

# ESCUELA SUPERIOR POLITECNICA DEL LITORAL



## Escuela de Diseño y Comunicación Visual

### TÓPICO DE GRADUACIÓN

Previo a la obtención del Título de  
Analista de Soporte de Microcomputadores

#### **T e m a :**

Administración y Seguridad de Redes  
EPSILUM S.A.

#### **Manual de Usuario y Configuraciones**

#### **A u t o r e s :**

Mayra Alexandra Sumba Chávez  
Dennys Fernanda Zambrano Moreno  
Angel Enrique Orellana Granda

#### **D I R E C T O R :**

Anl. Fabián Barboza

**A ñ o 2 0 0 7**



**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**



**ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL**

**TÓPICO DE GRADUACIÓN**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE:**

**ANALISTA DE SOPORTE DE MICROCOMPUTADORES**

**TEMA**

**ADMINISTRACIÓN Y SEGURIDAD DE REDES**

**EPSILUM S.A.**

**MANUAL DE USUARIO Y CONFIGURACIONES**

**AUTORES**

**MAYRA ALEXANDRA SUMBA CHAVEZ  
DENNY FERNANDA ZAMBRANO MORENO  
ANGEL ENRIQUE ORELLANA GRANDA**

**DIRECTOR**

**ANL. FABIÁN BARBOZA**

**AÑO**

**2007**

## **AGRADECIMIENTO**

*Gracias a Dios que nos dio la fortaleza y el valor para perseguir todos y cada uno de nuestros anhelos.*

*Gracias a las autoridades y a los docentes de la Escuela Superior Politécnica del Litoral que se preocuparon no solo por nuestra formación académica sino por impartir una educación integral, capaz de forjar un ser humano superior.*

*Gracias a nuestros padres que supieron comprendernos y apoyarnos en nuestra misión como estudiantes creando los medios necesarios para enfrentar la vida con éxito y eficiencia personal, a ellos va dedicado nuestro agradecimiento y todo nuestro esfuerzo.*

*Gracias a los compañeros que nos permitieron forjar nuestro carácter y nuestro espíritu en la convivencia diaria por nuestra superación, fortaleciendo los supremos valores de la vida y fomentando las virtudes humanas del respeto, amistad, compañerismo, solidaridad y amor a la humanidad.*

## **DEDICATORIA**

*El conocimiento es el mayor poder con que cuenta el ser humano y la educación es la mejor herencia que los padres pueden dejar a sus hijos, estamos conscientes de que alcanzar esta meta no ha sido tarea fácil, ha requerido de sacrificio, concentración y perseverancia, por esta razón, dedicamos este trabajo al ser Divino quién nos ha dado la fuerza y la constancia para poder alcanzar esta meta y seguir adelante, a nuestros padres que nos han apoyado en todo el transcurso de nuestra carrera universitaria, a nuestros compañeros y amigos que estuvieron siempre con nosotros en el desarrollo de este tópico.*

## **DECLARACIÓN EXPRESA**

*La responsabilidad de los hechos, ideas y doctrinas expuestas en este tópico de graduación nos corresponde exclusivamente; y el patrimonio intelectual de la misma, a EDCOM (**Escuela de Diseño y Comunicación Visual**) de la Escuela Superior Politécnica del Litoral.*

*(Reglamento de exámenes y títulos profesionales de la ESPOL).*

**FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN**



Ant. Fabián Barboza

**FIRMA DE LOS AUTORES DEL TÓPICO DE  
GRADUACIÓN**

  
Mayra Alexandra Sumba Chavez

  
Dennys Fernanda Zambrano Moreno

  
Angel Enrique Orellana Granda





# TABLA DE CONTENIDO

## CAPÍTULO 1

<b>1. GENERALIDADES</b>	<b>1</b>
1.1 INTRODUCCIÓN	1
1.2 OBJETIVO DE ESTE MANUAL	1
1.3 A QUIÉN VA DIRIGIDO ESTE MANUAL	1
1.4 LO QUE SE DEBE CONOCER	2
1.5 ORGANIZACIÓN DE ESTE MANUAL	2
1.6 ACERCA DE ESTE MANUAL	2

## CAPÍTULO 2

<b>2. SITUACIÓN ACTUAL</b>	<b>1</b>
2.1 ANTECEDENTES DE LA EMPRESA	1
2.1.1 ANTECEDENTES GENERALES	1
2.1.2 INFORMACIÓN GENERAL	2
2.1.3 MISIÓN	2
2.1.4 VISIÓN	2
2.1.5 OBJETIVOS GENERALES DE LA EMPRESA	2
2.1.6 OBJETIVOS OPERATIVOS DE LA EMPRESA	3
2.1.7 DEPARTAMENTOS DE LA EMPRESA	4
2.1.7.1 MATRIZ	4
2.1.7.2 SUCURSAL # 1 (AMBATO)	7
2.1.7.3 SUCURSAL # 2 (LOJA)	9
2.2 INFRAESTRUCTURA LAN	11
2.2.1 ESTACIONES DE TRABAJO	11
2.2.1.1 MATRIZ	12
2.2.1.2 SUCURSAL: AMBATO	21
2.2.1.3 SUCURSAL: LOJA	26
2.2.2 SERVIDORES	30
2.2.2.1 MATRIZ	30
2.2.2.2 SUCURSAL: AMBATO	31
2.2.2.3 SUCURSAL: LOJA	31
2.2.3 ANÁLISIS DE PISO	32
2.2.3.1 MATRIZ	32
2.2.3.2 SUCURSALES: AMBATO y LOJA	34
2.2.4 ANÁLISIS DE PISO LÓGICO	35
2.2.4.1 MATRIZ PLANTA BAJA	35
2.2.4.2 MATRIZ PLANTA ALTA	36
2.2.4.3 AMBATO	37
2.2.4.4 LOJA	38
2.2.5 ANÁLISIS DE PISO APLICATIVO	39
2.2.5.1 MATRIZ PLANTA BAJA	39
2.2.5.2 MATRIZ PLANTA ALTA	40
2.2.5.3 AMBATO	41
2.2.5.4 LOJA	42

2.2.6	MC	43
2.2.6.1	MATRIZ	43
2.2.6.2	GRÁFICO DEL MC	44
2.2.6.3	SUCURSALES: AMBATO y LOJA	45
2.2.7	MEDIOS DE COMUNICACIÓN	46
2.2.7.1	MEDIOS ALÁMBRICOS	46
2.2.7.1.1	MATRIZ y SUCURSALES	46
2.2.8	DISPOSITIVOS DE CONMUTACIÓN	47
2.2.8.1	MATRIZ	47
2.2.8.2	AMBATO	47
2.2.8.3	LOJA	48
<b>2.3</b>	<b>INFRAESTRUCTURA WAN</b>	<b>49</b>
2.3.1	COMUNICACIÓN MATRIZ Y SUCURSALES	49
2.3.1.1	MATRIZ GUAYAQUIL:	49
2.3.1.2	SUCURSAL 1.- LOJA	50
2.3.1.3	SUCURSAL 2.- AMBATO	50
2.3.2	DISPOSITIVOS DE ENRUTAMIENTO	52
2.3.2.1	COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS	53
2.3.3	MEDIOS DE COMUNICACIÓN:	54
2.3.3.1	MEDIOS INALÁMBRICOS	54
2.3.3.1.1	COMUNICACIÓN WAN A NIVEL DE MEDIOS	55
2.3.3.2	INFRAESTRUCTURA DE TELECOMUNICACIONES	56
<b>2.4</b>	<b>SEGURIDADES</b>	<b>58</b>
2.4.1	EDIFICIO MATRIZ Y SUCURSALES	58
2.4.2	NIVEL DE SEGURIDAD - EDIFICIO MATRIZ	60
2.4.3	NIVEL DE SEGURIDAD.- SUCURSALES AMBATO Y LOJA	61
<b>2.5</b>	<b>INTERNET</b>	<b>62</b>
2.5.1	ACCESO A INTERNET Y ANCHO DE BANDA	62
<b>2.6</b>	<b>PROBLEMAS ENCONTRADOS</b>	<b>63</b>

## CAPÍTULO 3

<b>3.</b>	<b>PROPUESTA</b>	<b>1</b>
3.1	PROBLEMAS ENCONTRADOS	1
3.2	SOLUCIÓN PROPUESTA	3
3.3	ESTUDIOS DE FACTIBILIDAD	5
3.3.1	ALTERNATIVA: A	5
3.3.1.1	FACTIBILIDAD TÉCNICA	5
3.3.1.1.1	DISPOSITIVOS DE ENRUTAMIENTO	5
3.3.1.1.2	DISPOSITIVOS DE CONMUTACIÓN	6
3.3.1.1.3	MEDIOS DE COMUNICACIÓN	6
3.3.1.1.4	EQUIPOS	6
3.3.1.1.5	CABLEADO ESTRUCTURADO	7
3.3.1.2	FACTIBILIDAD ECONÓMICA	8
3.3.1.2.1	COSTOS DE HARDWARE	8
3.3.1.2.2	COSTOS DE SOFTWARE	9
3.3.1.2.3	COSTOS DEL ENLACE DE DATOS	9
3.3.1.2.4	COSTOS OPERATIVOS	9
3.3.1.2.5	COSTO TOTAL DE LA PROPUESTA	10
3.3.1.3	FACTIBILIDAD OPERATIVA	10
3.3.1.4	FORMA DE PAGO Y TIEMPO DE DESARROLLO	11
3.3.1.5	VENTAJAS Y BENEFICIOS	11

3.3.1.5.1	VENTAJAS	11
3.3.1.5.2	BENEFICIOS	11
3.3.1.6	GARANTÍAS	12
3.3.2	ALTERNATIVA: B	14
3.3.2.1	FACTIBILIDAD TÉCNICA	14
3.3.2.1.1	DISPOSITIVOS DE ENRUTAMIENTO	14
3.3.2.1.2	DISPOSITIVOS DE CONMUTACIÓN	15
3.3.2.1.3	MEDIOS DE COMUNICACIÓN	15
3.3.2.1.4	EQUIPOS	15
3.3.2.1.5	CABLEADO ESTRUCTURADO	16
3.3.2.2	FACTIBILIDAD ECONÓMICA	17
3.3.2.2.1	COSTOS DE HARDWARE	17
3.3.2.2.2	COSTOS DE SOFTWARE	18
3.3.2.2.3	COSTOS DEL ENLACE DE DATOS	18
3.3.2.2.4	COSTOS OPERATIVOS	18
3.3.2.2.5	COSTO TOTAL DE LA PROPUESTA	19
3.3.2.3	FACTIBILIDAD OPERATIVA	19
3.3.2.4	FORMA DE PAGO Y TIEMPO DE DESARROLLO	20
3.3.2.5	VENTAJAS Y BENEFICIOS	20
3.3.2.5.1	VENTAJAS	20
3.3.2.5.2	BENEFICIOS	20
3.3.2.6	GARANTÍAS	21
<b>3.4</b>	<b>CONCLUSIONES</b>	<b>23</b>

## CAPÍTULO 4

<b>4.</b>	<b>IMPLEMENTACIÓN LAN Y WAN</b>	<b>1</b>
<b>4.1.</b>	<b>INFRAESTRUCTURA LAN</b>	<b>1</b>
4.1.1.	UBICACIÓN DEL EDIFICIO MATRIZ	1
4.1.2.	EDIFICIO MATRIZ.- CABLEADO INTRA-EDIFICIO	2
4.1.3.	SUCURSAL AMBATO.- CABLEADO INTRA-EDIFICIO	3
4.1.4.	SUCURSAL LOJA.- CABLEADO INTRA-EDIFICIO	4
4.1.5.	ANÁLISIS DE PISO LÓGICO	5
4.1.5.1.	MATRIZ PLANTA BAJA	5
4.1.5.2.	MATRIZ PLANTA ALTA	6
4.1.5.3.	SUCURSAL AMBATO	7
4.1.5.4.	SUCURSAL LOJA	8
4.1.6.	ANÁLISIS DE PISO APLICATIVO	9
4.1.6.1.	MATRIZ PLANTA BAJA	9
4.1.6.2.	MATRIZ PLANTA ALTA	10
4.1.6.3.	AMBATO	11
4.1.6.4.	LOJA	12
4.1.7.	CÁLCULO DEL BACKBONE INTRAEDIFICIO MATRIZ Y SUCURSALES	13
4.1.8.	MC MATRIZ	14
<b>4.2.</b>	<b>INFRAESTRUCTURA WAN</b>	<b>15</b>
4.2.1.	COMUNICACIÓN WAN: MATRIZ - ISP	15
4.2.1.1.	COMUNICACIÓN MAN: MATRIZ Y SUCURSALES	16
4.2.1.2.	COMUNICACIÓN MAN: MATRIZ Y TORRE CENTENARIO	17
4.2.1.3.	COMUNICACIÓN MAN: MATRIZ Y TORRE CEIBOS	18
4.2.1.4.	COMUNICACIÓN MAN: MATRIZ Y TORRE PUERTO AZUL	19
4.2.1.5.	COMUNICACIÓN MAN: MATRIZ Y TORRE SAMBORONDON	20

4.2.2.	COMUNICACIÓN WAN: AMBATO - ISP	21
4.2.2.1.	COMUNICACIÓN MAN: AMBATO Y SUCURSAL	22
4.2.3.	COMUNICACIÓN WAN: LOJA - ISP	23
4.2.3.1.	COMUNICACIÓN MAN: LOJA Y SUCURSAL	24
4.2.4.	COMUNICACIÓN A NIVEL DE DISPOSITIVOS	25
4.2.5.	COMUNICACIÓN A NIVEL DE MEDIOS	26
4.3.	RECEPCIÓN DE INTERNET	27
4.4.	INTRANET	28

## CAPÍTULO 5

5.	NORMATIVAS DE CABLEADO ESTRUCTURADO	1
5.1	NORMATIVA # 1	1
5.2	NORMATIVA # 2	1
5.3	NORMATIVA 3	2
5.3.1	RECOMENDACIÓN 1	2
5.3.2	RECOMENDACIÓN 2	3
5.4	NORMATIVA 4	3
5.4.1	RECOMENDACIÓN 3	4
5.5	NORMATIVA 5	4
5.6	NORMATIVA 6	5
5.6.1	RECOMENDACIÓN 4	5
5.7	NORMATIVA 7	6
5.8	NORMATIVA 8	6
5.8.1	RECOMENDACIÓN 5	7
5.9	NORMATIVA 9	7
5.10	NORMATIVA 10	8
5.11	NORMATIVA 11	8
5.12	NORMATIVA 12	9
5.13	NORMATIVA 13	10
5.14	NORMATIVA 14	10
5.15	NORMATIVA 15	11
5.16	NORMATIVA 16	11
5.17	NORMATIVA 17	12
5.17.1	RECOMENDACIÓN 6	12
5.18	NORMATIVA 18	13
5.18.1	RECOMENDACIÓN 7	13
5.19	NORMATIVA 19	14
5.20	NORMATIVA 20	14
5.21	NORMATIVA 21	15

5.22	NORMATIVA 22	15
5.22.1	RECOMENDACIÓN 8	16
5.23	NORMATIVA 23	16
5.23.1	RECOMENDACIÓN 9	17
5.24	NORMATIVA 24	17
5.25	NORMATIVA 25	18
5.25.1	RECOMENDACIÓN 10	18
5.26	NORMATIVA 26	19
5.26.1	RECOMENDACIÓN 11	20
5.27	NORMATIVA 27	20
5.28	NORMATIVA 28	21
5.29	NORMATIVA 29	21
5.30	NORMATIVA 30	22
5.31	NORMATIVA 31	22
5.32	NORMATIVA 32	23
5.33	NORMATIVA 33	23
5.34	NORMATIVA 34	24
5.34.1	RECOMENDACIÓN 12	24
5.34.2	RECOMENDACIÓN 13	25
5.35	NORMATIVA 35	25
5.36	NORMATIVA 36	26
5.37	NORMATIVA 37	26
5.38	NORMATIVA 38	27
5.39	NORMATIVA 39	27
5.40	NORMATIVA 40	27
5.41	NORMATIVA 41	28
5.42	NORMATIVA 42	28
5.43	NORMATIVA 43	29
5.44	NORMATIVA 44	29
5.45	NORMATIVA 45	30
5.46	NORMATIVA 46	30
5.47	NORMATIVA 47	31
5.48	NORMATIVA 48	31
5.49	NORMATIVA 49	32
5.50	NORMATIVA 50	32
5.51	NORMATIVA 51	33
5.52	NORMATIVA 52	33
5.53	NORMATIVA 53	34
5.54	NORMATIVA 54	34
5.55	NORMATIVA 55	35
5.56	NORMATIVA 56	35
5.57	NORMATIVA 57	36

## CAPÍTULO 6

<b>6.</b>	<b>LINUX</b>	<b>1</b>
6.1	INTRODUCCIÓN	1
6.2	CARACTERÍSTICAS DE LINUX	2
6.3	EL KERNEL	3
6.4	EL SHELL	3
6.5	INSTALACIÓN DE LINUX FEDORA CORE 3	4
6.5.1	REQUERIMIENTOS DE HARDWARE	4
6.5.2	CONFIGURACIÓN DEL BIOS	4
6.5.3	INSTALACIÓN DEL SISTEMA OPERATIVO LINUX	6
6.5.4	CONFIGURACIÓN POST-INSTALACIÓN	18
6.5.5	INICIANDO EL SISTEMA OPERATIVO	20
6.5.5.1	AMBIENTE GRÁFICO	20
6.5.5.2	MODO TEXTO	22
6.6	COMANDOS UNIX-LINUX	23
6.6.1	MANEJO DE CONSOLA	23
6.6.2	VISUALIZACIÓN Y EDICIÓN DE TEXTO	25
6.6.3	COMANDOS DEL EDITOR VI	26
6.6.4	ADMINISTRACIÓN DE ARCHIVOS Y DIRECTORIO	28
6.6.5	MANEJO DE PAQUETES	32
6.6.6	INFORMACIÓN DEL SISTEMA Y MANEJO DE RECURSOS	33
6.6.7	UTILITARIOS BÁSICOS DE BASH	35
6.7	CONFIGURACIÓN DE LA TARJETA DE RED	36
6.7.1	MODO TEXTO	36
6.7.2	MODO GRÁFICO	37
6.8	SERVIDOR DNS	38
6.8.1	ACERCA DE DNS	38
6.8.2	FUNCIONAMIENTO	42
6.8.3	BENEFICIOS DNS	43
6.8.4	REQUERIMIENTOS PARA CONFIGURAR EL SERVIDOR DNS	43
6.8.5	CONFIGURACIÓN DNS:	43
6.8.6	CONFIGURACIÓN EN CLIENTE WINDOWS	48
6.9	SERVIDOR WEB	50
6.9.1	ACERCA DE SERVIDOR WEB	50
6.9.2	ACERCA DEL PROTOCOLO HTTP.	51
6.9.3	ACERCA DE APACHE.	51
6.9.4	CARACTERÍSTICAS DEL SERVIDOR APACHE	52
6.9.5	FUNCIONAMIENTO	52
6.9.6	BENEFICIOS SERVIDOR WEB	53
6.9.7	REQUERIMIENTOS	53
6.9.8	CONFIGURACIÓN DE WEB SERVER:	53
6.9.9	CONFIGURACIÓN EN CLIENTE WINDOWS	56
6.10	SERVIDOR PROXY	59
6.10.1	ACERCA DE PROXY	59
6.10.2	ACERCA DE SQUID.	60
6.10.3	FUNCIONAMIENTO	61
6.10.4	BENEFICIOS DEL SERVIDOR PROXY	61
6.10.5	REQUERIMIENTOS PROXY	61
6.10.6	CONFIGURACIÓN DE PROXY:	62
6.10.7	ACL (ACCESS CONTROL LIST – LISTA DE CONTROL DE ACCESO)	65
6.10.8	CONFIGURACIÓN EN CLIENTE WINDOWS	66

6.10.9	DENEGAR ACCESO POR HORA	69
6.10.10	ACCESO POR AUTENTIFICACIÓN	70
6.10.10.1	CONFIGURACIÓN EN CLIENTE WINDOWS	72
6.10.11	BLOQUEAR PÁGINAS	74
6.10.11.1	CONFIGURACIÓN EN CLIENTE WINDOWS	75
6.10.12	ANCHO DE BANDA	76
6.10.12.1	DEFINICIÓN DE DELAY POOLS	76
6.10.12.2	CLASES DE DELAY POOLS	76
6.10.12.2.1	CLASE 1	76
6.10.12.2.2	CLASE 2	76
6.10.12.2.3	CLASE 3	77
6.10.12.3	PARÁMETROS DEL DELAY POOL	77
6.10.12.4	DELAY_ACCESS	78
<b>6.11</b>	<b>SERVIDOR DE CORREO</b>	<b>79</b>
6.11.1	ACERCA DE SENDMAIL	79
6.11.2	ACERCA DE DOVECOT	79
6.11.3	PROTOCOLOS UTILIZADOS	80
6.11.3.1	SMTP (SIMPLE MAIL TRANSFER PROTOCOL)	80
6.11.3.2	POP3 (POST OFFICE PROTOCOL VERSION 3)	81
6.11.3.3	IMAP (INTERNET MESSAGE ACCESS PROTOCOL)	82
6.11.4	FUNCIONAMIENTO	84
6.11.5	BENEFICIOS SERVIDOR DE CORREO	85
6.11.6	REQUERIMIENTOS SERVIDOR DE CORREO	85
6.11.7	CONFIGURACIÓN DE SENDMAIL	85
6.11.8	CONFIGURACIÓN EN CLIENTE WINDOWS	91
<b>6.12</b>	<b>FIREWALL</b>	<b>97</b>
6.12.1	ACERCA DE FIREWALL	97
6.12.2	FUNCIONAMIENTO DE FIREWALL	97
6.12.3	REQUERIMIENTOS FIREWALL	98
6.12.4	FILTRADO DE PAQUETES	98
6.12.5	COMANDOS IPTABLES	100
6.12.6	PARÁMETROS	101
6.12.7	OPCIONES DEL OBJETIVO	102
6.12.8	CONFIGURACIÓN DE FIREWALLS	103
6.12.8.1	HABILITAR SMTP	104
6.12.8.2	HABILITAR DNS	104
6.12.8.3	HABILITAR HTTP	105
6.12.8.4	HABILITAR POP3	105
6.12.8.5	BLOQUEAR DEMÁS PUERTOS	106
6.12.9	COMPROBACIÓN CLIENTE WINDOWS	107
<b>6.13</b>	<b>MRTG</b>	<b>108</b>
6.13.1	ACERCA DE MRTG	108
6.13.2	REQUERIMIENTOS DE MRTG	108
6.13.3	CONFIGURACIÓN	109

## CAPÍTULO 7

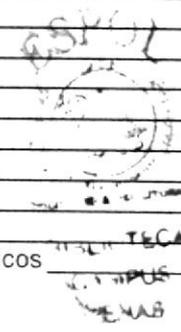
<b>7.</b>	<b>CONFIGURACIÓN DE ROUTERS Y SWITCH</b>	<b>1</b>
7.1	INTRODUCCIÓN A LOS ROUTERS	1
7.2	COMPONENTES INTERNOS DE UN ROUTER	1
7.3	CONEXIONES EXTERNAS DEL ROUTER	4
7.4	CONEXIONES DEL PUERTO DE ADMINISTRACIÓN	4
7.5	CONFIGURACIONES EN EL ROUTER	5
7.5.1	MODOS DE INTERFAZ DE USUARIO	5
7.5.2	CONFIGURACIÓN DEL NOMBRE DE ROUTER	8
7.5.3	CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER	9
7.5.4	AYUDA MEDIANTE EL TECLADO EN LA INTERFAZ DE LÍNEA DE COMANDO	11
7.5.5	DIAGNÓSTICO DE FALLAS DE LOS ERRORES DE LÍNEA DE COMANDOS	12
7.6	USO DE LOS COMANDOS SHOW	13
7.6.1	CONFIGURACIÓN DE UNA INTERFAZ SERIAL	15
7.6.2	CONFIGURACIÓN DE UNA INTERFAZ ETHERNET	18
7.6.3	DESCRIPCIÓN DE INTERFACES	18
7.6.4	CONFIGURACIÓN DEL MENSAJE DEL DIA (MOTD)	19
7.7	CONFIGURACIÓN DE TABLAS DE HOST	20
7.7.1	ENRUTAMIENTO	21
7.7.1.1	ENRUTAMIENTO ESTÁTICO	21
7.7.1.2	ENRUTAMIENTO POR DEFECTO	22
7.7.1.3	ENRUTAMIENTO DINÁMICO	23
7.7.1.3.1	PROTOCOLOS DE ENRUTAMIENTO	23
7.7.1.3.1.1	TIPOS DE PROTOCOLOS DE ENRUTAMIENTO	23
7.7.1.4	PROTOCOLOS DE ENRUTAMIENTO RIP	24
7.7.1.4.1	MEJORAS EN RIP V2	25
7.7.1.5	PROTOCOLOS DE ENRUTAMIENTO DE ESTADO DEL ENLACE	26
7.7.1.5.1	PROTOCOLO DE ENRUTAMIENTO OSPF	26
7.7.1.5.1.1	TIPOS DE RED OSPF	27
7.7.1.5.1.2	PROTOCOLOS HELLO DE OSPF	27
7.7.1.5.1.3	DIRECCIÓN DE LOOPBACK OSPF	29
7.7.1.5.1.4	MODIFICACIÓN DE LA MÉTRICA DE COSTOS DE OSPF	30
7.7.1.5.1.5	CONFIGURACIÓN DE LOS TEMPORIZADORES	31
7.7.1.5.1.6	VERIFICACIÓN DE CONFIGURACIÓN OSPF	31
7.7.2	LISTAS DE CONTROL DE ACCESO (ACL'S)	33
7.7.3	TIPOS DE ACL's	37
7.7.4	FIREWALLS	39
7.8	PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE ROUTERS (EPSILUM)	40
7.8.1	CONEXIÓN DE UNA TERMINAL CON LA CONSOLA DEL ROUTER	40
7.8.2	CONFIGURACIONES EN DISPOSITIVOS DE CONMUTACIÓN Y ENRUTAMIENTO IMPLEMENTADOS	46
7.8.2.1	ROUTER MATRIZ	47
7.8.2.1.1	SHOW RUNNING ROUTER MATRIZ	57
7.8.2.1.2	SHOW IP ROUTE ROUTER MATRIZ	62
7.8.2.2	ROUTER PUERTO AZUL	64
7.8.2.2.1	SHOW RUNNING ROUTER PTO_AZUL	68
7.8.2.2.2	SHOW IP ROUTE ROUTER PTO_AZUL	70
7.8.2.3	ROUTER CEIBOS	72
7.8.2.3.1	SHOW RUNNING ROUTER CEIBOS	76
7.8.2.3.2	SHOW IP ROUTE ROUTER CEIBOS	78

7.8.2.4	ROUTER PUERTO CENTENARIO	80
7.8.2.4.1	SHOW RUNNING ROUTER CENTENARIO	83
7.8.2.4.2	SHOW IP ROUTE ROUTER CENTENARIO	85
7.8.2.5	ROUTER SAMBORONDON	87
7.8.2.5.1	SHOW RUNNING ROUTER SAMBORONDON	91
7.8.2.5.2	SHOW IP ROUTE ROUTER SAMBORONDON	93
7.8.2.6	ROUTER LOJA	95
7.8.2.6.1	SHOW RUNNING ROUTER LOJA	102
7.8.2.6.2	SHOW IP ROUTE ROUTER LOJA	105
7.8.2.7	ROUTER MACARA	107
7.8.2.7.1	SHOW RUNNING ROUTER MACARA	110
7.8.2.7.2	SHOW IP ROUTE ROUTER MACARA	112
7.8.2.8	ROUTER SAN ANTONIO	114
7.8.2.8.1	SHOW RUNNING ROUTER SAN_ANTONIO	117
7.8.2.8.2	SHOW IP ROUTE ROUTER SAN_ANTONIO	119
7.8.2.9	ROUTER AMBATO	121
7.8.2.9.1	SHOW RUNNING ROUTER AMBATO	127
7.8.2.9.2	SHOW IP ROUTE ROUTER AMBATO	130
<b>7.9</b>	<b>INTRODUCCIÓN A LOS SWITCHES</b>	<b>132</b>
7.9.1	INDICADORES LED DEL SWITCH	132
7.9.2	CONECTÁNDOSE AL SWITCH	133
7.9.3	CONFIGURACIÓN DE SWITCHES	133
7.9.4	EXAMINANDO EL COMANDO HELP EN LA CLI DEL SWITCH	136
7.9.5	ASPECTOS BÁSICOS DE LAS VLAN	136
7.9.6	VLAN POR DEFECTO	137
7.9.7	CREACIÓN DE VLAN'S	138
7.9.8	ELIMINANDO VLAN'S	138
7.9.9	ASIGNACIÓN DE VLAN'S A LOS PUERTOS	139
7.9.10	ENRUTAMIENTO ENTRE VLAN	139
7.9.11	INTERFACES FÍSICAS Y LÓGICAS	140
7.9.12	ASIGNAR SWITCH DE TIPO SERVER	141
7.9.13	ENRUTAMIENTO ENTRE DISTINTAS VLAN	141
<b>7.10</b>	<b>PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE SWITCH (EPSILUM)</b>	<b>143</b>
7.10.1	CONEXIÓN DE UNA TERMINAL CON LA CONSOLA DEL SWITCH	143
7.10.2	CONFIGURACIÓN DE SWITCH MATRIZ	149
7.10.3	CONFIGURACIÓN DE SWITCH LOJA	158
7.10.4	CONFIGURACIÓN DE SWITCH AMBATO	165

## TABLA DE ILUSTRACIONES

### CAPÍTULO 2

Figura 2. 1.	Grupo FAUR _____	1
Figura 2. 2.	Departamento de Networking _____	4
Figura 2. 3.	Departamento de Ventas _____	5
Figura 2. 4.	Matriz: Infraestructura Física _____	6
Figura 2. 5.	Departamento de Ventas _____	7
Figura 2. 6.	Ambato: Infraestructura física _____	8
Figura 2. 7.	Jefe del departamento de Networking _____	9
Figura 2. 8.	Loja: Infraestructura física _____	10
Figura 2. 9.	Matriz: Departamento de Gerencia General _____	12
Figura 2. 10.	Matriz: Departamento de Ventas _____	13
Figura 2. 11.	Matriz: Departamento de Desarrollo _____	14
Figura 2. 12.	Matriz: Departamento de Networking _____	15
Figura 2. 13.	Matriz: Departamento de Compras _____	16
Figura 2. 14.	Matriz: Departamento de Cobranzas _____	17
Figura 2. 15.	Matriz: Departamento Técnico _____	18
Figura 2. 16.	Matriz: Gerencia Administrativa _____	19
Figura 2. 17.	Matriz: Departamento de Recepción _____	20
Figura 2. 18.	Ambato: Gerencia Administrativa _____	21
Figura 2. 19.	Ambato: Departamento de Networking _____	22
Figura 2. 20.	Ambato: Departamento Técnico _____	23
Figura 2. 21.	Ambato: Departamento de Ventas _____	24
Figura 2. 22.	Ambato: Departamento de Recepción _____	25
Figura 2. 23.	Loja: Gerencia Administrativa _____	26
Figura 2. 24.	Loja: Departamento de Networking _____	27
Figura 2. 25.	Loja: Departamento de Ventas _____	28
Figura 2. 26.	Loja: Departamento de Recepción _____	29
Figura 2. 27.	Face Plate con su etiqueta respectiva _____	32
Figura 2. 28.	Cableado Horizontal(Terminales) _____	32
Figura 2. 29.	Edificio Matriz.- Cableado Horizontal(Canaletas) _____	33
Figura 2. 30.	Edificio Matriz .- Cañerías eléctricas y de agua _____	33
Figura 2. 31.	Sucursal Ambato.- Cableado Horizontal _____	34
Figura 2. 32.	Matriz planta baja: Análisis de Piso lógico _____	35
Figura 2. 33.	Matriz planta alta: Análisis de Piso lógico _____	36
Figura 2. 34.	Ambato: Análisis de Piso lógico _____	37
Figura 2. 35.	Loja: Análisis de Piso lógico _____	38
Figura 2. 36.	Matriz planta baja: Análisis de Piso aplicativo _____	39
Figura 2. 37.	Matriz planta alta: Análisis de Piso aplicativo _____	40
Figura 2. 38.	Ambato: Análisis de Piso aplicativo _____	41
Figura 2. 39.	Loja: Análisis de Piso aplicativo _____	42
Figura 2. 40.	MC Matriz _____	43
Figura 2. 41.	Gráfico del MC Matriz _____	44
Figura 2. 42.	MC Sucursal Loja y Ambato _____	45
Figura 2. 43.	Infraestructura WAN _____	49
Figura 2. 44.	Infraestructura MAN – Guayaquil _____	49
Figura 2. 45.	Infraestructura MAN – Loja _____	50
Figura 2. 46.	Infraestructura MAN – Ambato _____	50
Figura 2. 47.	Enlace Inter-edificio Epsilum S.A. _____	51
Figura 2. 48.	Comunicación WAN a nivel de dispositivos _____	53
Figura 2. 49.	Comunicación WAN a nivel de medios _____	55
Figura 2. 50.	Torres de Porta _____	56
Figura 2. 51.	Infraestructura de Telecomunicaciones _____	57
Figura 2. 52.	Firewall D-LINK _____	58
Figura 2. 53.	Gráfico de Servidor Linux _____	59
Figura 2. 54.	Edificio Matriz.- Firewalls Físicos y Lógicos _____	60
Figura 2. 55.	Sucursales Ambato y Loja.- Firewalls Físicos y Lógicos _____	61



## CAPÍTULO 3

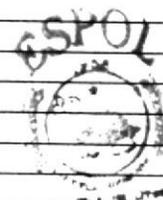
Figura 3.1.	Diagrama Gannt – Alternativa A	13
Figura 3.2.	Diagrama Gannt – Alternativa B	22

## CAPÍTULO 4

Figura 4.1.	Ubicación del Edificio Matriz	1
Figura 4.2.	Edificio Matriz.- Cableado Intra-edificio	2
Figura 4.3.	Sucursal Ambato.- Cableado Intra-edificio	3
Figura 4.4.	Sucursal Loja .- Cableado Intra-edificio	4
Figura 4.5.	Matriz planta baja: Análisis de piso lógico	5
Figura 4.6.	Matriz planta alta: Análisis de piso lógico	6
Figura 4.7.	Ambato: Análisis de piso lógico	7
Figura 4.8.	Loja: Análisis de piso lógico	8
Figura 4.9.	Matriz planta baja: Análisis de piso aplicativo	9
Figura 4.10.	Matriz planta alta: Análisis de piso aplicativo	10
Figura 4.11.	Ambato: Análisis de piso aplicativo	11
Figura 4.12.	Loja: Análisis de piso aplicativo	12
Figura 4.13.	Cálculo del Backbone Intra-edificio	13
Figura 4.14.	Gráfico del MC Matriz	14
Figura 4.15.	Comunicación WAN Matriz - ISP	15
Figura 4.16.	Comunicación MAN: Matriz y sucursales	16
Figura 4.17.	Comunicación MAN: Matriz y Torre Centenario	17
Figura 4.18.	Comunicación MAN: Matriz y Torre Ceibos	18
Figura 4.19.	Comunicación MAN: Matriz y Torre Puerto Azul	19
Figura 4.20.	Comunicación MAN: Matriz y Torre Samborondon	20
Figura 4.21.	Comunicación WAN: Ambato - ISP	21
Figura 4.22.	Comunicación MAN: Ambato y sucursal	22
Figura 4.23.	Comunicación WAN: Loja - ISP	23
Figura 4.24.	Comunicación MAN: Loja y sucursal	24
Figura 4.25.	Comunicación a nivel de dispositivos	25
Figura 4.26.	Comunicación a nivel de medios	26
Figura 4.27.	Recepción de Internet	27
Figura 4.28.	Intranet	28

## CAPÍTULO 5

Figura 5. 1.	Normativa 1	1
Figura 5. 2.	Normativa 2	1
Figura 5. 3.	Normativa 3	2
Figura 5. 4.	Recomendación 1	2
Figura 5. 5.	Recomendación 2	3
Figura 5. 6.	Normativa 4	3
Figura 5. 7.	Recomendación 3	4
Figura 5. 8.	Normativa 5	4
Figura 5. 9.	Normativa 6	5
Figura 5. 10.	Recomendación 4	5
Figura 5. 11.	Normativa 7	6
Figura 5. 12.	Normativa 8	6
Figura 5. 13.	Recomendación 5	7
Figura 5. 14.	Normativa 9	7
Figura 5. 15.	Normativa 10	8
Figura 5. 16.	Normativa 11	8
Figura 5. 17.	Punto de consolidación	9
Figura 5. 18.	Normativa 12	9
Figura 5. 19.	Normativa 13	10
Figura 5. 20.	Normativa 14	10



315LK TECA  
UNIVERSIDAD DE LOJA  
FACULTAD DE INGENIERIA

Figura 5. 21.	Normativa 15	11
Figura 5. 22.	Normativa 16	11
Figura 5. 23.	Normativa 17	12
Figura 5. 24.	Recomendación 6	12
Figura 5. 25.	Normativa 18	13
Figura 5. 26.	Recomendación 7	13
Figura 5. 27.	Normativa 19	14
Figura 5. 28.	Normativa 20	14
Figura 5. 29.	Normativa 21	15
Figura 5. 30.	Normativa 22	15
Figura 5. 31.	Recomendación 8	16
Figura 5. 32.	Normativa 23	16
Figura 5. 33.	Recomendación 9	17
Figura 5. 34.	Normativa 24	17
Figura 5. 35.	Normativa 25	18
Figura 5. 36.	Recomendación 10	18
Figura 5. 37.	Normativa 26	19
Figura 5. 38.	Recomendación 11	20
Figura 5. 39.	Normativa 27	20
Figura 5. 40.	Normativa 28	21
Figura 5. 41.	Normativa 29	21
Figura 5. 42.	Normativa 30	22
Figura 5. 43.	Normativa 31	22
Figura 5. 44.	Normativa 32	23
Figura 5. 45.	Normativa 33	23
Figura 5. 46.	Normativa 34	24
Figura 5. 47.	Recomendación 12	24
Figura 5. 48.	Recomendación 13	25
Figura 5. 49.	Normativa 35	25
Figura 5. 50.	Normativa 36	26
Figura 5. 51.	Normativa 37	26
Figura 5. 52.	Normativa 38	27
Figura 5. 53.	Normativa 39	27
Figura 5. 54.	Normativa 40	27
Figura 5. 55.	Normativa 41	28
Figura 5. 56.	Normativa 42	28
Figura 5. 57.	Normativa 43	29
Figura 5. 58.	Normativa 44	29
Figura 5. 59.	Normativa 45	30
Figura 5. 60.	Normativa 46	30
Figura 5. 61.	Normativa 47	31
Figura 5. 62.	Normativa 48	31
Figura 5. 63.	Normativa 49	32
Figura 5. 64.	Normativa 50	32
Figura 5. 65.	Normativa 51	33
Figura 5. 66.	Normativa 52	33
Figura 5. 67.	Normativa 53	34
Figura 5. 68.	Normativa 54	34
Figura 5. 69.	Normativa 55	35
Figura 5. 70.	Normativa 56	35
Figura 5. 71.	Normativa 57	36



## CAPÍTULO 6

Figura 6. 1.	Funcionamiento del Kernel	3
Figura 6. 2.	Requerimientos mínimos y recomendados para instalación	4
Figura 6. 3.	Pantalla de acceso al BIOS	5
Figura 6. 4.	Pantalla inicial de instalación de Fedora Core 3	6
Figura 6. 5.	Pantalla de bienvenida de la instalación de Fedora Core 3	6
Figura 6. 6.	Pantalla de selección de idioma	7
Figura 6. 7.	Pantalla de configuración del teclado	7
Figura 6. 8.	Pantalla de tipo de instalación	8
Figura 6. 9.	Pantalla: Particionamiento de disco	9
Figura 6. 10.	Pantalla Particionamiento con Disk Druid	10
Figura 6. 11.	Pantalla de partición boot	11
Figura 6. 12.	Pantalla de partición swap	11
Figura 6. 13.	Pantalla de partición root	12
Figura 6. 14.	Pantalla: Partición del disco	12
Figura 6. 15.	Pantalla de partición boot	13
Figura 6. 16.	Pantalla para configurar la tarjeta de red	13
Figura 6. 17.	Pantalla de configuración de red	14
Figura 6. 18.	Pantalla de firewall	14
Figura 6. 19.	Pantalla de selección de idioma	15
Figura 6. 20.	Pantalla de selección de región	15
Figura 6. 21.	Pantalla de asignación de contraseña root	16
Figura 6. 22.	Pantalla de elección de servicios a instalar	16
Figura 6. 23.	Pantalla de inicio de instalación	17
Figura 6. 24.	Pantalla: Instalación completa	17
Figura 6. 25.	Pantalla de acuerdo de licencia	18
Figura 6. 26.	Pantalla de creación de nuevos usuarios	18
Figura 6. 27.	Pantalla de finalización de la instalación	19
Figura 6. 28.	Pantalla de inicio de sesión : ingresando usuario	20
Figura 6. 29.	Pantalla de inicio de sesión : ingresando contraseña	20
Figura 6. 30.	Pantalla de escritorio de Fedora Core 3	21
Figura 6. 31.	Pantalla para Ingresar login	22
Figura 6. 32.	Pantalla ingresando login	22
Figura 6. 33.	Pantalla para ingresar password	22
Figura 6. 34.	Pantalla ingresando password	22
Figura 6. 35.	Pantalla de configuración de la tarjeta de red de ISP (Internet).	36
Figura 6. 36.	Pantalla de configurar la tarjeta de red interna (Intranet).	36
Figura 6. 37.	Pantalla de netconfig	37
Figura 6. 38.	Pantalla de configuración de red	37
Figura 6. 39.	Funcionamiento del Servidor DNS	42
Figura 6. 40.	Pantalla de verificación del paquete bind	43
Figura 6. 41.	Pantalla de configuración del archivo named.conf	44
Figura 6. 42.	Pantalla de iniciar el servicio named	46
Figura 6. 43.	Pantalla de verificar el estatus del servicio named.	47
Figura 6. 44.	Pantalla para realizar ping a www. epsilum.com	47
Figura 6. 45.	Icono de Mis sitios de Red	48
Figura 6. 46.	Pantalla de Mis sitios de Red	48
Figura 6. 47.	Pantalla de Propiedades de Conexión de Área Local	48
Figura 6. 48.	Pantalla: Propiedades de Protocolo Internet (TCP/IP)	49
Figura 6. 49.	Pantalla de realizar ping a epsilum.com	49
Figura 6. 50.	Funcionamiento del Servidor Web	52
Figura 6. 51.	Pantalla para verificar si está instalado el paquete httpd	53
Figura 6. 52.	Pantalla de iniciar el servicio httpd	55
Figura 6. 53.	Pantalla del estatus del servicio httpd	55
Figura 6. 54.	Icono de Internet Explorer	56
Figura 6. 55.	Pantalla para configurar la navegación	56
Figura 6. 56.	Pantalla: Opciones de Internet	56



Figura 6. 57.	Pantalla: Opciones de Internet	57
Figura 6. 58.	Pantalla: Configuración de la Red de Área Local	57
Figura 6. 59.	Pantalla: Página Web de Epsilon	58
Figura 6. 60.	Funcionamiento del Servidor Proxy	61
Figura 6. 61.	Pantalla para verificar si está instalado el paquete squid	62
Figura 6. 62.	Pantalla de configuración de archivo squid.conf	62
Figura 6. 63.	Pantalla para iniciar el servicio squid	64
Figura 6. 64.	Pantalla de status del servicio squid	64
Figura 6. 65.	Icono de Internet Explorer	66
Figura 6. 66.	Pantalla para configurar la navegación	66
Figura 6. 67.	Pantalla: Opciones de Internet	66
Figura 6. 68.	Pantalla Opciones de Internet	67
Figura 6. 69.	Pantalla de configuración de la Red de área local (LAN)	67
Figura 6. 70.	Pantalla: Página accesada por medio de Proxy creada por web server	68
Figura 6. 71.	Icono de Internet Explorer	72
Figura 6. 72.	Pantalla: Autenticación de usuario	72
Figura 6. 73.	Pantalla: Ingresando usuario y contraseña	72
Figura 6. 74.	Pantalla: Accediendo al Internet por medio de autenticación de usuario.	73
Figura 6. 75.	Icono de Internet Explorer	75
Figura 6. 76.	Pantalla de acceso denegado al dominio.	75
Figura 6. 77.	Funcionamiento del Servidor de Correo	84
Figura 6. 78.	Pantalla de configuración de archivo dovecot.conf	85
Figura 6. 79.	Pantalla iniciar el servicio dovecot	86
Figura 6. 80.	Pantalla iniciar el servicio Sendmail	87
Figura 6. 81.	Pantalla iniciar el servicio network	89
Figura 6. 82.	Pantalla envío mail	89
Figura 6. 83.	Pantalla mail enviado	90
Figura 6. 84.	Pantalla configurar cuentas de correo	91
Figura 6. 85.	Pantalla: Cuentas de Internet	91
Figura 6. 86.	Pantalla: Asistente para la conexión a Internet	92
Figura 6. 87.	Pantalla de la dirección de correo.	92
Figura 6. 88.	Pantalla nombre del servidor de correo entrante y saliente.	93
Figura 6. 89.	Pantalla ingreso de usuario y contraseña	93
Figura 6. 90.	Pantalla terminar la configuración	94
Figura 6. 91.	Pantalla comprobación del correo	94
Figura 6. 92.	Pantalla recibiendo correo de otros usuarios	95
Figura 6. 93.	Pantalla de Envío de mensajes	95
Figura 6. 94.	Pantalla enviando correo a otra cuenta	96
Figura 6. 95.	Pantalla recibiendo mail	96
Figura 6. 96.	Pantalla de lectura del mail	96
Figura 6. 97.	Funcionamiento de Firewall Linux	97
Figura 6. 98.	Pantalla realizar ping	103
Figura 6. 99.	Pantalla acceso a Telnet	103
Figura 6. 100.	Pantalla: Visualización de los iptables configurados	106
Figura 6. 101.	Pantalla Bloqueo Ping	107
Figura 6. 102.	Pantalla no acceso Telnet	107
Figura 6. 103.	Pantalla: Iniciar el servicio snmpd	109
Figura 6. 104.	Pantalla de configuración del snmp	110
Figura 6. 105.	Pantalla gráfico del tráfico	111

## CAPÍTULO 7

Figura 7.1.	Componentes internos del Router	4
Figura 7.2.	Conexiones externas del Router	4
Figura 7.3.	Conexiones del puerto de administración	5
Figura 7.4.	Esquema de permisos tipos de usuarios	6
Figura 7.5.	Pantalla tipos de usuario	7
Figura 7.6.	Pantalla tipos de Interfaz de Usuario	7
Figura 7.7.	Pantalla configuración del nombre del Router	8
Figura 7.8.	Pantalla configuración de contraseña del usuario privilegiado	9
Figura 7.9.	Pantalla configuración de contraseña para el acceso remoto por telnet	10
Figura 7.10.	Pantalla cifrado de contraseñas	10
Figura 7.11.	Pantalla encriptación de contraseñas	11
Figura 7.12.	Pantalla ayuda en la interfaz de línea de comando	11
Figura 7.13.	Pantalla configuración del reloj del router	12
Figura 7.14.	Pantalla diagnóstico de fallos	12
Figura 7.15.	Pantalla comando show interfaces	13
Figura 7.16.	Pantalla comando show interfaces	13
Figura 7.17.	Pantalla configuración de una interfaz serial DCE	15
Figura 7.18.	Conexiones del Router DCE/DTE	16
Figura 7.19.	Tipos de seriales de un router	16
Figura 7.20.	Pantalla configuración de una interfaz serial DCE	17
Figura 7.21.	Pantalla descripción de interfaces	18
Figura 7.22.	Pantalla configuración de mensaje del Día	19
Figura 7.23.	Pantalla configuración de tablas de host	20
Figura 7.24.	Pantalla configuración de enrutamiento estático	21
Figura 7.25.	Pantalla configuración de enrutamiento estático 2	21
Figura 7.26.	Pantalla configuración de enrutamiento por defecto	22
Figura 7.27.	Pantalla configuración de Protocolo RIP v1	24
Figura 7.28.	Pantalla configuración de protocolos Rip V2	25
Figura 7.29.	Pantalla comando show ip route	25
Figura 7.30.	Pantalla tipos de red OSPF	27
Figura 7.31.	Pantalla Configuración del Protocolo de enrutamiento OSPF	28
Figura 7.32.	Pantalla configuración de la interfaz loopback	29
Figura 7.33.	Pantalla modificación de la métrica de los costos de OSPF	30
Figura 7.34.	Pantalla modificación de la métrica de los costos	30
Figura 7.35.	Pantalla comando show ip protocol	31
Figura 7.36.	Pantalla comando show ip route	32
Figura 7.37.	Gráfico de ubicación de ACL's	33
Figura 7.38.	Pantalla creación de ACL's	34
Figura 7.39.	Pantalla borrar ACL's	35
Figura 7.40.	Pantalla verificación de las ACL's	36
Figura 7.41.	Pantalla implementación acl extendida en la interfaz	38
Figura 7.42.	Ubicación de la ACL	38
Figura 7.43.	Implementación de Firewall	39
Figura 7.44.	Pantalla escritorio de Windows accediendo al botón inicio	40
Figura 7.45.	Pantalla escritorio de Windows opción todos los programas	41
Figura 7.46.	Pantalla escritorio de Windows opción accesorios	41
Figura 7.47.	Pantalla escritorio de Windows opción comunicaciones	42
Figura 7.48.	Pantalla escritorio de Windows icono Hyperterminal	42
Figura 7.49.	Pantalla de recomendación de programa predeterminado para Telnet	43
Figura 7.50.	Pantalla ventana descripción de la conexión del Hyperterminal	43
Figura 7.51.	Pantalla: Conectar a	44
Figura 7.52.	Pantalla propiedades del puerto COM 1	44
Figura 7.53.	Pantalla Hyperterminal con la conexión al router	45
Figura 7.54.	Gráfico WAN	46
Figura 7.55.	Switches de la serie Cisco Catalyst 2900.	132
Figura 7.56.	Cable UTP Rollover y conector DB9	133
Figura 7.57.	Conexión de un switch a el PC	133

## ÍNDICE DE TABLAS

### CAPÍTULO 2

Tabla. 2.1	Matriz: Estaciones de trabajo	11
Tabla. 2.2	Ambato: Estaciones de trabajo	11
Tabla. 2.3	Loja: Estaciones de trabajo	11
Tabla. 2.4	Matriz: Servidores	30
Tabla. 2.5	Ambato: Servidores	31
Tabla. 2.6	Loja: Servidores	31
Tabla. 2.7	Medios de comunicación: Alámbricos	46
Tabla. 2.8	Matriz: Dispositivos de conmutación	47
Tabla. 2.9	Ambato: Dispositivos de conmutación	47
Tabla. 2.10	Loja: Dispositivos de conmutación	48
Tabla. 2.11	Dispositivos de Enrutamiento	52
Tabla. 2.12	Medios Inalámbricos	54
Tabla. 2.13	Firewall matriz y sucursales	58
Tabla. 2.14	Ancho de Banda asignado por sector	62

### CAPÍTULO 3

Tabla. 3.1	Problemas encontrados	2
Tabla. 3.2	Solución Propuesta	4
Tabla. 3.3	Alternativa A: Dispositivos de enrutamiento	5
Tabla. 3.4	Alternativa A: Dispositivos de Conmutación	6
Tabla. 3.5	Alternativa A: Medios de comunicación	6
Tabla. 3.6	Alternativa A: Equipos	6
Tabla. 3.7	Alternativa A: Cableado Estructurado	7
Tabla. 3.8	Alternativa A: Factibilidad económica	8
Tabla. 3.9	Alternativa A: Costos de Software	9
Tabla. 3.10	Alternativa A: Costos del Enlace Total	9
Tabla. 3.11	Alternativa A: Costos Operativos	9
Tabla. 3.12	Alternativa A: Costo total de la propuesta	10
Tabla. 3.13	Alternativa A: Factibilidad operativa	10
Tabla. 3.14	Alternativa B: Dispositivos de enrutamiento	14
Tabla. 3.15	Alternativa B Dispositivos de comunicación	15
Tabla. 3.16	Alternativa B Medios de comunicación	15
Tabla. 3.17	Alternativa B: Equipos	15
Tabla. 3.18	Alternativa B: Cableado estructurado	16
Tabla. 3.19	Alternativa B: Factibilidad económica	17
Tabla. 3.20	Alternativa B: Costos del software	18
Tabla. 3.21	Alternativa B: Costos de enlace de datos	18
Tabla. 3.22	Alternativa B: Costos operativos	18
Tabla. 3.23	Alternativa B: Costo total de la propuesta	19
Tabla. 3.24	Alternativa B: Factibilidad operativa	19

### CAPÍTULO 7

Tabla. 7.1	Descripción de las líneas del show running mediante iconos	61
Tabla. 7.2	Descripción de las líneas del show running mediante iconos	69
Tabla. 7.3	Descripción de las líneas del show running mediante iconos	77
Tabla. 7.4	Descripción de las líneas del show running mediante iconos	84
Tabla. 7.5	Descripción de las líneas del show running mediante iconos	92
Tabla. 7.6	Descripción de las líneas del show running mediante iconos	104
Tabla. 7.7	Descripción de las líneas del show running mediante iconos.	111
Tabla. 7.8	Descripción de las líneas del show running mediante iconos	118
Tabla. 7.9	Descripción de las líneas del show running mediante iconos	129

<b>Figura 7.58.</b>	Modo de Usuario	135
<b>Figura 7.59.</b>	Configuración de contraseñas	135
<b>Figura 7.60.</b>	Comando Help	136
<b>Figura 7.61.</b>	Comparación de una LAN tradicional y una VLAN	136
<b>Figura 7.62.</b>	Administración de VLAN	137
<b>Figura 7.63.</b>	Configuración de Vlan por defecto	137
<b>Figura 7.64.</b>	Creación de las Vlan's	138
<b>Figura 7.65.</b>	Borrado de las Vlan's	138
<b>Figura 7.66.</b>	Asignación de vlan's a los puertos	139
<b>Figura 7.67.</b>	Enlace Troncal	139
<b>Figura 7.68.</b>	Enlace Switch - Router	139
<b>Figura 7.69.</b>	Interfaces físicas y lógicas	140
<b>Figura 7.70.</b>	Asignar switch de tipo server	141
<b>Figura 7.71.</b>	Enrutamiento entre distintas vlan's	141
<b>Figura 7.72.</b>	Configuración de enrutamiento entre distintas vlan's	142
<b>Figura 7.73.</b>	Escritorio de Windows accediendo al botón inicio	143
<b>Figura 7.74.</b>	Escritorio de Windows opción todos los programas	144
<b>Figura 7.75.</b>	Escritorio de Windows opción accesorios	144
<b>Figura 7.76.</b>	Escritorio de Windows opción comunicaciones	145
<b>Figura 7.77.</b>	Escritorio de Windows icono Hyperterminal	145
<b>Figura 7.78.</b>	Pantalla de recomendación de programa predeterminado para Telnet	146
<b>Figura 7.79.</b>	Ventana descripción de la conexión del Hyperterminal	146
<b>Figura 7.80.</b>	Ventana: Conectar a	147
<b>Figura 7.81.</b>	Propiedades del puerto COM 1	147
<b>Figura 7.82.</b>	Hyperterminal con la conexión al switch	148



## CAPÍTULO 1

---



# GENERALIDADES

# 1. GENERALIDADES

## 1.1 INTRODUCCIÓN

*Este manual fue elaborado con la finalidad de servir como guía de consulta para el usuario a nivel de redes, ya que contiene información clara y concisa de cómo manejar una red LAN y WAN.*

*Este manual permitirá configurar un router desde los comandos más básicos hasta la comunicación de los mismos con diferentes protocolos, también levantar un servidor Linux completo de la forma más sencilla, todo esto lo podrán realizar desde un técnico o un administrador de redes hasta un jefe de networking.*

## 1.2 OBJETIVO DE ESTE MANUAL

*El objetivo de este manual es guiar a todos aquellos usuarios interesados en el área de redes como al personal encargado de la administración de la misma, en el aspecto tanto de seguridades como configuración de equipos con la finalidad de despejar cualquier tipo de inquietud relacionado a este tema lo cual se basa en dos puntos básicos.*

- *Cómo configurar routers y switches*
- *Establecer un servidor de redes*

## 1.3 A QUIÉN VA DIRIGIDO ESTE MANUAL

*Va orientado a los usuarios finales involucrados en la etapa de implementación de la red tanto a nivel LAN como WAN.*

**Administrador de Redes;** *es la persona encargada de asistir a las redes y llevar la correcta organización de la red.*

**Jefe de networking;** *persona encargada de dar seguridad a nivel de hardware y software en una red LAN o WAN.*

## 1.4 LO QUE SE DEBE CONOCER

Se debe tener conocimientos mínimos que deben tener las personas que operan en la administración de redes tanto a nivel **LAN** como **WAN**.

Conocimientos básicos en aspecto de diseño de redes:

1. Conocimientos básicos de ruteadores, switches.
2. Conocimientos en sistemas operativos para cliente como para Servidor.
3. Conocimientos de comandos básicos de Linux.

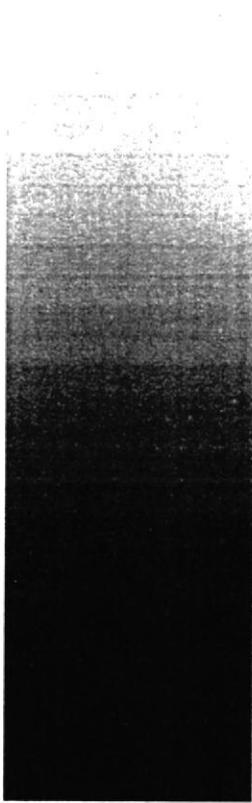
## 1.5 ORGANIZACIÓN DE ESTE MANUAL

Este manual está organizado en siete partes principales:

<b>Generalidades</b>	
<b>Capítulo 1</b>	<b>Generalidades</b> <i>Se explica brevemente el contenido del manual.</i>
<b>Capítulo 2</b>	<b>Situación Actual</b> <i>Se especifica el estado de la empresa en aspecto de redes, los dispositivos con que cuenta en la actualidad así como el resultado de los mismos con sus problemas.</i>
<b>Capítulo 3</b>	<b>Propuesta</b> <i>Aquí se le da dos soluciones enfocados en los problemas que se ha encontrado detallando los requerimientos en factibilidades técnicas, operativas y económicas.</i>
<b>Capítulo 4</b>	<b>Implementación LAN y WAN</b> <i>A través de gráficos se demuestra como será los enlaces WAN entre las sucursales y la matriz con los dispositivos.</i>
<b>Capítulo 5</b>	<b>Normativas de Cableado Estructurado</b> <i>En este capítulo se menciona las normativas y recomendaciones que deben de utilizarse para implementar un cableado estructurado.</i>
<b>Capítulo 6</b>	<b>Linux</b> <i>En este capítulo se menciona los requerimientos para poder instalar y configurar un servidor Linux en la versión Fedora Core 3</i>
<b>Capítulo 7</b>	<b>Configuración de Router y Switch</b> <i>En este capítulo se habla de los aspectos básicos con los cuales cuenta un router y switch como también la manera de configurar los equipos mencionados anteriormente.</i>

## 1.6 ACERCA DE ESTE MANUAL

Este manual contiene diversas ilustraciones e instrucciones que debe seguir un administrador de redes para poder configurar equipos de enrutamiento y conmutación así como un servidor con sus respectivos servicios.



## CAPÍTULO 2

---



## SITUACIÓN ACTUAL

## 2. SITUACIÓN ACTUAL

### 2.1 ANTECEDENTES DE LA EMPRESA

#### 2.1.1 ANTECEDENTES GENERALES

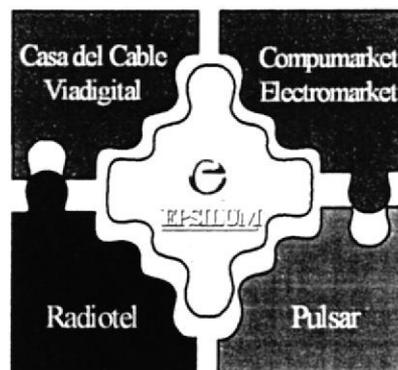


Figura 2. 1. Grupo FAUR

*EPSILUM es una empresa de tecnología con una clara misión de servicio al cliente, que forma parte del Grupo Faour con más de 15 años con experiencia en el mercado, con la finalidad de poder cubrir las necesidades del cliente final, en productos, servicios tecnológicos y soluciones llave en mano, mediante la comercialización directa de las principales marcas a nivel mundial.*

*Es por eso que en estos 7 años de vida de la empresa, ha llegado a posicionarse como un verdadero aliado de negocios para sus clientes.*

*Somos una empresa comprometida con el desarrollo de relaciones interpersonales con la finalidad de conocer la funcionalidad del negocio y así poder determinar las correctas soluciones tecnológicas, siendo sus asesores permanentes para su plataforma IT.*

*Nuestra función por medio de los ejecutivos de ventas, es en asesorarle a tomar las decisiones más adecuadas, ya que cuentan con años de experiencia en el manejo de proyectos tecnológicos. Esto adicionalmente garantiza el Retorno sobre la Inversión (siglas en inglés R.O.I) que toda empresa espera recibir del producto, solución o servicio adquirido.*

*Epsilon es una empresa de tecnología con una amplia visión del servicio al cliente, entre sus servicios están desde venta de PC's hasta diseño de páginas web, soluciones e-commerce, consultoría y de Servicios de Internet Inalámbrico tanto a nivel local como a nivel nacional.*

*Como objetivos principales, están los siguientes:*

- *Posicionar la imagen institucional del EPSILUM S.A. como una empresa ágil, eficiente, dinámica y con una alta capacidad de respuesta.*
- *Atender y ejecutar con sentido de urgencia sus requerimientos.*
- *Ejecutar y entregar los servicios con calidad.*
- *Desarrollar compromisos con los clientes.*
- *Lograr su satisfacción por la inversión realizada.*

## 2.1.2 INFORMACIÓN GENERAL

Razón Social:	EPSILUM S.A.
R.U.C.:	0991520600001
Número de Sucursales:	2 (Ambato y Loja)
Total de empleados:	52 empleados
Fecha de Constitución:	Junio 7 de 1.999
Representante Legal:	Ing. Hugo Carvajal Amaya
Dirección Comercial:	Cdla. La Herradura, Mz. 7 Solar 8 Av. Agustín Freire y Calle 1era Guayaquil - Ecuador
Teléfonos:	(593)-(4)-2230-313 / 2230-574 / 2230-440
Fax:	(593)-(4)-2234-858
e-Mail:	<a href="mailto:epsilum@epsilum.com">epsilum@epsilum.com</a>
Web:	<a href="http://www.epsilum.com">www.epsilum.com</a>

## 2.1.3 MISIÓN

Identificar las oportunidades del mercado y las necesidades reales de los clientes, para ofrecer productos, servicios o soluciones llave en mano como integradores, aprovechando al máximo la tecnología como herramienta eficiente para aumentar la productividad en los negocios de nuestros clientes, ejecutado por profesionales capacitados y motivados por una empresa rentable con claras metas y objetivos.

## 2.1.4 VISIÓN

Ser reconocidos para el 2006, como una empresa de servicios de valor agregado, destacada por su responsabilidad en el servicio y soporte a lo largo de todas las soluciones comercializadas para apoyar los negocios de nuestros clientes, apalancados en las fortalezas del Grupo Empresarial Faour.

## 2.1.5 OBJETIVOS GENERALES DE LA EMPRESA

- Desarrollar una relación a largo plazo y de beneficio mutuo.
- Promover la participación de Epsilum en eventos comerciales a nivel nacional e internacional.
- Construir una imagen de prestigio internacional, basada en el uso intensivo de la tecnología en sus procedimientos internos y en su relación con los clientes, mejorando los índices de competitividad internacional y generando de este modo un mejor escenario para la atracción de inversión extranjera y una mejor inserción en la nueva economía global.
- Ejecutar programas de servicios regionales, relativos al desarrollo de las áreas de comercialización, en permanente interacción de alianzas estratégicas con otras empresas bajo criterios de esfuerzo compartido.



- *Contribuir al desarrollo y consolidación de la empresa, bajo criterios de complementariedad y esfuerzo compartido entre los directivos y empleados.*
- *Apoyar a proyectos integrales, con enfoque sistemático, destinados al mejoramiento sostenido de los procesos de investigación y comercialización que se ejecutan en las empresas, contribuyendo a mejorar las condiciones cuantitativas y cualitativas de sus recursos humanos, organizacionales, informáticos, infraestructurales y materiales.*
- *Identificar las oportunidades negocios entre los sectores productivos.*

### **2.1.6 OBJETIVOS OPERATIVOS DE LA EMPRESA**

- *Atender y ejecutar con sentido de urgencia los requerimientos de los clientes.*
- *Ejecutar y entregar servicios con calidad.*
- *Lograr la satisfacción de los clientes por la inversión realizada.*
- *Desarrollar una relación a largo plazo y de beneficio mutuo.*
- *Mejoramiento de la tecnología de punta.*
- *Capacitación y mejoramiento del personal*
- *Desarrollar la prestación de los servicios buscando la simplicidad de los procedimientos para incrementar el grado de satisfacción de los clientes a través del uso generalizado de medios electrónicos de última generación.*
- *Realizar un esfuerzo permanente para un manejo racional de los costos operativos.*
- *Establecer mecanismos para la obtención de recursos financieros.*
- *Reactivar y direccionar la comercialización de productos y servicios según la demanda de los clientes.*
- *Promover la formación continua de los recursos humanos internos.*
- *Crear líneas de productos y servicios novedosos.*
- *Fomentar alianzas estratégicas con otras empresas dedicadas a la investigación y comercialización de productos o servicios.*



## 2.1.7 DEPARTAMENTOS DE LA EMPRESA

### 2.1.7.1 MATRIZ

- **Nombre del departamento:** *Gerencia General*  
**Nº de personas:** 2  
**Responsable:** *Ing. Hugo Carvajal*  
**Cargo:** *Gerente General*
  
- **Nombre del departamento:** *Gerencia Administrativa*  
**Nº de personas:** 2  
**Responsable:** *Ing. Carla Tutiven*  
**Cargo:** *Gerente Administrativa*
  
- **Nombre del departamento:** *Diseño y Desarrollo*  
**Nº de personas:** 3  
**Responsable:** *Ing. Xavier Carlieri*  
**Cargo:** *Jefe Dpto. de Desarrollo*
  
- **Nombre del departamento:** *Ventas*  
**Nº de personas:** 4  
**Responsable:** *Ing. Com. Carla Tutivén*  
**Cargo:** *Jefe de Ventas*
  
- **Nombre del departamento:** *Departamento Técnico*  
**Nº de personas:** 4  
**Responsable:** *Ing. Marcos Calderón*  
**Cargo:** *Jefe Departamento Técnico*
  
- **Nombre del departamento:** *Networking*  
**Nº de personas:** 5  
**Responsable:** *Ing. Fernando Calderón*  
**Cargo:** *Jefe de Networking*



Figura 2. 2. Departamento de Networking



- **Nombre del departamento:** *Compras y Bodega*  
**Nº de personas:** 2  
**Responsable:** *Ing. Com. Roxana Carrillo*  
**Cargo:** *Jefe de Bodega*
  
- **Nombre del departamento:** *Transporte y Logística*  
**Nº de personas:** 2  
**Responsable:** *José Luis Chávez*  
**Cargo:** *Jefe de Transporte*
  
- **Nombre del departamento:** *Secretaría y Recepción*  
**Nº de personas:** 1  
**Responsable:** *Ing. Com. Olga Moreira*  
**Cargo:** *Secretaria-Recepcionista*
  
- **Nombre del departamento:** *Cobranzas*  
**Nº de personas:** 2  
**Responsable:** *Ing. Com. Carmen Arteaga*  
**Cargo:** *Jefe de Cobranzas*
  
- **Nombre del departamento:** *Mensajería*  
**Nº de personas:** 2  
**Responsable:** *Angel Zambrano*  
**Cargo:** *Mensajero*



*Figura 2. 3. Departamento de Ventas*

- INFRAESTRUCTURA FÍSICA

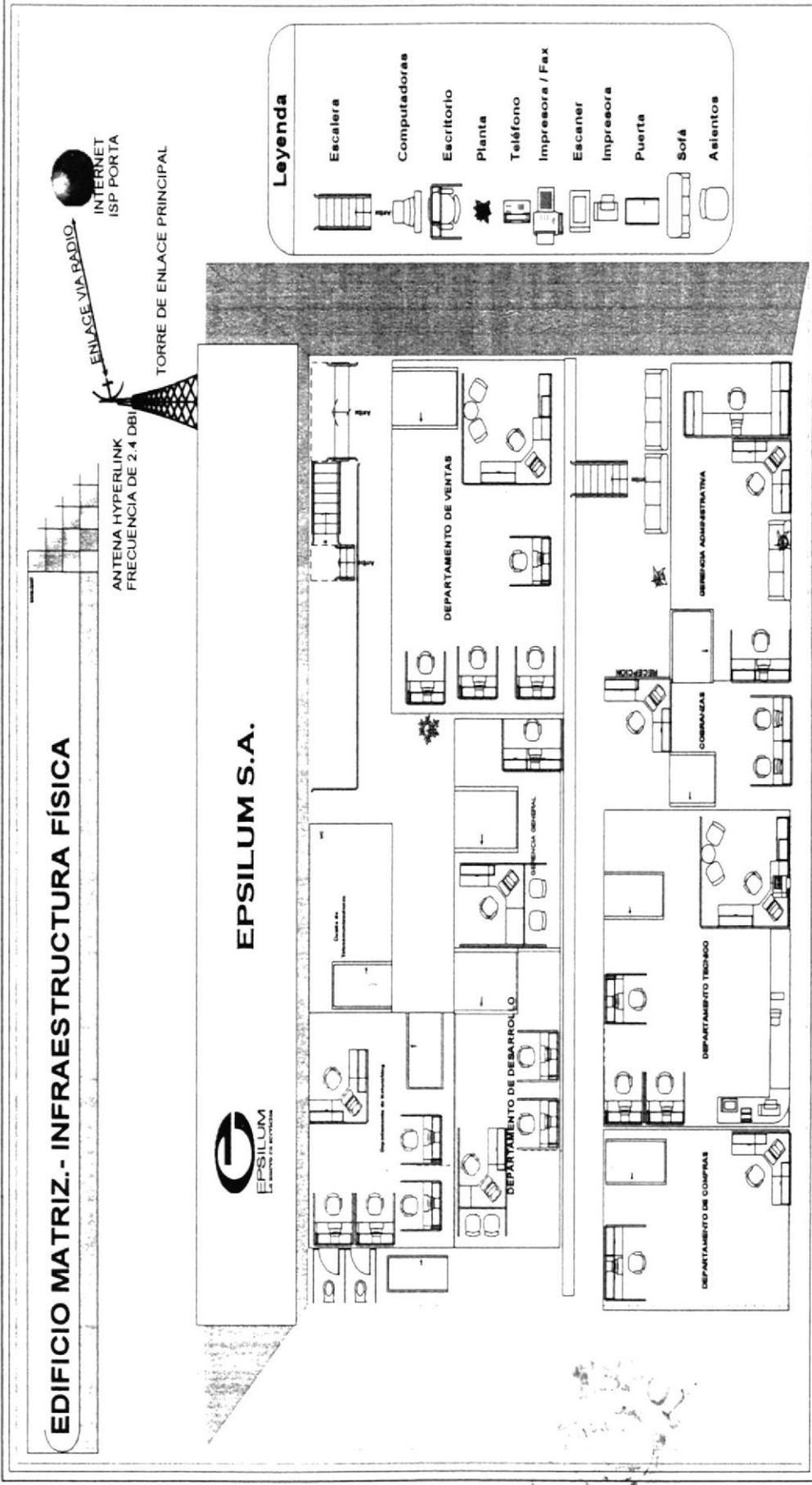


Figura 2. 4. Matriz: Infraestructura Física

## 2.1.7.2 SUCURSAL # 1 (AMBATO)



Figura 2. 5. Departamento de Ventas

- |                                                                                                                                                                         |                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ <b>Nombre del departamento:</b></li> <li><b>Nº de personas:</b></li> <li><b>Responsable:</b></li> <li><b>Cargo:</b></li> </ul> | <ul style="list-style-type: none"> <li><b>Gerencia Administrativa</b></li> <li>2</li> <li>Ing. Fernando Carvajal</li> <li>Gerente Administrativo</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
  
- |                                                                                                                                                                         |                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ <b>Nombre del departamento:</b></li> <li><b>Nº de personas:</b></li> <li><b>Responsable:</b></li> <li><b>Cargo:</b></li> </ul> | <ul style="list-style-type: none"> <li><b>Departamento Técnico</b></li> <li>2</li> <li>Ing. Gonzalo Rosero</li> <li>Jefe de Departamento Técnico</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
  
- |                                                                                                                                                                         |                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ <b>Nombre del departamento:</b></li> <li><b>Nº de personas:</b></li> <li><b>Responsable:</b></li> <li><b>Cargo:</b></li> </ul> | <ul style="list-style-type: none"> <li><b>Networking</b></li> <li>3</li> <li>Ing. Guillermo Rolando</li> <li>Jefe de Networking</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
  
- |                                                                                                                                                                         |                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ <b>Nombre del departamento:</b></li> <li><b>Nº de personas:</b></li> <li><b>Responsable:</b></li> <li><b>Cargo:</b></li> </ul> | <ul style="list-style-type: none"> <li><b>Secretaría y Recepción</b></li> <li>1</li> <li>Ing. Com. Claudia Loza</li> <li>Secretaria-Recepcionista</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
  
- |                                                                                                                                                                         |                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ <b>Nombre del departamento:</b></li> <li><b>Nº de personas:</b></li> <li><b>Responsable:</b></li> <li><b>Cargo:</b></li> </ul> | <ul style="list-style-type: none"> <li><b>Ventas</b></li> <li>2</li> <li>Ing. Com. Patricia Chávez</li> <li>Jefe de Ventas</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|

- **INFRAESTRUCTURA FÍSICA**

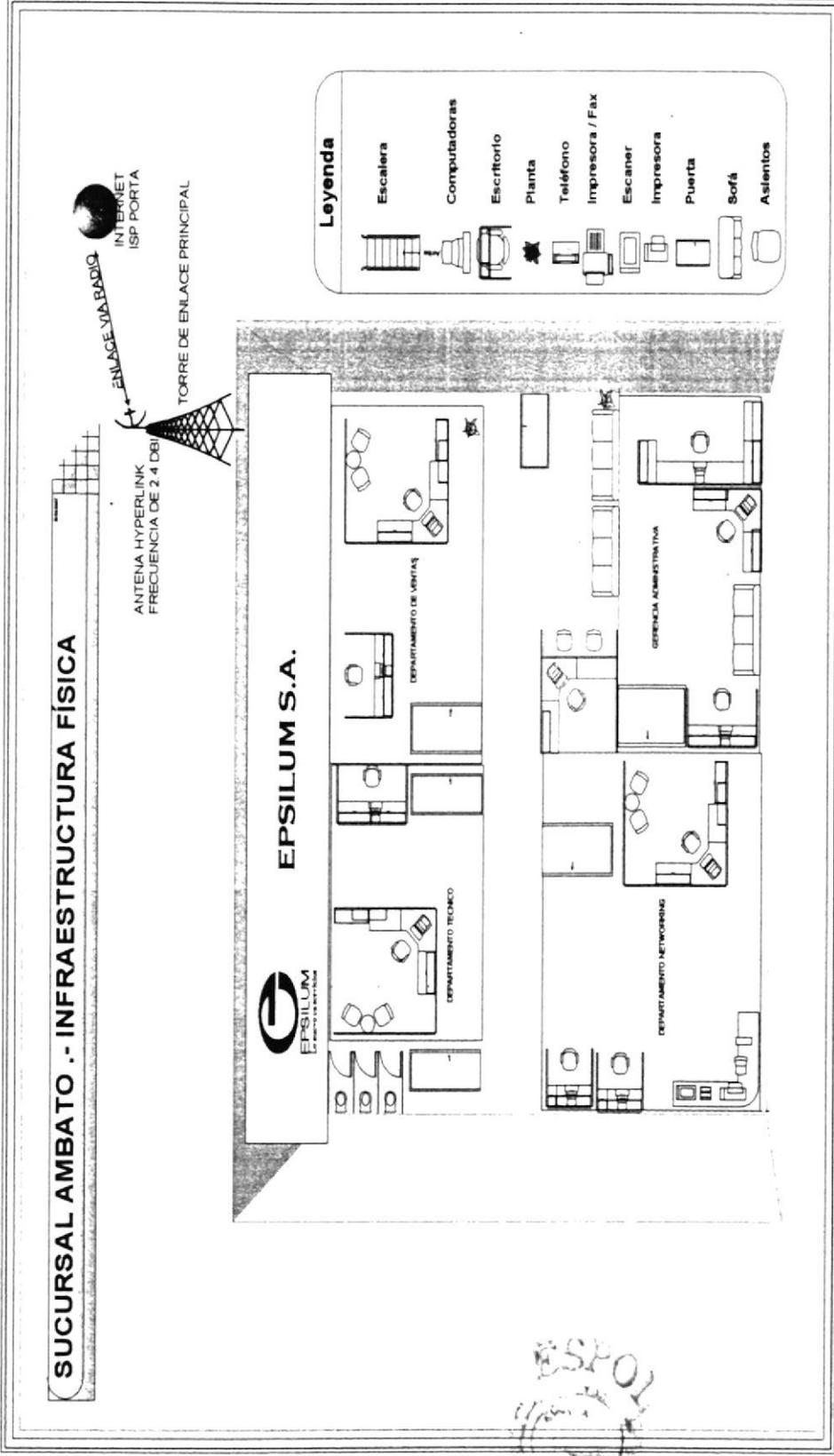


Figura 2. 6. Ambato: Infraestructura física

## 2.1.7.3 SUCURSAL # 2 (LOJA)



Figura 2. 7. Jefe del departamento de Networking

- **Nombre del departamento:** Gerencia General  
**N° de personas:** 3  
**Responsable:** Ing. Patricia Carvajal  
**Cargo:** Gerente General
- **Nombre del departamento:** Networking  
**N° de personas:** 3  
**Responsable:** Ing. Gabriel Morán  
**Cargo:** Jefe de Networking
- **Nombre del departamento:** Secretaría y Recepción  
**N° de personas:** 1  
**Responsable:** Ing. Com. Zoraida Quinde  
**Cargo:** Secretaria-Recepcionista
- **Nombre del departamento:** Ventas  
**N° de personas:** 2  
**Responsable:** Ing. Com. Wendy Vera  
**Cargo:** Jefe de Ventas

- INFRAESTRUCTURA FÍSICA

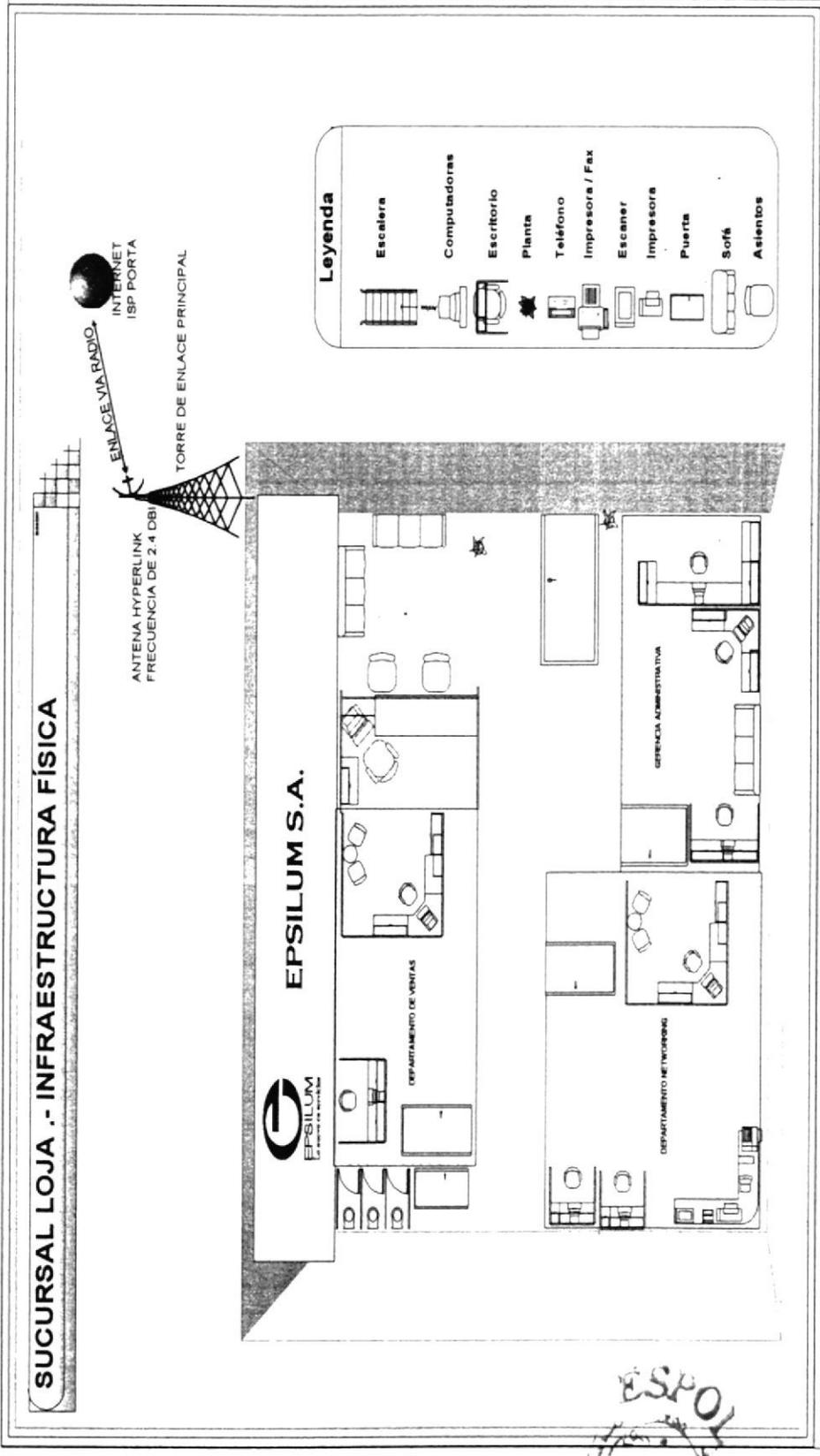


Figura 2. 8. Loja: Infraestructura física



## 2.2 INFRAESTRUCTURA LAN

### 2.2.1 ESTACIONES DE TRABAJO

- MATRIZ**

	<b>Dispositivo :</b> HOST (Clientes) <b>Número de Host:</b> 25 computadoras <b>Marca:</b> Clones
	<b>CARACTERÍSTICAS TÉCNICAS</b> Intel Pentium IV 2,80 GHz
	256 Mb de Ram
	1 Disco 40 Gb/80GB
	Tarjeta de Red 10/100 Mbps
	Video/Sonido/Fax

Tabla. 2.1 Matriz: Estaciones de trabajo

- SUCURSAL: AMBATO**

	<b>Dispositivo :</b> HOST <b>Número de Host:</b> 10 computadoras <b>Marca:</b> Clones
	<b>CARACTERÍSTICAS TÉCNICAS</b> Intel Pentium IV 2,80 GHz
	256 Mb de Ram
	1 Disco 40 Gb/80GB
	Tarjeta de Red 10/100 Mbps
	Video/Sonido/Fax

Tabla. 2.2 Ambato: Estaciones de trabajo

- SUCURSAL: LOJA**

	<b>Dispositivo :</b> HOST <b>Número de Host:</b> 9 computadoras <b>Marca:</b> Clones
	<b>CARACTERÍSTICAS TÉCNICAS</b> Intel Pentium IV 2,80 GHz
	256 Mb de Ram
	1 Disco 40 Gb/80GB
	Tarjeta de Red 10/100 Mbps
	Video/Sonido/Fax

Tabla. 2.3 Loja: Estaciones de trabajo

2.2.1.1 MATRIZ

DEPARTAMENTO: GERENCIA GENERAL



Figura 2. 9. Matriz: Departamento de Gerencia General

**Nombre del departamento:**

*Gerencia General*

**N° de personas:**

2

**Cantidad de Host:**

2

**Puntos de datos:**

2

**Puntos de Voz:**

2

**Características de los computadores:**

*Pentium IV 2.08 Ghz*

*Disco Duro de 80 Gb.*

*Memoria RAM 512 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*



**DEPARTAMENTO: VENTAS**

**Figura 2. 10.** Matriz: Departamento de Ventas

**Nombre del departamento:**

*Ventas*

**Nº de personas:**

*4*

**Cantidad de Host:**

*4*

**Puntos de Datos:**

*4*

**Puntos de Voz:**

*4*

**Características de los computadores:**

*Pentium IV 2.06 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

**DEPARTAMENTO: DESARROLLO**

**Figura 2. 11.** Matriz: Departamento de Desarrollo

**Nombre del departamento:**

*Desarrollo*

**N° de personas:**

3

**Cantidad de Host:**

3

**Puntos de Datos:**

3

**Puntos de Voz:**

3

**Características de los computadores:**

*Pentium IV 3.06 Ghz*

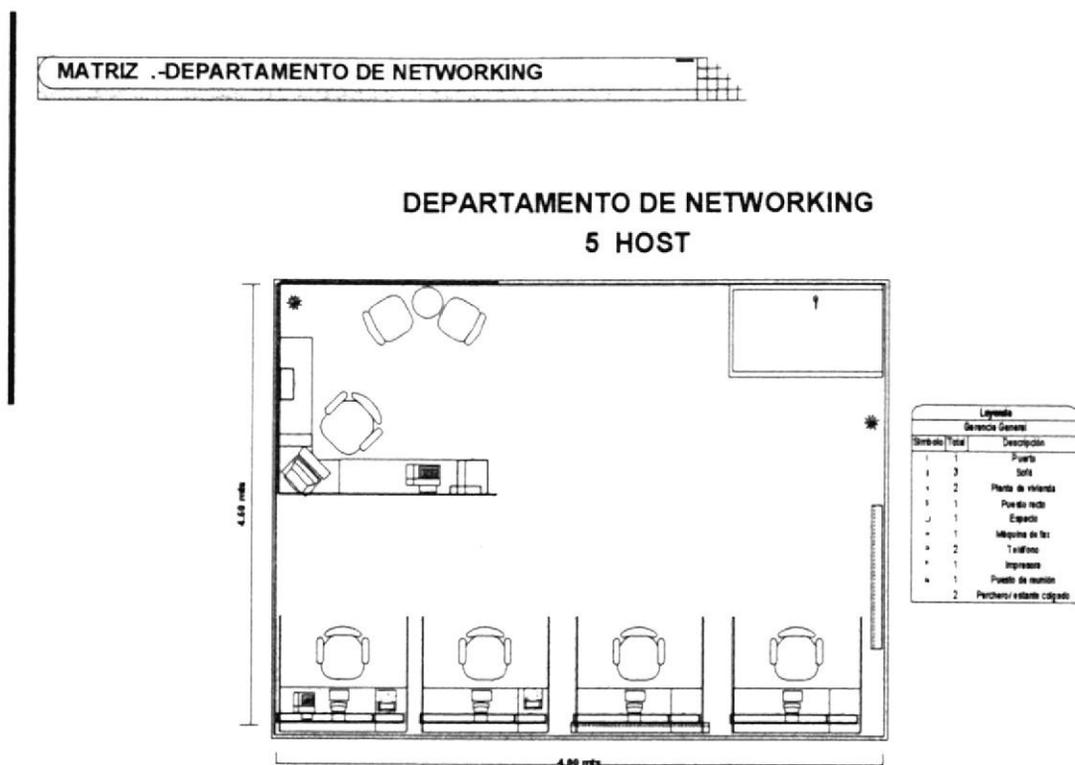
*Disco Duro de 80 Gb.*

*Memoria RAM 512 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*



**DEPARTAMENTO: NETWORKING**

**Figura 2. 12.** Matriz: Departamento de Networking

**Nombre del departamento:**

*Networking*

**N° de personas:**

4

**Cantidad de Host:**

4

**Puntos de Datos:**

5

**Puntos de Voz:**

5

**Características de los computadores:**

*Celeron 2.06 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

**DEPARTAMENTO: COMPRAS**

**Figura 2. 13.** Matriz: Departamento de Compras

**Nombre del departamento:**

*Compras*

**Nº de personas:**

*2*

**Cantidad de Host:**

*2*

**Puntos de Datos:**

*2*

**Puntos de Voz:**

*1*

**Características de los computadores:**

*Celeron 2.06 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*



**DEPARTAMENTO: COBRANZAS**

**Figura 2. 14.** Matriz: Departamento de Cobranzas

**Nombre del departamento:**

*Cobranzas*

**Nº de personas:**

2

**Cantidad de Host:**

2

**Puntos de Datos:**

2

**Puntos de Voz:**

1

**Características de los computadores:**

*Celeron 2.05 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

**DEPARTAMENTO: TÉCNICO**

**Figura 2. 15.** Matriz: Departamento Técnico

**Nombre del departamento:**

*Técnico*

**Nº de personas:**

4

**Cantidad de Host:**

4

**Puntos de Datos:**

5

**Puntos de Voz:**

3

**Características de los computadores:**

*Celeron 2.60 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

**DEPARTAMENTO: GERENCIA ADMINISTRATIVA**

**Figura 2. 16.** Matriz: Gerencia Administrativa

**Nombre del departamento:**

*Gerencia Administrativa*

**Nº de personas:**

2

**Cantidad de Host:**

2

**Puntos de Datos:**

2

**Puntos de Voz:**

2

**Características de los computadores:**

*Pentium IV 2.80 Ghz*

*Disco Duro de 80 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

## DEPARTAMENTO: RECEPCIÓN

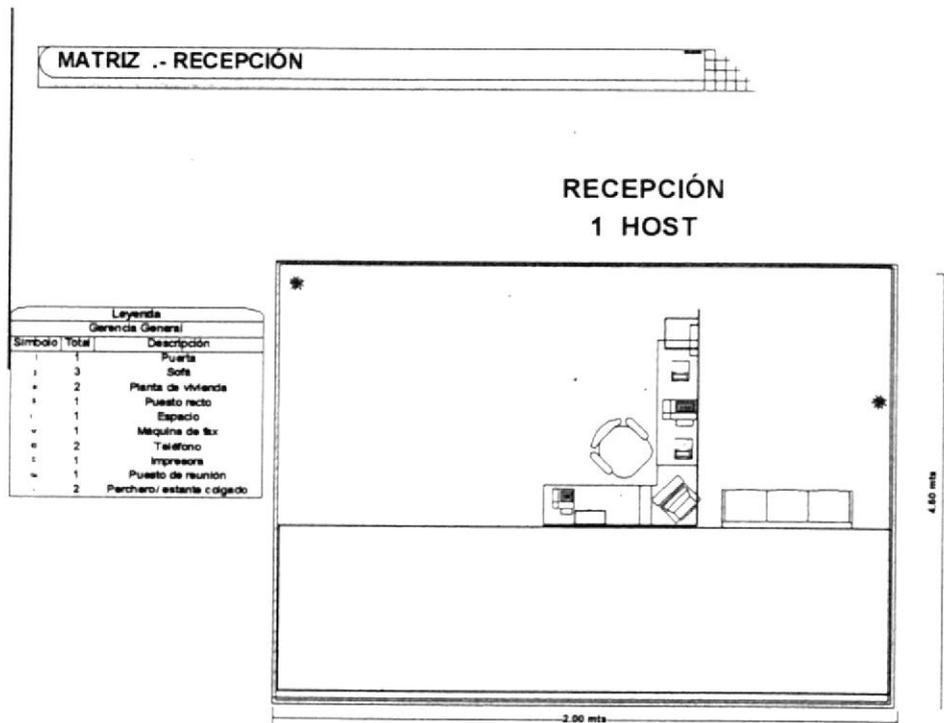


Figura 2. 17. Matriz: Departamento de Recepción

*Nombre del departamento:*

*Recepción*

*Nº de personas:*

*1*

*Cantidad de Host:*

*1*

*Puntos de Datos:*

*2*

*Puntos de Voz:*

*1*

*Características de los computadores:*

*Celeron 2.05 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*



## 2.2.1.2 SUCURSAL: AMBATO

## DEPARTAMENTO: GERENCIA ADMINISTRATIVA



Figura 2. 18. Ambato: Gerencia Administrativa

*Nombre del departamento:*

*Gerencia Administrativa*

*Nº de personas:*

2

*Cantidad de Host:*

2

*Puntos de Datos:*

3

*Puntos de Voz:*

2

*Características de los computadores:*

*Pentium IV 2.60 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

## DEPARTAMENTO: NETWORKING

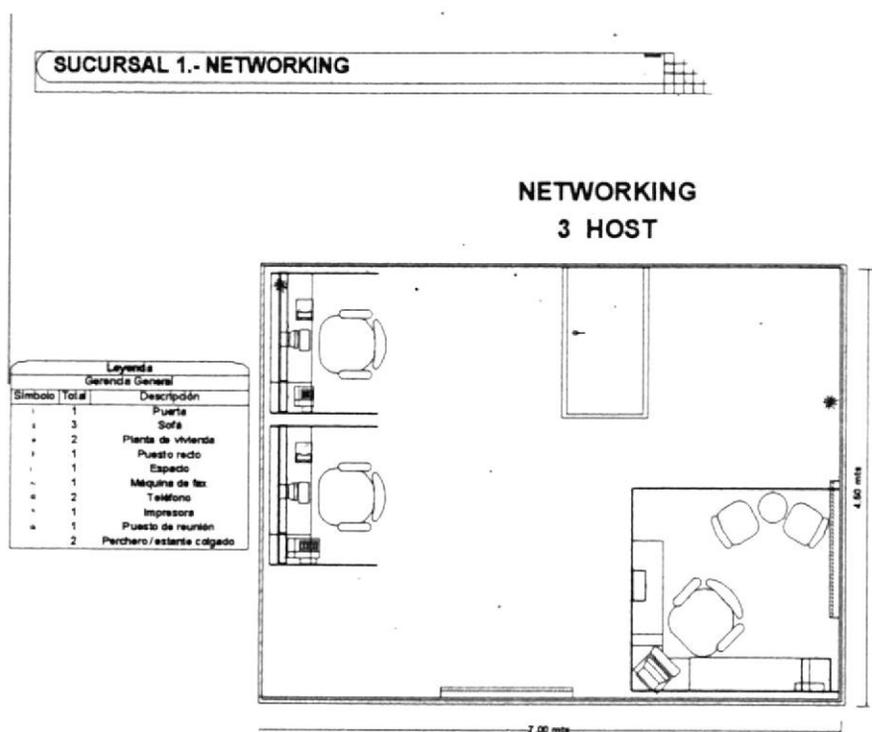


Figura 2. 19. Ambato: Departamento de Networking

*Nombre del departamento:*

*Networking*

*Nº de personas:*

3

*Cantidad de Host:*

3

*Puntos de Datos:*

6

*Puntos de Voz:*

4

*Características de los computadores:*

*Celeron 2.60 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

**DEPARTAMENTO: TÉCNICO**

Figura 2. 20. Ambato: Departamento Técnico

*Nombre del departamento:*

*Técnico*

*N° de personas:*

2

*Cantidad de Host:*

2

*Puntos de Datos:*

3

*Puntos de Voz:*

2

*Características de los computadores:*

*Celeron 2.50 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

**DEPARTAMENTO: VENTAS**

Figura 2. 21. Ambato: Departamento de Ventas

**Nombre del departamento:***Ventas***N° de personas:**

2

**Cantidad de Host:**

2

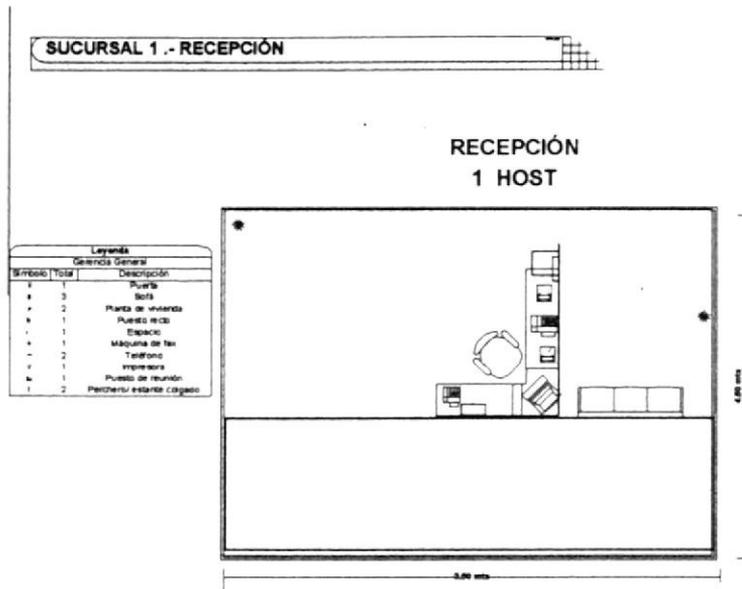
**Puntos de Datos:**

2

**Puntos de Voz:**

2

**Características de los computadores:***Celeron 2.50 Ghz**Disco Duro de 40 Gb.**Memoria RAM 256 Mb**Tarjeta de Red D-Link 10 100 1000 Mbps**Sistema Operativo Windows XP*

**DEPARTAMENTO: RECEPCIÓN**

**Figura 2. 22.** Ambato: Departamento de Recepción

**Nombre del departamento:**

*Recepción*

**Nº de personas:**

*1*

**Cantidad de Host:**

*1*

**Puntos de Datos:**

*2*

**Puntos de Voz:**

*1*

**Características de los computadores:**

*Celeron 2.05 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

## 2.2.1.3 SUCURSAL: LOJA

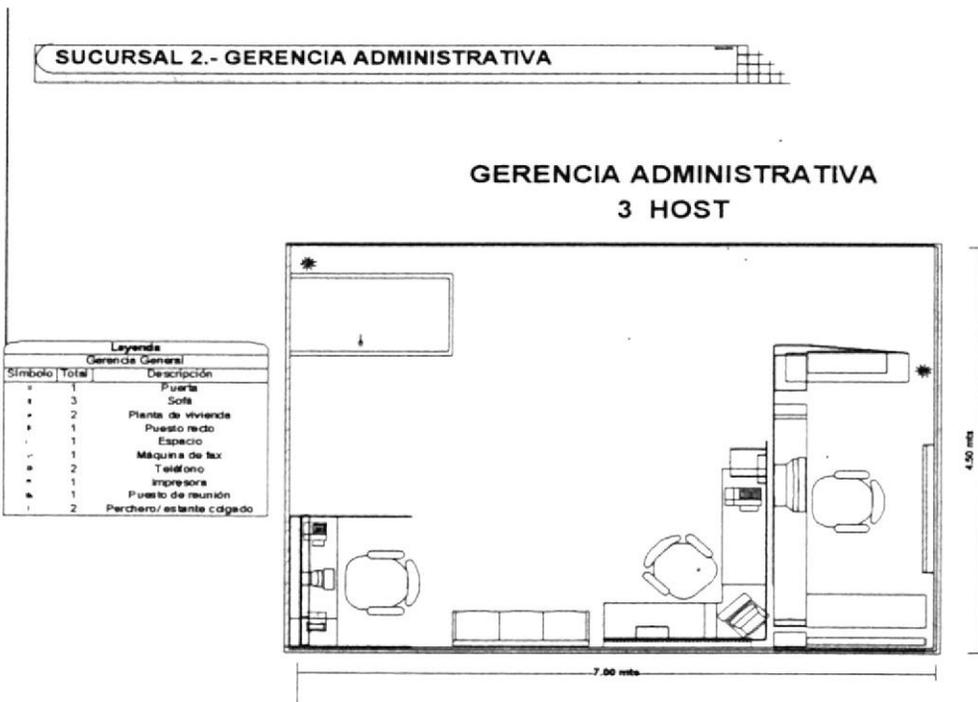
**DEPARTAMENTO: GERENCIA ADMINISTRATIVA**

Figura 2. 23. Loja: Gerencia Administrativa

Nombre del departamento:

Gerencia Administrativa

N° de personas:

3

Cantidad de Host:

3

Puntos de Datos:

3

Puntos de Voz:

3

Características de los computadores:

Pentium IV 2.60

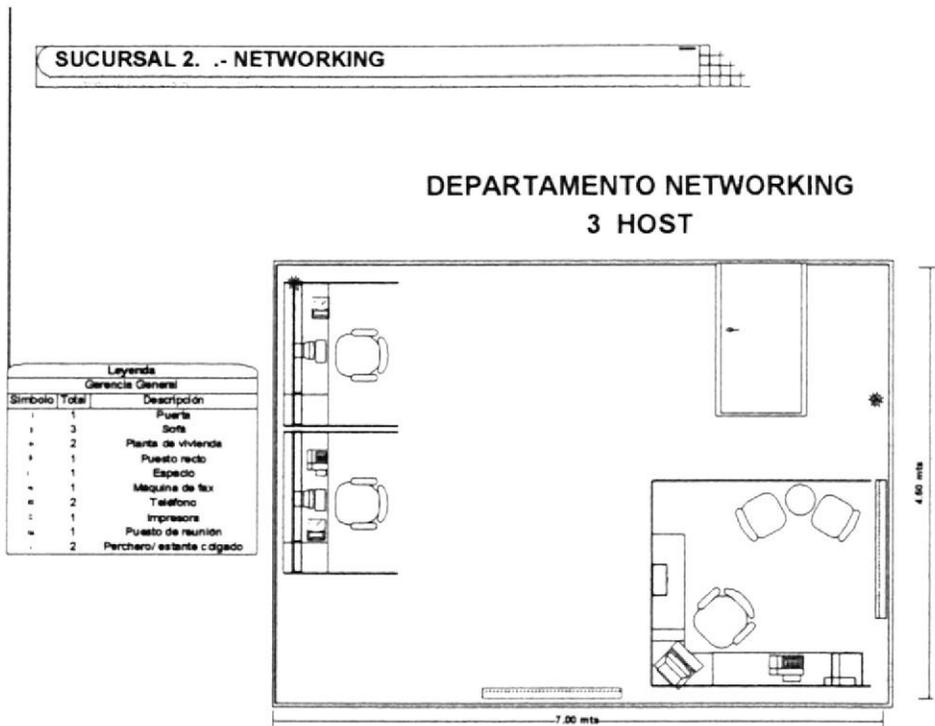
Disco Duro de 80 Gb.

Memoria RAM 256 Mb

Tarjeta de Red D-Link 10 100 1000 Mbps

Sistema Operativo Windows XP



**DEPARTAMENTO: NETWORKING**

**Figura 2. 24.** Loja: Departamento de Networking

**Nombre del departamento:**

*Networking*

**N° de personas:**

3

**Cantidad de Host:**

3

**Puntos de Datos:**

6

**Puntos de Voz:**

4

**Características de los computadores:**

*Celeron 2.06 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

## DEPARTAMENTO: VENTAS



Figura 2. 25. Loja: Departamento de Ventas

**Nombre del departamento:**

*Ventas*

**Nº de personas:**

2

**Cantidad de Host:**

2

**Puntos de Datos:**

2

**Puntos de Voz:**

2

**Características de los computadores:**

*Celeron 2.05 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*



**DEPARTAMENTO: RECEPCIÓN**

**Figura 2. 26.** Loja: Departamento de Recepción

**Nombre del departamento:**

*Recepción*

**Nº de personas:**

*1*

**Cantidad de Host:**

*1*

**Puntos de Datos:**

*2*

**Puntos de Voz:**

*1*

**Características de los computadores:**

*Celeron 2.05 Ghz*

*Disco Duro de 40 Gb.*

*Memoria RAM 256 Mb*

*Tarjeta de Red D-Link 10 100 1000 Mbps*

*Sistema Operativo Windows XP*

## 2.2.2 SERVIDORES

## 2.2.2.1 MATRIZ

<b>SERVIDORES</b>	
	<b>Tipo de Servidor:</b> Servidor de Correo <b>Ubicación:</b> MC MATRIZ <b>Características</b>
	<b>Modelo Servidor</b> IBM xSeries o SUPERMICRO Intel Pentium IV 3.20 GHz 512 Mb de Ram 1 Disco 80 Gb 2 Tarjetas de Red 10/100/1000 Mbps
	<b>Software Instalado</b> Linux Mandrake Servidor de acceso remoto Servidor Web Internet Information Server Servidor de Correo
	<b>Tipo de Servidor:</b> Servidor de Aplicaciones <b>Ubicación:</b> MC MATRIZ <b>Características</b>
	<b>Modelo Servidor</b> IBM System p5 185 Express Procesadores PowerPC 970 de 1 ó 2 procesadores Hasta 8 GB de memoria 1 Disco 80 Gb 2 Tarjetas de Red 10/100/1000 Mbps
	<b>Software Instalado</b> Linux Mandrake
	<b>Tipo de Servidor:</b> Servidor Web <b>Características</b>
	<b>Ubicación: MC Matriz</b> <b>Modelo Servidor</b> Clon Intel Pentium IV 3.06 GHz 512 Mb de Ram 1 Disco 80 Gb 1 Tarjetas de Red 10/100/1000 Mbps
	<b>Tipo de Servidor:</b> Servidor Proxy <b>Características</b>
	<b>Ubicación: MC Matriz</b> <b>Software Instalado</b> Linux Mandrake

Tabla. 2.4 Matriz: Servidores

## 2.2.2.2 SUCURSAL: AMBATO

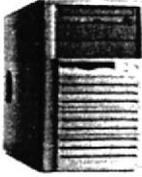
SERVIDORES		
	Tipo de Servidor:	Servidor de Correo
	Ubicación:	MC SUCURSAL AMBATO
	Características	
	Modelo Servidor	IBM xSeries o SUPERMICRO
		Intel Pentium IV 3.20 GHz
		512 Mb de Ram
1 Disco 80 Gb		
2 Tarjetas de Red 10/100/1000 Mbps		
Software Instalado	Linux Mandrake	
	Tipo de Servidor:	Servidor Proxy
	Ubicación:	MC SUCURSAL AMBATO
	Características	
	Modelo Servidor	Clon
		Intel Pentium IV 3.06 GHz
		512 Mb de Ram
2 Tarjetas de Red 10/100/1000 Mbps		
1 Disco 80 Gb		
Software Instalado	Linux Mandrake	

Tabla. 2.5 Ambato: Servidores

## 2.2.2.3 SUCURSAL: LOJA

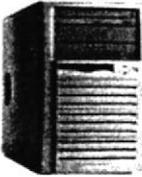
	Tipo de Servidor:	Servidor de Correo
	Ubicación:	MC SUCURSAL LOJA
	Características	
	Modelo Servidor	IBM xSeries o SUPERMICRO
		Intel Pentium IV 3.20 GHz
		512 Mb de Ram
1 Disco 80 Gb		
2 Tarjetas de Red 10/100/1000 Mbps		
Software Instalado	Linux Mandrake	
	Tipo de Servidor:	Servidor Proxy
	Ubicación:	MC SUCURSAL LOJA
	Características	
	Modelo Servidor	Clon
		Intel Pentium IV 3.06 GHz
		512 Mb de Ram
2 Tarjetas de Red 10/100/1000 Mbps		
1 Disco 80 Gb		
Software Instalado	Linux Mandrake	

Tabla. 2.6 Loja: Servidores

## 2.2.3 ANÁLISIS DE PISO

### 2.2.3.1 MATRIZ

#### **CONEXIÓN A TIERRA:**

El edificio cuenta con conexión a tierra, lo que brinda seguridad a los equipos en caso de una descarga o anomalía eléctrica imprevista.

La conexión a tierra se encuentra ubicada en el lado izquierdo del edificio (cuarto de medidores).

#### **CABLEADO ESTRUCTURADO:**

El sistema de Cableado Estructurado con el que cuenta la empresa está de acuerdo al siguiente detalle:

- **TOMAS MODULARES**

Líneas de Red con conectores RJ-45 asignados para cada computador.

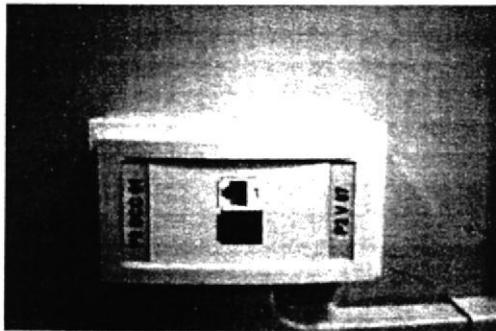


Figura 2. 27. Face Plate con su etiqueta respectiva

- **CANALIZACIÓN**

En lo relacionado a canalización, la empresa cuenta con lo siguiente:

- Tubería metálica.
- Cajas de Paso.
- Canaletas Decorativas, con todos los accesorios de acoplamiento a techos falsos, placas de pared, codos.

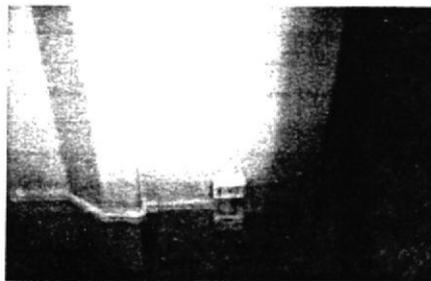


Figura 2. 28. Cableado Horizontal(Terminales)





*Figura 2. 29. Edificio Matriz.- Cableado Horizontal(Canaletas)*

**POP:**

*La central telefónica de la empresa se encuentra ubicada en la planta alta, en un departamento independiente en la parte posterior del edificio.*

**CAÑERÍAS ELÉCTRICAS Y DE AGUA:**

*Estas recorren la parte izquierda del edificio.*



*Figura 2. 30. Edificio Matriz .- Cañerías eléctricas y de agua*

### 2.2.3.2 SUCURSALES: AMBATO y LOJA

#### CONEXIÓN A TIERRA:

Los edificios cuenta con conexiones a tierra, lo que brinda seguridad a los equipos en caso de una descarga o anomalía eléctrica imprevista, estas conexiones se encuentran ubicadas en el lado izquierdo del edificio (cuarto de medidores).

#### CABLEADO ESTRUCTURADO:

El sistema de Cableado Estructurado con el que cuenta la empresa está de acuerdo al siguiente detalle:

- **TOMAS MODULARES**

Líneas de Red con conectores RJ-45 asignados para cada computador.

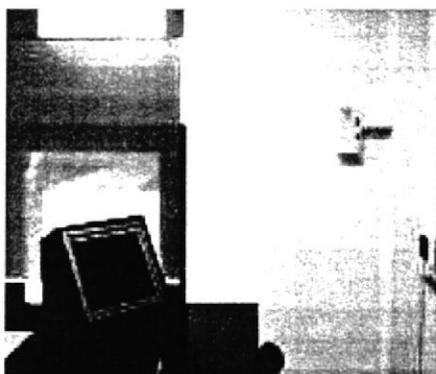


Figura 2. 31. Sucursal Ambato.- Cableado Horizontal

#### POP:

La central telefónica de las sucursales se encuentra ubicada en la planta baja, en un departamento independiente en la parte central del edificio.

#### CAÑERÍAS ELÉCTRICAS Y DE AGUA:

Estas recorren la parte derecha del edificio.



