

# **ESCUELA POLITÉCNICA NACIONAL**

**FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA**

**DISEÑO DE UNA RED CONVERGENTE DE VOZ Y DATOS PARA EL  
EDIFICIO MATRIZ DE TRANSELECTRIC S.A Y SU ENLACE CON EL  
COT**

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

**TULIA ISABEL PAVÓN SIERRA  
tulisabel@hotmail.com  
MARÍA DEL CARMEN PEÑAHERRERA PLÚA  
mariaca49@hotmail.com**

**DIRECTOR: ING. PABLO WILLIAM HIDALGO LASCANO  
phidalgo@ieee.org**

**Quito, Mayo 2009**

## CONTENIDO

### CAPÍTULO 1

#### MARCO TEÓRICO. INTRODUCCIÓN A REDES LAN

1.1	INTRODUCCIÓN A LAS REDES INFORMÁTICAS.....	1
1.2	CONSIDERACIONES GENERALES DE REDES INFORMÁTICAS .....	2
1.2.1	REDES DE ÁREA PERSONAL ( <i>PAN</i> ).....	2
1.2.2	REDES DE ÁREA LOCAL ( <i>LAN</i> ) .....	2
1.2.3	REDES DE ÁREA METROPOLITANA ( <i>MAN</i> ) .....	3
1.2.4	REDES DE ÁREA EXTENDIDA ( <i>WAN</i> ).....	3
1.2.5	RED <i>INTERNET</i> .....	4
1.2.6	REDES INALÁMBRICAS.....	4
1.2.7	REDES CONVERGENTES .....	6
1.3	VENTAJAS Y DESVENTAJAS DE LAS REDES .....	7
1.3.1	VENTAJAS .....	7
1.3.2	DESVENTAJAS.....	8
1.4	CLASIFICACIÓN DE LAS REDES DE ÁREA LOCAL .....	8
1.4.1	SEGÚN LAS TÉCNICAS DE TRANSMISIÓN Y DE CONMUTACIÓN .....	8
1.4.1.1	Redes Punto a Punto .....	8
1.4.1.2	Redes de Difusión .....	9
1.4.1.3	Redes de Conmutación de Circuitos .....	9
1.4.1.4	Redes de Conmutación de Mensajes .....	9
1.4.1.5	Redes de Conmutación de Paquetes .....	10
1.4.2	SEGÚN LA TOPOLOGÍA .....	10
1.4.2.1	Topología en Estrella .....	10
1.4.2.2	Topología en Bus .....	11
1.4.2.3	Topología en Anillo .....	12
1.4.2.4	Topologías Híbridas .....	13
1.4.3	POR EL MÉTODO DE ACCESO AL MEDIO .....	13
1.4.3.1	Acceso por Contención, Aleatorio o no Determinístico .....	14
1.4.3.1.1	CSMA ( <i>Carrier Sense Multiple Access</i> ).....	14
1.4.3.1.2	CSMA/CD ( <i>Carrier Sense Multiple Access/Collision Detect</i> ) .....	14
1.4.3.1.3	CSMA/CA ( <i>Carrier Sense Multiple Access/Collision Avoidance</i> ).....	15

1.4.3.2	Acceso Determinístico .....	15
1.4.3.2.1	<i>Token</i> o Testigo .....	15
1.5	EL MODELO OSI .....	16
1.5.1	CAPAS O NIVELES DEL MODELO DE REFERENCIA OSI .....	16
1.5.1.1	Capa Física (Capa 1) .....	17
1.5.1.2	Capa de Enlace de Datos (Capa 2) .....	17
1.5.1.3	Capa de Red (Capa 3) .....	17
1.5.1.4	Capa de Transporte (Capa 4).....	18
1.5.1.5	Capa de Sesión (Capa 5).....	18
1.5.1.6	Capa de Presentación (Capa 6).....	18
1.5.1.7	Capa de Aplicación (Capa 7).....	19
1.5.2	UNIDAD DE DATOS DE PROTOCOLOS (PDU).....	19
1.5.3	TRANSMISIÓN DE LOS DATOS .....	20
1.6	ARQUITECTURA DE REDES LAN .....	20
1.6.1	RED <i>ETHERNET</i> .....	21
1.6.2	REDES <i>TOKEN RING</i> .....	21
1.6.3	FDDI ( <i>Fiber Distributed Data Interface</i> ).....	21
1.7	MEDIOS DE TRANSMISIÓN .....	22
1.7.1	MEDIOS GUIADOS .....	22
1.7.1.1	Par Trenzado .....	22
1.7.1.1.1	Cable STP ( <i>Shielded Twisted Pair</i> ).....	22
1.7.1.1.2	Cable UTP ( <i>Unshielded Twisted Pair</i> ).....	23
1.7.1.1.3	Cable FTP ( <i>Foiled Twisted Pair</i> ) .....	24
1.7.1.2	Par Coaxial .....	25
1.7.1.3	Fibra Óptica .....	26
1.7.1.3.1	Fibra Monomodo .....	27
1.7.1.3.2	Fibra Multimodo .....	27
1.7.1.3.3	Tipos de Conectores .....	29
1.7.1.4	Cable AUI ( <i>Attachment Unit Interface</i> ).....	30
1.7.2	MEDIOS INALÁMBRICOS .....	30
1.7.2.1	Radiofrecuencia .....	31
1.7.2.2	Micro Ondas .....	31
1.7.2.2.1	Microondas Terrestres .....	31
1.7.2.2.2	Microondas por Satélite .....	32
1.7.2.3	Infrarrojo .....	32
1.8	CABLEADO ESTRUCTURADO .....	33
1.8.1	ESTÁNDARES DE CABLEADO ESTRUCTURADO .....	34

1.8.1.1	Estándar EIA/TIA 568.....	35
1.8.2	SUBSISTEMAS DEL SISTEMA DE CABLEADO ESTRUCTURADO .....	36
1.8.2.1	Entrada al Edificio .....	36
1.8.2.2	Cuarto de Equipos .....	36
1.8.2.3	Cableado Horizontal .....	37
1.8.2.4	<i>Backbone</i> .....	37
1.8.2.5	Gabinete o <i>Rack</i> de Telecomunicaciones .....	38
1.8.2.6	Área de Trabajo .....	38
1.9	COMPONENTES DE UNA RED .....	38
1.9.1	EQUIPOS QUE INTERCONECTAN REDES .....	38
1.9.1.1	Repetidores .....	38
1.9.1.2	Concentradores o <i>Hubs</i> .....	39
1.9.1.3	Conmutadores o <i>Switches</i> .....	39
1.9.1.4	Puentes o <i>Bridges</i> .....	39
1.9.1.5	Enrutadores o <i>Routers</i> .....	40
1.9.1.6	<i>Gateways</i> o Puertas de Enlace .....	40
1.9.1.7	Cortafuegos o <i>Firewalls</i> .....	41
1.10	REDES TCP/IP .....	42
1.10.1	DEFINICIÓN .....	42
1.10.2	ARQUITECTURA TCP/IP .....	43
1.10.2.1	Aplicación .....	43
1.10.2.2	Transporte .....	43
1.10.2.2.1	Protocolo UDP ( <i>User Datagram Protocol</i> ).....	44
1.10.2.2.2	Protocolo TCP ( <i>Transport Control Protocol</i> ).....	44
1.10.2.3	<i>Internet</i> o de Red .....	45
1.10.2.3.1	Protocolos del Nivel de Red .....	45
1.10.2.4	Acceso de Red .....	46
1.11	ENRUTAMIENTO Y DIRECCIONAMIENTO .....	46
1.11.1	DIRECCIONAMIENTO .....	46
1.11.2	DIRECCIÓN IP .....	47
1.11.2.1	Direcciones IPv4.....	47
1.11.2.2	Direcciones IPv6.....	47
1.11.2.3	Clases de Dirección IPv4 .....	48
1.11.2.3.1	Clase A .....	48
1.11.2.3.2	Clase B .....	48
1.11.2.3.3	Clase C .....	49
1.11.2.3.4	Clase D .....	49

1.11.2.3.5	Clase E .....	49
1.11.2.4	Direcciones de Red Reservadas .....	49
1.11.2.5	Dirección IP Dinámica .....	50
1.11.2.5.1	Asignación de Direcciones IP .....	50
1.11.2.6	Dirección IP Fija .....	51
1.11.3	MÁSCARA DE SUBRED .....	51
1.11.4	CREACIÓN DE SUBREDES .....	52
1.11.5	TIPOS DE ENRUTAMIENTO .....	52
1.11.5.1	Enrutamiento Estático .....	52
1.11.5.2	Enrutamiento Dinámico .....	52
1.12	RED PRIVADA VIRTUAL (VPN) .....	53
1.12.1	DEFINICIÓN .....	53
1.12.2	REQUERIMIENTOS PARA VPN .....	53
1.12.2.1	Seguridad .....	53
1.12.2.2	Confiabilidad .....	53
1.12.3	TIPOS DE VPN .....	54
1.12.3.1	VPN de Acceso Remoto .....	54
1.12.3.2	VPN Punto a Punto .....	54
1.12.3.3	VPN Interna WLAN .....	54
1.12.4	PROTOCOLOS UTILIZADOS .....	54
1.12.4.1	PPTP .....	55
1.12.4.2	L2F .....	56
1.12.4.3	L2TP .....	56
1.12.5	TIPOS DE CONEXIÓN .....	56
1.12.5.1	Conexión de Acceso Remoto .....	56
1.12.5.2	Conexión VPN <i>Router a Router</i> .....	56
1.12.5.3	Conexión VPN <i>Firewall ASA a Firewall ASA</i> .....	56
1.13	VOZ SOBRE IP .....	57
1.13.1	VOZ SOBRE <i>INTERNET</i> .....	57
1.13.2	FUNCIONALIDAD .....	58
1.13.3	EL ESTÁNDAR VoIP (H.323) .....	58
1.13.3.1	Características Principales .....	58
1.13.3.2	Pila de Protocolos H.323 .....	58
1.13.3.2.1	Direccionamiento .....	59
1.13.3.2.2	Señalización .....	59
1.13.3.2.3	Compresión de Voz .....	59
1.13.3.2.4	Transmisión de Voz .....	59

1.13.3.2.5	Control de la Transmisión .....	59
1.13.3.3	Alcance del Protocolo H.323 .....	60
1.13.4	PROCOLO SIP ( <i>SESSION INITIATION PROTOCOL</i> ) .....	61
1.13.4.1	Definición .....	61
1.13.4.2	Funciones Básicas .....	61
1.13.4.3	Características .....	61
1.13.4.4	Elementos del Protocolo.....	62
1.13.4.4.1	Agentes de Usuario .....	62
1.13.4.4.2	Servidores de Registro .....	62
1.13.4.4.3	Servidores <i>Proxy</i> y de Redirección .....	63
1.13.4.5	Formato de los Mensajes .....	63
1.13.4.6	Establecimiento de una Sesión .....	63
1.13.5	ARQUITECTURA DE RED .....	64
1.13.5.1	Terminales.....	64
1.13.5.2	<i>Gatekeepers</i> .....	65
1.13.5.3	<i>Gateways</i> .....	66
1.13.5.4	Protocolos de VoIP.....	67
1.13.6	PARÁMETROS DE VoIP .....	69
1.13.6.1	<i>Codecs</i> .....	69
1.13.6.2	Retardo o Latencia .....	69
1.13.6.1	Calidad del Servicio.....	69

## **CAPÍTULO 2**

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

2.1	ANTECEDENTES .....	70
2.1.1	MISIÓN .....	71
2.1.2	VISIÓN.....	71
2.1.3	VALORES.....	72
2.1.4	COMPETENCIAS DE LA ORGANIZACIÓN .....	72
2.1.5	INFRAESTRUCTURA .....	72
2.2	SITUACIÓN ACTUAL .....	73
2.2.1	INFRAESTRUCTURA DEL CABLEADO ESTRUCTURADO .....	73
2.2.1.1	Cuarto de Telecomunicaciones .....	74
2.2.1.2	Sala de Servidores .....	77
2.2.1.3	Puntos de Red .....	79

2.2.1.3.1	Contabilización de Puntos de Voz y Datos y su Distribución .....	81
2.2.1.3.2	Muestreo de Puntos existentes de Datos .....	82
2.2.1.4	Cableado Horizontal .....	83
2.2.1.5	Cableado Vertical .....	83
2.2.1.6	Utilización y Características de los <i>Patch Pannels</i> .....	84
2.2.1.6.1	<i>Patch Pannel</i> de Datos (24 ó 48 Puertos) .....	84
2.2.1.6.2	<i>Patch Pannel</i> de Voz (24 Puertos) .....	84
2.2.2	ANÁLISIS DE INFRAESTRUCTURA DE RED .....	85
2.2.2.1	Red LAN .....	85
2.2.2.1.1	Generalidades .....	85
2.2.2.1.2	Elementos de la Red.....	89
2.2.2.1.3	Servicios y Aplicaciones .....	99
2.2.2.1.4	Análisis de Tráfico de la Red .....	105
2.2.2.1.5	Seguridad de la Red .....	117
2.2.2.1.6	Administración de la Red .....	117
2.2.2.2	Red WAN de la Compañía .....	118
2.2.3	ESTRUCTURA DE LA RED DE VOZ .....	120
2.2.3.1	Generalidades .....	120
2.2.3.2	Equipos .....	122
2.2.3.2.1	PABX Panasonic .....	122
2.2.3.2.2	PABX Siemens Hipath 4500.....	123
2.2.3.2.3	ITS Telecom VME Pro .....	124
2.2.3.2.4	Multi-Tech MultiVoIP MVP200.....	125
2.2.3.2.5	<i>Modem</i> Hayes Accura V.92 .....	125
2.2.3.2.6	Base Celular TECOM .....	126
2.2.3.2.7	Base Celular Ericsson .....	127
2.3	REQUERIMIENTOS .....	127
2.3.1	INFRAESTRUCTURA DEL CABLEADO ESTRUCTURADO .....	127
2.3.2	ESTRUCTURA DE LA RED DE DATOS .....	129
2.3.3	ESTRUCTURA DE LA RED DE VOZ .....	131

## CAPÍTULO 3

### DISEÑO DE LA RED LAN DE TRANSELECTRIC S.A.

3.1	INTRODUCCIÓN .....	132
3.2	REQUERIMIENTOS DE ANCHO DE BANDA DE LA RED .....	134

3.2.1	DETERMINACIÓN DEL ANCHO DE BANDA REQUERIDO PARA VOZ .....	134
3.2.1.1	Cálculo de Tráfico en Enlaces hacia la Red de Telefonía Pública .....	139
3.2.2	ESTIMACIÓN DEL ANCHO DE BANDA REQUERIDO PARA DATOS .....	140
3.2.2.1	Tráfico Generado en la Red .....	140
3.2.2.2	Estimación de Tráfico a 10 Años .....	145
3.3	DISEÑO DE LA RED LAN DEL EDIFICIO PRINCIPAL .....	147
3.3.1	CABLEADO ESTRUCTURADO .....	147
3.3.1.1	Subsistema de Administración y Distribución Principal .....	147
3.3.1.2	Subsistema de Cableado Vertical .....	151
3.3.1.3	Subsistema de Distribución Secundaria .....	154
3.3.1.4	Subsistema de Cableado Horizontal .....	158
3.3.1.5	Subsistema de Estaciones de Trabajo .....	161
3.3.1.6	Planos del Edificio con el Nuevo Cableado .....	161
3.3.2	DISEÑO DE LA RED ACTIVA .....	162
3.3.2.1	Elementos Activos a utilizarse .....	162
3.3.2.2	VLANs .....	166
3.3.2.3	Direccionamiento .....	168
3.3.2.4	Diagrama Jerárquico de la Nueva Red .....	169
3.3.2.5	Diagrama Físico de la Nueva Red .....	171
3.3.2.6	Diagrama de VoIP .....	173
3.3.2.7	Aplicaciones, Servicios, Protocolos que soporta .....	173
3.3.3	DISEÑO DEL ENLACE CON CALDERÓN .....	174
3.3.3.1	Dimensionamiento y Cálculo del Enlace .....	174
3.3.3.2	Dimensionamiento del Enlace .....	176
3.4	SEGURIDAD DE LA RED .....	177
3.4.1	SEGURIDAD FÍSICA .....	178
3.4.1.1	Seguridad de Equipos .....	179
3.4.1.2	Seguridad y Respaldo de la Información .....	179
3.4.2	SEGURIDAD LÓGICA .....	180
3.4.3	POLÍTICAS DE SEGURIDAD .....	181
3.4.4	PLAN DE CONTINGENCIA PARA MEJORAR LA DISPONIBILIDAD DE ELEMENTOS DE RED .....	185
3.5	ADMINISTRACIÓN Y MONITOREO DE LA RED .....	186
3.5.1	POSIBLES HERRAMIENTAS PARA LA ADMINISTRACIÓN .....	186



## CAPÍTULO 4

### ANÁLISIS DE COSTOS

4.1	INFRAESTRUCTURA DE ELEMENTOS DE RED .....	188
4.2	ALTERNATIVAS DE EQUIPOS .....	192
4.2.1	ALTERNATIVA 3COM .....	192
4.2.1.1	<i>Switch de Core</i> .....	192
4.2.1.2	<i>Switch de Distribución</i> .....	193
4.2.1.3	<i>Switch de Acceso</i> .....	194
4.2.1.4	<i>Switch de Voz</i> .....	179
4.2.1.5	<i>Switches para Enlace Metro Ethernet</i> .....	198
4.2.1.6	Teléfonos IP .....	198
4.2.2	ALTERNATIVA CISCO .....	200
4.2.2.1	<i>Switch de Core</i> .....	200
4.2.2.2	<i>Switch de Distribución</i> .....	202
4.2.2.3	<i>Switch de Acceso</i> .....	204
4.2.2.4	<i>Switch de Voz</i> .....	207
4.2.2.5	<i>Switches para Enlace Metro Ethernet</i> .....	207
4.2.2.6	Teléfonos IP .....	208
4.3	OTROS ELEMENTOS DE RED .....	210
4.3.1	<i>PATCH PANNELS</i> .....	210
4.3.2	ODFs .....	210
4.3.3	<i>RACKS</i> .....	211
4.3.4	CABLE .....	211
4.3.5	<i>PATCH CORDS</i> .....	211
4.3.6	CAJETINES .....	211
4.3.7	OTROS ELEMENTOS .....	211
4.4	ANÁLISIS DE COSTOS .....	212
4.4.1	COSTOS PARTE ACTIVA .....	212
4.4.1.1	<i>Switches de Core</i> .....	212
4.4.1.2	<i>Switches de Distribución</i> .....	212
4.4.1.3	<i>Switches de Acceso</i> .....	213
4.4.1.4	<i>Switches de VoIP</i> .....	213
4.4.1.5	<i>Switches Metro Ethernet</i> .....	214
4.4.1.6	Teléfonos IP .....	214
4.4.1.7	Costo Total .....	215
4.4.1.8	Alternativa que se escoge .....	215
4.4.2	COSTOS PARTE PASIVA .....	216

4.4.2.1	<i>Patch Pannels</i> .....	216
4.4.2.2	<i>Patch Cords</i> de Fibra .....	217
4.4.2.3	ODFs .....	218
4.4.2.4	<i>Racks</i> .....	218
4.4.2.5	Cableado .....	218
4.2.3	COSTOS DE INSTALACIÓN Y MONTAJE .....	219
4.2.4	TOTAL COSTOS .....	220
4.2.5	BENEFICIOS DE LA NUEVA RED .....	221

## CAPÍTULO 5

### CONCLUSIONES Y RECOMENDACIONES

5.1	CONCLUSIONES .....	223
5.2	RECOMENDACIONES .....	229

REFERENCIAS BIBLIOGRÁFICAS .....	232
----------------------------------	-----

### ANEXOS

Anexo 1.1	Estándares IEEE 802.3 <i>Ethernet</i> e IEEE 802.5 <i>Token Ring</i>
Anexo 1.2	Estándares de Cableado Estructurado ANSI/EIA-TIA
Anexo 2.1	Equipo <i>Check Point</i> VPN-1 UTM
Anexo 2.2	Equipos <i>PacketShaper</i> 3500 y <i>Packeteer</i> 1550
Anexo 2.3	Tipos de Paquetes encontrados en el Monitoreo de la Red LAN
Anexo 3.1	Planos de los Puntos de Red del Edificio
Anexo 4.1	Especificaciones Técnicas de Nuevos Equipos considerados para el Diseño
Anexo 4.2	Cotizaciones de Equipos

## ÍNDICE DE FIGURAS

### FIGURAS CAPITULO 1

Figura 1.1 Redes de Área Local .....	2
Figura 1.2 Redes de Área Extendida .....	4
Figura 1.3 Estándares <i>Wireless</i> .....	5
Figura 1.4 Red Convergente.....	6
Figura 1.5 Topología en Estrella .....	11
Figura 1.6 Topología en Bus .....	11
Figura 1.7 Topología en Anillo .....	12
Figura 1.8 Topologías Híbridas.....	13
Figura 1.9 CSMA/CD.....	14
Figura 1.10 Capas del modelo de referencia OSI .....	16
Figura 1.11 PDUs en La transmisión de los datos en el modelo OSI .....	19
Figura 1.12 Cable STP .....	23
Figura 1.13 Cable UTP .....	23
Figura 1.14 Cable FTP .....	25
Figura 1.15 Componentes del cable FTP .....	25
Figura 1.16 Cable Coaxial .....	26
Figura 1.17 Fibra Óptica .....	27
Figura 1.18a Fibra Monomodo .....	28
Figura 1.18b Fibra Multimodo .....	28
Figura 1.19 Tamaños de la Fibra Óptica .....	29
Figura 1.20 Tipos de Conectores para Fibra Óptica .....	30
Figura 1.21 Estándares EIA/TIA 568-A y EIA/TIA 568-B .....	36
Figura 1.22 Niveles de Arquitectura TCP/IP .....	43
Figura 1.23 Protocolos de capa transporte en Arquitectura TCP/IP .....	44
Figura 1.24 Control de Transmisión en Protocolo H.323 .....	60
Figura 1.25 Alcance del Protocolo H.323.....	60
Figura 1.26 Teléfono IP .....	64
Figura 1.27 Elementos de una red VoIP .....	68

### FIGURAS CAPÍTULO 2

Figura 2.1 Red de Fibra Óptica de Transelectric S.A. ....	71
Figura 2.2 Ubicación del Edificio Matriz de Transelectric S.A. ....	73
Figura 2.3 Cuarto de Telecomunicaciones Piso 5 .....	75
Figura 2.4 Cuarto de Telecomunicaciones Piso 9 .....	76
Figura 2.5 Gabinetes de servidores de la sala de servidores Piso 5 .....	78

Figura 2.6 <i>Racks</i> de comunicaciones de la sala de servidores Piso 5.....	79
Figura 2.7a Resultados de <i>Fluke</i> cuando un cable pasa las pruebas .....	80
Figura 2.7b Resultados de <i>Fluke</i> cuando un cable falla .....	80
Figura 2.8 <i>Patch Pannel</i> de 48 puertos .....	84
Figura 2.9 <i>Patch Pannel</i> de 24 puertos .....	84
Figura 2.10 Red LAN .....	87
Figura 2.11 <i>Switches</i> Cisco Systems .....	90
Figura 2.12 <i>Switches</i> 3Com .....	92
Figura 2.13 <i>Switches</i> D-Link .....	93
Figura 2.14 <i>Router</i> Cisco 2800 series .....	94
Figura 2.15 <i>Router</i> Cisco 2600 series .....	94
Figura 2.16 <i>Switch</i> Cisco 871 .....	95
Figura 2.17 <i>Check Point</i> VPN-1 UTM <i>Edge</i> .....	96
Figura 2.18 <i>PacketShaper</i> .....	97
Figura 2.19a Tráfico promedio de la red del edificio matriz .....	107
Figura 2.19b Tráfico pico de la red del edificio matriz .....	107
Figura 2.20a Utilización total de la red en entrada .....	108
Figura 2.20b Rendimiento total de la red en entrada .....	109
Figura 2.21a Utilización total de la red en salida .....	109
Figura 2.21b Rendimiento total de la red en salida .....	110
Figura 2.22 Red WAN de Transelectric S.A .....	119
Figura 2.23 Red de Voz .....	121
Figura 2.24 PABX Panasonic .....	122
Figura 2.25 PABX Siemens .....	123
Figura 2.26 Autocontestador VME Pro .....	124
Figura 2.27 MultiVoIP MVP200.....	125
Figura 2.28 <i>Modem</i> Hayes Accura V.92 .....	125
Figura 2.29 Base TECOM .....	126
Figura 2.30 Base Ericsson .....	127

### FIGURAS CAPÍTULO 3

Figura 3.1 Gráfica de <i>Erlangs</i> .....	136
Figura 3.2 Calculadora de <i>Erlangs</i> y Ancho de Banda en VoIP .....	138
Figura 3.3 Tráfico promedio de uso de <i>Internet</i> .....	142
Figura 3.4 Tráfico pico de uso de <i>Internet</i> .....	143
Figura 3.5 Tráfico promedio de uso de Correo .....	143
Figura 3.6 Tráfico pico de uso de Correo .....	144
Figura 3.7 Estimación de tráfico del edificio matriz a 10 años .....	146
Figura 3.8 <i>Rack</i> de Datos .....	148
Figura 3.9 <i>Rack</i> de Voz .....	149
Figura 3.10 Elementos del <i>Rack</i> de Ala .....	155
Figura 3.11 <i>Patch Pannel</i> de 48 puertos .....	158
Figura 3.12 <i>Patch Pannel</i> de 24 puertos .....	158
Figura 3.13 Ubicación del <i>Rack</i> de ala .....	162
Figura 3.14 Configuración de VLANs .....	167

Figura 3.15 Diagrama jerárquico físico de la nueva red .....	170
Figura 3.16 Ejemplo de conexión de una de las alas con el 5to Piso .....	172
Figura 3.17 Diagrama de VoIP .....	173
Figura 3.18 Características de <i>Metro Ethernet</i> con fibra óptica .....	175
Figura 3.19 Servicios de <i>Metro Ethernet</i> .....	175
Figura 3.20 Comunicación del Edificio Matriz de TRANSELECTRIC con la oficina de Calderón .....	176

#### FIGURAS CAPÍTULO 4

Figura 4.1 <i>Switch</i> 3Com 8810 .....	192
Figura 4.2 <i>Switch</i> 3Com 5500G-EI .....	193
Figura 4.3 <i>Switch</i> 3Com 4500G para VoIP .....	194
Figura 4.4 <i>Switch</i> 3Com 2250 Plus .....	195
Figura 4.5 <i>Switch</i> 3Com 2024 .....	195
Figura 4.6 <i>Switch</i> 3Com Office Connect Manager Gigabit .....	197
Figura 4.7 <i>Switch</i> 3Com <i>Intellijack</i> .....	198
Figura 4.8 Teléfono IP 3Com 3100 .....	198
Figura 4.9 Teléfono IP 3Com 3101 .....	199
Figura 4.10 Teléfono IP 3Com 3106 .....	200
Figura 4.11 <i>Switch</i> CISCO Catalyst 6509-E .....	201
Figura 4.12 <i>Switch</i> CISCO Catalyst 3560-E .....	202
Figura 4.13 <i>Switch</i> CISCO Catalyst 2960 Series .....	204
Figura 4.14 <i>Switch</i> CISCO Catalyst 2960 de 8 Puertos .....	207
Figura 4.15 <i>Switch</i> CISCO Catalyst ME 3400 .....	208
Figura 4.16 Teléfono IP de la serie 500 .....	209

## ÍNDICE DE TABLAS

### TABLAS CAPÍTULO 1

Tabla 1.1 Categoría de cables UTP .....	24
Tabla 1.2 Rango de Frecuencias de Medios Inalámbricos.....	31
Tabla 1.3 Características de las bandas en medios inalámbricos.....	33
Tabla 1.4 Tipo de cables requeridos para cableado <i>backbone</i> .....	37
Tabla 1.5 Direcciones IP .....	47
Tabla 1.6 Clases de Direcciones IP .....	49
Tabla 1.7 Determinación de Subredes .....	52
Tabla 1.8 Protocolos de VoIP .....	68

### TABLAS CAPÍTULO 2

Tabla 2.1 Puntos de voz y datos del edificio .....	81
Tabla 2.2 Funcionamiento actual de los puntos de datos .....	82
Tabla 2.3a Distancias de los diferentes pisos al Cuarto de Telecomunicaciones del Piso 5 .....	84
Tabla 2.3b Distancias de los diferentes pisos al Cuarto de Telecomunicaciones del Piso 9 .....	84
Tabla 2.4 Distribución de <i>Switches</i> en el Edificio Matriz.....	91
Tabla 2.5 Servidores .....	98
Tabla 2.6 PC's .....	99
Tabla 2.7 Aplicaciones de la Compañía .....	100
Tabla 2.8 Servicios de la Compañía .....	103
Tabla 2.9 Tráfico del <i>switch</i> del Piso 5 promedio semanal .....	113
Tabla 2.10 Tráfico del <i>switch</i> del Piso 9 promedio semanal .....	115
Tabla 2.11 Promedio aproximado del tráfico de los <i>switches</i> de distribución en cada media hora .....	116

### TABLAS CAPÍTULO 3

Tabla 3.1 <i>Codecs</i> .....	137
Tabla 3.2 Utilización de consumo de ancho de banda por estación de trabajo.....	144
Tabla 3.3 Estimación de tráfico del edificio matriz a 10 años .....	146
Tabla 3.4 Área del Cuarto de Equipos .....	150
Tabla 3.5 Distancias aproximadas de fibra óptica para el cableado vertical .....	152
Tabla 3.6 Características de la fibra óptica .....	153
Tabla 3.7 Puntos a instalar, cortar y certificar .....	156
Tabla 3.8 Características de cable UTP categoría 5E (Marca Nexxt) .....	157
Tabla 3.9 Cables permitidos en las tuberías .....	160
Tabla 3.10 Asignación de <i>switches</i> por ala .....	165
Tabla 3.11 Características de los <i>switches</i> de <i>core</i> , distribución y acceso .....	166
Tabla 3.12 Usuarios que ocupan la red de TRANSELECTRIC S.A .....	168

Tabla 3.13 Direccionamiento IP del edificio Matriz .....	168
--	-----

#### **TABLAS CAPÍTULO 4**

Tabla 4.1a Requerimientos de <i>switch</i> de <i>core</i> .....	191
Tabla 4.1b Requerimientos de <i>switch</i> de distribución. ....	191
Tabla 4.1c Requerimientos de <i>switch</i> de acceso .....	191
Tabla 4.2 Distribución de <i>switches</i> 3Com .....	196
Tabla 4.3 Distribución de <i>switches</i> Cisco .....	206
Tabla 4.4 Costo de los equipos de <i>core</i> .....	212
Tabla 4.5 Costo de los equipos de distribución .....	213
Tabla 4.6 Costo de los equipos de acceso.....	213
Tabla 4.7 Costo de los equipos de VoIP .....	214
Tabla 4.8 Costo de los equipos para Metro Ethernet .....	214
Tabla 4.9 Costo de Teléfonos IP .....	214
Tabla 4.10 Costo total de ambas alternativas .....	215
Tabla 4.11 Costo total de <i>patch pannels</i> .....	217
Tabla 4.12 Costo total de <i>patch cords</i> de fibra .....	217
Tabla 4.13 Costo total de ODFs .....	218
Tabla 4.14 Costo total de <i>racks</i> .....	218
Tabla 4.15 Costo total de otros elementos de cableado .....	219
Tabla 4.16 Costo total de instalación .....	220
Tabla 4.17 Costo total del proyecto .....	220

## RESUMEN

En el primer capítulo se revisan los conceptos esenciales y fundamentos de las Redes de Área Local (voz y datos). Se analizan también sus características, funcionalidades, aplicaciones, direccionamiento, cableado, entre otros, siendo útil esta teoría para comprender mejor los conceptos necesarios en el diseño de la red. Se mencionan también conceptos de la tecnología VoIP que son de utilidad para el diseño.

En el segundo capítulo se indica la misión, visión, valores, infraestructura, ubicación y cantidad de usuarios de TRANSELECTRIC S.A. Además se presenta el análisis de la situación actual de la Compañía, identificando elementos activos y pasivos, topología física y lógica, cableado (puntos de red, cuantificación, conocimiento de los existentes y requeridos y distribución de los mismos), equipos, etc. Se realiza un análisis del tráfico generado por servicios y aplicaciones informáticos, rendimiento de la red, entre otros.

También en este segundo capítulo se establecen los puntos de voz, los equipos que se tiene para lograr la comunicación y se presenta a manera de conclusión los requerimientos que tiene la infraestructura tanto de datos como de voz.

En el tercer capítulo, a partir de los resultados y requerimientos obtenidos en el análisis de la situación actual, se procede al diseño de la nueva Red Convergente de voz y datos para el edificio matriz de TRANSELECTRIC S.A. incluyendo el redimensionamiento del enlace hacia el COT en Calderón a través de la tecnología Metro Ethernet para tener ambos lugares como parte de una misma red LAN.

El diseño especifica los subsistemas de cableado estructurado, los elementos activos y pasivos (los que aún serán utilizados y los que se añadirán o cambiarán de acuerdo a los requerimientos), el diagrama, la nueva propuesta de



direccionamiento IP, los servidores y demás elementos, de tal manera que cumpla con todos los requerimientos existentes y futuros de la Red de TRANSELECTRIC S.A.

El diseño incluye también algunos lineamientos que se pueden usar para la administración y seguridad de red, como posibles herramientas de administración, criterios para establecer políticas de seguridad para lograr confiabilidad en la misma, entre otros. A su vez se menciona un plan de contingencia básico para mejorar la disponibilidad, basándose en la información existente sobre la red de servidores, equipos de conectividad y otros elementos críticos.

En el cuarto capítulo se proponen dos alternativas de equipos acorde a las características mínimas y requerimientos explicados en el capítulo 3, siendo estas dos alternativas Cisco y 3Com, que son marcas reconocidas y por razones de homogenización de equipos y administración de red. Se incluye el costo total de las alternativas y se escoge una de ellas de acuerdo a criterios organizacionales que se tienen en la Compañía; algunos de los criterios que se toman en cuenta son: aspectos económicos, técnicos, futuro crecimiento y aplicaciones. Este análisis de costos permite evaluar la inversión que pudiera tener la empresa en caso de que decida implementar el proyecto.

En el quinto capítulo, se exponen las conclusiones y recomendaciones obtenidas con el desarrollo del proyecto.

Este proyecto no contempla el diseño de la Red de Área Local en el COT, así como la implementación de la nueva infraestructura diseñada en el presente estudio.

Dentro de los anexos se presentan los estándares 802.3 *Ethernet* e IEEE 802.5 *Token Ring*, estándares de cableado estructurado ANSI/EIA-TIA, tipos de paquetes encontrados en el monitoreo al analizar la situación actual, *datasheets* de principales equipos, planos de puntos de red del edificio y cotizaciones de los proveedores.

## PRESENTACIÓN

El presente plan de proyecto de titulación pretende diseñar la Red Convergente de voz y datos del edificio matriz de TRANSELECTRIC S.A. y su enlace con el COT, cumpliendo los requerimientos de ancho de banda necesarios para los Servicios y Aplicaciones informáticos de Red de la compañía.

El edificio matriz de TRANSELECTRIC S.A. se encuentra situado en la ciudad de Quito, tiene 10 pisos y un número aproximado de 200 usuarios locales. A su vez se conecta a la red LAN del COT (oficinas en Calderón) a través de un enlace de 512 Kbps. En el Centro de Operación de Transmisión se tiene un número aproximado de 40 usuarios locales y es el área responsable de la operación del SNT (Sistema Nacional de Transmisión de Electricidad).

El análisis de la infraestructura actual de la red (arquitectura y topología, elementos activos y pasivos, equipos, aplicaciones y servicios) permite conocer los requerimientos actuales que posee la Compañía en cuanto su red LAN y establece un punto de partida para el nuevo diseño.

El diseño de una Red Convergente de voz y datos para el edificio matriz de la Compañía incluyendo políticas de seguridad y administración de red, permitirá su adecuado funcionamiento en cuanto a servicios y aplicaciones informáticos y a la vez el futuro crecimiento de los mismos, a partir de la infraestructura actual de comunicaciones e informática.

Resumiendo, el objetivo de este diseño es que preste un servicio óptimo a sus usuarios, garantizando menor tiempo de acceso, mayor confiabilidad, aumento de los niveles de seguridad tanto en la red convergente como en la comunicación entre el edificio matriz de TRANSELECTRIC y el COT en Calderón.

# CAPÍTULO 1

**MARCO TEÓRICO.  
INTRODUCCIÓN A  
REDES LAN**

## **MARCO TEÓRICO. INTRODUCCIÓN A REDES LAN**

### **1.1 INTRODUCCIÓN A LAS REDES INFORMÁTICAS**

Una red es un conjunto de dispositivos físicos (*hardware*) y de programas (*software*), mediante el cual se pueden comunicar computadoras para compartir ya sea recursos o trabajo. A cada computadora conectada a la red se le denomina un nodo.

La generalización del computador personal y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas, enviar mensajes y compartir archivos desde un computador personal.

Las primeras redes que se instalaron en algunas compañías, incluyendo IBM, Honeywell y DEC (*Digital Equipment Corporation*), tenían sus propios estándares que definían la forma de conectar las computadoras entre sí. Estos estándares establecieron los mecanismos necesarios para transmitir información de una computadora a otra, pero estas primeras especificaciones no fueron enteramente compatibles entre ellas.

Posteriormente, las organizaciones dedicadas a la creación de estándares, incluyendo la ISO (*International Standards Organization*) y el IEEE (*Institute of Electrical and Electronic Engineers*), desarrollaron modelos que fueron reconocidos y aceptados internacionalmente como estándares para el diseño de cualquier red de

computadoras.

## 1.2 CONSIDERACIONES GENERALES DE REDES INFORMÁTICAS

### 1.2.1 REDES DE ÁREA PERSONAL (PAN)

Son redes orientadas a las personas, ya que les permite comunicarse a través de dispositivos personales (PDAs, agendas electrónicas, computadoras portátiles, etc.). Son redes pequeñas que normalmente alcanzan unos pocos metros, están conformados por no más de 8 equipos. Pueden tener una capacidad entre los 10 bps hasta los 10 Mbps. Existen soluciones que operan en la frecuencia libre para instrumentación, ciencia y medicina (2.4 GHz) y pueden tener una velocidad máxima de 54 Mbps.

### 1.2.2 REDES DE ÁREA LOCAL (LAN)

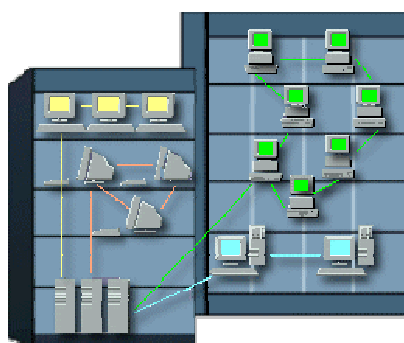


Figura 1.1 Redes de Área Local <sup>[1]</sup>

Permiten la interconexión de varios computadores y periféricos para compartir recursos e intercambiar información; están limitadas físicamente a un edificio o a un entorno de hasta unos cuantos kilómetros (Figura 1.1). Suelen emplear tecnología de difusión mediante un cable al que están conectadas todas las máquinas. Operan

generalmente a velocidades entre 10 y 1000 Mbps. Tienen bajo retardo y experimentan pocos errores.

### **1.2.3 REDES DE ÁREA METROPOLITANA (MAN)**

Son una versión más grande que las redes LAN y se basan en una tecnología similar a ésta. Abarcan desde un grupo de oficinas corporativas cercanas a una ciudad y son redes de alta velocidad que ofrecen velocidades que van usualmente desde los 2 Mbps a los 155 Mbps.

En los últimos tiempos, el servicio Ethernet sobre redes metropolitanas de fibra óptica ha estado cobrando impulso. Los principales motivos de este desarrollo son el aumento de las prestaciones de alta velocidad con un buen servicio y el mantenimiento uniforme de los protocolos entre el cliente y las redes de los proveedores, a fin de eliminar la complejidad de las interconexiones y los gastos indirectos.

Las unidades de terminación de redes Ethernet permiten a los proveedores de servicios implementar un lazo local de acceso basado en Ethernet. Estos dispositivos dedicados con gestión actúan como una demarcación entre las instalaciones del cliente y la red de la operadora. Incorporan funciones de gestión de tráfico, como limitación de velocidad, y realizan diferenciación de clase de servicio mediante compresión/etiquetado VLAN (*Virtual Local Area Network*). Este enfoque extiende el alcance del proveedor de servicios sobre fibra óptica, facilitando la gestión de servicios diferenciados hasta las instalaciones del cliente.

Últimamente han aparecido en el mercado equipos con Gigabit Ethernet, es decir, que trabajan a 1000 Mbps; como sigue siendo una tecnología de área local, es más barata que las otras de gran alcance.

#### 1.2.4 REDES DE ÁREA EXTENDIDA (WAN)

Generalmente conectan entre sí varias LAN atravesando importantes distancias geográficas, del orden del tamaño de un país o de un continente, como se puede ver en la Figura 1.2. La velocidad disponible en las WAN varía según la tecnología y el costo de las conexiones (aumenta con la distancia). Funcionan con *routers*<sup>1</sup> que tomarán los datos para llegar a un nodo de la red eligiendo la ruta más apropiada.

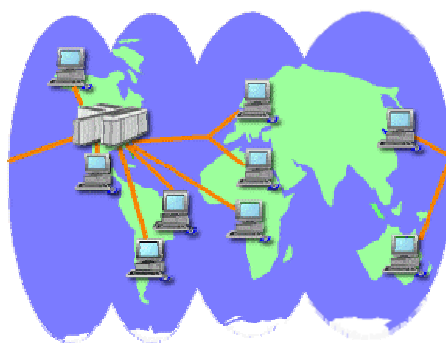


Figura 1.2 Redes de Área Extendida <sup>[1]</sup>

Tienen varios elementos:

- ✓ *Líneas de comunicación*: Mueven *bits* de una máquina a otra.
- ✓ *Elementos de conmutación*: Máquinas especializadas que conectan dos o más líneas de transmisión.

#### 1.2.5 RED INTERNET

Es una interconexión descentralizada de redes locales implementada en un conjunto de protocolos denominado TCP/IP (*Transmission Control Protocol / Internet Protocol*). Garantiza que redes físicas heterogéneas funcionen como una red lógica única, de alcance mundial, empleando computadores especiales para cada red, conocidos como *gateways*<sup>1</sup>.

<sup>1</sup> Referirse al numeral 1.9 de este capítulo

## 1.2.6 REDES INALÁMBRICAS

Son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

Estas redes son de rápida y fácil instalación, permiten la movilidad y tienen menor costo de mantenimiento que una red convencional. Se pueden clasificar según el tamaño (cobertura) de red. En la figura 1.3 se muestran las diferentes redes inalámbricas con los estándares correspondientes.

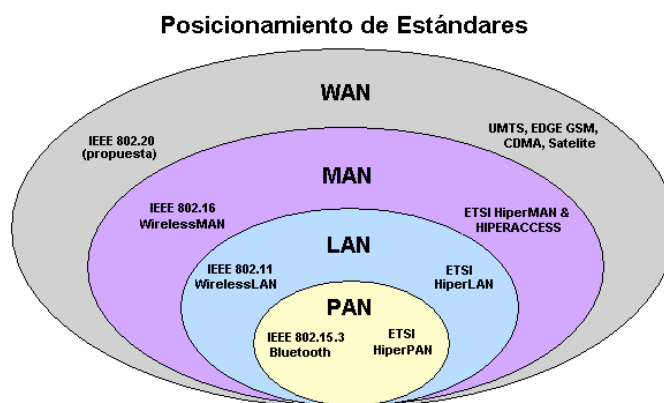


Figura 1.3 Estándares Wireless <sup>[2]</sup>

- ✓ **WPAN (Wireless Personal Area Network):** Basadas en HomeRF (Conecta todos los teléfonos móviles de la casa y los ordenadores); Bluetooth (IEEE 802.15.1); ZigBee (IEEE 802.15.4); RFID (Radio Frequency Identification).
- ✓ **WLAN (Wireless Local Area Network):** Basadas en HiperLAN (High Performance Radio LAN), un estándar del grupo ETSI; o, en Wi-Fi (Wireless-Fidelity) que sigue el estándar IEEE 802.11 con diferentes variantes.
- ✓ **WMAN (Wireless Metropolitan Area Network):** Basadas en el estándar de comunicación inalámbrica Wimax (Worldwide Interoperability for Microwave Access).



- ✓ *WWAN (Wireless Wide Area Network)*: Basadas en UMTS (*Universal Mobile Telecommunications System*). Utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología GSM (para móviles 2G), o también GPRS (*General Packet Radio Service*).

### 1.2.7 REDES CONVERGENTES

Son llamadas también redes multiservicio, hacen referencia a la integración de los servicios de voz, datos y video en una sola red basada en el protocolo IP de nivel de red (Figura 1.4). Tradicionalmente, estos servicios se han ofrecido en forma separada sobre redes especializadas.



Figura 1.4 Red Convergente <sup>[3]</sup>

En la gran mayoría de corporaciones, por ejemplo, la red de voz se basa en uno o varios PBX (*Private Branch eXchange*) conectados a la PSTN (*Public Switched Telephone Network*) externa; mientras que la red de datos se basa en conmutadores y enrutadores IP interconectando redes LAN y permitiendo el acceso a *Internet*. Sin embargo, cada vez es mayor la necesidad de una red única en la que tanto la voz como los datos y el video converjan naturalmente. Así mismo, se amplían los servicios con soluciones de alto valor añadido: correo de voz, almacenamiento y envío de *faxes*, mensajería unificada, centro de atención de llamadas en *Web*, llamada de Internet en espera, etc.

Además, las redes convergentes permiten reducir costos de administración, mantenimiento y manejo de la información, aumentar la productividad y disminuir los tiempos de atención a los clientes.

### **1.3 VENTAJAS Y DESVENTAJAS DE LAS REDES**

Las redes de área local tienen un papel muy importante dentro de las diferentes organizaciones, han evolucionado de forma tal que se tiene contacto con ellas todos los días. Una de las utilidades significativas que brindan son los servicios de red, como correo y agendas electrónicas, que facilitan la comunicación dentro de las organizaciones para notificar a alguien de un evento.

El hecho de compartir recursos dentro de la red se convierte en algo natural y ayuda a economizar recursos y a incrementar el nivel de productividad en las organizaciones. Además, se puede decir que el único camino disponible para utilizar un solo programa en una aplicación específica en toda la organización y ayudar a la estandarización del *software* es el uso de las redes de área local.

#### **1.3.1 VENTAJAS**

- ✓ Permiten la integración de varios puntos en un mismo enlace.
- ✓ Permiten que los usuarios compartan diferentes periféricos tales como *scanner*, *modem*, *fax* o impresora.
- ✓ Permiten que los usuarios puedan compartir grandes cantidades de información a través de distintos programas, bases de datos, etc., de manera que sea más fácil su uso y actualización.
- ✓ Permiten que los usuarios “corran” programas que no se hallan instalados en sus propias computadoras sino, en alguna otra parte de la red. Esto reduce el esfuerzo de los administradores de las redes para mantener los programas correctamente configurados y ahorra mucho espacio de almacenamiento.

- ✓ Establece enlaces con *mainframes*, así una computadora de gran potencia actúa como servidor haciendo que puedan acceder a los recursos disponibles en ella cada una de las computadoras personales conectadas.
- ✓ Permite mejorar la seguridad y control de la información que se utiliza, permitiendo el acceso de determinados usuarios únicamente a cierta información o impidiendo la modificación de diversos datos.

### **1.3.2 DESVENTAJAS**

- ✓ Debido a que acceden a cualquier información a lo largo de una red, la búsqueda es más lenta que acceder a la propia computadora.
- ✓ Existen algunos programas capaces de capturar paquetes, de forma que se puede disponer de la contraseña de la red y de esta forma tener acceso al sistema, poniendo en peligro la seguridad de la información.
- ✓ Debido a que los archivos compartidos se pueden encontrar en todos los equipos es difícil hacer un control de manera centralizada, ya que la política de seguridad mínima es la protección mediante contraseñas y no todos los usuarios las configuran.
- ✓ Toda red es vulnerable a *sniffers*, analizadores de protocolos, *spoofing* (comunicación TCP/IP usando una dirección IP de usuarios autorizados).
- ✓ Un punto débil en una red inalámbrica es el hecho de no poder controlar el área que cubre la señal de la red. Por eso, es posible que la señal exceda el perímetro del edificio y alguien desde afuera pueda visualizar la red e intentar ganar acceso a ésta.

## **1.4 CLASIFICACIÓN DE LAS REDES DE ÁREA LOCAL**

### **1.4.1 SEGÚN LAS TÉCNICAS DE TRANSMISIÓN Y DE CONMUTACIÓN**

#### **1.4.1.1 Redes Punto a Punto**

Consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete puede visitar primero una o más máquinas intermedias.

Un enlace punto a punto resulta apropiado para organizaciones con pocas localizaciones y velocidades de transmisión constantes. Sin embargo, la principal desventaja es la pérdida de ancho de banda por mala utilización lo cual es casi inevitable por la propia naturaleza del tráfico a ráfagas tan común en las aplicaciones actuales.

#### **1.4.1.2 Redes de Difusión**

Tienen un solo canal de transmisión compartido por todas las máquinas de la red. Los mensajes o paquetes que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a qué máquina se dirige. Al recibir un paquete, una máquina verifica el campo de dirección; si el paquete está dirigido a ella, lo procesa, si está dirigido a otra máquina, lo ignora.

#### **1.4.1.3 Redes de Conmutación de Circuitos**

Son aquellas en la que los equipos de conmutación deben establecer un camino físico entre los medios de comunicación previo a la conexión entre los usuarios. Este camino permanece activo durante la comunicación, liberándose al terminar ésta. El ejemplo más común es una red telefónica conmutada. Su funcionamiento pasa por las siguientes etapas: solicitud, establecimiento, transferencia de datos y liberación de la conexión.

#### **1.4.1.4 Redes de Conmutación de Mensajes**

Este método es el más antiguo que existe. Para transmitir un mensaje a un receptor, el emisor debe enviar primero el mensaje completo a un nodo intermedio el cual lo añade a la cola donde almacena los mensajes que le son enviados por otros nodos. Luego, cuando llega su turno, lo reenviará a otro y éste a otro y así las veces que sean necesarias antes de llegar al receptor. El mensaje deberá ser almacenado por

completo y de forma temporal en el nodo intermedio antes de poder ser reenviado al siguiente, por lo que los nodos temporales deben tener una gran capacidad de almacenamiento.

#### **1.4.1.5 Redes de Conmutación de Paquetes**

El emisor divide los mensajes a enviar en un número arbitrario de paquetes, donde adjunta una cabecera, las direcciones origen y destino y los datos de control que luego serán transmitidos por diferentes medios de conexión entre nodos temporales hasta llegar a su destino. Este método de conmutación es el que más se utiliza en las redes de computadores actuales. Surge para optimizar la capacidad de transmisión a través de las líneas existentes. Al igual que en la conmutación de mensajes, los nodos temporales almacenan los paquetes en colas en sus memorias que no necesitan ser demasiado grandes. En estas redes se definen dos términos importantes:

- ✓ *Circuito Virtual*: Cada paquete se encamina por el mismo circuito virtual que los anteriores. Por tanto, se controla y asegura el orden de llegada de los paquetes a destino.
- ✓ *Datagrama*: Cada paquete se encamina de manera independiente de los demás. Por tanto, la red no puede controlar el camino seguido por los paquetes, ni asegurar el orden de llegada al destino.

### **1.4.2 SEGÚN LA TOPOLOGÍA**

Se entiende por topología de una red local la distribución física en la que se encuentran dispuestos los ordenadores que la componen.

#### **1.4.2.1 Topología en Estrella**

Esta topología se caracteriza por existir en ella un punto o nodo central al cual se conectan todos los equipos, tal como se puede apreciar en la Figura 1.5. Esto es también el principal inconveniente ya que la máxima vulnerabilidad se encuentra en dicho nodo central, si éste falla, toda la red fallaría. Sin embargo, presenta como

principal ventaja una gran modularidad, lo que permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red. La topología en estrella es una red punto a punto.

Para aumentar el número de estaciones o nodos, no es necesario interrumpir ni parcialmente la actividad de la red, realizándose la operación casi inmediatamente. Generalmente es empleada en redes Ethernet y ArcNet.

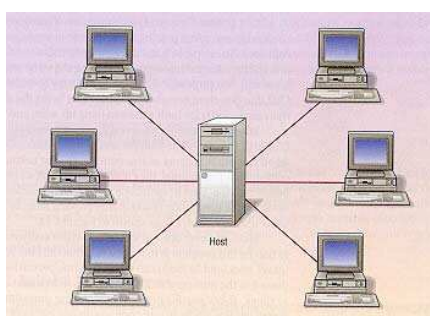


Figura 1.5 Topología en Estrella <sup>[3]</sup>

#### 1.4.2.2 Topología en Bus

En la topología en bus todos los dispositivos comparten el mismo medio y quedan unidos entre sí linealmente uno a continuación del otro (ver Figura 1.6); así, los mensajes que se transmiten a través de éste son atendidos por todos los demás dispositivos que lo comparten. El cableado presenta menos problemas puesto que no se acumulan cables en torno al nodo central. Tiene la desventaja de que un fallo en una parte del cableado detendría el sistema, total o parcialmente, dependiendo del lugar en que se produzca.

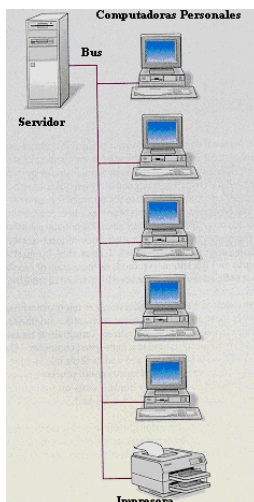


Figura 1.6 Topología en Bus <sup>[4]</sup>

La red en bus posee un retardo mínimo en la propagación de la información, debido a que los nodos no deben amplificar la señal, siendo su función pasiva respecto al tráfico de la red. Se necesita incluir en ambos extremos del bus unos dispositivos llamados terminales, los cuales evitan los posibles rebotes de la señal.

Añadir nuevos puestos a una red en bus supone detener al menos por tramos la actividad de la red. Sin embargo, es un proceso rápido y sencillo. Es la topología tradicionalmente usada en redes multipunto y en las redes Ethernet en su parte lógica, ya que físicamente tienen una topología en estrella.

### 1.4.2.3 Topología en Anillo

El anillo consiste en conectar linealmente entre sí todos los ordenadores en un bucle cerrado como se ve en la Figura 1.7. La información se transfiere en un solo sentido a través del anillo; mediante un paquete especial llamado testigo, que se transmite de un nodo a otro y así se tiene acceso a la red para transmitir información.

El cableado de la red en anillo es complejo, debido por una parte al alto costo del cable, así como a la necesidad de emplear unos dispositivos denominados MAU (*Multistation Access Unit*) para implementar físicamente el anillo. Tiene la ventaja de poder derivar partes de la red mediante los MAU's, aislando las partes defectuosas

del resto mientras se determina el problema.

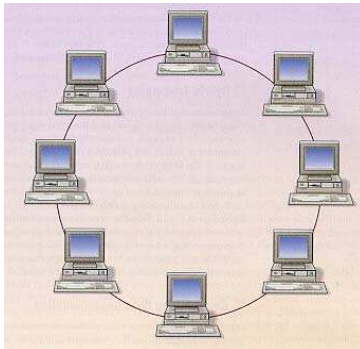


Figura 1.7 Topología en Anillo <sup>[4]</sup>

#### 1.4.2.4 Topologías Híbridas

Son las más frecuentes y se derivan de la unión de topologías puras. Su implementación se debe a la complejidad de la solución de red, o bien al aumento en el número de dispositivos (Figura 1.8).

Tienen un costo muy elevado debido a su administración y mantenimiento, ya que cuentan con segmentos de diferentes tipos, lo que obliga a invertir en equipo adicional para lograr la conectividad deseada.

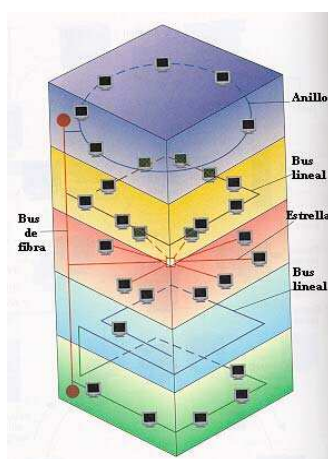


Figura 1.8 Topologías Híbridas <sup>[4]</sup>



### **1.4.3 POR EL MÉTODO DE ACCESO AL MEDIO**

El método de acceso es la manera de controlar el tráfico de mensajes por la red. Hay dos métodos de acceso de uso generalizado en redes locales: por contención, (llamado también aleatorio) y el determinístico.

Básicamente, el método de acceso por contención permite que cualquier usuario empiece a transmitir en cualquier momento siempre que el camino o medio físico no esté ocupado. En el método determinístico, cada estación tiene asegurada su oportunidad de transmitir siguiendo un criterio rotatorio.

#### **1.4.3.1 Acceso por Contención, Aleatorio o no Determinístico**

##### *1.4.3.1.1 CSMA (Carrier Sense Multiple Access)*

El método de contención más común es el CSMA (*Carrier Sense Multiple Access*). Opera bajo el principio de escuchar antes de hablar; está diseñado para redes que comparten el medio de transmisión. Cuando una estación quiere enviar datos, primero escucha el canal para ver si alguien está transmitiendo. Si la línea está desocupada, la estación transmite; si está ocupada, espera hasta que esté libre.

##### *1.4.3.1.2 CSMA/CD (Carrier Sense Multiple Access/Collision Detect)*

En CSMA/CD se sensa el medio físico y se mira cuando se puede transmitir. Si no hay portadora se trasmite, pero puede ocurrir que alguna estación ya haya trasmitido y existirá una colisión. Cuando la colisión es detectada, ambos equipos dejan de transmitir y lo volverán a intentar en un tiempo aleatorio, que dependerá del tipo de persistencia de CSMA/CD (Figura 1.9).

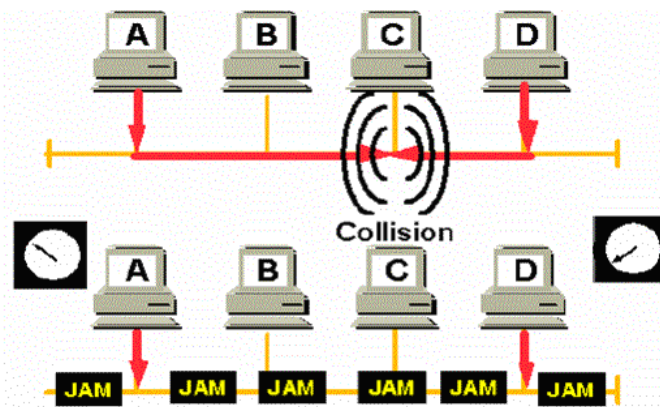


Figura 1.9 CSMA/CD <sup>[5]</sup>

La aleatoriedad del tiempo se incrementa de forma binaria exponencial; a este proceso de detenerse y volver a intentar se le llama Algoritmo de *Backoff*. El *backoff* es realizado hasta 16 veces, si no se logra transmitir el paquete, el envío se descarta, pudiendo existir pérdida de paquetes en este método.

#### 1.4.3.1.3 CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*)

Es un proceso que permite que múltiples estaciones utilicen un mismo medio de transmisión. Primero se intercambian tramas de *handshake*, es decir, el equipo origen envía una trama corta de control de solicitud de transmisión RTS (*Request To Send*) en la cual pide reservar un ancho de banda para la transmisión. El equipo destino devolverá una trama de contestación CTS (*Clear To Send*). Si la respuesta es afirmativa el equipo origen transmitirá los datos. Si el equipo destino recibe correctamente el mensaje contestará con una trama de confirmación positiva ACK (*Acknowledged*) y si no la recibe correctamente contestará con una trama de confirmación negativa NAK (*No Acknowledged*) y el equipo origen volverá a enviar los datos.

### 1.4.3.2 Acceso Determinístico

#### 1.4.3.2.1 *Token o Testigo*

Este método de acceso se utiliza en diferentes redes con variantes que disponen de

un anillo lógico: *Token Ring*, *Token Bus* y FDDI. Un terminal de la red puede transmitir en un intervalo de tiempo fijado. Se vale de una trama especial o testigo, la cual es monitorizada por cada ordenador.

