilizará como referencia del contexto. La fuente mantendrá este valor para todos los paquetes que envíe para esta aplicación y este destino. El procesamiento se optimiza debido a que el router ahora sólo tiene que consultar cinco campos para determinar el origen de un paquete. Además, si se utiliza una extensión de confidencialidad, la información relacionada con los números de puerto está enmascarada para los routers intermediarios.

- **El campo Payload limit** (Longitud de carga útil) de dos bytes contiene sólo el tamaño de la carga útil, sin tener en cuenta la longitud del encabezado. Para paquetes en los que el tamaño de datos es superior a 65.536, este campo vale 0 y se utiliza la opción de jumbograma de la extensión "salto a salto".
- **El campo Next header** (Siguiente encabezado) tiene una función similar a la del campo *protocol (protocolo)* en el paquete IPv4: simplemente identifica el encabezado siguiente (en el mismo datagrama IPv6). Puede ser un protocolo (de una capa superior ICMP, UDS, TCP, etc.) o una extensión.

- **El campo Hop limit** (Límite de saltos) reemplaza el campo *"TTL"* (*Time-to-Live [Tiempo de vida]*) en IPv4. Su valor (de 8 bits) disminuye con cada nodo que reenvía el paquete. Si este valor llega a 0 cuando el paquete IPv6 pasa por un router, se rechazará y se enviará un mensaje de error ICMPv6. Esto se utiliza para evitar que los datagramas circulen indefinidamente. Tiene la misma función que el campo *Time to live (Tiempo de vida)* en IPv4, es decir, contiene un valor que representa la cantidad de saltos y que disminuye con cada paso por un router. En teoría, en IPv4, hay una noción del tiempo en segundos, pero ningún router la utiliza. Por lo tanto, se ha cambiado el nombre para que refleje su verdadero uso.
- Los siguientes campos son **Source address** (Dirección de origen) y **Destination address** (Dirección de destino). Después de diferentes debates, se acordó que lo mejor era que las direcciones tuvieran una longitud fija equivalente a 16 bytes.

Los primeros bits de la dirección —el prefijo— definen el tipo de dirección. Las direcciones que comienzan con 8 ceros se reservan, en particular para las direcciones IPv4. Por lo tanto, todas las direcciones que comienzan con 8 ceros se reservan para las direcciones IPv4. Se admiten dos variantes, que se distinguen según los 16 bits siguientes (o sea 16 bits a 0 ó 1).

2.7.3.3 Notación IPv6

Se ha definido una nueva notación para describir las direcciones de 16 bytes IPv6. Comprende 8 grupos de 4 números hexadecimales separados por dos puntos. Por ejemplo:

8000:0000:0000:0000:0123:4567:89AB: CDEF

2.7.3.4 Autenticación para el protocolo IPv6

El encabezado de *autenticación* brinda un mecanismo que le permite al destinatario de un datagrama asegurarse de la identidad de la fuente. En IPv4 no se proporciona ninguna garantía similar. [28]

El uso de cifrado de datos para el datagrama (su carga útil) refuerza su seguridad; sólo el verdadero destinatario puede leerlo.

Cuando un remitente y un receptor desean comunicarse de manera segura, primero deben acordar una o varias claves secretas que sólo ellos conozcan. Se asigna un número clave de 32 bits a cada una de las 2 claves.

Los números clave son globales, de manera que, por ejemplo, si A utiliza la clave 4 para comunicarse con B, A no puede utilizar esta clave para comunicarse con C. Existen otros parámetros que se asocian con cada clave, como su tiempo de vida, etc.

El encabezado de *autenticación* consta de 3 partes. La primera tiene 4 bytes que especifican el número del encabezado siguiente, la longitud del encabezado de autenticación y 16 bits cero. La segunda define el número clave de 32 bits. La tercera contiene la suma de comprobación del cifrado (con MD5 o cualquier otro algoritmo).

El destinatario utiliza el número clave para encontrar la clave secreta. El valor completo de la clave secreta se agrega antes y después de que se complete la carga útil, los campos de encabezados variables eliminan sus ceros, y después se calcula la suma de comprobación del cifrado. Si el resultado del cálculo es equivalente a la suma de comprobación del cifrado contenida en el encabezado de autenticación, el destinatario puede estar seguro de que el datagrama realmente proviene de la fuente con la que comparte la clave secreta. También se asegura de que el datagrama no se haya falsificado sin su conocimiento.

[28] http://es.kioskea.net/internet/ipv6.php3

Podemos utilizar IPv6 incluso en redes IPv4 y podemos sacar partido a viejas aplicaciones, incluso a aquellas que no han tenido éxito, por ejemplo: automatización, control remoto, monitorización, vigilancia, alarmas, etc…

2.8 MODELO DE REFERENCIA Y ESTÁNDARES 802.11

El estándar 802.11 de IEEE se publica en junio 1997, luego de seis años de proceso de creación. Propone velocidades de 1 y 2Mbps y un rudimentario sistema de cifrado (el WEP: Wired Equivalent Privacy), opera en 2,4 GHz con RF.

En septiembre de 1999 salen a la luz el estándar 802.11b que ofrece 11Mbps y el 802.11a que ofrece 54 Mbps, si bien los productos de la primera aparecieron en el mercado mucho antes.[29]

El estándar IEEE 802.11 se basa en el mismo marco de estándares que Ethernet. Esto garantiza un excelente nivel de interoperatividad y asegura una implantación sencilla de las funciones y dispositivos de interconexión Ethernet/WLAN.

El comité IEEE encargado de la tecnología de red de área local desarrolló el primer estándar para redes LAN inalámbricas (IEEE 802.11).
El IEEE revisó ese estándar en octubre de 1999 para conseguir una comunicación por RF a velocidades de datos más altas. El IEEE 802.11b resultante describe las características de las comunicaciones LAN RF de 11 Mbps.[30]

El estándar IEEE 802.11 está en constante desarrollo. Existen varios grupos de trabajo encargados de proponer y definir nuevas mejoras y apéndices al estándar WLAN:

El estándar 802.11 define varios métodos y tecnologías de transmisión para implantaciones de LAN inalámbricas. Este estándar no sólo engloba la tecnología de radiofrecuencia sino también la de infrarrojos.

---

[29] http://www.wikilearning.com/curso_gratis/seguridad_en_wifi_tecnico-los_estandares_802_11/4171-1
[30] http://www.e-advento.com/tecnologia/wlan_intro.php

2.8.1 Técnicas de transmisión del estándar 802.11

- Modulación por saltos de frecuencia (FHSS)
- Expectro de extensión de secuencia directa (DSSS)
- Multiplexación por división en frecuencias octogonales (OFDM)

Todos estos enfoques distintos tienen la misma capa MAC implantada. La mayoría de los productos WLAN de 11 Mbps utilizan tecnología de RF y se sustentan en DSSS para la comunicación.

2.8.1.1 DSSS

Funciona transmitiendo simultáneamente por varias frecuencias diferentes. De esta forma, se incrementa la probabilidad de que los datos transmitidos lleguen a su destino. Además, los patrones de bits redundantes, llamados “chips”, se incluyen en la señal. En cualquier momento, se reciben partes de la señal simultáneamente en las distintas frecuencias en el receptor. Para poder recibir y descodificar la señal completa de modo satisfactorio, la estación receptora debe conocer el patrón de descodificación correcto. Realizar el seguimiento y la descodificación de los datos durante la transmisión es extremadamente difícil.

2.8.1.2 FHSS

La segunda técnica importante de transmisión de espectro de extensión, es de hecho una señal de banda estrecha que cambia la frecuencia de un modo rápido y continúo.

El inconveniente del DSSS en relación con el FHSS es que es más vulnerable a las interferencias de la banda estrecha.

Todos los productos electrónicos del mercado deben cumplir con unas normativas rigurosas sobre radiación electromagnética. Los organismos de estandarización nacionales, europeos e internacionales establecen las normativas con detalle para asegurar que las tecnologías inalámbricas no tengan consecuencias negativas sobre los diversos sistemas que utilizan tecnología de radiofrecuencia (RF).

2.8.1.3 OFDM

Se ha desarrollado para ser utilizada en sistemas 802.11a que ya operen en las bandas de 5 GHz. El mayor problema a la hora de introducir la modulación OFDM en la banda de 2,4 GHz fue hacerla compatible con los productos 802.11b heredados.

El principal mecanismo para compartir caneles en el sistema 802.11 es CSMA/CA. Para que este método funcione, cada radio debe ser capaz de detectar a todas las demás radios asociadas al mismo punto de acceso (incluido, obviamente, el propio PA). Pero con sistemas 802.11g que utilizaran OFDM, las radios 802.11b heredadas serían incapaces de detectar a los nuevos dispositivos.

2.8.2 El estándar IEEE802.11 ofrece dos métodos de autenticación

- ***Open System Authentification*** es un tipo de autenticación que prácticamente no restringe el acceso a la WLAN.
- ***La autenticación Shared Key Authentification***, por su parte, utiliza claves WEP para realizar su cometido. Los clientes que no posean una clave WEP válida no podrán conectarse al punto de acceso. La WEP proporciona un elevado nivel de seguridad a las LAN inalámbricas, aunque no se trata de un sistema inviolable.

2.8.3 Capas del modelo OSI que intervienen en el estándar IEEE 802.11.

2.8.3.1 CAPA FÍSICA

Especifica las características eléctricas, ópticas o de radio de las señales transmitidas (signaling) y las conexiones (conectores) mecánicas/físicas aplicables al tipo de medio en uso.[31]

Las funciones de esta capa incluyen:

- Codificación/Decodificación de las señales (Ejemplo: PSK, QAM)
- Generación de los preámbulos que se utilizan para la sincronización

[31] http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Inalambricas/CLASES/802-11ParteIa.pdf

- Transmisión/ recepción de bits

La capa física del modelo 802.incluye una especificación del medio de transmisión. Generalmente esto es considerado “Bajo” el nivel más bajo del modelo OSI la decisión del medio de transmisión es crítico en las LANs, por lo que se incluye una especificación del medio y la topología.

Además de desarrollar un modelo de referencia, también se desarrolló un modelo de implementación para guiar el desarrollo de estándares y protocolos específicos.

La diferencia es que el modelo de implementación resalta la complejidad de estandarización de la capa física. En la mayoría de casos en la especificación de la capa física hay una porción:

- Independiente del medio que trata con: codificación de las señales, sincronización y otros aspectos comunes entre diferentes medios
- Dependiente del medio que trata con aspectos eléctricos y mecánicos
- Dependiendo de la implementación, estas dos partes pueden implementarse separadamente con una interfaz entre ellas.

La capa física de cualquier red define la modulación y la señalización, características de la transmisión de datos. Se separa en 2 partes:
PLCP (Physical Layer Convergence Protocol)
PMD (Physical Médium Dependet)

2.8.3.1 PLCP (Physical Layer Convergence Protocol)

PLCP consiste en un encabezado de 144 bits que sirve para sincronizar para determinar la ganancia y para establecer el CCA (Clear Channel Assessment) que es necesaria para que la capa de MAC sepa si el medio esta en uso. Este preámbulo está compuesto por 128 bits de sincronización más 16 bits llamados SFD (Start Frame Delimiter) que consiste en una secuencia fija de 0 y 1 (1111001110100000) que marca el principio del paquete. El PLCP es siempre transmitido a 1Mbps. Los próximos 48 bits son llamados Encabezado PLCP.

Cuenta con 4 campos: señal, servicio, longitud y HEC ("header error check" para control de errores). La señal indica a qué velocidad se deberá transmitir (1, 2, 5.5 u 11Mbps). El campo de servicio se reserva para uso futuro. El campo de longitud indica la longitud del paquete y el HEC es un CRC de 16bits del encabezado de 48bits. El PMD es dependiente del protocolo antes explicado.

2.8.3.2 PMD (Physical Médium Dependet)

Esta sub-capa proyecta el medio físico para la sub-capa PCS. Esta capa define la señalización de la capa física usada por diferentes medios. La MDI (Medium Dependent Interface) la cual es parte de PMD es actualmente la interfaz de la capa física. Esta capa define la actual capa física de unión, como los conectores de los diferentes medios de trasmisión.

Es dependiente del protocolo antes mencionado. Posee 3 medios de modulación y señalización:

FHSS (Frecuency Hopping Spread Spectrum)

DSSS (Direct Sequence Spectrum)

OFDM (Orthogonal Frecuency Division Multiplexing)

Estos métodos permiten tener muchas transmisiones al mismo tiempo, haciéndose poca interferencia unas sobre otras.

2.8.3.1.3 PROTOCOLOS IEEE 802.11 DE LA CAPA FÍSICA

Todos los estándares aquí mencionados son parte de IEEE, que está formada por grupos de ingenieros que se unen para estandarizar la implementación de distintos tipos de tecnología. Ellos escriben las normas que los fabricantes de hardware y los desarrolladores deben usar para lograr la compatibilidad entre diferentes marcas y sistemas operativos. Lo más importante es que las normas que ellos escriben no son propietarias, sino que son libres.

También existen protocolos propietarios. La desventaja de usar éstos reside en que sólo se pueden interconectar equipos de ese fabricante.

Se detallaran sólo unos pocos de esos protocolos libres: 802.11a, 802.11b, 802.11g y 802.11n.

Todos son más o menos parecidos, sólo se diferencian en algunos detalles, velocidad de transferencia y algunos en la frecuencia en la que transmiten.

2.8.3.1.3.1 IEEE 802.11a

La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.[32]

Dado que la banda de 2.4 GHz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a, únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

[32] http://es.wikipedia.org/wiki/IEEE_802.11

Tabla 2.7: Indicadores de canales de IEEE802.11a

Identificador de Canal	Frecuencia en MHz	Dominios Reguladores			
		América (-A)	EMEA (-E)	Israel (-I)	Japón (-J)
34	5170	—	×	—	—
36	5180	×	—	×	—
38	5190	—	×	—	—
40	5200	×	—	×	—
42	5210	—	×	—	—
44	5220	×	—	×	—
46	5230	—	×	—	—
48	5240	×	—	×	—
52	5260	×	—	—	×
56	5280	×	—	—	×
60	5300	×	—	—	×
64	5320	×	—	—	×
149	5745	—	—	—	—
153	5765	—	—	—	—
157	5785	—	—	—	—
161	5805	—	—	—	—

Fuente: http://es.wikipedia.org/wiki/IEEE_802.11

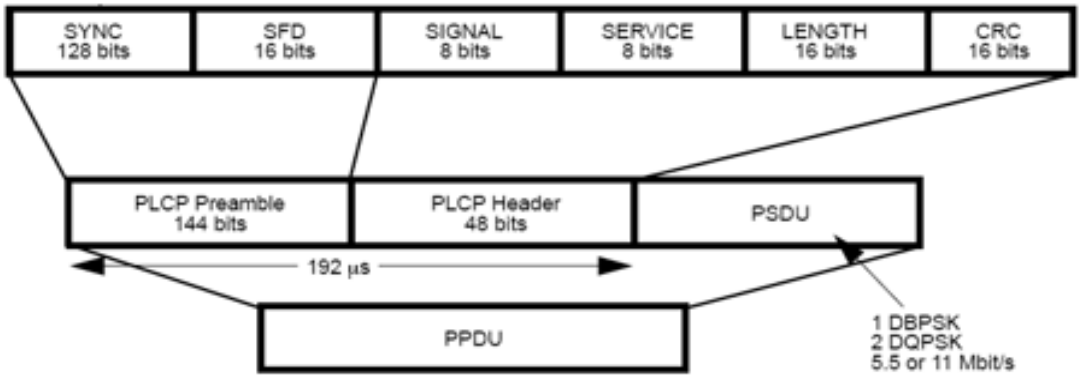
Para la compatibilidad con sistemas de radar existentes y evitar interferencias con comunicaciones por satélite, en Europa se requiere la implementación de un control dinámico de las frecuencias y un control automático de las potencias de transmisión. Es por eso que para su uso en Europa, las redes 802.11a deben incorporar las modificaciones del 802.11h.

2.8.3.1.3.2 IEEE 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

Aunque también utiliza una técnica de ensanchado de espectro basada en DSSS, en realidad la extensión 802.11b introduce CCK (Complementary Code Keying) para llegar a velocidades de 5,5 y 11 Mbps (tasa física de bit). El estándar también admite el uso de PBCC (Packet Binary Convolutional Coding) como opcional. Los dispositivos 802.11b deben mantener la compatibilidad con el anterior equipamiento DSSS especificado a la norma original IEEE 802.11 con velocidades de 1 y 2 Mbps.

Figura 2.15: Trama del nivel físico de 802.11b



Fuente:
http://rinuex.unex.es/modules.php?op=modload&name=Articulos&file=article&sid=88&mode=thread&order=0&thold=0

2.8.3.1.3.3 IEEE 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Que es la evolución del estándar 802.11b, Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

Tabla 2.8: Identificadores de canales de IEEE802.11b y IEEE 802.11g

Identificador de Canal	**Frecuencia en MHz**	**Dominios Reguladores**			
		América (-A)	**EMEA (-E)**	**Israel (-I)**	**China (-C)**
1	2412	×	×	—	×
2	2417	×	×	—	×
3	2422	×	×	×	×
4	2427	×	×	×	×
5	2432	×	×	×	×
6	2437	×	×	×	×
7	2442	×	×	×	×
8	2447	×	×	×	×
9	2452	×	×	×	×
10	2457	×	×	—	×
11	2462	×	×	—	×
12	2467	—	×	—	—
13	2472	—	×	—	—
14	2484	—	—	—	—

Fuente: http://es.wikipedia.org/wiki/IEEE_802.11

El ancho de banda de la señal (22MHz) es superior a la separación entre canales consecutivos (5MHz), por eso se hace necesaria una separación de al menos 5 canales con el fin de evitar interferencias entre celdas adyacentes. Tradicionalmente se utilizan los canales 1, 6 y 11, aunque se ha documentado que el uso de los canales 1, 5, 9 y 13 (en dominios europeos) no es perjudicial para el rendimiento de la red.

Los estándares 802.11b y 802.11g utilizan la banda de 2.4 – 2.5 Ghz. En esta banda, se definieron 11 canales utilizables por equipos WIFI, que pueden configurarse de acuerdo a necesidades particulares. Sin embargo, los 11

canales no son completamente independientes (canales contiguos se superponen y se producen interferencias) y en la práctica sólo se pueden utilizar 3 canales en forma simultánea (1, 6 y 11). Esto es correcto para Estado Unidos y muchos países de América Latina, pues en Europa, el ETSI ha definido 13 canales. En este caso, por ejemplo en España, se pueden utilizar 4 canales no-adyacentes (1, 5, 9 y 13). Esta asignación de canales usualmente se hace sólo en el Access Point, pues los "clientes" automáticamente detectan el canal, salvo en los casos en que se forma una red "Ad-Hoc" o punto a punto cuando no existe Access Point.

2.8.3.1.3.4 IEEE 802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. [33]

También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008. A principios de 2007 se aprobó el segundo borrador del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial éste estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo estuviera implantado).

A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje

[33] http://es.wikipedia.org/wiki/IEEE_802.11

en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

2.8.3.2 LA CAPA MAC

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas.

A pesar de todo ello la norma IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas. Ayudando a la fabricación en serie de chips. [34]

Se debe tener en cuenta:

- Perturbaciones ambientales (interferencias)
- Variaciones en la potencia de la señal
- Conexiones y desconexiones repentinas en la red
- Roaming. Nodos móviles que van pasando de celda en celda.

2.8.3.2.1 Mecanismos de Acceso de la capa MAC

Hay de dos tipos:

- Protocolos con arbitraje:

  FDMA - Frequency Division Multiple Access,

  TDMA - Time Division Multiple Access

- Protocolos de contienda

  CDMA/CA - Carrier-Sense, Multiple Access, Collision Avoidance)

  CDMA (Code Division, Multiple Access)

  CDMA/CD (detección de colisión).

Aunque también se han diseñado protocolos que son una mezcla de ambos.

[34] http://www.canal-ayuda.org/a-informatica/inalambrica.htm

2.8.3.2.1.1 Protocolos con arbitraje

La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).[35]

Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama multiplexación en el tiempo (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

2.8.3.2.1.2 Protocolos de acceso por contienda

Tienen similitudes al de Ethernet cableada de línea normal 802.3.

2.8.3.2.1.2.1 CSMA

(Code-division multiple access) Acceso múltiple por división de tiempo.

Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia PN. En este esquema se asigna una secuencia PN distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias PN pertenecientes a los demás nodos. Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia PN del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

[35] http://www.canal-ayuda.org/a-informatica/inalambrica.htm

2.8.3.2.1.2.2 CSMA/CD

(Carrier Sense, Multiple Access, Collision Detection). Como en estos medios de difusión (radio, infrarrojos), no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las LAN alambradas. Se diseño una variación denominada detección de colisiones (peine) para redes inalámbricas. En este esquema, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria seudoaleatoria corta, llamada peine la cual se añade al preámbulo de la trama. A continuación, el nodo realiza la detección de la portadora si el canal está libre transmite la secuencia del peine. Por cada 1 del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada 0 del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama.

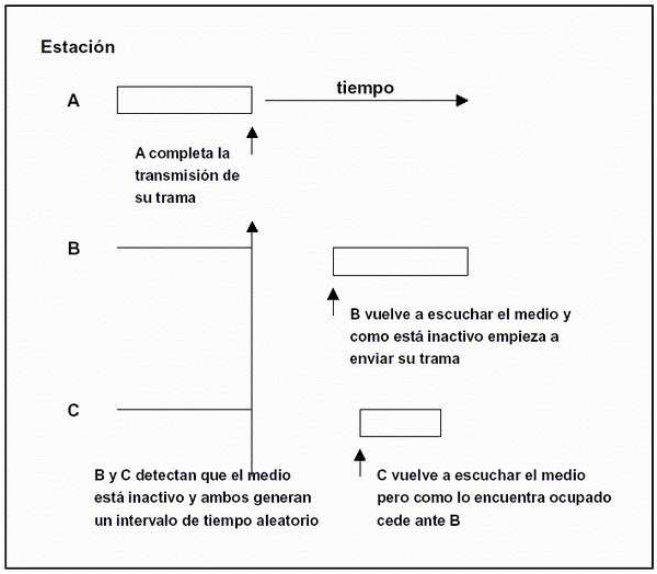
La eficiencia del esquema depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

2.8.3.2.1.2.3 CSMA/CA

(Carrier-Sense, Múltiple Access, Collision Avoidance). Es el más utilizado, este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3.

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

Figura 2.16: Mecanismo De intercambio de mensajes



Fuente: http://www.canal-ayuda.org/a-informatica/inalambrica.htm

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF[6] de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI.

Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

El Standard proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible. Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11.

En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido)[6] RF = RadioFrecuencia.

Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión. Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina Reservation-Based Protocol, que es la 2ª subcapa MAC.

Cuando una estación está lista para transmitir, primero envía una solicitud (destino y longitud del mensaje) al punto de acceso (RTS – "request to send") quien difunde el NAV (Network Allocation Vector) -un tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos para que queden informados de que se va a transmitir (y que por lo tanto no transmitan) y cuál va a ser la duración de la transmisión. Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de backoff (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS – "clear to send") que permite al solicitante enviar su trama (datos).[36]

Después de que se recibe la trama de los datos, se devuelve una trama de reconocimiento (ACK - ACKnowledged) notificando al transmisor que se ha recibido correctamente la información (sin colisiones).

Aún así permanece el problema de que las tramas RTS sean enviadas por varias estaciones a la vez, sin embargo estas colisiones son menos dañinas ya que el tiempo de duración de estas tramas es relativamente corto.

Este mismo protocolo también puede utilizarse si no existen dispositivos auxiliares en las redes ad-hoc, en este caso no aparecería la trama NAV.

[36] http://www.canal-ayuda.org/a-informatica/inalambrica.htm

2.9 ESTUDIO DE LAS REDES INALÁMBRICAS

2.9.1 INTRODUCCIÓN

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. [37]

Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de más de 10 Mbps.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

1. De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.[38]

[37] http://www.monografias.com/trabajos12/reina/reina.shtml

[38]http://www.monografias.com/trabajos12/reina/reina.shtml

2. De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

2.9.2 HISTORIA

La primera red de computadores inalámbrica registrada, data de 1971 en la Universidad de Hawai cuando se conectaron siete computadores desplegados en cuatro islas hawaianas, AlohaNet, trabajando alrededor de los 400 MHz.

E l origen de las redes inalámbricas (WLAN) o también conocida como Wi-Fi (Wireless Fidelity) se remonta a la publicación, en 1979, de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés), pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. [39]

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro expandido (spread spectrum), donde su funcionamiento consta en dividir las señales informativas en varias frecuencias.

Existen dos tipos generales de señalización de Espectro Expandido:

- Espectro Expandido con Salto de Frecuencia (FHSS), que es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto donde se tiene una cantidad de receptores dimensionados en un área relativamente cercana al punto de acceso.
- Espectro Expandido en Secuencia Directa (DSSS), a diferencia de FHSS este espectro no requiere enviar la información a través de varias frecuencias, sino que lo hace mediante un transmisor.

En mayo de 1985, y tras cuatro años de estudios, la Comisión Federal de Comunicaciones (CFC), la agencia federal del gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (industrial, scientific and medical) para uso en las redes

[39] http://www.jornada.unam.mx/2006/02/02/033a1tec.php

inalámbricas basadas en ese espectro. La técnica de espectro expandido es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias. La asignación de esta banda de frecuencias propició mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de un Mbit/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

Las redes inalámbricas (WLAN) se componen fundamentalmente de dos elementos: los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un concentrador o hub, que recibe y envía información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente una PC o PDA con una tarjeta de red inalámbrica, con o sin antena, que se instala en una de las ranuras libres o bien se enlazan a los puertos USB de los equipos.

La principal ventaja de estas redes, que no necesitan licencia para su instalación, es la libertad de movimientos que permite a sus usuarios, ya que la posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información en todos los lugares por donde puedan estar trabajando. A esto se añade la ventaja de que son mucho más sencillas de instalar que las redes de cable y permiten la fácil reubicación de las terminales en caso necesario.

También presentan alguna desventaja, o más bien inconveniente, que es la "baja" velocidad que alcanzan, por lo que su éxito comercial es más bien escaso, y hasta que los nuevos estándares no permitan un incremento significativo, no es de prever su uso masivo, ya que por ahora no pueden competir con las LAN basadas en cable.

El uso más popular de las WLAN implica la utilización de tarjetas de red inalámbricas, cuya función es permitir al usuario conectarse a la LAN empresarial sin necesidad de una interfaz física.

Con WiFi nos acostumbramos a la banda ancha inalámbrica (BAI). Dentro de nuestra casa u oficina nos podemos mover sin problemas y estar conectados casi siempre. "Casi", ya que el gran problema de WiFi es su alcance, con un máximo teórico de 100 metros, que se convierten en algo así como 10 metros si hay muros en su camino. Por esta razón hay una carrera por mejorar el alcance y la calidad de las conexiones de BAI, que solamente puede terminar por beneficiar a los usuarios.

Las redes de área local inalámbrica funcionan desde hace más de quince años en entornos industriales y de investigación.

En estos últimos años se ha producido un crecimiento en el mercado de hasta un 100 % anual.

2.9.3 VENTAJAS DE WLANS SOBRE LAS REDES ALÁMBRICAS

2.9.3.1 Movilidad

Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica. [40]

2.9.3.2 Simplicidad y rapidez en la instalación

La instalación de una red inalámbrica puede ser tan rápida y fácil y además que puede eliminar la posibilidad de tirar cable a través de paredes y techos.

2.9.3.3 Flexibilidad en la instalación

La tecnología inalámbrica permite a la red ir donde la alámbrica no puede ir.

---

[40] http://www.gestiopolis.com/canales8/ger/definicion-y-tipo-de-redes-inalambricas.htm

2.9.3.4 Costo de propiedad reducido

Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN alámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo, son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

2.9.3.5 Escalabilidad

Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

2.9.4 DESVENTAJAS DE LAS REDES INALÁMBRICAS

Las redes inalámbricas también tienen unos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes: [41]

2.9.4.1 Menor ancho de banda

Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.

2.9.4.2 Mayor inversión inicial

Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

[41] http://www.gestiopolis.com/canales8/ger/definicion-y-tipo-de-redes-inalambricas.htm

2.9.4.3 Seguridad

Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no esta definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad valida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

2.9.4.4 Interferencias

Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GAZ. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía de nuestro entorno radioelectrónico este completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

2.9.4.5 Incertidumbre tecnológica.

La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11B). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.[42]

2.9.5 DIFERENCIAS DE UNA RED INALÁMBRICA FRENTE A UNA RED CABLEADA

La red inalámbrica, por su propia naturaleza, está sujeta a muchas limitaciones. No es la red recomendada para puestos de trabajo permanentes.[43]

1. Problemas de cobertura e interferencias con otros dispositivos u objetos inertes pueden hacer que el rendimiento de la red disminuya mucho o sea casi nulo. El medio de transmisión son las bandas de RadioFrecuencia de 2,4 y 5GHz, que también son utilizadas por otros dispositivos. Por tanto, al ser un medio de transmisión de condiciones muy variables, se pueden producir interferencias en cualquier momento, con lo que la fuerza de la señal, la relación señal/ruido, y la velocidad de transmisión fluctúan conforme cambian las condiciones ambientales.
2. La velocidad nominal máxima de las redes inalámbricas es de 54 Mbs. Esta velocidad se comparte entre la transmisión y la recepción.
3. Esa velocidad nominal máxima mencionada, en velocidad *efectiva* de transmisión de datos supone 23 Mbs o menos. Y también se reparte entre transmisión y recepción.

[42] http://www.gestiopolis.com/canales8/ger/definicion-y-tipo-de-redes-inalambricas.htm
[43] http://www.uam.es/servicios/ti/servicios/wifi/miscelanea.html

4. Ambas velocidades disminuyen rápidamente si el AP (Access Point) que nos conecta a la red está alejado.
5. Todos los usuarios conectados a un mismo AP comparten el acceso y el caudal disponible de transmisión.
6. En un puesto de trabajo inalámbrico no se puede tener una extensión telefónica propia de la universidad (91 497 XX XX).

A cambio, con la red cableada, todos los puntos anteriores se convierten en los siguientes:

1. No hay problemas de cobertura ni interferencias. El cable es un medio controlado, con una fuerte protección frente a interferencias y en el que los parámetros básicos de transmisión son constantes.
2. La velocidad nominal máxima de las redes cableadas en la universidad es 100 Mbs en transmisión y 100 Mbs en recepción.
3. Esa velocidad nominal máxima mencionada, en velocidad *efectiva* de transmisión de datos podría suponer 93 o 95 Mbs. En transmisión y en recepción por separado. Esto se cumplirá siempre que la transferencia se realice con otra máquina de la propia universidad que tenga una tarjeta a 100Mbs. Si la otra máquina es antigua (tarjeta 10Mbs) o está muy cargada entonces ella establecerá el límite.
4. La velocidad no disminuye por lejanía del PC.
5. La velocidad asignada a cada PC no se comparte con los PCs contiguos.
6. En un puesto de trabajo cableado se puede poner una extensión telefónica.

2.9.6 IDENTIFICACIÓN DE UNA RED INALÁMBRICA

Hay muchas maneras de identificar una red inalámbrica, dependiendo de su tamaño y componentes:[44]

- **El Nombre de la red o Identificador del conjunto de servicios (SSID):** Identifica una red inalámbrica. Todos los dispositivos inalámbricos de la red deben utilizar el mismo SSID.
- **SSID de difusión:** Un punto de acceso que difunde su nombre de red. Si se activa esta función en un punto de acceso, cualquier usuario inalámbrico podrá conectarse a él utilizando un SSID en blanco (nulo).
- **Conjunto de servicios básicos (BSS):** Se compone de un mínimo de dos o más nodos o estaciones inalámbricos e incluye al menos un punto de acceso o router inalámbrico, que se han reconocido entre sí y han establecido comunicaciones.
- **Conjunto de servicios básicos independientes (IBSS):** Es un modo de funcionamiento en un sistema 802.11 que permite la comunicación directa entre dispositivos 802.11 sin necesidad de establecer una sesión de comunicación con un punto de acceso.

2.9.7 CLASIFICACIÓN DE LAS REDES INALÁMBRICAS

Las redes inalámbricas se clasifican en dos tipos:

- Redes inalámbricas personales
- Redes inalámbricas por consumo

2.9.7.1 REDES INALÁMBRICAS PERSONALES

Se permite que la comunicación sea por dos 2 medios:

- Infrarrojos
- Bluetooth

[44] http://support.dell.com/support/edocs/network/p94583i/SP/wlan.htm

2.9.7.1.1 INFRARROJOS.

Las redes por infrarrojos permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita "ver" al otro para realizar la comunicación por ello es escasa su utilización a gran escala.[45]

Esa es su principal desventaja, a diferencia de otros medios de transmisión inalámbricos (Bluetooth, Wireless, etc.).

La comunicación se realiza entre un diodo emisor que emite una luz en la banda de IR, sobre la que se superpone una señal, convenientemente modulada con la información de control, y un fotodiodo receptor cuya misión consiste en extraer de la señal recibida la información de control.

Los controladores de equipos domésticos basados en la transmisión de ondas en Comodidad y la banda de los infrarrojos tienen las siguientes ventajas: Admiten gran número de aplicaciones. Flexibilidad.

