



REPÚBLICA DEL ECUADOR

Escuela Politécnica Nacional

" E SCIENTIA HOMINIS SALUS "

La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del (los) autor(es).

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.
- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.
- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

***Respeto hacia sí mismo y hacia los demás.***

# **ESCUELA POLITÉCNICA NACIONAL**

**FACULTAD DE INGENIERÍA ELÉCTRICA Y  
ELECTRÓNICA**

**DISEÑO Y SIMULACIÓN DE UNA RED INTEGRADA DE VOZ Y  
DATOS PARA LA UNIDAD EDUCATIVA TEMPORAL  
“JAIME ROLDÓS AGUILERA”**

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

**RAMÓN BEDOYA JORGE ALBERTO**

jorge\_ramon14@hotmail.com

**DIRECTOR: ING. PABLO HIDALGO LASCANO**

pablo.hidalgo@epn.edu.ec

**Quito, Noviembre 2014**

## DECLARACIÓN

Yo, **Jorge Alberto Ramón Bedoya**, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado previamente 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 correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

---

Jorge Alberto Ramón Bedoya

## **CERTIFICACIÓN**

Certifico que el presente trabajo fue desarrollado por Jorge Alberto Ramón, bajo mi supervisión.

Ing. Pablo Hidalgo Lascano  
DIRECTOR DE PROYECTO

## AGRADECIMIENTOS

A Dios por guiar mi camino siempre,

A mis padres por ese constante y desinteresado apoyo,

A grandes personas como Diego (Chupillita), Jawico, JIGA y Beto,

quienes brindaron su apoyo para lo obtención de este logro,

A mi Andre que me acolitaba en las madrugadas aunque sea por Skype,

Al Ing. Pablo Hidalgo que más que mi tutor se convirtió en un gran amigo

por la confianza depositada en mí y sus valiosos consejos,

A ti Caro, por llegar en el momento preciso a ser la persona adecuada,

A todas las personas que de una u otra manera aportaron

en mi formación profesional.

## DEDICATORIA

Definitivamente a aquella mujer que siempre estuvo detrás de mí,  
por su incansable labor, apoyo e infinito amor,  
por esas riñas innecesarias, por esa palmada que nunca estuvo de más,  
A ti MADRE.

A mi Ché, que me enseñó que la vida no solo es responsabilidades,  
por las travesuras, por hacer que la pelota forme parte de mi vida,  
en definitiva por enseñarme a ser así, así como Soy.

A ti Jordy, para indicarte que la meta siempre la pones Tú.

Dedico esto a ustedes MI FAMILIA.

## CONTENIDO

DECLARACIÓN.....	I
CERTIFICACIÓN .....	II
AGRADECIMIENTOS.....	III
DEDICATORIA .....	IV
CONTENIDO.....	V
ÍNDICE DE FIGURAS .....	XV
ÍNDICE DE TABLAS.....	XIX
PRESENTACIÓN.....	XXIII
RESUMEN.....	XXIV
<b>CAPÍTULO 1: FUNDAMENTOS TEÓRICOS..</b> .....	<b>1</b>
<b>1.1 INTRODUCCIÓN</b> .....	<b>1</b>
<b>1.2 REDES DE ÁREA LOCAL</b> .....	<b>1</b>
1.2.1 ETHERNET E IEEE 802.3 .....	2
1.2.2 TECNOLOGÍAS LAN.....	3
<b>1.3 REDES CONVERGENTES</b> .....	<b>5</b>
<b>1.4 VOZ SOBRE IP (VoIP)</b> .....	<b>6</b>
1.4.1 ESTANDARIZACIÓN DE LA VoIP.....	7
1.4.2 ESPECIFICACIÓN H.323 .....	7
1.4.2.1 Componentes H.323 .....	8
1.4.2.1.1 <i>Terminal</i> .....	8
1.4.2.1.2 <i>Gateway</i> .....	12

1.4.2.1.3	<i>Gatekeeper</i> .....	12
1.4.2.1.4	<i>Unidad de control de multipunto (MCU)</i> .....	12
1.4.2.2	Stack de Protocolos H.323.....	12
1.4.2.3	Establecimiento de Llamadas H.323.....	14
1.4.2.3.1	<i>Fase de Establecimiento de la llamada H.323</i> .....	15
1.4.2.3.2	<i>Fase de Señalización de Control</i> .....	16
1.4.2.3.3	<i>Fase de Transmisión de Datos</i> .....	17
1.4.2.3.4	<i>Fase de Liberación de la Conexión</i> .....	17
1.4.3	SIP (Session Initiation Protocol).....	18
1.4.3.1	Componentes SIP .....	19
1.4.3.1.1	<i>Agentes de usuario (UAs)</i> .....	19
1.4.3.1.2	<i>Servidores de registro</i> .....	19
1.4.3.1.3	<i>Servidores proxy y de redirección</i> .....	20
1.4.3.1.4	<i>Servidores de localización</i> .....	21
1.4.3.2	Establecimiento de Llamadas SIP .....	22
1.4.4	TIPOS DE ARQUITECTURAS PARA VoIP .....	24
1.4.4.1	Arquitectura Centralizada.....	24
1.4.4.2	Arquitectura Distribuida .....	25
1.4.5	SIMILITUDES Y DIFERENCIAS ENTRE H.323 Y SIP .....	25
1.4.6	FACTORES QUE AFECTAN LA CALIDAD DE VOZ.....	27
1.4.6.1	Codec's.....	27
1.4.6.2	Pérdida de Paquetes.....	29
1.4.6.2.1	<i>Protocolos de QoS</i> .....	29
1.4.6.2.2	<i>Intercalado</i> .....	29
1.4.6.2.3	<i>Supresión de silencio y ruido</i> .....	30
1.4.6.2.4	<i>Interpolación</i> .....	30
1.4.6.2.5	<i>Corrección</i> .....	30
1.4.6.3	Retardo de Paquetes .....	31
1.4.6.3.1	<i>Retardo de Algoritmo</i> .....	31
1.4.6.3.2	<i>Retardo de Paquetización</i> .....	32
1.4.6.3.3	<i>Retardo de Serialización</i> .....	33
1.4.6.3.4	<i>Retardo de Propagación</i> .....	33
1.4.6.3.5	<i>Retardo de Componente</i> .....	33



1.4.6.4	<i>Jitter</i> .....	34
<b>1.5</b>	<b>TELEFONÍA IP</b> .....	<b>35</b>
1.5.1	CLASES DE TELEFONÍA IP .....	35
1.5.1.1	Telefonía IP Privada.....	35
1.5.1.2	Telefonía IP por Internet.....	36
1.5.1.3	Telefonía IP Pública .....	37
1.5.2	VENTAJAS DE LA TELEFONÍA IP [36].....	37
1.5.3	DESVENTAJAS DE LA TELEFONÍA IP .....	39
1.5.4	ESQUEMAS PARA TELEFONÍA IP.....	39
1.5.4.1	Esquema de Telefonía IP Híbrido .....	40
1.5.4.2	Esquema de Telefonía IP Puro .....	40
1.5.5	SOLUCIONES PARA TELEFONÍA IP .....	41
1.5.5.1	Soluciones Basadas en Hardware .....	42
1.5.5.1.1	<i>Ventajas de soluciones basadas en hardware</i> .....	42
1.5.5.1.2	<i>Desventajas de soluciones basadas en hardware</i> .....	42
1.5.5.2	Soluciones Basadas en Software .....	43
1.5.5.2.1	<i>Ventajas de soluciones basadas en software</i> .....	43
1.5.5.2.2	<i>Desventajas de soluciones basadas en software</i> .....	43
<b>1.6</b>	<b>SISTEMA DE CABLEADO ESTRUCTURADO</b> .....	<b>44</b>
1.6.1	SUBSISTEMAS DEL CABLEADO ESTRUCTURADO .....	44
1.6.1.1	Área de Trabajo.....	45
1.6.1.2	Cableado Horizontal.....	45
1.6.1.3	Cableado Vertical .....	46
1.6.1.4	Cuarto de Telecomunicaciones.....	48
1.6.1.5	Sala de Equipos .....	48
1.6.1.6	Entrada de Servicios .....	49
1.6.2	ESTÁNDARES DE SISTEMA DE CABLEADO ESTRUCTURADO.....	49
1.6.2.1	Estándares ANSI/TIA 568-C .....	49
1.6.2.2	Estándares ANSI/EIA-569-B .....	51
1.6.2.3	Estándares ANSI/TIA 606-A .....	52
1.6.2.4	Estándares ANSI/TIA-607-A .....	52
1.6.3	SEGURIDAD DE LA RED.....	53

1.6.3.1 Norma ISO/ICE 27002 .....	53
<b>CAPÍTULO 2: ANÁLISIS DE LA SITUACIÓN ACTUAL Y REQUERIMIENTOS...</b>	<b>58</b>
<b>2.1 INTRODUCCIÓN .....</b>	<b>58</b>
<b>2.2 UNIDAD EDUCATIVA TEMPORAL “JAIME ROLDÓS AGUILERA” .....</b>	<b>59</b>
2.2.1 MISIÓN INSTITUCIONAL.....	60
2.2.2 VISIÓN INSTITUCIONAL .....	60
<b>2.3 DESCRIPCIÓN DE LA INFRAESTRUCTURA FÍSICA DE LA INSTITUCIÓN.....</b>	<b>60</b>
<b>2.4 DESCRIPCIÓN DE LA RED DE DATOS.....</b>	<b>63</b>
<b>2.5 ANÁLISIS DE LA TOPOLOGÍA ACTUAL.....</b>	<b>65</b>
<b>2.6 EQUIPAMIENTO DE LA RED DE DATOS .....</b>	<b>66</b>
2.6.1 ELEMENTOS PASIVOS .....	66
2.6.1.1 Sistema de Cableado Estructurado (SCE) .....	66
2.6.1.2 Sistema de Puesta a Tierra .....	67
2.6.2 ANÁLISIS DE LOS ELEMENTOS PASIVOS DE LA RED .....	68
2.6.3 ELEMENTOS ACTIVOS .....	70
2.6.3.1 Equipos Periféricos .....	70
2.6.3.2 Equipos de Conectividad.....	72
2.6.4 Análisis de los Elementos Activos de la Red .....	72
2.6.5 SISTEMA TELEFÓNICO .....	74
2.6.5.1 Análisis del Sistema Telefónico Actual.....	76
2.6.6 RED INALÁMBRICA .....	77
2.6.6.1 Análisis de la Red Inalámbrica .....	79
2.6.7 SERVICIO DE INTERNET CONTRATADO .....	81
2.6.7.1 Análisis del Servicio de Internet .....	81
2.6.8 APLICACIONES ACTUALES .....	82
2.6.9 REQUERIMIENTOS FUTUROS.....	83
2.6.9.1 Servicios de Red Requeridos.....	84
2.6.9.1.1 <i>Servidor Web</i> .....	84

2.6.9.1.2 Servidor DNS (Domain Name Server).....	84
2.6.9.1.3 Servidor de Correo Electrónico .....	85
2.6.9.1.4 Servidor de Descarga de Archivos (FTP).....	85
2.6.9.1.5 Servidor DHCP.....	85
2.6.9.2 Servicios en Tiempo Real .....	86
2.6.10 ADMINISTRACIÓN DE LA RED .....	86
2.6.10.1 Análisis de la Administración Actual de la Red.....	87
2.6.11 SEGURIDAD EN LA RED.....	87
2.6.11.1 Análisis de la Seguridad Actual en la Red.....	88
2.6.12 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL Y REQUERIMIENTOS DE LA RED.....	89
<b>CAPÍTULO 3: DISEÑO DE LA RED INTEGRADA DE VOZ Y DATOS .....</b>	<b>91</b>
<b>3.1 VISIÓN GENERAL.....</b>	<b>91</b>
<b>3.2 MODELO DE RED .....</b>	<b>91</b>
3.2.1 CAPA DE ACCESO.....	92
3.2.2 CAPA DE DISTRIBUCIÓN .....	92
3.2.3 CAPA NÚCLEO.....	93
<b>3.3 TECNOLOGÍA DE RED .....</b>	<b>93</b>
<b>3.4 TOPOLOGÍA DE RED .....</b>	<b>94</b>
<b>3.5 DISEÑO DE LA RED PASIVA.....</b>	<b>97</b>
3.5.1 DISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO .....	97
3.5.1.1 Distribución de los Puntos de Red .....	98
3.5.2 DISEÑO DEL SUBSISTEMA DE CABLEADO HORIZONTAL.....	100
3.5.2.1 Rutas para el Cableado Horizontal.....	104
3.5.2.2 Accesorios para el Cableado Horizontal .....	105
3.5.3 DISEÑO DEL SUBSISTEMA DE CABLEADO VERTICAL .....	107
3.5.4 DISEÑO DEL SUBSISTEMA ÁREA DE TRABAJO .....	108
3.5.5 DISEÑO DEL SUBSISTEMA CUARTO DE TELECOMUNICACIONES	108
3.5.5.1 Selección de los Rack`s.....	110

3.5.5.1.1 <i>Rack</i> Principal.....	111
3.5.5.1.2 Gabinetes.....	112
3.5.6 DISEÑO DEL SUBSISTEMA SALA DE EQUIPOS .....	113
3.5.7 ADMINISTRACIÓN DEL SISTEMA DE CABLEADO	
ESTRUCTURADO.....	114
3.5.7.1 Etiquetado.....	114
3.5.8 DIMENSIONAMIENTO DEL TRÁFICO DE LA RED.....	117
3.5.8.1 Cálculo del Ancho de Banda Correo Electrónico.....	117
3.5.8.2 Cálculo del Ancho de Banda de Acceso a la Web .....	118
3.5.8.3 Cálculo del Ancho de Banda de acceso a Base de Datos .....	119
3.5.8.4 Cálculo del Ancho de Banda para Descargas de Archivos .....	119
3.5.8.5 Cálculo del Ancho de Banda para VoIP .....	120
3.5.8.5.1 Procedimiento para calcular el Ancho de Banda para VoIP .....	120
3.5.8.5.2 Cálculo del Ancho de Banda para VoIP de la UET “JRA” .....	122
3.5.8.6 Cálculo del Ancho de Banda para la WLAN.....	123
3.5.9 ANCHO DE BANDA REQUERIDO PARA DATOS.....	124
3.5.10 ANCHO DE BANDA REQUERIDO PARA VOZ.....	126
3.5.11 ANCHO DE BANDA DE LA CONEXIÓN A INTERNET .....	126
3.5.12 REQUERIMIENTOS DE VOZ.....	127
3.5.12.1 Número de Usuarios .....	128
3.5.12.2 Proyección de Crecimiento .....	128
3.5.12.3 Circuitos Troncales hacia la PSTN.....	129
<b>3.6 DISEÑO DE LA RED ACTIVA.....</b>	<b>131</b>
3.6.1 CAPA ACCESO.....	131
3.6.2 CAPA DISTRIBUCIÓN .....	131
3.6.3 NÚCLEO DE LA RED.....	131
3.6.4 ELECCIÓN DE EQUIPOS PARA LA RED.....	132
3.6.4.1 Administración de los Equipos .....	132
3.6.4.2 Escalabilidad y Versatilidad.....	132
3.6.4.3 Calidad de Servicio y Seguridad .....	132
3.6.5 SWITCHES DE ACCESO.....	133
3.6.6 SWITCHES DE DISTRIBUCIÓN .....	135

3.6.7 SWITCHES DE CORE.....	136
3.6.8 SERVIDORES .....	137
3.6.8.1 Servidor WEB.....	137
3.6.8.2 Servidor de Correo Electrónico .....	138
3.6.8.3 Servidor FTP .....	139
3.6.8.4 Servidor DCHP.....	140
3.6.8.5 Servidor DNS .....	140
3.6.8.6 Servidor de Llamadas IP .....	140
3.6.9 CARACTERÍSTICAS GENERALES DE LOS SERVIDORES.....	140
3.6.10 CARACTERÍSTICAS ESPECÍFICAS DE LOS SERVIDORES .....	141
3.6.11 EQUIPOS PARA TELEFONÍA IP.....	142
3.6.11.1 Servidor de Llamadas IP .....	142
3.6.11.2 Gateway IP.....	142
3.6.11.3 Terminales de Telefonía IP .....	142
3.6.12 DISEÑO DE LA RED DE ÁREA LOCAL INALÁMBRICA.....	144
3.6.12.1 Site Survey Pasivo .....	145
3.6.12.2 Aplicaciones de la WLAN.....	147
3.6.12.3 Áreas de Cobertura.....	149
3.6.12.4 Integración con la Red Cableada .....	149
3.6.12.5 Parámetros de Operación .....	149
3.6.12.6 Identificador SSID ( <i>Service Set Identifier</i> ) .....	150
3.6.12.7 Seguridad en los Puntos de Acceso.....	150
3.6.12.7.1 WEP.....	151
3.6.12.7.2 WPA.....	151
3.6.12.7.3 WPA2 .....	151
3.6.13 SELECCIÓN DE LOS ACCESS POINT.....	152
3.6.14 DISEÑO LÓGICO DE LA RED .....	152
3.6.15 DMZ .....	153
3.6.15.1 Direccionamiento IP .....	154
3.6.15.2 VLAN's .....	155
3.6.15.2.1 VLAN Empleados .....	155
3.6.15.2.2 VLAN Estudiantes.....	155
3.6.15.2.3 VLAN Profesores.....	155

3.6.15.2.4 VLAN de Voz .....	156
3.6.16 POLÍTICAS BÁSICAS DE SEGURIDAD PAR LA UET “JRA” .....	156
3.6.16.1 Seguridad Física de la UET “JRA” .....	156
3.6.16.2 Seguridad Lógica de la UET “JRA” .....	157
3.6.17 ADMINISTRACIÓN DE LA RED .....	158

## **CAPÍTULO 4: ANÁLISIS DE COSTOS Y SIMULACIÓN DE LA RED**

<b>INTEGRADA DE VOZ Y DATOS.....</b>	<b>160</b>
<b>4.1 SOFTWARE A UTILIZAR PARA LA SIMULACIÓN .....</b>	<b>160</b>
4.1.1 GNS3 ( <i>Graphical Network Simulator</i> ) .....	161
4.1.1.1 Ventajas del Simulador GNS3.....	162
4.1.1.2 Desventajas del Simulador GNS3.....	162
4.1.1.3 Instalación de GNS3 .....	163
4.1.2 ZIMBRA SERVER .....	163
4.1.3 ASTERISK .....	163
4.1.4 WEBMIN .....	164
4.1.5 INSTALACIÓN DEL SERVIDOR PROFTP .....	165
4.1.6 INSTALACIÓN SERVIDOR WEB APACHE .....	166
4.1.7 INSTALACIÓN DEL FIREWALL IPTABLES .....	167
4.1.8 NAGIOS XI .....	167
4.1.9 VPCS (SIMULADOR VIRTUAL DE PC’S) .....	168
<b>4.2 SIMULACIÓN DE LA RED .....</b>	<b>169</b>
4.2.1 CONFIGURACIÓN DE UN SWITCH EN GNS3 .....	169
4.2.1.1 Configuración de un Router en modo <i>Switch</i> .....	170
4.2.1.2 Carga de los IOS para los <i>Switches</i> .....	172
4.2.2 TOPOLOGÍA A SIMULARSE.....	173
4.2.3 CONFIGURACIÓN BÁSICA DE LOS SWITCHES.....	175
4.2.4 CONFIGURACIÓN DE LOS SWITCHES DE ACCESO .....	177
4.2.5 CONFIGURACIÓN DE LOS SWITCHES DE DISTRIBUCIÓN.....	177
4.2.6 CONFIGURACIÓN DE LOS SWITCHES DE CORE .....	177
4.2.7 CONFIGURACIÓN DE USUARIOS PROFTP .....	177
4.2.8 CONFIGURACIÓN DEL SERVIDOR WEB.....	181

4.2.9 CONFIGURACIÓN DEL SERVIDOR ZIMBRA .....	183
4.2.9.1 Creación de Usuarios.....	183
4.2.10 CONFIGURACIÓN NAGIOS XI .....	184
4.2.10.1.1 Monitoreo del host Cliente .....	184
4.2.10.1.2 Monitoreo de un Servicio .....	186
4.2.11 CONFIGURACIÓN DE ASTERISK.....	188
4.2.11.1 Configuración del fichero sip.conf .....	188
4.2.11.2 Configuración del fichero extensions.conf .....	189
4.2.12 CONFIGURACIÓN DEL <i>FIREWALL</i> DE LINUX .....	191
4.2.13 CONFIGURACIÓN DE LOS PC VIRTUALES .....	192
<b>4.3 PRUEBAS DE SIMULACIÓN DE LA RED .....</b>	<b>194</b>
4.3.1 PRUEBAS DEL SERVIDOR WEB.....	195
4.3.2 PRUEBAS DEL SERVIDOR FTP .....	197
4.3.3 PRUEBAS DEL SERVIDOR DNS.....	198
4.3.4 PRUEBAS DEL SERVIDOR ZIMBRA.....	199
4.3.4.1 Correo Electrónico de Prueba .....	200
4.3.5 PRUEBAS DEL SERVIDOR ASTERISK .....	201
4.3.5.1 Configuración de Usuarios en Media5Fone .....	203
4.3.6 PRUEBAS DEL SERVIDOR NAGIOS XI.....	204
4.3.7 PRUEBAS DE LAS VLANs.....	205
<b>4.4 ANÁLISIS DE LAS PRUEBAS REALIZADAS .....</b>	<b>207</b>
<b>4.5 ANÁLISIS DE COSTOS DE LA RED INTEGRADA DE VOZ Y DATOS</b>	
<b>DISEÑADA .....</b>	<b>208</b>
4.5.1 ANÁLISIS DE COSTOS DE LA RED PASIVA.....	209
4.5.1.1 Elementos de la Red Pasiva .....	209
4.5.2 ANÁLISIS DE COSTOS DE LA RED ACTIVA.....	217
4.5.2.1 <i>Switches</i> de Acceso .....	217
4.5.2.2 <i>Switches</i> de Distribución .....	219
4.5.2.3 <i>Switches</i> de Core .....	219
4.5.2.4 <i>Access Point</i> .....	222
4.5.2.5 Teléfonos IP .....	223

4.5.2.6 Costo Total de la Red Activa .....	224
4.5.3 ANÁLISIS DE COSTOS DE OPERACIÓN .....	224
4.5.4 PARÁMETROS DE SELECCIÓN DE LA MEJOR ALTERNATIVA .....	226
4.5.4.1 Garantía y Soporte Técnico Cisco .....	226
4.5.4.1.1 <i>Cisco Limited Lifetime Hardware Warranty</i> .....	227
4.5.4.2 Garantía y Soporte Técnico Juniper .....	227
4.5.4.2.1 <i>Enhanced Limited Lifetime Warranty</i> .....	227
4.5.5 SELECCIÓN DE LA MEJOR ALTERNATIVA .....	228
4.5.6 COSTO TOTAL DE LA RED .....	229
<b>CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES.....</b>	<b>231</b>
<b>5.1 CONCLUSIONES.....</b>	<b>231</b>
<b>5.2 RECOMENDACIONES .....</b>	<b>234</b>



## ÍNDICE DE FIGURAS

Figura 1. 1 Trama Ethernet vs trama 802.3 .....	2
Figura 1. 2 Relación de 802.3 con el modelo OSI .....	3
Figura 1. 3 Tecnologías Ethernet .....	4
Figura 1. 4 Componentes de la red según recomendación H.323 de la ITU .....	8
Figura 1. 5 Diagrama de bloques de un terminal H.323 .....	11
Figura 1. 6 <i>Stack</i> de Protocolos H.323 .....	14
Figura 1. 7 Fase de Establecimiento de Llamada H.323 .....	15
Figura 1. 8 Fase de señalización de control.....	16
Figura 1. 9 Fase de transmisión de voz .....	17
Figura 1. 10 Fase de Liberación de Conexión .....	17
Figura 1. 11 Servidor de Registro SIP.....	20
Figura 1. 12 Servidor <i>Proxy</i> SIP .....	21
Figura 1. 13 Servidor de Localización SIP .....	22
Figura 1. 14 Establecimiento y liberación de Llamada SIP .....	23
Figura 1. 15 Arquitectura Centralizada.....	24
Figura 1. 16 Retardo de Paquetes .....	31
Figura 1. 17 <i>Jitter</i> .....	34
Figura 1. 18 Telefonía IP privada .....	36
Figura 1. 19 Telefonía IP por Internet .....	36
Figura 1. 20 Telefonía IP pública .....	37
Figura 1. 21 Telefonía IP Híbrida .....	40
Figura 1. 22 Telefonía IP Puro .....	41
Figura 1. 23 Subsistemas del sistema de cableado estructurado .....	44
Figura 1. 24 Cableado Horizontal .....	46
Figura 1. 25 Cableado Vertical (Campus Educativo).....	47
Figura 1. 26 Cableado Vertical (Edificio Comercial) .....	47
Figura 1. 27 Sala de Equipos .....	48
Figura 1. 28 Estándar ANSI/TIA 568-C .....	50
Figura 1. 29 Asignación pares/pines T568A y T568B .....	51
Figura 1. 30 Dominios de Control para Gestión de Seguridad Informática .....	55

Figura 2. 1 Diagrama de ubicación de la UET “JRA” .....	59
Figura 2. 2 Distribución Zonal de la UET “JRA” .....	62
Figura 2. 3 Bloque de aulas de la UET “JRA” .....	63
Figura 2. 4 Diagrama de la red actual de la UET “JRA” .....	64
Figura 2. 5 Diagrama de cableado del Laboratorio de Informática I .....	67
Figura 2. 6 Sistema de puesta a tierra mallado .....	68
Figura 2. 7 Sistema Telefónico de la UET “JRA” .....	75
Figura 2. 8 <i>Router Status</i> .....	78
Figura 2. 9 Configuraciones de seguridad y acceso del <i>Router</i> .....	78
Figura 2. 10 Configuraciones LAN del <i>Router</i> .....	79
Figura 2. 11 Radio de alcance del <i>router</i> D´Link DIR 600 .....	80
Figura 3. 2 Modelo jerárquico de una red .....	92
Figura 3. 3 Topología de la red a diseñar .....	96
Figura 3. 4 Distancias hacia el cuarto de equipos .....	97
Figura 3. 5 Cable UTP Categoría 6A, corte transversal . .....	101
Figura 3. 6 <i>Rack</i> de 24 UR .....	111
Figura 3. 7 Nomenclatura para el Etiquetado. ....	115
Figura 3. 8 Ejemplo de Etiquetado en el UET “JRA” .....	116
Figura 3. 9 Utilización de servidores <i>web</i> en el mercado .....	138
Figura 3. 10 WLAN´s cercanas a la institución .....	145
Figura 3. 11 Pérdida de potencia en la WLAN de la institución .....	146
Figura 3. 12 Canales y frecuencias de WLAN´s cercanas a la institución .....	146
Figura 3. 13 Cobertura de la WLAN .....	148
Figura 3. 14 Zona Desmilitarizada .....	153
Figura 4. 1 Elementos de GNS3 .....	162
Figura 4. 2 Listado de Servidores FTP compatibles con Webmin .....	165
Figura 4. 3 Servidor ProFTP .....	166
Figura 4. 4 Listado de módulos Apache compatible con Webmin .....	166
Figura 4. 5 Servidor Web Apache .....	167
Figura 4. 6 Módulo <i>IPtables / Firewall</i> Linux .....	167
Figura 4. 7 Configuración del Router como <i>Switch</i> .....	170
Figura 4. 8 Selección del módulo NM-16ESW .....	170
Figura 4. 9 Mensaje de Conexión para el <i>Switch</i> .....	171

Figura 4. 10 Edición de símbolos en GNS3 .....	171
Figura 4. 11 Cambio de imagen para el nuevo <i>Switch</i> .....	172
Figura 4. 12 Imagen de <i>Switch</i> agregada exitosamente .....	172
Figura 4. 13 Configuración para la carga de los IOS en GNS3.....	173
Figura 4. 14 Topología física a simularse.....	174
Figura 4. 15 Topología lógica a simularse.....	175
Figura 4. 16 Configuración básica de los <i>Switches</i> .....	176
Figura 4. 17 Desactivación de traducción de nombres.....	177
Figura 4. 18 Usuarios FTP .....	178
Figura 4. 19 Opciones de configuración del Servidor ProFTP .....	178
Figura 4. 20 Configuración de las Opciones de Red del Servidor ProFTP.....	179
Figura 4. 21 Control de Acceso para el Servidor ProFTP .....	179
Figura 4. 22 Autenticación de Usuarios en el Servidor ProFTP .....	180
Figura 4. 23 Usuarios denegados en el Servidor ProFTP .....	180
Figura 4. 24 Archivo proftpd.conf .....	181
Figura 4. 25 Configuración <i>host</i> Virtual Servidor Web Apache.....	181
Figura 4. 26 Plantilla de prueba para el servidor <i>web</i> Apache .....	182
Figura 4. 27 Creación exitosa del <i>host</i> virtual.....	182
Figura 4. 28 Administración de Zimbra.....	183
Figura 4. 29 Configuración de un nuevo usuario en Zimbra.....	183
Figura 4. 30 Consola <i>Core Configure Manager</i> .....	184
Figura 4. 31 Creación de nuevo <i>host</i> .....	185
Figura 4. 32 Configuraciones generales de monitoreo del <i>host</i> .....	185
Figura 4. 33 Configuraciones generales del servicio a monitorear.....	186
Figura 4. 34 Asignación del servicio al <i>host</i> a monitorear. ....	187
Figura 4. 35 Configuración general del fichero sip.conf .....	188
Figura 4. 36 Configuración de canales SIP .....	189
Figura 4. 37 Permisos generales para el contexto teléfonos IP .....	189
Figura 4. 38 <i>Dial-Plan</i> para el contexto Interno y Pruebas .....	190
Figura 4. 39 Configuración Contexto IVR_MENU .....	190
Figura 4. 40 Reglas del <i>firewall</i> .....	191
Figura 4. 41 Configuración de reglas en el <i>firewall</i> .....	192
Figura 4. 42 <i>Shell</i> de VPCS.....	193

Figura 4. 43 Lista de PC virtuales .....	193
Figura 4. 44 Mapeo de los <i>host</i> virtuales con su respectivo puerto .....	194
Figura 4. 45 Añadir IP a <i>host</i> virtual .....	194
Figura 4. 46 IP de la nube perteneciente a la VLAN Estudiantes .....	195
Figura 4. 47 <i>Ping</i> al Servidor Web .....	196
Figura 4. 48 Acceso a la página precargada en el Servidor Web .....	196
Figura 4. 49 <i>Ping</i> al Servidor FTP .....	197
Figura 4. 50 <i>Login</i> al Servidor FTP .....	197
Figura 4. 51 Transferencia de un archivo a un usuario FTP .....	197
Figura 4. 52 Confirmación de archivo transferido al usuario FTP .....	198
Figura 4. 53 <i>Ping</i> al servidor DNS .....	198
Figura 4. 54 <i>Ping</i> al Servidor Zimbra .....	199
Figura 4. 55 <i>Traceroute</i> al Servidor Zimbra .....	199
Figura 4. 56 Acceso web al Servidor Zimbra .....	200
Figura 4. 57 <i>Email</i> de prueba a través de Zimbra .....	201
Figura 4. 58 NATEO de la interfaz de Internet al servidor Asterisk .....	201
Figura 4. 59 <i>Ping</i> desde el servidor Asterisk al cliente .....	202
Figura 4. 60 <i>Traceroute</i> desde el servidor Asterisk al Cliente .....	202
Figura 4. 61 Configuración General de Usuario Media5Fone .....	203
Figura 4. 62 Configuración de Red para Media5Fone .....	203
Figura 4. 63 Registro usuario SIP Media5Fone .....	204
Figura 4. 64 <i>Ping</i> al Servidor Nagios XI .....	204
Figura 4. 65 <i>Trace route</i> al servidor Nagios XI .....	205
Figura 4. 66 Estado de los <i>host</i> Cliente y SW- ACC .....	205
Figura 4. 67 <i>Ping</i> entre VLAN de datos .....	206
Figura 4. 68 Trama de datos .....	206
Figura 4. 69 <i>Ping</i> entre VLAN de voz .....	206
Figura 4. 70 Trama de voz .....	207

## ÍNDICE DE TABLAS

Tabla 1. 1 Cronología de la especificación H.323 .....	7
Tabla 1. 2 Codec's de audio .....	9
Tabla 1. 3 Codec's de video .....	10
Tabla 1. 4 Diferencias entre H.323 y SIP .....	26
Tabla 1. 5 Retardos de algoritmos .....	32
Tabla 1. 6 Retardo de Paquetización .....	32
Tabla 1. 7 Retardo de Serialización .....	33
Tabla 2. 1 Lista de equipos periféricos.....	71
Tabla 2. 2 Listado de equipos de conectividad .....	72
Tabla 2. 3 Listado de equipos de voz .....	76
Tabla 2. 4 Aplicaciones Actuales.....	83
Tabla 3. 1 Tecnologías Ethernet.....	94
Tabla 3. 2 Distribución de los puntos Zona A .....	99
Tabla 3. 3 Distribución de los Puntos Zona B.....	99
Tabla 3. 4 Distribución de los puntos Zona C.....	100
Tabla 3. 5 Distribución de los puntos Zona D.....	100
Tabla 3. 6 Distribución de los puntos Zona E.....	100
Tabla 3. 7 Longitudes para el Cableado Horizontal Zona A .....	102
Tabla 3. 8 Longitudes para el Cableado Horizontal Zona B .....	102
Tabla 3. 9 Longitudes para el Cableado Horizontal Zona C .....	103
Tabla 3. 10 Longitudes para el Cableado Horizontal Zona D .....	103
Tabla 3. 11 Longitudes para el Cableado Horizontal Zona E .....	103
Tabla 3. 12 Longitud Total de UTP para la UET "JRA" .....	104
Tabla 3. 13 Rutas Estandarizadas para el Cableado Horizontal .....	104
Tabla 3. 14 Capacidad de UTPs por canaleta.....	105
Tabla 3. 15 Elementos para el cableado horizontal por zona.....	106
Tabla 3. 16 Distancias entre los cuartos de telecomunicaciones al MDF .....	107
Tabla 3. 17 Distribución de los Cuartos de Telecomunicaciones .....	109
Tabla 3. 18 Dimensiones estandarizadas para cuartos de telecomunicaciones	109
Tabla 3. 19 Números de equipos a almacenar en los <i>Racks</i> .....	110
Tabla 3. 20 Dimensionamiento <i>Rack</i> Principal.....	111

Tabla 3. 21 Dimensionamiento de Gabinetes de Comunicaciones .....	112
Tabla 3. 22 Código de Colores para el SCE .....	114
Tabla 3. 23 Nomenclatura de los Cuartos de Telecomunicaciones.....	116
Tabla 3. 24 Tamaño de la trama de VoIP con PPP .....	120
Tabla 3. 25 Tamaño de la trama de VoIP con PPP y compresión RTP .....	121
Tabla 3. 26 Tamaño de la trama para una LAN sin cRTP .....	122
Tabla 3. 27 Usuarios potenciales y reales de la institución .....	124
Tabla 3. 28 Índices de Simultaneidad .....	124
Tabla 3. 29 Tráfico Total para Datos .....	125
Tabla 3. 30 Usuarios reales y potenciales del sistema de voz .....	126
Tabla 3. 31 Ancho de Banda hacia la Nube .....	127
Tabla 3. 32 Número de personal en los cinco últimos años .....	128
Tabla 3. 33 Características de los <i>Switches</i> de Acceso .....	134
Tabla 3. 34 Número de <i>switches</i> necesarios por Zona .....	134
Tabla 3. 35 Número de puertos a utilizar .....	135
Tabla 3. 36 Características de los <i>switches</i> de Distribución.....	136
Tabla 3. 37 Características de los <i>switches</i> de Core.....	137
Tabla 3. 38 Características Específicas de los Servidores .....	141
Tabla 3. 39 Características del <i>Gateway</i> IP .....	143
Tabla 3. 40 Características de los terminales de Telefonía IP .....	143
Tabla 3. 41 Distribución de <i>Access Point</i> .....	147
Tabla 3. 42 Estándares para redes inalámbricas .....	150
Tabla 3. 43 SSID para los <i>access-point</i> .....	150
Tabla 3. 44 Características mínimas para los <i>access-point</i> .....	152
Tabla 3. 45 Direccionamiento IP para la UET “JRA” .....	154
Tabla 4. 1 Elementos de la red pasiva .....	209
Tabla 4. 2 Elementos de la red pasiva zona A .....	212
Tabla 4. 3 Elementos de la red pasiva zona B .....	213
Tabla 4. 4 Elementos de la red pasiva zona C .....	214
Tabla 4. 5 Elementos de la red pasiva zona D .....	215
Tabla 4. 6 Elementos de la red pasiva zona E .....	216
Tabla 4. 7 Valor total de la red pasiva .....	217
Tabla 4. 8 Costo de los <i>switches</i> de acceso.....	218

Tabla 4. 9 Costo total de <i>switches</i> de acceso .....	219
Tabla 4. 10 Costo de los <i>switches</i> de distribución.....	220
Tabla 4. 11 Costo total de <i>switches</i> de distribución.....	220
Tabla 4. 12 Costo de los <i>switches</i> de <i>core</i> .....	221
Tabla 4. 13 Costo total de la <i>switches core</i> .....	222
Tabla 4. 14 Costo de los <i>access-point</i> .....	222
Tabla 4. 15 Costo total de la red inalámbrica .....	223
Tabla 4. 16 Costo de teléfonos IP .....	223
Tabla 4. 17 Costo total teléfonos IP .....	224
Tabla 4. 18 Costo total de la red activa por fabricante .....	224
Tabla 4. 19 Costo de operación de la red .....	225
Tabla 4. 20 Costo total de la inversión inicial para la red de la UET “JRA” .....	229
Tabla 4. 21 Costo total de los valores recurrentes para la UET “JRA” .....	230

## ÍNDICE DE ECUACIONES

Ecuación 3. 1 Cálculo del número de UTP por canaleta .....	105
Ecuación 3. 2 Ancho de Banda para Correo Electrónico .....	118
Ecuación 3. 3 Ancho de Banda de la red cableada para acceso a la <i>Web</i> .....	119
Ecuación 3. 4 Ancho de Banda para el acceso a base de datos.....	119
Ecuación 3. 5 Ancho de Banda para Descargas .....	119
Ecuación 3. 6 Trama de Voz .....	120
Ecuación 3. 7 Número de bits por trama de VoIP con PPP .....	121
Ecuación 3. 8 Ancho de banda requerido por llamada de VoIP con PPP .....	121
Ecuación 3. 9 Ancho de Banda total con VoIP y PPP .....	122
Ecuación 3. 10 Número de bits por trama con <i>Ethernet</i> .....	123
Ecuación 3. 11 Ancho de Banda por llamada para una LAN .....	123
Ecuación 3. 12 Ancho de Banda para la WLAN .....	123
Ecuación 3. 13 Ancho de Banda Total para VoIP .....	126
Ecuación 3. 14 Ancho de Banda total para la institución.....	127
Ecuación 3. 15 Intensidad de tráfico .....	129
Ecuación 3. 16 Intensidad de tráfico para la UET Jaime Roldós Aguilera.....	129
Ecuación 3. 17 Intensidad de tráfico proyectado.....	130

Ecuación 3. 18 Intensidad de tráfico proyectado para la UET "JRA".....	130
Ecuación 3. 19 Cálculo de la velocidad de <i>backplane</i> en el <i>Switch</i> .....	133
Ecuación 3. 20 Velocidad de <i>backplane</i> del <i>switch</i> de acceso.....	133



## PRESENTACIÓN

El avance de las Tecnologías de Información y Comunicación ha generado un nuevo concepto dentro del mundo de la Educación. Las instituciones educativas han buscado ir a la par con estos avances incluyendo dentro de sus organizaciones estas tecnologías y así mejorar su proceso de educadores mediante el uso de nuevas metodologías, herramientas y aplicaciones para la enseñanza de la sociedad.

La Unidad Educativa Temporal “Jaime Roldós Aguilera”, con el afán de ser pioneros en el ámbito educacional dentro de la Provincia de Santo Domingo de los Tsáchilas debe adaptarse a estos cambios e incorporar en su organización un sistema de comunicaciones lo suficientemente flexible, organizado y de fácil administración.

En el presente proyecto de titulación se realiza el diseño de la red INTEGRADA de voz y datos para la Unidad Educativa Temporal “Jaime Roldós Aguilera” con la finalidad de proporcionar un sistema de comunicación conforme a los avances que se están teniendo, el mismo que ofrezca servicios de calidad a profesores, estudiantes y personal administrativo de la institución.

En el diseño de la red se integran los servicios de voz y datos; también se muestran configuraciones para los servicios que la red proporciona, recomendaciones de seguridad y administración de red; siendo este proyecto base de conocimiento para futuros diseños en caso de requerirlo.

## RESUMEN

La Unidad Educativa Temporal “Jaime Roldós Aguilera”, es una institución educativa pública, ubicada en la provincia de Santo Domingo de los Tsáchilas, cabecera cantonal Santo Domingo de los Colorados; brinda servicios de educación básica y bachillerato.

Este proyecto de titulación se fundamenta en el diseño y simulación de una red integrada de voz y datos para la Unidad Educativa; basándose en los fundamentos teóricos necesarios, el análisis de requerimientos, el diseño y simulación de la red, y el análisis de costo para la solución planteada.

En el primer capítulo se realiza un resumen de los fundamentos teóricos, así como se enumeran las principales normas y estándares que serán necesarios para el posterior diseño.

El segundo capítulo contiene el análisis de la situación actual de la Unidad Educativa Temporal “Jaime Roldós Aguilera”; aquí se puede encontrar información como distribución física de la institución, equipamiento, cableado estructurado, servicios actuales y requeridos. Se realiza una división estratégica de los departamentos de la institución con la finalidad de facilitar el posterior diseño.

En el tercer capítulo se realiza el diseño de la red integrada de voz y datos, dividiendo el mismo en diseño de la red pasiva y activa.

Dentro del diseño de la red pasiva se encuentran los subsistemas de cableado estructurado a diseñar, elementos pasivos necesarios y dimensionamiento del tráfico a cursar por la red. El diseño de la red activa muestra las características que deben poseer los equipos de conectividad, servidores, terminales IP, etc.

También se realiza el diseño de la red inalámbrica de la Institución, el diseño lógico de la red que involucra direccionamiento IP, creación de VLAN, DMZ; y finalmente se establecen políticas básicas de seguridad.

En el cuarto capítulo se realiza la simulación de la red diseñada, se muestran las configuraciones de los diferentes servidores utilizados y las pruebas necesarias para validar el funcionamiento de los mismos.

Se presenta un costo referencial de la red diseñada, evaluando dos casas fabricantes; la selección de la alternativa sugerida para la institución está basada en el análisis técnico y económico.

En el capítulo quinto se recogen las conclusiones y recomendaciones encontradas durante el desarrollo del presente proyecto de titulación.

Finalmente se muestran los anexos con información referente al levantamiento de los servidores requeridos en el diseño de la red, propuestas comerciales para elementos pasivos, equipos activos e información ligada al desarrollo del presente proyecto.

# CAPÍTULO 1

## FUNDAMENTOS TEÓRICOS

### 1.1 INTRODUCCIÓN

En este capítulo se detallan los conceptos fundamentales sobre redes de comunicación, definiendo tópicos tales como: Sistema de Cableado Estructurado, redes convergentes, tecnologías de transmisión de datos y VoIP<sup>1</sup> entre otros, los mismos que posteriormente son utilizados en el diseño de la red INTEGRADA de voz y datos para la Unidad Educativa Temporal “Jaime Roldós Aguilera” de la ciudad de Santo Domingo de los Tsáchilas.

### 1.2 REDES DE ÁREA LOCAL [13]

Una red de área local está definida como un sistema de comunicación de datos que permite la comunicación directa de cierto número de dispositivos entre sí dentro de un área geográfica reducida, hasta 5000 metros dependiendo del medio de transmisión a utilizar, y empleando canales físicos de comunicación de velocidad moderada o alta, que puede variar entre 10 Mbps a 1000 Mbps.

Entre sus principales beneficios se tienen:

- **La compartición de recursos.**- Permite tener datos e información actualizados, el acceso a periféricos remotos, utilizar programas y aplicaciones de una forma centralizada.
- **Incremento de la capacidad de comunicaciones.**- Brinda un gran abanico de posibilidades, como correo electrónico, intranet, etc.
- **Reducción de costos.**- El número de recursos a utilizar son menores ya que éstos se comparten por un conjunto de ordenadores, e indirectamente por el aumento de la productividad.

---

<sup>1</sup> **VoIP:** Tecnología utilizada para la transmisión de paquetes de voz sobre una red IP

Al hablar de redes de área local es indudable hacer referencia a Ethernet y al estándar 802.3 de la IEEE<sup>2</sup>.

### 1.2.1 ETHERNET E IEEE 802.3

Ethernet es un estándar de redes de área local para computadores con acceso al medio por detección de portadora y detección de colisiones CSMA/CD (*Carrier Sense Multiple Access / Collision Detection*). [14]

IEEE 802.3 fue el primer intento para estandarizar Ethernet, estableciendo así lo que ahora se llama redes *Ethernet*. [15]

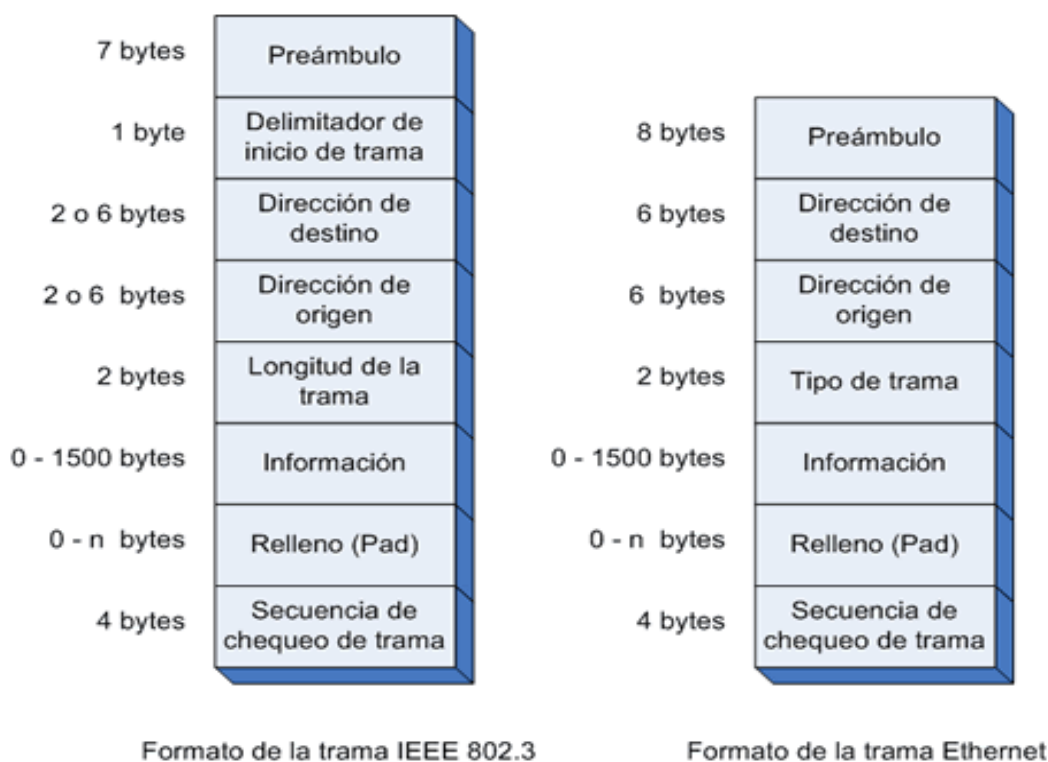


Figura 1. 1 Trama Ethernet vs trama 802.3 [16]

Si bien Ethernet y 802.3 son muy similares, existen ciertos campos que los diferencian, como se lo puede apreciar en la figura 1.1 donde se muestra la trama de cada uno de los estándares.

<sup>2</sup> IEEE: Institute of Electrical and Electronics Engineers

También se puede evidenciar las diferencia entre Ethernet y 802.3 en la definición de las funciones de sus capas en relación al modelo OSI<sup>3</sup>.

La figura 1.2 muestra el alcance que tiene 802.3 dentro del modelo de referencia OSI.

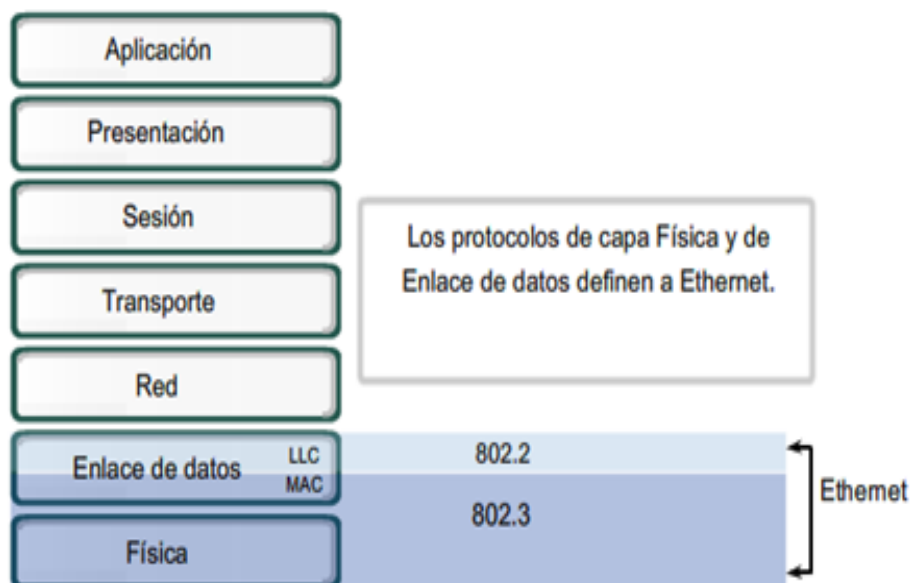


Figura 1. 2 Relación de 802.3 con el modelo OSI [17]

Como se observa 802.3 se encarga de indicar el medio físico para la red y parte de la capa de enlace de datos, mediante la subcapa MAC.

La acogida que tuvo 802.3 ha permitido que el estándar siga avanzando y genere nuevos estándares para las diferentes aplicaciones que se tiene en la actualidad, estableciendo así estándares para redes inalámbricas, redes de alta velocidad, etc.

## 1.2.2 TECNOLOGÍAS LAN

Las tecnologías de redes de área local están definidas principalmente por los siguientes parámetros.

<sup>3</sup> OSI: *Open System Interconnection*

- **Velocidad de transmisión.-** Velocidad a la que transmite la tecnología LAN.
- **Tipo de cable.-** Especifica el tipo de medio de transmisión.
- **Longitud máxima.-** Distancia máxima que puede haber entre dos nodos adyacentes (sin estaciones repetidoras).
- **Topología.-** Determina la forma física de la red. Bus si se usan conectores T (hoy sólo usados con las tecnologías más antiguas) y estrella si se usan *hubs* (estrella de difusión) o *switches* (estrella conmutada).

En base a estos parámetros se tienen las tecnologías mostradas en la figura 1.3, donde cada una tiene sus propias definiciones pero siempre basadas en el estándar 802.3.

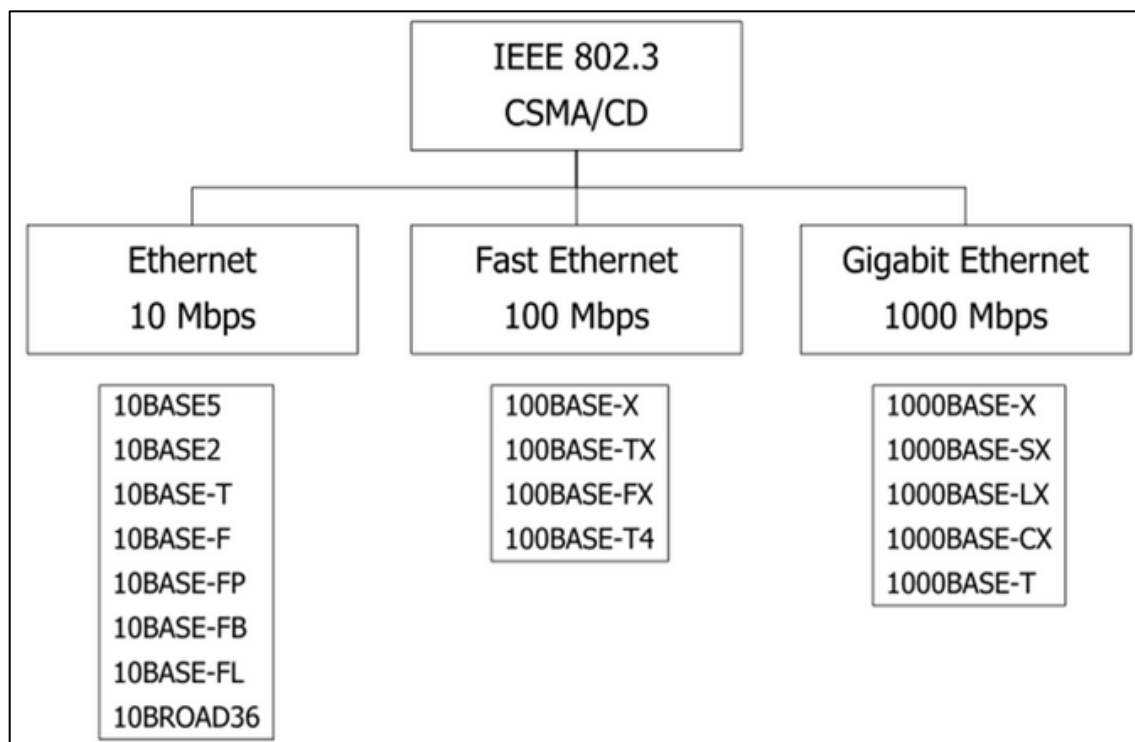


Figura 1. 3 Tecnologías Ethernet [18]

El nombre de las tecnologías viene dado directamente por la velocidad a la que se transmiten los datos, por ejemplo si es una tecnología 100BASE-X hace referencia a que su velocidad de transmisión es de 100 Mbps y la letra subsiguiente al medio de transmisión que utiliza.

### 1.3 REDES CONVERGENTES [19]

Los sistemas de comunicación han evolucionado drásticamente en los últimos años, generando nuevos conceptos y formas de establecer las comunicaciones.

Hace poco se tenían grandes redes de datos y voz indistintamente dentro de las organizaciones que así lo requerían; sin embargo, hoy en día aparece un nuevo concepto llamado redes convergentes.

Las redes convergentes, son aquellas redes de comunicación que permiten integrar varios servicios dentro de la misma basados en el protocolo IP<sup>4</sup>; es decir, se rompe el esquema tradicional de manejar servicios por separados, para manejarlos en conjunto. Este concepto aparece gracias a los avances que han sufrido las Tecnologías de Información y Comunicación (TIC) y el Internet.

Entre las necesidades que mejor satisfacen las redes convergentes están: administración, mantenimiento y manejo de la información, llevando a quienes decidan optar por este nuevo concepto a tener ahorros sustanciales en tiempo y dinero, además de aumentar la productividad dentro del ambiente a desenvolverse.

Uno de los principales beneficios que brindan la redes convergentes es la integración de voz y datos; probablemente los dos servicios más requeridos en el ambiente empresarial.

Al ofrecer servicios que demandan grandes anchos de banda y que no son tolerantes a retardos, como lo es el video, las redes convergentes utilizan tecnologías LAN de alta velocidad y conceptos de calidad de servicio QoS<sup>5</sup> para lograr una transmisión adecuada, sin pérdidas ni bloqueos.

---

<sup>4</sup> **IP:** *Internet Protocol.*- Es un protocolo de comunicación de datos clasificado funcionalmente en la Capa de Red según el modelo internacional OSI.

<sup>5</sup> **QoS:** *Quality of Service.*- Es la capacidad de manejar con prioridad los diferentes tipos de datos que cursan por la red



La calidad de servicio hace referencia a cómo se debe tratar la información que atraviesa por la red, dependiendo si la misma es o no susceptible a retardos, pérdidas, y errores en la transmisión.

Para ello se utilizan diferentes mecanismos detallados en el estándar 802.3 Q, como por ejemplo etiquetar tramas de diferentes VLAN's<sup>6</sup>, o priorizarlas con el uso de bits adicionales mediante el estándar 802.3 p, etc. [20]

#### 1.4 VOZ SOBRE IP (VoIP)

Una de las primeras necesidades surgidas dentro de una red convergente fue la integración de voz con el servicio de datos, apareciendo así tecnologías para la transmisión de voz como VoFR<sup>7</sup>, VoATM<sup>8</sup> y la más popular voz sobre IP, denominada comúnmente como VoIP.

La tecnología de transmisión de voz sobre IP, es aquella que ha tenido mayor acogida, gracias a que la mayoría de redes *Ethernet* trabajan conjuntamente con el protocolo IP; su funcionamiento está basado en transportar la voz, previamente convertida a datos, entre dos puntos distantes.

Con esto se posibilita utilizar redes de datos para efectuar conversaciones de voz, y por ende desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, en un principio voz, datos y posteriormente video o cualquier tipo de información multimedia.

La VoIP por lo tanto, no es en sí un servicio sino una tecnología, que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales proporcionados por la RTPC<sup>9</sup>.

---

<sup>6</sup> **VLAN's:** *Virtual Local Area Network.*- método de crear redes lógicas e independientes dentro de una misma red física

<sup>7</sup> **VoFR:** *Voice over Frame Relay.*- Mecanismo utilizado para transmitir paquetes de voz sobre una red FR

<sup>8</sup> **VoATM:** *Voice Over ATM.*- Mecanismo utilizado para transmitir paquetes de voz sobre una red ATM

<sup>9</sup> **RTPC:** *Red Telefónica Pública Conmutada.*- Red analógica de conmutación para transmitir voz.

### 1.4.1 ESTANDARIZACIÓN DE LA VoIP

Con el surgimiento de la tecnología de transmisión de voz sobre IP, también aparecieron organismos reguladores de la misma, con la finalidad de estandarizar su uso en los diferentes ambientes a desenvolverse.

Los principales organismos de estandarización para la transmisión de VoIP son la ITU<sup>10</sup>, IETF<sup>11</sup>, IMTC<sup>12</sup> y ETSI<sup>13</sup>. Estos organismos han generado estándares para VoIP entre los cuales destacan por ejemplo H.323 y SIP.

### 1.4.2 ESPECIFICACIÓN H.323

En el año 1996 la ITU presenta la especificación H.323 titulada “Sistemas Telefónicos Visuales y Equipo para Redes de Área Local que Proporcionan una Calidad de Servicio No Garantizada”.

H.323 hace referencia a una gran cantidad de protocolos, por lo que se conoce como especificación. Estos protocolos son específicos para realizar la codificación de voz, establecimiento de llamadas, señalización, transporte de datos y otras tareas.

La tabla 1.1 muestra el desarrollo cronológico de lo que hoy en día se conoce como especificación H.323.

Norma	Año	Transporte	Audio	Video	Control	Multiplexado
H.320	1990	ISDN	G.711	H.261	H.242	H.221
H.324	1995	POTS	G.723	H.263	H.245	H.223
H.310/321	1996	ATM	MPEG-1	H.262	H.245	H.222
H.323	1996/8	LAN	G.711	H.261/3	H.245	H.225

Tabla 1. 1 Cronología de la especificación H.323 [21]

<sup>10</sup> ITU: *International Telecommunication Union*

<sup>11</sup> IETF: *Internet Engineering Task Force*

<sup>12</sup> IMTC: *International Multimedia Teleconferencing Consortium*

<sup>13</sup> ETSI: *European Telecommunications Standards Institute*

Finalmente y gracias a la acogida de la especificación por parte de los usuarios, H.323 se convierte en estándar validado por la ITU, que brinda flexibilidad para transmisiones de audio y video.

#### 1.4.2.1 Componentes H.323

La recomendación H.323 de la ITU, también hace referencia a los componentes de la red que se muestran en la figura 1.4, los cuales existirán o no dependiendo de la complejidad de la misma, disponiendo así de uno o varios elementos, o simplemente los terminales.

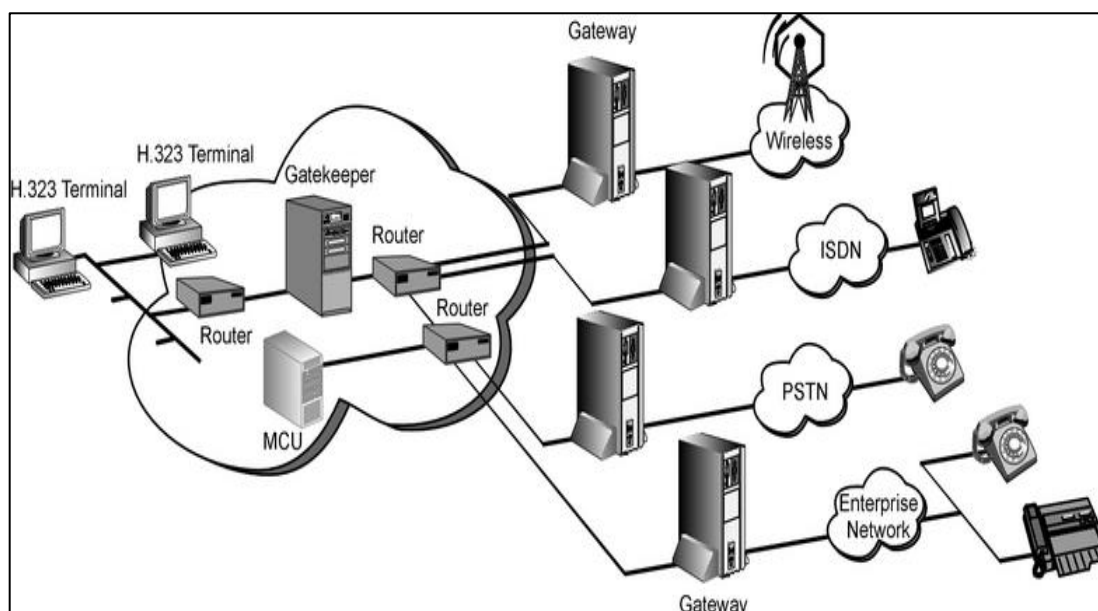


Figura 1. 4 Componentes de la red según recomendación H.323 de la ITU [21]

A continuación se realizará una breve descripción de cada uno de los componentes mostrados en la figura en mención.

##### 1.4.2.1.1 Terminal [22]

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU).

Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y/o datos entre los dos terminales.

Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

Un terminal H.323 consta de las interfaces del equipo de usuario, el códec de video, el códec de audio, el equipo telemático, la capa H.225, las funciones de control del sistema y la interfaz con la red por paquetes.

- **Equipos de adquisición de información.-** Es un conjunto de cámaras, monitores, dispositivos de audio (micrófono y altavoces) y aplicaciones de datos, e interfaces de usuario asociados a cada uno de ellos.
- **Códec de audio.-** Todos los terminales deberán disponer de un códec de audio, para codificar y decodificar señales vocales de los diferentes algoritmos de codificación de la voz como son, ley A y ley *u*. La tabla 1.2 muestra algunos ejemplos de *codecs* de audio.

Codec	Name	Bit rate (kb/s)	Comments
G.711	PCM: Pulse Code Modulation	64,56	Codec "base", utiliza dos posibles leyes de compresión: u-law y A-law
G.723.1	Hybrid MPC-MLQ and ACELP	6.3, 5.3	Desarrollado originalmente para video conferencias en la PSTN, es actualmente utilizado en sistemas de VoIP
G.728	LD-CELP: Low-Delay code excited linear prediction	40, 16, 12.8, 9.6	Creado para aplicaciones DCME (Digital Circuit Multiplex Encoding)
G.729	CS-ACELP Conjugate Structure Algebraic Codebook Excited Linear Prediction	11.8, 8, 6.4	Ampliamente utilizado en aplicaciones de VoIP, a 8 kb/s
AMR	Adaptive Multi Rate	12.2 A 4.75	Utilizado en redes celulares GSM

Tabla 1. 2 Codecs de audio [23]

- **Códec de video.-** En los terminales H.323 es opcional, algunos ejemplos de codecs de video con sus respectivas características se puede apreciar en la tabla 1.3.

Característica	MPEG-1	MPEG-2	MPEG-4	H.264/MPEG-4 Part 10/AVC
Tamaño del macro-bloque	16x16	16x16 (frame mode) 16x8 (field mode)	16x16	16x16
Tamaño del bloque	8x8	8x8	16x16 8x8, 16x8	8x8, 16x8, 8x16, 16x16, 4x8, 8x4, 4x4
Transformada	DCT	DCT	DCT/DWT	4x4 Integer transform
Tamaño de la muestra para aplicar la transformada	8x8	8x8	8x8	4x4
Codificación	VLC	VLC	VLC	VLC, CAVLC, CABAC

Tabla 1. 3 Codec´s de video [23]

- **Canal de datos.-** Uno o más canales de datos son opcionales y pueden ser unidireccionales o bidireccionales. Es por estos canales por donde se transmite la información entre un terminal y otro.
- **Retardo en el trayecto de recepción.-** Incluye el retardo añadido a las tramas para mantener la sincronización, y tiene en cuenta la fluctuación de las llegadas de paquetes.

No suele usarse en la transmisión sino en recepción, para añadir el retardo necesario en el trayecto de audio para, por ejemplo, lograr la sincronización con el movimiento de los labios en una videoconferencia.

- **Unidad de control del sistema.-** Proporciona la señalización necesaria para el funcionamiento adecuado del terminal. Está formada por tres bloques principales: Función de control H.245, función de señalización de llamada H.225 y función de señalización RAS.

- **Capa H.225.-** Se encarga de dar formato a las tramas de video, audio, datos y control transmitidos en mensajes de salida hacia la interfaz de red, así como de recuperarlos de los mensajes que han sido introducidos desde la interfaz de red.

Además lleva a cabo la alineación de trama, la numeración secuencial y la detección/corrección de errores.

- **Interfaz de red de paquetes.-** Es específica en cada implementación. Debe proveer los servicios descritos en la recomendación H.225.

La figura 1.2 muestra el diagrama de bloques un terminal H.323.