Este sistema evita la colisión debido a que limita el derecho a transmitir a una máquina, solo transmite quien tiene el *token*. Si el testigo está libre, cualquier ordenador que tenga necesidad de transmitir pasará el testigo al estado de ocupado e iniciará la comunicación insertando los datos detrás del testigo. En ese momento el propietario del testigo es la estación que está transmitiendo y es la que dispone del control absoluto del anillo.

Una vez que la trama llega al ordenador destino se copia en su memoria, éste la retransmite sobre la red cambiando una serie de bits para que el ordenador que envió la información compruebe que el terminal destino la recibió correctamente. Si es así, el terminal se encarga de liberar el testigo de manera que otros ordenadores puedan realizar sus comunicaciones. Si el terminal destino no hubiera recibido correctamente la trama, el terminal origen de la comunicación la retransmitirá.

## **1.5 EL MODELO OSI**

Para enfrentar el problema de incompatibilidad de redes, la ISO investigó modelos de *networking* como la red de *DECnet*, SNA (*System Network Architecture*) y TCP/IP, a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló el modelo de referencia OSI (*Open System Interconnection*), el cual fue lanzado en 1984 y es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

### **1.5.1 CAPAS O NIVELES DEL MODELO DE REFERENCIA OSI**



Figura 1.10 Capas del modelo de referencia OSI <sup>[6]</sup>

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, por eso suele hablarse de modelo de referencia. Este modelo está dividido en siete capas (Figura 1.10).

#### 1.5.1.1 Capa Física (Capa 1)

En esta capa se definen las características físicas, mecánicas y eléctricas que debe cumplir el sistema para poder operar. Se encarga de las comunicaciones físicas entre dispositivos y su correcta operación. Las PDU de la capa 1 son los bits.

En este nivel, se deben reglamentar las interfaces de sistemas de cómputo y telecomunicaciones (RS-232 o V.24, V.35), los tipos de conectores asociados a las interfaces (DB-24 y RJ-45 para RS-232 o V.24, Coaxial 75 ohms para G.703), así como los medios de transmisión para redes WAN y LAN y todos aquellos dispositivos pasivos y activos que permiten la transmisión de datos a través de los medios de comunicación.

### **1.5.1.2 Capa de Enlace de Datos (Capa 2)**

Se encarga de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar. Ensambla los datos en tramas y las transmite a través del medio. Ofrece un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores. La PDU (*Protocol Data Unit*) de la capa 2 es la trama.

En este nivel se lleva a cabo el direccionamiento físico de la información a través de las direcciones MAC (*Media Access Control*) para el caso de LAN y de las direcciones manejadas por protocolos como por ejemplo HDLC (*High-Level Data Link Control*), SDLC (*Synchronous Data Link Control*), LAPB (*Link Access Procedure Balance*), entre otros para el caso WAN.

### **1.5.1.3 Capa de Red (Capa 3)**

Se encarga de que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan *routers*.

La capa de red debe administrar la congestión de red. La PDU de la capa 3 es el paquete.

### **1.5.1.4 Capa de Transporte (Capa 4)**

Se encarga del flujo de datos del transmisor al receptor verificando la integridad de los mismos por medio de algoritmos de detección y corrección de errores, con ello se garantiza la calidad de la comunicación. Se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama del nivel 2 detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.

Los protocolos TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*) son ejemplos de protocolos de transporte.

#### **1.5.1.5 Capa de Sesión (Capa 5)**

Se encarga de proveer servicios de conexión entre las aplicaciones tales como: iniciar, mantener y finalizar una sesión. Se puede decir que la capa de sesión es un espacio en tiempo que se asigna al acceder al sistema por medio de un registro en el cual se obtiene acceso a los recursos del mismo servidor.

#### **1.5.1.6 Capa de Presentación (Capa 6)**

Se encarga de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (*little-endian* tipo Intel, *big-endian* tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Es la capa que trabaja con el contenido de la comunicación, en ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos. Por lo tanto, se puede definir a esta capa como la que maneja las estructuras de datos abstractas y realiza las conversiones de representación de datos necesarias para la correcta interpretación de los mismos. Permite también cifrar los datos y comprimirlos.

#### **1.5.1.7 Capa de Aplicación (Capa 7)**

Es el nivel más cercano al usuario. Las aplicaciones que generalmente se transmiten son: bases de datos, hojas de cálculo, archivos de texto, etc. Sin embargo, en el contexto del modelo de referencia OSI, el nivel de aplicación se refiere a las aplicaciones de red que se van a utilizar para transportar las aplicaciones del usuario. FTP, Mail, Telnet, son entre otros ejemplos de aplicaciones de red.

### **1.5.2 UNIDAD DE DATOS DE PROTOCOLOS (PDU)**

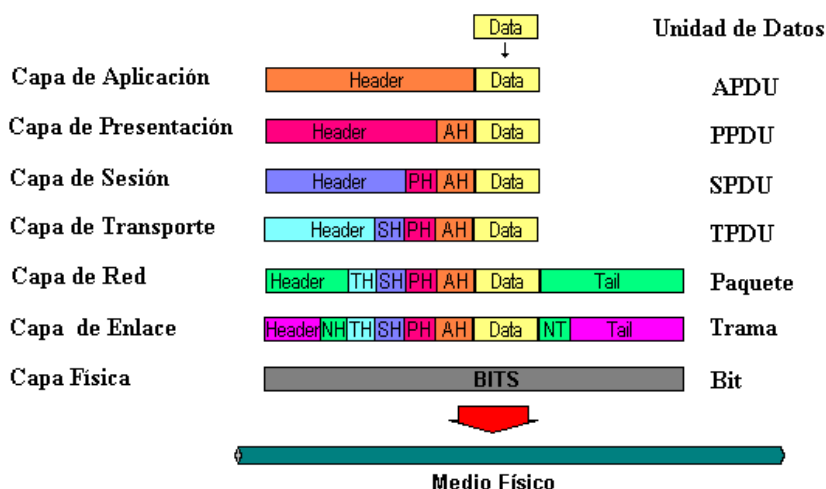


Figura 1.11 PDUs en la transmisión de los datos en el modelo OSI <sup>[6]</sup>

Los datos que viajan a través de las capas del modelo OSI reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren. Debido a la adición de una serie de encabezados e información final (Figura 1.11), los formatos de información son:

- APDU:* Unidad de datos en la capa de aplicación (*Capa 7*).
- PPDU:* Unidad de datos en la capa de presentación (*Capa 6*).
- SPDU:* Unidad de datos en la capa de sesión (*Capa 5*).
- Segmento:* Unidad de datos en la capa de transporte (*Capa 4*).
- Paquete:* Unidad de datos en el nivel de red (*Capa 3*).
- Trama:* Unidad de datos en la capa de enlace (*Capa 2*).
- Bits:* Unidad de datos en la capa física (*Capa 1*).

Como se puede observar, la capa 1 es la única que no realiza encapsulamiento de la información.

### 1.5.3 TRANSMISIÓN DE LOS DATOS

1. La capa de aplicación recibe el mensaje del usuario, le añade una cabecera

constituyendo así la PDU de la capa de aplicación y la transmite a la capa de presentación.

2. La capa de presentación recibe la PDU de la capa aplicación, a ésta le añade su propia cabecera constituyendo así la PDU de la capa de presentación.
3. Esta PDU es transferida a su vez a la capa de sesión mediante el mismo proceso, repitiéndose así para todas las capas.
4. Al llegar al nivel físico se envían los datos para ser recibidos por la capa física del receptor.
5. Cada capa del receptor se ocupa de extraer la cabecera que fue añadida por su capa homóloga, interpretarla y entregar la PDU a la capa superior.
6. Finalmente llega a la capa de aplicación del receptor, ésta elimina la cabecera y entrega el mensaje al usuario.

El proceso de transmisión de datos se muestra en la figura 1.11.

## **1.6 ARQUITECTURA DE REDES LAN**

Las redes están compuestas por muchos componentes que deben trabajar juntos para crear una red funcional.

### **1.6.1 RED ETHERNET**

Ethernet conocida como IEEE 802.3<sup>2</sup>, emplea una topología lógica de bus y una topología física de estrella o de bus. Permite una velocidad de 10 Mbps y usa como método de acceso la técnica CSMA/CD.

La topología lógica de bus de Ethernet permite que cada nodo compita en la transmisión de información a través de la red. Así, la falla de un solo nodo no hace

---

<sup>2</sup> Referirse al anexo 1.1



que falle la red completa. Aunque CSMA/CD es una forma rápida y eficiente para transmitir datos, una red muy cargada podría llegar al punto de saturación.

Entre algunos estándares de Ethernet están: 10BASE5, 10BASE2, y 10BASE-T, que definen el tipo de cable de red, las especificaciones de longitud y la topología física que debe utilizarse para conectar nodos en la red. Fast Ethernet es una extensión del estándar Ethernet que opera a velocidades de 100 Mbps.

### **1.6.2 REDES TOKEN RING**

También llamada IEEE 802.5<sup>2</sup>, fueron ideadas por IBM y otros fabricantes. Opera a una velocidad de 4 Mbps o 16 Mbps y emplea una topología lógica de anillo y una topología física de estrella. Tiende a ser menos eficiente que CSMA/CD en redes con poca actividad, pues requiere una sobrecarga adicional. Sin embargo, conforme aumenta la actividad de la red, *Token Ring* llega a ser más eficiente.

### **1.6.3 FDDI (*Fiber Distributed Data Interface*)**

Es un estándar para la transferencia de datos por cable de fibra óptica. El estándar ANSI X3T9.5 especifica una velocidad de 100 Mbps. Dado que el cable de fibra óptica no es susceptible a la interferencia eléctrica o a la degradación de la señal de red, FDDI permite el empleo de cables más largos que otros estándares de red, y presenta una gran tolerancia a fallas en la red.

## **1.7 MEDIOS DE TRANSMISIÓN**

Son utilizados para transportar las señales de la red de un punto a otro. Las redes LAN se conectan con diferentes tipos de medios ya sean cableados o inalámbricos.

## 1.7.1 MEDIOS GUIADOS

### 1.7.1.1 Par Trenzado

El cable de par trenzado es una forma de conexión en la que dos conductores son entrelazados para cancelar las EMI (*ElectroMagnetic Interference*) de fuentes externas y la diafonía de los cables adyacentes.

Entre los tipos de cable par trenzado se tiene:

- ✓ *STP (apantallado)*: 2 pares de hilos, recubiertos por malla metálica.
- ✓ *UTP (no apantallado)*: 4 pares de hilos.
- ✓ *FTP (no apantallado)*: 4 pares de hilos, recubiertos con papel de aluminio.

#### 1.7.1.1.1 Cable STP (*Shielded Twisted Pair*)

Este cable combina las técnicas de blindaje, cancelación y trenzado de cables. Cada par de hilos está envuelto en un papel metálico y los dos pares envueltos juntos en una trenza o blindaje metálico como se puede apreciar en la Figura 1.12. Generalmente es un cable de 150 ohmios de impedancia característica, en el que se reduce el ruido eléctrico dentro del cable.

El STP también reduce el ruido desde el exterior del cable, como la EMI y la RFI (*Radio Frequency Interference*). Los materiales metálicos de blindaje deben estar conectados a tierra; si no lo están o si hubiera discontinuidades en toda la extensión del material del blindaje, el STP se puede volver susceptible a graves problemas de ruido.

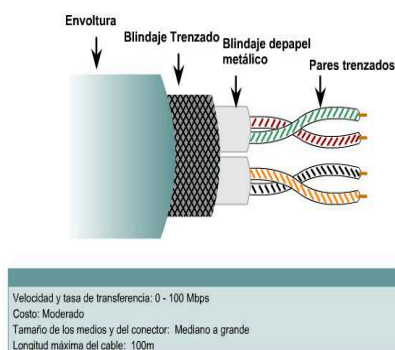
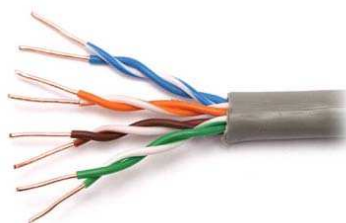


Figura 1.12 Cable STP <sup>[7]</sup>

El uso de aislamiento y blindaje adicionales aumenta de manera considerable el tamaño, peso y costo del cable. Además, los materiales de blindaje hacen que las terminaciones sean más difíciles y aumentan la probabilidad de que se produzcan defectos de mano de obra.

#### 1.7.1.1.2 Cable UTP (*Unshielded Twisted Pair*)<sup>3</sup>

El cable UTP se compone de cuatro pares de cobre con centro sólido cubiertos por una funda de plástico para ayudar a incrementar las velocidades de transmisión de datos y protegerlos del ruido exterior (Figura 1.13). La diferencia principal entre el cable UTP y STP es el recubrimiento que tienen para aislar el ruido, ganar mayores distancias y obtener altas velocidades.

Figura 1.13 Cable UTP <sup>[8]</sup>

El IEEE logró generar el estándar 10BaseT, el cual ha tenido mucha aceptación por los administradores de redes y compañías de cableado. Este estándar corresponde a una arquitectura LAN que emplea cable UTP ya que este tipo de cable es mucho más fácil de manejar que el coaxial.

El cable UTP se recomienda por los estándares de cableado estructurado de la EIA/TIA 568 para las instalaciones de cableados horizontales. Actualmente existen varias categorías, la razón es que el nivel del cable se escoge dependiendo de la velocidad a la que se quiera transmitir. Las categorías se diferencian en su atenuación, impedancia y capacidad de línea y se muestran en la Tabla 1.1 para una distancia de 100 metros.

---

<sup>3</sup> Referirse a la página Web [http://es.wikipedia.org/wiki/Cable\\_par\\_trenzado](http://es.wikipedia.org/wiki/Cable_par_trenzado)

Categoría	Velocidad – Ancho de Banda	Características y/o Aplicaciones
1	100 Kbps	Para telefonía
2	Hasta 4 Mbps	Tiene cuatro pares trenzados de hilo de cobre.
3	Hasta 16 Mbps – 16 MHz	<i>Ethernet</i> 10Base-T
4	Hasta 20 Mbps – 20 MHz	<i>Token-Ring</i> , 10Base-T
5e	Hasta 1 Gbps – 100 MHz	Categoría 5 mejorado, ya que produce menos atenuación
6	Hasta 1 Gbps – 250 MHz	100Base-T, 1000Base-T
6a	Hasta 10 Gbps – 500 MHz	100Base-T, 1000Base-T
7	Mayor 10 Gbps – 600 MHz	Aprobada para los elementos que conforman la clase F en el estándar internacional ISO 11801.

Tabla 1.1 Categoría de cables UTP

Entre mayor sea la categoría, también lo son los costos. La diferencia entre cada una de las categorías es el número de trenzas por pulgada con que cuenta el cable, además del recubrimiento que se le da a cada uno de ellos. Usar cable que no esté trenzado genera grandes problemas en la comunicación de datos como diafonía (*cross talk*).

### 1.7.1.1.3 Cable FTP (Foiled Twisted Pair)

Al igual que el cable UTP no es apantallado pero está cubierto por una envoltura de aluminio para mejorar su nivel de protección ante interferencias externas (Figura 1.14). Se lo usa generalmente en los sistemas de cableado de edificios u otros ambientes donde el ruido adyacente a los cables puede causar interferencia. Su utilización conjunta con UTP permite la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones del cableado. La desventaja de este cable es que requiere cuidar el sistema de tierra.



Figura 1.14 Cable FTP [9]

Su impedancia característica típica es de 120 ohmios y sus propiedades de transmisión son más parecidas a las del UTP. Además, puede utilizar los mismos conectores RJ45. Tiene un precio intermedio entre el UTP y STP.

La figura 1.15 muestra como está compuesto este cable:

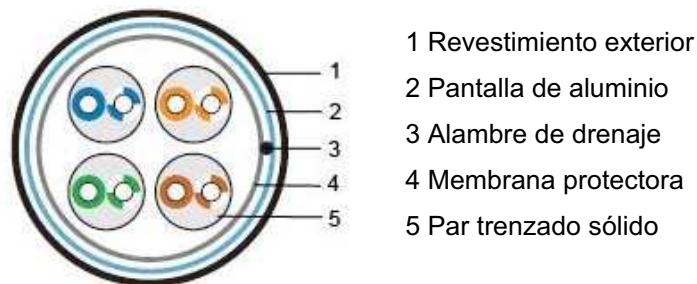


Figura 1.15 Componentes del cable FTP [9]

### 1.7.1.2 Cable Coaxial

Consiste de un conductor de cobre rodeado de una capa de aislante flexible. Sobre este material aislante existe una malla de cobre tejida u hoja metálica que actúa como el segundo hilo del circuito; y, como un blindaje para el conductor interno, el cual reduce la cantidad de interferencia electromagnética. Cubriendo la pantalla está la chaqueta del cable (Figura 1.16).

Principalmente se tienen cables de dos valores de impedancias características:

- ✓ 75 *ohmios*: banda ancha, utilizado en TV, distintos canales, 300 MHz.
- ✓ 50 *ohmios*: banda base, utilizado en Ethernet, un canal. Se emplea principalmente en redes:
  - 10BASE5: coaxial grueso, 500 metros, 10 Mbps, conector "N".
  - 10BASE2: coaxial fino, 185 metros, 10 Mbps, conector "BNC".

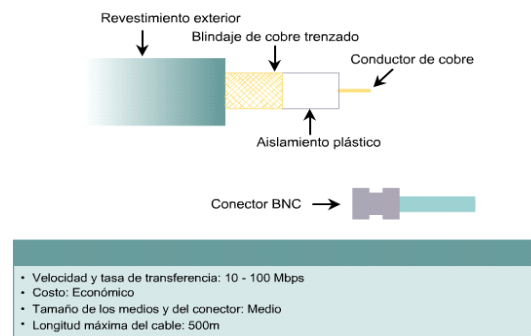


Figura 1.16 Cable Coaxial [7]

El cable coaxial para banda base y para banda ancha son muy parecidos en su construcción, pero sus principales diferencias son: la cubierta del cable, los diámetros y el valor de impedancia.

El cable coaxial para banda base es de 3/8 de pulgada y utiliza una cubierta de plástico, mientras que el cable coaxial para banda ancha es de 1/2 pulgada y está cubierto de una malla o tela de aluminio y una funda protectora de plástico. Ethernet puede trabajar con ambos cables, pero lo más común es con banda base.

### 1.7.1.3 Fibra Óptica

Se usa para transmitir señales digitales de datos en forma de pulsos modulados de luz. Un cable de fibra óptica se compone de cinco partes: núcleo, revestimiento, amortiguador, material resistente y revestimiento exterior (Figura 1.17). El *core* es el centro de la fibra y está fabricado de vidrio, el *cladding* o revestimiento recubre al *core* y ayuda a mantener la luz dentro de éste. El *buffer* es la cubierta de plástico que le da a la fibra una rigidez adicional.

Existen fibras con dos hilos de fibra por cable, una para la transmisión y otra para la recepción. Pueden transmitir a 100 Mbps y alcanzar velocidades de hasta 200 Gbps. Este tipo de cable no está sujeto a interferencias de ningún tipo.

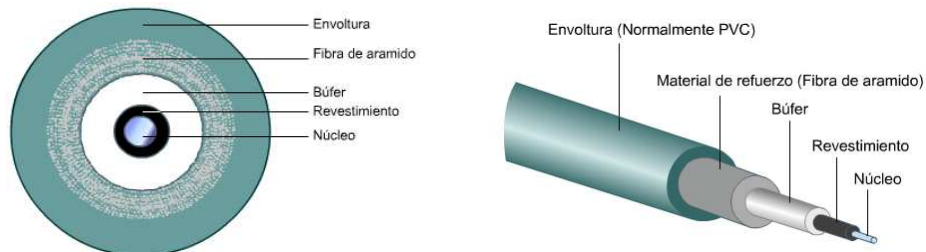


Figura 1.17 Fibra Óptica [7]

Debido a su construcción puede alcanzar grandes distancias, la distancia máxima recomendada por el IEEE para redes locales es de 2 Km. De acuerdo a los modos de propagación existen dos tipos de fibra en la actualidad: monomodo (*single mode*) y multimodo (*multi mode*).

#### 1.7.1.3.1 Fibra Monomodo

Tiene un núcleo muy pequeño que permite que los rayos de luz viajen a través de la fibra con un solo modo de propagación. Se utiliza principalmente en telecomunicaciones para alcanzar grandes distancias; esto se debe a que el espectro de luz recorre varios miles de metros antes de requerir algún repetidor. Generalmente se maneja con rayo láser, permitiendo la entrada al *core* de un solo rayo de luz, lo que le brinda una clara y fina señal hasta el final del cable (Figura 1.18a).

#### 1.7.1.3.2 Fibra Multimodo

Tiene un núcleo lo suficientemente grande como para permitir que la luz pueda recorrer varios trayectos a lo largo de la fibra (Figura 1.18b). Se usa generalmente en aplicaciones en donde las distancias son pequeñas (10 km). Es mucho más barata que la monomodo y se ilumina con un LED.

Actualmente existen dos tipos de fibra multimodo en el mercado: *step index* y *grade index*. Las fibras de *step index* tienen un gran cambio en el índice de

refracción que va del *core* hacia el *cladding*, mientras que la fibra de *grade index* presenta un índice de refracción que decrece gradualmente partiendo del *core* hacia el *cladding*.

La luz utilizada en esta fibra no daña al ojo humano, por lo que se puede ver directamente al cable sin temor a perder la vista.



Figura 1.18a Fibra Monomodo <sup>[7]</sup>

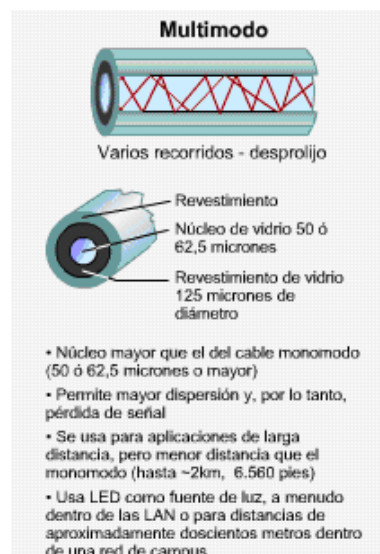


Figura 1.18b Fibra Multimodo <sup>[7]</sup>

Cada fibra es reconocida por el tamaño del *core* en relación con el del *cladding* como se puede en la Figura 1.19. El tipo de fibra que se puede usar en Ethernet es la fibra multimodo *grade index*, 62.5/125.

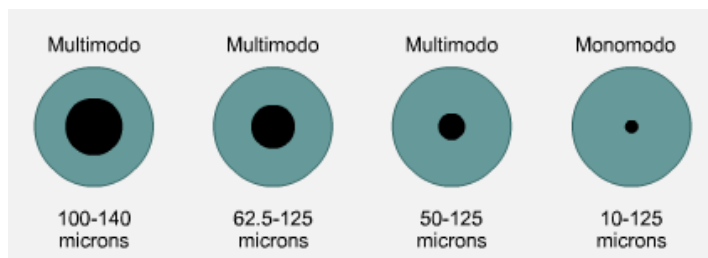


Figura 1.19 Tamaños de la Fibra Óptica <sup>[7]</sup>

Algunas características técnicas de la Fibra Óptica son:

- ✓ Necesita una fuente de luz: láser o LED.



- ✓ Recepción de la luz por foto diodos.
- ✓ Puede alcanzar un ancho de banda de 30000GHz .
- ✓ No hay interferencias. No es susceptible al ruido.
- ✓ Pesa 8 veces menos que el cable par trenzado.
- ✓ Se usa tanto para la transmisión de banda base como para banda ancha.
- ✓ Altos niveles de transferencia de datos, 50 Gbps en distancias de 1 km y 10 Mbps en distancias de 2 km.
- ✓ Grandes distancias. En el caso de Ethernet se pueden tener nodos remotos a distancias de hasta 2 km sin necesidad de un repetidor.
- ✓ Requiere de herramientas especiales para el armado de los conectores.
- ✓ El equipo de pruebas es costoso.
- ✓ Es un enlace punto a punto. Con la tecnología actual no es posible tener ningún tipo de transferencia multipunto.

#### 1.7.1.3.3 Tipos de Conectores

Estos elementos se encargan de conectar las líneas de fibra a un elemento, puede ser un transmisor o un receptor. En la actualidad, existen varios conectores para fibra (Figura 1.20), entre ellos se tienen:

- ✓ *FC*: Se usa en la transmisión de datos y en telecomunicaciones.
- ✓ *FDDI*: Se usa para redes de fibra óptica de 100 Mbps.
- ✓ *LC y MT-Array*: Se utilizan en transmisiones de alta densidad de datos.
- ✓ *SC y SC-Dúplex*: Se utilizan para la transmisión de datos.
- ✓ *ST*: Se usa en redes de edificios y en sistemas de seguridad.
- ✓ *SMA*: Se utilizan para las telecomunicaciones y en LANs.

Los conectores ST y SMA son los dos más usados en la industria para las redes de área local; el conector ST se ha convertido en el más común y confiable de los dos.

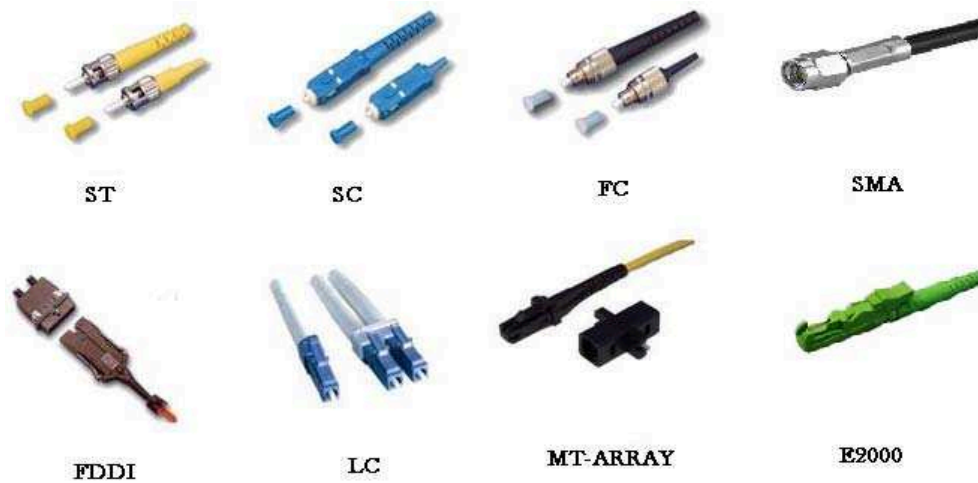


Figura 1.20 Tipos de Conectores para Fibra Óptica <sup>[10]</sup>

#### 1.7.1.4 Cable AUI (*Attachment Unit Interface*)

Es conocido como el cable para *transceiver*. Es del tipo STP y se usa principalmente para la tecnología Ethernet. Usa el conector DB-15 definido por el IEEE, aunque solo ocupa cuatro pines para lograr la conectividad, dos para emisión y dos para recepción. La impedancia de este cable es de 780 ohmios.

Hay dos formas de utilizarlo: AUI de oficina o IEEE 802.3 AUI. El cable AUI de oficina es relativamente más flexible y fácil de manejar, comparándolo con el cable IEEE 802.3. El cable AUI es el único cable que además de transmitir información, también puede conducir corriente eléctrica o potencia suficiente para hacer que el *transceiver* funcione.

## 1.7.2 MEDIOS INALÁMBRICOS

En el estudio de las comunicaciones inalámbricas se considera tres rangos de frecuencias que se muestran en la tabla 1.2.

TRANSMISIÓN INALÁMBRICA	BANDA
Radio Frecuencia	10 KHz a 300 MHz
Micro Ondas	300 MHz a 300 GHz
Infra Rojo	300 GHz a 400 THz

Tabla 1.2 Rango de Frecuencias de Medios Inalámbricos <sup>[11]</sup>

### 1.7.2.1 Radiofrecuencia

Puede parecer idóneo para el control a distancia de los sistemas domóticos por la flexibilidad que supone su uso. Sin embargo, resulta sensible a las perturbaciones electromagnéticas producidas por medios de transmisión, equipos domésticos, etc.

Ventajas:

- ✓ Fácil intervención de las comunicaciones.

Desventaja:

- ✓ Dificultad para la integración de las funciones de control y comunicación, en su modalidad de transmisión analógica.
- ✓ Alta sensibilidad a las interferencias.

### 1.7.2.2 Micro Ondas

El intervalo va desde los 300 MHz a 300 GHz. En estas frecuencias de trabajo se pueden conseguir haces altamente direccionales, por lo que las microondas son adecuadas para enlaces punto a punto. Las microondas también se usan para las comunicaciones vía satélite.

#### 1.7.2.2.1 Microondas Terrestres

Suelen utilizarse antenas parabólicas, el tamaño típico del diámetro es de unos 3 metros. Estas antenas se fijan rígidamente y transmiten un haz estrecho que debe estar perfectamente enfocado hacia la antena receptora. Las antenas de microondas se sitúan a una altura apreciable sobre el nivel del suelo, para con ello conseguir mayores separaciones posibles entre ellas y a su vez ser capaces de salvar posibles obstáculos. Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas.

Se usan para transmisión de televisión y voz. La principal causa de pérdidas es la atenuación debido a que las pérdidas aumentan con el cuadrado de la distancia (con cable coaxial y par trenzado son logarítmicas). La atenuación aumenta con

las lluvias. Las interferencias es otro inconveniente de las microondas ya que al proliferar estos sistemas, puede haber más solapamientos de señales.

#### *1.7.2.2 Microondas por Satélite*

Un satélite de comunicaciones es esencialmente una estación que retransmite microondas. Se usa como enlace entre dos o más receptores/transmisores terrestres, denominados estaciones base. El satélite recibe la señal en una banda de frecuencia (canal ascendente), la amplifica o repite, y posteriormente la retransmite en otra banda de frecuencia (canal descendente) en la dirección adecuada. Cada uno de los satélites geoestacionarios operará en una serie de bandas de frecuencias llamadas "*transponders*". El satélite debe ser geoestacionario para mantener la alineación con los receptores y emisores de la tierra teniendo un periodo de rotación igual al de la tierra y esto solo ocurre a una distancia de 35.784 Km.

El rango de frecuencias en la recepción del satélite es diferente del rango del que éste emite, para que no haya interferencias entre las señales que ascienden y las que descienden.

#### **1.7.2.3 Infrarrojo**

El rango de frecuencias es la zona de infrarrojos del espectro que va en términos generales desde los 300 GHz a 400 THz. Los infrarrojos son útiles para las conexiones locales punto a punto así como para aplicaciones multipunto dentro de un área de cobertura limitada.

La comunicación se lleva a cabo mediante transmisores y receptores de infrarrojos ("*transceivers*") que modulan luz infrarroja no coherente. Los emisores y receptores deben estar alineados o bien estar en línea tras la posible reflexión de rayo en superficies como las paredes. En infrarrojos no existen problemas de seguridad ni de interferencias ya que estos rayos no pueden atravesar objetos. Tampoco se necesita permiso para su utilización.

SIGLA	DENOMINACIÓN	BANDA DE FRECUENCIA	LONGITUD DE ONDA	DATOS ANALÓGICOS		DATOS DIGITALES		APLICACIONES PRINCIPALES
				MODULACIÓN	ANCHO DE BANDA	MODULACIÓN	RAZÓN DE DATOS	
VLF	Very Low Frequencies	10-30 KHz	30.000m a 10.000m	Normalmente no se usa		ASK, FSK, MSK	-	Enlaces de radio a gran distancia.
LF	Low Frequencies	30-300 KHz	10.000m a 1.000m	Normalmente no se usa		ASK, FSK, MSK	0,1-100 bps	Enlaces de radio a gran distancia, navegación aérea y marítima.
MF	Médium Frequencies	300-3000 KHz	1.000m a 1000m	AM	Hasta 4 KHz	ASK, FSK, MSK	10-1000 bps	Radiodifusión (Radio AM Comercial).
HF	High Frequencies	3-30 MHz	100m a 10m	AM, SSB	Hasta 4 KHz	ASK, FSK, MSK	10-3000 bps	Comunicaciones de todo tipo a media y larga distancia.
VHF	Very High Frequencies	30-300 MHz	10m a 1m	FM, SSB;FM	5 KHz a 5 MHz	FSK, PSK	Hasta 100 Kbps	Enlaces de radio a corta distancia, TV VHF, frecuencia modulada.
UHF	Ultra High Frequencies	300-3000 MHz	1m a 10cm	FM, SSB	Hasta 20 MHz	PSK	Hasta 10 Kbps	Enlaces de radio, ayuda a la navegación aérea, radar, microondas terrestres, TV UHF.
SHF	Super High Frequencies	3-30 GHz	10cm a 1cm	FM	Hasta 500 MHz	PSK	Hasta 100 Mbps	Radar, microondas terrestres y por satélite, enlaces de radio.
EHF	Extra High Frequencies	30-300 GHz	1cm a 1mm	FM	Hasta 1 GHz	PSK	Hasta 750 Mbps	Radar, enlaces de radio y cercanos con punto a punto experimentales

Tabla 1.3 Características de las bandas en medios inalámbricos <sup>[12]</sup>

En la Tabla 1.3 se resumen las características de transmisión en medios no guiados para las distintas bandas de frecuencia. Las microondas cubren parte de la banda de UHF y cubren totalmente la banda SHF; la banda de ondas de radio cubre la VHF y parte de la banda UHF.

## 1.8 CABLEADO ESTRUCTURADO

El cableado estructurado nació como una integración de marcas, aplicaciones y necesidades de un mercado cada vez más competitivo y amplio, que hacía difícil la convivencia de dos o más sistemas de datos en un solo cableado.

Es una forma ordenada y planeada de realizar cableados, que permite conectar teléfonos, equipo de procesamiento de datos, computadoras personales, redes de área local (LAN) y equipos de oficina entre sí. Al mismo tiempo permite conducir señales de control como son: sistemas de seguridad y acceso, control de iluminación, control ambiental, etc. El objetivo primordial es proveer de un sistema completo de transporte de información a través de un medio común.

### 1.8.1 ESTÁNDARES DE CABLEADO ESTRUCTURADO <sup>11</sup>

Los sistemas de cableado estructurado deben emplear una arquitectura de sistemas abiertos y soportar aplicaciones basadas en estándares como el EIA/TIA-568A, EIA/TIA-568B, EIA/TIA-569, EIA/TIA-606, EIA/TIA-607. Provee un solo punto para efectuar movimientos y adiciones de tal forma que la administración y mantenimiento se convierten en una acción simplificada. La gran ventaja de los sistemas de cableado estructurado es que cuenta con la capacidad de incorporar nuevas tecnologías.

Las normas europeas ISO/IEC 11801 y americanas ANSI/TIA/EIA, reglamentan hoy los sistemas de cableado estructurado, donde la europea incluye todas las normas americanas:

- ✓ *ANSI/EIA/TIA 568 (A) B1*: Estándar para cableado de Telecomunicaciones en Edificios Comerciales, parte 1, Requerimientos Generales.
- ✓ *ANSI/EIA/TIA 568 (A) B2*: Es la parte 2, Balance de los Componentes del Cableado en Par Trenzado.
- ✓ *ANSI/EIA/TIA 568 B3*: Estándar de los Componentes para Cableados en Fibra Óptica.
- ✓ *ANSI/EIA/TIA 606*: Determina la forma de Administración de la Infraestructura del Cableado de Telecomunicaciones.
- ✓ *ANSI/EIA/TIA 569*: Estándar para Espacios y Ductos para el Cableado de Telecomunicaciones en Edificios Comerciales.
- ✓ *ANSI/EIA/TIA 526-7*: Especifica las Mediciones de Atenuación en Fibra Óptica Monomodo (*single-mode*).
- ✓ *ANSI/EIA/TIA 526 – 14 A*: Especifica las Mediciones de Atenuación en Fibra Óptica Multimodo (*multi-mode*).
- ✓ *ANSI/EIA/TIA 607*: Determina los Sistemas de Puesta a Tierra.
- ✓ *ANSI/EIA/TIA 758*: Estándar para Cableados de Telecomunicaciones en el exterior del Edificio.
- ✓ *ANSI/TIA/EIA 570*: Cableado de Telecomunicaciones Residencial y

---

<sup>11</sup> Referirse al anexo 1.2

## Pequeños Negocios.

### 1.8.1.1 Estándar EIA/TIA 568

El estándar EIA/TIA 568 se desarrolló para la instalación de cableados de telecomunicaciones en edificios comerciales. Los puntos principales son:

- ✓ Definir un sistema genérico de cableado, tanto para voz como para datos, que soporte múltiples productos y fabricantes.
- ✓ Proporcionar el diseño de telecomunicaciones con base en productos internacionalmente comerciales.
- ✓ Planear e instalar el cableado en un edificio con el conocimiento previo de los productos utilizados en telecomunicaciones.

El estándar EIA/TIA 568 cubre una gran variedad de aspectos que deben tomarse en cuenta antes de diseñar, construir o comprar una solución de cableado. Dos esquemas de asignación de pines están definidos por la EIA/TIA, el 568A y el 568B. Ambos esquemas son casi idénticos, excepto que los pares 2 y 3, están al revés (Figura 1.21).

Para aplicaciones de red como Ethernet, 10/100BaseT o *Token Ring* solo son usados dos pares, los 2 pares restantes se utilizan para otro tipo de aplicaciones, voz, por ejemplo.

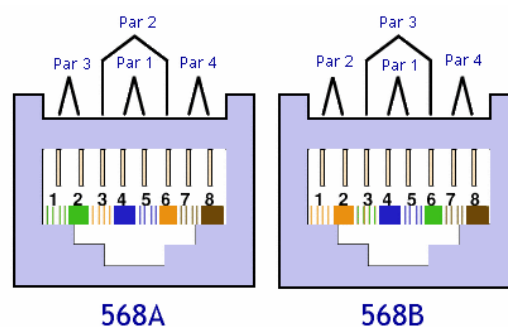


Figura 1.21 Estándares T-568A y T-568B <sup>[13]</sup>

Si los colores aparecen en el mismo orden en ambos conectores, entonces, el cable es directo. Si los pares 2 y 3 del segundo conector aparecen en sentido inverso al del primero, el cable es cruzado. Un cable directo sirve para conectar

una computadora a un *Hub*, o a un *Switch*; mientras que un cable cruzado sirve para conectar dos PCs, dos *routers*, *switches* o *hubs* entre sí.

## **1.8.2 SUBSISTEMAS DEL SISTEMA DE CABLEADO ESTRUCTURADO**

### **1.8.2.1 Entrada al Edificio**

La entrada a los servicios del edificio es el punto en el cual el cableado externo hace interfaz con el *backbone* interno. Este punto consiste en la entrada de los servicios de telecomunicaciones (acometidas), incluyendo el punto de entrada a través de la pared, hasta el cuarto o espacio de entrada. Los requerimientos de la interfaz de red están definidos en el estándar TIA/EIA-569.

### **1.8.2.2 Cuarto de Equipos**

Es un espacio centralizado dentro del edificio donde se albergan los equipos de red (enrutadores, *switches*), equipos de datos, voz, video, etc. Los aspectos de diseño del cuarto de equipos están especificados en el estándar TIA/EIA 569.

### **1.8.2.3 Cableado Horizontal**

Se extiende desde el área de trabajo de telecomunicaciones al *rack* de telecomunicaciones y consiste de lo siguiente:

- ✓ Cableado horizontal.
- ✓ Punto de red de telecomunicaciones.
- ✓ Terminaciones de cable (asignaciones de guías del conector modular RJ-45).
- ✓ Conexiones de transición.

Tres tipos de medios son reconocidos para el cableado horizontal, cada uno debe de tener una extensión máxima de 90 metros:

- ✓ Cable UTP 100-ohm, 4-pares, (24 AWG sólido).
- ✓ Cable 150-ohm STP, 2-pares.
- ✓ Fibra óptica 62.5/125- $\mu$ m, 2 hilos de fibra.

### **1.8.2.4 Backbone**

Permite la interconexión entre los gabinetes y cuartos de telecomunicaciones y los



servicios de la entrada. Consiste de cables *cross-connects* principales y secundarios (Tabla 1.4), terminaciones mecánicas y regletas o *jumpers* usados para la conexión *backbone-backbone*. Incluye:

- ✓ Conexión vertical entre pisos.
- ✓ Cables entre un cuarto de equipos y cable de entrada a los servicios del edificio.
- ✓ Cables entre edificios.

TIPO DE CABLE	DISTANCIAS MÁXIMAS
100 ohm UTP (24 or 22 AWG)	800 metros (Voz)
150 ohm STP	90 metros (Datos)
Fibra Multimodo 62.5/125 $\mu\text{m}$	2,000 metros
fibra Monomodo 8.3/125 $\mu\text{m}$	3,000 metros

Tabla 1.4 Tipo de cables requeridos para cableado *backbone* <sup>[13]</sup>

#### 1.8.2.5 Gabinete o *Rack* de Telecomunicaciones

Es el área dentro de un edificio que alberga el equipo del sistema de cableado de telecomunicaciones. Éste incluye las terminaciones mecánicas y/o *cross-connects* para el sistema de cableado horizontal y del *backbone*.

#### 1.8.2.6 Área de Trabajo

Se extiende desde el cajetín a los dispositivos o estaciones de trabajo. Los componentes del área de trabajo son:

- ✓ Dispositivos: computadoras, terminales, teléfonos, etc.
- ✓ Cables de parcheo: cables modulares, cables adaptadores/conversores, *jumpers* de fibra, etc.
- ✓ Adaptadores.

## 1.9 COMPONENTES DE UNA RED

### 1.9.1 EQUIPOS QUE INTERCONECTAN REDES

#### 1.9.1.1 Repetidores

Son dispositivos electrónicos que reciben una señal débil o de bajo nivel y la

retransmiten a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas, sin o con degradación tolerable.

Trabajan al nivel 1 del modelo OSI y su función es extender una red más allá de un segmento.

El número máximo de repetidores en cascada es cuatro, pero con la condición de que los segmentos 2 y 4 no tengan ningún equipo conectado que no sean los repetidores. En caso contrario, el número máximo es dos, interconectando tres segmentos de red.

#### **1.9.1.2 Concentradores o *Hubs***

Son dispositivos que permiten centralizar el cableado de una red y poder ampliarlo. Los concentradores funcionan repitiendo cada trama de datos en cada uno de los puertos con los que cuentan, excepto en el que han recibido el paquete, de forma que todos los puntos tienen acceso a los datos. Simplemente unen conexiones y no alteran las tramas que llegan. Son la base para las redes de topología tipo estrella. Existen 3 clases:

- ✓ *Pasivos*: No necesitan energía eléctrica.
- ✓ *Activos*: Necesitan alimentación.
- ✓ *Inteligentes*: Son *hubs* activos que incluyen administración.

#### **1.9.1.3 Conmutadores o *Switches***

Se utilizan para conectar múltiples redes, fusionándolas en una sola. Operan en la capa 2 del modelo OSI e interconectan dos o más segmentos de red, pasando datos entre ellos, de acuerdo a la dirección MAC destino de las tramas en la red. Son el centro de una red en estrella mejorando el rendimiento y la seguridad de las LAN.

##### ✓ *Switch Ethernet*

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Esto permite que, a diferencia de los concentradores o *hubs*, la información dirigida a un dispositivo vaya desde el puerto origen al puerto

destino.

✓ *Conmutadores de nivel 3*

Permiten encaminar los paquetes (nivel 3) entre las redes, realizando por tanto las funciones de enrutamiento.

#### **1.9.1.4 Puentes o *Bridges***

Al igual que los *switches*, se utilizan para interconectar segmentos de red y se utilizan cuando el tráfico no es excesivamente alto en las redes; pero, aísla las colisiones que se producen en los segmentos interconectados entre sí. Los *bridges* trabajan en el nivel 2 de OSI, con direcciones físicas, por lo que filtra tráfico de un segmento a otro.

Para realizar el filtrado de tráfico:

- ✓ Escuchan los paquetes que pasan por la red y van configurando una tabla de direcciones físicas de equipos que tienen a un lado y otro.
- ✓ No filtran los *broadcasts*.

El número máximo de puentes en cascada es de siete; no pueden existir bucles o lazos activos, es decir, si hay caminos redundantes para ir de un equipo a otro, solo uno de ellos debe estar activo, mientras que el redundante debe ser de *backup*.

#### **1.9.1.5 Enrutadores o *Routers***

Estos equipos trabajan a nivel de capa 3 del modelo OSI, es decir pueden filtrar protocolos y direcciones a la vez. Los equipos envían los paquetes directamente al *router* cuando se trata de equipos en otro segmento. Además, pueden interconectar redes distintas entre sí. Su método de funcionamiento es el encapsulamiento de paquetes.

Eligen el mejor camino para enviar la información, balancean tráfico entre líneas. Trabajan con tablas de enrutamiento con la información que generan los protocolos de enrutamiento, deciden si hay que enviar un paquete o no, deciden

cuál es la mejor ruta para enviar la información de un equipo a otro, pueden contener filtros a distintos niveles, etc.

#### **1.9.1.6 Gateways o Puertas de Enlace**

Son equipos que sirven de intermediarios entre los diferentes protocolos de comunicaciones para facilitar la interconexión de equipos distintos entre sí. Reciben los datos encapsulados de un protocolo, los van desencapsulando hasta el nivel más alto, para posteriormente ir encapsulando los datos en el otro protocolo (desde el nivel más alto al nivel más bajo) y vuelven a dejar la información en la red ya traducida. Los *gateways* también pueden interconectar redes entre sí.

#### **1.9.1.7 Cortafuegos o Firewalls**

Son elementos de *hardware* o *software* utilizados en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que se hayan definido en la organización.

La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red externa (*Internet*); de este modo, se protege la red interna de intentos de acceso no autorizados desde el exterior que pueden aprovechar vulnerabilidades de los sistemas de la red.

También es frecuente conectar el *firewall* a la DMZ (*zona desmilitarizada*), en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

#### ✓ *Cortafuegos de capa de red o de filtrado de paquetes*

Funcionan a nivel de red de la pila de protocolos TCP/IP como filtro de paquetes IP. Se realizan los filtros según los campos de los paquetes IP como dirección IP origen y dirección IP destino. A menudo, en este tipo de cortafuegos se permiten filtrados según los campos del nivel de transporte como el puerto origen y destino, o del nivel de enlace de datos como la dirección MAC.

✓ *Cortafuegos de capa aplicación*

Trabajan en el nivel de aplicación de manera que los filtros se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que está intentando acceder. Los cortafuegos a nivel 7 de tráfico HTTP son normalmente denominados *Proxy* y permiten que los computadores de una organización entren a Internet de una manera controlada.

## 1.10 REDES TCP/IP

### 1.10.1 DEFINICIÓN

La arquitectura TCP/IP es utilizada por todos los ordenadores conectados a *Internet*, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con *hardware* y *software* incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Esa es una de las grandes ventajas de TCP/IP, pues se encarga de que la comunicación entre todos sea posible; es compatible con cualquier sistema operativo y con cualquier tipo de *hardware*.

Este nombre viene dado por los protocolos de esta familia:

- ✓ El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI proporcionando un transporte fiable de datos.
- ✓ El protocolo IP, funciona en el nivel de red del modelo OSI y permite encaminar los datos hacia otras máquinas.

Se debe tener en cuenta una serie de particularidades sobre las que ha sido diseñado TCP/IP:

- ✓ Los programas de aplicación no tienen conocimiento del *hardware* que se utilizará para realizar la comunicación (*modem*, tarjeta de red, etc).

- ✓ La comunicación no está orientada a la conexión, es decir, cada paquete de información es independiente y puede viajar por caminos diferentes para llegar al destino final.
- ✓ La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre qué tipo de red trabajan.
- ✓ El uso de la red no impone ninguna topología en especial.

### 1.10.2 ARQUITECTURA TCP/IP

La arquitectura TCP/IP consta de cuatro capas en las que se agrupan diferentes protocolos (Figura 1.22).



Figura 1.22 Niveles de Arquitectura TCP/IP <sup>[6]</sup>

#### 1.10.2.1 Aplicación

Constituye el nivel más alto de TCP/IP. Corresponde a los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como: correo electrónico con SMTP (*Simple Mail Transfer Protocol*), transferencia de ficheros con FTP (*File Transfer Protocol*), conexión remota con TELNET y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*).

#### 1.10.2.2 Transporte

Coincide con el nivel de transporte del modelo OSI. Los protocolos de esta capa,

TCP y UDP (Figura 1.23), se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos. Esta capa proporciona una comunicación extremo a extremo entre programas de aplicación.

En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores y se los pasa al nivel de red junto con la dirección destino. En el receptor este nivel se encarga de ordenar y unir los paquetes para generar de nuevo la información original.

#### 1.10.2.2.1 Protocolo UDP (User Datagram Protocol)

Proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade información al paquete que envía al nivel inferior (solo la necesaria para la comunicación extremo a extremo). Lo utilizan aplicaciones como NFS (*Network File System*) y RPC (*Remote Procedure Call*), pero sobre todo se emplea en tareas de control. Se utiliza UDP cuando es más importante la velocidad que la fiabilidad.

#### 1.10.2.2.2 Protocolo TCP (Transport Control Protocol)

Es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. La complejidad de la gestión de la fiabilidad tiene un costo en eficiencia, ya que para llevar a cabo las gestiones se tiene que añadir bastante información a los paquetes a enviar.

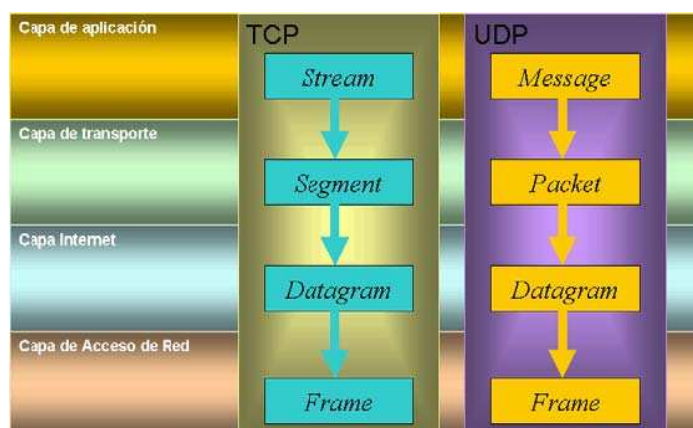


Figura 1.23 Protocolos de capa transporte en Arquitectura TCP/IP <sup>[14]</sup>

Debido a que los paquetes a enviar tienen un tamaño máximo, cuanto más información añadida el protocolo para su gestión, menos información que proviene de la aplicación contendrá ese paquete. TCP asegura la recepción de la información a transmitir en el destino.

### 1.10.2.3 Internet o de Red

Coloca la información que le pasa la capa transporte en datagramas IP, le añade cabeceras necesarias para su nivel y lo envía al nivel inferior. En esta capa se emplea el algoritmo de enrutamiento, al recibir un datagrama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra máquina.

#### 1.10.2.3.1 Protocolos del Nivel de Red

- ✓ *IP (Internet Protocol)*: Es no orientado a conexión, no confiable y tiene mensajes con un tamaño máximo. Cada datagrama se gestiona de forma independiente, por lo que dos datagramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que puedan llegar en diferente orden.
- ✓ *ICMP (Internet Control Message Protocol)*: Proporciona un mecanismo de información de control y de errores entre máquinas intermedias por las que viajarán los paquetes. Los mensajes ICMP están encapsulados en datagramas IP.
- ✓ *IGMP (Internet Group Management Protocol)*: Este protocolo está íntimamente ligado a IP. Se lo utiliza en máquinas que emplean IP *multicast* (datagramas con múltiples destinatarios).

También en este nivel se tiene una serie de protocolos que se encargan de la resolución de direcciones:

- ✓ *ARP (Address Resolution Protocol)*: Cuando una máquina desea ponerse en contacto con otra y necesita conocer su dirección física, entonces envía una petición ARP por *broadcast*. Solo contestará la máquina que corresponde a la dirección IP buscada, con un mensaje que incluye la dirección MAC. El



*software* de comunicaciones debe mantener una cache con los pares IP-MAC para tener conocimiento de las direcciones físicas y lógicas.

- ✓ *RARP (Reverse Address Resolution Protocol)*: Cuando una máquina conoce su dirección física y desea conocer su dirección lógica, envía por *broadcast* una petición RARP con su dirección física, para que un servidor pueda darle su correspondiente IP.

#### **1.10.2.4 Acceso de Red**

Este nivel se limita a recibir datagramas del nivel superior (capa *Internet*) y transmitirlo al *hardware* de la red. Pueden usarse diversos protocolos: LLC (*IEEE 802.2*), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las máquinas se identifican mediante una dirección de red lógica. Sin embargo, a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas.

## **1.11 ENRUTAMIENTO Y DIRECCIONAMIENTO**

### **1.11.1 DIRECCIONAMIENTO**

La dirección es el identificador que permite a otras máquinas enviar información; en el protocolo IP se especifica un punto de unión en la red llamado interfaz. Una máquina puede tener múltiples interfaces, teniendo una dirección IP por cada una de ellas; las interfaces son por lo general conexiones físicas distintas, pero también pueden ser conexiones lógicas compartiendo una misma interfaz.

### **1.11.2 DIRECCIÓN IP**

Una dirección IP puede ser escrita en varias formas: binaria, decimal y hexadecimal. Está formada por 32 bits que se agrupan en octetos; aunque, para entender mejor se utilizan las direcciones IP en formato decimal, representando el

valor decimal de cada octeto y separándolos con puntos, como se puede ver en la tabla 1.5.

Binario	01000001 00001010 00000010 00000011
Decimal	65.10.2.3

Tabla 1.5 Direcciones IP <sup>[15]</sup>

La dirección de una máquina se compone de dos partes cuya longitud puede variar:

- ✓ *Bits de red:* son los bits que definen la red a la que pertenece el equipo, siempre están a la izquierda.
- ✓ *Bits de host:* son los bits que distinguen a un equipo de otro dentro de una red. Siempre están a la derecha.

#### 1.11.2.1 Direcciones IPv4

En la versión 4, una dirección IP se representa mediante un número binario de 32 bits o como números de notación decimal (se dividen los 32 bits de la dirección en cuatro octetos). El valor decimal de cada octeto puede ser entre 0 y 255 (el número binario de 8 bits más alto es 11111111).

#### 1.11.2.2 Direcciones IPv6

Posee la misma funcionalidad que IPv4, está compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits, el equivalente a unos  $3.4 \times 10^{38}$  hosts direccionables. La ventaja con respecto a la dirección IPv4 es su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas acerca de la representación de direcciones IPv6 son:

- ✓ Los ceros iniciales se pueden obviar.

2001:0123:0004:00ab:0cde:3403:0001:0063 -> **2001:123:4:ab:cde:3403:1:63**

- ✓ Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación solo se puede hacer una vez.

*2001:0:0:0:0:0:4 -> 2001::4*

La dirección IP debe estar dentro del rango de direcciones asignadas al organismo o empresa a la que pertenece, estos rangos son concedidos por un organismo central de Internet denominado NIC (*Network Information Center*).

### **1.11.2.3 Clases de Dirección IPv4**

#### *1.11.2.3.1 Clase A*

En una dirección IP de clase A, el primer *byte* representa la red. El *bit* más significativo está en cero, lo que significa que hay  $2^7 = 128$  posibilidades de red. Sin embargo, la red 0 no existe y la 127 está reservado para indicar al propio equipo.

Las redes clase A disponibles van desde *1.0.0.0* a *126.0.0.0*. Los tres *bytes* restantes representan los equipos de la red; se puede tener una cantidad igual a:  $2^{24} - 2 = 16.777.214$  equipos.

#### *1.11.2.3.2 Clase B*

En una dirección IP clase B, los primeros dos *bytes* representan la red y los *bits* más significativos son 10; esto significa que existen  $2^{14}$  posibilidades de red, es decir, 16.384 redes posibles. Las redes disponibles de clase B van de *128.0.0.0* a *191.255.0.0*.

Los dos *bytes* restantes representan los equipos o *hosts* de la red. La red puede entonces contener una cantidad de equipos equivalente a:  $2^{16} - 2 = 65.534$  equipos.

#### *1.11.2.3.3 Clase C*

En una dirección IP clase C, los primeros tres *bytes* representan la red y los *bits* más significativos son 110. Esto significa que hay  $2^{21}$  posibilidades de red, es

decir, 2.097.152. Por lo tanto, las redes disponibles clase C van desde 192.0.0.0 a 223.255.255.0. El *byte* de la derecha representa los equipos de la red la cual puede tener:  $2^8 - 2 = 254$  equipos.

#### 1.11.2.3.4 Clase D

Las direcciones de clase D son un grupo especial que se utilizan para dirigirse a grupos de máquinas (*multicast*), estas direcciones son muy poco utilizadas. Los cuatro primeros *bits* de una dirección de clase D son 1110.

#### 1.11.2.3.5 Clase E

Los cuatro *bits* más significativos del primer octeto son: 1111 (primer número entre 240 y 255). Se encuentran reservados para usos futuros.

Clase	Dirección IP (R=Red – H=Host)	Rango	Nº de Redes	Nº de Hosts	Máscara de Red
A	0rrrrrrr.hhhhhhhh.hhhhhhhh.hhhhhhhh	1.0.0.0-127.255.255.255	126	16777214	255.0.0.0
B	10rrrrrr.rrrrrrr.hhhhhhhh.hhhhhhhh	128.0.0.0-191.255.255.255	16384	65534	255.255.0.0
C	110rrrrr.rrrrrrr.rrrrrrr.hhhhhhhh	192.0.0.0-223.255.255.255	2097152	254	255.255.255.0
D	1110 [Dirección de <i>Multicast</i> ]	224.0.0.0-239.255.255.255			
E	1111 [Reservado]	240.0.0.0-255.255.255.255			

Tabla 1.6 Clases de direcciones IP <sup>[16]</sup>

#### 1.11.2.4 Direcciones de Red Reservadas

Es habitual que en una empresa u organización un solo equipo tenga conexión a *Internet* y los otros equipos de la red accedan a *Internet* a través de éste (por lo general un *proxy*). Así, solo el equipo conectado a la red necesita reservar una dirección IP con la ICANN (*Internet Corporation for Assigned Names and Numbers*). Sin embargo, los otros equipos necesitarán una dirección IP privada para comunicarse entre ellos.

La ICANN ha reservado direcciones de cada clase para facilitar la asignación de direcciones IP a los equipos de una red local conectada a *Internet*, sin riesgo de crear conflictos de direcciones IP en la red de redes. Estas direcciones son:

- ✓ *Direcciones IP privadas de clase A*: 10.0.0.1 a 10.255.255.254; hacen posible la creación de grandes redes privadas con miles de equipos.
- ✓ *Direcciones IP privadas de clase B*: 172.16.0.1 a 172.31.255.254; hacen

posible la creación de redes privadas de tamaño medio.

- ✓ *Direcciones IP privadas de clase C*: 192.168.0.1 a 192.168.255.254; para establecer pequeñas redes privadas.

#### **1.11.2.5 Dirección IP Dinámica**

Una dirección IP dinámica es una IP asignada mediante un servidor DHCP (*Dynamic Host Configuration Protocol*). La IP que se obtiene tiene una duración máxima determinada o suelen cambiar cada vez que el usuario reconecta el equipo por cualquier causa. Las direcciones IPs dinámicas son las que actualmente ofrecen la mayoría de operadores.

##### *1.11.2.5.1 Asignación de direcciones IP*

- ✓ Asignación Manual

Utilizada cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP creadas manualmente por el administrador de la red. Solo clientes con una dirección MAC válida recibirán una dirección IP del servidor.

- ✓ Asignación Dinámica

Es el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su *software* de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

#### **1.11.2.6 Dirección IP Fija**

Una dirección IP fija es una IP asignada por el usuario, o bien dada por el proveedor ISP. Permite tener servicios dirigidos directamente a la IP; esto permite al usuario asignar estas direcciones a servidores *WEB*, correo, FTP, etc. y dirigir un nombre de dominio a esta IP sin tener que mantener actualizado el servidor DNS cada vez que cambie la IP como ocurre con las IPs dinámicas. Son más vulnerables al ataque, ya que el usuario no puede conseguir otra IP.

### 1.11.3 MÁSCARA DE SUBRED

Una máscara se genera con bits uno en la ubicación de los *bits* que se quiera conservar y ceros en aquellos que quiera cancelar. Por lo tanto, la máscara de red se presenta bajo la forma de 4 *bytes* separados por puntos (como una dirección IP), y está compuesta (en su notación binaria) por ceros en el lugar de los *bits* que corresponden a los *hosts* y por unos en el lugar de los *bit* de red.