## 2.2.4 ANÁLISIS DE PISO LÓGICO

### 2.2.4.1 MATRIZ PLANTA BAJA

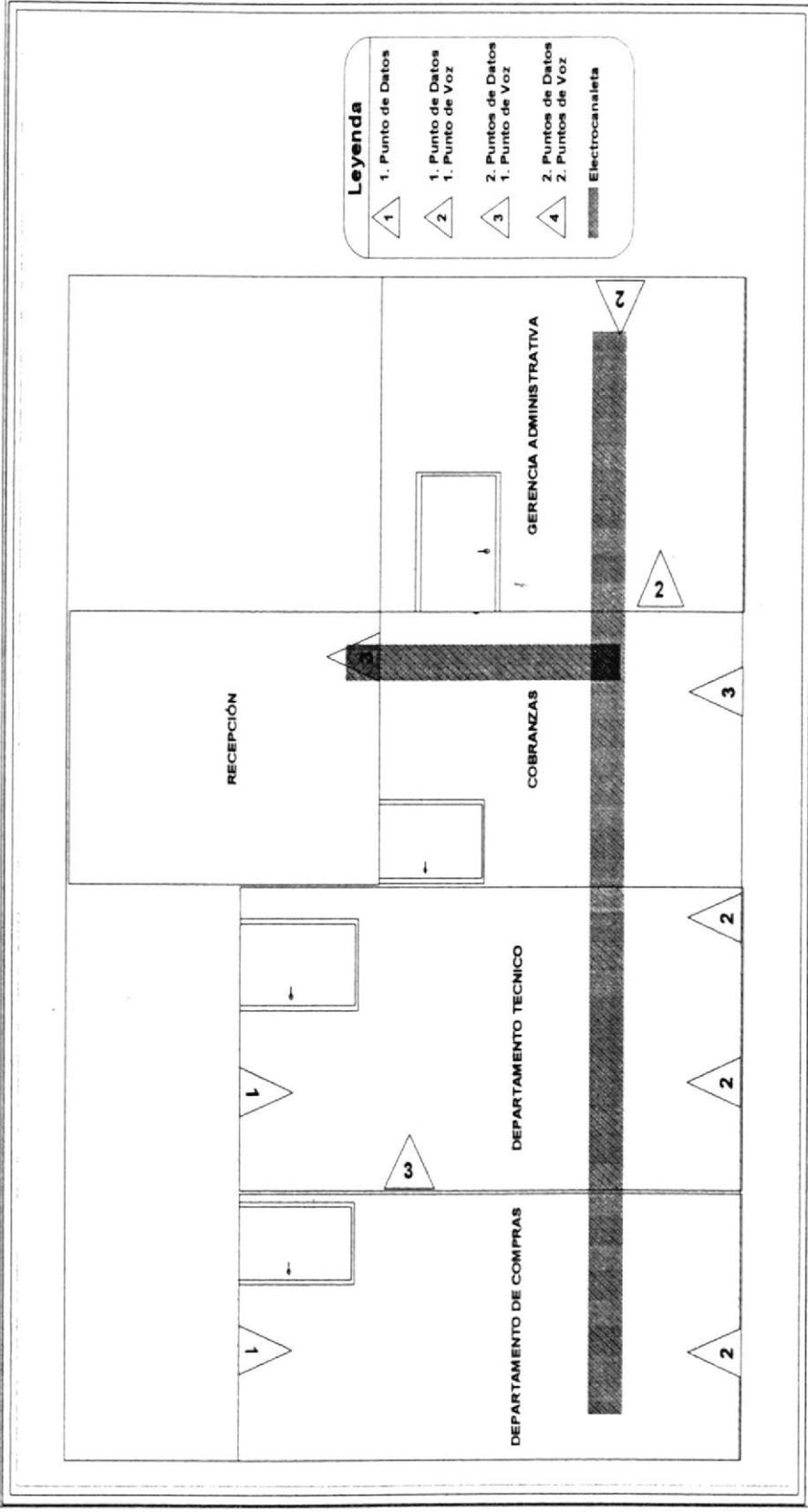


Figura 2. 32. Matriz planta baja: Análisis de Piso lógico

2.2.4.2 MATRIZ PLANTA ALTA

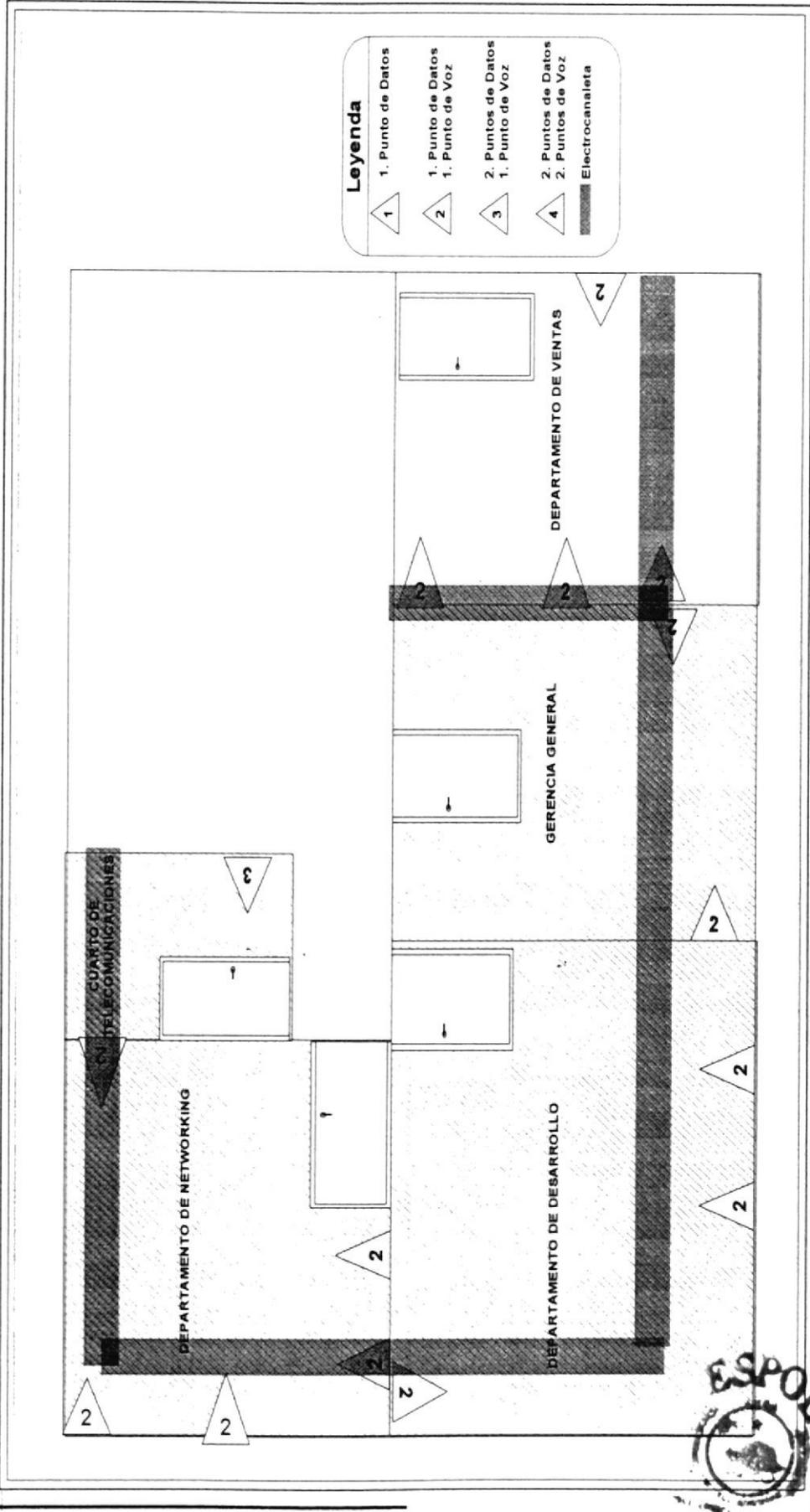


Figura 2. 33. Matriz planta alta: Analisis de Piso lógico

2.2.4.3 AMBATO

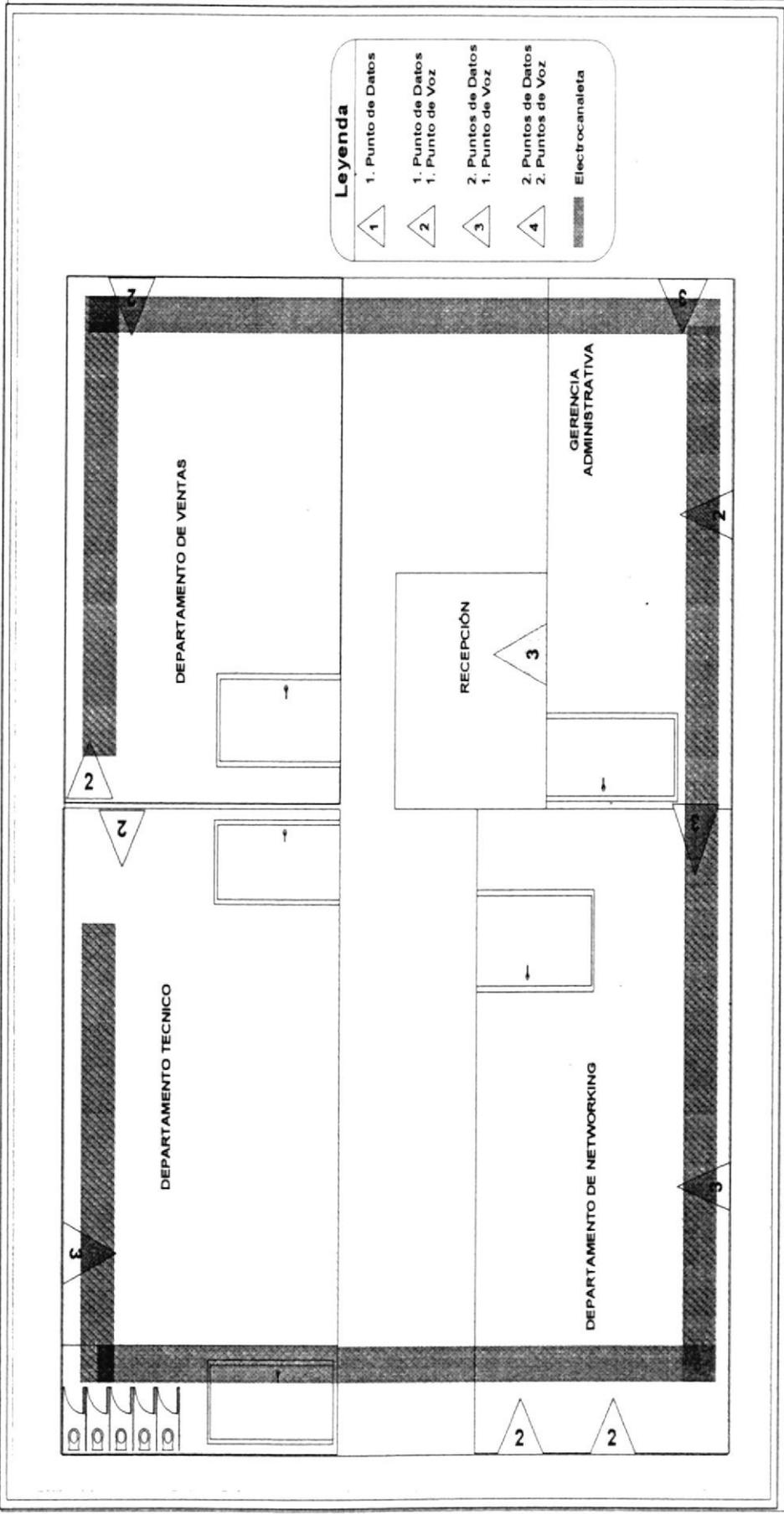


Figura 2. 34. Ambato: Análisis de Piso lógico

2.2.4.4 LOJA

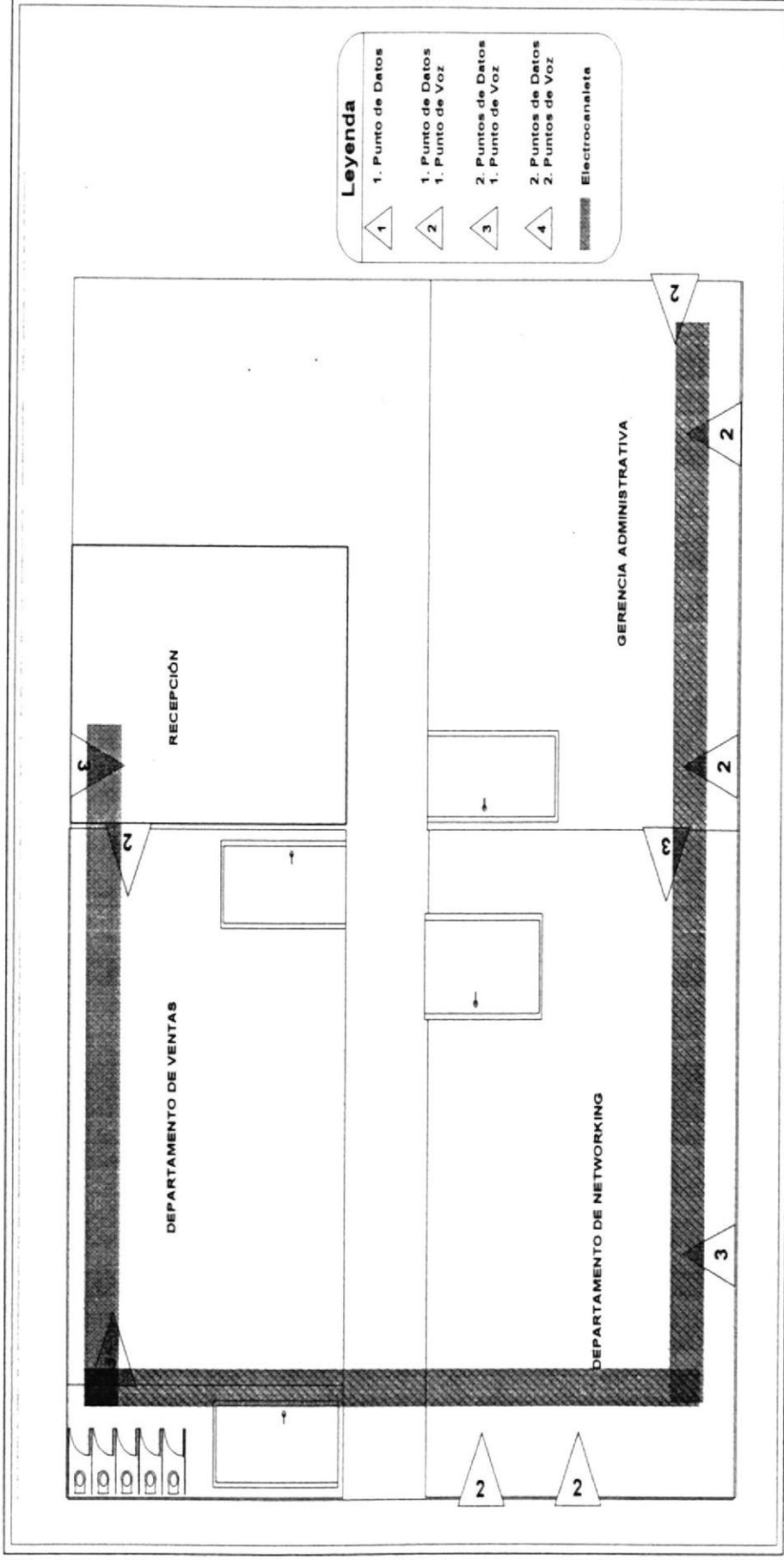


Figura 2. 35. Loja: Análisis de Piso lógico

## 2.2.5 ANÁLISIS DE PISO APLICATIVO

### 2.2.5.1 MATRIZ PLANTA BAJA

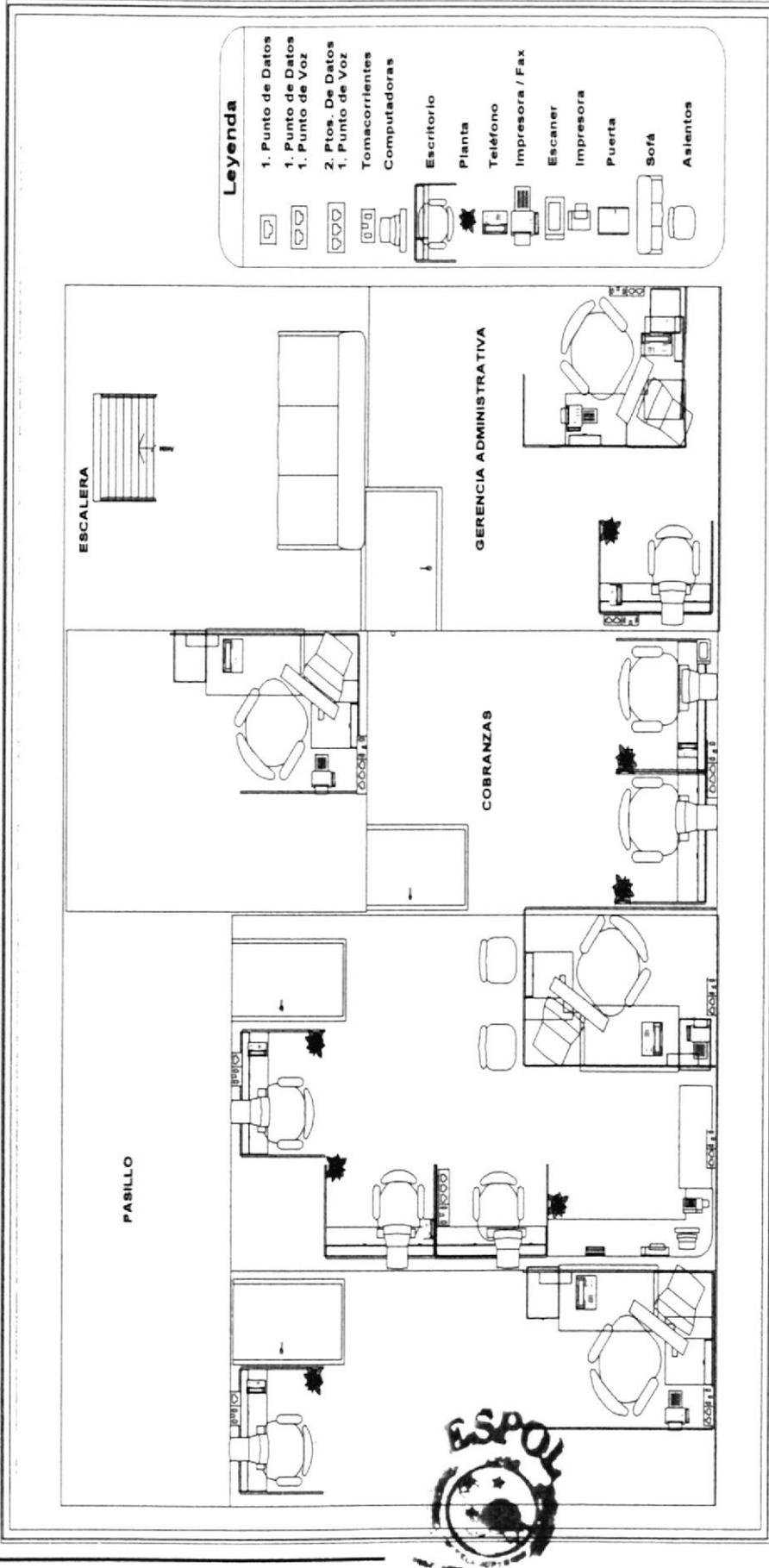


Figura 2. 36. Matriz planta baja: Análisis de Piso aplicativo



### 2.2.5.2 MATRIZ PLANTA ALTA

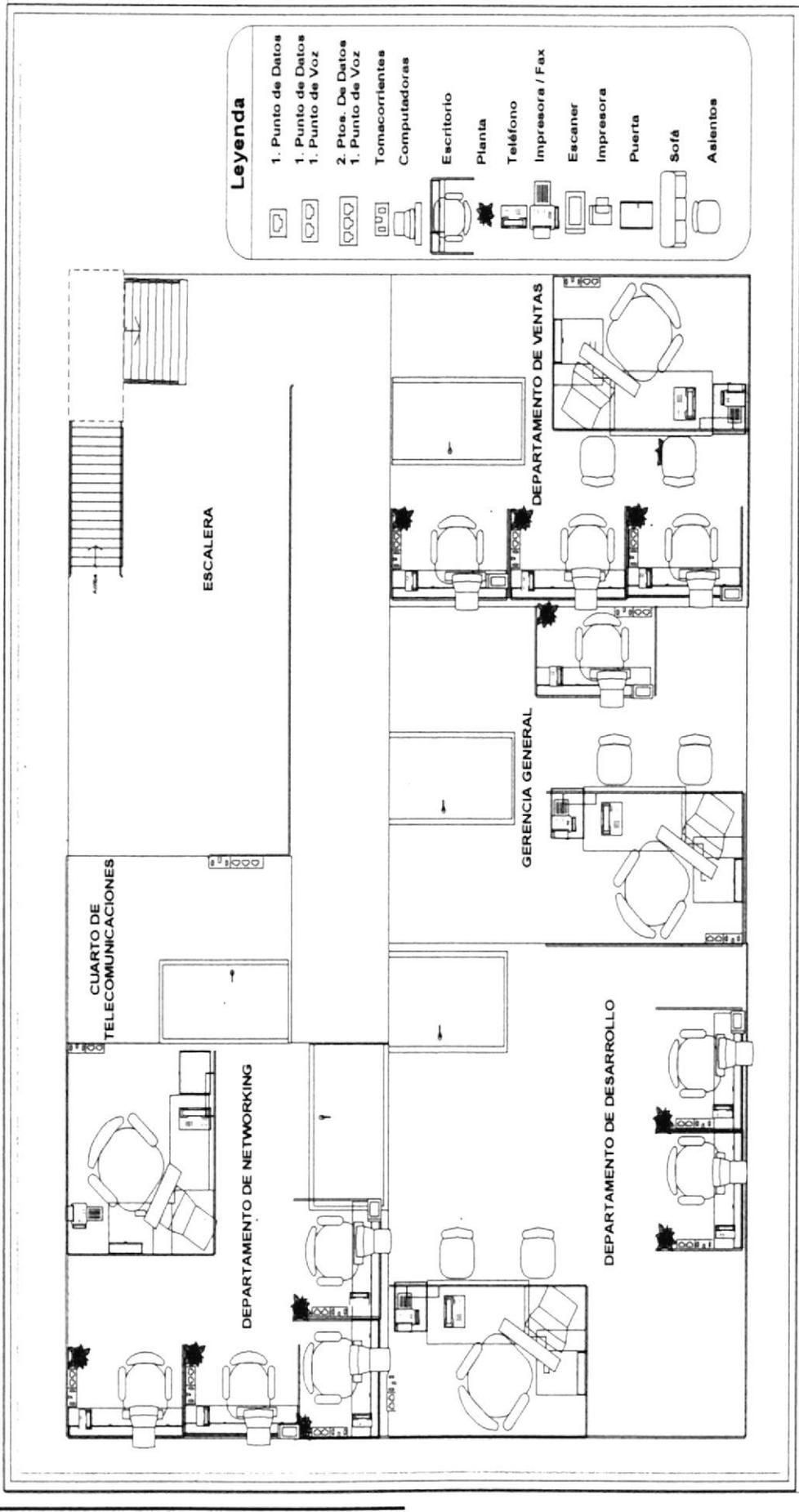


Figura 2. 37. Matriz planta alta: Análisis de Piso aplicativo



### 2.2.5.3 AMBATO

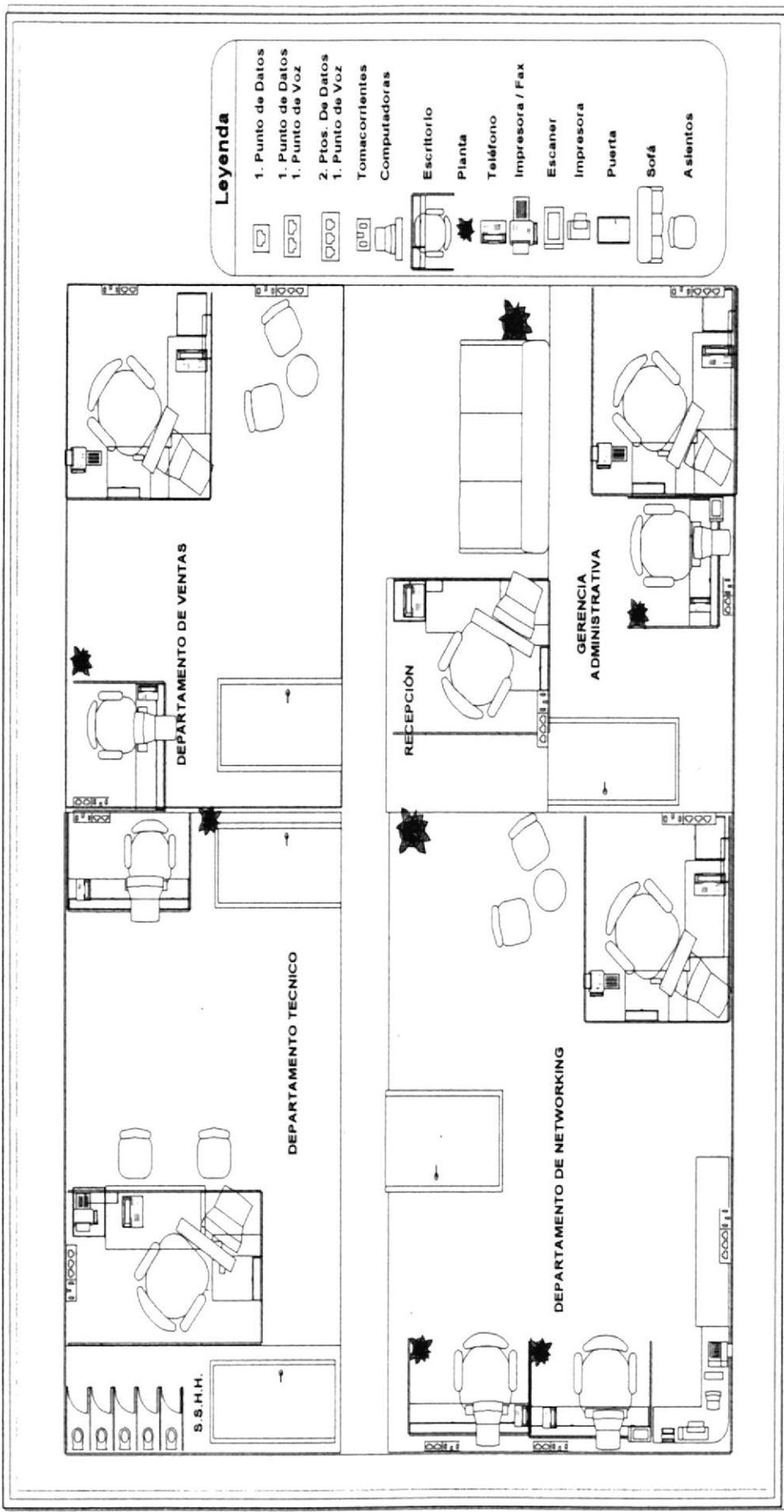


Figura 2. 38. Ambato: Análisis de Piso aplicativo

### 2.2.5.4 LOJA

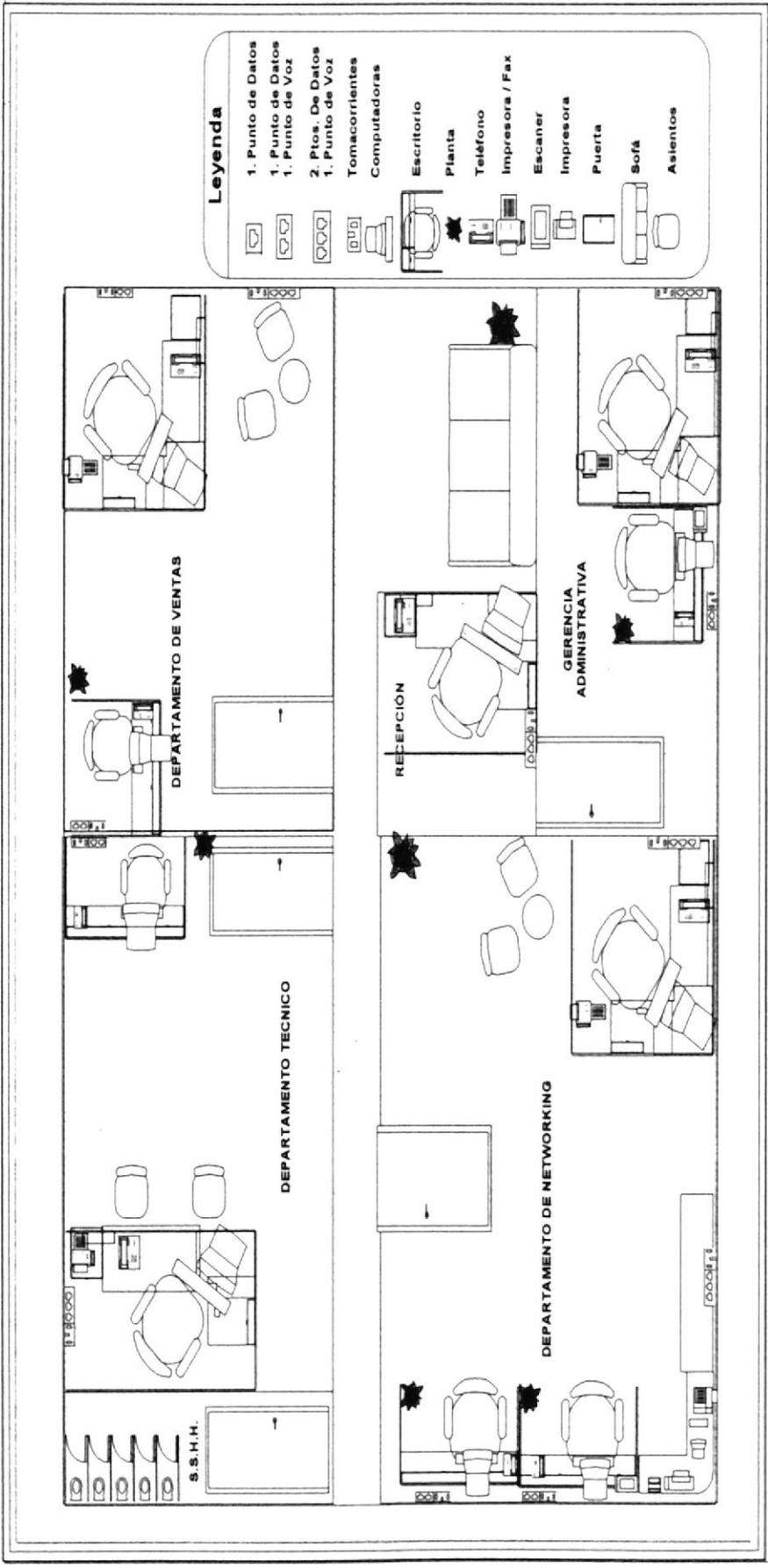


Figura 2. 39. Loja: Analisis de Piso aplicativo

## 2.2.6 MC

### 2.2.6.1 MATRIZ

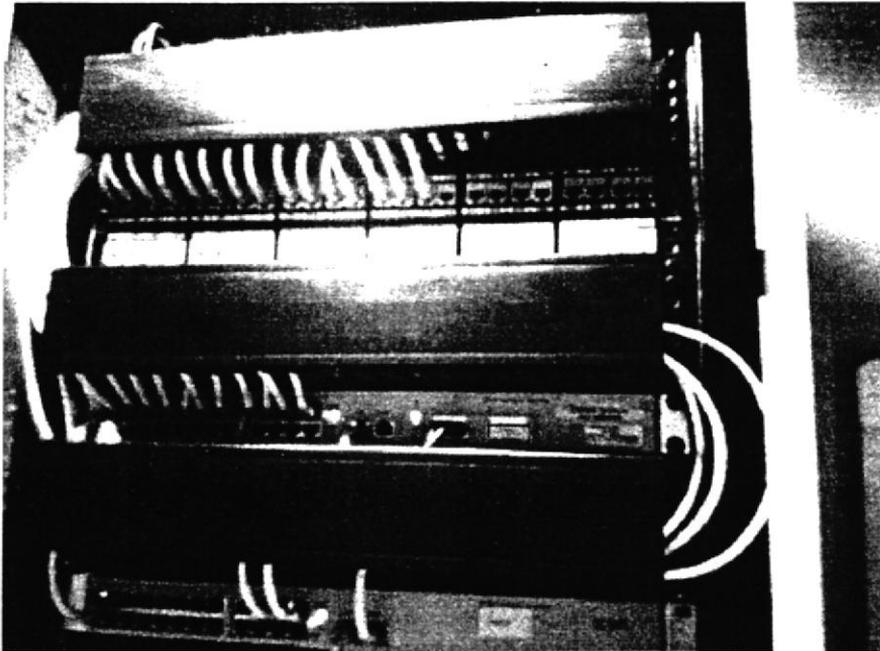


Figura 2. 40. MC Matriz

*Características Generales del MC MATRIZ del cuarto de comunicaciones:*

#### **MC de Piso Tipo Armario**

- *Ángulos Superiores de alta resistencia.*
- *Seis manejadores horizontales.*
- *Dos manejadores verticales.*
- *Puerta posterior perforada.*
- *Panel superior con perforación central.*
- *Dos ventiladores incorporados.*
- *Dos regletas de 8 tomas de energía cada una, ubicadas en la parte posterior del MC.*

2.2.6.2 GRÁFICO DEL MC

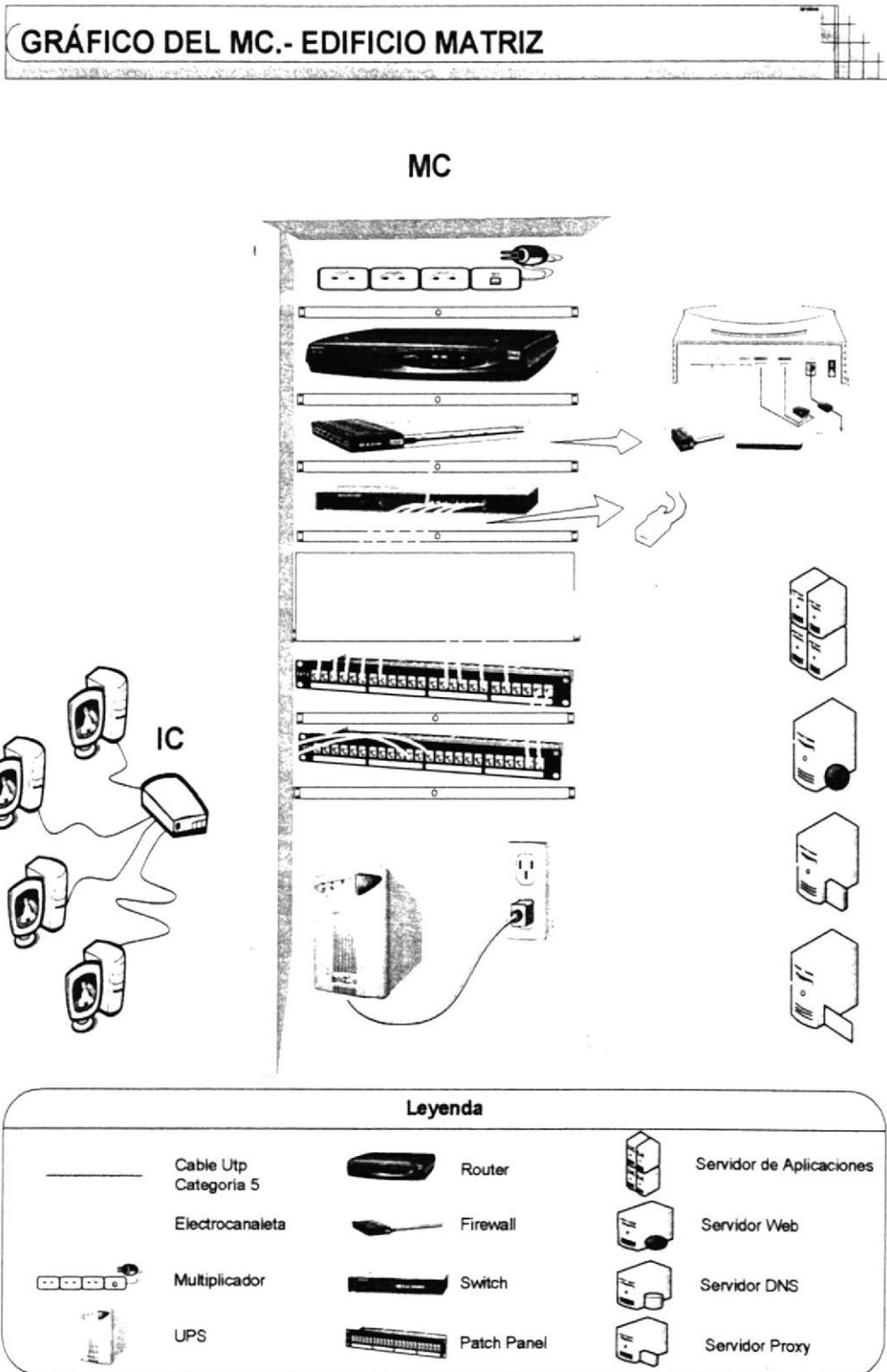


Figura 2. 41. Gráfico del MC Matriz

### 2.2.6.3 SUCURSALES: AMBATO y LOJA

#### Características Generales:

- *MC de Piso Tipo Armario.*
- *MC de 19" regulable en profundidad, deslizable adelante y atrás.*
- *Puerta fácilmente desmontable.*
- *Entradas para cable superior e inferior mediante aberturas rectangulares.*
- *Respiraderos laterales y frontales para ventilación pasiva de los componentes activos.*
- *Todos los componentes se afianzan en el MC atornillados a tuercas estándar.*
- *Cerradura con llave para protección frente a accesos no autorizados.*



Figura 2. 42. MC Sucursal Loja y Ambato

## 2.2.7 MEDIOS DE COMUNICACIÓN

### 2.2.7.1 MEDIOS ALÁMBRICOS

#### 2.2.7.1.1 MATRIZ y SUCURSALES

	<b>Medios de Comunicación</b>	<b>Cable UTP Categoría 5</b>
		Implementado en todo el edificio

Tabla. 2.7 Medios de comunicación: Alámbricos

#### Características técnicas:

- *Conductor: alambre de cobre desnudo de  $\varnothing 0,51 \pm 0,01$  mm, 24 AWG. Aislamiento: polietileno de consistencia incrementada, grosor mínimo 0,18 mm. Diámetro del cable  $0,9 \pm 0,02$  mm.*
- *Color de los pares trenzados: azul-blanco/azul, naranja-blanco/naranja, verde-blanco/verde, marrón-blanco/marrón.*
- *4 pares trenzados cubiertos con forro de PVC (grosor mínimo del forro 0.4 mm).*
- *Diámetro exterior del cable  $5,1 \pm 0,2$  mm.*
- *Temperatura máxima admisible: 75°C.*
- *Resistencia al fuego: CM.*



## 2.2.8 DISPOSITIVOS DE CONMUTACIÓN

## 2.2.8.1 MATRIZ

DISPOSITIVOS DE CONMUTACIÓN	
	<b>Tipo de Switch:</b> Switch Administrable <b>Marca :</b> D-Link <b>Cantidad:</b> 1 Switch
	<b>CARACTERÍSTICAS TÉCNICAS</b> Puertas 24 puertos 1000Base-T- Autosensing, 4 Puertas RS-232, Consola Puertas Stack 2 puertos de 10Gbps. 1000BASE-TX Operación Full Duplex. Conectores RJ-45 para las puertas 1000 BaseT, Rutas Estáticas, definida por el usuario FastEthernet : 148810 pps por puerta GigabitEthernet : 1488100 pps por puerta MAC address/ IP address
	<b>Tipo de Switch:</b> Switch D-Link 24 puertos <b>Modelo :</b> DES-1026G <b>Cantidad:</b> 2 Switchs
	<b>CARACTERÍSTICAS TÉCNICAS</b> Marca: D-Link Puertos:(24) puertos 10/100Mbps plus (2) puertos 10/100/1000Mbps MAC Address Table Size: 8,000 Switch de fábrica: 8.8Gbps Capacidad. Fuente de alimentación: 100 - 240VAC 50/60Hz, Internal Universal Power Supply. Seguridad: UL. Temperatura de operación: 32 grados - 122 grados F (0 grados - 40 grados C). Dimensiones: 44 x 20 x 4.4 cm Peso: 2.8 kg

Tabla. 2.8 Matriz: Dispositivos de conmutación

## 2.2.8.2 AMBATO

DISPOSITIVOS DE CONMUTACIÓN	
	<b>Tipo de Switch:</b> Switch D-Link 24 puertos <b>Ubicación:</b> MC SUCURSAL AMBATO <b>Modelo :</b> DES-1026G <b>Cantidad:</b> 1 Switch
	<b>CARACTERÍSTICAS TÉCNICAS</b> Marca: D-Link Puertos:(24) puertos 10/100/1000Mbps MAC Address Table Size: 8,000 Switch de fábrica: 8.8Gbps Capacidad. Seguridad: UL. Temperatura de operación: 32 grados - 122 grados F (0 grados - 40 grados C). Dimensiones: 44 x 20 x 4.4 cm Peso: 2.8 kg

Tabla. 2.9 Ambato: Dispositivos de conmutación

## 2.2.8.3 LOJA

DISPOSITIVOS DE CONMUTACIÓN		
	Tipo de Switch: Switch D-Link 24 puertos	
	Ubicación: MC SUCURSAL LOJA	
	Modelo : DES-1026G	
	Cantidad: 1 Switch	
	<b>CARACTERÍSTICAS TÉCNICAS</b>	Marca: D-Link
		Puertos:(24) puertos10/100/1000Mbps
		MAC Address Table Size: 8,000
Switch de fabrica: 8.8Gbps Capacidad.		
Seguridad: UL.		
Temperatura de operación: 32 grados - 122 grados F (0 grados - 40 grados C).		
Dimensiones: 44 x 20 x 4.4 cm		
Peso: 2.8 kg		

Tabla. 2.10 Loja: Dispositivos de conmutación



## 2.3 INFRAESTRUCTURA WAN

### 2.3.1 COMUNICACIÓN MATRIZ Y SUCURSALES

La comunicación entre ciudades está dada de la siguiente manera:



Figura 2. 43. Infraestructura WAN

#### 2.3.1.1 MATRIZ GUAYAQUIL:

La comunicación se realiza por medio del ISP Porta vía comunicación de radio con equipos de 2.4 Ghz., enlazando los equipos ubicados en las torres de Centenario, Puerto Azul, Ceibos y Samborondón, para que de esta forma el Servicio de Internet Inalámbrico proporcionado por Epsilon pueda tener cobertura en ciertos sectores de Guayaquil

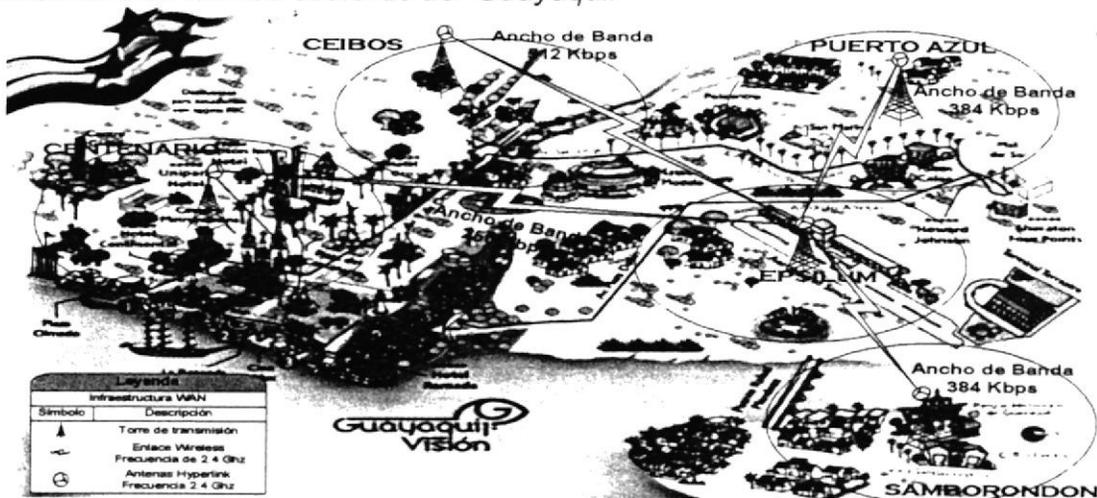


Figura 2. 44. Infraestructura MAN – Guayaquil

### 2.3.1.2 SUCURSAL 1.- LOJA

La comunicación con la Matriz se realiza por medio de ISP Porta vía comunicación de radio con equipos de 2.4 Ghz

El servicio de Internet se distribuye a los clientes por medio de la infraestructura física de Epsilon ubicada al Norte y Sur de la Ciudad.

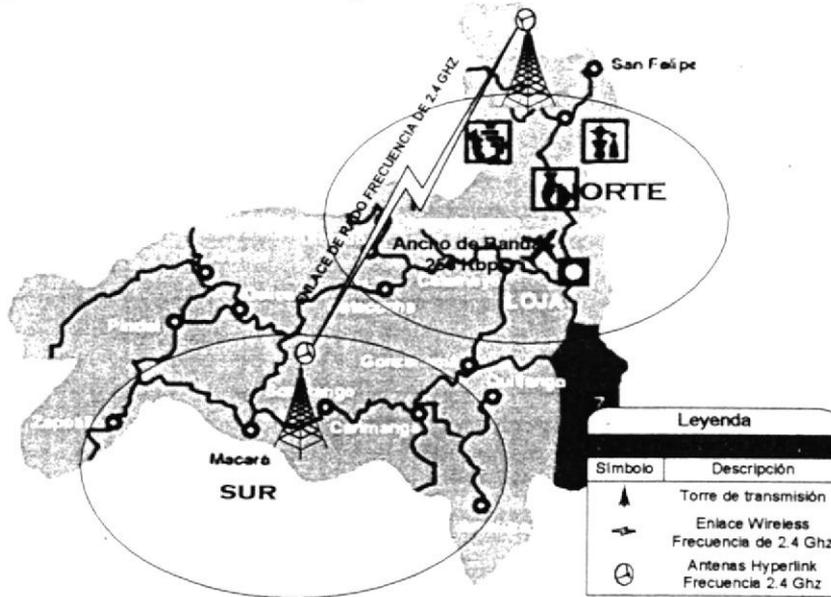


Figura 2. 45. Infraestructura MAN – Loja

### 2.3.1.3 SUCURSAL 2.- AMBATO

La comunicación con la Matriz se realiza por medio de Epsilon quien a la vez se enlaza con el ISP Porta.

El servicio de Internet se distribuye a los clientes por medio de la infraestructura física de Epsilon ubicada al Centro y Sur de la Ciudad.

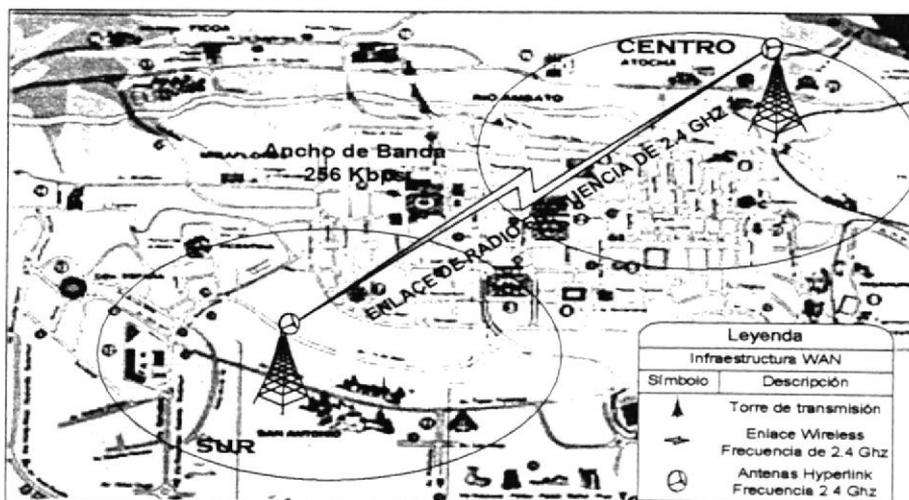


Figura 2. 46. Infraestructura MAN – Ambato

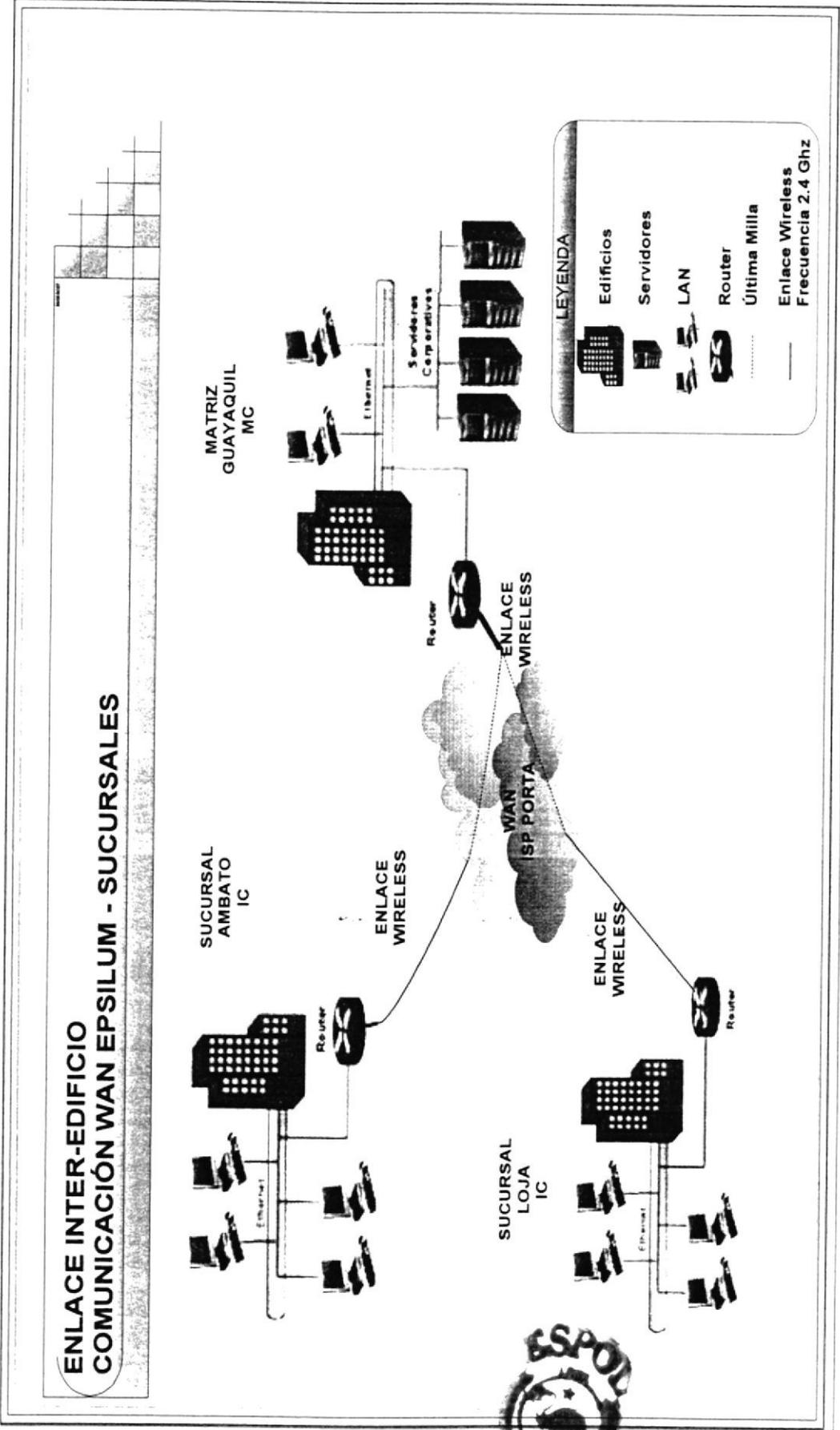


Figura 2. 47. Enlace Inter-edificio Epsilon S.A.



## 2.3.2 DISPOSITIVOS DE ENRUTAMIENTO

Epsilon posee 9 routers Cisco 1700 con las siguientes características:

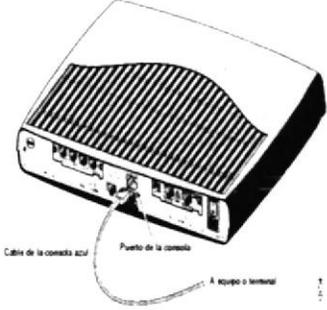
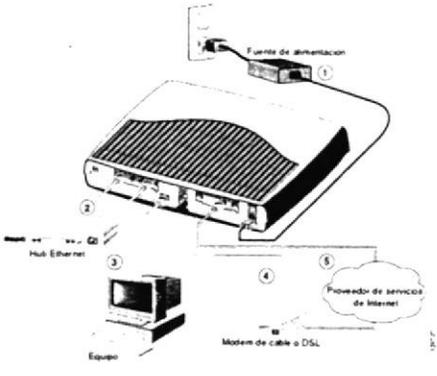
DISPOSITIVOS DE ENRUTAMIENTO		
	<b>Tipo de Dispositivo :</b> Routers	
	<b>Marca :</b> Cisco	
	<b>Modelo:</b> Cisco 1700	
	<b>Cantidad:</b> 9 Routers	
	<b>CARACTERÍSTICAS TÉCNICAS</b>	Encaminamiento y seguridad avanzadas al conectar con el Internet usando un módem de banda ancha
		Conmutación integrada
		Servicios de voz integrados
		VPN-Alambre-velocidad de alto rendimiento VPN con cifrado del hardware
		Servicios integrados de red inalámbrica.
		Alta disponibilidad
		Content Networking
		Servicios de seguridad integrados
<b>Ubicación:</b>		
		Matriz Guayaquil
	Celda Centenario	
	Celda Puerto Azul	
	Celda Celbos	
	Celda Samborondon	
	Sucursal Ambato	
	Celda San Antonio	
	Sucursal Loja	
	Celda Macará	

Tabla. 2.11 Dispositivos de Enrutamiento

### 2.3.2.1 COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS

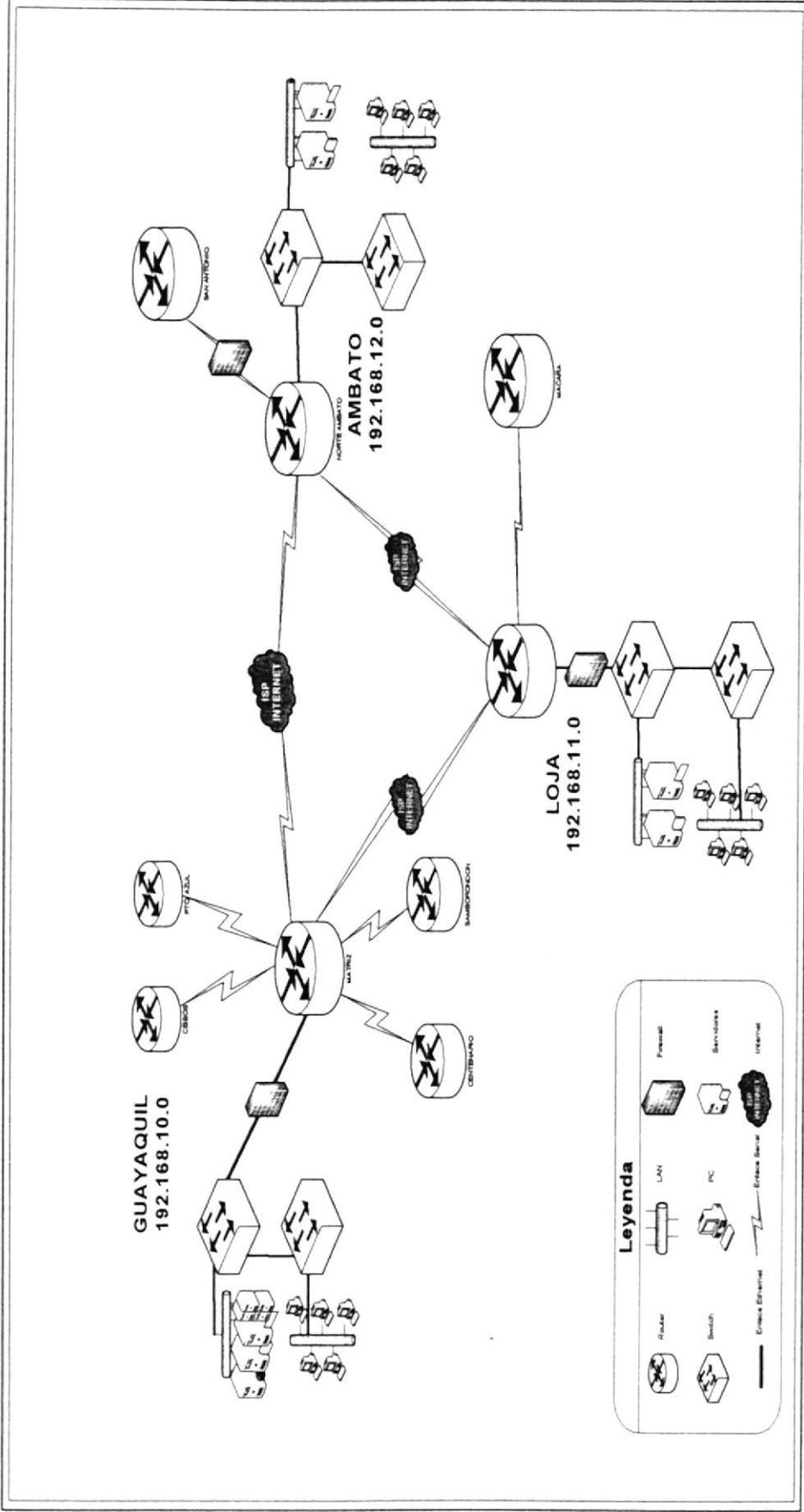


Figura 2. 48. Comunicación WAN a nivel de dispositivos



### 2.3.3 MEDIOS DE COMUNICACIÓN:

#### 2.3.3.1 MEDIOS INALÁMBRICOS

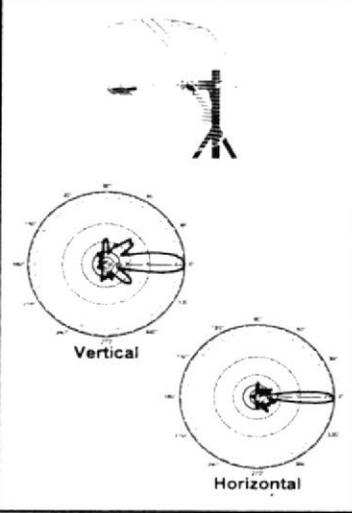
	<b>Tipo de Dispositivo :</b>	<b>Antenas</b>	
	<b>Marca :</b>	<b>Antena de 24 dBi HyperLink 2.4 GHz Wireless LAN WIFI</b>	
	<b>Modelo:</b>	<b>Antenas de 2.4 dBi</b>	
	<b>CARACTERÍSTICAS TÉCNICAS</b>		Telefonía por IP (VOIP).
			Vigilancia y monitoreo remoto , cámaras IP . Proveer servicios de internet inalámbrico (ISP Inalámbrico).
			Frecuencia : 2.4 - 2.5 GHZ
			Ganancia: 24 dBi
			3 dBi Ancho de onda : 8 grados
			Respuesta polarización cruzada : 26 dBi
			Impedancia : 50 Ohm
	Peso : 4.8 lbs. (2.18 kg)		
	Montage : 2 in. (50.8 mm) max.		
	Temperatura de operación : (-40° F to 185° F)		
	Angulo de elevación: -40° C to to 85° C		

Tabla. 2.12 Medios Inalámbricos

### 2.3.3.1.1 COMUNICACIÓN WAN A NIVEL DE MEDIOS

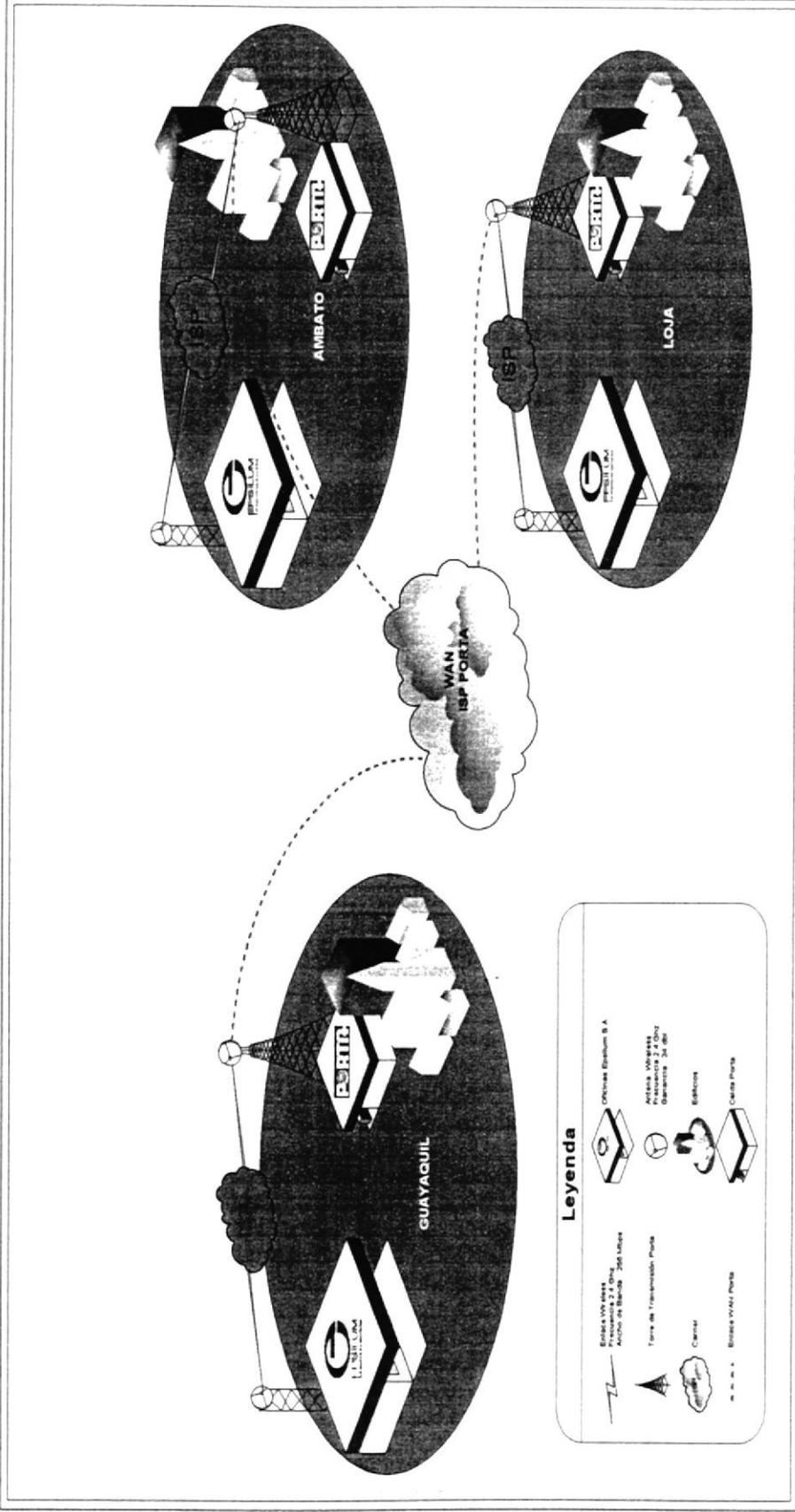


Figura 2. 49. Comunicación WAN a nivel de medios



### 2.3.3.2 INFRAESTRUCTURA DE TELECOMUNICACIONES



**Figura 2. 50.** Torres de Porta

La infraestructura de telecomunicaciones que utiliza Epsilum S.A. para proveer el Servicio de Internet inalámbrico en las ciudades de Guayaquil, Ambato y Loja es la siguiente:

- Torres de Porta.
- Antenas Wireless Omnidireccionales con frecuencia de 2.4 Ghz.
- Antenas Wireless Unidireccionales con frecuencia 2.4 Ghz
- Servidor Linux.
- Routers Cisco 1700.
- Tsunami Power Suplí.

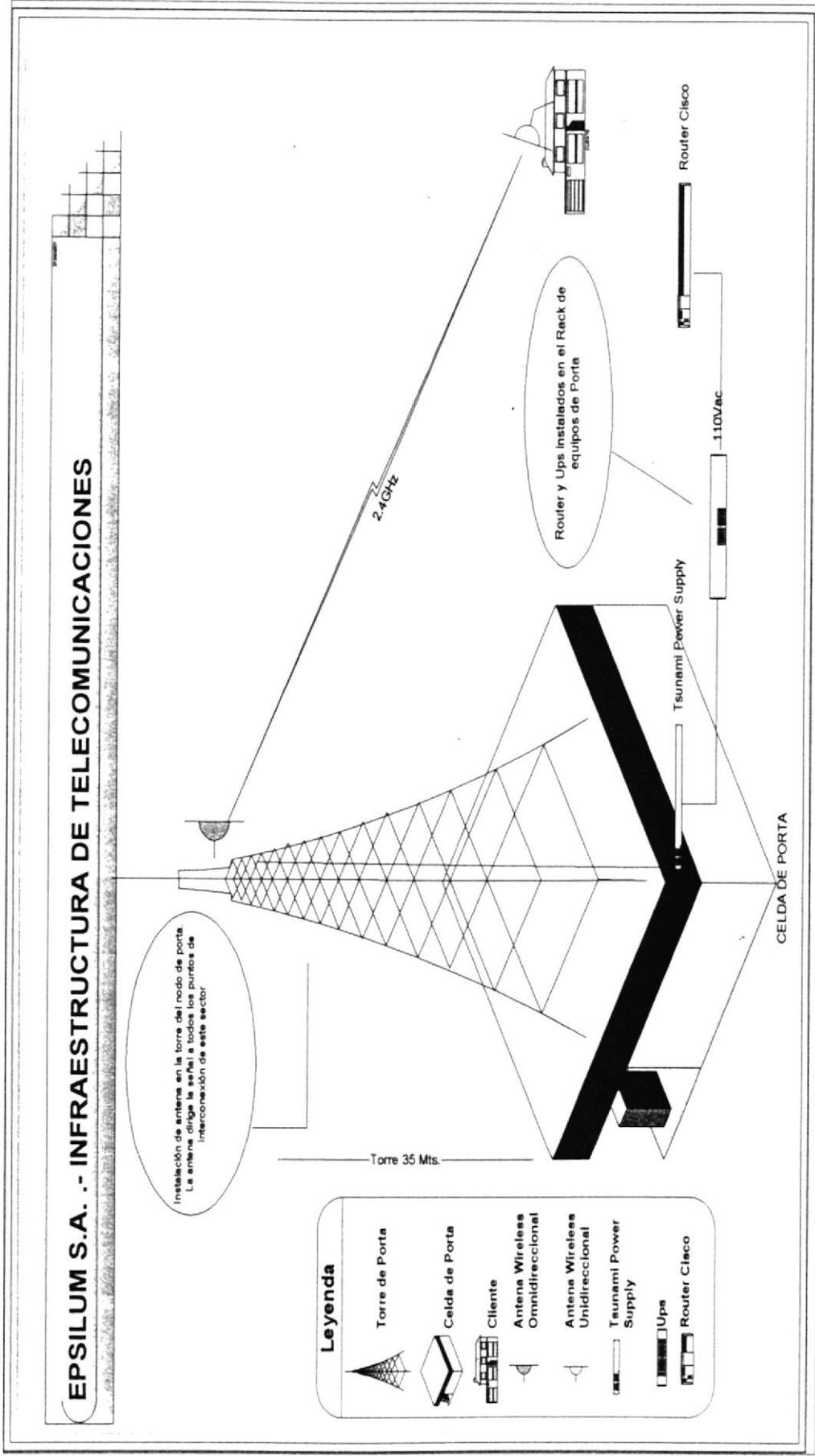


Figura 2. 51. Infraestructura de Telecomunicaciones

## 2.4 SEGURIDADES

### 2.4.1 EDIFICIO MATRIZ Y SUCURSALES

Los dispositivos de seguridad físicos y lógicos con los que actualmente cuenta Epsilon S.A. son los siguientes:

#### Físicos:

- ↓ Firewall D-Link DFL – 700



Figura 2. 52. Firewall D-LINK

#### Características principales:

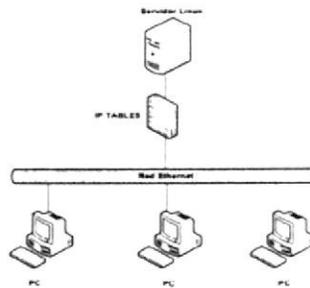
- El DFL-700 de D-Link es un firewall de fácil uso, diseñado para pequeñas, medianas empresa y grupos de trabajo.
- Integra traducción de dirección de red (NAT),
- Firewall
- Filtrado de contenido
- Protección IDS
- Gestión del ancho de banda y soporte de red privada virtual (VPN).
- Incluye soporte de enlace WAN, puerto LAN de confianza y puerto DMZ para correo electrónico local y servidores Web.

	<b>Ubicación:</b> Edificio Matriz y Sucursales <b>Marca:</b> D-Link <b>Modelo:</b> DFL-700 <b>Cantidad:</b> 3
	<b>CARACTERÍSTICAS TÉCNICAS</b> Firewall de 47Mbps rendimiento 1 puerta WAN, 1 puerta DMZ y 1 LAN Soporte hasta 10000 sesiones concurrentes Soporte de hasta 200 túneles VPNs. Administración del ancho de banda Filtrado de contenido

Tabla. 2.13 Firewall matriz y sucursales

Lógicos:

↓ **Servidor Linux Fedora Core 3**



**Figura 2. 53.** Gráfico de Servidor Linux

La empresa cuenta con un servidor Linux, en cual se ha configurado la herramienta de Firewall el mismo que previene ataques de usuarios no autorizados, y a la vez realiza una inspección del tráfico entrante y saliente. Esto impide que servicios o dispositivos no autorizados accedan a ciertos recursos y de esta manera protegerse contra ataques de denegación de servicios por ejemplo (DoS).

↓ **Antivirus Symantec Norton Antivirus 2006**

**Características principales.**

- Detección automática de virus, troyanos y gusanos.
- Detección y borrado de spyware y software de monitorización no deseado.
- Análisis de ficheros adjuntos en correos electrónicos y mensajería instantánea.
- Chequeo de ficheros comprimidos.
- Bloqueo de la entrada de gusanos desde Internet.



### 2.4.2 NIVEL DE SEGURIDAD - EDIFICIO MATRIZ

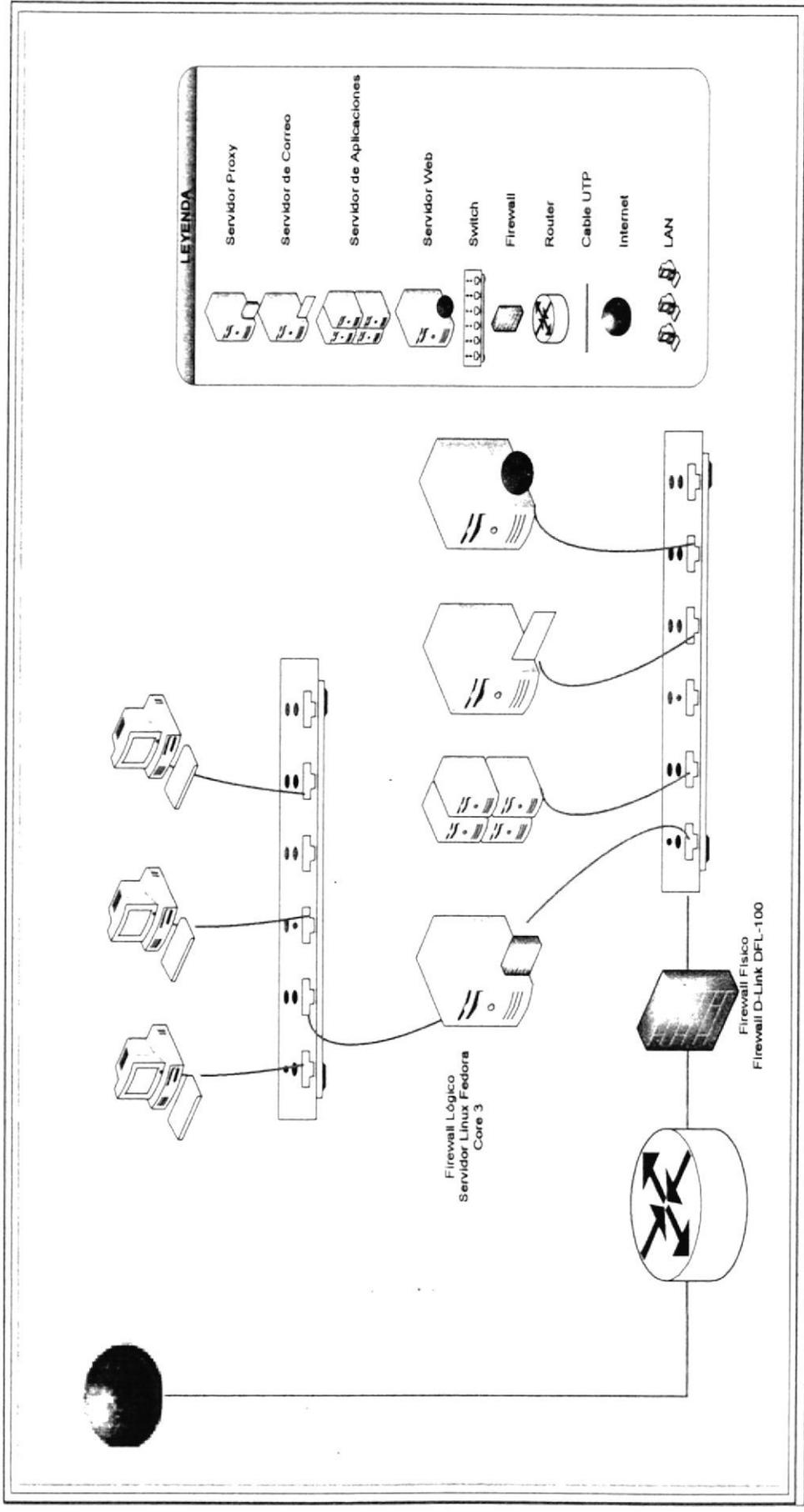


Figura 2. 54. Edificio Matriz. - Firewalls Físicos y Lógicos

### 2.4.3 NIVEL DE SEGURIDAD.- SUCURSALES AMBATO Y LOJA

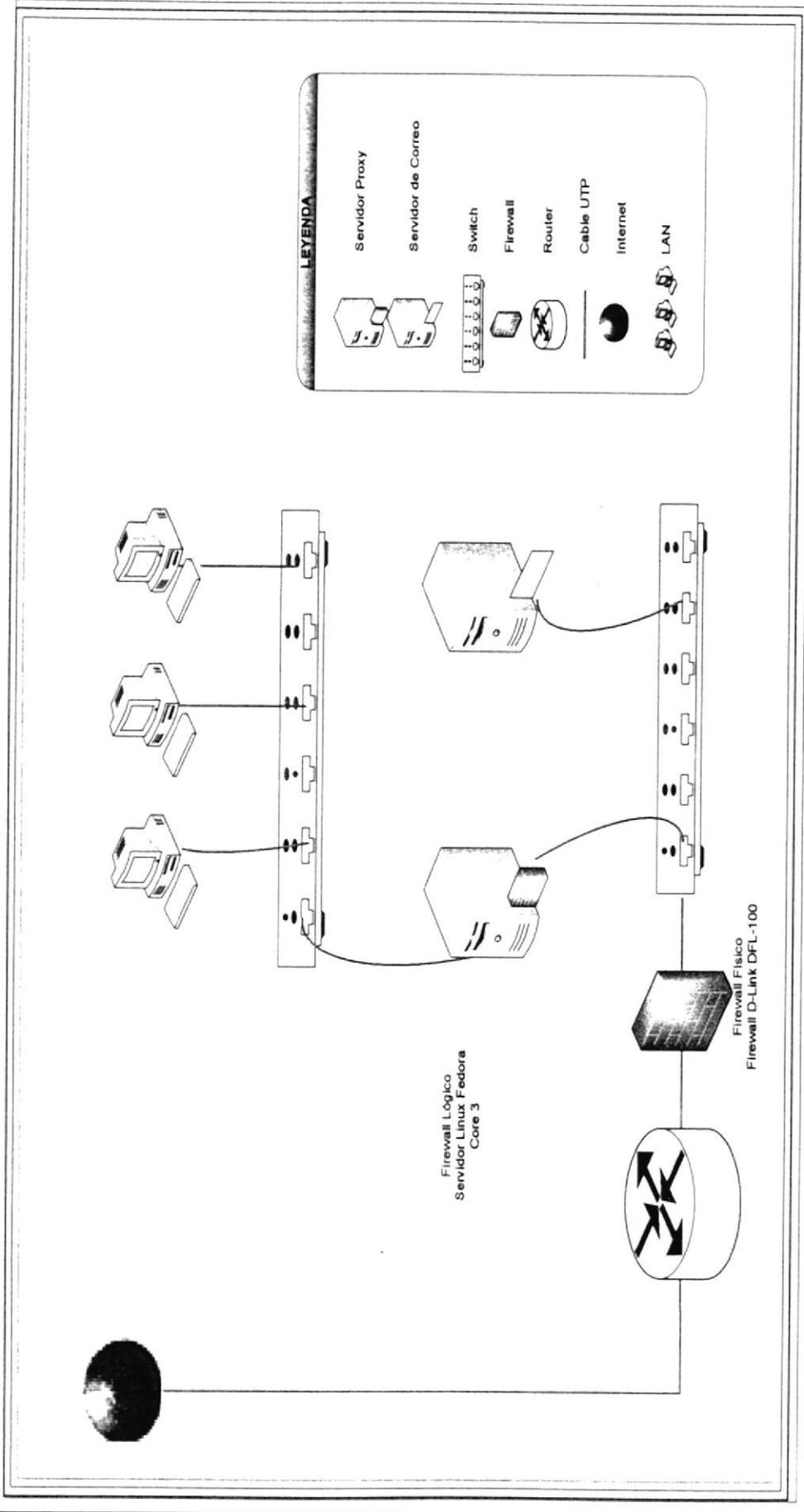


Figura 2. 55. Sucursales Ambato y Loja.- Firewalls Físicos y Lógicos

## 2.5 INTERNET

### 2.5.1 ACCESO A INTERNET Y ANCHO DE BANDA

El acceso a Internet se realiza por medio del ISP (PROVEEDOR DE SERVICIOS DE INTERNET), Epsilon mantiene un contrato con PORTA para que les provean del ancho de banda necesario para ofrecer a sus clientes el Servicio de Internet Inalámbrico, en el contrato Porta se compromete a:

- Prestar el servicio de internet ininterrumpidamente.
- Alquilar las Torres de Porta para colocar los equipos, y poder proveer el Servicio de Internet Inalámbrico a los hogares.
- Conectar las 2 sucursales: Ambato y Loja.
- Transmisión de datos continúa.

Epsilon cuenta con un Ancho de Banda de 1.054 Mbps que están distribuidos de la siguiente forma:

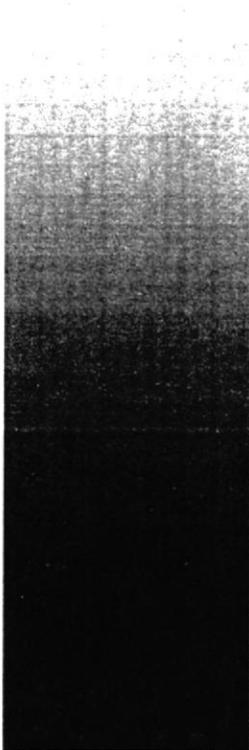
<b>ANCHO DE BANDA ASIGNADOS POR SECTOR</b>			
EPSILUM	512 Kbps	SAMBORONDON	384 Kbps
CENTENARIO	256 Kbps	MACARA	256 Kbps
PUERTO AZUL	384 Kbps	LOJA	384 Kbps
CEIBOS	512 Kbps	AMBATO	256 Kbps

**Tabla. 2.14** Ancho de Banda asignado por sector



## **2.6 PROBLEMAS ENCONTRADOS**

- *La empresa no cuenta con cableado estructurado.*
- *Saturación del Servidor de Correo.*
- *Falta de Ancho de Banda de Internet.*
- *No existen medios de comunicación de respaldo a nivel WAN.*
- *Falta de software para monitoreo de los enlaces (WAN) y de la red (LAN).*
- *Ups y reguladores operando al 30% de su capacidad.*



## CAPÍTULO 3

---

# SOLUCIÓN PROPUESTA

### 3. PROPUESTA

#### 3.1 PROBLEMAS ENCONTRADOS

Mediante un análisis efectuado y de acuerdo a los datos recopilados, producto de la observación y de una entrevista directa con las personas involucradas, hemos podido determinar los problemas departamentales que se están suscitando en este momento en la empresa los cuales se procede a detallar a continuación:

<b>PROBLEMA</b>	<b>CAUSA</b>	<b>EFECTO</b>
<ul style="list-style-type: none"> <li>▪ <b>La empresa no cuenta con cableado estructurado.</b></li> </ul>	<ul style="list-style-type: none"> <li>▪ Falta de electro-canaletas.</li> <li>▪ Los cables del MC no se encuentran etiquetados.</li> <li>▪ Los cables se encuentran expuestos en el área de trabajo.</li> <li>▪ Los dispositivos de enrutamiento y conmutación no se encuentran bien ubicados en el M.C.</li> <li>▪ La red no esta documentada.</li> <li>▪ Acceso a Cuarto de telecomunicaciones no se encuentra restringido.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Cables expuestos a interferencias electromagnéticas</li> <li>▪ Pérdida de tiempo al momento de identificar problemas en la red (cables, switches, routers.)</li> <li>▪ Acceso de personas no autorizadas al Cuarto de Telecomunicaciones quienes desconfiguran los equipos de la empresa.</li> <li>▪ No se pueden compartir recursos con algunos usuarios de la red.</li> </ul>
<ul style="list-style-type: none"> <li>▪ <b>Saturación del Servidor de Correo.</b></li> </ul>	<ul style="list-style-type: none"> <li>▪ El Servidor de correo no cumple con requerimientos de Hardware y Software necesarios para un óptimo rendimiento.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Los servicios que brinda el servidor se congestionan y llegan a colapsar la red.</li> <li>▪ Inconformidad de los usuarios.</li> </ul>

- |                                                                                                                                     |                                                                                                                                                           |                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ <b>Falta de Ancho de Banda de Internet.</b></li> </ul>                                     | <ul style="list-style-type: none"> <li>▪ La empresa no contaba con presupuesto para contratar un mayor ancho de banda.</li> </ul>                         | <ul style="list-style-type: none"> <li>▪ Inconformidad por parte de los usuarios (Navegación lenta).</li> </ul>                                                                                                                                |
| <ul style="list-style-type: none"> <li>▪ <b>No existen medios de comunicación de respaldo a nivel WAN.</b></li> </ul>               | <ul style="list-style-type: none"> <li>▪ La empresa no ha invertido en ningún medio de transmisión de respaldo.</li> </ul>                                | <ul style="list-style-type: none"> <li>▪ Cuando falla el enlace principal, la empresa no se puede conectar con las sucursales.</li> </ul>                                                                                                      |
| <ul style="list-style-type: none"> <li>▪ <b>Falta de software para monitoreo de los enlaces (WAN) y de la red (LAN).</b></li> </ul> | <ul style="list-style-type: none"> <li>▪ Desconocimiento por parte del departamento encargado de este tipo de software.</li> </ul>                        | <ul style="list-style-type: none"> <li>▪ Falta de control cuando existe pérdida de comunicación en alguno de los enlaces.</li> <li>▪ Saturación de la red por parte de los usuarios del Servicio de Internet (exceso de descargas).</li> </ul> |
| <ul style="list-style-type: none"> <li>▪ <b>Ups y reguladores operando al 30% de su capacidad.</b></li> </ul>                       | <ul style="list-style-type: none"> <li>▪ UPS y reguladores antiguos que no abastecen los servidores y dispositivos de comunicación conectados.</li> </ul> | <ul style="list-style-type: none"> <li>▪ No se tiene un respaldo de energía de óptimo rendimiento y protección para el equipamiento electrónico, ante un eventual corte de energía, lo que ocasiona daños en los servidores.</li> </ul>        |

Tabla. 3.1 Problemas encontrados

## 3.2 SOLUCIÓN PROPUESTA

PROBLEMA	SOLUCIÓN	ALCANCE
<p>1. <b>La empresa no cuenta con cableado estructurado.</b></p>	<ul style="list-style-type: none"> <li>▪ Implementación y adecuación del cableado estructurado con sus respectivas normas y estándares, así como efectuar la respectiva documentación de la red, restringir el acceso al Cuarto de Telecomunicaciones</li> </ul>	<ul style="list-style-type: none"> <li>▪ La empresa contará con un mejor control en la infraestructura del cableado estructurado.</li> <li>▪ Mejor administración de las redes y de los equipos de comunicación.</li> </ul>
<p>2. <b>Saturación del Servidor de Correo.</b></p>	<ul style="list-style-type: none"> <li>▪ Actualización de hardware y software del servidor de correo con las últimas tecnologías y seguridades.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Servidor de Correo óptimo y con mejores tiempos de respuesta acorde a los requerimientos de los usuarios.</li> <li>▪ Mayor eficiencia y confiabilidad en el servicio.</li> </ul>
<p>3. <b>Falta de Ancho de Banda de Internet.</b></p>	<ul style="list-style-type: none"> <li>▪ Contratar con un proveedor (ISP) un ancho de banda de 1.024 kbps y segmentarlo por zonas según el número de usuario, efectuar un análisis del posible incremento de usuarios donde se brinda el servicio de Internet.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Mejor administración del ancho de banda de Internet, lo que se reflejará en una mayor satisfacción de los clientes.</li> </ul>

<p><b>4. No existen medios de comunicación de respaldo a nivel WAN.</b></p>	<ul style="list-style-type: none"> <li>▪ Contratar con un proveedor (ISP), un enlace de fibra óptica para el Edificio Matriz y sus dos sucursales el cuál pasaría a ser el enlace principal y como enlace de respaldo implementaremos individualmente un enlace wireless para datos y otro para Internet.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Comunicación constante entre el edificio matriz y las sucursales.</li> </ul>
<p><b>5. Falta de software de monitoreo de los enlaces (WAN) y de la red (LAN).</b></p>	<ul style="list-style-type: none"> <li>▪ Adquisición de un Software de monitoreo de red que permita una administración más eficiente de los recursos en la red.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Este Software permitirá efectuar un constante control de la red, y proporcionará información útil para el análisis de enlaces y dispositivos de red.</li> </ul>
<p><b>6. Ups y reguladores operando al 30% de su capacidad.</b></p>	<ul style="list-style-type: none"> <li>▪ Adquisición de UPS con nuevas tecnologías que reemplacen a los existentes.</li> </ul>	<ul style="list-style-type: none"> <li>▪ La empresa contará con un respaldo de energía de óptimo rendimiento y protección.</li> </ul>

**Tabla. 3.2** Solución Propuesta

### 3.3 ESTUDIOS DE FACTIBILIDAD

#### 3.3.1 ALTERNATIVA: A

El objetivo principal de esta alternativa es implementar cableado estructurado y establecer un Enlace Backup en el edificio Matriz y en las dos Sucursales (Ambato y Loja), siendo esta alternativa la más conveniente ya que se implementarán equipos eficientes y de marcas reconocidas.

##### 3.3.1.1 FACTIBILIDAD TÉCNICA

###### 3.3.1.1.1 DISPOSITIVOS DE ENRUTAMIENTO

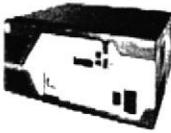
Cant.	Equipo	Descripción	Ubicación	Uso
3	Cisco 2821 <b>Integrated Services Router</b> 	<b>General</b> Tipo de dispositivo: Encaminador Factor de forma: Externo - modular - 2U Factor de forma: Externo - modular - 2U Profundidad: 41.7 cm Profundidad: 41.7 cm Anchura: 43.8 cm Altura: 8.9 cm Peso: 11.4 kg Peso: 11.4 kg <b>Memoria</b> Tecnología de conectividad: Cableado Protocolo de interconexión de datos: Ethernet, Fast Ethernet, Gigabit Ethernet Red / Protocolo de transporte: IPSec Protocolo de gestión remota: SNMP 3 Indicadores de estado: Actividad de enlace, alimentación Características: Protección firewall, VPN, Cumplimiento de normas: IEEE 802.3af <b>Interfaces:</b> 2 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x USB 1 x gestión - consola 1 x red - auxiliar	1 Edificio Matriz 1 Sucursal Loja 1 Sucursal Ambato	Dispositivo de Enrutamiento
3	Placa CISCO WS-G5486 GBIC fibra óptica Gigaethernet 	<b>Data Transfer Rate</b> 1000 Mbps <b>Interface Converter Module Type</b> GBIC <b>Cabling Type</b> Ethernet 1000Base-LH • Ethernet 1000Base-LX	1 Edificio Matriz 1 Sucursal Loja 1 Sucursal Ambato	Dispositivo de Enrutamiento

Tabla. 3.3 Alternativa A: Dispositivos de enrutamiento

## 3.3.1.1.2 DISPOSITIVOS DE CONMUTACIÓN

Cant.	Equipo	Descripción	Ubicación	Uso
2	Switch Cisco 2950 	<b>Fabricante</b> Cisco <b>Serie</b> WS-C3508G-XL-EN <b>Tipo de Dispositivo</b> Switch 8 MB DRAM, 4 MB Flash <b>Memoria</b> Memory <b>Número de Puertos:</b> 24 <b>Vel. de transmisión</b> 1000 Mbps <b>Protocolos de</b> Telnet, - CWSI - Web-based interface <b>Modo de Comunicación</b> Full-Duplex, Half-Duplex <b>Características</b> Manageable, stackable  <b>Interfaces</b> 8 x GBIC Module Expansion Slots 1 x RJ-45 Console (Management)	1 Sucursal Loja 1 Sucursal Ambato	Administración de VLAN's

Tabla. 3.4 Alternativa A: Dispositivos de Conmutación

## 3.3.1.1.3 MEDIOS DE COMUNICACIÓN

Cant.	Equipo	Descripción	Ubicación	Uso
600 mts	Fibra Óptica Multimodo	<b>Marca:</b> Genérico <b>Número de Hilos</b> 12 Hilos <b>Transmisión:</b> 1000 Mbps	150 mts 250 mts 200 mts	Enlace Principal

Tabla. 3.5 Alternativa A: Medios de comunicación

## 3.3.1.1.4 EQUIPOS

Cant.	Equipo	Descripción	Ubicación	Uso
3	Disco Duro de 120 Gb	<b>Modelo</b> IBM	1 Matriz	Actualización de Servidor de Correo
3	Memoria Ram 512 Mb	<b>Marca:</b> IBM	1 Sucursal Loja 1 Sucursal Ambato	
3	UPS POWERWARE 5125 	<b>Modelo</b> POWERWARE 5125 <b>Características</b> Administrador Avanzado de Energía duplica la vida útil de las baterías. <b>Control de segmentos de carga</b> Permite programar grupos de tomacorrientes para apagados programados <b>Supresor de Transientes :</b> Protege a los PC's, servidores, switches, ruteadores de voltajes transientes que viajan por el cableado de red y línea telefónica. <b>Garantía:</b> 2 años de garantía.	1 Matriz 1 Sucursal Loja 1 Sucursal Ambato	Administración de Energía

Tabla. 3.6 Alternativa A: Equipos

## 3.3.1.1.5 CABLEADO ESTRUCTURADO

Cant.	Equipo	Descripción	Ubicación	Uso
17	Bobinas Cat.6 305 mts.	Marca: Genérico Cable: UTP Categoría: 6 Velocidad de Transmisión: 10/100/1000 Mbps Ancho de Banda: 200 Mhz	Matriz Sucursal Loja Sucursal Ambato	Cableado General
50	Patch Cord	Marca: Genérico	Matriz Sucursal Loja Sucursal Ambato	Cableado General
408	Conectores Rj-45	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General
200	Jack	De Presión: 100 Jack De Impacto: 100 Jack Marca: Genérico	Matriz Sucursal Loja Sucursal Ambato	Cableado General
16 Mtrs	Canaletas Decorativas	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General
2	Cintas Velcro	Marca: Genérico	Matriz	Cableado General
5	Paquetes de sticker para la identificación de los puntos de red	Marca: Genérico Marca: Genérico	Sucursal Loja Sucursal Ambato	
10	Organizadores Verticales	Marca: Genérico	Matriz	
571	Amarras	Marca: Genérico	Suc. Loja y Ambato Suc. Loja y Ambato	Cableado General
36	Codos	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General
10	Face Plate	3 Servicios: 5 2 Servicios: 3 1 Servicio: 2	Matriz Sucursal Loja Sucursal Ambato	Cableado General
10	Cajas Sobrepuestas	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General

Tabla. 3.7 Alternativa A: Cableado Estructurado

## 3.3.1.2 FACTIBILIDAD ECONÓMICA

## 3.3.1.2.1 COSTOS DE HARDWARE

**Cableado Estructurado**

Cant.	Detalle	Precio Unitario	Costo Total
17	Bobinas Cat.6 305 mts.	\$ 105,00	\$ 1.785,00
50	Patchs Cords	\$ 5,00	\$ 250,00
408	Conectores Rj-45	\$ 0,30	\$ 122,40
200	Jack de Impacto	\$ 1,34	\$ 268,00
16 Mtrs	Canaletas Decorativas calibre 20	\$ 42,00	\$ 672,00
5	Amarras (fundas de 100)	\$ 5,50	\$ 27,50
2	Cinta velcro	\$ 15,00	\$ 30,00
5	Paquetes de sticker para la identificación de los puntos en la red.	\$ 5,00	\$ 25,00
10	Organizadores Horizontales	\$ 35,00	\$ 350,00
36	Codos	\$ 0,21	\$ 7,56
10	Face Plate	\$ 0,43	\$ 4,30
10	Cajas Sobrepuestas	\$ 0,76	\$ 7,60
<b>Total de Costos de Cableado Estructurado</b>			<b>\$ 3.549,36</b>

**Medios de Comunicación**

Cant.	Detalle	Precio Unitario	Costo Total
600 mts	Instalación Fibra Óptica	\$ 2 mt	\$ 1.200,00
<b>Total de Medios de Comunicación</b>			<b>\$ 1.200,00</b>

**Hardware**

Cant.	Detalle	Precio Unitario	Costo Total
3	Memorias IBM 512 MB	\$ 169,00	\$ 507,00
3	Discos Duros de 120 Gb IBM	\$ 190,00	\$ 570,00
3	Cisco 2821 Integrated Services Router	\$ 2.540,50	\$ 7.621,50
3	Placa CISCO WS-G5486 GBIC fibra óptica Gigaethernet	\$ 100,00	\$ 300,00
2	Switch Cisco 2950	\$ 775,00	\$ 1.550,00
3	UPS	\$ 295,80	\$ 887,40
<b>Total</b>			<b>\$ 11.435,90</b>
<b>Total Costos de Hardware</b>			<b>\$ 16.185,26</b>

Tabla. 3.8 Alternativa A: Factibilidad económica



## 3.3.1.2.2 COSTOS DE SOFTWARE

Cant.	Detalle	Precio Unitario	Costo Total
3	Sistema Operativo Linux Fedora Core 3	\$ -	\$ -
1	Software de Monitoreo de Red	\$ 458,00	\$ 458,00

**Total Costos de Software** \$ 458,00

Tabla. 3.9 Alternativa A: Costos de Software

## 3.3.1.2.3 COSTOS DEL ENLACE DE DATOS

Cant.	Detalle	Precio Unitario	Costo Total
1	Comunicación WAN con un enlace de fibra óptica y un ancho de banda de 1024 Kps. (mensual)	\$ 800,00	\$ 800,00

**Costo Total del Enlace** \$ 800,00

Tabla. 3.10 Alternativa A: Costos del Enlace Total

## 3.3.1.2.4 COSTOS OPERATIVOS

Cant.	Detalle	Semanas	Costo Semanal	Costo Total
<b>Fase de Diseño LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	2	\$ 150,00	\$ 300,00
1	Administrador de Redes	2	\$ 80,00	\$ 160,00
<b>Fase de Implementación LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	4	\$ 150,00	\$ 600,00
2	Técnicos en Red	4	\$ 80,00	\$ 640,00
1	Administrador de Redes	4	\$ 100,00	\$ 400,00
1	Técnico en Electricidad	4	\$ 100,00	\$ 400,00
<b>Fase de Prueba red LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	1	\$ 150,00	\$ 150,00
1	Técnico en Redes	1	\$ 80,00	\$ 80,00
<b>Fase de Documentación red LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	2	\$ 150,00	\$ 300,00
2	Técnicos en Red	2	\$ 80,00	\$ 320,00
<b>Viáticos</b>				
Gastos de Viáticos				\$ 750,00
<b>Total</b>				<b>\$ 4.100,00</b>

Tabla. 3.11 Alternativa A: Costos Operativos

## 3.3.1.2.5 COSTO TOTAL DE LA PROPUESTA

<b>Factibilidad</b>	<b>Costo Total</b>
Costos de Hardware.	\$ 16.185,26
Costos de Enlace de datos	\$ 800,00
Costos de Software	\$ 458,00
Servicios Profesionales	\$ 7.331,49
<b>Subtotal</b>	<b>\$ 24.774,75</b>
IVA (12%)	\$ 2.972,97
<b>Total</b>	<b>\$ 27.747,72</b>

Tabla. 3.12 Alternativa A: Costo total de la propuesta

## 3.3.1.3 FACTIBILIDAD OPERATIVA

<b>Cantidad</b>	<b>Detalle</b>	<b>Actividad</b>	<b>Semanas</b>
<b>Fase de Análisis LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Líder del proyecto, encargado del análisis de la situación actual	2
1	Administrador de Redes	Recopilación de información.	
<b>Fase de Diseño LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Líder del proyecto, encargado del diseño LAN y WAN	2
1	Administrador de Redes	Diseño de Cableado LAN	
<b>Fase de Implementación LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Líder, coordinador del grupo	4
2	Técnicos en Red	Cableado LAN y WAN	
1	Administrador de Redes	Configuración de equipos	
1	Técnico en Electricidad	Instalación de tomas eléctricas	
<b>Fase de Prueba LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Pruebas WAN y LAN	1
1	Técnico en Redes	Ayudar al Ingeniero a realizar las pruebas	
<b>Fase de Documentación LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Lineamientos de Manuales	2
2	Técnicos en Red	Elaboración de Manuales	

Tabla. 3.13 Alternativa A: Factibilidad operativa

### 3.3.1.4 FORMA DE PAGO Y TIEMPO DE DESARROLLO

- La forma de pago se realizará en tres partes, la primera parte será del 60 % y se abonará al momento de aceptación de la propuesta, para cubrir gastos de materiales, costos operativos, equipos e imprevistos. La segunda parte será del 20 % y se cancelará al momento se comenzar la fase de Implementación, la tercera parte será del 20 % restante se cancelará al término del proyecto.
- Además, se debe recalcar que durante la implementación de la solución escogida, EPSILUM S.A. tendrá que ofrecer todas las garantías y facilidades que se requieran para el cumplimiento del proyecto.
- El tiempo estimado para la implementación de la red a nivel WAN y LAN, se muestra en el Diagrama GANNT, que está representado en días y tiene una duración de 60 días (2 meses) (ver figura 3.1).

### 3.3.1.5 VENTAJAS Y BENEFICIOS

#### 3.3.1.5.1 VENTAJAS

- Una de las ventajas de implementar cableado estructurado en la empresa es que se encuentra regulado mediante estándares, lo que garantiza a los usuarios su disposición para las aplicaciones existentes, independientemente del fabricante de las mismas, siendo soluciones abiertas, fiables y muy seguras.
- Aprovechar y administrar eficientemente la adquisición de equipos de comunicación con nuevas tecnologías para ayudan a mejorar el rendimiento de red y disminuir las colisiones.
- Mayor rendimiento y velocidad en el acceso a Internet.
- Protección en la red evitando ingresos maliciosos.
- Protección de los equipos de comunicación con un respaldo de energía de óptimo rendimiento y protección.

#### 3.3.1.5.2 BENEFICIOS

- Productividad y seguridad en la comunicación.
- Agilidad en reubicación y detección de posibles errores en la comunicación entre unidades.
- Mejor administración del ancho de banda de Internet.
- Comunicación constante entre el Edificio Matriz y sus sucursales.
- Acceso rápido y de manera eficiente a la información.
- Información en línea.



### 3.3.1.6 GARANTÍAS

#### **Hardware:**

- *Los componentes de hardware empleados para integrar la red LAN tienen una garantía de un año.*
  - *Switchs Cisco*
  - *UPS*
- *Los componentes de hardware empleados para integrar la red WAN tienen una garantía de cinco años.*
  - *Routers Cisco*
- *La Garantía implica que, durante su vigencia, al reportar el cliente un producto que presenta fallas, un ingeniero de soporte lo asistirá en el sitio donde se originó el problema. Si la causa de la falla no es imputable, se aplicará el cargo al cliente. Ésta garantía tiene un plazo de duración de 1 año.*

#### **Cableado Estructurado:**

- *La Garantía para cableado estructurado comprende un periodo de 5 años e implica que cuando el cliente reporta una falla, un ingeniero de soporte lo asistirá en el sitio donde se originó el problema.*

*Si la causa de la falla no es imputable, se aplicará el cargo al cliente.*

#### **Internet:**

- *La garantía del proveedor de Servicios de Internet comprende una velocidad de transmisión mínima del 70% del ancho de banda contratado.*



### 3.3.2 ALTERNATIVA: B

El objetivo principal de esta alternativa es implementar cableado estructurado y establecer un Enlace Backup en el edificio Matriz y en las dos Sucursales (Ambato y Loja), siendo esta alternativa la que reduce costos en equipos.

#### 3.3.2.1 FACTIBILIDAD TÉCNICA

##### 3.3.2.1.1 DISPOSITIVOS DE ENRUTAMIENTO

Cant.	Equipo	Descripción	Ubicación	Uso
3	DI-1750 Corporate Modular Multi-Service Access Router 	<b>General</b>	1 Edificio Matriz	Dispositivo de Enrutamiento
		Tipo de dispositivo	1 Sucursal Loja	
		Enrutador	1 Sucursal Ambato	
		<b>Memoria</b>		
		Memoria RAM	SDRAM: 64MBytes	
		<b>Conexión de redes</b>		
		Protocolos de Red	ARP, ARP Proxy, NHRP DNS, NAT, IP Filtering ICMP, IGMP, DHCP client	
		Enrutamiento	Enrutamiento Estático RIP v1, v2, OSPF v1, v2	
		Firewall	ACL, NAT	
		Alta Disponibilidad	Port backup	
<b>Interfaces</b>	RJ-45 10/100M Fast Ethernet Puerta de Consola RJ-45 Puerto Auxiliar RJ-45 con interface RS-232 serial asincrónica DTE			

Tabla. 3.14 Alternativa B: Dispositivos de enrutamiento

## 3.3.2.1.2 DISPOSITIVOS DE CONMUTACIÓN

Cant.	Equipo	Descripción	Ubicación	Uso
2	DGS-1224T Corporate Switch Layer 2+/4 - 24- port GE  	Número de Puertos: 24 puertos 10/100/1000  Características: - Segmentación del tráfico - Control del ancho de banda, desde 64Kbps - Control del ancho de banda por flujos  Administrable/Stackeable  - 802.3ad Link Aggregation (Port Trunks) - Basade en Web - Servidor Telnet	1 Sucursal Loja 1 Sucursal Ambato	Administración de VLAN's

Tabla. 3.15 Alternativa B Dispositivos de comunicación

## 3.3.2.1.3 MEDIOS DE COMUNICACIÓN

Cant.	Equipo	Descripción	Ubicación	Uso
600 mts	Fibra Óptica Multimodo	Marca: Genérico Número de Hilos: 12 Hilos Transmisión: 1000 Mbps	150 mts 250 mts 200 mts	Enlace Principal

Tabla. 3.16 Alternativa B Medios de comunicación

## 3.3.2.1.4 EQUIPOS

Cant.	Equipo	Descripción	Ubicación	Uso
3	Disco Duro de 120 Gb	Modelo: IBM	1 Matriz	Actualización de Servidor de Correo
3	Memoria Ram 512 Mb	Marca: IBM	1 Sucursal Loja 1 Sucursal Ambato	
3	UPS POWERWARE 5125  	Modelo: POWERWARE 5125 Características: Administrador Avanzado de Energía duplica la vida útil de las baterías. Control de segmentos de carga: Permite programar grupos de bornamientos para apagados programados Supresor de Transientes: Protege a los PC's, servidores, switches, ruteadores de voltajes transientes que viajan por el cableado de red y línea telefónica. Garantía: 2 años de garantía.	1 Matriz 1 Sucursal Loja 1 Sucursal Ambato	Administración de Energía

Tabla. 3.17 Alternativa B: Equipos

## 3.3.2.1.5 CABLEADO ESTRUCTURADO

Cant.	Equipo	Descripción	Ubicación	Uso
17	Bobinas Cat.6 305 mts.	Marca: Genérico	Matriz	Cableado General
		Cable: UTP	Sucursal Loja	
		Categoría: 6	Sucursal Ambato	
		Velocidad de Transmisión: 10/100/1000 Mbps		
		Ancho de Banda: 200 Mhz		
50	Patch Cord	Marca: Genérico	Matriz Sucursal Loja Sucursal Ambato	Cableado General
408	Conectores Rj-45	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General
200	Jack	De Presión: 100 Jack De Impacto: 100 Jack Marca: Genérico	Matriz Sucursal Loja Sucursal Ambato	Cableado General
16 Mtrs	Canaletas Decorativas	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General
2	Cintas Velcro	Marca: Genérico	Matriz	Cableado General
5	Paquetes de sticker para la identificación de los puntos de red	Marca: Genérico	Sucursal Loja	
		Marca: Genérico	Sucursal Ambato	
10	Organizadores Verticales	Marca: Genérico	Matriz	
571	Amarras	Marca: Genérico	Suc. Loja y Ambato Suc. Loja y Ambato	Cableado General
36	Codos	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General
10	Face Plate	3 Servicios: 5	Matriz	Cableado General
		2 Servicios: 3	Sucursal Loja	
		1 Servicio: 2	Sucursal Ambato	
10	Cajas Sobrepuestas	Marca: Genérico	Matriz Suc. Loja y Ambato	Cableado General

Tabla. 3.18 Alternativa B: Cableado estructurado

## 3.3.2.2 FACTIBILIDAD ECONÓMICA

## 3.3.2.2.1 COSTOS DE HARDWARE

**Cableado Estructurado**

<b>Cant.</b>	<b>Detalle</b>	<b>Precio Unitario</b>	<b>Costo Total</b>
17	Bobinas Cat.6 305 mts.	\$ 105,00	\$ 1.785,00
50	Patchs Cords	\$ 5,00	\$ 250,00
408	Conectores Rj-45	\$ 0,30	\$ 122,40
200	Jack de Impacto	\$ 1,34	\$ 268,00
16 Mtrs	Canaletas Decorativas calibre 20	\$ 42,00	\$ 672,00
5	Amarras (fundas de 100)	\$ 5,50	\$ 27,50
2	Cinta velcro	\$ 15,00	\$ 30,00
5	Paquetes de sticker para la identificación de los puntos en la red.	\$ 5,00	\$ 25,00
10	Organizadores Horizontales	\$ 35,00	\$ 350,00
36	Codos	\$ 0,21	\$ 7,56
10	Face Plate	\$ 0,43	\$ 4,30
10	Cajas Sobrepuestas	\$ 0,76	\$ 7,60
<b>Total de Costos de Cableado Estructurado</b>			<b>\$ 3.549,36</b>

**Medios de Comunicación**

<b>Cant.</b>	<b>Detalle</b>	<b>Precio Unitario</b>	<b>Costo Total</b>
600 mts	Instalación Fibra Óptica	\$ 2 mt	\$ 1.200,00
<b>Total de Medios de Comunicación</b>			<b>\$ 1.200,00</b>

**Hardware**

<b>Cant.</b>	<b>Detalle</b>	<b>Precio Unitario</b>	<b>Costo Total</b>
3	Memorias IBM 512 MB	\$ 169,00	\$ 507,00
3	Discos Duros de 120 Gb IBM	\$ 190,00	\$ 570,00
3	Router D-Link DI-175D	\$ 1.305,20	\$ 3.915,60
2	Switch D-Link DGS-1224T	\$ 378,00	\$ 756,00
3	UPS	\$ 295,80	\$ 887,40
<b>Total</b>			<b>\$ 6.636,00</b>
<b>Total Costos de Hardware</b>			<b>\$ 11.385,36</b>

Tabla. 3.19 Alternativa B: Factibilidad económica

## 3.3.2.2.2 COSTOS DE SOFTWARE

Cant.	Detalle	Precio Unitario	Costo Total
3	Sistema Operativo Linux Fedora Core 3	\$ -	\$ -
1	Software de Monitoreo de Red	\$ 458,00	\$ 458,00

**Total Costos de Software** \$ **458,00**

Tabla. 3.20 Alternativa B: Costos del software

## 3.3.2.2.3 COSTOS DEL ENLACE DE DATOS

Cant.	Detalle	Precio Unitario	Costo Total
1	Comunicación WAN con un enlace de fibra óptica y un ancho de banda de 1024 Kps. (mensual)	\$ 800,00	\$ 800,00

**Costo Total del Enlace** \$ **800,00**

Tabla. 3.21 Alternativa B: Costos de enlace de datos

## 3.3.2.2.4 COSTOS OPERATIVOS

Cant.	Detalle	Semanas	Costo Semanal	Costo Total
<b>Fase de Diseño LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	2	\$ 150,00	\$ 300,00
1	Administrador de Redes	2	\$ 80,00	\$ 160,00
<b>Fase de Implementación LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	4	\$ 150,00	\$ 600,00
2	Técnicos en Red	4	\$ 80,00	\$ 640,00
1	Administrador de Redes	4	\$ 100,00	\$ 400,00
1	Técnico en Electricidad	4	\$ 100,00	\$ 400,00
<b>Fase de Prueba red LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	1	\$ 150,00	\$ 150,00
1	Técnico en Redes	1	\$ 80,00	\$ 80,00
<b>Fase de Documentación red LAN y WAN</b>				
1	Ingeniero de Telecomunicaciones	2	\$ 150,00	\$ 300,00
2	Técnicos en Red	2	\$ 80,00	\$ 320,00
<b>Viáticos</b>				
Gastos de Viáticos				\$ 750,00
<b>Total</b>				<b>\$ 4.100,00</b>

Tabla. 3.22 Alternativa B: Costos operativos

## 3.3.2.2.5 COSTO TOTAL DE LA PROPUESTA

<b>Factibilidad</b>	<b>Costo Total</b>
Costos de Hardware.	\$ 11.385,36
Costos de Enlace de datos	\$ 800,00
Costos de Software	\$ 458,00
Servicios Profesionales	\$ 6.611,50
<b>Subtotal</b>	<b>\$ 19.254,86</b>
IVA (12%)	\$ 2.310,58
<b>Total</b>	<b>\$ 21.565,44</b>

Tabla. 3.23 Alternativa B: Costo total de la propuesta

## 3.3.2.3 FACTIBILIDAD OPERATIVA

<b>Cantidad</b>	<b>Detalle</b>	<b>Actividad</b>	<b>Semanas</b>
<b>Fase de Análisis LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Líder del proyecto, encargado del análisis de la situación actual	2
1	Técnico en Redes	Recopilación de información.	
<b>Fase de Diseño LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Líder del proyecto, encargado del diseño LAN y WAN	2
1	Administrador de Redes	Diseño de Cableado LAN	
<b>Fase de Implementación LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Líder, coordinador del grupo	4
2	Técnicos en Red	Cableado LAN y WAN	
1	Administrador de Redes	Configuración de equipos	
1	Técnico en Electricidad	Instalación de tomas eléctricas	
<b>Fase de Prueba LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Pruebas WAN y LAN	1
1	Técnico en Redes	Ayudar al Ingeniero a realizar las pruebas	
<b>Fase de Documentación LAN y WAN</b>			
1	Ingeniero de Telecomunicaciones	Lineamientos de Manuales	2
2	Técnicos en Red	Elaboración de Manuales	

Tabla. 3.24 Alternativa B: Factibilidad operativa

### 3.3.2.4 FORMA DE PAGO Y TIEMPO DE DESARROLLO

- La forma de pago se realizará en tres partes, la primera parte será del 50 % y se abonará al momento de aceptación de la propuesta, para cubrir gastos de materiales, costos operativos, equipos e imprevistos. La segunda parte será del 20 % y se cancelará al momento se comenzar la fase de Implementación, La tercera parte será del 20% restante se cancelará al término del proyecto.
- Además, se debe recalcar que durante la implementación de la solución escogida, EPSILUM S.A. tendrá que ofrecer todas las garantías y facilidades que se requieran para el cumplimiento del proyecto.
- El tiempo estimado para la implementación de la red a nivel WAN y LAN, se muestra en el Diagrama GANNT, que está representado en días y tiene una duración de 60 días (2 meses) (ver figura 3.2).

### 3.3.2.5 VENTAJAS Y BENEFICIOS

#### 3.3.2.5.1 VENTAJAS

- El sistema de cableado estructurado va permitir hacer convivir muchos servicios en la red (voz, datos, vídeo, etc.) con la misma instalación, independientemente de los equipos y productos que se utilicen.
- Mejora la productividad.
- Ahorro de presupuesto.
- Mayor rendimiento y velocidad en el acceso a Internet.
- Protección en la red evitando ingresos maliciosos.
- Protección de los equipos de comunicación con un respaldo de energía de óptimo rendimiento y protección.

#### 3.3.2.5.2 BENEFICIOS

- Inversión eficaz
- Productividad y seguridad en la comunicación.
- Agilidad en reubicación y detección de posibles errores en la comunicación entre unidades.
- Clientes satisfechos con Internet más rápido.
- Mejor administración del ancho de banda de Internet.
- Comunicación constante entre el Edificio Matriz y sus sucursales.
- Acceso rápido y de manera eficiente a la información.
- Ahorro del presupuesto (A largo plazo).
- Información en línea.

### 3.3.2.6 GARANTÍAS

#### Hardware:

- Los componentes de hardware empleados para integrar la red LAN tienen una garantía de un año.
  - Switchs D-Link
  - UPS
- Los componentes de hardware empleados para integrar la red WAN tienen una garantía de tres años.
  - Routers D-Link
- La Garantía implica que, durante su vigencia, al reportar el cliente un producto que presenta fallas un ingeniero de soporte lo asistirá en el sitio donde se originó el problema. Si la causa de la falla no es imputable, se aplicará el cargo al cliente. Ésta garantía tiene un plazo de duración de 1 año.

#### Cableado Estructurado:

- La Garantía para cableado estructurado comprende un periodo de 5 años e implica que cuando el cliente reporta una falla, un ingeniero de soporte lo asistirá en el sitio donde se originó el problema.

*Si la causa de la falla no es imputable, se aplicará el cargo al cliente.*

#### Internet:

- La garantía del proveedor de Servicios de Internet comprende una velocidad de transmisión mínima del 70% del ancho de banda contratado.





### 3.4 CONCLUSIONES

*El afán de toda empresa es conseguir ampliar su mercado, esto sólo se lo puede lograr teniendo bases firmes y brindando una atención rápida y excelente al cliente.*

*Teniendo como finalidad dar a conocer el estado actual de la estructura de la red de Epsilon S.A., sugiriendo cambios a nivel de estructura física de la red, orientándolo al cableado estructurado donde encontrar falencias, y estableciendo un respectivo respaldo a nivel de comunicación entre sus sucursales (Ambato y Loja).*

*Se utilizará el sistema operativo Linux, el mismo que es de distribución gratuita y uno de los más robustos en el mercado para brindar soporte a todos los usuarios de la red por medio de los diferentes servicios que posee.*

*Proporcionarán un respaldo a nivel de comunicaciones entre las sucursales Guayaquil, Loja y Ambato (enlace WAN), por medio de creación de VPN (Virtual Private Network), para mayor seguridad en la comunicación.*

*Esta propuesta es completa ya que muestra como cubrir las necesidades de la manera más conveniente. Además le garantiza a usted un retorno rápido de su inversión en corto tiempo. El lograr acaparar el mercado no es fácil de realizar en la actualidad, para ello se deben tomar decisiones importantes.*

*La misión es brindarle ayuda para que pueda cumplir este objetivo.*



## CAPÍTULO 4

---

# IMPLEMENTACIÓN LAN y WAN

## 4. IMPLEMENTACIÓN LAN Y WAN

### 4.1. INFRAESTRUCTURA LAN

#### 4.1.1. UBICACIÓN DEL EDIFICIO MATRIZ

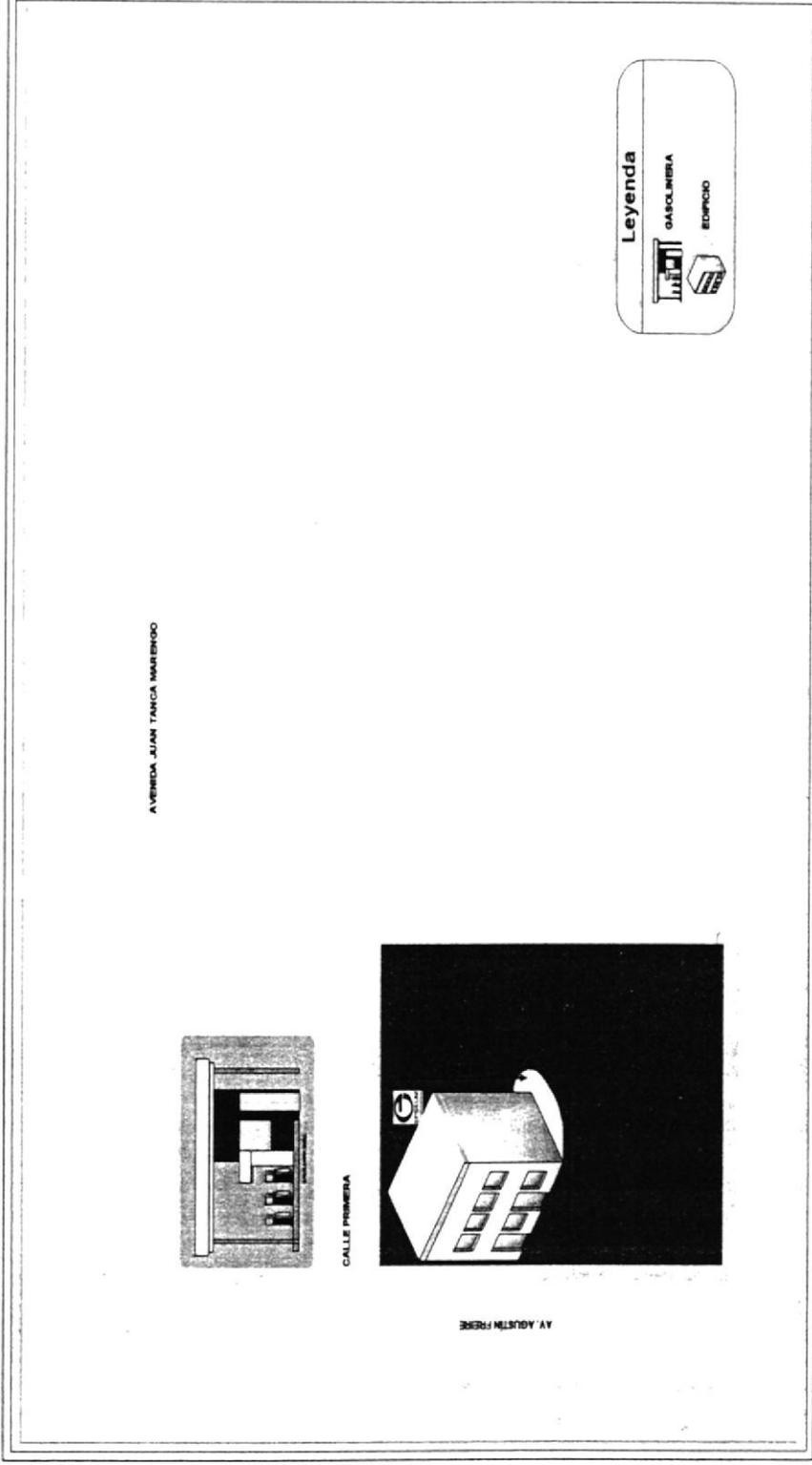


Figura 4.1. Ubicación del Edificio Matriz

### 4.1.2. EDIFICIO MATRIZ.- CABLEADO INTRA-EDIFICIO

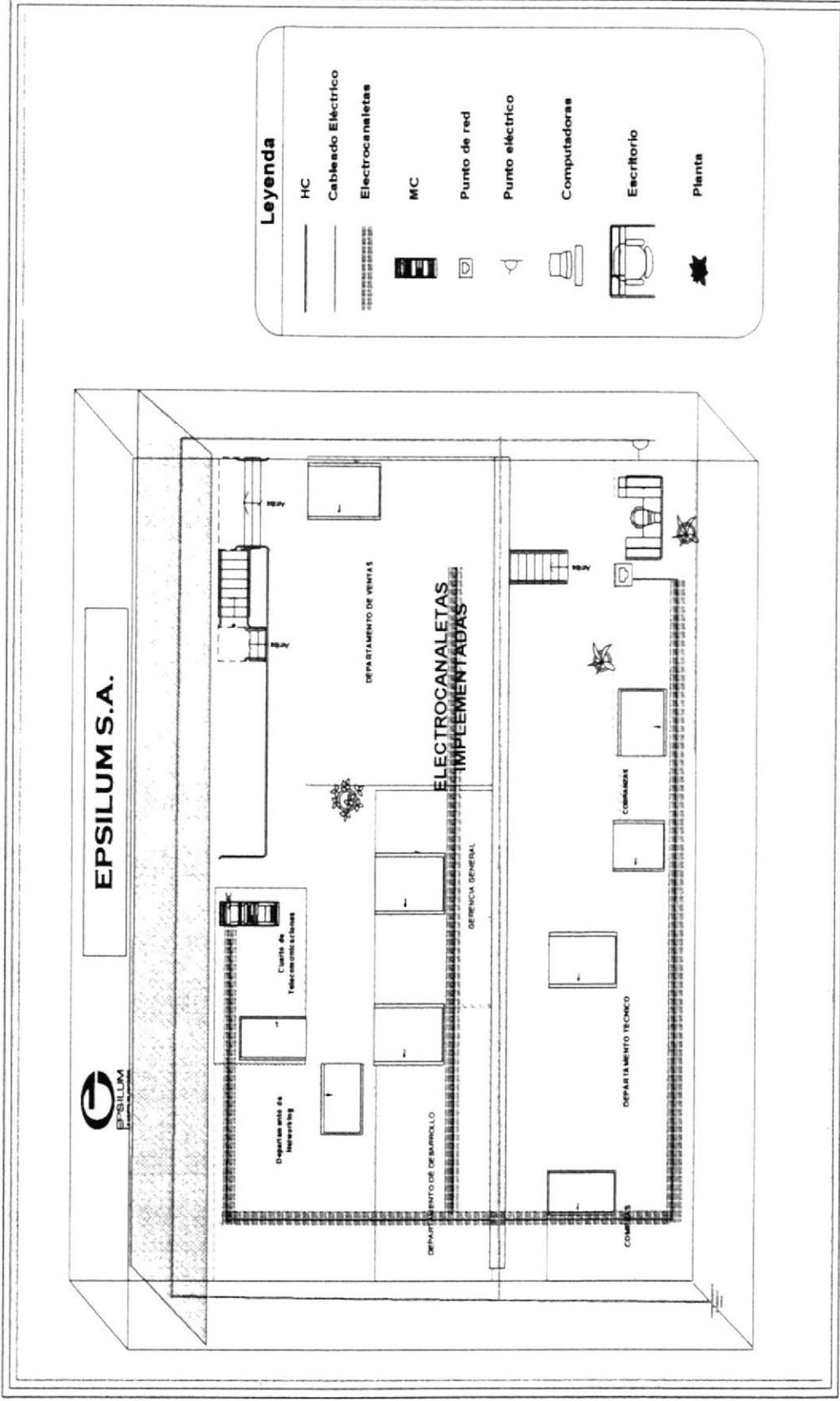


Figura 4.2. Edificio Matriz. - Cableado Intra-edificio

### 4.1.3. SUCURSAL AMBATO.- CABLEADO INTRA-EDIFICIO

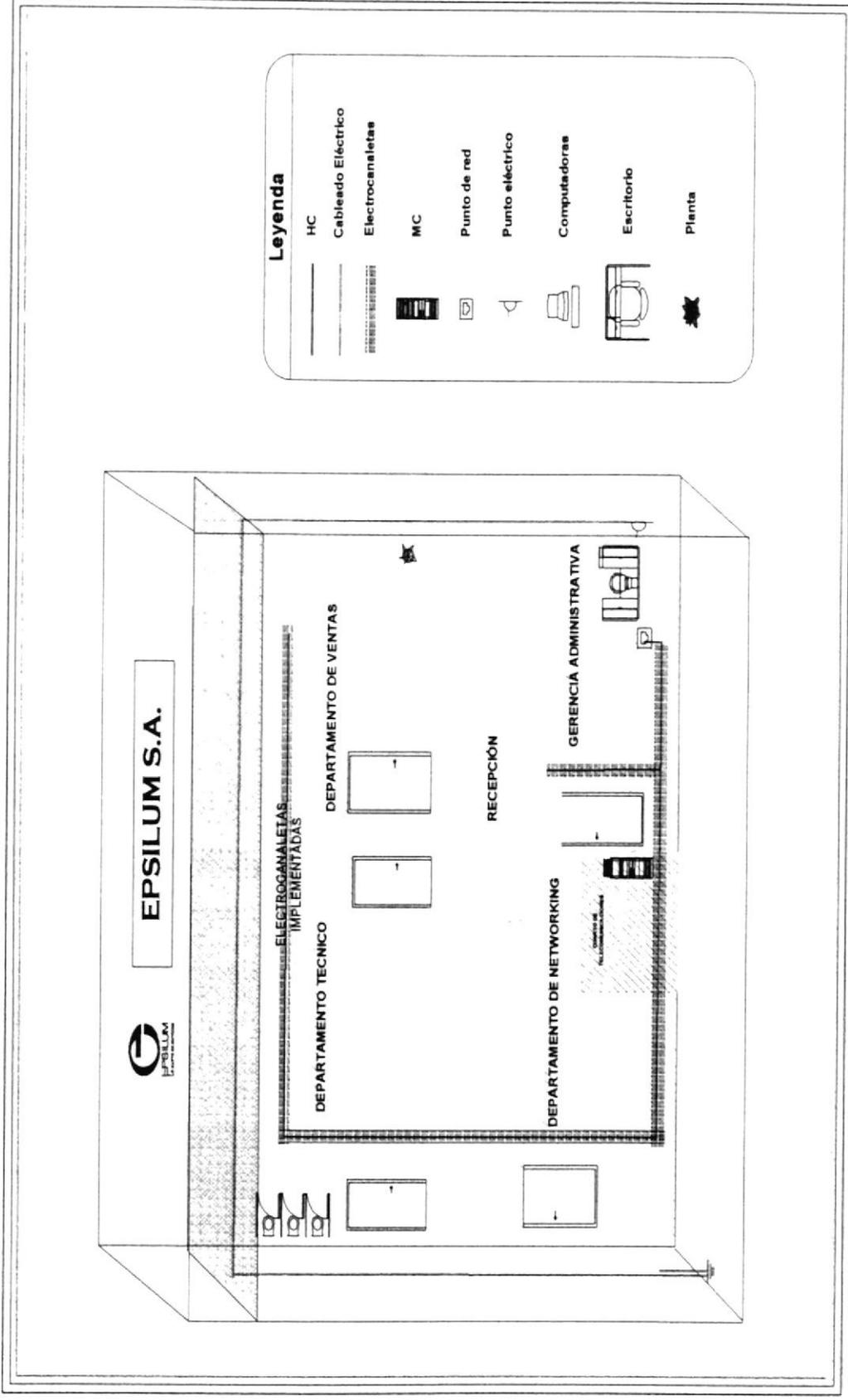


Figura 4.3. Sucursal Ambato.- Cableado Intra-edificio

#### 4.1.4. SUCURSAL LOJA.- CABLEADO INTRA-EDIFICIO

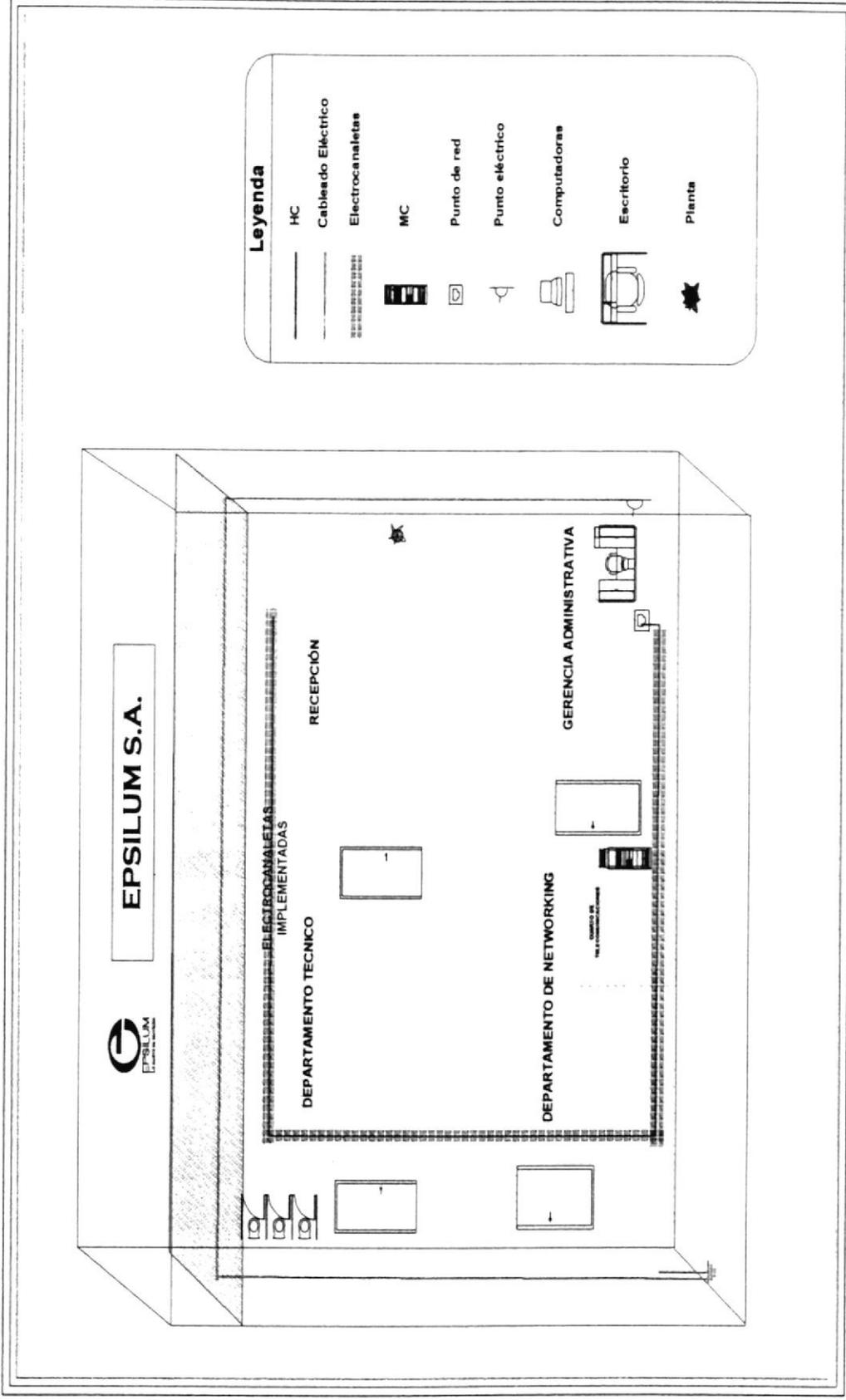


Figura 4.4. Sucursal Loja .- Cableado Intra-edificio

### 4.1.5. ANÁLISIS DE PISO LÓGICO

#### 4.1.5.1. MATRIZ PLANTA BAJA

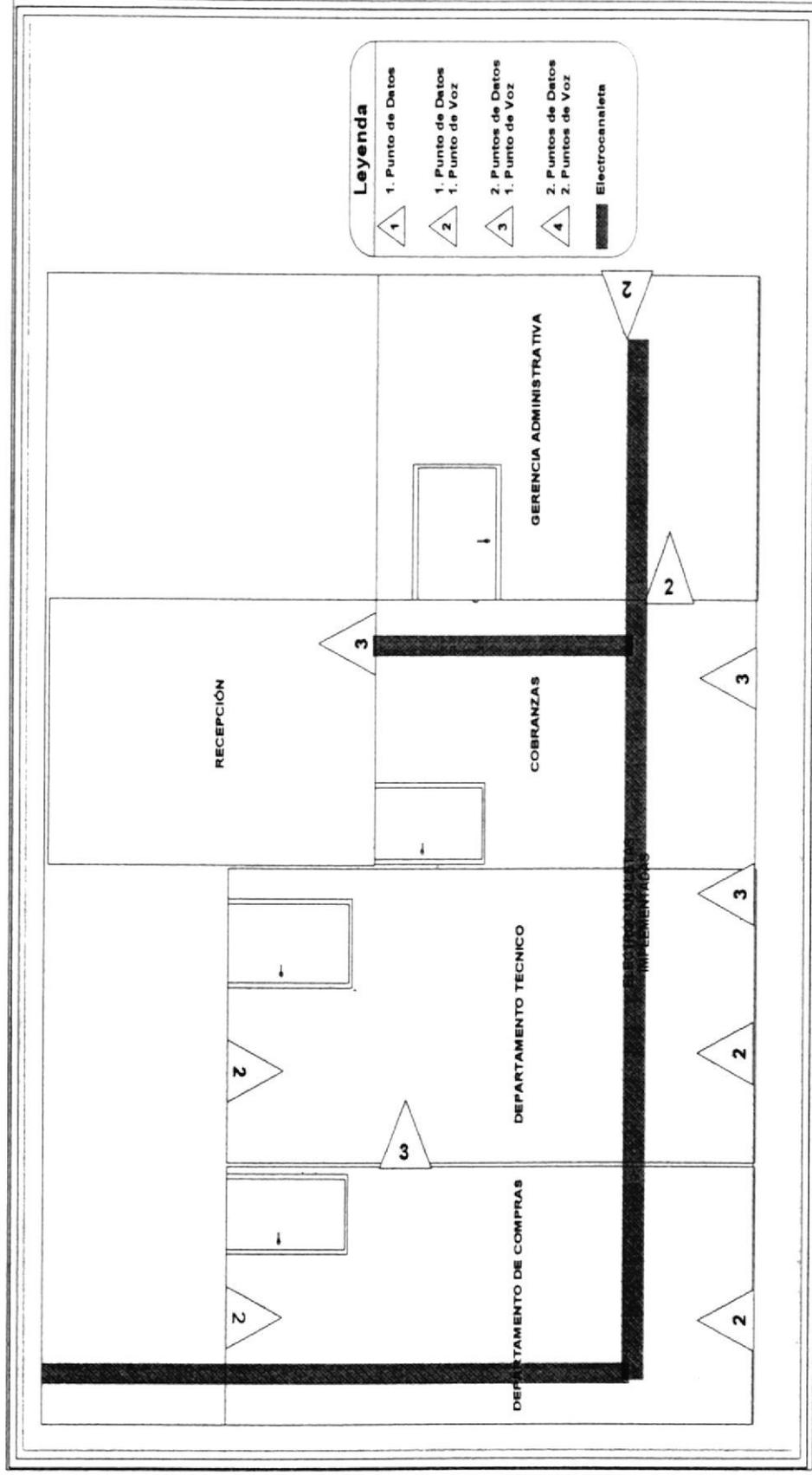


Figura 4.5. Matriz planta baja: Análisis de piso lógico

### 4.1.5.2. MATRIZ PLANTA ALTA

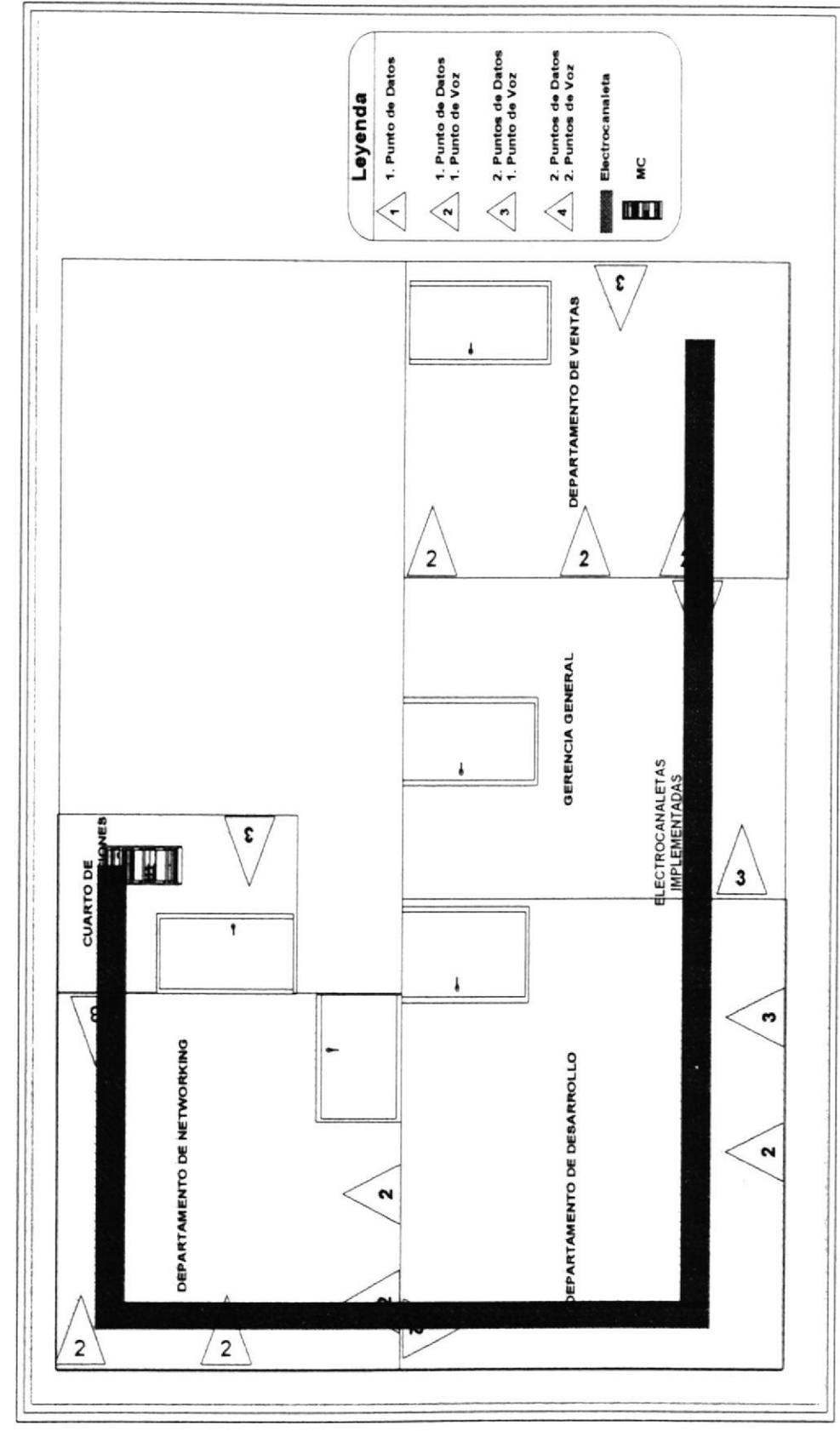


Figura 4.6. Matriz planta alta: Análisis de piso lógico

4.1.5.3. SUCURSAL AMBATO

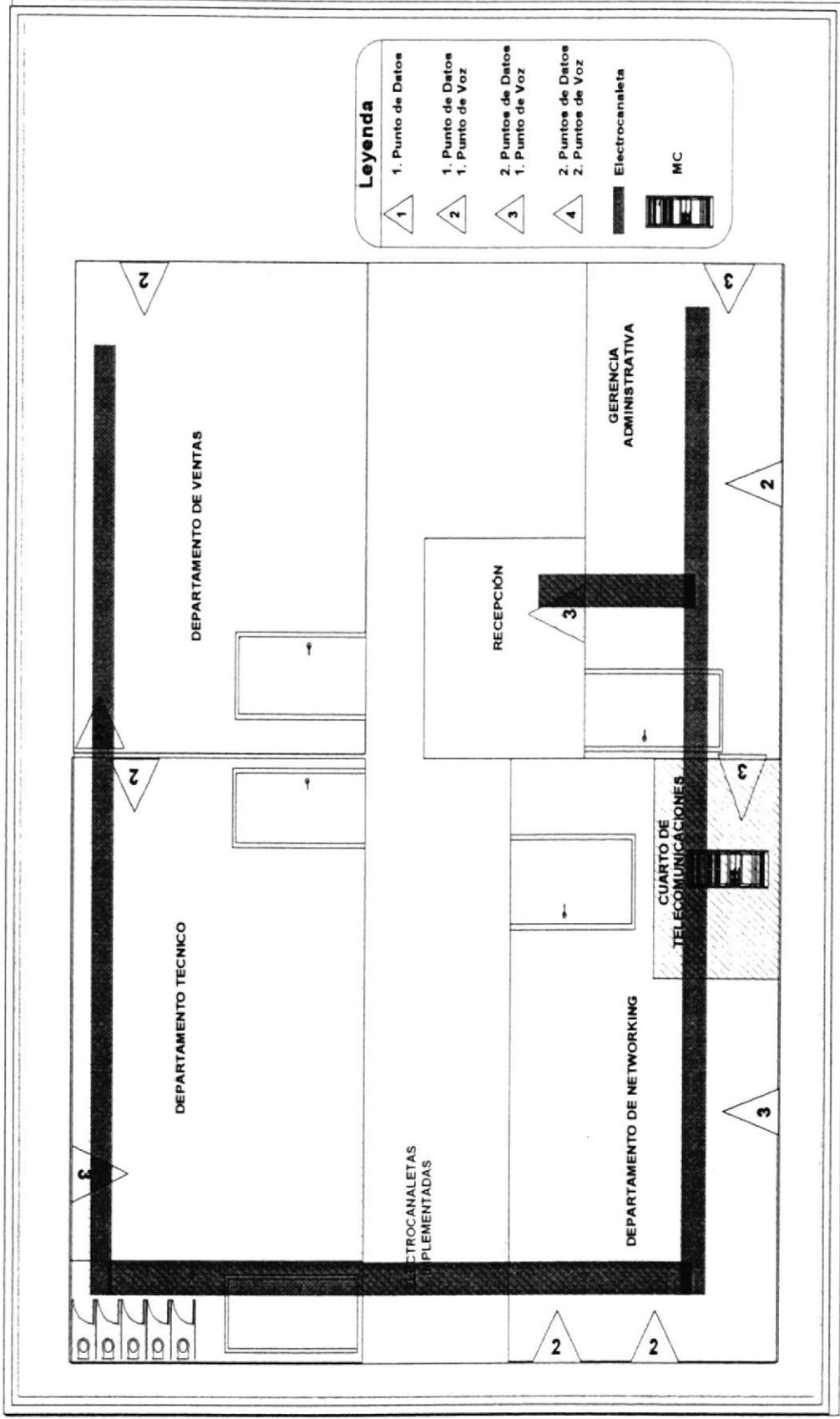


Figura 4.7. Ambato: Análisis de piso lógico

4.1.5.4. SUCURSAL LOJA

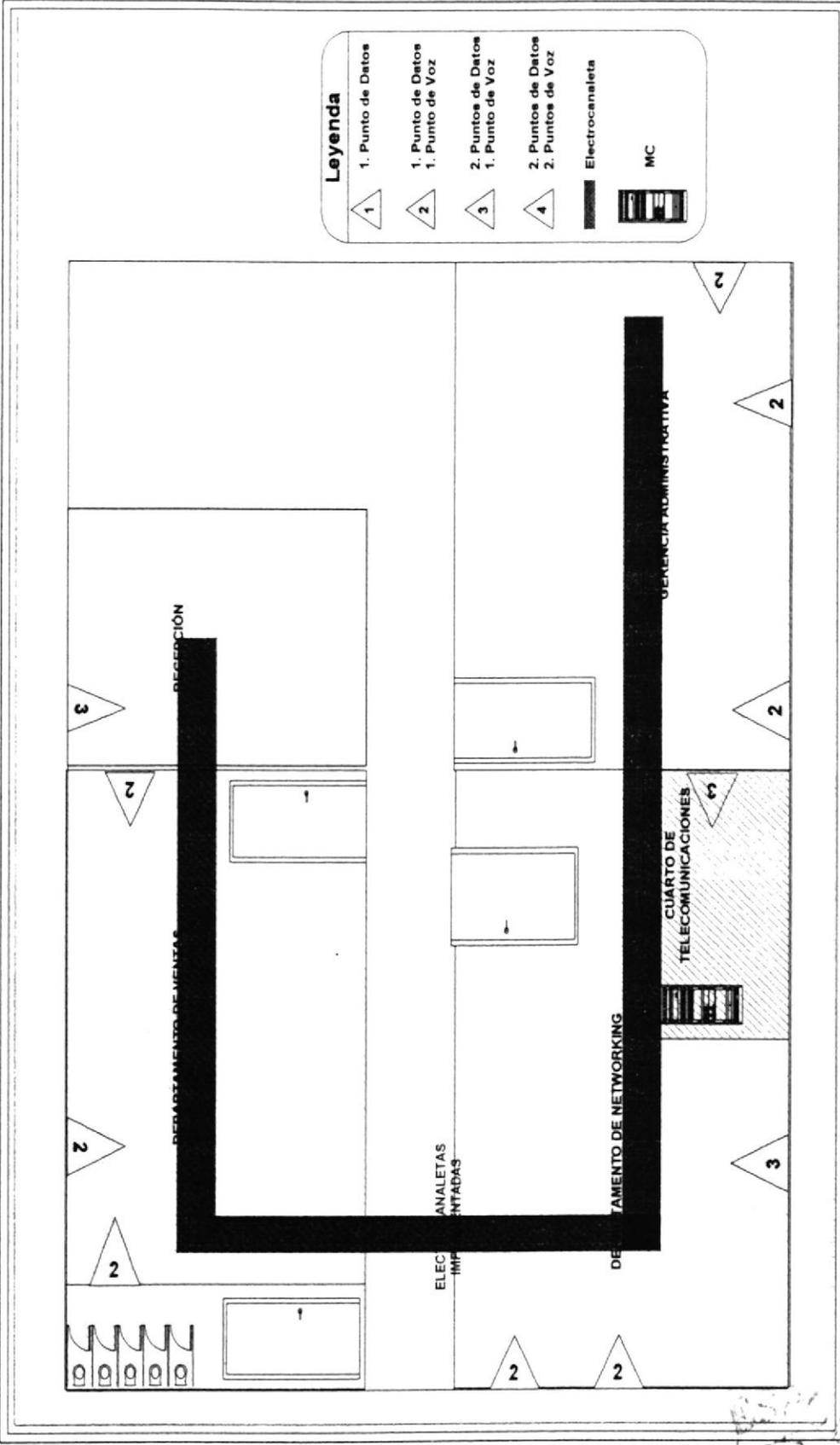


Figura 4.8. Loja: Análisis de piso lógico

ESTAMPADO  
BIBLIOTECA  
SUCURSAL  
LOJA

### 4.1.6. ANÁLISIS DE PISO APLICATIVO

#### 4.1.6.1. MATRIZ PLANTA BAJA

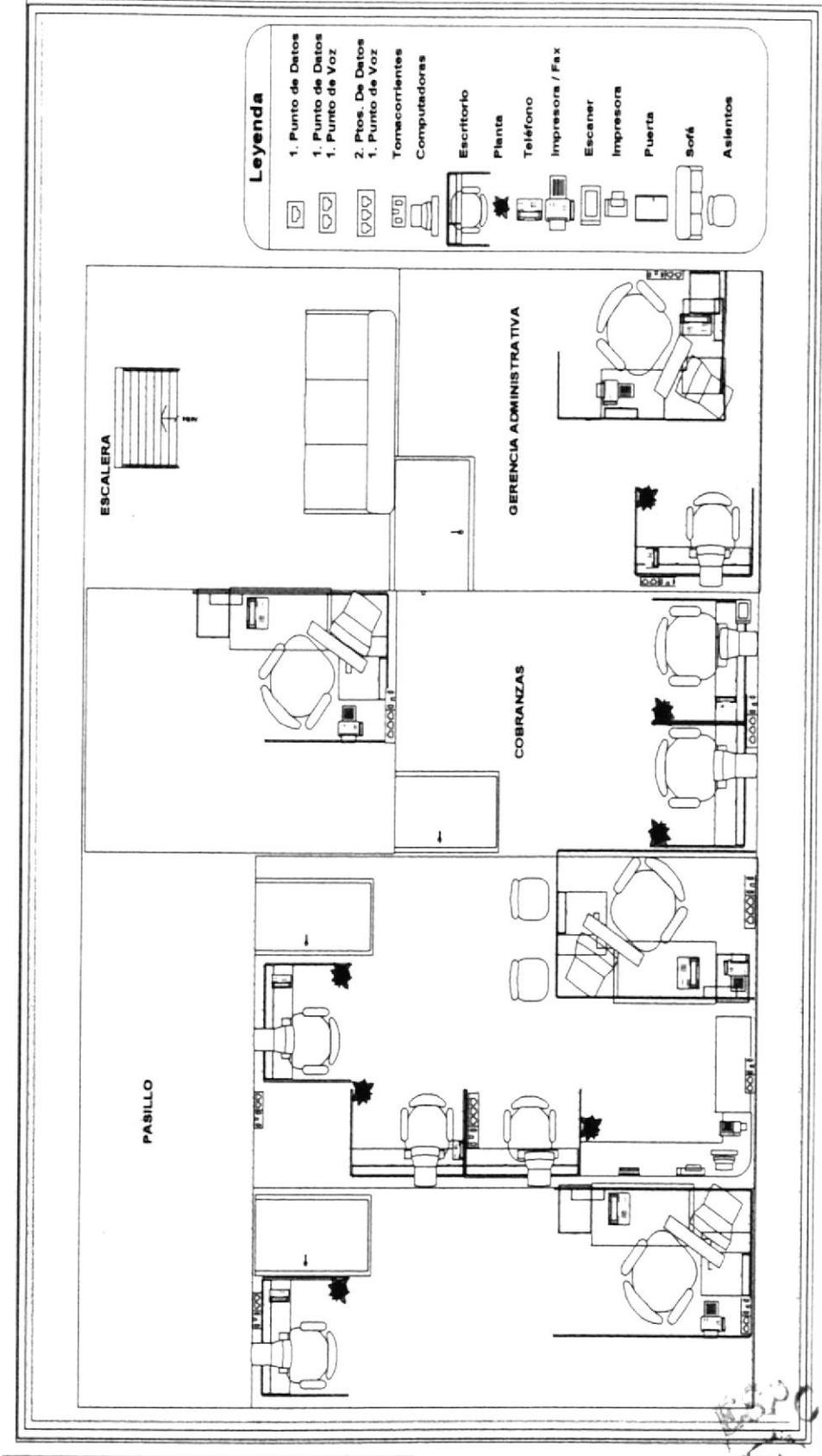
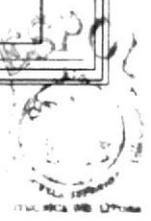