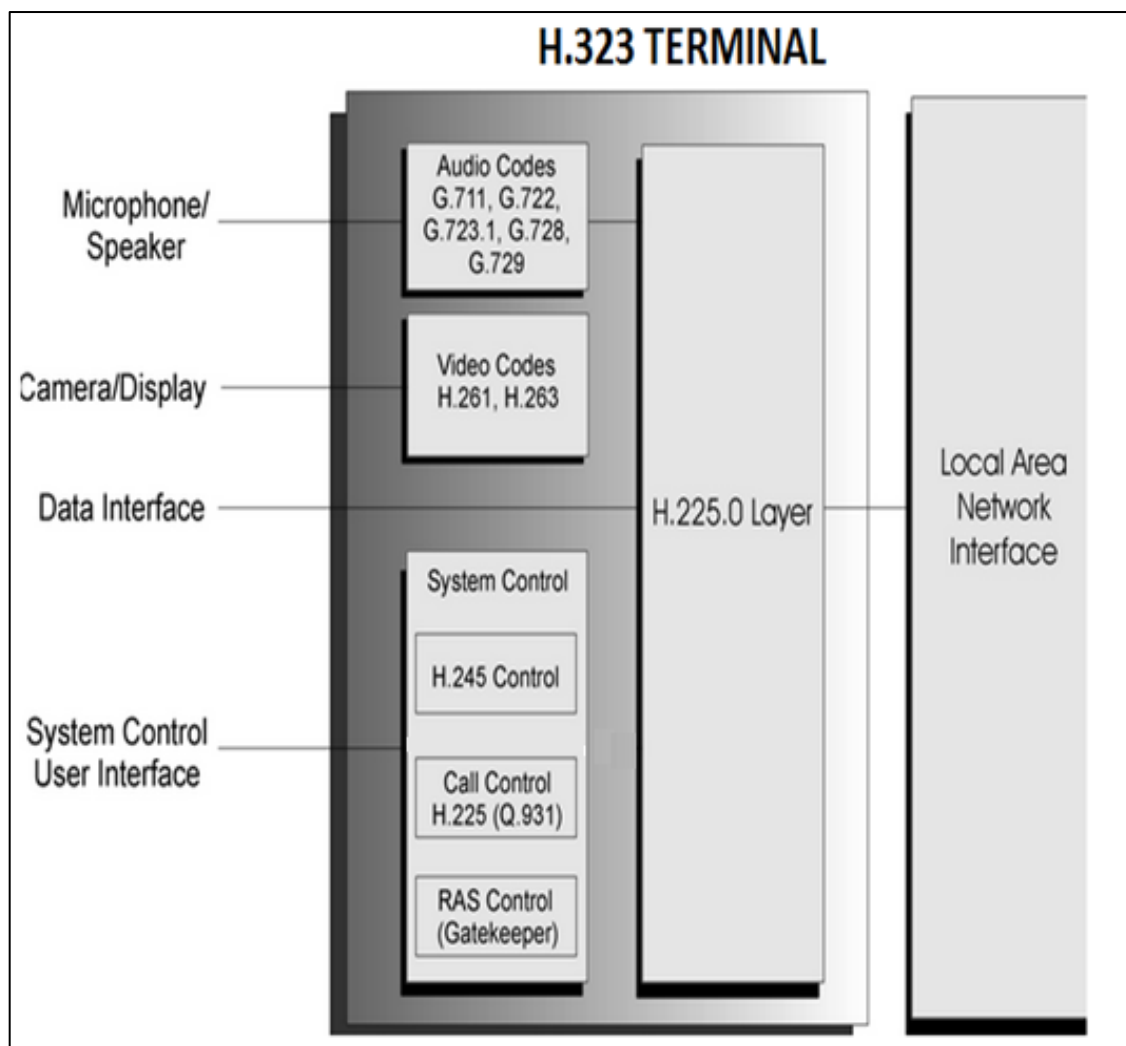


Figura 1. 5 Diagrama de bloques de un terminal H.323 [24]

#### 1.4.2.1.2 *Gateway*

El *gateway* es el componente que permite a las terminales que estén dentro de una red H.323 comunicarse con usuarios fuera de la red, que usen terminales no compatibles con H.323, tales como teléfonos comunes, teléfonos ISDN<sup>14</sup>, etc.

En otras palabras, el *gateway* permite interoperabilidad con otras redes de comunicaciones. Si solamente se requiere comunicación entre usuarios de una misma red H.323, no se necesita de un *gateway*.

#### 1.4.2.1.3 *Gatekeeper*

El *Gatekeeper* (GK) o controlador de acceso, es un dispositivo opcional que proporciona servicio de control de llamada a los puntos finales. En una red H.323 puede existir más de un *gatekeeper* que interactúan entre sí.

Además puede realizar funciones como: traducción de direcciones, control de admisión, control de ancho de banda, registro de actividad

#### 1.4.2.1.4 *Unidad de control de multipunto (MCU)*

La unidad de control multipunto (MCU) soporta conferencias entre tres o más terminales y *gateway* en una conferencia multipunto. También puede negociar capacidades de los terminales en una conferencia y revisarlos durante la misma para garantizar un nivel común para el proceso de audio y video.

### 1.4.2.2 **Stack de Protocolos H.323**

Como se mencionó anteriormente, la recomendación H.323 hace referencia a una gran cantidad de protocolos para su funcionamiento.

---

<sup>14</sup> **ISDN**: *Integrated Services Digital Network*.- Red analógica que se utiliza para transmitir también señales digitales.

A continuación se explica un poco más a detalle los protocolos más significativos para H.323.

- **RTP (*Real-Time Transport Protocol*).**- El Protocolo de Transporte en Tiempo Real o RTP, surgió con la idea de crear un protocolo específico para la gran demanda de recursos en tiempo real por parte de los usuarios, recursos tales como la música, videoconferencia, video, telefonía en Internet y más aplicaciones multimedia. En 1996 se publica en el RFC 1889 el estándar del protocolo RTP.

RTP se ejecuta, por lo general, sobre UDP, ya que posee menor retardo que TCP. Por tanto con UDP se gana velocidad a cambio de sacrificar la confiabilidad que TCP ofrece. Debido a esto, RTP no garantiza la entrega de todos los paquetes, ni la llegada de éstos en el instante adecuado.

La función básica de RTP es multiplexar varios flujos de datos en tiempo real en un solo flujo de paquetes UDP, pudiéndose enviar tanto a un solo destino (*unicast*) o múltiples destinos (*multicast*).

- **H225 - RAS (*Registration, Admission and Status*).**- Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323; se encarga del registro, control de admisión, control del ancho de banda, el estado y desconexión de los participantes de una comunicación.
- **H.245.**- Protocolo de control utilizado en el establecimiento y control de una llamada.
- **Q.931: (*Digital Subscriber Signalling*).**- Este protocolo se define para la señalización de accesos a ISDN básicos.
- **RSVP (*Resource ReSerVation Protocol*).**- Protocolo de reserva de recursos en la red para cada flujo de información de usuarios.



- **T.120.-** La recomendación T.120 define un conjunto de protocolos para conferencia de datos multimedia, proporcionando así al usuario una experiencia multimedia muy flexible.

T.120 proporciona capacidades tales como compartición de aplicaciones (T.128), pizarrón electrónico (T.126), transferencia de archivos (T.127) y chat de texto (T.134).

En la figura 1.6 se puede observar el *stack* de protocolos de H.323 antes descritos.

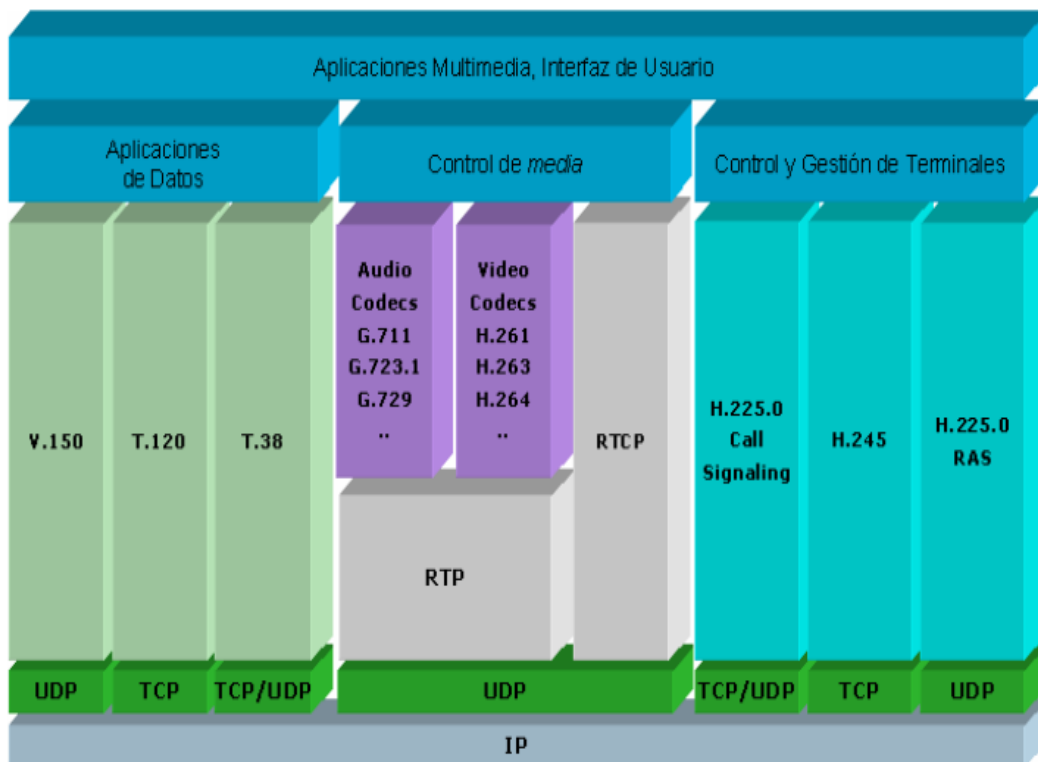


Figura 1. 6 *Stack* de Protocolos H.323 [22]

#### 1.4.2.3 Establecimiento de Llamadas H.323

El establecimiento de llamadas en una red que utiliza H.323 está especificada en varias fases; cada una de ellas utiliza los protocolos antes mencionados.

#### 1.4.2.3.1 Fase de Establecimiento de la llamada H.323

En esta fase lo primero que se observa es que uno de los terminales se registra en el *gatekeeper* utilizando el protocolo RAS (Registro, admisión y estado) con los mensajes ARQ (*Admission Request*) y ACF (*Admission Confirmation*). Luego utilizando el protocolo H.225 se envía un mensaje de *SETUP* para iniciar una llamada H.323; entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante, y la dirección IP y puerto del llamado.

El terminal llamado contesta con un *CALL PROCEEDING* advirtiendo del intento de establecer una llamada. En este momento el segundo terminal tiene que registrarse con el *gatekeeper* utilizando el protocolo RAS de manera similar al primer terminal, y luego procede a generar tono y lo indica al terminal que llama mediante el mensaje *ALERTING*; finalmente la conexión se establece y se envía el mensaje de *CONNECT*.

En la figura 1.7 se pueden apreciar los mensajes y procesos que intervienen en la fase de establecimiento de la llamada H.323.

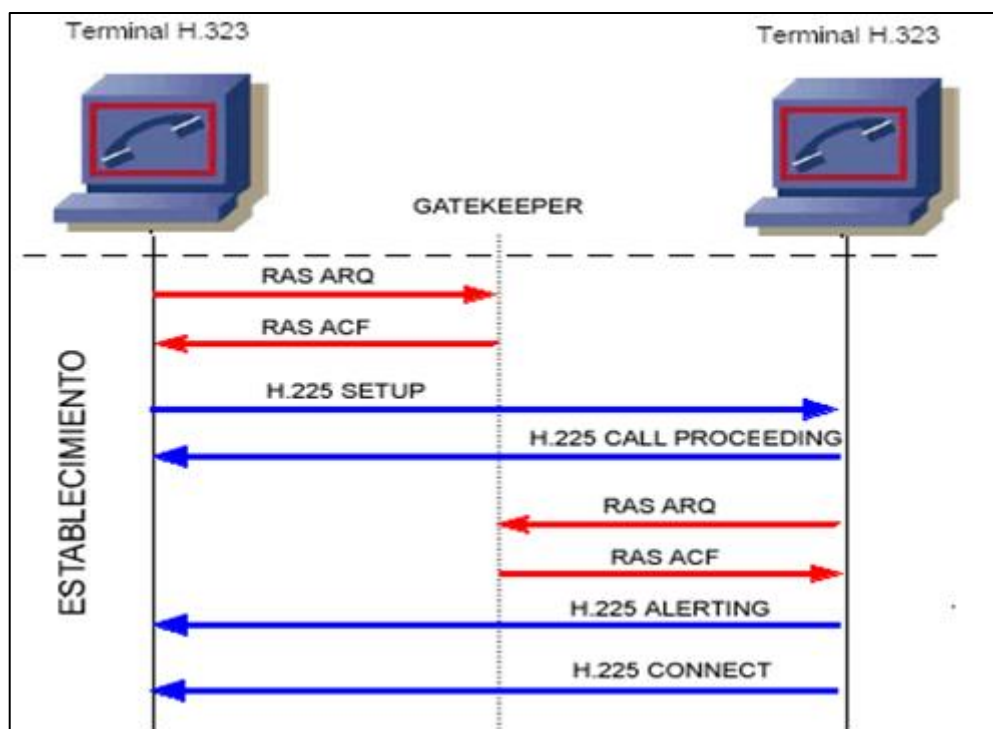


Figura 1. 7 Fase de Establecimiento de Llamada H.323 [25]

#### 1.4.2.3.2 Fase de Señalización de Control

En esta fase mediante el protocolo H.245 se establece la negociación entre los dos terminales (control de conferencia) determinando las capacidades de los usuarios, codecs a utilizar, etc. Así mismo y mediante el intercambio de los mensajes (petición y respuesta) se establece quién será master y esclavo en la comunicación, para finalmente abrir el canal de comunicación mediante las direcciones IP y puertos de los participantes. Los principales mensajes H.245 que se utilizan en esta fase son:

- **Terminal Capability Set (TCS).**- Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.
- **Open Logical Channel (OLC).**- Mensaje para abrir el canal lógico de información que contiene información para permitir la recepción y codificación de los datos. Contiene información del tipo de datos que será transportado.

En la figura 1.8 se observan los mensajes que son intercambiados entre los terminales H.323 en la fase de señalización.

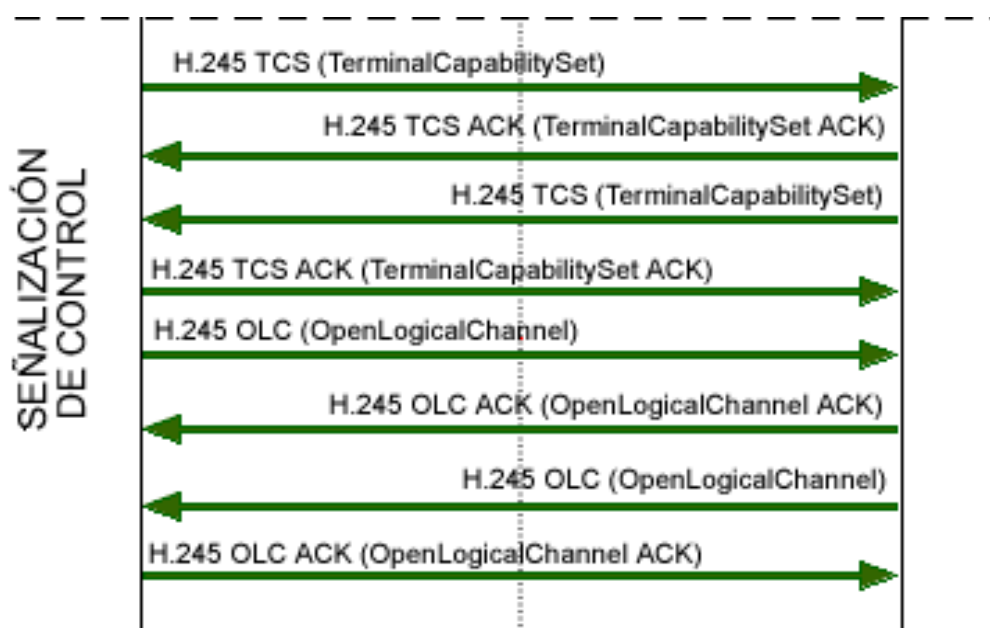


Figura 1. 8 Fase de señalización de control [25]

#### 1.4.2.3.3 Fase de Transmisión de Datos

Una vez que se terminan todas las negociaciones, puede comenzar el flujo de datos utilizando RTP. Tal flujo se maneja mediante RTCP, que juega un papel importante en el control de congestión. Si el vídeo está presente, RTCP maneja la sincronización de audio/vídeo. La figura 1.9 muestra el flujo de datos entre dos terminales H.323.

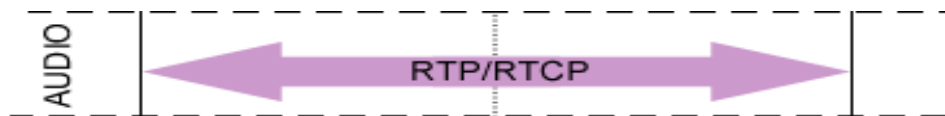


Figura 1. 9 Fase de transmisión de voz [25]

#### 1.4.2.3.4 Fase de Liberación de la Conexión

En esta fase cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes CLC (*Close Logical Channel*) y ESC (*End Session Command*) de H.245. Posteriormente utilizando H.225 se cierra la conexión con el mensaje *RELEASE COMPLETE* y por último liberan los registros utilizando mensajes del protocolo RAS. La figura 1.10 muestra la fase de liberación de la llamada H.323.

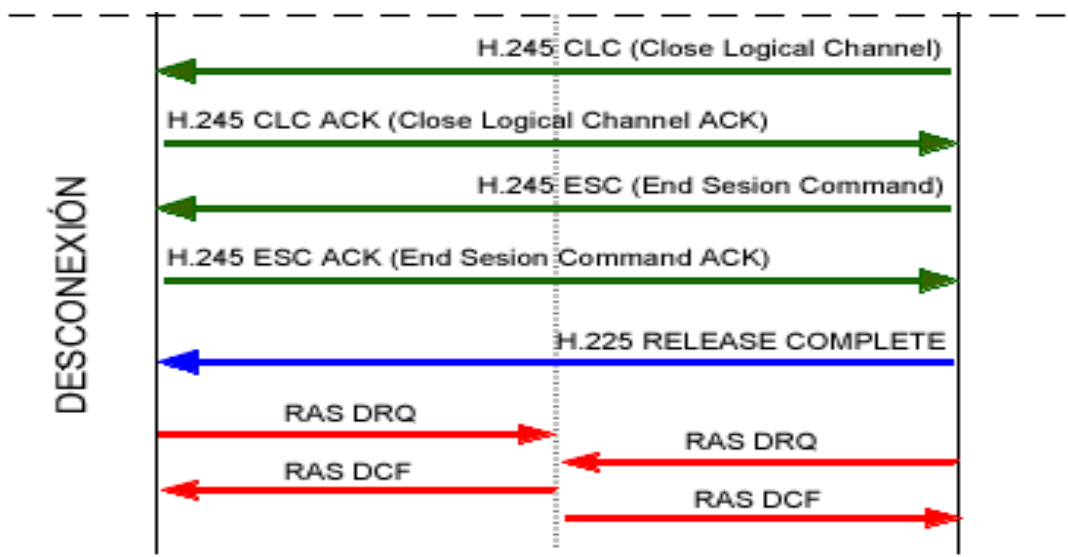


Figura 1. 10 Fase de Liberación de Conexión [25]

### 1.4.3 SIP (Session Initiation Protocol)

SIP es un protocolo de control desarrollado por la Fuerza de Tarea en Ingeniería de Internet - IETF (RFC 2543). Se aprobó a principios de 1999 para el control, tanto de conferencias multimedia y llamadas telefónicas por Internet, como de distribución de contenidos multimedia.

Es un protocolo joven que se ha convertido en la alternativa a H.323, y son los dos únicos protocolos que existen en la actualidad para el control de sesiones multimedia en Internet.

Mientras que H.323 surgió inicialmente orientado al soporte de comunicaciones multimedia en entornos LAN, SIP es un protocolo pensado desde un primer momento para Internet, con arquitectura cliente/servidor mensajes tipo texto similares a los mensajes HTTP<sup>15</sup>, frente a los mensajes binarios con codificación ASN.1<sup>16</sup> de H.323.

El conjunto amplio de protocolos que incorpora H.323 repercute negativamente en los tiempos de respuesta, así como en el tamaño del código que tienen que incorporar los equipos H.323; lo que lleva a que los fabricantes a veces incorporen sólo aquellas partes que necesitan, con los consiguientes problemas de interconexión.

Dadas las ventajas de SIP frente a H.323, han empezado a aparecer pasarelas SIP-H.323 para soportar la transición a SIP sin perder las inversiones realizadas en los equipos H.323. SIP utiliza al SDP (*Session Description Protocol*) para el intercambio y negociación de las capacidades de la sesión y adicionalmente puede interactuar con un amplio número de protocolos (DNS<sup>17</sup>, DHCP<sup>18</sup>, provisión de QoS, transporte, etc.).

---

<sup>15</sup> **HTTP:** *Hypertext Transfer Protocol.*- Protocolo utilizado en la web para la transferencia de texto.

<sup>16</sup> **ASN1:** *Abstract Syntax Notation.*- es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas.

<sup>17</sup> **DNS:** *Domain Name Server.*- Sistema para asignar nombres a equipo y servicios de red.

<sup>18</sup> **DHCP:** *Dinamic Host Configuration Protocol.*- Protocolo utilizado para la asignación automática de IPs.

### 1.4.3.1 Componentes SIP

El protocolo SIP para su correcto funcionamiento define algunos elementos, cuyas funciones y características serán detalladas a continuación.

#### 1.4.3.1.1 Agentes de usuario (UAs)

Son los puntos extremos del protocolo; es decir, son los que emiten y consumen los mensajes del protocolo SIP como por ejemplo: videoteléfonos o teléfonos IP, un cliente de *software* (*softphone*) y cualquier otro dispositivo similar. Todos los agentes de usuario se comportan como clientes UAC (*User Agent Clients*) y como servidores UAS (*User Agent Servers*).

#### 1.4.3.1.2 Servidores de registro

El protocolo SIP permite establecer la ubicación física de un usuario determinado, esto es, en qué punto de la red está conectado. Para ello se vale del mecanismo de registro.

Este mecanismo funciona como sigue: cada usuario tiene una dirección lógica que es invariable respecto de la ubicación física del usuario.

Una dirección lógica del protocolo SIP es de la forma usuario@dominio, es decir tiene la misma forma que una dirección de correo electrónico.

La dirección física (denominada "dirección de contacto") es dependiente del lugar en donde el usuario está conectado (de su dirección IP).

Cuando un usuario inicializa su terminal (por ejemplo conectando su teléfono o abriendo su *software* de telefonía SIP) el agente de usuario SIP que reside en dicho terminal envía una petición con el método REGISTER a un servidor de registro, informando a qué dirección física debe asociarse la dirección lógica del usuario.

El servidor de registro realiza entonces dicha asociación denominada (*binding*), esta asociación tiene un período de vigencia y si no es renovada, caduca. También puede terminarse mediante un “desregistro”; la forma en que dicha asociación es almacenada en la red no es determinada por el protocolo SIP, pero es vital que los elementos de la red SIP accedan a dicha información.

En la figura 1.11 se puede apreciar cómo se establece el registro de un UA con el servidor de registro.

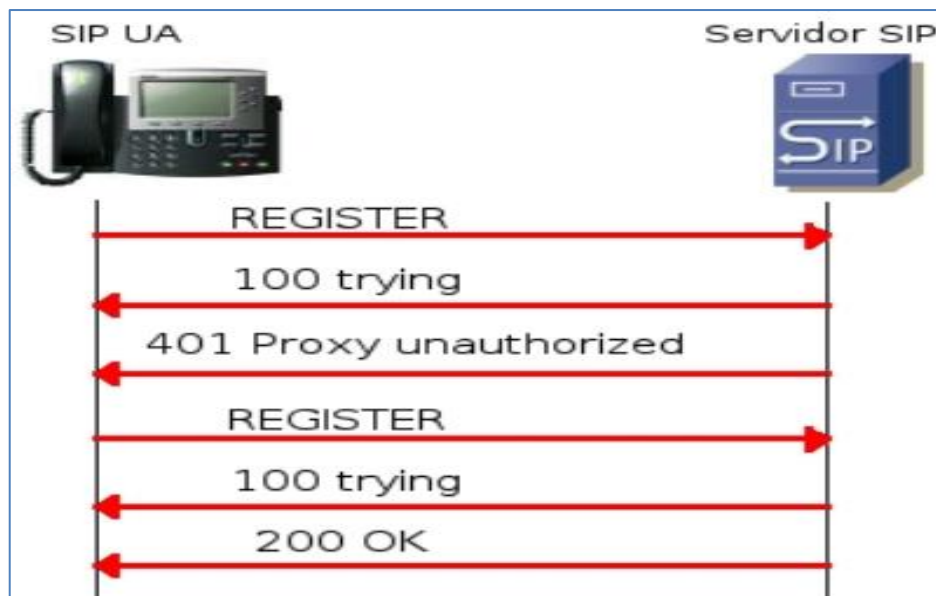


Figura 1. 11 Servidor de Registro SIP [26] [27]

#### 1.4.3.1.3 Servidores proxy y de redirección

Para encaminar un mensaje entre un UAC y un UAS normalmente se recurre a los servidores. Estos servidores a su vez se sirven del sistema DNS para localizar los dominios, pudiendo actuar de dos maneras:

- Como intermediario, encaminando el mensaje hacia destino
- Como redirector, generando una respuesta que indica al remitente la dirección del destino o de otro servidor que lo acerque al destino.

La principal diferencia es que el servidor intermediario forma parte de la comunicación, mientras que el servidor de redirección una vez que indica al UAC cómo encaminar el mensaje ya no interviene más.

Un mismo servidor puede actuar como redirector o como intermediario dependiendo de la situación. En la figura 1.12 se observa un servidor *proxy* cumpliendo el papel de intermediario, ya que está formando parte de la comunicación.

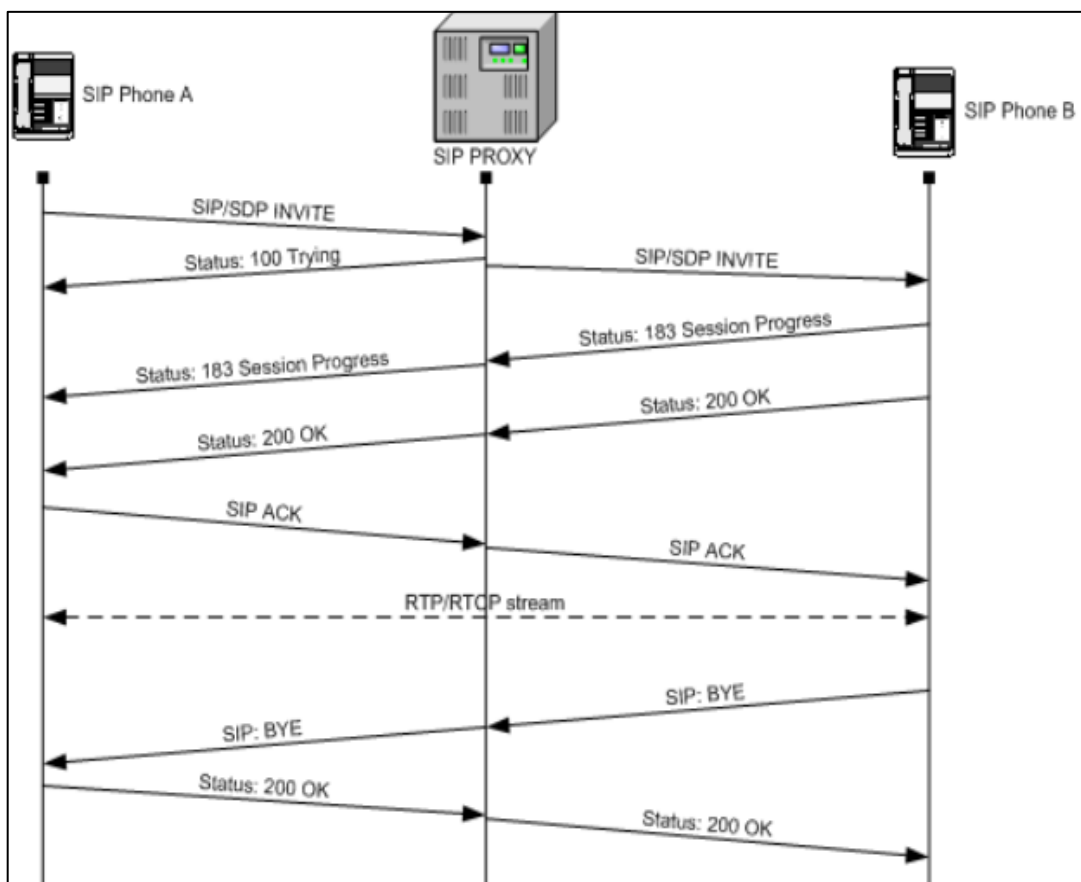


Figura 1. 12 Servidor Proxy SIP [26] [27]

#### 1.4.3.1.4 Servidores de localización

Son bases de datos que contienen información de localización para los UA registrados; pueden ser utilizados por los servidores de redirección o *proxy* como lo muestra la figura 1.13.



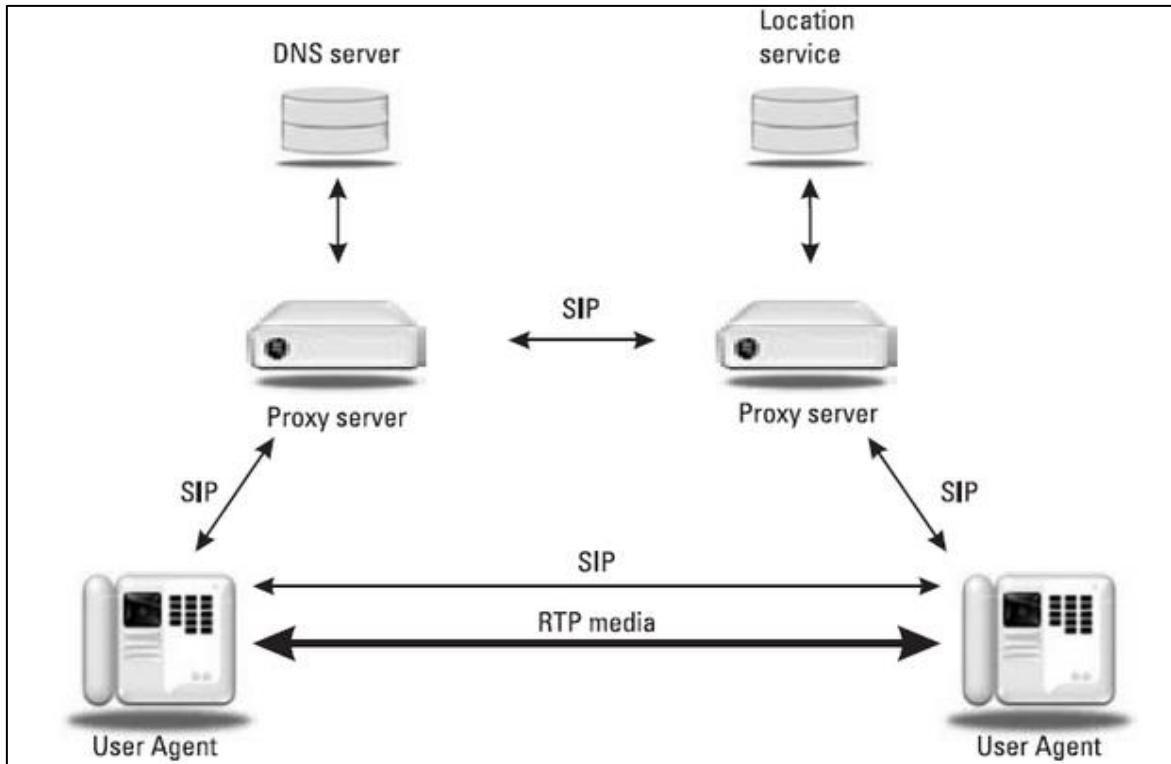


Figura 1. 13 Servidor de Localización SIP [26] [27]

#### 1.4.3.2 Establecimiento de Llamadas SIP

Para establecer una llamada, el llamante crea una conexión TCP con el llamado; ésta se realiza utilizando un acuerdo de tres vías. El UA que desea establecer la sesión envía un mensaje *INVITE* en un paquete TCP al servidor *proxy*, indicando la dirección de destino, la capacidad, los tipos de medios y los formatos que él posee.

El servidor *proxy* SIP investiga donde está el usuario B y lo solicita en el servidor de localización, a continuación responde al usuario A con un mensaje 100 *TRYING*.

Una vez que la petición llega al usuario B se genera el mensaje 180 *RINGING* y si la llamada es aceptada se envía al usuario A un código de respuesta tipo HTTP de numeración 200, que indica la aceptación de la llamada.

Finalmente el usuario A genera un ACK que señala que la comunicación se encuentra establecida; indicando que pueden comenzar el flujo de datos utilizando el protocolo RTP y que será controlado mediante el protocolo RTCP

Una vez terminada la comunicación cualquiera de los usuarios puede solicitar la terminación de la llamada enviando un mensaje *BYE*. Cuando el otro lado confirma su recepción, se termina la llamada. El proceso detallado de una llamada se puede apreciar de mejor manera en la figura 1.14.

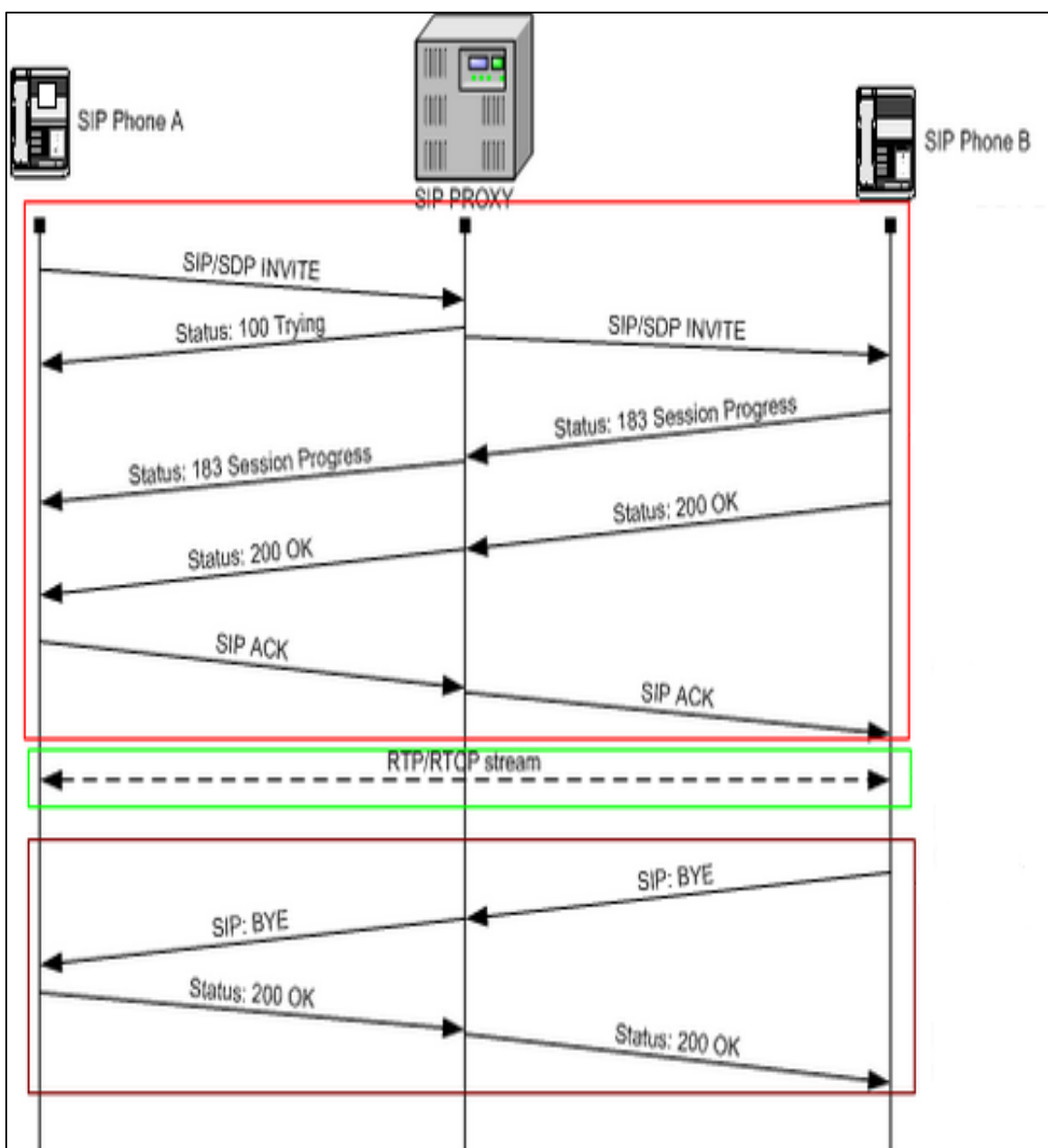


Figura 1. 14 Establecimiento y liberación de llamada SIP [28]

#### 1.4.4 TIPOS DE ARQUITECTURAS PARA VoIP

En el pasado, todas las redes de voz fueron construidas usando una arquitectura centralizada, en la cual los teléfonos eran controlados por los conmutadores centralizados; este modelo trabajó bien para los servicios de telefonía básica.

Uno de los beneficios de la tecnología VoIP, es que permite a las redes ser construidas usando una arquitectura centralizada o distribuida. Esta flexibilidad permite a las compañías construir redes caracterizadas por una administración simplificada e innovación de teléfonos, dependiendo del protocolo utilizado.

##### 1.4.4.1 Arquitectura Centralizada

En general, la arquitectura centralizada está asociada con los protocolos MGCP y MEGACO.

Estos protocolos fueron diseñados para un dispositivo centralizado llamado *Controlador Media Gateway* o *Call Agent*, que maneja la lógica de conmutación y control de llamadas como lo muestra la figura 1.15.

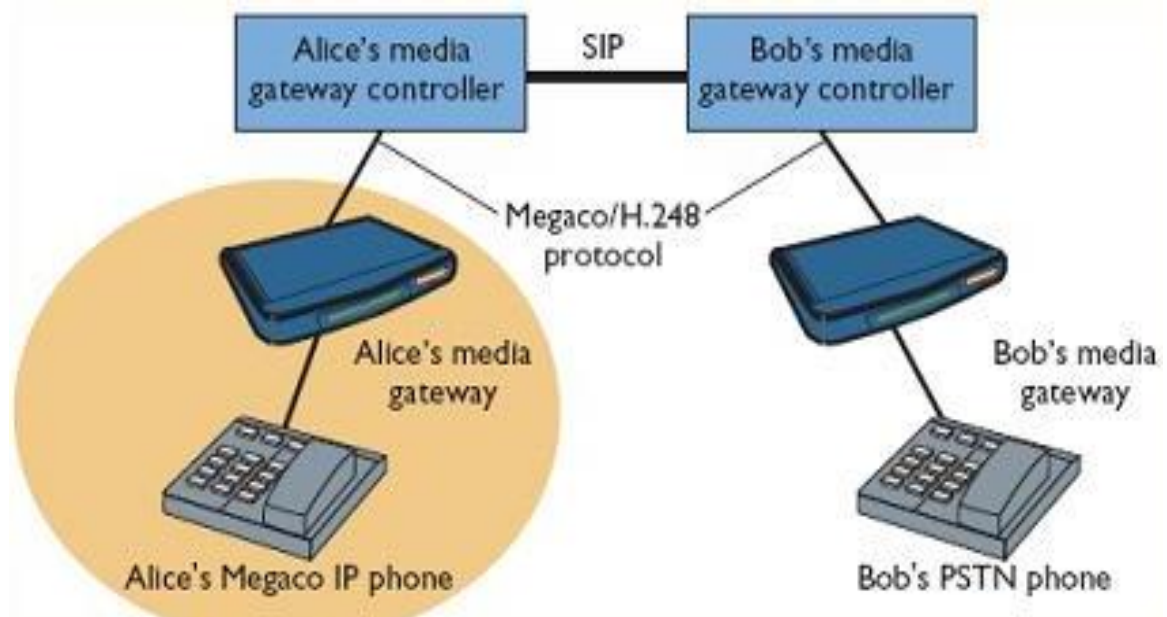


Figura 1. 15 Arquitectura Centralizada

#### 1.4.4.2 Arquitectura Distribuida

La arquitectura distribuida está asociada con los protocolos H.323 y SIP. Estos protocolos permiten que la inteligencia de la red sea distribuida entre dispositivos de control de llamadas y sus *endpoints*.

La inteligencia en esta instancia se refiere a establecer las llamadas y sus características, enrutamiento de llamadas, provisionamiento, facturación o cualquier otro aspecto de manejo de llamadas.

Los *endpoints* pueden ser *gateways VoIP*, teléfonos IP, servidores, o cualquier dispositivo que pueda iniciar y terminar una llamada VoIP.

Los dispositivos de control de llamadas son llamados *gatekeepers* en una red H.323, y servidores *proxy* o servidores de redirección en una red SIP.

Los defensores de la arquitectura VoIP distribuida apoyan este modelo por su flexibilidad ya que permite que las aplicaciones VoIP sean tratadas como cualquier otra aplicación IP distribuida.

#### 1.4.5 SIMILITUDES Y DIFERENCIAS ENTRE H.323 Y SIP

Si bien H.323 y SIP son protocolos distintos existen algunas particularidades similares entre ellos, entre las cuales se tiene:

- Permiten llamadas de dos partes y múltiples partes utilizando las computadoras y teléfonos como puntos finales.
- Soportan negociación de parámetros, codificación y los protocolos RTP y RTCP.
- Utilizan la arquitectura distribuida para su diseño e implementación

Así mismo entre H.323 y SIP existen varias diferencias marcadas, entre las cuales se tienen:

- H.323 es un estándar grande, complejo y rígido, que especifica toda la pila de protocolos en cada capa lo que facilita la tarea de interoperabilidad, pero es difícil de adaptar a aplicaciones futuras.
- SIP es un protocolo de Internet típico que funciona intercambiando líneas cortas de texto ASCII, que interactúa bien con otros protocolos de Internet.
- SIP a diferencia de H.323 es altamente modular y flexible, y se puede adaptar con facilidad a nuevas aplicaciones.

En la tabla 1.4 se muestran las principales diferencias entre las características de los dos protocolos.

ELEMENTO	H.323	SIP
Diseñado por	ITU	IETF
Arquitectura	Distribuida	Distribuida
Versión ultima	H.323V4	RFC 2543
Control de llamadas	Gatekeeper	Servidor Proxy, redirección
Endpoints	Gateway, terminal	User Agent
Compatibilidad con PSTN	Si	Ampliamente
Compatibilidad con Internet	No	Si
Negociación de parámetros	Si	Si
Señalización de llamadas	Q.931 sobre TCP	SIP sobre TCP o UDP
Formato de mensajes	Binario	ASCII
Transporte de medios	RTP/RTCP	RTP/RTCP
Llamadas de múltiples partes	Si	Si
Conferencias multimedia	Si	No
Direccionamiento	Host o número telefónico	URL's
Terminación de llamadas	Explicita o liberación de TCP	Explicita o terminación de temporizador
Mensajes instantáneos	No	Si
Encriptación	Si	Si
Estado	Distribuido ampliamente	Prometedor

Tabla 1. 4 Diferencias entre H.323 y SIP [29]

## 1.4.6 FACTORES QUE AFECTAN LA CALIDAD DE VOZ

Uno de los retos que presenta el diseño de una red de VoIP, sin duda alguna constituyen los factores que pueden deteriorar la calidad de la voz, haciendo que el mensaje no llegue de la manera correcta y por ende no se tenga una buena comunicación.

### 1.4.6.1 Codec's

Al ser la voz de carácter analógica, y querer transmitirla sobre una red IP, uno de los primeros pasos a efectuarse es la digitalización de la voz, lo cual se lo realiza mediante el uso de un códec. Este dispositivo toma su nombre de la conjunción de las palabras codificador-decodificador, y su proceso consiste en transformar las señales analógicas en digitales.

La tabla 1.5 muestra una lista de los códec's estandarizados por la ITU-T sus respectivas características.

Nombre	Descripción	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	Observaciones	MOS
<b>G.711*</b>	Pulse code modulation (PCM)	64	8	Muestreada	Tiene dos versiones u-law y A-law para muestrear la señal	4.1
<b>G.711.1*</b>	Pulse code modulation (PCM)	80-96 Kbps	8	Muestreada	Mejora del códec G.711 para abarcar la banda de 50 Hz a 7 KHz.	
<b>G.721</b>	Adaptive differential pulse code modulation (ADPCM)	32	8	Muestreada	Obsoleta. Se ha transformado en G.726.	
<b>G.722</b>	7 KHz audio-coding within 64 Kbit/s	64	16	Muestreada	Divide los 16 KHz en dos bandas cada una usando ADPCM	

Tabla 1. 5 Codecs de Audio (parte 1 de 2)

<b>G.722.1</b>	Codificación a 24 y 32 kbit/s	24/32	16	20		
<b>G.728</b>	Coding of speech at 16 Kbit/s using low-delay code excited linear prediction	16	8	2.5	CELP.	3.61
<b>G.729**</b>	Coding of speech at 8 Kbit/s using (CS-ACELP)	8	8	10	Bajo retardo (815 ms)	3.92
<b>G.729.1</b>	Coding of speech at 8 Kbit/s using (CS-ACELP)	8/12/14/16/18/20/22/24/26/28/30/32	8	10	Ancho de banda desde 50Hz a 7Khz	
<b>G.723</b>	Extensión de la norma G.721 a 24 y 40 kbit/s para aplicaciones en circuitos digitales	24/40	8	Muestreada	Obsoleta por G.726. Es totalmente diferente de G.723.1	
<b>G.723.1</b>	Dual rate speech code for multimedia communications transmitting at 5.3 and 6.3 Kbit/s	5.6/6.3	8	30	Parte de H.324 video conferencing.	3.8-3.9
<b>G.726</b>	40,32,24,16 Kbit/s (ADPCM)	16/24/32/40	8	Muestreada	ADPCM; reemplaza a G.721 y G.723	3.85
<b>G.727</b>	5-, 4-, 3-, and 2-bit/sample (ADPCM)	Var.		Muestreada	ADPCM Relacionada con G.726	

Tabla 1.5 Codecs de Audio (parte 2 de 2) [30]

\* G711 tiene dos versiones una utilizada en Europa y conocida como Ley A y otra utilizada en USA y Japón conocida como Ley  $\mu$ .

\*\* G729 es el códec original, aunque posee otras versiones como G.729

### 1.4.6.2 Pérdida de Paquetes

La VoIP al ser transmitida por una red de conmutación de paquetes, puede sufrir los mismos errores que los datos, uno de ellos y además muy común, es la pérdida de paquetes, lo cual puede influir en la calidad de la conversación y en el entendimiento en sí del mensaje a transmitir. Esta pérdida de paquetes se puede dar por varias razones, como por ejemplo:

- Congestión de la red
- Tráfico de prioridad más alta que bloquea al tráfico de prioridad baja
- Problemas en los parámetros / configuración (*software*)
- Problemas de conexión (físicos)

Como es de conocimiento dentro de una red de conmutación de paquetes, si se tratan de servicios en tiempo no real, una de las maneras de corregir la pérdida de paquetes sería con su retransmisión; sin embargo al tratarse de servicios en tiempo real esto no sería práctico y podría ocasionar retardos adicionales.

Es por ello que existen varias estrategias para minimizar la pérdida de paquetes dentro de la transmisión de VoIP. [31]

#### 1.4.6.2.1 *Protocolos de QoS*

La inclusión de protocolos que ofrezcan calidad de servicio, permitirá que la transmisión de paquetes de voz sea manejada con prioridad, reduciendo la cantidad de paquetes encolados y generando prioridades al tipo de tráfico, lo que hará que la tasa de pérdida de paquetes sea baja.

#### 1.4.6.2.2 *Intercalado*

Este proceso consiste en intercalar las tramas de un paquete en el transmisor y reordenarlas en el receptor, y así ayudar a minimizar el efecto de los paquetes faltantes a la salida.



#### 1.4.6.2.3 *Supresión de silencio y ruido*

Una de las grandes ventajas del empaquetamiento de la voz, es que no se generan paquetes al momento de realizar pausas entre la conversación, o al estar en silencio una persona mientras la otra está hablando.

En una conversación telefónica el tiempo en que los dos usuarios hablan simultáneamente es muy reducido; actualmente la tecnología provee un mecanismo llamado supresión de datos en silencio, el cual no envía datos si no hay sonido.

Mientras que para la supresión de ruido se usa el VAD (Detección activada por Voz) el cual diferencia entre la existencia de sonido y la voz, con lo que al no existir señal de voz se genera el llamado ruido de *confort* al otro extremo de la línea.

#### 1.4.6.2.4 *Interpolación*

Consiste en interpolar los paquetes de voz perdidos al repetir el último paquete recibido, durante el intervalo cuando el paquete perdido supuestamente debía ser analizado.

Es un método simple que llena el tiempo entre tramas de voz no continuos; trabaja bien cuando la incidencia de tramas perdidas es poco frecuente. Si el número de paquetes perdidos es alto no trabaja muy bien.

#### 1.4.6.2.5 *Corrección*

Hace referencia al envío redundante del mensaje en paquetes subsiguientes, de tal manera que si se pierde un fragmento de un paquete, puede extraer información de los paquetes vecinos; este mecanismo actualmente se lo ha propuesto para ser utilizado por el protocolo RTP.

### 1.4.6.3 Retardo de Paquetes

Otra consideración importante en el diseño de una red VoIP es el efecto de retardo. El efecto de retardo en la transmisión de voz es discutido en la ITU G.114.

Dentro de la transmisión de VoIP se ha determinado que un promedio de retardo aceptable es de hasta 150 ms; sin embargo dentro de dicha transmisión existen varios retardos que sumados hacen uno solo, haciendo así una labor muy complicada la disminución de estos tiempos para que la comunicación sea exitosa. La figura 1.16 muestra los distintos retrasos que existen dentro de una comunicación de VoIP extremo a extremo.

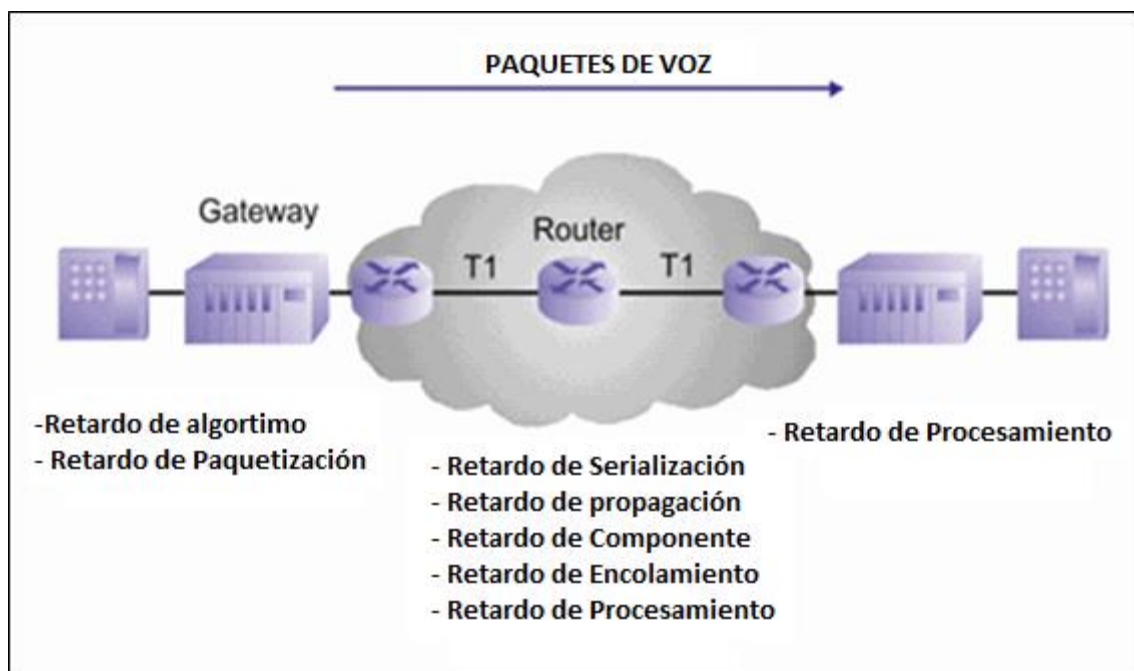


Figura 1. 16 Retardo de Paquetes [32]

#### 1.4.6.3.1 Retardo de Algoritmo

Es el retardo inherente a la digitalización de la señal analógica de la voz, es decir este retardo es introducido por el códec y su algoritmo de codificación.

La tabla 1.6 muestra los retardos de algoritmos introducidos por los códecs más comunes.

Coding Standards	Algorithmic Delay (ms)
<b>G.711</b>	0.125
<b>G.726</b>	1
<b>G.728</b>	3-5
<b>G.729</b>	15
<b>G.723.1</b>	37.5

Tabla 1. 5 Retardos de algoritmos [32]

#### 1.4.6.3.2 Retardo de Paquetización

Es el tiempo que se tarda en llenar un paquete de información (carga útil), de la conversación ya codificada y comprimida.

Este retardo es función del tamaño de bloque requerido por el codificador de voz y el número de bloques de una sola trama.

La RFC 1890 especifica que el retardo de paquetización por defecto debe ser de 20 ms. En la tabla 1.7 se indica el retardo de paquetización de acuerdo a la carga útil de cada códec.

Codificador	Tasa de Bits	Carga útil(Bytes)	Retardo de paquetizacion(ms)	Carga útil(Bytes)	Retardo de paquetizacion(ms)
<b>PCM G.711</b>	64 Kbps	160	20	240	30
<b>ADPCM, G.726</b>	32 Kbps	80	20	120	30
<b>CS-ACELP, G.729</b>	80 Kbps	20	20	30	30
<b>MP-MLQ, G.723.1</b>	6.3 Kbps	24	24	60	48
<b>MP-ACELP, G.723.1</b>	5.3 Kbps	20	30	60	60

Tabla 1. 6 Retardo de Paquetización [32]

#### 1.4.6.3.3 Retardo de Serialización

Este retardo está relacionado directamente con la tasa del reloj de transmisión, es decir, es el tiempo que tarda en ponerse el paquete en la línea de transmisión; mientras el paquete sea de mayor longitud mayor será el retraso. La tabla 1.8 indica el tiempo de retraso de serialización para diferentes tamaños de tramas.

Tamaño de trama (bytes)	Velocidad de línea (Kbps)										
	19.2	56	64	128	256	384	512	768	1024	1544	2048
38	15.83	5.43	4.75	2.38	1.19	0.79	0.59	0.40	0.30	0.20	0.15
48	20.00	6.86	6.00	3.00	1.50	1.00	0.75	0.50	0.38	0.25	0.19
64	26.67	9.14	8.00	4.00	2.00	1.33	1.00	0.67	0.50	0.33	0.25
128	53.33	18.29	16.00	8.00	4.00	2.67	2.00	1.33	1.00	0.66	0.50
256	106.67	36.57	32.00	16.00	8.00	5.33	4.00	2.67	2.00	1.33	1.00
512	213.33	73.14	64.00	32.00	16.00	10.67	8.00	5.33	4.00	2.65	2.00
1024	426.67	149.29	128.00	64.00	32.00	21.33	16.00	10.67	8.00	5.31	4.00
1500	625.00	214.29	187.50	93.75	46.88	31.25	23.44	15.63	11.72	7.77	5.86
2048	853.33	292.57	256.00	128.00	64.00	42.67	32.00	21.33	16.00	10.61	8.00

Tabla 1. 7 Retardo de Serialización [32]

#### 1.4.6.3.4 Retardo de Propagación

Es el tiempo que toma la señal en llegar de un punto a otro, ya sea como señales ópticas o eléctrico-magnéticas.

#### 1.4.6.3.5 Retardo de Componente

Este retardo se da al momento que una trama está intentando pasar través de un componente de red, por ejemplo un *switch*, por lo que se tiene retardo cuando el componente pasa del puerto de entrada al puerto de salida a través del *backplane*<sup>19</sup>.

<sup>19</sup> **Backplane:** Matriz de conmutación que conecta todos los puertos de un componente de red.

Existen otras fuentes de retardo consideradas mínimas como son, el retardo de procesamiento y encolamiento en cada uno de los dispositivos que atraviesa el paquete.

#### 1.4.6.4 Jitter

El *jitter* es un problema muy común dentro de las redes de conmutación por paquetes; la naturaleza de este tipo de redes, hace que cada paquete puede ir por un camino distinto, generando así una variación en el retardo en llegar a su destino de cada paquete perteneciente a un mensaje.

El *jitter* está definido técnicamente como la variación del tiempo de llegada de los paquetes, por congestión en la red, pérdidas de sincronización o por seguir diferentes rutas, hacia su destino.

Éste es una de los grandes problemas que enfrentan los servicios en tiempo real, debido a la congestión que puede existir dentro de la red o a que los enlaces son demasiados lentos.

Para solucionar este tipo de inconvenientes han aparecido estrategias de calidad de servicio QoS como, priorización de tráfico, reservas de ancho de banda o enlaces de mayor velocidad.

En la figura 1.17 se puede apreciar el efecto del *jitter*.

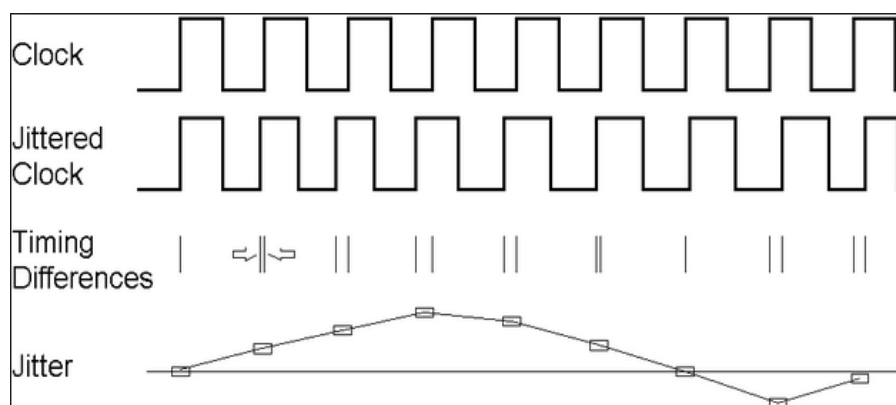


Figura 1. 17 *Jitter* [33]

## **1.5 TELEFONÍA IP [34]**

La Telefonía IP es un servicio que permite integrar en una red IP las comunicaciones de voz y datos, esto es conocido como redes convergentes o convergencia IP.

La Telefonía IP basa su funcionamiento en la tecnología de transmisión de VoIP ya antes detallada, en la cual se convierte la voz analógica en digital, se empaqueta el mensaje, éste viaja por la red IP y finalmente llega a su destino para ser nuevamente transformados en señal analógica.

Si bien este servicio lleva varios años en el mercado (desde finales de los 90), ha ido tomando fuerza en los últimos años, esto debido a los avances ofrecidos por protocolos de QoS, su estandarización y sobre todo por la gran acogida que ha tenido el Internet.

Cuando se habla de un sistema de telefonía IP se hace referencia a un conjunto de elementos que juntos proporcionan el servicio de voz a una empresa; por mencionar algunos elementos básicos se tiene: central telefónica IP, *Gateway*, y teléfonos IP.

### **1.5.1 CLASES DE TELEFONÍA IP**

Las clases de telefonía IP hace referencia al medio por el cual se va a prestar el servicio de telefonía. A continuación se da una breve explicación de las diferentes clases de telefonía IP que se tiene.

#### **1.5.1.1 Telefonía IP Privada**

La Telefonía IP privada es aquella utilizada por la INTRANET de una empresa en particular, la cual permite comunicaciones de voz entre sus distintos departamentos, ya sean éstos en el mismo campus o ciudad, o en ciudades distintas. La figura 1.18 muestra un ejemplo de telefonía IP privada.

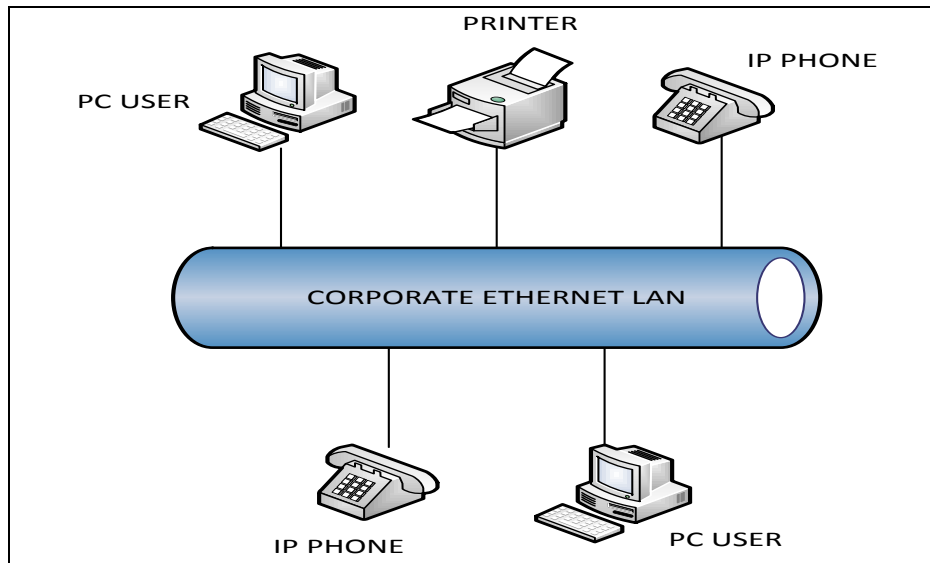


Figura 1. 18 Telefonía IP privada [35]

### 1.5.1.2 Telefonía IP por Internet

La Telefonía IP por Internet es aquella que hace el uso del Internet para realizar las llamadas a teléfonos IP, ya sean de su propia empresa o de una distinta.

En la figura 1.19 se puede apreciar el funcionamiento de la Telefonía IP por Internet.

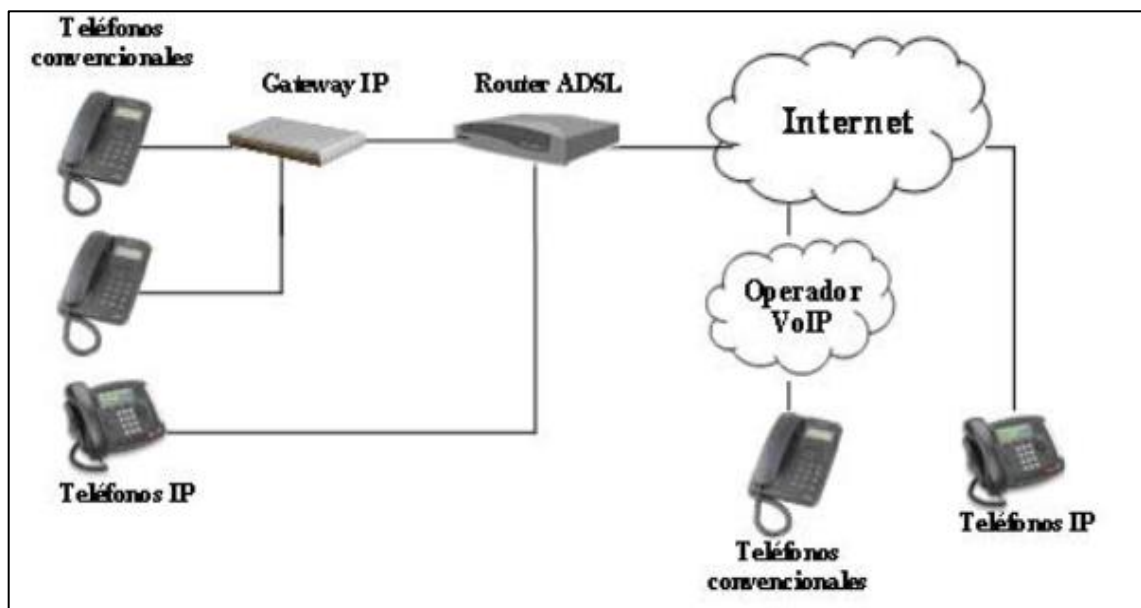


Figura 1. 19 Telefonía IP por Internet [35]

### 1.5.1.3 Telefonía IP Pública

Este tipo de telefonía IP es aquella que permite las llamadas desde y hacia cualquier teléfono regular, pasando por la PSTN, tal como lo muestra la figura 1.20.

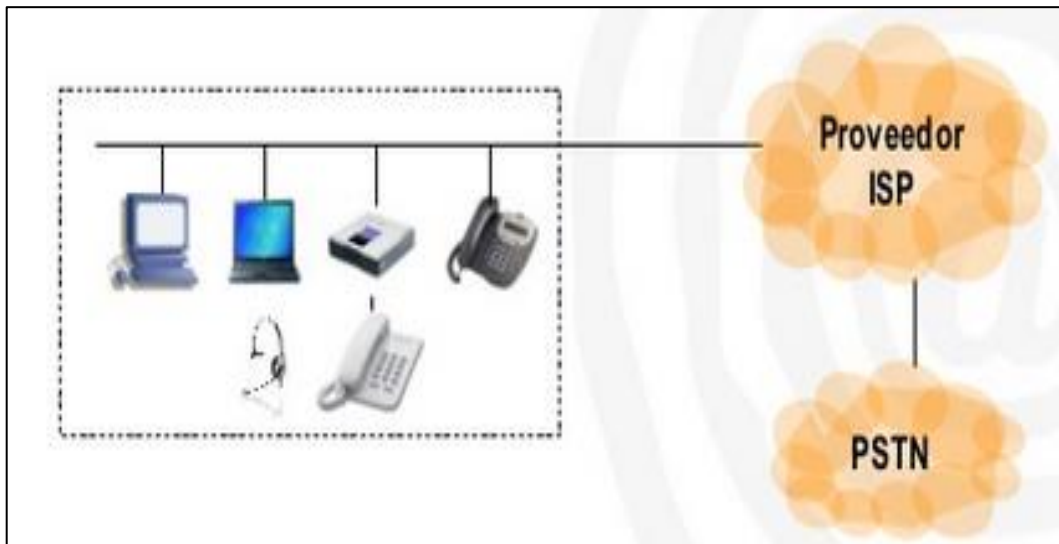


Figura 1. 20 Telefonía IP pública [35]

### 1.5.2 VENTAJAS DE LA TELEFONÍA IP [36]

Los beneficios que ofrece la telefonía IP están enfocados mayoritariamente a los ambientes empresariales, teniendo como fin común el ahorro en las comunicaciones de la misma; sin embargo no solo esos son los beneficios que este servicio puede ofrecer.