El interés principal de una máscara de subred reside en que permite la identificación de la red asociada con una dirección IP. Es posible obtener máscaras relacionadas con cada clase de dirección:

- ✓ Para una dirección *Clase A*, se debe conservar solo el primer *byte*. La máscara tiene el siguiente formato `11111111.00000000.00000000.00000000`, es decir, `255.0.0.0` en decimal;
- ✓ Para una dirección *Clase B*, se deben retener los primeros dos *bytes* `11111111.11111111.00000000.00000000`, que corresponde a `255.255.0.0` en decimal;
- ✓ Para una dirección *Clase C*, siguiendo el mismo razonamiento, la máscara tendrá el formato `11111111.11111111.11111111.00000000`, es decir, `255.255.255.0` en decimal.

### 1.11.4 CREACIÓN DE SUBREDES

El enmascaramiento puede dividir a una red en subredes. La cantidad de subredes dependerá del número de bits adicionales asignados a la red; esto se puede ver en la Tabla 1.7.

NÚMERO DE BITS	NÚMERO DE SUBREDES
1	2
2	4
3	8
4	16
5	32
6	64
7 (no para clase C)	128
8 (imposible para clase C)	256

Tabla 1.7 Determinación de Subredes <sup>[16]</sup>

## **1.11.5 TIPOS DE ENRUTAMIENTO**

### **1.11.5.1 Enrutamiento Estático**

Una red con un número mínimo de enrutadores o con un solo *gateway* puede ser configurada con enrutamiento estático. Una tabla de enrutamiento estático es construida manualmente por el administrador de la red.

Las tablas de enrutamiento estático no se ajustan a los cambios de la red, ellos trabajan mejor cuando las rutas no cambian. El enrutador al recibir un paquete, busca la ruta por la cual debe enviarlo, tomando en cuenta primero las de menos saltos, luego las específicas y de no encontrar el destino en ninguna de éstas, lo envía por la ruta por defecto.

### **1.11.5.2 Enrutamiento Dinámico**

Una ruta dinámica es construida mediante información intercambiada por los protocolos de enrutamiento. Esta información permite ajustar las rutas reflejadas en las condiciones de la red y manejar complejas situaciones de enrutamiento más rápido de lo que un administrador del sistema podría hacerlo. Los protocolos no solo están diseñados para cambiar a una ruta de respaldo cuando la primaria se vuelve inoperante sino que también evalúan y deciden cuál es la mejor ruta para un destino.

## **1.12 RED PRIVADA VIRTUAL (VPN)**

### **1.12.1 DEFINICIÓN**

Brinda conectividad de diferentes segmentos de red o usuarios a una red principal a través de una red pública. Provee integridad y seguridad de la información manteniendo la privacidad a través del uso de un protocolo de túnel o aislamiento.

Las VPNs inalámbricas permiten la conexión segura a redes corporativas, a través de dispositivos móviles como: *laptops*, PDAs, teléfonos celulares. Dentro de este tipo de VPN's se debe considerar la tasa de transferencia y capacidad de procesamiento por parte de los equipos. La mayor ventaja de las VPN inalámbricas es la conectividad y la movilidad para los usuarios finales.

## **1.12.2 REQUERIMIENTOS PARA VPN**

### **1.12.2.1 Seguridad**

- ✓ Todo el tráfico en la VPN debe estar encriptado y autenticado.
- ✓ La seguridad debe ser acordada por todas las partes de la VPN.
- ✓ Nadie fuera de la VPN puede afectar las propiedades de ésta. Debe ser imposible para un atacante cambiar las propiedades de seguridad de cualquier parte de la VPN.

### **1.12.2.2 Confiabilidad**

- ✓ Nadie más que el proveedor puede afectar o modificar el canal en la VPN.
- ✓ El direccionamiento y el ruteo usado en una VPN deberán ser establecidos antes que sea creada.

## **1.12.3 TIPOS DE VPN**

### **1.12.3.1 VPN de Acceso Remoto**

Consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos utilizando *Internet* como vínculo de acceso. Muchas empresas han reemplazado con esta tecnología su infraestructura *dial-up* (*modems* y líneas telefónicas).

### **1.12.3.2 VPN Punto a Punto**

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, posee un vínculo permanente a *Internet* donde acepta las conexiones provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a *Internet* utilizando los servicios de su



proveedor local, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto, sobre todo en las comunicaciones internacionales.

### **1.12.3.3 VPN Interna WLAN**

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar *Internet* como medio de conexión, emplea la misma red de área local de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

### **1.12.4 PROTOCOLOS UTILIZADOS**

Usando una combinación de encriptación, autenticación y control de acceso, una VPN proporciona a los usuarios un método seguro de acceso a los recursos de las redes corporativas. La implementación de una VPN involucra dos tecnologías: un protocolo de túnel y un método de autenticación de los usuarios del túnel.

Tres diferentes protocolos de túnel son los más usados para la construcción de VPN sobre la *Internet*:

- ✓ Protocolo de túnel punto - punto (PPTP).
- ✓ Envío de capa 2 (L2F)
- ✓ Protocolo de túnel de capa 2 (L2TP)

La razón de la diversidad de protocolos es porque las empresas que implementan VPN's tienen requerimientos diferentes. Los protocolos PPTP, L2F y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN punto - punto.

#### 1.12.4.1 PPTP

PPTP se basa en la funcionalidad de PPP (*punto a punto*) para proveer acceso remoto que puede estar dentro de un túnel a través de la *Internet* hacia su destino.

PPTP encapsula los paquetes PPP usando una versión modificada del GRE (*Generic Routing Encapsulation*), lo que le da la flexibilidad de manejo de otros protocolos como: IPX (*Intercambio de Paquetes de Internet*) y la NetBEUI (*Interfaz Gráfica de Sistema Básico de Entrada/Salida de red*).

PPTP está diseñado para “correr” en la capa de enlace de datos del sistema OSI, por ello se permite transmitir protocolos distintos a los IP sobre los túneles. Una desventaja de este protocolo es que no provee una fuerte encriptación para proteger la información y tampoco soporta métodos de autenticación basados en *tokens*.

#### 1.12.4.2 L2F

L2F fue diseñado como protocolo de túnel de tráfico desde usuarios remotos hacia los corporativos. Una diferencia entre PPTP y L2F es que el túnel creado por L2F no es dependiente en IP, y le permite trabajar directamente con otro tipo de redes como *Frame Relay* o ATM. Al igual que PPTP, L2F emplea PPP para la autenticación del usuario remoto. L2F permite túneles para soportar más de una conexión.

#### 1.12.4.3 L2TP

L2TP es un protocolo de capa 2, permite a los usuarios la misma flexibilidad que PPTP para manejar protocolos diferentes a los IP, como IPX y NetBEUI. L2TP es una combinación de PPTP y L2F y puede ser implementado en diferentes topologías como *Frame Relay* y ATM. Para proveer mayor seguridad con la encriptación, se pueden emplear los métodos de encriptación de *IPSec*. La recomendación es que para procesos de encriptación y manejo de llaves criptográficas en ambientes IP, el protocolo *IPSec* sea implementado de manera conjunta.

### **1.12.5 TIPOS DE CONEXIÓN**

#### **1.12.5.1 Conexión de Acceso Remoto**

Una conexión de acceso remoto es realizada por un usuario de un computador que se conecta a una red privada. Para enviar los paquetes a través de la conexión VPN el cliente se autentica al servidor y viceversa.

#### **1.12.5.2 Conexión VPN Router a Router**

Es realizada por un *router* que a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier *router* no se originan en ellos. El *router* que realiza la llamada se autentica ante el *router* que responde y viceversa.

#### **1.12.5.3 Conexión VPN Firewall ASA a Firewall ASA**

Es realizada por uno de los *firewall* que a su vez se conecta a una red privada. En esta conexión, los paquetes son enviados desde cualquier usuario en *Internet*. El *firewall* que realiza la llamada se autentica ante el que responde y viceversa.

## **1.13 VOZ SOBRE IP**

### **1.13.1 VOZ SOBRE INTERNET**

VoIP es un grupo de recursos que hacen posible que la señal de voz viaje a través de *Internet* empleando el protocolo IP. La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. Esto significa que se envía la señal de voz en forma digital en lugar de enviarla a través de circuitos solo para telefonía como una compañía telefónica convencional o PSTN (*Public Switched Telephone Network*). El tráfico de voz sobre IP puede circular por cualquier red IP.

La VoIP es más económica que la convencional porque el sistema de

encaminamiento y conmutación es más eficiente que el de las grandes centrales telefónicas, las cuales necesitan un circuito por cada conversación; mientras que en IP al dividir la información en paquetes, se pueden enviar varias conversaciones multiplexadas sobre un único circuito físico.

Para establecer una comunicación de voz utilizando la red *Internet*, lo primero que se necesita es establecer la conexión entre los dos terminales de los usuarios que desean comunicarse equipados con el mismo *software* o compatible. La evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien repartidas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, *Frame Relay*, ATM o SONET.

### 1.13.2 FUNCIONALIDAD

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas comunes:

- ✓ Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar dónde se esté conectado a la red.
- ✓ Los agentes de *call center* usando teléfonos VoIP pueden trabajar en cualquier lugar con conexión a Internet lo suficientemente rápida.
- ✓ Algunos paquetes de VoIP incluyen los servicios por los que PSTN normalmente cobra un cargo extra, o que no se encuentran disponibles en algunos países, como son las llamadas de 3 a la vez, retorno de llamada, remarcación automática, o identificación de llamadas.

### 1.13.3 EL ESTÁNDAR VoIP (H.323)<sup>12</sup>

Definido en 1996 por la UIT (*Unión Internacional de Telecomunicaciones*).

---

<sup>12</sup> Referirse a la página Web [http://es.wikipedia.org/wiki/Voz\\_sobre\\_IP](http://es.wikipedia.org/wiki/Voz_sobre_IP) h.323

### 1.13.3.1 Características Principales

- ✓ Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento.
- ✓ Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes IP actuales.
- ✓ Es independiente del *hardware* utilizado.
- ✓ Permite ser implementado tanto en *software* como en *hardware*.

### 1.13.3.2 Pila de Protocolos H.323

El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

#### 1.13.3.2.1 Direccionamiento

- ✓ *RAS (Registration, Admission and Status)*: Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del *Gatekeeper*.
- ✓ *DNS (Domain Name Service)*: Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS

#### 1.13.3.2.2 Señalización

- ✓ Q.931 Señalización inicial de llamada
- ✓ H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del flujo de voz
- ✓ H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para flujos de voz

#### 1.13.3.2.3 Compresión de Voz<sup>13</sup>

- ✓ *Requeridos*: G.711 y G.723.
- ✓ *Opcionales*: G.728, G.729 y G.722.

---

<sup>13</sup> Referirse a la tabla 3.1 en el Capítulo 3

#### 1.13.3.2.4 Transmisión de Voz

- ✓ *UDP*: La transmisión se realiza sobre paquetes UDP, aunque no ofrece integridad en los datos, se aprovecha mejor el ancho de banda que con TCP.
- ✓ *RTP (Real Time Protocol)*: Maneja los aspectos relativos a la temporización, marca los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

#### 1.13.3.2.5 Control de la Transmisión

- ✓ *RTCP (Real Time Control Protocol)*: Se utiliza principalmente para detectar situaciones de congestión de la red y tomar acciones correctoras en caso de ser necesario.



Figura 1.24 Control de Transmisión en Protocolo H.323 <sup>[17]</sup>

#### 1.13.3.3 Alcance del Protocolo H.323

El protocolo H.323 hace referencia a una gran cantidad de protocolos específicos para codificación de voz, establecimiento de llamadas, señalización, transporte de datos, entre otros.

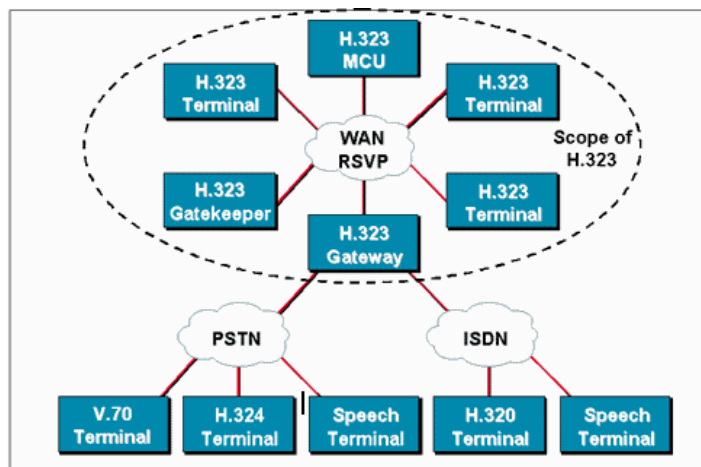


Figura 1.25 Alcance del Protocolo H.323 <sup>[18]</sup>

El modelo general se ilustra en la figura 1.25. En el centro se encuentra un *Gateway* H.323 que conecta *Internet* con la Red Telefónica (PSTN o ISDN). Los dispositivos de comunicación se llaman Terminales. Una red LAN puede tener un *Gatekeeper*, el cual controla los terminales bajo su jurisdicción, llamados zona.

#### 1.13.4 PROTOCOLO SIP (*SESSION INITIATION PROTOCOL*) <sup>14</sup>

##### 1.13.4.1 Definición

Es un protocolo que se encarga de la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia. SIP es uno de los protocolos de señalización para voz sobre IP.

Se complementa, entre otros, con el SDP (*Session Description Protocol*), que describe el contenido multimedia de la sesión, como cuáles direcciones IP, puertos y *codecs* se usarán durante la comunicación; y, con el RTP (*Real-time Transport Protocol*) que es el portador para el contenido de voz y video que intercambian los participantes en una sesión establecida por SIP.

##### 1.13.4.2 Funciones Básicas

- ✓ Determina la ubicación de los usuarios, proveyendo nomadicidad.
- ✓ Establece, modifica y termina sesiones multipartitas entre usuarios.

<sup>14</sup> Referirse a la página Web [http://es.wikipedia.org/wiki/Session\\_Initiation\\_Protocol](http://es.wikipedia.org/wiki/Session_Initiation_Protocol)

SIP adopta el modelo cliente-servidor y es transaccional. El cliente realiza peticiones que el servidor atiende y genera una o más respuestas. Los servidores, por defecto, utilizan el puerto 5060 para recibir las peticiones de los clientes SIP.

#### **1.13.4.3 Características**

- ✓ Utilizado en telefonía.
- ✓ Aporta un conjunto de funciones de procesamiento de llamadas en la PSTN.
- ✓ Permite llamar a un número, provocar que un teléfono suene al ser llamado, escuchar la señal de tono o de ocupado.
- ✓ Estandarizado principalmente por el IETF (*Internet Engineering Task Force*).
- ✓ SIP es similar a HTTP, comparte con él algunos de sus principios de diseño: es legible por humanos y sigue una estructura de petición-respuesta.
- ✓ Es más simple que H.323.

#### **1.13.4.4 Elementos del Protocolo**

##### *1.13.4.4.1 Agentes de Usuario*

Son los puntos extremos del protocolo, es decir son los que emiten y reciben los mensajes del protocolo SIP como un videoteléfono, un teléfono o cualquier otro dispositivo similar.

El protocolo SIP no se ocupa de la interfaz de estos dispositivos con el usuario final, solo se interesa en los mensajes que éstos generan y cómo se comportan al recibir determinados mensajes.

Los agentes de usuario se comportan como clientes UAC (*User Agent Clients*) y como servidores UAS (*User Agent Servers*). Son UAC cuando realizan una petición y son UAS cuando la reciben.

##### *1.13.4.4.2 Servidores de Registro*

El protocolo SIP permite establecer la ubicación física de un usuario determinado, es decir, a qué punto de la red está conectado y para ello usa un mecanismo de



registro. Este mecanismo funciona de la siguiente manera:

Cada usuario tiene una dirección lógica que es invariable respecto de su ubicación física. Una dirección lógica del protocolo SIP es de la forma *usuario@dominio*. La dirección física o dirección de contacto es dependiente del lugar en donde el usuario está conectado. Cuando un usuario inicializa su terminal conectando el teléfono o abriendo el *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.

#### 1.13.4.4.3 Servidores Proxy y de Redirección

Para encaminar un mensaje entre un agente de usuario cliente y un agente de usuario servidor normalmente se recurre a los servidores. Estos servidores pueden actuar de dos maneras:

1. Como *Proxy*, encaminando el mensaje hacia destino,
2. Como Redirector, generando una respuesta que indica al origen la dirección del destino o de otro servidor que lo acerque al destino.

La principal diferencia es que el servidor *proxy* queda formando parte del camino entre el UAC y el o los UAS, 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 *Proxy* dependiendo de la situación.

#### 1.13.4.5 Formato de los Mensajes

Los mensajes que se intercambian en el protocolo SIP pueden ser peticiones o respuestas. Las peticiones tienen una línea de petición, una serie de encabezados y un cuerpo. Las respuestas varían de las peticiones en que tienen una línea de respuesta.

En la línea de petición se indica el propósito de la petición y el destinatario. En la

línea de respuesta se encuentra el código de estado de la respuesta, siendo éste un número que indica el resultado del procesamiento de la petición.

#### **1.13.4.6 Establecimiento de una Sesión**

1. Un usuario ingresa la dirección lógica de la persona con la que quiere comunicarse, puede indicar también las características de la sesión que quiere establecer (voz, voz y video, etc.).
2. El agente de usuario SIP que reside en el terminal, actuando como UAC envía la petición *INVITE* al servidor que tiene configurado. Este servidor se vale del sistema DNS para determinar la dirección del servidor SIP del dominio del destinatario y encamina hacia allí la petición.
3. El servidor de dominio destino establece que la petición es para alguien de su dominio y mediante la información de registro del usuario establece su ubicación física. Si la encuentra, encamina la petición hacia dicha dirección.
4. El agente de usuario destino si se encuentra desocupado comenzará a alertar al usuario destino y envía una respuesta hacia el usuario origen con un código de estado que indica esta situación (180).
5. Cuando el usuario destino finalmente acepta la invitación, se genera una respuesta con un código de estado (200) que indica que la petición fue aceptada.
6. La recepción de la respuesta final es confirmada por el UAC origen mediante una petición con el método ACK; esta petición no genera respuestas y completa la transacción de establecimiento de la sesión.
7. Al terminar la sesión, el agente de usuario de la parte que terminó la sesión, actuando como UAC, envía hacia la otra una petición con el método BYE.
8. Cuando lo recibe el UAS genera la respuesta con el código de estado correspondiente.

### **1.13.5 ARQUITECTURA DE RED**

#### **1.13.5.1 Terminales**

Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en *software* como en *hardware*. Pueden ser de dos tipos:

- ✓ *IP PHONE*: O teléfonos IP, se muestra en la figura 1.26.



Figura 1.26 Teléfono IP <sup>[18]</sup>

- ✓ *SOFT PHONE*: Se trata normalmente de una PC multimedia que simula un teléfono IP, por ejemplo, el servicio de *NetMeeting* utiliza protocolo H.323.

#### 1.13.5.2 *Gatekeepers*

Son el centro de toda la organización VoIP, y serían el sustituto para las actuales centrales. Normalmente implementadas en *software*, en caso de existir, todas las comunicaciones pasarían por él.

Todos los elementos de red de VoIP (terminales, *Gateways*, MCU) tienen que usar el *Gatekeeper* como punto intermedio para la señalización. Los elementos de red se comunican con el *Gatekeeper* de VoIP utilizando el protocolo RAS. Los *Gatekeepers* actúan como controladores del sistema y cumplen con el segundo nivel de funciones esenciales en VoIP de clase *carrier*, es decir, autenticación, enrutamiento del servidor de directorios, contabilidad de llamadas y determinación de tarifas.

Los *Gatekeepers* utilizan la interfaz estándar de la industria ODBC-32 (*Open Data Base Connectivity*), para acceder a los servidores de *backend* en el centro de cómputo del *carrier* y así autenticar a las personas que llaman como abonados válidos al servicio, optimizar la selección del *gateway* de destino y sus alternativas, hacer un seguimiento y una actualización de los registros de llamadas y la información de facturación, y guardar detalles del plan de facturación de la persona que efectúa la llamada.

Tiene las siguientes funciones básicas:

- ✓ Autenticación y control de admisión, para permitir o denegar el acceso de usuarios.
- ✓ Proporciona servicios de control de llamada.
- ✓ Servicio de traducción de direcciones (DNS), de tal manera que se puedan usar nombres en lugar de direcciones IP.
- ✓ Gestionar y controlar los recursos de la red: Administración del ancho de banda.
- ✓ Localizar los distintos *Gateways* y MCU's cuando se necesita.

### 1.13.5.3 Gateways

El *Gateway* es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica PSTN o RDSI. Se puede considerar al *Gateway* como una caja que por un lado tiene un interfaz LAN Ethernet, *Frame Relay* o ATM y por el otro dispone de uno o varios de los siguientes interfaces:

- ✓ FXO. Para conexión a extensiones de centrales ó a la red telefónica básica.
- ✓ FXS. Para conexión a enlaces de centrales o a teléfonos analógicos.
- ✓ E&M. Para conexión específica a centrales.
- ✓ BRI. Acceso básico RDSI (2B+D)
- ✓ PRI. Acceso primario RDSI (30B+D)
- ✓ G703/G.704. (E&M *digital*) Conexión específica a centrales a 2 Mbps.

El procesamiento que realiza el *gateway* de la cadena de audio que atraviesa una red IP es transparente para los usuarios. Desde el punto de vista de la persona que llama, la experiencia es muy parecida a utilizar una tarjeta de llamada telefónica. La persona que realiza la llamada ingresa a un *gateway* por medio de un teléfono convencional discando un número de acceso. Una vez que fue autenticada, disca el número deseado y escucha los tonos de llamada habituales hasta que alguien responde del otro lado.

Se tiene dos tipos de *Gateways*:

- ✓ *Gateway H.323/H.320*: Básicamente realiza la conversión entre estos dos

formatos de forma que los terminales H.323 se pueden comunicar con equipos RDSI de videoconferencia, que pueden formar parte de la red corporativa o estar situados en la red pública.

- ✓ *Gateway H.323/RTB (Voz sobre IP)*: Posibilita las comunicaciones de voz entre los terminales H.323 y los teléfonos convencionales.

Con los tres elementos mencionados, la estructura de la red VoIP podría ser la conexión de dos delegaciones de una misma empresa, así todas las comunicaciones entre las delegaciones son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores.

#### **1.13.5.4 Protocolos de VoIP**

Es el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

- ✓ Por orden de antigüedad (del más antiguo al más nuevo):
  - H.323 - Protocolo definido por la ITU-T
  - SIP - Protocolo definido por la IETF
  - MGCP - Protocolo de control, propietario de Cisco
  - Megaco (También conocido como H.248) - Protocolo de control
  - *Skinny Client Control Protocol* - Protocolo propiedad de Cisco
  - MiNet - Protocolo propiedad de Mitel
  - CorNet-IP - Protocolo propiedad de Siemens
  - IAX - Protocolo original para la comunicación entre PBXs Asterisk (obsoleto)
  - Skype - Protocolo propietario *peer-to-peer* utilizado en la aplicación Skype
  - IAX2 - Protocolo para la comunicación entre *PBXs Asterisk* en reemplazo de IAX
  - Jingle - Protocolo abierto utilizado en tecnología *Jabber*
  - Telme- Protocolo propietario Woip2 utilizado en la aplicación *DeskCall*

La tabla 1.8 realiza una comparación entre las características más importantes de los protocolos para VoIP antes descritos. En la primera columna se tiene los protocolos y en la primera fila se tiene a las características que se explican a continuación:

- ✓ *Tecnología*: Se refiere a los protocolos de red tradicionales utilizados por el protocolo VoIP; a la arquitectura y a mecanismos de transmisión.
- ✓ *Disponibilidad*: Varía si es propietario, si tiene una especificación simple o compleja o si es *open*.
- ✓ *Seguridad*: Se refiere a los mecanismos de seguridad que implementa como la autenticación, el cifrado del flujo, etc.
- ✓ *NAT*: Varía de acuerdo a la medida en que es soportado por el protocolo VoIP.

	TECNOLOGÍA	DISPONIBILIDAD	SEGURIDAD	NAT	TOTAL
SIP	2	2	2	1	7
IAX	2	3	1	3	9
H.323	3	1	2	1	7
MGCP	2	1			3
SCCP	3	1			4

Tabla 1.8 Protocolos de VoIP <sup>[19]</sup>

Las redes de VoIP suelen contener componentes fundamentales como: teléfonos IP's, adaptadores para PC's, Hubs telefónicos, Gateways H.323, Gatekeeper, MCUs (*Unidades de Conferencia Multimedia*), que se los puede apreciar en la Figura 1.27.

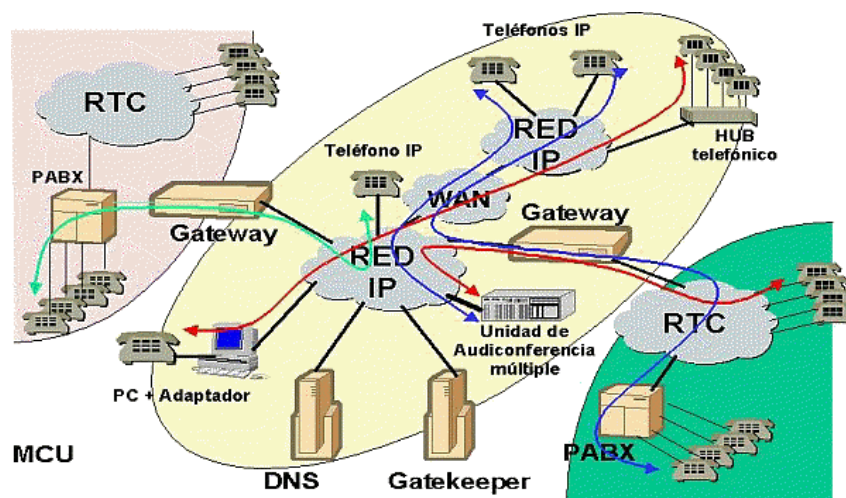


Figura 1.27 Elementos de una red VoIP<sup>[17]</sup>

### 1.13.6 PARÁMETROS DE VoIP

#### 1.13.6.1 Codecs

Garantizan la codificación y compresión del audio o del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el *codec* utilizado en la transmisión, se utilizará mayor o menor ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos. Entre los *codecs* utilizados en VoIP se encuentran los G.711, G.723.1 y el G.729 (especificados por la ITU-T).

#### 1.13.6.2 Retardo o Latencia

Una vez establecidos los retardos de tránsito y el retardo de procesamiento la conversación se considera aceptable por debajo de los 150 ms.

#### 1.13.6.3 Calidad del Servicio

La calidad de servicio se logra en base a los siguientes criterios:

- ✓ La supresión de silencios otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.
- ✓ Compresión de cabeceras aplicando los estándares RTP/RTCP.
- ✓ Priorización de los paquetes que requieran menor latencia. Las tendencias

actuales son:

- *CQ (Custom Queuing)*: Asigna un porcentaje del ancho de banda disponible.
- *PQ (Priority Queuing)*: Establece prioridad en las colas.
- *WFQ (Weight Fair Queuing)*: Se asigna la prioridad al tráfico de menos carga.
- *DiffServ*: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.



# CAPÍTULO 2

**ANÁLISIS DE LA  
SITUACIÓN ACTUAL Y  
REQUERIMIENTOS**

## ANÁLISIS DE LA SITUACIÓN ACTUAL Y REQUERIMIENTOS

### 2.1 ANTECEDENTES<sup>15</sup>

La Compañía Nacional de Transmisión Eléctrica, TRANSELECTRIC S.A., es una Sociedad Anónima que tiene como único accionista al Fondo de Solidaridad. En abril de 1999, la Compañía inicia sus actividades de servicio a los agentes del MEM (*Mercado Eléctrico Mayorista*).

TRANSELECTRIC S.A. es responsable de operar el Sistema Nacional de Transmisión mediante el transporte de energía eléctrica, garantizando el libre acceso a las redes de transmisión a los agentes del MEM, compuesto por generadores, distribuidores y grandes consumidores. Además, transmite la energía eléctrica en forma continua, segura y con calidad, así como la entrega en bloque a cada empresa de distribución.

Como se puede ver en la figura 2.1, TRANSELECTRIC S.A. tiene instalada una red de telecomunicaciones por fibra óptica que posibilita la óptima operación del SNI (*Sistema Nacional Interconectado*); provee los canales respectivos con la finalidad de tener un adecuado funcionamiento del SNT (*Sistema Nacional de Transmisión*), así como un correcto despacho de energía al MEM, garantizando la disponibilidad del fluido eléctrico a todo el país con calidad y seguridad. Funciona además, en el mercado de telecomunicaciones, bajo la modalidad de portador de portadores a nivel nacional.

Actualmente TRANSELECTRIC S.A. es el mayor portador de servicios de Internet en el Ecuador, con un 60% del mercado nacional, a través de TRANSNEXA, empresa Colombo-Ecuatoriana cuya constitución tiene su origen en la alianza estratégica con INTERNEXA, filial de ISA Colombia.

---

<sup>15</sup> Tomado del Resumen Ejecutivo 2008 de TRANSELECTRIC S.A.

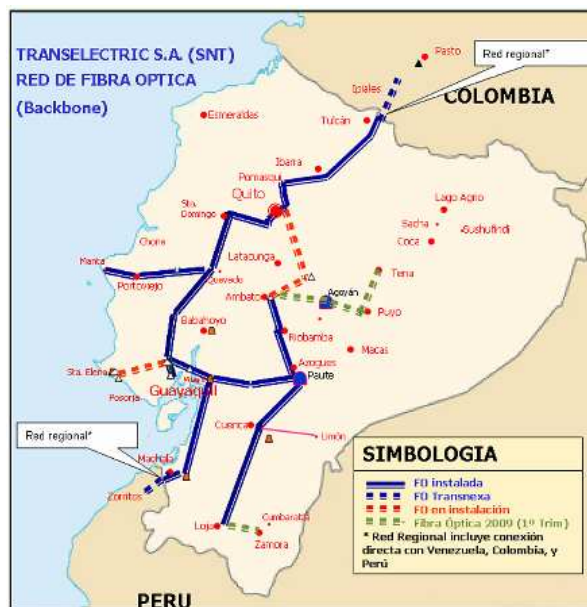


Figura 2.1 Red de Fibra Óptica de TRANSELECTRIC S.A. [1]

TRANSELECTRIC S.A. forma parte de la red continental de fibra óptica más grande de Sudamérica, denominada Red Bolivariana de Telecomunicaciones, la cual tiene una extensión de 11 mil kilómetros e incluye a Venezuela, Colombia, Ecuador, Perú y Bolivia. Esto permitirá que el Ecuador cuente con otras alternativas de conexión nacional e internacional, disminuyendo el costo del servicio y mejorando su calidad.

### 2.1.1 MISIÓN

Garantizar al país y a sus clientes la disponibilidad del SNT y de la red de Telecomunicaciones, con calidad y eficiencia, generando valor para los accionistas, colaboradores y la comunidad, promoviendo así el desarrollo del Sector Eléctrico y de las Telecomunicaciones.

### 2.1.2 VISIÓN

Hasta el 2012 ser una corporación empresarial, líder del país en el sector eléctrico y de telecomunicaciones, ubicada entre las 5 empresas de Sudamérica en calidad de transmisión de energía eléctrica.

### 2.1.3 VALORES

- ✓ Transparencia
- ✓ Calidad
- ✓ Proactividad
- ✓ Responsabilidad Social Empresarial
- ✓ Cumplimiento de Normas
- ✓ Mejora Continua

### 2.1.4 COMPETENCIAS DE LA ORGANIZACIÓN

- ✓ Comunicación relevante a todo nivel
- ✓ Orientación a Resultados
- ✓ Servicio al Cliente Interno y Externo
- ✓ Trabajo en Equipo

### 2.1.5 INFRAESTRUCTURA

El edificio matriz de TRANSELECTRIC S.A. está ubicado en la Avenida 6 de Diciembre N26-235 y Avenida Orellana. Tiene 10 pisos y dos alas por cada uno, donde se encuentran las diferentes áreas de la Compañía. Una de las alas del cuarto piso está alquilada a TermoPichincha y no posee usuarios de TRANSELECTRIC. En el edificio existen aproximadamente 350 usuarios, los que dependiendo de sus funciones tienen su propio computador y/o *laptop* en el puesto de trabajo.

En la Figura 2.2 se puede ver la ubicación del edificio matriz de TRANSELECTRIC en Quito descrito anteriormente.

El COT (*Centro de Operaciones de Transmisión*) queda ubicado en Calderón y éste se comunica con el edificio matriz a través de un enlace de fibra óptica. Las instalaciones del COT son relativamente nuevas y tienen aproximadamente 40 usuarios.

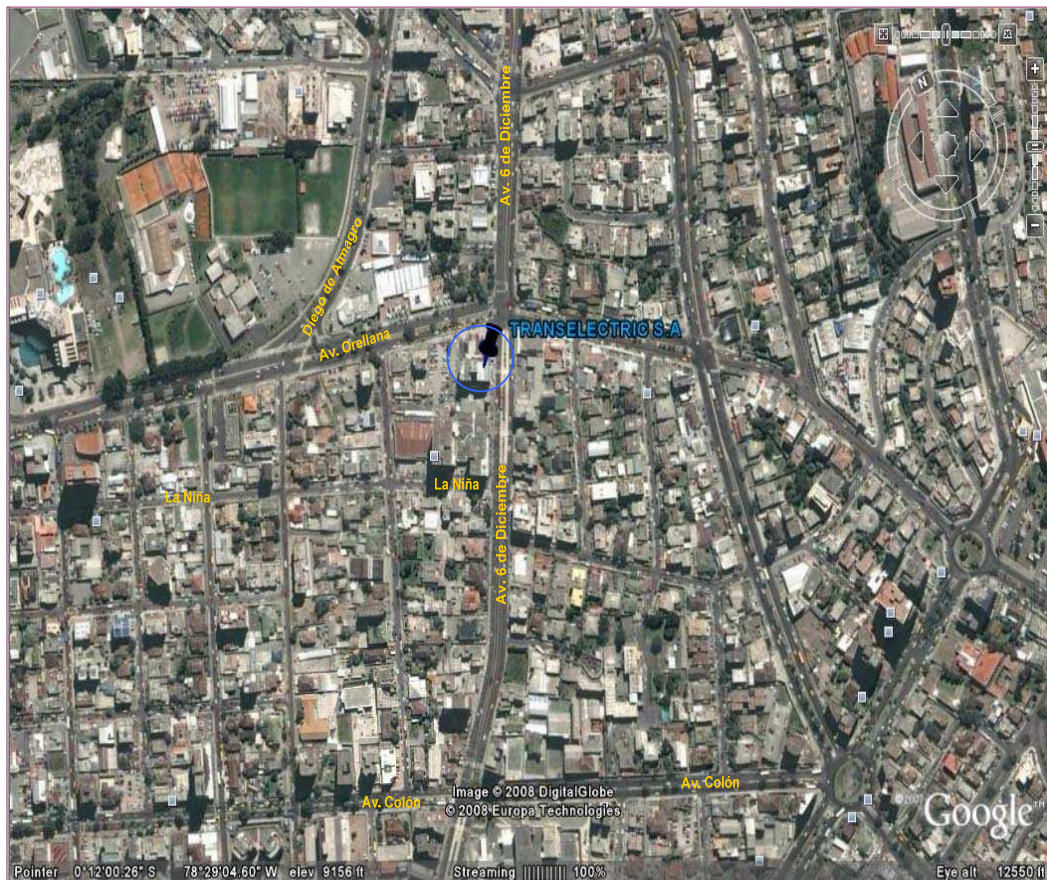


Figura 2.2 Ubicación del Edificio Matriz de Transelectric S.A.

## 2.2 SITUACIÓN ACTUAL

### 2.2.1 INFRAESTRUCTURA DEL CABLEADO ESTRUCTURADO

El edificio matriz de TRANSELECTRIC S.A. posee dos “cuartos de telecomunicaciones”, los cuales son una combinación de Cuarto de Telecomunicaciones y Cuarto de Equipos debido a que contienen elementos tales como *switches*, *routers* y *PABX*. Éstos se encuentran ubicados en el quinto y noveno piso.

En estos pisos están principalmente los *switches* de acceso, de distribución, *modems*, bases celulares y las centrales telefónicas; para describirlos de manera

más detallada, se los mencionará en adelante como Cuarto de Telecomunicaciones.

Cabe mencionar que según los estándares de cableado estructurado es recomendable tener un cuarto de telecomunicaciones por piso. Esto no se cumple debido a que se tienen más pisos que cuartos de telecomunicaciones.

También se tiene un “*cuarto de equipos*” dentro del área de Informática donde están principalmente el *switch* de *core*, los servidores y los *firewalls*, a este lugar se lo mencionará en adelante como Sala de Servidores.

Dentro del área de Telecomunicaciones, en el Centro de Gestión se tiene además otro “*cuarto de equipos*”, donde se encuentran dispositivos para las conexiones con los clientes de TRANSELECTRIC S.A. que no corresponden a la red LAN, por ello no se los detallará. En este cuarto se encuentra el *router* de *Internet* de la Compañía (Cisco 871), el cual se conecta al *router* de TRANSNEXA (Cisco 7613), siendo esta última la empresa portadora. En este proyecto solo se llegará hasta la conexión con el *router* Cisco 871 para la salida a *Internet*.

Se debe indicar que en el edificio no se respeta ninguna planificación, normativas ni leyes de cableado estructurado ya que se combinan en un mismo “*cuarto*” varios ambientes (cuarto de telecomunicaciones y cuarto de equipos), se tiene un sistema cableado categoría tipo 5e y 6, entre otros.

#### **2.2.1.1 Cuarto de Telecomunicaciones**

El cuarto de telecomunicaciones del quinto piso consta de 3 *racks* denominados A, B y C. En el *rack* A están ubicados uno de los *switches* de distribución (Cisco 3500) y 4 *switches* de acceso de marcas Cisco y 3Com; a estos últimos se encuentran conectados los puntos de red de los usuarios de las diferentes áreas del edificio, que principalmente van desde la planta baja hasta el quinto piso, ya que algunos puntos van directamente al noveno piso.

En el B están los *patch pannels* de voz y datos y en el C los equipos de

comunicación para voz tales como un autocontestador, bases celulares, etc. Esto se puede ver en la figura 2.3.

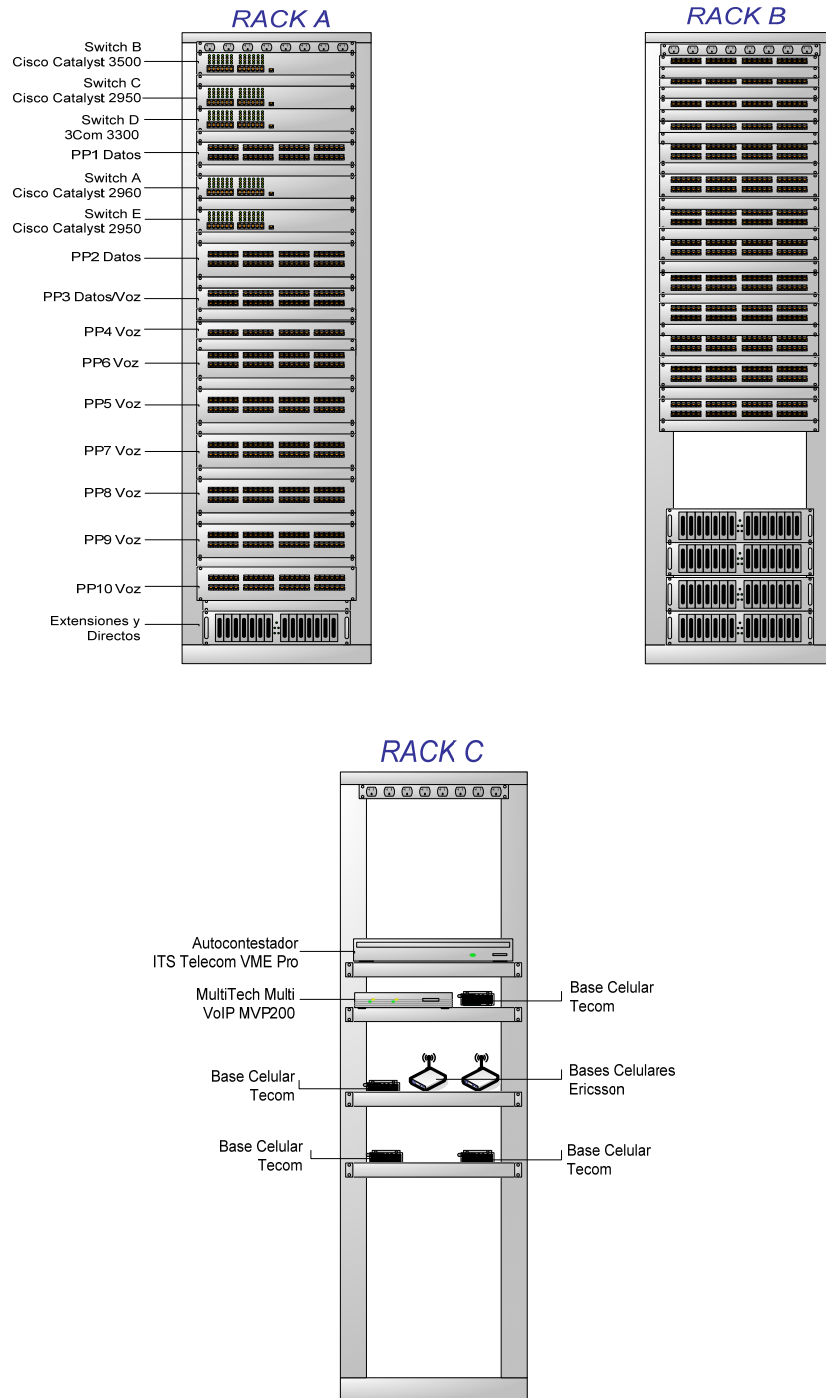


Figura 2.3 Cuarto de Telecomunicaciones Piso 5

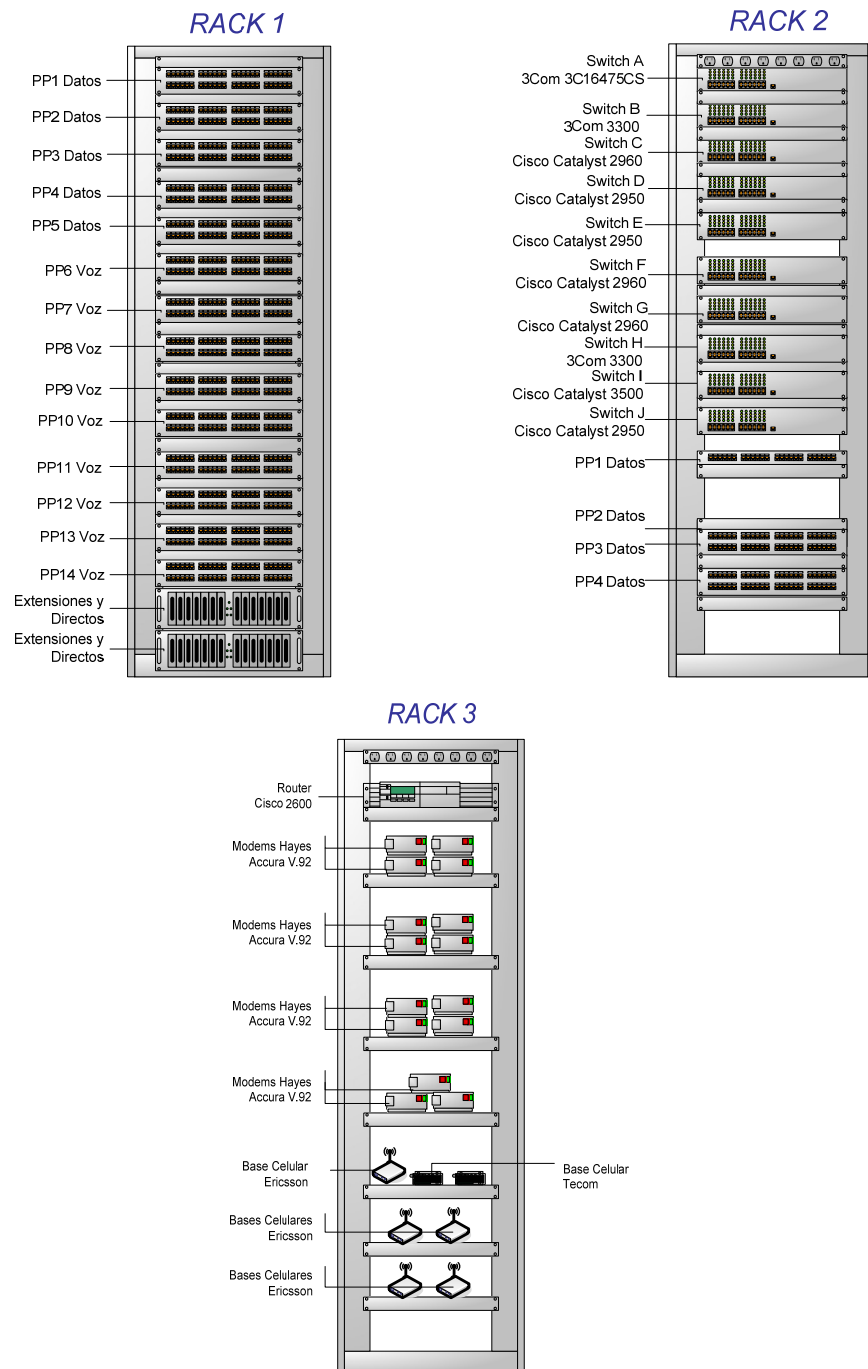


Figura 2.4 Cuarto de Telecomunicaciones Piso 9

El cuarto de telecomunicaciones del noveno piso contiene 3 *racks*. En el primero están los *patch pannels* de voz y datos, en el segundo se encuentra el otro *switch* de distribución (Cisco 3500) y 9 *switches* de acceso de marcas Cisco y 3Com, y en el tercero están un *router* Cisco 2600, las bases celulares y *modems*.



A los *switches* de acceso de este cuarto se conectan los puntos desde el sexto hasta el décimo piso, pero de igual manera como en el quinto, existen conexiones que llegan desde pisos inferiores. Los *racks* de este cuarto se pueden ver en la figura 2.4.

Es importante mencionar que no se tiene una organización ni documentación en los puntos y conexiones, por lo que si se daña alguno, se toma otro punto que esté libre sin importar su ubicación.

El *router* Cisco 2600, ubicado en uno de los *racks* del noveno piso, permite ingresar a la red de TRANSELECTRIC desde el exterior; fue adquirido antes de tener enlaces con fibra óptica, funciona con conexión *Dial-up*. Esto se lo hace mediante *modems* que están acoplados en la parte posterior del *router* y el acceso se encuentra protegido mediante usuario y contraseña.

Los cuartos de telecomunicaciones cuentan con aire acondicionado que mantiene la temperatura apropiada para no tener problemas en el funcionamiento de los equipos. Están conectados al sistema de energía de emergencia de servidores y otros equipos críticos. El sistema cuenta en su mayoría con UPSs permitiendo la operación prolongada de los equipos de red, servidores y estaciones de trabajo, en caso de interrupción de la energía eléctrica comercial.

Se debe indicar que recientemente la Compañía ha comenzado con la política de reordenar y estandarizar su red; por ello se comenzó a crear cuartos de telecomunicaciones exclusivos en algunos pisos, tal es el caso de PBB, 2A, 2B, 3A, 5B y 10B. No es un ambiente exclusivo, sino que consiste de un *rack* de pared al que llega el sistema de cableado horizontal para posteriormente enlazarse a los *switches* Cisco 3500 del quinto o del noveno piso.

#### **2.2.1.2 Sala de Servidores**

En esta sala existen 3 gabinetes de servidores, dos son marca HP y uno APC. Además están 2 *racks* de comunicación de uso general, en uno se encuentran los equipos de la red LAN y en el otro los de las redes de los segmentos DMZ.

Las figuras 2.5 y 2.6 muestran un esquema de los gabinetes de servidores y *racks* de comunicación de los equipos de esta sala.

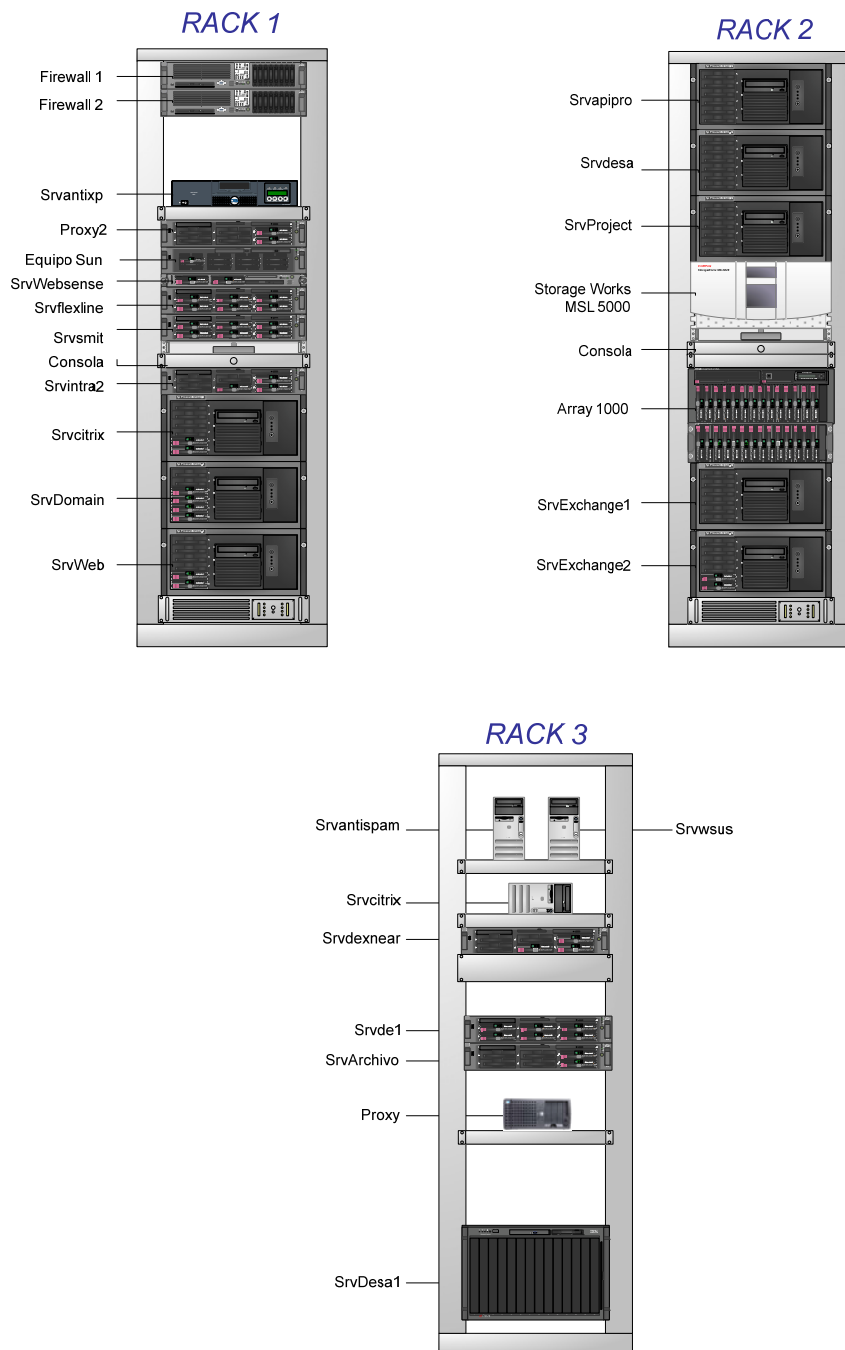


Figura 2.5 Gabinetes de servidores de la sala de servidores piso 5

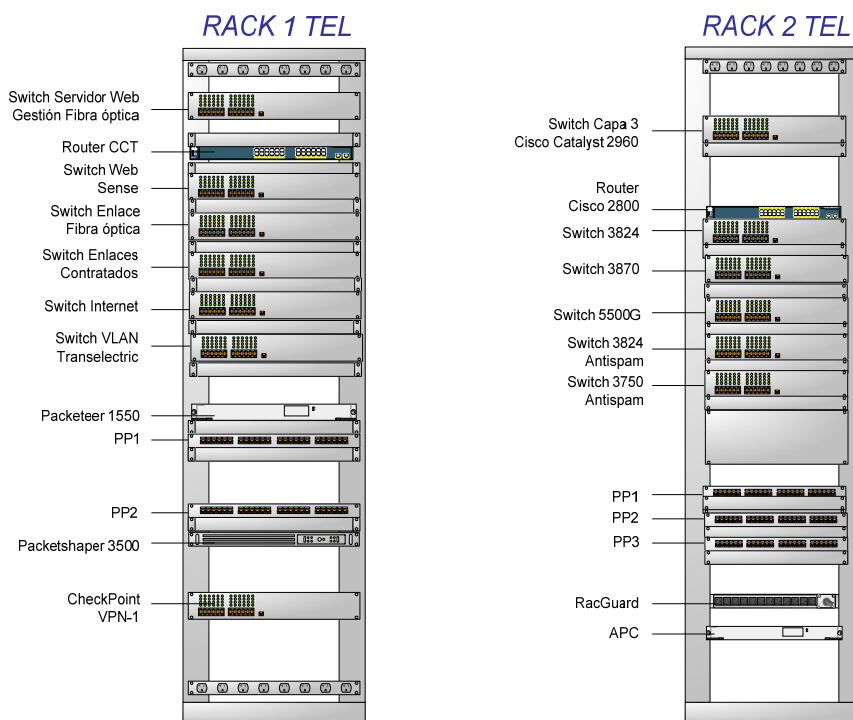


Figura 2.6 Racks de comunicaciones de la sala de servidores piso 5

Entre los principales elementos que se encuentran en esta sala se tienen: 20 servidores aproximadamente que ayudan para el correcto funcionamiento de las aplicaciones que maneja TRANSELECTRIC S.A., el *switch* de core 3Com 5500G-EI, el *Check Point firewall* con una configuración de alta disponibilidad por medio de 2 servidores en *cluster*; y, varios *switches* que permiten la conexión entre los servidores y otros equipos con *switch* de core.

Al igual que los cuartos de telecomunicaciones tiene un conjunto de climatización (aire acondicionado) que proporciona un ambiente controlado de humedad y temperatura requeridas.

### 2.2.1.3 Puntos de Red

Mediante el analizador de cables de *Fluke Network Cable Analyzer*, se realizó una verificación y certificación de los puntos de red existentes en el edificio; así se pudo comprobar distancias, atenuación, *next*, *next*, mapa de cableado y otras características de los cables utilizados en las conexiones.

**9b6d - Bloc de notas**

Archivo Edición Formato Ver Ayuda

Cable: 9850 Sumario de Pruebas: PASA  
 TRANSELECTRIC S.A. PASO LIBRE: 8.4 dB (NEXT 12-36)  
 LUGAR: QUITO-ECUADOR Fecha / Hora: 01/07/2008 12:35:19  
 OPERADOR: ANITA ZURITA Estand. Pruebas: TIA cat 5e Channel  
 Version de Estándares: 5.0 Tipo de cable: UTP 100 ohm cat 5e  
 Version de Software: 1.9 FLUKE DSP-4300 N/S: 8180001 LIA013  
 NVP: 69.0% UMBRAL DE ANOMALIA DE FALLO: 15% FLUKE DSP-4300SR N/S: 8180001 LIA012  
 PRUEBA DEL APANTALLAMIENTO: N/A

Mapa de Cableado PASA Result. TERM. RJ45: 1 2 3 4 5 6 7 8 A  
 1 2 3 4 5 6 7 8

Par	Longitud (m)	Limite (dB)	tiempo de Prop. (dB)	Diferenc. Retardo (dB)	Resistencia ohm. Limite	Impedancia ohm. Limite	Anom.	Atenuación Result. (dB)	Frec. (MHz)	Limite (dB)
12	25.3	100.0	144.555	3	50			6.3	100.0	24.0
36	29.4	100.0	142.555	1	50			6.3	100.0	24.0
45	30.0	100.0	144.555	4	50			6.3	100.0	24.0
78	29.2	100.0	141.555	0	50			6.3	100.0	24.0

Resultados Principales

Par	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Valor Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	
RL	21.8	31.6	15.1	21.2	80.2	10.9	22.8	31.4	15.1	19.9
36	15.1	98.8	10.1	15.1	98.8	10.1	15.1	82.6	10.8	16.1
45	24.3	23.6	16.3	24.3	23.6	16.3	27.7	22.9	16.5	23.8
78	32.9	31.3	15.1	19.8	100.0	10.0	38.8	80.4	10.9	18.8

Resultados del Remoto

Par	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Valor Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	
RL	21.8	31.6	15.1	21.2	80.2	10.9	22.8	31.4	15.1	19.9
36	15.1	98.8	10.1	15.1	98.8	10.1	15.1	82.6	10.8	16.1
45	24.3	23.6	16.3	24.3	23.6	16.3	27.7	22.9	16.5	23.8
78	32.9	31.3	15.1	19.8	100.0	10.0	38.8	80.4	10.9	18.8

Figura 2.7.a Resultados de Fluke cuando un cable pasa las pruebas

**6b11d - Bloc de notas**

Archivo Edición Formato Ver Ayuda

Cable: 6B11D Sumario de Pruebas: FALLO  
 TRANSELECTRIC S.A. PASO LIBRE: 1.2 dB (NEXT 36-45)  
 LUGAR: QUITO-ECUADOR Fecha / Hora: 02/07/2008 09:52:59  
 OPERADOR: ANITA ZURITA Estand. Pruebas: TIA cat 5e Channel  
 Version de Estándares: 5.0 Tipo de cable: UTP 100 ohm cat 5e  
 Version de Software: 1.9 FLUKE DSP-4300 N/S: 8180001 LIA013  
 NVP: 69.0% UMBRAL DE ANOMALIA DE FALLO: 15% FLUKE DSP-4300SR N/S: 8180001 LIA012  
 PRUEBA DEL APANTALLAMIENTO: N/A

Mapa de Cableado FALLO Result. TERM. RJ45: 1 2 3 4 5 6 7 8 A  
 1 2 3 4 5 6 7 8

Par	Longitud (m)	Limite (dB)	tiempo de Prop. (dB)	Diferenc. Retardo (dB)	Resistencia ohm. Limite	Impedancia ohm. Limite	Anom.	Atenuación Result. (dB)	Frec. (MHz)	Limite (dB)
12	45.1	100.0	218.555	194F50				9.4	100.0	24.0
36	44.3	100.0	214.555	190F50				9.6	100.0	24.0
45	5.0	100.0	24.555	0	50			1.8	100.0	24.0
78	43.9	100.0	212.555	188F50				9.2	100.0	24.0

Resultados Principales

Par	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Valor Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	
RL FALLO	22.4	55.2	14.6	20.6	71.0	11.5	23.3	19.1	17.0	18.9
36	15.1	98.8	10.1	15.1	98.8	10.1	17.1	99.6	10.0	17.1
45	2.2	1.2	17.0	2.2	1.2	17.0	3.9	1.0	17.0	3.9
78	26.0	12.9	17.0	1.8	94.8	10.3	21.7	27.8	15.6	19.9

Resultados del Remoto

Par	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Valor Result. (dB)	Frec. (MHz)	Limite (dB)	Peor Margen Result. (dB)	Frec. (MHz)	Limite (dB)	
RL FALLO	22.4	55.2	14.6	20.6	71.0	11.5	23.3	19.1	17.0	18.9
36	15.1	98.8	10.1	15.1	98.8	10.1	17.1	99.6	10.0	17.1
45	2.2	1.2	17.0	2.2	1.2	17.0	3.9	1.0	17.0	3.9
78	26.0	12.9	17.0	1.8	94.8	10.3	21.7	27.8	15.6	19.9

Figura 2.7.b Resultados de Fluke cuando un cable falla

En las figuras 2.7a y 2.7b se puede ver un ejemplo de cómo se muestran los resultados en la herramienta *Fluke* en un cable que pasa las pruebas señaladas y en uno que no pasa. La información se la pudo obtener mediante conexión serial del equipo al computador con *Hyper Terminal*.

