

UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio Politécnico

Departamento de Ingeniería Electrónica

Propuesta de Diseño Jerárquico de la Red de Área Local para el Edificio Matriz de la Compañía TRANSELECTRIC S.A. ubicado en la ciudad de Quito

Tesis de grado presentada como requisito para la obtención del título de
Ingeniero Electrónico en Telecomunicaciones

José Javier Orozco Echeverría

Quito, 18 de Diciembre de 2008

**Propuesta de Diseño Jerárquico de la Red de Área Local para el
Edificio Matriz de la Compañía TRANSELECTRIC S.A.
ubicado en la ciudad de Quito**

Hoja de Aprobación de Tesis

Fausto Vasco, Ing.
Director de Tesis

.....

Santiago Navarro, Ph.D.
Miembro del Comité de Tesis

.....

Fernando Romo, M.Sc.
Decano Colegio Politécnico

.....

© Derechos de autor
José Javier Orozco Echeverría
2008

Resumen

Este proyecto ofrece una introducción a los conceptos relacionados con medios de transmisión de cobre y fibra óptica utilizados para voz, datos y video; los subsistemas de cableado estructurado; el diseño de una red según el modelo jerárquico y la configuración de dispositivos de conmutación. Ante la necesidad de renovar la infraestructura de telecomunicaciones e implementar tecnologías de alto rendimiento, la Compañía TRANSELECTRIC S.A. permite llevar a cabo un estudio sobre las condiciones operativas de la Red de Área Local instalada en su edificio matriz. La investigación comprende el reconocimiento del espacio físico destinado para el Cuarto de Telecomunicaciones, la documentación de los elementos activos y pasivos existentes, la determinación de los requerimientos actuales, el análisis de tráfico y la medición del consumo de ancho de banda. Con base en esta información, se plantea una solución integral que considera el diseño de una topología redundante, en la cual se fusionan las Capas de Núcleo y Distribución para administrar eficientemente los recursos informáticos y garantizar alta disponibilidad. A nivel de Acceso se colocan equipos con capacidad de implementar seguridad y segmentación para las redes de datos individuales. Para configurar los conmutadores y verificar su funcionamiento se emplea una herramienta especializada de simulación de redes así como una topología equivalente en ambiente de laboratorio. Además, se hace referencia a un programa de gestión que cuenta con una gama de funcionalidades para supervisar y controlar el desempeño de los elementos de red. Finalmente, se analizan varias ofertas económicas para elegir la mejor opción de adquisición en caso de implementar la propuesta formulada.

Abstract

This Project offers an introduction to the concepts related with copper and fiber optics transmission media, which are used in voice, data and video; structured cabling subsystems; network design according to the hierarchical model and the configuration of switching devices. Due to the need for renewing the telecommunications infrastructure and to implement high performance technologies, TRANSELECTRIC S.A. supported a study regarding the operative conditions of the LAN (Local Area Network) installed at its headquarters. The research covers the identification of the area where the Telecommunications Room is located, the registration of existent active and passive elements, the determination of actual requirements, traffic analysis and the measurement of bandwidth consumption. Based upon this information, a global solution that considers the design of a redundant topology is created, joining the Core and Distribution Layers in order to efficiently manage the computing resources and guarantee high availability. On the Access Layer, equipment capable of implementing security and segmenting individual data networks is incorporated. As a means to configure the switches and verify its operation, a specialized network simulation tool as well as an equivalent topology in lab environment is used. Moreover, a management software with a variety of applications to supervise and control the performance of the network elements is included. Finally, a series of economical offers are analyzed in order to choose the most suitable buying option in the event of implementing the suggested proposal.

Índice General

Capítulo 1 - TRANSELECTRIC S.A.	1
1.1 Historia	1
1.2 Funcionamiento	1
1.2.1 Sistema Nacional de Transmisión (SNT)	5
1.2.1.1 Estructura	5
1.2.1.2 Manejo	6
1.2.2 Telecomunicaciones	7
1.2.2.1 Servicios	7
1.2.2.2 Clientes	7
1.2.2.3 Sistema de PLC	8
1.2.2.4 Red de Fibra Óptica	8
1.2.2.5 Gerencia de Telecomunicaciones	15
1.3 Estrategia Organizacional	17
1.3.1 Misión	17
1.3.2 Visión	17
1.3.3 Valores Institucionales	17
1.3.4 Áreas de la Compañía	18
 Capítulo 2 - FUNDAMENTOS TEÓRICOS	 28
2.1 Elementos Pasivos	28
2.1.1 Cable de Cobre	28
2.1.1.1 Cable de Par Trenzado	29
2.1.1.2 Cable Coaxial	34
2.1.2 Cable de Fibra Óptica	35
2.1.2.1 Funcionamiento	36
2.1.2.2 Tipos	39
2.1.2.3 Ventajas	40
2.1.2.4 Desventajas	41

2.1.2.5 Conectores	41
2.1.3 Cableado Estructurado	44
2.1.3.1 Reglas	45
2.1.3.2 Estándares	45
2.1.3.3 Subsistemas	49
2.1.3.4 Cableado de Backbone (Vertical)	60
2.1.3.5 Cableado del Área de Trabajo	61
2.2 Elementos Activos	62
2.2.1 Red Jerárquica	62
2.2.1.1 Beneficios	63
2.2.1.2 Principios de Diseño	64
2.2.2 Red Convergente	65
2.2.3 Selección de Conmutadores	66
2.2.3.1 Análisis de Flujo de Tráfico	66
2.2.3.2 Diagramas Topológicos	68
2.2.3.3 Modelos de Conmutadores	69
2.2.3.4 Características de los Conmutadores	70
2.2.3.5 Características de los Conmutadores en una Red Jerárquica	71
2.2.4 Redes Ethernet/802.3	73
2.2.4.1 Conceptos Básicos	73
2.2.4.2 Consideraciones de Diseño	77
2.2.4.3 Métodos de Conmutación	81
2.2.4.4 Tipos de Conmutación	83
2.2.4.5 Búfer de Memoria	83
2.2.4.6 Conmutación de Capa 2 y Capa 3	84
2.2.5 Elección del Fabricante	84
2.2.6 Cisco IOS (Internetwork Operating System)	85
2.2.7 CLI (Command Line Interface)	85
2.2.7.1 Modos	85
2.2.7.2 Ayuda	86
2.2.7.3 Secuencia de Boteo	87

2.2.7.4 Configuración Básica	87
2.2.7.5 Administración Básica	88
2.2.7.6 Seguridad Básica	89
2.2.7.7 Telnet y SSH	90
2.2.7.8 Seguridad de Puertos	91
2.2.7.9 Modos de Violación de Seguridad	92
2.2.7.10 Puertos No Utilizados	93
2.2.8 VLAN	93
2.2.8.1 Beneficios	93
2.2.8.2 Rangos	94
2.2.8.3 Tipos	95
2.2.8.4 Tipos de Tráfico de Red	95
2.2.8.5 Puertos de un Conmutador	96
2.2.8.6 Troncales	97
2.2.8.7 Configuración	100
2.2.8.8 Administración	101
2.2.9 VTP	102
2.2.9.1 Beneficios	102
2.2.9.2 Componentes	102
2.2.9.3 Parámetros VTP	105
2.2.9.4 Configuración	107
2.2.10 STP (Spanning Tree Protocol)	108
2.2.10.1 Redundancia	108
2.2.10.2 Algoritmo	112
2.2.10.3 BPDU	114
2.2.10.4 Bridge ID	115
2.2.10.5 Roles de Puertos	117
2.2.10.6 Estados de Puertos y Temporizadores	118
2.2.10.7 Convergencia	119
2.2.10.8 Proceso de Notificación de Cambio en la Topología	121
2.2.11 RSTP (Rapid Spanning Tree Protocol)	121
2.2.11.1 Roles de Puerto	122

2.2.11.2 Estados de Puerto	122
2.2.11.3 BPDUs	122
2.2.11.4 Tipos de Puerto	123
2.2.11.5 Sincronización	123
2.2.11.6 Configuración	124
2.2.12 RPVST+ (Rapid Per-VLAN Spanning Tree Protocol)	125
2.2.13 MST o MSTP (Multiple Spanning Tree Protocol)	125
2.2.13.1 Regiones MST	125
2.2.13.2 Instancias	126
2.2.13.3 Configuración	127
2.2.14 Agrupación de Enlaces	128
2.2.14.1 Balanceo de Carga	128
2.2.14.2 Protocolos de Negociación	128
2.2.15 HSRP (Hot Standby Router Protocol)	129
2.2.15.1 Elección del Enrutador HSRP	129
2.2.15.2 Autenticación	129
2.2.15.3 Direccionamiento de la Puerta de Enlace HSRP ...	130
2.2.16 VRRP (Virtual Router Redundancy Protocol)	130
2.2.17 GLBP (Gateway Load Balancing Protocol)	130
2.2.17.1 AVG (Active Virtual Gateway)	130
2.2.17.2 AVF (Active Virtual Forwarder)	131
2.2.17.3 Balanceo de Carga	131
2.2.18 Pruebas	132
2.2.18.1 Ping	132
2.2.18.2 Tracert	132

Capítulo 3 - SITUACIÓN ACTUAL Y PROPUESTA DE DISEÑO

3.1 Situación Actual	133
3.1.1 Ubicación	133
3.1.2 Cuartos de Telecomunicaciones	134
3.1.2.1 Noveno Piso	134
3.1.2.2 Quinto Piso	147

3.1.3 Cuartos de Telecomunicaciones y Sala de Servidores	157
3.1.4 Cableado Horizontal y Áreas de Trabajo	159
3.1.5 Cableado Vertical y Dispositivos por Ala	159
3.1.5.1 Conmutadores Administrables	161
3.1.5.2 Conmutadores No Administrables	164
3.1.6 Número de Usuarios	165
3.1.7 Sistemas Empresariales	166
3.1.8 Tráfico y Ancho de Banda	172
3.1.8.1 Análisis de Tráfico	172
3.1.8.2 Medición del Ancho de Banda	189
3.2 Propuesta de Diseño	200
3.2.1 Cuarto de Telecomunicaciones	200
3.2.1.1 Estructura, Control de Temperatura y Equipamiento	200
3.2.1.2 Identificación de Dispositivos y Cables de	
Interconexión	205
3.2.2 Cableado Vertical	205
3.2.3 Cableado Horizontal y Áreas de Trabajo	206
3.2.3.1 Componentes del Armario por Ala	207
3.2.4 Configuración de los Conmutadores	208
3.2.4.1 Configuración Básica	208
3.2.4.2 Configuración de VTP	212
3.2.4.3 Configuración de STP	213
3.2.4.4 Configuración de EtherChannel	213
3.2.4.5 Configuración de HSRP (Hot Standby Router	
Protocol)	214
3.2.4.6 Configuración de SNMP (Simple Network	
Management Protocol)	214
3.2.5 Simulación en Packet Tracer	214
3.2.5.1 Configuración Básica	214
3.2.5.2 Capa de Core/Distribución	220
3.2.5.3 Capa de Acceso	233
3.2.5.4 Verificar la conectividad	240

3.2.6 Simulación en Laboratorio	243
3.2.6.1 Configuración Básica	245
3.2.6.2 Capa de Core/Distribución	250
3.2.6.3 Capa de Acceso	262
3.2.6.4 Verificar la Conectividad	268
3.2.7 Gestión de la Red	271
3.2.7.1 Creación de Mapas	271
3.2.7.2 Estado de los Dispositivos	274
3.2.7.3 Servidor Web	275
3.2.7.4 Opciones de Notificaciones	276
3.2.7.5 Simulación de la Topología Completa	279
3.2.7.6 Gestión de la Topología Equivalente	286
3.3 Análisis de Costos	295
3.3.1 Cuarto de Telecomunicaciones	295
3.3.1.1 Infraestructura de Seguridad, Sistema de Climatización y Control de Incendios	295
3.3.1.2 Bastidores para Extensiones y Líneas Telefónicas ..	295
3.3.1.3 Armarios para Conmutadores de Core/Distribución	296
3.3.2 Distribución de Armarios para Conmutadores de Acceso	298
3.3.3 Cableado Vertical	307
3.3.4 Ofertas Económicas	308
Capítulo 4 - CONCLUSIONES Y RECOMENDACIONES	315
4.1 Conclusiones	315
4.2 Recomendaciones	317
BIBLIOGRAFÍA	319

Índice de Figuras

Capítulo 1 - TRANSELECTRIC S.A.

1.1: Relaciones de la Compañía	2
1.2: Mapa del SNT	5
1.3: Red de Fibra Óptica TRANSELECTRIC S.A.	9
1.4: Red SIEMENS TRANSELECTRIC S.A.	13
1.5: Red HUAWEI TRANSNEXA E.M.A.	14
1.6: Orgánico Estructural de TRANSELECTRIC S.A.	27

Capítulo 2 - FUNDAMENTOS TEÓRICOS

2.1: Cable de Par Trenzado	29
2.2: Cable Coaxial	29
2.3: Conector RJ-45	29
2.4: Cable UTP	31
2.5: Cable STP	32
2.6: Cable Multipar	33
2.7: Elementos del Cable Coaxial	34
2.8: Conectores BNC y Tipo F	34
2.9: Cable de Fibra Óptica	36
2.10: Elementos del Cable de Fibra Óptica	36
2.11: Refracción de la Luz	37
2.12: Refracción de la Luz en Superficies Planas y Curvas	38
2.13: Ángulo Crítico	38
2.14: Fibra Monomodo	39
2.15: Fibra Multimodo	40
2.16: Conectores y Cables de Interconexión	42
2.17: Conector ST	42
2.18: Conector SC	42
2.19: Conector FC	43

2.20: Conector MT-RJ	43
2.21: Conectores LC Simplex y Dúplex	43
2.22: Conector MTP	44
2.23: Cableado Estructurado	44
2.24: Estándares T568A y T568B	48
2.25: Subsistemas del Cableado Estructurado	49
2.26: Punto de Demarcación	50
2.27: Cuarto de Telecomunicaciones	51
2.28: Planificación de los MCs, ICs y HCs	52
2.29: Conexión de los MCs, ICs y HCs	53
2.30: Canaletas e Interductos	54
2.31: Armario	54
2.32: Código de Colores para Terminaciones de Cables	55
2.33: Cable de Interconexión	56
2.34: Cable Cruzado	56
2.35: Cable Directo	57
2.36: Cable Rollover	57
2.37: Áreas de Trabajo	60
2.38: Instalación de un MUTOA	61
2.39: Punto de Consolidación	61
2.40: Red Jerárquica	62
2.41: Principios de Diseño	65
2.42a: Equipo Antiguo	66
2.42b: Tecnología Actual	66
2.43: Comunidades de Usuario	67
2.44a: Cliente-Servidor	68
2.44b: Servidor-Servidor	68
2.45: Diagrama Topológico	69
2.46: Conmutadores Fijos, Modulares y Apilables	70
2.47: Conmutadores de 24 y 48 Puertos Gigabit Ethernet	71
2.48: Capas de Acceso, Distribución y Core	71
2.49: Comunicaciones Unicast, Broadcast y Multicast	74
2.50: Campos de la Trama Ethernet	75

2.51a: Half Dúplex	76
2.51b: Full Dúplex	76
2.52: Dominios de Colisión	78
2.53: Dominio de Broadcast	79
2.54: Dominios de Broadcast y Colisión Controlados	80
2.55: Cuellos de Botella	81
2.56: Conmutación Simétrica y Asimétrica	83
2.57: Conexión al Conmutador	88
2.58: Configuración de HyperTerminal	88
2.59: VLANs	94
2.60: Tipos de VLAN	97
2.61: Enlace Troncal	97
2.62: Etiqueta 802.1q en la Trama Ethernet	98
2.63: Campos de la Etiqueta VLAN	99
2.64: Funcionamiento VTP	102
2.65: Dominios VTP	103
2.66: Anuncios VTP y Pruning	104
2.67: Modos VTP	105
2.68: Trama VTP	107
2.69a: Diseño Redundante	109
2.69b: Falla en una Trayectoria entre las Capas de Acceso y Distribución	109
2.69c: Falla en un Conmutador de Core	109
2.70: Lazos en el Armario	111
2.71: Lazos en los Cubículos	112
2.72: Algoritmo STP	113
2.73: Campos de la Trama BPDU	115
2.74: Campos de la Bridge ID	116
2.75: Notificación de Cambio en la Topología	121
2.76: Proceso de Sincronización	124
2.77: Instancias MST para dos VLANs	125
2.78: Región MST e Instancias IST	126
2.79: Instancias MST en una Región	127

Capítulo 3 - SITUACIÓN ACTUAL Y PROPUESTA DE DISEÑO

3.1: Puerta de Ingreso al Cuarto de Telecomunicaciones del Noveno Piso	134
3.2: Cuarto de Telecomunicaciones del Noveno Piso	135
3.3: Aire Acondicionado FUJITSU	136
3.4a: UPS FE4.3KVA (Vista Frontal)	136
3.4b: UPS FE4.3KVA (Vista Posterior)	136
3.5a: Central Telefónica PANASONIC EMSS 336 KX-T336100	136
3.5b: Tarjetas de la Central Telefónica PANASONIC (Panel Superior)	137
3.5c: Tarjetas de la Central Telefónica PANASONIC (Panel Inferior)	137
3.6: Bastidor de Paneles de Interconexión de Voz y Datos	138
3.7: Bastidor de Conmutadores y Paneles de Interconexión	139
3.8a: Conmutadores A, B y C	140
3.8b: Conmutadores D, E, F y G	140
3.8c: Conmutadores G, H, I y J	140
3.9: Interconexiones de los Conmutadores del Noveno Piso	141
3.10: Conexiones del Conmutador Principal del Noveno Piso	142
3.11: Regletas KRONE para Interconexión de las Centrales Telefónicas	143
3.12: Troncales y Extensiones entre las Centrales Telefónicas	143
3.13a: Bastidor del Enrutador, Módems y Bases Celulares	144
3.13b: Bastidor del Enrutador, Módems y Bases Celulares (Vista Lateral)	144
3.14a: Bases Celulares TECOM	145
3.14b: Bases Celulares ERICSSON	145
3.15: Cables de Interconexión, Organizadores y Canaletas	146
3.16: Paneles de Interconexión para Bases Celulares y Líneas Telefónicas	146
3.17: Puerta de Ingreso del Cuarto de Equipos del Quinto Piso	147
3.18: Cuarto de Equipos del Quinto Piso	148
3.19: Aire Acondicionado LG	149
3.20: Banco de Baterías	149
3.21: Cargador de Baterías	149
3.22a: Central Telefónica SIEMENS HiPath 4500	150
3.22b: Tarjetas de la Central Telefónica SIEMENS (Panel Superior)	150
3.22c: Tarjetas de la Central Telefónica SIEMENS (Panel Inferior)	151

3.23: Bastidor de Conmutadores y Paneles de Interconexión	152
3.24a: Conmutadores B, C y D	152
3.24b: Conmutadores A y E	152
3.25: Interconexiones de los Conmutadores del Quinto Piso	153
3.26: Conexiones del Conmutador Principal del Quinto Piso	154
3.27: Bastidor de Paneles de Interconexión para Líneas Urbanas y Extensiones ...	155
3.28a: Bastidor de Paneles de Interconexión y Equipos Telefónicos	156
3.28b: Voice Mail System	156
3.28c: Bases Celulares	156
3.29: Codificación de los Paneles de Interconexión	157
3.30 Regletas KRONE en reemplazo de Paneles de Interconexión	157
3.31: Conexiones entre los Cuartos de Telecomunicaciones, la Sala de Servidores y el CGTT	158
3.32: Cableado Horizontal por Ala	159
3.33a: Puntos de Acceso Inalámbricos y Conmutadores por Ala (Pisos 10, 8 y 6)	160
3.33b: Puntos de Acceso Inalámbricos y Conmutadores por Ala (Pisos 5, 3, 2 y Planta Baja)	161
3.34a: Caja Metálica PBA	162
3.34b: Conmutador Sala de Uso Múltiple	162
3.35: Conmutador Auditoría Interna	162
3.36a: Armario 2A	163
3.36b: Conmutador Gerencia de Telecomunicaciones	163
3.37a: Caja Metálica 2B	163
3.37b: Conmutador Asesoría Jurídica	163
3.38: Conmutador de la División de Mantenimiento de Líneas de Transmisión ...	164
3.39a: Caja Metálica 10B	164
3.39b: Conmutador Comunicación Corporativa	164
3.40a: Conmutador Sala de Reuniones	165
3.40b: Conmutador Planoteca	165
3.41a: Conmutador Líneas de Transmisión	165
3.41b: Conmutador Talento Humano	165
3.42: Sistemas Empresariales y Número de Usuarios por Piso	171

3.43: Total de Usuarios de cada Sistema Empresarial	171
3.44: Captura del Protocolo SMB	173
3.45: Captura del Protocolo HTTP	174
3.46: Captura del Protocolo SNMP	175
3.47: Captura del Protocolo DNS	176
3.48: Captura del Protocolo TCP	177
3.49: Captura del Protocolo UDP	178
3.50: Captura del Protocolo ICMP	180
3.51: Captura del Protocolo ARP	182
3.52: Captura del Protocolo LLC	183
3.53: Captura del Protocolo STP	184
3.54: Análisis de Tráfico en el Conmutador Principal del Noveno Piso	186
3.55: Análisis de Tráfico en el Conmutador Principal del Quinto Piso	188
3.56: Medición del Ancho de Banda del Martes 29 de Julio	189
3.57: Medición del Ancho de Banda del Miércoles 30 de Julio	190
3.58: Medición del Ancho de Banda del Lunes 4 de Agosto	191
3.59: Medición del Ancho de Banda del Martes 5 de Agosto	191
3.60: Medición del Ancho de Banda del Miércoles 6 de Agosto	192
3.61: Medición del Ancho de Banda del Jueves 7 de Agosto	193
3.62: Valores Significativos del Martes 29 de Julio	193
3.63: Valores Significativos del Miércoles 30 de Julio	194
3.64: Valores Significativos del Lunes 4 de Agosto	195
3.65: Valores Significativos del Martes 5 de Agosto	195
3.66: Valores Significativos del Miércoles 6 de Agosto	196
3.67: Medición del Ancho de Banda en la Semana del 28 de Julio al 1 de Agosto	197
3.68: Medición del Ancho de Banda en la Semana del 4 al 8 de Agosto	198
3.69: Bastidor de Extensiones y Líneas Directas	201
3.70: Diagrama Topológico de la Red Propuesta	202
3.71: Bastidor de los Conmutadores de Core/Distribución	203
3.72: Conmutadores Cisco Catalyst 6500	204
3.73: Tarjeta Supervisora 720	204
3.74: Tarjeta 10/100/1000 Ethernet de 48 Puertos	205

3.75: Tarjeta Gigabit Ethernet de 24 Puertos SFP	205
3.76: Trayectorias del Cableado Vertical	206
3.77: Conmutadores Cisco Catalyst 2960	207
3.78: Armario a Instalarse en Cada Ala	208
3.79: Topología de Red en Programa de Simulación	215
3.80: Borrado de la Base de Datos VLAN	216
3.81: Borrado de la Configuración	216
3.82: Información VLAN	216
3.83a: Archivo de Configuración (1 de 2)	217
3.83b: Archivo de Configuración (2 de 2)	217
3.84: Información de la Interfaz VLAN 1	218
3.85a: Información de un Conmutador (1 de 3)	219
3.85b: Información de un Conmutador (2 de 3)	219
3.85c: Información de un Conmutador (3 de 3)	219
3.86: Nombre de Conmutador de Core/Distribución	220
3.87: Contraseñas de Consola y de Acceso al Modo de Privilegio	220
3.88: Acceso Remoto con SSH	221
3.89a: Apagado de Interfaces Fast Ethernet en Conmutador de Core/Distribución	221
3.89b: Apagado de Interfaces Gigabit Ethernet en Conmutador de Core/Distribución	221
3.90: Estado VTP por Defecto en Conmutador de Core/Distribución	222
3.91: Modo de Operación, Nombre de Dominio y Contraseña en Servidor VTP ...	222
3.92a: Números y Nombres de VLANs (1 de 2)	223
3.92b: Números y Nombres de VLANs (2 de 2)	223
3.93: Estado de VLANs en Conmutador de Core/Distribución	224
3.94a: Interfaz VLAN 83 del Conmutador TELESRVA	224
3.94b: Interfaz VLAN 83 del Conmutador TELESRVB	224
3.95a: Enlaces Troncales en la Capa de Core/Distribución	225
3.95b: Enlaces Troncales entre las Capas de Core/Distribución y Acceso (1 de 2)	226
3.95c: Enlaces Troncales entre las Capas de Core/Distribución y Acceso (2 de 2)	226
3.96: Interface Port-Channel en la Capa de Core/Distribución	226
3.97: Modo Troncal y VLAN Nativa en la Capa de Core/Distribución	226
3.98: Agrupación de Puertos en el Canal Lógico de la Capa de Core/Distribución	227

3.99: Estado del EtherChannel entre Conmutadores de Core/Distribución	227
3.100a: Modo de Acceso y Asignación VLAN en el Conmutador TELESRVA ...	228
3.100b: Modo de Acceso y Asignación VLAN en el Conmutador TELESRVB ...	228
3.101a: Conmutador Raíz para las VLANs 10-15	228
3.101b: Conmutador Raíz para las VLANs 16-20 y 83	228
3.102a: Estado de STP para la VLAN 10 en el Conmutador TELESRVA	229
3.102b: Estado de STP para la VLAN 83 en el Conmutador TELESRVA	230
3.103a: Estado de STP para la VLAN 83 en el Conmutador TELESRVB	231
3.103b: Estado de STP para la VLAN 10 en el Conmutador TELESRVB	232
3.104: Copiado del Archivo de Configuración	232
3.105a: Borrado del Archivo vlan.dat	233
3.105b: Borrado del Archivo startup-config	233
3.106: Información de VLANs y Puertos Asociados	233
3.107a: Nombre de Conmutador de Acceso en el Ala Oriental	234
3.107b: Nombre de Conmutador de Acceso en el Ala Occidental	234
3.108a: Apagado de Interfaces Gigabit Ethernet en Conmutador de Acceso	234
3.108b: Apagado de Interfaces Fast Ethernet en Conmutador de Acceso	234
3.109: Estado VTP por Defecto en Conmutador de Acceso	235
3.110: Modo de Operación, Nombre de Dominio y Contraseña en Cliente VTP ...	235
3.111: Modo de Operación Cliente y Nombre de Dominio TRANSELECTRIC ...	236
3.112: Modo Troncal y VLAN Nativa en Conmutador de Acceso	236
3.113a: Interface Port-Channel en la Capa de Acceso	237
3.113b: Modo Troncal y VLAN Nativa en la Capa de Acceso	237
3.113c: Agrupación de Puertos en el Canal Lógico de la Capa de Acceso	237
3.114: Estado de EtherChannel entre los Conmutadores de Acceso	237
3.115: Modo de Acceso y Asignación VLAN en Conmutador de Acceso	238
3.116: Interfaz VLAN 83 del Conmutador 10APRESEJEC	238
3.117: Estado de VLANs en Conmutador de Acceso	239
3.118. Estado de VTP en Conmutador de Acceso	239
3.119a: Estado de STP para la VLAN 10 en el Conmutador 10APRESEJEC	240
3.119b: Estado de STP para VLAN 83 en el Conmutador 10APRESEJEC	240
3.120a: Envío y Recepción de Paquetes desde el Conmutador TELESRVA	241
3.120b: Envío y Recepción de Paquetes desde el Conmutador TELESRVB	241

3.120c: Intercambio de Paquetes entre las Capas de Core/Distribución y de Acceso (1 de 2)	241
3.120d: Intercambio de Paquetes entre las Capas de Core/Distribución y de Acceso (2 de 2)	242
3.120e: Comunicación entre los Conmutadores de Acceso	242
3.121: Topología de Red Equivalente	243
3.122a: Conmutadores y Emuladores de Terminal (Vista Frontal)	244
3.122b: Conmutadores y Emuladores de Terminal (Vista Posterior)	244
3.123: HyperTerminal en Menú de Comunicaciones	245
3.124: Propiedades de Conexión y Parámetros de Puerto	245
3.125: Borrado de Base de Datos VLAN y Configuración	246
3.126: VLANs por Defecto	246
3.127: Inicialización de un Conmutador	247
3.128a: Configuración Actual (1 de 3)	247
3.128b: Configuración Actual (2 de 3)	248
3.128c: Configuración Actual (3 de 3)	248
3.129: Parámetros de la Interfaz VLAN 1	249
3.130a: Características de un Conmutador (1 de 2)	249
3.130b: Características de un Conmutador (2 de 2)	250
3.131: Nombre de los Conmutadores de Core/Distribución	250
3.132: Encriptación de las Contraseñas de Consola y de Acceso al Modo de Privilegio	251
3.133a: Apagado de Puertos Fast Ethernet en Conmutador de Core/Distribución	
3.133b: Apagado de Puertos Gigabit Ethernet en Conmutador de Core/Distribución	251
3.134: Estado de VTP por Defecto en Conmutador de Core/Distribución	252
3.135: Modo de Operación, Dominio y Contraseña en Servidor VTP	252
3.136a: Nombres y Números de VLANs (1 de 2)	253
3.136b: Nombres y Números de VLANs (2 de 2)	253
3.137: Estado de VLANs en Conmutador de Core/Distribución	254
3.138: Estado de VTP en Conmutador de Core/Distribución	254
3.139a: Dirección de Capa 3 en Conmutador TELESRVA	255
3.139b: Dirección de Capa 3 en Conmutador TELESRVB	255

3.140: Protocolo de Encapsulamiento, Modo Troncal y VLAN Nativa entre Capas de Core/Distribución y de Acceso	255
3.141: Estado de los Enlaces Troncales	256
3.142a: Canal Lógico en la Capa de Core/Distribución	256
3.142b: Agrupación de Puertos en la Capa de Core/Distribución	256
3.143: Resumen de EtherChannel en la Capa de Core/Distribución	257
3.144: Seguridad de Puerto en la VLAN 10	257
3.145a: Control en la Elección del Conmutador Raíz para las VLANs 10-15	258
3.145b: Control en la Elección del Conmutador Raíz para las VLANs 16-20 y 83	258
3.146a: Datos de STP para la VLAN 10 en el Conmutador TELESRVA	258
3.146b: Datos de STP para la VLAN 83 en el Conmutador TELESRVA	259
3.147a: Datos de STP para la VLAN 83 en el Conmutador TELESRVB	259
3.147b: Datos de STP para la VLAN 10 en el Conmutador TELESRVB	260
3.148a: Conmutador HSRP Activo para VLAN 10	260
3.148b: Conmutador HSRP Standby para VLAN 83	260
3.149a: Comunidad, Notificaciones y Versión SNMP en Conmutador TELESRVA	261
3.149b: Comunidad, Notificaciones y Versión SNMP en Conmutador TELESRVB	261
3.150. Copiado de Archivos de Configuración	261
3.151: VLANs Existentes en Conmutador de Acceso	262
3.152a: Nombre de Conmutador en Ala A del Noveno Piso	262
3.152b: Nombre de Conmutador en Ala B del Noveno Piso	262
3.153a: Apagado de Puertos Fast Ethernet en el Conmutador 9BINVEDESA	263
3.153b: Apagado de Puertos Gigabit Ethernet en el Conmutador 9BINVEDESA	263
3.154: Estado VTP por Defecto en el Conmutador 9BINVEDESA	264
3.155: Modo de Operación, Dominio y Contraseña en Cliente VTP	264
3.156: Estado de VTP en el Conmutador 9BINVEDESA	264
3.157: Modo Troncal y VLAN Nativa en el Conmutador 9BINVEDESA	265
3.158: Estado de Enlaces Troncales en el Conmutador 9BINVEDESA	265
3.159: Seguridad de Puerto en la VLAN 19	265
3.160a: Dirección Administrativa del Conmutador 9AVICETEC1	266
3.160b: Dirección Administrativa del Conmutador 9AVICETEC2	266

3.160c: Dirección Administrativa del Conmutador 9BINVEDESA	266
3.161: Estado de VLANs en Conmutador de Acceso	266
3.162a: Información de STP para la VLAN 10 en el Conmutador 9BINVEDESA	267
3.162b: Información de STP para la VLAN 83 en el Conmutador 9BINVEDESA	267
3.163a: Parámetros SNMP en Conmutador 9AVICETEC1	268
3.163b: Parámetros SNMP en Conmutador 9AVICETEC2	268
3.163c: Parámetros SNMP en Conmutador 9BINVEDESA	268
3.164a: Comunicación en la Capa de Core/Distribución desde el TELESRVA	269
3.164b: Comunicación en la Capa de Core/Distribución desde el TELESRVB	269
3.164c: Intercambio de Paquetes entre las Capa de Core/Distribución y de Acceso (1 de 2)	269
3.164d: Intercambio de Paquetes entre las Capas de Core/Distribución y de Acceso (2 de 2)	270
3.164e: Interacción de los Conmutadores de Acceso	270
3.165a: Asistente de Nuevo Mapa del Menú Archivo	271
3.165b: Descubrimiento de Dispositivos	271
3.166: Espacio para la Edición de Mapas	272
3.167: Categoría General de Propiedades de Dispositivos	272
3.168: Categoría SNMP de Propiedades de Dispositivos	273
3.169: Categoría Menú de Propiedades de Dispositivos	273
3.170a: Simbología para Estado de Dispositivos (1 de 2)	274
3.170b: Simbología para Estado de Dispositivos (2 de 2)	275
3.171: Categoría General de Propiedades del Servidor Web	275
3.172: Categoría Usuarios de Propiedades del Servidor Web	276
3.173: Conjunto de Notificaciones Disponibles	277
3.174a: Notificación de Radiolocalizador	277
3.174b: Notificación de SMS	278
3.174c: Notificación de Correo Electrónico	278
3.174d: Notificación de Sonido	279
3.175: Diagrama para Monitoreo de Red	280
3.176a: Esquema de los Conmutadores de Acceso en el Ala Oriental	280
3.176b: Esquema de los Conmutadores de Acceso en el Ala Occidental	281
3.177a: Nombre y Dirección IP en la Categoría General	281

3.177b: Comunidades SNMP de Lectura y Escritura	282
3.178: Número del Puerto TCP en Servidor Web	283
3.179a: Creación de Nuevo Usuario para Servidor Web (1 de 2)	283
3.179b: Creación de Nuevo Usuario para Servidor Web (2 de 2)	284
3.180a: Usuario y Contraseña para Conexión a Servidor Web	284
3.180b: Pantalla Principal del Software de Gestión	285
3.181a: Respuesta de Dispositivo ante Reconocimiento	286
3.181b: Pérdida de 1 y 2 Paquetes	286
3.181c: Pérdida de 3 a 7 Paquetes	286
3.181d: Pérdida de más de 8 Paquetes	286
3.182a: Rastreo Inteligente utilizando SNMP	287
3.182b: Exploración de Servicios	287
3.183a: Progreso de la Exploración	288
3.183b: Identificación de Nombres, Servicios y Tipos de Dispositivos	288
3.184: Resultados de la Exploración	289
3.185: Campos de la Categoría General del Dispositivo TELESRVA	289
3.186: Campos de la Categoría SNMP del Dispositivo TELESRVA	290
3.187: Servicios Identificados en el Dispositivo TELESRVA	290
3.188: Categoría Estado del Dispositivo TELESRVA	291
3.189: Categoría Tiempo de Funcionamiento del Dispositivo TELESRVA	291
3.190: Bitácora del Dispositivo TELESRVA	292
3.191a: Interfaz Web del Programa de Gestión	292
3.191b: Topología Equivalente para Administración	293
3.192a: Falla en un Dispositivo y Reconocimiento en Ejecución	293
3.192b: Pérdida de 1 Paquete en Conmutadores	294
3.192c: Desconexión en la Capa de Core/Distribución	294
3.193: Bastidor para Distribución de Extensiones y Líneas Directas	296
3.194: Armario para los Conmutadores de Core/Distribución	297
3.195: Armario del Décimo Piso (A y B)	299
3.196a: Armario del Noveno Piso (A)	299
3.196b: Armario del Noveno Piso (B)	300
3.197: Armario del Octavo Piso (A y B)	301

3.198a: Armario del Séptimo Piso (A)	301
3.198b: Armario del Séptimo Piso (B)	302
3.199: Armario del Sexto Piso (A y B), Quinto Piso (A), Cuarto y Tercer Pisos (B)	303
3.200: Armario del Quinto Piso (B)	303
3.201: Armario del Tercer Piso (A)	304
3.202: Armario del Segundo Piso (A y B)	305
3.203a: Armario de la Planta Baja (A)	306
3.203b: Armario de la Planta Baja (B)	306

Índice de Tablas

Capítulo 1 - TRANSELECTRIC S.A.

1.1: Descripción de las Subestaciones	3
1.2a: Líneas de Transmisión Zona Norte	3
1.2b: Líneas de Transmisión Zona Sur	4
1.3: Líneas de Transmisión	6
1.4: Capacidad de Transformación Instalada	6
1.5: Zonas que operan y mantienen el SNT	6

Capítulo 2 - FUNDAMENTOS TEÓRICOS

2.1: Tipo de Tráfico según Modo de Violación	93
2.2: Interacciones DTP	100
2.3: Estados de los Puertos	119

Capítulo 3 - SITUACIÓN ACTUAL Y PROPUESTA DE DISEÑO

3.1: Departamentos del Edificio Matriz de TRANSELECTRIC S.A.	133
3.2: Conmutadores del Cuarto de Telecomunicaciones del Noveno Piso	141
3.3: Conmutadores del Cuarto de Telecomunicaciones del Quinto Piso	153
3.4: Conmutadores instalados en cada Ala	160
3.5: Número de Usuarios de la red LAN	166
3.6a: Sistema Empresarial Xnear CRM Workflow	167
3.6b: Sistema Empresarial Flexline ERP	167
3.6c: Sistema Empresarial APIPRO	168
3.6d: Sistema Empresarial Project Server	168
3.6e: Sistema Empresarial Evolution	169
3.6f: Sistema Empresarial Portal Web	169
3.6g: Otros Sistemas Empresariales	170
3.7: Sistemas Empresariales y Usuarios	170

3.8: Porcentaje de Paquetes Capturados en el Conmutador Principal del Noveno Piso	185
3.9: Porcentaje de Paquetes Capturados en el Conmutador Principal del Quinto Piso	187
3.10: Conmutadores Cisco de la Red Actual	206
3.11: Codificación para los Conmutadores de Acceso	210
3.12: Direccionamiento de los Conmutadores	211
3.13: Número y Nombre de las VLANs	213
3.14: Enlaces Troncales entre las Capas de Core/Distribución y de Acceso	225
3.15: Características de los Conmutadores Utilizados en la Simulación	244
3.16: Especificaciones para el Bastidor de Distribución de Extensiones y Líneas Directas	296
3.17a: Especificaciones para el Armario de Core/Distribución (1 de 2)	298
3.17b: Especificaciones para el Armario de Core/Distribución (2 de 2)	298
3.18: Especificaciones para el Armario del Décimo Piso (A y B)	299
3.19a: Especificaciones para el Armario del Noveno Piso (A)	300
3.19b: Especificaciones para el Armario del Noveno Piso (B)	300
3.20: Especificaciones para el Armario del Octavo Piso (A y B)	301
3.21a: Especificaciones para el Armario del Séptimo Piso (A)	302
3.21b: Especificaciones para el Armario del Séptimo Piso (B)	302
3.22: Especificaciones para el Armario del Sexto Piso (A y B), Quinto Piso (A), Cuarto y Tercer Pisos (B)	303
3.23: Especificaciones para el Armario del Quinto Piso (B)	304
3.24: Especificaciones para el Armario del Tercer Piso (A)	304
3.25: Especificaciones para el Armario del Segundo Piso (A y B)	305
3.26a: Especificaciones para el Armario de la Planta Baja (A)	306
3.26b: Especificaciones para el Armario de la Planta Baja (B)	307
3.27: Resumen de Especificaciones para los Armarios	307
3.28: Distancias entre el Cuarto de Telecomunicaciones y cada Piso	308
3.29a: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (1 de 4)	309

3.29b: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (2 de 4)	310
3.29c: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (3 de 4)	311
3.29d: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (4 de 4)	312
3.30: Cotización de Equipos Activos y Cableado Estructurado (Andean Trade) ...	313
3.31: Cotización de Equipos Activos y Cableado Estructurado (TOTALTEK)	314

Capítulo 2

2 FUNDAMENTOS TEÓRICOS

2.1 Elementos Pasivos

2.1.1 Cable de Cobre

Es un medio que sirve para transmitir señales. Los hilos de cobre transportan señales entre dispositivos. Las propiedades más importantes de este tipo de cable son:

- **Conductividad:** Es un gran conductor eléctrico.
- **Resistencia a la corrosión:** No se oxida ni corroe.
- **Ductilidad:** Pueden hacerse alambres delgados sin que se rompan.
- **Maleabilidad:** Es fácil darle forma tanto en altas como bajas temperaturas y no se rompe al ser martillado, sellado, forjado o moldeado.
- **Fuerza:** Su fuerza a bajas temperaturas está en el orden de 3500 a 4900 kg/cm² y mantiene su dureza hasta 204 °C.

Las Figuras 2.1 y 2.2 muestran los cables de par trenzado y coaxial que se utilizan en redes. El primero se compone de pares de alambre de cobre y se emplea en la mayoría de redes de voz y datos. El segundo tiene cobre sólido como conductor central y se utiliza en conexiones de video y de alta velocidad (T-3 o E-3). Estos cables están formados por:

- **Chaqueta Protectora:** Es un aislante que previene corto circuitos entre los conductores.
- **Espaciadores:** Sirven para preservar las propiedades eléctricas del cable.

El cable de cobre está formado por un núcleo sólido o hilos delgados de cobre trenzados como una cuerda. La flexibilidad de estos hilos es conveniente cuando el cable experimenta vibración o tensión durante el proceso de instalación.

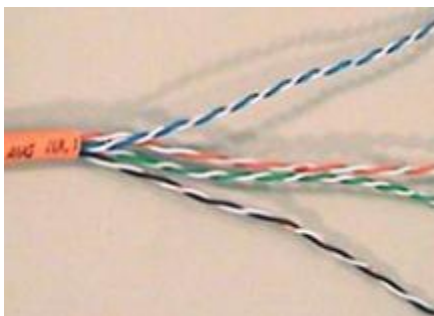


Figura 2.1: Cable de Par Trenzado



Figura 2.2: Cable Coaxial

2.1.1.1 Cable de Par Trenzado

Es un sistema que sirve para transmitir señales electrónicas. Este cable está formado por alambres de cobre trenzados. Para terminarlo se utiliza el conector modular 8P8C (8 posiciones y 8 contactos) o RJ-45 (Registered Jack) que se observa en la Figura 2.3. Puede ser instalado en paneles de interconexión, los cuales se colocan en los armarios de los Cuartos de Telecomunicaciones.



Figura 2.3: Conector RJ-45

2.1.1.1.1 Categorías

Especifican el grado del cable de par trenzado y la velocidad de transmisión de datos que soporta. La calidad del cable influye en la transmisión de datos. El ruido de los cables de baja calidad interfiere con la transmisión. Si los datos son ilegibles se debe retransmitir.

Un cable de mejor calidad implica menos mensajes perdidos, retransmisiones y tráfico innecesario. La EIA (Electronic Industries Association) y la TIA (Telecommunications Industry Association) definen los estándares para cableado en edificaciones.

2.1.1.1.1.1 Categoría 1

Inicialmente se utilizó en telefonía y se la encuentra en hogares y empresas antiguas. El sistema de medida en Estados Unidos es AWG (American Wire Gauge). La distancia de transmisión se incrementa con un conductor más grueso. Generalmente, el cable de Categoría 1 es 22AWG o 24AWG sin trenzar con distinta impedancia y atenuación. No es recomendable para datos o señalización con velocidades mayores a 1 Mbps. Tampoco se la reconoce como parte de ANSI/TIA/EIA-568-B.1 o ANSI/TIA/EIA-568-B.2, por lo que no es parte de los sistemas de cableado estructurado modernos.

2.1.1.1.1.2 Categoría 2

Se utiliza en cableado IBM (International Business Machines) para redes Token Ring. Tiene una tasa de datos máxima de 4 Mbps (16 Mbps en aplicaciones pasivas). No es reconocida como parte de ANSI/TIA/EIA-568-B.1 o ANSI/TIA/EIA-568-B.2. Utiliza alambre sólido 22AWG o 24AWG en pares trenzados.

2.1.1.1.1.3 Categoría 3

Se aplica a cables UTP (Unshielded Twisted-Pair) de 100 ohmios con cuatro pares trenzados de alambre sólido de cobre 24AWG. Se utilizaba en instalaciones 10BASE-T y aún se lo emplea en instalaciones telefónicas.

2.1.1.1.1.4 Categoría 4

Estos cables fueron diseñados para soportar redes 16-MB Token Ring. No se reconoce como parte de ANSI/TIA/EIA-568-B.1 o ANSI/TIA/EIA-568-B.2. Tiene cuatro pares de alambre 22AWG o 24AWG y una impedancia de 100 ohmios.

2.1.1.1.1.5 Categoría 5

Se aplica a cables UTP de 100 ohmios con cuatro pares de alambre de cobre 24AWG y tiene características de transmisión especificadas hasta 100 MHz. Puede operar en 1000BASE-T utilizando múltiples pares y aún se utiliza en redes residenciales.

2.1.1.1.6 Categoría 5e

Tiene mayor cantidad de torceduras por unidad de longitud, lo cual mejora la resistencia a la interferencia y el rendimiento. Una torcedura más apretada permite que los cables resistan la separación y el agrupamiento durante la instalación.

2.1.1.1.7 Categoría 6

Consiste de cuatro pares de alambres de cobre 24AWG. Tiene más torceduras y es más costoso, pero la reducción de la diafonía lo hace un medio confiable para 1000BASE-TX, siendo éste el estándar más rápido para UTP.

2.1.1.1.2 Cable UTP (*Unshielded Twisted-Pair*)

Se utiliza en una variedad de redes y viene en diferentes números de pares, siendo el más común cuatro (Categorías 3, 5e y 6). El efecto de cancelación producido por los pares trenzados limita la degradación de la señal causada por EMI (Electromagnetic Interference) y RFI (Radio Frequency Interference). Este cable sigue especificaciones respecto a cuantas torceduras son permitidas por unidad de longitud (Figura 2.4). Un mayor número de torceduras disminuye la degradación de la señal. Para la instalación de redes se emplea Categoría 5e o 6. La Categoría 3 se utilizaba en cableado telefónico.

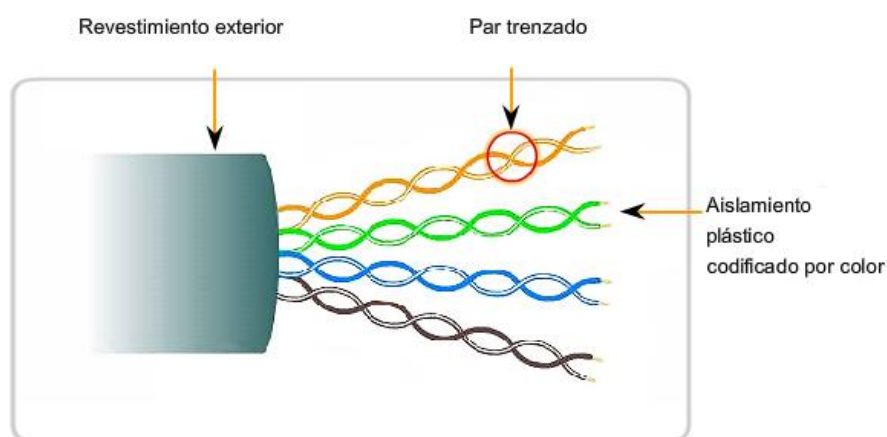


Figura 2.4: Cable UTP

2.1.1.1.3 Cable STP (Shielded Twisted-Pair)

Es cable UTP con una capa de apantallamiento que protege a los hilos de la interferencia externa. La Figura 2.5 muestra el escudo (hoja de metal) que cubre los pares individuales y el blindaje trenzado que envuelve los cuatro pares. Este cable no se utiliza con frecuencia porque las capas protectoras deben estar aterrizadas para minimizar la degradación de la señal. Si existe una diferencia de potencial en varias partes de la red, los escudos conducen estos lazos de tierra y pueden convertirse en fuentes de interferencia. Al halar el cable, se debe evitar doblarlo excesivamente ya que el escudo se puede dañar y producir interferencia.

Este cable es más costoso que el UTP por la protección adicional, es menos flexible y más difícil de instalar. Requiere que el alambre de tierra se conecte a la banda metálica alrededor de cada conector RJ-45. Los paneles de interconexión, hubs y otros elementos hacen contacto con esta banda y la aterrizan. Este proceso demanda más tiempo y los costos se incrementan.

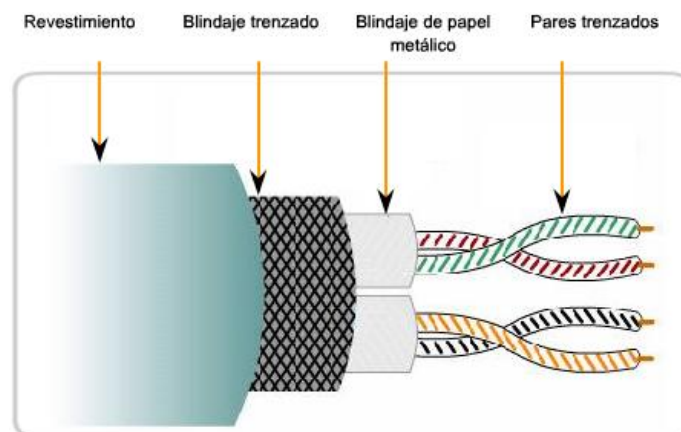


Figura 2.5: Cable STP

2.1.1.1.4 Otros tipos de cable STP

2.1.1.1.4.1 Cable ScTP (Screened Twisted-Pair)

Tiene solo un escudo que protege los pares del cable. Es menos costoso y pesado, tiene un diámetro más pequeño y es más fácil de aterrizan.

2.1.1.1.4.2 Cable STP de 100 ohms

Se utiliza principalmente en redes Ethernet. El escudo no es parte del circuito de datos, por lo que se aterriza solo en un extremo (Cuarto de Telecomunicaciones). De esta manera, el escudo intercepta EMI y RFI.

2.1.1.1.4.3 Cable STP de 150 ohms

Es la forma más común de cable STP y tiene un diámetro de 0.98 mm. Su escudo no es parte de la trayectoria de la señal, pero está aterrizado en ambos extremos. Puede transmitir datos utilizando señalización rápida con poca distorsión, pero el escudo causa pérdida de la señal, por lo que se necesita mayor aislamiento entre los pares de hilos y el escudo. La gran cantidad de aislante y protección incrementan el tamaño, peso y costo del cable.

2.1.1.1.5 Otras Configuraciones

Los cables multipar se utilizan para circuitos de voz y datos en el mismo cable. El cable multipar más utilizado es el de 25 pares. Los cables con gran cantidad de pares se agrupan con un hilo de color.

2.1.1.1.5.1 Cable Multipar

Los cables de telecomunicaciones vienen en muchos tamaños, desde 1 a 4200 pares. En instalaciones grandes, estos se terminan en el Punto de Demarcación, van a otros pisos o edificios y terminan en los Cuartos de Telecomunicaciones, donde los circuitos se distribuyen utilizando cables más pequeños. Las configuraciones típicas son: 1, 2, 4, 5, 6, 8, 12, 25, 50, 75, 100, 150, 200, 300, 400, 600, 900, 1200, 1500, 1800, 2100, 2400, 2700, 3000, 3600 y 4200 pares (Figura 2.6).

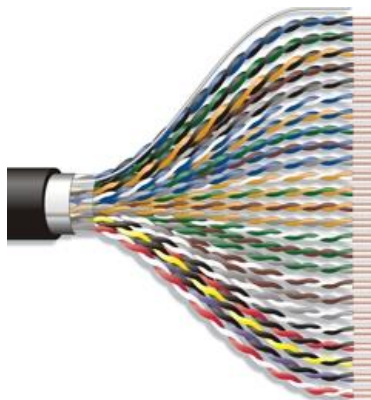


Figura 2.6: Cable Multipar

2.1.1.2 Cable Coaxial

Se utilizaba en aplicaciones de red. Hoy en día, se emplea en video o televisión por cable. En la Figura 2.7 se puede apreciar que el conductor de cobre central está cubierto por tres capas: aislamiento, blindaje y revestimiento exterior. Los conectores más utilizados son el BNC (British Naval Connector) y Tipo F que se observan en la Figura 2.8. El primero se utiliza en redes y aplicaciones de video y el segundo en aplicaciones de radio frecuencia modulada, tales como televisión por cable y sistemas de entretenimiento.

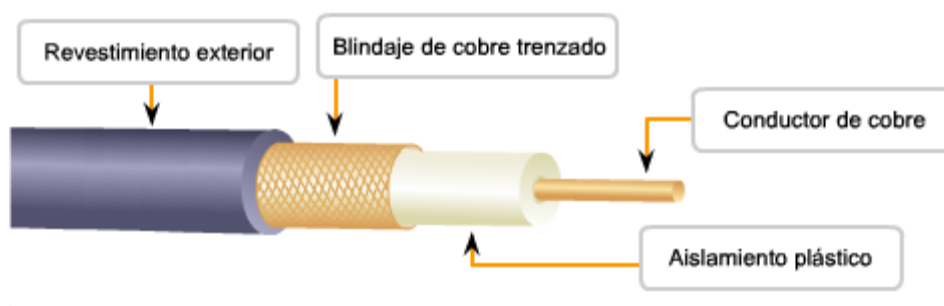


Figura 2.7: Elementos del Cable Coaxial



Figura 2.8: Conectores BNC y Tipo F

El cable coaxial es mejor que el cable de par trenzado en ciertas aplicaciones, pues este último tiene alambres más pequeños (22 o 24) y es menos robusto. La ventaja principal del cable coaxial es la respuesta en frecuencia, ya que deja pasar frecuencias bajas y ultra altas (UHF). Este cable se utiliza para señales de gran ancho de banda (video análogo). Algunos sistemas de comunicación digital (T-3) emplean cable coaxial.

El cable de par trenzado ha reemplazado al coaxial en la industria de redes porque:

- Aunque la protección del cable coaxial disminuye la interferencia, éste debe estar aterrizado.
- Ciertos cables coaxiales tienen mayor diámetro, no son flexibles y requieren grandes conductos.
- Las tasas de datos que los cables coaxiales pueden soportar (10 Mbps) son menores que aquellas soportadas por los cables de par trenzado (100 Mbps, 1 Gbps, y 10 Gbps).

2.1.1.2.1 Funcionamiento

El cable coaxial forma una línea de transmisión, es decir, una red con efectos eléctricos causados por su forma. Este cable es más difícil de manipular e instalar y es más costoso que el cable de par trenzado. Tiene tres impedancias características: 50 ohmios para radio y redes (RG-58), 75 ohmios para video (RG-6 y RG-59) y 93 ohmios para ARCnet (RG-62). Las terminaciones para este cable incluyen conectores T y barril.

El diámetro del conductor y la elección del dieléctrico influyen en la impedancia de estos dispositivos. Los conectores para cable coaxial en aplicaciones de redes tienden a ser el enlace más débil. Es preferible utilizar los conectores BNC que se ponchan y no aquellos que se atornillan.

2.1.2 Cable de Fibra Óptica

Es un medio de comunicación que utiliza luz modulada para transmisiones a través de tiras delgadas de vidrio. Las señales que representan los bits de datos se convierten en haces de luz. El cable de fibra óptica, los conectores, herramientas e instalación son costosos.

La fibra óptica no es susceptible a EMI o RFI, tiene altas tasas de transmisión, cubre grandes distancias, soporta 2, 4, 8, 12, 24 o más circuitos, no necesita ser aterrizada y es más resistente a factores ambientales.

Cada circuito de fibra óptica para redes consiste en dos fibras de vidrio, uno para transmitir y otro para recibir. Dado que no existe diafonía con fibra óptica, es común observar múltiples pares revestidos en el mismo cable, permitiendo que un solo cable se instale entre pisos o armarios de datos.

2.1.2.1 Funcionamiento

Los sistemas de fibra óptica utilizan pulsos de luz para transmitir información a través de sus circuitos. La luz se envía por el centro de la fibra (núcleo) a diferentes ángulos y se refleja en una especie de vidrio que lo rodea (revestimiento).

En la Figura 2.9, los extremos Tx son los transmisores y los extremos Rx son los receptores. Un par Tx/Rx se puede conectar a un enrutador, conmutador, panel de interconexión, servidor o estación de trabajo.



Figura 2.9: Cable de Fibra Óptica

El cable de fibra óptica está constituido por: núcleo, revestimiento, búfer, material de refuerzo y envoltura (Figura 2.10). El núcleo es el elemento de transmisión de luz que se encuentra en el centro de la fibra óptica y es de silicona o vidrio. Alrededor del revestimiento se encuentra un material que protege al núcleo de daños. Un material de refuerzo rodea al búfer para evitar que el cable se estire cuando es halado. La envoltura protege la fibra contra abrasión, solventes y otros contaminantes.

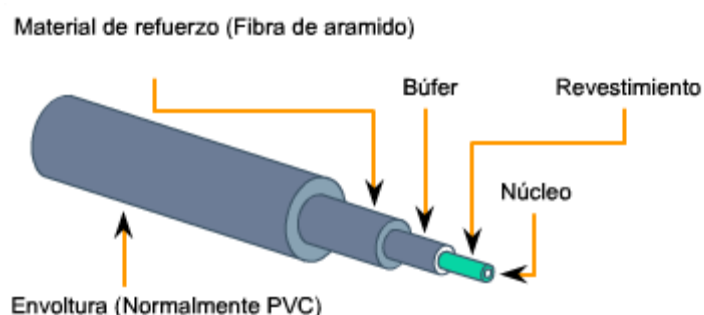


Figura 2.10: Elementos del Cable de Fibra Óptica

La luz viaja a menor velocidad en un medio comparado con el vacío, por lo que el índice de refracción (relación entre la velocidad de la luz en el vacío y en un medio determinado) es siempre mayor que 1 en la parte óptica del espectro. Aunque los rayos de

luz viajan en línea recta a través de los materiales, un fenómeno distinto ocurre en la superficie. La luz se curva a medida que pasa una superficie en la cual el índice de refracción cambia. La magnitud de esta curvatura depende de los índices de refracción de ambos medios y del ángulo con el cual la luz incide en la superficie. La relación entre los ángulos de incidencia y refracción que se miden respecto a una línea perpendicular a la superficie (normal) se conoce como la ley de Snell:

$$n_i \cdot \sin(\theta_i) = n_r \cdot \sin(\theta_r)$$

donde n_i , n_r son los índices de refracción de cada medio y θ_i , θ_r son los ángulos de incidencia y refracción, respectivamente (Figura 2.11).

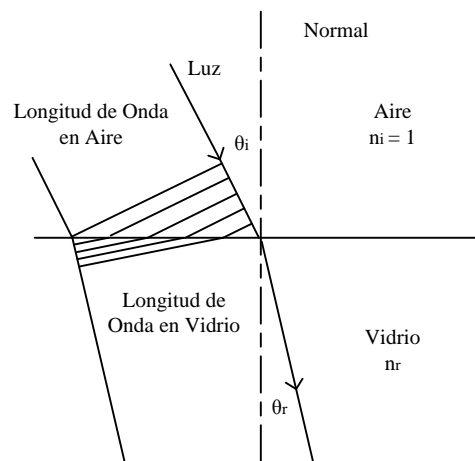


Figura 2.11: Refracción de la Luz

La frecuencia de la onda no cambia, pero como viaja más lentamente, la longitud de onda se reduce, ocasionando que la luz se curve sin importar si la superficie es plana o curva. No obstante, si las dos superficies son planas, la luz sale con el mismo ángulo que ingresó y la refracción es cero. Si una o ambas superficies son curvas, los ángulos de incidencia y refracción son distintos como se observa en la Figura 2.12.

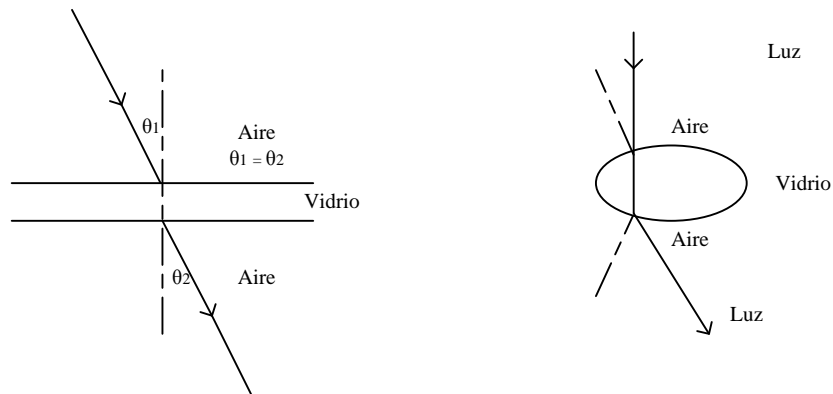


Figura 2.12: Refracción de la Luz en Superficies Planas y Curvas

La ley de Snell indica que la refracción no puede ocurrir cuando el ángulo de incidencia es demasiado grande. La luz no puede salir del vidrio cuando el ángulo de incidencia sobrepasa un valor denominado ángulo crítico ($\theta_c = \sin^{-1}(n_r/n_i)$). Es así que la reflexión interna provoca que la luz rebote contra el vidrio según la ley antes mencionada. Esta reflexión mantiene la luz dentro de la fibra óptica (Figuras 2.13).

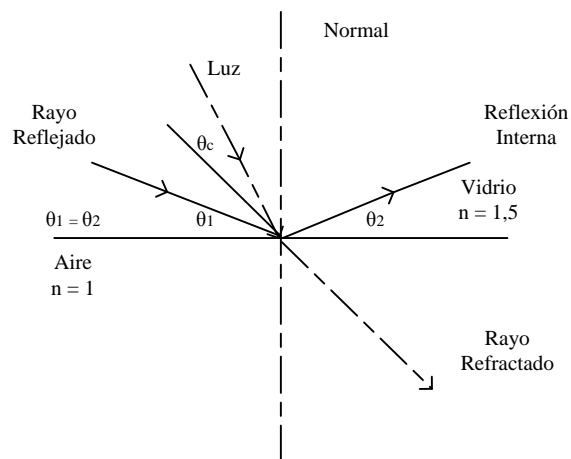


Figura 2.13: Ángulo Crítico

Como los cables de fibra óptica utilizan señales de luz para transmitir, es necesario instalar dispositivos especiales para interpretar estas señales. Cada fibra se conecta a un transmisor en un extremo y a un receptor en el otro. El transmisor convierte los datos en pulsos de luz codificados y los envía por la fibra. Un dispositivo especial conocido como LED (Light-Emitting Diode) produce la luz. Cuando los pulsos de luz alcanzan el destino,

éstos se canalizan en el receptor óptico, el cual los convierte en señales eléctricas que pueden ser transmitidas a través de circuitos de cobre.

2.1.2.2 Tipos

El cable de fibra óptica puede ser monomodo o multimodo. El primero utiliza un solo modo (rayo de luz que entra al núcleo con un ángulo particular para transmitir la señal) y el segundo emplea múltiples modos.

Según los estándares ANSI/TIA/EIA, la fibra monomodo instalada como backbone tiene mayores capacidades de ancho de banda y un alcance de 3000 m. La fibra multimodo transmite señales hasta 2000 m. La fibra monomodo se utiliza con frecuencia para enlazar edificios o WANs (Wide Area Networks), mientras que la fibra multimodo se emplea en backbones de LANs (Local Area Networks).

La fibra multimodo utiliza LEDs como fuente de luz y la fibra monomodo emplea láser (dispositivo que produce un haz de luz intenso). El vidrio monomodo es menos costoso que el vidrio multimodo. Los conectores y dispositivos electrónicos monomodo son más costosos.

2.1.2.2.1 Monomodo

Utiliza solo un modo de luz para propagarse a través del núcleo, cuyo diámetro está entre 8 y 10 micrones. El núcleo en este tipo de fibra es diez veces más grande que la longitud de onda de la luz que transporta. Los pulsos de luz son transmitidos en una línea recta por el núcleo (Figura 2.14). Utiliza una fuente de luz láser, puede transportar datos hasta 3000 m y se utiliza en exteriores para enlazar edificios.



Figura 2.14: Fibra Monomodo

2.1.2.2.2 Multimodo

Permite que múltiples modos de luz se propaguen a través del núcleo y recorran distancias según su ángulo de entrada, causando que lleguen a su destino a diferentes tiempos (dispersión modal). Utiliza vidrio de índice gradual, el cual ocasiona que la velocidad de la luz disminuya al pasar por el centro del núcleo y se incremente cuando recorre las áreas externas (Figura 2.15).

Una fibra óptica de 62.5/125 indica que los diámetros del núcleo y revestimiento son 62.5 y 125 micrones respectivamente. Como el diámetro del revestimiento es mayor que la longitud de onda de la luz transmitida, ésta se refleja dentro del núcleo conforme se propaga por la línea de transmisión. La fibra de 50/125 micrones se utiliza en backbones de edificios. Su gran ancho de banda permite soportar 1 Gigabit Ethernet. Esta fibra utiliza LEDs como dispositivos generadores de luz. Puede transportar datos a distancias de hasta 2000 m y se la utiliza en aplicaciones LAN, incluyendo cableado de backbone.

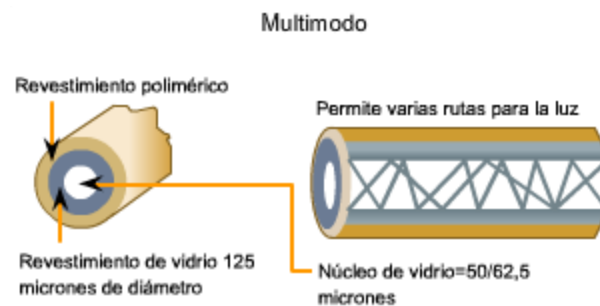


Figura 2.15: Fibra Multimodo

2.1.2.3 Ventajas

2.1.2.3.1 Inmunidad Electromagnética

No sufre EMI, RFI o cambios de voltaje. Es la solución en ambientes inflamables como cuartos de pintura, áreas de solventes o tanques de combustible. Su naturaleza no conductiva la hace ideal para áreas donde se producen rayos o existen líquidos (fondo de los océanos). Una conexión de fibra óptica evita el problema de las variaciones de potencial, eliminando así el peligro al que puede estar expuesto tanto el personal como los equipos. Como la fibra aísla los dispositivos que se conectan en cada extremo, es una

excelente opción para conectar sistemas completamente separados como dos LANs entre edificios.

2.1.2.3.2 Seguridad

Resulta difícil detectar remotamente la señal que está siendo transmitida por el cable. Para intervenir un circuito es necesario acceder a la fibra óptica y el personal de seguridad puede detectar fácilmente tal intervención.

2.1.2.3.3 Atenuación y Distancia

Un cable de fibra óptica funciona mejor respecto a la atenuación porque utiliza un repetidor óptico para amplificar el pulso de luz. Tiene un gran ancho de banda (cantidad de información que un medio puede transportar por unidad de tiempo). A mayor ancho de banda, mayor capacidad de transporte del cable. Los circuitos de fibra utilizados en conexiones troncales transmiten información hasta 2.5 Gbps. Las tasas de datos para LAN son 10 Mbps y 100 Mbps, con Gigabit Ethernet (1000 Mbps) en el backbone y armarios.

2.1.2.3.4 Tamaño y Peso

Es más ligera y su diámetro es más pequeño comparada con el cable de cobre.

2.1.2.4 Desventajas

La velocidad que se gana con la transmisión por fibra puede perderse en los puntos de conversión a cobre. La fibra es más costosa que el cobre, resiste menos a la manipulación, los conectores son más delicados, se requiere un mayor nivel de entrenamiento y habilidad durante la instalación y las herramientas así como los medidores de fibra son más costosos.

2.1.2.5 Conectores

Se utilizan para conectar la fibra a los paneles o dispositivos activos. La Figura 2.16 muestra algunos conectores que se utilizan para elaborar cables de interconexión, los cuales sirven para hacer conexiones en los paneles. Cuando se empalman las fibras, se utiliza una bandeja para proteger las fibras y sus conectores. El estándar ANSI/TIA/EIA 568B.3 establece que la máxima pérdida por empalme debe ser 0.75 dB y especifica que el conector recomendado para la instalación es el dúplex SC.



Figura 2.16: Conectores y Cables de Interconexión

2.1.2.5.1 *ST (Straight Tip)*

Fue definido por el estándar ANSI/TIA/EIA 568B.3. Utiliza una conexión de tipo bayoneta similar al cable coaxial pero más pequeña como se observa en la Figura 2.17. Es el más utilizado pero está siendo relegado porque requiere mayor espacio para asegurarlo y desconectarlo. El conector se inserta completamente en el receptáculo y se lo gira en el sentido horario para asegurarlo. Los conectores ST de alta calidad utilizan una férula cerámica para conseguir una alineación precisa y mayor durabilidad.



Figura 2.17: Conector ST

2.1.2.5.2 *SC (Subscriber Channel)*

Es el conector recomendado para instalaciones de fibra óptica según el estándar ANSI/TIA/EIA 568B.3 (Figura 2.18). Como tiene un mecanismo empuja-hala, reduce la cantidad de espacio necesario para agregar o remover una conexión. La forma del conector permite insertarlo de una sola forma y asegurar su alineación.



Figura 2.18: Conector SC

2.1.2.5.3 FC (Fixed Connection)

En la Figura 2.19 se puede apreciar que su diseño es similar al de los conectores SC y ST. El conector se inserta en el receptáculo y se lo enrosca para asegurar la conexión.



Figura 2.19: Conector FC

2.1.2.5.4 MT-RJ (Mechanical Transfer-Registered Jack)

Este conector ocupa poco espacio e incorpora dos fibras, una para transmitir y otra para recibir. Generalmente, se los utiliza en cajetines para Áreas de Trabajo y no en paneles de interconexión. La Figura 2.20 muestra que su apariencia es similar a un conector RJ-45 para cable de cobre.



Figura 2.20: Conector MT-RJ

2.1.2.5.5 LC (Lucent Connector)

Es ideal para aquellas aplicaciones donde el espacio es limitado. Su apariencia es similar al conector SC, pero son de menor tamaño (Figura 2.21). Tiene un mecanismo de sujeción parecido al de los conectores RJ-45 o RJ-11. Este conector inserta una pérdida de 0.3 dB en comparación con los 0.5 dB causados por otros conectores.

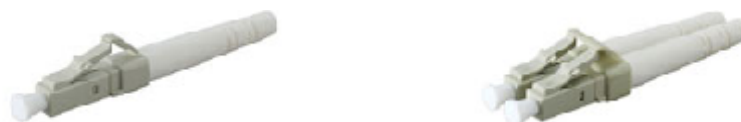


Figura 2.21: Conectores LC Simplex y Dúplex

2.1.2.5.6 MTP (Mechanical Transfer Pull Off)

Provee una interconexión confiable y de alto rendimiento de hasta 12 fibras. La alineación entre férulas se logra mediante dos guías de precisión que están pre-instaladas en un conector macho como el que se presenta en la Figura 2.22. Este conector utiliza el mecanismo empuja-hala.



Figura 2.22: Conector MTP

2.1.3 Cableado Estructurado

Es el sistema que considera las necesidades de cableado del cliente y las combina en un paquete. Este método de cableado organizado es reconocido por los instaladores, administradores de red y técnicos que manejan cables. Requiere planificación organizada y métodos para etiquetar y organizar los cables (Figura 2.23).



Figura 2.23: Cableado Estructurado

2.1.3.1 Reglas

2.1.3.1.1 Buscar una solución completa

Incluye los sistemas que están diseñados para conectar, enrutar, administrar e identificar sistemas de cableado estructurado. Una implementación basada en estándares asegura que las tecnologías actuales y futuras puedan ser soportadas. Muchos fabricantes producen sistemas de componentes modulares que pueden ser utilizados en conjunto para obtener una solución confiable. Estos componentes incluyen conectores, paneles y cables de interconexión, organizadores de cables, bastidores para ensamblaje y herramientas para identificación de la planta de cableado.

2.1.3.1.2 Planificar un crecimiento futuro

Asegura que la infraestructura necesaria sea la correcta conforme aparecen nuevos requerimientos. Los cables de Categorías 5e, 6 y de fibra óptica deben ser considerados para satisfacer las necesidades futuras. El número de circuitos instalados también debe cumplir con estos requerimientos. Se debe planificar una instalación de Capa Física que funcione para diez años o más.

2.1.3.1.3 Estar consciente de los costos

Una instalación y los costos involucrados con los modernos sistemas de redes están relacionados con la infraestructura. Instalar y mantener infraestructuras separadas para voz, datos y video es costoso e ineficiente. Una solución de cableado que maneje todas las aplicaciones puede reducir los costos de instalación y mantenimiento.

2.1.3.1.4 No cerrarse en las opciones

Considera varios fabricantes. Una ventaja de los sistemas de Categoría 5 que utilizan conectores RJ-45 es su aceptación universal y disponibilidad de componentes que pueden ser conectados sin adaptadores.

2.1.3.2 Estándares

Son procedimientos que se especifican oficialmente y sirven como modelo de excelencia. Los estándares pueden estar especificados por un solo fabricante o soportar interoperabilidad multi-fabricante. Varias compañías, organizaciones y entidades

gubernamentales regulan los cables que se utilizan. Los planes de cableado integral denominados SCSs (Structured Cable Systems) proveen:

- Descripciones de medios estandarizados y planos para cableado de backbone y horizontal.
- Interfaces de conexión estándar para la conexión física de equipos.
- Diseño consistente y uniforme que sigue principios de diseño básicos.
- Componentes probados que minimizan el riesgo de incompatibilidad.
- Arquitectura abierta que soporta equipos y aplicaciones de varios fabricantes, incluyendo teléfonos análogos y digitales, computadores personales y equipos de video conferencia.
- Costos de mantenimiento reducidos.
- Entrenamiento específico y certificación.

2.1.3.2.1 American National Standards Institute (ANSI)

Es una organización que administra y coordina el sistema de estandarización y evaluación de conformidad en Estados Unidos. Identifica los requerimientos industriales para los estándares nacionales y coordina su desarrollo, resuelve problemas de estándares nacionales y asegura la participación efectiva en la estandarización internacional. ANSI no desarrolla estándares, pero facilita el desarrollo mediante procesos de consenso entre grupos calificados.

2.1.3.2.2 TIA y EIA

Son asociaciones que desarrollan y publican conjuntamente estándares que cubren cableado estructurado de voz y datos para LANs. La TIA (Telecommunications Industry Association) y EIA (Electronic Industries Alliance) están acreditadas por la ANSI para desarrollar estándares de industria para productos de telecomunicaciones, por lo que muchos estándares se etiquetan como ANSI/TIA/EIA. Los comités y subcomités de la TIA/EIA desarrollan estándares para fibra óptica, equipo en las premisas del usuario, equipo de red y comunicaciones inalámbricas y satelitales.

2.1.3.2.3 *Estándares ANSI/TIA/EIA*

Han creado la necesidad de estandarizar el diseño de los medios de telecomunicaciones y el proceso de implementación. Las adecuaciones físicas son inevitables en la mayoría de edificios y crean la necesidad de interoperabilidad, escalabilidad, soporte y flexibilidad.

2.1.3.2.3.1 TIA/EIA-568-A (Estándar de Cableado de Telecomunicaciones para Edificios Comerciales)

- **ANSI/TIA/EIA 568-B.1:** Especifica un sistema de cableado genérico para edificios comerciales que soporta un ambiente multi-fabricante. Establece el rendimiento y los criterios técnicos para varias configuraciones de sistemas de cableado. Especifica requerimientos de cableado, distancias, configuraciones de cajetines, conectores de telecomunicaciones y topología recomendada para diseño de redes.
- **ANSI/TIA/EIA 568-B.2:** Especifica los requerimientos mínimos para cableado de telecomunicaciones de par trenzado y sus componentes. También explica los procedimientos de medida que se necesitan para la verificación de cableado de par trenzado, los instrumentos de prueba y procedimientos de medida para verificar los parámetros de transmisión.
- **ANSI/TIA/EIA 568-B.3:** Especifica los requerimientos mínimos para componentes de fibra óptica (cables, conectores, hardware, cables de interconexión y equipo de prueba).

2.1.3.2.3.2 TIA/EIA-568-B (Requerimientos de componentes y transmisión para un medio)

El estándar de cableado de telecomunicaciones para edificios comerciales TIA/EIA-568-B es el más utilizado e identifica los requerimientos mínimos, topología y distancias recomendadas, especificaciones de medios, conexiones de hardware y asignación de conectores y pines.

Estos estándares ANSI/TIA/EIA indican la distribución de los colores de cada hilo en un conductor al terminar los cables de datos de 4 pares. En la Figura 2.24 se observa que los dos esquemas son similares pero se invierten dos de los cuatro pares.

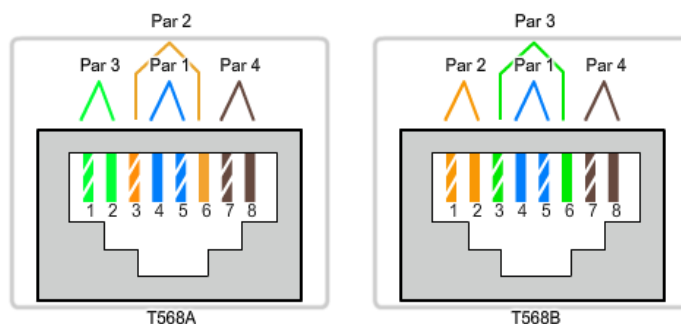


Figura 2.24: Estándares T568A y T568B

2.1.3.2.3.3 TIA/EIA-569-A (Estándar de Rutas y Espacios para Edificios Comerciales)

Especifica las prácticas de diseño y construcción para las rutas y espacios que soportan medios y equipos de telecomunicaciones en edificios. Proporciona especificaciones para Cuartos de Telecomunicaciones y equipo de administración de cables (bastidores, bandejas y rieles).

2.1.3.2.3.4 TIA/EIA-570-A (Estándar de Cableado de Telecomunicaciones Residenciales y Comerciales)

Presenta especificaciones de cableado para seguridad, audio, televisión, sensores, alarmas e intercomunicación. Este estándar está orientado a implementaciones en construcciones nuevas, adiciones y remodelaciones.

2.1.3.2.3.5 TIA/EIA-606 (Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales)

Especifica que cada unidad de terminación de hardware debe tener un identificador, el cual tiene que marcarse en la unidad o etiqueta. Cuando se utilizan identificadores en el Área de Trabajo, debe colocarse una etiqueta en el cajetín o conector.

2.1.3.2.3.6 TIA/EIA-607 (Requerimientos de Aterrizaje de Edificios Comerciales para Telecomunicaciones)

Especifica las prácticas de aterrizaje para varios sistemas que pueden ser instalados en las premisas del cliente, así como la interfaz entre los sistemas de aterrizaje del edificio y los equipos de telecomunicaciones.

2.1.3.3 Subsistemas

Los subsistemas que describen las funciones e identifican las necesidades de cada área son (Figura 2.25):

- **Punto de Demarcación:** Está en la entrada del cuarto de equipos y es el lugar donde los cables del proveedor de servicio externo se conectan con el sistema local.
- **Cuarto de Telecomunicaciones:** Lugar donde se realizan las conexiones para distribuir los servicios del cableado de backbone al cableado horizontal.
- **Cableado de Backbone:** Cableado Vertical.
- **Cableado de Distribución:** Cableado Horizontal.
- **Área de Trabajo**

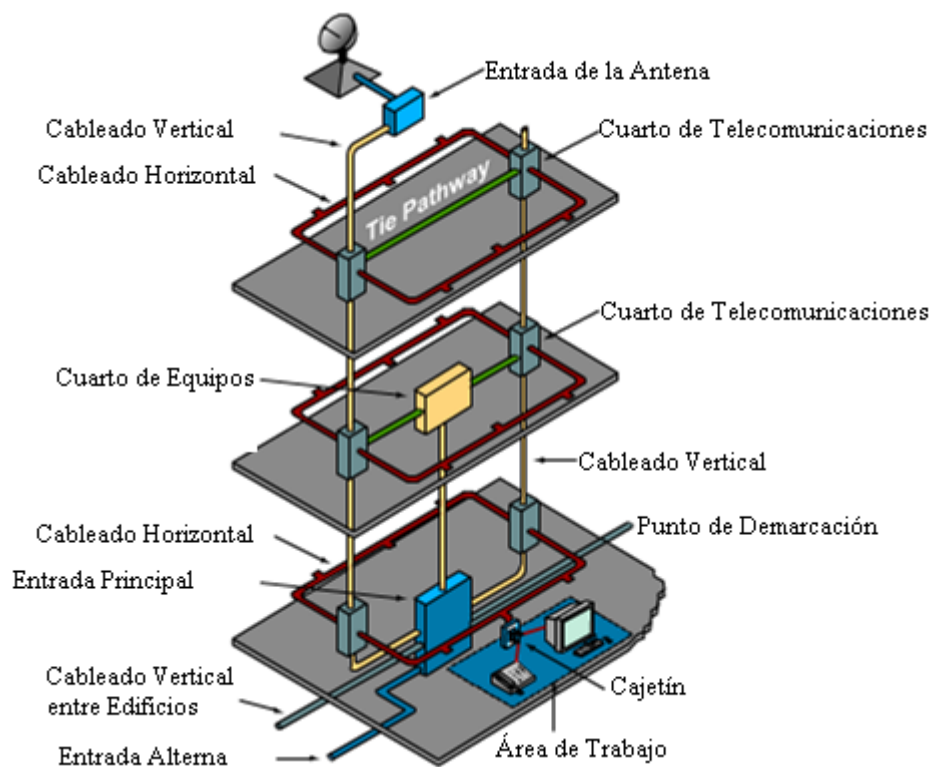


Figura 2.25: Subsistemas del Cableado Estructurado

2.1.3.3.1 *Punto de Demarcación*

Es el punto en el cual el cableado de exteriores se conecta con el cableado de backbone en el interior del edificio como se observa en la Figura 2.26. Representa el límite entre la responsabilidad del proveedor de servicio y la del cliente. En muchos edificios, este es el mismo PoP (Point-of-Presence) para electricidad y agua.



Figura 2.26: Punto de Demarcación

2.1.3.3.2 *Cuarto de Telecomunicaciones*

Es el centro de la red de voz y datos donde se instalan los equipos del sistema de telecomunicaciones (conmutadores y enrutadores) y las terminaciones mecánicas para el sistema de cableado horizontal y de backbone (Figura 2.27). Estos cuartos deben estar lejos de fuentes de EMI (transformadores, motores, equipos de rayos X, calefactores de inducción, soldadores de arco, radios y equipo de radar). Los cuartos con tuberías de agua deben evitarse. Es conveniente colocar los Cuartos de Telecomunicaciones junto a paredes estructurales, pues soportan la estructura del edificio y no sufren alteraciones. Estas habitaciones deben ubicarse de manera que se pueda acceder a la red de telecomunicaciones cuando ocurran cambios en la estructura del edificio, ya que es una tarea difícil moverlos cuando están instalados y activos.

Al planificar una red es necesario saber dónde colocar el Cuarto de Telecomunicaciones, porque este espacio contiene los cables de red y dispositivos. Debe ser fácil acceder a este lugar, pero como es un punto vulnerable en la red tiene que estar bien asegurado. Los edificios de oficinas deben tener un Cuarto de Telecomunicaciones en cada piso para unir el cableado de backbone y el horizontal. Se requiere más de uno de estos espacios por piso si la distancia en un Área de Trabajo excede los 90 m o si el piso atendido sobrepasa los 1000 m².



Figura 2.27: Cuarto de Telecomunicaciones

2.1.3.3.2.1 MCs, ICs y HCs

La Figura 2.28 muestra que en algunas redes existe más de un Cuarto de Telecomunicaciones porque suelen distribuirse en varios pisos o edificios y se necesitan repetidores, hubs, bridges o conmutadores para regenerar la señal y transmitirla. El Cuarto de Telecomunicaciones primario (MC) es el centro de la red porque allí se origina todo el cableado e instala la mayor parte del equipo. El IC se conecta al MC. En el HC se encuentran los cables de distribución de un solo piso.