A continuación se enumeran algunas de las principales ventajas de la telefonía IP y por ende de la tecnología VoIP.

- **La primera ventaja y por muchos considerada la más importante es el costo**, una llamada mediante telefonía IP es en la mayoría de los casos mucho más económica que su equivalente en telefonía convencional. Esto es básicamente debido a que se utiliza la misma red para la transmisión de datos y voz.



- **Usualmente para una llamada entre dos teléfonos IP la llamada es gratuita**, cuando se realiza una llamada de un teléfono IP a un teléfono convencional el costo corre a cargo del teléfono IP.
- **Permite un ahorro en la infraestructura**, esto debido a que se utiliza la misma red de datos para transmisión de voz, ahorrando así incluso, en aspectos como cableado estructurado, mantenimiento y otros.
- **Con telefonía IP los usuarios pueden realizar una llamada desde cualquier lugar donde exista conectividad a Internet**. Dado que los teléfonos IP transmiten su información a través de Internet, éstos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión.
- La mayoría de los proveedores de telefonía IP entregan características por las cuales las operadoras de telefonía convencional cobran tarifas adicionales, por ejemplo:
  - Identificación de llamadas
  - Servicio de llamadas en espera
  - Servicio de transferencia de llamadas
  - Repetición de llamada
  - Devolución de llamada
  - Llamada de 3 líneas (*three-way calling*)

La Telefonía IP permite el uso de características adicionales que la telefonía tradicional no posee, como por ejemplo:

- Desviar la llamada a un teléfono particular
- Enviar la llamada directamente al correo de voz
- Dar a la llamada una señal de ocupado.
- Mostrar un mensaje de fuera de servicio

### 1.5.3 DESVENTAJAS DE LA TELEFONÍA IP

Si bien la Telefonía IP es un servicio que está tomando fuerza en el mercado, no todo lo que ofrece es mejor a los sistemas de comunicación de voz tradicional; es decir, también existen desventajas al momento de implementar el servicio. A continuación se menciona algunas desventajas que este servicio posee.

- **Es necesario un gran ancho de banda disponible para el uso de Telefonía IP**, ya que si no existe el ancho de banda suficiente la comunicación puede ser de mala calidad, con cortes o retrasos muy significativos.
- **La Telefonía IP requiere de una conexión eléctrica**, en caso de un corte eléctrico los teléfonos IP dejan de funcionar, a diferencia de los sistemas de comunicación tradicional que no sentían este efecto a menos que los teléfonos sean inalámbricos.
- **Al transmitir la voz a través de una red IP, el servicio es susceptible a virus, gusanos y *hacking*<sup>20</sup>**, si bien esto no es muy común puede darse el caso; es por ello que los desarrolladores están buscando la manera de encriptar la voz para evitar posibles problemas.
- **Puede existir problemas por el uso del PC**, esto cuando se utiliza un *softphone*; es decir la calidad de la voz puede verse afectada, debido a que la computadora está usando el 100% de la capacidad del CPU.

### 1.5.4 ESQUEMAS PARA TELEFONÍA IP

Dentro de la problemática surgida por el avance de la telefonía IP, uno de los factores a tomar en cuenta es el esquema que se va manejar dentro de las empresas para la implementación de este servicio. Para ello se va a presentar cuáles serán los esquemas alternativos para la implementación de telefonía IP dentro de cualquier tipo de Institución.

---

<sup>20</sup> **Hacking:** Capacidad de obtener de forma inadecuada información que se transmite sobre la Red.

### 1.5.4.1 Esquema de Telefonía IP Híbrido

El esquema IP híbrido es una solución que en esencia es una extensión de la infraestructura telefónica tradicional a base de conmutación de circuitos. Se clasifica como una modalidad de IP por la incorporación de troncales y/o tarjetas de línea IP.

Debido a que el esquema IP híbrido consta tanto de elementos de telefonía convencional como de tecnología IP, presenta limitantes en varias de sus funciones. En la figura 1.21 se puede apreciar que la red cuenta con una PBX híbrida la cual incorpora telefonía IP a la infraestructura telefónica tradicional.

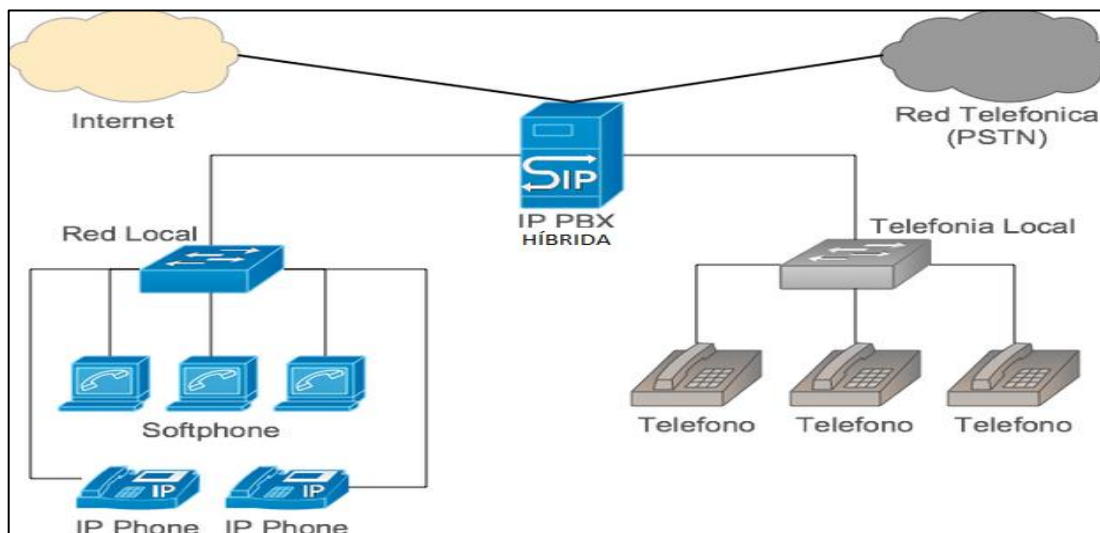


Figura 1. 21 Telefonía IP Híbrida [27]

### 1.5.4.2 Esquema de Telefonía IP Puro

El esquema IP puro se refiere a una solución desarrollada para estar basada totalmente en IP.

La tecnología permite enrutamiento inteligente y administración centralizada de varios departamentos, al tiempo que facilita la comunicación multicanal sobre una única red corporativa. Un ejemplo de este esquema se puede apreciar en la figura 1.22



A continuación se muestra un breve detalle de estas soluciones, con sus respectivas ventajas y desventajas.

#### **1.5.5.1 Soluciones Basadas en *Hardware* [4]**

Este tipo de solución está basado en equipos físicos que se conectarán a la red de datos para permitir la comunicación de voz por la misma red. Entre los grandes fabricantes que utilizan este tipo de solución se tiene a Cisco y Avaya, los cuales mediante el uso *de hardware* especializado permiten la transmisión de voz sobre una red IP.

##### *1.5.5.1.1 Ventajas de soluciones basadas en hardware*

Las soluciones basadas en *hardware* presentan las siguientes ventajas:

- Generalmente proveen aplicaciones y servicios incluidos dentro de la solución, facilitando así la administración para la organización.
- El procesamiento de la información es más rápido que el ofrecido por *software*.
- Provee de gran confiabilidad al sistema telefónico a implementar.

##### *1.5.5.1.2 Desventajas de soluciones basadas en hardware*

Al seleccionar una solución basada en *hardware*, se debe tener en cuenta las siguientes desventajas:

- Costos elevados de *hardware* y dispositivos
- Costos altos de licenciamientos
- El soporte es únicamente de la casa fabricante de la solución
- Se necesita un gran ancho de banda para que la solución sea efectiva
- La integración con otras soluciones puede resultar compleja

### 1.5.5.2 Soluciones Basadas en *Software* [4]

La solución para telefonía IP basada en *software* es aquella que hace uso de un PC en el cual es instalada una aplicación para que la misma funcione como una PBX<sup>21</sup> IP. Algunas de estas soluciones son *Asterisk*, *Elastix*, *3XC*, etc.

#### 1.5.5.2.1 *Ventajas de soluciones basadas en software*

A continuación se muestran las principales ventajas que tienen las soluciones basadas en *software*.

- El *software* es gratuito y su código fuente está disponible al usuario.
- Versiones, actualizaciones y soporte se lo puede encontrar en Internet.
- Provee de gran flexibilidad al administrador para la selección de terminales a utilizar, permitiendo así que la organización no sea dependiente de una sola casa fabricante.
- No es estrictamente necesario tener una PBX dentro de la organización, reduciendo así costos y espacio.

#### 1.5.5.2.2 *Desventajas de soluciones basadas en software*

Las desventajas que este tipo de soluciones presenta son las siguientes:

- El administrador debe poseer experiencia sobre la solución seleccionada
- Al ser *software* existe una complejidad adicional, lo que puede generar que el sistema telefónico sea menos confiable, tomando en cuenta el ambiente donde se va a desenvolver.
- El *software* necesario para una implementación puede resultar costoso.
- Este tipo de soluciones por lo general incluyen costos adicionales tales como licencias, permisos, entre otros.

---

<sup>21</sup> **PBX:** *Private Branch Exchange*.- Central telefónica conectada directamente a la PSTN y permitiendo comunicar a la organización con el exterior.

## 1.6 SISTEMA DE CABLEADO ESTRUCTURADO [37]

Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus.

Las características e instalación de estos elementos se deben hacer en cumplimiento de estándares para que califiquen como cableado estructurado.

### 1.6.1 SUBSISTEMAS DEL CABLEADO ESTRUCTURADO

El Sistema de Cableado Estructurado (SCE) está compuesto por varios subsistemas, que en unión permiten el correcto tránsito de la información dentro de una organización.

Esto se puede apreciar de mejor manera en la figura 1.23.



Figura 1. 23 Subsistemas del sistema de cableado estructurado [37]

### 1.6.1.1 Área de Trabajo

El Área de Trabajo se extiende desde el terminal de salida de telecomunicaciones (fin del cableado horizontal) hasta la estación de trabajo.

El cableado del área de trabajo está diseñado para ser relativamente simple de interconectar, de tal manera que la estación de trabajo pueda ser removida, cambiada de lugar sin ninguna complicación, además de poder agregar nuevas estaciones muy fácilmente.

Los componentes del área de trabajo generalmente son: *patch cords* y *face plate*, los cuales permiten conectar a la red los equipos finales como teléfonos, Fax, PCs, etc.

### 1.6.1.2 Cableado Horizontal

El sistema de cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones o viceversa.

Este subsistema debe estar en condiciones de soportar diferentes servicios como son voz, datos, video y demás.

Su topología debe ser en estrella y la distancia máxima entre el área de trabajo y el cuarto de telecomunicaciones no debe exceder los 90 m, independientemente del cable que se utilice.

El cableado horizontal consiste de dos elementos básicos:

- **Cable Horizontal y Hardware de Conexión** (también llamado "cableado horizontal") que proporciona los medios básicos para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones.



- **Rutas y Espacios Horizontales** (también llamado "sistemas de distribución horizontal"). Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar *hardware* entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado Horizontal.

En la Figura 1.24 se muestra una conexión de cableado horizontal con sus respectivos componentes y distancias permitidas.

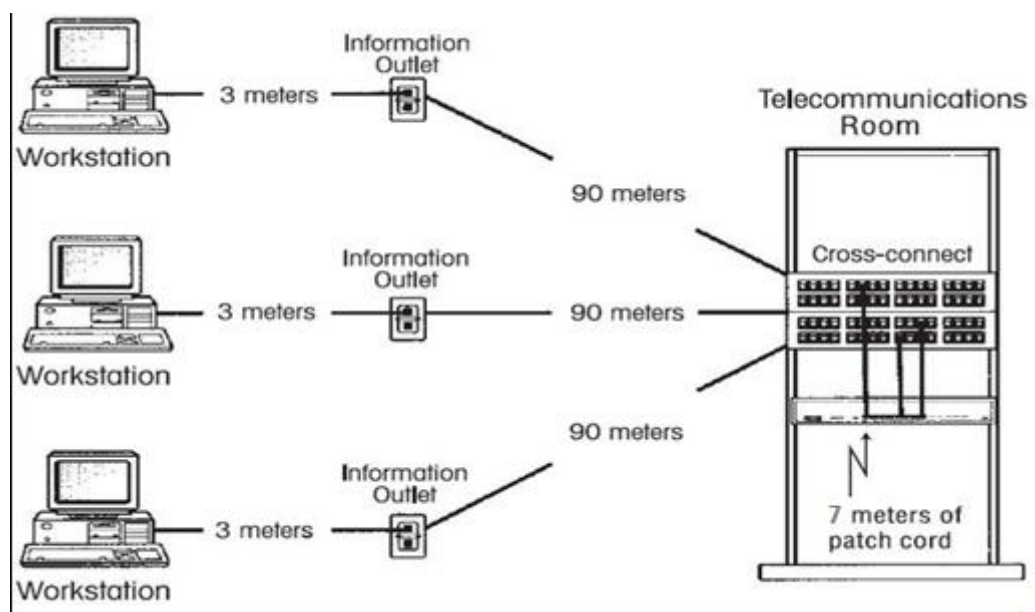


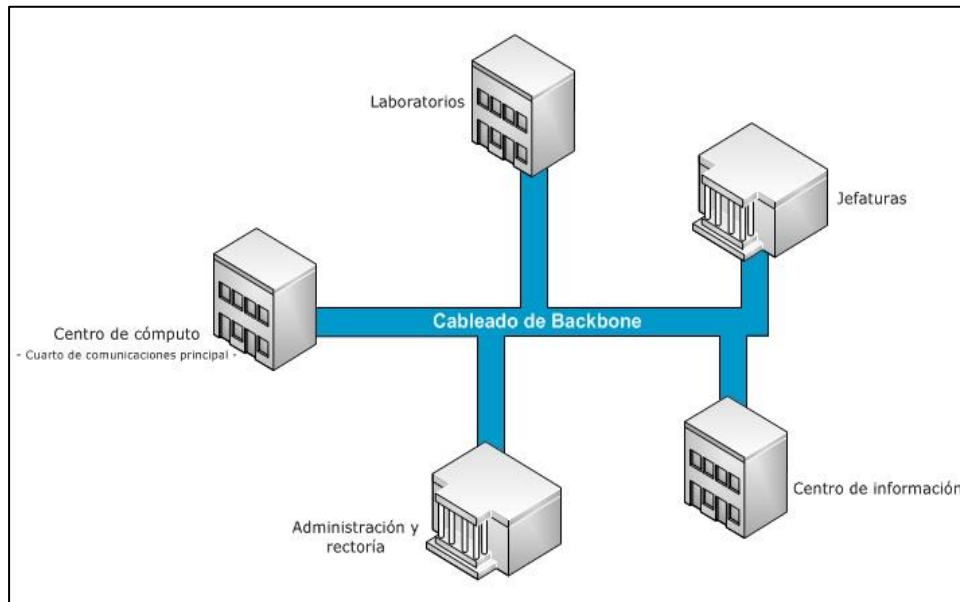
Figura 1. 24 Cableado Horizontal [37]

### 1.6.1.3 Cableado Vertical

El propósito del cableado de *backbone* o cableado vertical es proporcionar interconexiones entre cuartos de entrada de servicios del edificio, cuartos de equipo y cuartos de telecomunicaciones. Incluye la conexión vertical entre pisos en edificios de varios pisos, así como, los medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas.

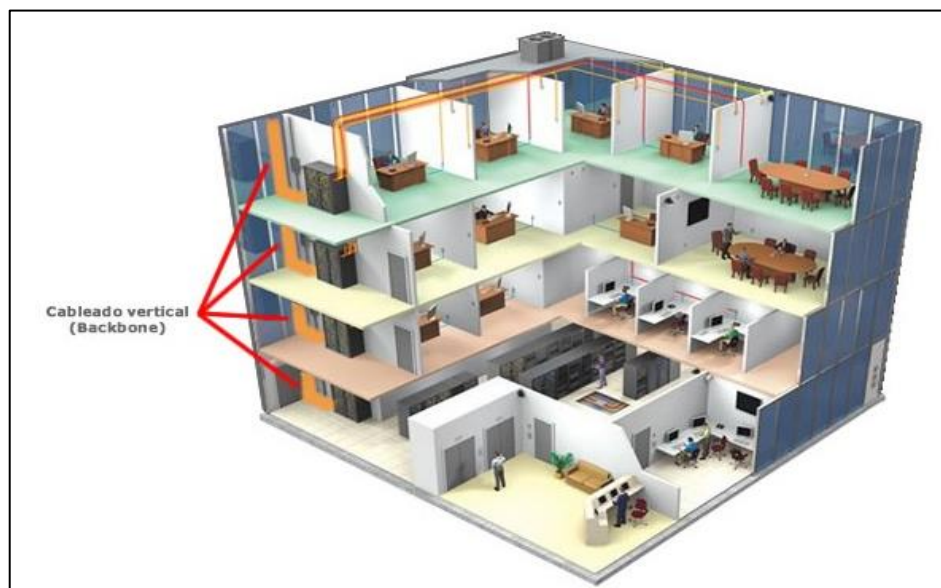
El cableado vertical realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y la sala de equipos.

En la figura 1.25 se muestra un ejemplo de cableado vertical para un campus universitario, donde se desean conectar diferentes cuartos de telecomunicaciones ubicados en las diferentes zonas y la sala de equipos (Centro de Cómputo).



**Figura 1. 25 Cableado Vertical (Campus Educativo)**

Otro ejemplo de cableado vertical es el que se realiza entre los pisos de un edificio compartiendo así diversos recursos y servicios, donde también cada piso tiene su cableado horizontal como lo muestra la figura 1.26.



**Figura 1. 26 Cableado Vertical (Edificio Comercial) [37]**

#### **1.6.1.4 Cuarto de Telecomunicaciones**

Un cuarto de telecomunicaciones es el área de un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones.

El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones y debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado; es decir es el punto de encuentro del cableado vertical y horizontal.

#### **1.6.1.5 Sala de Equipos**

La sala de equipos es un espacio centralizado de uso específico para equipo de telecomunicaciones tales como: centrales telefónicas, equipos de cómputo y/o conmutadores de video. Varias o todas las funciones de un cuarto de telecomunicaciones pueden ser proporcionadas por un cuarto de equipos. Los cuartos de equipos se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen.

Los cuartos de equipos incluyen espacio de trabajo para personal de telecomunicaciones como se puede apreciar en la figura 1.27.



**Figura 1. 27 Sala de Equipos [37]**

### 1.6.1.6 Entrada de Servicios

La entrada de servicios del edificio es el punto en el cual el cableado externo hace interfaz con el cableado de *backbone* dentro del edificio, es decir es el punto donde entran los servicios al edificio y se les realiza una adaptación para unirlos al edificio y hacerlos llegar a los diferentes lugares del edificio en su parte interior.

## 1.6.2 ESTÁNDARES DE SISTEMA DE CABLEADO ESTRUCTURADO

Realizar el SCE dentro de una institución no es una tarea sencilla, es por ello que se debe tener mucho cuidado al momento de diseñarlo, ya que gran parte de la red dependerá del correcto dimensionamiento del cableado. Además se lo debe realizar de manera jerárquica y organizada, para lo cual organizaciones como la TIA<sup>22</sup>, ANSI<sup>23</sup> y la EIA<sup>24</sup>, han generado estándares para poder llevar a cabo este propósito. A continuación se realizará una breve descripción de los principales estándares de Cableado Estructurado.

### 1.6.2.1 Estándares ANSI/TIA 568-C [38]

El estándar ANSI/TIA 568-C.- *Estándar para el Cableado de Telecomunicaciones Genérico para Instalaciones de Clientes*, es el sucesor del estándar 568.B; esto debido a la gran cantidad de adendas que la norma anterior posee y otros avances que se deben tener en cuenta.

La serie 568-C incorpora material de 568 B.1, 568-B .2, 568-B.3, las adiciones 18 a la serie 568 B, así como actualizaciones y revisiones necesarias.

En la figura 1.28 se presenta un resumen de los contenidos que aparecen en los cuatro documentos principales 568-C. En ésta se muestra cómo el documento 568 C se interrelaciona entre sí y con otros importantes estándares de cableado TIA.

---

<sup>22</sup> TIA: Asociación de Industrias de Telecomunicaciones

<sup>23</sup> ANSI: Instituto de Estándares Nacionales Americano

<sup>24</sup> EIA: Asociación de Industrias Electrónicas

- **ANSI/TIA-568-C.1:** Estándares para el cableado de telecomunicaciones en Edificios Comerciales.
- **ANSI/TIA-568-C.2:** Componentes de sistemas de cable de pares balanceados
- **ANSI/TIA-568-C.3:** Componentes de sistemas de cable de fibra óptica.

Sin embargo una de las características más conocidas de este estándar es la asignación de pares/pines en los cables de 8 hilos y 100 ohmios (UTP). Esta asignación se conoce como T568A y T568B, y a menudo es nombrada erróneamente como TIA/EIA-568A y TIA/EIA-568B.

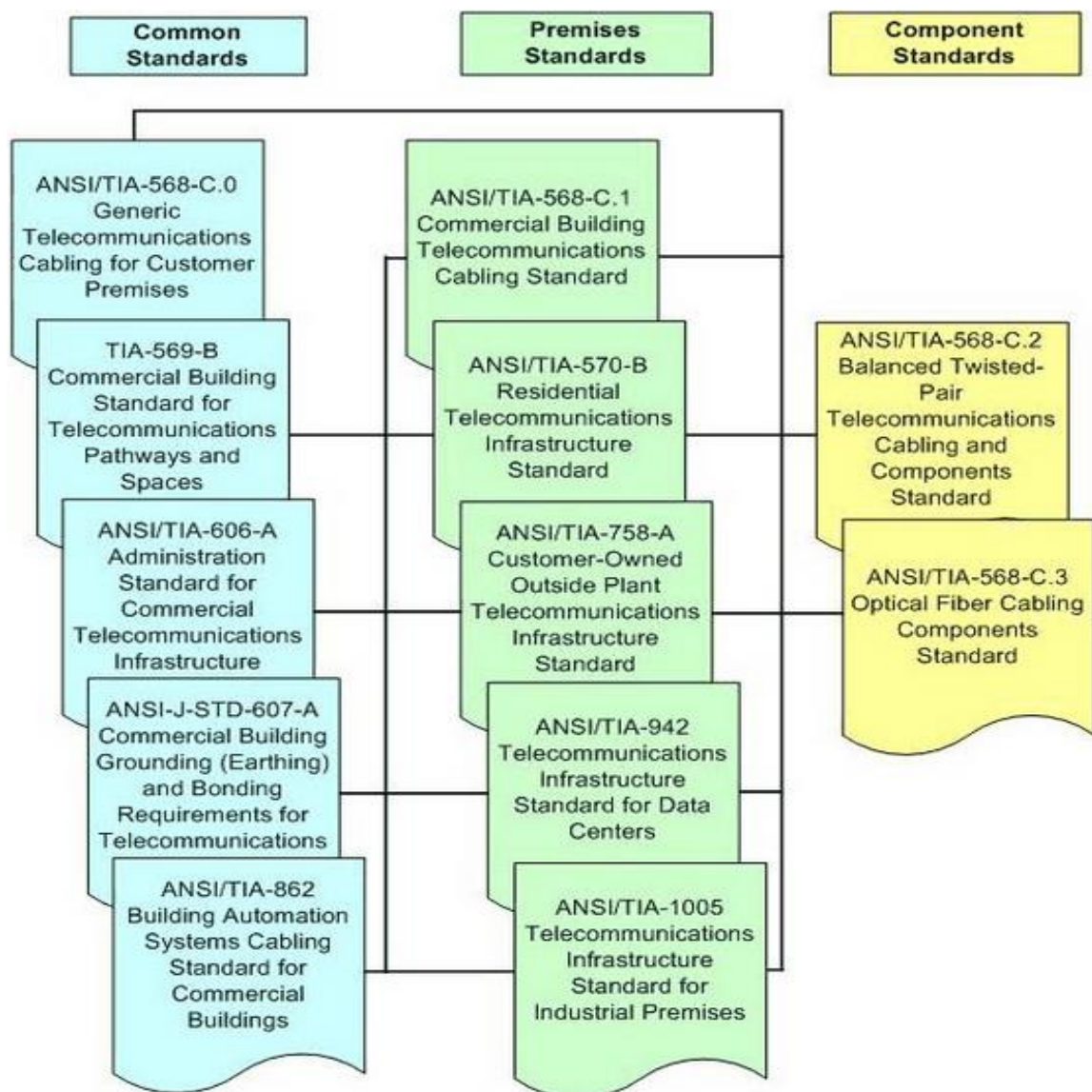


Figura 1. 28 Estándar ANSI/TIA 568-C [38]

La figura 1.29 muestra las dos formas de asignación pares/pines que establece el estándar ANSI/TIA/EIA-568B, denominadas T568A y T568B, respectivamente.

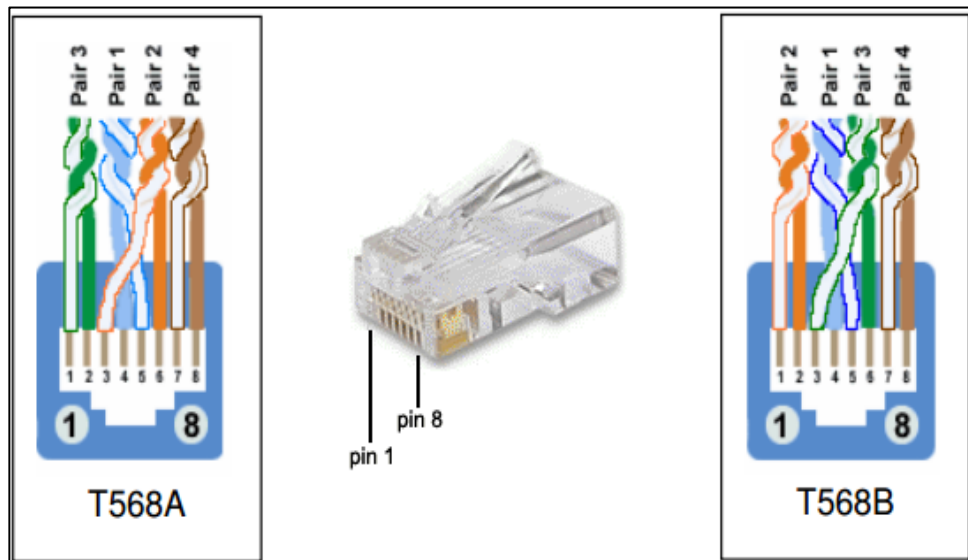


Figura 1. 29 Asignación pares/pines T568A y T568B [38]

### 1.6.2.2 Estándares ANSI/EIA-569-B [39]

Este estándar especifica las Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales, es decir, cómo enrutar el cableado.

Adicionalmente provee los requerimientos para los espacios tales como sala de equipos, cuartos de telecomunicaciones, etc. A continuación se mencionarán algunas de las consideraciones más importantes de este estándar para el enrutamiento del cable.

Como vías para cableado Horizontal la norma permite:

- Sistemas bajo Suelo
- Sistemas de Piso Removible
- Tubos *Conduit* metálico o de PVC
- Ductos y Canaletas Perimetrales
- Sistemas de Cielo

Las vías para Cableado de *backbone* Interno pueden ser:

- Tubos *Conduit*
- Manguitos o Ranuras de piso
- Bandejas Portacable

Las vías para cableado *backbone* entre edificios pueden ser:

- Ductos Subterráneos
- Instalaciones Aéreas (por postes)
- Túneles

El estándar también dice que debe existir un cuarto de telecomunicaciones en cada piso y deben existir cuartos adicionales cuando el área a servir sea superior a 1000 m<sup>2</sup>.

#### **1.6.2.3 Estándares ANSI/TIA 606-A [40]**

El estándar ANSI/TIA-606-A hace referencia a las *Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales*.

Es vital para el buen funcionamiento del cableado estructurado, ya que habla sobre la identificación basado en etiquetas, códigos y colores, de cada uno de los subsistemas, con la finalidad de que se puedan identificar cada uno de los servicios que en algún momento se tenga que habilitar o deshabilitar.

#### **1.6.2.4 Estándares ANSI/TIA-607-A [41]**

Establece los requerimientos para *Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales*. Discute el esquema básico y los componentes necesarios para proporcionar protección eléctrica a los usuarios e infraestructura de las telecomunicaciones mediante el empleo de un sistema de puesta a tierra adecuadamente configurado e instalado.



### 1.6.3 SEGURIDAD DE LA RED

La seguridad dentro de una red es uno de los temas más importantes a considerar, con la incursión de correctas políticas se podrá mantener a la red libre de amenazas o ataques maliciosos. Para este propósito existen diferentes recomendaciones y/o normas desarrolladas para la protección de las organizaciones.

#### 1.6.3.1 NORMA ISO/ICE 27002 [66]

ISO/ICE 27002 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización

Define la información como un activo que posee valor para la organización y que requiere una protección adecuada.

El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Para la norma ISO/ICE 27002 la seguridad de la información se define como la preservación de:

- **Confidencialidad**

Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

- **Integridad**

Garantía de la exactitud y que la información esté completa, incluyendo los métodos de su procesamiento.



- **Disponibilidad**

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Así mismo establece 11 dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de Incidentes de la Seguridad
10. Gestión de continuidad del negocio.
11. Conformidad con la legislación.

Si bien esta norma sugiere establecer todos sus dominios, cabe indicar que es potestad propia de cada organización decidir si las acepta o no, es por ello que para la Unidad Educativa Temporal “Jaime Roldós Aguilera” se seguirán los dominios sobresalientes al fin de tener un sistema de gestión de seguridad lo suficientemente robusto para sus requerimientos.

Estos dominios pueden ser apreciados de mejor manera en la figura 3.14, donde se tiene una pirámide con los tipos de seguridad con los que debe contar una Organización, tales como seguridad organizativa, lógica, física y legal.

- **Gestión de Continuidad del Negocio**

Es la manera en cómo la institución va reaccionar a la interrupción de actividades del negocio y como va a proteger sus procesos críticos frente grandes fallos o desastres.

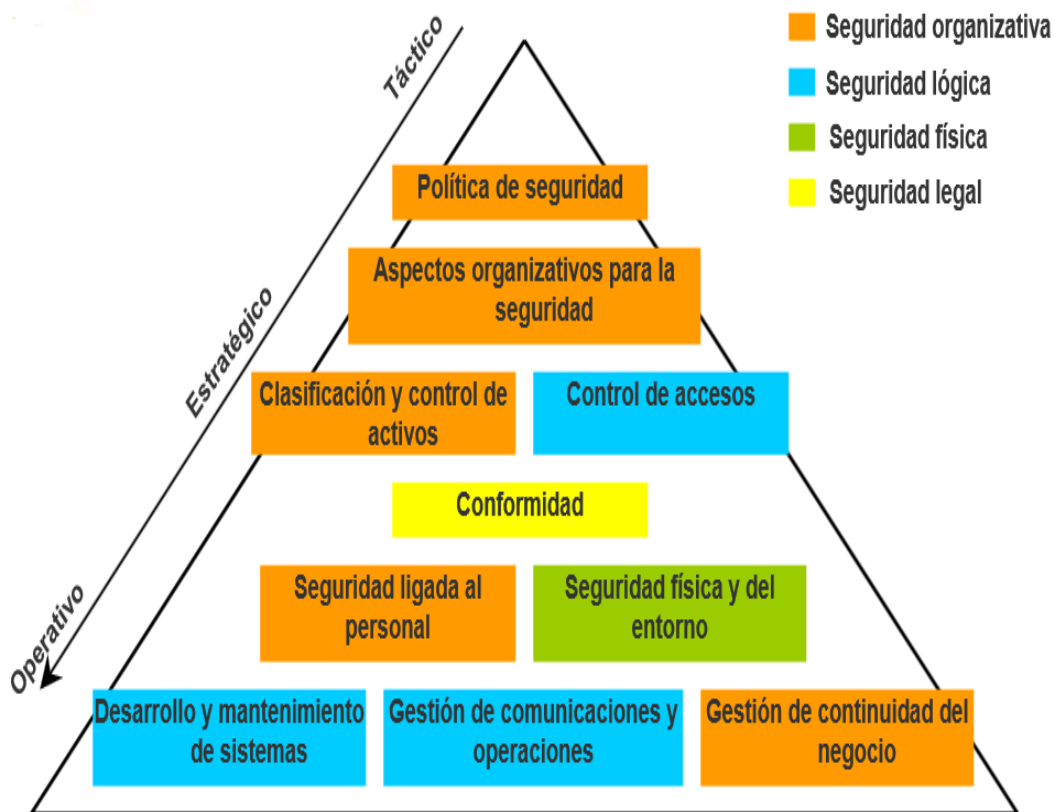


Figura 1. 30 Dominios de Control para Gestión de Seguridad Informática [66]

- **Gestión de Comunicaciones y Operaciones**

Se debe garantizar la seguridad de las comunicaciones y de la Operación de los sistemas críticos para el negocio.

- **Gestión de Incidentes de la seguridad**

Se encarga de asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

- **Desarrollo y Mantenimiento de Sistemas**

Es el dominio encargado de evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones, protegiendo la confidencialidad, autenticidad e integridad de la información.

- **Seguridad Física y de Entorno**

Las áreas de trabajo de la organización y sus activos deben ser clasificados y protegidos en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio.)

- **Seguridad Ligada al Personal**

Las implicaciones del factor humano en la seguridad de la información son muy elevadas. Todo el personal, tanto interno como externo a la organización, debe conocer las líneas generales de la política de seguridad corporativa y las implicaciones de su trabajo en el mantenimiento de la seguridad global.

- **Conformidad**

Habla acerca de definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información

- **Control de Acceso**

Se refiere a establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc.

- **Políticas de Seguridad**

Su objetivo es dirigir y dar soporte a la gestión de la seguridad de la información. La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicarla de la forma adecuada a todo el personal implicado en la seguridad de la información

- **Clasificación y Control de Activos**

Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcione a cada activo el nivel de protección adecuado a su criticidad en la organización.

- **Aspectos Organizativos para la Seguridad**

Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma

## **CAPÍTULO 2**

### **ANÁLISIS DE LA SITUACIÓN ACTUAL Y REQUERIMIENTOS**

#### **2.1 INTRODUCCIÓN**

El auge de las tecnologías de información ha llevado a un nuevo mundo de comunicaciones, donde hoy en día se convergen servicios antes separados; este tipo de comunicaciones toman el nombre de comunicaciones convergentes.

Si bien tradicionalmente las instituciones manejaban sus redes de voz y datos por separado, en la actualidad esto ya no resulta conveniente; es por ello que el presente proyecto pretende la unificación de estos dos servicios dentro de una misma red, con la finalidad de tener una administración sistemática y sencilla, que a su vez derive en un ahorro económico para la institución.

El presente capítulo tiene como objetivo fundamental determinar la situación actual de la Unidad Educativa Temporal “Jaime Roldós Aguilera”, describiendo la infraestructura actual de la institución y detallando los requerimientos necesarios para el posterior diseño de la red INTEGRADA de voz y datos.

Dentro de la descripción de la infraestructura actual se indicará la distribución física de las instalaciones, los elementos pasivos y activos con los que se cuenta, topología y sistema de administración de las “redes” que se mantiene en los diferentes departamentos, etc.

Con el levantamiento y análisis de la información antes mencionada se tendrá una visión más clara del estado actual de la institución, con lo cual se podrá determinar cómo se va a proceder con el posterior diseño de la red INTEGRADA de voz y datos para la Unidad Educativa Temporal “Jaime Roldós Aguilera”.

## 2.2 UNIDAD EDUCATIVA TEMPORAL “JAIME ROLDÓS AGUILERA” [9]

La Unidad Educativa Temporal “Jaime Roldós Aguilera”, es una institución educativa fundada en el año de 1980, según acuerdo ministerial 9716; se encuentra ubicada en la Provincia de Santo Domingo de los Tsáchilas, en su cabecera cantonal Santo Domingo de los Colorados, Ciudadela Los Unificados, calle Biblián y Catacocha. La figura 2.1 muestra el diagrama de ubicación de la institución.

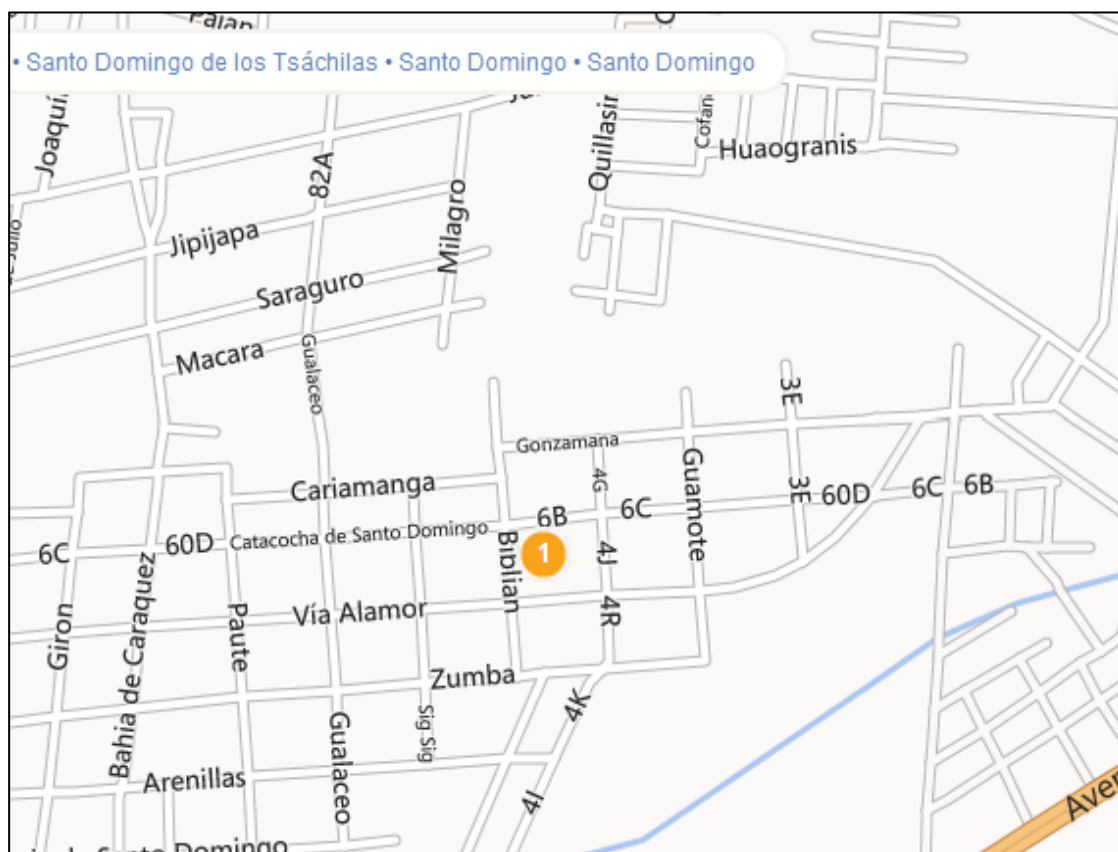


Figura 2. 1 Diagrama de ubicación de la Unidad Educativa Temporal “Jaime Roldós Aguilera” [9]

Actualmente brinda sus servicios a estudiantes en tres secciones, matutina la cual está destinada a los cursos de especialización, vespertina al ciclo básico, y nocturna a una combinación de las dos antes mencionadas. La institución cuenta con las especializaciones de Mecánica Industrial, Mecánica Automotriz, Electricidad e Informática.

Su alumnado es aproximadamente de 1500 estudiantes; en la parte administrativa y académica se tiene cerca de 60 personas, entre profesores, secretarías, auxiliares, laboratoristas, etc.

La Unidad Educativa Temporal “Jaime Roldós Aguilera” tiene como finalidad mejorar la calidad de estudio dentro de la ciudad, implementando nuevos proyectos de educación, especialidades, metodologías de estudios y sobre todo un cambio en la ideología tanto de profesores y estudiantes; formando así nuevos bachilleres que aporten técnica y éticamente al desarrollo de la comunidad.

### **2.2.1 MISIÓN INSTITUCIONAL**

“Formar bachilleres técnicos con suficiente capacidad de emprendimiento, calidad y pertenencia, que les permita aplicar nuevas tecnologías en armonía absoluta con la práctica de valores.”

### **2.2.2 VISIÓN INSTITUCIONAL**

“Situarnos como modelo de la educación técnica con calidad, eficiencia, integrando los valores y formando personas críticas, autocríticas, activas y proactivas para una nueva sociedad.”

## **2.3 DESCRIPCIÓN DE LA INFRAESTRUCTURA FÍSICA DE LA INSTITUCIÓN**

Antes de empezar por la descripción de los elementos con los cuales cuenta la Unidad Educativa Temporal “Jaime Roldós Aguilera”, es conveniente presentar un diagrama en el cual se muestre la distribución física de los distintos departamentos que la constituyen; esto con el propósito de poder detallar los requerimientos necesarios de forma más organizada y de fácil entendimiento para el posterior diseño.

La institución cuenta con una extensión aproximada de 7 Ha, dentro de las cuales aproximadamente 3 Ha están destinadas a canchas deportivas, zonas de recreación, y jardines; el resto del área es utilizada directamente por el plantel tanto para la enseñanza como para labores administrativas. La extensión antes mencionada se encuentra distribuida de la siguiente manera: Rectorado, Secretaría General y Colecturía, Dispensario Médico, Vicerrectorado, Biblioteca, Inspección General, Sala de Profesores, Laboratorios Informáticos, Laboratorios de Mecánica, Laboratorios de Electricidad, Salón Audiovisual, Aulas, bar y parqueaderos.

Para hacer más fácil la labor, se procederá a dividir el área de la institución en varias zonas, las cuales contarán con distintos departamentos y aulas. A continuación se detallarán las zonas de la Unidad Educativa Temporal “Jaime Roldós Aguilera”.

- **Zona A**, en esta zona se encuentra ubicado el Rectorado, Vicerrectorado, Secretaría General, Colecturía, Biblioteca y Departamento Médico.
- **Zona B** se ubican las aulas correspondientes a los sextos y terceros cursos, así como el laboratorio de PLC's digitales perteneciente a la especialidad de Electricidad.
- **Zona C** está conformada por la Inspección General, Sala de Profesores, Departamento de Electricidad, Departamento de Música y las aulas correspondientes a los primeros, segundos, cuartos y quintos cursos.
- **Zona D** corresponde al Departamento de Mecánica, Salón de Audiovisuales y las aulas de los sextos cursos, especialidades Mecánica y Electricidad respectivamente.
- **Zona E** donde se encuentran ubicados los laboratorios de Informática, y Mecánica; además aulas para la especialidad de Informática.
- Finalmente la **Zona F** corresponde a parqueaderos y bar de la Unidad Educativa Temporal “Jaime Roldós Aguilera”

La figura 2.2 muestra las zonas que se han enumerado anteriormente y su distribución física dentro de la institución.





Figura 2. 2 Distribución Zonal de la Unidad Educativa Temporal "Jaime Roldós Aguilera" [12]

También es importante indicar que dentro de la institución todos los departamentos y aulas son de una planta; cada bloque de aulas está constituido por 8 aulas, y por lo general existen dos bloques por zona, como lo muestra la figura 2.3.



Figura 2. 3 Bloque de aulas de la Unidad Educativa Temporal “Jaime Roldós Aguilera” [12]

## 2.4 DESCRIPCIÓN DE LA RED DE DATOS

Si bien la institución no cuenta con una red de datos unificada para todos los departamentos antes señalados, las necesidades que se han venido presentando en el transcurso de los últimos años, han obligado a la creación de “redes” dentro del área administrativa como en los laboratorios de Informática y Mecánica.

Estas mencionadas “redes” fueron creadas sin orden o especificación alguna, simplemente se buscó, en base a las necesidades presentadas por la Institución, una manera breve de que las estaciones de trabajo pertenecientes a los distintos laboratorios tengan acceso a Internet; para ello se realizó la conexión de cada estación de trabajo a un *switch*. Sin embargo, con ello no se cubrían otras necesidades presentes dentro de la institución como son: compartición de archivos, de impresoras, así como otras tareas de red en sí.

Sin duda alguna esto ha sido un gran problema ya que se maneja la información de manera separada; es por ello que se va a identificar cada una de estas “redes” y describirlas para conocer con qué equipos cuenta la institución.

Una vez descritas cada una de estas “redes”, la idea será unificar todas ellas dentro de una sola, la cual brindará transporte de datos y de VoIP con calidad de servicio (QoS).

En la Figura 2.4 se muestra el esquema actual de las “redes” de los distintos departamentos de la institución donde claramente se puede apreciar cómo las mismas son totalmente independientes; es decir que no están interconectadas entre sí.

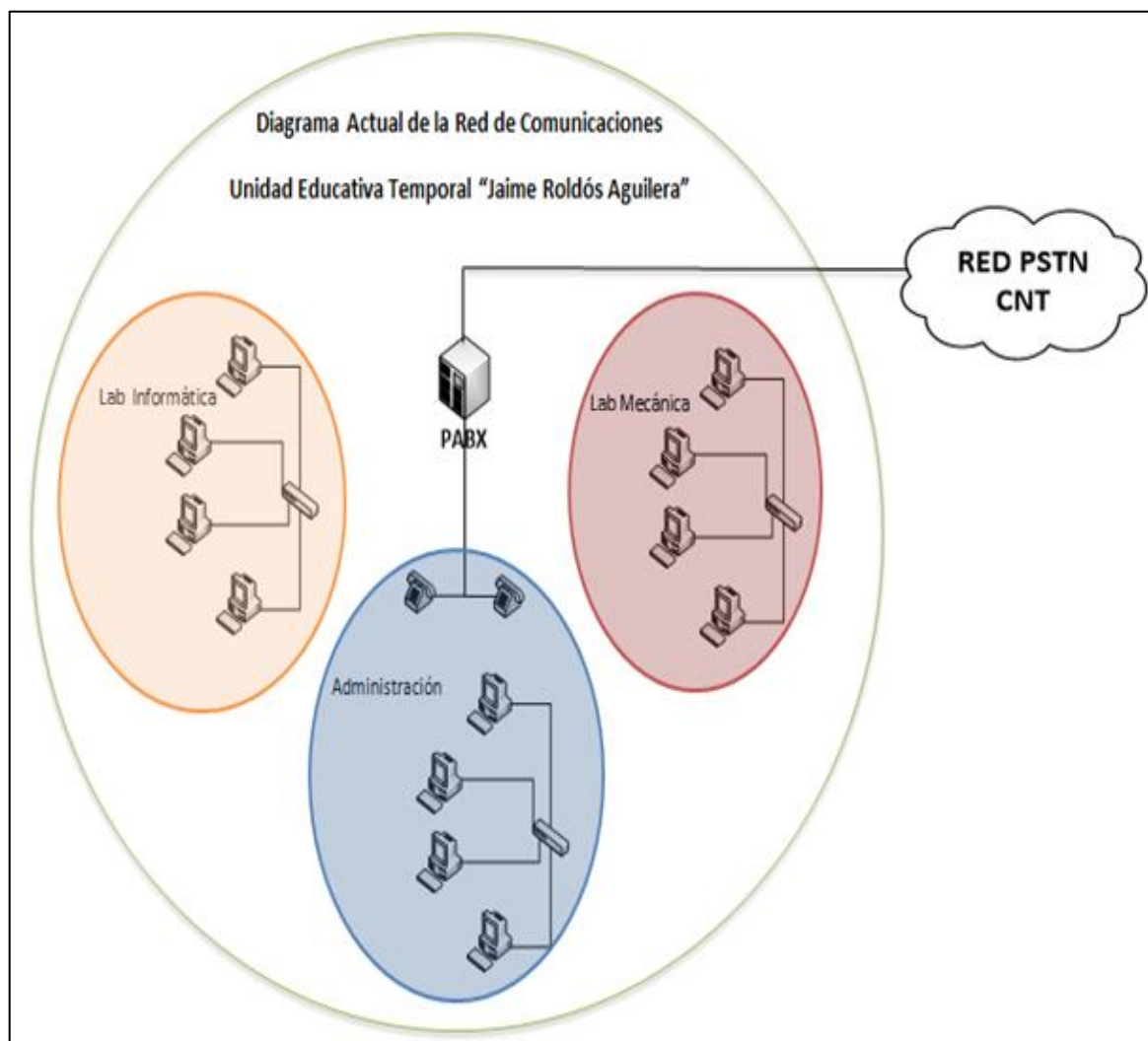


Figura 2. 4 Diagrama de la red actual de la Unidad Educativa Temporal “Jaime Roldós Aguilera” [12]

## 2.5 ANÁLISIS DE LA TOPOLOGÍA ACTUAL

Las “redes” mencionadas anteriormente fueron creadas desordenadamente y sin apearse a ninguna norma ni estándar, simplemente los equipos detallados en el numeral 2.6.3.1 se encuentran conectados a un equipo de conectividad, mediante una topología en estrella, utilizando puertos *Fast Ethernet* y cable UTP categoría 5e.

A pesar de que las “redes” cuenten con una topología estrella definida, el problema radica en que el mismo no cuenta con un sistema de cableado estructurado basado en normativas y estándares desarrollados para este propósito; obviamente esta práctica no es la adecuada ya que puede causar problemas en la administración de la red y en la solución de los mismos.

El correcto diseño de la topología juega un rol importante dentro de una red, pues es la encargada de determinar cómo se realizarán las interconexiones entre los diferentes equipos; de ella depende el porcentaje de falla que puede tener la misma al sufrir algún daño en el sistema de cableado estructurado o sus equipos de conectividad.

En la actualidad la topología que se tiene en la institución ha generado algunos conflictos, en ocasiones los cables UTP conectados a las estaciones de trabajo se han visto afectados, y se tiene que dejar sin servicio a la misma hasta proceder con el cambio del cable, principalmente en los laboratorios. Tampoco se cuenta con un correcto sistema de etiquetado en los puntos de red, lo que deriva en una administración compleja de las “redes”.

En base a lo mencionado en párrafos anteriores, este proyecto deberá determinar qué topología física y lógica va a tener la red INTEGRADA de voz y datos a diseñar en base a los requerimientos encontrados en este capítulo, permitiendo así una correcta administración y brindando la seguridad necesaria a la red.

## 2.6 EQUIPAMIENTO DE LA RED DE DATOS

Para poder realizar el correcto diseño de una red de comunicaciones es necesario saber qué posee la institución actualmente, es decir los elementos y equipos con los que se cuenta para determinar si están cumpliendo su función o si es necesario la adquisición o cambio de los mismos.

Al tener “redes” en algunos departamentos es obvio pensar que existen equipos de conectividad, estaciones de trabajo, entre otros; es por ello que se describirán los elementos con que cuenta la Unidad Educativa Temporal “Jaime Roldós Aguilera” para su posterior análisis. Una forma sencilla de determinar cómo están equipadas las “redes” de datos antes mencionadas, es dividiendo esta labor en dos partes: elementos activos y elementos pasivos.

### 2.6.1 ELEMENTOS PASIVOS [10]

Son aquellos elementos que se utilizan para interconectar mecánicamente los enlaces de una red de datos; no se encargan de generar o amplificar la señal, su función es simplemente transmitir la señal.

Entre los principales elementos pasivos de la red se encuentra el cableado estructurado, con todos los componentes que esto incluye, como son: cables, paneles de conexión, conectores, *racks*, entre otros.

#### 2.6.1.1 Sistema de Cableado Estructurado (SCE)

Al momento la institución no cuenta con un sistema de cableado estructurado, sin embargo se podría decir que las “redes” que se han generado en cada uno de los departamentos posee un cableado “**no estructurado**” propio, el cual emplea cable UTP categoría 5e; además dispone un *rack* que da acogida al dispositivo de interconectividad, en este caso un *switch*, un *patch panel* QPCOM QP-PP24E y los respectivos RJ45 de cada punto de red, como se lo puede apreciar en la figura 2.5.



**Figura 2. 5 Diagrama de cableado del Laboratorio de Informática I [12]**

Como se puede evidenciar, los elementos que forman parte del cableado no están apegados a ningún estándar, los mismos se encuentran al acceso de cualquier persona, lo que podría ocasionar problemas con los equipos que se encuentren conectados. También se puede visualizar que no se tiene un espacio definido para los equipos, incluso teniendo la extensión física necesaria para hacerlo.

Los *patchcords* no cuentan con etiquetas o identificativos que hagan saber a qué equipos proveen del servicio; el sistema de enrutamiento es inadecuado, pues aun teniendo canaletas para el enrutado existen cables que no se encuentran dentro de las mismas quedando expuestos a la intemperie, esto debido a que no se estableció un dimensionamiento adecuado para el cableado.

#### **2.6.1.2 Sistema de Puesta a Tierra [11]**

Al ser el plantel de carácter técnico y poseer dentro de sus instalaciones laboratorios de Electricidad, Mecánica e Informática, los cuales pueden ser afectados por descargas eléctricas, se ha implementado un sistema de puesta a tierra que se ubica junto al laboratorio de Mecánica y que es utilizado por los laboratorios de Informática y Mecánica respectivamente.

El tipo de sistema de puesta a tierra implementado es de tipo mallado y se encuentra debidamente diseñado en base a lo que establecen las recomendaciones del estándar 81 del ANSI/ IEEE y el estándar 607 ANSI/EIA/TIA, debido a que la puesta a tierra no solo debe cubrir sistemas de telecomunicaciones, sino también el uso de instrumentación mecánica, como son tornos, limadoras, motores y demás equipos propios de la actividad.

En la figura 2.6 se puede observar un esquema de la malla realizada en la zona donde se encuentran los laboratorios.

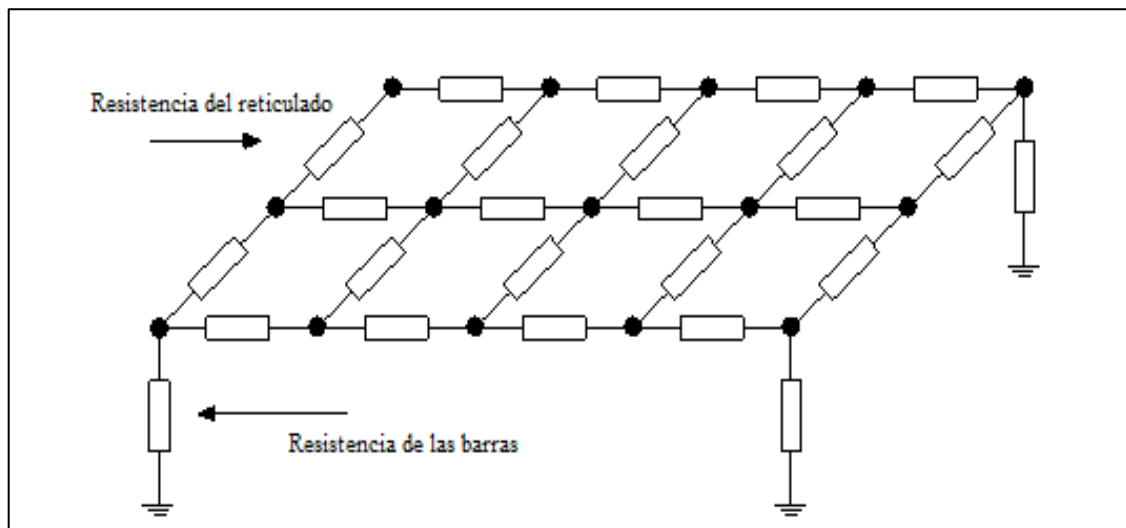


Figura 2. 6 Sistema de puesta a tierra mallado [12]

Sin duda alguna este sistema de tierra está realizado adecuadamente lo cual permite conectar los diferentes equipos de red a tierra, para las debidas protecciones.

### 2.6.2 ANÁLISIS DE LOS ELEMENTOS PASIVOS DE LA RED

Los elementos pasivos con los que cuenta actualmente la Unidad Educativa Temporal “Jaime Roldós Aguilera” no se encuentran en buenas condiciones, existen varias debilidades que pueden dejar sin servicio a las “redes” o parte de ellas.

El sistema de cableado que se tiene no es óptimo y fue levantado sin ninguna especificación técnica como recomiendan los organismos internacionales; los equipos se encuentran sin protección física alguna y ubicados en zonas de fácil acceso; así mismo las instalaciones y sus componentes están deteriorados y en cualquier momento pueden ocasionar pérdida de información o una caída total de la “red”.

Al no seguir un estándar para el sistema de cableado fácilmente se puede observar un desorden en las conexiones de las estaciones de trabajo a los equipos de conectividad, el enrutamiento no es el adecuado y varias estaciones de trabajo están conectadas sin la protección adecuada de sus respectivos *patchcords*, lo que ha llevado a que los mismos se encuentren expuestos a diferentes riesgos, tales como: humedad, cortes, desconexiones, entre otros, afectando así el rendimiento de las “redes”.

Tampoco ha sido tomado en cuenta la expansión de las estaciones de trabajo, por tal motivo, las pocas canaletas con las que se cuentan no dan el abasto suficiente para la cantidad de *patchcords* que deben cruzar por ella; además ninguno de los elementos que forman el sistema de cableado posee un sistema de etiquetado y por ende no se puede tener una correcta administración, mantenimiento y reparación de la red en caso de ser necesario.

Al no tener un sistema de cableado estructurado es difícil pensar en que se cuente con las pruebas de certificación necesarias para el mismo, lo cual sería una muy buena carta de presentación para la Unidad Educativa Temporal “Jaime Roldós Aguilera” frente a la comunidad Tsáchila, además de permitir mejorar la eficiencia de la institución.

También es importante señalar que algunos de los elementos que se encuentran en las diferentes “redes” podrían ser reutilizados en el diseño, como es el caso del *rack* que contiene al *switch* del laboratorio de Informática I, pues al momento se puede notar que se encuentra en buena condición; sin embargo, esto se determinará después del diseño a realizar en el capítulo siguiente.



En base al análisis realizado se puede concluir que la Unidad Educativa Temporal “Jaime Roldós Aguilera” necesita el diseño de un sistema de cableado estructurado, que contenga un correcto enrutamiento, sistema de etiquetado, dimensionamiento de ancho de banda y todo lo establecido en los estándares internacionales mostrados en el capítulo 1.

### **2.6.3 ELEMENTOS ACTIVOS [10]**

Están constituidos por aquellos dispositivos que se caracterizan principalmente por ser electrónicos y que se encargan de distribuir la información a través de la red; se tiene como ejemplo: concentradores, *switches*, *router*, etc.

Si bien la institución no cuenta con una LAN, debido a las necesidades ha tenido que ir adquiriendo varios equipos activos, por lo cual se debe detallar los equipos con los que cuenta actualmente; para ello se presenta un inventario de dichos equipos, determinando sus principales características y ubicación, dentro de las zonas de la institución.

#### **2.6.3.1 Equipos Periféricos**

En cada una de las zonas pertenecientes a la institución existen diferentes equipos periféricos, ya sean éstos, estaciones de trabajo, impresoras, cámaras web, entre otros. Los de mayor impacto constituyen las estaciones de trabajo e impresoras. A continuación se presenta una descripción de los equipos periféricos de las zonas antes mencionadas.

Las estaciones se encuentran ubicadas principalmente en los laboratorios y departamento administrativo, poseen distintas características pues no todas están destinadas a la misma labor. Por otro lado se tienen las impresoras, las mismas que solo se encuentran ubicadas en la zona A, en el Rectorado, Secretaría General y Colecturía. En la tabla 2.1 se muestran los equipos periféricos antes mencionados con sus respectivas cantidades, ubicaciones, y principales características.

<b>EQUIPO</b>	<b>CANTIDAD</b>	<b>MODELO/ PROCESADOR</b>	<b>RAM</b>	<b>SISTEMA OPERATIVO</b>	<b>UBICACIÓN</b>
<b>ESTACIÓN DE TRABAJO</b>	20	INTEL 2,40 GHZ PENTIUM 4	512 MB	Windows XP Professional	Lab. Informática II Lab. Informática I
<b>ESTACIÓN DE TRABAJO</b>	20	INTEL 2,80 GHZ PENTIUM 4	1GB	Windows XP Professional	Lab. Informática I Lab. Mecánica Rectorado Vicerrectorado Secretaría General Contabilidad.
<b>ESTACIÓN DE TRABAJO</b>	18	AMD SEPPROM 2,7 GHz	1 GB	Windows XP Professional	Lab. PLC Digitales Departamento Música Departamento Electricidad Departamento Mecánica Salón Audiovisual
<b>ESTACIÓN DE TRABAJO</b>	7	CELERON 1,7 GHz, PENTIUM 4	512 MB	Windows XP Professional	Lab. Electricidad
<b>ESTACIÓN DE TRABAJO</b>	3	INTEL 2,40 GHZ PENTIUM 4	256 MB	Windows XP Professional	Colecturía Biblioteca Departamento Médico Inspección General Sala de Profesores
<b>IMPRESORA</b>	1	SAMSUNG ML-2010	N/A	N/A	Rectorado
<b>IMPRESORA</b>	1	SAMSUNG MI-1610	N/A	N/A	Secretaría General
<b>IMPRESORA</b>	1	EPSON LQ- 2090	N/A	N/A	Secretaría General
<b>IMPRESORA</b>	1	CANON MP-280	N/A	N/A	Secretaría General
<b>IMPRESORA</b>	1	HP F-2480	N/A	N/A	Colecturía

**Tabla 2. 1 Lista de equipos periféricos [12]**

### 2.6.3.2 Equipos de Conectividad

Al tener creadas “redes” dentro de algunos departamentos es lógico pensar que existen equipos de conectividad, como son *switches*, *routers*, *AP*, etc. Estos equipos se encargan de distribuir el ancho de banda en los departamentos a los que pertenecen y el principal servicio que ofrecen es acceso *web*.

Fueron adquiridos en base a la necesidad de compartir el ancho de banda entre los usuarios, sin realizar el adecuado dimensionamiento que los equipos deben tener, lo que ha llevado a tener problemas cuando éstos se conectan de manera simultánea al Internet. En la tabla 2.2 se muestra la lista de los dispositivos de conectividad que posee la institución.

EQUIPO	CANTIDAD	MODELO	UBICACIÓN
SWITCH	2	CNET CSH-2400	Lab. Informática I Secretaría General Colecturía
SWITCH	2	ADVANTEK ANS-24RC	Lab. Informática II Lab. Mecánica
ROUTER INALÁMBRICO	1	D´LINK DSL-524D	Lab. Informática I
ROUTER INALÁMBRICO (AP)	1	D´LINK DIR-600	Lab. Informática I

Tabla 2. 2 Listado de equipos de conectividad [12]

### 2.6.4 Análisis de los Elementos Activos de la Red

A partir de la información levantada en el numeral 2.6.3 donde se detalla los elementos activos con que cuenta la institución, así como sus características técnicas, se puede determinar lo siguiente:

Las estaciones de trabajo están funcionando correctamente y su principal inconveniente es la poca memoria RAM que poseen, algunas llegan a tener 512 y hasta 256 MB.

También se observa que el sistema operativo de las estaciones de trabajo está desactualizado, presentando problemas a los usuarios al momento de realizar sus actividades, tales como bloqueos o congelamiento de sus estaciones de trabajo, generando así malestar entre ellos.

Por tal motivo se recomienda a la institución para el posterior diseño la expansión de la RAM en los equipos, de ser posible que todos cuenten con 4 GB, debido a las aplicaciones que van a soportar. También es recomendable la actualización del sistema operativo de las estaciones de trabajo para ir acorde al avance informático.

Sin duda alguna el hecho de no adquirir nuevos equipos permitirá un ahorro para la institución; sin embargo, se debe considerar la adquisición de nuevas estaciones de trabajo para los departamentos que actualmente no cuentan con ellas.

Otro elemento importante son las impresoras; actualmente se encuentran funcionando correctamente y sin ningún inconveniente; no obstante, se debe considerar la compra de nuevas impresoras para los demás departamentos, ya que como se observa todos estos equipos se encuentran ubicados en la Zona A, y dichos departamentos con el nuevo diseño deberán tener la facilidad de imprimir desde sus áreas de trabajo.

Finalmente, se tienen los equipos de conectividad, si bien al momento están funcionando, han empezado a presentar problemas, lo que ha llevado a tener varios inconvenientes en los diferentes laboratorios y en algunas ocasiones se tienen que proceder a reiniciar dichos dispositivos para que puedan proveer el servicio a los usuarios.

El último equipo adquirido fue el *Router* inalámbrico *D'Link DIR 600*, el mismo que se encuentra funcionando sin ningún inconveniente. Este equipo fue adquirido para reemplazar al *Router D'Link DSL 524-D* que ha presentado varias dificultades.

En el capítulo siguiente se determinarán los requisitos que deben tener los equipos de conectividad en base al diseño de la red, y así determinar si alguno de los equipos mostrados puede ser reutilizado.

### 2.6.5 SISTEMA TELEFÓNICO [12]

La infraestructura telefónica actual con la que cuenta la institución se basa en la conexión directa a la PSTN<sup>25</sup> mediante la CNT<sup>26</sup>, la cual provee de 2 líneas telefónicas arrendadas, y que se encuentran a nombre de la Unidad Educativa Temporal “Jaime Roldós Aguilera”, con los números 022756729 y 022767966.