Figura 4.9. Matriz planta baja. Analisis de piso aplicativo



4.1.6.2. MATRIZ PLANTA ALTA

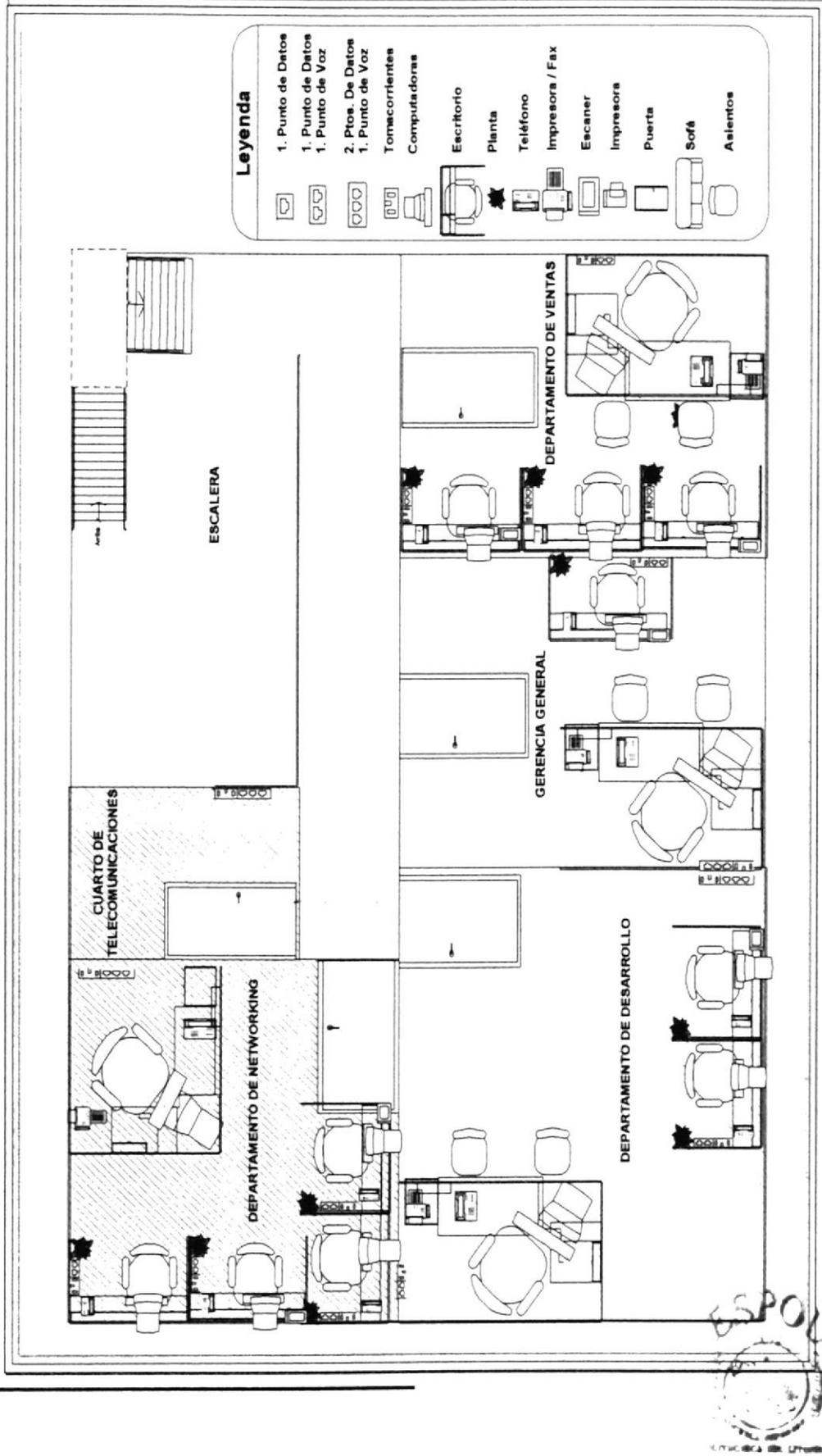


Figura 4.10. Matriz planta alta: Análisis de piso aplicativo



4.1.6.3. AMBATO

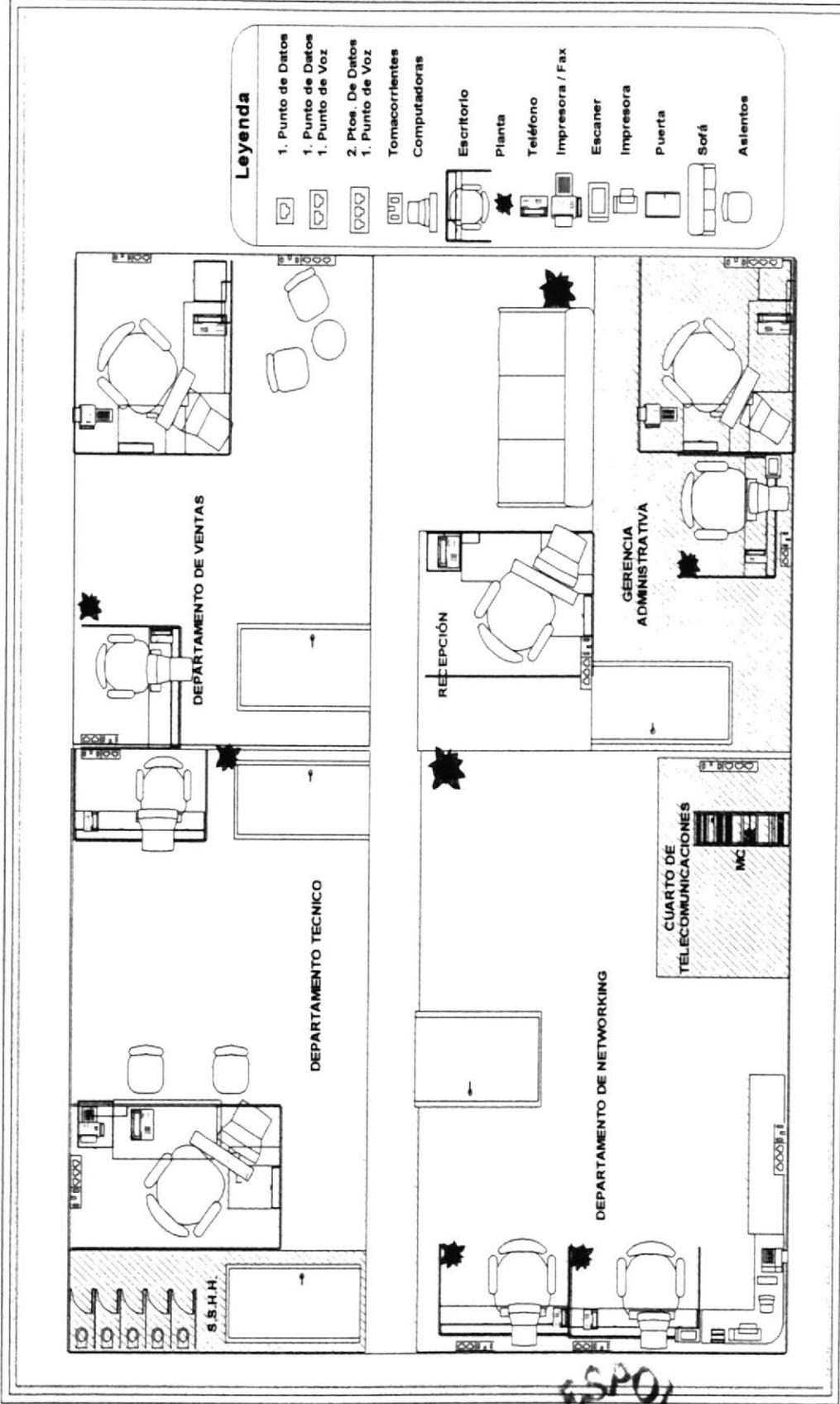


Figura 4.11. Ambato: Análisis de piso aplicativo



4.1.6.4. LOJA

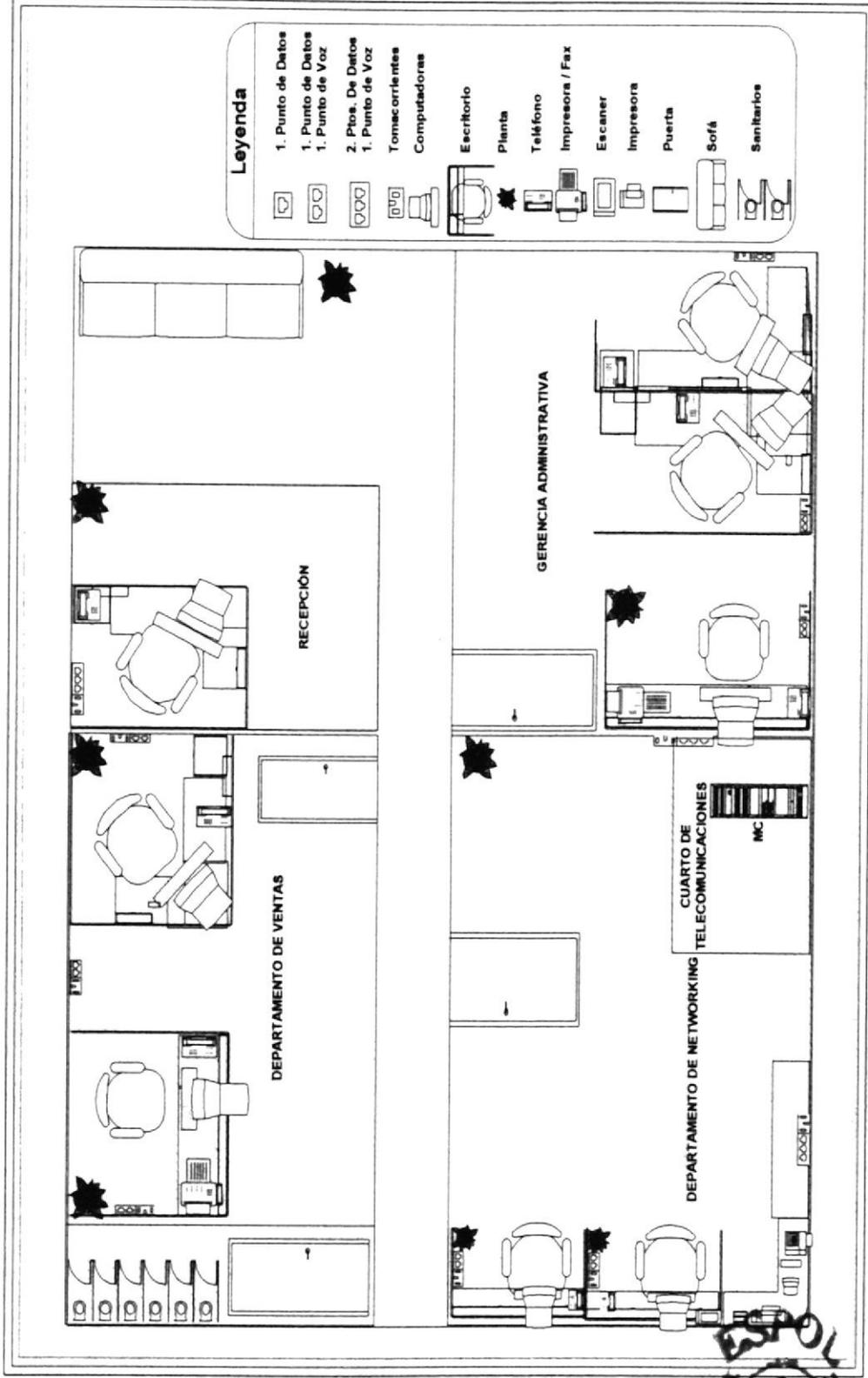


Figura 4.12. Loja: Análisis de piso aplicativo



## 4.1.7. CÁLCULO DEL BACKBONE INTRAEDIFICIO MATRIZ Y SUCURSALES

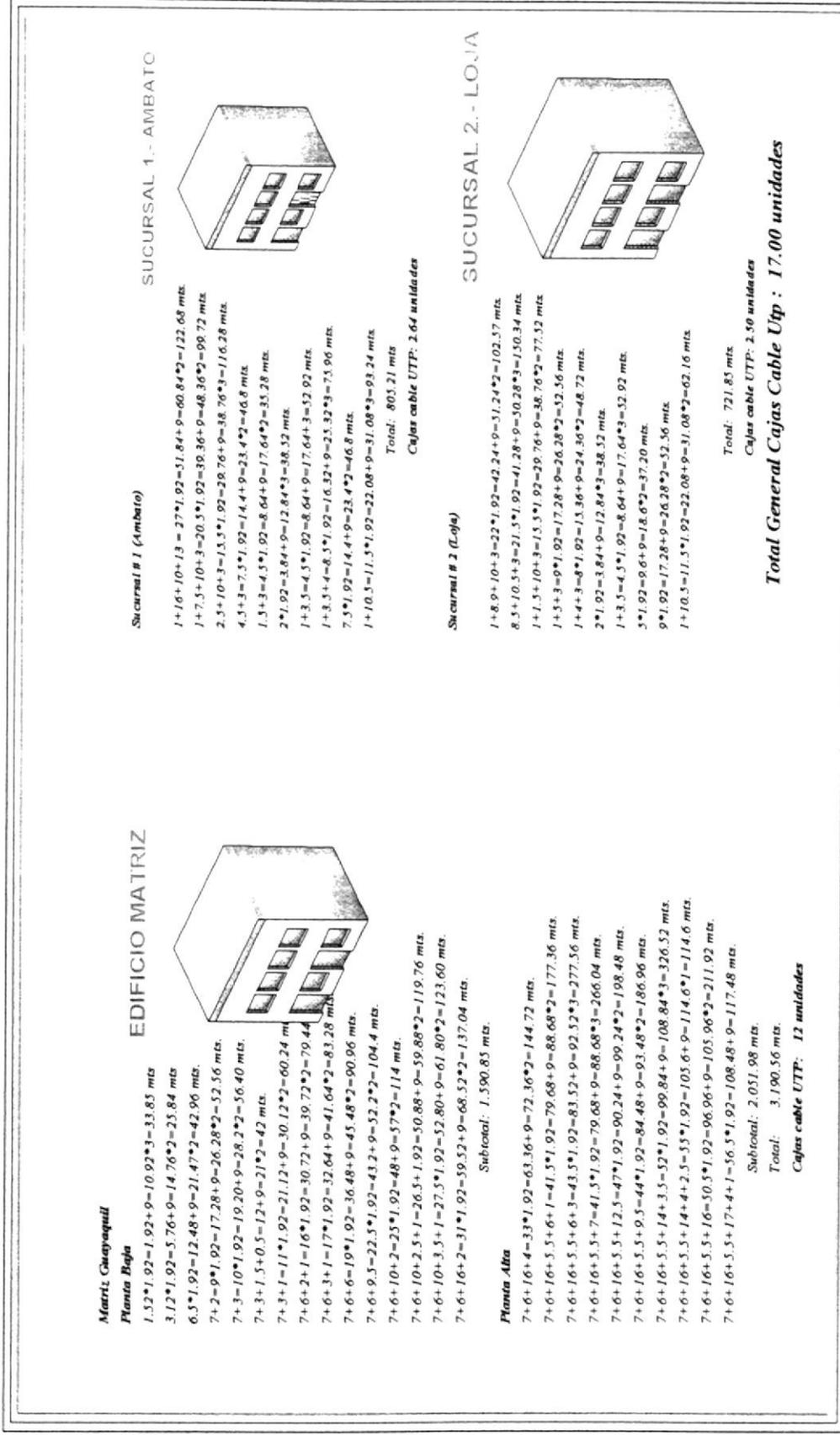


Figura 4.13. Cálculo del Backbone Intra-edificio

### 4.1.8. MC MATRIZ

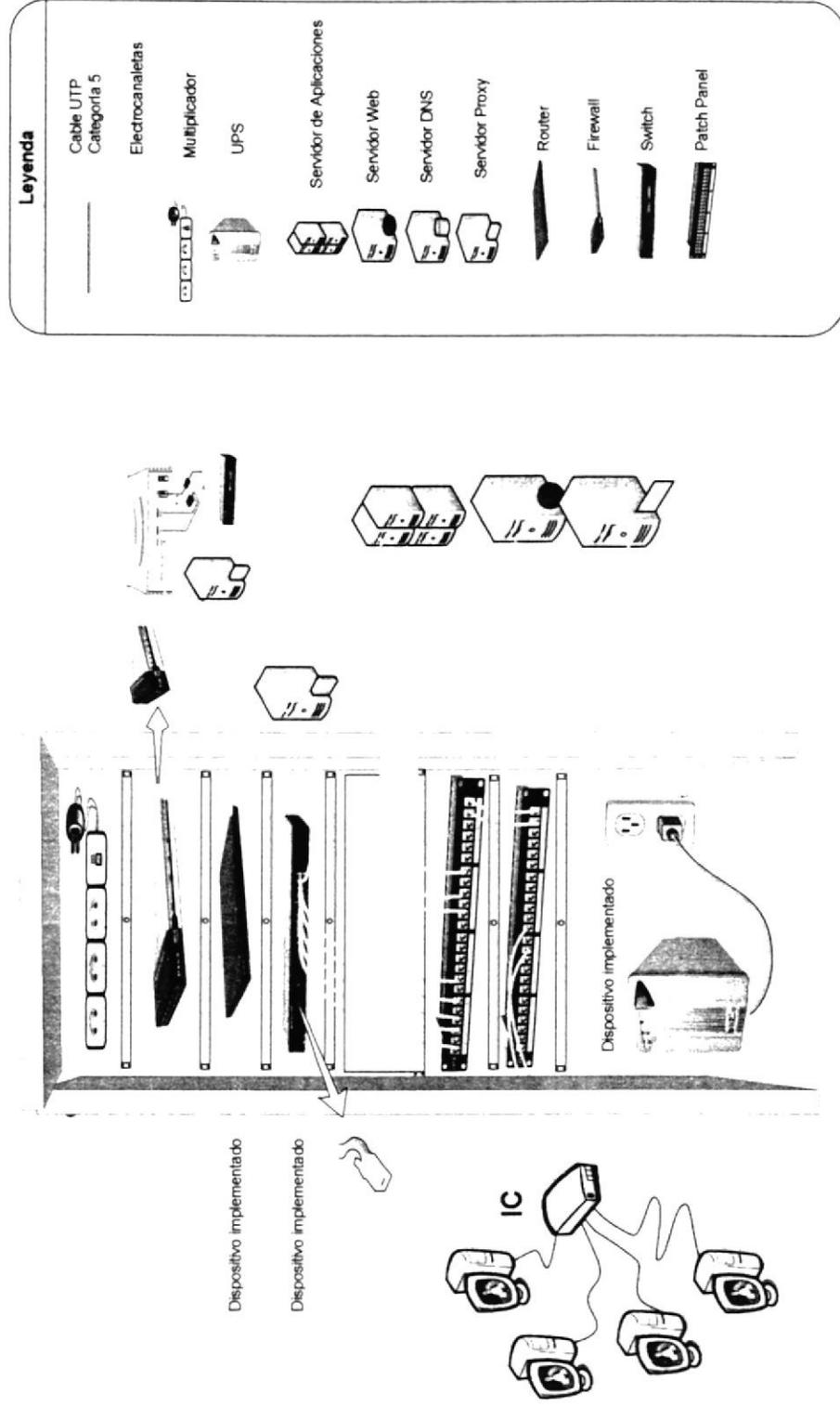


Figura 4.14. Gráfico del MC Matrix

## 4.2. INFRAESTRUCTURA WAN

### 4.2.1. COMUNICACIÓN WAN: MATRIZ - ISP

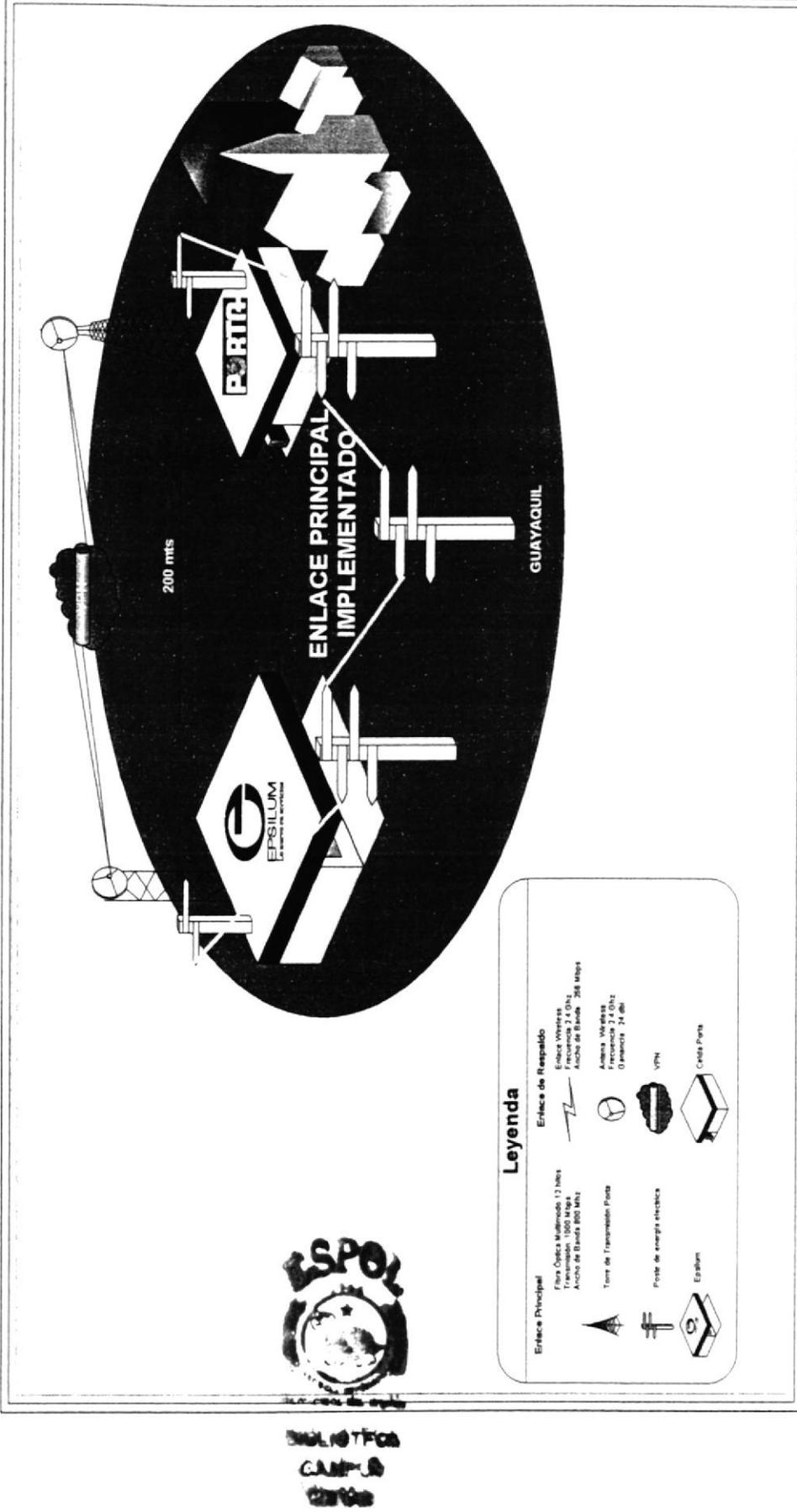


Figura 4.15. Comunicación WAN Matriz - ISP

### 4.2.1.1. COMUNICACIÓN MAN: MATRIZ Y SUCURSALES

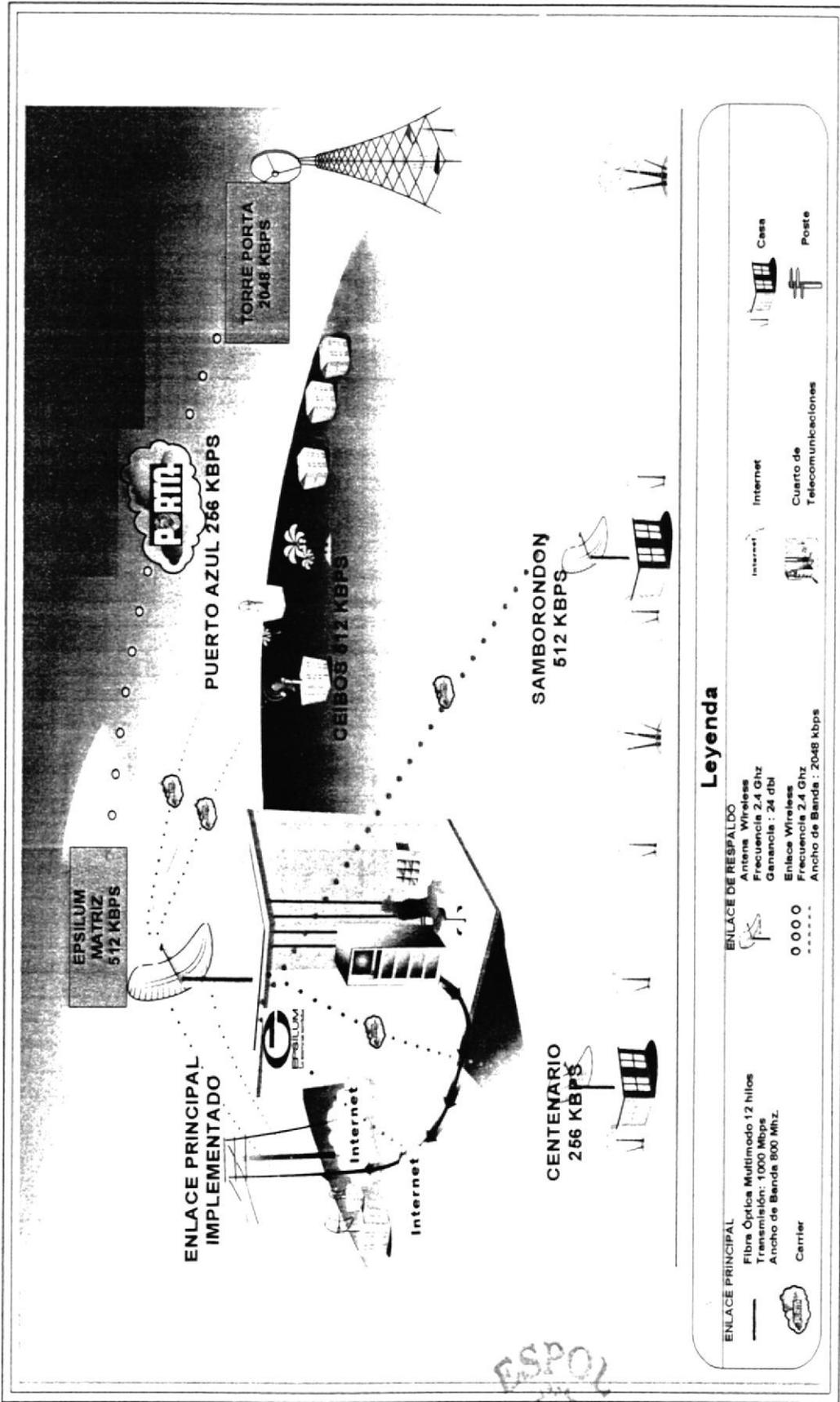
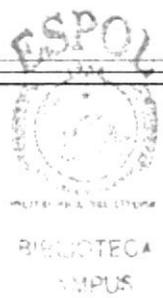


Figura 4.16. Comunicación MAN: Matriz y sucursales



4.2.1.2. COMUNICACIÓN MAN: MATRIZ Y TORRE CENTENARIO

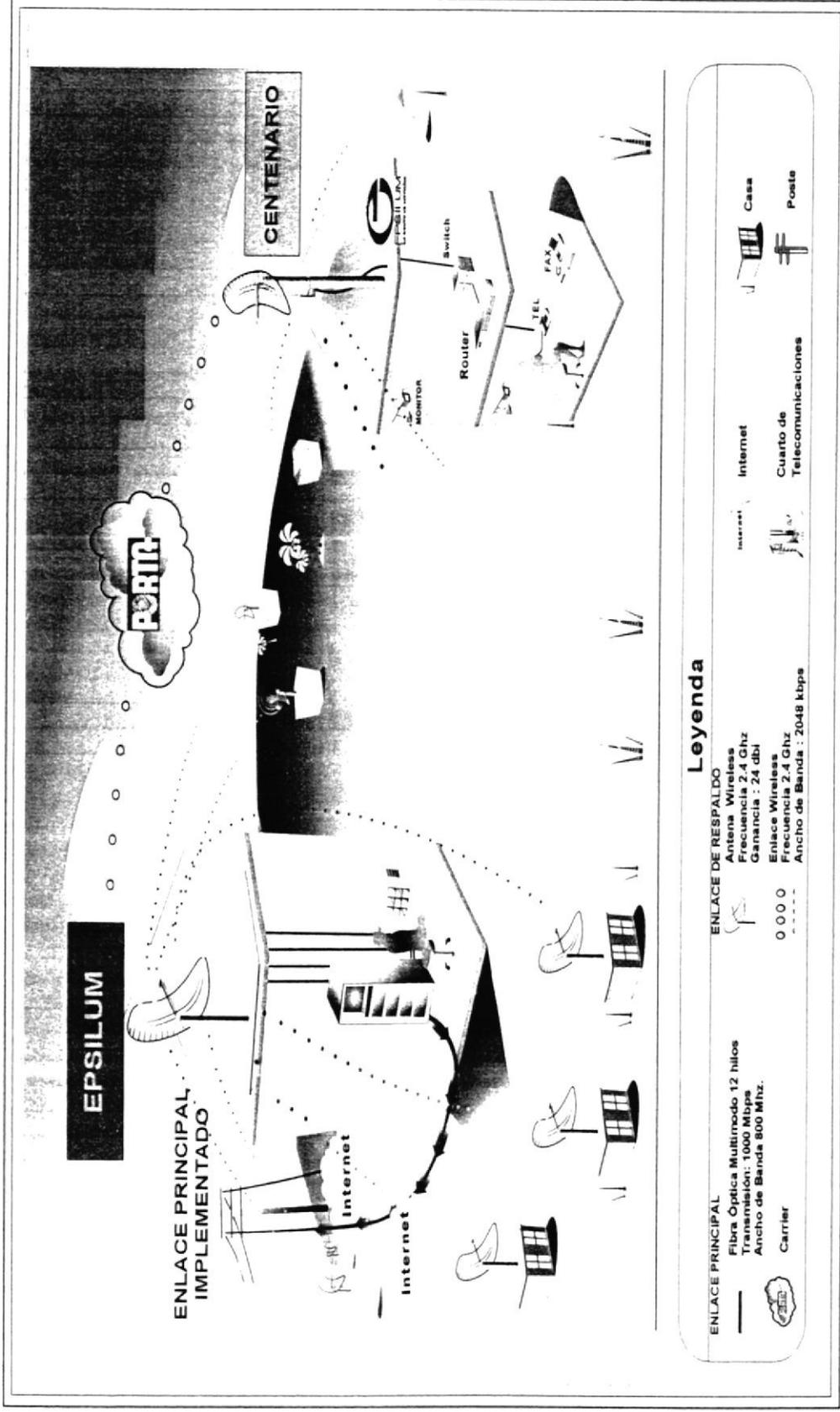


Figura 4.17. Comunicación MAN: Matriz y Torre Centenario

### 4.2.1.3. COMUNICACIÓN MAN: MATRIZ Y TORRE CEIBOS

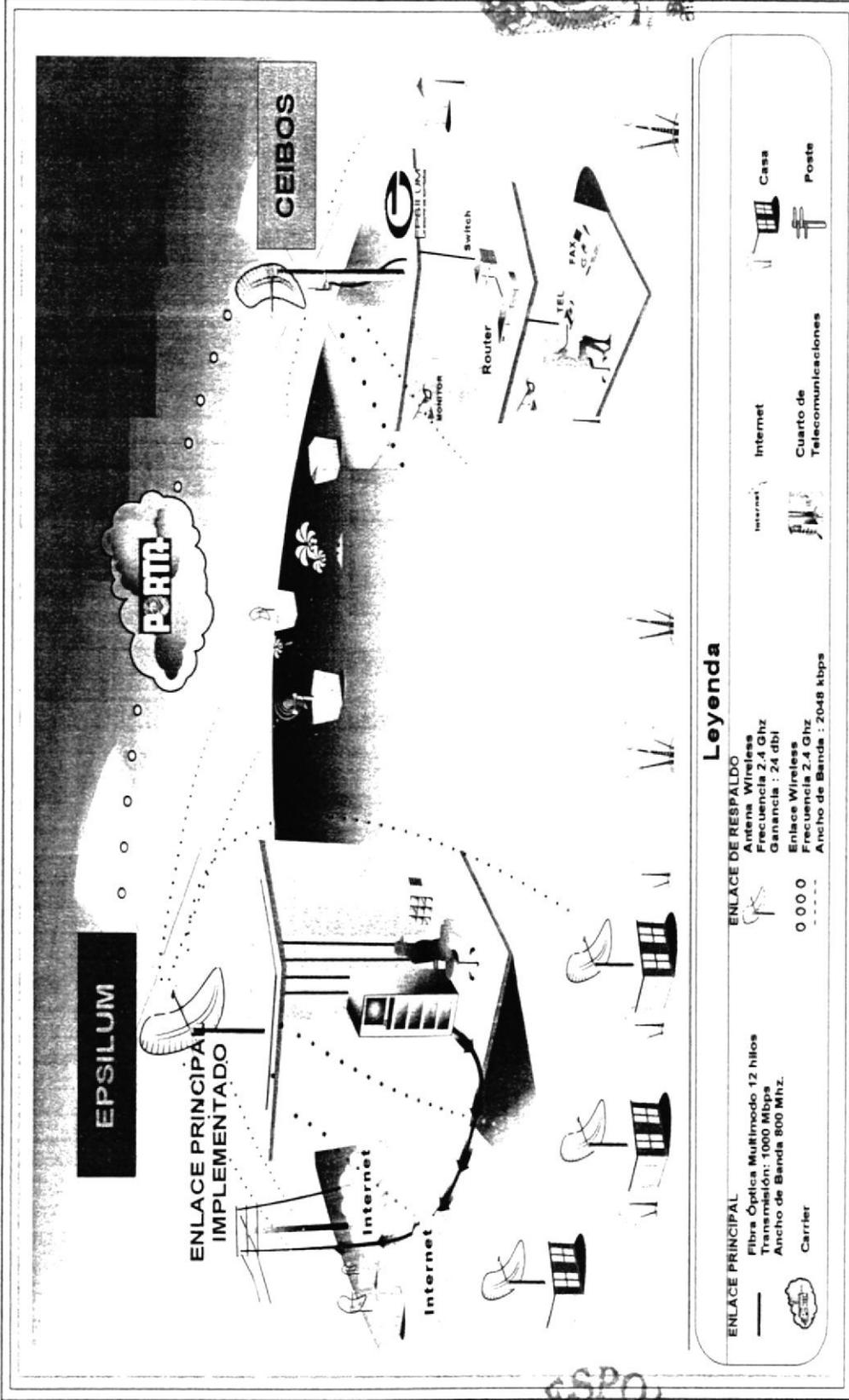


Figura 4.18. Comunicación MAN: Matriz y Torre Ceibos

4.2.1.4. COMUNICACIÓN MAN: MATRIZ Y TORRE PUERTO AZUL

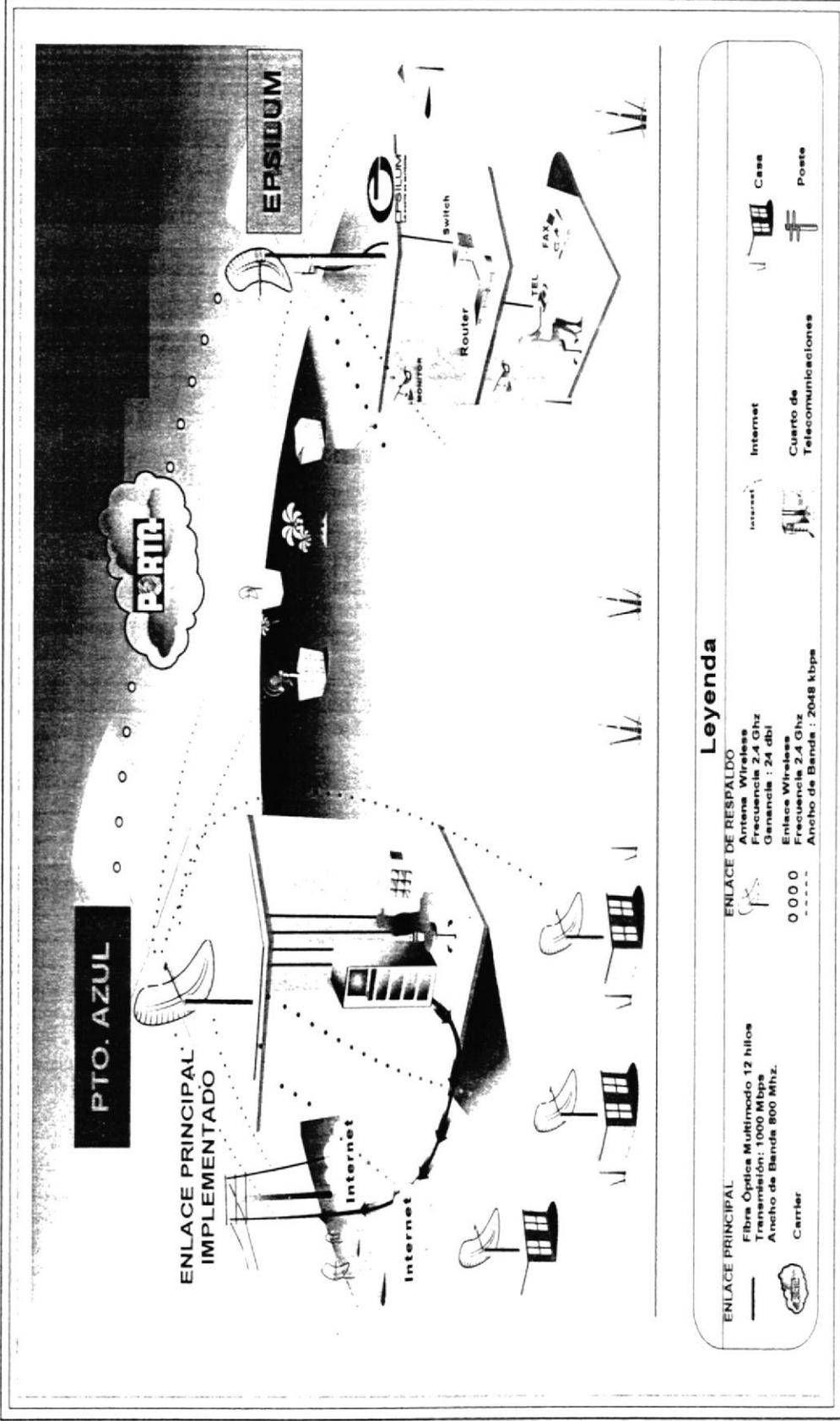


Figura 4.19. Comunicación MAN: Matriz y Torre Puerto Azul

4.2.1.5. COMUNICACIÓN MAN: MATRIZ Y TORRE SAMBORONDON

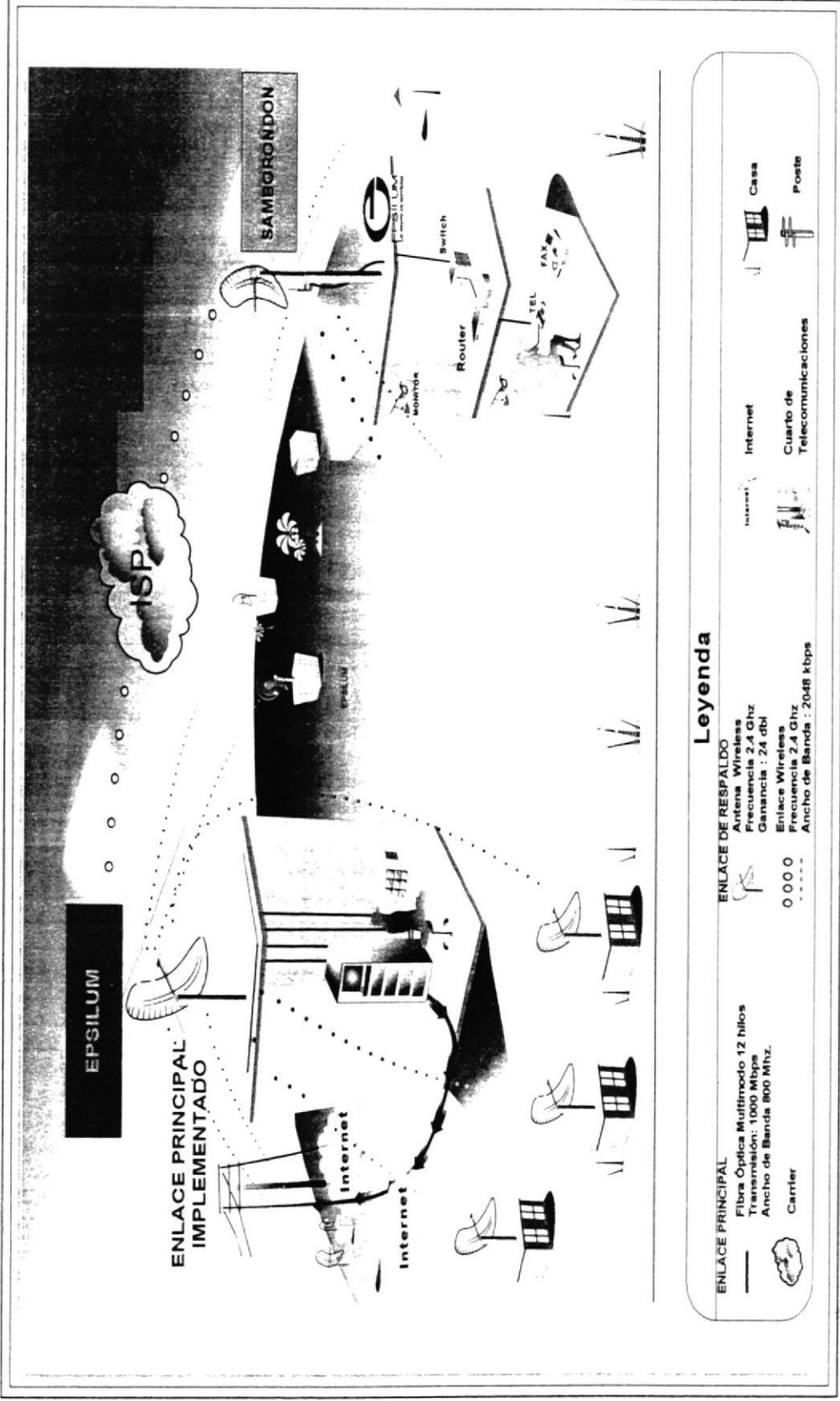


Figura 4.20. Comunicación MAN: Matriz y Torre Samborondon

4.2.2. COMUNICACIÓN WAN: AMBATO - ISP

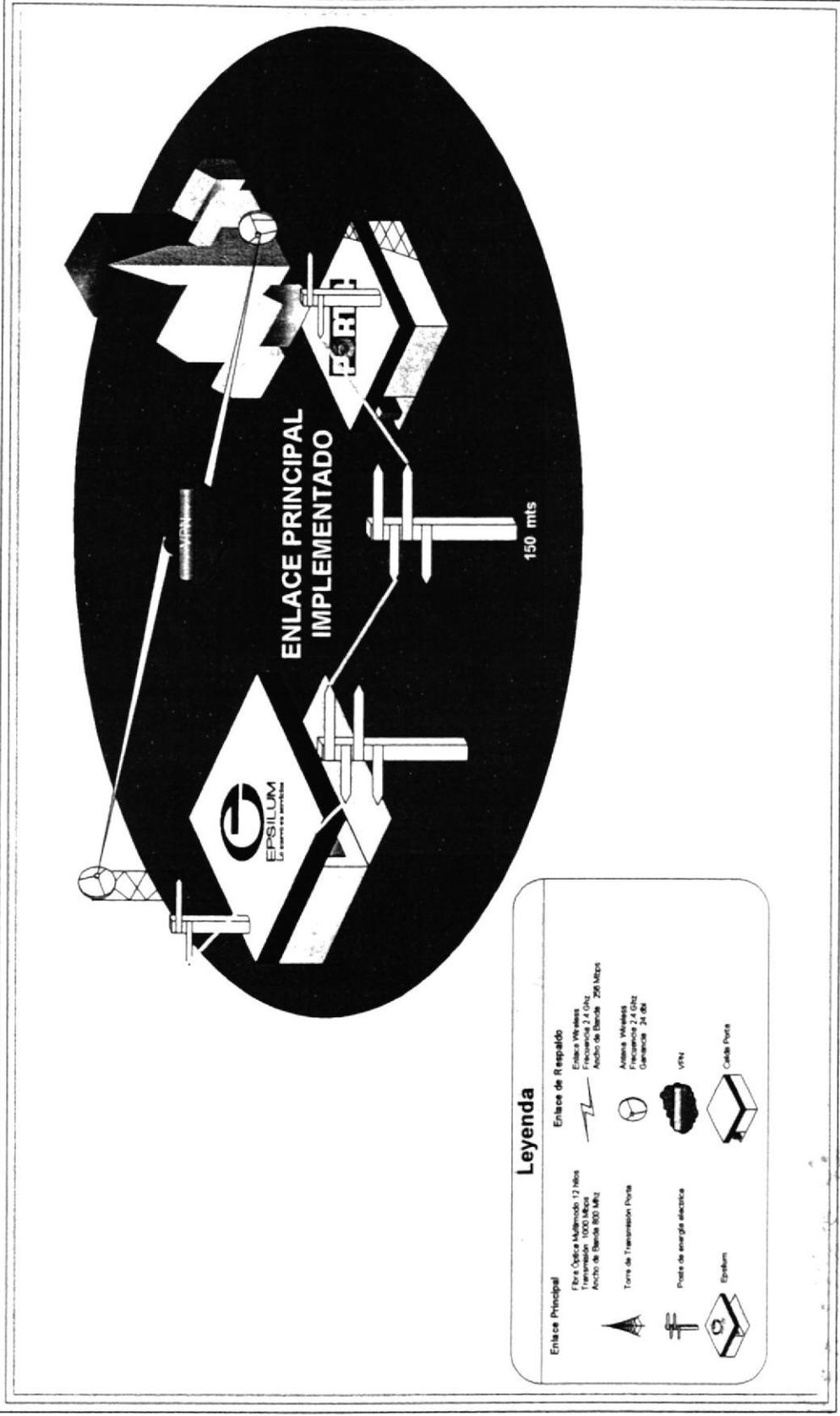


Figura 4.21. Comunicación WAN: Ambato - ISP

### 4.2.2.1. COMUNICACIÓN MAN: AMBATO Y SUCURSAL

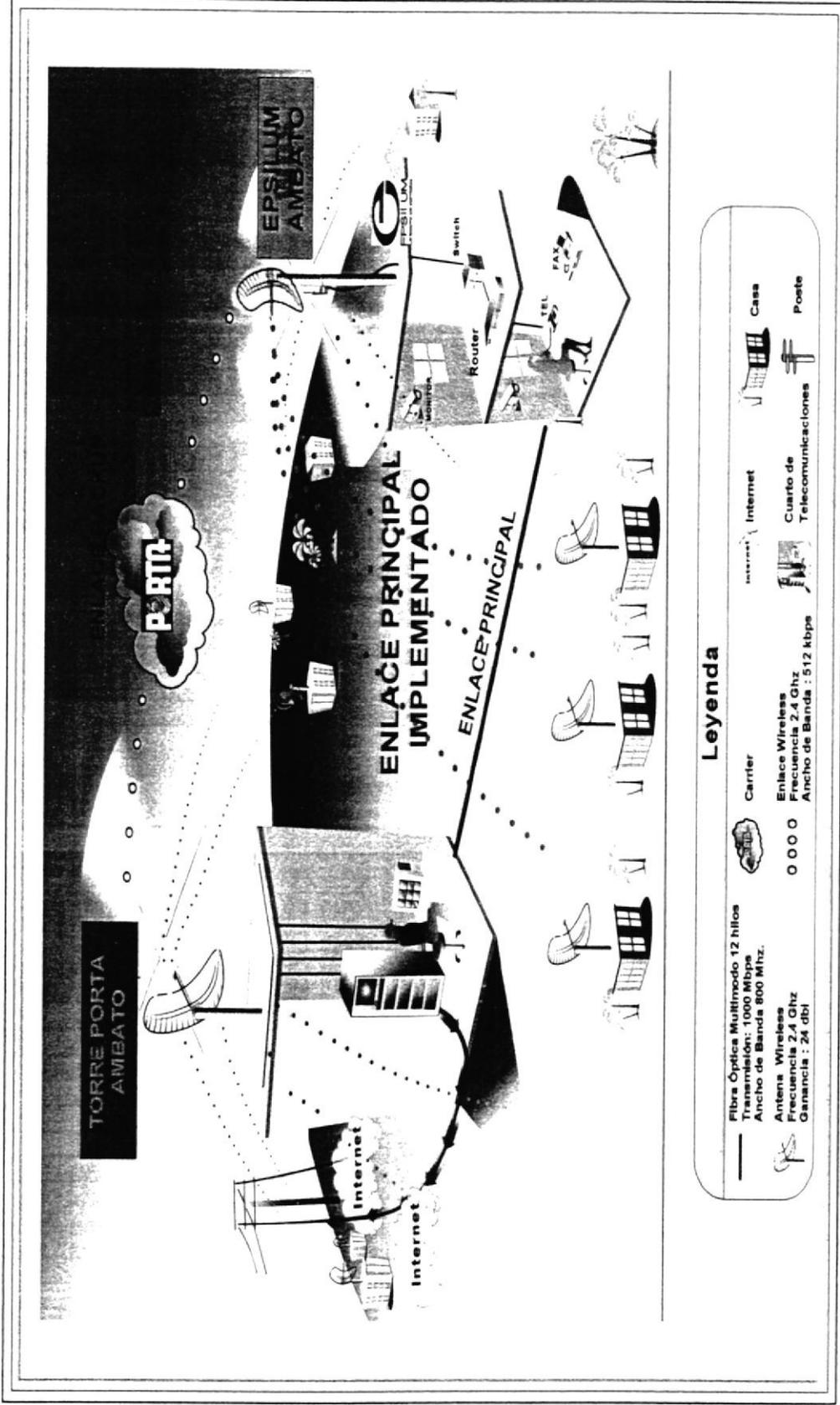


Figura 4.22. Comunicación MAN: Ambato y sucursal

### 4.2.3. COMUNICACIÓN WAN: LOJA - ISP

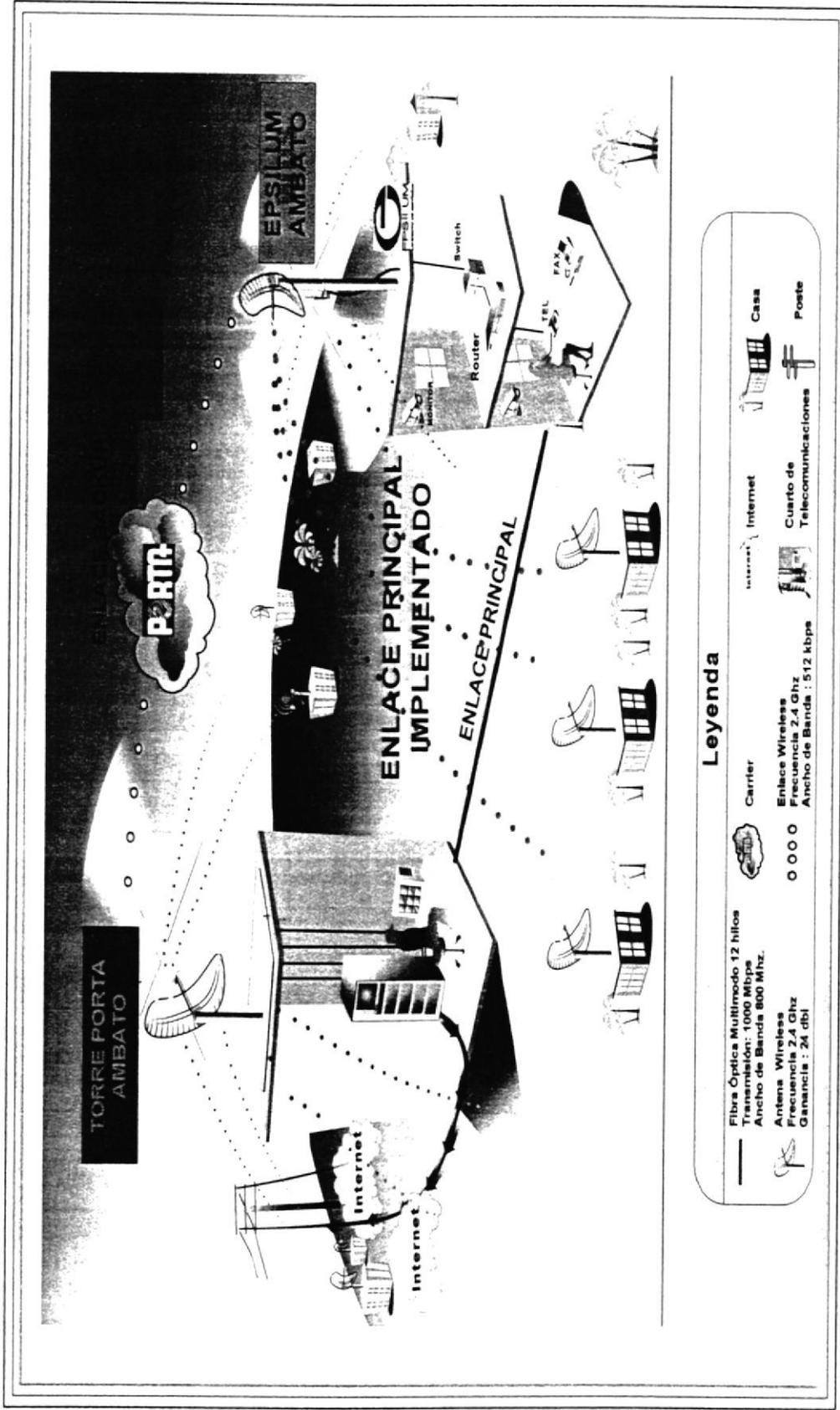


Figura 4.23. Comunicación WAN: Loja - ISP

### 4.2.3.1. COMUNICACIÓN MAN: LOJA Y SUCURSAL

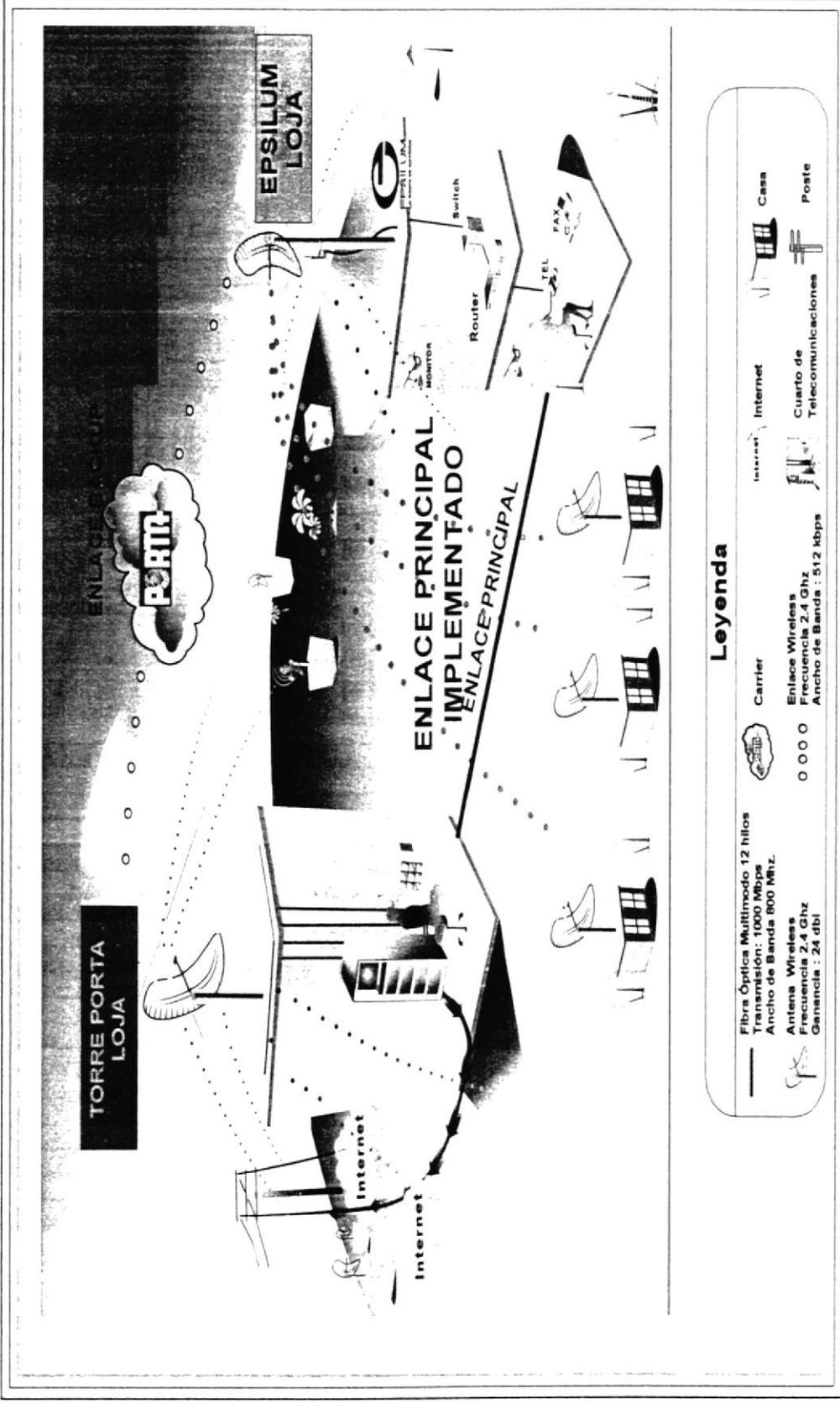


Figura 4.24. Comunicación MAN: Loja y sucursal



### 4.2.4. COMUNICACIÓN A NIVEL DE DISPOSITIVOS

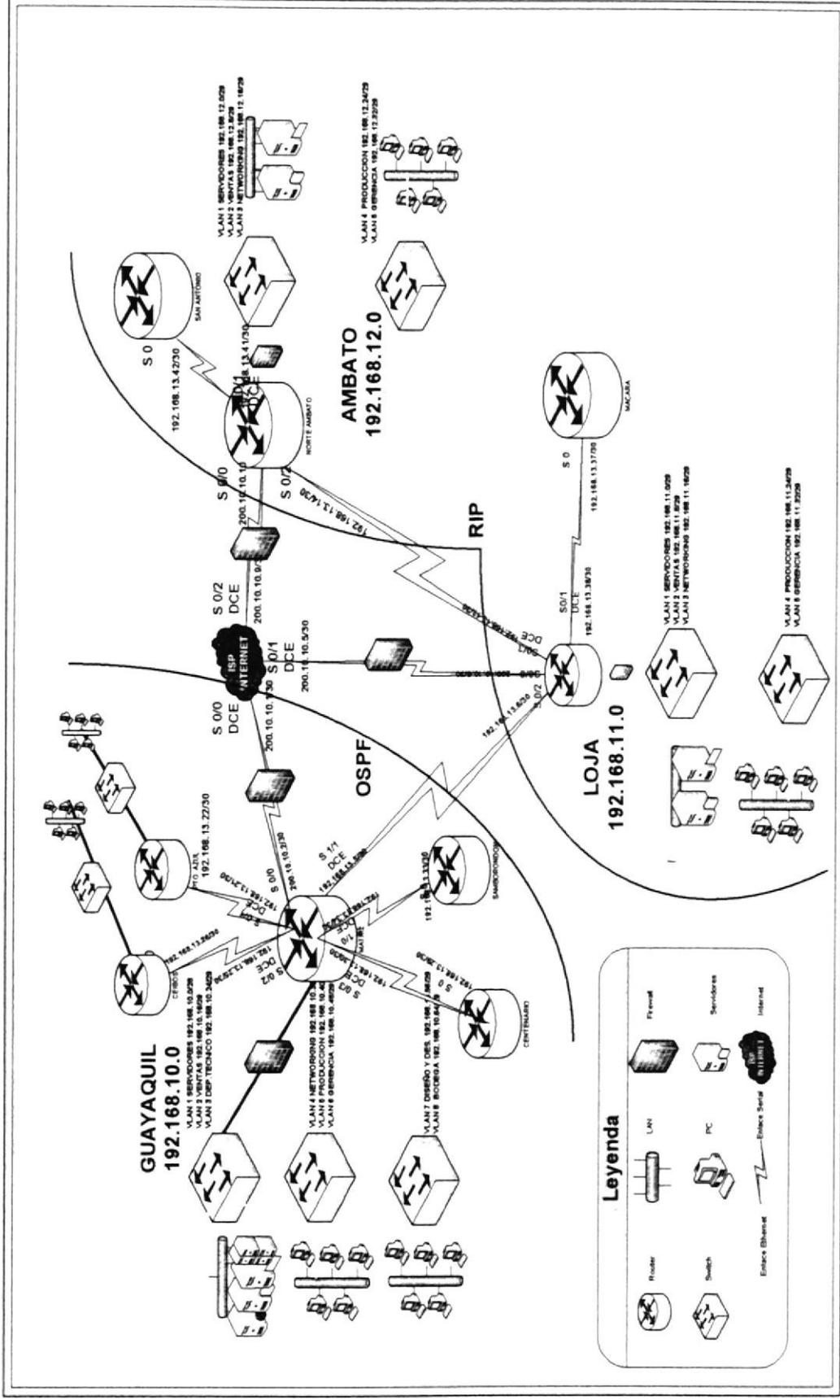


Figura 4.25. Comunicación a nivel de dispositivos

4.2.5. COMUNICACIÓN A NIVEL DE MEDIOS

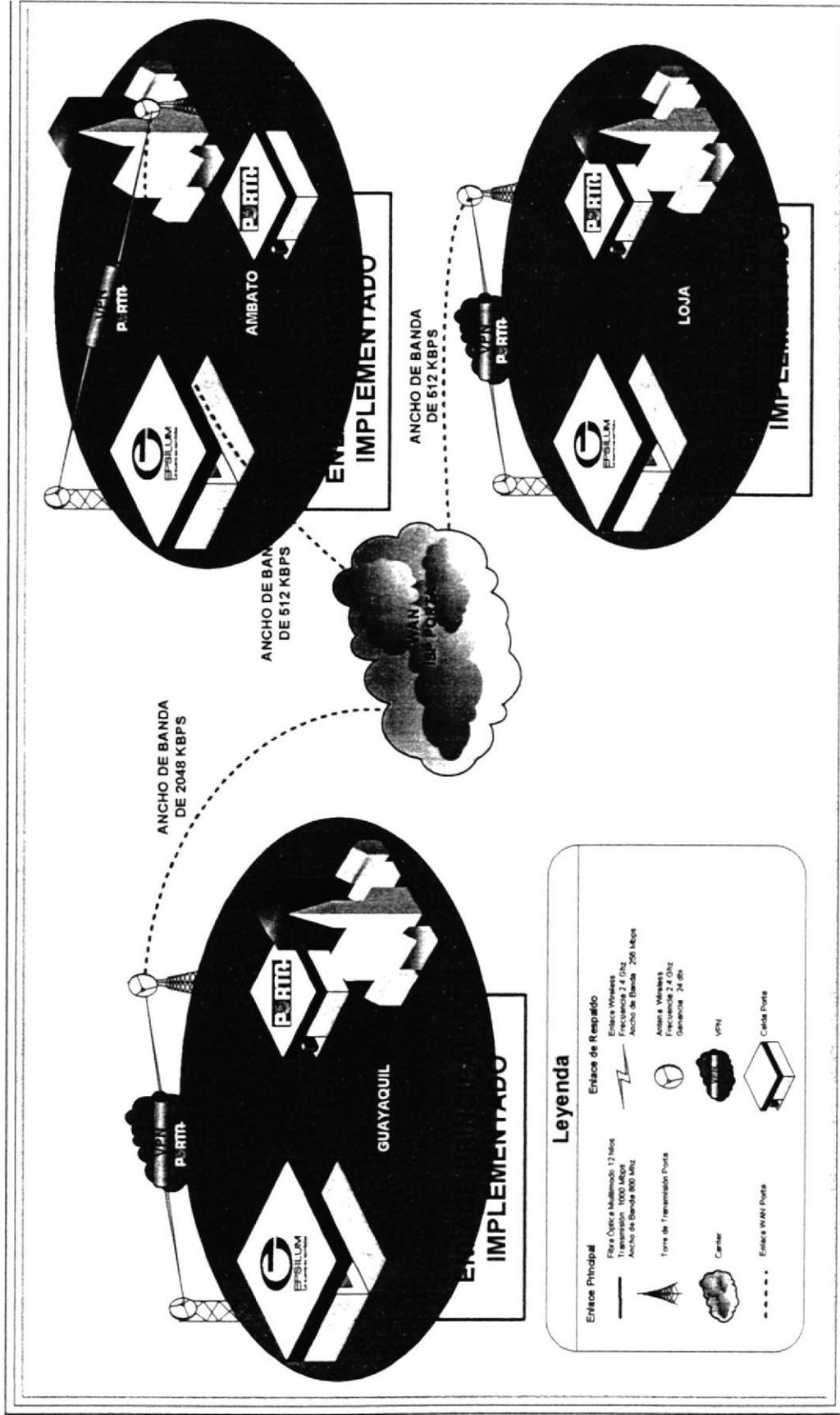


Figura 4.26. Comunicación a nivel de medios

### 4.3. RECEPCIÓN DE INTERNET

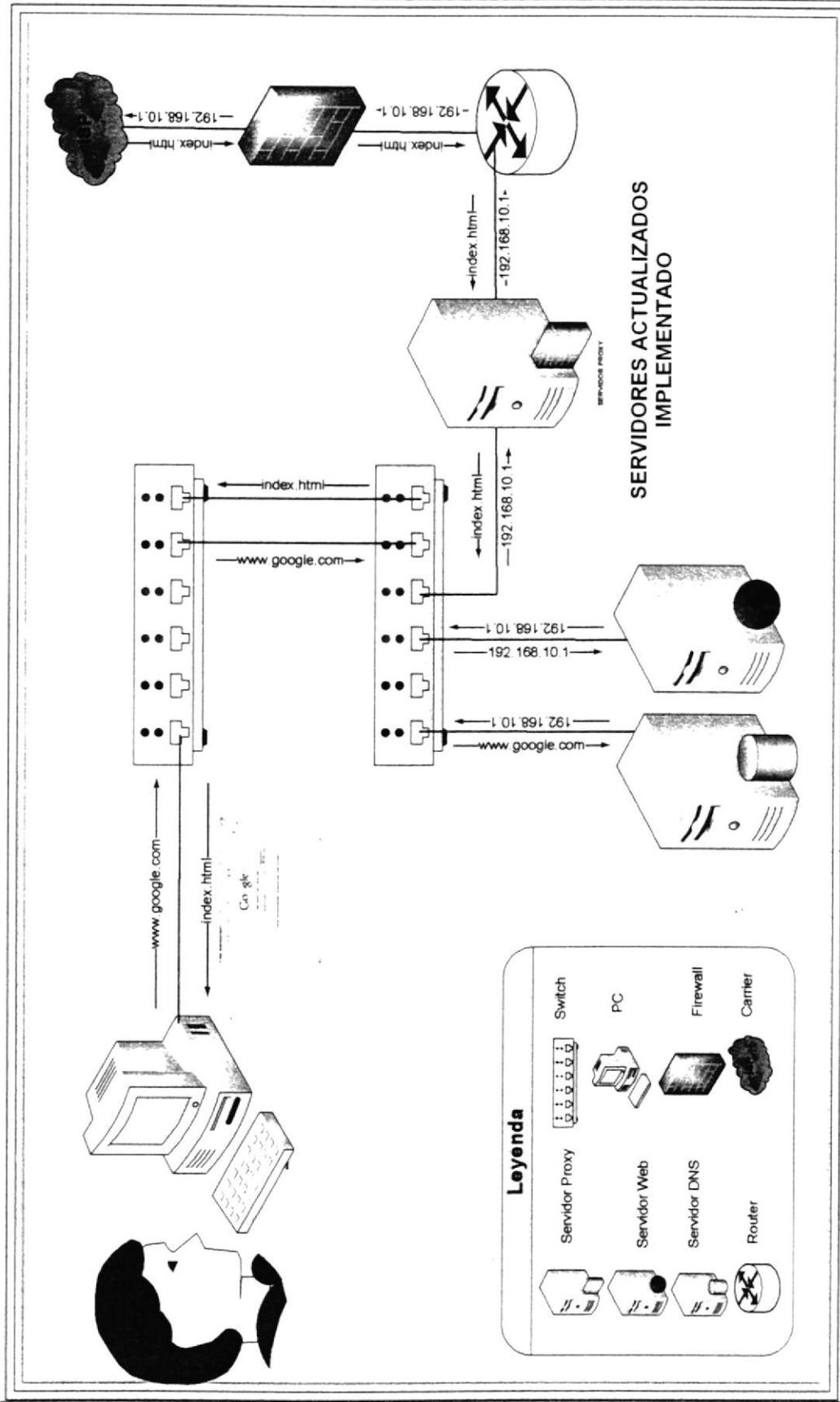


Figura 4.27. Recepción de Internet

### 4.4. INTRANET

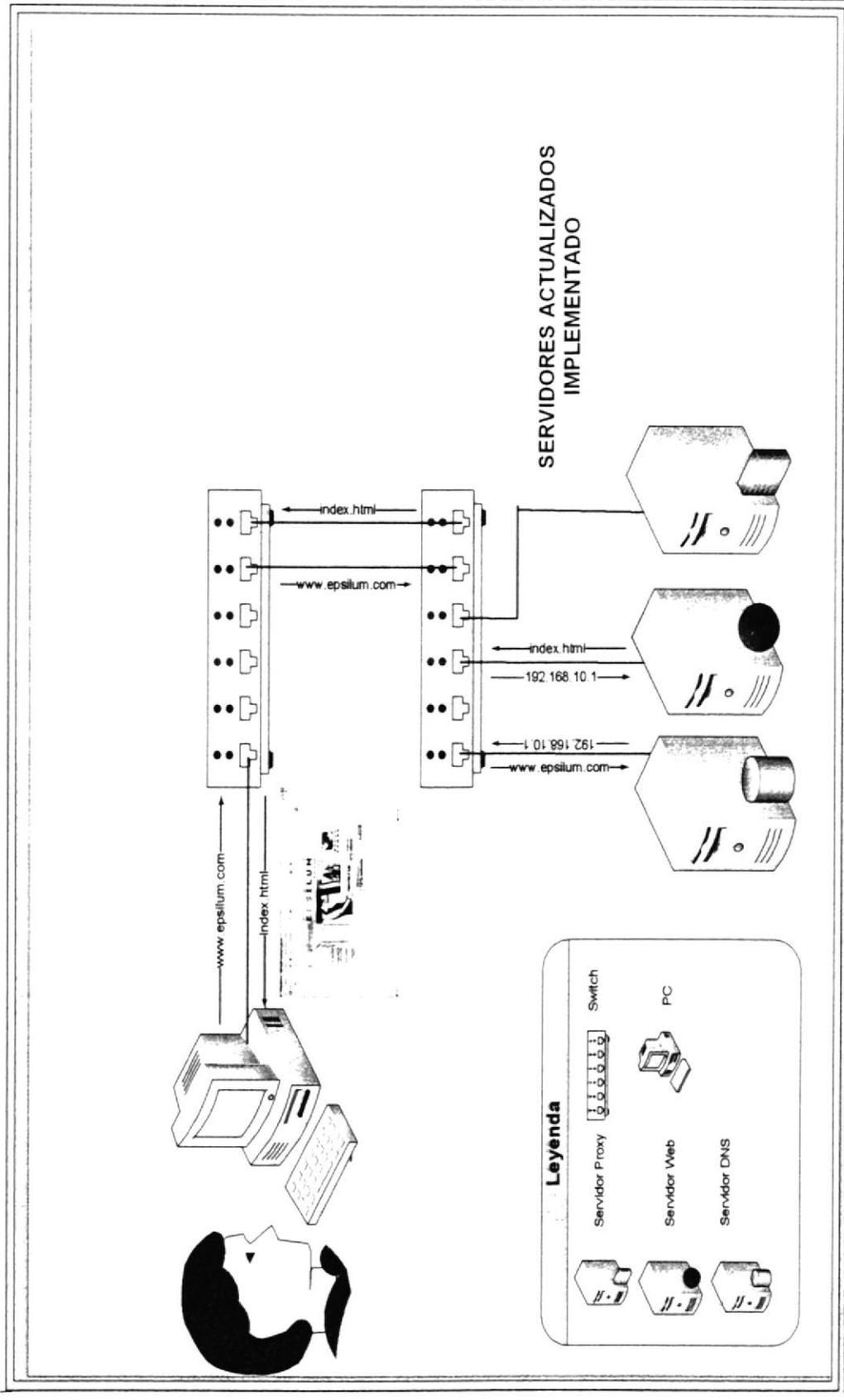
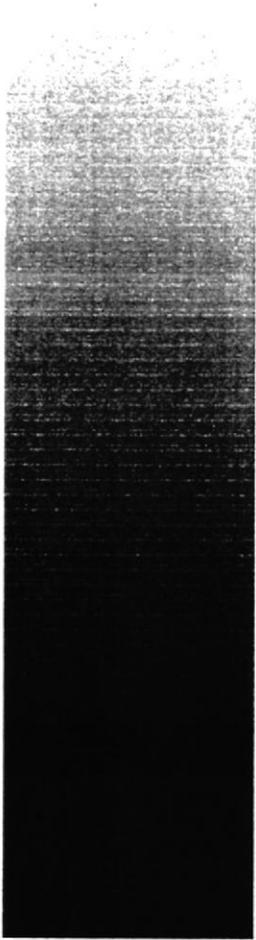


Figura 4.28. Intranet



## **CAPÍTULO 5**

---

# **NORMATIVAS DE CABLEADO ESTRUCTURADO**

## 5. NORMATIVAS DE CABLEADO ESTRUCTURADO

### 5.1 NORMATIVA # 1

Para evitar problemas causados por emisiones electromagnéticas provenientes de cable de potencia y otros equipos, todo el sistema debe estar puesto y unido a tierra cumpliendo los reglamentos y normas aplicables.

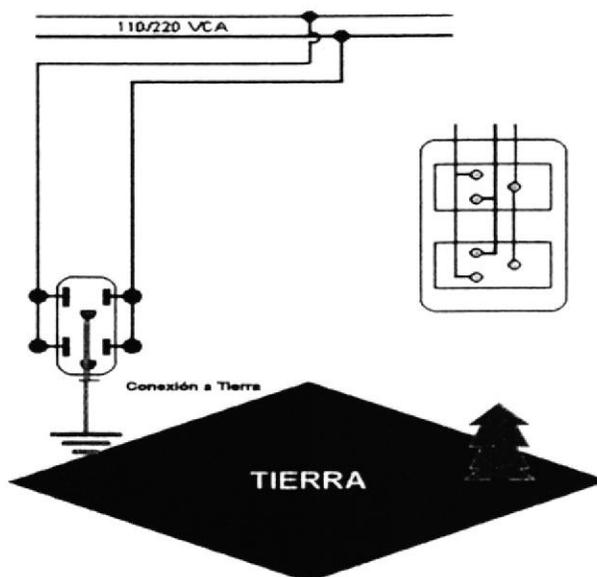


Figura 5. 1. Normativa 1

### 5.2 NORMATIVA # 2

El cableado horizontal debe estar configurada como topología estrella, cada salida de telecomunicaciones conectada a un HC.

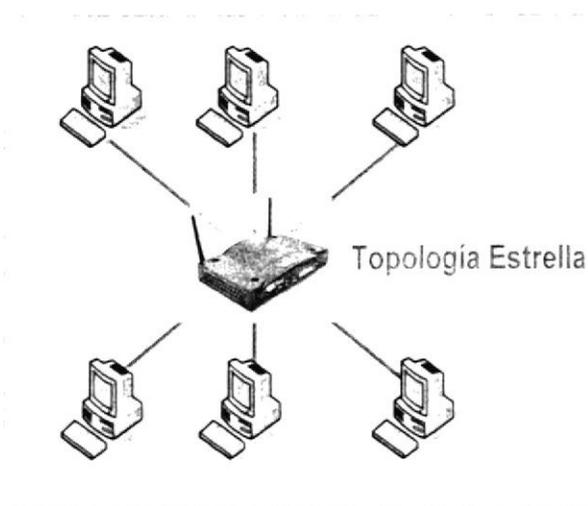


Figura 5. 2. Normativa 2

### 5.3 NORMATIVA 3

Se empleará conexiones cruzadas para conexiones entre cableado horizontal y backbone y para conexiones entre cableado horizontal y equipos con salida de puerto múltiple.

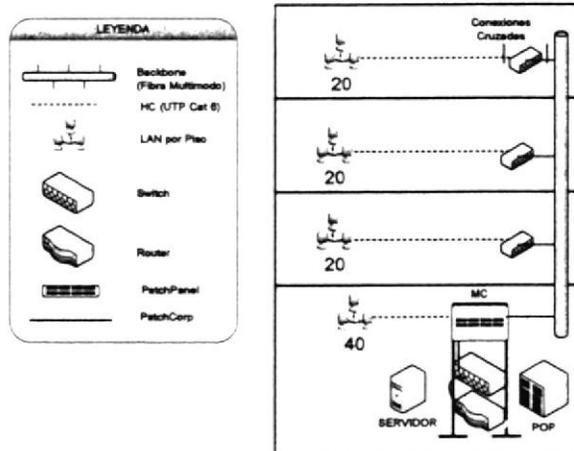


Figura 5. 3. Normativa 3

#### 5.3.1 RECOMENDACIÓN 1

Se puede emplear interconexiones para conexiones entre cableado horizontal y equipos con puertos individuales.

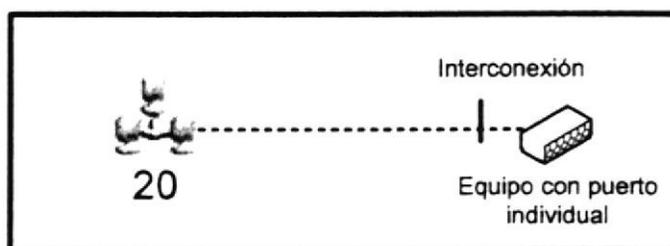


Figura 5. 4. Recomendación 1

### 5.3.2 RECOMENDACIÓN 2

Con el fin de proveer una infraestructura capaz de acomodar un ambiente de oficina dinámica, se recomienda enfáticamente un mínimo de un cuarto de telecomunicaciones en cada piso.

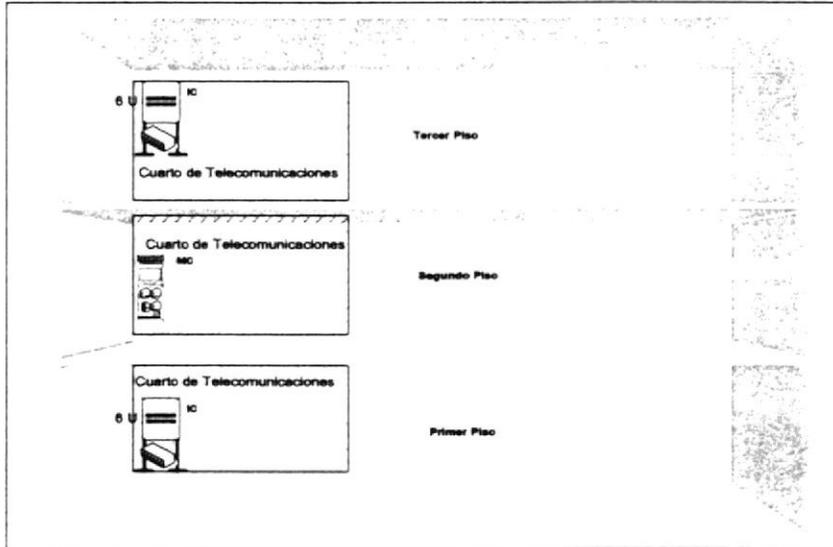


Figura 5. 5. Recomendación 2



### 5.4 NORMATIVA 4

Cada área de trabajo será atendida por un HC, localizado en el mismo piso o en un piso adyacente.

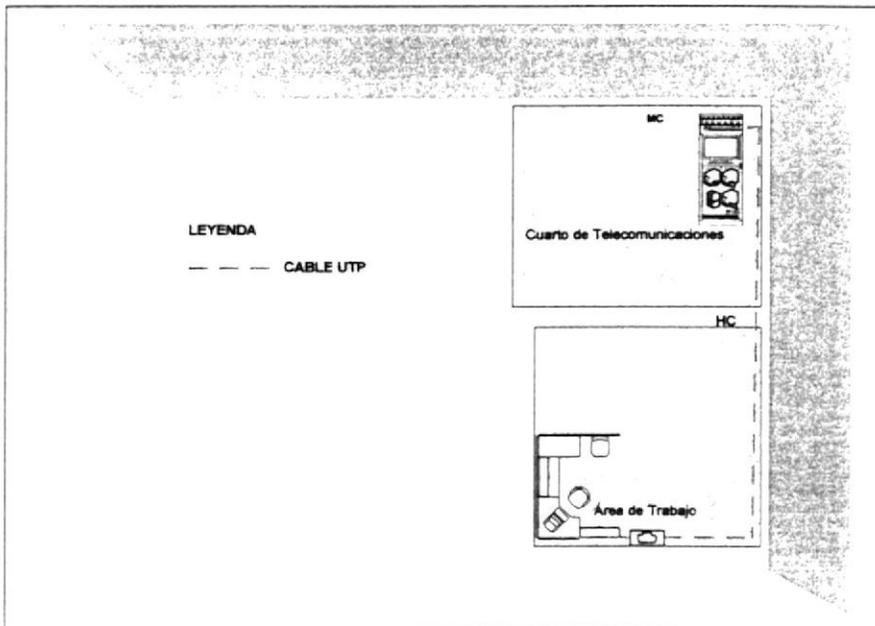


Figura 5. 6. Normativa 4

### 5.4.1 RECOMENDACIÓN 3

El área que puede atenderse efectivamente por un cuarto de telecomunicaciones abarca un radio máximo de 60 metros.

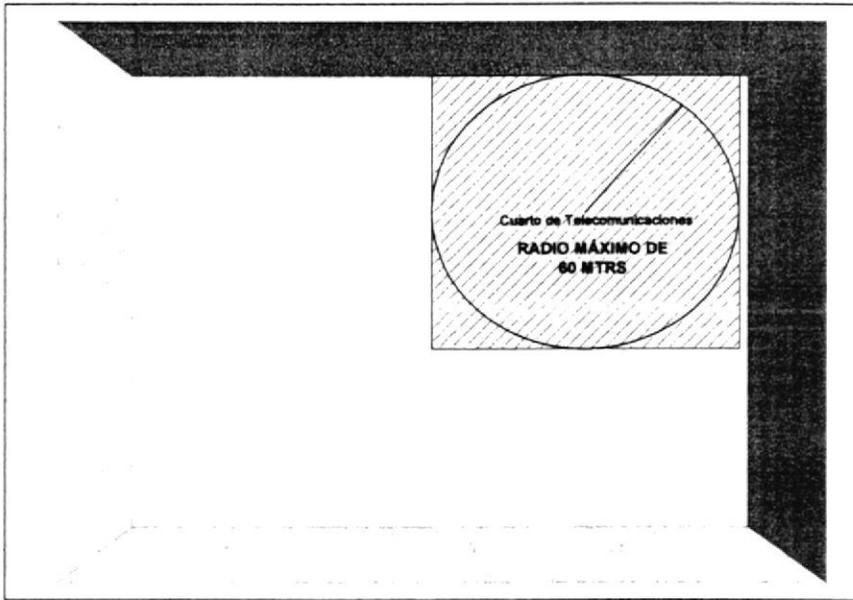


Figura 5. 7. Recomendación 3

### 5.5 NORMATIVA 5

No se permite el uso de derivaciones puenteadas en el cableado horizontal

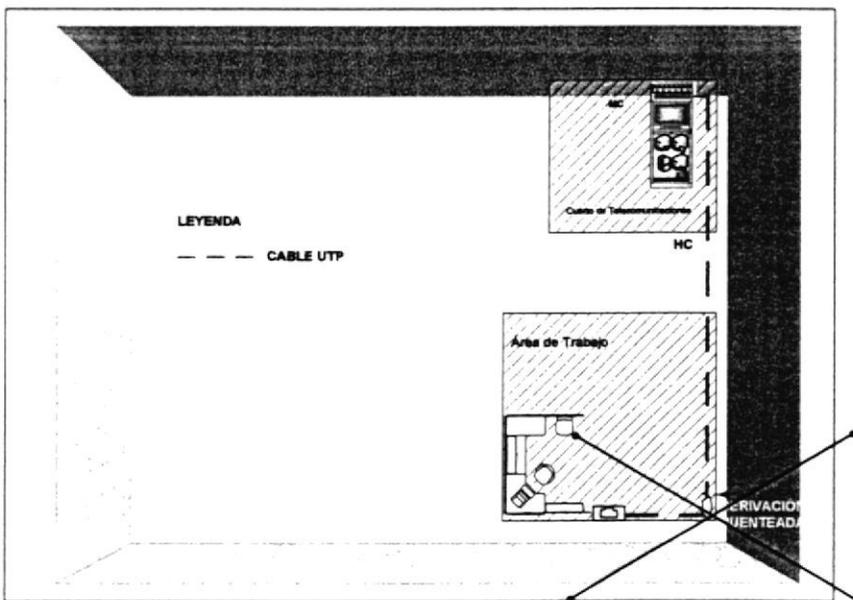


Figura 5. 8. Normativa 5

## 5.6 NORMATIVA 6

La longitud del cable entre la salida de telecomunicaciones y el HC no se excederá los 90 metros, independiente del tipo de medio.

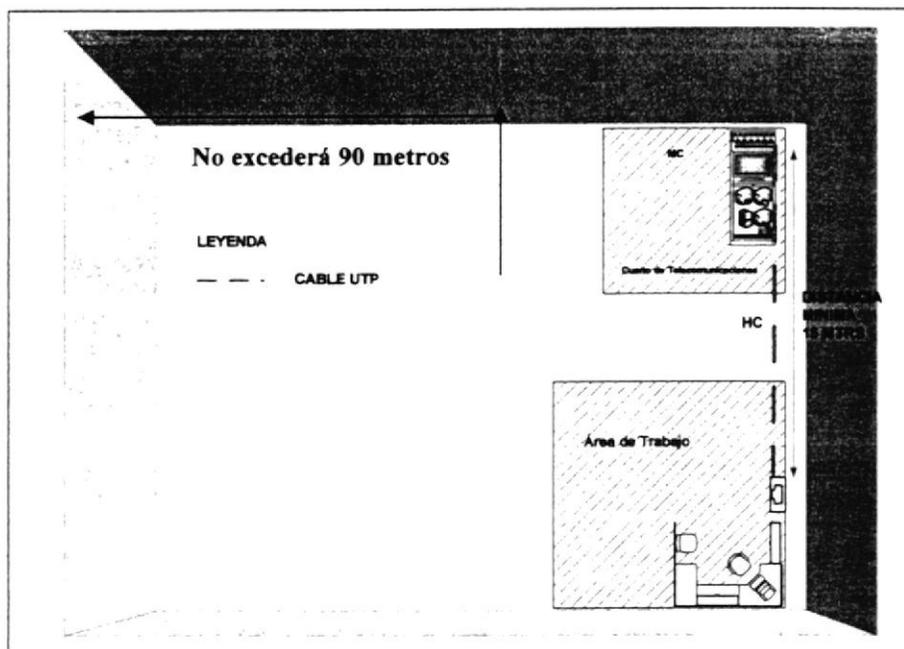


Figura 5. 9. Normativa 6

### 5.6.1 RECOMENDACIÓN 4

Se recomienda un mínimo de 15 metros entre el HC y la salida de telecomunicaciones.

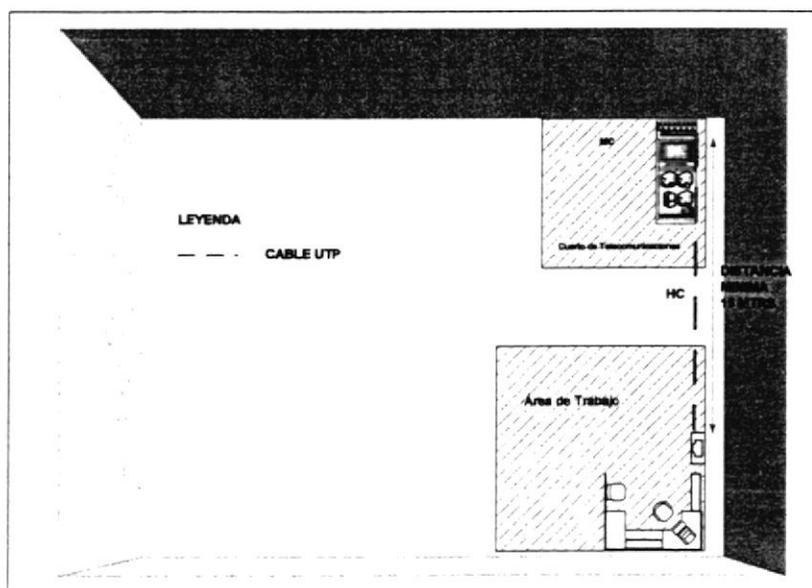


Figura 5. 10. Recomendación 4

## 5.7 NORMATIVA 7

La longitud individual o combinada del Patch Cord de Par Trenzado balanceado 24 awg (calibre americano de alambre) o fibra óptica usado en el HC, no excederá los 5 metros.

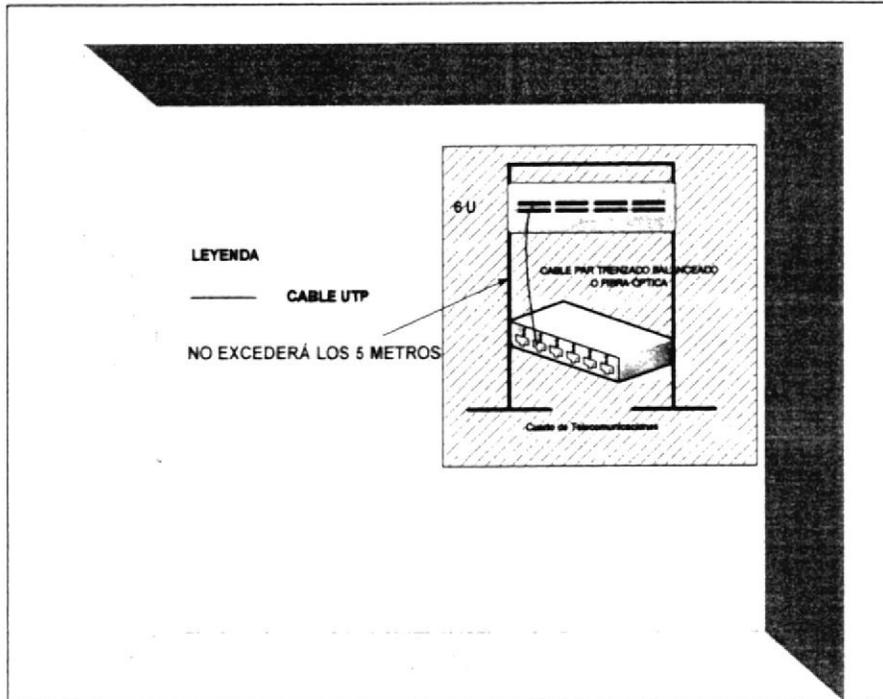


Figura 5. 11. Normativa 7

## 5.8 NORMATIVA 8

La longitud del canal del cableado horizontal incluyendo los Patch Cord de equipos en ambos términos no excederá los 100 metros independiente del medio.

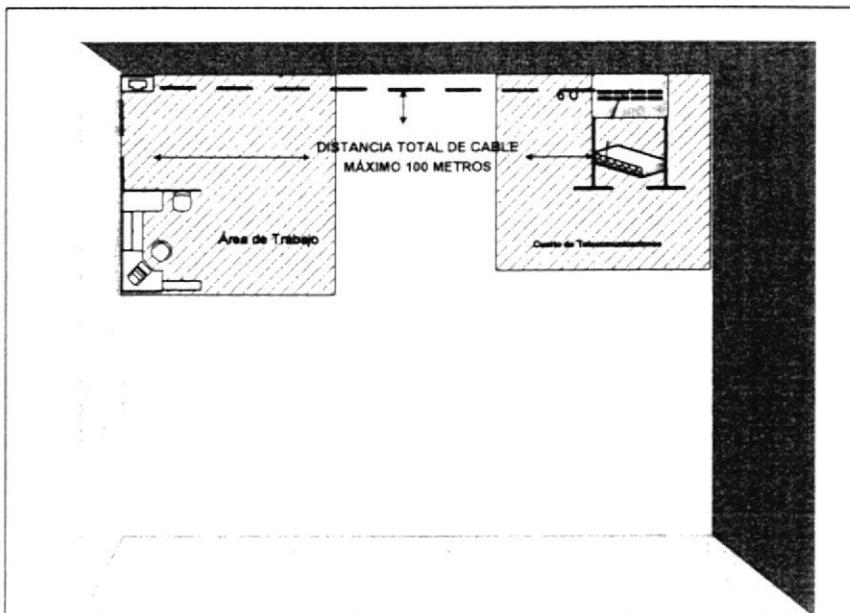


Figura 5. 12. Normativa 8

### 5.8.1 RECOMENDACIÓN 5

Se recomienda un mínimo de dos salidas de categoría 6 por cada área de trabajo individual con el fin de soportar las numerosas aplicaciones diseñadas para operar sobre cableado de par trenzado.

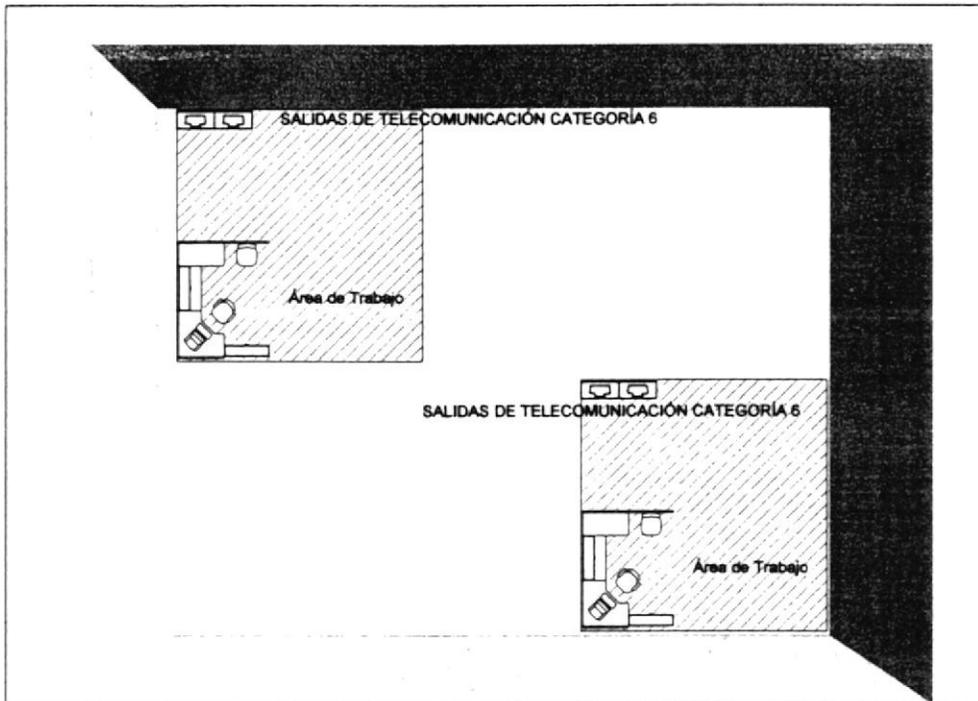


Figura 5. 13. Recomendación 5

### 5.9 NORMATIVA 9

La longitud de los cordones de equipos del área de trabajo de par trenzado balanceado no excederá los 20 metros cuando se use un punto de consolidación.

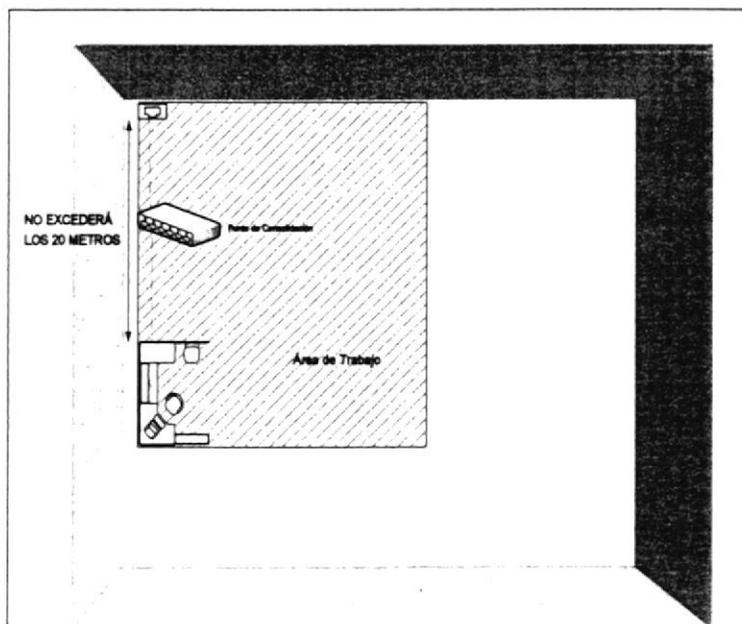
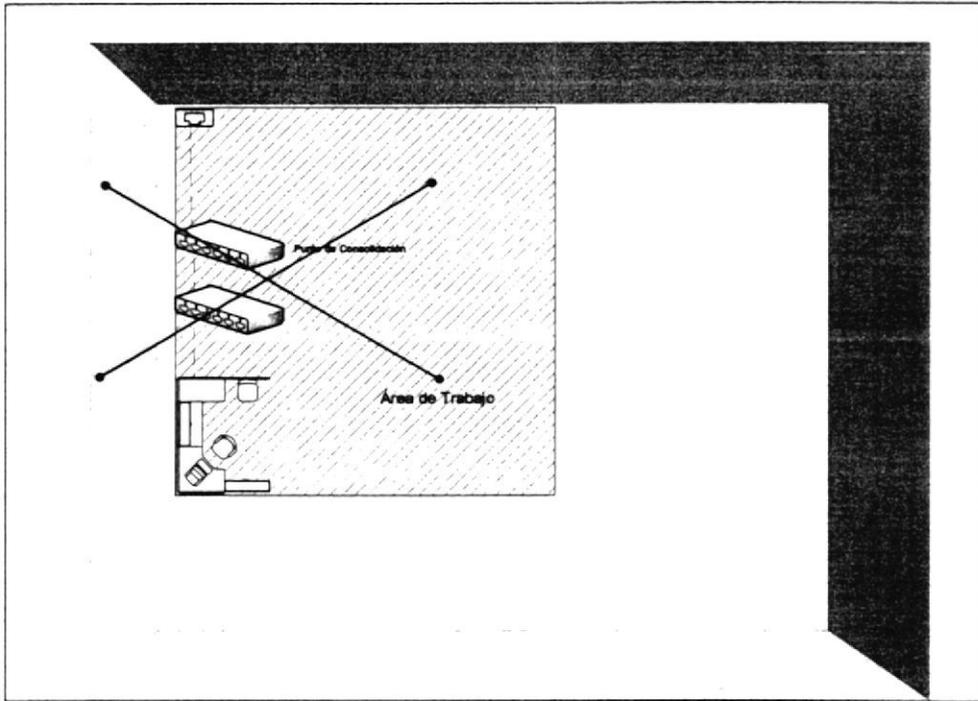


Figura 5. 14. Normativa 9

### 5.10 **NORMATIVA 10**

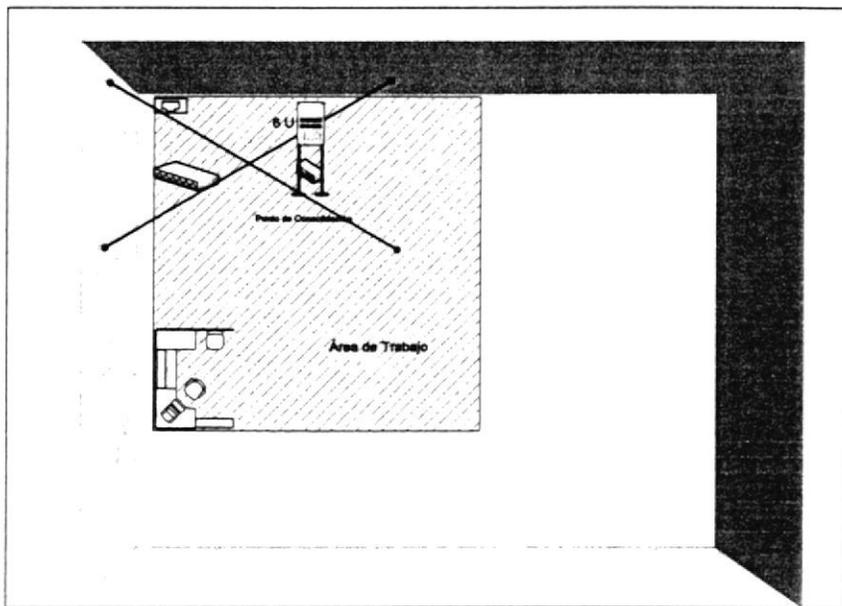
No se permitirá más de un punto de consolidación dentro del mismo tendido de cable horizontal.



**Figura 5. 15.** Normativa 10

### 5.11 **NORMATIVA 11**

No se permitirán conexiones cruzadas o equipos activos en el punto de consolidación.



**Figura 5. 16.** Normativa 11

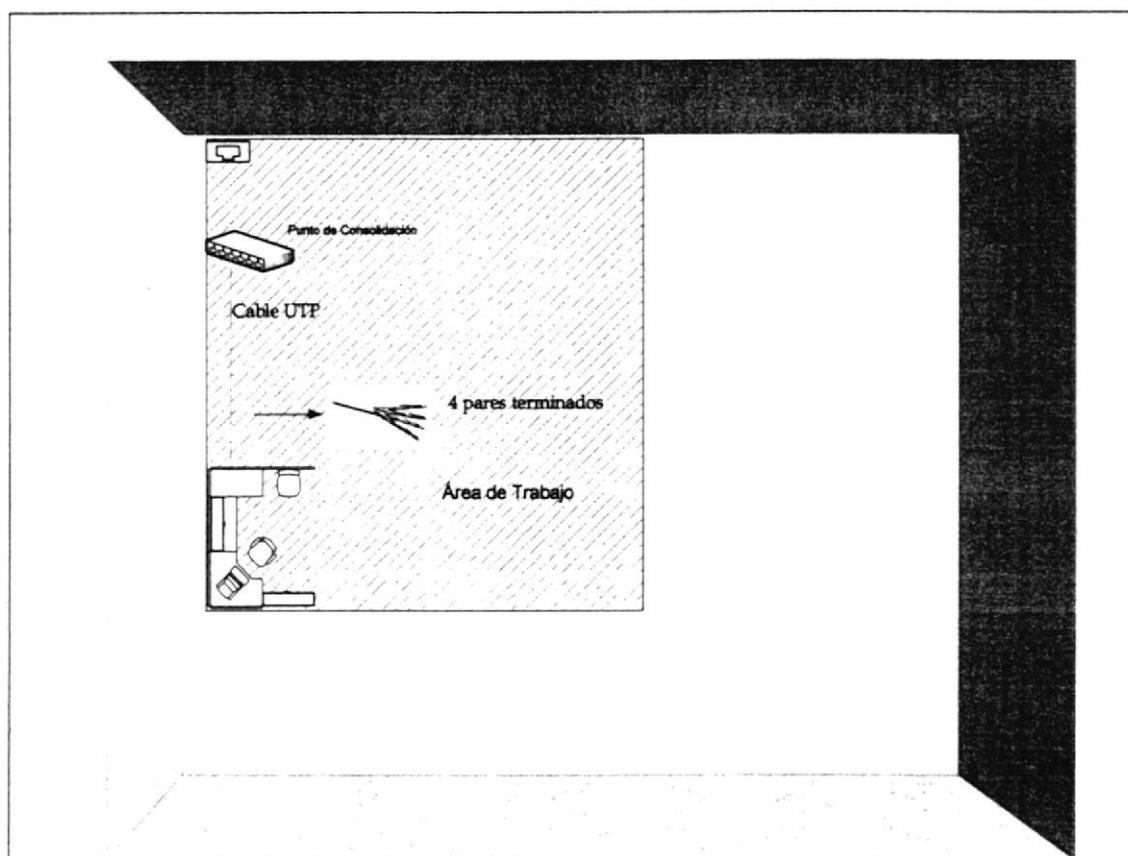
**PUNTO DE CONSOLIDACIÓN.-** Es un hardware de conexión que proporciona una interconexión entre el cableado de oficina abierta y el cableado horizontal.



**Figura 5. 17.** Punto de consolidación

## 5.12 NORMATIVA 12

Cada cable horizontal que sale del punto de consolidación tendrá sus 4 pares terminados en una toma modular de 8 posiciones en el área de trabajo.



**Figura 5. 18.** Normativa 12

### 5.13 NORMATIVA 13

La distancia máxima entre el HC y la salida de telecomunicaciones será de 90 metros.

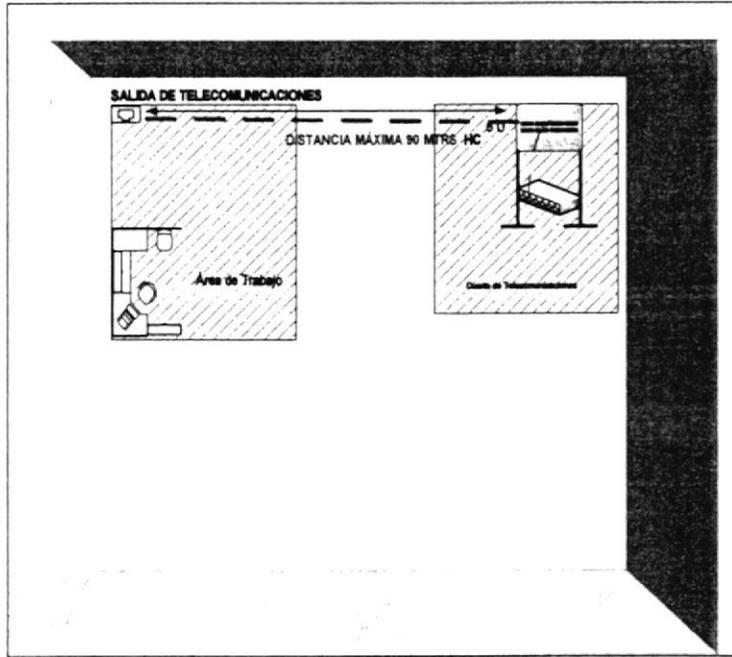


Figura 5. 19. Normativa 13

### 5.14 NORMATIVA 14

La distancia mínima entre el HC y el punto de consolidación será de 15 metros.

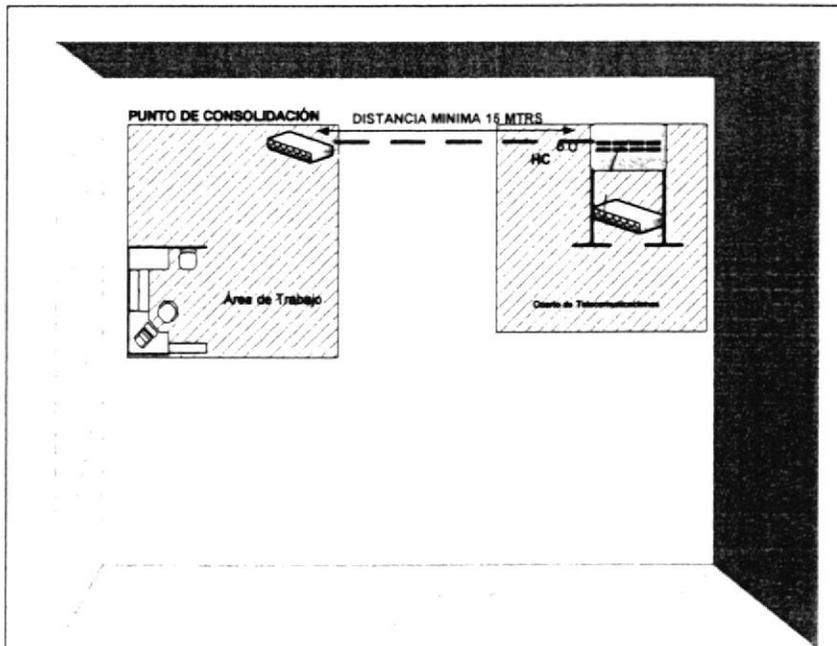


Figura 5. 20. Normativa 14

### 5.15 NORMATIVA 15

La distancia mínima entre el punto de consolidación y la salida de telecomunicación será de 5 metros.

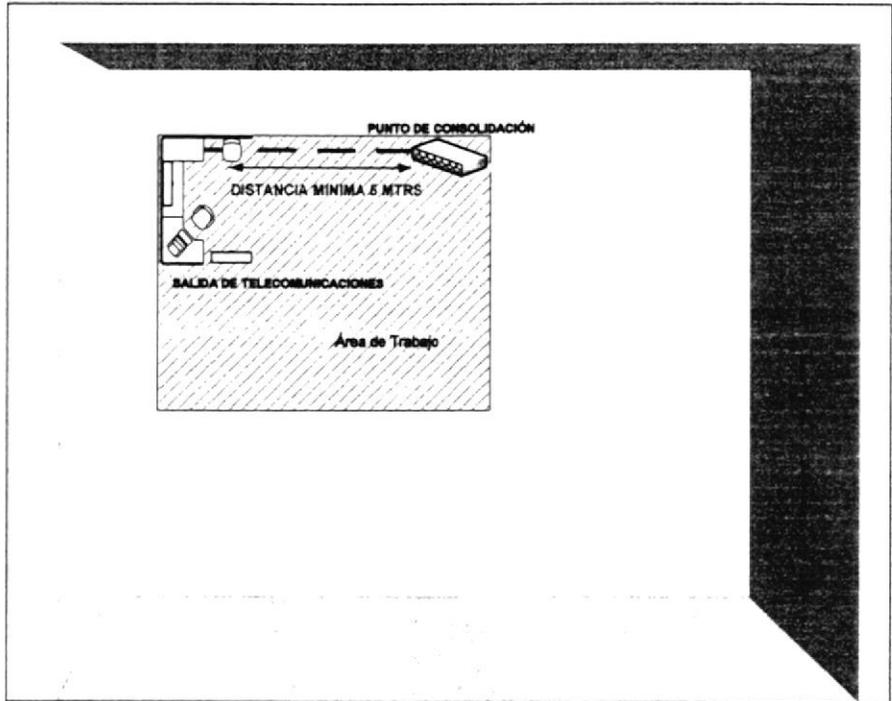


Figura 5. 21. Normativa 15

### 5.16 NORMATIVA 16

La distancia del canal del cableado horizontal incluyendo los dos cables de equipo en ambos extremos no excederá los 100 metros, independiente del medio.

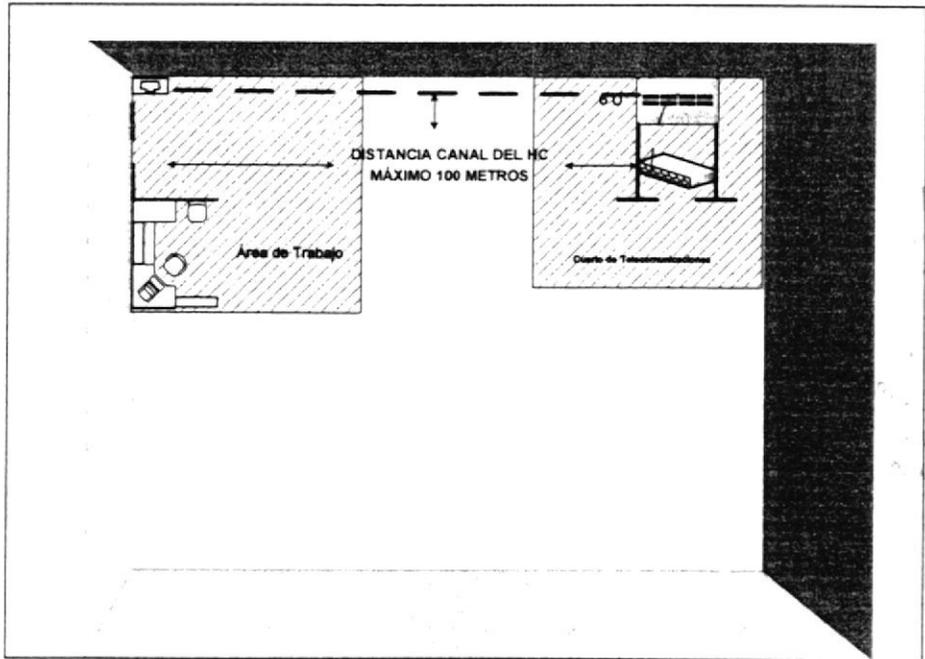


Figura 5. 22. Normativa 16

### 5.17 **NORMATIVA 17**

Todos los pares del cable estarán totalmente terminados en ambos extremos.

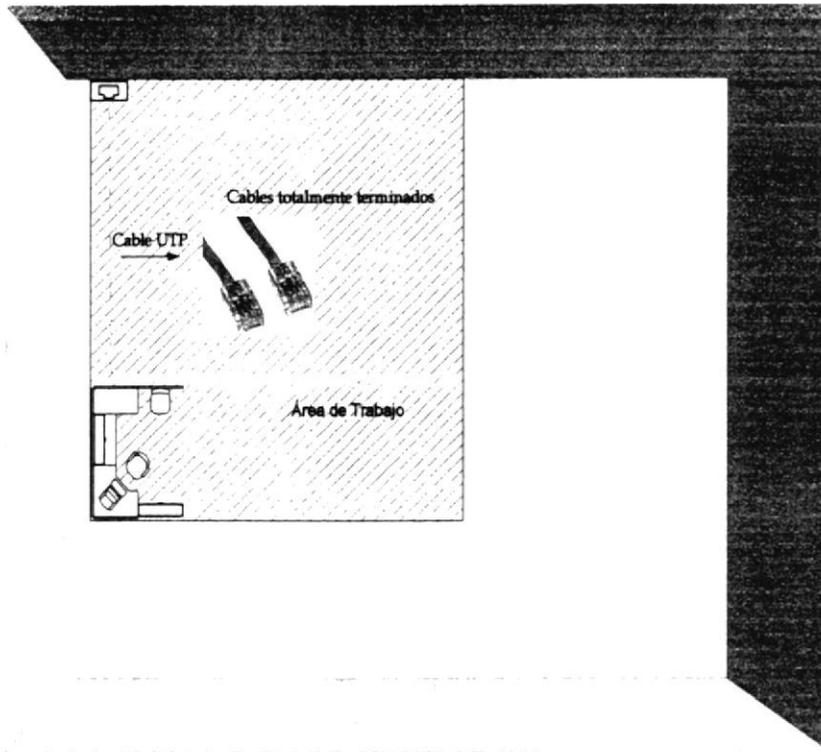


Figura 5. 23. Normativa 17

#### 5.17.1 **RECOMENDACIÓN 6**

El punto de consolidación debe estar localizado a una altura y ubicación conveniente de trabajo con el fin de facilitar la instalación y los cambios.

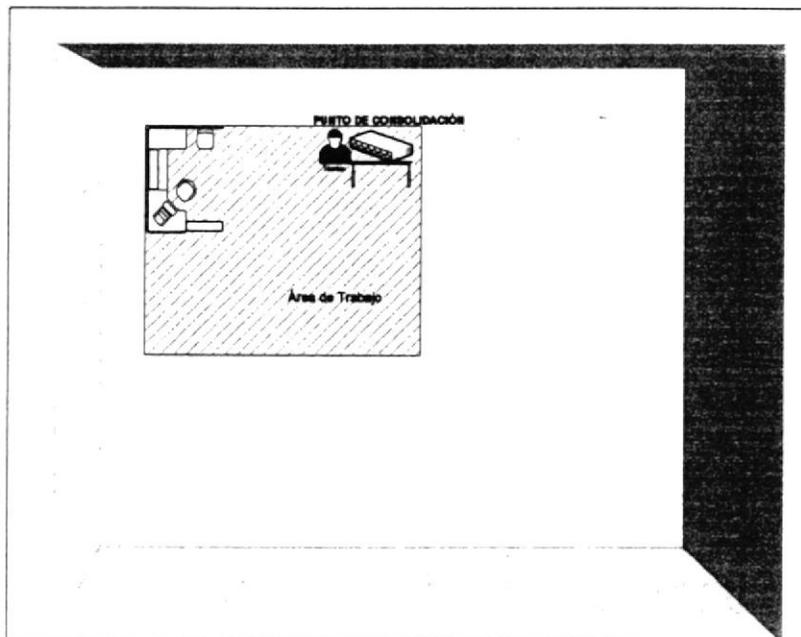


Figura 5. 24. Recomendación 6

## 5.18 NORMATIVA 18

La longitud del canal del cableado de fibra óptica multimodo no excederá los 300 metros.

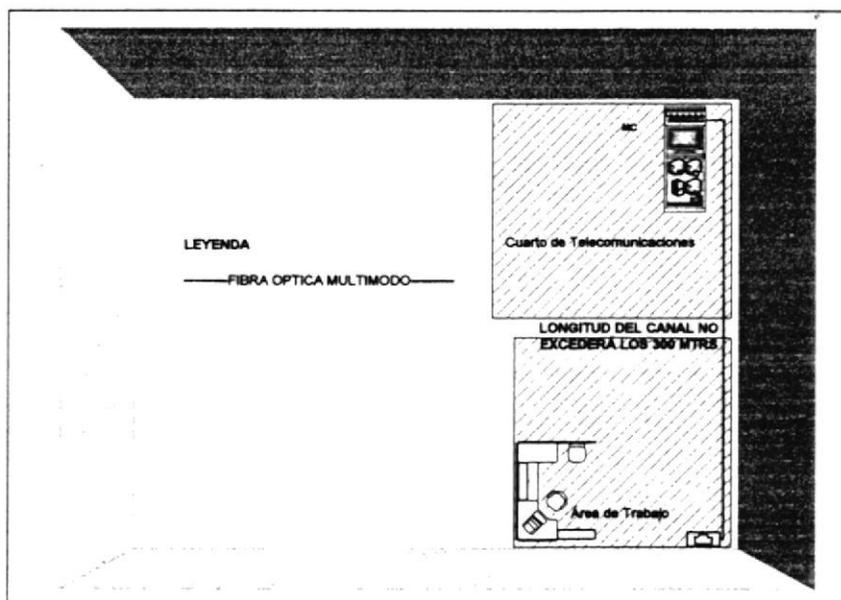


Figura 5. 25. Normativa 18

### 5.18.1 RECOMENDACIÓN 7

El cableado de backbone de edificio debe diseñarse con la capacidad de reserva suficiente para atender salidas adicionales de telecomunicaciones desde el MC.

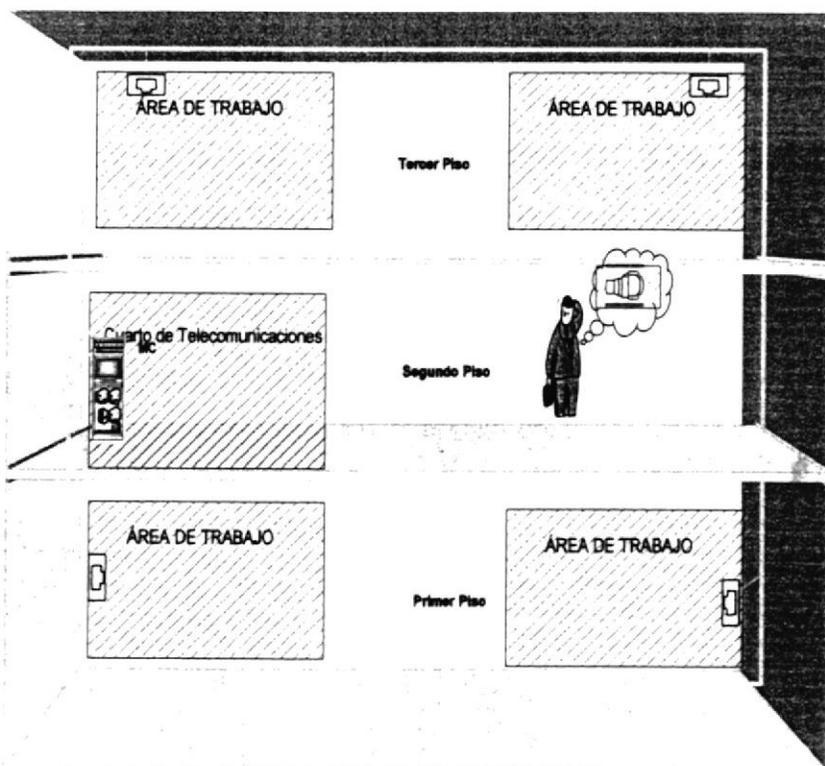


Figura 5. 26. Recomendación 7

## 5.19 NORMATIVA 19

La longitud del cableado de fibra óptica multimodo entre el HC y la salida de telecomunicaciones no excederá los 90 metros.

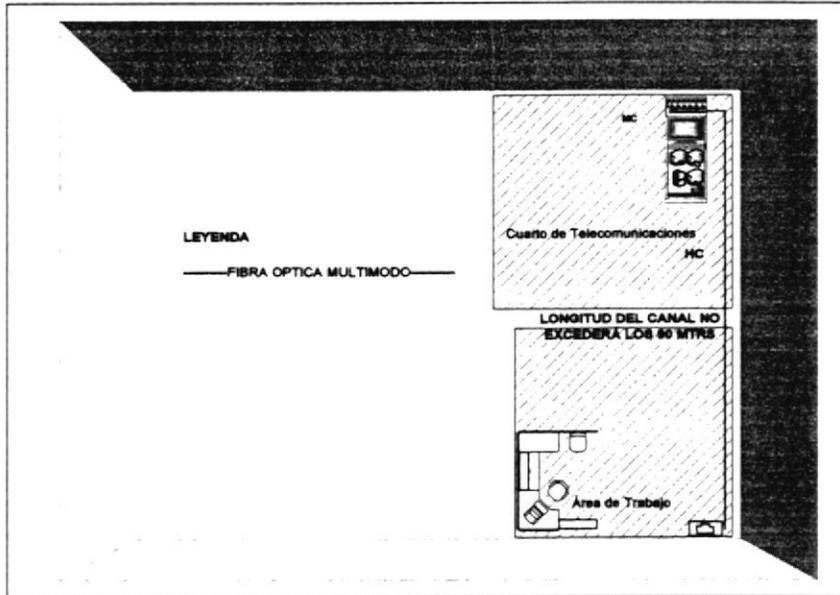


Figura 5. 27. Normativa 19

## 5.20 NORMATIVA 20

Las canalizaciones horizontales de cableado se diseñaran e instalaran para cumplir los reglamentos eléctricos, de construcciones locales y nacionales, y normas aplicables.

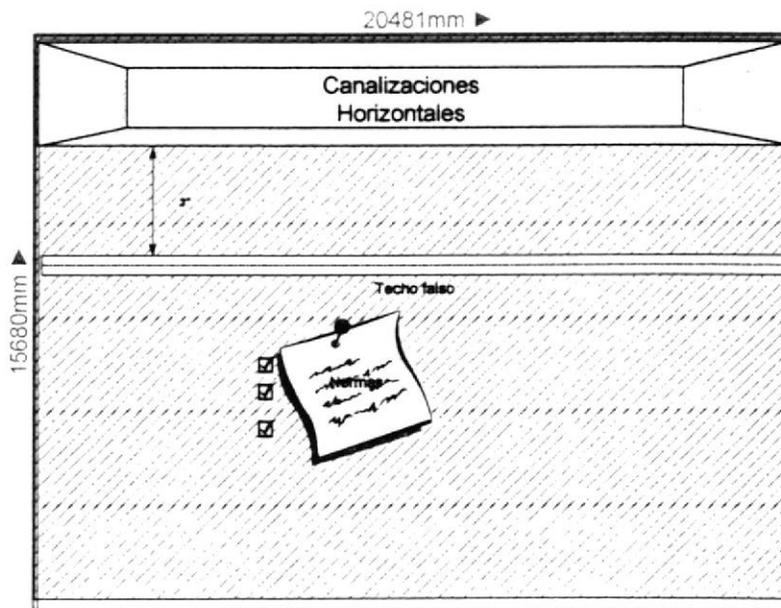


Figura 5. 28. Normativa 20

### 5.21 NORMATIVA 21

Las canalizaciones horizontales serán apropiadas para el ambiente en el cual se instalarán y no se obstaculizará por ductos de calefacción, ventilación y aire acondicionado, distribución de energía eléctrica o estructuras de edificios.