Con el procedimiento realizado se pudo verificar que los materiales y elementos utilizados en el sistema de cableado son categoría 5 y 5e, cumplen con la norma 568B y no exceden los 90 metros en cableado horizontal.

Los trabajos de instalación de cables fueron realizados en distintas ocasiones por lo que no se tiene un ordenamiento secuencial de los puntos de red. Además, se pudo observar que existen puntos de red que se conectan directamente a los equipos sin pasar por los cajetines de pared, es decir, cables que bajan directamente desde el techo al computador.

#### 2.2.1.3.1 Contabilización de Puntos de Voz y Datos y su Distribución

<b>Puntos de Voz y Datos</b>			
<b>Piso</b>	<b>Ala</b>	<b>Voz</b>	<b>Datos</b>
Planta Baja	A	14	11
	B	22	40
Segundo	A	31	32
	B	23	24
Tercero	A	29	29
	B	26	26
Cuarto	A	-	-
	B	13	13
Quinto	A	23	29
	B	22	37
Sexto	A	32	27
	B	27	27
Séptimo	A	-	-
	B	24	21
Octavo	A	19	19
	B	19	19
Noveno	A	37	27
	B	29	25
Décimo	A	21	22
	B	21	17
	<b>TOTAL</b>	<b>432</b>	<b>445</b>

Tabla 2.1 Puntos de voz y datos del edificio

Se contabilizaron los puntos existentes en cada ala, ya sean conectados a los *racks* de los cuartos de telecomunicaciones y los que poseen conexión directa a *switches* propios. Cabe indicar que existen puntos etiquetados como voz pero están conectados a datos. En la Tabla 2.1 se presenta el resumen de los puntos de voz y datos del edificio.

No se tiene datos de las alas A de los pisos cuarto y séptimo porque en el primero está el personal de TERMOPICHINCHA y el otro está en remodelación actualmente.

#### 2.2.1.3.2 Muestreo de Puntos Existentes de Datos

Se realizó un muestreo en cada ala de cada piso para conocer de una manera aproximada la distribución actual de puntos y su funcionamiento.

Piso	Ala	# puntos	Pasan el análisis	No pasan el análisis	Observaciones
PB	A	11	11	-	
	B	40	40	-	<i>switch</i> propio
2	A	32	32	-	<i>switch</i> propio
	B	24	24	-	<i>switch</i> propio
3	A	29	29	-	<i>switch</i> propio
	B	26	26	-	
4	A	-	TERMOPICHINCHA		
	B	13	11	2	
5	A	29	26	3	
	B	37	37	-	<i>switch</i> propio
6	A	27	27	-	
	B	27	24	3	
7	A	-	REMODELACIÓN		
	B	21	20	1	
8	A	19	19	-	
	B	19	17	2	
9	A	27	27	-	
	B	25	25	-	
10	A	22	22	-	
	B	17	17	-	<i>switch</i> propio

Tabla 2.2 Funcionamiento actual de los puntos de datos

La tabla 2.2 muestra los puntos medidos con el analizador de cables donde se verificó los que están funcionando correctamente, es decir, los que respondieron en ambos extremos del cable y los que no presentaron resultados positivos por cortes en alguna parte del cable.

#### **2.2.1.4 Cableado Horizontal**

Con las pruebas realizadas en la medición de distancias de los cables, se pudo conocer que los que tienen conexión en el *switch* de ala poseen longitudes entre 13 y 30 metros, desde el *switch* hasta las salidas de telecomunicaciones (cajetines) en el *stand* de cada usuario de la red; por ello se tomará estas distancias como una referencia de cableado horizontal.

Actualmente, desde los *switches* de ala al cuarto de telecomunicaciones, la distancia difiere según la ubicación del mismo, siendo para PBB, 2A, 2B, 3A y 5B 8 metros y para 10B 10 metros.

No existe un etiquetado en todos los cajetines de los usuarios ni en el lado de los *patch pannels*, por lo que si existiera algún problema el proceso de reparación éste sería más demorado.

#### **2.2.1.5 Cableado Vertical**

Para este cableado se considera una altura de piso de 3 metros y una distancia referencial promedio de 8 metros desde la ubicación de los *switches* de ala al centro del edificio de ese piso. En este tramo se utiliza cable UTP categoría 5e. Desde la sala de servidores (5B) y desde 10B al 9no piso se tiene cable UTP categoría 6.

Las Tablas 2.3a y 2.3b presentan el rango de distancias totales del cable UTP desde las salidas de telecomunicaciones o desde los *switches* de ala, según sea el caso, a los *switches* en los cuartos de telecomunicaciones de los pisos 5 y 9. Estos rangos fueron medidos con la herramienta de *Fluke Networks* antes mencionada. Se debe indicar que en casi todos los puntos se usan cables de longitudes mayores a las necesarias.

Piso	Rango de distancias al piso 5 en metros		Piso	Rango de distancias al piso 9 en metros	
PB	A) 33-50	B) 20	PB	A) 45-62	B) 32
2	A) 17	B) 17	2	A) 29	B) 29
3	A) 14	B) 27-44	3	A) 26	B) 39-56
4	A) 24-41	B) 24-41	4	A) 36-53	B) 36-53
5	A) 21-38	B) 8	5	A) 33-50	B) 20
6	A) 24-41	B) 24-41	6	A) 30-47	B) 30-47
7	A) 27-44	B) 27-44	7	A) 27-44	B) 27-44
8	A) 30-47	B) 30-47	8	A) 24-41	B) 24-41
9	A) 33-50	B) 33-50	9	A) 21-38	B) 21-38
10	A) 36-53	B) 25	10	A) 24-41	B) 13

Tablas 2.3a y 2.3b Distancias de los diferentes pisos a cuartos de telecomunicaciones de pisos 5 y 9

### 2.2.1.6 Utilización y Características de los *Patch Pannels*

#### 2.2.1.6.1 *Patch Pannel de Datos (24 ó 48 Puertos)*

Cumple con los estándares mínimos TIA/EIA-568-B de Categoría 5e e ISO 11801. Cada puerto contiene una etiqueta universal codificada para esquemas de cableado T568A y T568B, puede ser instalado en un *rack* estándar de 19". Tiene áreas para identificación de puertos (Figura 2.8).



Figura 2.8 *Patch Pannel* de 48 puertos<sup>[2]</sup>

#### 2.2.1.6.2 *Patch Pannel de Voz (24 Puertos)*

Formado por conectores hembra, con 24 puertos para conectores RJ45 ó RJ11. Permite el uso de cable multipar de 25 pares para equipos de voz. Tiene áreas disponibles para identificación de puertos (Figura 2.9).



Figura 2.9 *Patch Pannel* de 24 puertos<sup>[2]</sup>



## 2.2.2 ANÁLISIS DE INFRAESTRUCTURA DE RED

### 2.2.2.1 Red LAN

#### 2.2.2.1.1 Generalidades

##### a. Edificio Matriz

En el edificio matriz de TRANSELECTRIC se interconecta toda la red LAN a través de sus dos cuartos de telecomunicaciones y de la sala de servidores. En la figura 2.10 se puede observar que los *switches* de acceso de los usuarios se conectan a los Cisco 3500 de cada cuarto de telecomunicaciones y éstos al 3Com 5500G-EI, el cual se encuentra en la sala de servidores. Este *switch* concentra la conexión y distribuye el tráfico hacia los diferentes segmentos especificados en cada una de las interfaces del *firewall*, que se detallarán más adelante, para la salida del tráfico al exterior o hacia el segmento interno de servidores y/o *switches* de acceso cuando se tiene tráfico interno.

Desde el *switch* 3Com 5500 de capa 3, se tiene la conexión al *firewall* de marca Check Point y a través de éste al equipo *PacketShaper* el cual se encarga de la administración del ancho de banda. Este último equipo se comunica con el *router* Cisco 871 para la salida a *Internet* a través del *router* de TRANSNEXA.

Los *switches* de acceso y de distribución se encuentran en los cuartos de telecomunicaciones del quinto y noveno piso, el *router* de *Internet* de TRANSELECTRIC y el de TRANSNEXA están el Centro de Gestión de Telecomunicaciones. Los *switches* que sirven para la comunicación a las redes WAN de Fibra Óptica y de Enlaces Contratados, al igual que el de la DMZ y el de la red de servidores, incluyendo a los servidores se encuentran en la sala de servidores dentro del área de Informática.

Se tienen dos *firewalls*, uno de ellos se lo utiliza para disponibilidad en caso de que el otro falle. Las diferentes interfaces del *firewall* van a las redes WAN, LAN, VPN, etc, como se explicará más adelante<sup>16</sup>. Como se ha visto, se tiene redundancia en cuanto a equipos tales como *firewalls* y enlaces hacia los mismos,

---

<sup>16</sup> Referirse al numeral 2.2.2.1.2 de este capítulo

pero solo uno de los enlaces está activo a la vez.

Estos *firewalls* están conectados a los diversos segmentos de red a partir de *switches* en cada una de sus interfaces. A su vez una de las interfaces del *firewall* así como su correspondiente en el otro *firewall* están conectadas entre sí para proveer redundancia.

El *router* Cisco 871 tiene las direcciones 208.19.64.66/26 como principal y 190.90.187.129/29 como secundaria. Las interfaces de este equipo tienen la siguiente disposición: eth0 hacia el *firewall* y posteriormente al resto del edificio, eth1 está libre, eth2 tiene una conexión directa hacia el centro de gestión de telecomunicaciones a una computadora para pruebas de tal forma que no se tiene restricciones de páginas visitadas en el *Internet*, eth3 está libre y por último se tiene la interfaz WAN hacia el *router* de TRANSNEXA.

En la figura 2.10 se pueden ver las conexiones de la red LAN, descritas en esta sección. Se tienen algunos datos de las direcciones para cada red pero no en su totalidad, debido a la falta de información y organización existente en la administración de esta red.

Otros elementos importantes que cabe mencionar son los administradores de ancho de banda tales como *PacketShaper* 3500 y *Packeteer* 1550. Estas herramientas se utilizan no solo para la administración y asignación del ancho de banda en el edificio matriz, sino a través del *software* que posee se realiza la monitorización de la red, principalmente el acceso a *Internet*.

La red de servidores está conectada a un *switch* (Cisco 2960) y éste directamente al *switch* de *core*. El servidor *web* y los servidores *proxy* están dentro de la DMZ en uno de los brazos del *firewall*.

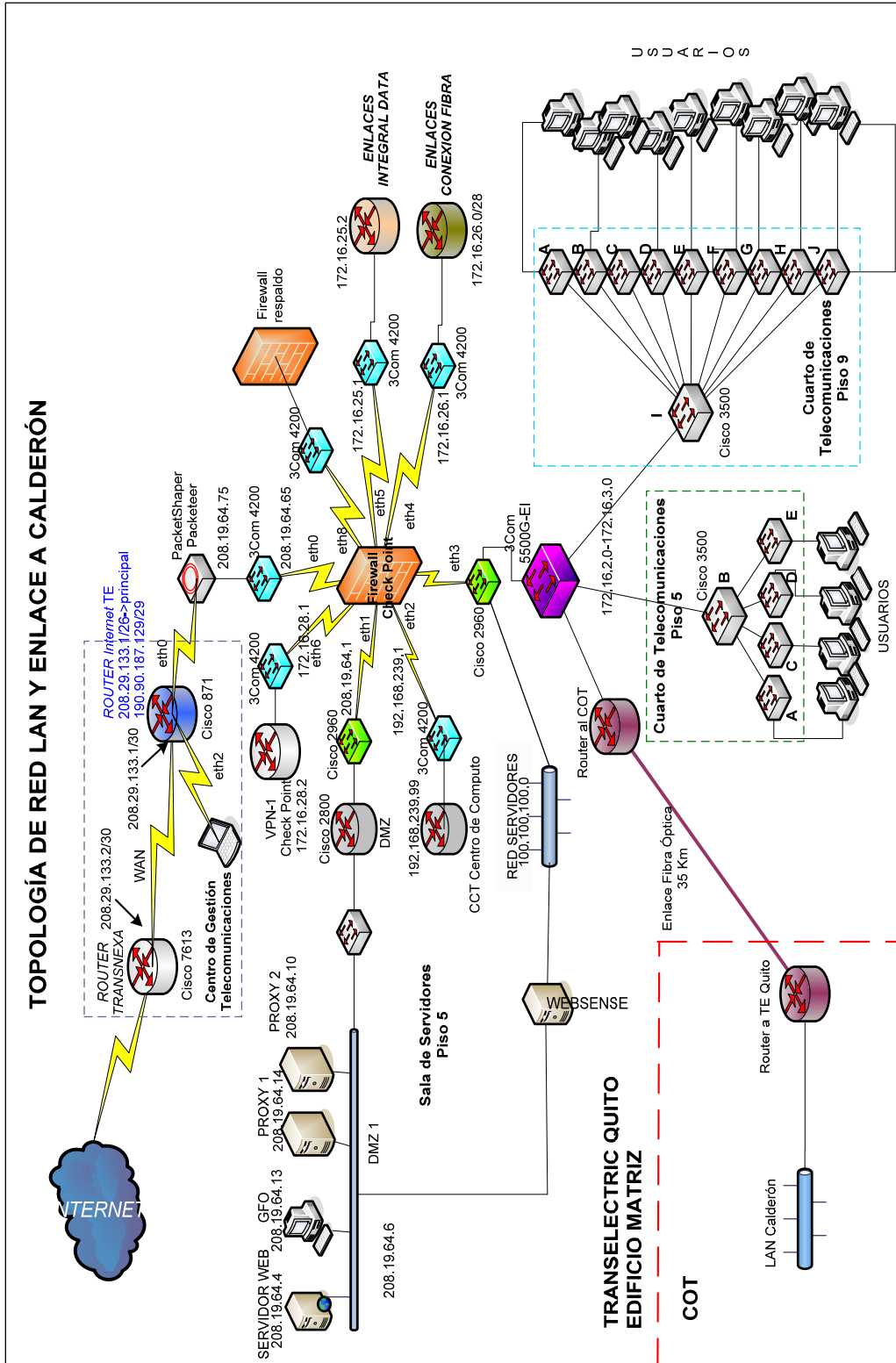


Figura 2.10 Red LAN

En dominios y direcciones IP, TRANSELECTRIC tiene como dominio de *Internet transelectric.com.ec* y como dominio interno *transelectric.com*. El esquema de direccionamiento IP está dividido de la siguiente manera:

- ✓ Para servidores la red 100.100.100.0/24 y unas pocas direcciones dentro del *pull* de la red 172.16.2.0/23 de donde están reservadas las 40 primeras direcciones para servidores y usuarios privilegiados. *Mail* y *Citrix* son traducidos a direcciones públicas a través de NAT.
- ✓ Para la red LAN en el edificio matriz la red 172.16.2.0/23 a partir de la dirección 41.

Los computadores se encuentran con una configuración dinámica de IP en donde el DHCP asigna las direcciones desde la 172.16.2.41 hasta la 172.16.3.254. Además se tienen otros *pull* de direcciones del DHCP para las impresoras, *wireless* y para RAS (*Remote Access System*).

No se tiene una documentación precisa de cuáles son los rangos de los *pulls* de direcciones, solo que están entre la 172.16.2.41 hasta 172.16.3.254, lo que hace más complicado su entendimiento y organización.

*b. Instalaciones en el Centro de Operaciones en Calderón*

La red del COT se interconecta a toda la red del edificio matriz a través de un enlace WAN de Fibra Óptica con una distancia total de 35 kilómetros por medio del protocolo HDLC (*High Level Data Link Control*). Para realizar este enlace se pasa previamente por las subestaciones de Vicentina y Pomasqui.

La red LAN de Calderón es nueva, por lo tanto, está diseñada en base a criterios y estudios de voz y datos, cumpliendo con las normas y estándares actuales por lo que no es incluida en este Proyecto de Titulación.

El enlace hacia estas instalaciones se puede ver también en la figura 2.10

### 2.2.2.1.2 Elementos de la Red

#### a. Switches

Los diferentes *switches* de los cuartos de telecomunicaciones concentran toda la red del edificio matriz de TRANSELECTRIC S.A. Esta red tiene un esquema a nivel de capas por ello se utilizan *switches* de acceso, distribución y de *core*.

Entre los *switches* de acceso están los Cisco Catalyst 2900, 2950 y 2960, 3Com SuperStack II 3300 y SuperStack 3 3300 y D-LINK DES que se encuentran dentro de los cuartos de telecomunicaciones o en las alas de algunos pisos que tienen *switches* propios.

Existen también dos Cisco Catalyst 3500 que funcionan como *switches* de distribución, uno en cada cuarto de telecomunicaciones y éstos concentran a todos los *switches* de acceso. Finalmente, hay un 3Com SuperStack 4 5500G-EI como *switch* de *core* por el que se logra la comunicación al *firewall* y con ello a las diferentes interfaces del mismo.

En la sala de servidores se tienen *switches* Cisco Catalyst 2960, 3Com SuperStack 3 4200 y 3Com OfficeConnect 8 con *Gigabit Uplink* conectados a la salida de las interfaces del *firewall*.

Además existen diferentes *switches* que ayudan en la conexión de los servidores, así se tienen dos *switches* 3Com 3824 para los servidores de antivirus, *Websense* y *antispam*, un Cisco Catalyst 3750 al que también se conecta el *antispam* y un 3Com 3870 el cual se encuentra vacío.

Algunos de estos *switches* únicamente tienen conectados dos o tres de sus interfaces, por ello se debería utilizarlos de manera más eficiente sin desperdiciar recursos.

En la figura 2.6 se pueden ver los *switches* mencionados, mismos que se encuentran en los *racks* de la sala de servidores.

Tampoco existe información documentada de a cuáles de los *switches* están conectados cada servidor, ni qué puertos están siendo utilizados; las referencias que se han podido presentar se las ha obtenido a simple vista, a pesar de que esta área posee restricción de ingreso.

La Figura 2.11 muestra los *switches* existentes de la marca Cisco Systems.

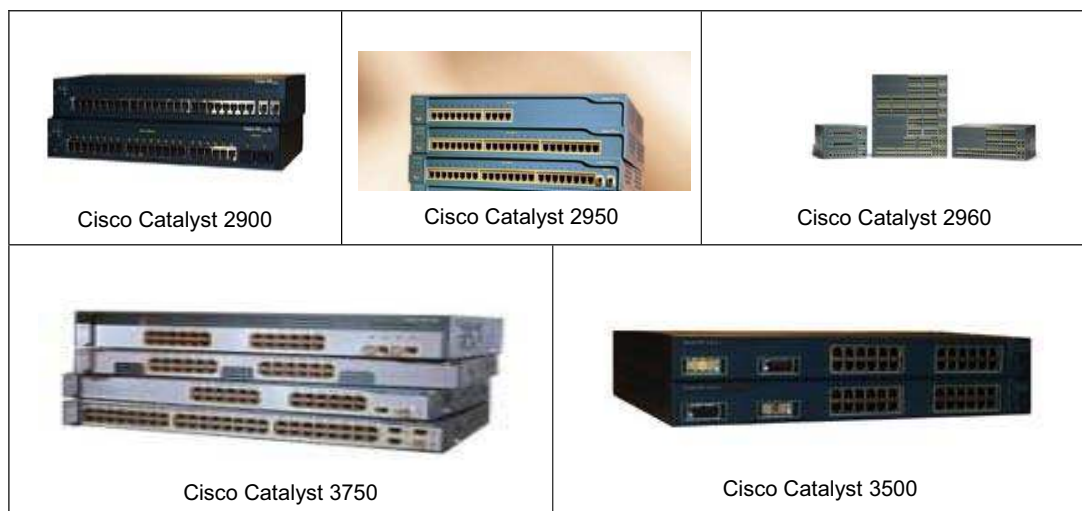


Figura 2.11 *Switches* Cisco Systems<sup>[3]</sup>

Como reseña se puede indicar que la familia Catalyst de Cisco<sup>17</sup> es una línea de *switches* de alto rendimiento diseñados para migrar de forma sencilla de las redes LAN compartidas tradicionales a redes completamente conmutadas.

Ofrecen rendimiento, administración y escalabilidad, se puede encontrar equipos *Ethernet*, *Fast Ethernet* y con opciones modulares las cuales permiten adaptarlos a las necesidades de la Compañía.

En la tabla 2.4 se especifica la distribución de los *switches* presentes en el edificio matriz de TRANSELECTRIC S.A.

<sup>17</sup> Tomado de las características ofrecidas por el fabricante Cisco

DISTRIBUCIÓN DE LOS SWITCHES DEL EDIFICIO MATRIZ DE TRANSELECTRIC S.A					
CANTIDAD	UBICACIÓN	MARCA	MODELO	NÚMERO Y TIPO DE PUERTOS	IDENTIFICADOR
1	10mo piso	D-Link	DES 1024R	SWITCH 24 PUERTOS	
1	9no piso Rack	CISCO	Catalyst 3500 Series XL	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	I
2	9no piso Rack	CISCO	Catalyst 2950-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps	A, G
1	9no piso Rack	CISCO	Catalyst 2950SX-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS 1000BASE-SX	F
1	9no piso Rack	CISCO	Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	H
2	9no piso Rack	CISCO	Catalyst 2960 Series SI	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	D, E
2	9no piso Rack	3Com	SuperStack II Switch 3300 3C16980	SWITCH 24 PUERTOS 10/100 Mbps	B, C
1	9no piso Rack	3Com	SuperStack II 3300 XM 3C16985	SWITCH 24 PUERTOS 10/100 Mbps	J
1	5to piso Rack	CISCO	Catalyst 3500 Series XL	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	B
1	5to piso Rack	CISCO	Catalyst 2950-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	C
1	5to piso Rack	CISCO	Catalyst 2950SX-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS 1000BASE-SX	E
1	5to piso Rack	CISCO	Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	A
1	5to piso Rack	3Com	SuperStack 3 Switch 3300 3C16980A	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	D
2	5to piso Inform.	CISCO	Catalyst 2950	SWITCH 24 PUERTOS 10/100 Mbps	
1	5to piso Inform.	3Com	SuperStack 4 Switch 5500G-EI	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	
2	5to piso Inform.	CISCO	Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	
6	5to piso Inform.	3Com	SuperStack 3 Switch 4200	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	
2	5to piso Inform.	3Com	Switch 3824	SWITCH 24 PUERTOS y 4 PUERTOS SFP	
1	5to piso Inform.	3Com	Switch 3870	SWITCH 24 PUERTOS y 4 PUERTOS SFP	
1	5to piso Inform.	3Com	Switch 3750	SWITCH 24 PUERTOS y 4 PUERTOS SFP	
1	5to piso Inform.	3Com	OfficeConnect Switch 8 ports	SWITCH 8 PUERTOS con Gigabit Uplink	
1	3er piso	D-Link	DES-1016D 16-Port Desktop Switch	SWITCH 16 PUERTOS 10/100 Mbps	
1	2do piso	CISCO	Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	
1	2do piso	CISCO	Catalyst 2900 Series	SWITCH 24 PUERTOS 10/100 Mbps	
1	Planta Baja	3Com	SuperStack II Switch 3300 XM	SWITCH 24 PUERTOS 10/100 Mbps	
1	Planta Baja	CISCO	Catalyst 2950-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps	

Tabla 2.4 Distribución de Switches en el Edificio Matriz

Además, se tienen algunos *switches* marca 3Com<sup>18</sup>, entre ellos los de la familia SuperStack II que es una línea que permite conectar directamente a los usuarios de red y eliminar la competencia por acceder a ella. Son útiles cuando el tráfico de red entre estaciones y servidores es elevado, y posibilitan la implementación de aplicaciones multimedia, voz y vídeo sobre red, acceso a Internet, etc. Los *switches* 3Com existentes se pueden ver en la figura 2.12.

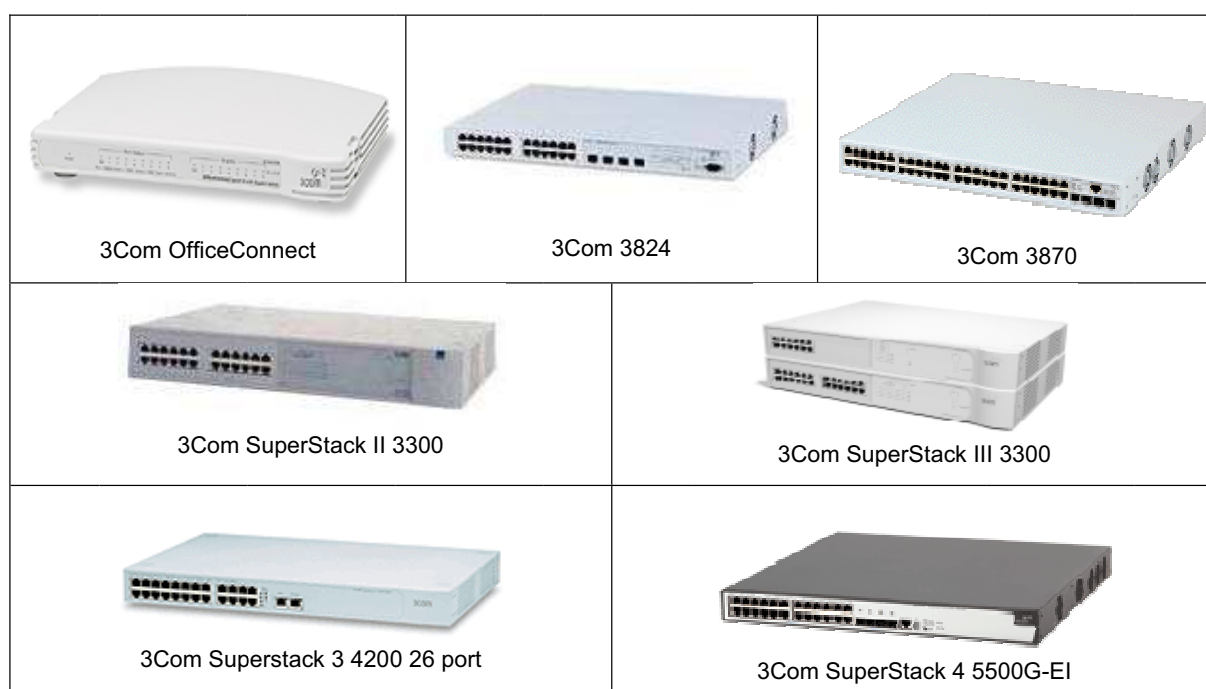


Figura 2.12 Switches 3Com<sup>[4]</sup>

Cada uno de los cuatro modelos del SuperStack 3 *Switch* 3300 (SuperStack 3 *Switch* 3300 TM/SM/XM/MM) permite una configuración simple del *hardware* y *software*. También, la aplicación *Transcend Network Supervisor* (propia de 3Com) admite ampliar las funciones de administración de red.

El *switch* 3824 10/100/1000 *Gigabit Ethernet* posee características de capa 2 y de fácil instalación; proporciona conexiones flexibles que permiten una combinación de equipos de escritorio y servidores habilitados para 10/100 Mbps y *Gigabit Ethernet*.

<sup>18</sup> Tomado de las características ofrecidas por el fabricante 3Com



Los *switches* D-Link<sup>19</sup> son diseñados para funcionar en grupos de trabajo con requerimientos de tráfico de información. Son adaptables a la estructura de montaje en bastidor y a través de sus puertos 10/100 Mbps permiten la conexión a estaciones de trabajo o servidores (Figura 2.13).



Figura 2.13 Switches D-Link<sup>[5]</sup>

#### b. Routers

En la sala de servidores se encuentra un *router* Cisco 2800 que tiene conexión al *switch* que se enlaza a la interfaz *eth1* del *firewall* correspondiente a la DMZ, tal como se pudo ver en la figura 2.10 y que se especificará más adelante cuando se detalle el *firewall*.

Los *routers*<sup>20</sup> de la serie 2800 de Cisco entregan aplicaciones concurrentes de video, voz y datos de manera segura, y su desempeño no se degrada cuando todas sus funciones están en uso. Permiten a empresas grandes y medianas desplegar soluciones de comunicaciones convergentes ofreciendo buen desempeño y protección de la inversión (Figura 2.14).

Los *routers* de servicios integrados de Cisco vienen con encriptación y una mejora en el *hardware* para VPNs. Adicionalmente posee la funcionalidad de IPS (*Intrusion Prevention System*) en línea. Se pueden añadir módulos de red adicionales para una aceleración VPN de mayor desempeño, IPS y filtración de seguridad de contenido *web*.

<sup>19</sup> Tomado de las características de *switches* ofrecidas por el fabricante D-Link

<sup>20</sup> Tomado de las características de *routers* ofrecidas por el fabricante Cisco



Figura 2.14 Router Cisco 2800 series<sup>[6]</sup>

En el cuarto de telecomunicaciones del noveno piso existe un *router* Cisco 2600 el cual permite a los usuarios que no se encuentren en el edificio acceder mediante conexión *Dial-Up* a la red de TRANSELECTRIC S.A. Éste es un *router* modular multiservicio de clase empresarial.

La serie Cisco 2600 soporta los siguientes servicios:

- ✓ Integración multiservicio de voz y datos.
- ✓ Acceso a redes privadas virtuales (VPN) con opciones de *firewall*.
- ✓ Servicios de acceso telefónico analógico y digital.
- ✓ Enrutamiento con gestión de ancho de banda.
- ✓ Enrutamiento entre VLANs.

Todos los modelos disponen de dos ranuras para tarjetas de interfaz WAN, una ranura para el módulo de red y una ranura para un módulo de integración avanzada (*MIA*); este equipo se puede ver en la figura 2.15.



Figura 2.15 Router Cisco 2600 series<sup>[7]</sup>

En el cuarto de equipos del Centro de Gestión de Telecomunicaciones se encuentra el *router* Cisco 871 el cual se conecta al *router* de TRANSNEXA y es por el cual la red de TRANSELECTRIC tiene salida a *Internet* como se puede ver en la figura 2.10.

Los *routers* de la serie Cisco 870 ejecutan servicios concurrentes que incluyen *firewall*, VPNs y *Wireless LAN*. Fueron diseñados para ser desplegados en pequeñas oficinas que serán conectadas a redes mayores, a través de conexiones de VPN seguras. (Figura 2.16).



Figura 2.16 Switch Cisco 871<sup>[8]</sup>

### c. Firewall

Se utiliza el producto CheckPoint *Firewall-1*, con una configuración de alta disponibilidad, por medio de 2 servidores en *cluster*. Estos servidores son HP DL 380 G5 con sistema operativo *Secure Platform RG65*. Tienen 10 interfaces de red, de las cuales 7 están siendo utilizadas, asignadas de la siguiente manera:

*Eth0* para *Internet*.

*Eth1* para la DMZ (*Proxy*, *websense* y gestión de fibra óptica).

*Eth2* para el CCT.

*Eth3* para la LAN de TRANSELECTRIC.

*Eth4* para las redes de fibra.

*Eth5* para las redes de cobre (*Integral Data*).

*Eth6* para las VNP's utilizando el producto VPN-1 UTM de *Check Point*.

*Eth7* está libre.

*Eth8* para la conexión al otro *firewall*.

*Eth9* está libre.

La solución de *firewall* está conformada por varios módulos: IPS *Smart Defense*, QoS, módulos de Antivirus que se encuentran deshabilitados, módulo de Reportes llamado *Eventia Reporter*, módulo de manejo de *log* denominado *Smart Tracker*.

A través del *firewall* se verifica la autenticación de los accesos de VPN.

*d. Check Point VPN-1 UTM*<sup>21</sup>

Este equipo se encuentra en la sala de servidores y permite el manejo de VPNs en la Compañía. Tiene doble autenticación, una es propia del equipo y otra es con el *firewall*, debido a que los dos son equipos de *Check Point*. Esta doble autenticación permite el acceso remoto a otras localidades usando VPNs sin poner en riesgo la seguridad.

Al entregar tecnologías de *firewall*, VPN, prevención de intrusos y antivirus de *Check Point* en una sola solución, VPN-1 UTM *Edge* permite que los sitios remotos permanezcan tan seguros como el sitio corporativo.

Para simplificar la administración de seguridad en la instalación de sitios remotos grandes, los dispositivos VPN-1 UTM *Edge* pueden administrarse de forma centralizada junto con otras soluciones de seguridad de *Check Point* (Figura 2.17).



Figura 2.17 *Check Point VPN-1 UTM Edge*<sup>[9]</sup>

*e. PacketShaper*<sup>22</sup>

En la sala de servidores se encuentran dos equipos de *Packeteer*, un *PacketShaper* 3500 y un *Packeteer* 1500. El equipo que se encuentra en funcionamiento es el

<sup>21</sup> Referirse al anexo 2.1

<sup>22</sup> Referirse al anexo 2.2

*PacketShaper* 3500 y permite la administración del ancho de banda de la red (Figura 2.18).

Este equipo está conectado por un extremo a una de las interfaces del *firewall* y por el otro al *router* 871 para la salida a *Internet*. Ayuda en el rendimiento de las aplicaciones a través de *Internet* ya que el correo electrónico y las descargas *peer to peer* compiten por los recursos y pueden afectar al rendimiento de aplicaciones críticas.

Basado en la inteligencia a nivel de aplicación de *Packeteer*, *PacketShaper* supervisa, controla y acelera el tráfico en la red, proporcionando así una elevada calidad de servicio a las aplicaciones críticas, permitiendo el alineamiento de los recursos de red de una organización con sus necesidades.

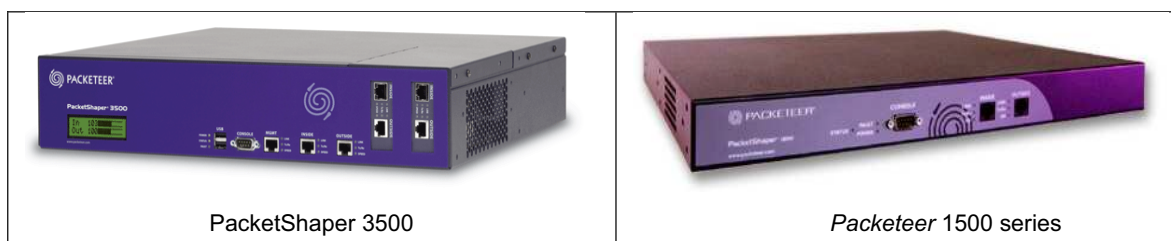


Figura 2.18 *PacketShaper*<sup>[10]</sup>

#### *f. Servidores*

Se disponen de varios servidores ubicados en los diferentes *racks* de la sala de servidores. Existen equipos que son soporte de algunos servidores para proveer de una máxima disponibilidad en los servicios. En la tabla 2.5 se muestran los servidores existentes en la red.

SERVIDOR	MARCA	MODELO	SISTEMA OPERATIVO	PARCHES	PROCESADOR	IP
firewall1	HP	Proliant DL 380 G5	Secure Plataform		Intel Xeon E5320 , 1.86 Ghz.	100.100.100.252
firewall2	HP	Proliant DL 380 G5	Secure Plataform		Intel Xeon E5320 , 1.86 Ghz.	100.100.100.251
Srvantixp	DELL	CPU	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2	Intel(R) Pentium(R) 4 CPU 2.40GHz	100.100.100.127
proxy2	HP	Proliant DL 380 G4	Linux		Intel(R) Xeon(TM) CPU 3.40GHz	208.19.64.10
srvwebsense	HP	Proliant DL 360	Microsoft(R) Windows(R) Server 2003, Standard Edition		Intel(R) Xeon(TM) CPU 3.60GHz	172.16.2.2
Srvflexline	HP	Proliant DL 380 G4	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP1	Intel(R) Xeon(TM) CPU 3.40GHz	100.100.100.14
Srvsmit	HP	Proliant DL 380 G4	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP1	Intel(R) Xeon(TM) CPU 3.40GHz	100.100.100.19
srvintra2	HP	Proliant DL 380 G4	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2	Intel(R) Xeon(TM) CPU 3.40GHz	100.100.100.36
Srvcitrix	HP	Proliant ML 370 G3	Microsoft(R) Windows(R) Server 2000, Standard Edition	SP4	Intel(R) Xeon(TM) CPU 3.06GHz	100.100.100.3
Srvdomain	HP	Proliant ML 370 G3	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2	Intel(R) Xeon(TM) CPU 3.20GHz	100.100.100.10
srvWeb	HP	Proliant ML 370 G3	Microsoft(R) Windows(R) Server 2003 R2, Standard Edition	SP2	Intel(R) Xeon(TM) CPU 3.20GHz	208.19.64.4
Srvapipro	HP	Proliant ML 370 G3	Microsoft Windows 2000 Server	SP4	Intel(R) Xeon(TM) CPU 3.06GHz	100.100.100.4
Srvdesa	HP	Proliant ML 370 G3	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2	Intel(R) Xeon(TM) CPU 3.20GHz	172.16.2.12
Srvproject	HP	Proliant ML 370 G3	Microsoft(R) Windows(R) Server 2003, Standard Edition		Intel(R) Xeon(TM) CPU 3.20GHz	100.100.100.5
srvexch1	HP	Proliant ML 370 G3	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	SP1	Intel(R) Xeon(TM) CPU 3.20GHz	100.100.100.16
srvexch2	HP	Proliant ML 370 G3	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	SP1	Intel(R) Xeon(TM) CPU 3.20GHz	100.100.100.15
Srvantispam	HP	Compaq	Linux		Intel(R) Pentium(R) 4 CPU 3.00GHz	100.100.101.45
Srvwsus	HP	Compaq	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2	Intel(R) Pentium(R) 4 CPU 3.00GHz	172.16.2.190.
Srvcitrixp	HP	Compaq	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP1	Intel(R) Pentium(R) 4 CPU 3.00GHz	172.16.2.10
Srvdexnear	HP	Proliant DL 380 G4	Microsoft Windows 2000 Server	SP4	Intel(R) Xeon(TM) CPU 3.40GHz	100.100.100.9
srvde1	HP	Proliant DL 380 G4	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2	Intel(R) Xeon(TM) CPU 3.40GHz	100.100.100.89
Srvarchivo	HP	Proliant DL 380 G4	Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2	Intel(R) Xeon(TM) CPU 3.40GHz	100.100.100.22
Srvarchive			Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2		100.100.100.23
Srvdigital			Microsoft(R) Windows(R) Server 2003 R2, Standard Edition	SP2		172.16.2.11
Proxy	DELL	Optiplex	Linux			208.19.64.14
Srvfsecure			Microsoft(R) Windows(R) Server 2003, Standard Edition	SP2		172.16.2.3

Tabla 2.5 Servidores<sup>[1]</sup>

*g. PCs*

En la tabla 2.6 se muestra un inventario de computadores en el edificio matriz de TRANSELECTRIC S.A. en base a su procesador.

PROCESADOR	CANTIDAD
Centrino	3
Pentium 3	2
Pentium 4	203
Pentium D	6
Pentium M	19
Centrino Duo	33
Core Duo	3
Core 2 Duo	39
Sin Especificación	20
<b>TOTAL</b>	<b>328</b>

Tabla 2.6 PC's<sup>[11]</sup>

*2.2.2.1.3 Servicios y Aplicaciones*

*a. Aplicaciones*

La Compañía maneja diferentes aplicaciones para facilitar trámites al personal como es el caso de permisos, seguro médico, y a las diferentes áreas como Tesorería, Contabilidad, Bodegas, etc.

En la Tabla 2.7 se muestran las diferentes aplicaciones que se manejan en la Compañía.

APLICACIÓN	MÓDULO	DESCRIPCIÓN
<b>Xnear CRM Workflow</b>		Herramienta para diseño de flujos de trabajo
	Solicitud de Pago	Permite el manejo del procedimiento para generar anticipo de sueldo, pago de viáticos por concepto de comisiones y pago a proveedores
	Solicitud de Almacén	Controla el procedimiento de la solicitud de suministros, materiales, bienes de operación, provisión e inversión
	Formulación Presupuestaria	Permite el registro del presupuesto anual por centro de costo o proyecto
	Control de Activos	Permite el manejo de la notificación de alta, baja y traspaso de un bien
	Plan de Compras	Permite el registro del plan inicial de compras de suministros, materiales, bienes y servicios
	Control de Contratos y Garantías	Permite controlar el manejo de los contratos y garantías firmados con los contratistas.
	Memos y Oficios	Permite generar, imprimir, archivar y mantener control y seguimiento de documentos internos y externos
	Seguro Médico	Permite el registro de reclamos, liquidaciones y co-pagos (ambulatorio y hospitalización) por concepto de seguro médico
	Reposición	Permite cancelar el valor correspondiente a ropa de trabajo personal femenino (cartera y zapatos)
	Programación Hebdomadario	Permite mantener control y seguimiento de la programación semanal del mantenimiento de las instalaciones eléctricas de TRANSELECTRIC S.A.
	OT fuera de programa	Permite mantener control y seguimiento de las órdenes de trabajo fuera de la programación del mantenimiento de las instalaciones eléctricas de TRANSELECTRIC S.A
	Programación Mensual	Permite mantener control y seguimiento de la programación semanal del mantenimiento de las instalaciones eléctricas de TRANSELECTRIC S.A
<b>Flexline ERP</b>		Sistema Integrado Administrativo Financiero
	Contabilidad	Permite el ingreso y la administración de los registros contables para proporcionar a su vez los informes necesarios para conocer la situación económica de la Compañía y aportar a la toma de decisiones
	Tesorería	Permite la administración y control de las cuentas de chequera de la Compañía
	Activo Fijo con Tenencia	Controla y administra los activos fijos con tenencia permitiendo actividades sobre ellos
	Comercial	Permite el mantenimiento del inventario y los documentos que manejan las bodegas de TRANSELECTRIC S.A
	Ventas	Facturación por transporte de energía y Servicios de Telecomunicaciones
	Presupuesto	Permite el control y análisis de la ejecución de la formulación presupuestaria
	Gestión	Permite la recolección de información para la toma de decisión gerencial

Tabla 2.7 Aplicaciones de la Compañía<sup>[11]</sup>



<b>APIPRO</b>		<b>Sistema para Gestión de Mantenimiento</b>
	Básico	Usuarios, documentación de planta (objetos de mantenimiento, mano de obra, estructura de cuentas, funciones de presupuesto, características técnicas, instrucciones de trabajo, códigos de error, causa, efecto, unidades de medida, bodegas); estructura de planta
	Mantenimiento	Control de trabajos a través de órdenes de trabajo sobre equipos, con uso y coordinación extensa de recursos
	Inspección	Monitoreo y registro de operación de equipos a través de parámetros y medidores configurables
	Control de Bodega	Inventario y control multibodega de repuestos y demás materiales. Incluye estadísticas y coordinación con trabajos de mantenimiento
	Dibujos y documentos	Permite anexar todo tipo de documentación técnica electrónica a actividades de mantenimiento y, en general, a la estructura de planta.
	Interfaz PALM	Permite la utilización de <i>Handhelds</i> tipo <i>palm</i> para registrar en sitio y <i>offline</i> la inspección y el reporte de trabajos; posteriormente esta información se integra al sistema
	Importación/exportación	Permite importar y exportar diverso tipo de información del sistema APIPRO desde y hacia archivos electrónicos. El proceso puede configurarse de manera automática.
	Report Builder	Reportador que permite extraer información de APIPRO, con facilidades de diseño para pantalla e impresión
	Compras	Gestiona órdenes de compra a proveedores, con ingreso de facturas y enlace especialmente a bodegas. Materiales que intervienen en Mantenimiento.
	Navegador Gráfico	Da una interfaz "viva" gráfica para acceder a información de APIPRO a través de planos y dibujos de equipos e instalaciones en general
<b>PROJECT SERVER</b>	<b>Project Server</b>	<b>Herramienta para Manejo Empresarial de Proyectos</b>
	Project Professional	Cliente de Project. Funcionalidad amplia para planificación, reporte y seguimiento de proyectos, con recursos materiales, económicos y humanos. Análisis de costos.
	Project Web Access	Interfaz <i>web</i> que permite realizar el seguimiento y reporte de proyectos publicados, bajo diferentes perfiles de usuario.
	Windows Share Point Services	Plataforma Microsoft para habilitar el manejo documental de MS - Project Server
<b>EVOLUTION</b>		<b>Sistema para Gestión de Personal</b>
	Recursos Humanos	Permite administrar el recurso humano de TRANSELECTRIC (capacitación, competencias, beneficios, acciones laborales, ropa de trabajo, evaluación, reclutamiento, estructura empresarial)
	Nómina	Permite administrar y ejecutar proceso de pagos de haberes al empleado (pago mensual, décimos, utilidades) y el respectivo pago de impuestos
	Administración de tiempo	Establece el calendario de trabajo del empleado; recoge los registros de asistencia del empleado y analiza esa información frente al rol de pagos
	Seguridad	Permite crea usuarios, perfiles y asignar permisos
	E-business	Permite al personal de TRANSELECTRIC S.A consultar vía <i>Internet</i> la información histórica de ficha personal, roles de pago, bienes asignados, permisos, vacaciones
	Evolution Reporter	Permite al usuario diseñar reportes personalizados acordes a sus necesidades

Tabla 2.7 Aplicaciones de la Compañía (Continuación)

APLICACIÓN	MÓDULO	DESCRIPCIÓN
<b>PORTAL WEB</b>		Portal Web de TRANSELECTRIC
	Administración de seguridad	Permite la creación de usuarios, roles y asignación de permisos a los menús, secciones y contenido del portal <i>web</i>
	Administración de contenido	Permite la actualización (añadir, eliminar, cambiar) del contenido del portal <i>web</i>
	Facturación	Permite a los clientes de TRANSELECTRIC S.A consultar en línea la facturación por mes y por año por concepto del transporte de energía
	Registro de Proveedores	Permite a las empresas naturales o jurídicas ingresar la información como proveedores de TRANSELECTRIC
<b>OTROS</b>		
	SISAFO	Sistema que maneja la información de los activos en operación (activos sin tenencia), altas, bajas, transferencias, depreciaciones
	PRESUPUESTO REFERENCIAL	Sistema para Administrar equipos del SNT y formular presupuestos referencial de obras
	SILECPRO	Sistema Integrado de Legislación Ecuatoriana
	ANEXIVA	Anexos del IVA. Toma las transacciones de egresos y liquidaciones de Contabilidad para generar información tributaria requerida por el SRI
	EVT	Registro y seguimiento de fallas y demás eventos acontecidos en el SNT de TRANSELECTRIC S.A. a través de la visualización de la consola del COT (Centro de Operaciones de TRANSELECTRIC)
	CONTRATOS	Sistema para mantener un control y seguimiento de contratos (tabla de cantidades y precios) , así como sus pagos respectivos
	CALIFICACIÓN DE PROVEEDORES	Sistema que permite calificar a los proveedores registrados a través del Portal Web de acuerdo a ciertos criterios
	INTRANET	Portal Web interno TRANSELECTRIC S.A
	SGN	Sistema para Gestión de Novedades del SNT
	HOJA DE TIEMPO	Sistema para registro de horas trabajadas en los proyectos de la Gerencia de Ingeniería y Construcción
	CARTERA DE CLIENTES	Sistema para conciliar la cartera de clientes de TRANSELECTRIC por concepto de transporte de energía y servicios de Telecomunicaciones

Tabla 2.7 Aplicaciones de la Compañía (Continuación)

### *b. Servicios*

La Compañía utiliza algunos servicios comunes tales como el *Internet*, Correo Electrónico, Servicios de Red, *Active Directory*, etc. Para cada uno de ellos posee algunas herramientas que facilitan su administración.

Para el *Internet* se tiene un Servidor *Proxy* para permitir o denegar accesos, *Web Sense* también es utilizado para configurar reglas, *firewall*, medidores de ancho de banda como el *Packet Shaper*, etc.

En la tabla 2.8 se puede ver de manera más explícita cada uno de estos servicios.

SERVICIOS	COMPONENTES	ESPECIFICACIONES
Internet	Servidor <i>Proxy</i>	Configuraciones, Rutas IP, <i>IP Tables</i> , accesos.
	<i>Web Sense</i>	Configuraciones, permisos, reglas.
	<i>Firewall</i>	Configuraciones, Reglas, Licencias, Accesos Rutas IP, Permisos Especiales.
	Ancho de Banda	QoS Rendimiento, Contingencia.
Correo Electrónico	Servidores de Correo <i>Exchange</i>	Reglas, Políticas, Buzones, <i>Service Pack</i> , actualizaciones automáticas, respaldos de configuración.
	<i>Firewall</i>	Configuraciones, Reglas Aplicables.
Antivirus	Servidores Antivirus (Bloqueo de <i>Spyware</i> , <i>Adware</i> , <i>Malware</i> )	Políticas, Configuraciones, <i>Service Pack</i> , actualizaciones, respaldos de configuraciones, manejo de equipos clientes.
	<i>Firewall</i>	Configuraciones, reglas aplicables al servicio.
	Actualizaciones	Actualizaciones
Antispam	Servidor <i>Antispam</i> (Bloqueo de virus y <i>spam</i> )	Políticas, Configuraciones, <i>Service Pack</i> , actualizaciones, respaldos de configuración.
	<i>Firewall</i>	Configuraciones, reglas aplicables al servicio.
	Actualizaciones	Actualizaciones
WEB	<i>Firewall</i>	Configuraciones, reglas aplicables.
	Servidor <i>Web</i> (ISS y Apache)	Políticas, Configuraciones, <i>Service Pack</i> , actualizaciones, respaldos de configuraciones, manejo de equipos clientes.
Citrix	<i>Firewall</i>	Configuraciones, reglas aplicables.
	Acceso Remoto	Configuraciones, permisos.
	Servidor Citrix	Aplicaciones publicadas, permisos, configuraciones.
Servicios de Red	DNS, DHCP	Configuración, vulnerabilidades, servicios.
Accesos Remotos	RAS	Configuración, permisos, accesos.
	VPN	Configuraciones, accesos, permisos.
	FTP	Configuraciones, accesos, permisos.
<i>Firewall</i>	<i>SmartDashBoard</i>	Configuraciones, Reglas Aplicables, Licencias, Accesos Rutas IP, Permisos Especiales.
	<i>SmartViewMonitor</i>	Configuraciones, Reglas Aplicables, Licencias, Accesos Rutas IP, Permisos Especiales.
	<i>EventingReporter</i>	Reportes de la utilización, Reglas
	<i>SmartUpdate</i>	Actualizaciones
Active Directory	Sistema Operativo	Políticas, claves, grupos, <i>Service Pack</i> , actualización permanente, respaldo de configuración.
	Servidor	Políticas, configuraciones, <i>Service Pack</i> , actualizaciones, respaldos de configuración.
Bloqueador de URL	<i>WebManager</i>	Configuración, permisos, accesos.
	<i>WebReporter</i>	Reportes de los accesos.
	<i>WebReportingTools</i> (on-line)	Reportes de los accesos en línea.

Tabla 2.8 Servicios de la Compañía<sup>[11]</sup>

✓ *Optimizador Ancho de Banda*

Se utilizan el equipo especializado *PacketShaper* de *Packeteer* para la gestión de uso de ancho y priorización de servicios. Las reglas han sido depuradas y configuradas de acuerdo a los requerimientos de la Compañía por el personal de Informática.

✓ *Antispam App*

Actualmente existe una solución ISS para protección de borde de *spam*. Este equipo fue adquirido recientemente y tiene configurado algunas reglas para el filtrado. Este equipo se lo usa para filtrar correo electrónico.

✓ *VPN*

Se utiliza el equipo especializado *Check Point* modelo *VPN-1 UTM Edge* para seguridad de las conexiones VPN y otros accesos remotos. Trabaja conjuntamente con la autenticación del *firewall*.

✓ *Proxy*

Se utilizan dos equipos para la función de *Proxy* los cuales tienen las direcciones IP 208.19.64.10 y 208.19.64.14 respectivamente. Debido a que se basan en linux, las listas de control de acceso están especificadas en el archivo *squid.conf*, mientras que las reglas están configuradas en *iptables*. Estas reglas son solo para los *Proxies*.

Los *logs* de acceso se almacenan en el directorio */var/log/squid/access.log*, y cada semana la información de este archivo es añadida al archivo *access1.log* el cual contienen una recopilación de la información semanal del archivo *access.log*, quedando el primero vacío al finalizar cada semana.

Se utiliza el programa *WebSpy Analyzer Premium* para consolidar los *logs* del *Proxy* y generar reportes de utilización de los canales de navegación. Están desglosados por *top* usuarios, *sites*, horarios y *profiles*; se emiten mensualmente.

✓ *Red Inalámbrica (“Wireless”)*

Los servicios de conexión a la red inalámbrica se encuentran instalados en los pisos 5 y 10. Los equipos utilizados son marca 3Com y D-Link. Están en el mismo rango de direcciones IP: 172.17.2.0/23 con un *pull* de direcciones del DHCP específicas para éstos.

Solo proporcionan conectividad en un área específica, los funcionarios no pueden movilizarse de un ambiente a otro, ya que sus equipos portátiles eventualmente pierden conexión.

✓ *Impresoras de Red (Print Server)*

Al momento se cuenta con impresoras de grupo configuradas sin seguridad. Por ejemplo, si se encuentra una impresora de red sin contraseña, ésta puede ser modificada y ocasionar molestias a los usuarios.

✓ *Sistema NMS (Network Management System) de Transelectric (SCADA)*

TRANSELECTRIC puede operar su red eléctrica a través del *software* NMS en tiempo real, con la versión en producción NM 2003 implementado por la empresa ABB. Este sistema posee las siguientes características:

- Servidores de Aplicaciones, que trabajan sobre plataforma UNIX.
- Servidores de Adquisición de Datos que trabajan sobre plataforma UNIX.
- Servidores Oracle que contienen la base de datos de configuración del sistema y de aplicaciones; almacenan todos los eventos relacionados con el sistema eléctrico y *Network Manager*. Su plataforma es WINDOWS.
- Consolas de Operación donde se encuentra la interfaz de usuario utilizada para la supervisión del SNT. El sistema operativo es Windows.

#### 2.2.2.1.4 *Análisis de Tráfico de la Red*

Uno de los temas a considerar para identificar la situación actual y mejorar el funcionamiento de la red LAN del edificio matriz de TRANSELECTRIC S.A. es el

análisis del tráfico que circula por dicha red. Es decir, conocer con qué protocolos se está trabajando, cuáles son los más utilizados, velocidades, ancho de banda requerido, etc.

Para realizar el análisis descrito anteriormente se emplearon básicamente dos tipos de herramientas:

- ✓ *PacketShaper* que se utiliza dentro de la Compañía para administrar el ancho de banda de la red, el cual también presenta gráficamente el consumo y rendimiento de la red de datos.
- ✓ El analizador de protocolos *WireShark* que muestra los paquetes enviados y recibidos por los usuarios durante un lapso de tiempo, indicando las direcciones IP y el tipo de protocolo por el que se envía permitiendo filtrar los resultados de acuerdo a la aplicación que se requiera.

Como se explicó en el punto 2.2.1.2, el edificio tiene dos cuartos de equipos donde están los *switches* de distribución (Cisco 3500). Para realizar el monitoreo general en estos equipos se configuró un puerto espejo de los demás, de tal manera que pueda ser monitoreado el tráfico de toda la red a través de este puerto. A su vez, se habilitaron las funciones SNMP de los *switches*.

Las pruebas con *Wireshark* fueron tomadas durante dos semanas importantes en agosto de 2008 ya que hubo fin e inicio de mes. De esta manera se puede tener idea de altos y bajos de tráfico y las aplicaciones son las que principalmente manejan/utilizan los usuarios.

#### *a. Monitoreo con PacketShaper*

Los datos del monitoreo del tráfico generado en toda la red del edificio Matriz durante el mes de agosto fueron proporcionados por el área de Informática de la Compañía; con ellos se pudo obtener el promedio, valores pico de la utilización de ancho de banda de entrada y salida. Este tráfico fue medido a la salida de la interfaz *eth0* del *firewall* la cual está conectada por medio de un *switch* al equipo *PacketShaper*.

Report: Monitoreo Proxy For: 208.19.64.75  
Generated: Aug 30 2008 16:02:31

Last

Show   before

### Average Rate

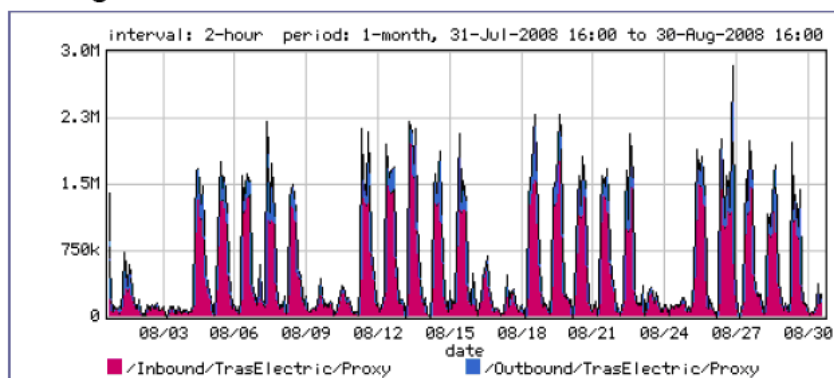


Figura 2.19 a Tráfico promedio de la red del edificio matriz <sup>[11]</sup>

### Peak Rate

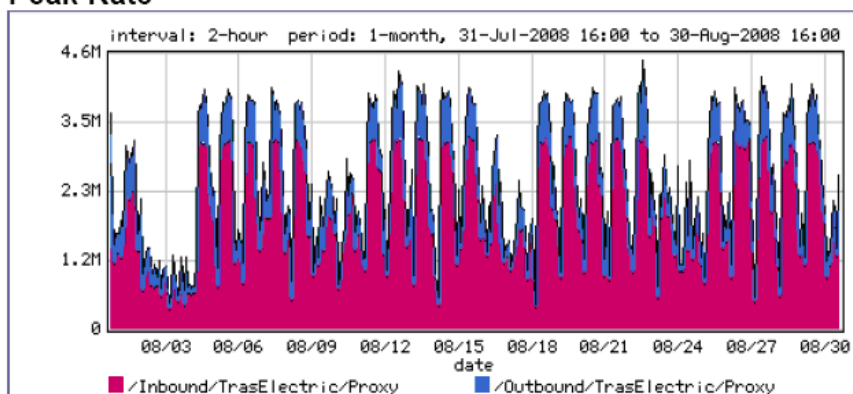


Figura 2.19 b Tráfico pico de la red del edificio matriz <sup>[11]</sup>

Como se puede ver en la figura 2.19a, se tiene una utilización del ancho de banda<sup>23</sup> promedio de 2 Mbps para salida y de 1,5 Mbps para entrada; esto es monitoreando en el Proxy, lo que indica la utilización de *Internet*.

Si se consideran los valores picos se llega a consumir hasta 4 Mbps de salida y 3

<sup>23</sup> Se menciona ancho de banda como la capacidad de canal.

Mbps de entrada (Figura 2.19b). Se puede también notar que por lo general el día de mayor tráfico es el martes, que se obtuvo de un promedio de todo el mes.

Asimismo, se pudo obtener gráficas (proporcionadas por el área de Informática) de la utilización y el rendimiento de la red tanto de entrada como de salida.

Con respecto a la utilización, en entrada se llega hasta picos de 4.2 Mbps y un promedio de 2 Mbps. Estos resultados incluyen toda la red, es decir, todos los tipos de tráfico y protocolos utilizados por las diferentes aplicaciones (Figura 2.20a).



### Utilization

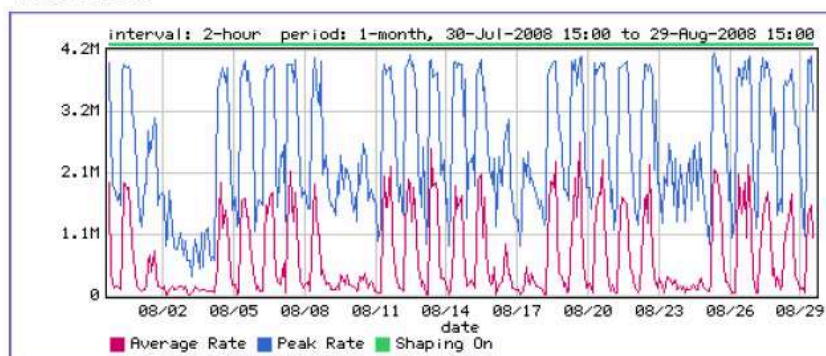


Figura 2.20a Utilización total de la red en entrada <sup>[11]</sup>

Al analizar la eficiencia de la red (Figura 2.20b), se puede concluir que posee un buen rendimiento, ya que en casi todo el mes se tuvo el 100% excepto en dos días, entre el 2 y 4 de Agosto, los cuales debido a que coincidieron con fin de semana, no se considera un mayor problema.