De dichas líneas telefónicas la correspondiente al número 022756729 provee a la institución el servicio de fax y se encuentra ubicada en la oficina de Rectorado, mientras que la otra línea telefónica cuenta con varias extensiones de su mismo número, ubicadas en oficinas de Secretaría General y Colecturía.

Dentro de la institución no existe una central telefónica para el sistema de voz, generando así problemas con las comunicaciones de voz.

Al momento para poder comunicarse con una persona de la institución se debe esperar que la misma llegue desde su lugar de trabajo al departamento administrativo donde se encuentra el teléfono, lo que conlleva al malestar de los usuarios y del personal de la institución.

Otro de los principales problemas que se tienen con la comunicación es el bloqueo y pérdidas de llamadas desde el exterior, esto debido a que la institución no cuenta con un mecanismo que permita la transferencia de llamadas de una línea a otra (*key system*); es decir, si una persona está utilizando uno de los teléfonos el servicio se bloquea para los demás usuarios, lo que deriva en pérdidas de llamadas.

---

<sup>25</sup> PSTN: Red Pública Telefónica Conmutada

<sup>26</sup> CNT: Corporación Nacional de Telecomunicaciones

Para la institución resulta primordial tener un sistema de comunicación de voz interno para poder evitar estos inconvenientes; es por ello que en el presente proyecto se contemplará el diseño de un sistema de telefonía, al fin de satisfacer las necesidades mencionadas. Para establecer el sistema de voz se tienen dos opciones; la primera mediante los mecanismos tradicionales de telefonía, o a su vez una red convergente que incluya transmisión de voz sobre la red de datos.

El presente proyecto contemplará el diseño de un sistema de Telefonía IP, pues al tener que diseñar una red de datos es muy conveniente integrarla con el servicio de voz, teniendo así una sola red que manejará las comunicaciones de voz y datos, y no redes separadas como sería el caso de tener un sistema de telefonía convencional.

Tener una red convergente determinará un ahorro para la institución, pues con una sola inversión se tendrá los servicios de voz y datos, una administración sistemática y sencilla; además de las ventajas ya mencionadas acerca de la Telefonía IP en el capítulo 1. La Figura 2.7 muestra el sistema de voz actual de la Institución y la ubicación de las líneas telefónicas proporcionadas por la CNT.

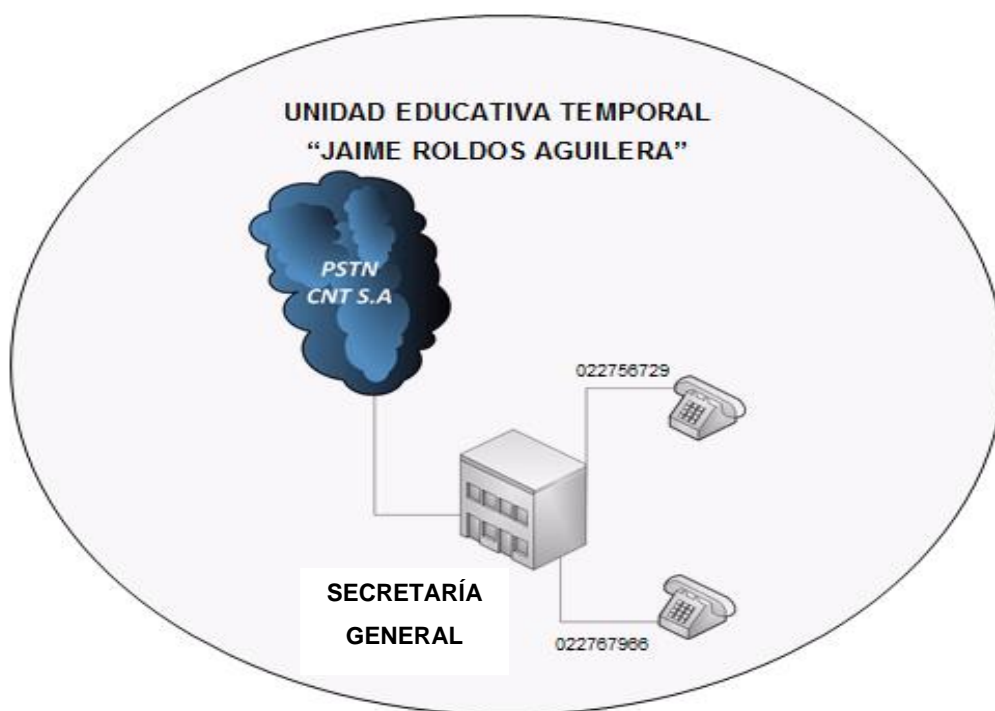


Figura 2. 7 Sistema Telefónico de la Unidad Educativa Temporal "Jaime Roldós Aguilera" [12]

La institución actualmente cuenta con varios equipos de voz, los mismos que se muestran en la tabla 2.3.

EQUIPO	CANTIDAD	MODELO	UBICACIÓN
TELÉFONO / FAX	1	PANASONIC KX-FT901	Rectorado
TELÉFONO	3	PANASONIC KX-TS560	Secretaría General Colecturía
TELÉFONO	1	PANASONIC KX-FT937	Lab. Informática I

Tabla 2. 3 Listado de equipos de voz [12]

#### 2.6.5.1 Análisis del Sistema Telefónico Actual

El sistema telefónico que maneja la Unidad Educativa Temporal “Jaime Roldós Aguilera” aun no siendo el adecuado ha permitido la comunicación de la institución con el exterior con las limitantes antes señaladas como bloqueos o pérdidas de llamadas al no poseer una central telefónica; sin embargo, el principal problema se presenta en las comunicaciones internas entre los departamentos ya mencionados, debido a la extensión y distribución del plantel.

Por lo tanto, el sistema actual no cumple todas las necesidades requeridas, y resulta insuficiente para sus usuarios. Basado en esto, se plantea el diseño de un sistema telefónico interno basado en la transmisión de VoIP sobre la misma red de datos, generando así una red mucho más completa, comunicando a todos los departamentos, y generando un ahorro a la institución.

De los equipos mostrados en la tabla 2.3, se puede decir que todos los teléfonos están en perfectas condiciones, y que se los puede seguir utilizando. En el próximo capítulo se detallarán los requisitos que deben poseer cada uno de los teléfonos necesarios para el diseño de la red , y cuántos de ellos se necesitarán para poder establecer un servicio de voz IP interno dentro de la Unidad Educativa Temporal “Jaime Roldós Aguilera”.

### 2.6.6 RED INALÁMBRICA [12]

La red inalámbrica se utiliza generalmente para tener acceso a la información de una red sin la necesidad de estar conectado a un punto físico de la misma; sin embargo, en la actualidad es muy común que uno de los principales usos de una red inalámbrica sea brindar acceso a Internet a los visitantes de la institución, profesores y estudiantes en general.

Al momento se cuenta con dos dispositivos inalámbricos (*routers*) como se detalló en la tabla 2.2; mediante ellos se provee de acceso a Internet al Laboratorio de Informática I y a sectores cercanos al mismo.

Estos dispositivos pueden ser configurados vía *web* y a partir de esta opción se puede ver las configuraciones actuales de los mismos; sin embargo, solo de uno de ellos se posee las contraseñas necesarias y es la que se mostrará a continuación.

Para ingresar a la interfaz de configuración del Router *D'Link DIR 600*, se debe digitar en la barra URL de un *browser*<sup>27</sup> la dirección IP: 10.1.1.1, con la cual se accede al dispositivo; después de ingresar correctamente se puede configurarlo y administrarlo de acuerdo a las necesidades.

En la figura 2.8 se muestran las configuraciones básicas del *Router* como son su SSID, su configuración TCP/IP y otras características propias del dispositivo; se puede observar que el dispositivo se encuentra en modo *Access-Point*.

Este dispositivo trabaja en la banda de 2.4 GHz y con una encriptación WPA2<sup>28</sup>; así mismo maneja una lista de control de acceso basada en direcciones MAC<sup>29</sup>, tal como se puede apreciar en la figura 2.9.

---

<sup>27</sup> **Browser:** Es una aplicación software que permite al usuario visualizar documentos de hipertexto

<sup>28</sup> **WAP:** Acceso al Wifi Protegido

<sup>29</sup> **MAC:** Control de Acceso al Medio.- Identificador único de una tarjeta o dispositivo de red



Access Point Status	
<b>System</b>	
Uptime	2day:1h:1m:27s
Firmware Version	v6.2.3.0.1e
<b>Wireless Configuration</b>	
Wireless Mode	AP
SSID	enlace
Channel Number	1
Encryption	WPA2
Associated Clients	2
BSSID	00:12:0e:99:d2:0c
<b>TCP/IP Configuration</b>	
IP Protocol	Fixed IP
IP Address	10.1.1.254
Subnet Mask	255.0.0.0
Default Gateway	10.1.1.1
MAC Address	00:12:0e:99:d2:0b

Figura 2. 8 Router Status

También se pueden observar las configuraciones para la conexión con el servicio de Internet, es decir la dirección IP, la sub-máscara de red, y las configuraciones básicas TCP, en la figura 2.10

Wireless Access Control		
Wireless Access Control Mode:	Disable	
MAC Address:	<input type="text"/>	Comment: <input type="text"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>		
<b>Current Access Control List:</b>		
MAC Address	Comment	Select
00:21:00:ce:00:f1	basantes	<input type="checkbox"/>
00:12:0e:99:d2:0c	Pic enlace	<input checked="" type="checkbox"/>
00:16:ec:ad:bb:18	galo ocellana	<input type="checkbox"/>
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>		
Wireless Security Setup		
Encryption:	WPA2(AES)	
<input checked="" type="checkbox"/> Use 802.1x Authentication	<input type="button" value="Set WEP Key"/>	
WPA Authentication Mode:	<input type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits	
WPA Cipher Suite:	<input checked="" type="radio"/> Enterprise (RADIUS) <input type="radio"/> Personal (Pre-Shared Key)	
Pre-Shared Key Format:	Passphrase	
Pre-Shared Key:	<input type="text"/>	
Group Key Life Time:	86400 sec	
<input checked="" type="checkbox"/> Enable Pre-Authentication		
Authentication RADIUS Server:	Port: 1812	IP address: <input type="text"/> Password: <input type="text"/>
<small>Note: When encryption WEP is selected, you must set WEP key value.</small>		
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>		

Figura 2. 9 Configuraciones de seguridad y acceso del Router

Si bien el dispositivo cuenta con varias opciones útiles no todas se encuentran activas, como es el caso del servidor DHCP, el protocolo *Spanning-Tree*, entre otras, esto se debe a la sencillez con la que se ha implementado la red inalámbrica por así llamarla.

Figura 2. 10 Configuraciones LAN del Router

### 2.6.6.1 Análisis de la Red Inalámbrica

Una vez observadas las configuraciones de *router* inalámbrico *D'Link DIR 600*, se determina que el mismo está trabajando sin ningún inconveniente y que está cumpliendo su propósito, que es proveer Internet a los dispositivos móviles que estén dentro de su radio de alcance.

Si bien se puede hacer mejoras en la configuración cabe indicar que este dispositivo es bastante simple y que incluso está destinado para áreas muy limitadas, y redes pequeñas. Para determinar el alcance máximo de este dispositivo se ha utilizado un mecanismo conocido como *Site Survey*, y que será detallado en el numeral 3.6.11.1.

En base a este mecanismo se determinó que al llegar a una distancia aproximada de 10 metros desde el lugar donde se tiene el dispositivo, la señal comienza a debilitarse, y finalmente entre 12-15 metros la señal se pierde por completo como se muestra en la figura 2.11.

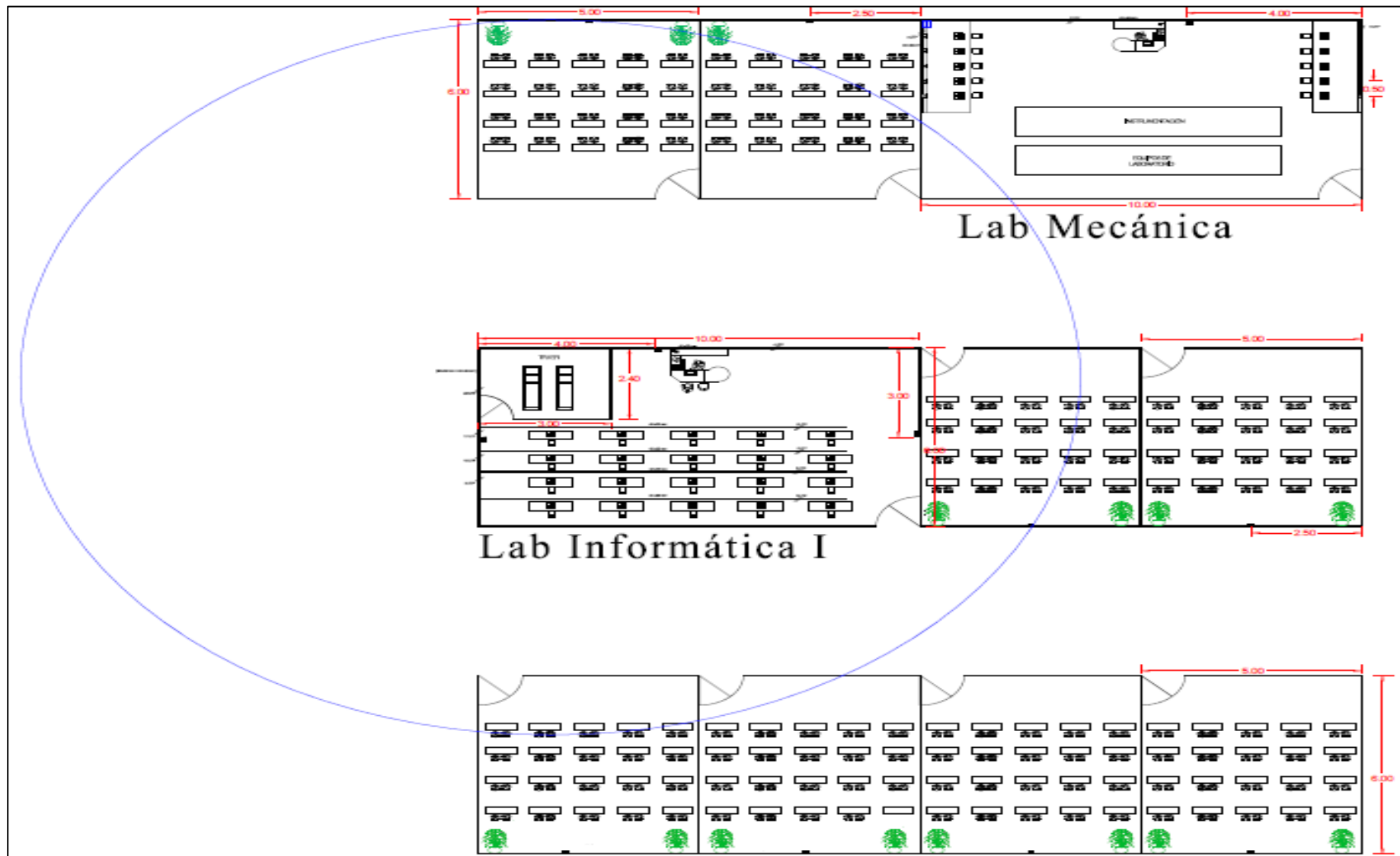


Figura 2. 11 Radio de alcance del *router* D'Link DIR 600

## **2.6.7 SERVICIO DE INTERNET CONTRATADO [12]**

Al momento la institución cuenta con un servicio de Internet provisto por la CNT, el cual es mediante una línea dedicada ADSL que cuenta con una capacidad de 2 Mbps a través de la línea telefónica, es decir, utilizando como medio de transmisión el cobre, y a través de un *modem* WI-FI que dispone de 4 puertos Ethernet; además cuenta con el servicio que otorga el Gobierno a cada uno de los planteles educativos con una capacidad de 1 Mbps dedicado.

El servicio de Internet que es auspiciado por el Gobierno se lo utiliza para los laboratorios de Informática principalmente, en tanto que la línea dedicada está destinada para la zona administrativa, es decir, Rectorado, Vicerrectorado, Secretaría General y Colecturía.

### **2.6.7.1 Análisis del Servicio de Internet**

El servicio de Internet con el que se cuenta en la institución resulta bastante deficiente, pues el servicio que se ha contratado está orientado al uso doméstico y no pensado en una red de comunicaciones; si bien el ancho de banda actual permite el uso de aplicaciones comunes, esto no ha evitado la molestia como demoras y difícil acceso.

Actualmente el servicio que las mencionadas “redes” proporcionan es de acceso a la *web*, y el principal problema se presenta en la zona de laboratorios, ya que pueden existir 40 usuarios simultáneos que deseen utilizar el servicio, lo cual ocasiona una saturación de las “redes” y el rendimiento de las mismas se ve afectado.

Al diseñarse una red convergente que incluirá servicios de voz y datos, con aplicaciones como correo electrónico, VoIP, entre otras, se debe realizar un correcto dimensionamiento del ancho de banda que la nueva red requerirá y así poder contratar el servicio de Internet adecuado.

En consecuencia a lo mencionado se puede decir que el servicio de Internet contratado no es el suficiente para el nuevo diseño y que se debe realizar el correcto dimensionamiento del mismo.

### **2.6.8 APLICACIONES ACTUALES**

Dentro de toda institución educativa existen aplicaciones que son utilizadas muy frecuentemente, como por ejemplo: *Microsoft office*, acceso a páginas web, antivirus, *Adobe Reader*, compresores de archivos como WinRAR, WinZip, etc.

Para la Unidad Educativa Temporal “Jaime Roldós Aguilera” esto no es una excepción; sin embargo, así como existen aplicaciones que se usan de manera común, existen otras aplicaciones que son de uso particular, es decir, aplicaciones que se utilizan en sectores especializados dentro de la institución, como son los laboratorios de Informática, Mecánica, Electricidad; dentro de estas aplicaciones se pueden encontrar las siguientes: Autocad 2007, AVR, *Circuit Maker*, Matlab, entre otras.

Cabe indicar que estas aplicaciones han sido instaladas en las estaciones de trabajo que lo han necesitado de manera independiente, es decir, no se encuentran en red y por tal motivo en caso de querer realizar alguna actualización o mantenimiento se tendría que hacer en cada máquina.

En la tabla 2.4 se detallan las aplicaciones que actualmente están siendo utilizadas por las distintas estaciones de trabajo con que cuenta la institución.

Con el diseño de la red INTEGRADA se espera que la mayor parte de estaciones de trabajo cuenten con las mismas aplicaciones, obviamente con las excepciones respectivas, es decir; todas las estaciones de trabajo deberán poseer las mismas versiones de aplicaciones, exploradores, y demás aplicaciones, facilitando así la administración de las estaciones de trabajo que va a tener la institución.

### 2.6.9 REQUERIMIENTOS FUTUROS

Las autoridades de la Unidad Educativa Temporal “Jaime Roldós Aguilera” al conocer que se va a diseñar una red para su institución han mostrado gran interés en presentar sus requerimientos para dar la solución en un futuro y así tener mayor competitividad con otras instituciones del Cantón. Para ello se han analizado las necesidades que los docentes, personal administrativo y estudiantes consideran deben ser provistas por la red de la institución.

En este contexto se detallarán las principales aplicaciones que se consideran necesarias y los servidores que se requieren para poder cumplir con dichas aplicaciones.

Aplicaciones/ Ubicación	Zona A	Inspecciones	Departamentos	Lab Informática	Lab PLC	Lab Mecánica	Lab Electricidad
Microsoft Office 2003	7	0	0	0	0	0	0
Microsoft Office 2007	8	6	4	24	10	6	12
WinRar Archive	10	2	0	24	10	1	1
Internet Explorer 6.0	4	6	4	0	0	0	0
Mozilla Firefox	11	0	0	0	0	0	0
Google Chrome	6	3	0	24	10	6	12
Adobe Profesional	8	3	1	24	1	1	1
Antivirus NOD32	2	3	0	24	10	6	12
Visual Studio Profesional	6	0	0	24	0	0	0
Autocad 2007	6	0	0	0	0	0	12
Matlab	6	0	0	24	10	0	12
AVR studio	0	0	0	0	10	0	12
Circuit Maker 2000	0	0	0	0	10	0	12

Tabla 2. 4 Aplicaciones Actuales

### **2.6.9.1 Servicios de Red Requeridos**

Dentro de una entidad educativa existen varios servicios que son indispensables para que la información pueda ser manejada de manera estructurada y eficiente, de tal manera que se puedan satisfacer los requerimientos de los diferentes tipos de usuarios que existen dentro del plantel, ya sean éstos estudiantes, profesores o personal administrativo.

A continuación se detallan los principales servicios que los usuarios creen necesario implementar en la intranet, así, como los servicios con que una entidad educativa debe contar.

#### *2.6.9.1.1 Servidor Web*

Uno de los servicios más utilizados dentro de cualquier institución pública o privada, sin duda alguna, es el servicio *web*; este servicio proveerá a la institución su propio sitio *web*, así como implementar educación virtual, sistema de matrículas, calificaciones vía *web*, y otras aplicaciones útiles en el mundo actual de la educación.

#### *2.6.9.1.2 Servidor DNS (Domain Name Server)*

Dentro de una institución es muy importante el poder identificar a sus equipos de forma clara y concisa, esto se lo puede hacer de manera más eficiente con el uso de un servidor de nombres, ya que dentro de la red resulta más sencillo identificar a cada equipo mediante un nombre que con su respectiva dirección IP.

El servidor DNS forma una estructura jerárquica a partir de un dominio, y así identifica a cada sector de la institución.

También ayudará a una rápida identificación del equipo dentro de la red que se desea acceder, como la fácil administración de los mismos.

El dominio para la institución será *jra.net*

#### 2.6.9.1.3 *Servidor de Correo Electrónico*

Este servicio facilita el intercambio de información tanto dentro de la Intranet como fuera de ella, pudiendo enviar a diferentes usuarios de la red información, sin importar su ubicación geográfica.

Este servicio se encarga de generar cuentas tanto para el personal administrativo, profesores y de ser requeridos a estudiantes, así como de la administración de las mismas, configuraciones de cada uno de ellas tanto en capacidad, rendimiento, y otras opciones propias del servicio.

#### 2.6.9.1.4 *Servidor de Descarga de Archivos (FTP)*

Por la naturaleza propia de la institución es necesario contar con un servicio que permita a sus miembros, ya sean éstos estudiantes, profesores o personal administrativo, descargar información de la Intranet.

Este servicio mantendrá almacenada la información como formularios, tipos de solicitudes, boletines de notas, entre otra información importante para los miembros de la institución.

#### 2.6.9.1.5 *Servidor DHCP*

Uno de los problemas principales dentro de una Institución es el direccionamiento de la red, sobre todo cuando existe una gran cantidad de estaciones de trabajo actuales y futuras que se deberán manejar.

Por ello se hace necesario un servidor DHCP, con la finalidad de que el direccionamiento IP sea dinámico y así facilitar la administración de la red optimizando las direcciones IP públicas.



### **2.6.9.2 Servicios en Tiempo Real**

A medida que la tecnología avanza aparecen nuevas tendencias al momento de integrar servicios tradicionales, y que ahora se lo puede tener dentro de la misma infraestructura de datos, concepto conocido como redes convergentes. Uno de estos servicios es la telefonía, la cual hace poco tiempo solo se la podía implementar a través de la PSTN o una red privada mediante el uso de una PABX; sin embargo, con el auge del Internet, el avance de tecnologías de codificación de voz y el apareamiento de la ingeniería de tráfico, ahora se puede integrar este servicio dentro de una red de datos.

Una de los servicios en tiempo real con que toda Institución debe contar es el de telefonía, tanto para comunicaciones internas como externas, si bien antes se tenía como opciones principales el uso de la PSTN o centrales telefónicas privadas, hoy en día esto ha tomado un giro diferente y las empresas están recurriendo a la integración de la telefonía en las redes de datos. La Unidad Educativa Temporal “Jaime Roldós Aguilera” está presentado grandes problemas debido a no contar con un adecuado sistema de voz.

La gran cantidad de estudiantes y personal administrativo que alberga se muestra preocupado al no poder establecer comunicaciones de voz con la institución; los profesores tienen que caminar varios trayectos desde sus aulas hasta poder atender una llamada, teniendo que dejar en muchas ocasiones sus jornadas de trabajo y afectando la calidad de enseñanza que se brinda a los estudiantes.

Por tal motivo es indispensable tener un sistema de comunicación de voz interno en la institución, el mismo que permita no desapegarse de la misión y visión que la Unidad Educativa Temporal “Jaime Roldós Aguilera” se ha planteado.

### **2.6.10 ADMINISTRACIÓN DE LA RED**

La administración de la red es un parámetro a tener muy en cuenta, más aún cuando la red está constituida por un gran número de usuarios.

Una correcta administración puede generar muchos beneficios a la hora de realizar mantenimiento, inserción o eliminación de equipos, usuarios y servicios. La administración abarca tanto el *hardware* como el *software* de la red, y entre las principales tareas a cumplir se tienen las siguientes:

- Instalación y mantenimiento de la red
- Determinación del grado de utilización de los distintos servicios
- Diagnóstico de problemas y evaluación de posibles mejoras
- Documentación de la red y sus características

#### **2.6.10.1 Análisis de la Administración Actual de la Red**

La Unidad Educativa Temporal “Jaime Roldós Aguilera” al momento no cuenta con una correcta administración de la red, sus pequeñas “redes” simplemente fueron implementándose para cubrir los requerimientos que se venían presentando.

Sus equipos no han tenido mantenimiento desde su instalación, y tampoco se tiene documentación de los cambios realizados, como inserción de nuevas estaciones de trabajo, aplicaciones, etc.

Las mejoras realizadas han sido en base a los inconvenientes que los equipos han presentado y a las nuevas necesidades.

Por esta razón se hace indispensable que el diseño de la red contemple un correcto mecanismo para la administración de la red.

#### **2.6.11 SEGURIDAD EN LA RED**

Uno de los aspectos más difícil de controlar y manejar dentro de una red de comunicaciones es la seguridad, por lo tanto es conveniente mantener la información de la red bajo cuidado y control, mediante el uso de políticas de seguridad.

El desarrollo de un sistema de seguridad se lo debe hacer en base a estándares internacionales; para este propósito existen varios organismos como ISO/ICE con su estándar 27002 que ofrece varias recomendaciones para la seguridad de una red.

#### **2.6.11.1 Análisis de la Seguridad Actual en la Red**

La seguridad dentro de una red, involucra aspectos de seguridad física como lógica, etc. Actualmente dentro de la Unidad Educativa Temporal “Jaime Roldós Aguilera” este factor no está siendo considerado como debe ser.

La forma mediante la cual la institución está brindando seguridad a sus “redes” se basa en la instalación de antivirus en cada estación de trabajo; sin embargo, la mayoría de ellos se encuentran desactualizados, lo que no garantiza la protección de la información de sus equipos.

Así mismo se observa que la seguridad de los equipos de conectividad es inapropiada, los dispositivos se encuentran al alcance de todo persona, pudiendo afectar el funcionamiento de las “redes” existentes.

A nivel lógico tampoco se tiene la seguridad adecuada, es decir, si algún equipo de conectividad se ve afectado, todo el “red” dejaría de tener el servicio de Internet que ésta proporciona; no existen mecanismos de redundancia que puedan restablecer el servicio en caso de presentarse un incidente.

Pese a los inconvenientes detallados, la institución ha desarrollado un instructivo de uso para los equipos de los laboratorios, el cual podría ser considerado como políticas de seguridad. [35]

Entre las principales normas a cumplir dentro de los laboratorios se tienen:

1. El uso de las computadoras de laboratorio es exclusivo para personal académico y estudiantes.
2. Los equipos del laboratorio no pueden ser cambiados de ubicación.

3. Se permite un máximo de dos estudiantes por computadora.
4. No se permite el ingreso de bebidas, *snacks*, o cualquier otro tipo de alimento.
5. El uso de los equipos es solo para fines académicos, queda prohibido el uso de los computadores para otros fines.
6. Se debe mantener el orden y silencio dentro del Laboratorio.

Si bien esto ha ayudado a tener cierto control dentro de los laboratorios, se debe tener un mejor plan para la seguridad de la red para todos los departamentos, por lo tanto en el capítulo siguiente se establecerán políticas básicas de seguridad, con la finalidad de mantener protegida la red en todos sus niveles.

#### **2.6.12 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL Y REQUERIMIENTOS DE LA RED**

La Unidad Educativa Temporal “Jaime Roldós Aguilera”, carece de las mayorías de prestaciones que una red debe proveer, no cuenta con una correcta administración y seguridad, así como tampoco tiene un sistema de conmutación de voz para la comunicación interna.

El crecimiento desordenado ha permitido tener “*redes*” aisladas dentro de una misma institución pudiendo causar conflictos internos, y pérdida de información; generando también inconvenientes en el mantenimiento y administración de cada una de ellas por separado.

Este proyecto plantea la unificación de dichas “*redes*” en una sola, a fin de manejar la información de forma organizada, estructurada y segura. Para ello se plantea el desarrollo de un sistema de voz basado en la tecnología VoIP, ya que se desea tener una red que maneje tanto voz como datos y no redes independientes para cada servicio; para lo cual se debe considerar conceptos como calidad de servicio, de tal manera que la red no genere bloqueos y brinde el máximo provecho a los usuarios.

Otro de las consideraciones a tener cuenta es el diseño de un Sistema de Cableado Estructurado ya que actualmente la institución no cuenta con ello, siendo éste un factor del cual dependerá el correcto funcionamiento de la red, pudiendo evitar fallas, pérdidas de información y demás problemas.

La seguridad es otro de los temas que se debe manejar con sumo cuidado, ya que al momento no se maneja de manera adecuada, no se posee mecanismos de seguridad propios de una red de comunicaciones, tan solo se tienen instalados antivirus en las estaciones de trabajo, algunos de ellos ya desactualizados, y un normativo de uso de los laboratorios; por lo tanto, al momento de diseñar la red se debe tener en cuenta estas consideraciones para prevenir de ataques maliciosos a la institución.

El diseño de mecanismos de seguridad debe estar basado en estándares internacionales, de tal manera que la red esté protegida correctamente y como lo dicta las normas. Este proyecto propone generar políticas básicas de seguridad basadas en la dominios sugeridos por la norma ISO/ICE con su estándar 27002, las que deberán ser implementadas en el plantel para la protección de la red INTEGRADA de voz y datos a diseñar.

## CAPÍTULO 3

### DISEÑO DE LA RED INTEGRADA DE VOZ Y DATOS

#### 3.1 VISIÓN GENERAL

El diseño de la red INTEGRADA de voz y datos para la Unidad Educativa Temporal “Jaime Roldós Aguilera”, permitirá crear un sistema de comunicación integrado, centralizado, correctamente administrado, seguro, flexible, escalable y de bajo costo, en comparación a los sistemas tradicionales. Con esta solución se integrarán los servicios más utilizados dentro de una organización, voz y datos, posibilitando la comunicación interna de los departamentos de la institución, de manera sencilla y rápida, sin tener bloqueos o pérdida de información.

Las principales autoridades de la institución, han considerado necesario contar con varios servicios locales para mejorar su rol de educadores, entre los cuales se tiene: correo electrónico, servicios web y descargas de archivos, para lo cual se realizará un análisis a fin de elegir las herramientas idóneas para poder proveer estos servicios a la institución con una adecuada solución tanto técnica como económica.

Finalmente se ha pedido que dentro del proyecto se incluya el diseño de una red inalámbrica básica en los lugares de difícil acceso de la red cableada o desde sitios en los que el usuario no se encuentre fijo, y así permitir el acceso a la red desde equipos portátiles tales como: *Laptops, Tablets, Smartphones, etc.*

#### 3.2 MODELO DE RED [42]

La manera más eficiente de diseñar una LAN es realizarlo de manera jerárquica; este tipo de modelo permite flexibilidad y escalabilidad mucho mayor que otros modelos, facilitando así el diseño y administración de la red.

El diseño jerárquico divide la red en capas independientes, proporcionando a cada una de ellas tareas específicas dentro de la red, de manera que el diseño sea modular y mejore su rendimiento. El modelo jerárquico establecido por Cisco define tres capas: Acceso, Distribución y Núcleo.

La figura 3.1 muestra las capas existentes dentro del modelo jerárquico según Cisco.

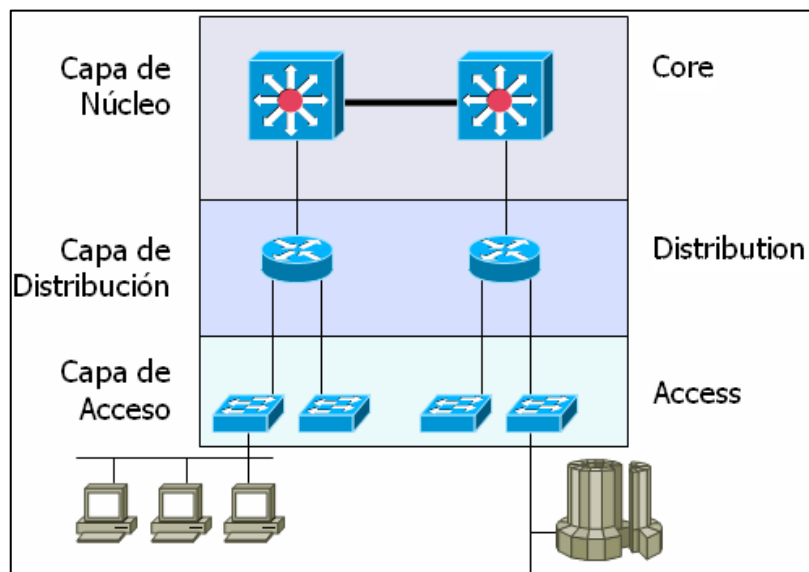


Figura 3. 1 Modelo jerárquico de una red

### 3.2.1 CAPA DE ACCESO

Es aquella que se encuentra del lado del cliente, es decir la que interactúa directamente con los dispositivos finales, como computadoras, teléfonos IP, impresoras, etc. Su principal función es la de aportar un medio y una técnica de conexión de los dispositivos a la red, además de controlar qué dispositivos pueden comunicarse en la red.

### 3.2.2 CAPA DE DISTRIBUCIÓN

La capa de Distribución representa el punto medio entre la capa de Acceso y los servicios principales de la red.

Es la capa encargada de la implementación de políticas de red, por ejemplo: ruteo, listas de acceso, filtrado de paquetes, cola de espera; se implementa la seguridad y políticas de red a través de “traducciones NAT<sup>30</sup> y *firewall*”, la redistribución entre protocolos de ruteo, ruteo entre VLANs y otras funciones de grupo de trabajo, así como la definición de dominios de *broadcast*<sup>31</sup> y *multicast*<sup>32</sup>.

### 3.2.3 CAPA NÚCLEO

La capa Núcleo del diseño jerárquico constituye el *backbone* de alta velocidad de la *internetwork*. Es esencial para la interconectividad entre los dispositivos de la capa de Distribución, por lo que es importante que el Núcleo sea sumamente disponible y redundante.

La función principal de la capa es conmutar tráfico tan rápido como sea posible y llevar grandes cantidades de datos de manera confiable y veloz, por lo que la latencia y la velocidad son factores importantes en esta capa.

Dentro de esta capa se debe evitar que se realicen tareas tales como: ruteo VLAN's, filtrado de paquetes, listas de accesos y otras tareas, que aumentarían la latencia de la capa.

## 3.3 TECNOLOGÍA DE RED

La tecnología a utilizar en el diseño de la red para la Unidad Educativa Temporal “Jaime Roldós Aguilera” deberá soportar una variedad de aplicaciones que demandan gran ancho de banda actualmente como en el futuro, tales como: navegación *WEB*, telefonía IP, video, e-learning entre otras. Además se debe tener en consideración la cantidad de usuarios que utilizarán la red.

---

<sup>30</sup> **NAT:** *Network Address Translation.*- Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

<sup>31</sup> **Broadcast:** *Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo del conjunto.*

<sup>32</sup> **Multicast:** *Envío de la información en una red a múltiples destinos simultáneamente.*



La selección de la tecnología de red también se encuentra ligada al dimensionamiento del tráfico a cursar por la red y que se presenta en el numeral 3.5.8; en base a estos parámetros se elegirá la tecnología Gigabit Ethernet para el diseño, a fin de cubrir todas las demandas actuales y las futuras mejoras que la misma podría ofrecer a la institución.

La tabla 3.1 muestra las tecnologías Ethernet existentes con sus respectivas características como son: tipo de cable, distancia máxima y velocidad de transmisión.

	<b>Velocidad</b>	<b>Longitud Segmento</b>	<b>Tipo Cable</b>
<b>10BaseF</b>	10 Mbps	2000 Metros	Fibra óptica
<b>10Base2</b>	10 Mbps	185 Metros	Cable coaxial
<b>10Base5</b>	10 Mbps	500 Metros	Cable coaxial
<b>10BaseT</b>	10 Mbps	100 Metros	Cable UTP
<b>100BaseT4</b>	100 Mbps	100 Metros	Cable UTP
<b>FastEthernet</b>	100 Mbps	100 Metros	Cable UTP y fibra óptica
<b>GigabitEthernet</b>	1000 Mbps	Cable: 100 Metros Fibra monomodo: 2 Kilómetros Fibra multimodo: 500 Metros	Fibra óptica y cable UTP
<b>10GBaseT</b>	10000 Mbps	100 Metros	Cable de par trenzado
<b>1000BaseSX</b>	1000 Mbps	550 Metros	Fibra óptica multimodo
<b>1000BaseLX</b>	1000 Mbps	5000 Metros	Fibra óptica monomodo

Tabla 3. 1 Tecnologías Ethernet [43]

### 3.4 TOPOLOGÍA DE RED

La topología de la red define la forma en que se encuentran conectados los equipos de conectividad, estaciones de trabajo y demás equipos dentro de la red.

Para el presente diseño se ha decidido que éste debe tener una topología en estrella extendida, debido a la distribución de los diferentes equipos a interconectarse, el tipo de aplicaciones a soportar, el crecimiento futuro, el presupuesto a ser utilizado y las recomendaciones de los estándares del Sistema de Cableado Estructurados antes mencionados.

Al hablar de topología estrella extendida se debe tomar en cuenta dos conceptos a utilizar como son el MDF (Punto de distribución Principal) y los IDF (Punto de distribución intermedio). Para este caso el MDF se ubicará en la Zona E; y es ahí donde convergen todos los demás IDF, es decir los cuartos de telecomunicaciones de las distintas zonas.

Cabe recalcar que para el diseño del Sistema de Cableado Estructurado se utilizará cable UTP categoría 6A para los enlaces de acceso, mientras que para el enlace de *backbone* se utilizará fibra óptica multimodo, debido a la extensión de la institución y para brindar un mejor rendimiento a la red.

En la figura 3.2 se muestra la topología propuesta para el diseño de la red, donde se puede apreciar los diferentes niveles jerárquicos que la red va a poseer, los tipos de medios de transmisión a utilizar, la ubicación de los cuartos de telecomunicaciones y los principales componentes de la red.

Así mismo es importante identificar las distancias existentes entre las diferentes zonas hacia el Laboratorio de Informática I (MDF) ubicado en la zona E donde se encontrará el cuarto de equipos como se detallará más adelante; en la figura 3.3 se observan las distancias entre los diferentes cuartos de telecomunicaciones al cuarto de equipos.

Una vez determinada la tecnología, topología y el modelo de la red se procede a realizar el diseño de la misma, para lo cual se ha dividido el diseño en dos partes: diseño de la red pasiva y diseño de la red activa.

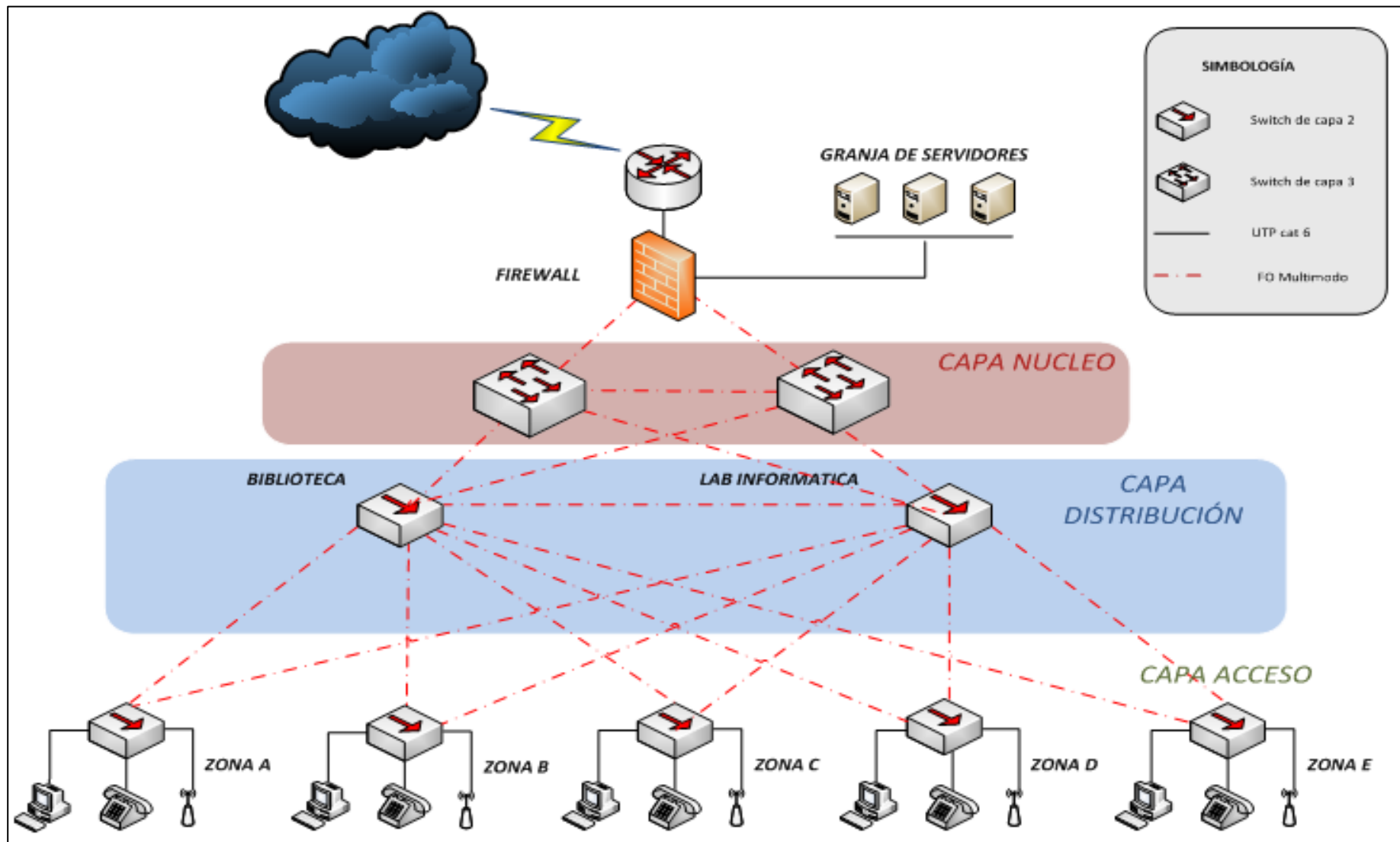


Figura 3. 2 Topología de la red a diseñar

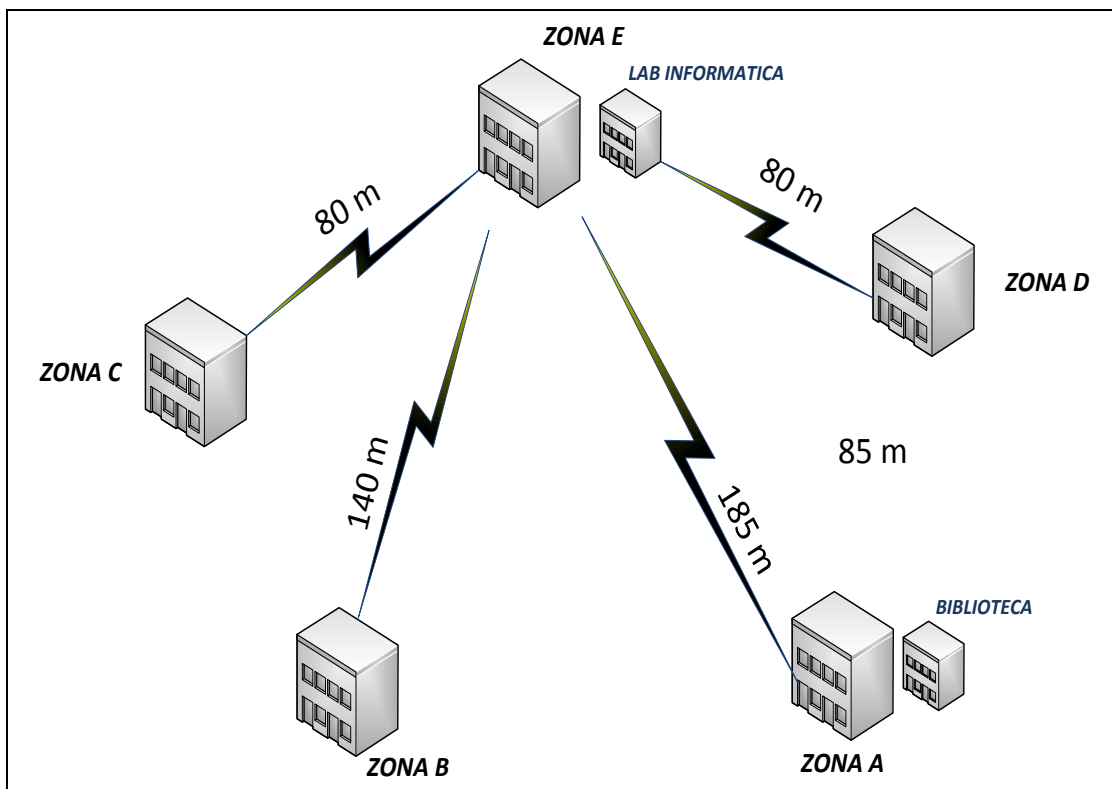


Figura 3. 3 Distancias hacia el cuarto de equipos

### 3.5 DISEÑO DE LA RED PASIVA

El diseño de la red pasiva considera la estructura que va soportar la red en sí, es decir, todos aquellos componentes que intervienen en la transmisión de datos pero sin generarlos, modificarlos o cambiarlos al momento de cruzar por ella, pero que son necesarios para su transmisión.

#### 3.5.1 DISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO

La Unidad Educativa Temporal “Jaime Roldós Aguilera” requiere del diseño de un Sistema de Cableado Estructurado que pueda brindar el soporte adecuado a la red INTEGRADA a diseñar, para esto se deben considerar los puntos de red y su correspondiente ubicación que se requerirán para satisfacer las necesidades dentro de la institución.

### 3.5.1.1 Distribución de los Puntos de Red

Como se detalló en el capítulo anterior, la Unidad Educativa Temporal “Jaime Roldós Aguilera” se ha dividido en zonas con el propósito de hacer más fácil su diseño; en cada una de estas zonas se ubicará un cuarto de telecomunicaciones para brindar el servicio a los departamentos cercanos y así cumplir la recomendación de la norma EIA/TIA 568-C donde dice que la distancia máxima del cableado horizontal no debe superar los 90 metros.

Para empezar el diseño del SCE se debe conocer el número de puntos de red dentro de la institución, su ubicación y la función a que están destinados cada uno de ellos; además como consideración del diseño se tomará en cuenta un crecimiento del 30% en cada zona, con el propósito de que existan los suficientes puertos y espacios para el cableado estructurado futuro al menos en un periodo de 10 años, sin tener que realizar cambios en el sistema por adiciones de usuarios, cambios de ubicaciones, etc.

En la zona A, se encuentran el Rectorado, Vicerrectorado, Secretaría General, Colecturía, Contabilidad, Biblioteca, Orientación Vocacional y Departamento Médico.

La tabla 3.2 muestra la distribución de puntos de datos y voz que se va a diseñar para la Zona A.

En la Zona B se ubican 16 aulas correspondientes a los sextos cursos y un laboratorio de PLC's digitales. Se ha decidido que las aulas tengan un punto de acceso a la red. El detalle de los puntos antes mencionados se lo puede apreciar de mejor manera en la tabla 3.3.

La Zona C está conformada por Inspección General, Sala de Profesores, Departamento de Electricidad, Departamento de Música, y 16 aulas. En la tabla 3.4 se detallan los puntos para esta Zona.

	Área de Trabajo	Puntos de Datos	Puntos de Voz	Total
<b>ZONA A</b>	<i>Rectorado</i>	2	2	4
	<i>Vicerrectorado</i>	2	2	4
	<i>Secretaría General</i>	2	2	4
	<i>Colecturía</i>	1	1	2
	<i>Contabilidad</i>	1	1	2
	<i>Biblioteca</i>	12	2	14
	<i>Orientación Vocacional</i>	2	2	4
	<i>Departamento Médico</i>	2	2	4
	<i>Aulas</i>	8	0	8
<b>Sub-Total</b>		32	14	46
<b>30 % de crecimiento</b>		10	4	14
<b>Total</b>		<b>42</b>	<b>18</b>	<b>60</b>

Tabla 3. 2 Distribución de los puntos Zona A

	Área de Trabajo	Puntos de Datos	Puntos de Voz	Total
<b>ZONA B</b>	<i>Aulas</i>	16	0	16
	<i>Laboratorio PLC</i>	11	1	12
<b>Sub-Total</b>		27	1	28
<b>30 % de crecimiento</b>		9	1	10
<b>Total</b>		<b>36</b>	<b>2</b>	<b>38</b>

Tabla 3. 3 Distribución de los Puntos Zona B

La Zona D está conformada por 16 aulas, el Departamento de Mecánica y Salón Audiovisual como se muestra en la tabla 3.5.

La Zona E abarca los laboratorios de Informática y Mecánica, así como seis aulas para impartir clases. En la tabla 3.6 se detallan los puntos de red antes mencionados.

La zona F que está conformada por el parqueadero y el bar de la institución no será contemplada dentro de la red cableada; sin embargo la misma será considerada dentro del diseño de la red inalámbrica para que sus usuarios tengan acceso a la red.

	Área de Trabajo	Puntos de Datos	Puntos de Voz	Total
<b>ZONA C</b>	<i>Inspección General</i>	4	2	6
	<i>Sala de Profesores</i>	8	2	10
	<i>Departamento de Electricidad</i>	3	3	6
	<i>Departamento de Música</i>	1	1	2
	<i>Aulas</i>	16	0	16
<b>Sub-Total</b>		32	8	40
<b>30 % de crecimiento</b>		10	2	12
<b>Total</b>		<b>42</b>	<b>10</b>	<b>52</b>

Tabla 3. 4 Distribución de los puntos Zona C

	Área de Trabajo	Puntos de Datos	Puntos de Voz	Total
<b>ZONA D</b>	<i>Departamento de Mecánica</i>	1	1	2
	<i>Salón Audiovisual</i>	5	1	6
	<i>Aulas</i>	8	0	8
<b>Sub-Total</b>		14	2	16
<b>30% de Crecimiento</b>		4	1	5
<b>Total</b>		<b>18</b>	<b>3</b>	<b>21</b>

Tabla 3. 5 Distribución de los puntos Zona D

	Área de Trabajo	Puntos de Datos	Puntos de Voz	Total
<b>ZONA E</b>	<i>Lab. Informática I</i>	25	1	26
	<i>Lab. Informática II</i>	25	1	26
	<i>Lab. Mecánica</i>	11	1	12
	<i>Aulas</i>	10	0	10
<b>Sub-Total</b>		71	3	74
<b>30% de Crecimiento</b>		21	1	22
<b>Total</b>		<b>92</b>	<b>4</b>	<b>96</b>

Tabla 3. 6 Distribución de los puntos Zona E

### 3.5.2 DISEÑO DEL SUBSISTEMA DE CABLEADO HORIZONTAL

El diseño debe ir acorde a la distribución arquitectónica de la institución, En el Anexo A se detalla la distribución de los puntos de voz y datos, en los planos correspondientes a la Unidad Educativa Temporal “Jaime Roldós Aguilera”.

El diseño del cableado estructurado debe dar cabida a aplicaciones de distinta índole como son: transmisión de datos, telefonía IP, interconexión con LAN de alta velocidad, y redes WAN. Por esta razón se ha optado por el uso de cable UTP, categoría 6A, de 4 pares con sus respectivos conectores RJ45, como lo dicta la norma TIA/EIA 568-C.

Si bien las aplicaciones que se utilizan dentro de la institución no son todas las antes nombradas, es necesario que el diseño tome en cuenta todas ellas, de tal manera que el SCE tenga un tiempo de vida útil al menos de 10 años sin tener necesidad de rediseñarlo para el soporte de nuevas aplicaciones.

Las características del cable UTP categoría 6A, están definidas en el estándar TIA/EIA 568-C.2, donde se definen parámetros mecánicos, eléctricos y de transmisión.

*La norma dice:*

“Cable UTP, Categoría 6A: Aplica a cables UTP de 100  $\Omega$  y sus componentes de conexión, es totalmente compatible con cables UTP categorías 6, 5, 5e y 3 respectivamente. Alcanza frecuencias de hasta 500 MHz en cada par y una velocidad de 10 Gbps a 100 metros”. [44]

La figura 3.4 muestra la composición de un cable UTP categoría 6A.

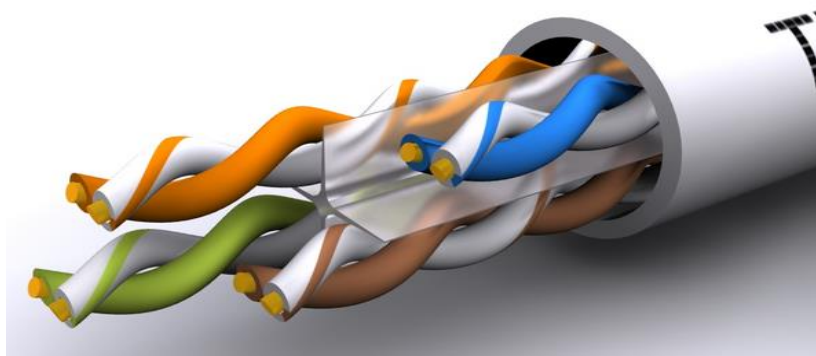


Figura 3. 4 Cable UTP Categoría 6A, corte transversal [44].



Mediante el plano arquitectónico se realizará el cálculo de las longitudes que se necesita para llegar a las estaciones de trabajo desde sus respectivos cuartos de telecomunicaciones. Cabe señalar que para el cálculo se tomará en cuenta la holgura de terminación y de error, de 2.5 metros y 10 % respectivamente.

En las tablas 3.7 a 3.11 se puede apreciar la cantidad de cable UTP que se necesitan para cada zona, en base a la cantidad de puntos que cada una posee y a las distancias establecidas en el Anexo A.

Una vez encontrada la longitud necesaria para cada zona se determinará la cantidad de cable total para el subsistema de cableado horizontal de la Unidad Educativa Temporal “Jaime Roldós Aguilera”, como se detalla en la tabla 3.12.

	Área de Trabajo	Puntos de Red	Longitud (metros)
<b>ZONA A</b>	<i>Rectorado</i>	4	104
	<i>Vicerrectorado</i>	4	14
	<i>Secretaría General</i>	4	91
	<i>Colecturía</i>	2	39
	<i>Contabilidad</i>	2	36
	<i>Biblioteca</i>	14	65
	<i>Orientación Vocacional</i>	4	24
	<i>Departamento Médico</i>	4	22
	<i>Aulas</i>	8	160
<b>Sub-Total</b>		46	555
<b>Holgura</b>			170
<b>Total</b>			<b>725</b>

Tabla 3. 7 Longitudes para el Cableado Horizontal Zona A

	Área de Trabajo	Puntos de Red	Longitud (metros)
<b>ZONA B</b>	Aulas	16	684
	Laboratorio PLC	12	65
<b>Sub-Total</b>		28	749
<b>Holgura</b>			143
<b>Total</b>			<b>892</b>

Tabla 3. 8 Longitudes para el Cableado Horizontal Zona B

	Área de Trabajo	Puntos de Red	Longitud (metros)
<b>ZONA C</b>	<i>Inspección General</i>	6	122
	<i>Sala de Profesores</i>	10	246
	<i>Departamento de Electricidad</i>	4	36
	<i>Departamento de Música</i>	2	4
	<i>Aulas</i>	16	352
<b>Sub-Total</b>		38	760
<b>Holgura</b>			171
<b>Total</b>			<b>931</b>

Tabla 3. 9 Longitudes para el Cableado Horizontal Zona C

	Área de Trabajo	Puntos de Red	Longitud (metros)
<b>ZONA D</b>	<i>Departamento de Mecánica</i>	2	25
	<i>Salón Audiovisual</i>	6	58
	<i>Aulas</i>	8	320
<b>Sub-Total</b>		16	403
<b>Holgura</b>			80
<b>Total</b>			<b>483</b>

Tabla 3. 10 Longitudes para el Cableado Horizontal Zona D

	Área de Trabajo	Puntos de Red	Longitud (metros)
<b>ZONA E</b>	<i>Lab Informática I</i>	26	414
	<i>Lab Informática II</i>	26	682
	<i>Lab Mecánica</i>	12	302
	<i>Aulas</i>	10	256
<b>Sub-Total</b>		74	1654
<b>Holgura</b>			350
<b>Total</b>			<b>2004</b>

Tabla 3. 11 Longitudes para el Cableado Horizontal Zona E

Cabe señalar que para el cálculo de la longitud de UTP necesario en cada una de las zonas se tomó en cuenta una holgura de terminación y de error, de 2.5 metros y 10% de error respectivamente. En base a la tabla 3.12 y conociendo que cada rollo de cable UTP es de 305 metros longitud se determina que son necesarios 17 rollos para el diseño del sistema de cableado horizontal.

	Zona	Longitud (metros)
JRA	A	725
	B	892
	C	931
	D	483
	E	2004
<b>TOTAL</b>		<b>5035</b>

Tabla 3. 12 Longitud Total de UTP para la UET "JRA"

### 3.5.2.1 Rutas para el Cableado Horizontal

Se tienen varias formas por la cual el cable UTP puede ser enrutado hacia el cuarto de telecomunicaciones.

La norma TIA/EIA indica claramente cómo se lo puede hacer y cuáles son los elementos que los componen, además define que la distancia máxima es de 90 metros y que en conjunto con los *patch cords* puede llegar a 100 metros.

La tabla 3.13 muestra las alternativas que existen para realizar el cableado horizontal dentro de la institución.

<b>Vías para enrutar el Cableado Horizontal (ANSI/TIA/EIA 569-A)</b>
Sistemas Bajo Suelo
Sistemas de Piso Removible
Tubos metálicos Conduit o PVC
Ductos y Canaletas
Sistemas de Cielo Falso

Tabla 3. 13 Rutas Estandarizadas para el Cableado Horizontal [39]

El presente diseño sugerirá que las conexiones desde cada punto de red hacia el cuarto de telecomunicaciones sea mediante el uso de canaletas decorativas, para interiores, mientras que para exteriores se utilizará tubo *conduit*, y esto debe ir acorde a las consideraciones de la norma 569A.

Para la selección de las canaletas se debe conocer cuántos cables UTP van a pasar por la misma, considerando una holgura del 40% como lo dicta la norma; como ejemplo de cálculo se tomará en cuenta una canaleta de 60x40 mm.

Se conoce que el diámetro del cable UTP categoría 6A es de 9 mm y que la canaleta posee 2400 mm<sup>2</sup> de área, de la cual, en base a la norma se podrá hacer uso de 1440 mm<sup>2</sup>. Con esto se determina que dentro de una canaleta de 60x40, caben 17 cables UTP categoría 6A. Además es importante señalar que la longitud estandarizada para las canaletas decorativas es de 2 m de longitud.

La ecuación 3.1 muestra cómo se obtuvo el valor antes indicado.

$$UTP \times Can_{60 \times 40} = \frac{\text{Área utilizable Canaleta}}{\text{Área Cable UTP}} = \frac{2400 \text{ mm}^2 * 60\% \text{ de uso}}{81 \text{ mm}^2} = 17 \frac{utp}{canaleta}$$

Ecuación 3. 1 Cálculo del número de UTP por canaleta

Realizando el mismo proceso y en base a la cantidad de cables que cursarán por las canaletas en las distintas zonas, se determinó la tabla 3.14 que muestra la capacidad de almacenamiento de cable UTP en cada canaleta.

Elemento	Cantidad de UTP soportados
Canaleta 60 x 40 mm	17 Cables
Canaleta 40 x 40 mm	11 Cables
Canaleta 40 x 22 mm	6 Cables
Canaleta 32 x 12 mm	2 Cables

Tabla 3. 14 Capacidad de UTPs por canaleta

### 3.5.2.2 Accesorios para el Cableado Horizontal

Con la información antes mostrada y con la distribución de los puntos del numeral 3.5.1.1 se procede a determinar la lista de elementos que se necesitan para el subsistema de cableado horizontal en cada una de las zonas.

En la tabla 3.15 se puede apreciar los elementos necesarios para el subsistema de cableado horizontal y la cantidad necesaria para cada zona de la Institución.

ACCESORIOS REQUERIDOS POR ZONA					
DESCRIPCIÓN	CANTIDAD				
	ZONA A	ZONA B	ZONA C	ZONA D	ZONA E
<b>Canaleta Plástica 60x40 mm</b>	4	-	9	-	115
<b>Canaleta Plástica 40x40 mm</b>	7	5	-	-	-
<b>Canaleta Plástica 40x22 mm</b>	22	9	32	37	14
<b>Canaleta Plástica 32x12 mm</b>	9	2	4	9	4
<b>Ángulo Interno 60x40 mm</b>	1	-	1	-	4
<b>Ángulo Interno 40x40 mm</b>	1	-	-	-	-
<b>Ángulo Interno 40x22 mm</b>	1	-	7	1	1
<b>Ángulo Interno 32x12 mm</b>	1	-	-	3	-
<b>Derivación T 60x40 mm</b>	6	-	5	-	52
<b>Derivación T 40x40 mm</b>	-	9	-	-	-
<b>Derivación T 40x22 mm</b>	3	12	1	13	5
<b>Derivación T 32x12 mm</b>	-	-	-	-	1
<b>Jack Categoría 6 A</b>	46	28	40	24	74
<b>Face Plate Doble</b>	19	1	12	4	7
<b>Face Plate Simple</b>	8	26	16	16	60
<b>Patch Cord Cat 6A 3 ft</b>	46	28	40	24	74
<b>Tubo Conduit EMT</b>	-	2	1	1	6
<b>Patch Panel 24 puertos</b>	2	2	2	1	4

Tabla 3. 15 Elementos para el cableado horizontal por zona

“Cabe recalcar que la cantidad de elementos detallados no están sujetos a ningún tipo de fallo o imprevisto, por lo cual se recomienda que si la institución desea realizar la compra de materiales, estimar un margen de error de al menos 10%, y se puede elegir libremente la marca a utilizar tomando en cuenta que se cumplan las características técnicas antes mencionadas.”

### 3.5.3 DISEÑO DEL SUBSISTEMA DE CABLEADO VERTICAL

El subsistema de cableado vertical de la Unidad Educativa Temporal “Jaime Roldós Aguilera” es aquel que proveerá la interconexión entre las distintas zonas descritas en el capítulo 2.

Debido a que entre ellas existe una distancia mayor a la admitida por el estándar, para el diseño de este subsistema se ha optado por el uso de fibra óptica multimodo 62.5/125  $\mu\text{m}$  la cual para cableado de *backbone* soporta hasta una longitud máxima de 2000 m.

Si bien este medio de transmisión es de mayor costo que el par trenzado, su inclusión dentro del proyecto está justificada por la flexibilidad y el gran ancho de banda que proporciona, lo que resulta ideal para las aplicaciones que la institución proveerá y el crecimiento futuro que puede tener.

No se debe olvidar que al momento de diseñar este subsistema se deben seguir las recomendaciones establecidas en el estándar EIA/TIA 568C- 3 para la instalación de fibra óptica en sistemas de cableado *backbone*.

En la tabla 3.16 se observa las distancias que necesita cada zona para llegar al MDF y que será cubierto por fibra óptica.

ZONA	LONGITUD (metros)
A-E	185 m
B-E	140 m
C-E	80 m
D-E	80 m
<b>TOTAL</b>	<b>485 m</b>

Tabla 3. 16 Distancias entre los cuartos de telecomunicaciones al MDF

### 3.5.4 DISEÑO DEL SUBSISTEMA ÁREA DE TRABAJO

El área de trabajo está conformada generalmente por una computadora y/o teléfono IP, los cuales pueden estar conectados a cada punto de red; para ello se deben instalar *faceplates* dobles, tanto para voz como datos, dichos *faceplates* deben estar ubicados a 50 cm del nivel del piso.

Cada dispositivo será conectado a los diferentes puntos de red, mediante *patchcords* RJ45 tal como lo establece la norma TIA/EIA 568-C; éstos deben ser elaborados en fábrica con cables UTP de la misma categoría utilizados para el subsistema de cableado horizontal, es decir cable UTP, categoría 6A, y la terminación de los mismos deben ser apegados a la norma, T568B.

Cabe señalar que los *patchcords* deben ser elaborados en fábrica y estar debidamente certificados, además de ser flexibles por el uso que los mismos tendrán dentro del área de trabajo.

### 3.5.5 DISEÑO DEL SUBSISTEMA CUARTO DE TELECOMUNICACIONES

El cuarto de telecomunicaciones es aquella área exclusiva dentro del edificio para los equipos de telecomunicaciones; su función principal es la distribución e interconexión del cableado y la terminación mecánica. [45]

Debido a la gran extensión de la institución se debe considerar varios cuartos de telecomunicaciones, de tal manera que los mismos puedan proveer a los usuarios conectividad sin exceder los 100 metros, incluidos los respectivos *patchcords* establecido en la norma EIA/TIA 568-C.

Todos los cuartos de telecomunicaciones de la institución deberán converger en la Sala de Equipos, que se ubicará en el Laboratorio de Informática I en la Zona E. En la tabla 3.17 se lista la ubicación de los diferentes cuartos de telecomunicaciones.