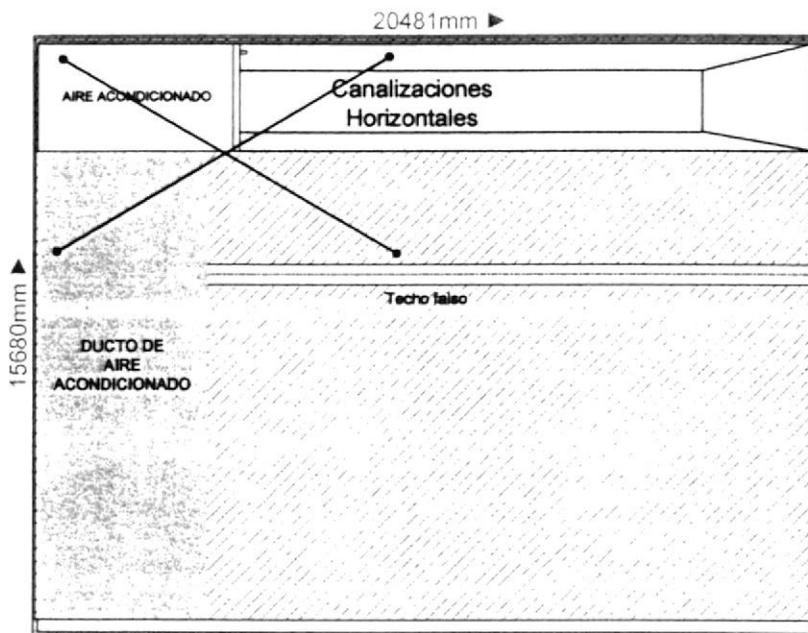


Figura 5. 29. Normativa 21

### 5.22 NORMATIVA 22

Las canalizaciones horizontales se instalaran o seleccionaran de manera que el radio mínimo de curvatura de los cables horizontales se mantengan dentro de las especificaciones del fabricante durante o después de la instalación.

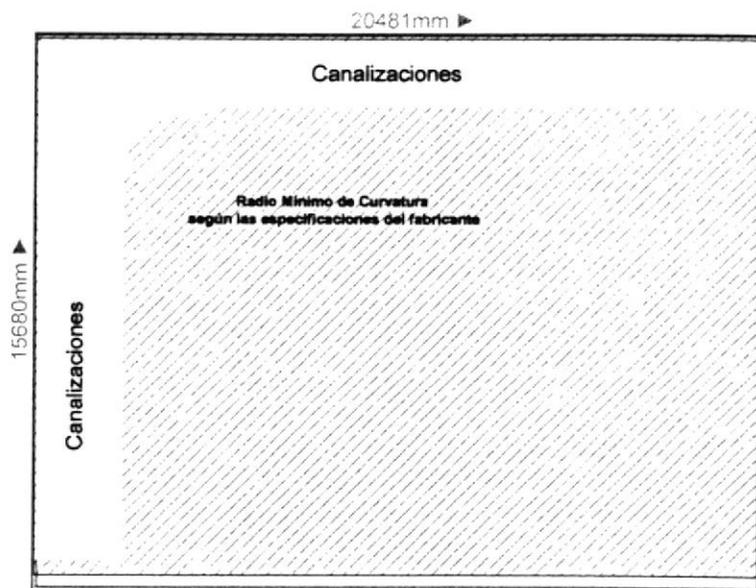


Figura 5. 30. Normativa 22

### 5.22.1 RECOMENDACIÓN 8

El radio de curvatura interior mínima de las canalizaciones horizontales no debe ser inferior a 10 veces el mayor diámetro de los cables a instalarse.

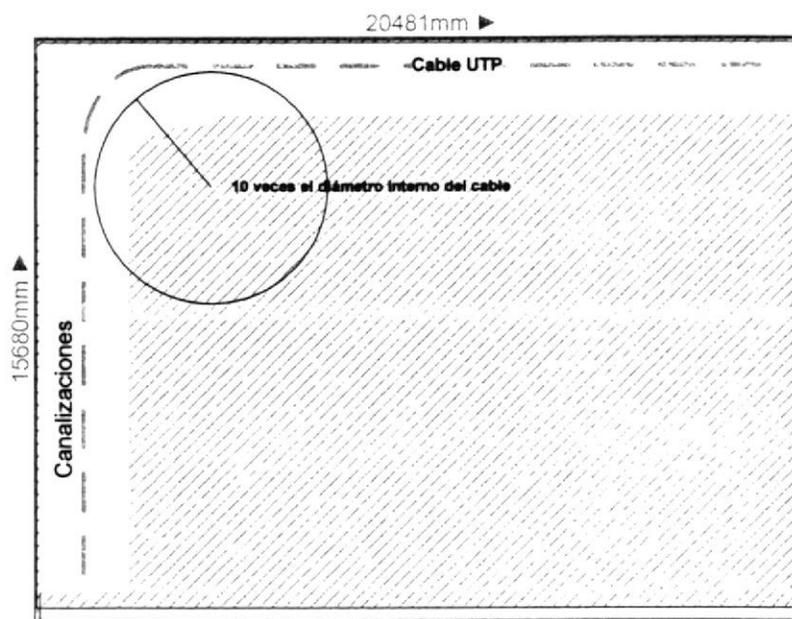


Figura 5. 31. Recomendación 8

### 5.23 NORMATIVA 23

Todas las canalizaciones instaladas serán accesibles con el fin de efectuar ediciones, cambios o retiros de cables. Las canalizaciones cerradas tendrán un punto de acceso espaciado como máximo cada 30 metros.

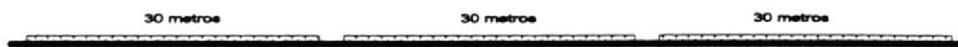


Figura 5. 32. Normativa 23

5.23.1 RECOMENDACIÓN 9

Ningún segmento del canal contendrá más de dos curvas de 90 grados entre punto de acceso.

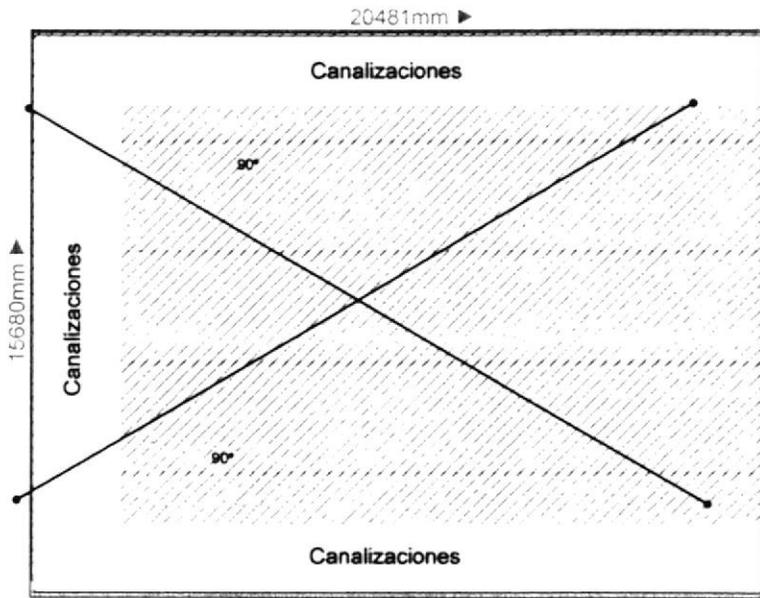


Figura 5. 33. Recomendación 9



5.24 NORMATIVA 24

El backbone usará la topología tipo estrella jerárquica con respecto al MC.

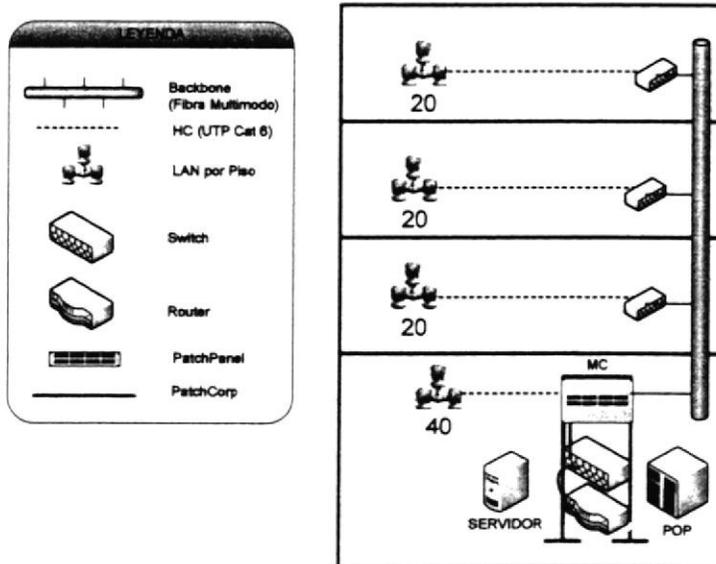


Figura 5. 34. Normativa 24

## 5.25 NORMATIVA 25

Para cada tendido de Backbone de edificio que sea mayor de 90 metros de longitud debe proveerse de un cable de fibra óptica.

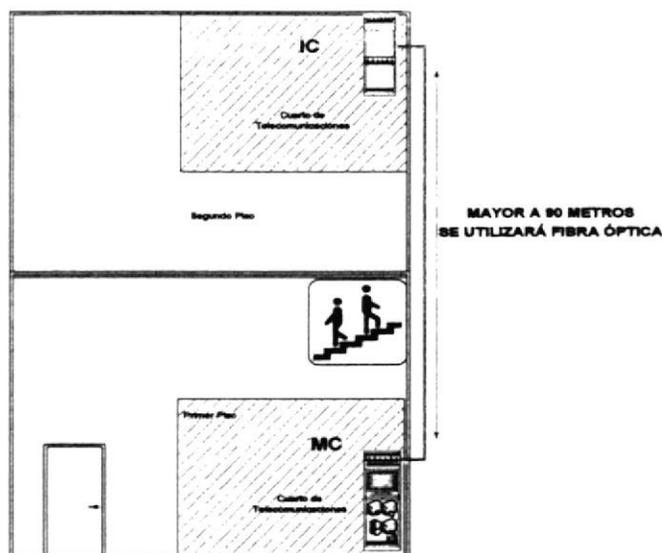


Figura 5. 35. Normativa 25

### 5.25.1 RECOMENDACIÓN 10

Se recomienda que se provean, como mínimo 2 hilos de fibra óptica para cada aplicación conocida, en atender por el sistema de Backbone de edificio durante su período de planificación. Debe proveerse un factor de crecimiento del 100%.

Aplicación	No. de hilos de fibra
Voz	2
Video	2
LAN	2
Crecimiento	6
Total	12

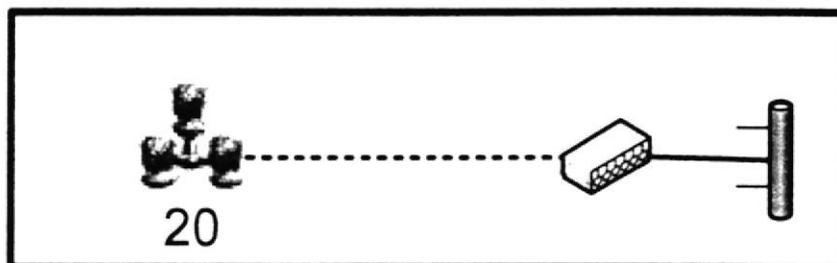


Figura 5. 36. Recomendación 10

### 5.26 NORMATIVA 26

La longitud total del canal de cable entre el MC y cualquier HC no excederá los siguientes límites.

- 3.000 Mt para fibra óptica monomodo.
- 2.000 Mt para fibra óptica multimodo.
- 2.000 Mt para par trenzado balanceado para aplicaciones PBX.

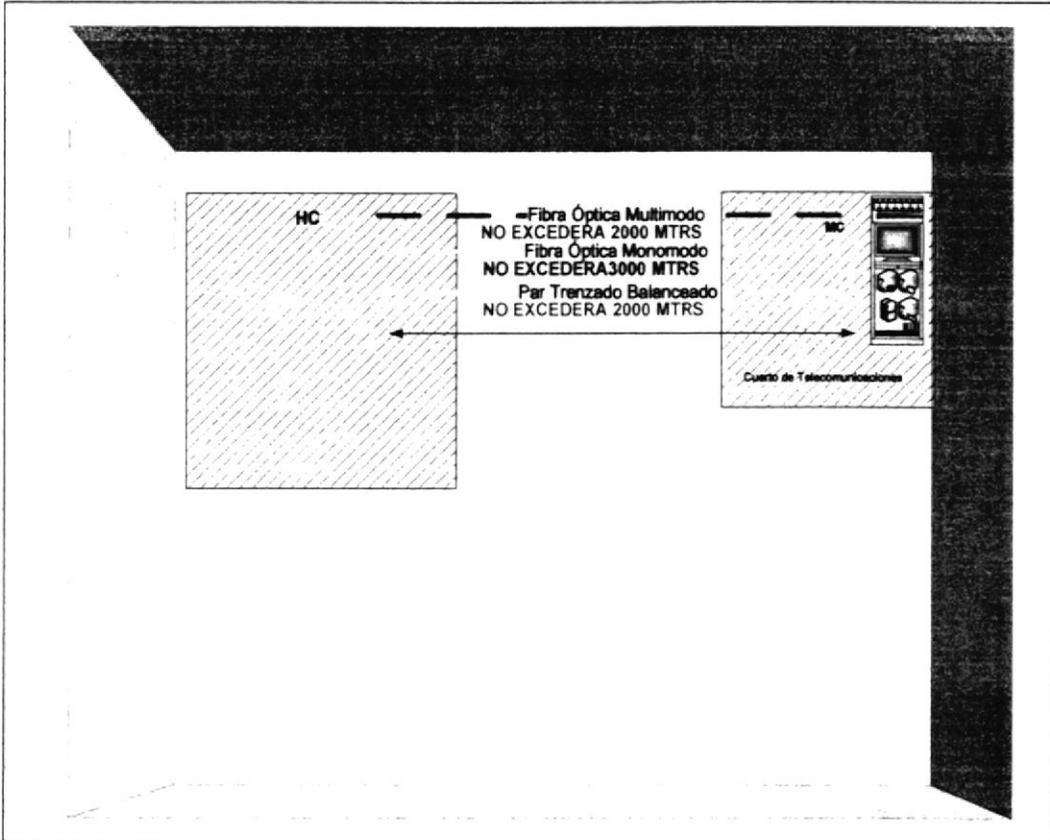


Figura 5. 37. Normativa 26



### 5.26.1 RECOMENDACIÓN 11

Para cables de Backbone se recomienda como mínimo de 3 metros de reserva de cable en cada extremo.

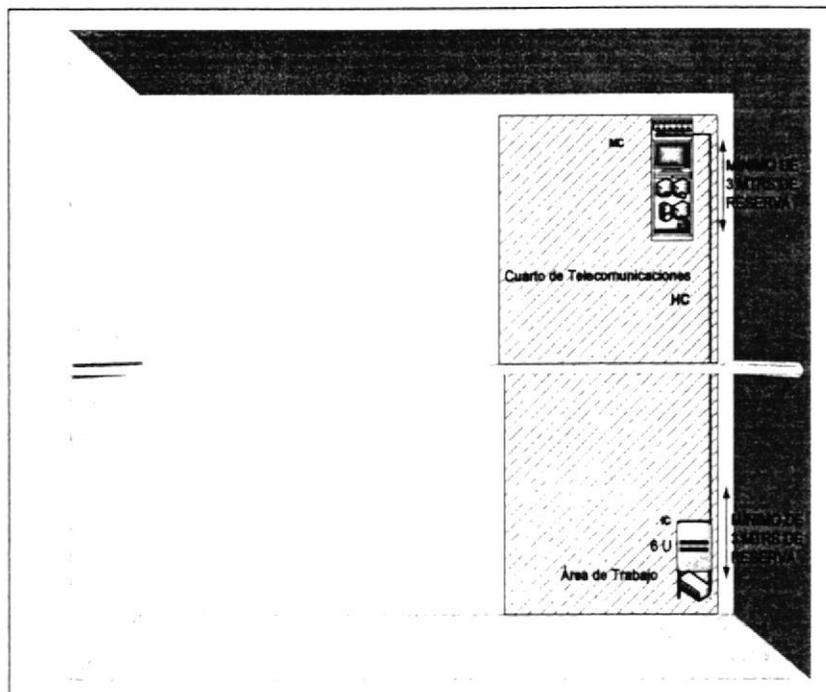


Figura 5. 38. Recomendación 11

### 5.27 NORMATIVA 27

Las canalizaciones de edificio proveerán acceso a todos los cuartos de telecomunicaciones, cuarto de equipos y acometida localizadas en el mismo edificio.

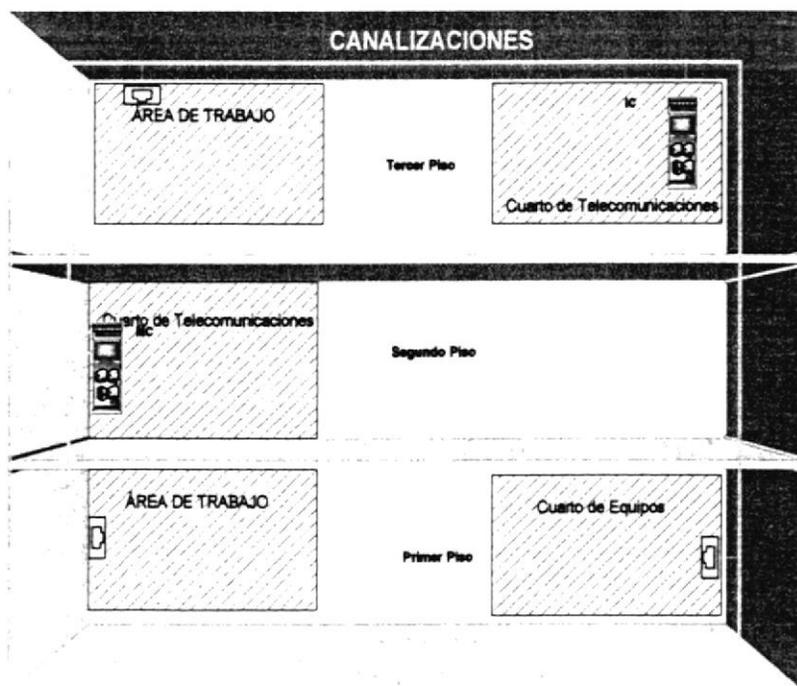


Figura 5. 39. Normativa 27

## 5.28 NORMATIVA 28

Las canalizaciones no se ubicarán en ductos de ascensores.

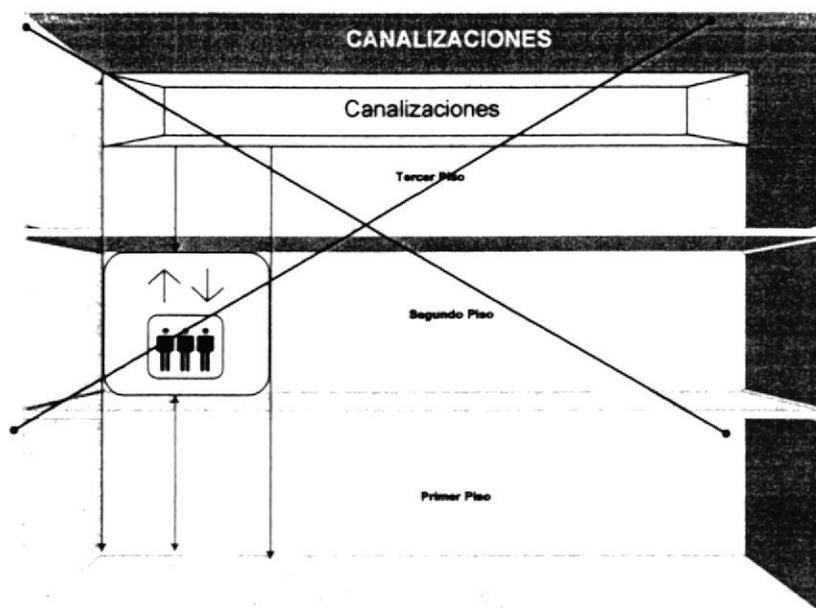


Figura 5. 40. Normativa 28

## 5.29 NORMATIVA 29

El cable que corre entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará expuesto en el área de trabajo u otros espacios con acceso público.

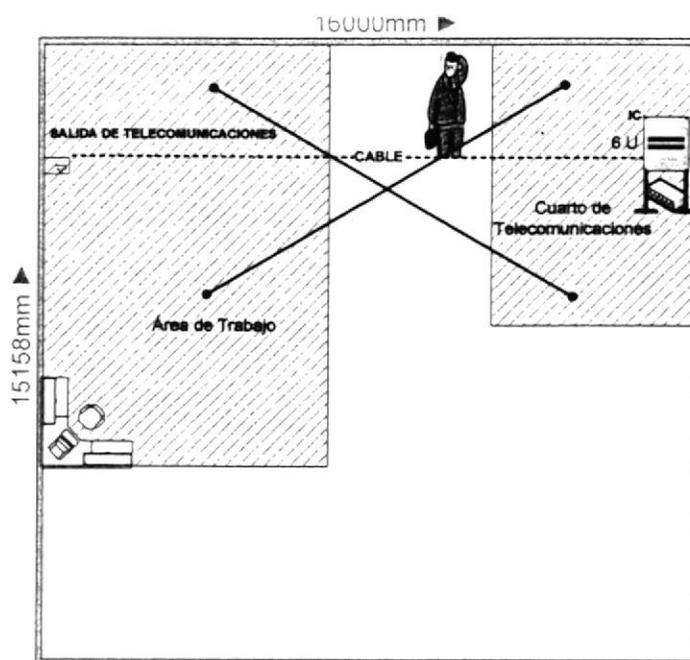


Figura 5. 41. Normativa 29



### 5.30 NORMATIVA 30

El cuarto de telecomunicaciones se diseñaran y equiparan para contener equipo de telecomunicaciones, terminaciones de cables y asociados.

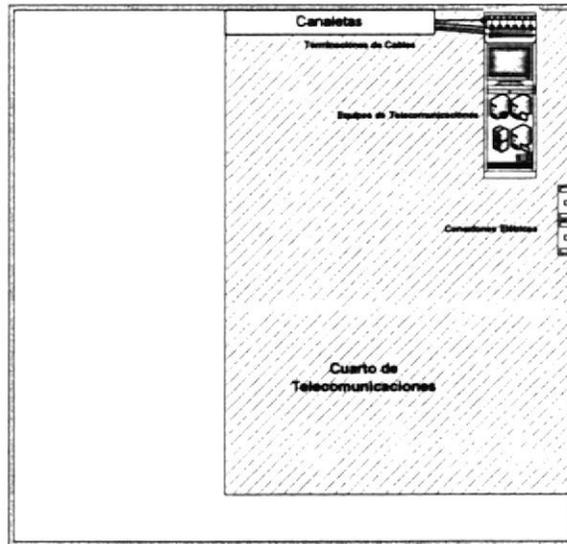


Figura 5. 42. Normativa 30

### 5.31 NORMATIVA 31

El cuarto de telecomunicaciones estará dedicado al cuarto de telecomunicaciones. El acceso a los cuartos de telecomunicaciones se restringirá al personal de servicio autorizado y no será compartido por servicios de edificio que puedan intervenir con los servicios de telecomunicaciones o se utilicen para servicio de mantenimiento del edificio.

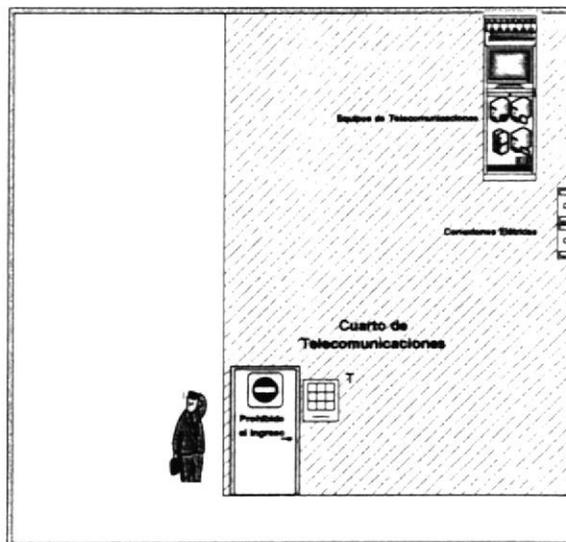


Figura 5. 43. Normativa 31

### 5.32 NORMATIVA 32

Las instalaciones de puesta y unida a tierra cumplirán con los reglamentos y normas aplicables.

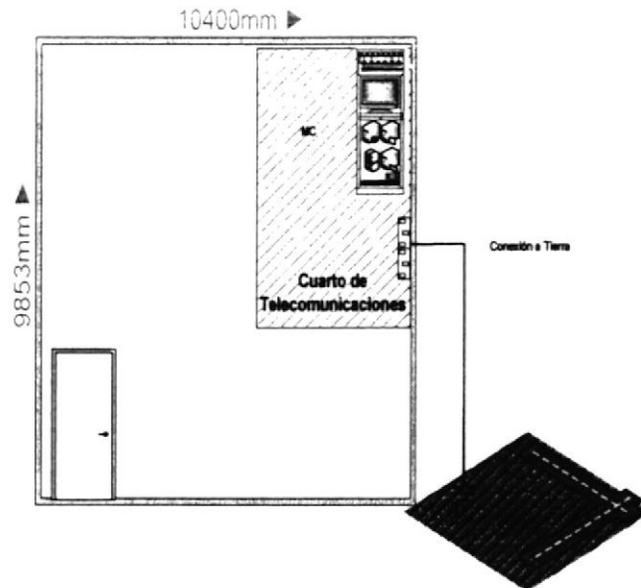


Figura 5. 44. Normativa 32

### 5.33 NORMATIVA 33

Las cajas o gabinetes usados como espacios alternativos cumplirá con los requisitos de separación, tendrán una puerta provista con cerradura y se mantendrá en una ubicación fija.

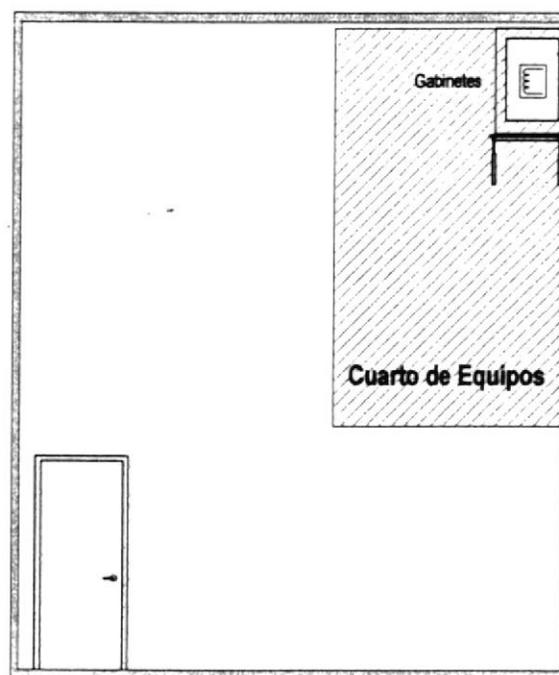


Figura 5. 45. Normativa 33

### 5.34 NORMATIVA 34

El cuarto de equipos no será compartido por servicios del edificio que pueda interferir con sistemas de telecomunicaciones o se utilicen para servicios de mantenimiento del edificio.

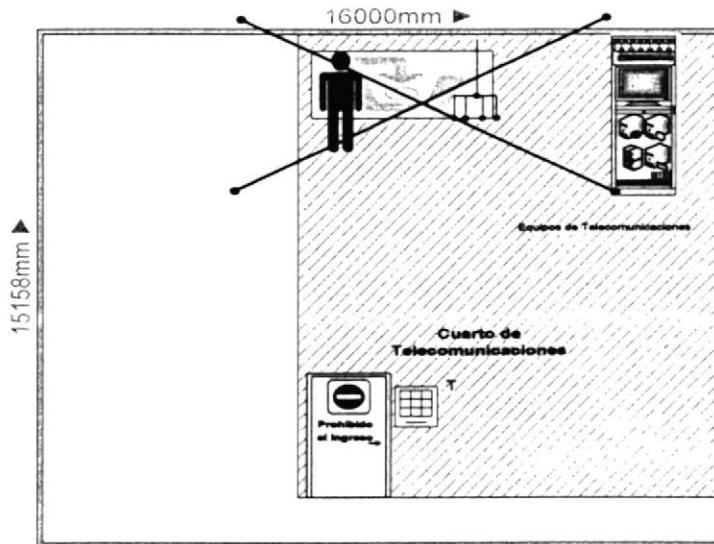


Figura 5. 46. Normativa 34

#### 5.34.1 RECOMENDACIÓN 12

Cuando sea factible, en un edificio de varios pisos, se recomienda que el cuarto de equipo se localice en el piso medio y en una ubicación que facilite el acceso a las canalizaciones de los cuartos de telecomunicaciones de los otros pisos.

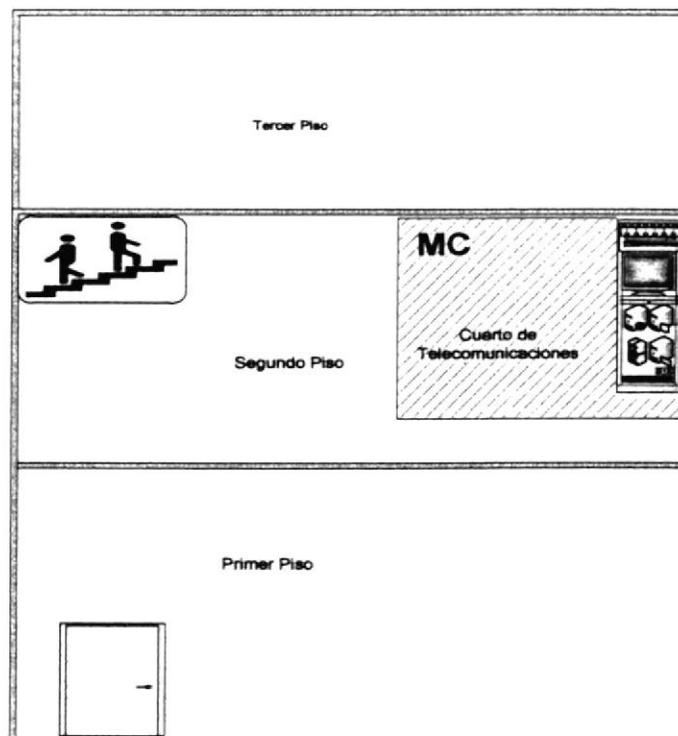


Figura 5. 47. Recomendación 12

### 5.34.2 RECOMENDACIÓN 13

Se recomienda que el cuarto de equipos se ubique por encima del nivel de inundación y esté protegido contra infiltraciones de tuberías de agua y drenaje.

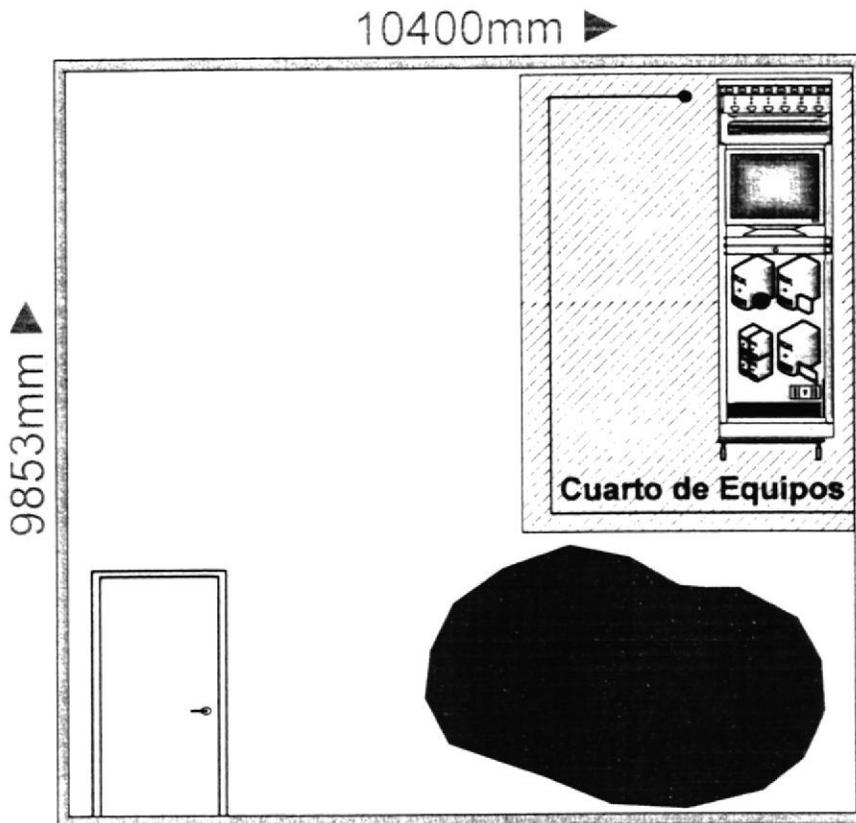


Figura 5. 48. Recomendación 13

### 5.35 NORMATIVA 35

El cableado se instalará para facilitar el rotulado y la documentación, y para permitir el código del color, en forma consistente de acuerdo a los requisitos.

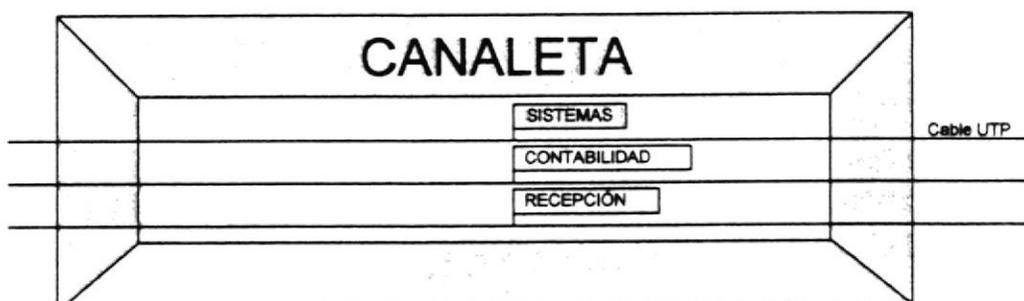


Figura 5. 49. Normativa 35

### 5.36 **NORMATIVA 36**

La instalación de gabinetes y de Rack deberá proporcionar las separaciones estipuladas en los reglamentos y normas aplicables.



Figura 5. 50. Normativa 36

### 5.37 **NORMATIVA 37**

Los cables de telecomunicaciones se soportaran con los dispositivos diseñados para este fin en forma independiente de cualquier infraestructura.

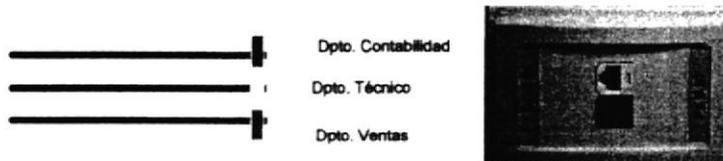


Figura 5. 51. Normativa 37

### 5.38 NORMATIVA 38

Los cables enrutados verticalmente como en el caso de los cables backbone u horizontales enrutados entre pisos, se soportarán con abrazaderas u otros mecanismos. Se requiere un mínimo de dos soportes por piso.

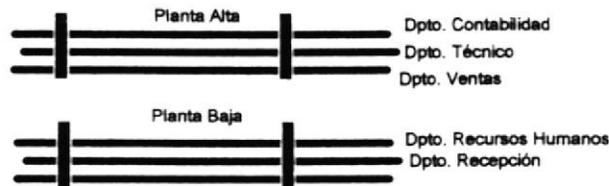


Figura 5. 52. Normativa 38

### 5.39 NORMATIVA 39

El número de cables horizontales (par trenzado balanceado o cable de fibra óptica) colocados en un soporte o canalización se limitará a una cantidad que no altere la forma geométrica de los cables.

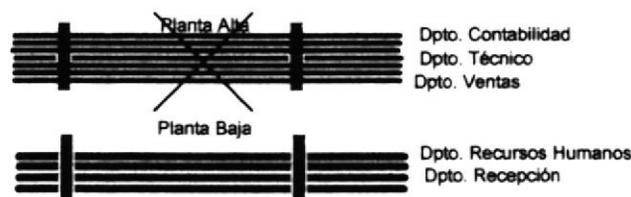


Figura 5. 53. Normativa 39

### 5.40 NORMATIVA 40

Las canalizaciones tipo bandeja o canal no excederán una capacidad máxima del 50% de llenado y una altura máxima interior de 6 pulgadas.

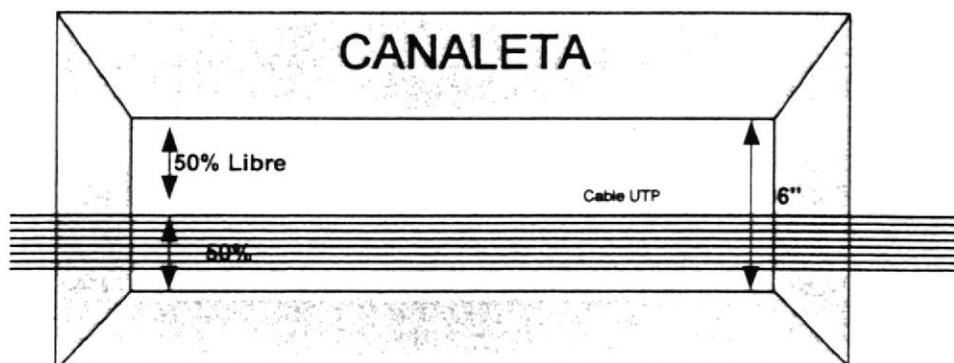
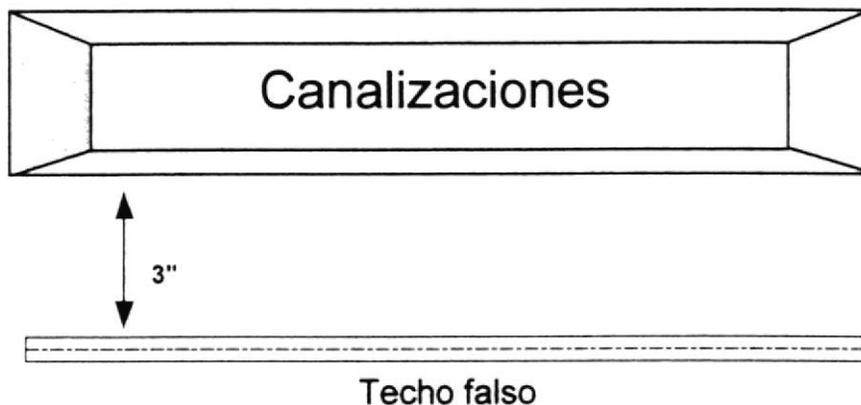


Figura 5. 54. Normativa 40

### 5.41 NORMATIVA 41

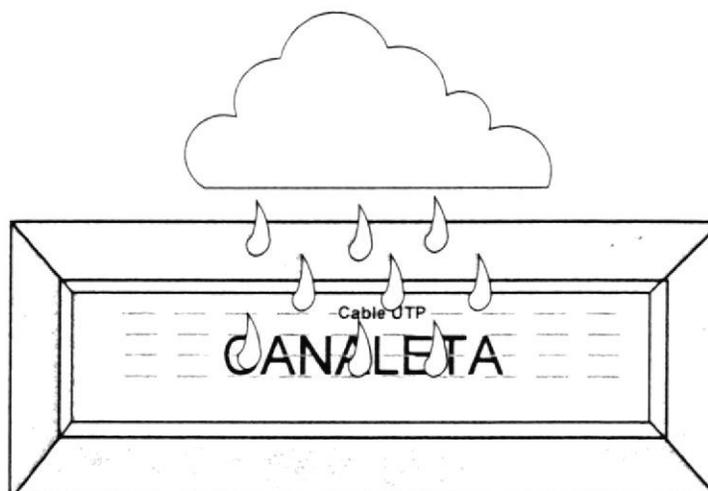
Para canalizaciones sin espacio de techo falso, los sistemas de soporte de cable se diseñaran e instalaran con un número de 3 pulgadas por encima de la rejilla del techo soportado.



**Figura 5. 55.** Normativa 41

### 5.42 NORMATIVA 42

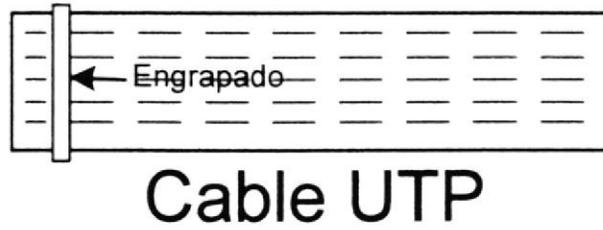
Los cables se instalarán en canalizaciones y espacio que brinden protección adecuada contra la intemperie y demás riesgos del entorno.



**Figura 5. 56.** Normativa 42

### 5.43 NORMATIVA 43

No se permitirá el engrapado de ningún cable reconocido.



**Figura 5. 57.** Normativa 43

### 5.44 NORMATIVA 44

El radio mínimo de curvatura en condiciones de no tensión (cuando el cable sólo es colocado, no jalado), será de:

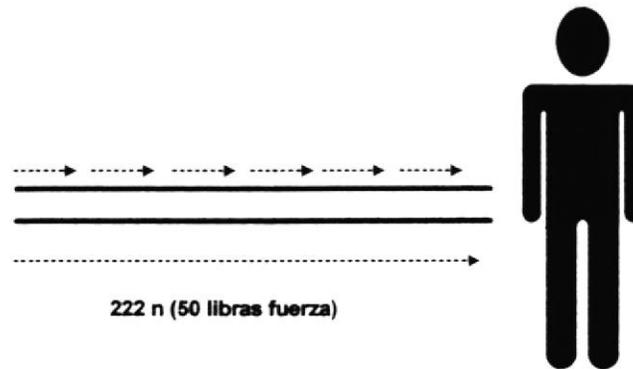
- 4 veces el cable diámetro externo del cable para UTP.
- 1 pulgada para SCTP o SFTP de diámetro menor igual a 6 milímetros.
- 2 pulgadas para SCTP o SFTP de diámetro mayor a 6 milímetros (0.25 pulgadas).



**Figura 5. 58.** Normativa 44

### 5.45 NORMATIVA 45

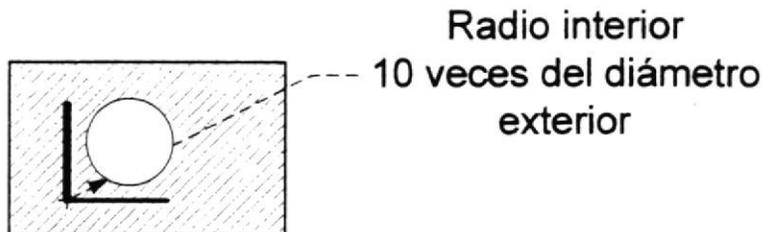
El radio mínimo de curvatura para cable horizontal de 2 y 4 fibras será de 25 milímetros (1 pulgada bajo condiciones de no tensión y de 50 milímetros bajo condiciones de no tensión), en donde la tensión máxima de jalado permitida será 222 newton (50 libras fuerza)



**Figura 5. 59.** Normativa 45

### 5.46 NORMATIVA 46

El radio de curvatura para cable de Backbone de fibra óptica de interiores no será menor a 10 veces del diámetro exterior del cable bajo condiciones de no tensión y no menor a 15 veces bajo condiciones de tensión.



**Figura 5. 60.** Normativa 46

### 5.47 NORMATIVA 47

El radio de curvatura para cable de backbone exterior de fibra óptica no será menor a 10 veces el diámetro exterior del cable bajo condiciones de tensión, en donde la tensión de jalado permitida usualmente es menor a 2.670 newton (600 libras fuerzas)

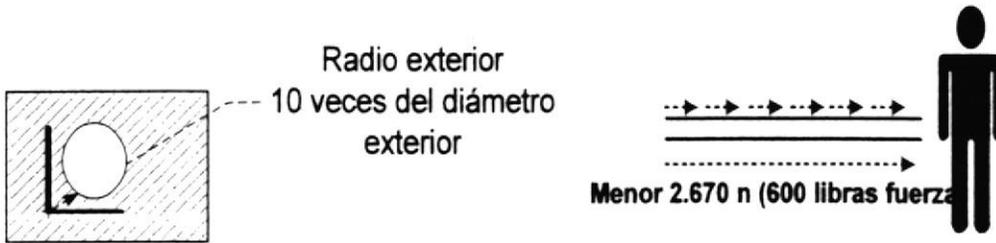


Figura 5. 61. Normativa 47

### 5.48 NORMATIVA 48

El cable que corre entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará expuesto en el área de trabajo ni en otros espacios con acceso público.

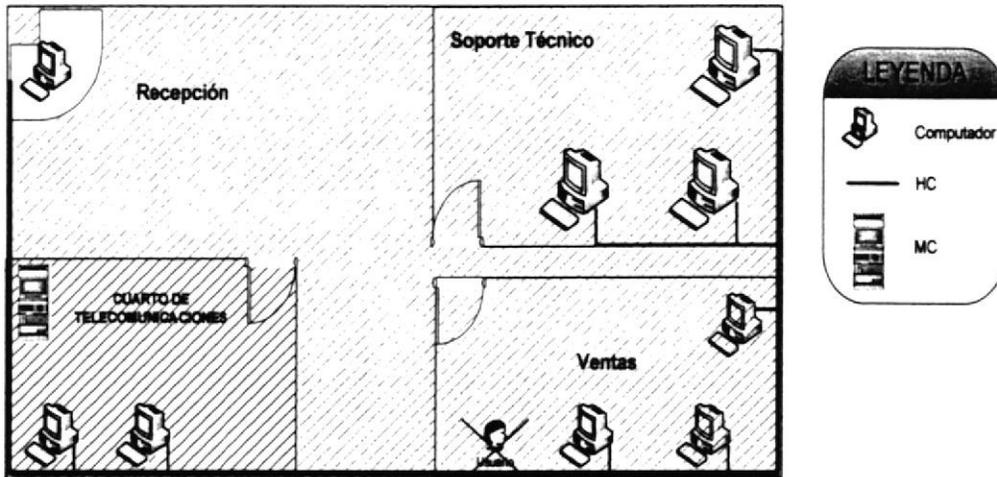


Figura 5. 62. Normativa48

## 5.49 NORMATIVA 49

El hardware de conexión se instalará de manera que se brinde un control de cable ordenado y bien organizado.



Figura 5. 63. Normativa 49

## 5.50 NORMATIVA 50

Con el fin de reducir el destrenzado de los pares de cable, el instalador debe pelar solo aquella cantidad de forro que se requerirá para terminar en el hardware de conexión para par trenzado balanceado.

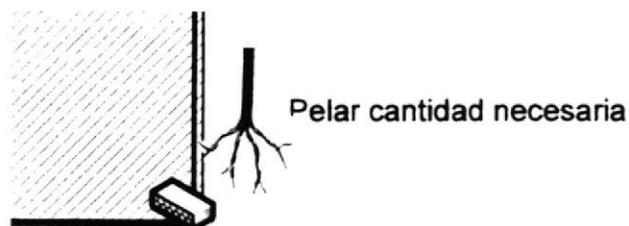


Figura 5. 64. Normativa 50

### 5.51 NORMATIVA 51

La cantidad máxima de destrenzado de cada par resultante de la terminación en el hardware de comunicación será de 13 milímetros para cables de categoría 5e o mayor y de 75 milímetros para cables categoría 3.

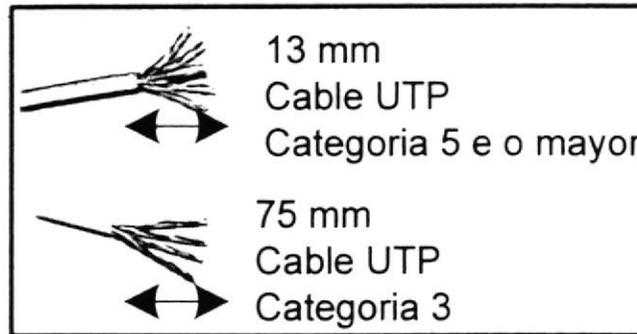


Figura 5. 65. Normativa 51

### 5.52 NORMATIVA 52

No se deberá terminar cables de diferentes categorías de desempeño en el mismo hardware de conexión.

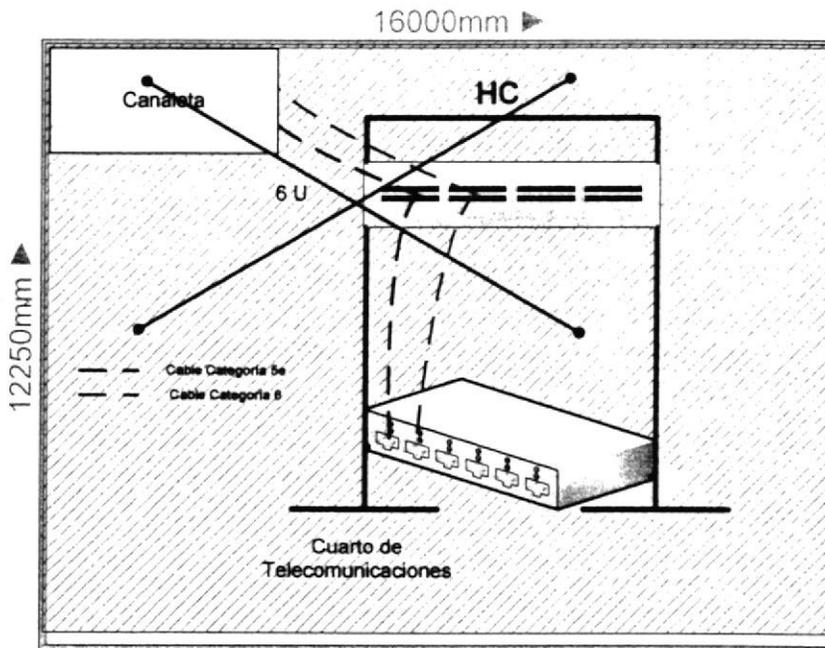


Figura 5. 66. Normativa 52

### 5.53 NORMATIVA 53

Los identificadores que se utilizan para acceder a grupos de registros del mismo tipo deben ser únicos.

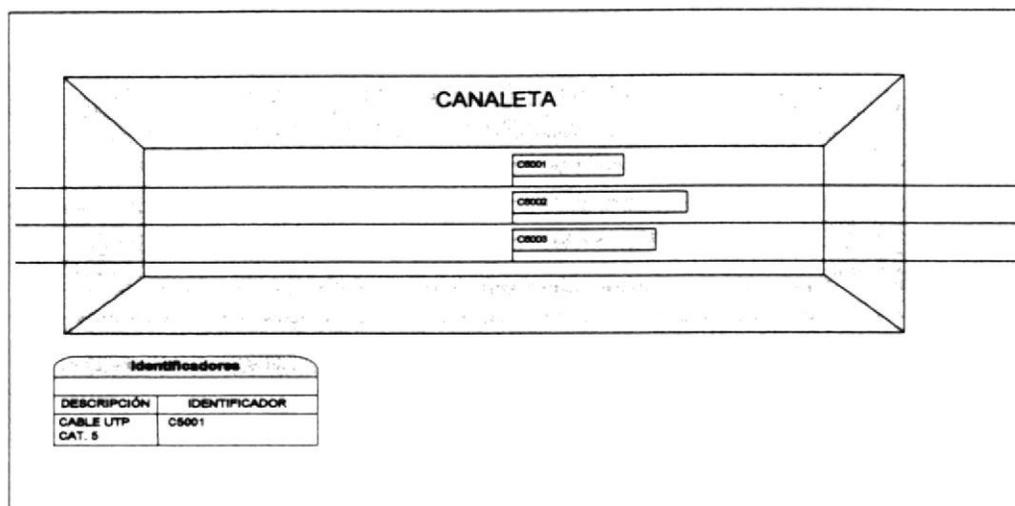


Figura 5. 67. Normativa 53

### 5.54 NORMATIVA 54

El rotulado debe realizarse ya sea pegado o colocando firmemente una etiqueta independiente al elemento que se va a administrar o marcando el elemento directamente.

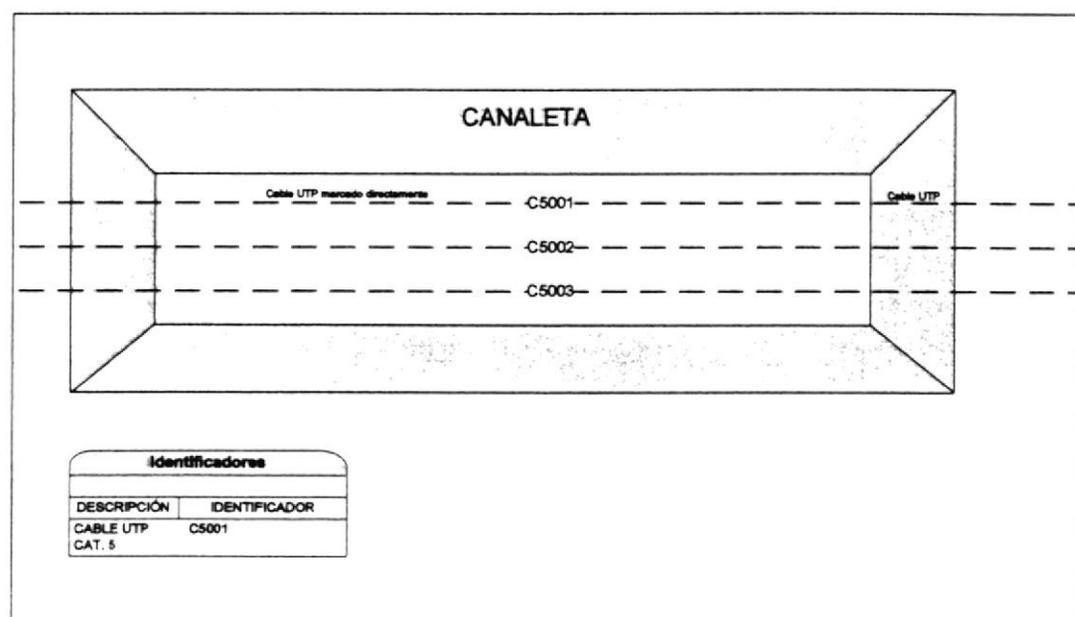


Figura 5. 68. Normativa 54

### 5.55 NORMATIVA 55

El rotulado deberá ser legible y permanecer firmemente unido al elemento durante todo el periodo de garantía.

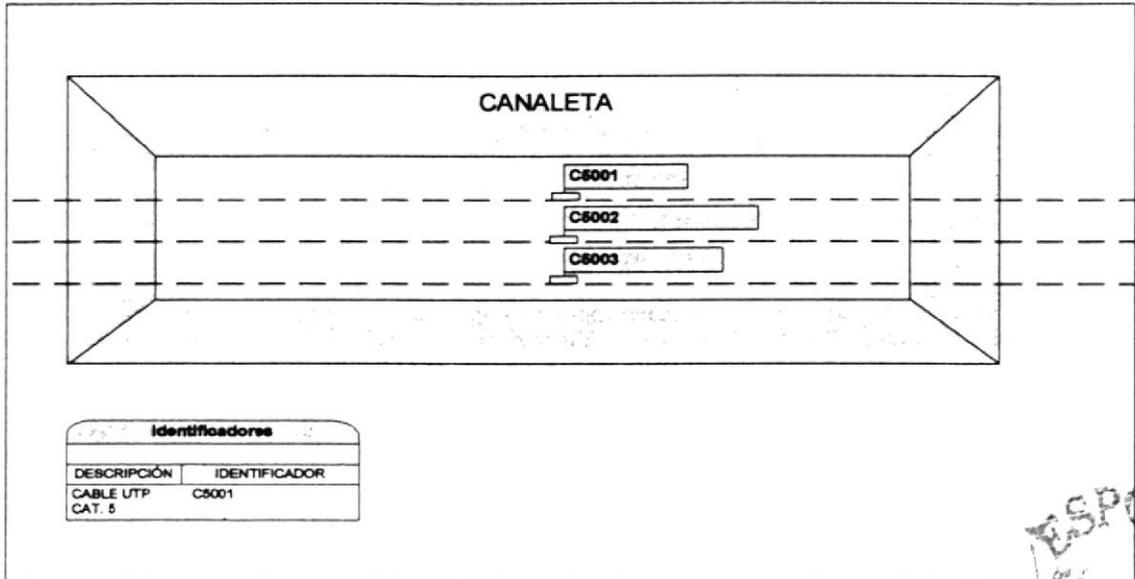


Figura 5. 69. Normativa 55

### 5.56 NORMATIVA 56

A cada cable se le asignará un identificador único que sirva de referencia en sus registros respectivos. Ej.:

Descripción	Identificador
Cable No. 9 de Fibra Óptica Multimodo	FOM009
Cable No. 5 UTP Categoría 5e	C5005

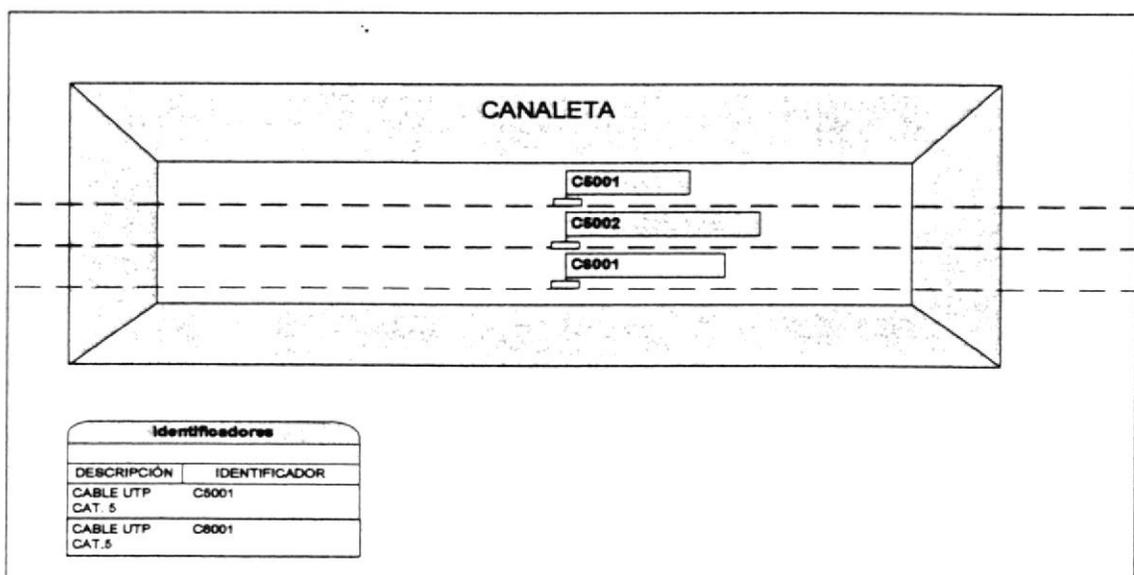


Figura 5. 70. Normativa 56

## 5.57 NORMATIVA 57

Los cables de los subsistemas horizontales y de backbone deberán rotularse en cada extremo. El cable o su etiqueta se marcará con su identificador y colocado dentro de los 30 cm del extremo del cable, esta marca deberá permanecer en el cable después de terminar la instalación.

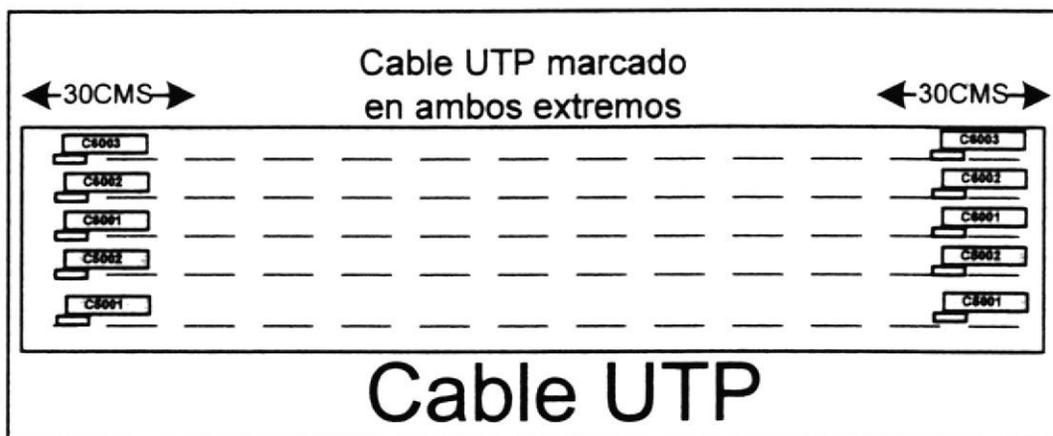
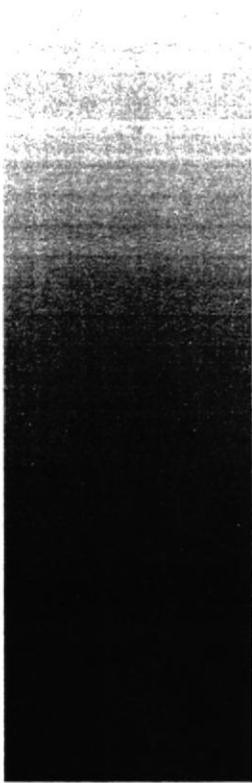


Figura 5. 71. Normativa 57



## CAPÍTULO 6

---



# LINUX

## 6. LINUX

### 6.1 INTRODUCCIÓN

*Linux es la denominación de un sistema operativo y el nombre de un núcleo. Es uno de los paradigmas del desarrollo de software libre (y de código abierto), donde el código fuente está disponible públicamente y cualquier persona, con los conocimientos informáticos adecuados, puede libremente estudiarlo, usarlo, modificarlo y redistribuirlo.*

*El término Linux estrictamente se refiere al núcleo Linux, pero es comúnmente utilizado para describir al sistema operativo tipo Unix (que implementa el estándar POSIX), que utiliza primordialmente filosofía y metodologías libres (también conocido como GNU/Linux) y que está formado mediante la combinación del núcleo Linux con las bibliotecas y herramientas del proyecto GNU y de muchos otros proyectos/grupos de software (libre o no libre). El núcleo no es parte oficial del proyecto GNU (el cual posee su propio núcleo en desarrollo, llamado Hurd), pero es distribuido bajo los términos de la licencia GPL (GNU General Public License).*

*La marca Linux (Número de serie: 1916230) pertenece a Linus Torvalds y se define como "un sistema operativo para computadoras que facilita su uso y operación".*

*Desde su lanzamiento, Linux ha incrementado su popularidad en el mercado de servidores. Su gran flexibilidad ha permitido que sea utilizado en un rango muy amplio de sistemas de cómputo y arquitecturas: computadoras personales, supercomputadoras, dispositivos portátiles, etc.*

*La expresión Linux también es utilizada para referirse a las distribuciones Linux, colecciones de software que suelen contener grandes cantidades de paquetes además del núcleo. El software que suelen incluir consta de una enorme variedad de aplicaciones, como: entornos gráficos, suites ofimáticas, servidores web, servidores de correo, servidores FTP, etcétera. Coloquialmente se aplica el término Linux a éstas, aunque en estricto rigor sea incorrecto, dado que la distribución es la forma más simple y popular para obtener un sistema Linux.*

*Los sistemas Linux funcionan sobre más de 20 plataformas diferentes de hardware; entre ellas las más comunes son las de los sistemas compatibles con PC's x86 y x86-64, computadoras Macintosh, Power PC, Sparc y MIPS.*

## 6.2 CARACTERÍSTICAS DE LINUX

<i>Multitarea</i>	<i>Es la capacidad de realizar varios procesos en forma simultánea.</i>
<i>Multiusuario</i>	<i>Tiene la capacidad de atender varios usuarios en forma simultánea manteniendo estrictamente su perfil en altos niveles de seguridad.</i>
<i>Multiplataforma</i>	<i>Por lo mismo que el Linux soporta gran cantidad de hardware se vuelve totalmente Portable, no es ningún problema el cambiar tu sistema a otro hardware totalmente distinto.</i>
<i>Estándar</i>	<i>Maneja protocolos e interfaces dentro de las normas estándar como POSIX, BSD, IEEE, ISO y System V.</i>
<i>Interacción</i>	<i>Capaz de operar con todos los sistemas de archivos estándar como FAT de DOS, VFAT de Win95/98, OS2/FS, ISO9660(CD-ROM), MINIX, UNIX , UFS de BSD y otros mas.</i>
<i>Red</i>	<i>Su protocolo madre es TCP/IP, soporta todo tipo de tarjetas de red. SLIP/PPP para acceso serial a TCP/IP, PLIP para conexiones en paralelo, NFS sistema de archivo de red, Telnet, SSH, NNTP, SMTP, IPX, AppleTalk, Samba para compartir archivos e impresoras con sistemas Windows, etc.</i>
<i>Arquitectura</i>	<i>Su arquitectura es de 32 bits reales en una PC y de 64 bits en un Alpha, su sistema utiliza las características del modo protegido del los micros 386 y superiores.</i>
<i>Librerías Dinámicas</i>	<i>Quiere decir que varias aplicaciones pueden utilizar las mismas librerías al mismo tiempo sin necesidad de cargarla varias veces en memoria.</i>
<i>Hardware</i>	<i>Soporta gran variedad de Multimedia, módems, impresoras, tarjetas de video, monitores, teclados, mouse, etc.</i>
<i>Entorno Gráfico</i>	<i>Soporta distintos entornos gráficos, los más populares son GNOME, KDE, FWVM, CDE, Enlightenment, Afterstep, Nextlevel, TWM, etc.</i>
<i>Licencia GPL</i>	<i>Se tiene el código fuente, puede ser modificado y mejorado, puede ser reproducido libremente sin necesidad del pago de una licencia, lo que lo hace de adquisición gratuita.</i>

### 6.3 EL KERNEL

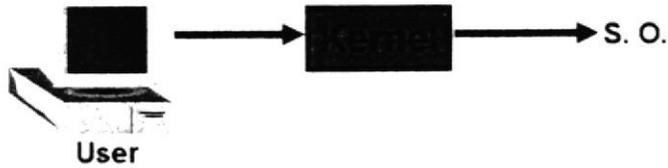


Figura 6. 1. Funcionamiento del Kernel

*El kernel (también conocido como núcleo) es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es la encargada de gestionar recursos, a través de servicios de llamada al sistema.*

*Como hay muchos programas y el acceso al hardware es limitado, el núcleo también se encarga de decidir qué programa podrá hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado. Acceder al hardware directamente puede ser realmente complejo, por lo que los núcleos suelen implementar una serie de abstracciones del hardware. Esto permite esconder la complejidad, y proporciona una interfaz limpia y uniforme al hardware subyacente, lo que facilita su uso para el programador.*

### 6.4 EL SHELL

*Un Shell es un pequeño programa diseñado para aceptar sus comandos y ejecutarlos, en pocas palabras es la interfaz entre el sistema operativo y el usuario.*

*El Shell predeterminado de Linux es bash, pero existen algunos intérpretes de comandos Unix: sh: bourne Shell (Unix), ash, csh: C Shell (Unix), bash: bourne again Shell (Linux), Tc Shell (Linux), mc.*

## 6.5 INSTALACIÓN DE LINUX FEDORA CORE 3

### 6.5.1 REQUERIMIENTOS DE HARDWARE

#### 6.5.1.1. REQUERIMIENTOS MÍNIMOS Y RECOMENDADOS DE INSTALACIÓN

A continuación se detallan los requerimientos mínimos esto implica que si el servidor implementa esas características puede tener ciertas limitaciones, mientras que si utiliza los requerimientos recomendados o superiores a estos se obtendrá un mejor rendimiento de todos los servicios de red que necesite la empresa.

MINIMO	RECOMENDADO
Pentium II	Pentium IV
192 en memoria RAM	256 o superior en memoria RAM
3 GB en espacio de disco duro	5 GB en espacio de disco duro
Una unidad de CD-ROM	Una unidad de CD-ROM
Tarjeta de red 10/100/1000 base T	Tarjeta de red 10/100/1000 base T

Figura 6. 2. Requerimientos mínimos y recomendados para instalación

### 6.5.2 CONFIGURACIÓN DEL BIOS

Para poder instalar correctamente Linux Fedora Core 3 será necesario seguir los pasos que a continuación se detallan:

1. Cuando la máquina esté encendiendo se accede al BIOS de la máquina digitando la tecla **Supr** (en algunas F2) de inmediato aparecerá una pantalla en la cual se realiza las configuraciones del BIOS de la tarjeta madre
2. Se va a la opción Boot Device aquí seleccionar la unidad a la cual hace referencia para que comience a bootear el sistema operativo en este caso será la unidad del Cd rom ya que desde aquí comenzara la instalación del sistema operativo.

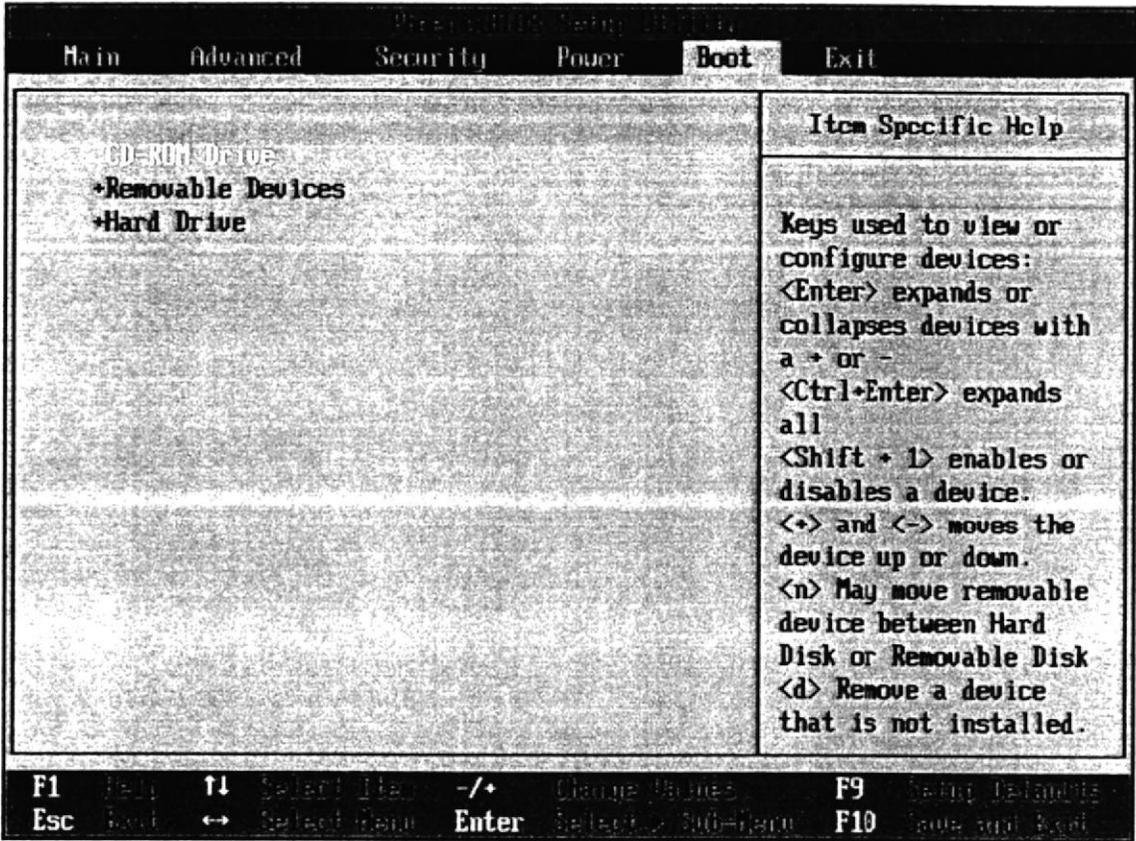


Figura 6. 3. Pantalla de acceso al BIOS

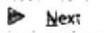
3. Luego que se ha seleccionado la unidad del Cd rom digite la tecla **Esc** y aparecerá un mensaje que le indicará si se desea guardar la configuración del BIOS aquí pedirá ingresar **Y** (salir y guardar) o **N** (salir sin guardar) debiendo presionar la tecla **Y**.
4. Después de salir de la pantalla del BIOS se reiniciará la máquina y de inmediato se ingresa el primer Cd de instalación.

### 6.5.3 INSTALACIÓN DEL SISTEMA OPERATIVO LINUX

1. Una vez arrancado el computador e insertado el CD, se presionará la tecla **Enter**.



Figura 6. 4. Pantalla inicial de instalación de Fedora Core 3

2. Después de presionar la tecla **enter** se mostrará una pantalla de bienvenida de Linux Fedora Core 3 aquí dará clic al botón **Next** 

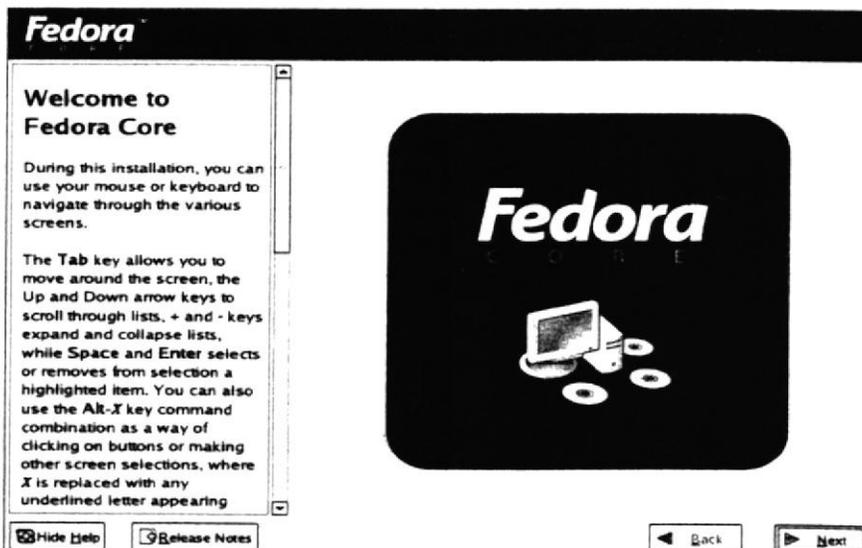


Figura 6. 5. Pantalla de bienvenida de la instalación de Fedora Core 3

3. En la siguiente pantalla seleccionará con el mouse el idioma a utilizar durante la instalación, en este caso **Spanish (español)** y dará clic al botón **Next** .

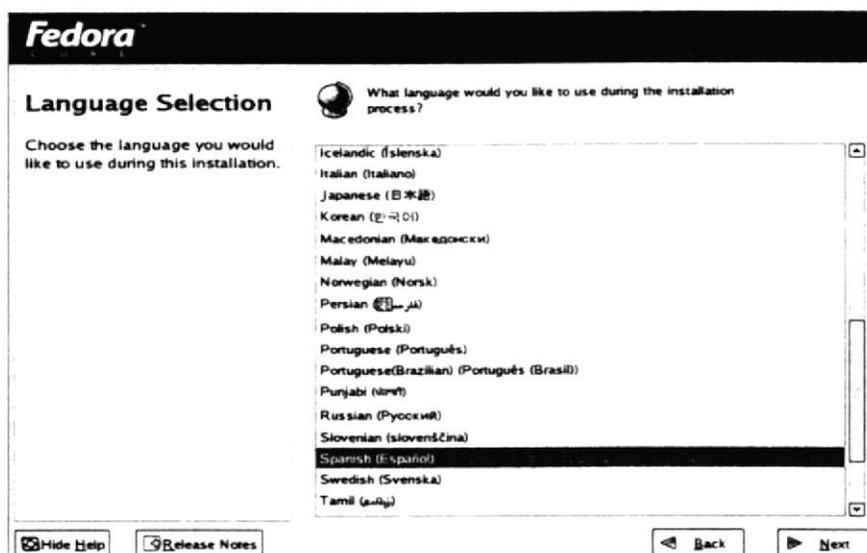


Figura 6. 6. Pantalla de selección de idioma

4. En la siguiente pantalla seleccionará con el mouse la configuración del teclado, en este caso **Spanish** y dará clic al botón **Next** .

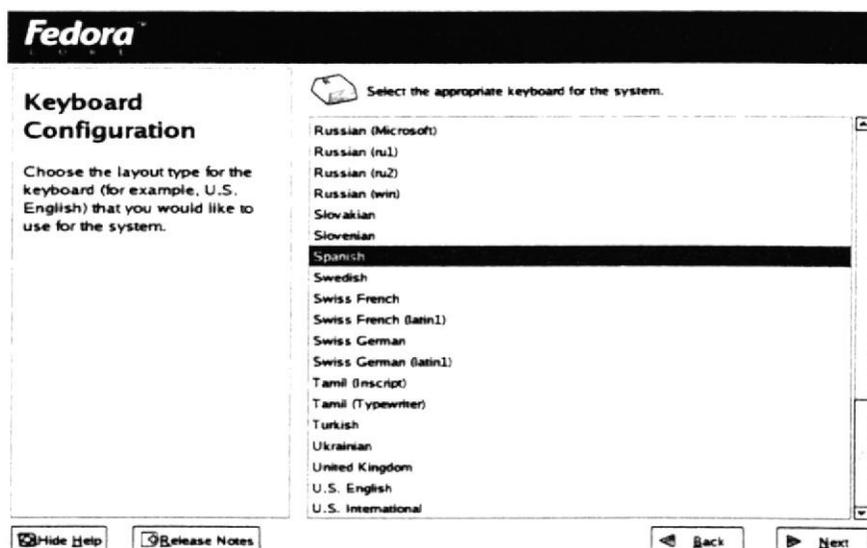


Figura 6. 7. Pantalla de configuración del teclado

5. Luego se elige el tipo de instalación que se va a utilizar, en este caso será la instalación **Personalizada (Custom)** para poder elegir los servicios que deseen instalar y dará clic en el botón **Next** .

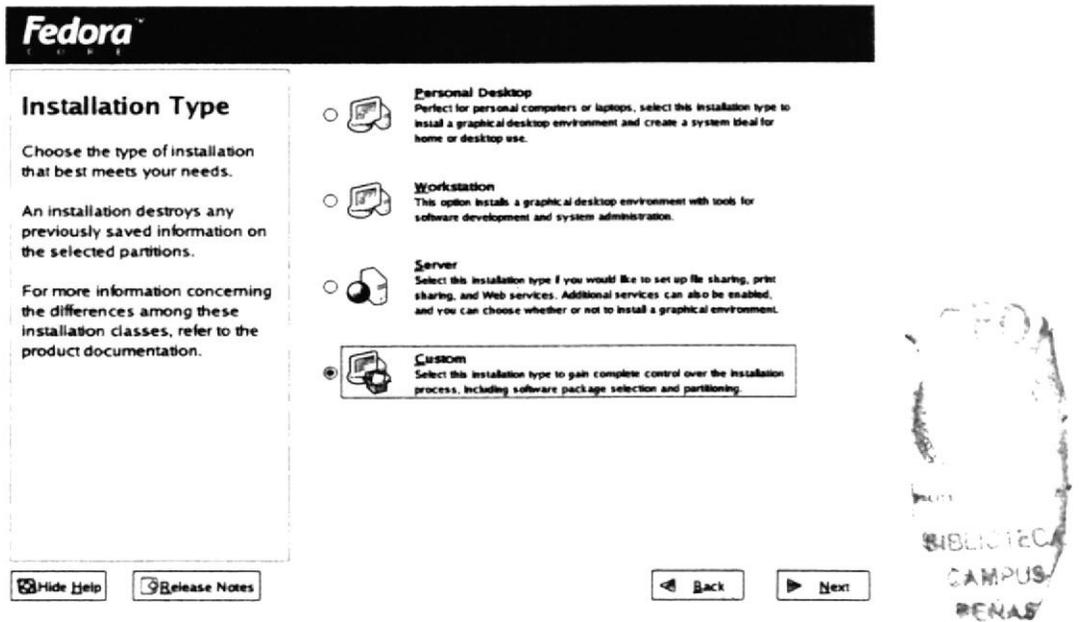


Figura 6. 8. Pantalla de tipo de instalación

A continuación se explica cada uno de los tipos de instalación:

- a. **Personal Desktop / Escritorio personal:** ideal para estaciones de trabajo o portátiles, seleccione este tipo de instalación para instalar un entorno de escritorio gráfico y crear un sistema ideal para el uso del directorio principal o del escritorio.
- b. **Workstation / Estación de trabajo:** Ésta opción instala un entorno de escritorio gráfico con herramientas para el desarrollo del software y la administración del sistema.
- c. **Server / Servidor:** Para configurar la compartición de ficheros y de la impresora, así como los de servicio Web. También se habilitan los servicios adicionales y puede escoger si desea o no instalar un entorno gráfico.
- d. **Custom / Personalizada:** Se obtiene un control completo sobre el proceso de instalación, incluyendo la selección de paquetes de software y las preferencias de particionamiento.

6. Seleccionar el tipo de partición que se va a usar y dará clic en el botón **Next** 

- *Particionamiento Automático.*
- *Partición con Disk Fruid.*

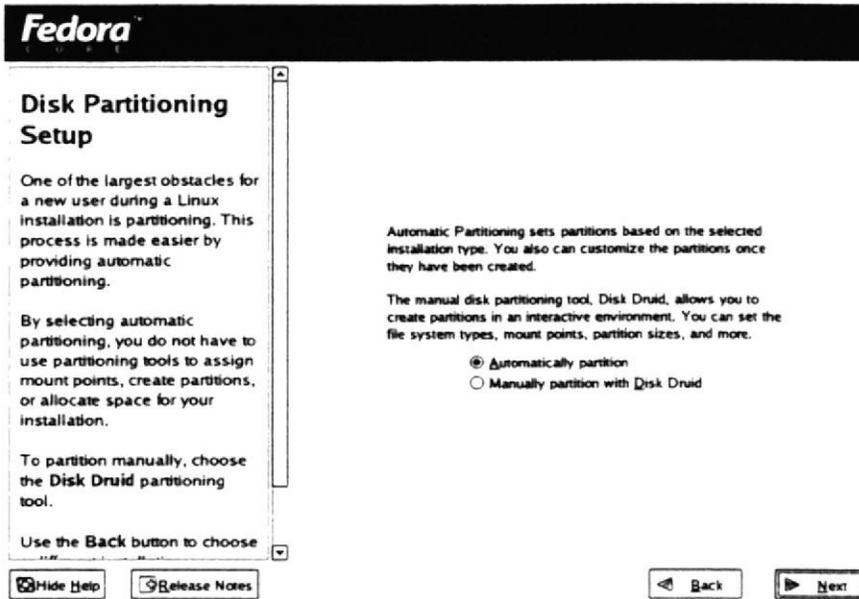


Figura 6. 9. Pantalla: Particionamiento de disco

## 6.1. Particionamiento Automático

6.1.1. Una vez seleccionado **particionamiento automático**, la siguiente ventana muestra las siguientes 3 opciones:

- *Eliminar todas las particiones Linux de este sistema.*
- *Eliminar todas las particiones de este sistema.*
- *Guarda todas las particiones y use el espacio libre.*

*Seleccionar eliminar todas las particiones de Linux de este sistema si es que existiese alguna instalación anterior de Linux en el servidor.*

*Seleccionar eliminar todas las particiones de este sistema si anteriormente existiese algún otro sistema operativo instalado en el servidor.*

*Seleccionar guardar todas las particiones y use el espacio libre si es que hubiese alguna partición en el disco duro la cual no se desee borrar y ocupar el espacio libre del disco.*

De acuerdo a lo que se haya seleccionado dará clic al botón **Next**  y de inmediato comenzará la instalación de Linux.

## 6.2. Particionamiento utilizando Disk Druid.

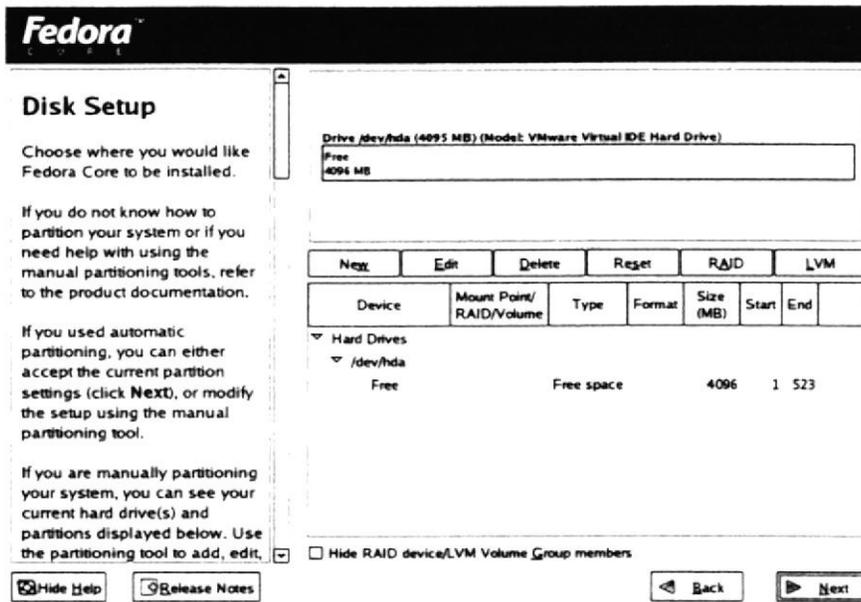


Figura 6. 10. Pantalla Particionamiento con Disk Druid

6.2.1. Una vez seleccionado particionamiento utilizando Disk Druid, crear tres particiones:

1. La partición *Boot*: Se creará el MBR el cual indica desde el gestor de arranque de booteo.
2. La partición *Swap*: Hace referencia a la memoria virtual que usará el servidor.
3. La partición *Root (/)*: Donde se alojarán los archivos del sistema operativo

6.2.2. Creará la partición *Boot* dando clic en el botón **New**  seguidamente muestra la siguiente pantalla.

En el combo llamado **Punto de montaje** seleccionar */boot*, luego en el siguiente combo seleccionar el **tipo de sistema de archivos** que será *ext3* y como paso siguiente deberá asignar el valor de 100 en el cuadro de texto **Tamaño (MB)** y dar clic en **Ok** .

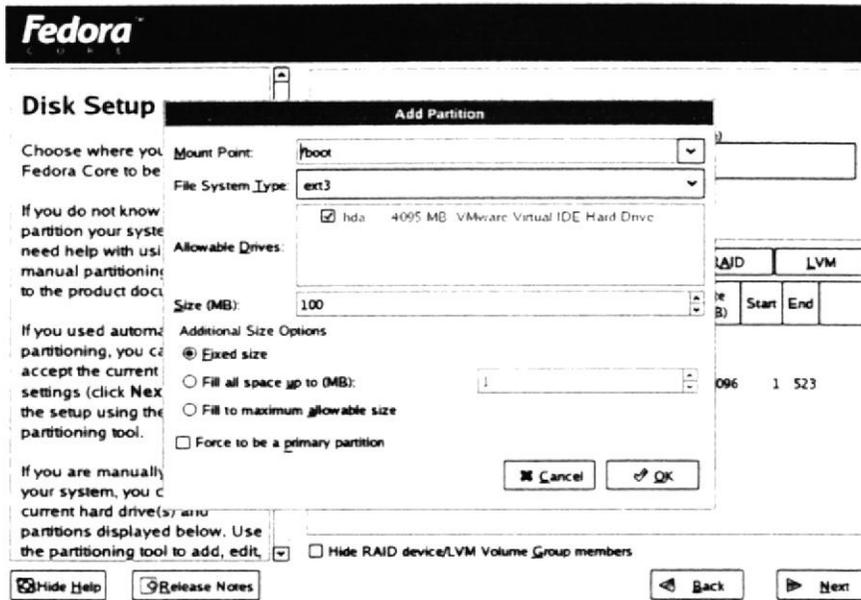


Figura 6. 11. Pantalla de partición boot

- 6.2.3. Seguido al paso anterior creará la partición Swap la cual se encuentra en el combo llamado **Punto de montaje** y en el cuadro de texto **Tamaño (MB)** asignar el doble de memoria RAM en este caso será 512 megabytes, ya que la memoria física del computador donde se instaló es de 256 megabytes y dará clic en **OK** .

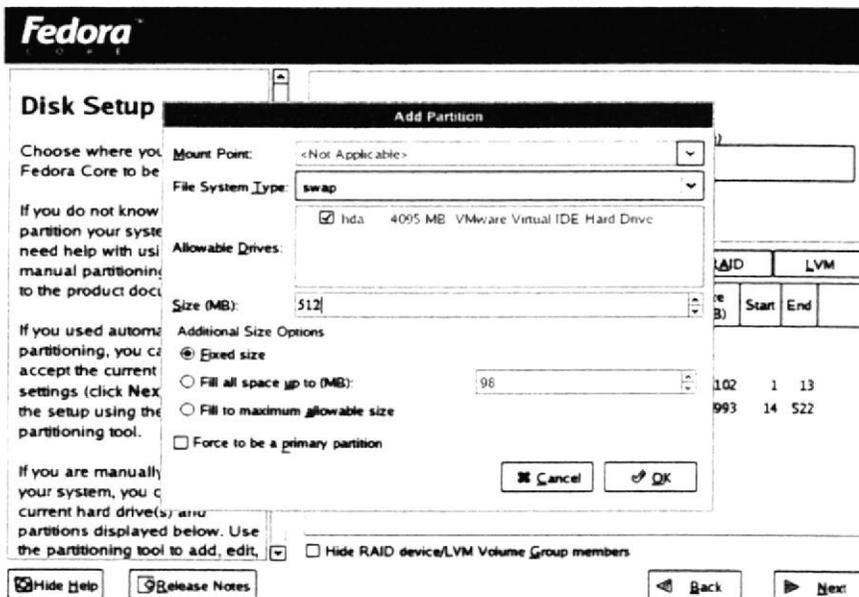


Figura 6. 12. Pantalla de partición swap

- 6.2.4. Cuando se haya terminado de crear las particiones anteriores se procede a crear la partición Root (/) la cual se encuentra en el combo llamado **Punto de montaje**, deberá seleccionar el símbolo de /, luego en el siguiente combo seleccionar **el tipo de sistema de archivos** que será **ext3** y como paso siguiente escoger **Completar espacio permitido**, mismo que será asignado en el disco duro para instalación en el cuadro de texto **Tamaño (MB)**. Y dar clic en **OK** .

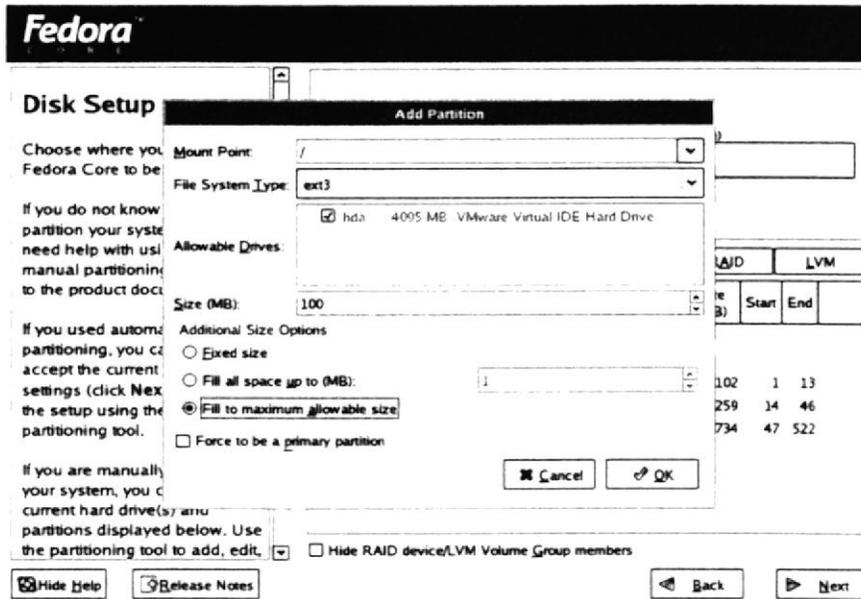


Figura 6. 13. Pantalla de partición root

- 6.2.5. Después de haber asignado los valores correspondientes en el orden anteriormente explicado (Boot, Swap y Root) dará clic en el botón **OK**  de la ventana **Añadir Particiones** y culminará la partición manual con **Disk Druid**.

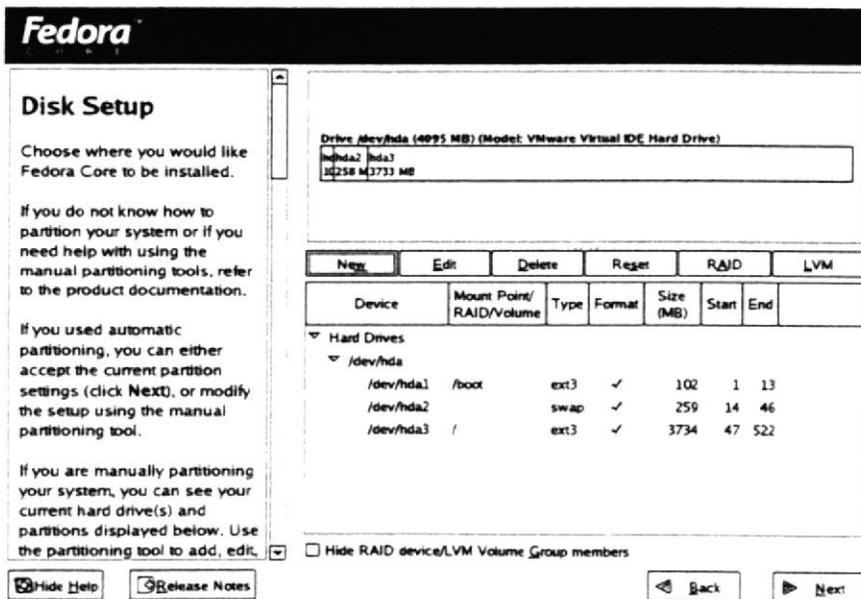


Figura 6. 14. Pantalla: Partición del disco

7. La siguiente pantalla es de configuración del gestor de arranque el cual por defecto es el **GRUP** y dará clic en el botón **Next** .

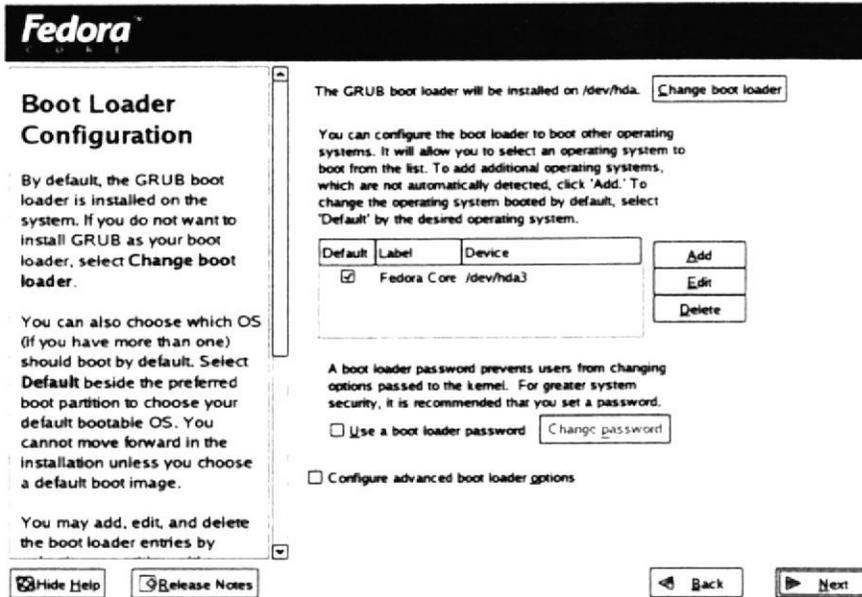


Figura 6. 15. Pantalla de partición boot

8. Para configurar los parámetros de red del sistema, haga clic sobre el botón [Edit](#) para la interfaz eth0.

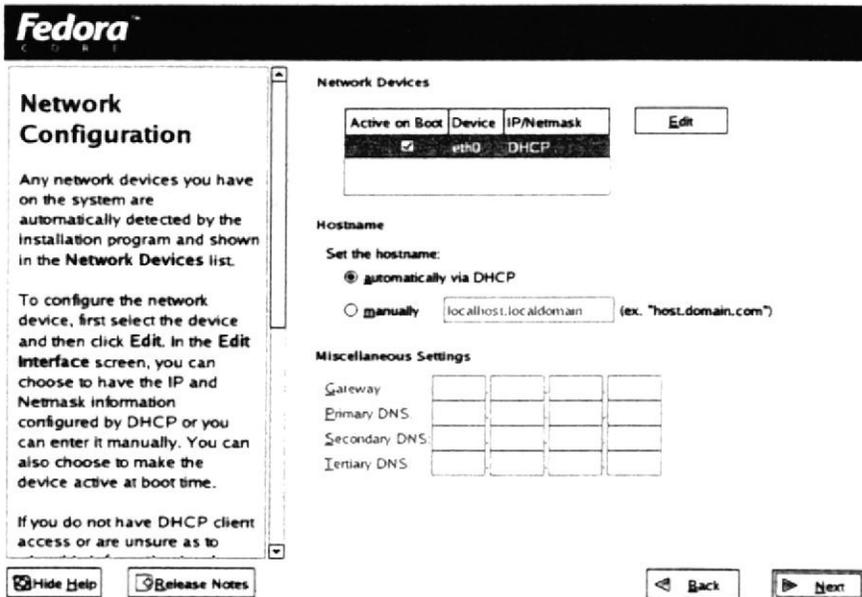


Figura 6. 16. Pantalla para configurar la tarjeta de red

9. En la siguiente ventana para modificar la interfaz `eth0`, desactive la casilla **Configure using DHCP** y especifique la IP address (dirección IP) y Netmask (máscara de subred) que utilizará en adelante el sistema. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, haga clic sobre el botón .

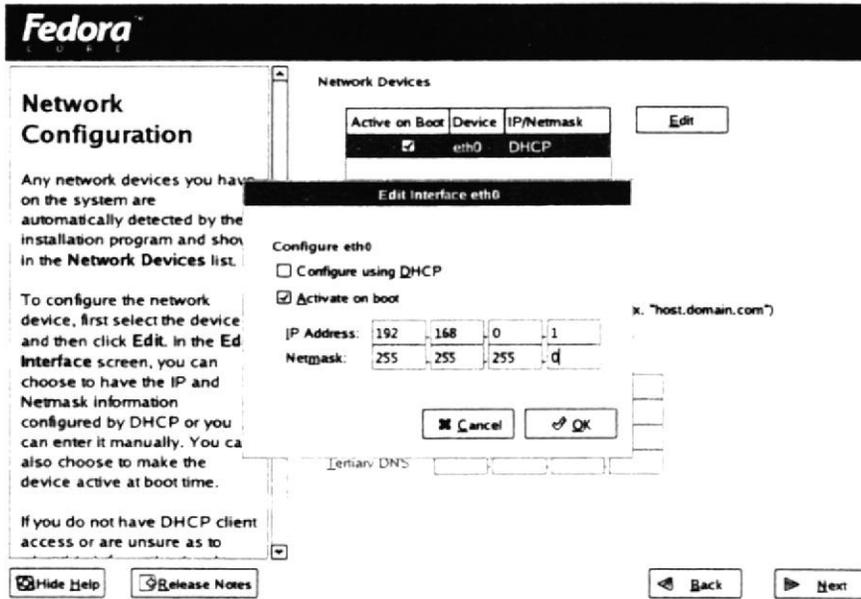


Figura 6. 17. Pantalla de configuración de red

10. En la pantalla de cortafuegos deberá dar clic en la opción **No firewall** (ningún cortafuego) y dará clic al botón **Next** .

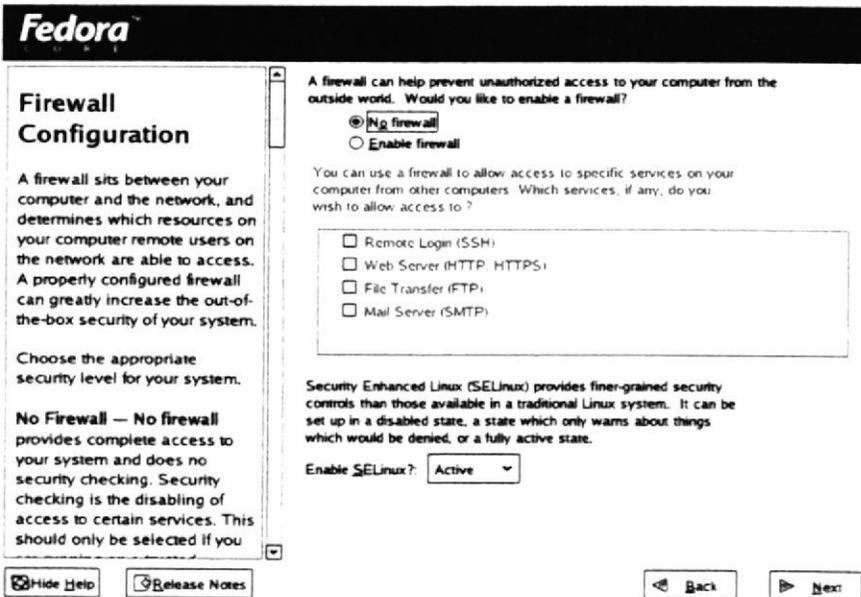
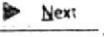


Figura 6. 18. Pantalla de firewall

11. Seleccionar el idioma por defecto para el sistema en este caso será (English – USA) el idioma puede variar de acuerdo a la región y dará clic en el botón **Next** .

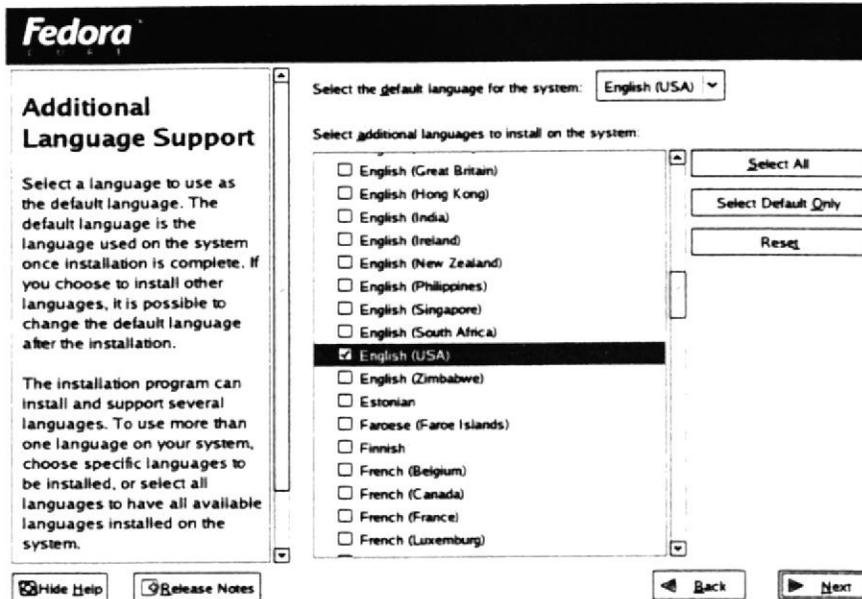
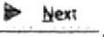


Figura 6. 19. Pantalla de selección de idioma

12. Seleccionar la ubicación y huso horario en este caso será (América/Guayaquil) a continuación dará clic en el botón **Next** .

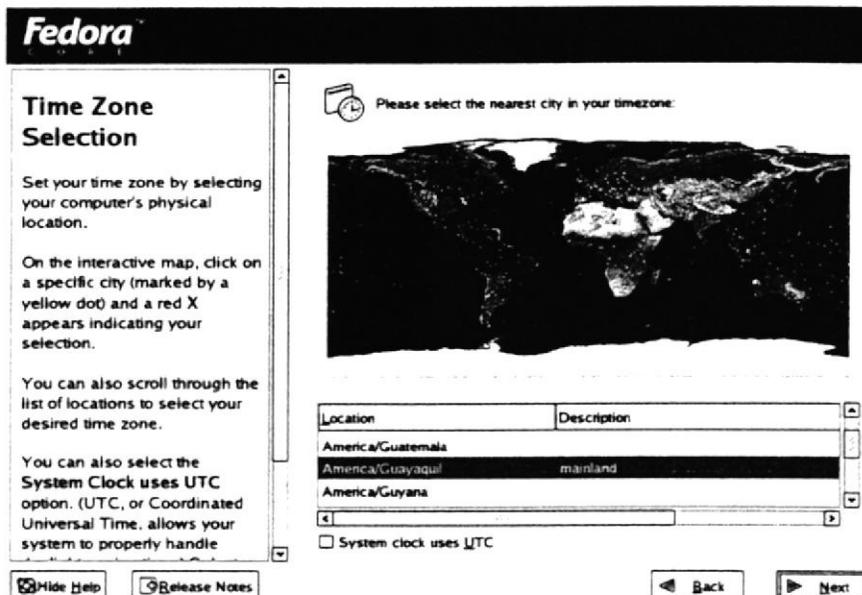


Figura 6. 20. Pantalla de selección de región

13. Asignar la clave del root la cual hace referencia al Administrador del Sistema y a paso siguiente pedirá confirmarla, después de haber digitado la contraseña dará clic en el botón **Next** .



Figura 6. 21. Pantalla de asignación de contraseña root

14. En esta opción se instalan los paquetes a utilizarse en el servidor, pero lo recomendado es seleccionar **Everything** para realizar una instalación completa de todos los paquetes y dar clic en **Next** .

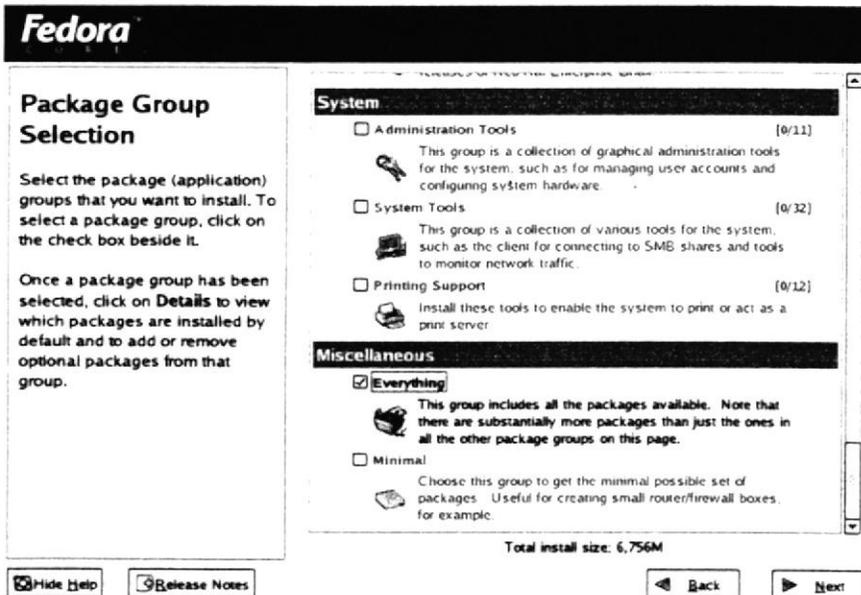


Figura 6. 22. Pantalla de elección de servicios a instalar

15. La siguiente pantalla que aparece es de Instalación de Linux Fedora Core 3 aquí dará clic al botón **Next**  pedirá uno por uno los discos de instalación, ésta pantalla durará un tiempo determinado de acuerdo a la cantidad de paquetes de servicio seleccionados.

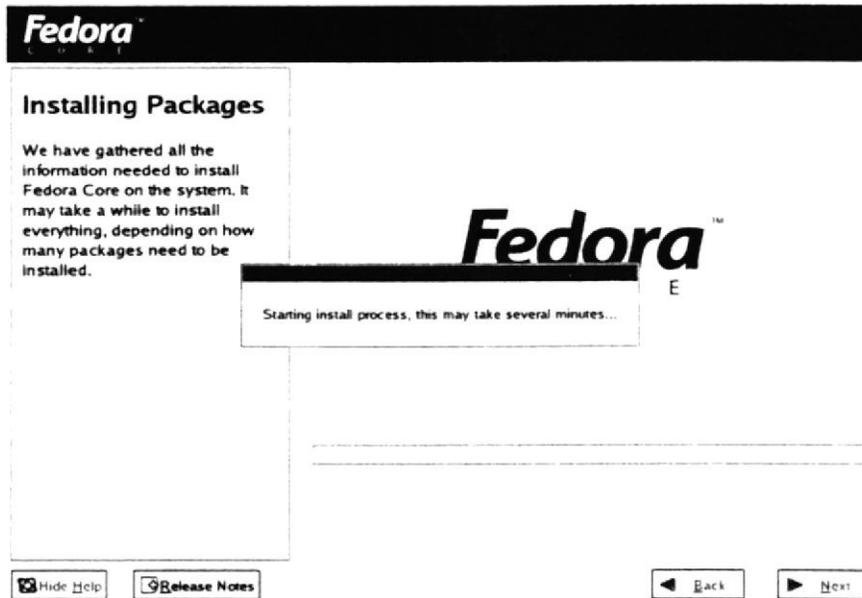


Figura 6. 23. Pantalla de inicio de instalación

16. Al finalizar la instalación de todos los paquetes aparecerá la siguiente pantalla la cual le pedirá dar clic en el botón **Reboot** .

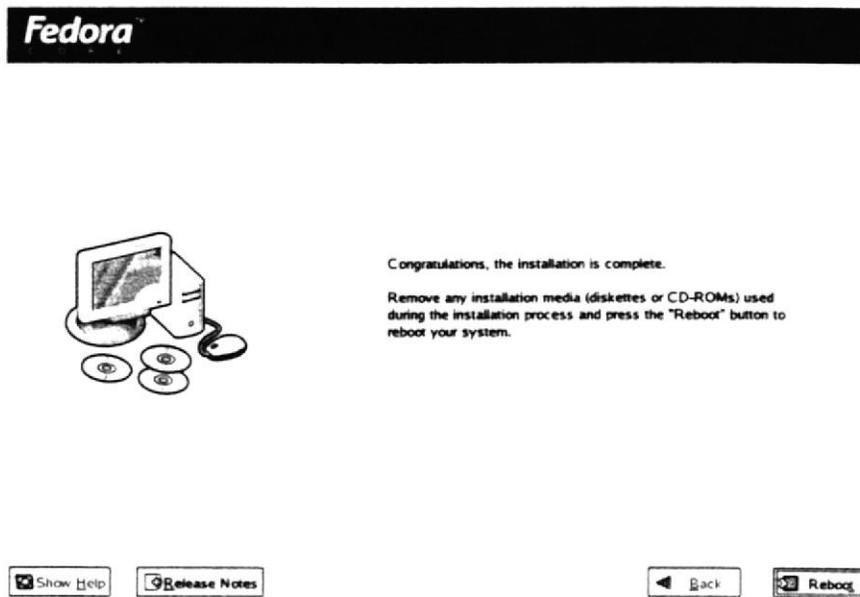


Figura 6. 24. Pantalla: Instalación completa

## 6.5.4 CONFIGURACIÓN POST-INSTALACIÓN

1. Una vez reiniciada la computadora, deberá aceptar el acuerdo de licenciamiento seleccionando la opción **"Si, acepto el acuerdo de licencia"** y dará clic en el botón **Next** .

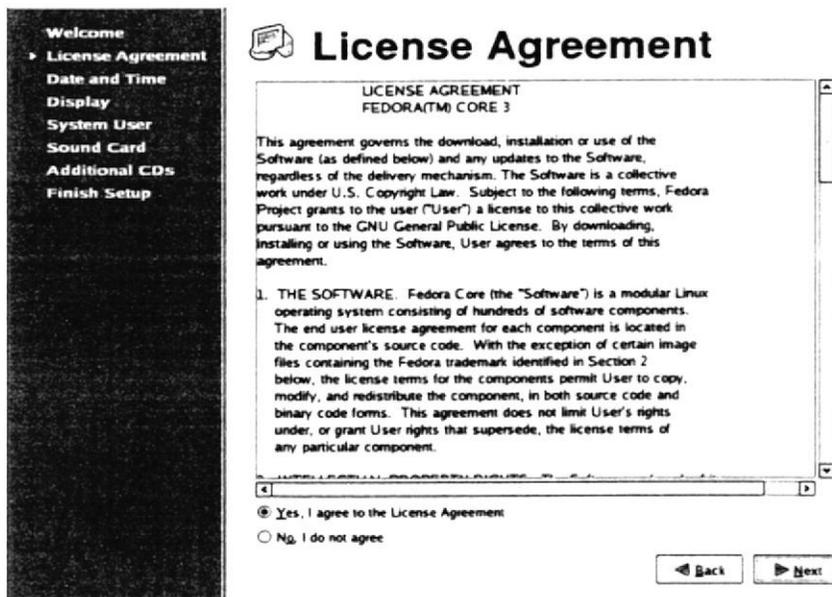


Figura 6. 25. Pantalla de acuerdo de licencia

2. Luego, si desea, pueden ser creados usuarios del sistema que no tendrán privilegios administrativos como el súper-usuario **root** y dará clic en el botón **Next** , si este paso se obvia se puede crear los usuarios en la consola modo texto.

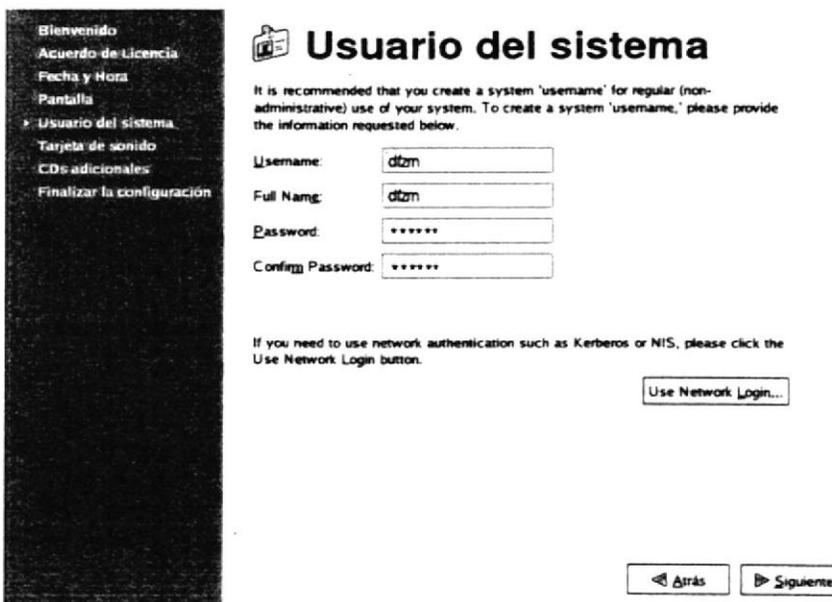


Figura 6. 26. Pantalla de creación de nuevos usuarios

3. Finalmente se da por terminada la instalación dando clic en el botón **Next**  **Next** .

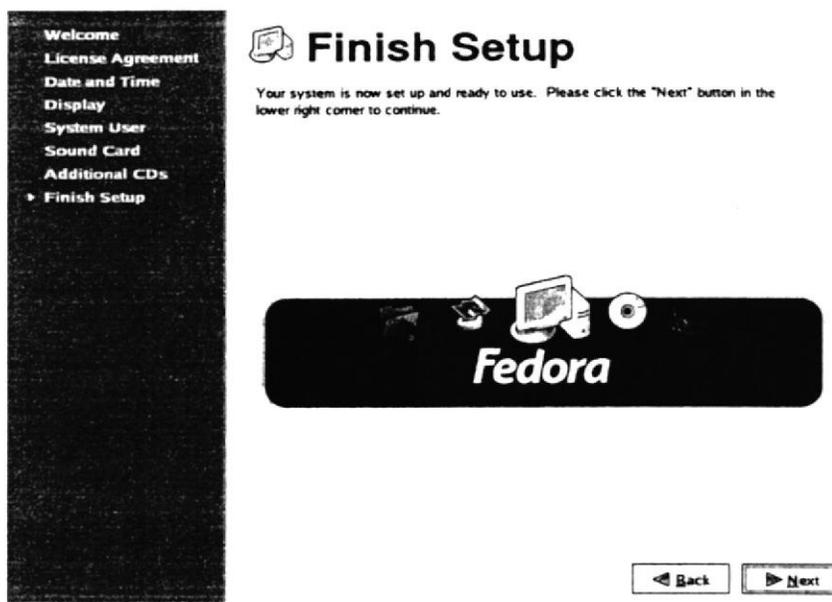


Figura 6. 27. Pantalla de finalización de la instalación



## 6.5.5 INICIANDO EL SISTEMA OPERATIVO

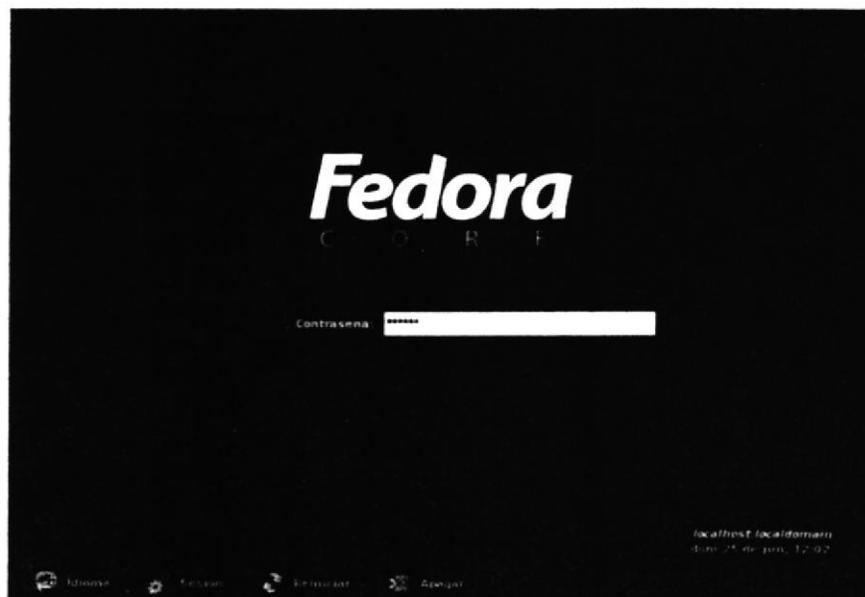
### 6.5.5.1 AMBIENTE GRÁFICO

1. Luego iniciará la primera sesión en Linux Fedora Core 3 con el respectivo usuario.



**Figura 6. 28.** Pantalla de inicio de sesión : ingresando usuario

2. Después deberá ingresar con la respectiva contraseña.



**Figura 6. 29.** Pantalla de inicio de sesión : ingresando contraseña

3. Luego podrá acceder a la Pantalla de Fedora Core 3.

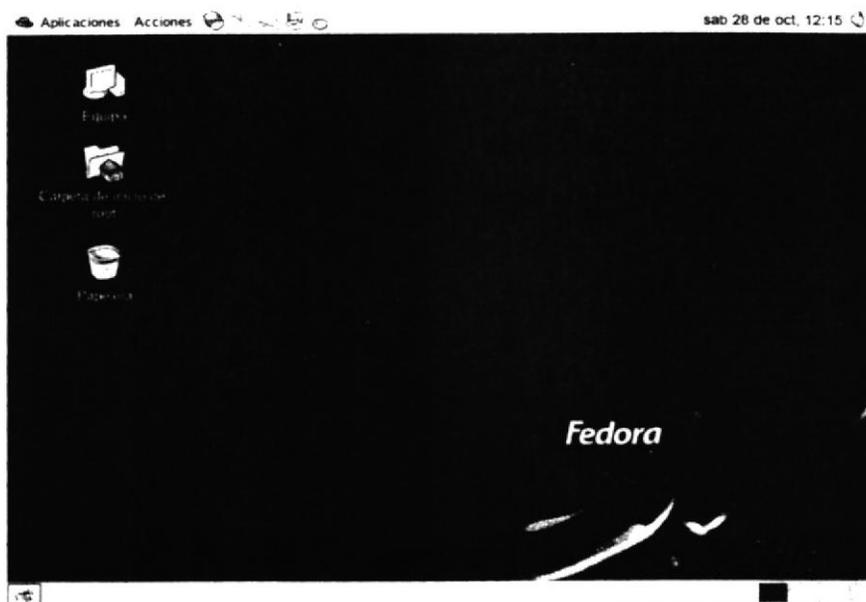


Figura 6. 30. Pantalla de escritorio de Fedora Core 3

### 6.5.5.2 MODO TEXTO

En el sistema operativo Linux utiliza gran variedad de comandos, para cambiar de ambiente gráfico a modo texto debe presionar las teclas CTRL + ALT + F1, F2 F3, F4 y F6.

1. Iniciando el sistema operativo Linux en modo texto, primero se solicita ingresar el login.

```
Kernel 2.6.9-11.EL on an i686
epsilon login: _
```

Figura 6. 31. Pantalla para Ingresar login

2. Después ingresar el nombre del usuario, en este caso el **root**.

```
Kernel 2.6.9-11.EL on an i686
epsilon login: root_
```

Figura 6. 32. Pantalla ingresando login

3. Luego se solicita la contraseña

```
Kernel 2.6.9-11.EL on an i686
epsilon login: root
Password: _
```

Figura 6. 33. Pantalla para ingresar password

4. Ingresar la contraseña respectiva **\*\*\*\*\***

```
Kernel 2.6.9-11.EL on an i686
epsilon login: root
Password: *****
[root@epsilon ~]# _
```

Figura 6. 34. Pantalla ingresando password



## 6.6 COMANDOS UNIX-LINUX

El sistema Linux tiene una gran cantidad de comandos que se pueden utilizar en cualquier momento, para lo cual deberá conocer que para ingresar en la consola de modo texto se mantiene presionada las teclas CTRL.+ ALT + F1, F2, F3, F4, F5 y F6. Con las combinación CTRL+ALT+F7 se accede al modo gráfico, dentro de esta consola le pedirá ingresar el root y la contraseña.

Linux identifica a los dispositivos como la tarjeta de red, disco duro, etc. de la siguiente manera:

- Disco Duro: HDA
- Tarjeta de Red: ETH0
- Mouse: TTYS0
- Modem: CUA0
- Cd Room: CD ROOM
- Disquetera: FDO

La tecla [tab] es muy útil ya que sirve para completar los comandos, los nombres de los archivos o directorios cuando se los está escribiendo en el prompt.

En muchos casos puede utilizarse el "\*" (asterisco) para reemplazar texto o el "?" (signo de interrogación) para reemplazar letras.

### 6.6.1 MANEJO DE CONSOLA

#### ➤ **man**

Muestra la ayuda sobre un comando específico, muestra los modificadores y las funciones que cumple cada comando.

```
# man <comando>
```

#### **Ejemplo**

```
# man ls
```

#### ➤ **pwd**

Muestra la ruta del directorio actual.

```
# pwd
```

#### ➤ **who**

Lista los usuarios conectados al sistema especificando su tipo, fecha y hora de conexión.

```
# who
```

**➤ ls**

Lista el contenido de un directorio.

```
# ls <parámetros> <directorio>
```

**Ejemplo**

```
- # ls -la /etc/sysconfig
```

"ls" -->	Comando de listado
"-l" -->	Modificador de listado detallado
"-a" -->	Modificador que muestra archivos ocultos
"/etc/sysconfig"-->	Lista el contenido del directorio especificado, si no lo especifica, lista el contenido del directorio actual.

**➤ cd**

Cambia la ruta de trabajo.

```
# cd <directorio>
```

**Ejemplo**

```
- # cd /etc
```

Cambia de directorio al directorio "etc" que se encuentra en la raíz, si no se especifica el "/", buscará el directorio como un subdirectorio o sea dentro de la carpeta en donde se encuentre.

```
- # cd ..
```

Retrocede un directorio.

```
- #cd /
```

Va al directorio raíz.

Si ejecuta el comando "cd" sólo lo llevará a la carpeta personal del usuario que esté usando, si está trabajando como root entonces lo llevará a la carpeta personal del root (/root).

➤ **su**

Comando para tomar la identidad de otro usuario, este comando le solicitará la contraseña del usuario que desea asumir. El root puede tomar la identidad de cualquier usuario sin necesidad de tener la contraseña.

```
# su <nombre_de_usuario>
```

**Ejemplo**

- # su alumno  
Tomará la identidad del usuario alumno.
- # su -  
Tomará la identidad del root pero previamente le solicitará la contraseña.

➤ **shutdown**

Comando para bajar el sistema.

```
# shutdown <modificador> now
```

**Ejemplo**

- # shutdown -r now  
Reinicia el sistema ( r = restart ).
- # shutdown -h now  
Apaga el sistema ( h = halt ).

## 6.6.2 VISUALIZACIÓN Y EDICIÓN DE TEXTO

➤ **cat**

Similar al **type** de DOS, muestra en pantalla el contenido de un archivo.

```
# cat <modificador> <archivo>
```

**Ejemplo**

- # cat /etc/inittab

Muestra en la pantalla el contenido del archivo "inittab".

➤ **tail**

Muestra las últimas líneas del contenido de un archivo.

```
# tail <archivo>
```

**Ejemplo**

- # tail /var/log/messages  
Muestra los últimos sucesos registrados en el archivo los "messages".

➤ **vi**

Editor de texto por excelencia en todos los sistemas UNIX.

Este editor es muy importante ya que demuestra a detalle todo el contenido de un archivo que otros editores de texto posiblemente no muestran.

Con este comando se puede crear y editar archivos de texto, sobretodo los archivos de configuración de Linux.

```
# vi <nombre_de_archivo>
```

Si el archivo no existe entonces creará uno nuevo según el nombre especificado, si no especifican ningún nombre entonces se abrirá el editor con documento y nombre en blanco.

### 6.6.3 COMANDOS DEL EDITOR VI

Para los comandos del editor **vi** hay que respetar las mayúsculas.

- [esc] tecla para entrar en modo comando

#### **Comandos para Insertar**

- i      Insertar texto.
- I      Insertar al inicio de la línea.
- A      Insertar al final de la línea.
- o      Agrega una línea debajo de línea actual.
- O      Agrega una línea arriba de la línea actual.

**Comandos de movimiento**

- *j* Desplazarse una línea hacia abajo.
- *k* Desplazarse una línea hacia arriba.
- *h* Desplazarse un carácter hacia la izquierda.
- *l* Desplazarse un carácter hacia la derecha.
- *[Ctrl]F* Desplazarse una pantalla hacia abajo.
- *[Ctrl]B* Desplazarse una pantalla hacia arriba.
- *\$* Moverse al final de la línea.
- *G* Desplazarse al final del archivo.
- *nG* Desplazarse a la línea *n*.

**Comandos para borrar**

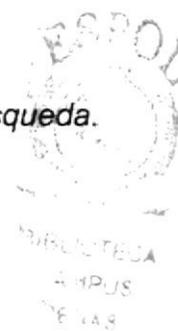
- *x* Borra un carácter sobre el cursor.
- *dd* Borra la línea en donde se encuentre el cursor
- *u* Deshacer el último comando.

**Comandos para buscar**

- */<texto>* Busca en el archivo el texto especificado
- *n* Encuentra la siguiente concordancia de la búsqueda.
- *p* Encuentra la previa concordancia de la búsqueda.

**Comandos para copiar y pegar**

- *yn* Copia en memoria *n* números de líneas
- *p* Pega lo copiado después del cursor
- *P* Pega lo copiado antes del cursor



### Comandos para guardar y salir

- :w Guarda el archivo
- :w <nombre>  
Guarda el archivo con el nombre especificado
- :wq Guarda el archivo y sale del vi
- :q Sale del archivo  
(en caso de que no hayan modificaciones)
- :q! Sale del archivo sin grabar

## 6.6.4 ADMINISTRACIÓN DE ARCHIVOS Y DIRECTORIO

### ➤ **mkdir**

Crear directorio.

```
# mkdir <nombre_del_directorio>
```

#### **Ejemplo**

- # mkdir prueba  
Crea el directorio **prueba** en el directorio actual

### ➤ **rm**

Borra archivos o directorios.

```
# rm <modificador> <nombre>
```

#### **Ejemplo**

- # rm -rf <nombre>  
Borrará un directorio con su contenido.  
-r recursivo, archivos y directorios  
-f fuerza, sin solicitar confirmación

### ➤ **rmdir**

Borrar directorio vacíos.

```
# rmdir <nombre_de_directorio>
```



➤ **chmod**

Cambia los permisos de lectura/escritura/ejecución de ficheros/directorios.

La sintaxis del comando `chmod` es la siguiente:

```
chmod [ugo][+][rwx] [nombre_archivo]
```

Donde [u=user, g=group y o=other]; [+/- activa o desactiva los atributos siguientes] [r=read, w=write, x=execute]

➤ **chown**

Cambia los permisos de usuario.

La sintaxis del comando `chown` es la siguiente:

```
chown [opciones] <usuario[.grupo]> <archivo[dir.> [archivo[dir. ...]
```

Las opciones incluyen:

- -R

Recursivo; para cambiar el dueño de todos los archivos y sub-directorios de un directorio dado.

- -v

Modo verboso; describe todas las acciones efectuadas por `chown`; reporta cuales archivos cambiaron de dueño como resultado del comando y cuales no han cambiado.

- -c

Como -v, pero sólo reporta cuales archivos cambiaron.

**Algunos ejemplos:**

- `chown nobody /shared/book.tex:`

Cambiar el dueño del archivo `/shared/book.tex` a `nobody`.

