

**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**



**ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL**

**TÓPICO DE GRADUACIÓN**

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

**ANÁLISIS DE SOPORTE DE MICROCOMPUTADORES**

**TEMA**

**ADMINISTRACIÓN Y SEGURIDAD DE REDES**

**ALESSA**

**MANUAL DE USUARIO**

**AUTORES**

**ALEJANDRO EDUARDO TINGO YUNGAN  
OLGER EDUARDO GALARZA ROBLES**

**DIRECTOR**

**ANL. FABIÁN BARBOZA**

**AÑO  
2007**

## **AGRADECIMIENTO**

Al culminar mis estudios, al cual dedique todo mi esfuerzo durante todo este tiempo, quiero agradecer a Dios por guiarme y estar a mi lado brindándome la fuerza y paciencia para lograrlo.

En Especial a mis padres, el Sñr. Eduardo Tingo y la Sñr. Rosa Yungan que siempre creyeron en mí y a toda mi familia que me dieron el apoyo necesario a lo largo de mi carrera.

A la universidad Escuela Superior Politécnica del Litoral y a cada uno de los profesores que conocí a lo largo de mi carrera universitaria.

Quiero también agradecer a todos mis amigos que de una u otra manera me han brindado su ayuda y apoyo.

Al Director Analista Fabián Barboza quien supo guiarme en el transcurso de la elaboración de este manual, brindándome no solo su tiempo, sino también sus conocimientos.

**ALEJANDRO TINGO YUNGAN**

## **DEDICATORIA**

Este proyecto se lo dedico a Dios por todo lo que me ha dado y haberme permitido dar un nuevo paso en mi vida.

A mis padres, por ser los mejores y estar conmigo incondicionalmente, gracias porque sin ellos y sus enseñanzas no estaría aquí ni sería quien soy ahora, a ellos les dedico este triunfo.

A mi hermana y a mis sobrinos Valeria y Andrés siempre los llevare en mi corazón.

**ALEJANDRO TINGO YUNGAN**

## **AGRADECIMIENTO**

Agradezco primeramente a Dios, por darme la sabiduría y orientarme en todos mis actos, también a mi familia por apoyarme siempre y darme la fuerza y el ejemplo moral para seguir luchando, por alcanzar nuevos peldaños.

También mis sinceros agradecimientos a los Almacenes Estuardo Sánchez ALESSA, por haberme dado la oportunidad de poder realizar nuestro trabajo en tan prestigiosa empresa.

Y también a mis amigos y profesores por apoyarme siempre y creer en mí.

**OLGER EDUARDO GALARZA ROBLES**

## **DEDICATORIA**

Dedico con todo mi corazón este trabajo de graduación, a mi madre que con su ejemplo de tenacidad, esfuerzo, dedicación y amor me ha dado fuerzas para escalar otro peldaño en mi vida y profesión.

También a mis hermanos, padre y sobrinos que siempre han creído en mí y están apoyándome.

Y con mucho amor a mi esposa que me dá esa seguridad, felicidad y fortaleza para seguir luchando con fuerza y mucha fé; también a mi hija Isabel que es lo más grande que tengo en este mundo.

**OLGER EDUARDO GALARZA ROBLES**

## **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, al EDCOM (*Escuela de Diseño y Comunicación Visual*) de la escuela Superior politécnica del litoral.


(Reglamento de exámenes y títulos de la ESPOL).

**FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN**



**CARL FABIAN BARBOZA**

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

  
ALEJANDRO TINGO YUNGAN

  
EDUARDO GALARZA ROBLES

# CONTENIDO GENERAL

## CAPÍTULO 1

1.	GENERALIDADES .....	1
1.1.	INTRODUCCIÓN .....	1
1.2.	OBJETIVO DE ESTE MANUAL .....	1
1.3.	A QUIÉN VA DIRIGIDO. ....	1

## CAPÍTULO 2

2.	SITUACIÓN ACTUAL.....	1
2.1.	ANTECEDENTES.....	1
2.2.	MISIÓN .....	1
2.3.	VISIÓN .....	1
2.4.	INFRAESTRUCTURA LAN .....	2
2.4.1.	ESTACIONES DE TRABAJO.....	2
2.4.1.1.	MATRIZ .....	2
2.4.1.1.1.	DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO EDIFICIO MATRIZ .....	2
2.4.1.1.2.	CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE MATRIZ .....	2
2.4.1.2.	SUCURSAL CENTRO.....	2
2.4.1.2.1.	DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL CENTRO.....	3
2.4.1.2.2.	CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL CENTRO.....	3
2.4.1.3.	EDIFICIO SUR.....	3
2.4.1.3.1.	DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL SUR .....	3
2.4.1.3.2.	CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL SUR .....	4
2.4.1.4.	EDIFICIO BAHÍA.....	4
2.4.1.4.1.	DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL BAHÍA .....	4
2.4.1.4.2.	CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL BAHÍA .....	4
2.4.1.5.	EDIFICIO NORTE .....	5
2.4.1.5.1.	DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL NORTE .....	5
2.4.1.5.2.	CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL NORTE .....	5
2.4.2.	SERVIDORES .....	5
2.4.2.1.	MATRIZ .....	5
2.4.2.1.1.	DISTRIBUCIÓN DE LOS SERVIDORES EN MATRIZ .....	5
2.4.2.1.2.	CARACTERÍSTICAS DE SERVIDORES EN MATRIZ.....	6
2.4.2.2.	SUCURSAL CENTRO.....	6
2.4.2.2.1.	DISTRIBUCIÓN DE LOS SERVIDORES SUCURSAL CENTRO	6

2.4.2.2.2.	CARACTERÍSTICAS DE SERVIDORES EN SUCURSAL CENTRO .....	7
2.4.2.3.	SUCURSAL SUR.....	7
2.4.2.3.1.	DISTRIBUCIÓN DE LOS SERVIDORES SUCURSAL SUR.....	7
2.4.2.3.2.	CARACTERÍSTICAS DE SERVIDORES EN SUCURSAL SUR.....	7
2.4.2.4.	SUCURSAL BAHÍA .....	7
2.4.2.4.1.	DISTRIBUCIÓN DE LOS SERVIDORES SUCURSAL BAHÍA ..	7
2.4.2.4.2.	CARACTERÍSTICAS DE SERVIDORES EN SUCURSAL BAHÍA .....	8
2.4.3.	DISTRIBUCIÓN DE CABLEADO .....	9
2.4.3.1.	MATRIZ .....	9
2.4.3.2.	SUCURSAL CENTRO.....	10
2.4.3.3.	SUCURSAL SUR.....	11
2.4.3.4.	SUCURSAL BAHÍA .....	12
2.4.3.5.	SUCURSAL NORTE .....	13
2.4.4.	ANÁLISIS DE PISO .....	14
2.4.4.1.	MEZANINE EDIFICIO MATRIZ .....	14
2.4.4.2.	PRIMER PISO EDIFICIO MATRIZ .....	15
2.4.4.3.	SEGUNDO PISO EDIFICIO MATRIZ .....	16
2.4.4.4.	TERCER PISO EDIFICIO MATRIZ .....	17
2.4.4.5.	CUARTO PISO EDIFICIO MATRIZ.....	18
2.4.4.6.	MEZANINE EDIFICIO CENTRO .....	19
2.4.4.7.	PRIMER PISO EDIFICIO CENTRO.....	20
2.4.4.8.	SEGUNDO PISO EDIFICIO CENTRO.....	21
2.4.4.9.	TERCER PISO EDIFICIO CENTRO .....	22
2.4.4.10.	CUARTO PISO EDIFICIO CENTRO .....	23
2.4.4.11.	MEZANINE EDIFICIO SUR.....	24
2.4.4.12.	PRIMER PISO EDIFICIO SUR.....	25
2.4.4.13.	SEGUNDO PISO EDIFICIO SUR.....	26
2.4.4.14.	TERCER PISO EDIFICIO SUR.....	27
2.4.4.15.	CUARTO PISO EDIFICIO SUR .....	28
2.4.4.16.	MEZANINE EDIFICIO BAHÍA.....	29
2.4.4.17.	PRIMER PISO EDIFICIO BAHÍA .....	30
2.4.4.18.	SEGUNDO PISO EDIFICIO BAHÍA .....	31
2.4.4.19.	TERCER PISO EDIFICIO BAHÍA.....	32
2.4.4.20.	CUARTO PISO EDIFICIO BAHÍA.....	33
2.4.4.21.	SUCURSAL NORTE .....	34
2.4.5.	DISPOSITIVOS DE CONMUTACIÓN .....	35
2.4.6.	MATRIZ .....	35
2.4.6.1.	SUCURSAL CENTRO.....	35
2.4.6.2.	SUCURSAL SUR.....	36
2.4.6.3.	SUCURSAL BAHÍA .....	36
2.4.7.	MEDIOS DE COMUNICACIÓN .....	36
2.4.7.1.	ALAMBICO .....	36
2.4.7.1.1.	MATRIZ – SUCURSAL CENTRO .....	36
2.4.7.1.2.	MATRIZ – SUCURSAL SUR .....	37
2.4.7.1.3.	MATRIZ – SUCURSAL BAHÍA.....	37
2.4.8.	INFRAESTRUCTURA WAN.....	37
2.4.8.1.	DISPOSITIVOS DE ENRUTAMIENTO .....	37
2.4.8.1.1.	MATRIZ – SUCURSAL CENTRO .....	37

2.4.8.1.2.	MATRIZ – SUCURSAL SUR .....	38
2.4.8.1.3.	MATRIZ – SUCURSAL BAHÍA.....	38
2.4.9.	COMUNICACIÓN WAN A NIVEL DE MEDIOS.....	39
2.4.10.	COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS .....	40
2.4.11.	INTERNET .....	41
2.4.11.1.	RECEPCIÓN DE INTERNET EN MATRIZ.....	41
2.4.12.	PROBLEMAS ENCONTRADOS.....	42

## CAPÍTULO 3

3.	PROPUESTA .....	1
3.1.	PROBLEMAS ENCONTRADOS.....	1
3.2.	SOLUCIÓN PROPUESTA .....	2
3.3.	ESTUDIO DE FACTIBILIDAD .....	3
3.3.1.	ALTERNATIVA 1 .....	3
3.3.1.1.	FACTIBILIDAD TÉCNICA .....	3
3.3.1.2.	FACTIBILIDAD OPERATIVA.....	5
3.3.1.3.	FACTIBILIDAD ECONÓMICA .....	6
3.3.1.3.1.	COSTOS DE HARDWARE.....	6
3.3.1.3.2.	COSTOS DE OPERATIVOS.....	7
3.3.1.4.	COSTO DE FACTIBILIDAD ALTERNATIVA 1 .....	7
3.3.1.5.	PLAN DE TRABAJO.....	8
3.3.1.6.	VENTAJAS .....	9
3.3.1.7.	BENEFICIOS .....	9
3.3.1.8.	GARANTÍAS .....	9
3.3.1.9.	FORMA DE PAGO .....	9
3.3.2.	ALTERNATIVA 2 .....	10
3.3.2.1.	FACTIBILIDAD TÉCNICA .....	10
3.3.2.2.	FACTIBILIDAD OPERATIVA.....	12
3.3.2.3.	FACTIBILIDAD ECONÓMICA .....	13
3.3.2.3.1.	COSTOS DE HARDWARE.....	13
3.3.2.3.2.	COSTOS DE OPERATIVOS.....	14
3.3.2.4.	COSTO DE FACTIBILIDAD ALTERNATIVA 1 .....	14
3.3.2.5.	PLAN DE TRABAJO.....	15
3.3.2.6.	VENTAJAS .....	16
3.3.2.7.	BENEFICIOS .....	16
3.3.2.8.	GARANTÍAS .....	16
3.3.2.9.	FORMA DE PAGO .....	16

## CAPÍTULO 4

4.	IMPLEMENTACIÓN .....	1
4.1.	IMPLEMENTACIÓN LAN .....	1
4.1.1.	DEPARTAMENTO DE CONTABILIDAD MATRIZ.....	1
4.1.2.	LAN SUCURSAL NORTE.....	2
4.2.	IMPLEMENTACIÓN WAN.....	3
4.2.1.	GRAFICO DE RESPALDO MEDIOS MATRIZ SUCURSAL .....	3

4.2.2.	GRAFICO WAN DE COMUNICACIÓN MATRIZ - SUCURSAL NORTE	4
4.2.3.	GRAFICO WAN DE SEGURIDAD MATRIZ – SUCURSALES	5

## CAPÍTULO 5

5.	LINUX	1
5.1.	INTRODUCCIÓN	1
5.2.	¿QUÉ ES LINUX?	1
5.3.	CARACTERÍSTICAS DEL LINUX	1
5.4.	REQUERIMIENTOS DE HARDWARE PARA INSTALACIÓN DE LINUX	2
5.5.	CONFIGURACIÓN DE BIOS EN EL SERVIDOR LINUX	3
5.6.	EMPEZAR INSTALACIÓN DE LINUX FEDORA CORE 3	5
5.7.	CONFIGURACIONES POST DE LINUX FEDORA CORE 3	18
5.8.	INICIANDO CON EL SISTEMA DE MODO GRAFICO	22
5.9.	COMANDOS BÁSICOS LINUX	24
5.10.	CONFIGURACIÓN DE TARJETA DE RED	26
5.10.1.	CONFIGURAR FIREWALL	29
5.11.	SERVIDOR SAMBA	31
5.11.1.	¿QUÉ ES SAMBA O SMB?	31
5.11.2.	CARACTERÍSTICAS	31
5.11.3.	REQUISITOS PARA LEVANTAR UN SERVIDOR SAMBA	32
5.11.4.	CONFIGURACIÓN DE SAMBA	32
5.11.4.1.	CONFIGURACIÓN EN EL CLIENTE	40
5.12.	DNS	47
5.12.1.1.	¿QUÉ ES DNS?	47
5.12.1.2.	ZONAS	48
5.12.1.2.1.1	ZONAS ESTÁNDARES	48
5.12.1.2.1.2	ZONAS PRIMARIAS	48
5.12.1.2.1.3	ZONAS SECUNDARIAS	48
5.12.1.3.	REQUISITOS PARA SU CONFIGURACIÓN	48
5.12.1.4.	CONFIGURACIÓN DEL SERVICIO DNS	49
5.12.1.5.	CONFIGURACIÓN EN EL CLIENTE	57
5.13.	WEB SERVER	61
5.13.1.	¿QUÉ ES WEB SERVER?	61
5.13.2.	REQUISITOS PARA SU CONFIGURACIÓN	61
5.13.3.	CONFIGURACIÓN DEL SERVICIO APACHE	62
5.13.4.	CONFIGURACIÓN EN EL CLIENTE	67
5.14.	SERVIDOR DE CORREO	70
5.14.1.	¿QUÉ ES EL SERVIDOR DE CORREO?	70
5.14.2.	REQUISITOS PARA SU CONFIGURACIÓN	71
5.14.3.	CONFIGURACIÓN DEL SERVIDOR DE CORREO	71
5.14.3.1.	CONFIGURACIÓN EN EL CLIENTE	79
5.15.	PROXY	84
5.15.1.	¿QUÉ ES PROXY?	84
5.15.2.	REQUISITOS PARA SU CONFIGURACIÓN	84
5.15.3.	CONFIGURACIÓN DEL SQUID	85
5.15.3.1.	CONFIGURACIÓN EN EL CLIENTE	96

5.16.	DHCP.....	100
5.16.1.	¿QUÉ ES DHCP? .....	100
5.16.2.	REQUISITOS PARA SU CONFIGURACIÓN .....	101
5.16.3.	CONFIGURACIÓN DE SERVICIO DHCP .....	101
5.16.4.	CONFIGURACIÓN EN EL CLIENTE .....	107
5.17.	FIREWALL .....	111
5.17.1.	¿QUÉ ES FIREWALL?.....	111
5.17.2.	REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR FIREWALL .....	113
5.17.3.	CONFIGURACIÓN DEL FIREWALL .....	113
5.17.4.	BLOQUEAR PING .....	113
5.17.5.	BLOQUEAR TELNET.....	113
5.17.6.	BLOQUEAR FTP.....	114
5.17.7.	CONFIGURACIÓN DEL CLIENTE.....	115
5.17.8.	BLOQUEO DEL PING Y DEL TELNET .....	116

## CAPÍTULO 6

6.	ROUTER .....	1
6.1.	¿QUE ES UN ROUTER? .....	1
6.2.	MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER .....	3
6.2.1.	CABLE DTE Y DCE.....	3
6.2.2.	CABLE UTP.....	4
6.2.3.	CONECTOR RJ – 45.....	4
6.2.4.	PUERTO SERIAL (CONECTOR COM).....	5
6.3.	COMPONENTES DE CONFIGURACIÓN INTERNA DEL ROUTER .....	6
6.3.1.	RAM .....	6
6.3.2.	NVRAM.....	6
6.3.3.	MEMORIA FLASH .....	7
6.3.4.	MEMORIA DE SÓLO LECTURA (ROM) .....	7
6.4.	PARTES EXTERNAS DEL ROUTER.....	7
6.4.1.	INTERFACES .....	7
6.5.	CONEXIÓN A CONSOLA.....	9
6.6.	SISTEMA DE ARRANQUE BOOTSTRAP .....	10
6.7.	ENRUTAMIENTO.....	11
6.7.1.	ENRUTAMIENTO ESTÁTICO .....	11
6.7.2.	ENRUTAMIENTO DINÁMICO .....	12
6.7.2.1.	PROTOCOLOS DE ENRUTAMIENTO .....	12
6.7.2.2.	CLASES DE PROTOCOLOS DE ENRUTAMIENTO.....	12
6.7.3.	TIPOS DE PROTOCOLOS.....	13
6.7.3.1.	EL PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP) .....	13
6.7.3.2.	FUNCIONAMIENTO RIP .....	14
6.7.3.2.1.	VENTAJAS .....	15
6.7.3.2.2.	DESVENTAJAS.....	15
6.7.3.3.	MENSAJES RIP .....	15
6.7.3.3.1.	TIPOS DE MENSAJES RIP.....	15
6.7.3.3.2.	FORMATO DE LOS MENSAJES RIP.....	16

6.7.4.	EL PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY (IGRP)	16
6.7.5.	EL PROTOCOLO EIGRP	16
6.7.6.	EL PROTOCOLO CONOCIDO COMO "PRIMERO LA RUTA MÁS CORTA" (OSPF)	17
6.8.	LISTAS DE CONTROL DE ACCESO	21
6.8.1.	FUNCIONAMIENTO DE LAS ACL	22
6.8.2.	CREACIÓN DE LAS ACL	23
6.8.3.	FUNCIÓN DE LA MÁSCARA WILDCARD EN UNA ACL	23
6.8.4.	TIPOS DE ACL	25
6.8.4.1.	ACL ESTÁNDAR	25
6.8.4.2.	ACL EXTENDIDA	25
6.8.5.	UBICACIÓN DE UNA ACL	26
6.8.6.	PORQUE CREAR UNA ACL	27
6.9.	SWITCH	27
6.9.1.	ENCAPSULAMIENTO	28
6.9.2.	SEGMENTACIÓN	29
6.9.3.	COLISIÓN	30
6.9.4.	VLAN (REDES VIRTUALES)	31
6.9.5.	TIPOS DE VLAN	32
6.9.5.1.	VLAN DE PUERTO CENTRAL	32
6.9.5.2.	VLAN ESTÁTICAS	32
6.9.5.3.	VLAN DINÁMICAS (DVLAN)	33
6.9.5.4.	VLAN POR PUERTO	33
6.10.	ESTABLECER UNA SESIÓN HYPERTERMINAL	36
6.11.	CONEXIONES DE LOS ROUTERS	39
6.12.	COMANDOS BÁSICOS DEL ROUTER	40
6.13.	MODOS DEL ROUTER	41
6.13.1.	MODO USUARIO	41
6.13.2.	MODO PRIVILEGIADO	42
6.13.3.	MODO DE CONFIGURACIÓN INICIAL (SETUP)	42
6.13.4.	MODO DE CONFIGURACIÓN GLOBAL	42
6.13.5.	MODO RXBOOT	43
6.13.6.	DESCRIPCIÓN GENERAL DE LOS MODOS DEL ROUTER	43
6.14.	CONFIGURACIONES GENERAL DE UN ROUTER	43
6.14.1.	MODO DE CONFIGURACIÓN GLOBAL	44
6.14.2.	GUARDAR CAMBIOS EN EL ROUTER	44
6.14.3.	ASIGNAR NOMBRE AL ROUTER "HOSTNAME"	44
6.14.4.	ASIGNAR CONTRASEÑA "PASSWORD"	45
6.14.5.	CONFIGURACIÓN DE INTERFACES	45
6.14.5.1.	INTERFACES SERIALES / ETHERNET	46
6.14.6.	OSPF	47
6.14.7.	REDISTRIBUCIÓN DE RUTAS	48
6.15.	CASO DE ESTUDIO	49
6.16.	CONFIGURACIÓN DE ROUTER DE LOS ALMACENES ESTUARDO SÁNCHEZ	50
6.16.1.	ROUTER MATRIZ	50
6.16.1.1.	ASIGNAR NOMBRE AL ROUTER	50
6.16.1.2.	ASIGNAR CONTRASEÑA	50
6.16.1.3.	ASIGNAR DIRECCIÓN IP AL ROUTER	51

6.16.1.3.1.	ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0 .....	51
6.16.1.3.2.	ASIGNAR DIRECCIÓN IP INTERFAZ SERIAL 1 .....	51
6.16.1.3.3.	ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET .....	52
6.16.1.4.	DECLARAR EL PROTOCOLO OSPF .....	52
6.16.1.5.	ENRUTAMIENTO DE VLAN 10 .....	52
6.16.1.6.	ENRUTAMIENTO DE LA VLAN 20 .....	53
6.16.1.7.	SHOW RUN .....	53
6.16.1.8.	SHOW IP ROUTE .....	55
6.16.1.9.	SHOW INTERFACES .....	56
6.16.1.10.	SWITCH MATRIZ .....	58
6.16.1.11.	CREACIÓN DE UNA VLAN .....	58
6.16.1.12.	SHOW VLAN .....	59
6.16.1.13.	SHOW INTERFACES .....	59
6.16.2.	ROUTER CENTRO .....	65
6.16.2.1.	ASIGNAR NOMBRE AL ROUTER .....	65
6.16.2.2.	ASIGNAR CONTRASEÑA .....	65
6.16.2.3.	ASIGNAR DIRECCIÓN IP AL ROUTER .....	66
6.16.2.3.1.	ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0 .....	66
6.16.2.3.2.	ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 1 .....	66
6.16.2.3.3.	ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET .....	67
6.16.2.4.	ENRUTAMIENTO DE LA VLAN 30 .....	67
6.16.2.5.	SHOW RUN .....	68
6.16.2.6.	SHOW IP ROUTE .....	69
6.16.2.7.	SHOW INTERFACES .....	71
6.16.2.8.	SWITCH CENTRO .....	73
6.16.2.9.	CREACIÓN DE UNA VLAN .....	73
6.16.2.10.	SHOW VLAN .....	73
6.16.2.11.	SHOW INTERFACES .....	74
6.16.3.	ROUTER SUR .....	80
6.16.3.1.	ASIGNAR NOMBRE AL ROUTER .....	80
6.16.3.2.	ASIGNAR CONTRASEÑA .....	80
6.16.3.3.	ASIGNAR DIRECCIÓN IP AL ROUTER .....	81
6.16.3.3.1.	ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0 .....	81
6.16.3.3.2.	ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET .....	81
6.16.3.4.	DECLARAR EL PROTOCOLO OSPF .....	82
6.16.3.5.	ENRUTAMIENTO DE LA VLAN 50 .....	82
6.16.3.6.	SHOW RUN .....	83
6.16.3.7.	SHOW IP ROUTE .....	84
6.16.3.8.	SHOW INTERFACES .....	86
6.16.4.	SWITCH SUR .....	88
6.16.4.1.	CREACIÓN DE UNA VLAN .....	88
6.16.4.2.	SHOW VLAN .....	88
6.17.	ROUTER BAHÍA .....	95
6.17.1.	ASIGNAR NOMBRE AL ROUTER .....	95
6.17.2.	ASIGNAR CONTRASEÑA .....	95
6.17.3.	ASIGNAR DIRECCIÓN IP AL ROUTER .....	96
6.17.3.1.	ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0 .....	96
6.17.3.2.	ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 1 .....	96
6.17.3.3.	ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET .....	97
6.17.4.	DECLARAR EL PROTOCOLO RIP .....	97