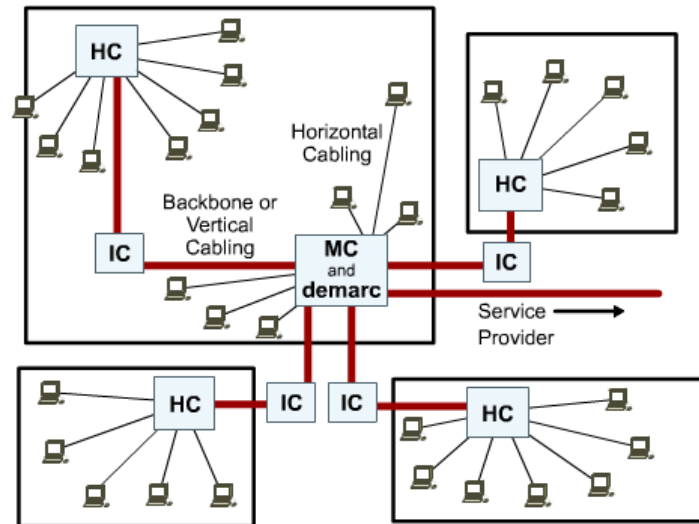


Figura 2.28: Planificación de los MCs, ICs y HCs

- **MCs (Main Cross-Connects):** Es el punto principal de un edificio que controla los demás Cuartos de Telecomunicaciones. Es parte de un cuarto de servidores que contiene servidores de comunicaciones y de archivos. Los ICs o HCs se conectan al MC. El cableado de backbone se utiliza para conectar los ICs y HCs que están en diferentes pisos. Cuando la red está en un solo edificio, el MC se ubica en el piso del medio, aun cuando el Punto de Demarcación se encuentre en el primer piso o subsuelo. Para redes con varios edificios, en uno de ellos se coloca el MC, y los demás tienen su propio IC que conecta los HCs.
- **ICs (Intermediate Cross-Connects):** En este cuarto está el cableado y los dispositivos que se utilizan para un piso. El cuarto está equipado con paneles de interconexión, unidades de terminación de fibra, conmutadores, hubs y organizadores. El estándar ANSI/TIA/EIA-568-B especifica que los ICs deben conectarse al MC mediante cableado vertical. Cuando las longitudes del cableado de backbone son mayores que las soportadas por el cable UTP de Categoría 5e, se debe utilizar cableado de fibra óptica.
- **HCs (Horizontal Cross-Connects):** Es el Cuarto de Telecomunicaciones más cercano a las estaciones de trabajo, está formado por un panel de interconexión y dispositivos de red (repetidores, hubs o conmutadores) y puede ser un armario

montado en un cuarto. El cableado horizontal incluye los medios de red desde el armario hasta las estaciones de trabajo. El estándar ANSI/TIA/EIA-568-B.1 especifica que la longitud del cableado horizontal desde el HC hasta el Área de Trabajo no puede exceder los 90 m. La longitud máxima del cable desde el cajetín a la estación de trabajo es 5 m (Figura 2.29).

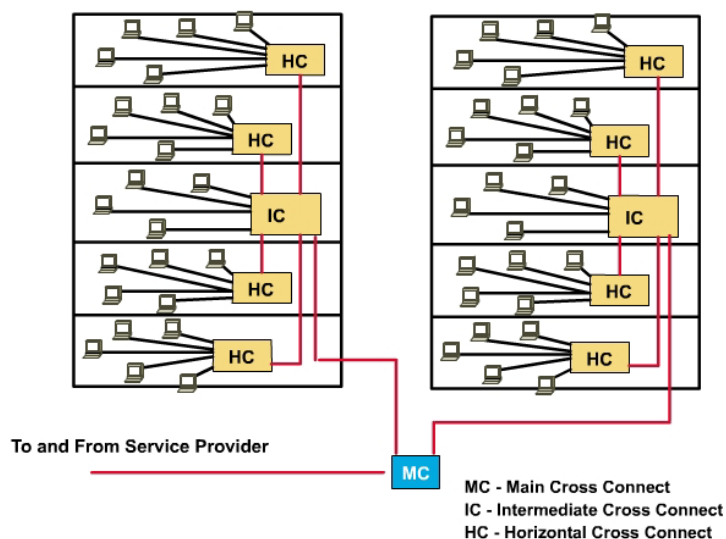


Figura 2.29: Conexión de los MCs, ICs y HCs

2.1.3.3.2.2 Administración de Cables

Los dispositivos de administración de cables se utilizan para organizar los cables, crear una ruta estructurada y realizar modificaciones fácilmente. Las bandejas se pueden utilizar en instalaciones livianas y los bastidores de escalera para soportar cargas pesadas. En la Figura 2.30 se observan los conductos de diferentes tipos se utilizan para llevar los cables por las paredes, techos y pisos. Los interductos (tubos plásticos que protegen el cable y están atados a bastidores de escalera) se utilizan para cables de fibra óptica.



Figura 2.30: Canaletas e Interductos

2.1.3.3.2.3 Armarios

Los equipos de un Cuarto de Telecomunicaciones se colocan en armarios, los cuales son marcos metálicos que se montan en el piso y permiten la instalación de paneles de interconexión y equipo activo (conmutadores, enrutadores o servidores). Los equipos que requieren acceso frontal y posterior se montan en armarios abiertos (Figura 2.31). Muchos fabricantes colocan supresores de picos en los armarios y luego tienden cables de poder por los carriles a fin de proporcionar energía. Como los equipos generan calor, es importante no bloquear los ventiladores. Es necesario dejar espacio para nuevos armarios y paneles de interconexión.



Figura 2.31: Armario

Existe un código de colores estándar que permite identificar los cables rápidamente como se aprecia en la Figura 2.32:

- **Naranja:** Punto de demarcación.
- **Verde:** Conexiones de red.
- **Púrpura:** Equipo común, PBXs (Private Branch Exchanges), LANs (Local Area Networks) y multiplexores.
- **Blanco:** Backbone primario.
- **Gris:** Backbone secundario.
- **Azul:** Cableado horizontal.
- **Café:** Backbone entre edificios.
- **Amarillo:** Miscelaneos (auxiliar, alarmas y seguridad).
- **Rojo:** Reservado para uso futuro.

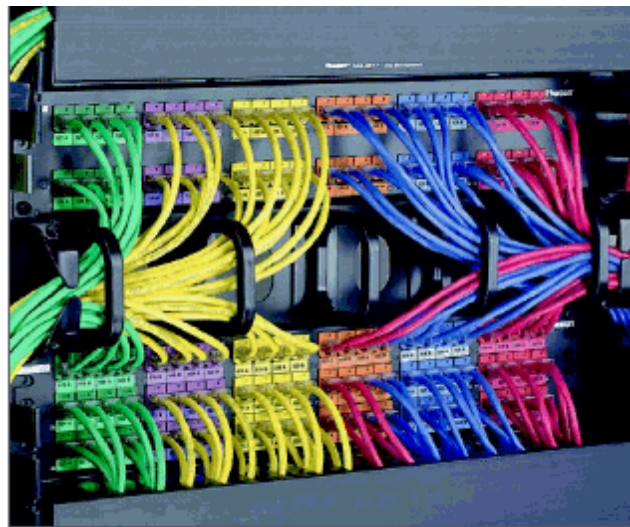


Figura 2.32: Código de Colores para Terminaciones de Cables

2.1.3.3.2.4 Cables Cross-Connect

Los MCs (Main Cross-Connects) se utilizan para incorporar servicios al sistema de distribución conectando los cables de los proveedores al cableado de backbone. Los ICs (Intermediate Cross-Connects) conectan los servicios del cableado de backbone de los MCs. Los HCs (Horizontal Cross-Connects) conectan los servicios a las estaciones de trabajo.

2.1.3.3.2.5 Cables de Interconexión

Los cables de interconexión se utilizan cuando se necesitan cambios frecuentes. El estándar TIA/EIA-568-B.1 especifica una longitud máxima de 5 m para los cables de interconexión (Figura 2.33).



Figura 2.33: Cable de Interconexión

- Cables Cruzados:** Se utilizan como cables troncales o de backbone para conectar los conmutadores en una LAN o dos estaciones de trabajo para crear una red pequeña. En un cable cruzado de 4 pares se invierte el segundo y tercer par en uno de sus extremos. La Figura 2.34 muestra que un cable cruzado utiliza el esquema T568A en un extremo y T568B en el otro. Esta configuración permite que los pares de transmisión de un dispositivo envíen señales a los pares de recepción de otro. Los cables cruzados se utilizan para conectar dispositivos similares.

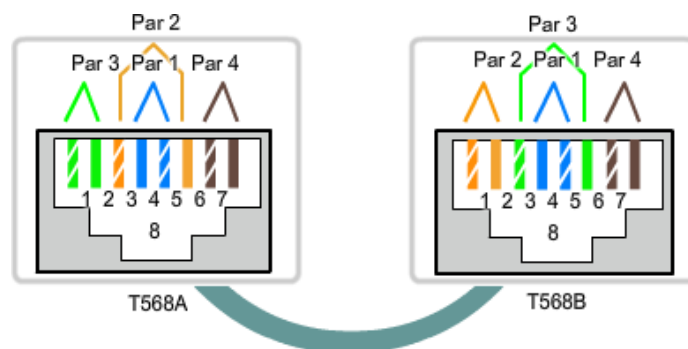


Figura 2.34: Cable Cruzado

- **Cables Directos:** En los cables directos se asignan los mismos pines en ambos extremos como se observa en la Figura 2.35. Si se utilizan entre un conmutador y una estación de trabajo, se considera parte del cableado horizontal. Estos cables también se utilizan para conectar un cajetín a una estación de trabajo.

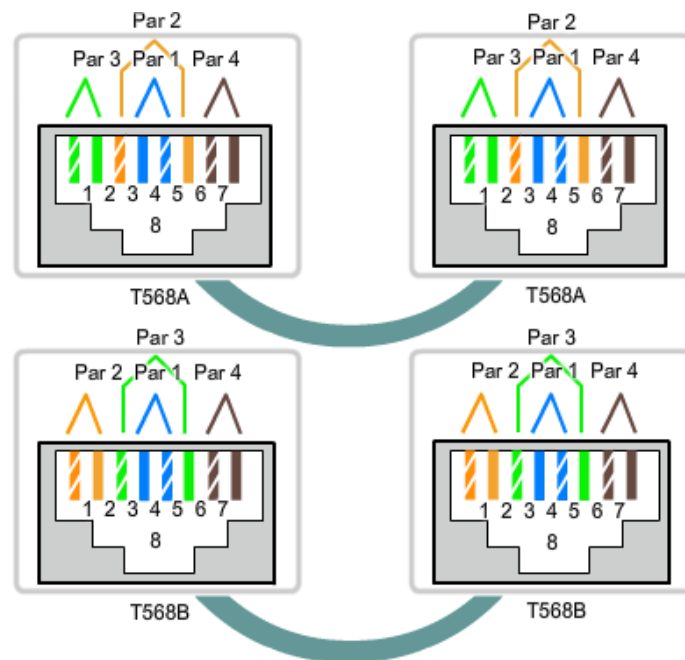


Figura 2.35: Cable Directo

- **Cables Rollover:** Se utilizan como cables de consola para conectar un computador a un enrutador o conmutador. Un extremo del cable corresponde al esquema 568-B o A, y el otro extremo se invierte pin a pin (Figura 2.36).

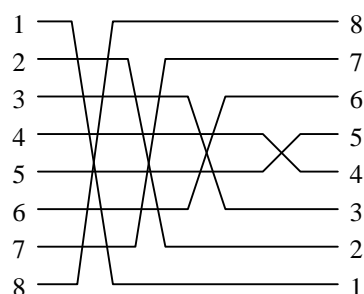


Figura 2.36: Cable Rollover

2.1.3.3.2.6 Densidades de Cableado

Es el número de cables que entran al Cuarto de Telecomunicaciones. Un etiquetamiento apropiado es importante cuando se considera la densidad de las terminaciones en un Cuarto de Telecomunicaciones.

2.1.3.3.2.7 Equipo de Montaje

Un hub y panel de interconexión pueden ser instalados en un bastidor de pared con bisagra o un armario de distribución. El primero debe estar adherido al panel que cubre la superficie de la pared. La bisagra permite la oscilación de manera que el personal pueda acceder fácilmente. Se debe considerar 48 cm para que el panel oscile. El segundo debe tener un mínimo de 15 cm de separación entre la pared y el equipo, y alrededor de 30 a 45 cm para acceso físico. Si se monta un panel de interconexión, hub u otro equipo en un armario se requiere 76 cm de espacio libre en la parte frontal para abrir la puerta.

2.1.3.3.2.8 Puertas y Cerraduras

El estándar TIA/EIA-569 especifica el tamaño de la puerta y el tipo de seguros utilizados en un Cuarto de Telecomunicaciones. La puerta debe tener por lo menos 0.9 m de ancho y abrirse hacia afuera del cuarto. El seguro debe estar ubicado en la parte exterior pero debe permitir salir en cualquier momento a quien se encuentre en el interior.

2.1.3.3.2.9 Paredes, Piso y Techo

El piso donde está ubicado un Cuarto de Telecomunicaciones debe soportar la carga especificada por las instrucciones de instalación incluidas en el equipo, siendo la capacidad mínima 4.8 kPa o 100 lb/pie². El cuarto debe tener un piso elevado para acomodar los cables horizontales que vienen de las áreas de trabajo. Si esto no es posible, el cuarto debe tener un bastidor de 31 cm que soporte los equipos y cables. Las cubiertas de los pisos deben ser de azulejo u otro tipo de acabado similar, porque ayuda a controlar el polvo y protege a los equipos de estática. Además, se deben utilizar materiales de prevención de incendios que cumplan con todas las regulaciones vigentes. Los cuartos no deben tener cielo falso, pues crean una instalación insegura que permite acceso no autorizado.

2.1.3.3.2.10 Iluminación

El Cuarto de Telecomunicaciones debe tener un mínimo de dos tomacorrientes dobles AC en circuitos separados. También debe tener por lo menos un tomacorriente doble colocado cada 1.8 m en cada pared del cuarto y a 150 mm sobre el piso. Un interruptor de pared que controle la iluminación principal del cuarto debe colocarse cerca de la puerta de ingreso. Los requerimientos para un Cuarto de Telecomunicaciones especifican un mínimo de 500 lux (resplandor de luz) y las lámparas deben ser montadas sobre el piso a un mínimo de 2.6 m.

2.1.3.3.2.11 Temperatura y Humedad

El control ambiental en un Cuarto de Telecomunicaciones debe ser independiente y mantenerse las 24 horas del día y los 365 días del año. Este cuarto debe tener aire acondicionado para mantener la temperatura entre 17 y 21 grados centígrados cuando los equipos se encuentran operando a su máxima capacidad. La humedad debe estar entre 30 y 50%.

2.1.3.3.3 *Cuarto de Equipos*

Pueden existir en grandes redes o en compañías que se especializan en telecomunicaciones. En estos lugares se encuentran PBXs, protección de voltaje secundaria, receptores satelitales, moduladores, equipo de Internet de alta velocidad, etc. El estándar TIA/EIA-569-A especifica el diseño de este cuarto.

2.1.3.3.4 *Áreas de Trabajo*

Son las áreas atendidas por un Cuarto de Telecomunicaciones. Las áreas pueden delimitarse con un bosquejo del plano del piso y marcando círculos con los Cuartos de Telecomunicaciones en el centro como se muestra en la Figura 2.37. La longitud máxima permitida por cada medio establece el límite externo. Para el caso de UTP, el límite se considera como 100 m, pero debe reducirse porque los alambres van por bandejas y escaleras. Estos elementos guían los cables sobre las Áreas de Trabajo (techos falsos), por lo que el estándar ANSI/TIA/EIA-568-B especifica un máximo de 5 m para cada cable de interconexión que interconecta los paneles con los equipos, así como la pared al teléfono o computador. Normalmente se utiliza 50 m como el radio del Área de Trabajo en el diseño.

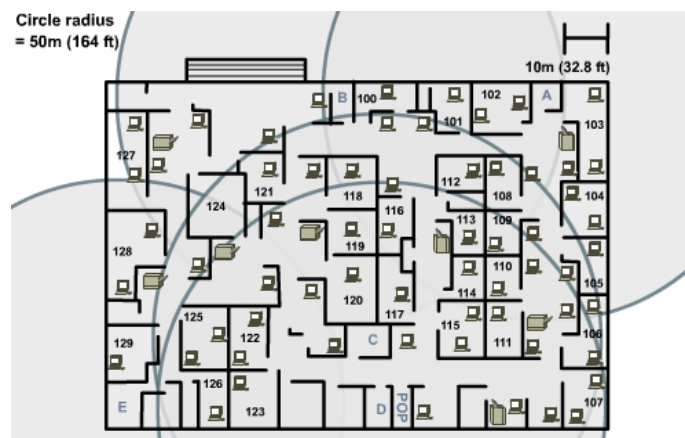


Figura 2.37: Áreas de Trabajo

2.1.3.4 Cableado de Backbone (Vertical)

Está formado por los cables de backbone, cross-connects intermedios y principales, terminaciones mecánicas y cables de interconexión. Existen dos niveles: el primero entre el MC y los ICs y el segundo entre los ICs y HCs. El cableado horizontal conecta las áreas de trabajo a los HCs. Este tipo de cableado incluye los cables entre los Cuartos de Telecomunicaciones de un mismo piso, conexiones verticales entre Cuartos de Telecomunicaciones en pisos diferentes, cables entre el Cuarto de Telecomunicaciones y el Punto de Demarcación y cables entre edificios.

2.1.3.4.1 Cable de Fibra Óptica

La fibra óptica es un medio efectivo para transportar tráfico de backbone, ya que no se ve afectada por la interferencia de ruido eléctrico o radio frecuencia. Tampoco conduce corrientes que pueden causar lazos de tierra. Estos sistemas tienen gran ancho de banda y operan a altas velocidades.

2.1.3.4.2 Cable Multipar

Este tipo de cable se utiliza para telefonía. No es conveniente para datos porque la diafonía entre aplicaciones puede ser severa.

2.1.3.5 Cableado del Área de Trabajo

El equipo del Área de Trabajo puede conectarse a los servicios a través de un MUTOA (Multiuser Telecommunications Outlet Assembly) o CP (Consolidation Point) como se puede apreciar en las Figuras 2.38 y 2.39. El Área de Trabajo permite conectar dispositivos al cableado horizontal utilizando un cable de interconexión. Una MUTOA es un dispositivo de interconexión que se utiliza para conectar equipo directamente al HC. El punto de consolidación permite usar las salidas en el Área de Trabajo y realizar cambios en estas interconexiones. El cableado del Área de Trabajo se extiende desde el cajetín de telecomunicaciones hasta la estación de trabajo. Los componentes del Área de Trabajo incluyen el equipo de la estación de trabajo (computadores, teléfonos, fax e impresoras), cables de interconexión y adaptadores externos para los cajetines.

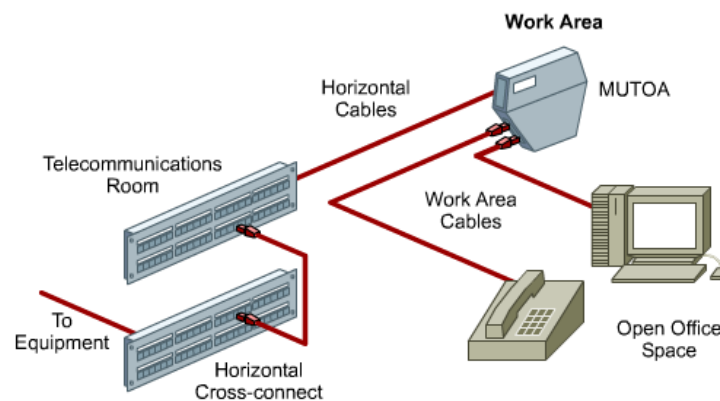


Figura 2.38: Instalación de un MUTOA

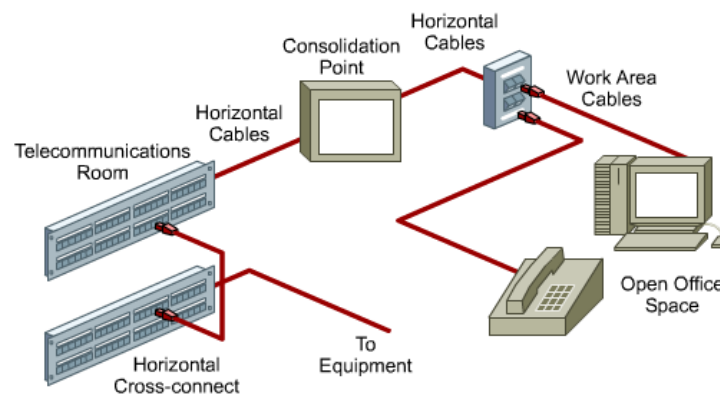


Figura 2.39: Punto de Consolidación

2.2 Elementos Activos

2.2.1 Red Jerárquica

En esta clase de red se facilita la administración, expansión y resolución de problemas. La Figura 2.40 muestra que su diseño consiste en dividir la red en tres capas: Acceso, Distribución y Core, las cuales tienen funciones específicas que permiten la escalabilidad y mejoran el funcionamiento.

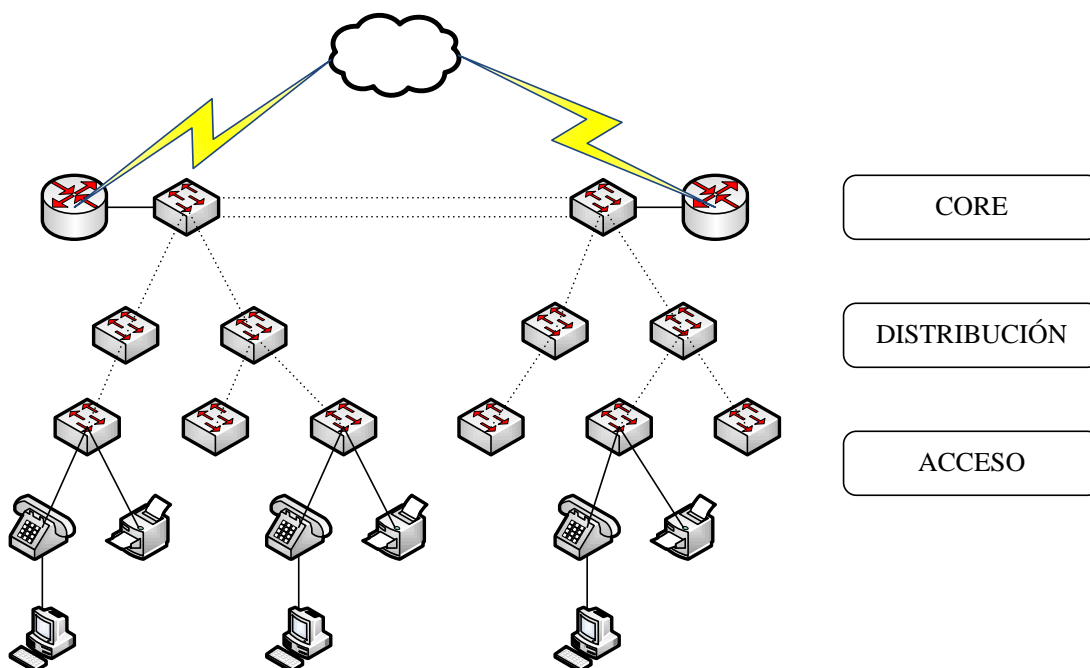


Figura 2.40: Red Jerárquica

- **Acceso:** Se conecta con los dispositivos de usuario final (computadores, impresoras y teléfonos IP) para proveer acceso a la red. Puede incluir enrutadores, conmutadores, bridges, hubs y puntos de acceso inalámbricos. Su objetivo principal es proporcionar un medio para conectar y controlar los dispositivos de red.
- **Distribución:** Agrega los datos recibidos de la capa inferior antes de transmitirlos al Core para enrutarlos hacia su destino. Controla el flujo de tráfico utilizando políticas y limita los dominios de broadcast mediante enrutamiento entre VLANs

(Virtual Local Area Networks), las mismas que permiten segmentar el tráfico en subredes. Los conmutadores de Distribución son dispositivos de alto rendimiento, disponibilidad y redundancia.

- **Core:** Es el backbone de alta velocidad de la Internet y permite la interconectividad entre dispositivos de Distribución, razones por las cuales debe ser altamente disponible y redundante. Agrega el tráfico de todos los dispositivos de Distribución y transmite grandes cantidades de datos rápidamente. Usualmente se implementa un modelo de Core colapsado, donde las capas de Distribución y Core se combinan.

2.2.1.1 Beneficios

- **Escalabilidad:** El diseño modular permite reproducir elementos conforme la red crece. La consistencia de los módulos hace que la planificación e implementación sea fácil.
- **Redundancia:** La disponibilidad es más importante conforme la red crece y puede incrementarse con implementaciones redundantes. Los conmutadores de Acceso se conectan a dos conmutadores de Distribución para asegurar la redundancia. Si un conmutador de Distribución falla, el conmutador de Acceso puede cambiarse al otro conmutador de Distribución. Los conmutadores de Distribución se conectan a dos o más conmutadores de Core para asegurar disponibilidad. La redundancia es limitada en la Capa de Acceso, porque los dispositivos de usuario final no pueden conectarse a varios conmutadores de Acceso. En caso de que un conmutador de Acceso falle, solamente los dispositivos conectados a ese conmutador resultarán afectados.
- **Rendimiento:** Se mejora al evitar la transmisión de datos a través de conmutadores intermedios de bajo rendimiento. Los datos se envían utilizando puertos agrupados desde la Capa de Acceso a la Capa de Distribución, ésta última emplea sus capacidades de alto rendimiento para transmitir el tráfico al Core y enrutarlo hacia

su destino. Como las capas de Core y Distribución operan a velocidades muy altas, no existe competencia por el ancho de banda.

- **Seguridad:** Los puertos de los conmutadores de Acceso se pueden configurar con varias opciones de seguridad. En la Capa de Distribución se utilizan políticas de seguridad más avanzadas.
- **Administración:** Es relativamente simple, pues cada capa realiza una función específica. Si se necesita cambiar la funcionalidad de un conmutador de Acceso, se puede repetir el cambio en los demás conmutadores, ya que realizan las mismas funciones. La instalación de conmutadores se simplifica porque las configuraciones pueden ser copiadas entre dispositivos.
- **Mantenimiento:** La modularidad hace que el mantenimiento sea fácil. Algunos modelos de diseño tienen un límite para el tamaño de la red, porque si se lo excede, el mantenimiento se vuelve complicado y costoso.

2.2.1.2 Principios de Diseño

- **Diámetro de Red:** Es el número de dispositivos que un paquete tiene que cruzar antes que alcance su destino y debe mantenerse pequeño para asegurar retardos bajos y predecibles (Figura 2.41).
- **Agregación de Ancho de Banda:** En cualquier capa se puede agregar ancho de banda. Al conocer los requerimientos de ancho de banda, los enlaces entre conmutadores pueden ser agrupados mediante tecnología EtherChannel (Figura 2.41).
- **Redundancia:** Forma parte de una red altamente disponible (Figura 2.41).

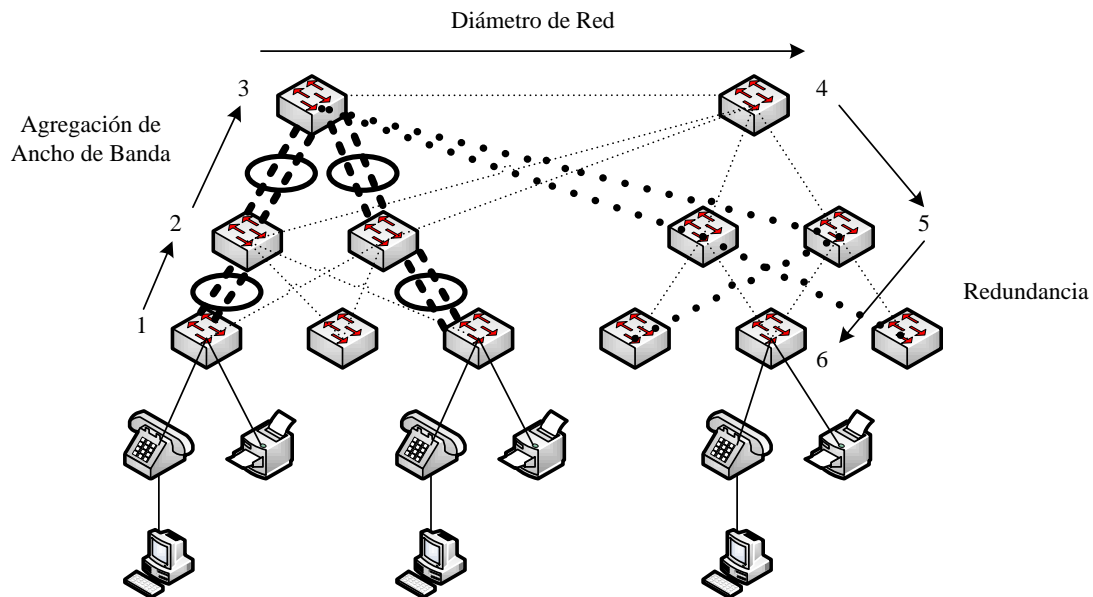


Figura 2.41: Principios de Diseño

2.2.2 Red Convergente

La combinación de comunicaciones de voz y video en una red de datos se denomina convergencia. Las redes convergentes han existido solamente en grandes empresas debido a la complejidad involucrada en su funcionamiento. Las redes convergentes requerían administración relacionada con QoS (Quality of Service), porque el tráfico de voz y video necesitaba ser clasificado y priorizado. El equipo antiguo dificulta el proceso (Figura 2.42a). Las redes convergentes se han vuelto populares en el mercado de las pequeñas y medianas empresas por los avances tecnológicos (Figura 2.42b). En una red convergente existe una sola red para administrar. Resulta menos costoso implementar una sola infraestructura de red que tres distintas. Dado que las redes jerárquicas actuales consideran los requerimientos de ancho de banda para voz, video y datos se puede lograr la convergencia.



Figura 2.42a: Equipo Antiguo



Figura 2.42b: Tecnología Actual

2.2.3 Selección de Conmutadores

2.2.3.1 Análisis de Flujo de Tráfico

Para seleccionar un conmutador para una red jerárquica, se necesita tener especificaciones sobre el flujo de tráfico (datos enviados a través de la red por un periodo determinado de tiempo), comunidades de usuario y servidores de datos y de almacenamiento. Consiste en medir la utilización del ancho de banda en una red y analizar los datos para planificar la capacidad y mejorar el rendimiento. Este proceso se realiza utilizando software de análisis de tráfico.

El flujo de tráfico en una red se puede monitorear a través de los puertos de un conmutador para registrar la utilización del ancho de banda. Cuando se analizan los datos se puede determinar los requerimientos según la capacidad en ciertos momentos del día y dónde se genera la mayor cantidad de datos. Entre las herramientas de análisis de tráfico que automáticamente registran los datos en una base de datos y realizan un análisis de tendencia se pueden mencionar: Cisco NetFlow, FlowScan, Autofocus, Fluxoscope, PRTG (Paessler Router Traffic Grapher), sFlow, Cricket, Wireshark, etc.

2.2.3.1.1 Análisis de Comunidades de Usuario

Consiste en identificar grupos de usuarios y su impacto en el rendimiento de la red. La manera en que los usuarios se agrupan influye en la densidad de puertos y el flujo de tráfico, el cual incide en la selección de los conmutadores.

En un edificio de oficinas, los usuarios finales se agrupan según su función porque requieren acceso similar a los recursos y aplicaciones. Cada departamento tiene un número diferente de usuarios y requiere acceso a diferentes recursos. Un buen diseño de red considera el crecimiento de cada departamento para asegurar que existan suficientes puertos.

Al medir el tráfico generado por las aplicaciones en uso y determinar la ubicación de la fuente de datos, se puede identificar el efecto de añadir más usuarios a una comunidad. La ubicación de las comunidades de usuarios determina dónde se ubican los servidores de almacenamiento y las granjas de servidores. En la Figura 2.43 se observa que si los usuarios se encuentran cerca de los servidores, es posible reducir el diámetro de la red y disminuir el impacto del tráfico.

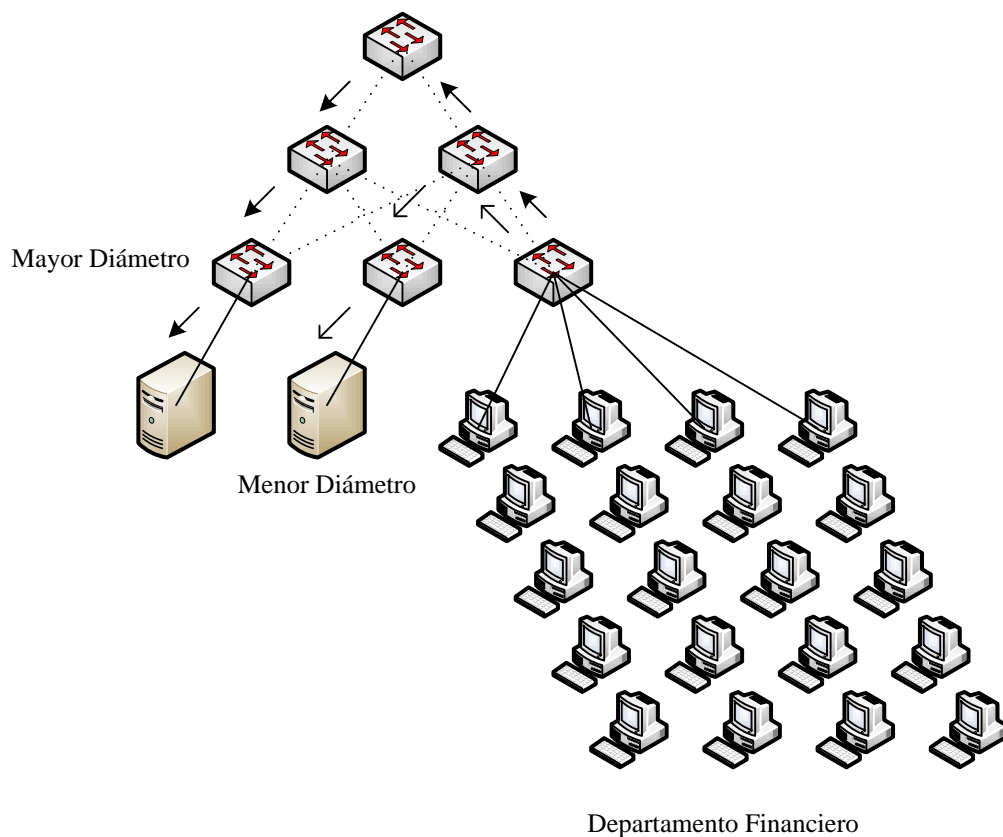


Figura 2.43: Comunidades de Usuario

2.2.3.1.2 Análisis de Servidores de Datos y de Almacenamiento

El análisis de tráfico debe considerar donde se ubican los servidores de datos y de almacenamiento para determinar el impacto del tráfico en la red. Los servidores de datos pueden ser SANs (Storage Area Networks), NAS (Network-Attached Storage), unidades de respaldo o dispositivos de almacenamiento.

Es importante considerar el tráfico cliente-servidor y servidor-servidor. Las Figuras 2.44a y 2.44b muestran que el tráfico cliente-servidor se genera cuando un dispositivo cliente accede a los servidores y que el tráfico servidor-servidor se genera entre dispositivos de almacenamiento. Para optimizar el tráfico servidor-servidor, los equipos que necesitan acceso frecuente a ciertos recursos deben estar cerca para que el tráfico generado no afecte al funcionamiento de la red.

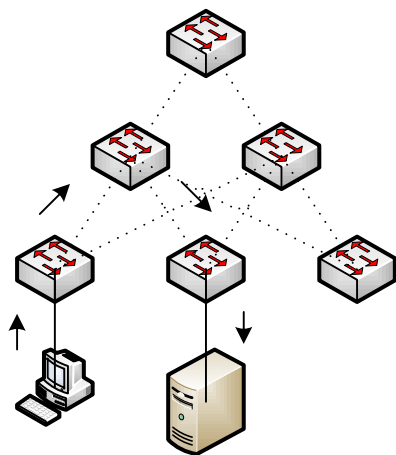


Figura 2.44a: Cliente-Servidor

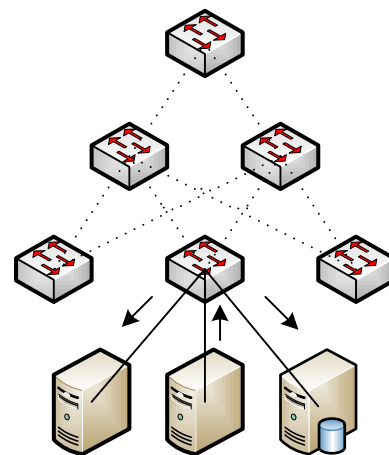


Figura 2.44b: Servidor-Servidor

2.2.3.2 Diagramas Topológicos

Son representaciones gráficas de la infraestructura de red que indican las interconexiones entre conmutadores. Estos diagramas muestran trayectorias redundantes y puertos agrupados. Además, especifican la cantidad de conmutadores en la red con su configuración, las densidades de los dispositivos y comunidades de usuarios (Figura 2.45). Los diagramas topológicos permiten identificar cuellos de botella para enfocar el análisis de tráfico en aquellas áreas donde las mejoras puedan tener mayor impacto.

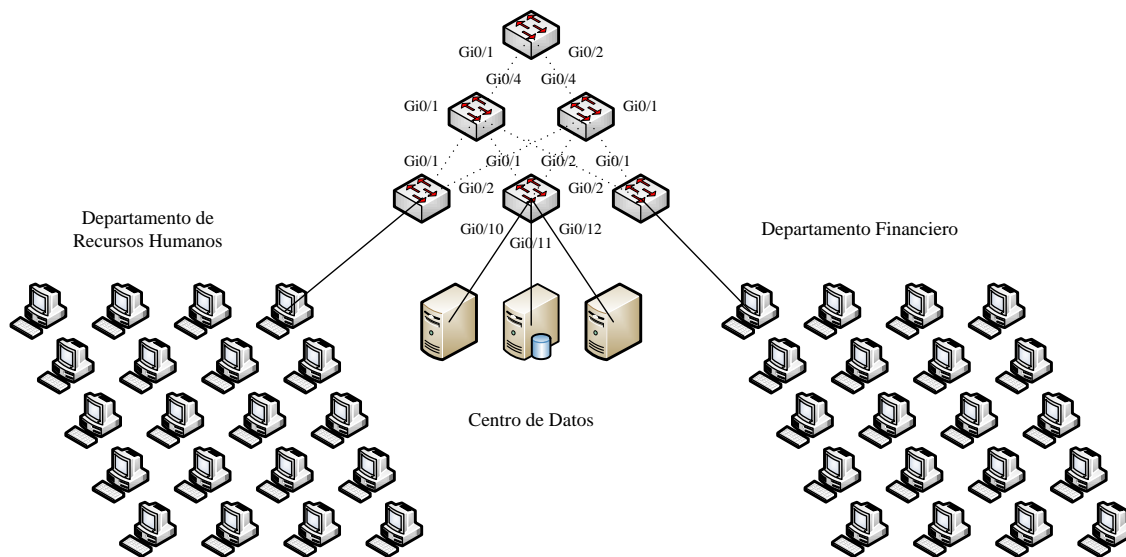


Figura 2.45: Diagrama Topológico

2.2.3.3 Modelos de Conmutadores

- **Fijos:** No se pueden añadir características a estos conmutadores y su configuración incluye el tipo y número de puertos (Figura 2.46).
- **Modulares:** Tienen chasis de diferentes tamaños que permiten la instalación de varias tarjetas modulares. Mientras más grande es el chasis, más cantidad de módulos se puede soportar (Figura 2.46).
- **Apilables:** Pueden interconectarse utilizando un cable de backplane que proporciona un alto throughput (promedio de datos que se transmiten efectivamente) entre los conmutadores que se apilan uno sobre otro. Estos conmutadores operan efectivamente en conjunto. Son preferibles cuando la tolerancia de fallas y disponibilidad de ancho de banda son críticos y un conmutador modular resulta muy costoso. Los conmutadores apilables utilizan un puerto especial para interconexiones entre conmutadores y sus velocidades son más rápidas (Figura 2.46).



Figura 2.46: Conmutadores Fijos, Modulares y Apilables

2.2.3.4 Características de los Conmutadores

- **Rendimiento:** Cuando se selecciona un conmutador es necesario considerar la densidad de puertos, tasas de transmisión y requerimientos de agregación de ancho de banda.
- **Densidad de Puertos:** Es el número de puertos disponibles en un conmutador. En la Figura 2.47 se pueden apreciar conmutadores fijos de 24 y 48 puertos con opción de hasta cuatro puertos adicionales para dispositivos SFP (Small Form-Factor Pluggable). Una alta densidad de puertos permite un mejor uso del espacio y energía. Los conmutadores modulares pueden soportar densidades de puertos muy altas añadiendo múltiples tarjetas.
- **Tasas de Transmisión:** Definen las capacidades de procesamiento de un conmutador. Las tasas de transmisión son importantes cuando se selecciona un conmutador. Si la tasa de transmisión es muy baja, no se puede alcanzar la velocidad del cable en todos los puertos (100 Mbps Fast Ethernet o 1000 Mbps Gigabit Ethernet).

- **Agregación de Enlaces:** Se debe determinar si existen puertos suficientes en un conmutador para agruparse, soportar el ancho de banda requerido y reducir los cuellos de botella.
- **PoE (Power over Ethernet):** Permite que el conmutador entregue energía a un dispositivo mediante el cableado Ethernet. Puede ser utilizada por teléfonos IP (Internet Protocol) y puntos de acceso inalámbricos.



Figura 2.47: Conmutadores de 24 y 48 Puertos Gigabit Ethernet

2.2.3.5 Características de los Conmutadores en una Red Jerárquica

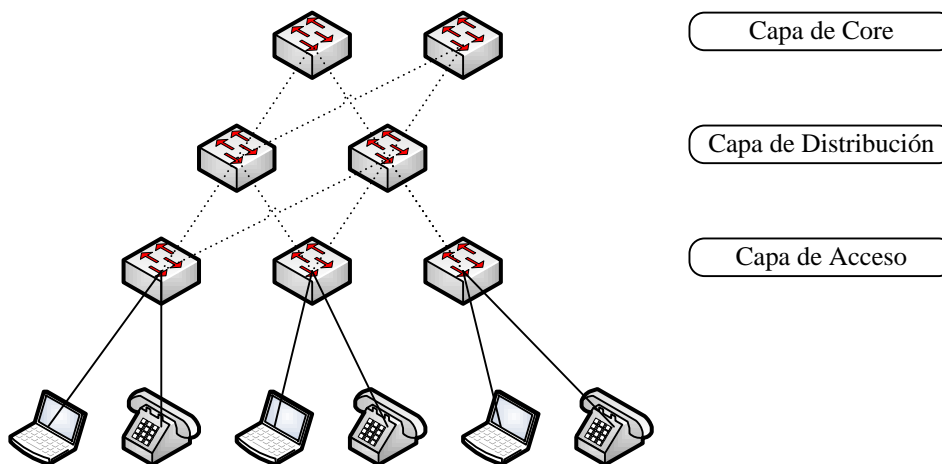


Figura 2.48 Capas de Acceso, Distribución y Core

2.2.3.5.1 Acceso

Facilitan la conexión de los dispositivos finales y deben tener seguridad de puertos, VLANs, PoE y agrupación de enlaces. La seguridad de puertos permite decidir cuáles dispositivos pueden conectarse a un conmutador. Las VLANs son un componente importante de una red convergente y el tráfico de voz se asigna a una VLAN separada.

Dependiendo de los requerimientos de la red, se escoge entre puertos Fast Ethernet o Gigabit Ethernet. PoE es un requerimiento de la Capa de Acceso que incrementa el precio de los conmutadores y debe ser considerado cuando la convergencia de voz sea necesaria, se requiera implementar puntos de acceso inalámbricos o resulte difícil ubicar un tomacorriente. La agrupación de enlaces es otra característica común para la mayoría de conmutadores de Acceso (Figura 2.48).

2.2.3.5.2 Distribución

Reúnen los datos de los conmutadores de Acceso y los envían al Core. El tráfico de Capa 2 necesita ser administrado o segmentado en VLANs para reducir el tamaño de los dominios de broadcast. Los conmutadores de Distribución proporcionan las funciones de enrutamiento inter-VLAN porque estos equipos tienen mayores capacidades de procesamiento y soportan funciones de Capa 3 (Figura 2.48).

2.2.3.5.2.1 Políticas de Seguridad

Las ACLs (Access Control Lists) controlan el flujo de tráfico en una red. Una ACL permite restringir o permitir cierto tipo de tráfico. Utilizar ACLs requiere procesamiento intenso porque el conmutador necesita revisar cada paquete y ver si coincide con una de las reglas definidas.

2.2.3.5.2.2 QoS Quality of Service

Los conmutadores de Distribución deben soportar QoS para mantener la priorización de tráfico de la Capa de Acceso. Las políticas de prioridad aseguran que las comunicaciones de audio y video tengan garantizado el ancho de banda adecuado. Estos conmutadores deben soportar redundancia. Los conmutadores de la Capa de Distribución deben soportar agrupación de enlaces. Los conmutadores de Acceso utilizan múltiples enlaces para conectarse al conmutador de Distribución para asegurar un ancho de banda adecuado y proveer tolerancia de fallas si se pierde un enlace. Los conmutadores de Distribución deben ser capaces de transmitir todo el tráfico tan rápido como sea posible al Core.

2.2.3.5.3 Core

Es el backbone de alta velocidad de la red y requiere conmutadores que manejen tasas de transmisión muy altas. La tasa de transmisión se determina realizando análisis de tráfico y de comunidades de usuario (Figura 2.48).

2.2.3.5.3.1 Agrupación de Enlaces

La Capa de Core necesita soportar agrupación de enlaces para garantizar el ancho de banda desde la Capa de Distribución. Estos conmutadores deben soportar conexiones agrupadas de 10 Gigabit Ethernet.

2.2.3.5.3.2 Redundancia

La disponibilidad de la Capa de Core es crítica, por lo que se debe implementar la mayor redundancia posible. Los conmutadores deben soportar características de redundancia de hardware, tales como fuentes de poder que puedan ser cambiadas mientras el conmutador continua operando y opciones de enfriamiento más sofisticadas.

2.2.4 Redes Ethernet/802.3

2.2.4.1 Conceptos Básicos

Las señales Ethernet se transmiten utilizando un conjunto de reglas basadas en la tecnología CSMA/CD (Carrier Sense Multiple Access/Collision Detect) para determinar cuál estación puede acceder a la red. En este método de acceso, todos los dispositivos que tienen mensajes para enviar deben escuchar antes de transmitir. Si un dispositivo detecta una señal de otro dispositivo, debe esperar cierto tiempo antes de intentar transmitir. Cuando no se detecta tráfico, un dispositivo transmite su mensaje. Durante esta transmisión, el dispositivo continúa escuchando por tráfico o colisiones.

Si la distancia entre dispositivos impide detectar las señales, uno de los dispositivos puede comenzar a transmitir al mismo tiempo. Los mensajes se propagan en el medio hasta que se destruyen (colisión). Cuando un dispositivo está escuchando puede detectar una colisión porque se produce un incremento en la amplitud de la señal. Al detectar una colisión, los dispositivos que transmiten envían una señal para que los demás dispositivos invoquen un algoritmo de backoff, el cual impide que todos los dispositivos transmitan por un periodo aleatorio y logra que las señales de colisión disminuyan. Luego que este tiempo

ha expirado, el dispositivo vuelve a escuchar antes de transmitir. El periodo aleatorio de backoff asegura que los dispositivos involucrados en la colisión no traten de enviar tráfico al mismo tiempo, caso contrario el proceso se repetiría.

2.2.4.1.1 Comunicaciones Ethernet

- **Unicast:** Una trama se envía desde un computador hacia un destino específico (emisor y receptor). Es la forma predominante de transmisión en LANs y en la Internet. HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol) y Telnet son ejemplos de unicast (Figura 2.49).
- **Broadcast:** Una trama se envía desde una dirección a las demás direcciones en la red (emisor y receptores). Es esencial cuando se envía el mismo mensaje a todos los dispositivos en la LAN. La petición que ARP (Address Resolution Protocol) envía a todos los computadores en una red es un ejemplo de broadcast (Figura 2.49).
- **Multicast:** Una trama se envía a un grupo específico de dispositivos. Las transmisiones de video y voz son ejemplos de multicast (Figura 2.49).

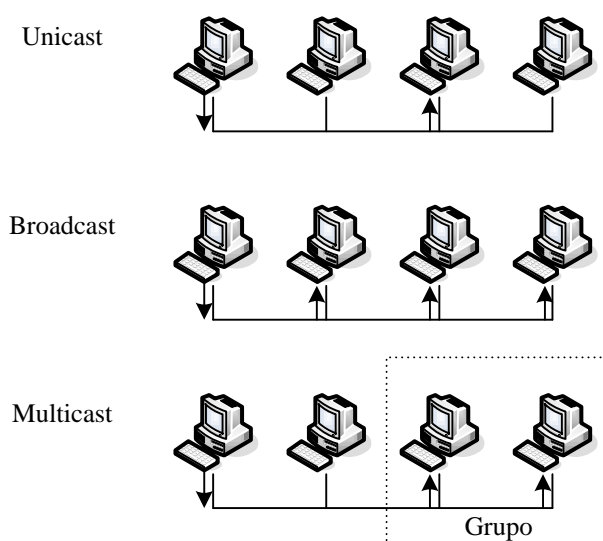


Figura 2.49: Comunicaciones Unicast, Broadcast y Multicast

2.2.4.1.2 Trama Ethernet

En la trama Ethernet se añaden encabezados y colas para encapsular el mensaje que se envía. Los campos que utiliza el protocolo Ethernet se muestran en la Figura 2.50.

IEEE 802.3						
7	1	6	6	2	46 a 1500	4
Preámbulo	SFD	Dirección Destino	Dirección Origen	Longitud/ Tipo	Encabezado y Datos	FCS

Figura 2.50: Campos de la Trama Ethernet

- **Preámbulo y SFD (Start Delimiter Frame):** El preámbulo (7 bytes) y SFD (1 byte) se utilizan para sincronización entre los dispositivos que envían y reciben.
- **Dirección MAC de Destino:** Este campo de 6 bytes es el identificador del receptor. Si existe una coincidencia entre las direcciones MAC (Media Access Control) de la trama y del dispositivo se acepta la trama.
- **Dirección MAC de Origen:** Este campo de 6 bytes identifica la NIC (Network Interface Card) que origina la trama.
- **Longitud o Tipo:** Este campo de 2 bytes define la longitud del campo de datos y se utiliza como parte del FCS (Frame Check Sequence) para asegurar que el mensaje fue recibido adecuadamente. Si el valor es igual o mayor que 0x0600 (hexadecimal) o 1536 (decimal), el contenido del campo de datos se decodifica según el protocolo indicado y si es menor que 0x0600 entonces el valor representa la longitud de los datos.
- **Datos y Relleno:** Estos campos de 46 a 1500 bytes contienen los datos encapsulados de una capa superior. Todas las tramas deben tener una longitud mínima de 64 bytes. Si se encapsula un paquete pequeño, el campo Relleno se utiliza para completar el tamaño.

- **FCS:** Este campo de 4 bytes detecta errores en una trama mediante un CRC (Cyclic Redundancy Check). Si los resultados de los cálculos entre el emisor y receptor coinciden, no existe error, caso contrario la trama se descarta.

2.2.4.1.3 Características Dúplex

- **Half Dúplex:** Se basa en el flujo de información unidireccional (envío y recepción no se realizan al mismo tiempo). Este tipo de comunicación que se ilustra en la Figura 2.51a implementa CSMA/CD para detectar y reducir las colisiones. Las conexiones half-dúplex se utilizaban en equipos antiguos.
- **Full Dúplex:** En la Figura 2.51b se observa que el flujo es bidireccional (la información se envía y recibe al mismo tiempo). Las tramas enviadas por dos nodos no colisionan, ya que se utilizan dos circuitos separados en el cable de red. La eficiencia en una configuración Ethernet con hubs es alrededor de 50 a 60% del ancho de banda de 10 Mbps. Las conexiones Fast Ethernet ofrecen una eficiencia del 100% en ambas direcciones.

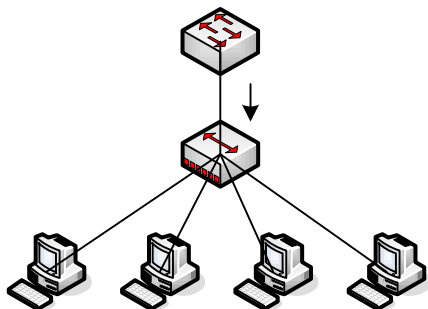


Figura 2.51a: Half Dúplex

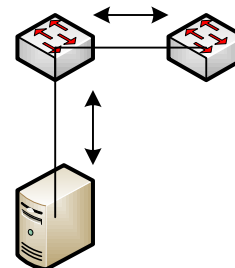


Figura 2.51b: Full Dúplex

2.2.4.1.4 Configuración de Puertos

Los puertos de un conmutador se configuran según el tipo de medio:

- **auto:** Auto negociación del modo dúplex.
- **full:** Modo full dúplex.
- **half:** Modo half dúplex.

Para los puertos Fast Ethernet y 10/100/1000 la configuración por defecto es auto y para los puertos 100BASE-FX es full.

2.2.4.1.5 Direccionamiento MAC

Los conmutadores utilizan direcciones MAC para dirigir las comunicaciones de red por el puerto apropiado. Para que un conmutador conozca por cuál puerto debe transmitir una trama unicast, necesita saber cuáles nodos están conectados en cada uno de sus puertos. Un conmutador maneja las tramas entrantes mediante su tabla de direcciones MAC, la cual se crea guardando las direcciones de los nodos que están conectados a los puertos. Cuando un conmutador recibe una trama y la dirección MAC de destino no se encuentra en la tabla, el equipo envía la trama por todos los puertos excepto por el que fue recibida. Cuando el nodo destino responde, el conmutador graba la dirección MAC en la tabla.

2.2.4.2 Consideraciones de Diseño

2.2.4.2.1 Ancho de Banda y Throughput

La mayor desventaja de las redes Ethernet/802.3 son las colisiones que ocurren cuando dos computadores transmiten simultáneamente. Cuando se produce una colisión, las tramas se destruyen. El computador que envía se abstiene de transmitir por un periodo aleatorio, de acuerdo con las reglas de CSMA/CD. Como Ethernet no puede controlar cuál dispositivo transmitirá, las colisiones ocurren cuando más de un nodo trata de acceder a la red. Conforme se añaden dispositivos al medio, la probabilidad de colisiones se incrementa. El número de nodos que comparten la red Ethernet influirá en el throughput de la red.

2.2.4.2.2 *Dominios de Colisión*

Cuando se expande una LAN Ethernet para incluir más usuarios con mayores requerimientos de ancho de banda, las colisiones se incrementan. Para reducir el número de nodos en un segmento de red, se pueden crear segmentos de red separados llamados dominios.

El área de la red donde se originan y colisionan las tramas se denomina dominio de colisión (Figura 2.52). Cuando un computador se conecta a un puerto, el conmutador crea una conexión dedicada, la cual es un dominio de colisión individual. Los conmutadores reducen las colisiones y mejoran la utilización del ancho de banda en los segmentos de red porque proveen ancho de banda dedicado para cada segmento de red.

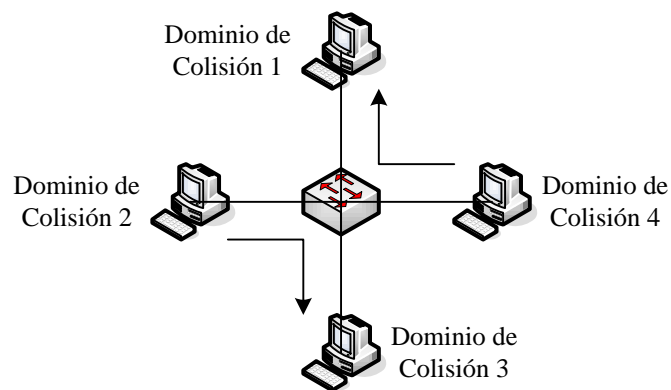


Figura 2.52: Dominios de Colisión

2.2.4.2.3 *Dominios de Broadcast*

Los conmutadores filtran las tramas según su dirección MAC, pero no filtran tramas de broadcast. Un grupo de conmutadores interconectados forma un dominio de broadcast como el de la Figura 2.53. Solamente una entidad de Capa 3 (enrutador o VLAN) delimita este dominio. Cuando un dispositivo envía un broadcast de Capa 2, la dirección MAC de destino se envía a todos los dispositivos, los cuales aceptan y procesan la trama de broadcast.

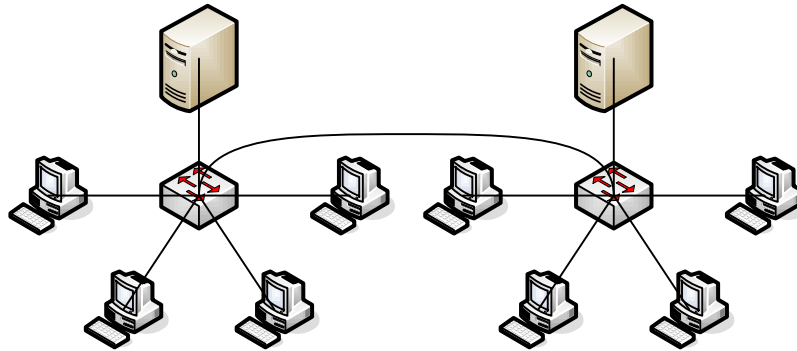


Figura 2.53: Dominio de Broadcast

2.2.4.2.4 Latencia

Es el tiempo que le toma a una trama viajar desde el origen al destino. Los usuarios de aplicaciones de red experimentan latencia cuando tienen que esperar para acceder a la información de un centro de datos o cuando se carga un sitio Web en un navegador. La latencia se origina por:

- **Retardo de la NIC:** Tiempo que les toma a la NIC de origen enviar los pulsos de voltaje por el cable y a la NIC de destino interpretar estos pulsos.
- **Retardo de Propagación:** Tiempo que le toma a la señal viajar por el cable.
- **Demora de Procesamiento:** Tiempo que les toma a los equipos de telecomunicaciones intermedios procesar los datos.

La latencia se añade dependiendo de la cantidad de dispositivos que están en la trayectoria entre dos equipos. La causa más importante de latencia en una LAN conmutada es función de la información que se transmite, los protocolos de enrutamiento y los tipos de aplicaciones.

2.2.4.2.5 Congestión

La principal razón para segmentar una LAN en partes más pequeñas es aislar el tráfico y lograr una mejor utilización del ancho de banda por usuario. Las causas principales de congestión son:

- Computadores y tecnologías de red poderosas que pueden procesar mayor cantidad de datos a altas velocidades.
- Incremento en el volumen de tráfico de red.
- Aplicaciones que requieren gran ancho de banda, tales como diseño ingenieril, VoD (Video on Demand) y aprendizaje electrónico.

2.2.4.2.6 Segmentación LAN

Las LANs se segmentan en dominios de colisión y broadcast más pequeños utilizando enrutadores y conmutadores. Aunque los conmutadores reducen el tamaño de los dominios de colisión, todos los computadores conectados al conmutador están en el mismo dominio de broadcast. Como los enrutadores no envían tráfico de broadcast, pueden utilizarse para crear dominios de broadcast, reduciendo así el tráfico de broadcast y proporcionando mayor disponibilidad de ancho de banda para comunicaciones unicast (Figura 2.54).

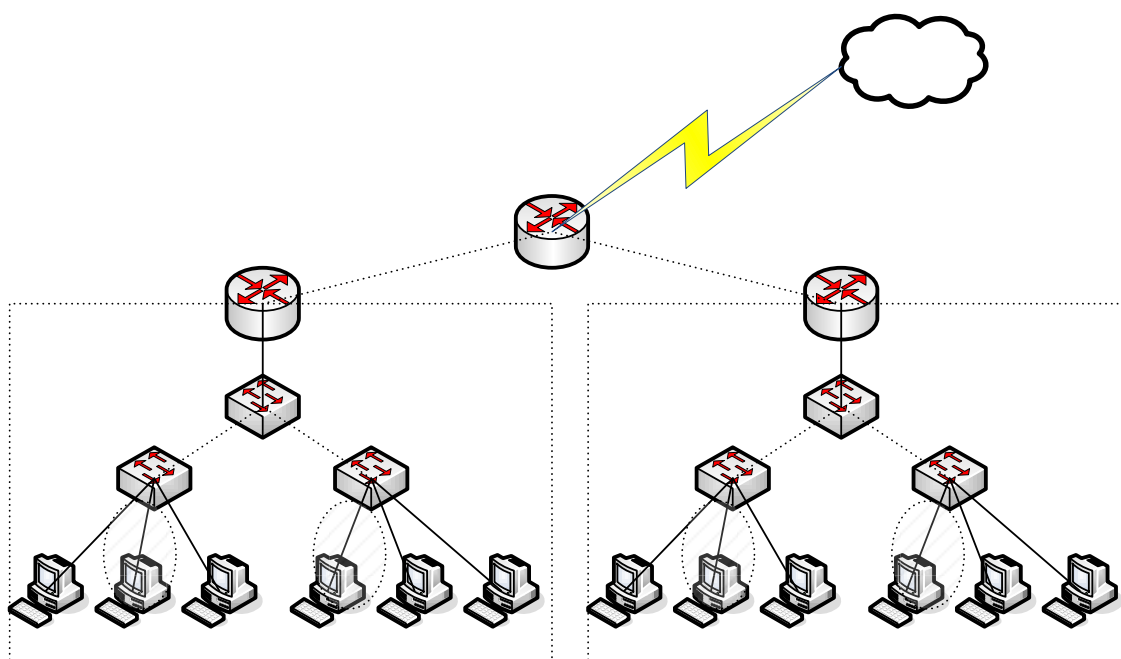


Figura 2.54: Dominios de Broadcast y Colisión Controlados

2.2.4.2.7 Controlar la Latencia de Red

Cuando se diseña una red, se debe considerar la latencia causada por cada dispositivo en la red. El uso de dispositivos de capas superiores puede incrementar la latencia en una red. Cuando un dispositivo de Capa 3 (enrutador) necesita examinar la información de direccionamiento contenida en la trama se requiere un tiempo de procesamiento mayor. Sin embargo, el uso apropiado de estos dispositivos limita el tráfico de broadcast o la tasa de colisiones.

2.2.4.2.8 Cuellos de Botella

En la Figura 2.55 se puede observar que son aquellos lugares donde la alta congestión causa un funcionamiento lento.

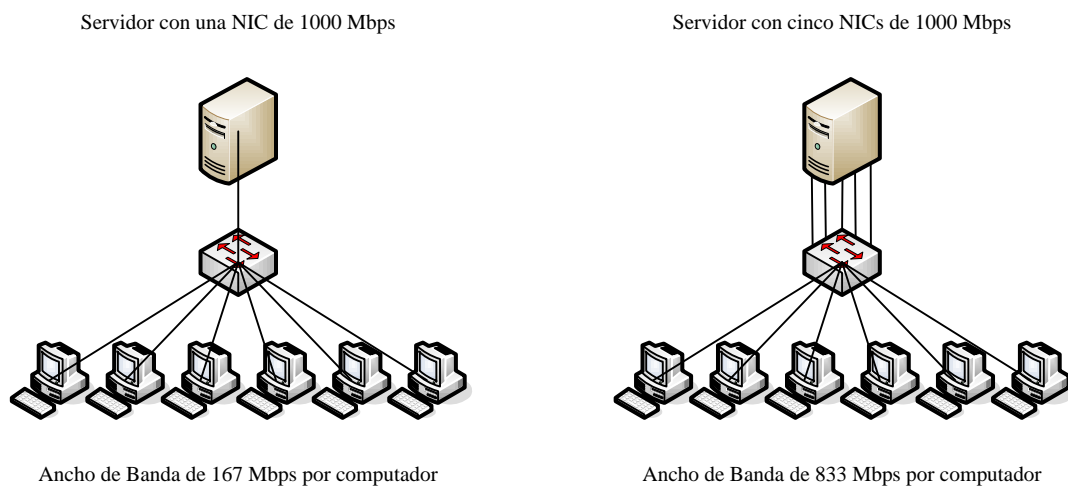


Figura 2.55: Cuellos de Botella

2.2.4.3 Métodos de Conmutación

2.2.4.3.1 Store-and-Forward

Cuando el conmutador recibe una trama, éste almacena la información en búferes hasta terminar de recibirla. Durante el proceso de almacenamiento, el conmutador analiza la trama en búsqueda de información sobre el destino. En este proceso, el conmutador realiza una comprobación de errores utilizando el CRC de la trama Ethernet, el cual utiliza una fórmula matemática para determinar si la trama tiene error. Luego de confirmar la integridad de la trama, ésta se envía por el puerto apropiado hacia su destino. Cuando se

detecta un error, el conmutador descarta la trama. Esta clase de conmutación se requiere para QoS en redes convergentes donde se necesita clasificar las tramas para priorizar el tráfico.

Los dispositivos de red que utilizan store-and-forward agregan una demora al inicio de cada enlace que se encuentra en la trayectoria del paquete. Este retardo es proporcional a la longitud de la trama en bits. Por tanto, un paquete de L bits que será transmitido por un enlace de R bps introducirá una demora de L/R segundos. Además, los paquetes experimentan retardos variables que dependen del nivel de congestión en la red.

2.2.4.3.2 Cut-Through

El conmutador procesa los datos cuando los recibe, aun cuando la transmisión no se ha completado. El conmutador almacena parte de la trama para leer la dirección MAC de destino y determinar por cuál puerto enviar la información. El conmutador revisa la dirección MAC de destino en la tabla de conmutación, determina el puerto de salida y envía la trama. El conmutador no realiza comprobación de errores en la trama. La conmutación cut-through es más rápida que la store-and-forward. Sin embargo, como el conmutador no realiza ningún control de errores, éste envía las tramas incorrectas por la red, consumiendo ancho de banda mientras son transmitidas. La NIC de destino descarta las tramas con errores.

2.2.4.3.2.1 Fast-Forward

Envía un paquete luego de identificar la dirección de destino. Como los dispositivos que utilizan este método de conmutación empiezan a transmitir antes de recibir un paquete completo, es posible que se retransmitan errores. Esta situación no ocurre con frecuencia y la NIC descarta el paquete cuando lo recibe.

2.2.4.3.2.2 Fragment-Free

Almacena los primeros 64 bytes de cada paquete antes de enviarlo, ya que la mayoría de errores y colisiones se producen en esta sección.

2.2.4.4 Tipos de Conmutación

2.2.4.4.1 Asimétrica

Permite asignar mayor ancho de banda a un puerto para prevenir cuellos de botella. De esta manera, el flujo de tráfico se mejora cuando varios clientes se comunican al mismo tiempo. En un conmutador asimétrico se requiere búferes de almacenamiento. Para que el conmutador maneje las diferentes tasas de datos en distintos puertos, éstas se almacenan y se dirigen hacia el puerto una tras otra (Figura 2.56).

2.2.4.4.2 Simétrica

En un conmutador simétrico todos los puertos tienen el mismo ancho de banda. Esta conmutación se optimiza para una carga de tráfico distribuida, como es el caso de un ambiente peer-to-peer (Figura 2.56).

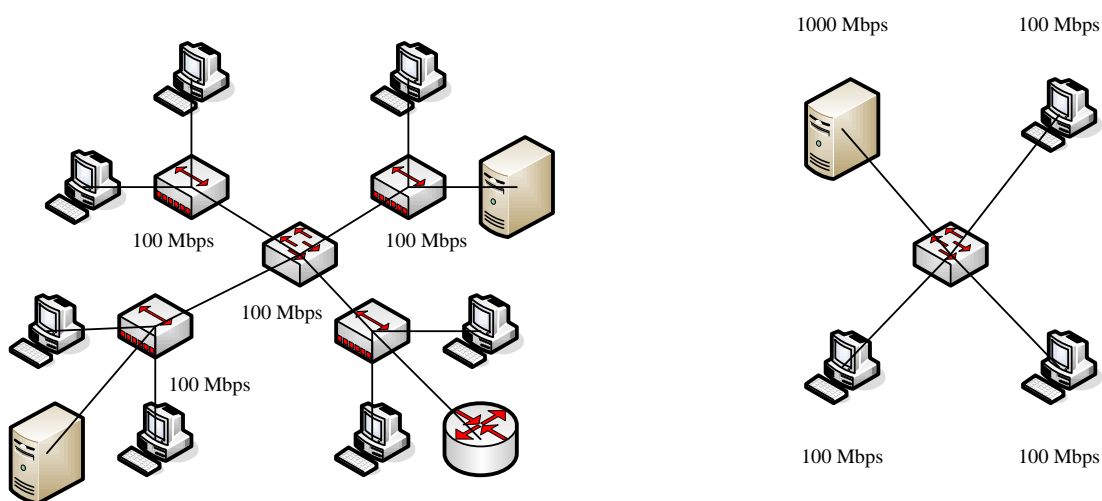


Figura 2.56: Conmutación Simétrica y Asimétrica

2.2.4.5 Búfer de Memoria

Un conmutador Ethernet utiliza esta técnica para almacenar tramas antes de enviarlas. También se utiliza cuando existe congestión en el puerto de destino y el conmutador debe almacenar la trama hasta que pueda ser transmitida.

Existen dos métodos:

- **Port based:** Las tramas se almacenan en colas asociadas a puertos específicos. Una trama se transmite al puerto de salida solo cuando todas las tramas anteriores se han transmitido exitosamente.
- **Shared:** Deposita las tramas en un búfer común que comparten todos los puertos. Las tramas en el búfer se asocian dinámicamente al puerto de destino. El conmutador mantiene un registro de las asociaciones trama-puerto que muestran a dónde debe transmitirse un paquete.

2.2.4.6 Conmutación de Capa 2 y Capa 3

Un conmutador de Capa 2 opera en base a la dirección MAC y es transparente para los protocolos de red y las aplicaciones de usuario. En tanto que un conmutador de Capa 3 utiliza direcciones IP para tomar decisiones. Los conmutadores de Capa 3 pueden realizar funciones de enrutamiento, reduciendo así la necesidad de enrutadores en una LAN.

2.2.5 Elección del Fabricante

Cisco se ha constituido como líder en áreas tales como enrutamiento y conmutación, comunicaciones unificadas, movilidad y seguridad. Además se caracteriza por ser una compañía innovadora que desarrolla la mayoría de sus productos internamente y participa en grupos interesados en estándares para redes informáticas. Para garantizar la satisfacción de los clientes, Cisco ofrece asistencia técnica en línea y soporte telefónico las 24 horas del día y durante los 365 días del año. Los programas de certificación permiten que los ingenieros contribuyan con soluciones de calidad.

Dado que la compañía considera a una red como un todo, diseña y desarrolla productos y tecnologías para proporcionar grandes beneficios. Cisco dispone de una gama de conmutadores que robustecen, simplifican y extienden el valor de la infraestructura de red. Algunas de sus innovaciones se han convertido en estándares de industria que incluyen EtherChannel, Power over Ethernet y Multiple Instance Spanning Tree. Todos estos aspectos justifican haber elegido a Cisco como la mejor opción para el diseño de una red jerárquica conmutada.

2.2.6 Cisco IOS (Internetwork Operating System)

Es el sistema operativo de los dispositivos Cisco que administra los recursos de hardware y software de un equipo, tales como asignación de memoria, procesos, seguridad y archivos de configuración. Una imagen de IOS representa un archivo que tiene el sistema operativo de un dispositivo. Este fabricante desarrolla varios tipos de imágenes según el modelo y características de un equipo. Para acceder a los servicios se emplea la CLI (Command Line Interface). El tamaño del archivo del IOS está en el orden de los megabytes y se almacena en una memoria no volátil (el contenido no se borra cuando el equipo se desconecta) denominada flash. Los archivos de configuración contienen los comandos utilizados para personalizar las funcionalidades de un dispositivo. Existen dos tipos de archivos de configuración:

- **running-config:** Se utiliza durante la operación de un dispositivo, los cambios de configuración se aplican de manera inmediata y se guarda en la RAM (Random Access Memory).
- **startup-config:** Se emplea como respaldo, carga cuando se enciende el equipo y se almacena en la NVRAM (Non-Volatile Random Access Memory).

2.2.7 CLI (Command Line Interface)

De aquí en adelante se utilizará letra tipo Courier New de tamaño 10 para especificar los comandos, cuya sintaxis incluye el comando y las palabras clave o argumentos. El texto con negrita se empleará para aquellos comandos que deban ser ingresados literalmente. Los argumentos que requieran ser agregados por el usuario se indicarán con cursiva. Los corchetes encerrarán elementos opcionales y una línea vertical separará las alternativas disponibles. El modo de operación podrá ser reconocido a través de un par de paréntesis.

2.2.7.1 Modos

2.2.7.1.1 Usuario

Es el modo por defecto que permite acceder a comandos básicos de monitoreo y se lo identifica por el signo ">".

2.2.7.1.2 *Privilegio*

Permite acceder a todos los comandos, puede protegerse con una contraseña y se lo reconoce por el signo “#”. Para cambiar entre los modos de usuario y privilegio se ingresan los comandos **enable** y **disable**. En este nivel se puede acceder a otros modos de configuración, los cuales tienen comandos específicos según la operación.

2.2.7.1.3 *Configuración*

2.2.7.1.3.1 Global

Se utiliza para configurar parámetros globales en un conmutador, tales como el nombre o la dirección IP. Para acceder a este modo se ingresa el comando **configure terminal** y se lo distingue por “(config)#”.

2.2.7.1.3.2 Interfaz

Para acceder a este modo se ingresa el comando **interface nombre de la interfaz**, se lo distingue por “(config-if)#” y para salir se utiliza el comando **exit**.

2.2.7.2 *Ayuda*

2.2.7.2.1 *Palabras*

En caso de recordar parte de un comando se ingresa la secuencia de caracteres seguida de un signo de interrogación (?) sin incluir espacios en blanco.

2.2.7.2.2 *Sintaxis de Comandos*

Cuando se desconocen los comandos o parámetros se recurre al comando “?”. Si se ingresa después de un comando específico, se despliegan sus argumentos.

2.2.7.2.3 *Mensajes de Error*

Ayudan a identificar problemas cuando se ingresa un comando incorrecto.

2.2.7.2.4 *Historial de Comandos*

La interfaz de línea de comandos tiene un historial de los comandos que han sido ingresados y ayuda a recordar comandos extensos o complicados. Esta opción permite

mostrar el contenido del búfer de comandos, establecer el tamaño del historial de comandos y recordar comandos ingresados anteriormente. El historial de comandos está habilitado por defecto y el sistema almacena las diez últimas líneas. Se puede utilizar el comando `show history` para ver los comandos ingresados recientemente. El historial de comandos puede deshabilitarse mediante el comando `terminal no history`.

2.2.7.3 Secuencia de Booteo

Después que un conmutador se enciende, éste carga el software boot loader que está almacenado en NVRAM (Non-Volatile Random Access Memory), el cual:

- Realiza la inicialización de la CPU (Central Processing Unit) a bajo nivel e inicializa los registros que controlan la memoria física, la cantidad de memoria y la velocidad.
- Realiza el POST (Power-On Self Test) para el subsistema de la CPU.
- Prueba la DRAM (Dynamic Random-Access Memory) y el sistema de archivos flash.
- Carga la imagen de un software de sistema operativo en la memoria y bootea el conmutador.

Luego, el sistema operativo inicializa las interfaces utilizando los comandos del archivo de configuración (`config.text`) que está almacenado en la memoria flash.

2.2.7.4 Configuración Básica

La configuración inicial de un conmutador debe cumplir los siguientes pasos:

- Antes de encender el conmutador es necesario verificar que todas las conexiones sean seguras, el computador se encuentre conectado al puerto de consola y la aplicación de emulación de terminal (HyperTerminal) se encuentre corriendo y haya sido configurada correctamente (Figuras 2.57 y 2.58).
- Conectar el cable de poder al conmutador para que se encienda.
- Observar la secuencia de booteo.



Figura 2.57: Conexión al Conmutador

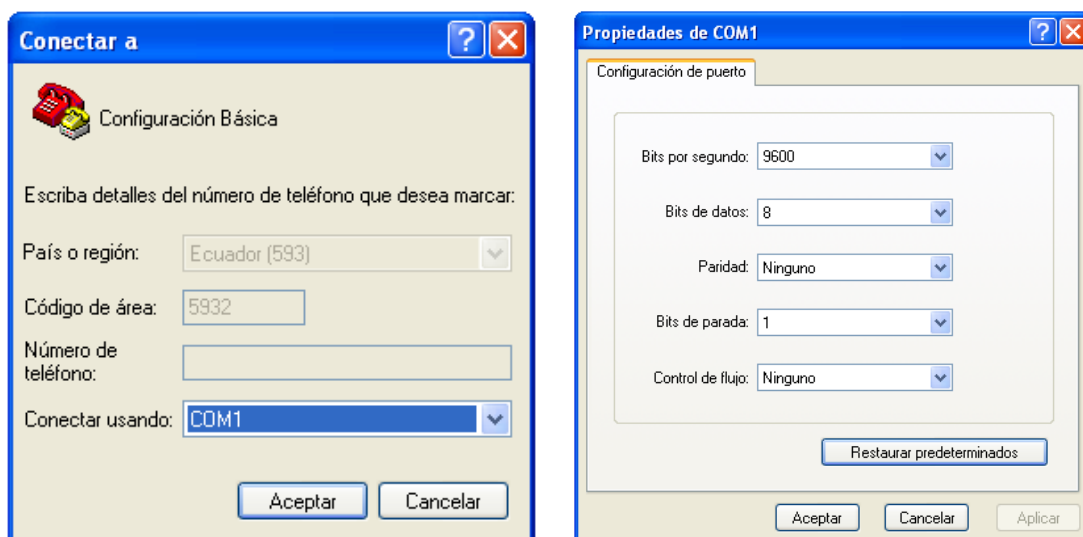


Figura 2.58: Configuración de HyperTerminal

2.2.7.5 Administración Básica

La running-config se almacena en DRAM y la startup-config en la sección NVRAM de la memoria flash. Cuando se ejecuta el comando `copy running-config startup-config`, el software copia la running-config a la NVRAM para que cuando el conmutador se encienda, la nueva configuración se cargue.

2.2.7.5.1 Respaldo de Configuración

Para tener múltiples archivos startup-config en un conmutador se puede copiar la configuración con nombres diferentes, utilizando el comando `copy startup-config flash:nombre del archivo`. El software tiene un cliente TFTP incorporado que permite conectarse a un servidor TFTP en una red. Para cargar un archivo de configuración en un servidor TFTP se debe:

- Verificar que el servidor TFTP está corriendo en la red.
- Conectarse al conmutador a través del puerto de consola o una sesión Telnet, habilitar el conmutador y hacer ping al servidor TFTP.
- Cargar la configuración del conmutador al servidor TFTP y especificar la dirección IP del servidor TFTP y el nombre del archivo de destino con el comando: `#copy system:running-config tftp:[[/ubicación]/directorio]/nombre del archivo` o `#copy nvram:startup-config tftp:[[/ubicación]/directorio]/nombre del archivo`.

2.2.7.5.2 Restauración de Configuración

Una vez que la configuración ha sido almacenada exitosamente en el servidor TFTP, se puede copiarla en el conmutador de la siguiente manera:

- Copiar el archivo de configuración en el servidor TFTP.
- Verificar que el servidor TFTP esté corriendo en la red.
- Conectarse al conmutador a través del puerto de consola o sesión Telnet, habilitar el conmutador y hacer ping al servidor TFTP.
- Descargar el archivo de configuración desde el servidor TFTP y especificar la dirección IP del servidor TFTP y el nombre del archivo a descargar con el comando: `#copy tftp:[[/ubicación]/directorio]/nombre del archivo system:running-config` o `#copy tftp:[[/ubicación]/directorio]/nombre del archivo nvram:startup-config`.

2.2.7.5.3 Borrar la Configuración

Se utiliza el comando `erase nvram: o erase startup-config`. Para borrar un archivo de la memoria flash se emplea el comando `delete flash:nombre del archivo`.

2.2.7.6 Seguridad Básica

2.2.7.6.1 Acceso a la Consola

Para proteger el puerto de consola se establece una contraseña utilizando el comando `password contraseña`. Para ingresar al modo de configuración de línea para la consola 0

se digita el comando `line console 0`. Para asegurar que un usuario ingrese la contraseña, se incluye el comando `login`.

2.2.7.6.2 Puertos vty

Para establecer una contraseña se ingresa al modo de configuración de línea con el comando `line vty 0 4`, ya que es posible ejecuta varias sesiones de forma simultánea.

2.2.7.6.3 Modo de Ejecución

El comando `enable password` permite especificar una contraseña para restringir el acceso al modo de privilegio. La forma encriptada de esta contraseña utiliza el algoritmo MD5 (Message Digest 5) y se asigna con el comando `enable secret`.

2.2.7.6.4 Encriptación

Por defecto todas las contraseñas se almacenan en texto en claro. Con el comando `service password-encryption` todas las contraseñas del sistema se encriptan utilizando el algoritmo Vigenere.

2.2.7.6.5 Mensaje de Registro

Se muestra antes que el dispositivo solicite el nombre de usuario y contraseña. El comando que se utiliza es `banner login` seguido del texto entre comillas.

2.2.7.6.6 Mensaje del Día

Es útil para enviar mensajes que afectan a todos los usuarios de una red. Se muestra antes que el mensaje de registro. Para configurar este mensaje se ingresa el comando `banner motd` junto con el texto entre comillas.

2.2.7.7 Telnet y SSH

2.2.7.7.1 Telnet

Es un protocolo muy conocido que se utiliza para acceso a dispositivos de red. Sin embargo, es inseguro porque envía las comunicaciones en texto en claro. La dirección IP de administración que se asigna a un conmutador permite establecer una conexión utilizando un cliente Telnet.

2.2.7.7.2 SSH

La comunicación entre el cliente y el servidor SSH está encriptada. Es recomendable implementar la versión 2 porque utiliza un algoritmo de encriptación mejorado. Esta opción tiene un servidor y cliente SSH integrado. Este protocolo soporta los algoritmos DES (Data Encryption Standard), 3DES (Triple DES) y autenticación basada en contraseña. Para implementar SSH es necesario generar llaves RSA (Ron Rivest, Adi Shamir & Leonard Adleman), una pública para el servidor y otra privada tanto para el emisor como para el receptor. La primera sirve para encriptar los mensajes y la segunda permite descryptarlos. Para crear estas llaves se utiliza el comando `crypto key generate rsa`. Si se configura un conmutador como servidor SSH es necesario especificar un nombre y dominio con los comandos `hostname nombre del conmutador` e `ip domain-name nombre del dominio`, respectivamente. Para borrar un par de llaves RSA se utiliza el comando `crypto key zeroize rsa`.

2.2.7.7.2.1 Configuración del Servidor

- Especificar la versión de SSH mediante el comando `ip ssh version [1 | 2]`.
- Configurar los parámetros de control SSH utilizando el comando `ip ssh {timeoutseconds | authentication-retriesnumber}`:
- Establecer el valor de time-out (duración de una conexión) entre 0 y 120 segundos.
- Especificar el número de veces que un cliente puede re-autenticarse con el servidor entre 0 y 5.
- Para prevenir otro tipo de conexión distinta a SSH se utiliza el comando `transport input ssh`.

2.2.7.8 Seguridad de Puertos

Limita el número de direcciones MAC permitidas en un puerto. Si se configura un puerto seguro y se alcanza el número máximo de direcciones MAC ocurre una violación de seguridad. Existen tres formas de configuración para direcciones MAC seguras:

2.2.7.8.1 Estáticas

Se configuran con el comando `switchport port-security mac-address dirección MAC`.

2.2.7.8.2 Dinámicas

Se aprenden y almacenan dinámicamente en la tabla de direcciones.

2.2.7.8.3 Sticky

Se aprenden dinámicamente y se almacenan en la running-config utilizando el comando `switchport port-security mac-address sticky`.

Estos mecanismos evitan que ocurran ataques tales como inundación de direcciones MAC, falsificación, intrusión, etc. El primero consiste en llenar la tabla MAC con direcciones de origen falsas para que un conmutador actúe como un concentrador y envíe paquetes a todos los equipos en la red. Un servidor DHCP falso puede responder a los pedidos de los clientes entregando la dirección IP del espía como puerta de enlace predeterminada e interceptar el flujo de información. Por último, un computador intruso puede solicitar continuamente direcciones IP a un servidor DHCP real cambiando su dirección MAC para que ninguno de los usuarios reales obtenga los datos de configuración.

2.2.7.9 Modos de Violación de Seguridad

Una interfaz se puede configurar en uno de los siguientes modos:

2.2.7.9.1 Proteger

Cuando el número de direcciones MAC sobrepasa el límite permitido, los paquetes con procedencia desconocida se descartan y no se produce una notificación al respecto.

2.2.7.9.2 Restringir

Es similar al modo anterior con la diferencia de que se envía una notificación SNMP.

2.2.7.9.3 Apagar

La interfaz se apaga y se envía una notificación SNMP.

La Tabla 2.1 muestra el tipo de tráfico que se envía dependiendo del modo de violación configurado.