- `chown -Rc juan.musica *.mid conciertos/`

Atribuye todos los archivos en el directorio actual que terminan con `.mid` y todos los archivos y sub-directorios del directorio **conciertos/** al usuario **juan** y al grupo **musica**, reportando solo los archivos afectados por el comando.

➤ **touch**

El comando `touch` archivo puede tener dos consecuencias: si el archivo no existe aún, lo crea con tamaño 0 y como propiedad de nuestro usuario. Por otro lado, si el archivo ya existe, actualiza la fecha de modificación.

La sintaxis del comando `touch` es la siguiente:

```
touch [filename.]
```

➤ **find**

El comando `find` permite encontrar archivos, utilizando diversas técnicas. En principio, si se le pasa como parámetro únicamente una determinada ruta, por ejemplo `find /home/user`, el comando buscará todos los archivos y directorios que se encuentren a partir de esa ruta.

Utilizando algunos otros parámetros es posible buscar los archivos por diversos criterios.

- `find . -name "hola.txt"` encuentra todos los archivos llamados `hola.txt` que se encuentren a partir del directorio actual. Las comillas no son obligatorias, pero son recomendables si se quieren usar opciones más complejas.
- `find . -size 50k` busca los archivos que ocupan 50 kilobytes a partir del directorio actual. Si se utiliza `find . -size 20c`, buscará los archivos que ocupen 20 bytes. Y si se utiliza `find . -size 5b`, buscará los archivos que ocupen 5 bloques de 512 bytes cada uno.
- `find /home/user -empty` busca todos los archivos que se encuentran vacíos, a partir del directorio `/home/user`.

Es posible, además, utilizar opciones adicionales para la búsqueda, que indiquen la profundidad de la búsqueda, que agreguen otros criterios adicionales a los explicados, o que indiquen una acción a llevar a cabo una vez encontrados los archivos.

➤ **cp**

Comando para copiar archivos o directorios.

- `# cp <archivo1> <archivo2>`
- `# cp -rf <directorio1> <directorio2>`  
Copia directorios con su contenido  
-r recursivo, archivos y directorios.  
-f fuerza, sin solicitar confirmación.

➤ **mv**

Mueve un archivo o un directorio, también sirve para renombrar archivos o directorios en el caso de que no se especifique ruta destino.

- `# mv <ruta_archivo1> <ruta_archivo2>`
- `# mv <ruta_directorio1> <ruta_directorio2>`

➤ **wget**

Programa para descargar ficheros por http o ftp.



➤ **updatedb**

Actualiza la base de datos de directorios y archivos, este comando puede tardar algunos minutos dependiendo de la cantidad de archivos en el sistema.

# updatedb

➤ **locate**

Localiza archivos según la base de datos de archivos y directorios.

# locate <nombre>

➤ **mail**

Envío y lectura de correo electrónico.

➤ **mount**

Monta dispositivos como cdrom, disquetes, particiones de disco, particiones compartidas en red, etc., Para esto el directorio destino tiene que existir.

# mount <modificador> <sistema\_de\_archivos> <ruta\_origen> <ruta\_destino>

**Ejemplo**

- # mount -t iso9660 /dev/cdrom /media/cdrom

Monta unidad de cd-rom.

- #mount -t vfat /dev/hda1 /media/win

Monta una partición windows que se encuentre en el disco duro por ejemplo en la partición hda1.

- #mount -t smbfs //nombre\_server/recurso /media/directorio

Para montar recursos compartidos en red por windows.

➤ **umount**

Desmontar unidades.

- # umount directorio

- # umount /media/cdrom

Desmonta unidad de cd-rom.



## 6.6.5 MANEJO DE PAQUETES

### ➤ tar

Para desempaquetar o empaquetar un archivos o directorios.

```
# tar <modificador> <archivo>
```

#### Modificadores

- x *Extrae archivos empaquetados*
- f <nombre>  
*Crea el nombre del archivo contenedor*
- z *Comprime con formato gzip*
- t *Crea índice de archivos almacenados*
- v *Modo detallado*

#### **Ejemplo**

- # tar -xvf <nombre\_del\_archivo>  
*Desempaqueta un archivo con extensión .tar*
- # tar -cvf empaquetado.tar <nombre\_de\_archivo>  
*Empaqueta un archivo o un directorio con su contenido en un archivo llamado empaquetado.tar.*
- # tar -cvfz comprimido.tgz <nombre\_de\_archivo>  
*Comprime un archivo o un directorio con su contenido en un archivo llamado comprimido.tgz.*

### ➤ rpm

Creado por RedHat este comando es para instalar, desinstalar, actualizar, interrogar, verificar y construir paquetes de software.

```
# rpm <modificador> <nombre_archivo>
```

#### **Ejemplo**

- # rpm -ivh <nombre\_archivo>  
*Instalación de paquetes.*
- # rpm -Uvh <nombre\_archivo>  
*Upgrade de paquetes.*
- # rpm -ev  
*Desinstala un paquete.*
- # rpm -q <nombre>  
*Verifica si el paquete se encuentra instalado.*
- # rpm -ql <nombre>  
*Lista todos los paquetes relacionados (resuelve dependencias).*
- # rpm -qa | grep <nombre>  
*Verifica todos los paquetes instalados con ese nombre.*

➤ **unzip**

*Descomprime un archivo de formato .zip.*

```
# unzip <archivo.zip>
```

➤ **gzip**

*Comprime o descomprime un archivo.*

```
# gzip <modificador> <nombre_de_archivo>
```

**Ejemplo**

- # gzip ejemplo  
*Crea un archivo ejemplo.gz*
- #gzip -d ejemplo.gz  
*Descomprime el archivo ejemplo.gz*

## 6.6.6 INFORMACIÓN DEL SISTEMA Y MANEJO DE RECURSOS

➤ **uname**

*Muestra el sistema operativo instalado.*

```
# uname <modificador>
```

**Ejemplo**

- # uname -a  
*Muestra el nombre del sistema operativo nombre del servidor y versión del sistema.*

➤ **df**

*Muestra las particiones físicas montadas detallando su capacidad y la cantidad usada.*

```
# df
```

➤ **fdisk -l**

*Muestra todas las particiones creadas en el o los discos duros.*

```
# fdisk -l
```

➤ **top**

*Muestra los procesos o demonios que se están ejecutando, de acá se puede determinar el número asignado al proceso PID.*

```
# top
```



➤ **free**

Muestra cantidad usada y libre de la memoria RAM y memoria SWAP. En kilobyte por defecto.

# free <modificador>

- b Muestra la información en bytes.
- k Muestra la información en Kilobytes.
- m Muestra la información en Mega bytes.

➤ **ps**

Muestra reporte de procesos.

# ps

**Ejemplo**

- # ps aux  
Muestra todos los procesos que están en ejecución.

➤ **kill**

Comando para matar procesos

**Ejemplo**

# kill -9 <número del proceso - PID>  
Mata el proceso especificado.

➤ **netstat**

Muestra el estado de puertos levantados de red.

# netstat

**Ejemplo**

- # netstat -a  
Especifica los nombres de los puertos IP que se encuentran activos.
- # nestat -an  
Especifica los número de los puertos que se encuentran activos.

➤ **ifconfig**

Muestra la configuración de las tarjetas de red instaladas.

# ifconfig

➤ **route**

Muestra la configuración del gateway.

# route



### 6.6.7 UTILITARIOS BÁSICOS DE BASH

➤ **more**

*Opción de ver paso a paso cuando la información es extensa.*

**Ejemplo**

- # `cat archivo | more`
- # `ps aux | more`

➤ **grep**

*Utilitario que permite buscar palabras en el contenido del archivo.*

**Ejemplo**

- # `ps aux | grep squid`

## 6.7 CONFIGURACIÓN DE LA TARJETA DE RED

### 6.7.1 MODO TEXTO

Para configurar la tarjeta de red, primero iniciara sesión como **root**, colocando el nombre de usuario y contraseña en la pantalla que aparecerá de la siguiente manera:

```
localhost login: root
Password:*****
[root @ Epsilon ~]#
```

Después, iniciar sesión como usuario **root**, se configura la tarjeta de red, tanto del proveedor de servicios de internet como de la red interna.

Primero, configurar la tarjeta de red con la dirección IP asignada por el proveedor de Servicios de Internet, colocando además el Gateway y la máscara correspondiente.

```
[root @ Epsilon ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```



```
root@epsilon:~# vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=20.20.20.1
NETMASK=255.0.0.0
```

Figura 6. 35. Pantalla de configuración de la tarjeta de red de ISP (Internet).

Luego, configurar la tarjeta de red con la dirección IP de la red interna, colocando además el Gateway y la máscara correspondiente.

```
[root @ epsilon ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth1
```



```
root@epsilon:~# vi /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.0.1
GATEWAY=20.20.20.1
NETMASK=255.255.255.0
```

Figura 6. 36. Pantalla de configurar la tarjeta de red interna (Intranet).

Finalmente, reiniciar la red

```
[root @ epsilon ~]# service network restart
```

## 6.7.2 MODO GRÁFICO

Después de haber ingresado como usuario **root** digitar el comando **setup**, el cual permite ingresar a la utilidad de configuración.

```
[Root @ Epsilon ~]# netconfig
```

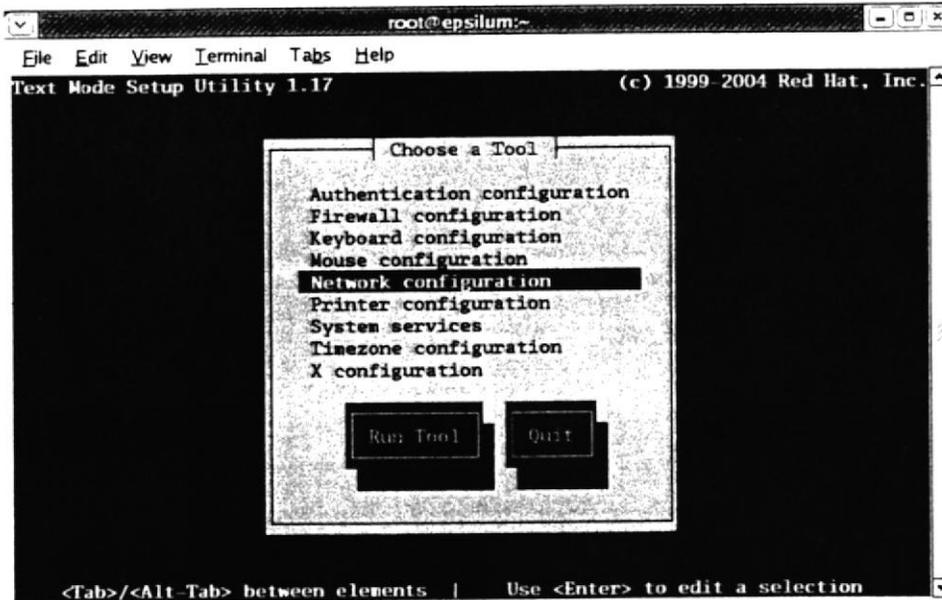


Figura 6. 37. Pantalla de netconfig

Dentro de esta ventana se puede configurar los firewalls, mouse, impresoras, tarjetas de red, etc.

Escoger la opción **Network configuration**, y se procede a configurar la tarjeta de red, colocando la dirección IP, máscara y default Gateway.

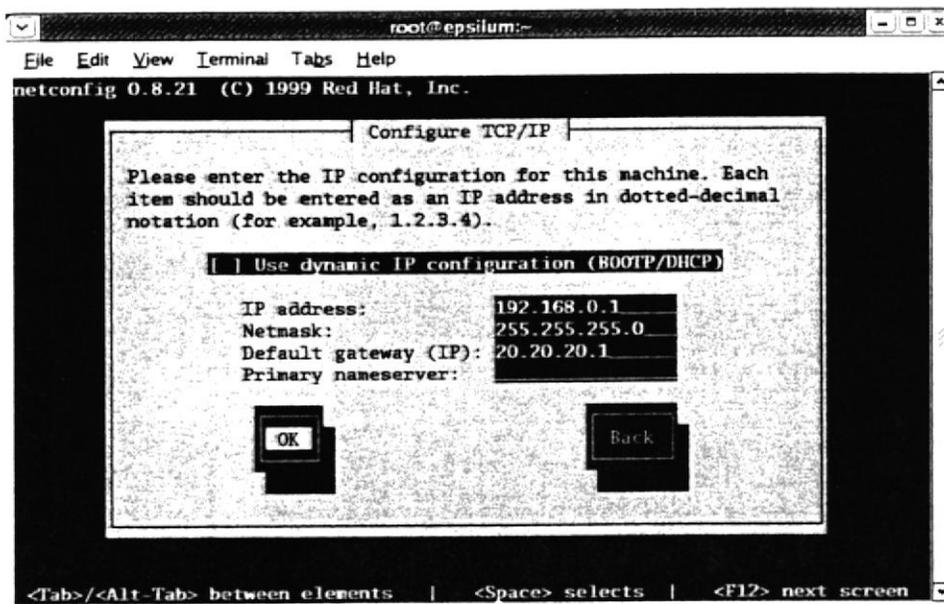


Figura 6. 38. Pantalla de configuración de red

Finalmente, reiniciar la red

```
[root @ epsilon ~]# service network restart
```

## 6.8 SERVIDOR DNS

### 6.8.1 ACERCA DE DNS

Un **DNS** (Domain Name System) es un conjunto de protocolos y servicios (base de datos distribuida), que permiten a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP. Por ejemplo, si la dirección IP del sitio FTP de prox.ve es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.ve y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente los DNS nacieron de la necesidad de recordar fácilmente los sitios visitados o a visitar y sustituir el antiguo sistema de identificación de "host" en Internet que consistía en un gran archivo donde estaban almacenados los nombres y las direcciones IP de cada nodo de la red con el cual se podía establecer comunicación.

#### 6.8.1.1 Bind (Berkeley Internet Name Domain).

**BIND** (acrónimo de **Berkeley Internet Name Domain**) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

- Un servidor de sistema de nombres de dominio (named).
- Una biblioteca resolutoria de sistema de nombres de dominio.
- Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

El Servidor DNS BIND es ampliamente utilizado en la Internet (99% de los servidores DNS) proporcionando una robusta y estable solución.

#### 6.8.1.2 DNS (Domain Name System).

**DNS** (acrónimo de **Domain Name System**) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombre de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El **DNS** nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección IP.

#### 6.8.1.3 NIC (Network Information Center).

**NIC** (acrónimo de **Network Information Center** o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genéricos o por países, permitiendo

personas o empresas montar sitios de Internet a través de un **ISP** mediante un **DNS**. Técnicamente existe un **NIC** por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país.

#### 6.8.1.4 FQDN (Fully Qualified Domain Name).

**FQDN** (acrónimo de **Fully Qualified Domain Name** o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del **DNS**. Se distingue de un nombre regular porque lleva un punto al final.

Como ejemplo: suponiendo que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y un dominio llamado «dominio.com», el **FQDN** sería «**maquina1.dominio.com.**», así es que se define de forma única al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solo puede haber uno llamado «**maquina1.dominio.com.**». La ausencia del punto al final definiría que se pudiera tratar tan solo de un prefijo, es decir «**maquina1.dominio.com**» pudiera ser un dominio de otro más largo como «**maquina1.dominio.com.mx**».

La longitud máxima de un **FQDN** es de 255 bytes, con una restricción adicional de 63 bytes para cada etiqueta dentro del nombre del dominio. Sólo se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-». No se distinguen mayúsculas y minúsculas.

#### 6.8.1.5 Componentes de un DNS.

Los **DNS** operan a través de tres componentes: Clientes **DNS**, Servidores **DNS** y Zonas de Autoridad.

##### 6.8.1.5.1 Clientes **DNS**.

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección **IP** que corresponde a un nombre determinado.

##### 6.8.1.5.2 Servidores **DNS**.

Son servicios que contestan las consultas realizadas por los **Clientes DNS**. Hay dos tipos de servidores de nombres:

- **Servidor Maestro:** También denominado **Primario**. Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.
- **Servidor Esclavo:** También denominado **Secundario**. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado **transferencia de zona**.

El DNS requiere que **al menos tres servidores existan** para todos los dominios delegados (o zonas).

Una de las principales razones para **tener al menos tres servidores** para cada zona es permitir que la información de la zona misma esté disponible siempre y en forma confiable hacia los **Clientes DNS** a través de Internet cuando un servidor DNS de dicha zona falle, no esté disponible y/o esté inalcanzable.

Contar con múltiples servidores también facilita la **propagación** de la zona y mejoran la eficiencia del sistema en general al brindar opciones a los **Clientes DNS** si acaso encontraran dificultades para realizar una consulta en un **Servidor DNS**.

Con múltiples servidores, por lo general uno actúa como **Servidor Maestro o Primario** y los demás como **Servidores Esclavos o Secundarios**. Correctamente configurados y una vez creados los datos para una zona, no será necesario copiarlos a cada **Servidor Esclavo o Secundario**, pues éste se encargará de transferir los datos de manera automática cuando sea necesario.

Los **Servidores DNS** responden dos tipos de consultas:

- **Consultas Iterativas (no recursivas):** El cliente hace una consulta al **Servidor DNS** y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro **Servidor DNS** repitiéndose este proceso hasta encontrar al **Servidor DNS** que tiene la **Zona de Autoridad** capaz de resolver la consulta.
- **Consultas Recursivas:** El **Servidor DNS** asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el **Ciente DNS**. El **Servidor DNS** desarrolla entonces **Consultas Iterativas** separadas hacia otros **Servidores DNS** (en lugar de hacerlo el **Ciente DNS**) para obtener la respuesta solicitada.

#### 6.8.1.6 Zonas de Autoridad.

Permiten al **Servidor Maestro o Primario** cargar la información de una zona. Cada **Zona de Autoridad** abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

La información de cada **Zona de Autoridad** es almacenada de forma local en un fichero en el **Servidor DNS**. Este fichero puede incluir varios tipos de registros:

Tipo de Registro.	Descripción.
A (Address)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv4 de 32 bits.

Tipo de Registro.	Descripción.
<b>AAAA</b>	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección <b>IPv6</b> de 128 bits.
<b>CNAME</b> (Canonical Name)	Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los sub-dominios y registros DNS del dominio original.
<b>MX</b> (Mail Exchanger)	Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.
<b>PTR</b> (Pointer)	Registro de apuntador que resuelve direcciones <b>IPv4</b> hacia el nombre anfitriones. Es decir, hace lo contrario al registro <b>A</b> . Se utiliza en zonas de <b>Resolución Inversa</b> .
<b>NS</b> (Name Server)	Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio.
<b>SOA</b> (Start of Authority)	Registro de inicio de autoridad que especifica el <b>Servidor DNS Maestro</b> (o <b>Primario</b> ) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.
<b>SRV</b> (Service)	Registro de servicios que especifica información acerca de servicios disponibles a través del dominio. Protocolos como <b>SIP</b> ( <b>Session Initiation Protocol</b> ) y <b>XMPP</b> ( <b>Extensible Messaging and Presence Protocol</b> ) suelen requerir registros <b>SRV</b> en la zona para proporcionar información a los clientes.
<b>TXT</b> (Text)	Registro de texto que permite al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras <b>DNSBL</b> ( <b>DNS-based Blackhole List</b> ) para la filtración de Spam. Otro ejemplo de uso son las VPN, donde suele requerirse un registro <b>TXT</b> para definir una llave que será utilizada por los clientes.

Las zonas que se pueden resolver son:

#### Zonas de Reenvío.

Devuelven **direcciones IP** para las búsquedas hechas para nombres **FQDN** (**Fully Qualified Domain Name**).

En el caso de dominios públicos, la responsabilidad de que exista una **Zona de Autoridad** para cada **Zona de Reenvío** corresponde a la autoridad misma del dominio, es decir, y por lo general, quien esté registrado como autoridad del dominio tras consultar una base de datos **WHOIS**. Quienes compran dominios a través de un **NIC** (por ejemplo ejemplo: [www.nic.mx](http://www.nic.mx)) son quienes se hacen cargo de las **Zonas de Reenvío**, ya sea a través de su propio **Servidor DNS** o bien a través de los **Servidores DNS** de su **ISP**.

Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un **NIC** como requisito para tener derecho legal a utilizarlo y poder propagarlo a través de Internet.

### Zonas de Resolución Inversa.

Devuelven nombres **FQDN (Fully Qualified Domain Name)** para las búsquedas hechas para **direcciones IP**.

En el caso de segmentos de red públicos, la responsabilidad de que exista una **Zona de Autoridad** para cada **Zona de Resolución Inversa** corresponde a la autoridad misma del segmento, es decir, y por lo general, quien esté registrado como autoridad del segmento tras consultar una base de datos **WHOIS**.

Los grandes **ISP**, y en algunos casos algunas empresas, son quienes se hacen cargo de las **Zonas de Resolución Inversa**.

### 6.8.2 FUNCIONAMIENTO

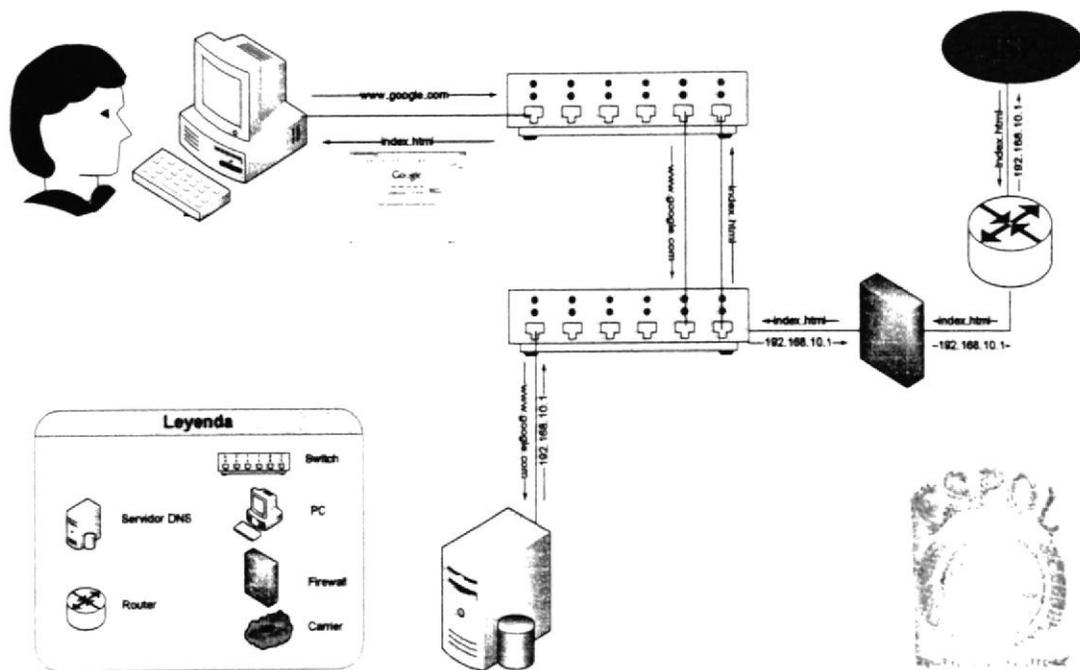


Figura 6. 39. Funcionamiento del Servidor DNS

### 6.8.3 BENEFICIOS DNS

Los beneficios que tiene el servidor DNS son los siguientes:

- **Conveniencia:**  
Nombres conocidos por el usuario son más fácil de recordar que sus respectivas direcciones IP.
- **Consistencia:**  
Las direcciones IP pueden cambiar pero los nombres permanecen constantes.
- **Simplicidad:**  
Usuarios necesitan aprender sólo un nombre para encontrar recursos ya sea en internet o en una Intranet.

### 6.8.4 REQUERIMIENTOS PARA CONFIGURAR EL SERVIDOR DNS

- Sistema Operativo Linux Fedora Core 3.
- Tener la tarjeta de red configurada con una IP estática.
- Tener un dominio.
- Tener instalado el paquete bind.

### 6.8.5 CONFIGURACIÓN DNS:

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul

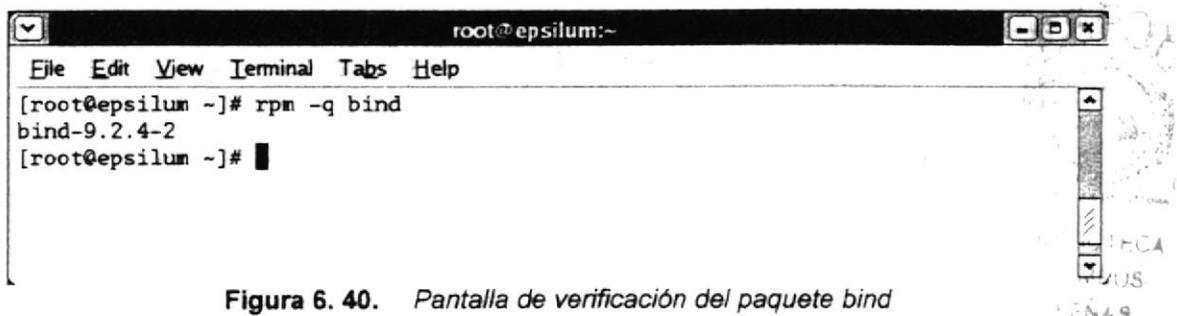
Para configurar un DNS debe instalarse el paquete **bind**; el proceso que atiende las consultas se denomina **named**, y corre en forma permanente en la máquina, escuchando y atendiendo las consultas que le llegan. Un programa que actúa de esta manera se denomina un "demonio".

Lo primero que se debe hacer es verificar si el paquete bind está instalado; esto se lo hace de la siguiente manera:

#### **rpm -q bind** (verificar si esta instalado el paquete bind)

- El paquete **BIND** instala una configuración simple y útil para un servidor de nombres de usuario final. Esta configuración básica actúa como un servidor de nombres "caché": sólo guarda las direcciones IP y los nombres de máquinas que va conociendo, para responder las consultas sin tener que repetir la búsqueda cada vez.

Al presionar la tecla **ENTER** aparecerá la siguiente pantalla:



```
root@epsilon:~  
File Edit View Terminal Tabs Help  
[root@epsilon ~]# rpm -q bind  
bind-9.2.4-2  
[root@epsilon ~]#
```

Figura 6. 40. Pantalla de verificación del paquete bind

Una vez comprobado que el paquete `bind` está instalado, ingrese al archivo de configuración `named.conf`, esto se lo hace de la siguiente manera:

**vi /etc/named.conf** (ingresar al archivo `named.conf`)

➤ **named.conf:**

Archivo de configuración para el servidor DNS local. Aquí figuran todos los nombres de archivos locales consultados, direcciones de servidores DNS próximos y ajustes de operación para el DNS.

Al presionar la tecla **ENTER** aparecerá la siguiente pantalla:

```

root@epsilon:/var/named
File Edit View Terminal Tabs Help

zone "." IN {
    type hint;
    file "named.ca";
};

zone "localdomain" IN {
    type master;
    file "localdomain.zone";
    allow-update { none; };
};

zone "localhost" IN {
    type master;
    file "localhost.zone";
    allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    allow-update { none; };
};

```

**Figura 6. 41.** Pantalla de configuración del archivo `named.conf`

Una vez dentro del archivo `named.conf` creara una nueva zona de dominio.

```

zone "epsilon.com" IN { ( dirección DNS)
    type master; (servidor principal o secundario)
    file"epsilon.com.zone" ( nombre de la zona donde configuro mi
dominio)
    Allow-update { none; }; (Realiza actualizaciones dinámicas)
};

```

Después salir y guardar.

**Esc** (Salir de modo de edición)

**:wq** (Grabar y salir)

Luego de crear la zona, es necesario acceder al lugar donde está el archivo **.zone** en el DNS (file"epsilon.com.zone"), se lo hace de la siguiente manera:

```
cd /var/named/
```

(Ruta donde se encuentra el archivo .zone)

**Importante**

El comando cd permite cambiar de directorio, igual que en DOS.

Después verificar la lista de archivos donde debe de estar la zona **localhost.zone**.

```
ls
```

(Listar el contenido del directorio)

**Importante**

El comando ls permite listar el contenido de un directorio.

Una vez accedida a la ruta indicada crear el archivo **epsilon.com.zone**, pero en este caso copiar el archivo **localhost.zone** en **epsilon.com.zone** haciendo uso del comando **cp**.

```
cp localhost.zone epsilon.com.zone
```

(Copiar el archivo localhost.zone a epsilon.com.zone)

**Importante**

El comando cp permite copiar archivos o directorios.

Una vez creado el archivo **epsilon.com.zone**, ingresar a él para editarlo y digitar lo siguiente para proceder con la configuración respectiva:

```
vi epsilon.com.zone
```

(Editar el archivo epsilon.com.zone)

**Importante**

El comando vi permite editar archivos.



**Configuración:**

```

@IN SOA (dirección DNS) epsilon.com. root.epsilon.com. (
    42 ; serial (d. adams)
    3H ; refresh
    15M ; retry
    1W ; expiry
    1D) ; minimum

localhost IN NS epsilon.com. (apunta posición específica)
epsilon.com. IN A 127.0.0.1 (dirección del loopback)
www IN CNAME epsilon.com. (nombre del dominio).

```

Algunas claves para la interpretación de estos archivos incluyen:

- @ Abreviatura para el nombre de la zona actual.
- SOA "Start Of Authority", responsable y otros para esta zona de autoridad.
- NS "NameServer", indica el nombre del servidor de nombres.
- A "Address", dirección IP para un nombre de máquina (directo).
- CNAME "Canonical NAME", indica el nombre real para un alias.
- Serial número de serie para control de modificaciones.

Copiar la zona creada al directorio **chroot** para que reconozca la zona, y esto lo realizara digitando la siguiente línea:

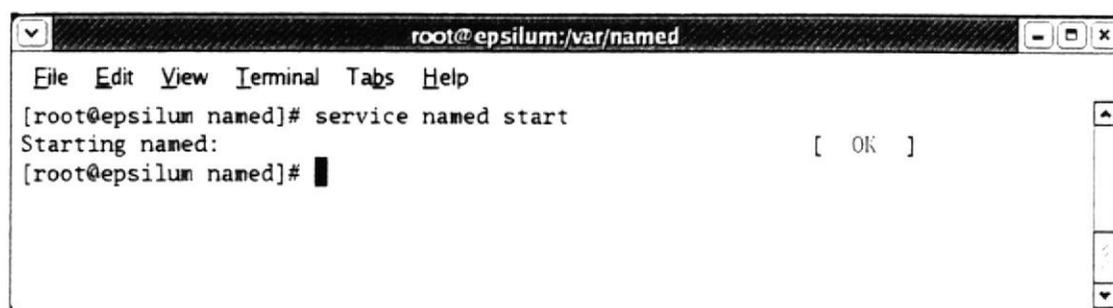
```
cp epsilon.com.zone chroot/var/named/
```

(Copiar el archivo `epsilon.com.zone` a `chroot/var/named/`)

Una vez asignada la configuración correspondiente, iniciara el servicio **named** para que se actualice.

```
service named start
```

(Iniciar el servicio `named`)



```

root@epsilon:/var/named
File Edit View Terminal Tabs Help
[root@epsilon named]# service named start
Starting named: [ OK ]
[root@epsilon named]# █

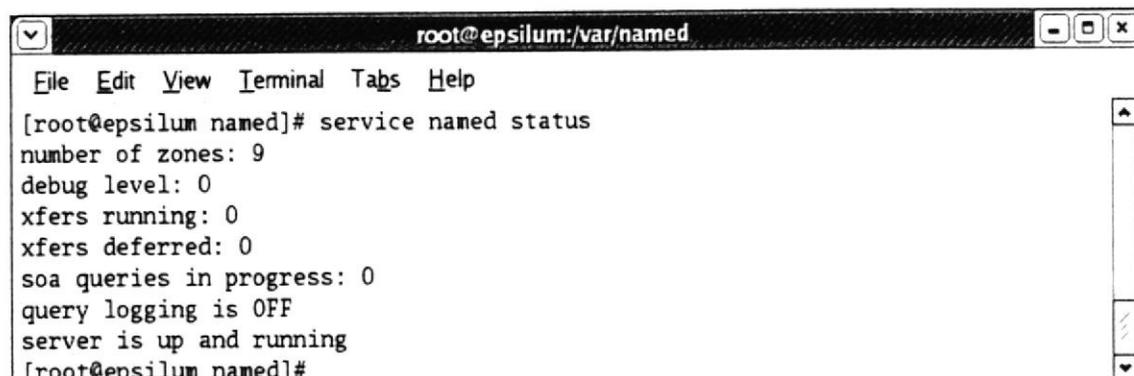
```

**Figura 6. 42.** Pantalla de iniciar el servicio `named`

Luego hacer un status para ver si no hay ningún error en la configuración.

### **service named status**

(Verificar el estado del servicio named)



```

root@epsilon:/var/named
File Edit View Terminal Tabs Help
[root@epsilon named]# service named status
number of zones: 9
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
server is up and running
[root@epsilon named]#
  
```

**Figura 6. 43.** Pantalla de verificar el estatus del servicio named.

Para cambiar la configuración del servidor DNS local en Linux se debe ingresar al archivo **resolv.conf**.

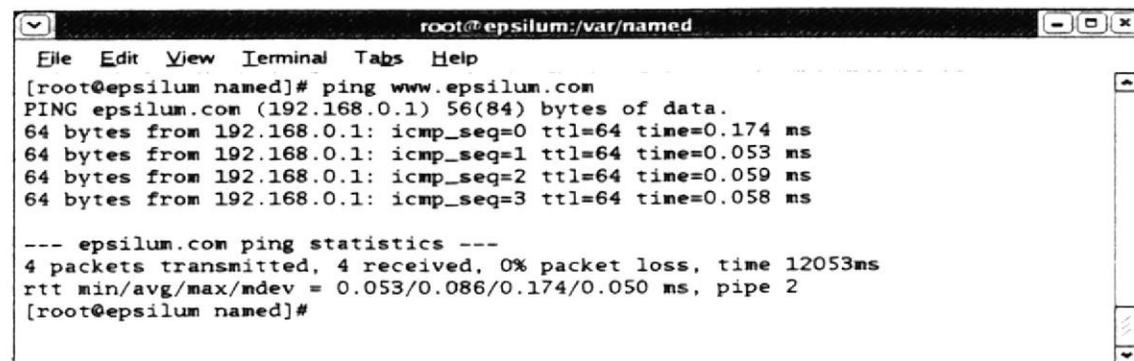
### **vi /etc/resolv.conf** (ruta para acceder a resolv.conf)

➤ Los servidores de nombres a usar se indican en el archivo /etc/resolv.conf.

Ahí encontrará el NameServer, se debe cerciorarse de que la IP sea la misma que la de la tarjeta de red, sino establecerla.

**search localdomain** (buscara dominios locales)  
**nameserver 192.168.0.1** (dirección del servidor)  
**nameserver 127.0.0.1** (dirección del loopback)

Para realizar una comprobación y de esta manera verificar si el servicio DNS está funcionando correctamente, realizara un **ping**. Si éste no está funcionando, ping "icmp" lanzará un mensaje de fin de tiempo de espera, indicando que no fue posible realizar una conexión.



```

root@epsilon:/var/named
File Edit View Terminal Tabs Help
[root@epsilon named]# ping www.epsilon.com
PING epsilon.com (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=0.174 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.058 ms

--- epsilon.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 12053ms
rtt min/avg/max/mdev = 0.053/0.086/0.174/0.050 ms, pipe 2
[root@epsilon named]#
  
```

**Figura 6. 44.** Pantalla para realizar ping a www.epsilon.com

### 6.8.6 CONFIGURACIÓN EN CLIENTE WINDOWS

1. Dar doble clic al icono mis sitios de red.



Figura 6. 45. Icono de Mis sitios de Red

2. Clic secundario en el icono conexiones de área local y seleccionar propiedades.

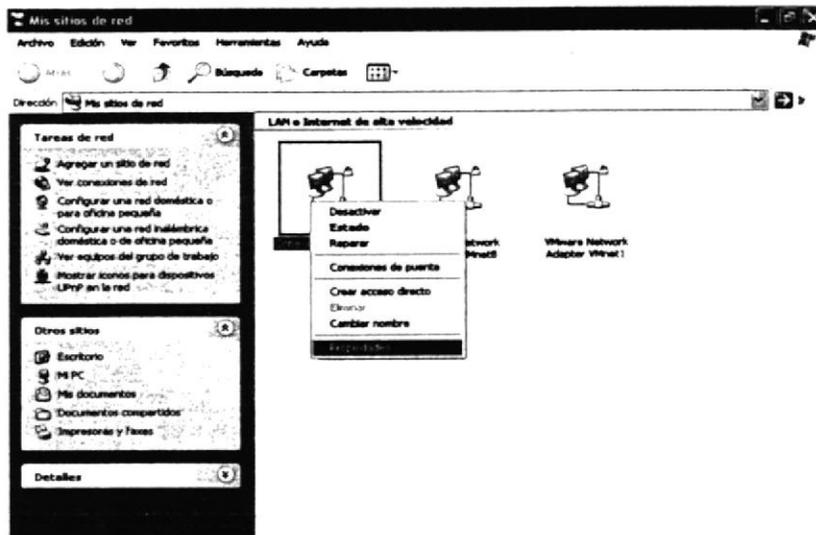


Figura 6. 46. Pantalla de Mis sitios de Red

3. Luego ir a la opción Protocolo de Internet TCP/IP y dar clic en propiedades.

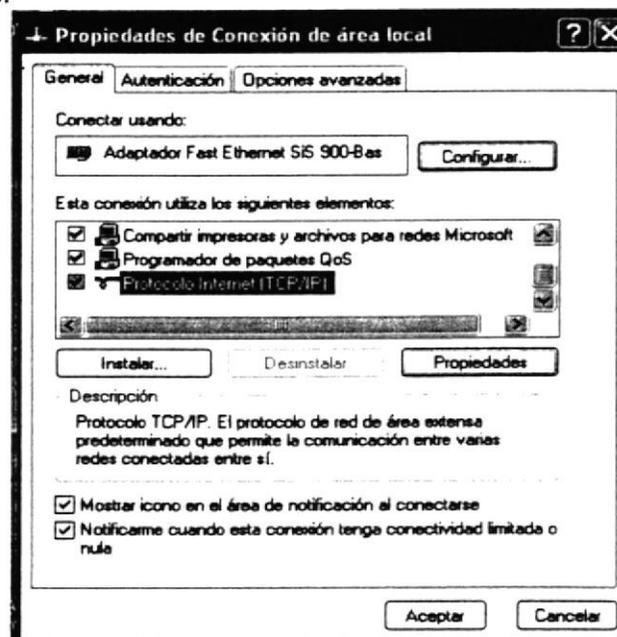


Figura 6. 47. Pantalla de Propiedades de Conexión de Área Local

4. Configurar la tarjeta de red y asignar la dirección del DNS de Linux a la tarjeta de red.

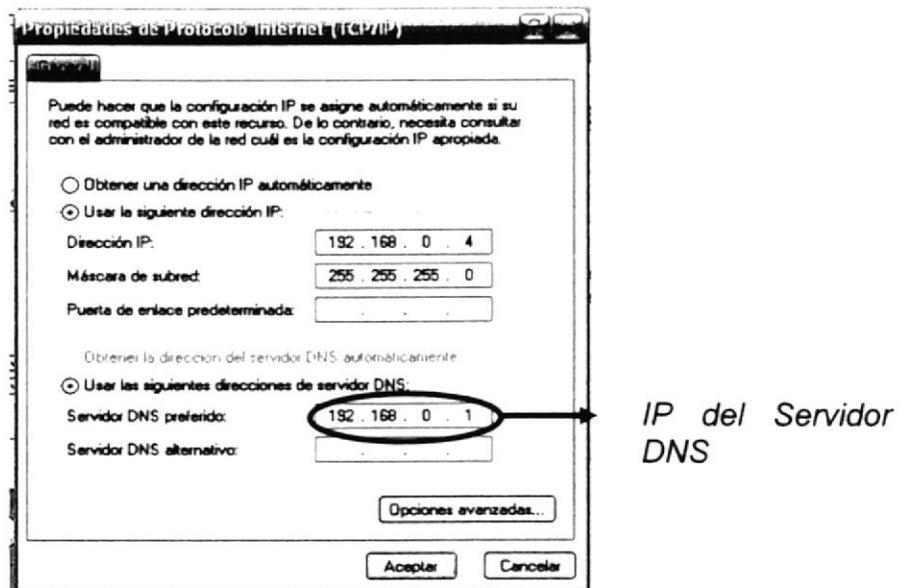


Figura 6. 48. Pantalla: Propiedades de Protocolo Internet (TCP/IP)

Luego de haber colocado la dirección del Servidor DNS, comprobar si hay respuesta de parte de dicho servidor realizando ping a la dirección [www.epsilon.com](http://www.epsilon.com).

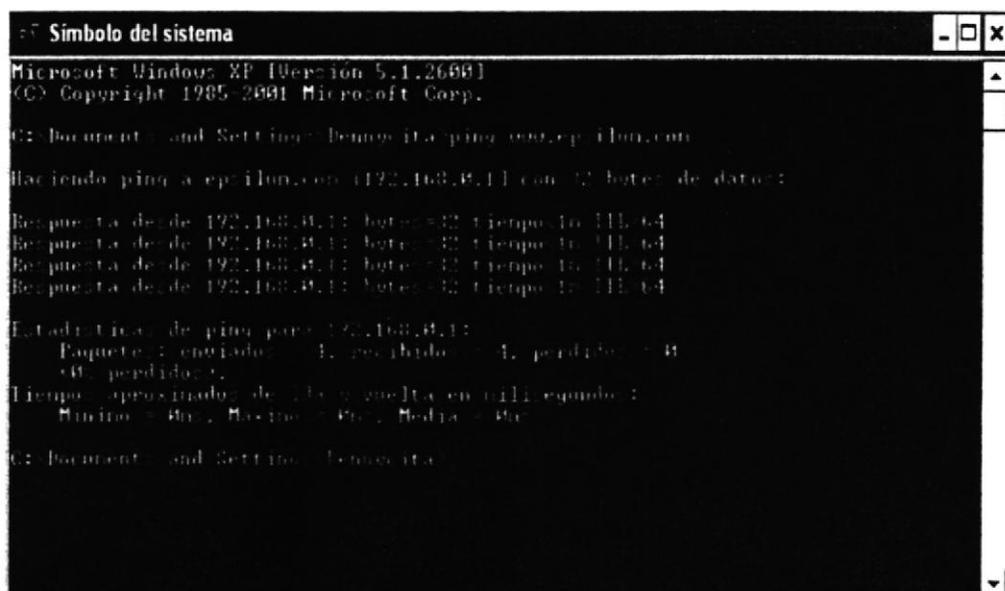


Figura 6. 49. Pantalla de realizar ping a [epsilon.com](http://www.epsilon.com)



## 6.9 SERVIDOR WEB

### 6.9.1 ACERCA DE SERVIDOR WEB

Apache surgió a partir del servidor de HTTP más famoso y difundido en su época: NCSA. Desde entonces se convirtió en un poderoso rival de todos los servidores Unix utilizados hasta la fecha por su eficiencia, funcionalidad y rapidez. Es por ello que se conoce como el rey de los servidores Web. Se desarrolla de forma estable y segura gracias a la cooperación y los esfuerzos de un grupo de personas conocidas como grupo Apache (Apache Group), los cuales se comunican a través de Internet y del Web. Juntos se dedican a perfeccionar el servidor y su documentación regidos por la ASF (Apache Software Foundation).

En la actualidad Apache es el servidor Web más utilizado en el mundo de acuerdo con las estadísticas que lo colocan en más de 7 millones de servidores que sirven poco más de 18 millones de sitios Web, lo cual significa más del 60% en todo el mundo.

Entre las características principales del Apache se encuentran:

- Es un servidor Web potente, flexible y ajustado al HTTP/1.1
- Es altamente configurable y extensible.
- Puede ser ajustado a través de la definición de módulos empleando su propio API (Application Programming Interface).
- Provee todo su código fuente de forma libre y se distribuye bajo una licencia no restrictiva.
- Se ejecuta en diversas plataformas operativas tales como: Windows 9x/NT, Macintosh, Novell NetWare, OS/2, Linux y la mayoría de los Unix existentes: IRIX, Solaris, HPUX, SCO, FreeBSD, NetBSD, AIX, Digital Unix, etc.
- Se desarrolla de forma acelerada estimulando la retroalimentación desde sus usuarios a través de nuevas ideas, reportes de errores y parches.
- Implementa muchas posibilidades frecuentemente demandadas, tales como:
  - ✓ Bases de datos DBM para autenticación.  
Permiten establecer fácilmente la protección de documentos a través de passwords para una gran cantidad de usuarios sin dañar el funcionamiento del servidor.
  - ✓ Respuestas adaptables a los errores o problemas.  
Se pueden definir ficheros o scripts de tipo CGI que respondan ante la ocurrencia de errores internos o en las solicitudes realizadas.
  - ✓ Directiva para definir múltiples índices.  
Se utiliza cuando se solicitan directorios por parte de los clientes a partir de lo cual se puede buscar en estos y devolver un documento índice cuyo nombre puede ser por ejemplo: index.html, index.cgi o default.html.

- ✓ *Ilimitadas y flexibles posibilidades de redireccionamiento y definición de alias para los URLs.*

*Apache no tiene un límite establecido para definir alias y redireccionamientos que pueden ser declarados en sus ficheros de configuración.*

- ✓ *Negociación del contenido de las respuestas.*

*Apache es capaz de ofrecer la mejor representación de la información accedida de acuerdo con las capacidades del cliente solicitante.*

- ✓ *Soporte de hosts virtuales.*

*Es la habilidad del servidor de distinguir entre los pedidos hechos a diferentes direcciones IP o nombres de dominio definidos en la misma máquina.*

- ✓ *Configuración flexible de las trazas generadas.*

*Es posible adaptar el formato de las trazas obtenidas así como redireccionarlas a través de tuberías (Unix) en aras de filtrarlas. De esta forma se puede lograr por ejemplo dividir dinámicamente las trazas de los hosts virtuales en distintos ficheros.*

### **6.9.2 ACERCA DEL PROTOCOLO HTTP.**

*HTTP (Hypertext Transfer Protocol, o Protocolo de Tránsito de Hipertext), es el método utilizado para transferir o transportar información en la Red Mundial (WWW, World Wide Web). Su propósito original fue el proveer una forma de publicar y recuperar documentos HTML.*

*El desarrollo del protocolo fue coordinado por World Wide Web Consortium y la IETF (Internet Engineering Task Force, o Fuerza de Trabajo en Ingeniería de Internet), culminando con la publicación de varios RFC (Request For Comments), de entre los que destaca el RFC 2616, mismo que define la versión 1.1 del protocolo, que es el utilizado hoy en día.*

*HTTP es un protocolo de solicitud y respuesta a través de TCP, entre agentes de usuarios (Navegadores, motores de índice y otras herramientas) y servidores, regularmente utilizando el puerto 80. Entre la comunicación entre éstos puede intervenir como servidores Intermedarios (Proxies), puertas de enlace y túneles.*

### **6.9.3 ACERCA DE APACHE.**

*Apache es un servidor HTTP, de código abierto y licenciamiento libre, que funciona en Linux, sistemas operativos derivados de Unix™, Windows, Novell Netware y otras plataformas. Ha desempeñado un papel muy importante en el crecimiento de la red mundial, y continua siendo el servidor HTTP más utilizado, siendo además el servidor de facto contra el cual se realizan las pruebas comparativas y de desempeño para otros productos competidores.*

### 6.9.4 CARACTERÍSTICAS DEL SERVIDOR APACHE

El Servidor Apache, incluye las siguientes funcionalidades:

- Los módulos Apache API — se utiliza un nuevo conjunto de interfaces de programación de aplicaciones (APIs).
- Filtrado — Los módulos pueden actuar como filtros de contenido.
- Soporte a IPv6 — Se soporta la próxima generación de formato de direcciones IP.
- Directrices simplificadas — Se han eliminado una serie de directrices complicadas y otras se han simplificado.
- Respuestas a errores en diversos idiomas — Cuando usa documentos Server Side Include (SSI), las páginas de errores personalizables se pueden entregar en diversos idiomas

### 6.9.5 FUNCIONAMIENTO

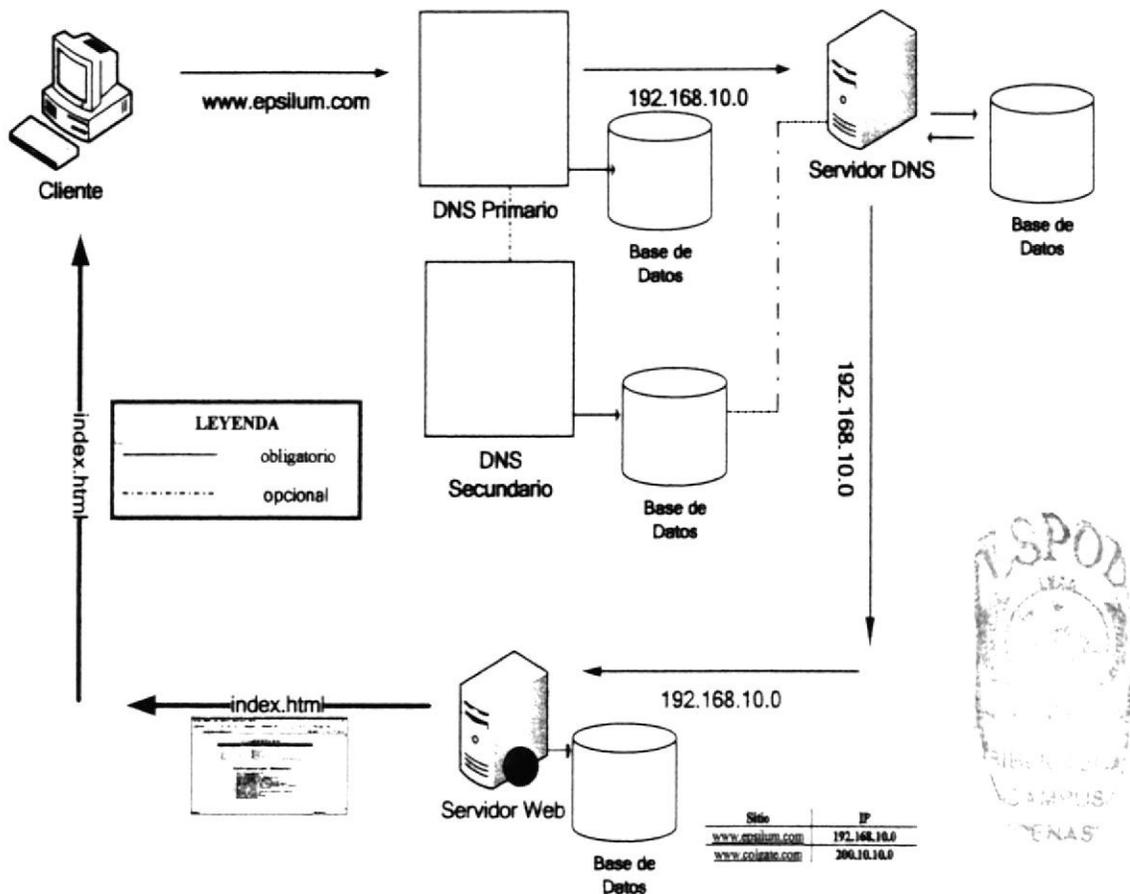


Figura 6. 50. Funcionamiento del Servidor Web

Apache extiende este diseño modular hasta las funciones más básicas de un servidor web. El servidor viene con una serie de Módulos de MultiProcesamiento que son responsables de conectar con los puertos de red de la máquina, aceptar las peticiones, y generar los procesos hijo que se encargan de servirlos.

### 6.9.6 BENEFICIOS SERVIDOR WEB

- Apache puede soportar de una forma más fácil y eficiente una amplia variedad de sistemas operativos.
- El servidor puede personalizarse mejor para las necesidades de cada sitio web.

### 6.9.7 REQUERIMIENTOS

- Sistema operativo Linux Fedora Core 3.
- Tener la tarjeta de red configurada con una IP estática.
- Dirección IP.
  - Se necesita una IP PÚBLICA en caso de que haya salida a Internet.
- Tener levantado el servidor DNS, con su respectivo dominio registrado.

### 6.9.8 CONFIGURACIÓN DE WEB SERVER:

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

Para poder empezar a configurar el servidor Apache es necesario verificar si está instalado el paquete http, y lo hará de la siguiente manera:

```
rpm -q httpd (verificar si está instalado el paquete httpd)
```

- **HTTPD:** El programa servidor HTTP Apache, contiene las directivas que controlan el funcionamiento del demonio servidor (httpd).



```
root@epsilon:/etc/httpd
File Edit View Terminal Tabs Help
[root@epsilon httpd]# rpm -q httpd
httpd-2.0.52-12.ent.centos4
[root@epsilon httpd]#
```

Figura 6. 51. Pantalla para verificar si está instalado el paquete httpd

Luego se ingresa al archivo de configuración correspondiente: **httpd.conf**. Accederá de la siguiente forma:

```
vi /etc/httpd/conf/httpd.conf (ruta de archivo de configuración)
```

**Importante**

El comando `vi` permite editar archivos.

Una vez dentro del archivo de configuración, efectuar varios cambios. Las siguientes líneas por default están des-comentadas, pero hay que verificarlas.

Primero habilitar la etiqueta **listen 80**, para permitir la navegación web.

**Listen 80**

(Permite la navegación por medio del puerto 80 que es el puerto `httpd`).

Es necesario especificar que tipo de extensión tendrá la página de inicio, ya que si no se especifica, el sitio nunca podrá ser mostrado. Se hace de la siguiente manera:

**Directory Index index.html index.htm**

(Se define tipo de archivo página principal).

La línea que viene a continuación se la des-comentada, ya que es la que permite la navegación.

**NameVirtualHost \*:80** (Permite navegación a través del sitio).

Establecer la ruta en la que se encontrará el sitio Web y el nombre del mismo. Agregar las siguientes líneas:

**<VirtualHost \*:80>**

Define el puerto en el cual escucha el servidor (0 - 65535). Hay que tener en cuenta la relación que tiene esta directiva con el fichero `/etc/services` y que algunos puertos, especialmente los situados por debajo del 1024, están reservados para protocolos específicos. El puerto estándar para el protocolo HTTP es el 80.

**ServerAdmin root@localhost.localdomain**

Define la dirección de correo que el servidor incluirá en cualquier mensaje de error que devuelva al cliente.

**DocumentRoot /var/www/html/epsilon**

Define el directorio desde el cual el servidor servirá los documentos. A menos que la URL solicitada coincida con una directiva Alias, el servidor añadirá el PATH a la URL.

**ServerName www.epsilon.com**

(Define el nombre de host del servidor. Se suele utilizar cuando se crean redirecciones. Sino se define el nombre de servidor, intentará deducirlo a través de su dirección IP.)

**</VirtualHost>**

Luego, ir a la ruta que se ha especificado para ubicar y crear el sitio.

```
cd /var/www/html/ (Ruta del sitio web)
```

Crear la carpeta donde estará almacenada la página e ingresar a la carpeta, lo realiza digitando lo siguiente:

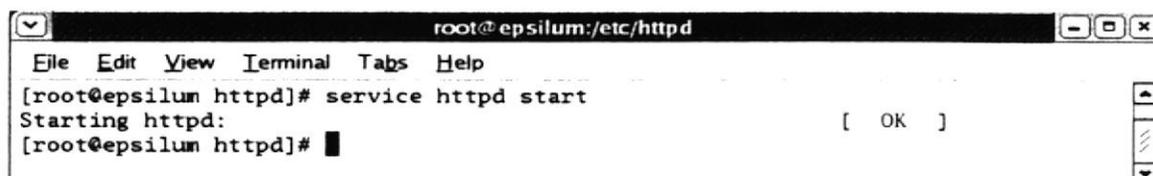
```
mkdir Epsilon (Crear la carpeta que va a contener sitio Web)
```

```
cd Epsilon (Ingresar a la carpeta que va a contener sitio Web)
```

*Copiar el archivo index.html que contiene la pagina web que se va a levantar por medio del Servidor Web, en la carpeta creada.*

*Iniciar el servicio httpd:*

```
service httpd start (Iniciar el servicio httpd)
```

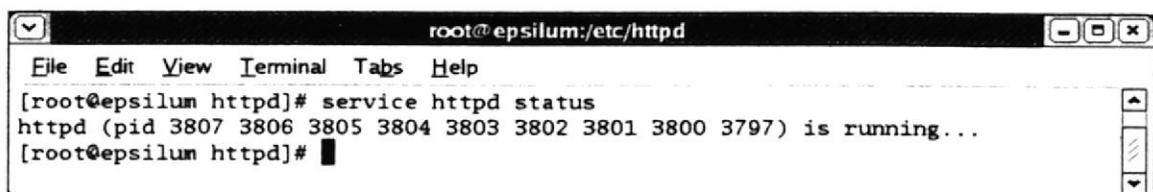


```
root@epsilon:/etc/httpd
File Edit View Terminal Tabs Help
[root@epsilon httpd]# service httpd start
Starting httpd:                                     [ OK ]
[root@epsilon httpd]# █
```

**Figura 6. 52.** Pantalla de iniciar el servicio httpd

*Verificar el estado del servicio HTTPD para ver si no hay ningún error en la configuración y comprobar que está funcionando correctamente.*

```
service httpd status (Verificar el estado del servicio httpd)
```



```
root@epsilon:/etc/httpd
File Edit View Terminal Tabs Help
[root@epsilon httpd]# service httpd status
httpd (pid 3807 3806 3805 3804 3803 3802 3801 3800 3797) is running...
[root@epsilon httpd]# █
```

**Figura 6. 53.** Pantalla del estatus del servicio httpd

### 6.9.9 CONFIGURACIÓN EN CLIENTE WINDOWS

1. Abrir Internet Explorer.



Figura 6. 54. Icono de Internet Explorer

2. Dirigirse al Menú Herramientas.

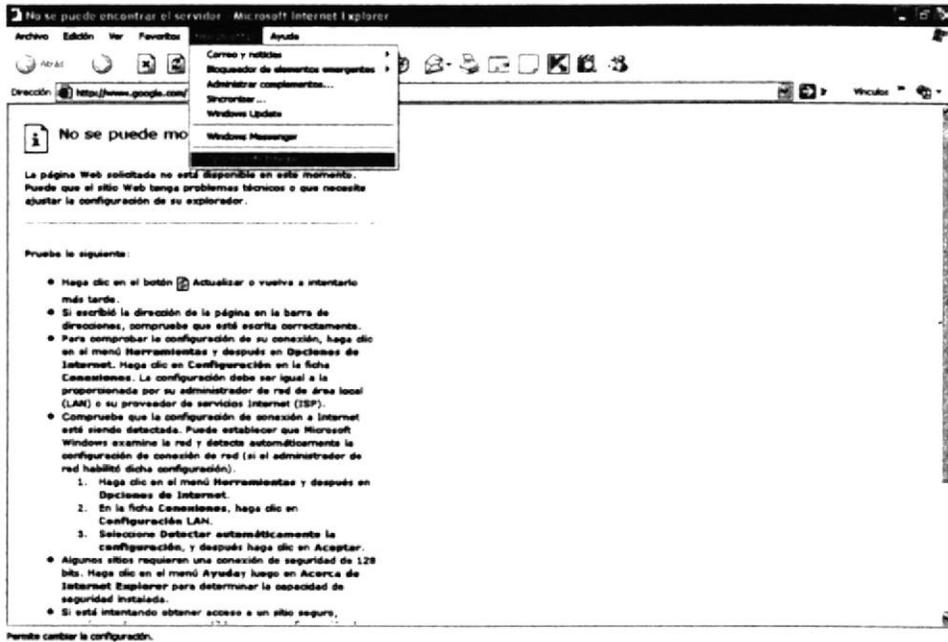


Figura 6. 55. Pantalla para configurar la navegación

3. Dar clic en Opciones de Internet.

4. Hacer clic en la pestaña Conexiones.



Figura 6. 56. Pantalla: Opciones de Internet



5. Ir al botón Configuración Lan Configuración de LAN...

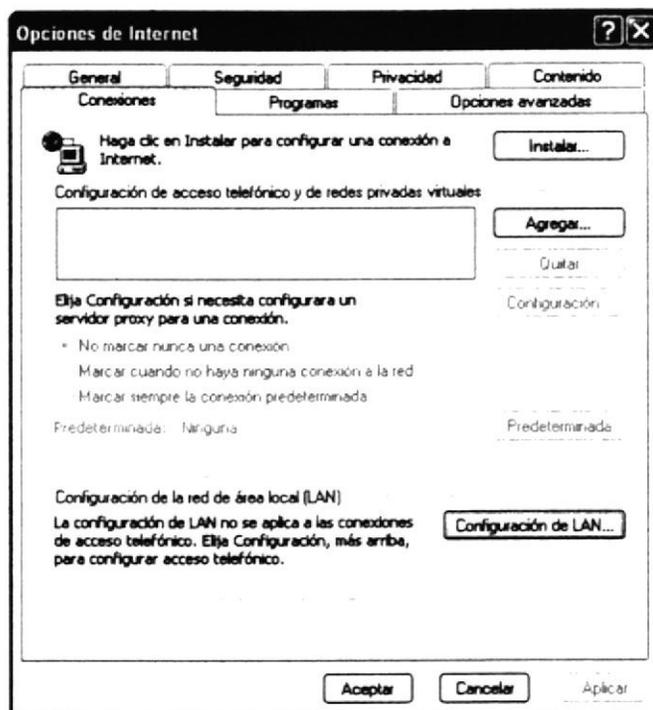


Figura 6. 57. Pantalla: Opciones de Internet

6. Detectar la configuración automáticamente.



Figura 6. 58. Pantalla: Configuración de la Red de Área Local

7. Acceder al sitio Web mediante el navegador. Recordar haber asignado la dirección DNS en la máquina Windows.

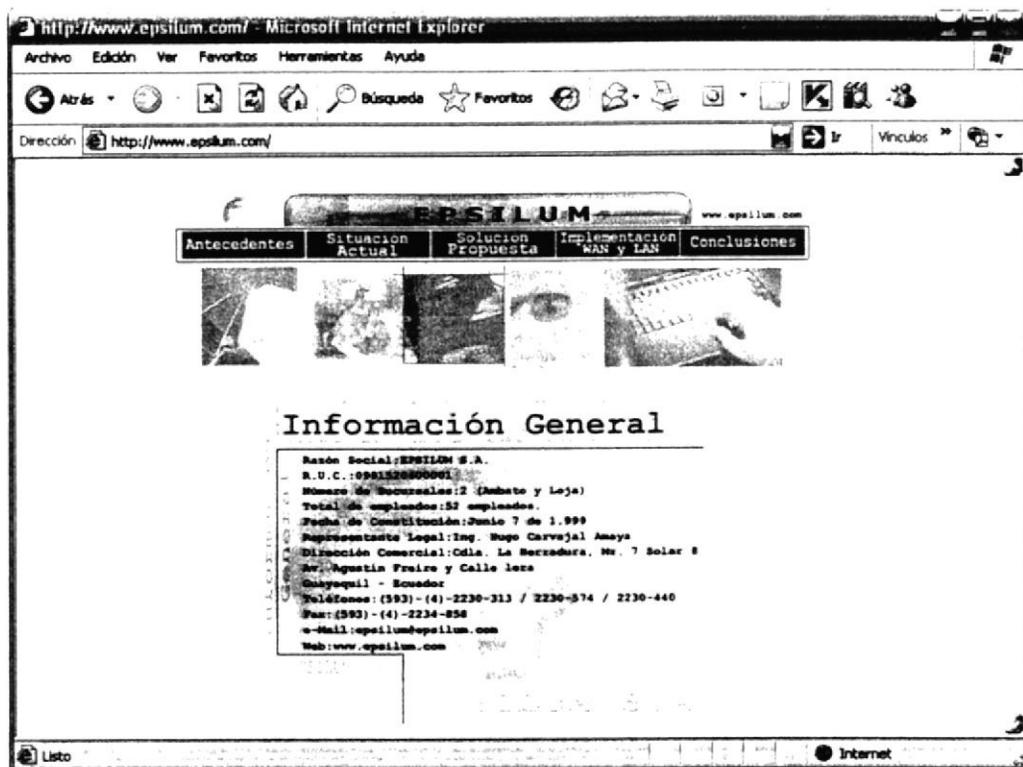


Figura 6. 59. Pantalla: Página Web de Epsilon

## 6.10 SERVIDOR PROXY

### 6.10.1 ACERCA DE PROXY

Un proxy es una aplicación o un dispositivo hardware que hace de intermediario entre los usuarios, normalmente de una red local, e Internet.

El término en inglés «Proxy» tiene un significado muy general y al mismo tiempo ambiguo, aunque invariablemente se considera un sinónimo del concepto de «Intermediario». Se suele traducir, en el sentido estricto, como delegado o apoderado (el que tiene el poder sobre otro).

Un Servidor Intermediario (Proxy) se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:

- Cliente se conecta hacia un Servidor Intermediario (Proxy).
- Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto.
- Servidor Intermediario (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.
- En algunos casos el Servidor Intermediario (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los Servidores Intermediarios (Proxies) generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el Nivel de Red, actuando como filtro de paquetes, como en el caso de iptables, o bien operando en el Nivel de Aplicación, controlando diversos servicios, como es el caso de TCP Wrapper. Dependiendo del contexto, el muro cortafuegos también se conoce como BPD o Border Protection Device o simplemente filtro de paquetes.

Una aplicación común de los Servidores Intermediarios (Proxies) es funcionar como caché de contenido de Red (principalmente HTTP), proporcionando en la proximidad de los clientes un caché de páginas y ficheros disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un URL (Uniform Resource Locator) el Servidor Intermediario busca el resultado del URL dentro del caché. Si éste es encontrado, el Servidor Intermediario responde al cliente proporcionando inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el Servidor Intermediario lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado a través de un algoritmo de expiración de acuerdo a la antigüedad,

tamaño e historial de respuestas a solicitudes (hits) (ejemplos: LRU, LFUDA y GDSF).

Los Servidores Intermediarios para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

Lo que hace realmente un proxy es recibir peticiones de usuarios y redirigirlas a Internet. La ventaja que presenta es que con una única conexión a Internet podrá conectar varios usuarios.

Normalmente, un proxy es a su vez un servidor de caché. La función de la caché es almacenar las páginas web a las que se accede más asiduamente en una memoria. Así cuando un usuario quiere acceder a Internet, lo hace a través del proxy, que mirará en la caché a ver si tiene la página a la cual quiere acceder el usuario. Si es así le devolverá la página de la caché y si no, será el proxy el que acceda a Internet, obtenga la página y la envíe al usuario. Con la caché se aceleran en gran medida los accesos a Internet, sobre todo si los usuarios suelen acceder a las mismas páginas.

Los últimos proxies que han aparecido en el mercado realizan además funciones de filtrado, como por ejemplo, dejar que un usuario determinado acceda a unas determinadas páginas de Internet o que no acceda a ninguna. Con esta función podrá configurar una red local en la que haya usuarios a los que se les permita salir a Internet, otros a los que se les permita enviar correo, pero no salir a Internet y otros que no tengan acceso a Internet. Esta característica muchas veces hace que se confundan con un cortafuego.

### 6.10.2 ACERCA DE SQUID.

Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo sustento lógico libre, está disponible el código fuente para quien así lo requiera.

Entre otras cosas, Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes. Al iniciar Squid da origen a un número configurable (5, de modo predefinido a través del parámetro `dns_children`) de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores DNS.

## 6.10.3 FUNCIONAMIENTO

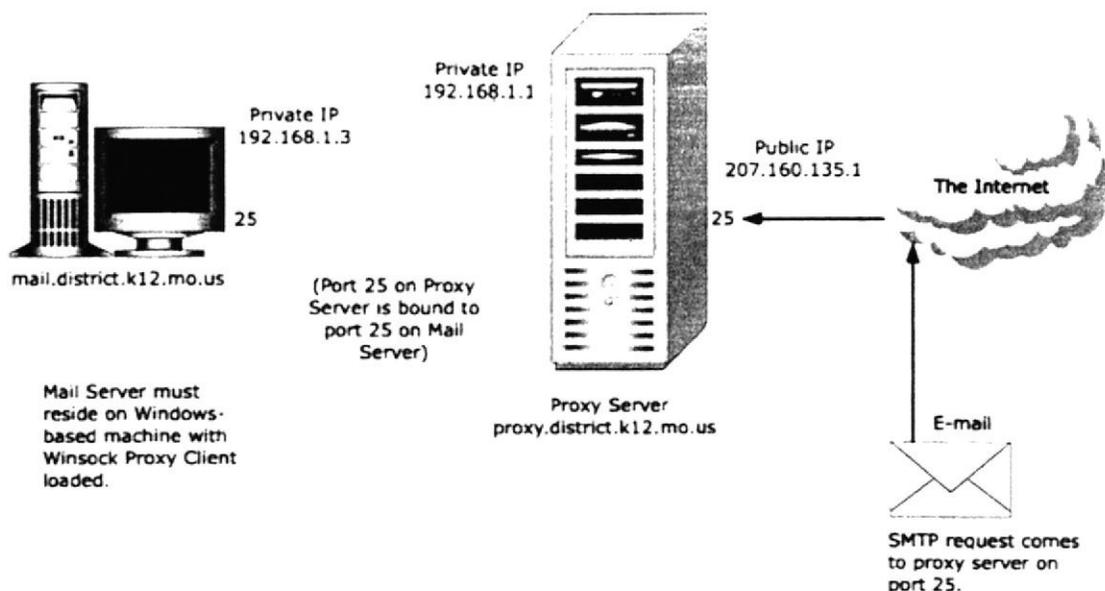


Figura 6. 60. Funcionamiento del Servidor Proxy

La función principal del servidor Proxy es distribuir Internet a los usuarios de una manera controlada, es decir con este servidor se pueden controlar el uso del Internet.

## 6.10.4 BENEFICIOS DEL SERVIDOR PROXY

- Acceso transparente a Internet, por medio de cualquier programa, y a cualquier servicio.
- Mayor velocidad en la navegación: aquellas páginas que hayan sido visitadas serán guardadas en el servidor para que no haya que solicitarlas de Internet salvo que hayan cambiado.
- Optimización de uno o varios accesos ADSL que disponga.
- Posibilidad de un control absoluto de los accesos a Internet, por fecha, hora, lugar, e incluso persona.
- Capacidad de control de Páginas prohibidas.

## 6.10.5 REQUERIMIENTOS PROXY

- Sistema operativo Linux Fedora Core 3.
- Tener instalado el paquete squid.
- Tener la tarjeta de red configurada con una IP estática.
  - IP Pública.
  - IP Privada.
- Deshabilitar los firewalls.

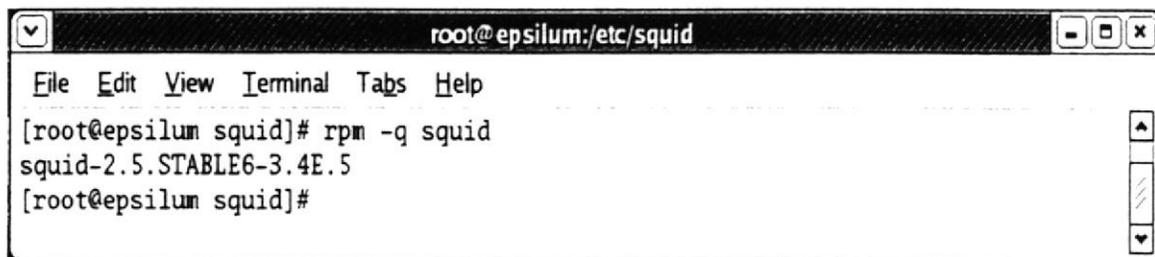
### 6.10.6 CONFIGURACIÓN DE PROXY:

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

Para configurar el servidor Proxy deberá verificar si el paquete squid está instalado, lo realiza de la siguiente manera:

**`rpm -q squid`** (verificar si está instalado el paquete squid).

- El fichero de configuración de SQUID se halla en `/etc/squid/squid.conf` y hay que editarlo para realizar los cambios adecuados y conseguir que cumpla su tarea con cierta seguridad para su sistema.
- Este fichero de configuración consta de multitud de parámetros configurables que ajustan el servidor a sus necesidades. Tratará de reflejar aquellos indispensables para un óptimo funcionamiento.



```

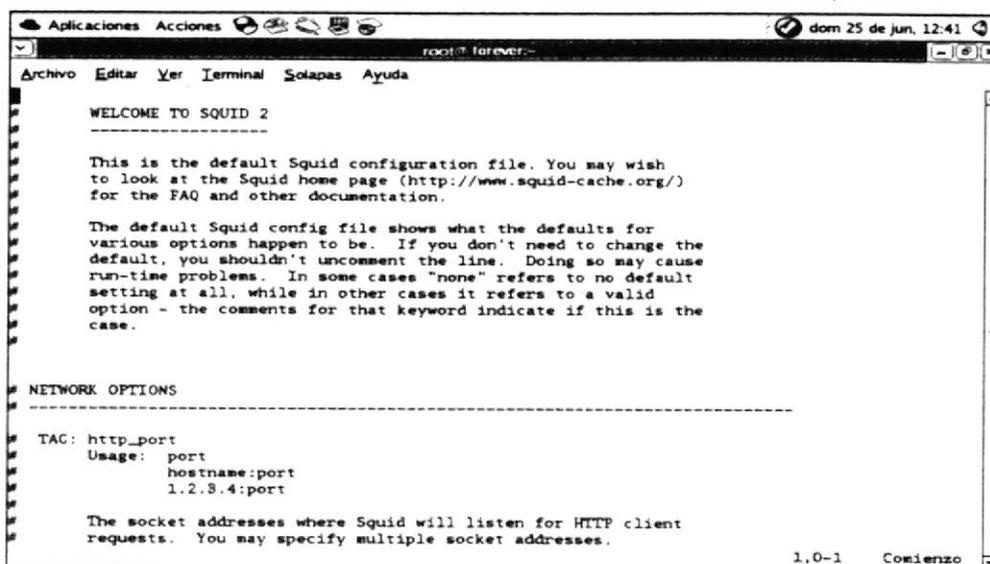
root@epsilon:/etc/squid
File Edit View Terminal Tabs Help
[root@epsilon squid]# rpm -q squid
squid-2.5.STABLE6-3.4E.5
[root@epsilon squid]#
  
```

Figura 6. 61. Pantalla para verificar si está instalado el paquete squid

Luego ingresara al archivo de configuración **squid.conf**. El cual se encuentra en la siguiente ruta:

**`vi /etc/squid/squid.conf`** (Ruta de archivo squid)

- Squid utiliza el fichero de configuración localizado en `/etc/squid/squid.conf`, y podrá trabajar sobre este utilizando su editor de texto preferido.



```

Aplicaciones Acciones root@forever:~
dom 25 de jun, 12:41
Archivo Editar Ver Terminal Solapas Ayuda
-----
WELCOME TO SQUID 2

This is the default Squid configuration file. You may wish
to look at the Squid home page (http://www.squid-cache.org/)
for the FAQ and other documentation.

The default Squid config file shows what the defaults for
various options happen to be. If you don't need to change the
default, you shouldn't uncomment the line. Doing so may cause
run-time problems. In some cases "none" refers to no default
setting at all, while in other cases it refers to a valid
option - the comments for that keyword indicate if this is the
case.

NETWORK OPTIONS
-----
TAC: http_port
Usage: port
hostname:port
1.2.3.4:port

The socket addresses where Squid will listen for HTTP client
requests. You may specify multiple socket addresses.

1,0-1 Comienzo
  
```

Figura 6. 62. Pantalla de configuración de archivo squid.conf

Efectuar varios cambios dentro de esté archivo.

**http\_port 8080**

# Línea 53

- Permite especificar uno o varios puertos de escucha para el servidor Squid.(El puerto por defecto es 3128, pero por cuestiones de seguridad cambiar al puerto 8080. El puerto no necesariamente el 8080, puede ser cualquier puerto que no este siendo usado)

**cache\_mem 16 MB**

# Línea 480

- Permite indicar la cantidad ideal de memoria RAM como máximo para almacenar caché de objetos en tránsito, objetos Hot y objetos negativamente almacenados en la caché.
- Los datos de estos objetos se almacenan en bloques de 4KB.
- Cache\_mem especifica un limite ideal en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad, es decir que el resto de objetos la podrán usar hasta que sea requerida.
- (Establece la cantidad de memoria para objetos en tránsito, objetos host y objetos navegantes almacenados en caché)

**cache\_dir ufs /var/spool/squid 6000 16 256**

# Línea 695

- Permite indicar la cantidad de memoria física máxima para almacenar caché en el disco duro, es decir cuanto espacio almacenar de objetos de Internet. Sus valores pueden ser: tipo directorio tamaño numero\_subdir numero\_niveles, tal como se muestra a continuación.
- El numero 6000 corresponde a 6000MB como espacio máximo para almacenar caché, el 16 son el numero de subdirectorios que contendrá el directorio principal (en este caso /var/spool/squid) y el 256 significa el numero de niveles para cada subdirectorio. En caso de especificar un tamaño máximo inferior al espacio real disponible, el servidor Squid se bloqueará.

**cache\_access\_log /var/log/squid/access\_log**

# Línea 703

- Permite definir en que fichero Squid debe guardar una lista de las peticiones que va recibiendo, con la información de la página que se ha consultado y si ésta ha sido facilitada desde la caché o desde el servidor web
- Monitorear la actividad de los hosts que tenga a cargo el Proxy.
- Estas líneas tienen que descomentarlas.

**Luego se agrega a la siguiente línea la palabra Epsilon.**

**Visible\_hostname Epsilon**

- (Agregue la siguiente sintaxis para designarle el nombre de su servidor en el SQUID)

Realizar los cambios anteriormente mencionados, salir y grabar.

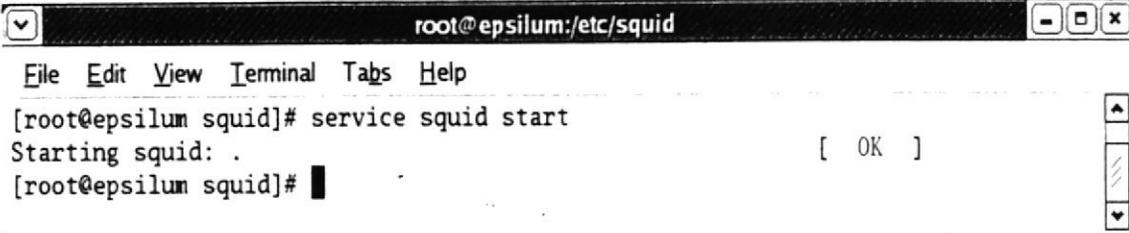
**Esc** (Salir de modo de edición)

**: wq** (Grabar y salir)

Iniciar el servicio. Si está bien la configuración no debe salir ningún mensaje, caso contrario ocurre un error.

**service squid start**

(Iniciar el servicio)



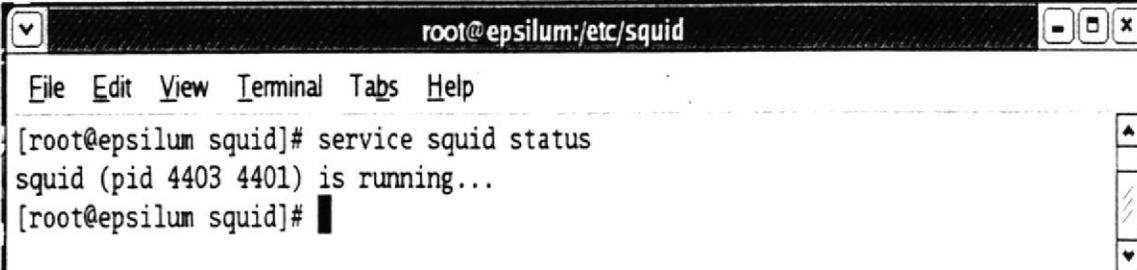
```
root@epsilon:/etc/squid
File Edit View Terminal Tabs Help
[root@epsilon squid]# service squid start
Starting squid: . [ OK ]
[root@epsilon squid]#
```

Figura 6. 63. Pantalla para iniciar el servicio squid

Luego realizará un status para ver si no hay ningún error en la configuración.

**service squid status**

(Verificar el estado del servicio)



```
root@epsilon:/etc/squid
File Edit View Terminal Tabs Help
[root@epsilon squid]# service squid status
squid (pid 4403 4401) is running...
[root@epsilon squid]#
```

Figura 6. 64. Pantalla de status del servicio squid

### 6.10.7 ACL (ACCESS CONTROL LIST – LISTA DE CONTROL DE ACCESO)

Es necesario establecer **Listas de Control de Acceso** que definan una red o bien ciertas máquinas en particular. A cada lista se le asignará una **Regla de Control de Acceso** que permitirá o denegará el acceso a **Squid**.

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

```
acl [nombre de la lista] src [lo que compone a la lista]
```

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 192.168.1.n con máscara de sub-red 255.255.255.0, podrá utilizar lo siguiente:

```
acl red_epsilon src 192.198.0.0/255.255.255.0
```

(Línea que permite la navegación para toda la red)

Si uno desea establecer una lista de control de acceso que defina a toda la red local se define la IP que corresponde a la red y la máscara de la sub-red.

Deberá especificar porque puerto va a navegar, teniendo en cuenta que las acl manejan rangos, los cuales se detallaran a continuación.

```
acl name port 0 – 1024...
```

Port acepta desde el puerto 0 al 1024

```
acl name myport 3128.....
```

Myport acepta desde el 3128 en adelante

En este caso necesitará el puerto 8080 y utilizará la sintaxis **myport**.

```
acl puerto myport 8080
```

(Línea que permite la navegación por el puerto 8080)

La regla **http\_access allow** permite el acceso a **Squid** a la **Lista de Control de Acceso** denominada **red\_epsilon**, la cual está conformada por las direcciones IP especificadas anteriormente por el puerto 8080. Esto significa que cualquier máquina no incluida en **/etc/squid/red\_epsilon** no tendrá acceso a **Squid**

```
http_access allow red_epsilon puerto
```

(En esta línea se define que toda la red\_epsilon puede salir por el puerto 8080)

Luego de haber realizado todos los cambios, salir y grabar.

```
Esc (Salir de modo de edición)
```

```
:wq (grabar y salir)
```

## 6.10.8 CONFIGURACIÓN EN CLIENTE WINDOWS

## 1. Abrir Internet Explorer.



Figura 6. 65. Icono de Internet Explorer

## 2. Dirigirse al Menú Herramientas.

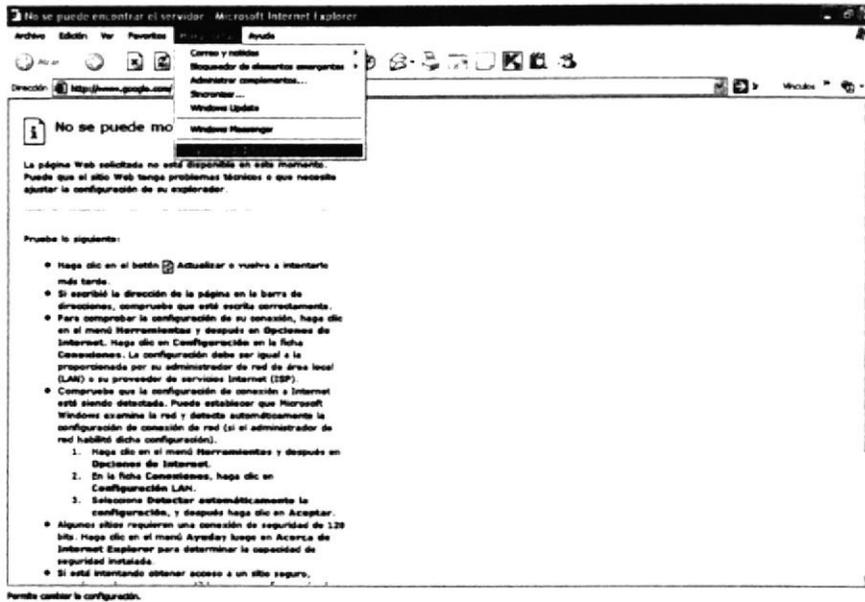


Figura 6. 66. Pantalla para configurar la navegación

## 3. Dar clic a la pestaña Opciones de Internet.

## 4. Hacer clic en la pestaña Conexiones

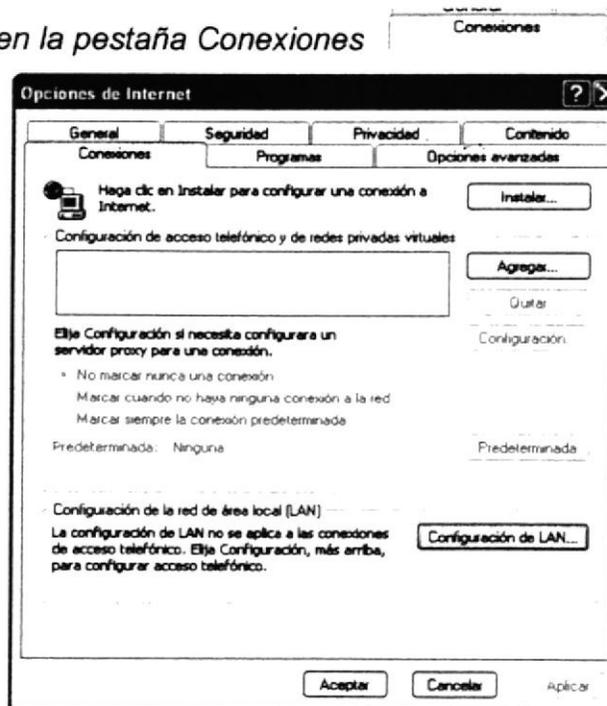


Figura 6. 67. Pantalla: Opciones de Internet

8. Ir al botón **Configuración Lan** Configuración de LAN...

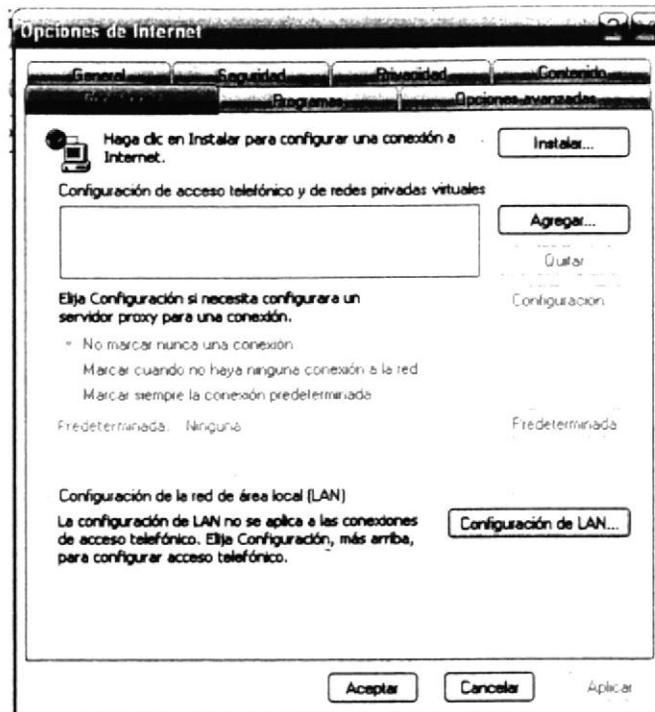


Figura 6. 68. Pantalla Opciones de Internet

5. Seleccionar **utilizar servidor Proxy** y colocar IP del servidor **Puerto 8080**.

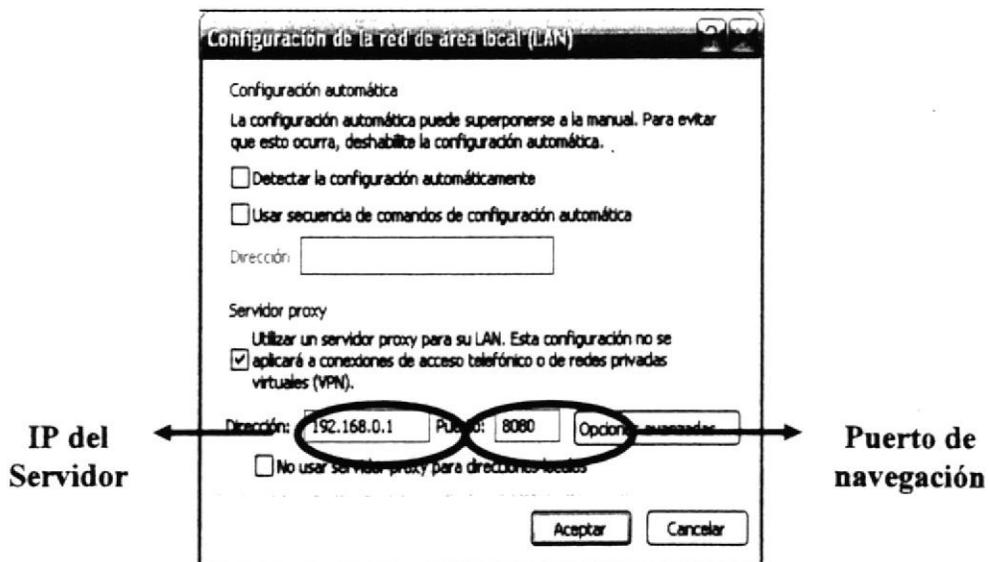


Figura 6. 69. Pantalla de configuración de la Red de área local (LAN)

6. Luego ir al navegador en el Internet Explorer y cargar la página.

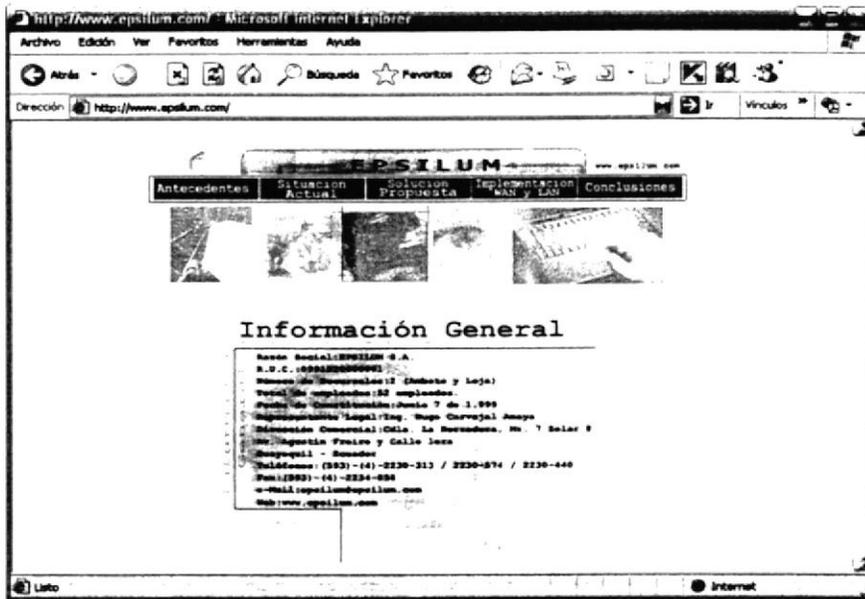


Figura 6. 70. Pantalla: Página accesada por medio de Proxy creada por web server

### 6.10.9 DENEGAR ACCESO POR HORA

Denegar el acceso a ciertos en ciertos horarios, permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso en horarios y días de la semana.

La sintaxis para crear Listas de control de acceso que definan horarios es la siguiente:

**acl** [nombre del horario] **time** [días de la semana] hh:mm-hh:mm



#### Importante

Los días están determinados de la siguiente manera:

Lunes	M
Martes	T
Miércoles	W
Jueves	H
Viernes	F
Sábado	A
Domingo	S

La hora de inicio y fin deben ser asignados en formato 24:00  
Procederá a crear la acl para denegar el acceso por horario.

**acl nombre time día hora inicio – hora fin**

(Línea que permite definir la acl con su(s) día(s) y sus respectivas horas)

**acl tarde time M 13:00 – 16:00**

(Esta regla define a la lista *tarde* que permite la navegación del día Lunes de 13:00 a 16:00)

Luego tendrá que definir la IP que se le restrinja o autorice la navegación.

**acl clientes src 192.168.0.4**

Lista de Control de Acceso denominada clientes, la cual está conformada por la dirección IP 192.168.0.4.

La regla **http\_access deny denny** deniega el acceso a **Squid** a la **Lista de Control de Acceso** denominada **clientes** en el horario definido por la **acl tarde**.

**http\_access deny clientes tarde**

(En esta línea se define que la IP 192.168.0.4 no puede navegar los Lunes de 13:00 a 16:00)

Después se actualiza el servicio del squid.

**service squid reload** (Actualiza el servicio del squid)

### 6.10.10 ACCESO POR AUTENTIFICACIÓN

Se requerirá la creación previa de un fichero que contendrá los nombres de usuarios y sus correspondientes claves de acceso (cifradas). El fichero puede localizarse en cualquier lugar del sistema, con la única condición que sea asequible para el usuario squid.

#### **touch /etc/squid/claves**

(Crear el archivo de claves)



#### **Importante**

El comando **touch** no está orientado a la creación de archivos sino a la actualización de la hora de acceso y modificación de los archivos. Sin embargo, uno de sus efectos secundarios es crear los archivos que se mencionan si es que ya no existen.

Salvo que vaya a utilizarse un guión a través del servidor web para administrar las claves de acceso, como medida de seguridad, este fichero debe hacerse *leíble y escribible sólo para el usuario squid*:

#### **chmod 600 /etc/squid/claves**

(Cambiar permisos de lectura y escritura al archivo claves)



#### **Importante**

El comando **chmod** cambia los permisos sobre los archivos y directorios. Se puede especificar de la siguiente manera:

- En octal; entonces los derechos del usuario dueño se corresponden a números de la forma  $\langle x \rangle 00$ , donde  $\langle x \rangle$  corresponde al permiso asignado: 4 para lectura, 2 para escritura, y 1 para ejecución; similarmente, los derechos del grupo propietario toman la forma  $\langle x \rangle 0$  y los derechos de los «**otros**» la forma  $\langle x \rangle$ . Por lo tanto, todo lo que Ud. necesita hacer es sumar los derechos asignados para obtener el número correcto. Así, los derechos **rwX** corresponden a  $400+200+100$  (derechos del dueño, **rwX**).

Luego cambiar de propietario al archivo "**claves**", usando el comando **chown** el cual permitirá asignar al archivo al usuario squid para claves de autenticación.

#### **chown squid:squid /etc/squid/claves**

(Cambiar de propietario el archivo claves)



#### **Importante**

El mandato **chown** se utiliza para cambiar el propietario al que pertenece un fichero o directorio. Puede especificarse tanto el nombre de un usuario, así como un número de identidad de usuario (**UID**). Opcionalmente, utilizando un signo de dos puntos (:), o bien un punto (.), permite especificar también un nombre de grupo.

A continuación deberá crear las cuentas que sean necesarias, utilizando el mandato `htpasswd` el mismo que viene incluido en el paquete `httpd-2.0.x-`. Ejemplo:

```
htpasswd /etc/squid/claves dzambano
```

(Asignar una clave al archivo)

Lo anterior solicitará teclear una nueva clave de acceso para el usuario `dzambano` y confirmar tecleando ésta de nuevo. Repita con el resto de las cuentas que requiera crear.



#### Importante

Todas las cuentas que se crean por medio del comando `htpasswd` son independientes a las ya existentes en el sistema. Al crear una cuenta o cambiar una clave de acceso lo estará haciendo **EXCLUSIVAMENTE** para el acceso al servidor Proxy. Las cuentas son independientes a las que se tengan existentes en el sistema como serían `shell`, correo y Samba.

Lo siguiente, será especificar que programa de autenticación se utilizará. Localice la sección que corresponde a la etiqueta `auth_param basic program`. Por defecto no está especificado programa alguno. Considerando que `ncsa_auth` se localiza en `/usr/lib/squid/ncsa_auth`, procederá a añadir el siguiente parámetro:

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves
```

(En la línea 1093 modifique esta ruta).

- `/usr/lib/squid/ncsa_auth` corresponde a la localización de el programa para autenticar.
- `/etc/squid/claves` al fichero que contiene las cuentas y sus claves de acceso.

El siguiente paso corresponde a la definición de una Lista de Control de Acceso. Se especifica una denominada `password` la cual se configurará para utilizar obligatoriamente la autenticación para acceder a `Squid`. Debe localizarse la sección de Listas de Control de Acceso y añadirse la siguiente línea:

```
acl password proxy_auth REQUIRED
```

(Línea que permite la autenticación)

Procederá entonces a modificar la regla de control de accesos que ya tenía para permitir el acceso a Internet. Le añadirá `password`, la definición de la Lista de Control de Acceso que requiere utilizar clave de acceso, a su regla actual, de modo que quede como se muestra a continuación:

```
http access_allow red_epsilon password
```

(Control de acceso a la red por password)

Después se actualiza el servicio `squid` digitando la siguiente línea.

```
service squid reload (Actualiza el servicio del squid)
```

### 6.10.10.1 CONFIGURACIÓN EN CLIENTE WINDOWS

1. Abrir Internet Explorer.



Internet Explorer

Figura 6. 71. Icono de Internet Explorer

2. Automáticamente aparecerá la ventana de autenticación de usuario.

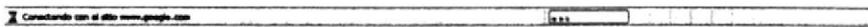
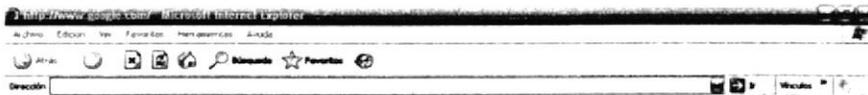


Figura 6. 72. Pantalla: Autenticación de usuario

3. Ingresar el nombre de usuario con su respectiva contraseña.



Figura 6. 73. Pantalla: Ingresando usuario y contraseña

4. Luego podrá tener acceso al Internet.



Figura 6. 74. Pantalla: Accediendo al Internet por medio de autenticación de usuario.

### 6.10.11 BLOQUEAR PÁGINAS

Deberá definir una Lista de Control de Acceso que a su vez defina al fichero `/etc/squid/prohibidos`. Esta lista se la denominara como "prohibidos". De modo que, la línea correspondiente quedaría del siguiente modo.

**`acl prohibidos url_regex -i"/etc/squid/prohibidos"`**

(Creada la acl establezca la ruta del archivo donde se encontrará sus sitios prohibidos).

Luego en el archivo `squid.conf` agregara una nueva línea de control del acceso, la cual establecerá las nuevas restricciones.

**`http access_deny prohibidos`**

A continuación se especificará una Lista de Control de Acceso en la cuál se denegará el acceso a los sitios especificados en la Lista de Control de Acceso denominada prohibidos.

Es importante crear el archivo donde establecerá los sitios que se van a excluir, el mismo deberá estar creado en la siguiente ruta `"/etc/squid/"` caso contrario la lista de acceso no funcionara, dentro del archivos **prohibidos** se colocara las paginas que no desea que utilicen los empleados.

En el archivo "prohibidos" solo se escribe el url como en el navegador.

**`www.hi5.com`**

**`www.hotmail.com`**



**Ejemplo:**

Lo primero será generar una lista la cual contendrá direcciones Web y palabras usualmente utilizadas en nombres de ciertos dominios.

- \.avi\$
- \.mp4\$
- \.mp3\$
- \.mp4\$
- \.mpg\$
- \.mpeg\$
- \.mov\$
- \.ra\$
- \.rm\$
- \.rpm\$
- www.hotmail.com
- www.hi5.com

Esta lista, deberá ser completada con todas las extensiones de fichero que el administrador considere pertinentes, la guardara como `/etc/squid/prohibidos`.

Después se actualiza el servicio squid digitando la siguiente línea.

**`service squid reload`** (Actualiza el servicio del squid)

### 6.10.11.1 CONFIGURACIÓN EN CLIENTE WINDOWS

1. Abrir Internet Explorer.



Figura 6. 75. Icono de Internet Explorer

2. Digitará la página www.hi5.com.

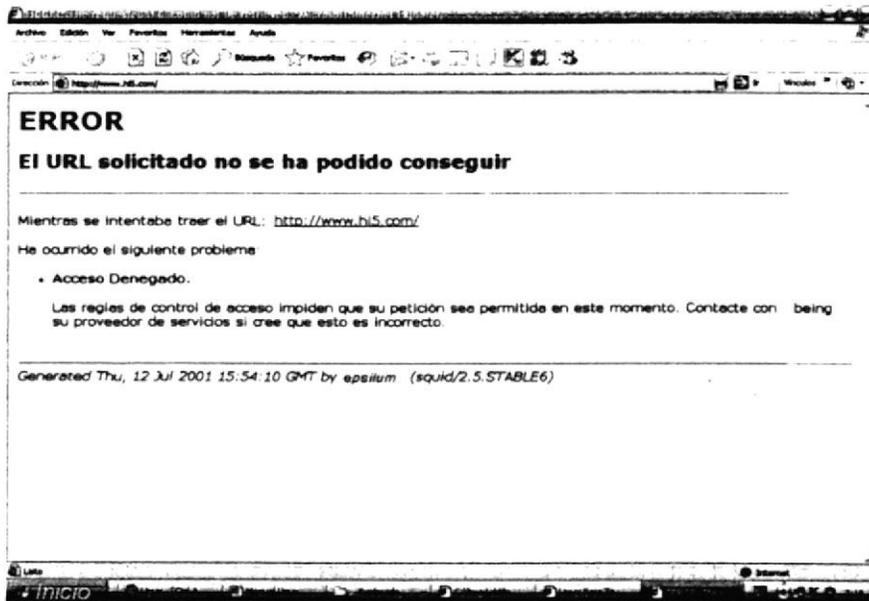


Figura 6. 76. Pantalla de acceso denegado al dominio.

### 6.10.12 ANCHO DE BANDA

Los Delay Pools son la herramienta para llevar a cabo el control de ancho de banda del Proxy.

#### 6.10.12.1 DEFINICIÓN DE DELAY POOLS

La cantidad de Delays Pools a emplear se define con la directiva `delay_pools`.

##### **Sintaxis:**

- `delay_pools N`

donde  $N > 0$  representa la cantidad de Delay Pools a usar.

##### **Ejemplo:**

- `delay_pools 3`

Con esto se le dice a Squid que se van a usar y definir tres Delay Pools.

Existen tres clases de Delay Pool lo que permite tener cierta flexibilidad en su uso.

#### 6.10.12.2 CLASES DE DELAY POOLS

En Squid existen tres clases de Delay Pool.

##### 6.10.12.2.1 CLASE 1

El Delay Pool clase 1 define una única estructura de control. Este limita el uso del canal de manera global sin importar cómo lo usan los clientes internamente o cómo esta definida lógicamente la LAN. Esta es la opción indicada si usted desea limitar el ancho de banda que usa Squid, sin importar cómo lo emplean los usuarios.

##### 6.10.12.2.2 CLASE 2

Este es un Delay clase 1 con un 256 Delay Pools clase 1 subordinados a este. Con este Delay es posible controlar el canal que usan 256 clientes.

Cuando se asigna el canal a cada cliente Squid asume que su LAN es de clase C y usa los últimos 8 bits del número IP del cliente para identificarlo y manejarlo en su individual bucket correspondiente. En la práctica solo se pueden controlar 253 clientes descontando la dirección de red, la dirección de broadcast y la dirección del proxy.

### 6.10.12.2.3 CLASE 3

Este es un Delay Pool clase 1 con 256 Delay Pools clase 2 subordinados a este. Está orientado para manejar la asignación de ancho de banda en redes clase B. los bits 17 a 24 del número IP identifican la red y los bits 17 a 32 el cliente.

La clase del Delay Pool se especifica con la directiva `delay_class`.

**Syntaxis:**

- `delay_class id class`

donde  $id > 0$ ,  $class = [1|2|3]$ ;  $id$  es el identificador y  $class$  la clase

**Ejemplo:**

- `delay_class 1 3 ##` el Delay Pool número 1 será clase 3
- `delay_class 2 1 ##` el Delay Pool número 2 será clase 1
- `delay_class 3 2 ##` el Delay Pool número 3 será clase 2

Los Delay Pools no tienen nombre, se identifican con un número que empieza en 1 y termina en N.

### 6.10.12.3 PARÁMETROS DEL DELAY POOL

Los parámetros de cada Delay Pool se definen por medio de la directiva `delay_parameters`:

**Sintaxis:**

`delay_parameters id rate/size [rate/size [rate/size]]`

Los valores de `rate` y `size` son dados en Bytes. Por ende no olvide hacer la conversión respectiva de Kbits como le venden el canal a Bytes. `size` es dos o tres veces el valor de `rate`.

**Ejemplos:**

`delay_parameters 1 76800/230400 42800/100000 10000/70000`

Un Delay clase 3 con 600Kb/s (76800B/s) en total para navegación, con un tamaño para ráfagas (burst) globales de 1800Kb (230400Bytes). Para cada subred se asigna un canal máximo de 334.3Kb/s un tamaño para ráfagas de 781.2Kb (100000Bytes) con un ancho de banda para cada host de 78.1Kb/s (10000B/s) con la posibilidad de ráfagas de descargas de 546.8Kb (70000Bytes). Note que los valores para cada subred y host exceden los límites de canal disponible si hay más de 4 clientes navegando en una subred o dos

subredes demandan todo el canal asignado. En este caso se produce una condición de competencia y el primero que solicita el canal es el que lo obtiene. Es de suponer que esta asignación es para una organización con usuarios que navegan poco y requieren un buen desempeño al momento de solicitar un archivo. Este es un buen ejemplo de cómo se puede jugar con los parámetros del Delay Pool teniendo en cuenta las costumbres de navegación de la organización.

```
delay_parameters 1 76800/230400
```

Un Delay clase 1. Se usan máximo 600Kb/s de ancho de banda con ráfagas de descarga de 1800Kb. Solo se limita el ancho de banda que usa en total sin importar cómo se distribuye el canal entre los clientes, lo cual da la posibilidad a condiciones de competencia por el ancho de banda en todo momento.

```
delay_parameters 1 340787/1022361 10000/200000
```

Un Delay clase 2. Define que se usarán máximo 2.6Mb/s para navegación con ráfagas de 7.8Mb para una asignación de canal a máximo 256 clientes de 78.1Kb/s con ráfagas de descarga de 195.3Kb (esto es, pueden descargar 195.3Kb a todo lo que de el canal si tienen el individual bucket lleno). Este montaje es para una organización cuyos usuarios demandan una gran cantidad de canal. Aquí el peor caso se presenta cuando hay 34 clientes demandando todo el canal asignado de forma continua.

En los Delay Pools clase 2 y clase 3 es posible deshabilitar los buckets que no se desea utilizar colocando -1/-1 en el bucket correspondiente. Por ejemplo:

# asigno el canal a hosts en una red clase C sin límite global

```
delay_parameters 1 -1/-1 10000/200000
```

# asigno canal en una red clase B a hosts individuales sin límites por subred

```
delay_parameters 2 340787/1022361 -1/-1 10000/200000
```

# asigno canal en una red clase B a cada su red sin importar los hosts

```
delay_parameters 3 340787/1022361 10000/200000 -1/-1
```

#### 6.10.12.4 DELAY\_ACCESS

Definen por medio de acl's cuáles peticiones pasan por el Delay y cuáles no. Ver los ejemplos.

##### Sintaxis:

```
delay_access id allow acl name | deny acl name
```

## 6.11 SERVIDOR DE CORREO

### 6.11.1 ACERCA DE SENDMAIL

*Es el más popular agente de transporte de correo (MTA o Mail Transport Agent), responsable quizá de poco más del 70% del correo electrónico del mundo. Aunque por largo tiempo se le ha criticado por muchos incidentes de seguridad, lo cierto es que éstos siempre han sido resueltos en pocas horas.*

*El servicio de transferencia de correo electrónico entre máquinas pertenecientes a Internet es de los más antiguos que se vienen ofreciendo en la historia de esta gran red. También es, quizás, el más representativo de la filosofía cliente servidor dentro de la extensa familia de protocolos TCP/IP.*

*El servicio de correo electrónico permite llevar a cabo el envío y recepción de mensajes con usuarios de otros ordenadores de la red. El modo más sencillo de implementar este servicio es mantener ficheros de correo, llamados buzones, en cada uno de los sistemas en los que se pretende intercambiar mensajes con alguno de sus usuarios. Este sistema se basa en un método que permite añadir un mensaje a esos ficheros, o bien recuperarlos.*

*El servicio encargado de proporcionar el intercambio de correo electrónico entre las máquinas se denomina servicio de e-mail, y puede ser ofrecido por distintos programas daemon, de los que el más extendido se llama "sendmail".*

*El daemon sendmail es el servidor de correo electrónico más popular entre las máquinas de Internet. También se conoce con el nombre de "delivery", o bien distribuidor de correo. Realiza su función manteniéndose a la espera del puerto 25, comunicándose con los daemons de otros sistemas para recibir el correo entrante y enviar el correo saliente.*

### 6.11.2 ACERCA DE DOVECOT.

*Dovecot es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo.*

*Dovecot puede utilizar tanto el formato mbox como maildir y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.*

### 6.11.3 PROTOCOLOS UTILIZADOS.

#### 6.11.3.1 SMTP (SIMPLE MAIL TRANSFER PROTOCOL).

Es un **protocolo estándar** de Internet del **Nivel de Aplicación** utilizado para la transmisión de correo electrónico a través de una conexión TCP/IP. Este es de hecho el único protocolo utilizado para la transmisión de correo electrónico a través de Internet. Es un protocolo basado sobre texto y relativamente simple donde se especifican uno más destinatarios en un mensaje que es transferido. A lo largo de los años han sido muchas las personas que han editado o contribuido a las especificaciones de **SMTP**, entre las cuales están Jon Postel, Eric Allman, Dave Crocker, Ned Freed, Randall Gellens, John Klensin y Keith Moore.

Para determinar el servidor **SMTP** para un dominio dado, se utilizan los registros **MX (Mail Exchanger)** en la Zona de Autoridad correspondiente a ese mismo dominio contestado por un **Servidor DNS**. Después de establecerse una conexión entre el remitente (el cliente) y el destinatario (el servidor), se inicia una sesión **SMTP**, ejemplificada a continuación.

```
Cliente: $ telnet 127.0.0.1 25
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sat, 18 Mar 2006 16:02:27 -
          0600
Cliente: HELO localhost.localdomain
Servidor: 250 nombre.dominio Hello localhost.localdomain [127.0.0.1], pleased to meet you
Cliente: MAIL FROM:<fulano@localhost.localdomain>
Servidor: 250 2.1.0 <fulano@localhost.localdomain>... Sender ok
Cliente: RCPT TO:<root@localhost.localdomain>
Servidor: 250 2.1.5 <root@localhost.localdomain>... Recipient ok
Cliente: DATA
Servidor: 354 Enter mail, end with "." on a line by itself
Cliente: Subject: Mensaje de prueba
          From: fulano@localhost.localdomain
          To: root@localhost.localdomain

          Hola. Este es un mensaje de prueba.

          Adios.
          .
Servidor: 250 2.0.0 k2IM2RjA003987 Message accepted for delivery
Cliente: QUIT
Servidor: 221 2.0.0 nombre.dominio closing connection
Servidor: Connection closed by foreign host.
```

**SMTP** trabaja sobre **TCP** en el puerto 25.

### 6.11.3.2 POP3 (POST OFFICE PROTOCOL VERSION 3).

Es un **protocolo estándar** de Internet del **Nivel de Aplicación** que recupera el correo electrónico desde un servidor remoto a través de una conexión TCP/IP desde un cliente local. El diseño de **POP3** y sus predecesores es permitir a los usuarios recuperar el correo electrónico al estar conectado hacia una red y manipular los mensajes recuperados sin necesidad de permanecer conectados. A pesar de que muchos clientes de correo electrónico incluyen soporte para dejar el correo en el servidor, todos los clientes de POP3 recuperan todos los mensajes y los almacenan como **mensajes nuevos** en la computadora o anfitrión utilizado por el usuario, eliminan los mensajes en el servidor y terminan la conexión.

Después de establecerse una conexión entre el cliente y el servidor, se inicia una sesión **POP3**, ejemplificada a continuación.

```

Cliente: $ telnet 127.0.0.1 110
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^'.
          +OK dovecot ready.

  Cliente: USER fulano
  Servidor: +OK
  Cliente: PASS clave de acceso
  Servidor: +OK Logged in.
  Cliente: STAT
  Servidor: +OK 1 728
  Cliente: LIST
  Servidor: +OK 1 messages:
          1 728
          .

  Cliente: RETR 1
  Servidor: +OK 728 octets
          Return-Path: <fulano@localhost.localdomain>
          Received: from localhost.localdomain (localhost.localdomain [192.168.1.254])
            by localhost.localdomain (8.13.1/8.13.1) with SMTP id k2IM2RjA003987
            for <root@localhost.localdomain>; Sat, 18 Mar 2006 16:03:21 -0600
          Date: Sat, 18 Mar 2006 16:02:27 -0600
          Message-Id: <200603182203.k2IM2RjA003987@localhost.localdomain>
          Subject: Mensaje de prueba
          From: fulano@localhost.localdomain
          To: root@localhost.localdomain
          Status: O
          Content-Length: 43
          Lines: 2
          X-UID: 202
          X-Keywords:

          Hola. Este es un mensaje de prueba.
          Adios.
          .

  Cliente: QUIT
  Servidor: +OK Logging out.
          Connection closed by foreign host.

```

**POP3** trabaja sobre **TCP** en el puerto 110.

### 6.11.3.3 IMAP (INTERNET MESSAGE ACCESS PROTOCOL).

Es un **protocolo estándar** de Internet del **Nivel de Aplicación** utilizado para acceder hacia el correo electrónico en un servidor remoto a través de una conexión TCP/IP desde un cliente local.

**IMAP** trabaja sobre **TCP** en el puerto 143.

Fue diseñado por Mark Crispin en 1986 como una alternativa más moderna que cubriera las deficiencias de **POP3**. Las características más importantes de **IMAP** incluyen:

- Soporte para los modos de operación conectado (connected) y desconectado (disconnected), permitiendo a los clientes de correo electrónico permanezcan conectados el tiempo que su interfaz permanezca activa, descargando los mensajes conforme se necesite.
- A diferencia de **POP3**, permite accesos simultáneos desde múltiples clientes y proporciona los mecanismos necesarios para éstos para que se detecten los cambios hechos por otro cliente de correo electrónico concurrentemente conectado en el mismo buzón de correo.
- Permite a los clientes obtener individualmente cualquier parte **MIME** (acrónimo de **Multi-Purpose Internet Mail Extensions** o Extensiones de correo de Internet de propósitos múltiples), así como también obtener porciones de las partes individuales o bien los mensajes completos.
- A través de **banderas** definidas en el protocolo, vigilar la información de estado de los mensajes de correo electrónico que se mantengan en el servidor. Por ejemplo si el estado del mensaje es **leído, no leído, respondido o eliminado**.
- Incluye soporte para múltiples buzones de correo electrónico que permite crear, renombrar o eliminar mensajes de correo electrónico presentados en el servidor dentro de carpetas, y mover éstos mensajes entre distintas cuentas de correo electrónico. Esta característica también permite al servidor proporcionar acceso hacia los carpetas públicas y compartidas.
- Incluye soporte para realizar búsquedas del lado del servidor a través de mecanismos que permiten obtener resultados de acuerdo a varios criterios, permitiendo evitar que los clientes de correo electrónico tengan que descargar todos los mensajes desde el servidor.
- Las especificaciones del protocolo **IMAP** definen un mecanismo explícito mediante el cual puede ser mejorada su funcionalidad a través de extensiones. Un ejemplo es la extensión **IMAP IDLE**, la cual permite sincronizar ente el servidor y el cliente a través de avisos.

Después de establecerse una conexión entre el cliente y el servidor, se inicia una sesión **IMAP**, ejemplificada a continuación.

```

Cliente: $ telnet 127.0.0.1 143
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^'.
          * OK dovecot ready.
          +OK dovecot ready.
  Cliente: x LOGIN fulano clave de acceso
Servidor: x OK Logged in.
  Cliente: x SELECT inbox
Servidor: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
          * OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags
          permitted.
          * 1 EXISTS
          * 0 RECENT
          * OK [UNSEEN 1] First unseen.
          * OK [UIDVALIDITY 1100569382] UIDs valid
          * OK [UIDNEXT 203] Predicted next UID
          x OK [READ-WRITE] Select completed.
  Cliente: x FETCH 1 (flags body[header.fields (subject)])
Servidor: * 1 FETCH (FLAGS (\Seen) BODY[HEADER.FIELDS (SUBJECT)] {30}
          Subject: Mensaje de prueba
          )
          x OK Fetch completed.
  Cliente: x FETCH 1 (body[text])
Servidor: * 1 FETCH (BODY[TEXT] {45}
          Hola. Este es un mensaje de prueba.
          Adios.
          )
          x OK Fetch completed.
  Cliente: x LOGOUT
Servidor: * BYE Logging out
          x OK Logout completed.
          Connection closed by foreign host.

```



## 6.11.4 FUNCIONAMIENTO

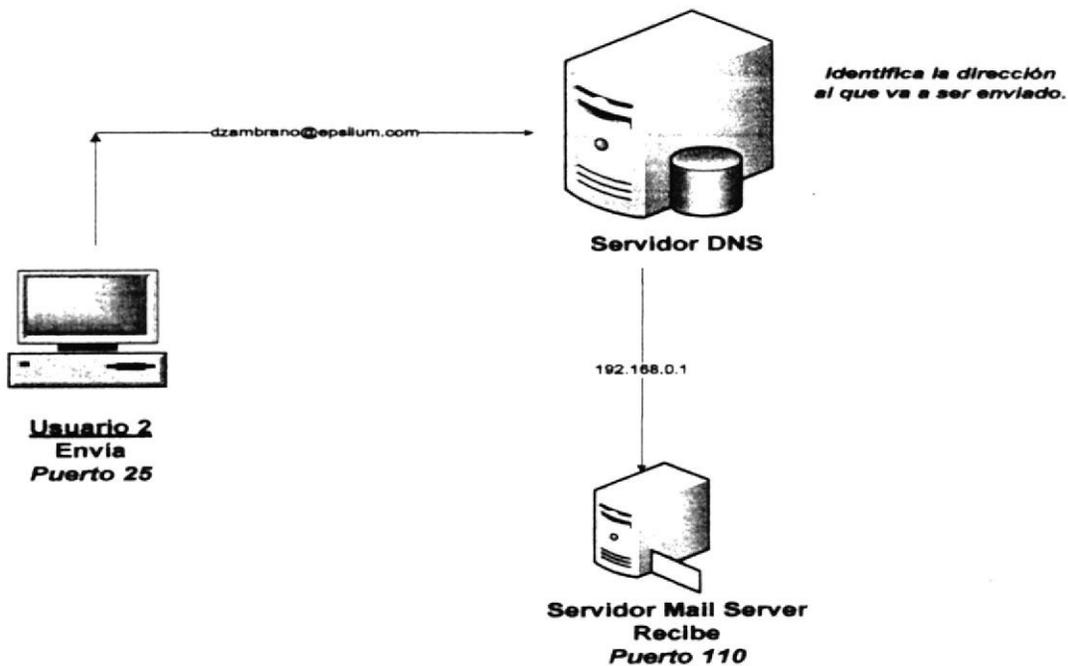


Figura 6. 77. Funcionamiento del Servidor de Correo

Un servidor de correo es una aplicación que permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

- **SMTP, Simple Mail Transfer Protocol:** Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.
- **POP, Post Office Protocol:** Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.
- **IMAP, Internet Message Access Protocol:** Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario (como el caso de Mozilla Mail, Evolution, Microsoft Outlook). Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario.

### 6.11.5 BENEFICIOS SERVIDOR DE CORREO

Los beneficios con los que cuenta el servidor de correo son los siguientes.

- Puede enviar correos masivos a grupos y garantizar que los mensajes son recibidos en las cuentas de los destinatarios.
- Puede crear todos los grupos de correo que necesite.
- El correo puede ser consultado a través de Internet o descargado a su PC.
- No necesita adquirir ningún software.
- Es muy fácil de manejar para el usuario o el administrador.

### 6.11.6 REQUERIMIENTOS SERVIDOR DE CORREO

- Sistema operativo Linux Fedora Core 3.
- Tener la tarjeta de red configurada con una IP estática.
- Haber instalado el paquete sendmail.
- Haber instalado el paquete dovecot.
- Adquirir un Dominio para que se pueda crear el servidor de correo
- Deshabilitar los firewalls.
- Habilitar los Puertos 25 y 110 desde la red Local y desde el Internet.

### 6.11.7 CONFIGURACIÓN DE SENDMAIL:

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

Para configurar un servidor de correo deberá editar el archivo de configuración de correo entrante (pop3). En el archivo de configuración **dovecot.conf**, el cual se encuentra en la siguiente ruta:

**vi /etc/dovecot.conf** (ruta del archivo dovecot.conf)

- Dovecot es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo.

```

Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# Dovecot 1.0 configuration file
# Default values are shown after each value, it's not required to uncomment
# any of the lines. Exception to this are paths, they're just examples
# with real defaults being based on configure options. The paths listed here
# are for configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
# --with-sasl=/usr/share/sasl
# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/
# Protocols we want to be serving:
# imap imaps pop3 pop3s
#protocols = imap imaps
# IP or host address where to listen in for connections. It's not currently
# possible to specify multiple addresses. "*" listens in all IPv4 interfaces.
# "[::]" listens in all IPv6 interfaces, but may also listen in all IPv4
# interfaces depending on the operating system. You can specify ports with
# "host:port".
#imap_listen = [::]
#pop3_listen = [::]
# IP or host address where to listen in for SSL connections. Defaults
# to above non-SSL equivalents if not specified.
#imaps_listen =
#pop3s_listen =
/etc/dovecot.conf" 488L, 20291C                               1.1  Comienzo

```

Figura 6. 78. Pantalla de configuración de archivo dovecot.conf

En el archivo `dovecot.conf` editar lo siguiente:

**protocols = imap imaps pop3**

(Agregar el Puerto pop3)



**Importante:**

- **POP:** Es un **protocolo estándar** de Internet del **Nivel de Aplicación** que recupera el correo electrónico desde un servidor remoto a través de una conexión TCP/IP desde un cliente local. El diseño de **POP3** y sus predecesores es permitir a los usuarios recuperar el correo electrónico al estar conectado hacia una red y manipular los mensajes recuperados sin necesidad de permanecer conectados.
- **IMAP, Internet Message Access Protocol:** Es un **protocolo estándar** de Internet del **Nivel de Aplicación** utilizado para acceder hacia el correo electrónico en un servidor remoto a través de una conexión TCP/IP desde un cliente local.

Iniciar el servicio `dovecot`

```

root@epsilon:/etc
File Edit View Terminal Tabs Help
[root@epsilon etc]# service dovecot start
Starting Dovecot Imap: [ OK ]
[root@epsilon etc]#
  
```

**Figura 6. 79.** Pantalla iniciar el servicio `dovecot`

Luego, se deberá configurar el archivo `sendmail.mc`, el cual permitirá configurar el correo saliente.

**vi /etc/mail/sendmail.mc (ruta del archivo `sendmail.mc`)**

- Sendmail incluye soporte para realizar en re-encaminamiento de dominios de correo a través del parámetro `FEATURE('mailertable', 'hash -o /etc/mail/mailertable.db')` que debe estar habilitado de modo predefinido en el fichero `/etc/mail/sendmail.mc`. Esta función permite a Sendmail realizar traducción de dominios, especificar un agente de entrega y cambiar el encaminamiento establecido en un DNS.

Editar lo siguiente:

**Daemon\_Options ('Port=smtP.Addr=0.0.0.0, Name=MTA') dni**

(Esta línea permite el acceso de todas las IP)

- **DAEMON\_OPTIONS.** : De modo predefinido Sendmail escucha peticiones a través de la interfaz de retorno del sistema a través de IPv4 (127.0.0.1) y no a través de otros dispositivos de red. Solo se necesita eliminar las restricciones de la interfaz de retorno para poder recibir correo desde Internet o la LAN.

**Local\_domain ('epsilon.com')**

➤ Se coloca el nombre del dominio

**Cwepsilum.com**

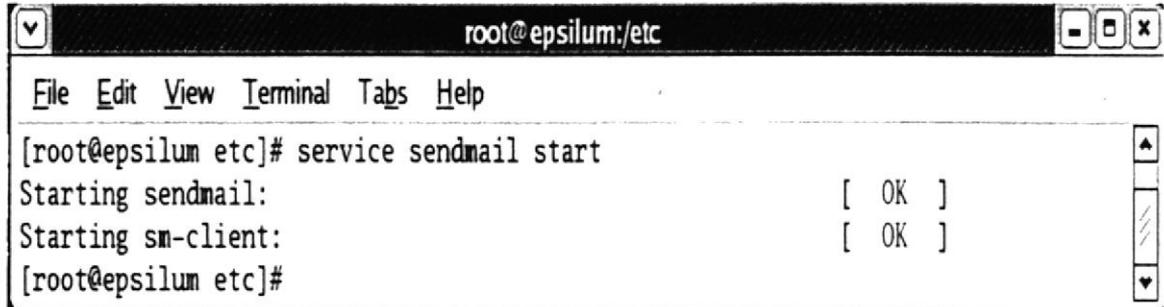
(Nombre de dominio de servidor, esta línea hay que agregarla en la final de la configuración).

➤ **PARÁMETRO CW.:** Añadir al final del fichero /etc/mail/sendmail.mc un parámetro que defina que dominio.com se trata de un dominio local. Note que no debe haber espacios entre Cw y dominio.com, y que Cw se escribe con una C mayúscula y una w minúscula.

*Iniciar el servicio sendmail.*

**service sendmail start**

(Iniciar el servicio Sendmail)



```

root@epsilon:/etc
File Edit View Terminal Tabs Help
[root@epsilon etc]# service sendmail start
Starting sendmail:           [ OK ]
Starting sm-client:         [ OK ]
[root@epsilon etc]#
  
```

**Figura 6. 80.** Pantalla iniciar el servicio Sendmail

*Una vez iniciado el servicio de sendmail, compilar el archivo de sendmail.mc al sendmail.cf, esto se lo hace digitando la siguiente línea:*

**m4 sendmail.mc > sendmail.cf**

**Importante**

A fin de facilitar la configuración de Sendmail para los usuarios ocasionales y los administradores en general, existe un mecanismo complementario que evita la escritura y modificación directa del archivo "cf". Este mecanismo consiste en escribir un archivo relativamente sencillo usando la sintaxis del lenguaje "M4", el cual se proporciona en prácticamente todos los sistemas Unix/Linux (a veces como software opcional.)

Mediante este sistema, el usuario creará (o modificará) un archivo relativamente breve, el cual se traducirá en muchas líneas del archivo "cf".

Lo cierto es que es absolutamente impráctico escribir "desde cero" un archivo "cf" medianamente utilizable, así que el método M4 es una opción casi obligatoria.

Configurar los archivos correspondientes para poder levantar el servidor de correo es necesario editar también el archivo **hosts**.

**vi /etc/hosts**

Ruta de acceso a archivo hosts



#### Importante

El archivo /etc/hosts es complementario al sistema DNS. Para su correcta operación Sendmail normalmente requiere que el computador en que se ejecuta tenga una configuración como la siguiente:

**127.0.0.1 localhost**

La dirección IP suministrada debe coincidir con lo que se configuró en el DNS, y el nombre del host debe ser "full", es decir, debe incluir el nombre del dominio.

Editar de la siguiente manera para indicarle el nombre del dominio y el nombre del correo.

**127.0.0.1 epsilum.com mail**

(Se coloca el nombre del dominio)

Especificar el nombre del servidor de correo, en la siguiente ruta:

**vi /etc/sysconfig/network**

(Ruta de archivo network)

Modificar de la siguiente manera:

**Networking = yes** (Habilita la red)

**Hostname = epsilum.com** (Nombre de dominio)



#### Importante

El nombre del computador donde se ejecuta Sendmail debe corresponder a lo configurado en el DNS y el archivo hosts. La configuración de este parámetro varía de sistema en sistema. Por ejemplo, en RedHat, la configuración del hostname se efectúa en el archivo /etc/sysconfig/network en la variable HOSTNAME.

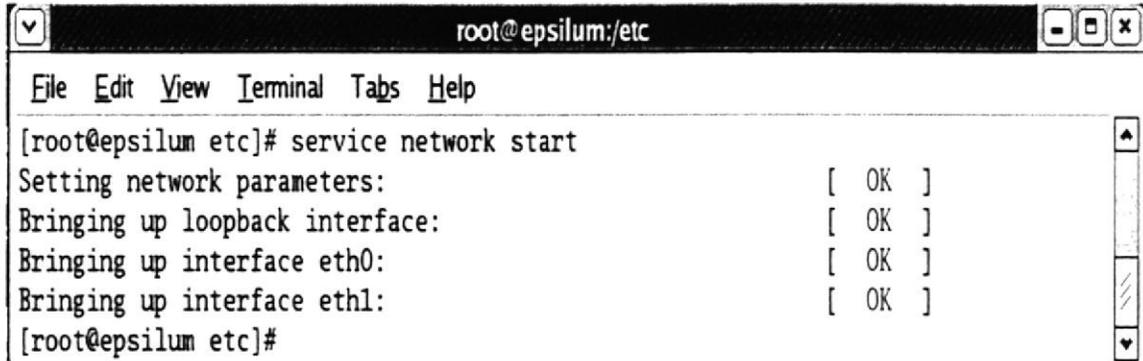
```
[NETWORKING=yes  
HOSTNAME=epsilum.com
```

La forma más fácil -pero no la única- de proseguir tras modificar el hostname, consiste en reiniciar el computador.

Iniciar la red para que los cambios surtan efecto, en algunos casos tendrá que reiniciar el equipo.