## Network Efficiency

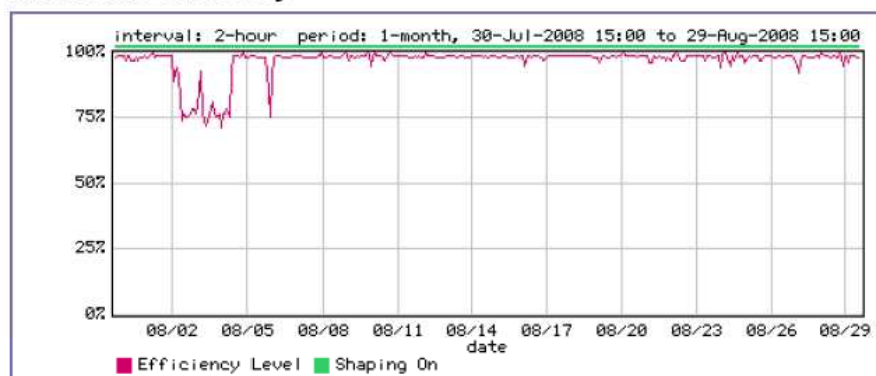


Figura 2.20b Rendimiento total de la red en entrada <sup>[11]</sup>

En salida, se llega hasta picos de 2,5 Mbps y un promedio de 500 Kbps. Como se mencionó anteriormente, estos resultados incluyen todos los tipos de tráfico y protocolos utilizados por las diferentes aplicaciones (Figura 2.21a).

## Outbound

### Utilization

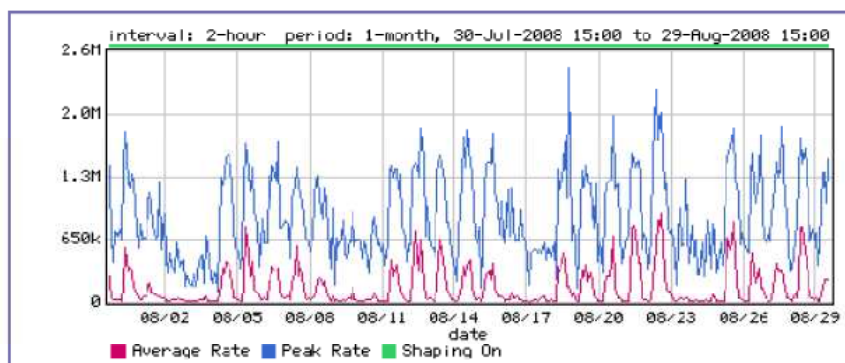


Figura 2.21a Utilización total de la red en salida <sup>[11]</sup>

La eficiencia de la red (Figura 2.21b) es la misma que la de entrada.

### Network Efficiency

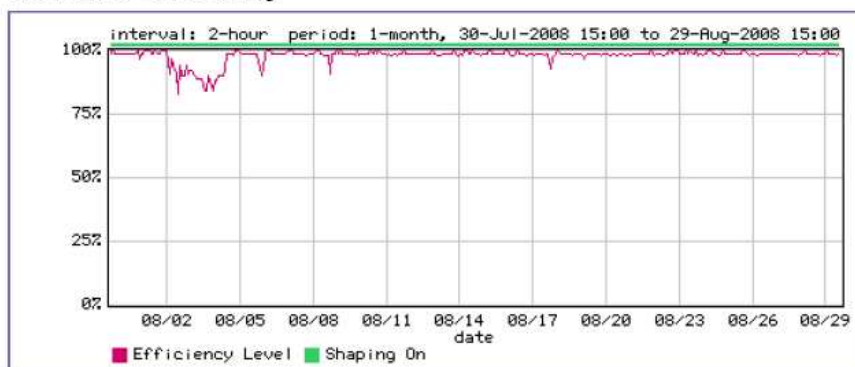


Figura 2.21b Rendimiento total de la red en salida <sup>[11]</sup>

No se tiene definida una capacidad máxima contratada de entrada y salida a *Internet*, pero está autorizado limitarla generalmente hasta 4 Mbps de entrada y 3 Mbps de salida; en casos especiales y bajo permiso de autoridades principales, se aumenta la capacidad de entrada hasta 8 Mbps.

Por último, la herramienta proporciona resultados de la cantidad de información recibida y enviada a través de la red. Se recibe mayor cantidad de la que se envía, lo que explica el porqué de la diferencia de tráfico de entrada con respecto al de salida. El resultado del mes fue 209.3 Gbytes recibidos y 49.5 Gbytes enviados con una diferencia de 4 a 1.

#### *b. Monitoreo mediante WireShark*

Paralelamente en las semanas del 28 de Julio al 1 de Agosto y del 4 al 8, se realizó el monitoreo de los *switches* con *Wireshark*, donde se verificó de una forma más específica el tipo de paquetes que circulan a través de la red LAN del edificio, además de su origen y destino.

La cantidad de paquetes que circulan por la red es muy alta y no se puede capturar continuamente esta información, es por ello que se realizaron muestreos durante intervalos de tiempo hasta llegar aproximadamente a los 500.000 paquetes, que

entre los dos *switches* suman 1 millón de paquetes.

Las muestras se tomaron tres veces al día en lapsos de media hora entre 10h00 a 12h30, 12h30 a 15h00 y 15h00 a 17h30, para no tener problemas con la herramienta utilizada; siendo generalmente las 11h00, 13h00 y 16h30 las horas pico donde mayor cantidad de paquetes circulaban por la red.

Los tipos de paquetes<sup>24</sup> que se obtuvieron del monitoreo a los *switches* fueron los siguientes:

- ✓ ARP (*Address Resolution Protocol*)
- ✓ CDP (*Cisco Discovery Protocol*)
- ✓ CLDAP (*Connectionless Lightweight Directory Access Protocol*)
- ✓ CLNP (*Connectionless Network Protocol*)
- ✓ DHCP (*Dynamic Host Configuration Protocol*)
- ✓ DNS (*Domain Name System*)
- ✓ DTP (*Dynamic Trunking Protocol*)
- ✓ HTTP (*Hypertext Transfer Protocol*)
- ✓ HTTP/XML (*eXtensible Markup Language*)
- ✓ ICMP (*Internet Control Message Protocol*)
- ✓ IGMP (*Internet Group Management Protocol*)
- ✓ IP (*Internet Protocol*)
- ✓ IPX RIP (*Internetwork Packet eXchange Routing Information Protocol*)
- ✓ IPX SAP (*IPX Service Advertisement Protocol*)
- ✓ LDAP (*Lightweight Directory Access Protocol*)
- ✓ LLC (*Logical Link Protocol*)
- ✓ LLDP (*Link Layer Discovery Protocol*)
- ✓ LSA (*Microsoft Local Security Architecture*)
- ✓ NBIPX (*NetBios over IPX*)
- ✓ NBSS (*NetBios Session Service*)

---

<sup>24</sup> Referirse al anexo 2.3

- ✓ NMPI (*Name Management Protocol over IPX*)
- ✓ NSPI (*Name Service Provider*)
- ✓ NTP (*Network Time Protocol*)
- ✓ RTP (*Real-time Transport Protocol*)
- ✓ RIPV1 (*Routing Information Protocol version1*)
- ✓ SMB (*Server Message Block Protocol*)
- ✓ SNMP (*Simple Network Management Protocol*)
- ✓ SSL (*Secure Socket Layer*), SSLV2, SSLV3
- ✓ STP (*Spanning Tree Protocol*)
- ✓ TCP (*Transmission Control Protocol*)
- ✓ TDS (*Tabular Data Stream*)
- ✓ UDP (*User Datagram Protocol*)

No se realizó un análisis de cada tipo de paquete ya que la mayoría no alcanzaba ni el 1% del tráfico total, por ello se procedió a filtrar y analizar los protocolos que son utilizados con mayor frecuencia, es decir que en el monitoreo aparecieron en cantidades considerables. Este análisis se presenta a continuación:

✓ *Switch del Piso 5*

De una muestra de 539605 paquetes (en media hora aproximadamente), aparece representativamente el protocolo IP como el protocolo más común dentro de la red *Internet*, y en un porcentaje muy reducido el protocolo ARP que permite resolver entre direcciones IP a MAC; al hacer un análisis dentro de una LAN es lógico que este protocolo aparezca ya que se envía información entre *hosts*.

En la Tabla 2.9 se presenta el resumen de la muestra semanal del monitoreo del *switch* del piso 5 que se explicará a continuación.

Protocolo	Porcentaje de paquetes por muestra	Número de Paquetes por muestra
Frame	100	539604,7
Ethernet	99,995	539586,7
Internet Protocol	96,79	523461,75
Transmission Control Protocol	77,17	415543,41
Data	1,18	6062,92
DCE RPC	0,71	3573,67
NetBIOS Session Service	13,85	74739,84
Server Message Block Protocol	13,8	74495,29
Tabular Data Stream	0,505	2968,75
Hypertext Transfer Protocol	13,36	70458,29
Secure Socket Layer	0,54	2884,25
Line-based text data	0,1	486,17
Media Type	0,01	58,25
User Datagram Protocol	18,92	104251,618
Domain Name Service	0,545	2655,625
Simple Network Management Protocol	7,94	41964,25
NetBIOS Name Service	0,648	3307,71
Hypertext Transfer Protocol	0,125	674,04
Real-time Transport Protocol	9,2825	53455,79
Internet Control Message Protocol	0,69	3632,375
Address Resolution Protocol	2,31	12146,67
Logical-Link Control	0,585	2337,825
Dinamic Trunking Protocol	0,013	48,168
Spanning Tree Protocol	0,398	1442,918
Cisco Discovery Protocol	0,023	81
Configuration Test Protocol (loopback)	0,105	552,5
Cisco ISL	0,005	18

Tabla 2.9 Tráfico del switch del piso 5 promedio semanal

Dentro de IP están TCP en una diferencia de 4 a 1 con respecto a UDP, por lo que se puede decir que el transporte de información se lo hace estableciendo conexión y con mayor seguridad.

En TCP se destacan NBSS y HTTP en porcentajes similares; NetBIOS permite acceder a la red, es decir a sus servicios además de permitir compartir recursos de red y se lo encontró dentro de TCP y UDP siendo en TCP donde tiene mayor porcentaje.

Con TDS se pueden transferir datos entre una base de datos del servidor y un cliente

y con HTTP se trabaja en lo que se refiere a acceso a *Web*.

Dentro de UDP se destacan SNMP y RTP utilizados para la administración de la red y aplicaciones en tiempo real como video conferencia primordialmente y envío de audio y video a través de *Internet* ya que permite la encapsulación de tráfico en tiempo real.

✓ *Switch del Piso 9*

De una muestra de 570483 paquetes aparece representativamente el protocolo IP como el protocolo más común en el *Internet* y en un porcentaje muy reducido los protocolos LLC y ARP.

Dentro de IP están segmentos TCP en una relación de 17 a 1 con respecto a UDP, por lo que el transporte de información se lo hace estableciendo conexión y con mayor seguridad; casi nada del tráfico se envía por UDP.

En TCP se destacan NBSS, TDS y HTTP, los dos primeros llegando a 17 y 10 por ciento respectivamente y HTTP en un 5 por ciento.

NetBIOS es el que permite acceder a la red, es decir a sus servicios además de permitir compartir recursos de red y se lo encontró dentro de TCP y UDP siendo en TCP donde tiene mayor porcentaje.

Dentro de UDP se destaca SNMP utilizado para la administración de la red. La gran diferencia con el *switch 5* es que aquí no aparece el protocolo RTP. ■

En la Tabla 2.10 se presenta el resumen de la muestra semanal del monitoreo del *switch* del piso 9, resumen que se lo explicará a continuación.

Protocolo	Porcentaje de paquetes por muestra	Número de paquetes por muestra
Frame	100	570482,71
Ethernet	99,95	570183,55
Internet Protocol	91,72	523449,41
Transmission Control Protocol	86,21	492357,08
Data	4,41	24981,58
DCE RPC	1,39	7998,67
NetBIOS Session Service	17,31	96331,41
Server Message Block Protocol	14,31	84641,29
Tabular Data Stream	10,13	62898,5
Hypertext Transfer Protocol	5,32	29478
Secure Socket Layer	0,27	1730,42
Line-based text data	0,12	847,42
Media Type	0,27	1606,42
User Datagram Protocol	4,98	28032,29
Domain Name Service	0,44	2478,88
Simple Network Management Protocol	3,37	19014,71
NetBIOS Name Service	0,8	4322,25
Hypertext Transfer Protocol	0,17	937,46
Real-time Transport Protocol		
Internet Control Message Protocol	0,61	3756,71
Address Resolution Protocol	1,88	10176,42
Logical-Link Control	5,46	31262,75
Dynamic Trunking Protocol	0,14	798,5
Spanning Tree Protocol	4,96	28386,29
Cisco Discovery Protocol	0,25	1444,96
Configuration Test Protocol (loopback)	0,38	2179,67
Cisco ISL	0,05	299,17

Tabla 2.10 Tráfico del switch del piso 9 promedio semanal

✓ *Tráfico Total*

Sumando ambos monitoreos de los switches de los pisos 5 y 9 se puede ver que se reciben en media hora aproximadamente un millón cien mil paquetes.

Entre los paquetes que aparecen en mayor cantidad estuvieron *NetBios*, HTTP, TDS, que indica compartición de archivos, acceso a *Internet* y acceso a base de datos.

Comparando la cantidad de paquetes promedio que circulan por la red en entrada y

salida con lo obtenido mediante *Packet Shaper* ( $2 \text{ Mbps}_{(\text{entrada})} + 500 \text{ Kbps}_{(\text{salida})} = 2,5 \text{ Mbps}$ ) se puede ver que se tiene un valor de 2.5 Mbps y se envían aproximadamente 2 millones de paquetes cada hora (1 millón cada media hora).

En la Tabla 2.11 se sumaron los promedios de paquetes que circulan por la red en un intervalo aproximado de media hora, medidos desde cada *switch* de distribución. Se puede ver que de igual manera predomina el envío bajo conexión TCP en relación a UDP de 8 a 1 aproximadamente con lo que se reitera que para enviar información se establece enlaces de conexión previos.

Protocolo	Promedio Total en media hora	Total pack
Frame	100	1110087
Ethernet	99,97	1109770
Internet Protocol	94,26	1046911
Transmission Control Protocol	81,69	907900
Data	2,8	31045
DCE RPC	1,05	11572
NetBIOS Session Service	15,58	171071
Server Message Block Protocol	14,06	159137
Tabular Data Stream	5,32	65867
Hypertext Transfer Protocol	9,34	99936
Secure Socket Layer	0,41	4615
Line-based text data	0,11	1334
Media Type	0,14	1665
User Datagram Protocol	11,95	132284
Domain Name Service	0,49	5135
Simple Network Management Protocol	5,66	60979
NetBIOS Name Service	0,72	7630
Hypertext Transfer Protocol	0,15	1612
Real-time Transport Protocol	4,64	53456
Internet Control Message Protocol	0,65	7389
Address Resolution Protocol	2,1	22323
Logical-Link Control	3,02	33601
Dinamic Trunking Protocol	0,08	847
Spanning Tree Protocol	2,68	29829
Cisco Discovery Protocol	0,14	1526
Configuration Test Protocol (loopback)	0,24	2732
Cisco ISL	0,03	317

Tabla 2.11 Promedio aproximado del tráfico de los *switches* de distribución en cada media hora



En TCP se reconocen claramente paquetes NetBIOS, TDS y HTTP que corresponden a acceso y compartición de recursos de red, transferencia de datos entre cliente y servidor y acceso Web respectivamente. En UDP se tiene en mayor porcentaje paquetes SNMP y RTP que corresponden a administración de red y aplicaciones en tiempo real respectivamente.

El tráfico RTP se debe a las aplicaciones en tiempo real de TRANSELECTRIC S.A como cámaras de videovigilancia.

#### *2.2.2.1.5 Seguridad de la Red*

TRANSELECTRIC S.A. tiene políticas de seguridad mínimas, como el establecimiento de contraseñas en los equipos críticos tales como servidores y equipos de red. A su vez las PCs poseen contraseñas que deben ser cambiadas cada cierto tiempo.

Existen contraseñas para Telnet, HTTPs y consola en los equipos de red tales como *switches* y *routers*.

También está habilitado SNMP pero no con un dominio específico ya que en algunos se mantienen *public* y en otros se tiene un dominio privado el cual provee mayor seguridad.

Se permite el acceso al *firewall* y *Proxy* a través de SSH y están configuradas las IPs de las máquinas que pueden acceder.

#### *2.2.2.1.6 Administración de la Red*

Las herramientas de administración y monitoreo de la red facilitan la generación de estadísticas de uso de recursos, necesarias para calcular crecimiento y para evaluar niveles de servicio (% de utilización de memoria, disco, CPU, ancho de banda, y otros indicadores SNMP de la base MIB genérica y/o particular).

A su vez ayudan a saber cuáles son los protocolos más utilizados con los que se

está trabajando, las velocidades que se están manejando, el ancho de banda requerido en la red, entre otros.

TRANSELECTRIC S.A. utiliza el producto PRTG *Traffic Grapher* para el monitoreo del uso de ancho de banda (análisis cuantitativo) de los enlaces locales y remotos de la red.

PRTG registra también el total del tráfico entrante y saliente de cada una de las interfaces que están siendo observadas (monitoreadas).

A través del producto *PacketShaper*, utilizado dentro de la Compañía para reportes diarios, se puede verificar el uso del ancho de banda utilizado por los usuarios. Además proporciona gráficas del consumo y rendimiento de la red de datos; a su vez se puede monitorear los enlaces del *firewall*.

#### **2.2.2.2 Red WAN de la Compañía**

TRANSELECTRIC posee una Gerencia de Telecomunicaciones, que a través del Centro de Gestión puede proveer servicios de transmisión de voz, video y datos mediante la red WAN en gran parte del país. A través de ellos se garantiza la alta disponibilidad del servicio e interconecta el edificio matriz en Quito con las subestaciones, bodegas y oficinas en otras ciudades.

Cada vez se están instalando más enlaces de fibra óptica en las diferentes provincias del Ecuador, con el objetivo de generar mayor desarrollo del país a través de las Telecomunicaciones.

En la figura 2.22 se presenta el diagrama de toda la red que maneja TRANSELECTRIC S.A. a lo largo del país.

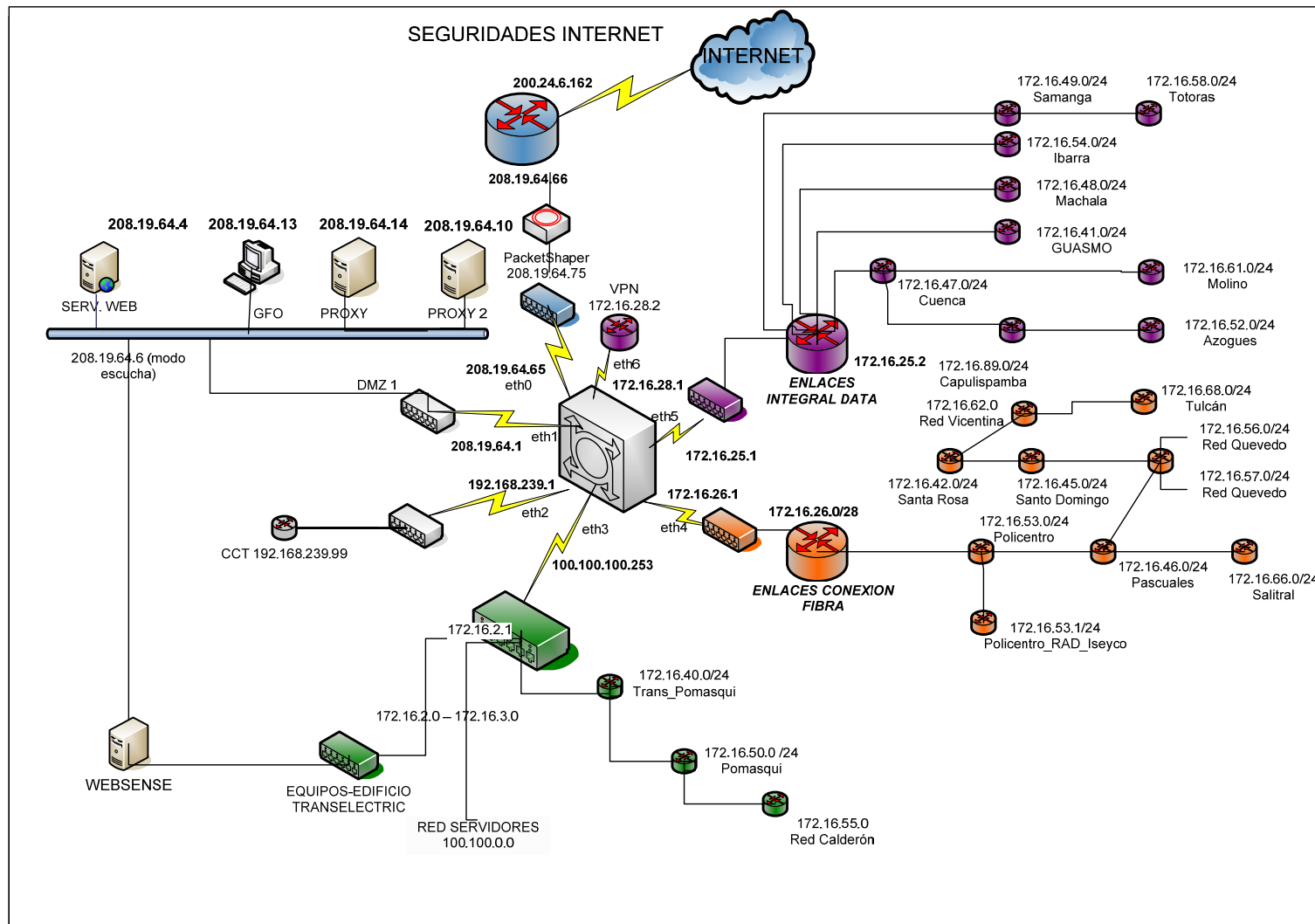


Figura 2.22 Red WAN de Transelectric S.A. [12]

Parte de esta red se la explicó anteriormente al describir las conexiones de las diferentes interfaces del *firewall*. Se debe añadir las conexiones de la *eth4* y *eth5* pertenecen a enlaces de fibra óptica e *Integral Data* que no son totalmente propiedad de la Compañía. Se recalca que este proyecto de titulación solo tendrá enfoque en la red LAN del edificio matriz y del enlace de éste con Calderón.

La administración de la Red WAN está a cargo del área de Telecomunicaciones quienes siendo parte de TRANSNEXA, alianza entre TRANSELECTRIC de Ecuador e INTERNEXA de Colombia, se encargan de ofrecer el mejor servicio en comunicaciones a los diferentes clientes, entre los principales se tiene a Andinanet, Global Crossing, Etapa, Etapa Telecom, Movistar, Porta, Alegro, Megadatos, etc. Esto no es parte de nuestro estudio.

En el desarrollo de este capítulo se ha dado énfasis a la red LAN del edificio matriz, analizando el cableado estructurado, los equipos de la red, la salida a Internet, la interconexión con Calderón, etc.

### **2.2.3 ESTRUCTURA DE LA RED DE VOZ**

#### **2.2.3.1 Generalidades**

El edificio matriz de TRANSELECTRIC cuenta con 2 centrales telefónicas que se encuentran en los cuartos de telecomunicaciones.

En el piso 9 se tiene una central telefónica marca Panasonic que tiene varias tarjetas para troncales que pueden ser líneas urbanas y extensiones de otras centrales; los usuarios que se encuentran conectados a esta central poseen extensiones de 3 dígitos. Para llamar a extensiones de esta central se lo hace de forma directa y para otras se debe marcar primeramente un código; de igual manera para llamar de extensiones a números convencionales y celulares se requiere de un código de salida.

En el piso 5 se tiene una central telefónica marca Siemens que al igual que la anterior soporta tanto líneas urbanas como extensiones; en esta central las

extensiones son de 4 dígitos. Si los usuarios pertenecen a esta central marcan directo las extensiones, caso contrario se utiliza un código para llamar a las de 3 dígitos al igual que para salida a números convencionales o celulares.

Esta *PABX* soporta funcionalidades de Voz sobre IP y se las utiliza a través de los enlaces de datos en subestaciones, bodegas u oficinas de TRANSELECTRIC S.A., pero no se las utiliza en el edificio matriz.

Para la comunicación entre las centrales hay un enlace, es decir varias extensiones de la PBX Panasonic entran a varias troncales de la central Siemens y varias extensiones de la central Siemens ingresan a varias troncales de la central Panasonic (Figura 2.23).

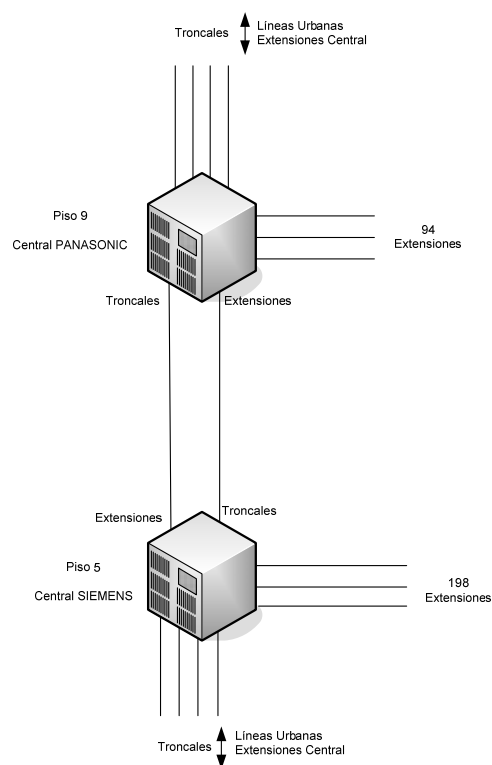


Figura 2.23 Red de Voz

Se cuenta también con bases celulares tanto de Porta como de Movistar en ambos cuartos de telecomunicaciones, las mismas que están conectadas como troncales a las PBX. Aproximadamente entre ambas centrales hay 110 líneas

directas, 94 extensiones de 3 dígitos que pertenecen a la PBX Panasonic del piso 9 y 198 extensiones de 4 dígitos que pertenecen a la PBX Siemens del piso 5.

Se utilizan además equipos como autocontestador con sistema de correo de voz. Este equipo permite dejar mensajes de voz si una extensión o línea no contesta; puede ser a nivel interno o externo. Además si se llama desde fuera de la red de voz una operadora automática contesta y al marcar la extensión requerida se realiza el cambio, es importante ya que no requiere de una persona que realice este trabajo.

### 2.2.3.2 Equipos<sup>37</sup>

Se explicará de una manera más detallada los equipos que se encuentran en los cuartos de telecomunicaciones que intervienen en la red de Voz. Principalmente se cuenta con las dos centrales telefónicas, el autocontestador, el conversor de línea analógica a IP y las bases celulares.

#### 2.2.3.2.1 PABX Panasonic



Figura 2.24 PBX Panasonic<sup>[13]</sup>

#### *Características Principales:*

- ✓ Sistema con crecimiento modular desde 8 hasta 144 líneas y desde 8 hasta 288 extensiones (336 puertos).
- ✓ Compatible para enlaces E&M y E1.
- ✓ Capacidad para 2 voceos externos.
- ✓ Numeración flexible de estaciones.
- ✓ Seguridad de línea de datos.

---

<sup>37</sup> Referirse a las características ofrecidas por los diferentes fabricantes

- ✓ Bloqueo de usuarios.
- ✓ Programación vía PC.
- ✓ Numeración de 3 dígitos con nombre.
- ✓ Desvío de llamadas.
- ✓ Reporte de llamadas.
- ✓ Intercomunicador interno.

#### 2.2.3.2.2. PABX Siemens Hipath 4500



Figura 2.25 PBX Siemens<sup>[14]</sup>

#### *Características Principales:*

- ✓ Soporta hasta 15 *Access Points* conectados directamente y 83 *Access Points* adicionales distribuidos sobre IP. En estas configuraciones es posible un máximo de 12,000 abonados digitales.
- ✓ Para el control común se dispone de una *Duplex Option* y opciones de alimentación redundante para incrementar la disponibilidad del sistema
- ✓ Debido al concepto de *Access Point Modular Stackable*, *HiPath 4500* realiza configuraciones *duplex* rentables también en negocios de medio tamaño.

- ✓ Número de identificación personal (PIN) y *HiPath relocate* (reubica a los usuarios de la terminal).
- ✓ Acceso a múltiples líneas.

#### 2.2.3.2.3 ITS Telecom VME Pro



Figura 2.26 Autocontestador VME Pro<sup>[15]</sup>

#### Características Principales:

- ✓ Hasta 500 casillas de correo.
- ✓ Versión de 4 puertos (72 horas de capacidad de memoria *flash*) expandible a 8 puertos (144 horas).
- ✓ Administración local/remota.
- ✓ Carga de *Software*, EPROM basado en *flash*.
- ✓ Herramienta de monitoreo de línea.
- ✓ Autocontestador en tres idiomas.
- ✓ Transferencia de llamadas.
- ✓ Identificación de llamadas.
- ✓ Protección de administrador mediante contraseña.
- ✓ Integración con las más conocidas PBX y *Key System*.

#### 2.2.3.2.4 Multi-Tech MultiVOIP MVP200



Figura 2.27 MultiVOIP MVP200<sup>[16]</sup>

#### Características Principales:

- ✓ Protocolo de interconexión de datos: *Ethernet*.



- ✓ Protocolo de transporte: TCP/IP.
- ✓ Protocolo de gestión remota: SNMP.
- ✓ Telefonía IP.
- ✓ Protocolos VoIP: H.323.
- ✓ Codecs de voz: G.723.1, G.729.
- ✓ Interfaces de telefonía: 2 teléfonos (FXS), 2 líneas (FXO).
- ✓ Interfaces: 2 x *modem* - E&M - RJ-48 – 2; 2 x *modem* - FXO - RJ-11 – 2; 2 x módem - FXS - RJ-11 – 2; 1 x gestión - RS-232C - RJ-45 – 1; 1 x red - *Ethernet* 10Base-T - RJ-45 – 1.
- ✓ Sistema operativo requerido: Microsoft Windows 95/98, Microsoft Windows NT 4.0 o posterior.

#### 2.2.3.2.5 Modem Hayes Accura V.92



Figura 2.28 Modem Hayes Accura V.92<sup>[17]</sup>

#### Características Principales:

- ✓ Cumple con el estándar internacional V.92 adoptado por la ITU y con el estándar de compresión V.44 para comunicaciones vía *Internet*.
- ✓ Una ventaja fundamental es el incremento en la velocidad de navegación *Web*, entregada por el estándar V.44.
- ✓ *QuickConnect*: Permite cortar la negociación para conectarse al principio de una llamada.
- ✓ Llamada en espera: Permite colocar una sesión en espera mientras se recibe una llamada de voz, y luego reanudar la conexión de datos.
- ✓ Totalmente compatible con el actual estándar V.90 y puede conectarse automáticamente a cualquier sistema utilizando V.90 o V.92.

#### 2.2.3.2.6 Base Celular TECOM



Figura 2.29 Base TECOM<sup>[18]</sup>

##### Características Principales:

- ✓ Simula una línea fija.
- ✓ Enmascara llamadas compatible con otra línea (fija, celular, IP entre otras).
- ✓ Puede abrirle bandas con solo programación (versión GMTFTC B004 o superior).

#### 2.2.3.2.7 Base Celular Ericsson



Figura 2.30 Base Ericsson<sup>[19]</sup>

##### Características Principales:

- ✓ Banda GSM doble (E-GSM 850, GSM 1900).
- ✓ Interfaz analógica RJ11 para Voz, Fax Grupo 3 y transmisión de datos V.90.
- ✓ GPRS & EDGE - *Internet "always on"*.
- ✓ HSCSD (*High Speed Circuit Switched Data*).
- ✓ Acceso al *modem* interno vía USB.
- ✓ Permite minimizar el costo de llamadas a teléfonos móviles y acceso al *Internet*, y permite acceso a voz, fax y datos en ubicaciones remotas o marítimas.

- ✓ Se conecta con una central PBX en forma simple y muy efectiva.
- ✓ Utiliza "*wireless local loop*" para operar con la red móvil. Acceso veloz de *Internet* en oficinas temporarias o rodantes.
- ✓ Permite la administración remota (*Remote Management*) y, cuando está conectado con una computadora o PC, es capaz de recibir mensajes SMS.

## 2.3 REQUERIMIENTOS

### 2.3.1 INFRAESTRUCTURA DEL CABLEADO ESTRUCTURADO

- ✓ Se requiere una reorganización del cableado estructurado debido a que cuando se daña algún punto se deja libre el conector en el *rack* para tomar otro al azar sin especificar el que está dañado.
- ✓ Se requiere nuevamente la instalación de los puntos cuyos cables no pasaron la prueba con el analizador de cables de *Fluke*<sup>38</sup>.
- ✓ Se requiere realizar pruebas de certificación de los puntos que están conectados a *switches* propios de ala y que pasaron la prueba del analizador de cables.
- ✓ Se requiere clasificar los puntos de voz y datos porque en algunos casos los puntos de voz se los habilita para datos sin ninguna especificación.
- ✓ Es necesario bloquear los puntos de red que están libres, ya que actualmente se tiene un bajo nivel de seguridad de múltiples puntos para ganar acceso no autorizado a la red.
- ✓ El cableado del edificio no está desarrollado en su totalidad bajo normas y estándares por ello es necesario certificarlo bajo normas ANSI/EIA-TIA.
- ✓ Mejorar condiciones físicas de los cuartos de telecomunicaciones.
- ✓ Implementar cuartos de telecomunicaciones de acuerdo a los estándares internacionales ya que los actuales son una combinación de cuarto de telecomunicaciones y cuarto de equipos.

---

<sup>38</sup> Referirse a la tabla 2.2 de este capítulo

- ✓ El sistema que se tiene en el edificio no constituye un sistema de cableado estructurado porque no respeta las normas internacionales respectivas y existe una mezcla de cables entre categorías 5E y 6, por lo que se pierde la de mayor grado.
- ✓ Se debería seguir el estándar de cableado estructurado en cuanto a conexiones de equipos, ya que en unos pocos casos se conecta directamente del computador al *switch* sin pasar por un *patch pannel*.
- ✓ No se tiene una administración de cableado estructurado definida.
- ✓ No existe documentación de los puntos de red de los usuarios, falta un correcto etiquetado de los mismos además de los cajetines y *patch pannels*.

### 2.3.2 ESTRUCTURA DE LA RED DE DATOS

- ✓ Se requiere mayor seguridad en lo que respecta a ataques internos, sobretodo en el edificio matriz donde es posible y muy peligroso si fuera realizado por usuarios no autorizados que logren adquirir información confidencial. También desde una estación de trabajo con programas de uso libre descargados desde Internet, se puede obtener información de los servidores y estaciones de trabajo de la red de TRANSELECTRIC.
- ✓ La actual estructura y topología en la red no cuenta con mecanismos que controlen e impidan que algún usuario instale por su cuenta un *Access Point* y obtenga acceso remoto vía inalámbrica.
- ✓ Los servidores no tienen instaladas todas las actualizaciones de los parches, por lo que es necesario que se los actualice para una mayor seguridad.
- ✓ No todos los usuarios han sido capacitados en los mecanismos de seguridad en uso de contraseñas ya que por lo general mantienen las dadas por el administrador. Se requiere una política de seguridad en cuanto a dificultad de predecirlas, cambiarlas periódicamente, usar elementos numéricos, alfabéticos (mayúsculas y minúsculas) y caracteres especiales.
- ✓ No se tienen fuertes políticas de seguridad físicas y lógicas.

- ✓ No se ha desarrollado un plan de seguridad informática que incluya políticas de acuerdo a las necesidades de la Compañía. Por ello se requiere desarrollar políticas de seguridad para la aplicación de éstas.
- ✓ No existe un plan de contingencia informática que incluya la operación desde un sitio alternativo, no se cuenta con equipos adicionales para poder disponer de alta disponibilidad en caso de que falle algún equipo. No se dispone de un sitio alternativo para manejo de contingencias con respecto a sala de servidores, cuarto de equipos, etc.
- ✓ El esquema de direccionamiento IP es heredado y no cumple las mejores prácticas técnicas de diseño e implementación, debido a ello no existe una asignación ordenada de direcciones IP en la subred ni para VLANs, se requiere el rediseño para un mejor funcionamiento general.
- ✓ La red actual está diseñada por capas y los equipos que en ella funcionan incluyen estas características. Para poder reutilizar algunos de éstos se requiere también un rediseño por capas; además con esta propuesta se puede ofrecer mayor disponibilidad mediante la redundancia de equipos.
- ✓ Se requiere seguridad en impresoras con respecto a contraseñas.
- ✓ Existe un alto consumo de canal de *Internet* de usuarios frecuentes. No todos los usuarios pasan por control de *proxy*. Existen usuarios con alto nivel de descarga de archivos y conexión permanente de navegación que deben ser controlados.
- ✓ No se tiene un programa con el cual se administre y monitoree los equipos LAN/WAN, a su vez algunos no pueden ser administrados porque no tienen el protocolo básico SNMP. Se requiere homogeneidad de las marcas para poder administrarlos a todos a través del mismo programa de ser el caso.
- ✓ Existe una subutilización del DHCP y los *pull* de direcciones no están asignados ordenadamente por lo que se requiere una organización y documentación exacta en lo referente al direccionamiento que maneja la Compañía.

- ✓ Debido a que se está gestionando y desarrollando el sistema integrado para TRANSELECTRIC S.A., se requiere un redimensionamiento de los enlaces en especial del que va hacia el COT, de tal manera que soporte las aplicaciones a futuro.
- ✓ No existe una administración correcta de la red de datos y no se maneja políticas de limitación de ancho de banda definidas.
- ✓ Se debe dar mejor utilización a las herramientas de monitoreo, especialmente a las que corresponden a la administración de ancho de banda como *PacketShaper* y *Packeteer*.
- ✓ En la sala de servidores existen *switches* que están subutilizados, es decir se usan 2 ó 3 puertos de los 24 que poseen, se debe optimizar su uso y desempeño.

### 2.3.3 ESTRUCTURA DE LA RED DE VOZ

- ✓ Debido a que la central Siemens posee mejores características y funcionalidades y está más actualizada tecnológicamente comparada con la central Panasonic se requiere una reorganización de las extensiones o un traspaso a la central del quinto piso para un mejor servicio.
- ✓ Dar exclusividad a los diferentes dispositivos de voz de acuerdo a sus funciones principales, si es un fax utilizarlo únicamente para ello y no como herramienta de comunicación en largos períodos de tiempo ya que se puede perder información importante y de mayor urgencia.
- ✓ Educar al personal acerca de la utilización de la red de voz debido a que el uso de sus elementos es exclusivamente profesional y no de carácter personal.
- ✓ Mediante VoIP converger las redes de voz y datos para reducir el tráfico de voz, lo que mejorará las comunicaciones tanto a nivel interno como externo.
- ✓ De acuerdo a los estándares de cableado estructurado, la central telefónica debería estar en la sala de servidores (cuarto de equipos).

# CAPÍTULO 3

**DISEÑO DE LA RED  
LAN DE  
TRANSELECTRIC  
S.A.**

## **DISEÑO DE LA RED LAN DE TRANSELECTRIC S.A.**

### **3.1 INTRODUCCIÓN**

El diseño de una red convergente de voz y datos es el esquema de solución que se plantea en el presente capítulo para que la red de TRANSELECTRIC S.A. tenga: mejor rendimiento, velocidad de transmisión de datos, calidad de servicio, entre otros. A su vez se establece un sistema de comunicación confiable, funcional, que permita la escalabilidad en la red y que sea de fácil administración.

En la solución a presentarse se reflejarán los objetivos, características, políticas de la Compañía y se mantendrá el cumplimiento de los requerimientos organizacionales y tecnológicos de la misma; con este diseño se pretende satisfacer las necesidades especificadas en el capítulo anterior, la demanda de tráfico necesario para voz y datos, además lograr que todos los usuarios tengan acceso de una manera rápida, eficiente y segura a los servicios y aplicaciones que la red brinda.

El diseño que se ofrecerá en este capítulo para TRANSELECTRIC S.A. se lo realizará de acuerdo a las normas y estándares establecidos internacionalmente, brindando una solución eficiente para el cableado estructurado, el diagrama físico y lógico de la red LAN, sugerencias de políticas de seguridad y administración, etc.

También se dimensionará el enlace entre el edificio matriz y el COT y se los integrará en un solo sistema de red de comunicaciones.

Además se proyecta tener un diseño exitoso dentro de un presupuesto aceptable, bajo las normas y reglas que se dispongan en la Compañía.

Este capítulo se divide en cuatro partes para explicar de manera clara y precisa la



solución propuesta.

En la primera se realizarán los cálculos para el dimensionamiento del tráfico de voz que ayudará a determinar la capacidad del enlace requerido y ofrecerá escalabilidad utilizando VoIP. Se presentarán también los cálculos y dimensionamiento de usuarios, equipos, tráfico generado por servicios y aplicaciones de la red para la determinación del ancho de banda necesario respecto a voz y datos.

Se debe tener en cuenta que no se envían ni se reciben datos todo el tiempo, pero se considerarán las situaciones más críticas para realizar un buen dimensionamiento de los enlaces, por ello se asume que el 80%<sup>39</sup> de los usuarios utilizan recursos simultáneamente.

La segunda parte estará enfocada al diseño de la red LAN del edificio matriz, donde se especificará el sistema de cableado estructurado, los elementos tanto pasivos como activos a utilizarse, el diagrama físico y lógico de la nueva red y su direccionamiento IP.

Además se propondrá un plan de contingencia para mejorar la disponibilidad de los equipos y servidores de la red. Se dimensionará el enlace con las oficinas del COT en Calderón para cumplir con requerimientos de ancho de banda y aplicaciones que la Compañía implemente próximamente.

En la tercera parte se especificarán las políticas de seguridad, usando criterios para lograr confiabilidad en la red, integridad y confidencialidad de la información que circulará a través de la misma.

Por último se mencionarán las posibles herramientas para la administración de la red a través del monitoreo de los dispositivos de red, servidores, tráfico existente en los enlaces, entre otras.

---

<sup>39</sup> Usuarios que trabajan en el edificio simultáneamente

### **3.2 REQUERIMIENTOS DE ANCHO DE BANDA DE LA RED**

La red LAN del edificio matriz de TRANSELECTRIC debería soportar diferentes tipos de tráfico; se tiene principalmente uso de *Internet*, correo electrónico, acceso a base de datos, archivos compartidos entre usuarios (utilizado comúnmente por el personal de soporte técnico).

La red de voz será tratada de dos maneras, una de ellas será encapsularla en paquetes IP y transportarla dentro de la red de datos usando VoIP. La otra es usar telefonía convencional mediante la utilización de una de las centrales telefónicas con la que actualmente se cuenta en el edificio matriz.

En las oficinas en Calderón se tiene el mismo tipo de tráfico de datos de la matriz pero difiere en la consecuencia de uso y cantidad de usuarios. Con respecto a la voz no se modificará nada ya que en este proyecto de titulación se especificó que solo se realizará el dimensionamiento del enlace.

#### **3.2.1 DETERMINACIÓN DEL ANCHO DE BANDA REQUERIDO PARA VOZ**

Como se vio en el capítulo anterior, se tienen dos PABX que ofrecen tanto líneas troncales como extensiones; una de las PABX está utilizada en un 3% de su capacidad ya que soporta hasta 12 mil líneas analógicas y posee alrededor de 300 usuarios.

El objetivo de este diseño es converger las redes de voz y datos para mejorar la comunicación de los usuarios tanto a nivel interno como externo. Para la transmisión de voz se considerará la tecnología VoIP que permite integrar aplicaciones de voz con los servicios de datos que actualmente se llevan a cabo sobre IP.

Para no desperdiciar recursos existentes, se reutilizará la central telefónica Siemens que posee características relacionadas con VoIP. Los costos de los equipos de VoIP son relativamente bajos con respecto a los de las diferentes

alternativas tecnológicas que se tienen tales como voz sobre *TDM, ATM, Frame Relay*.

Al realizar la migración de telefonía convencional a VoIP, se generará mayor tráfico en la red de datos y reducirá el de voz, descongestionando la red convencional de voz.

Esta migración será por partes, se dará prioridad a los usuarios que se encuentren dentro de la PABX Panasonic del noveno piso que está desactualizada en tecnología y que incluye actualmente las líneas del personal de directorio de la Compañía y otros usuarios privilegiados.

Sin embargo, para el dimensionamiento del tráfico de voz y requerimientos es importante determinar el número de canales de voz necesarios en el edificio Matriz, para ello se considera el volumen de llamadas generadas y la duración de las mismas. La central permite configurar un límite de duración de llamadas pero en la Compañía no se aplica dicha funcionalidad.

Con los datos obtenidos en TRANSELECTRIC S.A. se tiene un promedio de 17 llamadas entrantes y salientes en una hora, con una duración promedio de 5 minutos asumiendo las peores condiciones. Se determina el tráfico a partir de la ecuación de *Erlang*<sup>40</sup>.

$$A = C_a * T_p \quad [\text{ec. 3.1}]$$

Donde: A = Intensidad de tráfico o velocidad de flujo de llamadas, es un valor adimensional dado en *Erlangs*.

$C_a$  = Número de llamadas originadas durante la hora pico.

$T_p$  = Tiempo promedio de duración de llamadas.

Calculando:

---

<sup>40</sup> Tomada de la tesis "Diseño del sistema de red para transmisión de voz y datos para el municipio de Santo Domingo y criterios de Administración" de Yadira Acurio.

$$A = 17 \frac{\text{llamadas}}{\text{hora}} * \frac{1 \text{ hora}}{60 \text{ minutos}} * 5 \text{ minutos}$$

$$A = 1.42 \text{ Erlang}$$

Con el valor calculado en *Erlangs* de intensidad de tráfico, considerando una probabilidad de pérdida (GoS) de 0.01 (Valor recomendado para telefonía) y utilizando la Gráfica de *Erlang B* (Figura 3.1) se concluye que son necesarios 6 canales de voz en el edificio matriz.

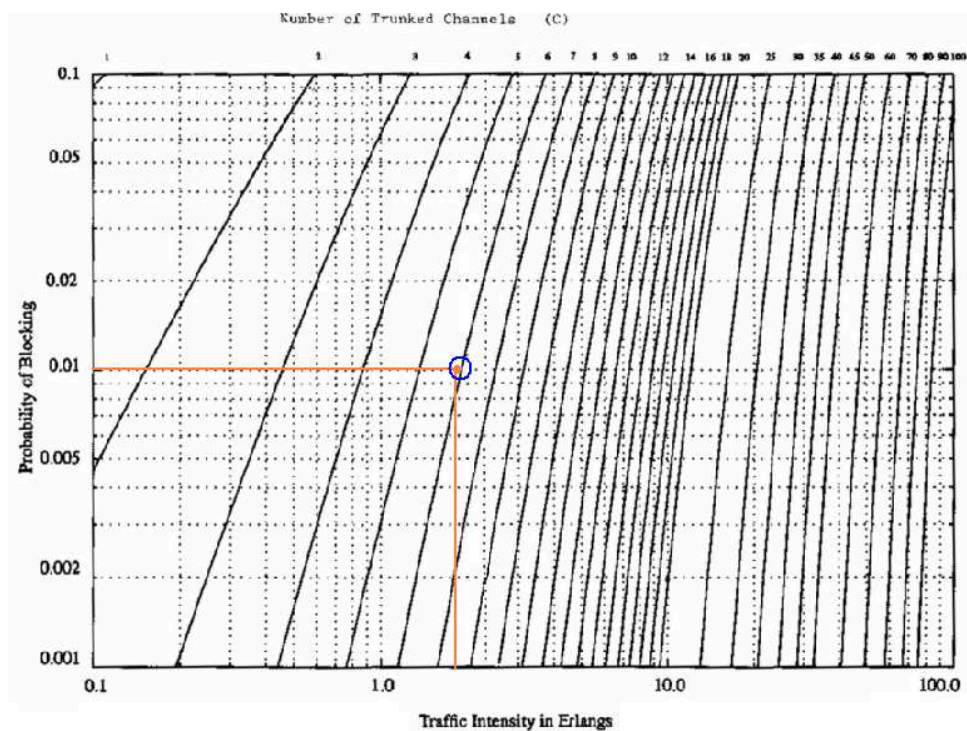


Figura 3.1 Gráfica de *Erlangs*<sup>[1]</sup>

Para la implementación de VoIP es necesario la utilización de los *Voice CODEC's* (codificadores-decodificadores de voz) que son dispositivos que emplean algoritmos de codificación que convierten la señal de voz analógica en un flujo digital de datos. Además de convertir de analógico a digital, el *CODEC* comprime la secuencia de datos, y proporciona cancelación de eco.

La compresión de la forma de onda de voz ahorra ancho de banda, esto es útil especialmente en los enlaces de poca capacidad y permite tener un mayor

número de conexiones de VoIP simultáneamente. Otra manera de ahorrar ancho de banda, es utilizar supresión de silencios, que es el proceso de no enviar los paquetes de la voz que contienen silencios durante la conversación.

En la tabla 3.1 se muestra un resumen con los *codecs* más utilizados actualmente, los cuales fueron definidos por ITU-T (*International Telecommunication Union*).

Codec	Descripción	Ancho de Banda (Kbps)	Frecuencia de Muestreo	Observaciones
G.711	Modulación por impulsos codificados (MIC) de frecuencias vocales.	64	8 KHz	Representa señales de audio con frecuencia de la voz humana, mediante muestras comprimidas de una señal de audio digital. Posee dos versiones para muestrear la señal G.711a (Europa y resto del mundo) y G.711u (US, Japón).
G.721	Modulación por impulsos codificados diferencial adaptativa (MICDA).	32	8 KHz	Obsoleto. Su contenido se abarca en el G.726.
G.722	Codificación de audio de 7 KHz dentro de 64 Kbit/s.	64	7 KHz	Describe las características (50 a 7000 Hz) de un sistema audio de codificación utilizable para alta calidad de la voz. El sistema de codificación utiliza modulación de código de pulso diferenciado adaptante del sub-band (sb-adpcm-adpcm) dentro de un índice binario de 64 Kbps.
G.722.1	Codificación de baja complejidad para el funcionamiento manos libres en los sistemas con baja pérdida de tramas.	24 y 32	16 KHz	Describe un algoritmo <i>wideband</i> digital del codificador que proporciona un ancho de banda audio de 50 a 7000 Hz.
G.722.2	Codificación en banda ancha de voz utilizando banda ancha multivelocidad adaptativa.	16	16 KHz	Se utiliza para la voz sobre usos IP (VoIP) y del <i>Internet</i> (IP), comunicaciones móviles, usos de la PSTN, telefonía <i>wideband</i> de ISDN, videotelefonía de ISDN y videoconferencia.
G.723	Extensiones de la modulación por impulsos codificados diferencial adaptativa de la recomendación G.721 para aplicaciones en equipos de multiplicación de circuitos digitales.	24 y 40	8 KHz	Obsoleto. Su contenido se abarca en el G.726.
G.723.1	Codec de voz de baja velocidad para la transmisión en comunicaciones multimediales.	5.3 y 6.3	8 KHz	Diseñado para videoconferencia-telefonía a través de línea de teléfono estándares. Optimizado para codificar y decodificar en tiempo real.
G.726	Modulación por impulsos codificados diferencial adaptativa (MICDA).	16, 24, 32 y 40	8 KHz	ADPCM. Reemplazó al G.721 y G.723
G.728	Codificación de señales vocales utilizando predicción lineal con excitación por código de bajo retardo.	16	8 KHz	CELP
G.729	Codificación de la voz mediante predicción lineal con excitación por código de bajo retardo.	8	8 KHz	Bajos requerimientos en ancho de banda. Comprime audio de voz en segmentos de 10 milisegundos.
G.729.1	Codificador incorporado a velocidad binaria variable basado en el codificador G.729: Tren de bits de un codificador de banda ancha adaptable.	8 a 32		Compatible con G.729.

Tabla 3.1 *Codecs* de voz<sup>[2]</sup>

Para el presente diseño se escoge el *CODEC* G.729a debido a que cuenta con un ancho de banda relativamente bajo (8 Kbps) y una mayor calidad de voz; además, es el más utilizado para aplicaciones de VoIP.

De acuerdo a estudios realizados el tiempo de duración del paquete, óptimo para el muestreo es de 20 milisegundos<sup>41</sup>. Al aumentar el tiempo de duración del paquete, se incrementa la carga útil; es decir, se puede tomar más muestras mejorando la calidad, pero a su vez se eleva el retardo total en la transmisión. Con ello es más probable la pérdida de paquetes y por consiguiente un decaimiento en la calidad de voz.

Para bajar la tasa de pérdida de paquetes se implementan *buffers* de variación de retardo para paquetes de gran tamaño, pero como resultado se obtienen retardos de encolamiento muy elevados. Se debe tener en cuenta que por encima de los 30 milisegundos se tienen niveles de calidad de voz inaceptables.

Por otro lado, el tiempo de duración del paquete no debe ser inferior a los 10 milisegundos ya que al reducirlo excesivamente, aparecen dos limitaciones. La primera es la necesidad de tomar al menos una muestra y la segunda es que la relación carga útil versus el encabezado debe mantenerse en proporciones razonables (eficiencia del paquete).

Determinado el número de canales, se traduce este valor al ancho de banda ocupado en la red mediante la utilización de la calculadora de *Erlangs*<sup>41</sup> para la tecnología de VoIP.

Figura 3.2 Calculadora de *Erlangs* y Ancho de Banda en VoIP

<sup>41</sup> Tomado de la página <http://www.erlang.com/calculator/eipb/>

Estos valores se calculan de acuerdo a las características de compresión del *codec* seleccionado, la duración del paquete, la medida de tráfico de voz en *Erlangs* y el porcentaje de bloqueo de llamada requerido. A través de esta herramienta (Figura 3.2) se puede ver que el ancho de banda necesario para el tráfico de voz es 144 Kbps.

Al emplear supresión de silencios VAD (*Voice Activity Detection*) se obtiene un menor ancho de banda; se consigue reducirlo incluso hasta el 50%. VAD evita que paquetes sin información de voz sean enviados; es decir, en una conversación donde normalmente se tiene intercambio de voz en ambos sentidos y donde por lo general solo una persona habla a la vez, VAD se encarga de suprimir los paquetes que carecen de información audible (silencios durante una conversación).

El *CODEC* que se utilizará en este diseño será el G.729a con VAD y con la duración del paquete de 20 milisegundos, considerado un tiempo óptimo como se explicó anteriormente; además se encuentra dentro del intervalo (10 ms < t < 30 ms) permitido para una calidad aceptable de voz.

Es así que, el ancho de banda requerido para voz será de 72 Kbps, que representa la mitad del valor obtenido mediante la calculadora.

### **3.2.1.1 Cálculo de Tráfico en Enlaces hacia la Red de Telefonía Pública**

En la central telefónica Siemens existen troncales para acceder a la red de telefonía pública. Para el cálculo aproximado de la capacidad de este enlace se puede utilizar la ecuación 3.2<sup>42</sup>:

$$NE1 = \frac{N_e * F_m}{N_c} 70\% \quad [\text{ec. 3.2}]$$

Donde: NE1 = Número de E1s.

<sup>42</sup> Tomado de la tesis "Diseño de la red de comunicaciones de la Mutualista Pichincha para la ciudad de Quito basado en tecnologías Ethernet de alta velocidad" de Mauricio Carrión

- $N_e$  = Número de extensiones telefónicas.  
 $F_m$  = Factor de multiplexación.  
 $N_c$  = Número de canales de voz por E1. Un enlace primario E1 equivale a 30 canales de voz.

El número de extensiones en la matriz de TRANSELECTRIC son aproximadamente 300. Se asume que el 30% de las llamadas son internas; es decir, no se direccionan hacia la PSTN, por lo que se tendría como tráfico exterior el 70% de todo el tráfico de voz. El factor de multiplexación será  $1/6^{43}$  en cuanto al número de extensiones que pueden acceder al exterior simultáneamente (valor medio entre un mínimo de calidad de multiplexación de  $1/8$  y un alto nivel de calidad de  $1/4$ ). Calculando:

$$N_{E1} = \frac{300 * 1/6}{30} 70\%$$

$$N_{E1} = 1.2$$

De acuerdo a lo obtenido al aplicar la ecuación 3.2, se deberán tener dos enlaces E1s hacia la PSTN. Este dimensionamiento permitirá el posible crecimiento de la Compañía y proveerá seguridad.

### 3.2.2 ESTIMACIÓN DEL ANCHO DE BANDA REQUERIDO PARA DATOS

#### 3.2.2.1 Tráfico Generado en la Red

Dentro del edificio matriz se tienen aproximadamente 400 usuarios. El personal del Directorio tiene privilegios en la utilización de la red de datos ya que poseen exclusivamente 1 Mbps para *Internet* y correo electrónico, no tienen restricciones de acceso a páginas *web* ni de envío y recepción de correo.

El área de Informática puede ingresar y modificar las bases de datos y aplicaciones informáticas tales como *Flexline*, *Apipro*, *Xnear*, *Evolution* que fueron descritas en el capítulo 2.

---

<sup>43</sup> Valor promedio tomado para calidad de multiplexación.



Talento Humano tiene acceso a *Evolution*, las bodegas a *Flexline*, las secretarías a *Xnear*, entre las áreas más destacadas. El resto de usuarios tiene permitido el ingreso a *Internet* y correo electrónico principalmente. Todos los usuarios de la red (excepto Directorio y usuarios privilegiados) tienen que pasar por el servidor *Proxy*, lo que los restringe de entrar a cualquier página que no posea autorización de la Compañía.

Como en toda red, se habla de tráfico interno y externo; actualmente se tiene una capacidad de transmisión dentro de la LAN del edificio de 100 Mbps a través de tecnología *Fast Ethernet*, por lo que no es importante considerar el tráfico interno como el acceso a base de datos o archivos compartidos que no sobrepasan este valor. En cuanto a tráfico externo se tiene fundamentalmente acceso a *Internet* y a correo electrónico.

En general se permite un ancho de banda de 3 Mbps para todos los usuarios del edificio matriz, pero se tiene reservado 2 Mbps adicionales para casos de mayor congestión. A esto se suma el 1 Mbps exclusivo para personal del Directorio.

Por lo regular, el ancho de banda asignado en condiciones normales (3 Mbps) se encuentra utilizado en su totalidad, pero no por todos los usuarios de la red sino a nivel personal; es decir, con pocos usuarios se logra el límite de asignación y eso no permite un correcto funcionamiento de la red, además se utiliza el ancho de banda para otras tareas que no son estrictamente laborales.

Incrementar el ancho de banda asignado para el edificio no solo acarrea mayores costos del servicio sino que, al no tener un control en su administración seguiría sucediendo lo mismo y sin importar el límite permitido se seguiría copando este ancho de banda.

Por ello se necesita una mejor administración del ancho de banda a través de las herramientas existentes como *PacketShaper* pudiéndose asignarlo de acuerdo a aplicaciones a ser usadas o por protocolos sin necesidad de incrementarlo; así, para cada tipo de aplicación ya sea ftp, http, etc., se debe designar un limitante de

USO.

Para conocer los valores que se están alcanzando se detallará el tráfico generado en la red mediante el monitoreo de la misma.

### 3.2.2.1.1 Tráfico por Estación de Trabajo

#### a. Tráfico Web<sup>44</sup>

En el monitoreo del ancho de banda utilizado por toda la red en *Internet* se puede observar que diariamente se tiene una utilización considerable entre las 7h00 y las 20h00, dentro de las cuales se encuentran las horas laborables y a partir de esta última comienza el tráfico a decaer.

En la figura 3.3 se puede ver los promedios del ancho de banda utilizado; así se tiene para el tráfico de entrada valores entre 1.5 Mbps y 3.0 Mbps, obteniendo un promedio en cada hora aproximadamente de 2.3 Mbps. Para la salida se tiene valores entre 1.7 y 3.2 Mbps; en cada hora aproximadamente se consume en promedio 2.5 Mbps. Sumando los promedios de entrada, se tiene en total un ancho de banda de 4.8 Mbps de la red del edificio matriz para *Internet*.