6.17.5.	ENRUTAMIENTO DE LA VLAN 70.....	97
6.17.6.	SHOW RUN .....	98
6.17.7.	SHOW IP ROUTE.....	99
6.17.8.	SHOW INTERFACES .....	101
6.17.9.	SWITCH BAHÍA .....	103
6.17.9.1.	CREACIÓN DE UNA VLAN.....	103
6.17.9.2.	SHOW VLAN.....	104
6.17.9.3.	SHOW INTERFACES .....	105
6.18.	ROUTER NORTE .....	110
6.18.1.	ASIGNAR NOMBRE AL ROUTER .....	110
6.18.2.	ASIGNAR CONTRASEÑA.....	111
6.18.3.	ASIGNAR DIRECCIÓN IP AL ROUTER.....	111
6.18.3.1.	ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 1 .....	111
6.18.3.2.	ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET .....	111
6.18.4.	DECLARAR EL PROTOCOLO RIP.....	112
6.18.5.	ENRUTAMIENTO DE LA VLAN 90.....	112
6.18.6.	SHOW RUN .....	113
6.18.7.	SHOW IP ROUTE.....	114
6.18.8.	SHOW INTERFACES .....	116
6.18.9.	SWITCH NORTE.....	118
6.18.9.1.	CREACIÓN DE UNA VLAN.....	118
6.18.9.2.	SHOW VLAN.....	119
6.18.9.3.	SHOW INTERFACES .....	119

## **ANEXO A**

### **A. GLOSARIO GENERAL**

# CONTENIDO DE FIGURAS

## CAPÍTULO 2

Figura 2-1: DISTRIBUCIÓN DE CABLEADO EN MATRIZ.....	9
Figura 2-2: DISTRIBUCIÓN DE CABLEADO EN SUCURSAL CENTRO.....	10
Figura 2-3: DISTRIBUCIÓN DE CABLEADO EN SUCURSAL SUR.....	11
Figura 2-4: DISTRIBUCIÓN DE CABLEADO EN SUCURSAL BAHÍA.....	12
Figura 2-5: SUCURSAL NORTE.....	13
Figura 2-6: MEZANINE EDIFICIO MATRIZ.....	14
Figura 2-7: PRIMER PISO EDIFICIO MATRIZ.....	15
Figura 2-8: SEGUNDO PISO EDIFICIO MATRIZ.....	16
Figura 2-9: TERCER PISO EDIFICIO MATRIZ.....	17
Figura 2-10: CUARTO PISO EDIFICIO MATRIZ.....	18
Figura 2-11: MEZANINE EDIFICIO SUCURSAL CENTRO.....	19
Figura 2-12: PRIMER PISO EDIFICIO SUCURSAL CENTRO.....	20
Figura 2-13: SEGUNDO PISO EDIFICIO SUCURSAL CENTRO.....	21
Figura 2-14: TERCER PISO EDIFICIO SUCURSAL CENTRO.....	22
Figura 2-15: CUARTO PISO EDIFICIO SUCURSAL CENTRO.....	23
Figura 2-16: MEZANINE EDIFICIO SUCURSAL SUR.....	24
Figura 2-17: PRIMER PISO EDIFICIO SUCURSAL SUR.....	25
Figura 2-18: SEGUNDO PISO EDIFICIO SUCURSAL SUR.....	26
Figura 2-19: TERCER PISO EDIFICIO SUCURSAL SUR.....	27
Figura 2-20: CUARTO PISO EDIFICIO SUCURSAL SUR.....	28
Figura 2-21: MEZANINE EDIFICIO SUCURSAL BAHÍA.....	29
Figura 2-22: PRIMER PISO EDIFICIO SUCURSAL BAHÍA.....	30
Figura 2-23: SEGUNDO PISO EDIFICIO SUCURSAL BAHÍA.....	31
Figura 2-24: TERCER PISO EDIFICIO SUCURSAL BAHÍA.....	32
Figura 2-25: CUARTO PISO EDIFICIO SUCURSAL BAHÍA.....	33
Figura 2-26: SUCURSAL NORTE.....	34
Figura 2-27: COMUNICACIÓN WAN A NIVEL DE MEDIOS.....	39
Figura 2-28: COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS.....	40
Figura 2-29: RECEPCIÓN DEL INTERNET EN MATRIZ.....	41

## CAPÍTULO 3

Figura 3-1: PLAN DE TRABAJO ALTERNATIVA 1.....	8
Figura 3-2: PLAN DE TRABAJO ALTERNATIVA 2.....	15

## CAPÍTULO 4

Figura 4-1: DEPARTAMENTO DE CONTABILIDAD MATRIZ.....	1
Figura 4-2: LAN SUCURSAL NORTE.....	2
Figura 4-3: ENLACE DE RESPALDO MATRIZ – SUCURSALES.....	3
Figura 4-4: ENLACE DE COMUNICACIÓN MATRIZ - SUCURSAL NORTE.....	4
Figura 4-5: SEGURIDAD WAN MATRIZ – SUCURSALES.....	5

## CAPÍTULO 5

Figura 5-1: TECLADO .....	3
Figura 5-2: BIOS .....	3
Figura 5-3: ORDEN DE ARRANQUE .....	3
Figura 5-4: UNIDAD DE CD-ROM IDE.....	4
Figura 5-5: GUARDAR CAMBIOS Y SALIR DEL BIOS .....	4
Figura 5-6: INICIANDO BOTELO.....	5
Figura 5-7: DETECTANDO HARDWARE.....	5
Figura 5-8: VERIFICACIÓN DE DISCOS.....	6
Figura 5-9: BIENVENIDO A FEDORA CORE .....	6
Figura 5-10: SELECCIÓN DE LENGUAJE.....	7
Figura 5-11: CONFIGURACIÓN DEL TECLADO.....	7
Figura 5-12: TIPO DE INSTALACIÓN.....	8
Figura 5-13: CONFIGURACIÓN DE PARTICIONAMIENTO DEL DISCO.....	8
Figura 5-14: CONFIGURACIÓN DEL DISCO.....	9
Figura 5-15: AÑADIR PARTICIÓN RAÍZ (/).....	10
Figura 5-16: AÑADIR PARTICIÓN SWAP.....	10
Figura 5-17: PARTICIONES CREADAS EN EL DISCO.....	11
Figura 5-18: CONFIGURACIÓN GESTOR DE ARRANQUE.....	11
Figura 5-19: CONFIGURACIÓN DE LA RED.....	12
Figura 5-20: CONFIGURACIÓN DEL CORTAFUEGO.....	12
Figura 5-21: SOPORTE ADICIONAL DEL IDIOMA.....	13
Figura 5-22: SELECCIÓN DEL HUSO HORARIO.....	13
Figura 5-23: CONFIGURAR CONTRASEÑA DEL ROOT .....	14
Figura 5-24: SELECCIÓN DE GRUPOS PAQUETES.....	14
Figura 5-25: LISTO PARA LA INSTALACIÓN .....	15
Figura 5-26: MEDIOS DE INSTALACIÓN REQUERIDOS.....	15
Figura 5-27: INSERTAR DISCO 2.....	16
Figura 5-28: INSERTAR DISCO 3.....	16
Figura 5-29: INSTALACIÓN COMPLETA.....	17
Figura 5-30: CARGANDO SISTEMA.....	17
Figura 5-31: BIENVENIDO AL SISTEMA .....	18
Figura 5-32: ACUERDO DE LICENCIA.....	18
Figura 5-33: FECHA Y HORA.....	19
Figura 5-34: RESOLUCIÓN DEL MONITOR DE PANTALLA.....	19
Figura 5-35: USUARIO DEL SISTEMA.....	20
Figura 5-36: TARJETA DE SONIDO.....	20
Figura 5-37: FINALIZACIÓN DE CONFIGURACIÓN.....	21
Figura 5-38: INGRESO DE USUARIO.....	22
Figura 5-39: INGRESO DE CONTRASEÑA.....	22
Figura 5-40: ESCRITORIO DE LINUX .....	23
Figura 5-41: INGRESAR AL TERMINAL.....	23
Figura 5-42: TERMINAL.....	24
Figura 5-43: INGRESAR AL TERMINAL.....	26
Figura 5-44: COMANDO NETCONFIG .....	27
Figura 5-45: CONFIGURACIÓN DE RED .....	27
Figura 5-46: CONFIGURAR TCP/IP.....	28
Figura 5-47: INICIAR LOS SERVICIOS .....	28
Figura 5-48: VERIFICACIÓN DE DIRECCIÓN IP.....	29

Figura 5-49: COMANDO SETUP.....	29
Figura 5-50: UTILIDAD DE CONFIGURACIÓN DE MODO GRAFICO.....	30
Figura 5-51: CONFIGURACIÓN DEL CORTAFUEGOS.....	30
Figura 5-52: SAMBA.....	31
Figura 5-53: VERIFICACIÓN DE PAQUETE DE SAMBA.....	32
Figura 5-54: COMANDO SETUP.....	33
Figura 5-55: UTILIDAD DE CONFIGURACIÓN DE MODO TEXTO.....	33
Figura 5-56: HABILITAR SERVICIO SMB.....	34
Figura 5-57: SALIR UTILIDAD DE CONFIGURACIÓN DE MODO TEXTO.....	34
Figura 5-58: INGRESAR AL FICHERO SMB.CONF.....	35
Figura 5-59: EDITAR FICHERO SMB.CONF SECCIÓN [GLOBAL].....	35
Figura 5-60: EDITAR FICHERO SMB.CONF SECCIÓN [SHARE DEFINITIONS].....	36
Figura 5-61: CREAR DIRECTORIO A COMPARTIR.....	37
Figura 5-62: CREAR FICHERO A COMPARTIR.....	37
Figura 5-63: ASIGNAR PERMISO AL FICHERO CREADO.....	38
Figura 5-64: CREAR USUARIO DE SISTEMA.....	38
Figura 5-65: ASIGNAR CONTRASEÑA.....	39
Figura 5-66: CREAR USUARIO SAMBA.....	39
Figura 5-67: INICIAR SERVICIO SAMBA.....	40
Figura 5-68: PROPIEDADES DE MIS SITIOS DE RED.....	40
Figura 5-69: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL.....	41
Figura 5-70: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL.....	41
Figura 5-71: PROPIEDADES DE PROTOCOLO DE INTERNET (TCP/IP).....	42
Figura 5-72: PROPIEDADES DE MI PC.....	42
Figura 5-73: PROPIEDADES DEL SISTEMA – NOMBRE DE EQUIPO.....	43
Figura 5-74: PROPIEDADES DEL SISTEMA – CAMBIAR.....	43
Figura 5-75: CAMBIOS EN EL NOMBRE DE EQUIPO.....	44
Figura 5-76: BIENVENIDO AL GRUPO DE TRABAJO.....	44
Figura 5-77: INICIO – EJECUTAR.....	45
Figura 5-78: BUSCAR AL SERVIDOR POR IP.....	45
Figura 5-79: CONECTARSE AL SERVIDOR.....	46
Figura 5-80: CARPETA COMPARTIDA.....	46
Figura 5-81: DNS.....	47
Figura 5-82: VERIFICAR EL PAQUETE BIND.....	49
Figura 5-83: COMANDO SETUP.....	49
Figura 5-84: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO.....	50
Figura 5-85: HABILITAR EL SERVICIO NAMED.....	50
Figura 5-86: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO ...	51
Figura 5-87: INGRESAR AL FICHERO NAMED.CONF.....	51
Figura 5-88: EDITAR EL FICHERO NAMED.CONF.....	52
Figura 5-89: COPIAR EL FICHERO LOCALHOST.ZONE.....	52
Figura 5-90: VERIFICAR EL FICHERO ALESSA.COM.ZONE.....	53
Figura 5-91: FICHERO ALESSA.COM.ZONE SIN EDITAR.....	54
Figura 5-92: FICHERO ALESSA.COM.ZONE EDITADO.....	54
Figura 5-93: COPIAR FICHERO ALESSA.COM.....	55
Figura 5-94: INICIAR SERVICIO BIND.....	55
Figura 5-95: INGRESAR AL FICHERO RESOLV.CONF.....	56
Figura 5-96: EDITAR FICHERO RESOLV.CONF.....	56
Figura 5-97: HACER PING A LA ZONA CREADA [ WWW.ALESSA.COM ].....	57
Figura 5-98: PROPIEDADES DE MI SITIOS DE RED.....	57

Figura 5-99: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL.....	58
Figura 5-100: PROTOCOLO DE INTERNET PROPIEDADES.....	58
Figura 5-101: PROPIEDADES PROTOCOLO DE INTERNET (TCP/IP).....	59
Figura 5-102: INICIO – EJECUTAR.....	59
Figura 5-103: EJECUTAR.....	60
Figura 5-104: PING AL DOMINIO.....	60
Figura 5-105: WEB SERVER.....	61
Figura 5-106: VERIFICAR PAQUETE HTTPD.....	62
Figura 5-107: COMANDO SETUP.....	62
Figura 5-108: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO.....	63
Figura 5-109: HABILITAR EL SERVICIO HTTPD.....	63
Figura 5-110: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO.....	64
Figura 5-111: EDITAR EL FICHERO HTTPD.CONF.....	64
Figura 5-112: FICHERO HHTTPD.CONF [LISTEN 80].....	65
Figura 5-113: FICHERO HHTTPD.CONF [DOCUMENTROOT].....	65
Figura 5-114: FICHERO HHTTPD.CONF [DIRECTORY INDEX].....	65
Figura 5-115: FICHERO HHTTPD.CONF [NAME VIRTUAL HOST].....	65
Figura 5-116: FICHERO HHTTPD.CONF [VIRTUAL HOST].....	66
Figura 5-117: CREACIÓN DE DIRECTORIO SITIOS _ WEB.....	66
Figura 5-118: INICIAR SERVICIO HTTPD.....	67
Figura 5-119: CLIC EN INTERNET.....	67
Figura 5-120: HERRAMIENTAS - OPCIONES DE INTERNET.....	68
Figura 5-121: OPCIONES DE INTERNET.....	68
Figura 5-122: CONFIGURACIÓN DE LA RED DE ÁREA LOCAL (LAN).....	69
Figura 5-123: CARGANDO EL SITIO [ WWW.ALESSA.COM ].....	69
Figura 5-124: SERVIDOR DE CORREO.....	70
Figura 5-125: VERIFICAR EL PAQUETE SENDMAIL.....	71
Figura 5-126: COMANDO SETUP.....	71
Figura 5-127: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO.....	72
Figura 5-128: HABILITAR SERVICIO DOVECOT.....	72
Figura 5-129: HABILITAR SERVICIO SENDMAIL.....	73
Figura 5-130: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO.....	73
Figura 5-131: INGRESAR AL FICHERO NETWORK.....	74
Figura 5-132: EDITAR EL FICHERO NETWORK.....	74
Figura 5-133: INGRESAR AL FICHERO DOVECOT.CONF.....	75
Figura 5-134: EDITAR FICHERO DOVECOT.CONF [PROTOCOLS].....	75
Figura 5-135: INICIAR SERVICIO DOVECOT.....	76
Figura 5-136: INGRESAR AL FICHERO SENDMAIL.....	76
Figura 5-137: EDITAR FICHERO SENDMAIL [CWLOCALHOST].....	77
Figura 5-138: EDITAR FICHERO SENDMAIL [DAEMONPORTOPTIONS].....	77
Figura 5-139: INICIAR SERVICIO SENDMAIL.....	78
Figura 5-140: VERIFICAR PUERTOS 110 Y 125.....	78
Figura 5-141: ABRIR OUTLOOK EXPRESS.....	79
Figura 5-142: AGREGAR NOMBRE A LA CUENTA.....	79
Figura 5-143: AGREGAR DIRECCIÓN DE CORREO ELECTRONICO.....	80
Figura 5-144: ESPECIFICAR SERVIDOR DE CORREO ENTRANTE Y SALIENTE.....	80
Figura 5-145: INGRESAR USUARIO Y CONTRASEÑA.....	81
Figura 5-146: CREACIÓN DE CUENTA FINALIZADA.....	81
Figura 5-147: BANDEJA DE ENTRADA.....	82

Figura 5-148: ENVIÓ DE CORREO.....	82
Figura 5-149: VERIFICAR MENSAJE ENVIADO .....	83
Figura 5-150: VERIFICACIÓN DE CORREO.....	83
Figura 5-151: VERIFICACIÓN DE CORREO.....	84
Figura 5-152: VERIFICACIÓN DEL PAQUETE SQUID.....	85
Figura 5-153: COMANDO SETUP.....	85
Figura 5-154: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO .....	86
Figura 5-155: HABILITAR SERVICIO SQUID .....	86
Figura 5-156: SALIR UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO.....	87
Figura 5-157: EDITAR EL FICHERO SQUID.CONF .....	87
Figura 5-158: EDITAR FICHERO SQUID.CONF [HTTPORT 8080].....	88
Figura 5-159: EDITAR FICHERO SQUID.CONF [CACHE MEN].....	88
Figura 5-160: EDITAR FICHERO SQUID.CONF [CACHE DIR].....	89
Figura 5-161: EDITAR FICHERO SQUID.CONF [CACHE ACCESS LOG].....	89
Figura 5-162: ESTABLECER LISTA DE ACCESO PARA NUESTRA RED.....	90
Figura 5-163: REGLA DE LISTA DE ACCESO PARA NUESTRA RED .....	90
Figura 5-164: EDITAR FICHERO SQUID.CONF [VISIBLE_HOSTNAME].....	91
Figura 5-165: EDITAR FICHERO SQUID.CONF [AUTH_PARAM].....	91
Figura 5-166: ESTABLECER LISTA DE ACCESO DE AUTENTICACIÓN.....	92
Figura 5-167: REGLA DE LISTA DE ACCESO AUTENTICACIÓN.....	92
Figura 5-168: ESTABLECER LISTA DE ACCESO PARA TIEMPO .....	93
Figura 5-169: REGLA DE LISTA DE ACCESO PARA TIEMPO .....	93
Figura 5-170: INICIANDO SERVICIO SQUID.....	94
Figura 5-171: CREAR FICHERO CLAVES.....	94
Figura 5-172: PERMISO AL FICHERO CLAVES .....	95
Figura 5-173: CAMBIO DE PROPIETARIO FICHERO CLAVES.....	95
Figura 5-174: ASIGNAR CONTRASEÑA.....	96
Figura 5-175: INGRESAR A INTERNET EXPLORER .....	96
Figura 5-176: HERRAMIENTAS - OPCIONES DE INTERNET .....	97
Figura 5-177: OPCIONES DE INTERNET .....	97
Figura 5-178: CONEXIÓN DE RED DE ÁREA LOCAL (LAN).....	98
Figura 5-179: INGRESAR USUARIO Y CONTRASEÑA .....	98
Figura 5-180: PÁGINA WEB CARGADA.....	99
Figura 5-181: DHCP.....	100
Figura 5-182: VERIFICAR PAQUETE DHCP.....	101
Figura 5-183: COMANDO SETUP.....	102
Figura 5-184: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO .....	102
Figura 5-185: HABILITAR SERVICIO DHCPD.....	103
Figura 5-186: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO.....	103
Figura 5-187: COPIAR FICHERO DHCPD.CONF.....	104
Figura 5-188: EDITAR FICHERO DHCPD.CONF.....	104
Figura 5-189: FICHERO DHCPD.CONF .....	105
Figura 5-190: CREAR FICHERO DHCPD.LEASES.....	106
Figura 5-191: AÑADIR DHCP AL ARRANQUE DEL SISTEMA.....	106
Figura 5-192: INICIAR SERVICIO DHCP .....	107
Figura 5-193: MIS SITIOS DE RED - PROPIEDADES.....	107
Figura 5-194: CONEXIÓN DE ÁREA LOCAL - PROPIEDADES.....	108
Figura 5-195: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL.....	108
Figura 5-196: PROPIEDADES DE PROTOCOLO DE INTERNET.....	109
Figura 5-197: INGRESAR A EJECUTAR.....	109

Figura 5-198: EJECUTAR.....	110
Figura 5-199: CONSOLA DOS.....	110
Figura 5-200: FIREWALL .....	111
Figura 5-201: BLOQUEAR PING .....	113
Figura 5-202: BLOQUEAR TELNET.....	113
Figura 5-203: BLOQUEAR FTP.....	114
Figura 5-204: VERIFICACIÓN DE LAS REGLAS DE FIREWALL .....	114
Figura 5-205: EJECUTAR.....	115
Figura 5-206: PING AL SERVIDOR.....	115
Figura 5-207: INGRESAR USUARIO Y CONTRASEÑA.....	115
Figura 5-208: BLOQUEO DEL PING Y DEL TELNET.....	116