Modo de Violación	Transmite Tráfico	Envía Mensajes Syslog	Muestra Mensajes de Error	Incrementa el Contador de Violaciones	Apaga el Puerto
Proteger	No	Sí	No	Sí	No
Restringir	No	No	No	No	No
Apagar	No	Sí	No	Sí	Sí

Tabla 2.1: Tipo de Tráfico según Modo de Violación

2.2.7.10 Puertos No Utilizados

Para proteger una red de acceso no autorizado se pueden deshabilitar todos los puertos no utilizados.

2.2.8 VLAN

Una VLAN (Virtual Local Area Network) reduce un dominio de broadcast mediante la creación de redes lógicas dentro de una misma red física, limita la cantidad de dispositivos participantes y permite agruparlos según su función o distribución geográfica (Figura 2.59).

2.2.8.1 Beneficios

- **Seguridad:** Aquellos grupos que manejan información sensible pueden separarse para reducir vulnerabilidades.
- **Reducción de Costos:** Existe un ahorro económico pues no se requieren actualizaciones costosas y se utiliza eficientemente el ancho de banda disponible y los enlaces.
- **Mejor Desempeño:** Al dividir redes de Capa 2 en grupos de trabajo lógicos se reduce el tráfico innecesario en la red y se potencia el funcionamiento.
- **Disminuir el Broadcast:** Cuando se divide una red en VLANs se reduce la cantidad de dispositivos involucrados en una tormenta de broadcast.
- **Mejora el Desempeño del Personal de IT (Information Technology):** Las VLANs permiten administrar la red con mayor facilidad pues los usuarios que

tienen iguales necesidades comparten la misma VLAN. El personal de IT puede identificar la función de una VLAN a través de su nombre.

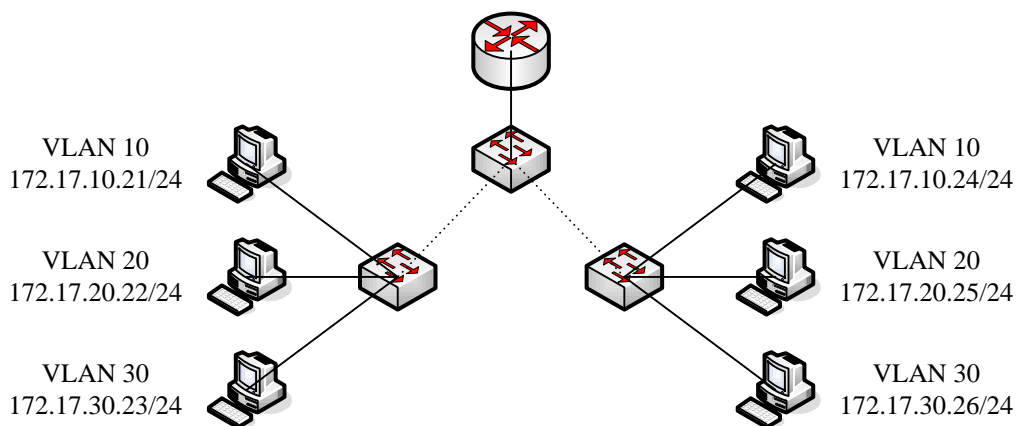


Figura 2.59: VLANs

2.2.8.2 Rangos

2.2.8.2.1 Normal

Se las utiliza en pequeñas y medianas empresas y están identificadas por un número entre 1 y 1005. El intervalo 1002-1005 está reservado para VLANs Token Ring y FDDI (Fiber Distributed Data Interface). Los identificadores 1 y 1002 a 1005 se crean automáticamente y no pueden ser borrados. Las configuraciones se guardan en una base de datos denominada `vlan.dat` (memoria flash). El protocolo VTP (VLAN Trunking Protocol) ayuda en la administración de las configuraciones entre conmutadores y solamente aprende VLANs de este rango.

2.2.8.2.2 Extendido

Se las identifica mediante un número entre 1006 y 4094. Permiten ampliar la infraestructura a un mayor número de usuarios, pero tienen menos funcionalidades que las VLANs de rango normal. Se guardan en el archivo `running-config` y el protocolo VTP no aprende estas VLANs.

2.2.8.3 Tipos

2.2.8.3.1 Datos

Se configura para transportar el tráfico generado por los usuarios. Es conveniente separar el tráfico de voz y administración de los datos.

2.2.8.3.2 Defecto

Todos los puertos de un conmutador pertenecen a la VLAN 1 cuando el dispositivo se enciende por primera vez. Esta VLAN no puede ser renombrada o borrada.

2.2.8.3.3 Nativa

Se asigna a un puerto troncal 802.1Q, el cual admite tráfico de varias VLANs (tráfico etiquetado) así como tráfico que no se origina en una VLAN (tráfico no etiquetado).

2.2.8.3.4 Administrativa

Es la VLAN configurada para acceder a las opciones de administración de un conmutador. Se debe asignarle una dirección IP y máscara de subred. Un conmutador puede ser administrado a través de HTTP, Telnet, SSH (Secure Shell) o SNMP (Simple Network Management Protocol).

2.2.8.4 Tipos de Tráfico de Red

2.2.8.4.1 Telefonía IP

- **Señalización:** Se ocupa del establecimiento, duración y terminación de llamadas en la red.
- **Voz:** Son los paquetes de datos de la conversación.

2.2.8.4.2 Multicast IP

Es el tráfico enviado desde una dirección de origen hacia un grupo multicast identificado por un conjunto de direcciones IP y MAC de destino.

2.2.8.4.3 *Datos*

Consiste en la creación y almacenamiento de archivos, servicios de impresión, acceso a correo electrónico y otras aplicaciones.

2.2.8.4.4 *Scavenger*

Proporciona servicios de menor calidad. Esta clase de aplicaciones no influye en los procesos de una empresa y están relacionadas con entretenimiento (peer-to-peer, juegos y videos).

2.2.8.5 **Puertos de un Conmutador**

Son interfaces de Capa 2 asociadas a un puerto físico y se utilizan para administrar la interfaz física y los protocolos de Capa 2.

2.2.8.5.1 *Modos*

Cuando se configura una VLAN es necesario asignar un número de identificación y nombre. Un puerto puede ser configurado para admitir los siguientes tipos de VLAN (Figura 2.60):

- **Estática:** Los puertos se asignan manualmente a una VLAN. Al asignar una interfaz a una VLAN que no existe, ésta se crea automáticamente.
- **Dinámica:** Este modo no se utiliza en redes que se encuentran en producción. La membresía dinámica se configura utilizando un servidor denominado VMPS (VLAN Membership Policy Server) que asigna puertos dinámicamente en base a la dirección MAC del dispositivo conectado a un puerto. Es conveniente cuando se cambia un terminal de un conmutador a otro, pues el puerto se asigna a la VLAN adecuada.
- **Voz:** Un puerto se configura en este modo para que admita un teléfono IP. Antes de configurar una VLAN de voz en un puerto se debe crear una VLAN para voz y otra para datos.

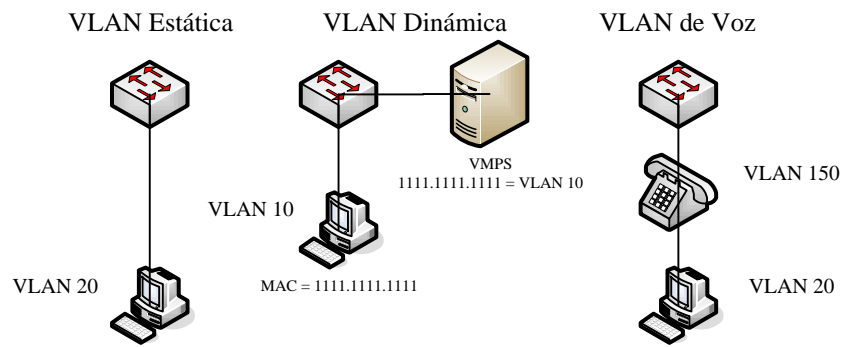


Figura 2.60: Tipos de VLAN

2.2.8.6 Troncales

Una troncal es un enlace punto a punto entre una o más interfaces Ethernet de un conmutador y otro dispositivo de red. La Figura 2.61 ilustra cómo los puertos troncales transportan el tráfico de varias VLANs por un solo enlace.

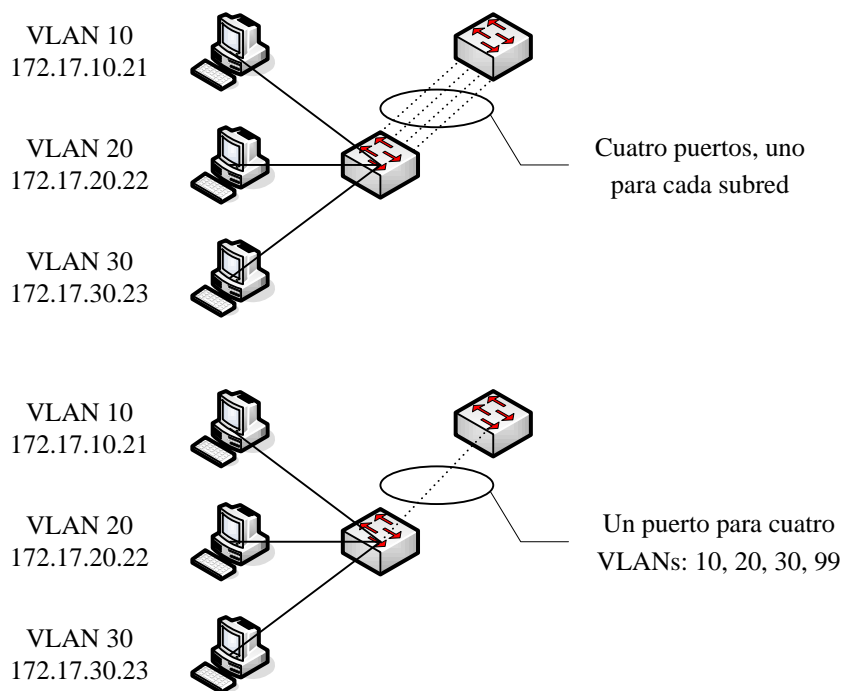


Figura 2.61: Enlace Troncal

2.2.8.6.1 *Etiquetamiento 802.1q*

Los conmutadores son dispositivos de Capa 2 que utilizan la información del encabezado de la trama Ethernet para transmitir paquetes. Dicho encabezado no contiene información sobre la VLAN a la cual pertenece la trama. Este método de identificación estándar añade una etiqueta a la trama Ethernet que especifica la VLAN a la cual pertenece y permite la operación entre equipos de varios fabricantes (Figura 2.62).

IEEE 802.3							
7	1	6	6	4	2	46 a 1500	4
Preámbulo	SFD	Dirección Destino	Dirección Origen	Etiqueta 802.1q	Longitud/ Tipo	Encabezado y Datos	FCS

Figura 2.62: Etiqueta 802.1q en la Trama Ethernet

2.2.8.6.2 *Etiquetamiento de tramas VLAN*

Cuando un conmutador recibe una trama en un puerto de acceso, el conmutador separa la trama e inserta una etiqueta VLAN, recalcula el FCS y envía la trama por un puerto troncal.

2.2.8.6.3 *Campos de la etiqueta VLAN*

2.2.8.6.3.1 Tipo Ether

Tiene el valor hexadecimal 0x8100 denominado TPID (Tag Protocol ID). Con este valor el conmutador que recibe la trama busca la información en el campo de información de control de la etiqueta (Figura 2.63).

2.2.8.6.3.2 Información de Control de la Etiqueta

- **3 bits de prioridad de usuario:** Se utilizan por el estándar 802.1p que especifica como transmitir tramas de Capa 2.
- **1 bit de CFI (Canonical Format Identifier):** Permite que las tramas Token Ring sean transportadas a través de los enlaces Ethernet.

- **12 bits de VID (VLAN ID):** Número de identificación de una VLAN que admite hasta 4096 identificadores.

2.2.8.6.3.3 FCS

Luego que el conmutador inserta los campos anteriores, éste recalcula los valores FCS y los inserta en la trama. En la actualidad se utiliza 802.1Q, pero algunas redes antiguas utilizan ISL (Inter-Switch Link). Un puerto troncal 802.1Q admite tráfico etiquetado y no etiquetado. A un puerto troncal 802.1Q se le asigna un PVID y el tráfico no etiquetado viaja por el puerto con el mismo nombre. Un paquete con la misma identificación que el puerto de salida se envía sin etiqueta. El resto del tráfico se envía con una etiqueta VLAN. Todos los paquetes que se transmiten y reciben por un puerto troncal ISL tienen un encabezado ISL. Las tramas sin etiqueta recibidas en un puerto troncal ISL se descartan (Figura 2.63).

6	Dirección de Destino
6	Dirección de Origen
2	Tipo Ether = 0x8100
2	Información de Control de la Etiqueta
2	Prioridad de Usuario
	Datos
4	Relleno
	FCS

Figura 2.63: Campos de la Etiqueta VLAN

2.2.8.6.4 DTP (Dynamic Trunking Protocol)

Se habilita automáticamente en un puerto de un conmutador cuando se configuran varios modos troncales. DTP administra la negociación troncal solo si ambos conmutadores están configurados en un modo troncal que admita DTP. Se puede apagar DTP para que el puerto local no envíe tramas DTP al puerto remoto utilizando el comando `switchport nonegotiate`.

2.2.8.6.5 Modos de Troncalización

El modo de troncalización define la forma en que DTP negocia para establecer un enlace troncal según la Tabla 2.2.

- **On:** El comando `switchport mode trunk` ocasiona que el puerto local anuncie al remoto que está cambiando a un estado de troncalización.
- **Dynamic auto:** El comando `switchport mode dynamic auto` hace que el puerto local anuncie al remoto que puede troncalizar pero no solicita que cambie al estado de troncalización. Luego de una negociación DTP, el puerto local se encuentra en el estado de troncalización solamente si el modo de troncalización del puerto remoto se ha configurado para estar en on o desirable. Si los puertos de dos conmutadores se configuran en auto, no negocian un estado de troncalización.
- **Dynamic Desirable:** El comando `switchport mode dynamic desirable` permite que el puerto local anuncie al remoto que puede troncalizar y le solicita que se cambie al modo de troncalización. Si el puerto local detecta que el remoto se configuró en el modo on, desirable o auto, el puerto local se cambia al modo de troncalización. Si el puerto remoto está en el modo nonegotiate, el puerto local se mantiene como puerto no troncalizable.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Acceso	Troncal	Troncal	Acceso
Dynamic Desirable	Troncal	Troncal	Troncal	Acceso
Trunk	Troncal	Troncal	Troncal	No Recomendado
Access	Acceso	Acceso	No Recomendado	Acceso

Tabla 2.2: Interacciones DTP

2.2.8.7 Configuración

2.2.8.7.1 Añadir una VLAN

Los comandos utilizados para añadir una VLAN a un conmutador son:

```
(config)#vlan identificador de la vlan
```

```
(config-vlan)#name nombre de la vlan
```

2.2.8.7.2 Asignar un Puerto

Luego de crear una VLAN se le asigna uno o más puertos. Cuando se asigna manualmente un puerto a una VLAN se lo conoce como puerto de acceso estático. Los comandos que se emplean son:

```
(config)#interface identificador de la interfaz
(config-if)#switchport mode access
(config-if)#switchport access vlan identificador de la interfaz
```

2.2.8.8 Administración

El comando **show vlan summary** muestra el número de VLANs configuradas.

2.2.8.8.1 Reasignación de Puertos

Un puerto de acceso estático puede pertenecer a una sola VLAN. Cuando se reasigna un puerto de acceso estático a una VLAN existente, el puerto se remueve automáticamente.

2.2.8.8.2 Borrar una VLAN

El archivo `vlan.dat` se puede borrar con el comando **delete flash:vlan.dat**. Cuando el conmutador se reinicie, las VLANs configuradas anteriormente ya no estarán. Antes de borrar una VLAN con el comando **no vlan** *identificador de la vlan* se debe reasignar todos los puertos a otra VLAN. Cualquier puerto que no se mueva a una VLAN activa no podrá comunicarse con otras estaciones después de borrar la VLAN.

2.2.8.8.3 Puerto Troncal 802.1Q

Para configurar un puerto troncal se utiliza el comando **switchport mode trunk**. Los comandos para especificar una VLAN nativa son:

```
(config)#interface identificador de la interfaz
(config-if)#switchport mode trunk
(config-if)#switchport trunk native vlan identificador de la vlan
(config-if)#switchport trunk allowed vlan add lista de vlans
(config-if)#end
```

Para verificar la configuración de un puerto se utiliza el comando **show interfaces** *identificador de la interfaz* **switchport**. A continuación se muestran los comandos para cambiar las VLANs permitidas y la VLAN nativa al estado de defecto. También se muestra el comando para cambiar un puerto troncal a uno de acceso.

```
(config-if)#no switchport trunk allowed vlan
(config-if)#no switchport trunk native vlan
(config-if)#switchport mode access
```

2.2.9 VTP

Permite que un administrador de redes configure un conmutador para que propague la configuración VLAN a otros conmutadores en la red. VTP solamente aprende VLANs de rango normal. Un conmutador puede configurarse como servidor o cliente. El servidor VTP distribuye y sincroniza la información VLAN a los conmutadores que tienen habilitado VTP como se muestra en la Figura 2.64.

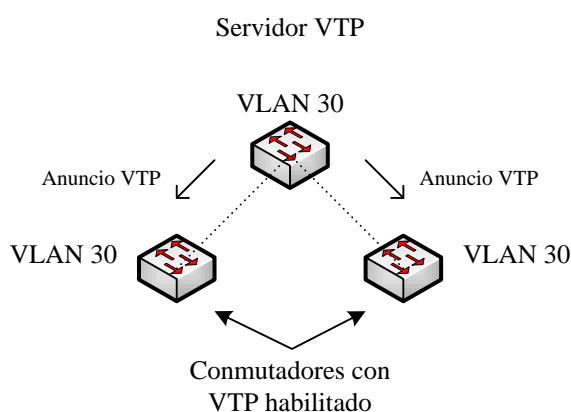


Figura 2.64: Funcionamiento VTP

2.2.9.1 Beneficios

VTP mantiene la consistencia en la configuración VLAN administrando la creación, eliminación y renombramiento de VLANs en varios conmutadores en una red. Los beneficios VTP incluyen: consistencia en la configuración VLAN, rastreo y monitoreo de VLANs, reporte dinámico de las VLANs añadidas y configuración dinámica de troncales cuando se añaden VLANs.

2.2.9.2 Componentes

2.1.9.2.1 Dominio

VTP permite separar una red en dominios más pequeños para reducir la administración de VLANs. Un dominio VTP limita la extensión de propagación de los cambios de configuración en la red. Un dominio VTP consiste en uno o varios conmutadores interconectados que comparten el mismo nombre como se puede apreciar en la Figura

2.65. Antes de crear o modificar VLANs en un servidor VTP se debe especificar el dominio VTP. Para que un servidor o cliente VTP participe en una red, éste debe formar parte del mismo dominio de lo contrario no intercambia mensajes VTP.

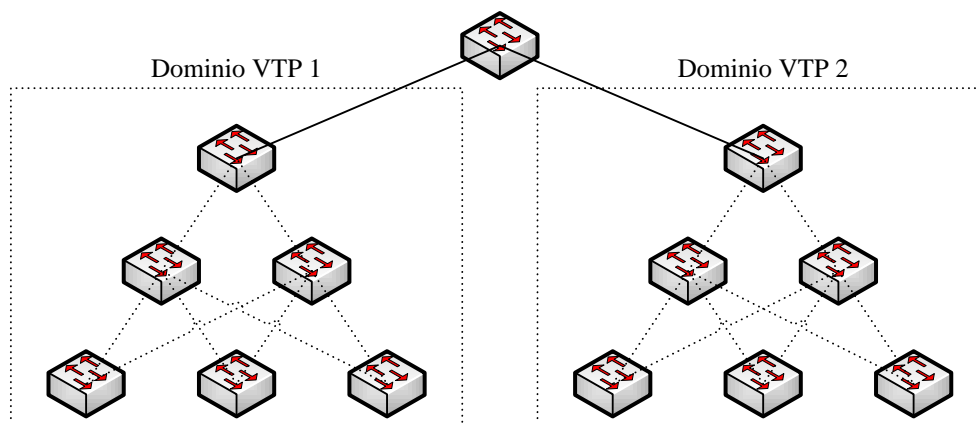


Figura 2.65: Dominios VTP

2.1.9.2.2 Anuncios

VTP utiliza los anuncios para distribuir y sincronizar la información sobre la configuración de los dominios y VLANs (Figura 2.66). Existen tres anuncios VTP y cada uno envía información sobre varios parámetros.

- **Resumen:** Contiene el nombre de dominio VTP, número de revisión actual y otros detalles de la configuración. Estos anuncios se envían cada 5 minutos por un servidor o cliente VTP para informar el número de revisión de configuración para el dominio y luego de haber realizado una configuración.
- **Subset:** Contiene la información VLAN y se produce cuando se crea o borra, suspende, activa o cambia el nombre o MTU (Maximum Transfer Unit) de una VLAN.
- **Solicitud:** Cuando se envía una solicitud a un servidor VTP, éste responde con anuncios resumen y subset. Las solicitudes se envían si el nombre del dominio ha sido cambiado, el conmutador recibe un resumen con un número de revisión más alto, un subset se pierde o el conmutador ha sido reiniciado.

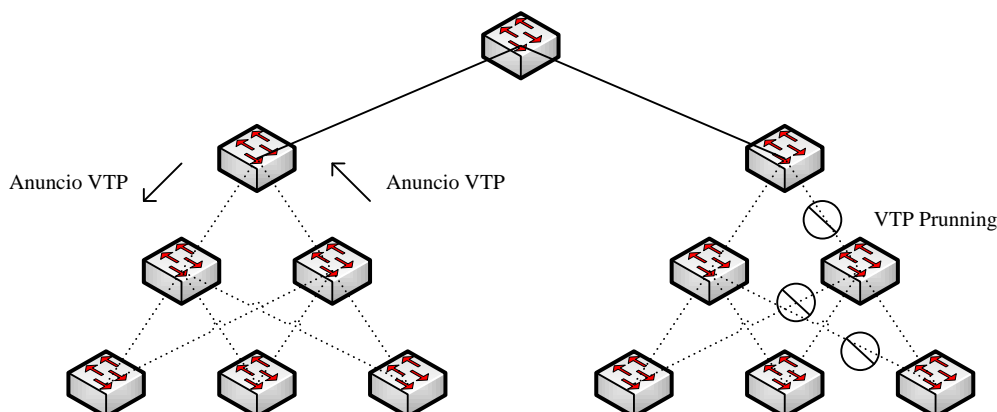


Figura 2.66: Anuncios VTP y Pruning

2.1.9.2.3 Modos

- **Servidor:** Puede crear, modificar y borrar VLANs en un dominio VTP. Anuncia y sincroniza las configuraciones VLAN con otros conmutadores mediante anuncios recibidos en enlaces troncales. Mantiene un registro de actualizaciones a través de un número de revisión de configuración. Todos los conmutadores están configurados para ser servidores VTP por defecto (Figura 2.67).
- **Cliente:** No puede crear, cambiar o borrar VLANs. Como la información de configuración VLAN recibida por un conmutador cliente se almacena en la base de datos VLAN, estos conmutadores requieren menos memoria que los servidores. Cuando un cliente se reinicia, éste envía una solicitud a un servidor para obtener la información de configuración actualizada (Figura 2.67).
- **Transparente:** Reenvía anuncios VTP a otros conmutadores en una red. No anuncia ni sincroniza su configuración VLAN con otros conmutadores. Un conmutador se configura en este modo cuando las configuraciones VLAN tienen significancia local y no deben ser compartidas. Las configuraciones VLAN se graban en NVRAM para tenerlas disponibles luego de reiniciar el conmutador (Figura 2.67).

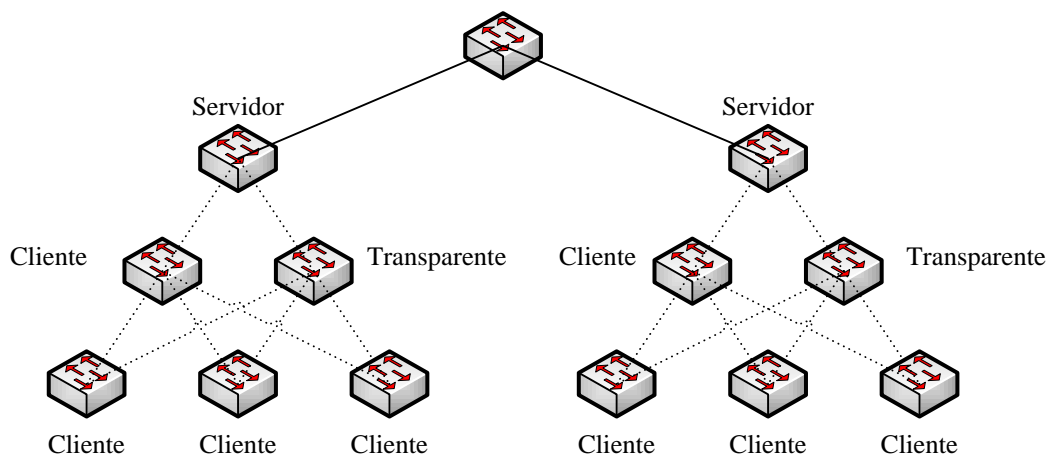


Figura 2.67: Modos VTP

2.1.9.2.4 Pruning

Previene la inundación innecesaria de información de broadcast desde una VLAN a través de los enlaces troncales en un dominio VTP (Figura 2.66). Permite que los conmutadores negocien cuáles VLANs se asignan al otro extremo de un enlace troncal y elimina las VLANs que no están asignadas en el conmutador remoto. VTP Pruning se debe habilitar solamente en un servidor del dominio con el comando `vtp pruning`.

2.2.9.3 Parámetros VTP

Para ver el estado VTP se utiliza el comando `show vtp status` y sus parámetros son:

- **Versión:** Muestra la versión VTP que se utiliza. La versión por defecto es la 1.
- **Revisión de Configuración:** Es el número de revisión de configuración actual.
- **Número máximo de VLANs admitidas localmente**
- **Número de VLANs existentes**
- **Modo de operación VTP:** Puede ser servidor, cliente o transparente.
- **Nombre del dominio VTP**
- **Modo Pruning VTP:** Indica si pruning está habilitado.
- **Modo V2 VTP:** Indica si el modo VTP versión 2 está habilitado. La versión por defecto es la 2.
- **Generación de notificaciones VTP:** Indica si se envían notificaciones VTP a una estación de administración de red.

- **Resumen MD5:** Es un checksum de 16 bytes de la configuración VTP.
- **Ultima modificación de configuración:** Muestra la fecha y hora de la última modificación de configuración y la dirección IP del conmutador que causó el cambio.

2.2.9.3.1 Trama

2.2.9.3.1.1 Encapsulamiento

Una trama VTP está formada por un encabezado y un mensaje. La información VTP se inserta en el campo de datos de una trama Ethernet, la misma que se encapsula como una trama troncal 802.1Q o ISL. Cada conmutador envía anuncios periódicos a través de los puertos troncales a una dirección multicast reservada. Estos anuncios se reciben por los conmutadores vecinos que actualizan las configuraciones VTP y VLAN.

2.2.9.3.1.2 Estructura

El contenido del mensaje VTP determina los campos de esta trama. El conmutador que recibe la trama busca campos y valores específicos para saber qué debe procesar. La trama VTP encapsulada como 802.1Q que se ilustra en la Figura 2.68 tiene los siguientes campos:

- **Dirección MAC de Destino:** Es la dirección multicast reservada para todos los mensajes VTP (01-00-0C-CC-CC-CC).
- **LLC (Logical Link Control):** Este campo tiene un DSAP (Destination Service Access Point) y un SSAP (Source Service Access Point) con un valor de AA.
- **SNAP (Subnetwork Access Protocol):** Tiene un OUI y tipo establecidos en AAAA y 2003 respectivamente.
- **Encabezado VTP:** Su contenido varía dependiendo del tipo de mensaje VTP (resumen, subset o solicitud), pero siempre contiene estos campos: nombre de dominio, longitud del nombre de dominio, versión y número de revisión de configuración.
- **Mensaje VTP:** Varía dependiendo del tipo.

- **Contenido del Mensaje:** Nombre del dominio VTP, identidad del conmutador que envía el mensaje, configuración del resumen MD5 de la VLAN incluyendo el tamaño de la MTU para cada VLAN, formato de la trama (ISL u 802.1Q). Las tramas VTP contienen la siguiente información por cada VLAN: identificador, nombre, tipo y estado.
- **Número de Revisión:** Es un número de 32 bits que indica el nivel de revisión para una trama VTP y tiene un valor por defecto de 0. Cada vez que se añade o remueve una VLAN, este número se incrementa. El número de revisión determina si la información de configuración recibida de otro conmutador es más reciente y vuelve a 0 si se cambia el nombre de dominio.

Dirección Destino	Dirección Origen	Etiqueta 802.1Q	Tipo o Longitud	LLC	SNAP	Encabezado VTP	Tipo de Mensaje VTP	FCS
-------------------	------------------	-----------------	-----------------	-----	------	----------------	---------------------	-----

Figura 2.68: Trama VTP

2.2.9.4 Configuración

2.2.9.4.1 Servidores

- Confirmar que los conmutadores tengan la configuración por defecto.
- Resetear el número de revisión antes de instalar un conmutador previamente configurado.
- Configurar dos servidores VTP en una red. Dado que solamente los servidores pueden crear, borrar y modificar VLANs se debe tener un servidor VTP de respaldo. Si todos los conmutadores se configuran en modo cliente, no se puede crear nuevas VLANs en la red.
- Configurar un dominio VTP en el servidor. Los conmutadores conectados mediante enlaces troncales reciben la información del dominio VTP a través de anuncios VTP.
- La contraseña y versión VTP deben ser las mismas en todos los conmutadores en el dominio que necesitan intercambiar información VTP.

- Es importante crear las VLANs después de habilitar VTP en el servidor y configurar los puertos troncales para interconectar los conmutadores, pues la información VTP se transmite por puertos troncales.
- Se utiliza el comando `vtp mode server`.
- El nombre de dominio se configura con el comando `vtp domain nombre de dominio`.
- La contraseña se configura con el comando `vtp password contraseña`.

2.2.9.4.2 Clientes

- Confirmar que exista la configuración por defecto.
- Configurar el modo cliente y los puertos troncales y conectarlos a un servidor.
- Antes de configurar los puertos de acceso, es necesario confirmar que el número de revisión y VLANs se hayan actualizado.
- Antes de configurar un cliente, se debe verificar el estado VTP actual.
- Para configurar un cliente VTP se utiliza el comando `vtp mode client`.

2.2.10 STP (Spanning Tree Protocol)

Los enlaces adicionales en conmutadores y enrutadores introducen lazos de tráfico que necesitan ser controlados. Cuando se pierde una conexión, otro enlace debe reemplazarlo sin introducir lazos de tráfico. STP previene estos lazos y calcula los puertos que deben bloquearse.

2.2.10.1 Redundancia

La redundancia de Capa 2 mejora la disponibilidad de la red implementando trayectorias alternas mediante equipamiento y cableado. En un diseño jerárquico, la redundancia se consigue en las capas de Distribución y Core con hardware y trayectorias alternas (Figuras 2.69a, 2.69b y 2.69c).

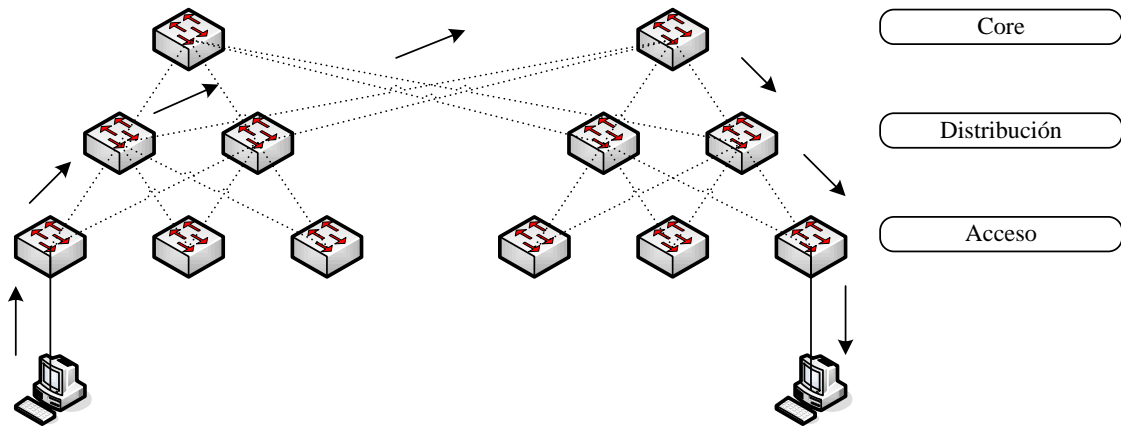


Figura 2.69a: Diseño Redundante

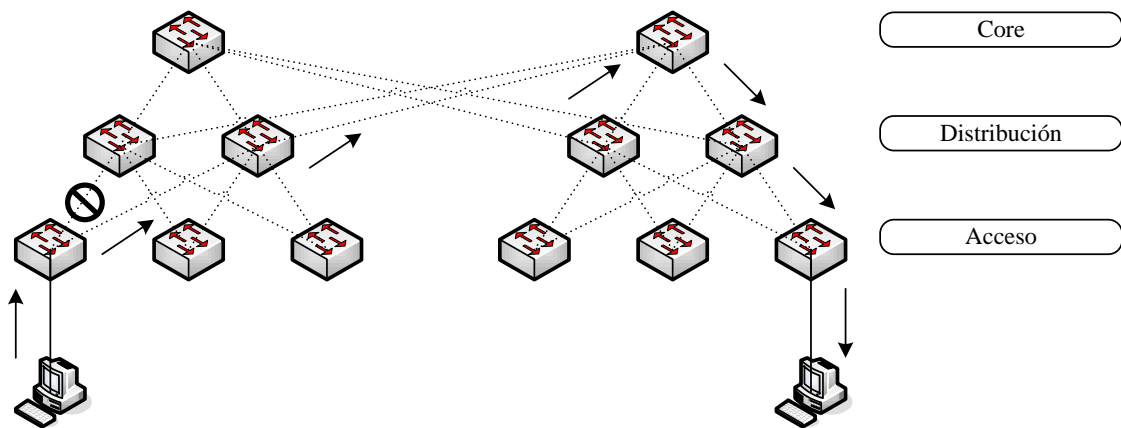


Figura 2.69b: Falla en una Trayectoria entre las Capas de Acceso y Distribución

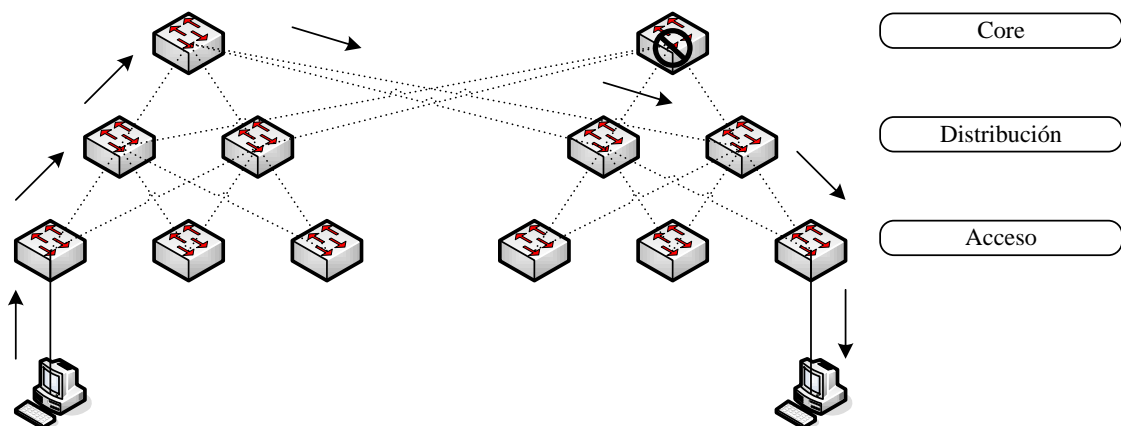


Figura 2.69c: Falla en un Conmutador de Core

2.2.10.1.1 Lazos de Capa 2

Cuando existen múltiples trayectorias entre dos dispositivos y se deshabilita STP puede ocurrir un lazo. Si las tramas Ethernet no alcanzan su destino, éstas continúan pasando entre los conmutadores hasta que se rompa el lazo. Como las tramas de broadcast son reenviadas por todos los puertos de un conmutador (excepto por el puerto de origen) se asegura que todos los dispositivos en el dominio reciban la trama. Si existe más de una trayectoria por donde reenviar la trama, puede ocurrir un lazo sin fin. Los lazos producen una alta carga de CPU en los conmutadores que están atrapados en el lazo. Como la tabla de direcciones MAC cambia constantemente con las actualizaciones de las tramas de broadcast, el conmutador no sabe por cuál puerto enviar las tramas unicast. Esta gran cantidad de tramas produce una tormenta de broadcast.

2.2.10.1.2 Tormentas de Broadcast

Ocurren cuando existen demasiadas tramas de broadcast atrapadas en un lazo de Capa 2. Cuando se incrementa el número de dispositivos que envían broadcasts, una mayor cantidad de tráfico se queda atrapado en el lazo y se crea una tormenta de broadcast que causa fallas en la red. Como el tráfico de broadcast se envía por todos los puertos de un conmutador, todos los dispositivos conectados tienen que procesar este tráfico. Esta situación puede provocar que un dispositivo de usuario final funcione incorrectamente pues los requerimientos de procesamiento son altos.

2.2.10.1.3 Lazos en el Armario

La redundancia es muy importante en una red jerárquica, pero los lazos pueden ocurrir como resultado de haber configurado múltiples trayectorias. El cableado de red puede volverse muy confuso ya que los cables entre los conmutadores de Acceso desaparecen en las paredes, pisos y techos. Si los cables no están etiquetados es difícil determinar su trayectoria. Los lazos que resultan de conexiones duplicadas accidentales son comunes. La Figura 2.70 muestra un lazo que ocurre cuando se conecta dos conmutadores que también están interconectados. Este lazo tiene mayor impacto porque afecta a un mayor número de conmutadores. Aunque el lazo se encuentra en los conmutadores interconectados, éste afecta al resto de la red debido al envío de gran cantidad de broadcast que llega a los demás conmutadores.

Estos lazos ocurren cuando un administrador conecta equivocadamente un cable al mismo conmutador que ya había sido conectado, pues los cables no están etiquetados o las conexiones no han sido verificadas. La agrupación de puertos Ethernet en un conmutador (EtherChannel) actúa como una sola conexión lógica. Dado que el conmutador considera a los puertos agrupados como un solo enlace, no se producen lazos.

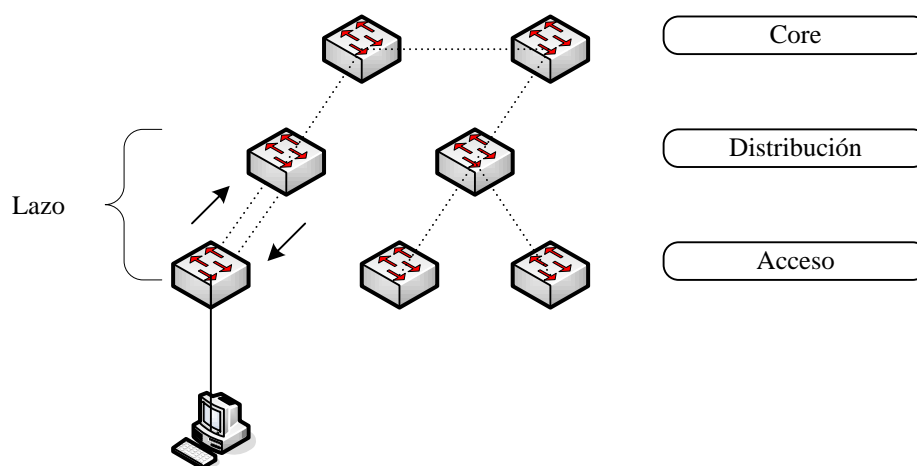


Figura 2.70: Lazos en el Armario

2.2.10.1.4 Lazos en los Cubículos

La escasez de conexiones de red ocasiona que algunos usuarios utilicen un hub o conmutador personal en su Área de Trabajo. Un administrador de red no tiene control respecto a la utilización de los hubs o conmutadores personales, por lo que el usuario final puede accidentalmente interconectar dichos equipos. En la Figura 2.71, los hubs interconectados producen un lazo.

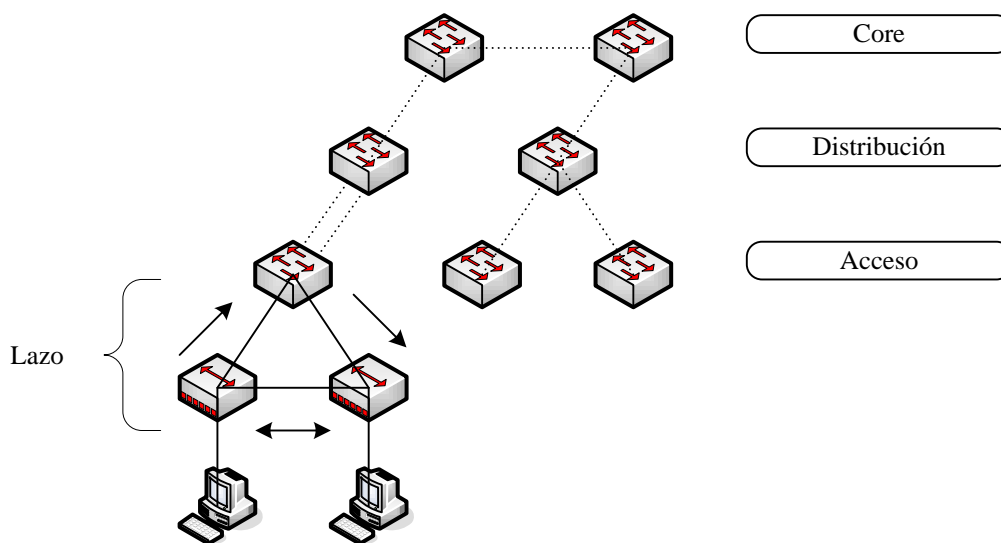


Figura 2.71: Lazos en los Cubículos

2.2.10.2 Algoritmo

La Redundancia incrementa la disponibilidad de la red y la protege de un punto único de falla. Cuando se introduce redundancia en un diseño de Capa 2, pueden aparecer lazos y tramas duplicadas. STP asegura que exista una sola trayectoria lógica entre todos los conmutadores al bloquear trayectorias redundantes que puedan causar un lazo. Un puerto se bloquea para evitar el ingreso y salida de tráfico, a excepción de las tramas BPDU (Bridge Protocol Data Unit), para prevenir lazos. Las trayectorias físicas existen para proveer redundancia, pero se deshabilitan para evitar lazos. Si la trayectoria se necesita para compensar una falla, STP recalcula las trayectorias y desbloquea los puertos necesarios para permitir que la trayectoria se active.

STP utiliza un algoritmo para determinar los puertos que deben bloquearse. El algoritmo designa al Conmutador Raíz y lo utiliza como punto de referencia para todos los cálculos de trayectorias. Todos los conmutadores participan en el intercambio de tramas BPDU para determinar cuál conmutador tiene la menor BID (Bridge ID) en la red y convertirlo en el Conmutador Raíz para realizar los cálculos. Cada BPDU contiene una BID que identifica al conmutador que envió la trama. La BID tiene un valor de prioridad, la dirección MAC del conmutador que envía y un identificador de sistema extendido opcional. El valor más bajo de BID está determinado por la combinación de estos tres campos.

Una vez que se determina el Conmutador Raíz, se calcula la trayectoria más corta. Cada conmutador utiliza el algoritmo para determinar cuáles puertos debe bloquear. El algoritmo toma en cuenta los costos de trayectoria y puerto cuando determina qué trayectoria deja desbloqueada. Los costos de la trayectoria son calculados utilizando valores asociados con las velocidades de los puertos. La suma de estos valores determina el costo total de la trayectoria al Conmutador Raíz.

Luego de haber determinado cuáles trayectorias deben estar disponibles, el algoritmo configura los roles de puerto que describen su relación con el Conmutador Raíz (Figura 2.72).

- **Raíz:** Puertos cercanos al Conmutador Raíz.
- **Designados:** Puertos que no son raíz y pueden reenviar tráfico.
- **No Designados:** Puertos en estado de bloqueo para prevenir lazos.

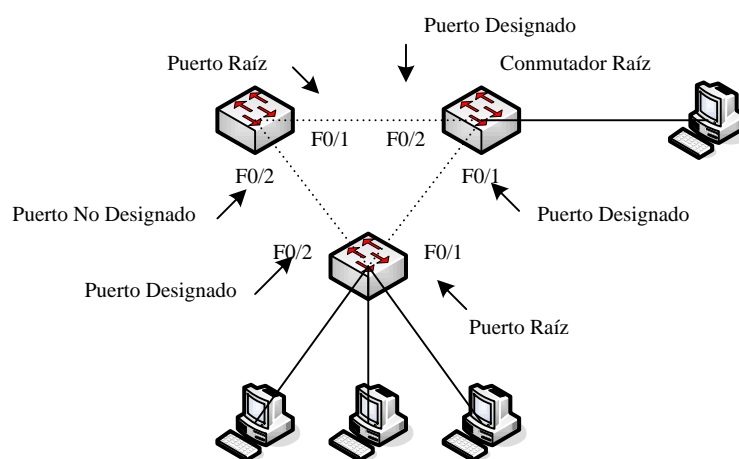


Figura 2.72: Algoritmo STP

2.2.10.2.1 El Conmutador Raíz

Cada instancia de spanning-tree tiene un conmutador designado como raíz, el mismo que sirve como punto de referencia para todos los cálculos y para determinar las trayectorias redundantes que se deben bloquear. El Conmutador Raíz se determina a través de un proceso de elección. Todos los conmutadores en el dominio de broadcast participan en la elección. Después que un conmutador se inicia, éste envía tramas BPDU que

contienen la BID del conmutador y la identificación del Conmutador Raíz cada 2 segundos.

Inicialmente, todos los conmutadores se identifican como el Conmutador Raíz. Conforme se reenvían las tramas BPDU, los conmutadores registran la identificación del Conmutador Raíz. Si la identificación en la BPDU recibida es menor que la identificación del receptor, éste actualiza su identificación y reconoce al conmutador adyacente como raíz.

Después que se ha designado el Conmutador Raíz, se determinan las mejores trayectorias sumando los costos individuales de los puertos en la trayectoria hacia el Conmutador Raíz. Los costos de los puertos se definen por su velocidad. El costo de un puerto es configurable y permite controlar las trayectorias al Conmutador Raíz. El comando que se utiliza es `spanning-tree cost valor`. El valor puede estar entre 1 y 200000000. Las trayectorias con el costo más bajo son las preferidas y las redundantes se bloquean.

2.2.10.3 BPDU

2.2.10.3.1 Trama

En la Figura 2.73 se muestra la trama BPDU (12 campos) que transmite la información de trayectoria y prioridad que STP utiliza para determinar el Conmutador Raíz y las trayectorias correspondientes. Los primeros cuatro campos identifican el protocolo, versión, tipo de mensaje y estado de las banderas. Los siguientes cuatro campos identifican el Conmutador Raíz y el costo de la trayectoria. Los últimos cuatro campos son temporizadores que determinan la frecuencia de envío de los mensajes BPDU y cuánto tiempo se mantiene la información recibida a través del proceso BPDU.

2	Protocolo
1	Versión
1	Tipo de Mensaje
1	Banderas
8	Identificación del Conmutador Raíz
4	Costo de la Trayectoria
8	Identificación del Conmutador
2	Identificación del Puerto
2	Message age
2	Max age
2	Hello time
2	Forward delay

Figura 2.73: Campos de la Trama BPDU

2.2.10.3.2 Proceso

Todos los conmutadores inicialmente asumen que son el Conmutador Raíz para la instancia de spanning-tree, de manera que las tramas BPDU enviadas tienen la BID del conmutador local como identificación. Las tramas BPDU se envían cada 2 segundos después que un conmutador se inicia (temporizador hello). Cada conmutador tiene información local sobre su BID, identificación y costo de la trayectoria.

Cuando los conmutadores reciben una trama BPDU, comparan la identificación de la trama con la identificación local. Si la primera es menor que la segunda, el conmutador actualiza tanto su identificación como la de sus mensajes BPDU para indicar el nuevo Conmutador Raíz. Luego de actualizar la identificación, las tramas BPDU enviadas desde el conmutador tienen el nuevo costo de trayectoria. Así, todos los conmutadores pueden identificar la menor identificación. Conforme las tramas BPDU pasan entre los conmutadores, el costo de la trayectoria se actualiza continuamente para indicar el costo total al Conmutador Raíz.

2.2.10.4 Bridge ID

Sirve para determinar el Conmutador Raíz en una red. Tiene tres campos que se utilizan durante el proceso de elección como se observa en la Figura 2.74:

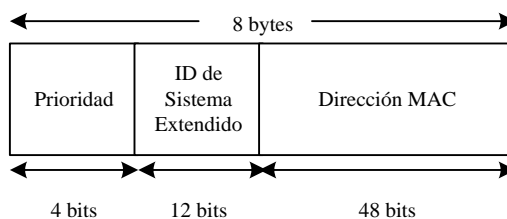


Figura 2.74: Campos de la Bridge ID

- **Prioridad:** Es un valor que se utiliza para decidir cuál conmutador se convierte en raíz (valor más bajo). El valor por defecto es 32768. El rango de prioridad está entre 1 y 65536, siendo 1 la prioridad más alta.
- **ID de Sistema Extendido:** Este campo contiene la identificación de la VLAN asociada. Cuando se lo utiliza, cambia el número de bits disponibles para el valor de la prioridad, (1 a 4096). Este valor se añade a la prioridad en la BID para identificar la prioridad y VLAN.
- **Dirección MAC:** Cuando dos conmutadores se configuran con igual prioridad e ID de sistema extendido, el conmutador que tiene la dirección MAC con el valor hexadecimal más bajo tiene la menor BID. Se debe configurar el Conmutador Raíz con una prioridad más baja para asegurar que gane la elección.

2.2.10.4.1 Configuración

Existen dos métodos para configurar la prioridad en un conmutador:

- Utilizando el comando `spanning-tree vlan identificador de vlan root primary`. La prioridad se establece en 24576 o el siguiente valor incremental de 4096 debajo de la prioridad más baja detectada. Si se requiere un Conmutador Raíz alternativo, se utiliza el comando `spanning-tree vlan identificador de vlan root secondary` que establece la prioridad en 28672 y asegura que este conmutador sea el Conmutador Raíz en caso de que el primario falle y ocurra una nueva elección.
- Utilizando el comando `spanning-tree vlan identificador de vlan priority valor`. Este comando proporciona mayor control sobre el valor de prioridad y se configura en incrementos de 4096 entre 0 y 65536.

2.2.10.5 Roles de Puertos

El Conmutador Raíz es elegido para cada instancia de spanning-tree y su ubicación en la topología determina cómo se calculan los roles de los puertos. Existen cuatro roles de puertos:

- **Raíz:** Este puerto existe en conmutadores que no sean raíz y tiene la mejor trayectoria al Conmutador Raíz. Los puertos raíz reenvían tráfico a través del Conmutador Raíz. Se permite un solo puerto de esta clase por conmutador.
- **Designado:** En los Conmutadores Raíz todos los puertos son designados. Para los demás conmutadores, un puerto designado es aquel que recibe y envía tramas a través del Conmutador Raíz. Se permite un solo puerto designado por segmento. En caso de existir múltiples conmutadores, un proceso de elección determina el conmutador designado y el puerto correspondiente comienza a enviar tramas.
- **No Designado:** Es un puerto que se bloquea y no envía tramas de datos.
- **Deshabilitado:** Es un puerto que está apagado administrativamente y no funciona en el proceso spanning-tree.

Cuando se determina el puerto raíz, el conmutador compara los costos de las trayectorias en todos los puertos. Aquel con el costo de trayectoria más bajo al Conmutador Raíz asume el rol de puerto raíz porque está más cerca. En una topología de red, todos los conmutadores excepto el Conmutador Raíz, tienen un solo puerto raíz. Si hay dos puertos que tienen el mismo costo al Conmutador Raíz y ambos son los más bajos, el conmutador utiliza la prioridad o identificación del puerto (interfaz) más baja para determinar el puerto raíz.

2.2.10.5.1 Prioridad de Puerto

Se utiliza el comando `spanning-tree port-priority valor`. Los valores están en el rango de 0 a 240, en incrementos de 16. El valor por defecto para la prioridad de un puerto es 128.

2.2.10.5.2 Decisiones de los Roles de Puertos

Luego que se determina cuál de los puertos está configurado como raíz, se necesita decidir cuáles puertos son designados y no designados. El Conmutador Raíz configura

todos sus puertos como designados. Los demás conmutadores en la topología configuran sus puertos como designados o no designados.

Los puertos designados se configuran para todos los segmentos. Cuando dos conmutadores están conectados al mismo segmento y se han definido los puertos raíz, ambos conmutadores tienen que decidir cuál puerto se configura como designado y no designado.

El conmutador con la menor BID tiene el puerto designado, mientras que aquel con la mayor BID tiene el puerto no designado. Por ende, cada conmutador determina los roles de cada puerto para crear el spanning-tree libre de lazos.

2.2.10.6 Estados de Puertos y Temporizadores

STP determina la trayectoria lógica libre de lazos mediante el intercambio de tramas BPDU entre conmutadores. Para facilitar el proceso, cada puerto pasa por cinco estados y utiliza tres temporizadores BPDU.

2.2.10.6.1 Estados

- **Bloqueado:** Es un puerto no designado que no participa en el envío de tramas y recibe tramas BPDU para determinar la ubicación e identificación del Conmutador Raíz y los roles que debe asumir cada puerto (Tabla 2.3).
- **Escuchando:** Este puerto recibe y transmite tramas BPDU informando que el puerto va a participar en la topología (Tabla 2.3).
- **Aprendiendo:** Este puerto se prepara para participar en el envío de tramas y comienza a poblar la tabla de direcciones MAC (Tabla 2.3).
- **Transmitiendo:** Este puerto es parte de la topología enviando y recibiendo tramas (Tabla 2.3).
- **Deshabilitado:** Este puerto no participa en spanning tree y tampoco envía tramas (Tabla 2.3).

Procesos	Bloqueado	Escuchando	Aprendiendo	Transmitiendo	Deshabilitado
Recibe y procesa BPDUs	Sí	Sí	Sí	Sí	No
Transmite tramas de datos recibidas en una interfaz	No	No	No	Sí	No
Transmite tramas de datos conmutadas por otro dispositivo	No	No	No	Sí	No
Aprende direcciones MAC	No	No	Sí	Sí	No

Tabla 2.3: Estados de los Puertos

2.2.10.6.2 Temporizadores

El tiempo que un puerto se mantiene en los distintos estados depende de los temporizadores BPDUs. Solo el Conmutador Raíz puede enviar información para ajustar los temporizadores. Los siguientes temporizadores determinan el funcionamiento STP: hello time, forward delay y maximum age.

Cada puerto pasa por los tres primeros estados cuando se enciende para luego estabilizarse en los estados transmitiendo o bloqueado. Cuando se produce un cambio de topología, un puerto temporalmente pasa por los estados escuchando y aprendiendo por un periodo llamado “forward delay interval”. Estos estados proporcionan tiempo suficiente para la convergencia (tiempo que toma recalcularse el spanning tree si un conmutador o enlace falla) en una red con un diámetro de siete conmutadores.

2.2.10.6.3 PortFast

Un puerto de acceso configurado con PortFast pasa de estar bloqueado a transmitir inmediatamente. Esta tecnología se utiliza en puertos que están conectados a una estación de trabajo o servidor para permitir una conexión inmediata y no esperar la convergencia. El comando que se utiliza es `spanning-tree portfast`.

2.2.10.7 Convergencia

Es el tiempo que le toma a la red determinar cuál conmutador será el raíz, pasar por los diferentes estados de puertos y establecer los roles correspondientes.

2.2.10.7.1 Elección del Conmutador Raíz

El Conmutador Raíz es la base para todos los cálculos de costo de trayectoria y permite la asignación de los roles de puerto. La elección del Conmutador Raíz ocurre luego que un conmutador se enciende o cuando se detecta una falla en una trayectoria. Inicialmente, todos los puertos de un conmutador están configurados en el estado de bloqueo (20 segundos) para prevenir que ocurra un lazo antes que STP calcule las mejores trayectorias al Conmutador Raíz y configure los roles de puertos.

Después, los conmutadores envían tramas BPDU anunciando su BID tratando de convertirse en el Conmutador Raíz. Inicialmente, todos los conmutadores asumen que son el Conmutador Raíz. A medida que los conmutadores reciben las tramas BPDU, se compara la identificación de la trama recibida con la identificación local. Si la primera es menor que la segunda, la identificación se actualiza para indicar el nuevo candidato para ser el Conmutador Raíz.

Luego, el conmutador incorpora la nueva identificación en las transmisiones para asegurar que la menor identificación se transmita a todos los conmutadores en la red. Los conmutadores continúan enviando sus tramas BPDU para anunciar la identificación del Conmutador Raíz cada 2 segundos. Cada conmutador tiene un temporizador (max age) que determina cuánto tiempo se conserva la configuración BPDU actual en caso de no recibir actualizaciones. Este temporizador se establece en 20 segundos. Si un conmutador no recibe 10 tramas BPDU consecutivas de uno de sus vecinos, éste asume que existe una falla en una trayectoria lógica y que la información BPDU no es válida, produciendo otra elección.

2.2.10.7.2 Elección de los Puertos Raíz

El primer rol de puerto que se determina es el raíz. Los puertos con costos equivalentes al Conmutador Raíz utilizan su valor de prioridad de puerto para desempatar. El puerto que pierde se configura como no designado.

2.2.10.7.3 Elección de Puertos Designados y No Designados

Luego que se determina el puerto raíz, los puertos restantes se configuran como designados (DP) o no designados (non-DP). Cada segmento en una red puede tener solamente un puerto designado. Cuando dos puertos que no son raíz están conectados en el mismo segmento, se produce una competencia por roles de puerto. El conmutador con la

menor BID configura su puerto como designado y el que pierde configura su puerto como no designado.

2.2.10.8 Proceso de Notificación de Cambio en la Topología

Un conmutador detecta un cambio en la topología cuando se interrumpe la transmisión en un puerto o cuando un puerto comienza a transmitir y el conmutador tiene un puerto designado. Cuando un conmutador necesita indicar un cambio de topología, éste envía TCNs (Topology Change Notifications) por su puerto raíz como se ilustra en la Figura 2.75. La TCN es una BPDU que no contiene información y se envía en el intervalo de tiempo de hello. El conmutador que recibe envía una BPDU con el bit TCA (Topology Change Acknowledgement) encendido como respuesta. Cuando el Conmutador Raíz conoce del cambio de topología, éste envía BPDUs con el bit TC (Topology Change) activado.

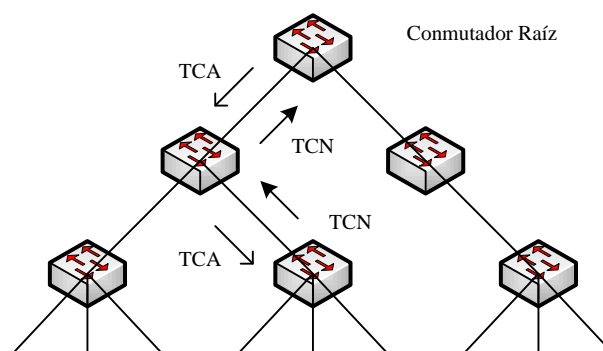


Figura 2.75: Notificación de Cambio en la Topología

2.2.11 RSTP (Rapid Spanning Tree Protocol)

El STP (Spanning Tree Protocol) mantiene una red conmutada libre de lazos mediante ajustes dinámicos en la topología. Los cambios en la topología toman alrededor de 30 segundos. RSTP (Rapid Spanning Tree Protocol) fue desarrollado para lograr la convergencia en menor tiempo. La funcionalidad de este protocolo puede aplicarse como una o varias instancias. Al utilizar RSTP como fundamento para PVST+ (Per-VLAN Spanning Tree Protocol) se obtiene RPVST+ (Rapid PVST+).

2.2.11.1 Roles de Puerto

RSTP permite que cada conmutador interactúe con sus vecinos a través de todos los puertos, basándose en su rol y no solamente en las BPDUs (Bridge Protocol Data Units) retransmitidas por el Conmutador Raíz. Una vez que se ha determinado el rol, a cada puerto se le asigna un estado que decide cómo procesar la información. El dispositivo con la menor BID (Bridge ID) se convierte en el Conmutador Raíz. Luego que todos los equipos conocen la identidad del Conmutador Raíz se determinan los roles de puerto:

- **Raíz:** Es un puerto en cada dispositivo que tiene el mejor costo de trayectoria al Conmutador Raíz.
- **Designado:** Es el puerto en un segmento de red que tiene el mejor costo de trayectoria al Conmutador Raíz.
- **Alternativo:** Es un puerto que tiene una trayectoria alterna al Conmutador Raíz.
- **Respaldo:** Es un puerto que proporciona un enlace redundante a un segmento donde ya se encuentra conectado otro puerto.

2.2.11.2 Estados de Puerto

Cualquier puerto puede estar en uno de los siguientes estados:

- **Descartando:** Las tramas entrantes se descartan y no se aprenden direcciones MAC (Media Access Control). Aquí se combinan los estados Deshabilitado, Bloqueado y Escuchando de STP (Spanning-Tree Protocol) porque ninguno tiene la capacidad de transmitir. El estado Escuchando no es necesario ya que RSTP negocia rápidamente cambios de estado sin escuchar BPDUs.
- **Aprendiendo:** Las tramas entrantes se descartan pero si se aprenden direcciones MAC.
- **Transmitiendo:** Las tramas entrantes se transmiten según las direcciones MAC que han sido aprendidas.

2.2.11.3 BPDUs

RSTP utiliza el formato BPDUs de STP por cuestiones de compatibilidad y activa ciertos bits del campo Tipo de Mensaje. El puerto que envía se identifica mediante su rol y estado. RSTP emplea un proceso interactivo para que los conmutadores vecinos puedan negociar

cambios de estado. Las BPDUs se envían por cada puerto a intervalos determinados por el temporizador hello, independientemente si los mensajes fueron recibidos por el Conmutador Raíz. Cuando se pierden tres BPDUs seguidos, se asume una falla en el dispositivo vecino y toda la información relacionada a ese puerto se caduca.

2.2.11.4 Tipos de Puerto

Cuando un dispositivo se agrega a una topología u ocurre una falla, RSTP toma decisiones en base al tipo de puerto:

- **Frontera:** Es un puerto en el borde la red que conecta a un solo equipo. Como este puerto no puede formar lazos, es posible hacerlo que transmita inmediatamente (PortFast).
- **Raíz:** Es el puerto que tiene el mejor costo hacia el Conmutador Raíz. Solamente un puerto puede estar activo a la vez, aunque existan trayectorias alternas a través de otros puertos.
- **Punto a Punto:** Es cualquier puerto que se conecta a otro conmutador y se convierte en Designado.

RSTP controla la convergencia a través de negociaciones en los enlaces punto a punto. Cuando un conmutador debe tomar una decisión, se produce una negociación con el vecino más cercano y en caso de ser exitosa se transmite a los siguientes dispositivos.

2.2.11.5 Sincronización

Para participar en la convergencia, un dispositivo tiene que decidir el estado de todos sus puertos. Los puertos que no son de frontera inician en el estado Descartando. Luego del intercambio de BPDUs, se elige el Conmutador Raíz. En cada puerto, los dispositivos negocian con mensajes de Propuesta y Aceptación para decidir el estado de cada extremo de un enlace. La Figura 2.76 muestra el proceso que se lleva a cabo el momento que un conmutador recibe una Propuesta.

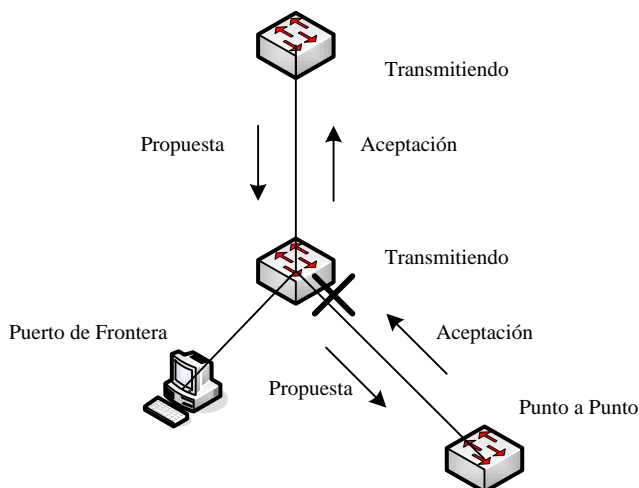


Figura 2.76: Proceso de Sincronización

- Si el equipo que envía la propuesta tiene una BPDU mayor, el conmutador local se percata de que el emisor debe ser el dispositivo designado y que su puerto se convertirá en Raíz.
- Después de aceptar la propuesta, el conmutador debe sincronizarse con la topología.
- Todos los puertos que no son de frontera pasan al estado Descartando a fin de que no se originen lazos.
- Un mensaje se envía al emisor para informar que el conmutador ha aceptado la nueva elección de puertos.
- El puerto Raíz pasa al estado Transmitiendo.
- Cada puerto que no es de frontera y se encuentra en el estado Descartando envía una Propuesta al vecino respectivo.
- Un mensaje de Aceptación se recibe de un vecino a través de un puerto que no es de frontera, el cual pasa a transmitir inmediatamente.

2.2.11.6 Configuración

La configuración RSTP afecta al puerto o tipo de enlace, el mismo que se utiliza para determinar la manera en que un conmutador negocia la información de la topología con sus vecinos. El comando `spanning-tree portfast` permite configurar un puerto que no es

de frontera. RSTP decide que un puerto forma parte de un enlace punto a punto cuando opera en modo full dúplex.

2.2.12 RPVST+ (Rapid Per-VLAN Spanning Tree Protocol)

En este modo una instancia de spanning-tree se crea y utiliza para cada VLAN activa definida en un conmutador. La eficiencia de cada instancia STP puede ser mejorada al configurar un conmutador con el comando `spanning-tree mode rapid-pvst`.

2.2.13 MST o MSTP (Multiple Spanning Tree Protocol)

Se basa en el concepto de establecer una correspondencia en una o más VLANs en una sola instancia STP. En la red de la Figura 2.77 solamente se requieren dos instancias MST, pues cada una representa una topología diferente. La primera instancia (VLAN A) transmitirá en el enlace del extremo izquierdo y la segunda (VLAN B) en el derecho.

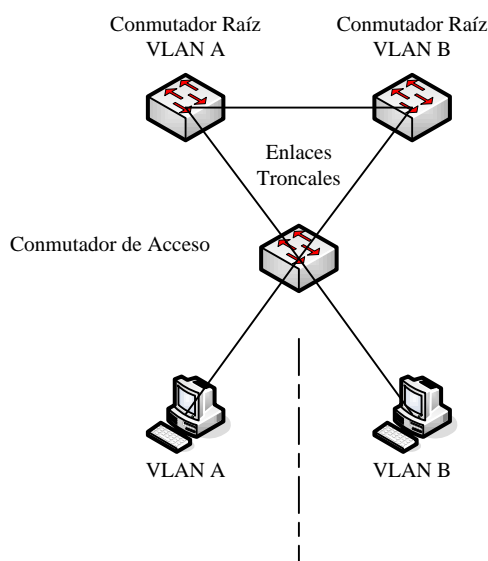


Figura 2.77: Instancias MST para dos VLANs

2.2.13.1 Regiones MST

Un conmutador configurado con MST debe conocer el tipo de STP que están utilizando sus vecinos, por lo que es necesario definir regiones en las cuales los dispositivos operan con parámetros compatibles. En una región todos los conmutadores deben correr la

instancia MST definida por: el nombre de configuración, el número de revisión de configuración y la tabla de correspondencias instancia a VLAN.

2.2.13.2 Instancias

MST funciona con las variantes de STP. En una red donde existe una topología CST (Common Spanning Tree) una instancia STP representa todas las VLANs y regiones MST. El CST considera cada región como una caja negra porque no sabe que existe dentro de la región. Además, una instancia IST (Internal Spanning Tree) se origina para mantener una topología libre de lazos entre el CST y los conmutadores que integran la región. En la Figura 2.78 se observa una región MST como un conmutador virtual para el CST. Varias instancias MST pueden existir en una sola región (Figura 2.79).

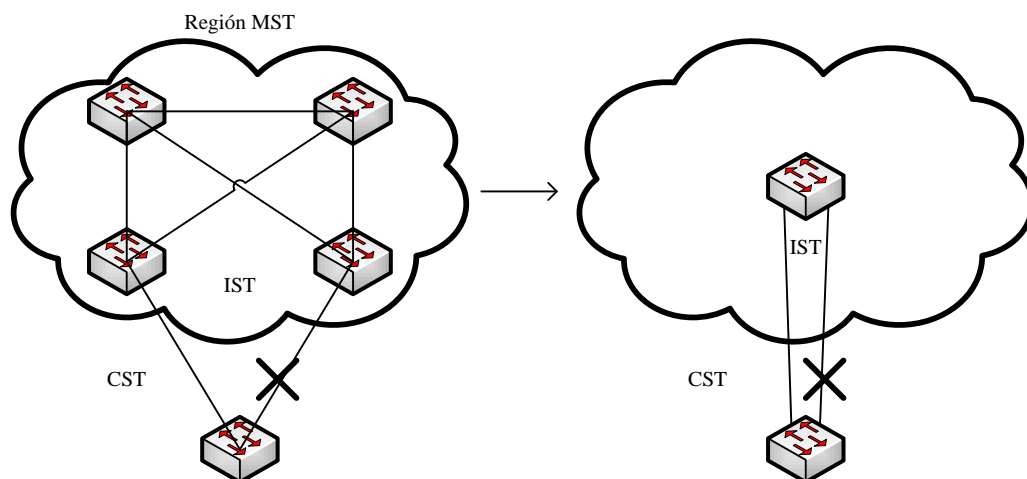


Figura 2.78: Región MST e Instancias IST

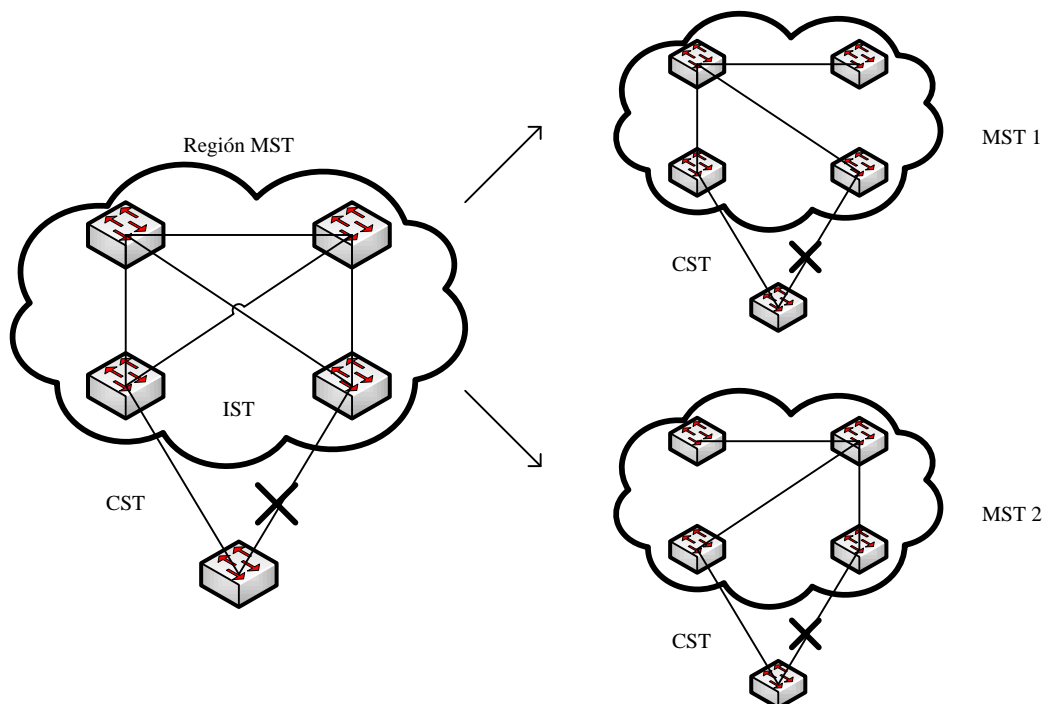


Figura 2.79: Instancias MST en una Región

2.2.13.3 Configuración

Los atributos MST deben configurarse en cada conmutador que forma parte de una región cumpliendo el siguiente esquema:

- Habilitar MST

```
(config)#spanning-tree mode mst
```
- Ingresar al modo de configuración

```
(config)#spanning-tree mst configuration
```
- Asignar un nombre de configuración y un número de revisión

```
(config-mst)#name nombre
```

```
(config-mst)#revision versión
```
- Establecer una correspondencia entre las VLANs y la instancia MST

```
(config-mst)#instance identificador de la instancia vlan lista de vlans
```

2.2.14 Agrupación de Enlaces

Este método permite incrementar el ancho de banda de una conexión al juntar entre dos y ocho enlaces paralelos de Fast Ethernet (FE) o Gigabit Ethernet (GE). Esta tecnología contribuye a expandir la capacidad de un enlace entre dos conmutadores sin tener que adquirir nuevo hardware.

2.2.14.1 Balanceo de Carga

Para configurar la distribución de tramas en un enlace de este tipo se utiliza el comando `port-channel load-balance método`. La configuración por defecto emplea el método `src-dst-ip` (Source and Destination IP Address).

2.2.14.2 Protocolos de Negociación

2.2.14.2.1 PAgP (*Port Aggregation Protocol*)

Los paquetes PAgP se intercambian entre los conmutadores que utilizan agrupación de enlaces. Este protocolo forma un EtherChannel solamente en los puertos configurados para VLANs estáticas idénticas o troncales. Puede ser configurado en modo activo, en el cual un conmutador pregunta al remoto para negociar, o en modo pasivo, en el cual un conmutador negocia únicamente si el remoto inicia el proceso. Para configurar un puerto con PAgP se utilizan los siguientes comandos:

```
(config)# interface identificador de la interfaz
(config-if)# channel-protocol pagp
(config-if)# channel-group número mode {on | {auto | desirable} [non-silent]}
```

2.2.14.2.2 LACP (*Link Aggregation Protocol*)

Este protocolo asigna roles a los puertos que forman el EtherChannel. El conmutador con la prioridad más baja decide cuáles puertos participan en un momento dado. Los puertos se seleccionan y activan según la prioridad del puerto. Se puede definir un arreglo de hasta 16 enlaces. Un conmutador con LACP selecciona hasta 8 puertos con las prioridades más bajas como enlaces activos. Los enlaces restantes se colocan en estado de espera y se habilitan si uno de los enlaces activos falla. Puede configurarse en modo activo o pasivo. Para configurar un puerto con LACP se utilizan los siguientes comandos:


```
(config)# lacp system-priority prioridad
(config)# interface identificador de la interfaz
(config-if)# channel-protocol lacp
(config-if)# channel-group número mode {on | passive | active}
(config-if)# lacp port-priority prioridad
```

2.2.15 HSRP (Hot Standby Router Protocol)

Permite que varios enrutadores o conmutadores multicapa aparezcan como una sola puerta de enlace. Cada uno de los enrutadores que proveen redundancia para una puerta de enlace determinada se asigna a un grupo HSRP. Un enrutador se elige como primario o activo, otro se mantiene en espera y los demás escuchan. Los grupos HSRP se identifican con un número arbitrario entre 0 y 255.

2.2.15.1 Elección del Enrutador HSRP

Se basa en un valor de prioridad que se configura en cada enrutador del grupo. Aquel dispositivo con mayor prioridad se convierte en el enrutador activo. La prioridad se configura con el comando **standby grupo priority** *prioridad*.

Para que un enrutador asuma inmediatamente el rol activo en cualquier momento, siempre y cuando su prioridad sea la más alta, se utiliza el comando **standby grupo preempt**.

2.2.15.2 Autenticación

2.2.15.2.1 Texto Simple

Los mensajes HSRP se envían con una llave en texto sencillo de hasta ocho caracteres para autenticar a los miembros del grupo. El comando **standby grupo authentication llave** permite configurar este tipo de autenticación.

2.2.15.2.2 MD5 (Message Digest 5)

Se calcula en una parte de cada mensaje HSRP y una llave secreta conocida solamente por los miembros del grupo. Esta clase de autenticación se configura asociando una llave a una interfaz con el comando **standby grupo authentication md5 key-string [0|7] llave**.

2.2.15.3 Direccionamiento de la Puerta de Enlace HSRP

Cada enrutador en un grupo HSRP tiene una dirección IP común para la puerta de enlace (enrutador virtual). Los clientes pueden apuntar a esta dirección sabiendo que el enrutador la mantiene activa en todo momento. Para configurar la dirección HSRP se utiliza el comando `standby grupo ip dirección ip [secondary]`.

2.2.16 VRRP (Virtual Router Redundancy Protocol)

Es un protocolo definido en el RFC 2338 que proporciona una dirección redundante para la puerta de enlace de un grupo de dispositivos. El equipo activo se denomina el enrutador maestro y los demás se encuentran en el estado de respaldo. El número de un grupo VRRP puede estar entre 0-255 y la prioridad de los enrutadores tiene un rango de 1 a 254, siendo 100 el valor por defecto. La dirección MAC del enrutador virtual tiene la forma 0000.5e00.01xx, donde xx es un número hexadecimal de dos dígitos que indica el grupo VRRP. No tiene mecanismo alguno para rastrear interfaces que permitan a otros enrutadores asumir el rol de maestro.

2.2.17 GLBP (Gateway Load Balancing Protocol)

Para disponer de un enrutador virtual se asignan varios enrutadores a un grupo GLBP. Todos los equipos pueden balancear la carga al transmitir una parte del tráfico. Ninguno de los clientes apunta a una dirección de puerta de enlace específica, ya que todos tienen definida una dirección IP virtual. El balanceo de carga se logra mediante direcciones MAC virtuales. Cuando un cliente envía una solicitud ARP, GLBP responde con la dirección MAC virtual de un enrutador del grupo.

2.2.17.1 AVG (Active Virtual Gateway)

El enrutador con la prioridad o dirección IP más alta se elige como AVG para responder las peticiones ARP sobre la dirección virtual del enrutador. La AVG asigna las direcciones MAC virtuales a los enrutadores que participan en el grupo. El comando `glbp grupo priority nivel` permite asignar la prioridad en un enrutador. Para que un dispositivo con mayor prioridad se convierta en el AVG se recurre al comando `glbp grupo preempt [delay minimum segundos]`.

2.2.17.2 AVF (Active Virtual Forwarder)

Cada enrutador debe enviar mensajes de hello a su compañero para detectar fallas. La función del temporizador redirect consiste en determinar cuando la AVG no utiliza la dirección MAC virtual en las respuestas ARP. Cuando el temporizador timeout expira, las direcciones MAC antiguas son eliminadas. La AVG asume que el AVF defectuoso no volverá a estar en servicio, de manera que los recursos asignados deben ser recuperados. GLBP puede utilizar una función de ponderación para determinar cuál enrutador se convertirá en AVF. Cada equipo comienza con un valor máximo y a medida que las interfaces dejan de funcionar, el peso disminuye.

2.2.17.3 Balanceo de Carga

AVG distribuye direcciones MAC virtuales a los clientes de manera determinística. Existen tres métodos para balancear la carga:

- **Todos contra Todos:** Cada solicitud ARP sobre la dirección del enrutador virtual recibe la siguiente dirección MAC disponible. La carga de tráfico se distribuye equitativamente a todos los enrutadores que participan como AVFs en el grupo.
- **Ponderado:** El peso de cada interfaz determina la proporción de tráfico que debe enviarse a un AVF.
- **Dependiente del Dispositivo:** Cada cliente que genera una petición ARP recibe la misma dirección MAC. Este método se utiliza cuando los clientes requieren una dirección MAC consistente.

Para definir el método de balanceo de carga se utiliza el comando `glbp grupo load-balancing [round robin | weighted | host-dependent]`. El comando `glbp grupo ip [dirección ip [secondary]]` asigna una dirección IP virtual al grupo.

2.2.18 Pruebas

Luego que el enrutador y conmutador han sido configurados para realizar enrutamiento inter-VLAN, se debe verificar su funcionamiento.

2.2.18.1 Ping

Este comando envía un pedido ICMP a la dirección destino. Ante un pedido ICMP, un computador envía una respuesta ICMP de confirmación. Esta prueba calcula la diferencia de tiempo entre el envío del ping y la recepción de la respuesta para determinar la latencia de la conexión. Si se recibe la respuesta con éxito se confirma la existencia de una trayectoria entre los dispositivos.

2.2.18.2 Tracert

Confirma la trayectoria entre dos dispositivos, utilizando peticiones ICMP con valores específicos de TTL (Time-To-Live) que determinan cuántos saltos puede alcanzar el eco ICMP. La primera petición expira en el primer enrutador que se encuentra en la trayectoria hacia el dispositivo destino. Cuando se acaba el tiempo de esta petición, se envía una confirmación desde el enrutador al dispositivo de origen, el cual graba esta respuesta y envía otra petición, pero con un TTL mayor. De esta forma, la petición pasa el primer enrutador y llega al segundo dispositivo en la trayectoria hacia el destino final. Este proceso se repite hasta que la petición se envía por toda la trayectoria. Cuando la utilidad termina de ejecutarse, se presenta una lista de las interfaces que la petición ICMP alcanzó durante el viaje.

Capítulo 3

3 SITUACIÓN ACTUAL Y PROPUESTA DE DISEÑO

3.1 Situación Actual

3.1.1 Ubicación

La Compañía Nacional de Transmisión Eléctrica se encuentra situada en la Avenida 6 de Diciembre N26-235 y Francisco de Orellana. El edificio TRANSELECTRIC S.A. tiene diez pisos divididos en dos alas: Oriental (A) y Occidental (B). En la Tabla 3.1 se indica el departamento que funciona en cada piso.

Piso	Ala	Área
Décimo	A	Presidencia Ejecutiva
		Presidencia del Directorio
		Sala de Reuniones del Directorio
	B	Comunicación Corporativa
		Directorio
		Secretaría General
Noveno	A	División de Investigación
		Vicepresidencia Técnica
	B	Investigación y Desarrollo de Proyectos Especiales
		Estudios y Plan de Expansión
Octavo	A	División Subestaciones
	B	División Líneas de Transmisión
Séptimo	A	Gerencia de Operación y Mantenimiento
	B	Departamento de Gestión de la Disponibilidad
Sexto	A	Departamento Financiero
	B	Talento Humano
		Recursos Administrativos
		Circuito de Monitoreo
		Vicepresidencia Administrativa y Financiera
Quinto	A	Departamento de Administración de Redes y Gestión de Fibra Óptica
	B	Informática
Cuarto	A	TERMOPICHINCHA
	B	Gerencia de Ingeniería y Construcción/Subestaciones
		Seguros y Riesgos
Tercero	A	Departamento de Adquisiciones, Logística y Bodegas
	B	Gerencia de Ingeniería y Construcción
		División Mantenimiento de Líneas de Transmisión
Segundo	A	Gerencia de Telecomunicaciones
	B	Asesoría Jurídica
Planta Baja	A	Recepción
		Dispensario Médico
		Laboratorio de Telecomunicaciones
		Registro de Documentos
		Suministros
	Copiadora	
	B	Laboratorio de Protecciones/Gerencia de Explotación
		Auditoría Interna
		Planoteca
Comedor		

Tabla 3.1: Departamentos del Edificio Matriz de TRANSELECTRIC S.A.

3.1.2 Cuartos de Telecomunicaciones

3.1.2.1 Noveno Piso

3.1.2.1.1 Dimensiones y Equipamiento

La red LAN (Local Area Network) se instaló hace aproximadamente 9 años. El Cuarto de Telecomunicaciones se ubicó en el noveno piso en el área que separa ambas alas. Las paredes frontales están fabricadas en madera y vidrio como se aprecia en la Figura 3.1. El acceso está protegido por una puerta con doble cerradura y existen tres pares de llaves, uno se mantiene en el CGTT (Centro de Gestión de Telecomunicaciones de TRANSELECTRIC), otro es responsabilidad del administrador de la red y el último está a cargo de un asistente del Departamento de Administración de Redes y Gestión de Fibra Óptica. El piso es de hormigón armado y está cubierto de vinil. El techo está formado por láminas de cielo falso con sus respectivas luminarias. La altura entre el piso y el techo es alrededor de 2,38 metros.