Al tratarse de un medio de transmisión óptico es inmune a las radiaciones electromagnéticas producidas por los equipos domésticos o por los demás medios de transmisión (coaxial, cables pares, red de distribución de energía eléctrica, Las etc.). Sin embargo, habrá que tomar precauciones en los siguientes casos: interferencias electromagnéticas sólo afectaran a los extremos del medio IR, es decir, a partir de los dispositivos opto electrónicos (diodo emisor y fotodiodo Es necesario tener en cuenta otras posibles fuentes de IR. Hoy en receptor). Hoy en día, existen diferentes dispositivos de iluminación que emiten cierta radiación IR

Se utiliza principalmente para realizar intercambio de datos entre dispositivos móviles, como PDA's o móviles, ya que el rango de velocidad y el tamaño de los datos a enviar/recibir es pequeño. Adicionalmente, se puede usar para jugar juegos de dos jugadores.

---

[45] http://es.wikipedia.org/wiki/Red_por_infrarrojos

El uso de mandos a distancia basados en transmisión por infrarrojos esta ampliamente extendidas en el mercado residencial para tele comandar equipos de Audio y Vídeo.[46]

2.9.7.1.1.1 Tipos de Infrarrojos

Existen 3 Tipos

- Punto a punto
- Cuasi-difuso
- Difuso

2.9.7.1.1.1.1 Modo punto-a-punto

Los patrones de radiación del emisor y del receptor deben de estar lo más cerca posible y que su alineación sea correcta. Como resultado, el modo punto-a-punto requiere una línea-de-visión entre las dos estaciones a comunicarse. Este modo, es usado para la implementación de redes Inalámbricas Infrarrojas Tomen-Ring. El "Ring" físico es construido por el enlace inalámbrico individual punto-a-punto conectado a cada estación.[47]

El uso de esta técnica tiene ciertas desventajas. El haz infrarrojo es afectado por el clima, interferencia atmosférica y por obstáculos físicos. Como contrapartida, tiene inmunidad contra el ruido magnético o sea la interferencia eléctrica.

Los dispositivos emisores y receptores deben ser ubicados “a la vista” uno del otro. Su velocidad de transmisión de hasta 100 Kbps puede ser soportadas a distancias hasta de 16 Km. Reduciendo la distancia a 1.6 Km. Se puede alcanzar 1.5 Mbps.

[46] http://es.wikibooks.org/wiki/Componentes_de_una_red/Medios_de_Transmision_Inalambricos/
[47] http://es.wikipedia.org/wiki/Red_por_infrarrojos

2.9.7.1.1.1.2 Modo Cuasi-difuso

Son de emisión radial, ósea que cuando una estación emite una señal óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo en la célula. En el modo cuasi–difuso las estaciones se comunican entre si, por medio de superficies reflectantes. No es necesaria la línea-de-visión entre dos estaciones, pero sí deben de estarlo con la superficie de reflexión. Además es recomendable que las estaciones estén cerca de la superficie de reflexión, ésta puede ser pasiva ó activa. En las células basadas en reflexión pasiva, el reflector debe de tener altas propiedades reflectivas y dispersivas, mientras que en las basadas en reflexión activa se requiere de un dispositivo de salida reflexivo, conocido como satélite, que amplifica la señal óptica. La reflexión pasiva requiere más energía, por parte de las estaciones, pero es más flexible de usar.

2.9.7.1.1.1.3 Modo Difuso

El poder de salida de la señal óptica de una estación, debe ser suficiente para llenar completamente el total del cuarto, mediante múltiples reflexiones, en paredes y obstáculos del cuarto. Por lo tanto la línea-de-vista no es necesaria y la estación se puede orientar hacia cualquier lado. El modo difuso es el más flexible, en términos de localización y posición de la estación, sin embargo esta flexibilidad esta a costa de excesivas emisiones ópticas. Por otro lado la transmisión punto-a-punto es el que menor poder óptico consume, pero no debe de haber obstáculos entre las dos estaciones. En la topología de Ethernet se puede usar el enlace punto-a-punto, pero el retardo producido por el acceso al punto óptico de cada estación es muy representativo en el rendimiento de la red. Es más recomendable y más fácil de implementar el modo de radiación cuasi-difuso. La tecnología infrarroja está disponible para soportar el ancho de banda de Ethernet, ambas reflexiones son soportadas (por satélites y reflexiones pasivas).[48]

[48] http://es.wikipedia.org/wiki/Red_por_infrarrojos

2.9.7.1.2 Bluetooth

Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre (2,4 GHz.). Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

Los dispositivos que con mayor intensidad utilizan esta tecnología son los de los sectores de las telecomunicaciones y la informática personal, como PDAs, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras y cámaras digitales.

De acuerdo con la Universidad Autónoma de Bucaramanga esta tecnología estará obsoleta pronto, ya que Wi-Fi la reemplazará por sus innumerables ventajas.

2.9.7.1.2.1 USO Y APLICACIONES DE Bluetooth

Bluetooth se denomina al protocolo de comunicaciones diseñado especialmente para dispositivos de bajo consumo, con una cobertura baja y basada en transceptores de bajo coste.

Gracias a este protocolo, los dispositivos que lo implementan pueden comunicarse entre ellos cuando se encuentran dentro de su alcance. Las comunicaciones se realizan por radiofrecuencia de forma que los dispositivos no tienen por qué estar alineados, pueden incluso estar en habitaciones separadas si la potencia de transmisión lo permite.

La clasificación de los dispositivos Bluetooth como "Clase 1", "Clase 2" o "Clase 3" es únicamente una referencia de la potencia de trasmisión del

dispositivo, siendo totalmente compatibles los dispositivos de una clase con los de la otra.

Tabla 2.9: Clasificación de los dispositivos bluetooth

Clase	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	Rango (aproximado)
Clase 1	100 mW	20 dBm	~100 metros
Clase 2	2.5 mW	4 dBm	~20 metros
Clase 3	1 mW	0 dBm	~1 metro

Fuente: http://es.wikipedia.org/wiki/Red_por_infrarrojos

Cabe mencionar que en la mayoría de los casos, la cobertura efectiva de un dispositivo de clase 2 se extiende cuando se conecta a un transceptor de clase 1. Esto es así gracias a la mayor sensibilidad y potencia de transmisión del dispositivo de clase 1. Es decir, la mayor potencia de transmisión del dispositivo de clase 1 permite que la señal llegue con energía suficiente hasta el de clase 2. Por otra parte la mayor sensibilidad del dispositivo de clase 1 permite recibir la señal del otro pese a ser más débil.

Tabla 2.10: Ancho de banda de bluetooth

Versión	Ancho de banda
Versión 1.2	1 Mbit/s
Versión 2.0 + EDR	3 Mbit/s
UWB Bluetooth	53 - 480 Mbit/s

Fuente: http://es.wikipedia.org/wiki/Red_por_infrarrojos

Se pueden citar algunas aplicaciones:

- Conexión sin cables entre los celulares y equipos de manos libres y kit para vehículos.
- Red inalámbrica en espacios reducidos donde no sea tan importante un ancho de banda grande.

- Comunicación sin cables entre la computadora y dispositivos de entrada y salida. Mayormente impresora, teclado y mouse.
- Transferencia de ficheros entre dispositivos vía OBEX.
- Transferencia de fichas de contactos, citas y recordatorios entre dispositivos vía OBEX.
- Reemplazo de la tradicional comunicación por cable entre equipos GPS y equipamiento médico.
- Controles remotos (tradicionalmente dominado por el infrarrojo).
- Enviar pequeñas publicidades desde anunciantes a dispositivos con Bluetooth. Un negocio podría enviar publicidad a teléfonos móviles cuyo Bluetooth (los que lo posean) estuviera activado al pasar cerca.
- Las consolas Sony PlayStation 3 y Nintendo Wii incorporan Bluetooth, lo que les permite utilizar mandos inalámbricos.

2.9.7.1.2.2 Especificación y características de Bluetooth

En 1994, Ericsson inició un estudio para investigar la viabilidad de una nueva interfaz de bajo costo y consumo para la interconexión vía radio (eliminando así cables) entre dispositivos como teléfonos móviles y otros accesorios. El estudio partía de un largo proyecto que investigaba unos multicomunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance, llamado *MC link*. Conforme este proyecto avanzaba se fue haciendo claro que éste tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenía como principal virtud que se basaba en un chip de radio.

- Bluetooth v.1.1
- Bluetooth v.1.2
- Bluetooth v.2.0
- Bluetooth v.2.1

La versión 1.2, a diferencia de la 1.1, provee una solución inalámbrica complementaria para co-existir Bluetooth y Wi-Fi en el espectro de los 2.4 GHz, sin interferencia entre ellos.

La versión 1.2 usa la técnica "Adaptive Frequency Hopping (AFH)", que ejecuta una transmisión más eficiente y un cifrado más seguro. Para mejorar las experiencias de los usuarios, la V1.2 ofrece una calidad de voz (Voice Quality - Enhanced Voice Processing) con menor ruido ambiental, y provee una más rápida configuración de la comunicación con los otros dispositivos bluetooth dentro del rango del alcance, como pueden ser PDAs, HIDs (Human Interface Devices), computadoras portátiles, computadoras de escritorio, impresoras y celulares.

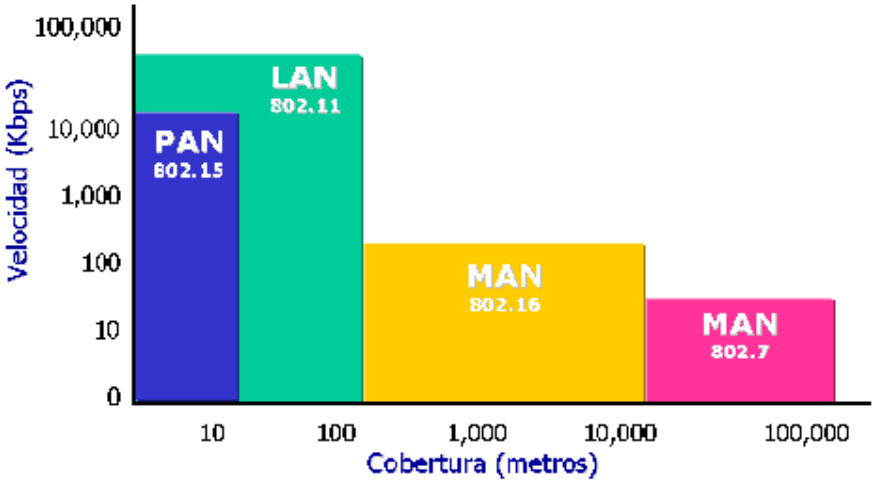
La versión 2.0, creada para ser una especificación separada, principalmente incorpora la técnica "Enhanced Data Rate" (EDR) que le permite mejorar las velocidades de transmisión en hasta 3Mbps a la vez que intenta solucionar algunos errores de la especificación 1.2.

2.9.8 TIPOS DE REDES INALÁMBRICAS

Al igual que las redes tradicionales cableadas vamos a clasificar a las redes inalámbricas en tres categorías.

- Wireless WAN/MAN (Wide Area Network/Metropolitan Area Network)
- Wireless LAN (Local Area Network)
- Wireless PAN (Personal Area Network)

FIGURA 2.17: Comparativa Distancia/Velocidad de tipos de redes



Fuente:http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

En la primera categoría WAN/MAN, se ubicarán a las redes que cubren desde decenas hasta miles de kilómetros. En la segunda categoría LAN, estarán las redes que comprenden de varios metros hasta decenas de metros. Y en la última y nueva categoría PAN, se colocarán a las redes que comprenden desde metros hasta 30 metros.

2.9.8.1 Wireless WAN/MAN (Wide Area Network/Metropolitan Area Network)

Red de computadores que abarca un área geográfica relativamente. Por medio de una WAN Inalámbrica se pueden conectar las diferentes localidades utilizando conexiones satelitales, o por antenas de radio microondas. Estas redes son mucho más flexibles, económicas y fáciles de instalar.

En sí la forma más común de implantación de una red WAN es por medio de Satélites, los cuales enlazan una o más estaciones bases, para la emisión y recepción, conocidas como estaciones terrestres. Los satélites utilizan una banda de frecuencias para recibir la información, luego amplifican y repiten la señal para enviarla en otra frecuencia.

Para que la comunicación satelital sea efectiva generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para

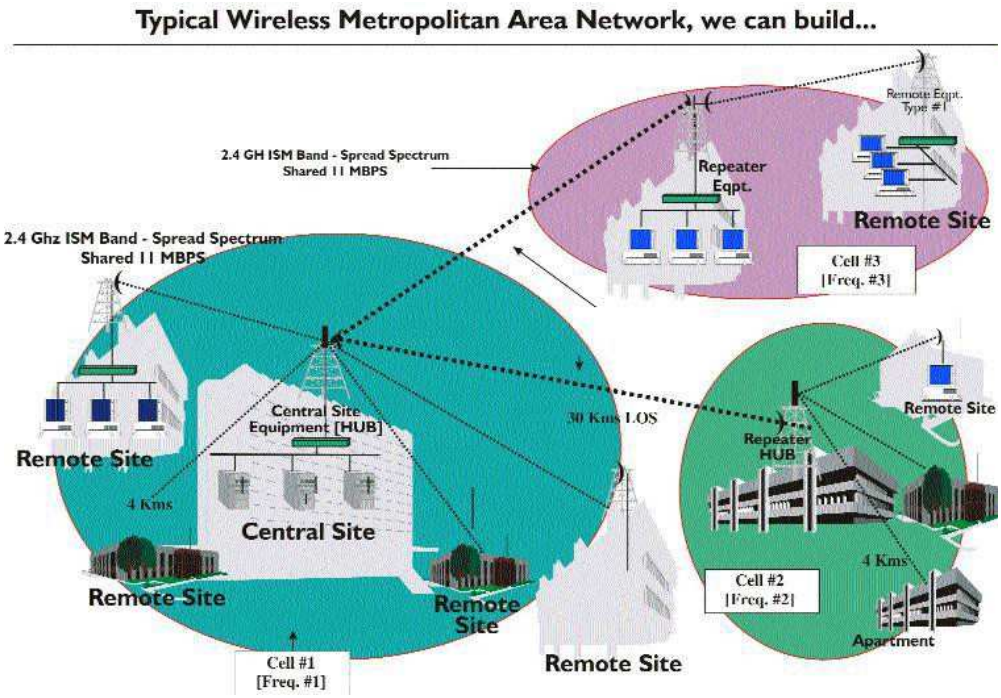
mantenerse estacionario, el satélite debe tener un periodo de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra a una altura de 35,784 Km.

Las redes Wi-Fi permiten la construcción de microceldas, áreas de cobertura de un radio inferior a pocas centenas de metros. Pero, ¿cómo asociar microceldas próximas para constituir redes inalámbricas de mayor cobertura? El procedimiento empleado es la interconexión de cada una a las redes públicas cableadas de operadores. Este modelo, habitual en las grandes ciudades, es de difícil implantación en zonas rurales y dispersas, así como liga el despliegue de una red de cobertura amplia (WAN) inalámbrica a las habitualmente caras redes fijas. [49]

Considerando esta limitación, el IEEE ha establecido un grupo de trabajo, el IEEE 802.16, para proponer una tecnología inalámbrica de largo alcance para redes WAN inalámbricas. El resultado ha sido el desarrollo de un nuevo estándar, cuyas características más destacables son una importante compatibilidad técnica con la serie 802.11 (lo que facilitará la inmediata salida de productos al mercado), y el permitir flujos binarios de hasta 70 Mbps con rangos de cobertura cercanos a los 50 Kms. Se orienta hacia un uso eficiente de 45 frecuencias en las bandas licenciadas entre 10 y 66 GHz (también está trabajando en las no licenciadas entre 2 y 11 GHz) y define una capa de control de acceso al medio (MAC) que soporta especificaciones de múltiples capas físicas según la frecuencia de uso. Emulando el éxito que el consorcio Wi-Fi Alliance tiene en la homologación de equipos sobre el 802.11, ha nacido WiMAX, con el objetivo de promover el uso e interoperabilidad de equipos 802.16a. Rápidamente ha tenido el apoyo activo de destacados actores del sector, entre ellos Intel, Proxim y Fujitsu.

[49] http://www.coit.es/pub/ficheros/informewificoit_definitivo_2464518b.pdf

Figura 2.18: Wireless WAN/MAN



Fuente: http://www.networkmagazineindia.com/200204/net200204_16.jpg

2.9.8.2 Wireless LAN (Local Area Network).

Una red de área local o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, ...).

Permiten conectar una red de computadores en una localidad geográfica, de manera inalámbrica para compartir archivos, servicios, impresoras, y otros recursos. Usualmente utilizan señales de radio, las cuales son captadas por PC-Cards, o tarjetas PCMCIA conectadas a laptops, o a slots PCI para PCMCIA de PCs de escritorio. Estas redes a grosso modo, soportan generalmente tasas de transmisión entre los 11Mbps y 54Mbps (mega bits por segundo) y tienen un rango de entre 30 a 300 metros, con señales capaces de atravesar paredes.

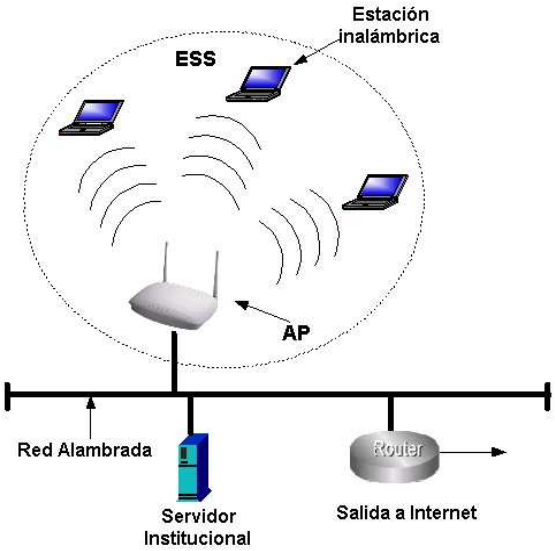
Las Wireless LANs ofrecen muchas ventajas sobre las LANs Ethernet convencionales, tales son, movilidad, flexibilidad, escalabilidad, velocidad,

simplicidad, y costos reducidos de instalación. Son una solución para edificios que por su arquitectura, o su valor histórico, no pueden ser perforados para instalar cableado estructurado.

Una red LAN inalámbrica se compone de dos elementos principales:

- Un cliente habilitado en una LAN inalámbrica
- Un Punto de Acceso (access point)[50]

Figura 2.19: ENLACE WLAN (Wireless Local Area Network)



Fuente: http://ccomputo.itam.mx/redes/servicios/wlan/802_11b.htm

Un cliente habilitado en una LAN inalámbrica es un computador portátil, una impresora, un PDA o cualquier otro dispositivo capaz de comunicarse a través de una red LAN inalámbrica. Muchos de estos dispositivos, especialmente algunos, tienen las capacidades de conectividad inalámbricas incluidas en ellos mismos de fábrica.

Los dispositivos que no están listos para conectarse a una red inalámbrica pueden convertirse rápidamente, agregándoles una tarjeta de red inalámbrica. Una tarjeta de red inalámbrica es una tarjeta que se le coloca al portátil, o a un equipo de escritorio usando un adaptador PCI, o uno con conector USB

[50] http://es.geocities.com/alfredo061/Redes.html

(Universal Serial Bus). Las impresoras y PDA´s usan tarjetas iguales o similares para comunicarse inalámbrica mente.[51]

El Access Point es un dispositivo que actúa como “puente” entre la red cableada y la red inalámbrica. Un access point permite que los dispositivos habilitados para trabajar de forma inalámbrica se comuniquen con una red cableada, dando la habilidad de mover las computadoras libremente dentro de la oficina y accedan desde cualquier sitio a la red LAN, el correo electrónico, internet, archivos o impresoras, tan lejos como la señal del Access point lo permita.

El estándar que hace posible hacer una red LAN inalámbrica es el 802.11b. Las redes LAN son comunes en oficinas, las usan para transferir archivos, compartir impresoras y especialmente para dar acceso a Internet. La ventaja de las redes inalámbricas parece obvia cuando se piensa en la dificultad y el alto costo que implica cablear y usar Ethernet en su casa o en su pequeña oficina. Un usuario puede cargar su equipo portátil para reuniones y compartir archivos, impresoras y acceso a internet cuando está conectado a la red LAN. Normalmente con una red inalámbrica un usuario se puede alejar entre 150 y 200 pies del access point y todavía tener acceso a la red. Para hacer que esta proposición tenga éxito, los precios de las redes inalámbricas se han reducido considerablemente, haciendo que las redes cableadas sean en la mayoría de los casos más costosas, teniendo en cuenta que éstas necesitan de una obra civil y muchos materiales como canaletas, cable, conectores, cajas, etc.. Además que se debe tener en cuenta que al momento de cambiar de distribución la oficina o simplemente abandonarla para moverse a otro sitio, las redes cableadas prácticamente se pierden, teniendo que volver a incurrir en gastos para construir la nueva red.

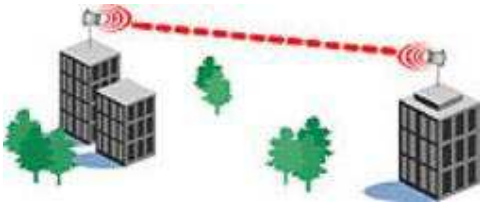
WLAN ofrece algunos modos de conexión:

[51] http://es.geocities.com/alfredo061/Redes.html

2.9.8.2.1 CONEXIÓN PUNTO A PUNTO

Esta opción se conoce como punto (nodo) a punto, es decir se trasmite de un edificio a otro.

Figura 2.20: Conexión punto a punto



Fuente: http://www.cez.com.pe/Wireless/Wireless.htm

2.9.8.2.2 CONEXIÓN PUNTO MULTIPUNTO

Esta opción se conoce como punto multipunto, en donde hay un equipo base o central y todos trasmiten a él, sería la solución para enlazar una matriz y sucursales. Bajo la legislación vigente en nuestro país esta solución solo se pueden implementar en instalaciones internas mas no en instalaciones externas.

Figura 2.21: Conexión punto a multipunto

Fuente: http://www.cez.com.pe/Wireless/Wireless.htm

2.9.8.2.3 CONEXIÓN DE REJILLA O MALLA

Esta última configuración se le conoce como rejilla o malla en donde cada punto o nodo puede trasmitir a cualquier otro que este disponible o accesible. Esta configuración es muy flexible ya que permite un nodo trasmitir a otro vía cualquier otro nodo.

Figura 2.22: Conexión tipo malla

Fuente: http://www.cez.com.pe/Wireless/Wireless.htm

2.9.8.2.4 Wireless PAN (Personal Area Network)

En nuestro país las Wireless PAN (Personal Área Network) permiten interconectar dispositivos electrónicos dentro de un rango de pocos metros, para comunicar y sincronizar información. Por lo general se utilizan en nuestro país por medio del servicio Home – RF.[52]

Es un concepto relativamente nuevo, una PAN es una red *ad hoc* (temporal) creada para dispositivos habilitados con tecnología Bluetooth y se refiere a redes confinadas en un corto rango. Si usted tiene un conjunto de equipos habilitados Bluetooth en su cubículo, tiene una red PAN inalámbrica. Si su computadora portátil y su asistente personal digital (PDA) están habilitados con Bluetooth usted tiene una red inalámbrica personal que puede usar en el cuarto de su Hotel mientras está de viaje por ejemplo.[53]

Todo lo que usted necesita para crear una PAN inalámbrica es caminar dentro de una habitación con un dispositivo compatible con Bluetooth y este se conectará con otros dispositivos Bluetooth en esa habitación. Esta simplicidad hace a Bluetooth perfecta para usuarios que no son técnicos pero que tienen la necesidad de tener sus computadoras y dispositivos conectados fácilmente.

Las redes PAN inalámbricas son especialmente útiles para hacer sincronización de portátiles, PDAs (como el iPaq Pocket PC) y teléfonos celulares. Otras aplicaciones donde las PANs son beneficiosas incluyen:

[52] http://es.geocities.com/yulaidysramirez/tempresa/t1/redesi.html
[53] http://es.geocities.com/alfredo061/Redes.html

- Usar su PDA para controlar sus presentaciones en el portátil
- Compartir datos y archivos entre portátiles equipados con Bluetooth
- Bajar fotos de cámaras digitales a portátiles o impresoras
- Configurar un teléfono celular para conectarlo al portátil
- Usar un teléfono celular para conectarse a la red corporativa, de la misma forma que se hace hoy usando un módem.

Figura 2.23: Wireless PAN (Personal Area Network)

Fuente: http://www.gmtvaritec.com/index.php?mod=productos&idL=2&niv=2&id=3

2.9.9 TOPOLOGÍAS DE UNA RED INALÁMBRICA

La tecnología WiFi (también llamada 802.11) es la tecnología de redes de área local inalámbrica más usada. Permite conectar equipos que se encuentren a distancias de aproximadamente 90 metros (300 pies) con una velocidad compartida que oscila entre una docena de Megabits por segundo (Mbps) a varias docenas de Mbps.

La tecnología WiFi ofrece dos modos operativos:

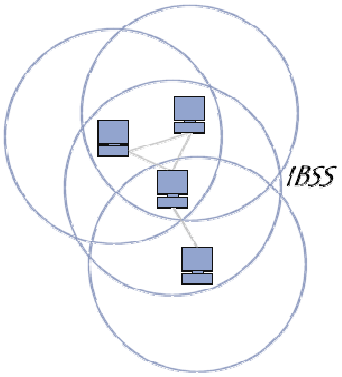
- **"Ad hoc"**, un modo de equipo a equipo que permite conectar dos equipos que cuenten con adaptadores inalámbricos;
- **"Infraestructura"**, un modo que permite conectar equipos a una red conectada por cable usando un dispositivo llamado "**punto de acceso**", cuya abreviatura es **AP**.

2.9.9.1 Redes Ad-Hoc

Las redes Ad-Hoc son la última frontera en comunicación inalámbrica. Esta tecnología permite a los nodos de las redes comunicarse directamente entre cada usuario usando transmisores inalámbricos (posiblemente a través de caminos multisaltos) sin la necesidad de mezclar infraestructura. Se distingue claramente las propiedades de las redes Ad-Hoc con respecto a las tradicionales redes inalámbricas tales como las redes celulares y las redes inalámbricas LAN en sus nodos (por ejemplo, los usuarios de teléfonos móviles) para comunicarse entre usuarios deben utilizar una estación base (antena de radio alámbrica).[54]

En el modo ad hoc los equipos cliente inalámbrico se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

Figura 2.24: Red Ad-Hoc



Fuente: http://es.kioskea.net/wifi/wifimodes.php3

54 http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/Oct06Marzo07/ComInalam/TRabajos/TRABAJO3/G1/PROYECTO%203%20-%20GRUPO%201.doc

La configuración que forman las estaciones se llama conjunto de servicio básico independiente o IBSS. [55]

Un IBSS es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Por eso, el IBSS crea una red temporal que le permite a la gente que esté en la misma sala intercambiar datos. Se identifica a través de un SSID de la misma manera en que lo hace un ESS en el modo infraestructura.

En una red ad hoc, el rango del BSS independiente está determinado por el rango de cada estación. Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse, ni siquiera cuando puedan "ver" otras estaciones. A diferencia del modo infraestructura, el modo ad hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra. Entonces, por definición, un IBSS es una red inalámbrica restringida.

Se espera que las redes Ad-Hoc revolucionen la comunicación inalámbrica en los siguientes próximos años complementando los más tradicionales modelos (Internet, redes celulares, comunicación satelital), estas redes pueden ser consideradas como la contraparte tecnológica de la computación “ubicua”. Explotando la tecnología inalámbrica Ad-Hoc, varios dispositivos portátiles (teléfonos celulares, PDA´s, laptops, beepers y muchos más) y equipos fijos (estaciones base, puntos de acceso de Internet inalámbricos, etc.) pueden ser conectadas juntas formando un conjunto, una red “global” o “ubicua”.

[55] http://es.kioskea.net/wifi/wifimodes.php3

2.9.10 DISPOSITIVOS PARA LA CONEXIÓN DE UNA RED INALÁMBRICA

- Un ***access point*** o punto de acceso (mejor conocido como AP).
- Una **interface de red inalámbrica** (o simplemente tarjeta de red inalámbrica, o wireless NIC).
- ***Antenas*** con sus respectivos componentes (Pigtails, PoE)

2.9.10.1 ACCESS POINT

O punto de acceso, es el dispositivo de red que enlaza todas las terminales en una sección inalámbrica de tu LAN y además, hace la función de conectar por cable toda esa información a un MODEM o ruteador que luego transfiere la información a una central de datos de Internet. Es una interfaz necesaria entre una red cableada y una red inalámbrica, o sea, traduce de lo alámbrico a lo inalámbrico y viceversa.

Figura 2.25: Access Point D-Link DWL-G700AP

Fuente: http://guia.mercadolibre.com.ve/wifi-wireless-que-es-redes-inalambricas-tutorial-8825-VGP

2.9.10.2 TARJETA DE RED INALÁMBRICA

Este dispositivo se instala en cada terminal, es decir, en este caso sería en cada computadora que se desee tener acceso a la red inalámbrica. De la misma manera que un concentrador de red alámbrica se conecta a sus clientes con un cable, estas tarjetas de red, envían sus peticiones de forma inalámbrica (electromagnética) y así negocian los parámetros de la conexión automáticamente. Estas tarjetas de red, pueden ser de al menos tres tipos:[56]

- **Interfaz de red inalámbrica USB**.- Es la más sencilla de instalar, pues ni siquiera tienes que abrir el computador. Además de que son portátiles, simplemente lo enchufas a una terminal USB libre que quede en el PC y de inmediato lo reconocerá tu sistema operativo. En algunos casos, se tendrá que usar el disco de instalación que viene con el dispositivo, pero aun esto es muy fácil de realizar, solo se sigue los sencillos pasos que te indique el mismo proceso de instalación.

Figura 2.26: Tarjeta de red inalámbrica

Fuente:http://images.google.com.ec/images?gbv=2&ndsp=20&hl=es&q=tarjeta+inalambrica+USB&start=60&sa=N

- **Interfaz de red inalámbrica PCI**.-En este caso, el dispositivo es una tarjeta que hay que instalar en el interior de la PC. Sin embargo, tampoco es difícil., Se busca un slot (puerto) PCI que no esté ocupado, y ahí se inserta la tarjeta de red viendo que coincidan los conectores de cobre en las ranuras correspondientes y sin forzarla mucho. Cuando inicie el sistema operativo, te dirá que ha detectado tu tarjeta de red y en la mayoría de los casos instalará automáticamente los controladores

[56] http://guia.mercadolibre.com.mx/componentes-necesarios-establecer-una-red-lan-inalambrica-22594-VGP

para que funcione correctamente; pero, también en algunos casos puede ser que te solicite insertar el disco que venía con el dispositivo.[57]

Figura 2.27: Tarjeta de red inalámbrica

Fuente: http://guia.mercadolibre.com.ve/instalar-una-red-inalambrica-wi-fi-paso-12964-VGP

- **Interfaz de red inalámbrica PCMCIA**.- Destinada a ordenadores portátiles, se conecta por la ranura de la tarjeta de red.

Figura 2.28: Tarjeta de red para laptop

Fuente:http://images.google.com.ec/images?gbv=2&hl=es&q=tarjeta+inalambrica+PCMCIA&start=20&sa=N&ndsp=20

2.9.10.3 ANTENAS Y ACCESORIOS

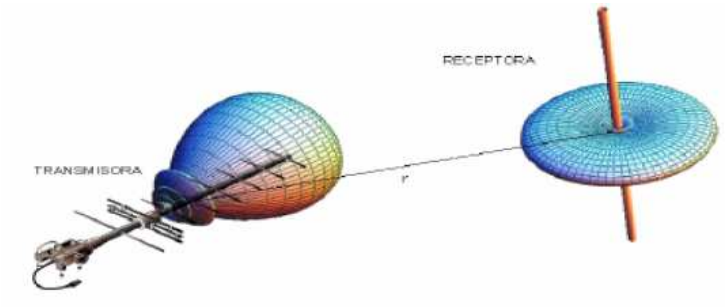
Conjunto de conductores debidamente asociados, que se emplea tanto para la recepción como para la transmisión de ondas electromagnéticas, que comprenden los rayos gamma, los rayos X, la luz visible y las ondas de radio.[58]

Cuando hablamos de antenas nos referimos por igual de antenas para emitir que para recibir. La antena propiamente tiene las mismas características para

[57] http://guia.mercadolibre.com.mx/componentes-necesarios-establecer-una-red-lan-inalambrica-22594-VGP
[58] http://www.monografias.com/trabajos10/coin/coin.shtml

ambas tareas. Así que la misma precisión que tiene para enviar en una determinada dirección es la que tiene para recibir en esa dirección.[59]

Figura 2.29: Antenas



Fuente:http://www.astronomos.cl/conocimientos/avanzado/Presentacion-antenas.pdf

Tenemos dos factores que atenúan la señal a medida que avanza por el aire.
La atenuación del aire no es muy importante, ya que el aire es bastante transparente para frecuencias de microondas como las que usamos para Wireless.