## CAPÍTULO 6

Figura 6-1: VISTA POSTERIOR DEL ROUTER .....	1
Figura 6-2: VISTA FRONTAL DEL ROUTER.....	1
Figura 6-3: CABLE DTE Y DCE.....	3
Figura 6-4: CABLE UTP.....	4
Figura 6-5: CONECTOR RJ 45.....	4
Figura 6-6: CONECTOR COM.....	5
Figura 6-7: COMPONENTES DE CONFIGURACIÓN INTERNA DEL ROUTER .....	6
Figura 6-8: INTERFACES DEL ROUTER.....	7
Figura 6-9: INTERFACES LAN .....	8
Figura 6-10: INTERFACES WAN.....	8
Figura 6-11: PUERTO DE CONSOLA.....	9
Figura 6-12: CONFIGURACIÓN DE UNA CONEXIÓN DE CONSOLA .....	10
Figura 6-13: ENRUTAMIENTO ESTÁTICO .....	11
Figura 6-14: RUTAS DINÁMICAS.....	12
Figura 6-15: CLASES DE PROTOCOLO DE ENRUTAMIENTO .....	13
Figura 6-16: PROTOCOLO DE ENRUTAMIENTO RIP .....	14
Figura 6-17: PROTOCOLO DE ENRUTAMIENTO OSPF.....	18
Figura 6-18: LISTAS DE CONTROL DE ACCESO.....	21
Figura 6-19: COMO FUNCIONAN LAS ACL .....	22
Figura 6-20: PROTOCOLOS CON ACL ESPECIFICADAS .....	23
Figura 6-21: BITS DE MASCARA WILDCARD .....	24
Figura 6-22: ACL ESTANDAR .....	25
Figura 6-23: ACL EXTENDIDAS .....	25
Figura 6-24: NÚMERO DE PUERTO COMUNES DE LAS ACL EXTENDIDAS .....	26
Figura 6-25: UBICACIÓN DE LAS ACL .....	26
Figura 6-26: SWITCH .....	27
Figura 6-27: ENCAPSULAMIENTO .....	28
Figura 6-28: VLAN .....	31
Figura 6-29: VLAN DE PUERTO CENTRAL .....	32
Figura 6-30: VLAN ESTÁTICAS.....	32
Figura 6-31: VLAN DINÁMICAS.....	33
Figura 6-32: INGRESAR AL HYPERTERMINAL.....	36
Figura 6-33: NUEVA CONEXIÓN.....	37
Figura 6-34: ELEGIR PUERTO COM.....	37
Figura 6-35: CONFIGURACIÓN DE PUERTO.....	38
Figura 6-36: HYPERTERMINAL.....	38

Figura 6-37: CONEXIONES DE LOS ROUTERS.....	39
Figura 6-38: PUERTO DE CONSOLA.....	39
Figura 6-39: MODOS DEL ROUTER .....	41
Figura 6-40: MODOS DEL USUARIO – MODO PRIVILEGIADO .....	42
Figura 6-41: DESCRIPCIÓN GENERAL DE LOS MODOS DEL ROUTER.....	43
Figura 6-42: CASO DE ESTUDIO .....	49

# CONTENIDO DE TABLAS

## CAPÍTULO 2

Tabla 2-1: DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO EN MATRIZ ....	2
Tabla 2-2 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO DE MATRIZ.....	2
Tabla 2-3: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL CENTRO .....	3
Tabla 2-4 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL CENTRO .....	3
Tabla 2-5: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL SUR.....	3
Tabla 2-6 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL SUR .....	4
Tabla 2-7: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL BAHÍA	4
Tabla 2-8 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL BAHÍA .....	4
Tabla 2-9: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL NORTE	5
Tabla 2-10 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL NORTE .....	5
Tabla 2-11 DISTRIBUCIÓN DE SERVIDORES EN MATRIZ .....	5
Tabla 2-12 CARACTERÍSTICAS DE SERVIDOR DE BASE DE DATOS EN MATRIZ .....	6
Tabla 2-13 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN MATRIZ .....	6
Tabla 2-14 CARACTERÍSTICAS DE SERVIDOR WEB EN MATRIZ.....	6
Tabla 2-15 DISTRIBUCIÓN DE SERVIDORES EN SUCURSAL CENTRO.....	6
Tabla 2-16 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN SUCURSAL CENTRO.....	7
Tabla 2-17 DISTRIBUCIÓN DE SERVIDORES EN SUCURSAL SUR.....	7
Tabla 2-18 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN SUCURSAL SUR.....	7
Tabla 2-19 DISTRIBUCIÓN DE SERVIDORES EN SUCURSAL BAHÍA .....	7
Tabla 2-20 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN SUCURSAL BAHÍA .....	8
Tabla 2-21: DISPOSITIVOS DE CONMUTACIÓN EN MATRIZ .....	35
Tabla 2-22: DISPOSITIVOS DE CONMUTACIÓN EN SUCURSAL CENTRO .....	35
Tabla 2-23: DISPOSITIVOS DE CONMUTACIÓN EN SUCURSAL CENTRO .....	36
Tabla 2-24: DISPOSITIVOS DE CONMUTACIÓN EN SUCURSAL BAHÍA.....	36
Tabla 2-25: MEDIO INALÁMBRICO MATRIZ – SUCURSAL CENTRO .....	36
Tabla 2-26: MEDIO INALÁMBRICO MATRIZ – SUCURSAL SUR.....	37
Tabla 2-27: MEDIO INALÁMBRICO MATRIZ – SUCURSAL BAHÍA.....	37
Tabla 2-28: DISPOSITIVOS DE ENRUTAMIENTO MATRIZ – SUCURSAL CENTRO .....	37
Tabla 2-29: DISPOSITIVOS DE ENRUTAMIENTO MATRIZ – SUCURSAL SUR.	38
Tabla 2-30: DISPOSITIVOS DE ENRUTAMIENTO MATRIZ – SUCURSAL BAHÍA .....	38

### **CAPÍTULO 3**

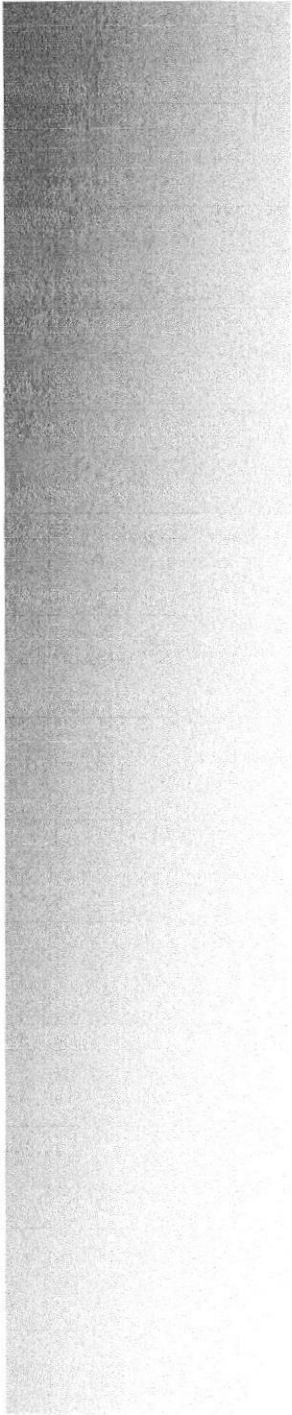
Tabla 3-1: PROBLEMA ENCONTRADOS .....	1
Tabla 3-2: SOLUCIÓN PROPUESTA.....	2
Tabla 3-3: FACTIBILIDAD TÉCNICA ALTERNATIVA 1 .....	4
Tabla 3-4: FACTIBILIDAD OPERATIVA ALTERNATIVA 1 .....	5
Tabla 3-5: COSTOS DE HARDWARE ALTERNATIVA 1.....	7
Tabla 3-6: COSTOS OPERATIVOS ALTERNATIVA 1 .....	7
Tabla 3-7: COSTOS DE LA FACTIBILIDAD DE LA ALTERNATIVA 1 .....	7
Tabla 3-8: FACTIBILIDAD TÉCNICA ALTERNATIVA 2 .....	11
Tabla 3-9: FACTIBILIDAD OPERATIVA ALTERNATIVA 2.....	12
Tabla 3-10: COSTOS DE HARDWARE ALTERNATIVA 2.....	14
Tabla 3-11: COSTOS OPERATIVOS ALTERNATIVA 2 .....	14
Tabla 3-12: COSTOS DE FACTIBILIDAD DE LA ALTERNATIVA 2 .....	14

### **CAPÍTULO 5**

Tabla 5-1 COMANDOS BÁSICOS DE LINUX .....	26
---	----

### **CAPÍTULO 6**

Tabla 6-1: COMANDOS BÁSICOS DEL ROUTER .....	41
--	----



# CAPÍTULO 1 GENERALIDADES

# **1. GENERALIDADES**

## **1.1. INTRODUCCIÓN**

En este tópic de graduación, hemos realizado un estudio completo de las comunicaciones LAN y WAN de los Almacenes Estuardo Sánchez, y en este manual lo explicamos paso a paso.

- ✓ El primer capítulo tenemos las generalidades de este manual.
- ✓ En el segundo capítulo encontramos la situación actual de la empresa.
- ✓ En el tercer capítulo damos soluciones a los problemas encontrados.
- ✓ En el cuarto capítulo encontramos la implementación LAN y WAN que vamos a realizar.
- ✓ En el quinto capítulo podemos encontrar la instalación y configuración del sistema operativo Linux fedora core 3.
- ✓ En el sexto capítulo mostramos la configuración en los dispositivos de ruteo y conmutación.

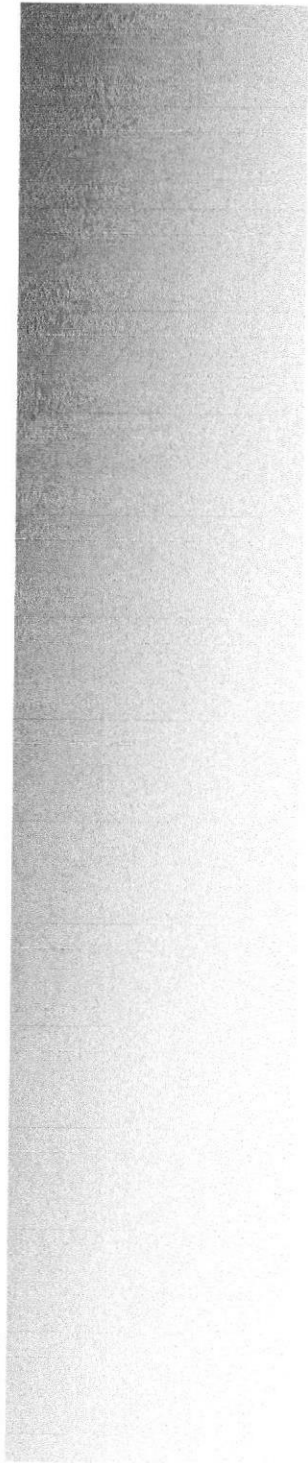
## **1.2. OBJETIVO DE ESTE MANUAL.**

El objetivo de este manual es guiar a los usuarios interesados en el manejo y administración de redes.

- ✓ Conocer la realización de un estudio de cableado estructurado.
- ✓ Conocer las configuraciones realizadas a los dispositivos.
- ✓ Conocer sistema operativo Linux

## **1.3. A QUIÉN VA DIRIGIDO.**

Este manual esta dirigido a las personas involucradas o que quieran conocer acerca del estudio de las redes LAN, WAN y sistema operativo Linux aplicados a la empresa ALESSA.



## CAPÍTULO 2

### SITUACIÓN ACTUAL

## 2. SITUACIÓN ACTUAL

### 2.1. ANTECEDENTES

Hablar de la trayectoria de Almacenes Estuardo Sánchez, es reconocer en su principal Gestor, el Sr. Estuardo Sánchez García, una vida llena de trabajo y esfuerzo constante y quien por más de 50 años, ha llevado esta empresa a un sitial digno de admiración, como así lo han reconocido varias Instituciones tanto públicas como privadas.

Es una empresa familiar, que inició su gestor un 20 de Diciembre de 1950, en un local del Mercado Central y luego, mediante el esfuerzo diario, lleno de sacrificio, constancia y perseverancia, se traslada a su primer edificio propio ubicado en las calles 10 de agosto y 6 de marzo.

En la actualidad, atiende personalmente a su clientela, en un moderno edificio ubicado en las calles Sucre y Lorenzo de Garaycoa, como casa matriz y una sucursal en el sector de la bahía de Guayaquil, en Eloy Alfaro 324 y Av. Olmedo

Estuardo Sánchez García, sostiene que todo lo logrado hasta el momento no es más que el reflejo de mucho trabajo y buena voluntad, además de la creencia de que no hay días malos, sino difíciles, filosofía que lo ha impulsado.

### 2.2. MISIÓN

Servir a nuestros clientes mediante la importación y venta de la mayor gama de productos con niveles de calidad y precios adecuados, apoyando de esta manera el Desarrollo Económico y Social del Ecuador, y brindando a la vez puestos de trabajo con remuneraciones justas para nuestros colaboradores y la máxima rentabilidad en beneficio de nuestros accionistas.

### 2.3. VISIÓN

Obtener, mediante la continua evaluación del mercado y de la competencia, el más alto nivel de surtido de productos para nuestros clientes, convirtiéndonos en la empresa líder en importaciones de Artículos de Bazar, Juguetes, Navideños y Ferretería.



## 2.4. INFRAESTRUCTURA LAN

### 2.4.1. ESTACIONES DE TRABAJO

#### 2.4.1.1. MATRIZ


La matriz es un edificio de cinco pisos que se encuentra ubicado en la ciudad de Guayaquil en las calles seis de marzo y Lorenzo de Garaycoa el medio de conexión que utilizan para el Backbone Horizontal es cable UTP categoría 6 con velocidad de transmisión 10/100/1000 Mbps poseen 47 estaciones de trabajo distribuidas de la siguiente manera.

##### 2.4.1.1.1. DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO EDIFICIO MATRIZ

CANTIDAD	UBICACIÓN	DESCRIPCIÓN
28	Ventas	<b>IBM PENTIUM IV</b>
4	Gerencia de Ventas	
3	Gerencia General	
1	Secretaria de Gerencia	
1	Recepción	
5	Sistemas	
5	Contabilidad	

**Tabla 2-1: DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO EN MATRIZ**

##### 2.4.1.1.2. CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE MATRIZ

	CARACTERÍSTICAS
	Procesador 3,0 GHZ
	Memoria RAM 256 MB
	Disco Duro 80GB
	Tarjeta de red 10/100/1000 MBPS

**Tabla 2-2 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO DE MATRIZ**

#### 2.4.1.2. SUCURSAL CENTRO

La sucursal centro es un edificio de cuatro pisos, se encuentra ubicada en la ciudad de Guayaquil en las calles Córdova y Aguirre el medio de conexión que utilizan para el Backbone Horizontal es cable UTP categoría 6 con velocidad de transmisión 10/100/1000 poseen 15 estaciones de trabajo distribuidas de la siguiente manera.

### 2.4.1.2.1. DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL CENTRO

CANTIDAD	UBICACIÓN	DESCRIPCIÓN
7	Ventas	<b>IBM PENTIUM IV</b>
1	Gerencia de Ventas	
1	Gerencia General	
1	Secretaria de Gerencia	
1	Recepción	
2	Sistemas	
2	Contabilidad	

Tabla 2-3: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL CENTRO

### 2.4.1.2.2. CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL CENTRO


	CARACTERÍSTICAS
	Procesador 3,0 GHZ
	Memoria RAM 256 MB
	Disco Duro 80GB
	Tarjeta de red 10/100/1000 MBPS

Tabla 2-4 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL CENTRO

### 2.4.1.3. EDIFICIO SUR

La sucursal centro es un edificio de cuatro pisos, se encuentra ubicada en la ciudad de Guayaquil en las calles García Goyena y seis de Marzo el medio de conexión que utilizan para el Backbone Horizontal es cable UTP categoría 6 con velocidad de transmisión 10/100/1000 poseen 16 estaciones de trabajo distribuidas de la siguiente manera.

#### 2.4.1.3.1. DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL SUR

CANTIDAD	UBICACIÓN	DESCRIPCIÓN
6	Ventas	<b>IBM PENTIUM IV</b>
1	Gerencia de Ventas	
1	Gerencia General	
1	Secretaria de Gerencia	
1	Recepción	
2	Sistemas	
3	Contabilidad	

Tabla 2-5: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL SUR

### 2.4.1.3.2. CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL SUR


	CARACTERÍSTICAS	
	Procesador	3,0 GHZ
	Memoria RAM	256 MB
	Disco Duro	80GB
	Tarjeta de red	10/100/1000 MBPS

Tabla 2-6 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL SUR



### 2.4.1.4. EDIFICIO BAHÍA

La sucursal centro es un edificio de cuatro pisos, se encuentra ubicada en la ciudad de Guayaquil en las calles Eloy Alfaro y Olmedo el medio de conexión que utilizan para el Backbone Horizontal es cable UTP categoría 6 con velocidad de transmisión 10/100/1000 poseen 16 estaciones de trabajo distribuidas de la siguiente manera.

#### 2.4.1.4.1. DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL BAHÍA

CANTIDAD	UBICACIÓN	DESCRIPCIÓN
6	Ventas	<b>IBM PENTIUM IV</b>
1	Gerencia de Ventas	
1	Gerencia General	
1	Secretaria de Gerencia	
1	Recepción	
2	Sistemas	
3	Contabilidad	

Tabla 2-7: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL BAHÍA

#### 2.4.1.4.2. CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL BAHÍA


	CARACTERÍSTICAS	
	Procesador	3,0 GHZ
	Memoria RAM	256 MB
	Disco Duro	80GB
	Tarjeta de red	10/100/1000 MBPS

Tabla 2-8 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL BAHÍA

### 2.4.1.5. EDIFICIO NORTE

La sucursal Norte es un edificio de un piso, se encuentra ubicada en la ciudad de Guayaquil en la ciudadela Alborada décima etapa no poseen ningún tipo de cableado de red y no se encuentra conectada a la matriz, tiene 2 estaciones de trabajo.

#### 2.4.1.5.1. DISTRIBUCIÓN DE LAS ESTACIONES DE TRABAJO SUCURSAL NORTE

CANTIDAD	UBICACIÓN	DESCRIPCIÓN
1	Ventas	CLON
1	Bodega	

Tabla 2-9: DISTRIBUCIÓN DE ESTACIONES DE TRABAJO SUCURSAL NORTE

#### 2.4.1.5.2. CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO DE SUCURSAL NORTE


	CARACTERÍSTICAS
	Procesador 2,8 GHZ
	Memoria RAM 256 MB
	Disco Duro 120GB
	Tarjeta de red 10/100/1000 MBPS

Tabla 2-10 CARACTERÍSTICAS DE ESTACIONES DE TRABAJO SUCURSAL NORTE

## 2.4.2. SERVIDORES

### 2.4.2.1. MATRIZ

#### 2.4.2.1.1. DISTRIBUCIÓN DE LOS SERVIDORES EN MATRIZ

CANTIDAD	DESCRIPCIÓN	UBICACIÓN
1	Clon – Base de datos	SISTEMAS
1	IBM – Aplicaciones	
1	IBM – WEB	

Tabla 2-11 DISTRIBUCIÓN DE SERVIDORES EN MATRIZ

## 2.4.2.1.2. CARACTERÍSTICAS DE SERVIDORES EN MATRIZ

## SERVIDOR DE BASE DE DATOS

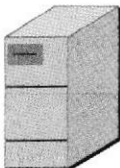
	CARACTERÍSTICAS	
	Procesador	2,5 GHZ
	Memoria RAM	4 GB
	4 Disco Duro	40 GB
	Tarjeta de red 10/100/1000 MBPS	

Tabla 2-12 CARACTERÍSTICAS DE SERVIDOR DE BASE DE DATOS EN MATRIZ

## SERVIDOR DE APLICACIONES

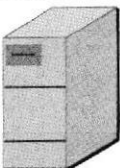
	CARACTERÍSTICAS	
	Procesador	1,3 GHZ
	Memoria RAM	3 GB
	3 Disco Duro	40 GB
	Tarjeta de red 10/100/1000 MBPS	

Tabla 2-13 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN MATRIZ



## SERVIDOR WEB

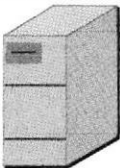
	CARACTERÍSTICAS	
	Procesador	1,3 GHZ
	Memoria RAM	256 MB
	3 Disco Duro	40 GB
	Tarjeta de red 10/100/1000 MBPS	

Tabla 2-14 CARACTERÍSTICAS DE SERVIDOR WEB EN MATRIZ

## 2.4.2.2. SUCURSAL CENTRO

## 2.4.2.2.1. DISTRIBUCIÓN DE LOS SERVIDORES SUCURSAL CENTRO

CANTIDAD	DESCRIPCIÓN	UBICACIÓN
1	IBM – Aplicaciones	SISTEMAS

Tabla 2-15 DISTRIBUCIÓN DE SERVIDORES EN SUCURSAL CENTRO

2.4.2.2. CARACTERÍSTICAS DE SERVIDORES EN SUCURSAL CENTRO

SERVIDOR DE APLICACIONES

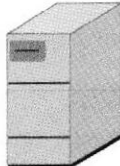
	CARACTERÍSTICAS	
	Procesador	1,3 GHZ
	Memoria RAM	3 GB
	3 Disco Duro	40 GB
	Tarjeta de red 10/100/1000 MBPS	

Tabla 2-16 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN SUCURSAL CENTRO

2.4.2.3. SUCURSAL SUR

2.4.2.3.1. DISTRIBUCIÓN DE LOS SERVIDORES SUCURSAL SUR

CANTIDAD	DESCRIPCIÓN	UBICACIÓN
1	IBM – Aplicaciones	SISTEMAS

Tabla 2-17 DISTRIBUCIÓN DE SERVIDORES EN SUCURSAL SUR

2.4.2.3.2. CARACTERÍSTICAS DE SERVIDORES EN SUCURSAL SUR

SERVIDOR DE APLICACIONES

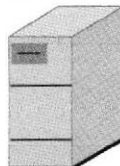
	CARACTERÍSTICAS	
	Procesador	1,3 GHZ
	Memoria RAM	3 GB
	3 Disco Duro	40 GB
	Tarjeta de red 10/100/1000 MBPS	

Tabla 2-18 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN SUCURSAL SUR

2.4.2.4. SUCURSAL BAHÍA

2.4.2.4.1. DISTRIBUCIÓN DE LOS SERVIDORES SUCURSAL BAHÍA

CANTIDAD	DESCRIPCIÓN	UBICACIÓN
1	IBM – Aplicaciones	SISTEMAS

Tabla 2-19 DISTRIBUCIÓN DE SERVIDORES EN SUCURSAL BAHÍA

### 2.4.2.4.2. CARACTERÍSTICAS DE SERVIDORES EN SUCURSAL BAHÍA

#### SERVIDOR DE APLICACIONES

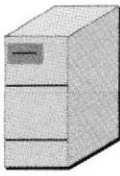
	CARACTERÍSTICAS	
	Procesador	1,3 GHZ
	Memoria RAM	3 GB
	3 Disco Duro	40 GB
	Tarjeta de red	10/100/1000 MBPS

Tabla 2-20 CARACTERÍSTICAS DE SERVIDOR DE APLICACIONES EN SUCURSAL BAHÍA



## 2.4.3. DISTRIBUCIÓN DE CABLEADO

### 2.4.3.1. MATRIZ

Matriz cuenta con cableado de categoría 6, en su backbone horizontal y vertical y una conexión inalámbrica por vía microonda.