Figura 3.1: Puerta de Ingreso al Cuarto de Telecomunicaciones del Noveno Piso

3.1.2.1.2 Mobiliario, Control de Temperatura y Suministro de Energía

La Figura 3.2 muestra las dimensiones de este espacio y la distribución de los equipos. En la parte posterior de este lugar existe una ventana (1,48 x 1,48 metros) y un equipo de aire acondicionado FUJITSU (Figura 3.3), el cual mantiene la temperatura en 22 °C. Frente a la puerta de ingreso se encuentra un armario pequeño donde se guarda material de instalación y herramientas que incluyen cable UTP (Unshielded Twisted Pair) Categoría 5e, conectores RJ-45 y RJ-11, capuchones, cables de interconexión directos y cruzados,

cortadoras, peladoras, prensas y probadores de cables. Bajo la ventana se encuentra un UPS (Uninterruptible Power Supply) modelo FE4.3KVA (Figuras 3.4a y 3.4b) que sirve de respaldo en caso de un corte de energía eléctrica. Luego está colocada una mesa de trabajo.

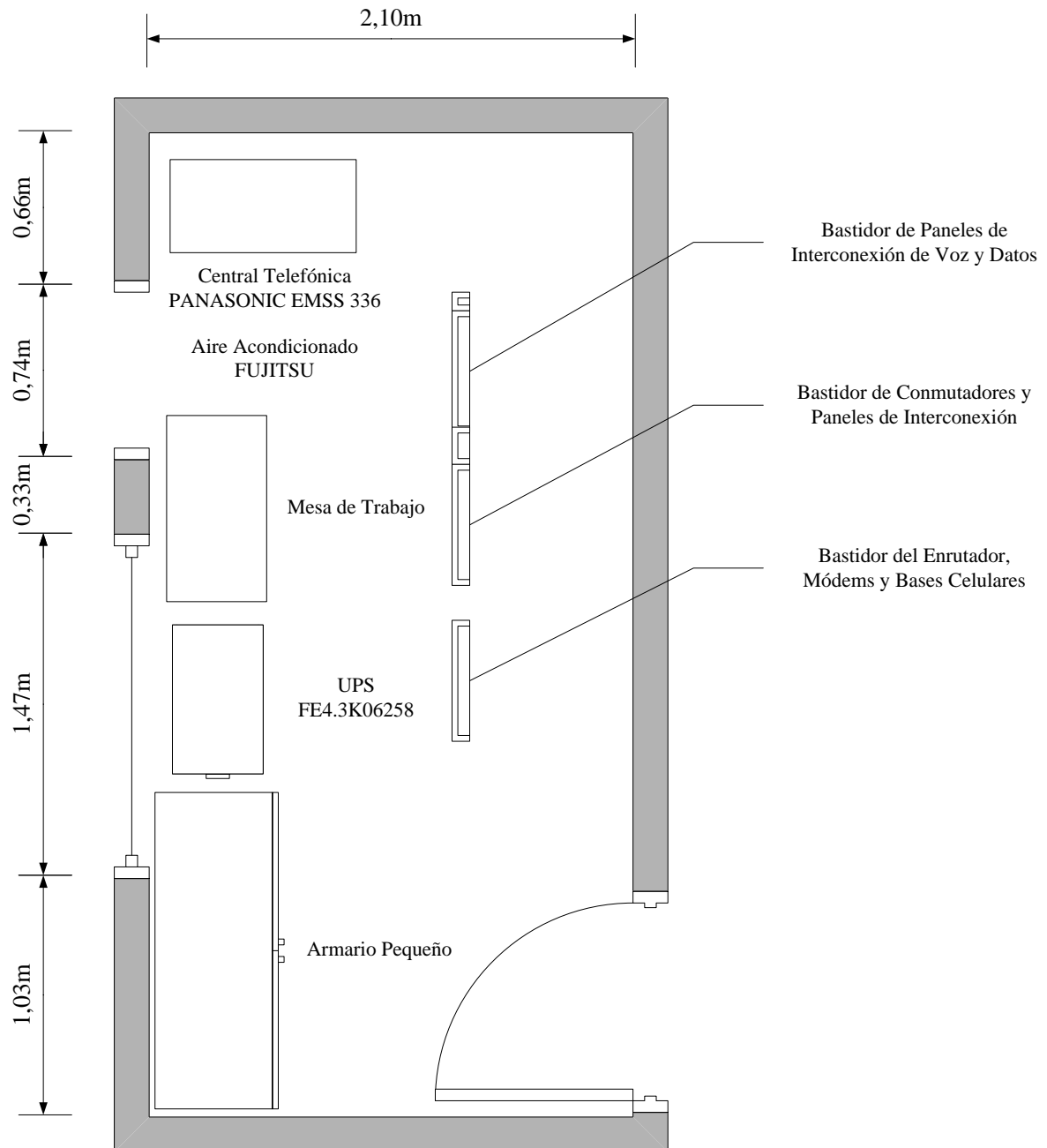


Figura 3.2: Cuarto de Telecomunicaciones del Noveno Piso



Figura 3.3: Aire Acondicionado FUJITSU



Figura 3.4a: UPS FE4.3KVA
(Vista Frontal)



Figura 3.4b: UPS FE4.3KVA
(Vista Posterior)

3.1.2.1.3 Central Telefónica

Las Figuras 3.5a, 3.5b y 3.5c muestran la central telefónica PANASONIC EMSS 336 modelo KX-T336100 que se encuentra en el extremo derecho del cuarto e inicialmente atendía a todo el personal de la Compañía.



Figura 3.5a: Central Telefónica PANASONIC EMSS 336 KX-T336100

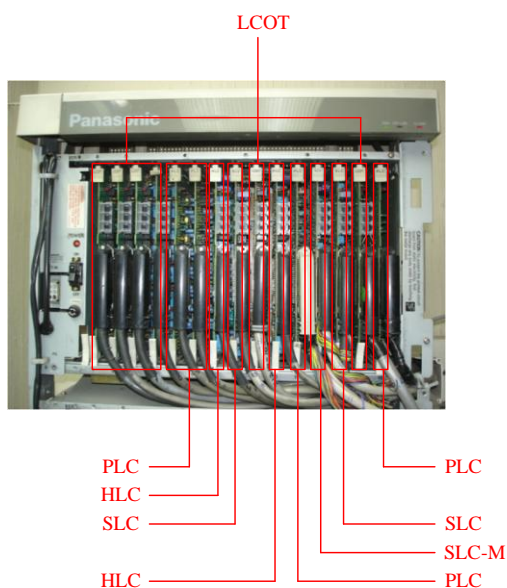


Figura 3.5b: Tarjetas de la Central Telefónica PANASONIC (Panel Superior)

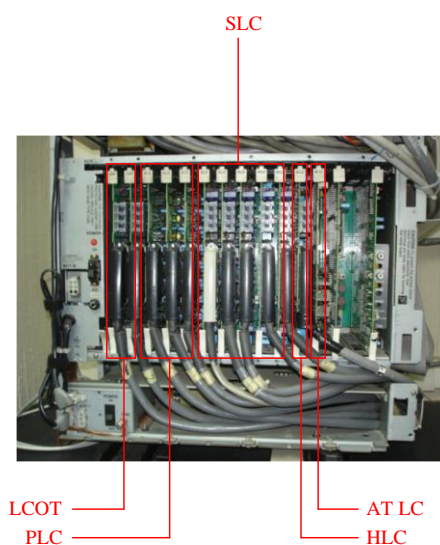


Figura 3.5c: Tarjetas de la Central Telefónica PANASONIC (Panel Inferior)

3.1.2.1.4 Bastidores, Paneles de Interconexión y Dispositivos de Red

Existen tres bastidores en el Cuarto de Telecomunicaciones del noveno piso. La Figura 3.6 muestra el primero donde existen 5 paneles de interconexión de 48 puertos (4 SOUTH HILLS DATACOM y 1 PANDUIT) que sirven para administrar los puntos de datos que corresponden a la mitad superior del edificio (pisos 6, 7, 8, 9 y 10). De igual manera, están colocados 5 paneles de interconexión de 48 puertos (4 MOD-TAP y 1 PANDUIT) que se

utilizan para organizar las extensiones y líneas directas de la central telefónica PANASONIC.

Se cuenta con un panel adicional de 48 puertos (MOD-TAP) donde se conectan las líneas telefónicas de las bases celulares entre los puertos 1 a 24 y los restantes manejan extensiones. Los dos paneles de interconexión (PANDUIT) siguientes controlan únicamente extensiones. En el último panel de interconexión (PANDUIT) se distribuyen las líneas urbanas a los usuarios. Al final de este bastidor están colocados 8 bloques de conexión de 25 pares cada uno que reciben las 171 líneas urbanas asignadas por la PSTN (Public Switched Telephone Network), las mismas que están instaladas en el Punto de Demarcación de la Planta Baja.

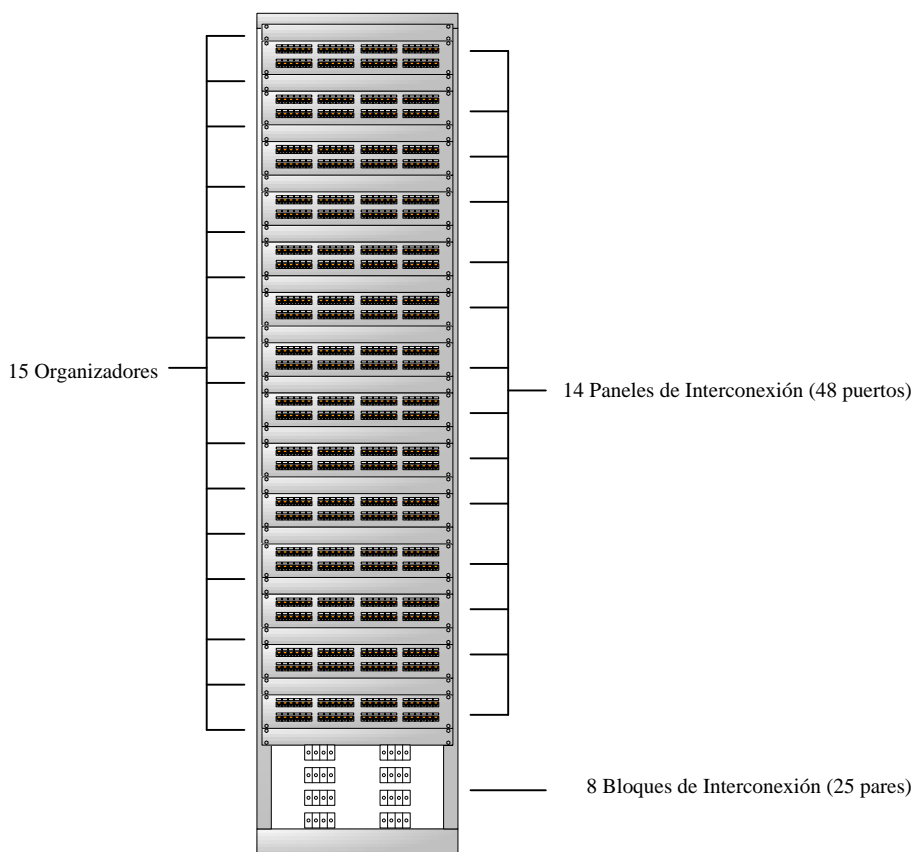


Figura 3.6: Bastidor de Paneles de Interconexión de Voz y Datos

El bastidor contiguo que se muestra en la Figura 3.7 alberga los conmutadores que controlan el tráfico generado por los usuarios ubicados entre el sexto y décimo pisos. En la parte superior existe una multitoma (8 tomacorrientes) que suministra energía a estos

dispositivos. El primer conmutador (A) es un equipo Cisco Catalyst 2950 de 24 puertos 10Base-T/100Base-TX. Los dos siguientes conmutadores (B y C) son dispositivos 3Com 3300 SuperStackII de 24 puertos 10/100Base-TX cada uno (Figura 3.8a). El cuarto y quinto conmutador (D y E) son equipos Cisco Catalyst 2960 que tienen 24 puertos 10Base-T/100Base-TX, 2 puertos 10Base-T/100Base-TX/1000Base-T y 2 ranuras de expansión SFP (Small Form-Factor Pluggable).

Aunque los dos conmutadores siguientes (F y G) son Cisco Catalyst 2950 de 24 puertos 10Base-T/100Base-TX, solamente el dispositivo F cuenta con 2 puertos 1000Base-SX adicionales (Figura 3.8b). El siguiente conmutador (H) es un Cisco Catalyst 2960 con las mismas características que los equipos D y E. El noveno conmutador (I) pertenece a la familia Cisco Catalyst 3500 que tiene 24 puertos 10Base-T/100Base-TX y dos ranuras de expansión para módulos GBIC (Gigabit Interface Converter). El último conmutador es un 3Com SuperStack II XM de 24 puertos 10/100Base-TX (Figura 3.8c).

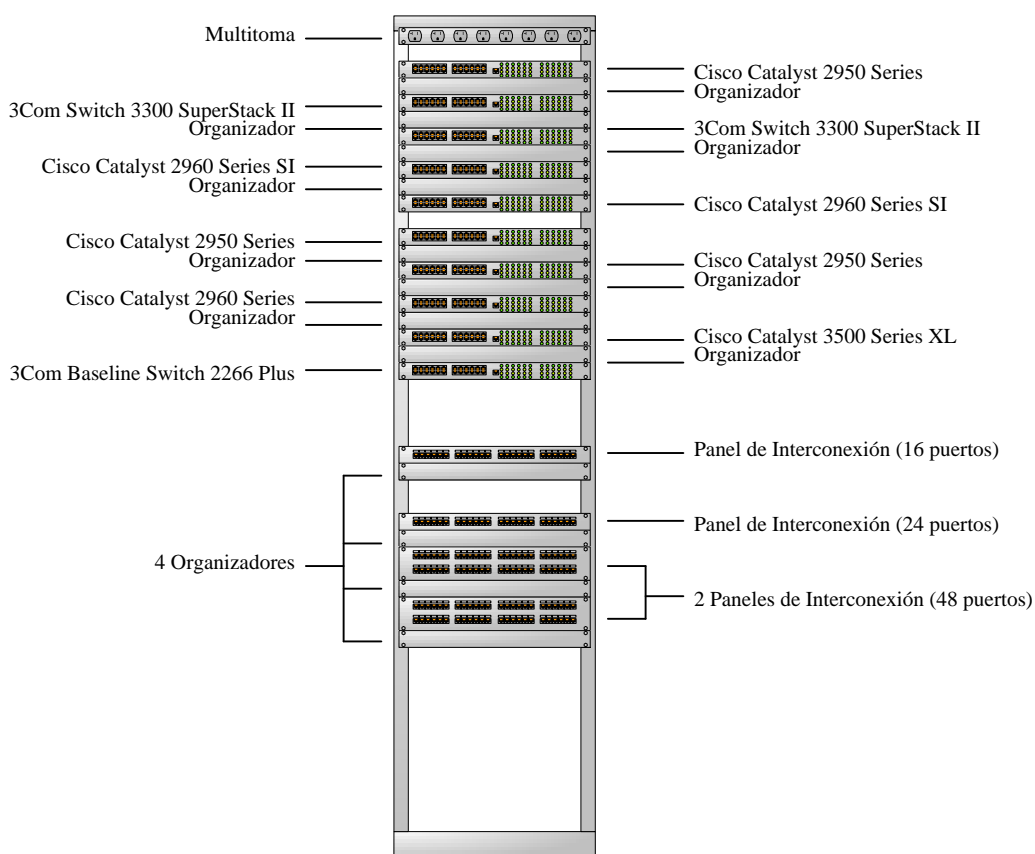


Figura 3.7: Bastidor de Conmutadores y Paneles de Interconexión



Figura 3.8a: Conmutadores A, B y C

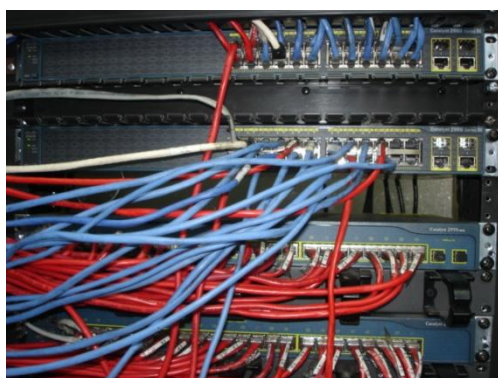


Figura 3.8b: Conmutadores D, E, F y G

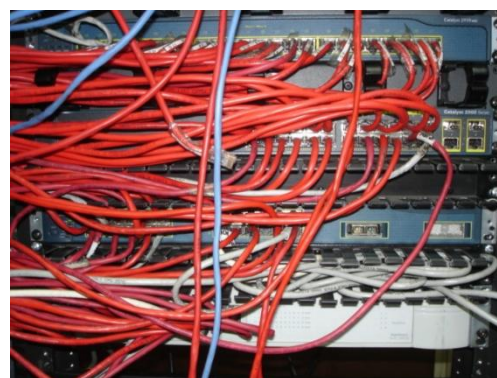


Figura 3.8c: Conmutadores G, H, I y J

La marca, modelo, número de serie, dirección MAC (Media Access Control) y versión del sistema operativo de los conmutadores del Cuarto de Telecomunicaciones del noveno piso se listan en la Tabla 3.2. El dispositivo principal del Cuarto de Telecomunicaciones del noveno piso es el Cisco Catalyst 3500, al cual se conectan los demás conmutadores. En la Figura 3.9 se especifican las marcas, modelos, puertos disponibles e interconexiones de estos equipos. La Figura 3.10 muestra las conexiones del conmutador principal hacia los pisos que disponen de un conmutador por ala, paneles de interconexión y demás dispositivos de Capa 2 colocados en dicho cuarto.

Marca	Modelo		Número de Serie	Dirección MAC	Versión
Cisco	Catalyst 2950 Series	WS-C2950-24	FOC0842Z4DN	00:12:7F:18:C6:80	12.1 (22) EA1
3Com	3Com Switch 3300	3C16980	0602/7ZNV3EA28F8	00:D0:96:EA:28:F8	-
3Com	3Com Switch 3300	3C16980	0602/7ZNV4B56358	00:30:1E:B5:63:58	-
Cisco	Catalyst 2960 Series SI	WS-C2960-24TC-S V01	FOC1203Z4G0	00:1F:27:AD:A6:00	12.2 (37) EY
Cisco	Catalyst 2960 Series SI	WS-C2960-24TC-S V01	FOC1203Z4CS	00:1F:27:27:A5:00	12.2 (37) EY
Cisco	Catalyst 2950 Series	WS-C2950SX-24	FOC1035Z0N2	00:19:2F:FC:A9:C0	12.1 (22) EA8
Cisco	Catalyst 2950 Series	WS-C2950-24	FOC0842Y48S	00:12:7F:1C:28:40	12.1 (22) EA1
Cisco	Catalyst 2960 Series	WS-2960-24TC-L V03	FOC1142U2AW	00:1E:14:91:87:80	12.2 (35) SE5
Cisco	Catalyst 3500 Series XL	WS-C3524-XL-EN	FAB0532U1PS	00:07:0E:DB:DC:80	-
3Com	3Com Switch 3300	3C16985	0102/7N4V46E65D8	00:30:1E:6E:65:D8	-

Tabla 3.2: Conmutadores del Cuarto de Telecomunicaciones del Noveno Piso

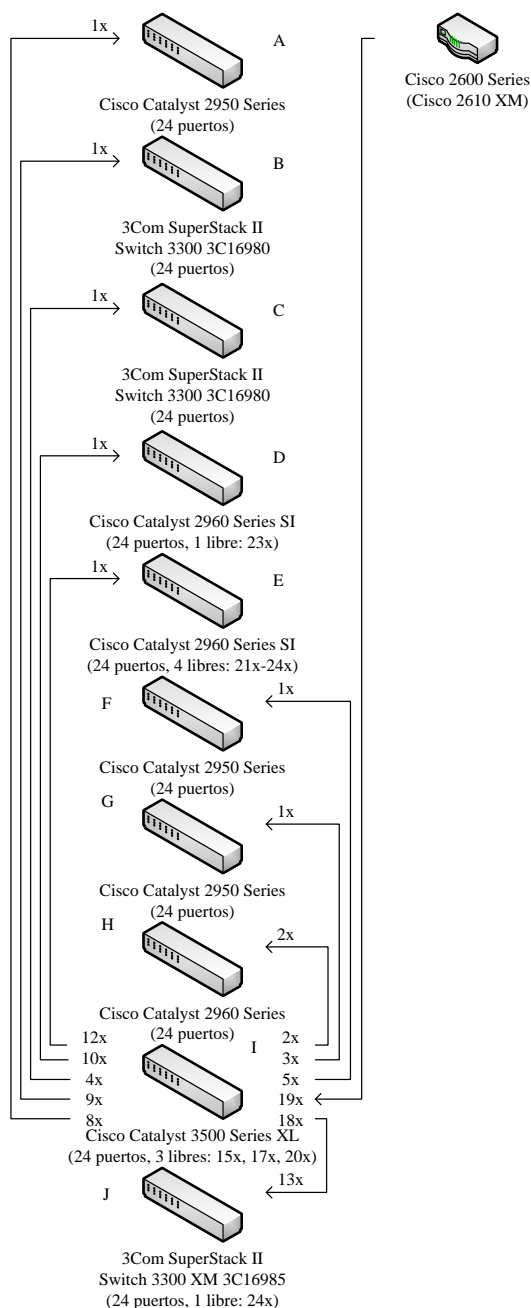
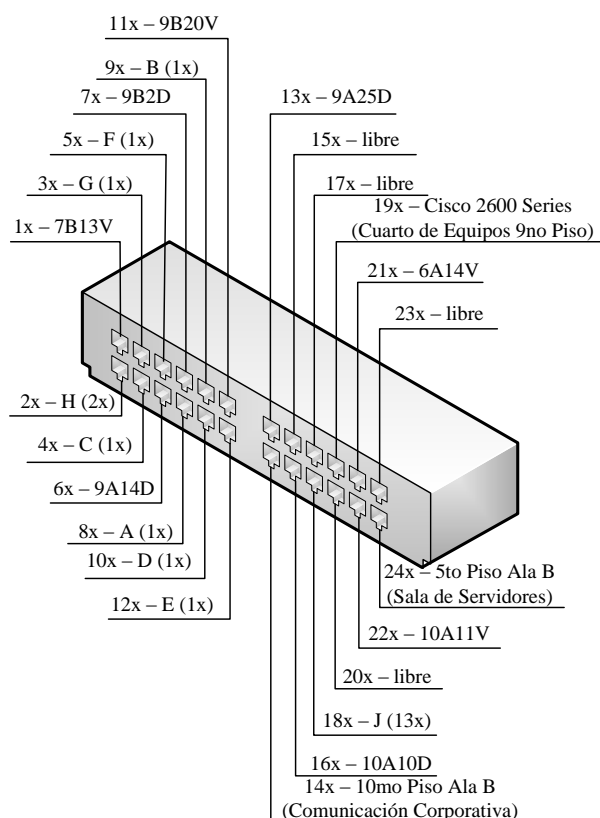


Figura 3.9: Interconexiones de los Conmutadores del Noveno Piso



Cisco Catalyst 3500 Series XL
(24 puertos, 3 libres: 15x, 17x, 20x)

Figura 3.10: Conexiones del Conmutador Principal del Noveno Piso

En la parte media de este bastidor está colocado un panel de interconexiones de 16 puertos (QUEST), de los cuales únicamente se utilizan el 1 y 2 para el doble enlace Fast Ethernet con la Sala de Servidores. En la parte inferior existe un panel de interconexión QUEST de 24 puertos destinado para extensiones ejecutivas de la central telefónica SIEMENS que pertenecen a los usuarios de los pisos 6, 7 y 8. Los dos paneles de interconexión QUEST (de 24 puertos cada uno) restantes manejan extensiones simples de la misma central. Entre el primero y segundo bastidor existen 3 regletas KRONE (Figura 3.11) que interconectan las centrales telefónicas SIEMENS y PANASONIC. La comunicación entre las centrales telefónicas del noveno y quinto pisos se realiza mediante cuatro enlaces que manejan troncales y extensiones como se muestra en la Figura 3.12.

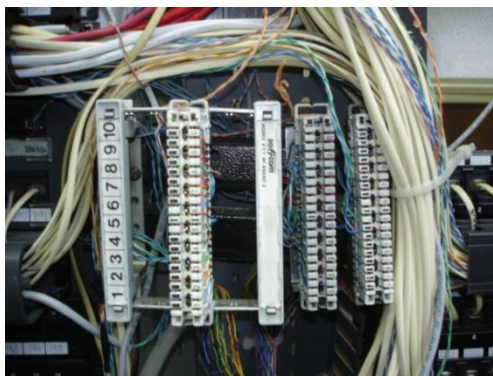


Figura 3.11: Regletas KRONE para Interconexión de las Centrales Telefónicas

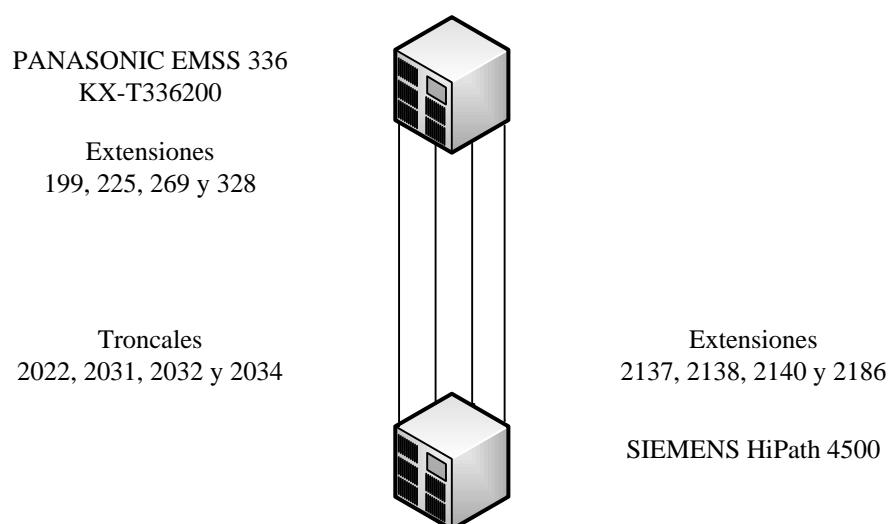


Figura 3.12: Troncales y Extensiones entre las Centrales Telefónicas

Las Figuras 3.13a y 3.13b muestran el tercer bastidor donde existe otra multitoma (8 tomacorrientes) y un enrutador Cisco 2600 XM al cual se conectan 15 módems HAYES ACURA V.92 modelo 15328, los cuales permiten que los usuarios de las Subestaciones accedan a los recursos de la red mediante conexiones Dial-Up. Además existen 5 bases celulares ERICSSON G36a que se conectan a la central telefónica PANASONIC y 2 TECOM Sony Ericsson GR48 que se conectan directamente a usuarios en varios departamentos (Figuras 3.14a y 3.14b).

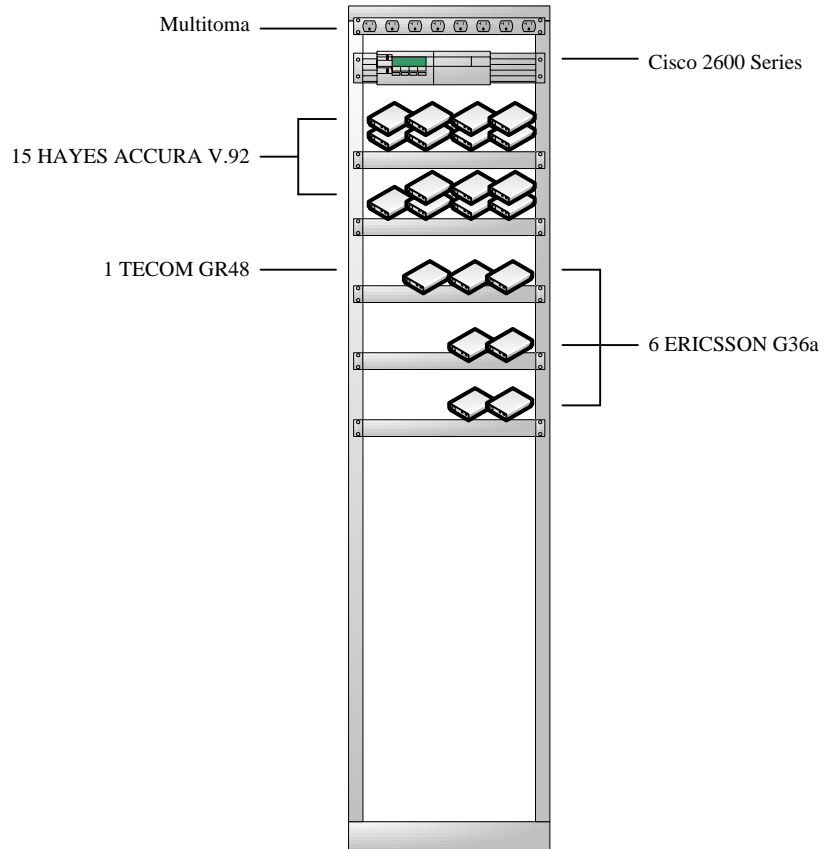


Figura 3.13a: Bastidor del Enrutador, Módems y Bases Celulares



Figura 3.13b: Bastidor del Enrutador, Módems y Bases Celulares (Vista Lateral)



Figura 3.14a: Bases Celulares TECOM

Figura 3.14b: Bases Celulares ERICSSON

3.1.2.1.5 Cables de Interconexión, Organizadores y Canaletas

Los cables de interconexión utilizados entre los paneles y conmutadores están fabricados con cable UTP Categoría 5e, conectores RJ-45 y capuchones. La distribución de hilos sigue el estándar ANSI/TIA/EIA 568-B. La longitud de estos cables varía según la distancia que separa los elementos activos y pasivos. Los cables telefónicos utilizan cable de 4 hilos y conectores RJ-11. Ambos tipos de cables siguen las trayectorias creadas mediante organizadores y canaletas pero algunos se conectan directamente como se observa en la Figura 3.15.

Los paneles de interconexión destinados para datos y voz del primer bastidor cuentan con etiquetas impresas en computador que son legibles. Mientras que en los paneles utilizados para conectar las bases celulares, extensiones y líneas urbanas existen etiquetas escritas a mano (Figura 3.16). En el bloque de conexiones que enlaza las centrales telefónicas con las líneas urbanas no existe identificación alguna. La mayoría de cables de interconexión no tienen etiqueta en los extremos y algunos poseen un identificador escrito con marcador indeleble.

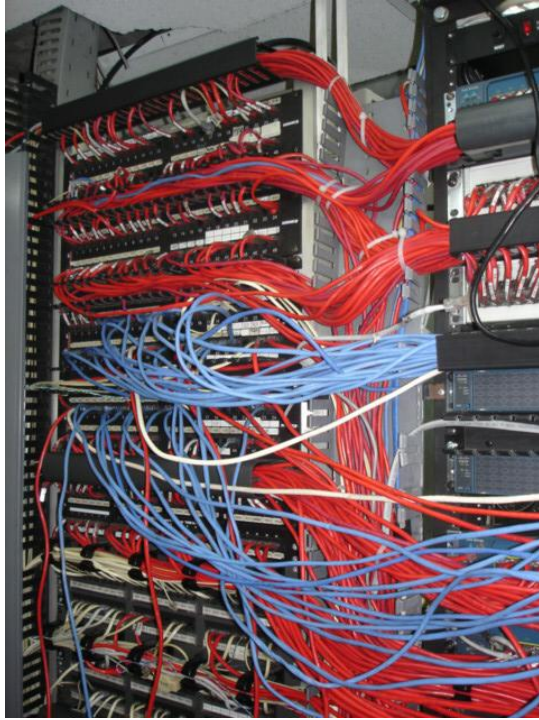


Figura 3.15: Cables de Interconexión, Organizadores y Canaletas

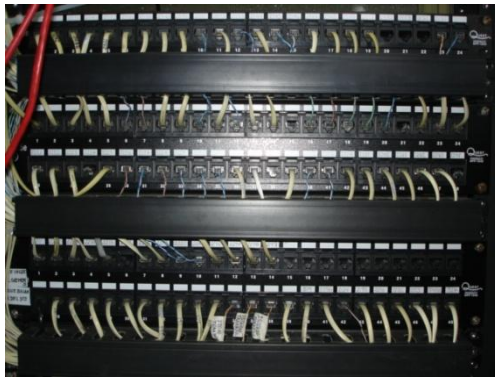


Figura 3.16: Paneles de Interconexión para Bases Celulares y Líneas Telefónicas

3.1.2.2 Quinto Piso

3.1.2.2.1 Dimensiones y Equipamiento

A causa del incremento de usuarios, se adecuó un segundo Cuarto de Telecomunicaciones en el quinto piso. Al igual que en el noveno piso, las paredes frontales son de madera y vidrio (Figura 3.17). El piso es de cemento y está cubierto por parquet. El techo está formado por láminas de cielo raso y varias luminarias. La distancia aproximada desde el piso al techo es 2,38 metros.



Figura 3.17: Puerta de Ingreso del Cuarto de Equipos del Quinto Piso

3.1.2.2.2 Mobiliario, Control de Temperatura y Suministro de Energía

En la Figura 3.18 se especifican las dimensiones de esta área así como la distribución de los equipos. La puerta de ingreso tiene doble cerradura y las llaves están custodias por las mismas personas mencionadas anteriormente. En la parte posterior existe una ventana (1,50 x 1,49 metros) y un equipo de aire acondicionado LG (Figura 3.19), el mismo que conserva la temperatura en 22 °C. En el extremo derecho del cuarto está colocado un banco de baterías de 48 voltios marca EVER EXXEED (Figura 3.20), un cargador de baterías CELCO PP-48V-300A (Figura 3.21) y dos inversores AC/DC (uno de marca CDP y otro TRIPP-LITE), los cuales trabajan en conjunto para alimentar a los equipos de telecomunicaciones del CGTT.

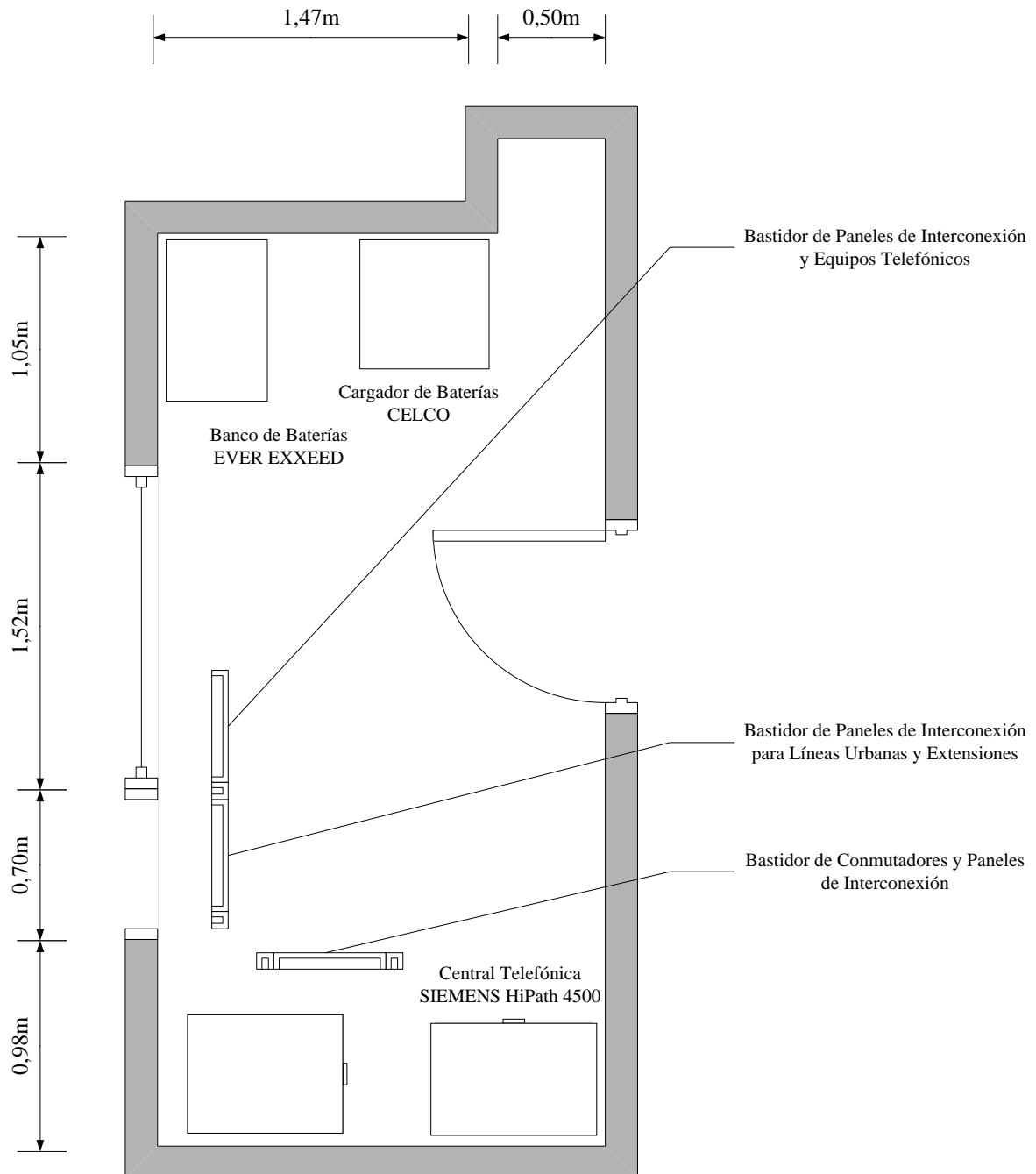


Figura 3.18: Cuarto de Equipos del Quinto Piso



Figura 3.19: Aire Acondicionado LG



Figura 3.20: Banco de Baterías



Figura 3.21: Cargador de Baterías

3.1.2.2.3 Central Telefónica

En el extremo izquierdo se ubica la central telefónica SIEMENS HiPath 4500 (Figuras 3.22a y 3.22b y 3.22c), la cual atiende a los usuarios entre la Planta Baja y el noveno piso y que en un futuro reemplazará a la central telefónica PANASONIC cuando la migración se complete.



Figura 3.22a: Central Telefónica SIEMENS HiPath 4500

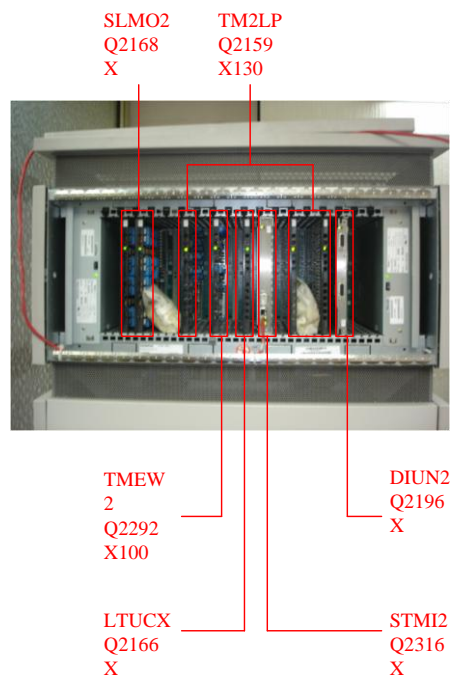


Figura 3.22b: Tarjetas de la Central Telefónica SIEMENS (Panel Superior)

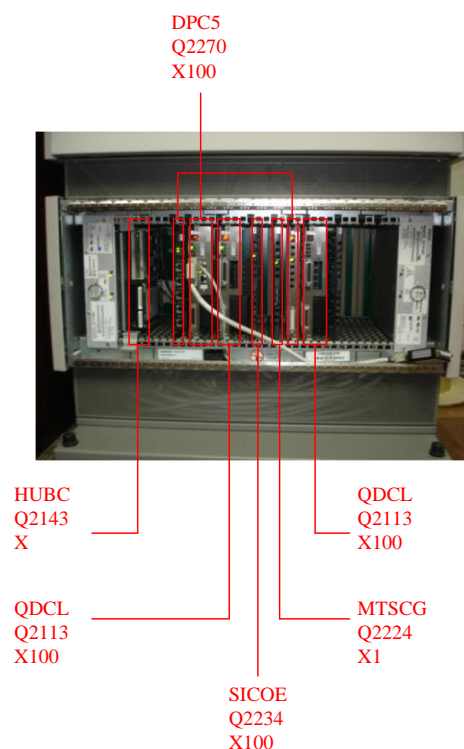


Figura 3.22c: Tarjetas de la Central Telefónica SIEMENS (Panel Inferior)

3.1.2.2.4 Bastidores, Paneles de Interconexión y Dispositivos de Red

En el centro de la habitación se encuentran tres bastidores. En el primero, que se muestra en la Figura 3.23, están colocados los conmutadores y paneles de interconexión que comunican a los usuarios de la parte inferior del edificio (Planta Baja y pisos 1, 2, 3, 4 y 5). En la parte superior de este bastidor existe una multitoma (8 tomacorrientes) que provee energía a los dispositivos. El primer conmutador (B) es un Cisco Catalyst 3500 de 24 puertos 10Base-T/100Base-TX y dos ranuras de expansión GBIC. El siguiente (C) es un conmutador Cisco Catalyst 2950 de 24 puertos 10Base-T/100Base-TX.

El tercero (D) es un conmutador 3Com SuperStack III de 24 puertos 10/100Base-TX. Después está un panel de interconexión PANDUIT de 24 puertos (Figura 3.24a). Un panel (PANDUIT) de 16 puertos se ubica en la posición siguiente. El cuarto conmutador (A) es un Cisco Catalyst 2960 que tiene 24 puertos 10Base-T/100Base-TX, 2 puertos 10Base-T/100Base-TX/1000Base-T y 2 ranuras de expansión SFP. El próximo conmutador (E) es un Cisco Catalyst 2950 de 24 puertos 10Base-T/100Base-TX y 2 puertos 1000Base-SX (Figura 3.24b).

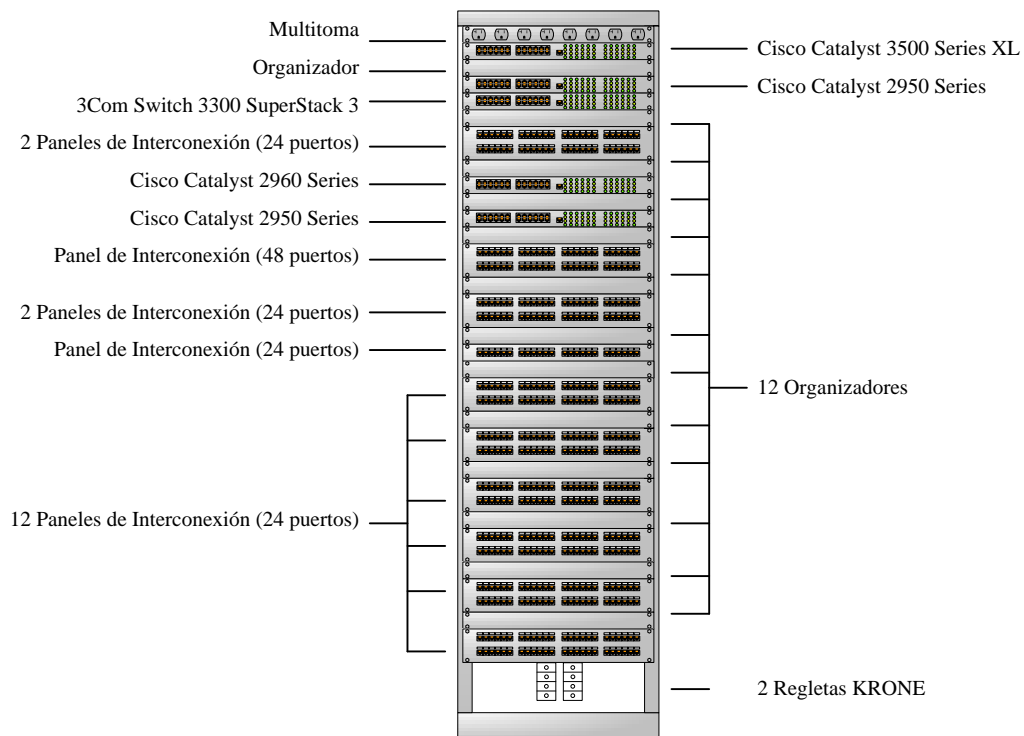


Figura 3.23: Bastidor de Conmutadores y Paneles de Interconexión



Figura 3.24a: Conmutadores B, C y D



Figura 3.24b: Conmutadores A y E

La Tabla 3.3 detalla la marca, modelo, número de serie, dirección MAC, versión del sistema operativo y cantidad de puertos de los conmutadores del Cuarto de Telecomunicaciones del quinto piso. Dos paneles de interconexión MOD-TAP de 24 puertos cada uno e identificados con las siglas PP2 ocupan los espacios siguientes. Un panel de interconexión de 48 puertos junto con uno de 24 puertos se pueden reconocer

mediante las etiquetas PP3 y PP4-5Av, respectivamente. Luego están colocados dos paneles PANDUIT de 24 puertos (5Bv y 4Bv).

Tres paneles NEWLINK de 24 puertos vienen a continuación (3Bv, 3Av y PBBD 7A-D). El siguiente es un panel PANDUIT de 24 puertos con etiqueta PBBV/7B”A”v. Después están instalados dos paneles QUEST de 24 puertos (2Bv y PBBV). Desde el panel de interconexión PP3 hasta el PBBV se manejan puntos de datos y voz (líneas directas y extensiones). Esta serie de elementos pasivos termina con dos paneles de interconexión NEXXT de 24 puertos. Al final de este bastidor se encuentran 2 regletas KRONE que también manejan líneas directas y extensiones.

Marca	Modelo		Número de Serie	Dirección MAC	Versión
Cisco	Catalyst 3500 Series XL	WS-C3524-XL-EN	FAB0532U1P9	00:07:0E:DC:55:00	-
Cisco	Catalyst 2950 Series	WS-2950-24	FOC0842Y48W	00:12:7F:18:FD:40	12.1 (22) EA1
3Com	3Com Switch 3300	3C16980A	04027MMV7EDA098	00:0A:04:ED:A0:98	-
Cisco	Catalyst 2960 Series	WS-C2960-24TC-L V02	FOC1121Z4WU	00:1C:0F:BA:FE:80	12.2 (25) SEE3
Cisco	Catalyst 2950 Series	WS-C2950SX-24	FOC1043Z9TP	00:19:E7:7D:94:80	12.1 (22) EA8a

Tabla 3.3: Conmutadores del Cuarto de Telecomunicaciones del Quinto Piso

Los dispositivos de red del Cuarto de Telecomunicaciones del quinto piso se conectan al conmutador Cisco Catalyst 3500 tal y como se indica en la Figura 3.25. En la Figura 3.26 se puede observar las conexiones del equipo principal hacia los pisos que cuentan con conmutador por ala, paneles de interconexión y demás dispositivos de Capa 2 instalados en el cuarto.

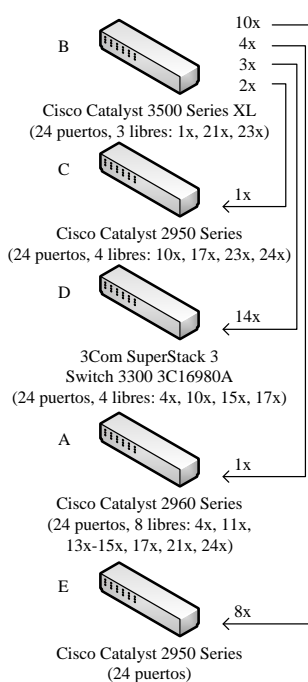
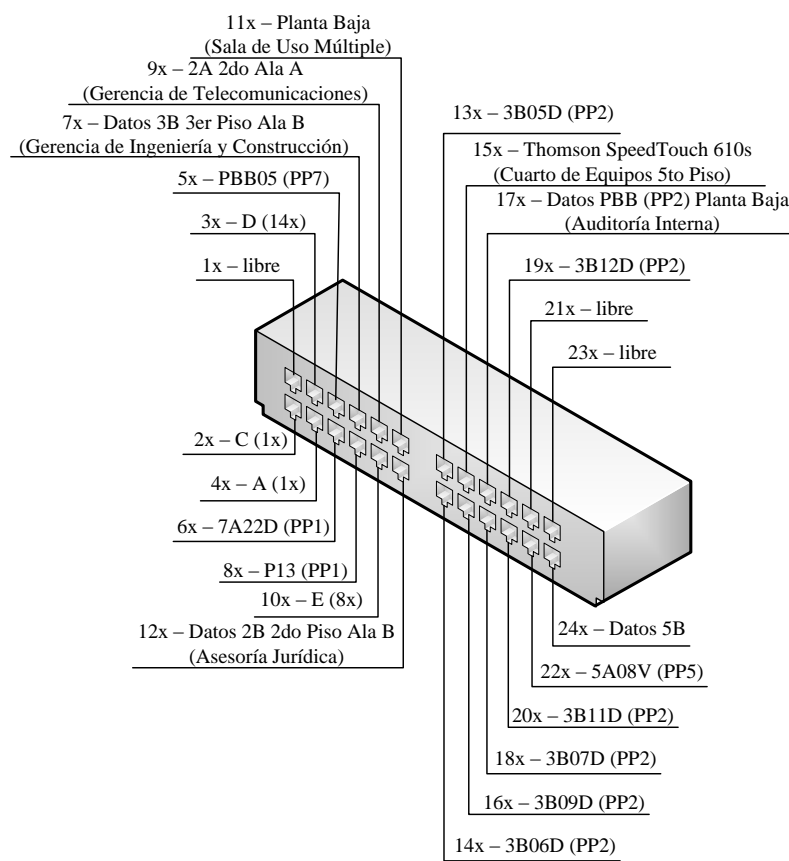


Figura 3.25: Interconexiones de los Conmutadores del Quinto Piso

B



Cisco Catalyst 3500 Series XL
(24 puertos, 3 libres: 1x, 21x, 23x)

Figura 3.26: Conexiones del Conmutador Principal del Quinto Piso

La Figura 3.27 muestra el segundo bastidor donde están los paneles de interconexión de las líneas urbanas y extensiones de la central SIEMENS. Al inicio se dispone de una multitoma (8 tomacorrientes) para alimentar los dispositivos activos del bastidor adjunto. Un par de paneles de interconexión PANDUIT (PP9) de 24 puertos cada uno controlan los grupos de extensiones 2501-2523 (ejecutivas) y 2101-2124 (simples). El siguiente par de 24 puertos se encarga del grupo de extensiones simples 2125-2148 y líneas troncales. El panel que viene después maneja 48 troncales en sus puertos. Los dos paneles siguientes controlan 3 grupos de extensiones ejecutivas: 2524-2547, 2548-2571 y 2572-2595.

Luego se encuentran tres paneles adicionales a los cuales se conectan 5 grupos de extensiones simples 2149-2172, 2173-2196, 2197-2220, 2221-2244 y 2245-2268 y 2269-2292. La primera mitad del siguiente panel de 48 puertos maneja el grupo de extensiones simples 2245-2268 mientras que la segunda tiene extensiones ejecutivas que se conectan a la central PANASONIC. Los dos últimos paneles de 48 puertos tienen extensiones simples que se dirigen hacia el Cuarto de Telecomunicaciones del noveno piso.

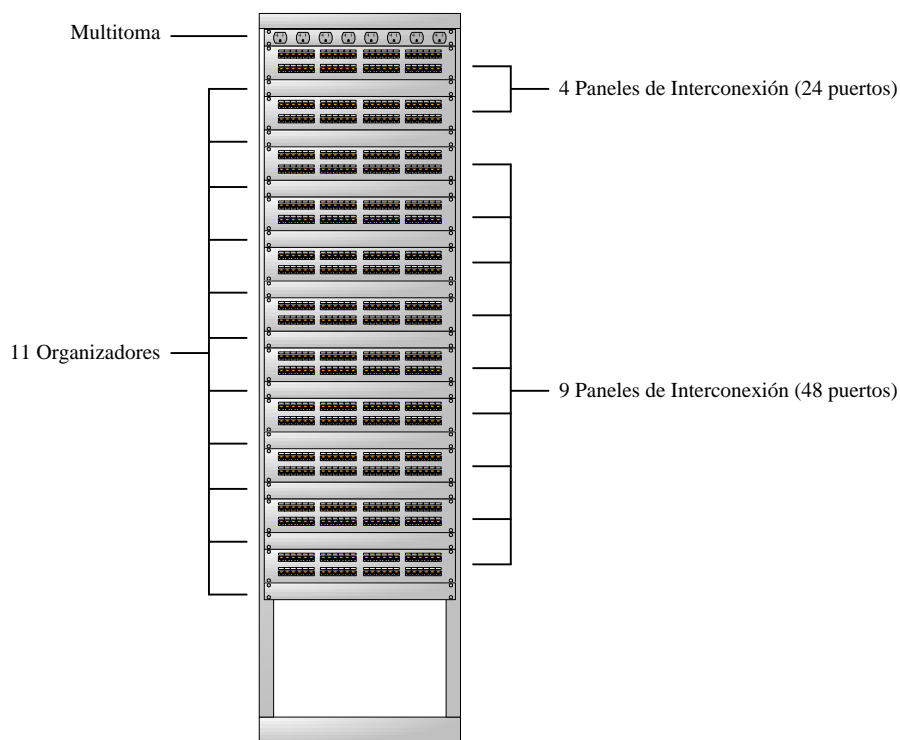


Figura 3.27: Bastidor de Paneles de Interconexión para Líneas Urbanas y Extensiones

En el tercer bastidor que se muestra en la Figura 3.28a se cuenta con otra multitoma (8 tomacorrientes) y un panel de interconexión de 24 puertos que recibe el doble enlace Fast Ethernet de la Sala de Servidores y conecta tres líneas telefónicas que pertenecen a las Subestaciones Santa Rosa, Pomasqui y Calderón. Además existe un equipo ITS Telecom VME Pro-Voice Mail System que maneja el correo de voz (Figura 3.28b). En las siguientes bandejas se encuentra un dispositivo de VoIP de marca Multi Tech Systems modelo Multi VoIP Voice/Fax over IP Networks y 2 bases celulares ERICSSON y 4 TECOM (Figura 3.28c).

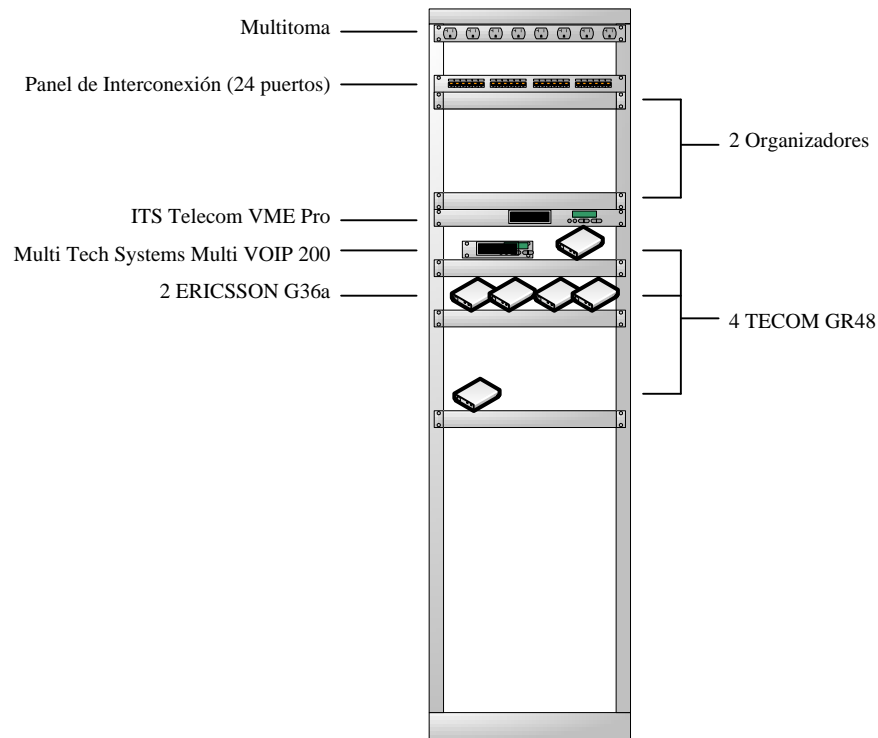


Figura 3.28a: Bastidor de Paneles de Interconexión y Equipos Telefónicos



Figura 3.28b: Voice Mail System



Figura 3.28c: Bases Celulares

3.1.2.2.5 Cables de Interconexión, Organizadores y Canaletas

Los cables de interconexión entre elementos activos y pasivos del primer bastidor cuentan con etiquetas generadas por computador que identifican el puerto del conmutador o panel al cual están conectados. La codificación inicial de los paneles de interconexión fue impresa con el número de piso y ala respectiva seguido del nombre del punto (V/D

para voz o datos). En algunos casos se ha creado un distintivo con cinta adhesiva y marcador indeleble (Figura 3.29).

Los conmutadores se han rotulado con el rango de letras A-E. Tanto organizadores como canaletas permiten guiar los cables de interconexión entre conmutadores y paneles. En la Figura 3.30 se observan pares de cable UTP descubiertos para instalaciones de voz y regletas KRONE como sustituto de los paneles de interconexión. Las etiquetas del segundo bastidor han sido escritas con esferográfico o marcador permanente. Al igual que en el caso anterior, una serie de organizadores y canaletas establecen las trayectorias para los cables.

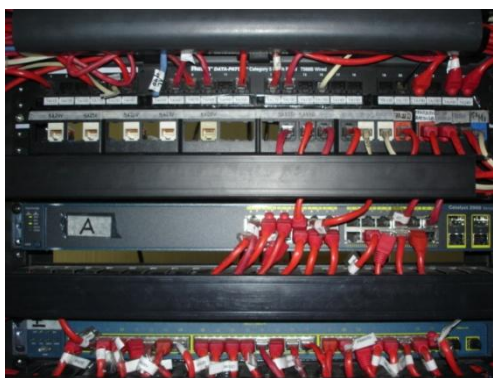


Figura 3.29: Codificación de los Paneles de Interconexión



Figura 3.30: Regletas KRONE en reemplazo de Paneles de Interconexión

3.1.3 Cuartos de Telecomunicaciones y Sala de Servidores

La comunicación entre los Cuartos de Telecomunicaciones y la Sala de Servidores, la misma que está controlada por el Departamento de Informática, se logra mediante dos

pares de enlaces Fast Ethernet. Los usuarios deben atravesar un Firewall para acceder a cualquier recurso de la red. Tres redes de servidores (172.16.2.0/23, 100.0.0.0/8 y 208.19.64.0/26) se enlazan al Firewall a través de un par de conmutadores.

La conexión a Internet se realiza mediante un enrutador Cisco 800 (INTERNET_TE) que tiene cuatro interfaces LAN asociadas a una VLAN (FE0-FE3) y una interfaz WAN (FE4). Los conmutadores principales (Cisco Catalyst 3500) de los Cuartos de Telecomunicaciones se conectan al Firewall y éste a la interfaz FE0 del dispositivo de Capa 3. La interfaz FE4 se conecta al enrutador del proveedor (TNX). La Figura 3.31 muestra las conexiones entre los Cuartos de Telecomunicaciones, la Sala de Servidores y el CGTT.

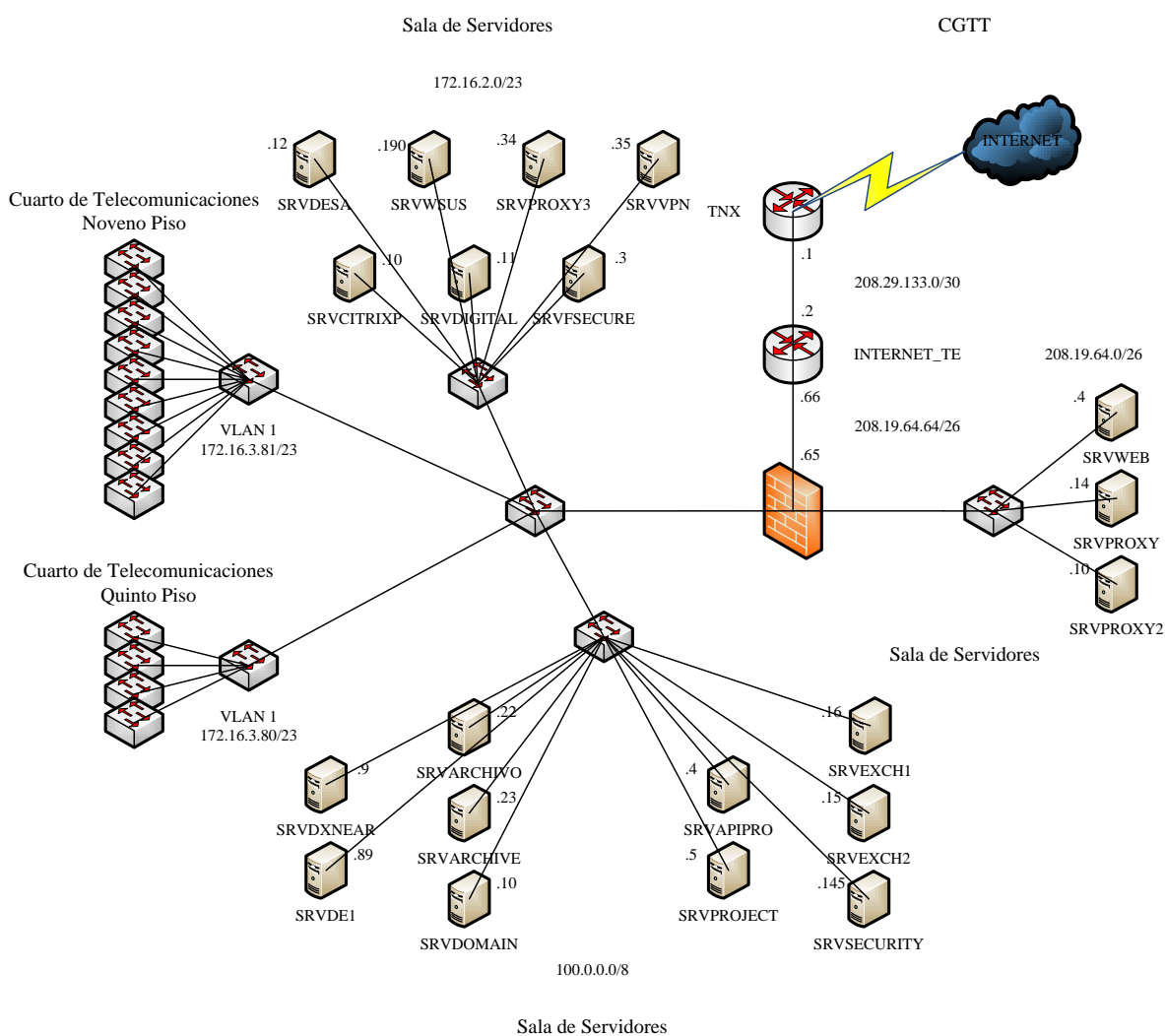


Figura 3.31: Conexiones entre los Cuartos de Telecomunicaciones, la Sala de Servidores y el CGTT

3.1.4 Cableado Horizontal y Áreas de Trabajo

En la Figura 3.32 se muestra el cableado horizontal que se ha tendido en cada ala. Sobre el centro del techo falso existen bandejas metálicas que se dividen en tres secciones. El cable UTP Categoría 5e sigue estas trayectorias y desciende por canaletas plásticas hasta llegar a los cajetines que cuentan con conectores RJ-45 hembra y están ubicados en las Áreas de Trabajo. Para conectar los dispositivos de usuario final se utilizan cables de interconexión que tienen una longitud aproximada de 3 metros y la distribución de hilos cumple con el estándar ANSI/TIA/EIA 568-B.

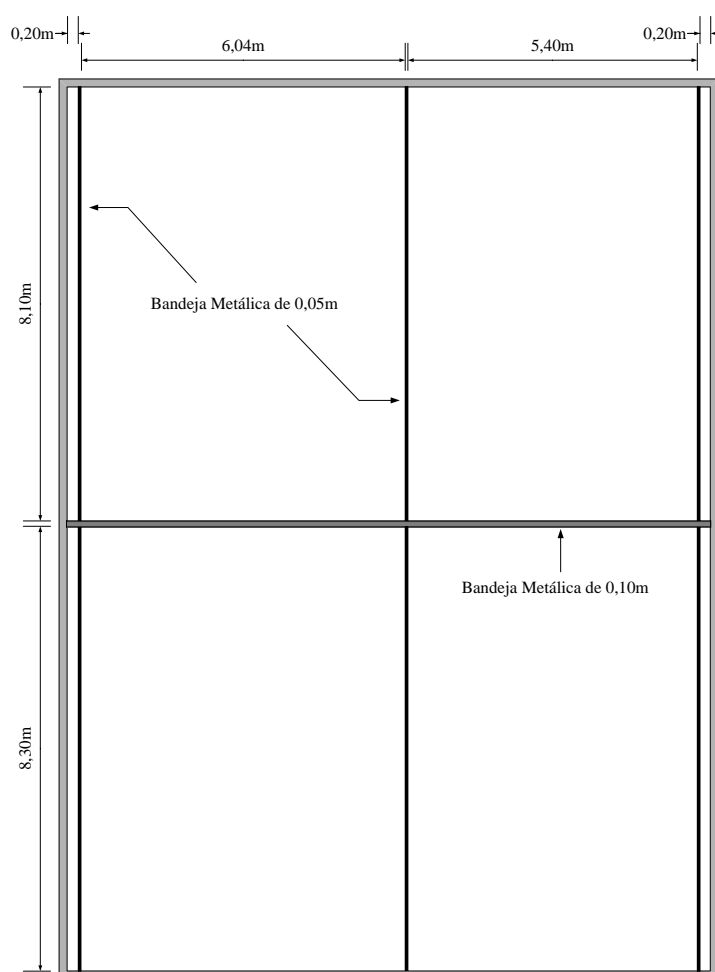


Figura 3.32: Cableado Horizontal por Ala

3.1.5 Cableado Vertical y Dispositivos por Ala

En varios pisos se ha instalado un conmutador por ala. La seguridad de estos dispositivos está limitada a cajas metálicas y la fuente de poder a un tomacorriente regular.

Para las conexiones hacia los Cuartos de Telecomunicaciones se utiliza un par de cables cruzados (uno para el enlace principal y otro de reserva) Categoría 5e o 6 que siguen una trayectoria vertical creada por tuberías PVC (Polyvinyl Chloride) de 2 pulgadas (5,08 centímetros).

En aquellos lugares donde se ha colocado un armario de pared, se cuenta con un panel de interconexión para enlazar los puertos del conmutador y las secciones del cableado horizontal. Mientras que en el resto de pisos se tienden una serie de cables directos desde el Cuarto de Telecomunicaciones hasta el cajetín del usuario. La Tabla 3.4 detalla la marca, modelo y cantidad de puertos de los conmutadores administrables instalados en cada ala. Las Figuras 3.33a y 3.33b muestran la distribución de los puntos de acceso inalámbricos y conmutadores que existen en cada ala.

Piso	Marca	Modelo	Cantidad de Puertos
Décimo	D-Link	DES 1024R	24
Tercero	D-Link	DES-1016D	16
Segundo	Cisco	Catalyst 2960 Series	24
	Cisco	Catalyst 2900 Series	24
Planta Baja	Cisco	Catalyst 2950 Series	24
	3Com	3Com 3300	24

Tabla 3.4: Conmutadores instalados en cada Ala

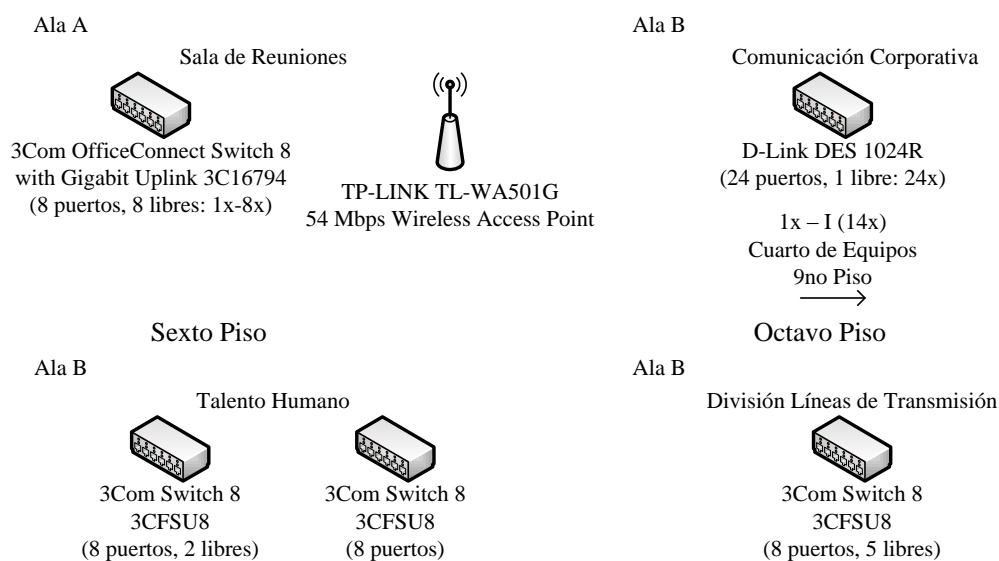


Figura 3.33a: Puntos de Acceso Inalámbricos y Conmutadores por Ala (Pisos 10, 8 y 6)

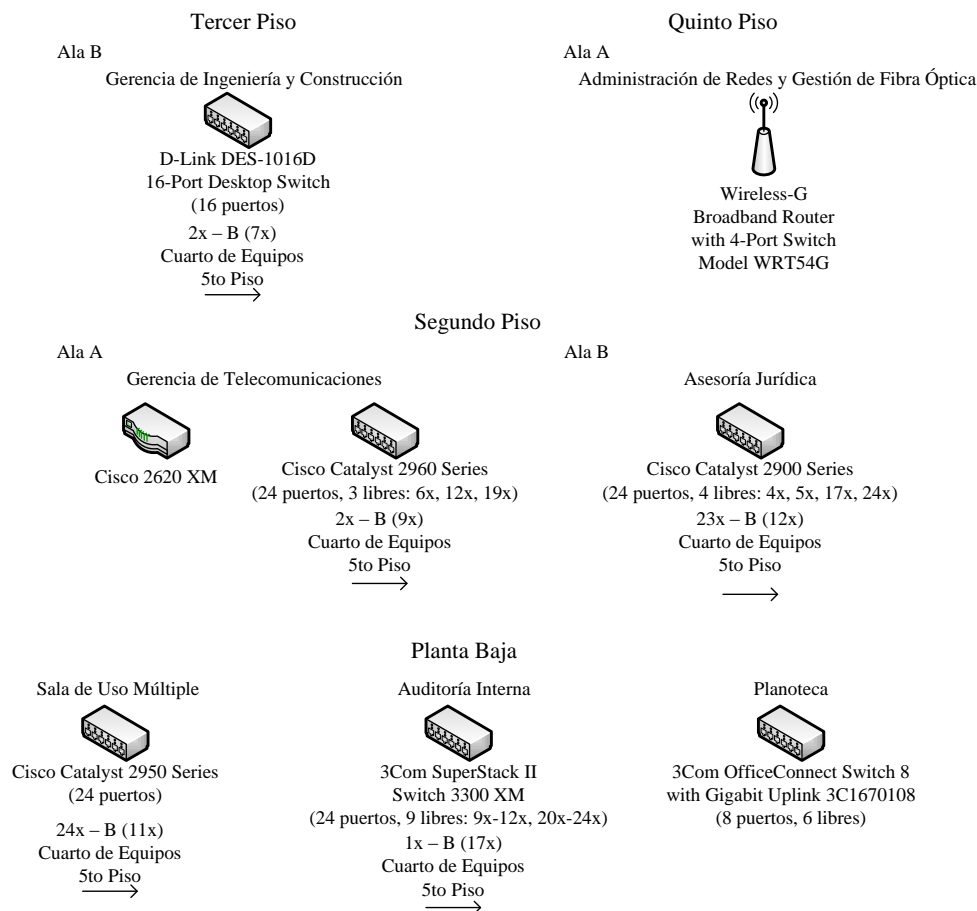


Figura 3.33b: Puntos de Acceso Inalámbricos y Conmutadores por Ala (Pisos 5, 3, 2 y Planta Baja)

3.1.5.1 Conmutadores Administrables

Las Figuras 3.34a y 3.34b muestran el conmutador de la Sala de Uso Múltiple (Planta Baja, Ala B), el cual tiene solamente dos etiquetas para identificar los cables que se dirigen hacia el Cuarto de Telecomunicaciones del quinto piso. Ninguno de los paneles de interconexión tiene distintivos para ubicar los cajetines en la habitación. El conmutador de Auditoría Interna (Planta Baja, Ala A) está montado en un bastidor de pared descubierto que tiene tres paneles de interconexión y no existe manera de reconocer ningún cable de interconexión pues no están marcados (Figura 3.35).

La Gerencia de Telecomunicaciones (Segundo Piso, Ala A) es el único sitio donde se ha colocado un armario de pared abatible BEAUCOUP que contiene un conmutador y cuatro paneles de interconexión para voz y datos. Los organizadores no abastecen completamente

para acomodar los cables de interconexión y los identificadores fueron creados a mano (Figuras 3.36a y 3.36b).



Figura 3.34a: Caja Metálica PBA



Figura 3.34b: Conmutador
Sala de Uso Múltiple



Figura 3.35: Conmutador Auditoría Interna



Figura 3.36a: Armario 2A

Figura 3.36b: Conmutador
Gerencia de Telecomunicaciones

En las Figuras 3.37a y 3.37b se observa que los cables de interconexión del conmutador instalado en el Departamento de Asesoría Jurídica (Segundo Piso, Ala B) no disponen de identificadores y tan solo un grupo reducido de puertos de los paneles están etiquetados. En la División de Mantenimiento de Líneas de Transmisión (Tercer Piso, Ala B) existe un bastidor descubierto con dos paneles de interconexión que no tienen instalados todos los conectores RJ-45 hembra y una cinta adhesiva indica los cajetines que están habilitados. Dos regletas KRONE permiten interconectar los puntos de voz y la central telefónica (Figura 3.38). Por último, el dispositivo ubicado en Comunicación Corporativa (Décimo Piso, Ala B) no tiene codificación alguna, excepto por el cable de interconexión que llega al Cuarto de Telecomunicaciones del noveno piso y ciertos puertos destinados para extensiones telefónicas (Figuras 3.39a y 3.39b).



Figura 3.37a: Caja Metálica 2B



Figura 3.37b: Conmutador Asesoría Jurídica



Figura 3.38: Conmutador de la División de Mantenimiento de Líneas de Transmisión

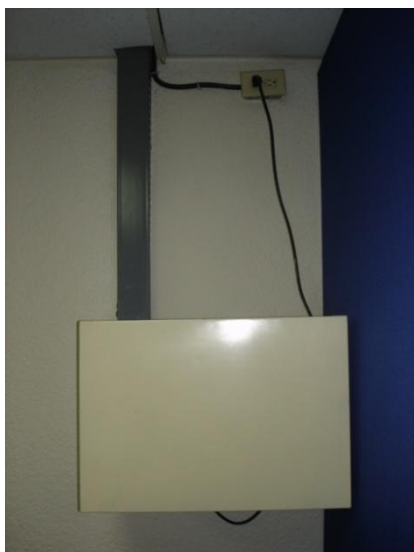


Figura 3.39a: Caja Metálica 10B



Figura 3.39b: Conmutador
Comunicación Corporativa

3.1.5.2 Conmutadores No Administrables

A fin de incorporar nuevos usuarios a la red, se han instalado conmutadores no administrables como una solución temporal en ciertas áreas de la Compañía. Tanto en la Sala de Reuniones del Directorio (Décimo Piso, Ala A) como en la Planoteca (Planta Baja, Ala B) existe un conmutador 3Com OfficeConnect Switch 8 with Gigabit Uplink 3C16794 (Figuras 3.40a y 3.40b). En la División de Líneas de Transmisión (Octavo Piso, Ala B) y

en Talento Humano (Sexto Piso, Ala B) están en uso tres conmutadores 3Com Switch 8 3CFSU8 (Figuras 3.41a y 3.41b).



Figura 3.40a: Conmutador Sala de Reuniones



Figura 3.40b: Conmutador Planoteca



Figura 3.41a: Conmutador
Líneas de Transmisión



Figura 3.41b: Conmutador
Talento Humano

3.1.6 Número de Usuarios

Para determinar el número de usuarios que existen en la Compañía se llevó a cabo una inspección física en cada uno de los pisos que conforman el edificio. Con la ayuda de los planos arquitectónicos y una base de datos impresa que detallaba la codificación de los puntos de voz y datos en todas las áreas se verificó su existencia y funcionamiento. En la Tabla 3.5 se muestra un resumen de este proceso. Cabe indicar que en el Ala Oriental del cuarto piso no se dispone de datos, ya que dicha área es propiedad de la empresa TERMOPICHINCHA.

Piso	Ala	Voz	Datos
Décimo	A	21	20
	B	21	21
Noveno	A	37	28
	B	29	21
Octavo	A	19	19
	B	19	19
Séptimo	A	29	29
	B	24	21
Sexto	A	32	27
	B	27	24
Quinto	A	23	27
	B	22	37
Cuarto	A	-	-
	B	13	13
Tercero	A	29	29
	B	26	26
Segundo	A	31	30
	B	23	20
Planta Baja	A	14	17
	B	22	49
Total		461	477

Tabla 3.5: Número de Usuarios de la red LAN

3.1.7 Sistemas Empresariales

A fin de establecer una relación entre los sistemas empresariales y las personas que utilizan dichos recursos se realizó encuestas en cada departamento. La descripción de los sistemas empresariales y sus módulos se presenta desde la Tabla 3.6a hasta la 3.6g. Dada la gran cantidad de trabajadores fue necesario seleccionar una muestra de 5 sujetos por ala. Los resultados de esta investigación se presentan de manera condensada en la Tabla 3.7.

Sistema	Módulo	Descripción
Xnear CRM Workflow		Herramienta para diseño de flujos de trabajo.
	Solicitud de Pago	Permite el manejo del procedimiento para generar anticipos 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 copagos (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 el 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.	

Tabla 3.6a: Sistema Empresarial Xnear CRM Workflow

Sistema	Módulo	Descripción
Flexline ERP		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 la mantención del inventario y los diferentes 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 3.6b: Sistema Empresarial Flexline ERP

Sistema	Módulo	Descripción
APIPRO		Sistema para Gestión de Mantenimiento.
	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 anexas todo tipo de documentación técnica electrónica a actividades de mantenimiento y, en general, a la estructura de planta.
	Interfase PALM	Permite la utilización de Handhelds tipo palm para registrar en sitio y offline la inspección y el reporte de trabajos; posteriormente esta información se integra al sistema.
	Importación/exportación	Permite importar y exportar diversos tipos 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	Proporciona una interfaz "viva" gráfica para acceder a información de APIPRO a través de planos y dibujos de equipos e instalaciones en general.	

Tabla 3.6c: Sistema Empresarial APIPRO

Sistema	Módulo	Descripción
Project Server	Project Server	Herramienta para Manejo Empresarial de Proyectos.
	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 Web que permite realizar el seguimiento y reporte de proyectos publicados, bajo diferentes perfiles de usuario, entre ellos el ejecutivo.
	Windows Share Point Services	Plataforma Microsoft para habilitar el manejo documental de MS-Project Server.

Tabla 3.6d: Sistema Empresarial Project Server

Sistema	Módulo	Descripción
Evolution		Sistema para Gestión de Personal.
	Recursos Humanos	Permite administrar el recurso humano de TRANSELECTRIC S.A. (capacitación, competencias, beneficios, acciones laborales, ropa de trabajo, evaluación, reclutamiento y 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 crear usuarios, perfiles y asignar permisos.
	E-business	Permite al personal de TRANSELECTRIC S.A. consultar vía internet la información histórica de ficha personal, roles de pago, bienes asignados, permisos y vacaciones.
	Evolution Reporter	Permite al usuario diseñar reportes personalizados acordes a sus necesidades.

Tabla 3.6e: Sistema Empresarial Evolution

Sistema	Módulo	Descripción
Portal Web		Portal Web de TRANSELECTRIC S.A.
	Administración de seguridad	Permite la creación de usuarios, roles y asignación de permisos a los menús, secciones y contenido del Portal Web.
	Administración de contenido	Permite la actualización (añadir, eliminar, cambiar) del contenido del Portal Web.
	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.

Tabla 3.6f: Sistema Empresarial Portal Web

Sistema	Módulo	Descripción
Otros	SISAFO	Sistema que maneja la información de los activos en operación (activos sin tenencia), altas, bajas, transferencias y depreciaciones.
	PRESUPUESTO REFERENCIAL	Sistema para Administrar equipos del SNT y formular presupuestos referenciales 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.
	CALIFICACION DE PROVEEDORES	Sistema que permite calificar a los proveedores registrados a través del Portal Web de acuerdo a ciertos criterios.
	INTRANET	Portal Web interno de 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 S.A. por concepto de transporte de energía y servicios de Telecomunicaciones.

Tabla 3.6g: Otros Sistemas Empresariales

Piso	Sistema Empresarial						
	Xnear CRM Workflow	Flexline ERP	APIPRO	Project Server	Evolution	Portal Web	Otros
Décimo	4	1	0	0	5	1	5
Noveno	4	0	0	2	5	2	5
Octavo	4	0	1	3	5	2	5
Séptimo	4	0	5	5	5	1	5
Sexto	3	3	0	0	5	1	5
Quinto	-	-	-	-	-	-	-
Cuarto	3	0	0	0	3	0	3
Tercero	5	0	2	3	4	0	5
Segundo	4	2	2	2	5	1	5
Planta Baja	1	2	2	0	1	0	5
Total	32	8	12	15	38	8	43

Tabla 3.7: Sistemas Empresariales y Usuarios

La Figura 3.42 muestra que los sistemas empresariales “Xnear CRM Workflow”, “Evolution” y el conjunto catalogado como “Otros” son utilizados por la mayoría de colaboradores que desarrollan sus actividades entre el segundo y décimo pisos. Además, el

“Project Server” únicamente se emplea en los grupos de pisos 7-9 y 2-3. En el sexto piso existe una demanda promedio respecto al “Flexline ERP”. Mientras que el “APIPRO” es un recurso altamente utilizado por quienes laboran en el séptimo piso. En la Figura 3.43 se puede apreciar la totalidad de usuarios de cada sistema empresarial.

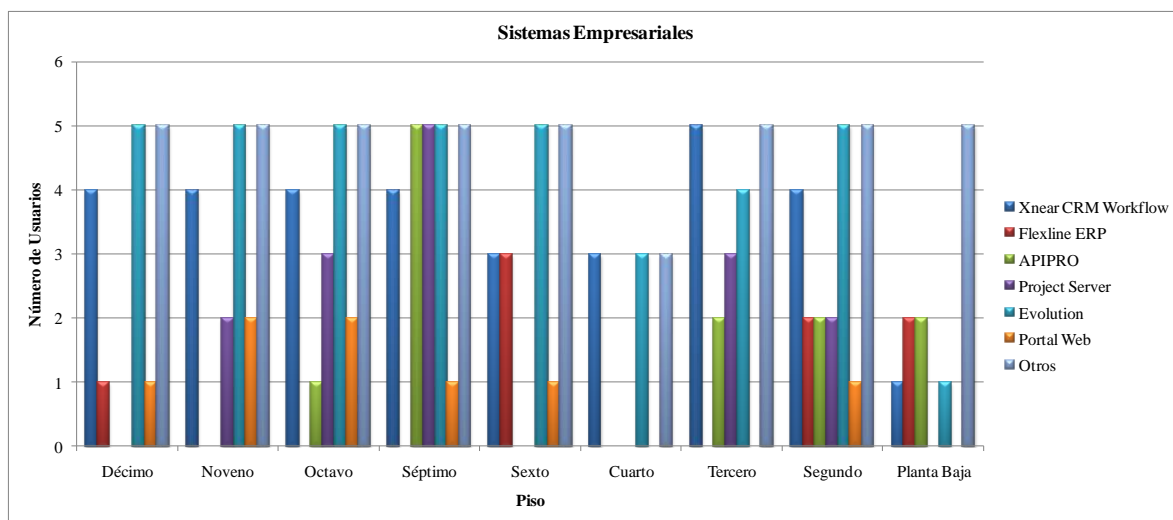


Figura 3.42: Sistemas Empresariales y Número de Usuarios por Piso

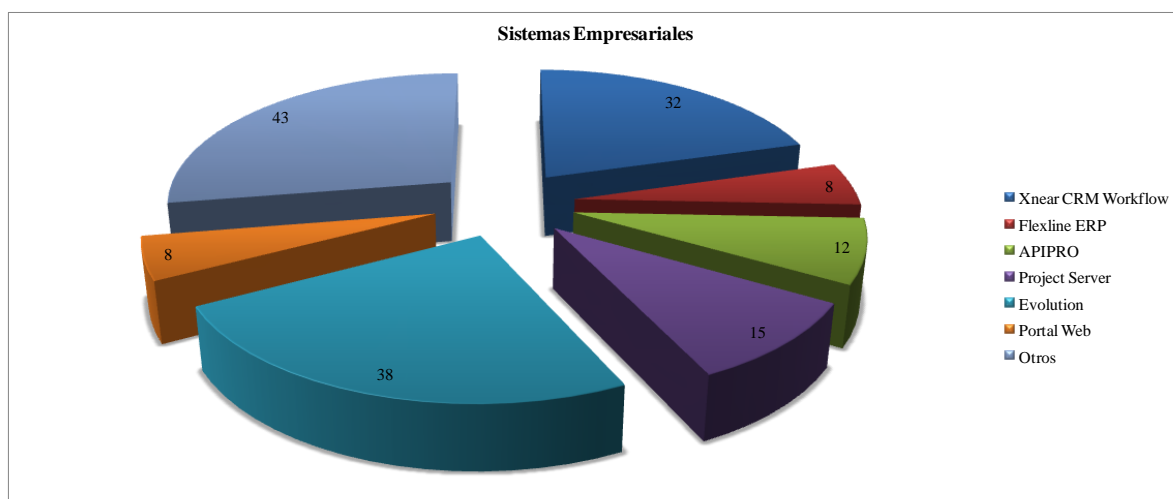


Figura 3.43: Total de Usuarios de cada Sistema Empresarial

3.1.8 Tráfico y Ancho de Banda

Para realizar el análisis de tráfico y medición del ancho de banda fue necesario configurar los conmutadores principales de los Cuartos de Telecomunicaciones para que una interfaz registre el tráfico de todos los usuarios de la red. Primero se verificó que todas las notificaciones SNMP (Simple Network Management Protocol) se encuentren habilitadas. Luego se ejecutó el comando `port monitor identificador de la interfaz` en los puertos 24 y 15 de los conmutadores Cisco Catalyst 3500 ubicados en el quinto y noveno pisos, respectivamente. Aprovechando la existencia de 2 puntos de red en el CGTT se realizaron las conexiones pertinentes.