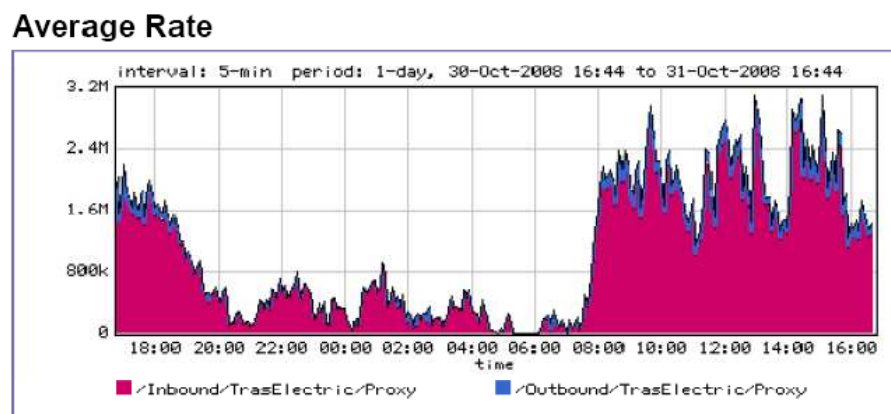


Figura 3.3 Tráfico promedio de uso de *Internet*

Como se pudo ver en la gráfica anterior se llegan a valores por encima de los 3 Mbps que se tienen asignados para *Internet*, pero al aumentar los 2 que se tienen de reserva se alcanza a cubrir los requerimientos.

<sup>44</sup> Información proporcionada por el área de Informática mediante la monitorización con *PacketShaper*

### Peak Rate

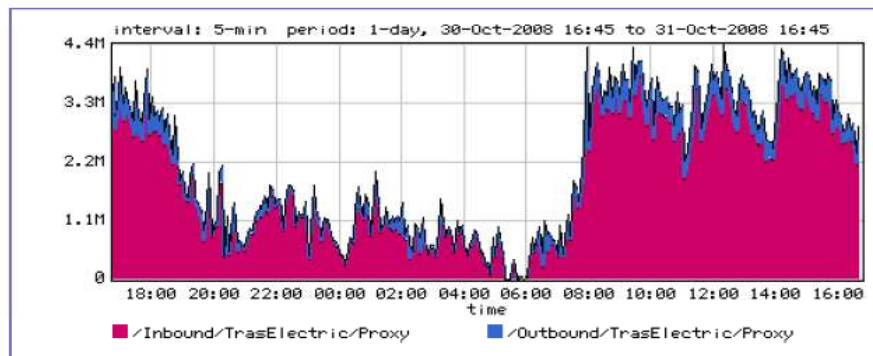


Figura 3.4 Tráfico pico de uso de *Internet*

En la figura 3.4 se pueden ver los valores picos; se observa que se llega hasta 3.5 Mbps de entrada y hasta 4.2 Mbps de salida en toda la empresa.

De los 400 usuarios conectados a los puntos de red del edificio se tiene una simultaneidad del 80%, ya que el porcentaje restante se considera como personal que está fuera del lugar de trabajo por comisiones u otros asuntos. Por lo tanto se tienen 320 usuarios simultáneos.

Si se divide el valor total de ancho de banda de *Internet* para los 320 usuarios permanentes se tiene un consumo promedio de 15 Kbps por cada estación de trabajo aproximadamente.

#### b. Tráfico *Email*<sup>45</sup>

### Average Rate

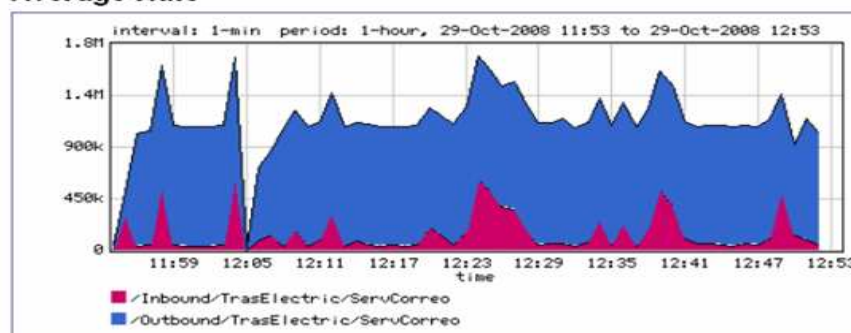


Figura 3.5 Tráfico promedio de uso de Correo

<sup>45</sup> Información proporcionada por el área de Informática mediante la monitorización con *PacketShaper*

En el monitoreo realizado en cuanto a utilización de correo electrónico, se puede observar que en una hora se tiene valores entre 180 y 600 Kbps, dando un promedio de 422 Kbps de tráfico de entrada, y valores entre 1 y 1.7 Mbps con un promedio de 1.4 Mbps de tráfico de salida (Figura 3.5). Sumando los promedios se obtiene un total de 1.822 Mbps del ancho de banda de la red del edificio matriz.

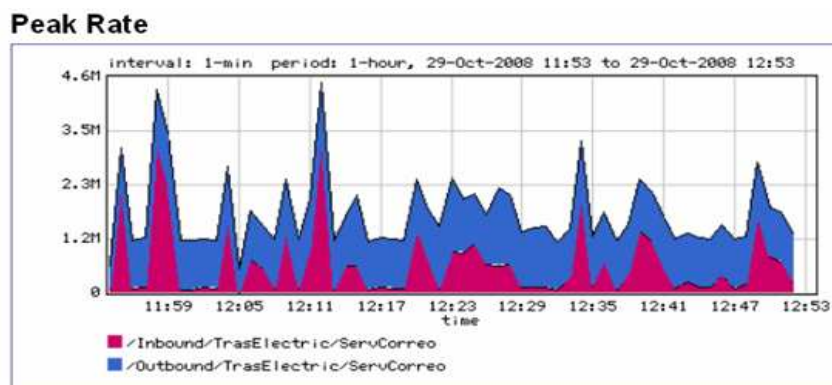


Figura 3.6 Tráfico pico de uso de Correo

Analizando la gráfica de valores pico (Figura 3.6) se puede ver que en momentos se llega hasta 3 Mbps de entrada y hasta 4.5 Mbps de salida. Si se divide el ancho total para los 320 usuarios simultáneos se tiene para correo electrónico un valor promedio de 5.7 Kbps por estación de trabajo aproximadamente.

### 3.2.2.1.2 Cálculo de Ancho de Banda en el Edificio

Se obtiene el valor total de consumo de ancho de banda de todo el edificio al multiplicar el tráfico de un usuario por el factor de simultaneidad del 80% (ausentismo por comisión) de toda la red. Con los datos obtenidos en el dimensionamiento del tráfico por estación de trabajo, se puede calcular el total del ancho de banda por usuario, para ello se suman los resultados anteriores (Tabla 3.2).

Aplicaciones	Ancho de banda (Kbps)
Internet	15
Correo	5.7
<b>TOTAL por usuario</b>	<b>20.70</b>

Tabla 3.2 Utilización de consumo de ancho de banda por estación de trabajo

Multiplicando:  $(400 \text{ usuarios} * 80\%) * 20.70 \text{ Kbps} = \mathbf{6.624 \text{ Mbps}}$ .

Se tiene un total de uso de ancho de banda de 6.624 Mbps.

Como se pudo verificar mediante el cálculo anterior, el ancho de banda requerido sobrepasa los límites permitidos (6 Mbps total); se podría concluir que el valor asignado es algo bajo para los requerimientos existentes actualmente, pero en realidad no lo es, sino corresponde al mal uso de la asignación de ancho de banda explicado anteriormente. Así, con un valor de 6 Mbps se puede tener acceso al exterior de todos los usuarios, pero considerando la necesidad de mejorar la administración de ancho de banda según el tipo de aplicaciones para no tener problema con usuarios que pueden utilizar todo el permitido en la red.

### **3.2.2.2 Estimación de Tráfico a 10 Años**

Un punto importante en el diseño de la red es la estimación de tráfico a futuro, ya que se debe asegurar un correcto funcionamiento de la misma; para ello, se considerará una proyección de crecimiento anual del 1%<sup>46</sup> incluyendo aumento de personal y actualización tecnológica.

Este crecimiento se lo obtiene prácticamente sobre la red de datos ya que el objetivo de este Proyecto de Titulación es enviar voz sobre la red de datos mediante VoIP y se estima que en 10 años esta migración estará completamente terminada.

Como se vio en el punto 3.2.1 en cuanto a VoIP y en el punto 3.2.2.1.2 en cuanto a la red de datos se tiene en total un tráfico actual de **6.624 Mbps**.

Mediante estos datos y la ecuación 3.3<sup>21</sup> se estimará el crecimiento de tráfico en un período de 10 años.

$$T_f = T_o (1 + f_c)^n \quad [\text{ec. 3.3}]$$

---

<sup>46</sup> Crecimiento máximo dado en los últimos años en la Compañía.

Donde:

$T_f$	=	Tráfico proyectado a n años
$T_o$	=	Tráfico inicial actual
$f_c$	=	Factor de crecimiento anual (1%)
$n$	=	número de años

En la tabla 3.3 se muestran los resultados de crecimiento a 10 años.

Años (n)	Tráfico final (Tf) en Mbps
1	6.690
2	6.757
3	6.825
4	6.893
5	6.962
6	7.032
7	7.102
8	7.173
9	7.245
10	7.317

Tabla 3.3 Estimación de tráfico del edificio matriz a 10 años

La figura 3.7 muestra gráficamente los resultados de estimación de tráfico.

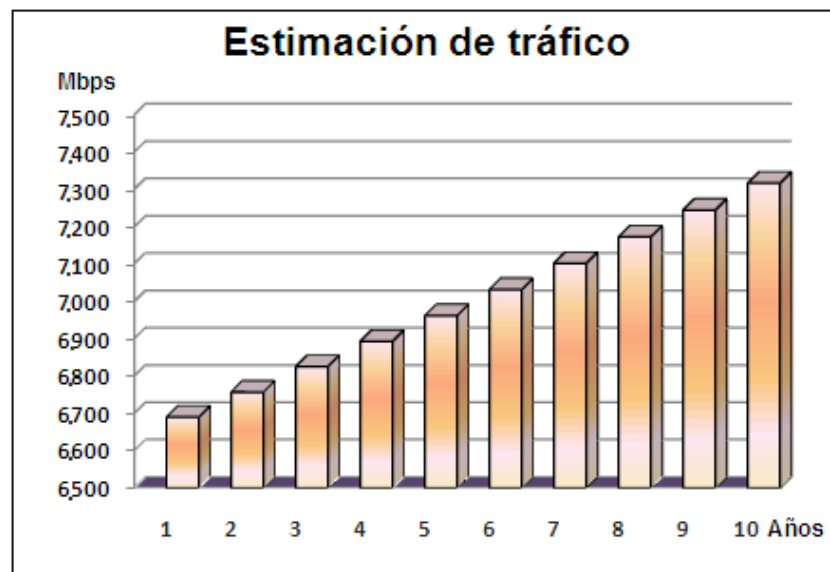


Figura 3.7 Estimación de tráfico del edificio matriz a 10 años

### **3.3 DISEÑO DE LA RED LAN DEL EDIFICIO PRINCIPAL**

Para el diseño de la red LAN de TRANSELECTRIC S.A. se mantendrá un esquema jerárquico por niveles, en donde se especificarán los componentes necesarios para las capas de *core*, distribución y acceso.

Se propondrá un esquema que provea mayor disponibilidad y para ello se tendrá redundancia de equipos en la red.

Se usarán las tecnologías *Fast Ethernet* (100 Mbps), *Gigabit Ethernet* (1000 Mbps) y 10 *Gigabit Ethernet* (10000 Mbps), debido a que están entre las soluciones de *Networking* más utilizadas hoy en día y proporcionan una buena velocidad de transmisión a un costo aceptable. A su vez, permiten escalabilidad y movilidad de la red de manera dinámica y eficiente sin causar mayores problemas.

#### **3.3.1 CABLEADO ESTRUCTURADO**

Con los requerimientos presentados en el punto 2.3.1 se llegó a la conclusión de rediseñar el sistema de cableado estructurado y adecuarlo a las necesidades actuales de la Compañía. En este caso, donde el cableado tenga un óptimo funcionamiento, se reutilizará el tendido de cables que se encuentran en el edificio matriz realizando cambios para optimizar el tráfico de la red.

El diseño de cableado estructurado contemplará cinco subsistemas específicos: Distribución Principal (cuarto de equipos), Cableado Vertical, Distribución Secundaria (*racks* de ala ó cuartos de telecomunicaciones), Cableado Horizontal y Área de Trabajo de los usuarios.

##### **3.3.1.1 Subsistema de Administración y Distribución Principal**

Estará ubicado dentro del Cuarto de Equipos y permitirá la conexión del *switch* de *core* con los *switches* de distribución del edificio.

### 3.3.1.1.1 Cuarto de Equipos

Para una mejor distribución del cableado en el edificio matriz se reacondicionará uno de los “cuartos de telecomunicaciones”<sup>47</sup> actuales, llevando todos los puntos de conexión de los usuarios de los diferentes pisos del edificio a éste.

El nuevo Cuarto de Equipos del quinto piso contará con un *rack* de datos donde se ubicará un *switch* de *core*, que posteriormente se conectará al *router* (existente) para el acceso al *Internet* de todos los usuarios de la red.

También tendrá *switches* de distribución (uno que funcionará como principal y un segundo para respaldo proveyendo de redundancia a la red) que estarán conectados jerárquicamente mediante cableado vertical a los *switches* de acceso, a los cuales llegarán los puntos de red de los usuarios. Además constará de los *firewall* que actualmente se encuentran en el área de Informática. Los *patch cords* de conexión de fibra deberán tener una longitud que no exceda los tres metros de tal manera que se cumplan las normas para esta área.

Contará con ODFs para la comunicación de los *switches* de distribución con cada uno de los *switches* de los *racks* de ala. En la figura 3.8 se puede observar la conformación del *rack* de datos.

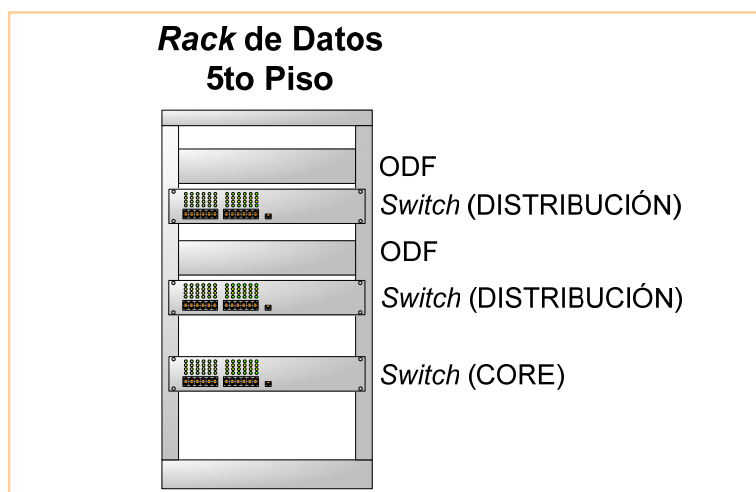


Figura 3.8 Rack de datos

<sup>47</sup> Llamado así en el capítulo 2



✓ *ODFs (Optical Fiber Distribution Frame)*

En cada uno de los *racks* del edificio se contará con ODFs que son distribuidores de fibra óptica (para el cableado vertical), con funcionalidad similar a los *patch pannels* de conexión mediante UTP. Como se mencionó anteriormente, estos ODFs permitirán la conexión de los *switches* de distribución con los *switches* de acceso y tendrán las siguientes características técnicas:

- ✓ Adaptables a un *rack* de 19".
- ✓ Diseño modular completo: Unidad de caja y bandeja de distribución.
- ✓ La fibra óptica, coleta de fibra y cables de red podrán ser supervisados claramente.
- ✓ Adaptadores como FC, SC, LC podrán ser instalados.
- ✓ Trabajar a temperaturas entre -5 y 40° C.
- ✓ Humedad relativa: ≤ 85% (30° C).
- ✓ Norma de trabajo de longitud de onda: 850 nm, 1310 nm, 1550 nm.

El *rack* de voz contendrá principalmente los *patch pannels* para la comunicación con los diferentes pisos (excepto para los que serán migrados a VoIP que son tratados como datos). En la figura 3.9 se puede ver cómo quedará el *rack* de voz.

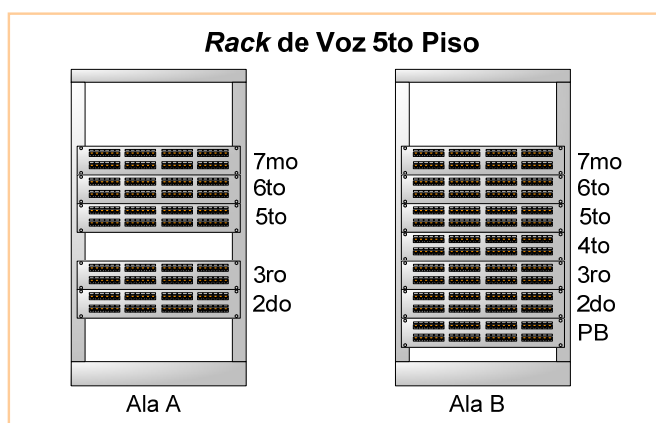


Figura 3.9 Rack de voz

Se tendrán *patch pannels* de 48 y 24 puertos de acuerdo a los puntos necesarios en cada piso; no existirán *patch pannels* de voz para el ala A de planta baja ni

para los pisos 8, 9 y 10 ya que los puntos de estos pisos serán migrados a voz sobre IP.

Dentro de las especificaciones generales del cuarto de equipos<sup>48</sup> están:

- ✓ Altura mínima de 2.60 m, idealmente 3 metros.
- ✓ No se deben tener rutas para otras instalaciones, como ductos de aire acondicionado, tubos de agua, etc.
- ✓ La puerta debe tener mínimo un ancho de 0.9 m; un alto de 2.4 m y abrir hacia fuera o ambos lados. Debe ser posible abrir la puerta desde adentro.
- ✓ No se debe utilizar techo falso en esta área.
- ✓ Debe ser ubicado en el centro del edificio (área a atender).
- ✓ Se debe colocar mínimo dos tomas eléctricas en circuitos separados.
- ✓ Las tomas eléctricas auxiliares deben estar cada 1.8 m alrededor del perímetro del cuarto, a una altura de 15 cm. sobre el suelo.
- ✓ Debe tener una barra para la puesta a tierra de 12" de largo por 2" de ancho y ¼ de espesor con huecos de ¼" conforme a la norma ANSI/EIA-TIA.
- ✓ Debe estar bien ventilado y ambientalmente controlado 24 horas al día, siete días por semana. Se debe mantener una temperatura entre 18 y 24 grados centígrados con una humedad relativa entre 30 y 55 por ciento.

El tamaño del cuarto de equipos debe estar acorde a la tabla 3.4:

Área de Servicio		Tamaño Mínimo del Cuarto	
M <sup>2</sup>	pies <sup>2</sup>	m <sup>2</sup>	pies <sup>2</sup>
500	5000	3x2.2	10x7
800	8000	3x2.8	10x9
1000	10000	3x3.4	10x11

Tabla 3.4 Área del Cuarto de Equipos<sup>[3]</sup>

El edificio se ubica en el área de 1000 m<sup>2</sup> y requiere de un Cuarto de Equipos de mínimo 3x3.4 metros; por ello, se utilizará el existente en el quinto piso que

<sup>48</sup> Especificaciones según normas de cableado estructurado

cumple con requisitos de aire acondicionado, mantenimiento de equipos, tomas de corriente, dimensiones, entre otras y se encuentra en el centro del edificio.

Se deben realizar adecuaciones como la eliminación del techo falso, cambio de tipo de piso y puertas, para cumplir con las normas establecidas internacionalmente, y proveer mayor seguridad y facilidad de mantenimiento.

Se maneja de forma separada el cuarto de equipos del quinto piso y la sala de servidores debido a que la administración del cableado está realizada por un área (Telecomunicaciones) y la de los servidores por otra (Informática).

En la actual Sala de Servidores, descrita en el capítulo 2 se tienen los servidores, éstos quedarán allí debido que están dentro del Área de Informática. Además dentro de ella se ubicará la Central Telefónica Siemens que se comunicará mediante cableado horizontal a los *patch pannels* de voz del Cuarto de Equipos y a sus demás dispositivos como bases celulares, módems, etc., ubicados en esta misma sala.

### **3.3.1.2 Subsistema de Cableado Vertical**

Interconecta la distribución principal (Cuarto de Telecomunicaciones) con la distribución secundaria (*Racks* ubicados en cada ala).

#### **3.3.1.2.1 Cableado Vertical**

El cableado vertical conectará el Cuarto de Equipos con cada piso mediante fibra óptica multimodo, que soporta hasta una distancia de 2 kilómetros sin emplear repetidores. Se utilizará un par de fibras, una de ellas para transmisión y la otra para recepción y se considerará un par de fibra óptica adicional para contingencia (se enviará a ambos *switches* de distribución).

La topología de la red se mantendrá en estrella. Este cableado será utilizado para la parte de datos y para el servicio de VoIP. Los *racks* de cada ala se ubicarán cerca a los ductos por donde pasan los cables; sin embargo, para llegar a éstos se necesita recorrer una distancia aproximada de 10 metros. Esa distancia

sumada a la que debe recorrer hasta llegar al cuarto de equipos del quinto piso establece las distancias totales de la tabla 3.5, considerando que la altura piso-techo de cada ala es de 3 metros, la distancia *rack-techo* es de 1.5 metros.

Por ejemplo desde PBA:

$$1.5_{(\text{ala; rack-techo})} + 10_{(\text{distancia interna})} + 12_{(4\text{pisos-techo})} + 1.5_{(\text{c.e.; rack-techo})} = 25 \text{ metros.}$$

Piso	Distancia en metros	
	Ala A	Ala B
PB	25	25
2	22	22
3	19	19
4	-	16
5	13	13
6	16	16
7	19	19
8	22	22
9	25	25
10	28	28
<b>Total</b>	<b>394</b>	

Tabla 3.5 Distancias aproximadas de fibra óptica para el cableado vertical

Entre las especificaciones generales para el cableado vertical se tiene que la fibra óptica multimodo será del tipo 62.5/125 con la respectiva protección, con los pares necesarios para transmisión y recepción.

Todas las fibras terminarán en ambos extremos con conectores del tipo SC ó LC. El radio mínimo de curvatura para el cable no deberá ser violado, se realizarán pruebas antes de colocarla.

✓ *Fibra Óptica Multimodo 62.5/125*

La tabla 3.6 indica las características que tendrá la fibra óptica a utilizarse para el cableado de *backbone*.

Fibra Óptica	Multimodo 62,5 $\mu\text{m}$
Recubrimiento primario	Acrilato
Atenuación óptica típica en 850 nm	3.0 dB/km
Atenuación óptica máxima en 850 nm	3.5 dB/km
Atenuación óptica típica en 1300 nm	1.0 dB/km
Atenuación óptica máxima en 1300 nm	1.5 dB/km
Diámetro del núcleo	$(62.5 \pm 3) \mu\text{m}$
Diámetro del revestimiento	$(125 \pm 2) \mu\text{m}$
Diámetro del recubrimiento primario	$(245 \pm 10) \mu\text{m}$
Ancho de banda en 1310 nm	500 MHz.km
Ancho de banda en 850 nm	200 MHz.km
Apertura numérica	$0.275 \pm 0.015$
No circularidad del núcleo (máxima)	6 %
No circularidad del revestimiento (máxima)	2 %
Error de concentricidad de núcleo/revestimiento	6 %
Error de concentricidad fibra/recubrimiento	12 $\mu\text{m}$

Tabla 3.6 Características de la fibra óptica<sup>[4]</sup>

Las demás características de las fibras cumplen con las recomendaciones del ITU-T G.651 para fibra óptica multimodo.

✓ *Interferencias Electromagnéticas*

Los sistemas de canalización para cableado de la infraestructura de telecomunicaciones serán enrutados de tal manera que se evite interferencias electromagnéticas o ruido ambiental eléctrico siempre que sea posible.

✓ *Canaleta Metálica*

- Sin división interna que le permita separar la parte eléctrica de la parte de datos.
- Alta resistencia a la corrosión.
- Cumplir con el porcentaje del 60 % de ocupación de acuerdo al estándar TIA-EIA.

Para el servicio de voz convencional se usará cable UTP categoría 5E porque

este medio de transmisión ya está instalado en el edificio y aún se considera en buen estado; solo en pisos donde se iniciará la migración a VoIP y se tiene conectados los usuarios a la red de datos, se utilizará el *switch* de acceso y se tendrá el cableado vertical mediante fibra óptica.

No se utiliza otros tipos de cables para no separar la red de voz con la de datos sino por el contrario y a su vez reutilizar recursos de red.

### **3.3.1.3 Subsistema de Distribución Secundario**

Permite la interconexión del cableado vertical con el horizontal. En cada ala de cada piso se tendrá un *rack* de acceso, *patch pannels* de conexión de categoría 5E para los pisos sin migración o 6 para los que inicien el cambio de voz a VoIP y *switches* de acceso. Posee subsistemas de administración secundaria vertical y horizontal.

El vertical constará del *patch pannel* de fibra óptica (ODF) para datos que llega del quinto piso mediante un par de fibra con conectores tipo SC ó LC, éstos deberán tener tapas de protección contra la humedad y daños físicos de la fibra. El horizontal tiene los *patch pannels* que permitirán la comunicación de los *switches* de acceso con las estaciones de trabajo y demás dispositivos de usuarios.

Con respecto a la parte de voz se tendrá lo mismo que en la de datos pero se transmitirá voz sobre IP para ciertos usuarios como se ha mencionado a lo largo de este capítulo. Es decir, se conectará verticalmente desde estos ODFs hacia los *switches* de distribución y horizontalmente a los *patch pannels* que se conectarán a los teléfonos IP.

#### **3.3.1.3.1 Rack de Ala**

Para una mejor distribución y facilidad de administración del cableado se propone la instalación de un *rack* en cada ala, que estará compuesto por los elementos que se muestran en la figura 3.10

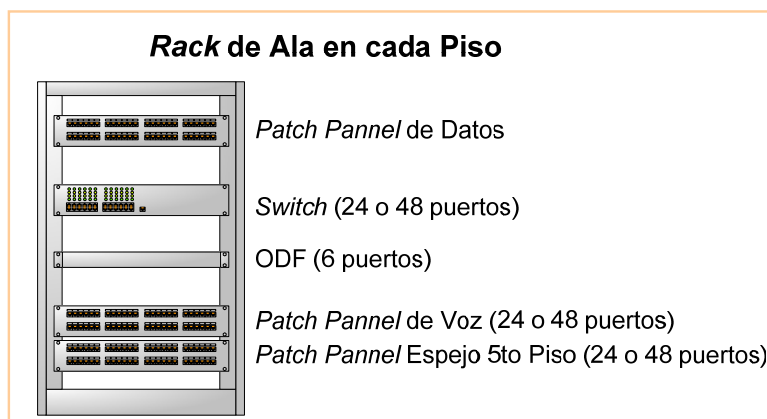


Figura 3.10 Elementos del *rack* de ala

1 *Patch Pannel* para datos.

1 *Switch* de 24 o 48 puertos de acuerdo a requerimientos.

1 ODF de 6 puertos para la comunicación a través de fibra óptica de los subsistemas de distribución principal con el de distribución secundaria.

1 *Patch Pannel* de 24 o 48 puertos para voz.

1 *Patch Pannel* de 24 o 48 puertos usado como espejo del *patch pannel* del piso 5.

Los *patch pannels* de voz serán utilizados para los puntos de voz convencional que se encuentran en la central telefónica Siemens, ya que esta parte de la red de voz no será modificada. Al *switch* de acceso se conectarán puntos de datos y los que transmitirán voz sobre IP, éstos estarán agrupados en VLANs diferentes respectivamente.

De acuerdo con los datos de la tabla 3.7 se tiene una cantidad de puntos a instalar (faltantes, sin funcionamiento o por migración a cat6), cortar (correcto funcionamiento a los *racks* del cuarto de equipos pero no poseen su propio *rack* de ala) y certificar (puntos que se encuentran conectados a un *switch* propio de ala).

Estos datos se obtuvieron al realizar el muestreo de puntos de datos en el capítulo 2.

Piso	Ala	# puntos datos	Nuevos	Cortar e Instalar	Certificar	Observaciones	
PB	A	11	11	0	0	VoIP con cat6	
	B	40	0	40	0		
2	A	32	0	0	32	switch propio	
	B	24	0	0	24	switch propio	
3	A	29	0	0	29	switch propio	
	B	26	0	26	0		
4	A	-	<b>TERMOPICHINCHA</b>				
	B	13	2	11	0		
5	A	29	3	26	0		
	B	37	0	0	37	switch propio	
6	A	27	0	27			
	B	27	3	24	0		
7	A	-	<b>REMODELACIÓN</b>				
	B	21	1	20	0		
8	A	19	19	0	0	VoIP con cat6	
	B	19	19	0	0	VoIP con cat6	
9	A	27	27	0	0	VoIP con cat6	
	B	25	25	0	0	VoIP con cat6	
10	A	22	22	0	0	VoIP con cat6	
	B	17	17	0	0	VoIP con cat6	

Tabla 3.7 Puntos a instalar, cortar o certificar

Para la comunicación de las máquinas de los usuarios a los puntos de red en los módulos de acceso de pared, desde los módulos al *patch panel* y de estos últimos a los *switches* de ala se utilizará cable UTP categoría 5E que es la que está actualmente en uso y 6 para los nuevos puntos a instalar en los pisos de migración a VoIP, como se mencionó anteriormente. Cabe aclarar que para los pisos que se utilice categoría 6 se lo hará en todo su recorrido horizontal y con todos los elementos respectivos, por lo que en ningún momento interactúan entre 5E y 6 perdiéndose la mayor de ambas. Los conectores a utilizar serán RJ-45, cumpliendo con las normas indicadas anteriormente y las características técnicas presentadas a continuación:

- ✓ Para los cables que se van a certificar:
  - Cable UTP de 4 pares, 8 conductores, trenzado, Categoría 5E, calibre #24 AWG, tipo sólido CM.



- Diseñado bajo estándar ANSI/TIA/EIA (Especificaciones de la marca Next señaladas en la tabla 3.8).
- Probado hasta 350 Mhz.
- Traer impreso las especificaciones en el cable.
- Probada y habilitada su conexión tanto a los puntos eléctricos como a los puertos del *switch*.

Frequency MHz	Att. Solid	Pr-Pr NEXT	PS NEXT	Prop. Delay ns	Delay Skew ns	Return Loss	Pr-Pr ELFEXT	PS ELFEXT
1	2.0	65.3	62.3	538.5	45	20.0	63.8	60.8
10	5.9	50.3	47.3	545.0	45	25.0	43.8	40.8
16	8.0	47.3	44.4	539.9	45	25.0	39.7	36.7
20	9.2	45.8	42.8	540.2	45	25.0	37.7	34.7
25	10.6	44.4	41.3	540.8	45	24.3	35.8	32.8
31.25	11.7	42.9	39.9	541.4	45	23.6	33.9	30.9
62.5	17.0	38.4	35.4	542.5	45	21.5	27.8	24.8
100	22.0	35.3	32.3	543.0	45	20.1	23.8	20.8

Tabla 3.8 Características de cable UTP categoría 5E (Marca Next)<sup>[5]</sup>

✓ *Para los cables que se van a cortar:*

- Las características técnicas de estos cables son las mismas de los que únicamente deben certificarse.
- De igual manera se probó el correcto funcionamiento en ambos extremos del cable y al responder sin problemas en distancias largas también son aptos para conectarlos directamente a un *switch* de ala.

✓ *Para los cables que se van a instalar:*

- Cable UTP de 4 pares, 8 conductores, trenzado, Categoría 6, calibre #23 AWG, tipo sólido CM.
- Probado hasta 350 Mhz.
- Bajo los estándares de categoría 6 ANSI/EIA-TIA.
- Deberán traer impreso claramente el código de colores de la norma que cumplen los ya instalados.

✓ *Patch Pannel de Datos*

Cumplirán con el estándar mínimo TIA/EIA-568-B. Cada puerto deberá contener una etiqueta universal codificada para esquemas de cableado T568A y T568B. Se instalarán en un *rack* estándar de los existentes en el cuarto de equipos y en los *racks* de ala. Contendrán áreas para identificación de puertos y *panel* (Figuras 3.11 y 3.12).



Figura 3.11 *Patch Pannel* de 48 puertos<sup>[6]</sup>



Figura 3.12 *Patch Pannel* de 24 puertos<sup>[6]</sup>

✓ *ODFs*

Los ODFs que estarán presentes en el *rack* de ala deberán ser de 6 puertos con las especificaciones antes mencionadas en el punto 3.3.1.1.1.

✓ *Conectores RJ-45*

Tanto las salidas para datos como las de voz usan conectores RJ-45 CAT 6, los mismos que cumplen los requerimientos establecidos en el estándar ANSI/EIA-TIA.

Para la comunicación de los teléfonos convencionales al punto de voz se utilizará cable telefónico con conectores RJ-11, mientras que para los teléfonos IP se usará cable de red UTP con conector RJ-45.

### **3.3.1.4 Subsistema de Cableado Horizontal**

Permite la interconexión del *rack* de ala de cada piso con el subsistema de estaciones de trabajo o puntos finales de los usuarios de la red. Compuesto por una red en estrella definida con cables UTP categoría 5E ó 6 (de acuerdo al caso) y módulos de acceso de pared (cajetines).

Los módulos de acceso cuentan con puntos dobles de cable UTP, uno para la transmisión de datos conectado por un *patch cord* al computador y otro conectado al teléfono IP o al teléfono común. La distancia del cable no debe ser mayor a 90 metros en los existentes y de igual manera se cumplirá con los puntos que requieran instalación o corte para llegar al *switch* de cada ala.

El cableado horizontal estará distribuido a través del techo falso y canaletas en los diferentes pisos del edificio.

#### **3.3.1.4.1** *Cableado Horizontal*

De acuerdo a las pruebas realizadas en el capítulo anterior, las distancias de los cables que conectan los módulos de pared a los *switches* de acceso en cada ala están entre los 13 y 30 metros, lo que indica que se encuentran dentro de las normas para cableado horizontal (90 metros). Así, se justifica que los puntos de datos que están conectados a *switches* propios y que funcionan correctamente únicamente deben ser certificados.

De igual forma que para los otros subsistemas, no se mezclarán categorías en cuanto al medio de transmisión sino que el cableado horizontal será de categoría 6 para los nuevos puntos y 5E para los existentes. Posteriormente se terminará la migración a categoría 6, para proveer mejores características y funcionalidades, además permitirá el cambio total de telefonía convencional a VoIP.

Se mejorará y completará la red de tal manera que cumpla en su totalidad con las normas especificadas para cableado horizontal descritas a continuación<sup>49</sup>:

- ✓ Debe atender a las especificaciones y normas contenidas en el estándar EIA/TIA 568-B para cableado UTP categoría 6.
- ✓ Desde el *rack* de ala partirá en forma de estrella el tendido de cableado horizontal a cada uno de los puntos de datos de los usuarios de la red empleando cable UTP categoría 6.

---

<sup>49</sup> Características para nuevo cableado horizontal categoría 6

- ✓ El *patch pannel*, los conectores usados en los módulos de acceso de pared, así como los *patch cords* deberán ser categoría 6.
- ✓ La manipulación de los cables UTP, se deberá realizar con cuidado y siguiendo todas las recomendaciones del fabricante.
- ✓ Se definirá un sistema de identificación mediante letras y números con etiquetas, desde los *patch pannels* en el *rack* de ala hasta los puntos finales a nivel del usuario con la finalidad de facilitar la administración de la red.
- ✓ Para el sistema de canalizaciones horizontales y verticales, se dispondrá de un ducto principal que recorrerá cada una de las plantas a lo largo de éstas y se llevarán los cables hacia cada destino, empleando canaletas plásticas para áreas visibles e interior de las oficinas. La altura de los módulos de acceso de pared desde el piso debe ser de 30 - 45 cm.
- ✓ Se hará especial énfasis en ocultar al máximo las canalizaciones a instalar y en no deteriorar los ambientes en las oficinas.
- ✓ Todas las tuberías cumplirán con las condiciones de separación de 20 cm de cualquier línea AC, 12 cm de balastos de lámparas fluorescentes, 1 metro de cualquier línea AC de más de 5 KVA y 1.2 metros de cualquier motor o transformador, aire acondicionado, ventiladores, calentadores.
- ✓ La distancia a la toma de telecomunicaciones no excederá los 90 metros.

En la tabla 3.9 se indica la cantidad de cables que pasan en una tubería según la norma ANSI/EIA-TIA 569.

Medida de la tubería		Número de Cables. Diámetro externo del cable UTP: 6,1 mm (0.24 pulgadas)
Cm	Pulgadas	
1.6	½	0
2.1	¾	3
2.7	1	6
3.5	1 ¼	10
4.1	1 ½	15
5.3	2	20
6.3	2 ½	30
7.8	3	40

Tabla 3.9 Cables permitidos en las tuberías<sup>[7]</sup>

Es importante conocer estos datos para evitar un mal manejo de los cables y evitar roces excesivos al momento de la instalación (nuevos a instalar y mejoramiento de los existentes).

### **3.3.1.5 Subsistema de Estaciones de Trabajo**

Permite la conexión de los equipos de usuario y estaciones de trabajo (computadores, *fax*, teléfonos, etc.) a los módulos de acceso de pared.

Los cables a utilizar desde los puntos de pared a los equipos deben ser de distancias no menores a 2 metros y máximo 3 metros. Debido a que actualmente se cumplen estas distancias, no se requiere cambiar completamente las conexiones sino en un mínimo porcentaje.

### **3.3.1.6 Planos del Edificio con el Nuevo Cableado**

Como se estableció anteriormente, se tendrán *racks* de ala que estarán ubicados en un lugar central para los puntos de red de los usuarios, de tal manera que no excedan los 90 metros en cableado horizontal; de igual manera estos *racks* deberán estar cercanos al Cuarto de Equipos.

En la figura 3.13 se señala donde se encontrará el *rack* del piso 6 ala B. En cada uno de los pisos se tratará que la ubicación sea aproximadamente la misma.

Se eligió este sitio porque es un punto cercano al cuarto de equipos; de preferencia se lo colocaría en la sala de reuniones pero debido a que ésta se encuentra en el centro del área y es pequeña no es factible ubicarlo aquí, además por el hecho de reutilizar parte del cableado se pondrá el *rack* cerca al ducto de cables donde pasan la mayor cantidad de ellos a los puntos de usuario.

Los números en rojo que se pueden ver en la figura son los cajetines existentes para la comunicación de los usuarios a la red. Adicionalmente en cada cajetín se identificará qué puntos contiene, esto se lo realizará para tener una mejor organización de los mismos; se tendrá la misma etiqueta en los *patch panels* para identificarlos a qué punto se conectan. Por ejemplo para esta área se tendrá

la etiqueta 6B que identifica el ala B del sexto piso y de acuerdo al cajetín se identificará al punto de voz o de datos con el mismo número; así, para el cajetín 1 se tendrá 1V1D que significa punto de voz del cajetín 1 y punto de datos del cajetín 1; se realizará lo mismo para cada uno de ellos en todas las alas del edificio. En el anexo 3.1 constan los planos de todo el edificio especificando los puntos de voz y datos y la ubicación del *rack* de ala.

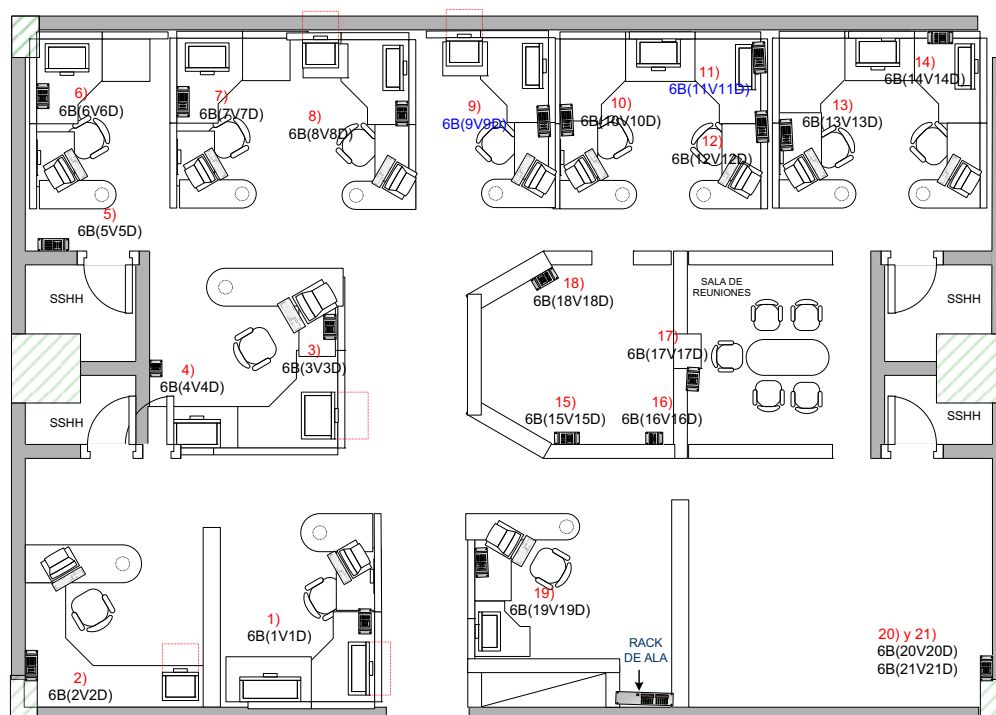


Figura 3.13 Ubicación del rack de ala

### 3.3.2 DISEÑO DE LA RED ACTIVA

#### 3.3.2.1 Elementos Activos a Utilizarse

Para cumplir con los requerimientos actuales y futuros especificados en el capítulo anterior, se tendrá en la parte activa *switches* de *core*, de distribución y de acceso para lograr una mejor organización y rendimiento de la red.

Los servidores serán los mismos ya que en su mayoría han sido adquiridos recientemente. Los pocos servidores que estaban desactualizados, están siendo reemplazados por nuevos equipos.

Con respecto a las estaciones de trabajo, actualmente todas son *Pentium 4*, las que no lo eran, están siendo reemplazadas por tecnologías superiores.

#### **3.3.2.1.1** *Cuarto de Equipos*

En el cuarto de equipos, dentro de la parte activa, se colocarán dos *switches* de distribución los cuales se acoplarán a través de enlaces 10 *Gigabit* al *switch* de *core* y a la central telefónica Siemens, por lo que deberán tener puertos de alta velocidad. Los puertos 10/100/1000 *Ethernet* se conectarán a los ODFs para la comunicación con los *switches* de acceso (Figura 3.17).

Se tendrán dos *switches* de distribución para proveer alta disponibilidad mediante redundancia de equipos.

Entre las principales características técnicas que deberán tener los *switches* de distribución están:

- ✓ Soportar *switching* de capa 2 y 3.
- ✓ Ofrecer auto-sensado y auto-negociación en las interfaces.
- ✓ Tener puertos 10/100/1000 *Ethernet* y 10 *Gigabit Ethernet*. Para este caso es necesario 24 puertos *Gigabit Ethernet* y 2 ó 4 puertos 10 *Gigabit Ethernet*.
- ✓ Permitir una transferencia de velocidad alta.
- ✓ Tener componentes redundantes.
- ✓ Permitir políticas de seguridad y listas de control de acceso (ACLs).
- ✓ Agrupación de enlaces.
- ✓ Calidad de servicio (QoS).

Debido a que el *switch* de *core* se conectará a los *switches* de distribución, a los servidores y al *router* que dará salida para *Internet* (Figura 3.17), éste deberá ser capaz de transmitir a muy altas velocidades ya que debería soportar todo el tráfico de la red del edificio matriz de TRANSELECTRIC.

Dentro de las principales características técnicas del *switch* de *core* están:

- ✓ Soportar *switching* de capas 2, 3 y 4.
- ✓ Ofrecer auto-sensado y auto-negociación en las interfaces.
- ✓ Tener puertos 10/100/1000 *Ethernet* y 10 *Gigabit Ethernet*. Para este caso es necesario 24 puertos *Gigabit Ethernet* al cual se conectarán los servidores y 2 ó 4 puertos 10 *Gigabit Ethernet* que se conectarán a los *switches* de distribución.
- ✓ Permitir una transferencia de velocidad muy alta.
- ✓ Tener componentes redundantes.
- ✓ Agrupación de enlaces.
- ✓ Calidad de servicio (QoS).

#### 3.3.2.1.2 Rack de Ala

Dentro de los elementos activos que se encuentran en cada *rack* de ala se tiene un *switch* de acceso. Estos dispositivos se conectarán a los *switches* de distribución a través de un puerto *Giga* del *switch* y a través de los puertos 10/100 *Ethernet* a las estaciones de trabajo y a los teléfonos IP (Figura 3.17).

Las principales características técnicas que tendrá el *switch* de acceso son:

- ✓ Seguridad de puertos.
- ✓ Ofrecer auto-sensado y auto-negociación en las interfaces.
- ✓ Tener entre 24 y 48 puertos 10/100 *Ethernet* de acuerdo a los requerimientos de cada ala y dos puertos 10/100/1000 *Ethernet* para la conexión con el ODF.
- ✓ Permitir VLANs.
- ✓ Soporte de protocolos tales como VTP (*Vlan Trunking Protocol*), STP (*Spanning Tree Protocol*) o PVRST+ (*Per-VLAN Rapid Spanning Tree Plus*), entre otros.
- ✓ Tener PoE
- ✓ Posibilidad de crear troncales desde cualquier puerto usando 802.1q.
- ✓ Agrupación de enlaces.
- ✓ Calidad de servicio (QoS).



Los *switches* asignados a cada piso de acuerdo al número de puntos necesarios serán:

PISO	ALA	NÚMERO DE PUNTOS DE DATOS NECESARIOS	NÚMERO DE PUNTOS DE VOZ NECESARIOS	NÚMERO DE PUERTOS EN EL SWITCH
Planta Baja	A	11	9	24
Planta Baja	B	40	0	48
Segundo	A	32	0	48
Segundo	B	24	0	48
Tercero	A	29	0	48
Tercero	B	26	0	48
Cuarto	A	-	-	-
Cuarto	B	13	0	24
Quinto	A	29	0	48
Quinto	B	37	0	48
Sexto	A	27	0	48
Sexto	B	27	0	48
Séptimo	A	-	-	-
Séptimo	B	21	0	24
Octavo	A	19	17	48
Octavo	B	19	9	48
Noveno	A	27	14	48
Noveno	B	25	18	48
Décimo	A	22	16	48
Décimo	B	17	11	48

Tabla 3.10 Asignación de *switches* por ala

Como muestra la tabla 3.10, en los pisos octavo, noveno, décimo y planta baja A se señalan puntos de voz, éstos son los que actualmente pertenecen a la central Panasonic y serán migrados a VoIP como se especificó en el punto 3.2.1, por ello, se conectarán a *switches* y serán tratados como red de datos.

En la tabla 3.11 se puede observar de mejor manera las principales características de los diferentes *switches* a utilizarse:

	Access	Distribution	Core
Bandwidth aggregation	✓	✓	✓
Fast Ethernet/Gigabit Ethernet	✓		
Gigabit Ethernet/10Gigabit Ethernet		✓	✓
High forwarding rate		✓	
Layer-3 Support		✓	✓
Port security	✓		
Power over Ethernet(PoE)	✓		
Quality of Service(QoS)	✓	✓	✓
Redundant components		✓	✓
Security Policies/Access Control Lists		✓	
Very High forwarding rate			✓
VLANs	✓		

Tabla 3.11 Características de los switches de core, distribución y acceso<sup>[8]</sup>

### 3.3.2.2 VLANs

Debido a que en el edificio no se tienen VLANs, es necesario implementarlas para tener un mejor ordenamiento, administración, rendimiento y optimización del tráfico de acuerdo a los usos de las diferentes áreas que componen la Compañía.

Se deberá implementar una VLAN específica para la voz y será la misma en todos los switches para que puedan tener comunicación entre los usuarios que la componen. Además se tendrá una VLAN para el tráfico de datos la cual se encontrará en la VLAN por *default* que ya viene en los switches.

Como se puede apreciar en la figura 3.14, las VLANs se las realizará en los switches de acceso de acuerdo a los puertos a los que se conecten los diferentes dispositivos. Cabe mencionar que en los pisos del 8vo al 10mo y el ala A de PB se tendrá una VLAN para voz, ya que aquí se implementará la primera fase de la migración a VoIP.

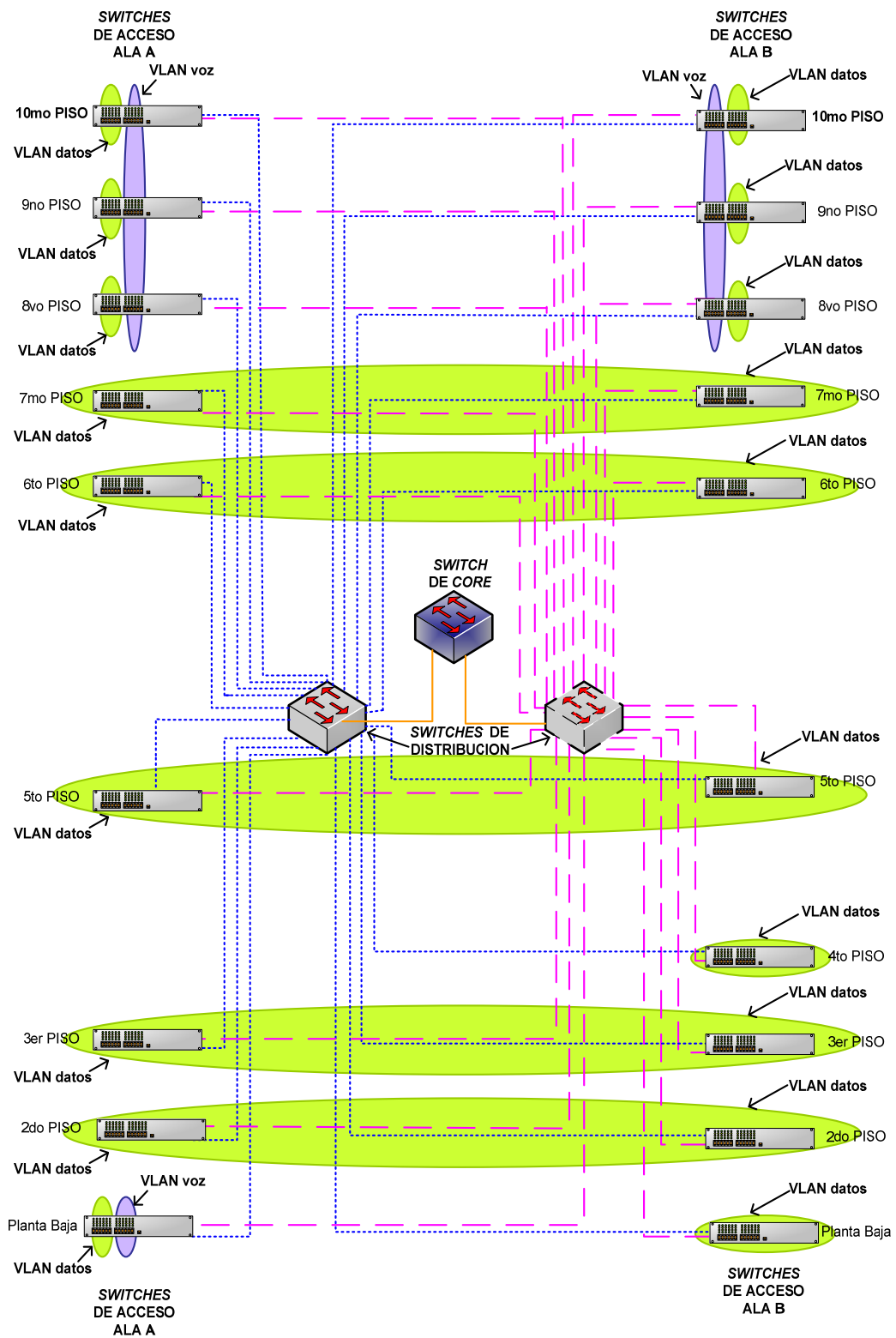


Figura 3.14 Configuración de VLANs.

### 3.3.2.3 Direccionamiento

Para simplificar la administración de la red de TRANSELECTRIC S.A., a una red grande se la puede dividir en subredes aplicando VLSM (*Variable Length Subnet Mask*) de acuerdo a las regiones administrativas y en este caso a los usuarios de cada piso (Tabla 3.12).

Piso	Número de usuarios
PB	23
2	27
3	26
4	9
5	41
6	28
7	25
8	26
9	24
10	20
Voz	94

Tabla 3.12 Usuarios que ocupan la red de TRANSELECTRIC S.A.

Se realizará un nuevo dimensionamiento en la red 172.16.2.0 /23 para optimizar el tráfico en la red. Al dividir a esta red se tendrán 510 direcciones IP válidas que se las deberá distribuir de la mejor manera.

Piso	Dirección de la subred	1a. Dirección IP válida	última dir. IP válida	Dirección broadcast	Máscara de subred
PB	172. 16. 2. 32	172. 16. 2. 33	172. 16. 2. 62	172. 16. 2. 63	255.255.224.0 /27
2	172. 16. 2. 64	172. 16. 2. 65	172. 16. 2. 94	172. 16. 2. 95	255.255.224.0 /27
3	172. 16. 2. 96	172. 16. 2. 97	172. 16. 2. 126	172. 16. 2. 127	255.255.224.0 /27
4	172. 16. 2. 128	172. 16. 2. 129	172. 16. 2. 142	172. 16. 2. 143	255.255.240.0 /28
5	172. 16. 2. 144	172. 16. 2. 145	172. 16. 2. 206	172. 16. 2. 207	255.255.192.0 /26
6	172. 16. 2. 208	172. 16. 2. 209	172. 16. 2. 238	172. 16. 2. 239	255.255.224.0 /27
7	172. 16. 2. 240	172. 16. 2. 241	172. 16. 3. 14	172. 16. 3. 15	255.255.224.0 /27
8	172. 16. 3. 16	172. 16. 3. 17	172. 16. 3. 46	172. 16. 3. 47	255.255.224.0 /27
9	172. 16. 3. 48	172. 16. 3. 49	172. 16. 3. 78	172. 16. 3. 79	255.255.224.0 /27
10	172. 16. 3. 80	172. 16. 3. 81	172. 16. 3. 110	172. 16. 3. 111	255.255.224.0 /27
Voz	172. 16. 3. 112	172. 16. 3. 113	172. 16. 3. 238	172. 16. 3. 239	255.255.128.0 /25

Tabla 3.13 Direccionamiento IP del edificio Matriz

En la tabla 3.13 se muestra el direccionamiento IP del edificio Matriz al especificar las subredes por piso que se asignarán a la Compañía. Además existirá una subred de voz la cual permitirá la agrupación de todos los usuarios que tendrán voz sobre IP.

La subred 172.16.2.0 /27 estará reservada para equipos de red y estaciones de trabajo de usuarios que tengan privilegios. Las direcciones de la 172.16.3.241 hasta la 172.16.3.255 son las que quedan libres para uso futuro.

Además, en el DHCP se reservarán desde la dirección 172.16.4.0 hasta la 172.16.6.255 para un futuro crecimiento. A su vez, la subred 172.16.7.0 con máscara 255.255.255.128 (126 direcciones IP válidas) será asignada a los servidores internos, mientras que la subred 172.16.7.128 /25 se la usará para la *wireless* del 10mo. Piso en donde se encuentra el Directorio de la Compañía.

Los *switches* de acceso enviarán una petición de asignación de dirección IP a los *switches* de distribución, los cuales, valiéndose de la opción *dhcp-helper* se conectarán con el servidor DHCP para la petición de la dirección IP dentro del *pool* determinado para cada piso.

Este *switch* puede utilizar este comando ya que es de capa 3.

#### **3.3.2.4 Diagrama Jerárquico de la Nueva Red**

En la figura 3.15 se puede observar la conexión física entre los *switches* de acceso, distribución y *core*.

Se provee redundancia en las conexiones hacia los *switches* de distribución y de *core* para permitir una alta disponibilidad de la red.

En caso de que falle uno de los *switches* que actúa como primario, entrarán automáticamente a funcionar los *switches* secundarios o de respaldo.

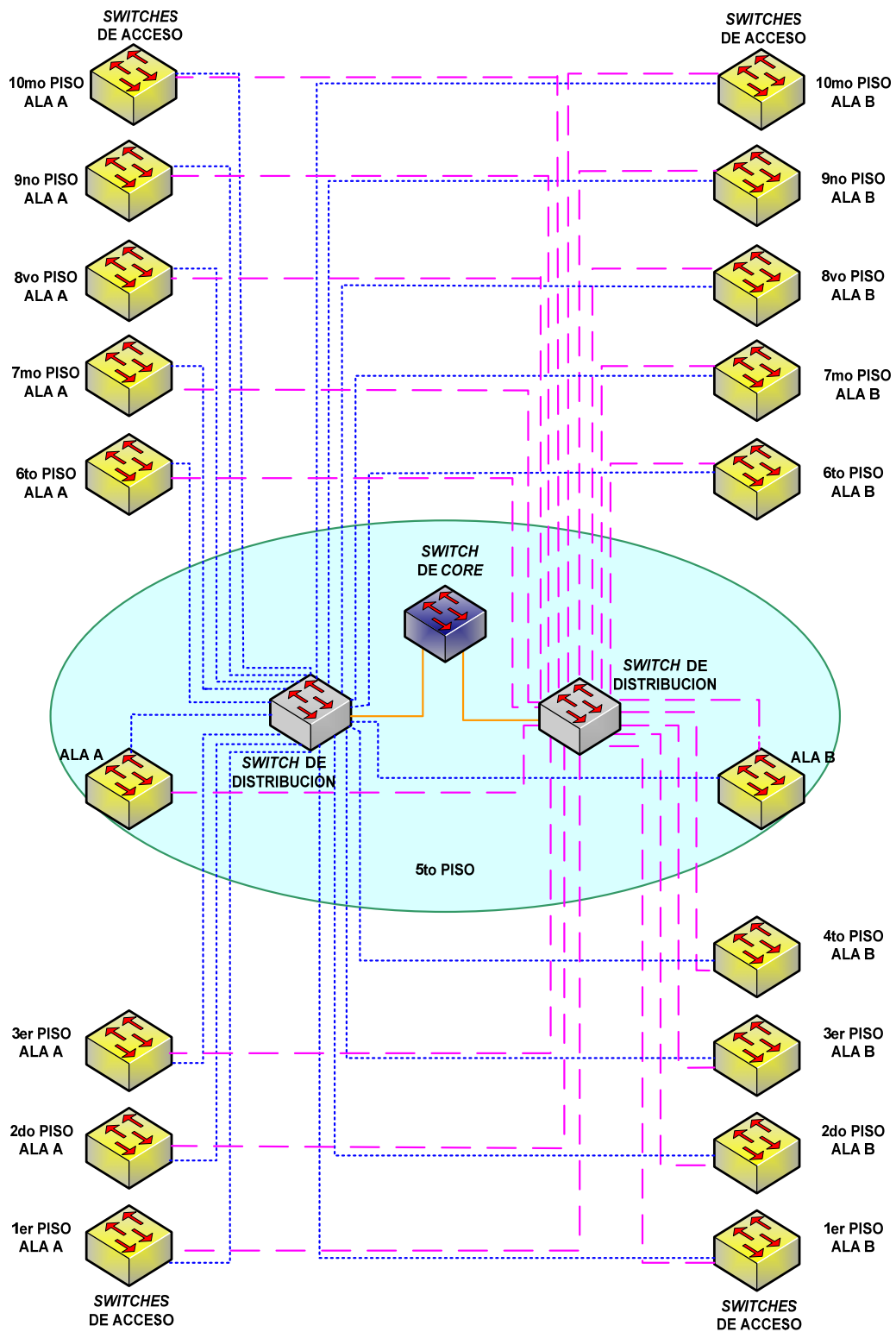


Figura 3.15 Diagrama jerárquico físico de la nueva red

### **3.3.2.5 Diagrama Físico de la Nueva Red**

La figura 3.16 muestra las conexiones que se tendrán entre los *racks* de ala con el del quinto piso.

De acuerdo a lo que se mencionó anteriormente las PCs y los teléfonos IP irán al *patch pannel* de datos, que posteriormente se enlazarán a los puertos 10/100 Mbps del *switch* de acceso correspondiente.