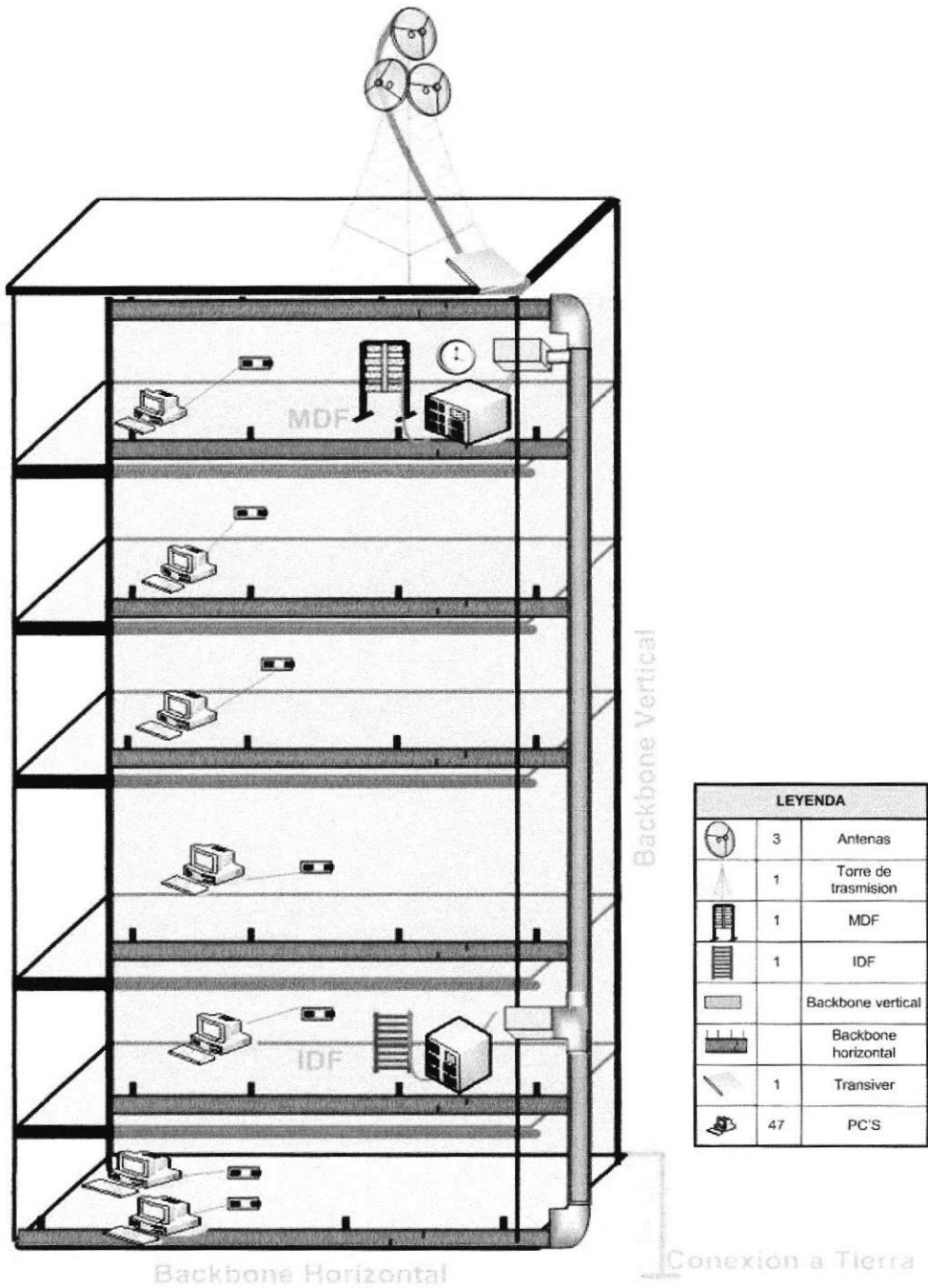


Figura 2-1: DISTRIBUCIÓN DE CABLEADO EN MATRIZ

### 2.4.3.2. SUCURSAL CENTRO

La sucursal centro cuenta con cableado de categoría 6, en su backbone horizontal y vertical y una conexión inalámbrica por vía microonda.

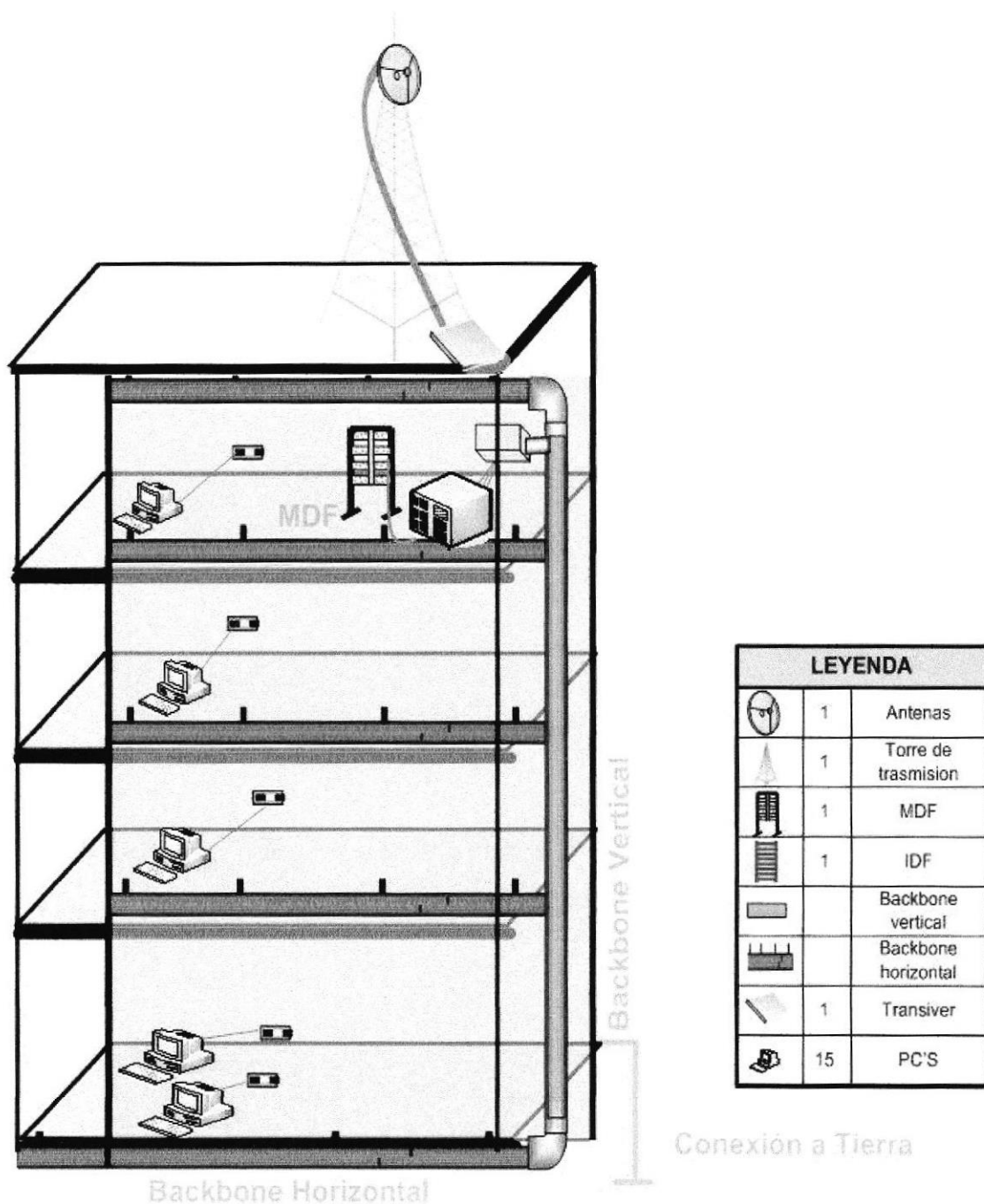


Figura 2-2: DISTRIBUCIÓN DE CABLEADO EN SUCURSAL CENTRO

## 2.4.3.3. SUCURSAL SUR

La sucursal sur cuenta con cableado de categoría 6, en su backbone horizontal y vertical y una conexión inalámbrica por vía microonda.

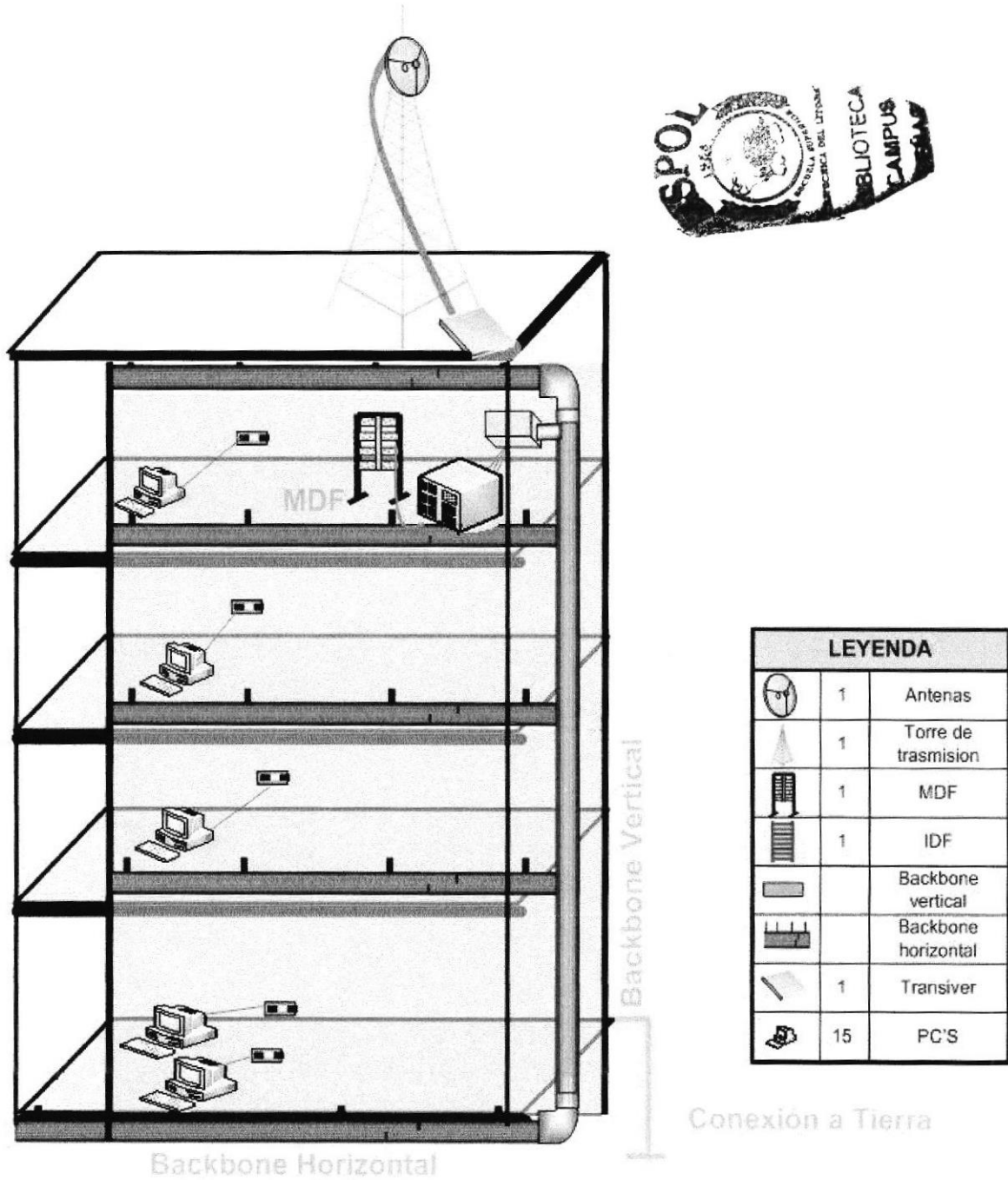


Figura 2-3: DISTRIBUCIÓN DE CABLEADO EN SUCURSAL SUR

#### 2.4.3.4. SUCURSAL BAHÍA

La sucursal Bahía cuenta con cableado de categoría 6, en su backbone horizontal y vertical y una conexión inalámbrica por vía microonda.

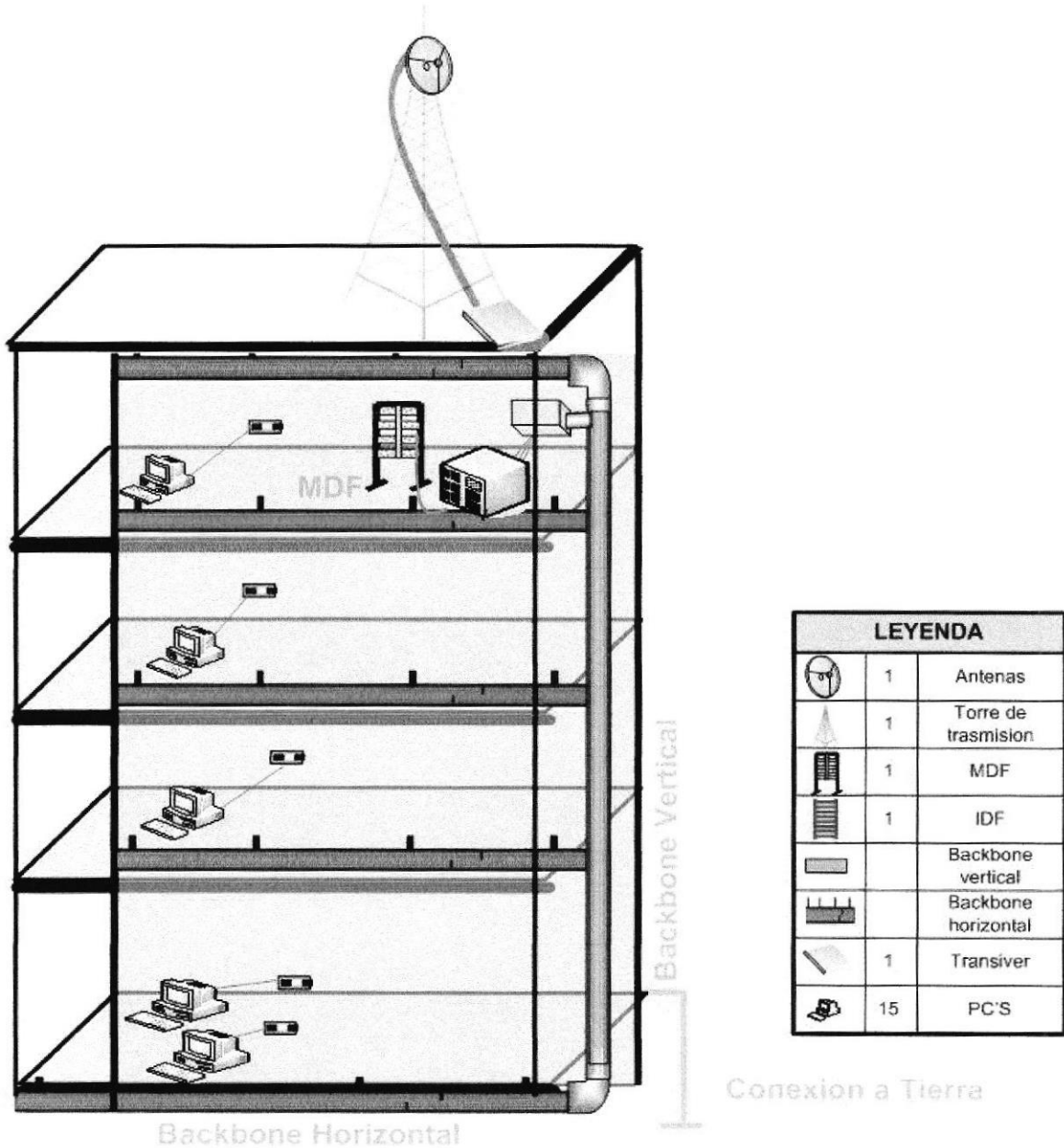


Figura 2-4: DISTRIBUCIÓN DE CABLEADO EN SUCURSAL BAHÍA

### 2.4.3.5. SUCURSAL NORTE

La sucursal Bahía no cuenta con ningún tipo de cableado de red.