La atenuación que sí es realmente importante es la dispersión de la señal debido a la forma de transmisión. La intensidad de señal se calcula en intensidad de campo eléctrico por metro cuadrado. Como la señal sale de forma radial desde la antena hacia todas las direcciones, así si enviamos un vatio de potencia ésta se reparte en la esfera alrededor de la antena, a medida que la señal se va alejando de la antena la esfera crece y la misma potencia se reparte en esta esfera mayor, así la intensidad de la señal por metro cuadrado ha bajado. Para hacernos una idea la intensidad de la señal disminuye a razón del cuadrado de la distancia ($1/r^2$ donde r es la distancia a la antena).

Existen algunos accesorios que sirven para la conexión de un Access Point a una antena por ejemplo:

- Poe
- Pigtail

[59] http://80.24.102.10/wireless/antenas/Conceptos_basicos_sobre_antenas.pdf

2.9.10.3.1 PoE (Power over Ethernet)

Es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red ethernet. PoE se rige según el estándar IEEE 802.3af y abre grandes posibilidades a la hora de dar alimentación a dispositivos tales como cámaras de seguridad o puntos de acceso inalámbricos.[60]

Actualmente existen en el mercado varios dispositivos de red como switches o hubs que soportan esta tecnología. Para implementar PoE en una red que no se dispone de dispositivos que la soporten directamente se usa una unidad base (con conectores RJ45 de entrada y de salida) con un adaptador de alimentación para recoger la electricidad y una unidad terminal (también con conectores RJ45) con un cable de alimentación para que el dispositivo final obtenga la energía necesaria para su funcionamiento.

Figura 2.30: Dispositivo POE Comercial

Fuente: http://www.zero13wireless.net/foro/showthread.php?t=2693

2.9.10.3.2 Ventajas que tiene un Sistema de alimentación POE

- *PoE es una fuente de alimentación inteligente.-* El equipo de suministro eléctrico integrado en PoE es capaz de proporcionar un alto nivel de gestión de sistemas empleando los protocolos de gestión de sistemas existentes, tales como el Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol). Esto permite, por ejemplo, apagar la alimentación centralmente a través de la red para su mantenimiento.
- *PoE simplifica y abarata la creación de un suministro eléctrico altamente robusto para los sistemas de vigilancia IP.-* La centralización de la

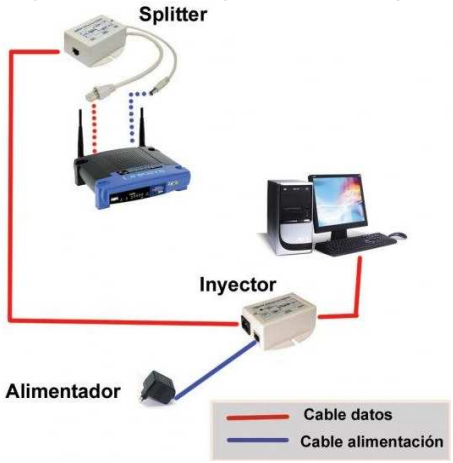
[60] http://www.zero13wireless.net/foro/showthread.php?t=2693

alimentación a través de concentradores (*hubs*) PoE (a menudo llamados *Mid-spans*) también significa que los sistemas basados en PoE se pueden enchufar al sistema de alimentación ininterrumpida (SAI) central, que ya se emplea en la mayor parte de las redes informáticas formadas por más de uno o dos PC. Esto asegura que cualquier corte de alimentación no afectará a la integridad del sistema de vigilancia IP.[61]

- *Los concentradores PoE o mid-spans también permiten a los encargados de seguridad apagar o reiniciar los dispositivos a distancia.-* El sistema PoE es capaz de detectar los dispositivos de red averiados y permitir a los encargados de seguridad reiniciarlos pulsando un botón. De este modo se pueden aislar fácilmente de la corriente los dispositivos que se están sustituyendo, instalar un nuevo dispositivo y conectar de nuevo la alimentación.
- *La centralización del control de la fuente de alimentación también elimina la vulnerabilidad de la seguridad.-* Creada tan a menudo por la situación en la que alguien que lleva a cabo un servicio, tal como una tarea de limpieza o construcción, puede necesitar la utilización de un punto de alimentación utilizado por una cámara particular.
- *PoE dificulta enormemente cortar o destrozar el cableado.-* Generalmente el cableado se encuentra unido a bandejas en los huecos del techo o detrás de conductos de plástico de muy difícil acceso. Cualquier corte de estos cables resultará obvio al momento para quien pase por el lugar y, por supuesto, para los usuarios de los ordenadores que serán incapaces de proseguir con su trabajo.

[61] http://www.zero13wireless.net/foro/showthread.php?t=2693

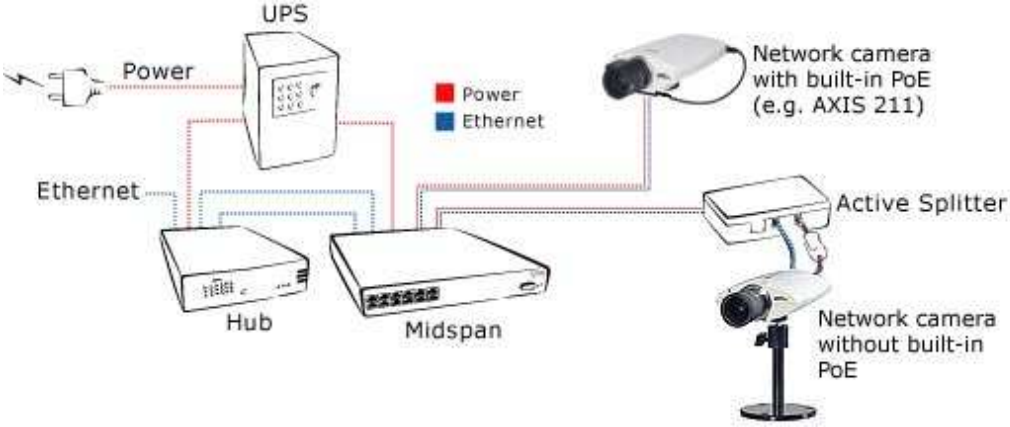
Figura 2.31: Esquema PoE típico



Fuente: http://www.zero13wireless.net/foro/showthread.php?t=2693

También hay otras maneras en las cuales se puede utilizar el Sistema de Alimentación POE añadiendo dispositivos como un SAI (Sistema de Alimentación Ininterrumpida - Baterías) para asegurar que aunque se vaya la luz de general, seguir alimentación dicho dispositivo.

Figura 2.32: Otra forma de conexión de un PoE



Fuente: http://www.zero13wireless.net/foro/showthread.php?t=2693

2.9.10.3.3 PIGTAIL

Es un cable pequeño, que lleva dos conectores, su función es la de adaptar la antena o el cable que vaya a ésta con el adaptador Wifi o Punto de acceso.
Como las pérdidas por atenuación de la señal dentro del cable en la frecuencia de 2.4GHz son muy altas, se procurará elegir el de muy corta longitud posible y realizado con el cable de mayor calidad que se disponga.
Dependiendo del conector que tenga la antena que se va a utilizar y del conector que tenga el aparato wireless al que se quiera conectar se opta entre los diversos tipos de pigtails.

2.9.10.3.4 TIPOS DE ANTENAS

2.9.10.3.4.1 Antenas Omnidireccionales

Definimos una antena omnidireccional como aquella que es capaz de radiar energía prácticamente en todas direcciones. El uso habitual hace que una antena omnidireccional no emita exactamente en todas direcciones, sino que tiene una zona donde irradia energía por igual (por ejemplo el plano horizontal).[62]

El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

Pueden clasificarse también en: Dipolo, Monopolo, Colineares, Guia ondas ranuradas

[62] http://80.24.102.10/wireless/antenas/Conceptos_basicos_sobre_antenas.pdf

2.9.10.3.4.1.1 Dipolo (vertical):

Tiene las siguientes características:

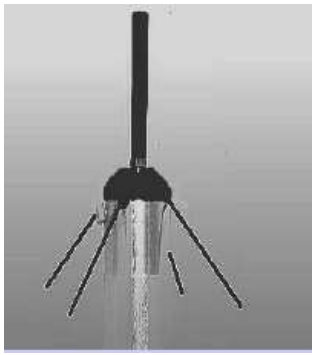
* Antena fundamental
* Dos conductores de cuarto de onda
* Ganancia baja: 2.2 dBi
* Angulo de radiación ancho

2.9.10.3.4.1.2 Monopolo vertical de cuarto de onda:

Tiene las siguientes características:

* Básicamente igual al dipolo
* Se sustituye un conductor por un plano de tierra
* Ganancia baja: 0-2 dBi

Figura 2.33: Antena Monopolo



Fuente: http://www.e-oss.net/portuwireless/taller-nodos/antenas.pdf

2.9.10.3.4.1.3 Colineares

* Varios monopolos o dipolos verticales alimentados en fase.
* Ganancia moderada - elevada: 5 - 12 dBi
* Ángulo de radiación medio

2.9.10.3.4.1.4 Guía ondas ranuradas

* Cavidad (tubo) metálico ranurado
* Ganancia elevada: 12-15 dBi
* Ángulo de radiación estrecho

2.9.10.3.4.2 Antenas direccionales

Las antenas direccionales son aquellas que han sido concebidas y construidas para favorecer que la mayor parte de la energía sea radiada en una dirección en concreto. Puede darse el caso en que se desee emitir en varias direcciones, pero siempre estaremos hablando de un número de direcciones determinado donde se encontrarán el lóbulo principal y los secundarios.[63]

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.[64]

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

Con las antenas direccionales descubrimos el término de lóbulo principal, se trata de la dirección donde se proyectará la mayor parte de la energía. Como es imposible hacer una antena que radie en una sola dirección nos interesará saber qué rango de direcciones (o abertura) recibirá el mayor porcentaje de energía. Nos interesará que el lóbulo principal sea lo más estrecho posible, así ganamos en direccionalidad, pero esto repercute directamente en el coste económico de la antena.[65]

Pueden clasificarse también en: Dipolo (horizontal), Yagi, Panel o Patch, Guia-ondas

---

[63] http://80.24.102.10/wireless/antenas/Conceptos_basicos_sobre_antenas.pdf
[64] http://www.34t.com/Unique/wiFiAntenas.asp
[65] http://80.24.102.10/wireless/antenas/Conceptos_basicos_sobre_antenas.pdf

2.9.10.3.4.2.1 Dipolo (horizontal):

* Ganancia baja: 2.2dBi
* Directividad baja
* Amplio ángulo de radiación

2.9.10.3.4.2.2 Uda-Yagi: sucesión de dipolos

* Sucesión de dipolos dispuestos en paralelo. La señal se acople de uno a otro, radiándose de nuevo cada vez.
* Ganancia elevada: 8-15 dBi
* Alta directividad
* Ángulo de radiación medio

Figura 2.34: Antena Direccional

Fuente: http://www.e-oss.net/portuwireless/taller-nodos/antenas.pdf

2.9.10.3.4.2.3 Panel o 'Patch Antenna'

* Panel o parche metálico radiante sobre un plano de tierra metálico. Normalmente planas, en encapsulado de PVC.
* Ganancia media-elevada: 5-20 dBi
* Directividad moderada
* Ángulo de radiación medio

Figura 2.35: Antena Direccional

Fuente: http://www.e-oss.net/portuwireless/taller-nodos/antenas.pdf

2.9.10.3.4.2.4 Guía-ondas

* Cavidad o Tubo metálico con un monopolo que introduce las ondas
* Ganancia media-alta: 5-15 dBi
* Directividad alta
* Ángulo de radiación medio-bajo

2.9.10.3.5 PARÁMETROS DE UNA ANTENA

2.9.10.3.5.1 Resistencia de radiación

Debido a la radiación en las antenas se presenta pérdida de potencia. Por ello se ha establecido un parámetro denominado resistencia de radiación Rr, cuyo valor se puede definir como el valor de una resistencia típica en la cual, al circular la misma corriente que circula en la antena, disipará la misma cantidad de potencia.[66]

2.9.10.3.5.2 Eficiencia de una antena

Se conoce con el nombre de eficiencia de una antena (rendimiento) a la relación existente entre la potencia radiada y la potencia entregada a la misma.

[66] http://www.monografias.com/trabajos10/coin/coin.shtml

2.9.10.3.5.3 Impedancia de entrada de una antena

En general, la impedancia de entrada de la antena dependerá de la frecuencia, estando formada por una componente activa (Re) y una reactiva (Xe). De esta forma, (Re) se puede asimilar a la resistencia total de la antena en sus terminales de entrada. Generalizando, podemos decir entonces que la impedancia de entrada de la antena es simplemente la relación entre el voltaje de entrada de la antena y la corriente de entrada.

2.9.10.3.5.4 Ganancia de una antena

La ganancia de una antena representa la capacidad que tiene este dispositivo como radiador. Es el parámetro que mejor caracteriza la antena. La forma más simple de esquematizar la ganancia de una antena es comparando la densidad de potencia radiada en la dirección de máxima radiación con el valor medio radiado en todas las direcciones del espacio, ofreciéndose en términos absolutos.

Aquellas antenas que radian por igual en todas las direcciones se llaman isotrópicas y su ganancia es de 1.

Basados en esta definición, se puede hablar de la ganancia como la relación entre la potencia y campo eléctrico producido por la antena (experimental) y la que producirá una antena isotrópica (referencia), la cual radiará con la misma potencia.

2.9.10.3.5.5 Longitud eficaz de la antena

Sobre una antena se inducen corrientes y voltajes. Por tal razón, a la antena receptora se le puede considerar como un generador ideal de voltaje (V), con una impedancia interna que resulta ser igual a la de entrada.[67]

[67] http://www.monografias.com/trabajos10/coin/coin.shtml

2.9.10.3.5.6 Polarización de la antena

La onda electromagnética posee el campo eléctrico vibrando en un plano transversal a la dirección de propagación, pudiendo tener diversas orientaciones sobre el mismo. La polarización de la antena hace referencia a la orientación del campo eléctrico radiado. De esta forma, si un observador en un punto lejano a la antena "visualizara" el campo eléctrico lo podría mirar de las siguientes formas:

Describiendo una elipse. En este caso se dice que la onda esta polarizada elípticamente.

Describiendo una circunferencia (polarización circular).

Polarización horizontal o vertical, *describiendo una línea recta.*

Es importante anotar que, para que una antena "responda" a una onda incidente, tiene que tener la misma polarización que la onda. Por ejemplo, un dipolo vertical responderá a una onda incidente si la polarización de dicha onda es vertical también.

2.9.10.3.5.7 Ancho de haz de una antena

Podemos hablar del ancho de haz de una antena como el espaciamiento angular entre dos puntos determinados de potencia media, ubicándolos con respecto a la posición del lóbulo principal perteneciente al patrón de radiación de la antena.

2.9.10.3.5.8 Ancho de banda de la antena

Se puede describir como los valores de frecuencia para los cuales la antena desarrolla su trabajo de manera correcta. De igual forma, el ancho de banda de una antena depende de las condiciones de los puntos de potencia media.

2.9.10.3.6 FACTORES QUE INFLUYEN LA CLARIDAD DE LA SEÑAL EN UNA ANTENA

La claridad de señal es la clave para la realización de una comunicación Wireless. Algunos de los factores que afectan la claridad son:[68]

2.9.10.3.6.1 Potencia de la señal

Obviamente, una señal fuerte permite una mejor recepción en largas distancias. La normativa en España para el nivel de señal en transmisión Wireless es de 100mW para la frecuencia de 2'4GHz y de 1W para la frecuencia de 5'4GHz.

2.9.10.3.6.2 Distancia

La potencia de la señal de radiofrecuencia (RF) disminuye con la distancia. Además se pueden sumar interferencias no deseadas con lo que se consiguen distancias menores. Como veremos más adelante, la señal puede ser modificada de diferentes formas para adecuarla a la distancia que tenga que recorrer (tipos de antenas).

2.9.10.3.6.3 Interferencias

Los factores atmosféricos, como la nieve, la lluvia o el granizo, pueden interferir en la señal. Es un dato a tener en cuenta cuando se quieren realizar enlaces wireless en exteriores. Normalmente las interferencias de RF son causadas por aparatos que están emitiendo cerca, en la misma banda y mismo canal que nosotros. También se consideran interferencias a las transmisiones wifi que estén en el mismo canal que nuestra señal, por lo que siempre es conveniente utilizar el canal menos utilizado. Incluso otros sistemas de RF como puede ser microondas o cualquier otro sistema también puede interferir y degradar el nivel de nuestra señal.

[68] http://www.wifisafe.com/conceptos_wireless.php

2.9.10.3.6.4 Línea de visión

La señal necesita *visión directa* para realizar bien la comunicación. Si hay obstáculos en la línea de visión, no se podrá realizar la conexión. La transmisión Wifi está sólo es válida para enlaces con visión directa. Aunque en interiores es posible que aprovechando los rebotes de la señal en paredes u otros objetos, pero en *ningún caso se ofrece una garantía de señal al traspasar un objeto* por fino que pueda ser este, se podría conseguir un enlace wireless.

2.9.10.3.6.5 Transmisión de la señal

Las ondas de señal de radio viajan como las vibraciones del agua de una piscina cuando se lanza un objeto. La potencia de la señal disminuye a medida que la señal se aleja de la primera onda.[69]

Una antena direccional refleja la señal en una dirección y crea un foco en forma de cono con gran potencia. La señal no se propagada a partes iguales por todo el foco. Igual que la luz es enfocada con más intensidad con una lupa, la señal de RF es más fuerte con un área más estrecha y central. Nos referimos al área donde la señal es más fuerte como el centro del lóbulo. Siempre siendo más débil en los extremos.

El ancho del haz de la señal de RF depende de cómo la antena forma la señal (tipo de antena) y la distancia de la fuente de la señal. La señal se atenúa gradualmente en el borde del cono y no es aconsejable medir la señal desde el borde. La amplitud del haz (no el nivel de potencia) de señal aumenta con la distancia, si se desea medir la anchura de la señal en metros, no se podrá determinar hasta que no se sepa a qué distancia estará. La potencia de la señal se mide en decibelios (dB). El número de decibelios indica la distancia de la señal respecto a su punto central, es decir el alcance de esta.

Las ondas pueden rebotar en algunos objetos que encuentren por su camino, en este caso las ondas se desfasan con mayor o menor grado en función del material en el que reboten y su ángulo de incisión. Una vez una señal es rebotada/desfasada puede ser recuperada o no en función del desfase de la misma. Normalmente si los desfases son muy pequeños, casi despreciables se puede recuperar la señal. Existen tipos de antenas que emiten con una

[69] http://www.wifisafe.com/conceptos_wireless.php

polarización concreta, horizontal, vertical, circular y la novedad que es multipolaridad que recupera las señales desfasadas. Se ha de resaltar que si se utiliza en un emisor una antena con polarización horizontal, es lógico, que en la recepción se utilice una antena con la misma polarización, ya que en caso contrario no se recuperaría la señal debido al desfase natural que hay entre las dos antenas (90 grados).

2.9.10.3.6.6 Enfocar la señal

Si la distancia de transmisión aumenta, es necesario compensar la distancia seleccionando una antena con una transmisión más enfocada y un foco más estrecho, es decir una antena directiva.

Algunos de los beneficios de utilizar antenas directivas es que al tener un foco más estrecho, las señales interferentes se minimizan a aquellas que pasen y coincidan en el haz de la misma. En casos anteriores, al tener un haz más ancho la posibilidad de encontrar interferencias era superior.

Para conseguir un enlace entre dos puntos, lo más conveniente es que los dos lóbulos principales del emisor y el receptor coincidan en al menos un punto, no es necesario que el lóbulo de cada uno de los extremos este superpuesto con el otro. Pero cuanto más superposición exista entre los lóbulos del emisor y el receptor mejor será la señal en el enlace, por lo que es aconsejable que siempre estén superpuestos al 100%.

Por ejemplo: Para hacer un enlace de 1km, se tendría que poner una antena en el emisor y en el receptor que tengan un alcance de 1km, y no poner dos que tuviesen un alcance de 600 metros que solo coincidirían sus lóbulos en 200 metros.

Cuando se quieren enlazar grandes distancias, incluso una antena muy direccional puede tener un gran cono de cobertura. Por ejemplo, con algunas parabólicas de mucha ganancia se pueden conseguir distancias de hasta 20km aproximadamente, y a estas distancias el haz de la señal habrá abierto o aumentado mucho y se puede ver afectada por interferencias.

2.9.10.3.6.7 Línea de visión

El éxito de un enlace de RF depende de la línea de visión. Una línea de visión sin obstáculos se llama “free space path” (Camino con espacio libre). Sin línea de visión directa, tal y como se ha comentado con anterioridad, no es posible realizar un enlace vía Wifi.

Un obstáculo en la línea de visión del enlace reduce o elimina totalmente la señal. La desviación de la señal al pasar alrededor de un obstáculo se llama difracción. Una reducción de la potencia de la señal es conocida como atenuación.

Si una antena apunta hacia una ventana de cristal, el cristal debido a su coeficiente de difracción atenuará en gran medida la señal. Algunos tipos de cristal reflectante ofrecen un nivel de atenuación. La señal que pasa por una construcción de madera o un bosque también será atenuada. Las hojas mojadas pueden afectar substancialmente en la señal.

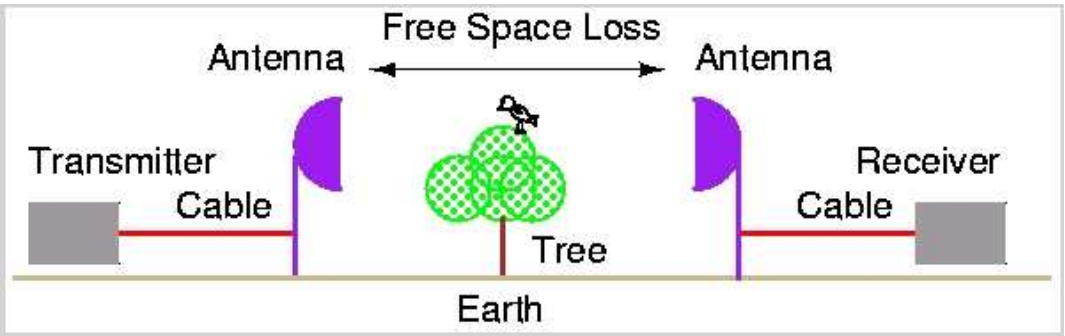
También se ha de comentar, que no siempre es suficiente una visión directa entre dos puntos para realizar un enlace wireless. Ya que ha de tener un campo de visión lo suficientemente ancho como para que pase un cierto porcentaje del haz del emisor y el receptor.

Existen las zonas de Fresnel que definen las anchuras y alturas necesarias para tener una línea de visión suficiente para realizar los enlaces,

Una Zona de Fresnel es un área en donde se difunde una onda luego de ser emitida por una antena. Mientras menos obstáculos haya en esta área, mejor será transmitida la onda. En los sistemas inalámbricos que se manejan en la frecuencia de 2.4 GHz, la zona fresnel es muy importante, pues debe mantenerse limpia de obstáculos que detengan la señal. Por ejemplo, los árboles suelen detener mucho más esas señales que las paredes, por su alto contenido en agua.[70]

[70] http://www.alegsa.com.ar/Dic/zona%20de%20fresnel.php

Figura 2.36: Línea de visión de una antena



Fuente: http://www.zero13wireless.net/foro/showthread.php?t=511

2.9.10.3.6.8 Posición estable de la antena

Para obtener un óptimo rendimiento, se debe ajustar las antenas con la máxima precisión posible. Para asegurar un buen alineamiento de las antenas, es preciso mantenerlas en una posición estable y rígida. Esto es difícil de conseguir en exteriores y sobre todo cuando se utilizan antenas parabólicas de plato rígido montadas en mástiles flexibles, ya que el viento hará mover la antena. Hay que asegurarse que el mástil donde se instala sea rígido. Para instalaciones interiores este fenómeno es despreciable.[71]

2.9.11 SEGURIDAD PARA LAS REDES INALÁMBRICAS

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.[72]

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la

[71] http://www.wifisafe.com/conceptos_wireless.php
[72] http://www.saulo.net/pub/inv/SegWiFi-art.htm

información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

2.9.11.1 MECANISMOS DE SEGURIDAD DE LAS REDES INALÁMBRICAS

Los mecanismos utilizados habitualmente son:

1. CIFRADO.- Cuando el transmisor y receptor no comparten un medio de transporte de datos en común, los datos deben ser descifrados y re cifrados en cada uno de los nodos en el camino al receptor. El cifrado en el nivel de enlace se usa en caso de que no se aplique un protocolo de cifrado de mayor nivel.

El algoritmo de cifrado mejor conocido para la norma IEEE 802.11 es el llamado en ingles Wired Equivalent Privacy (WEP)
Otras alternativas, como el protocolo Wi-Fi Protected Access (WPA), es considerado como standard (WPA2). La nueva norma IEEE 802.11i va a incluir una extensión de WPA, llamada WPA2.

2. AUTENTICACIÓN.- Es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas. Los sistemas que intervienen son:
    - Sistema abierto
    - Clave compartida

2.9.11.1.1 CIFRADO WEP (Wired Equivalent Privacy)

WEP (privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.[73]

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama.

El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

[73] http://www.saulo.net/pub/inv/SegWiFi-art.htm

WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits).

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

Una variante de WEP utilizada en algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autentificación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP. Entre algunas debilidades de WEP tenemos:[74]

- El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP. Este mecanismo de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad).
- WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este

[74] http://www.saulo.net/pub/inv/SegWiFi-art.htm

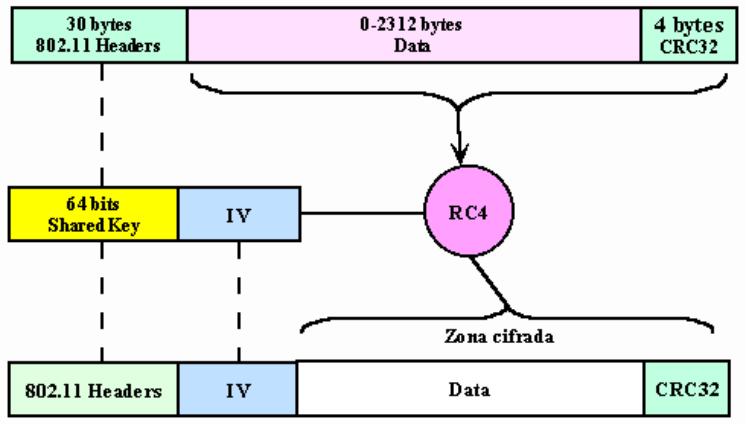
caso tendríamos una autentificación de sistema abierto, es decir, sin autentificación.

2.9.11.1.1.1Modo de funcionamiento de WEP

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un valor de comprobación de integridad (ICV). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

Figura 2.37: Algoritmo de Encriptación WEP



Fuente: http://www.saulo.net/pub/inv/SegWiFi-art.htm

2.9.11.1.2 CIFRADO WPA (Wi-Fi Protected Access)

WPA (Acceso Protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación. WPA incluye las siguientes tecnologías:[75]

[75] http://www.saulo.net/pub/inv/SegWiFi-art.htm

2.9.11.1.2.1 IEEE 802.1X.

Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. Se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

2.9.11.1.2.2 EAP.

Es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).

2.9.11.1.2.3 TKIP

(Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.

2.9.11.1.2.4 MIC

(Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

2.9.11.1.2.5 Mejoras de WPA respecto a WEP

1) Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

2) Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

3) Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

2.9.11.1.2.6 Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

1.- *Con servidor AAA, RADIUS normalmente.* Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

2.- Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.9.11.1.3 CIFRADO WPA2 (IEEE 802.11i)

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits.[76]

Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

[76] http://www.saulo.net/pub/inv/SegWiFi-art.htm

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

2.9.11.1.3.1 Características criptográficas de WPA2

La siguiente tabla muestra la manera en que WPA2 aborda esos puntos débiles.

Tabla 2.11: Como WPA2 aborda el punto débil de WEP

Punto débil de WEP	**Cómo WPA2 aborda el punto**
Vector de inicialización (IV) demasiado corto	En AES CCMP, se reemplazó el IV por un campo Número de paquete y se duplicó su tamaño a 48 bits.
Integridad débil de los datos	El cálculo de suma de comprobación cifrado con WEP se reemplazó por el algoritmo AES CBC-MAC, que está diseñado para proporcionar una sólida integridad de los datos. El algoritmo CBC-MAC calcula un valor de 128 bits y WPA2 utiliza los 64 bits de orden superior como un código de integridad de mensaje (MIC). WPA2 cifra el MIC con el cifrado de modo contador de AES.
Usa la clave principal en lugar de una clave derivada	Al igual que WPA y el Protocolo de integridad de claves temporales (TKIP, Temporal Key Integrity Protocol), AES CCMP usa un conjunto de claves temporales derivadas de una clave principal y otros valores. La clave principal se origina en el proceso de autenticación 802.1X mediante Protocolo de autenticación extensible-Seguridad de la capa de transporte (EAP-TLS) o EAP protegido (PEAP).
No reasigna claves	AES CCMP reasigna claves automáticamente para crear nuevos conjuntos de claves temporales.
No ofrece protección contra la reproducción	AES CCMP usa el campo Número de paquete como contador para ofrecer protección contra la reproducción.

Fuente: http://www.microsoft.com/spain/technet/recursos/articulos/cg0805.mspx#top

2.9.11.1.3.1 Claves temporales de WPA2

A diferencia de WEP, que utiliza una única clave para el cifrado de datos de difusión única y generalmente una clave separada para el cifrado de datos de difusión y de multidifusión, WPA2 usa un conjunto de cuatro claves diferentes para cada par de clientes inalámbricos-AP inalámbricos (conocidas como las claves temporales de par o "pairwise") y un conjunto de dos claves diferentes para el tráfico de difusión y de multidifusión.[77]

El conjunto de claves de par utilizado para los datos de difusión única y los mensajes de clave EAPOL (EAP sobre LAN) consta de lo siguiente:

• *Clave de cifrado de datos*.- Una clave de 128 bits utilizada para cifrar tramas de difusión única.

• *Clave de integridad de datos*.- Una clave de 128 bits utilizada para calcular el MIC de tramas de difusión única.

• *Clave de cifrado de clave EAPOL.*- Una clave de 128 bits utilizada para cifrar mensajes de clave EAPOL.

• *Clave de integridad de clave EAPOL.*- Una clave de 128 bits utilizada para calcular el MIC de mensajes de clave EAPOL.

WPA2 deriva las claves temporales de par mediante un proceso de negociación de 4 vías, que es el mismo que el del WPA

Para cifrar una trama de datos de difusión única, WPA2 utiliza el siguiente proceso:

1. Se ingresa el bloque inicial, el encabezado MAC 802.11, el encabezado CCMP, la longitud de los datos y los campos de relleno en el algoritmo CBC-MAC con la clave de integridad de datos para generar el MIC.[78]

---

[77] http://www.microsoft.com/spain/technet/recursos/articulos/cg0805.mspx#top

[78] http://www.microsoft.com/spain/technet/recursos/articulos/cg0805.mspx#top

2. Se ingresa el valor inicial del contador y la combinación de los datos con el MIC calculado en el algoritmo de cifrado de modo contador de AES con la clave de cifrado de datos para generar el MIC y los datos cifrados.

3. Se agrega el encabezado CCMP que contiene el Número de paquete a la parte cifrada de la carga 802.11, y se encapsula el resultado con el encabezado y el finalizador 802.11.

Para descifrar una trama de datos de difusión única y examinar la integridad de los datos, WPA2 utiliza el siguiente proceso:

1. Se determina el valor inicial del contador a partir de los valores de los encabezados 802.11 y CCMP.

2. Se ingresa el valor inicial del contador y la parte cifrada de la carga 802.11 en el algoritmo de descifrado de modo contador de AES con la clave de cifrado de datos para generar el MIC y los datos descifrados. Para el descifrado, el modo contador de AES realiza una XOR del valor cifrado del contador con el bloque de datos cifrados, lo que genera el bloque de datos descifrados.

3. Se ingresa el bloque inicial, el encabezado MAC 802.11, el encabezado CCMP, la longitud de los datos y los campos de relleno en el algoritmo AES CBC-MAC con la clave de integridad de datos para calcular el MIC.

4. Se compara el valor calculado del MIC con el valor del MIC descifrado. Si los valores del MIC no coinciden, WPA2 descarta los datos silenciosamente. Si los valores del MIC coinciden, WPA2 transfiere los datos a las capas superiores de las redes para su procesamiento.

2.9.11.1.4 AUTENTICACIÓN POR SISTEMA ABIERTO

Todos los usuarios tienen permiso para acceder a la WLAN. En la autenticación de Sistema Abierto, el cliente WLAN no se tiene que identificar en el Punto de Acceso durante la autenticación. Así, cualquier cliente, independientemente de su clave WEP, puede verificarse en el Punto de Acceso y luego intentar conectarse. En efecto, la no autenticación (en el sentido estricto del término) ocurre. Después de que la autenticación y la asociación, el sistema WEP pueden ser usado para cifrar los paquetes de datos. En este punto, el cliente tiene que tener las claves correctas.[79]

Cualquier estación inalámbrica puede solicitar la autenticación. La estación que necesita autenticarse con otra estación inalámbrica envía una solicitud de gestión de autenticación que contiene la identidad de la estación emisora. La estación receptora o el punto de acceso otorgan cualquier solicitud de autenticación. La autenticación abierta permite el acceso a la red a cualquier dispositivo. Si no se activa la codificación en la red, cualquier dispositivo que conozca el Identificador de conjunto de servicios (SSID) del punto de acceso puede obtener acceso a la red.[80]

El sistema abierto es obligatorio y consta de dos pasos.