**service network start**

(Iniciar el servicio Sendmail)



```
root@epsilon:/etc
File Edit View Terminal Tabs Help
[root@epsilon etc]# service network start
Setting network parameters:           [ OK ]
Bringing up loopback interface:      [ OK ]
Bringing up interface eth0:         [ OK ]
Bringing up interface eth1:         [ OK ]
[root@epsilon etc]#
```

Figura 6. 81. Pantalla iniciar el servicio network

Se reinicia el equipo con el comando **reboot**.

**Reboot**

(Reiniciar el equipo)

Probar la configuración enviando correos entre usuarios. Digitando en la consola de texto de Linux lo siguiente **mail dzambrano**, agregar el **asunto** y finalizar con punto (.).



```
root@epsilon:/etc/mail
File Edit View Terminal Tabs Help
[root@epsilon ~]# mail dzambrano@epsilon.com
Subject: REPORTE DE CLIENTES
Se envia reporte actualizado de los clientes
.
Cc:
[root@epsilon mail]#
```

Figura 6. 82. Pantalla envlo mail

Para verificar si se le ha llegado el correo al usuario dzambrano se hace lo siguiente:



Figura 6. 83. Pantalla mail enviado

## 6.11.8 CONFIGURACIÓN EN CLIENTE WINDOWS

1. En el Outlook Express.
2. En el menú Herramientas.
3. Escoger Cuentas...

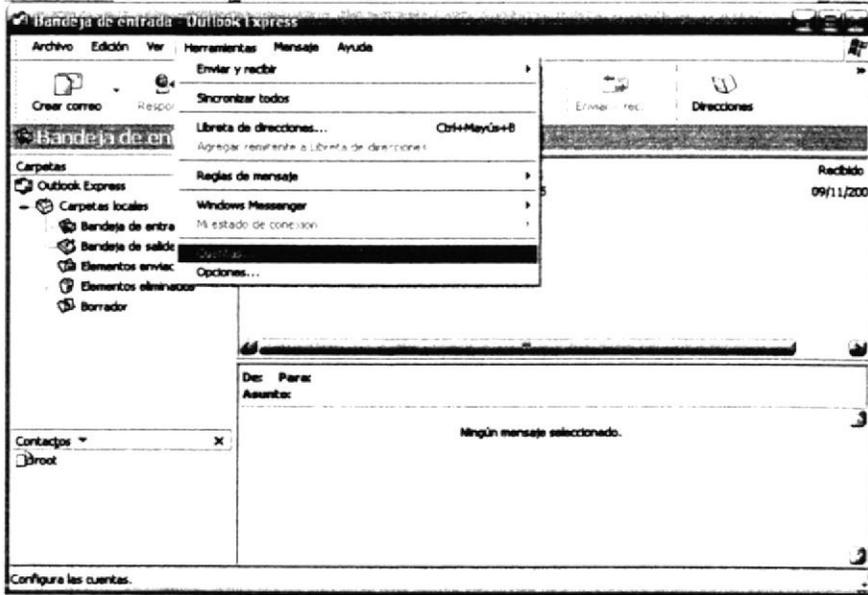


Figura 6. 84. Pantalla configurar cuentas de correo

4. Dar clic en la pestaña Correo.
5. Luego escoger la opción Agregar – Correo.

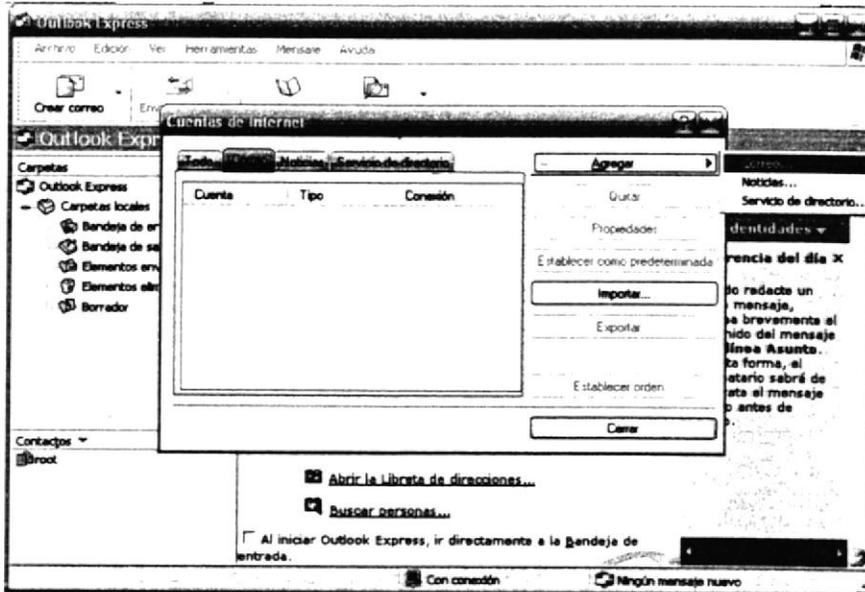


Figura 6. 85. Pantalla: Cuentas de Internet

- 6. Colocará el nombre con el cual aparecerá en el campo del mensaje saliente.

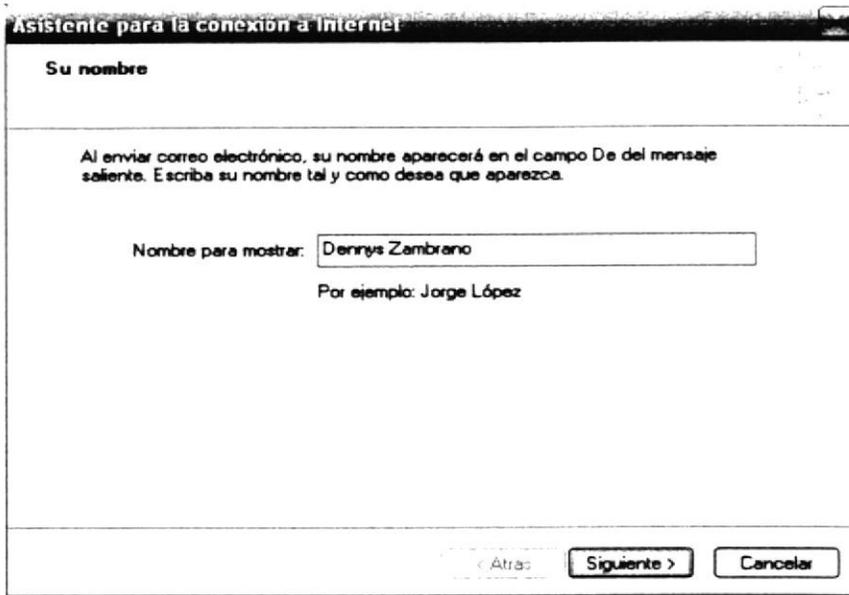


Figura 6. 86. Pantalla: Asistente para la conexión a Internet

- Se le agrega la dirección de correo electrónico.

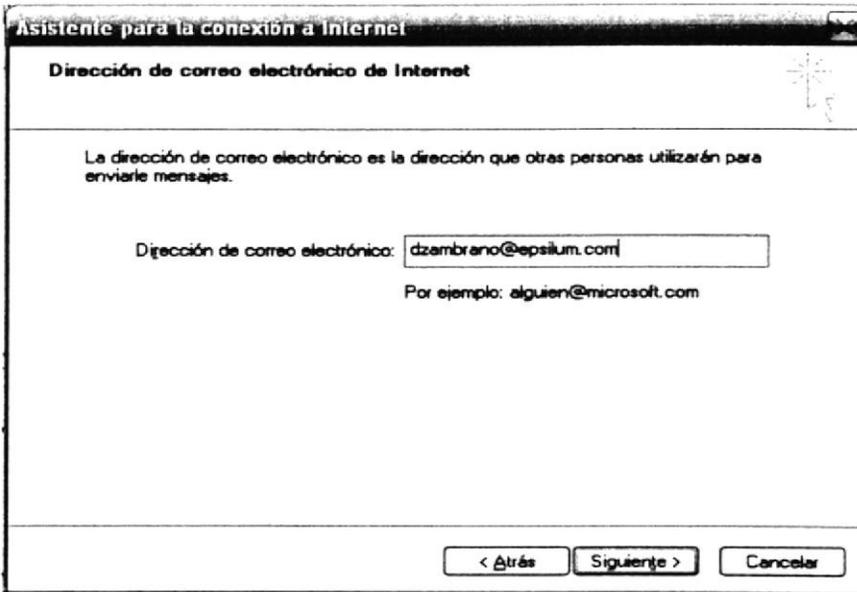


Figura 6. 87. Pantalla de la dirección de correo.

- Agregaré el nombre de su servidor de correo entrante y saliente.

Asistente para la conexión a Internet

Nombre del servidor de correo electrónico

Mi servidor de correo entrante es: POP3

Servidor de correo entrante (POP3, IMAP o HTTP):  
mail.epsalum.com

El servidor SMTP se utiliza para el correo saliente.  
Servidor de correo saliente (SMTP):  
mail.epsalum.com

< Atrás    Siguiete >    Cancelar

Figura 6. 88. Pantalla nombre del servidor de correo entrante y saliente.

- Luego se agrega la contraseña, ya que el nombre de usuario sale por default.

Asistente para la conexión a Internet

Inicio de sesión del correo de Internet

Escribe el nombre de la cuenta y la contraseña que su proveedor de servicios Internet le ha proporcionado.

Nombre de cuenta: dzambrano

Contraseña: .....

Recordar contraseña

Si su proveedor de servicios Internet requiere autenticación de contraseña segura (SPA) para tener acceso a su cuenta de correo, active la casilla de verificación "Iniciar sesión usando autenticación de contraseña segura (SPA)".

Iniciar sesión usando autenticación de contraseña segura (SPA)

< Atrás    Siguiete >    Cancelar

Figura 6. 89. Pantalla ingreso de usuario y contraseña

- Dará clic en finalizar.

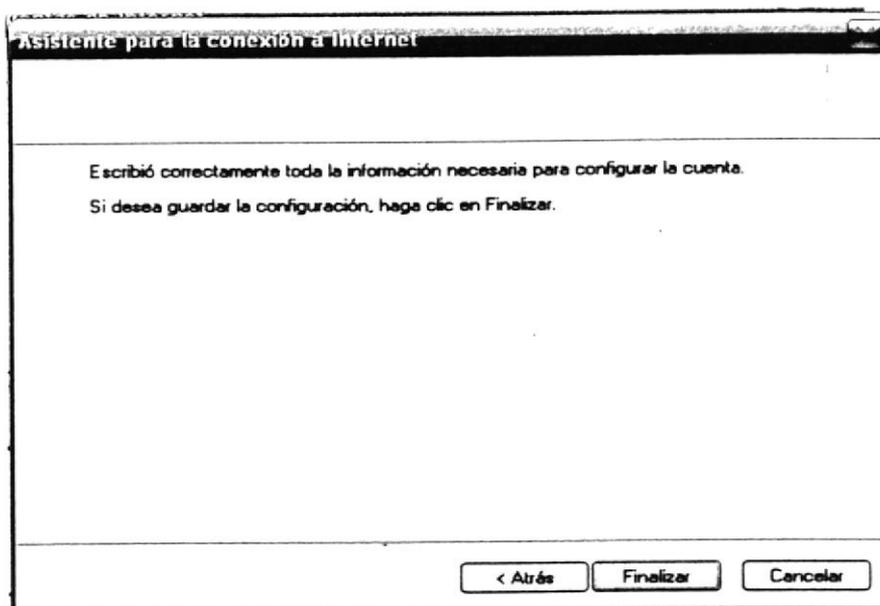


Figura 6. 90. Pantalla terminar la configuración

- Luego cerrar la ventana del asistente para la conexión a Internet.
- Después dar clic en Enviar y Recibir.

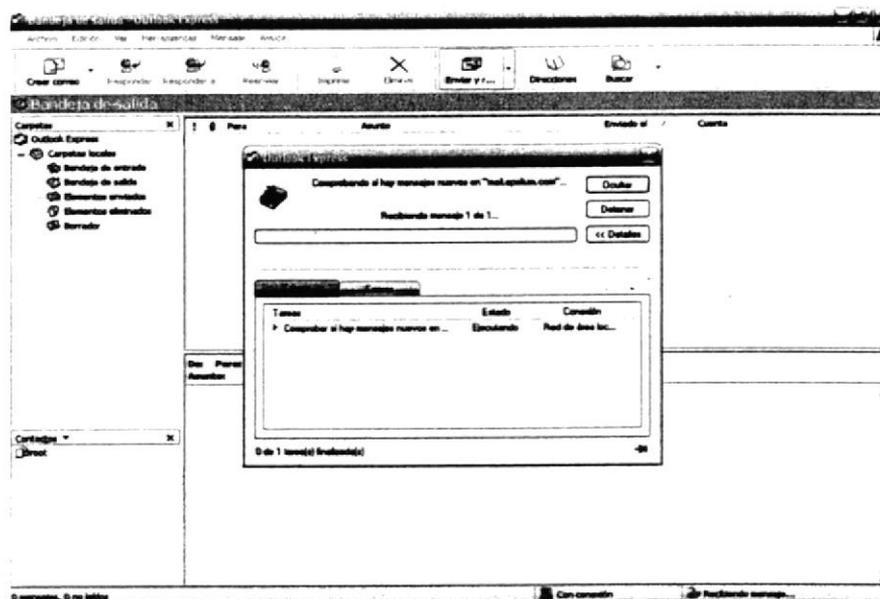


Figura 6. 91. Pantalla comprobación del correo

- Comprobado si hay mensaje en "mail.epsilon.com" aparecerá la siguiente pantalla.

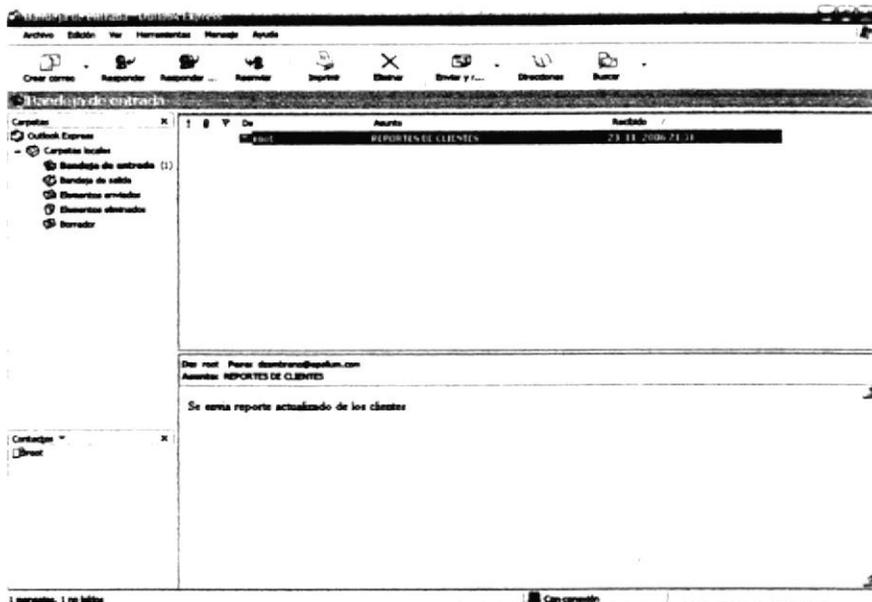


Figura 6. 92. Pantalla recibiendo correo de otros usuarios

- Enviar un correo al root.

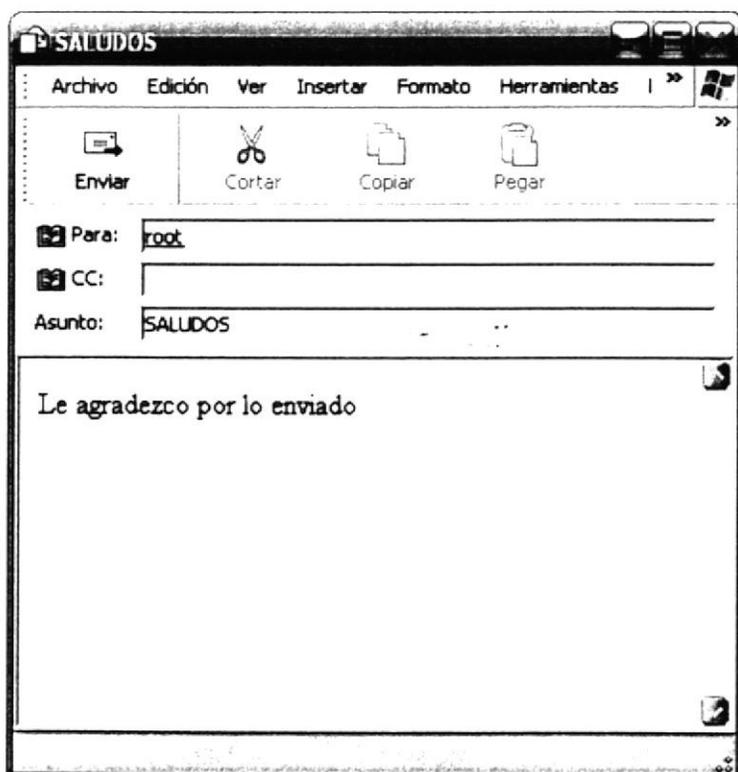


Figura 6. 93. Pantalla de Envío de mensajes

- Si el correo se ha enviado exitosamente deberá aparecer en la opción "**Elementos Enviados**" de Microsoft Outlook.

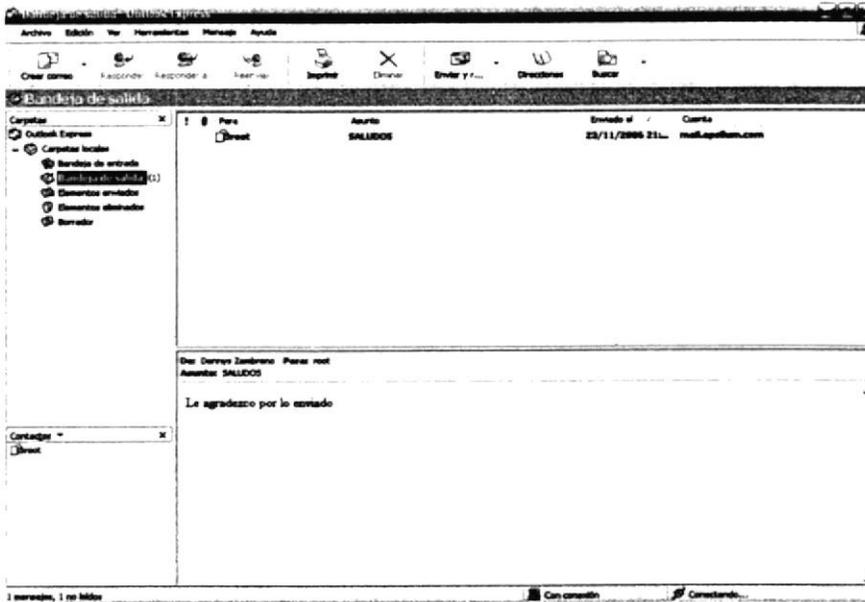


Figura 6. 94. Pantalla enviando correo a otra cuenta

Una vez enviado el correo, ingresará al servidor y revisará el correo.

```

root@epsilon:/etc/mail
File Edit View Terminal Tabs Help
[root@epsilon ~]# mail
Mail version 8.1 6/6/93. Type ? for help.
"/var/spool/mail/root": 1 messages 1 new
>N 1 dzanbrano@epsilon.co Thu Nov 23 21:47 24/798 "SALUDOS"
&

```

Figura 6. 95. Pantalla recibiendo mail

Para leer el mensaje, solamente digitará el número del mensaje, en este caso es 1.

```

& 1
Message 1:
From dzanbrano@epsilon.com Thu Nov 23 21:47:07 2006
From: "Dennys Zambrano" <dzanbrano@epsilon.com>
To: "root" <root@epsilon.com>
References: <200611240231.kA02ViZm003976@epsilon.com>
Subject: SALUDOS
Date: Thu, 23 Nov 2006 21:49:09 -0500
MIME-Version: 1.0
Content-Type: text/plain;
    format=flowed;
    charset="iso-8859-1";
    reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2670
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2670

Le agradezco por lo enviado
&

```

Figura 6. 96. Pantalla de lectura del mail

## 6.12 FIREWALL

### 6.12.1 ACERCA DE FIREWALL

El Firewall es una herramienta preventiva contra ataques, que realiza una inspección del tráfico entrante y saliente. Esto impide que servicios o dispositivos no autorizados accedan a ciertos recursos y de esta manera protegerse contra ataques de denegación de servicios por ejemplo (DOS).

### 6.12.2 FUNCIONAMIENTO DE FIREWALL

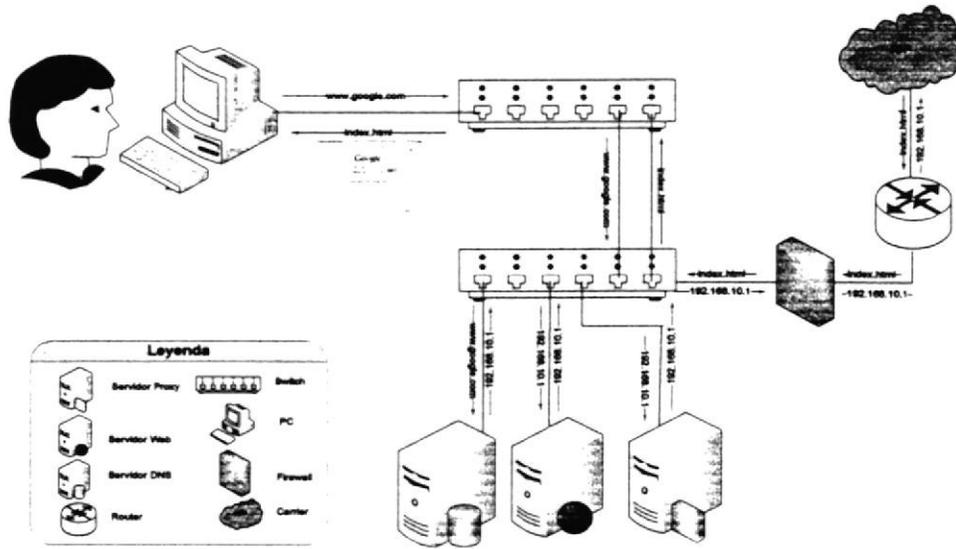


Figura 6. 97. Funcionamiento de Firewall Linux

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para su trabajo. También se puede configurar los accesos que se hagan desde Internet hacia la red local y denegar todos o permitir algunos servicios como el de la web, (si es que posee un servidor web y quiere que sea accesible desde Internet). Dependiendo del firewall que tenga, también podrá permitir algunos accesos a la red local desde Internet si el usuario se ha autenticado como usuario de la red local.

### 6.12.3 REQUERIMIENTOS FIREWALL

- Sistema Operativo Linux Fedora Core 3.
- Tener instalado paquete IPTABLES.
- Configurar el servicio de IPTABLES.
- Haber iniciado el servicio IPTABLES.
- Tener la tarjeta de red configurada con una IP estática.

### 6.12.4 FILTRADO DE PAQUETES

El tráfico se mueve a través de una red en paquetes. Un paquete de red es una colección de datos en diferentes tamaños y formatos. Para enviar un fichero por red, el ordenador emisor debe en primer lugar partirlo en diferentes paquetes usando las reglas del protocolo de red. Cada uno de estos paquetes contiene una parte pequeña de los datos del fichero. Cuando recibe la transmisión, el ordenador receptor, reensambla los paquetes y construye de nuevo el fichero.

Cada paquete contiene información que le ayuda a navegar por la red y moverse hacia su destino. El paquete puede decirle a los ordenadores a lo largo del camino, así como al ordenador destino, de dónde viene, a dónde va, qué tipo de paquete es, y otras muchas cosas más. La mayoría de los paquetes se diseñan para transportar datos, pero algunos protocolos pueden usar los paquetes de forma especial. El protocolo Transmisión Control Protocolo (TCP), por ejemplo, utiliza un paquete SYN, que no contiene datos, para iniciar la comunicación entre dos sistemas.

El kernel de Linux contiene la característica interna de filtrado de paquetes, permitiendo aceptar algunos de ellos en el sistema mientras que intercepta y para a otros. El filtro de red tiene tres tablas o listas de reglas. Son las siguientes:

- filter* — La tabla por defecto para el manejo de paquetes de red.
- nat* — Usada para alterar paquetes que crean una nueva conexión.
- mangle* — Usada por tipos específicos de alteración de paquetes.

Cada una de estas tablas tiene un grupo de cadenas internas que corresponden a las acciones llevadas a cabo por el filtro de red en el paquete.

Las cadenas internas para la tabla filtro son las siguientes:

- INPUT* — Aplica a los paquetes recibidos a través de una interfaz de red.
- OUTPUT* — Esta cadena sirve para paquetes enviados por medio de la misma interfaz de red que recibió los paquetes.
- FORWARD* — Esta cadena sirve para paquetes recibidos en una interfaz de red y enviados en otra.

Las cadenas internas para la tabla nat son las siguientes:

*PREROUTING* — Esta cadena altera paquetes recibidos por medio de una interfaz de red cuando llegan.

*OUTPUT* — Esta cadena altera paquetes generados localmente antes de que sean dirigidos por medio de una interfaz de red.

*POSTROUTING* — Esta cadena altera paquetes antes de que sean enviados por medio de una interfaz de red.

Las cadenas internas para la tabla mangle son las siguientes:

*PREROUTING* — Esta cadena altera paquetes recibidos por medio de una interfaz de red antes de que sean dirigidos.

*OUTPUT* — Esta cadena altera paquetes generados localmente antes de que sean dirigidos por medio de una interfaz de red.

Cada paquete de red recibido o enviado de un sistema Linux está sujeto a al menos una tabla.

Un paquete puede que sea verificado contra muchas reglas dentro de la lista de reglas antes de llegar al final de una cadena. La estructura y propósito de estas reglas puede variar, pero normalmente buscan identificar un paquete que viene de o se dirige a una dirección IP en particular o un conjunto de direcciones al usar un determinado protocolo y servicio de red.

Independientemente de su destino, cuando un paquete cumple una regla en particular en una de las tablas, se asignan a un objetivo (target) particular. Si la regla especifica un objetivo ACCEPT para un paquete que coincida, el paquete se salta el resto de las verificaciones de la regla y se permite que continúe hacia su destino. Si una regla especifica un objetivo DROP, a ese paquete se le niega el acceso al sistema y no se envía nada de vuelta al servidor que envió el paquete. Si una regla especifica un objetivo QUEUE, el paquete se pasa al espacio del usuario. Si una regla especifica el objetivo opcional REJECT, el paquete es entregado, pero se envía un paquete de error al que envió el paquete.

Cada cadena tiene una política por defecto de ACCEPT, DROP, REJECT, o QUEUE. Si ninguna de estas reglas en la cadena se aplica al paquete, entonces el paquete es tratado de acuerdo a la política por defecto.

El comando iptables configura estas tablas, así como también configura nuevas tablas si es necesario.



## 6.12.5 COMANDOS IPTABLES

Los comandos le dicen a iptables que realice una tarea específica. Solamente un comando se permite por cada cadena de comandos iptables. Excepto el comando de ayuda, todos los comandos se escriben en mayúsculas.

Los comandos de iptables son los siguientes:

*-A* — Añade la regla iptables al final de la cadena especificada. Este es el comando utilizado para simplemente añadir una regla cuando el orden de las reglas en la cadena no importa.

*-C* — Verifica una regla en particular antes de añadirla en la cadena especificada por el usuario. Este comando puede ser de ayuda para construir reglas iptables complejas pidiéndole que introduzca parámetros y opciones adicionales.

*-D* — Borra una regla de una cadena en particular por número (como el 5 para la quinta regla de una cadena). Puede también teclear la regla entera e iptables borrará la regla en la cadena que corresponda.

*-E* — Renombra una cadena definida por el usuario. Esto no afecta la estructura de la tabla.

*-F* — Libera la cadena seleccionada, que borra cada regla de la cadena. Si no se especifica ninguna cadena, este comando libera cada regla de cada cadena,

*-h* — Proporciona una lista de estructuras de comandos, así como también un resumen rápido de parámetros de comandos y opciones.

*-I* — Inserta una regla en una cadena en un punto especificado por un valor entero definido por el usuario. Si no se especifica ningún número, iptables colocará el comando en el tope de la cadena.

*-L* — Lista todas las reglas de la cadena especificada tras el comando. Para ver una lista de todas las cadenas en la tabla filter por defecto. La sintaxis siguiente deberá utilizarse para ver todas las listas de todas las reglas de una cadena específica en una tabla en particular:

```
iptables -L <chain-name> -t  
<table-name>
```

Opciones más potentes para el comando *-L*, que proporcionan números a las reglas y permiten más descripciones en las reglas.

*-N* — Crea una nueva cadena con un nombre especificado por el usuario.

*-P* — Configura la política por defecto para una cadena en particular de tal forma que cuando los paquetes atraviesen la cadena completa sin cumplir ninguna regla, serán enviados a un objetivo en particular, como puedan ser ACCEPT o DROP.

*-R* — Reemplaza una regla en una cadena particular. El número de la regla debe ser especificado después del nombre de la cadena. La primera regla en una cadena corresponde a la regla número uno.

*-X* — Borra una cadena especificada por el usuario. No se permite borrar ninguna de las cadenas predefinidas para cualquier tabla.

*-Z* — Pone ceros en los contadores de byte y de paquete en todas las cadenas de una tabla en particular.

### 6.12.6 PARÁMETROS

Una vez que se especifiquen ciertos comandos iptables, incluyendo aquellos para añadir, anexar, eliminar, insertar o reemplazar reglas dentro de una cadena, se requieren parámetros para construir una regla de filtrado de paquetes.

-c Resetea los contadores de una regla en particular. Este parámetro acepta las opciones PKTS y BYTES para especificar qué contador hay que resetear.

-d — Configura el nombre de la máquina destino, dirección IP o red de un paquete que coincide con la regla. Cuando se coincida una red, los siguientes formatos de direcciones IP o máscaras de red son soportados:

N.N.N.N/M.M.M.M — Donde N.N.N.N es el rango de direcciones IP y M.M.M.M es la máscara de la red.

N.N.N.N/M — Donde N.N.N.N es el rango de direcciones IP y M es la máscara de la red.

-f Aplica esta regla sólo a los paquetes fragmentados.

Usando la opción ! después de este parámetro, únicamente los paquetes no fragmentados se tendrán en cuenta.

-i — Configura la interfaz de red entrante, tal como eth0 o ppp0. Con iptables, este parámetro opcional puede ser usado solamente con las cadenas INPUT y FORWARD cuando es usado con la tabla filter y la cadena PREROUTING con las tablas nat y mangle.

Este parámetro también soporta las siguientes opciones especiales:

! — Dice a este parámetro que no concuerde, queriendo decir esto que las interfaces especificadas se excluirán de esta regla.

+ — Un caracter tipo comodín utilizado para coincidir todas las interfaces con una cadena de caracteres particular. Por ejemplo, el parámetro -i eth+ aplicará esta regla a cualquier interfaz Ethernet pero excluirá cualquier otra interfaz, tal como ppp0.

Si el parámetro -i se utiliza sin especificar ninguna interfaz, todas las interfaces estarán afectadas por la regla.

-j — Le dice a iptables que salte a un objetivo particular cuando un paquete coincide con una regla. Los objetivos válidos a usar después de la opción -j incluye las opciones estándar, ACCEPT, DROP, QUEUE, y RETURN, así como también las opciones extendidas que están disponibles a través de los módulos.

-o — Configura la interfaz de red de salida para una regla y puede ser usada solamente con las cadenas OUTPUT y FORWARD en la tabla de filtro y la cadena POSTROUTING en las tablas nat y mangle. Estos parámetros de opciones son los mismos que aquellos de la interfaz de entrada (-i).

-p — Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all, para coincidir todos los protocolos soportados. Además, se puede usar cualquier protocolo listado en /etc/protocols. Si esta opción es omitida cuando se esté creando una regla, la opción all es la opción por defecto.

-s — Configura la fuente para un paquete particular usando la misma sintaxis que el parámetro (-d).

### 6.12.7 OPCIONES DEL OBJETIVO

Una vez que un paquete ha coincidido con una regla, la regla puede dirigir el paquete a un número de objetivos diferentes que deciden su suerte y, posiblemente, toman acciones adicionales. Cada cadena tiene un objetivo por defecto, el cual es usado si ninguna de las reglas en esa cadena coincide con un paquete o si ninguna de las reglas que coinciden con el paquete específico un objetivo.

Los siguientes son los objetivos estándar:

`<user-defined-chain>` — Reemplace `<user-defined-chain>` con el nombre de una cadena definida por el usuario dentro de la tabla. Este objetivo pasa el paquete a la cadena objetivo.

`ACCEPT` — Permite que el paquete se mueva hacia su destino (o hacia otra cadena, si no ha sido configurado ningún destino para seguir a esta cadena).

`DROP` — Deja caer el paquete sin responder al solicitante. El sistema que envía el paquete no es notificado de esta falla.

`QUEUE` — El paquete se pone en una cola para ser manejado por una aplicación en el espacio de usuario.

`RETURN` — Para la verificación del paquete contra las reglas de la cadena actual. Si el paquete con un destino `RETURN` cumple una regla de una cadena llamada desde otra cadena, el paquete es devuelto a la primera cadena para retomar la verificación de la regla allí donde se dejó. Si la regla `RETURN` se utiliza en una cadena predefinida, y el paquete no puede moverse hacia la cadena anterior, el objetivo por defecto de la cadena actual decide qué acción llevar a cabo.

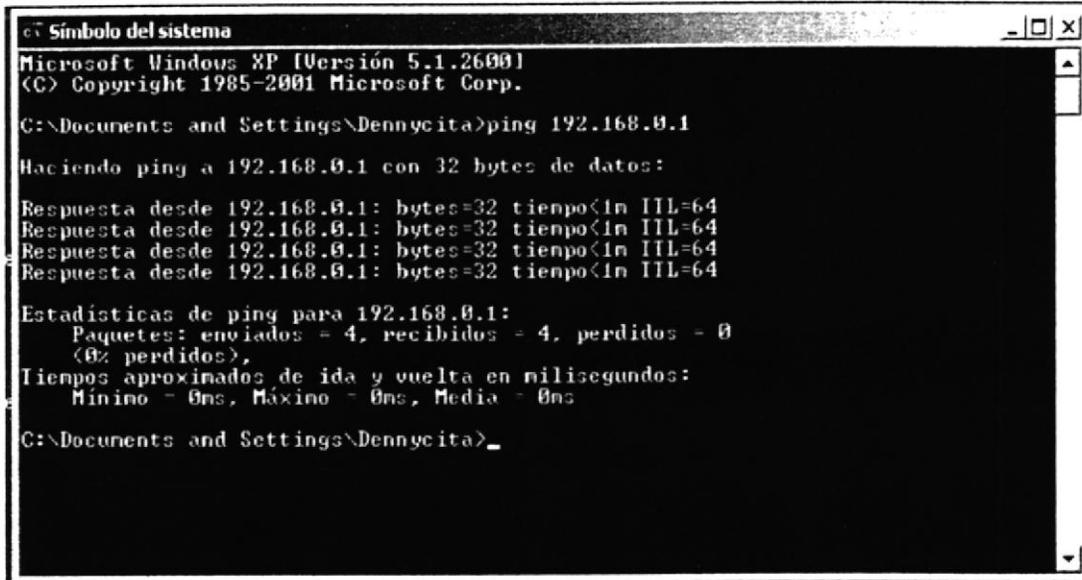
`REJECT` — Envía un paquete de error de vuelta al sistema remoto y deja caer el paquete.

El objetivo `REJECT` acepta `--reject-with <type>` (donde `<type>` es el tipo de rechazo) el cual permite que se envíe información más detallada devuelta con el paquete de error.

### 6.12.8 CONFIGURACIÓN DE FIREWALLS

Antes de configurar los iptables procederá a verificar la conexión desde el cliente Windows hasta su servidor Linux.

Realizará un ping desde el cliente hasta el servidor recibiendo respuesta del mismo.



```
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dennycita>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:

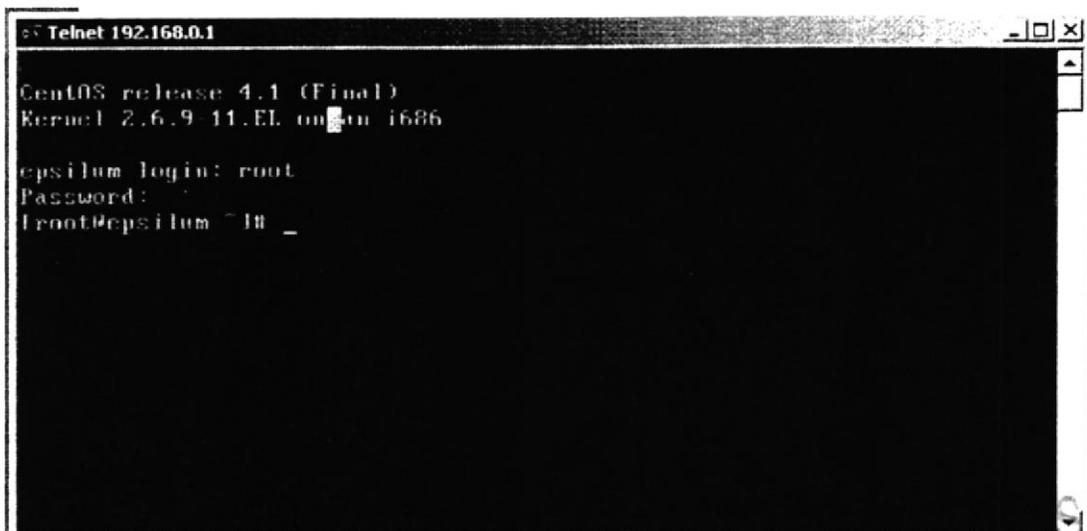
Respuesta desde 192.168.0.1: bytes=32 tiempo<In ILL=64

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Medio = 0ms

C:\Documents and Settings\Dennycita>
```

Figura 6. 98. Pantalla realizar ping

Luego hará telnet del cliente hasta el servidor Linux recibiendo respuesta favorable.



```
Telnet 192.168.0.1

CentOS release 4.1 (Final)
Kernel 2.6.9-11.EL on i686

epsilon login: root
Password:
root@epsilon ~#
```

Figura 6. 99. Pantalla acceso a Telnet

### 6.12.8.1 HABILITAR SMTP

Permite el ingreso al servidor por el Puerto 25

```
iptables -A INPUT -p tcp -dport 25 -j ACCEPT
```

- **iptables -A :**  
Para crear una nueva regla al final de las ya existentes
- **INPUT:**  
Aceptación de paquetes de entrada. Todos los paquetes que vienen de una de las interfaces de la red local son revisados por la regla de entrada. Si el paquete no coincide con alguna de las reglas de entrada este los rechaza
- **-p [protocolo]:**  
Protocolo al que pertenece el paquete.
- **-d [destino/puerto]:**
  - Al igual que el anterior, puede ser un nombre de host, dirección de red, número de puerto o dirección IP singular.
- **-j [target] :**
  - Permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.
- **ACCEPT:**
  - Este valor quiere decir que permite pasar a los paquetes que pasan a través del Firewall. Todos aquellos paquetes que cumplan con la regla de entrada podrán tener acceso de entrada o salida.

### 6.12.8.2 HABILITAR DNS

Permite el ingreso de ese segmento de red al servidor por el puerto 53.

```
iptables -A INPUT -s 192.168.0.0/24 -p tcp -dport 53 -j ACCEPT
```

- **iptables -A :**  
Para crear una nueva regla al final de las ya existentes.
- **INPUT:**  
Aceptación de paquetes de entrada. Todos los paquetes que vienen de una de las interfaces de la red local son revisadas por la regla de entrada. Si el paquete no coincide con alguna de las reglas de entrada este los rechaza.
- **-s [origen]:**  
Dirección de origen del paquete, puede ser un nombre de host, una dirección IP normal, o una dirección de red (con máscara, de forma dirección/máscara).
- **-p [protocolo]:**  
Protocolo al que pertenece el paquete.
- **-d [destino/puerto]:**  
Al igual que el anterior, puede ser un nombre de host, número de puerto dirección de red o dirección IP singular.

- **-j [target]** :
  - Permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.
- **ACCEPT:**
  - Este valor quiere decir que permite pasar a los paquetes que pasan a través del Firewall. Todos aquellos paquetes que cumplan con la regla de entrada podrán tener acceso de entrada o salida.

### 6.12.8.3 HABILITAR HTTP

Permite el ingreso al servidor por el Puerto 80

```
iptables -A INPUT -p tcp -dport 80 -j ACCEPT
```

- **iptables -A :**  
Para crear una nueva regla al final de las ya existentes.
- **INPUT:**  
Aceptación de paquetes de entrada. Todos los paquetes que vienen de una de las interfaces de la red local son revisados por la regla de entrada. Si el paquete no coincide con alguna de las reglas de entrada este los rechaza.
- **-p [protocolo]:**  
Protocolo al que pertenece el paquete.
- **-d [destino/puerto]:**  
Al igual que el anterior, puede ser un nombre de host, número de puerto dirección de red o dirección IP singular.
- **-j [target]** :
  - Permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.
- **ACCEPT:**
  - Este valor quiere decir que permite pasar a los paquetes que pasan a través del Firewall. Todos aquellos paquetes que cumplan con la regla de entrada podrán tener acceso de entrada o salida.

### 6.12.8.4 HABILITAR POP3

Permite el ingreso al servidor por el Puerto 110

```
iptables -A INPUT -p tcp -dport 110 -j ACCEPT
```

- **iptables -A :**  
Para crear una nueva regla al final de las ya existentes.
- **INPUT:**  
Aceptación de paquetes de entrada. Todos los paquetes que vienen de una de las interfaces de la red local son revisadas por la regla de entrada. Si el paquete no coincide con alguna de las reglas de entrada este los rechaza.
- **-p [protocolo]:**  
Protocolo al que pertenece el paquete.



- **-d [destino/puerto]:**  
Al igual que el anterior, puede ser un nombre de host, número de puerto dirección de red o dirección IP singular.
- **-j [target] :**
  - Permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.
- **ACCEPT:**
  - Este valor quiere decir que permite pasar a los paquetes que pasan a través del Firewall. Todos aquellos paquetes que cumplan con la regla de entrada podrán tener acceso de entrada o salida.

#### 6.12.8.5 BLOQUEAR DEMÁS PUERTOS

Bloquea el ingreso por otros puertos.

```
iptables -A INPUT -j DROP
```

- **iptables -A :**  
Para crear una nueva regla al final de las ya existentes.
- **INPUT:**  
Aceptación de paquetes de entrada. Todos los paquetes que vienen de una de las interfaces de la red local son revisadas por la regla de entrada. Si el paquete no coincide con alguna de las reglas de entrada este los rechaza.
- **-j [target] :**  
Permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.
- **DROP :**  
Deja caer el paquete sin responder al solicitante. El sistema que envía el paquete no es notificado de esta falla.

Luego se muestran los iptables configurados en el servidor.

```
[root@epsilon etc]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source      destination
DROP      all  --  anywhere   anywhere
ACCEPT    tcp  --  anywhere   anywhere    tcp dpt:smtp
ACCEPT    tcp  --  192.168.8.8/24  anywhere   tcp dpt:domain
ACCEPT    tcp  --  anywhere   anywhere    tcp dpt:http
ACCEPT    tcp  --  anywhere   anywhere    tcp dpt:http
ACCEPT    tcp  --  anywhere   anywhere    tcp dpt:pop3

Chain FORWARD (policy ACCEPT)
target     prot opt source      destination

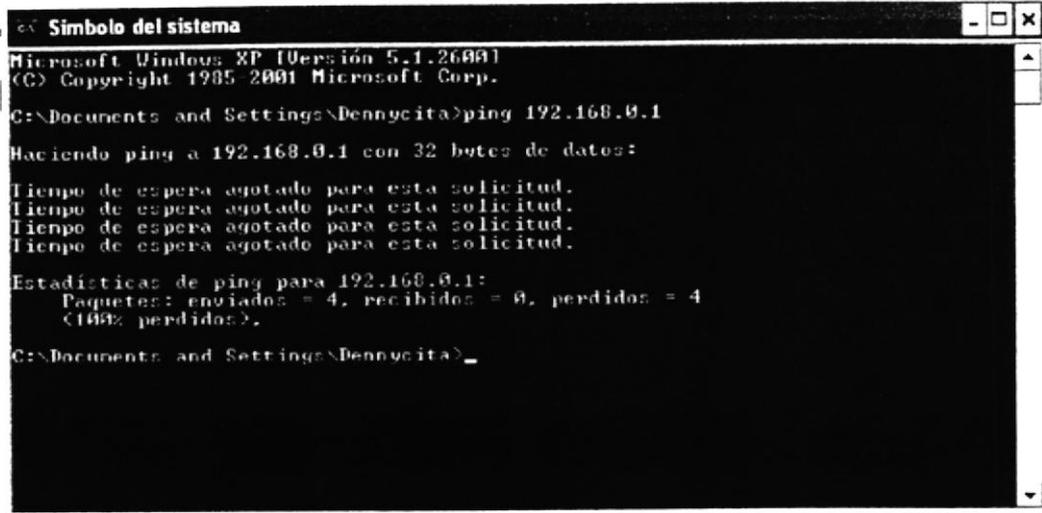
Chain OUTPUT (policy ACCEPT)
target     prot opt source      destination
[root@epsilon etc]# _
```

Figura 6. 100. Pantalla: Visualización de los iptables configurados

### 6.12.9 COMPROBACIÓN CLIENTE WINDOWS

Configurados los iptables, realizará la verificación de los puertos bloqueados.

#### Bloqueo de ICMP



```
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dennycita>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:

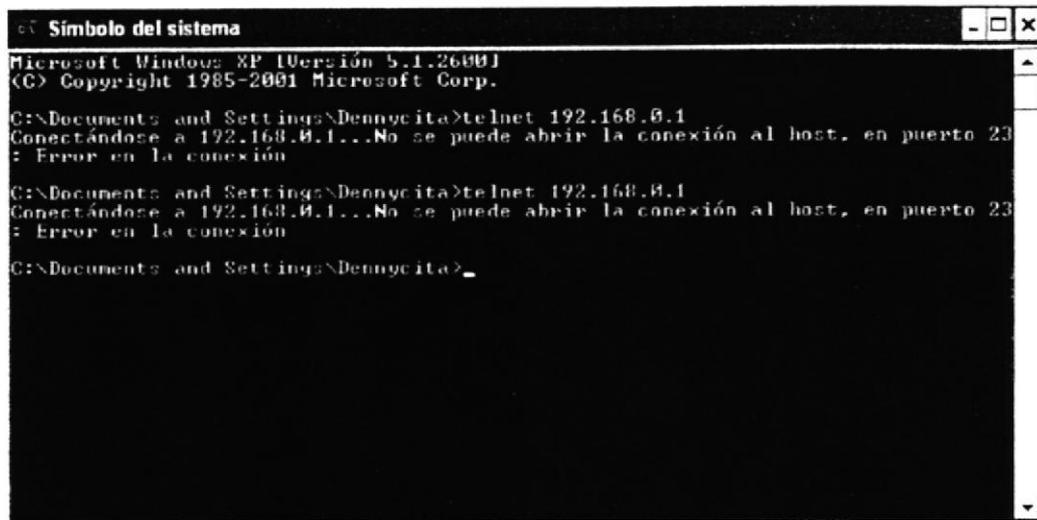
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos).

C:\Documents and Settings\Dennycita>
```

Figura 6. 101. Pantalla Bloqueo Ping

#### Bloqueo de telnet



```
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dennycita>telnet 192.168.0.1
Conectándose a 192.168.0.1...No se puede abrir la conexión al host, en puerto 23
: Error en la conexión

C:\Documents and Settings\Dennycita>telnet 192.168.0.1
Conectándose a 192.168.0.1...No se puede abrir la conexión al host, en puerto 23
: Error en la conexión

C:\Documents and Settings\Dennycita>
```

Figura 6. 102. Pantalla no acceso Telnet



## 6.13 MRTG

### 6.13.1 ACERCA DE MRTG

MRTG (*Multi Router Traffic Grapher*) es una herramienta, escrita por Tobias Oetiker y Dave Rand, para monitorizar la carga de tráfico sobre determinados nodos de una red. MRTG genera páginas HTML que incluyen representaciones gráficas, en formato GIF, del tráfico registrado en un determinado nodo de la red.

MRTG consiste en un script en Perl que utiliza SNMP para obtener información de gestión sobre los nodos de la red y un programa en C para generar los registros de tráfico (logs) y crear representaciones gráficas de los datos recopilados. Estos gráficos se integran dentro de un documento en formato HTML.

Mediante MRTG es posible monitorizar cualquier variable SNMP que se quiera, de manera que se puede configurar para monitorizar la carga de un sistema, las sesiones abiertas por los usuarios de un determinado equipo, disponibilidad de módems. MRTG permite generar gráficas con cuatro niveles de detalle por cada interfaz: tráfico registrado en las últimas 24 horas, la última semana, el último mes y gráfica anual. Además de generar una primera página con la representación del tráfico registrado diariamente a través de cada uno de los posibles interfaces de un router.

### 6.13.2 REQUERIMIENTOS DE MRTG

- Sistema operativo Linux Fedora Core 3.
- Tener instalado el paquete SNMP.
- Tener instalado el paquete MRTG.
- Tener dos tarjetas de red.
- Tener la tarjeta de red configurada con una IP estática.

## 6.13.3 CONFIGURACIÓN

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

Para configurar el MRTG tendrá primero que configurar el SNMP, para que el servidor se monitoree a sí mismo, lo hará digitando la siguiente línea.

**vi /etc/snmp/snmpd.conf**

- **SNMP** (*Simple Network Management Protocol*) es el protocolo definido por los comités técnicos de Internet para ser utilizado como una herramienta de gestión de los distintos dispositivos en cualquier red. El funcionamiento de SNMP es sencillo, como dice el protocolo, aunque su implementación es tremendamente compleja. SNMP utiliza la capa de transporte de TCP/IP mediante el envío de datagramas UDP, sin embargo, el hecho de usar UDP hace que el protocolo no sea fiable (en UDP no se garantiza la recepción de los paquetes enviados, como en TCP).

Ingresado al archivo de configuración, realizará las siguientes modificaciones:

<b>com2sec local 127.0.0.1/32 Epsilon</b>	<b>Línea 74</b>
Se le asigna un control de acceso llamado <b>local</b> y el nombre de la comunidad en este caso <b>Epsilon</b> .	
<b>group GRUPO any local</b>	<b>Línea 78</b>
Permite crear los grupos y luego asociar con el control de acceso.	
<b>view all included.1 80</b>	<b>Línea 85</b>
Descomentarla, especifica las ramas que se van a permitir ver a través del servicio.	
<b>access GRUPO "" any noauth 0 all all all</b>	<b>Línea 94</b>
Estas líneas dan permisos al grupo anteriormente especificado.	

Luego se inicia el servicio **snmp**, digitando la siguiente línea.

**service snmpd start**

(Inicia el servicio **snmpd**)

```

root@epsilon:/etc/snmp
File Edit View Terminal Tabs Help
[root@epsilon snmp]# service snmpd start
Starting snmpd: [ OK ]
[root@epsilon snmp]#

```

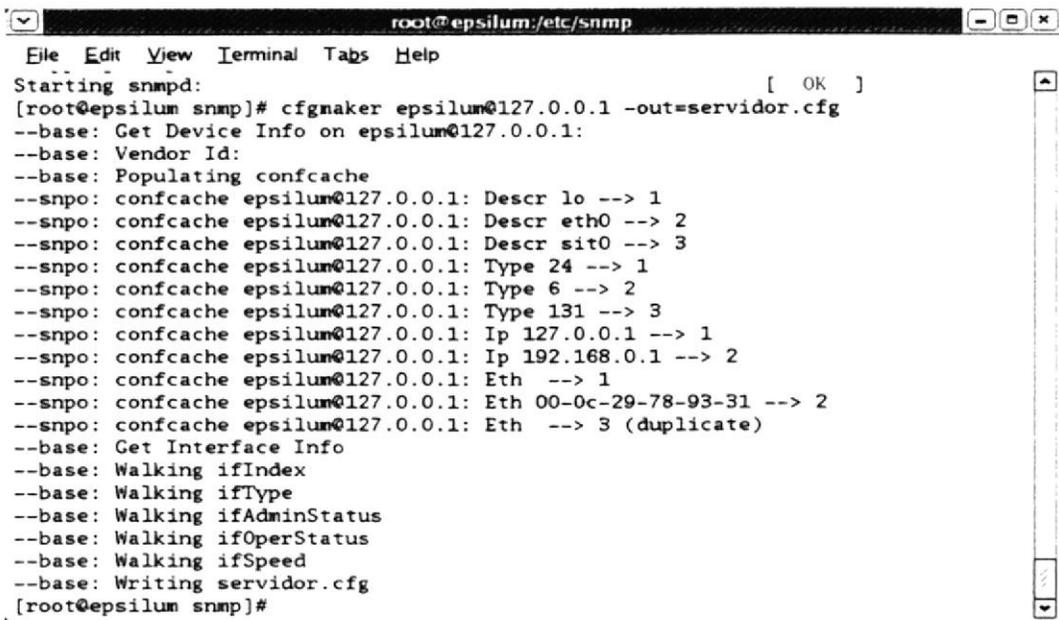
Figura 6. 103. Pantalla: Iniciar el servicio **snmpd**

Luego monitoreará las interfaces de su servidor, ahora generará el archivo de configuración de su servidor digitando la siguiente línea.

### **cfgmaker epsilon@127.0.0.1 --out=servidor.cfg**

- Usará el comando **cfgmaker** para crear un archivo de configuración llamado **localhost.cfg** para el servidor "servidor" usando un community string de solo lectura **clave**. Todos los archivos de datos serán ubicados en el directorio **/var/www/html/mrtg/stats**.

Después aparecerá por pantalla las siguientes líneas indicando que el archivo fue generado con éxito.



```

root@epsilon:/etc/snmp
File Edit View Terminal Tabs Help
Starting snmpd: [ OK ]
[root@epsilon snmp]# cfgmaker epsilon@127.0.0.1 --out=servidor.cfg
--base: Get Device Info on epsilon@127.0.0.1:
--base: Vendor Id:
--base: Populating confcache
--snpo: confcache epsilon@127.0.0.1: Descr lo --> 1
--snpo: confcache epsilon@127.0.0.1: Descr eth0 --> 2
--snpo: confcache epsilon@127.0.0.1: Descr sit0 --> 3
--snpo: confcache epsilon@127.0.0.1: Type 24 --> 1
--snpo: confcache epsilon@127.0.0.1: Type 6 --> 2
--snpo: confcache epsilon@127.0.0.1: Type 131 --> 3
--snpo: confcache epsilon@127.0.0.1: Ip 127.0.0.1 --> 1
--snpo: confcache epsilon@127.0.0.1: Ip 192.168.0.1 --> 2
--snpo: confcache epsilon@127.0.0.1: Eth --> 1
--snpo: confcache epsilon@127.0.0.1: Eth 00-0c-29-78-93-31 --> 2
--snpo: confcache epsilon@127.0.0.1: Eth --> 3 (duplicate)
--base: Get Interface Info
--base: Walking ifIndex
--base: Walking ifType
--base: Walking ifAdminStatus
--base: Walking ifOperStatus
--base: Walking ifSpeed
--base: Writing servidor.cfg
[root@epsilon snmp]#
  
```

Figura 6. 104. Pantalla de configuración del snmp

Luego deberá crear una carpeta donde se almacenen los monitoreos realizados.

### **mkdir /var/www/html/grafico**



#### **Importante**

El comando **mkdir** permite crear directorios.

Una vez generado el archivo de configuración lo editará y le realizará los siguientes cambios:

### **vi servidor.cfg**



#### **Importante**

El comando **vi** permite editar archivos.

**WorkDir: /var/www/html/grafico/****Línea 8**

Descomente la línea y agregue la ruta donde se guardarán los archivos html y log de la gráfica.

**Options[\_]: growright, bits****Línea 16**

Descomente la línea para que mi gráfico lo genere sobre el ancho de banda.

**RunAsDaemon:yes**

Línea que permite que cada 5 minutos se actualice mi gráfico; se agrega después de la anterior

Para generar la grafica MRTG se procede a digitar la siguiente línea de comando

```
env LANG=C mrtg /server.cfg
```

Luego de haber realizado esto, reinicie el servicio de httpd; podrá observar los resultados accediendo a través de Apache hacia <http://www.epsilon.com/gráfico>.

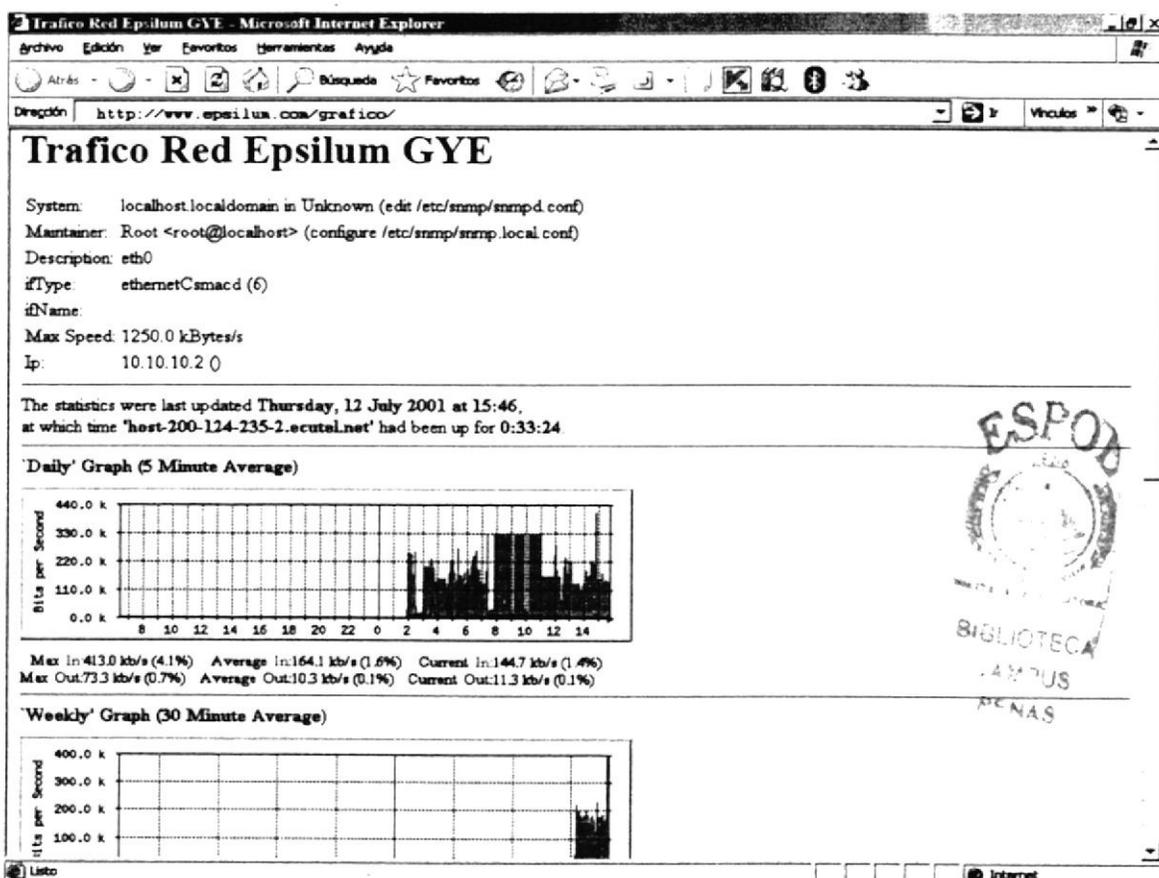
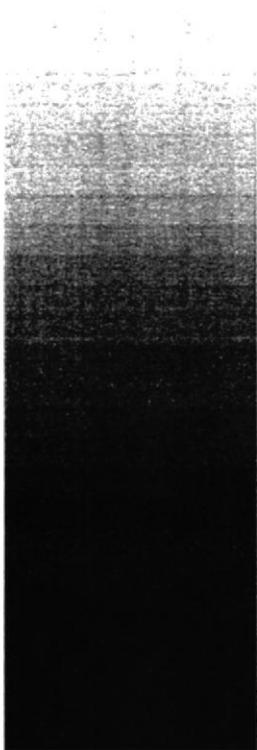


Figura 6. 105. Pantalla gráfico del tráfico



## CAPÍTULO 7

---

# CONFIGURACIÓN DE ROUTER Y SWITCH

## 7. CONFIGURACIÓN DE ROUTERS Y SWITCH

### 7.1 INTRODUCCIÓN A LOS ROUTERS

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio, además con un CPU, memoria, bus de sistema y distintas interfaces de entrada /salida. Sin embargo, los routers están diseñados para cumplir algunas funciones muy específicas que, en general, no realizan los computadores de escritorio. Por ejemplo, los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

Al igual que los computadores, que necesitan sistemas operativos para ejecutar aplicaciones de software, los routers necesitan el software denominado Sistema Operativo de Internetworking (IOS) para ejecutar los archivos de configuración. Estos archivos de configuración contienen las instrucciones y los parámetros que controlan el flujo del tráfico entrante y saliente de los routers. Específicamente, a través de los protocolos de enrutamiento, los routers toman decisiones sobre cual es la mejor ruta para los paquetes. El archivo de configuración especifica toda la información necesaria para una correcta configuración y usos de los protocolos enrutados y de enrutamiento seleccionados, o habilitados, en el router.

### 7.2 COMPONENTES INTERNOS DE UN ROUTER

Los principales componentes internos del router son: CPU, la memoria de acceso aleatorio (RAM), la memoria de acceso aleatorio no volátil (NVRAM), la memoria flash, la memoria de sólo lectura (ROM) y las interfaces.

- **Procesador o CPU:** La unidad central de procesamiento (CPU) ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varios CPU.
- **Memoria RAM (Random Access Memory):** La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el cache de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Por lo general, la RAM se divide de forma lógica en memoria del procesador principal y memoria compartida de entrada/salida (I/O). Las interfaces de almacenamiento temporal de los paquetes comparten la memoria de I/O compartida. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más módulos de memoria en línea doble (DIMM).

Tiene las siguientes características y funciones:

- Almacena las tablas de enrutamiento.
  - Guarda el caché ARP.
  - Guarda el caché de conmutación rápida.
  - Crea el buffer de los paquetes (RAM compartida).
  - Mantiene las colas de espera de los paquetes.
  - Brinda una memoria temporal para el archivo de configuración del router mientras está encendido.
  - Pierde el contenido cuando se apaga o reinicia el router.
- **Memoria NVRAM (No -Volátil RAM):** Se la utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

La NVRAM tiene las siguientes características y funciones:

- Almacena el archivo de configuración inicial.
  - Retiene el contenido cuando se apaga o reinicia el router.
- **Memoria FLASH:** La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los módulos de memoria en línea simples flash (Simas) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.

La memoria flash tiene las siguientes características y funciones.

- Guarda la imagen del sistema operativo (IOS)
  - Permite que el software se actualice sin retirar ni reemplazar chips en el procesador.
  - Retiene el contenido cuando se apaga o reinicia el router.
  - Puede almacenar varias versiones del software IOS.
  - Es un tipo ROM programable, que se puede borrar electrónicamente (EEPROM).
- **Memoria ROM:** La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS

de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM.

La memoria ROM tiene las siguientes características y funciones.

- Guarda las instrucciones para el diagnóstico de la prueba al inicio (POST).
  - Guarda el programa bootstrap y el software básico del sistema operativo.
  - Requiere del reemplazo de chips que se pueden conectar en el motherboard para las actualizaciones del software.
- **Interfaces:** Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la consola /AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring. Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser configuraciones fijas o modulares.

Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de configuraciones fijas o modulares.

Las interfaces tienen las siguientes características y funciones:

- Conectan el router a la red para permitir que las tramas entren y salgan.
  - Pueden estar en el motherboard o en un módulo aparte.
- **Bus del Sistema:** Éste se utiliza para la comunicación entre el procesador y las interfaces del router.
  - **Bus de CPU:** Se utiliza básicamente para comunicarse entre el procesador y las memorias.

Éste brinda unas funciones básicas a nivel de red como son: las de enrutamiento, escalabilidad a nivel de red, acceso seguro a los recursos de la red, entre otras. La interfaz que posee el IOS de cisco para interactuar con el usuario es una Interfaz de Línea de Comandos (CLI).

- **Fuente de Alimentación:** Ésta brinda la energía necesaria para operar los componentes internos. Los routers de mayor tamaño puede contar con varias fuentes de alimentación o fuentes modulares. En algunos de los routers de menor tamaño, la fuente de alimentación puede ser externa al router.

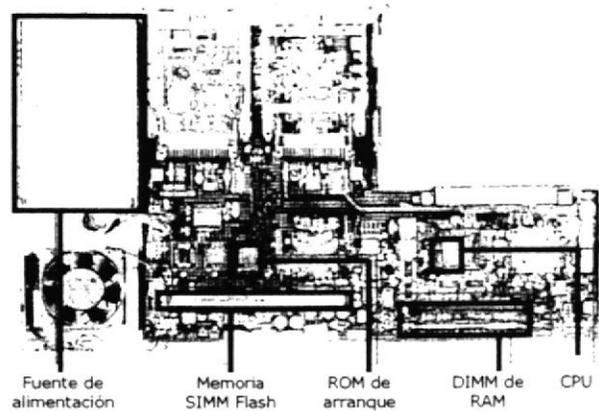


Figura 7.1. Componentes internos del Router

### 7.3 CONEXIONES EXTERNAS DEL ROUTER

La función de los puertos de administración es diferente a la de las otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red por donde se transmiten los paquetes. El puerto de administración proporciona una conexión basada en texto para la configuración y diagnóstico de fallas del router. Los puertos auxiliares y de consola constituyen las interfaces de administración comunes. Estos son puertos seriales asíncronos EIA-232. Están conectados a un puerto de comunicaciones de un computador. El computador debe ejecutar un programa de emulación de Terminal para iniciar la sesión basada en texto con el router.

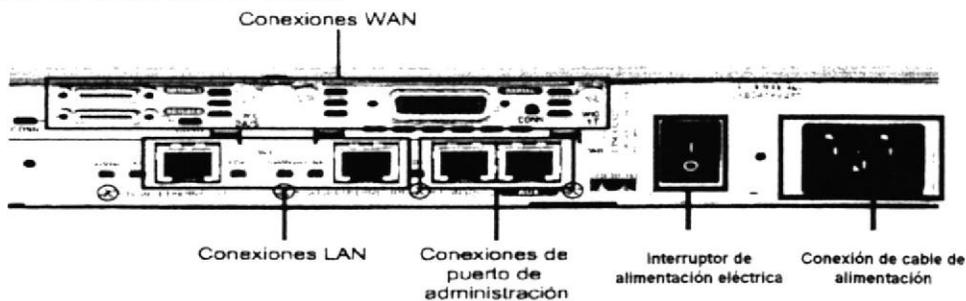


Figura 7.2. Conexiones externas del Router

### 7.4 CONEXIONES DEL PUERTO DE ADMINISTRACIÓN

El puerto de consola y el puerto auxiliar (AUX) son puertos de administración. Estos puertos seriales asíncronos no se diseñaron como puertos de networking. Uno de estos dos puertos es necesario para la configuración inicial del router. Se recomienda el puerto de consola para esta configuración inicial. No todos los routers cuentan con un puerto auxiliar.

Cuando el router entra en servicio por primera vez, los parámetros de networking no están configurados. Por lo tanto, el router no puede comunicarse con ninguna red. Para prepararlo para la puesta en marcha y configuración inicial, conecte una Terminal ASCII RS-232 o un computador que emule una Terminal ASCII Terminal al puerto de consola del sistema. Entonces, se podrán ingresar los comandos de configuración para poner en marcha el router.

Una vez que la configuración inicial se ha introducido en el router a través del puerto de consola o auxiliar, entonces, se puede conectar el router a la red para realizar un diagnóstico de fallas o monitoreo. Además, el router puede configurarse desde un lugar remoto haciendo telnet a una línea de Terminal virtual o marcando el número de un módem conectando al puerto de consola o auxiliar del router.

El puerto de consola es un puerto de administración que se utiliza para proveer acceso al router fuera de banda. Se usa para la configuración inicial del router, el monitoreo y los procedimientos de recuperación de desastres. Para realizar la conexión al puerto de consola, se usa un cable transpuesto o de consola y un adaptador **RJ-45 a DB-9** para conectarse al PC.

Para conectar una Terminal al puerto de consola del router, conecte la Terminal mediante un cable transpuesto **RJ-45 a RJ-45** y un adaptador **RJ-45 a DB-9** o **RJ-45 a DB-25**.

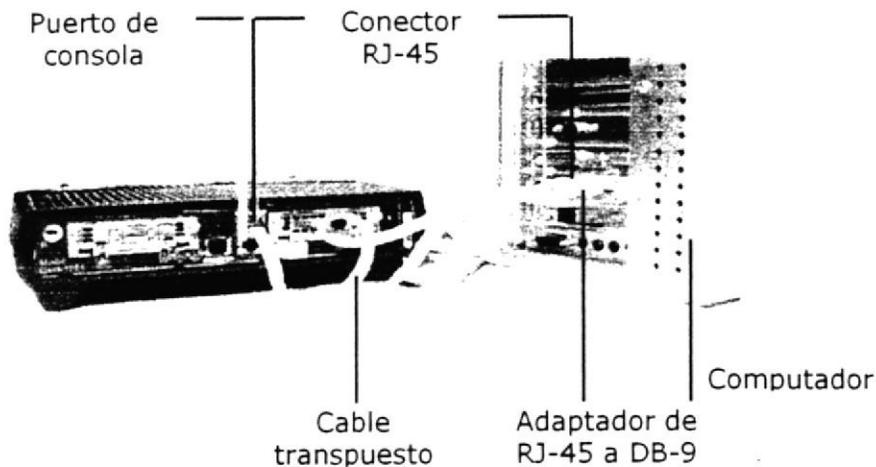


Figura 7.3. Conexiones del puerto de administración

## 7.5 CONFIGURACIONES EN EL ROUTER

### 7.5.1 MODOS DE INTERFAZ DE USUARIO

La interfaz de línea de comando (CLI) de Cisco usa una estructura jerárquica. Esta estructura requiere el ingreso a distintos modos para realizar tareas particulares. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces. Desde el modo de configuración de interfaces, todo cambio de configuración que se realice, tendrá efecto únicamente en esa interfaz en particular.

El IOS suministra un servicio de intérprete de comandos, denominado comando ejecutivo (EXEC). Luego de ingresar un comando, el EXEC lo valida y ejecuta.

Como característica de seguridad, el software Cisco IOS divide las sesiones EXEC en dos niveles de acceso. Estos niveles son el modo EXEC usuario y el modo EXEC privilegiado. El modo EXEC privilegiado también se denomina el modo enable.

Las siguientes son las características resaltantes del modo EXEC usuario y del modo EXEC privilegiado:

- El modo EXEC usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo "de visualización solamente". El nivel EXEC usuario no permite ningún comando que pueda cambiar la configuración del router. El modo EXEC usuario se puede reconocer por la petición de entrada: ">".
- El modo EXEC privilegiado da acceso a todos los comandos del router. Se puede configurar este modo para que solicite una contraseña del usuario antes de dar acceso. Para ingresar al modo de configuración global y a todos los demás específicos, es necesario encontrarse en el modo EXEC privilegiado. El modo EXEC privilegiado se puede reconocer por la petición de entrada "#".

Para ingresar al nivel EXEC privilegiado desde el nivel EXEC usuario, ejecute el comando **enable** con la petición de entrada ">" en pantalla. Si se ha configurado una contraseña, el router solicitará la contraseña. Por razones de seguridad, los dispositivos de red de Cisco no muestran la contraseña al ser introducida. Una vez que se ha introducido la contraseña correcta, la petición de entrada del router cambia a "#", lo que indica que el usuario se encuentra ahora en el nivel EXEC privilegiado. Si se introduce un signo de interrogación (?) en el nivel EXEC privilegiado, se mostrarán muchas opciones de comando, adicionales a las disponibles en el nivel EXEC usuario.

A continuación verá un esquema de los diferentes usuarios y a los permisos que tiene cada uno:

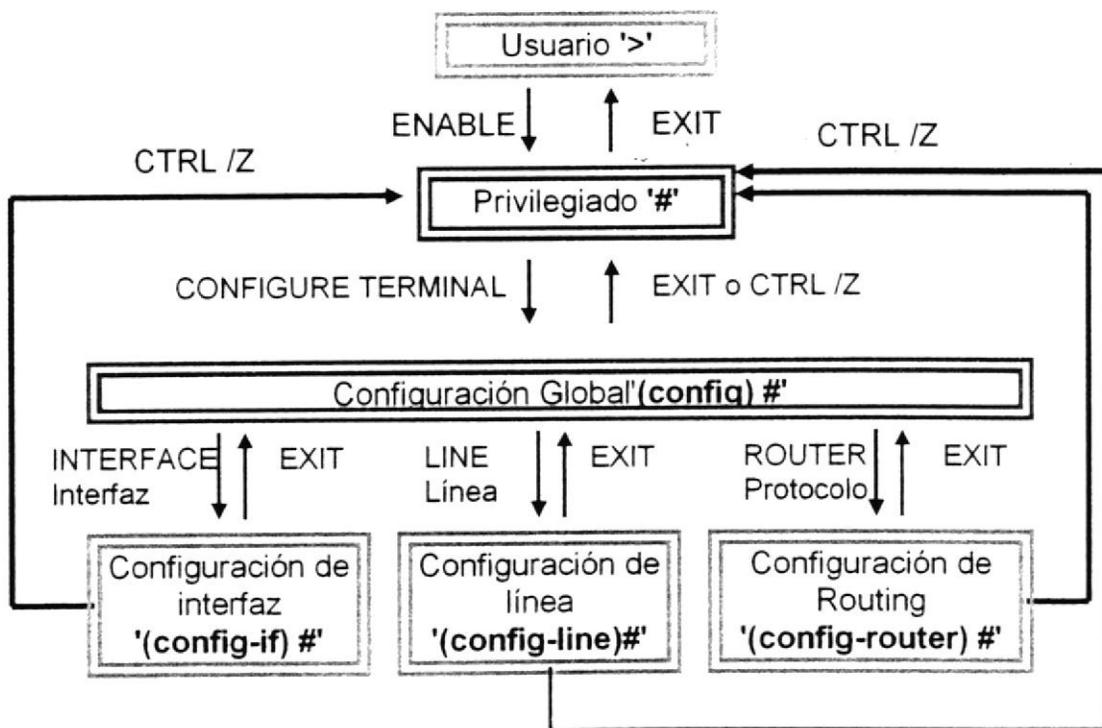


Figura 7.4. Esquema de permisos tipos de usuarios

Sólo se puede ingresar al modo de configuración global desde el modo EXEC privilegiado. Los siguientes son modos específicos a los que también se puede ingresar desde el modo de configuración global.

- Interfaces
- Sub-interfaces
- Línea
- Router
- Mapas de enrutamiento.

Para regresar al modo EXEC usuario desde el modo EXEC privilegiado, se pueden ejecutar los comandos **disable** o **exit**. Para regresar al modo EXEC privilegiado desde el modo de configuración global, ejecute **exit** o **CTRL Z**.

**CTRL Z** también se puede usar para regresar directamente al modo EXEC privilegiado desde cualquier modo de configuración global secundario.

Para ingresar al modo EXEC privilegiado, escriba **enable** o su abreviatura **ena**. Esto puede hacer que el router pida una contraseña, que se haya fijado con anterioridad.

```

Router con0 is now available

Press RETURN to get started.

Password:
Router>
Router>enable
Password:
Router#
Router#disable
Router>
Router>exit
  
```

← Símbolo del EXEC Usuario

← Símbolo del EXEC Privilegiado

Figura 7.5. Pantalla tipos de usuario

Los comandos del modo de configuración global se utilizan en un router para ejecutar comandos de configuración que afectan al sistema como un todo.

```

Router con0 is now available

Press RETURN to get started.

Password:
Router>
Router>enable
Password:
Router#
Router#configure terminal
Router(config)#
  
```

Figura 7.6. Pantalla tipos de Interfaz de Usuario

El modo de configuración global, a menudo abreviado como "**global config**", es el modo de configuración principal. Estos son algunos de los modos de operación a los que se puede ingresar desde el modo de configuración global:

- Modo de interfaz
- Modo de línea
- Modo de router
- Modo de subinterfaz
- Modo de controlador

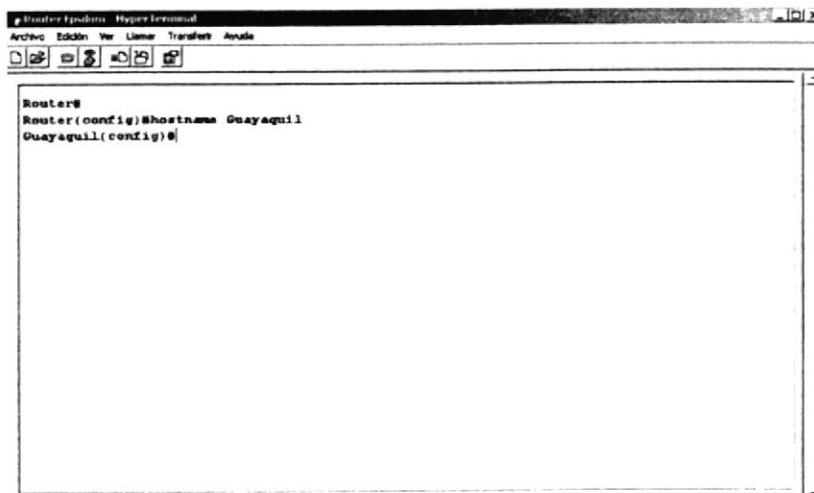
Al ingresar a estos modos específicos, la petición de entrada del router cambia para señalar el modo de configuración en uso. Todo cambio de configuración que se realice, tendrá efecto únicamente en las interfaces o procesos relativos a ese modo particular.

Al escribir **exit** desde alguno de estos modos de configuración específicos, el router regresa al modo de configuración global. Al presionar **CTRL Z**, se sale por completo del modo de configuración y el router vuelve al modo EXEC privilegiado.

### 7.5.2 CONFIGURACIÓN DEL NOMBRE DE ROUTER

Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante el comando **hostname** seguido del nombre que le asigne al router.

Al presionar la tecla **enter**, la petición de entrada ya no mostrará el nombre de host por defecto (**Router**), sino el nombre de host que se acaba de configurar.



```
Router#
Router(config)#hostname Guayaquil
Guayaquil(config)#
```

Figura 7.7. Pantalla configuración del nombre del Router

### 7.5.3 CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER

Las contraseñas restringen el acceso a los routers. Se debe siempre configurar contraseñas para las líneas de terminales virtuales y para la línea de consola. Las contraseñas también se usan para controlar el acceso al modo EXEC privilegiado, a fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración.

Aunque es opcional, se recomienda configurar una contraseña para la línea de comando. Los siguientes comandos se utilizan para fijar dicha contraseña.

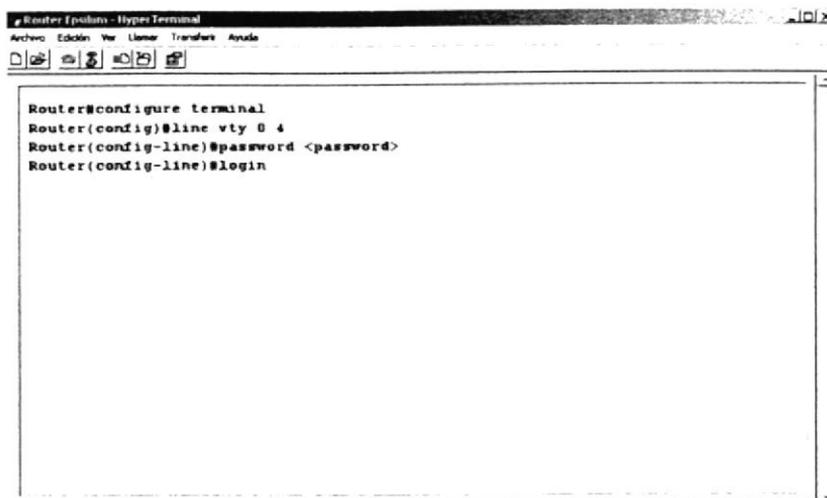


```
Router#configure terminal
Router(config)#line console 0
Router(config-line)#password <password>
Router(config-line)#login
```

Figura 7.8. Pantalla configuración de contraseña del usuario privilegiado

Se debe fijar contraseñas en una o más de las líneas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante Telnet.

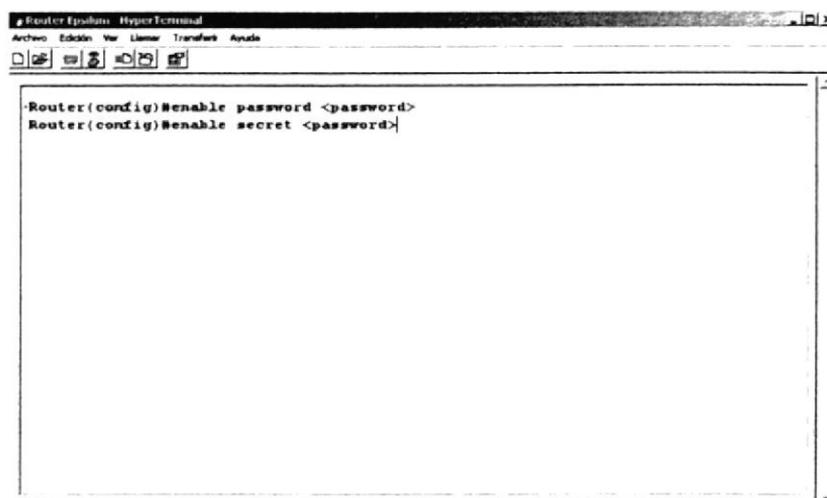
Normalmente, los routers Cisco permiten cinco líneas de VTY identificados del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY. Se suele usar la misma contraseña para todas las líneas, pero a veces se reserva una línea mediante una contraseña exclusiva, para que sea posible el acceso al router aunque haya demanda de más de cuatro conexiones. Los siguientes comandos se utilizan para establecer contraseñas en las líneas de VTY.



```
Router#configure terminal
Router(config)#line vty 0 4
Router(config-line)#password <password>
Router(config-line)#login
```

Figura 7.9. Pantalla configuración de contraseña para el acceso remoto por telnet

Los comandos **enable password** y **enable secret** se utilizan para restringir el acceso al modo EXEC privilegiado. El comando **enable password** se utiliza sólo si no se ha configurado previamente **enable secret**. Se recomienda habilitar siempre **enable secret**, ya que a diferencia de **enable password**, la contraseña estará siempre cifrada. Estos son los comandos que se utilizan para configurar las contraseñas.



```
Router(config)#enable password <password>
Router(config)#enable secret <password>
```

Figura 7.10. Pantalla cifrado de contraseñas

En ocasiones es deseable evitar que las contraseñas se muestren en texto sincifrar al ejecutar los comandos **show running-config** o **show startup-config**. El siguiente comando se utiliza para cifrar las contraseñas al mostrar los datos de configuración:

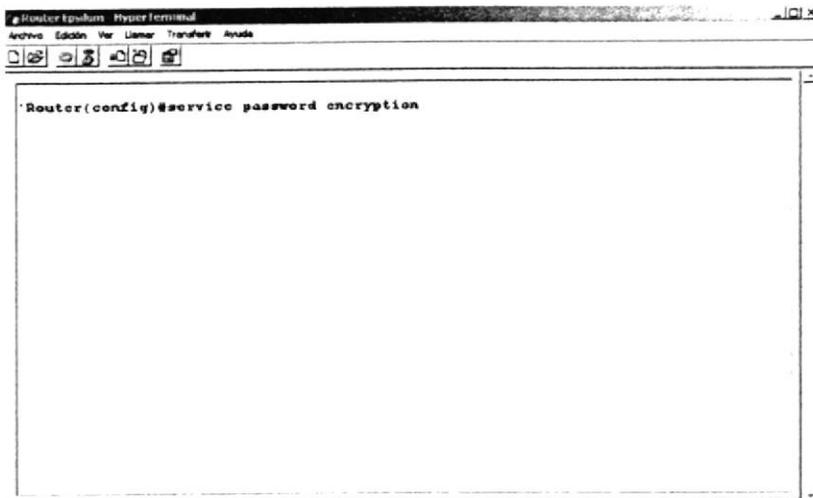


Figura 7.11. Pantalla encriptación de contraseñas

El comando **service password-encryption** aplica un cifrado débil a todas las contraseñas sin cifrar. El comando **enable secret <password>** usa un fuerte algoritmo MD5 para cifrar.

#### 7.5.4 AYUDA MEDIANTE EL TECLADO EN LA INTERFAZ DE LÍNEA DE COMANDO

Al escribir un signo de interrogación (?) en la petición de entrada del modo usuario o del modo privilegiado, aparece una útil lista de los comandos disponibles. Observe el "--More--" (Más) que aparece en la parte inferior de la pantalla de muestra. La pantalla muestra varias líneas a la vez. La petición de entrada "--More--" que aparece en la parte inferior de la pantalla indica que hay más pantallas disponibles.



Figura 7.12. Pantalla ayuda en la interfaz de línea de comando

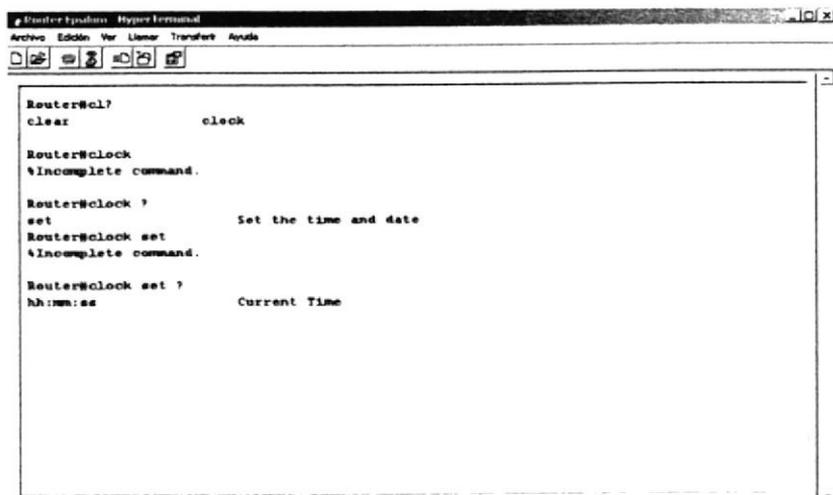
Esto se lo puede utilizar con cualquier comando, por ejemplo si un usuario desea configurar el reloj del router pero no sabe cuál es el comando adecuado, puede usar la función de ayuda para conocer cuál es el comando correcto. El ejercicio siguiente ilustra uno de los muchos usos de la función de ayuda.

La tarea es configurar el reloj del router. Considere que no conoce el comando correspondiente, y efectúe lo siguiente:

**Paso 1** Use? Para encontrar el comando adecuado para configurar el reloj. El resultado de la ayuda indica que se requiere el comando **clock** (reloj).

**Paso 2** Verifique la sintaxis para hacer cambios en la hora.

**Paso 3** Introduzca la hora actual en horas, minutos y segundos, tal como se muestra en la figura de abajo. El sistema indica que se debe suministrar información adicional para completar el comando.



```
Router#?
clear          clock

Router#clock
%incomplete command.

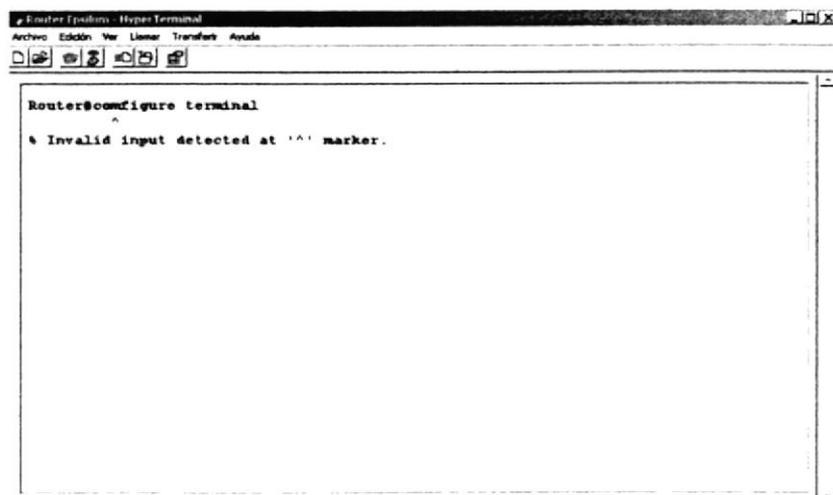
Router#clock ?
set            Set the time and date
Router#clock set
%incomplete command.

Router#clock set ?
hh:mm:ss      Current Time
```

Figura 7.13. Pantalla configuración del reloj del router

### 7.5.5 DIAGNÓSTICO DE FALLAS DE LOS ERRORES DE LÍNEA DE COMANDOS

Los errores de línea de comandos se producen principalmente debido a errores de teclado. Si un comando es escrito de forma incorrecta, la interfaz del usuario muestra el error mediante un indicador de error (^). El símbolo “^” aparece en el punto de la cadena del comando donde se colocó el comando, palabra clave o argumento incorrecto.



```
Router#configure terminal
^
% Invalid input detected at '^' marker.
```

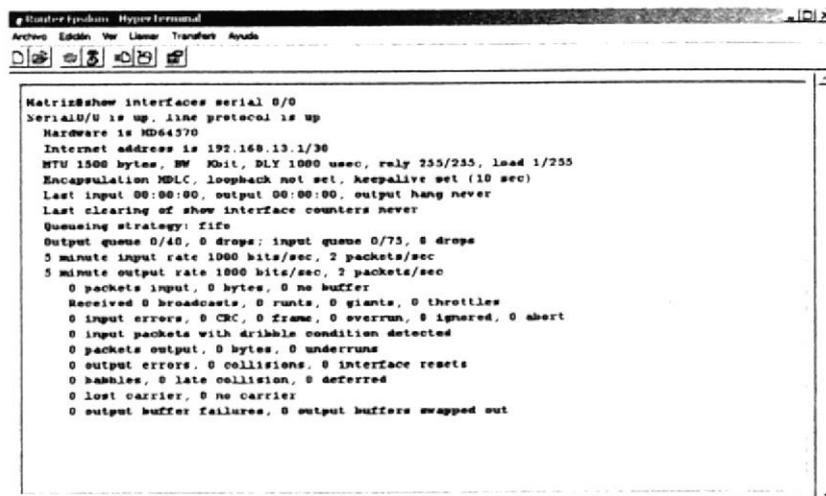
Figura 7.14. Pantalla diagnóstico de fallos

Si una línea de comando es escrita de forma incorrecta y se presiona la tecla **enter**, se puede presionar la tecla flecha-arriba para reescribir el último comando. Use las teclas flecha-derecha e izquierda para mover el cursor hasta el lugar donde se cometió el error. Luego escriba la corrección necesaria. Si es necesario eliminar algo, use la tecla retroceso.

## 7.6 USO DE LOS COMANDOS SHOW

Los numerosos comandos **show** se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas. Tanto en el modo EXEC privilegiado como en el modo EXEC de usuario, el comando **show ?** muestra una lista de los comandos **show** disponibles. La lista en el modo EXEC privilegiado es considerablemente más larga que en el modo EXEC de usuario.

- **Show interfaces:** Muestra las estadísticas completas de todas las interfaces del router.

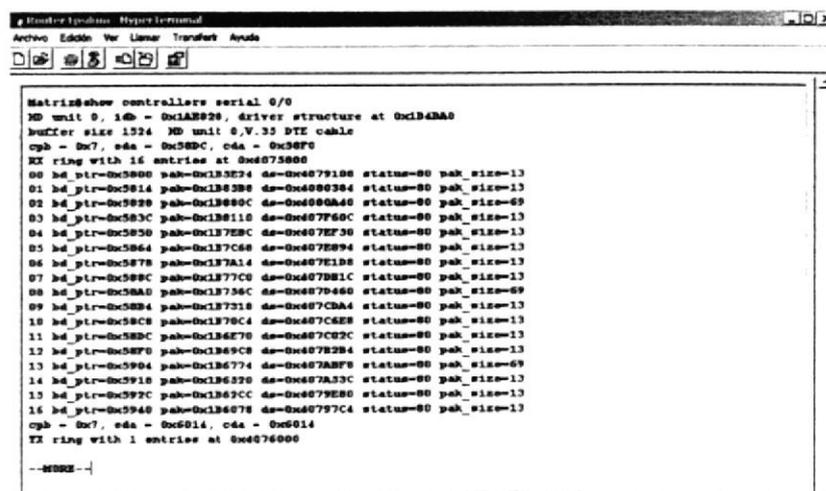


```

Matrix#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is HD64370
  Internet address is 192.168.13.1/30
  MTU 1500 bytes, BW 30Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of show interface counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
  
```

Figura 7.15. Pantalla comando show interfaces

- **Show controllers serial:** Muestra información específica de la interfaz de hardware. El comando debe incluir el número de puerto y/o de ranura de la interfaz.



```

Matrix#show controllers serial 0/0
MD unit 0, 160 - 0x1A8228, driver structure at 0xc148A0
buffer size 1524 MD unit 0,V.33 DTE cable
cph - 0x7, eba - 0x58DC, cda - 0x38F0
XX ring with 16 entries at 0xc075800
00 hd_ptr=0x5800 pab=0x183E24 da=0x4079108 status=00 pak_size=13
01 hd_ptr=0x5814 pab=0x183E28 da=0x4080364 status=00 pak_size=13
02 hd_ptr=0x5828 pab=0x183E3C da=0x40808d0 status=00 pak_size=09
03 hd_ptr=0x583C pab=0x183E10 da=0x407F6C0 status=00 pak_size=13
04 hd_ptr=0x5850 pab=0x187EBC da=0x407EF30 status=00 pak_size=13
05 hd_ptr=0x5864 pab=0x187C48 da=0x407E894 status=00 pak_size=13
06 hd_ptr=0x5878 pab=0x187A14 da=0x407E1D8 status=00 pak_size=13
07 hd_ptr=0x588C pab=0x1877C0 da=0x407D81C status=00 pak_size=13
08 hd_ptr=0x58A0 pab=0x18756C da=0x407D460 status=00 pak_size=09
09 hd_ptr=0x58B4 pab=0x187318 da=0x407C8A4 status=00 pak_size=13
10 hd_ptr=0x58C8 pab=0x1870C4 da=0x407C6E8 status=00 pak_size=13
11 hd_ptr=0x58DC pab=0x186E70 da=0x407C2CC status=00 pak_size=13
12 hd_ptr=0x58F0 pab=0x186C9C da=0x407B2B4 status=00 pak_size=13
13 hd_ptr=0x5904 pab=0x186774 da=0x407A8F0 status=00 pak_size=09
14 hd_ptr=0x5918 pab=0x186320 da=0x407A33C status=00 pak_size=13
15 hd_ptr=0x593C pab=0x1859CC da=0x4079E20 status=00 pak_size=13
16 hd_ptr=0x5960 pab=0x184E78 da=0x40797C4 status=00 pak_size=13
cph - 0x7, eba - 0x5814, cda - 0x3814
XX ring with 1 entries at 0xc076000
--MORE--
  
```

Figura 7.16. Pantalla comando show interfaces

- **Show clock:** Muestra la hora fijada en el router.
- **Show hosts:** Muestra la lista en caché de los nombres de host y sus direcciones.
- **Show users:** Muestra todos los usuarios conectados al router.
- **Show history:** Muestra un historial de los comandos ingresados.
- **Show flash:** Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí.
- **Show version:** Despliega la información acerca del router y de la imagen de IOS que esté corriendo en la RAM. Este comando también muestra el valor del registro de configuración del router.
- **Show ARP:** Muestra la tabla ARP del router
- **Show protocols:** Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado.
- **Show startup-configuration:** Muestra el archivo de configuración almacenado en la NVRAM.
- **Show running-configuration:** Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

### 7.6.1 CONFIGURACIÓN DE UNA INTERFAZ SERIAL

Es posible configurar una interfaz serial desde la consola o a través de una línea de Terminal Virtual. Siga estos pasos para configurar una interfaz serial:

1. Ingrese al modo de configuración global.
2. Ingrese al modo de configuración de interfaz.
3. Especifique la dirección de la interfaz y la máscara de subred.
4. Si el cable de conexión es DCE, fije la velocidad de sincronización. Omita este paso si el cable es DTE.
5. Active la interfaz.

A cada interfaz serial activa se le debe asignar una dirección IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP. Configure la dirección de IP mediante los siguientes comandos:



```
#Router [posible] Hyper Terminal
Archivo Edición Ver Línea Transferir Ayuda
Router(config)#interface serial 0
Router(config-if)#ip address <ip address> <netmask>
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

Figura 7.17. Pantalla configuración de una interfaz serial DCE

Las interfaces seriales necesitan una señal de sincronización que controle la comunicación. En la mayoría de los entornos, un dispositivo DCE, por ejemplo un CSU, proporciona dicha señal. Por defecto, los routers Cisco son dispositivos DTE, pero se pueden configurar como dispositivo DCE.

Tal vez, las interfaces de router que más se usan en los servicios WAN son las interfaces seriales.

Los routers Cisco pueden usar diferentes conectores para las interfaces seriales. La interfaz de la izquierda es una interfaz serial inteligente. La interfaz de la derecha es una conexión DB-60. Esto hace que la selección del cable

serial que conecta el sistema de la red a los dispositivos seriales sea una parte fundamental de la configuración de una WAN.

El DTE y el DCE son dos tipos de interfaces seriales que los dispositivos usan para comunicarse. La diferencia clave entre los dos es que el dispositivo DCE proporciona la señal reloj para las comunicaciones en el bus. La documentación del dispositivo debe especificar si es DTE o DCE.

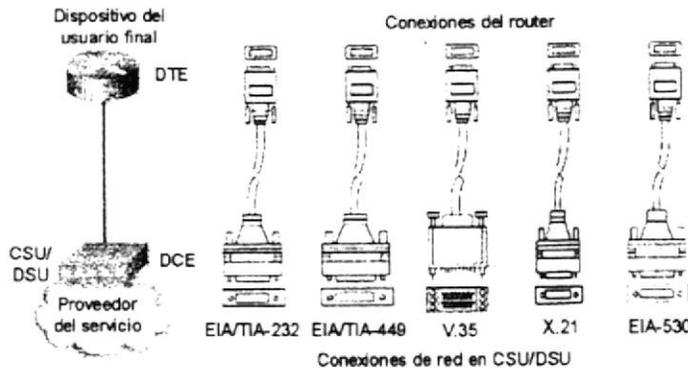


Figura 7.18. Conexiones del Router DCE/DTE

Cada dispositivo podría requerir un estándar serial diferente. Cada estándar define las señales del cable y especifica el conector del extremo del cable. Siempre se debe consultar la documentación del dispositivo para obtener información sobre el estándar de señalización.

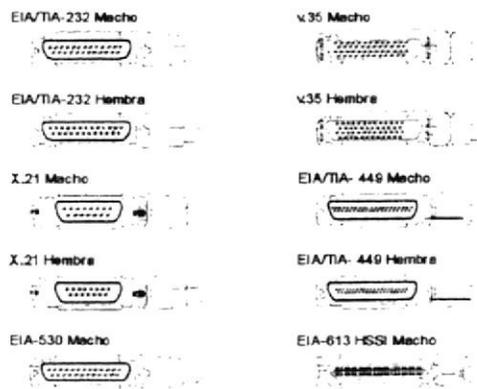


Figura 7.19. Tipos de seriales de un router

Si el conector tiene pines salientes visibles, es macho. Si el conector tiene tomas para los pines salientes, es hembra.

En los enlaces seriales interconectados directamente, un extremo debe considerarse como un DCE y debe proporcionar la señal de sincronización. Se activa la sincronización y se fija la velocidad mediante el comando **clock rate**.

Las velocidades de sincronización disponibles (en bits por segundo) son: 56000, 64000, 72000, etc... No obstante, es posible que algunas de estas velocidades no estén disponibles en algunas interfaces seriales, según su capacidad.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o de diagnóstico de fallas, se utiliza el comando **shutdown** para desactivarla.

Se utilizará una velocidad de sincronización de 64000. Los comandos para fijar la velocidad de sincronización y activar una interfaz serial son los siguientes:



```
Router Emulador - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Router(config)#interface serial 0
Router(config-if)#ip address <ip address> <netmask>
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

Figura 7.20. Pantalla configuración de una interfaz serial DCE

## 7.6.2 CONFIGURACIÓN DE UNA INTERFAZ ETHERNET

Se puede configurar una interfaz Ethernet desde la consola o a través de una línea de Terminal virtual. A cada interfaz Ethernet activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

Para configurar una interfaz Ethernet, siga estos pasos:

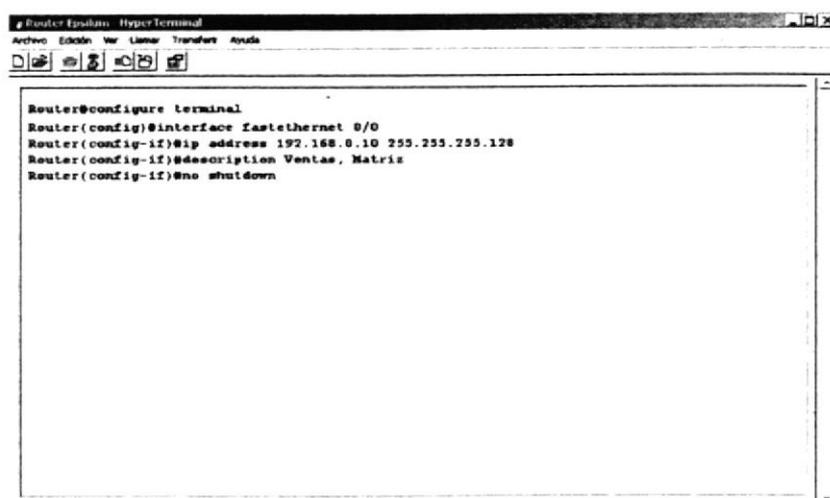
1. Ingrese al modo de configuración global.
2. Ingrese al modo de configuración de interfaz.
3. Especifique la dirección de la interfaz y la máscara de subred.
4. Active la interfaz.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ejecuta el comando **no shutdown**.

Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o diagnóstico de fallas, se utiliza el comando **shutdown** para desactivarla.

## 7.6.3 DESCRIPCIÓN DE INTERFACES

La descripción de las interfaces se emplea para indicar información importante, como puede ser la relativa a un router distante, el número de un circuito, o un segmento de red específico. La descripción de la interfaz puede ayudar a un usuario de red a recordar información específica de la interfaz, como por ejemplo, a cuál red atiende dicha interfaz. La descripción es sólo un comentario escrito acerca de la interfaz.



```
Router@configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.0.10 255.255.255.128
Router(config-if)#description Ventas, Matris
Router(config-if)#no shutdown
```

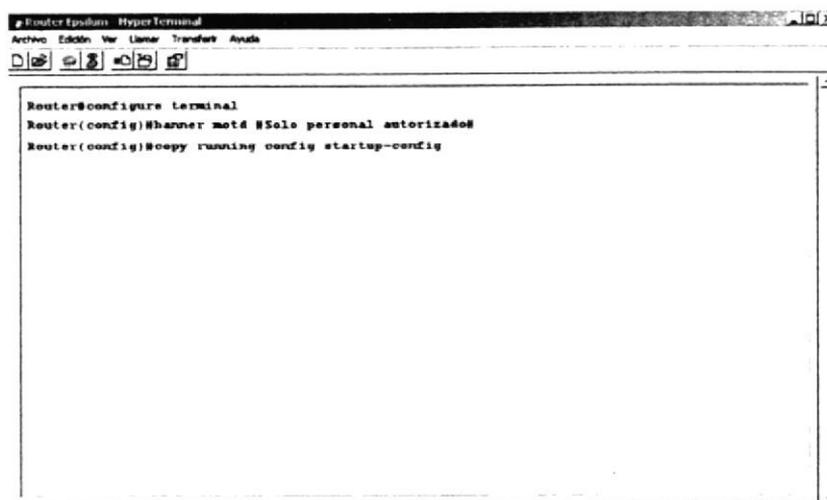
Figura 7.21. Pantalla descripción de interfaces

#### 7.6.4 CONFIGURACIÓN DEL MENSAJE DEL DÍA (MOTD)

Ingrese al modo de configuración global para configurar un texto como mensaje del día (MOTD). Use el comando `banner motd`, seguido de un espacio y un delimitador, como por ejemplo el signo numeral (#). Escriba el mensaje del día (MOTD) seguido de un espacio y de nuevo el delimitador.

Siga estos pasos para crear y mostrar un mensaje del día:

- Ingrese al modo de configuración global, mediante el comando **configure Terminal**.
- Escriba el comando `banner motd # solo persona autorizado #`.
- Guarde los cambios mediante el comando `copy running-config startup-config`.



```
Router#configure terminal
Router(config)#banner motd #Solo personal autorizado#
Router(config)#copy running-config startup-config
```

Figura 7.22. Pantalla configuración de mensaje del Día

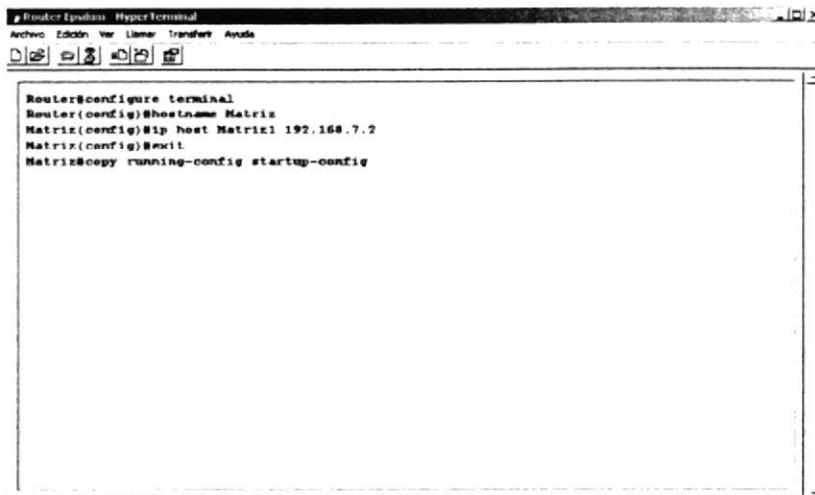


## 7.7 CONFIGURACIÓN DE TABLAS DE HOST

Para asignar nombres de host a direcciones, primero ingrese al modo de configuración global. Ejecute el comando **ip host** seguido del nombre de destino y todas las direcciones de IP con las que se puede llegar al dispositivo.

El procedimiento para configurar la tabla de host es:

- Ingrese al modo de configuración global en el router.
- Ejecute el comando **ip host** seguido del nombre del router y todas direcciones de IP asociadas con las interfaces en cada router.
- Repita el proceso, hasta que todos los routers de la red hayan sido configuradas.
- Guarde la configuración en la NVRAM.



```
Router#configure terminal
Router(config)#hostname Matrix
Matrix(config)#ip host Matrix1 192.168.7.2
Matrix(config)#exit
Matrix#copy running-config startup-config
```

Figura 7.23. Pantalla configuración de tablas de host

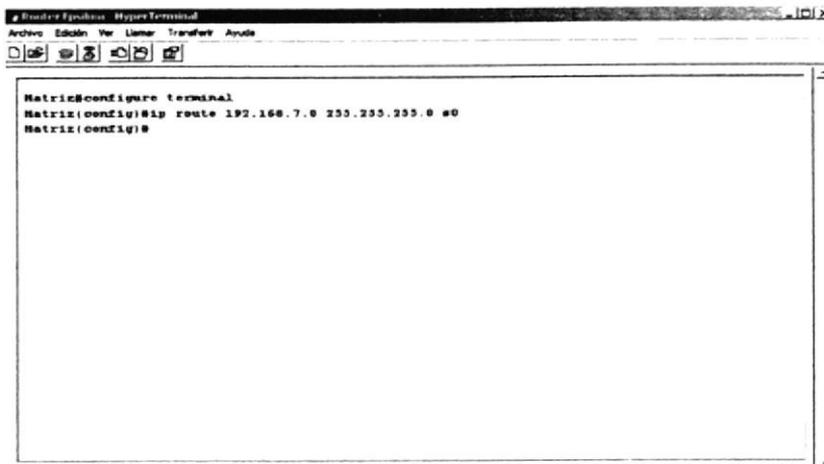
## 7.7.1 ENRUTAMIENTO

### 7.7.1.1 ENRUTAMIENTO ESTÁTICO

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:

- El administrador de red configura la ruta.
- El router instala la ruta en la tabla de enrutamiento.
- Los paquetes se enrutan de acuerdo a la ruta estática.

Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando **ip router**.



```
Router-Espolans - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
[Icons]
-----
Matrix#configure terminal
Matrix(config)#ip route 192.168.7.0 255.255.255.0 #0
Matrix(config)#
```

Figura 7.24. Pantalla configuración de enrutamiento estático

La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. Un valor menor de distancia administrativa indica una ruta más confiable. La distancia administrativa por defecto cuando se usa una ruta estática es 1.

Para verificar la distancia administrativa de una ruta en particular use el comando **show ip route address**, donde la dirección ip de dicha ruta se inserta en la opción **address**. Si se desea una distancia administrativa diferente a la distancia por defecto, se introduce un valor entre 0 y 255 después de la interfaz de salida o el siguiente salto, como se muestra a continuación:



```
Router-Espolans - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
[Icons]
-----
Matrix#configure terminal
Matrix(config)#ip route 172.16.7.0 255.255.255.0 172.16.4.1 130
Matrix(config)#
```

Figura 7.25. Pantalla configuración de enrutamiento estático 2

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta. A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

### 7.7.1.2 ENRUTAMIENTO POR DEFECTO

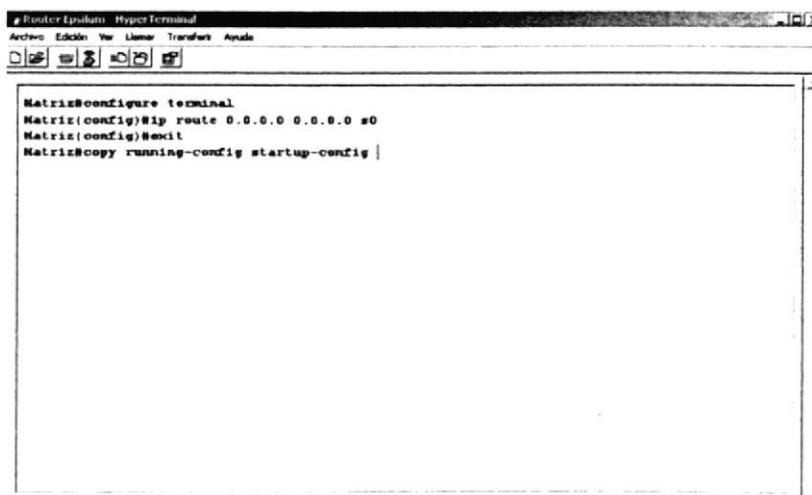
Las rutas por defecto se usan para enviar paquetes a destinos que no coinciden con los de ninguna de las otras rutas en la tabla de enrutamiento. Generalmente, los routers están configurados con una ruta por defecto para el tráfico que se dirige a la Internet, ya que a menudo resulta poco práctico e innecesario mantener rutas hacia todas las redes de la Internet. En realidad, una ruta por defecto es una ruta estática especial que utiliza este formato:

```
Router (config) #ip route 0.0.0.0 0.0.0.0 s0
```

La máscara 0.0.0.0, cuando se ejecuta el AND lógico hacia la dirección de IP de destino del paquete, siempre obtiene la red 0.0.0.0. Si el paquete no coincide con una ruta más específica en la tabla de enrutamiento, será enviado hacia la red 0.0.0.0.

Siga estos pasos para configurar rutas por defecto.

1. Ingrese al modo de configuración global.
2. Ejecute el comando **ip route** con **0.0.0.0** como la dirección de red de destino y **0.0.0.0** como máscara de subred. La opción **address** para la ruta por defecto puede ser la interfaz del router local que está conectado a las redes externas, o puede ser la dirección IP del router del siguiente salto. En la mayoría de los casos, es preferible especificar la dirección IP del router del siguiente salto.
3. Salga del modo de configuración global.
4. Guarde la configuración activa en la NVRAM mediante el comando **copy running-config startup-config**.



```
Matriz#configure terminal
Matriz(config)#ip route 0.0.0.0 0.0.0.0 s0
Matriz(config)#exit
Matriz#copy running-config startup-config |
```

Figura 7.26. Pantalla configuración de enrutamiento por defecto

### 7.7.1.3 ENRUTAMIENTO DINÁMICO

El enrutamiento dinámico significa que el router va averiguando las rutas para llegar al destino de actualizaciones periódicas enviadas desde otros routers.

#### 7.7.1.3.1 PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento son diferentes a los protocolos enrutados tanto en su función como en su tarea.

Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.

Ejemplos de protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP).
- Protocolo de enrutamiento de Gateway interior (IGRP).
- Protocolo de enrutamiento de Gateway interior mejorada (EIGRP).
- Protocolo "Primero la ruta más corta"(OSPF).
- Protocolo de enrutamiento exterior por vector- distancia (BGP).

Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

Ejemplos de protocolos enrutados

- Protocolo Internet (IP).
- Intercambio de paquetes de internetwork (IPX).

El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos. Cuando todos los routers de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia.

#### 7.7.1.3.1.1 TIPOS DE PROTOCOLOS DE ENRUTAMIENTO

El Protocolo de información de enrutamiento (RIP). Sus características principales son las siguientes:

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete es desechado.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

El Protocolo de enrutamiento interior de Gateway (IGRP) es un protocolo patentado desarrollado por Cisco. Entre las características de diseño claves del IGRP se destacan las siguientes:

- Es un protocolo de enrutamiento por vector-distancia.
- Se considera el ancho de banda, la carga, el retardo y la confiabilidad para crear una métrica compuesta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

El EIGRP es un protocolo mejorado de enrutamiento por vector-distancia, patentado por Cisco. Las características claves del EIGRP son las siguientes:

- Es un protocolo mejorado de enrutamiento por vector-distancia.
- Utiliza balanceo de carga asimétrico.
- Utiliza una combinación de los algoritmos de vector-distancia y de estado del enlace.
- Utiliza el algoritmo de actualización difusa (DUAL) para el cálculo de la ruta más corta.
- Las actualizaciones son mensajes de multicast a la dirección 224.0.0.10 generadas por cambios en la topología.

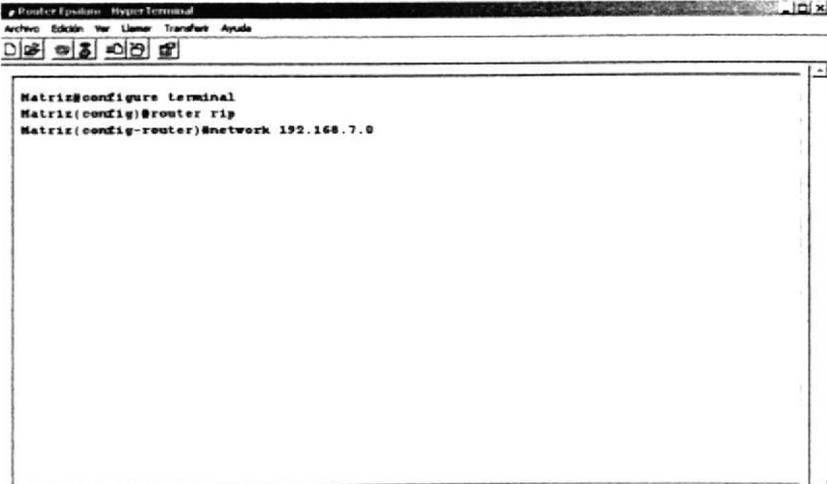
#### 7.7.1.4 PROTOCOLOS DE ENRUTAMIENTO RIP

El Protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento por vector-distancia, en uso en miles de redes en todo el mundo. El hecho que RIP se basa en estándares abiertos y que sea de fácil implementación hace que resulte atractivo para algunos administradores de redes, aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados.

RIP ha evolucionado a lo largo de los años desde el Protocolo de enrutamiento con definición de clases, RIP Versión (RIP v1), hasta el Protocolo de enrutamiento sin clase, RIP Versión 2 (RIP v2).

Para configurar RIP v1 empezará digitando el comando **router** el cual inicia el proceso de enrutamiento.

El comando **network** es necesario, ya que permite que el proceso de enrutamiento determine cuáles son las interfaces que participan en el envío y la recepción de las actualizaciones de enrutamiento.



```
Router-Espol> HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Matrix#configure terminal
Matrix(config)#router rip
Matrix(config-router)#network 192.168.7.0
```

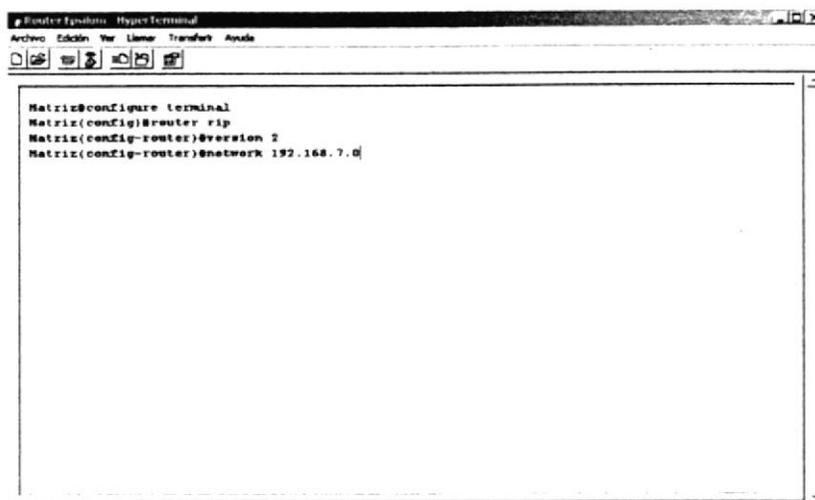
Figura 7.27. Pantalla configuración de Protocolo RIP v1

### 7.7.1.4.1 MEJORAS EN RIP V2

Capacidad para transportar mayor información relativa al enrutamiento de paquetes. Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de las tablas. Soporta enmascaramiento de subredes de longitud variable (VLSM).

Entre las tareas opcionales se encuentran:

- Aplicar compensaciones a la métrica de enrutamiento.
- Ajustar los temporizadores.
- Especificar una versión de RIP.
- Habilitar la autenticación de RIP.
- Configurar el resumen de las rutas en una interfaz.
- Verificar el resumen de las rutas IP.
- Inhabilitar el resumen automático de rutas.

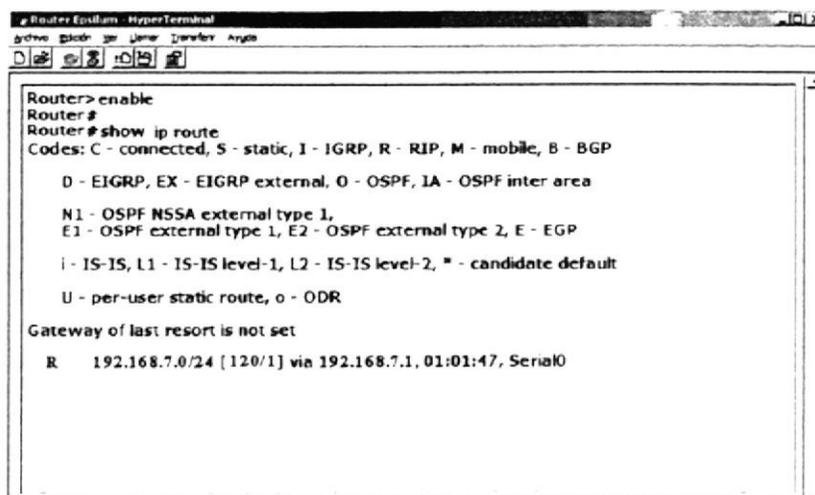


```

Router-Equiliam - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Matriz@configure terminal
Matriz(config)#router rip
Matriz(config-router)#version 2
Matriz(config-router)#network 192.168.7.0
  
```

Figura 7.28. Pantalla configuración de protocolos Rip V2

El comando **show ip route** se puede utilizar para verificar que las rutas recibidas por los routers RIP vecinos estén instaladas en la tabla de enrutamiento. Examine el resultado del comando y busque las rutas RIP que señaladas con "R". Recuerde que la red tardará algún tiempo en converger, de modo que puede que no aparezcan las rutas de forma inmediata.



```

Router-Equiliam - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Router> enable
Router#
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1,
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route, o - ODR
Gateway of last resort is not set

R    192.168.7.0/24 [120/1] via 192.168.7.1, 01:01:47, Serial0
  
```

Figura 7.29. Pantalla comando show ip route

### 7.7.1.5 PROTOCOLOS DE ENRUTAMIENTO DE ESTADO DEL ENLACE

Los algoritmos de estado del enlace también se conocen como SPF (“primero la ruta más corta”). Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. El algoritmo de vector-distancia provee información indeterminada sobre las redes lejanas y no tiene información acerca de los routers distantes. El algoritmo de enrutamiento de estado del enlace mantiene información completa sobre routers lejanos y su interconexión.

El algoritmo SPF determina la conectividad de la red. El router construye esta topología lógica en forma de árbol, con él mismo como raíz, y cuyas ramas son todas las rutas posibles hacia cada subred de la red. Luego ordena dichas rutas, y coloca la ruta más corta primero (SPF). El router que primero conoce de un cambio en la topología envía la información al resto de los routers, para que puedan usarla para hacer sus actualizaciones y publicaciones.

El protocolo público conocido como “Primero la ruta más corta” (OSPF) es un protocolo de enrutamiento de estado del enlace no patentado. Las características clave del OSPF son las siguientes:

- Es un protocolo de enrutamiento de estado del enlace.
- Es un protocolo de enrutamiento público (open Standard).
- Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.
- Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

El Protocolo de Gateway de frontera (BGP) es un protocolo de enrutamiento exterior.

Las características claves del BGP son las siguientes:

- Es un protocolo de enrutamiento exterior por vector-distancia
- Se usa entre ISP o entre los ISPs y sus clientes
- Se usa para enlutar el tráfico de Internet entre sistemas autónomos.

#### 7.7.1.5.1 PROTOCOLO DE ENRUTAMIENTO OSPF

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). El término “libre” en “Primero la ruta libre más corta” significa que está abierto al público y no es propiedad de ninguna empresa.

OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes. Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento.

OSPF es apropiado para Internet Works grandes, escalables y la mejor ruta se determina a base de la velocidad del enlace. OSPF selecciona la ruta mediante el costo, una métrica basada en el ancho de banda. Los routers que

implementan los protocolos de vector-distancia necesitan menos memoria y menos potencia de procesamiento que los que implementan el protocolo OSPF.

OSPF ofrece soluciones a los siguientes problemas:

- Velocidad de convergencia.
- Admite la máscara de subred de longitud variable (VLSM).
- Tamaño de la red.
- Selección de ruta.
- Agrupación de miembros.

#### 7.7.1.5.1.1 TIPOS DE RED OSPF

Las interfaces OSPF reconocen tres tipos de redes:

- Multiacceso OSPF reconocen tres tipos de redes.
- Redes punto a punto.
- Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay.

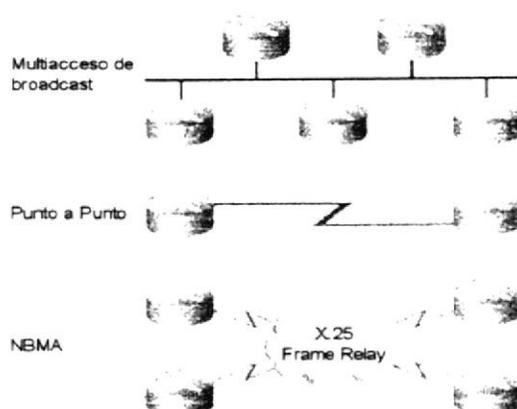


Figura 7.30. Pantalla tipos de red OSPF

#### 7.7.1.5.1.2 PROTOCOLOS HELLO DE OSPF

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete hello y sigue enviando hellos a intervalos regulares. Las reglas de intercambio de paquetes hello de OSPF se denominan protocolo Hello.

En la capa 3 del modelo OSI, los paquetes hello es direccional hacia la dirección multicast 224.0.0.5. Esta dirección equivale a "todos los routers OSPF". Los routers OSPF utilizan los paquetes hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los hellos se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes NBMA, como por ejemplo Frame Relay, el tiempo por defecto es de 30 segundos.

En las redes multiacceso el protocolo hello elige un router designado (DR) y un router designado de respaldo (BDR). El paquete hello transmite información para la cual todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

La configuración de OSPF requiere que el proceso de enrutamiento esté activo en el router con las direcciones de red y la información de área especificadas.

Para habilitar el enrutamiento **OSPF**, utilice la sintaxis de comando de configuración global:

```
Router (config) #router ospf process-id
```

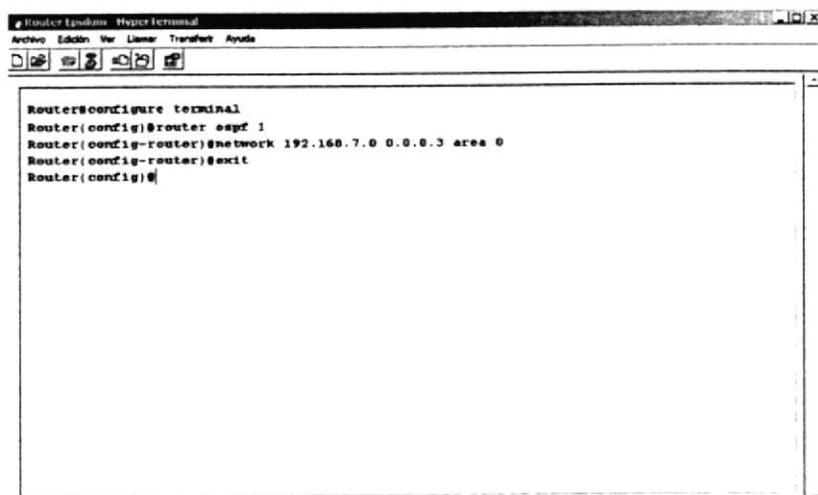
El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en el router. Se pueden iniciar varios procesos OSPF en el mismo router. El número puede tener cualquier valor entre 1 y 65.535.

```
Router (config-router) #network address wildcard-mask área área-id
```

**Dirección:** Esta puede ser la dirección de red, subred o de la interfaz. Indica a los routers cuales son los enlaces en los que se deben escuchar publicaciones y que enlaces y redes se deben publicar.

**Máscara de wildcard:** Ésta es una máscara inversa que se utiliza para determinar como se lee una dirección. La máscara tiene bits wildcard donde 0 representa coincidencia y 1 no es importante.

**Id de área:** Éste valor indica el área que se debe asociar con una dirección. Puede ser un número o puede ser similar a una dirección ip. Para un área backbone, la id debe ser igual a 0.

A screenshot of a terminal window titled "Router: Eshim: Hyper Terminal". The terminal shows the following commands and prompts:

```
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 192.168.7.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#
```

Figura 7.31. Pantalla Configuración del Protocolo de enrutamiento OSPF

### 7.7.1.5.1.3 DIRECCIÓN DE LOOPBACK OSPF

Cuando se inicia el proceso OSPF, Cisco IOS utiliza la dirección IP activa local más alta como su ID de router OSPF. Si no existe ninguna interfaz activa, el proceso OSPF no se iniciará. Si la interfaz activa se desactiva, el proceso OSPF se queda sin ID de router y por lo tanto deja de funcionar hasta que la interfaz vuelve a activarse.

Para asegurarse la estabilidad de OSPF, deberá haber una interfaz activa para el proceso OSPF en todo momento. Es posible configurar una interfaz de loopback, que es una interfaz lógica, para este propósito. Al configurarse una interfaz loopback, OSPF usa esta dirección como ID del router, sin importar el valor. En un router que tiene mas de una interfaz loopback, OSPF toma la dirección IP de loopback más alta como su ID de router.

Para crear y asignar una dirección IP a una interfaz de loopback use los siguientes comandos:

```
Router (config) #interface loopback number  
Router (config-if) #ip address 192.168.0.1 255.255.255.255
```

Se considera buena práctica usar interfaces loopback para todos los routers que ejecutan OSPF. Esta interfaz de loopback se debe configurar con una dirección que use una máscara de subred de 32 bits de 255.255.255.255. Una máscara de subred de 32 bits se denomina una máscara de host porque la máscara de subred especifica la red de un host. Cuando se solicita que OSPF publique una red loopback, OSPF siempre publica el loopback como una ruta de host con una máscara de 32 bits.