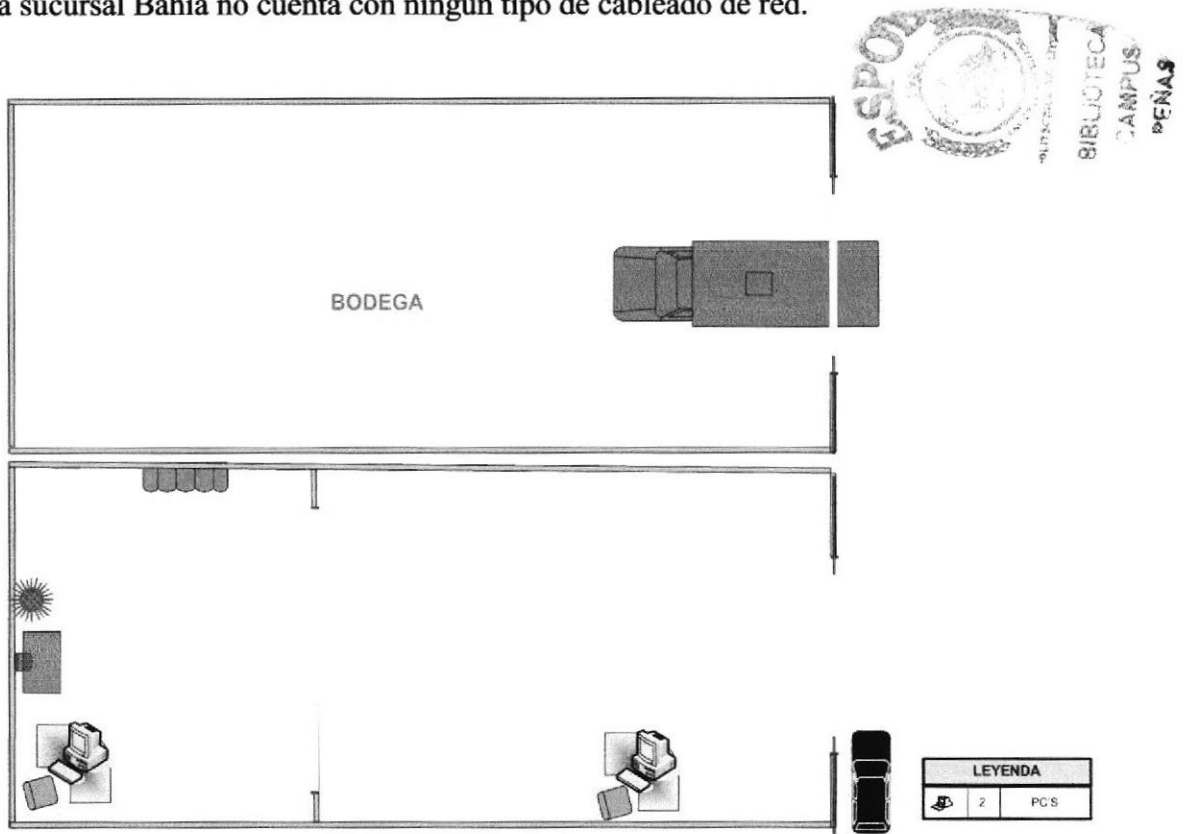


Figura 2-5: SUCURSAL NORTE

### 2.4.4. ANÁLISIS DE PISO

#### 2.4.4.1. MEZANINE EDIFICIO MATRIZ

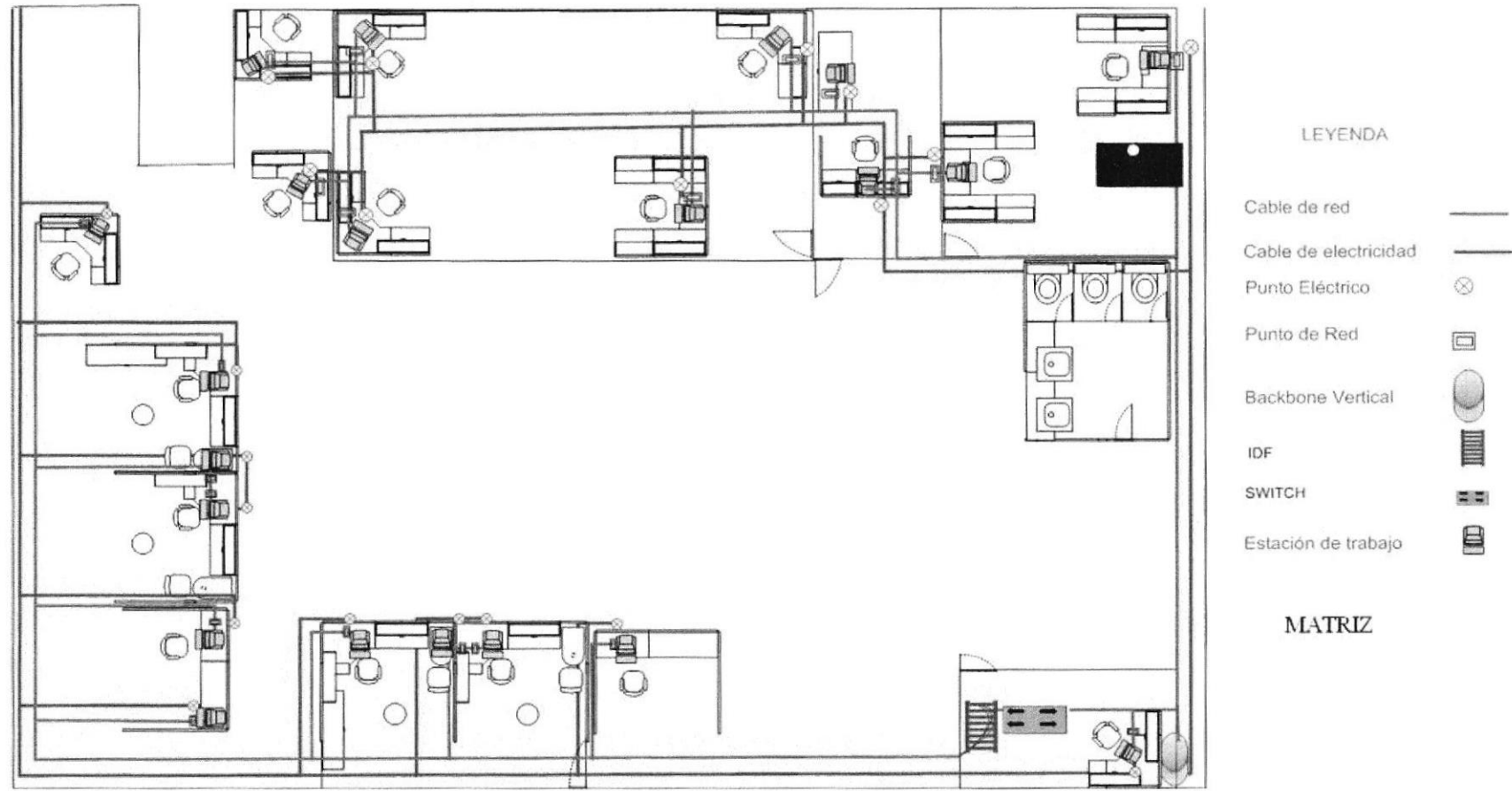


Figura 2-6: MEZANINE EDIFICIO MATRIZ

### 2.4.4.2. PRIMER PISO EDIFICIO MATRIZ

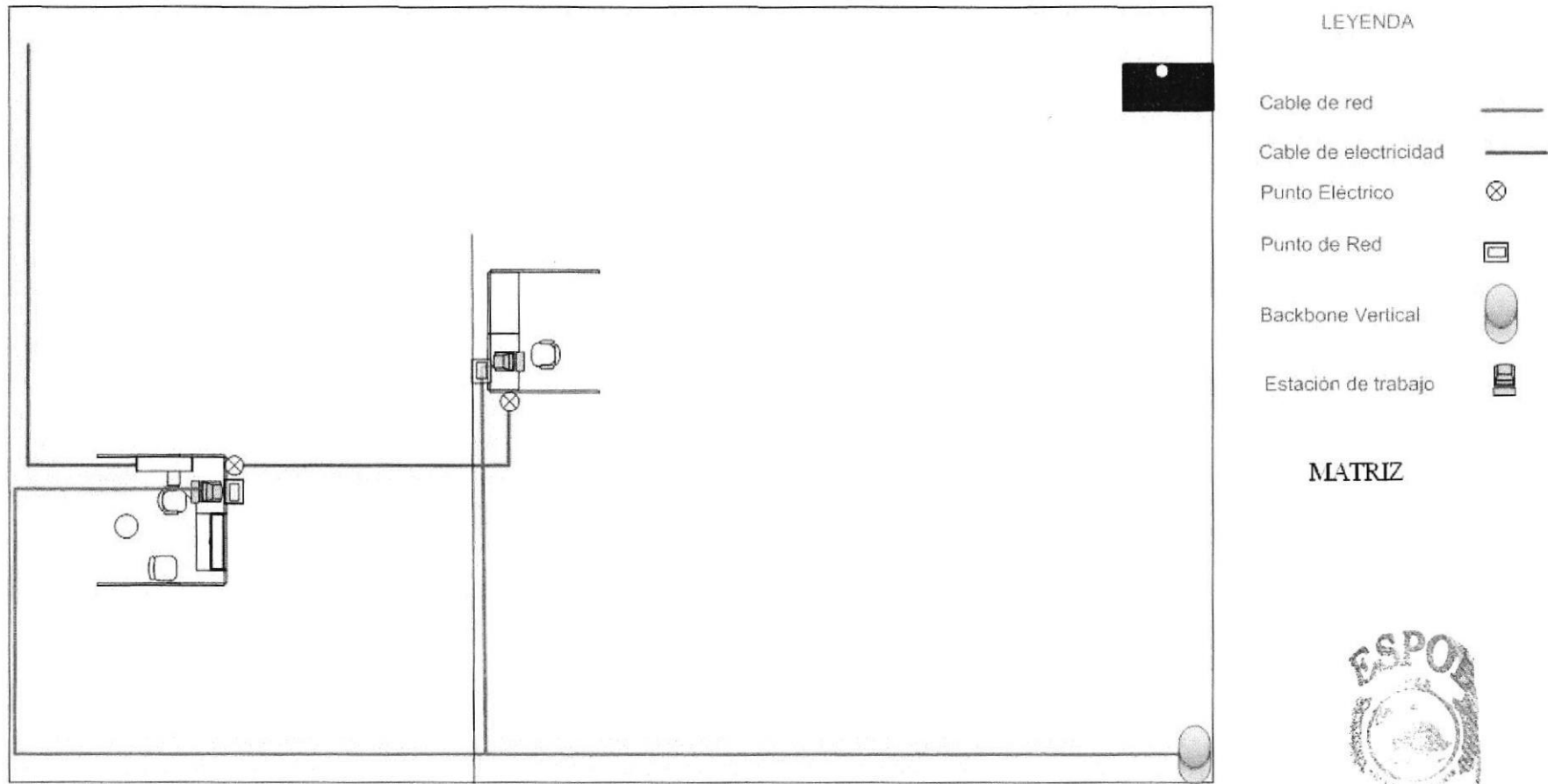


Figura 2-7: PRIMER PISO EDIFICIO MATRIZ

### 2.4.4.3. SEGUNDO PISO EDIFICIO MATRIZ

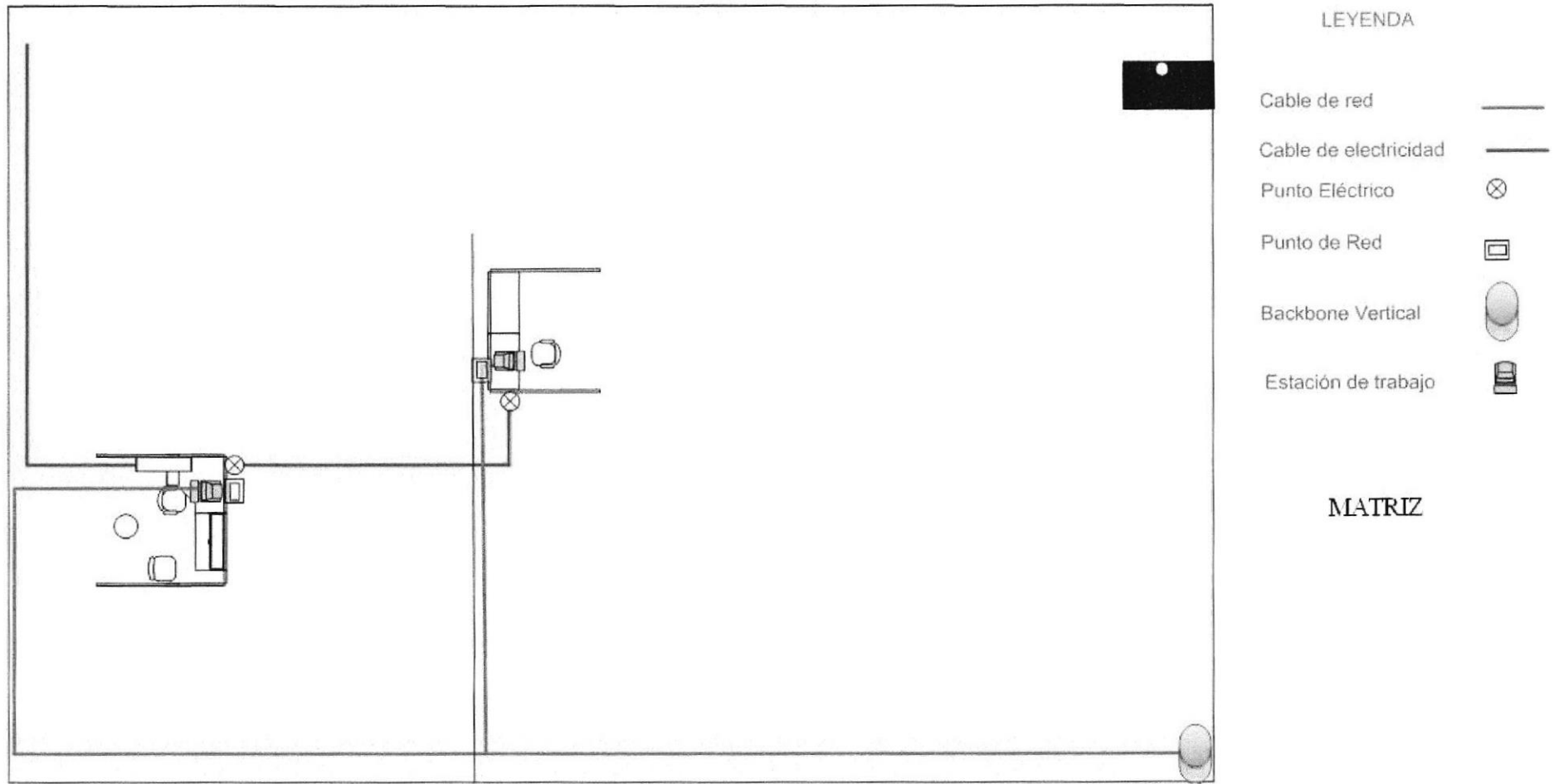


Figura 2-8: SEGUNDO PISO EDIFICIO MATRIZ

### 2.4.4.4. TERCER PISO EDIFICIO MATRIZ

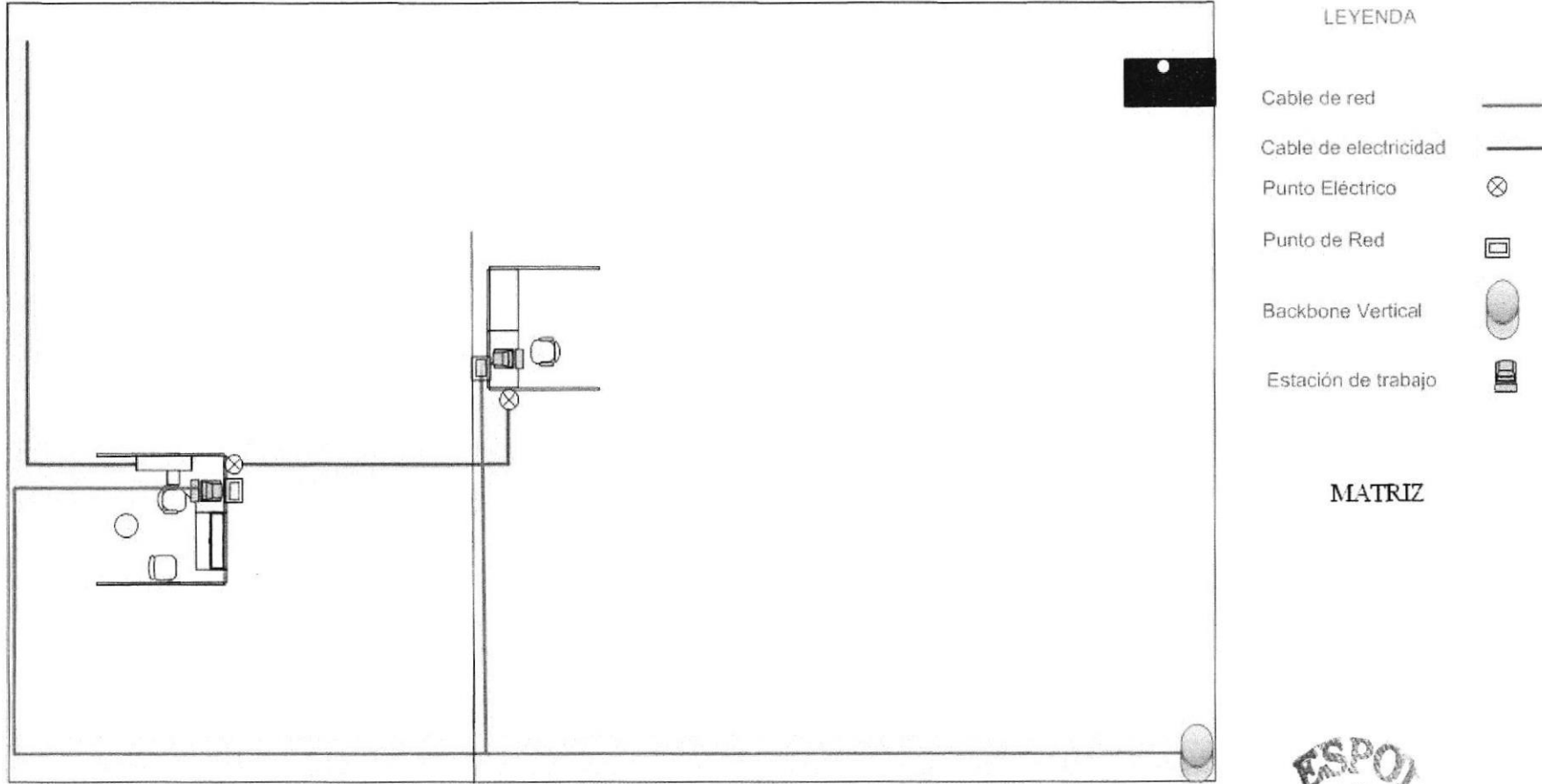


Figura 2-9: TERCER PISO EDIFICIO MATRIZ



### 2.4.4.5. CUARTO PISO EDIFICIO MATRIZ

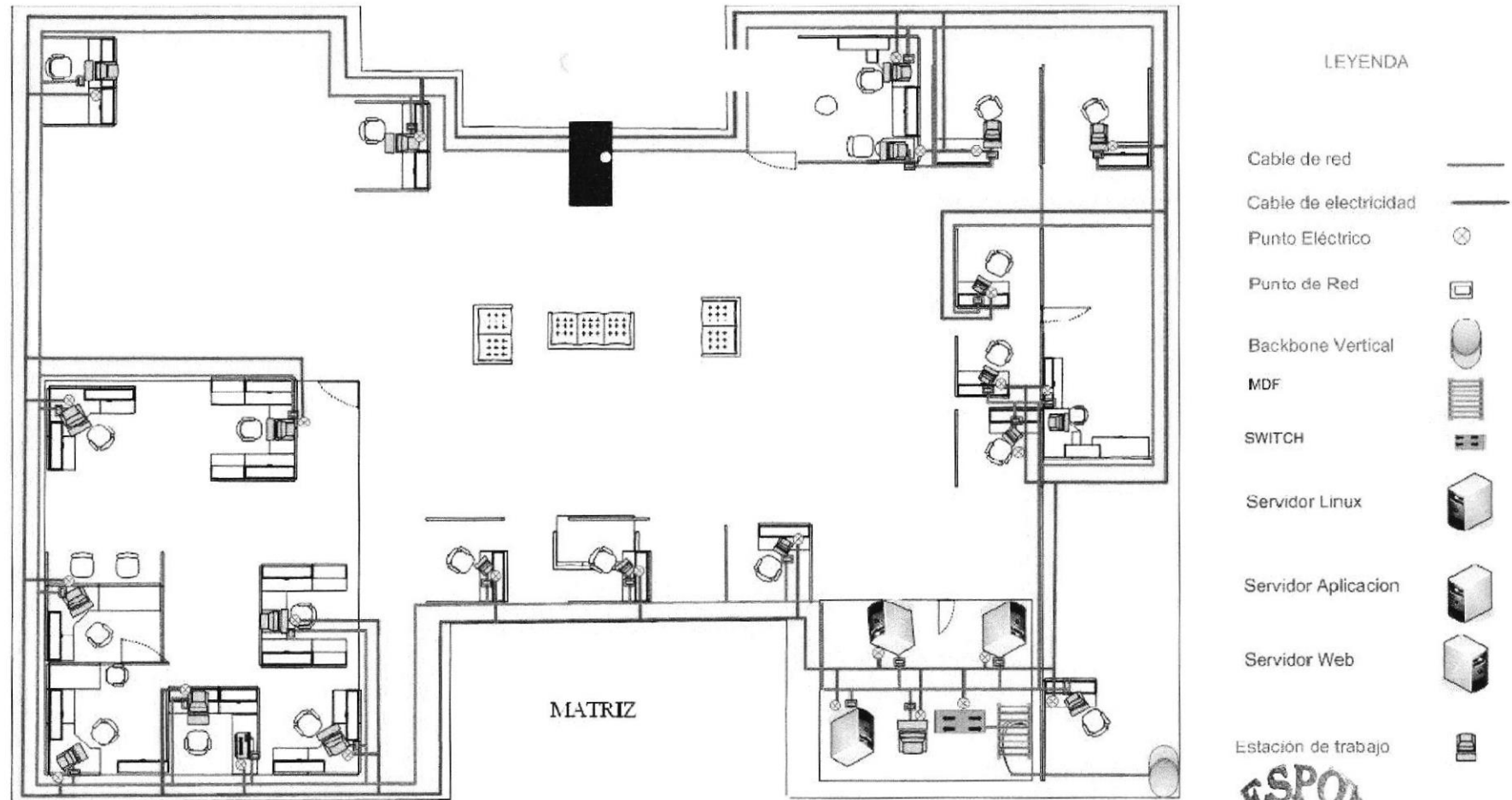


Figura 2-10: CUARTO PISO EDIFICIO MATRIZ



### 2.4.4.6. MEZANINE EDIFICIO CENTRO

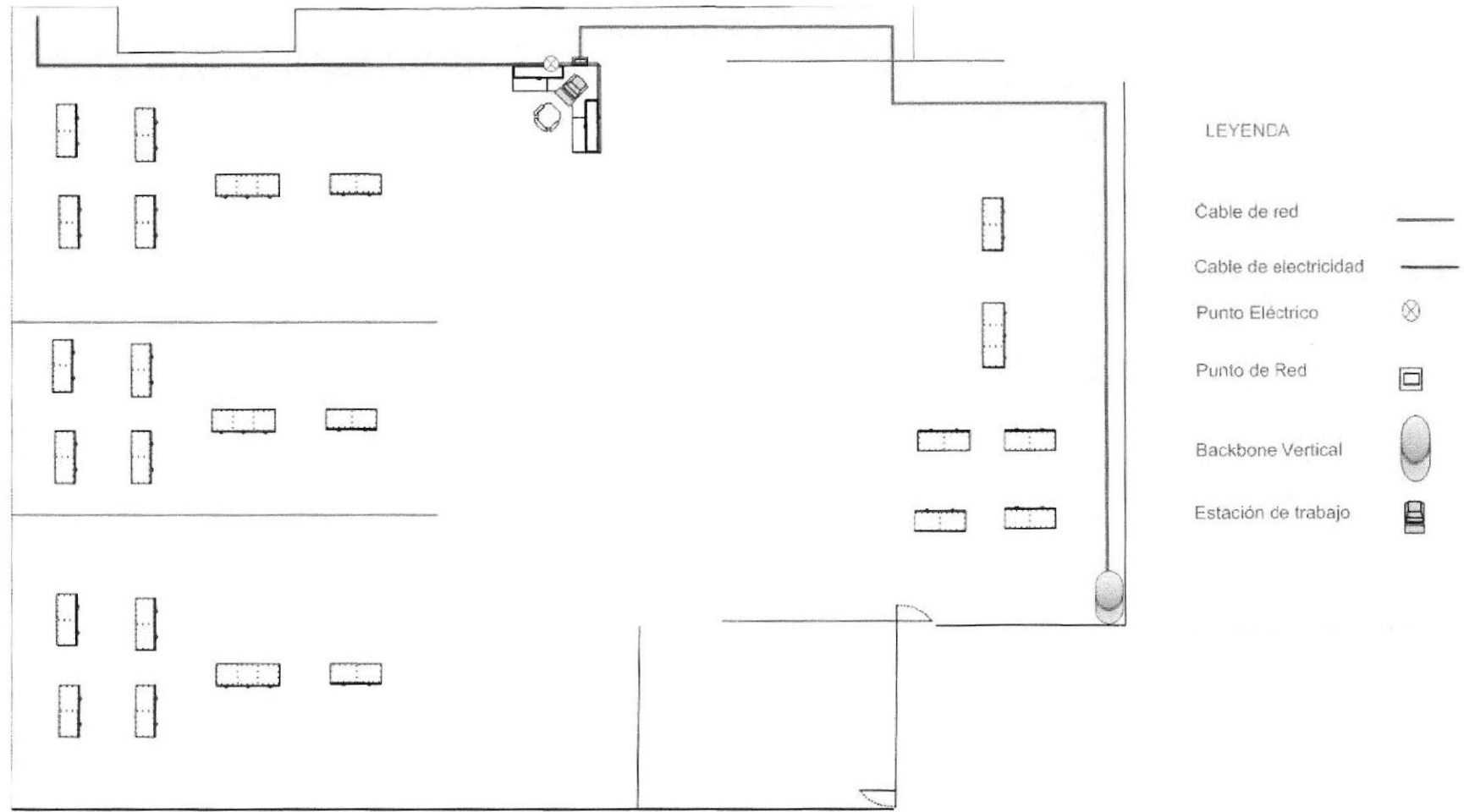


Figura 2-11: MEZANINE EDIFICIO SUCURSAL CENTRO

### 2.4.4.7. PRIMER PISO EDIFICIO CENTRO

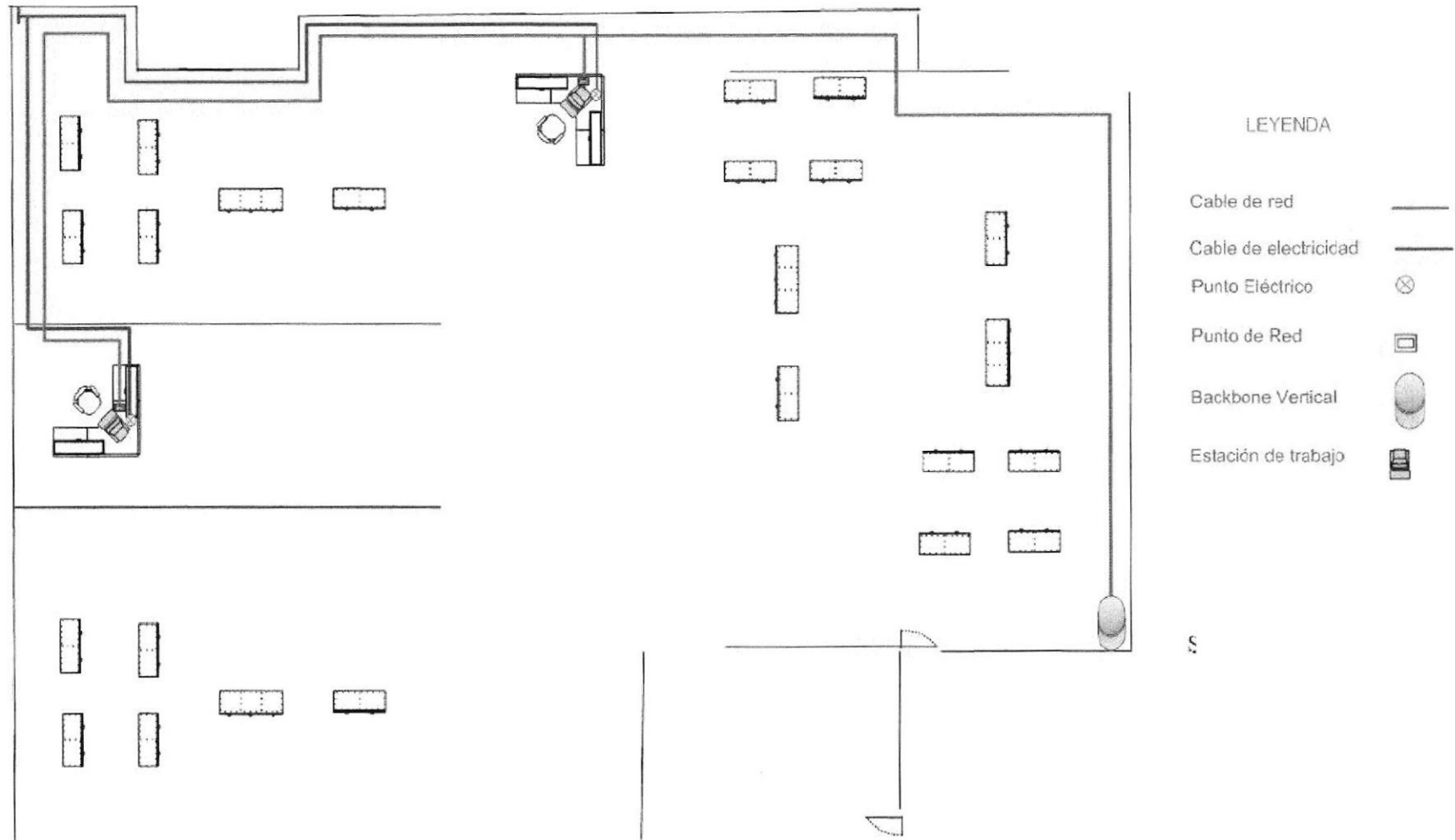


Figura 2-12: PRIMER PISO EDIFICIO SUCURSAL CENTRO

### 2.4.4.8. SEGUNDO PISO EDIFICIO CENTRO

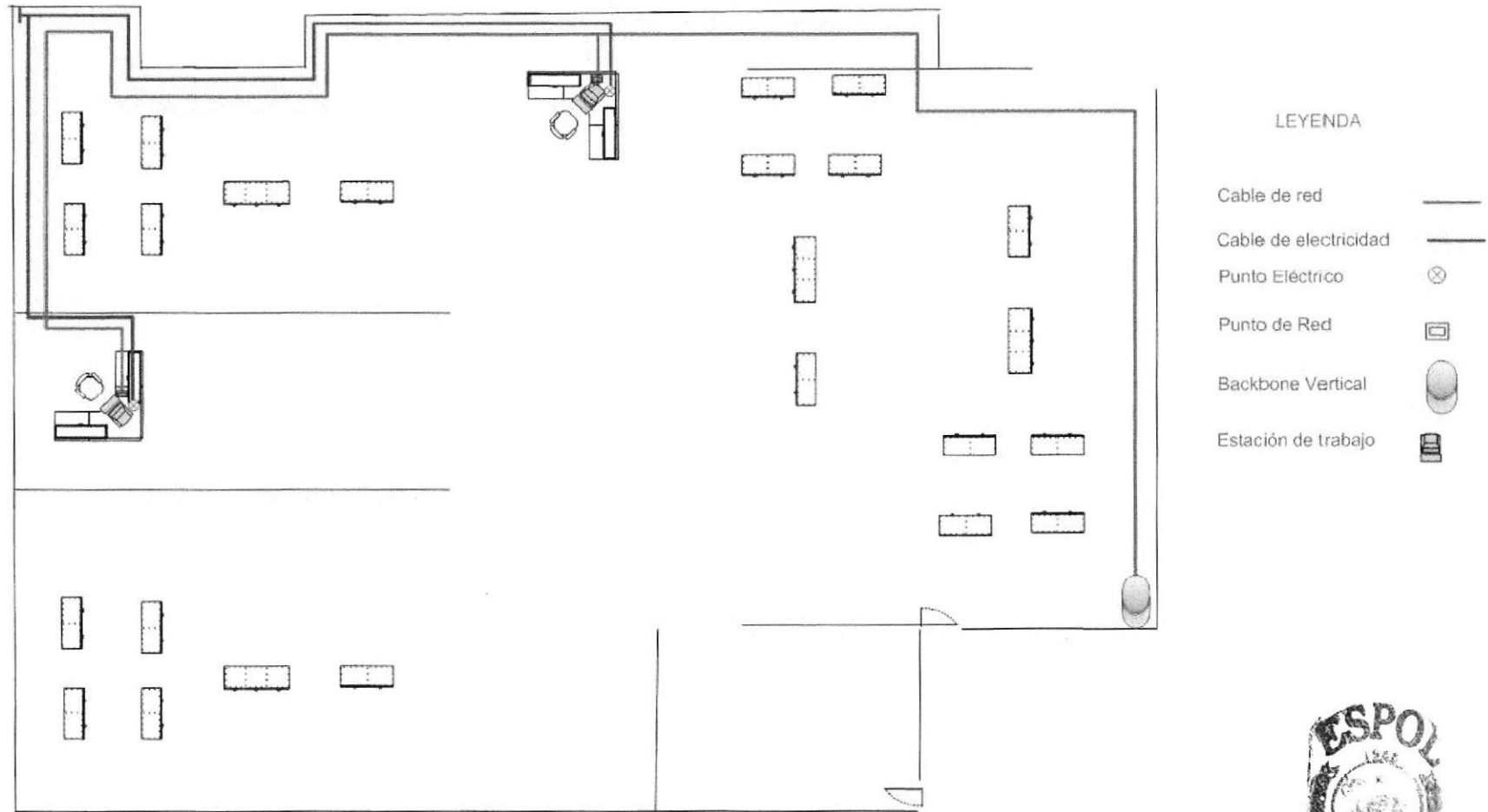


Figura 2-13: SEGUNDO PISO EDIFICIO SUCURSAL CENTRO



### 2.4.4.9. TERCER PISO EDIFICIO CENTRO

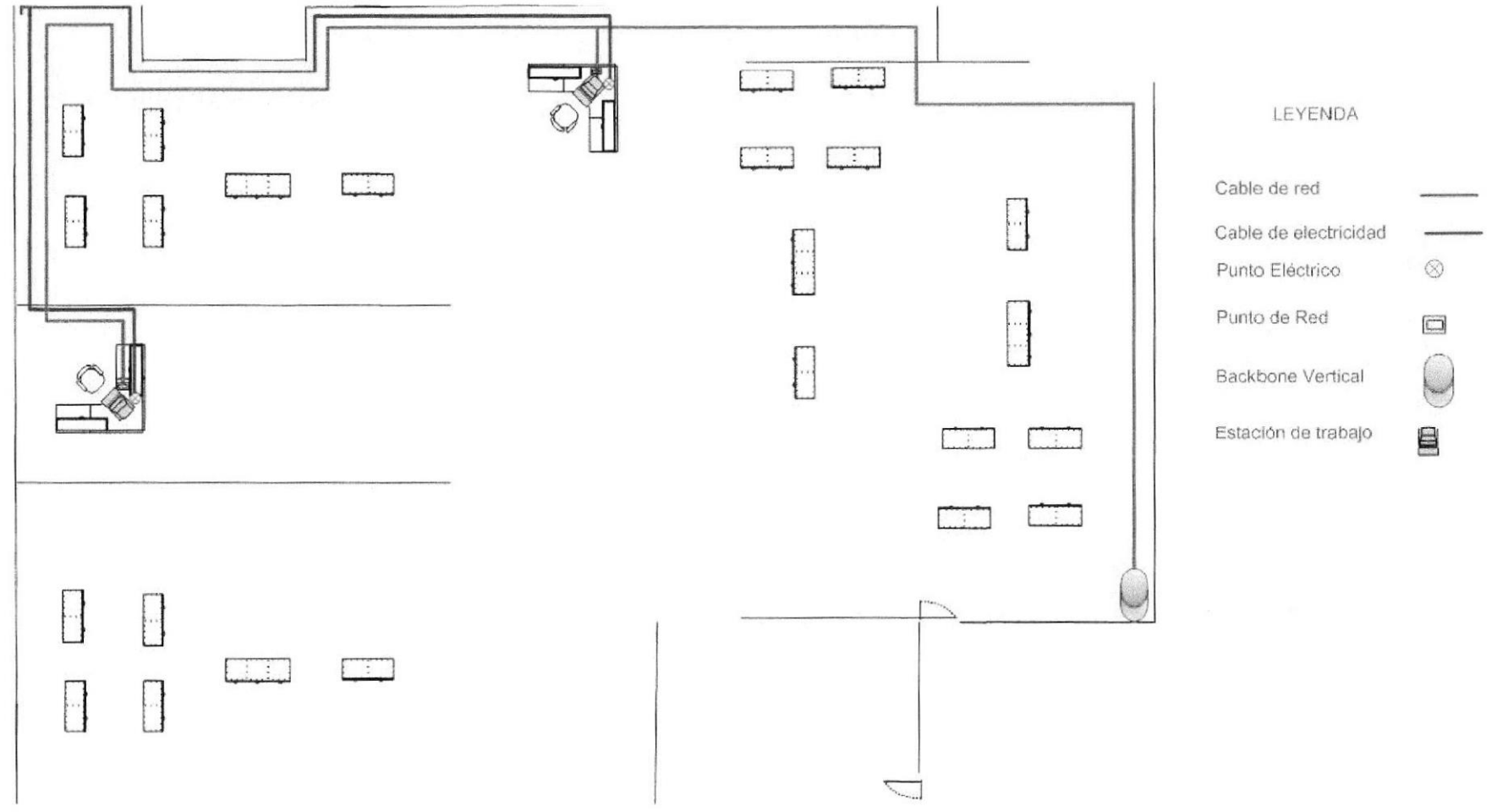


Figura 2-14: TERCER PISO EDIFICIO SUCURSAL CENTRO

### 2.4.4.10. CUARTO PISO EDIFICIO CENTRO

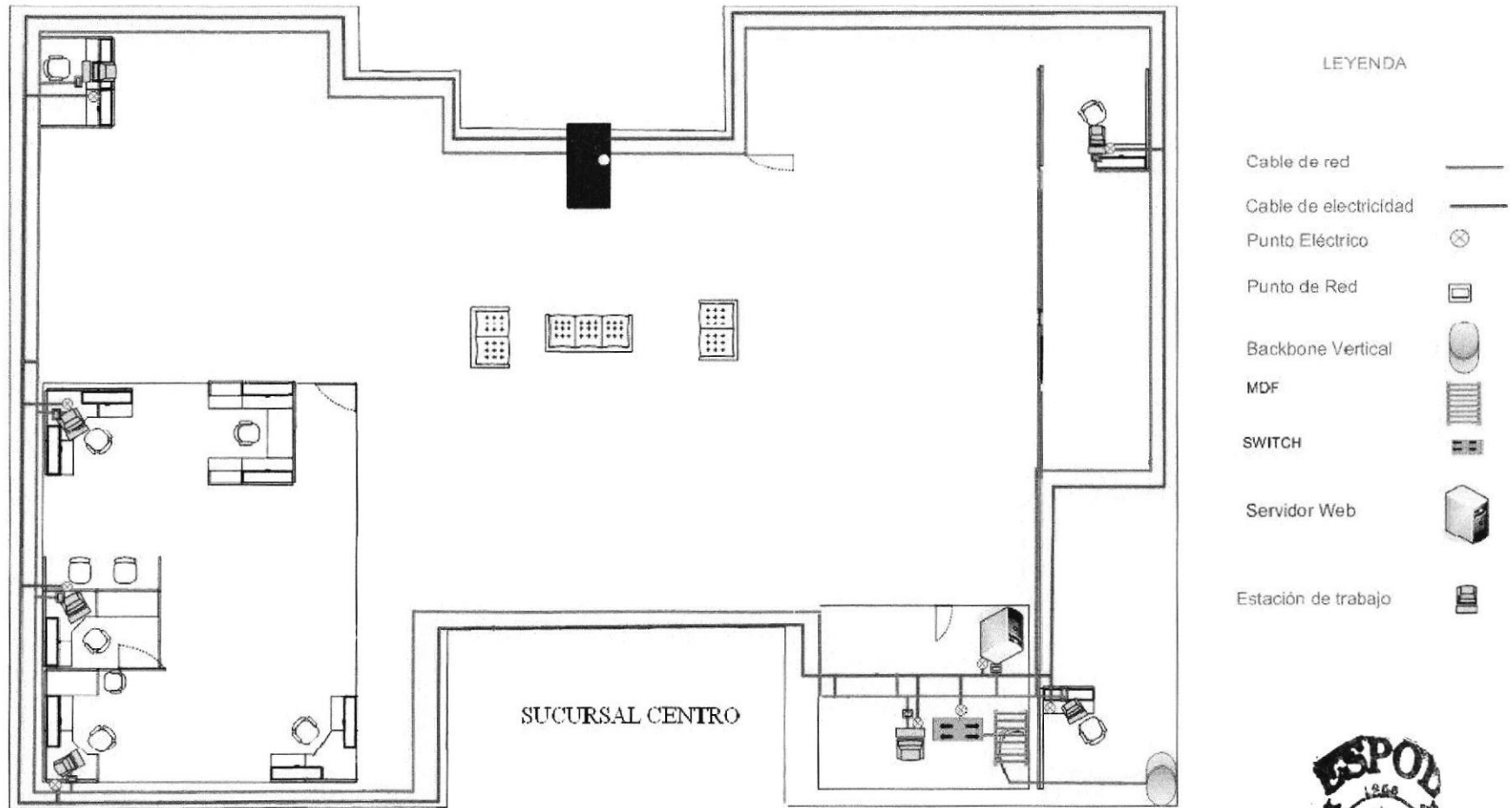


Figura 2-15: CUARTO PISO EDIFICIO SUCURSAL CENTRO



### 2.4.4.11. MEZANINE EDIFICIO SUR

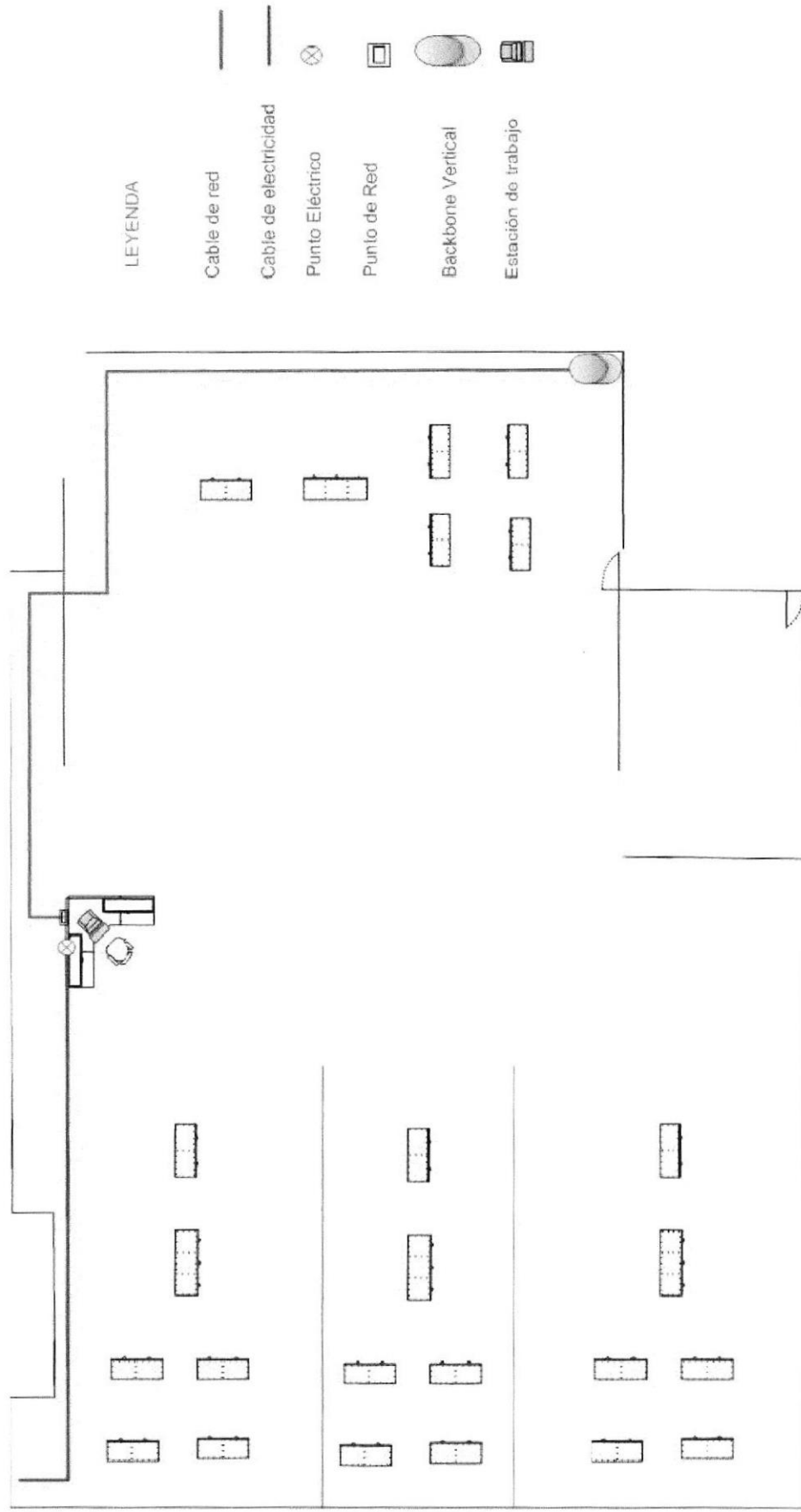


Figura 2-16: MEZANINE EDIFICIO SUCURSAL SUR

2.4.4.12. PRIMER PISO EDIFICIO SUR

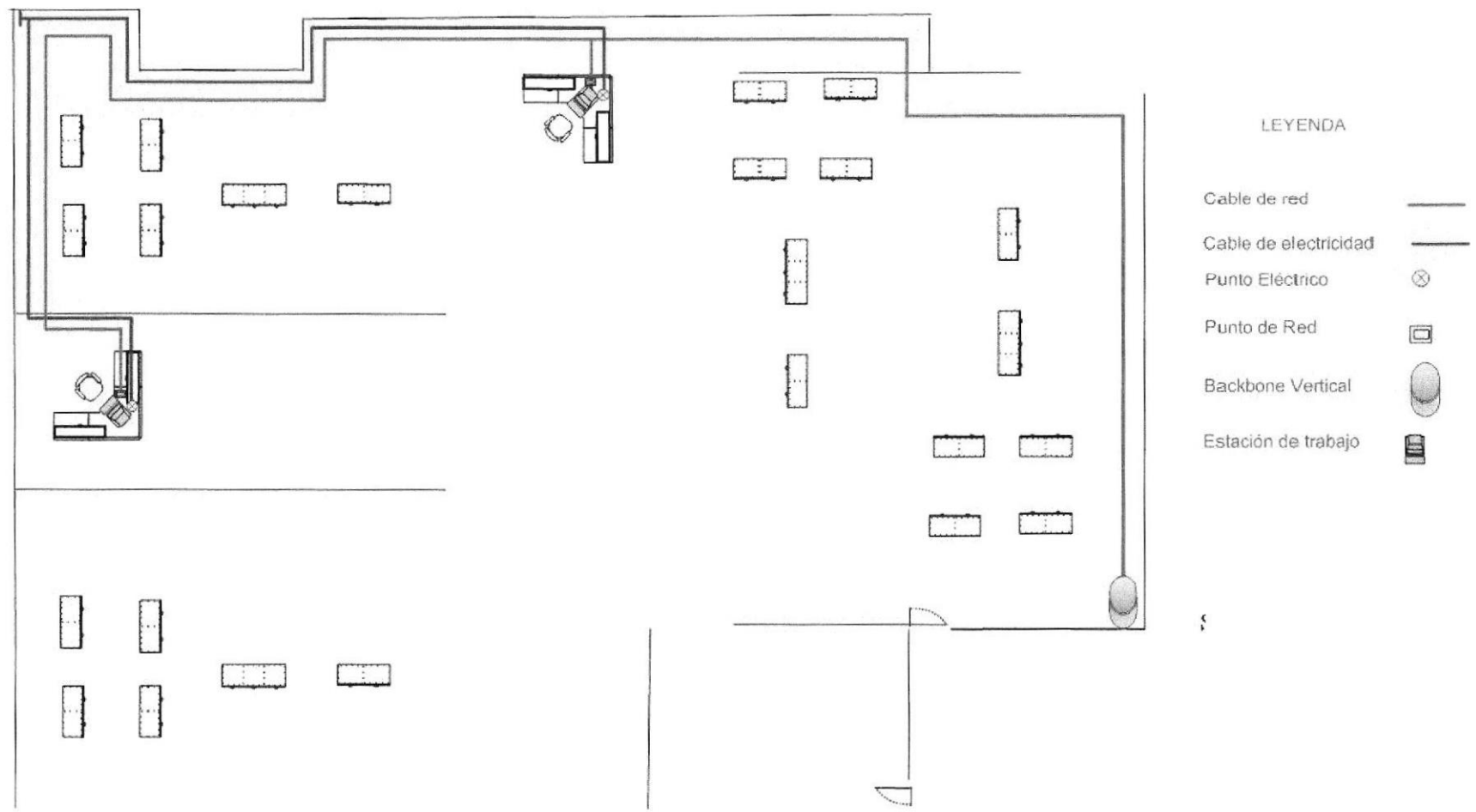


Figura 2-17: PRIMER PISO EDIFICIO SUCURSAL SUR

### 2.4.4.13. SEGUNDO PISO EDIFICIO SUR

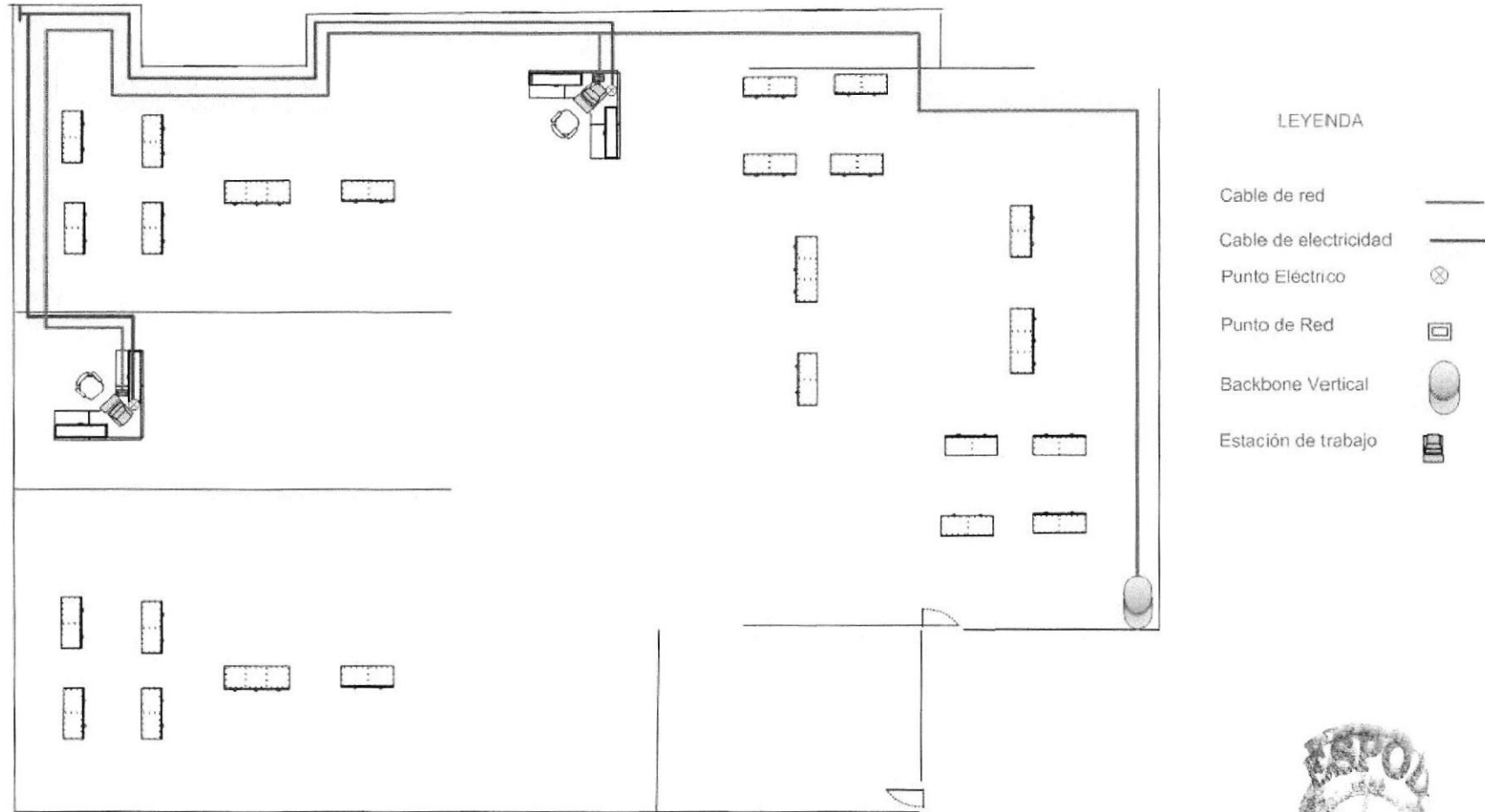