- El adaptador de red inicia el proceso enviando una trama de solicitud de autenticación al punto de acceso.
- El punto de acceso responde con una trama de autenticación que indica si acepta o rechaza la autenticación en el campo de código de estado de la trama.

[79] http://es.wikipedia.org/wiki/WEP
[80] http://support.dell.com/support/edocs/network/P94583/sp/security.htm#Open

2.9.11.1.5 AUTENTICACIÓN MEDIANTE CLAVE COMPARTIDA

Controla el acceso a la WLAN y evita accesos no autorizados a la red. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN.

Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el *desafío (challenge)*. La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.[81]

La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes.

Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red.

Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más

[81] http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml

usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

La autenticación de clave compartida es opcional y básicamente comprueba si la clave WEP es la correcta. El hecho de ser opcional para el protocolo no impide que esté en la práctica totalidad de los adaptadores y puntos de acceso. Este proceso consta de cuatro pasos: [82]

- El adaptador de red inicia el proceso enviando una trama de solicitud de autenticación al punto de acceso.
- El punto de acceso responde con una trama de autenticación que contiene un texto de desafío.
- El adaptador de red utiliza su clave WEP para cifrar el texto de desafío y lo devuelve al punto de acceso en otra trama de autenticación.
- El punto de acceso descifra el valor cifrado, lo compara con el original y responde con una trama de autenticación que indica si acepta o rechaza la autenticación. Si coinciden el valor original y el de la respuesta el punto de acceso supone que el solicitante tiene la clave correcta. [83]

2.10 CÁMARA DE SEGURIDAD IP

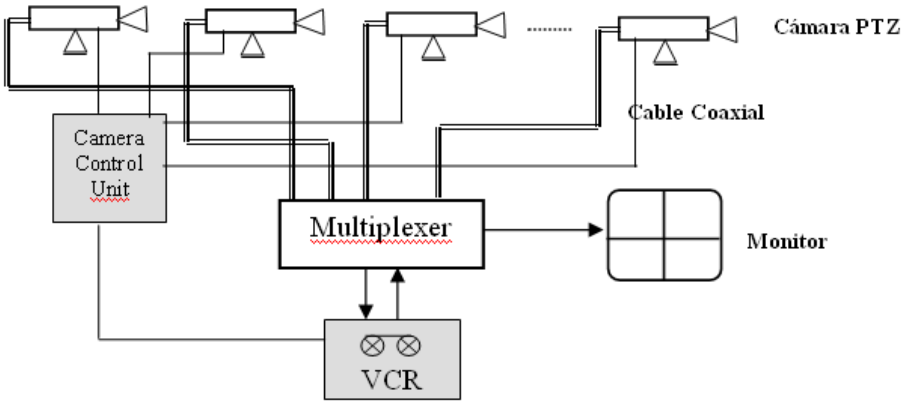
Los sistemas de televisión de circuito cerrado CCTV y los de vigilancia por video IP se está convirtiendo en un componente vital en la mayoría de la Instituciones, la vigilancia es un componente integral de los métodos de control y acceso implementando sistemas de autenticación biométricos, sistemas de rastreo de seguridad y sistemas de rastreo de acceso.[84]

Los sistemas análogos tradicionales CCTV fueron diseñados para transmisión punto a punto de video desde una cámara hasta una grabadora en el mismo sitio utilizando cable coaxial de 75 Ohm. Varias cámaras se conectaban por medio de este cableado y se conectaban en home-run a multiplexores que alimentaban varias grabadoras de video en un cuarto de control central, se podía mirar las imágenes en tiempo real por medio de varios monitores, se disponía de un switch para cambiar a la cámara deseada a un monitor

[82] http://dns.bdat.net/seguridad_en_redes_inalambricas/c113.html
[83] http://dns.bdat.net/seguridad_en_redes_inalambricas/c113.html
[84] http://www.siemon.com/es/white_papers/SD-03-08-CCTV.asp

específico, o de monitores capaces de aceptar múltiples fuentes de video en ventanas separadas.

Figura2.38: Video Analógico CCTV



Fuente: http://www.siemon.com/es/white_papers/SD-03-08-CCTV.asp

La desventaja en este método radica en el costo de la estación de monitoreo, el monitoreo centralizado constituye un punto de falla crítico dentro de la infraestructura de seguridad. Todas las alimentaciones de video y cables de control tienen que ser instalados en home-run hacia este punto.

Si una cámara era reubicada frecuentemente se requería un nuevo tendido de cable, las cinto tecas requerían muchas cintas y debido a que los medios magnéticos son susceptibles a descargas magnéticas o electroestáticas estos sistemas no siempre proporcionaban el total de la funcionalidad para lo cual fueron diseñadas. El factor humano también era parte de este sistema ya que una persona era el responsable de cambiar físicamente las cintas, monitorear las sesiones de grabación, etc. En ocasiones el uso de fibra óptica era necesario en ambientes donde las distancias requerían el uso de repetidores para ampliar la señal a donde la interferencia electromagnética representa un problema.

Con el aparecimiento de cámaras de red nace un sistema de segunda generación. Las cámaras direccionables IP pueden ser incorporadas actualmente en la infraestructura existentes en edificios. El desarrollo de imágenes digitales se almacena en formato digital en servidores u otras

computadoras en lugar de cintas de video, aliviando los problemas inherentes a medios magnéticos.[85]

Esta nueva especie de video permite transmisiones IP de las señales de video a los dispositivos direccionables IP y pueden transmitirse en combinación con secuencia de voz y/o video.

Adicionalmente los movimientos y cambios son más fáciles ya que las cámaras pueden instalarse dondequiera que exista un punto de red. El cableado viaja hacia un multiplexor que soporta los populares conectores RJ45. Las cámaras tradicionales o analógicas con conectores coaxiales pueden reacondicionarse con baluns (balanced/unbalanced) que convierten la señal de un cable coaxial (no balanceada) a la del cable de par trenzado (balanceada).

Los Equipos electrónicos que manejan el tráfico en la red IP se han vuelto parte integral en los sistemas de vigilancia por el almacenamiento de video en formato digital que pueden ser vistos desde cualquier lugar de la red con nuevas capacidades de seguridad para los archivos administrados como parte de las políticas de seguridad de la red.

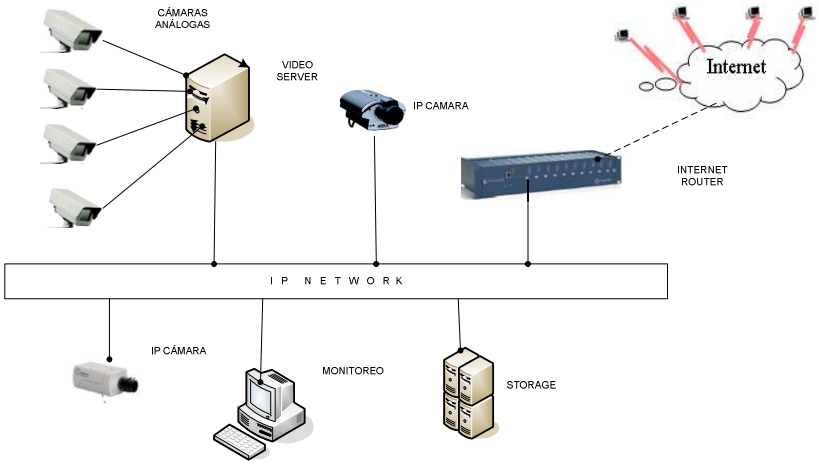
TCP/IP es el protocolo utilizado para la mayoría de redes su arquitectura abierta permite que varios sistemas puedan compartir el espacios de red y aprovechar estas nuevas tecnologías para aumentar su capacidad, escalabilidad u accesibilidad de los recursos de la red. Los administradores y usuarios de la red tienen la ventaja de monitorear desde cualquier estación de trabajo con acceso a la red, de igual forma el personal de seguridad de la Institución. La cámara digital se vuelve ahora en el punto de falla y ya no en el centro de control ya que se puede tener servidores redundantes digitales ya sea en solo sitio o distribuido en múltiples ubicaciones.

Un sistema típico CCTV basado en IP se indica en el gráfico 1.8 como se puede apreciar las cámaras y los servidores de video IP pueden colocarse en cualquier punto de la red, como en el protocolo IP las funciones de administración son incorporadas en la transmisión, esto incluye DSP (Digital Signal Procesing) manejo de alarmas, grabación capacidades de búsqueda y/o archivo, calendarización y automatización. Estas funciones de administración y control utilizan SNMP (Simple Network Management Protocol).[86]

---

[85] http://www.nexo-tech.com/srv_ip.php?menu=2
[86] http://www.nexo-tech.com/srv_ip.php?menu=2

Figura 2.39: Video IP Digital CCTV



Fuente: http://www.siemon.com/la/white_papers/SD-03-08-CCTV.asp

Las cámaras IP pueden equiparse con características avanzadas según la necesidades del caso tales como sensores de movimiento, PTZ (Pan Tild and Zoom) automatizado, y si se desea salidas análogas de video, las versiones más actualizadas de estas cámaras vienen equipadas con DVR internos que pueden replicarse con un servidor DVR centralizado.

Es necesario establecer el ancho de banda de la red que consiste en decidir cuántas cámaras se necesitan, qué calidad de vídeo es necesaria para el visionado y la grabación, y cuántos días de grabación se necesitan. Después se puede utilizar esta información para calcular cuánto ancho de banda y almacenamiento de grabaciones se necesita.

Es fundamental que a cada cámara se le asigne una dirección IP, asegurándose que se encuentran en la misma subred y por lo tanto se pueden realizar pruebas de comunicación para verificar si cada cámara responde.

2.10.1 CÁMARAS IP.

Una cámara de red tiene su propia dirección IP y características propias para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad. Una cámara de red puede describirse como una cámara y un computador combinados.

Se conecta directamente a la red como cualquier otro dispositivo de red e incorpora software propio para servidor Web, servidor FTP, cliente FTP y cliente de correo electrónico. También incluye entradas para alarmas y salida de relé. Las cámaras de red más avanzadas también pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico.[87]

La razón más habitual de una calidad de imagen pobre es la insuficiencia de luz. Con un nivel de luz muy bajo el nivel de los colores será sombrío y las imágenes borrosas. El nivel de luz se mide en Lux. La luz solar fuerte tiene aproximadamente 100.000 Lux, la luz diurna tiene aproximadamente 10.000 Lux y la luz de una vela tiene aproximadamente 1 Lux. Habitualmente se precisan al menos 200 Lux para capturar imágenes de buena calidad. Las áreas brillantes deben ser evitadas dado que las imágenes pueden resultar sobre-expuestas y que los objetos aparezcan muy oscuros. Este problema ocurre igualmente cuando se intenta capturar un objeto con luz negra. Una cámara ajusta la exposición para conseguir una buena media de nivel de luz para la imagen, pero el contraste de color entre el objeto y el fondo influye en la exposición. Para evitar este problema los objetos oscuros pequeños deberían disponerse delante de un fondo oscuro para conseguir el color y el contraste correctos.[88]

A continuación se describen las siguientes características que deben considerar en la elección de las cámaras IP:

---

[87] http://www.camarasip.cl/que_es_una_camara_de_red.htm
[88] http://www.camarasip.cl/que_es_una_camara_de_red.htm

2.10.1.1 CALIDAD DE IMAGEN.

Esta característica es una de las más importantes, si la calidad de la imagen no es buena el resto de factores es irrelevante, una mejor calidad de la imagen permite al usuario obtener mejores resultados en detalles y cambio en la imágenes según su evento, es importante tener en consideración cuál es su sensibilidad lumínica, si la imagen es clara, que calidad tiene la imagen cuando existe movimiento. Se debe considerar los siguientes factores:

- Permitir zoom de la imagen
- Sensibilidad lumínica día noche
- Permitir ángulos de cobertura
- Cámaras día noche, grabación con detección de movimiento, audio
- Cámaras día noche espía
- Cámaras día, grabación con detección de movimiento

2.10.1.2 FACILIDAD DE INTEGRACIÓN.

Las cámaras IP deben ser capaces de integrarse a plataformas abiertas es decir que puedan ser configuradas fácilmente para operar con otros tipos de cámaras de fabricantes distintos con sus respectivas aplicaciones de software.

Una particularidad importante se trata que cuando la cámara sea instalada, configurada y posea una dirección IP dentro de la red local ésta sea fácil de incorporarse a cualquier software de monitoreo y que no limitarse exclusivamente al software del fabricante específico.

2.10.1.3 COMPRESIÓN COMPATIBLE CON LOS ESTÁNDARES JPEG, MPEG4

Una compatibilidad a los estándares asegura flexibilidad en el uso de muchas aplicaciones de video diferente garantizándose así la visualización de video por largo tiempo con sistemas patentados de acuerdo a las normas internacionales. Se debe tener en consideración la cantidad de licencias que se deben adquirir para el circuito IP.

Las cámaras de tecnología IP que se incorporarán al presente proyecto deben cumplir con los estándares de video existentes en el mercado por la sencilla

razón que permite la optimización de los sistemas para que consigan la mejor calidad de imagen y el menor consumo de ancho de banda y que sean compatibles con diferentes tipos de cámaras que usan los mismos tipos de estándares.

2.10.1.4 Requisitos de sistema para visualización de cámaras vía IP.

Las siguientes especificaciones corresponden a la aplicación de visualización mediante Navegador. [89]

- Navegadores Web compatibles: Windows -
- Internet Explorer
- Mozilla 1.4* ó posterior
- Mac OS X - Mozilla 1.4* ó posterior y
- Netscape 7.1* ó posterior
- Sistemas operativos compatibles:
- Windows XP, 2000, NT4.0, ME y 98, Linux y Mac OS X

Hardware: según las especificaciones del sistema que puede ser las estaciones de trabajo con las características mencionas anteriormente operativo y el navegador.

2.10.1.5 SOFTWARE DE MONITOREO

Se requiere implementar un software que permita gestionar el sistema de cámaras de video IP para potencializar al máximo las aplicaciones en calidad tecnología de compresión y beneficios del video IP.

Dichas aplicaciones de software posibilitan el control, administración y visionado tanto de las grabaciones en directo como del vídeo grabado a través de la red IP.[90]

El poder construir un circuito cerrado de monitoreo IP no se encuentra en la cámara sino en el software de gestión, que ofrece una aplicación útil al usuario

[89] http://www.ipcamarasvigilancia.com/camara-axis-p-6.html
[90] http://www.indigovision.com/files/international/IP-Cameras%20-%20Apr06-Spanish-Revised.pdf

final. Por lo tanto, el rendimiento general depende fundamentalmente de la interacción del software con la cámara IP, el hardware de grabación y la red.

El circuito cerrado IP se trata de un conjunto de componentes que se distribuyen a través de una red IP, siendo el componente absolutamente esencial el software que gestiona el resto de los componentes. Así que las cámaras IP no son suficientes por sí solas. Su funcionalidad real se encuentra en el software, que debería ser la prioridad al decidir qué solución de vídeo IP se va a elegir, dicho software depende en última instancia del rendimiento del sensor de imagen y la calidad de compresión.

Además debe incorporar la visualización o monitoreo dentro de la red local como hacia fuera, la posibilidad de integrar cámaras de distinta tecnología que disponga una interfaz de sistema abiertos es decir una interfaz de programación.

2.10.1.6 FUNCIONALIDAD Y SEGURIDAD DE LAS CÁMARAS DE VIGILANCIA IP.

Se debe determinar si la cámara ofrece funciones y seguridad de red adecuadas por la razón que cada dispositivo de estos utiliza una dirección de red, de igual forma el acceso o monitoreo remoto se deben establecer las seguridades en el protocolo HTTPS.

Para el acceso remoto los protocolos a utilizarse son el HTTP puerto 80 y el protocolo HTTPS que utiliza el puerto 8080, estas configuraciones de acceso se los configura en el servidor ISA con las reglas de publicación de un servidor para permitir tráfico de redes externas.

2.10.1.7 MEDIOS DE ALMACENAMIENTO DE LAS CÁMARAS IP

Todos los eventos ocurridos deben ser registrados o almacenados en algún lugar de la red de acuerdo a la política de grabación previamente definida por la Gerente de Hostal La Carolina.

Los eventos digitales se graban en discos duros de la misma forma en que un archivo se almacena en una PC, este método permite obtener redundancia,

monitoreo descentralizado y mayor longevidad de las grabaciones. En las computadoras se cuentan con discos duros de tecnología IDE - ATA.

La mayor parte de las computadoras tienen discos de tipo IDE (que por evidentes razones económicas son los más utilizados en la actualidad), es posible afirmar que en los últimos años sus prestaciones han mejorado bastante, se ha conseguido que los últimos modelos de discos IDE alcancen las 7.200 revoluciones por minuto (los IDE anteriores eran de 5.400 r.p.m.), lo cual significa mayor velocidad en la lectura de los datos.

Serial ATA o S-ATA es una interfaz para discos que sustituye al tradicional Paralelo ATA o P-ATA (estándar que también se conoce como IDE o ATA). El S-ATA proporciona mayores velocidades, mejor aprovechamiento cuando hay varios discos, mayor longitud del cable de transmisión de datos y capacidad para conectar discos en caliente (con la computadora encendida).[91]

Mientras que la especificación SATA1 llega como máximo a unos 1.5 GBit/s, SATA2 incrementa el límite a 3 GBit/s. Actualmente es una interfaz ampliamente aceptada y estandarizada en las placas base de PC.

A continuación se describe los *requerimientos necesarios* y características de los discos que se necesitan como medios de almacenamiento:[92]

Capacidad. Cantidad de datos que pueden almacenar. Un disco duro actual debe de tener, al menos, 20 Gb.

Velocidad de giro. Muy importante que sea de al menos 7.200 R.P.M., se nota la diferencia de velocidad respecto de los de 5.400 R.P.M. Si es SCSI lo podremos encontrar de hasta 10.000 R.P.M.

Tiempo de acceso. Nos marca el tiempo que tarda en acceder a cualquier parte del disco de manera aleatoria. Lógicamente, cuanto más baja menor. Se suele medir en milisegundos (ms) y actualmente ronda los 10-8 ms.

---

[91] http://www.maximotec.com/showthread.php?t=27836
[92] http://usuarios.lycos.es/todohardware/hd.htm

Tipo de transmisión. Hay que fijarse que un disco duro IDE sea ATA 100. Esto es el sistema de transmisión, que podría alcanzar los 100 Mb por segundo, pero, claro está, esto es teórico porque un disco duro suele mover unos 30 Mb por segundo como mucho, aunque ya empiezan a aparecer discos duros y placas base ATA 133. Si es SCSI la transmisión podrá ser de 80, 160 o 320 Mb/s.

Caché del disco. Este es un dato importante. Es un tipo de memoria que intenta mantener constante el envío de datos a la controladora. Suelen rondar los 2 Mb,

Estas características de los discos duros son parámetros referenciados desde la información de los fabricantes, con el fin de obtener la mayor información posible para ser incorporada a las estaciones de trabajo que forman parte del proyecto.

En este ámbito, los nuevos equipos que se están adquiriendo en este caso los computadores tienen tecnología SATA2 por los beneficios anteriormente mencionados.

2.10.1.8 FORMATOS DE COMPRESIÓN DE VIDEO

La resolución de las imágenes digitales se mide en píxeles. La imagen más detallada es la que tiene más datos y por tanto mayor número de píxeles. Las imágenes con más detalles ocupan más espacio en los discos duros y precisan mayor ancho de banda para su transmisión. Para almacenar y transmitir imágenes a través de una red los datos deben estar comprimidos o consumirán mucho espacio en disco o mucho ancho de banda.

Si el ancho de banda está limitado la cantidad de información que se envía debe ser reducida rebajando el número de frames por segundo o aceptando un nivel de calidad inferior. Existen múltiples estándares de compresión que resuelven los problemas de número de frames por segundo y calidad de imagen de diferentes formas. De los estándares más comunes tanto el JPEG como el MPEG transmiten vídeo de alta calidad, mientras que los estándares-

H, usados normalmente en videoconferencia, no generan imágenes claras de objetos que se mueven a gran velocidad.[93]

Cada punto de la imagen se le asigna un determinado número de bits que representarán el color de dicho punto. Si la imagen es en blanco y negro, bastará un bit para representarlo, mientras que para 256 colores serán necesarios 8 bits. De esta forma tendremos la imagen digitalizada, pero almacenar esta información dependerá del número de pixeles que utilicemos por imagen. Por ejemplo una imagen de 640 x 480 puntos con 256 colores ocupa 300 Kb, y si tenemos una secuencia de vídeo a 25 fotogramas por segundo significaría que un solo segundo ocuparía 7.500 Kb. La información de vídeo compuesta de esta manera posee una cantidad tremenda de información; por lo que, para transmisión o almacenamiento, se requiere de la compresión de la imagen.

La compresión del vídeo generalmente implica una pérdida de información y una consecuente disminución de calidad. Pero esto es aceptable porque los algoritmos de codificación están diseñados para descartar la información redundante o que no es perceptible por el ojo humano.[94]

El vídeo comprimido en general debe transmitir información por un canal más pequeño del que necesitaría para ser transmitido y poder ser visualizado en tiempo real. Así la información de audio y vídeo deben ser procesadas por los codecs antes de ser transmitidos. Los codecs derivan de las palabras compresor y descompresor, y son los módulos de software que permiten la compresión y descompresión de los ficheros de audio y vídeo para que puedan ser transmitidos por redes de baja velocidad. 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

[93] http://www.camarasip.cl/que_es_una_camara_de_red.htm
[94] http://www.monografias.com/trabajos10/vire/vire.shtml

comprimidas son transmitidas a través de la línea de transmisión digital y se hacen llegar al receptor donde son reconvertidas al formato común CIF.[95]

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 descompresión es el proceso inverso de la compresión. 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.

Los estándares de vídeo digital más conocidos son: MPEG, Quicktime, AVI, MOV, real vídeo, ASF. JMPEG MPEG (Grupo de Expertos en Imágenes en movimiento) 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.

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 I o Intra-fotogramas, son los fotogramas normales o de imagen fija, proporcionando una compresión moderada, en JPEG.

[95] http://www.monografias.com/trabajos10/vire/vire.shtml

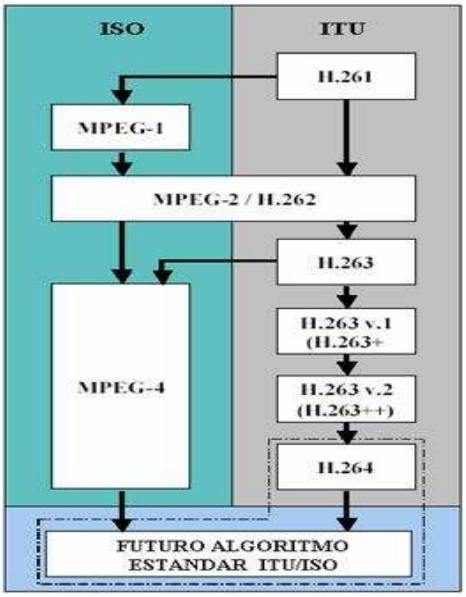
Fotogramas P o Predichos: son imágenes predichas a partir de la inmediatamente anterior. Se alcanza una tasa de compresión muy superior.

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. Estándar escogido por Vídeo-CD: calidad VHS con sonido digital.

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.[96]

MPEG4 es un estándar relativamente nuevo orientado inicialmente a las videoconferencias, 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. JPEG utiliza una técnica de compresión espacial, la de intracuadros o DCT. El sistema JPEG solamente utiliza la compresión espacial al estar diseñado para comprimir imágenes individuales.

Figura 2.40: Técnicas de compresión de video



[96] http://www.monografias.com/trabajos10/vire/vire.shtml

2.10.1.9 TRANSPORTE DE PAQUETES DE VIDEO

La transmisión digital y la distribución de audio y video permite la comunicación multimedia sobre las redes que soportan la transmisión de datos, brindando la posibilidad de enviar imágenes en movimiento a cualquier sitio remoto, el video es muy sensible al retardo en la red, ya que puede provocar cortes en la secuencias.

La pérdida de información en el video sin comprimir no es muy sensible ya que al perderse un fotograma, el siguiente fotograma proporciona la suficiente información para poder interpretar la secuencia, en cambio el video comprimido es más sensible a errores de transmisión ya que las técnicas de compresión se valen de redundancia temporal que pueden perder información.[97]

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. Si se dispone de una alto ancho de banda el tipo de red adecuada sería ATM; para un entorno de red de área local podríamos usar Fast Ethernet, y actualmente para que el usuario de Internet ADSL. 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.

[97] http://www.monografias.com/trabajos10/vire/vire.shtml

2.10.1.10 DIGITALIZACIÓN DE IMÁGENES DE VIDEO

Cada muestra de color se codifica en señal Y-U-V (Y- luminancia, U y V crominancia) partiendo de los valores del sistema RGB. Con este sistema las diferencias de color pueden ser muestreadas sin resultados visibles, lo que permite que la misma información sea codificada con menos ancho de banda.

Luminancia (Y): 720x576x25x8 = 82.944.000 bits por segundo

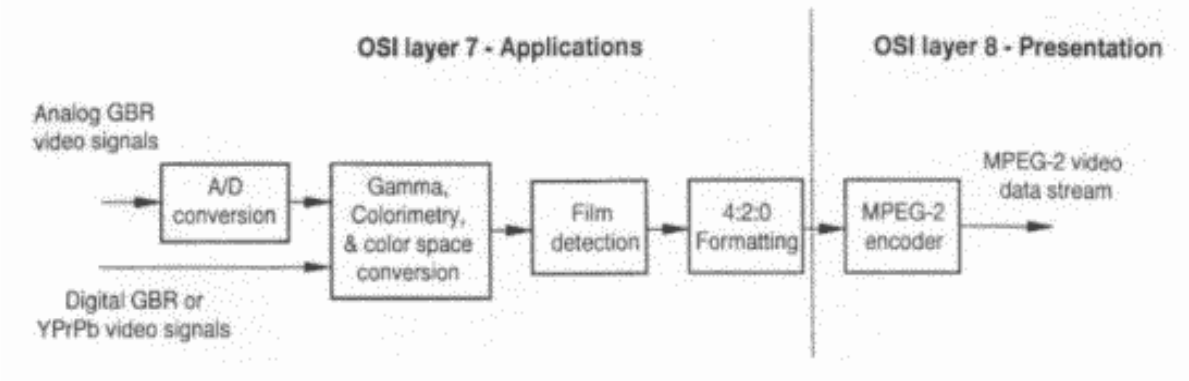
Crominancia (U): 360x576x25x8 = 41.472.000 bits por segundo

Crominancia (V): 360x576x25x8 = 41.472.000 bits por segundo

Las imágenes de vídeo están compuestas de información en el dominio del espacio y el tiempo.

La información en el dominio del espacio es provista por los píxel, y la información en el dominio del tiempo es provista por imágenes que cambian en el tiempo. Puesto que los cambios entre cuadros colindantes son diminutos, los objetos aparentan moverse suavemente. El valor de luminancia de cada píxel es cuantificado con ocho bits para el caso de imágenes blanco y negro. En el caso de imágenes de color, cada píxel mantiene la información de color asociada; una imagen completa es una composición de tres fotogramas, uno para cada componente de color, así los tres elementos de la información de luminancia designados como rojo, verde y azul, son cuantificados a ocho bits.

Figura 2.41: Codificación de fuente de video



Fuente:http://www.monografias.com/trabajos16/ingenieria-de-tv/ingenieria-de-tv.shtml

2.10.1.11 FALLAS EN LA TRANSMISIÓN.

Muchas cosas pueden pasar entre la fuente del video y el receptor de video, en este contexto se derivan fallas de transmisión en la red que se deben considerar cuando se planea la transmisión de video.

2.10.1.11.1 PÉRDIDA DE PAQUETES.

Un paquete es declarado perdido cuando no llega a tiempo a su destino, esto puede ser causado por muchas circunstancias tales como fallas en la red debido a que un simple bit dentro del paquete puede estar defectuoso o erróneo o por fallas en la configuración de la red como envíos de paquetes erróneos al destino, en muchos de los casos los paquetes pueden perderse ocasionalmente en la transmisión sobre redes IP.

Los paquetes IP incluyen un checksum en cada cabecera, este checksum es utilizado para realizar pruebas en la cabecera si esta corrupta en la transmisión. En cada lapso de tiempo un paquete es recibido, el checksum es recalculado, si el resultado de la re calculación no es igual al checksum entrante, la cabecera ha sido corrompida y el paquete será rechazado.

Una forma de calcular el porcentaje de error de transmisión de los paquetes es chequear el BER (Bit Error Ratio) es el número de bits defectuosos dividido par el número total de bits transmitidos. Muchos tipos de fibra óptica especifican el BER como 1 x 10 -9 en porcentaje de error.

2.10.1.11.2 REORDENAMIENTO DE PAQUETES.

Los paquetes se reordenan en una red cuando los paquetes son recibidos en diferente orden que originalmente fueron enviados, como por ejemplo algún tipo de e-mail o transferencias de archivos esto no es un problema mientras los paquetes sigan llegando.

El video streaming particularmente MPEG tiene definida una buena estructura y secuencia, esta estructura es necesaria para permitir una correcta decodificación y determinar en donde cada píxel necesita ser reemplazado en la imagen, la sincronización de estos datos es muy importante, si algunos de los datos para una imagen no es el correcto en esta sincronización para

desplegar una imagen, la imagen tendrá errores y no podrá ser desplegada completamente.

Cuando los paquetes llegan fuera de orden deben ser retransmitidos en una secuencia correcta para que la decodificación de video sea operable.

Los paquetes pueden llegar en desorden por varia razones, una de las posibles causas pueden darse cuando existe muchos caminos desde la fuente a los destinos, los paquetes destinos pueden utilizar diferentes caminos y diferentes tiempos para llegar a su destino, también puede darse por congestión en la red, los paquetes pueden retardarse mientras esperan por su turno para ser enviados.

Los paquetes que llegan en desorden pueden fácilmente reordenarse a través del uso de un buffer de manera que esto puede causar mas retardo en el envío de información, cuando se evalúa una red para el tráfico de video se debe examinar este parámetro de reordenamiento de paquetes, para lo cuál se podrá decidir si va a servir la transmisión de video.

2.10.1.11.3 Retardo

Existen dos causas principales para el retardo: Propagación en el retardo y switching retardo.

Propagación Delay. Es la cantidad de tiempo que toma la información para viajar desde una localización a otra, con las redes modernas la información puede viajar tomando como referencia la velocidad de la luz usando ondas de radio o fibra óptica.

Switching delay ocurre en cualquier punto de la red don de una señal necesita ser ruteada o switched. El retardo en este punto puede darse por varios motivos como la cantidad de paquetes que el ruteador esta procesando, también por congestión o el tiempo de procesamiento que utiliza el ruteador.

El ruteador utiliza el mecanismo de llamada de colas para manejar los paquetes que es muy similar a línea de cajeros en un supermercado, los paquetes van ubicándose en diferentes colas dependiendo de su prioridad, tamaño y tiempo.

La cantidad de tiempo que toma un paquete para viajar a través de un ruteador es afectado por el sitio donde este ubicada.

2.10.1.11.4 JITTER

Es una medición de la variación de tiempo de la llegada de los paquetes, por ejemplo un remitente esta transmitiendo 500 paquetes por segundo o uno cada 2000 microsegundos un jitter ideal a cero sería que los paquetes lleguen al receptor sincronizadamente de la misma forma que fueron enviados es decir uno cada 2000 microsegundos, jitter puede ocurrir cuando los paquetes recibidos tienen diferente sincronización que puede ser 20 microsegundos temprano o 50 microsegundos después, es decir que el retardo entre paquetes no es constante.

Latencia es el tiempo que se tarda en obtener una respuesta, es la suma del retardo de la red y los servidores, retardo de propagación y de transmisión (dependiente del tamaño del paquete).

Un tiempo de latencia variable se define como Jitter (fluctuación del retardo) sobre los datos de recepción, la solución del jitter es guardar los datos en memorias buffer, lo cuál hace al retardo mayor formas de buffer[98]

2.10.1.12 POLÍTICAS DE BACKUP

Como se mencionó anteriormente toda la información que se genera se almacena en las carpetas de almacenamiento de cada cámara, esta información posteriormente se trasladará al servidor de respaldos donde solo tiene acceso el administrador de red.

- Con ayuda de la herramienta de copia de seguridad propia de Windows se puede configurar el respaldo de la siguiente forma:
- El respaldo se lo debe realizar diariamente.
- Realizar un respaldo normal la primera vez
- Cada día realizar un respaldo normal y diferencial
- Verificar periódicamente la integridad de los respaldos

[98] http://www4.ujaen.es/~jcbago/progrupo/resumenes/Resumen%20Equipos%20QoS.pdf

- Evaluar la información respaldada conjuntamente con el jefe de seguridad antes que los respaldos sean borrados físicamente teniendo en cuenta que los archivos de video generan gran espacio en disco.

De igual forma realizar una restauración periódica con el fin de comprobar la integridad de la información.

CAPÍTULO 3

3.1 SOLUCIONES PARA REDES INALÁMBRICAS

Para satisfacer todas las necesidades en redes inalámbricas, en el mercado existe una amplia gama de productos y proveedores orientados a los diferentes categorías de las empresas (grandes, medianas, pequeñas y para el hogar), en esta sección se analizan algunas de estas.