Por medio de los puertos Gbps del mismo se conectará mediante fibra óptica multimodo al ODF del *rack* de ala y a través de cableado vertical al ODF del quinto piso y éste a su vez a los puertos Gbps del *switch* de distribución. Por último, la comunicación entre los *switches* de distribución y el de *core* será a través de puertos de 10 Gbps.

El *router* de *Internet* y los servidores se enlazan al *switch* de *core*, así éste tendrá salida hacia la red externa y a *Internet*. Se tendrán las mismas conexiones a los equipos que funcionan como secundarios que proveerán redundancia a la red para mayor disponibilidad.

Los *switches* de distribución se comunicarán a través de puertos Gbps a la PABX por medio de la cual se podrá tener comunicación interna (entre las extensiones convencionales y las extensiones IP) y externa (hacia la PSTN).

Con respecto a la red de voz convencional se conectarán los teléfonos al *patch pannel* de voz del *rack* de ala, el cual a través de cable UTP se enlazarán a los *patch pannel* de voz y espejo del quinto piso, luego a la central telefónica que también se encuentra en el mismo piso.

A la central Siemens a su vez se encuentran conectados las bases celulares.

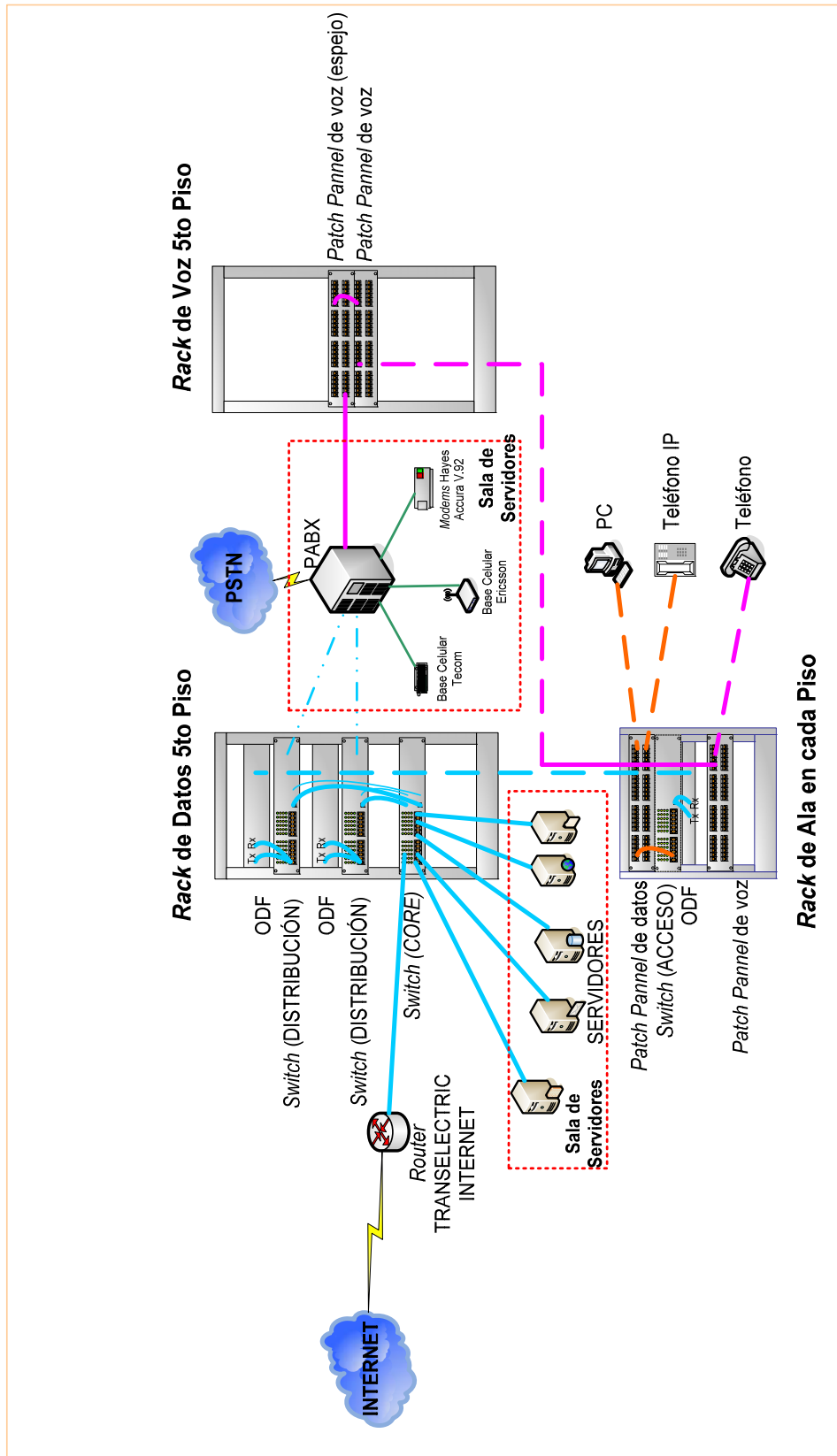


Figura 3.16 Ejemplo de conexión de una de las alas con el 5to piso



### 3.3.2.6 Diagrama de VoIP

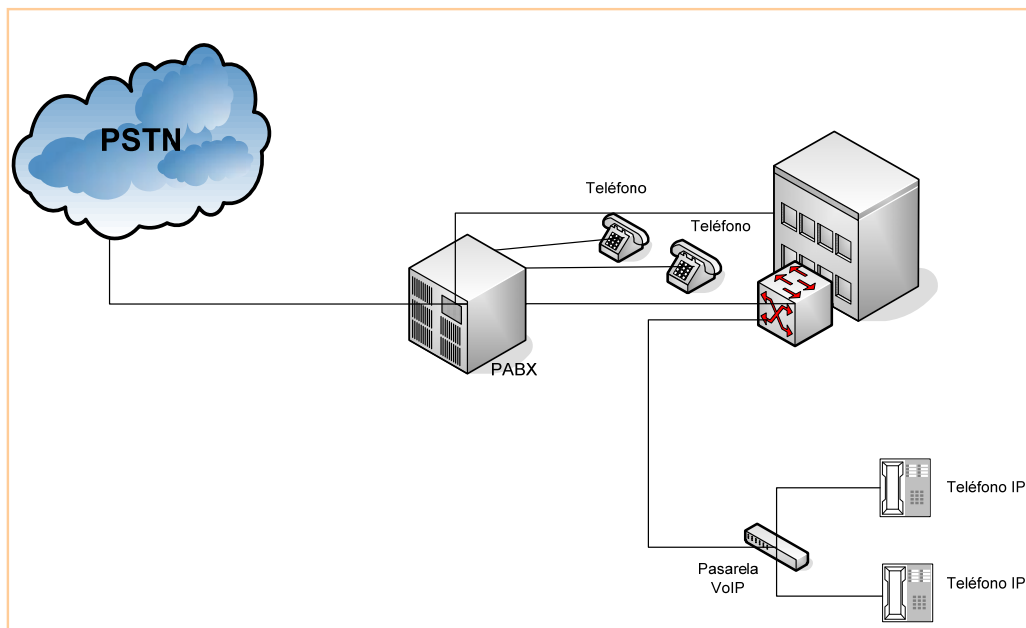


Figura 3.17 Diagrama de VoIP

La figura 3.17 indica de una manera general la comunicación de la red de voz; como se puede apreciar existen teléfonos analógicos conectados a la PABX, éstos provienen de los usuarios de telefonía convencional y también se tienen usuarios con VoIP.

Los teléfonos IP se conectarán al *switch* de acceso en cada ala y al igual que con los puntos de red pasan a los de distribución que se comunican con la PABX quien sale a la red de telefonía pública.

### 3.3.2.7 Aplicaciones, Servicios, Protocolos que soporta

Dentro de las aplicaciones y servicios que soportará la nueva red para TRANSELECTRIC S.A. se tienen las mismas aplicaciones antes mencionadas. Entre las más utilizadas se tienen *Flexline* (Sistema Integrado Administrativo Financiero), *Apipro* (Sistema para Gestión de Mantenimiento), *Evolution* (Sistema para Gestión de Personal) y *Xnear* (Diseño de Flujos de Trabajo).

Estas aplicaciones facilitan al personal tramitar permisos, gastos de seguro médico, vacaciones, pago de cheques en el caso de Tesorería, trámites de Contabilidad, Bodegas, etc.

Se proveerá de los mismos servicios tales como *Web*, correo electrónico, entre otros y se utilizarán los mismos protocolos actuales, entre ellos http, smtp, snmp, ftp, etc.

Para el caso del servicio *Web* se lo manejará de la misma manera como se lo ha venido tratando mediante la utilización de *Proxy* y *Firewall* y además limitando el ancho de banda; para el correo electrónico también se pasa por *Firewall*, se establecerán políticas, permisos, reglas y además se tendrán servicios adicionales como *antispam* y antivirus.

Además se contará, como actualmente, con el servidor de DHCP para una mejor asignación de direcciones y organización.

### **3.3.3 DISEÑO DEL ENLACE CON CALDERÓN**

#### **3.3.3.1 Dimensionamiento y Cálculo del Enlace**

La distancia existente entre el edificio matriz y las oficinas en Calderón es de aproximadamente 35 Km. A lo largo de este enlace se tiene fibra óptica que permite altas velocidades de transmisión y tráfico dentro del mismo.

En la red LAN del edificio en Quito se trabaja con tecnología *Fast Ethernet*, en la de Calderón también, y el enlace entre estos dos puntos se lo tiene mediante fibra óptica. Una de las principales y más atractivas soluciones para este acoplamiento de tecnologías es el uso de *Metro Ethernet* y más específicamente *Ethernet* sobre fibra óptica que permitirá trabajar normalmente en ambos lugares al ser considerados como una misma red LAN.

*Metro Ethernet* es una arquitectura eficiente para redes de paquetes, punto a punto, punto a multipunto y multipunto a multipunto. Las interfaces que utiliza son

de bajo costo pero ofrecen flexibilidad y escalabilidad en el ancho de banda (10/100/1000/10000 Mbps). Una de las ventajas es que al aplicar esta tecnología se puede mantener la misma estructura y jerarquía de la red (Figura 3.18).

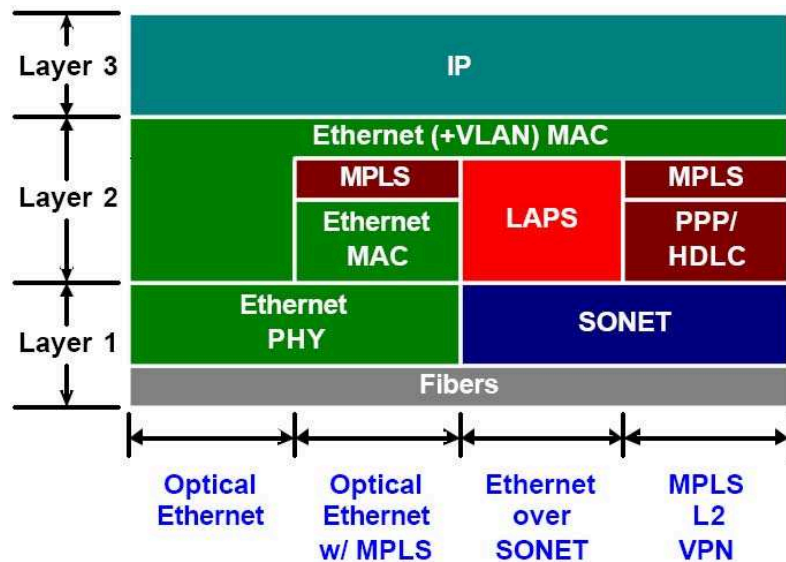


Figura 3.18 Características de *Metro Ethernet* con fibra óptica<sup>[9]</sup>

Frente a soluciones sobre circuitos convencionales, la tecnología *Metro Ethernet* (Figura 3.19) permite la interconexión entre redes locales a velocidad nativa sobre fibra óptica, con mayores niveles de flexibilidad. Esta tecnología al basarse en el *Ethernet* tradicional, resulta más sencilla de implementar y gestionar y ofrece transparencia en cuanto a protocolos con un menor costo.

## Servicios Metro-Ethernet

<b>Aplicación sobre ethernet</b>	Almacenamiento	Acceso a Internet	VPN ethernet	CESoE	Telefonía IP	VoD
<b>Servicio de conectividad ethernet</b>	Servicios E-Line y E-LAN (virtual y privado, MAN y WAN)					
<b>Tecnología de suministro de ethernet</b>	Ethernet sobre fibra óptica	Ethernet sobre SDH (NGN)	Ethernet sobre RPR	Ethernet sobre MPLS	Ethernet sobre xWDM	

Figura 3.19 Servicios de *Metro Ethernet*<sup>[9]</sup>

En la figura 3.20 se puede apreciar cómo sería el enlace hacia las oficinas del COT en Calderón. En cada lugar se tendría un equipo de cliente (CE), los cuales se conectarán entre ellos a través de un circuito virtual *Ethernet* (EVC). En este caso, los CE serán *switches* con tarjetas *metro ethernet* que permitirán la conexión de cada red LAN local con el extremo de fibra óptica que se tenga en el edificio. El EVC contendrá el interfaz de usuario de red (UNI) que será la fibra óptica que ya se encuentra tendida entre estos dos puntos.

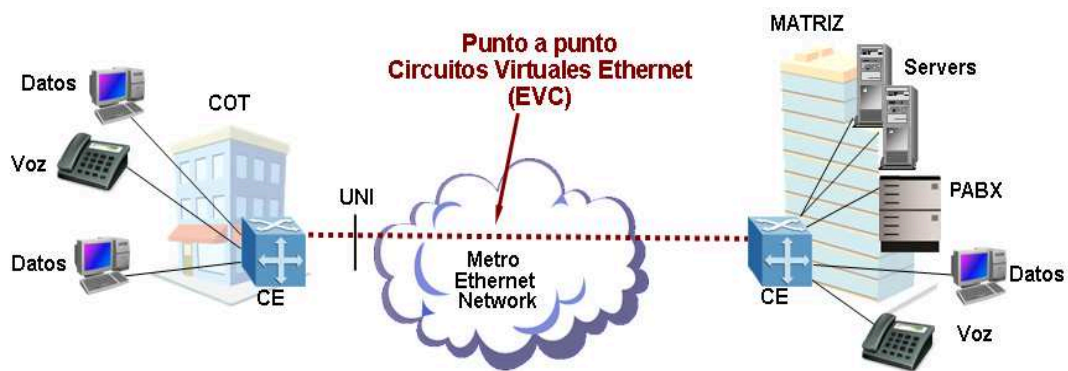


Figura 3.20 Comunicación del Edificio Matriz de TRANSELECTRIC con la oficina de Calderón

### 3.3.3.2 Dimensionamiento del Enlace

El tráfico que se maneja en estas oficinas es menor debido principalmente a que la cantidad de usuarios disminuye significativamente a 40; en cuanto a aplicaciones se tienen de igual forma *Flexline*, *Apipro*, *Xnear* y se adicionan el SGN (*Sistema de Gestión de Novedades del SNT*) y EVT (*Sistema de Eventos del SNT*). También se consideran usuarios que pueden entrar a la red *Citrix*.

Haciendo uso de la tabla 3.2 y en el peor de los casos, asumiendo que todos los 40 usuarios ingresan simultáneamente a las aplicaciones y al exterior, se tiene:

$$40 \text{ usuarios} * 20.7 \text{ Kbps} = 0.828 \text{ Mbps.}$$

Con este resultado el enlace de 100 Mbps está sobredimensionado, pero se deben considerar ciertos criterios importantes, tales como la creación de una sala

de servidores idéntica a la existente en el quinto piso del edificio Matriz; parte que no consta en este diseño debido a la integridad del proyecto pero que cabe mencionarla, así, en el caso de llegar a suceder algún evento en la principal, todos los usuarios seguirán comunicándose a dichos servidores hacia Calderón lo que generará un tráfico adicional de 7.5<sup>63</sup> Mbps aproximadamente.

Otro aspecto importante es que la fibra óptica para este enlace se encuentra ya instalada y se debe hacer uso de la misma.

### 3.4 SEGURIDAD DE LA RED

Entre los requerimientos que tiene la red está la seguridad, la misma que se podrá implementar estableciendo normas para el acceso a la información y a los equipos de conectividad, además deben permitir la protección de sistemas informáticos y *software* de administración.

La seguridad de la red debe reforzar la confidencialidad y la integridad de la información, involucra a todo el personal que es parte de la red por lo que las normas a implantarse deben ser conocidas por todos los usuarios y éstos deben tener una capacitación básica acerca de su utilización y funcionamiento.

Es primordial conocer qué es lo que se va a proteger, es decir, los elementos, equipos, herramientas, *software* e información que pueden ser principal blanco de ataque.

#### ✓ **Activos a proteger**

- Equipos de conectividad tales como *routers*, *switches*, etc.
- Servidores.
- Bases de datos.
- Licencias de *Software*.
- Respaldo de configuración de equipos y servidores.

---

<sup>63</sup> Sumado el tráfico del edificio matriz

- Equipos de Usuarios.
- Información confidencial.

✓ **Vulnerabilidades**

- Falta de seguridad física de los “cuartos de telecomunicaciones”<sup>64</sup> y cuarto de equipos.
- Claves de equipos de conectividad establecidas por *default*.
- Bajo control de acceso a base de datos.
- Falta de seguridad lógica, inapropiada administración del ancho de banda con privilegios.
- Usuarios que pueden ser administradores de equipos.

✓ **Posibles Amenazas**

- Ataques internos.
- Ataques externos.

✓ **Riesgos**

- Pérdida de información por falta de documentación.
- Salida de información por parte del personal.
- Mal uso de respaldos de las bases de datos y de información de servidores.
- Mal uso de equipos de administración de ancho de banda.
- Mal uso y falta de confidencialidad en configuración de equipos de conectividad.
- Pérdida de licencias de *software* por renovación tardía.

### 3.4.1 SEGURIDAD FÍSICA

Principalmente consiste en proteger los equipos de conectividad del cuarto de equipos, de la sala de servidores y de cada uno de los *racks* del edificio. El riesgo que se puede tener por falta de seguridad física es el robo o pérdida de los equipos o falta de funcionamiento por accesos no autorizados.

---

<sup>64</sup> Se refiere a los racks de ala de la nueva propuesta de diseño.

La seguridad física puede ser analizada en dos campos: Equipos e Información.

#### **3.4.1.1 Seguridad de Equipos**

Como se ha mencionado en el desarrollo de este diseño, se tendrá un cuarto de equipos principal en el quinto piso y *racks* de ala.

A pesar de que los *racks* estarán a la vista de los usuarios se deberá tener más control en su acceso, por ello se deberán asegurar con llave de tal manera que ningún usuario que no esté autorizado pueda manipularlos

El tener *racks* de ala ayudará a supervisar de mejor manera cualquier falla en puntos de red y pérdida de conexión de los usuarios, pero cualquier problema debería ser avisado al personal autorizado.

Después de haber analizado la situación actual de la red se llegó a la conclusión de que el cableado estructurado tiene deficiencias, principalmente de falta de organización y normas. Por ello se propone rediseñar el cableado bajo estándares que proporcionan mayor seguridad de funcionamiento de los equipos.

El edificio matriz consta de una planta eléctrica para cuando se dan fallas de red, pero entre el tiempo de falla y recuperación pueden presentarse problemas con los equipos, por ello se propone contar con UPSs en los principales equipos.

#### **3.4.1.2 Seguridad y Respaldo de la Información**

Se deben tener respaldos físicos y en discos o cintas de la información que se manipula en la Compañía de acuerdo al grado de importancia.

Es primordial respaldar la información de configuración de los equipos y de los servidores incluso hasta con tres copias en cajas de seguridad que deberán estar en cada una de las áreas que administran estos equipos. Para el caso de servidores, bajo la tutela de Informática y para el caso de equipos de conectividad y equipos de voz bajo la tutela de Telecomunicaciones.

A pesar de que se habla de áreas debe existir un par o un grupo de personas que tendrán a cargo la seguridad de esta información.

El respaldo de la información debe ser manejado a la par con la seguridad física, es decir, si solo se respalda configuraciones pero no se asegura el acceso a ellas, puede existir pérdida o fuga de esta información confidencial.

La información de configuraciones y demás respaldos debe tener un tiempo de vida, es decir, que pasado un tiempo límite (1 año máximo), esta información debe ser desechada por completo para que no existan riesgos.

De igual manera si la persona encargada de manipular esta información sale de la Compañía, se deberán cambiar las claves de acceso para configuración y verificar las facilidades de acceso remoto.

### **3.4.2 SEGURIDAD LÓGICA**

Se deberá implementar el cambio de contraseñas en el acceso a todos los equipos de red, esto incluye a servidores y equipos de conectividad.

Las contraseñas que se establezcan deberán tener normas de escritura y de intentos erróneos de ingreso.

Cuando los usuarios estén de comisión o ausentes de su lugar de trabajo temporalmente, el administrador de red deberá bloquear el equipo de ese usuario para que ninguno otro pueda acceder sin autorización. Cualquier inconveniente o problema presentado recaerá sobre el encargado de este bloqueo. A su vez el administrador puede hacer uso de las diferentes funcionalidades de *Active Directory* para realizar esto automáticamente y restringir el acceso desde su lugar de trabajo.

El diseño propuesto menciona homogenizar equipos ya sea en marca Cisco o 3Com, en cualquiera de ambas alternativas se tienen herramientas que permiten



la autorización y autenticación de usuarios al habilitar estas funcionalidades en los diferentes *switches*.

A su vez se deberá mejorar el manejo y administración de *antispam* y antivirus (*F-Secure*) para evitar virus, gusanos, troyanos que pueden afectar el rendimiento de la red. También se deberá manejar de mejor manera las funciones de los equipos de administración de ancho de banda para no tener problemas de mal uso del mismo por parte de varios usuarios que acceden a páginas de donde se descargan información que no corresponde al uso profesional.

Se deberá bloquear el tráfico por aplicaciones o por protocolos y además filtrar el contenido *web* para optimizar el uso de la capacidad de *Internet*. Al bloquear sitios *web*, éstos deben ser ingresados a una base de datos para información posterior.

El *firewall* es quien analiza los paquetes que por él circulan, por ello se deben implementar reglas que impidan el paso de paquetes maliciosos. Se deberá incluso bloquear puertos para que éstos paquetes pasen a través de los que estén abiertos. Cualquier bloqueo también puede darse por rangos de direcciones.

Se deberán instalar todos los parches de seguridad necesarios, presentados por los desarrolladores del *software* instalado, sino se puede tener la intrusión de atacantes en la información.

Ya que todos los equipos a utilizar soportan el protocolo SNMP se debería configurar una comunidad para que solo ingresen quienes están autorizados y no dejar el valor *public* configurado por defecto.

### **3.4.3 POLÍTICAS DE SEGURIDAD**

A manera de resumen y una vez mencionados los riesgos y las posibles soluciones se establecen políticas de seguridad que deben ser respetadas por cada uno de los usuarios de la red.

- ✓ Todo acceso a las máquinas de los usuarios será mediante contraseñas que tendrán validez limitada, al cabo de este período que no podrá exceder 15 días, éstas deben ser cambiadas.
- ✓ No se deberán utilizar contraseñas demasiado cortas sino al menos de 8 caracteres y deberán contener al menos una letra mayúscula, 2 números y 1 carácter especial, de tal manera que resulte difícil cualquier ataque de fuerza bruta (combinaciones posibles).
- ✓ La contraseña de red deberá ser fácil de recordar para los propietarios de la misma, pero difícil de adivinar para cualquier otra persona, además será absolutamente personal.
- ✓ Se deberá limitar los intentos de acceso erróneo de contraseña a un máximo de 3, pasado este número de intentos, el equipo deberá bloquearse temporalmente.
- ✓ Cualquier acceso a base de datos será exclusivo de personal de Informática mediante una contraseña de acceso (también temporal) que le permitirá manejar un perfil administrativo de las bases y los servidores deberán tener una dirección IP definida.
- ✓ Cualquier acceso a carpetas compartidas en la red ya sean de información o de instalación será dando acceso exclusivo por usuarios, no a todos los que se encuentren bajo el mismo dominio y cada usuario responderá por el tipo de permiso que otorgue ya sea de solo lectura o lectura y escritura.
- ✓ Para prevenir instalación de *software* sin autorización, quien utilice cada PC tendrá permisos limitados, es decir, no constará como administrador del equipo, de esta manera el personal de soporte técnico serán los únicos encargados de instalar cualquier tipo de programa necesario. Cabe indicar que por normas de la Compañía habrá excepciones en esta regla pero analizadas previamente por los administradores de red.

- ✓ Se recomienda la política de escritorio limpio, de tal manera que no se tenga a la vista información importante y que solo incumbe a quien la maneja, además cada vez que un usuario se retira de su lugar de trabajo es importante dejar bloqueando el equipo.
- ✓ Se recuerda que el uso del correo interno de la Compañía es para uso estrictamente laboral y se deberá incluir entre sus limitaciones un envío de adjuntos no mayor a 6 MB y no se podrán enviar archivos adjuntos de extensión .ppt para evitar posibles cadenas de mensajes.
- ✓ La administración de la red deberá ser exclusiva para determinados usuarios “administradores de red” ya sea de cableado, voz y datos para Telecomunicaciones y servidores, administradores de ancho de banda y *firewall* para Informática.
- ✓ Cualquier cambio o solución de problemas de red deberá ser realizado estrictamente por el personal autorizado, sino quien lo realice y no tenga esta autoridad deberá ser sancionado.
- ✓ Toda la información de equipos, cableado, servidores, central telefónica debe estar documentado de manera física y digital, de tal manera que si llegaran a suceder inconvenientes o fallas de equipos, puedan ser reemplazados temporalmente por otros solo copiando la configuración y la red pueda recuperarse rápidamente de fallas.
- ✓ Además de ofrecer un sistema de contraseñas a nivel de usuarios también se resguardarán los equipos físicamente, por este motivo se tendrá mayor seguridad en el nuevo Cuarto de Equipos principalmente, ya que dentro de éste estarán los equipos principales para el correcto funcionamiento de la red tales como *switches* de *core* y de distribución, se mantendrá este cuarto bajo dos llaves y con cámaras. La sala de servidores permanecerá de igual manera bajo el resguardo del área de Informática.

- ✓ Los *switches*, *routers*, *firewall* y otros equipos de red también tendrán acceso mediante contraseñas, pero no las que vienen en los equipos por defecto porque serían un punto débil de seguridad, además se recomienda configurar cada una de las herramientas que posean dichos equipos, es decir, eliminar en su mayoría todas las configuraciones por defecto provisto por los fabricantes.
- ✓ Establecer una sesión de acceso seguro mediante SSH eligiendo previamente la dirección a la que se debe comunicar y desde donde.
- ✓ Los *switches* de distribución que estarán en el Cuarto de Equipos y poseerán redundancia, lo que ayuda a incrementar la seguridad y disponibilidad de los servicios, así, si el principal deja de funcionar el secundario entrará inmediatamente en funcionamiento.
- ✓ Todos los equipos de red importantes tales como servidores, equipos de monitoreo, *switches* y otros estarán conectados a UPS ya sea directamente para el caso de los primeros o desde las regletas de alimentación.
- ✓ La red inalámbrica actualmente posee seguridades mediante contraseña WAP y/o WAP2, lo que la defiende de posibles ataques externos, será importante establecer contraseñas para la red inalámbrica con caducidad de máximo 1 mes.
- ✓ Es recomendable realizar un estudio de estándares de seguridad para quienes administren la red posteriormente, para de ello poder definir estos estándares y ponerlos en práctica.
- ✓ Apropiado direccionamiento IP para tener de una manera más ordenada la red de acuerdo a las necesidades y a un futuro crecimiento, esto mejora también la administración de la red.

- ✓ La utilización de un antivirus previamente probado y con ventajas a nivel corporativo puede proveer de una gran seguridad de la información y puede prevenir gran cantidad de ataques, sobre todo de los que vienen desde la red externa.
- ✓ El uso de *Proxy* y *Firewall* obliga a la restricción de páginas *Web*, lo que incrementa la seguridad.

#### **3.4.4 PLAN DE CONTINGENCIA PARA MEJORAR LA DISPONIBILIDAD DE ELEMENTOS DE RED**

Como plan de contingencia se contará con tener redundancia de equipos para poder proveer la mayor disponibilidad posible a la red. En el caso de los elementos críticos tales como *switches* se dispondrá de dos equipos de distribución. Para el caso de los servidores se tiene dispuesto en la Compañía establecer una sala de servidores idéntica a la del edificio matriz, con copias de cada uno de ellos en las oficinas de Calderón.

La seguridad que se dará al cuarto de equipos y a los *racks* de ala forma parte fundamental de este plan de contingencia.

El respaldar la información de la configuración de equipos y de servidores, permite en caso de pérdida de uno de los equipos, utilizar uno temporal que puedan reemplazar al principal.

La configuración de VLANs también es parte de este plan ya que mediante ellas se puede establecer una mejor comunicación interna entre las áreas que corresponden a cada una de las VLANs.

Para el caso de los usuarios que pasarán de telefonía tradicional a VoIP, estarán conectados a *switches*, es decir, dentro de estos *switches* de acceso se tendrá puntos de VoIP y de datos, si llegase a ocurrir un problema con este *switch*, no se perderá toda la comunicación en el área sino se podrá recurrir a los usuarios

cuyos puntos de voz y datos no pertenezcan a ese *switch* sino a otro que también posea la misma combinación.

### **3.5 ADMINISTRACIÓN Y MONITOREO DE LA RED**

#### **3.5.1 POSIBLES HERRAMIENTAS PARA LA ADMINISTRACIÓN**

Con respecto a la administración de la red se deberá habilitar SNMP que es un protocolo de gestión básico para redes TCP/IP, en los dispositivos activos para poder monitorearlos a través de herramientas tales como *What's Up*, *Loriot*, entre otros.

SNMP posee algunas versiones llegando actualmente a v3, dependiendo de la versión se puede dar mayores datos de información para la administración de equipos como nombre, comunidad, etc. Incluso en esta versión se puede proporcionar de acceso a los equipos mediante una combinación de autenticación y encriptación.

Se debe tener en adelante un monitoreo constante de la red y obtener reportes de capacidades, utilización, rendimiento, etc; para de esta manera saber si la herramienta elegida para la administración está trabajando correctamente y con los resultados esperados.

Ya que se propone una homogenización de equipos y entre las alternativas presentadas en el capítulo 4, están Cisco y 3Com, se podrá obtener herramientas de administración que proponen estos fabricantes.

Entre las características básicas que debe tener cualquier sistema de administración están:

- ✓ Se debe elegir un sistema de gestión de red que soporte todas las versiones de SNMP, para tener mayores ventajas.

- ✓ Los equipos que se utilicen para monitoreo deberán tener una cantidad de memoria que soporte este tipo de aplicaciones, actualmente no menor a 512 MB.
- ✓ Capacidad del sistema para crear mediante herramientas de desarrollo MIB's, específicas para determinados elementos de red.
- ✓ Es recomendable que el sistema de administración elegido posea compatibilidad con VLANs que se establecen en este diseño.
- ✓ Administración remota de equipos por cualquier inconveniente que pueda presentarse, pero con la debida autenticación y autorización.
- ✓ Este *software* debe ser compatible con los elementos de red tales como *routers, switches, etc.*

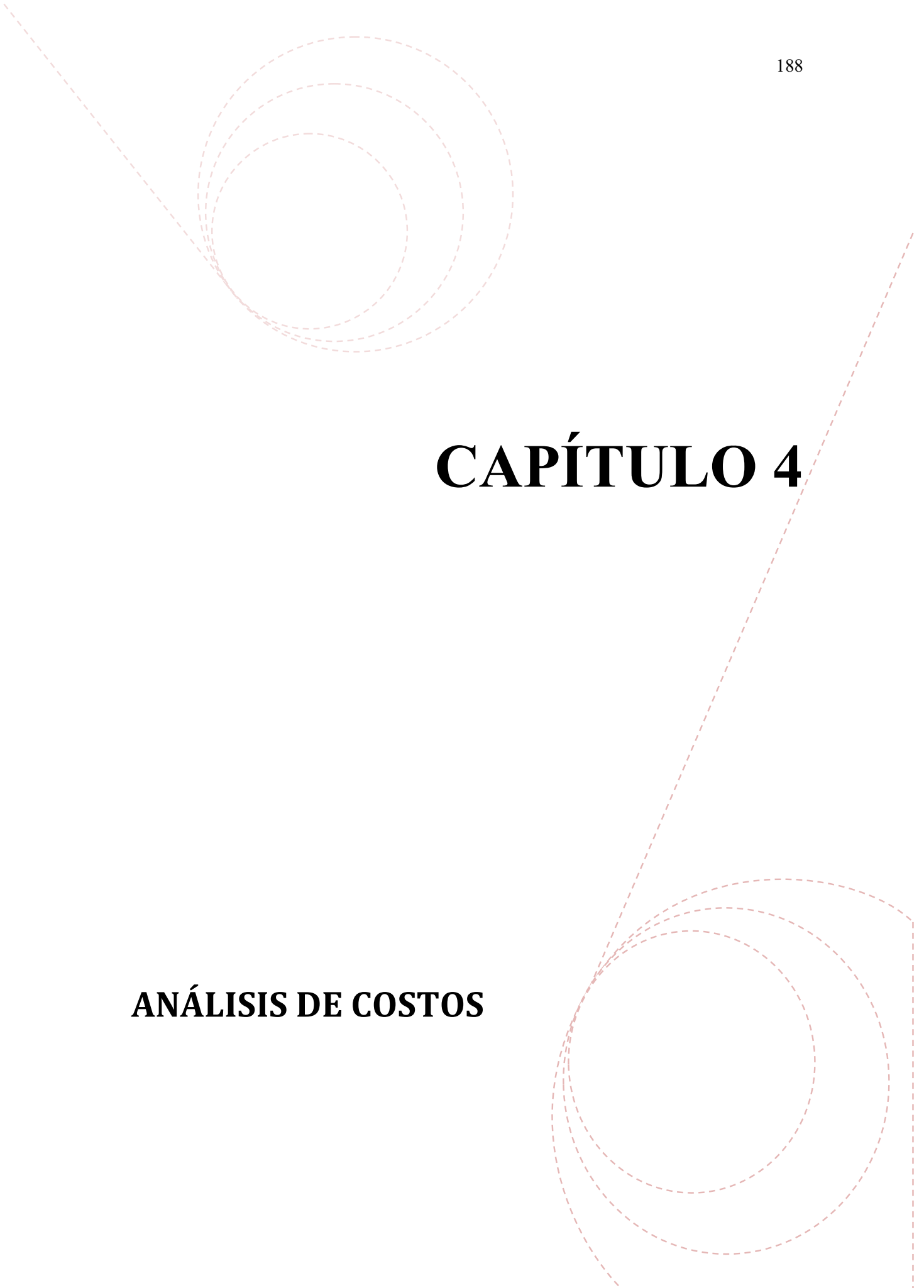
3Com posee la herramienta 3Com *Network Director* que permite esquematizar la red, administración remota, este software incluye 3Com *Network Access Manager* que permite la administración de usuarios, autenticación, permisos, entre otras funcionalidades.

Cisco posee *Cisco Works* en diferentes versiones, que también permiten trabajar conjuntamente con *What's Up* para el monitoreo de equipos, servidores, impresoras, etc. Se menciona la herramienta *Cisco Works* debido a que esta licencia la poseen actualmente en la Compañía, pero no se la está utilizando debido a la heterogeneidad de equipos activos.

Las herramientas de administración que se utilicen estarán acorde a la alternativa elegida en cuanto a equipos, la misma que se detallará posteriormente en el siguiente capítulo.

# CAPÍTULO 4

## ANÁLISIS DE COSTOS





## ANÁLISIS DE COSTOS

### 4.1 INFRAESTRUCTURA DE ELEMENTOS DE RED

En el presente capítulo se hace un análisis de costos de los equipos que pueden ser utilizados acorde al diseño realizado en el capítulo anterior; se proponen dos alternativas de los mismos incluyendo marcas de reconocido prestigio en el medio.

En su mayoría los equipos que actualmente forman parte de la red LAN del edificio matriz son Cisco y 3Com. Las opciones presentadas serán una homogenización de cada una de las dos marcas; así, se reutilizarán los equipos existentes de la una o de la otra.

Para el desarrollo de este capítulo se ha consultado a varias empresas proveedoras de equipos de *networking* y de elementos de cableado estructurado, de esta manera, se trabajará con costos actuales del mercado ecuatoriano.

El análisis de costos implica una cuantización de egresos, es decir, conocer cuál es el costo de inversión de la nueva red; para ello se incluye el precio de los equipos y demás elementos de cableado estructurado necesarios, la instalación de *racks* y equipos, así como las licencias de herramientas de administración principalmente. Además, mediante los beneficios que se tendrán de la nueva red, se determinará cuáles podrían ser las ganancias y la forma de recuperación de la inversión.

En la red LAN del edificio matriz de TRANSELECTRIC S.A. se incluirán todos los elementos de *networking* necesarios para el correcto funcionamiento; algunos de los que existen actualmente se reutilizarán para no desperdiciar recursos. Tal es el caso del *firewall*, que mediante reglas establecidas, normará el tráfico entrante y saliente. Éste se conectará a una de las interfaces Gigabit Ethernet del *switch*

de *core*.

Otros elementos existentes a reutilizarse son los *racks* y *patch pannels* del cuarto de equipos, así como los *patch cords* de categoría 5E para los usuarios que no entran en la migración inicial a Voz IP<sup>65</sup>, etc.

Se especificarán los materiales necesarios que deben ser adquiridos para la parte activa y pasiva del diseño de red propuesto. Para la selección de los equipos se consideran las características especificadas en el capítulo 3, en el punto 3.3.2.1.

Con respecto a los *switches*, dentro de las características básicas que deberá tener el que actuará como *Core* están: puertos SFP 10 Gigabit para la comunicación con los *switches* de distribución, puertos 10/100/1000 para la conexión a través de cable UTP categoría 6 con los servidores y con el *switch* utilizado en la comunicación hacia Calderón mediante Metro Ethernet. Además son necesarios puertos SFP de 1 Gigabit donde se conectarán los enlaces externos con los diferentes clientes (estos enlaces no corresponden a la red LAN de TRANSELECTRIC S.A.).

Las características básicas que deberán tener los *switches* que serán usados para distribución son: puertos para módulos SFP 1 Gigabit necesarios para conectarse con cada uno de los *switches* de acceso y hacia el *switch* que se enlazará a la PABX; puertos con módulos SFP 10 Gigabit para la comunicación con el *switch* de *core* y entre los *switches* de distribución.

Los *switches* de acceso deberán tener una cantidad de puertos 10/100 necesarios, de acuerdo al número de usuarios de cada ala y al menos 2 puertos para módulos SFP de 1 Gigabit que se dirigirán a través del *backbone* de fibra hacia el cuarto de equipos. Para reutilizar los *switches* existentes en el edificio matriz, se comprobó si poseen o no puertos de fibra. Cabe mencionar que todos ellos son de 24 puertos y en la mayoría de alas se requieren de 48 puertos; así, los *racks* se conformarán combinando un *switch* que posee puertos de fibra para

---

<sup>65</sup> Referirse al punto 3.2.1 del capítulo 3

comunicarse al *backbone* con uno que no los tiene y de esta manera disminuir gastos.

Los usuarios que serán migrados a tecnología VoIP se conectarán a los *switches* de acceso, posteriormente a los de distribución y por último a la central telefónica. Entre el *switch* de distribución y la PABX se conectará un *switch* que tenga puertos 10/100 y SFP de 1 Gigabit para fibra óptica.

Es necesaria la adquisición de teléfonos IP que permitan la comunicación de los usuarios; para ello se escogieron modelos simples de una sola línea para usuarios normales y con más de una línea para las secretarías y usuarios privilegiados.

Otro de los temas importantes en el diseño es la utilización de la fibra óptica tendida entre el edificio matriz y las instalaciones en Calderón. Se los hará parte de la misma red LAN mediante la tecnología Metro Ethernet. Se necesitará adquirir para cada uno de los extremos un *switch* que soporte Metro Ethernet, lo que permitirá que estas dos redes sean transparentes para los usuarios como una sola red LAN.

Todos los módulos SFP de los *switches* deberán ser para conectores de fibra LC y los ODFs tendrán conectores FC/UPC, por lo que los *patch cords* de fibra serán LC/FC para la conexión entre *switches* y ODFs, y LC/LC para la conexión entre *switches*.

A continuación en las tablas 4.1a, 4.1b y 4.1c se presenta un resumen de los principales requerimientos que se tienen para los diferentes *switches* de *core*, distribución y de acceso.

El número de puertos que se mencionan no son el número exacto de los requeridos pero son los valores que vienen como estándar por los fabricantes. En el anexo 4.1 se muestran los *datasheet* de los equipos nuevos.

REQUERIMIENTOS DEL SWITCH DE CORE		
Módulo o tarjeta	# Puertos	Uso
Con puertos 10/100/1000	48	Conexión a servidores y a <i>switch</i> para salida a Calderón
Con puertos SFP de 1 Gb	24	Conexión a clientes de la Compañía
Con puertos SFP de 10 Gb	Mínimo 4	Conexión a <i>switches</i> de distribución
OTROS REQUERIMIENTOS		
<ul style="list-style-type: none"> <li>- Conmutación y enrutamiento de capas 2, 3 y 4.</li> <li>- Soporte de PoE.</li> <li>- Soporte de módulos WAN.</li> <li>- Monitoreo y administración de red.</li> <li>- Seguridad de control de acceso y encriptación.</li> <li>- Funcionalidades bajo estándares IEEE.</li> <li>- Calidad de servicio.</li> </ul>		

Tabla 4.1a Requerimientos de *switch* de core

REQUERIMIENTOS DEL SWITCH DE DISTRIBUCIÓN		
Módulo o tarjeta	# Puertos	Uso
Con puertos SFP de 1 Gb	24	Conexión a <i>switches</i> de acceso y hacia <i>switch</i> de comunicación a la PABX
Con puertos SFP de 10 Gb	Mínimo 4	Conexión a <i>switch</i> de core y entre los de distribución
OTROS REQUERIMIENTOS		
<ul style="list-style-type: none"> <li>- Conmutación y enrutamiento de capas 2 y 3.</li> <li>- Monitoreo y administración de red.</li> <li>- Seguridad de control de acceso y encriptación.</li> <li>- Funcionalidades bajo estándares IEEE.</li> <li>- Calidad de servicio.</li> </ul>		

Tabla 4.1b Requerimientos de *switch* de distribución

REQUERIMIENTOS DEL SWITCH DE ACCESO		
Módulo o tarjeta	# Puertos	Uso
Con puertos 10/100	24 ó 48	Conexión a usuarios de red
Con puertos SFP de 1 Gb	2	Conexión a <i>switches</i> de distribución.
OTROS REQUERIMIENTOS		
<ul style="list-style-type: none"> <li>- Conmutación capa 2.</li> <li>- Soporte de VLANs.</li> <li>- Monitoreo y administración de red.</li> <li>- Seguridad de control de acceso.</li> <li>- Funcionalidades bajo estándares IEEE.</li> <li>- Soporte de VoIP*</li> </ul>		
<p>* Solo para equipos utilizados en migración a VoIP.</p> <p>Nota: No todos los equipos deben tener puertos de fibra, debido a que algunos solo actúan como segundo para completar el número de puertos requeridos junto a los <i>switches</i> existentes que sí tienen puertos de fibra para la comunicación a los de distribución.</p>		

Tabla 4.1c Requerimientos de *switch* de acceso

## 4.2 ALTERNATIVAS DE EQUIPOS

### 4.2.1 ALTERNATIVA 3COM

#### 4.2.1.1 *Switch de Core*

Acorde a las características descritas se ha escogido el *switch* 3Com 8810 capa 4, que posee 10 *slots* que permiten insertar las tarjetas necesarias para las conexiones requeridas. Este equipo puede soportar hasta 32 puertos 10Gbit ó 384 puertos, ya sean 10/100/1000, 10/100/1000 PoE o SFP (Figura 4.1). Las tarjetas, dependiendo de las características, permiten la comunicación por cobre o por fibra óptica.



Figura 4.1 *Switch* 3Com 8810<sup>[1]</sup>

Entre las principales características técnicas dadas por el fabricante están:

- Los módulos aplicables al *switch* proveen flexibilidad para añadir un *firewall*, encriptación IPSec, monitoreo de red con *NetFlow* y *networking* de VPNs de capa 2.
- QoS (calidad de servicio) garantizada para aplicaciones, incluyendo VoIP, almacenamiento y video.
- Seguridad de control de acceso de red, encriptación y protección de recursos corporativos.
- Control de acceso a la red y amplia seguridad bajo el estándar IEEE 802.1x, autenticación RADIUS y listas de control de acceso avanzado.
- Soporte de PoE (*Power over Ethernet*) para teléfonos IP, *access points* inalámbricos y otros dispositivos, reduciendo costos de implementación y mantenimiento.
- Capacidad de conmutación y enrutamiento de capas 2, 3, 4.

Las tarjetas adicionales para este *switch* serán:

- 3Com *Switch* 8800 48-Port 10/100/1000BASE-T 3C17528A: Tarjeta de 48 puertos 10/100/1000 con conectores RJ-45.
- 3Com *Switch* 8800 24-Port 1000BASE-X (SFP) 3C17530: Tarjeta de 24 puertos Gigabit para fibra óptica.
- 3Com *Switch* 8800 4-Port 10GBASE-X (XFP) 3C17526: Tarjeta de 4 puertos 10 Gigabit para fibra óptica.

#### 4.2.1.2 *Switches* de Distribución

Debido a que el cableado de *backbone* será mediante fibra óptica, se escogió el modelo de 3Com 5500G-EI que proporciona 24 puertos SFP de fibra óptica y además puertos 10/100/1000 (Figura 4.2).



Figura 4.2 *Switch* 3Com 5500G-EI<sup>[1]</sup>

Entre las principales características técnicas dadas por el fabricante están:

- Alta disponibilidad de la red (99,999%).
- 24 puertos SFP que funcionan a 1 Gigabit; 4 puertos de uso dual con puertos 10/100/1000.
- *Routing* avanzado de Capa 3 (RIP/OSPF).
- QoS de Capa 2-4.
- Funcionalidades de limitación de velocidades.
- Seguridad mediante SNMP v3, SSH, *login* de red para administración y monitorización simplificadas.
- Comparte el mismo sistema operativo de los *switches* y *routers* modulares de primera clase, incluyendo los 3Com 8800; esta característica permite administrar una infraestructura distribuida de *switching* y *routing* mediante una única plataforma de administración como 3Com *Enterprise Management Suite* o 3Com *Network Director*.
- Permite insertar módulos 10 Gigabit Ethernet.
- Capacidad de *switching* de hasta 184 Gbps.

Los módulos adicionales para este *switch* serán:

- Módulos de 8 puertos 1000Base-X SFP 3C17260
- Módulos de 2 puertos 10 Gigabit 3CXFP94

#### 4.2.1.3 *Switches de Acceso*

Para los casos de los pisos PBA, 8, 9 y 10 que serán migrados a VoIP se utilizarán equipos que soporten dicha tecnología y faciliten la administración de direcciones IP para VoIP. Para ello, se propone utilizar los *switches* 3Com 4500G de 48 o 24 puertos 10/100/1000 y 4 puertos SFP para la comunicación con los *switches* de distribución.

Para el resto de pisos se utilizarán *switches* 3Com 2250 plus de 48 puertos que de igual manera poseen puertos 10/100/1000 y 2 puertos SFP. Los demás pisos tendrán los *switches* existentes en el edificio considerando uno con puertos SFP y el otro sin dichos puertos de fibra. Para estos últimos los *switches* que se utilizarán son los 3Com 2024 de 24 puertos 10/100.

Entre las características técnicas dadas por el fabricante para los equipos están:

#### 3Com 4500G



Figura 4.3 Switch 3Com 4500G para VoIP<sup>[1]</sup>

- 48 puertos 10BASE-T/100BASE-TX/1000BASE-T con auto-negociación; 4 puertos de uso dual con puertos 10/100/1000.
- *Switching* de Capa 2.
- 2 ranuras traseras para módulos 10 Gigabit de 2 puertos.
- Proporciona conectividad de LAN segura y flexible.
- Funcionalidades avanzadas para voz tales como VLAN automática de voz y QoS.
- Idóneo para empresas que desean construir redes convergentes seguras.

### Base Line 2250 Plus



Figura 4.4 Switch 3Com 2250 Plus<sup>[1]</sup>

- 48 puertos 10/100 y 2 puertos Gigabit de uso dual (cobre o SFP).
- La interfaz del conmutador permite a los usuarios configurarlo de forma rápida y segura.
- Permite hasta 8196 *MAC address* y 256 VLANs para segmentar la red.
- Control de acceso a la red IEEE 802.1X que proporciona seguridad basada en estándares, combinada con autenticación local.

### 3Com BaseLine 2024



Figura 4.5 Switch 3Com 2024<sup>[1]</sup>

- 24 puertos 10/100 para conexión por cobre.
- MDI/MDIX automático en todos los puertos lo que simplifica la instalación al permitir una conexión directa a otro dispositivo, utilizando cables directos o cruzados.
- Soporte RMON (*Remote Monitoring*, Monitorización remota) fácil de utilizar para la administración de todos los puertos conmutados.
- Soporte 802.1p para priorización del tráfico utilizado por las aplicaciones multimedia y 802.1q para la creación de funciones VLAN.
- No necesita configuración o *software* de administración.

Para la utilización de los *switches* de acceso que se conectarán a los de distribución, se necesitarán módulos adicionales de fibra de 1 Gigabit de 2 puertos para cada uno.

En la tabla 4.2 se muestra la distribución final de los *switches* de acceso de marca 3Com entre nuevos y existentes.



NUEVA DISTRIBUCIÓN DE LOS SWITCHES DE ACCESO MARCA 3COM DEL EDIFICIO MATRIZ DE TRANSELECTRIC S.A				
PISO	ALA	MODELO	NÚMERO Y TIPO DE PUERTOS	UBICACIÓN ACTUAL
10	A	3Com 4500G 3CR17762-91	SWITCH 48 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	Nuevo
	B	3Com 4500G 3CR17762-91	SWITCH 48 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	Nuevo
9	A	3Com 4500G 3CR17762-91	SWITCH 48 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	Nuevo
	B	3Com 4500G 3CR17762-91	SWITCH 48 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	Nuevo
8	A	3Com 4500G 3CR17762-91	SWITCH 48 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	Nuevo
	B	3Com 4500G 3CR17762-91	SWITCH 48 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	Nuevo
7	A	SuperStack 3 Switch 4200	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
		3Com BaseLine 2024 3C16471	SWITCH 24 PUERTOS 10/100 Mbps	Nuevo
	B	SuperStack 3 Switch 4200	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
6	A	SuperStack 3 Switch 4200	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
		SuperStack II Switch 3300 3C16980	SWITCH 24 PUERTOS 10/100 Mbps	9no Piso (ID: B)*
	B	SuperStack 3 Switch 4200	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
		SuperStack II Switch 3300 3C16980	SWITCH 24 PUERTOS 10/100 Mbps	9no Piso (ID: C)*
5	A	SuperStack 3 Switch 4200	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
		SuperStack II Switch 3300 XM 3C16985	SWITCH 24 PUERTOS 10/100 Mbps	9no Piso (ID: J)*
	B	SuperStack 3 Switch 4200	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
		SuperStack II Switch 3300 XM	SWITCH 24 PUERTOS 10/100 Mbps	Planta Baja*
4	A	TERMOPICHINCHA		
	B	SuperStack 3 Switch 3300 3C16980A	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso (ID: D)*
3	A	3Com BaseLine 2250 plus 3CBLSF50	SWITCH 48 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
	B	3Com BaseLine 2250 plus 3CBLSF50	SWITCH 48 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
2	A	Switch 3824	SWITCH 24 PUERTOS y 4 PUERTOS SFP	5to Piso Informática*
		3Com BaseLine 2024 3C16471	SWITCH 24 PUERTOS 10/100 Mbps	Nuevo
	B	Switch 3824	SWITCH 24 PUERTOS y 4 PUERTOS SFP	5to Piso Informática*
		3Com BaseLine 2024 3C16471	SWITCH 24 PUERTOS 10/100 Mbps	Nuevo
PB	A	3Com 4500G 3CR17762-91	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	Nuevo
	B	Switch 3870	SWITCH 24 PUERTOS y 4 PUERTOS SFP	5to Piso Informática*
		3Com BaseLine 2024 3C16471	SWITCH 24 PUERTOS 10/100 Mbps	Nuevo

\*Estos switches son los que se reutilizarán y la letra de identificación indica la etiqueta que tienen los equipos actualmente.

Tabla 4.2 Distribución de switches 3Com

Como se puede ver en la tabla anterior, para los pisos PBB, 2, 4, 5, 6 y 7 se combinarán los *switches* de 24 puertos 10/100 y puertos SFP con los más sencillos que no poseen puertos de fibra. En los pisos PBA, 8, 9 y 10 se priorizó la migración de telefonía convencional a VoIP.

#### 4.2.1.4 *Switch de Voz*

El *switch* de comunicación seleccionado entre la central telefónica y los *switches* de distribución es el 3Com *Office Connect Managed Gigabit PoE* de 8 puertos 10/100/1000 y 2 puertos SFP (Figura 4.6).



Figura 4.6 *Switch 3Com Office Connect Managed Gigabit*<sup>[1]</sup>

Entre las principales características técnicas dadas por el fabricante están:

- 8 puertos 10/100/1000 y 2 puertos Gigabit SFP de uso dual (configurable como 10/100/1000 o SFP); puerto de consola en panel frontal para administración CLI.
- Conmutador Gigabit Ethernet de Nivel 2 administrado.
- VLAN de voz que asigna automáticamente el tráfico VoIP a una VLAN dedicada, optimizando así este tráfico sensible al retraso.
- Control de acceso a la red IEEE 802.1X que proporciona seguridad basada en estándares, combinada con autenticación local.
- Soporte del protocolo *Rapid Spanning Tree* (RSTP) que permite mejorar la compatibilidad, escalabilidad y disponibilidad de la red.
- Puede administrarse con *software* compatible con SNMP, como por ejemplo [3Com Network Supervisor](#) y [Network Director](#).

Para su funcionamiento se necesita un módulo adicional SFP de 1 Gigabit de dos puertos para la conexión con los *switches* de distribución; a través de los puertos 10/100/100 se conectará a la PABX.

#### 4.2.1.5 Switches para Enlace Metro Ethernet

Los *switches* seleccionados son los 3Com Intellijack NJ2400FX de 4 puertos (Figura 4.7).



Figura 4.7 Switch 3Com Intellijack<sup>[2]</sup>

Entre sus principales características técnicas están:

- 4 puertos LAN de *switching* 10/100 Mbps; un puerto adicional para conexiones de teléfono o de red.
- La conexión soporta un puerto adicional separado para voz y datos.
- Soporta administración SNMP v3 segura, así como redes IPv6.
- QoS sobre voz con priorización de paquetes IEEE 802.1p que permite priorizar el tráfico VoIP.

#### 4.2.1.6 Teléfonos IP

Para la comunicación de los usuarios que serán migrados a VoIP se utilizarán teléfonos IP de características simples con una línea o más; y, para usuarios privilegiados se utilizarán teléfonos inalámbricos.

##### 3Com 3100



Figura 4.8 Teléfono IP 3Com 3100<sup>[1]</sup>

Entre las principales características técnicas del teléfono se encuentran:

- Alta calidad de audio.

- Diseño compacto y de fácil funcionamiento.
- Al estar diseñado como alternativa de sustitución rentable de un teléfono analógico tradicional, el modelo 3100 puede usar una conexión Ethernet estándar.
- Su diseño mejora la acústica y la ergonomía.
- Capacidad de auto-ubicación que permite ahorrar tiempo y gastos de llamadas de servicio, reduciendo así el costo total de propiedad.
- La administración basada en navegador facilita las tareas de configuración y el soporte basado en la *web* facilita el aprendizaje de sus funcionalidades avanzadas.
- Posee capacidad para correo de voz.
- Soporte para alimentación mediante Ethernet (PoE).
- Soporta *codecs* de voz como G.711, G.722, G.729a, ADPCM.
- Posee calidad de servicio IEEE 802.1q para VLANs.
- Permite asignación de dirección IP mediante DHCP.
- 1 puerto de red Ethernet 10/100 Base-TX.

### 3Com 3101



Figura 4.9 Teléfono IP 3Com 3101<sup>[1]</sup>

Además de las características del 3Com 3100 presenta:

- 2 puertos de red Ethernet 10Base-T/100Base-TX.
- Dispositivo adicional manos libres.
- Posee 4 botones programables que permiten a los usuarios administrar llamadas y acceder a las funciones más utilizadas.
- Los botones de Llamada en espera y Mensaje se distinguen claramente para ayudar a los usuarios a manejar llamadas de forma profesional.
- Soporta el Protocolo de Iniciación de Sesión (SIP).

- Capacidad de llamadas en conferencia.

### 3Com 3106



Figura 4.10 Teléfono IP 3Com 3106<sup>[1]</sup>

Además de las características del 3Com 3101 este teléfono:

- Permite a los usuarios desplazarse libremente mientras conversan por la red IP de la organización.
- A diferencia de un teléfono móvil, este teléfono inalámbrico de 900 MHz proporciona un acceso completo al sistema de telefonía IP.
- Posee 4 teclas programables y 8 con funciones predefinidas que facilitan y agilizan el uso de las funciones más frecuentes.
- La comprobada tecnología de espectro ampliado no interferirá con las señales de radio de la red *Wi-Fi* IEEE 802.11.
- Se puede tener en funcionamiento en el área circundante hasta 10 teléfonos, con un alcance máximo de 305 m desde la unidad base.
- Cada teléfono puede manejar hasta cuatro líneas, conectándose a la red mediante un puerto 10/100 en la unidad base.

## 4.2.2 ALTERNATIVA CISCO

### 4.2.2.1 *Switch de Core*

Acorde a las características descritas se ha escogido al *switch* Cisco Catalyst 6509-E. Ofrece soluciones de conmutación y enrutamiento de capas 2,3 y 4 de alto rendimiento para redes empresariales y de proveedores de servicios. Entrega seguridad, convergencia y diversos servicios que ayudan al buen funcionamiento de la red (Figura 4.11).

Está diseñado para afrontar los crecientes requisitos de densidad Gigabit, alta disponibilidad y conmutación inteligente multicapa en el *backbone*/distribución. Proporciona una amplia gama de soluciones, que posibilitan la existencia tanto de extranets, intranets empresariales como *Internet* para multimedia, datos de tareas críticas y aplicaciones de voz.



Figura 4.11 Switch CISCO Catalyst 6509-E<sup>[3]</sup>

Entre sus principales características técnicas se encuentran:

- Soporta un motor de supervisión (Supervisor Engines 720) para su administración.
- Permite módulos Fast Ethernet con IEEE 802.3af *Power over Ethernet*.
- Soporta módulos Gigabit Ethernet con IEEE 802.3af PoE.
- Permite módulos 10 Gigabit Ethernet.
- Soporta módulos WAN.
- Soporta módulos Multi-Gigabit que contienen servicios, *firewall*, detección de intrusos, IPSec, VPN, análisis de red, SSL.
- Soporta Cisco Catalyst OS y Cisco IOS *Software*.
- Ofrece una mejora en la alimentación llegando a 8700 W y soporta un gran número de dispositivos IEEE 802.3af PoE.
- Provee redundancia y rapidez.
- Puede añadirse el sistema de seguridad Cisco Catalyst 6509-E *Firewall*, el cual es un modelo de 9 *slots* que provee una solución de desarrollo fácil que integra a las series *Supervisor Engine 720* (con políticas integradas y tarjetas con características de *switches* multicapas para sistemas de control, servicios de enrutamiento y puertos dual Gigabit Ethernet) con módulos de servicios de *firewall* de las series Cisco Catalyst 6500 al proveer 5 Gbps para los servicios de *firewall*.

- Los sistemas IPsec VPN toman las ventajas de los módulos de servicios IPsec VPN de Cisco 7600/Catalyst 6500 y provee sobre los 2 Gbps de encriptación 3DES.

Las tarjetas adicionales para este *switch* serán:

- Módulo de 48 puertos 10/100/1000 Ethernet con PoE 802.3af: Tarjeta de 48 puertos Gigabit Ethernet con una tarjeta hija PoE con conectores RJ-45.
- 24-Port SFP GE: Tarjeta de 24 puertos Gigabit con puertos SFP para conectores LC.
- 4-Port SFP 10 GE: Tarjeta de 4 puertos 10 Gigabit Ethernet con puertos SFP con conectores LC.