Figura 2-18: SEGUNDO PISO EDIFICIO SUCURSAL SUR



### 2.4.4.14. TERCER PISO EDIFICIO SUR

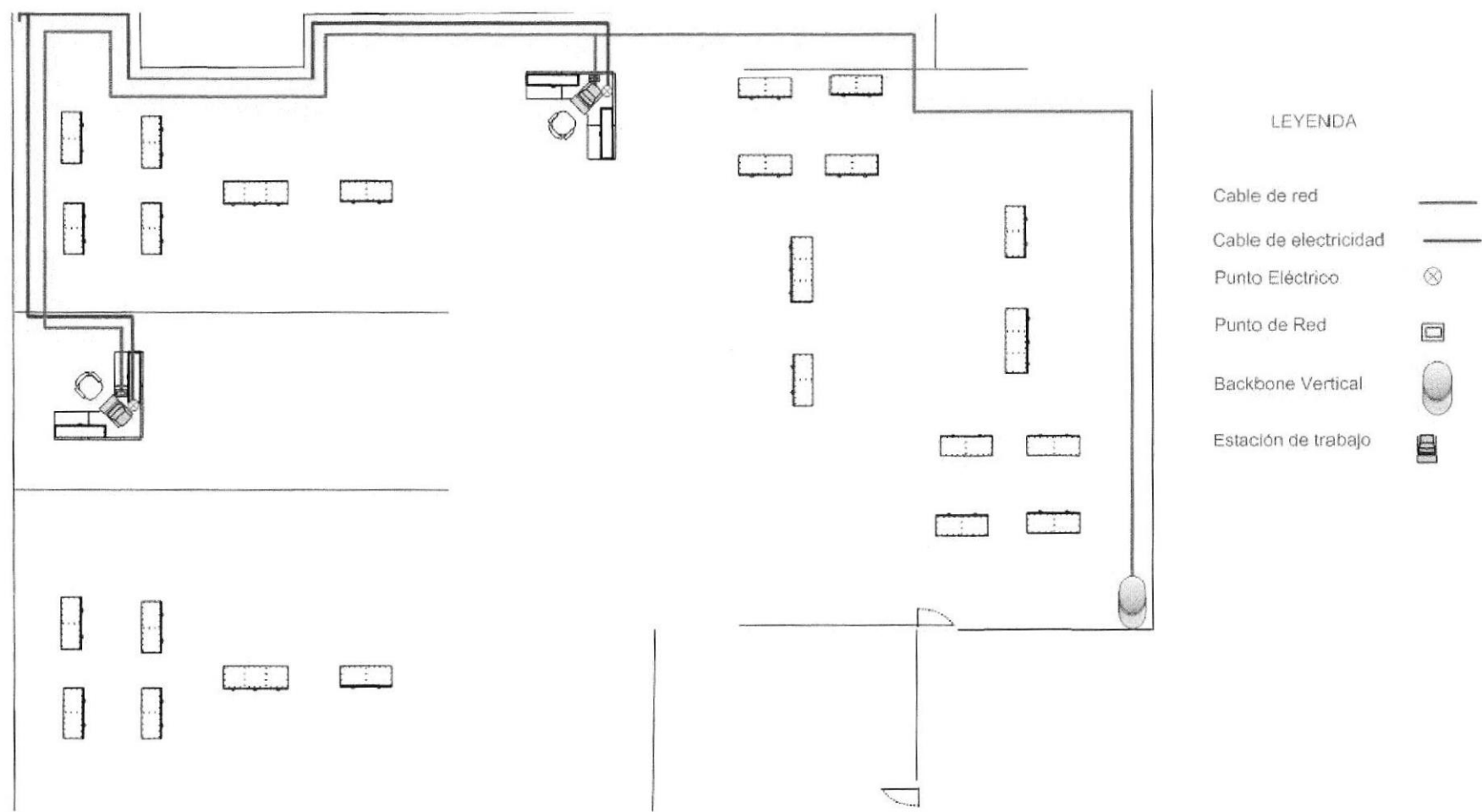


Figura 2-19: TERCER PISO EDIFICIO SUCURSAL SUR

### 2.4.4.15. CUARTO PISO EDIFICIO SUR

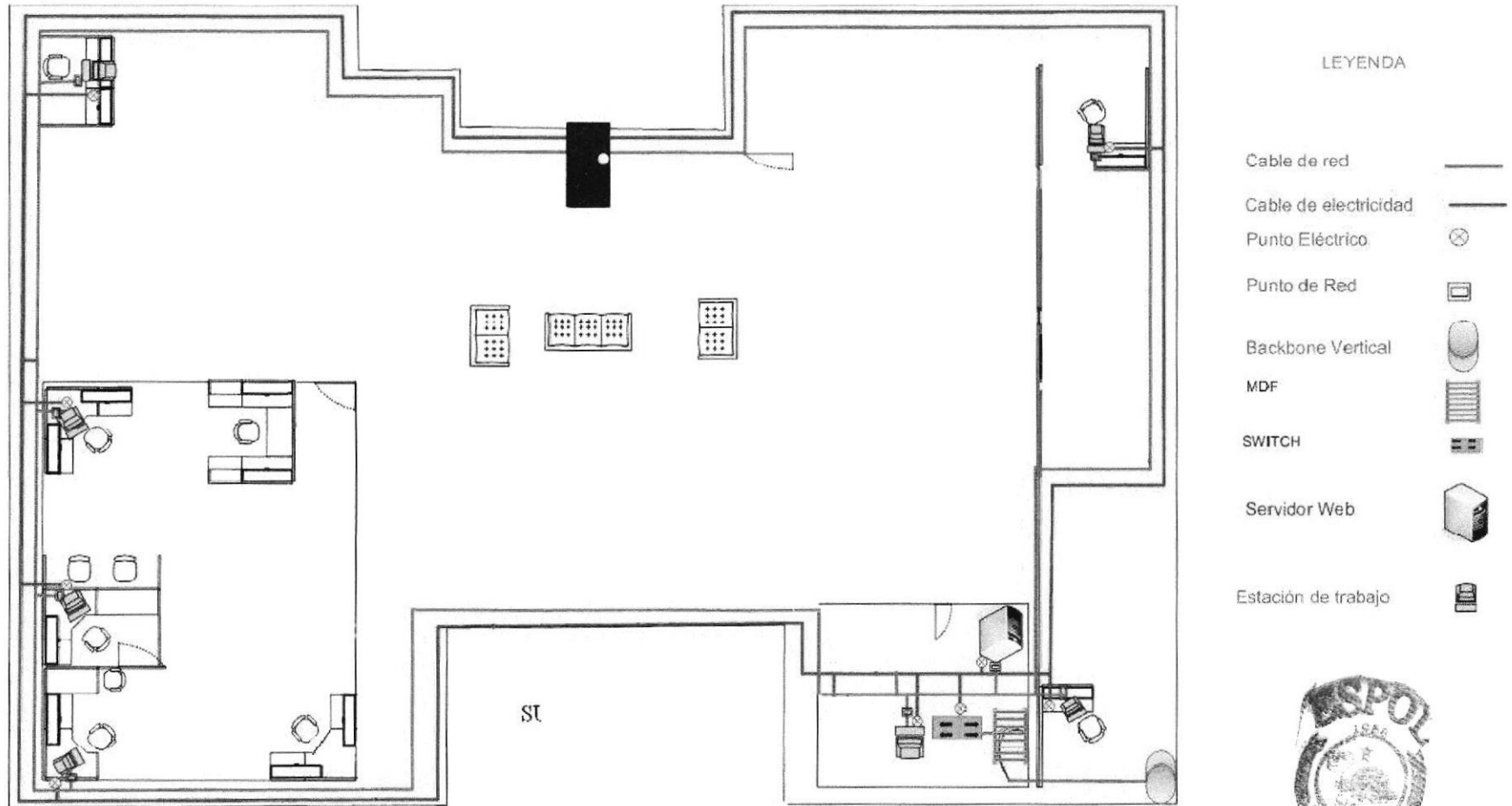


Figura 2-20: CUARTO PISO EDIFICIO SUCURSAL SUR



### 2.4.4.16. MEZANINE EDIFICIO BAHÍA

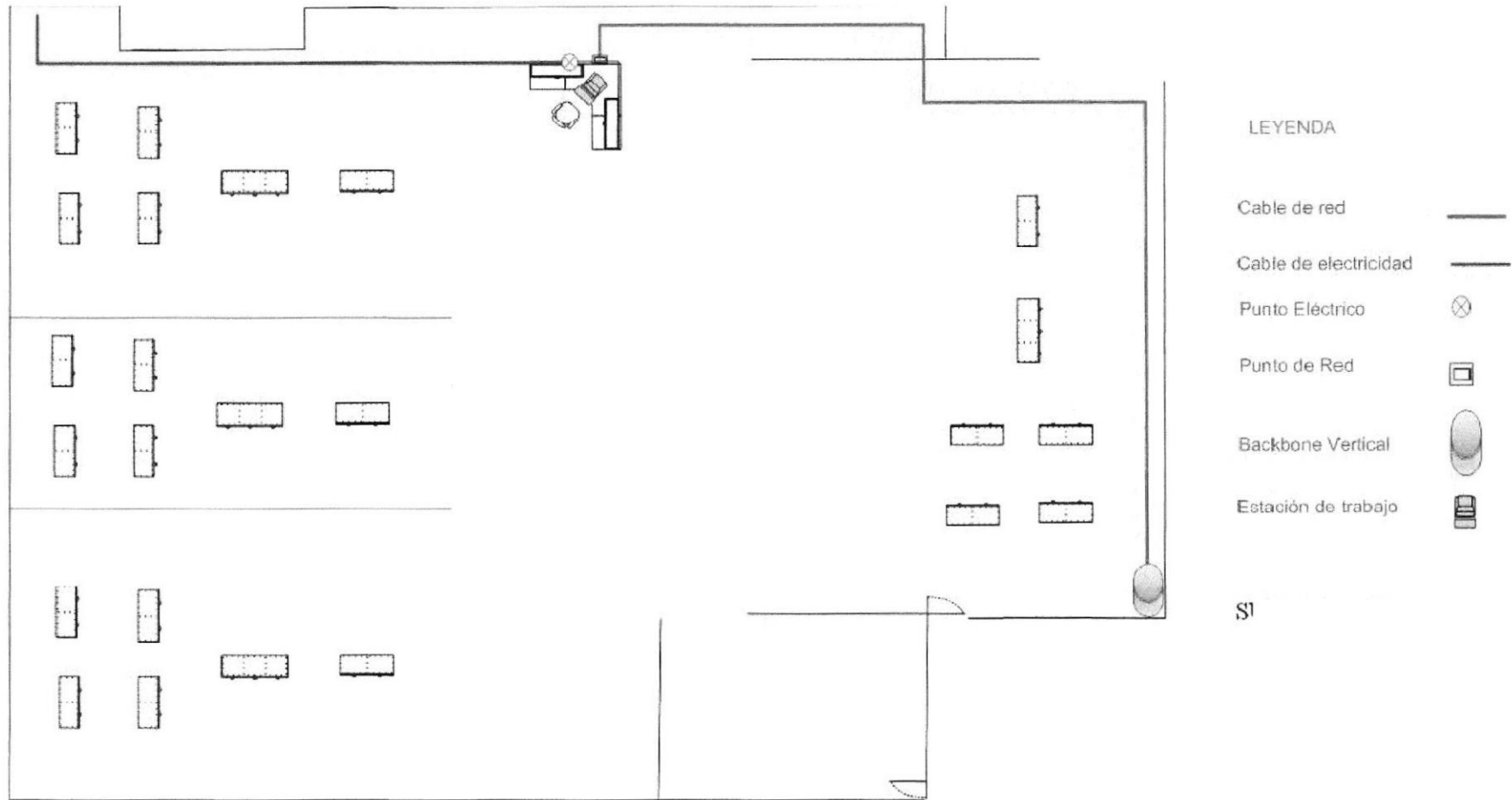


Figura 2-21: MEZANINE EDIFICIO SUCURSAL BAHÍA

### 2.4.4.17. PRIMER PISO EDIFICIO BAHÍA



Figura 2-22: PRIMER PISO EDIFICIO SUCURSAL BAHÍA



### 2.4.4.18. SEGUNDO PISO EDIFICIO BAHÍA

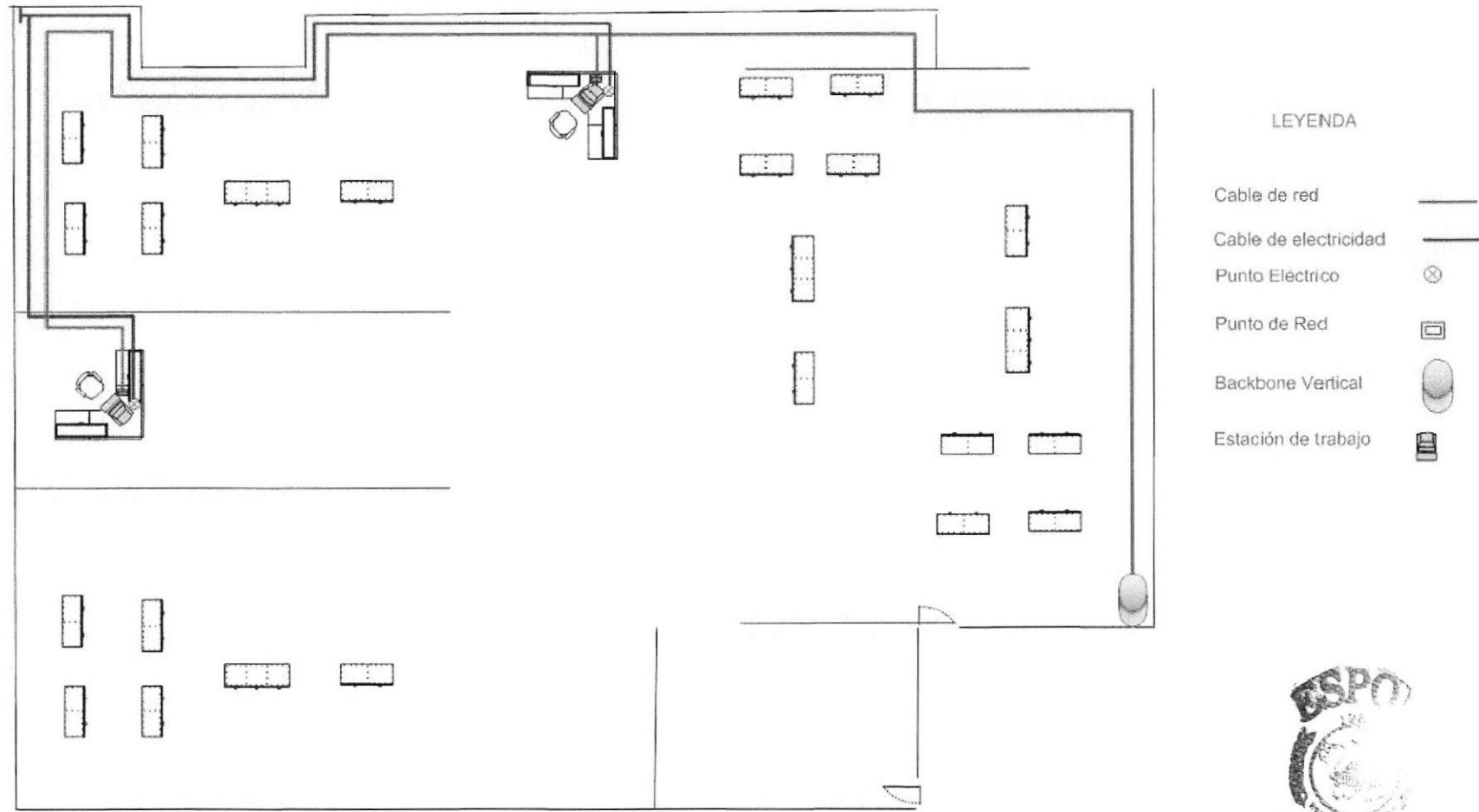


Figura 2-23: SEGUNDO PISO EDIFICIO SUCURSAL BAHÍA



### 2.4.4.19. TERCER PISO EDIFICIO BAHÍA

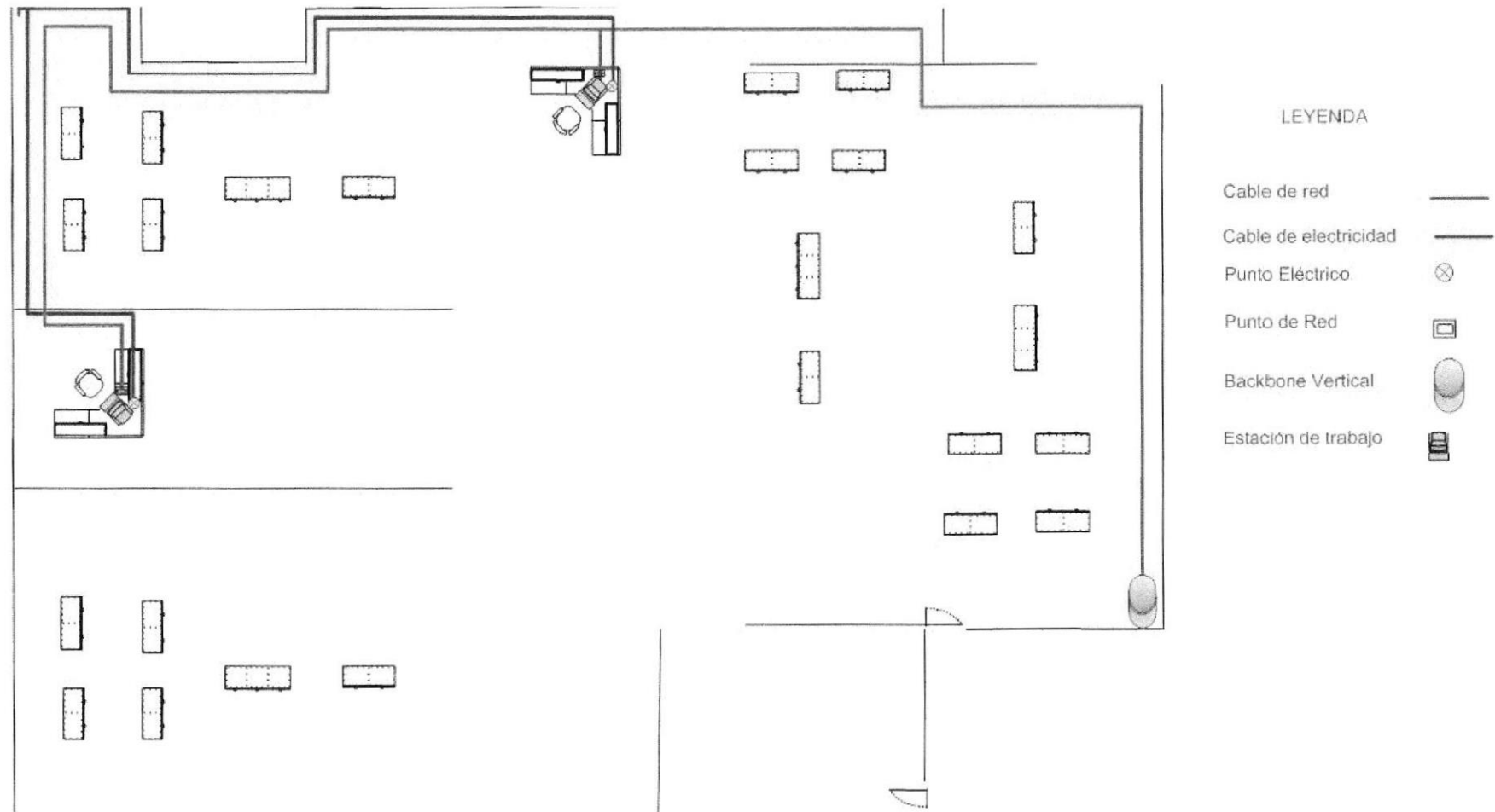


Figura 2-24: TERCER PISO EDIFICIO SUCURSAL BAHÍA

### 2.4.4.20. CUARTO PISO EDIFICIO BAHÍA

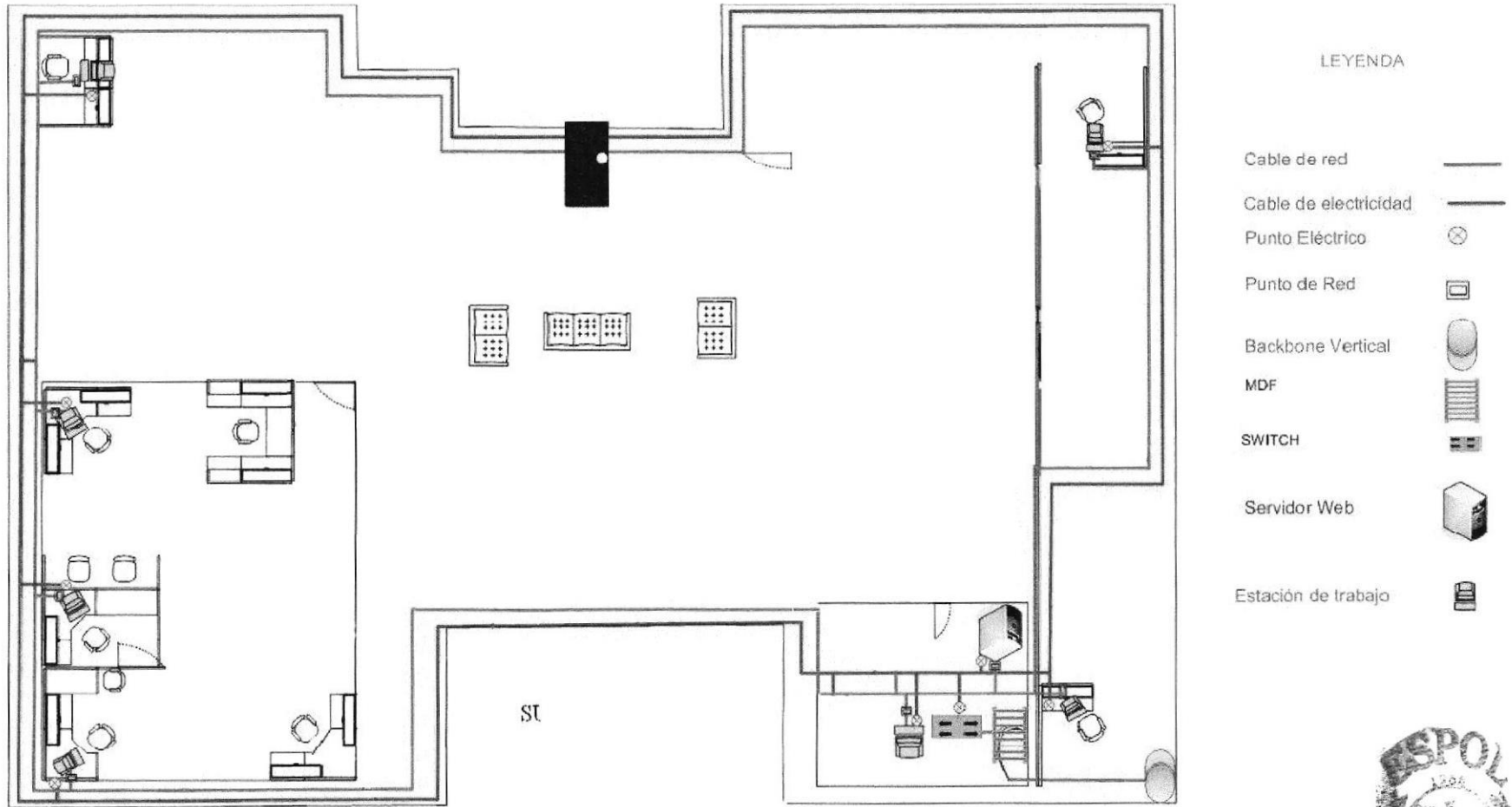


Figura 2-25: CUARTO PISO EDIFICIO SUCURSAL BAHÍA



2.4.4.21. SUCURSAL NORTE

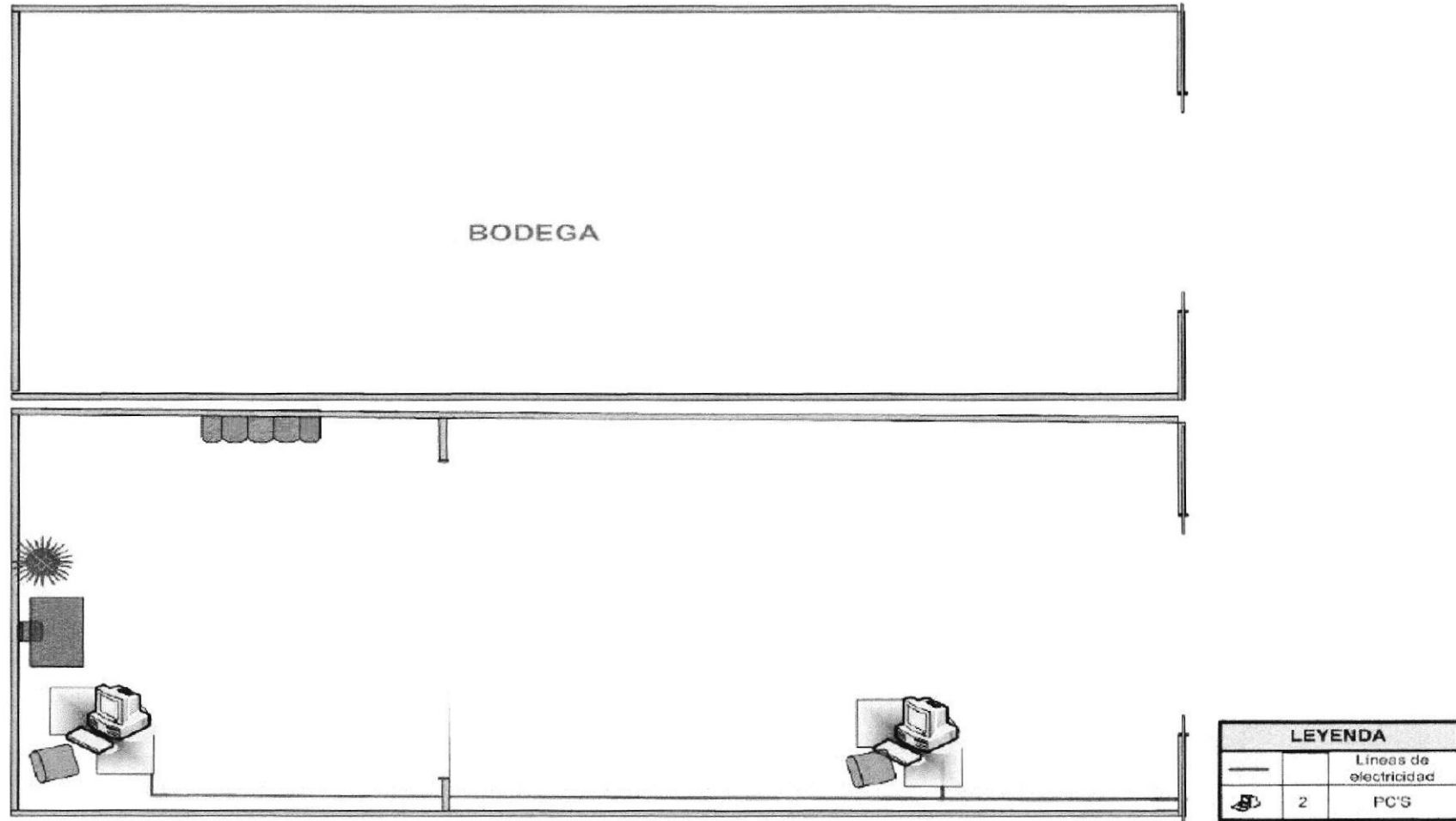


Figura 2-26: SUCURSAL NORTE


 BIBLIOTECA  
 CAMPUS  
 PEÑAS

## 2.4.5. DISPOSITIVOS DE CONMUTACIÓN

### 2.4.6. MATRIZ



CANT	DISPOSITIVOS	MODELOS	CARACTERÍSTICAS
2	Switch 	3 COM Modelo 4500	<ul style="list-style-type: none"> <li>✓ Interfaces: 24 – Giga Ethernet RJ-45 Velocidad de 10/100/1000 Mbps.</li> <li>✓ Capa 2 administrable</li> <li>✓ Modo comunicación: Full dúplex.</li> </ul>
1	Switch 	3 COM Modelo 4500	<ul style="list-style-type: none"> <li>✓ Interfaces: 48 – Giga Ethernet RJ-45 Velocidad de 10/100/1000 Mbps.</li> <li>✓ Capa 2 administrable</li> <li>✓ Modo comunicación: Full dúplex.</li> </ul>

Tabla 2-21: DISPOSITIVOS DE CONMUTACIÓN EN MATRIZ