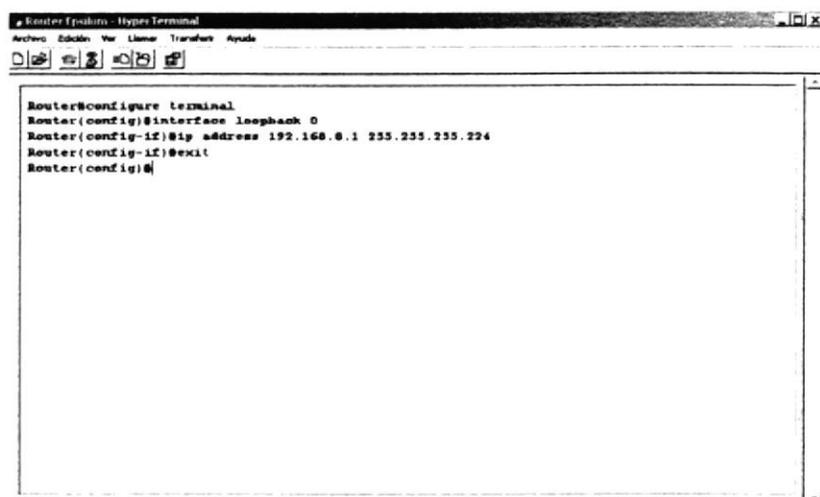
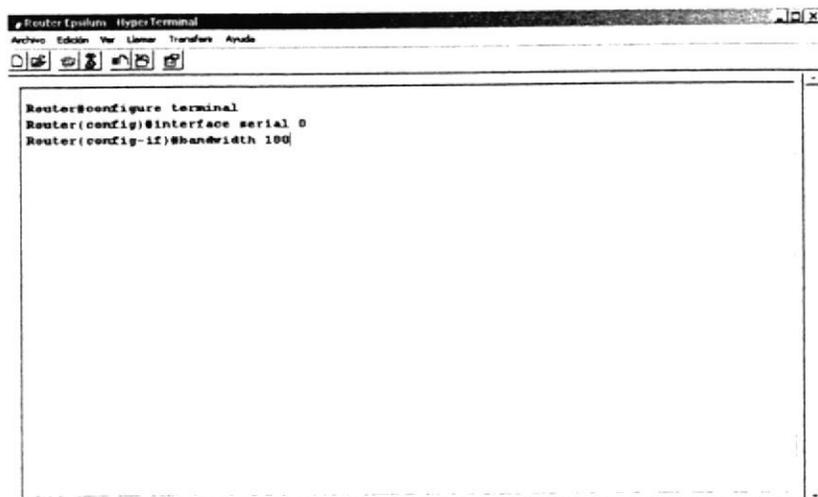


Figura 7.32. Pantalla configuración de la interfaz loopback

#### 7.7.1.5.1.4 MODIFICACIÓN DE LA MÉTRICA DE COSTOS DE OSPF

OSPF utiliza el costo como métrica para determinar la mejor ruta. Un costo se asocia con el lado de salida de cada interfaz de router. Los costos también se asocian con datos de enrutamiento derivados en forma externa. Por lo general, el costo de ruta se calcula mediante la fórmula  $10^8/\text{ancho de banda}$ , donde el ancho de banda se expresa en bps.

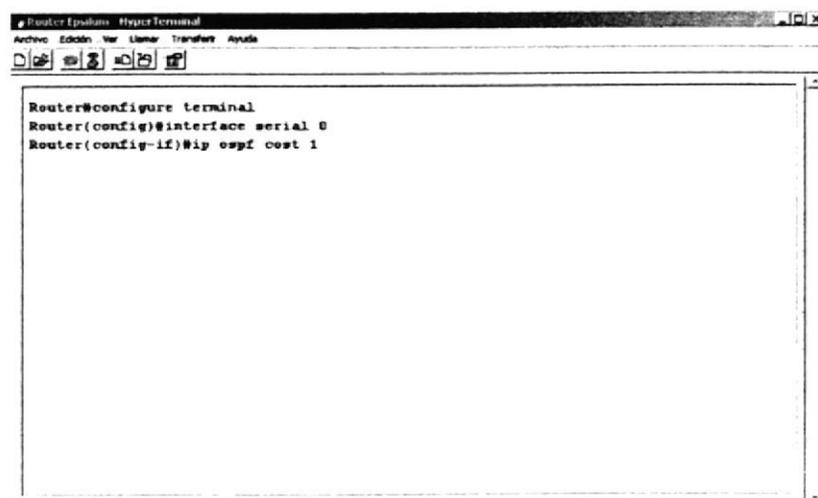
Resulta esencial para la operación correcta de OSPF que se establezca el ancho de banda de interfaz correcto. El ancho de banda por defecto para las interfaces seriales Cisco es 1.544 Mbps o 1544 Kbps



```
Router#configure terminal
Router(config)#interface serial 0
Router(config-if)#bandwidth 100
```

Figura 7.33. Pantalla modificación de la métrica de los costos de OSPF

Es posible cambiar el costo para afectar el resultado de los cálculos de costo OSPF. Una situación se produce al utilizar Gigabit Ethernet. Con la configuración por defecto, se asigna el valor de costo más bajo (1) a un enlace de 100 Mbps. En una situación con enlaces Gigabit Ethernet y 100-Mbps, los valores de costo por defecto podrían hacer que el enrutamiento tome una ruta menos deseable a menos que estos se ajusten. El número de costo se puede establecer entre 1 y 65.535.



```
Router#configure terminal
Router(config)#interface serial 0
Router(config-if)#ip ospf cost 1
```

Figura 7.34. Pantalla modificación de la métrica de los costos

### 7.7.1.5.1.5 CONFIGURACIÓN DE LOS TEMPORIZADORES

Los routers OSPF deben tener los mismos intervalos hello y los mismos intervalos muertos para intercambiar información. Por defecto, el intervalo muerto es de cuatro veces el valor del intervalo hello. Esto significa que un router tiene cuatro oportunidades de enviar un paquete hello antes de ser declarado muerto.

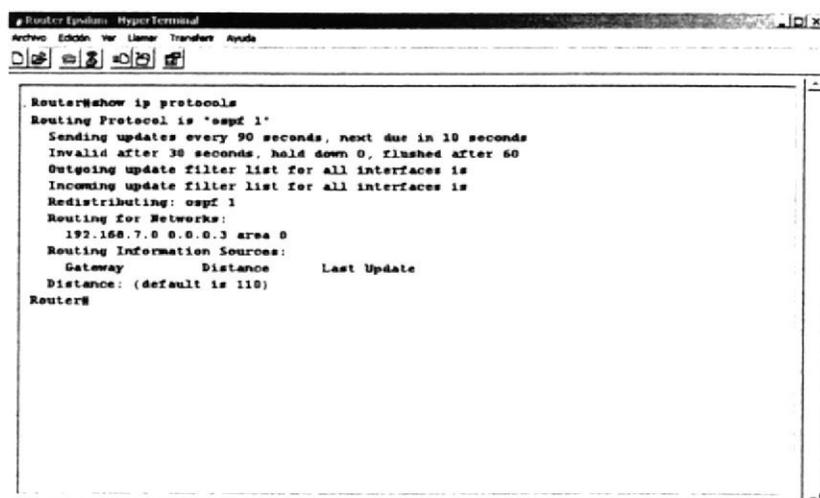
En las redes OSPF de broadcast, el intervalo hello por defecto es de 10 segundos y el intervalo muerto por defecto es de 40 segundos. En las redes que no son de broadcast, el intervalo hello por defecto es de 30 segundos y el intervalo muerto por defecto es de 120 segundos. Estos valores por defecto dan como resultado una operación eficiente de OSPF y muy pocas veces necesitan ser modificados.

Un administrador de red puede elegir estos valores de temporizador. Se necesita una justificación de que el rendimiento de red OSPF mejorará antes de cambiar los temporizadores. Estos temporizadores deben configurarse para que coincidan con los de cualquier router vecino.

### 7.7.1.5.1.6 VERIFICACIÓN DE CONFIGURACIÓN OSPF

Para verificar la configuración de OSPF existe una serie de comandos show. Se explica la manera en que los comandos **show** se pueden utilizar el diagnóstico de fallas de OSPF.

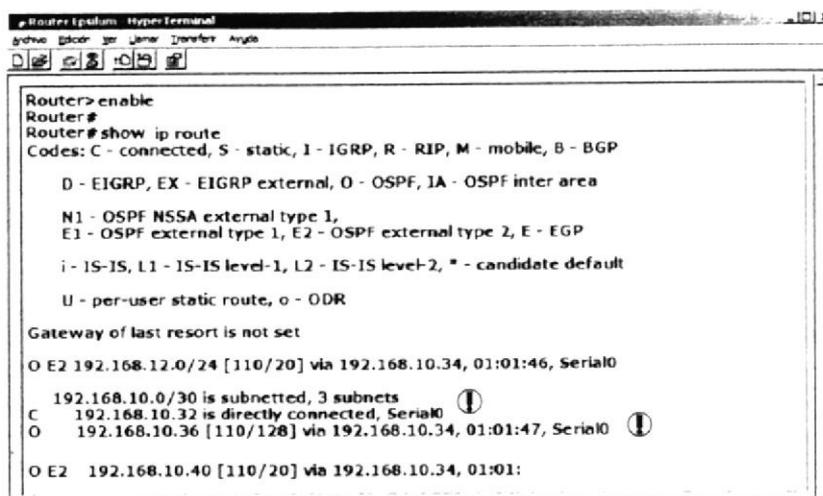
**Show ip protocol:** Ésto muestra parámetros para temporizadores, filtros, métricas, redes y otra información acerca de todo el router.



```
Router-Espolan: HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Router#show ip protocols
Routing Protocol is "ospf 1"
  Sending updates every 90 seconds, next due in 10 seconds
  Invalid after 30 seconds, hold down 0, flushed after 60
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: ospf 1
  Routing for Networks:
    192.168.7.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
Router#
```

Figura 7.35. Pantalla comando show ip protocol

**Show ip route:** Esto muestra las rutas que el router conoce y describe como se conocieron. Ésta es una de las mejores maneras para determinar la conectividad entre el router local y el resto de la red.



```

Router>enable
Router#
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set

O E2 192.168.12.0/24 [110/20] via 192.168.10.34, 01:01:46, Serial0
   192.168.10.0/30 is subnetted, 3 subnets
   C   192.168.10.32 is directly connected, Serial0
   O   192.168.10.36 [110/128] via 192.168.10.34, 01:01:47, Serial0
   O E2 192.168.10.40 [110/20] via 192.168.10.34, 01:01:
  
```

Figura 7.36. Pantalla comando show ip route

	<p><b>C 192.168.10.32 is directly connected, serial0</b>          Segmento de red conectado directamente al router - Serial conectada</p>
	<p><b>O 192.168.10.36 [110/128] vía 192.168.10.34,01:01:47, serial0</b>          Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente          Al ser O el protocolo es OSPF          El 110 es la distancia administrativa por default en OSPF          El 128 es el número de saltos que realiza OSPF          El 01:01:47 es el tiempo que se tardó en conectarse</p>

**Show ip ospf interface:** Esto verifica que las interfaces se hayan configurado en las áreas planificadas. Si no se especifica una dirección loopback, la interfaz con la dirección más alta se considera como el ID del router. Además proporciona los intervalos de temporización como el intervalo hello y muestra las adyacencias del router.

**Show ip ospf:** Muestra la cantidad de veces en que se ha usado el algoritmo SPF. También muestra el intervalo de actualización de estado de enlace si no se han producido cambios topológicos.

**Show ip ospf neighbor detail:** Este comando muestra un listado detallado de vecinos, sus prioridades y estados.

**Show ip ospf database:** Esto muestra el contenido de la base de datos topológica que mantiene el router y el ID del proceso OSPF.

## 7.7.2 LISTAS DE CONTROL DE ACCESO (ACL'S)

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos.

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACL's). Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior.

Las ACL pueden ser tan simples como una sola línea destinada a permitir paquetes desde un host específico o pueden ser un conjunto de reglas y condiciones extremadamente complejas que definan el tráfico de forma precisa y modelen el funcionamiento de los procesos de los routers.

Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX). Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones específicas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

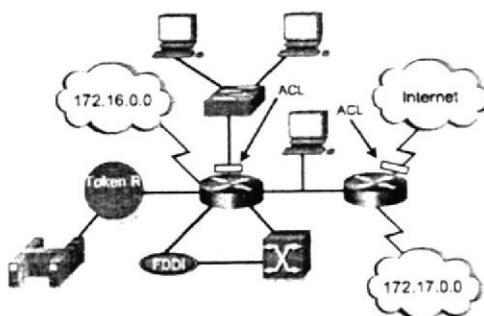


Figura 7.37. Gráfico de ubicación de ACL's

### 7.7.2.1. FUNCIONAMIENTO DE LAS ACL

El orden en el que se ubican las sentencias de la ACL es importante. El Software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo. Si se requieren más cantidades de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

A manera de revisión, las sentencias de las ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no

tienen coincidencias, se coloca una sentencia implícita que dice **deny any** (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea **deny any** no se ve visible como última línea de una ACL, está ahí y no permitirá que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada. Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el **deny any** al final de las ACL para reforzar la presencia dinámica de la prohibición implícita **deny**.

### 7.7.2.2. CREACIÓN DE LAS ACL

Las ACL se crean en el modo de configuración global. Existen varias clases diferentes de ACL's: estándar, extendidas, IPX, AppleTalk, entre otras. Cuando configure las ACL en el router, cada ACL debe identificarse de forma única, asignando un número. Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista.

Protocolo	Intervalo
IP	1 – 99, 1300 – 1999
IP EXTENDIDO	100-199, 2000-2699
APPLE TALK	600 – 699
IPX	800-899
IPX EXTENDIDO	900-999

Después de ingresar al modo de comando apropiado y que se decide el número de tipo de lista, el usuario ingresa sentencias de lista de acceso utilizando el comando **access-list**, seguida de los parámetros necesarios. Este es el primero de un proceso de dos pasos. El segundo paso consiste en asignar la lista a la interfaz apropiada.

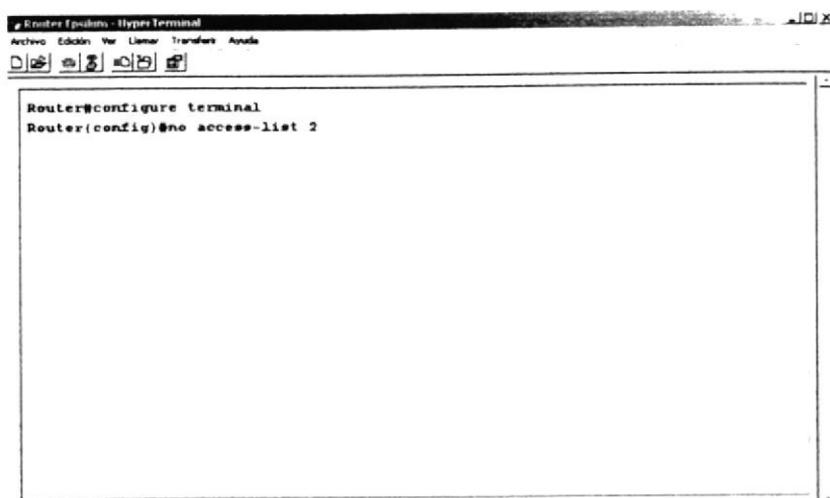
En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, usando el comando **ip access-group** en el modo de configuración de interfaz. Al asignar una ACL a una interfaz, se debe especificar la ubicación entrante o saliente. Después de crear una ACL numerada, se la debe asignar a una interfaz.

```

Router#configure terminal
Router(config)#access-list 2 deny 192.168.7.1
Router(config)#access-list 2 permit 192.168.7.0 0.0.0.255
Router(config)#access-list 2 deny 192.168.0.0 0.0.255.255
Router(config)#access-list 2 permit 192.0.0.0
Router(config)#interface fastethernet 0/0
Router(config-if)#ip access-group 2 in
  
```

Figura 7.38. Pantalla creación de ACL's

Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando **no access-list** list-number y entonces proceder a crear una nueva ACL.



```
Router#configure terminal
Router(config)#no access-list 2
```

Figura 7.39. Pantalla borrar ACL's

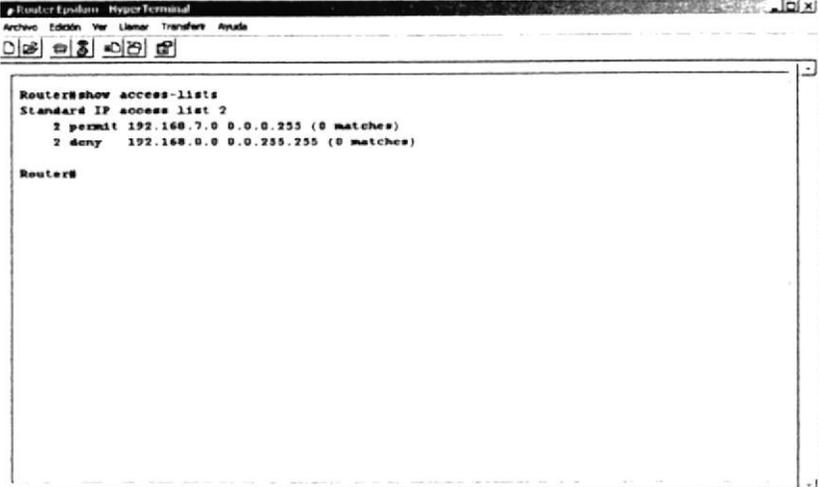
### 7.7.2.3. FUNCIÓN DE LA MÁSCARA WILLCARD

Una máscara willcard es una cantidad de 32-bits que se divide en cuatro octetos. Una máscara willcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar cómo tratar los bits de la dirección IP correspondientes. Las máscaras willcard no guardan relación funcional con las máscaras de subred. Se utilizan con distintos propósitos y siguen distintas reglas. Las máscaras de subred y las máscaras de willcard representan dos cosas distintas al compararse con una dirección IP. Las máscaras de subred usan unos y ceros binarios para identificar las porciones de red, de subred y de host de una dirección IP. Las máscaras de willcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara willcard y la de subred es que ambos tienen 32 bits de longitud y se componen de unos y ceros.

Hay dos palabras claves especiales que se utilizan en las ACL, las opciones **any** y **host**. Para explicarlo de forma sencilla, la opción **any** reemplaza la dirección IP con **0.0.0.0** y la máscara willdcard por **255.255.255.255**. Esta opción concuerda con cualquier dirección con la que se la compare. La máscara 0.0.0.0 reemplaza la opción host. Esta máscara necesita todos los bits de la dirección ACL y la concordancia de dirección del paquete. Esta opción sólo concuerda con una dirección.

#### 7.7.2.4. VERIFICACIÓN DE LAS ACL

El comando **show ip interface** muestra información de la interfaz IP e indica si se ha establecido alguna ACL. El comando **show access-list** muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número ACL como opción a este comando. El comando **show running-config** también revela las listas de acceso en el router y la información de asignación de interfaz.



```
Router#show access-lists
Standard IP access list 2
 2 permit 192.168.7.0 0.0.0.255 (0 matches)
 2 deny 192.168.0.0 0.0.255.255 (0 matches)

Router#
```

Figura 7.40. Pantalla verificación de las ACL's

### 7.7.3 TIPOS DE ACL's

#### 7.7.3.1. ACL ESTÁNDAR

En la versión 12.0.1 del IOS de Cisco, se usaron por primera vez números adicionales (1300 al 1999) para las ACL's estándar pudiendo así proveer un máximo posible de 798 ACLs estándar adicionales, a las cuales se les conoce como ACLs IP expandidas. (También entre 1300 y 1999) en IOS recientes). En la primera sentencia ACL, cabe notar que no hay máscara wildcard. En este caso donde no se ve ninguna lista, se utiliza la máscara por defecto, que es la 0.0.0.0. Esto significa que toda la dirección debe concordar o que esta línea en la ACL no aplica y el router debe buscar una concordancia en la línea siguiente de la ACL.

La sintaxis completa del comando ACL estándar es:

```
Router (config) #access-list access-list-number {deny | permit | remark}
source [source-wildcard][log]
```

El uso de **remark** facilita el entendimiento de la lista de acceso. Cada remark está limitado a 100 caracteres. Por ejemplo, no es suficientemente claro cual es el propósito del siguiente comando: **access-list 1 permit 192.168.0.1**. Es mucho más fácil leer un comentario acerca de un comando para entender sus efectos, así como sigue:

La forma de este comando se utiliza para eliminar una ACL estándar. Ésta es la sintaxis.

```
Router (config) #no access-list access-list-number
```

El comando **ip access-group** relaciona una ACL existente a una interface:

```
Router (config) #ip access-group {access-list-number | access-list-name} {in |
out}
```

#### 7.7.3.2. ACL EXTENDIDAS

Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos y números de puerto. Esto ofrece mucha flexibilidad para establecer qué verifica la ACL. Una vez descartados los paquetes, algunos protocolos devuelven un paquete al emisor, indicando que el destino era inalcanzable.

Es posible configurar múltiples sentencias en una sola ACL. Puede haber tanta cantidad de sentencias de condición como sean necesarias, siendo la única limitación la memoria disponible en el router.

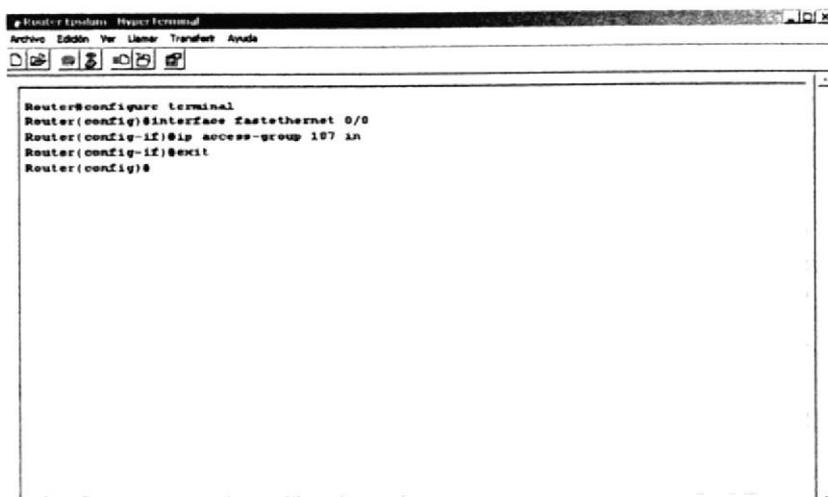
La sintaxis de una sentencia ACL extendida puede ser muy extensa y a menudo, se vuelve engorrosa en la ventana Terminal. Las wildcards también tienen la opción de utilizar las palabras clave **host** o **any** en el comando.

Al final de la sentencia de la ACL extendida, se obtiene más precisión con un campo que especifica el Protocolo para el control de la transmisión (TCP) o el número de puerto del Protocolo de data gama del usuario (UDP).

Las operaciones lógicas pueden especificarse como igual (*eq*), desigual (*neq*), mayor a (*gt*) y menor a (*lt*) aquellas que efectuarán las ACL extendidas en protocolos específicos. Las ACL extendidas utilizan el número de lista de acceso entre 100 y 199.

El comando **ip access-group** enlaza una ACL extendida existente a una interfaz.

Recuerde que sólo se permite una ACL por interfaz por protocolo por dirección.



```
Router#configure terminal
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip access-group 107 in
Router(config-if)#exit
Router(config)#
```

Figura 7.41. Pantalla implementación acl extendida en la interfaz

### 7.7.3.3. UBICACIÓN DE LAS ACL

Las ACL se utilizan para controlar el tráfico, filtrando paquetes y eliminando el tráfico no deseado de la red. Otra consideración importante a tener en cuenta al implementar la ACL es dónde se ubica la lista de acceso. Si las ACL se colocan en el lugar correcto, no sólo es posible filtrar el tráfico sino también toda la red se hace más eficiente. Si se tiene que filtrar el tráfico, la ACL se debe colocar en un lugar donde mejore la eficiencia de forma significativa.

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican las direcciones destino, de modo que se deben colocar lo más cerca posible del destino. Por ejemplo, una ACL estándar se debe colocar en Fa0/0 del Router D para evitar el tráfico desde el Router A.

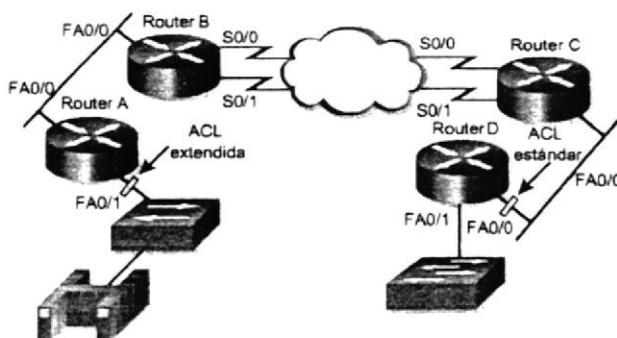


Figura 7.42. Ubicación de la ACL

### 7.7.4 FIREWALLS

Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos. En la mayoría de los casos, los intrusos provienen de la Internet mundial y de las miles de redes remotas que interconecta. Normalmente, un firewall de red se compone de varias máquinas diferentes que funcionan al mismo tiempo para impedir el acceso no deseado e ilegal.

Se debe utilizar ACL en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet. Esto permite el control del tráfico entrante o saliente de alguna parte específica de la red interna. El router firewall proporcionar un punto de aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada.

Se necesita configurar las ACL en router fronterizos, que son aquellos situados en las fronteras de la red, para brindar mayor seguridad. Esto proporciona protección básica contra la red externa u otra parte menos controlada de la red, en un área más privada de la red. En estos routers fronterizos, es posible crear ACL's para cada protocolo de red configurado en las interfaces del routers.

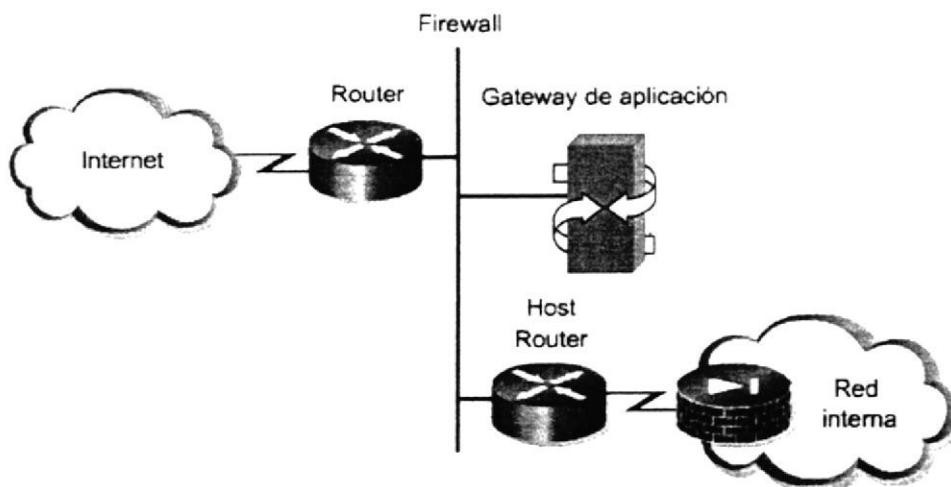


Figura 7.43. Implementación de Firewall

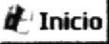
## 7.8 PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE ROUTERS (EPSILUM)

### 7.8.1 CONEXIÓN DE UNA TERMINAL CON LA CONSOLA DEL ROUTER

Antes de empezar, tendrá que tener claro que la conexión se realizará a través de la Aplicación HyperTerminal de Windows.

**HyperTerminal** es un programa que se puede utilizar para conectar con otros equipos, sitios Telnet, sistemas de boletines electrónicos (BBS, Bulletin Board Systems), servicios en línea y equipos host, mediante un módem, un cable de módem nulo o una conexión (WinSock) TCP/IP.

A continuación los pasos a seguir para la configuración:

1. Con un cable transpuesto **RJ-45 a RH-45** y un adaptador **RJ-45 a DB-9** o **RJ-45 a DB-25** se conectará de una Terminal (PC – Personal Computer) al puerto de consola del Router.
2. Abrirá la aplicación HyperTerminal:
  - a. En la barra de tareas de Windows seleccionará con el Mouse la opción .

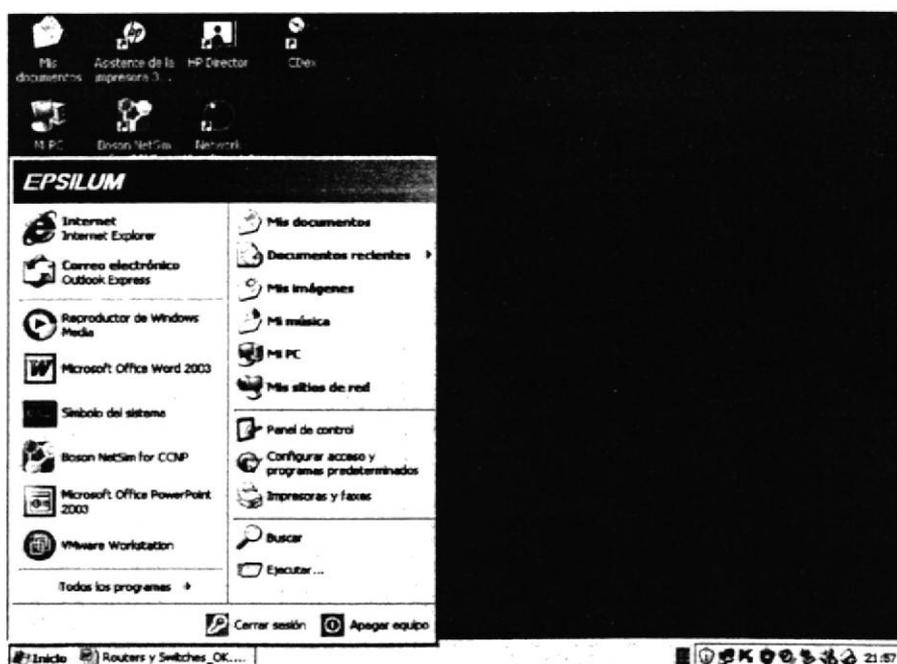


Figura 7.44. Pantalla escritorio de Windows accediendo al botón inicio

- b. Se abrirá un menú donde seleccionará la opción **Todos los programas**.

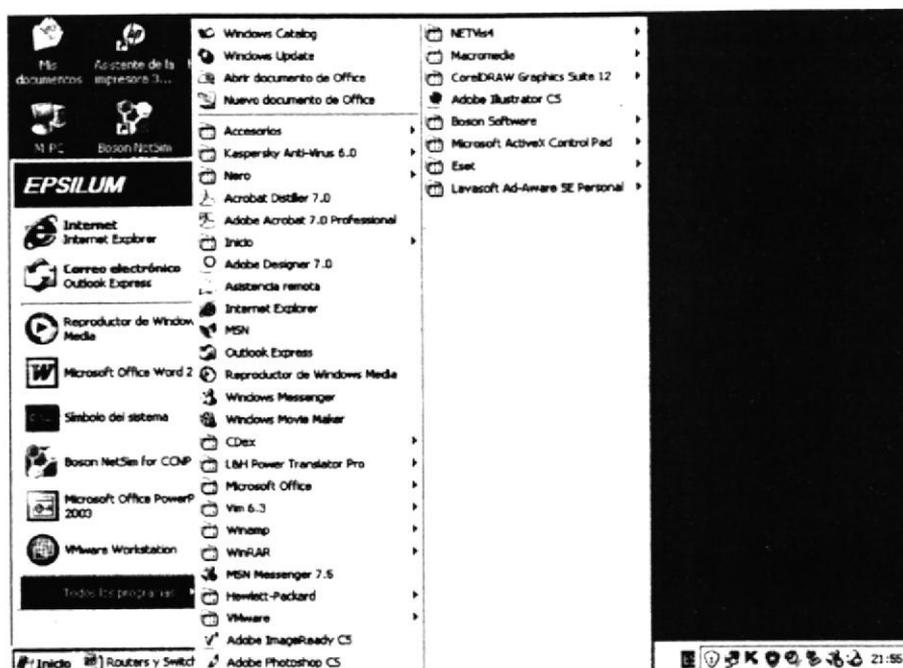


Figura 7.45. Pantalla escritorio de Windows opción todos los programas

- c. Seguidamente se desplegará un submenú donde seleccionará la opción **Accesorios**.

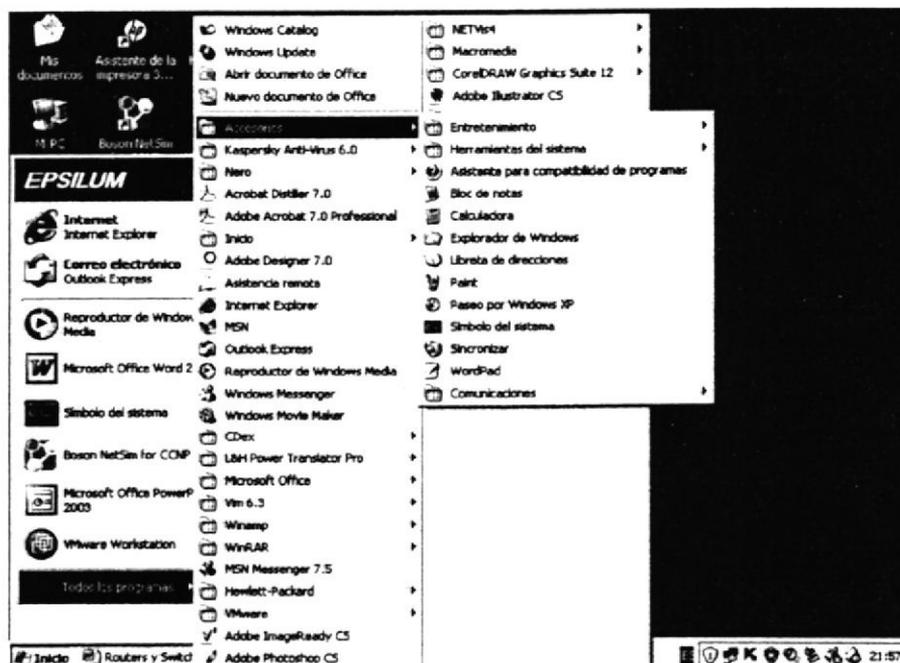


Figura 7.46. Pantalla escritorio de Windows opción accesorios

- d. Dentro de este submenú se encontrará la opción **Comunicaciones** la cual deberá ser seleccionada.

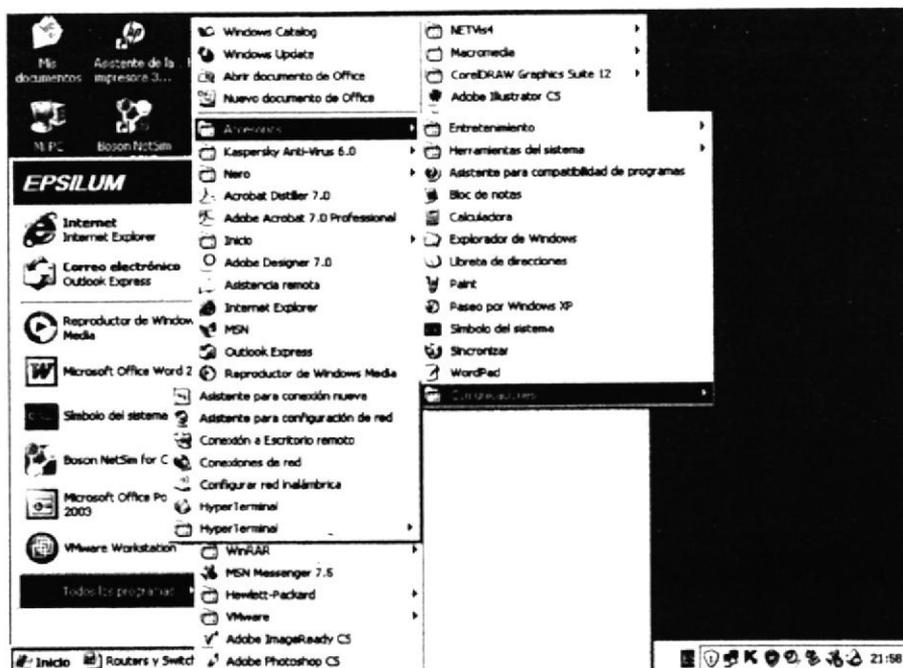


Figura 7.47. Pantalla escritorio de Windows opción comunicaciones

- e. Aquí encontrará un acceso directo llamado **HyperTerminal**, al cual le dará clic.

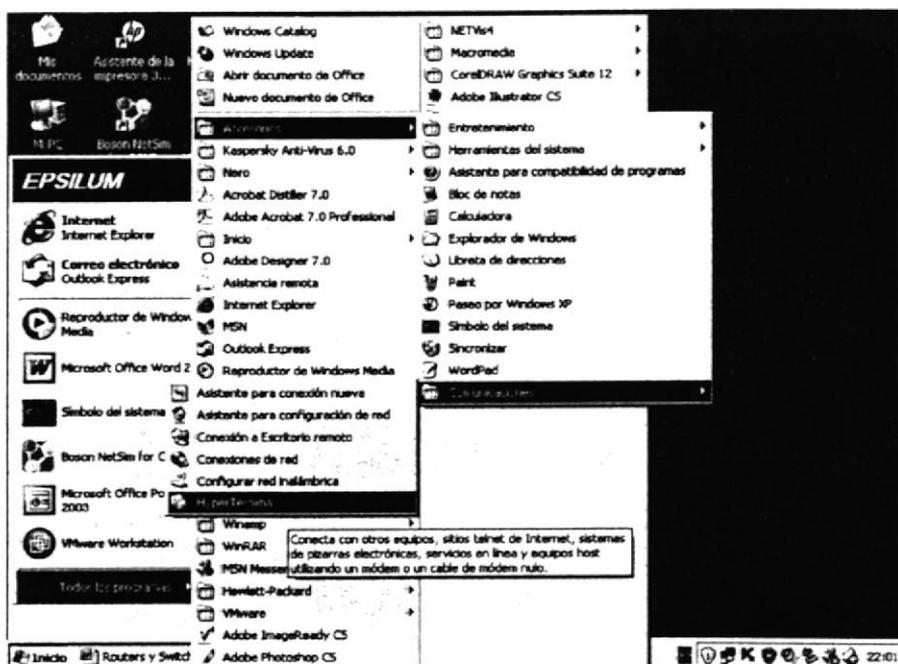


Figura 7.48. Pantalla escritorio de Windows icono Hyperterminal



3. Una vez que de clic en la opción de **Hyperterminal**, si es la primera vez que accede a esta aplicación, aparecerá una ventana de Advertencia, donde se recomienda establecer la Aplicación HyperTerminal como programa predeterminado de Telnet.

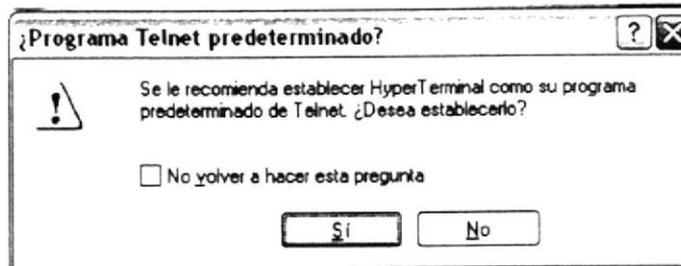


Figura 7.49. Pantalla de recomendación de programa predeterminado para Telnet

- a. La primera opción que da, es si desea volver a ver esta pregunta la próxima vez que acceda a la HyperTerminal. Esta opción no afectará en lo más mínimo a la conexión.
  - b. Ahora se presentan dos opciones de respuesta referente a la recomendación que hace Windows, si acepta "Sí" automáticamente aparecerá una ventana, la cual solicita cierta información para una conexión mediante MODEM; pero como este no es el caso simplemente "cancela", y automáticamente aparecerá la ventana de "Descripción de conexión" de la HyperTerminal.
  - c. Si en caso de que la ventana que Windows recomienda establecer a la aplicación HyperTerminal como predeterminada para Telnet, se la cancela, automáticamente aparecerá la ventana de "Descripción de la conexión" de la HyperTerminal.
4. En la ventana de "Descripción de la conexión" de HyperTerminal pedirá un nombre y un icono para la conexión.
- a. El Nombre puede ser cualquiera, en este caso se llamara Router Epsilon.
  - b. Cada icono es un tipo de conexión diferente, para este caso se utilizara el primero, el que viene marcado por default.



Figura 7.50. Pantalla ventana descripción de la conexión del Hyperterminal

5. En la siguiente pantalla se pedirá ingresar algunos detalles de conexión como País o región, Código de área, Número de teléfono y Conectar usando. Las tres primeras no son obligatorias son opcionales mientras que la última opción deberá escoger el puerto del computador al cual se va a conectar el router en este caso va a ser el puerto COM 1 y da clic en el botón Aceptar.

Figura 7.51. Pantalla: Conectar a

6. En la siguiente pantalla encontrará algunos parámetros de conexión los cuales deberá establecer y dar clic en el botón Aceptar.
- 9600 bps. (velocidad de transmisión del cable serial de conexión)
  - 8 bits de Datos ( configuración del procesamiento de datos al pasar al hyperterminal en bits pos segundo)
  - Ninguno (paridad) (utilizado para comprobar errores en el grupo de bits de datos transferidos entre uno o varios equipos)
  - 1 (bit de parada) (medida de transporte por la que pasan datos al Hyperterminal)
  - Ninguno (control de flujo se refiere a la información que viaja)

Figura 7.52. Pantalla propiedades del puerto COM 1



**Sugerencia:**

Se los puede establecer al dar clic en el botón **Restaurar predeterminados**.

7. Una vez colocado los parámetros dará clic en el botón Aceptar y podrá empezar con la configuración del router a través de la consola del Hyperterminal.

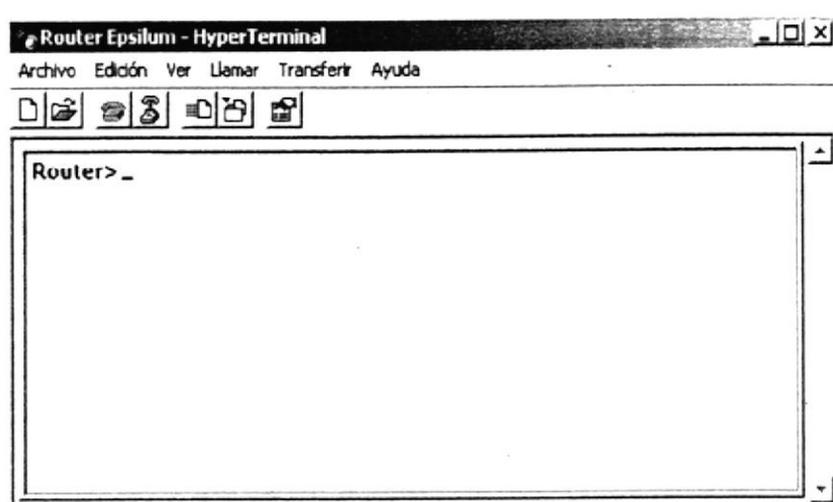


Figura 7.53. Pantalla Hyperterminal con la conexión al router

## 7.8.2 CONFIGURACIONES EN DISPOSITIVOS DE CONMUTACIÓN Y ENRUTAMIENTO IMPLEMENTADOS

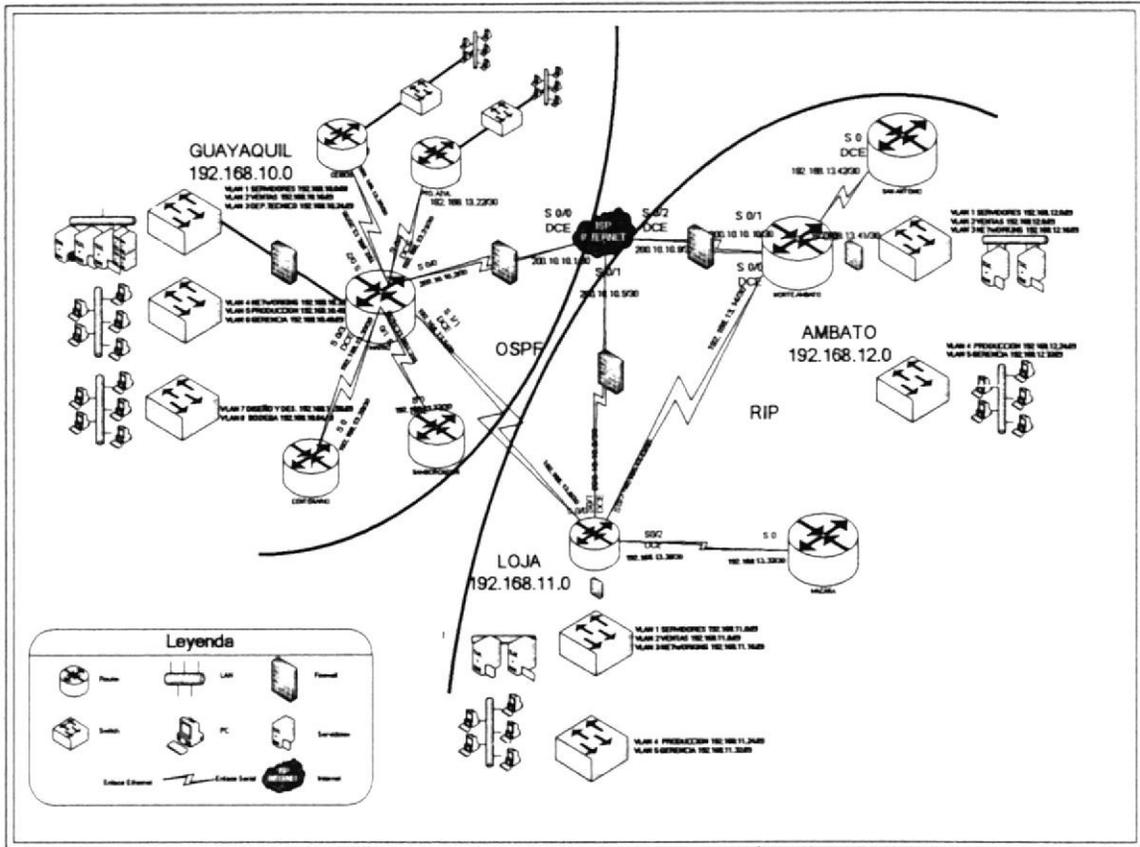


Figura 7.54. Gráfico WAN

A continuación se va a pasar a configurar de manera detallada el Gráfico WAN de los routers de la empresa Epsilon, donde se trabajará con los siguientes segmentos de red: **192.168.10.0 – 192.168.11.0 – 192.168.12.0 – 192.168.13.0**

Se posee 9 routers en donde el router Matriz es el principal y a su vez tiene 4 sucursales en el cual se establecerá el protocolo **OSPF** y en los Router Loja y Ambato con sus respectivas sucursales se establecerá el protocolo de **RIP VERSION 2**.

### 7.8.2.1 ROUTER MATRIZ

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start  
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>  
Router>enable  
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal  
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asignara el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname Matriz  
Nombre asignado al router
```

```
Matriz (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
Matriz (config)#line console 0  
Consola a la que se le asignara la contraseña
```

```
Matriz (config-line)#password cisco  
Contraseña establecida
```

```
Matriz (config-line)#login  
Se usa para que solicite contraseña al ingresar
```

**Matriz (config-line)#exit**

Sale de la configuración de la consola

**Matriz (config)#****Matriz (config)#line vty 0 4**

Ingresa a configurar la Terminal Virtual

**Matriz (config-line)#password cisco**

Contraseña establecida

**Matriz (config-line)#login**

Se usa para que se pueda establecer telnet a la interfaz

**Matriz (config-line)#exit**

Sale de la configuración de la consola

**Matriz (config)#****Matriz (config)#line aux 0**

Ingresa a configurar el puerto auxiliar

**Matriz (config-line)#password cisco**

Contraseña establecida

**Matriz (config-line)#login**

Se usa para que se pueda establecer telnet a la interfaz

**Matriz (config-line)#exit**

Sale de la configuración de la consola

**Matriz (config)#****Matriz (config-line)#enable password cisco**

Agrega una contraseña para ingresar al router

**Matriz (config-line)#enable secret cisco**

Agrega una contraseña encriptada para ingresar al router

**Configuración de las Interfaces**

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Matriz (config)#interface serial 0/0**

Interfaz a configurar

**Matriz (config-if)#ip address 192.168.13.1 255.255.255.252**

Dirección y máscara asignada, es 252 debido a ser una interfaz serial

7. Proceda a levantar la interfaz con el siguiente comando

**Matriz (config-if)#no shutdown**

Levanta la interfaz

**%LINK-3-UPDOWN:** Interface Serial0/0, changed state to up

Indica que la interfaz ha cambiado y su respectivo estado

8. Después de esto salga del modo de configuración con el comando **exit** para pasar a configurar la siguiente interfaz.

**Matriz (config-if)#exit**

Sale de la configuración de la interfaz

**Matriz (config)#**



#### Importante

En la serial 0/0 se obvia el **clock rate** debido a que esta interfaz es un DTE (data terminal equipment).

9. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

**Matriz (config)#interface serial 0/1**

Número y tipo de Interfaz que va a ser configurada

**Matriz (config-if)#ip address 192.168.13.21 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial.

10. Se le asignara su respectivo clock rate debido a que esta interfaz es un DCE (data communication equipment)

**Matriz (config-if)#clock rate 64000**

El clock rate lo que permite es la sincronización de datos con los demás routers es 64000 para obtener una mayor velocidad.

11. Proceda a levantar la interfaz con el siguiente comando.

**Matriz (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN:** Interface Serial0/1, changed state to up

Indica que la interfaz ha cambiado y su respectivo estado

**Matriz (config-if)#**

12. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

**Matriz (config)#interface serial 0/2**

Número y tipo de Interfaz que va a ser configurada

**Matriz (config-if)#ip address 192.168.13.25 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial

13. Proceda a levantar la interfaz con el siguiente comando.

**Matriz (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN: Interface Serial0/2, changed state to up**

Indica que la interfaz ha cambiado y su respectivo estado



**Importante**

En la serial 0/2 se obvia el **clock rate** debido a que esta interfaz es un **DTE** (data terminal equipment).

14. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

**Matriz (config)#interface serial 0/3**

Número y tipo de Interfaz que va a ser configurada.

**Matriz (config-if)#ip address 192.168.13.30 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial.

15. Se le asignara su respectivo clock rate debido a que esta interfaz es un DCE (data communication equipment)

**Matriz (config-if)#clock rate 64000**

El clock rate lo que permite es la sincronización de datos con los demás routers es 64000 para obtener una mayor velocidad.

16. Proceda a levantar la interfaz con el siguiente comando.

**Matriz (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN: Interface Serial0/3, changed state to up**

Indica que la interfaz ha cambiado y su respectivo estado

17. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

**Matriz (config)#interface serial 1/0**

Número y tipo de Interfaz que va a ser configurada

**Matriz (config-if)#ip address 192.168.13.34 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial

18. Proceda a levantar la interfaz con el siguiente comando.

**Matriz (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN: Interface Serial1/0, changed state to up**

Indica que la interfaz ha cambiado y su respectivo estado

19. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

**Matriz (config)#interface serial 1/1**

Número y tipo de Interfaz que va a ser configurada

**Matriz (config-if)#ip address 192.168.13.5 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial

20. Se le asignara su respectivo clock rate debido a que esta interfaz es un DCE (data communication equipment)

**Matriz (config-if)#clock rate 64000**

El clock rate lo que permite es la sincronización de datos con los demás routers es 64000 para obtener una mayor velocidad.

21. Proceda a levantar la interfaz con el siguiente comando.

**Matriz (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN: Interface Serial1/1, changed state to up**

Indica que la interfaz ha cambiado y su respectivo estado

**Matriz (config-if)#exit**

Sale de la configuración de la interfaz

## Configuración de Protocolo de Enrutamiento OSPF

El protocolo de enrutamiento OSPF debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

22. Se ingresa al modo de configuración global.

```
Matriz#
Matriz#configure terminal
Entrar al modo de configuración global
```

23. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

```
Matriz(config)#router ospf 1
Habilita el protocolo de enrutamiento a configurar
```

24. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es OSPF va con su respectiva willcard y el área)

	DIRECCIÓN DE RED	WILLCARD	ÁREA
Matriz (config-router)#network	192.168.13.20	0 0.0.3	area 0
Matriz (config-router)#network	192.168.13.24	0.0.0.3	area 0
Matriz (config-router)#network	192.168.13.28	0.0.0.3	area 0
Matriz (config-router)#network	192.168.13.32	0.0.0.3	area 0
Matriz (config-router)#network	192.168.10.0	0.0.0.15	area 0
Matriz (config-router)#network	192.168.10.16	0.0.0.7	area 0
Matriz (config-router)#network	192.168.10.24	0.0.0.7	area 0
Matriz (config-router)#network	192.168.10.32	0.0.0.7	area 0
Matriz (config-router)#network	192.168.10.40	0.0.0.7	area 0
Matriz (config-router)#network	192.168.10.48	0.0.0.7	area 0
Matriz (config-router)#network	192.168.10.56	0.0.0.7	area 0
Matriz (config-router)#network	192.168.10.64	0.0.0.7	area 0

Asignar la dirección de la red, willdcard y área respectiva

```
Matriz (config-router)#
```

25. Se aplica la redistribución del protocolo de enrutamiento Rip.

```
Matriz(config-router)#redistribute rip
Distribuye ospf hacia las subredes rip
```

Para deshabilitar el protocolo de enrutamiento OSPF se utiliza el comando “no router OSPF”.

```
Matriz #configure terminal
Entra al modo de configuración global
```

```
Matriz (config)#no router ospf 1
Desactiva el protocolo de enrutamiento ospf
```

**Matriz (config)#exit***Sale del modo de configuración global*

### **Configuración de Protocolo de Enrutamiento RIP**

El protocolo de enrutamiento RIP debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

26. Se ingresa al modo de configuración global

**Matriz#****Matriz#configure terminal***Entrar al modo de configuración global*

27. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

**Matriz (config)#router rip***Protocolo a configurar***Matriz (config-router)#version 2***Versión del protocolo*

28. Se establece el segmento de red que se quiere que este router aprenda.

**Matriz (config-router)#network 192.168.13.4***DIRECCIÓN DE RED**Asigna la dirección de red*

29. Se aplica la redistribución (en esta caso es de RIP a OSPF)

**Matriz (config-router)#redistribute ospf 1**

*Se aplica la redistribución de protocolos para que las tablas de enrutamiento se actualicen con los segmentos conectados en el otro protocolo y exista la comunicación*

*Para deshabilitar el protocolo de enrutamiento RIP se utiliza el comando "no router RIP".*

**Matriz #configure terminal***Entra al modo de configuración global***Matriz (config)#no router rip***Desactiva el protocolo de enrutamiento rip***Matriz (config)#exit***Sale del modo de configuración global*

## Configuración de Listas de Acceso



### Importante

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list : comando
- 1-99 ,1300-1 999 : # acl estandar
- permit/deny : permitir o denegar una red específica
- source : ( direccion de red – willcard)
- any : cualquier host o red

*Bloquear toda la subred 192.168.10.16/24, excepto los servidores 192.168.10.0/28*

#### **Matriz #configure Terminal**

*Ingresa al modo de configuración global*

**Matriz (config)# access-list 1 permit 192.168.10.0 0.0.0.3**

*Asigna permiso a una subred específica*

**Matriz (config)#access-list 1 deny 192.168.10.16 0.0.0.255**

*Niega el acceso a la red a las demás ip's*

**Matriz (config)#access-list 1 permit any**

*Luego se coloca una línea implícita para esta acl*

**Matriz (config)#exit**

*Sale del modo de configuración global*

*Luego levantar la acl estándar en la interfaz correspondiente.*

#### **Matriz #configure terminal**

*Ingresa al modo de configuración global*

**Matriz (config) #interface fastethernet 0/0**

*Ingresa a la interfaz que quiere asignar la acl*

**Matriz (config)#ip access-group 1 in**

*Levanta la acl de manera entrante*



### Importante

La sintaxis de las Listas de Control de acceso es la siguiente:

- ip access-group : relaciona una acl a una interface.
- 1 : # acl estandar o extendida
- in / out : entrante / saliente

**ACL extendida****Importante**

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list : comando
- 100-199, 2000-2699 : # acl extendida
- permit/deny : permitir o denegar una red específica
- source : ( dirección de red – wildcard)
- any : cualquier host o red

**Matriz #configure terminal**

*Ingresar al modo de configuración global*

**Matriz (config) #access-list 101 permit 192.168.10.32 0.0.0.7 192.168.10.0 0.0.0.3**

*Asigna permiso específico*

**Matriz (config)#access-list 101 deny 192.168.10.64 0.0.0.7 192.168.10.0 0.0.0.3**

*Niega el acceso a la red a las demás ip's*

**Matriz (config) #access-list 101 permit any any**

*Luego poner una línea implícita para esta acl*

**Matriz (config)#exit**

*Salir del modo de configuración global*

*Luego levantar la acl extendida en la interfaz correspondiente.*

**Matriz #configure terminal**

*Ingresar al modo de configuración global*

**Matriz (config) #interface fastethernet 0/0**

*Ingresar a la interfaz que quiere asignar la acl*

**Matriz (config) #ip access-group 101 in**

*Levanta la acl de manera entrante*

**Importante**

La sintaxis de las Listas de Control de acceso es la siguiente:

- ip access-group: relaciona una acl a una interface.
- 1 : # acl estandar o extendida
- in / out : entrante / saliente

Permitir tráfico (ICMP) desde una subred hacia el servidor

**Matriz #configure terminal**

Ingresar al modo de configuración global

**Matriz (config)#access-list 102 permit icmp 192.168.10.32 0.0.0.7  
192.168.10.0 0.0.0.3**

Asigna permiso específico

**Matriz (config) #access-list 102 deny any any**

Se coloca una línea implícita



### Importante

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list: comando
- 100-199, 2000-2699 : # acl extendida
- permit/deny : permitir o denegar una red específica
- icmp : protocolo puede ser (entre otros) IP (todo tráfico de tipo TCP/IP), TCP, UDP, ICMP.
- source : ( dirección de red – willcard)
- any : cualquier host o red

### Guardar configuración

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

**Matriz#copy running-config startup-config**

Guarda una copia de la configuración en la NVRAM

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

## 7.8.2.1.1 SHOW RUNNING ROUTER MATRIZ

**Building configuration...****Current configuration:**

!

**Version 12.1**

Versión del IOS del router

**service timestamps debug uptime****service timestamps log uptime****no service password-encryption**

No se está utilizando la encriptación de passwords

!

**hostname Matriz**

Nombre Router

**enable password cisco**

La contraseña para ingresar al modo privilegiado es cisco

!

!

!

**ip subnet-zero**

Sirve para poder usar la dirección de red como IP

!

!

!

**interface Serial0/0**

Tipo de Interfaz

**ip address 192.168.13.1 255.255.255.252**

Dirección IP y máscara de dicha interfaz

**no ip directed-broadcast**

!

**interface Serial0/1**

Tipo de Interfaz

**ip address 192.168.13.21 255.255.255.252**

Dirección IP y máscara de dicha interfaz

**no ip directed-broadcast****clock rate 64000**

Indica la velocidad del puerto en bits por segundo, lo encuentra en la DCE

!

**interface Serial0/2**

Tipo de Interfaz

**ip address 192.168.13.25 255.255.255.252**

Dirección IP y máscara de dicha interfaz

**no ip directed-broadcast**

!

!

**interface Serial0/3**

Tipo de Interfaz



```
ip address 192.168.13.30 255.255.255.252
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

```
clock rate 64000
```

Indica la velocidad del puerto en bits por segundo, lo encuentra en la DCE

!

```
interface Serial1/0
```

Tipo de Interfaz

```
ip address 192.168.13.34 255.255.255.252
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

!

```
interface Serial1/1
```

Tipo de Interfaz

```
ip address 192.168.13.5 255.255.255.252
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

```
clock rate 64000
```

Indica la velocidad del puerto en bits por segundo, lo encuentra en la DCE.

!

```
interface FastEthernet2/0
```

Tipo de Interfaz

```
no ip address
```

```
no ip directed-broadcast
```

!

!



```
interface FastEthernet2/0.10
```

Tipo de Interfaz

```
encapsulation dotq1 10
```

encapsulamiento asociado a la vlan 10

```
ip address 192.168.10.1 255.255.25.240
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

!

!

```
interface FastEthernet2/0.20
```

Tipo de Interfaz

```
encapsulation dotq1 20
```

encapsulamiento asociado a la vlan 20

```
ip address 192.168.10.17 255.255.25.248
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

!

!

```
interface FastEthernet2/0.30
```

Tipo de Interfaz

```
encapsulation dotq1 30
```

encapsulamiento asociado a la vlan 30

```
ip address 192.168.10.125 255.255.25.248
```

Dirección IP y mascara de dicha interfaz

```
no ip directed-broadcast
```

```
!
```

```
!
```

```
interface FastEthernet2/0.40
```

Tipo de Interfaz

```
encapsulation dotq1 40
```

encapsulamiento asociado a la vlan 40

```
ip address 192.168.10.33 255.255.25.248
```

Dirección IP y mascara de dicha interfaz

```
no ip directed-broadcast!
```

```
!
```

```
!
```

```
interface FastEthernet2/0.50
```

Tipo de Interfaz

```
encapsulation dotq1 50
```

encapsulamiento asociado a la vlan 50

```
ip address 192.168.10.41 255.255.25.248
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

```
!
```

```
!
```

```
!
```

```
interface FastEthernet2/0.60
```

Tipo de Interfaz

```
encapsulation dotq1 60
```

encapsulamiento asociado a la vlan 20

```
ip address 192.168.10.49 255.255.25.248
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

```
!
```

```
!
```

```
interface FastEthernet2/0.70
```

Tipo de Interfaz

```
encapsulation dotq1 70
```

encapsulamiento asociado a la vlan 70

```
ip address 192.168.10.57 255.255.25.248
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

```
!
```

```
!
```

```
interface FastEthernet2/0.80
```

Tipo de Interfaz

```
encapsulation dotq1 80
```

encapsulamiento asociado a la vlan 20

```
ip address 192.168.10.65 255.255.25.248
```

Dirección IP y máscara de dicha interfaz

```
no ip directed-broadcast
```

**router rip***Protocolo de Enrutamiento***Version 2***Versión del protocolo de Enrutamiento***redistribute OSPF 1***Distribuye protocolo Rip hacia las redes ospf***network 192.168.13.0***Redes configuradas con el protocolo de Enrutamiento Rip***!****router ospf 1***Protocolo de Enrutamiento***redistribute RIP***Distribuye protocolo Ospf hacia las redes Rip*

<b>DIRECCIÓN RED</b>	<b>WILLCARD</b>	<b>ÁREA</b>
<b>network 192.168.13.20</b>	<b>0 0.0.3</b>	<b>area 0</b>
<b>network 192.168.13.24</b>	<b>0.0.0.3</b>	<b>area 0</b>
<b>network 192.168.13.28</b>	<b>0.0.0.3</b>	<b>area 0</b>
<b>network 192.168.13.32</b>	<b>0.0.0.3</b>	<b>area 0</b>
<b>network 192.168.10.0</b>	<b>0.0.0.15</b>	<b>area 0</b>
<b>network 192.168.10.16</b>	<b>0.0.0.7</b>	<b>area 0</b>
<b>network 192.168.10.24</b>	<b>0.0.0.7</b>	<b>area 0</b>
<b>network 192.168.10.32</b>	<b>0.0.0.7</b>	<b>area 0</b>
<b>network 192.168.10.40</b>	<b>0.0.0.7</b>	<b>area 0</b>
<b>network 192.168.10.48</b>	<b>0.0.0.7</b>	<b>area 0</b>
<b>network 192.168.10.56</b>	<b>0.0.0.7</b>	<b>area 0</b>
<b>network 192.168.10.64</b>	<b>0.0.0.7</b>	<b>area 0</b>

**!****ip classless***Indica acceso a las redes no remotas con máscara de sub red diferente.***no ip http server****!****line con 0***Consola del router***password cisco***Password asignado al usuario normal***login***Esta línea es para que aparezca la petición de clave***line aux 0***Consola auxiliar***password cisco***Password asignado al usuario normal***login***Esta línea es para que aparezca la petición de clave*

**line vty 0 4**

Consola del router

**password cisco**

Password asignado al usuario privilegiado

**login**

Esta línea es para que aparezca la petición de clave y para poder realizar telnet

!

**end**

	<p><b>no ip address</b> significa que no tiene IP asignada, <b>no ip directed-broadcast</b> significa que la interfaz no tiene una dirección IP directa de broadcast, <b>shutdown</b> que no se ha levantado la interfaz</p>
	<p>El 0.0.0.3 es la <b>willcard</b> y debido a que era un salto de 4 en la segmentación la <b>willcard</b> es 3 ya que equivale a uno menos que el salto mientras que el área 0 es a la que pertenece</p>

**Tabla. 7.1** Descripción de las líneas del show running mediante iconos

## 7.8.2.1.2 SHOW IP ROUTE ROUTER MATRIZ

**Matriz#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
U - per-user static route

Gateway of last resort is not set

200.10.10.0/30 is subnetted, 3 subnets

C 200.10.10.0 is directly connected, Serial0/0  
O 200.10.10.4 [110/0] via 192.168.13.6, 00:00:12, Serial1/1  
O 200.10.10.8 [110/0] via 200.10.10.1, 00:00:06, Serial0/0

192.168.10.0/24 is variably subnetted, 8 subnets

C 192.168.10.0/28 is directly connected, 192.168.10.1  
C 192.168.10.16/29 is directly connected, 192.168.10.17  
C 192.168.10.24/29 is directly connected, 192.168.10.25  
C 192.168.10.32/29 is directly connected, 192.168.10.33  
C 192.168.10.40/29 is directly connected, 192.168.10.41  
C 192.168.10.48/29 is directly connected, 192.168.10.49  
C 192.168.10.56/29 is directly connected, 192.168.10.57  
C 192.168.10.64/29 is directly connected, 192.168.10.65

192.168.13.0/30 is subnetted, 7 subnets

C 192.168.13.20 is directly connected, Serial0/1  
C 192.168.13.24 is directly connected, Serial0/2  
C 192.168.13.28 is directly connected, Serial0/3  
C 192.168.13.32 is directly connected, Serial1/0  
C 192.168.13.4 is directly connected, Serial1/1  
O 192.168.13.12 [110/0] via 192.168.13.6, 00:00:12, Serial1/1  
O 192.168.13.36 [110/0] via 192.168.13.6, 00:00:06, Serial1/1

192.168.11.0/29 is subnetted, 5 subnets

O 192.168.11.0 [110/0] via 192.168.13.6, 00:00:12, Serial1/1  
O 192.168.11.8 [110/0] via 192.168.13.6, 00:00:12, Serial1/1  
O 192.168.11.16 [110/0] via 192.168.13.6, 00:00:12, Serial1/1  
O 192.168.11.24 [110/0] via 192.168.13.6, 00:00:12, Serial1/1  
O 192.168.11.32 [110/0] via 192.168.13.6, 00:00:12, Serial1/1

192.168.12.0/29 is subnetted, 5 subnets

R 192.168.12.0 [120/2] via 192.168.13.6, 00:04:14, Serial1/1  
R 192.168.12.8 [120/2] via 192.168.13.6, 00:07:26, Serial1/1  
R 192.168.12.16 [120/2] via 192.168.13.6, 00:02:27, Serial1/1  
R 192.168.12.24 [120/2] via 192.168.13.6, 00:08:43, Serial1/1  
R 192.168.12.32 [120/2] via 192.168.13.6, 00:09:20, Serial1/1  
C 192.168.13.0 is directly connected, Serial0/0  
C 192.168.13.20 is directly connected, Serial0/1  
C 192.168.13.24 is directly connected, Serial0/2  
C 192.168.13.28 is directly connected, Serial0/3  
C 192.168.13.32 is directly connected, Serial1/0  
C 192.168.13.4 is directly connected, Serial1/1  
O 192.168.13.8 [110/0] via 192.168.13.6, 00:13:15, Serial1/1



### Importante

Explicación del comando show ip route :

#### **C 200.10.10.0 is directly connected, Serial0/0**

- C : Segmento de red ,conectado directamente al router.
- 192.168.10.16/29 : Dirección de Red- Máscara
- Serial0/1 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

#### **O 192.168.11.0 [110/0] via 192.168.13.6, 00:00:12, Serial1/1**

- O : Protocolo OSPF
- 192.168.11.0 : Dirección de Red
- 110 : distancia administrativa por default en OSPF
- 0 : Número de saltos que realiza OSPF.
- 192.168.13.6 : Interfaz a la que llega
- 00:13:15 : Tiempo que se tardó en conectarse.
- Serial1/1 : Interfaz saliente

#### **R 192.168.12.0 [120/2] via 192.168.13.6, 00:04:14, Serial1/1**

- R : Protocolo RIP
- 192.168.12.0 : Dirección de Red
- 120 : distancia administrativa por default en RIP.
- 2 : Número de saltos que realiza RIP.
- 192.168.13.6 : Interfaz a la que llega
- 00:04:14 : Tiempo que se tardó en conectarse.
- Serial 1/1 : Interfaz saliente

### 7.8.2.2 ROUTER PUERTO AZUL

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>
Router>enable
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asignara el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname Pto_Azul
Nombre asignado al router
```

```
Pto_Azul (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
Pto_Azul (config) #line console 0
Consola a la que se le asignara la contraseña
```

```
Pto_Azul (config-line) #password cisco
Contraseña establecida
```

```
Pto_Azul (config-line) #login
Se usa para que solicite contraseña al ingresar
```



**Pto\_Azul (config-line) #exit**

*Sale de la configuración de la consola*

**Pto\_Azul (config) #**

**Pto\_Azul (config) #line vty 0 4**

*Ingresa a configurar la Terminal Virtual*

**Pto\_Azul (config-line) #password cisco**

*Contraseña establecida*

**Pto\_Azul (config-line) #login**

*Se usa para que se pueda establecer telnet a la interfaz*

**Pto\_Azul (config-line) #exit**

*Sale de la configuración de la consola*

**Pto\_Azul (config) #**

**Pto\_Azul (config) #line aux 0**

*Ingresa a configurar el puerto auxiliar*

**Pto\_Azul (config-line) #password cisco**

*Contraseña establecida*

**Pto\_Azul (config-line) #login**

*Se usa para que se pueda establecer telnet a la interfaz*

**Pto\_Azul (config-line) #exit**

*Sale de la configuración de la consola*

**Pto\_Azul (config) #**

**Pto\_Azul (config-line) #enable password cisco**

*Agrega una contraseña para ingresar al router*

**Pto\_Azul (config-line) #enable secret cisco**

*Agrega una contraseña encriptada para ingresar al router*

### **Configuración de las Interfaces**

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Pto\_Azul (config) #interface serial 0**

*Interfaz y tipo que va a ser configurada*

**Pto\_Azul (config-if) #ip address 192.168.13.22 255.255.255.252**

*Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial.*

**Importante**

En este router se obvia el **clock rate** debido a que esta interfaz es un **DTE** (data terminal equipment).

7. Se procede a levantar la interfaz con el siguiente comando.

```
Pto_Azul (config-if) #no shutdown
Levanta la interfaz
```

```
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Indica que la interfaz ha cambiado y su respectivo estado
```

**Sugerencia**

Puede que les aparezca unos mensajes similar a los que se muestran en la parte inferior lo que da a entender que la interfaz no se levanto, esto indica que la interfaz conectada en el siguiente router aun no a sido configurada

```
%LINK-3-UPDOWN: Interface Serial0, changed state to down
Indica que la interfaz ha cambiado y su respectivo estado
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
to down
Indica el protocolo, la interfaz y el respectivo estado al que ha cambiado la o las
interfaces de los routers cercanos
```

**Configuración de Protocolo de Enrutamiento OSPF**

El protocolo de enrutamiento OSPF debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

8. Se ingresa al modo de configuración global

```
Pto_Azul#
Pto_Azul#configure terminal
Entrar al modo de configuración global
```

9. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

```
Pto_Azul (config) #router ospf 1
Protocolo a configurar
```

10. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es OSPF va con su respectiva willcard y el área)

```
Pto_Azul (config-router) #network 192.168.13.20 0.0.0.3 area 0  
DIRECCIÓN DE RED WILLCARD ÁREA
```

Red que aprende con la respectiva willcard y el área en que se encuentra.  
Es la dirección de red del segmento conectado al router

```
Pto_Azul (config-router) #
```

Para deshabilitar el protocolo de enrutamiento OSPF se utiliza el comando "no router OSPF".

```
Pto_Azul #configure terminal
```

Entra al modo de configuración global

```
Pto_Azul (config) #no router ospf 1
```

Desactiva el protocolo de enrutamiento ospf

```
Pto_Azul (config) #exit
```

Sale del modo de configuración global

### Guardar configuración

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

```
Pto_Azul#copy running-config startup-config
```

Guarda una copia de la configuración en la NVRAM

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

## 7.8.2.2.1 SHOW RUNNING ROUTER PTO\_AZUL

**Building configuration...****Current configuration:**

!

!

**Versión 12.1***Versión del IOS del router***service timestamps debug uptime****service timestamps log uptime****no service password-encryption***No se está utilizando la encriptación de passwords*

!

**hostname Pto\_Azul***Nombre del Router***enable password cisco***La contraseña para ingresar al modo privilegiado es cisco*

!

!

!

**ip subnet-zero***Sirve para poder usar la dirección de red como IP***spanning-tree vlan 1 priority**

!

**interface Serial0***Tipo y número de la interfaz***ip address 192.168.13.22 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast***Significa que la interfaz no tiene una dirección IP directa de broadcast*

!

**interface Serial1***Tipo y número de la interfaz***no ip address***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast***Significa que la interfaz no tiene una dirección IP directa de broadcast***shutdown**

!

!

!

!

!

**interface FastEthernet0/0***Tipo y número de la interfaz***no ip address****no ip directed-broadcast****shutdown**

!



**interface Bri0**

Tipo y número de la interfaz

**no ip address**

**no ip directed-broadcast**

**shutdown**

!

**router ospf 1**

Protocolo configurado, el 1 significa un identificador de protocolo

**network 192.168.13.20 0.0.0.3 area 0**

Segmento aprendido OSPF

!

**ip classless**

!

!

!

**line con 0**

Consola del router

**password cisco**

Password asignado al usuario normal

**login**

Esta línea es para que aparezca la petición de clave

**line aux 0**

Consola auxiliar

**password cisco**

Password asignado al usuario normal

**login**

Esta línea es para que aparezca la petición de clave

**line vty 0 4**

Consola del router

**password cisco**

Password asignado al usuario privilegiado

**login**

Esta línea es para que aparezca la petición de clave y para poder realizar telnet

!

**end**



Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**).

Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

**Tabla. 7.2** Descripción de las líneas del `show running` mediante iconos

## 7.8.2.2.2 SHOW IP ROUTE ROUTER PTO\_AZUL

**Pto\_Azul#show ip route**

**Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
U - per-user static route**

**Gateway of last resort is not set**

**192.168.13.0/30 is subnetted, 8 subnets**

**C 192.168.13.20 is directly connected, Serial0**

Segmento de red conectado directamente al router - Serial conectada  
Al ser C va conectada directamente

**O 192.168.13.24 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.28 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.32 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.0 [110/64] via 192.168.13.21, 00:50:03, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF.

El 110 es la distancia administrativa por default en OSPF.

El 64 es el número de saltos que realiza OSPF.

El 00:50:03 es el tiempo que se tardó en conectarse.

**O 192.168.13.4 [110/64] vía 192.168.13.21, 00:50:03, Serial0**  
 Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

*Al ser O el protocolo es OSPF*

*El 110 es la distancia administrativa por default en OSPF*

*El 64 es el número de saltos que realiza OSPF*

*El 00:50:03 es el tiempo que se tardó en conectarse*

**O 192.168.13.36 [110/64] vía 192.168.13.21, 00:30:05, Serial0**  
 Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

*Al ser O el protocolo es OSPF*

*El 110 es la distancia administrativa por default en OSPF.*

*El 64 es el número de saltos que realiza OSPF.*

*El 00:30:05 es el tiempo que se tardó en conectarse.*



### Importante

Explicación del comando show ip route :

**C 192.168.13.0/30 is directly connected, Serial0**

- C : Segmento de red, conectado directamente al router.
- 192.168.13.0/30 : Dirección de Red- Máscara
- Serial0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**O 192.168.13.4 [110/64] via 192.168.13.21, 00:00:12, Serial0**

- O : Protocolo OSPF
- 192.168.13.3 : Dirección de Red
- 110 : distancia administrativa por default en OSPF
- 64 : Número de saltos que realiza OSPF.
- 192.168.13.21 : Interfaz a la que llega
- 00:00:12 : Tiempo que se tardó en conectarse.
- Serial 0 : Interfaz saliente

### 7.8.2.3 ROUTER CEIBOS

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start  
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>  
Router>enable  
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal  
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asignara el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname Ceibos  
Nombre asignado al router  
Ceibos (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
Ceibos (config) #line console 0  
Consola a la que se le asignara la contraseña  
Ceibos (config-line) #password cisco  
Contraseña establecida  
Ceibos (config-line) #login  
Se usa para que solicite contraseña al ingresar  
Ceibos (config-line) #exit  
Sale de la configuración de la consola  
Ceibos (config) #
```

**Ceibos (config) #line vty 0 4**

Ingresar a configurar la Terminal Virtual

**Ceibos (config-line) #password cisco**

Contraseña establecida

**Ceibos (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Ceibos (config-line) #exit**

Salir de la configuración de la consola

**Ceibos (config) #**

**Ceibos (config) #line aux 0**

Ingresar a configurar el puerto auxiliar

**Ceibos (config-line) #password cisco**

Contraseña establecida

**Ceibos (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Ceibos (config-line) #exit**

Salir de la configuración de la consola

**Ceibos (config) #**

**Ceibos (config-line) #enable password cisco**

Agregar una contraseña para ingresar al router

**Ceibos (config-line) #enable secret cisco**

Agregar una contraseña encriptada para ingresar al router

### Configuración de las Interfaces

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Ceibos (config) #interface serial 0**

Interfaz y tipo que va a ser configurada

**Ceibos (config-if) #ip address 192.168.13.26 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial



#### Importante

En este router se omite el **clock rate** debido a que esta interfaz es un DTE (data terminal equipment).

7. Una vez finalizado se procede a levantar la interfaz con el siguiente comando.

**Ceibos (config-if) #no shutdown**

Levanta la interfaz

**%LINK-3-UPDOWN:** Interface Serial0, changed state to up  
Indica que la interfaz ha cambiado y su respectivo estado

**Ceibos (config-if) #**



#### Sugerencia

Puede que les aparezca unos mensajes similar a los que se muestran en la parte inferior lo que da a entender que la interfaz no se levanto, esto indica que la interfaz conectada en el siguiente router aun no a sido configurada

**%LINK-3-UPDOWN:** Interface Serial0, changed state to down  
Indica que la interfaz ha cambiado y su respectivo estado

**%LINEPROTO-5-UPDOWN:** Line protocol on Interface Serial0, changed state to down

El protocolo, la interfaz y el respectivo estado al que ha cambiado la o las interfaces de los routers cercanos

### Configuración de Protocolo de Enrutamiento OSPF

El protocolo de enrutamiento OSPF debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

8. Se ingresa al modo de configuración global

**Ceibos#**

**Ceibos#configure terminal**

Entrar al modo de configuración global

9. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

**Ceibos (config) #router ospf 1**

Protocolo a configurar

10. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es OSPF va con su respectiva willcard y el área)

**Ceibos (config-router) # network 192.168.13.24 0.0.0.3 area 0**  
DIRECCIÓN DE RED WILLCARD ÁREA

Es la dirección de red del segmento conectado al router

**Ceibos (config-router) #**

### Guardar configuración

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

```
Ceibos#copy running-config startup-config
```

Guarda una copia de la configuración en la NVRAM

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.



## 7.8.2.3.1 SHOW RUNNING ROUTER CEIBOS

**Building configuration...****Current configuration: 555 bytes****Versión 12.1**

Versión del IOS del router

**service timestamps debug uptime****service timestamps log uptime****no service password-encryption**

No se está utilizando la encriptación de passwords

!

**hostname Ceibos**

Nombre del Router

**enable password cisco**

La contraseña para ingresar al modo privilegiado es cisco

!

!

!

**ip subnet-zero**

Sirve para poder usar la dirección de red como IP

**spanning-tree vlan 1 priority**

!

**interface Serial0**

Tipo y número de la interfaz

**ip address 192.168.13.26 255.255.255.252**

Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default

**no ip directed-broadcast**

Significa que la interfaz no tiene una dirección IP directa de broadcast

!

**interface Serial1**

Tipo y número de la interfaz

**no ip address**

Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default

**no ip directed-broadcast**

Significa que la interfaz no tiene una dirección IP directa de broadcast

**shutdown**

!

**interface FastEthernet0/0**

Tipo y número de la interfaz

**no ip address****no ip directed-broadcast****shutdown**

!

**interface Bri0**

Tipo y número de la interfaz

**no ip address****no ip directed-broadcast****shutdown**

```

!
router ospf 1
  Protocolo configurado, el 1 significa un identificador de protocolo
  network 192.168.13.24 0.0.0.3 area 0
  Segmento aprendido OSPF
!
ip classless
!
!
!
line con 0
  Consola del router
  password cisco
  Password asignado al usuario normal
  login
  Esta línea es para que aparezca la petición de clave
  line aux 0
  Consola auxiliar
  password cisco
  Password asignado al usuario normal
  login
  Esta línea es para que aparezca la petición de clave
  line vty 0 4
  Consola del router

  password cisco
  Password asignado al usuario privilegiado
  login
  Esta línea es para que aparezca la petición de clave y para poder realizar telnet
!
end

```



Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**).  
 Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

Tabla. 7.3 Descripción de las líneas del show running mediante iconos



## 7.8.2.3.2 SHOW IP ROUTE ROUTER CEIBOS

**Ceibos#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
U - per-user static route

**Gateway of last resort is not set**

**192.168.13.0/30 is subnetted, 1 subnets**

**C 192.168.13.24 is directly connected, Serial0**

Segmento de red conectado directamente al router - Serial conectada  
Al ser C va conectada directamente

**O 192.168.13.24 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.28 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.32 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.0 [110/64] via 192.168.13.21, 00:50:03, Serial0**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser O el protocolo es OSPF.

El 110 es la distancia administrativa por default en OSPF.

El 64 es el número de saltos que realiza OSPF.

El 00:50:03 es el tiempo que se tardó en conectarse.

**O 192.168.13.4 [110/64] vía 192.168.13.21, 00:50:03, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:03 es el tiempo que se tardó en conectarse

**O 192.168.13.36 [110/64] vía 192.168.13.21, 00:30:05, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF.

El 64 es el número de saltos que realiza OSPF.

El 00:30:05 es el tiempo que se tardó en conectarse.

**Importante**

Explicación del comando show ip route :

**C 192.168.13.24/30 is directly connected, Serial0**

- C : Segmento de red ,conectado directamente al router.
- 192.168.13.24/30 : Dirección de Red- Máscara
- Serial0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**O 192.168.13.4 [110/64] via 192.168.13.21, 00:00:12, Serial0**

- O : Protocolo OSPF
- 192.168.13.4 : Dirección de Red
- 110 : distancia administrativa por default en OSPF
- 64 : Número de saltos que realiza OSPF.
- 192.168.13.21 : Interfaz a la que llega
- 00:00:12 : Tiempo que se tardó en conectarse.
- Serial 0 : Interfaz saliente



BIBLIOTECA  
CAMPUS

ESPOL

### 7.8.2.4 ROUTER PUERTO CENTENARIO

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start  
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>  
Router>enable  
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal  
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asignara el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname Centenario  
Nombre asignado al router
```

```
Centenario (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
Centenario (config) #line console 0  
Consola a la que se le asignara la contraseña
```

```
Centenario (config-line) #password cisco  
Contraseña establecida
```

```
Centenario (config-line) #login  
Se usa para que solicite contraseña al ingresar
```

```
Centenario (config-line) #exit  
Sale de la configuración de la consola
```

```
Centenario (config) #
```

```
Centenario (config) #line vty 0 4  
Ingresa a configurar la Terminal Virtual
```

```
Centenario (config-line) #password cisco  
Contraseña establecida
```

**Centenario (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Centenario (config-line) #exit**

Sale de la configuración de la consola

**Centenario (config) #****Centenario (config) #line aux 0**

Ingresa a configurar el puerto auxiliar

**Centenario (config-line) #password cisco**

Contraseña establecida

**Centenario (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Centenario (config-line) #exit**

Sale de la configuración de la consola

**Centenario (config) #****Centenario (config-line) #enable password cisco**

Agrega una contraseña para ingresar al router

**Centenario (config-line) #enable secret cisco**

Agrega una contraseña encriptada para ingresar al router

**Configuración de las Interfaces**

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Centenario (config) #interface serial 0**

Interfaz y tipo que va a ser configurada

**Centenario (config-if) #ip address 192.168.13.29 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial.

**Importante**

En este router se obvia el **clock rate** debido a que esta interfaz es un DTE (data terminal equipment).

7. Una vez finalizado se procede a levantar la interfaz con el siguiente comando.

**Centenario (config-if) #no shutdown**

Levanta la interfaz

**%LINK-3-UPDOWN: Interface Serial0, changed state to up**

Indica que la interfaz ha cambiado y su respectivo estado

**Centenario (config-if) #**

**Sugerencia**

Puede que les aparezca unos mensajes similar a los que se muestran en la parte inferior lo que da a entender que la interfaz no se levantó, esto indica que la interfaz conectada en el siguiente router aún no a sido configurada

**%LINK-3-UPDOWN:** Interface Serial0, changed state to down

Indica que la interfaz ha cambiado y su respectivo estado

**%LINEPROTO-5-UPDOWN:** Line protocol on Interface Serial0, changed state to down

El protocolo, la interfaz y el respectivo estado al que ha cambiado la o las interfaces de los routers cercanos

**Configuración de Protocolo de Enrutamiento OSPF**

El protocolo de enrutamiento OSPF debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

8. Se ingresa al modo de configuración global

**Ceibos#**

**Ceibos#configure terminal**

Entrar al modo de configuración global

9. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

**Ceibos (config) #router ospf 1**

Protocolo a configurar

10. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es OSPF va con su respectiva willcard y el área)

**Centenario (config-router) #network 192.168.13.28 0.0.0.3 area 0**  
DIRECCIÓN DE RED WILLCARD ÁREA

Red que aprende

Es la dirección de red del segmento conectado al router

**Centenario (config-router) #**

**Guardar configuración**

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

**Centenario#copy running-config startup-config**

Guarda una copia de la configuración en la NVRAM

## 7.8.2.4.1 SHOW RUNNING ROUTER CENTENARIO

**Building configuration...****Current configuration:**

!

**Version 12.1***Versión del IOS del router***service timestamps debug uptime****service timestamps log uptime****no service password-encryption***No se está utilizando la encriptación de passwords*

!

**hostname Centenario***Nombre del Router***enable password cisco***La contraseña para ingresar al modo privilegiado es cisco*

!

!

!

**ip subnet-zero***Sirve para poder usar la dirección de red como IP***spanning-tree vlan 1 priority**

!

**interface Serial0***Tipo y número de la interfaz***ip address 192.168.13.29 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast***Significa que la interfaz no tiene una dirección IP directa de broadcast*

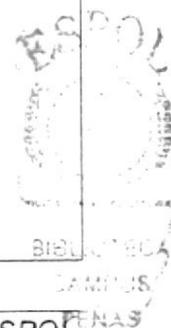
!

**interface Serial1***Tipo y número de la interfaz***no ip address***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast***Significa que la interfaz no tiene una dirección IP directa de broadcast***shutdown**

!

**interface FastEthernet0/0***Tipo y número de la interfaz***no ip address****no ip directed-broadcast****shutdown**

!



**interface Bri0***Tipo y número de la interfaz***no ip address****no ip directed-broadcast****shutdown**

!

**router ospf 1***Protocolo configurado, el 1 significa un identificador de protocolo***network 192.168.13.28 0.0.0.3 area 0***Segmento aprendido OSPF*

!

**ip classless**

!

!

!

**line con 0***Consola del router***password cisco***Password asignado al usuario normal***login***Esta línea es para que aparezca la petición de clave***line aux 0***Consola auxiliar***password cisco***Password asignado al usuario normal***login***Esta línea es para que aparezca la petición de clave***line vty 0 4***Consola del router***password cisco***Password asignado al usuario privilegiado***login***Esta línea es para que aparezca la petición de clave y para poder realizar telnet*

!

**end**

Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**).  
 Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

Tabla. 7.4 Descripción de las líneas del show running mediante iconos

## 7.8.2.4.2 SHOW IP ROUTE ROUTER CENTENARIO

Centenario#

Centenario#sho ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
U - per-user static route

**Gateway of last resort is not set**

**192.168.13.0/30 is subnetted, 1 subnets**

**C 192.168.13.28 is directly connected, Serial0**

Segmento de red conectado directamente al router - Serial conectada  
Al ser C va conectada directamente

**O 192.168.13.24 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.28 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.32 [110/64] via 192.168.13.21, 00:50:09, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:09 es el tiempo que se tardó en conectarse

**O 192.168.13.0 [110/64] via 192.168.13.21, 00:50:03, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF.

El 110 es la distancia administrativa por default en OSPF.

El 64 es el número de saltos que realiza OSPF.

El 00:50:03 es el tiempo que se tardó en conectarse.

**O 192.168.13.4 [110/64] vía 192.168.13.21, 00:50:03, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF

El 64 es el número de saltos que realiza OSPF

El 00:50:03 es el tiempo que se tardó en conectarse

**O 192.168.13.36 [110/64] vía 192.168.13.21, 00:30:05, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser O el protocolo es OSPF

El 110 es la distancia administrativa por default en OSPF.

El 64 es el número de saltos que realiza OSPF.

El 00:30:05 es el tiempo que se tardó en conectarse.

**Importante**

Explicación del comando show ip route :

**C 192.168.13.28/30 is directly connected, Serial0**

- C : Segmento de red ,conectado directamente al router.
- 192.168.13.28/30 : Dirección de Red- Máscara
- Serial0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**O 192.168.13.4 [110/64] via 192.168.13.21, 00:00:12, Serial0**

- O : Protocolo OSPF
- 192.168.13.3 : Dirección de Red
- 110 : distancia administrativa por default en OSPF
- 64 : Número de saltos que realiza OSPF.
- 192.168.13.21 : Interfaz a la que llega
- 00:00:12 : Tiempo que se tardó en conectarse.
- Serial 0 : Interfaz saliente



### 7.8.2.5 ROUTER SAMBORONDON

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

**Press Enter to Start**  
Presionar enter para empezar

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

**Router>**  
**Router>enable**  
Ingresa al modo privilegiado

3. Digitar el comando **configure terminal** para acceder a la configuración global.

**Router#configure terminal**  
Entra al modo de configuración global

#### Configuración de los nombres de los Routers

4. Se le asignara el respectivo nombre en el modo de configuración global.

**Router (config) #hostname Samborondon**  
Nombre asignado al router

**Samborondon (config) #**

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

**Samborondon (config) #line console 0**  
Consola a la que se le asignara la contraseña

**Samborondon (config-line) #password cisco**  
Contraseña establecida

**Samborondon (config-line) #login**  
Se usa para que solicite contraseña al ingresar

**Samborondon (config-line) #exit**  
Sale de la configuración de la consola

**Samborondon (config) #**

**Samborondon (config) #line vty 0 4**  
Ingresa a configurar la Terminal Virtual

**Samborondon (config-line) #password cisco**  
Contraseña establecida



**Samborondon (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Samborondon (config-line) #exit**

Sale de la configuración de la consola

**Samborondon (config) #****Samborondon (config) #line aux 0**

Ingresa a configurar el puerto auxiliar

**Samborondon (config-line) #password cisco**

Contraseña establecida

**Samborondon (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Samborondon (config-line) #exit**

Sale de la configuración de la consola

**Samborondon (config) #****Samborondon (config-line) #enable password cisco**

Agrega una contraseña para ingresar al router

**Samborondon (config-line) #enable secret cisco**

Agrega una contraseña encriptada para ingresar al router

### Configuración de las Interfaces

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Samborondon (config) #interface serial 0**

Interfaz y tipo que va a ser configurada

**Samborondon (config-if) #ip address 192.168.13.33 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial.

**Importante**

En este router se obvia el **clock rate** debido a que esta interfaz es un DTE (data terminal equipment).

7. Una vez finalizado se procede a levantar la interfaz con el siguiente comando.

**Samborondon (config-if) #no shutdown**

Levanta la interfaz

**%LINK-3-UPDOWN:** Interface Serial0, changed state to up

Indica que la interfaz ha cambiado y su respectivo estado

**Samborondon (config-if) #**

**Sugerencia**

Puede que les aparezca unos mensajes similar a los que se muestran en la parte inferior lo que da a entender que la interfaz no se levanto, esto indica que la interfaz conectada en el siguiente router aun no a sido configurada

**%LINK-3-UPDOWN:** Interface Serial0, changed state to down Indica que la interfaz ha cambiado y su respectivo estado

**%LINEPROTO-5-UPDOWN:** Line protocol on Interface Serial0, changed state to down

El protocolo, la interfaz y el respectivo estado al que ha cambiado la o las interfaces de los routers cercanos

**Configuración de Protocolo de Enrutamiento OSPF**

El protocolo de enrutamiento OSPF debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

8. Se ingresa al modo de configuración global

**Samborondon#**

**Samborondon #configure terminal**

Entrar al modo de configuración global

9. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

**Samborondon (config) #router ospf 1**

Protocolo a configurar

10. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es **OSPF** va con su respectiva willcard y el área)

**Samborondon (config-router) #network 192.168.13.32 0.0.0.3 area 0**  
DIRECCIÓN DE RED WILLCARD ÁREA

Red que aprende

Es la dirección de red del segmento conectado al router

**Samborondon (config-router) # wr**

**Guardar configuración**

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán.

**Samborondon** #copy running-config startup-config  
Guarda una copia de la configuración en la NVRAM

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

## 7.8.2.5.1 SHOW RUNNING ROUTER SAMBORONDON

**Building configuration...****Current configuration:**

!

**Versión 12.1***Versión del IOS del router***service timestamps debug uptime****service timestamps log uptime****no service password-encryption***No se está utilizando la encriptación de password*

!

**hostname Samborondon***Nombre del Router***enable password cisco***La contraseña para ingresar al modo privilegiado es cisco*

!

!

!

**ip subnet-zero***Sirve para poder usar la dirección de red como IP***spanning-tree vlan 1 priority**

!

**interface Serial0***Tipo y número de la interfaz***ip address 192.168.13.33 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast***Significa que la interfaz no tiene una dirección IP directa de broadcast*

!

**interface Serial1***Tipo y número de la interfaz***no ip address***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast***Significa que la interfaz no tiene una dirección IP directa de broadcast***shutdown**

!

**interface FastEthernet0/0***Tipo y número de la interfaz***no ip address****no ip directed-broadcast****shutdown**

!

**interface Bri0***Tipo y número de la interfaz***no ip address****no ip directed-broadcast**

<pre> <b>shutdown</b> ! <b>router ospf 1</b> <i>Protocolo configurado, el 1 significa un identificador de protocolo</i> <b>network 192.168.13.32 0.0.0.3 area 0</b> <i>Segmento aprendido OSPF</i> ! <b>ip classless</b> ! ! ! <b>line con 0</b> <i>Consola del router</i> <b>password cisco</b> <i>Password asignado al usuario normal</i> <b>login</b> <i>Esta línea es para que aparezca la petición de clave</i> <b>line aux 0</b> <i>Consola auxiliar</i> <b>password cisco</b> <i>Password asignado al usuario normal</i> <b>login</b> <i>Esta línea es para que aparezca la petición de clave</i> <b>line vty 0 4</b> <i>Consola del router</i>  <b>password cisco</b> <i>Password asignado al usuario privilegiado</i> <b>login</b> <i>Esta línea es para que aparezca la petición de clave y para poder realizar telnet</i> ! <b>end</b> </pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**).  
 Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

**Tabla. 7.5** Descripción de las líneas del `show running` mediante iconos

## 7.8.2.5.2 SHOW IP ROUTE ROUTER SAMBORONDON

**Samborondon#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
 U - per-user static route

**Gateway of last resort is not set**

**192.168.13.0/30 is subnetted, 8 subnets**

**C 192.168.13.32 is directly connected, Serial0**

Segmento de red conectado directamente al router - Interfaz conectada  
 Al ser C va conectada directamente

**O 192.168.13.20 [110/128] vía 192.168.13.34, 00:35:14, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega  
 Al ser O el protocolo es Ospf

El 110 es la distancia administrativa por default en OSpf  
 El 128 es el número de saltos que realiza Ospf  
 El 00:35:14 es el tiempo que se tardó en conectarse

**O 192.168.13.24 [110/64] vía 192.168.13.34, 00:35:14, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega  
 Al ser O el protocolo es Ospf

El 110 es la distancia administrativa por default en OSpf  
 El 64 es el número de saltos que realiza Ospf  
 El 00:35:14 es el tiempo que se tardó en conectarse

**O 192.168.13.28 [110/64] vía 192.168.13.34, 00:35:14, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega  
 Al ser O el protocolo es Ospf

El 110 es la distancia administrativa por default en OSpf  
 El 64 es el número de saltos que realiza Ospf  
 El 00:35:14 es el tiempo que se tardó en conectarse

**O 192.168.13.0 [110/64] vía 192.168.13.34, 00:35:08, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega  
 Al ser O el protocolo es Ospf

El 110 es la distancia administrativa por default en OSpf  
 El 64 es el número de saltos que realiza Ospf  
 El 00:35:14 es el tiempo que se tardo en conectarse

**O 192.168.13.4 [110/64] vía 192.168.13.34, 00:35:08, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega  
 Al ser O el protocolo es Ospf

El 110 es la distancia administrativa por default en OSpf  
 El 64 es el número de saltos que realiza Ospf  
 El 00:35:14 es el tiempo que se tardó en conectarse

**O 192.168.13.8 [110/64] vía 192.168.13.34, 00:35:08, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega

Al ser O el protocolo es Ospf

El 110 es la distancia administrativa por default en OSpf

El 64 es el número de saltos que realiza Ospf

El 00:35:14 es el tiempo que se tardó en conectarse

**O 192.168.13.36 [110/64] vía 192.168.13.34, 00:35:08, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega

Al ser O el protocolo es Ospf

El 110 es la distancia administrativa por default en OSpf

El 64 es el número de saltos que realiza Ospf

El 00:35:14 es el tiempo que se tardó en conectarse



### Importante

Explicación del comando show ip route :

**C 192.168.13.32 is directly connected, Serial0**

- C : Segmento de red ,conectado directamente al router.
- 192.168.13.32/30 : Dirección de Red- Máscara
- Serial0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**O 192.168.13.36 [110/64] vía 192.168.13.34, 00:35:08, Serial0**

- O : Protocolo OSPF
- 192.168.13.36 : Dirección de Red
- 110 : distancia administrativa por default en OSPF
- 64 : Número de saltos que realiza OSPF.
- 192.168.13.34 : Interfaz a la que llega
- 00:00:12 : Tiempo que se tardó en conectarse.
- Serial 0 : Interfaz saliente

### 7.8.2.6 ROUTER LOJA

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start  
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>  
Router>enable  
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal  
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asignara el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname Loja  
Nombre asignado al router
```

```
Loja (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
Loja (config) #line console 0  
Consola a la que se le asignara la contraseña
```

```
Loja (config-line) #password cisco  
Contraseña establecida
```

```
Loja (config-line) #login  
Se usa para que solicite contraseña al ingresar
```

```
Loja (config-line) #exit  
Sale de la configuración de la consola
```

```
Loja (config) #
```

```
Loja (config) #line vty 0 4  
Ingresa a configurar la Terminal Virtual
```

```
Loja (config-line) #password cisco  
Contraseña establecida
```

**Loja (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Loja (config-line) #exit**

Sale de la configuración de la consola

**Loja (config) #**

**Loja (config) #line aux 0**

Ingresa a configurar el puerto auxiliar

**Loja (config-line) #password cisco**

Contraseña establecida

**Loja (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Loja (config-line) #exit**

Sale de la configuración de la consola

**Loja (config) #**

**Loja (config-line) #enable password cisco**

Agrega una contraseña para ingresar al router

**Loja (config-line) #enable secret cisco**

Agrega una contraseña encriptada para ingresar al router

### Configuración de las Interfaces

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Loja(config)#interface serial 0/0**

Interfaz a configurar

**Loja (config-if)#ip address 192.168.13.9 255.255.255.252**

Dirección y máscara asignada, es 252 debido a ser una interfaz serial

7. Proceda a levantar la interfaz con el siguiente comando

**Loja (config-if)#no shutdown**

Levanta la interfaz

**%LINK-3-UPDOWN: Interface Serial0/0, changed state to up**

Indica que la interfaz ha cambiado y su respectivo estado

8. Después de esto salga del modo de configuración con el comando exit para pasar a configurar la siguiente interfaz.

**Loja (config-if)#exit**

Sale de la configuración de la interfaz

**Loja (config)#exit**

Sale de la configuración global

**Loja #**

**Importante**

En este router se obvia el **clock rate** debido a que esta interfaz es un **DTE** (data terminal equipment).

9. Digitar el comando `configure terminal` para acceder a la configuración global.

**Loja #configure terminal**

Entra al modo de configuración global

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir

10. En este momento se procede a ingresar a la siguiente interfaz para asignarle la dirección respectiva establecida en el gráfico WAN anteriormente expuesto.

**Loja (config)#interface serial 0/1**

Interfaz y tipo que va a ser configurada

**Loja (config-if)#ip address 192.168.13.38 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial

11. Se le asignara su respectivo **clock rate** debido a que esta interfaz es un **DCE** (data communication equipment)

**Loja (config-if)#clock rate 64000**

El **clock rate** lo que permite es la sincronización de datos con los demás routers es 64000 para obtener una mayor velocidad.

12. Proceda a levantar la interfaz con el siguiente comando.

**Loja (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN: Interface Serial0/1, changed state to up**

Indica que la interfaz ha cambiado y su respectivo estado

**Loja (config-if)#**

13. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

**Loja (config)#interface serial 0/2**

Interfaz y tipo que va a ser configurada

**Loja (config-if)#ip address 192.168.13.6 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial

**Importante**

En este router se obvia el **clock rate** debido a que esta interfaz es un **DTE** (data terminal equipment).

14. Proceda a levantar la interfaz con el siguiente comando.

**Loja (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN:** Interface Serial0/2, changed state to up  
Indica que la interfaz ha cambiado y su respectivo estado

15. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

**Loja (config)#interface serial 0/3**

Interfaz y tipo que va a ser configurada

**Loja (config-if)#ip address 192.168.13.13 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial

16. Se le asignara su respectivo clock rate debido a que esta interfaz es un DCE (data communication equipment)

**Loja (config-if)#clock rate 64000**

El clock rate lo que permite es la sincronización de datos con los demás routers es 64000 para obtener una mayor velocidad.

17. Proceda a levantar la interfaz con el siguiente comando.

**Loja (config-if)#no shut**

Levanta la interfaz configurada

**%LINK-3-UPDOWN:** Interface Serial0/3, changed state to up  
Indica que la interfaz ha cambiado y su respectivo estado

18. Para finalizar con las configuraciones se le asignara el respectivo nombre en el modo de configuración global.

**Loja #configure terminal**

Entra al modo de configuración global

### Configuración de Protocolo de Enrutamiento RIP

El protocolo de enrutamiento RIP debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

19. Se ingresa al modo de configuración global

**Loja#**

**Loja #configure terminal**

Entrar al modo de configuración global

20. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

**Loja(config)#router rip**

Protocolo a configurar

**Loja (config-router) #version 2**

Versión del protocolo

21. Se establece el segmento de red que se requiere para que este router aprenda.

**Loja (config-router) #network 192.168.13.4**  
DIRECCIÓN DE RED

**Loja (config-router) #network 192.168.13.8**

**Loja (config-router) #network 192.168.13.12**

**Loja (config-router) #network 192.168.13.36**

**Loja (config-router) #network 192.168.11.0**

**Loja (config-router) #network 192.168.11.8**

**Loja (config-router) #network 192.168.11.16**

**Loja (config-router) #network 192.168.11.24**

**Loja (config-router) #network 192.168.11.32**

Red que aprende

Es la dirección de red del segmento conectado al router

**Loja (config-router) #**

### Configuración de ACL



#### Importante

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list : comando
- 1-99 , 1300-1 999 : # acl estandar
- permit/deny : permitir o denegar una red específica
- source : ( direccion de red – willcard)
- any : cualquier host o red

Bloquear toda la subred 192.168.11.16/24, excepto los servidores 192.168.11.0/28

**Loja #configure Terminal**

*Ingresa al modo de configuración global*

**Loja (config) #access-list 1 permit 192.168.11.0 0.0.0.3**

*Asigna permiso a una subred específica*

**Loja (config) #access-list 1 deny 192.168.11.16 0.0.0.255**

*Niega el acceso a la red a las demás ip's*

**Loja (config) #access-list 1 permit any**

*Luego poner una línea implícita para esta acl*

**Loja (config) #exit**

*Sale del modo de configuración global*

*Luego levantar la acl estándar en la interfaz correspondiente.*

**Loja #configure terminal**

*Ingresa al modo de configuración global*

**Loja (config) #interface fastethernet 0/0**

*Ingresa a la interfaz que quiere asignar la acl*

**Loja (config) #ip access-group 1 in**

*Levanta la acl de manera entrante*

## ACL extendida



### Importante

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list : comando
- 100-199, 2000-2699 : # acl extendida
- permit/deny : permitir o denegar una red específica
- source : ( dirección de red – willcard)
- any : cualquier host o red

**Loja #configure terminal**

*Ingresa al modo de configuración global*

**Loja (config) #access-list 101 permit 192.168.11.32 0.0.0.7 192.168.10.0 0.0.0.3**

*Asigna permiso específico*

**Loja (config) #access-list 101 deny 192.168.11.64 0.0.0.7 192.168.10.0 0.0.0.3**

*Niega el acceso a la red a las demás ip's*

**Loja (config) #access-list 101 permit any any**

*Luego poner una línea implícita para esta acl*

**Loja (config) #exit**

*Sale del modo de configuración global*



Luego levantar la acl extendida en la interfaz correspondiente.

**Loja #configure terminal**

*Ingresa al modo de configuración global*

**Loja (config) #interface fastethernet 0/0**

*Ingresa a la interfaz que quiere asignar la acl*

**Loja (config) #ip access-group 101 in**

*Levanta la acl de manera entrante*

*Permitir tráfico (ICMP) desde una subred hacia el servidor*

**Loja #configure terminal**

*Ingresa al modo de configuración global*

**Loja (config) #access-list 102 permit icmp 192.168.11.32 0.0.0.7 192.168.11.0 0.0.0.3**

*Asigna permiso específico*

**Loja (config) #access-list 102 deny any any**

*Se coloca una línea implícita*



#### Importante

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list: comando
- 100-199, 2000-2699 : # acl extendida
- permit/deny : permitir o denegar una red específica
- icmp : protocolo puede ser (entre otros) IP (todo tráfico de tipo TCP/IP), TCP, UDP, ICMP.
- source : ( dirección de red – wildcard)
- any : cualquier host o red

#### Guardar configuración

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

**Loja #copy running-config startup-config**

*Guarda una copia de la configuración en la NVRAM*

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

## 7.8.2.6.1 SHOW RUNNING ROUTER LOJA

**Building configuration...****Current configuration:**

!

**Version 12.1***Versión del IOS del router***service timestamps debug uptime****service timestamps log uptime****no service password-encryption***No se esta utilizando la encriptación de passwords*

!

**hostname Loja***Nombre del Router***enable password cisco***La contraseña para ingresar al modo privilegiado es cisco*

!

**ip subnet-zero***Sirve para poder usar la dirección de red como IP***spanning-tree vlan 1 priority**

!

**interface Serial0/0***Tipo y número de la interfaz***ip address 192.168.13.9 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast**

!

**interface Serial0/1***Tipo y número de la interfaz***ip address 192.168.13.38 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast****clock rate 64000***Indica la velocidad del puerto en bits por segundo, lo encuentra en el DCE*

!

**interface Serial0/2***Tipo y número de la interfaz***ip address 192.168.13.6 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast**

!

**interface Serial0/3***Tipo y número de la interfaz***ip address 192.168.13.13 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast**

!

**interface FastEthernet1/0**

Tipo y número de la interfaz

**no ip address****no ip directed-broadcast****shutdown**

!

**interface FastEthernet1/0.10**

Tipo y número de la interfaz

**encapsulation dotq 10**

encapsulamiento asociado a la vlan 10

**ip address 192.168.11.1 255.255.255.248**

Dirección IP – Máscara

**no ip directed-broadcast**

!

!

**interface FastEthernet1/0.20**

Tipo y número de la interfaz

**encapsulation dotq 20**

encapsulamiento asociado a la vlan 20

**ip address 192.168.11.9 255.255.255.248**

Dirección IP – Máscara

**no ip directed-broadcast**

!

!

**interface FastEthernet1/0.30**

Tipo y número de la interfaz

**encapsulation dotq 30**

encapsulamiento asociado a la vlan 30

**ip address 192.168.11.17 255.255.255.248**

Dirección IP – Máscara

**no ip directed-broadcast**

!

!

**interface FastEthernet1/0.40**

Tipo y número de la interfaz

**encapsulation dotq 40**

encapsulamiento asociado a la vlan 40

**ip address 192.168.11.25 255.255.255.248**

Dirección IP – Máscara

**no ip directed-broadcast**

!

**interface FastEthernet1/0.50**

Tipo y número de la interfaz

**encapsulation dotq 50**

encapsulamiento asociado a la vlan 50

**ip address 192.168.11.33 255.255.255.248**

Dirección IP – Máscara

**no ip directed-broadcast**

!

```

interface Bri1/0
  no ip address
  no ip directed-broadcast
  shutdown
  !
router rip
  Protocolo configurado
  version 2
  Version del protocolo configurado, el 1 significa un identificador de protocolo
  network 192.168.13.0
  network 192.168.11.0
  Segmento aprendido RIP
  !
  !
  ip classless
  !
  line con 0
  Consola del router
  password cisco
  Password asignado al usuario normal
  login
  Esta línea es para que aparezca la petición de clave
  line aux 0
  Consola auxiliar
  password cisco
  Password asignado al usuario normal
  login
  Esta línea es para que aparezca la petición de clave
  line vty 0 4
  Consola del router
  password cisco
  Password asignado al usuario privilegiado
  login
  Esta línea es para que aparezca la petición de clave y para poder realizar telnet
  !
end

```



Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**).  
 Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

**Tabla. 7.6** Descripción de las líneas del show running mediante iconos

### 7.8.2.6.2 SHOW IP ROUTE ROUTER LOJA

#### Loja#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
U - per-user static route

#### Gateway of last resort is not set

**192.168.13.0/30 is subnetted, 7 subnets**

**C 192.168.13.8 is directly connected, Serial0/0**

**C 192.168.13.36 is directly connected, Serial0/1**

**C 192.168.13.4 is directly connected, Serial0/2**

Segmento de red conectado directamente al router - Interfaz conectada  
Al ser C va conectada directamente

**R 192.168.13.20 [120/1] vía 192.168.13.5, 00:06:14, Serial0/2**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:06:14 es el tiempo que se tardó en conectarse

**R 192.168.13.24 [120/1] vía 192.168.13.5, 00:09:43, Serial0/2**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:43 es el tiempo que se tardó en conectarse

**R 192.168.13.28 [120/1] vía 192.168.13.5, 00:03:44, Serial0/2**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:03:44 es el tiempo que se tardó en conectarse

**R 192.168.13.32 [120/1] vía 192.168.13.5, 00:09:40, Serial0/2**

Protocolo - dirección de red conectada - interfaz a la que llega - interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:40 es el tiempo que se tardó en conectarse



### Importante

Explicación del comando show ip route :

**C 192.168.13.8 is directly connected, Serial0/0**

- C : Segmento de red ,conectado directamente al router.
- 192.168.13.8 : Dirección de Red- Máscara
- Serial0/0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**R 192.168.13.20 [120/1] vía 192.168.13.5, 00:06:14, Serial0/2**

- R : Protocolo RIP
- 192.168.13.20 : Dirección de Red
- 120 : distancia administrativa por default en RIP.
- 1 : Número de saltos que realiza RIP.
- 192.168.13.5 : Interfaz a la que llega
- 00:06:14 : Tiempo que se tardo en conectarse.
- Serial 0/2 : Interfaz saliente

### 7.8.2.7 ROUTER MACARA

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>
Router>enable
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asigna el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname Macara
Nombre asignado al router
Macara (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
Macara (config) #line console 0
Consola a la que se le asigna la contraseña
Macara (config-line) #password cisco
Contraseña establecida
Macara (config-line) #login
Se usa para que solicite contraseña al ingresar
Macara (config-line) #exit
Sale de la configuración de la consola
Macara (config) #
Macara (config) #line vty 0 4
Ingresa a configurar la Terminal Virtual
Macara (config-line) #password cisco
Contraseña establecida
```

**Macara (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Macara (config-line) #exit**

Sale de la configuración de la consola

**Macara (config) #****Macara (config) #line aux 0**

Ingresa a configurar el puerto auxiliar

**Macara (config-line) #password cisco**

Contraseña establecida

**Macara (config-line) #login**

Se usa para que se pueda establecer telnet a la interfaz

**Macara (config-line) #exit**

Sale de la configuración de la consola

**Macara (config) #****Macara (config-line) #enable password cisco**

Agrega una contraseña para ingresar al router

**Macara (config-line) #enable secret cisco**

Agrega una contraseña encriptada para ingresar al router

**Configuración de las Interfaces**

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Macara (config) #interface serial 0**

Interfaz y tipo que va a ser configurada

**Macara (config-if) #ip address 192.168.13.37 255.255.255.252**

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial.

**Importante**

En este router se obvia el **clock rate** debido a que esta interfaz es un DTE (data terminal equipment).

### Configuración de Protocolo de Enrutamiento RIP

El protocolo de enrutamiento RIP debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

7. Se ingresa al modo de configuración global

**Macara#****Macara#configure terminal**

Entrar al modo de configuración global

8. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

**Macara (config) #router rip**

Protocolo a configurar

**Macara (config-router) #versión 2**

Versión del protocolo

9. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es **OSPF** va con su respectiva willcard y el área)

**Macara (config-router) #network 192.168.13.36**

Red que aprende

Es la dirección de red del segmento conectado al router

**Macara (config-router) #**

### Guardar configuración

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

**Macara #copy running-config startup-config**

Guarda una copia de la configuración en la NVRAM

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

## 7.8.2.7.1 SHOW RUNNING ROUTER MACARA

**Building configuration...****Current configuration:**

!

**Versión 12.1**

Versión del IOS del router

**service timestamps debug uptime****service timestamps log uptime****no service password-encryption**

No se está utilizando la encriptación de passwords

!

**hostname Macara**

Nombre del Router

**enable password cisco**

La contraseña para ingresar al modo privilegiado es cisco

!

!

!

**ip subnet-zero**

Sirve para poder usar la dirección de red como IP

**spanning-tree vlan 1 priority**

!

**interface Serial0**

Tipo y número de la interfaz

**ip address 192.168.13.37 255.255.255.252**

Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default

**no ip directed-broadcast**

Significa que la interfaz no tiene una dirección IP directa de broadcast

!

**interface Serial1**

Tipo y número de la interfaz

**no ip address**

Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default

**no ip directed-broadcast**

Significa que la interfaz no tiene una dirección IP directa de broadcast

**shutdown**

!

**interface FastEthernet0/0**

Tipo y número de la interfaz

**no ip address****no ip directed-broadcast****shutdown**

!

**interface Bri0**

Tipo y número de la interfaz

**no ip address****no ip directed-broadcast****shutdown**

```

!
router rip
Protocolo configurado
Version 2
Version del protocolo configurado, el 1 significa un identificador de protocolo
network 192.168.13.0
Segmento aprendido RIP
!
ip classless
!
!
!
line con 0
Consola del router
password cisco
Password asignado al usuario normal
login
Esta línea es para que aparezca la petición de clave
line aux 0
Consola auxiliar
password cisco
Password asignado al usuario normal
login
Esta línea es para que aparezca la petición de clave
line vty 0 4
Consola del router
password cisco
Password asignado al usuario privilegiado
login
Esta línea es para que aparezca la petición de clave y para poder realizar
telnet.
!
end

```



Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**).  
 Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

**Tabla. 7.7** Descripción de las líneas del show running mediante iconos.



### 7.8.2.7.2 SHOW IP ROUTE ROUTER MACARA

#### Macara#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default

U - per-user static route

#### Gateway of last resort is not set

**192.168.13.0/30 is subnetted, 7 subnets**

**C 192.168.13.36 is directly connected, Serial0**

Segmento de red conectado directamente al router - Interfaz conectada  
Al ser C va conectada directamente

**R 192.168.13.8 [120/1] vía 192.168.13.38, 00:09:17, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:17 es el tiempo que se tardó en conectarse

**R 192.168.13.4 [120/1] vía 192.168.13.38, 00:08:41, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:08:41 es el tiempo que se tardó en conectarse

**R 192.168.13.20 [120/2] vía 192.168.13.38, 00:03:27, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:03:27 es el tiempo que se tardó en conectarse

**R 192.168.13.24 [120/2] vía 192.168.13.38, 00:01:33, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:01:33 es el tiempo que se tardó en conectarse

**R 192.168.13.28 [120/2] vía 192.168.13.38, 00:08:33, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:08:33 es el tiempo que se tardó en conectarse

**R 192.168.13.32 [120/2] vía 192.168.13.38, 00:09:14, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:14 es el tiempo que se tardó en conectarse



### Importante

Explicación del comando show ip route :

**C 192.168.13.36 is directly connected, Serial0**

- C : Segmento de red ,conectado directamente al router.
- 192.168.13.36 : Dirección de Red- Máscara
- Serial0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**R 192.168.13.28 [120/2] vía 192.168.13.38, 00:08:33, Serial0**

- R : Protocolo RIP
- 192.168.13.28 : Dirección de Red
- 120 : distancia administrativa por default en RIP.
- 2 : Número de saltos que realiza RIP.
- 192.168.13.38 : Interfaz a la que llega
- 00:06:14 : Tiempo que se tardó en conectarse.
- Serial 0/2 : Interfaz saliente

### 7.8.2.8 ROUTER SAN ANTONIO

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start  
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>  
Router>enable  
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal  
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asignara el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname San_Antonio  
Nombre asignado al router  
San_Antonio (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
San_Antonio (config) #line console 0  
Consola a la que se le asignara la contraseña  
San_Antonio (config-line) #password cisco  
Contraseña establecida  
San_Antonio (config-line) #login  
Se usa para que solicite contraseña al ingresar  
San_Antonio (config-line) #exit  
Sale de la configuración de la consola  
San_Antonio (config) #  
San_Antonio (config) #line vty 0 4  
Ingresa a configurar la Terminal Virtual  
San_Antonio (config-line) #password cisco  
Contraseña establecida
```

**San\_Antonio (config-line) #login***Se usa para que se pueda establecer telnet a la interfaz***San\_Antonio (config-line) #exit***Sale de la configuración de la consola***San\_Antonio (config) #****San\_Antonio (config) #line aux 0***Ingresa a configurar el puerto auxiliar***San\_Antonio (config-line) #password cisco***Contraseña establecida***San\_Antonio (config-line) #login***Se usa para que se pueda establecer telnet a la interfaz***San\_Antonio (config-line) #exit***Sale de la configuración de la consola***San\_Antonio (config) #****San\_Antonio (config-line) #enable password cisco***Agrega una contraseña para ingresar al router***San\_Antonio (config-line) #enable secret cisco***Agrega una contraseña encriptada para ingresar al router*

### Configuración de las Interfaces

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Router (config) #interface serial 0***Interfaz y tipo que va a ser configurada***Router (config-if) #ip address 192.168.13.42 255.255.255.252***Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial.***Importante**

En este router se obvia el **clock rate** debido a que esta interfaz es un DTE (data terminal equipment).

7. Proceda a levantar la interfaz con el siguiente comando.

**Ambato (config-if) #no shut***Levanta la interfaz configurada***%LINK-3-UPDOWN: Interface Serial0, changed state to up***Indica que la interfaz ha cambiado y su respectivo estado*

### Configuración de Protocolo de Enrutamiento RIP

El protocolo de enrutamiento RIP debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

8. Se ingresa al modo de configuración global

```
San_Antonio#
```

```
San_Antonio #configure terminal  
Entrar al modo de configuración global
```

9. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

```
San_Antonio (config) #router rip  
Protocolo a configurar
```

```
San_Antonio (config-router) #version 2  
Versión del protocolo
```

10. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es **OSPF** va con su respectiva willcard y el área)

```
San_Antonio (config-router) #network 192.168.13.40  
Red que aprende  
Es la dirección de red del segmento conectado al router
```

```
San_Antonio (config-router) #
```

### Guardar configuración

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

```
San_Antonio#copy running-config startup-config  
Guarda una copia de la configuración en la NVRAM
```

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

## 7.8.2.8.1 SHOW RUNNING ROUTER SAN\_ANTONIO

**Building configuration...****Current configuration:**

!

**Version 12.1**

Versión del IOS del router

**service timestamps debug uptime****service timestamps log uptime****no service password-encryption**

No se está utilizando la encriptación de passwords

!

**hostname San\_Antonio**

Nombre del Router

**enable password cisco**

La contraseña para ingresar al modo privilegiado es cisco

!

!

!

**ip subnet-zero**

Sirve para poder usar la dirección de red como IP

**spanning-tree vlan 1 priority**

!

**interface Serial0**

Tipo y número de la interfaz

**ip address 192.168.13.42 255.255.255.252**

Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default

**no ip directed-broadcast**

Significa que la interfaz no tiene una dirección IP directa de broadcast

!

**interface Serial1**

Tipo y número de la interfaz

**no ip address**

Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default

**no ip directed-broadcast**

Significa que la interfaz no tiene una dirección IP directa de broadcast

**shutdown**

!

**interface FastEthernet0/0**

Tipo y número de la interfaz

**no ip address****no ip directed-broadcast****shutdown**

!

**interface Bri0**

Tipo y número de la interfaz

**no ip address****no ip directed-broadcast****shutdown**

```

!
router rip
Protocolo configurado

Versión 2
Version del protocolo configurado, el 1 significa un identificador de protocolo

network 192.168.13.0
Segmento aprendido RIP
!
ip classless
!
!
!
line con 0
Consola del router
  password cisco
Password asignado al usuario normal
  login
Esta línea es para que aparezca la petición de clave
line aux 0
Consola auxiliar
  password cisco
Password asignado al usuario normal
  login
Esta línea es para que aparezca la petición de clave
line vty 0 4
Consola del router
  password cisco
Password asignado al usuario privilegiado
  login
Esta línea es para que aparezca la petición de clave y para poder realizar telnet
!
end

```



Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**). Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

**Tabla. 7.8** Descripción de las líneas del show running mediante iconos

7.8.2.8.2 **SHOW IP ROUTE ROUTER SAN\_ANTONIO**

San\_Antonio#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
U - per-user static route

**Gateway of last resort is not set**

**192.168.13.0/30 is subnetted, 1 subnets**

**C 192.168.13.40 is directly connected, Serial0**

Segmento de red conectado directamente al router - Interfaz  
conectada

Al ser C va conectada directamente

**192.168.13.8 [120/1] vía 192.168.13.38, 00:09:17, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz  
saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:17 es el tiempo que se tardó en conectarse

**R 192.168.13.4 [120/1] vía 192.168.13.38, 00:08:41, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz  
saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:08:41 es el tiempo que se tardó en conectarse

**R 192.168.13.20 [120/2] vía 192.168.13.38, 00:03:27, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz  
saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:03:27 es el tiempo que se tardó en conectarse

**R 192.168.13.24 [120/2] vía 192.168.13.38, 00:01:33, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz  
saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:01:33 es el tiempo que se tardó en conectarse

**R 192.168.13.28 [120/2] vía 192.168.13.38, 00:08:33, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:08:33 es el tiempo que se tardó en conectarse

**R 192.168.13.32 [120/2] vía 192.168.13.38, 00:09:14, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:14 es el tiempo que se tardó en conectarse



### Importante

Explicación del comando show ip route :

**C 192.168.13.40 is directly connected, Serial0**

- C : Segmento de red ,conectado directamente al router.
- 192.168.13.40 : Dirección de Red- Máscara
- Serial0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**R 192.168.13.28 [120/2] vía 192.168.13.38, 00:08:33, Serial0**

- R : Protocolo RIP
- 192.168.13.28 : Dirección de Red
- 120 : distancia administrativa por default en RIP.
- 2 : Número de saltos que realiza RIP.
- 192.168.13.38 : Interfaz a la que llega
- 00:06:14 : Tiempo que se tardó en conectarse.
- Serial 0/2 : Interfaz saliente

### 7.8.2.9 ROUTER AMBATO

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

#### Acceso al modo de Configuración principal

1. Una vez conectado al hyperterminal presiona la tecla ENTER para entrar a la configuración del router

```
Press Enter to Start  
Presionar enter para empezar
```

2. Se ingresa el comando **enable** para acceder de modo usuario al modo privilegiado del router.

```
Router>  
Router>enable  
Ingresa al modo privilegiado
```

3. Digitar el comando **configure terminal** para acceder a la configuración global.

```
Router#configure terminal  
Entra al modo de configuración global
```

#### Configuración de los nombres de los Routers

4. Se le asignará el respectivo nombre en el modo de configuración global.

```
Router (config) #hostname Ambato  
Nombre asignado al router  
Ambato (config) #
```

#### Creación de Contraseñas

5. Deberá configurar las respectivas contraseñas tanto a nivel de usuario normal como privilegiado para darle un mayor nivel de seguridad al router.

```
Ambato (config) #line console 0  
Consola a la que se le asignara la contraseña  
Ambato (config-line) #password cisco  
Contraseña establecida  
Ambato (config-line) #login  
Se usa para que solicite contraseña al ingresar  
Ambato (config-line) #exit  
Sale de la configuración de la consola  
Ambato (config) #  
Ambato (config) #line vty 0 4  
Ingresa a configurar la Terminal Virtual  
Ambato (config-line) #password cisco  
Contraseña establecida
```

**Ambato (config-line) #login***Se usa para que se pueda establecer telnet a la interfaz***Ambato (config-line) #exit***Sale de la configuración de la consola***Ambato (config) #****Ambato (config) #line aux 0***Ingresa a configurar el puerto auxiliar***Ambato (config-line) #password cisco***Contraseña establecida***Ambato (config-line) #login***Se usa para que se pueda establecer telnet a la interfaz***Ambato (config-line) #exit***Sale de la configuración de la consola***Ambato (config) #****Ambato (config-line) #enable password cisco***Agrega una contraseña para ingresar al router***Ambato (config-line) #enable secret cisco***Agrega una contraseña encriptada para ingresar al router*

### Configuración de las Interfaces

6. En este momento se procede a ingresar a las interfaces para asignarles las direcciones respectivas establecidas en el gráfico WAN anteriormente expuesto.

**Ambato (config) #interface serial 0/1***Interfaz y tipo que va a ser configurada***Ambato (config-if) #ip address 192.168.13.41 255.255.255.252***Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial*

7. Se le asignara su respectivo clock rate debido a que esta interfaz es un DCE (data communication equipment)

**Ambato (config-if) #clock rate 64000***El clock rate lo que permite es la sincronización de datos con los demás routers es 64000 para obtener una mayor velocidad.*

8. Proceda a levantar la interfaz con el siguiente comando.

**Ambato (config-if) #no shut***Levanta la interfaz configurada***%LINK-3-UPDOWN: Interface Serial0/1, changed state to up***Indica que la interfaz ha cambiado y su respectivo estado***Ambato (config-if) #**

9. Ingrese a la siguiente interfaz y proceda a realizar lo siguiente

```
Ambato (config) #interface serial 0/2
Interfaz y tipo que va a ser configurada
```

```
Ambato (config-if) #ip address 192.168.13.14 255.255.255.252
```

Dirección asignada, en este caso la máscara es 252 debido a que es una interfaz serial



#### Importante

En este router se obvia el **clock rate** debido a que esta interfaz es un DTE (data terminal equipment).

10. Proceda a levantar la interfaz con el siguiente comando.