3.1.8.1 Análisis de Tráfico

La herramienta que se empleó para capturar los paquetes que circulan por la red fue el Wireshark versión 1.0.4, en el cual basta con seleccionar la NIC (Network Interface Card) del dispositivo para que se inicie el proceso. La gran cantidad de información transmitida obligó a limitar las capturas a 50000 paquetes, ya que el programa emitía un mensaje de falta de memoria en caso de exceder dicha cantidad.

Los datos sobre tipo y porcentaje de protocolos utilizados se recolectaron entre los días martes 29 de julio y viernes 1 de agosto del año en curso. Con el objeto de registrar la jornada laboral completa se estimó conveniente realizar las capturas en cuatro periodos: 10h00-12h00, 12h00-14h00, 14h00-16h00 y 16h00-18h00. A pesar de que las estadísticas generadas por Wireshark revelaron una diversidad de protocolos que circulan por la red, solamente se examinaron aquellos con un porcentaje representativo. A continuación se describen los protocolos analizados.

3.1.8.1.1 *Capa de Aplicación*

3.1.8.1.1.1 SMB (Server Message Block Protocol)

Es un protocolo de compartición de archivos cliente-servidor. Describe la estructura de los recursos compartidos, tales como directorios, archivos, impresoras y puertos seriales. Los clientes establecen una conexión de largo plazo con los servidores. Cuando la conexión se establece, el cliente puede acceder a los recursos del servidor como si fueran locales. Este protocolo describe el acceso a los sistemas de archivos y la manera en que los clientes pueden solicitar archivos.

Todos los mensajes SMB tienen un formato común que utiliza un encabezado de tamaño fijo seguido de un parámetro y un componente de datos de tamaño variable. Los mensajes SMB pueden iniciar, autenticar y terminar sesiones, controlar el acceso a archivos e impresoras y permitir que una aplicación envíe o reciba mensajes (Figura 3.44).

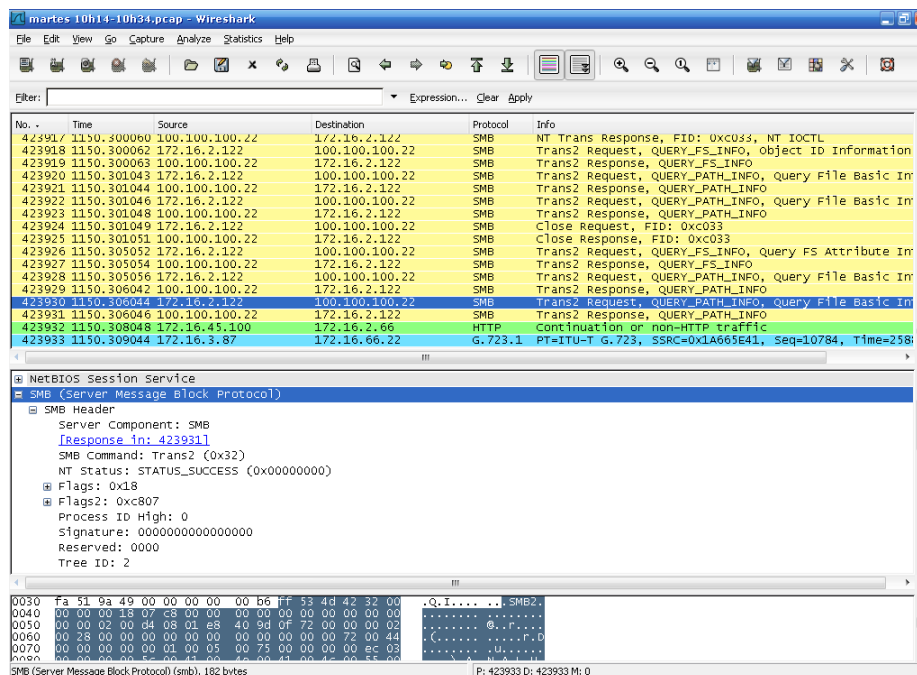


Figura 3.44: Captura del Protocolo SMB

3.1.8.1.1.2 HTTP (Hypertext Transfer Protocol)

Cuando se escribe un URL (Uniform Resource Identifier) en un navegador Web se establece una conexión con un servidor que utiliza el protocolo HTTP. Los navegadores Web son aplicaciones de tipo cliente que se emplean para conectarse a la WWW (World Wide Web) y acceder a los recursos almacenados en un servidor. Los clientes Web establecen conexiones con el servidor y solicitan los recursos. El servidor responde con los recursos y el navegador interpreta la información para presentarla al usuario. Es un protocolo del grupo TCP/IP (Transmission Control Protocol/Internet Protocol) desarrollado para publicar y recuperar páginas HTML (Hypertext Markup Language) y se lo utiliza en sistemas de información distribuidos.

Cuando un cliente envía una solicitud al servidor, el protocolo HTTP define los tipos de mensajes que utiliza el cliente para solicitar una página Web y los que el servidor emplea

para responder. Los tipos de mensajes más comunes son GET, POST y PUT. GET es una solicitud de datos por parte del cliente. Un navegador Web envía este mensaje para solicitar páginas de un servidor. POST y PUT se utilizan para enviar mensajes que cargan información en el servidor. No es un protocolo seguro ya que los mensajes POST cargan información al servidor en texto simple y las respuestas del servidor no están encriptadas. Para comunicaciones seguras en Internet se utiliza el protocolo HTTPS (HTTP Secure) para acceder o publicar información en el servidor. HTTPS utiliza autenticación y encriptación para proteger la información que viaja entre el cliente y el servidor (Figura 3.45).

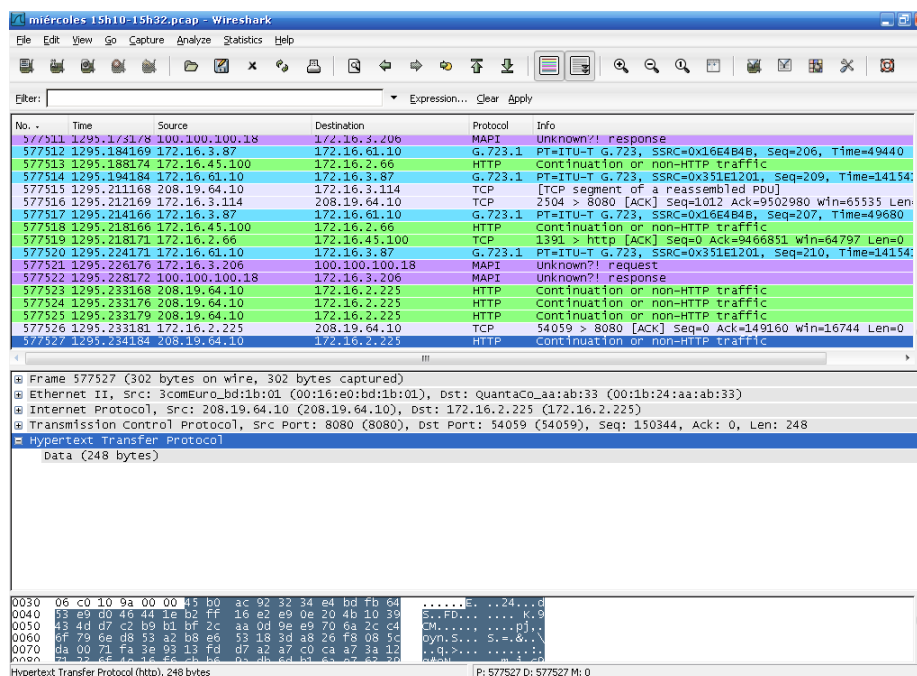


Figura 3.45: Captura del Protocolo HTTP

3.1.8.1.1.3 SNMP (Simple Network Management Protocol)

Es un estándar para administración de redes y sus componentes principales son: agentes, administradores y MIBs (Management Information Bases). Los agentes SNMP son entidades que se encuentran en los dispositivos administrados, reciben mensajes por el puerto 161 y envían notificaciones por el puerto 162. Entre sus funcionalidades están: implementar y mantener los objetos MIB, responder a las operaciones de administración,

generar notificaciones e informes, implementar seguridad y establecer la política de acceso para administradores externos.

Los administradores SNMP son aquellas entidades que interactúan con los agentes y proveen las siguientes funcionalidades: obtener y establecer los valores de las instancias de los objetos MIB en los agentes, recibir notificaciones de los agentes e intercambiar mensajes con otros administradores. Los MIBs contienen las definiciones para los objetos administrados. Una MIB es una descripción de la información del objeto administrado que define su sintaxis y semántica. Los administradores y agentes SNMP intercambian instancias de los objetos administrados utilizando el protocolo SNMP. Los administradores recuperan la información de un agente utilizando operaciones get y modifican los datos del agente utilizando operaciones set (Figura 3.46).

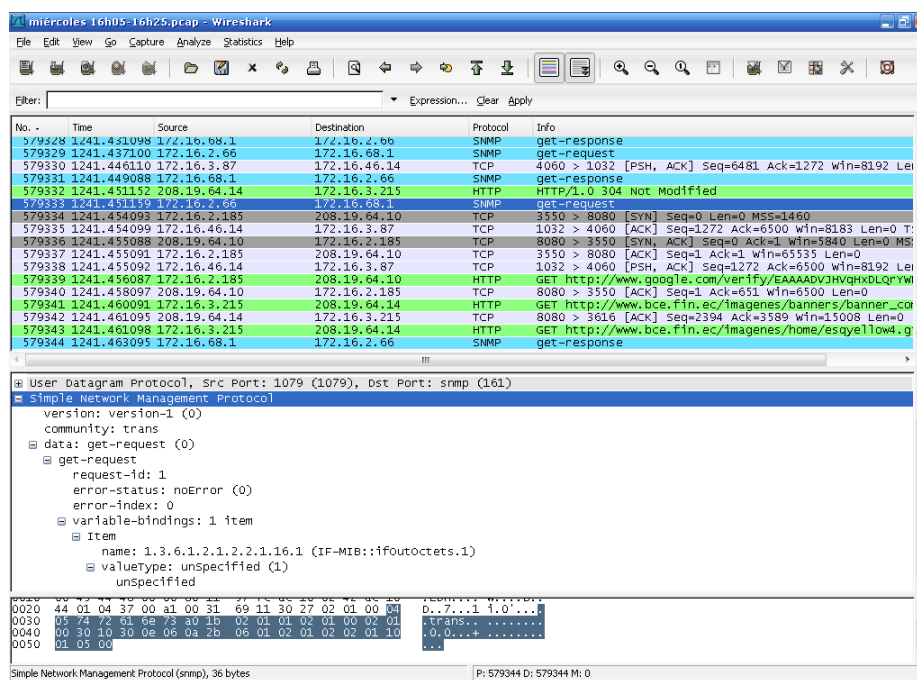


Figura 3.46: Captura del Protocolo SNMP

3.1.8.1.1.4 DNS (Domain Name Service)

Es un servicio cliente-servidor cuya función es resolver nombres de dominio a direcciones, utilizando un conjunto distribuido de servidores para crear una base de datos. Este protocolo define un servicio automatizado que establece correspondencias entre los nombres y las direcciones (Figura 3.47).

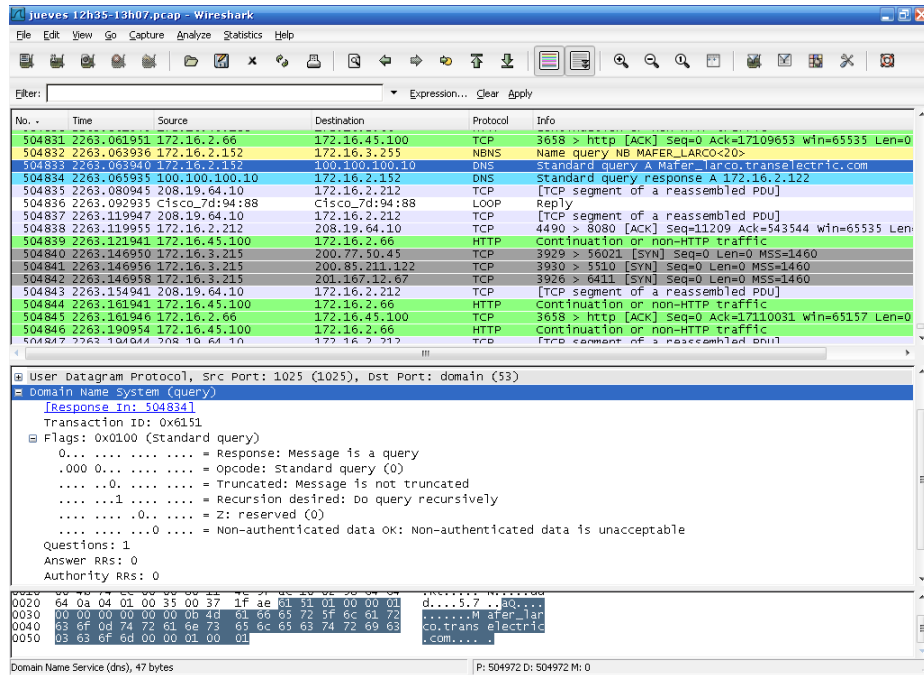


Figura 3.47: Captura del Protocolo DNS

3.1.8.1.2 Capa de Transporte

3.1.8.1.2.1 TCP (Transmission Control Protocol)

Es un protocolo orientado a conexión descrito en el RFC (Request for Comments) 793. TCP agrega sobrecarga para incorporar las siguientes funciones: entrega ordenada, confiabilidad y control de flujo. Las aplicaciones que utilizan TCP son navegadores Web, correo electrónico y transferencia de datos (Figura 3.48).

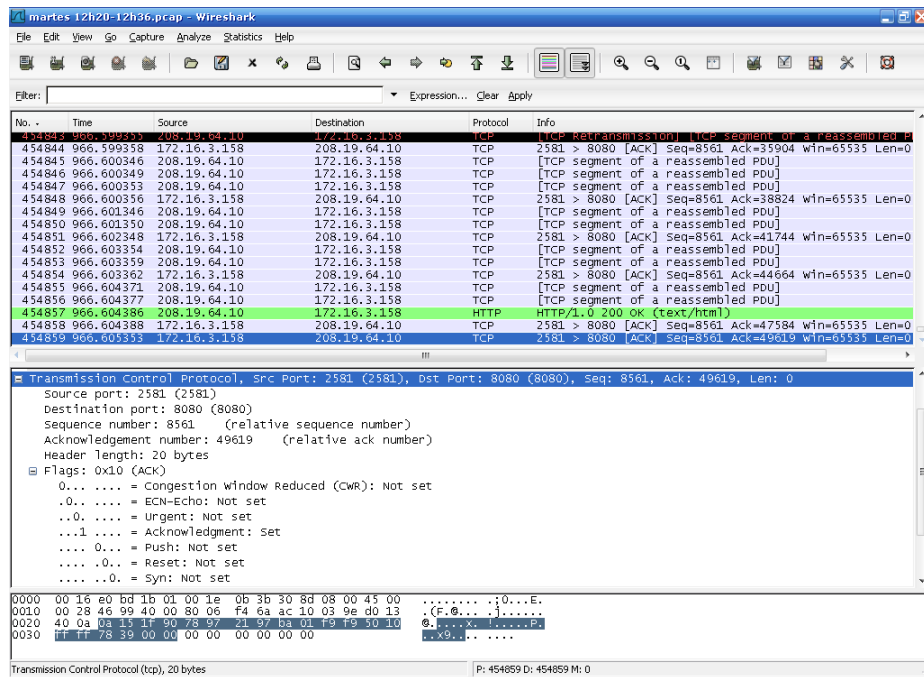


Figura 3.48: Captura del Protocolo TCP

3.1.8.1.2.2 UDP (User Datagram Protocol)

Es un protocolo simple no orientado a conexión descrito en el RFC 768. Tiene la ventaja de entregar información con poca sobrecarga. Las unidades de comunicación en UDP se llaman datagramas, los cuales se envían como mejor esfuerzo (Figura 3.49). Las aplicaciones que utilizan UDP incluyen DNS (Domain Name System), transmisión de video y VoIP (Voice over IP).

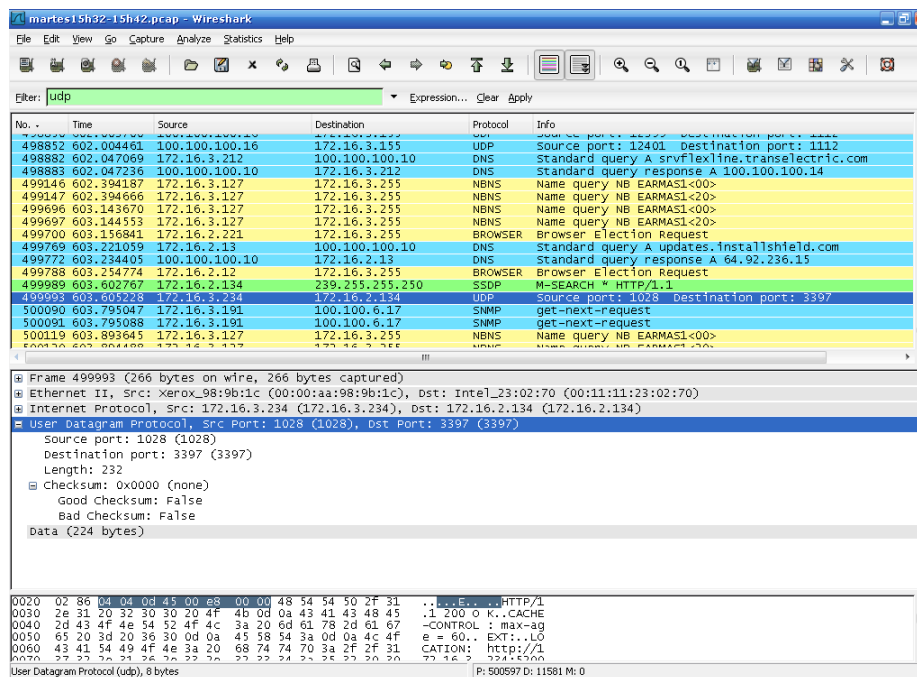


Figura 3.49: Captura del Protocolo UDP

3.1.8.1.3 Capa de Red

3.1.8.1.3.1 IP (Internet Protocol)

Es el único protocolo de Capa 3 utilizado para transportar información de usuario a través de la Internet. IPv6 (Internet Protocol versión 6) se está desarrollando e implementando en ciertas áreas y operará junto con IPv4 en el futuro. IP fue diseñado como un protocolo con baja sobrecarga. Provee solamente las funciones que son necesarias para entregar paquetes a través de un sistema interconectado de redes. Este protocolo no fue diseñado para rastrear y administrar el flujo de paquetes. Las características básicas de IPv4 son:

- **No está orientado a conexión:** Los paquetes IP se envían sin notificar al destino. IP no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes que los paquetes sean enviados y tampoco requiere campos adicionales en el encabezado PDU (Protocol Data Unit) para mantener la conexión. Este proceso reduce considerablemente la sobrecarga. La

entrega de paquetes no orientados a conexión pueden resultar en paquetes que llegan al destino fuera de secuencia.

- **Mejor esfuerzo:** El encabezado IP es más pequeño, requiere menos sobrecarga y existe menos retardo. IP es un protocolo no confiable en el sentido de que no tiene la capacidad de manejar y recuperarse de paquetes no entregados. El encabezado de un paquete IP no incluye campos requeridos para entrega confiable. No existen acuses recibo para entrega de paquetes, control de errores o rastreo de paquetes, por lo que no es posible retransmitir paquetes.
- **Independiente del Medio:** IPv4 e IPv6 operan independientemente del medio que transporta la información. Un paquete IP puede ser comunicado eléctricamente mediante un cable, con señales ópticas a través de fibra o inalámbricamente con señales de radio. La Capa de Enlace de Datos se encarga de llevar un paquete IP y transmitirlo a través del medio.

3.1.8.1.3.2 ICMP (Internet Control Message Protocol)

Los dispositivos de usuario final y enrutadores utilizan este protocolo para comunicar información de Capa 3. Su aplicación más conocida es reporte de errores. Los mensajes ICMP se transmiten como la carga útil de IP. Traceroute está implementado con mensajes ICMP, ya que para determinar las direcciones de los enrutadores que se encuentran entre el origen y el destino, este programa envía una serie de paquetes. El primero tiene un TTL (Time-To-Live) de 1, el segundo de 2, el tercero de 3 y así sucesivamente. Cuando el último paquete llega al enrutador final, éste observa que el TTL ha expirado. El enrutador descarta el paquete y envía un mensaje de advertencia al origen que incluye la dirección IP del enrutador. Cuando este mensaje ICMP regresa al enrutador, el origen conoce el tiempo de viaje del temporizador y la dirección IP del último enrutador (Figura 3.50).

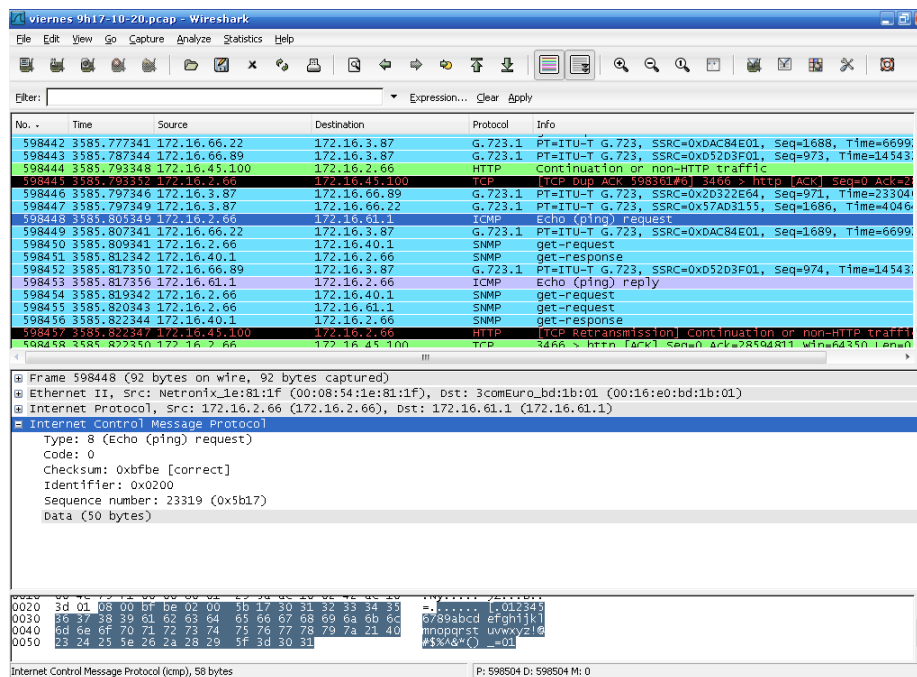


Figura 3.50: Captura del Protocolo ICMP

3.1.8.1.4 Capa de Enlace de Datos

3.1.8.1.4.1 Ethernet

Los estándares Ethernet definen los protocolos de Capa 2 y las tecnologías de Capa 1. Ethernet es la tecnología LAN más utilizada y soporta anchos de banda de 10, 100, 1000 o 10000 Mbps (Megabits por segundo). Ethernet provee un servicio no orientado a conexión sin acuse recibo sobre un medio compartido utilizando CSMA/CD (Carrier Sense Multiple Access/Collision Detection) como método de acceso al medio. Un medio compartido requiere que el encabezado del paquete Ethernet utilice una dirección de la Capa de Enlace de Datos (dirección MAC) para identificar los nodos de origen y destino.

3.1.8.1.4.2 ARP (Address Resolution Protocol)

Provee dos funciones básicas:

- **Resolver direcciones IPv4 a direcciones MAC:** Para colocar una trama en el medio LAN, ésta debe tener una dirección MAC de destino. Cuando un paquete se envía a la Capa de Enlace de Datos para ser encapsulado en una trama, el nodo

busca en su memoria (tabla ARP) para encontrar la dirección que corresponde a la dirección IPv4 de destino. Cada fila de la tabla ARP tiene un par de valores: una dirección IP y una dirección MAC. La relación entre estos dos valores se denomina mapa. Para comenzar el proceso, un nodo que transmite intenta ubicar en la tabla ARP la dirección MAC que corresponde al destino IPv4. Si este mapa está registrado en la tabla, el nodo utiliza la dirección MAC de destino en la trama que encapsula el paquete IPv4.

- **Mantener un registro de las correspondencias:** La tabla ARP se mantiene dinámicamente. Existen dos formas mediante las cuales un dispositivo puede obtener direcciones MAC. La primera consiste en monitorear el tráfico que se produce en el segmento de red local. Conforme un nodo recibe tramas de un medio, éste puede grabar las direcciones IP y MAC de origen como un mapa en la tabla ARP. La segunda forma consiste en enviar una solicitud broadcast ARP. La trama contiene un paquete de solicitud ARP con la dirección IP del dispositivo de destino. El nodo que recibe la trama e identifica la dirección IP como suya responde enviando un paquete ARP de respuesta al emisor como una trama unicast. Cuando se recibe una solicitud para establecer una correspondencia entre una dirección IPv4 y una dirección MAC, ARP busca en el mapa. Si no se encuentra una correspondencia, el encapsulamiento del paquete IPv4 falla y los procesos de Capa 2 notifican a ARP que necesita un mapa. El proceso ARP luego envía un paquete de solicitud ARP para descubrir la dirección MAC del dispositivo destino. El dispositivo que recibe la solicitud y tiene la dirección IP destino responde con una respuesta ARP. En caso de que ningún dispositivo responda a la solicitud ARP, el paquete se descarta porque la trama no puede ser creada. Esta falla de encapsulación se reporta a las capas superiores del dispositivo (Figura 3.51).

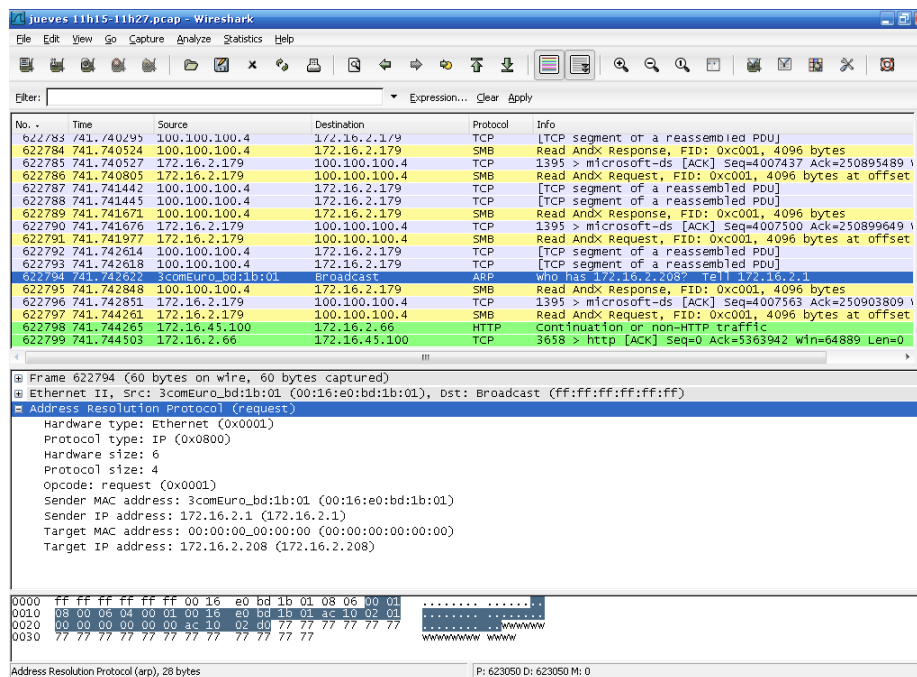


Figura 3.51: Captura del Protocolo ARP

3.1.8.1.4.3 LLC (Logical Link-Control)

Especifica los mecanismos para direccionar estaciones a través del medio y controlar el intercambio de información entre dos usuarios (Figura 3.52). Su operación y formato están basados en HDLC (High-Level Data Link Control). Provee tres servicios alternativos:

- **No orientado a conexión sin acuse recibo:** La entrega de información no está garantizada porque no existe ningún mecanismo de control de flujo o de errores. Sin embargo, en muchos dispositivos existirá alguna capa superior o software que trate asuntos de confiabilidad.
- **En modo de conexión:** Es similar al servicio ofrecido por HDLC, ya que establece una conexión lógica entre dos usuarios que intercambian información y proporciona control de flujo y de errores.
- **No orientado a conexión con acuse recibo:** Es una combinación de los servicios anteriores, pues existen acuses recibo pero no se establece una conexión lógica previa.

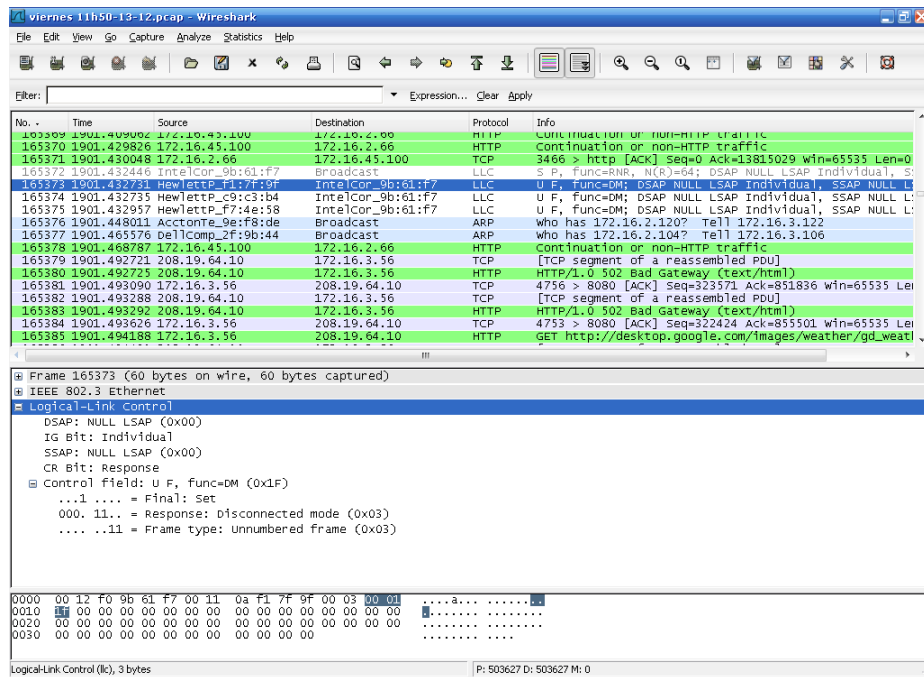


Figura 3.52: Captura del Protocolo LLC

3.1.8.1.4.4 STP (Spanning Tree Protocol)

Los lazos se forman en una red porque conmutadores paralelos no están al tanto de su condición. STP elimina los lazos para que los conmutadores y trayectorias redundantes sean utilizadas. Este protocolo permite que los conmutadores identifiquen a sus vecinos y negocien una trayectoria libre de lazos. Los enlaces redundantes se apagan para prevenir que se formen lazos. Cada conmutador ejecuta el STA (Spanning Tree Algorithm) de acuerdo a la información que recibe de sus vecinos. El algoritmo escoge un punto de referencia en la red y calcula todas las trayectorias redundantes hacia dicho lugar. Cuando aparecen enlaces redundantes, el STA elige uno de ellos para enviar tramas y bloquea la transmisión por las demás trayectorias.

STP calcula una estructura de árbol que considera todos los conmutadores en una red. Las trayectorias redundantes se colocan en estado de Bloqueo o Alerta para evitar el envío de tramas. Sin embargo, sin un puerto falla, el STA re-calcula la topología para que los enlaces necesarios sean reactivados. Los mensajes intercambiados se denominan BPDUs (Bridge Protocol Data Units). Un conmutador envía una trama BPDU utilizando la dirección MAC del puerto como origen. Como el conmutador no sabe de la presencia del resto de equipos, las tramas BPDU se envían con la dirección multicast 01-80-c2-00-00-00

como destino. Existen dos clases de BPDUs: de configuración para realizar cálculos y TCN (Topology Change Notification) para anunciar cambios en la topología de red (Figura 3.53).

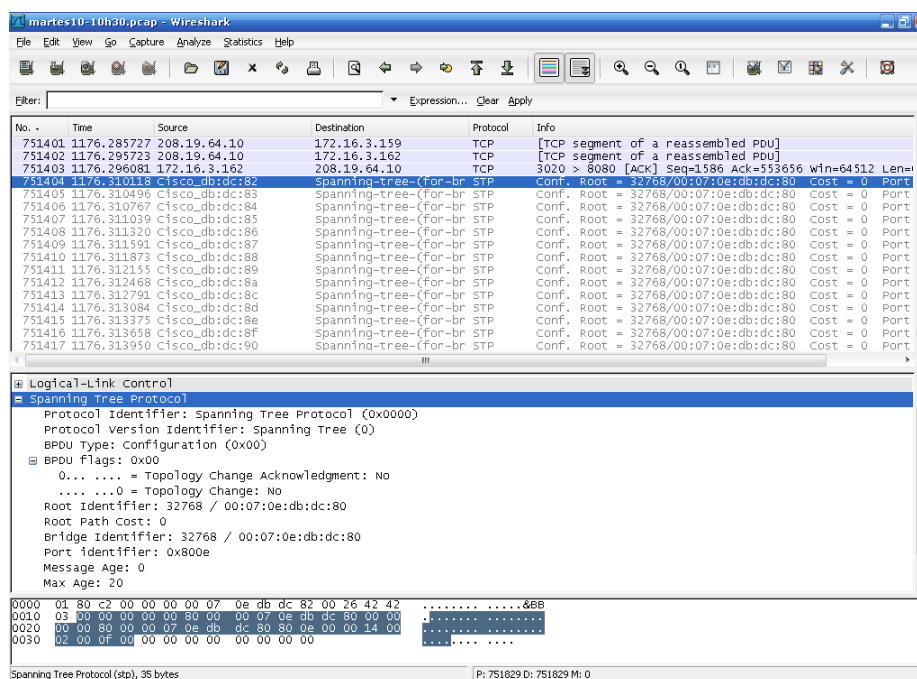


Figura 3.53: Captura del Protocolo STP

En las Tablas 3.8 y 3.9 se presentan los nombres de los protocolos analizados junto con el porcentaje de paquetes capturados. Las Figuras 3.54 y 3.55 muestran que el protocolo con mayor porcentaje en la serie de capturas es Ethernet. Con tan solo unos puntos de diferencia están IP y TCP. Por debajo del 30% se encuentra SMB y UDP. Tanto HTTP como SNMP superan el 15%. Los tres protocolos que oscilan entre 1 y 2% son LLC, ARP y STP. DNS, ICMP y los demás protocolos tienen un porcentaje mínimo (menor a 1).

Protocolo	Porcentaje de Paquetes												
	Martes, 29 de Julio de 2008			Miércoles, 30 de Julio de 2008				Jueves, 31 de Julio de 2008				Viernes, 01 de Agosto de 2008	
	10h00-10h30	15h32-15h42	17h07-17h30	11h05-11h25	13h05-13h25	15h05-15h25	16h05-16h22	11h15-11h32	12h35-12h47	15h03-15h28	17h03-17h24	09h35-12h00	12h35-15h10
Address Resolution Protocol	1,46	1,24	2,97	1,6	2,5	1,97	1,88	1,71	2,34	2,95	3,41	3,57	2,09
Cisco Discovery Protocol	0,07	0,06	0,12	0,07	0,12	0,06	0,08	0,08	0,1	0,08	0,12	0,84	0,67
Connectionless Lightweight Directory Access Protocol	0,03	0,02	0,04	0,04	0,06	0,03	0,03	0,04	0,03	0,04	0,04	0,05	0,03
Domain Name Service	0,34	0,21	0,53	0,51	0,64	0,52	0,53	0,4	0,51	0,59	0,44	0,35	0,28
Dynamic Trunking Protocol	0,04	0,03	0,07	0,04	0,07	0,04	0,05	0,04	0,05	0,05	0,07	0,47	0,37
Ethernet	99,98	99,99	99,97	99,99	99,97	99,99	99,98	99,98	99,98	99,98	99,98	99,83	99,86
Hypertext Transfer Protocol	4,02	18,17	2,68	5,74	3,53	4,98	8,24	5,89	9,1	5,17	7,71	1,31	1,5
Internet Control Message Protocol	0,26	0,22	0,79	0,3	0,43	0,26	0,32	0,25	0,29	0,29	0,28	0,32	1,8
Internet Control Message Protocol v6	0	0	0	0	0,01	0	0,01	0	0	0,01	0	0,02	0
Internet Protocol	96,68	97,31	94,04	96,64	94,33	96,35	95,67	96,38	95,25	95,01	93,64	76,73	82,29
Internet Protocol Version 6	0,02	0,03	0,02	0,05	0,06	0,1	0,07	0,01	0,04	0,04	0,01	0,11	0,07
Kerberos	0,06	0,03	0,11	0,09	0,09	0,06	0,04	0,05	0,08	0,08	0,21	0,05	0,04
Lightweight-Directory-Access-Protocol	0,05	0,07	0,07	0,06	0,12	0,05	0,1	0,04	0,03	0,07	0,06	0,07	0,05
Link Layer Discovery Protocol	0,01	0,01	0,02	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,02	0,12	0,09
Logical-Link Control	1,68	1,3	2,72	1,55	2,84	1,44	2,19	1,73	2,15	1,84	2,69	18,01	14,31
Point-to-Point Tunnelling Protocol	0,02	0	0	0	0	0	0	0	0	0	0	0,01	0
Routing Information Protocol	0,01	0	0,01	0	0,01	0	0,01	0,01	0,01	0,01	0,01	0,06	0,05
Secure Socket Layer	0,32	0,12	0,09	0,55	0,34	0,15	0,62	0,41	0,44	0,91	0,98	0,31	0,31
Simple Network Management Protocol	2,07	1,47	3,4	1,88	3,19	1,92	2,83	2,62	3,16	2,25	2,64	6,84	5,53
SMB (Server Message Block Protocol)	11,43	14,19	12,9	16,82	15,18	32,27	17,4	13,19	15,54	12,84	16,94	16,29	7,08
Spanning Tree Protocol	1,41	1,09	2,34	1,34	2,45	1,27	1,66	1,51	1,92	1,62	2,39	16,61	13,2
Transmission Control Protocol	93,15	94,81	88,23	93,08	88,81	92,83	91,13	92,44	90,51	91,02	89,24	66,57	73,22
User Datagram Protocol	3,27	2,31	5,03	3,29	5,13	3,36	4,28	3,69	4,49	3,72	4,12	9,91	7,34

Tabla 3.8: Porcentaje de Paquetes Capturados en el Conmutador Principal del Noveno Piso

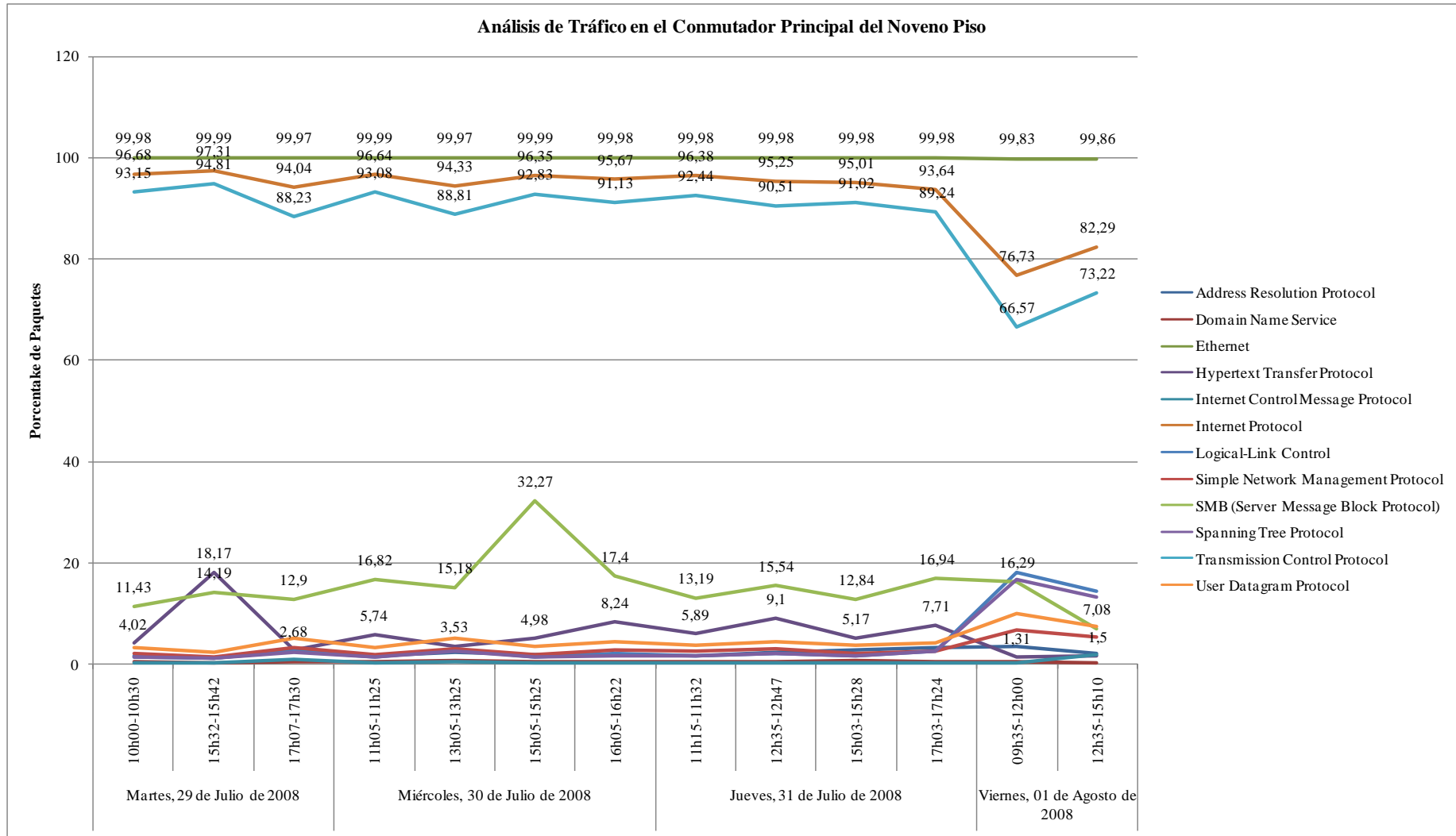


Figura 3.54: Análisis de Tráfico en el Conmutador Principal del Noveno Piso

Protocolo	Porcentaje de Paquetes													
	Martes, 29 de Julio de 2008				Miércoles, 30 de Julio de 2008				Jueves, 31 de Julio de 2008				Viernes, 01 de Agosto de 2008	
	10h14-10h34	12h20-12h36	14h40-15h10	16h30-16h47	10h14-10h32	13h07-13h35	15h10-15h32	16h05-16h25	11h15-11h27	12h35-13h07	15h05-15h25	16h05-16h33	09h17-10h20	11h50-13h12
Address Resolution Protocol	2,27	2,55	1,55	1,55	2,33	3,06	2,51	2,24	1,05	4,16	2,97	1,84	2,01	1,52
Cisco Discovery Protocol	0,12	0,09	0,09	0,1	0	0	0	0	0	0	0	0	0	0
Connectionless Lightweight Directory Access Protocol	0,03	0,02	0,03	0,02	0,02	0,05	0,03	0,03	0,02	0,07	0,03	0,02	0,01	0,03
Domain Name Service	0,61	0,91	0,2	0,82	1	0,29	1,01	0,36	0,45	0,95	0,18	0,67	0,21	0,22
Dynamic Trunking Protocol	0,07	0,05	0,05	0,06	0	0	0	0	0	0	0	0	0	0
Ethernet	99,97	99,98	99,98	99,98	100	100	100	100	100	100	100	100	100	100
Hypertext Transfer Protocol	9,54	9,58	17,32	5,92	7,21	13,11	9,86	10,23	4,13	15,24	9,39	2,83	19,67	30,58
Internet Control Message Protocol	0,58	0,46	0,45	0,48	0,42	0,74	0,53	0,49	0,26	0,89	0,43	0,51	0,88	1,4
Internet Control Message Protocol v6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Internet Protocol	94,79	95,22	96,27	96,14	97,33	96,38	97,05	97,26	98,77	95,23	96,72	97,76	97,53	97,77
Internet Protocol Version 6	0,04	0,04	0,04	0,03	0,07	0,07	0,12	0,08	0,01	0,09	0,04	0,05	0,01	0,04
Kerberos	0,05	0,05	0,06	0,04	0,02	0,06	0,07	0,04	0,02	0,07	0,06	0,03	0,02	0,02
Lightweight-Directory-Access-Protocol	0,06	0,02	0,04	0,06	0,05	0,08	0,08	0,06	0,03	0,08	0,05	0,06	0,01	0,03
Link Layer Discovery Protocol	0,01	0,01	0,01	0,01	0	0	0	0	0	0	0	0	0	0
Logical-Link Control	2,68	2,02	1,98	2,11	0,12	0,23	0,14	0,26	0,08	0,16	0,13	0,17	0,08	0,09
Point-to-Point Tunnelling Protocol	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Routing Information Protocol	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0	0,01	0,01	0,01	0,02	0,03
Secure Socket Layer	0,04	1,37	0,37	0,17	0,2	0,04	0,94	1,09	0,14	0,07	2,18	0,05	0,24	0,04
Simple Mail Transfer Protocol	0	0	0	0	0	0,04	0	0	0	0	0	0	0	0
Simple Network Management Protocol	6,17	4,8	4,84	5,06	4,44	7,23	5,5	5,27	2,88	10,53	4,6	5,92	11,82	18,58
SMB (Server Message Block Protocol)	19,97	19,21	19,44	16,12	33,01	12,61	23,55	15,61	20,54	11,36	11,83	22,88	5	2,38
Telnet	0	0	0	0	0	0	0	0	0	0,01	0	0	0	0
Spanning Tree Protocol	2,17	1,67	1,65	1,74	0	0	0	0	0	0	0	0	0	0
Transmission Control Protocol	80,24	87,98	89,69	82,42	83,56	81,92	85,55	88,23	86,05	74,6	89,39	79,07	51,09	60,98
User Datagram Protocol	14,01	6,82	6,16	13,27	13,41	13,79	11,08	8,62	12,46	19,83	6,92	18,23	45,57	35,43

Tabla 3.9: Porcentaje de Paquetes Capturados en el Conmutador Principal del Quinto Piso

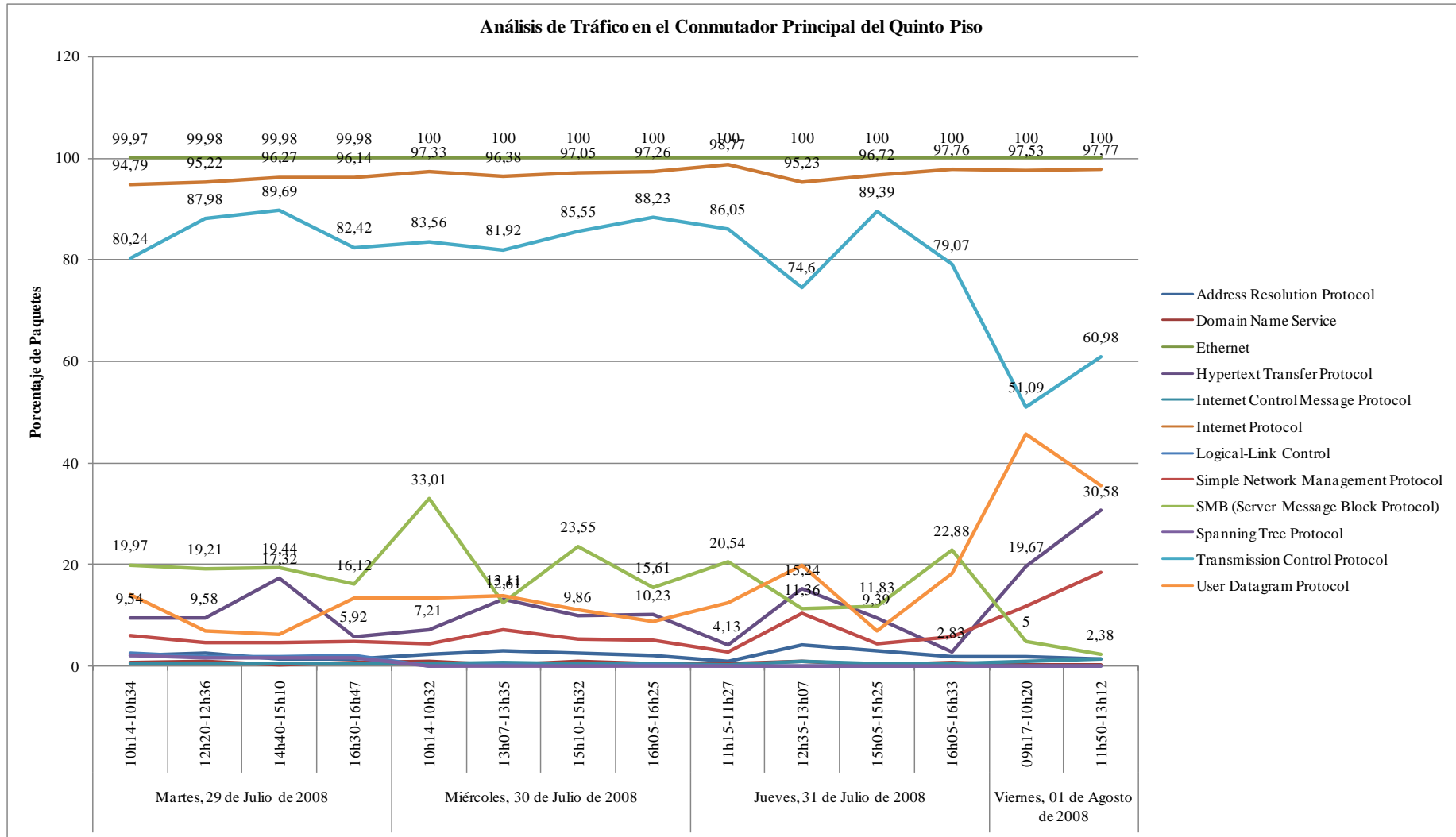


Figura 3.55: Análisis de Tráfico en el Conmutador Principal del Quinto Piso

3.1.8.2 Medición del Ancho de Banda

Para determinar el consumo de ancho de banda en la red se añadieron dos sensores en el programa PRTG (Paessler Router Traffic Grapher) versión 6.0.5.451 y se programaron reportes tanto diarios como semanales. Aunque la medición de ancho de banda fue continua durante 2 periodos (desde el martes 29 al miércoles 30 de julio y a partir del lunes 4 al jueves 7 de agosto), únicamente se consideraron las muestras entre las 08h00-19h30. Para evaluar los resultados se delimitaron tres intervalos: 08h00-12h00 (ingreso), 12h00-15h00 (almuerzo) y 15h00-19h30 (salida). A continuación se presenta un análisis diario respecto al consumo de ancho de banda, haciendo énfasis en las crestas y valles así como en los cambios de comportamiento repentinos. También se presta atención a los incrementos más significativos durante los tres intervalos y se incluye una discusión sobre la tendencia semanal.

3.1.8.2.1 Noveno Piso

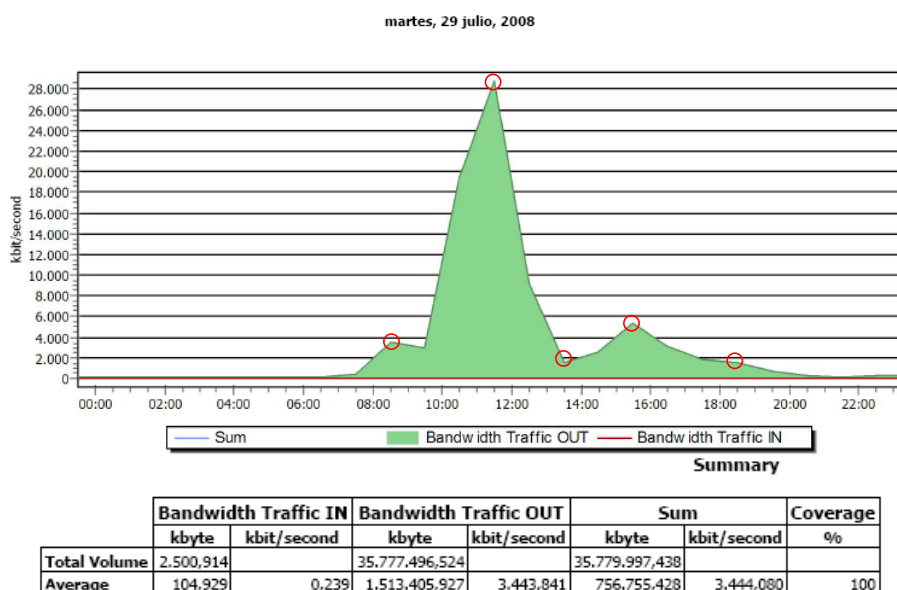


Figura 3.56: Medición del Ancho de Banda del Martes 29 de Julio

La Figura 3.56 muestra un pico de 3567,671 Kbps (Kilobits por segundo) a las 08h30 del martes 29 de julio. Después de un ligero descenso, se produce un incremento significativo que alcanza los 28773,622 Kbps aproximadamente a las 11h30. Este comportamiento sufre un cambio repentino hasta llegar a 1596,654 Kbps. Entre las 13h30 y 15h30 se registra un incremento que logra alcanzar los 5320,221 Kbps. Desde ese instante el consumo baja hasta 721,880 Kbps.

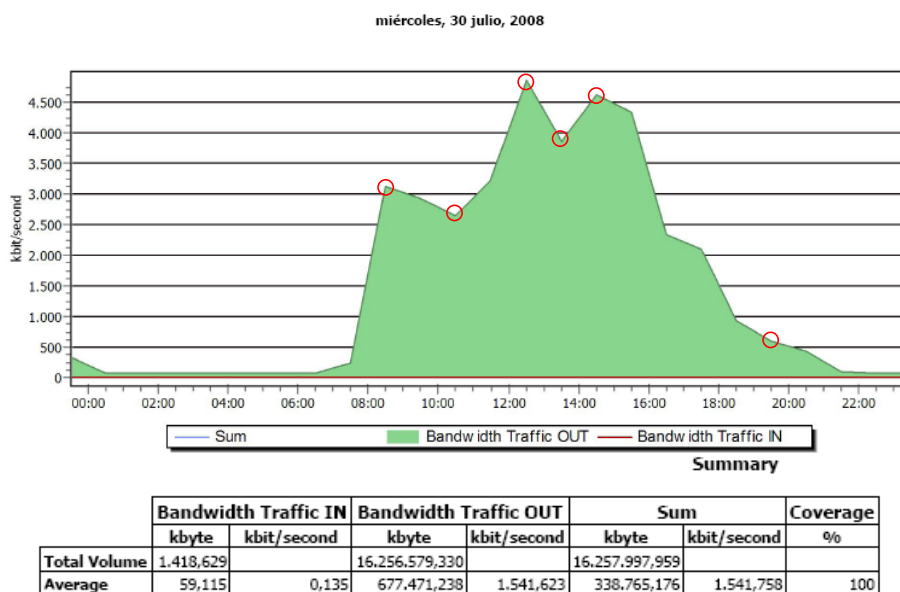


Figura 3.57: Medición del Ancho de Banda del Miércoles 30 de Julio

Desde las 07h30 del miércoles 30 de julio se observa un incremento que alcanza los 3126,730 Kbps en una hora (Figura 3.57). Luego se produce un descenso paulatino que marca un valle de 2644,443 Kbps. Alrededor de las 10h30 el consumo aumenta y supera los 4862 Kbps. En el segundo intervalo existe un valle de 3863,180 Kbps y media hora después una pendiente positiva que llega hasta 4628,431 Kbps. Momentos antes de que inicie el tercer intervalo el consumo disminuye progresivamente hasta 591,989 Kbps.

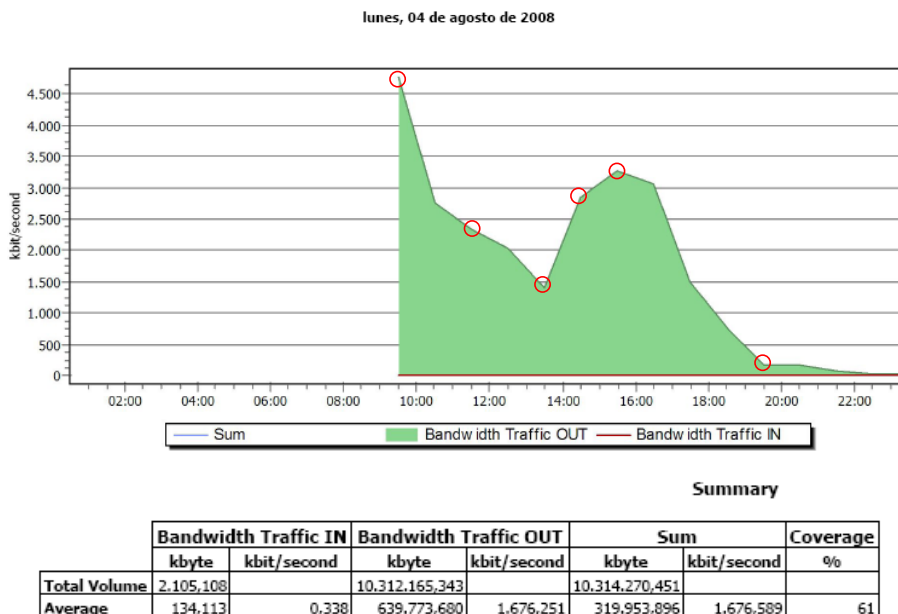


Figura 3.58: Medición del Ancho de Banda del Lunes 4 de Agosto

En la Figura 3.58 (lunes 4 de agosto) se registra un pico de 4762,797 Kbps en el primer intervalo y un decrecimiento paulatino hasta llegar a 2337,880 Kbps. Esta tendencia se mantiene y alcanza su punto mínimo (1401,453 Kbps) aproximadamente a las 13h30. Al final del segundo intervalo se observa un incremento de 2859,161 Kbps. Este comportamiento alcanza un máximo de 3272,834 Kbps durante los treinta primeros minutos del último intervalo. De ahí en adelante, el consumo disminuye significativamente alrededor de las 19h30 (158,040 Kbps).

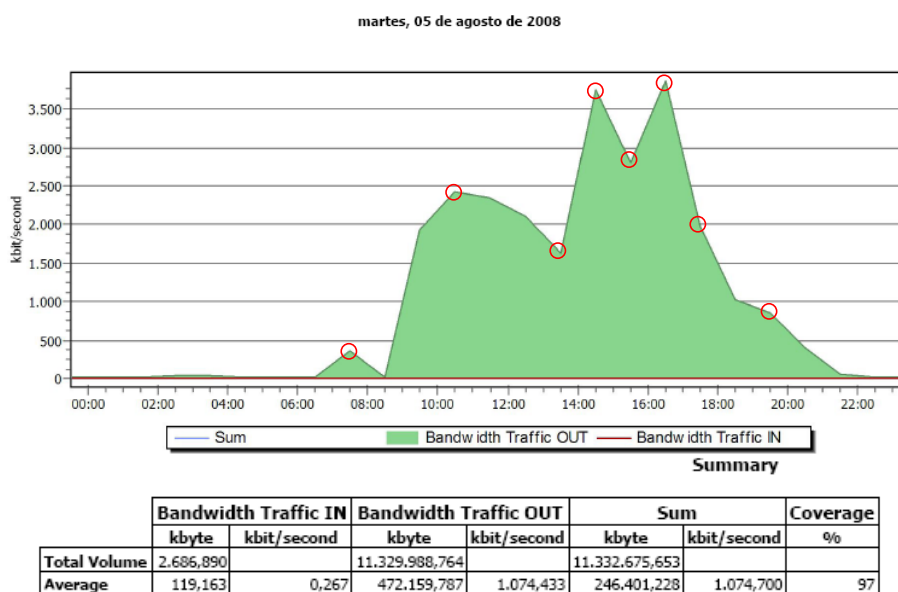


Figura 3.59: Medición del Ancho de Banda del Martes 5 de Agosto

Alrededor de las 07h30 del martes 5 de agosto se produce un pico de 362,778 Kbps que desciende abruptamente (Figura 3.59). Una hora más tarde existe un incremento que alcanza los 2429,145 Kbps. El consumo disminuye progresivamente hasta un valle de 1624,900 Kbps a las 13h30. Inmediatamente ocurre un incremento que llega a 3740,928 Kbps y luego desciende a 2811,574 Kbps. Durante los primeros minutos del tercer intervalo la tendencia cambia y se registra una cresta de 3863,094 Kbps que rápidamente disminuye hasta 1975,224 Kbps. Al cabo de dos horas el consumo se reduce a 857,941 Kbps.

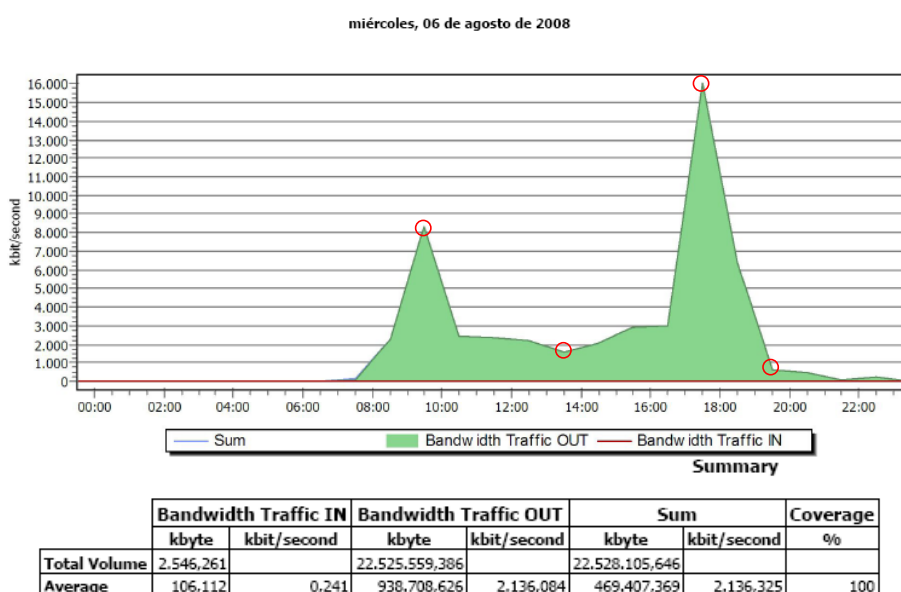
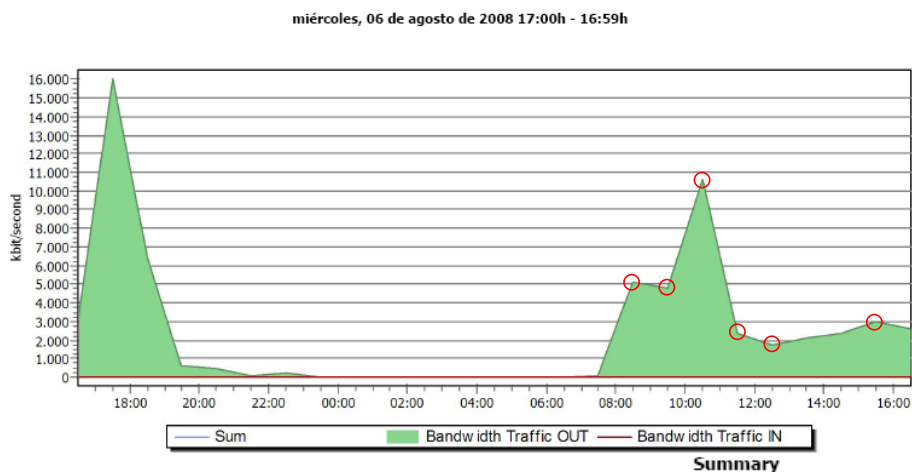


Figura 3.60: Medición del Ancho de Banda del Miércoles 6 de Agosto

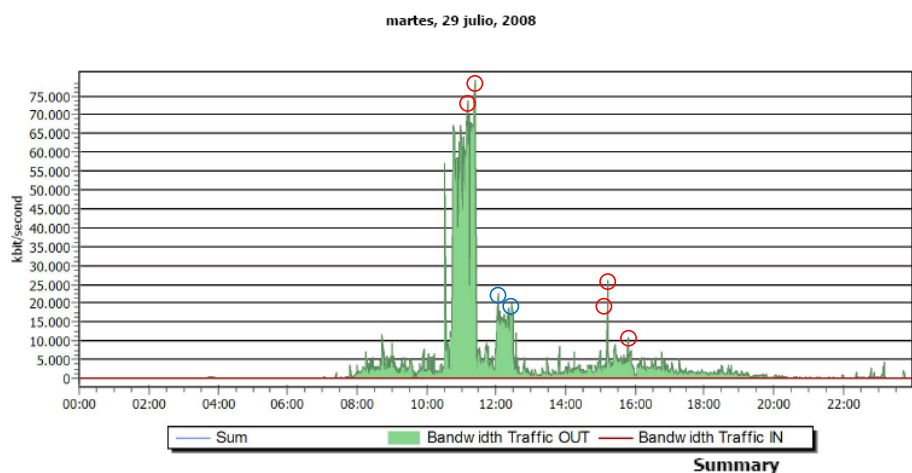
En el primero intervalo del miércoles 6 de agosto (Figura 3.60) se observa una pendiente que alcanza los 8342,222 Kbps alrededor de las 09h30. Luego se produce un descenso que marca un valle de 1589,111 Kbps. A partir de las 13h30 este comportamiento se modifica y se registra una cima de 16034,511 en los últimos minutos del tercer intervalo. La medición muestra una reducción considerable (637,560 Kbps) a las 19h30 aproximadamente.



	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage %
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	
Total Volume	5,138,397		25,820,666,765		25,825,805,162		
Average	214,135	0,487	1,076,022,752	2,448,550	538,118,443	2,449,037	100

Figura 3.61: Medición del Ancho de Banda del Jueves 7 de Agosto

En la Figura 3.61 se registra un incremento desde las 07h30 del jueves 7 de agosto hasta alcanzar los 5081,966 Kbps. Luego se observa una pendiente negativa que origina un valle (4800,045 Kbps) y al cabo de unos minutos la tendencia cambia y establece una cresta en 10626,143 Kbps. Nuevamente ocurre un descenso (2382,301 Kbps) justo antes de concluir el primer intervalo. Un valle (1701,365 Kbps) se produce en el segundo intervalo, pero este comportamiento se modifica y origina una cresta de 3025,218 Kbps.



	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage %
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	
Total Volume	2,500,914		35,777,496,524		35,779,997,438		
Average	1,740	0,238	24,776,966	3,457,301	12,393,665	3,457,539	100

Figura 3.62: Valores Significativos del Martes 29 de Julio

En la Figura 3.62 se registran los valores más elevados en los periodos de interés. Durante la mañana del martes 29 de julio se identifican tres crestas: 73476,692; 79096,955 y 77796,105 Kbps. Al medio día se producen incrementos de 22579,923; 18763,701 y 19815,521 Kbps. Mientras que en la tarde y noche existen picos de 19029,869; 26106,117 y 10792,995 Kbps.

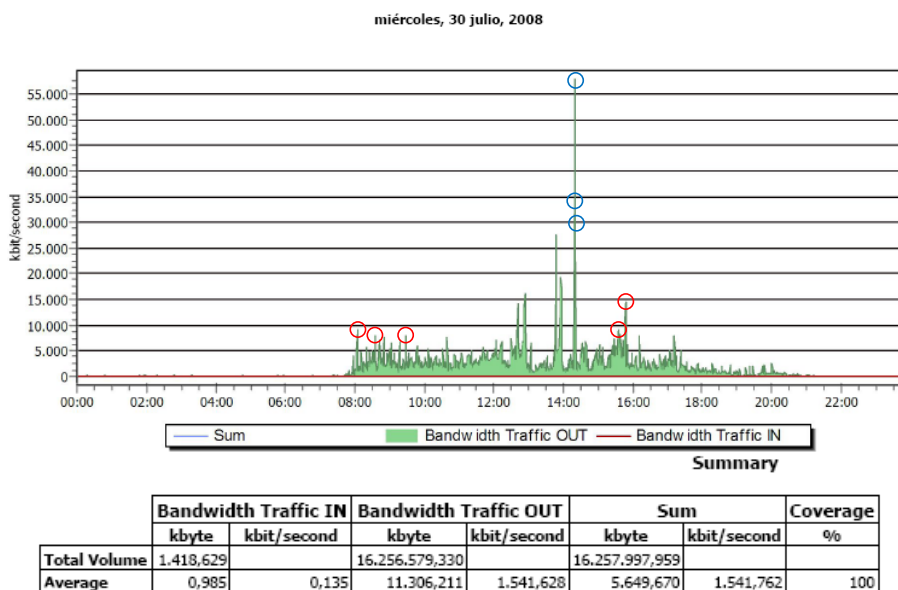


Figura 3.63: Valores Significativos del Miércoles 30 de Julio

Los puntos más altos en el primer intervalo del miércoles 30 de julio (Figura 3.63) son: 9027,523; 8007,554 y 8053,951 Kbps. En tanto que los valores más importantes para el segundo intervalo son: 34453,988; 57860,308 y 29047,087 Kbps. Tres crestas de sobresalen al terminar el día: 9075,847; 10490,202 y 14367,110 Kbps.

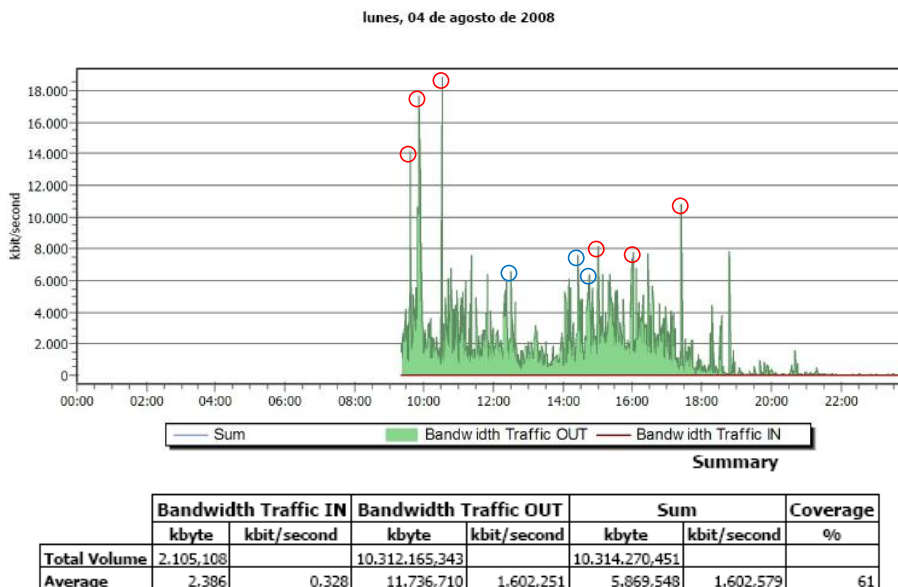


Figura 3.64: Valores Significativos del Lunes 4 de Agosto

La Figura 3.64 muestra las crestas más pronunciadas en cada uno de los tres intervalos del lunes 4 de agosto. Los valores registrados para el primer intervalo son: 14150,314; 17643,376 y 18843,784 Kbps. En el segundo intervalo cabe mencionar cantidades tales como: 6517,278; 7615,682 y 6350,396 Kbps. Mientras que en el tercer intervalo sobresalen los siguientes valores: 8090,158; 7739,400 y 10848,826 Kbps.

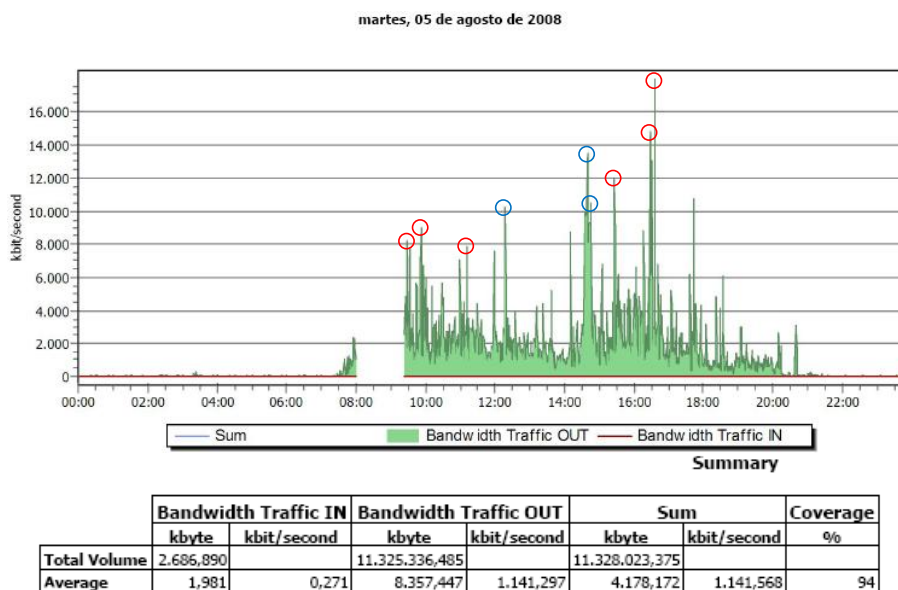


Figura 3.65: Valores Significativos del Martes 5 de Agosto

La Figura 3.65 revela que los valores más significativos del primer intervalo del martes 5 de agosto son: 8172,741; 9031,817 y 7826,006 Kbps. Resulta imprescindible considerar las crestas de 10212,365; 13501,178 y 10461,245 Kbps en el segundo intervalo. Los picos más pronunciados del último intervalo son: 11992,449; 14833,400 y 17980,187 Kbps.

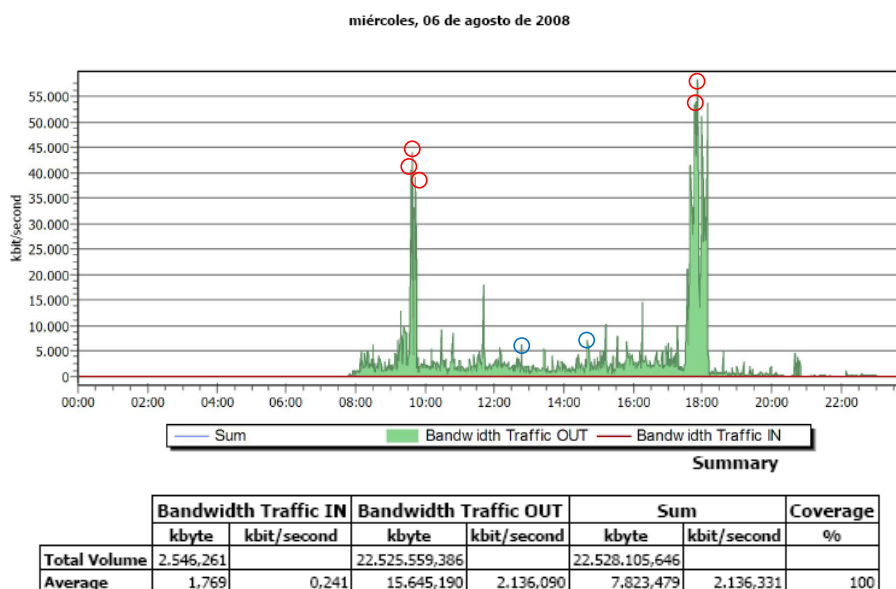


Figura 3.66: Valores Significativos del Miércoles 6 de Agosto

Las crestas que sobresalen en el primer intervalo del miércoles 6 de agosto (Figura 3.66) son: 40556,077; 44040,754 y 39245,755 Kbps. De manera similar, el segundo intervalo está marcado por tres incrementos: 7204,617; 6868,767 y 6219,542 Kbps. En el tercer intervalo es importante mencionar valores como: 54120,299; 54462,552 y 58271,102 Kbps.

3.1.8.2.2 Quinto Piso

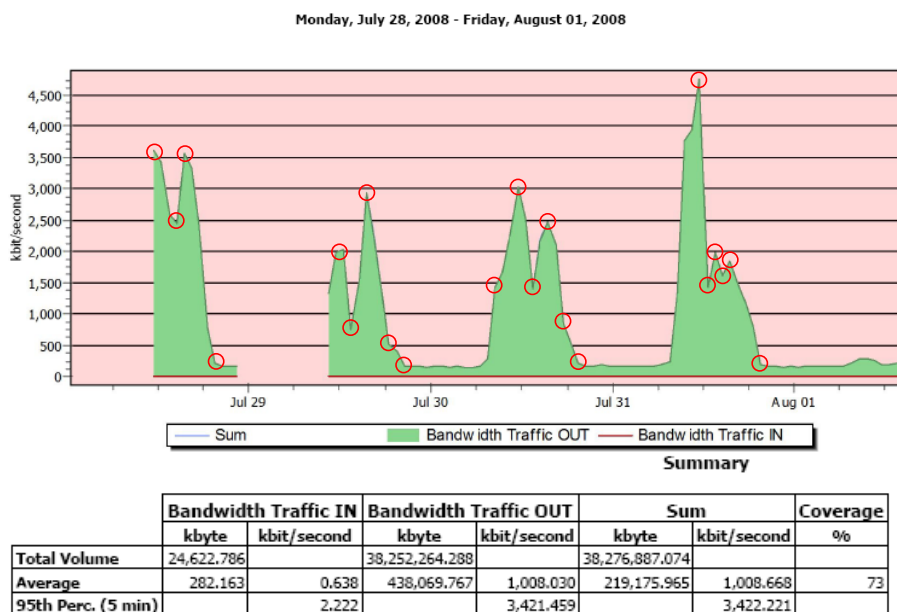


Figura 3.67: Medición del Ancho de Banda en la Semana del 28 de Julio al 1 de Agosto

Durante la mañana del lunes 28 de julio se registra un pico de 3620,928 Kbps (Figura 3.67). En el segundo intervalo se observa un valle de 2443,095 Kbps así como una cresta de 3565,479 Kbps. El tercer intervalo se caracteriza por una reducción en el consumo que llega hasta los 159,743 Kbps. Al día siguiente se observa una pendiente que crece hasta 2038,123 Kbps y luego desciende a 752,849 Kbps. La cresta del tercer intervalo tiene un valor de 2932,966 Kbps y desciende a 522,275 Kbps. En horas de la tarde se observa un valle de 147,937 Kbps.

La medición indica un incremento progresivo (de 1429,766 a 3023,367 Kbps) en el transcurso del miércoles 30 de julio. En el segundo intervalo se registra tanto un valle (1392,970 Kbps) como una cresta (2478,720 Kbps). La jornada concluye con un tendencia negativa entre 840,308 y 199,083 Kbps. Un par de horas antes del medio día del jueves 31 de julio se observa una cresta de 4757,659 Kbps que disminuye rápidamente hasta un valor de 1433,026 Kbps. El segundo intervalo se caracteriza por un par de crestas (1984,170 y 1852,214 Kbps) y un valle (1602,570 Kbps). Una pendiente pronunciada que alcanza los 191,491 Kbps se registra en horas de la tarde.

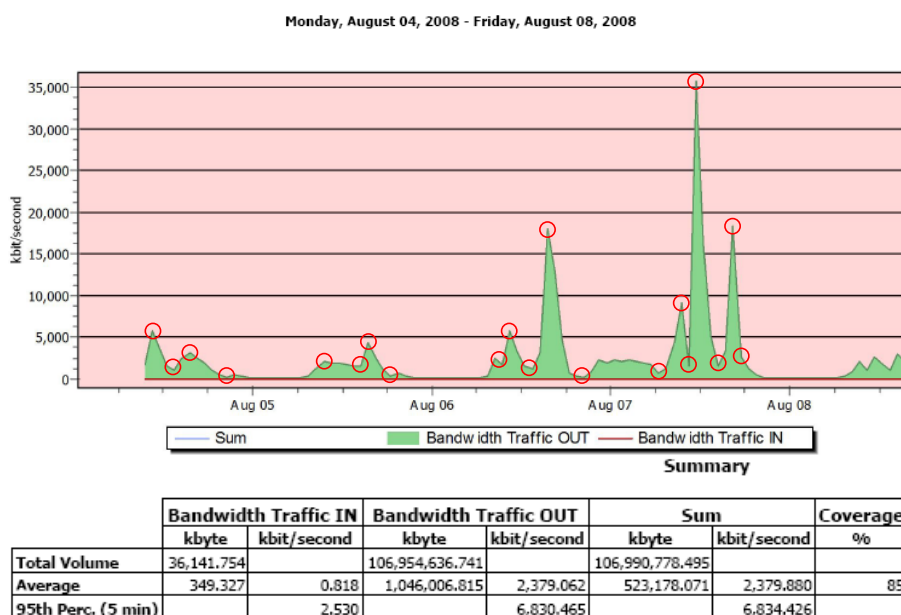


Figura 3.68: Medición del Ancho de Banda en la Semana del 4 al 8 de Agosto

En el primer intervalo del lunes 4 de agosto se produce una cresta (5814,874 Kbps) que súbitamente disminuye luego del medio día y crea un valle en 1000,382 Kbps (Figura 3.68). En el segundo intervalo se observa un incremento que alcanza los 3199,874 Kbps y desciende progresivamente hasta los 160,291 Kbps. La primera cresta que ocurre al día siguiente sobrepasa los 2150 Kbps. Durante el segundo intervalo se origina un valle en 1603,003 Kbps y luego el consumo se incrementa hasta 4297,364 Kbps. Una caída súbita (202,886 Kbps) se registra al final del tercer intervalo.

El miércoles 6 de agosto inicia con una pendiente positiva que llega hasta los 2426,647 Kbps, decae a 1688,536 Kbps y vuelve a definir una cresta en 5855,455 Kbps. En el segundo intervalo se produce un valle en 1257,857 Kbps y luego la tendencia cambia para alcanzar los 18093,189 Kbps. En el tercer intervalo el nivel se reduce hasta 198,899 Kbps. El primer intervalo del día siguiente comienza en 635,525 Kbps y logra alcanzar un valor de 9167,928 Kbps. Después se registran dos pares valle-cresta que tienen los siguientes valores: 1573,737; 35696,394 y 1643,660; 18431,165 Kbps. En el tercer intervalo el consumo disminuye a 2662,693 Kbps.

Aunque el consumo de ancho de banda no presenta valores típicos en el transcurso de la semana, es posible concluir que la primera hora de la jornada laboral está caracterizada por un incremento paulatino. En la mañana se producen fluctuaciones que culminan con una pendiente positiva minutos antes del medio día. Durante el tiempo asignado para el almuerzo, la tendencia cambia y permanece relativamente estable. Un par de horas antes de concluir las actividades, el comportamiento exhibe un ligero aumento que disminuye al caer la noche.