#### 2.4.6.1. SUCURSAL CENTRO


CANT	DISPOSITIVOS	MODELOS	CARACTERÍSTICAS
1	Switch 	3 COM Modelo 4500	<ul style="list-style-type: none"> <li>✓ Interfaces: 24 – Giga Ethernet RJ-45 Velocidad de 10/100/1000 Mbps.</li> <li>✓ Capa 2 administrable</li> <li>✓ Modo comunicación: Full dúplex.</li> </ul>

Tabla 2-22: DISPOSITIVOS DE CONMUTACIÓN EN SUCURSAL CENTRO

## 2.4.6.2. SUCURSAL SUR


CANT	DISPOSITIVOS	MODELOS	CARACTERÍSTICAS
1	Switch 	3 COM Modelo 4500	<ul style="list-style-type: none"> <li>✓ Interfaces: 24 – Giga Ethernet RJ-45 Velocidad de 10/100/1000 Mbps.</li> <li>✓ Capa 2 administrable</li> <li>✓ Modo comunicación: Full dúplex.</li> </ul>

Tabla 2-23: DISPOSITIVOS DE CONMUTACIÓN EN SUCURSAL CENTRO

## 2.4.6.3. SUCURSAL BAHÍA


CANT	DISPOSITIVOS	MODELOS	CARACTERÍSTICAS
1	Switch 	3 COM Modelo 4500	<ul style="list-style-type: none"> <li>✓ Interfaces: 24 – Giga Ethernet RJ-45 Velocidad de 10/100/1000 Mbps.</li> <li>✓ Capa 2 administrable</li> <li>✓ Modo comunicación: Full dúplex.</li> </ul>

Tabla 2-24: DISPOSITIVOS DE CONMUTACIÓN EN SUCURSAL BAHÍA

## 2.4.7. MEDIOS DE COMUNICACIÓN

## 2.4.7.1. ALAMBICO

## 2.4.7.1.1. MATRIZ – SUCURSAL CENTRO

TIPO DE MEDIO	DESCRIPCIÓN	FRECUENCIA
Antena Microonda	Tipo Grid	2.4 Ghz

Tabla 2-25: MEDIO INALÁMBRICO MATRIZ – SUCURSAL CENTRO

## 2.4.7.1.2. MATRIZ – SUCURSAL SUR

TIPO DE MEDIO	DESCRIPCIÓN	FRECUENCIA
Antena Microonda	Tipo Grid	2.4 Ghz

Tabla 2-26: MEDIO INALÁMBRICO MATRIZ – SUCURSAL SUR

## 2.4.7.1.3. MATRIZ – SUCURSAL BAHÍA

TIPO DE MEDIO	DESCRIPCIÓN	FRECUENCIA
Antena Microonda	Tipo Gris	2.4 Ghz

Tabla 2-27: MEDIO INALÁMBRICO MATRIZ – SUCURSAL BAHÍA