```
Ambato (config-if) #no shut
Levanta la interfaz configurada
```

```
%LINK-3-UPDOWN: Interface Serial0/2, changed state to up
Indica que la interfaz ha cambiado y su respectivo estado
```

### Configuración de Protocolo de Enrutamiento RIP

El protocolo de enrutamiento RIP debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red.

11. Se ingresa al modo de configuración global

```
Ambato#
Ambato#configure terminal
Entrar al modo de configuración global
```

12. Se ingresa al protocolo que se quiere configurar (OSPF, RIP)

```
Ambato (config) #router rip
Protocolo a configurar
Ambato (config-router) #version 2
Versión del protocolo
```

13. Se establece el segmento de red que se requiere para que este router aprenda (dirección de red del segmento conectado si es **OSPF** va con su respectiva willcard y el área)

```
Ambato (config-router) #network 192.168.13.16
DIRECCIÓN DE RED
Ambato (config-router) #network 192.168.13.40
Ambato (config-router) #network 192.168.13.12
Ambato (config-router) #network 192.168.12.0
Ambato (config-router) #network 192.168.12.8
```

```
Ambato (config-router) #network 192.168.12.16
Ambato (config-router) #network 192.168.12.24
Ambato (config-router) #network 192.168.12.32
Red que aprende
Es la dirección de red del segmento conectado al router

Ambato (config-router) #
```

## Configuración de Listas de Acceso



### Importante

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list : comando
- 1-99 ,1300-1 999 : # acl estandar
- permit/deny : permitir o denegar una red especifica
- source : ( direccion de red – willcard)
- any : cualquier host o red

*Bloquear toda la subred 192.168.12.16/24, excepto los servidores 192.168.12.0/28*

```
Ambato #configure Terminal
```

*Ingresa al modo de configuración global*

```
Ambato (config) #access-list 1 permit 192.168.12.0 0.0.0.3
```

*Asigna permiso a una subred específica*

```
Ambato (config) #access-list 1 deny 192.168.12.16 0.0.0.255
```

*Niega el acceso a la red a las demás ip´s*

```
Ambato (config) #access-list 1 permit any
```

*Luego poner una línea implícita para esta acl*

```
Ambato (config) #exit
```

*Sale del modo de configuración global*

*Luego levantar la acl estándar en la interfaz correspondiente.*

```
Ambato #configure terminal
```

*Ingresa al modo de configuración global*

```
Ambato (config) #interface fastethernet 0/0
```

*Ingresa a la interfaz que quiere asignar la acl*

```
Ambato (config) #ip access-group 1 in
```

*Levanta la acl de manera entrante*

**ACL extendida****Importante**

La sintaxis de las Listas de Control de acceso es la siguiente:

- access-list : comando
- 100-199, 2000-2699 : # acl extendida
- permit/deny : permitir o denegar una red específica
- source : ( dirección de red – wildcard)
- any : cualquier host o red

**Ambato #configure terminal**

*Ingresa al modo de configuración global*

**Ambato (config) #access-list 101 permit 192.168.12.32 0.0.0.7 192.168.12.0 0.0.0.3**

*Asigna permiso específico*

**Ambato (config) #access-list 101 deny 192.168.12.64 0.0.0.7 192.168.12.0 0.0.0.3**

*Niega el acceso a la red a las demás ip's*

**Ambato (config) #access-list 101 permit any any**

*Luego poner una línea implícita para esta acl*

**Ambato (config) #exit**

*Sale del modo de configuración global*

*Luego levantar la acl extendida en la interfaz correspondiente.*

**Ambato #configure terminal**

*Ingresa al modo de configuración global*

**Ambato (config) #interface fastethernet 0/0**

*Ingresa a la interfaz que quiere asignar la acl*

**Ambato (config) #ip access-group 101 in**

*Levanta la acl de manera entrante*

*Permitir trafico (ICMP) desde una subred hacia el servidor*

**Ambato #configure terminal**

*Ingresa al modo de configuración global*

**Ambato (config) #access-list 102 permit icmp 192.168.12.32 0.0.0.7 192.168.12.0 0.0.0.3**

*Asigna permiso específico*

**Ambato (config) #access-list 102 deny any any**

*Se coloca una línea implícita*

## Guardar configuración

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

```
Ambato #copy running-config startup-config  
Guarda una copia de la configuración en la NVRAM
```

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **statup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config)**.

## 7.8.2.9.1 SHOW RUNNING ROUTER AMBATO

**Building configuration...****Current configuration:**

!

**Version 12.1***Versión del IOS del router***service timestamps debug uptime****service timestamps log uptime****no service password-encryption***No se está utilizando la encriptación de passwords*

!

**Hostname Ambato***Nombre del Router***enable password cisco***La contraseña para ingresar al modo privilegiado es cisco*

!

**ip subnet-zero***Sirve para poder usar la dirección de red como IP***spanning-tree vlan 1 priority**

!

**interface Serial0/0***Tipo y número de la interfaz***ip address 192.168.13.17 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast**

!

**interface Serial0/1***Tipo y número de la interfaz***ip address 192.168.13.41 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast****clock rate 64000***Indica la velocidad del puerto en bits por segundo, lo encuentra en el DCE*

!

**interface Serial0/2***Tipo y número de la interfaz***ip address 192.168.13.14 255.255.255.252***Dirección IP – Máscara, la máscara para interfaces seriales es 252 por default***no ip directed-broadcast**

!

**interface Serial0/3***Tipo y número de la interfaz***no ip address***no ip directed-broadcast*

!

**interface FastEthernet1/0***Tipo y número de la interfaz***no ip address**

```
no ip directed-broadcast
shutdown
!
interface FastEthernet1/0.10
Tipo y número de la interfaz
Encapsulation dotq 10
Encapsulamiento asociado a la vlan 10
ip address 192.168.12.1 255.255.255.248
no ip directed-broadcast
!
!
interface FastEthernet1/0.20
Tipo y número de la interfaz
Encapsulation dotq 20
Encapsulamiento asociado a la vlan 20
ip address 192.168.12.9 255.255.255.248
no ip directed-broadcast
!
!
interface FastEthernet1/0.30
Tipo y número de la interfaz
Encapsulation dotq 30
Encapsulamiento asociado a la vlan 30
ip address 192.168.12.17 255.255.255.248
no ip directed-broadcast
!
interface FastEthernet1/0.40
Tipo y número de la interfaz
Encapsulation dotq 40
Encapsulamiento asociado a la vlan 40
ip address 192.168.12.25 255.255.255.248
no ip directed-broadcast
!
interface FastEthernet1/0.50
Tipo y número de la interfaz
Encapsulation dotq 50
Encapsulamiento asociado a la vlan 50
ip address 192.168.12.33 255.255.255.248
no ip directed-broadcast
!

interface Bri1/0
no ip address
no ip directed-broadcast
shutdown
!
router rip
Protocolo configurado
```

**Versión 2**

Version del protocolo configurado, el 1 significa un identificador de protocolo

**network 192.168.13.0**

**network 192.168.12.0**

Segmento aprendido RIP

!

!

**ip classless**

!

!

**line con 0**

Consola del router

**password cisco**

Password asignado al usuario normal

**login**

Esta línea es para que aparezca la petición de clave

**line aux 0**

Consola auxiliar

**password cisco**

Password asignado al usuario normal

**login**

Esta línea es para que aparezca la petición de clave

**line vty 0 4**

Consola del router

**password cisco**

Password asignado al usuario privilegiado

**login**

Esta línea es para que aparezca la petición de clave y para poder realizar telnet

!

**End**



Si aparecen estas líneas significa que la interfaz no tiene IP asignada y no está levantada (**DOWN**).  
Donde **no ip address** significa que no tiene IP asignada y **shutdown** que no ha sido levantada.

**Tabla. 7.9**

Descripción de las líneas del `show running` mediante iconos

## 7.8.2.9.2 SHOW IP ROUTE ROUTER AMBATO

Ambato#

Ambato#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
 U - per-user static route

**Gateway of last resort is not set**

**192.168.13.0/30 is subnetted, 2 subnets**

**C 192.168.13.16 is directly connected, Serial0/0**

**C 192.168.13.40 is directly connected, Serial0/1**

Segmento de red conectado directamente al router - Interfaz conectada  
 Al ser C va conectada directamente

**192.168.13.8 [120/1] vía 192.168.13.38, 00:09:17, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:17 es el tiempo que se tardó en conectarse

**R 192.168.13.4 [120/1] vía 192.168.13.38, 00:08:41, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:08:41 es el tiempo que se tardó en conectarse

**R 192.168.13.20 [120/2] vía 192.168.13.38, 00:03:27, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:03:27 es el tiempo que se tardó en conectarse

**R 192.168.13.24 [120/2] vía 192.168.13.38, 00:01:33, Serial0**

Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:01:33 es el tiempo que se tardó en conectarse

**R 192.168.13.28 [120/2] vía 192.168.13.38, 00:08:33, Serial0**  
 Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:08:33 es el tiempo que se tardó en conectarse

**R 192.168.13.32 [120/2] vía 192.168.13.38, 00:09:14, Serial0**  
 Protocolo – dirección de red conectada – interfaz a la que llega – interfaz saliente

Al ser R el protocolo es Rip

El 120 es la distancia administrativa por default en RIP

El 1 es el número de saltos que realiza RIP

El 00:09:14 es el tiempo que se tardó en conectarse



### Importante

Explicación del comando show ip route :

**C 192.168.13.16 is directly connected, Serial0/0**  
 ➤ C : Segmento de red ,conectado directamente al router.  
 ➤ 192.168.13.16 : Dirección de Red- Máscara  
 ➤ Serial0/0 : Serial conectada directamente.

Redes aprendidas por medio de protocolo:

**R 192.168.13.28 [120/2] vía 192.168.13.38, 00:08:33, Serial0**  
 ➤ R : Protocolo RIP  
 ➤ 192.168.13.28 : Dirección de Red  
 ➤ 120 : distancia administrativa por default en RIP.  
 ➤ 2 : Número de saltos que realiza RIP.  
 ➤ 192.168.13.38 : Interfaz a la que llega  
 ➤ 00:06:14 : Tiempo que se tardó en conectarse.  
 Serial 0/2 : Interfaz saliente

## 7.9 INTRODUCCIÓN A LOS SWITCHES

Un switch es un dispositivo de red de Capa 2 que actúa como punto de concentración para la conexión de estaciones de trabajo, servidores, routers, hubs y otros switches.

Los switches son puentes multipuerto. Los switches pertenecen a la tecnología estándar actual de las LAN Ethernet que utilizan una topología en estrella. Un switch ofrece varios circuitos virtuales punto a punto dedicados entre los dispositivos de red conectados, de manera que es poco probable que se produzcan colisiones.

Los switches son computadoras dedicadas y especializadas que contienen una unidad de procesamiento central (CPU), memoria de acceso aleatorio (RAM), y un sistema operativo. Los switches generalmente poseen varios puertos a los cuales los hosts se pueden conectar así como puertos especializados para fines de administración. Los switches se pueden administrar y la configuración se puede visualizar y cambiar mediante el puerto de consola.

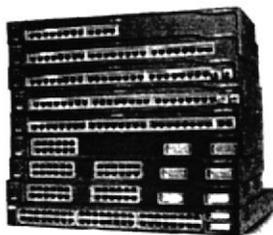


Figura 7.55. Switches de la serie Cisco Catalyst 2900.

### 7.9.1 INDICADORES LED DEL SWITCH

El panel frontal de un switch tiene varias luces que ayudan a controlar la actividad y desempeño del sistema. Esas luces se llaman diodos emisores de luz (LED). En esta página se analizan los LED que se encuentran en la parte frontal de un switch:

- LED del sistema
- LED de suministro remoto de energía (RPS)
- LED de modo de puerto
- LED de estado de puerto

El LED del sistema analiza si el sistema está recibiendo energía y está funcionando correctamente.

El LED RPS indica si se está utilizando o no el suministro de energía remota.

Los LED de modo indican el estado del botón Mode (Modo). Los modos se utilizan para determinar de qué manera se interpretan los LED de estado de puerto. Para seleccionar o cambiar el modo de puerto, presione el botón Mode (Modo) reiteradas veces hasta que los LED de modo indiquen el modo deseado.

## 7.9.2 CONECTÁNDOSE AL SWITCH

### 7.9.2.1. EL CONECTOR DB 9 DEL PC

El DB9 se conecta directamente a la PC y el cable ROLLOVER va desde el DB9 hasta el puerto de consola del Switch.



Figura 7.56. Cable UTP Rollover y conector DB9

En los PCs hay conectores DB9 macho, de 9 pines, por el que se conectan los dispositivos al puerto serie. Los conectores hembra que se enchufan tienen una colocación de pines diferente, de manera que se conectan el pin 1 del macho con el pin 1 del hembra, el pin 2 con el 2, etc.

Para poder configurar o verificar el estado de un switch, conecte una computadora al switch para establecer una sesión de comunicación. Utilice un cable transpuesto (rollover) para conectar el puerto de consola de la parte trasera del switch a un puerto **COM** en la parte trasera de la computadora.

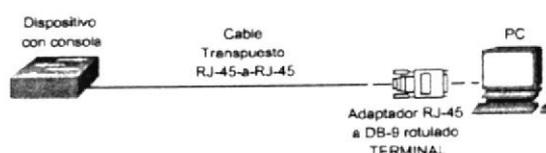


Figura 7.57. Conexión de un switch a el PC

Una vez que el switch ha arrancado y completado la POST, aparecen indicadores de diálogo de configuración del sistema. El switch se puede configurar manualmente con o sin ayuda del diálogo de configuración del sistema. El diálogo de configuración del sistema del switch es mucho más simple que el de los routers.

## 7.9.3 CONFIGURACIÓN DE SWITCHES

Proceda ahora con la configuración de los switches.

### 7.9.3.1 MODOS DE INTERFAZ DE USUARIO

El modo por defecto es el modo EXEC usuario. El modo EXEC usuario se reconoce por su indicador, que termina en un carácter de "mayor que" (>). Los comandos disponibles en el modo EXEC usuario se limitan a los que cambian las configuraciones del terminal, realizan pruebas básicas y muestran información del sistema.

Comandos **show** que están disponibles en el modo EXEC usuario:

- Show versión
- Show flash
- Show mac-address-table
- Show controllers
- Show ethernet-controllers
- Show running-config
- Show post
- Show vlan
- Show interfaces

### **Show versión**

Proporciona información sobre la versión del software y hardware. Se usa para ver exactamente cuáles son módulos y el software en uso.

### **Show flash**

Muestra información acerca del sistema de archivos flash.

### **Show mac-address-table**

Muestra el contenido de la tabla de envío MAC.

### **Show controllers, ethernet-controllers**

Proporciona información de tramas descartadas, tramas diferidas, errores de alineación, colisiones, etc.

### **Show running-config**

Muestra el archivo de configuración actual del switch.

### **Show post**

Indica si el switch pasó la prueba de autocomprobación de encendido (POST).

### **Show vlan**

Verifica la configuración de la VLAN.

### **Show interfaces**

Muestra el estado y la configuración de la interfaz.

### **Enable**

El comando enable nos permite cambiar el modo de usuario de normal a privilegiado (esto se lo puede ver reflejado en el cambio del Prompt en donde se vera el cambio del signo mayor > al signo #).

### **Configure Terminal**

El comando configure Terminal ingresa al modo de configuración global.

### **Copy running-config startup-config**

El comando copy running-config startup-config copia la configuración almacenada en la NVRAM a la RAM del router.

### **Line console 0:**

Comando para ingresar al modo de configuración del puerto consola.

### **Login:**

Habilita la posibilidad de logonearse introduciendo una password.

### **Password [xxxxxxxx]:**

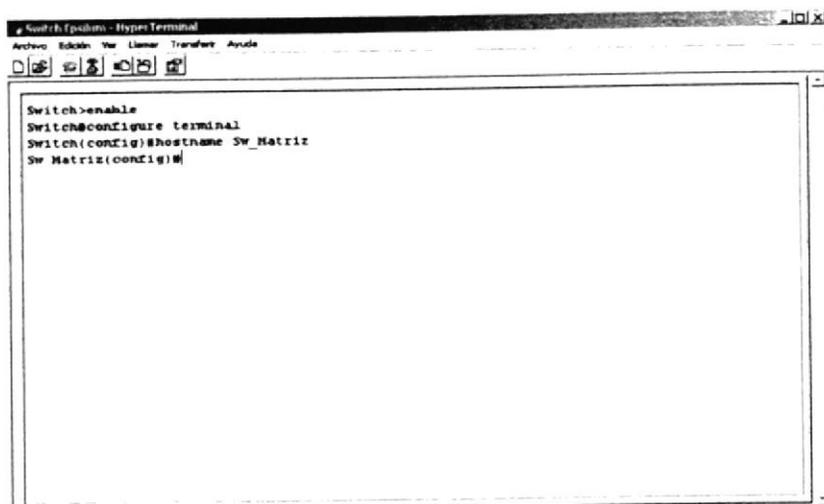
Configura la password de acceso.

**Line vty 0 15:**

Comando para ingresar al modo de configuración de las terminales virtuales (sesiones telnet).

**Show running-config:**

Muestra los parámetros de configuración activos.

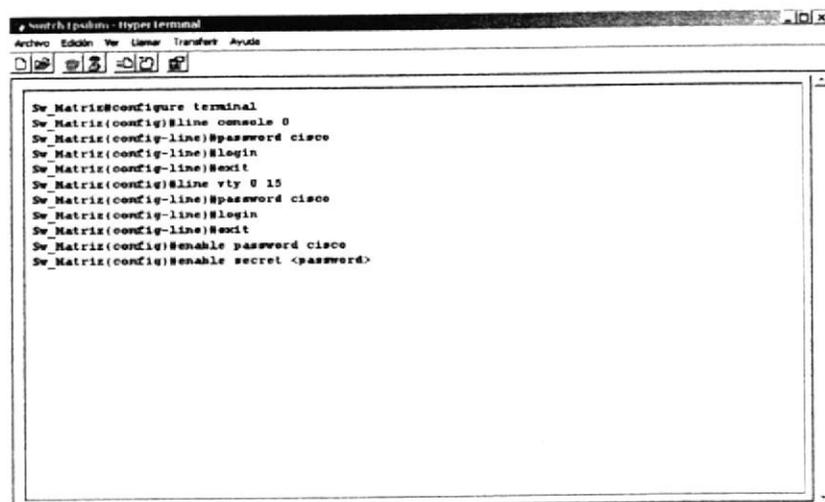


```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Sw_Matriz
Sw_Matriz(config)#
```

Figura 7.58. Modo de Usuario

### 7.9.3.2 ASIGNACIÓN DE CONTRASEÑAS

Con fines de seguridad y administración, se deben establecer contraseñas en las líneas de consola y vty. También se debe establecer una contraseña **enable** y una contraseña **enable secret**.



```
Sw_Matriz#configure terminal
Sw_Matriz(config)#line console 0
Sw_Matriz(config-line)#password cisco
Sw_Matriz(config-line)#login
Sw_Matriz(config-line)#exit
Sw_Matriz(config)#line vty 0 15
Sw_Matriz(config-line)#password cisco
Sw_Matriz(config-line)#login
Sw_Matriz(config-line)#exit
Sw_Matriz(config)#enable password cisco
Sw_Matriz(config)#enable secret <password>
```

Figura 7.59. Configuración de contraseñas

En ciertas ocasiones es posible que se produzca acceso físico al switch, pero no pueda accederse al modo EXEC usuario o privilegiado debido a que las contraseñas no se conocen o se han olvidado.



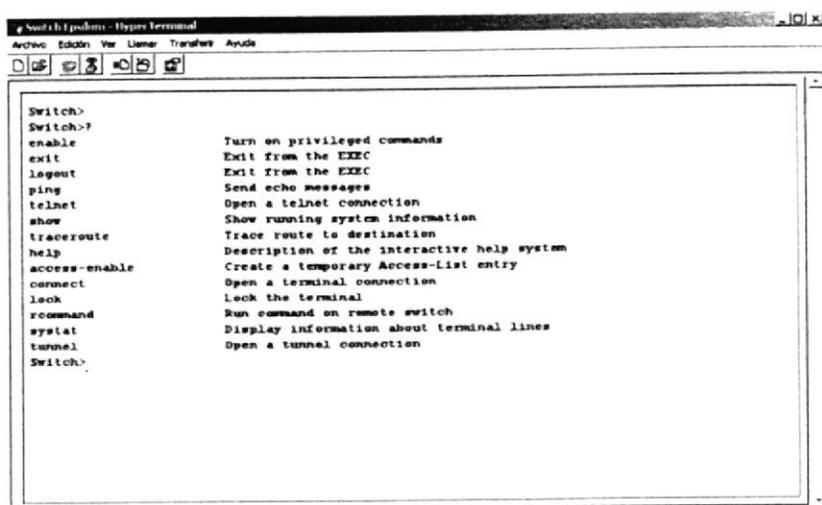
### 7.9.4 EXAMINANDO EL COMANDO HELP EN LA CLI DEL SWITCH

En esta página se explica de qué manera el comando `help` se utiliza en la CLI de los switches Cisco.

La CLI de los switches Cisco es muy similar a la CLI de los routers Cisco.

Introduzca un signo de interrogación (?) para emitir el comando `help`. Cuando se introduce este comando en el indicador del sistema, aparece una lista de comandos disponibles para el modo de comandos actual.

El comando `help` es muy flexible. Para obtener una lista de comandos que empiecen con una determinada secuencia de caracteres, introduzca estos caracteres seguidos inmediatamente por el signo de interrogación (?).



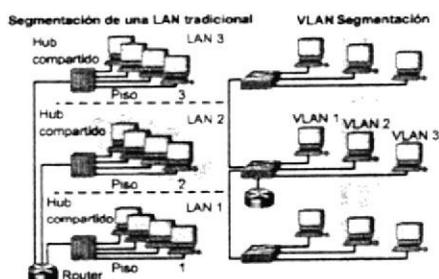
```

Switch>
Switch>?
enable          Turn on privileged commands
exit            Exit from the EXEC
logout         Exit from the EXEC
ping           Send echo messages
telnet         Open a telnet connection
show           Show running system information
traceroute     Trace route to destination
help           Description of the interactive help system
access-enable  Create a temporary Access-List entry
connect        Open a terminal connection
lock           Lock the terminal
rcommand       Run command on remote switch
sysstat        Display information about terminal lines
tunnel         Open a tunnel connection
Switch>
  
```

Figura 7.60. Comando Help

### 7.9.5 ASPECTOS BÁSICOS DE LAS VLAN

Una VLAN es una agrupación lógica de dispositivos o usuarios que se pueden agrupar por función, departamento o aplicación, sin importar su ubicación física.



Las VLAN permiten agrupar dispositivos, sin importar su ubicación física

Figura 7.61. Comparación de una LAN tradicional y una VLAN

Las VLAN se configuran en el switch a través del software. Debido a la cantidad de implementaciones de VLAN que compiten entre sí es posible que deba requerirse el uso de un software propietario por parte del fabricante del switch. La agrupación de puertos y usuarios en comunidades de interés, conocidos como organizaciones VLAN, puede obtenerse mediante el uso de un

solo switch o una conexión más potente entre los switches ya conectados dentro de la empresa.

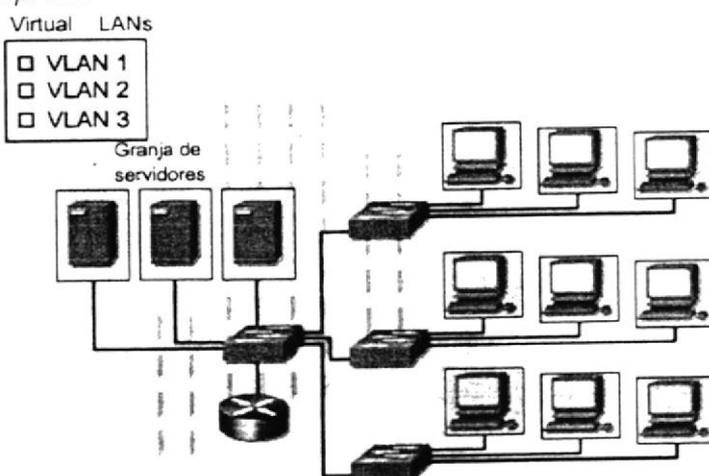


Figura 7.62. Administración de VLAN

Las VLAN ayudan a controlar el tamaño de los dominios de broadcast y a ubicar el tráfico. Las VLAN se asocian con redes individuales. Por lo tanto, los dispositivos de red en las distintas VLAN no se pueden comunicar directamente entre sí sin la intervención de un dispositivo de enrutamiento de Capa 3.

Cuando un nodo en una VLAN necesita comunicarse con un nodo de otra VLAN, se necesita un router para enrutar el tráfico entre las distintas VLAN. Sin este dispositivo de enrutamiento, el tráfico entre las VLAN no puede efectuarse.

### 7.9.6 VLAN POR DEFECTO

Para permitir que Telnet y otras aplicaciones TCP/IP puedan acceder al switch, se deberán establecer direcciones IP y un Gateway por defecto. Por defecto, la VLAN 1 es la VLAN de administración. En una red basada en switch, todos los dispositivos de red deberán estar en la VLAN de administración. Esto permite que una sola estación de trabajo de administración acceda, configure y administre todos los dispositivos de red.

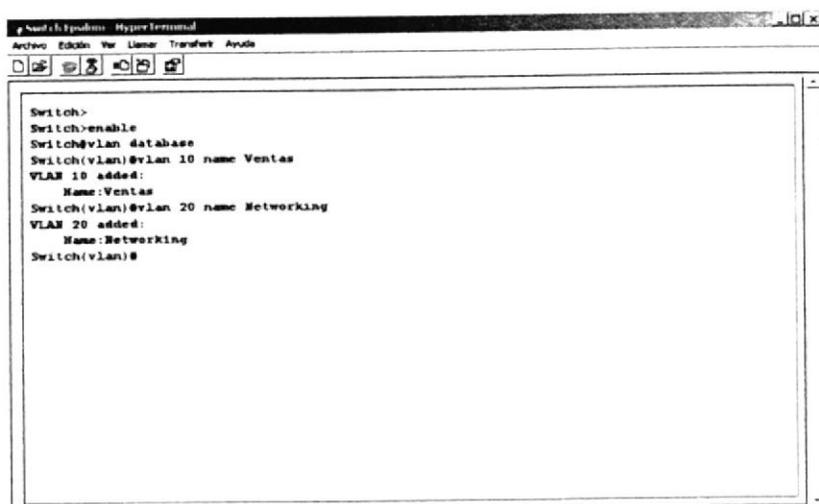
```
Switch>
Switch#enable
Switch#configure terminal
Switch(config)#interface VLAN1
Switch(config-if)#ip address 192.168.15.5 255.255.255.0
Switch(config-if)#ip default-gateway 192.168.15.1
```

Figura 7.63. Configuración de Vlan por defecto

### 7.9.7 CREACIÓN DE VLAN'S

Las VLAN se configuran en el switch a través del software.

- Ingrese al modo de configuración de vlan con el comando `vlan database`.
- Asigne un número y un nombre con el comando `vlan number name` nombre.



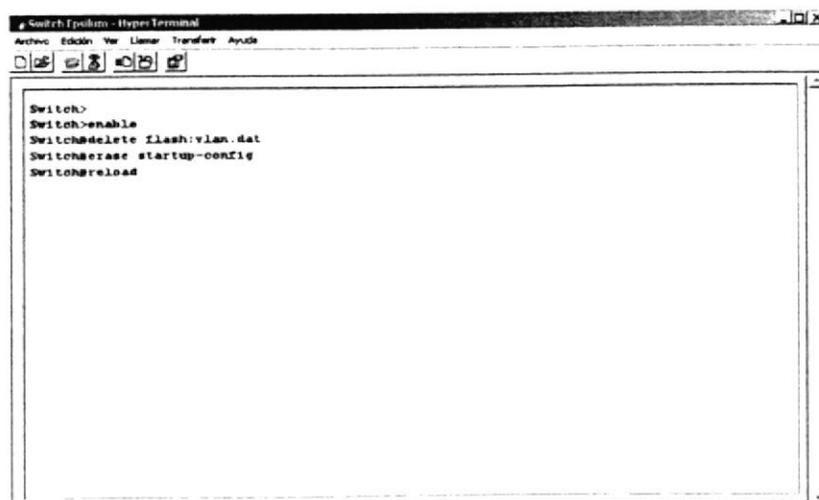
```
Switch>
Switch>enable
Switch>vlan database
Switch(vlan)#vlan 10 name Ventas
VLAN 10 added:
  Name:Ventas
Switch(vlan)#vlan 20 name Networking
VLAN 20 added:
  Name:Networking
Switch(vlan)#
```

Figura 7.64. Creación de las Vlan's

### 7.9.8 ELIMINANDO VLAN'S

Los siguientes pasos permitirán que una nueva configuración se sobrescriba completamente a la configuración actual:

- Para eliminar la información de VLAN actual, borre el archivo de la base de datos VLAN, denominados `vlan.dat`, del directorio flash.
- Borre el archivo de configuración de respaldo con el nombre `startup-config`.
- Reinicie el switch con el comando `reload`.



```
Switch>
Switch>enable
Switch>delete flash:vlan.dat
Switch>erase startup-config
Switch>reload
```

Figura 7.65. Borrado de las Vlan's

### 7.9.9 ASIGNACIÓN DE VLAN'S A LOS PUERTOS

```

Switch>
Switch>enable
Switch>configure terminal
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit

```

Figura 7.66. Asignación de vlan's a los puertos

### 7.9.10 ENRUTAMIENTO ENTRE VLAN

Cuando el host en un dominio de broadcast desea comunicarse con un host en otro dominio de broadcast, debe utilizarse un router.

El puerto 1 es un switch forma parte de la VLAN 1 y el puerto 2 forma parte de la VLAN 200.

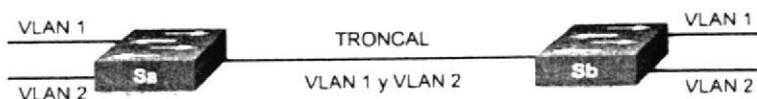


Figura 7.67. Enlace Troncal

Si todos los puertos de switch formaran parte de la VLAN 1, es posible que los hosts conectados a estos puertos puedan comunicarse entre sí. Sin embargo, en este caso, los puertos forman parte de distintas VLAN, la VLAN 1 y VLAN 200. Se debe utilizar un router si los hosts de las distintas VLAN necesitan comunicarse entre sí.

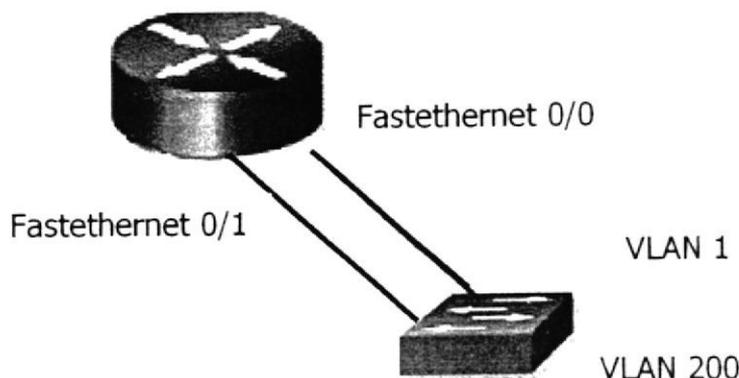


Figura 7.68. Enlace Switch - Router

Dado que los routers evitan la propagación de broadcast y utilizan algoritmos de envío más inteligentes que los switches, los puertos ofrecen un uso más eficiente del ancho de banda. Esto da como resultado simultáneamente una selección de ruta flexible y óptima.

Si una VLAN abarca varios dispositivos, se utiliza un enlace troncal para interconectar los dispositivos. El enlace troncal transporta el tráfico para varias VLAN.

Recuerde que cuando un host en una VLAN desea comunicarse con un host de otra VLAN, se debe utilizar un router.

### 7.9.11 INTERFACES FÍSICAS Y LÓGICAS

En una situación tradicional, una red con cuatro VLAN requeriría cuatro conexiones físicas entre el switch y el router externo.

A medida que las tecnologías como por ejemplo el Enlace inter-switch (ISL) se vuelven más comunes, los diseñadores de red empiezan a utilizar enlaces troncales para conectar los routers a los switches. A pesar de que se puede utilizar cualquier tecnología de enlace troncal como por ejemplo ISL, 802.1Q, 802.10 o la emulación LAN (LANE), los enfoques basados en Ethernet como por ejemplo ISL y 802.1Q son más comunes.

A medida que aumenta la cantidad de VLAN en una red, el enfoque físico de tener una interfaz de router por VLAN se vuelve rápidamente no escalable. Las redes con muchas VLAN deben utilizar el enlace troncal de VLAN para asignar varias VLAN a una interfaz de router única.

El router puede admitir varias interfaces lógicas en enlaces físicos individuales. Por ejemplo, la interfaz de FastEthernet 0/0 puede admitir tres interfaces virtuales numeradas como FastEthernet 0/0.1, 0/0.2 y 0/0.3.

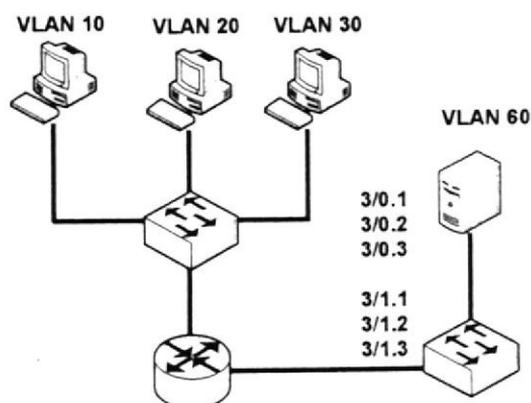


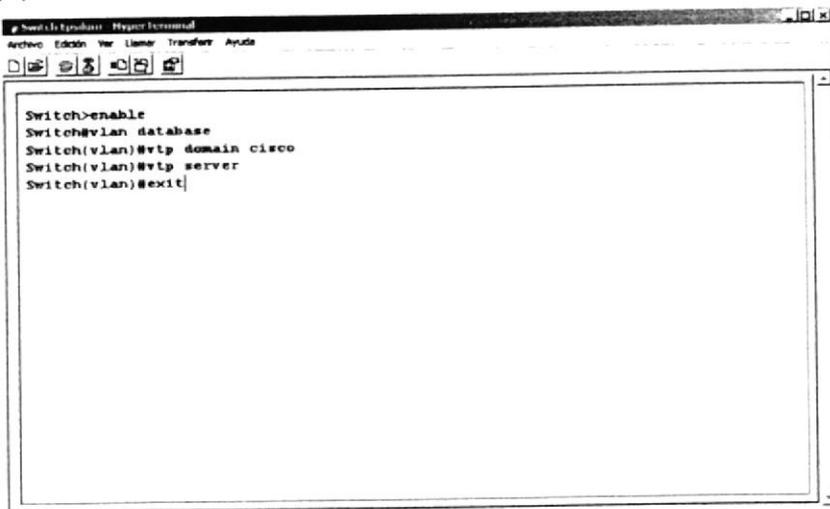
Figura 7.69. Interfaces físicas y lógicas

La ventaja principal del uso del enlace troncal es una reducción en la cantidad de puertos de router y switch que se utiliza. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de router conectado a un enlace troncal puede ampliarse hasta un número mucho más alto de VLAN que el diseño de "un enlace por VLAN".

### 7.9.12 ASIGNAR SWITCH DE TIPO SERVER

El rol de VTP es mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común. VTP es un protocolo de mensajería que usa tramas de enlace troncal de Capa 2 para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio. VTP también admite cambios centralizados que se comunican a todos los demás switches de la red.

Para determinar un switch de tipo Server deberá estar en el MODO PRIVILEGIADO EXEC e ingresar al modo de configuración de vlans con el comando "**vlan database**" una vez adentro digitar la línea de comando **vtp <Server o cliente>** después digitar el comando **vtp domain <nombre del dominio>** y por último salir de la configuración con el comando **exit**.



```

Switch>enable
Switch#vlan database
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp server
Switch(vlan)#exit
  
```

Figura 7.70. Asignar switch de tipo server

### 7.9.13 ENRUTAMIENTO ENTRE DISTINTAS VLAN

Para que el enrutamiento entre VLAN funcione correctamente, todos los routers y switches involucrados deben admitir el mismo encapsulamiento.

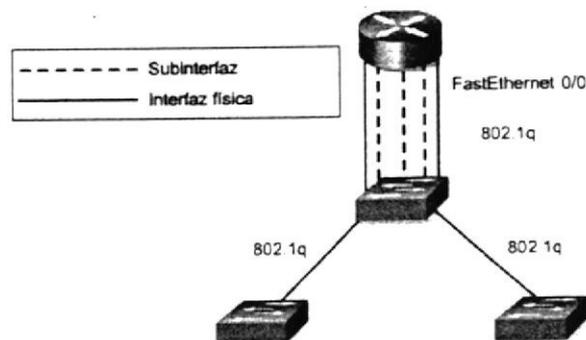


Figura 7.71. Enrutamiento entre distintas vlan's

En un router, una interfaz se puede dividir lógicamente en varias subinterfaces virtuales. Las subinterfaces ofrecen una solución flexible para el enrutamiento de varias corrientes de datos a través de una interfaz física única.

Para definir las subinterfaces en una interfaz física, realice las siguientes tareas:

- Identifique la interfaz.
- Defina el encapsulamiento de la VLAN.
- Asigne una dirección IP a la interfaz.

Para identificar la interfaz utilice el comando **interface** en el modo de configuración global.

**Router (config) #interface fastethernet port-number. subinterface-number**

**Port-number** identifica la interfaz física y **subinterface-number** identifica la interfaz virtual (vlan).

El router debe poder comunicarse con el switch utilizando un protocolo de enlace troncal estandarizado. Esto significa que ambos dispositivos conectados entre sí deben comprenderse. Para definir el encapsulamiento de la VLAN, introduzca el comando **encapsulation** en el modo de configuración de interfaz.

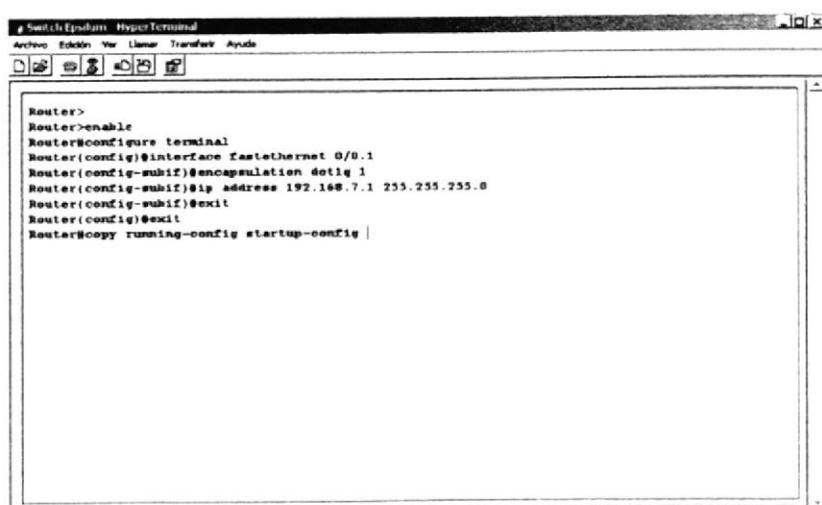
**Router (config-if) #encapsulation dot1q vlan-number**

**Vlan-number** identifica la VLAN para la cual la subinterfaz transportará el tráfico. Se agrega un ID de VLAN a la trama sólo cuando la trama está destinada a una red no local. Cada paquete de VLAN transporta el ID de VLAN dentro del encabezado del paquete.

Para asignar una dirección IP a la interfaz, introduzca el siguiente comando en el modo de configuración de interfaz.

**Router (config-if) #ip address ip-address subnet-mask**

**IP-address y subnet-mask** son las direcciones y la máscara de red de 32 bits de la interfaz específica.



```
Router>
Router>enable
Router#configure terminal
Router(config)#interface fastethernet 0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 192.168.7.1 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
Router#copy running-config startup-config |
```

Figura 7.72. Configuración de enrutamiento entre distintas vlan's

## 7.10 PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE SWITCH (EPSILUM)

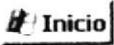
Ahora pasará a configurar paso a paso los diferentes Switch de la red EPSILUM.

### 7.10.1 CONEXIÓN DE UNA TERMINAL CON LA CONSOLA DEL SWITCH

Antes de empezar, tendrá que tener claro que la conexión se realizará a través de la Aplicación HyperTerminal de Windows.

**HyperTerminal** es un programa que se puede utilizar para conectar con otros equipos, sitios Telnet, sistemas de boletines electrónicos (BBS, Bulletin Board Systems), servicios en línea y equipos host, mediante un módem, un cable de módem nulo o una conexión (WinSock) TCP/IP.

A continuación los pasos a seguir para la configuración:

1. Con un cable transpuesto **RJ-45 a RH-45** y un adaptador **RJ-45 a DB-9** o **RJ-45 a DB-25** se conecta de una Terminal (PC – Personal Computer) al puerto de consola del Router.
2. Abrir la aplicación HyperTerminal:
  - a. En la barra de tareas de Windows seleccionará con el Mouse la opción .

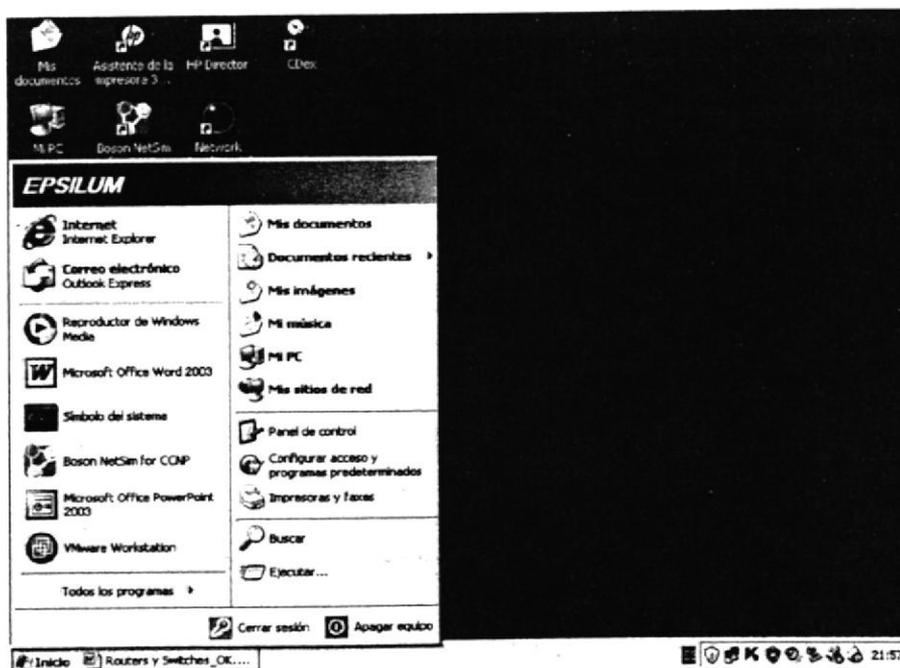


Figura 7.73. Escritorio de Windows accediendo al botón inicio

- b. Se abrirá un menú donde seleccionará la opción **Todos los programas**.

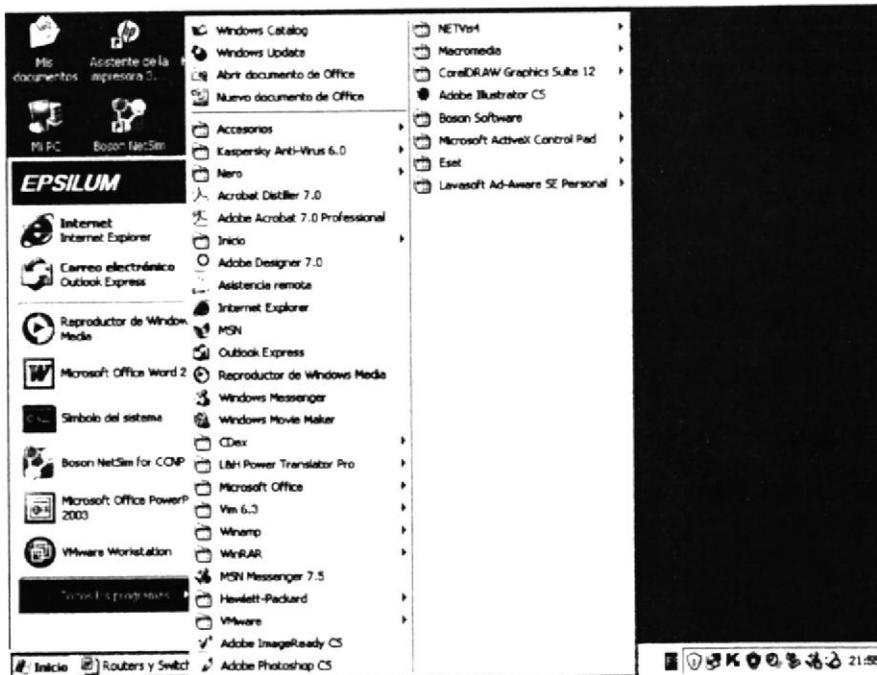


Figura 7.74. Escritorio de Windows opción todos los programas

- c. Seguidamente se desplegará un submenú donde seleccionará la opción **Accesorios**.

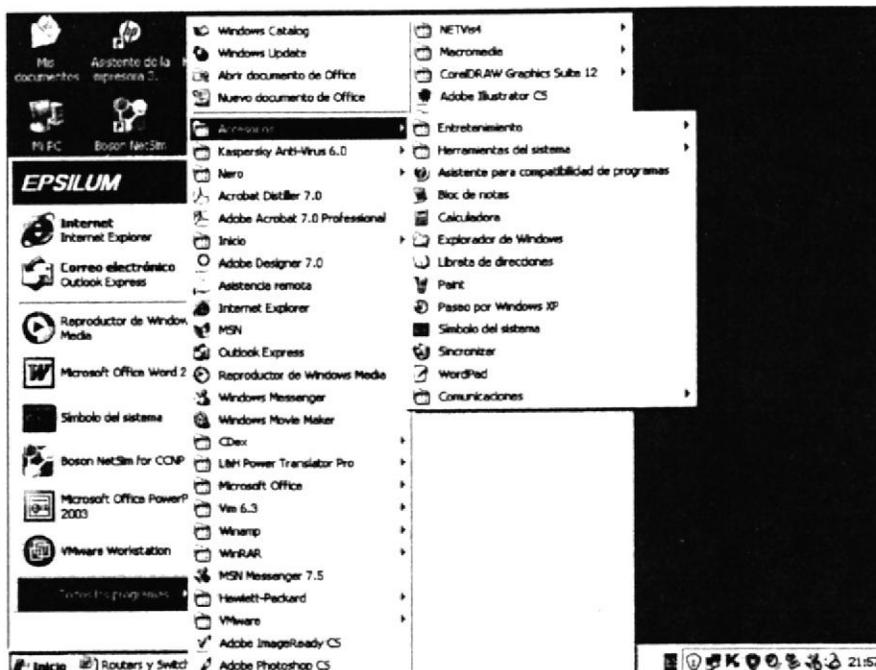


Figura 7.75. Escritorio de Windows opción accesorios

- d. Dentro de este submenú se encontrará la opción **Comunicaciones** la cual deberá ser seleccionada.

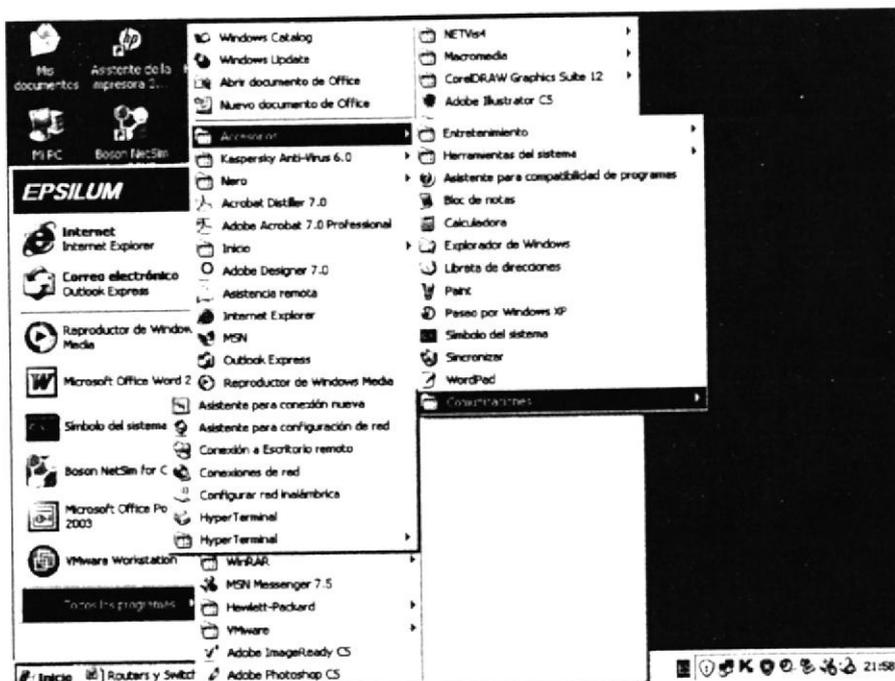


Figura 7.76. Escritorio de Windows opción comunicaciones

- e. Aquí encontrará un acceso directo llamado **HyperTerminal**, al cual le dará clic.

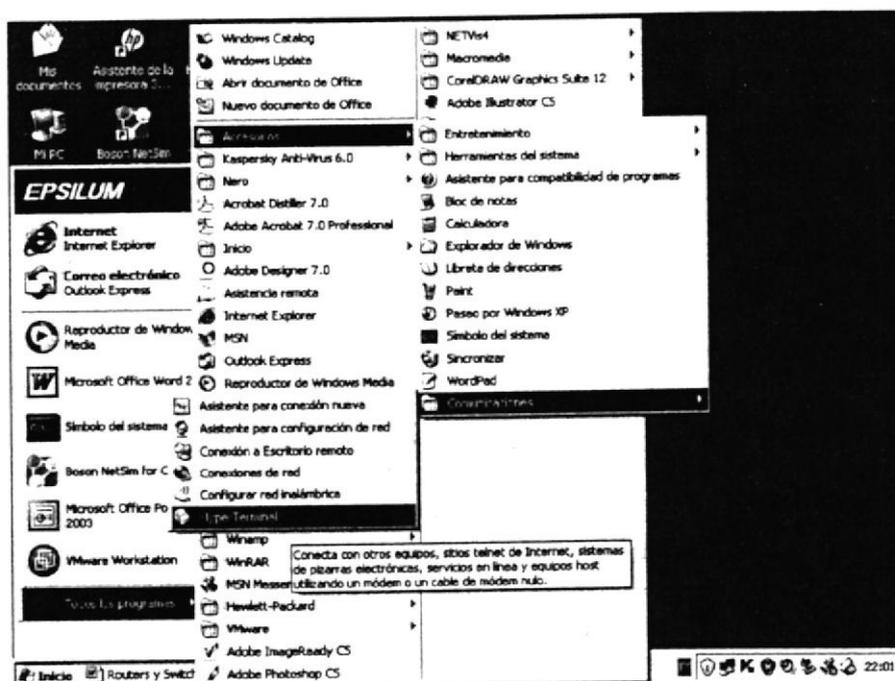


Figura 7.77. Escritorio de Windows icono Hyperterminal

3. Una vez que de clic en la opción de **Hyperterminal**, si es la primera vez que accede a esta aplicación, aparecerá una ventana de Advertencia, donde se recomienda establecer la Aplicación HyperTerminal como programa predeterminado de Telnet.

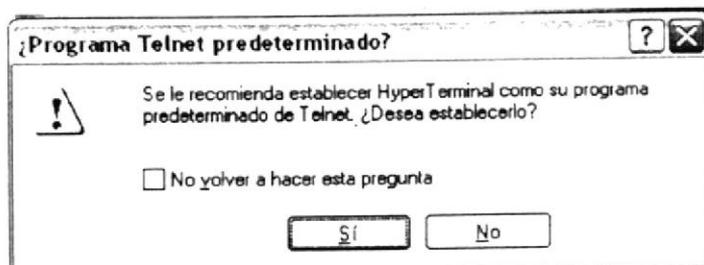


Figura 7.78. Pantalla de recomendación de programa predeterminado para Telnet

- a. La primera opción que nos da es si desea volver a ver esta pregunta la próxima vez que acceda a la HyperTerminal. Esta opción no afectará en lo más mínimo a la conexión.
  - b. Ahora presentan dos opciones de respuesta referente a la recomendación que nos hace Windows, si acepta "Sí" automáticamente aparecerá una ventana, la cual solicita cierta información para una conexión mediante MODEM; pero como este no es el caso simplemente "cancela", y automáticamente aparecerá la ventana de "Descripción de conexión" de la HyperTerminal.
  - c. Si en caso de que la ventana que Windows recomienda establecer a la aplicación HyperTerminal como predeterminada para Telnet, se la cancela, automáticamente aparecerá la ventana de "Descripción de la conexión" de la HyperTerminal.
4. En la ventana de "Descripción de la conexión" de la HyperTerminal pedirá un nombre y un icono para la conexión.
- a. El Nombre puede ser cualquiera, en este caso se llamara Router Epsilon.
  - b. Cada icono es un tipo de conexión diferente, para este caso se utilizara el primero, el que viene marcado por default.

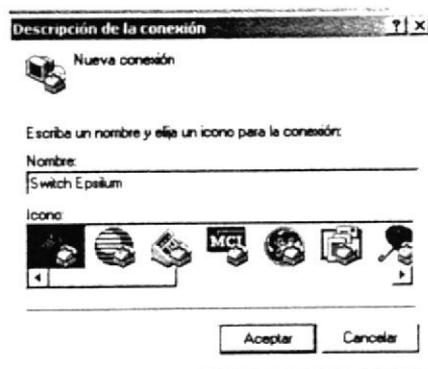


Figura 7.79. Ventana descripción de la conexión del Hyperterminal

5. En la siguiente pantalla se pedirá ingresar algunos detalles de conexión como País o región, Código de área, Número de teléfono y Conectar usando. Las tres primeras no son obligatorias son opcionales mientras que la ultima opción deberá escoger el puerto del computador al cual se va a conectar el router en este caso va a ser el puerto COM 1 y da clic en el botón Aceptar.

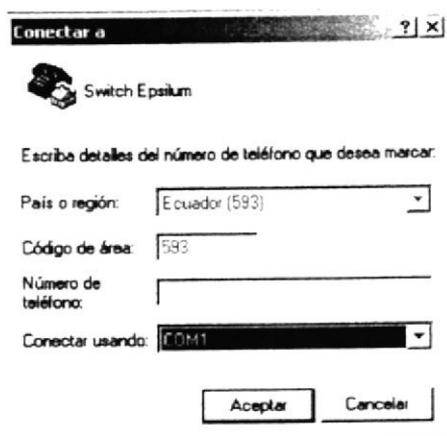


Figura 7.80. Ventana: Conectar a

6. En la siguiente pantalla encontrará algunos parámetros de conexión los cuales deberá establecer y dar clic en el botón Aceptar.
- 9600 bps. (velocidad de transmisión del cable serial de conexión)
  - 8 bits de Datos ( configuración del procesamiento de datos al pasar al hyperterminal en bits pos segundo)
  - Ninguno (paridad) (utilizado para comprobar errores en el grupo de bits de datos transferidos entre uno o varios equipos)
  - 1 (bit de parada) (medida de transporte por la que pasan datos al Hyperterminal)
  - Ninguno (control de flujo se refiere a la información que viaja)

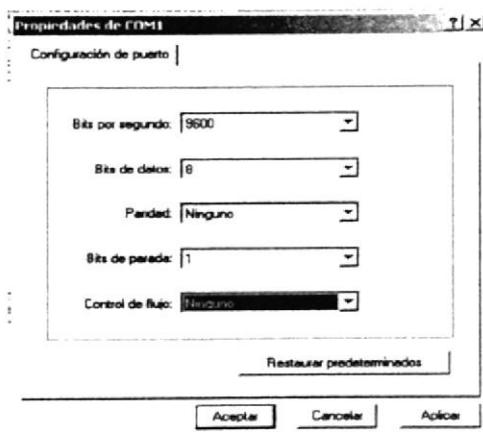


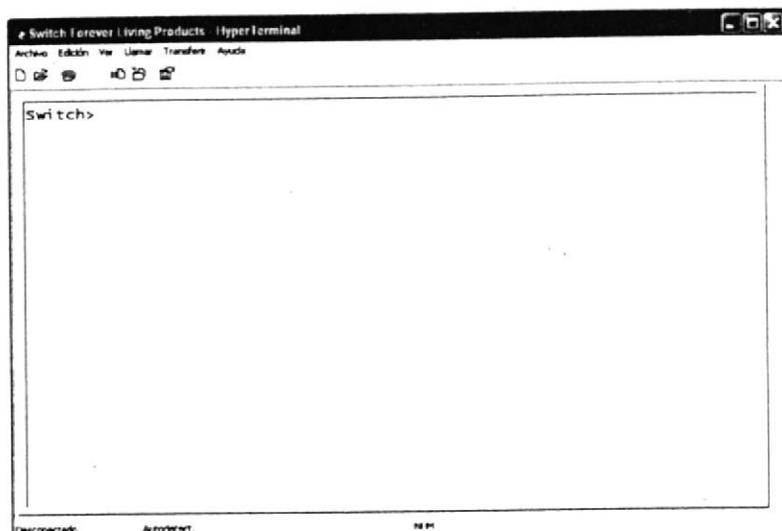
Figura 7.81. Propiedades del puerto COM 1



**Sugerencia:**

Se los puede establecer al dar clic en el botón **Restaurar predeterminados**.

7. Una vez colocado los parámetros dará clic en el botón **Aceptar** y podrá empezar con la configuración del router a través de la consola del Hyperterminal.



**Figura 7.82.** Hyperterminal con la conexión al switch

### 7.10.2 CONFIGURACIÓN DE SWITCH MATRIZ

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

1. Se ingresará el comando *enable* para acceder de modo usuario al modo privilegiado del switch

```
Switch >  
Switch>enable  
Ingresará al modo privilegiado
```

2. Ingresará al modo de configuración global

```
Switch#configure terminal  
Accederá al modulo privilegiado con el comando configure Terminal
```

3. Una vez ingresado a la configuración global, se le asigna un nombre al Switch para identificarlos.

```
Switch (config) #hostname Sw_Matriz  
Sirve para asignarle un nombre, en este caso Sw_ Matriz  
Sw_Matriz (config) #
```

4. Luego se configura las contraseñas

```
Sw_Matriz (config) #line console 0  
Ingresa a configurar la consola  
Sw_Matriz (config-line) #password < password >  
Asigna una contraseña a la consola  
Sw_Matriz (config-line) #login  
Sw_Matriz (config-line) #exit  
Sale de la configuración de la consola  
Sw_Matriz (config) #line vty 0 15  
Ingresa a configurar la Terminal Virtual  
Sw_Matriz (config-line) #password < password >  
Asigna una contraseña a la Terminal Virtual  
Sw_Matriz (config) #enable password <password>  
Agrega una contraseña para ingresar al router  
Sw_Matriz (config) #enable secret <password>  
Agrega una contraseña encriptada para ingresar al router
```

5. Se crean las VLAN's

```
Sw_Matriz >  
Sw_Matriz >enable  
Ingresará al modo privilegiado  
Sw_Matriz#vlan database  
Ingresa al modo de configuración de vlan's
```

**Sw\_Matriz (vlan) #vlan 10 name Servidores**  
Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Matriz (vlan) #vlan 20 name Ventas**  
Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Matriz (vlan) #vlan 30 name Dep\_Tecnico**  
Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Matriz (vlan) #vlan 40 name Networking**  
Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Matriz (vlan) #vlan 50 name Produccion**  
Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Matriz (vlan) #vlan 60 name Gerencia**  
Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Matriz (vlan) #vlan 70 name Diseño**  
Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Matriz (vlan) #vlan 80 name Bodega**  
Asigna un número referencial y un nombre a la vlan que quiere crear

6. Asignará las VLAN a los puertos.

**Sw\_Matriz >enable**  
Ingresará al modo privilegiado

**Sw\_Matriz#configure terminal**  
Ingresa al modo de configuración global

**Sw\_Matriz (config) # interface fastethernet 0/2**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 10**  
Asigna en puerto a la vlan 10

**Sw\_Matriz (config) # interface fastethernet 0/3**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 20**  
Asigna en puerto a la vlan 20

**Sw\_Matriz (config) # interface fastethernet 0/4**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 30**  
Asigna en puerto a la vlan 30

**Sw\_Matriz (config) # interface fastethernet 0/5**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 40**  
Asigna en puerto a la vlan 40

**Sw\_Matriz (config) # interface fastethernet 0/6**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 50**  
Asigna en puerto a la vlan 50

**Sw\_Matriz (config) # interface fastethernet 0/7**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 60**  
Asigna en puerto a la vlan 60

**Sw\_Matriz (config) # interface fastethernet 0/8**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 70**  
Asigna en puerto a la vlan 70

**Sw\_Matriz (config) # interface fastethernet 0/9**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode access**  
Ingresa al modo de configuración para asignar la vlan

**Sw\_Matriz (config-if) # switchport access vlan 80**  
Asigna en puerto a la vlan 80

**Sw\_Matriz (config-if) # exit**  
Sale al modo de configuración global

#### 7. Crear el enlace troncal

**Sw\_Matriz >enable**  
Ingresará al modo privilegiado

**Sw\_Matriz#configure terminal**  
Ingresa al modo de configuración global

**Sw\_Matriz (config) # interface fastethernet 0/1**  
Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Matriz (config-if) # switchport mode trunk**  
Se trunca el puerto arriba mencionado

8. Procederá a configurar en el router las subinterfaces de las VLAN's creadas.

**Matriz (config) #interface FastEthernet 0/0.10**

Mediante el comando interface Fastethernet ingresará a la subinterfaz FastEthernet 0/0.10 asociada a la Vlan 10

**Matriz (config-subif) #encapsulation dot1q 10**

Mediante el comando encapsulation definirá el tipo de encapsulamiento.

**Matriz (config-subif) #ip address 192.168.10.1 255.255.255.240**

Asignará IP mediante el comando IP Address

192.168.10.1 Indica el default Gateway de las Vlan

255.255.255.240 máscara que le corresponde con un salto de 16

9. Ingresará a la siguiente subinterfaz

**Matriz (config) #interface FastEthernet 0/0.20**

Mediante el comando interface Fastethernet ingresará a la subinterfaz FastEthernet 0/0.20 asociada a la Vlan 20

**Matriz (config-subif) #encapsulation dot1q 20**

Mediante el comando encapsulation definirá el tipo de encapsulamiento

**Matriz (config-subif) #ip address 192.168.10.17 255.255.255.248**

Asignará IP mediante el comando IP Address

192.168.10.17 Indica el default Gateway de las Vlan

255.255.255.248 máscara que le corresponde con un salto de 8

10. Ingresará a la siguiente subinterfaz

**Matriz (config) #interface FastEthernet 0/0.30**

Mediante el comando interface Fastethernet ingresará a la subinterfaz

**Matriz (config-subif) #encapsulation dot1q 30**

Mediante el comando encapsulation definirá el tipo de encapsulamiento

**Matriz (config-subif) #ip address 192.168.10.25 255.255.255.248**

Asignará IP mediante el comando IP Address

192.168.10.25 Indica el default Gateway de las Vlan

255.255.255.248 máscara que le corresponde con un salto de 8

11. Ingresará a la siguiente subinterfaz

**Matriz (config) #interface FastEthernet 0/0.40**

Mediante el comando interface Fastethernet ingresará a la subinterfaz

**Matriz (config-subif) #encapsulation dot1q 40**

Mediante el comando encapsulation definirá el tipo de encapsulamiento

**Matriz (config-subif) #ip address 192.168.10.33 255.255.255.240**

Asignará IP mediante el comando IP Address

192.168.10.33 Indica el default Gateway de las Vlan

255.255.255.240 máscara que le corresponde con un salto de 16

12. Ingresará a la siguiente subinterfaz

**Matriz (config) #interface FastEthernet 0/0.50**

Mediante el comando `interface FastEthernet` ingresará a la subinterfaz

**Matriz (config-subif) #encapsulation dot1q 50**

Mediante el comando `encapsulation` definirá el tipo de encapsulamiento

**Matriz (config-subif) #ip address 192.168.10.41 255.255.255.248**

Asignará IP mediante el comando `IP Address`

192.168.10.41 Indica el default Gateway de las Vlan

255.255.255.248 máscara que le corresponde con un salto de 8

13. Ingresará a la siguiente subinterfaz

**Matriz (config) #interface FastEthernet 0/0.60**

Mediante el comando `interface FastEthernet` ingresará a la subinterfaz

**Matriz (config-subif) #encapsulation dot1q 60**

Mediante el comando `encapsulation` definirá el tipo de encapsulamiento

**Matriz (config-subif) #ip address 192.168.10.49 255.255.255.248**

Asignará IP mediante el comando `IP Address`

192.168.10.49 Indica el default Gateway de las Vlan

255.255.255.248 máscara que le corresponde con un salto de 8

14. Ingresará a la siguiente subinterfaz

**Matriz (config) #interface FastEthernet 0/0.70**

Mediante el comando `interface FastEthernet` ingresará a la subinterfaz

**Matriz (config-subif) #encapsulation dot1q 70**

Mediante el comando `encapsulation` definirá el tipo de encapsulamiento

**Matriz (config-subif) #ip address 192.168.10.57 255.255.255.248**

Asignará IP mediante el comando `IP Address`

192.168.10.57 Indica el default Gateway de las Vlan

255.255.255.248 máscara que le corresponde con un salto de 8

15. Ingresará a la siguiente subinterfaz

**Matriz (config) #interface FastEthernet 0/0.80**

Mediante el comando `interface FastEthernet` ingresará a la subinterfaz

**Matriz (config-subif) #encapsulation dot1q 80**

Mediante el comando `encapsulation` definirá el tipo de encapsulamiento

**Matriz (config-subif) #ip address 192.168.10.65 255.255.255.248**

Asignará IP mediante el comando `IP Address`

192.168.10.65 Indica el default Gateway de las Vlan

255.255.255.248 máscara que le corresponde con un salto de 8

16. Salir de la configuración

**Matriz (config-subif) #exit**

### 7.10.2.1 SHOW RUNNING SWITCH MATRIZ

```
Sw-Matriz#show running-config
!
Versión 12.1
(versión del Sistema Operativo del switch)
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
(el servicio de encriptación de contraseña no está activo)
!
hostname Sw-Matriz
(nombre del switch)
enable secret 5 $sdf$6978yhg$jnb76sd
(Indica que la contraseña de ingreso al switch se encuentra encriptada)
enable password cisco
(Indica que la contraseña al switch es cisco)
!
!
!
ip subnet-zero
(Sirve para utilizar la ip inicial al momento de subnetear)
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
interface FastEthernet0/1
(Puerto 0/1 con enlace troncal)
switchport mode trunk
!
interface FastEthernet0/2
(Puerto asignado a la vlan 10)
switchport mode access
switchport access vlan 10
!
interface FastEthernet0/3
(Puerto asignado a la vlan 20)
switchport mode access
switchport access vlan 20
!
interface FastEthernet0/4
(Puerto asignado a la vlan 30)
switchport mode access
switchport access vlan 30
!
```

```
interface FastEthernet0/5
(Puerto asignado a la vlan 40)
switchport mode access
switchport access vlan 40
!
interface FastEthernet0/6
(Puerto asignado a la vlan 50)
switchport mode access
switchport access vlan 50
!
interface FastEthernet0/7
switchport mode access
switchport access vlan 60
!
interface FastEthernet0/8
switchport mode access
switchport access vlan 70
!
interface FastEthernet0/9
switchport mode access
switchport access vlan 80
!
interface FastEthernet0/10
(Puerto sin configurar)
!
interface FastEthernet0/11
(Puerto sin configurar)
!
interface FastEthernet0/12
(Puerto sin configurar)
!
vtp Server
vtp domain bigdomain
!
interface Vlan 1
(Puerto 1 del switch, vlan de administración o defecto por donde salen los
demás puertos si no tuvieran ninguna vlan asignada)
no ip address
no ip route-cache
!
vlan 10 name Servidores
(Vlan's creadas)
vlan 20 name Ventas
vlan 30 name Dep_Tecnico
vlan 40 name Networking
vlan 50 name Produccion
vlan 60 name Gerencia
vlan 70 name Diseño_y_Des
vlan 80 name Bodega
!
```

```
ip classless
no ip http server
!
!
!
!
line con 0
(contraseña para la línea de comandos)
login
transport input none
password cisco
line aux 0
line vty 0 15
(contraseña para telnet)
login
password cisco
!
no scheduler allocate

end
```

## 7.10.2.2 SHOW VLAN SWITCH MATRIZ

```
Switch#show vlan
```

VLAN	Name	Status	Ports
-----	-----	-----	-----
<b>1</b>	<b>default</b>	<b>active</b>	<b>Fa0/1, Fa0/10, Fa0/11, Fa0/12</b>
# de VLAN	Nombre	Estado	Puertos asignados a VLAN
<b>10</b>	<b>Servidores</b>	<b>active</b>	<b>Fa0/2</b>
	(puertos asignados y activos a la vlan Servidores)		
<b>20</b>	<b>Ventas</b>	<b>active</b>	<b>Fa0/3</b>
	(puertos asignados y activos a la vlan Ventas)		
<b>30</b>	<b>Dep_Tecnico</b>	<b>active</b>	<b>Fa0/4</b>
	(puertos asignados y activos a la vlan Dep. Técnico)		
<b>40</b>	<b>Networking</b>	<b>active</b>	<b>Fa0/5</b>
	(puertos asignados y activos a la vlan Networking)		
<b>50</b>	<b>Produccion</b>	<b>active</b>	<b>Fa0/6</b>
	(puertos asignados y activos a la vlan Producción)		
<b>60</b>	<b>Gerencia</b>	<b>active</b>	<b>Fa0/7</b>
	(puertos asignados y activos a la vlan Gerencia)		
<b>70</b>	<b>Diseño_y_Des</b>	<b>active</b>	<b>Fa0/8</b>
	(puertos asignados y activos a la vlan Diseño y Ger)		
<b>80</b>	<b>Bodega</b>	<b>active</b>	<b>Fa0/9</b>
	(puertos asignados y activos a la vlan Bodega)		
<b>1002</b>	<b>fddi-default</b>	<b>active</b>	
	(vlan para red fddi activa)		
<b>1003</b>	<b>token-ring-default</b>	<b>active</b>	
	(vlan para red token ring activa)		
<b>1004</b>	<b>fddinet-default</b>	<b>active</b>	
<b>1005</b>	<b>trnet-default</b>	<b>active</b>	

### 7.10.3 CONFIGURACIÓN DE SWITCH LOJA

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

1. Se ingresará el comando `enable` para acceder de modo usuario al modo privilegiado del switch

```
Switch >  
Switch>enable  
Ingresará al modo privilegiado
```

2. Ingresará al modo de configuración global

```
Switch#configure terminal  
Accederá al modulo privilegiado con el comando configure Terminal
```

3. Una vez ingresado a la configuración global, se le asigna un nombre al Switch para identificarlos.

```
Switch (config) #hostname Sw_Loja  
Sirve para asignarle un nombre, en este caso Sw_ Loja  
Sw_Loja (config) #
```

4. Luego se configura las contraseñas

```
Sw_Loja (config) #line console 0  
Ingresa a configurar la consola  
Sw_Loja (config-line) #password < password >  
Asigna una contraseña a la consola  
Sw_Loja (config-line) #login  
Sw_Loja (config-line) #exit  
Sale de la configuración de la consola  
Sw_Loja (config) #line vty 0 15  
Ingresa a configurar la Terminal Virtual  
Sw_Loja (config-line) #password < password >  
Asigna una contraseña a la Terminal Virtual  
Sw_Loja (config) #enable password <password>  
Agrega una contraseña para ingresar al router  
Sw_Loja (config) #enable secret <password>  
Agrega una contraseña encriptada para ingresar al router
```

5. Se crean las VLAN's

```
Sw_Loja >  
Sw_Loja >enable  
Ingresará al modo privilegiado  
Sw_Loja #vlan database  
Ingresa al modo de configuracion de vlan's
```

**Sw\_Loja (vlan) #vlan 10 name Servidores**

Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Loja (vlan) #vlan 20 name Ventas**

Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Loja (vlan) #vlan 30 name Networking**

Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Loja (vlan) #vlan 40 name Producción**

Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Loja (vlan) #vlan 50 name Gerencia**

Asigna un número referencial y un nombre a la vlan que quiere crear

6. Asignará las VLAN a los puertos.

**Sw\_Loja >enable**

Ingresa al modo privilegiado

**Sw\_Loja #configure terminal**

Ingresa al modo de configuración global

**Sw\_Loja (config) # interface fastethernet 0/2**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Loja (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Loja (config-if) # switchport access vlan 10**

Asigna en puerto a la vlan 10

**Sw\_Loja (config) # interface fastethernet 0/3**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Loja (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Loja (config-if) # switchport access vlan 20**

Asigna en puerto a la vlan 20

**Sw\_Loja (config) # interface fastethernet 0/4**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Loja (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Loja (config-if) # switchport access vlan 30**

Asigna en puerto a la vlan 30

**Sw\_Loja (config) # interface fastethernet 0/5**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Loja (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Loja (config-if) # switchport access vlan 40**

Asigna en puerto a la vlan 40

**Sw\_Loja (config) # interface fastethernet 0/6**

Ingresa a la interfaz y puerto que quiere configurar

```
Sw_Loja (config-if) # switchport mode access  
Ingresa al modo de configuración para asignar la vlan  
Sw_Loja (config-if) # switchport access vlan 50  
Asigna en puerto a la vlan 50  
Sw_Loja (config-if) # exit  
Sale al modo de configuración global
```

#### 7. Crear el enlace troncal

```
Sw_Loja >enable  
Ingresará al modo privilegiado  
Sw_Loja #configure terminal  
Ingresa al modo de configuración global  
Sw_Loja (config) # interface fastethernet 0/1  
Ingresa a la interfaz y puerto que quiere configurar  
Sw_Loja (config-if) # switchport mode trunk  
Se trunca el puerto arriba mencionado
```

#### 8. Proceder a configurar en el router las subinterfases de las VLAN's creadas.

```
Loja (config) #interface FastEthernet 0/0.10  
Mediante el comando interface Fastethernet ingresará a la subinterfaz  
Loja (config-subif) #encapsulation dot1q 10  
Mediante el comando encapsulation definirá el tipo de encapsulamiento  
Loja (config-subif) #ip address 192.168.11.1 255.255.255.248  
Asignará IP mediante el comando IP Address
```

#### 9. Ingresará a la siguiente subinterfaz.

```
Loja (config) #interface FastEthernet 0/0.20  
Mediante el comando interface Fastethernet ingresará a la subinterfaz  
Loja (config-subif) #encapsulation dot1q 20  
Mediante el comando encapsulación definirá el tipo de encapsulamiento  
Loja (config-subif) #ip address 192.168.11.9 255.255.255.248  
Asignará IP mediante el comando IP Address
```

#### 10. Ingresará a la siguiente subinterfaz

```
Sw_Loja (config) #interface FastEthernet 0/0.30  
Mediante el comando interface Fastethernet ingresará a la subinterfaz  
Loja (config-subif) #encapsulation dot1q 30  
Mediante el comando encapsulation definirá el tipo de encapsulamiento  
Loja (config-subif) #ip address 192.168.11.17 255.255.255.248  
Asignará IP mediante el comando IP Address
```

11. Ingresará a la siguiente subinterfaz

**Loja (config) #interface FastEthernet 0/0.40**

Mediante el comando `interface FastEthernet` ingresará a la subinterfaz

**Loja (config-subif) #encapsulation dot1q 40**

Mediante el comando `encapsulation` definirá el tipo de encapsulamiento

**Loja (config-subif) #ip address 192.168.11.25 255.255.255.248**

Asignará IP mediante el comando `IP Address`

12. Ingresará a la siguiente subinterfaz

**Loja (config) #interface FastEthernet 0/0.50**

Mediante el comando `interface FastEthernet` ingresará a la subinterfaz

**Loja (config-subif) #encapsulation dot1q 50**

Mediante el comando `encapsulation` definirá el tipo de encapsulamiento

**Loja (config-subif) #ip address 192.168.11.33 255.255.255.248**

Asignará IP mediante el comando `IP Address`

13. Salir de la configuración

**Loja (config-subif) #exit**

**7.10.3.1. SHOW RUNNING SWITCH LOJA****Sw\_Loja#show running-config**

```
!  
!  
Version 12.1  
(versión del Sistema Operativo del switch)  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
(el servicio de encriptación de contraseña no está activo)  
  
!  
hostname Sw-Loja  
(nombre del switch)  
enable secret 5 $sdf$6978yhg$jnb76sd  
(Indica que la contraseña de ingreso al switch se encuentra encriptada)  
enable password cisco  
(Indica que la contraseña al switch es cisco)  
!  
ip subnet-zero  
(Sirve para utilizar la ip inicial al momento de subnetear)spanning-tree extend  
system-id)  
!  
interface FastEthernet0/1  
(Puerto con enlace troncal)  
switchport mode trunk  
!  
interface FastEthernet0/2  
(Puerto asignado a la vlan 10)  
switchport mode access  
switchport access vlan 10  
!  
interface FastEthernet0/3  
(Puerto asignado a la vlan 20)  
switchport mode access  
switchport access vlan 20  
!  
interface FastEthernet0/4  
(Puerto asignado a la vlan 30)  
switchport mode access  
switchport access vlan 30  
!  
interface FastEthernet0/5  
(Puerto asignado a la vlan 40)  
switchport mode access  
switchport access vlan 40  
!  
interface FastEthernet0/6  
(Puerto asignado a la vlan 50)  
switchport mode access
```

```
switchport access vlan 50
!  
interface FastEthernet0/7  
(Puerto sin configurar)  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
vtp Server  
vtp domain bigdomain  
!  
interface Vlan 1  
(Puerto 1 del switch, vlan de administración o defecto por donde salen los  
demás puertos si no tuvieran ninguna asignada)  
no ip address  
no ip route-cache  
!  
vlan 10 name Servidores  
(Vlan's creadas)  
vlan 20 name Ventas  
vlan 30 name Networking  
vlan 40 name Produccion  
vlan 50 name Gerencia  
!  
ip classless  
no ip http server  
!  
!  
line con 0  
( contraseña para la línea de comandos)  
login  
transport input none  
password cisco  
line aux 0  
line vty 0 15  
(contraseña para telnet)  
login  
password cisco  
!  
no scheduler allocate  
end
```

## 7.10.3.2. SHOW VLAN SWITCH LOJA

Sw\_Loja#show vlan

Switch#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/10, Fa0/11, Fa0/12
# de VLAN	Nombre	Estado	Puertos asignados a VLAN
10	Servidores	active	Fa0/2 (puertos asignados y activos a la vlan Servidores)
20	Ventas	active	Fa0/3 (puertos asignados y activos a la vlan Ventas)
30	Networking	active	Fa0/4 (puertos asignados y activos a la vlan Networking)
40	Produccion	active	Fa0/5 (puertos asignados y activos a la vlan Produccion)
50	Gerencia	active	Fa0/6 (puertos asignados y activos a la vlan Gerencia)
1002	fdi-default	active	(vlan para red fdi active)
1003	token-ring-default	active	(vlan para red token ring active)
1004	fdinet-default	active	
1005	trnet-default	active	

### 7.10.4 CONFIGURACIÓN DE SWITCH AMBATO

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, los reconocerá por su formato de color azul.

1. Se ingresará el comando enable para acceder de modo usuario al modo privilegiado del switch

```
Switch >  
Switch>enable  
Ingresará al modo privilegiado
```

2. Ingresará al modo de configuración global

```
Switch#configure terminal  
Accederá al modulo privilegiado con el comando configure Terminal
```

3. Una vez ingresado a la configuración global, se le asigna un nombre al Switch para identificarlos.

```
Switch (config) #hostname Sw_Ambato  
Sirve para asignarle un nombre, en este caso Sw_ Ambato  
Sw_Ambato (config) #
```

4. Luego se configura las contraseñas

```
Sw_Ambato (config) #line console 0  
Ingresa a configurar la consola  
Sw_Ambato (config-line) #password < password >  
Asigna una contraseña a la consola  
Sw_Ambato (config-line) #login  
Sw_Ambato (config-line) #exit  
Sale de la configuración de la consola  
Sw_Ambato (config) #line vty 0 15  
Ingresa a configurar la Terminal Virtual  
Sw_Ambato (config-line) #password < password >  
Asigna una contraseña a la Terminal Virtual  
Sw_Ambato (config) #enable password <password>  
Agrega una contraseña para ingresar al router  
Sw_Ambato (config) #enable secret <password>  
Agrega una contraseña encriptada para ingresar al router
```

5. Se crean las VLAN's

```
Sw_Ambato >  
Sw_Ambato >enable  
Ingresará al modo privilegiado  
Sw_Ambato #vlan database  
Ingresa al modo de configuración de vlan's  
Sw_Ambato (vlan) #vlan 10 name Servidores  
Asigna un número referencial y un nombre a la vlan que quiere crear
```

**Sw\_Ambato (vlan) #vlan 20 name Ventas**

Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Ambato (vlan) #vlan 30 name Nertworking**

Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Ambato (vlan) #vlan 40 name Produccion**

Asigna un número referencial y un nombre a la vlan que quiere crear

**Sw\_Ambato (vlan) #vlan 50 name Gerencia**

Asigna un número referencial y un nombre a la vlan que quiere crear

#### 6. Asignar las VLAN a los puertos.

**Sw\_Ambato >enable**

Ingresa al modo privilegiado

**Sw\_Ambato #configure terminal**

Ingresa al modo de configuración global

**Sw\_Ambato (config) # interface fastethernet 0/2**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Ambato (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Ambato (config-if) # switchport access vlan 10**

Asigna en puerto a la vlan 10

**Sw\_Ambato (config) # interface fastethernet 0/3**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Ambato (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Ambato (config-if) # switchport access vlan 20**

Asigna un puerto a la vlan 20

**Sw\_Ambato (config) # interface fastethernet 0/4**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Ambato (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Ambato (config-if) # switchport access vlan 30**

Asigna en puerto a la vlan 30

**Sw\_Ambato (config) # interface fastethernet 0/5**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Ambato (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

**Sw\_Ambato (config-if) # switchport access vlan 40**

Asigna en puerto a la vlan 40

**Sw\_Ambato (config) # interface fastethernet 0/6**

Ingresa a la interfaz y puerto que quiere configurar

**Sw\_Ambato (config-if) # switchport mode access**

Ingresa al modo de configuración para asignar la vlan

```
Sw_Ambato (config-if) # switchport access vlan 50
```

Asigna en puerto a la vlan 50

```
Sw_Ambato (config-if) # exit
```

Sale al modo de configuración global

7. Crear el enlace troncal

```
Sw_Ambato >enable
```

Ingresará al modo privilegiado

```
Sw_Ambato #configure terminal
```

Ingresa al modo de configuración global

```
Sw_Ambato (config) # interface fastethernet 0/1
```

Ingresa a la interfaz y puerto que quiere configurar

```
Sw_Ambato (config-if) # switchport mode trunk
```

Se trunca el puerto arriba mencionado

8. Proceder a configurar en el router las subinterfases de las VLAN's creadas

```
Ambato (config) #interface FastEthernet 0/0.10
```

Mediante el comando interface Fastethernet ingresará a la subinterfaz

```
Ambato (config-subif) #encapsulation dot1q 10
```

Mediante el comando encapsulation definirá el tipo de encapsulamiento

```
Ambato (config-subif) #ip address 192.168.12.1 255.255.255.248
```

Asignará IP mediante el comando IP Address

9. Ingresará a la siguiente subinterfaz

```
Ambato (config) #interface FastEthernet 0/0.20
```

Mediante el comando interface Fastethernet ingresará a la subinterfaz

```
Ambato (config-subif) #encapsulation dot1q 20
```

Mediante el comando encapsulación definirá el tipo de encapsulamiento

```
Ambato (config-subif) #ip address 192.168.12.9 255.255.255.248
```

Asignará IP mediante el comando IP Address

10. Ingresará a la siguiente subinterfaz

```
Ambato (config) #interface FastEthernet 0/0.30
```

Mediante el comando interface Fastethernet ingresará a la subinterfaz

```
Ambato (config-subif) #encapsulation dot1q 30
```

Mediante el comando encapsulación definirá el tipo de encapsulamiento.

```
Ambato (config-subif) #ip address 192.168.12.9 255.255.255.248
```

Asignará IP mediante el comando IP Address

11. Ingresará a la siguiente subinterfaz

```
Ambato (config) #interface FastEthernet 0/0.40
```

Mediante el comando interface Fastethernet ingresará a la subinterfaz.

**Ambato (config-subif) #encapsulation dot1q 40**

Mediante el comando encapsulación definirá el tipo de encapsulamiento

**Ambato (config-subif) #ip address 192.168.12.25 255.255.255.248**

Asignará IP mediante el comando IP Address

12. Ingresará a la siguiente subinterfaz

**Ambato (config) #interface FastEthernet 0/0.50**

Mediante el comando interface Fastethernet ingresará a la subinterfaz

**Ambato (config-subif) #encapsulation dot1q 50**

Mediante el comando encapsulation definirá el tipo de encapsulamiento

**Ambato (config-subif) #ip address 192.168.12.33 255.255.255.248**

Asignará IP mediante el comando IP Address

13. Salir de la configuración

**Ambato (config-subif) #exit**

**7.10.4.1. SHOW RUNNING SWITCH AMBATO**

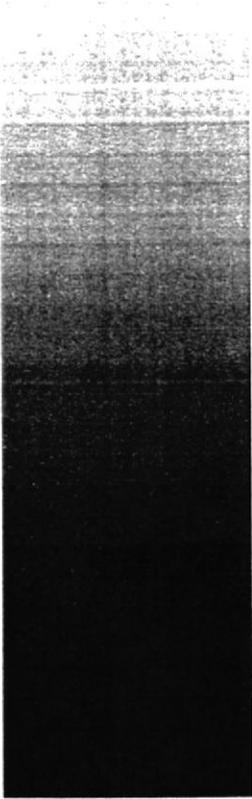
```
Sw_Ambato#show running-config
!
!
Version 12.1
(versión del Sistema Operativo del switch)
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
(el servicio de encriptación de contraseña no esta activo)
!
hostname Sw-Loja
(nombre del switch)
enable secret 5 $sdf$6978yhg$jnb76sd
(Indica que la contraseña de ingreso al switch se encuentra encriptada)
enable password cisco
(Indica que la contraseña al switch es cisco)
!
!
ip subnet-zero
(Sirve para utilizar la ip inicial al momento de subnetear)
spanning-tree extend system-id
!
interface FastEthernet0/1
(Puerto con enlace troncal)
switchport mode trunk
!
interface FastEthernet0/2
(Puerto asignado a la vlan 10)
switchport mode access
switchport access vlan 10
!
interface FastEthernet0/3
(Puerto asignado a la vlan 20)
switchport mode access
switchport access vlan 20
!
interface FastEthernet0/4
(Puerto asignado a la vlan 30)
switchport mode access
switchport access vlan 30
!
interface FastEthernet0/5
(Puerto asignado a la vlan 40)
switchport mode access
switchport access vlan 40
!
interface FastEthernet0/6
(Puerto asignado a la vlan 50)
```

```
switchport mode access
switchport access vlan 50
!
interface FastEthernet0/7
(Puerto sin configurar)
!
interface FastEthernet0/8
!
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
vtp Server
vtp domain bigdomain
!
interface Vlan 1
(Puerto 1 del switch, vlan de administración o defecto por donde salen los
demás puertos si no tuvieran ninguna asignada)
no ip address
no ip route-cache
!
vlan 10 name Servidores
(Vlan's creadas)
vlan 20 name Ventas
vlan 30 name Networking
vlan 40 name Production
vlan 50 name Gerencia
!
ip classless
no ip http server
!
line con 0
( contraseña para la línea de comandos)
login
transport input none
password cisco
line aux 0
line vty 0 15
(contraseña para telnet)
login
password cisco
!
no scheduler allocate
end
```

## 7.10.4.2. SHOW VLAN SWITCH LOJA

Sw\_Ambato#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/10, Fa0/11, Fa0/12
# de VLAN	Nombre	Estado	Puertos asignados a VLAN
VLAN	Administración	VLAN	
10	Servidores	active	Fa0/2 (puertos asignados y activos a la vlan Servidores).
20	Ventas	active	Fa0/3 (puertos asignados y activos a la vlan Ventas)
30	Networking	active	Fa0/4 (puertos asignados y activos a la vlan Networking)
40	Producción	active	Fa0/5 (puertos asignados y activos a la vlan Producción)
50	Gerencia	active	Fa0/6 (puertos asignados y activos a la vlan Gerencia)
1002	fddi-default	active	(vlan para red fddi active)
1003	token-ring-default	active	(vlan para red token ring active)
1004	fddinet-default	active	
1005	trnet-default	active	



---

# GLOSARIO

## GLOSARIO DE TÉRMINOS

# A

**Ancho de Banda:** La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también se usa para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

**ARP:** Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Comprar con RARP.

**Asignación de direcciones:** Técnica que permite que distintos protocolos interoperen traduciendo direcciones desde un formato a otro. Por ejemplo, al enrutar IP a través de una red Frame Relay, las direcciones IP se deben mapear a las direcciones Frame Relay de modo que los paquetes IP se puedan transmitir por la red. Ver también resolución de direcciones.

**ACPI:** Advanced Configuration and Power Interface. Especificación de administración de recursos de energía, que permite que el sistema operativo controle la cantidad de energía distribuida a distintos periféricos. Por ejemplo, los que no estén siendo usados en un determinado momento se apagan para consumir menos energía. Desarrollado por Intel, Compaq, Phoenix, Microsoft y Toshiba.

**ADSL:** Línea de Suscripción Asimétrica Digital. Tecnología que mejora el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps (Megabits por segundo) gracias a una serie de métodos de compresión.

**ARIN:** American Registry of Internet Numbers. Organización en Estados Unidos que gestiona las direcciones IP del país, y sus territorios asignados. Debido a que las direcciones en Internet son limitadas, es necesaria una organización que controle y asigne los bloques numéricos.

**ARPANet:** Advanced Research Projects Agency Network. Precursor del Internet desarrollado a finales de los 60's y principios de los 70's por el Departamento de Defensa de los Estados Unidos como un experimento de una red de área, no centralizada y amplia y que resista una guerra nuclear.

**ASCII:** American Standard Code for Information Interchange. Es de facto el estándar del World Wide para el código utilizado por computadoras para representar todas las letras (mayúsculas, minúsculas, letras latinas, números, signos de puntuación, etc.). El código estándar ASCII es de 128 letras representadas por un dígito binario de 7 posiciones (7 bits), de 0000000 a 1111111.

**ASF:** *Advanced Streaming Format:* Este formato de archivos almacena información de audio y video, y fue especialmente diseñado para trabajar en redes, como Internet. La información es descargada como un flujo continuo de datos, y por ende, no es necesario esperar la descarga completa del archivo para poder reproducirlo.

**ATM:** Acrónimo en inglés de *Asynchronous Transfer Mode*. Modo de Transferencia Asíncrona. Es una tecnología de redes de alta velocidad que transmite múltiples tipos de información (voz, video, datos) mediante la creación de "paquetes de datos".

**Atom:** Un protocolo para la sindicación y compartir contenido. Atom se desarrolla como un sucesor mejorado a RSS y será más complejo que RSS. Atom brindará soporte para firmas digitales.

**Antivirus:** Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

## B

**Banda Ancha:** Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 Khz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica.

**Broadcast:** Envío de información en cualquier formato a más de un lugar de destino.

**Banda Base:** Características de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha. Ver la diferencia con banda ancha. Término utilizado en la WWW.

**Bps:** (Bits per Second). Medida que representa la rapidez con que los bits de datos se transmiten a través de un medio de comunicaciones. Por ejemplo: un módem de 28.8 Kbps es capaz de transferir 28.800 bits por segundo.

**Bits:** (Binary Digit o Dígito Binario). Es un dígito en base 2, es decir, 0 ó 1. Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

**Byte:** Unidad de medida de cantidad de información en formato digital. Usualmente un byte consiste de 8 bits. Un bits es un cero (0) o un uno (1). Esa secuencia de números (byte) pueden simbolizar una letra o un espacio (un carácter). Un kilobyte (Kb) son 1024 bytes y un Megabyte (Mb) son 1024 Kilobytes.

**Bloqueo:** Es un sistema de conmutación, una condición al que no hay ninguna ruta disponible para completar un círculo. El término también se usa para describir una situación en la que no se puede hincar una actividad hasta que la otra no se hay completado.

## C

**Cable blindado:** Cable que posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

**Cable coaxial:** Cable compuesto por un conducto cilíndrico exterior hueco que rodea un conductor de alambre interno único. En la actualidad se usan dos tipos de cable coaxial en la LAN: cable de 50 ohmios, que se usa para la señalización digital, y cable de 75 ohmios que se usa para señales analógicas y señalización digital de alta velocidad.

**Cable de fibra óptica:** Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro, sin embargo no es susceptible a la interferencia electromagnética y es capaz de brindar velocidades de datos más altas.

**Cable neutro:** Cable de circuito que se conecta a la conexión a tierra en la central de energía y en el transformador.

**Cableado:** Columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.

**Cableado de Categoría 1:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 1 se usa para comunicaciones telefónicas y no es adecuado para transmitir datos. Comparar con cableado de Categoría 2, cableado de Categoría 3, cableado de categoría 4 y cableado de categoría 5.

**Cableado de Categoría 2:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3, cableado de categoría 4 y cableado de categoría 5.

**Cableado de Categoría 3:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 3 se usa en las redes 10BASE-T y puede transmitir datos a velocidades de hasta 10 Mbps. Comparar con cableado de Categoría 2, cableado de categoría 4 y cableado de categoría 5.

**Cableado de Categoría 4:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 4 Se usa en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Comparar con cableado de Categoría 2, cableado de Categoría 3, y cableado de categoría 5.

**Cableado de Categoría 5:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3 y cableado de categoría 4.

**Caché:** Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso mas rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los acceso a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

**CD:** Detección de portadora. Señal que indica si una interfaz está activa. También, una señal generada por un módem que indica que se ha conectado una llamada.

**Canaleta decorativa:** Tipo de canal montado en la pared que tiene una cubierta removible que se usa para admitir el cableado horizontal. La canaleta decorativa es lo suficientemente grande como para contener dos cables.

**Canaleta:** Un tipo de canal adosado a la pared que tiene una cubierta removible para dar apoyo al cableado horizontal. La canaleta es lo suficientemente grande como para contener varios cables.

**Capa física:** La Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

**Capa de control de enlace de datos:** La Capa 2 del modelo de arquitectura SNA. Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

**Capa de red:** La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

**Capa de transporte:** La capa 4 del modelo de referencia OSI. Esta capa es responsable de la comunicación confiable de red entre nodos finales. La capa de transporte suministra mecanismos para establecer, mantener y terminar los circuitos virtuales, detección y recuperación de errores de transporte y control del flujo de información.

**Capa de sesión:** La capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de capa de presentación.

**Capa de servicios de presentación:** La capa 6 del modelo de arquitectura SNA. Esta capa suministra administración de recursos de red, servicios de presentación de sesión y alfo de administración de aplicaciones. Corresponde aproximadamente a la capa de presentación del modelo OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control física, capa de servicios de transacción y capa de control de transmisión.

**Capa de aplicación:** La capa 7 del modelo de referencia OSI. Esta capa suministra servicios a los procesos de aplicación (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de Terminal) que están fuera del modelo OSI. La capa de aplicación identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos que se requieren para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos. Corresponde aproximadamente a la capa de servicios de transacción del modelo SNA. Ver también capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

**Carrier:** Compañía que proporciona servicios de telecomunicaciones a través de medios de comunicación de datos (fibra óptica, microondas, radio, conexión telefónica o enlace satelital). Los cuales pueden ser propios o alquilados, estos proveedores suelen suministrar sus servicios basándose en redes de compañías telefónicas.

**Cliente:** Nodo que solicita servicios a un servidor.

**Colisión:** En ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

**Cola:** Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

**Conector RJ:** Conector macho registrado. Conectores estándares que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ.

**Costo:** Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.

**Consola:** DTE a través del cual se introducen los comandos en un host.

**Correo electrónico:** Aplicación de red utilizado ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.

**CSMA/CD:** Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un periodo de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

**Clic:** Acción de presionar y soltar rápidamente el botón del Mouse.

**Cliente:** Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para trabajar con uno o más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

**Computador:** Es un dispositivo electrónico básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

**Contraseña ó Password:** Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los sistemas y recursos de la computadora.

**CPU:** (Central Processing Unit ó Unidad Central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

**Cuadro de Diálogo:** Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

**Cuadro de texto:** Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de dialogo, el cuadro de texto puede estar en blanco o contener texto.

**Cursor:** Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo carácter a visualizar cuando se pulse una tecla.

**CSU:** Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con loop telefónico digital local. A menudo se denominada, de forma conjunta con DSU, como CSU/DSU.

## D

**Db:** Decibelios.

**Dominio:** En Internet, una parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía.

**DCE:** Equipo de comunicación de datos. Equipo de comunicación de datos (expansión EIA) o equipo de terminación de circuito de datos (expansión ITU-T). El dispositivo y las conexiones de una red de comunicaciones que abarca el extremo de la red de la interfaz usuario a red. El DCE proporciona una conexión física con la red, envía tráfico y suministra una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE. Comparar con DTE.

**Descifrado:** La aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando por lo tanto los datos a su estado original, no cifrado.

**Dato:** Son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

**DTE:** Equipo de Terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario-red que actúa como origen de datos, destino de datos o ambas. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y por lo tanto general usa señales de temporización generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadores, traductores de protocolo y multiplexores.

**Directorio:** En D.O.S., una lista de nombres de archivo que contiene toda la información de los archivos almacenados. A partir de Windows 95 este término se reemplazó por CARPETA.

**Dirección:** Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico" (e-mail address); "IP" (dirección Internet); "dirección hardware".

**Dirección del Protocolo de Internet (dirección IP):** Dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red con Protocolo de control de transmisión/Protocolo Internet (TCP/IP). Número único que consta de 4 partes separadas por puntos. Una dirección IP se suele representar en una notación decimal con puntos que indica cada octeto (ocho bits o un byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 172.16.255.255.

Cada computadora conectada a Internet tiene un único número de IP. Si la máquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem).

**Disco Rígido:** Unidad de almacenamiento permanente de información. Éste es el que guarda la información cuando apagamos la computadora. Aquí se guardan la mayoría de los programas y el sistema operativo. Su capacidad de almacenamiento se mide en Megabytes (Mb) o Gigabytes (Gb), en donde 1024 Mb = 1Gb.

**Disquete:** Dispositivo que puede insertarse y extraerse en una unidad de disco.

**DNS:** (Domain Name System o Sistema de Nombres de Dominio). El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("host") basándose en los nombres de éstos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes son: .COM (comercial – empresas), .EDU (educación, centros docentes), .ORG (organización sin ánimo de lucro), .NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejército USA). La mayoría de los países tienen un dominio propio. Por ejemplo, AR (Argentina), .PY(Paraguay), :US (Estados Unidos de América), .Es (España), .AU(Australia), etc.

**Dominio:** (Domain Name). Nombre único que identifica a un sitio de Internet. Los nombres de dominio tienen 2 o más secciones, separadas por puntos. La sección de la izquierda es la más específica, y la de la derecha, la más general. Una computadora particular puede tener más de un nombre de dominio, pero un nombre de dominio se refiere únicamente a una PC.

**Download ó descargar:** En Internet es el proceso de transferir información desde un servidor de información a la propia PC.

**Documentación:** Manual escrito que detalla el manejo de un sistema o pieza de hardware.

**Doble clic:** Acción de presionar y soltar rápidamente el botón del Mouse (ratón) dos veces, sin desplazarlo. Esta acción sirve para ejecutar una determinada aplicación, como por ejemplo: inicializarla.

**DSU:** Unidad de servicio de datos. Dispositivo que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión como, por ejemplo, T1 y E1.

**DVD:** (Digital Versatile Disc o Disco Versátil Digital). Disco que sirve para almacenar más datos de contenido digital, como música o video, que un CD. Un DVD guarda un mínimo de 4.7 Gigabytes (el tamaño de una película de cine).

**Duplex:** Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir / transmitir cualquier tipo de información. Existen dos modalidades HALF-DUPLEX cuando puede recibir y transmitir alternativamente y FULL-DUPLEX cuando puede hacer ambas cosas simultáneamente.

**Directorio Activo:** El Directorio Activo (Active Directory) es el servicio de directorio incluido en Windows 2000 Server y posterior. Existen las características de las versiones anteriores de El Directorio Activo, es un servicio de directorio patentado por Microsoft, que se encuentra integrado en la arquitectura de Windows 2000 Server y posterior. Es similar a otros servicios de directorio, como el de Novell (NDS). Es un sistema centralizado que automatiza en la red la gestión de los datos de usuario, seguridad, y recursos distribuidos; también permite la interacción con otros directorios. El Directorio Activo está diseñado especialmente para entornos de red distribuidos.

**Dato:** Unidad mínima que compone cualquier información.

**Denegación de Servicio:** Incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red. En los peores casos, por ejemplo, un sitio web accedido por millones de personas puede verse forzado temporalmente a cesar de operar. Un ataque de denegación de servicio puede también destruir

programas y archivos de un sistema informático. Aunque normalmente es realizado de forma intencionada y maliciosa, este tipo de ataques puede también ocurrir de forma accidental algunas veces. Si bien no suele producirse robo de información estos ataques pueden costar mucho tiempo y dinero a la persona u organización afectada.

# E

**E1:** Estándar Europeo equivalente al americano T1. Los circuitos E1 y T1. Los dos usan canales de 64 Kbps, pero el T1 tiene 24 mientras que el E1 tiene 32 canales.

**EIA / TIA - 568:** Estándar que describe las características y aplicaciones para diversos grados de tendido UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

**Encapsulamiento:** El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

**Emulación de terminal:** Aplicación de red en la que un computador ejecuta software que la hace aparecer ante un host remoto como una Terminal conectada directamente.

**Enrutamiento:** Proceso para encontrar una ruta hacia un host destino. El enrutamiento en redes de gran tamaño es muy complejo dada la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

**Ethernet:** Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Seros Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3. Ver también 10BASE2, 10BASE5, 10BASE-F, 10BASE-T, 10Broad36 e IEEE 802.3.

**Elemento de Pantalla:** Partes que constituyen una ventana o cuadro de dialogo como por ejemplo: la barra de título, los botones de "Maximizar" y "Minimizar", los bordes de las ventanas y las barras de desplazamiento.

**Escritorio:** Fondo de la pantalla sobre la cual aparecen ventanas, iconos y cuadros de diálogo.

**Estación de trabajo:** Computador de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. Llamadas así para distinguirlas de los que se conocen como servidores.

**Expandir:** *Mostrar los niveles de directorio ocultos del árbol de directorios. Con el administrador de archivos es posible expandir un solo nivel de directorio, una rama del árbol de directorio o todas las ramas a la vez.*

**Explorador:** *Llamado también explorador Web. Interfaz cliente que permite al usuario ver documentos HTML en el World Wide Web, en otra red o un su propio equipo; seguir los hipervínculos y transferir archivos. Un ejemplo es Microsoft Internet Explorer.*

**Extensión:** *Está compuesto por un punto y un sufijo de hasta tres caracteres situados al final de un nombre de archivo. La extensión suele indicar el tipo de archivo o directorio.*

**Encriptación:** *Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.*

**ENIAC:** *Electronic Numerical Integrator and Computer. Primera computadora digital, creada por pedido del Army norteamericano para computar las tablas de balística de la II guerra mundial. Se termino de ensamblar en 1945.*

**Ergonomía:** *Ciencia que trata del encaje del hombre en su entorno técnico y laboral.*

**Ethernet:** *Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, tiene ancho de banda de 10 Mbps de forma que presenta una elevada velocidad de transmisión; y se ha convertido en un estándar de red corporativa.*

**Extranet:** *Cuando una intranet tiene partes públicas, en donde posiblemente usuarios externos al intranet pueden llenar formularios que forman parte de procesos internos del Intranet.*

## F

**Fibra monomodo:** *Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único. Ver también fibra multimodo.*

**Fibra multimodo:** *Fibra óptica que permite la propagación de múltiples frecuencias de luz.*

**Firewall:** *Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red*

privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

**Fluctuación de fase:** Distorsión analógica de la línea de comunicación provocada por la variación de una señal de sus posiciones de temporización de referencia. La fluctuación de fase puede provocar la pérdida de datos, especialmente a altas velocidades.

**Flujo de datos:** Todos los datos que se transmiten a través de la línea de comunicaciones en una sola operación de lectura o escritura.

**Frecuencia:** Cantidad de ciclos, medidos en hercios, de una señal de corriente alterna por unidad de tiempo.

**FTP:** Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP, que se usa para transferir archivos entre nodos de la red. El FTP se define en la RFC 959.

**Full duplex:** Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora.

## G

**Gateway:** En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función y gateway se refiere a un dispositivo con fines especiales que ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra.

**Gateway fronterizo:** Router que se comunica con router de otros sistemas autónomos.

**Giga:** Prefijo que indica un múltiplo de 1.000 millones, o sea  $10^9$ . Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de  $2^{30}$ , o sea 1.073.741.824.

**Grupo de Trabajo:** Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

# H

**Hardware:** Son todos los componentes físicos que componen una PC.

**Hercio:** Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

**Hexadecimal:** Base 16. Representación numérica que usa los dígitos 0 a 9, con su significado habitual, y las letras A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, luego  $16^2=256$ , etc.

**Host:** Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

**HTML:** (Hypertext Markup Language). Lenguaje utilizado para crear los documentos de hipertexto que se emplean en la www. Los documentos HTML son simples archivos de texto que contienen instrucciones (llamadas tags) entendibles por el Navegador (Browser).

**HTTP:** (Hypertext Transport Protocol). Protocolo utilizado para transferir archivos de hipertexto a través de Internet. Requiere de un programa "cliente" de http en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la www.

**Hub:** Dispositivo de hardware o software que contiene módulos de red y equipo de internetwork múltiples, independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen, las señales que se envían a través de ellos).

# I

**IEEE:** Instituto de Ingenieros Eléctricos y electrónicos. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN de IEEE son los estándares de LAN predominantes en el mundo actual.

**IEEE 802.1:** Especificación del IEEE que describe un algoritmo que evita los loops de capa dos mediante la creación de un spanning tree. El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo de Digital y el algoritmo IEEE 802.1 no son exactamente los mismos, ni tampoco son compatibles.

**IEEE 802.12:** Estándar LAN del IEEE que especifica la capa física y la subcapa MAC de la capa de enlace de datos. El IEEE 802.12 usa el esquema de acceso a los medios de prioridad de demanda a 100 Mbps a través de una diversidad de medios físicos. Ver también 100VG-Any LAN.

**IEEE 802.2:** Protocolo LAN del IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 administra errores, entramado, control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se usa en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

**IEEE 802.3:** Protocolo LAN del IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 usa acceso CSMA/CD a diversas velocidades sobre diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican las implementaciones de Fast Ethernet. Las variantes físicas de la especificación IEEE 802.3 original incluyen 10BASE2, 10BASE5, 10BASE-F, 10BASE-T y 10Broad36. Las variantes físicas de Fast Ethernet incluyen 100BASE-T, 100BASE-T4 y 100BASE-X.

**Icono:** Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc.

**IDF:** Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella.

**Impresora:** Dispositivo de salida, cuya funcionalidad es transcribir / pasar un documento (imagen y/o texto) desde el ordenador (procesador de textos, block de notas, visor de imágenes, etc.) a un medio físico, generalmente papel, mediante el uso de cinta, cartuchos de tinta también con tecnología láser.

**Impresora de Inyección a tinta:** Crean imágenes directamente sobre el papel al rociar tinta a través de una pequeña boquilla, su calidad de impresión es bastante alta.

**Impresora Predeterminada:** Impresoras que se utiliza si se elige el comando Imprimir, no habiendo especificado antes la impresora que se desea utilizar. Sólo puede haber una impresora predeterminada, que debe ser la que se utilice con mayor frecuencia.

**Información:** Es lo que se obtiene del procesamiento de datos, es el resultado final.

**Informático cliente - servidor:** Término que se usa para describir los sistemas de red informáticos distribuidos (de procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: cliente (front end) y servidor (back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas a software o a los dispositivos informáticos actuales.

**Internetwork:** Conjunto de red interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red.

**IP:** Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad. Documentado en la RFC-791.

**IP access-group:** Comando que enlaza una lista de acceso existente con una interfaz de salida.

**IP host:** Comando que se usa para crear una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.

**IP multicast:** Técnica de enrutamiento que permite que el tráfico IP se propague desde un origen hacia un número de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, se envía un paquete a un grupo de multicast que se identifica mediante una sola dirección de grupo de destino IP.

**IPX:** Intercambio de paquetes de internetworking. Protocolo de capa de red (Capa 3) de Netware que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

**Interfaz:** Una conexión e interacción entre hardware, software y usuario, es decir, como la plataforma o medio de comunicación entre usuario o programa.

**Internet:** Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

**Intranet:** Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno.

**ISO:** Organización Internacional de Normalización. Organización internacional que es responsable por una amplia gama de estándares, incluyendo aquellos relevantes para el networking. ISO desarrolló el modelo de referencia OSI, un modelo de referencia de networking sumamente popular.

**ISP:** Un proveedor de servicios de Internet compra acceso directo a Internet a través de una compañía de Internet, y revende el servicio a sus abonados a través de la conexión telefónica a redes mediante un MODEM (o a grandes clientes mediante circuitos de T1 o E1 de línea privada o retransmisión de trama) a demás de añadir servicios propios, como son el correo electrónico, las paginas web, etc.

# J

**Jumper:** Término que se usa para los cables de interconexión que se encuentran en el armario de cableado.

# K

**Kbps:** (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit está formado por mil bits.

**Kilobyte:** Es el equivalente a 1024 bytes.

# L

**LAN:** Red de área Local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido. Comparar con MAN y LAN.

**Latencia:** Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir también sucede en el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

**LED:** Diodo emisor de luz. Dispositivo semiconductor que emite luz producida por la conversión de energía eléctrica. Las lámparas de estado en los dispositivos de hardware generalmente son LED.

**Línea de acceso telefónico:** Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

**Línea de comunicación:** Enlace físico (como, por ejemplo, un cable o circuito de teléfono) que conecta uno o más dispositivos con uno o más dispositivos.

**Línea de mira:** Característica de determinados sistemas de transmisión como, por ejemplo, los sistemas láser, de microondas e infrarrojos, en los que no puede existir ninguna obstrucción en la ruta directa entre el transmisor y el receptor.

**Línea dedicada:** Línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir. Ver también línea arrendada.

**Línea de acceso:** Lista que mantienen los routers Cisco para controlar el acceso hacia o desde el router para diversos servicios (por ejemplo, para evitar que los paquetes que tienen una determinada dirección IP salgan de una interfaz específica del router).

**LSA:** Publicación de estado de enlace. Paquete de broadcast que usan los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de la ruta. Los routers receptores usan las LSA para mantener sus tablas de enrutamiento.

**Login:** Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del password, el login no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

## M

**MAC:** Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

**MICIP:** Protocolo de capa de red que encapsula paquetes IP en DOS o transmisión a través de AppleTalk.

**Malla:** Topología de red en la que los dispositivos se organizan de una manera administrable, segmentada, con varias interconexiones, a menudo redundantes, ubicadas estratégicamente entre nodos de la red. Ver también malla completa y malla parcial.

**Malla completa:** Término que describe a una red en la que los dispositivos están organizados en una topología de malla, en la que cada nodo de la red tiene un circuito físico o un circuito virtual que lo conecta a todos los otros nodos de la red. Una malla completa brinda una gran cantidad de redundancia pero, dado que su implementación puede resultar excesivamente cara, generalmente se la reserva para los backbones de la red. Ver también malla y malla parcial.

**MAN:** Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

**MAP:** Protocolo de automatización de fabricación. Arquitectura de red creada por General Motors para satisfacer las necesidades específicas, las instalaciones fabriles. El MAP especifica una LAN de transmisión de tokens similar a IEEE 802.4.

**Mapa de Cableado:** Características suministrada por la mayoría de los analizadores de cable. Se usa para probar las instalaciones de cableado de par trenzado, y muestra cuáles hilos están conectados a cuáles pines, en conectores macho y hembra.

**Mapa de topología:** Herramienta para administrar un switch ATM LightStream 2020 que examina una red y muestra el estado de sus nodos y enlaces troncales. El mapa de topología es una aplicación basada en HP OpenView que se ejecuta en NMS.

**Máscara de red:** Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

**Máscara wildcard:** Cantidad de 32 bits que se usan de forma conjunta con un dirección IP para determinar cuáles son los bits de una dirección que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

**MD5:** Message Digest 5. Algoritmo que se usa para la autenticación de mensajes en SNMP v.2. El MD5 verifica la integridad de la comunicación, autentica el origen y controla la puntualidad. Ver también SNMP2.

**MDF:** Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

**Megabyte (MB):** 1.048.576 bytes; 1.024 kilobytes.

**Megahertz:** Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

**Memoria RAM:** Memoria de acceso aleatorio cuyo contenido permanecerá presente mientras el computador permanezca encendido.

**Memoria ROM:** Memoria de sólo lectura. Chip de memoria que sólo almacena permanentemente instrucciones y datos de los fabricantes.

**Microonda:** Este enlace esta constituido por dos transceptores de radio provistos de antenas parabólicas que se apuntan directamente entre sí. La radio puede transportar transmisiones punto a punto de mucho ancho de

banda. Su alcance varía según el tamaño de la antena, el clima en la zona y la magnitud de la potencia emitida contemplando todos estos conjuntos la señal puede llegar hasta 80 Km.

**Módem:** (Modulator, Demodulator). Dispositivo que se conecta a la computadora y a la línea telefónica y que permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

**Mouse:** Permite convertir el movimiento de la mano en desplazamiento de un cursor sobre la pantalla.

**Multicast:** La multidifusión (multicast) permite que grupos de usuarios seleccionados reciban la misma transmisión de datos en una red los cuales están identificados por una única dirección de grupo de destino IP.

## N

**Navegador de Web:** Aplicación de cliente de hipertexto basada en GUI como, por ejemplo, Mosaic, que se usa para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a través de la www e Internet. Ver también hipertexto, Internet, Mosaic y www.

**NBP:** Protocolo de enlace de denominación. Protocolo AppleTalk de nivel de transporte que convierte un nombre dado en forma de una cadena de caracteres en una dirección de internetwork.

**NET:** Título de entidad de red. Direcciones de red, definidas por la arquitectura de red ISO.

**NetBIOS:** Sistema básico de entrada/salida de red. API que usan las aplicaciones de una LAN IBM para solicitar servicios de procesos de red de nivel inferior. Estos servicios pueden incluir establecimiento y terminación de sesión y transferencia de información.

**NetWare:** NOS distribuido de uso generalizado desarrollado por Novell. Suministra acceso remoto transparente a archivos, y muchos otros servicios de red distribuida.

**Networking:** Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

**NIC:** Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

**NOS:** Sistema Operativo de Red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos. Los ejemplos de NOS incluyen LAN Manager, NetWare y VINES.

**Número de host:** Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

**Número de red:** Parte de una dirección IP que especifica la red a la que pertenece el host.

**Número de saltos:** Métrica de enrutamiento que se usa para medir la distancia entre un origen y un destino. El RIP usa el número de saltos como su única métrica.

**NVRAM:** RAM no volátil. RAM que retiene su contenido cuando una unidad se apaga. En los productos Cisco, la NVRAM se usa para guardar la información de configuración.

**Nodo:** En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma.

**Nombre de usuario:** La secuencia de caracteres que lo identifica. Al conectarse a una computadora, generalmente necesita proporcionar su nombre y contraseña de usuario. Esta información se usa para verificar que la persona está autorizada para usar el Sistema.



**Operador de red:** Persona que monitorea y controla una red de forma continúa.

**Oscilación:** Señal secundaria superpuesta a la onda de 60 Hz. Tiene una magnitud que varía entre el 15% y el 100% del voltaje normal de la línea de alimentación. Ver sobrevoltaje, pico y baja de voltaje.

**OSI:** Interconexión de sistemas abiertos. Programa internacional de normalización creado por la ISO y la UIT-T para desarrollar estándares de interconexión que faciliten la interoperabilidad de equipos de múltiples proveedores.

**OSINET:** Asociación internacional diseñada para promover OSI en las arquitecturas de los proveedores.

**OSPF:** Versión abierta del algoritmo "Primero la ruta libre más corta". Algoritmo de enrutamiento IGP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad Internet. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga. El OSPF deriva de una versión inicial del protocolo ISIS.

## P

**PAD:** Ensamblador / desensamblador de paquetes. Dispositivos que se usa para conectar dispositivos simples (como terminales de modo de carácter) a una red, los cuales no admiten toda la funcionalidad de un protocolo específico. Los PAD almacenan los datos en el búfer de los PAD y ensamblan y desensamblan los paquetes que se envían a dichos dispositivos finales.

**Panel de conexión:** Conjunto de ubicaciones de pin y puertos que se puede montar en un bastidor o una consola de pared en el armario de cableado. Los paneles de conexión actúan como conmutadores que conectan los cables de las estaciones de trabajo entre sí y con exterior.

**Paquete:** Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

**Paquete de Choque:** Paquete que se envía al transmisor para informarle que hay congestión y que debe reducir su velocidad de envío.

**Par Trenzado:** Medio de transmisión de relativa baja velocidad compuesto por dos cables aislados dispuestos en un patrón en espiral regular. Los cables pueden ser blindados o no blindados. El uso del par trenzado es común en aplicaciones de telefonía y es cada vez más común en las redes de datos. Ver también STP y UTP.

**Paradiafonía:** Energía de interferencia transferida de un circuito a otro.

**PBX:** Central telefónica privada. Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas y públicas.

**PCI:** Información de control de protocolo. Información de control que se agrega a los datos del usuario para formar un paquete OSI.

**Pila de protocolo:** Conjunto de protocolos de comunicación relacionados que operan de forma conjunta y, como un grupo, cumplen con la comunicación en alguna o en las siete capas del modelo de referencia OSI. No todas las pilas de

protocolo abarcan cada capa del modelo y, a menudo, un solo protocolo de la pila se dirige a una cantidad de capas a la vez. El ECP/IP es un protocolo de pila típico.

**Ping:** Abreviatura para Packet Internet Groper o Packet Internetwork Groper, una utilidad que se usa para determinar si una dirección IP en particular está disponible. Funciona enviando un paquete a la dirección específica y esperando una respuesta. El PING se usa principalmente para diagnosticar las fallas de las conexiones de Internet.

**Plan de distribución:** Diagrama simple que indica dónde están ubicados los tendidos de cable y la cantidad de habitaciones hacia las que se dirigen.

**POP:** Punto de presencia. Punto de presencia es el punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y el servicio de distribución principal del edificio.

**Portadora:** Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos. Ver también modulación.

**POST:** Autocomprobación de encendido. Conjunto de diagnóstico de hardware que se ejecutan en un dispositivo de hardware cuando ese dispositivo se enciende.

**Protocolo de enrutamiento:** Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. Los ejemplos de protocolos de enrutamiento incluyen el IGRP, el OSPF y el RIP.

**Puerto:** Interfaz de un dispositivo de internetworking (como, por ejemplo, un router).

En terminología IP, un proceso de capa superior que recibe información de las capas inferiores.

Un conector hembra de un panel de conexión el cual acepta el mismo tamaño de conector que el de un RJ45. Los cables de conexión se usan en estos puertos para realizar interconexiones entre los computadores conectados al panel. Es esta interconexión la que permite la operación de la LAN.

**Página Web:** Documento de World Wide Web. Una página web suele consistir en un archivo HTML, con sus archivos asociados de gráficos y secuencias de comandos, en un directorio determinado de un equipo concreto (y, por tanto, identificable mediante una dirección URL).

**Periféricos:** Cualquier dispositivo de hardware conectado a una computadora.

**Pixel:** (Picture Cell). Es la parte más pequeña de una pantalla de video, constituido por uno o más puntos que se consideran como una unidad. Es por tanto, el bloque de construcción de imágenes.

**Protocolo:** Método por el que los equipos se comunican en Internet. El protocolo más común en el World Wide Web es HTTP. Otros protocolos de Internet incluyen FTP, Gopher y telnet. El protocolo forma parte de la dirección URL completa de un recurso.

**Proveedor:** Institución o empresa que provee acceso a uno o varios servicios de Internet.

## R

**RAM:** Memoria de acceso directo aleatorio. Memoria volátil que puede ser leída y escrita por un microprocesador.

**Red:** Conjunto de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

**Red de conexión única:** Red que tiene una sola conexión con un router.

**Redireccionar:** Parte de los protocolos ICMP y ES-IS que permiten que un router le indique a un host que puede ser más efectivo usar otro router.

**Redistribución:** Permitir que la información de enrutamiento detectada a través de un protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento. A veces denominada redistribución de ruta.

**Redundancia:** En internetworking, la duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan ejecutar el trabajo de aquellos que han fallado. Ver también sistema redundante.

**Rendimiento:** Velocidad de la información que llega a, y posiblemente atraviesa, un punto particular de un sistema de red.

**Retardo:** El tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. También, el tiempo que se requiere para mover un paquete desde el origen hacia el destino a través de una ruta específica.

**RF:** Radiofrecuencia. Término genérico que se usa para referirse a frecuencias que corresponden a transmisiones radioeléctricas. Las redes de televisión por cable y de banda ancha usan tecnología RF.

**Router:** Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red.

Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

**RIP:** Protocolo de información de enrutamiento. IGP más común de Internet.

**RMON:** Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitorio remoto de los dispositivos conectados a la red.

**ROM:** Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.

**Ruta Estática:** Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

**Ruta por defecto:** Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

## S

**Segmento:** La sección de una red limitada por puentes, routers o switches. Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

**SMTP:** Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico.

**Spread Spectrum:** Un sistema de espectro ensanchado es aquel que ocupa mas ancho de banda del mínimo requerido para la transferencia de señales de datos. La radio de espectro ensanchado emite y recibe señales portadoras en un espectro amplio de frecuencias.

**Sondeo:** Método de acceso en que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

**Switch:** Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

**Switch LAN:** Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches LAN envían tráfico basándose en las direcciones MAC. Esta variedad de switch LAN a veces se denomina switch de trama. Los switches LAN a menudo se clasifican de acuerdo con el método que usan para enviar tráfico: conmutación de paquetes por método de corte y conmutación de paquetes por almacenamiento y envío. Los switches multicapas son un subconjunto inteligente de los switches LAN.

**Servidor:** Computadora o programa que brinda un servicio específico al "cliente", que se ejecuta en otras computadoras. El término puede referirse tanto a un equipo de una red que envía archivos o ejecuta aplicaciones para otros equipos de una red; el software que se ejecuta en el equipo servidor y que efectúa la tarea de servir archivos y ejecutar aplicaciones; o bien, en la programación orientada a objetos, un fragmento de código de intercambiar información con otro fragmento de código cuando se pide.

**SO:** (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

**Software:** Todos los componentes no físicos de una PC (Programas).

## T

**T1:** Servicio de portadora de WAN digital. T1 transmite datos con formato DS-1 a 1.544 a través de la red de conmutación telefónica, usando codificación AMI o B8ZS. Comparar con E1. Ver también AMI, B8ZS y DS-1.

**Tabla de enrutamiento:** Tabla que se guarda en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas hacia destinos de red en particular y, en algunos casos, las métricas asociadas con esas rutas.

**TFTP:** Protocolo de Transferencia de Archivos Trivial. Versión simplificada del FTP que permite que los archivos se transfieran desde un computador a otra a través de una red.

**Terminal:** Dispositivo simple en el que los datos se pueden introducir o recuperar desde una red. Generalmente, las terminales tienen un monitor y un teclado pero no tienen ningún procesador ni unidad de disco local.

**Topología:** Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

**Topología de anillo:** Topología de red que consta de un conjunto de repetidores conectados entre sí mediante enlaces de transmisiones unidireccionales para formar un solo bucle cerrado. Cada estación de la red se conecta a la red en el repetidor. Aunque lógicamente están organizadas en

anillo, las topologías de anillo a menudo están organizadas en una estrella de bucle cerrado.

**Topología de bus:** Arquitectura LAN lineal en la que las transmisiones de las estaciones de red se propagan a lo largo del medio y son recibidas por todas las otras estaciones.

**Topología en árbol:** Topología LAN similar a la topología bus, salvo que las redes en árbol pueden tener ramificaciones con múltiples nodos. Las transmisiones desde una estación atraviesan la longitud del medio y son recibidas por todas las otras estaciones.

**Topología en estrella:** Topología LAN en la que los puntos de terminación de una red se conectan a un switch central común mediante enlaces punto a punto. Una topología de anillo que está organizada como estrella implementa una estrella de loop cerrado unidireccional en lugar de enlaces punto a punto.

**Topología en estrella jerárquica:** Topología en estrella extendida en la que un hub central se conecta a través de cableado vertical con otros hubs que dependen del mismo.

**Transceiver:** Unidad de conexión al medio. Dispositivo que se usa en las redes Ethernet e IEEE 802.3 que suministra la interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que se puede incorporar a una estación o puede ser un dispositivo individual, ejecuta funciones de capa física, incluyendo la conversión de datos digitales desde la interfaz Ethernet, detección de colisiones e inyecciones de bits en la red.

**TIA:** Asociación de la Industria de las Telecomunicaciones, Organización que desarrolla estándares relacionados con las tecnologías de telecomunicaciones.

**Tunneling:** Arquitectura que está diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.

**Tarjeta de Interfaz de Red: (NIC).** Dispositivo a través del cual computadoras de una red transmiten y reciben datos.

**TCP/IP:** (Transmisor Control Protocol / Internet Protocol). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

**Telnet:** Protocolo que permite al usuario de Internet conectarse y escribir comandos en un equipo remoto vinculado a Internet como si el usuario estuviera utilizando un Terminal de texto conectado directamente al equipo. Forma parte del conjunto de protocolos TCP/IP.

**Tiempo Real:** Método para procesar la información en cuanto se recibe.

# U

**Unicast:** En redes conmutadas ethernet, transferencia de archivos / paquetes entre dos entidades. Una difusión única puede iniciarla un servidor a una estación de trabajo, una estación a un servidor, una estación a una impresora o cualquier otra unidad única hacia otra entidad.

**UPS:** (Uninterruptible Power Suply ó Suministro de Energía Ininterrumpida). Es un estabilizador electrónico que está preparado para suplir al computador cuando se presenten caídas de energía o cambios de voltaje.

**URL:** (Universal Resource Locator ó Localizador de Recursos Universal). Identifica de manera única la ubicación de un equipo, directorio o archivo de Internet. La dirección URL también indica el protocolo de Internet apropiado, como HTTP o FTP. Por ejemplo: <http://www.microsoft.com>.

**USB:** Tecnología que facilita la conexión de periféricos a la computadora. Esta reconocer automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo, ya que se conecta a la parte trasera de la PC a un enchufe especial (puerto USB). La tarjeta madre debe tener esta tecnología en su CHIPSET para poder conectar dispositivos de este tipo.

**UTP:** Cable de para trenzado no apantallado, lo que significa que no tiene envoltura alrededor del grupo de conductores. Estos cables se usan principalmente en redes de voz y datos.

**Usuario:** Cualquier individuo que interactúa con el computador a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con el computador a nivel profesional.

# V

**Vector:** Segmento de datos de un mensaje SNA. Un vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

**Virtualización:** Proceso que se usa para implementar una red basada en segmentos de red virtuales. Los dispositivos se conectan a segmentos virtuales independientemente de su ubicación física y de su conexión física con la red.

**VLAN:** Lan Virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.

**VLSM:** Máscara de subred de longitud variable. Capacidad de especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

**VTP:** Protocolo de Terminal virtual. Aplicación ISO para establecer una conexión de Terminal virtual a través de una red.

**Virus:** Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan, se propagan a través de cualquier medio de almacenamiento, o a través de la LAN, o de la misma Internet.

## W

**WAN:** Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Frame Relay, SMDS y X.25 son ejemplos de WAN Comparar con LAN y MAN.

**WorkGroup Director:** Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroup Director se ejecuta en estaciones de trabajo UNIX, ya sea como una aplicación independiente o integrada con otra plataforma de administración de red basada en SNMP, brindando un sistema de gestión poderoso y transparente para los productos de grupo de trabajo de Cisco.

**WWW:** World Wide Web. Gran red de servidores de Internet la cual suministra servicios de hipertexto y otros a terminales que ejecutan aplicaciones de clientes como, por ejemplo, un navegador de web. Ver también navegador de web.

## X

**X Windows:** Protocolo que interconecta estaciones de trabajo de interfaz gráfica de usuario con programas servidores de aplicaciones que utiliza TCP/IP.

## Z

**Zona de autoridad:** Asociada con DNS, la zona de autoridad es una sección del árbol del nombre de dominio para el que un servidor de nombre es la autoridad.

# 0 - 9

**10 mbps:** Millones de bits por segundo unidad de velocidad de transferencia de información.

**10 base T:** Especificación Ethernet de banda base de 10 Mbps que usa dos pares de cables de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y otro para recibir datos. 10BASE-T, que forma parte de la especificación IEEE 802.3, tiene una limitación de distancia de aproximadamente 100 metros por segmento. Ver también Ethernet e IEEE 802.3.

**10 Base - F:** Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10 BASE-FB, 10BASE-FL y 10BASE-FP para Ethernet sobre cableado de fibra óptica. Ver también 10BASE-FB, 10BASE-FL, 10BASE-FP y Ethernet.

**100 Base FX:** Especificación Fast Ethernet de banda base de 100 Mbps que usa dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una temporización de señal adecuada, el enlace 100BASE-FX no puede exceder una longitud de 400 metros. Basado en el estándar IEEE 802.3. Ver también 100BASE-X, Fast Ethernet e IEEE 802.3.

**10 Base-F:** Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10 BASE-FB, 10 BASE-FL y 10BASE-FP para Ethernet sobre cableado de fibra óptica. Ver también 10BASE-FB, 10BASE-FL, 10BASE-FP y Ethernet.

**10 Base-FB:** Especificación Ethernet de banda base de 10 Mbps que usa cableado de fibra óptica. 10BASE-FB forma parte de la especificación IEEE 10BASE-F. No se utiliza para conectar estaciones de usuario pero, en cambio, suministra un backbone de señalización síncrona que permite que segmentos y repetidores adicionales se conecten a la red. Los segmentos 10BASE-FB pueden tener hasta 2000 metros de largo. Ver también 10BASE-F y Ethernet.

**10 Base-FL:** Especificación Ethernet de banda base de 10 Mbps que usa cableado de fibra óptica. 10BASE-FL forma parte de la especificación IEEE 10BASE-F y, aunque puede interoperar con FOIRL, está diseñado para reemplazar a la especificación FOIRL. Los segmentos 10BASE-FL pueden tener hasta 1000 metros de largo si se usan con FOIRL, y hasta 2000 metros si se usan exclusivamente con 10BASE-FL. Ver también 10BASE-F, Ethernet y FOIRL.

**10 Base - FP:** Especificación Ethernet de banda base de fibra pasiva de 10 Mbps que usa cableado de fibra óptica. La 10BASE-FP forma parte de la especificación IEEE 10BASE-F. Organiza una cantidad de computadores en una topología en estrella sin necesidad de usar repetidores. Los segmentos 10BASE-FP pueden tener hasta 500 metros de largo. Ver también 10BASE-F y Ethernet.