3.2 Propuesta de Diseño

En su afán por mejorar el desempeño de la red LAN (Local Area Network) del edificio matriz, TRANSELECTRIC S.A. ha considerado que la transición a una red jerárquica conmutada es imprescindible. La propuesta que se desarrolla a continuación contempla las características del Cuarto de Telecomunicaciones, las especificaciones del cableado vertical y horizontal, las regulaciones de las Áreas de Trabajo, la configuración de los conmutadores y la gestión de la red.

3.2.1 Cuarto de Telecomunicaciones

3.2.1.1 Estructura, Control de Temperatura y Equipamiento

El Cuarto de Telecomunicaciones se ubicará en el área que separa las alas Oriental y Occidental del quinto piso. Las paredes frontales de la habitación se reemplazarán por estructuras de hormigón armado y la puerta de ingreso se cambiará a un modelo blindado que se abra hacia afuera. El acceso se permitirá únicamente al administrador de la red y personal técnico del CGTT (Centro de Gestión de Telecomunicaciones de TRANSELECTRIC). Un sistema biométrico (lector de huellas digitales) garantizará que la entrada sea bloqueada a cualquier persona no autorizada.

La ventana situada en la pared posterior será eliminada y el equipo de aire acondicionado se reemplazará por un sistema industrial que mantenga la temperatura entre 17 y 21 °C así como el nivel de humedad entre 30 y 50%. La central telefónica SIEMENS HiPath 4500 y el bastidor que maneja las extensiones telefónicas conservarán su ubicación. Dos bastidores compuestos por 10 paneles de interconexión de 48 puertos distribuirán las extensiones y líneas directas para cada piso (Figura 3.69). El banco de baterías EVEREXXED de 48 voltios, el cargador de baterías CELCO PP-48V-300A y los dos inversores AC/DC (CDP y TRIPP-LITE) serán trasladados al Cuarto de Equipos del Departamento de Administración de Redes y Gestión de Fibra Óptica.

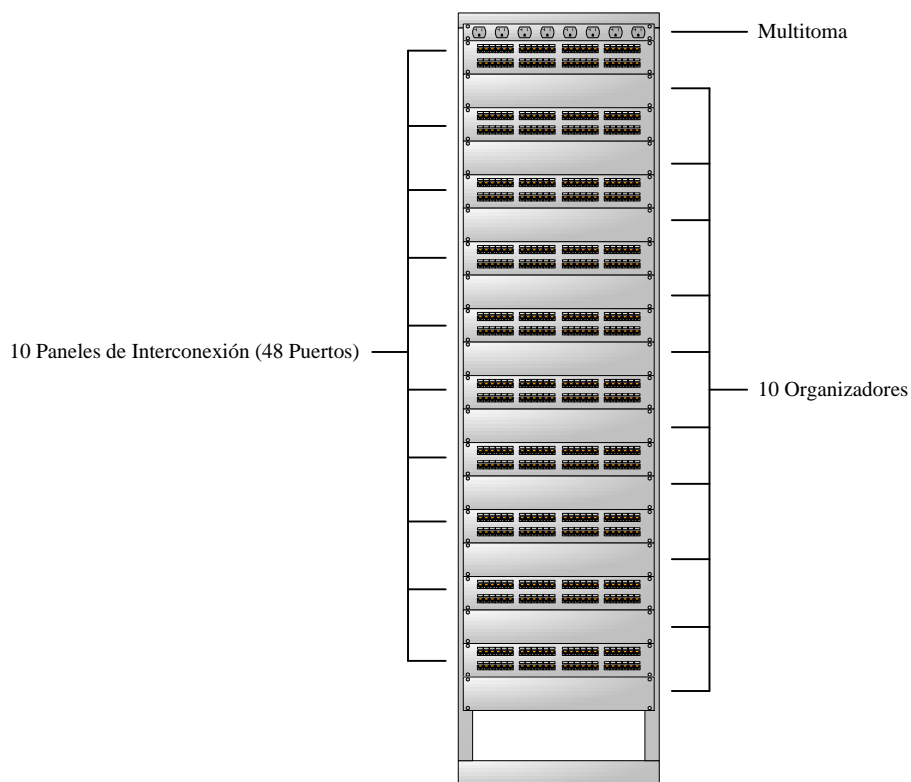


Figura 3.69: Bastidor de Extensiones y Líneas Directas

La nueva topología de red estará ceñida al modelo jerárquico, en el cual las capas de Core y Distribución se juntarán (Core colapsado) para brindar un servicio óptimo a la capa de Acceso (Figura 3.70). Dos conmutadores de Capa 3 conformarán el centro de la red y tendrán un doble enlace Gigabit Ethernet para asegurar la redundancia. Para el montaje de los conmutadores de Core/Distribución se utilizará un bastidor como el de la Figura 3.71.

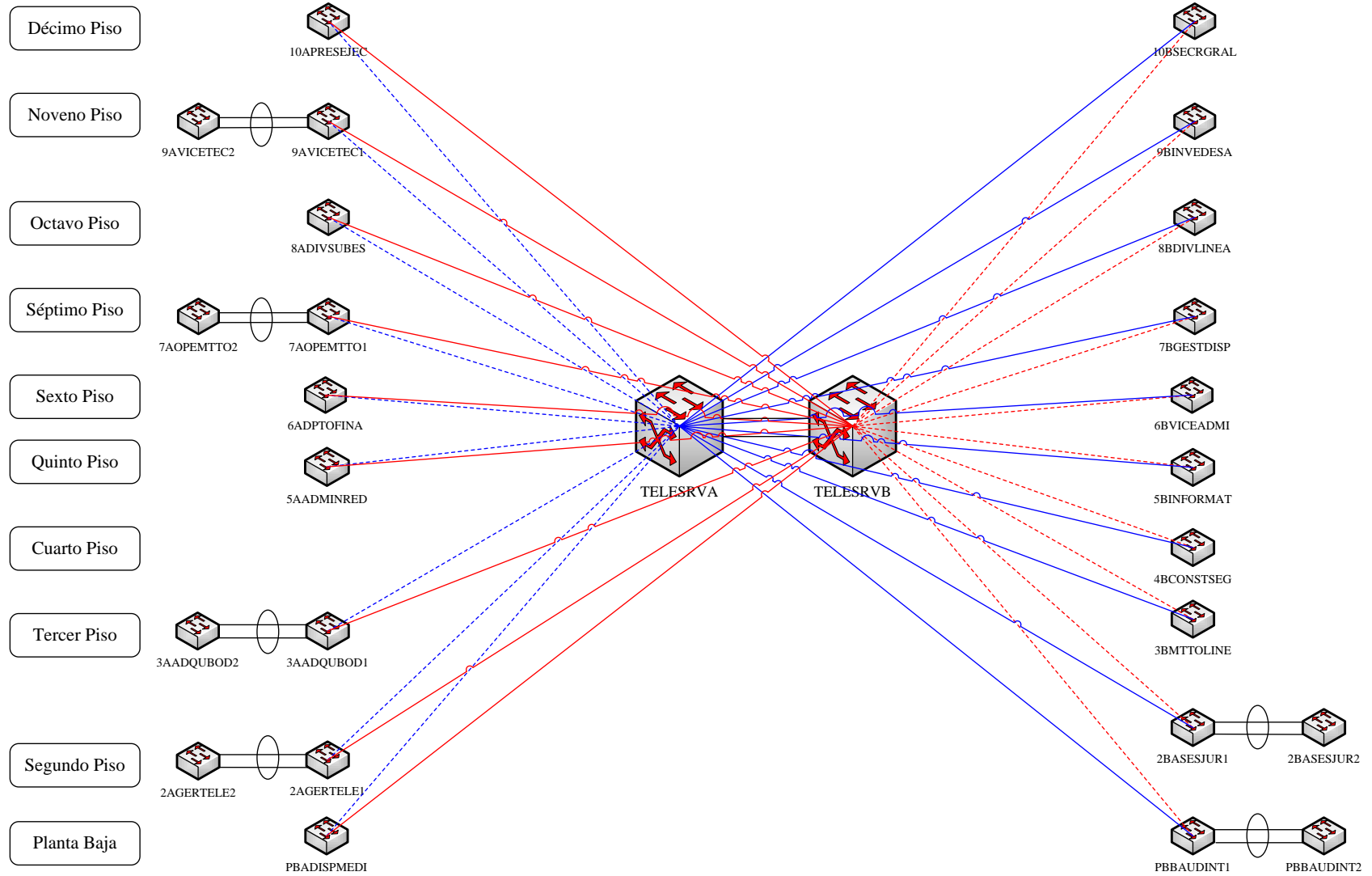


Figura 3.70: Diagrama Topológico de la Red Propuesta

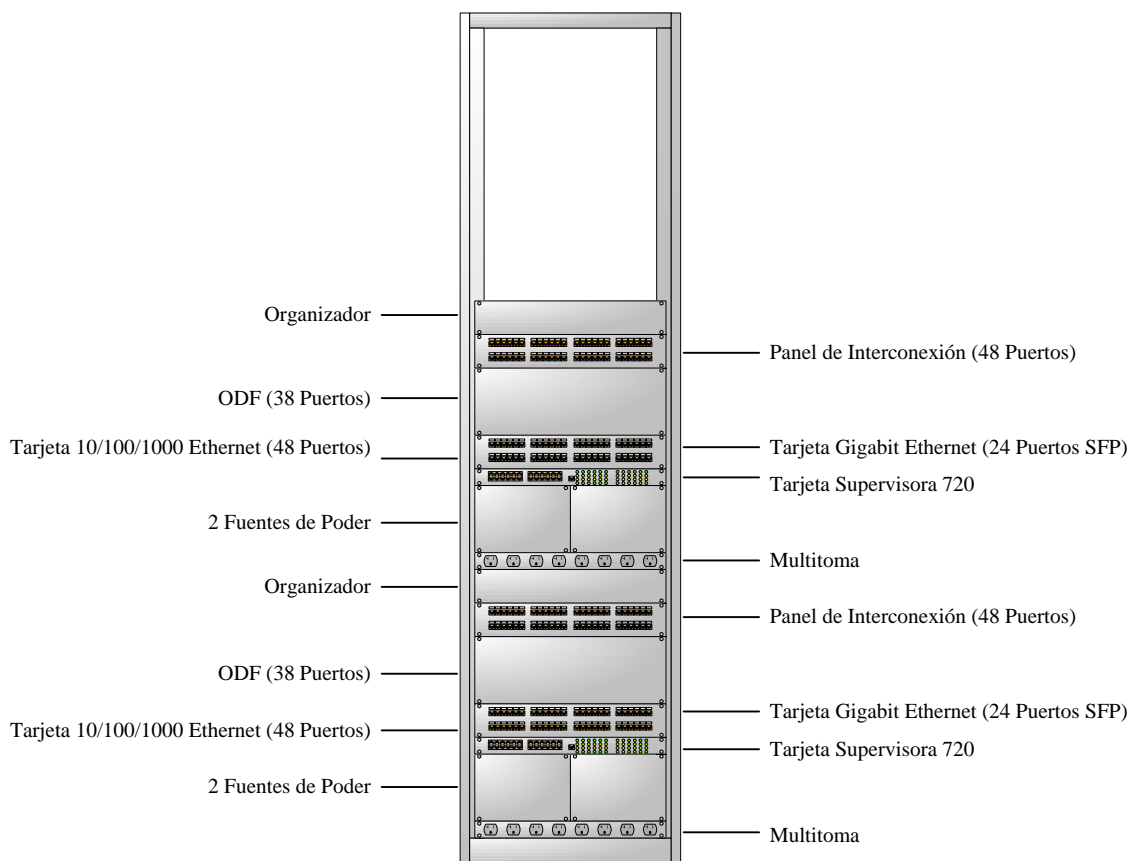


Figura 3.71: Bastidor de los Conmutadores de Core/Distribución

El conmutador Cisco Catalyst 6506-E tiene una capacidad de 6 módulos que permitirá acomodar los recursos informáticos y manejar el tráfico generado por los usuarios de la red (Figura 3.72). Cada uno de estos equipos estará formado por una tarjeta supervisor 720 y utilizará el Cisco IOS (Internetwork Operating System) como sistema operativo. Además contará con dos fuentes de poder y una bandeja de ventilación. Los servidores se conectarán a un módulo de 48 puertos 10/100/1000 Ethernet y los conmutadores de Acceso a una tarjeta Gigabit Ethernet de 24 puertos SFP (Small Form-Factor Pluggable).



Figura 3.72: Conmutadores Cisco Catalyst 6500

La tarjeta supervisora 720 que se presenta en la Figura 3.73 tiene una circuitería de alto rendimiento con una capacidad de conmutación por ranura de 40 Gbps (Gigabit por segundo). Entre sus características están seguridad de puerto y ACLs (Access Control Lists). Los sistemas operativos que admite esta tarjeta son el Cisco Catalyst OS y Cisco IOS. También provee alto rendimiento, conmutación multicapa y enrutamiento. Su procesador maneja protocolos de Capas 2 y 3 tales como STP (Spanning Tree Protocol) y VTP (VLAN Trunking Protocol).

Esta tarjeta es compatible con el chasis de 6 módulos (Cisco 6506), necesita un ventilador de alta velocidad y una fuente de poder de 2500W AC (Alternating Current) o DC (Direct Current) y admite la versión de sistema operativo 12.2(17d)SXB1 o superior y memorias DRAM (Dynamic Random Access Memory) de 1 GB (Gigabyte). Los dos puertos SFP permitirán interconectar los dos conmutadores de Core/Distribución.



Figura 3.73: Tarjeta Supervisora 720

La tarjeta 10/100/1000 Ethernet de 48 puertos proveerá acceso a los servidores mediante conectores RJ-45 (Figura 3.74). Entre sus características están la transmisión de hasta 30 Mpps (Millones de paquetes por segundo) por sistema y compatibilidad con la tarjeta supervisora 720. Con la tarjeta Gigabit Ethernet de 24 puertos SFP que transmite paquetes hasta 30 Mpps por sistema se enlazarán los conmutadores de Acceso a los dispositivos de Capa 3 (Figura 3.75).



Figura 3.74: Tarjeta 10/100/1000 Ethernet de 48 Puertos



Figura 3.75: Tarjeta Gigabit Ethernet de 24 Puertos SFP

3.2.1.2 Identificación de Dispositivos y Cables de Interconexión

Los equipos de Core/Distribución podrán ser identificados mediante etiquetas generadas por computador que especificarán el nombre respectivo. Los cables de interconexión de fibra óptica estarán señalados con el número de piso y ala de donde provienen. Asimismo, el cableado utilizado para los servidores tendrá el nombre de los dispositivos que se encuentran conectados.

3.2.2 Cableado Vertical

Desde el Cuarto de Telecomunicaciones se tenderá fibra óptica multimodo 62.5/125 hacia cada ala siguiendo las trayectorias longitudinales creadas por las tuberías de PVC

que existen actualmente (Figura 3.76). Un par de ODFs (Optical-Fiber Distribution Frames) de 24 puertos organizará el cableado vertical a fin de interconectar las interfaces Gigabit Ethernet de los conmutadores de Acceso a la tarjeta de 24 puertos SFP en cada dispositivo de Core/Distribución. Para enlazar los servidores controlados por el Departamento de Informática se instalarán 40 cables UTP Categoría 5e (cada uno de 30 metros aproximadamente) entre el Cuarto de Telecomunicaciones y la Sala de Servidores.

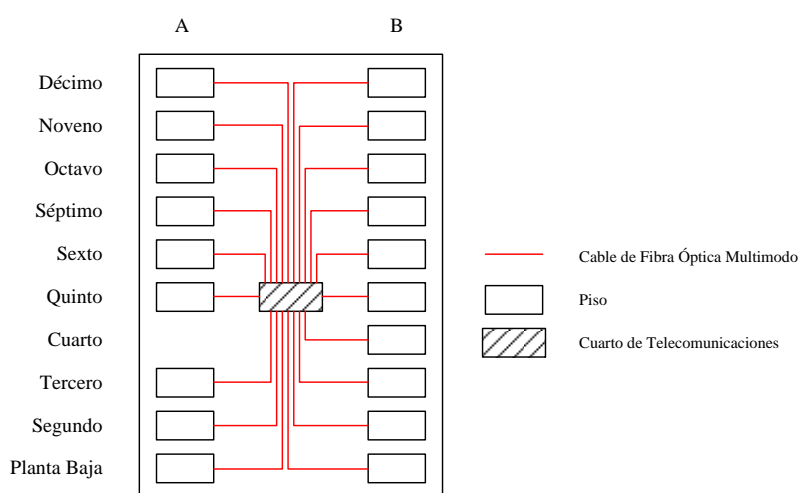


Figura 3.76: Trayectorias del Cableado Vertical

3.2.3 Cableado Horizontal y Áreas de Trabajo

A fin de aprovechar los conmutadores que forman parte de la red LAN (Local Area Network) actual se examinaron sus características, prestando especial atención al fabricante, tipo de interfaces y densidad de puertos. Dado que la nueva red estará formada solamente por dispositivos Cisco, se decidió incluir en el diseño todos los conmutadores de esta marca que existen en la red. La Tabla 3.10 detalla los conmutadores que podrán ser utilizados en la Capa de Acceso.

Cantidad	Modelo		Densidad de Puertos		Ranuras de Expansión		
			10/100 Ethernet	10/100/1000 Ethernet	MT-RJ	GBIC	SFP
2	Catalyst 3500 Series XL	WS-C3524-XL-EN	24	-	-	2	-
4	Catalyst 2950 Series	WS-C2950-24	24	-	-	-	-
2	Catalyst 2950 Series	WS-C2950SX-24	24	-	2	-	-
3	Catalyst 2960 Series	WS-2960-24TC-L	24	-	-	-	2
2	Catalyst 2960 Series SI	WS-C2960-24TC-S	24	2	-	-	2
1	Catalyst 2900 Series	-	24	-	-	-	-

Tabla 3.10: Conmutadores Cisco de la Red Actual

Debido a la gran cantidad de usuarios por ala es necesario incorporar 7 conmutadores Catalyst 2960 Series de 48 puertos y 3 de 24 puertos (Figura 3.77). Estos dispositivos tienen un par de enlaces Gigabit Ethernet de doble propósito (10/100/1000 Ethernet o SFP) que permitirán interconectar las Capas de Core/Distribución y de Acceso utilizando fibra óptica. Además ofrecen seguridad mediante una gama de métodos de autenticación y tecnologías de encriptación. La seguridad de puerto limita el acceso en un puerto Ethernet según la dirección MAC del dispositivo que se conecta, limitando el número de equipos y protegiendo al conmutador.



Figura 3.77: Conmutadores Cisco Catalyst 2960

3.2.3.1 Componentes del Armario por Ala

En cada ala del edificio se instalará un armario de pared con llave de seguridad junto a los ductos para cableado (Figura 3.78). Un ODF de 8 puertos recibirá el cable de fibra óptica procedente del Cuarto de Telecomunicaciones y facilitará la conexión de las interfaces Gigabit Ethernet del conmutador de Acceso. De acuerdo a las necesidades de cada departamento se colocarán paneles de interconexión de 24 o 48 puertos para enlazar los segmentos del cableado horizontal (desde los cajetines ubicados en las Áreas de Trabajo hasta la bandeja central) con los puertos del dispositivo de Capa 2.

Con un cable multipar (50 pares) se reflejará el bastidor que manejará las extensiones y líneas directas de la central telefónica SIEMENS HiPath 4500 a un segundo grupo de paneles de interconexión. La comunicación entre el cableado de voz tendido en cada ala y el que desciende del Cuarto de Telecomunicaciones se conseguirá con otro conjunto de paneles. Una multitoma (8 tomacorrientes) con circuito eléctrico independiente se colocará en el interior de cada armario para garantizar el suministro de energía.

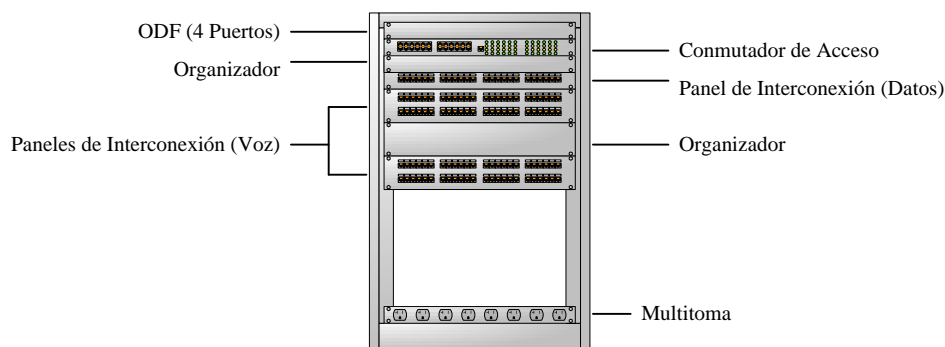


Figura 3.78: Armario a Instalarse en Cada Ala

3.2.3.1.1 Identificación de Dispositivos y Cables de Interconexión

Tanto el ODF como el conmutador estarán etiquetados con el número de piso y ala correspondientes. Cada puerto de los paneles de interconexión para voz y datos tendrán un identificador que permita reconocer su ubicación en el Área de Trabajo. Los dos extremos de los cables de interconexión se marcarán con el número de piso, ala y código de cajetín. Los cables de interconexión entre el ODF y el conmutador serán de fibra óptica multimodo 62.5/125 y tendrán conectores SC en un extremo y LC, SC o MT-RJ en el otro.

Para las conexiones de datos se empleará cable UTP (Unshielded Twisted Pair) Categoría 5e, conectores RJ-45 macho y capuchones. La distribución de hilos se registrará por el estándar ANSI/TIA/EIA-568-B. El cable telefónico de 4 pares se utilizará entre los paneles de interconexión de voz.

3.2.4 Configuración de los Conmutadores

3.2.4.1 Configuración Básica

3.2.4.1.1 Borrar la Configuración

La primera tarea antes de configurar todos los conmutadores, independientemente si pertenecen a la Capa de Core/Distribución o Acceso, consistirá en borrar los archivos que contienen la información de la base de datos VLAN (vlan.dat) y la configuración inicial (startup-config) de la NVRAM (Non-Volatile Random Access Memory) para evitar que cualquier configuración previa ocasione resultados impredecibles. Luego se reiniciarán los conmutadores para comenzar con la configuración.

3.2.4.1.2 Verificar la Configuración por Defecto

Para registrar el tipo de interfaces (Fast Ethernet y/o Gigabit Ethernet), la cantidad de puertos (24 o 48) y el rango de líneas virtuales (vty) se revisará la configuración actual de los conmutadores. Además se examinarán las características de la interfaz virtual VLAN 1 para comprobar que no se ha asignado una dirección IP (Internet Protocol) a los dispositivos pero si tiene una dirección MAC (Media Access Control) y no está en funcionamiento.

Por otra parte, se examinará la información del sistema operativo (Cisco IOS) que permitirá conocer la versión que los conmutadores están corriendo, el nombre del archivo de la imagen del sistema y la dirección MAC de los equipos. Después se explorará los parámetros de la VLAN (Virtual Local Area Network) por defecto (VLAN 1) para confirmar que está activa, su nombre es “default” y todos los puertos pertenecen a esta red virtual.

3.2.4.1.3 Asignar el Nombre de Dispositivo

Para identificar a los conmutadores se creará un nombre que contenga el número de piso y ala correspondiente seguido de una combinación de letras relacionadas con el departamento donde serán instalados. Aquellos equipos que dispongan de ranuras de expansión GBIC o SFP (mini GBIC) y controlen los enlaces hacia la Capa de Core/Distribución tendrán el número “1” al final de su nombre. Mientras que los dispositivos cuyo enlace se realice mediante agrupación de puertos (EtherChannel) podrán ser reconocidos por el número “2”.

Los nombres de los conmutadores de Core/Distribución estarán formados por la palabra TELE, seguido de las siglas SRV y la letra A o B, en razón de que estos equipos serán gestionados por el Departamento de Administración de Redes y Gestión de Fibra Óptica (Gerencia de Telecomunicaciones), actuarán como servidores en la configuración VTP (VLAN Trunking Protocol) y desempeñarán el papel de conmutadores raíz para distintos grupos de redes virtuales. La Tabla 3.11 muestra el número de piso, ala y codificación para cada conmutador.

Piso	Ala	Dispositivo	
Décimo	A	10APRESEJEC	-
	B	10BSECRGRAL	-
Noveno	A	9AVICETEC2	9AVICETEC1
	B	9BINVEDESA	-
Octavo	A	8ADIVSUBES	-
	B	8BDIVLINEA	-
Séptimo	A	7AOPEMTTO2	7AOPEMTTO1
	B	7BGESTDISP	-
Sexto	A	6ADPTOFINA	-
	B	6BVICEADMI	-
Quinto	A	5AADMINRED	-
	B	5BINFORMAT	-
Cuarto	A	-	-
	B	4BCONSTSEG	-
Tercero	A	3AADQUBOD2	3AADQUBOD1
	B	3BMTTOLINE	-
Segundo	A	2AGERTELE2	2AGERTELE1
	B	2BASESJUR1	2BASESJUR2
Planta Baja	A	PBADISPMEDI	-
	B	PBBAUDIINT1	PBBAUDIINT2

Tabla 3.11: Codificación para los Conmutadores de Acceso

3.2.4.1.4 Establecer las Contraseñas de Acceso

De aquí en adelante todas las contraseñas que se especifiquen serán utilizadas únicamente en ambiente de laboratorio, ya que las claves de producción se decidirán el momento de la implementación. Con el objeto de restringir el acceso al modo de consola se creará una contraseña única (trG5mn7NI) en todos los conmutadores. De igual manera, el acceso al modo de privilegio será protegido con una contraseña (c0m1A1n0d) para evitar el uso no autorizado, ya que algunos comandos se utilizan para configurar parámetros operativos. Ambas contraseñas estarán encriptadas mediante la funcionalidad propia de los equipos. Las conexiones remotas (líneas vty) se permitirán solamente a través de SSH (Secure Shell) para asegurar que la comunicación sea encriptada.

3.2.4.1.5 Configurar la Dirección de Capa 3

Para poder administrar los equipos de forma remota se asignará una dirección IP a cada conmutador. En la segunda posición del cuarto grupo de dígitos de la dirección de Capa 3 se hará referencia al número de piso donde se encuentra el dispositivo y la tercera cifra

indicará su distribución. Por ejemplo, la dirección 172.17.83.191 revelará que existe un conmutador en el noveno piso y ocupa el primer lugar en la clasificación. Aunque la configuración por defecto establece que la administración de los equipos está controlada a través de la VLAN 1, se utilizará la VLAN 83 porque se considera una buena práctica cambiar este parámetro. En la Tabla 3.12 se especifican las direcciones IP y máscara de subred para todos los conmutadores.

Dispositivo	Interfaz	Dirección IP	Máscara de Subred
TELESRVA	VLAN83	172.17.83.101	255.255.255.0
TELESRVB	VLAN83	172.17.83.102	255.255.255.0
10APRESEJEC	VLAN83	172.17.83.201	255.255.255.0
10BSECRGRAL	VLAN83	172.17.83.202	255.255.255.0
9AVICETEC2	VLAN83	172.17.83.191	255.255.255.0
9AVICETEC1	VLAN83	172.17.83.192	255.255.255.0
9BINVEDESA	VLAN83	172.17.83.193	255.255.255.0
8ADIVSUBES	VLAN83	172.17.83.181	255.255.255.0
8BDIVLINEA	VLAN83	172.17.83.182	255.255.255.0
7AOPEMTO2	VLAN83	172.17.83.171	255.255.255.0
7AOPEMTO1	VLAN83	172.17.83.172	255.255.255.0
7BGESTDISP	VLAN83	172.17.83.173	255.255.255.0
6ADPTOFINA	VLAN83	172.17.83.161	255.255.255.0
6BVICEADMI	VLAN83	172.17.83.162	255.255.255.0
5AADMINRED	VLAN83	172.17.83.151	255.255.255.0
5BINFORMAT	VLAN83	172.17.83.152	255.255.255.0
4BCONSTSEG	VLAN83	172.17.83.141	255.255.255.0
3AADQUBOD2	VLAN83	172.17.83.131	255.255.255.0
3AADQUBOD1	VLAN83	172.17.83.132	255.255.255.0
3BMTTOLINE	VLAN83	172.17.83.133	255.255.255.0
2AGERTELE2	VLAN83	172.17.83.121	255.255.255.0
2AGERTELE1	VLAN83	172.17.83.122	255.255.255.0
2BASESJUR1	VLAN83	172.17.83.123	255.255.255.0
2BASESJUR2	VLAN83	172.17.83.124	255.255.255.0
PBADISPMEDI	VLAN83	172.17.83.111	255.255.255.0
PBBAUDIINT1	VLAN83	172.17.83.112	255.255.255.0
PBBAUDIINT2	VLAN83	172.17.83.113	255.255.255.0

Tabla 3.12: Direccionamiento de los Conmutadores

3.2.4.1.6 Configurar la Seguridad de los Puertos de Acceso

Las interfaces 10/100 Ethernet de los conmutadores de Acceso podrán aceptar solamente tres dispositivos, aprenderán sus direcciones MAC dinámicamente y se

apagarán en caso de comprometer la seguridad. En tanto que las interfaces 10/100/1000 Ethernet de los conmutadores de Core/Distribución admitirán un solo equipo y mantendrán los parámetros indicados anteriormente.

3.2.4.2 Configuración de VTP

Por seguridad se deshabilitarán todos los puertos de los conmutadores. En vista de que se requieren 20 enlaces 10/100/1000 Ethernet para los servidores que controla el Departamento de Informática, se configurará en modo de acceso el rango de interfaces 1-20 en ambos dispositivos de Core/Distribución. La cantidad de usuarios en cada ala indicará el número de interfaces Fast Ethernet que serán habilitadas y configuradas en cada conmutador de Acceso. Después se revisarán los parámetros VTP por defecto (versión, número de revisión de configuración, número de VLANs existentes, modo de operación y nombre de dominio) en todos los conmutadores.

3.2.4.2.1 Configurar el Modo de Operación, Nombre de Dominio y Contraseña

Para controlar las instancias VLAN en la red se creará un dominio cuyo nombre será TRANSELECTRIC y una clave (DsnartMcirtceleN) en los conmutadores. Ambos dispositivos de Core/Distribución operarán en modo servidor de manera que las VLANs sean distribuidas a los conmutadores de Acceso que funcionarán como clientes.

3.2.4.2.2 Configurar los Enlaces Troncales y la VLAN Nativa

Las dos interfaces Gigabit Ethernet que tiene incorporada la tarjeta supervisora se establecerán como enlaces troncales entre los conmutadores de Core/Distribución. Asimismo, las interfaces 1-19 de la tarjeta de 24 módulos SFP se utilizarán como troncales hacia los equipos de Acceso. En ambos casos se especificará la VLAN 83 como nativa.

3.2.4.2.3 Configurar las VLANs en los Servidores VTP

De acuerdo con los requerimientos de la Compañía se creará una VLAN por piso, otra para los servidores y una adicional para asuntos administrativos. A cada red virtual se le asignará un nombre compuesto por palabras clave que permitan identificar los departamentos de un mismo piso. La Tabla 3.13 muestra los nombres que se asignarán a las 12 VLANs. Luego se verificará que los conmutadores de Acceso dispongan de esta información.

Piso	Número	Nombre
Décimo	20	Presidencia/Secretaría
Noveno	19	Vicepresidencia/Investigación
Octavo	18	Subestaciones/Líneas
Séptimo	17	Operación/Disponibilidad
Sexto	16	Financiero/Administración
Quinto	15	Redes/Informática
Cuarto	14	Construcción/Seguros
Tercero	13	Mantenimiento/Adquisiciones
Segundo	12	Telecomunicaciones/Jurídica
Planta Baja	11	Médico/Auditoría
	10	Servidores
	83	Administrativa

Tabla 3.13: Número y Nombre de las VLANs

3.2.4.2.4 *Asignar los Puertos de los Conmutadores a las VLANs*

Dada la índole geográfica de las redes virtuales que serán configuradas, todos los puertos de los conmutadores de Acceso instalados en un mismo piso estarán asociados a una sola VLAN. La creación de una VLAN exclusiva para los servidores implica que los puertos 1-20 de los conmutadores de Core/Distribución estarán asociados a dicha red.

3.2.4.3 **Configuración de STP**

Como existe una instancia distinta de STP para cada VLAN activa, se produce una elección del Conmutador Raíz por cada instancia. Si se utilizan las prioridades por defecto en este proceso, el mismo dispositivo se convierte en el Conmutador Raíz para cada STP. Para controlar dicha situación y evitar la subutilización de los enlaces troncales disponibles se obligará a que uno de los equipos de Core/Distribución sea el Conmutador Raíz para las 6 primeras VLANs (10-15) y actúe como respaldo para el otro grupo. De manera análoga, el segundo dispositivo de Core/Distribución será el Conmutador Raíz para las 6 últimas VLANs (16-20 y 83) y controlará el otro grupo en caso de falla del equipo principal.

3.2.4.4 **Configuración de EtherChannel**

A fin de evitar que se produzcan lazos entre los conmutadores de Core/Distribución se agruparán las troncales en un solo canal lógico. En aquellos pisos que requieran enlaces

troncales entre conmutadores de Acceso se juntarán dos puertos Fast Ethernet utilizando esta tecnología.

3.2.4.5 Configuración de HSRP (Hot Standby Router Protocol)

El par de conmutadores de Core/Distribución actuarán como una sola puerta de enlace predeterminada. Uno de estos equipos se establecerá como primario (activo) para las VLANs impares (11, 13, 15, 17, 19 y 83) y será el standby para las demás redes virtuales. Asimismo, el segundo dispositivo tendrá una prioridad alta para las VLANs pares (10, 12, 14, 16, 18 y 20) y se mantendrá alerta por si ocurre un desperfecto. De esta forma, en caso de que el conmutador activo falle, inmediatamente el standby ocupará su lugar.

3.2.4.6 Configuración de SNMP (Simple Network Management Protocol)

Para administrar los equipos a través del formato de mensajes SNMP se definirá una comunidad de lectura-escritura, habilitarán las notificaciones disponibles, especificarán los conmutadores que recibirán las alertas y utilizará la versión 2c de este protocolo.

3.2.5 Simulación en Packet Tracer

3.2.5.1 Configuración Básica

En el programa de simulación de redes Packet Tracer se creó la topología propuesta, ubicando los conmutadores de Core/Distribución en el centro del espacio de trabajo y los dispositivos de Acceso en ambos extremos como se observa en la Figura 3.79.

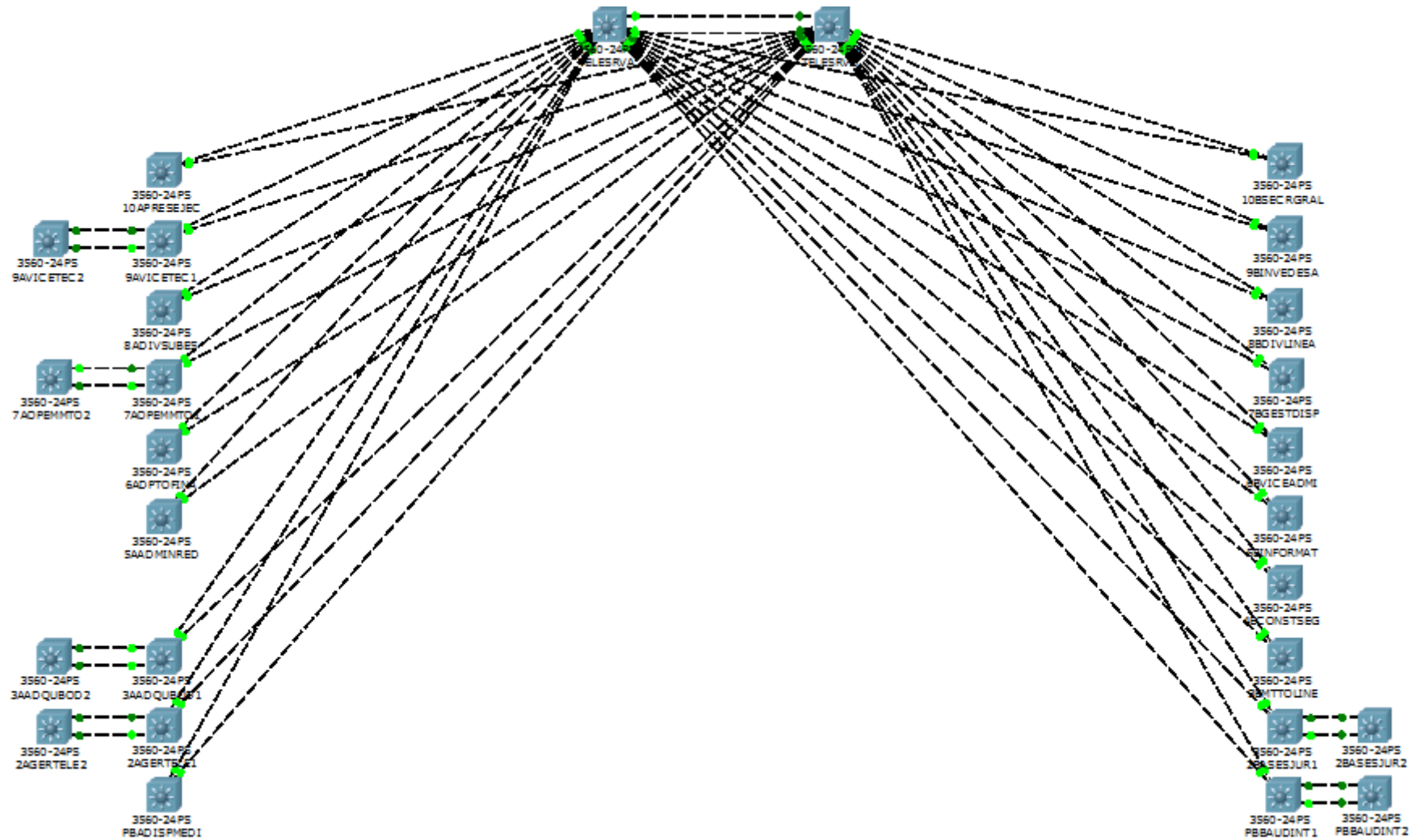


Figura 3.79: Topología de Red en Programa de Simulación

3.2.5.1.1 Borrar Base de Datos VLAN y Configuración

El primer paso consistió en borrar la configuración de todos los conmutadores. La Figura 3.80 muestra cómo se ingresó al modo de privilegio y se borró el archivo de información de la base de datos VLAN. El mensaje de error apareció porque no existía tal archivo.

```
Switch>enable
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)
```

Figura 3.80: Borrado de la Base de Datos VLAN

Además se borró el archivo startup-config de la NVRAM con el comando de la Figura 3.81. Para verificar que la información VLAN fue borrada se utilizó el comando `show vlan`. En la Figura 3.82 se puede ver que solamente existían las VLANs por defecto (1, 1002, 1003, 1004 y 1005), la VLAN 1 estaba activa, su nombre era “default” y todos los puertos estaban asignados a dicha red virtual.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Figura 3.81: Borrado de la Configuración

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	-	0	0

Figura 3.82: Información VLAN

3.2.5.1.2 Verificar Configuración por Defecto

Con el comando **show running-config** se examinó la configuración actual. Las Figuras 3.83a y 3.83b muestran que los conmutadores tenían 24 interfaces Fast Ethernet, 2 Gigabit Ethernet y que el rango para las líneas vty era de 0 a 4.

```

Building configuration...                               !
Current configuration : 984 bytes                       !
!                                                      !
version 12.2                                           !
no service password-encryption                       !
!                                                      !
hostname Switch                                       !
!                                                      !
!                                                      !
!                                                      !
!                                                      !
ip ssh version 1                                       !
!                                                      !
port-channel load-balance src-mac                    !
!                                                      !
interface FastEthernet0/1                             !
!                                                      !
interface FastEthernet0/2                             !
!                                                      !
interface FastEthernet0/3                             !
--More--                                             !
!                                                      !
interface FastEthernet0/4                             !
!                                                      !
interface FastEthernet0/5                             !
!                                                      !
interface FastEthernet0/6                             !
!                                                      !
interface FastEthernet0/7                             !
!                                                      !
interface FastEthernet0/8                             !
!                                                      !
interface FastEthernet0/9                             !
!                                                      !
interface FastEthernet0/10                            !
!                                                      !
interface FastEthernet0/11                            !
!                                                      !
interface FastEthernet0/12                            !
!                                                      !
interface FastEthernet0/13                            !
!                                                      !
interface FastEthernet0/14                            !
--More--

```

Figura 3.83a: Archivo de Configuración (1 de 2)

```

!                                                      !
interface FastEthernet0/15                            !
!                                                      !
interface FastEthernet0/16                            !
!                                                      !
interface FastEthernet0/17                            !
!                                                      !
interface FastEthernet0/18                            !
!                                                      !
interface FastEthernet0/19                            !
!                                                      !
interface FastEthernet0/20                            !
!                                                      !
interface FastEthernet0/21                            !
!                                                      !
interface FastEthernet0/22                            !
!                                                      !
interface FastEthernet0/23                            !
!                                                      !
interface FastEthernet0/24                            !
!                                                      !
interface GigabitEthernet0/1                          !
--More-- |                                           !
!                                                      !
interface GigabitEthernet0/1                          !
!                                                      !
interface GigabitEthernet0/2                          !
!                                                      !
interface Vlan1                                       !
no ip address                                         !
shutdown                                             !
!                                                      !
ip classless                                         !
!                                                      !
!                                                      !
!                                                      !
!                                                      !
line con 0                                           !
line vty 0 4                                         !
login                                               !
!                                                      !
!                                                      !
end
Switch#

```

Figura 3.83b: Archivo de Configuración (2 de 2)

A fin de examinar las características de la interfaz virtual VLAN 1 se ejecutó el comando `show interface vlan1` y se pudo constatar que no existía una dirección IP en los conmutadores pero si tenían dirección MAC y que la interfaz estaba apagada. En el caso del conmutador de Core/Distribución (Figura 3.84) la segunda línea indica que la interfaz estaba apagada (administratively down, line protocol is down) y la tercera especifica la dirección MAC (0009.7c77.c389).

```
Switch#show interface vlan1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0009.7c77.c389 (bia 0009.7c77.c389)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1682 packets input, 530955 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    563859 packets output, 0 bytes, 0 underruns
    0 output errors, 23 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Figura 3.84: Información de la Interfaz VLAN 1

El siguiente paso fue consultar la información del sistema operativo de red. Mediante el comando `show version` se identificó la versión del IOS como 12.2(37)SE1, el nombre del archivo de la imagen del sistema (C3560-ADVIPSERVICESK) y la dirección MAC de uno de los conmutadores de Core/Distribución (0009.7C77.C389), tal como indican las Figuras 3.85a, 3.85b y 3.85c.

```
ROM: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (f
c4)
```

```
System returned to ROM by power-on
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

```
If you require further assistance please contact us by sending email to
export@cisco.com.
```

```
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 122880K/8184K byte
s of memory.
```

```
--More-- |
```

Figura 3.85a: Información de un Conmutador (1 de 3)

```
Processor board ID CAT1037RJF7
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0009.7C77.C389
Motherboard assembly number     : 73-9673-09
Power supply part number        : 341-0029-05
Motherboard serial number       : CAT103758VY
Power supply serial number       : DTH1036C7UB
Model revision number           : P0
Motherboard revision number     : A0
Model number                    : WS-C3560-24PS-E
System serial number            : CAT1037RJF7
Top Assembly Part Number        : 800-26380-04
Top Assembly Revision Number    : B0
Version ID                      : V06
CLEI Code Number                : COM1100ARC
Hardware Board Revision Number  : 0x01
```

Figura 3.85b: Información de un Conmutador (2 de 3)

Switch	Ports	Model	SW Version	SW Image
* 1	26	WS-C3560-24PS	12.2(37)SE1	C3560-ADVIPSERVICESK

```
Configuration register is 0xF
```

```
Switch#
```

Figura 3.85c: Información de un Conmutador (3 de 3)

3.2.5.2 Capa de Core/Distribución

3.2.5.2.1 Asignar Nombres y Establecer Contraseñas

La Figura 3.86 muestra cómo se asignó el nombre al dispositivo de Core/Distribución para el Ala Occidental. Asimismo, se ingresó al modo de configuración de línea para establecer la misma contraseña de consola (trG5mn7Nl) en ambos conmutadores. Para proteger el acceso al modo de privilegio se incluyó la contraseña c0m1A1n0d. Los comandos que se utilizaron para ambas contraseñas se presentan en la Figura 3.87. El comando `service password-encryption` garantiza que todas las contraseñas sean encriptadas.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname TELESRVA
TELESRVA(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 3.86: Nombre de Conmutador de Core/Distribución

```
TELESRVA(config)#service password-encryption
TELESRVA(config)#line console 0
TELESRVA(config-line)#password trG5mn7Nl
TELESRVA(config-line)#login
TELESRVA(config-line)#exit
TELESRVA(config)#enable secret c0m1A1n0d
TELESRVA(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 3.87: Contraseñas de Consola y de Acceso al Modo de Privilegio

Con el objeto de que las conexiones remotas se lleven a cabo mediante SSH (Secure Shell) se creó un dominio, generaron las llaves RSA (Ronald Rivest, Adi Shamir & Leonard Adleman) de 1024 bits y se definió un nombre de usuario con la respectiva contraseña (Figura 3.88).

```

TELESRVA(config)#ip domain-name transelectric.com
TELESRVA(config)#crypto key generate rsa
The name for the keys will be: TELESRVA.transelectric.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

TELESRVA(config)#username cgtt password aR3M0eS
TELESRVA(config)#line vty 0 4
TELESRVA(config-line)#transport input ssh

```

Figura 3.88: Acceso Remoto con SSH

3.2.5.2.2 Apagar Puertos

Por seguridad se deshabilitaron todos los puertos de los conmutadores utilizando los comandos de las Figuras 3.89a y 3.89b.

```

TELESRVA(config)#interface range FastEthernet 0/1 - 24
TELESRVA(config-if-range)#shutdown

```

Figura 3.89a: Apagado de Interfaces Fast Ethernet en Conmutador de Core/Distribución

```

TELESRVA(config)#interface range GigabitEthernet 0/1 - 2
TELESRVA(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively
down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively
down

```

Figura 3.89b: Apagado de Interfaces Gigabit Ethernet en Conmutador de Core/Distribución

3.2.5.2.3 Configuración de VTP (VLAN Trunking Protocol)

Con el objeto de revisar los parámetros VTP existentes en los conmutadores se ejecutó el comando `show vtp status`. La Figura 3.90 muestra que la versión VTP era la 2, el número de revisión de configuración 0, el número máximo de VLANs admitidas 1005, el número de VLANs existentes 5 y el modo de operación VTP servidor.

```

TELESRVA#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           :
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

```

Figura 3.90: Estado VTP por Defecto en Conmutador de Core/Distribución

3.2.5.2.3.1 Establecer Modo de Operación, Nombre de Dominio y Contraseña

A continuación se configuró el modo de operación, nombre de dominio y contraseña VTP en los conmutadores mediante los comandos de la Figura 3.91.

```

TELESRVA(config)#vtp mode server
Device mode already VTP SERVER.
TELESRVA(config)#vtp domain TRANSELECTRIC
Changing VTP domain name from NULL to TRANSELECTRIC
TELESRVA(config)#vtp password DsnartMcirtceleN
Setting device VLAN database password to DsnartMcirtceleN
TELESRVA(config)#end
%SYS-5-CONFIG_I: Configured from console by console

```

Figura 3.91: Modo de Operación, Nombre de Dominio y Contraseña en Servidor VTP

3.2.5.2.3.2 Crear y Nombrar VLANs

En base a los requerimientos de la Compañía se configuraron 10 VLANs (una por cada piso). También se añadió una VLAN para los servidores y otra para cuestiones de administración. Las Figuras 3.92a y 3.92b muestran la creación de cada VLAN y el nombre asociado.

```

TELESRVA(config)#vlan 83
TELESRVA(config-vlan)#name Administrativa
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 10
TELESRVA(config-vlan)#name Servidores
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 11
TELESRVA(config-vlan)#name Medico/Auditoria
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 12
TELESRVA(config-vlan)#name Telecomunicaciones/Juridica
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 13
TELESRVA(config-vlan)#name Mantenimiento/Adquisiciones
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 14
TELESRVA(config-vlan)#name Construccion/Seguros
TELESRVA(config-vlan)#exit

```

Figura 3.92a: Números y Nombres de VLANs (1 de 2)

```

TELESRVA(config)#vlan 15
TELESRVA(config-vlan)#name Redes/Informatica
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 16
TELESRVA(config-vlan)#name Financiero/Administracion
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 17
TELESRVA(config-vlan)#name Operacion/Disponibilidad
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 18
TELESRVA(config-vlan)#name Subestaciones/Lineas
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 19
TELESRVA(config-vlan)#name Vicepresidencia/Investigacion
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 20
TELESRVA(config-vlan)#name Presidencia/Secretaria
TELESRVA(config-vlan)#exit

```

Figura 3.92b: Números y Nombres de VLANs (2 de 2)

Digitando el comando `show vlan brief` se pudo verificar que las 12 VLANs fueron creadas en los conmutadores de Core/Distribución (Figura 3.93).

```

TELESRVA#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/4, Fa0/21, Fa0/22
10   Servidores              active    Fa0/23, Fa0/24
11   Medico/Auditoria       active
12   Telecomunicaciones/Juridica active
13   Mantenimiento/Adquisiciones active
14   Construccion/Seguros   active
15   Redes/Informatica      active
16   Financiero/Administracion active
17   Operacion/Disponibilidad active
18   Subestaciones/Lineas   active
19   Vicepresidencia/Investigacion active
20   Presidencia/Secretaria active
83   Administrativa          active
1002 fddi-default            active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default         active
TELESRVA#

```

Figura 3.93: Estado de VLANs en Conmutador de Core/Distribución

3.2.5.2.3.3 Configurar Direcciones de Capa 3

Luego se configuró la dirección de la interfaz de administración en cada conmutador. Este procedimiento se muestra en las Figuras 3.94a y 3.94b.

```

TELESRVA(config)#interface vlan 83

%LINK-5-CHANGED: Interface Vlan83, changed state to upTELESRVA(config-if)#
TELESRVA(config-if)#ip address 172.17.83.101 255.255.255.0
TELESRVA(config-if)#no shutdown

```

Figura 3.94a: Interfaz VLAN 83 del Conmutador TELESRVA

```

TELESRVB(config)#interface vlan 83

%LINK-5-CHANGED: Interface Vlan83, changed state to upTELESRVB(config-if)#
TELESRVB(config-if)#ip address 172.17.83.102 255.255.255.0
TELESRVB(config-if)#no shutdown

```

Figura 3.94b: Interfaz VLAN 83 del Conmutador TELESRVB

3.2.5.2.3.4 Establecer Enlaces Troncales y VLAN Nativa

En vista de que los conmutadores del programa de simulación no contaban con ranuras de expansión para módulos GBIC o SFP, los enlaces troncales se configuraron en las interfaces Gigabit Ethernet entre los dos conmutadores de Core/Distribución (Figura 3.95a) y en las interfaces Fast Ethernet entre los conmutadores de Acceso y Core/Distribución (Figuras 3.95b y 3.95c) según la Tabla 3.14.

Core/Distribución		Acceso	
Dispositivo	Interfaz (Fa)	Dispositivo	Interfaz (Fa)
TELESRVA	0/1	PBADISPMEDI	0/1
	0/2	2AGERTELE1	
	0/3	3AADQUBOD1	
	0/4	-	
	0/5	5AADMINRED	
	0/6	6ADPTOFINA	
	0/7	7AOPEMTO1	
	0/8	8ADIVSUBES	
	0/9	9AVICETEC1	
	0/10	10APRESEJEC	
	0/11	PBBAUDIINT1	0/2
	0/12	2BASESJUR1	
	0/13	3BMTTOLINE	
	0/14	4BCONSTSEG	
	0/15	5BINFORMAT	
	0/16	6BVICEADMI	
	0/17	7BGESTDISP	
	0/18	8BDIVLINEA	
	0/19	9BINVEDESA	
	0/20	10BSECRGRAL	
	0/21	-	
	0/22	-	
	0/23	-	
	0/24	-	

Core/Distribución		Acceso	
Dispositivo	Interfaz (Fa)	Dispositivo	Interfaz (Fa)
TELESRVB	0/1	PBBAUDIINT1	0/1
	0/2	2BASESJUR1	
	0/3	3BMTTOLINE	
	0/4	4BCONSTSEG	
	0/5	5BINFORMAT	
	0/6	6BVICEADMI	
	0/7	7BGESTDISP	
	0/8	8BDIVLINEA	
	0/9	9BINVEDESA	
	0/10	10BSECRGRAL	
	0/11	PBADISPMEDI	0/2
	0/12	2AGERTELE1	
	0/13	3AADQUBOD1	
	0/14	-	
	0/15	5AADMINRED	
	0/16	6ADPTOFINA	
	0/17	7AOPEMTO1	
	0/18	8ADIVSUBES	
	0/19	9AVICETEC1	
	0/20	10APRESEJEC	
	0/21	-	
	0/22	-	
	0/23	-	
	0/24	-	

Tabla 3.14: Enlaces Troncales entre las Capas de Core/Distribución y de Acceso

```
TELESRVA(config)#interface range GigabitEthernet 0/1 - 2
TELESRVA(config-if-range)#switchport mode trunk
TELESRVA(config-if-range)#switchport trunk native vlan 83
TELESRVA(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to down
```

Figura 3.95a: Enlaces Troncales en la Capa de Core/Distribución

```

TELESRVA(config)#interface range FastEthernet 0/1 - 3
TELESRVA(config-if-range)#switchport mode trunk
TELESRVA(config-if-range)#switchport trunk native vlan 83
TELESRVA(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down

```

Figura 3.95b: Enlaces Troncales entre las Capas de Core/Distribución y Acceso (1 de 2)

```

TELESRVA(config)#interface range FastEthernet 0/5 - 20
TELESRVA(config-if-range)#switchport mode trunk
TELESRVA(config-if-range)#switchport trunk native vlan 83
TELESRVA(config-if-range)#no shutdown

```

Figura 3.95c: Enlaces Troncales entre las Capas de Core/Distribución y Acceso (2 de 2)

3.2.5.2.4 Agrupar Puertos

Para que los enlaces troncales entre los conmutadores de Core/Distribución trabajen en conjunto se creó una interfaz lógica, en la cual se definió el modo troncal y la VLAN nativa como se aprecia en la Figura 3.96. Los mismos parámetros se configuraron en las interfaces Gigabit Ethernet para agruparlas y obligarlas a que funcionen como EtherChannel (Figuras 3.97 y 3.98).

```

TELESRVA(config)#interface port-channel 1
TELESRVA(config-if)#switchport mode trunk
TELESRVA(config-if)#switchport trunk native vlan 83

```

Figura 3.96: Interface Port-Channel en la Capa de Core/Distribución

```

TELESRVA(config)#interface range GigabitEthernet 0/1 - 2
TELESRVA(config-if-range)#switchport mode trunk
TELESRVA(config-if-range)#switchport trunk native vlan 83

```

Figura 3.97: Modo Troncal y VLAN Nativa en la Capa de Core/Distribución

```

TELESRVA(config)#interface GigabitEthernet 0/1
TELESRVA(config-if)#channel-group 1 mode on

%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to
up
TELESRVA(config-if)#exit
TELESRVA(config)#interface GigabitEthernet 0/2
TELESRVA(config-if)#channel-group 1 mode on
TELESRVA(config-if)#exit

```

Figura 3.98: Agrupación de Puertos en el Canal Lógico de la Capa de Core/Distribución

Cuando se ejecutó el comando `show etherchannel summary` (Figura 3.99) se constató que ambas interfaces Gigabit Ethernet formaban parte del canal lógico establecido entre los conmutadores de Core/Distribución debido a la presencia de la bandera P junto a dichos puertos.

```

TELESRVA#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1            PAgP       Gig0/1(P) Gig0/2(P)
TELESRVA#

```

Figura 3.99: Estado del EtherChannel entre Conmutadores de Core/Distribución

3.2.5.2.5 Asignar Puertos de Acceso

Las interfaces Fast Ethernet 0/23 y 0/24 fueron configuradas en modo de acceso, vinculadas a la red virtual de servidores (VLAN 10) y habilitadas como se muestra en las Figuras 3.100a y 3.100b.

```

TELESRVA(config)#interface range FastEthernet 0/23 - 24
TELESRVA(config-if-range)#switchport mode access
TELESRVA(config-if-range)#switchport access vlan 10
TELESRVA(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to down

```

Figura 3.100a: Modo de Acceso y Asignación VLAN en el Conmutador TELESRVA

```

TELESRVB(config)#interface range FastEthernet 0/23 - 24
TELESRVB(config-if-range)#switchport mode access
TELESRVB(config-if-range)#switchport access vlan 10
TELESRVB(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to down

```

Figura 3.100b: Modo de Acceso y Asignación VLAN en el Conmutador TELESRVB

3.2.5.2.6 Configuración STP (Spanning Tree Protocol)

El control del primer grupo de VLANs (10-15) se adjudicó al conmutador TELESRVA y el segundo (16-20 y 83) al dispositivo TELESRVB. Si uno de los equipos experimenta algún tipo de falla, el otro cumplirá sus funciones (Figuras 3.101a y 3.101b).

```

TELESRVA(config)#spanning-tree vlan 10-15 root primary
TELESRVA(config)#spanning-tree vlan 16-20,83 root secondary

```

Figura 3.101a: Conmutador Raíz para las VLANs 10-15

```

TELESRVB(config)#spanning-tree vlan 16-20,83 root primary
TELESRVB(config)#spanning-tree vlan 10-15 root secondary

```

Figura 3.101b: Conmutador Raíz para las VLANs 16-20 y 83

Mediante el comando **show spanning-tree vlan 10** (Figura 3.102a) se comprobó que el dispositivo TELESRVA era el Conmutador Raíz para la red virtual de servidores, pues el valor de la prioridad era 24586, apareció el mensaje “This bridge is the root” y todos los puertos tenían el rol de Designados. La Figura 3.102b indica que el dispositivo

TELESRVA no era el Conmutador Raíz para la VLAN Administrativa (83), ya que la prioridad era menor y existía un puerto Raíz.

```

TELESRVA#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0009.7C77.C389
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586 (priority 24576 sys-id-ext 10)
             Address     0009.7C77.C389
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/3	Desg	FWD	19	128.3	P2p
Fa0/5	Desg	FWD	19	128.5	P2p
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/7	Desg	FWD	19	128.7	P2p
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/9	Desg	FWD	19	128.9	P2p
Fa0/10	Desg	FWD	19	128.10	P2p
Fa0/11	Desg	FWD	19	128.11	P2p
Fa0/12	Desg	FWD	19	128.12	P2p
Fa0/13	Desg	FWD	19	128.13	P2p
Fa0/14	Desg	FWD	19	128.14	P2p
Fa0/15	Desg	FWD	19	128.15	P2p
Fa0/16	Desg	FWD	19	128.16	P2p
Fa0/17	Desg	FWD	19	128.17	P2p
Fa0/18	Desg	FWD	19	128.18	P2p
Fa0/19	Desg	FWD	19	128.19	P2p
Fa0/20	Desg	FWD	19	128.20	P2p
Gi0/1	Desg	FWD	4	128.25	P2p
Gi0/2	Desg	FWD	4	128.26	P2p
Po1	Desg	FWD	19	128.27	Shr

Figura 3.102a: Estado de STP para la VLAN 10 en el Conmutador TELESRVA

```

TELESRVA#show spanning-tree vlan 83
VLAN0083
  Spanning tree enabled protocol ieee
  Root ID    Priority    24659
            Address    0060.47E8.A95C
            Cost      19
            Port      28 (Port-channel 1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28755  (priority 28672 sys-id-ext 83)
            Address    0009.7C77.C389
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Desg FWD 19        128.1   P2p
Fa0/2              Desg FWD 19        128.2   P2p
Fa0/3              Desg FWD 19        128.3   P2p
Fa0/5              Desg FWD 19        128.5   P2p
Fa0/6              Desg FWD 19        128.6   P2p
Fa0/7              Desg FWD 19        128.7   P2p
Fa0/8              Desg FWD 19        128.8   P2p
Fa0/9              Desg FWD 19        128.9   P2p
Fa0/10             Desg FWD 19        128.10  P2p
Fa0/11             Desg FWD 19        128.11  P2p
Fa0/12             Desg FWD 19        128.12  P2p
Fa0/13             Desg FWD 19        128.13  P2p
Po1                Root FWD 19        128.28  Shr
Fa0/14             Desg FWD 19        128.14  P2p
Fa0/15             Desg FWD 19        128.15  P2p
Fa0/16             Desg FWD 19        128.16  P2p
Fa0/17             Desg FWD 19        128.17  P2p
Fa0/18             Desg FWD 19        128.18  P2p
Fa0/19             Desg FWD 19        128.19  P2p
Fa0/20             Desg FWD 19        128.20  P2p
Gi0/1              Desg FWD 4         128.25  P2p
Gi0/2              Desg FWD 4         128.26  P2p

```

Figura 3.102b: Estado de STP para la VLAN 83 en el Conmutador TELESRVA

Por otra parte, según la información de la Figura 3.103a, el Conmutador Raíz para la VLAN 83 era el equipo TELESRVB. En tanto que el manejo de la red virtual de servidores no estaba asignado a este dispositivo (Figura 3.103b).

```

TELESRVB#show spanning-tree vlan 83
VLAN0083
  Spanning tree enabled protocol ieee
  Root ID    Priority    24659
             Address     0060.47E8.A95C
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24659  (priority 24576 sys-id-ext 83)
             Address     0060.47E8.A95C
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20

Interface                Role Sts Cost          Prio.Nbr Type
-----
Fa0/1                    Desg FWD 19            128.1   P2p
Fa0/2                    Desg FWD 19            128.2   P2p
Fa0/3                    Desg FWD 19            128.3   P2p
Fa0/4                    Desg FWD 19            128.4   P2p
Fa0/5                    Desg FWD 19            128.5   P2p
Fa0/6                    Desg FWD 19            128.6   P2p
Fa0/7                    Desg FWD 19            128.7   P2p
Fa0/8                    Desg FWD 19            128.8   P2p
Fa0/9                    Desg FWD 19            128.9   P2p
Fa0/10                   Desg FWD 19            128.10  P2p
Fa0/11                   Desg FWD 19            128.11  P2p
Fa0/12                   Desg FWD 19            128.12  P2p
Fa0/13                   Desg FWD 19            128.13  P2p
Fa0/15                   Desg FWD 19            128.15  P2p
Fa0/16                   Desg FWD 19            128.16  P2p
Fa0/17                   Desg FWD 19            128.17  P2p
Fa0/18                   Desg FWD 19            128.18  P2p
Fa0/19                   Desg FWD 19            128.19  P2p
Fa0/20                   Desg FWD 19            128.20  P2p
Gi0/1                    Desg FWD 4             128.25  P2p
Gi0/2                    Desg FWD 4             128.26  P2p
Po1                      Desg FWD 19            128.28  Shr

```

Figura 3.103a: Estado de STP para la VLAN 83 en el Conmutador TELESRVB

```

TELESRVB#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
            Address    0009.7C77.C389
            Cost      19
            Port      27 (Port-channel 1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28682 (priority 28672 sys-id-ext 10)
            Address    0060.47E8.A95C
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa0/1                    Desg FWD 19        128.1   P2p
Fa0/2                    Desg FWD 19        128.2   P2p
Fa0/3                    Desg FWD 19        128.3   P2p
Fa0/4                    Desg FWD 19        128.4   P2p
Fa0/5                    Desg FWD 19        128.5   P2p
Fa0/6                    Desg FWD 19        128.6   P2p
Fa0/7                    Desg FWD 19        128.7   P2p
Fa0/8                    Desg FWD 19        128.8   P2p
Fa0/9                    Desg FWD 19        128.9   P2p
Fa0/10                   Desg FWD 19        128.10  P2p
Fa0/11                   Desg FWD 19        128.11  P2p
Fa0/12                   Desg FWD 19        128.12  P2p
Fa0/13                   Desg FWD 19        128.13  P2p
Fa0/15                   Desg FWD 19        128.15  P2p
Po1                      Root FWD 19        128.27  Shr
Fa0/16                   Desg FWD 19        128.16  P2p
Fa0/17                   Desg FWD 19        128.17  P2p
Fa0/18                   Desg FWD 19        128.18  P2p
Fa0/19                   Desg FWD 19        128.19  P2p
Fa0/20                   Desg FWD 19        128.20  P2p
Gi0/1                    Desg FWD 4         128.25  P2p
Gi0/2                    Desg FWD 4         128.26  P2p

```

Figura 3.103b: Estado de STP para la VLAN 10 en el Conmutador TELESRVB

3.2.5.2.7 Grabar Configuración

Para grabar los cambios realizados se digitó el comando `copy running-config startup-config` tal como se observa en la Figura 3.104.

```

TELESRVA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

Figura 3.104: Copiado del Archivo de Configuración

3.2.5.3 Capa de Acceso

3.2.5.3.1 Configuración Básica

3.2.5.3.1.1 Borrar y Verificar VLANs por Defecto

En todos los conmutadores de Acceso se borró la base de datos VLAN y el archivo de configuración utilizando los comandos de las Figuras 3.105a y 3.105b.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)
```

Figura 3.105a: Borrado del Archivo vlan.dat

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Figura 3.105b: Borrado del Archivo startup-config

Para revisar que el procedimiento anterior surtió efecto se ingresó el comando `show vlan brief`. La Figura 3.106 muestra que únicamente existían las VLANs por defecto y que todos los puertos estaban asignados a la VLAN 1.

```
10APRESEJEC#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figura 3.106: Información de VLANs y Puertos Asociados

3.2.5.3.1.2 Asignar Nombres y Establecer Contraseñas

Los nombres de los conmutadores de Acceso se configuraron con el comando `hostname`. En las Figuras 3.107a y 3.107b se incluye la asignación para los conmutadores del décimo piso. Las contraseñas de consola y de acceso al modo de privilegio se configuraron de manera idéntica que en los conmutadores de Core/Distribución.

```
Switch(config)#hostname 10APRESEJEC
10APRESEJEC(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
10APRESEJEC#
```

Figura 3.107a: Nombre de Conmutador de Acceso en el Ala Oriental

```
Switch(config)#hostname 10BSECRGRAL
10BSECRGRAL(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
10BSECRGRAL#
```

Figura 3.107b: Nombre de Conmutador de Acceso en el Ala Occidental

3.2.5.3.1.3 Apagar Puertos

Como medida de precaución se deshabilitaron todas las interfaces de los conmutadores de Acceso. El comando `interface range` facilitó esta tarea, ya que permite configurar un grupo de puertos (Figuras 3.108a y 3.108b).

```
10APRESEJEC(config)#interface range GigabitEthernet 0/1 - 2
10APRESEJEC(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively
down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively
down
```

Figura 3.108a: Apagado de Interfaces Gigabit Ethernet en Conmutador de Acceso

```
10APRESEJEC(config)#interface range FastEthernet 0/1 - 24
10APRESEJEC(config-if-range)#shutdown
```

Figura 3.108b: Apagado de Interfaces Fast Ethernet en Conmutador de Acceso

3.2.5.3.2 Configuración VTP (VLAN Trunking Protocol)

Para verificar que los parámetros VTP por defecto estaban presentes en los conmutadores, se recurrió al comando `show vtp status`. En la Figura 3.109 se observa la versión VTP (2), número de revisión de configuración (0), cantidad de VLANs admitidas localmente (1005), número de VLANs existentes (5), modo de operación (servidor) y nombre de dominio (null).

```
10APRESEJEC#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            :
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MDS digest                  : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Figura 3.109: Estado VTP por Defecto en Conmutador de Acceso

3.2.5.3.2.1 Establecer Modo de Operación, Nombre de Dominio y Contraseña

El nombre de dominio (TRANSELECTRIC) y contraseña (DsnartMcirtceleN) se conservaron, pero el modo de operación se definió como cliente. La Figura 3.110 muestra los comandos que fueron aplicados. Luego de ejecutar el comando `show vtp status` fue posible comprobar los nuevos parámetros de los equipos (Figura 3.111).

```
10APRESEJEC(config)#vtp mode client
Setting device to VTP CLIENT mode.
10APRESEJEC(config)#vtp domain TRANSELECTRIC
Changing VTP domain name from NULL to TRANSELECTRIC
10APRESEJEC(config)#vtp password DsnartMcirtceleN
Setting device VLAN database password to DsnartMcirtceleN
10APRESEJEC(config)#end
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 3.110: Modo de Operación, Nombre de Dominio y Contraseña en Cliente VTP

```

10APRESEJEC#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode         : Client
VTP Domain Name            : TRANSELECTRIC
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xF5 0x7C 0xA3 0x0B 0x62 0x50 0x8E 0xC3
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

```

Figura 3.111: Modo de Operación Cliente y Nombre de Dominio TRANSELECTRIC

3.2.5.3.2.2 Establecer Enlaces Troncales y VLAN Nativa

A fin de que los conmutadores puedan intercambiar la información VLAN, las interfaces Fast Ethernet 0/1 y 0/2 se configuraron como enlaces troncales. Los comandos de la Figura 3.112 permitieron establecer el modo troncal, definir la VLAN nativa y habilitar los puertos.

```

10APRESEJEC(config)#interface range FastEthernet 0/1 - 2
10APRESEJEC(config-if-range)#switchport mode trunk
10APRESEJEC(config-if-range)#switchport trunk native vlan 83
10APRESEJEC(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

```

Figura 3.112: Modo Troncal y VLAN Nativa en Conmutador de Acceso

3.2.5.3.3 Agrupar Puertos

El canal lógico entre los conmutadores de Acceso requirió establecer el modo troncal y la VLAN nativa (Figura 3.113a). Además, fue necesario configurar estos parámetros en las interfaces Fast Ethernet 0/3 y 0/4, las cuales se asociaron al EtherChannel, obligándolas a trabajar en conjunto (Figuras 3.113b y 3.113c).

```

9AVICETEC1(config)#interface port-channel 1
9AVICETEC1(config-if)#switchport mode trunk
9AVICETEC1(config-if)#switchport trunk native vlan 83

```

Figura 3.113a: Interface Port-Channel en la Capa de Acceso

```

9AVICETEC1(config)#interface range FastEthernet 0/3 - 4
9AVICETEC1(config-if-range)#switchport mode trunk
9AVICETEC1(config-if-range)#switchport trunk native vlan 83
9AVICETEC1(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to down

```

Figura 3.113b: Modo Troncal y VLAN Nativa en la Capa de Acceso

```

9AVICETEC1(config)#interface FastEthernet 0/3
9AVICETEC1(config-if)#channel-group 1 mode on

%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to
up9AVICETEC1(config-if)#exit
9AVICETEC1(config)#interface FastEthernet 0/4
9AVICETEC1(config-if)#channel-group 1 mode on
9AVICETEC1(config-if)#exit

```

Figura 3.113c: Agrupación de Puertos en el Canal Lógico de la Capa de Acceso

Con el resultado del comando `show etherchannel summary` se constató que los puertos Fast Ethernet 0/3 y 0/4 estaban agrupados (Figura 3.114).

```

9AVICETEC1#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1              PAgP       Fa0/3(P) Fa0/4(P)

```

Figura 3.114: Estado de EtherChannel entre los Conmutadores de Acceso

3.2.5.3.4 Asignar Puertos de Acceso

Un par de interfaces se destinó para la comunicación entre los dispositivos de usuario final. La Figura 3.115 muestra cómo se especificó el modo de acceso y la asociación a la VLAN 20 (Presidencia/Secretaría).

```
10APRESEJEC(config)#interface range FastEthernet 0/23 - 24
10APRESEJEC(config-if-range)#switchport mode access
10APRESEJEC(config-if-range)#switchport access vlan 20
10APRESEJEC(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to down
```

Figura 3.115: Modo de Acceso y Asignación VLAN en Conmutador de Acceso

3.2.5.3.5 Configurar Direcciones de Capa 3

En la Figura 3.116 se observa la creación de la interfaz virtual y la asignación de la dirección IP.

```
10APRESEJEC(config)#interface vlan 83

%LINK-5-CHANGED: Interface Vlan83, changed state to up10APRESEJEC(config-if)#ip
address 172.17.83.201 255.255.255.0
```

Figura 3.116: Interfaz VLAN 83 del Conmutador 10APRESEJEC

3.2.5.3.6 Verificar Distribución de VLANs

Para comprobar que las redes virtuales creadas en los dispositivos de Core/Distribución fueron distribuidas a los conmutadores de Acceso se ejecutó el comando `show vlan brief`. El resultado indica que las 12 VLANs se transmitieron correctamente y que los puertos 23 y 24 pertenecen a la VLAN 20 (Figura 3.117). El incremento en los números de revisión de configuración y VLANs existentes se registra en la Figura 3.118.

```

10APRESEJEC#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Gig0/1, Gig0/2

10   Servidores             active
11   Medico/Auditoria       active
12   Telecomunicaciones/Juridica active
13   Mantenimiento/Adquisiciones active
14   Construccion/Seguros   active
15   Redes/Informatica      active
16   Financiero/Administracion active
17   Operacion/Disponibilidad active
18   Subestaciones/Lineas   active
19   Vicepresidencia/Investigacion active
20   Presidencia/Secretaria active    Fa0/23, Fa0/24
83   Administrativa         active
1002 fddi-default           active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active

```

Figura 3.117: Estado de VLANs en Conmutador de Acceso

```

10APRESEJEC#show vtp status
VTP Version                : 2
Configuration Revision     : 24
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 17
VTP Operating Mode        : Client
VTP Domain Name           : TRANSELECTRIC
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MDS digest                 : 0xC9 0xDA 0x1B 0x71 0xC8 0x89 0x69 0x20
Configuration last modified by 0.0.0.0 at 3-1-93 03:31:14

```

Figura 3.118. Estado de VTP en Conmutador de Acceso

3.2.5.3.7 Configuración STP (Spanning Tree Protocol)

La Figura 3.119a muestra que el Conmutador Raíz para la VLAN 10 (Servidores) era el dispositivo TELESRVA porque su dirección MAC formaba parte de las características “Root ID” y la interfaz Fast Ethernet 0/1 tenía el rol de Raíz. Los datos de la Figura 3.119b revelan que el Conmutador Raíz para la VLAN 83 era el equipo TELESRVB.

```

10APRESEJEC#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
            Address    0009.7C77.C389
            Cost      19
            Port      1(FastEthernet0/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
            Address    00E0.F989.6326
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Root FWD 19        128.1   P2p
Fa0/2              Altn BLK 19        128.2   P2p

```

Figura 3.119a: Estado de STP para la VLAN 10 en el Conmutador 10APRESEJEC

```

10APRESEJEC#show spanning-tree vlan 83
VLAN0083
  Spanning tree enabled protocol ieee
  Root ID    Priority    24659
            Address    0060.47E8.A95C
            Cost      19
            Port      2(FastEthernet0/2)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32851  (priority 32768 sys-id-ext 83)
            Address    00E0.F989.6326
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Altn BLK 19        128.1   P2p
Fa0/2              Root FWD 19        128.2   P2p

```

Figura 3.119b: Estado de STP para VLAN 83 en el Conmutador 10APRESEJEC

3.2.5.4 Verificar la conectividad

Para comprobar que los dispositivos de red fueron configurados adecuadamente se ejecutó el comando ping entre ambos equipos de Core/Distribución. Asimismo, se verificó la comunicación hacia los conmutadores de Acceso asegurando que no exista pérdida de paquetes. Por último, se comprobó que el intercambio de datos se producía entre los dispositivos de Capa 2.


```

TELESRVA#ping 172.17.83.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms

TELESRVA#ping 172.17.83.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.102, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 6/7/9 ms

```

Figura 3.120a: Envío y Recepción de Paquetes desde el Conmutador TELESRVA

```

TELESRVB#ping 172.17.83.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms

TELESRVB#ping 172.17.83.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/10 ms

```

Figura 3.120b: Envío y Recepción de Paquetes desde el Conmutador TELESRVB

```

TELESRVA#ping 172.17.83.192

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.192, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/4/6 ms

TELESRVA#ping 172.17.83.193

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.193, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/12/15 ms

```

Figura 3.120c: Intercambio de Paquetes entre las Capas de Core/Distribución y de Acceso

```

TELESRVB#ping 172.17.83.193

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.193, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/4/6 ms

TELESRVB#ping 172.17.83.192

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.192, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/3/5 ms

```

Figura 3.120d: Intercambio de Paquetes entre las Capas de Core/Distribución y de Acceso
(2 de 2)

```

9BINVEDESA#ping 172.17.83.193

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.193, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms

9BINVEDESA#ping 172.17.83.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.102, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms

9BINVEDESA#ping 172.17.83.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.101, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/12/15 ms

9BINVEDESA#ping 172.17.83.192

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.192, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 6/7/8 ms

```

Figura 3.120e: Comunicación entre los Conmutadores de Acceso

3.2.6 Simulación en Laboratorio

Dado que el programa de simulación de redes Packet Tracer versión 5.0 no admite ciertos comandos resulta imprescindible crear una topología equivalente en ambiente de laboratorio con equipos de características similares a los que se incluyen en la propuesta. Aprovechando las facilidades que presta la Academia Regional de Redes Cisco de la USFQ (Universidad San Francisco de Quito) para acceder a sus instalaciones y utilizar los recursos disponibles, se coordinó una serie de visitas a fin de configurar los dispositivos y realizar las pruebas del caso. El primer paso consistió en revisar el diagrama de red que se implementaría (Figura 3.121), verificar la disponibilidad de los equipos y confirmar que los comandos planteados sean correctos.

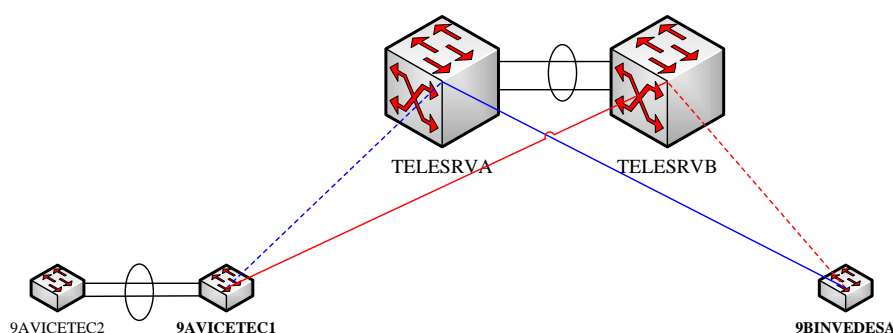


Figura 3.121: Topología de Red Equivalente

Una vez en el aula se confirmó la existencia de los conmutadores, estaciones de trabajo y cables de interconexión (de consola, directos y cruzados). Las Figuras 3.122a y 3.122b muestran que los equipos se organizaron según el diagrama para facilitar las conexiones. Los conmutadores que se utilizaron para Core/Distribución fueron 2 Cisco Catalyst 3550 SERIES, los cuales disponían de 24 puertos 10Base-T/100Base-TX y 2 ranuras para módulos GBIC (Gigabit Interface Converter). En el caso de los conmutadores de Acceso se emplearon dos Cisco Catalyst 3500 SERIES XL (48 puertos 10Base-T/100Base-TX y 2 ranuras de expansión para módulos GBIC) y un Cisco Catalyst 2950 SERIES (24 puertos 10Base-T/100Base-TX y 2 ranuras de expansión para módulos GBIC). En la Tabla 3.15 se detalla el nombre, modelo, número de serie y dirección MAC de dichos equipos.



Figura 3.122a: Conmutadores y Emuladores de Terminal (Vista Frontal)



Figura 3.122b: Conmutadores y Emuladores de Terminal (Vista Posterior)

Dispositivo	Modelo		Número de Serie	Dirección MAC
TELESRVA	Catalyst 3550 SERIES	WS-C3550-24-EMI	CAT0819R0MJ	00:11:20:A2:B2:80
TELESRVB	Catalyst 3550 SERIES	WS-C3550-24-EMI	CHK0631V10A	00:0A:8A:B3:0F:00
9AVICETEC2	Catalyst 3500 SERIES XL	WS-C3548-XL-EN	FAB0535M265	00:07:50:9A:7B:80
9AVICETEC1	Catalyst 3500 SERIES XL	WS-C3548-XL-EN	FAB0535M226	00:07:50:90:CD:40
9BINVEDESA	Catalyst 2950 SERIES	WS-C2950G-24-EI	FHK0620Z0MU	00:09:B7:4F:50:C0

Tabla 3.15: Características de los Conmutadores Utilizados en la Simulación

Para acceder a los equipos se estableció una conexión de consola y se abrió una ventana de HyperTerminal haciendo clic en el menú “Inicio” de la barra de tareas, seleccionando la opción “Accesorios” en la sección “Programas” y ejecutando “HyperTerminal” en “Comunicaciones” (Figura 3.123). El nombre de la conexión, puerto y parámetros asociados se muestran en la Figura 3.124.



Figura 3.123: HyperTerminal en Menú de Comunicaciones

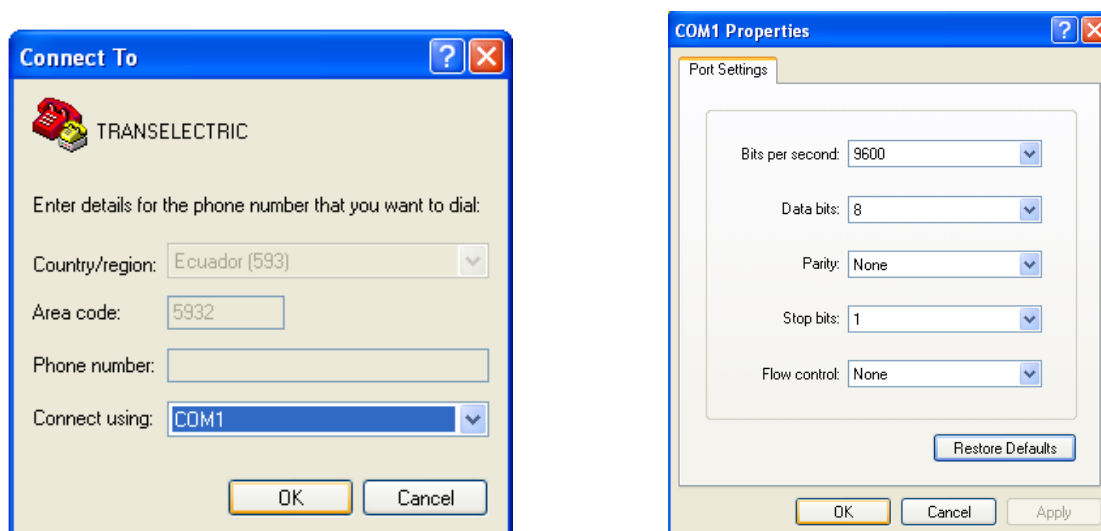


Figura 3.124: Propiedades de Conexión y Parámetros de Puerto

3.2.6.1 Configuración Básica

3.2.6.1.1 Borrar y Reiniciar

Antes de configurar los equipos se borró la configuración existente. En la Figura 3.125 se muestra dicho procedimiento. En la primera línea se ejecutó el comando `delete flash:vlan.dat` y se confirmó los mensajes de advertencia con la tecla “Enter”. Después se borró el archivo startup-config digitando el comando `erase startup-config` y

aceptando el mensaje que se desplegó. Para verificar que la información fue borrada se recurrió al comando `show vlan` como se observa en la Figura 3.126. El último paso consistió en reiniciar el software con el comando `reload` (Figura 3.127).

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
%Error deleting flash:vlan.dat (No such file or directory)
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
00:20:48: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram_
```

Figura 3.125: Borrado de Base de Datos VLAN y Configuración

```
Switch#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports

Switch#

Figura 3.126: VLANs por Defecto

```

Switch#reload
Proceed with reload? [confirm]

00:22:45: %SYS-5-RELOAD: Reload requestedBase ethernet MAC Address: 00:11:20:a2:
b2:80
Xmodem file system is available.
The password-recovery mechanism is enabled.
Initializing Flash...
flashfs[0]: 3 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 4088320
flashfs[0]: Bytes available: 11910656
flashfs[0]: flashfs fsck took 14 seconds.
..done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Loading "flash:/c3550-i5q3l2-mz.121-14.EA1.bin"...#####
#####
#####_

```

Figura 3.127: Inicialización de un Conmutador

3.2.6.1.2 Verificar la Configuración por Defecto

Los primeros conmutadores que se configuraron fueron los Cisco Catalyst 3550 SERIES que harían las veces de Core/Distribución. Las Figuras 3.128a, 3.128b y 3.128c muestran el resultado de ingresar el comando `show running-config`, el cual permitió verificar el tipo y cantidad de interfaces que tenían los dispositivos así como el rango de líneas virtuales.