#### 4.2.2.2 *Switches* de Distribución

Se escogió el modelo Cisco Catalyst 3560E que consta de 12 puertos SFP y 2 puertos de 2 x 10 GE. Debido a que se requieren 24 puertos para el *switch* de distribución se utilizarán dos de estos equipos para el *switch* principal y otros dos del mismo para el *switch* secundario (redundancia).

La serie CISCO Catalyst 3560-E mejora la productividad y protege la inversión con el buen desarrollo de la red. Permite escalabilidad, lo que facilita el desarrollo de la seguridad en aplicaciones convergentes.

Se emplea la nueva tecnología de CISCO ePoE (*enhanced Power over Ethernet*) que permite alimentar los puntos de acceso *wireless* 802.11n desde un único puerto del conmutador, lo que ofrece mayor simplicidad y flexibilidad.

Dentro de su serie Catalyst 3560-E presenta una solución de conmutación de 1 y 10 Gbps, se trata de un *switch* con 12 puertos de 1 Gbps y otros dos puertos 2 x 10 Gbps. Con un diseño compacto de un RU, se dirigen especialmente a entornos con limitaciones de espacio y energía.



Figura 4.12 *Switch* CISCO Catalyst 3560-E<sup>[4]</sup>

Los *switches* 3560E-12SD soportan aplicaciones convergentes en tiempo real, así como las herramientas de telepresencia y de comunicaciones unificadas de una compañía (Figura 4.12).

Entre las principales características técnicas del fabricante están:

- Mejoramiento en el estándar STP a PVST+.
- Autoconfiguración de DHCP de múltiples *switches*.
- Alto rendimiento en el enrutamiento IP.
- Seguridad avanzada para la conectividad y el control de acceso incluyendo ACLs, autenticación, seguridad a nivel de puerto y servicios de red basados en la identificación con 802.1x.
- AutoQoS que simplifica la configuración de QoS en redes de VoIP al publicar la interfaz y comandos globales del *switch*; detecta teléfonos IP Cisco, clasifica el tráfico y ayuda en la configuración de la cola de salida.
- Permite autonegociación automática en todos los puertos para seleccionar si la transmisión es en *half* o *full duplex* y así optimizar el ancho de banda.
- Facilita la configuración de puertos troncales dinámicos DTP (*Dynamic Trunking Protocol*) a través de todos los puertos del *switch*.
- PAgP (*Port Aggregation Protocol*) automatiza la creación de grupos *Cisco Fast EtherChannel* o grupos *Gigabit EtherChannel* para enlazarlo con otro *switch*, *router* o servidor.
- Soporta LACP (*Link Aggregation Control Protocol*) que permite la creación de canalización Ethernet con dispositivos IEEE 802.3ad. Esta característica es similar a la tecnología *Cisco EtherChannel*.
- Permite MDIX (Interfaces dependientes del medio) las cuales automáticamente ajustan los pares de transmisión y recepción si un tipo de cable (cruzado o directo) es instalado incorrectamente.
- Soporta UDLD (*Unidirectional Link Detection Protocol*) y UDLD Agresivo que permite deshabilitar las interfaces con fibra óptica al detectar enlaces unidireccionales causados por el incorrecto tendido de la fibra o por falla en los puestos.
- Características de control y administración.



Los módulos adicionales para este *switch* serán:

- Módulos SFP de 1 Gigabit Ethernet.
- Módulos SFP de 2 x 10 Gigabit Ethernet.

#### 4.2.2.3 *Switches de Acceso*

Dentro de los *switches* de acceso se tendrán varios modelos como se puede observar en la tabla 4.3. Para los casos de los pisos (PBA, 8, 9 y 10) que serán migrados a VoIP se utilizarán los *switches* Cisco Catalyst 2960-24PC-L. Estos equipos soportan dicha tecnología, detectan automáticamente teléfonos IP Cisco y facilitan la administración de los mismos.

Estos *switches* tienen 24 puertos 10/100 PoE y 2 puertos SFP de 1 Gigabit Ethernet, los cuales serán utilizados para la comunicación con los *switches* de distribución.

Para el resto de pisos, como se mencionó anteriormente, se reutilizarán los *switches* que existen actualmente en el edificio. Por lo general, en las alas en las que se requiera de dos *switches* de 24 puertos, se combinará un *switch* que tenga 24 puertos 10/100 y 2 puertos SFP de 1 Gigabit Ethernet con uno que únicamente tenga 24 puertos 10/100. Este último será el Cisco Catalyst 2960-24TT-L (Figura 4.13).



Figura 4.13 *Switch* CISCO Catalyst 2960 Series<sup>[5]</sup>

Debido a que los dos modelos de *switches* a conseguirse son de la misma familia, a continuación se presentan las características técnicas comunes:

- Provee conectividad Fast Ethernet y Gigabit Ethernet.
- Configuración PoE con 15.4 W.

- Características inteligentes como control de ACLs y seguridad mejorada.
- Soporta DHCP.
- Asegura alta disponibilidad, seguridad, escalabilidad y control de la red.
- Flexibilidad en los puertos Gigabit Ethernet permitiendo el uso de cobre o fibra óptica; es decir cada puerto tiene 10/100/1000 Ethernet y SFP basado en Gigabit Ethernet, con un puerto activo a la vez.
- Control de la red y optimización del ancho de banda usando QoS avanzado, limitación de la velocidad, ACLs y servicios *multicast*.
- Seguridad integrada a través de métodos de autenticación, tecnologías de encriptación de datos y NAC (*Network Admission Control*) basado en usuarios, puertos y direcciones MAC.
- Autoconfiguración para aplicaciones especiales usando puertos inteligentes.
- Sistema redundante de alimentación (RPS 2300) el cual incrementa la disponibilidad en las redes convergentes de datos, voz y video al proveer de un respaldo transparente en los puertos.
- Simplificación en la administración de la red al soportar SNMP y herramientas que permiten el control en tiempo real.

Con respecto al *switch* Cisco Catalyst 2960-24PC-L, éste provee PoE y permite una conexión fácil a dispositivos *Ethernet-powered* incluyendo teléfonos IP Cisco, *Access Points* y cámaras de video IP.

Soporta Auto QoS, característica que detecta los teléfonos IP Cisco y configura automáticamente al *switch* para la clasificación apropiada y las colas de salida. Esto optimiza la priorización del tráfico y la disponibilidad de la red sin la necesidad de configuraciones complejas.

Los módulos a usarse, en caso de ser necesario, serán:

- Módulos SFP de 1 Gigabit Ethernet.

En la tabla 4.3 se muestra la distribución final de los *switches* de acceso de marca Cisco entre nuevos y existentes.

NUEVA DISTRIBUCIÓN DE LOS SWITCHES DE ACCESO DE MARCA CISCO EN EL EDIFICIO MATRIZ DE TRANSELECTRIC S.A.				
PISO	ALA	MODELO	NÚMERO Y TIPO DE PUERTOS	UBICACIÓN
10	A	Catalyst 2960-24PC-L (x2)	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
	B	Catalyst 2960-24PC-L (x2)	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
9	A	Catalyst 2960-24PC-L (x2)	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
	B	Catalyst 2960-24PC-L (x2)	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
8	A	Catalyst 2960-24PC-L (x2)	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
	B	Catalyst 2960-24PC-L (x2)	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
7	A	Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	5to Piso (ID: A)*
		Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
	B	Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso Informática*
6	A	Catalyst 2960 Series SI	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	9no Piso (ID: D)*
		Catalyst 2960-24TT	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
	B	Catalyst 2960 Series SI	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	9no Piso (ID: E)*
		Catalyst 2960-24TT	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
5	A	Catalyst 3500 Series XL	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	5to Piso (ID: B)*
		Catalyst 2950	SWITCH 24 PUERTOS 10/100 Mbps	5to Piso Informática*
	B	Catalyst 3500 Series XL	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	9no Piso (ID: I)*
		Catalyst 2950	SWITCH 24 PUERTOS 10/100 Mbps	5to Piso Informática*
4	A	TERMOPICHINCHA		
	B	Catalyst 2950SX-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS 1000BASE-SX	9no Piso (ID: F)*
3	A	Catalyst 2950-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	5to Piso (ID: C)*
		Catalyst 2960-24TT	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
	B	Catalyst 2950SX-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS 1000BASE-SX	5to Piso (ID: E)*
		Catalyst 2960-24TT	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
2	A	Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	2do Piso*
		Catalyst 2950-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps	9no Piso (ID: A)*
	B	Catalyst 2900 Series	SWITCH 24 PUERTOS 10/100 Mbps	2do Piso*
		Catalyst 2960-24TC-L	SWITCH 24 PUERTOS 10/100 Mbps y 4 PUERTOS SFP	9no Piso (ID: H)*
PB	A	Catalyst 2960-24PC-L	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Nuevo
	B	Catalyst 2950-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	9no Piso (ID: G)*
		Catalyst 2950-24 Switch	SWITCH 24 PUERTOS 10/100 Mbps y 2 PUERTOS SFP	Planta Baja*

\*Estos switches son los que se reutilizarán y la letra de identificación indica la etiqueta que tienen los equipos actualmente.

Tabla 4.3 Distribución de switches CISCO

#### 4.2.2.4 *Switch de Voz*

El *switch* de comunicación entre la central telefónica y los *switches* de distribución será el Cisco Catalyst 2960G-8TC-L. Debido a que la conexión entre este *switch* y la PABX se lo realizará a través de cobre es necesario puertos RJ45 10/100/1000; mientras que la conexión entre los *switches* de distribución y este *switch* se lo hará mediante los puertos SFP 1 Gigabit Ethernet a través de fibra óptica.

Posee las mismas características técnicas de los *switches* de acceso especificadas en el punto anterior ya que son de la misma familia. Entre las características propias del *switch* están: 8 puertos Ethernet 10/100, dos puertos 10/100/1000 y SFP de doble propósito y un tamaño compacto (Figura 4.14).



Figura 4.14 *Switch* CISCO Catalyst 2960 de 8 puertos<sup>[6]</sup>

Para la utilización de este *switch* se necesitarán dos módulos de fibra de 1 Gigabit para la conexión con los *switches* de distribución; a través de los puertos 10/100/100 se conectará a la PABX.

#### 4.2.2.5 *Switches para Enlace Metro Ethernet*

El modelo seleccionado para este caso es el Cisco ME 3400G-2CS-A que tiene dos puertos de doble propósito 10/100/1000 y/o SFP, dos puertos SFP y una fuente de alimentación. Permitirá que la red del COT sea vista como parte de la red LAN de TRANSELECTRIC al utilizar la tecnología de Metro Ethernet.

Los *switches* de la serie Cisco ME 3400 (Figura 4.15) son dispositivos de capa 2 y 3

de próxima generación. Fueron diseñados en base a la experiencia de *switches* de acceso con cobertura más extendida a la de las series Catalyst 2950 y 3550.

Los proveedores de servicios están cambiando la tecnología Ethernet por redes MAN y WAN que soporten nuevos beneficios. Estos equipos de Ethernet inteligentes entregan seguridad avanzada de red y capacidades de QoS enriquecidas, permitiendo a los proveedores ofrecer una combinación entre las velocidades de datos y servicios para conexiones multipunto y punto a punto.



Figura 4.15 *Switch* CISCO Catalyst ME 3400<sup>[7]</sup>

Entre las principales características técnicas dadas por el fabricante están:

- Es una solución de seguridad completa para acceso de Metro Ethernet.
- Factor de forma compacta (1RU) para la facilidad de despliegue en un número limitado de espacios
- *Switch* Ethernet inteligente.
- Soporta múltiples imágenes de *software*, 3 características de opciones de imágenes Cisco IOS *Software* (METROBASE, METROACCESS y METROIPACCESS)
- Completa solución de seguridad de acceso Metro Ethernet
- Servicio VPN capa 2 y 3.
- Alto rendimiento en el enrutamiento IP.
- Disponibilidad y escalabilidad.
- Distribución *multicast* eficiente y control *multicast* robusto.
- QoS avanzada con control de tráfico avanzado.
- Soluciones de seguridad.

- Administración superior y soporte de herramientas de administración.

#### 4.2.2.6 Teléfonos IP

Para la comunicación de los usuarios que serán migrados a VoIP se utilizarán teléfonos IP de características simples. Para un usuario común se usará teléfonos IP de modelo 521SG de una línea y para usuarios como secretarías y ejecutivos se usará el modelo 524SG con más de una línea de acceso (Figura 4.16).



Figura 4.16 Teléfono IP de la serie 500<sup>[7]</sup>

La serie 500 de teléfonos IP de Cisco consiste en equipos económicos que ofrecen una excelente opción para negocios ya que han sido optimizados para sustituir sistemas de voz tradicionales o acordar una solución para la nueva generación tecnológica en un ambiente alambrado de categoría 5 o superior.

Poseen acceso “un toque” para volver a llamar, transferir, hacer una conferencia y poner en espera. Un puerto de *switch* 10/100 habilita la conexión LAN a un ordenador personal y así permite reducir el costo de alambrado adicional.

Además, pueden activarse a través de un *switch* con capacidad PoE o usando un adaptador de alimentación adicional. Están diseñados para separar VLAN para datos y voz y proveer seguridad y fiabilidad del tráfico de voz y datos.

Dentro de sus características comunes están:

- Fácilmente llenan la necesidad de servicios básicos telefónicos en todas partes en el ambiente de trabajo.

- Fácil configuración y traslación física.
- Presentan cuatro teclas que guían a través de las funciones esenciales.
- Tienen una pantalla LCD con color con teclas dinámicas para características y funciones de llamadas. Poseen una eficiente alimentación como apagado de la pantalla cuando no se lo utiliza.
- Accesibilidad para usuarios con necesidades especiales.
- Soportan *codecs* de voz como G729.a
- Soportan protocolos tales como H.323 y SIP.
- Soportan apariencia de línea compartida, intercomunicador y poseen capacidad de seguridad que permite la configuración de una contraseña para protección de los cambios a través del teléfono.

También pueden ser usados para mejorar la productividad de comunicaciones unificadas como la búsqueda en un directorio y otras características.

#### Cisco Unified IP Phone 521SG

Es un teléfono IP de una sola línea con dos accesos de línea de llamada.

#### Cisco Unified IP Phone 524SG

Es un teléfono IP de cuatro líneas con hasta ocho accesos de línea de llamada.

### **4.3 OTROS ELEMENTOS DE RED**

Considerando la existencia de un *rack* en cada ala de piso en el edificio, se necesitan elementos como el *rack*, *patch pannels*, ODFs y medios de transmisión como el cable UTP y la fibra. En el capítulo 3 se mencionan las características mínimas a cumplir de cada uno de los elementos.

#### **4.3.1 PATCH PANNELS**

Se escogió utilizar *patch pannels* de 24 y 48 puertos de acuerdo al número de

usuarios existentes en cada ala. Para el Cuarto de Equipos se utilizarán los que se tienen en el edificio.

#### **4.3.2 ODFs**

Se utilizará un ODF de 48 puertos para el Cuarto de Equipos y de 6 puertos en cada uno de los *racks* de ala. Se debe tener en cuenta que en las alas que poseen *switch* propio también se consideran los ODFs, para el cambio a fibra óptica en *backbone*.

#### **4.3.3 RACKS**

Se reutilizarán los *racks* existentes en el Cuarto de Equipos para el mismo y para cada ala se adquirirán gabinetes de 19" de 12 unidades de *rack*, como los que existen actualmente en algunas alas.

#### **4.3.4 CABLE**

Se reutilizará el cableado categoría 5E existente únicamente para los puntos que deben cortarse y para los que deben instalarse nuevamente; en los pisos PBA, 8, 9 y 10 se colocará todo el cableado con cable UTP categoría 6. Además, para este último caso se requieren *patch cords* y cajetines categoría 6.

#### **4.3.5 PATCH CORDS**

De acuerdo a cada ala, para los usuarios se tendrán *patch cords* de categoría 6 (nuevos) y de categoría 5E (existentes), que no excederán los 3 metros desde el computador o teléfono IP hasta el cajetín. Los de categoría 6 se comprarán hechos en fábrica de una distancia de 2 metros y los de categoría 5E se utilizarán los que se tienen actualmente. Adicionalmente se utilizarán *patch cords* de fibra óptica multimodo de 1.5 metros, para las conexiones entre ODFs y *switches* de acceso, entre ODFs y *switches* de distribución y entre *switches* de distribución y de *core* y de distancias mayores, de acuerdo a requerimientos para el *backbone*.



#### **4.3.6 CAJETINES**

De igual manera que con los demás elementos, se reutilizarán los existentes y se comprarán los nuevos de categoría 6 con 2 ranuras para puntos de datos y voz.

#### **4.3.7 OTROS ELEMENTOS**

En cuanto a regletas y organizadores, en lo posible se tratará de reutilizar los elementos con los que se cuenta actualmente en el edificio matriz de la Compañía.

### **4.4 ANÁLISIS DE COSTOS**

#### **4.4.1 COSTOS PARTE ACTIVA**

Para la obtención de costos de los elementos de la parte activa a adquirirse se tomaron los valores de las cotizaciones proporcionadas por los distribuidores de 3Com y Cisco en el país como son Integrated Services IntServ C.A. para el primer caso y Andean Trade y Akros para el segundo<sup>34</sup>.

Los precios indicados son valores en dólares americanos y su costo incluye el impuesto al valor agregado (IVA).

##### **4.4.1.1 *Switches de Core***

En la tabla 4.4 se muestra el costo de los *switches* de *core*, indicándose los elementos principales tales como chasis y demás tarjetas o módulos requeridos para su utilización.

---

<sup>34</sup> Referirse al anexo 4.2 acerca de cotizaciones de equipos.

Marca	Equipo	Código	Q	P. Unidad	P. Final
3Com 8810	Chasis	3C17541	1	9484.00	9484.00
	Tarjeta 48 puertos 10/100/1000	3C17528A	1	9003.00	9003.00
	Tarjeta 24 puertos SFP 1 Gb	3C17530	1	9510.00	9510.00
	Tarjeta 4 puertos SFP 10 Gb	3C17526	2	15516.00	31032.00
	<b>TOTAL</b>				
Cisco 6509-E	Chasis	WS-C6509-E	1	5901.00	5901.00
	Tarjeta 48 puertos 10/100/1000	WS-X6148A-GE-45AF	1	5590.00	5590.00
	Tarjeta 24 puertos SFP 1 Gb	WS-X6724-SFP	1	7317.00	7317.00
	Tarjeta 4 puertos SFP 10 Gb	WS-X6708-10G-3CXL	2	13253.50	26507.00
	<b>TOTAL</b>				

Tabla 4.4 Costo de los equipos de core

#### 4.4.1.2 *Switches* de Distribución

En la tabla 4.5 se muestra el costo de los *switches* de distribución indicando los elementos adicionales requeridos para su utilización.

Marca	Equipo	Código	Q	P. Unidad	P. Final
3Com	5500G-EI basado en SFP	3CR17258-91	2	6032.00	12064.00
	Módulos de 8 puertos 1Gb	3C17260	6	1289.00	7734.00
	Módulos de 1 puerto 10 Gb	3CXFP94	8	1510.00	12080.00
	<b>TOTAL</b>				
Cisco	Catalyst 3560E-12SD	WS-C3560E-12SD-E	4	5420.00	21680.00
	Módulos de 1 puerto 1 Gb	GLC-SX-MM=	42	310.00	13020.00
	Módulos de 4 puertos 10 Gb	WS-X6704-10GE	2	6626.75	13253.50
	<b>TOTAL</b>				

Tabla 4.5 Costo de los equipos de distribución

#### 4.4.1.3 *Switches* de Acceso

En la tabla 4.6 se muestra el costo de los *switches* de acceso, se mencionan por separado los módulos para fibra que se requieren, ya que no solo son para los equipos a adquirirse sino también para los ya existentes y que soportan esta comunicación.

Marca	Equipo	Código	Q	P. Unidad	P. Final
3Com	Switch 4500G 48p	3CR17762-91	6	4348.00	26088.00
	Switch 4500G 24p	3CR17762-91	1	3876.00	3876.00
	Baseline 2250 plus	3CBLSF50	2	375.00	750.00
	Baseline 2024	3C16471	4	110.00	440.00
	1000 Base SX-SFP	3CSFP91	40	262.00	10480.00
	<b>TOTAL</b>				
Cisco	Catalyst 2960 24 TT-L	WS-C2960-24TT-L	4	704.00	2816.00
	Catalyst 2960 24 PC-L	WS-C2960-24PC-L	13	1760.00	22880.00
	Módulo GE SFP	GLC-SX-MM=	40	310.00	12400.00
	<b>TOTAL</b>				

Tabla 4.6 Costo de los equipos de acceso

#### 4.4.1.4 *Switches de VoIP*

En la tabla 4.7 se muestra el costo de los switches que se utilizarán para conectar la central telefónica a los *switches* de distribución. Se indica además el valor de los módulos requeridos.

Marca	Equipo	Código	Q	P. Unidad	P. Final
3Com	3Com Office Connect Managed Gigabit PoE	3CDSG10PWR	1	425.00	425.00
	1000 Base SX-SFP	3CSFP91	2	262.00	524.00
	<b>TOTAL</b>				
Cisco	Catalyst 2960G-8TC-L	WS-C2960-8TC-L	1	530.00	530.00
	Módulo GE SFP	GLC-SX-MM=	2	310.00	620.00
	<b>TOTAL</b>				

Tabla 4.7 Costo de los equipos de VoIP

#### 4.4.1.5 *Switches Metro Ethernet*

En la tabla 4.8 se muestra el costo de los *switches* utilizados en la comunicación del edificio matriz hacia las instalaciones en Calderón mediante la tecnología Metro Ethernet. Se indica además el valor de los módulos requeridos.

Marca	Equipo	Código	Q	P. Unidad	P. Final
3Com	3Com Intellijack NJ2400FX	3CRNJ240FXLCTAA	2	200.00	400.00
	1000 Base SX-SFP	3CSFP91	4	262.00	1048.00
	<b>TOTAL</b>				<i>1448.00</i>
Cisco	ME 3400 Series	ME-3400G-2CS-A	2	1052.00	2104.00
	Módulo GE SFP	GLC-SX-MM=	4	310.00	1240.00
	<b>TOTAL</b>				<i>3344.00</i>

Tabla 4.8 Costo de los equipos para Metro Ethernet

#### 4.4.1.6 Teléfonos IP

En la tabla 4.9 se muestra el costo de los teléfonos necesarios para migrar a los usuarios a VoIP.

Marca	Equipo	Código	Q	P. Unidad	P. Final
3Com	3Com 3300	3C10399B	74	93.00	6882.00
	3Com 3301	3C10401B	10	142.00	1420.00
	3Com 3306	3C10406A	10	384.00	3840.00
	<b>TOTAL</b>				<i>12142.00</i>
Cisco	Cisco Unified IP Phone 521SG	CP-521SG	84	92.00	7728.00
	Cisco Unified IP Phone 524SG	CP-524SG	10	115.00	1150.00
	<b>TOTAL</b>				<i>8878.00</i>

Tabla 4.9 Costo de Teléfonos IP

#### 4.4.1.7 Costo Total

En la tabla 4.10 se muestra el costo total de los equipos necesarios descritos anteriormente de las 2 marcas propuestas para el diseño. Hasta aquí se puede definir la diferencia entre las alternativas ya que para la parte pasiva se propone un solo tipo de elementos y se presenta un único costo.

<b>Equipos</b>	<b>Marca 3Com</b>	<b>Marca Cisco</b>
<i>Switches de Core</i>	59029.00	45315.00
<i>Switches de Distribución</i>	31878.00	47953.50
<i>Switches de Acceso (y accesorios)</i>	41634.00	38096.00
<i>Switches para VoIP</i>	949.00	1150.00
<i>Switches para Metro Ethernet</i>	1448.00	3344.00
Teléfonos IP	12142.00	8878.00
<b>TOTAL</b>	<b>147080.00</b>	<b>144736.50</b>

Tabla 4.10 Costo total de ambas alternativas

#### 4.4.1.8 Alternativa que se escoge

Como se determinó en el capítulo 3 se realizará una homogenización de los equipos ya que la compatibilidad de tecnologías y la convergencia de la red son mucho más fáciles con esta característica.

Por ello, en este capítulo se han planteado dos alternativas, ambas poseen el mismo diseño de conectividad, topología, seguridad, redundancia y servicios; se diferencian únicamente en la marca de los equipos y las herramientas de administración a utilizarse.

Las dos alternativas están basadas en las recomendaciones que se presentaron previamente. La diferencia de precios entre las dos opciones no es significativa, sin embargo existente una mínima a favor de Cisco, se elige esta solución también porque es un fabricante reconocido internacionalmente que cuenta con profesionales capacitados alrededor del mundo ofreciendo soporte y capacitación continua para garantizar el funcionamiento y desempeño de redes de voz, datos y video integrándolas en una sola infraestructura.

Cisco ofrece el mejor nivel de confiabilidad y de disponibilidad de red de hasta 99.9% y siendo una red que trabaja 24 horas al día, los 7 días de la semana y que posee conexión hacia los clientes requiere de grana garantía en cuanto a disponibilidad.

A su vez, Cisco posee funcionalidades especiales que permiten reconocer todos los dispositivos de la red dinámicamente y administrarlos de una manera simple a través de herramientas compatibles con estos equipos.

TRANSELECTRIC S.A. cuenta con las licencias de *Cisco Works* para la administración y monitoreo de estos dispositivos, lo que facilitará su utilización. Esta herramienta no se puede utilizar actualmente debido a la heterogeneidad de equipos.

Cisco es una marca que provee flexibilidad y escalabilidad de red, además de seguridad, ofrece mejoras en las tecnologías que ocupa a cualquier nivel así como auto QoS y QoS avanzada.

Además, muestra una gran variedad de equipos que puedan ser usados en todas las áreas posibles que una empresa requiere y a su vez presenta compatibilidad entre sus equipos lo que facilita el manejo de los mismos.

#### **4.4.2 COSTOS PARTE PASIVA**

Para el establecimiento de costos de los elementos de la parte pasiva se tomaron los valores de las cotizaciones proporcionadas por Milestone Technologies para el caso de elementos de fibra y Tecompartes Cía. Ltda. para cableado y *racks*<sup>35</sup>.

##### **4.4.2.1 Patch Pannels**

En los pisos que serán migrados a VoIP son necesarios *patch pannels* categoría 6, mientras que para los otros pisos se requiere *patch pannel* categoría 5E. El número de puertos en los *patch pannels* depende del número de puntos de voz y datos necesarios en cada ala y de la categoría; así, se consideran de:

- 24 puertos cat6 para PBA.

---

<sup>35</sup> Referirse al anexo 4.2 acerca de cotizaciones de equipos.

- 48 puertos cat6 para 8A, 8B, 9A, 9B, 10A, 10B.
- 24 puertos cat5E para 4B, 7B.
- 48 puertos cat5E para PBB, 2B, 3B, 5A, 6A, 6B.
- Se usarán los existentes para 2A, 3A, 5B, 7A.
- No se considera el piso 4A de TermoPichincha.

En la tabla 4.11 se muestra el costo de los *patch pannels* utilizados para voz y datos de 24 y 48 puertos.

Descripción	Q	P. Unidad	P. Final
<i>Patch Pannel</i> de 48 puertos cat6	6	117.60	705.60
<i>Patch Pannel</i> de 24 puertos cat6	1	79.52	79.52
<i>Patch Pannel</i> de 48 puertos cat5E	6	84.00	504.00
<i>Patch Pannel</i> de 24 puertos cat5E	2	39.20	78.40
<b>TOTAL</b>			<b>1367.52</b>

Tabla 4.11 Costo total de *patch pannels*

#### 4.4.2.2 *Patch Cords* de Fibra

En la tabla 4.12 se muestra el costo de los *patch cords* de fibra utilizados en las diferentes conexiones, de *switch* de ala a ODF, de ODF de ala a ODF del Cuarto de Equipos, y entre *switches* de distribución y de *core*.

Descripción	Q	P. Unidad	P. Final
<i>Patchcord</i> FC - FC, <i>duplex</i> , Multimodo, 15m.	4	34.65	138.61
<i>Patchcord</i> FC - FC, <i>duplex</i> , Multimodo, 20m.	14	40.26	563.64
<i>Patchcord</i> FC - FC, <i>duplex</i> , Multimodo, 25m.	16	45.89	734.24
<i>Patchcord</i> FC - FC, <i>duplex</i> , Multimodo, 30m.	4	51.51	206.04
<i>Patchcord</i> FC - LC, <i>duplex</i> , Multimodo, 1.5m.	81	19.04	1542.24
<b>TOTAL</b>			<b>3184.77</b>

Tabla 4.12 Costo total de *patch cords* de fibra<sup>36</sup>

Los *patch cord* de 1.5 metros se usarán:

<sup>36</sup> Referirse a la tabla 3.5 Distancias aproximadas de fibra óptica. Para todos los *patch cords*, excepto de 1.5 m, se los considera

- Del *switch* de ala a su ODF: 19 alas\*2 = 38; por redundancia Q = 76.
- De ODF CE a *switches* de distribución: Q = 2.
- De *switches* de distribución a *switch* de *core* y entre distribución: Q = 3.

#### 4.4.2.3 ODFs

En la tabla 4.13 se muestra el costo de los ODFs necesarios en cada ala y en el Cuarto de Equipos.

Descripción	Q	P. Unidad	P. Final
ODF 48 puertos con Bandeja de empalmes para 12 fibras (4) y protectores de fusiones (48)	1	847.37	847.37
ODF 24 puertos, armado para 6 con Bandeja de empalmes para 12 fibras (1) y protectores de fusiones (6)	20	190.15	3803.07
<b>TOTAL</b>			<b>4650.44</b>

Tabla 4.13 Costo total de ODFs

#### 4.4.2.4 Racks

En la tabla 4.14 se muestra el costo de los gabinetes que se adquirirán para ubicarlos en cada ala. En los pisos 2A, 3A, 5B y 7A no se necesitan de nuevos *racks* porque los existentes cumplen con los requerimientos necesarios. El piso 4A no pertenece a la red de la Compañía sino a TermoPichincha.

Equipo	Q	P. Unidad	P. Final
Gabinete de pared de 12 u.	15	344.96	5174.40
<b>TOTAL</b>			<b>5174.40</b>

Tabla 4.14 Costo total de *racks*

#### 4.4.2.5 Cableado

En la tabla 4.15 se muestra el costo de los elementos de cableado, abarca el cable UTP cat6 para los puntos a instalarse en los pisos con VoIP (PBA, 8, 9 y 10), cat5E

---

dobles por tener conexión redundante.



para los de los demás pisos, así como *patch cords* de UTP cat6 y cajetines cat6 para los usuarios de VoIP y conectores RJ-45 para los de cat5E.

Las cantidades consideradas se miden de la siguiente manera:

- Usuarios migrados a tecnología VoIP (Cat6 en toda su extensión):

Cantidad: 234 usuarios<sup>37</sup>.

Distancias de cableado horizontal: entre 13 y 30<sup>38</sup>; promedio 22 metros.

Distancia del rollo de cable: 305 m.

$234 \text{ usuarios} * 22 \text{ metros} = 5184 \text{ metros}$ .

$5184 \text{ metros} / 305 \text{ metros} = 17 \text{ rollos}$ .

Total cable UTP cat6 = 18 rollos (sumando metros por holgura).

- Usuarios sin migración a VoIP que necesitan instalar nuevamente puntos (Cat5E en toda su extensión):

Cantidad: 9 usuarios<sup>39</sup>.

Distancias de cableado horizontal: 22 metros.

Distancia del rollo de cable: 305 m.

Total cable UTP cat5E = 1 rollo.

Elemento	Q	P. Unidad	P. Final
Cable UTP cat6 (rollos)	18	184.80	3326.40
Cable UTP cat5E (rollos)	1	120.96	120.96
<i>Patch cord</i> de 2m. cat6	234	3.86	904.18
Cajetines cat6 dobles	120	10.64	1276.80
Conectores RJ-45 nivel 5E	18	0.43	7.66
<b>TOTAL</b>			<b>5636.00</b>

Tabla 4.15 Costo total de otros elementos de cableado

<sup>37</sup> Referirse a tabla 3.10 Indica la asignación de *switches* por ala de acuerdo a número de usuarios.

<sup>38</sup> Referirse a punto 3.3.1.4.1 Cableado Horizontal.

<sup>39</sup> Referirse a tabla 3.7 Puntos nuevos.

#### 4.4.3 COSTOS DE INSTALACIÓN Y MONTAJE

Para estos costos se tomó datos de la persona encargada de realizar este trabajo en el edificio matriz. Los *patch cords* de fibra de 1.5m no se deben pasar por techos falsos sino solo se las conecta en los elementos, por ello se consideran como parte de instalación de *rack* y no como puntos separados. En la tabla 4.16 se muestra el costo de instalación.

*Costo por punto instalado y probado:*

Puntos en el mismo piso	10.00 usd
Puntos hacia otro piso	20.00 usd
Instalación de <i>rack</i>	60.00 usd

Nota: cortar puntos es igual que instalar

Instalación y Montaje	Q	P. Unidad	P. Final
Puntos cableado horizontal (mismo piso)	441	10.00	4410.00
Instalación de Gabinete	15	60.00	900.00
Puntos de fibra para <i>backbone</i>	40	20.00	800.00
<b>TOTAL</b>			<b>6110.00</b>

Tabla 4.16 Costo total de instalación

#### 4.4.4 TOTAL COSTOS

En la tabla 4.17 se puede ver el costo total del proyecto con los equipos de la parte activa de marca Cisco como se definió en el punto 4.4.1.8 y con los elementos de la parte pasiva.

Elementos	Costo
Costo alternativa Cisco activa	144736.50
Costo <i>Patch Pannels</i>	1367.52
Costo <i>Patch Cords</i> de Fibra	3184.77
Costo ODFs	4650.44
Costo <i>Racks</i>	5174.40
Costo Cableado	5636.00
Costo Instalación	6110.00
<b>TOTAL</b>	<b>170859.63</b>

Tabla 4.17 Costo total del proyecto

#### 4.4.5 BENEFICIOS DE LA NUEVA RED

Se debe tener en cuenta que la Compañía es una empresa que brinda servicios al público por lo que la recuperación de la inversión se dará con los beneficios que se obtendrán con el mejoramiento de la red.

TRANSELECTRIC S.A. es portador de portadores y a pesar de que el nuevo diseño involucra un gran gasto, le interesa mejorar la tecnología para proveer calidad en su servicio y manejar un mayor número de clientes. Para ello, debe tener una infraestructura de red consistente, con tecnología de vanguardia, facilidad de administración y seguridad avanzada.

Es además, una Compañía que trabaja a nivel nacional y el mejorar su infraestructura de red interna ayuda a incrementar el rendimiento, el tiempo de respuesta y el acceso a los servidores de la empresa. Es importante tener una buena estructura LAN para proveer un buen servicio WAN a sus clientes.

Con una red LAN óptima no se perderían correos, en especial los enviados por parte de los clientes, permitiendo una solución eficiente a los requerimientos de los mismos. A su vez, al tener VoIP se podría comunicar con los clientes que también

tengan esta tecnología y así se economiza en costo telefónico.

Mejorando la tecnología para soportar un mayor número de clientes, TRANSELECTRIC S.A. se beneficia con los ingresos que obtendrá al aumentar sus clientes, y más aún si se permite ofrecer servicios con mayor capacidad. Incrementando el nivel de seguridad se evitará el acceso de intrusos en la red que puedan de alguna manera obstruir el desempeño de ésta.

Este nuevo diseño le permitirá a la red obtener flexibilidad y escalabilidad para las nuevas aplicaciones que la Compañía requiera a futuro. Soportará el Sistema Integrado que será implementado en pocos meses en TRANSELECTRIC S.A. y podrá aceptar aplicaciones en tiempo real tales como videoconferencia si se desea.

Actualmente si ocurre un error debido al mal cableado, desorganización y falta de administración, la red no opera al 100% en un tiempo considerable. Se puede recuperar parte de la inversión bajando el tiempo de superación de falla y se eliminaría, en lo posible, el costo por horas de las personas que estén inactivas mientras dure la recuperación del sistema.

Al tener una reestructuración del cableado, se puede documentar toda la información, de tal manera, quienes se encargan de la administración de la red LAN solucionarían cualquier inconveniente menor que se presente sin la necesidad de utilizar los servicios de otras empresas certificadoras que realizan esta documentación a costos elevados.

# CAPÍTULO 5

**CONCLUSIONES Y  
RECOMENDACIONES**

## CONCLUSIONES Y RECOMENDACIONES

### 5.1 CONCLUSIONES

- ✓ El objetivo principal de la propuesta de diseño es mejorar la situación actual de la red LAN de TRANSELECTRIC S.A. proporcionando escalabilidad, flexibilidad, facilidad de administración, seguridad y soporte de nuevas aplicaciones.
- ✓ Las redes Ethernet a través del tiempo han tenido un gran crecimiento y constituyen una de las tecnologías más utilizadas a nivel mundial; su utilización ayuda en la reducción de costos y en un mayor desarrollo tecnológico de la Compañía.
- ✓ Con las bases teóricas descritas, se diseñó una red para TRANSELECTRIC S.A., presentando dos alternativas de equipos para su implementación, y un presupuesto referencial para cada una de ellas.
- ✓ Con el propósito de no desperdiciar recursos existentes en cuanto a equipos y cableado, se adoptó la topología en estrella vigente actualmente, pero solucionando los problemas encontrados.
- ✓ Se propusieron dos alternativas de equipos dentro del diseño para reutilizar los equipos existentes en la Compañía y a la vez adquirir equipos que soporten nuevas tecnologías, incremento de ancho de banda y nuevas aplicaciones. Estas alternativas además, permitirán la utilización de fibra óptica como medio de comunicación en el *backbone* del edificio.

- ✓ El análisis de la situación actual de la red LAN permitió definir las debilidades de la misma y encontrar los requerimientos actuales y futuros que tiene la Compañía.
- ✓ No existe una documentación actualizada ni un correcto etiquetado ni organización del cableado en el edificio matriz; así, cuando un usuario tiene fallas en la red es complicado averiguar dónde se encuentra conectado su punto y solucionar su problema.
- ✓ La infraestructura de Cuartos de Equipos necesita una mejora física, especialmente en seguridad, acceso, etiquetado de cables, entre otros.
- ✓ Los equipos activos de red se interconectan a un equipo central (3Com SuperStack 3 *Switch* 5500); este equipo es quien lleva todo tipo de tráfico existente en el edificio, si sucede algún inconveniente con él, se convierte en un punto crítico de operabilidad, ya que dejaría completamente inactiva a la red.
- ✓ Se cuenta con equipos de diferentes marcas, lo que no facilita la administración de los mismos porque se necesita de las licencias de los diferentes programas de administración, es por eso que no se cuenta con un sistema de administración de red.
- ✓ En el Cuarto de Equipos del quinto piso se tiene una central telefónica Siemens de excelentes características y muchas funcionalidades que no están siendo aprovechadas. Una de ellas es que soporta tecnologías como VoIP la cual representa una gran ventaja en costos en relación a una tecnología nueva a implementar.

- ✓ Las políticas de seguridad que se tiene actualmente en la Compañía no son lo suficientemente fuertes para prevenir el acceso de intrusos, sobre todo de los usuarios internos que constituyen la mayor amenaza de ataque en la intranet.
- ✓ La competitividad actual en servicios de Telecomunicaciones se da a nivel mundial. En lo que se refiere al país también se cuenta con empresas que se dedican a brindar estos servicios; por ello, se tiene la necesidad de una red escalable, adaptable, confiable y de gran capacidad como la del presente diseño, con la cual se podrá tener una red interna óptima que al conectarse a la red WAN podrá brindar servicios de telecomunicaciones de mejor calidad.
- ✓ Al emplear en el diseño un esquema jerárquico por capas se permitirá que en el futuro más usuarios puedan ser conectados a la red utilizando el mismo esquema de conexión, sin alterar el diseño.
- ✓ La administración no depende técnicamente del diseño de la red pero se lo debe incluir como parte de las alternativas planteadas. Dentro de ésta se tendrá: monitoreo de los recursos críticos, administración de servicios, administración de seguridad, etc.
- ✓ El costo del funcionamiento de medidas de seguridad y los resultados de uso de las mismas son directamente proporcionales; a mayor costo, mejores resultados y mejor tecnología.
- ✓ *Network Management System* es el *software* de monitoreo de red basado en SNMP que mantendría una base de datos de los dispositivos de red, su conectividad permitirá realizar actividades de monitoreo y configuración con interfaces gráficas de usuario. Dentro de la versión comercial de *software* que se requiere se tiene *Cisco Works*. La información de este producto se la puede obtener en los respectivos sitios de Internet de las empresas proveedoras.



- ✓ Los niveles de redundancia establecidos protegerán a los elementos críticos de la red. Se tiene redundancia en los elementos activos tales como los *switches* de distribución. También se cuenta con enlaces redundantes hacia estos dispositivos desde cada ala del edificio para respaldo en caso de falla.
- ✓ Es necesario presentar un plan de contingencia para posibles problemas que puedan suceder en la red, es por ello que el diseño lo incluye.
- ✓ Proveer seguridad a los equipos y a la red interna elimina o al menos disminuye considerablemente los accesos externos a la red y a la DMZ.
- ✓ La Voz sobre IP (VoIP) permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de ésta; así, se podrá realizar llamadas telefónicas ordinarias sobre la red de datos utilizando teléfonos IP. También se puede acceder a servicios como mensajes de voz, correos, etc. transportados vía redes IP, en lugar de ser transportados por la red telefónica convencional.
- ✓ La ventaja real de la Voz sobre IP es la transmisión de voz sobre la red de datos, sin necesidad de una red exclusiva para la voz, lo que reduce costos en la implementación.
- ✓ Ya que el nuevo diseño propone una red de datos con un amplio ancho de banda, también permite la utilización de esta red para el tráfico de voz entre las distintas áreas de la empresa (que inicialmente serán migradas) y hacia clientes que tengan esta tecnología. Son muchas las ventajas que se obtendrían al transmitir la voz y los datos por la misma red, por ejemplo un considerable ahorro en costos de comunicaciones.
- ✓ Actualmente la Compañía no tiene ninguna organización en el direccionamiento IP de la red, por lo que fue necesario realizarlo nuevamente,

para permitir una mejor distribución por áreas e incluso incrementar VLANs de voz y de datos para una óptima comunicación.

- ✓ La alternativa homogénea de equipos (red de datos) cumple con los requerimientos técnicos establecidos. Adicionalmente, se consideró el grado de confiabilidad para secciones críticas en la red (nivel de *core*, distribución), siendo Cisco la opción elegida para ello.
- ✓ La compatibilidad de dispositivos y la convergencia de la red son mucho más fáciles cuando se tiene equipos de la misma tecnología. Por ello, la propuesta de homogenización de equipos activos permitirá desarrollar la gestión y monitoreo de la red.
- ✓ Las políticas de seguridad fueron establecidas de manera específica, a fin de que cubran aspectos críticos de la red (*software*, *hardware*, usuarios, etc.), y evitar intrusiones de quienes no deberían tener acceso, por lo que es necesaria su vigencia en la red diseñada.
- ✓ La escalabilidad de la red le permitirá a TRANSELECTRIC S.A. incrementar más servicios como el Sistema Integrado sin mayores inconvenientes.
- ✓ Para el enlace con las instalaciones de Calderón se considera la tecnología Metro Ethernet. Metro Ethernet soporta aplicaciones de mayor ancho de banda, acceso a Internet más rápido para los trabajadores de ambas instalaciones, no desperdicia el ancho de banda, ofrece alta disponibilidad, es barata y fácil de implementar, provee calidad de servicio.
- ✓ La red diseñada permite tener un crecimiento en las aplicaciones y en la demanda de ancho de banda proyectado a 10 años.

- ✓ El tipo de fibra óptica escogida para la comunicación del *backbone* fue la multimodo ya que las distancias son pequeñas; recomendado por la UIT-T, garantiza un adecuado funcionamiento de la red con parámetros de atenuación y dispersión establecidos.
- ✓ La fibra, sin duda, es hasta ahora el medio más fiable de comunicaciones ópticas. La utilización de fibra óptica, a pesar de ser más costosa, provee mayor seguridad al evitar que se “caiga” la red por cortes, robos o vandalismo.
- ✓ Se buscaron equipos que soporten SNMP para monitoreo, de manera que sea factible integrarlos en un sistema NMS (*Network Management System*). Con ello se permitirá en especial identificar eventos generados en los dispositivos (*traps*) que puedan presentar alarmas. Además se puede realizar el monitoreo de rendimiento, con la recolección de datos del comportamiento de los dispositivos de red.
- ✓ En el diseño se reutilizan los equipos que tiene la Compañía como servidores, *firewall*, *router*, PBX, teléfonos, computadores, cableado estructurado, etc.
- ✓ La central telefónica IP Siemens permite tener el servicio de voz tradicional agregándole nuevos y mejores servicios como llamada por *Internet*, mensajería unificada, Voz sobre IP, entre otros servicios.
- ✓ La selección de equipos activos se realiza en base al análisis de modelos y marcas disponibles en el mercado, de manera que permita obtener resultados óptimos tanto a nivel operativo como económico.
- ✓ El óptimo funcionamiento de la red y de las aplicaciones dependen de la buena aplicación de las políticas de seguridad y calidad de servicio que utilice el administrador de la red.

- ✓ En el desarrollo de este trabajo se aplicaron los conocimientos adquiridos durante la carrera, lo que ayudó a tener un mejor criterio en el nuevo diseño de la red LAN de la Compañía.
- ✓ El realizar proyectos similares en materias superiores de la carrera desarrolla aptitudes en los estudiantes para tener un criterio más amplio y acorde a la realidad, que permita entender los requerimientos que pueden presentar las diferentes organizaciones y proveer de soluciones a las mismas.
- ✓ A medida que las empresas en el Ecuador conozcan las ventajas de tener redes convergentes, esta tecnología empezará a desarrollarse y asegurará interoperabilidad e integración entre ellas.

## 5.2 RECOMENDACIONES

- ✓ Que los equipos a usarse en la red y los que se adquirirán, cumplan como mínimo cada una de las especificaciones básicas detalladas en el presente proyecto para un correcto funcionamiento del sistema.
- ✓ Optimizar la potencia de procesamiento en el *switch* de *core* para tener la mayor tasa de transferencia posible en el *backbone*.
- ✓ No dejar las contraseñas que vienen por defecto en los equipos activos, ya que éstas son conocidas a nivel mundial y constituyen una alta amenaza de intrusión en la red, sobre todo en la administración y acceso a la información.
- ✓ La asignación de un encargado de soporte para la red, tanto en la parte de datos como en la de voz, de manera que se ocupe de la administración, gestión, instalación de aplicaciones, mantenimiento de los equipos, actualización de licencias, etc.

- ✓ Definir responsables de cada recurso de la organización y de su protección, siendo conveniente delimitar claramente el área de responsabilidad de cada persona para que no existan huecos o problemas de falta de soporte.
- ✓ Continuar y terminar la migración a VoIP del resto del edificio matriz ya que disminuiría el uso de red telefónica pública y permitiría llamadas gratuitas a todos los usuarios internos.
- ✓ Se pide actualizar la documentación de la red cada cierto tiempo y cada vez que se realice cambios de equipos, de puntos, ó se incremente aplicaciones, etc.
- ✓ Tener una adecuada monitorización del uso de los recursos de la red permite determinar posibles “cuellos de botella” que podrían ocasionar fallos del sistema y de seguridad.
- ✓ Definir y documentar reglas y derechos de acceso a los recursos del sistema de información para cada usuario o grupo de usuarios en una declaración de política de accesos. Esta política debe ser coherente con la clasificación de los activos e inventario de recursos.
- ✓ Limitar la asignación de privilegios de acceso ya que son la principal vulnerabilidad, por lo que deberán estar perfectamente identificados. Los privilegios tienen que revisarse de forma periódica para evitar la existencia de los que ya no sean necesarios.
- ✓ Archivar todos los planos de las distintas áreas, distribución de puntos tanto de voz como de datos, manuales del equipo activo, puesto que esto facilitará en un futuro la integración de voz, datos y video es decir la migración de Telefonía IP a una Red IP, y de una Red LAN a Telefonía o Red IP.

- ✓ La seguridad de la información debe ser considerada como un proceso de mejoramiento continuo y no un estado estático, los nuevos requerimientos de seguridad deben ajustarse a los cambios de la Compañía.
- ✓ Capacitar al personal para de esta manera motivarlo a utilizar el sistema y familiarizarse con su funcionamiento.
- ✓ Implementar el diseño propuesto con equipos de la marca Cisco que tiene participación mayoritaria en el mercado de equipos de conectividad para disminuir la posibilidad de no tener soporte en el futuro.
- ✓ Utilizar la herramienta de administración *Cisco Works* debido a que la alternativa de equipos elegida será Cisco y a su vez, en la Compañía ya se posee la licencia. Además con esta herramienta se puede trabajar conjuntamente con *What's Up* la cual es la herramienta que se maneja en el Centro de Gestión de Telecomunicaciones.
- ✓ Que al realizar los contratos en la adquisición de los equipos, se incluya una garantía técnica de al menos 12 meses contra defectos funcionales que se produzcan en los equipos en ese período.

## REFERENCIAS BIBLIOGRÁFICAS

### Proyectos de Titulación

- Diseño de la red de comunicaciones de la Mutualista Pichincha para la Ciudad de Quito basado en tecnologías Ethernet de alta velocidad - Carrión Morales, Mauricio Fabián.
- Diseño de la red de Telecomunicaciones para el Banco Continental - Díaz Cobo, Jaime Marcelo.
- Diseño de un anillo de fibra óptica para la ciudad de Manta - Guillén Robles, Wilson Marlon.
- Diseño de una red de comunicaciones para el Honorable Consejo Provincial de Cotopaxi - Acurio Cantuña, Yadira Fernanda.
- Diseño de una red de datos para la ciudad de Santo Domingo de los Colorados - Vintimilla Alulema, Gustavo Rafael.
- Diseño de una red de voz y datos para una industria agrícola utilizando plataforma CISCO - Arias Tapia, Geovanni Fernando.
- Diseño de una red integrada de voz y datos para el campus E.P.N. basado en un análisis comparativo de las soluciones existentes en el mercado nacional - Cevallos Martínez, Gabriel Francisco,
- Diseño del sistema de red para transmisión de voz y datos para el municipio de Santo Domingo y criterios para su administración - Salazar Armijos, Diego Ricardo.

### Referencias de figuras

Capítulo 1

- [1] <http://www.jegsworks.com/Lessons-sp/lesson7/lesson7-5.htm>
- [2] <http://www.monografias.com/trabajos60/wimax-banda-ancha/wimax-banda-ancha2.shtml>
- [3] [http://www.fujitsu.com/es/services/solutions/ip/index\\_Net.html](http://www.fujitsu.com/es/services/solutions/ip/index_Net.html)
- [4] <http://www.monografias.com/trabajos11/reco/reco.shtml>
- [5] <http://www.edufuturo.com/educacion.php?c=4050>
- [6] <http://albertjh.cymaho.com/?s=inalmente&x=1>
- [7] Currícula CISCO v3.1 Módulo 1
- [8] [http://tvcentlinea.com/tienda/catalog/product\\_info.php?cPath=87&products\\_id=617](http://tvcentlinea.com/tienda/catalog/product_info.php?cPath=87&products_id=617)
- [9] <http://esp.hyperlinesystems.com/catalog/cable/ftp-c5e-s.shtml>
- [10] <http://www.opcionweb.com/?p=114;>  
[http://www.cableparts.com.ar/productos/docs/fibra/CONECTORES\\_FIBRA.jpg](http://www.cableparts.com.ar/productos/docs/fibra/CONECTORES_FIBRA.jpg)
- [11] [http://www.unicrom.com/Tel\\_espectroelectromagnetico.asp](http://www.unicrom.com/Tel_espectroelectromagnetico.asp)

- [12] <http://arieldx.tripod.com/manualdx/bandas/bandas.htm>
- [13] <http://www.eveliux.com/mx/sistema-de-cableado-estructurado.php>
- [14] <http://www.monografias.com/trabajos15/arquitectura-tcp/arquitectura-tcp.shtml>
- [15] <http://html.rincondelvago.com/protocolo-de-internet-ip-v6.html>
- [16] <http://es.kioskea.net/contents/internet/ip.php3>
- [17] [http://www.uv.es/montanan/redes/trabajos/Voip\\_nuria.doc](http://www.uv.es/montanan/redes/trabajos/Voip_nuria.doc)
- [18] <http://www.monografias.com/trabajos33/estandar-voip/estandar-voip2.shtml>
- [19] [http://es.wikipedia.org/wiki/Protocolos\\_de\\_VoIP](http://es.wikipedia.org/wiki/Protocolos_de_VoIP)

## Capítulo 2

- [1] [http://www.transelectric.com.ec/transelectric\\_portal/portal/main.do?sectionCode=98](http://www.transelectric.com.ec/transelectric_portal/portal/main.do?sectionCode=98)
- [2] [http://www.matels.com/catalogo/index.php?manufacturers\\_id=18](http://www.matels.com/catalogo/index.php?manufacturers_id=18)
- [3] [http://www.ciao.com/Cisco\\_Catalyst\\_2924\\_XL\\_switch\\_24\\_ports\\_15370056](http://www.ciao.com/Cisco_Catalyst_2924_XL_switch_24_ports_15370056)  
[http://www.b2net.co.uk/cisco/cisco\\_catalyst\\_2950\\_series\\_switches.htm](http://www.b2net.co.uk/cisco/cisco_catalyst_2950_series_switches.htm)  
[http://www.cisco.com/en/US/products/ps6406/prod\\_view\\_selector.html](http://www.cisco.com/en/US/products/ps6406/prod_view_selector.html)  
[http://www.b2net.co.uk/cisco/cisco\\_catalyst\\_3500\\_series\\_switches.htm](http://www.b2net.co.uk/cisco/cisco_catalyst_3500_series_switches.htm)  
[http://newsroom.cisco.com/dlls/prod\\_041503b.html](http://newsroom.cisco.com/dlls/prod_041503b.html)
- [4] <http://www.kaboodle.com/reviews/3com-officeconnect-dual-speed-hub-16>  
[http://www.ciao.es/3Com\\_SuperStack\\_3\\_Switch\\_3824\\_24\\_637018](http://www.ciao.es/3Com_SuperStack_3_Switch_3824_24_637018)  
[http://www.ciao.es/3Com\\_SuperStack\\_II\\_RAS\\_1500\\_Expansion\\_Unit\\_690908](http://www.ciao.es/3Com_SuperStack_II_RAS_1500_Expansion_Unit_690908)  
<http://www.wikio.com/product/3com-superstack-ii-3300-24-ports-37853.html>  
[http://www.ciao.es/3Com\\_SuperStack\\_III\\_Dual\\_Speed\\_Hub\\_500\\_24\\_642721](http://www.ciao.es/3Com_SuperStack_III_Dual_Speed_Hub_500_24_642721)  
[http://www.ciao.es/3Com\\_SuperStack\\_3\\_Switch\\_4228G\\_24\\_640928](http://www.ciao.es/3Com_SuperStack_3_Switch_4228G_24_640928)  
<http://www.saz.com.ec/vercategoriap.asp?idcategoria=RED&page=9>
- [5] <http://www.itsky.com.au/assets/catalog/parts/>  
<http://www.twenga.pl/cena-DES-1024R-D-LINK-Hub-1441-0>
- [6] [http://www.cisco.com/en/US/products/ps5854/prod\\_view\\_selector.html](http://www.cisco.com/en/US/products/ps5854/prod_view_selector.html)
- [7] <http://www.abox.com/productos.asp?pid=279>
- [8] <http://www.ncix.com/products/index.php?sku=19885&vpn=CISCO871W-G-A-K9&manufacture=CISCO>
- [9] <http://www.dooyoo.es/equipos-de-red/check-point-vpn-1-utm-edge-x16>
- [10] <http://www.sonicguard.com/Packageer.asp>  
<http://www.dealtime.co.uk/xPF-Attachmate-Packageer-PacketShaper-1500-162682>
- [11] Información proporcionada por el área de Informática
- [12] Diagrama proporcionado por el área de Telecomunicaciones
- [13] <http://www.sulit.com.ph/index.php/view+classifieds/id/927394/Panasonic+KX->



TD1232+phone+system

- [14] <http://www.cleverttech.com.mx/hipath/4500.htm>
- [15] <http://www.its-tel.ru/>
- [16] [http://www.ciao.es/Multi\\_Tech\\_MultiVOIP\\_MVP200\\_691128](http://www.ciao.es/Multi_Tech_MultiVOIP_MVP200_691128)
- [17] [http://www.ciao.com/Hayes\\_ACCURA\\_V\\_92\\_External\\_Faxmodem\\_Model\\_H08\\_15328\\_fax\\_mode\\_m\\_15396910](http://www.ciao.com/Hayes_ACCURA_V_92_External_Faxmodem_Model_H08_15328_fax_mode_m_15396910)
- [18] [http://www.mundoanuncio.com/categoria/internet\\_multimedia\\_46/buscar/plantas.html/](http://www.mundoanuncio.com/categoria/internet_multimedia_46/buscar/plantas.html/)
- [19] <http://www.powertec.com.au/shop/ericsson-g36a-voicefaxinternetpabx-p-252.html>

## Capítulo 3

- [1] [http://www.futuretech.com/services\\_traffic.html](http://www.futuretech.com/services_traffic.html)
- [2] <http://www.sistemasyenlaces.com.ar/tabladecodecs.html>
- [3] <http://www.unicartagena.edu.co/invitacion4/Anexo%209%20Especificaciones%20t%E8cnicas%20cableado%20estructurado%20CEV.doc>
- [4] <http://www.procables.com.co/portal/modules/Downloads/files/1173286357-fibraoptica6hilosarmada.pdf>
- [5] <http://www.cable-master.com.tw/PE/PE-SFROT45E.html>
- [6] [http://www.matels.com/catalogo/index.php?manufacturers\\_id=18](http://www.matels.com/catalogo/index.php?manufacturers_id=18)
- [7] <http://www.ciens.ucv.ve/cccd/documentos/Especificaciones%20Tecnicas%20-%20ver.%205-11-032.doc>
- [8] Currícula CISCO v4.0 Módulo 3
- [9] [http://www.intitec.org/memorias\\_conferecias/Memorias\\_Metroethernet.pdf](http://www.intitec.org/memorias_conferecias/Memorias_Metroethernet.pdf)

## Capítulo 4

- [1] [http://www.3com.com/prod/es\\_](http://www.3com.com/prod/es_)
- [2] [http://www.3com.com/products/en\\_US/detail.jsp?tab=features&pathtype=purchase&sku=3CRNJ240FXLCTAA-75](http://www.3com.com/products/en_US/detail.jsp?tab=features&pathtype=purchase&sku=3CRNJ240FXLCTAA-75)
- [3] [http://www.ciao.es/Cisco\\_Catalyst\\_6509\\_E\\_Firewall\\_Security\\_System\\_Bundle\\_1216367](http://www.ciao.es/Cisco_Catalyst_6509_E_Firewall_Security_System_Bundle_1216367)
- [4] <http://www.twenga.co.uk/prices-Catalyst-3560E-12SD-S-CISCO-Network-hub-414595-0>
- [5] [http://www.esemanal.com.mx/articulos.php?id\\_sec=11&id\\_art=6555](http://www.esemanal.com.mx/articulos.php?id_sec=11&id_art=6555)
- [6] [http://www.acuista.com/x/190447-d-cisco\\_catalyst\\_2960\\_24lt\\_l\\_ws\\_c2960\\_24lt\\_l\\_switch\\_gestionable\\_](http://www.acuista.com/x/190447-d-cisco_catalyst_2960_24lt_l_ws_c2960_24lt_l_switch_gestionable_)
- [7] <http://www.provantage.com/cisco-systems-me-3400-24ts-d-7CSC90UL.htm>

## ANEXOS

1.1 Estándares IEEE 802.3 Ethernet e IEEE 802.5 *Token Ring*

1.2 Estándares de cableado estructurado ANSI/EIA-TIA

2.1 Equipo *Check Point* VPN-1 UTM

2.2 Equipos *PacketShaper* 3500 y *Packeteer* 1550

2.3 Tipos de paquetes encontrados en el monitoreo de la red LAN

3.1 Planos de los Puntos de Red del Edificio

4.1 Especificaciones Técnicas de nuevos equipos considerados para el diseño

4.2 Cotizaciones de equipos