Una de las características del mundo empresarial actual es la creciente movilidad de sus ejecutivos y técnicos. Las relaciones de redes entre los negocios, hacen que muchos de ellos se desarrollen fuera de las oficinas y que sea necesario estar integrados a los flujos de información de las empresas, conectarse a las aplicaciones de negocios, a través de soluciones de redes inalámbricas, de la computación móvil [99]

3.2 Soluciones 3COM

3Com ha continuado en su progreso inalámbrico y en su oferta de una estrategia de integración, a medida que han surgido los nuevos estándares Wi-Fi y la tecnología inalámbrica. Hace dos años, 3Com tuvo mucho éxito con la salida de sus soluciones inalámbricas basadas en 802.11b que soportaban transmisiones de datos de 11 Mbps en la frecuencia de 2.4 GHz. Después, 3Com introdujo soluciones inalámbricas basadas en 802.11a para brindarles a los usuarios acceso a velocidades inalámbricas más altas de 54 Mbps, que operan en la banda de 5 GHz. A medida que los estándares inalámbricos continuaron evolucionando, 3Com introdujo productos con modalidad dual en 802.11a y 802.11b en marzo del 2003 y productos inalámbricos basados en el estándar 802.11g en junio, ofreciendo una tecnología inalámbrica a velocidad más alta, compatible con equipos 802.11b.[100]

[99] http://www.coasin.cl/index.php?id=61
[100] http://lat.3com.com/lat/news/pr03/nov10.html

3.2.1 Access Point (3COM)

El punto de acceso a LAN Inalámbrica de 11 Mbps 3Com AirConnect actúa como puente entre el backbone de Ethernet de cable y sus clientes inalámbricos. Instalado normalmente en el techo o en la pared, el punto de acceso funciona con PC Cards de LAN inalámbrica para usuarios de ordenadores portátiles y con PCI Cards para usuarios de ordenadores de sobremesa, permitiéndoles acceder sin problemas a las redes desde cualquier lugar.[101]

Figura 3.1: AirConnect a 11 Mbps de 3Com

Precio: 100 USD

Fuente: http://www.ciao.es/3Com_AirConnect__690376

Tabla 3.1: Características de Access point 3Com

Tipo de dispositivo:	Punto de acceso inalámbrico
Dispositivos integrados:	Panel led
Anchura:	*19.7 cm*
Profundidad:	15 cm
Altura:	3.2 cm
Peso:	0.5 kg
Color incluido	Blanco
Factor de forma:	Externo
Tecnología de conectividad:	Inalámbrico
Velocidad de transferencia de datos:	11 Mbps
Protocolo de interconexión de datos:	Ethernet, IEEE 802.11b
Red / Protocolo de transporte:	TCP/IP, IPX/SPX, NetBEUI/NetBIOS
Protocolo de gestión remota:	SNMP, HTTP, SNMP, Telnet, HTTP
Modo comunicación:	Dúplex pleno
Alcance máximo en interior	90 m, 91 m
Alcance máximo al aire libre:	303 m, 91 m
Nº de canales seleccionables:	13, 63
Indicadores de estado:	Actividad de enlace
Características:	Capacidad duplex, criptografía 128 bits, soporte de DHCP, activable, Criptografía 128 bits, activable, Soporte de DHCP.

[101] http://www.ciao.es/3Com_AirConnect__690376

3.2.2 Tarjeta de red (3COM)

Conectividad inalámbrica para usuarios de computadoras portátiles. Si busca una red inalámbrica la tarjeta de red de 3Com es ideal.

La certificación Wi-Fi significa que la PC Card se comunica con cualquier red inalámbrica, o bien directamente con cualquier dispositivo que cumpla la especificación Wi-Fi. Además, soporta encriptación WEP de 64 y de 128 bits para proteger transmisiones inalámbricas.

Figura 3.2: 11Mbps Wireless LAN PC Card con antenna x-Jack

Fuente: http://www.apcnet.com.mx/3com/lan.htm

3.2.2.1 Características y beneficios:

- Velocidad de 11Mbps a una distancia de 100 mts. (330 ft)
- Su antena X-Jack se extiende para una recepción libre de interferencia mientras se encuentre en uso y se retrae para su seguridad y conveniencia.
- Dynamic rate shifting que ajusta la velocidad de la conexión mas confiables.
- Auto conexión con DHCP que mantiene usuarios móviles conectados en roming.
- Permite conexión inalámbrica simple uno a uno.
- La funcionalidad de Dynamic Security Link (enlace de seguridad dinámica) ofrece clave de encriptación de 128-bits por usuario que cambia en cada sesión de conexión, adicional a la autenficación del usuario"

3.2.3 Antenas (3COM)

3Com® ofrece una amplia selección de antenas específicamente diseñadas para optimizar la conectividad 802.11 en diferentes entornos. Estas antenas amplían el área de cobertura de los bridges para LAN inalámbrica y de los puntos de acceso con antenas desmontables; los cables de antena están disponibles en distintas longitudes.[102]

Figura 3.3: 3Com® 6/8dBi Dual-Band Omni Antenna

Fuente: http://www.3com.com/prod/es_ES_EMEA/detail.jsp?tab=features&sku=3CWE591

3.2.3.1 Características y ventajas

Esta antena es idónea para conexiones punto a multipunto de medio alcance con bridges de interiores entre edificios. Permite también ampliar el área de cobertura de puntos de acceso empresariales 3Com para LAN inalámbrica (WLAN) con antenas extraíbles. [103]

- La antena omnidireccional proporciona una cobertura uniforme en todas las direcciones en grandes espacios abiertos
- La antena de doble banda soporta radios de punto de acceso 802.11a 5,0 GHz ó 802.11b/g 2,4 GHz
- Se instala en interiores o en exteriores
- Se entrega con soporte de montaje

[102] http://www.3com.com/prod/es_ES_EMEA/prodlist.jsp?tab=cat&cat=13&subcat=91
[103] http://www.3com.com/prod/es_ES_EMEA/detail.jsp?tab=features&sku=3CWE591

3.2.4 Router (3COM)

Figura 3.4: 3Com® Office Connect® Remote 812 ADSL Router

Precio 80 USD

Fuente:http://www.fixya.com/Brands/Images/0/3Com/177x150/21066333.JPG

3.2.4.1 Características y ventajas

Soporta ADSL Full y Sub-Rate, y PPPoE Too. Conecta hasta 4 usuarios, o hasta 40 apilando más puertos, tales como el 3Com® OfficeConnect® hubs o switches. Todos pueden estar en línea al mismo tiempo. Con su cliente interno PPPoE, servidor DHCP/DNS, y los dos both estándares ADSL, este router hace seguras la conexiones ADSL.[104]

3.2.4.2 Especificaciones de producto

- Número de ordenadores para servicio ADSL: Hasta 4 directamente al router, hasta 40 con más hub o switch añadidos
- Servicios WAN: Servicios Full-rate ADSL incluyendo ITU G.992 (G.dmt) y ANSI T1.413, Issue 2; servicio sub-rate ADSL incluyendo ITU G.992.2 (G.lite)
- Protocolos soportados: IP (RIP v1, RIP v2), IPX, 802.1 transparent bridging, learning bridging, DHCP, NAT/PAT, DNS Server, direccionamiento estático, UNI 3.1, Unit 4.0, RFC 1483 (Multiprotocol over ATM), PPP, PPPoE
- Puerto/WAN: 1 ADSL (conector RJ-11)
- Puertos/LAN: 4 10BASE-T (conector RJ-45)

[104] http://www.3com.es/products/adsl/

- Requerimientos del sistema/puerto Ethernet: Ordenador con interfaz 10BASE-T y pila IP
- Requerimientos mínimos/Software incluido: PC con Windows 95 o posterior y lector CD-ROM
- Velocidades: Hasta 8 Mbps downstream (desde el proveedor) y 1 Mbps upstream (hacia el proveedor); G.lite: Hasta 1.5 Mbps downstream y 512 Kbps upstream
- Gestión: Gestionable vía cualquier aplicación de gestión SNMP o interfaz de línea de comandos vía Telnet y puerto de consola; local HTML- o instalación basada en asistente, configuración, y gestión usando un navegador Web estándar
- Altura: 13.3 cm (5.3 in)
- Anchura: 23.5 cm (9.3 in)
- Profundidad: 16.8 cm (6.6 in)

3.3 SOLUCIONES LINKSYS

Linksys es una alternativa en la industria de soluciones de conectividad y banda ancha para pequeñas y medianas empresas (PyMEs). Cada producto Linksys ha sido diseñado para darle la mayor velocidad, el menor precio, la simplicidad para conectar y operar, y la mejor compatibilidad con la mayoría de los sistemas operativos de red. Las soluciones de Linksys se diseñan para empresas que desean el mayor rendimiento de red posible.[105]

3.3.1 Access Point (Linksys)

Wireless-G es el novedoso estándar de red inalámbrica de 54 Mbps que proporciona una velocidad casi 5 veces superior que los populares productos Wireless-B (802.11b). El punto de acceso Wireless-G de Linksys permite conectar dispositivos Wireless-G o Wireless-B a la red. Ya que ambos estándares son incorporados, puede aprovechar la inversión realizada en infraestructura 802.11b y migrar los clientes de red al novedoso y velocísimo estándar Wireless-G a medida que aumentan sus necesidades. Además, para

[105] http://www.beep.es/Redes/C-maras-IP/Linksys-Wireless-G-Compact-Internet-Video-Camera-WVC54GCV1ZDNTRHQy1FVQ==.html

proteger datos y privacidad, puede encriptar todas las transmisiones inalámbricas, incluyendo filtros MAC y configuración basada en explorador web para facilitar la tarea. Prepárese con Linksys para la alta velocidad Wireless-G del mañana.[106]

Figura 3.5: Punto de Acceso Linksys WAP54G 54 Mbps

Precio: 75 USD

Fuente: http://www.ciudadwireless.com/product_info.php?products_id=172

3.3.1.1 Características

- Red Wireless-G de alta velocidad para el hogar o la oficina
- Transferencia de datos de hasta 54 Mbps: 5 veces más rápido que Wireless-B (802.11b)
- Compatible con las redes Wireless-B a 11 Mbps
- Seguridad inalámbrica avanzada con encriptación WEP de 128 bits y filtro de MAC

3.3.1.2 Especificaciones

- Estándares IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE802.3u Puertos 1 Auto-Cross Over 10/100 (MDI/MDI-X), potencia
- Botones Reset
- Cableado RJ-45
- LEDs Encendido, actividad, enlace
- Seguridad Web-browser WPA, WEP Encryption, MAC Filtering,

[106] http://www.ciudadwireless.com/product_info.php?products_id=172

- WEP 64/128 bit

3.3.2 Tarjeta de red (Linksys)

La tarjeta PCI Card Wireless-G de Linksys se puede instalar en la mayoría de ordenadores de escritorio y permite situar el equipo en prácticamente cualquier lugar del edificio.

La tarjeta PCI Card Wireless-G le permite conectar a las redes Wireless-G a 54 Mbps. Su versatilidad le permite funcionar con todos los productos Wireless-B (802.11b) de 11 Mbps del hogar, la oficina y establecimientos públicos con conexiones inalámbricas de todo el país. Sea cual sea la opción que elija, las comunicaciones inalámbricas están protegidas por encriptación de 128 bits, por lo que los datos permanecen seguros.

Figura 3.6: Linksys 54Mbps/2.4GHz PCI con chip BROADCOM

Precio: 14 USD

Fuente: http://articulo.mercadolibre.com.mx/MLM-20381271-tarjeta-red-inalambrica-linksys-pci-54mbps-11b-y-11g-dn8-_JM

3.3.2.1 Características:

- Funciona en el espectro de secuencia de 2,4 GHz, con rendimiento de hasta 54 Mbps
- Cumple con el borrador de los estándares 802.11g de IEEE y es compatible con productos 802.11b de IEEE.
- Encriptación WEP de hasta 128 bits

- Interfaz PCI de 32 bits
- Compatible con Windows 98 SE, Millennium, 2000, XP y VISTA

3.3.3 Antena (Linksys)

Con la antena externa HGA7S, es posible extender considerablemente el alcance de la red inalámbrica. [107]

La antena omnidireccional HGA7S utiliza la tecnología de transmisión inalámbrica 2,4 GHz para ofrecer una cobertura más importante, y minimizar los riesgos de interferencias provocados por obstáculos naturales o por las molestias causadas por las frecuencias de algunos aparatos en funcionamiento.

La antena WiFi HGA7S es un repetidor muy eficaz para una red inalámbrica sin límites.

Figura 3.7: Antena HGA7S Largo Alcance para Conexiones R-SMa

Precio 50 USD

Fuente: http://www.pixmania-pro.com/es/es/linksys/antena-wifi-hga7s-7-dbi/503464/fiche.html#tech-desc

[107] http://www.pixmania-pro.com/es/es/linksys/antena-wifi-hga7s-7-dbi/503464/fiche.html#tech-desc

3.3.3.1 Especificaciones Técnicas

- Fácil instalación: simplemente reemplaza a la antena corriente.
- Trabaja con ambos dispositivos Wireless-G y Wireless-B.
- Cobertura: 7DBi
- Rango de Frecuencia: 2.4GHz ~ 2.5GHz
- Voltage Standing Wave Ratio (VSWR) 1.92 Max.
- Polarización Linear Vertical
- Dirección Omni-Directional
- Impedance 50 ohm Nominal
- Connector Reverse SMA

3.3.4 Router (Linksys)

El compacto router Wireless-G Broadband de Linksys combina tres dispositivos en uno - router, switch y punto de acceso. Combina LAN y WLAN en una red con un cable de alta velocidad o conexión DSL a Internet. Además, el WRT54G2 ofrece encriptación WPA/WPA2 Personal.

Figura 3.8: Router WRT54G2 Linksys

Precio: 60 USD

Fuente: http://www.rigg.cl/riggweb/store/product.jsp?product=1995

3.3.4.1 Características:

- Estándares: IEEE 802.3
  IEEE 802.3u
  IEEE 802.11g
  IEEE 802.11b

- Conexiones: 4 x RJ-45 (LAN)
  1 x RJ-45 (WAN)
  1 x fuente de alimentación

- Luces: Power (Alimentación)
  Ethernet (1-4)
  Internet
  Wireless (Inalámbrico)
  Security (Seguridad)

- Tipo de cables: CAT 5
- Nº de antenas: 2 antenas internas
- Potencia de radiofrecuencia (EIRP) en dBm: 18 dBm
- Alimentación: 12V DC, 0.5ª
- Certificación: FCC, UL, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM

3.3.5 Cámara de vigilancia IP

El modelo WVC54GC de Linksys, cuyo nombre comercial es Compact Wireless-G Internet Video Camera, es una cámara IP que además de ofrecer las características propias de dicha tecnología emplea tecnología inalámbrica IEEE 802.11g.[108]

Incluye una base atornillable que se coloca sin necesidad de herramientas, cuenta con una ranura adicional en la parte trasera para sujetar la base cuando la cámara se colocará en un muro. Por su parte, la base circular cuenta, en su parte inferior, con dos ranuras para sujetarla con tornillos fijos en paredes o techo; de este modo la cámara puede montarse prácticamente en cualquier sitio o, bien, permanecer sobre una superficie plana.

[108] http://www.esemanal.com.mx/articulos.php?id_sec=4&id_art=3919

El software busca y detecta la cámara en la red y, una vez localizada, muestra su configuración de red, incluyendo su dirección IP, nombre, canal inalámbrico y opciones de seguridad; estas últimas se encuentran desactivadas por defecto.

Figura 3.9: WVC54GC Compact Wireless-G Internet Video Camera

Precio: 160USD

Fuente: http://www.esemanal.com.mx/articulos.php?id_sec=4&id_art=3919

3.3.5.1Características:

Tipo de dispositivo: Cámara de red

- **Dimensiones (Ancho x Profundidad x Altura):** 9 cm x 3.7 cm x 10.2 cm
- **Peso:** 0.1 kg
- **Localización:** Europa
- **Cámara:** Color
- **Tipo sensor óptico:** CMOS
- **Ajuste de foco**: Sin foco
- **Interfaces:** Ethernet 10Base-T/100Base-TX, IEEE 802.11b, IEEE 802.11g
- **Características:** Sensor de movimiento, impresión de fecha y hora, control de brillo, alertas de correo electrónico
- **Cables incluidos**: 1 x cable de red - externo
- **Requisitos del sistema:** Microsoft Windows 98SE/2000/ME/XP
- **Accesorios incluidos:** Base

3.4 SOLUCIONES D-LINK

D-Link, de origen taiwanés, es la principal empresa que desarrolla, fabrica y comercializa productos de networking para el mercado SMB, SOHO y grupos departamentales de grandes corporaciones. Posee plantas de producción en Estados Unidos, Taiwán, China e India; Centros de Investigación y Desarrollo en los mismos países mencionados anteriormente; y la capacidad de entregar soluciones de conectividad a un precio atractivo, la empresa ha sido rentable en cada año desde su fundación en 1986, y continúa teniendo altas tasas de crecimiento.[109]

D-Link complementa las alternativas de soluciones de redes con una amplia oferta de opciones que permiten la comunicación. Con los cimientos básicos conexión de banda ancha a Internet, conexiones inalámbricas, actualizaciones que mejoran el rendimiento de la red

D-Link está presente en cada paso del camino de crecimiento de la red, satisfaciendo las necesidades de la familia y la pequeña empresa. Integrando tecnología switch, wi-fi de alto rendimiento, servidor de internet y de impresión en dispositivos de alta funcionalidad.[110]

3.4.1 Switch 8 Puertos

- **General**

  El switch DES-1008D es un switch de alto rendimiento y gran versatilidad. Está diseñado para reforzar el rendimiento del SOHO y la pequeña empresa, otorgando flexibilidad y manejo a 10/100Mbps. Está provisto de 8 puertas auto-detect, lo que permite que grupos de trabajo aumenten el rendimiento en la red.

[109] http://www.dlinkla.com/home/news_desk/dlink_comunicado.jsp?id_comunicado=181

[110] http://www.dlinkla.com/home/soluciones/express.jsp

- **8 Puertas 10/100Mbps**

  Este switch provee de 8 puertas con soporte al estándar Nway, conectores: RJ-45. Las puertas tienen la capacidad de negociar las velocidades de red entre 10BASE-T y 100BASE-TX, como también el modo de operación en Half o Full Duplex.

- **Control de Flujo**

  La arquitectura de Parallel Switching para el modo de operación Store&Fordward, permite la transferencia de datos en forma directa entre las distintas puertas, con Full Error Checking, eliminando en el tráfico de la red el envío de Paquetes Incompletos, Fragmentados o con Errores de CRC, salvaguardando de esta forma la integridad de los datos.

- Estándares

  IEEE 802.3 10Base-T Ethernet Repeater, IEEE 802u 100Base-TX class II Fast Ethernet repeater y ANSI/IEEE Std 802.3 Nway auto-negotiation

- Características Físicas

  Tamaño: Palm-Size

  Dimensiones:

  - 197 x 115 x 28 mm Modelo Rev. C2
  - 171 x 98 x 29 mm Modelo Rev. D1

  Peso: 1,5 Kg

- Temperatura de Operación : 0ºC a 55ºC
- Temperatura de Almacenaje : -25ºC a 55ºC
- Emisión(EMI)

  EMI: CE Class A, C-Tick Class A, FCC Class A, VCCI Class A, BSMI class A

- Seguridad : UL/CUL

Figura 3.10: JD-LINK DES-1008D SWITCH 8 PUERTOS 10/100MBPS

Precio: 50 USD

Fuente: http://www.expansys.es/p.aspx?i=105686

3.4.1.1 Principales Características y Facilidades

• Velocidad de Transmisión de hasta 54Mbps, en 2.4GHz
• Compatible con productos que operen bajo el estándar 802.11b y 802.11g

• Seguridad Avanzada, WPA
• DHCP Server
• Fácil Instalación,
• Alto Rendimiento, y
• Fácil integración en red.

La máxima señal de transferencia inalámbrica está basada en las especificaciones del estándar IEEE 802.11g. La transferencia de datos puede variar. Las condiciones de la red y factores ambientales, incluyendo el volumen del tráfico de datos, materiales de construcción de edificaciones, entre otros factores, puede afectar y bajar el rango de transmisión inalámbrica. [111]

[111] http://www.dlinkla.com/home/productos/producto.jsp?idp=711

3.4.2 Tarjeta de red (D-LLINK)

Adaptador Inalámbrico PCI DWA-510. Una vez que se establece la comunicación con la red inalámbrica, se puede navegar a través de la conexión a Internet y además, compartir documentos, música, y fotos con otros computadores dentro de la red. El adaptador DWA-510 permite dotar de conectividad inalámbrica a un PC de escritorio de la manera más fácil, cómoda y sencilla, ya sea en el hogar o en la oficina.

Figura 3.11: DWA-510 Wireless G PCI Adapter 54mbps

Precio: 18 USD

Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=1009

3.4.2.1 CARACTERÍSTICAS PRINCIPALES

- Adaptador inalámbrico PCI para computadores de escritorio, que permite conexiones inalámbricas 802.11g a 54Mbps.[112]

- Compatible con otros dispositivos inalámbricos anteriores 802.11b para garantizar la plena interoperabilidad entre los productos nuevos y los ya existentes.

- Seguridad avanzada: Encriptación WEP y WPA/WPA2-PSK, WPA/WPA2-EA.

- Fácil instalación y alto rendimiento. Configurador amigable Quick Router Setup.

[112] http://www.dlinkla.com/home/productos/producto.jsp?idp=1009

• Incorpora como mecanismo de seguridad los estándares de encriptación WEP y WPA/WPA2-PSK, WPA/WPA2-EA, que permiten establecer la conexión con una amplia gama redes inalámbricas

• Está basado en el estándar 802.11g para establecer la comunicación y además es compatible con el estándar anterior 802.11b

• El asistente de configuración rápida de D-Link Quick Router Setup, le guía paso a paso a lo largo del proceso de instalación. La nueva utilidad de configuración de D-Link, descubre redes inalámbricas disponibles en el ambiente y se conecta a ellas de manera rápida y segura.

3.4.3 WIRELESS ROUTER D-Link DI-634M

El Wireless Router D-Link DI-634M es una solución potenciada con tecnología MIMO, con la cual se puede crear una red inalámbrica robusta, que proporciona un excelente rendimiento y extiende el rango de cobertura a la vez que mantiene los beneficios de la conectividad inalámbrica.
Esta solución permite implementar aplicaciones que demandan un gran ancho de banda, tales como audio y video streaming, juegos en-línea y grandes transferencias de archivos.

Extiende el rango de operación inalámbrica: Al operar en una banda de frecuencia de 2.4GHz, la información que se transmite desde el wireless router DI-634M se traspasa a través de múltiples antenas de alta ganancia. Las señales de radio generalmente reflejan objetos, creando múltiples senderos que en radios convencionales generan interferencia. El DI-634M usa estos senderos para transportar mayor información, lo cual es recombinado en el lado del receptor por algoritmos MIMO. Como resultado, el DI-634M reduce la caída de la señal en ciertos lugares y distribuye fuertes señales inalámbricas a mayores distancias, con suficiente ancho de banda para transmitir contenidos multimedia y archivos de mayor peso.

Hasta 108Mbps de velocidad inalámbrica: El Wireless Router DI-634M duplica la eficiencia espectral comparada con las redes inalámbricas actuales. La máxima tasa de transferencia no turbo para el estándar 802.11g es de 54Mbps, por lo que el throughput actual es cercano a los 20 o 30Mbps. Esto es mejorado con la solución en modo Turbo del DI-634M permitiendo aumentar la tasa de transferencia a 108Mbps, con un throughput real 8 veces más rápido que en equipamientos 802.11g.

Protección de inversión: Al tener compatibilidad con los estándares de la industria 802.11g y 802.11b, el DI-634M puede operar simultáneamente con los dispositivos existentes inalámbricos. El usuario no tiene que reemplazar los dispositivos inalámbricos actuales con que opera en la red para experimentar los beneficios de extender el rango y llegar a velocidades turbo con este wireless router.

Seguridad de la red: El D-634M proporciona protección NAT y SPI (Stateful Packet Inspection), además de control familiar para monitorear y mantener el uso de la Internet. Todas estas características más funciones avanzadas tales como system logging, DHCP estático, VPN pass-trough y herramientas de diagnóstico permiten tener una red completamente segura.

Seguridad inalámbrica: El Wireless Router DI-634M soporta el estándar WEP y el avanzado WPA-Personal data encryption (WPA-PSK). De forma adicional incluye características de seguridad como MAC e IP Filtering para limitar el acceso a la red basada en MAC Address o IP Address. Para prohibir intrusos a la red, el DI-634M también puede ser configurado en modo invisible y así el nombre de la red SSID no puede ser encontrado por clientes inalámbricos externos.

3.4.3.1 CARACTERÍSTICAS PRINCIPALES

- 1 puerto 10/100 WAN
- 4 puertos 10/100 LAN
- 4 Antenas MIMO: 2 internas y 2 externas
- Extiende el rango de operación de una red inalámbrica: Hasta 8 veces
- Protección de la Inversión: Compatible con productos que operen bajo el estándar 802.11b y 802.11g, y todos los productos wireless de D-Link,
- Seguridad de acceso de red: Protección NAT y SPI (Stateful Packet Inspection), control familiar.
- Seguridad inalámbrica Avanzada: WEP y WPA, Filtro por MAC e IP
- Funcionalidades de Firewall, DMZ host y Soporte VPN Pass-through,
- DHCP Server
- Fácil Instalación gracias al Soporte de UPnP,
- Alto Rendimiento, y
- Fácil integración en red.

Figura 3.13: WIRELESS ROUTER D-Link DI-634M

Precio: 180 USD

Fuente:http://tienda.jmo.cl/product_info.php?manufacturers_id=21&products_id=2120&osCsid=92210081feacf86ac8ad11b935e51929

3.4.4 Cámara de vigilancia IP DCS 5300 (D-LINK)

- Soporte PAN/TILT
- Sistema de monitoreo autónomo gracias a su Servidor Web Integrado.
- Monitoreo Remoto vía Web.
- Monitoreo de múltiples cámaras vía Software Windows, hasta 16 en forma simultánea.
- Activación de grabado de video, ante detección de movimiento.
- Puerto de I/O para comunicación hacia dispositivo externo.
- Soporte UnPnP y DDNS.
- Salida de audio y video, para conexión hacia televisor.
- Implementación de sistema de video vigilancia.
- Interfaces: 1 Puerto RJ-45 auto-sensing Fast Ethernet 10/100 MBPS.
- Resolución: 640 X 480 pixeles.
- Imagen: Modo compresión MPEG4, short header, Tamaño de imagen ajustable, quality y bit-rate.
- Audio: 8 KBPS.
- Detección de movimiento: Sí
- Alimentación: 12 VDC 1.5A. External universal power adapter (100 to 240 VAC, 50/60Hz).
- Control remoto: Sí para direccional la cámara hacia el objetivo deseado.
- Consumo de energía: 18 watts.

Figura 3.14: DCS-5300 SECURITY CAM IP

Precio: 450 USD

Fuente:http://www.mundoyaos.com/index.php?page=shop.product_details&flypage=shop.flypage&product_id=77&category_id=31&manufacturer_id=0&option=com_virtuemart&Itemid=4

3.4.4 Cámara de vigilancia IP DCS 5300 (D-LINK)

La cámara de seguridad de D-Link DCS-2100, está diseñada como un sistema de seguridad y monitoreo autónomo, que permite observar remotamente, desde el hogar u oficina, un lugar determinado a monitorear. Con todas las facilidades, la cámara DCS-2100 puede ser conectada a cualquier red Ethernet en una Oficina o Campus o a Internet de Banda Ancha, vía un DI-704UP (Internet Server) por ejemplo. La cámara provee una alta calidad de video, además tiene incorporado un Servidor Web y detecta movimiento para grabar. Adicionalmente incorpora gratuitamente un poderoso software para monitoreo y administración de múltiples cámaras. La cámara DCS-2100 es la solución de video vigilancia con la mejor relación costo/efectividad del mercado, ideal y conveniente para el SOHO.

La cámara de seguridad de D-Link DCS-2100, está diseñada como un sistema de seguridad y monitoreo autónomo, que permite observar remotamente, desde el hogar u oficina, un lugar determinado a monitorear. Con todas las facilidades, la cámara DCS-2100 puede ser conectada a cualquier red Ethernet en una Oficina o Campus o a Internet de Banda Ancha, vía un DI-704UP (Internet Server) por ejemplo. La cámara provee una alta calidad de video, además tiene incorporado un Servidor Web y detecta movimiento para grabar. Adicionalmente incorpora gratuitamente un poderoso software para monitoreo y administración de múltiples cámaras. La cámara DCS-2100 es la solución de video vigilancia con la mejor relación costo/efectividad del mercado, ideal y conveniente para el SOHO.

Características

- Sistema de monitoreo autónomo gracias a su Servidor Web Integrado,
- Monitoreo Remoto vía Web
- Monitoreo de múltiples cámaras vía Software Windows, hasta 16 en forma simultanea
- Activación de grabado de video ante detección de movimiento
- Fácil y rápida implementación de sistema de video vigilancia.
- Zoom digital de 4x

- Soporte de UPnP & DNS

Figura 3.15: DCS-2100 SECURITY CAM IP

Precio: 172 USD

Fuente: http://braincorp.com.ve/tienda/camara-de-seguridad-dlink-dcs2100-dcs2100-p-4555.html?osCsid=86f019846800bcb23082ee166ddba490

Tabla 3.2: Características de las posibles soluciones

Descripción	3Com Wireless LAN Managed Access Point AirConnect	Linksys Wireless-G Access Point WAP54G	D-Link Wireless Router MIMO DI-634M
Velocidad de transferencia de datos	54 Mbps	54 Mbps	54 Mbps
Formato código de línea:	OFDM	DBPSK, DQPSK, CCK, OFDM	DBPSK, DQPSK, CCK, 64 QAM, BPSK, QPSK, 16 QAM, OFDM
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g	IEEE 802.11b, IEEE 802.11g	IEEE 802.11b, IEEE 802.11g
Banda de frecuencia:	----	2.4 GHz	2.4 GHz
Protocolo de gestión remota:	Telnet, HTTP, HTTPS	HTTP	HTTP
Indicadores de estado:	Actividad de enlace, alimentación, estado	Actividad de enlace, alimentación, tinta OK	Estado puerto, actividad de enlace, alimentación
Características: especiales	Criptografía 128 bits, VPN, negociación automática, soporte VLAN, activable, repliegue automático	Auto-sensor por dispositivo, negociación automática, señal ascendente automática (MDI/MDI-X automático), filtrado de dirección MAC, actualizable por firmware, log de eventos	Auto-sensor por dispositivo, negociación automática, modo de repetición, filtrado de dirección MAC, 4 antenas cumple la función de wireless y Router
			AES, WEP de 128 bits,

Algoritmo de cifrado:	AES, SSL, WEP de 104 bits, TKIP, WPA	WEP de 128 bits, encriptación de 64 bits WEP, WPA	encriptación de 64 bits WEP, TKIP, WPA, WPA2, WPA-PSK
Método de autentificación	RADIUS, Identificación de conjunto de servicios de radio (SSID), Secure Shell v.2 (SSH2)	Identificación de conjunto de servicios de radio (SSID)	Identificación de conjunto de servicios de radio (SSID)
Cumplimiento de normas:	IEEE 802.3, IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 802.11i, Wi-Fi CERTIFIED	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g, Wi-Fi CERTIFIED
Antena: **Cantidad de antenas:** **Directividad:** **Nivel de ganancia:**	Externa integrada 2 Omnidireccional 2 dBi	Externa desmontable 2 Omnidireccional	Externa desmontable 1 Omnidireccional 2 dBi
Expansión / conectividad	1 x red – Radio Ethernet 1 x red - Ethernet 10 Base - T/100Base - T x Rj45 1 x gestión - D-Sub de 9 espigas (DB-9)	1 x red - Radio Ethernet 1 x red - Ethernet 10 Base - T/100Base - T x Rj45	1 x red - Radio Ethernet 1 x red - Ethernet 10 Base - T/100Base - T x Rj45
Power Over Ethernet (PoE)	Incluido	Adaptable	----
Garantía del fabricante	1 año de garantía	3 años de garantía	3 años de garantía

Fuente: Santiago Maldonado

CAPITULO 4

4.1 IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED INALÁMBRICA WLAN, Y CÁMARAS DE SEGURIDAD IP PARA HOSTAL LA CAROLINA

La alternativa más eficaz para dar solución a las necesidades planteadas, es la implementación y configuración de una red inalámbrica WLAN y de cámaras de seguridad IP, esto satisface los requerimientos actuales y futuros.

4.2 FACTORES DE DISEÑO

Factores que hay que tomar en consideración para la implementación y configuración de una red WLAN y cámaras de seguridad IP:

- Ancho de banda/Velocidad de transmisión.
- Compatibilidad con la red existente.
- Tipos de aplicaciones que van a correr en la WLAN y cámaras de seguridad IP.
- Área de cobertura.
- La señal
- Escalabilidad
- Conexión de la WLAN con la red cableada.
- Disponibilidad de productos en el mercado.
- Costes
- Planeación y administración de las direcciones IP.
- Seguridad.

Todos estos aspectos están señalados en el capítulo 3.