Zona	Ubicación
A	Biblioteca General
B	Laboratorio de PCI Digitales
C	Departamento de Música
D	Salón Audiovisual
E	Laboratorio de Informática I

Tabla 3. 17 Distribución de los Cuartos de Telecomunicaciones

Entre las consideraciones a tomarse en cuenta para un cuarto de telecomunicaciones se tienen las siguientes [46]:

- Únicamente debe ser para equipos de telecomunicaciones
- Las dimensiones del cuarto de telecomunicaciones varía de acuerdo al área a servir como se lo puede apreciar en la tabla 3.18.
- Su temperatura ambiente debe estar entre los 18 – 24 °C y humedad entre el 30% y el 50%.
- Las puertas tendrán un tamaño mínimo de 0.86 m x 1.9 m abriéndola hacia fuera.
- Altura mínima piso-techo 2.6 m.
- Mínimo dos tomas de corriente AC de 110 V y 15 A cada uno con circuitos independientes.

ÁREA	DIMENSIONES	EQUIPOS POR ÁREA
500 m <sup>2</sup>	3 m x 2.2 m	50
800 m <sup>2</sup>	3 m x 2.8 m	80
1000 m <sup>2</sup>	3 m x 3.4 m	100

Tabla 3. 18 Dimensiones estandarizadas para cuartos de telecomunicaciones

Tomando en cuenta la recomendación del área a servir se ha decidido que el cuarto de telecomunicaciones perteneciente a la Zona E, al tener el mayor número de equipos a servir, 74 en total, contará con todas las especificaciones de la norma.



Este cuarto de telecomunicaciones tendrá las dimensiones establecidas en el estándar, 3 m x 2.2 m, y se constituirá el punto central de conexión (MDF) de los demás cuartos de telecomunicaciones.

Para los demás cuartos de telecomunicaciones, debido a la infraestructura de la institución y el espacio que se posee, se determinará el lugar idóneo para ubicar los gabinetes necesarios, sin olvidar la seguridad y el correcto almacenamiento que deben tener los mismos.

Para el presente diseño se deben adquirir un *rack*<sup>33</sup> y cuatro gabinetes para los respectivos cuartos de telecomunicaciones que se va a tener dentro de la institución.

#### 3.5.5.1 Selección de los *Rack*'s

Para la selección de los *racks* de los cuartos de telecomunicaciones se debe conocer la cantidad de equipos a la cual se dará cabida en el mismo, es por ello que se debe determina la cantidad exacta de equipos que va a poseer cada uno de los *racks* de cada zona respectivamente.

La tabla 3.19 muestra el número de equipos por cada zona.

Ubicación	Switch 24 puertos	Servidores	Total
Zona A	3	0	3
Zona B	2	0	2
Zona C	2	0	2
Zona D	1	0	1
Zona E	4	3	7

Tabla 3. 19 Números de equipos a almacenar en los *Racks*

<sup>33</sup> **Rack:** Es un armario o estantería destinada a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas (un ancho de 19 pulgadas) para que sea compatible con el equipamiento de cualquier fabricante.

### 3.5.5.1.1 Rack Principal

El *rack* principal es aquel que se ubicará en la zona E, en el laboratorio de Informática I, ya que es éste el cuarto de telecomunicaciones que albergará la mayor cantidad de equipos. La tabla 3.20 muestra el detalle de los equipos a los que se debe dar cabida en el *rack* principal.

DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
<i>Patch panel FO</i>	1	1
<i>Switch 24 puertos</i>	4	4
<i>Patch Panel</i>	4	4
<b>Organizadores Horizontales</b>	4 (2UR)	8
<b>Monitor</b>	1	2
<b>Servidores</b>	3	3
<b>Multitomas Horizontales</b>	2	2
<b>Total</b>		24

Tabla 3. 20 Dimensionamiento Rack Principal

En base al detalle presentado se ubicará un *rack* cerrado de 24 UR y 19 pulgadas, que brindará cabida a los equipos antes mencionados. La figura 3.5 muestra un ejemplo del *rack* de 24 UR que se necesita.



Figura 3. 5 Rack de 24 UR

## 3.5.5.1.2 Gabinetes

Para las demás zonas de la institución se tendrán gabinetes que alojarán los equipos activos y elementos pasivos de la red. Se debe considerar para el cálculo de del tamaño de los gabinetes que si bien la mayoría de los equipos miden 1 UR, los organizadores horizontales pueden medir 1 ó 2 UR. En la tabla 3.21 se indica el tamaño de los gabinetes cerrados que se necesitan para las distintas zonas.

ZONA	DESCRIPCIÓN	CANTIDAD	TAMAÑO (UR)
ZONA A	<i>Patch panel FO</i>	1	1
	Organizadores Horizontal	2	4
	<i>Switch de 24 puertos</i>	3	3
	<i>Patch Panel 12 puertos</i>	3	3
	Multitomas Horizontales	1	1
	<b>Total</b>		<b>12</b>
ZONA B	<i>Patch panel FO</i>	1	1
	Organizadores Horizontal	2	4
	<i>Switch de 24 puertos</i>	2	2
	<i>Patch Panel 24 puertos</i>	2	2
	Multitomas Horizontales	1	1
	<b>Total</b>		<b>10</b>
ZONA C	<i>Patch panel FO</i>	1	1
	Organizadores Horizontal	2	4
	<i>Switch de 24 puertos</i>	2	2
	<i>Patch Panel 24 puertos</i>	2	2
	Multitomas Horizontales	1	1
	<b>Total</b>		<b>10</b>
ZONA D	<i>Patch panel FO</i>	1	1
	Organizadores Horizontal	2	4
	<i>Switch de 24 puertos</i>	1	1
	<i>Patch Panel 24 puertos</i>	1	1
	Multitomas Horizontales	1	1
	<b>Total</b>		<b>8</b>

Tabla 3. 21 Dimensionamiento de Gabinetes de Comunicaciones

### 3.5.6 DISEÑO DEL SUBSISTEMA SALA DE EQUIPOS [47]

El cuarto de equipos es un espacio centralizado para los equipos de telecomunicaciones a utilizar por los ocupantes del edificio. Únicamente debe guardar equipos directamente relacionados con el sistema de telecomunicaciones y sus sistemas de soporte. La norma que estandariza este subsistema es la EIA/TIA 569.

Entre los equipos y elementos que pueden encontrarse dentro de la sala de equipos se tienen:

- El armario de distribución principal MDF
- Servidores de Red y/o Computadores Centrales
- Centrales Telefónicas
- Consolas de circuitos cerrados de TV, etc.

Este subsistema debe cubrir varias recomendaciones, de tal manera que su funcionamiento sea el idóneo, entre las principales se pueden mencionar.

- Debe estar conectado al enrutamiento vertical
- Mantener la temperatura entre 18° y 27° C.
- Debe ser diseñado como un mínimo de 14 m<sup>2</sup>
- La altura mínima debe ser de 2.44 metros
- Iluminación, 500 Lx<sup>34</sup> a 1

“Aun sabiendo cuáles son las consideraciones necesarias para un buen sistema de cableado, la infraestructura de la institución no permite establecer para cada subsistema el espacio definido en las normas, por lo que se ha considerado que un cuarto de telecomunicaciones, la sala de equipos y acometida de entrada de servicios, se ubicarán en la misma ubicación física, es decir en la Zona E, en el Laboratorio de Informática I”

---

<sup>34</sup> **Lux:** Es la incidencia perpendicular de un lumen en una superficie de 1 metro cuadrado. Equivale a 0.0929 lúmenes.

### 3.5.7 ADMINISTRACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO

Está regida por el estándar EIA/TIA 606-A, la cual dicta parámetros para la correcta administración del sistema de cableado estructurado. La aplicación de esta norma permitirá que el manejo de la red sea mucho más sencillo, permitiendo flexibilidad y escalabilidad sin requerimientos de cambios en el sistema existente; también es indispensable para poder obtener una certificación, lo cual garantiza el correcto funcionamiento de red al menos por 10 años.

Para proveer un esquema de información sobre la administración del cableado de telecomunicaciones, espacios y medios independientes, se desarrolló un código de color para el etiquetado para su debida identificación como se muestra en la tabla 3.22.

COLOR	DESCRIPCIÓN
NARANJA	Terminación central de oficina
VERDE	Conexión de red lado del cliente
PÚRPURA	Conexión mayor
BLANCO	<i>Backbone</i> primer nivel
GRIS	<i>Backbone</i> segundo nivel
AZUL	Terminación de cable horizontal
CAFÉ	<i>Backbone</i> entre edificios
AMARILLO	Mantenimiento auxiliar
ROJO	Sistema de teléfono

Tabla 3. 22 Código de Colores para el SCE [48]

#### 3.5.7.1 Etiquetado

El etiquetado es una herramienta muy útil dentro de la administración del SCE, ya que gracias a esto se pueden identificar los diferentes dispositivos, puntos de red y elementos del cableado; está definido dentro de la norma EIA/TIA 606-A y especifica que el etiquetado debe realizarse en las terminaciones de los cables, en los *faceplates* y en los *patch panel* del cuarto de telecomunicaciones. [10]

La forma de etiquetar debe ser lo más clara posible, de tal manera, que si se desea saber el lugar al que pertenece un elemento del SCE no exista inconveniente; para esto se debe identificar cada elemento mediante el área donde se encuentra, el tipo de servicio que provee y al *faceplate* o *patch panel* al cual debe ir conectado.

Dentro de la institución se ha decidido diferenciar los diferentes servicios en los *faceplates* dobles de la siguiente manera, la salida izquierda será identificada para servicio de voz, esto como una forma de estándar interno; además tendrá su respectivo adhesivo con la figura de un teléfono para mayor facilidad de distinción, mientras que la salida de datos será la derecha, la cual contará con un identificativo de una computadora.

No obstante, esta señalización no indica que los puntos no puedan dar ambos servicios indistintamente, si en algún caso el usuario necesitara otro puerto para voz y/o datos lo puede ocupar sin inconveniente alguno.

Una forma de etiquetar puede ser la mostrada en la figura 3.6

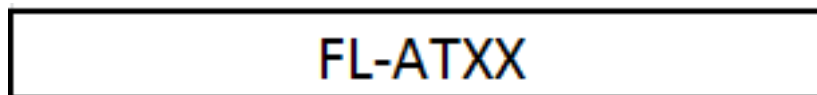


Figura 3. 6 Nomenclatura para el Etiquetado.

Dónde:

FL= El lugar donde se encuentra el cuarto de telecomunicaciones

A = 1 o 2 letras que identifiquen el *Patch Panel*

T = Tipo de Servicio, D si es datos y V si es voz.

XX= Puerto del Panel

Para poder distinguir a qué cuarto de telecomunicaciones llegarán los diferentes puntos de red, dentro de la institución se ha determinado la nomenclatura que muestra la tabla 3.23.

CUARTOS DE TELECOMUNICACIONES		
Zona	Ubicación	Nomenclatura
A	Biblioteca General	B
B	Laboratorio PCI Digitales	D
C	Departamento de Música	M
D	Salón Audiovisual	A
E	Laboratorio de Informática I	I

Tabla 3. 23 Nomenclatura de los Cuartos de Telecomunicaciones

Un ejemplo de esta forma de etiquetado se muestra en la figura 3.7.

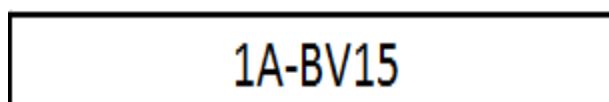


Figura 3. 7 Ejemplo de Etiquetado en el Unidad Educativa Temporal “Jaime Roldós Aguilera”

De acuerdo a la información mostrada se puede decir que esta etiqueta indica lo siguiente, el cuarto de telecomunicaciones al cual pertenece es el de la zona D, que se encuentra en la Salón Audiovisual, y está conectado al *patch panel B*, el servicio que ofrece es de voz, y que se encuentra conectado en el puerto número 15.

Éste será el esquema de etiquetado que se manejará dentro de la Unidad Educativa Temporal “Jaime Roldós Aguilera”, para poder distinguir los diferentes dispositivos, y conexiones que se utilizarán para el SCE.

Una vez realizado esto, se recomienda a la institución contratar los servicios de una empresa certificadora de cableado estructurado, al fin de garantizar que el SCE cumpla con los requerimientos mínimos establecidos por los estándares EIA/TIA.

El etiquetado completo de todos los puntos de red se lo puede apreciar de mejor manera en el Anexo B.

### 3.5.8 DIMENSIONAMIENTO DEL TRÁFICO DE LA RED

Como se estableció en el capítulo anterior, actualmente la Unidad Educativa Temporal “Jaime Roldós Aguilera” no cuenta con una red debidamente diseñada para su comunicación; es así que se debe realizar el dimensionamiento de tráfico para el diseño de la misma.

Para este diseño se deben considerar los servicios que va a ofrecer la red, tales como, descarga de archivos, acceso a la web, acceso a la base de datos, correo electrónico, VoIP, y los servicios mencionados anteriormente.

Es importante explicar y con el fin de no causar confusiones, que la **capacidad de transmisión** comercialmente se denomina ancho de banda, término obviamente mal utilizado, pero muchas veces más fácil de entender para el usuario promedio.

#### 3.5.8.1 Cálculo del Ancho de Banda Correo Electrónico

La Unidad Educativa Temporal “Jaime Roldós Aguilera” al ser una entidad educativa, debe contar con un servicio de correo electrónico, con la finalidad de que mediante este servicio pueda hacer conocer a autoridades, estudiantes y padres de familias, de eventos a realizarse en la institución como son: sesiones, entregas de boletines y demás avisos importantes.

Una de los inconvenientes al momento de realizar el cálculo de ancho de banda de un correo electrónico es determinar el valor promedio de un *mail*; según fuentes de la Escuela de Gestión de la Información, Berkeley, dice:

*"Alrededor de 31 millones de correos electrónicos son enviados cada día, en Internet, una cifra que se espera que se duplique para 2006 (fuente: International Data Corporation (IDC). El email media es de unos 59 kilobytes de tamaño, con lo que el flujo anual correos electrónicos en todo el mundo es de 667.585 terabytes". [49]*



Como se puede apreciar este artículo se refiere al año 2006, lo que indica que hoy en día, el tamaño promedio de un *e-mail* sería aún mayor; sin embargo, cabe recalcar que este valor es variable de acuerdo al tipo de información que se envíe; es decir, su valor dependerá de si se envía solo texto, imágenes, o si se envía algún archivo adjunto.

Para el presente diseño se ha considerado un valor promedio de e-mail de 250 KB, ya que la mayoría de correos que se utilizan dentro de la institución son de carácter informativo y poseen imágenes dentro de su formato; de igual manera se estableció que en una hora se revisan en promedio ocho e-mail, con lo cual se puede calcular el ancho de banda necesario para dicho servicio.

$$AB \text{ mail} = \frac{250 \text{ Kb}}{1 \text{ mail}} \times \frac{8 \text{ mail}}{1 \text{ hora}} \times \frac{1 \text{ hora}}{3600 \text{ seg}} \times \frac{8 \text{ bits}}{1 \text{ byte}} = 4.4 \text{ Kbps}$$

**Ecuación 3. 2 Ancho de Banda para Correo Electrónico**

### **3.5.8.2 Cálculo del Ancho de Banda de Acceso a la Web**

Acceder al Internet es uno de los servicios con frecuencia más utilizado dentro de cualquier entidad, y sucede lo mismo para la institución. En base a encuestas se pudo determinar entre las páginas web más utilizadas, se encuentran: páginas gubernamentales, informativas, y sociales; al ser un servicio en tiempo real se debe tener un tiempo de respuesta aceptable en el despliegue de la información el cual en éste proyecto es de 30 segundos para cargar una página.

Para determinar el tamaño promedio de una página web se ha utilizado la herramienta *Web Side Speed Test* que indica el tamaño de una página web al ingresar la url de la misma. Gracias a esta herramienta y tomando en consideración las páginas de mayor interés para la institución, se determina que el tamaño promedio a considerar en el diseño es de 350 KB por página web. [50]

La ecuación 3.3 muestra el ancho de banda necesario para acceso a la *web*.

$$AB_{web} = \frac{350 \text{ KB}}{1 \text{ página}} \times \frac{1 \text{ página}}{30 \text{ seg}} \times \frac{8 \text{ bits}}{1 \text{ byte}} = 93.3 \text{ Kbps}$$

**Ecuación 3. 3 Ancho de Banda de la red cableada para acceso a la Web**

### 3.5.8.3 Cálculo del Ancho de Banda de acceso a Base de Datos

El acceso a la base de datos dentro de la Unidad Educativa Temporal “Jaime Roldós Aguilera” será uno de los servicios más utilizados por las autoridades, profesores y personal administrativo, es por ello que se debe realizar el dimensionamiento para su acceso.

Este servicio es en tiempo real por lo que la respuesta a una consulta debe ser pronta y sin retraso considerable; una transacción común tiene un tamaño aproximado de 200 Kbytes, y se estima que el tiempo de respuesta sea en 30 segundos, con ello se tiene la siguiente ecuación:

$$AB_{web} = \frac{200 \text{ KB}}{1 \text{ transacción}} \times \frac{1 \text{ transacción}}{30 \text{ seg}} \times \frac{8 \text{ bits}}{1 \text{ byte}} \cong 53.33 \text{ kbps}$$

**Ecuación 3. 4 Ancho de Banda para el acceso a base de datos**

### 3.5.8.4 Cálculo del Ancho de Banda para Descargas de Archivos

Para dimensionar este servicio se considera que el tamaño promedio de un archivo a descargar es de 3 MB, este valor es tomado en cuenta para descargas de diferentes índoles como son audio, video, documentos, etc. Adicionalmente se considera que en una hora un usuario tiende a descargar 2 archivos, con lo cual se puede calcular el ancho de banda necesario para poder brindar este servicio en la red.

$$AB_{Descargas} = \frac{3000 \text{ KB}}{1 \text{ descarga}} \times \frac{2 \text{ descargas}}{1 \text{ hora}} \times \frac{1 \text{ hora}}{3600 \text{ seg}} \times \frac{8 \text{ bits}}{1 \text{ byte}} \cong 13.33 \text{ kbps}$$

**Ecuación 3. 5 Ancho de Banda para Descargas**

### 3.5.8.5 Cálculo del Ancho de Banda para VoIP [51]

Debido a que el propósito de este proyecto es el diseño de telefonía IP, se debe tener en cuenta ciertos parámetros para el cálculo del tráfico por cada punto de VoIP.

A continuación se presenta cómo calcular el ancho de banda requerido para transmitir VoIP y un ejemplo de su aplicación.

#### 3.5.8.5.1 Procedimiento para calcular el Ancho de Banda para VoIP

- **Paso 1. – Calcular el tamaño de las tramas de voz**

Este parámetro es el resultado del CODEC utilizado, que permite obtener el tamaño de la porción de datos. A esto debe sumarse el tamaño de los encabezados de capa 4, capa 3 y capa 2.

$$\text{Tamaño de trama} = \text{Payload} + \text{header 4} + \text{header 3} + \text{header 2}$$

**Ecuación 3. 6 Trama de Voz**

Por ejemplo, las tramas obtenidas al utilizar G.729 tienen una longitud de 20 *bytes*, a eso se debe sumar los encabezados RTP, UDP e IP necesarios, que son 40 B, y luego los *bytes* de encapsulamiento de la capa enlace, que si se trata de una trama PPP es de 6 B. En la tabla 3.24 se muestran los tamaños de las cabeceras que intervienen en este proceso.

<b>Cabecera IP</b>	20 Bytes
<b>Cabecera UDP</b>	12 Bytes
<b>Cabecera RTP</b>	8 Bytes
<b>Encapsulamiento PPP</b>	6 Bytes
<b><i>Payload (Voz)</i></b>	20 bytes
<b>Tamaño Total de la Trama</b>	<b>66 Bytes</b>

**Tabla 3. 24 Tamaño de la trama de VoIP con PPP**

Dado el peso del encabezado en el tamaño de la trama a transmitir, en enlaces de bajo ancho de banda (menos de 768 Kbps) es conveniente aplicar compresión de los encabezados de capa 3 y capa 4, lo que se suele denominar compresión de RTP (*cRTP*). Esto reduce esos 40 B iniciales a 2 o 4 B.

De este modo el ejemplo de cálculo quedaría como lo indica la tabla 3.25.

<b>Cabecera IP/UDP/RTP</b>	2 Bytes
<b>Cabecera PPP</b>	6 Bytes
<b><i>Payload (Voz)</i></b>	20 bytes
<b>Tamaño Total de la Trama</b>	<b>28 Bytes</b>

Tabla 3. 25 Tamaño de la trama de VoIP con PPP y compresión RTP

Ahora es necesario convertir el tamaño expresado en bytes a bits como se indica en la ecuación 3.7.

$$28 \text{ Bytes} \times 8 \text{ bits/Byte} = 224 \text{ bits/ trama}$$

Ecuación 3. 7 Número de bits por trama de VoIP con PPP

- **Paso 2 - Calcular el ancho de banda requerido por una llamada**

Los Codecs actualmente utilizados para la digitalización de voz y mostrados en la tabla 1.5 (G.711, G.728, G.729) generan 50 tramas por segundo.

Estos valores pueden ser apreciados de mejor manera en la tabla 1.5 donde se encuentra el detalle de cada uno de los codecs.

Para calcular el ancho de banda requerido para cada llamada se debe multiplicar el tamaño de cada trama por la cantidad de tramas que se envían por segundo:

$$AB_{VoIP} = 224 \text{ bits/trama} \times 50 \text{ tramas/seg.} = 11200 \text{ bps/llamada}$$

Ecuación 3. 8 Ancho de banda requerido por llamada de VoIP con PPP

- **Paso 3 - Calcular el ancho de banda requerido en la implementación.**

Para el presente ejemplo se va a suponer que se trata de cursar un máximo de 10 llamadas concurrentes generadas utilizando CODEC G.729 sobre un enlace PPP con cRTP. (Ver ecuación 3.9)

$$BW_{requerido} = 11,200 \text{ Kbps} \times 10 = 112 \text{ Kbps}$$

**Ecuación 3. 9 Ancho de Banda total con VoIP y PPP**

#### 3.5.8.5.2 Cálculo del Ancho de Banda para VoIP de la Unidad Educativa “JRA”

Con estas indicaciones se procede a encontrar el ancho de banda para VoIP requerido para la institución, para lo cual se debe tomar en cuenta las siguientes consideraciones.

- Códec a utilizarse: G.729
- Encapsulamiento de capa 2: Ethernet

Se debe tomar en consideración que para el encapsulamiento de Ethernet se utiliza los campos MAC Destino, MAC origen, *Type* y FCS que suman un total de 18 bytes adicionales.

Con esta aclaración se realiza el cálculo mencionado anteriormente y se tendrá el tamaño de trama mostrado en la tabla 3.26.

Cabecera IP	20 Bytes
Cabecera UDP	12 Bytes
Cabecera RTP	8 Bytes
Encapsulamiento <i>Ethernet</i>	18 Bytes
<i>Payload</i> (Voz)	20 bytes
<b>Tamaño Total de la Trama</b>	<b>78 Bytes</b>

**Tabla 3. 26 Tamaño de la trama para una LAN sin cRTP**

Posterior a esto se encuentra el número de bits que se transmiten por trama, como se muestra en la ecuación 3.10.

$$78 \text{ Bytes} * 8 \text{ bits/byte} = 624 \text{ bits/trama}$$

**Ecuación 3. 10 Número de bits por trama con *Ethernet***

Luego se encuentra el valor del ancho de banda requerido por cada punto de voz con la ecuación 3.11, tomando en consideración el número de tramas por segundo que tiene el códec G.729.

$$AB_{VoIP} = 624 \text{ bits/trama} \times 50 \text{ tramas/seg} = 31,2 \text{ Kbps}$$

**Ecuación 3. 11 Ancho de Banda por llamada para una LAN**

### 3.5.8.6 Cálculo del Ancho de Banda para la WLAN

Dentro del dimensionamiento del tráfico que soportará la red es muy general el error de no considerar el ancho de banda que utiliza la WLAN, generando problemas al momento de la implementación a los diferentes usuarios. Los usuarios que acceden a la WLAN utilizan principalmente el servicio *web*; sin embargo, se debe considerar que la misma debe proporcionar los mismos servicios que la red cableada tales como VoIP, descarga de archivos, etc.

Para el dimensionamiento de la WLAN se tomará en cuenta el 40 % de los valores encontrados para la red cableada, tomando en consideración que el acceso a la misma tiene restricciones y no es constante en comparación a los puntos de red cableada. La ecuación 3.12 muestra el cálculo del ancho de banda requerido por la red inalámbrica.

$$AB_{WLAN} = 40\% (AB_{web} + AB_{mail} + AB_{bdd} + AB_{ftp} + AB_{VoIP})$$

$$AB_{WLAN} = 40\% (4.4 + 93.33 + 53.33 + 13.33 + 31.2) \cong 78.24 \text{ kbps}$$

**Ecuación 3. 12 Ancho de Banda para la WLAN**

### 3.5.9 ANCHO DE BANDA REQUERIDO PARA DATOS

Una vez calculado el ancho de banda para cada una de las aplicaciones que van a ser utilizadas por los distintos usuarios de la red, se presenta el ancho de banda total que se requiere para datos. Para este cálculo es importante mencionar un concepto llamado “simultaneidad”; este concepto indica la cantidad de usuarios que utilizan concurrentemente los diferentes servicios.

Tomando en consideración lo antes mencionado se elabora la tabla 3.27, la cual muestra la cantidad de usuarios reales y potenciales con los la que cuenta cada zona; siendo usuarios reales los que actualmente existen y usuarios potenciales aquellos que se están considerando en el diseño del presente proyecto, es decir, los que utilizaran actualmente no poseen el servicio y que son considerados en el diseño de la red integrada de voz y datos.

Localización	Usuarios Reales	Usuarios Potenciales	Total de Usuarios
Zona A	9	13	22
Zona B	8	16	24
Zona C	9	23	32
Zona D	2	20	22
Zona E	50	21	71

Tabla 3. 27 Usuarios potenciales y reales de la institución

Una vez conocidos los usuarios con los que cuenta cada zona, se establecen los índices de simultaneidad de cada una de las aplicaciones con las que va contar la institución, como se lo muestra en la tabla 3.28

Aplicación	Índice de Simultaneidad
Correo Electrónico	25 %
Acceso a la Web	30 %
Acceso a la Base de Datos	15 %
Descarga de Archivos	10 %
WLAN	20 %

Tabla 3. 28 Índices de Simultaneidad

Finalmente determinar el ancho de banda necesario para datos como se muestra en la tabla 3.29.

Aplicación	Localización	AB Requerido [Kbps]	Índice de Simultaneidad [%]	Usuarios	AB [Kbps]
Correo Electrónico	Zona A	4.4	0,25	9	9.9
	Zona B			8	8.8
	Zona C			9	9.9
	Zona D			2	2.2
	Zona E			50	55.00
<b>Ancho de banda total para correo electrónico</b>				<b>78</b>	<b>85.80</b>
Acceso a la WEB	Zona A	93.3	0,3	9	251.91
	Zona B			8	223.92
	Zona C			9	251.91
	Zona D			2	55.98
	Zona E			50	1,399.50
<b>Ancho de banda total para acceso a la web</b>				<b>78</b>	<b>2,183.22</b>
Acceso a Base de Datos	Zona A	53.3	0,15	9	71.96
	Zona B			8	63.96
	Zona C			9	71.96
	Zona D			2	15.99
	Zona E			50	399.75
<b>Ancho de banda total para acceso a base de datos</b>				<b>78</b>	<b>623.62</b>
Descarga de Archivos	Zona A	13.33	0,10	9	11.99
	Zona B			8	10.66
	Zona C			9	11.99
	Zona D			2	2.66
	Zona E			50	66.65
<b>Ancho de banda total para descargas de archivos</b>				<b>78</b>	<b>103.95</b>
WLAN	Zona A	78.24	0,20	9	140.83
	Zona B			8	125.18
	Zona C			9	140.83
	Zona D			2	31.29
	Zona E			50	782.4
<b>Ancho de banda total para la WLAN</b>				<b>78</b>	<b>1,220.53</b>
<b>ANCHO DE BANDA TOTAL PARA DATOS</b>					<b>4,217.12</b>

Tabla 3. 29 Tráfico Total para Datos



### 3.5.10 ANCHO DE BANDA REQUERIDO PARA VOZ

Similar proceso al realizado para el cálculo del ancho de banda para datos se realiza para la voz, empezando por detallar los usuarios potenciales y reales de cada zona como se muestra en la tabla 3.30.

Localización	Usuarios Reales	Usuarios Potenciales	Total de Usuarios
Zona A	4	10	14
Zona B	0	1	1
Zona C	0	8	8
Zona D	0	2	2
Zona E	0	3	3

Tabla 3. 30 Usuarios reales y potenciales del sistema de voz

Para poder determinar el ancho de banda requerido para voz se debe multiplicar el número total de usuarios por índice de simultaneidad y el ancho de banda requerido para la transmisión de VoIP detallado en el numeral 3.5.8.5.2.

El índice de simultaneidad considerado para la VoIP es del 35 %, es decir al menos 10 usuarios utilizarían el servicio simultáneamente, obteniendo así el valor mostrado en la ecuación 3.13.

$$AB_{VoIP} = 28 * 0.35 * 31.2 \text{ Kbps} = 305.76 \text{ Kbps}$$

Ecuación 3. 13 Ancho de Banda Total para VoIP

### 3.5.11 ANCHO DE BANDA DE LA CONEXIÓN A INTERNET

La conexión a Internet considera todo el flujo de información que va al exterior o comúnmente llamada nube. Para ello se debe considerar que no todo el tráfico a cursar por la red saldrá a la nube, y debe ser considerado al momento de dimensionar el ancho de banda a contratar.

Para este proyecto se consideran los porcentajes mostrados en la tabla 3.31 como aquellos valores que saldrán a la nube.

SERVICIO	PORCENTAJE	ANCHO DE BANDA TOTAL [Kbps]	ANCHO DE BANDA EXTERNO [Kbps]
Correo Electrónico	75%	85.80	64.35
Acceso a la Web	90 %	2,123.82	1,911.44
Acceso a Base de Datos	10%	623.62	62.36
Descarga de Archivos	40%	103.95	41.58
WLAN	80%	1,220.53	976.42
<b>ANCHO DE BANDA TOTAL HACIA LA NUBE</b>			<b>3,056.15</b>

Tabla 3. 31 Ancho de Banda hacia la Nube

Como se puede apreciar el ancho de banda a contratar no considera el dimensionamiento de la VoIP, debido a que el sistema de voz diseñado para este proyecto es interno, es decir no saldrá a la nube.

Finalmente se reemplaza los valores antes encontrados y se encuentra el valor de AB de la conexión a Internet, como se puede apreciar en la ecuación 3.14.

$$AB \text{ total} = 3,056.15 \cong 3 \text{ Mbps}$$

Ecuación 3. 14 Ancho de Banda total para la institución

*Nota: Cabe mencionar que los valores de índices de simultaneidad como los porcentajes de consumo hacia el Internet, son valores estimados en conjunto con las autoridades del plantel, ya que al momento no es posible encontrar valores reales debido a que no existe una red en sí para la Institución.*

### 3.5.12 REQUERIMIENTOS DE VOZ

Como se mencionó anteriormente la tecnología que se va utilizar para la transmisión de voz dentro de la institución será VoIP, ya que mediante ella se puede hacer uso de la red de datos para la transmisión de voz con sus características propias.

### 3.5.12.1 Número de Usuarios

Actualmente el servicio telefónico brinda servicio tan solo a Secretaría General y Rectorado, el resto de personal no cuenta con este servicio.

Como se detalló en el numeral 3.5.10 los usuarios de voz estarán ligados a la distribución propia de la Institución, teniendo así un total de 28 usuarios como se muestra en la tabla 3.30.

Siendo así la zona Administrativa la que más extensiones necesita debido a la cantidad de personal que en ella labora.

Además de los puntos especificados para voz existe la posibilidad de que otros usuarios puedan acceder a la red de voz, sin la necesidad de contar con el *hardware* apropiado, sino con el uso de *software* denominado *softphone*, que instalado correctamente en un computador proporciona características adecuadas para la transmisión de VoIP sobre la red.

### 3.5.12.2 Proyección de Crecimiento

Para conocer la proyección de crecimiento del personal administrativo y docente dentro de la institución se ha consultado al departamento de contabilidad cuántas personas han estado laborando en la institución en los cinco últimos años, teniendo así la tabla 3.32.

Año	Personal
2009	20
2010	22
2011	23
2012	26
2013	28

Tabla 3. 32 Número de personal administrativo y docente en los cinco últimos años

En base a esta información se estima que para los 10 años de vida útil de la red a diseñar se tendrá un aumento de al menos ocho personas nuevas destinadas a laborar en la institución, las mismas que deberán contar con sus respectivas extensiones telefónicas, llegando a tener un total de 36 empleados.

### 3.5.12.3 Circuitos Troncales hacia la PSTN

Los circuitos troncales son los enlaces que interconectan las centrales telefónicas privadas con la red telefónica pública conmutada PSTN. Es por ello que se debe realizar un correcto dimensionamiento para que el sistema de voz no colapse dentro de la Institución. Este valor es medido en *Erlang* y se lo calcula en base a la ecuación 3.15.

$$A = C \times T$$

Ecuación 3. 15 Intensidad de tráfico

Donde:

- A = Intensidad de tráfico
- C = Número de llamadas realizadas en un hora
- T = Tiempo promedio de llamada

En vista que la institución no cuenta con una central telefónica, el cálculo estará basado en los nuevos requerimientos de voz ya indicados para la red. Por lo tanto, se han considerado los siguientes valores para el dimensionamiento, que representaría la condición crítica y con los cuales se tendría la ecuación 3.16.

- Número máximo de llamadas en una hora:15
- Número máximo de llamadas externas en una hora:10
- Promedio de duración de llamadas:3 min

$$A = \frac{10 \text{ llamadas}}{\text{hora}} \times \frac{3 \text{ min}}{1 \text{ llamada}} \times \frac{1 \text{ hora}}{60 \text{ minutos}} = 0.5 \text{ Erlang}$$

Ecuación 3. 16 Intensidad de tráfico para la UET Jaime Roldós Aguilera

Una vez encontrado este valor se procederá a proyectarlo para el tiempo de vida del proyecto, debido a que después de la implementación el número de usuarios crece; para ello utiliza la ecuación 3.17.

$$A_f = \frac{U_f}{U_a} \times A_o$$

**Ecuación 3. 17 Intensidad de tráfico proyectado**

Dónde:

- $A_f$  = Intensidad de tráfico proyectado
- $U_f$  = Número de usuarios proyectados
- $U_a$  = Número de usuarios Actuales
- $A_o$  = Intensidad de tráfico actual

Con los valores de proyección antes encontrados se tiene el valor mostrado por la ecuación 3.18.

$$A = \frac{36}{28} \times 0.5 = \mathbf{0.64 \textit{ Erlang}}$$

**Ecuación 3. 18 Intensidad de tráfico proyectado para la UET Jaime Roldós Aguilera**

Con este valor y en base a las pérdidas propias de los sistemas telefónicos, es decir, 1% del tráfico, se puede encontrar el número de líneas troncales que se necesitan para satisfacer las necesidades de la institución.

Para ello se utiliza la tabla de *Erlang B* mostrada en el anexo C, la cual indica que para estos requerimientos se necesitan 3 líneas troncales; es decir, que las líneas con que se cuenta actualmente no es suficiente para los requerimientos de la institución. [52]

*“En base al análisis anterior se recomienda a la institución la adquisición de nuevas líneas telefónicas al fin de que la red tenga un rendimiento óptimo y no exista ningún bloqueo con pérdida de comunicación.”*

## **3.6 DISEÑO DE LA RED ACTIVA**

El diseño de la red integrada de voz y datos para la Unidad Educativa Temporal “Jaime Roldós Aguilera” estará basado en un modelo jerárquico, que consta de tres niveles, acceso, distribución y núcleo.

### **3.6.1 CAPA ACCESO**

Esta capa proveerá acceso a los dispositivos finales de la red, como son: computadores, teléfonos IP, entre otros.

Estos dispositivos estarán conectados a un *switch* de acceso, el cual a su vez se conectará a los *switches* de distribución para manejar el flujo de datos emitidos por el usuario final.

### **3.6.2 CAPA DISTRIBUCIÓN**

Esta capa se encargará de funciones tales como listas de control de acceso, diferenciación de datos, manejo de seguridad, entre otras.

Así mismo debe tener conexión con la capa de núcleo para proveer de alta disponibilidad a la red.

### **3.6.3 NÚCLEO DE LA RED**

Como su nombre lo indica, esta capa es la encargada de brindar a la red un alto rendimiento y desempeño, para ello realiza tareas tales como, conmutación de paquetes, enrutamiento entre las diferentes VLAN`s, etc.

Dentro de esta capa es muy común encontrar equipos como *switches* multicapa o de capa 3, para que puedan realizar ciertas funciones que por lo general la cumplen los *routers*, además de equipos como centrales telefónicas, etc.

### 3.6.4 ELECCIÓN DE EQUIPOS PARA LA RED

Al momento de realizar la elección de los equipos que van a ser utilizados dentro de la red, es muy importante tomar en cuenta ciertos factores, que pueden simplificar algunas de las tareas que la misma necesita, tales como; administración, seguridad, calidad de servicio, entre otras.

#### 3.6.4.1 Administración de los Equipos

Los equipos que van a prestar los diferentes servicios ya antes mencionados, deben contener ciertas características al momento de ser seleccionados, como por ejemplo su administración; es decir, que puedan ser gestionados y administrados remotamente.

Deben soportar protocolos de autenticación y encriptación de datos tales como: SNMP<sup>35</sup> y RMON<sup>36</sup> y SSH<sup>37</sup>, etc.

#### 3.6.4.2 Escalabilidad y Versatilidad

Se hace referencia a estas características ya que la red seguirá con su crecimiento, por lo cual los equipos deben tener la capacidad de acoplarse a nuevas aplicaciones, servicios, y expansiones que ocurran en la red.

#### 3.6.4.3 Calidad de Servicio y Seguridad

Los equipos a adquirir deben contar con características que proporcionen seguridad y calidad de servicio a la red, tales como control de puerto mediante direcciones MAC, configuración de ACL, soporte de VLAN's, protocolos como IEEE 802.1X e IEEE 802.1p, los cuales sirven para control de acceso mediante puertos y priorización de servicios, respectivamente.

---

<sup>35</sup> **SNMP:** *Simple Network Management Protocol.*- Protocolo que facilita el intercambio de información de administración entre dispositivos de red

<sup>36</sup> **RMON:** *Remote Network Monitoring.*- Norma basada en SNMP para informar diversas condiciones de la red.

<sup>37</sup> **SSH:** *Secure Shell.*- Protocolo que sirve para acceder a máquinas remotas a través de una red.

### 3.6.5 SWITCHES DE ACCESO

Una vez mencionadas algunas de las características generales con las que deben contar los equipos de red, es necesario describir algunas de las características específicas para los equipos de cada una de las capas que involucra el diseño.

Como se mencionó en el numeral 3.5.1.1 la Institución necesita de un total de 204 puertos para su red, por lo que se requerirán nueve *switches* de acceso de 24 puertos, quedando así 12 puertos libres para futuras expansiones.

Adicional a esto, uno de los parámetros a tener en cuenta dentro de la adquisición de un *switch* es la velocidad del *backplane*; para lo cual se debe considerar el número de puertos que serán utilizados simultáneamente en la hora pico dentro de la institución.

Este cálculo se lo puede realizar con la ayuda de la ecuación 3.19. [53]

$$V_{backplane} = \# \text{ de puertos utilizados simultáneamente} \times 100 \text{ Mbps} \times 2$$

**Ecuación 3. 19 Cálculo de la velocidad de *backplane* en el *Switch***

Para el diseño se considera que la hora pico de uso de la red es de 11:00 am a 12:00 pm y que al menos 20 de los 24 puertos disponibles están siendo utilizados simultáneamente, por lo tanto se tiene la ecuación 3.20:

$$V_{backplane} = \{(20 \times 100 \text{ Mbps}) + (1 * 1000)\} \times 2 = 6 \text{ Gbps}$$

**Ecuación 3. 20 Velocidad de *backplane* del *switch* de acceso**

Con esta acotación se presenta en la tabla 3.34 las características mínimas que deben disponer los *Switches* de acceso.



<b>Switches de Acceso</b>	
<b>Parámetros</b>	<b>Características</b>
<b>Puertos Ethernet</b>	24 / 48 puertos 10/100 Mbps
<b>Puertos Uplink</b>	2 puertos GigabitEthernet 10/100/1000 Mbps
<b>Capa OSI</b>	2
<b>Backplane</b>	6,8 Gbps
<b>Throughput</b>	6 Mpps
<b>Entradas de direcciones MAC</b>	8000
<b>Manejo de VLAN's</b>	Sí
<b>Calidad de Servicio</b>	Sí
<b>Estándares</b>	IEEE 802.1d ; IEEE 802.1p ; IEEE 802.1q ; IEEE 802.1x ; IEEE 802.1w ; IEEE 802.3u ; IEEE 802.3x ; IEEE 802.3af
<b>Protocolos</b>	SNMPv1; SNMPv2; SNMPv3; Telnet; RMON
<b>Administración</b>	GUI; SNMP; Telnet; CLI

Tabla 3. 33 Características de los *Switches* de Acceso

La tabla 3.35 indica la cantidad de *switches* de acceso que se necesitan por cada zona.

<b>Ubicación</b>	<b>Número de Puertos</b>	<b>Cantidad</b>
<b>Zona A</b>	46	2 <i>Switches</i> de 24 puertos
<b>Zona B</b>	28	2 <i>Switches</i> de 24 puertos
<b>Zona C</b>	40	2 <i>Switches</i> de 24 puertos
<b>Zona D</b>	16	1 <i>Switch</i> de 24 puertos
<b>Zona E</b>	74	2 <i>Switches</i> de 48 puertos

Tabla 3. 34 Número de *switches* necesarios por Zona

Con estos valores se puede encontrar el número total de puertos que se necesita y el número total de puertos sobrantes para futuras expansiones o adecuaciones de la red, ver tabla 3.36

Ubicación	Número de Puertos	Puertos Utilizados	Puertos Disponibles
Zona A	48	46	2
Zona B	48	28	20
Zona C	48	40	8
Zona D	24	16	8
Zona E	96	74	22
<b>TOTAL</b>	<b>264</b>	<b>204</b>	<b>60</b>

Tabla 3. 35 Número de puertos a utilizar

En base a esta información se puede decir que la institución contará con 60 puertos disponibles en caso de desear agregar nuevos usuarios a la red; además se cumple con el 30 % de proyección que se había establecido en principio.

### 3.6.6 SWITCHES DE DISTRIBUCIÓN

Los *switches* de distribución deben tener características específicas, ya que es aquí donde se realizarán tareas como diferenciación de servicios, priorización, listas de control de accesos, conmutación entre VLAN`s, etc.

Para el presente proyecto se debe considerar que los nueve *switches* de la capa acceso, deberán estar conectados al nivel de distribución, por lo cual se necesitarán dos *switches*; el primero para dar los servicios de la capa de distribución y el otro para proporcionar redundancia a la red, esto con la finalidad de tener una red de alta disponibilidad y evitar la saturación de la misma.

Con estas consideraciones se tiene la tabla 3.37 donde se muestran las características mínimas que deben poseer los *switches* de distribución.

<b>Switches de Distribución</b>	
<b>Parámetros</b>	<b>Características</b>
<b>Puertos Ethernet</b>	12 / 24 puertos 10/100/1000 Mbps
<b>Puertos <i>Uplink</i></b>	2 puertos GigabitEthernet 10/100/100 Mbps
<b>Capa OSI</b>	2/3
<b><i>Backplane</i></b>	11,6 Gbps
<b><i>Throughput</i></b>	6 Mpps
<b>Entradas de direcciones MAC</b>	8000
<b>Manejo de VLAN`s</b>	Sí
<b>Seguridad</b>	Soporte a ACL estándar y extendidas en todos los puertos
<b>Estándares</b>	IEEE 802.1d ; IEEE 802.1p ; IEEE 802.1q ; IEEE 802.1x ; IEEE 802.1w ; IEEE 802.3u ; IEEE 802.3x ; IEEE 802.3af
<b>Protocolos</b>	IP; IPv6; OSPF; RIPv2; IGM; BGP; DHCP.
<b>Administración</b>	GUI; SNMP; Telnet; CLI

Tabla 3. 36 Características de los *switches* de Distribución

### 3.6.7 SWITCHES DE CORE

Estos *switches* proveen de alta velocidad hacia el exterior de la red, deben manejar los paquetes tan rápido como sea posible, así como un alto nivel de disponibilidad y la facilidad de adaptarse a los cambios que sufra la red de manera inmediata. La tabla 3.38 muestra los requerimientos mínimos que deben tener los *Switches* de *Core* para el diseño de la red.

<b>Switch de Core</b>	
<b>Parámetros</b>	<b>Características</b>
<b>Puertos Ethernet</b>	12 puertos 100/1000/10000 Mbps
<b>Capa OSI</b>	2/3
<b>Backplane</b>	48 Gbps
<b>Throughput</b>	50 Mpps
<b>Entradas de direcciones MAC</b>	16000
<b>Seguridad</b>	Soporte a ACL estándar y extendidas en todos los puertos
<b>Estándares</b>	IEEE 802.1d ; IEEE 802.1p ; IEEE 802.1q ; IEEE 802.1x ; IEEE 802.1w ; IEEE 802.3u ; IEEE 802.3x ; IEEE 802.3af
<b>Protocolos</b>	IP; OSPF; RIPv2; IGM; BGP; DHCP.
<b>Administración</b>	GUI; SNMP; Telnet; CLI

Tabla 3. 37 Características de los switches de Core

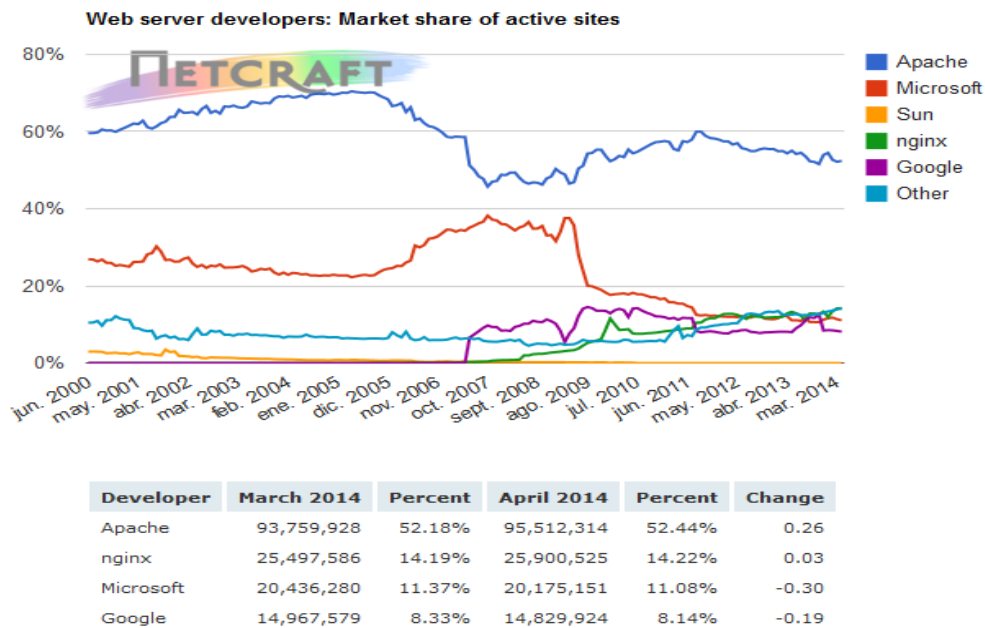
### 3.6.8 SERVIDORES

A continuación se determinarán las características que deben disponer los servidores para poder proveer los servicios mencionados en el capítulo anterior.

#### 3.6.8.1 Servidor WEB

La función de un servidor *web* es la de contestar las peticiones de ejecución que le hará un cliente o un usuario de Internet. Estas respuestas deberán ser de forma adecuada, entregando como resultado una página web o información de todo tipo de acuerdo a los comandos solicitados. [54]

Para brindar este servicio se instalará el servidor web Apache, sobre el sistema Operativo Linux; la elección de este servidor fue realizada en base a los estudios que se han realizado en los últimos años, donde se indica que Apache es el servidor web más utilizado en el mercado como lo indica la compañía inglesa *Netcraft* en su mediciones mensuales, tal como se observa en la figura 3.8



**Figura 3. 8 Utilización de servidores web en el mercado [55]**

Además de los estudios mostrados, cabe señalar que la elección de Apache también se debe por contar con características tales como las siguientes:

- Servidor multiplataforma
- Basado en código abierto
- Flexibilidad y alta seguridad

### 3.6.8.2 Servidor de Correo Electrónico

Es el encargado de manejar el flujo de correos electrónicos tanto internos como externos en la institución; existen varias alternativas especializadas de *software* que cumplen esta función, entre las cuales se pueden citar a *Postfix*, *Qmail* y una de la más utilizada en los últimos años, *Zimbra*.

El desarrollo de Zimbra ha sido muy rápido; proporciona características muy interesantes para proveer el servicio de correo electrónico, por lo que será instalado en sistema operativo Linux para cumplir dicha función. A continuación se muestran algunas de las características por las cuales se decidió instalar el servidor Zimbra. [56]

- **Flexibilidad.-** Personaliza fácilmente según las necesidades de la organización.
- **Libertad.-** Utiliza el cliente web de Zimbra junto con otros programas tradicionales, como plataforma mixta.
- **Durabilidad.-** Es un servidor altamente fiable, permitiendo así su prolongado tiempo de vida.
- **Bajo mantenimiento.-** Gestión completamente sencilla.

### 3.6.8.3 Servidor FTP

Es uno de los servicios básicos dentro de la institución, permite a los diferentes usuarios descargar información desde la intranet, tales como: formularios, bibliografías, publicaciones y demás.

Uno de los factores más a tomar en cuenta para este servidor es la seguridad; es por ello que ahora la mayoría de los servidores FTP soportan SSL<sup>38</sup>/TLS<sup>39</sup> y utilizan el mismo tipo de cifrado presente en los sitios web seguros.

Entre los principales servidores FTP se tienen: *ProFtp*, *BulletProof FTP*, *SecureFTP*, *SurgeFTP*, *TitanFTP*, y *WS\_FTP*.

Todos los servidores antes mencionados cumplen las características que la institución necesita, sin embargo se ha escogido el servidor *ProFTP* debido a su estabilidad y a su compatibilidad con la herramienta *Webmin*.

---

<sup>38</sup> **SSL:** *Secure Socket Layer.- Protocolo diseñado para permitir que las aplicaciones puedan transmitir información de manera segura*

<sup>39</sup> **TLS:** *Transport Layer Security.- Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través de Internet*

#### **3.6.8.4 Servidor DCHP**

Es el encargado de proporcionar direcciones IP automáticamente a cada usuario final, será instalado bajo Linux.

#### **3.6.8.5 Servidor DNS**

Es el encargado de traducir un nombre de dominio a una dirección IP; para el presente proyecto el dominio será el siguiente:

***@jra.net***

Se utilizará el servidor DNS de nombre BIND9, ya que es compatible con Zimbra que será el servidor de correo electrónico y por su fácil implementación.

#### **3.6.8.6 Servidor de Llamadas IP**

Es el encargado de efectuar llamadas y generar extensiones internas sin la necesidad de pasar por la PSTN para brindar servicios de telefonía dentro de una Institución. Entre las funciones principales que cumple este servidor se tienen:

- Establecimiento, control y desconexión de llamadas.
- Llamadas en espera
- Correos de Voz, etc.

Para este propósito se ha decidido utilizar Asterisk como se explicó en los capítulos 1 y 2.

### **3.6.9 CARACTERÍSTICAS GENERALES DE LOS SERVIDORES**

Una vez definidos los servidores que se necesitan dentro del proyecto es importante definir algunas características importantes dentro de la elección de los mismos.

- **Robustez**

Tolerante a fallas, proveer alta disponibilidad y de ser posible ser redundante.

- **Escalabilidad**

Debe poder aumentar la capacidad de clientes y servidores por separado.

- **Rendimiento**

Un servidor puede ser utilizado por varios clientes al mismo tiempo y regular su acceso a los recursos, es por ello, que se hace necesario un alto rendimiento a fin de no colapsar las comunicaciones.

- **Administración sencilla**

Al estar distribuidas las funciones y responsabilidades entre varios ordenadores independientes, es posible reemplazar, reparar, actualizar, o incluso trasladar un servidor, mientras que sus clientes no se verán afectados o su afectación será mínima por ese cambio.

### 3.6.10 CARACTERÍSTICAS ESPECÍFICAS DE LOS SERVIDORES

Una vez determinadas las características generales que deben poseer los servidores, es necesario, identificar sus características o específicas.

Estas características serán: espacio en disco, memoria RAM, y la velocidad del procesador, las mismas que se muestran en la tabla 3.39.

Servidor	Espacio en disco	RAM	Procesador
Apache	al menos 50 MB	256 MB mínimo 512 MB óptimo	250 MHz
Zimbra	10 GB	1 GB mínimo	2.0 GHz
ProFTP	8 GB	256 MB mínimo	250 MHz
DHCP	1 GB	256 MB mínimo	250 MHz
DNS	1 GB	256 MB mínimo	250 MHz
Servidor IP	1 GB	1 GB óptimo	2.0 GHz

Tabla 3. 38 Características Específicas de los Servidores [57] [58] [59]



### **3.6.11 EQUIPOS PARA TELEFONÍA IP**

La solución a diseñarse para la institución estará basada en un dispositivo que realice la conversión de analógico a digital entre la PSTN y la red IP (*Gateway*) y en el servidor de llamadas que será el encargado de su gestión.

#### **3.6.11.1 Servidor de Llamadas IP**

Su función es la realización y control de llamadas IP, también se encarga de convertir las señales de voz a datos mediante diferentes protocolos tales como: SIP y H.323 para posteriormente ser enviados dentro de una red IP.

Como se detalló en los capítulos 1 y 2, para el presente proyecto el servidor de llamadas será levantado con Asterisk.

#### **3.6.11.2 Gateway IP**

Es un dispositivo de red que convierte el tráfico de telefonía analógica en tráfico IP, para luego ser transmitido por una red de datos.

Si bien dentro de este proyecto no se realizará la integración entre Asterisk y la PSTN, se recomienda en caso de ser necesaria la adquisición de un *Gateway IP* que cumpla al menos con los requisitos mostrados en la tabla 3.40.

#### **3.6.11.3 Terminales de Telefonía IP**

Para los terminales de Telefonía IP se tienen dos opciones, teléfonos IP dedicados, es decir, *hardware*; y los denominados *softphone*, que son emuladores instalados en una computadora al fin de realizar las tareas de un teléfono IP.

Los terminales de Telefonía IP también deben poseer sus características propias para poder proporcionar el adecuado uso a los usuarios. Algunas de las características más importantes se muestran en la tabla 3.41.

<b>Gateway IP</b>	
<b>Parámetros</b>	<b>Características</b>
<b>Puertos Ethernet</b>	2 puertos 10/100 Mbps
<b>Interfaces FXO</b>	24
<b>Codecs de Voz</b>	G.711 ; G.723 ; G.726 ; G.729
<b>Cancelación de Eco</b>	Sí
<b>Supresión de Silencios</b>	Sí
<b>Manejo de VLAN`s</b>	Sí
<b>Estándares</b>	IEEE 802.1p ; IEEE 802.1q ; IEEE 802.3af ; H.323 ; SIP v2
<b>Protocolos</b>	SNMPv1; SNMPv2; SNMPv3; Telnet; RMON
<b>Administración</b>	GUI; SNMP; Telnet; CLI

Tabla 3. 39 Características del Gateway IP

<b>Teléfonos IP</b>	
<b>Parámetros</b>	<b>Características</b>
<b>Puertos</b>	2 puertos RJ45 10/100 Mbps
<b>Interfaces FXO</b>	24
<b>Codecs de Voz</b>	G.711 ; G.723 ; G.726 ; G.729
<b>Cancelación de Eco</b>	Sí
<b>Supresión de Silencios</b>	Sí
<b>Manejo de VLAN`s</b>	Sí
<b>Estándares</b>	IEEE 802.1p ; IEEE 802.1q ; H.323 ; SIP v2 ; 802.3af ; MPLS
<b>Protocolos</b>	SNMPv1; SNMPv2; SNMPv3; Telnet; RMON
<b>Administración</b>	GUI; SNMP; Telnet; CLI

Tabla 3. 40 Características de los terminales de Telefonía IP

### 3.6.12 DISEÑO DE LA RED DE ÁREA LOCAL INALÁMBRICA

Uno de los inconvenientes frecuentes con los que se tiene que lidiar dentro de una Institución de gran extensión, es el acceso a la red en ciertos lugares donde la red cableada no tiene manera de llegar.

Es por ello que aparece el concepto de redes de áreas locales inalámbricas, con el propósito, no solo de cubrir la necesidad antes mencionada, sino también de permitir acceso temporal a ciertos usuarios. La red inalámbrica a formar parte de la red diseñada para la Unidad Educativa Temporal “Jaime Roldós Aguilera” debe prestar los mismos servicios que la red cableada.

Se debe tomar en consideración las características adicionales que debe poseer la red inalámbrica por su naturaleza, sobre todo en el aspecto de seguridad ya que es más susceptible a ataques, por lo que debe contar con sus respectivos sistemas de autenticación, cifrado y encriptación.

Como se detalló en el capítulo II, la institución cuenta con una “red” inalámbrica de muy corto alcance que no cumple con las especificaciones técnicas necesarias para su correcto funcionamiento; es por ello, que dentro del diseño se debe plantear una solución de este tipo, para proveer acceso a lugares donde la red cableada no tiene forma de llegar, brindando así movilidad y flexibilidad a los usuarios de la red.

La WLAN<sup>40</sup> debe proveer servicio a sectores de la institución que no tienen acceso a la red cableada, tales como: patios, pasillos, zonas de recreación, y zonas que además de poseer puntos de red fijos necesitan ser considerados en el alcance de la red inalámbrica como laboratorios, aulas, área administrativa, entre otros.

Para este propósito se debe conocer los lugares estratégicos donde se ubicarán los *access-point*, esto se determinará mediante un *site survey* pasivo.

---

<sup>40</sup> **Wireless Local Area Network:** *Red Inalámbrica de Área Local*

### 3.6.12.1 Site Survey Pasivo [60]

Los *Site Surveys*, también referidos como estudios de propagación de señales *Wi-Fi*, son necesarios para garantizar el éxito y el despliegue eficaz de las redes inalámbricas.

Para el presente diseño se realizó un *Site Survey* pasivo dentro de la institución, mediante el cual se pudo determinar el alcance de la “red” inalámbrica actual y los parámetros de configuración de las redes aledañas tales como: SSID, Canal, Seguridad, etc.

Para este análisis se utilizó el *software Acrylic WiFi*, el mismo que es gratuito y de fácil manejo para el usuario; mediante esta herramienta se realizaron mediciones dentro de la institución y se puede observar que se tienen las redes mostradas en la figura 3.9.




























Access Points (Showing 17 of 17, Updated 17)									
	SSID	#	Mac Address	Rssi	Chan	802.11	WEP	WPA	WPA2
	CHICAIZA		4C:8B:EF:50:B9:24	-86 	11	b, g, n		PSK-CCMP	PSK-CCMP
	ANGELFLORES		BC:76:70:DD:BA:E0	-73 	11+7	b, g, n		PSK-CCMP	
	[Hidden]		02:0C:42:67:EB:62	-74 	6	b	Open		
	MASTERLAB		78:54:2E:5A:B1:54	-74 	11	b, g, n			PSK-CCMP
	wRoLDos		C2:9F:DB:9D:71:30	-67 	1	b, g, n		PSK- (TKIP   CCMP)	PSK- (TKIP   CCMP)
	ROSA CNT		00:66:4B:F3:55:24	-77 	11	b, g, n		PSK-CCMP	PSK-CCMP
	XIMENA CABRERA		D4:6E:5C:01:0C:9C	-72 	11	b, g, n		PSK-CCMP	PSK-CCMP
	DAYANA		4C:8B:EF:16:BE:B8	-73 	11	b, g, n		PSK-CCMP	PSK-CCMP
	JAVIER		D4:6E:5C:01:09:B8	-77 	11+7	b, g, n		PSK-CCMP	PSK-CCMP
	INTERNET CNT		00:26:B6:4C:0F:60	-72 	11	b, g		PSK-CCMP	
	ubnt		00:27:22:18:4D:88	-70 	8+4	b, g, n			PSK- (TKIP   CCMP)
	[Hidden]		00:0C:42:39:D3:AB	-86 	6	b	Open		
	RED EDUCATIVA		4C:8B:EF:50:D0:A8	-72 	11+7	b, g, n		PSK-CCMP	PSK-CCMP
	Soft_Solutions		F8:1A:67:ED:60:9E	-72 	6	b, g, n		PSK- (TKIP   CCMP)	PSK- (TKIP   CCMP)

Figura 3. 9 WLAN's cercanas a la institución

Después de realizar mediciones en los diferentes sectores, se puede apreciar que la potencia de la señal de la “red” inalámbrica de la institución se debilita al alejarse del lugar donde se encuentra el *router* inalámbrico, es decir, el Laboratorio de Informática I como lo indica la figura 3.10.

SSID	#	Mac Address	Rssi	Chan	802.11	WEP	WPA	WPA2
[Hidden]		00:0C:42:39:D3:AB	-74	6	b	Open		
Csed-Irenita		64:66:B3:37:AC:AC	-77	6+2	b, g, n		PSK- (TKIP   CCMP)	PSK- (TKIP   CCMP)
[Hidden]		02:0C:42:67:EB:62	-86	6	b	Open		
STAMAY		4C:8B:EF:16:1F:2C	-73	11	b, g, n		PSK-CCMP	PSK-CCMP
INTERNET CNT		F8:3D:FF:10:AC:2C	-72	11	b, g, n		PSK-CCMP	
ubnt		00:27:22:18:4D:88	-58	8+4	b, g, n			PSK- (TKIP   CCMP)
wRoLDos		C2:9F:DB:9D:71:30	-70	1	b, g, n		PSK- (TKIP   CCMP)	PSK- (TKIP   CCMP)

Figura 3. 10 Pérdida de potencia en la WLAN de la institución

También se puede observar que existen redes cercanas a la institución; en ellas se debe analizar el **canal** en el cual está funcionando y el **rango de frecuencias**; entre los más utilizados está el canal 11 y la frecuencia 2.4 GHz, como lo muestra la figura 3.11.

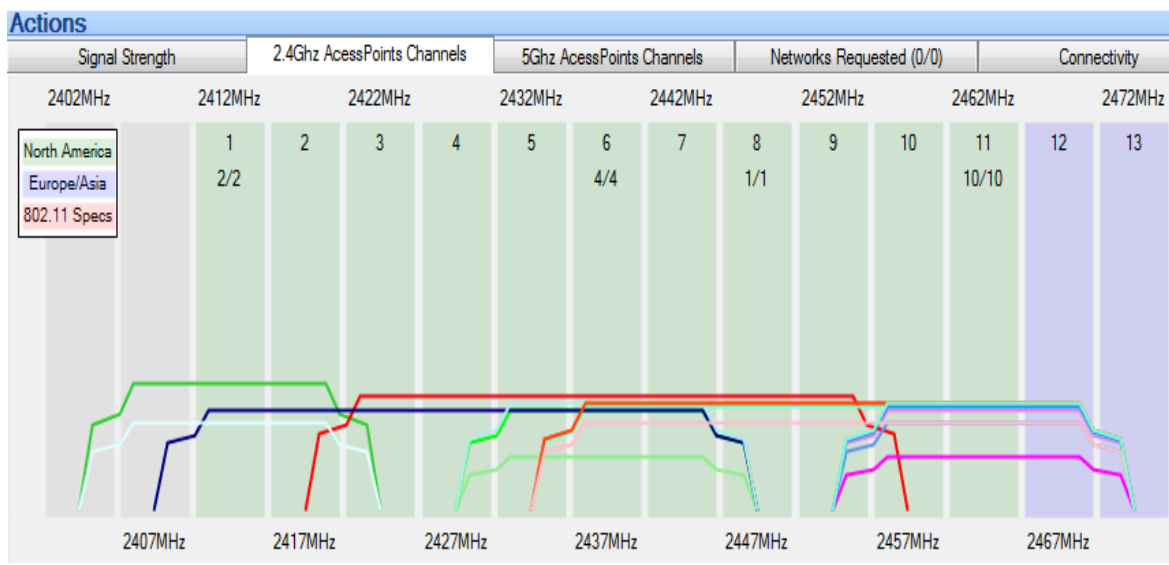


Figura 3. 11 Canales y frecuencias de WLAN's cercanas a la institución

Para el presente diseño se debe tomar en cuenta estas consideraciones con la finalidad de que la red inalámbrica a diseñar no se vea afectada y que no exista interferencia con los nuevos *access-points* a involucrar en la red.

En base a este análisis se muestra la tabla 3.42 con los lugares donde se ubicarán los *acces-point* y el área a cubrir por los mismos.

Descripción	Ubicación	Departamento	Áreas a Cubrir
AP-JRA01	Zona E	Lab Informática II	Patio Principal, Zona E Pasillo Zona E- Zona D,
AP-JRA02	Zona E	Lab Informática I	Patio Trasero, Zona E Pasillo Zona E- Zona C,
AP-JRA03	Zona C	Inspección General	Patio Lateral, Patio Principal, Zona C Pasillo Zona C- Zona E, Pasillo Zona C- Zona B,
AP-JRA04	Zona B	Lab PLC's	Patio Lateral, Bar, Parqueaderos, Pasillo Zona C- Zona B, Zona B,
AP-JRA05	Zona B	Aula	Patio Principal, Parqueaderos, Zona B Pasillo Zona A- Zona B
AP-JRA06	Zona A	Secretaría General	Patio Principal, Zona A Pasillo Zona A- Zona B.
AP-JRA07	Zona A	Aula	Patio Lateral, , Zona A Pasillo Zona A- Zona D
AP-JRA08	Zona D	Salón Audiovisual	Patio Principal, Patio Trasero, Patio Lateral, Zona D, Pasillo Zona A- Zona D,

Tabla 3. 41 Distribución de *Access Point*

En la figura 3.12 se puede apreciar las áreas que va a cubrir cada uno de los *access-point* dentro de la Unidad Educativa Temporal “Jaime Roldós Aguilera”.