```

Current configuration : 2006 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 switchport mode dynamic desirable
!
--More-- _

interface FastEthernet0/2
 switchport mode dynamic desirable
!
interface FastEthernet0/3
 switchport mode dynamic desirable
!
interface FastEthernet0/4
 switchport mode dynamic desirable
!
interface FastEthernet0/5
 switchport mode dynamic desirable
!
interface FastEthernet0/6
 switchport mode dynamic desirable
!
interface FastEthernet0/7
 switchport mode dynamic desirable
!
interface FastEthernet0/8
 switchport mode dynamic desirable
!
interface FastEthernet0/9
 switchport mode dynamic desirable
--More-- _

```

Figura 3.128a: Configuración Actual (1 de 3)

```

!
interface FastEthernet0/10
 switchport mode dynamic desirable
!
interface FastEthernet0/11
 switchport mode dynamic desirable
!
interface FastEthernet0/12
 switchport mode dynamic desirable
!
interface FastEthernet0/13
 switchport mode dynamic desirable
!
interface FastEthernet0/14
 switchport mode dynamic desirable
!
interface FastEthernet0/15
 switchport mode dynamic desirable
!
interface FastEthernet0/16
 switchport mode dynamic desirable
!
interface FastEthernet0/17
 --More--
!
 switchport mode dynamic desirable
!
interface FastEthernet0/18
 switchport mode dynamic desirable
!
interface FastEthernet0/19
 switchport mode dynamic desirable
!
interface FastEthernet0/20
 switchport mode dynamic desirable
!
interface FastEthernet0/21
 switchport mode dynamic desirable
!
interface FastEthernet0/22
 switchport mode dynamic desirable
!
interface FastEthernet0/23
 switchport mode dynamic desirable
!
interface FastEthernet0/24
 switchport mode dynamic desirable
!
 --More-- _

```

Figura 3.128b: Configuración Actual (2 de 3)

```

 switchport mode dynamic desirable
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface Vlan1
 no ip address
 shutdown
!
 ip classless
 ip http server
!
!
!
 line con 0
 speed 57600
 line vty 5 15
!
 end
Switch#_

```

Figura 3.128c: Configuración Actual (3 de 3)

Después se examinaron las características de la interfaz virtual VLAN 1 ejecutando el comando `show interface vlan1`. En la Figura 3.129 se observa que los conmutadores no

tenían asignada una dirección IP (Internet Protocol), tenían una dirección MAC (Media Access Control) y la interfaz estaba apagada.

```
Switch#show interface vlan1
Vlan1 is administratively down, line protocol is down
  Hardware is EtherSVI, address is 0011.20a2.b280 (bia 0011.20a2.b280)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
Switch#
```

Figura 3.129: Parámetros de la Interfaz VLAN 1

Para conocer la versión del Cisco IOS (Internetwork Operating System) que los conmutadores estaban corriendo, el nombre del archivo de la imagen del sistema y la dirección MAC se utilizó el comando `show version`, el mismo que desplegó la información de las Figuras 3.130a y 3.130b.

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(14)EA1, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 22-Jul-03 12:47 by antonino
Image text-base: 0x00003000, data-base: 0x007E6484

ROM: Bootstrap program is C3550 boot loader

Switch uptime is 7 minutes
System returned to ROM by power-on
System image file is "flash:/c3550-i5q3l2-mz.121-14.EA1.bin"

cisco WS-C3550-24 (PowerPC) processor (revision M0) with 65526K/8192K bytes of m
emory.
Processor board ID CAT0819R0MJ
Last reset from warm-reset
Bridging software.
Running Layer2/3 Switching Image

Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces
--More-- _
```

Figura 3.130a: Características de un Conmutador (1 de 2)

```

cisco WS-C3550-24 (PowerPC) processor (revision M0) with 65526K/8192K bytes of m
emory.
Processor board ID CAT0819R0MJ
Last reset from warm-reset
Bridging software.
Running Layer2/3 Switching Image

Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 3 has 1 Gigabit Ethernet/IEEE 802.3 interface
Ethernet-controller 4 has 1 Gigabit Ethernet/IEEE 802.3 interface

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is enabled.
384K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:11:20:A2:B2:80
Motherboard assembly number: 73-5700-11
Power supply part number: 34-0966-04
Motherboard serial number: CAT08190L0N
Power supply serial number: LIT080607XN
Model revision number: M0
Motherboard revision number: A0
Model number: WS-C3550-24-EMI
System serial number: CAT0819R0MJ
Configuration register is 0x10F

Switch#_

```

Figura 3.130b: Características de un Conmutador (2 de 2)

3.2.6.2 Capa de Core/Distribución

3.2.6.2.1 Asignar Nombres y Establecer Contraseñas

La configuración básica consistió en asignar un nombre a cada dispositivo y crear las contraseñas encriptadas para el puerto de consola y el acceso al modo de privilegio. La Figura 3.131 muestra cómo se asignaron los nombres a los conmutadores de Core/Distribución. El comando `service password-encryption` que se observa en la primera línea de la Figura 3.132 permite encriptar las contraseñas especificadas a continuación.

```

Switch(config)#hostname TELESRVA
TELESRVA(config)#exit
TELESRVA#
00:30:23: %SYS-5-CONFIG_I: Configured from console by console

Switch(config)#hostname TELESRVB
TELESRVB(config)#exit
TELESRVB#
00:20:27: %SYS-5-CONFIG_I: Configured from console by console_

```

Figura 3.131: Nombre de los Conmutadores de Core/Distribución

```

TELESRVA(config)#service password-encryption
TELESRVA(config)#line console 0
TELESRVA(config-line)#password trG5mn7N1
TELESRVA(config-line)#login
TELESRVA(config-line)#exit
TELESRVA(config)#enable secret c0m1A1n0d
TELESRVA(config)#exit
TELESRVA#
06:15:01: %SYS-5-CONFIG_I: Configured from console by console

```

Figura 3.132: Encipción de las Contraseñas de Consola y de Acceso al Modo de Privilegio

3.2.6.2.2 Apagar Puertos

Como medida de precaución se deshabilitaron todos los puertos de los conmutadores utilizando las secuencias de comandos descritas en las Figuras 3.133a y 3.133b.

```

TELESRVA(config-if-range)#interface range FastEthernet 0/1 - 24
TELESRVA(config-if-range)#shutdown
TELESRVA(config-if-range)#
00:33:37: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
00:33:37: %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
00:33:37: %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
00:33:37: %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
00:33:37: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
00:33:37: %LINK-5-CHANGED: Interface Fast

```

Figura 3.133a: Apagado de Puertos Fast Ethernet en Conmutador de Core/Distribución

```

TELESRVA(config)#interface range GigabitEthernet 0/1 - 2
TELESRVA(config-if-range)#shutdown
TELESRVA(config-if-range)#
00:35:04: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
00:35:04: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
00:35:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
00:35:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down_

```

Figura 3.133b: Apagado de Puertos Gigabit Ethernet en Conmutador de Core/Distribución

3.2.6.2.3 Configuración VTP (VLAN Trunking Protocol)

3.2.6.2.3.1 Establecer Modo de Operación, Nombre de Dominio y Contraseña

Cuando se ingresó el comando `show vtp status` fue posible comprobar que los conmutadores se encontraban en el modo VTP por defecto (servidor) como se observa en la Figura 3.134. Entre la información obtenida es importante identificar la versión VTP, el número de revisión de configuración, el número de VLANs (Virtual Local Area Networks) existentes, el modo de operación VTP y el nombre de dominio VTP (null). La Figura 3.135 muestra los comandos utilizados para configurar el modo de operación, dominio y contraseña VTP.

```
TELESRVA#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            :
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
TELESRVA#_
```

Figura 3.134: Estado de VTP por Defecto en Conmutador de Core/Distribución

```
TELESRVA(config)#vtp mode server
Device mode already VTP SERVER.
TELESRVA(config)#vtp domain TRANSELECTRIC
Changing VTP domain name from NULL to TRANSELECTRIC
TELESRVA(config)#vtp password DsnartMcirtceleN
Setting device VLAN database password to DsnartMcirtceleN
TELESRVA(config)#end
TELESRVA#
00:38:26: %SYS-5-CONFIG_I: Configured from console by console
```

Figura 3.135: Modo de Operación, Dominio y Contraseña en Servidor VTP

3.2.6.2.3.2 Crear y Nombrar VLANs

Las Figuras 3.136a y 3.136b muestran los comandos utilizados para crear las 12 VLANs con sus respectivos nombres. Ingresando el comando `show vlan brief` se confirmó que la configuración tuvo efecto (Figura 3.137). El incremento en el número de revisión de

configuración que resulta de la creación de las VLANs, el número de redes virtuales existentes, el modo de operación y el nuevo nombre de dominio VTP se observan en la Figura 3.138.

```

TELESRVA(config)#vlan 83
TELESRVA(config-vlan)#name Administrativa
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 10
TELESRVA(config-vlan)#name Servidores
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 11
TELESRVA(config-vlan)#name Medico/Auditoria
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 12
TELESRVA(config-vlan)#name Telecomunicaciones/Juridica
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 13
TELESRVA(config-vlan)#name Mantenimiento/Adquisiciones
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 14
TELESRVA(config-vlan)#name Construccion/Seguros
TELESRVA(config-vlan)#exit
TELESRVA(config)#_

```

Figura 3.136a: Nombres y Números de VLANs (1 de 2)

```

TELESRVA(config)#vlan 15
TELESRVA(config-vlan)#name Redes/Informatica
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 16
TELESRVA(config-vlan)#name Financiero/Administracion
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 17
TELESRVA(config-vlan)#name Operacion/Disponibilidad
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 18
TELESRVA(config-vlan)#name Subestaciones/Lineas
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 19
TELESRVA(config-vlan)#name Vicepresidencia/Investigacion
TELESRVA(config-vlan)#exit
TELESRVA(config)#vlan 20
TELESRVA(config-vlan)#name Presidencia/Secretaria
TELESRVA(config-vlan)#exit
TELESRVA(config)#

```

Figura 3.136b: Nombres y Números de VLANs (2 de 2)

```

TELESRVA#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gi0/1, Gi0/2
10   Servidores              active
11   Medico/Auditoria        active
12   Telecomunicaciones/Juridica active
13   Mantenimiento/Adquisiciones active
14   Construccion/Seguros    active
15   Redes/Informatica        active
16   Financiero/Administracion active
17   Operacion/Disponibilidad active
18   Subestaciones/Lineas    active
19   Vicepresidencia/Investigacion active
20   Presidencia/Secretaria  active
83   Administrativa          active
1002 fddi-default            act/unsup

VLAN Name                Status    Ports
-----
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
TELESRVA#_

```

Figura 3.137: Estado de VLANs en Conmutador de Core/Distribución

```

TELESRVA#show vtp status
VTP Version                : 2
Configuration Revision     : 12
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 17
VTP Operating Mode         : Server
VTP Domain Name            : TRANSELECTRIC
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x21 0x50 0x23 0xDB 0x82 0xF9 0xE5 0xAF
Configuration last modified by 0.0.0.0 at 3-1-93 00:45:47
Local updater ID is 0.0.0.0 (no valid interface found)
TELESRVA#_

```

Figura 3.138: Estado de VTP en Conmutador de Core/Distribución

3.2.6.2.3.3 Configurar Direcciones de Capa 3

Una vez creada la VLAN 83 (Administrativa) se establecieron las direcciones IP de los conmutadores en la interfaz virtual con los comandos de las Figuras 3.139a y 3.139b.

```
TELESRVA(config)#interface vlan 83
TELESRVA(config-if)#ip address 172.17.83.101 255.255.255.0
TELESRVA(config-if)#no shutdown
TELESRVA(config-if)#
```

Figura 3.139a: Dirección de Capa 3 en Conmutador TELESRVA

```
TELESRVB(config)#interface vlan 83
TELESRVB(config-if)#ip address 172.17.83.102 255.255.255.0
TELESRVB(config-if)#no shutdown
TELESRVB(config-if)#_
```

Figura 3.139b: Dirección de Capa 3 en Conmutador TELESRVB

3.2.6.2.3.4 Establecer Enlaces Troncales y VLAN Nativa

Como no se disponía de módulos GBIC se optó por configurar las interfaces Fast Ethernet 0/9 y 0/19 como enlaces troncales en ambos conmutadores. Mediante los comandos de la Figura 3.140 se accedió a este par de interfaces, estableció el modo troncal y especificó la VLAN nativa. Luego de ejecutar el comando `show interface trunk` se desplegó la información de la Figura 3.141 que permitió verificar la configuración.

```
TELESRVB(config)#interface FastEthernet 0/9
TELESRVB(config-if)#switchport trunk encapsulation dot1q
TELESRVB(config-if)#switchport mode trunk
TELESRVB(config-if)#switchport trunk native vlan 83
TELESRVB(config-if)#exit
TELESRVB(config)#interface FastEthernet 0/19
TELESRVB(config-if)#switchport trunk encapsulation dot1q
TELESRVB(config-if)#switchport mode trunk
TELESRVB(config-if)#switchport trunk native vlan 83
TELESRVB(config-if)#exit
```

Figura 3.140: Protocolo de Encapsulamiento, Modo Troncal y VLAN Nativa entre Capas de Core/Distribución y de Acceso

```

TELESRVB#show interface trunk

Port      Mode      Encapsulation  Status      Native vlan
Fa0/9     on        802.1q         trunking    83
Fa0/19    on        802.1q         trunking    83
Po1       on        802.1q         trunking    83

Port      Vlans allowed on trunk
Fa0/9     1-4094
Fa0/19    1-4094
Po1       1-4094

Port      Vlans allowed and active in management domain
Fa0/9     1,10-20,83
Fa0/19    1,10-20,83
Po1       1,10-20,83

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/9     1,10-20,83
Fa0/19    1,10-20,83
Po1       1,10-20,83

```

Figura 3.141: Estado de los Enlaces Troncales

3.2.6.2.4 Agrupar Puertos

El doble enlace entre los conmutadores de Core/Distribución implica que las interfaces Fast Ethernet 0/21 y 0/22 se configuren como troncales y sean agrupadas. La Figura 3.142a muestra los comandos necesarios para crear la interfaz lógica, establecer el modo troncal y asignar la VLAN nativa. Mediante el segundo comando de la Figura 3.142b se vincularon los puertos a la interfaz port-channel y aseguró que funcionen como EtherChannel.

```

TELESRVB(config)#interface port-channel 1
TELESRVB(config-if)#switchport trunk encapsulation dot1q
TELESRVB(config-if)#switchport mode trunk
TELESRVB(config-if)#switchport trunk native vlan 83

```

Figura 3.142a: Canal Lógico en la Capa de Core/Distribución

```

TELESRVB(config)#interface FastEthernet 0/21
TELESRVB(config-if)#channel-group 1 mode on
TELESRVB(config-if)#no shutdown
TELESRVB(config-if)#

TELESRVB(config)#interface FastEthernet 0/22
TELESRVB(config-if)#channel-group 1 mode on
TELESRVB(config-if)#no shutdown
TELESRVB(config-if)#_

```

Figura 3.142b: Agrupación de Puertos en la Capa de Core/Distribución

Luego de ejecutar el comando `show etherchannel summary` (Figura 3.143) se confirmó que el canal estaba operativo porque tenía las banderas S (Layer 2) y U (in use). Además, la bandera P (in port-channel) indica que los puertos agrupados estaban activos.

```
TELESRVB#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       u - unsuitable for bundling
       U - in use       f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        -           Fa0/21(P) Fa0/22(P)
```

Figura 3.143: Resumen de EtherChannel en la Capa de Core/Distribución

3.2.6.2.5 Proteger Puertos de Acceso

A fin de permitir la conexión de los servidores a los conmutadores de Core/Distribución se configuró la seguridad de puerto en las interfaces Fast Ethernet 0/23 y 0/24. Con el primer comando de la Figura 3.144 se ingresó a este par de interfaces. Las siguientes líneas permitieron definir el modo de acceso, asignar la VLAN correspondiente y restringir las conexiones a un solo equipo.

```
TELESRVA(config)#interface range FastEthernet 0/23 - 24
TELESRVA(config-if-range)#switchport mode access
TELESRVA(config-if-range)#switchport access vlan 10
TELESRVA(config-if-range)#switchport port-security maximum 1
TELESRVA(config-if-range)#switchport port-security mac-address sticky
```

Figura 3.144: Seguridad de Puerto en la VLAN 10

3.2.6.2.6 Configuración STP (Spanning Tree Protocol)

Los servidores VTP se configuraron de tal manera que uno de ellos sea el Conmutador Raíz para el rango de VLANs 10-15 y el otro para las VLANs 16-20 y 83 como se observa en las Figuras 3.145a y 3.145b.

```

TELESRVA(config)#spanning-tree vlan 10-15 root primary
TELESRVA(config)#spanning-tree vlan 16-20,83 root secondary
TELESRVA(config)#exit
TELESRVA#

```

Figura 3.145a: Control en la Elección del Conmutador Raíz para las VLANs 10-15

```

TELESRVB(config)#spanning-tree vlan 16-20,83 root primary
TELESRVB(config)#spanning-tree vlan 10-15 root secondary
TELESRVB(config)#exit
TELESRVB#
03:59:30: %SYS-5-CONFIG_I: Configured from console by console

```

Figura 3.145b: Control en la Elección del Conmutador Raíz para las VLANs 16-20 y 83

El comando `show spanning-tree` (Figura 3.146a) indicó que uno de los dispositivos de Core/Distribución (TELESRVA) era el Conmutador Raíz para la VLAN 10, ya que el valor de la prioridad era 24586, apareció el mensaje “This bridge is the root” y todos los puertos tenían el rol de Designados y estaban transmitiendo. Mientras que para la VLAN 83 este dispositivo no era el Conmutador Raíz, pues la prioridad era mayor (24659), dos puertos tenían el rol de Designados y el tercero era el Raíz (Figura 3.146b).

```

VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
           Address    0011.20a2.b280
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    24586 (priority 24576 sys-id-ext 10)
           Address    0011.20a2.b280
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/9	Desg	FWD	19	128.9	P2p
Fa0/19	Desg	FWD	19	128.19	P2p
Po1	Desg	FWD	12	128.65	P2p

Figura 3.146a: Datos de STP para la VLAN 10 en el Conmutador TELESRVA

```

VLAN0083
Spanning tree enabled protocol ieee
Root ID    Priority    24659
           Address    000a.8ab3.0f00
           Cost      12
           Port      65 (Port-channel1)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    28755 (priority 28672 sys-id-ext 83)
           Address    0011.20a2.b280
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/9          Desg FWD 19        128.9   P2p
Fa0/19         Desg FWD 19        128.19  P2p
Po1            Root FWD 12        128.65  P2p

```

Figura 3.146b: Datos de STP para la VLAN 83 en el Conmutador TELESRVA

La Figura 3.147a muestra que el otro equipo de Core/Distribución (TELESRVB) fue elegido como Conmutador Raíz para la VLAN 83, pues apareció el mensaje “This bridge is the root” y todos los puertos tenían el rol de Designados. En tanto que este equipo no era el Conmutador Raíz para la VLAN 10 porque existían dos puertos Designados y un Raíz (Figura 3.147b).

```

VLAN0083
Spanning tree enabled protocol ieee
Root ID    Priority    24659
           Address    000a.8ab3.0f00
           This bridge is the root
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    24659 (priority 24576 sys-id-ext 83)
           Address    000a.8ab3.0f00
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/9          Desg FWD 19        128.9   P2p
Fa0/19         Desg FWD 19        128.19  P2p
Po1            Desg FWD 12        128.65  P2p

```

Figura 3.147a: Datos de STP para la VLAN 83 en el Conmutador TELESRVB

```

VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
           Address    0011.20a2.b280
           Cost      12
           Port      65 (Port-channel1)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    28682 (priority 28672 sys-id-ext 10)
           Address    000a.8ab3.0f00
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/9          Desg FWD 19         128.9   P2p
Fa0/19        Desg FWD 19         128.19  P2p
Po1           Root FWD 12         128.65  P2p

```

Figura 3.147b: Datos de STP para la VLAN 10 en el Conmutador TELESRVB

3.2.6.2.7 Configuración HSRP (Hot Standby Router Protocol)

El dispositivo TELESRVA será el conmutador primario para las VLANs impares (11, 13, 15, 17, 19 y 83) y suplirá la ausencia del otro equipo en caso de presentarse una interrupción en el servicio. Mientras que el otro dispositivo de Core/Distribución (TELESRVB) estará activo para las redes virtuales pares (10, 12, 14, 16, 18 y 20) y controlará las demás VLANs si ocurriese alguna clase de inconveniente. Las Figuras 3.148a y 3.148b muestran que el primer equipo estaba activo en la VLAN 10 porque tenía una prioridad alta (200) y existía una dirección IP en espera. Por otro lado, este conmutador asumirá las funciones de su similar para la VLAN 83 al originarse una falla.

```

TELESRVA#show standby vlan 10 brief
                P indicates configured to preempt.
                |
Interface  Grp Prio P State   Active addr   Standby addr   Group addr
Vl10      1   200 P Active local        172.17.10.3    172.17.10.1

```

Figura 3.148a: Conmutador HSRP Activo para VLAN 10

```

TELESRVA#show standby vlan 83 brief
                P indicates configured to preempt.
                |
Interface  Grp Prio P State   Active addr   Standby addr   Group addr
Vl83      1   100  Standby 172.17.83.3   local          172.17.83.1

```

Figura 3.148b: Conmutador HSRP Standby para VLAN 83

3.2.6.2.8 Configuración SNMP (Simple Network Management Protocol)

En la primera línea de las Figuras 3.149a y 3.149b se define la comunidad de lectura-escritura como transelectric. Luego se habilitan todas las notificaciones, especifica las direcciones IP de los conmutadores a los cuales se reportará cualquier evento y establece la versión de SNMP.

```
TELESRVA(config)#snmp-server community transelectric rw
TELESRVA(config)#snmp-server enable traps
TELESRVA(config)#snmp-server host 172.17.83.101 version 2c transelectric
TELESRVA(config)#snmp-server host 172.17.83.102 version 2c transelectric
```

Figura 3.149a: Comunidad, Notificaciones y Versión SNMP en Conmutador TELESRVA

```
TELESRVB(config)#snmp-server community transelectric rw
TELESRVB(config)#snmp-server enable traps
TELESRVB(config)#snmp-server host 172.17.83.101 version 2c transelectric
TELESRVB(config)#snmp-server host 172.17.83.102 version 2c transelectric
```

Figura 3.149b: Comunidad, Notificaciones y Versión SNMP en Conmutador TELESRVB

3.2.6.2.9 Grabar Configuración

La Figura 3.150 muestra el comando utilizado para grabar los cambios en la NVRAM (Non-Volatile Random Access Memory).

```
TELESRVA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TELESRVA#
```

Figura 3.150. Copiado de Archivos de Configuración

3.2.6.3 Capa de Acceso

3.2.6.3.1 Configuración Básica

3.2.6.3.1.1 Borrar y Verificar VLANs por Defecto

Después de borrar el archivo que contiene la base de datos VLAN y la configuración de inicio de la NVRAM se comprobó la existencia de las VLANs por defecto en los tres conmutadores utilizando el comando `show vlan brief` (Figura 3.151).

```

9BINVEDESA#show vlan brief
-----
VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                Gi0/1, Gi0/2
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
9BINVEDESA#

```

Figura 3.151: VLANs Existentes en Conmutador de Acceso

3.2.6.3.1.2 Asignar Nombres y Establecer Contraseñas

Los conmutadores de Acceso fueron configurados con los nombres que se indican en las Figuras 3.152a y 3.152b. Además se conservaron las mismas contraseñas de consola y de acceso al modo de privilegio que se especificaron en los conmutadores de Core/Distribución.

```

Switch(config)#hostname 9AVICETEC1
9AVICETEC1(config)#exit
9AVICETEC1#
00:01:59: %SYS-5-CONFIG_I: Configured from console by console

```

Figura 3.152a: Nombre de Conmutador en Ala A del Noveno Piso

```

Switch(config)#hostname 9BINVEDESA
9BINVEDESA(config)#exit
9BINVEDESA#
00:03:45: %SYS-5-CONFIG_I: Configured from console by console

```

Figura 3.152b: Nombre de Conmutador en Ala B del Noveno Piso

3.2.6.3.1.3 Apagar Puertos

A fin de prevenir conexiones no autorizadas se deshabilitaron todos los puertos con el comando `shutdown` que se muestra en las Figuras 3.153a y 3.153b.

```
9BINVEDESA(config)#interface range FastEthernet 0/1 - 24
9BINVEDESA(config-if-range)#shutdown
9BINVEDESA(config-if-range)#_
```

Figura 3.153a: Apagado de Puertos Fast Ethernet en el Conmutador 9BINVEDESA

```
9BINVEDESA(config)#interface range GigabitEthernet 0/1 - 2
9BINVEDESA(config-if-range)#shutdown
9BINVEDESA(config-if-range)#
00:07:33: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to admini
stratively down
00:07:33: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to admini
stratively down
```

Figura 3.153b: Apagado de Puertos Gigabit Ethernet en el Conmutador 9BINVEDESA

3.2.6.3.2 Configuración VTP (VLAN Trunking Protocol)

3.2.6.3.2.1 Establecer Modo de Operación, Nombre de Dominio y Contraseña

Los parámetros VTP por defecto fueron revisados con el comando `show vtp status`. En la Figura 3.154 se observa que la versión VTP era la 2, el número de revisión de configuración estaba en 0, existían solamente las VLANs por defecto, el modo de operación era servidor, no existía dominio VTP y las demás características estaban deshabilitadas. Para lograr que las VLANs creadas en los conmutadores de Core/Distribución se distribuyan se configuró el mismo dominio y contraseña VTP, pero se cambió el modo de operación a cliente con el grupo de comandos presentados en la Figura 3.155. Al ejecutar por segunda vez el comando `show vtp status` (Figura 3.156) se pudieron observar los cambios realizados.

```

9BINVEDESA#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 250
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            :
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
9BINVEDESA#

```

Figura 3.154: Estado VTP por Defecto en el Conmutador 9BINVEDESA

```

9BINVEDESA(config)#vtp mode client
Setting device to VTP CLIENT mode.
9BINVEDESA(config)#vtp domain TRANSELECTRIC
Changing VTP domain name from NULL to TRANSELECTRIC
9BINVEDESA(config)#vtp password DsnartMcirtceleN
Setting device VLAN database password to DsnartMcirtceleN
9BINVEDESA(config)#

```

Figura 3.155: Modo de Operación, Dominio y Contraseña en Cliente VTP

```

9BINVEDESA#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 250
Number of existing VLANs   : 5
VTP Operating Mode         : Client
VTP Domain Name            : TRANSELECTRIC
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x34 0x2F 0x2F 0x1D 0xB1 0xFF 0x93 0x82
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
9BINVEDESA#

```

Figura 3.156: Estado de VTP en el Conmutador 9BINVEDESA

3.2.6.3.2.2 Establecer Enlaces Troncales y VLAN Nativa

Para que los conmutadores intercambien la información de todas las VLANs se definieron a las interfaces Fast Ethernet 0/1 y 0/2 como enlaces troncales. Los comandos de las Figuras 3.157 especifican el modo troncal, la VLAN nativa y habilitan el puerto respectivo. El resultado de ingresar el comando `show interface trunk` (Figura 3.158) permitió confirmar que ambos puertos estaban encendidos y troncalizando.


```

9BINVEDESA(config)#interface range FastEthernet 0/1 - 2
9BINVEDESA(config-if-range)#switchport mode trunk
9BINVEDESA(config-if-range)#switchport trunk native vlan 83
9BINVEDESA(config-if-range)#no shutdown
9BINVEDESA(config-if-range)#
01:58:45: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
01:58:45: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down_

```

Figura 3.157: Modo Troncal y VLAN Nativa en el Conmutador 9BINVEDESA

```

9BINVEDESA#show interface trunk

Port          Mode          Encapsulation  Status        Native vlan
Fa0/1         on            802.1q         trunking      83
Fa0/2         on            802.1q         trunking      83

Port          Vlans allowed on trunk
Fa0/1         1-4094
Fa0/2         1-4094

Port          Vlans allowed and active in management domain
Fa0/1         1,10-20,83
Fa0/2         1,10-20,83

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,16-20,83
Fa0/2         10-15

```

Figura 3.158: Estado de Enlaces Troncales en el Conmutador 9BINVEDESA

3.2.6.3.2.3 Proteger Puertos de Acceso

La interfaz Fast Ethernet 0/16 fue configurada en modo de acceso, permitiendo 3 dispositivos de usuario final como máximo y haciendo que el puerto se apague en caso de comprometer la seguridad (Figura 3.159).

```

9BINVEDESA(config)#interface FastEthernet 0/16
9BINVEDESA(config-if)#switchport mode access
9BINVEDESA(config-if)#switchport access vlan 19
9BINVEDESA(config-if)#switchport port-security
9BINVEDESA(config-if)#switchport port-security maximum 3
9BINVEDESA(config-if)#switchport port-security mac-address sticky

```

Figura 3.159: Seguridad de Puerto en la VLAN 19

3.2.6.3.2.4 Configurar Direcciones de Capa 3

En las Figuras 3.160a, 3.160b y 3.160c se asignan las direcciones IP a los conmutadores de Acceso.

```

9AVICETEC1(config)#interface vlan 83
9AVICETEC1(config-subif)#ip address 172.17.83.192 255.255.255.0
9AVICETEC1(config-subif)#no shutdown
9AVICETEC1(config-subif)#_

```

Figura 3.160a: Dirección Administrativa del Conmutador 9AVICETEC1

```

9AVICETEC2(config)#interface vlan 83
9AVICETEC2(config-subif)#ip address 172.17.83.191 255.255.255.0
9AVICETEC2(config-subif)#no shutdown
9AVICETEC2(config-subif)#

```

Figura 3.160b: Dirección Administrativa del Conmutador 9AVICETEC2

```

9BINVEDESA(config)#interface vlan 83
9BINVEDESA(config-if)#ip address 172.17.83.193 255.255.255.0
9BINVEDESA(config-if)#no shu
02:26:16: %LINK-3-UPDOWN: Interface Vlan83, changed state to up
02:26:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan83, changed state
tdown

```

Figura 3.160c: Dirección Administrativa del Conmutador 9BINVEDESA

3.2.6.3.2.5 Verificar Distribución de VLANs

Al ejecutar el comando `show vlan brief` en cada uno de los conmutadores de Acceso se verificó que las VLANs creadas en la Capa de Core/Distribución fueron distribuidas como muestra la Figura 3.161.

```

9BINVEDESA#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22
10	Servidores	active	
11	Medico/Auditoria	active	
12	Telecomunicaciones/Juridica	active	
13	Mantenimiento/Adquisiciones	active	
14	Construccion/Seguros	active	
15	Redes/Informatica	active	
16	Financiero/Administracion	active	
17	Operacion/Disponibilidad	active	
18	Subestaciones/Lineas	active	
19	Vicepresidencia/Investigacion	active	Fa0/16, Fa0/23, Fa0/24
20	Presidencia/Secretaria	active	
83	Administrativa	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```

9BINVEDESA#

```

Figura 3.161: Estado de VLANs en Conmutador de Acceso

3.2.6.3.3 Configuración STP (Spanning Tree Protocol)

La información de la Figura 3.162a se obtuvo al ejecutar el comando `show spanning-tree` en uno de los equipos de Acceso (9BINVEDESA) y permitió verificar que el dispositivo TELESRVA era el Conmutador Raíz para la VLAN 10, ya que la dirección MAC era 0011.20a2.b280. De manera análoga, el Conmutador Raíz para la VLAN 83 era el dispositivo TELESRVB porque la dirección MAC era 000a.8ab3.0f00 (Figura 3.162b).

```
VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
           Address    0011.20a2.b280
           Cost      19
           Port      2 (FastEthernet0/2)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
           Address    000f.8f8d.b300
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Altn BLK 19        128.1   P2p
Fa0/2          Root FWD 19        128.2   P2p
```

Figura 3.162a: Información de STP para la VLAN 10 en el Conmutador 9BINVEDESA

```
VLAN0083
Spanning tree enabled protocol ieee
Root ID    Priority    24659
           Address    000a.8ab3.0f00
           Cost      19
           Port      1 (FastEthernet0/1)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32851 (priority 32768 sys-id-ext 83)
           Address    000f.8f8d.b300
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Root FWD 19        128.1   P2p
Fa0/2          Altn BLK 19        128.2   P2p
```

Figura 3.162b: Información de STP para la VLAN 83 en el Conmutador 9BINVEDESA

3.2.6.3.4 Configuración SNMP (Simple Network Management Protocol)

Los parámetros definidos en la Capa de Core/Distribución se mantuvieron en los conmutadores de Acceso. Es así que se configuró el mismo nombre de comunidad, las direcciones IP de los equipos principales y la versión de SNMP (Figuras 3.163a, 3.163b y 3.163c).

```
9AVICETEC1(config)#snmp-server community transelectric rw
9AVICETEC1(config)#snmp-server enable traps
9AVICETEC1(config)#snmp-server host 172.17.83.101 version 2c transelectric
9AVICETEC1(config)#snmp-server host 172.17.83.102 version 2c transelectric
```

Figura 3.163a: Parámetros SNMP en Conmutador 9AVICETEC1

```
9AVICETEC2(config)#snmp-server community transelectric rw
9AVICETEC2(config)#snmp-server enable traps
9AVICETEC2(config)#snmp-server host 172.17.83.101 version 2c transelectric
9AVICETEC2(config)#snmp-server host 172.17.83.102 version 2c transelectric
```

Figura 3.163b: Parámetros SNMP en Conmutador 9AVICETEC2

```
9BINVEDESA(config)#snmp-server community transelectric rw
9BINVEDESA(config)#snmp-server enable traps
9BINVEDESA(config)#snmp-server host 172.17.83.101 version 2c transelectric
9BINVEDESA(config)#snmp-server host 172.17.83.102 version 2c transelectric
```

Figura 3.163c: Parámetros SNMP en Conmutador 9BINVEDESA

3.2.6.4 Verificar la Conectividad

Para verificar la comunicación entre los conmutadores se utilizó el comando ping. Las Figuras 3.164a y 3.164b muestran las pruebas realizadas entre los conmutadores de Core/Distribución. Después se comprobó que no exista pérdida de paquetes entre las Capas de Core/Distribución y de Acceso (Figuras 3.164c y 3.164d). Finalmente se probó la comunicación entre los conmutadores de Acceso mediante los comandos de la Figura 3.164e.

```

TELESRVA#ping 172.17.83.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.101, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
TELESRVA#ping 172.17.83.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.102, timeout is 2 seconds:
!!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

```

Figura 3.164a: Comunicación en la Capa de Core/Distribución desde el TELESRVA

```

TELESRVB#ping 172.17.83.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.102, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
TELESRVB#ping 172.17.83.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.101, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

```

Figura 3.164b: Comunicación en la Capa de Core/Distribución desde el TELESRVB

```

TELESRVA#ping 172.17.83.192

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.192, timeout is 2 seconds:
!!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
TELESRVA#ping 172.17.83.193

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.193, timeout is 2 seconds:
!!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

```

Figura 3.164c: Intercambio de Paquetes entre las Capa de Core/Distribución y de Acceso

```

TELESRVB#ping 172.17.83.193

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.193, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
TELESRVB#ping 172.17.83.192

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.192, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

```

Figura 3.164d: Intercambio de Paquetes entre las Capas de Core/Distribución y de Acceso
(2 de 2)

```

9BINVEDESA#ping 172.17.83.193

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.193, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
9BINVEDESA#ping 172.17.83.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.102, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
9BINVEDESA#ping 172.17.83.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.101, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
9BINVEDESA#ping 172.17.83.192