4.3 DEFINICIÓN DE EQUIPOS

La marca seleccionada de los equipos (Switch, Wíreles Router, cámaras), será D-Link porque cumple con las especificaciones técnicas y garantías de acuerdo a los requerimientos necesarios para brindar una buena señal como se indica en el capitulo 3. El número de dispositivos de cada tipo es el siguiente:

- 1 Switch D-Link
- 1Wireless Router D-Link
- 5 Cámaras D-Link
- PC servidor

4.3.1 ANÁLISIS DE UBICACIÓN DE EQUIPOS PARA LA RED WLAN Y CÁMARAS IP.

Todos los equipos que forman parte de la red WLAN (switch, PC Servidor) serán ubicados en Gerencia, ya que es un área segura y de esta nace la red. Mientras que el Wireless Router estará ubicado en el segundo piso.

Para realizar un monitoreo de las diferentes áreas de Hostal La Carolina se ha tomado en cuenta las siguientes referencias.

La cantidad de cámaras instaladas deben permitir un monitoreo adecuado, es decir el número de cámaras no debe ser excesivo.

La mayor parte de cámaras se instalarán en áreas de acceso, ingreso de puertas principales, zonas de circulación.

Analizados los puntos críticos, donde se necesita que el sistema de cámaras ayude a incrementar la seguridad se tiene:

TABLA 4.1: UBICACIÓN DE CÁMARAS (REFERENCIA)

UBICACIÓN	NÚMERO DE CÁMARAS
Recepción CAM 1	1
Cocina CAM2	1
Primer piso CAM3	1
Segundo Piso CAM4	1
Tercer Piso CAM5	1

Fuente: Santiago Maldonado

4.3.1.1Recepción

Esta cámara debe tener una cobertura de 180 grados ubicada en la parte central de la recepción, donde se puede visualizar los puntos críticos a ser monitoreados. También tiene la capacidad de detección de movimiento en el día y noche con zoom, la instalación se realizará desde Gerencia donde está el PC administrador

4.3.1.2 Cocina

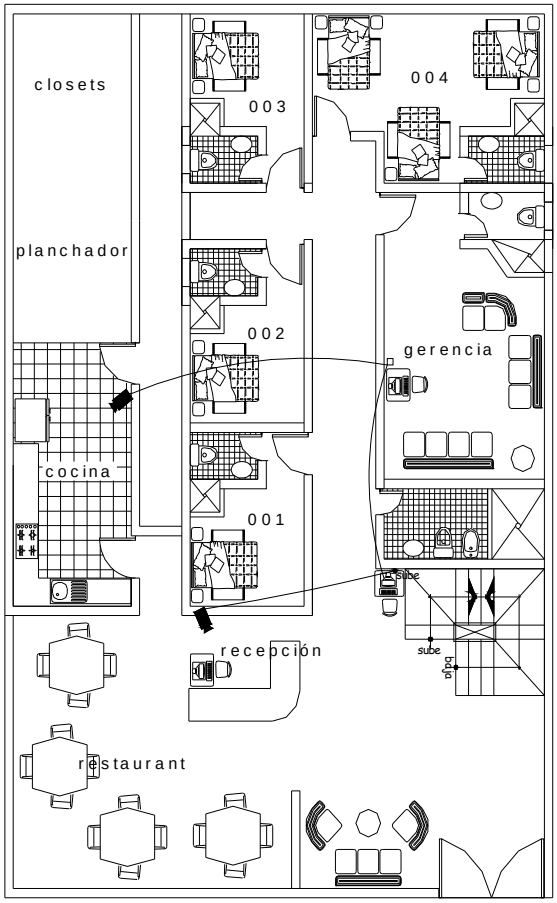
Esta cámara se ubica en un área que permita la supervisión de la actividad laboral del personal que trabaja en cocina.

4.3.1.3 Primer, Segundo y tercer piso

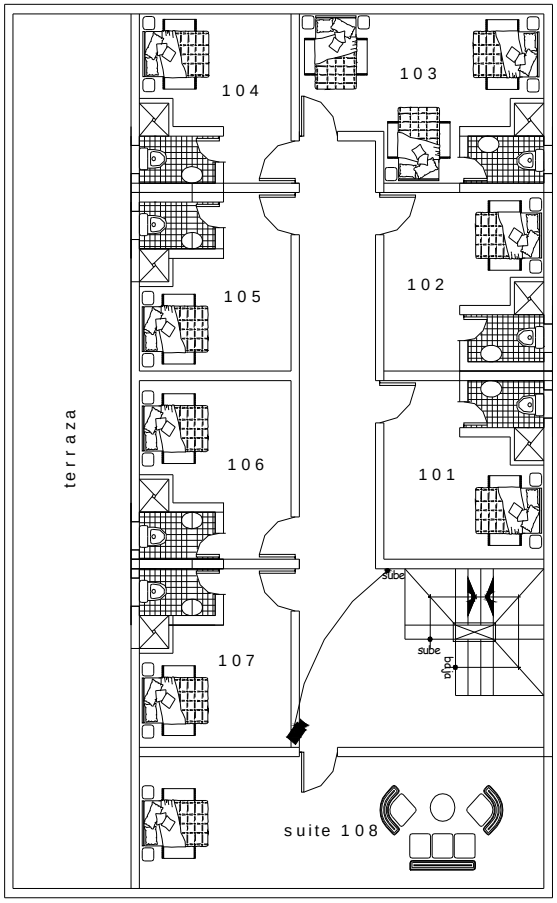
Esta cámara se debe ubicar en la parte superior de los pacillos del primer, segundo y tercer piso donde están las puertas de ingreso a las habitaciones. El cable para estas cámaras debe ser instalado desde gerencia, esta cámara debe tener la propiedad de poder realizar zoom de las imágenes monitoreadas y zoom de las imágenes grabadas.

4.4 DISEÑO FÍSICO

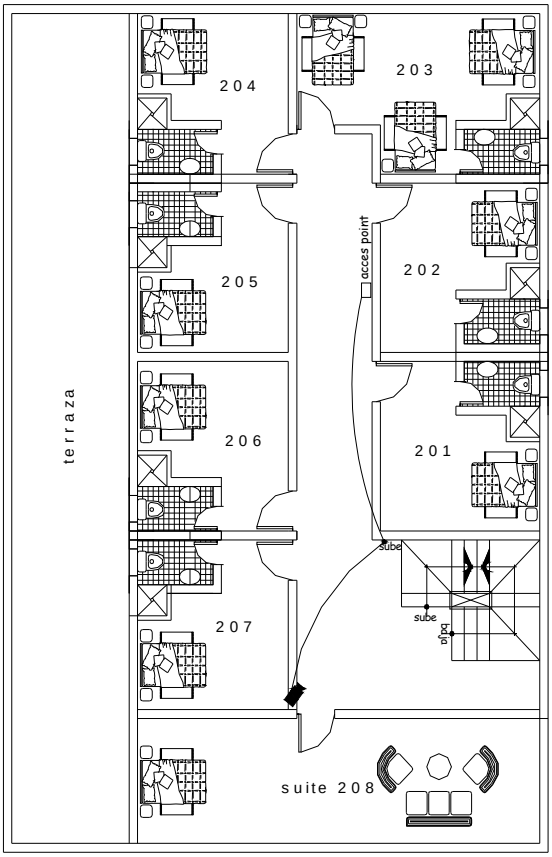
planta baja



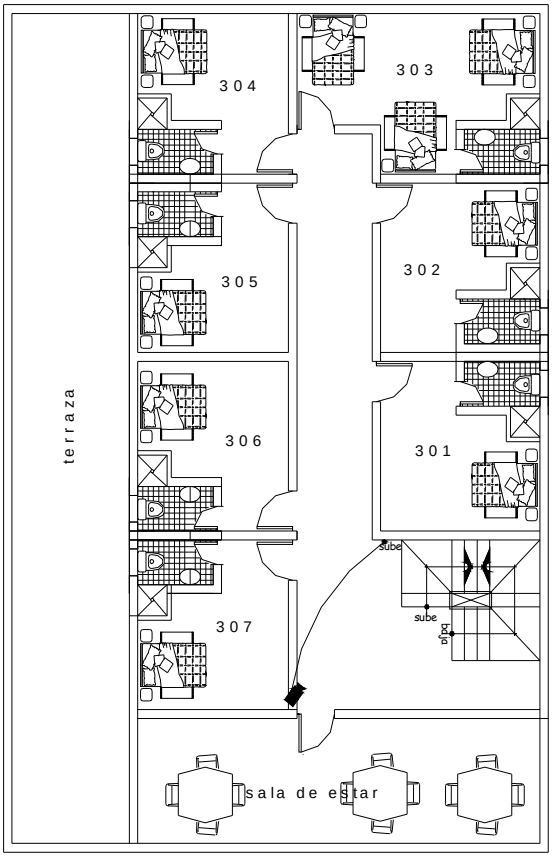
primer piso



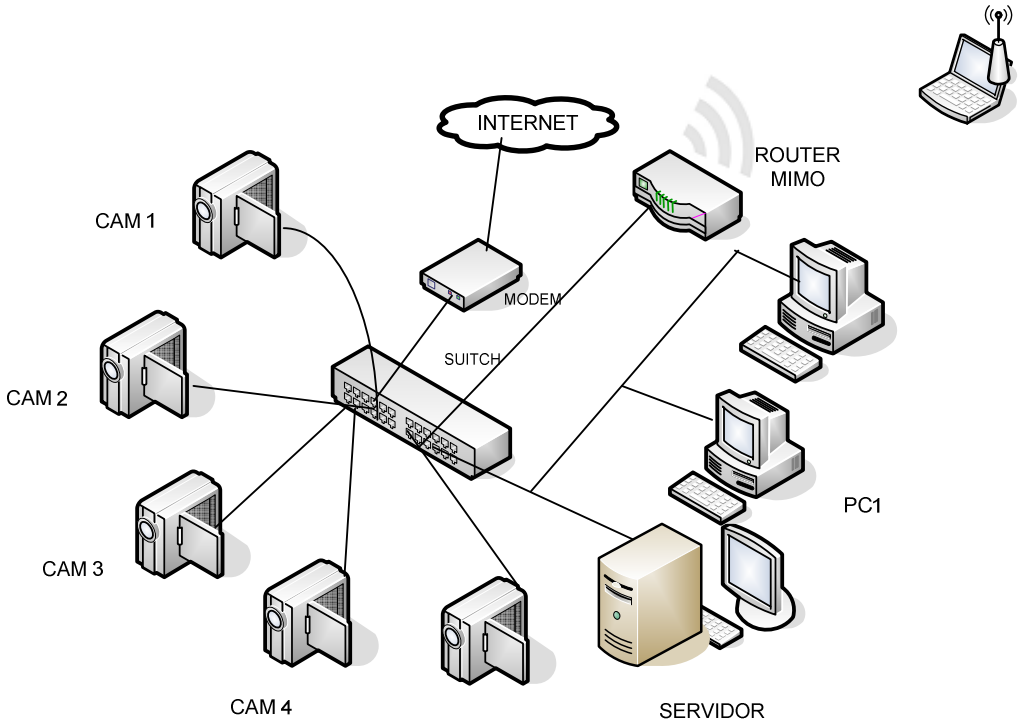
segundo piso



tercer piso



4.5 DISEÑO LÓGICO



4.6 Conexión de la WLAN con la red cableada:

Debemos tener en cuenta que los puntos de acceso necesitan electricidad para poder operar, y además, deben estar conectados a la red cableada (par trenzado). Se recomienda instalar el punto de acceso en lugares estratégicos sin olvidarse de éstas dos conexiones.

4.7 COSTO TOTAL DEL PROYECTO

Una vez revisadas las características de los equipos se procede a mencionar la proforma, y luego de una análisis a la compra de los mismos. De acuerdo a lo revisado se tiene:

4.7.1 Proforma

Tabla 4.2: Lista de precios

Cant.	Descripción	P. U.	P. Total
1	D-Link DCS 5300 Camera	450	450 USD
4	D-Link DCS 2100 Camera	172	688 USD
1	WIRELESS ROUTER D-Link DI-634M	150	150 USD
1	PC Servidor (clon)	800	800 USD
1	Switch DES-1008D D-Link	70	70 USD
6	Puntos eléctricos	15	90 USD
1	Cable UTP (90 m)	0.55	49.50 USD
1	Mano de obra (implementación)	400	400 USD
	Total sin IVA		2697.5 USD

4.8 IMPLEMENTACIÓN

4.8.1 Implementación Tendido de cables

Se procede al tendido de cable UTP, que parte de los equipos ubicados en Gerencia, se tiende cable con canaletas a cada cámara, esto es en recepción, cocina; primer, segundo y tercer piso y al wireless Router que esta ubicado en el segundo piso (aproximadamente 90m), esto se lo realiza en cuatro días de trabajo.

4.8.2 Implementación de Cámaras y Wireless Router

Una vez instalados los cables UTP y las tomas de corriente eléctrica, se procede a la conexión de cámaras y de Wireless Router en los lugares planificados y estratégicos.

4.8.2.1 Ilustración Montaje de equipos

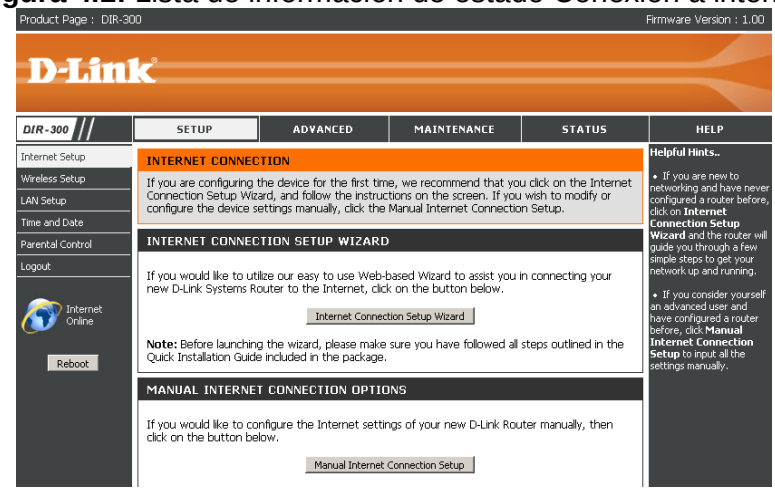
Fuente: Fotos de la implementación de equipos

4.9 CONFIGURACIÓN

4.9.1 Configuración WIRELESS ROUTER DLINK

1.-En esta pantalla se puede elegir la forma de instalación del internet ya sea con el asistente o manualmente, en este caso se ha elegido la opción "manualmente".

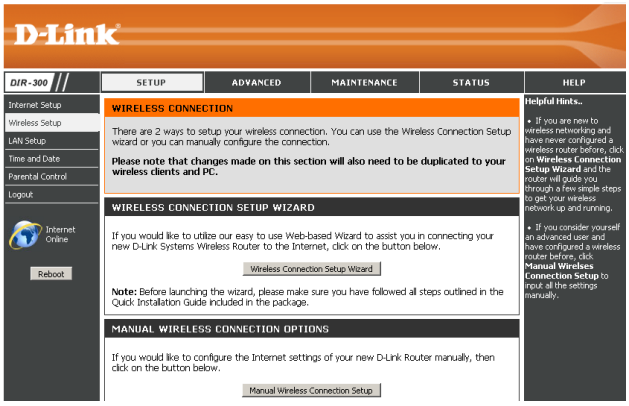
Figura 4.1: Lista de información de estado Conexión a internet



Fuente: Captura de Pantalla

2.- En esta pantalla se puede elegir la forma de instalación del Wireless ya sea con el asistente o manualmente, en este caso se ha elegido la opción "manualmente"

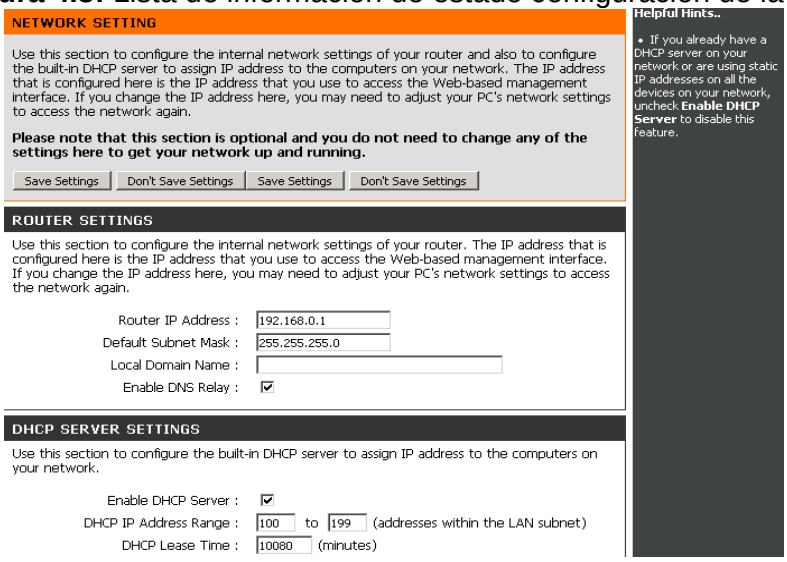
Figura 4.2: Lista de información de estado Conexión Wireless



Fuente: Captura de Pantalla

3.-En la pantalla de “configuración de la red” asignamos las direcciones IP del router así como las mascaras de subred.

Figura 4.3: Lista de información de estado configuración de la red

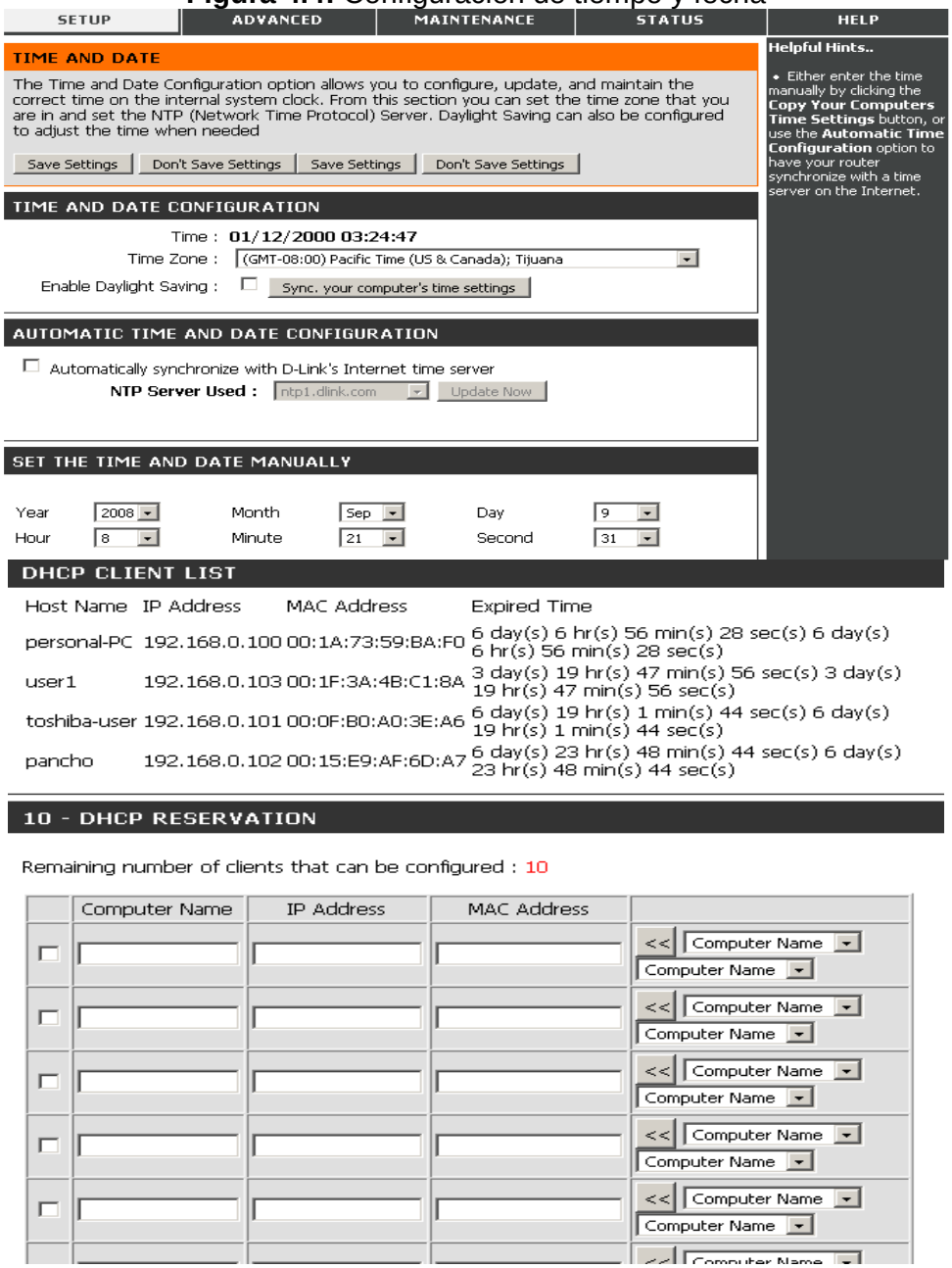


Fuente: Captura de pantalla

4.-En esta pantalla mantenemos actualizado la fecha y hora del router ya sea manualmente o automáticamente mediante conexión con el servidor de la casa fabricante del router.

En esta pantalla también se asigna las IP's de los clientes que van acceder mediante DHCP

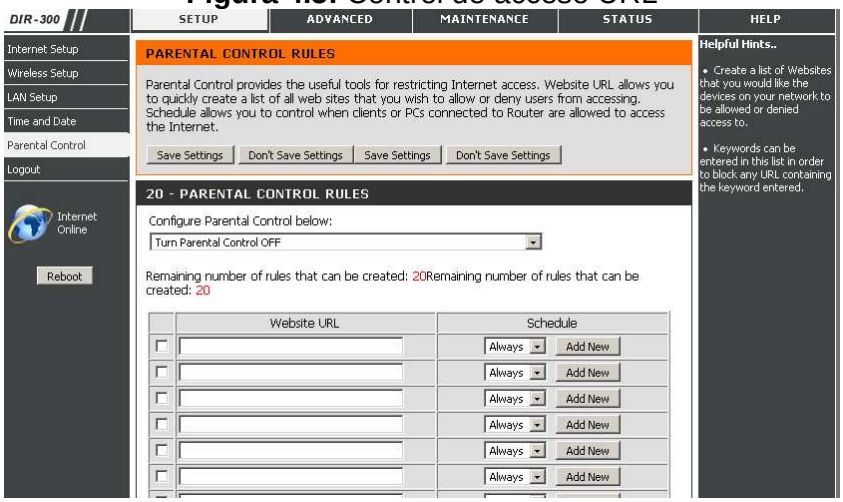
Figura 4.4: Configuración de tiempo y fecha



Fuente: Captura de pantalla

5.- Esta es la pantalla de control para padres, aquí se restringe páginas que no deseamos que nadie acceda, escribiendo la dirección URL, así como el horario en que estas pueden ser restringidas.

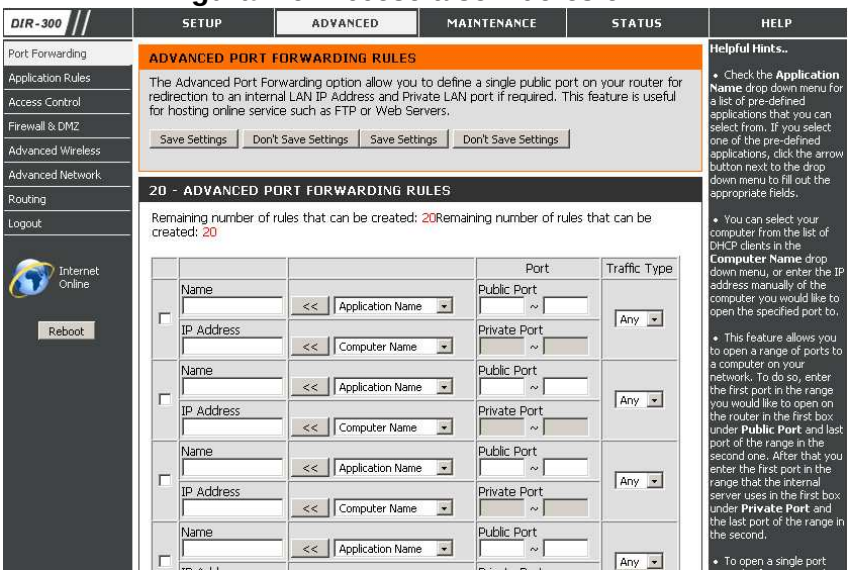
Figura 4.5: Control de acceso URL



Fuente: Captura de pantalla

6.- Aquí definimos los puertos públicos o privados del router, estas opciones nos permiten acceder a servidores web o FTP's

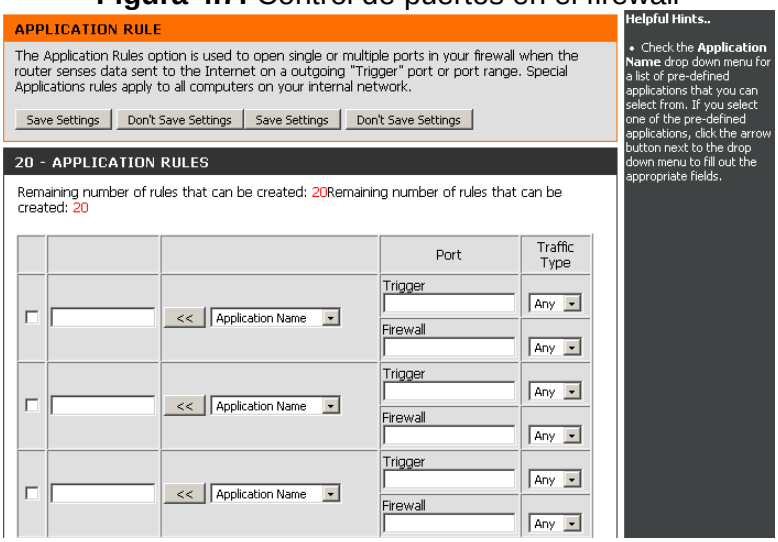
Figura 4.6: Acceso a servidores o FTP



Fuente: Captura de Pantalla

7.-Aquí se abre uno o varios puertos en nuestro Firewall

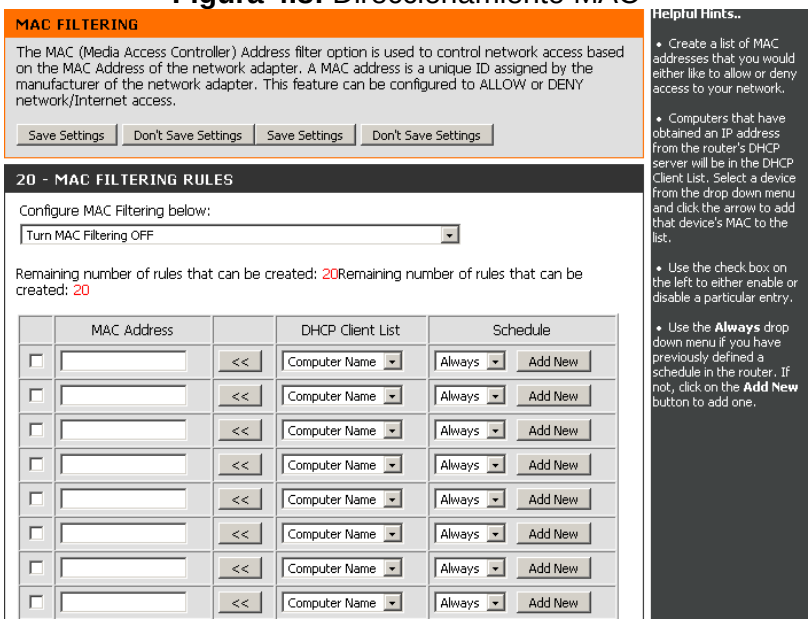
Figura 4.7: Control de puertos en el firewall



Fuente: Captura de pantalla

8.- Aquí asignamos las direcciones MAC, las cuales permiten o niegan el control de acceso a la red o Internet

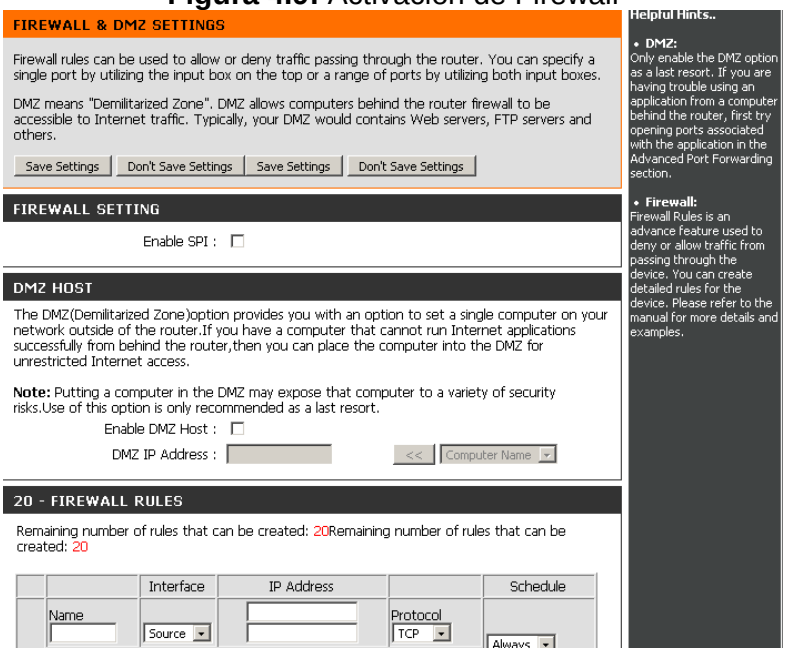
Figura 4.8: Direccionamiento MAC



Fuente: Captura de pantalla

9.- En esta pantalla es la activación del firewall

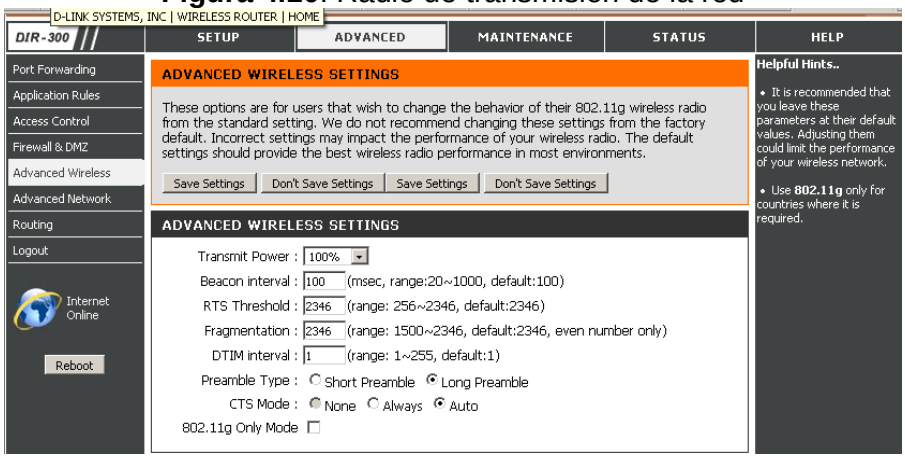
Figura 4.9: Activación de Firewall



Fuente: Captura de pantalla

10.-En esta página no se recomienda hacer cambios ya que vienen preestablecidos por la fabrica, aquí se designa el radio de transmisión de la red inalámbrica.

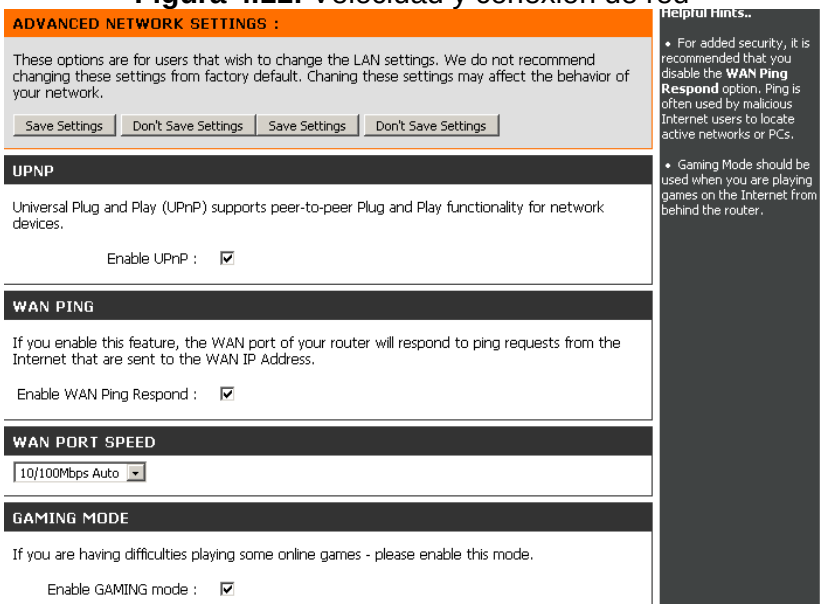
Figura 4.10: Radio de transmisión de la red



Fuente: Captura de pantalla

11.- Al igual no se recomienda cambiar las configuraciones ya preestablecidas por la casa fabricante ya que pueden afectar la conexión de la red.