### 3.6.12.2 Aplicaciones de la WLAN

La WLAN al ser parte de la red de la Institución, debe soportar las mismas aplicaciones que la red cableada, es decir, acceso a la *web*, correo electrónico, FTP, entre otras; tomando en consideración las limitantes que una red inalámbrica posee, como son: velocidad de acceso, degradación de la señal, etc.

Cabe señalar que la mayoría de usuarios al conectarse a la WLAN, principalmente utilizarán el servicio de acceso a la *web*, lo cual debe ser considerado en el dimensionamiento del tráfico; para el presente proyecto esto fue realizado en el numeral 3.5.8.6.

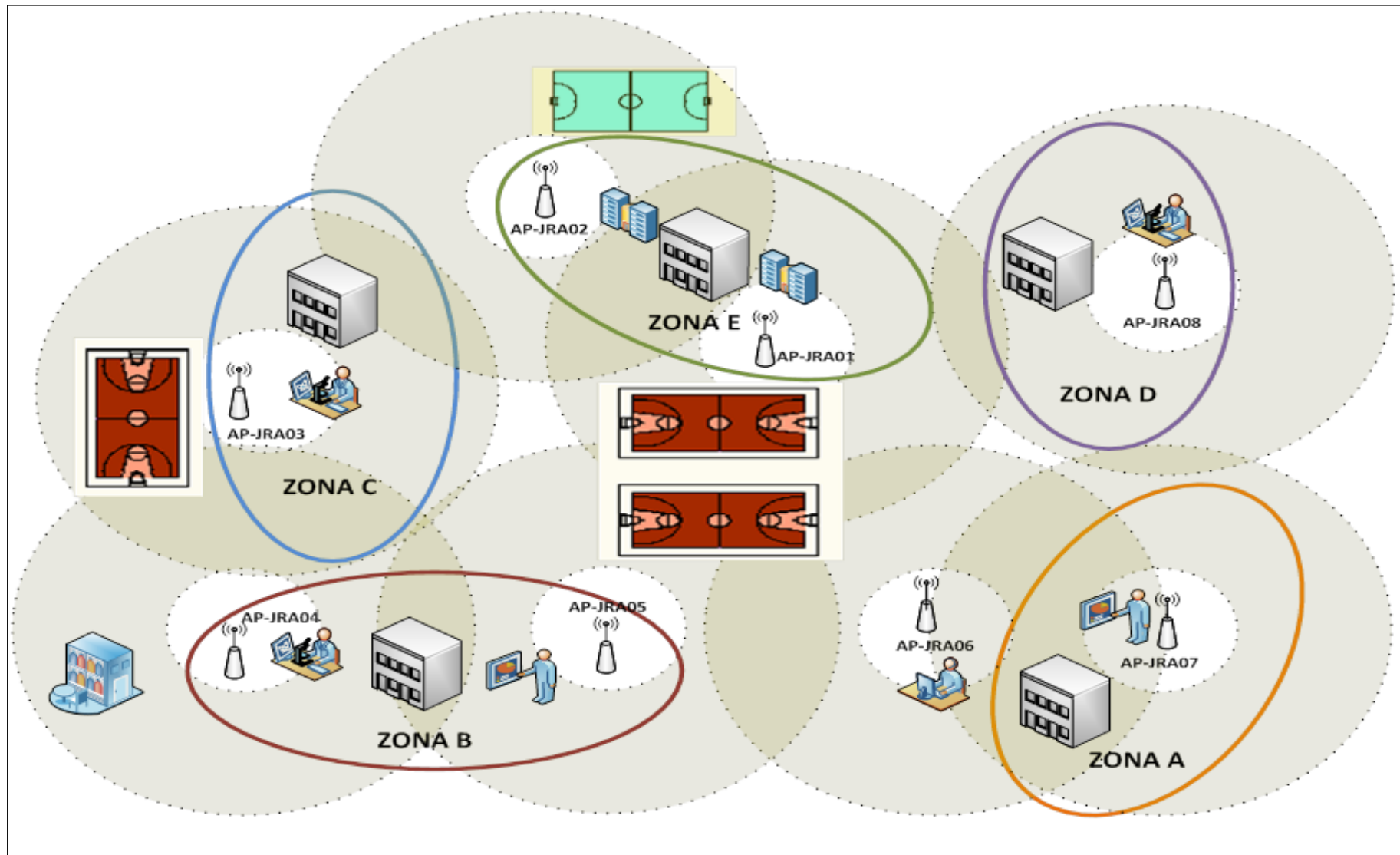


Figura 3. 12 Cobertura de la Red Inalámbrica

### 3.6.12.3 Áreas de Cobertura

Si bien ya se especificó los lugares a los cuales la WLAN debe proveer el servicio, aún no se tiene establecido el área en “m<sup>2</sup>” a cubrir en las diferentes zonas.

En base a los planos arquitectónicos de la Institución se determinó que la distancia máxima a cubrir es de 30 metros, por lo cual dispositivos a seleccionar deben tener una cobertura mayor o igual a la mencionada.

Por lo general el alcance de los *access-point* es de un radio de 100 metros teóricos, tomando en cuenta la degradación de la señal por las diferentes barreras que debe cruzar la misma.

Los equipos 802.11n se acoplan sin ningún problema a la distancia máxima, por lo cual se recomienda la adquisición de este tipo de dispositivos para la red inalámbrica.

### 3.6.12.4 Integración con la Red Cableada

La integración de la WLAN con red cableada debe ser con puntos de red específicos para ello, además de tener las respectivas tomas eléctricas para su alimentación, o en su defecto disponer la tecnología 802.3af (PoE<sup>41</sup>).

### 3.6.12.5 Parámetros de Operación

Al diseñar la red inalámbrica se debe tener en cuenta algunos parámetros importantes como son: velocidad de transmisión y frecuencia de operación.

Estos parámetros se encuentran estandarizados y se muestran en la tabla 3.43. En la actualidad el estándar 802.11n es aquel que ha tomado fuerza y el que cumple con los requisitos necesarios para este proyecto. .

---

<sup>41</sup> **PoE:** *Power over Ethernet*, permite que la alimentación eléctrica se suministre a un dispositivo de red usando el mismo cable que se utiliza para la conexión de red



Normas (capa física y de acceso al medio)	Velocidad transmisión máxima (Mbps)	Throughput máximo típico (Mbps)	Número máximo de redes localizadas	Banda de frecuencia	Radio de cobertura típico (interior)	Radio de cobertura típico (exterior)
IEEE 802.11a/h	54 Mbps	22 Mbps	14 (5.7 GHz)	5 GHz	85 m	185 m
IEEE 802.11b	11 Mbps	6 Mbps	3	2.4 GHz	50 m	140 m
IEEE 802.11g	54 Mbps	22 Mbps	3	2.4 GHz	65 m	150 m
IEEE 802.11n (40MHz)	> 300 Mbps	> 100 Mbps	1 (2.4 GHz) 7 (5.7 GHz)	5 GHz	120 m	300 m
IEEE 802.11n (20MHz)	144 Mbps	74 Mbps	3 (2.4 GHz) 14 (5.7GHz)	2.4 GHz 5 GHz	120 m	300 m

Tabla 3. 42 Estándares para redes inalámbricas [61]

### 3.6.12.6 Identificador SSID (*Service Set Identifier*) [62]

Es el nombre de la red *WiFi* que crea el punto de acceso. Por defecto suele ser el nombre del fabricante ("*3Com*" o "*Linksys*"), pero se puede cambiar y poner un nombre más intuitivo que haga referencia a la red como por ejemplo "*PerezWiFi*". En la tabla 3.44 se muestra los SSID de cada uno de los *access-point*.

Descripción	Ubicación	Departamento	SSID
AP-JRA01	Zona E	Lab Informática II	WLABII
AP-JRA02	Zona E	Lab Informática I	WLABI
AP-JRA03	Zona C	Inspección General	WING
AP-JRA04	Zona B	Lab PLC,s	WPLC
AP-JRA05	Zona B	Aula	WAULB
AP-JRA06	Zona A	Secretaría General	WSGN
AP-JRA07	Zona A	Aula	WAULA
AP-JRA08	Zona D	Salón Audiovisual	WAUDIO

Tabla 3. 43 SSID para los *access-point*

### 3.6.12.7 Seguridad en los Puntos de Acceso

La seguridad en un punto de acceso es algo a tener muy en cuenta, ya que al transmitir la información de modo inalámbrico la misma se vuelve más vulnerable y fácil de ser interceptada por entes maliciosos.

#### 3.6.12.7.1 WEP[63]

En un inicio la seguridad de las redes estuvo dada por WEP; su funcionamiento se basaba en cifrar los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire. Cuanto más larga sea la clave, más fuerte será el cifrado, cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos.

La activación del cifrado WEP de 128 bits evitará que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad. Sin embargo, si la clave de seguridad es estática o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo. Por lo tanto, se recomienda cambiar la clave WEP frecuentemente.

#### 3.6.12.7.2 WPA[63]

Con el propósito de superar las deficiencias de WEP aparece WPA que hace mucho más fuerte la seguridad de las redes inalámbricas.

WPA basa su funcionamiento en emplear el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente, lo que hace que las incursiones en la red inalámbrica sean más difíciles que con WEP. Es considerado como uno de los métodos con más altos niveles de seguridad inalámbrica para la red y es recomendado utilizarlo si el dispositivo es compatible con este cifrado

#### 3.6.12.7.3 WPA2

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, es compatible con los productos anteriores que son compatibles con WPA.

La principal diferencia entre WPA original y WPA2 es que la segunda necesita el estándar avanzado de cifrado (AES<sup>42</sup>) para los datos, mientras que WPA original emplea TKIP<sup>43</sup>. En la actualidad AES se ha posicionado como el mecanismo de cifrado más seguro dentro de las redes inalámbricas.

### 3.6.13 SELECCIÓN DE LOS *ACCESS POINT*

Una vez definidas las características principales de los *access-point*, se establece que los dispositivos a hacer parte del diseño de la red INTEGRADA de voz y datos debe tener al menos las características mostradas en la tabla 3.45.

<b>Access Point</b>	
<b>Parámetros</b>	<b>Características</b>
<b>Interfaces</b>	Ethernet RJ45
<b>Velocidad de Transmisión</b>	54 Mbps
<b>Algoritmos de Cifrado</b>	MD5, SHA, AES
<b>Mecanismos de Encriptación</b>	TKIP, WPA, WPA2
<b>Estándares</b>	IEEE 802.11x ; IEEE 802.11g ; IEEE 802.11n ; IEEE 802.3af ; IEEE 802.3u ; IEEE 802.1p ; IEEE 802.1q
<b>Administración</b>	GUI; SNMP

Tabla 3. 44 Características mínimas para los *access-point*

### 3.6.14 DISEÑO LÓGICO DE LA RED

Define la arquitectura de la red, es decir, cómo va a ser la comunicación entre los diferentes equipos pertenecientes a la red.

<sup>42</sup> **AES:** Estándar de Encriptación Avanzado.- Esquema de cifrado por bloques

<sup>43</sup> **TKIP:** Temporal Key Integrity Protocol.- Protocolo de seguridad utilizado por WPA

Es muy importante definir un correcto esquema lógico dentro del diseño de una red, ya que permitirá tener un concepto claro de cómo está funcionando la red y obtener el mayor rendimiento de la misma.

Para diseñar un correcto esquema lógico de existen algunas características importantes tales como: direccionamiento IP, generación de VLAN's, DMZ, entre otros.

### 3.6.15 DMZ [64]

En la seguridad informática una DMZ (Zona Desmilitarizada) se conoce como una red local que se ubica entre la red interna de una Organización y una red externa, por lo general Internet. La figura 3.13 muestra un ejemplo de DMZ.

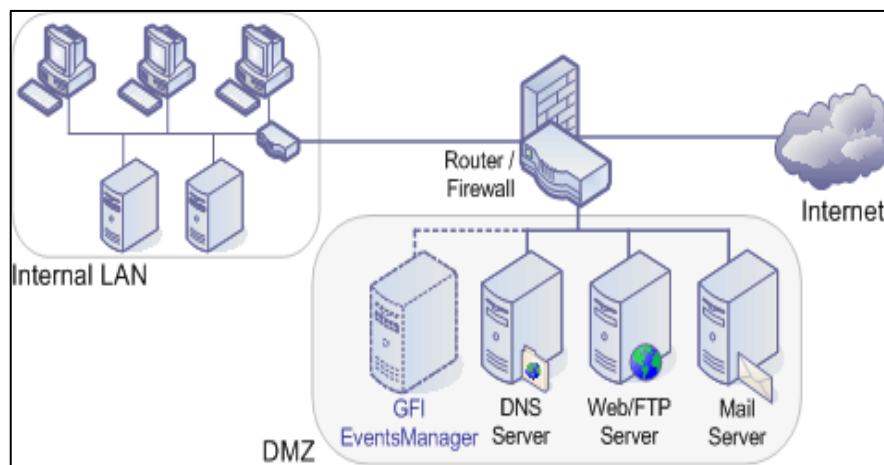


Figura 3. 13 Zona Desmilitarizada

El objetivo de la DMZ es que las conexiones internas y externas a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (*hosts*) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada.

La creación de la DMZ debe ir acompañada con un *firewall* ya que este dispositivo filtrará el tráfico a ingresar a la red; para el presente caso, se utilizará el *firewall* por defecto de Linux, que será manejado desde *WebMin* para proporcionar las reglas necesarias a la red.

### 3.6.15.1 Direccionamiento IP

El direccionamiento IP no es más que la asignación de una dirección IP a cada uno de los equipos de usuarios de la red para que se puedan utilizar los servicios que la red brinda. La red de la Unidad Educativa Temporal “Jaime Roldós Aguilera” cuenta con 204 puntos de voz y datos. Por ende se decide utilizar el esquema VLSM para la asignación de IPs a los diferentes puertos antes indicados.

Se escogió el esquema VLSM<sup>44</sup> ya que éste permite el ahorro de direcciones IP y la creación de una red lógica jerárquica. Para ello se partirá desde una IP privada clase B 172.24.0.0/24 para la LAN; mientras que para la DMZ se escoge la IP de clase A 10.0.0.0/24. Partiendo de estas direcciones IP y tomando en consideración el esquema VLSM se tienen las direcciones IP mostradas en la tabla 3.46.

VLAN	Subred	IP Inicial	IP Final	IP de Broadcast	IP Necesarias	IP Disponibles
Estudiantes	172.24.0.0/24	172.24.0.1	172.24.0.254	172.24.0.255	140	254
VoIP	172.24.1.0/27	172.24.1.1	172.24.1.30	172.24.1.31	28	30
Profesores	172.24.1.32/27	172.24.33	172.24.1.62	172.24.1.63	24	30
Empleados	172.24.1.64/28	172.24.1.65	172.24.1.78	172.24.1.79	13	14
Gestión	172.24.1.80/28	172.24.1.81	172.24.1.94	172.24.1.95	13	14
DMZ	10.0.0.0/28	10.0.0.1	10.0.0.14	10.0.0.15	8	14

Tabla 3. 45 Direccionamiento IP para la Unidad Educativa Temporal “Jaime Roldós Aguilera”

<sup>44</sup> **VLSM:** Variable Length Subnet Mask.- Método utilizado para optimizar el uso de direcciones IP.

### 3.6.15.2 VLAN`s [65]

Una VLAN (LAN Virtual) es un dominio lógico de *broadcast* que puede atravesar múltiples segmentos físicos de una LAN; dicho en otras palabras, permite que todos los miembros pertenecientes a una misma VLAN reciban cada uno de los paquetes enviados por miembros de la misma VLAN, pero no los paquetes enviados por miembros de una VLAN diferente. Se utilizan VLAN`s principalmente para:

- Segmentar y mejorar la calidad de la red
- Brindar flexibilidad a la red
- Seguridad

#### 3.6.15.2.1 VLAN Empleados

Será destinada al sector administrativo y docentes de la Institución, permitiendo información tal como: notas, oficios, notificaciones, etc.

Es muy importante generar esta VLAN para que el acceso a esta información solo sea para personal autorizado.

#### 3.6.15.2.2 VLAN Estudiantes

Los estudiantes es el mayor grupo dentro de la institución y los mismos deben tener acceso solo a la información deseada por las autoridades, es por ello importante tener una VLAN para ellos.

#### 3.6.15.2.3 VLAN Profesores

Permite el intercambio de información desde las distintas inspecciones, departamentos y laboratorios. Es creada principalmente para los docentes de la Institución.

#### 3.6.15.2.4 VLAN de Voz

Al transmitirse VoIP se requiere de una VLAN separada, debido a que el tráfico de voz requiere características como:

- Ancho de banda garantizado
- Prioridad en la transmisión
- Demoras mínimas (150 ms)

### **3.6.16 POLÍTICAS BÁSICAS DE SEGURIDAD PAR LA UNIDAD EDUCATIVA TEMPORAL “JAIME ROLDÓS AGUILERA”**

Existen normas internacionales como la ISO/IEC 27002 destinadas a proporcionar recomendaciones para la seguridad de la información dentro de una red, esta consiste en una *guía de buenas prácticas* describiendo los objetivos de control recomendables en cuanto a seguridad de la información. Tomando en consideración la flexibilidad que la norma brinda, se debe escoger cuáles de estos dominios pueden ser utilizados en cada organización.

La Unidad Educativa Temporal “Jaime Roldós Aguilera” ha decidido aceptar algunas de las recomendaciones para establecer sus políticas básicas de seguridad, con la finalidad de mantener protegida la información de los diferentes riesgos a los cuales puede ser susceptible.

Para esta labor se tomará cuenta tres factores muy importantes dentro de la red y los cuales se consideran necesarios para mantener una seguridad fiable dentro de la red, estos factores serán, seguridad física, seguridad lógica y políticas para los usuarios de la red.

#### **3.6.16.1 Seguridad Física de la UET “JRA”**

La seguridad física hace referencia a cómo mantener seguros los activos con los que cuenta la institución frente a eventualidades como robos, inundaciones, incendios, etc.

Aquí se debe hacer una diferenciación de los activos ya que pueden ser: equipos, documentos, *software*, entre otros. En base a esto se ha decidido sugerir a la institución los diferentes lineamientos.

- a) Cada estación de trabajo debe estar bajo custodia y responsabilidad del encargado del área.
- b) Las estaciones de trabajo, equipos de conectividad, servidores y demás dispositivos de red deben encontrarse en lugares cerrados, en el caso que en esa área de trabajo no se encuentre el usuario.
- c) La disposición física de los equipos no podrán ser manipulada por sus usuarios, sino por el área de encargada dentro de la Institución.
- d) La adquisición de nuevos equipos se lo debe realizar con garantía de índoles físicas como son: robos, incendios, inundaciones, etc.
- e) Se debe migrar la información escrita a archivos digitales.
- f) Se debe almacenar la información impresa en archivadores cerrados y bajo custodia.
- g) El acceso a la sala de equipos debe permanecer bajo llave y con acceso restringido por parte del área encargada de la Institución.
- h) El área de sistemas será el encargado de tener una bitácora de las personas que solicitaron permiso para ingresar a la sala de Equipos.

#### **3.6.16.2 Seguridad Lógica de la UET “JRA”**

La seguridad también debe ser proporcionada a nivel lógico, ya que la mayoría de los usuarios van a interactuar con la red. Para ello se debe implementar recomendaciones tales como:

- a) Se sugiere a las autoridades del plantel tener una red redundante, ya que si algún equipo sufre de algún daño o avería, la comunicación dentro de la Institución no se verá afectada.
- b) El administrador de la red, debe realizar mantenimientos periódicos a los equipos de red, verificando su correcto funcionamiento y así prevenir afectaciones a la red



- c) Se deben implementar contraseñas alfanuméricas a los usuarios de los diferentes servidores, las mismas que deberán actualizarse cada 3 meses.
- d) Se debe denegar el acceso remoto a conexiones inseguras.
- e) Monitorear y mantener correctamente actualizadas las VLAN's

### 3.6.17 ADMINISTRACIÓN DE LA RED [67]

La administración es un conjunto de técnicas para mantener una red operativa, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada. Para este propósito existen un sinnúmero de herramientas, mediante las cuales se puede monitorear constantemente la red, utilizando protocolos como: SNMP<sup>45</sup> y CMIP<sup>46</sup>.

El protocolo más utilizado para esta labor es SMNP, y las herramientas desarrolladas en base a este protocolo, definen los siguientes elementos.

- Dispositivos administrados
- Agentes

Un **dispositivo administrado** es aquel que contiene un agente SNMP y reside en una red administrada, éstos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP.

Los dispositivos administrados, a veces llamados elementos de red, pueden ser *routers*, servidores de acceso, *switches*, computadores o impresoras.

Un **agente** es un módulo de *software* de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

---

<sup>45</sup> **SNMP:** *Simple Network Management Protocol.- Protocolo de capa aplicación para utilizado para intercambiar información de administración.*

<sup>46</sup> **CMIP:** *Common Management Information Protocol.- Protocolo de administración de la red que define la comunicación entre aplicaciones de administración de red.*

Un **sistema administrador de red** (NMS) ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados.

Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red.

Para administrar la red a diseñar se utilizará el *software* de nombre NAGIOS XI, basado en código libre y en plataforma UNIX/ Linux.

Con esta herramienta se monitorearán los servidores de la red, para garantizar el correcto funcionamiento de la misma y en caso de haber dificultades, tomar los correctivos de manera rápida y eficiente.

## **CAPÍTULO 4**

### **ANÁLISIS DE COSTOS Y SIMULACIÓN DE LA RED INTEGRADA DE VOZ Y DATOS**

Una vez analizada la situación actual, y realizado el diseño de la Red INTEGRADA de Voz y Datos para la Unidad Educativa Temporal “Jaime Roldós Aguilera”, se quiere conocer si el diseño realizado brindará solución a las necesidades actuales y futuros requerimientos de la institución. Adicionalmente se requiere establecer un costo referencial para una futura implementación de la solución planteada en el presente proyecto.

Es por ello, que en este capítulo se analizarán los costos de dos de los más relevantes fabricantes de los elementos y equipos que se necesitan para el diseño establecido en el capítulo anterior, dentro de nuestro país; además se realizará la simulación de la red diseñada, con la finalidad de poder determinar si solventa los requerimientos actuales de la institución, y en caso de ser necesario, tomar los correctivos.

Se empezará realizando la simulación de la red INTEGRADA de voz y datos para lo cual se detallarán los elementos a ser utilizados, tanto de *hardware* como de *software*.

La simulación de la red permitirá determinar si el diseño es correcto y que en caso de querer ser implementado cumplirá los requisitos solicitados por la Unidad Educativa Temporal “Jaime Roldós Aguilera”.

#### **4.1 SOFTWARE A UTILIZAR PARA LA SIMULACIÓN**

Con la finalidad que la simulación sea lo más didáctica posible, en términos de *performance*, se ha decidido utilizar varias computadoras las cuales estarán destinadas a una tarea específica.

Cada una de estas computadoras, ya sean de escritorio o portátiles, contendrán el *software* establecido en el diseño de la red, y al final serán conectadas entre sí para las pruebas correspondientes; algunas de estas pruebas se efectuarán de manera independiente, debido a las limitantes que la simulación en sí presenta y por la gran cantidad de recursos que se necesitan, como es el caso de la Telefonía IP.

Otro de los factores importantes a mencionar es que el *software* a utilizar será instalado en diferentes Sistemas Operativos y de distintas maneras, brindando así una visión distinta en cada servidor; por ejemplo, existirán servidores levantados en distribuciones como Ubuntu y Centos, en sus versiones *desktop* como *server*.

Para poder utilizar estas distribuciones de Linux se hará uso de *VMWare*; programa que permite virtualizar diferentes Sistemas Operativos, y así poder tener más de un servidor en la misma PC.

En base a lo anteriormente indicado se procederá a detallar el *software* que se utilizará para la simulación de la red INTEGRADA de voz y datos.

#### **4.1.1 GNS3 (*Graphical Network Simulator*) [68]**

GNS3 es un simulador gráfico de red, permite elaborar topologías de red complejas y poner en marcha simulaciones sobre ellas. Principalmente fue desarrollado para simular IOS de *routers* Cisco, *ASA firewalls* y *juniper*, aunque con algunas configuraciones adicionales también existe la posibilidad de simular *Switching* Cisco.

Es un programa *Open Source*, y su principal función es poder emular a los dispositivos reales, agregando la mayoría de las características y funcionalidades de los mismos, como son: comandos, interfaces, etc. Este *software* está estrechamente vinculado con:

- **Dynamips**, que no es más que un emulador de IOS que permite a los usuarios ejecutar binarios de imágenes IOS de *Cisco Systems*.
- **Dynagen**, que es un *front-end* basado en texto para *Dynamips*

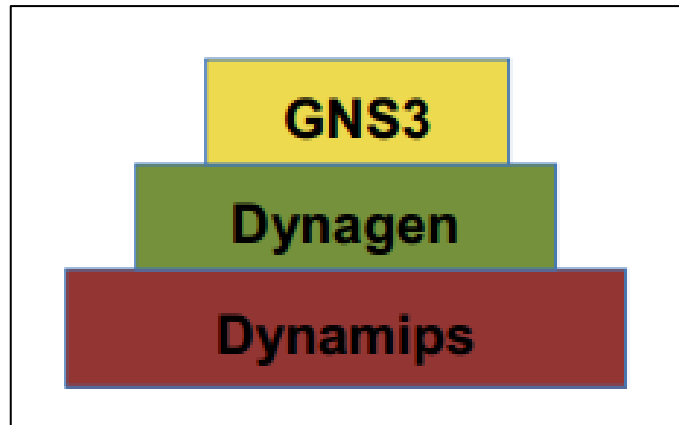


Figura 4. 1 Elementos de GNS3

#### 4.1.1.1 Ventajas del Simulador GNS3

GNS3 ofrece grandes ventajas en comparación a otros simuladores de red que existen en el medio, como por ejemplo el mismo *Packet Tracer*, propietario de Cisco; a continuación se detallarán las más relevantes:

- Es compatible con los Sistemas Operativos *Windows, Linux/Unix, MacOS*.
- Su código fuente es abierto
- Su interfaz de usuario es amigable y fácil de entender
- Trabaja con IOS de dispositivos reales
- Permite analizar la red simulada en tiempo real
- Conexión de la red simulada a un entorno real.
- Captura de paquetes integrada usando *Wireshark*

#### 4.1.1.2 Desventajas del Simulador GNS3

Así como GNS3 posee grandes virtudes, existen algunas particularidades que se podrían tomar como desventajas y que se indican a continuación.

- Su instalación puede resultar compleja, dependiendo del Sistema Operativo sobre el cual funcione.
- Consume gran cantidad de recursos en CPU y RAM
- Las imágenes de los IOS no vienen incluidas
- No provee todas las características para *Switching* a diferencia de *Routing* que si lo permite.

#### 4.1.1.3 Instalación de GNS3

Se instalará la herramienta GNS3 bajo el Sistema Operativo Windows 7, y dentro de ella se realizará la simulación de la red diseñada en el capítulo anterior. En el Anexo D se detalla el procedimiento correcto para la instalación y configuración básica de la herramienta GNS3 bajo el SO Windows 7.

#### 4.1.2 ZIMBRA SERVER [69]

Otra herramienta a utilizar para la simulación de la red INTEGRADA de voz y datos para la Unidad Educativa Temporal “Jaime Roldós Aguilera” es el servidor de Correo Electrónico *Zimbra*.

*Zimbra* es un servidor de mensajería de colaboración que permite compartir, almacenar y organizar mensajes de correo electrónico, citas, contactos, tareas, documentos y mucho más. Su interfaz intuitiva es una característica muy apreciada por los usuarios y administradores. La instalación de *Zimbra* se realizará en el Sistema Operativo Ubuntu Server 12.04. El proceso de instalación es sencillo pero se deben considerar algunos parámetros como la configuración del DNS. El proceso completo de instalación se lo presenta en el Anexo E.

#### 4.1.3 ASTERISK [70]

Asterisk es un programa de *software* libre que proporciona funcionalidades de una central telefónica.

Como cualquier PBX<sup>47</sup>, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI<sup>48</sup> tanto básicos como primarios.

En el presente proyecto se utilizará Asterisk para establecer el servicio de VoIP dentro de la Institución, y será instalado bajo Ubuntu Server 12.04, para lo cual se tiene una guía rápida de instalación en el Anexo F.

#### 4.1.4 WEBMIN [71]

*Webmin* es una herramienta de configuración de sistemas accesible vía web para Open Solaris, GNU/Linux y otros sistemas Unix.

Con *WebMin* se pueden configurar aspectos internos de muchos sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etc; así como modificar y controlar algunos servidores, como por ejemplo: Servidor Web Apache, PHP, MySQL, DNS, Samba, DHCP, entre otros.

Está construido a partir de módulos, los cuales tienen una interfaz a los archivos de configuración y al servidor *Webmin*.

Su mayor funcionalidad es brindar una interfaz gráfica al usuario, a la vez que facilita la configuración de los archivos correspondientes a los diferentes servicios, ahorrando tiempo y evitando la búsqueda de la ubicación de dichos ficheros dentro del sistema.

*Webmin* se utilizará para la configuración de los servidores más sencillos y en los cuales no se necesita de grandes recursos para la simulación establecida, entre ellos se tiene Servidor FTP, Servidor *Web*, *firewall*, etc.

---

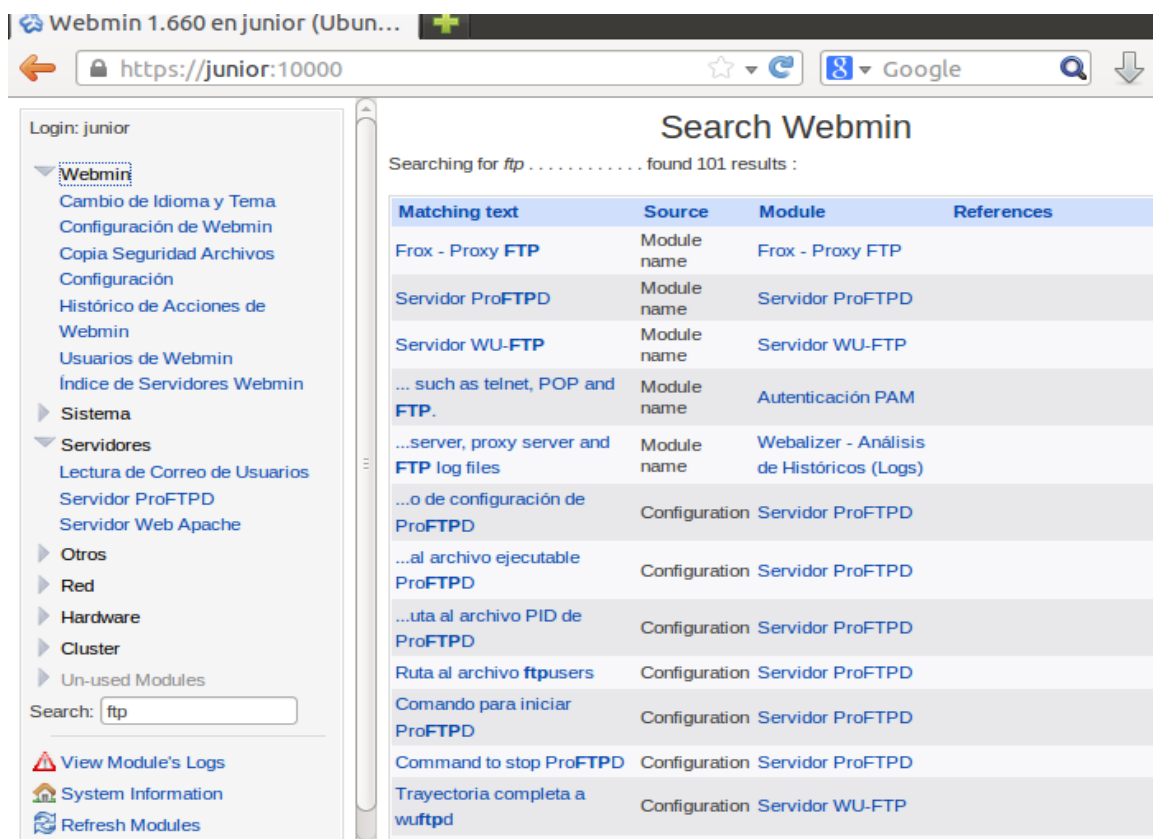
<sup>47</sup> **PBX:** *Private Branch Exchange*

<sup>48</sup> **RDSI:** *Red Digital de Servicios Integrados*

Dentro de *Webmin* se tiene el Servidor ProFTP para la transferencia de archivos, el Servidor *Web Apache*, y el *firewall* por *default* de los sistemas Linux *IPtables*. La instalación de esta herramienta es sumamente fácil y se encuentra detallada en el Anexo G.

#### 4.1.5 INSTALACIÓN DEL SERVIDOR PROFTP

La instalación de este Servidor en *Webmin* es muy sencilla. Para ello se entra al módulo administrador y en la opción buscar se ingresa FTP, desplegándose una lista de servidores FTP compatibles con *Webmin* entre ellos el Servidor *ProFT*. Esto se lo puede apreciar de mejor manera en la figura 4.2.



The screenshot shows the Webmin interface with a search for 'ftp'. The search results are as follows:

Matching text	Source	Module	References
Frox - Proxy FTP	Module name	Frox - Proxy FTP	
Servidor ProFTP	Module name	Servidor ProFTP	
Servidor WU-FTP	Module name	Servidor WU-FTP	
... such as telnet, POP and FTP.	Module name	Autenticación PAM	
...server, proxy server and FTP log files	Module name	Webalizer - Análisis de Históricos (Logs)	
...o de configuración de ProFTP	Configuration	Servidor ProFTP	
...al archivo ejecutable ProFTP	Configuration	Servidor ProFTP	
...uta al archivo PID de ProFTP	Configuration	Servidor ProFTP	
Ruta al archivo ftpusers	Configuration	Servidor ProFTP	
Comando para iniciar ProFTP	Configuration	Servidor ProFTP	
Command to stop ProFTP	Configuration	Servidor ProFTP	
Trayectoria completa a wuftp	Configuration	Servidor WU-FTP	

Figura 4. 2 Listado de Servidores FTP compatibles con Webmin

Una vez encontrado el servidor que se necesita se lo selecciona y éste será instalado dentro de *Webmin* en la pestaña Servidores, como lo muestra la figura 4.3.





Figura 4. 3 Servidor ProFTP

#### 4.1.6 INSTALACIÓN SERVIDOR WEB APACHE

Al igual que se realizó la búsqueda del servidor FTP dentro de *WebMin* se procede a encontrar el Servidor *Web Apache* como indica la figura 4.4 y se lo instala.

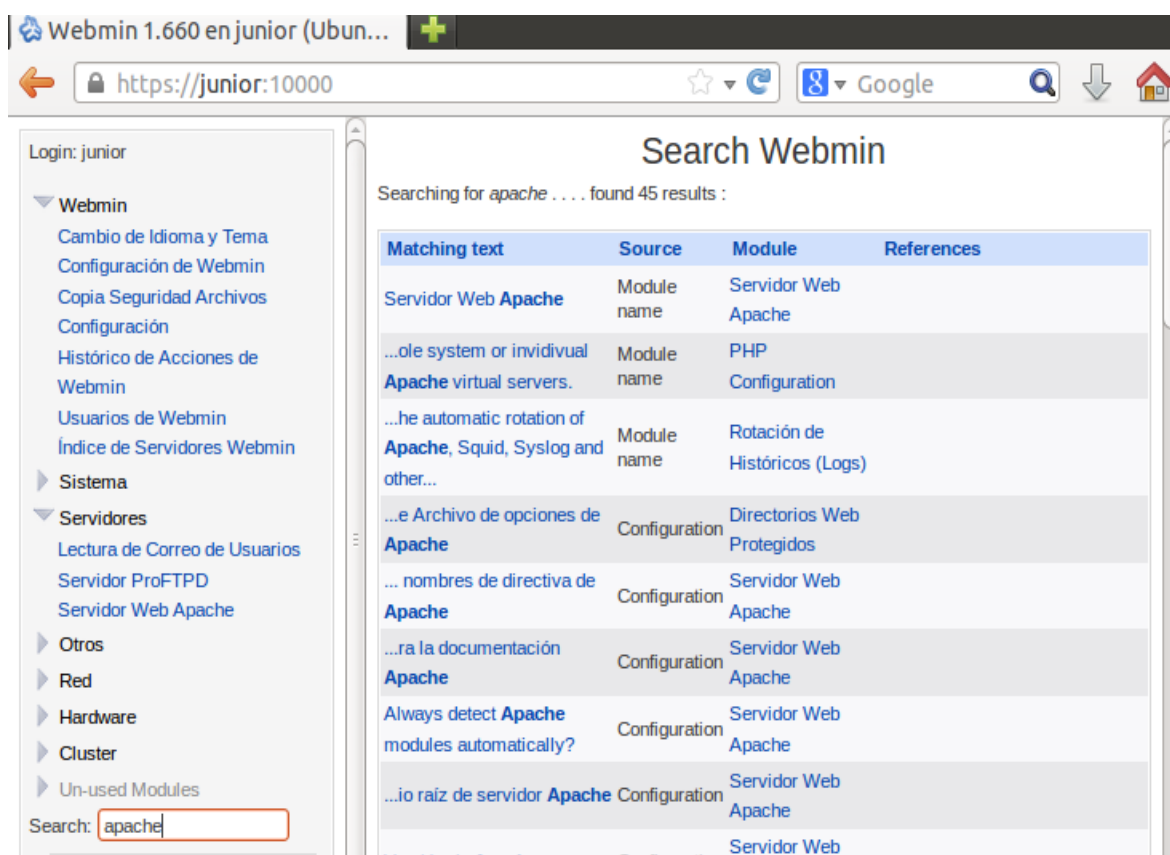


Figura 4. 4 Listado de módulos Apache compatible con Webmin

Una vez más para validar la correcta instalación del módulo se observa la opción Servidores y se valida que se encuentre el Servidor *Web Apache*, como lo muestra la figura 4.5.

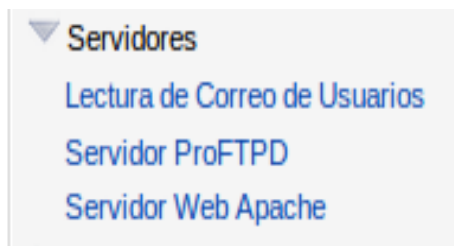


Figura 4. 5 Servidor Web Apache

#### 4.1.7 INSTALACIÓN DEL *FIREWALL IPTABLES*

*IPtables*, es por *default* el *firewall* de los sistemas Linux, por lo cual es instalado directamente con el Sistema Operativo. *Webmin* proporciona la facilidad de observar a este componente como un módulo y realizar las configuraciones de modo gráfico.

Como se muestra en la figura 4.6 se puede encontrar a los *IPtables* en la pestaña Red opción Cortafuegos Linux.



Figura 4. 6 Módulo *IPtables* / *Firewall* Linux

#### 4.1.8 NAGIOS XI [72]

Nagios es una herramienta de código libre orientada a la supervisión automática y continua de sistemas informáticos o *TIC's*<sup>49</sup>.

<sup>49</sup> **TIC's:** *Tecnologías de la Información y la Comunicación*

Está escrito bajo licencia GPL<sup>50</sup> y su principal función es observar el comportamiento de *host* (*server, switch, routers, impresoras, etc*), y servicios de red (*http, ssh, SQL<sup>51</sup>, etc*), con parámetros de comparación personalizables y escalables, que retornan diferentes reacciones como alertas vía correo electrónico, SMS, audibles, etc. Entre sus principales características se tiene:

- Supervisión Continua de la plataforma de TI
- Alertar a las personas encargadas de TI ante alertas preventivas (*Warning*) o críticas (*Critical*)
- Planificar mantenimiento del hardware o servicios
- Multiplataforma

Para este servidor se ha decidido utilizar la versión XI, la cual es pagada y tiene mayores prestaciones que la gratuita *Nagios Core*; sobre todo por la facilidad que presenta para el administrador de Red.

Se instalará Nagios XI en versión de prueba (60 días) en la distribución Centos Server; para ello se utiliza un paquete pre-configurado con Nagios, listo para instalar en *VMWare*. El proceso de instalación se muestra en la página oficial de Nagios y se lo puede apreciar de mejor manera en el Anexo H.

#### 4.1.9 VPCS (SIMULADOR VIRTUAL DE PC'S) [73]

*Virtual Simulator PC's* es una aplicación diseñada para *dynampis* de GNS3, su función es poder simular hasta 9 computadores e integrarlos con la topología desarrollada en GNS3. Estos PC virtuales permiten realizar pruebas dentro de la red simulada a través de los comandos como *ping* y *trace*, con la finalidad de corroborar conectividad entre los componentes de la red. La instalación del programa VPC's es una de los más sencillos a realizar en el presente proyecto, su proceso se muestra en el Anexo I.

---

<sup>50</sup> **GPL:** *General Public License.- Licencia ampliamente utilizada en el mundo del software; garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software.*

<sup>51</sup> **SQL:** *Structured Query Language.- Lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas*

## 4.2 SIMULACIÓN DE LA RED

Una vez instalados todos los elementos necesarios de la red, se procede con la simulación correspondiente. La simulación de la red se realiza utilizando el *software* antes mencionado tanto para el núcleo y servidores de la red. Debido a que el diseño incluye gran cantidad de dispositivos, la simulación será lo más simple posible, sin dejar de lado lo establecido en el capítulo anterior, como son: conceptos, definiciones, etc.

A continuación se muestran las configuraciones que se han realizado tanto en los *switches* como en los diferentes servidores para poder demostrar el funcionamiento de la red diseñada.

### 4.2.1 CONFIGURACIÓN DE UN SWITCH EN GNS3 [74]

Como ya se mencionó GNS3 fue diseñado con la finalidad prioritaria de simular dispositivos de capa 3, es decir, *routers*. El presente proyecto al ser el diseño de una LAN se hace indispensable el uso de *switches*, por lo cual lo primero que se debe hacer, es encontrar la manera de poder utilizar un *switch* dentro de GNS3.

En primera instancia la herramienta no permite cargar imágenes de IOS para *Switch Catalyst*, necesarios para la simulación de la red; a pesar de poseer dentro de sus módulos un *switch Ethernet*, éste resulta bastante básico y no permite realizar algunas configuraciones necesarias como creación de VLANs, servidor VTP<sup>52</sup>, etc.

A continuación se muestran los pasos para poder utilizar dentro de GNS3 un *switch* con más funcionalidades; para ello se tiene que usar el módulo de *Switching NM-16ESW* del *Router c3700*, del IOS *c3725-adventerprisek9-mz.124-15.T14.bin*, que permitirá tener entre el 50 y el 75 % de funciones de un *Switch Catalyst*.

---

<sup>52</sup> **VTP:** *VLAN Trunking Protocol*.- Protocolo de mensajes de nivel 2 utilizado para configurar y administrar VLANs en equipos Cisco

#### 4.2.1.1 Configuración de un *Router* en modo *Switch*

Lo primero que se debe hacer es cargar la imagen IOS del *Router* arrastrándola a la pantalla de GNS3, luego se da *click* derecho sobre el dispositivo y se selecciona la opción configurar tal como lo muestra la figura 4.7.

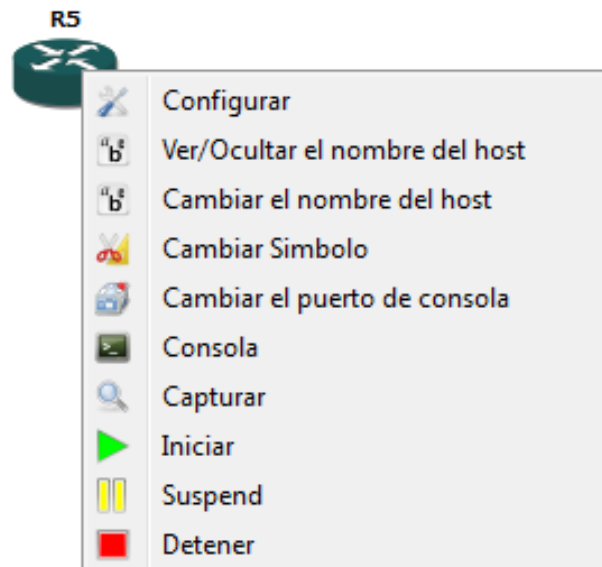


Figura 4. 7 Configuración del Router como *Switch*

Dentro de los *slots* que se observa en la figura 4.8, se escoge el módulo NM-16ESW y se lo acepta.

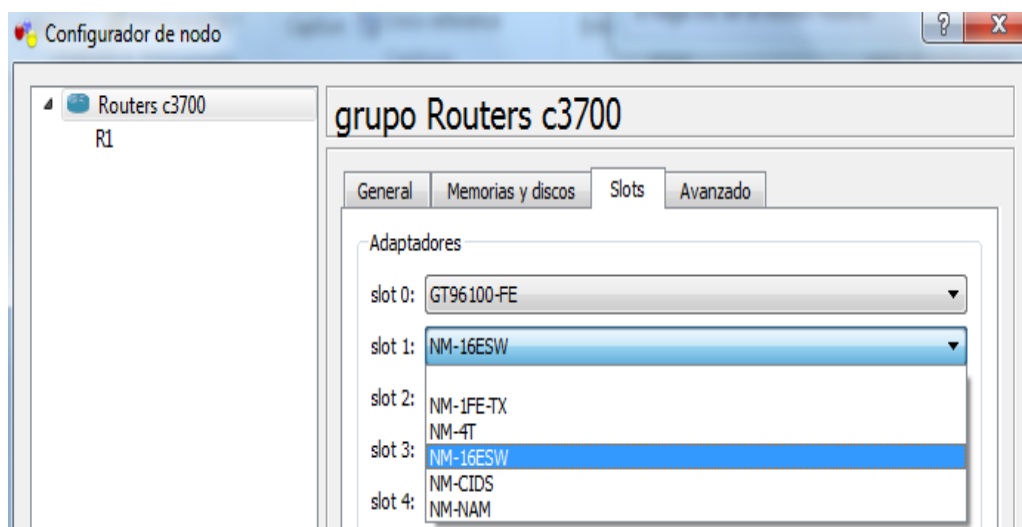


Figura 4. 8 Selección del módulo NM-16ESW

Una vez ocurrido esto se despliega el mensaje mostrado en la figura 4.9, que indica que se debe utilizar el modo manual para conectar el *switch* con algún otro componente; se da click en aceptar.

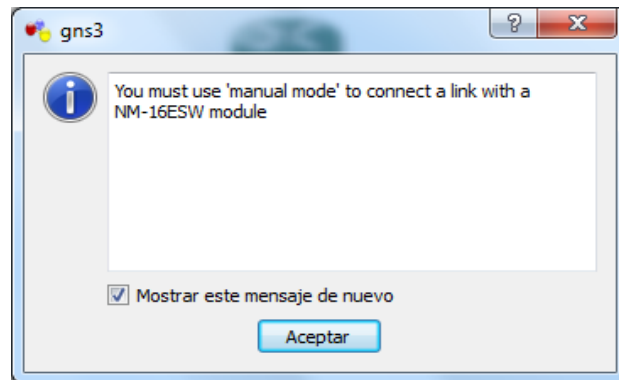


Figura 4. 9 Mensaje de Conexión para el *Switch*

Con estos cambios realizados se tendrá configurado el *router* como *switch* para utilizarlo dentro del proyecto; ahora para no causar confusiones se debe cambiar la imagen del *router* a la de un *switch*, para ello se selecciona desde la opción editar la pestaña *Symbol manager*, como lo muestra la figura 4.10.

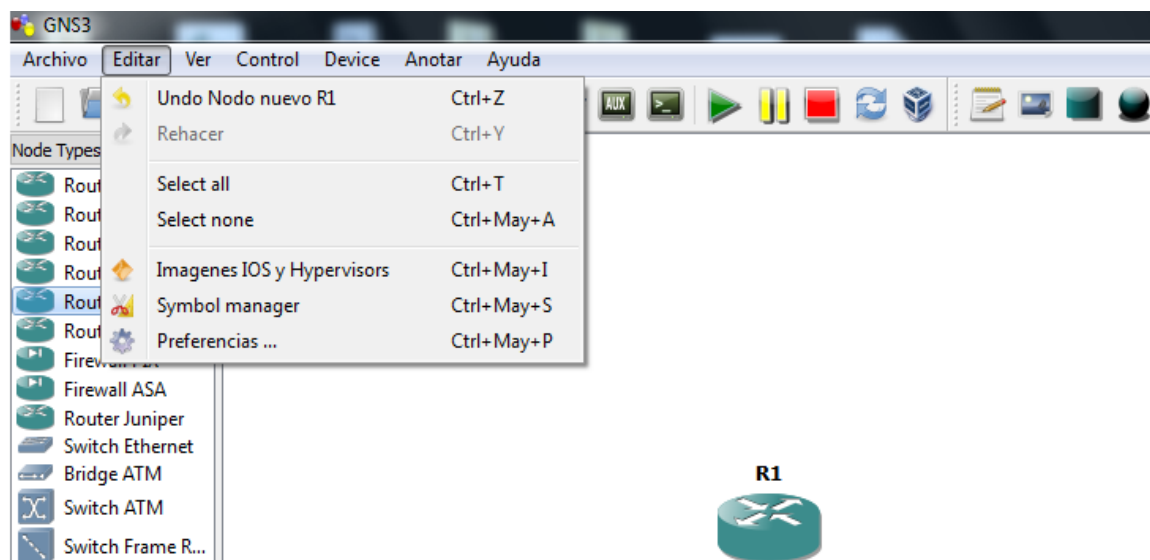


Figura 4. 10 Edición de símbolos en GNS3

Una vez dentro, y como muestra la figura 4.11, se selecciona un símbolo para el *switch* y se lo agrega; en el lado derecho se ingresa el nombre que se desea para el símbolo y se acepta.

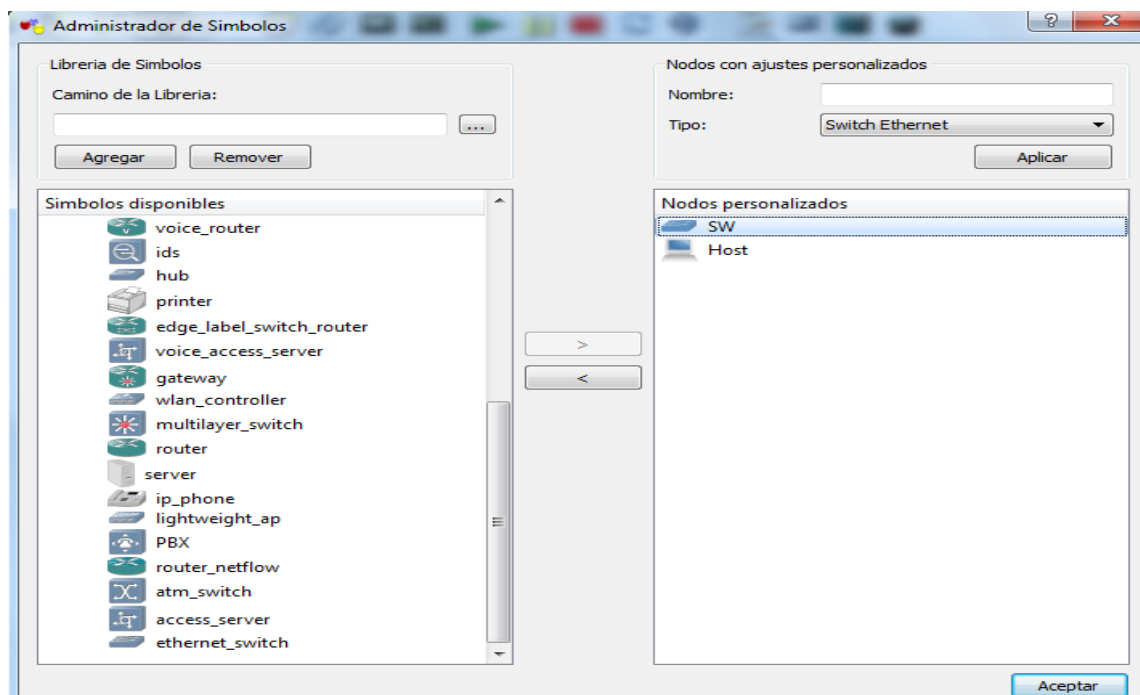


Figura 4. 11 Cambio de imagen para el nuevo *Switch*

Finalmente, la imagen agregada aparece en la lista de dispositivos y estará lista para ser utilizada, tal como lo muestra la figura 4.12.

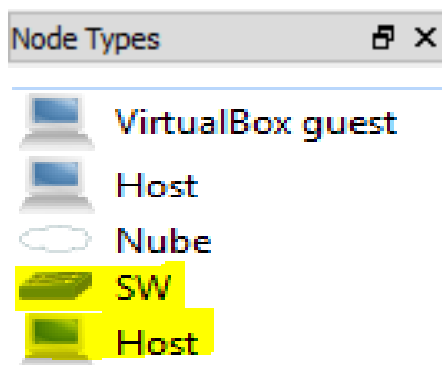


Figura 4. 12 Imagen de *Switch* agregada exitosamente

#### 4.2.1.2 Carga de los IOS para los *Switches*

Antes de realizar las configuraciones de los diferentes dispositivos, se debe cargar en GNS3 la imagen IOS que se desea utilizar, para ello se selecciona la opción Editar, pestaña imágenes IOS, y se indica a GNS3 la imagen que se va a utilizar y la ruta donde se encuentra la misma, como se indica en la figura 4.13.

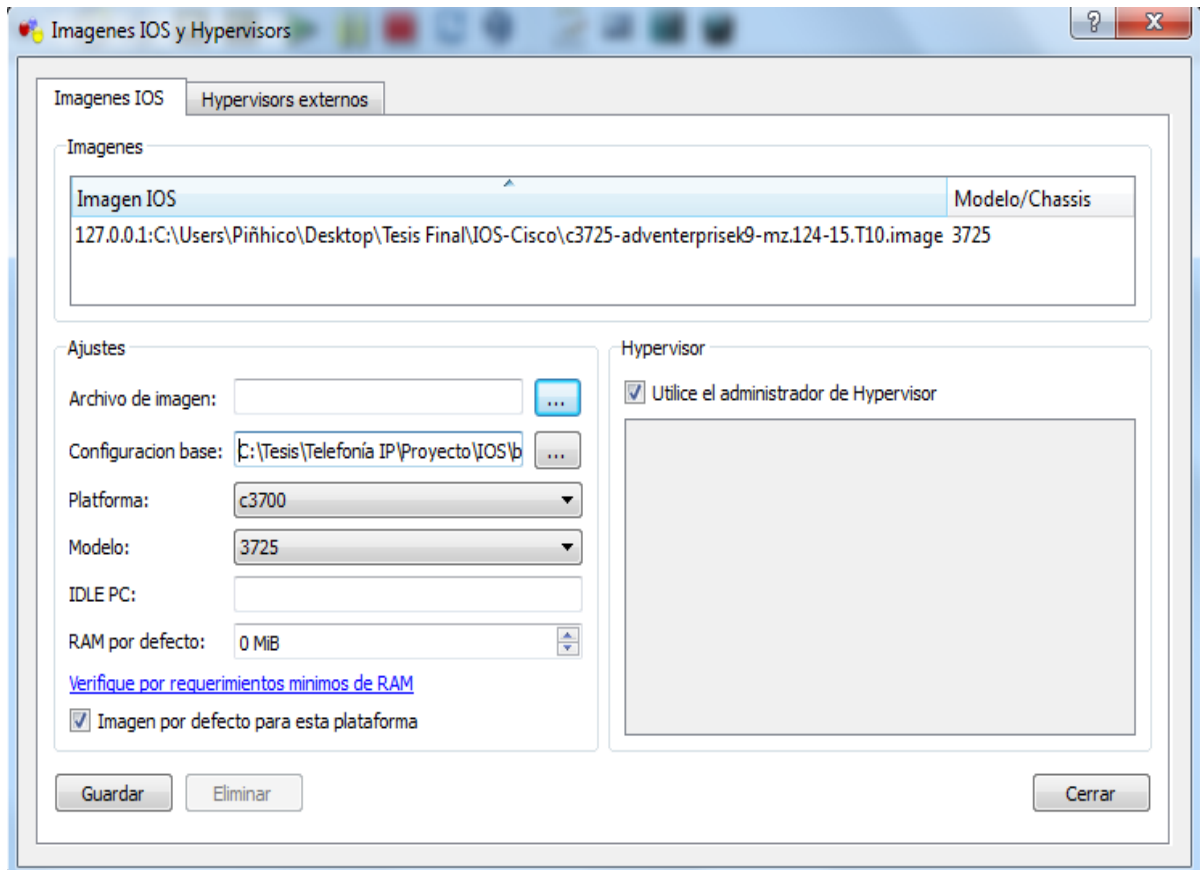


Figura 4. 13 Configuración para la carga de los IOS en GNS3

#### 4.2.2 TOPOLOGÍA A SIMULARSE

Una vez que están listos los elementos se procede a generar la topología de red a diseñar, para ello simplemente se arrastran los componentes de la red a la hoja de trabajo de GNS3 y se realizan las conexiones necesarias de acuerdo al diseño efectuado.

Una vez realizada la topología en GNS3 se establecen las configuraciones en los dispositivos, para lo cual simplemente se da *play* en la barra de tareas, y luego doble *click* en el elemento a configurar.

La figuras 4.14 y 4.15 muestran las topologías física y lógica a simularse en el presente proyecto.



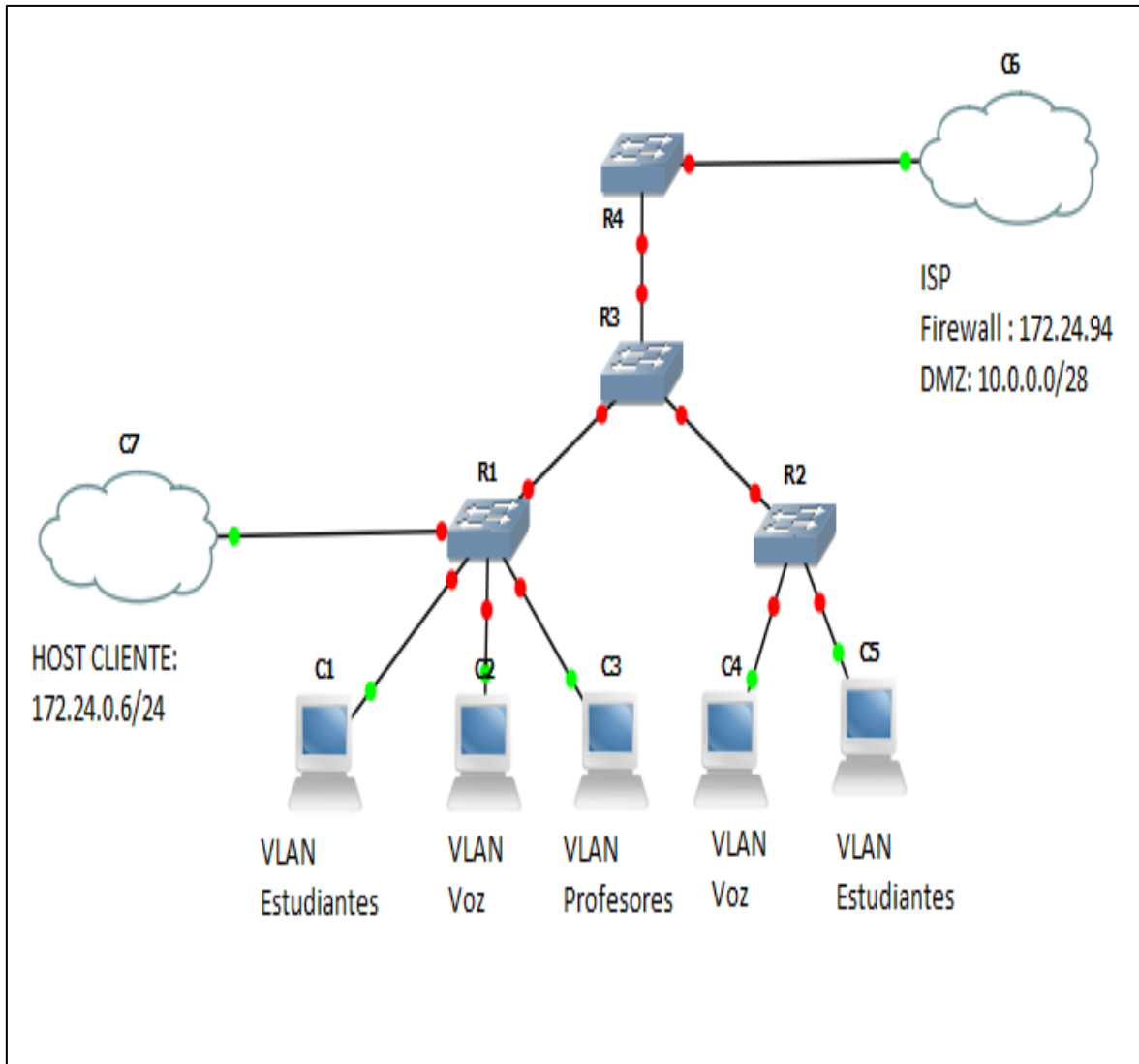


Figura 4. 14 Topología física a simularse

Donde:

R4: *Switches* de Core.

R3: *Switches* de Distribución

R1 y R2: *Switches* de Acceso

C6: Conexión hacia *Firewall* y DMZ

C7: *Host* cliente (para pruebas particulares)

C2 – C5: PCs Virtuales.

Cabe señalar que las configuraciones de los equipos serán realizadas como si fuese el caso real; es decir, existirán configuraciones redundantes, etc.

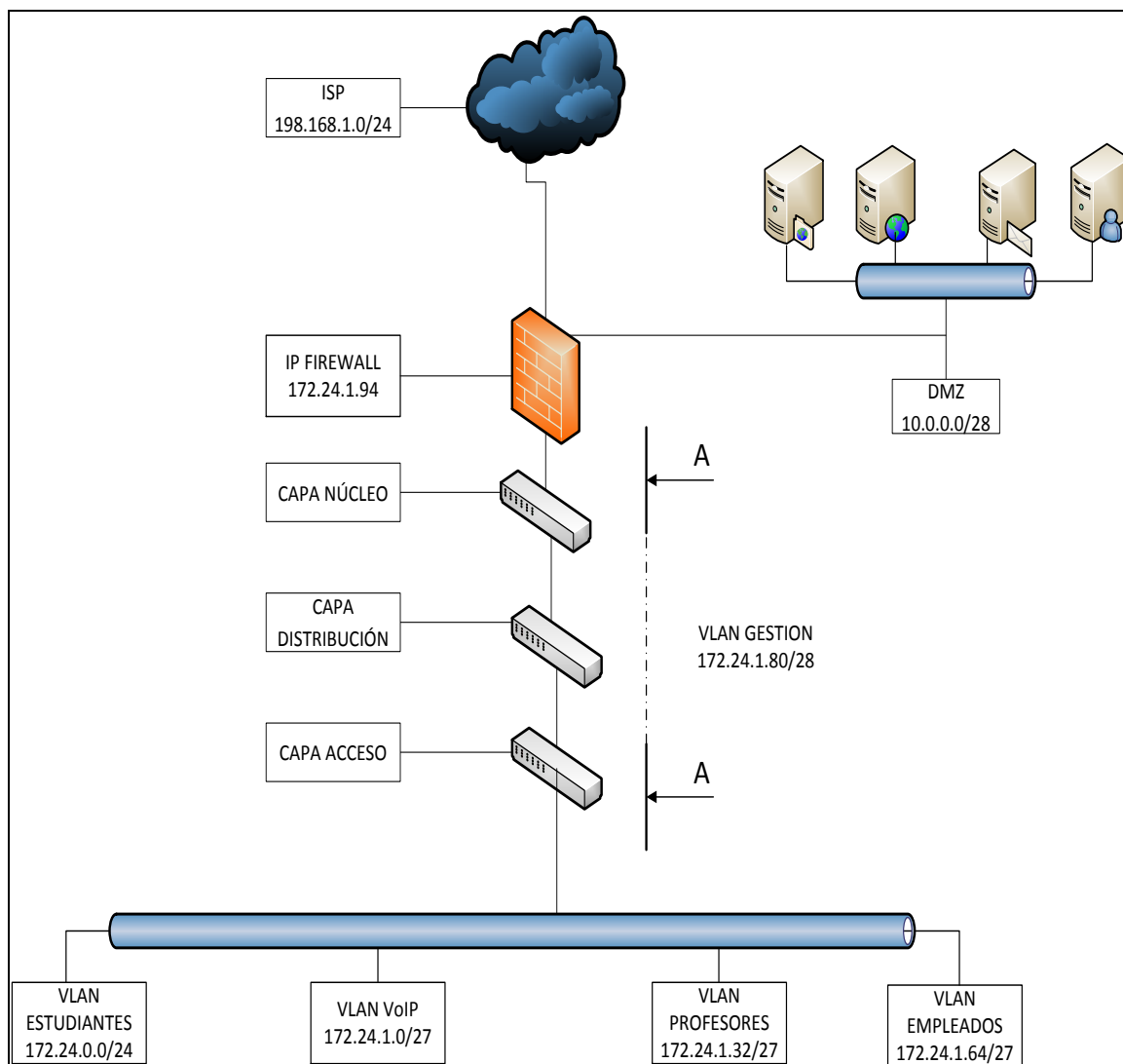


Figura 4. 15 Topología lógica a simularse

### 4.2.3 CONFIGURACIÓN BÁSICA DE LOS SWITCHES

Dentro de cada uno de los *Switches* de la red, indistintamente a la capa que pertenezcan, se deben realizar sus configuraciones básicas, esto con la finalidad de identificarlos de mejor manera y ofrecer ciertos niveles de seguridad y confidencialidad de acceso a los mismos.