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.83.192, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/15/56 ms

```

Figura 3.164e: Interacción de los Conmutadores de Acceso

3.2.7 Gestión de la Red

3.2.7.1 Creación de Mapas

El programa de administración de redes WhatsUp Gold ofrece la posibilidad de crear un mapa que incluye los elementos administrados y sus interconexiones. Al ejecutar “New Map Wizard” del menú “File” se despliega una ventana con dos opciones. La primera descubre los dispositivos de red a través de la información del computador principal o de la implementación existente. Mientras que la segunda presenta un espacio en blanco para distribuir los equipos con la ayuda de las herramientas disponibles (Figuras 3.165a y 3.165b).

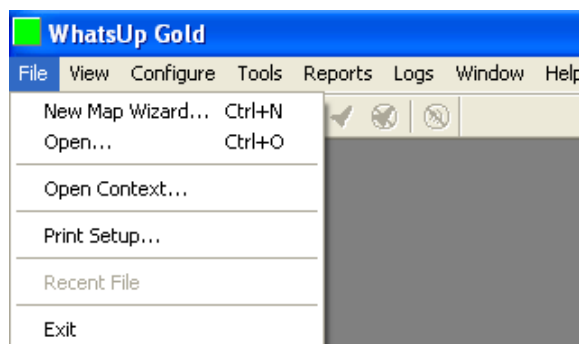


Figura 3.165a: Asistente de Nuevo Mapa del Menú Archivo

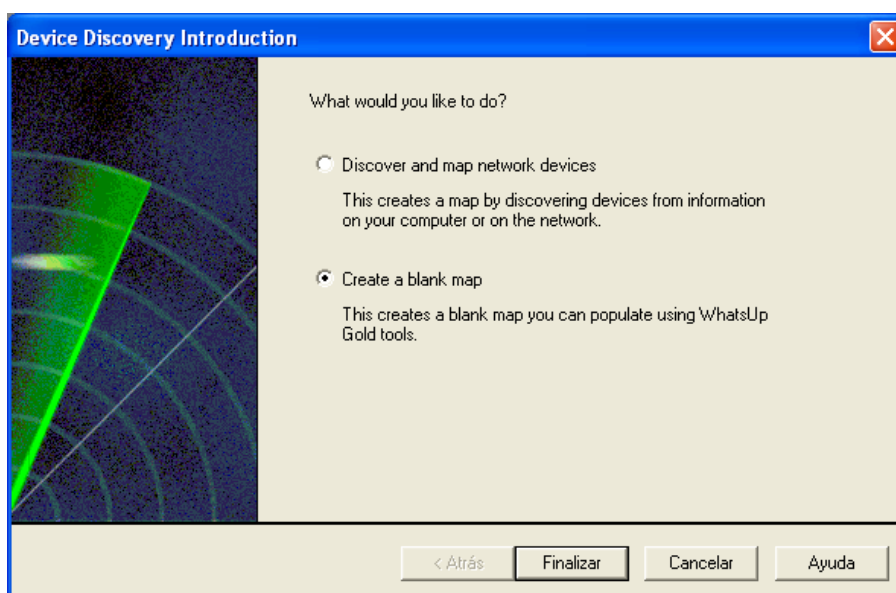


Figura 3.165b: Descubrimiento de Dispositivos

En el extremo izquierdo de la pestaña “Edit” que se observa en la Figura 3.166 existe una gama de dispositivos, objetos y formas que pueden ser utilizados para obtener una representación más cercana a la realidad. Para colocar los elementos simplemente se debe arrastrarlos hacia el área provista para el dibujo. Luego de hacer clic derecho sobre el dispositivo y escoger “Properties” se presenta la ventana de la Figura 3.167. En la categoría “General” se especifica el nombre que aparecerá en el diagrama, el tipo de equipo, el método de reconocimiento, el nombre del elemento de red y la dirección IP.

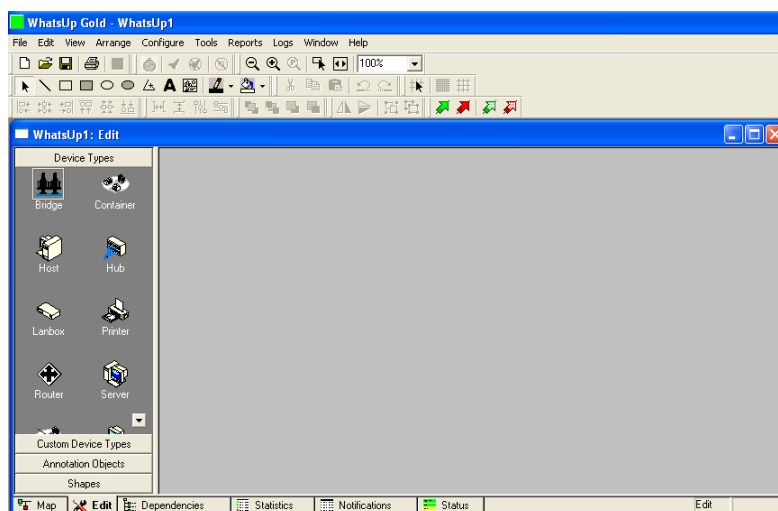


Figura 3.166: Espacio para la Edición de Mapas

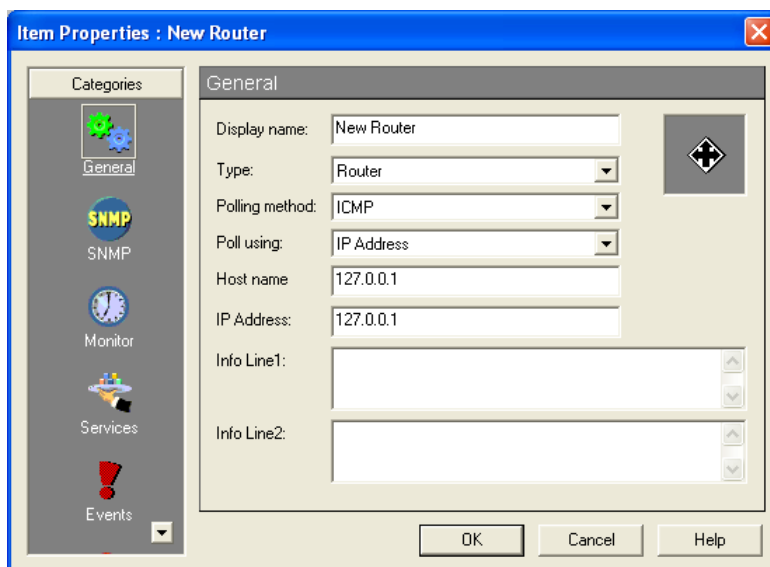


Figura 3.167: Categoría General de Propiedades de Dispositivos

La segunda categoría permite administrar el dispositivo a través de SNMP, ya que contiene los campos para definir los nombres de las comunidades de lectura y escritura (Figura 3.168). La frecuencia y vencimiento de los reconocimientos así como el periodo de monitoreo se establecen en la categoría “Monitor”. Todos los servicios que necesiten ser supervisados se añaden en “Services”. En la Figura 3.169 se muestra la categoría “Menu” donde se visualizan las herramientas “Connect”, “Ping”, “Traceroute” y “Browse”, las mismas que pueden ser editadas, borradas y reorganizadas según convenga.

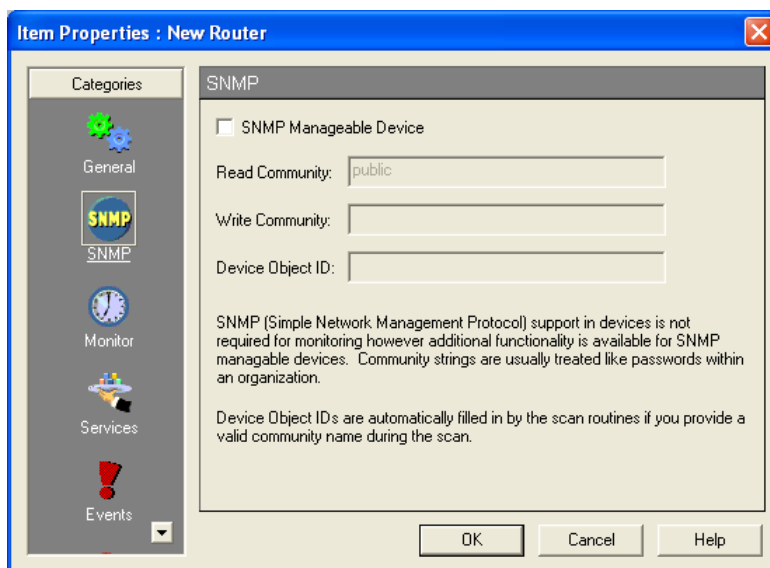


Figura 3.168: Categoría SNMP de Propiedades de Dispositivos

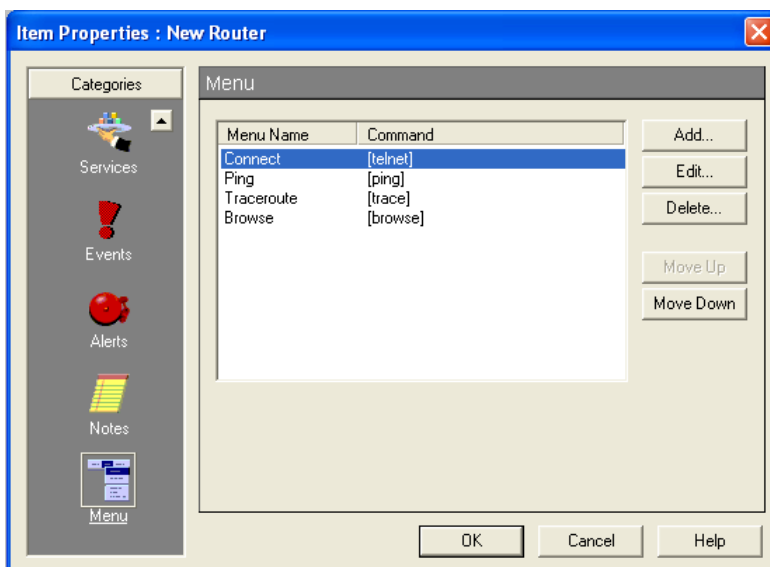


Figura 3.169: Categoría Menú de Propiedades de Dispositivos

3.2.7.2 Estado de los Dispositivos

Cuando se elige la opción “Program Options” del menú “Configure” se puede apreciar la simbología empleada para identificar el estado de cada dispositivo. Un cuadrado de color verde confirma que existe respuesta, pero si se pierde un paquete la figura se convierte en un rombo. En caso de perder otro paquete, el objeto se torna amarillo. Si este comportamiento persiste (tercer paquete perdido), aparece una especie de estrella (Figura 3.170a). Cuando se han perdido entre 4 y 7 paquetes consecutivos, la estrella se torna roja. Ante la ausencia de respuesta por más de 8 ocasiones, el objeto se convierte en una estrella de varias puntas. Si alguno de los servicios que presta un equipo falla, se visualiza un octágono rosa (Figura 3.170b).

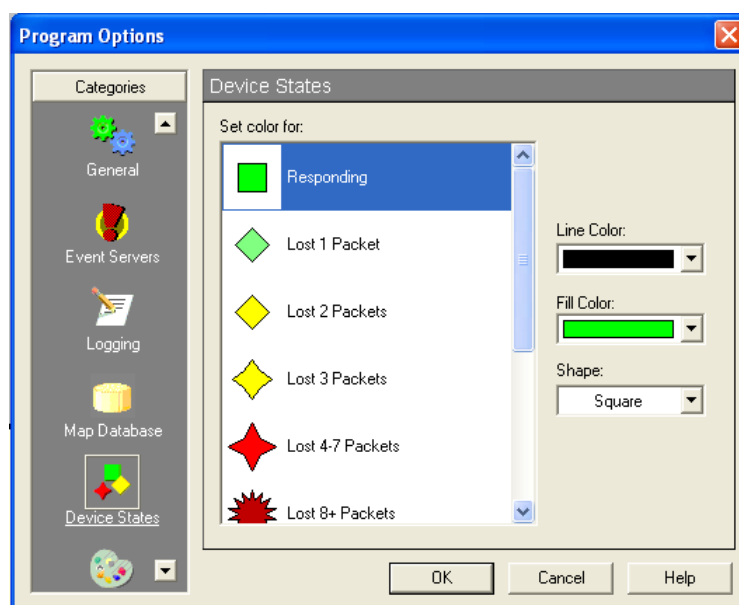


Figura 3.170a: Simbología para Estado de Dispositivos (1 de 2)

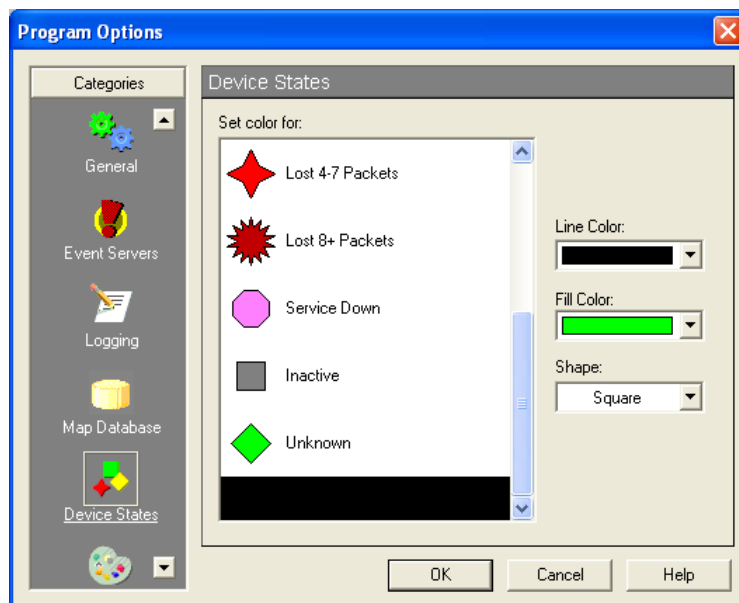


Figura 3.170b: Simbología para Estado de Dispositivos (2 de 2)

3.2.7.3 Servidor Web

La Figura 3.171 muestra la categoría “General” de la sección “Web Server” que contiene casillas para habilitar el servidor y la configuración Web, los gráficos y los sonidos. También se dispone de campos para escribir el título principal, determinar la frecuencia de actualización, establecer el puerto de comunicación e indicar la ubicación de los archivos. Para controlar el acceso a la interfaz Web se elige la categoría “Users”, habilita la seguridad y especifica los parámetros de cada usuario (Figura 3.172).

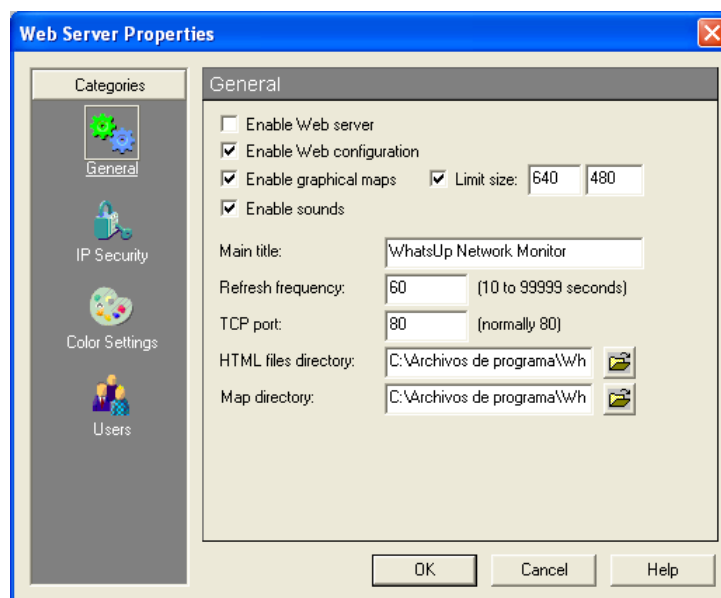


Figura 3.171: Categoría General de Propiedades del Servidor Web

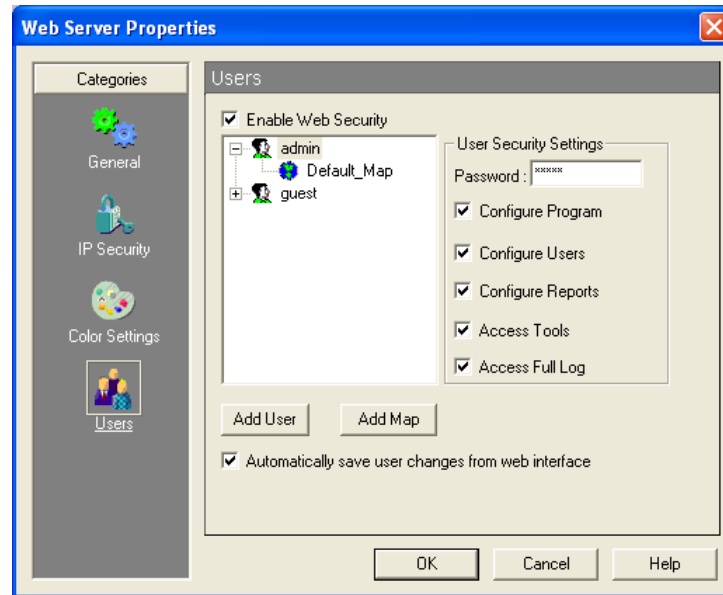


Figura 3.172: Categoría Usuarios de Propiedades del Servidor Web

3.2.7.4 Opciones de Notificaciones

Un grupo de notificaciones se presenta al seleccionar “Notifications Library” (Figura 3.173). Los campos que se deben llenar en un mensaje para radiolocalizador como el de la Figura 3.174a son: nombre de presentación, número del equipo, secuencia de marcado y los códigos para los estados activo, falla y evento. El envío de un SMS (Short Messaging Service) requiere escoger el país, proveedor de servicio, modo de conexión y número telefónico (Figura 3.174b). Los mensajes de correo electrónico necesitan la dirección del destinatario, un título y los caracteres del contenido que se observan en la Figura 3.174c.

Existen alarmas configuradas por defecto para anunciar la falla o restablecimiento de un elemento, un servicio defectuoso o su restitución y cualquier evento que ocurra. Los íconos ubicados junto a cada campo ayudan a personalizar la configuración y escuchar el sonido elegido antes de guardar los cambios (Figura 3.174d). Al hacer clic en la opción “Reports” es posible crear gráficos de rendimiento, informes de fallas y reportes estadísticos. Los parámetros a configurarse son: descripción, nombres del trabajo y mapa, tipo de reporte y fechas de inicio y fin.

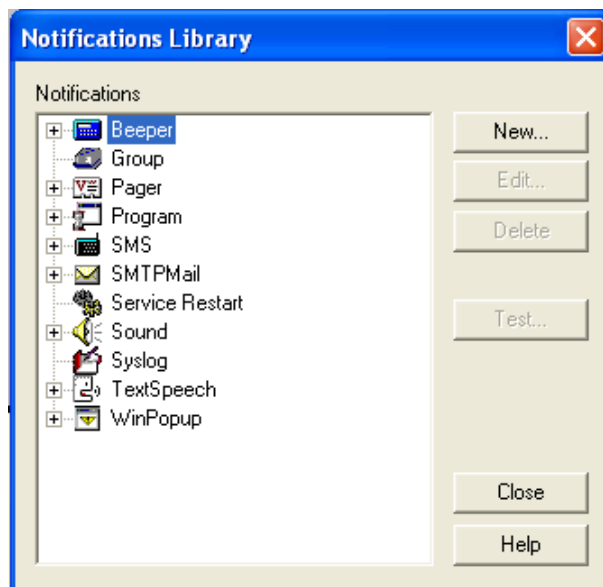


Figura 3.173: Conjunto de Notificaciones Disponibles

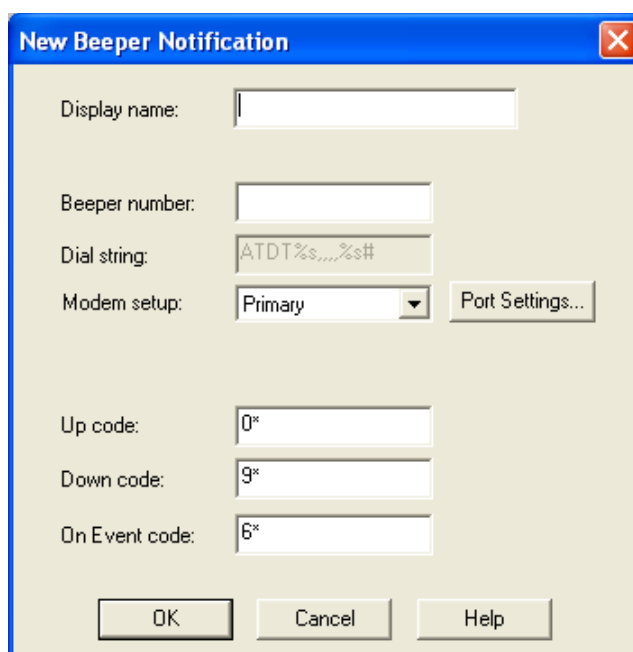


Figura 3.174a: Notificación de Radiolocalizador

New SMS Notification

Display name:

Country:

Provider: ...

—Connection Settings—

Mode: Email Dialup

Phone Number:

—Message—

Characters Remaining:

OK Cancel Help

Figura 3.174b: Notificación de SMS

New SMTP Notification

Display name:

Mail server:

To:

From:

Subject:

Address: %a
 Info 1: %1
 Info 2: %2
 Date: %d
 Status: %S (%s)
 Svcs: %v
 Notes: %N

OK Cancel Help

Figura 3.174c: Notificación de Correo Electrónico

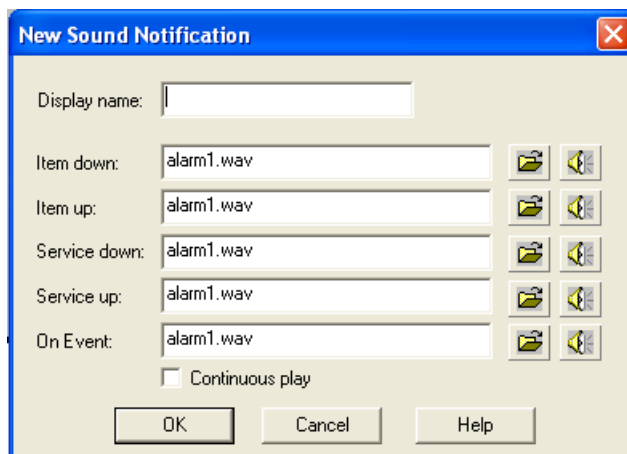


Figura 3.174d: Notificación de Sonido

3.2.7.5 Simulación de la Topología Completa

3.2.7.5.1 Creación del Mapa

Dado que el proyecto se encuentra en la etapa de diseño y aun no se dispone de los equipos, se creó un mapa en blanco. Ambos dispositivos de Core/Distribución fueron colocados en la parte superior de manera que el modelo jerárquico se reconozca fácilmente. Los conmutadores de Acceso se distribuyeron en orden descendente para reflejar su ubicación en el edificio. La Figura 3.175 muestra el diagrama completo en la pestaña “Map”. Tanto en el extremo izquierdo (Ala Oriental) como en el derecho (Ala Occidental) se utilizaron elipsoides rellenos como límite de cada VLAN. Con un par de cajas de texto se asignó el número y dirección de cada subred lógica. El último octeto perteneciente a la dirección administrativa se añadió en la parte inferior de los conmutadores de Acceso. Con un acercamiento se pudo observar los elementos administrables y las etiquetas que los identifican (Figuras 3.176a y 3.176b).

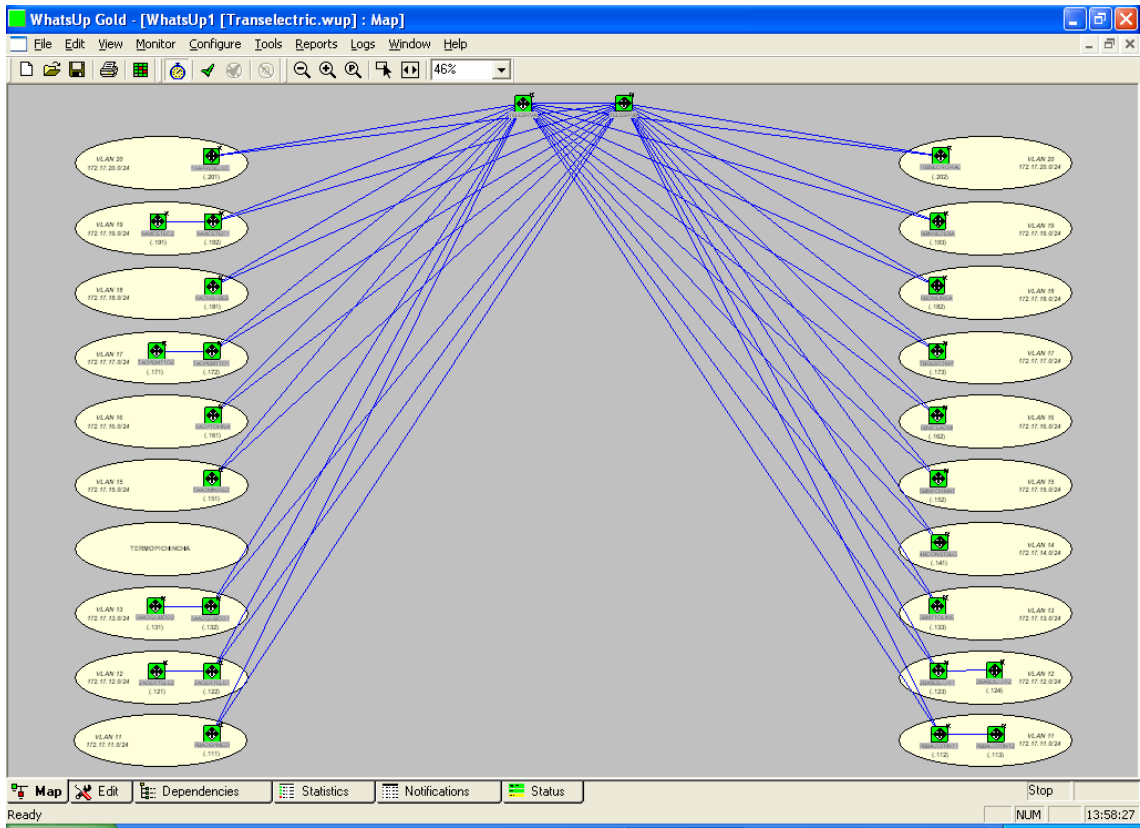


Figura 3.175: Diagrama para Monitoreo de Red

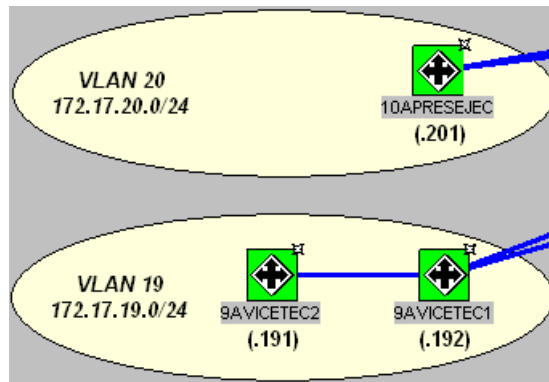


Figura 3.176a: Esquema de los Conmutadores de Acceso en el Ala Oriental

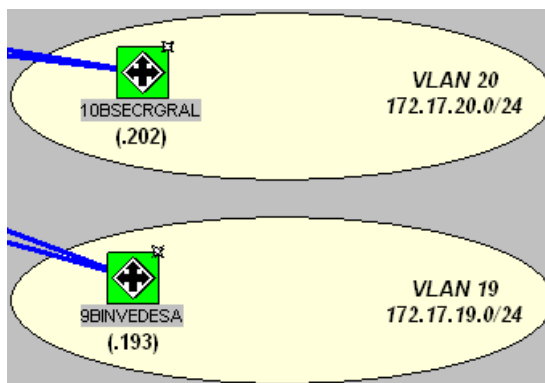


Figura 3.176b: Esquema de los Conmutadores de Acceso en el Ala Occidental

Haciendo clic sobre cada dispositivo y seleccionando la opción “Properties” se especificó el nombre y la dirección IP como se aprecia en la Figura 3.177a. El método de reconocimiento fue ICMP (Internet Control Message Protocol) y utilizando como referencia la dirección de Capa 3. Luego de marcar la casilla “SNMP Manageable Device” se digitaron los nombres de las comunidades de lectura y escritura (Figura 3.177b). Al hacer clic sobre un equipo se desplegó el menú que permite establecer una conexión remota, ejecutar los comandos ping y traceroute, crear los gráficos de rendimiento y revisar el estado del dispositivo.

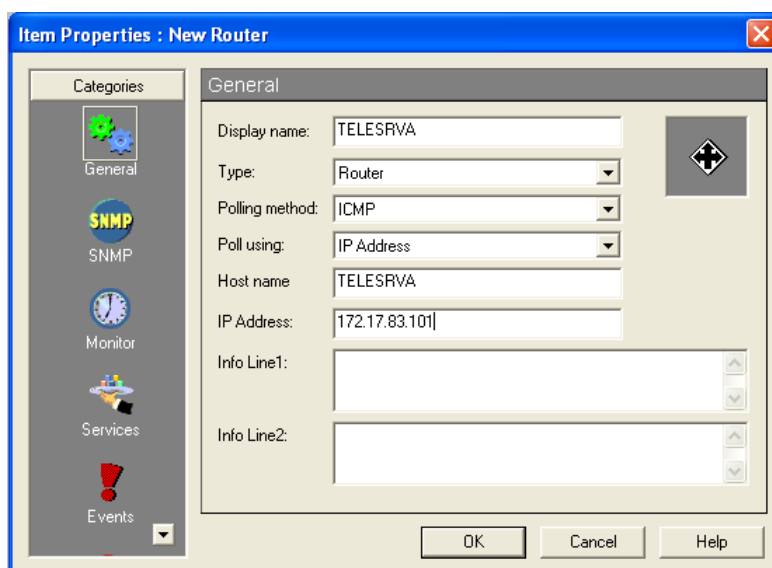


Figura 3.177a: Nombre y Dirección IP en la Categoría General

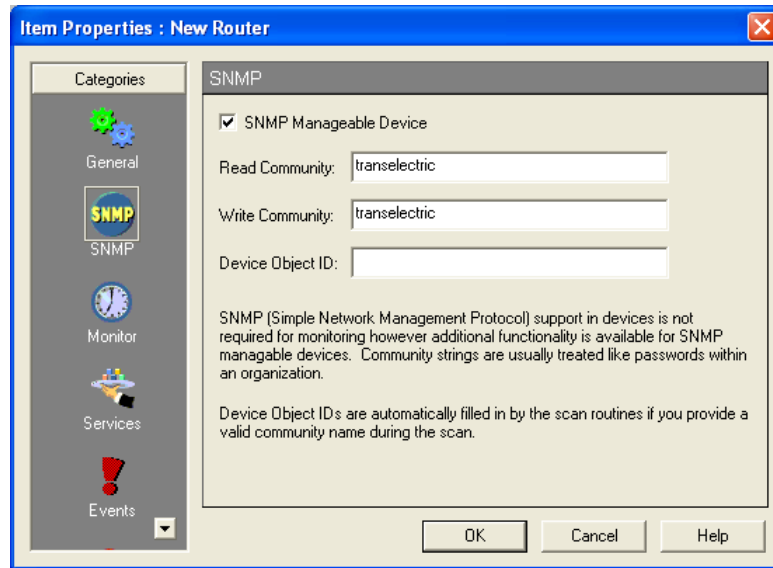


Figura 3.177b: Comunidades SNMP de Lectura y Escritura

3.2.7.5.2 Servidor Web

En las propiedades del servidor Web se cambió el número del puerto TCP (Transmission Control Protocol) a fin de incrementar la seguridad (Figura 3.178). Además se añadió un nuevo usuario (CGTT) con su respectiva contraseña (Mn3nT0Tr) en la categoría "Users" como se observa en las Figuras 3.179a y 3.179b. Para comprobar que el servidor Web estaba habilitado, se ingresó la dirección de la interfaz virtual del computador (127.0.0.1) seguida del número de puerto (8080) como URL (Uniform Resource Locator) en un navegador (Figura 3.180a). Como el acceso al servidor estaba protegido, se ingresó el nombre de usuario y contraseña definidos anteriormente. En la Figura 3.180b se muestra la pantalla principal del software de gestión y el hipervínculo al mapa en cuestión. Bastó un clic para que la topología se desplegara.

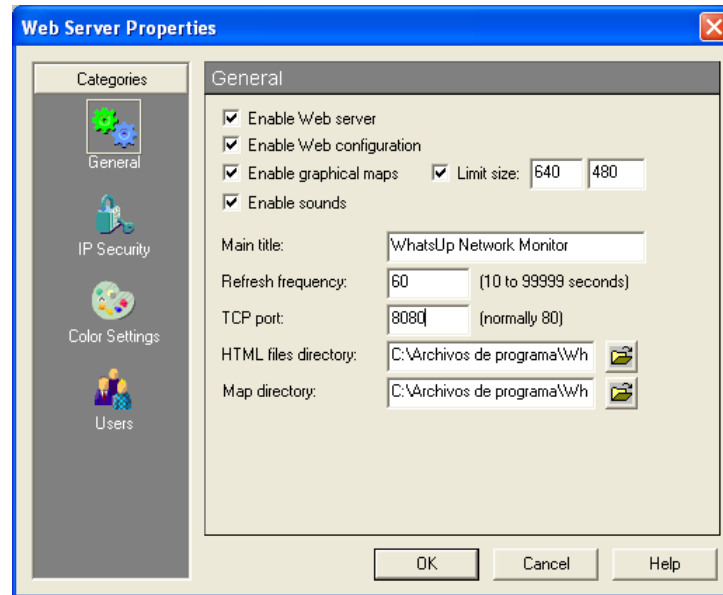


Figura 3.178: Número del Puerto TCP en Servidor Web

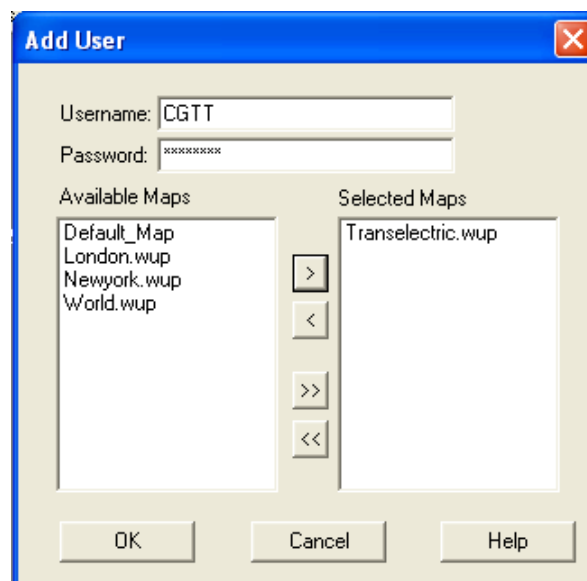


Figura 3.179a: Creación de Nuevo Usuario para Servidor Web (1 de 2)

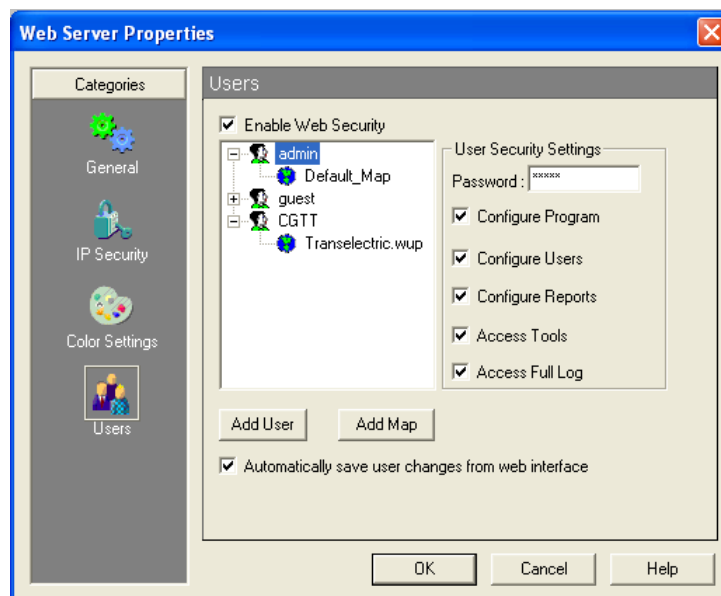


Figura 3.179b: Creación de Nuevo Usuario para Servidor Web (2 de 2)

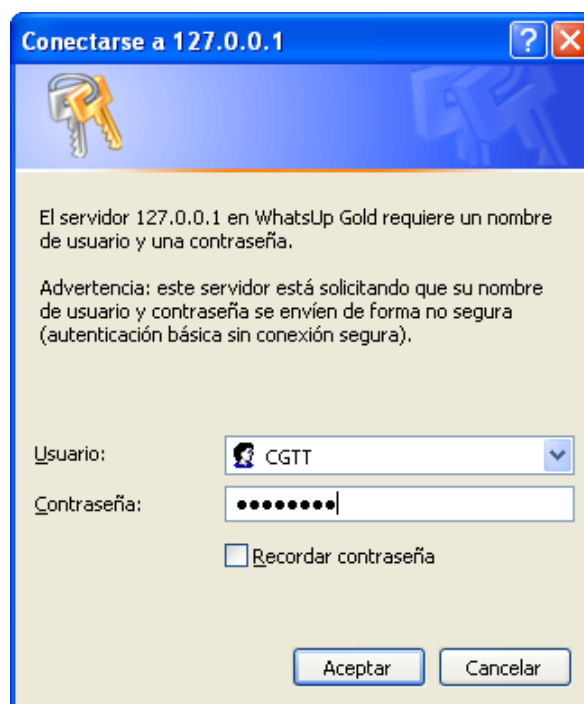


Figura 3.180a: Usuario y Contraseña para Conexión a Servidor Web

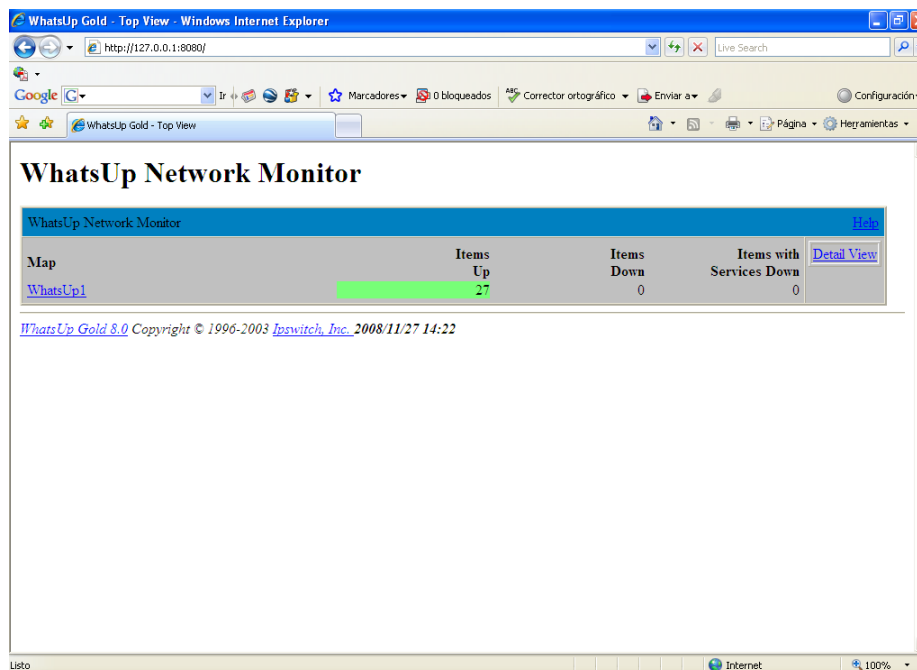


Figura 3.180b: Pantalla Principal del Software de Gestión

3.2.7.5.3 Estado de los Dispositivos

Con el objeto de observar la transición entre los distintos estados de un equipo se efectuaron reconocimientos periódicos mediante la opción “Poll Devices” del menú “Monitor”. El cuadrado verde que rodea los equipos de la Figura 3.181a indica que están funcionando normalmente. Cuando se perdió el primer paquete, el símbolo se convirtió en un rombo y el momento que expiró el temporizador del segundo reconocimiento, el objeto se tornó amarillo (Figura 3.181b). Luego de enviar el tercer paquete y no recibir respuesta, una estrella cubrió a los dispositivos (Figura 3.181c). Una estrella de color rojo apareció luego de revisar la comunicación por cuarta vez. Al cabo de 8 intentos fallidos, los equipos estaban cubiertos por una estrella de varias puntas (Figura 3.181d).

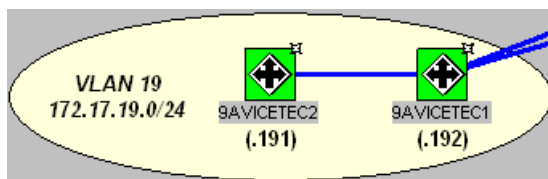


Figura 3.181a: Respuesta de Dispositivo ante Reconocimiento

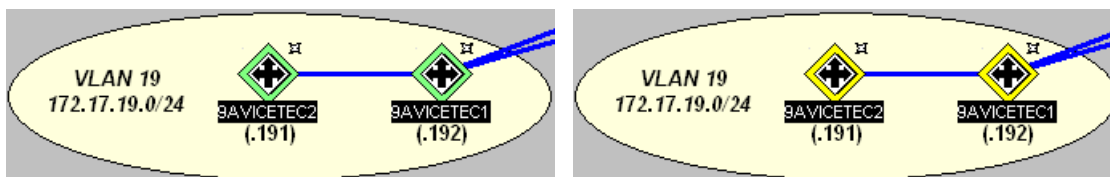


Figura 3.181b: Pérdida de 1 y 2 Paquetes

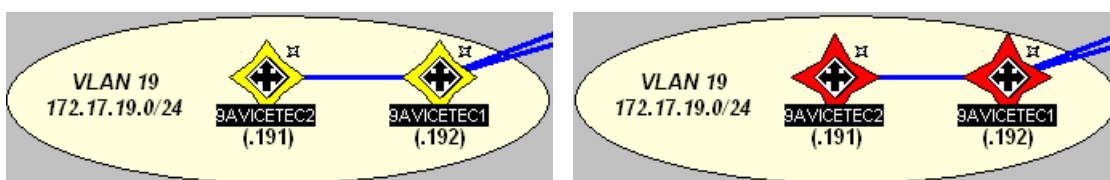


Figura 3.181c: Pérdida de 3 a 7 Paquetes



Figura 3.181d: Pérdida de más de 8 Paquetes

3.2.7.6 Gestión de la Topología Equivalente

3.2.7.6.1 Creación del Mapa

Una vez configurados los equipos de la topología equivalente se optó por descubrir los elementos de red utilizando SNMP. En las Figuras 3.182a y 3.182b se observa que el conmutador TELESRVA (172.17.83.101) se definió como dispositivo principal, se digitó la comunidad especificada previamente en los equipos y únicamente fueron consideradas

las interfaces en la exploración. Las Figuras 3.183a y 3.183b muestran el progreso del rastreo así como la identificación de nombres, servicios y tipos de dispositivos. Aunque se encontraron 32 dispositivos, únicamente se incluyeron 4 en el mapa porque el resto correspondían a interfaces y redes virtuales (Figura 3.184).

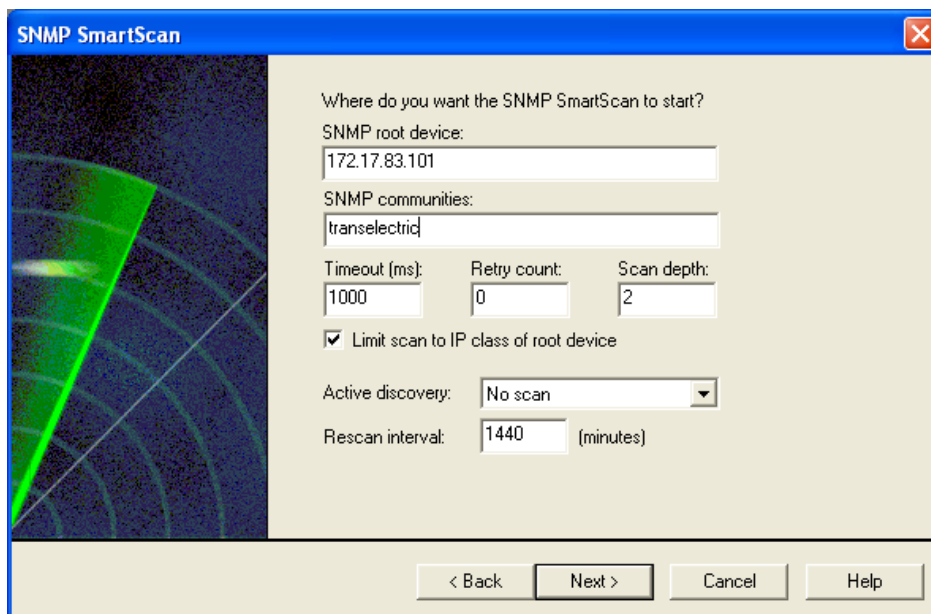


Figura 3.182a: Rastreo Inteligente utilizando SNMP

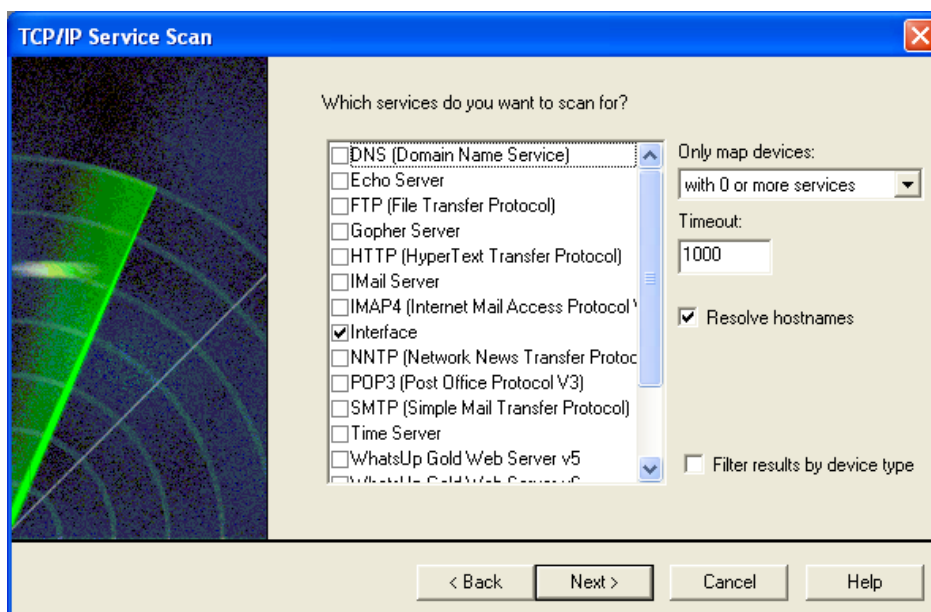


Figura 3.182b: Exploración de Servicios

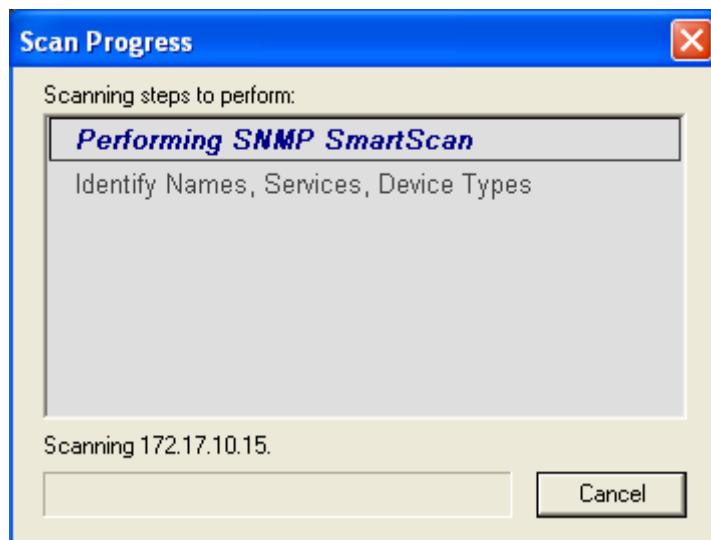


Figura 3.183a: Progreso de la Exploración

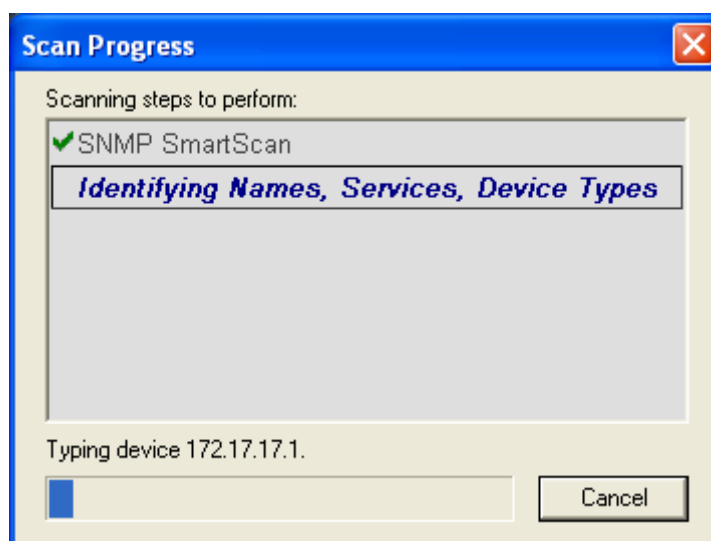


Figura 3.183b: Identificación de Nombres, Servicios y Tipos de Dispositivos

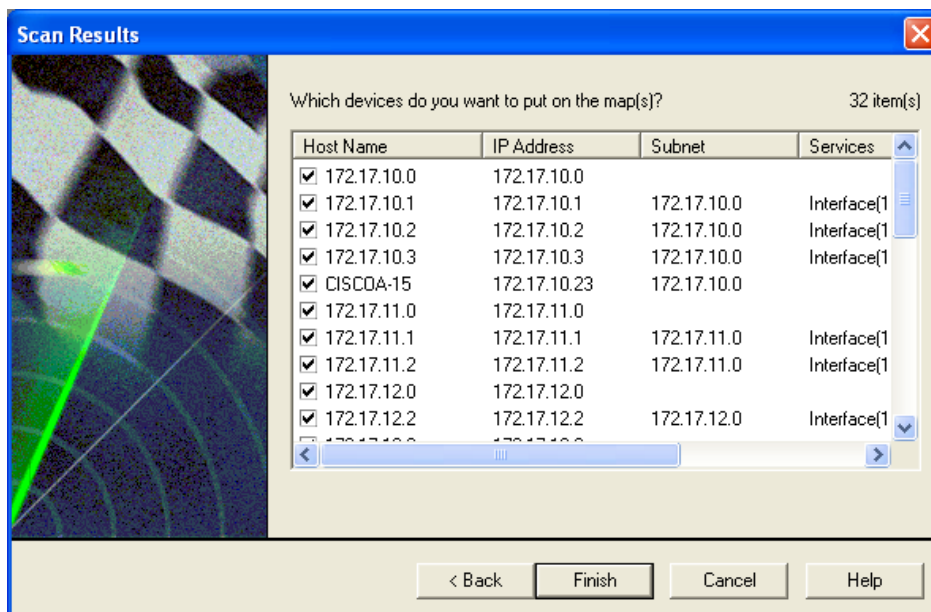


Figura 3.184: Resultados de la Exploración

3.2.7.6.2 Propiedades de los Dispositivos

La Figura 3.185 muestra que el nombre y dirección IP se había registrado automáticamente en los elementos administrables. Los nombres de las comunidades de lectura y escritura concuerdan con el parámetro establecido al inicio de la búsqueda. Ambos conmutadores de Core/Distribución tenían marcadas las casillas de monitoreo de las interfaces Fast Ethernet 9, 19, 21 y 22 (Figuras 3.186 y 3.187).

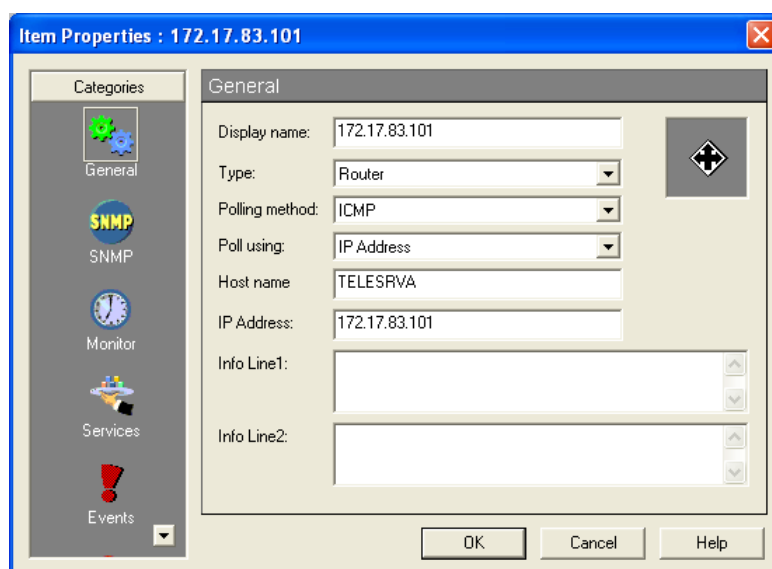


Figura 3.185: Campos de la Categoría General del Dispositivo TELESRVA

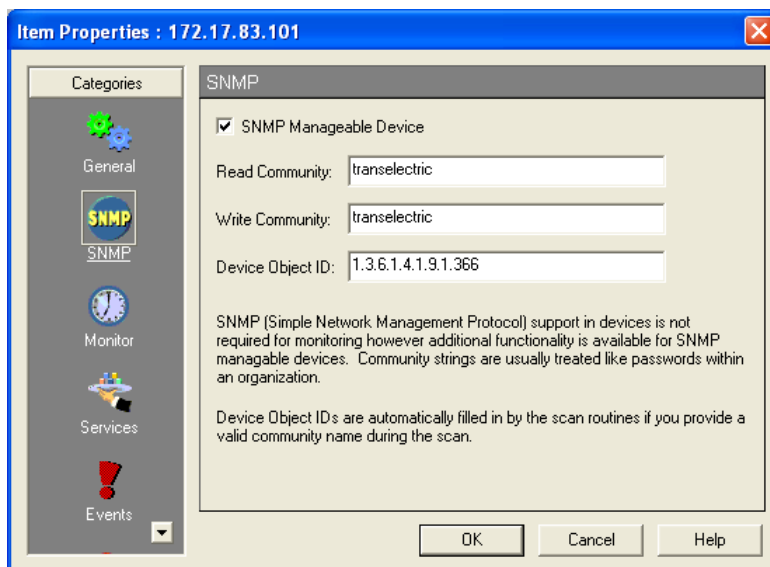


Figura 3.186: Campos de la Categoría SNMP del Dispositivo TELESRVA

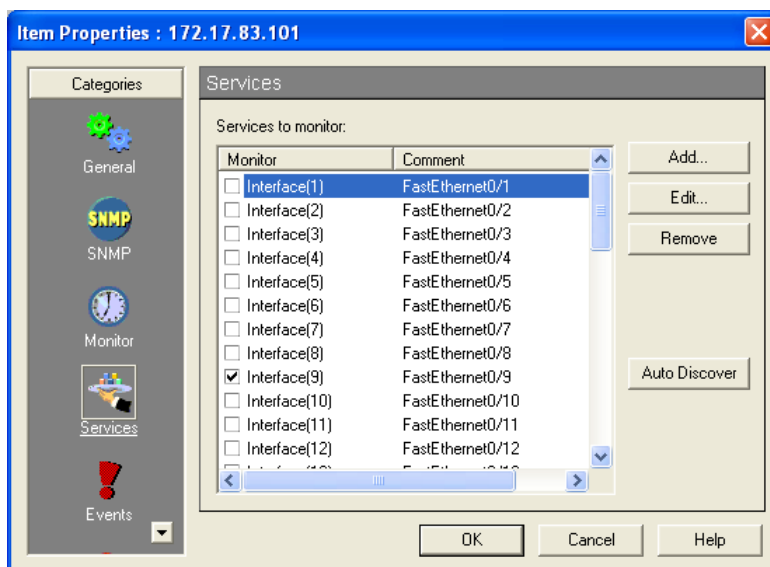


Figura 3.187: Servicios Identificados en el Dispositivo TELESRVA

La categoría “Status” de la Figura 3.188 indica que el dispositivo estaba activo y respondía a las peticiones. El gráfico de la Figura 3.189 proporciona información sobre el tiempo de operación satisfactoria en base a la cantidad de respuestas enviadas por el equipo. La bitácora (Log) muestra las instancias de los servicios (SVCUP/SVCDOWN). La Figura 3.190 detalla la fecha y hora del evento, el estado del servicio, la dirección del dispositivo y el servicio afectado. Para obtener un diagrama acorde a la implementación, se

organizaron los equipos de acuerdo a su ubicación en el edificio. En el centro del mapa se colocaron los elementos principales y en cada extremo se ubicó un conmutador de Acceso.

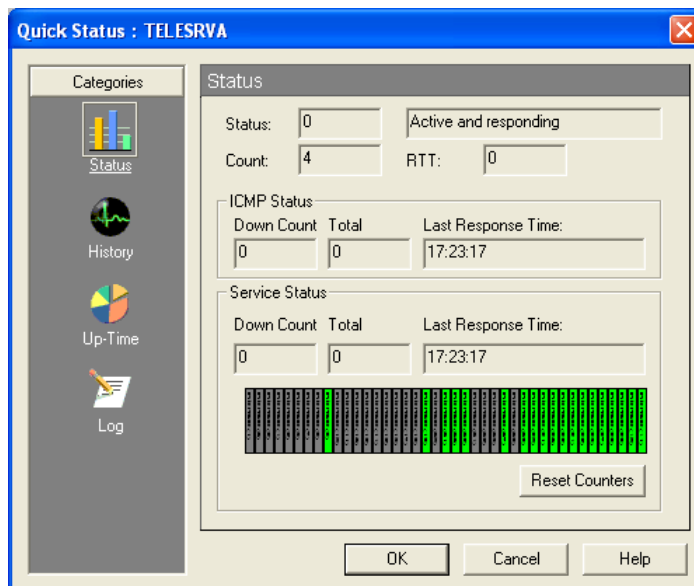


Figura 3.188: Categoría Estado del Dispositivo TELESRVA

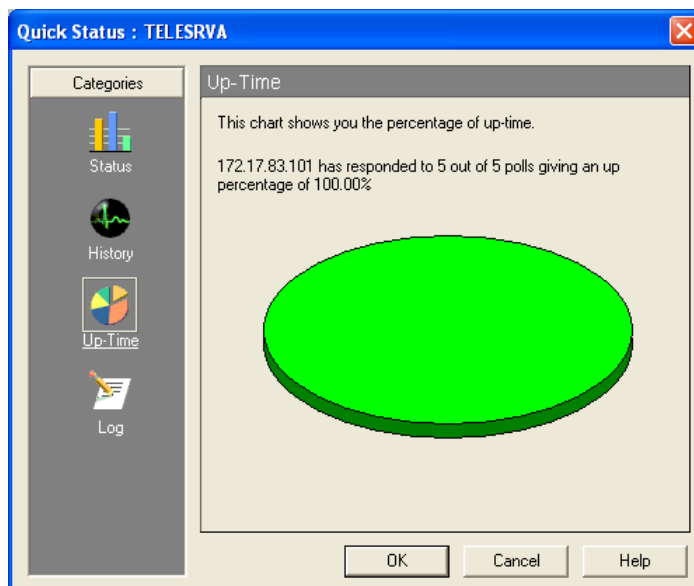


Figura 3.189: Categoría Tiempo de Funcionamiento del Dispositivo TELESRVA

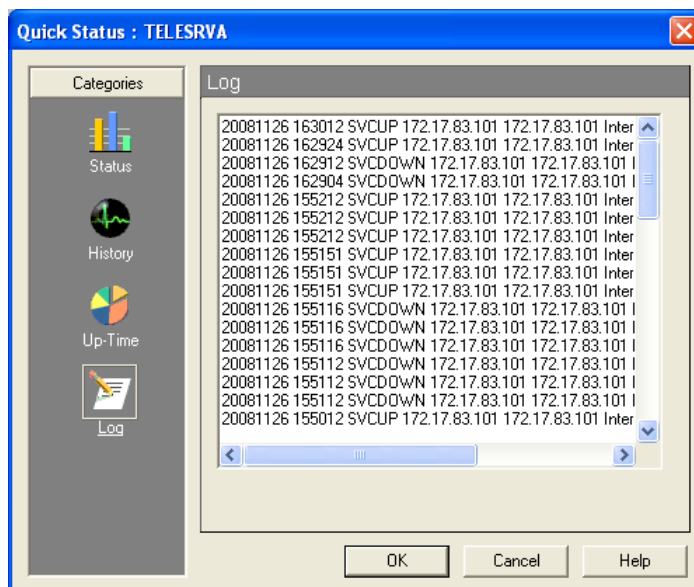


Figura 3.190: Bitácora del Dispositivo TELESRVA

3.2.7.6.3 Servidor Web y Estado de los Dispositivos

La interfaz Web presenta la dirección de la VLAN administrativa para acceder al mapa. Luego de hacer un clic en el hipervínculo se desplegó la topología (Figuras 3.191a y 3.191b).

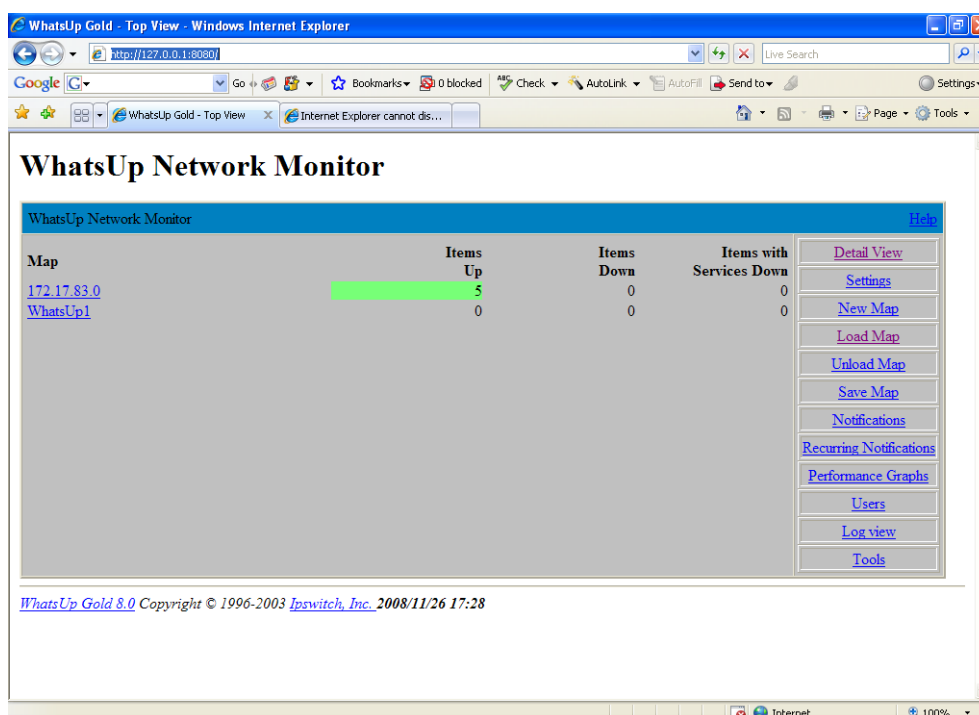


Figura 3.191a: Interfaz Web del Programa de Gestión

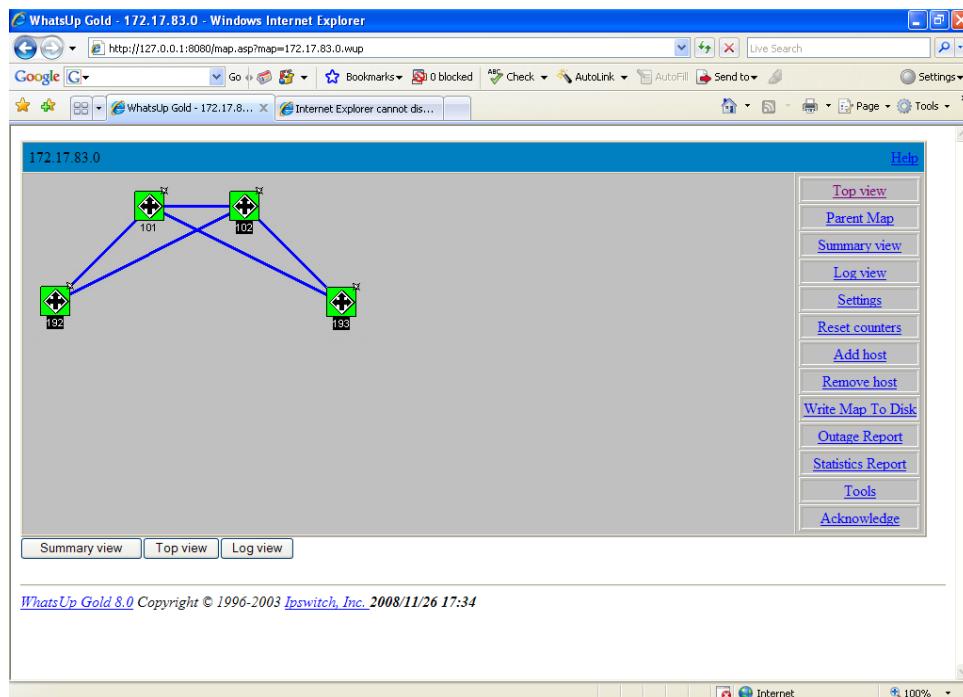


Figura 3.191b: Topología Equivalente para Administración

Cuando se desconectó un enlace y expiró el tiempo de reconocimiento apareció un hexágono de color rosa que indicó una falla en el servicio. El recuadro que se observa en el resto de dispositivos de la Figura 3.192a confirma que un reconocimiento estaba en proceso. La pérdida de un paquete ocasionó que la figura se convirtiera en un rombo (Figura 3.192b). Finalmente, un segundo dispositivo experimentó una falla en el servicio y surgió otro hexágono en la Figura 3.192c.

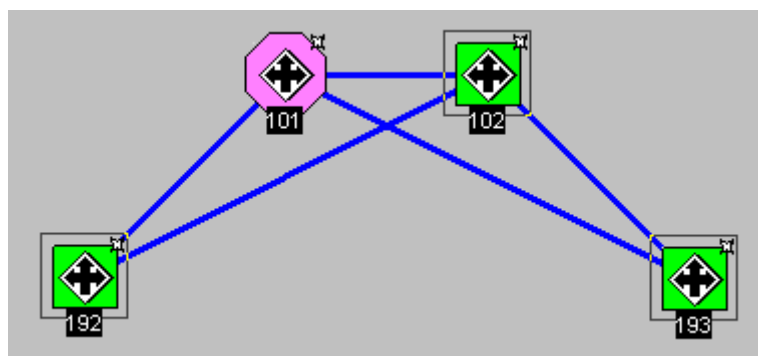


Figura 3.192a: Falla en un Dispositivo y Reconocimiento en Ejecución

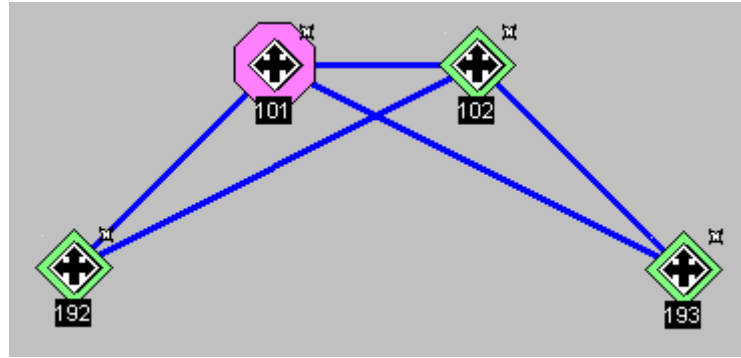


Figura 3.192b: Pérdida de 1 Paquete en Conmutadores

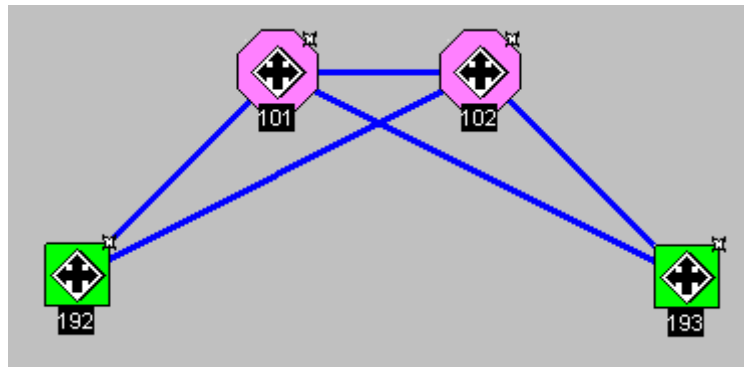


Figura 3.192c: Desconexión en la Capa de Core/Distribución

3.3 Análisis de Costos

3.3.1 Cuarto de Telecomunicaciones

3.3.1.1 Infraestructura de Seguridad, Sistema de Climatización y Control de Incendios

El Cuarto de Telecomunicaciones ubicado en el Quinto Piso necesita ciertas adecuaciones físicas para cumplir con los estándares actuales. Las paredes frontales así como la ventana posterior deben ser retiradas y reemplazadas por mampostería (bloques de cemento prefabricados). El ingreso tiene que estar protegido con una puerta de acero blindada con su respectivo control de acceso. La unidad de aire acondicionado debe ser cambiada por un sistema de climatización que regule la temperatura y humedad de la habitación. Además, es necesario incorporar un mecanismo de control de incendios que cuente con dispositivos de detección, panel de monitoreo y extintores.

3.3.1.2 Bastidores para Extensiones y Líneas Telefónicas

La distribución de extensiones y líneas directas implica el montaje de dos bastidores abiertos de 44U (1U = Unidad de Rack = 4,45cm) compuestos por 10 paneles de interconexión de 48 puertos, 10 organizadores horizontales de 2U y 2 organizadores verticales como se aprecia en la Figura 3.193. Una lista de los materiales necesarios se presenta en la Tabla 3.16.

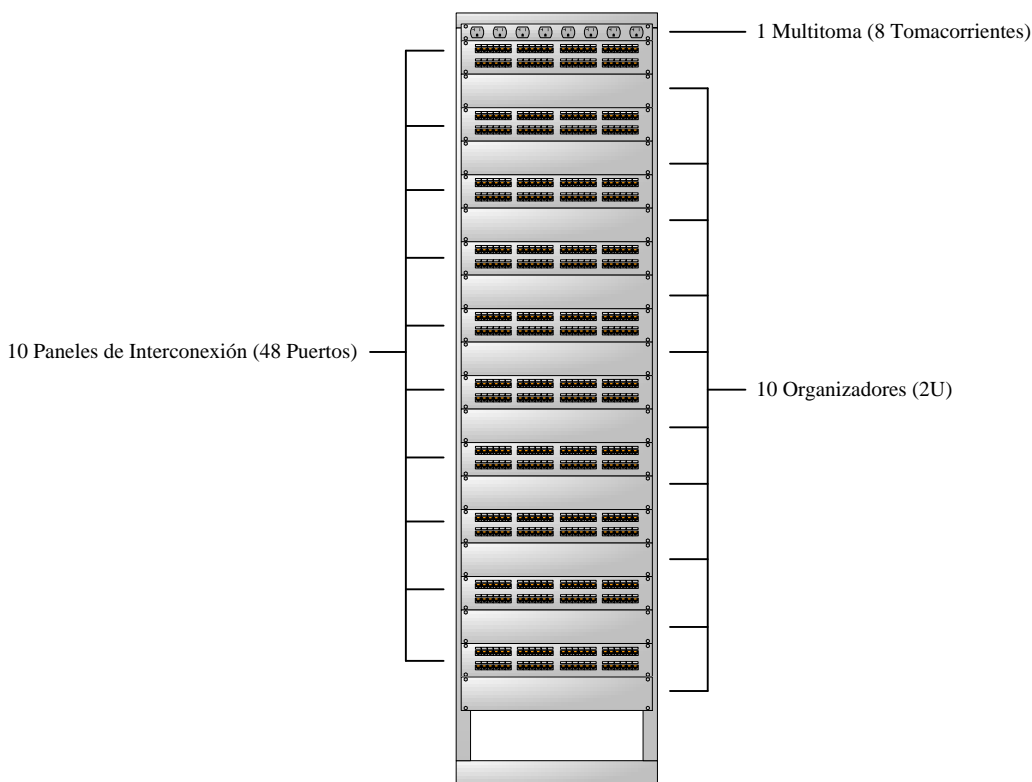


Figura 3.193: Bastidor para Distribución de Extensiones y Líneas Directas

Cantidad	Producto	Total
1	Bastidor (44U)	2
10	Organizadores Horizontal (2U)	20
10	Paneles de Interconexión de 48 Puertos RJ-45	20
480	Cables de Interconexión UTP RJ-45 de 1 metro	960
1	Multitoma (8 Tomacorrientes)	2

Tabla 3.16: Especificaciones para el Bastidor de Distribución de Extensiones y Líneas Directas

3.3.1.3 Armarios para Conmutadores de Core/Distribución

Para la instalación del par de conmutadores modulares de Core/Distribución Cisco Catalyst 6506 se requiere un armario cerrado de piso de 48U. En la parte inferior se colocará una Multitoma (8 tomacorrientes) para suministrar energía eléctrica al equipo. Luego, se montarán dos Fuentes de Poder, una Tarjeta Supervisora, una Tarjeta 10/100/1000 Ethernet de 48 puertos y una Tarjeta Gigabit Ethernet de 24 puertos SFP (Small Form-Factor Pluggable). Un ODF (Optical Fiber Distribution Frame) de 40 puertos

SC, un Panel de Interconexión de 48 puertos y un organizador horizontal de 2U se ubicarán a continuación.

Este conjunto de elementos activos y pasivos se duplicará en la parte superior como se observa en la Figura 3.194. Los dos puertos SFP de las Tarjetas Supervisoras permitirán interconectar ambos equipos con un par de cables de interconexión de fibra óptica multimodo LC a LC. Veinte de los 48 puertos de la Tarjeta 10/100/1000 Ethernet se conectarán al panel de interconexión de 48 puertos, el cual estará enlazado con la Sala de Servidores mediante cable sólido UTP (Unshielded Twisted Pair) de 4 pares. Los conmutadores de cada ala se conectarán a las Tarjetas Gigabit Ethernet de 24 puertos SFP utilizando los ODFs y 38 cables de interconexión de fibra óptica multimodo SC a LC. Las Tablas 3.17a y 3.17b detallan las cantidades y productos requeridos para la Capa de Core/Distribución.

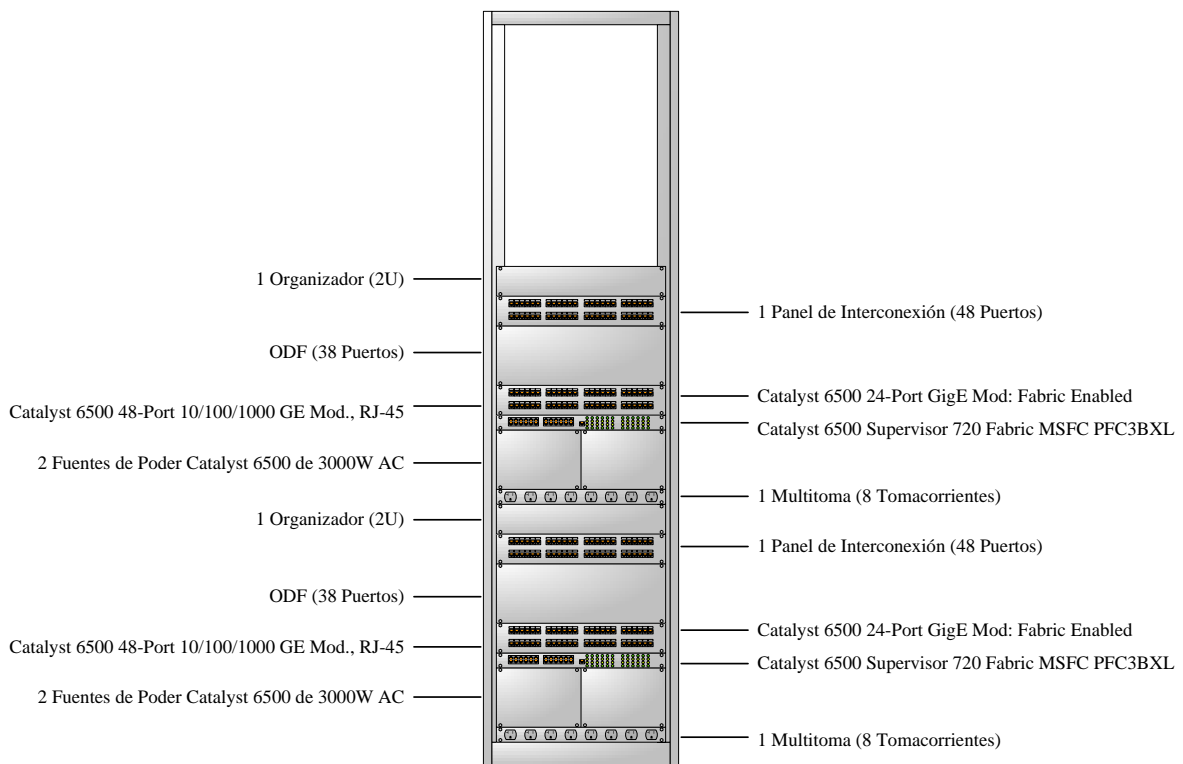


Figura 3.194: Armario para los Conmutadores de Core/Distribución

Cantidad	Producto	Total
1	Armario (48U)	2
1	Organizador Horizontal (2U)	2
2	Organizadores Verticales	4
1	Panel de Interconexión de 48 Puertos RJ-45	2
20	Cables de Interconexión UTP RJ-45 de 1 metro	40
1440	Metros de Cable UTP Sólido de 4 pares	2880
1	ODF (Optical-Fiber Distribution Frame) de 38 Puertos SC	2
76	Pigtails SC de 1 metro	152
19	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	38
1	Cable de Interconexión de Fibra Óptica Multimodo LC a LC de 1 metro	2
1	Multitoma (8 Tomacorrientes)	2
530	Metros de Cable de Fibra Óptica Multimodo de 4 hilos	1060

Tabla 3.17a: Especificaciones para el Armario de Core/Distribución (1 de 2)

Cantidad	Producto	Código	Descripción	Total
1	Chasis	WS-C6506-E	Catalyst 6500 Enhanced 6-slot chassis, 12RU, no PS, no Fan Tray	2
1	Tarjeta Supervisora	WS-SUP720-3BXL	Catalyst 65007Cisco 7600 Supervisor 720 Fabric MSFC3 PFC3BXL	2
1	Tarjeta 10/100/1000 Ethernet de 48 Puertos	WS-X6148-GE-TX	Catalyst 6500 48-port 10/100/1000 GE Mod., RJ-45	2
1	Tarjeta Gigabit Ethernet de 24 Puertos SFP	WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFPs)	2
1	Ventilador	WS-C6506-E-FAN	Catalyst 6506-E Chassis Fan Tray	2
2	Fuentes de Poder de 3000W AC	WS-CAC-3000W	Catalyst 6500 3000W AC power supply	4
26	Módulos SFP	GLC-SX-MM	GE SFP, LC connector SX transceiver	52

Tabla 3.17b: Especificaciones para el Armario de Core/Distribución (2 de 2)

3.3.2 Distribución de Armarios para Conmutadores de Acceso

En ambas alas de cada piso se colocará un armario cerrado de pared de 18U, el cual estará formado por un ODF de 4 puertos SC, uno o dos conmutadores según las necesidades de cada departamento, organizadores horizontales y paneles de interconexión de 24 o 48 puertos para datos y voz. Al final de cada armario se instalará una Multitoma (8 tomacorrientes) para proporcionar energía eléctrica a los dispositivos. Se ha estimado conveniente crear 12 grupos para determinar los elementos que deben ser adquiridos para la Capa de Acceso.

La Figura 3.195 muestra el armario que se ubicará en las Alas Oriental y Occidental del décimo piso. Los conmutadores Cisco Catalyst 3500 Series XL (5B y 9I) requieren cuatro cables de interconexión de fibra óptica multimodo SC a SC. En la Tabla 3.18 se listan los materiales necesarios para la instalación.

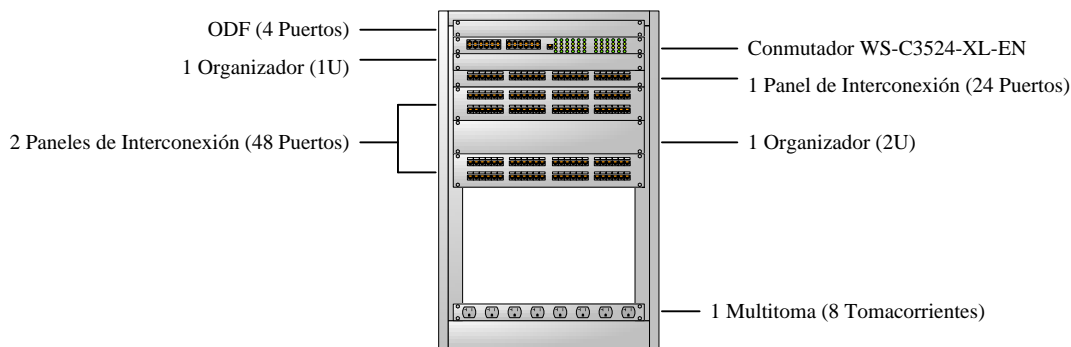


Figura 3.195: Armario del Décimo Piso (A y B)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	2
8	Pigtails SC de 1 metro	16
1	Organizador Horizontal (1U)	2
1	Organizador Horizontal (2U)	2
1	Panel de Interconexión de 24 Puertos RJ-45	2
2	Paneles de Interconexión de 48 Puertos RJ-45	4
1	Multitoma (8 Tomacorrientes)	2
2	Cables de Interconexión de Fibra Óptica Multimodo SC a SC de 1 metro	4
72	Cables de Interconexión UTP RJ-45 de 1 metro	144

Tabla 3.18: Especificaciones para el Armario del Décimo Piso (A y B)

Los armarios que se utilizarán en el noveno piso se ilustran en las Figuras 3.196a y 3.196b. Cuatro cables de interconexión de fibra óptica multimodo SC a MT-RJ permitirán interconectar los ODFs con los conmutadores Cisco Catalyst 2950 Series (5E y 9F). El conmutador Cisco Catalyst 2950 Series (5C) empleará un par de cables de interconexión de cable UTP RJ-45 para el enlace entre dispositivos. Las Tablas 3.19a y 3.19b detallan los implementos requeridos para el montaje.

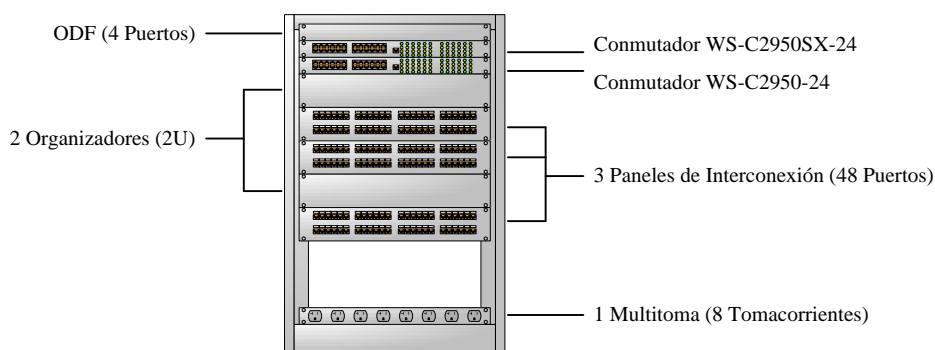


Figura 3.196a: Armario del Noveno Piso (A)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
2	Organizadores Horizontales (2U)	2
3	Paneles de Interconexión de 48 Puertos RJ-45	3
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a MT-RJ de 1 metro	2
96	Cables de Interconexión UTP RJ-45 de 1 metro	96

Tabla 3.19a: Especificaciones para el Armario del Noveno Piso (A)

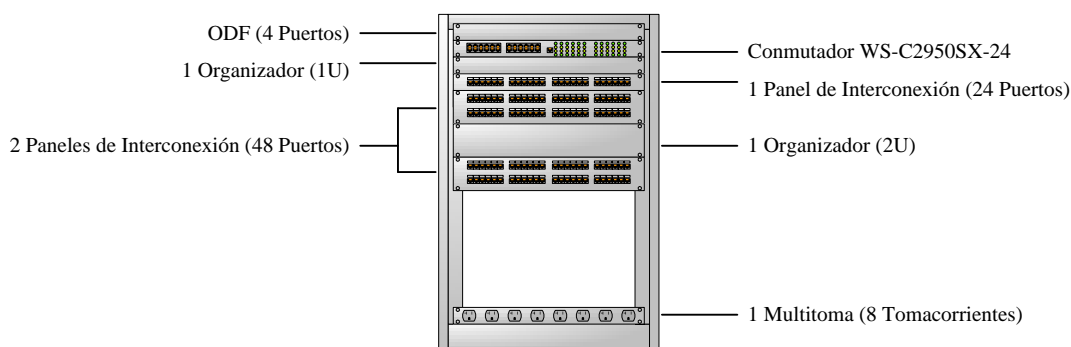


Figura 3.196b: Armario del Noveno Piso (B)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
1	Organizador Horizontal (1U)	1
1	Organizador Horizontal (2U)	1
1	Panel de Interconexión de 24 Puertos RJ-45	1
2	Paneles de Interconexión de 48 Puertos RJ-45	2
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a MT-RJ de 1 metro	2
72	Cables de Interconexión UTP RJ-45 de 1 metro	72

Tabla 3.19b: Especificaciones para el Armario del Noveno Piso (B)

La distribución de equipos para el octavo piso se puede apreciar en la Figura 3.197. Cada armario contará con un conmutador Cisco Catalyst 2960 Series (5A y 9H) y los cables de interconexión de fibra óptica multimodo SC a LC respectivos. Las cantidades y productos que deben incluirse en la licitación se indican en la Tabla 3.20.

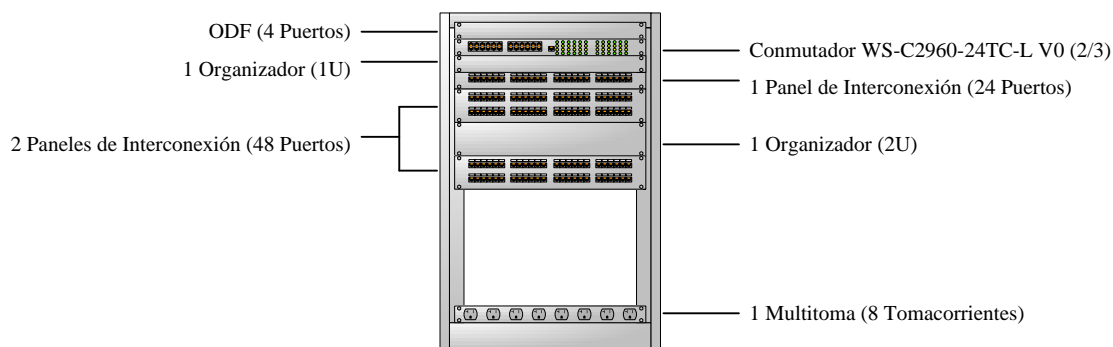


Figura 3.197: Armario del Octavo Piso (A y B)

Cantidad	Producto	Total
1	Armario (18U)	2
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	2
8	Pigtails SC de 1 metro	16
1	Organizador Horizontal (1U)	2
1	Organizador Horizontal (2U)	2
1	Panel de Interconexión de 24 Puertos RJ-45	2
2	Paneles de Interconexión de 48 Puertos RJ-45	4
1	Multitoma (8 Tomacorrientes)	2
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	4
72	Cables de Interconexión UTP RJ-45 de 1 metro	144

Tabla 3.20: Especificaciones para el Armario del Octavo Piso (A y B)

Dos conmutadores Cisco Catalyst 2960 Series SI (9D y 9E) y un Cisco Catalyst 2960 (9A) serán parte de los armarios diseñados para el séptimo piso que se muestran en las Figuras 3.198a y 3.198b. En los dos casos se necesitará un par de cables de interconexión de fibra óptica multimodo SC a LC. Para el enlace entre los conmutadores del Ala A se requieren dos cables de interconexión UTP RJ-45. Un detalle de los implementos necesarios para esta instalación se incluye en las Tablas 3.21a y 3.21b.

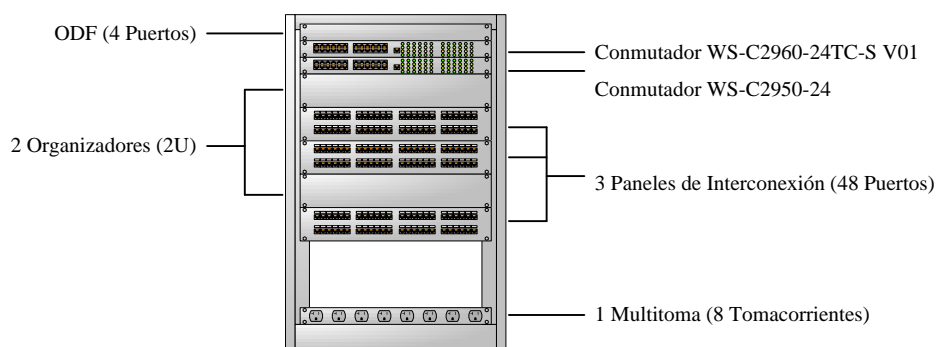


Figura 3.198a: Armario del Séptimo Piso (A)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
2	Organizadores Horizontales (2U)	2
3	Paneles de Interconexión de 48 Puertos RJ-45	3
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	2
96	Cables de Interconexión UTP RJ-45 de 1 metro	96

Tabla 3.21a: Especificaciones para el Armario del Séptimo Piso (A)

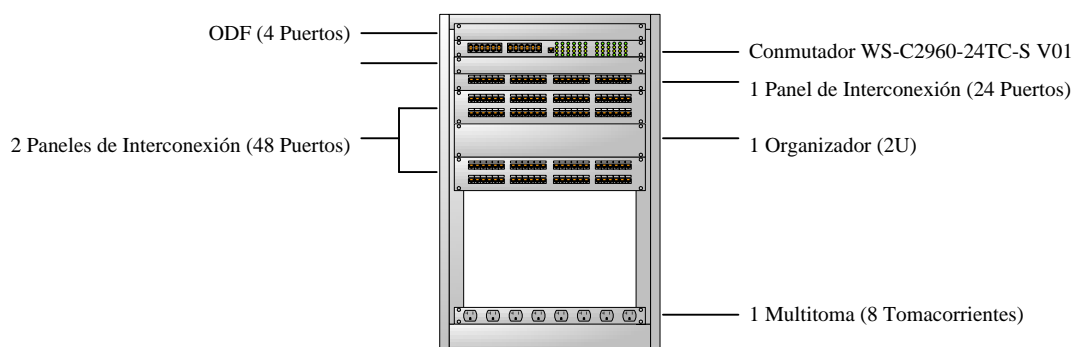


Figura 3.198b: Armario del Séptimo Piso (B)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
1	Organizador Horizontal (1U)	1
1	Organizador Horizontal (2U)	1
1	Panel de Interconexión de 24 Puertos RJ-45	1
2	Paneles de Interconexión de 48 Puertos RJ-45	2
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	2
72	Cables de Interconexión UTP RJ-45 de 1 metro	72

Tabla 3.21b: Especificaciones para el Armario del Séptimo Piso (B)

El modelo de armario que se colocará en ambas alas del sexto piso, el ala Oriental del quinto piso y Occidental del cuarto y tercer pisos se observa en la Figura 3.199. Un conmutador Cisco Catalyst 2960 Series (WS-C2960-48TC-L) de 48 puertos y un par de cables de interconexión de fibra óptica multimodo SC a LC deberán ser adquiridos para cada armario. La Tabla 3.22 especifica los implementos necesarios para el montaje.

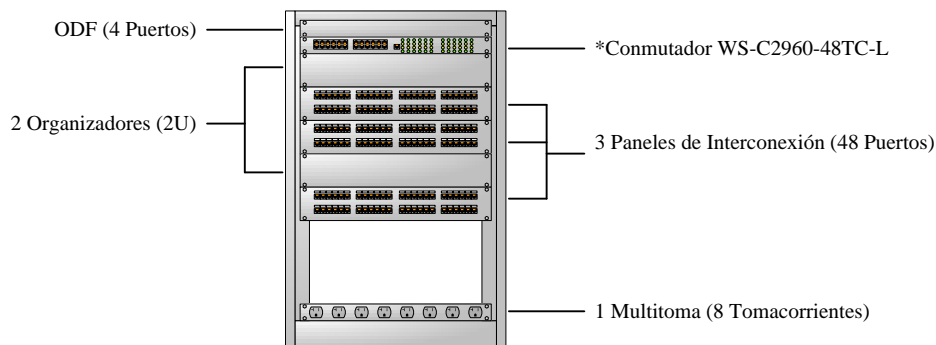


Figura 3.199: Armario del Sexto Piso (A y B), Quinto Piso (A), Cuarto y Tercer Pisos (B)

Cantidad	Producto	Total
1	Armario (18U)	5
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	5
8	Pigtails SC de 1 metro	40
1	Conmutador WS-C2960-48TC-L	5
2	Organizadores Horizontales (2U)	10
3	Paneles de Interconexión de 48 Puertos RJ-45	15
1	Multitoma (8 Tomacorrientes)	5
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	10
96	Cables de Interconexión UTP RJ-45 de 1 metro	480

Tabla 3.22: Especificaciones para el Armario del Sexto Piso (A y B), Quinto Piso (A), Cuarto y Tercer Pisos (B)

El armario previsto para el Departamento de Informática demanda un conmutador Cisco Catalyst 2960 Series (WS-C2960-48TC-L) adicional, dos cables de interconexión de fibra óptica multimodo SC a LC y dos paneles de interconexión de 48 puertos para recibir los enlaces de las Tarjetas 10/100/1000 Ethernet destinados para los servidores como se ilustra en la Figura 3.200. Los materiales requeridos para esta ala se listan en la Tabla 3.23.

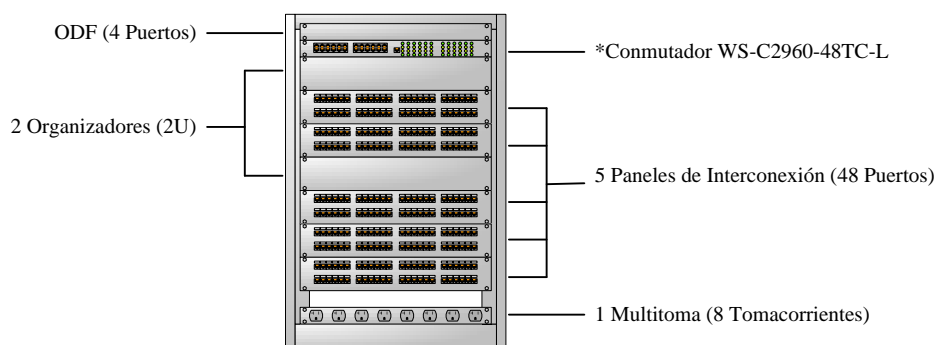


Figura 3.200: Armario del Quinto Piso (B)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
1	Conmutador WS-C2960-48TC-L	1
2	Organizadores Horizontales (2U)	2
5	Paneles de Interconexión de 48 Puertos RJ-45	5
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	2
96	Cables de Interconexión UTP RJ-45 de 1 metro	96

Tabla 3.23: Especificaciones para el Armario del Quinto Piso (B)

En la Figura 3.201 se presenta el armario destinado para el Ala Oriental del tercer piso. El conmutador Cisco Catalyst 2950 Series (9G) se interconectará al conmutador Cisco Catalyst 2960 (Departamento de Adquisiciones, Logística y Bodega) mediante dos cables de interconexión UTP RJ-45. El enlace hacia el ODF se realizará con la ayuda de un cable de interconexión de fibra óptica multimodo SC a LC. La Tabla 3.24 lista los componentes de este armario.

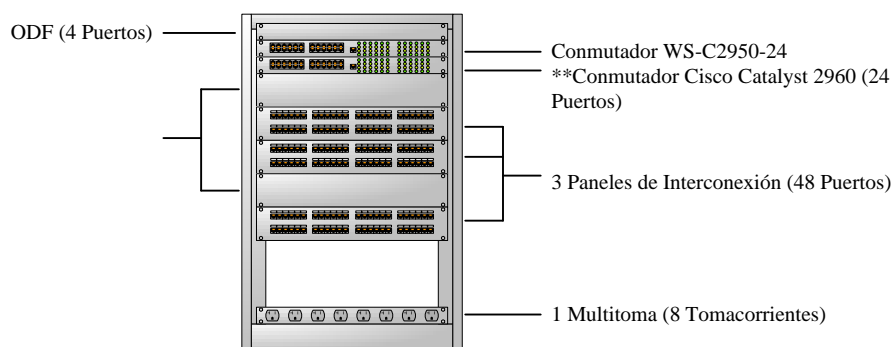


Figura 3.201: Armario del Tercer Piso (A)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
2	Organizadores Horizontales (2U)	2
3	Paneles de Interconexión de 48 Puertos RJ-45	3
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	2
96	Cables de Interconexión UTP RJ-45 de 1 metro	96

Tabla 3.24: Especificaciones para el Armario del Tercer Piso (A)

El equipamiento de las dos alas del segundo piso se organizó como indica la Figura 3.202. El conmutador Cisco Catalyst 2960 (Gerencia de Telecomunicaciones) así como un conmutador Cisco Catalyst 2960 (WS-C2960-24TC-L) estarán conectados a su respectivo ODF mediante cables de interconexión de fibra óptica multimodo SC a LC. Mientras que los dispositivos Cisco Catalyst 2900 (Asesoría Jurídica) y Cisco Catalyst 2960 (WS-C2960-24TC-L) utilizarán cables de interconexión UTP RJ-45 para agrupación de puertos. En la Tabla 3.25 se listan los materiales requeridos para la instalación.

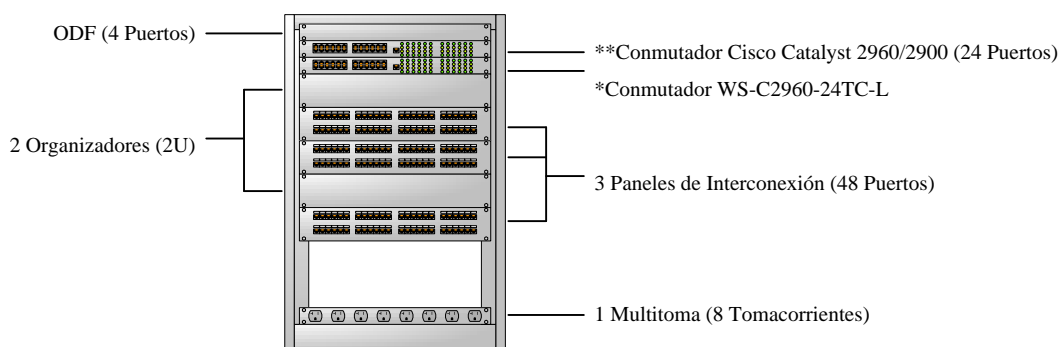


Figura 3.202: Armario del Segundo Piso (A y B)

Cantidad	Producto	Total
1	Armario (18U)	2
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	2
8	Pigtails SC de 1 metro	16
1	Conmutador WS-C2960-24TC-L	2
2	Organizadores Horizontales (2U)	4
3	Paneles de Interconexión de 48 Puertos RJ-45	6
1	Multitoma (8 Tomacorrientes)	2
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	4
96	Cables de Interconexión UTP RJ-45 de 1 metro	192

Tabla 3.25: Especificaciones para el Armario del Segundo Piso (A y B)

El armario que será ubicado en el Ala A de la Planta Baja demanda la adquisición de un conmutador Cisco Catalyst 2960 (WS-C2960-24TC-L) y un par de cables de interconexión de fibra óptica SC a LC (Figura 3.203). Las cantidades y productos que se necesitan para el montaje se detallan en la Tabla 3.26a.

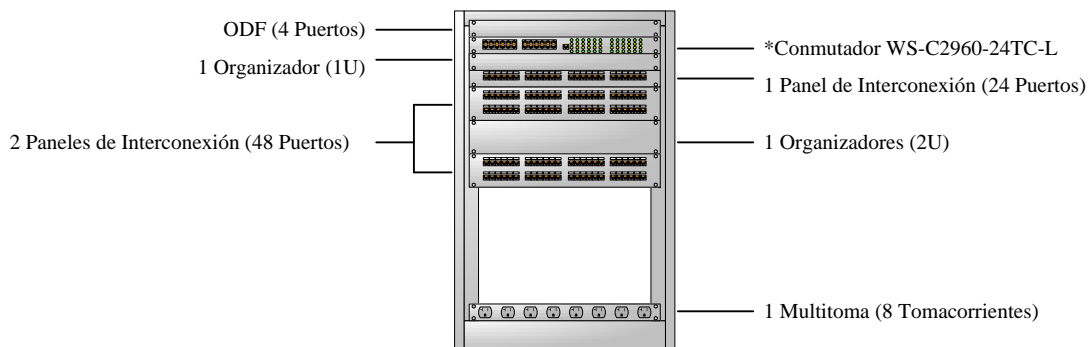


Figura 3.203a: Armario de la Planta Baja (A)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
1	Conmutador WS-C2960-24TC-L	1
1	Organizador Horizontal (1U)	1
1	Organizador Horizontal (2U)	1
1	Panel de Interconexión de 24 Puertos RJ-45	1
2	Paneles de Interconexión de 48 Puertos RJ-45	2
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	2
72	Cables de Interconexión UTP RJ-45 de 1 metro	72

Tabla 3.26a: Especificaciones para el Armario de la Planta Baja (A)

La Figura 3.203b muestra que para el Ala B de la Planta Baja será necesario incorporar un conmutador Cisco Catalyst 2960 (WS-C2960-48TC-L) y se conservará el dispositivo Cisco Catalyst 2960 (Sala de Uso Múltiple). En la Tabla 3.26b se detallan los implementos requeridos para dicho armario. Un resumen de los materiales necesarios para la Capa de Acceso se proporciona en la Tabla 3.27.

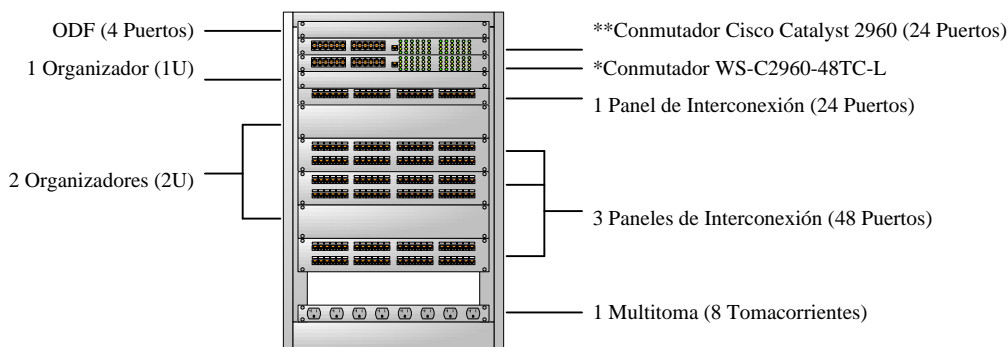


Figura 3.203b: Armario de la Planta Baja (B)

Cantidad	Producto	Total
1	Armario (18U)	1
1	ODF (Optical-Fiber Distribution Frame) de 4 Puertos SC	1
8	Pigtails SC de 1 metro	8
1	Conmutador WS-C2960-48TC-L	1
1	Organizador Horizontal (1U)	1
2	Organizadores Horizontales (2U)	2
1	Panel de Interconexión de 24 Puertos RJ-45	1
3	Paneles de Interconexión de 48 Puertos RJ-45	3
1	Multitoma (8 Tomacorrientes)	1
2	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro	2
120	Cables de Interconexión UTP RJ-45 de 1 metro	120

Tabla 3.26b: Especificaciones para el Armario de la Planta Baja (B)

Cantidad	Producto
19	Armarios (18U)
19	ODFs (Optical-Fiber Distribution Frames) de 4 Puertos SC
152	Pigtails SC de 1 metro
8	Organizadores Horizontal (1U)
31	Organizadores Horizontales (2U)
8	Paneles de Interconexión de 24 Puertos RJ-45
52	Paneles de Interconexión de 48 Puertos RJ-45
19	Multitomas (8 Tomacorrientes)
4	Cables de Interconexión de Fibra Óptica Multimodo SC a SC de 1 metro
4	Cables de Interconexión de Fibra Óptica Multimodo SC a MT-RJ de 1 metro
30	Cables de Interconexión de Fibra Óptica Multimodo SC a LC de 1 metro
1680	Cables de Interconexión UTP RJ-45 de 1 metro
3	Conmutadores WS-C2960-24TC-L
7	Conmutadores WS-C2960-48TC-L
30	Módulos SFP (Small Form-Factor Pluggable)
2	Módulos GBIC (Gigabit Interface Converter)

Tabla 3.27: Resumen de Especificaciones para los Armarios

*Conmutador que deberá ser adquirido según la Propuesta de Diseño.

**Conmutador que se encuentra instalado y funcionando.

3.3.3 Cableado Vertical

Un par de cables de fibra óptica multimodo 62.5/125 de 4 hilos se tenderá desde el Cuarto de Telecomunicaciones hasta llegar a los armarios de cada ala. Solamente se utilizarán dos hilos por cable para establecer la comunicación entre las Capas de Acceso y Core/Distribución. El resto de hilos se mantendrá como reserva para instalaciones futuras. La Tabla 3.28 muestra las distancias que deberán ser cubiertas.

Desde	Hasta	Distancia (m)
Cuarto de Telecomunicaciones	Décimo	34
	Noveno	31
	Octavo	28
	Séptimo	25
	Sexto	22
	Quinto	19
	Cuarto	22
	Tercero	25
	Segundo	28
	Planta Baja	31

Tabla 3.28: Distancias entre el Cuarto de Telecomunicaciones y cada Piso

3.3.4 Ofertas Económicas

Para conocer las alternativas que existen en el mercado respecto a seguridad, sistemas de ventilación y control de humedad y mecanismos de control de incendios se visitó la empresa PROTECOMPU, donde mostraron gran interés por brindar una solución integral que se incluye en las Tablas 3.29a - 3.29d.

Dos empresas altamente reconocidas en el área de las Telecomunicaciones fueron seleccionadas para solicitar las cotizaciones sobre dispositivos activos y cableado estructurado, obteniéndose la colaboración de dichas empresas aun cuando desconocen el nombre del cliente, situación que habla de su compromiso y aporte a un proyecto académico. Considerando las ofertas presentadas por Andean Trade (Tabla 3.30) y TOTALTEK (Tabla 3.31) se recomienda elegir la opción más conveniente en términos económicos.




COMPañIA :
CIUDAD : Quito
REFERENCIA : Proyecto para Infraestructura Centro de Cómputo
E-mail : josejavier_orozco@hotmail.com

ATENCIÓN : Sr. Javier Orozco
TELÉFONO : 2347-758
FECHA : Noviembre, 08 del 2008
No. OFERTA :

OFERTA ECONOMICA					
8	19	Rack Avante 18 U de producción nacional. Dimensiones: 79,20cms alto x 96 cms profundidad x 60 cms de ancho. Con Puerta	U	\$300,00	\$5.700,00
	8	Bandeja fija para equipos (2 por rack)	U	\$35,00	\$280,00
	4	Bandeja móvil para teclado (1 por rack)	U	\$75,00	\$300,00
	4	Kit de ventilación (1 po rack)	U	\$120,00	\$480,00
	4	Multitoma nacional de 12 puntos (1 por rack)	U	\$95,00	\$380,00
DISTRIBUIDOR ELECTRICO NACIONAL (PDU)					
10	1	Distribuidor eléctrico nacional. Tablero integral que incorpora las protecciones eléctricas para el aire acondicionado y el UPS. Adicionalmente incluye un centro de carga para energía regulada proveniente del UPS con las protecciones para alimentar la red regulada externa al centro de cómputo, mas 4 Cables con conectores Nema 5-20 para alimentar, bajo el piso falso, los Gabinetes instalados dentro del centro de cómputo. <i>La acometida electrica desde tablero general del edificio hasta el centro de computo no esta incluida.</i>	U	\$4.800,00	\$4.800,00
TOTAL OFERTADO ANTES DE IVA:					\$34.102,00
CONDICIONES COMERCIALES					
Tiempo Entrega:		Piso, Techo, Monitoreo, Aire Acondicionado, UPS: Inmediata (24 horas), salvo venta previa Detección de Incendios : 3 semanas recibida la orden de compra y el anticipo Extinción de Incendios : 6-7 semanas recibida la orden de compra y el anticipo Trabajos Eléctricos: A convenir con el cliente			
Instalación:		Se entregan todos los equipos y sistemas debidamente instalados y en perfecto estado funcional			

Tabla 3.29a: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (1 de 4)

	COMPANÍA :		ATENCION : Sr. Javier Orozco
	CIUDAD :	Quito	TELEFONO : 2347-758
	REFERENCIA :	Proyecto para Infraestructura Centro de Cómputo	FECHA : Noviembre, 08 del 2008
	E-mail :	josejavier_orozco@hotmail.com	No. OFERTA :

OFERTA ECONOMICA					
8	19	Rack Avante 18 U de producción nacional. Dimensiones: 79,20cms alto x 96 cms profundidad x 60 cms de ancho. Con Puerta	U	\$300,00	\$5.700,00
	8	Bandeja fija para equipos (2 por rack)	U	\$35,00	\$280,00
	4	Bandeja móvil para teclado (1 por rack)	U	\$75,00	\$300,00
	4	Kit de ventilación (1 po rack)	U	\$120,00	\$480,00
	4	Multitoma nacional de 12 puntos (1 por rack)	U	\$95,00	\$380,00
DISTRIBUIDOR ELECTRICO NACIONAL (PDU)					
10	1	Distribuidor eléctrico nacional. Tablero integral que incorpora las protecciones eléctricas para el aire acondicionado y el UPS. Adicionalmente incluye un centro de carga para energía regulada proveniente del UPS con las protecciones para alimentar la red regulada externa al centro de cómputo, mas 4 Cables con conectores Nema 5-20 para alimentar, bajo el piso falso, los Gabinetes instalados dentro del centro de cómputo. <i>La acometida electrica desde tablero general del edificio hasta el centro de computo no esta incluida.</i>	U	\$4.800,00	\$4.800,00
TOTAL OFERTADO ANTES DE IVA:					\$34.102,00
CONDICIONES COMERCIALES					
Tiempo Entrega:	Piso, Techo, Monitoreo, Aire Acondicionado, UPS: Inmediata (24 horas), salvo venta previa Detección de Incendios : 3 semanas recibida la orden de compra y el anticipo Extinción de Incendios : 6-7 semanas recibida la orden de compra y el anticipo Trabajos Eléctricos: A convenir con el cliente				
Instalación:	Se entregan todos los equipos y sistemas debidamente instalados y en perfecto estado funcional				

Tabla 3.29b: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (2 de 4)


	COMPANÍA : CIUDAD : Quito REFERENCIA : Proyecto para Infraestructura Centro de Cómputo E-mail : josejavier_orozco@hotmail.com	ATENCION : Sr. Javier Orozco TELEFONO : 2347-758 FECHA : Noviembre, 08 del 2008 No. OFERTA :
	OFERTA ECONOMICA	
Forma de pago:	50% anticipo con la confirmación de compra 50% contra entrega - instalado	
Garantía:	Los equipos ofertados tienen una garantía de 12 meses contra defectos de manufactura Excepto el gas FM200 como tal, daños por manejo inadecuado ó descargas fortuitas no estan cubiertas por la garantía Se entregará los manuales de operación del equipo y se desarrollará un plan de capacitación y entrenamiento para el personal responsable sobre la operación y la interpretación de alarmas	
Validez Oferta:	15 días a partir de la presente fecha	
SERVICIOS DE VALOR AGREGADO		
Representación	Somos representantes exclusivos de las marcas ofertadas y por tanto ofrecemos la garantía de fábrica. Contamos con personal entrenado y respuestos y partes de disponibilidad local.	
Entrenamiento :	Se proveerá el entrenamiento al personal que se designe en la operación de los equipos, interpretación de alarmas y acciones a tomar.	
Repuestos	Se cuenta con un stock de repuestos y partes originales de Fabrica localmente	
Experiencia :	Nuestra Empresa desde 1984 ha ejecutado el montaje y remodelación completa de grandes centros de cómputo del país para empresas como : Banco del Pacífico, Telefónica Móvil, ETAPA, EMAPQ, Repsol YPF, IMPSAT, AccessRam, UniBanco, CFN, Alegro PCS, Mobil, Texaco, IBM, Petroecuador, Produbanco, FAE, PORTA, MI COMISARIATO , Pronaca, Nestle, DHL, etc.	
Requerimientos de Instalación:	Sistema de Detección y Extinción Automática de Incendios: FM-200 : Una semana después del arribo de los equipos al lugar de ubicación final Aire Acondicionado : La instalación incluye el montaje del evaporador y condensador, la conexión de tuberías, de refrigerante, redes eléctricas y de agua y puesta en marcha.	

Tabla 3.29c: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (3 de 4)



	COMPañIA : CIUDAD : Quito REFERENCIA : Proyecto para Infraestructura Centro de Cómputo E-mail : josejavier_orozco@hotmail.com	ATENCIÓN : Sr. Javier Orozco TELÉFONO : 2347-758 FECHA : Noviembre, 08 del 2008 No. OFERTA :
	OFERTA ECONOMICA	
Atrasos	<p>PROTECOMPU C.A no será responsable económica o jurídicamente por daños o perjuicios que se pudiesen ocasionar por retrasos en la entrega y puesta en marcha de equipos motivo de importación que, por razones de fuerza mayor, caso fortuito o demoras imputables a empresas de transporte que debido a nuevas medidas de seguridad no acepten el transporte de cargas denominadas peligrosas, por demoras de las empresas verificadoras en puerto, por fallas demostrables en empresas de transporte que consolidan carga, por demoras inherentes a la Corporación Aduanera Ecuatoriana CAE en sus procesos de interpretación de aranceles y desaduanización y en general por retrasos que no son del control directo del vendedor, incluyendo desastres naturales, actos de gobierno o de la administración de sus agencias, pérdida de energía, incendios, inundaciones, disputas laborales, huelgas, actos de guerra o recortes/escasez de transporte y materiales. Las entregas en los bienes en caso de estar supeditadas o suspendidas por las razones antes mencionadas, deberán quedar por escrito y debidamente justificados por el vendedor al comprador y la entrega se efectuará en el menor tiempo posible una vez solucionado el motivo de la demora.</p>	
Propiedad	<p>Protecompu se reserva el derecho de posesión de los bienes contratados, hasta tanto y dentro de un plazo no mayor a dos meses de la fecha de entrega física de los bienes, el comprador cancele la totalidad de los bienes adquiridos y recibidos. Luego del plazo indicado, el vendedor además de mantener el derecho de posesión sobre los bienes, cobrará al comprador sobre el saldo de pago, la tasa de interés máxima del mercado financiero vigente, sin que ello lo exonere de retirar los bienes luego de un plazo prudencial.</p>	
PROTECOMPU C.A. Eco. Jorge Rodríguez Gerente Comercial		

Tabla 3.29d: Cotización de Seguridad, Sistema de Ventilación y Control de Incendios (4 de 4)



OFERTA ECONÓMICA - EQUIPOS

ATENCION:	Sr. Jose Orozco	Fecha:	08-Dec-2008
CLIENTE:	Sr. Jose Orozco	Páginas:	1

ITEM	DESCRIPCIÓN	CANT.	PRECIO UNITARIO US\$	PRECIO TOTAL US\$
EQUIPOS ACTIVOS				
WS-C2960-48TC-L	Catalyst 2960 48 10/100 + 2 T/SFP LAN Base Image	7	\$3,024.87	\$21,174.09
WS-C2960-24TC-L	Catalyst 2960 24 10/100 + 2T/SFP LAN Base Image	3	\$1,878.99	\$5,036.96
GLC-SX-MM	GE SFP, LC connector SX transceiver	62	\$336.47	\$27,590.59
WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)	2	\$336.47	\$672.94
			\$0.00	\$0.00
WS-C6506-E	Catalyst 6500 Enhanced 6-slot chassis, 12RU, no PS, no Fan Tray	2	\$3,701.18	\$7,402.35
S7331SK3-12233SXH	Cisco CAT6000-SUP720 IOS IP SERVICES SSH	2	\$0.00	\$0.00
WS-SUP720-3BXL	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric M3FC3 PFC3BXL	2	\$26,917.65	\$53,835.29
CF-ADAPTER-SP	SP adapter with compact flash for SUP720	2	\$0.00	\$0.00
WS-X6148-GE-TX	Catalyst 6500 48-port 10/100/1000 GE Mod., RJ-45	2	\$5,047.06	\$10,094.12
WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFPs)	2	\$10,094.12	\$20,188.24
GLC-SX-MM	GE SFP, LC connector SX transceiver	48	\$336.47	\$16,180.59
WS-C6506-E-FAN	Catalyst 6506-E Chassis Fan Tray	2	\$333.11	\$666.21
WS-CAC-3000W	Catalyst 6500 3000W AC power supply	2	\$2,018.82	\$4,037.65
CAB-7513AC	AC POWER CORD NORTH AMERICA (110V)	2	\$0.00	\$0.00
MEM-C6K-CPTFL512M	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	2	\$0.00	\$0.00
BF-S720-64MB-RP	Bootflash for SUP720-64MB-RP	2	\$0.00	\$0.00
CON-SNTE-WS-C6506	8x8x4 Service Catalyst 6506	2	\$5,379.49	\$10,758.98
SUBTOTAL SIN IVA				\$ 177,608.02
CABLEADO ESTRUCTURADO				
S/N	Cable UTP Sólido de 4 pares cat 5 E	2680	\$0.50	\$1,440.00
S/N	Organizadores Horizontal (1U)	8	\$13.75	\$110.00
S/N	Organizadores Horizontales (2U)	53	\$15.00	\$795.00
S/N	Patch panel 24 Puertos RJ-45 cat 5E	8	\$108.75	\$870.00
S/N	Patch panel 48 Puertos RJ-45 cat 5E	73	\$166.24	\$12,135.34
S/N	Multitomas (8 Tomacorrientes)	23	\$36.88	\$848.13
S/N	Patch cord de fibra optica multimodo SC a SC de 1 metro	4	\$15.50	\$62.00
S/N	Patch cord de fibra optica multimodo SC a MT-RJ de 1 metro	4	\$19.50	\$78.00
S/N	Patch cord de fibra optica multimodo SC a LC de 1 metro	68	\$19.50	\$1,326.00
S/N	Patch cord de fibra optica multimodo LC a LC de 1 metro	2	\$19.50	\$39.00
S/N	Patch cord cat 5E de 3 pies	2680	\$4.38	\$11,725.00
S/N	Pigtails SC de 1 metro	304	\$8.50	\$2,584.00
S/N	Fibra Optica Multimodo de 4 hilos	1060	\$3.50	\$3,710.00
S/N	Rack de 48 UR	2	\$612.50	\$1,225.00
S/N	Gabinete abatible de pared	19	\$360.00	\$6,840.00
S/N	ODF bandeja de FO deslizable 24 - 96 puntos	2	\$485.00	\$970.00
S/N	Placa Adaptadora SC X 8 F.O. NEGRO	12	\$83.75	\$1,005.00
SUBTOTAL SIN IVA				\$ 45,762.46
TOTAL SIN IVA				\$ 223,370.48

Atentamente,

Ing. Gerardo Trujillo
Responsable
ANDEANTRADE

Tabla 3.30: Cotización de Equipos Activos y Cableado Estructurado (Andean Trade)

Fecha: 12-dio-08
 Cliente: José Javier Orozco
 Descripción: COTIZACIÓN CABLEADO ESTRUCTURADO
 Responsable: FC

Cotización para Venta

Número de parte	Descripción	Cantidad	Precio Unitario	Precio Total	
SOLUCIONES/NOTAS					
WS-C2960-48TC-L	Catalyst 2960 48 10/100 + 2 T/SFP LAN Base Image	7	\$ 2,963.73	\$ 20,746.13	
WS-C2960-24TC-L	Catalyst 2960 24 10/100 + 2T/SFP LAN Base Image	3	\$ 1,645.05	\$ 4,935.16	
GLC-SX-MM	GE SFP, LC connector SX Transceiver	32	\$ 329.67	\$ 27,092.94	
WS-G5484	100GBASE-SX Short Wavelength GBIC (Multimode only)	2	\$ 329.67	\$ 659.34	
WS-C8506-E	Catalyst 6500 Enhanced 6-slot chassis, 12RU, no PS, no Fan Tray	2	\$ 3,628.37	\$ 7,256.74	
87338K0-T2233SAH	Cisco CAT8000-SUP720 IOS IP SERVICES SSH	2	\$ -	\$ -	
WS-SUP720-3BXL	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric M8FC3 PFC3BXL	2	\$ 26,373.60	\$ 52,747.20	
CF-ADAPTER-SP	SP adapter with compact flash for SUP72	2	\$ -	\$ -	
WS-X8148-GE-TX	Catalyst 6500 48-port 10/100/1000 GE Mod., RJ-45	2	\$ 4,945.05	\$ 9,890.10	
WS-C8506-E-FAN	Catalyst 6500-E Chassis Fan Tray	2	\$ 328.37	\$ 656.75	
WS-CAC-3000W	Catalyst 6500 3000W AC power supply	2	\$ 1,978.02	\$ 3,956.04	
CAB-7613AC	AC POWER CORD NORTH AMERICA (110V)	2	\$ -	\$ -	
MEM-C8K-CPTFL512M	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	2	\$ -	\$ -	
BF-S720-64MB-RP	Bootflash for SUP720-64MB-RP	2	\$ -	\$ -	
WS-X8724-SFP+	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFP+)	2	\$ 9,890.10	\$ 19,780.20	
CON-SNTE-WS-C8506	Serial Service, Catalyst 6506	2	\$ 8,918.31	\$ 17,836.61	
CABLEADO					
	UTP CABLE 5E SOLIDO SIEMON	2880	\$ 0.44	\$ 1,267.20	
	ORGANIZADOR HORIZONTAL METAL 1UR	8	\$ 13.50	\$ 108.00	
	ORGANIZADOR HORIZONTAL 2RMSX19"	33	\$ 25.30	\$ 1,340.90	
	PATCH PANE 24 PTOS 5E SOLID SMN	8	\$ 145.20	\$ 1,161.60	
	PATCH PANEL 48 PTOS MOD. 2RMS HUBELL	73	\$ 211.00	\$ 15,403.00	
	MULTITOMA 19" 10 PTOS. HORIZONTAL	23	\$ 58.32	\$ 1,355.36	
	Patch cord de fibra optica multimodo SC a SC de 1 metro	4	\$ 12.74	\$ 50.96	
	Patch cord de fibra optica multimodo SC a LC de 1 metro	68	\$ 17.99	\$ 1,223.32	
	Patch cord de fibra optica multimodo LC a LC de 1 metro	2	\$ 17.43	\$ 34.86	
	Patch cord de fibra optica multimodo SC a MT-RJ de 1 metro	4	\$ 18.60	\$ 74.40	
	PATCH cord Cat. 5E 3FT, azul.	2680	\$ 4.14	\$ 11,095.20	
	Pigtail SC de 1 metro	304	\$ 4.25	\$ 1,292.00	
	SF 30T25 Multimode Y-Buffer Distribution	1060	\$ 3.45	\$ 3,657.00	
GF-2130	GABIN. PISO 7' 19"X 24" 45 RMS ESTRUC. Y TAPAS C.R. NEGRO	2	\$ 977.50	\$ 1,955.00	
	GABINETE ABATIBLE 18 RMS, DIMENSIONES 773 X 525 X 590 mm	19	\$ 375.00	\$ 7,125.00	
AH-FDB-01	Slide in tray based fiber distribution box (4 tray 12 ports installed)	2	\$ 160.00	\$ 320.00	
				Subtotal	\$ 212,893.01
				12% IVA	\$ 25,547.16
				Total	\$ 238,440.17

Condiciones	
Tiempo de Entrega:	Equipos CISCO: 45 dias, Cableado Estructurado: inmediato previa confirmación de stock
Garantía:	CISCO: 90 dias por defectos de fábrica, CABLEADO ESTRUCTURADO: 1 año
Válidez de la oferta:	15 dias
Clasificación:	N.A.
Abr:	Francisco Cordova

Atestado:

 Francisco Cordova
 Gerente General
fcordova@totaltek.com.ec

Tabla 3.31: Cotización de Equipos Activos y Cableado Estructurado (TOTALTEK)

Capítulo 4

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- La adopción de seguridades físicas en los predios del Cuarto de Telecomunicaciones impedirá que personas no autorizadas accedan a los dispositivos de conmutación para alterar su configuración o apropiarse de datos confidenciales o peor aun poner en riesgo su integridad física (robo o atentados).
- El reemplazo del cableado vertical existente por fibra óptica multimodo mejorará notablemente la velocidad de transmisión de la información en la red, ya que este medio no se ve afectado por interferencia electromagnética o de radio frecuencia, además de soportar mayores anchos de banda y garantizar el crecimiento futuro.
- Un etiquetamiento correctamente planificado tanto para elementos activos como pasivos facilitará la documentación de procesos, resolución de problemas e instalaciones futuras.
- El modelo jerárquico planteado simplificará la agregación de nuevos segmentos, ya que los parámetros pueden ser replicados con ligeras modificaciones y sin causar interrupción alguna, dicho de otra manera, el diseño jerárquico debe ser además modular para garantizar un crecimiento ordenado y sin traumas.
- La elección del conmutador modular Cisco Catalyst 6506 para la Capa de Core/Distribución permitirá el crecimiento de la red tanto en número de usuarios como en servicios ofrecidos sin reducir el rendimiento, garantizando además la posibilidad de crecimiento con módulos que ofrezcan servicios adicionales como IDS/IPS (Intrusion Detection System/Intrusion Prevention System), NAM

(Network Analysis Module), WLC (Wireless LAN Controller), VSS (Virtual Switching System), etc.

- Recurriendo a la tecnología de agrupación de puertos (EtherChannel) será posible incrementar la capacidad de transmisión entre dispositivos, garantizar la disponibilidad y aprovechar los recursos existentes.
- La creación de VLANs (Virtual Local Area Networks) contribuirá a reducir el tamaño de los dominios de broadcast y por ende la retransmisión de paquetes en segmentos donde no se requiere procesar información destinada a otros usuarios.
- Utilizando el mecanismo denominado seguridad de puerto será posible regular el acceso a la red y disminuir la probabilidad de que un intruso intercepte, modifique, falsifique o interrumpa la comunicación.
- Mediante HSRP (Hot Standby Router Protocol) se logrará que los equipos de Core/Distribución aparezcan como una sola entidad (Puerta de Enlace) y el tráfico generado en las distintas redes virtuales pueda ser balanceado, además de ofrecer alta disponibilidad de presencia de la Puerta de Enlace para las estaciones de trabajo y servidores.
- Con la ayuda de un programa de gestión, el grupo de profesionales técnicos responsables del funcionamiento de la red dispondrá de herramientas suficientes para controlar los dispositivos y detectar cualquier eventualidad, permitiendo actuar proactivamente ante las fallas.

4.2 Recomendaciones

- Es esencial instalar un sistema de energía eléctrica desde la acometida principal, un regulador de transientes y una fuente de alimentación auxiliar para proteger los equipos que alberga el Cuarto de Telecomunicaciones. En lo posible un Cuarto de Telecomunicaciones debe tener dos circuitos eléctricos independientes para ser conectados a las fuentes redundantes.
- Aunque en la nueva topología se conservan los equipos Cisco Catalyst 3500, es aconsejable sustituirlos en el corto plazo, debido a que el fabricante ha suspendido su producción y tienen ciertas limitaciones en cuanto se refiere a soporte técnico, administración y compatibilidad.
- Es fuertemente recomendable mantener la uniformidad respecto a la versión del sistema operativo que los conmutadores utilicen y realizar actualizaciones periódicas, por ejemplo de manera trimestral.
- Una forma de controlar todos los dispositivos instalados en el edificio, incluyendo aquellos que operan en el Ala Oriental del cuarto piso donde funciona TERMOPICHINCHA, sería aprovechar la funcionalidad de VTP (VLAN Trunking Protocol) y establecer el modo de operación del conmutador en Transparente para que las dos redes sean independientes. De esta manera, se integra toda la red para futuras necesidades, manteniendo su independencia actual desde el punto de vista lógico.
- En la propuesta de diseño, la configuración de STP (Spanning Tree Protocol) permite controlar grupos de VLANs y eliminar los lazos de manera efectiva. Sin embargo, una alternativa más poderosa como MSTP (Multiple Spanning Tree Protocol) debe ser tomada en cuenta.
- A pesar de que la central telefónica SIEMENS HiPath 4500 continuará manejando las extensiones y líneas urbanas análogas, se recomienda incorporar un esquema de VoIP (Voice over IP) con equipos y accesorios Cisco, si bien la marca no es

determinante, ya que solamente serán necesarios algunos cambios en la configuración de los conmutadores para priorizar el tráfico de voz y conseguir un funcionamiento óptimo. Esta solución además tiene la ventaja de reducir el cableado necesario y poner toda la infraestructura de comunicaciones en manos de un solo grupo técnico.

- La elaboración de reportes de disponibilidad, tiempo de falla e identificación de ataques informáticos debe ser parte de las actividades encomendadas al equipo de profesionales encargados de monitorear el funcionamiento de la red.
- Para asegurar que la restitución del servicio en caso de ocurrir una falla crítica se lleve a cabo en el menor tiempo posible y reduciendo el impacto causado por la indisponibilidad, es importante considerar la adquisición del paquete SMARTnet que ofrece Cisco para los conmutadores principales, el cual supone la reposición de piezas en falla en plazos muy cortos, con disponibilidad local garantizada de los equipos y partes protegidos por el contrato.
- Dada la necesidad de movilidad experimentada por gran parte de los colaboradores de la Compañía, se sugiere instalar un módulo WLC (Wireless LAN Controller) y los respectivos APs (Access Points) para procurar una red de datos inalámbrica en el edificio que debe ser implementada tomando en cuenta factores de seguridad, integridad y confidencialidad de los datos.
- Con el objeto de salvaguardar la integridad de los datos que circulan por la red y reconocer vulnerabilidades que pretendan ser explotadas, es conveniente instalar un IDS (Intrusion Detection System).

BIBLIOGRAFIA

Cisco Catalyst 6500 Series Mixed Media Gigabit Ethernet Modules. Cisco Systems Inc. 14 de Diciembre de 2008 <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/product_data_sheet0900aecd801459a7.pdf>.

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules. Cisco Systems, Inc. 14 de Diciembre de 2008 <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/product_data_sheet0900aecd8017376e.pdf>.

Cisco Catalyst 6500/Cisco 7600 Series Supervisor Engine 720. Cisco Systems, Inc. 14 de Diciembre de 2008 <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/product_data_sheet09186a0080159856.pdf>.

Cisco Catalyst 6500 and 6500-E Series Switch. Cisco Systems, Inc. 14 de Diciembre de 2008 <http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916.pdf>.

Cisco Catalyst 2960 Series Switches with LAN Base Software. Cisco Systems, Inc. 14 de Diciembre de 2008 <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.pdf>.

Cisco IOS Password Encryption Facts. Document ID: 107614. Updated: Jul 22, 2008. 14 de Diciembre de 2008 <<http://www.cisco.com/application/pdf/paws/107614/64.pdf>>.

Cisco Networking Academy Program. CCNA 1: Networking Basics v3.0 - Structured Cabling Supplement, 2003.

Cisco Networking Academy. CCNA Exploration 4.0: Network Fundamentals, 2007.

Cisco Networking Academy. CCNA Exploration 4.0: Routing Protocols and Concepts, 2007.

Cisco Networking Academy. CCNA Exploration 4.0: LAN Switching and Wireless, 2007.

Cisco Networking Academy Program: Fundamentals of Voice and Data Cabling. Indianapolis: Cisco Press, 2003.

Hecht, Jeff. *Understanding Fiber Optics*. Indianapolis: SAMS Publishing, 1993.

How LAN Switches Work. Document ID: 10607. Updated: Aug 01, 2007. 14 de Diciembre de 2008 <<http://www.cisco.com/warp/public/473/lan-switch-cisco.pdf>>.

Hucaby, David. *CCNP Self-Study: CCNP BCMSN Exam Certification Guide*. Indianapolis: Cisco Press, 2005.

Kurose, James F., and Keith W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. United States of America: Pearson Education, 2005.

Manual de Inducción General 2007. TRANSELECTRIC S.A.

Morris, Stephen B. *Network Management, MIBS and MPLS: Principles, Design and Implementation*. New Jersey: Prentice Hall, 2003.

Plan Estratégico 2008-2012. TRANSELECTRIC S.A.

Portafolio de Telecomunicaciones. TRANSELECTRIC S.A. 14 de Diciembre de 2008 <http://www.transelectric.com.ec/transelectric_portal/portal/main.do?sectionCode=29>.

Presentación Visita alumnos de la USFQ. TRANSELECTRIC S.A., Junio 2008.

So-In, Chakchai. *Examples of Traffic Analysis Tools: A Survey of Network Traffic Monitoring and Analysis Tools*. Updated: December 03, 2006. 14 de Diciembre de 2008 <<http://www.cs.wustl.edu/~cs5/567/traffic/index.html>>.

Stallings, William. *Wireless Communications & Networks*. New Jersey: Prentice Hall, 2005.

Why Use Cisco Network Systems?. 14 de Diciembre de 2008 <http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns431/ns725/networking_solution_solution_overview0900aecd8063f786.pdf>.