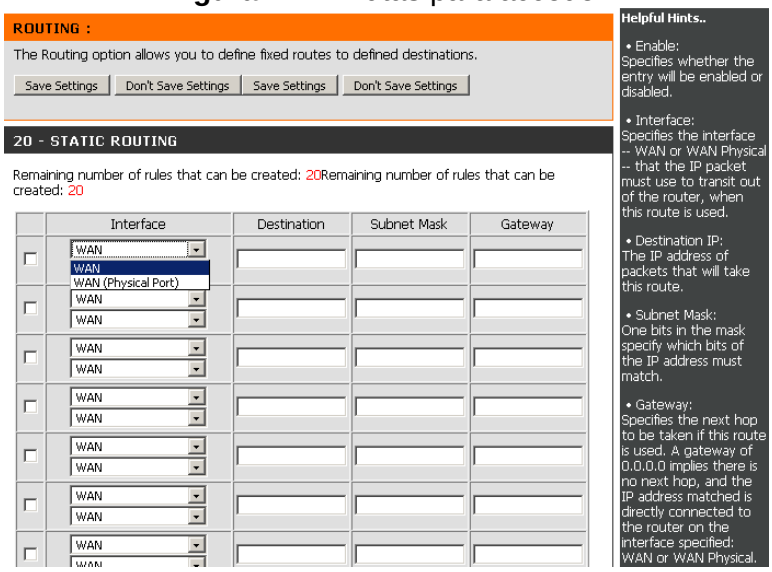
Figura 4.11: Velocidad y conexión de red



Fuente: Captura de pantalla

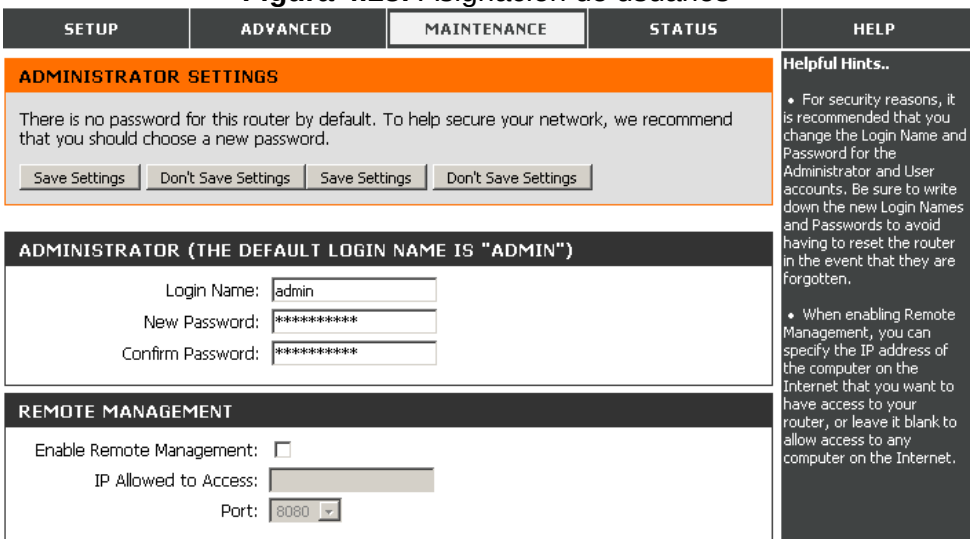
12.- Aquí definimos las rutas y destinos que vamos a permitir que se puedan acceder por la red

Figura 4.12: Rutas para acceder



13.- La pagina del administrador, aquí designamos el nombre de usuario con sus respectivas claves de acceso, así como podemos habilitar un acceso remoto ingresando su puerto

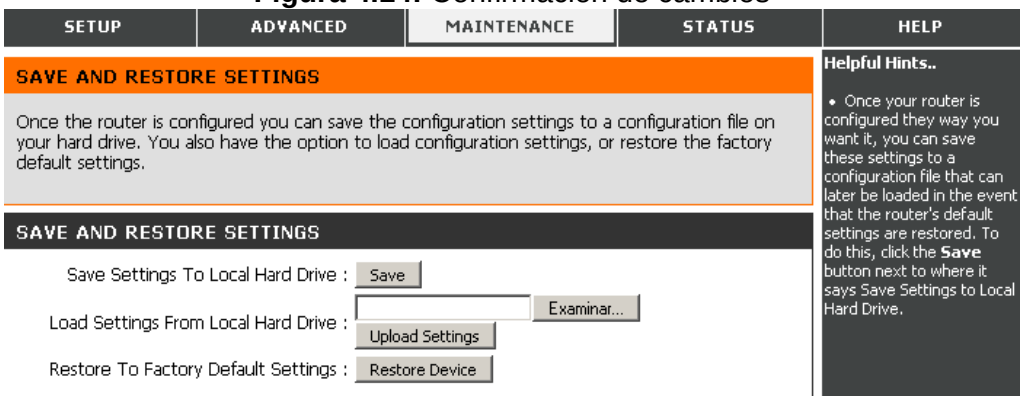
Figura 4.13: Asignación de usuarios



Fuente: Captura de pantalla

14.- Aquí guardamos los cambios realizados o cargamos una configuración preestablecida con anterioridad

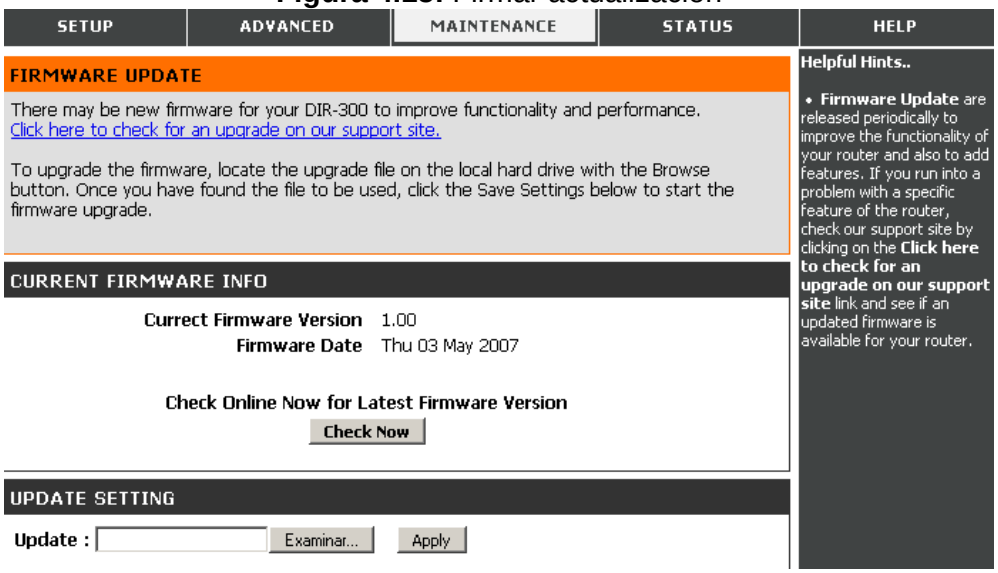
Figura 4.14: Confirmación de cambios



Fuente: Captura de pantalla

15.- En esta página podemos actualizar el software de configuración del router mediante internet.

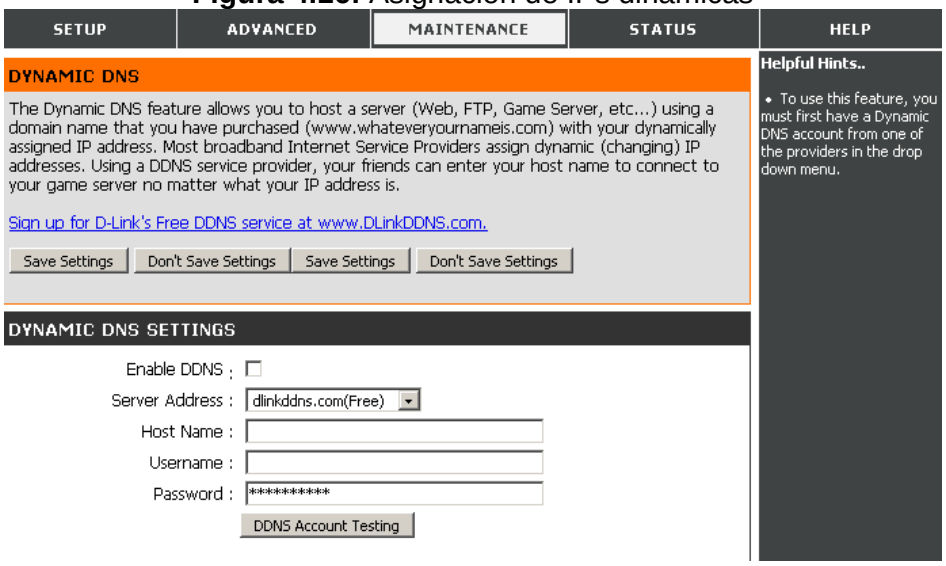
Figura 4.15: Firmar actualización



Fuente: Captura de pantalla

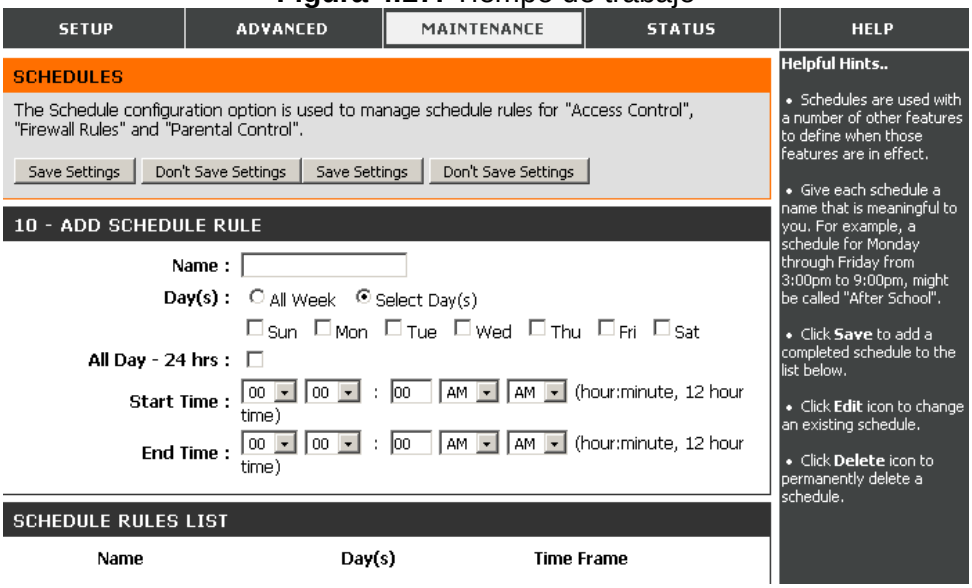
16.- Aquí asignamos las IP's dinámicas, las cuales las personas pueden acceder a nuestra interfaz

Figura 4.16: Asignación de IPs dinámicas



17.- Aquí configuramos el horario en que deseamos que se activen las reglas del firewall y los accesos de control.

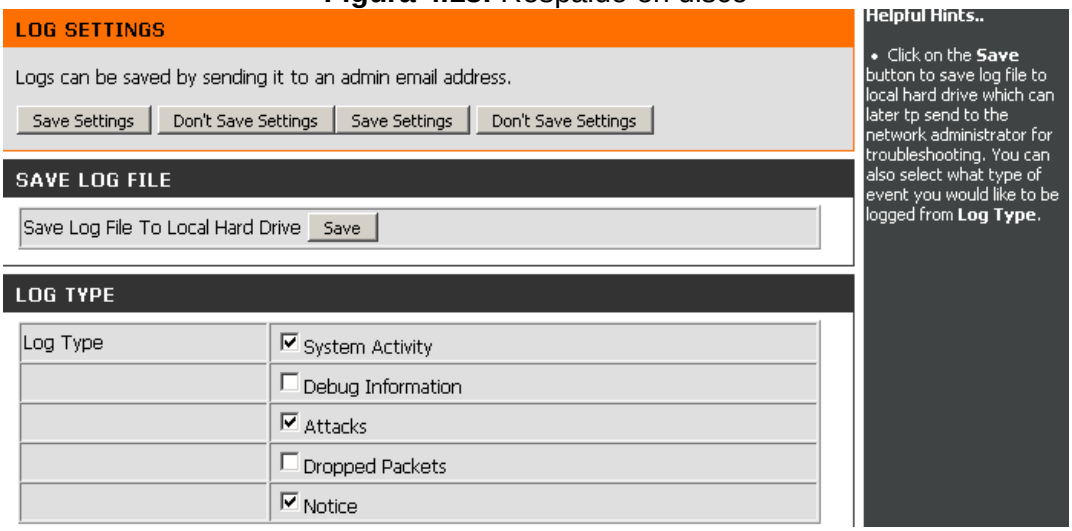
Figura 4.17: Tiempo de trabajo



Fuente: Captura de pantalla

18.- Aquí guardamos los datos del administrador en el disco duro para que en caso de que deseemos lo cargamos desde el disco duro

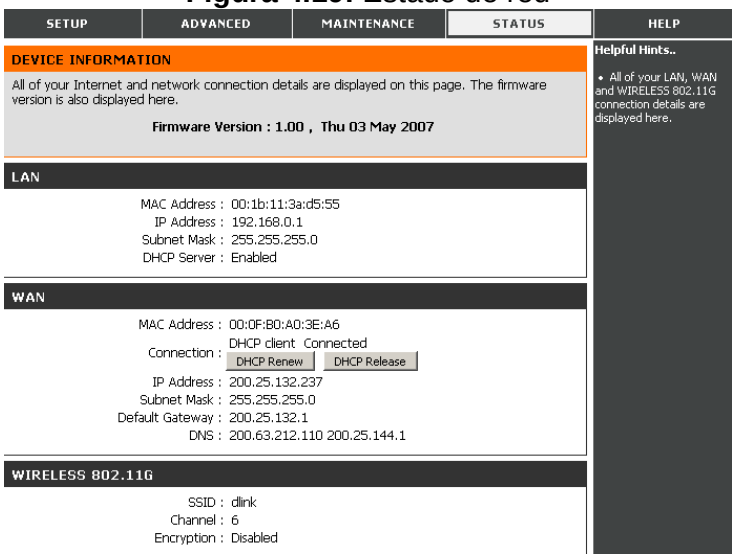
Figura 4.18: Respaldo en disco



Fuente: Captura de pantalla

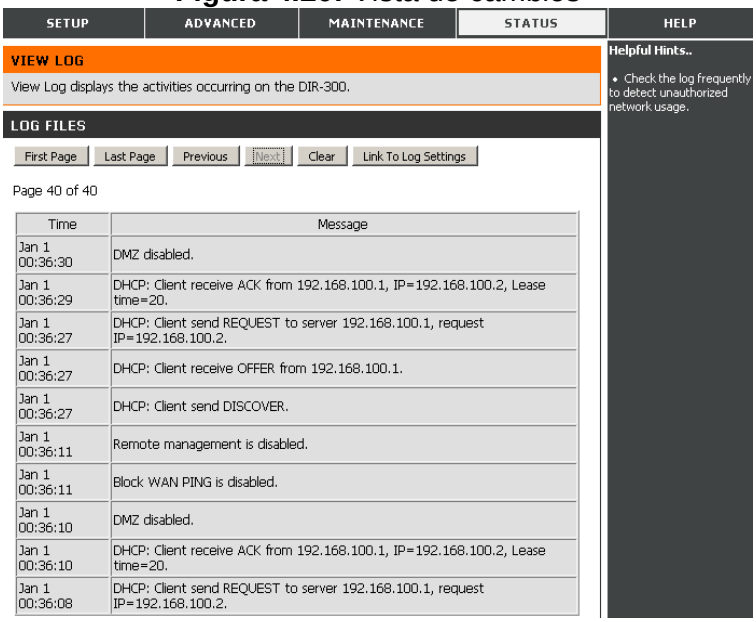
19.- En esta página vemos el estado de la red, las direcciones IP al igual que la red inalámbrica.

Figura 4.19: Estado de red



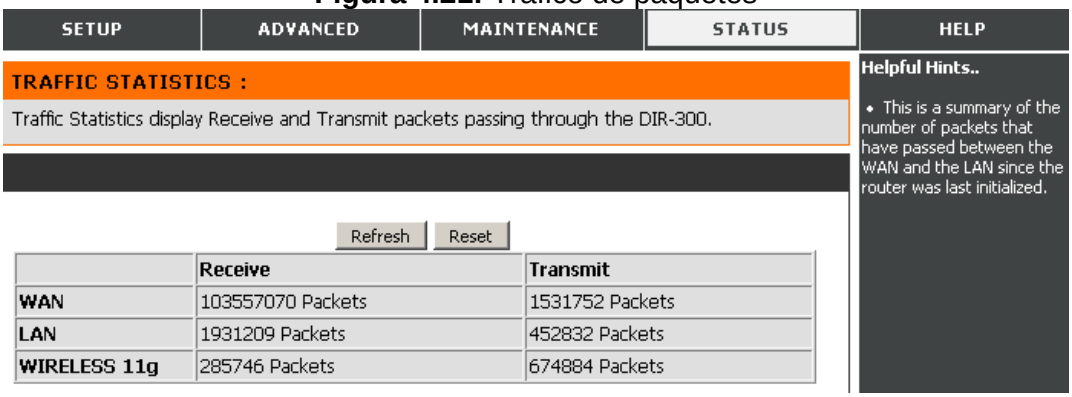
20.- Aquí podemos ver los cambios realizados por fecha y hora

Figura 4.20: Vista de cambios



21.- Aquí podemos ver la transmisión tanto de envió como de recepción

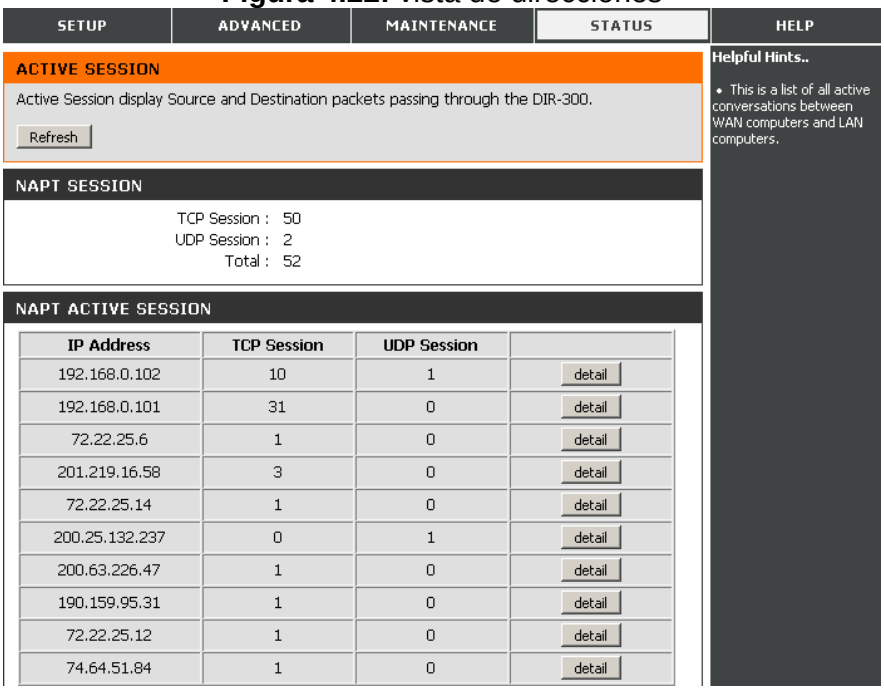
Figura 4.21: Tráfico de paquetes



Fuente: Captura de pantalla

22.- Aquí podemos ver las direcciones IP's asignadas para cada cliente.

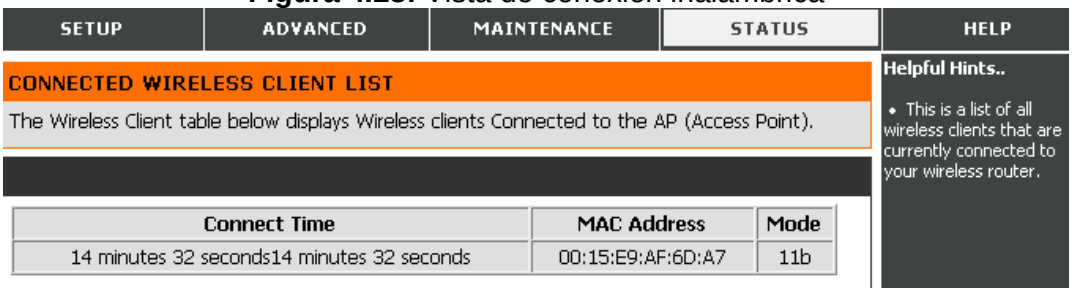
Figura 4.22: vista de direcciones



Fuente: Captura de pantallas

23.- En esta página podemos observar la conexión inalámbrica y la dirección del dispositivo que esté conectado al router.

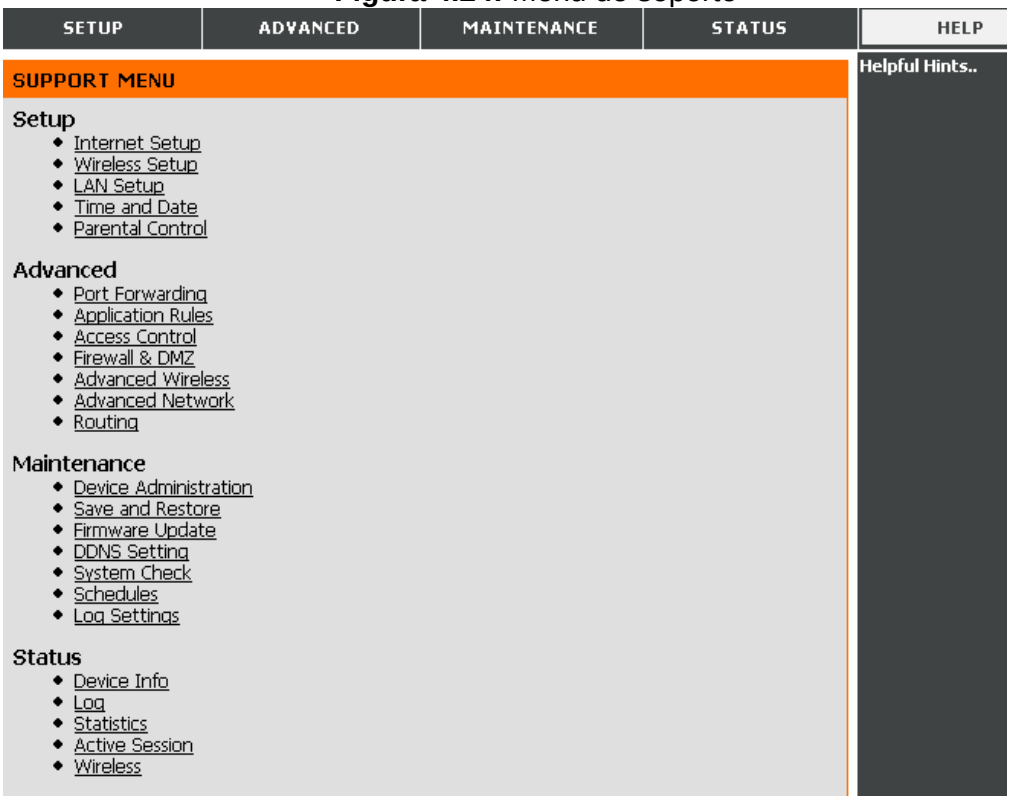
Figura 4.23: Vista de conexión inalámbrica



Fuente: Captura de pantalla

24.- Aquí recibimos ayuda de todas las configuraciones del router desde instalación hasta los estados del router

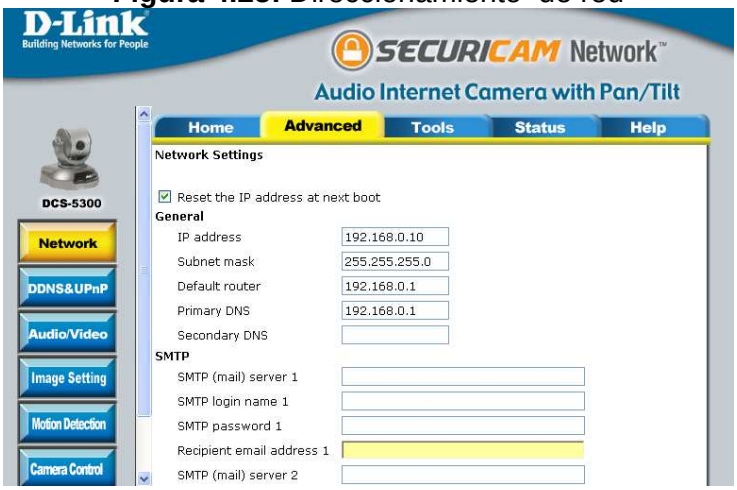
Figura 4.24: Menú de soporte



4.9.2 Configuración de la cámara IP

1.- Aquí se asigna la dirección por default y se asigna la dirección SMTP.

Figura 4.25: Direccionamiento de red



Fuente: Captura de pantalla

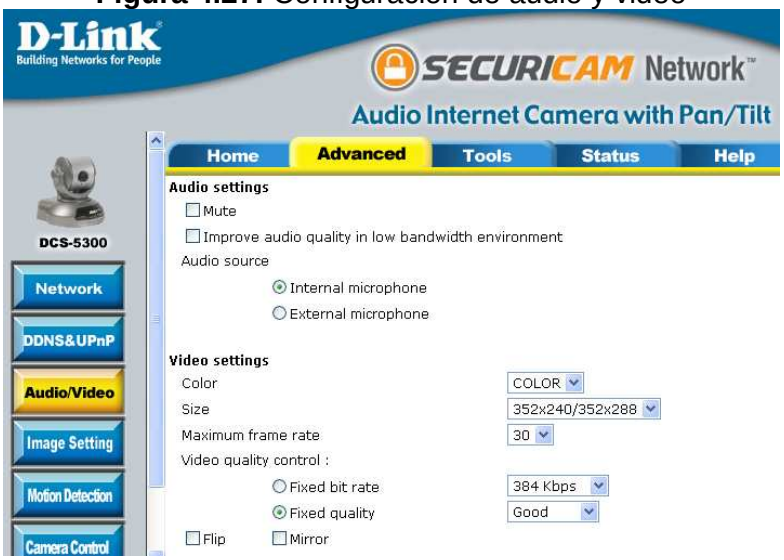
2.- Asignación de Dyn DNS y datos de la cámara.

Figura 4.26: Personalizar cámara

Fuente: Captura de pantalla

3.- Aquí se configura y se regula el audio y sonido

Figura 4.27: Configuración de audio y video



Fuente: Captura de pantalla

4.- En esta pantalla se configura el administrador, y se añade un usuario o se quita. Gerencia, tiene todos los permisos para poder administrar y configurar el sistema.

Figura 4.28: Pantalla creación de usuarios y permisos de acceso

Fuente: Captura de pantalla

5.- Configuración de fecha, puede ser automática o manual

Figura 4.29: Fecha y hora de la cámara

Fuente: Captura de pantalla

6.- Control de tiempo de captura de video.

Figura 4.30: Tiempo de retardo

Fuente: Captura de pantalla

7.- En esta pantalla se confirma o cancela la configuración que se ha realizado.

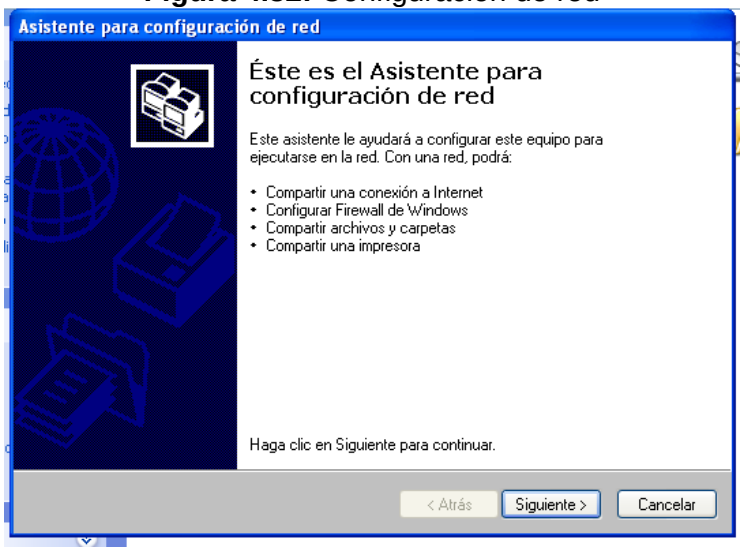
Figura 4.31: Aplicar cambios

Fuente: Captura de pantalla

4.9.3 Configuración de la estación de trabajo

1.- En esta pantalla se inicia el proceso de incluir al usuario a la red, con todos los servicios.

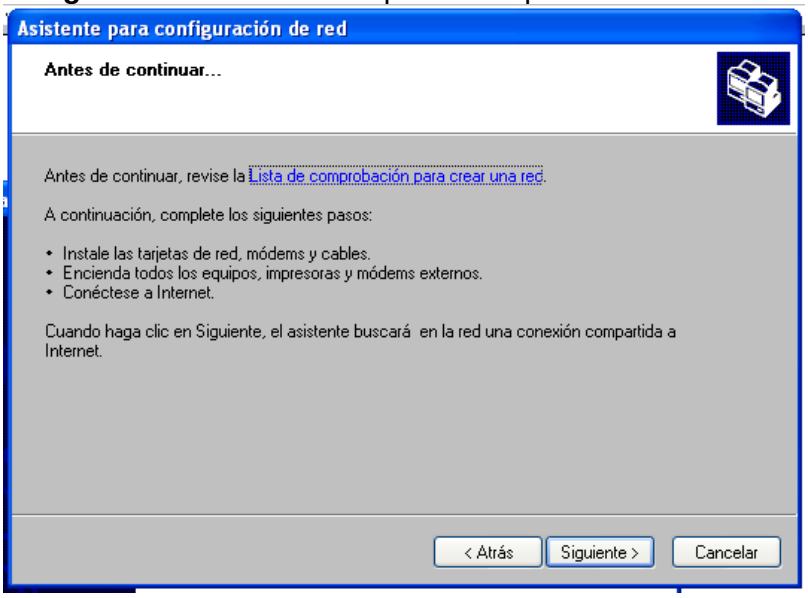
Figura 4.32: Configuración de red



Fuente. Captura de pantalla

2.- En esta pantalla se sugiere verificar que todos los dispositivos que se integraran a la red estén conectados.

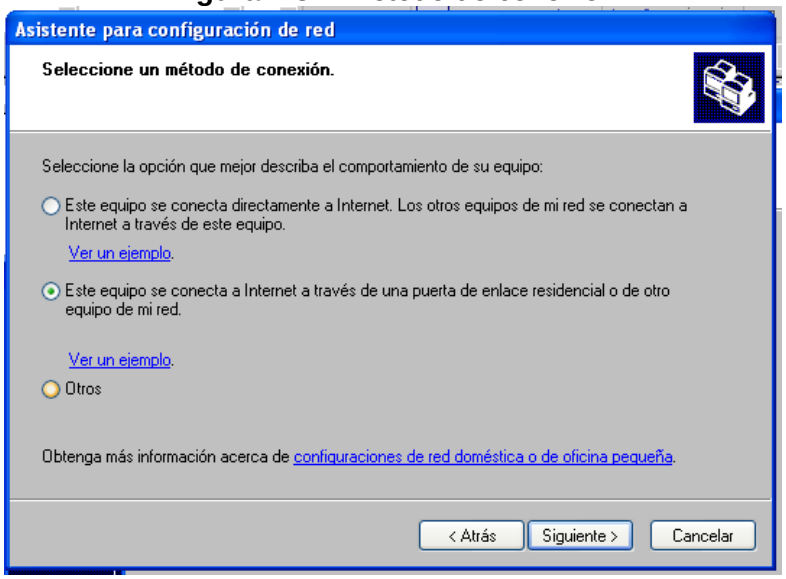
Figura 4.33: Lista de comprobación para crear una red



Fuente: Captura de pantalla

3.- En esta pantalla se elige el método de conexión.

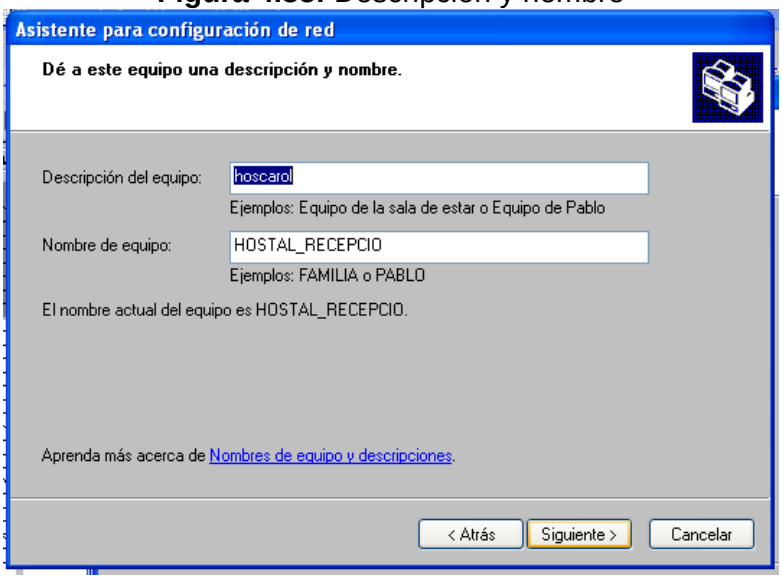
Figura 4.34: Método de conexión



Fuente: Captura de pantalla

4.- En esta pantalla se describe el equipo y se le da un nombre.