Algunas de estas configuraciones son: nombre, *password*, cantidad de accesos remotos y demás; para este propósito se utilizan los comandos mostrados en la figura 4.16 dentro de la configuración global desde la línea de consola.

```

Connected to Dynamips VM "R1" (ID 0, type c3725) - Console port
Press ENTER to get the prompt.

R1#
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname SW-2
SW-2(config)#enable secret tesisjr
SW-2(config)#line console 0
SW-2(config-line)#pas junior
SW-2(config-line)#login
SW-2(config-line)#line vty 0 15
SW-2(config-line)#pass junior
SW-2(config-line)#login
SW-2(config-line)#

```

Figura 4. 16 Configuración básica de los Switches

El comando *enable secret (password)* encripta una contraseña del ingreso al modo EXEC, es decir al modo seguro, en este caso se ha seleccionado el *password tesisjr*.

El segundo comando *line console 0* permite poner contraseña a la línea de consola y así restringir el acceso a la misma, la sintaxis de todo el comando es la siguiente:

```

line console 0
password (contraseña a poner)
login

```

Finalmente el comando *line vty* es aquel que indica la cantidad de personas que pueden conectarse remotamente al dispositivo en caso de tener activada esta opción y se lo hace con las siguientes líneas de comandos.

```

line vty 0 15
password (contraseña a poner)
login

```

Otro comando muy utilizado en la configuración básica de un dispositivo es el *no ip domain-lookup* mostrado en la figura 4.17; su función es desactivar la traducción de nombres a dirección del dispositivo, ya sea éste un *router* o un *switch*, lo que libraría de la molestia de esperar varios segundos en caso de escribir una palabra que no es reconocida como comando.

```
SW-1(config)#no ip domain-lookup  
SW-1(config)#
```

Figura 4. 17 Desactivación de traducción de nombres

Una vez realizadas estas configuraciones básicas se procederá con las configuraciones propias de cada dispositivo, de acuerdo a la función a cumplir.

#### 4.2.4 CONFIGURACIÓN DE LOS *SWITCHES* DE ACCESO

Dentro de los *switches* de acceso se realizarán configuraciones como: brindar accesos a los puertos, ya sean para datos o voz, QoS para VLAN de voz, entre otras. Las configuraciones de este dispositivo se las puede observar en el Anexo J.

#### 4.2.5 CONFIGURACIÓN DE LOS *SWITCHES* DE DISTRIBUCIÓN

Dentro de los *switches* de distribución se tienen configuraciones referentes a servidor VTP para la distribución de VLANs, creación de rutas, *Spanning-tree*, etc. La configuración de estos dispositivos se la muestra en el Anexo K.

#### 4.2.6 CONFIGURACIÓN DE LOS *SWITCHES* DE CORE

Finalmente dentro de la capa de núcleo se realizarán las configuraciones como interfaces a la nube, *firewall*, DMZ. Dicha configuración se la puede apreciar de mejor manera en el Anexo L.

#### 4.2.7 CONFIGURACIÓN DE USUARIOS PROFTP

Para la configuración de los usuarios en FTP, lo primero que se debe realizar es crear los usuarios del servicio en el servidor, en el presente caso en Ubuntu. Para la simulación se procedió a crear los usuarios Profesores, Estudiantes y Secretaria como se puede apreciar en la figura 4.18.



Figura 4. 18 Usuarios FTP

Una vez creadas las carpetas de los usuarios se deben configurar los permisos para los usuarios del servidor ProFTP; este proceso se lo realiza en *Webmin*. Para ello se selecciona la opción servidores y Servidor ProFTP, en la que se disponen los ítems de configuración mostrados en la figura 4.19.

Dentro de cada uno de estos ítems se encontrarán configuraciones que tan solo con un *click* serán agregadas al archivo de configuración de ProFTP.



Figura 4. 19 Opciones de configuración del Servidor ProFTP

En el módulo opciones de red mostrada en la figura 4.20, se pueden definir parámetros como tiempo de conexión, sesiones concurrentes, tiempo de desconexión, etc.

Índice de Módulo

## Opciones de Red

**Opciones de Red**

Máximas sesiones concurrentes  Defecto  30

Tipo de servidor

Tiempo sin hacer nada antes de desconectar  Defecto  1200 segundos

Tiempo a esperar por primera transferencia  Defecto  600 segundos

Figura 4. 20 Configuración de las Opciones de Red del Servidor ProFTP

Otro archivo importante a configurar es el de control de acceso, donde se pueden seleccionar *banners* para *login* correcto o incorrecto, etc. Esto se muestra en la figura 4.21.

Índice de Módulo

## Control de Acceso

Apply Changes  
Stop ProFTPd

**Control de Acceso**

¿No pregunto por clave de acceso si se deniega el login?  Si  No  Defecto

Mensaje de fallo de login  Defecto  Error de Autenticación

Mensaje de login con éxito  Defecto  ¡Bienvenido JRA!

Regex autorizadas de comandos FTP  Defecto

¿Permito sobrescribir archivos?  Si  No  Defecto

Regex de comandos FTP denegados  Defecto

Salvar

Figura 4. 21 Control de Acceso para el Servidor ProFTP

En la figura 4.22 se detalla la opción Autenticación, donde se puede definir los tipos de *login* que se pueden hacer, contraseñas para grupos, o qué usuarios serán tratados como anónimos, y varios mensajes para el usuario del servidor.

Indice de Módulo Autenticación [Apply Changes](#) [Stop ProFTPD](#)

### Autenticación

¿Permito hacer login a root?  Si  No  Defecto

Grupos en los que tratar a los miembros como anónimos  Defecto

¿Sólo permito hacer login a usuarios con alias?  Si  No  Defecto

Archivo de mensajes de pre-login  Ninguno

Demasiados archivos de mensajes de conexión  Ninguno

Archivo de mensajes de post-login  Ninguno

Archivo de mensajes de logout  Ninguno

Claves de acceso de grupo	Grupo Unix	Clave de acceso
<input type="text"/>	<input type="text"/>	<input type="text"/>

Máximos fallos de login por sesión  Defecto  3

¿Sólo permitir login a usuarios con shell válidos?  Si  No  Defecto

¿Denegar a usuarios en archivo `/etc/ftpusers`?  Si  No  Defecto

Alias de nombre de usuario	Nombre de usuario de login	Nombre de usuario real
<input type="text"/>	<input type="text"/>	<input type="text"/>

Claves de acceso de usuarios	Usuario Unix	Clave de acceso
sobrepasa	<input type="text"/>	<input type="text"/>

Salvar

Figura 4. 22 Autenticación de Usuarios en el Servidor ProFTP

En caso de querer denegar el servicio a ciertos usuarios se tiene el archivo usuarios de FTP negados, donde simplemente se añaden los usuarios que se desea no puedan acceder al servicio. En la figura 4.23 se tiene como ejemplo la negación del servicio al usuario *root*.

Indice de Módulo Usuarios de FTP denegados [Apply Changes](#) [Stop ProFTPD](#)

Si activado bajo el icono de Autenticación, a los usuarios listados debajo desde el archivo `/etc/ftpusers` se les denegará el acceso por login al usuario FTP.

```
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).
root
daemon
bin
sys
sync
games
man
lp
mail
```

Salvar

Figura 4. 23 Usuarios denegados en el Servidor ProFTP

Por último se tiene el archivo `proftpd.conf`, que se muestra en la figura 4.24 y es utilizado en caso de que el administrador prefiera hacer uso de este archivo antes que las configuraciones gráficas.

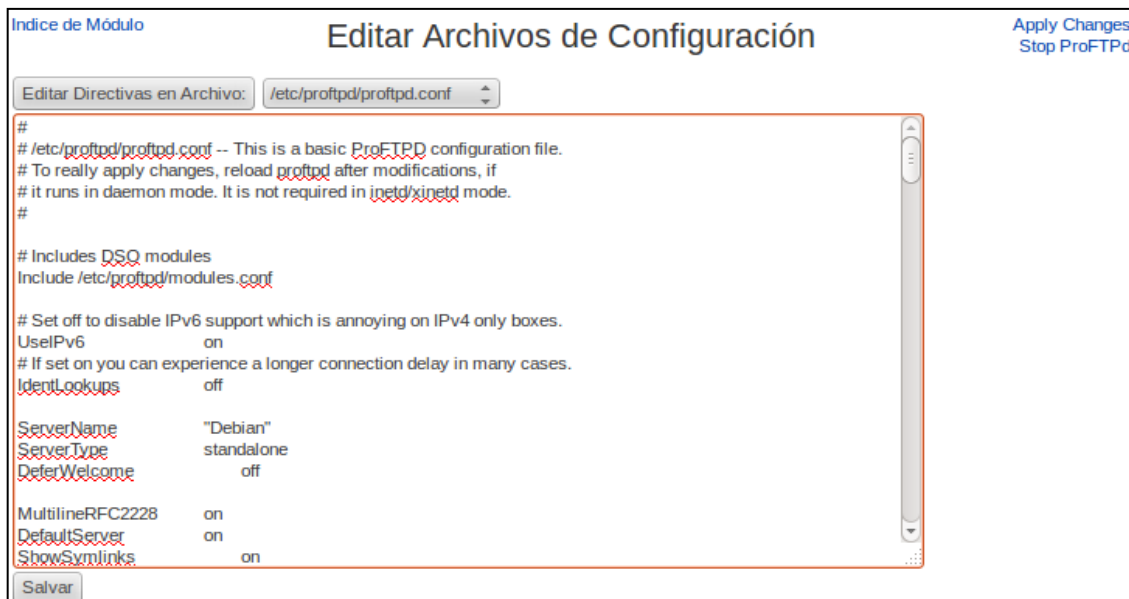


Figura 4. 24 Archivo proftpd.conf

## 4.2.8 CONFIGURACIÓN DEL SERVIDOR WEB

Para la configuración del Servidor *Web*, se ingresa a la pestaña servidores, y se selecciona Servidor Apache; aquí se observa una pestaña crear *host virtual*, y se da *click* en ella, desplegándose la ventana mostrada en la figura 4.25.

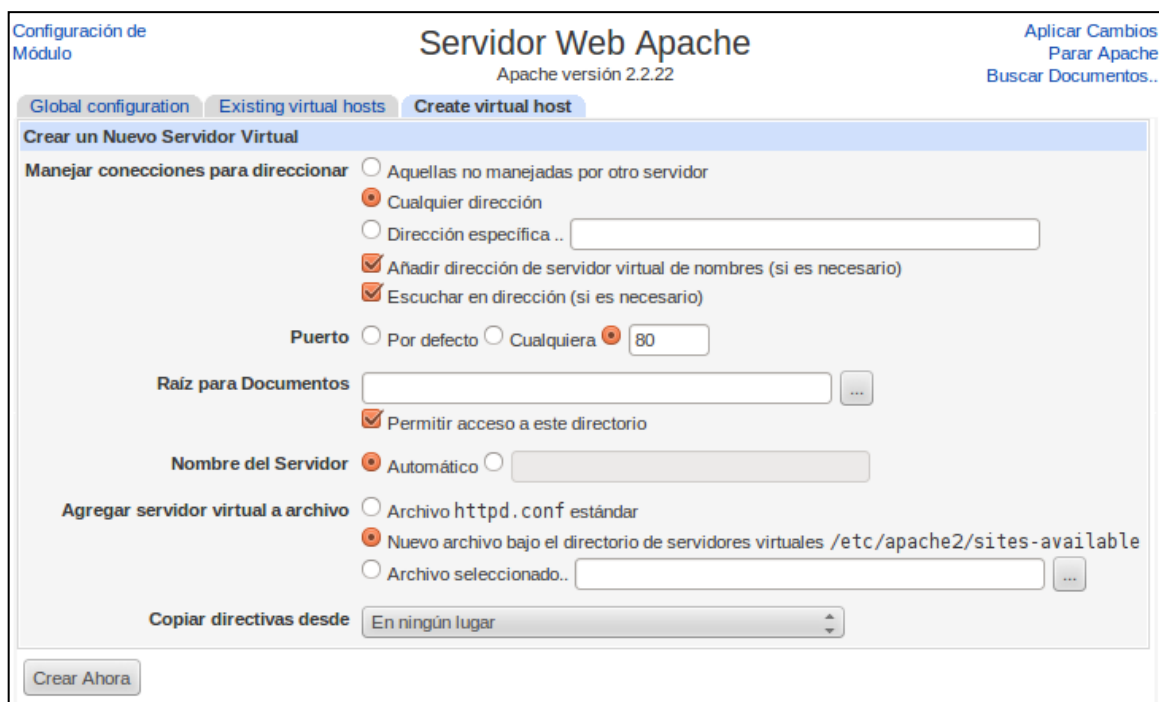


Figura 4. 25 Configuración *host* Virtual Servidor Web Apache



Una vez dentro de la opción se ingresan los campos necesarios como la IP del servidor, para este caso la 10.0.0.1/28 y la dirección del documento donde se encuentra la página web de la Institución. Para el presente proyecto y a modo de ejemplo será la dirección home/junior/descargas/www/prueba, ya que se ha descargado un formato de página web modelo para las pruebas correspondientes, como se lo muestra la figura 4.26.

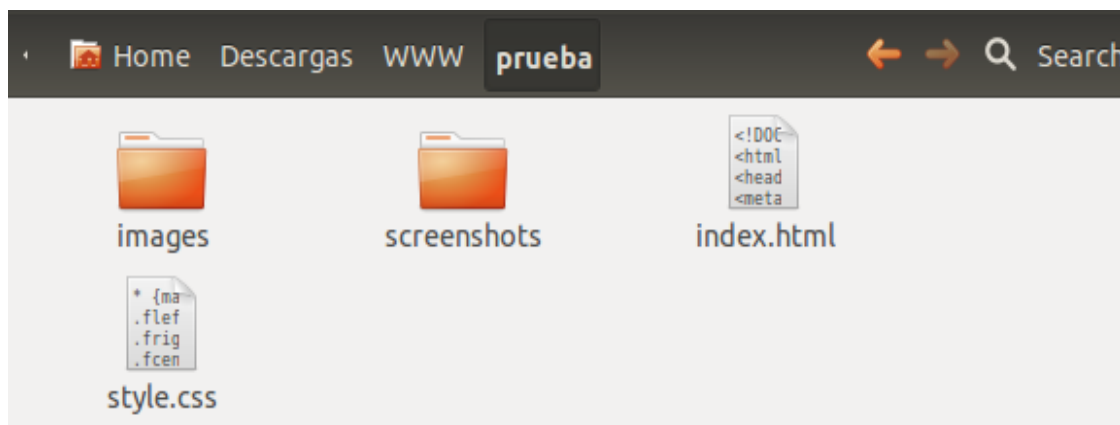


Figura 4. 26 Plantilla de prueba para el servidor web Apache

Finalmente, después de crear el *host*, el servidor estará activado y listo para las pruebas correspondientes, como se lo puede evidenciar en la figura 4.27.



Figura 4. 27 Creación exitosa del *host* virtual

## 4.2.9 CONFIGURACIÓN DEL SERVIDOR ZIMBRA

Una vez instalado el servidor de correo Zimbra se realizarán las configuraciones necesarias para que los diferentes usuarios puedan utilizar la herramienta.

### 4.2.9.1 Creación de Usuarios

Primeramente se crean los usuarios, para ello se ingresa a la página de *ZimbraAdmin*, donde se tienen las opciones mostradas en la figura 4.28.



Figura 4. 28 Administración de Zimbra

Dentro de la ventana se debe seleccionar la opción administrar y dar *click* a la opción nuevo usuario, desplegándose así la ventana mostrada en la figura 4.29, para las configuraciones del nuevo usuario.

Figura 4. 29 Configuración de un nuevo usuario en Zimbra

Finalmente una vez que se han creado los usuarios, se pueden realizar los envíos necesarios entre los diferentes usuarios de la red. En el presente proyecto se han creado los correos de secretaría general y del autor del proyecto, [secretaria@mail.jra.net](mailto:secretaria@mail.jra.net) y [jorge.ramon@mail.jra.net](mailto:jorge.ramon@mail.jra.net) respectivamente.

#### 4.2.10 CONFIGURACIÓN NAGIOS XI

Al ser un *software* pagado la configuración de Nagios XI en comparación de Nagios Core es sumamente sencilla e intuitiva, tomando en consideración qué es lo que se desea monitorear y cómo se lo va a realizar.

A continuación se presentan dos ejemplos de configuración para la simulación correspondiente. El primero consiste en monitorear un *host*, para este caso el *host* cliente de IP 172.24.0.6/24 perteneciente a la VLAN estudiantes, y el monitoreo de un servicio para uno de los *switches* de acceso.

##### 4.2.10.1.1 Monitoreo del host Cliente

Para monitorear un *host* dentro de Nagios hay que dirigirse a la pestaña *configure* encontrada de la página principal y luego acceder a la consola CCM (*Core Configure Manager*) como se muestra en la figura 4.30.

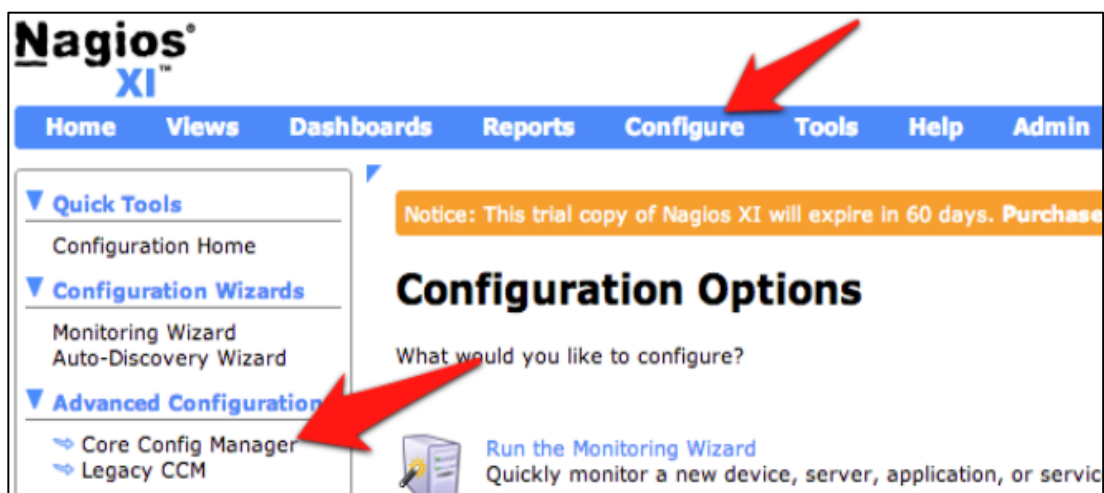






































Figura 4. 30 Consola *Core Configure Manager*

Una vez dentro de la consola, se puede observar en el lado izquierdo la opción *monitoring*, y debajo de ella la opción *host*. En esta opción se procede a ingresar el *host* que se desea monitorear, para ello se debe dar *click* a la opción *add new*, como se lo puede apreciar en la figura 4.31.

Check All

	Host Name	Alias	Active	Sync Status	Actions	ID
<input type="checkbox"/>	FSRVTSTDC1.focuscorptest.local	FSRVTSTDC1.focuscorptest.local	Yes	Sync Missed	   	731
<input type="checkbox"/>	FSRVTSTDC2.focuscorptest.local	FSRVTSTDC2.focuscorptest.local	Yes	Sync Missed	   	730
<input type="checkbox"/>	FSRVTSTGISAPP1.focuscorptest.local	FSRVTSTGISAPP1.focuscorptest.local	Yes	Synced To File	   	734
<input type="checkbox"/>	FSRVTSTGISAPP2.focuscorptest.local	FSRVTSTGISAPP2.focuscorptest.local	Yes	Synced To File	   	735
<input type="checkbox"/>	FSRVTSTGISSVC1.focuscorptest.local	FSRVTSTGISSVC1.focuscorptest.local	Yes	Synced To File	   	727
<input type="checkbox"/>	FSRVTSTGISSVC2.focuscorptest.local	FSRVTSTGISSVC2.focuscorptest.local	Yes	Synced To File	   	728
<input type="checkbox"/>	FSRVTSTGISSVC3.focuscorptest.local	FSRVTSTGISSVC3.focuscorptest.local	Yes	Synced To File	   	732
<input type="checkbox"/>	FSRVTSTGISSVC4.focuscorptest.local	FSRVTSTGISSVC4.focuscorptest.local	Yes	Synced To File	   	733
<input type="checkbox"/>	FSRVTSTWSUS1.focuscorptest.local	FSRVTSTWSUS1.focuscorptest.local	Yes	Synced To File	   	726

Add New Apply Configuration With Checked:  Go

Figura 4. 31 Creación de nuevo *host*

Dentro de la opción Nuevo se desplegará una ventana con datos a completar como IP, nombre del *host*, y qué comando se va utilizar para el monitoreo del *host*. Para el ejemplo será un *host-alive* como se puede apreciar en la figura 4.32.

### Host Management

Common Settings Check Settings Alert Settings Misc Settings

**Common Settings**

Host Name\*  
SW-ACC

Description  
Switch Acces

Address\*  
172.24.1.82

Display name

Manage Parents

Manage Templates

Manage Hostgroups

Save Abort

\* required

Check command  
check-host-alive

Active

Command view  
\$USER1\$/check\_icmp -H \$HOSTADDRESS\$ -w 3000.0,80% -c 5000.0,100% -p 5

\$ARG1\$

\$ARG2\$

\$ARG3\$

\$ARG4\$

\$ARG5\$

\$ARG6\$

\$ARG7\$

\$ARG8\$

Test Check Command

Figura 4. 32 Configuraciones generales de monitoreo del *host*

En las siguientes opciones se puede configurar la frecuencia para el *check* del *host*, a quién se debe notificar en caso de existir problemas, etc. Finalmente se guarda y con ello el *host* estará monitoreado por el sistema Nagios XI.

#### 4.2.10.1.2 Monitoreo de un Servicio

El proceso de monitoreo de un servicio es muy similar al de un *host*, con la diferencia conceptual de que un servicio está “corriendo” dentro de un *host*, por ende lo primero que se debe realizar es crear un *host* y ligar el servicio a monitorear al *host* creado.

Para el ejemplo, se va a monitorear un servicio del *switch* de acceso, más concretamente una de sus interfaces. Para esto nuevamente hay que dirigirse a la consola CCM, pero esta vez se debe seleccionar la opción *service*, desplegándose la ventana mostrada en la figura 4.33.

The screenshot displays the 'Service Management' interface in Nagios XI. It features a navigation bar with tabs for 'Common Settings', 'Check Settings', 'Alert Settings', and 'Misc Settings'. The 'Common Settings' tab is active, showing a form for configuring a service. The form includes the following fields and controls:

- Config Name\*:** SW-ACC
- Description\*:** Switch de Acceso
- Display name:** (empty)
- Check command:** check\_xi\_service\_ifoperstatus
- Active:**
- Command view:** \$USER1\$/check\_ifoperstatus -H \$HOSTADDRESS\$ -C \$ARG1\$ -k \$ARG2\$
- Arguments:**
  - \$ARG1\$: public
  - \$ARG2\$: 1
  - \$ARG3\$: -v 2
  - \$ARG4\$:
  - \$ARG5\$:
  - \$ARG6\$:
  - \$ARG7\$:
  - \$ARG8\$:
- Buttons:** Manage Hosts, Manage Templates, Manage Hostgroups, Manage Servicegroups, Save, Abort, Test Check Command
- Legend:** \* required

Figura 4. 33 Configuraciones generales del servicio a monitorear

Dentro de esta ventana se configura el nombre del servicio y el comando a utilizar, teniendo mayor precaución ya que cada comando tiene su formato establecido, por ejemplo:

```
Check_ifoperstatus -H $hostaddress$ -C $ARG1$ -k $ARG2$
```

Donde los argumentos significan lo siguiente:

H: *hostaddress* (será tomada del host relacionado al servicio)

C: *Community* (para el ejemplo será PUBLIC)

K: 0 ó 1 (Muestra si el comando está activo o no)

V: Versión del comando SNMP (Versión 2)

También se pueden seleccionar la frecuencia del monitoreo y opciones complementarias. Una vez determinado el servicio a monitorear, se debe mapear el *host* ya creado al nuevo servicio; para ello se escoge la opción *Manage Host*, y en la ventana de la figura 4.34 se selecciona el *host* al cual se desea monitorear el servicio creado, en el ejemplo el *host* SW-ACC, con esto Nagios XI estará monitoreando el servicio creado.



Figura 4. 34 Asignación del servicio al *host* a monitorear.

## 4.2.11 CONFIGURACIÓN DE ASTERISK

Después de la instalación de servidor Asterisk, se deben editar varios archivos de configuración para poder establecer el servicio dentro de la red.

A continuación se muestran las configuraciones básicas y los archivos que se deben editar para poder proveer del servicio de voz a la red.

### 4.2.11.1 Configuración del fichero sip.conf

En este archivo se realizan configuraciones relacionadas con el protocolo SIP y la adición de nuevos usuarios o la interconexión de Asterisk con otros proveedores SIP. En la figura 4.35 se muestran los parámetros principales establecidos para el servidor.



```
*sip.conf X
[general]
context=telefonos ip
allowguest=no
language=es
srvlookup=yes
enable=yes
udpbinaddr=10.0.0.5
tcpenable=no
qualify=yes
allowtransfer=yes
language=es
rtptimeout=60
rtpholdtimeout=300
directmedia=no
dtmfmode=rfc2833
insecure=invite,port
callcounter=yes
```

Figura 4. 35 Configuración general del fichero sip.conf

En este archivo también se definen los parámetros para cada usuario; en el presente caso se tienen los contextos teléfonos ip, para las extensiones a utilizar, tanto para teléfonos ip como para *softphones* y sus configuraciones se pueden observar en la figura 4.36

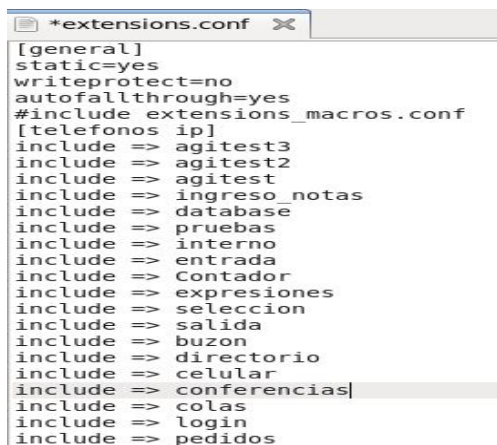


<pre>[telefono-interno](!) type=friend context=telefonos ip host=dynamic secret=tesisasterisk disallow=all allow=ulaw,alaw,gsm qualify=yes nat=no</pre>	<pre>[softphone](!) type=friend context=telefonosip host=dynamic secret=tesisasterisk disallow=all allow=ulaw,alaw,gsm qualify=yes nat=no</pre>
---	---

Figura 4. 36 Configuración de canales SIP

#### 4.2.11.2 Configuración del fichero extensions.conf

El archivo *extensions.conf* quizás sea el archivo más importante de Asterisk, su función principal es definir el *dial plan* (plan de numeración) que seguirá la central para los contextos antes establecidos en el sip.conf y por tanto para cada usuario. En la figura 4.37 se observan los privilegios que se han establecido para el contexto teléfonos ip.



```
*extensions.conf
[general]
static=yes
writeprotect=no
autofallthrough=yes
#include extensions_macros.conf
[telefonos ip]
include => agitest3
include => agitest2
include => agitest
include => ingreso_notas
include => database
include => pruebas
include => interno
include => entrada
include => Contador
include => expresiones
include => seleccion
include => salida
include => buzon
include => directorio
include => celular
include => conferencias
include => colas
include => login
include => pedidos
```

Figura 4. 37 Permisos generales para el contexto teléfonos IP

Dentro del archivo *extension.conf* se puede definir el plan de numeración para cada contexto, como por ejemplo, el contexto pruebas. Como se puede apreciar en la figura 4.38 el *dial plan* para el contexto interno va desde la extensión [200 – 219] ó [300 – 319]. Mientras que para el contexto pruebas, se tienen extensiones como la 500 o 600, donde se podrán escuchar mensajes precargados por Asterisk.



```

[interno]
exten => _[23][01]X,1,Macro(buzonvoz,SIP,telefono,curso)

[pruebas]
exten => 500,1,Playback(demo-congrats)
exten => 500,2,Hangup()

exten => 600,1,Playback(demo-echotest)
exten => 600,2,Echo()
exten => 600,3,Playback(demo-echodone)
exten => 500,4,Hangup()

exten => 501,1,Answer()
exten => 501,n,SayUnixTime(,ABdY \'digits/at\' KM)
exten => 501,n,Hangup()
exten => 502,1,Goto(pruebas2,s,1)

exten => 503,1,Answer()
same => n,Wait(2)
same => n,Record(/tmp/grabacion:wav,2,8)
same => n,Wait(2)
same => n,Playback(/tmp/grabacion)
same => n,Wait(2)
same => n,Hangup()

```

Figura 4. 38 *Dial-Plan* para el contexto Interno y Pruebas

Otro contexto muy utilizado dentro de Asterisk es *ivr\_menu* donde se define de forma escrita los mensajes que se le indicarán al usuario para poder comunicarse con las diferentes extensiones. En la figura 4.39 se puede observar el mensaje pre-grabado que el usuario escuchará al comunicarse a la Unidad Educativa Temporal “Jaime Roldós Aguilera”

```

[ivr_menu]
exten => s,1,Answer()
exten => s,n,Set(TIMEOUT(digit)=5)
exten => s,n,Set(TIMEOUT(response)=5)
exten => s,n,Wait(1)
exten => s,n(menu),Festival(Usted se ha comunicado con el colegio Jaime Roldos Aguilera si conoce el numero de extension
marquela ahora caso contrario espere)
exten => s,n,Waitexten(5)

exten => 201,1,Goto(interno,201,1)
exten => 201,n,Hangup()

exten => 301,1,Goto(interno,301,1)
exten => 301,n,Hangup()

```

Figura 4. 39 Configuración Contexto IVR\_MENU

Una vez configurados estos archivos se procede a realizar las pruebas correspondientes, mediante el uso de *softphones* instalados en el pc cliente 172.24.0.6 ó *smartphones*.

#### 4.2.12 CONFIGURACIÓN DEL *FIREWALL* DE LINUX

La configuración del *firewall* se realizará de manera gráfica mediante el uso de *Webmin*. Lo que se configura dentro del *firewall* son las reglas que deben cumplir los paquetes que desean ingresar o salir de la LAN a la DMZ o a su vez al Internet.

Este tipo de reglas deben ser realizadas por la persona encargada del área de *networking* de la institución, y que tenga pleno conocimiento de la topología tanto física como lógica de la red, para no generar bloqueos o permisos no deseados a los miembros de la red.

Algunos ejemplos de estas reglas se pueden apreciar en la figura 4.40.

Seleccionar todo. | Invertir selección.

Acccion	Condicion	Mover	Añadir
<input type="checkbox"/> Aceptar	Si interfaz de entrada es <b>eth1</b> y output interface is <b>eth0</b> y el estado de conexion es <b>RELATED,ESTABLISHED</b>	↓	↓ ↑
<input type="checkbox"/> Aceptar	Si interfaz de entrada es <b>eth1</b> y output interface is <b>not eth2</b> y el estado de conexion es <b>ESTABLISHED,RELATED</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si interfaz de entrada es <b>eth2</b> y output interface is <b>eth0</b> y el estado de conexion es <b>RELATED,ESTABLISHED</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si interfaz de entrada es <b>eth0</b> y output interface is <b>eth1</b>	↓ ↑	↓ ↑

Figura 4. 40 Reglas del *firewall*

Para la simulación se han establecido las reglas en base a los puertos, sin embargo, esto puede ser realizado en base a direcciones IP, subredes, etc. Para crear una regla nueva, se ingresa a *Webmin* pestaña red, opción Cortafuegos Linux. Una vez desplegada la ventana del cortafuegos, se tiene la opción de añadir regla, como se muestra en la figura 4.41.

Índice de Módulo

## Añadir regla

**Detalles de cadena y acción**

Parte de la cadena Paquetes redirigidos (FORWARD)

Rule comment

Acción a ejecutar  No  Aceptar  Denegar  Reject  Userspace  Salir de cadena

hacer nada  Log  Ejecutar cadena

packet

La acción seleccionada abajo solo será llevada a cabo si **todas** las condiciones de aquí se cumplen.

**Detalles de condición**

dirección o red origen <Cualquiera>

Dirección o red de Destino <Cualquiera>

Interfaz entrante <Cualquiera> eth1

Interfaz saliente <Cualquiera> eth1

Fragmentación  Cualquiera  Esta fragmentado  No esta fragmentado

Figura 4. 41 Configuración de reglas en el *firewall*

En esta pantalla se pueden elegir las acciones que van a tomarse con los paquetes entrantes, permitir establecimientos de comunicación, denegarlos, rechazarlos, etc.

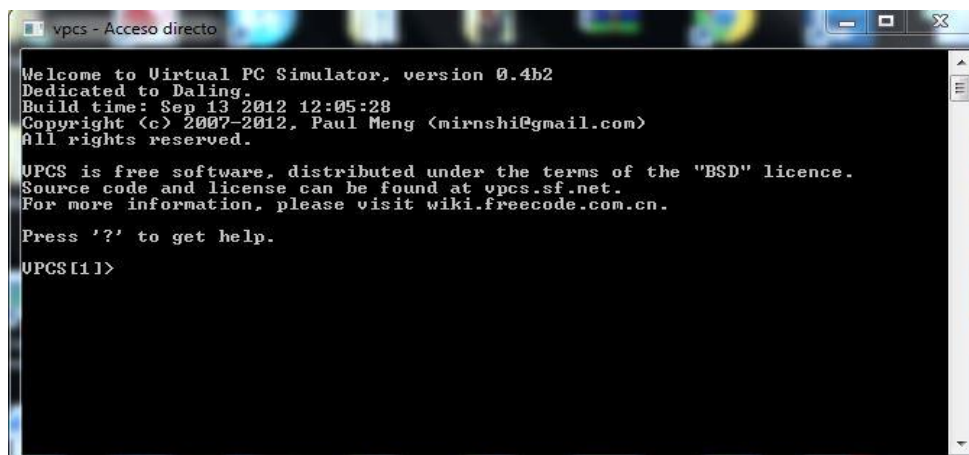
Una vez establecidas todas las reglas, lo que se debe realizar es la conexión de los equipos que intervienen en la red, y validar si efectivamente las reglas añadidas están proporcionando el acceso que se desea.

#### 4.2.13 CONFIGURACIÓN DE LOS PC VIRTUALES [75]

Al trabajar con topologías o laboratorios de redes, es de gran utilidad disponer de uno o varios *hosts/pc* virtuales para realizar pruebas de conectividad (*ping*, *traceroute*).

Obviamente para este tipo de pruebas no se necesita una máquina virtual completa (*Qemu/Virtualhost*) sino un *host* que simplemente permita ejecutar los comandos antes mencionados. Para ello se utiliza *Virtual PC Simulator*; VPCS está disponible para Linux y *Windows*, una vez instalado está listo para utilizarlo. Sin embargo, se debe realizar cierta configuración dentro de GNS3 para la integración con VPCS, esta configuración se muestra a continuación.

Lo primero a realizar es abrir la línea de comando *Shell* de VPCS, como se muestra en la figura 4.42.



```
vpcs - Acceso directo
Welcome to Virtual PC Simulator, version 0.4b2
Dedicated to Daling.
Build time: Sep 13 2012 12:05:28
Copyright (c) 2007-2012, Paul Meng <mirnshi@gmail.com>
All rights reserved.

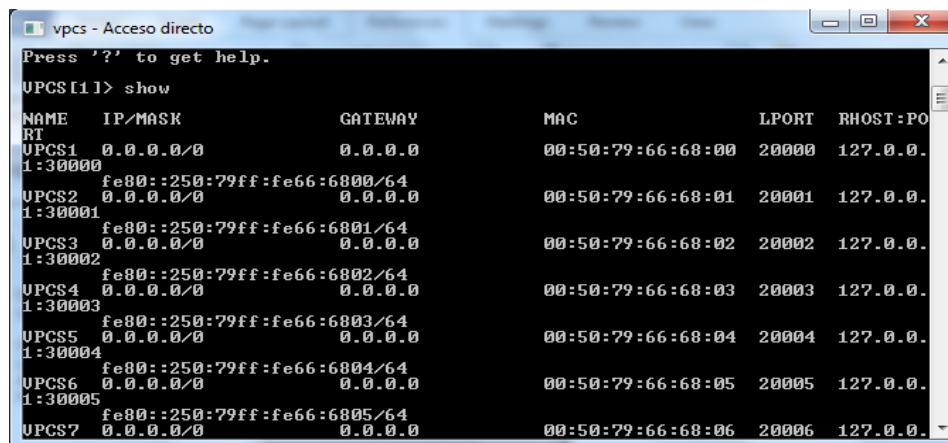
UPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

UPCS[1]>
```

Figura 4. 42 *Shell* de VPCS

Para saber con cuántas PCs virtuales se cuenta, se debe ejecutar el comando *show* y se desplegará la lista que se muestra en la figura 4.43.



```
vpcs - Acceso directo
Press '?' to get help.

UPCS[1]> show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PO
RT
UPCS1 0.0.0.0/0 0.0.0.0 00:50:79:66:68:00 20000 127.0.0.
1:30000
fe80::250:79ff:fe66:6800/64
UPCS2 0.0.0.0/0 0.0.0.0 00:50:79:66:68:01 20001 127.0.0.
1:30001
fe80::250:79ff:fe66:6801/64
UPCS3 0.0.0.0/0 0.0.0.0 00:50:79:66:68:02 20002 127.0.0.
1:30002
fe80::250:79ff:fe66:6802/64
UPCS4 0.0.0.0/0 0.0.0.0 00:50:79:66:68:03 20003 127.0.0.
1:30003
fe80::250:79ff:fe66:6803/64
UPCS5 0.0.0.0/0 0.0.0.0 00:50:79:66:68:04 20004 127.0.0.
1:30004
fe80::250:79ff:fe66:6804/64
UPCS6 0.0.0.0/0 0.0.0.0 00:50:79:66:68:05 20005 127.0.0.
1:30005
fe80::250:79ff:fe66:6805/64
UPCS7 0.0.0.0/0 0.0.0.0 00:50:79:66:68:06 20006 127.0.0.
```

Figura 4. 43 Lista de PC virtuales

Como se observa cada una de las PC virtuales posee su propio puerto y es gracias a ello que se podrá hacer la integración con GNS3. Una vez realizado esto, se ingresa a GNS3 y se da *click* derecho en uno de los PCs a utilizar, seleccionando la opción *Configure*; luego en la pestaña *NIO UDP*, se llenan los campos solicitados para que GNS3 pueda mapear cada uno de los PC a una interfaz de red virtual, estos campos se pueden apreciar en la figura 4.44.

Para el primer PC el valor por defecto es 1, así que para el noveno PC se debe sumar 8 al puerto local y al *remote port*.

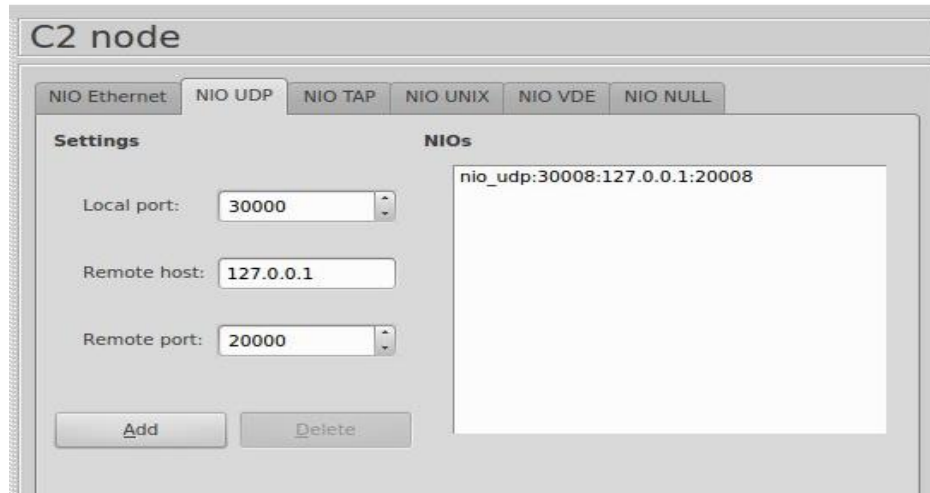


Figura 4. 44 Mapeo de los *host* virtuales con su respectivo puerto

Una vez realizado el proceso antes mencionado, es posible realizar pruebas como *ping* y *trace* desde los *host* virtuales, para ello se debe asignar una IP a los mismos mediante la sentencia mostrada en la figura 4.45.

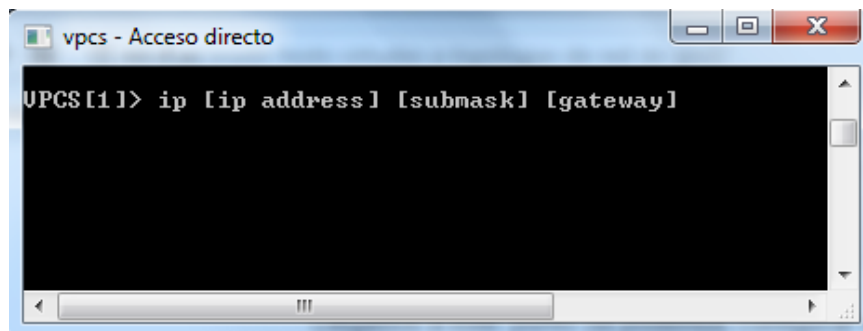


Figura 4. 45 Añadir IP a *host* virtual

Con esto se tendrían las configuraciones de todos los equipos listos para proceder a realizar las pruebas necesarias en la red INTEGRADA de voz y datos diseñada para la Unidad Educativa Temporal “Jaime Roldós Aguilera”.

### 4.3 PRUEBAS DE SIMULACIÓN DE LA RED

Para evaluar el diseño y simulación de la red se procederá con las pruebas respectivas desde los diferentes equipos establecidos para esta función.

Las pruebas principalmente estarán basadas en el uso de comandos como *ping* y *traceroute* para comprobar conectividad.

Para la comprobación de los servidores se utilizará un equipo destinado para ello, el mismo que estará conectado a la red y será parte de la VLAN de estudiantes con dirección IP 172.24.0.6/24, y desde el cual se procederá a realizar pruebas como acceso al servidor *web*, FTP, etc.

#### 4.3.1 PRUEBAS DEL SERVIDOR WEB

El servidor *web* Apache se encuentra alojado en la misma computadora donde se tiene el servidor FTP y el *firewall* de Linux, su dirección IP es la 10.0.0.1/28.

Para las pruebas se ha conectado una nube extra a GNS3, la cual está conectada a la PC física donde está corriendo GNS3; es decir, en la misma computadora se tiene la simulación de los *switches* y una computadora cliente de dirección IP 172.24.0.6/24 como se lo puede apreciar en la figura 4.46.

```

Adaptador de Ethernet VMware Network Adapter VMnet1:
  Sufijo DNS específico para la conexión. . . : 
  Descripción . . . . . : VMware Virtual Ethernet Adapter f
  or VMnet1
  Dirección física. . . . . : 00-50-56-C0-00-01
  DHCP habilitado . . . . . : no
  Configuración automática habilitada . . . : sí
  Vínculo: dirección IPv6 local. . . : fe80::d5a8:7b96:3c08:c2b2x15<Preferido>

  Dirección IPv4. . . . . : 172.24.0.6<Preferido>
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 172.24.0.254
  IAID DHCPv6 . . . . . : 335564886
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-15-3B-DB-31-70-71-BC-
  05-D4-A8
  Servidores DNS . . . . . : 10.0.0.3
  NetBIOS sobre TCP/IP. . . . . : habilitado

```

Figura 4. 46 IP de la nube perteneciente a la VLAN Estudiantes

La primera prueba que se va a realizar es desde la PC y se intentará llegar a la IP del servidor *web*, para ello se genera un *ping* desde la IP 172.24.0.6 a la 10.0.0.1.

En la figura 4.47 se observa que la respuesta del comando *ping* hacia la IP del servidor es correcta, además se puede apreciar que los tiempos son un poco altos debido a los recursos que tiene que utilizar GNS3.

```

C:\Users\Piñhico>ping 10.0.0.1

Haciendo ping a 10.0.0.1 con 32 bytes de datos:
Respuesta desde 10.0.0.1: bytes=32 tiempo=111ms TTL=63
Respuesta desde 10.0.0.1: bytes=32 tiempo=141ms TTL=63
Respuesta desde 10.0.0.1: bytes=32 tiempo=107ms TTL=63
Respuesta desde 10.0.0.1: bytes=32 tiempo=96ms TTL=63

Estadísticas de ping para 10.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 96ms, Máximo = 141ms, Media = 113ms

C:\Users\Piñhico>

```

Figura 4. 47 Ping al Servidor Web

La siguiente prueba a realizar es mucho más didáctica, pues se hará uso de un explorador y se ingresará la IP del servidor *web*, esperando como resultado la página de prueba precargada dentro del servidor. Esta prueba también será realizada desde la PC cliente. Como se observa en la figura 4.48, la respuesta que se obtiene por parte del servidor *web* es correcta, y en el explorador se ha desplegado la página de prueba *GUIDELINE* precargada.

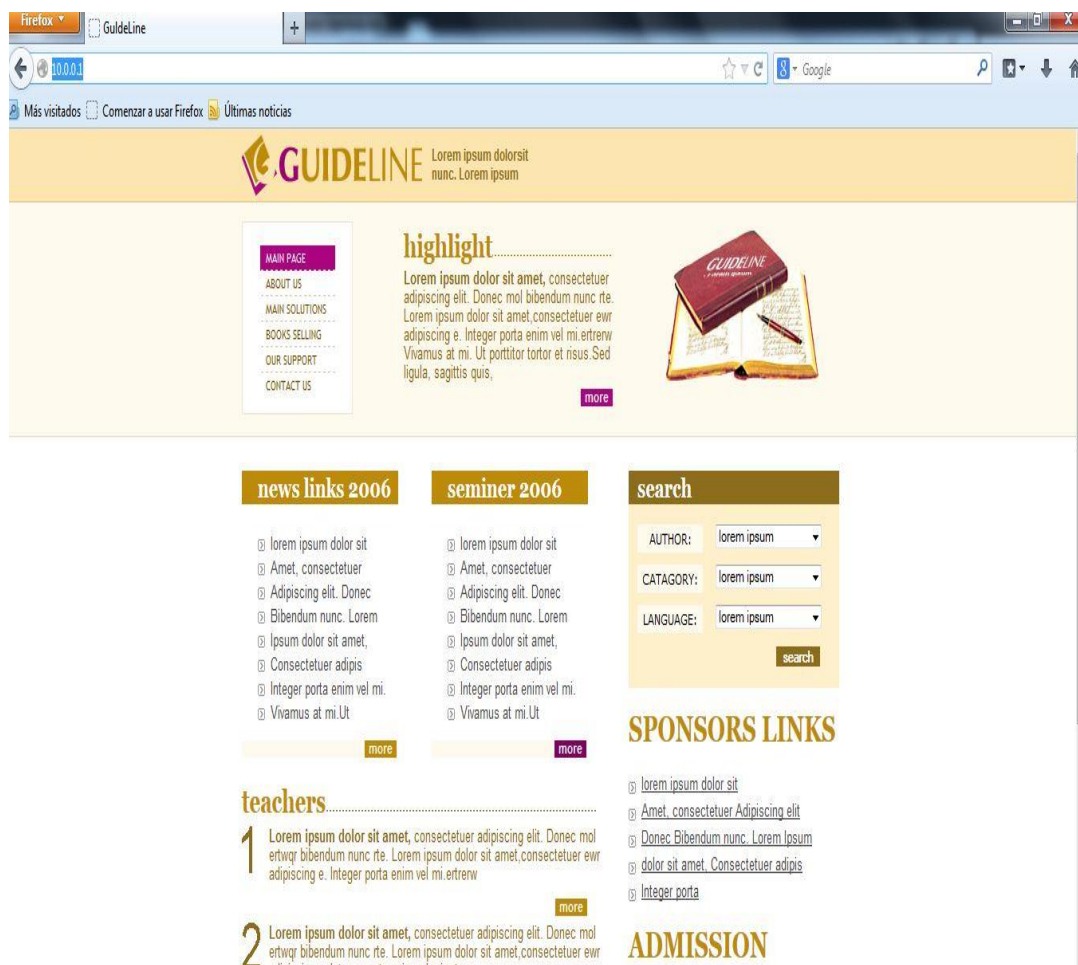


Figura 4. 48 Acceso a la página precargada en el Servidor Web



### 4.3.2 PRUEBAS DEL SERVIDOR FTP

Al igual que se realizaron las pruebas con el servidor *web*, se empleará la misma metodología para las pruebas del servidor FTP. Es decir se utilizará la PC cliente de la VLAN 172.24.0.6/24 y se realizará un *ping* y la carga de un archivo a uno de los usuarios FTP. La figura 4.49 muestra la respuesta al comando *ping* realizado.

```
C:\Users\Piñhico>ping 10.0.0.1

Haciendo ping a 10.0.0.1 con 32 bytes de datos:
Respuesta desde 10.0.0.1: bytes=32 tiempo=47ms TTL=63
Respuesta desde 10.0.0.1: bytes=32 tiempo=250ms TTL=63
Respuesta desde 10.0.0.1: bytes=32 tiempo=89ms TTL=63
Respuesta desde 10.0.0.1: bytes=32 tiempo=157ms TTL=63

Estadísticas de ping para 10.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 47ms, Máximo = 250ms, Media = 135ms
```

Figura 4. 49 *Ping* al Servidor FTP

En la figura 4.50 se muestra la prueba de conexión al servidor FTP desde uno de los usuarios creados; para este propósito se usa el comando **ftp 10.0.0.1**.

```
C:\Users\Piñhico>ftp 10.0.0.1
Conectado a 10.0.0.1.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:10.0.0.1]
Usuario (10.0.0.1:(none)): profesores
331 Password required for profesores
Contraseña:
230 User profesores logged in
```

Figura 4. 50 *Login* al Servidor FTP

Una vez dentro del servidor FTP se sube un archivo desde la PC local al usuario Profesores; esto lo se puede apreciar de mejor manera en la figura 4.51 donde se verifica que el archivo fue transferido por completo.

```
ftp> lcd
Directorio local ahora C:\Users\Piñhico.
ftp> put plot.txt
plot.txt: Archivo no encontrado
ftp> put plot.log
200 PORT command successful
150 Opening ASCII mode data connection for plot.log
226 Transfer complete
ftp: 1417 bytes enviados en 0,25segundos 5,58a KB/s.
```

Figura 4. 51 Transferencia de un archivo a un usuario FTP



Como se comprueba las pruebas del servidor FTP son exitosas, y se lo puede validar en el servidor dentro de la carpeta del usuario Profesores. Esto se evidencia en la figura 4.52.



Figura 4. 52 Confirmación de archivo transferido al usuario FTP

### 4.3.3 PRUEBAS DEL SERVIDOR DNS

Para validar que el Servidor DNS esté funcionando correctamente se realiza desde la máquina cliente un *ping* al dominio que se haya establecido y se debe observar la traducción a la IP correspondiente; para el ejemplo el servidor DNS se encuentra alojado en IP 10.0.0.3/28 y su dominio es mail.jra.net.

```
C:\Users\Piñhico>ping mail.jra.net

Haciendo ping a mail.jra.net [10.0.0.3] con 32 bytes de datos:
Respuesta desde 10.0.0.3: bytes=32 tiempo=3ms TTL=63
Respuesta desde 10.0.0.3: bytes=32 tiempo=4ms TTL=63
Respuesta desde 10.0.0.3: bytes=32 tiempo=3ms TTL=63
Respuesta desde 10.0.0.3: bytes=32 tiempo=2ms TTL=63

Estadísticas de ping para 10.0.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 4ms, Media = 3ms
```

Figura 4. 53 Ping al servidor DNS

Como se puede apreciar en la figura 4.53 el resultado al comando es exitoso y la traducción del nombre es correcta, ya que se realizó *ping* al dominio *mail.jra.net* y la respuesta fue entregada por la IP 10.0.0.3.

#### 4.3.4 PRUEBAS DEL SERVIDOR ZIMBRA

Para las pruebas del Servidor Zimbra nuevamente se utilizará la PC cliente con IP 172.24.0.6/24, con la diferencia que ahora el servidor se encuentra en otra computadora y obviamente con otra IP, en este caso la 10.0.0.3/28.

Lo primero a comprobar es conectividad mediante el uso del comando *ping* y se observa que los resultados sean exitosos, como lo evidencia la figura 4.54.

```
C:\Users\Piñhico>ping 10.0.0.3
Haciendo ping a 10.0.0.3 con 32 bytes de datos:
Respuesta desde 10.0.0.3: bytes=32 tiempo=3ms TTL=63
Respuesta desde 10.0.0.3: bytes=32 tiempo=2ms TTL=63
Respuesta desde 10.0.0.3: bytes=32 tiempo=3ms TTL=63
Respuesta desde 10.0.0.3: bytes=32 tiempo=2ms TTL=63
Estadísticas de ping para 10.0.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms
```

Figura 4. 54 Ping al Servidor Zimbra

Luego se ejecuta el comando *tracert* para comprobar el paso de los paquetes por el *firewall* 172.24.1.94, y que el mismo esté filtrando los paquetes de manera correcta (este ejemplo no se aplicó en el Servidor FTP y WEB por que se encontraban en el mismo PC y el salto era solo 1). Nuevamente se evidencia que el proceso es correcto, como se lo muestra en la figura 4.55.

```
C:\Users\Piñhico>tracert 10.0.0.3
Traza a la dirección mail.jra.net [10.0.0.3]
sobre un máximo de 30 saltos:

 1      1 ms    *      *      172.24.1.94
 2      2 ms    2 ms   2 ms   mail.jra.net [10.0.0.3]
Traza completa
```

Figura 4. 55 Traceroute al Servidor Zimbra

Finalmente se accede desde un *browser* a la consola de administración y se ingresa al sistema, donde se observa un mensaje en la esquina inferior derecha que confirma que el servidor está en buen estado, como lo muestra la figura 4.56.

#### 4.3.4.1 Correo Electrónico de Prueba

Una vez creados los usuarios, como se muestra en el numeral 4.3.8.1, se procedió a realizar un envío de prueba desde la cuenta de secretaria a la cuenta de un estudiante, en este caso, al email [jorge.ramon@mail.jra.net](mailto:jorge.ramon@mail.jra.net).

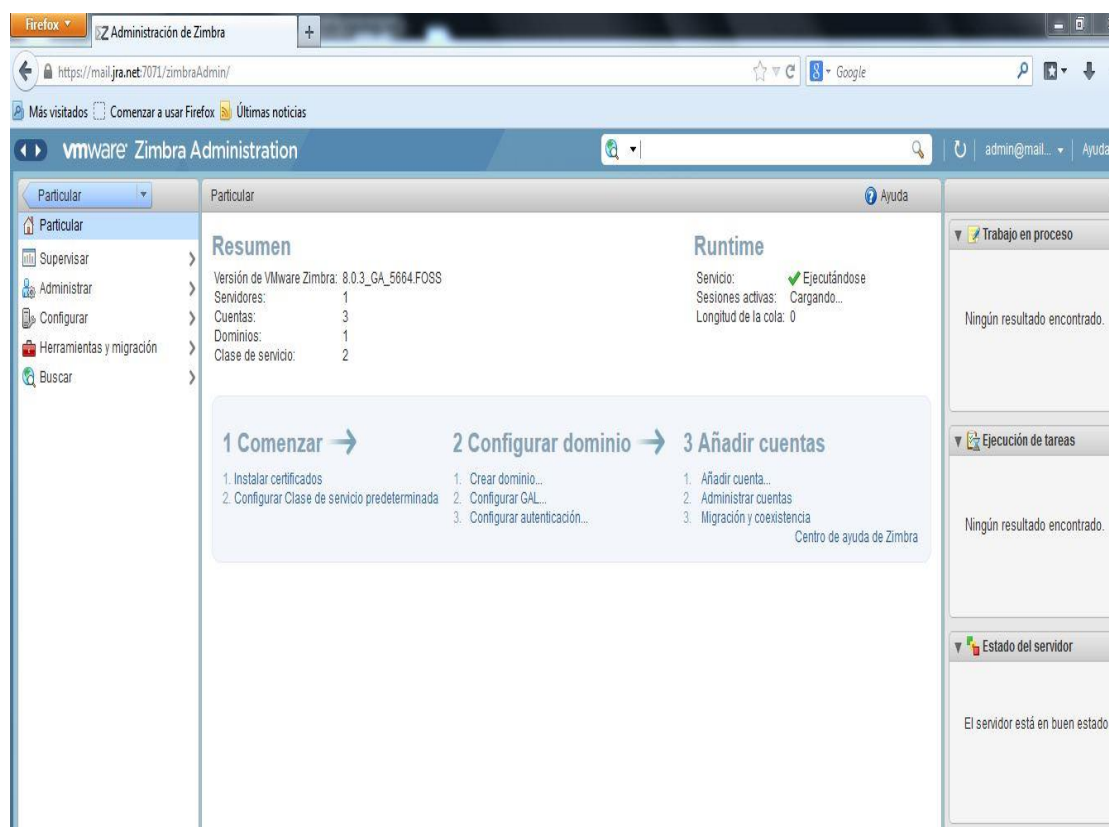


Figura 4. 56 Acceso web al Servidor Zimbra

Para poder validar el envío realizado, uno de los usuarios en mención se debe *logear* en *Zimbra Web Client*, digitando la dirección *mail.jra.net* en cualquier *browser*.

Una vez que se haya ingresado correctamente, se procede a validar que el correo de prueba enviado se encuentre en la bandeja de entrada o a su vez en la bandeja de salida, dependiendo del usuario; en el ejemplo se ha ingresado con el usuario *jorge.ramon*, por lo tanto se aprecia el *email* en la bandeja de entrada de dicha cuenta, como lo muestra la figura 4.57.

### 4.3.5 PRUEBAS DEL SERVIDOR ASTERISK

Para las pruebas del servidor Asterisk se ha considerado que al tener el *firewall* tres interfaces, una hacia la DMZ, otra hacía la LAN, y la última para el ISP, se realizarán las pruebas de las llamadas mediante el uso de la interfaz conectada al ISP, ya que las mismas se hacen desde dos *smartphones* y con el *softphone* adecuado.

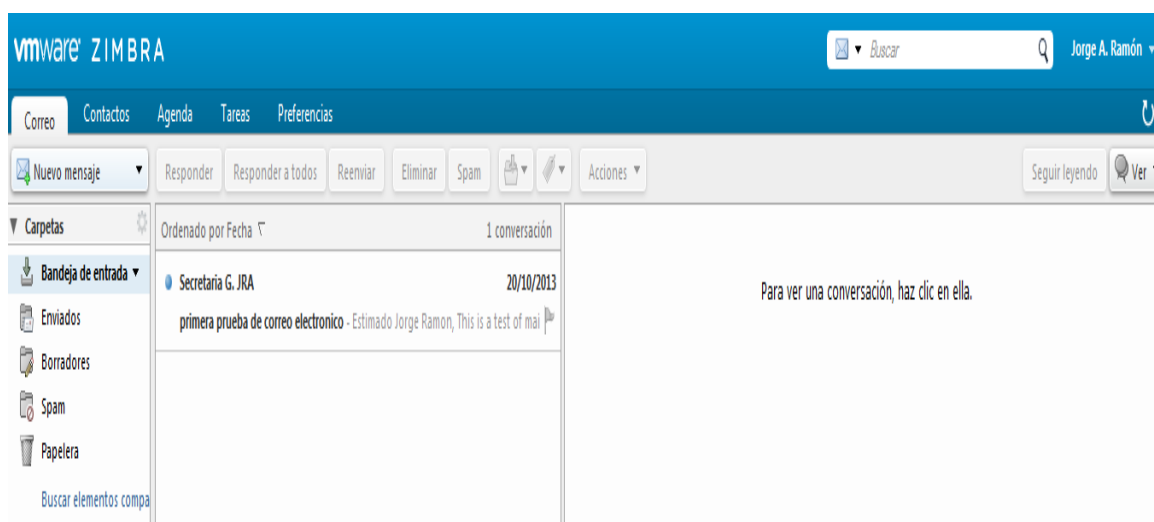


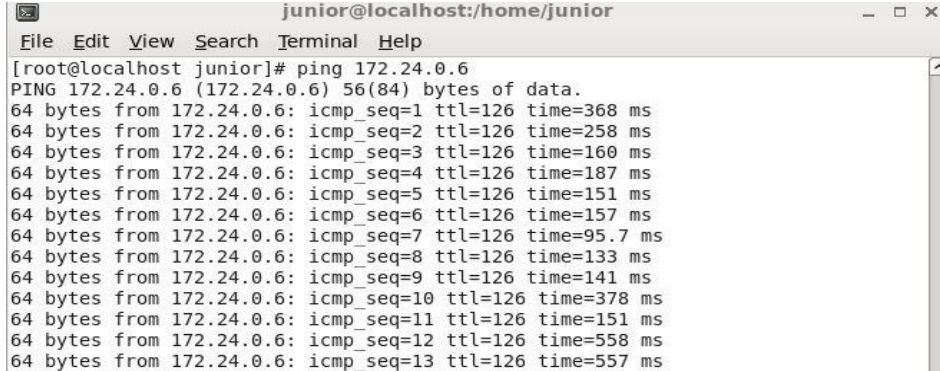
Figura 4. 57 Email de prueba a través de Zimbra

Si bien la interfaz por la cual se realizan las pruebas tendrá una IP distinta a la del servidor Asterisk, dentro del *firewall*, se han tomado las acciones necesarias para que toda petición a dicha IP sea “traducida” a la IP del servidor 10.0.0.5. Esta configuración adicional en el *firewall* se la realiza mediante el comando mostrado en la figura 4.58.

```
root@junior:/home/junior# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 5060 -j DNAT --to 10.0.0.5
```

Figura 4. 58 NATEO de la interfaz de Internet al servidor Asterisk

Para validar que efectivamente se tenga conectividad desde una PC cliente al servidor se realizan pruebas de *ping* desde el servidor al cliente o viceversa, como se puede apreciar en la figura 4.59.



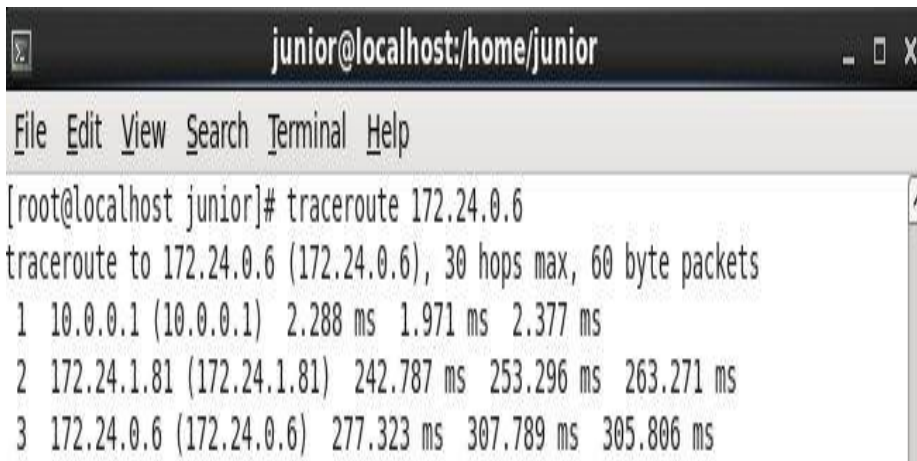
```

junior@localhost:/home/junior
File Edit View Search Terminal Help
[root@localhost junior]# ping 172.24.0.6
PING 172.24.0.6 (172.24.0.6) 56(84) bytes of data.
64 bytes from 172.24.0.6: icmp_seq=1 ttl=126 time=368 ms
64 bytes from 172.24.0.6: icmp_seq=2 ttl=126 time=258 ms
64 bytes from 172.24.0.6: icmp_seq=3 ttl=126 time=160 ms
64 bytes from 172.24.0.6: icmp_seq=4 ttl=126 time=187 ms
64 bytes from 172.24.0.6: icmp_seq=5 ttl=126 time=151 ms
64 bytes from 172.24.0.6: icmp_seq=6 ttl=126 time=157 ms
64 bytes from 172.24.0.6: icmp_seq=7 ttl=126 time=95.7 ms
64 bytes from 172.24.0.6: icmp_seq=8 ttl=126 time=133 ms
64 bytes from 172.24.0.6: icmp_seq=9 ttl=126 time=141 ms
64 bytes from 172.24.0.6: icmp_seq=10 ttl=126 time=378 ms
64 bytes from 172.24.0.6: icmp_seq=11 ttl=126 time=151 ms
64 bytes from 172.24.0.6: icmp_seq=12 ttl=126 time=558 ms
64 bytes from 172.24.0.6: icmp_seq=13 ttl=126 time=557 ms

```

Figura 4. 59 Ping desde el servidor Asterisk al cliente

Otra prueba para observar conectividad, es mediante el comando *trace*; y nuevamente se observa que la respuesta es la correcta como lo indica la figura 4.60.



```

junior@localhost:/home/junior
File Edit View Search Terminal Help
[root@localhost junior]# traceroute 172.24.0.6
traceroute to 172.24.0.6 (172.24.0.6), 30 hops max, 60 byte packets
 1 10.0.0.1 (10.0.0.1) 2.288 ms 1.971 ms 2.377 ms
 2 172.24.1.81 (172.24.1.81) 242.787 ms 253.296 ms 263.271 ms
 3 172.24.0.6 (172.24.0.6) 277.323 ms 307.789 ms 305.806 ms

```

Figura 4. 60 Traceroute desde el servidor Asterisk al Cliente

Analizando el resultado, se observa que efectivamente el paquete tiene 3 saltos para llegar a la red donde se encuentra el cliente, obviamente pasando por la red 10.0.0.1 donde se tiene el *firewall*, y por la red 172.24.1.81 que es el *switch* de distribución del núcleo de la red.

Una vez demostrado que se tiene conectividad entre los clientes, se procede a instalar los *softphones* en dos equipos celulares para realizar las pruebas, que como ya se indicó serán a través del Internet. Para este propósito, se utilizará el *softphone Media5 fone* compatible con los principales sistemas operativos para *Smartphone* como son *Android* e *IOS*.