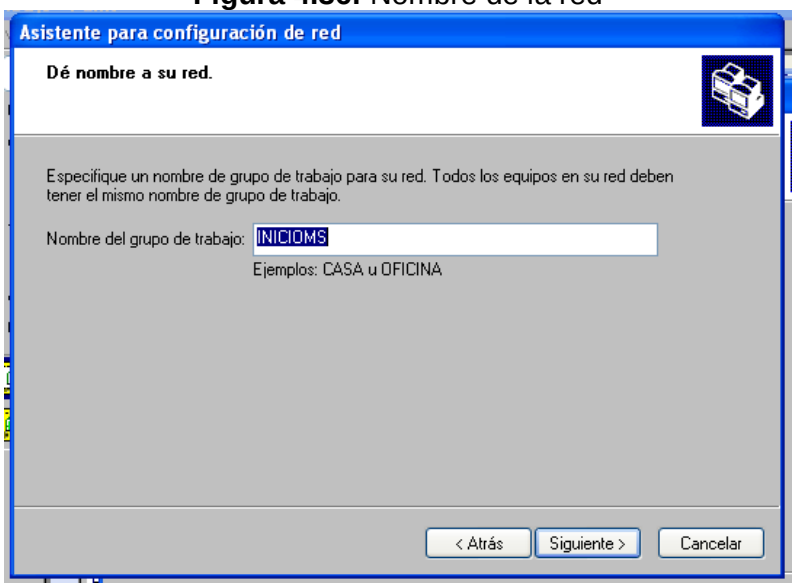
Figura 4.35: Descripción y nombre



Fuente: Captura de pantalla

5.- En esta pantalla se da nombre de la red.

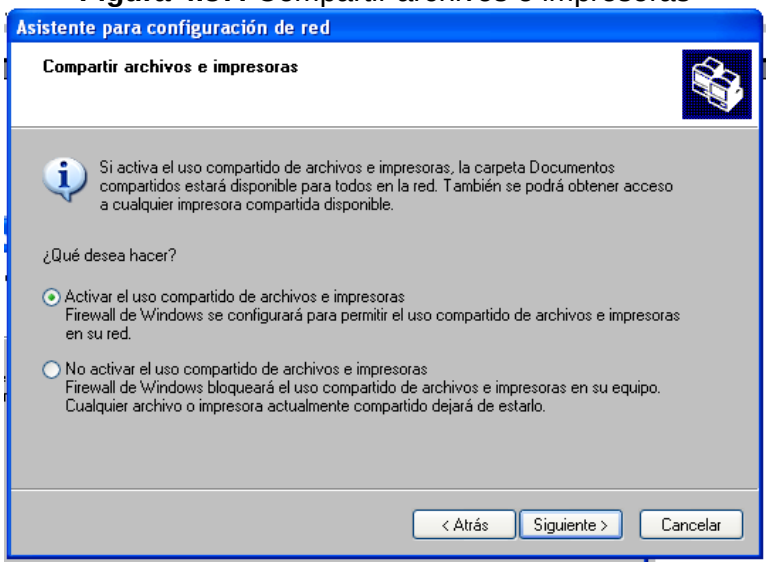
Figura 4.36: Nombre de la red



Fuente: captura de pantalla

6.- En esta pantalla se activa el uso compartido de archivos e impresoras.

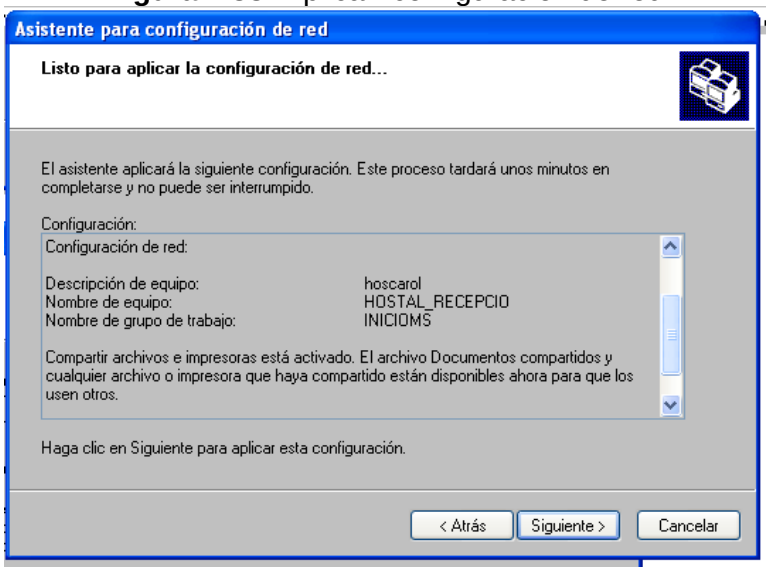
Figura 4.37: Compartir archivos e impresoras



Fuente: Captura de pantalla

7.- Aquí se describe la configuración realizada.

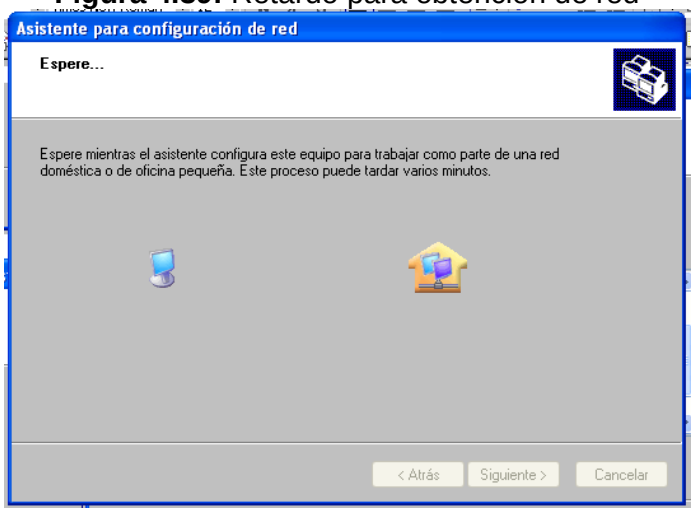
Figura 4.38: Aplicar configuración de red



Fuente: captura de pantalla

8.- Paso previo para acceder a la red

Figura 4.39: Retardo para obtención de red



Fuente: captura de pantalla

9.- Prueba de estado de red

Figura 4.40: Estado de red

Fuente: Captura de pantalla

10.- En esta pantalla se puede ver todos los detalles del usuario como se describe en la figura.

Figura 4.41: Detalles de conexión de red

Fuente: Captura de pantalla

4.10 PRUEBA DE EQUIPOS

4.10.1 PRUEBAS DE MONITOREO

Una vez instaladas las cámaras, el servidor de cámaras y el software de monitoreo se procede a realizar pruebas de funcionamiento del sistema dando como resultado:

Las cámaras cumplen las especificaciones y características del fabricante y se puede observar las imágenes en movimiento en base a estos parámetros.

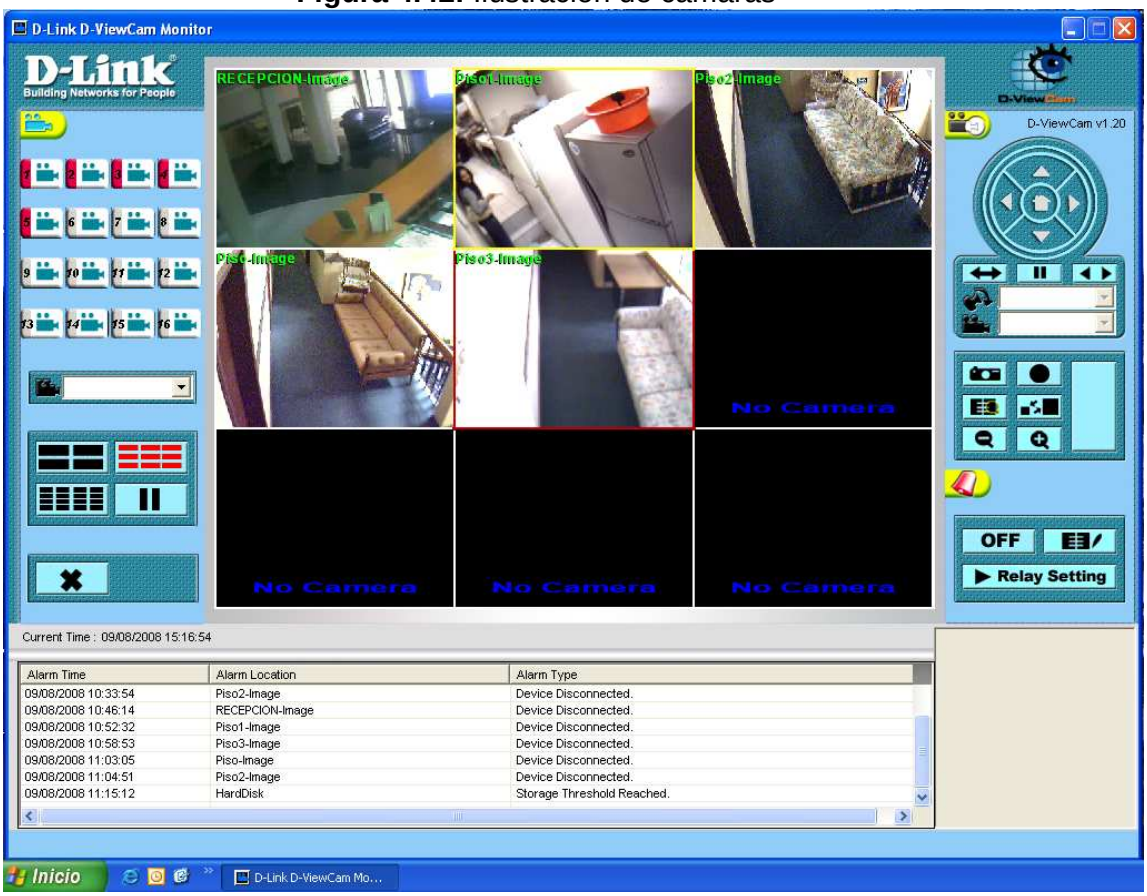
El software de monitoreo cumple con las expectativas antes planteadas y ejecuta los requerimientos de los usuarios.

El sistema puesta en marcha cumple con las expectativas requeridas por el personal de seguridad y demás usuarios.

El proceso de grabación de cámaras utiliza los recursos propios del servidor de respaldos en discos duros sin necesidad de utilizar otros dispositivos para este evento.

Este proyecto está en producción y forma parte de la solución final que se requiere alcanzar y está en pleno funcionamiento.

Figura 4.42: Ilustración de cámaras



Fuente: Captura de pantalla

4.10.2 PRUEBAS DE SEÑAL DE RED WLAN

Tabla 4.3: Pruebas de señal inalámbrica

Enlace	Longitud (m)aproximados	Ubicación	Piso
# 01	15.60	Habitación 001	PB
# 02	18.80	Habitación 003	PB
# 03	10.00	Habitación 108	1er piso
# 04	12.00	Habitación 103	1er piso
# 05	5.00	Habitación 206	2er piso
# 06	8.00	Habitación 204	2to piso
# 07	18.00	Habitación 305	3er piso
# 08	25.00	Habitación 302	3er piso

Figura 4.43: Estado red WLAN

Fuente: Captura de pantallas

4.11 CONCLUSIONES Y RECOMENDACIONES

4.11.1CONCLUSIONES

- Con la implementación de las cámaras de seguridad IP, los clientes de Hostal La Carolina se sienten más satisfechos por el cuidado de sus pertenencias.
- Con el apoyo de la gerencia y el presupuesto destinado al sistema cámaras y de la red WLAN fue posible la adquisición de equipos e instalación de las mismas.
- El software de monitoreo permite añadir cámaras de distinta tecnología y su funcionalidad es adaptable.
- Las cámaras IP tienen la ventaja de conectarse en cualquier lugar de la red de datos y la posibilidad de ir incrementándose según la necesidad.
- Este tipo de tecnología WLAN hace que la gestión sea más sencilla y económica ya que no requiere de cableado adicional.
- Los proveedores de soluciones de seguridad en IP se limitan solo a vender el hardware y software de la firma a cuál representan, cuando se trata de una solución completa que involucren hardware de diferente tecnología no ofrecen garantía en la integridad del sistema.
- El software de monitoreo tiene la particularidad de generar vistas de un conjunto de cámaras dando la posibilidad de generar monitoreo personalizado.
- Los beneficios de la implantación de este proyecto son satisfactorios dando la posibilidad de incrementar la vigilancia desde cualquier estación de trabajo.
- Una vez terminado el proyecto se ha obtenido enriquecimiento teórico y practico en los temas tratados, cumpliendo con el objetivo.

- Con el presente proyecto se logro la conexión inalámbrica en Hostal La Carolina, gracias a esta red es posible acceder al servicio de internet desde cualquier parte dentro de la empresa.

- La investigación de la tecnología de redes inalámbricas permitió determinar el crecimiento y la amplitud de aplicaciones que puede tener. Además de las ventajas en cuanto a movilidad, facilidad de instalación, flexibilidad y comodidad.

- La velocidad de transmisión depende de la distancia, esto es a mayor velocidad de transmisión, menor área de cobertura de la señal. Depende también de los obstáculos.

- Los dispositivos de acceso inalámbrico ya proveen la alternativa de implementación de políticas de seguridad (WPA, WEP, etc.), por lo que se debe hacer uso de ellas. En el caso de Hostal la carolina se aplica seguridad WPA.

4.11.2 RECOMENDACIONES

- Se recomienda que la red de energía eléctrica tenga instalación a tierra para proteger a los dispositivos de descargas ocasionadas por cortos circuitos producidos en la misma red eléctrica o por rayos.

- Las cámaras deben estar instaladas en lugares que no sean de fácil acceso o alcance y sean desconectadas, manipuladas o sustraídas fácilmente.

- El número de cámaras no debe ser excesivo, tener más de 8 cámaras en una pantalla será difícil monitorear, para lo que se recomienda instalar otro monitor o pantalla.

- En sitios sensibles se debería revisar la posibilidad de adquisición e instalación de cámaras de mejores características para gestión de eventos que permiten a la cámara tomar decisiones, y permita la entrada de sensores para robustecer la vigilancia.

- Se recomienda tener una planta generadora de energía eléctrica y un sistema de UPS al menos para el servidor de monitoreo, para que las cámaras de vigilancia no dejen de operar.
- Se recomienda instalar sensores de luz, en los pasillos de ingreso a las habitaciones, ya que la iluminación en los mismos es escasa y minimiza la resolución de las imágenes.
- Se recomienda sacar respaldos de los videos cada 15 días, de esta forma no se satura el disco duro de información y es posible tener un mejor control de eventos.
- Antes de realizar el diseño de una red inalámbrica se debe analizar factores tales como: ancho de banda y velocidad de transferencia necesarios, número de usuarios e intensidad de uso, limitaciones geográficas (radio de cobertura, existencia de paredes y ventanales, ubicación y alimentación de puntos de acceso, etc.), atención a dispositivos móviles presupuesto disponible, etc. y así seleccionar los equipos que satisfagan las necesidades de la aplicación.
- Las claves de ingreso al Access Point que tienen por defecto deben ser cambiadas, puesto que la mayoría de marcas en el mercado vienen con las mismas para todos los modelos, con lo cual se puede acceder a cualquiera de ellos, haciendo un acceso remoto a la red y poniéndola en riesgo a la misma.
- Para una administración adecuada de la red se recomienda considerar aspectos como el monitoreo, atención a fallas, configuración de tarjetas PCI o PCMCIA y seguridad, por lo que se deberá contar con un administrador de red que la mantenga activa, resuelva problemas eventuales que se puedan presentar en cuanto a permisos y autorizaciones de acceso y además realice un mantenimiento periódico (tanto físico como de software) a los equipos
- Se recomienda al menos implementar las políticas de seguridad WEP con cifrado 128 bits Hexadecimal, para mantener un grado de seguridad.

4.12 GLOSARIO

Access Point: (Punto de Acceso o AP) Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

Adaptador: Dispositivo que añada funcionalidad de red a su equipo.

Ancho de banda: Capacidad de transmisión de un dispositivo o red determinado.

Antena: Un dispositivo para transmitir y recibir señales. Frecuentemente disfrazadas en edificios existentes, árboles, torres de agua u otras estructuras altas, el tamaño y la forma de las antenas son determinadas generalmente por la frecuencia de la señal que manejan.

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

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

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

Antena Yagi: Antena compuesta por varios dipolos en línea, obteniendo una mayor ganancia y directividad.

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

Banda Ancha: Un término general que describe sistemas de telecomunicación que pueden mover datos tales como voz y servicios de video, a velocidades más altas.

Bluetooth: El nombre código para una nueva tecnología que permite a los dispositivos móviles equipados con un chip especial enviar y recibir información de forma inalámbrica. Usando Bluetooth, dispositivos electrónicos tales como computadoras de escritorio, teléfonos inalámbricos, organizadores electrónicos e impresoras en el rango de 2.4 GHz pueden “hablar” unos con otros. Ericsson, Intel, Nokia, IBM y Toshiba han sido líderes en el esfuerzo de desarrollo, y ahora se les han unido más de 700 socios, incluyendo Compaq, Dell, Motorola, Qualcomm, BMW y Casio.

Bridge: Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.

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

Conectividad: Estado que permite la transferencia de datos entre dos computadoras.

CDMA (Acceso Múltiple por División de Códigos): Una tecnología utilizada para transmitir llamadas inalámbricas asignándoles códigos. Las llamadas son esparcidas en el más amplio rango de canales disponibles. Entonces, los códigos permiten que muchas llamadas viajen en la misma frecuencia y también guían a esas llamadas al teléfono receptor correcto.

CSMA/CA: (Acceso múltiple de detección de portadora) Un método de transferencia de datos que se utiliza para prevenir una posible colisión de datos.

CSMA/CD: Sensor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica sumada (portadora). En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.

Cifrado: Cifrado es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos puedan realizar una interpretación precisa.

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

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

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

Dirección MAC (Media Access Control) En las redes wireless, MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo OSI. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí.

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

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

DSSS: (Espectro de dispersión de secuencia directa) Transmisión de la frecuencia con un patrón de bit redundante que se traduce en una menor probabilidad de que la información se pierda durante dicha transmisión.

EAP: (Protocolo de autenticación extensible) Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.

EAP-PEAP: (Protocolo de autenticación extensible-Protocolo de autenticación extensible protegido) Método de autenticación mutua que utiliza una combinación de certificados digitales y otros sistemas, como contraseñas.

EAP-TLS: (Protocolo de autenticación extensible-Seguridad de la capa de transporte) Método de autenticación mutua que utiliza certificados digitales.

Ethernet: Protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

FDDI: Estándar de transmisión de datos vía fibra óptica hasta de 100 Mbps con topología parecida a Token Ring/Token Passing.

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

Firewall: Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas no autorizadas. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.

Host: Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.

IEEE: (Instituto de ingenieros eléctricos y electrónicos) Instituto independiente que desarrolla estándares de redes. Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la sucesión 802.11 para las redes WLAN.

IEEE-802.11: Estándar para redes inalámbricas con línea de vista.

Internetworking: Término usado para referirse a la interacción entre varias redes.

Interoperabilidad: La habilidad de una red para coordinar y comunicarse con otras redes, tales como dos sistemas basados en diferentes protocolos o tecnologías.

IP: (Protocolo Internet) Protocolo utilizado para enviar datos a través de una red.

ISP: Internet Service Provider. Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

LAN: La Red de Área Local (LAN) es una pequeña red de datos que cubre un área limitada, tal como un edificio o grupo de edificios. La mayoría de las LAN conectan estaciones de trabajo o computadoras personales. Esto permite a muchos usuarios compartir dispositivos, tales como impresoras de rayo láser así como datos. La LAN también permite comunicación fácil, facilitando el correo electrónico (e-mail) o respaldando sesiones de conversación (Chat).

MAC: (Dirección de control de acceso al medio) Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

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

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

OFDM: (Multiplexado por división de frecuencia ortogonal) La transmisión de frecuencia que separa la corriente de datos en un número de corrientes de datos de velocidad inferior que se transmiten en paralelo para prevenir que se pierda información durante la transmisión.

OSI: Interconexión de Sistemas Abiertos (Open Systems Interconnect). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a través de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

PAP: (Password Authentication Protocol) Protocolo de Autentificación por Password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante una contraseña.

PEAP: (Protocolo de autenticación extensible protegido) Protocolo para la transmisión de de datos de autenticación, incluyendo contraseñas, a través de redes inalámbricas 802.11.

Par Trenzado: Dispositivo parecido al cable telefónico el cual contiene una mayor cantidad de cables. Es el medio físico por el cual pueden conectarse varias computadoras.

PCMCIA: Tarjeta estandarizada de expansión, del tamaño de una tarjeta de crédito, utilizada en ordenadores personales. En telecomunicaciones, uno de sus principales usos es la transmisión de mensajes, datos y faxes a través de computadoras portátiles y teléfonos móviles.

PDA: Personal Digital Assistent (Asistente Digital Personal) - Ordenador de pequeño tamaño cuya principal función era, en principio, mantener una agenda electrónica. No obstante, cada vez más se va confundiendo con los ordenadores de mano y de palma.

PKI: Infraestructura de Clave Pública. Procedimiento criptográfico que utiliza dos claves, una pública y otra privada; la primera para cifrar y la segunda para descifrar. Se utiliza en Internet, que es una red pública no segura, para

proteger aquellas comunicaciones cuya confidencialidad se desea garantizar (ejemplo transacciones comerciales o bancarias).

PLCP: (Physical Layer Convergente Protocol): Es la primera subcapa perteneciente a la capa física que se encarga de la codificación y modulación de los datos transmitidos.

PMD: (Physical Medium Dependence): Es la segunda subcapa que pertenece a la capa física, es la que crea la interfaz y controla la comunicación hacia la capa MAC (a través del SAP: Service Access Point)

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

RADIUS: (Servicio de usuario de marcado con autenticación remota) Protocolo que utiliza un servidor de autenticación para controlar acceso a redes.

Red: Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.

Red Inalámbrica de Área Local (WLAN): Utilizando tecnología de radio frecuencia (RF), las WLAN transmiten y reciben datos de forma inalámbrica en una cierta área. Esto permite a los usuarios en una zona pequeña transmitir datos y compartir recursos, tales como impresoras, sin conectar físicamente cada computadora con cables o alambres.

RJ-45: (Toma registrada 45) Conector Ethernet que alberga hasta ocho hilos.

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

Router: El router está conectado por lo menos a dos redes, y determina hacia que lado enviar el paquete de datos dependiendo en el entendimiento del

router sobre las redes que está conectado. Los routers crean o mantienen una "tabla" de rutas disponibles, y usa esta información para darle la mejor ruta a un paquete, en un determinado momento.

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

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

TCP: (Protocolo de control de transporte) Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

TCP/IP: El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet. Forma de comunicación básica que usa el Internet, la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

TFTP: (Protocolo trivial de transferencia de archivos) Versión del protocolo FTP TCP/IP que utiliza UDP y no dispone de capacidades de directorio ni de contraseña.

TKIP: (Protocolo de integridad de clave temporal) Protocolo de cifrado inalámbrico que cambia periódicamente la clave de cifrado, haciendo más difícil su decodificación.

Topología de Red: Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el

costo del cable y la confiabilidad de la red. Existen tres topologías principales de red anillo, bus y estrella.

UDP: (Protocolo de datagramas de usuario) Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.

USB: (Universal Serial Bus) Estándar utilizado en las PCs con el fin de reconocer los dispositivos hardware (impresora, teclado, etc.) y ponerlos en funcionamiento de forma rápida y sencilla. Elimina la necesidad de instalar adaptadores en la PC.

WEP: (Protocolo de equivalencia con cable) Es un protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña). WEP ofrece un nivel básico (pero satisfactorio) de seguridad para la transferencia de datos a través de redes inalámbricas.

Wi Fi: (Wireless Fidelity) es una de las tecnologías de comunicación inalámbrica (sin cables – wireless) más extendidas. También se conoce como WLAN o como IEEE 802.11.

Los subestándares de Wi-Fi que actualmente más se están explotando en el ámbito de las redes inalámbricas son:

802.11a: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.

802.11b: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2,4 GHz.

802.11g: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 2,4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.

802.11n: En plena fase de desarrollo, la última revisión del estándar del IEEE. Surge como respuesta a las crecientes necesidades de velocidad y ancho de banda de las redes inalámbricas actuales. Soporta tecnología MIMO basada en la utilización de varias antenas en un mismo dispositivo.

WPA: (Acceso protegido WiFi) Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. Asegura la transferencia de datos de forma inalámbrica mediante la utilización de una clave similar a WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica. La clave, en continuo cambio, dificulta que un pirata informático pueda conocer la clave y obtener acceso a la red.

WPA2: (Acceso protegido Wi-Fi 2) Es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.

WPA-Enterprise: Versión de WPA que utiliza las mismas claves dinámicas que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.

WPA-Personal: Versión de WPA que utiliza claves de cifrado en constante cambio y de mayor longitud para complicar el proceso de su decodificación.

4.13 BIBLIOGRAFÍA:

- http://html.rincondelvago.com/topologias.html
- http://www.unicrom.com/cmp_topologia_redes_estrella_malla.asp
- http://mx.geocities.com/alfonsoaraujocardenas/topologias.html
- http://comunidad.uach.mx/marana/materias/sir/material/El%20modelo%20OSI.doc:
- http://zator.com/Hardware/H12_2.htm
- http://www.tech-faq.com/lang/es/osi-model.shtml
- http://docs.sun.com/app/docs/doc/820-2981/ipov-10?l=es&a=view
- http://nuestrowiki.wikispaces.com/Medios+de+transmision?f=print
- http://www.eveliux.com/mx/index.php?option=com_content&task=view&id=21&Itemid=26
- http://es.wikipedia.org/wiki/Medio_de_transmisi%C3%B3n
- http://www.it.uniovi.es/docencia/Telematica/fundamentostelematica/material/apuntes/tema3/tema03.htm
- http://www.unav.es/cti/manuales/Redes_Internet/#6
- http://es.kioskea.net/internet/ipv6.php3
- http://es.wikipedia.org/wiki/IPv4
- http://www.andy21.com/ip/ip.html
- http://es.kioskea.net/internet/ipv6.php3
- http://www.wikilearning.com/curso_gratis/seguridad_en_wifi_tecnico-los_estandares_802_11/4171-1
- http://www.e-advento.com/tecnologia/wlan_intro.php
- http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Inalambricas/CLASES/802-11ParteIa.pdf
- http://es.wikipedia.org/wiki/IEEE_802.11
- http://rinuex.unex.es/modules.php?op=modload&name=Articulos&file=article&sid=88&mode=thread&order=0&thold=0
- http://www.canal-ayuda.org/a-informatica/inalambrica.htm
- http://www.monografias.com/trabajos12/reina/reina.shtml
- http://www.jornada.unam.mx/2006/02/02/033a1tec.php
- http://www.gestiopolis.com/canales8/ger/definicion-y-tipo-de-redes-inalambricas.htm

- http://www.gestiopolis.com/canales8/ger/definicion-y-tipo-de-redes-inalambricas.htm
- http://www.uam.es/servicios/ti/servicios/wifi/miscelanea.html
- http://support.dell.com/support/edocs/network/p94583i/SP/wlan.htm
- http://es.wikipedia.org/wiki/Red_por_infrarrojos
- http://es.wikibooks.org/wiki/Componentes_de_una_red/Medios_de_Transmision_Inalambricos/
- http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf
- http://www.coit.es/pub/ficheros/informewificoit_definitivo_2464518b.pdf
- http://www.networkmagazineindia.com/200204/net200204_16.jpg
- http://ccomputo.itam.mx/redes/servicios/wlan/802_11b.htm
- http://es.geocities.com/alfredo061/Redes.html
- http://www.cez.com.pe/Wireless/Wireless.htm
- http://es.geocities.com/yulaidysramirez/tempresa/t1/redesi.html
- http://www.gmtvaritec.com/index.php?mod=productos&idL=2&niv=2&id=3
- http://es.kioskea.net/wifi/wifimodes.php3
- http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/Oct06Marzo07/ComInalam/TRabajos/TRABAJO3/G1/PROYECTO%203%20-%20GRUPO%201.doc
- http://guia.mercadolibre.com.ve/wifi-wireless-que-es-redes-inalambricas-tutorial-8825-VGP
- http://guia.mercadolibre.com.mx/componentes-necesarios-establecer-una-red-lan-inalambrica-22594-VGP
- http://images.google.com.ec/images?gbv=2&ndsp=20&hl=es&q=tarjeta+inalambrica+USB&start=60&sa=N
- http://guia.mercadolibre.com.ve/instalar-una-red-inalambrica-wi-fi-paso-12964-VGP
- http://guia.mercadolibre.com.mx/componentes-necesarios-establecer-una-red-lan-inalambrica-22594-VGP
- http://www.astronomos.cl/conocimientos/avanzado/Presentacion-antenas.pdf

- http://www.monografias.com/trabajos10/coin/coin.shtml
- http://80.24.102.10/wireless/antenas/Conceptos_basicos_sobre_antenas.pdf
- http://www.zero13wireless.net/foro/showthread.php?t=2693
- http://80.24.102.10/wireless/antenas/Conceptos_basicos_sobre_antenas.pdf
- http://www.e-oss.net/portuwireless/taller-nodos/antenas.pdf
- http://www.34t.com/Unique/wiFiAntenas.asp
- http://www.monografias.com/trabajos10/coin/coin.shtml
- http://www.monografias.com/trabajos10/coin/coin.shtml
- http://www.wifisafe.com/conceptos_wireless.php
- http://www.zero13wireless.net/foro/showthread.php?t=511
- http://www.alegsa.com.ar/Dic/zona%20de%20fresnel.php
- http://www.saulo.net/pub/inv/SegWiFi-art.htm
- http://www.microsoft.com/spain/technet/recursos/articulos/cg0805.mspx#top
- http://es.wikipedia.org/wiki/WEP
- http://support.dell.com/support/edocs/network/P94583/sp/security.htm#Open
- http://dns.bdat.net/seguridad_en_redes_inalambricas/c113.html
- http://www.siemon.com/es/white_papers/SD-03-08-CCTV.asp
- http://www.nexo-tech.com/srv_ip.php?menu=2
- http://www.camarasip.cl/que_es_una_camara_de_red.htm
- http://www.ipcamarasvigilancia.com/camara-axis-p-6.html
- http://www.indigovision.com/files/international/IP-Cameras%20-%20Apr06-Spanish-Revised.pdf
- http://www.maximotec.com/showthread.php?t=27836
- http://usuarios.lycos.es/todohardware/hd.htm
- http://www.camarasip.cl/que_es_una_camara_de_red.htm
- http://www.monografias.com/trabajos10/vire/vire.shtml
- http://www.monografias.com/trabajos16/ingenieria-de-tv/ingenieria-de-tv.shtml

- http://www4.ujaen.es/~jcbago/progrupo/resumenes/Resumen%20Equipos%20QoS.pdf
- http://www.coasin.cl/index.php?id=61
- http://lat.3com.com/lat/news/pr03/nov10.html
- http://www.ciao.es/3Com_AirConnect__690376
- http://www.apcnet.com.mx/3com/lan.htm
- 3Com® 6/8dBi Dual-Band Omni Antenna
- http://www.3com.com/prod/es_ES_EMEA/detail.jsp?tab=features&sku=3CWE591
- http://www.3com.com/prod/es_ES_EMEA/prodlist.jsp?tab=cat&cat=13&subcat=91
- http://www.fixya.com/Brands/Images/0/3Com/177x150/21066333.JPG
- http://www.3com.es/products/adsl/
- http://www.beep.es/Redes/C-maras-IP/Linksys-Wireless-G-Compact-Internet-Video-Camera-WVC54GCV1ZDNTRHQy1FVQ==.html
- http://www.ciudadwireless.com/product_info.php?products_id=172
- http://articulo.mercadolibre.com.mx/MLM-20381271-tarjeta-red-inalambrica-linksys-pci-54mbps-11b-y-11g-dn8-_JM
- http://www.pixmania-pro.com/es/es/linksys/antena-wifi-hga7s-7-dbi/503464/fiche.html#tech-desc
- http://www.rigg.cl/riggweb/store/product.jsp?product=1995
- http://www.esemanal.com.mx/articulos.php?id_sec=4&id_art=3919
- http://www.dlinkla.com/home/news_desk/dlink_comunicado.jsp?id_comunicado=181
- http://www.dlinkla.com/home/soluciones/express.jsp
- JD-LINK DES-1008D SWITCH 8 PUERTOS 10/100MBPS
- http://www.expansys.es/p.aspx?i=105686
- http://www.dlinkla.com/home/productos/producto.jsp?idp=711
- http://www.dlinkla.com/home/productos/producto.jsp?idp=1009
- http://tienda.jmo.cl/product_info.php?manufacturers_id=21&products_id=2120&osCsid=92210081feacf86ac8ad11b935e51929

- http://www.mundoyaos.com/index.php?page=shop.product_details&flypage=shop.flypage&product_id=77&category_id=31&manufacturer_id=0&option=com_virtuemart&Itemid=4
- http://braincorp.com.ve/tienda/camara-de-seguridad-dlink-dcs2100-dcs2100-p-4555.html?osCsid=86f019846800bcb23082ee166ddba490