#### 4.3.5.1 Configuración de Usuarios en Media5Fone

Una vez descargado el aplicativo desde las tiendas respectivas de cada uno de los sistemas operativos, se procede a abrir la aplicación y realizar su configuración. Dentro del *softphone* se encuentra la opción *MÁS*, donde se pueden realizar las configuraciones necesarias para los usuarios SIP a conectarse a la central Asterisk. En la pantalla principal mostrada en la figura 4.61 se escogen parámetros como: título, nombre, y *password* para activar el usuario.



Figura 4. 61 Configuración General de Usuario Media5Fone

Una vez llenados estos campos, se selecciona la opción *Servidores*, para ingresar la IP a la cual el *softphone* va a apuntar para su registro; para este proyecto será una IP del ISP como se aprecia en la figura 4.62.



Figura 4. 62 Configuración de Red para Media5Fone

Una vez completados los datos mostrados, se da por finalizado el proceso y se desplegará una ventana igual a la indicada en la figura 4.63, hasta tener un aviso de que el registro fue exitoso, y sí poder realizar llamadas entre los usuarios registrados correctamente, o llamadas de prueba a los números establecidos en el contexto pruebas.



Figura 4. 63 Registro usuario SIP Media5Fone

#### 4.3.6 PRUEBAS DEL SERVIDOR NAGIOS XI

Las pruebas del Servidor Nagios XI quizá sean unas de las más fáciles de entender, esto gracias a su interfaz gráfica. Como se ha realizado ya con los otros servidores lo primero a realizar son las pruebas de conectividad mediante el uso del comando *ping*, para ello se ejecuta este comando desde la máquina cliente 172.24.0.6/24 y se intenta llegar a la IP del servidor 10.0.0.8/28. Como se puede apreciar en la figura 4.64 los resultados son exitosos.

```
C:\Users\Piñhico>ping 10.0.0.8
Haciendo ping a 10.0.0.8 con 32 bytes de datos:
Respuesta desde 10.0.0.8: bytes=32 tiempo=66ms TTL=62
Respuesta desde 10.0.0.8: bytes=32 tiempo=153ms TTL=62
Respuesta desde 10.0.0.8: bytes=32 tiempo=161ms TTL=62
Respuesta desde 10.0.0.8: bytes=32 tiempo=236ms TTL=62

Estadísticas de ping para 10.0.0.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 66ms, Máximo = 236ms, Media = 154ms
```

Figura 4. 64 Ping al Servidor Nagios XI



Ahora se ejecuta el comando *trace* para ver los saltos que se tienen antes de llegar al servidor Nagios XI; nuevamente el resultado es satisfactorio, donde se evidencia los saltos que se tienen hasta a llegar al servidor. La ejecución de este comando se la puede apreciar en la figura 4.65.

```
C:\Users\Piñhico>tracert 10.0.0.8
"tracert" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Piñhico>tracert 10.0.0.8

Traza a 10.0.0.8 sobre caminos de 30 saltos como máximo.

  1  166 ms   185 ms   134 ms   172.24.0.254
  2   80 ms    12 ms    *        172.24.1.94
  3  142 ms   226 ms   357 ms   10.0.0.8
```

Figura 4. 65 Trace route al servidor Nagios XI

Una vez comprobada la conectividad, se ingresa desde un *browser* a la página de administración de Nagios XI a través de la dirección <http://10.0.0.8/nagiosxi/>. En esta página se puede apreciar que el estado del *host* cliente y uno de los *switches* de la Red está *UP*, como lo muestra la figura 4.66.

The screenshot shows the Nagios XI interface. On the left, the 'Host Status' section displays a table with 3 records. On the right, there are two summary tables: 'Host Status Summary' and 'Service Status Summary'. A search bar is located at the bottom right.

Host	Status	Duration	Attempt	Last Check	Status Information
Client	Up	57m 21s	1/1	2014-03-17 02:08:55	OK - 172.24.0.6: rta 281,263ms, lost 0%
localhost	Up	5d 8h 40m 47s	1/10	2014-03-17 02:08:05	OK - 127.0.0.1: rta 0,020ms, lost 0%
SW-ACC	Up	16m 54s	1/1	2014-03-17 02:02:48	OK - 172.24.1.82: rta 483,358ms, lost 0%

Host Status Summary			
Up	Down	Unreachable	Pending
3	0	0	0
Unhandled	Problems	All	
0	0	3	

Service Status Summary				
Ok	Warning	Unknown	Critical	Pending
8	1	0	0	0
Unhandled	Problems	All		
1	1	9		

Figura 4. 66 Estado de los *host* Cliente y SW- ACC

### 4.3.7 PRUEBAS DE LAS VLANs

Una vez realizadas las pruebas hacia los servidores, es necesario verificar que la comunicación entre las VLANs sea la correcta. Para ello se utiliza la herramienta *Wireshark* para capturar los paquetes que cursan por la red simulada.



Mediante esta herramienta se capturará tráfico de las VLANs de datos y voz respectivamente, para así analizar los paquetes y encontrar sus diferencias. Para la primera prueba se ejecuta el comando *ping* entre dos PCs pertenecientes a la VLAN estudiantes, y se captura el tráfico con *Wireshark* como se puede observar en la figura 4.67.

No.	Time	Source	Destination	Protocol	Length	Info
66	48.644000	172.24.0.7	172.24.0.6	ICMP	106	Echo (ping) request id=0x0194, seq=1/256, ttl=64
69	48.772000	172.24.0.6	172.24.0.7	ICMP	106	Echo (ping) reply id=0x0194, seq=1/256, ttl=128
71	49.775000	172.24.0.7	172.24.0.6	ICMP	106	Echo (ping) request id=0x0394, seq=2/512, ttl=64
72	49.796000	172.24.0.6	172.24.0.7	ICMP	106	Echo (ping) reply id=0x0394, seq=2/512, ttl=128
73	50.840000	172.24.0.7	172.24.0.6	ICMP	106	Echo (ping) request id=0x0494, seq=3/768, ttl=64

Figura 4. 67 Ping entre VLAN de datos

Al ser tráfico de una VLAN de datos se observa que la trama Ethernet no posee ninguna encapsulación adicional, esto se puede apreciar de mejor manera en la figura 4.68

Frame 66: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Vmware_c0:00:01 (00:50:56:c0:00:01)
Internet Protocol Version 4, Src: 172.24.0.7 (172.24.0.7), Dst: 172.24.0.6 (172.24.0.6)
Internet Control Message Protocol

Figura 4. 68 Trama de datos

La siguiente prueba será generada desde una PC conectada a la VLAN de voz, la respuesta al comando *ping* es exitosa y se observa en la figura 4.69.

No.	Time	Source	Destination	Protocol	Length	Info
120	12.736000	172.24.1.2	172.24.1.1	ICMP	110	Echo (ping) request id=0x0a9c, seq=1/256, ttl=64
121	12.737000	172.24.1.1	172.24.1.2	ICMP	110	Echo (ping) reply id=0x0a9c, seq=1/256, ttl=64
135	13.809000	172.24.1.2	172.24.1.1	ICMP	110	Echo (ping) request id=0x0b9c, seq=2/512, ttl=64
136	13.810000	172.24.1.1	172.24.1.2	ICMP	110	Echo (ping) reply id=0x0b9c, seq=2/512, ttl=64

Figura 4. 69 Ping entre VLAN de voz

A diferencia del tráfico de datos, la VLAN de voz añade un encapsulamiento adicional en su paquete para indicar a la red que el tráfico se trata de voz y que debe ser tratada de distinta manera. En la figura 4.70 se muestra la composición de la trama de voz.

```

Frame 120: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:01 (00:50:79:66:68:01)
802.1Q Virtual LAN, PRI: 7, CFI: 0, ID: 20
  000. .... .... = Priority: Best Effort (default) (0)
  ...0 .... .... = CFI: Canonical (0)
  .... 0000 0001 0100 = ID: 20
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 172.24.1.2 (172.24.1.2), Dst: 172.24.1.1 (172.24.1.1)
Internet Control Message Protocol

```

Figura 4. 70 Trama de voz

Como se observa la trama de voz contiene una encapsulación adicional a la de datos, llamada 802.1Q, dentro de ella existen parámetros tales como *Priority*, CFI, y el VLAN ID; el campo *priority* es un campo de 3 bits que se refiere a la IEEE 802.1p e indica el nivel de prioridad de trama.

Los valores van de 0 (mejor esfuerzo) a 7 (más alto); Estos valores se pueden utilizar para dar prioridad a diferentes clases de tráfico como voz, video, datos, etc. Para este proyecto se tiene establecida la prioridad más alta para los paquetes que cursen por la VLAN de voz.

#### 4.4 ANÁLISIS DE LAS PRUEBAS REALIZADAS

Las pruebas realizadas en el numeral 4.4 constituyen las métricas de este proyecto para determinar si el diseño propuesto satisface las necesidades del Plantel.

Cabe indicar que la realización de pruebas mediante la herramienta GNS3 (núcleo de la red) provee ciertos limitantes al momento de realizarlas. Estos limitantes han sido solucionado con la inserción de algunos elementos (*hardware*) como *Switch* y adaptadores USB-RJ45 para poder evidenciar las pruebas, ya que al realizar una simulación totalmente basada en *software* existían problemas de retraso disminuyendo así la efectividad del presente proyecto.

Si bien la simulación de la red no permitió evaluar su rendimiento debido a las limitantes antes mencionadas, además de necesitar mediciones del total de paquetes transmitidos exitosamente; sin embargo brindó una visión general del funcionamiento que tendría la red en caso de ser implementada.

También es importante mencionar que después de realizar la simulación con los servidores necesarios, se evidenciaron ciertas fallas dentro del diseño lógico de la red, sobre todo en el direccionamiento IP para la VLAN de gestión, la definición de la DMZ, configuraciones dentro del *firewall*, *entre otros*. Basado en lo antes mencionado que se procedió a realizar nuevamente el subneteo y diseño de los errores encontrados para poder demostrar el correcto funcionamiento de la red diseñada.

Así mismo resultó necesario la utilización de diferentes herramientas y comandos ajenos a este proyecto, para que las pruebas sean lo más apegadas a la realidad, como por ejemplo comandos de “NAT” para que las pruebas de telefonía puedan realizarse entre dos equipos móviles, o el uso de la herramienta VPCS (*Virtual Simulators PC's*) que brinda la capacidad de simular hasta 9 PCs enlazados a GNS3 mediante una única interfaz física, permitiendo así generar máquinas clientes de las diferentes VLANs.

Con todo lo antes mencionado, y como se puede apreciar en las imágenes, las pruebas de funcionamiento de la red han resultado exitosas tanto desde el punto de vista de conectividad (evidenciadas por el comando *ping* y *traceroute*) como por el uso propio de herramientas para la comprobación de los demás servicios como son: telefonía IP, servidor *web* y FTP. En base a estos resultados y a todo lo expuesto en los párrafos anteriores se puede determinar que la red simulada cumple con el diseño propuesto y que podrá proveer de los servicios solicitados a la Unidad Educativa Temporal “Jaime Roldós Aguilera”, en caso de ser implementada.

#### **4.5 ANÁLISIS DE COSTOS DE LA RED INTEGRADA DE VOZ Y DATOS DISEÑADA**

Una vez que se han establecido los elementos necesarios con los que debe contar la red integrada de voz y datos, es indispensable hacer un análisis de costos de las diferentes alternativas que se tendría en caso de que la red quiera ser implementada.

La selección de los equipos que se podrían utilizar toma en consideración que los mismos cumplen a cabalidad los requerimientos técnicos establecidos y buscan el ahorro para la Institución. Este análisis se lo realiza en base a las características que se establecieron en el capítulo anterior, y se brindarán dos opciones de equipamiento a la Unidad Educativa Temporal “Jaime Roldós Aguilera”. Para este propósito se dividirá el análisis de costos, para los elementos pasivos y equipos activos de la red antes diseñada.

#### 4.5.1 ANÁLISIS DE COSTOS DE LA RED PASIVA

Como ya se mencionó la red pasiva es aquella parte de la red que se encarga de la propagación de los datos a través de la institución, es decir, corresponde al sistema de cableado estructurado sobre el cual funcionará la red. Entre los elementos que se evaluarán dentro de la red pasiva se tienen, *patch cords*, cable UTP, *racks*, gabinetes, etc.

##### 4.5.1.1 Elementos de la Red Pasiva

Primeramente se definirán los diferentes elementos que se necesitan para la red pasiva de la institución; luego se establecerán los elementos necesarios por cada zona para así poder encontrar el costo que tendría la red pasiva para la Unidad Educativa Temporal “Jaime Roldós Aguilera”. La tabla 4.1 muestra la lista de elementos y materiales que se necesitarán para la red pasiva diseñada.

ELEMENTOS NECESARIOS PARA LA RED PASIVA		
DESCRIPCIÓN	MEDIDA	IMÁGEN
Canaleta Decorativa	60x40 mm	
	32x12 mm	
	40X25 mm	
	40x40 mm	

Tabla 4. 1 Elementos de la red pasiva (Parte 1 de 3)

<b>Ángulo Interno</b>	60x40 mm 32x12 mm 40X25 mm 40x40 mm	
<b>Derivación en T</b>	60x40 mm 32x12 mm 40X25 mm 40x40 mm	
<b>Jack Cat 6A</b>	N/A	
<b>Face Plate Simple</b>	N/A	
<b>Face Plate Doble</b>	2UR	
<b>Patch-Cord Cat 6A</b>	3 pies	
<b>Patch Panel</b>	24 Puertos	

Tabla 4. 1 Elementos de la red pasiva (Parte 2 de 3)

<b>Tubo Conduit EMT</b>	12.7 mm (½ ") x 3m	
<b>Rack</b>	24 UR	
<b>Gabinetes de Pared</b>	12 UR 10 UR	
<b>Organizadores Horizontales</b>	19 "	
<b>Cable UTP Cat 6A</b>	305 m	

Tabla 4. 1 Elementos de la red pasiva (Parte 3 de 3)

En las tablas 4.2 a 4.6 se muestran los elementos necesarios por cada una de las zonas y su respectivo costo de acuerdo a las proformas de las casas distribuidoras de dichos materiales; estas proformas se las puede observar en el Anexo M.

PROFORMA ZONA A			
DESCRIPCIÓN	CANTIDAD	VALOR [ \$ ]	
		Unitario	Total
Canaleta Plástica 60x40 mm	4	\$ 8.84	\$ 35.36
Canaleta Plástica 40x40 mm	7	\$ 6.43	\$ 45.01
Canaleta Plástica 40x25 mm	22	\$ 5.67	\$ 124.74
Canaleta Plástica 32x12 mm	9	\$ 2.55	\$ 22.95
Ángulo Interno 60x40 mm	1	\$ 2.32	\$ 2.32
Ángulo Interno 40x40 mm	1	\$ 1.27	\$ 1.27
Ángulo Interno 40x25 mm	1	\$ 1.15	\$ 1.15
Ángulo Interno 32x12 mm	1	\$ 0.54	\$ 0.54
Derivación T 60 x 40 mm	6	\$ 3.35	\$ 20.10
Derivación T 40x40 mm	-	\$ 1.32	-
Derivación T 40x25 mm	3	\$ 1.16	\$ 3.48
Derivación T 32x12 mm	-	\$ 0.52	-
Jack Categoría 6 A	46	\$ 6.375	\$ 293.25
Face Plate Doble	19	\$ 1.96	\$ 37.24
Face Plate Simple	8	\$ 1.5715	\$ 12.57
Patch Cord Cat 6A 3 pies	46	\$ 8.634	\$ 397.16
Tubo Conduit EMT	-	\$ 2.37	-
Patch Panel 24 puertos	2	\$ 218.75	\$ 437.5
Organizador Horizontal	2	\$ 15.99	\$ 31.98
		<b>SUBTOTAL</b>	\$ 1,466.62
		<b>IVA</b>	\$ 175.99
		<b>TOTAL</b>	\$ 1,642.61

Tabla 4. 2 Elementos de la red pasiva zona A

PROFORMA ZONA B			
DESCRIPCIÓN	CANTIDAD	VALOR [\$]	
		Unitario	Total
Canaleta Plástica 60x40 mm	-	\$ 8.84	-
Canaleta Plástica 40x40 mm	5	\$ 6.43	\$ 32.15
Canaleta Plástica 40x22 mm	9	\$ 5.67	\$ 51.03
Canaleta Plástica 32x12 mm	2	\$ 2.55	\$ 5.10
Ángulo Interno 60x40 mm	-	\$ 2.32	-
Ángulo Interno 40x40 mm	-	\$ 1.27	-
Ángulo Interno 40x22 mm	-	\$ 1.15	-
Ángulo Interno 32x12 mm	-	\$ 0.54	-
Derivación T 60 x 40 mm	-	\$ 3.35	-
Derivación T 40x40 mm	9	\$ 1.32	\$ 11.88
Derivación T 40x22 mm	12	\$ 1.16	\$ 13.92
Derivación T 32x12 mm	-	\$ 0.52	-
Jack Categoría 6 A	28	\$ 6.375	\$ 178.5
Face Plate Doble	1	\$ 1.96	\$ 1.96
Face Plate Simple	26	\$ 1.5715	\$ 40.86
Patch Cord Cat 6A 3 pies	28	\$ 8.634	\$ 241.64
Tubo Conduit EMT	2	\$ 2.37	\$ 4.74
Patch Panel 24 puertos	2	\$ 218.75	\$ 437.5
Organizador Horizontal	2	\$ 15.99	\$ 31.98
		<b>SUBTOTAL</b>	\$ 1,051.26
		<b>IVA</b>	\$ 126.15
		<b>TOTAL</b>	\$ 1,177.41

Tabla 4. 3 Elementos de la red pasiva zona B



PROFORMA ZONA C			
DESCRIPCIÓN	CANTIDAD	VALOR [ \$ ]	
		Unitario	Total
Canaleta Plástica 60x40 mm	9	\$ 8.84	\$ 80.46
Canaleta Plástica 40x40 mm	-	\$ 6.43	-
Canaleta Plástica 40x22 mm	32	\$ 5.67	\$ 181.44
Canaleta Plástica 32x12 mm	4	\$ 2.55	\$ 10.20
Ángulo Interno 60x40 mm	1	\$ 2.32	\$ 2.32
Ángulo Interno 40x40 mm	-	\$ 1.27	-
Ángulo Interno 40x22 mm	7	\$ 1.15	\$ 8.05
Ángulo Interno 32x12 mm	-	\$ 0.54	-
Derivación T 60 x 40 mm	5	\$ 3.35	\$ 16.75
Derivación T 40x40 mm	-	\$ 1.32	-
Derivación T 40x22 mm	1	\$ 1.16	\$ 1.16
Derivación T 32x12 mm	-	\$ 0.52	-
Jack Categoría 6 A	40	\$ 6.375	\$ 255.00
Face Plate Doble	12	\$ 1.96	\$ 23.52
Face Plate Simple	16	\$ 1.5715	\$ 25.14
Patch Cord Cat 6A 3 pies	40	\$ 8.634	\$ 345.36
Tubo Conduit EMT	1	\$ 2.37	\$ 2.37
Patch Panel	2	\$ 218.75	\$ 437.5
Organizador Horizontal	2	\$ 15.99	\$ 31.98
		<b>SUBTOTAL</b>	\$ 1,421.25
		<b>IVA</b>	\$ 170.55
		<b>TOTAL</b>	\$ 1,591.80

Tabla 4. 4 Elementos de la red pasiva zona C

PROFORMA ZONA D			
DESCRIPCIÓN	CANTIDAD	VALOR [\$]	
		Unitario	Total
Canaleta Plástica 60x40 mm	-	\$ 8.84	-
Canaleta Plástica 40x40 mm	-	\$ 6.43	-
Canaleta Plástica 40x22 mm	37	\$ 5.67	\$ 209.79
Canaleta Plástica 32x12 mm	9	\$ 2.55	\$ 22.95
Ángulo Interno 60x40 mm	-	\$ 2.32	-
Ángulo Interno 40x40 mm	-	\$ 1.27	-
Ángulo Interno 40x22 mm	1	\$ 1.15	\$ 1.15
Ángulo Interno 32x12 mm	3	\$ 0.54	\$ 1.62
Derivación T 60 x 40 mm	-	\$ 3.35	-
Derivación T 40x40 mm	-	\$ 1.32	-
Derivación T 40x22 mm	13	\$ 1.16	\$ 15.08
Derivación T 32x12 mm	-	\$ 0.52	-
Jack Categoría 6 A	24	\$ 6.375	\$ 153.00
Face Plate Doble	4	\$ 1.96	\$ 7.84
Face Plate Simple	16	\$ 1.5715	\$ 25.14
Patch Cord Cat 6A 3 pies	24	\$ 8.634	\$ 207.22
Tubo Conduit EMT	1	\$ 2.37	\$ 2.37
Patch Panel	1	\$ 218.75	\$ 218.75
Organizador Horizontal	1	\$ 15.99	\$ 15.99
		<b>SUBTOTAL</b>	\$ 880.90
		<b>IVA</b>	\$ 105.71
		<b>TOTAL</b>	\$ 986.61

Tabla 4. 5 Elementos de la red pasiva zona D

PROFORMA ZONA E			
DESCRIPCIÓN	CANTIDAD	VALOR [ \$ ]	
		<i>Unitario</i>	<i>Total</i>
<b>Canaleta Plástica 60x40 mm</b>	115	\$ 8.84	\$ 1016.6
<b>Canaleta Plástica 40x40 mm</b>	-	\$ 6.43	-
<b>Canaleta Plástica 40x22 mm</b>	14	\$ 5.67	\$ 79.38
<b>Canaleta Plástica 32x12 mm</b>	4	\$ 2.55	\$ 10.20
<b>Ángulo Interno 60x40 mm</b>	4	\$ 2.32	\$ 9.28
<b>Ángulo Interno 40x40 mm</b>	-	\$ 1.27	-
<b>Ángulo Interno 40x22 mm</b>	1	\$ 1.15	\$ 1.15
<b>Ángulo Interno 32x12 mm</b>	-	\$ 0.54	-
<b>Derivación T 60 x 40 mm</b>	52	\$ 3.35	\$ 174.20
<b>Derivación T 40x40 mm</b>	-	\$ 1.32	-
<b>Derivación T 40x22 mm</b>	5	\$ 1.16	\$ 5.8
<b>Derivación T 32x12 mm</b>	1	\$ 0.52	\$ 0.52
<b>Jack Categoría 6 A</b>	74	\$ 6.375	\$ 471.75
<b>Face Plate Doble</b>	7	\$ 1.96	\$ 13.72
<b>Face Plate Simple</b>	60	\$ 1.5715	\$ 94.29
<b>Patch Cord Cat 6A 3 pies</b>	74	\$ 8.634	\$ 638.92
<b>Tubo Conduit EMT</b>	6	\$ 2.37	\$ 14.22
<b>Patch Panel 24 puertos</b>	4	\$ 218.75	\$ 875.00
<b>Organizador Horizontal</b>	4	\$ 15.99	\$ 63.96
		<b>SUBTOTAL</b>	\$ 3,468.99
		<b>IVA</b>	\$ 416.28
		<b>TOTAL</b>	\$ 3,885.27

Tabla 4. 6 Elementos de la red pasiva zona E

El costo total de la red pasiva se presenta en la tabla 4.7.

ZONA	VALOR
A	\$ 1,642,61
B	\$ 1,177,41
C	\$ 1,591,80
D	\$ 986,61
E	\$ 3,885,27
<b>TOTAL</b>	<b>\$ 9,283.70</b>

Tabla 4. 7 Valor total de la red pasiva

#### 4.5.2 ANÁLISIS DE COSTOS DE LA RED ACTIVA

Para la parte activa de la red, en la que se incluyen los equipos de conectividad, tales como *Switches*, *Access Point*, teléfonos IP, se realizará el análisis de los costos de las casas fabricantes Cisco, Juniper para los equipos de conectividad, mientras que para terminales IP se evaluará Cisco y Avaya.

Tanto Cisco como Juniper son grandes proveedores de equipos de conectividad, y sobre todo proporcionan gran rendimiento y desempeño en sus equipos; si bien dentro de nuestro mercado Juniper no tiene la acogida que tiene Cisco, no se debe menospreciar la calidad de equipos que presenta, además se debe considerar que es una casa fabricante americana y que en los últimos años ha venido tomando fuerza dentro del país.

Basado en lo antes mencionado en los siguientes numerales se muestran los equipos que cubren los requerimientos establecidos en el capítulo 3, y cuánto es su valor en el mercado para las marcas antes indicadas.

##### 4.5.2.1 *Switches* de Acceso [76][77]

Los *switches* de acceso cubrirán los 204 puntos diseñados y deben cumplir ciertas características mínimas para su correcto funcionamiento; por tal motivo en la tabla 4.8 se sugieren dos equipos de las marcas antes indicadas para esta labor.

<b>Switch de Acceso</b>			
<b>Parámetros</b>	<b>Características</b>	<b>SW-2960-24PC-S CISCO</b>	<b>JUNIPER EX2200 24P/24T</b>
<b>Puertos Ethernet</b>	24 / 48 puertos 10/100 Mbps	✓	✓
<b>Puertos Uplink</b>	2 puertos GigabitEthernet 10/100/1000 Mbps	✓	✓
<b>Capa OSI</b>	2	✓	✓
<b>Backplane</b>	6,8 Gbps	32 Gbps	56 Gbps
<b>Throughput</b>	6 Mpps	6.5 Mpps	42 Mpps
<b>Entradas de direcciones MAC</b>	8000	8000	8000
<b>Manejo de VLAN`s</b>	Sí	✓	✓
<b>Estándares</b>	IEEE 802.1d ; IEEE 802.1p ; IEEE 802.1q ; IEEE 802.1x ; IEEE 802.1w ; IEEE 802.3u ; IEEE 802.3x ; IEEE 802.3af	IEEE 802.1D ; IEEE 802.1p ; IEEE 802.1Q ; IEEE 802.1s ; IEEE 802.1w ; IEEE 802.1x ; IEEE 802.3af ; IEEE 802.3ab ; IEEE 802.3ah ; IEEE 802.3u ; IEEE 802.3x ; IEEE 802.3z ; IEEE 802.3ad	IEEE 802.3u ; IEEE 802.3z ; IEEE 802.1D ; IEEE 802.1Q ; IEEE 802.3ab ; IEEE 802.1p ; IEEE 802.3af ; IEEE 802.3x ; IEEE 802.3ad ; IEEE 802.1w ; IEEE 802.1x ; IEEE 802.1s ; IEEE 802.1ab
<b>Protocolos</b>	SNMPv1; SNMPv2; SNMPv3; Telnet; RMON	SNMPv1; SNMPv2c; SNMP; RMON; RMON 2RMON 3, RMON 9,	SNMP, RMON 1, RMON 2, RMON 3, RMON 9, , SNMP 3, SNMP 2c, SSH-2
<b>Administración</b>	GUI; SNMP; Telnet; CLI	Telnet; CLI	Telnet CLI
<b>COSTO</b>		<b>\$ 1,718.70</b>	<b>\$ 1,160.00</b>

Tabla 4. 8 Costo de los switches de acceso

En base a los costos referenciales se determina que para la capa de acceso se tienen las dos siguientes opciones y que su valor sería el mostrado en la tabla 4.9.

Fabricante	Cantidad	Valor Unitario	Valor Total
<b>CISCO</b>	9	\$ 1,718.70	\$ 15,468.30
<b>JUNIPER</b>	9	\$ 1,160.00	\$ 10,440,00

**Tabla 4. 9 Costo total de *switches* de acceso**

#### **4.5.2.2 *Switches* de Distribución [78] [79]**

Para los *switches* de distribución se ha optado por los modelos WS-C3650-24TS de Cisco y el modelo EX3300 de Juniper respectivamente, ya que como se puede apreciar en la tabla 4.10 cumplen con las características mostradas en el diseño.

Para la capa de distribución se necesitan dos *switches* de las características antes mencionadas, teniendo así los modelos mostrados en la tabla 4.11.

#### **4.5.2.3 *Switches* de Core [80] [81]**

La elección del *Switch* de *Core* es una de las más importantes, ya que es el encargado de conmutar lo más rápido posible y proveer la redundancia suficiente para la red.

Los *Switches* que cumplen con las recomendaciones establecidas en el diseño son el Cisco Catalyst 3750X-12S-S y el Juniper QFX3500. La tabla 4.12 muestra la comparación entre los equipos antes mencionados y el cumplimiento de los requerimientos mínimos establecidos en el diseño.

Una vez más se procede a encontrar el valor referencial a utilizar en esta capa, para la cual se necesitan 2 equipos como se mencionó en el capítulo anterior, teniendo así la tabla 4.13.

<b>Switch de Distribución</b>			
<b>Parámetros</b>	<b>Características</b>	<b>WS-C3650-24TS CISCO</b>	<b>JUNIPER EX3300 24P/24T-DC</b>
<b>Puertos Ethernet</b>	12/24 puertos 10/100/1000 Mbps	✓	✓
<b>Puertos Uplink</b>	2 puertos 10/100/100 Mbps	✓	✓
<b>Capa OSI</b>	2/3	✓	✓
<b>Backplane</b>	11,6 Gbps	32 Gbps	128 Gbps
<b>Throughput</b>	6 Mpps	6.5 Mpps	95 Mpps
<b>Entradas de direcciones MAC</b>	8000	12000	16000
<b>Manejo de VLAN` s</b>	Sí	✓	✓
<b>Estándares</b>	IEEE 802.1d; IEEE 802.1p; IEEE 802.1q IEEE 802.1x; IEEE 802.1w; IEEE 802.3u; IEEE 802.3x; IEEE 802.3af	IEEE 802.1s IEEE 802.1w IEEE 802.1x IEEE 802.3ad IEEE 802.3af IEEE 802.3x IEEE 802.1D IEEE 802.1p IEEE 802.1Q IEEE 802.3u IEEE 802.3ab IEEE 802.3z	IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad, IEEE 802.1w, IEEE 802.1x, IEEE 802.1s,
<b>Protocolos</b>	IPv4, IPv6, OSPF, RIPv2, IGM, BGP; DHCP, RMON, SNMP	IPv4-v6, OSPF; RIPv2, IGM; BGP, DHCP ; SNMP v1,v2c; RMON	IPv4-v6, OSPF; RIPv2, IGM; BGP, DHCP SNMPv1,v2c; SNMPv2c, RMON;
<b>Administración</b>	Telnet; CLI	Telnet; CLI	Telnet; CLI
<b>COSTO</b>		<b>\$ 3,540.56</b>	<b>\$ 2,066.25</b>

Tabla 4. 10 Costo de los switches de distribución

<b>Fabricante</b>	<b>Cantidad</b>	<b>Valor Unitario</b>	<b>Valor Total</b>
<b>CISCO</b>	2	\$ 3,540.56	\$ 7,081.12
<b>JUNIPER</b>	2	\$ 2,066.25	\$ 4,132.50

Tabla 4. 11 Costo total de switches de distribución

<b>Switch de Core</b>			
<b>Detalle</b>	<b>Características</b>	<b>WS-3750X-24S-S CISCO</b>	<b>JUNIPER QFX3500</b>
<b>Puertos Ethernet</b>	12 puertos 10/100/100 Base-TX	✓	✓
<b>Capa OSI</b>	2/3	✓	✓
<b>Backplane</b>	48 Gbps	160 Gbps	1.28 Tbps
<b>Throughput</b>	50 Mpps	65.5 Mpps	960 Mpps
<b>Entradas de direcciones MAC</b>	16000	24000	96000
<b>Seguridad</b>	Soporte a ACL estándar y extendidas en todos los puertos	✓	✓
<b>Estándares</b>	IEEE 802.1d ; IEEE 802.1p ; IEEE 802.1q ; IEEE 802.1x ; IEEE 802.1w ; IEEE 802.3u ; IEEE 802.3x ; IEEE 802.3af	IEEE 802.1s; IEEE 802.1w; IEEE 802.1x; IEEE 802.3ad; IEEE 802.3af; IEEE 802.3x; IEEE 802.1D; IEEE 802.1p; IEEE 802.1Q; IEEE 802.3u; IEEE 802.3ab; IEEE 802.3z;	IEEE 802.3u ; IEEE 802.3z ; IEEE 802.1D ; IEEE 802.1Q ; IEEE 802.3ab; IEEE 802.1p ; IEEE 802.3af; IEEE 802.3x ; IEEE 802.3ad; IEEE 802.1w ; IEEE 802.1x ; IEEE 802.1s ; IEEE 802.1ab; IEEE 802.3at
<b>Protocolos</b>	IPv4, IPv6, OSPF; RIPv2, IGM, BGP; DHCP, RMON, SNMP	IPv4, IPv6, OSPF; RIPv2, IGM, BGP; DHCP, SNMPv1; SNMPv2c, SNMP; RMON, RMON2, RMON3, RMON9	IPv4, IPv6, OSPF; RIPv2, IGM, BGP; DHCP, SNMPv1; SNMPv2c, SNMP; RMON, RMON2, RMON3, RMON9, SNTP, BFD
<b>Administración</b>	GUI; Telnet; CLI	GUI; Telnet; CLI	GUI; Telnet; CLI
<b>COSTO</b>		<b>\$ 10.371,83</b>	<b>\$ 15.992,75</b>

Tabla 4. 12 Costo de los switches de core



Casa Fabricante	Cantidad	Valor Unitario	Valor Total
CISCO	2	\$ 10,371.83	\$ 20,743.66
JUNIPER	2	\$ 15,992.75	\$ 31,985,50

Tabla 4. 13 Costo total de la switches core

#### 4.5.2.4 Access Point [82][83]

Tomando en consideración el desarrollo del *site survey* pasivo del capítulo 3, se puede decir que para brindar los servicios de la red a los usuarios que se encuentren en los espacios donde no se tiene acceso a la red cableada, se necesitan ocho *access-point*, los mismos que deben cumplir con las características técnicas de la tabla 4.14.

<b>Access Point</b>			
<b>Parámetros</b>	<b>Características</b>	<b>CISCO CAP1602-I</b>	<b>JUNIPER WLA322</b>
<b>Interfaces</b>	Ethernet RJ45	✓	✓
<b>Velocidad de Transmisión</b>	54 Mbps	✓	✓
<b>Algoritmos de Cifrado</b>	MD5, SHA, AES	✓	✓
<b>Mecanismos de Encriptación</b>	TKIP, WPA, WPA2	✓	✓
<b>PoE</b>	Sí	✓	✓
<b>Estándares</b>	IEEE 802.11x; IEEE 802.11g; IEEE 802.11n; IEEE 802.3af; IEEE 802.3u; IEEE 802.1p; IEEE 802.1q	✓	✓
<b>Administración</b>	GUI; SNMP	✓	✓
<b>COSTO</b>		<b>\$ 523.45</b>	<b>\$ 899.00</b>

Tabla 4. 14 Costo de los access-point

Con esto se tiene el valor referencial para la adquisición de los equipos de la red inalámbrica, como se muestra en la tabla 4.15

Casa Fabricante	Cantidad	Valor Unitario	Valor Total
CISCO	8	\$ 523.45	\$ 4,187.60
JUNIPER	8	\$ 899.00	\$ 7,192,00

Tabla 4. 15 Costo total de la red inalámbrica

#### 4.5.2.5 Teléfonos IP [84] [85]

Para la red de voz se ha optado por teléfonos IP Cisco ó Avaya, tomando en consideración que Avaya necesita de sus respectivas licencias para cada teléfono, lo que se debe considerar en el coste de las mismas en caso de su adquisición. Las características que deben poseer estos equipos son las mostradas en la tabla 4.16.

Teléfonos IP			
Parámetros	Características	CISCO SPA512-G	Avaya 1210
Puertos	2 puertos RJ45 10/100 Mbps	✓	✓
Interfaces FXO	24	✓	✓
Codecs de Voz	G.711; G.723; G.726; G.729	✓	✓
Cancelación de Eco	Sí	✓	✓
Supresión de Silencios	Sí	✓	✓
Manejo de VLAN`s	Sí	✓	✓
Estándares	IEEE 802.1p; IEEE 802.1q; H.323; SIP v2 ; 802.3af	✓	✓
Protocolos	SNMPv1; SNMPv2; SNMPv3; RMON	✓	✓
Administración	GUI; Telnet; CLI	✓	✓
<b>COSTO</b>		<b>\$ 202.00</b>	<b>\$ 245.05</b>

Tabla 4. 16 Costo de teléfonos IP

Dentro del diseño de la red de voz se determinó que se necesitan 28 teléfonos IP para los diferentes usuarios. En base a esta información se muestra los costos referenciales en la tabla 4.17.

Fabricante	Cantidad	Valor Unitario	Valor Total
<b>CISCO</b>	28	\$ 202.00	\$ 5,656.00
<b>AVAYA</b>	28	\$ 245.05	\$ 6,861.40

Tabla 4. 17 Costo total teléfonos IP

#### 4.5.2.6 Costo Total de la Red Activa

Una vez determinados los costos necesarios para los diferentes dispositivos de la red, se debe encontrar el costo total de la red activa a utilizarse en la Unidad Educativa Temporal "Jaime Roldós Aguilera". La tabla 4.18 muestra el costo total de la solución por cada una de las casas fabricantes.

DETALLE	CISCO	JUNIPER / AVAYA
<b>CAPA ACCESO</b>	\$ 15,468.30	\$ 10,440,00
<b>CAPA DISTRIBUCIÓN</b>	\$ 7,081.12	\$ 4,132.50
<b>CAPA CORE</b>	\$ 20,743.66	\$ 31,985,50
<b>ACCESS POINT</b>	\$ 4,187.60	\$ 7,192,00
<b>TELÉFONOS IP</b>	\$ 5,656.00	\$ 6,861.40
<b>SUBOTAL</b>	\$ 53,136.68	\$ 60,611.40
<b>IVA</b>	\$ 6,376.40	\$ 7,273.37
<b>TOTAL</b>	\$ 59,513.08	\$ 67,884.77

Tabla 4. 18 Costo total de la red activa por fabricante

#### 4.5.3 ANÁLISIS DE COSTOS DE OPERACIÓN

Una vez que se haya decidido implementar la red, se deben tomar en cuenta otros valores posteriores a la instalación, como administración y valores recurrentes para el funcionamiento de la misma, por ejemplo el servicio de Internet y sueldo a cancelar al administrador de la red.

Para el caso del servicio de Internet se han analizado dos propuestas comerciales de los principales proveedores de este servicio en la ciudad, las cuales son CNT y Punto Net. Estas propuestas se observan en el anexo O, donde se detallan características técnicas y los valores económicos de la solución planteada.

Entre las principales diferencias entre los dos proveedores se tiene el costo de instalación y la disponibilidad del servicio. CNT no factura valor alguno por la instalación siempre que la distancia máxima entre su nodo de distribución y el lugar a proveer el servicio no supere los 2 Km; mientras que Punto Net factura la instalación por cada metro de fibra óptica que sea tendida desde su nodo al lugar a proveer el servicio.

En cuanto al costo del servicio cabe indicar que es de \$ 90 por cada 1 Mbps, con compartición 1:1 asimétrico.

En la tabla 4.19 se presenta un costo referencial del valor a pagar al administrador de la red y el costo mensual que se debe cancelar por el servicio de Internet, esto en base al ancho de banda sugerido en el numeral 3.5.11 para soportar las aplicaciones diseñadas dentro de la institución.

<b>Servicio</b>	<b>Descripción</b>	<b>Costo</b>
<b>Internet CNT</b>	FO punto a punto, compartición 1:1	\$ 270
	Instalación *	\$ 380
	Inscripción **	\$ 300
<b>Administrador</b>	Sueldo estimado con todos los beneficios de ley	\$800
<b>Subtotal</b>		\$ 1,370.00
<b>IVA</b>		\$ 164.40
<b>Total</b>		\$ 1534.40

**Tabla 4. 19 Costo de operación de la red**

\* El costo de la instalación es facturado siempre y cuando la distancia entre el nodo de distribución más cercano al lugar a proveer del servicio sea mayor a 2000 metros.

\*\* El valor de la inscripción será cancelado una sola vez y con la contratación del servicio.

Para el caso de la Unidad Educativa Temporal “Jaime Roldós Aguilera” no se tendrá que cancelar el valor de la instalación ya que no supera la distancia máxima establecida por CNT.

#### **4.5.4 PARÁMETROS DE SELECCIÓN DE LA MEJOR ALTERNATIVA**

La selección de una alternativa de solución es una de las decisiones más importantes al momento de implementar una red de comunicaciones, por tal razón debe estar sustentada en varios parámetros que determinen el porqué de su selección. Estos parámetros no deben enfocarse solamente en el aspecto económico sino también en factores técnicos así como en garantía, soporte, personal capacitado, etc.

##### **4.5.4.1 Garantía y Soporte Técnico Cisco [86]**

Cisco propone una garantía general para todos sus productos, tanto hardware y *software* la cual cubre un periodo mínimo de 90 días, reemplazando así al equipo siempre y cuando sea verificado que el daño no sea causado por mala utilización.

Otra de las alternativas que ofrece Cisco es prolongar la garantía de los equipos para lo cual sugiere comprar contratos de servicio técnico, proponiendo al cliente poner su equipo en manos de su personal, a través de herramientas y recursos, acceso directo al hardware de Cisco, actualizaciones de contenido, etc.

La opción de soporte técnico al adquirir un equipo Cisco tiene una durabilidad de un año desde el momento de la entrega e igualmente existen servicios que permiten extender este tiempo con su respectivo recargo. Si bien éstos son los parámetros generales que Cisco cubre al adquirir un equipo, cada uno de sus dispositivos puede contar con su propia garantía, para ello se debe leer muy bien el *data sheet* que el fabricante proporciona en cada equipo.

#### 4.5.4.1.1 *Cisco Limited Lifetime Hardware Warranty [87]*

Para el caso de los *switches* la mayoría de estos equipos cuentan con la garantía *Cisco Limited Lifetime Hardware Warranty*; esta garantía dice lo siguiente:

**Duración de la garantía del *hardware*:** Mientras el usuario final original, continúe siendo el propietario o quien utilice el producto. En caso de interrupción de la fabricación de productos, la garantía de soporte Cisco se limita a cinco (5) años a partir del anuncio de la interrupción.

**Procedimiento de sustitución, reparación o reembolso del *hardware*:** Cisco o su centro de servicios hará todo lo comercialmente razonable para enviar una pieza de sustitución dentro de los diez (10) días hábiles siguientes a la recepción de la solicitud del cliente. Tiempos reales de entrega pueden variar según la ubicación del cliente.

#### 4.5.4.2 **Garantía y Soporte Técnico Juniper [88] [89] [90]**

Juniper, ofrece a sus clientes y usuarios una garantía de 90 días desde la entrega del equipo para su inscripción, con lo cual activa la garantía de *hardware* y soporte técnico por un año. Al igual que otros fabricantes cuenta con sus restricciones para poder cubrir sus garantía; así mismo existen garantías propias para cada equipo como la *Enhanced Limited Lifetime Warranty*.

##### 4.5.4.2.1 *Enhanced Limited Lifetime Warranty*

Este tipo de garantía la tienen los *Switches* modelos EX2200, EX3200, EX3300, EX4200, EX4300, EX6200 y está especificado en sus respectivos *data sheet*.

Esta garantía es muy similar a Cisco y se la proporciona solo si el usuario final sea el propietario y quien esté haciendo uso del equipo; cubre un periodo de 5 años la fuente de alimentación y el ventilador del equipo, también cubre el mismo periodo en caso de que este tipo de dispositivo se discontinúe en el mercado.

#### 4.5.5 SELECCIÓN DE LA MEJOR ALTERNATIVA

En base a todos los aspectos antes mencionados y detallados en los numerales anteriores, se recomienda optar por una solución Cisco en caso de querer ser implementada la red diseñada.

Esta recomendación se la hace debido a los siguientes análisis.

**Aspecto económico.-** Al realizar las cotizaciones de los equipos necesarios para la red diseñada, se observa que el costo total de la red con la solución Cisco es menor al costo de la solución Juniper; además Cisco tiene mayor confiabilidad dentro del mundo de las comunicaciones siendo una empresa ya establecida y madura a comparación de Juniper que es relativamente nueva dentro del país.

**Aspecto Técnico.-** Dentro de los equipos cotizados tanto Cisco como Juniper cumplen con las características técnicas mínimas para las necesidades de la institución, incluso se puede concluir que Juniper en algunos aspectos supera a Cisco, sin embargo para las necesidades que se presentan los equipos Cisco son adecuados.

**Garantía y Soporte Técnico.-** Al ser empresas de tecnología las políticas que ofrecen Cisco y Juniper son muy similares. Las garantías de registro son de 90 días y su tiempo de duración de un año desde la fecha de venta, cada casa; fabricante propone servicios adicionales para prolongar el tiempo de garantía y soporte dependiendo de sus equipos. Aquí el factor determinante es la facilidad de contar con un *Partner* dentro del mercado, siendo Cisco quien ofrece mayor facilidades en este factor.

**Administración de la Red.-** La administración de la red es más sencilla en Cisco que Juniper, esto debido a que el sistema operativo *Junos* no es tan difundido en el mundo de las redes, a diferencia del IOS de Cisco.

**Personal Capacitado.-** En los últimos años Cisco se ha difundido con mucha fuerza en el País, y por ende una gran gama de profesionales han optado por capacitarse en certificaciones Cisco como CCNA y CCNP, a diferencia de Juniper que todavía no tiene la acogida suficiente dentro del país por lo que conseguir personal para la administración de la red puede resultar complejo y más costoso.

#### 4.5.6 COSTO TOTAL DE LA RED

En base a la información mostrada en los numerales anteriores, se procede a encontrar el valor total que tendría la implementación de la red, para ello se debe diferenciar entre el costo de inversión inicial y los valores recurrentes para la Institución.

Los costos de la inversión inicial son aquellos en que tan solo se deben cancelar una vez, como por ejemplo la implementación de la red en sí. La tabla 4.20 muestra el costo de la inversión inicial.

DESCRIPCIÓN	COSTO
Red Pasiva	\$ 9,283.70
Red Activa	\$ 59,513.08
Inscripción Servicio Internet	\$ 300
<b>Costo Total</b>	<b>\$ 69,096.78</b>

Tabla 4. 20 Costo total de la inversión inicial para la red INTEGRADA de voz y datos de la Unidad Educativa Temporal “Jaime Roldós Aguilera”

Los valores recurrentes son aquellos que se tendrán que cancelar mensualmente para mantener la red operativa, entre los valores se pueden nombrar los siguientes: salario del administrador y servicio de Internet, en la tabla 4.21 muestra los valores recurrentes que se deberán cubrir por la institución.



DESCRIPCIÓN	COSTO
Servicio de Internet	\$ 270
Salario del Administrador de la red.	\$ 800
<b>Costo Total</b>	<b>\$ 1070</b>

**Tabla 4. 21 Costo total de los valores recurrentes para la Unidad Educativa Temporal “Jaime Roldós Aguilera”**

*“Nota: Los valores mostrados se obtuvieron en base a las proformas realizadas en diferentes distribuidoras de los elementos y equipos a utilizarse en la red; la solución planteada en este proyecto consiste en una sugerencia para la Unidad Educativa Temporal “Jaime Roldós Aguilera”. Sin embargo, la institución puede elegir libremente que elementos o equipos puede utilizar en caso de ser implementada la red INTEGRADA de voz y datos diseñada, siempre y cuando cumplan con las características técnicas recomendadas en el proyecto.”*

## CAPÍTULO 5

### CONCLUSIONES Y RECOMENDACIONES

#### 5.1 CONCLUSIONES

- Las definiciones, conceptos y estándares descritos en el primer capítulo, permiten tener una idea mucho más clara de lo que se necesita para el correcto diseño de una red INTEGRADA de voz y datos dentro de una organización.
- El análisis de la situación actual de la Unidad Educativa Temporal “Jaime Roldós Aguilera” brindó un amplio panorama de cómo se encuentra la Institución y cuáles son sus principales deficiencias, así como sus nuevos requerimientos y servicios.

Gracias a este análisis también se pudo determinar cómo se provee el servicio de Internet a las estaciones de trabajo que lo requieren, y de qué manera se encuentran levantadas estas “redes”, permitiendo así evaluar los elementos activos y pasivos utilizados para las mismas.

- El diseño del sistema de cableado estructurado proporciona el soporte adecuado a la red a diseñarse, además de tener la capacidad de adaptarse a futuras aplicaciones a implementarse y adición de nuevos puntos en caso de ser requerido, ya que el sistema fue diseñado con un margen de 30% de crecimiento.
- Para el diseño de la red INTEGRADA de voz y datos se eligió un modelo de red jerárquico basado en tres capas: acceso, distribución y núcleo; este modelo brinda a la red gran flexibilidad, escalabilidad y seguridad a la red, ya que cada capa tiene definida sus propias funciones.

- La topología seleccionada para el diseño de la red es estrella extendida debido a las características propias de la institución, además de ser la topología recomendada por los estándares de cableado estructurado, agrega ventajas como flexibilidad, movilidad y facilidad en la administración de los puntos de red a diseñarse.
- El diseño de la red INTEGRADA de voz y datos brinda redundancia a nivel de red y enlaces, este mecanismo evitará la caída total de la red de comunicaciones.
- La integración de comunicaciones de voz en la red de datos mediante la tecnología de transmisión de VoIP trae consigo beneficios a la Institución, tanto económicos como técnicos, ya que existirá un ahorro en el uso de líneas telefónicas y sobre todo porque la solución brindará un sistema de comunicación de voz interno a la institución.
- El diseño de la red inalámbrica permite brindar acceso a los usuarios temporales a los servicios ofrecidos por la red, facilitando a los mismos el desarrollo de sus actividades desde lugares donde no se cuenta con acceso a la red cableada.
- La simulación de la red diseñada permitió observar que los servicios a ofrecer cumplen con su objetivo y proveen del servicio a los diferentes puntos de red con que se cuenta. Para la simulación de la red diseñada se utilizó el *software* GNS3 apropiado para la simulación de cada uno de los elementos de la red y equipos de conectividad como son los *switches*,
- Dentro de la simulación de la red se puede apreciar lo importante que resulta establecer QoS, ya que al integrar datos y voz, esta última no puede sufrir retardos ni verse afectada de ninguna manera independientemente de los datos que puedan estarse transmitiendo por la red.

- Si bien la simulación puede resultar una muy buena métrica para valorar el diseño realizado, cabe señalar que su *performance* no será igual al realizado en equipos físicos; la simulación de este proyecto se basa en *software* lo que genera limitantes tanto en tiempos de respuesta como ejemplificaciones. No obstante esto no quiere decir que no sea un método válido para evaluar el diseño realizado.
- La utilización de las herramientas adecuadas puede simplificar en gran parte la realización de una simulación, ya que estas herramientas proporcionan diferentes facilidades como interfaces gráficas, archivos de configuración entre otros.

Dentro del presente proyecto se pueden nombrar herramientas útiles para este propósito, tales como: GNS3, VPCs, y WebMin. Gracias a estas herramientas las simulaciones realizadas se han visto facilitadas y sobre todo muestran un enfoque didáctico de las pruebas.

- Debido a que los equipos con los que la institución cuenta al momento no proveen las características necesarias para el diseño de la red y los mismos no están en condición de ser reutilizados, se han evaluado dos posibles soluciones; seleccionadas en base a las características técnicas determinadas en el capítulo 3 y a sus costos dentro del mercado.

Para ello se analizó las soluciones de los fabricantes CISCO y JUNIPER, líderes en soluciones de comunicaciones para *PYMES*.

- Para la selección de la casa fabricante que proveerá de los equipos de conectividad se analizaron parámetros como seguridad, soporte, flexibilidad entre otros, y en base a ello se determinó que la solución más factible tanto técnica como económica sea CISCO.

- La implementación de la red resulta indispensable para la institución, de no hacerlo la comunicación de la misma se está viendo afectada, generando inconvenientes entre los miembros de la misma y comunidad.

Con la nueva red se tendrá un mejor control de la información, proporcionando a los usuarios seguridad, integridad y confiabilidad. Además de permitir identificar de manera oportuna los posibles incidentes que la red presente, tema que al momento no es factible debido a las características propias de las “redes” creadas.

## **5.2 RECOMENDACIONES**

- Es recomendable tener claros los conceptos a utilizar dentro del diseño, ya que esto facilitará el posterior diseño y sobre todo se tendrá el pleno conocimiento del por qué de las decisiones tomadas en el desarrollo del proyecto.
- Siempre que la institución sea de una gran área física, se recomienda, dividir a la misma en diferentes zonas, esto con la finalidad de facilitar el análisis de estado actual y diseño de la red.
- El correcto levantamiento de la información actual de la Institución permite tener una idea clara y concisa de lo que se necesita para el posterior diseño, por lo que se recomienda que la información tomada sea manejada con cuidado y de manera directa por quien es el encargado del proyecto.
- Se recomienda siempre utilizar los estándares actualizados y aprobados por los diferentes organismos de estandarización, como son la ITU, IEEE, EIA, entre otros. Existen varios estándares descontinuados que aún están siendo implementados, lo que es considerado un error dentro del mundo de comunicaciones, sobre todo si se tiene como propósito certificar a las Organizaciones.

- Para la dimensionamiento del tráfico total a soportarse en la red se recomienda considerar valores promedios actuales para los diferentes servicios, pues estos valores cambian constantemente o son dependientes de la actividad de la organización, por ejemplo accesos a la web, o descargas de archivos.
- Para el diseño de la red inalámbrica es recomendable hacer un estudio in situ de las propagaciones de las señales WiFi, esto con la finalidad de que la red no tenga problemas de bloqueos o interferencias por otras señales, garantizar los servicios en lugares donde no se tiene acceso a la red cableada y permitir movilidad a los usuarios.
- *E-learning* es la nueva propuesta del mundo de las comunicaciones en el ámbito educativo, por lo que se recomienda a la Unidad Educativa Temporal “Jaime Roldós Aguilera” realizar un estudio de esta metodología, puesto que la red INTEGRADA de voz y datos diseñada brinda la flexibilidad suficiente como para agregar este tipo de aplicaciones a la red.
- Es recomendable que la Institución empiece a llevar a cabo una correcta administración de la red, mediante la documentación de los diferentes procesos que se tienen, creación de manuales, SLA de los proveedores y demás información que se considere útil en caso de que nuevo personal ingrese a laborar en la Institución.
- Es recomendable en caso de ser implementada la red INTEGRADA de voz y datos, que en la misma se realicen mantenimientos periódicos preventivos, es decir, al menos 2 mantenimientos anuales.
- Se recomienda a la Unidad Educativa Temporal “Jaime Roldós Aguilera” contratar personal idóneo para la administración y operación de la red INTEGRADA de voz y datos, y en caso de no ser posible, brindar a su actual personal la adecuada capacitación y así poder tener controlado el funcionamiento de la red.

- Para realizar la simulación se recomienda tener interfaces de red físicas, si bien la simulación puede realizarse totalmente basada en software, esto implica una demora bastante considerable, que al momento de realizar pruebas resulta ineficiente y que con el uso de una tarjeta física mejora notablemente.
- En cuanto al desarrollo de los proyectos de titulación, se recomienda que los estudiantes sigan realizando este tipo de proyectos ya que así se tendrá una competitividad dentro del medio, y se buscarán nuevas tecnologías para mejores y más efectivas soluciones.

## BIBLIOGRAFÍA

### PROYECTOS DE TITULACIÓN

- [1] Montaluisa Vera, Daniel Eduardo, “Estudio y Diseño de una red integrada de voz y datos para el Gobierno Provincial de Santo Domingo de los Tsáchilas”, Quito, 2011.
- [2] Solano Pozo, Diego Vinicio, “Estudio y Diseño de una red de voz y datos para la Unidad Educativa Municipal Quitumbe utilizando la tecnología Gigabit Ethernet para soportar servicios en tiempo real de VoIP, video seguridad y videoconferencia”, Quito,2009.
- [3] Bazurto Leones, Juan David y Mena Amores , Diego Alberto, “Rediseño de la red del Instituto Tecnológico Superior Central Técnico”, Quito,2011
- [4] Piedra Orellana, María Esther y Solórzano Valencia, Lucía Marcela, “Análisis comparativo entre alternativas libres y propietarias para la migración de Telefonía tradicional a Telefonía IP”, Universidad Politécnica Salesiana, Cuenca, 2011.

### LIBROS

- [5] TANENBAUM, Andrew S, Redes de Computadoras, Quinta Edición. Prentice Hall, Boston 2011.
- [6] STALLINGS, William; “Comunicaciones y Redes de Computadores”, Séptima Edición, Prentice Hall, Madrid 2004
- [7] Santosh S. Chavan, Generic SNMP Proxy Agent Framework for Management of Heterogeneous Network Elements, India.



- [8] Currículo CCNA, Routing Protocols and Concepts, Versión 4.0,
- [9] Secretaría General de la Unidad Educativa Temporal “Jaime Roldós Aguilera”
- [10] Ing. HIDALGO, Pablo, Folleto de Redes de Área Local (LAN).
- [11] Departamento de Electricidad de la Unidad Educativa Temporal “Jaime Roldós Aguilera”
- [12] Departamento de Informática de la Unidad Educativa Temporal “Jaime Roldós Aguilera”

## REFERENCIAS BIBLIOGRÁFICAS ELECTRÓNICAS

- [13] <http://www.ing.unlp.edu.ar/electrotecnia/procesos/ieee8023.pdf>
- [14] <http://es.wikipedia.org/wiki/Ethernet>
- [15] [http://es.wikipedia.org/wiki/IEEE\\_802.3](http://es.wikipedia.org/wiki/IEEE_802.3)
- [16] <http://www.textoscientificos.com/redes/ethernet/ethernet-vs-ieee8023>
- [17] [http://es.wikipedia.org/wiki/Ethernet#Formato\\_de\\_la\\_trama\\_Ethernet](http://es.wikipedia.org/wiki/Ethernet#Formato_de_la_trama_Ethernet)
- [18] <http://www.ingenieriasystems.com/2013/10/Tecnologias-LAN-Parte-1-de-2.html>
- [19] <http://dialnet.unirioja.es/servlet/articulo?codigo=2332462>
- [20] [http://www.uv.es/~montanan/ampliacion/ampli\\_6.pdf](http://www.uv.es/~montanan/ampliacion/ampli_6.pdf)
- [21] <http://www.monografias.com/trabajos33/estandar-voip/estandar-voip2.shtml>
- [22] <http://www.monografias.com/trabajos33/telecomunicaciones2.shtml>
- [23] <https://eva.fing.edu.uy/mod/resource/view.php?id=32165>
- [24] <http://www.protocols.com/papers/voip2.htm>
- [25] <http://www.voipforo.com/H323/H323ejemplo.php>
- [26] <http://neutron.ing.ucv.ve/fernandezl/Multimedia/Tareas%202005-1/Estandares%20de%20VoIP%20H323%20&%20SIP%20-%20B&W.pdf>
- [27] <http://www.monografias.com/trabajos33/estandar-voip/estandar-voip2.shtml>
- [28] <http://elastixtech.com/puertos-tcp-udp-utilizados-en-elastix/>

- [29] <http://www.monografias.com/trabajos33/estandar-voip/estandar-voip2.shtml>
- [30] <http://www.voipforo.com/codec/codecs.php>
- [31] <http://dspace.ups.edu.ec/bitstream/123456789/158/5/Capitulo%204.pdf>
- [32] [http://www.scielo.org.co/scielo.php?pid=S0123-921X2012000100008&script=sci\\_arttext](http://www.scielo.org.co/scielo.php?pid=S0123-921X2012000100008&script=sci_arttext)
- [33] <http://users.rcn.com/wpacino/jitwtutr/jitwtutr.htm>
- [34] <http://www.slideshare.net/joseorestes/como-funciona-la-telefonía-ip-cisco>
- [35] <http://www.slideshare.net/wilquis/comunicaciones-basadas-en-telefonía-ip>
- [36] <http://www.telefoniavozip.com/voip/ventajas-de-la-telefonía-ip.htm>
- [37] <http://trabajo-sce.blogspot.com/2011/03/definicion-sce.html>
- [38] <http://www.simon.com/us/standards/09-06-10-update-568-c.asp>
- [39] <http://cableado3103.es.tl/Normas-TIA-EIA-568-Y-569.htm>
- [40] <http://buubulubuenajimdo.com/infraestructuras-de-red/norma-ansi-tia-eia-606/>
- [41] <http://www.slideshare.net/neyneyney/norma-ansitiaeia607-11469888>
- [42] <http://aprenderedes.com/2006/06/las-tres-capas-del-modelo-jerarquico-de-cisco/>
- [43] <http://davidmoro.wordpress.com/2013/02/05/>
- [44] [http://es.wikipedia.org/wiki/Cable\\_de\\_categoria\\_6](http://es.wikipedia.org/wiki/Cable_de_categoria_6)
- [45] <http://estoesredes.blogspot.com/2008/07/cuarto-de-telecomunicaciones.html>
- [46] <http://www.slideshare.net/vafalungo/cuarto-de-telecomunicaciones-3294539>
- [47] <http://www.electronica.7p.com/cableado/equipos.htm>
- [48] <http://www.slideshare.net/orrrtiz/cableado-estructurado-1164811>
- [49] [http://e-tcs.org/wp-content/uploads/2012/10/Lyman\\_y\\_Varian\\_-\\_HMI2003.pdf](http://e-tcs.org/wp-content/uploads/2012/10/Lyman_y_Varian_-_HMI2003.pdf)
- [50] <http://tools.pingdom.com/fpt/>

- [51] <http://librosnetworking.blogspot.com/2009/04/metodo-simplificado-para-el-calculo-de.html>
- [52] <http://www.ece.utah.edu/~ece5960/exams/Mldterm%20III/Furse-Erlang%20B%20chart.jpg>
- [53] <http://www.slideshare.net/Comdat4/conmutacion#btnNext>
- [54] <http://www.misrespuestas.com/que-es-un-servidor-web.html>
- [55] <http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html>
- [56] <http://www.zimbra.com/buzz/index.es.html>
- [57] <http://miniacademia.wordpress.com/2013/11/04/instalacin-de-zimbra-server/>
- [58] <http://es.scribd.com/doc/22300726/Especificaciones-Tecnicas-IIS-vs-Apache>
- [59] <http://www.estebanrestrepo.com/es/asterisk/instalacion-de-asterisk>
- [60] <http://www.emb.cl/gerencia/articulo.mvc?xid=865>
- [61] <http://cnmcblog.es/2010/05/28/conceptos-basicos-de-telecos-redes-inalambricas-fijas-y-en-bandas-de-uso-comun/>
- [62] <http://www.consumer.es/web/es/tecnologia/internet/2005/04/04.php>
- [63] <http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa/>
- [64] [http://es.wikipedia.org/wiki/Zona\\_desmilitarizada\\_\(informática\)](http://es.wikipedia.org/wiki/Zona_desmilitarizada_(informática))
- [65] <http://es.wikipedia.org/wiki/VLAN>
- [66] <http://www.shutdown.es/ISO17799.pdf>
- [67] [http://es.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol)
  
- [68] [http://iespicasso-1asir-par.wikispaces.com/file/view/GNS3-0.4.1\\_documentation\\_spanish.pdf/324094426/GNS3-0.4.1\\_documentation\\_spanish.pdf](http://iespicasso-1asir-par.wikispaces.com/file/view/GNS3-0.4.1_documentation_spanish.pdf/324094426/GNS3-0.4.1_documentation_spanish.pdf)
- [69] <http://es.wikipedia.org/wiki/Zimbra>
- [70] <http://es.wikipedia.org/wiki/Asterisk>
- [71] <http://es.wikipedia.org/wiki/Webmin>
- [72] <http://www.nagios-cl.org/que-es-nagios>
- [73] <http://rm-rf.es/anadir-hosts-virtuales-a-topologias-de-red-de-gns3/>

- [74] <http://delfirosales.blogspot.com/2012/02/como-utilizar-un-switch-engns3.html>
- [75] <http://enable-chibcha.blogspot.com/2009/03/trabajando-con-pcs-engns3-metodo-1.html>
- [76]  
[http://www.cisco.com/cisco/web/solutions/small\\_business/products/routers\\_switches/catalyst\\_2960\\_series\\_switches/docs/Catalyst\\_2960\\_Series\\_Switches\\_LAN\\_Lite\\_DS\\_FINAL.pdf](http://www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/catalyst_2960_series_switches/docs/Catalyst_2960_Series_Switches_LAN_Lite_DS_FINAL.pdf)
- [77] <http://www.juniper.net/es/es/products-services/switching/ex-series/ex2200/>
- [78]  
[http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product\\_data\\_sheet09186a00801f3d7d.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.html)
- [79] <http://www.juniper.net/es/es/products-services/switching/ex-series/ex3300/>
- [80]  
[http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/data\\_sheet\\_c78-584733.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/data_sheet_c78-584733.html)
- [81] <http://www.juniper.net/es/es/products-services/switching/qfx-series/qfx3500/>
- [82] <http://www.juniper.net/es/es/products-services/wireless/wla-series/wla322/>
- [83]  
[http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps12555/data\\_sheet\\_c78-715702.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps12555/data_sheet_c78-715702.html)
- [84]  
[http://www.cisco.com/web/ES/solutions/smb/products/voice\\_conferencing/sipa\\_500/index.html](http://www.cisco.com/web/ES/solutions/smb/products/voice_conferencing/sipa_500/index.html)
- [85] <http://www.avaya.com/mx/producto/1200-series-ip-deskphones#Deskphone IP 1210>

- [86]  
[https://supportforums.cisco.com/sites/default/files/legacy/1/0/1/15377101-SB%20Support%20Services\\_AAG\\_FNL\\_Sp.pdf](https://supportforums.cisco.com/sites/default/files/legacy/1/0/1/15377101-SB%20Support%20Services_AAG_FNL_Sp.pdf)
- [87]  
[http://www.cisco.com/c/en/us/td/docs/general/warranty/English/LH2DEN\\_.html](http://www.cisco.com/c/en/us/td/docs/general/warranty/English/LH2DEN_.html)
- [88] <http://www.juniper.net/support/warranty/990220.pdf>
- [89] <http://www.juniper.net/support/warranty/990205.pdf>
- [90] <http://www.juniper.net/support/warranty/990240.pdf>

**Nota:** Todas las referencias electrónicas estuvieron vigentes hasta el día 06/10/2014.