## 2.4.8. INFRAESTRUCTURA WAN

## 2.4.8.1. DISPOSITIVOS DE ENRUTAMIENTO

## 2.4.8.1.1. MATRIZ – SUCURSAL CENTRO


CANT.	DISPOSITIVOS	MODELOS	CARACTERÍSTICAS
1	Router PROXIM 	T – Sunami Mp 11a	<ul style="list-style-type: none"> <li>✓ Ofrece una tarifa de datos de 54 Mbps en frecuencia diferentes de 5 GHz.</li> <li>✓ No requieren ningún contacto visual.</li> <li>✓ Posee puertos ethernet.</li> </ul>

Tabla 2-28: DISPOSITIVOS DE ENRUTAMIENTO MATRIZ – SUCURSAL CENTRO

## 2.4.8.1.2. MATRIZ – SUCURSAL SUR


CANT.	DISPOSITIVOS	MODELOS	CARACTERÍSTICAS
1	Router PROXIM 	T – Sunami Mp 11a	<ul style="list-style-type: none"> <li>✓ Ofrece una tarifa de datos de 54 Mbps en frecuencia diferentes de 5 GHz.</li> <li>✓ No requieren ningún contacto visual.</li> <li>✓ Posee puertos ethernet.</li> </ul>

Tabla 2-29: DISPOSITIVOS DE ENRUTAMIENTO MATRIZ – SUCURSAL SUR

## 2.4.8.1.3. MATRIZ – SUCURSAL BAHÍA


CANT.	DISPOSITIVOS	MODELOS	CARACTERÍSTICAS
1	Router PROXIM 	T – Sunami Mp 11a	<ul style="list-style-type: none"> <li>✓ Ofrece una tarifa de datos de 54 Mbps en frecuencia diferentes de 5 GHz.</li> <li>✓ No requieren ningún contacto visual.</li> <li>✓ Posee puertos ethernet.</li> </ul>

Tabla 2-30: DISPOSITIVOS DE ENRUTAMIENTO MATRIZ – SUCURSAL BAHÍA



INSTITUCIÓN DEL ESTADO

BIBLIOTECA

CAMPUS

PENAS

### 2.4.9. COMUNICACIÓN WAN A NIVEL DE MEDIOS

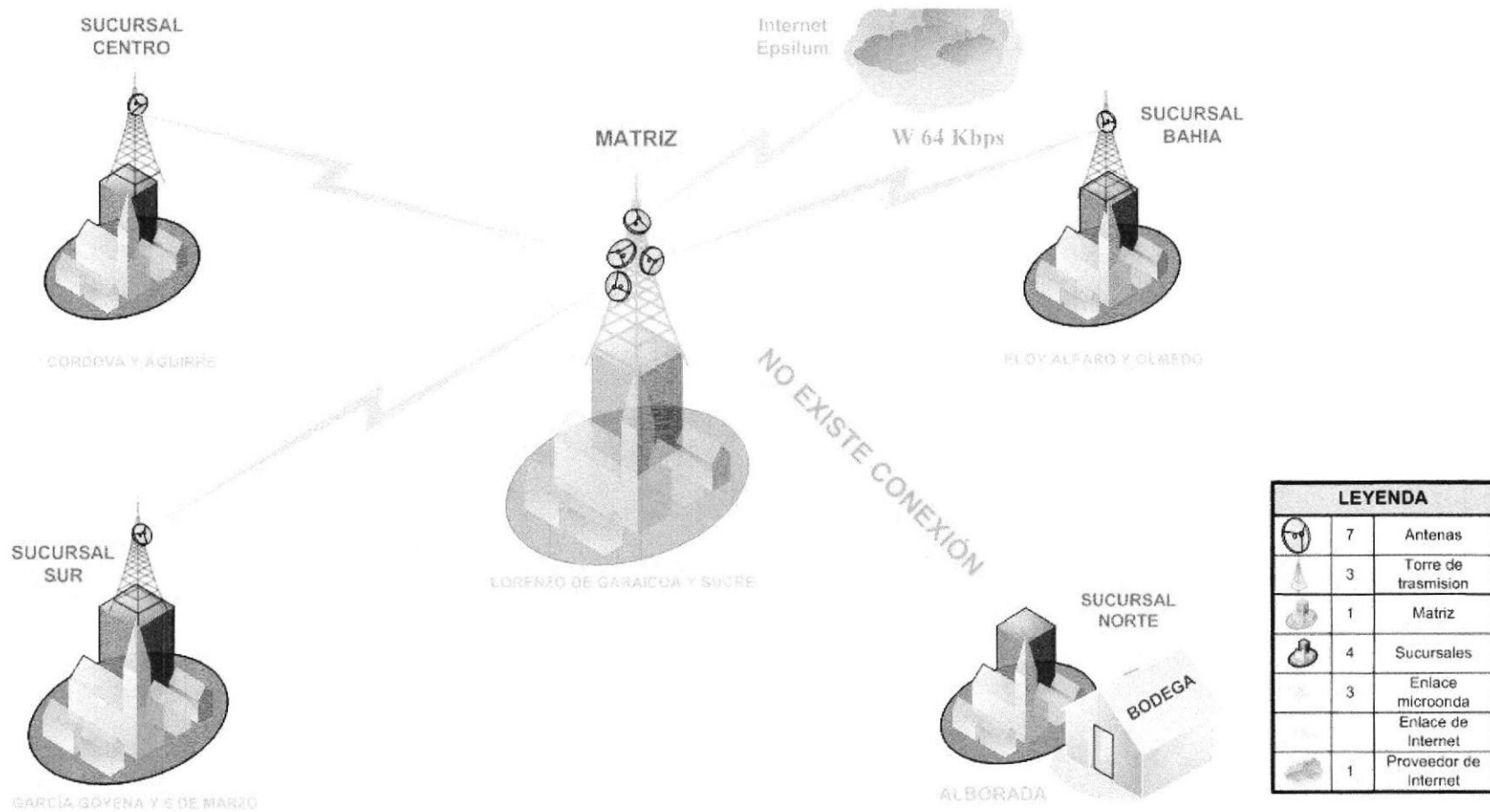


Figura 2-27: COMUNICACIÓN WAN A NIVEL DE MEDIOS

### 2.4.10.COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS

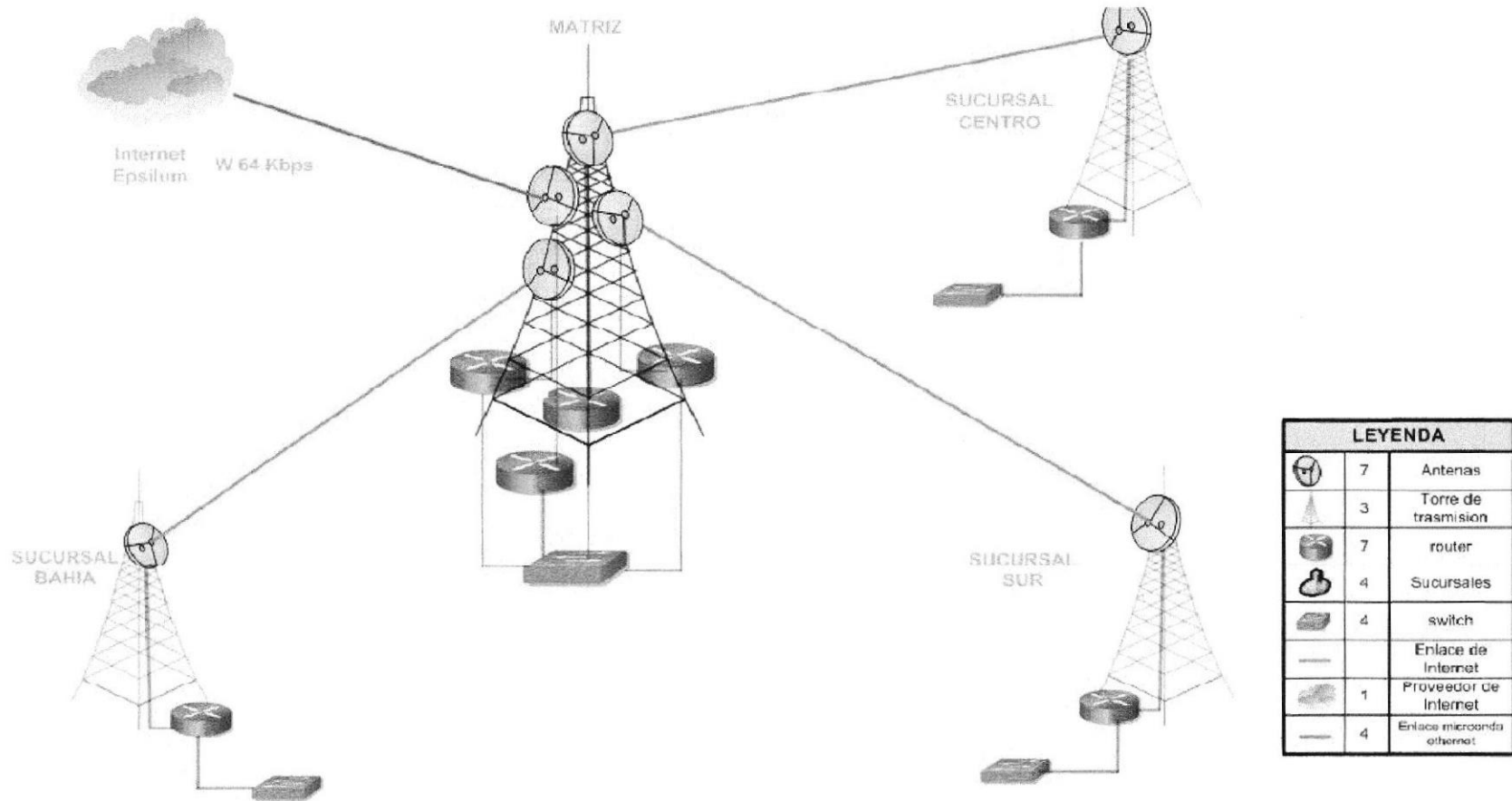


Figura 2-28: COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS

## 2.4.11. INTERNET

### 2.4.11.1. RECEPCIÓN DE INTERNET EN MATRIZ

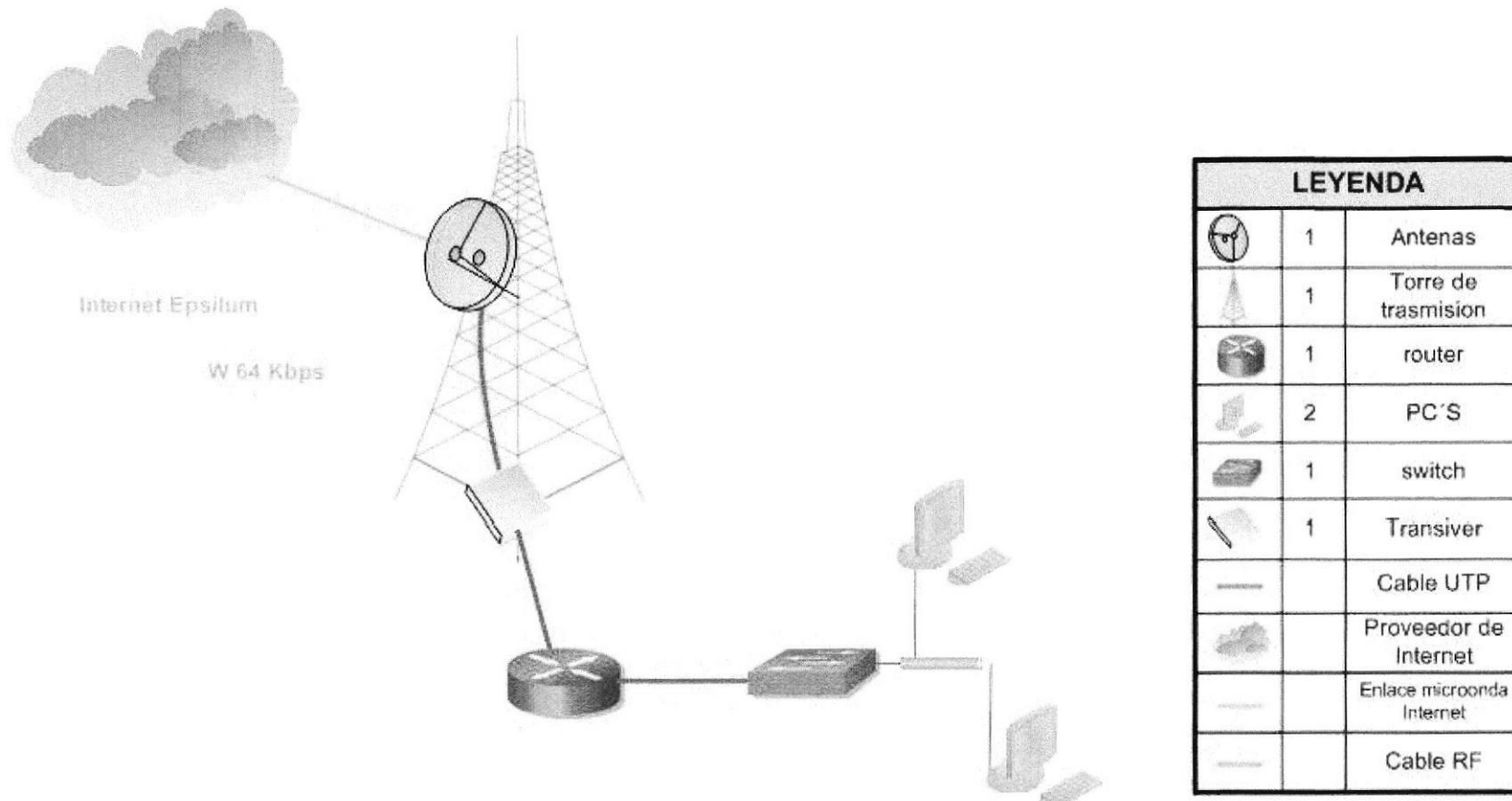


Figura 2-29: RECEPCIÓN DEL INTERNET EN MATRIZ

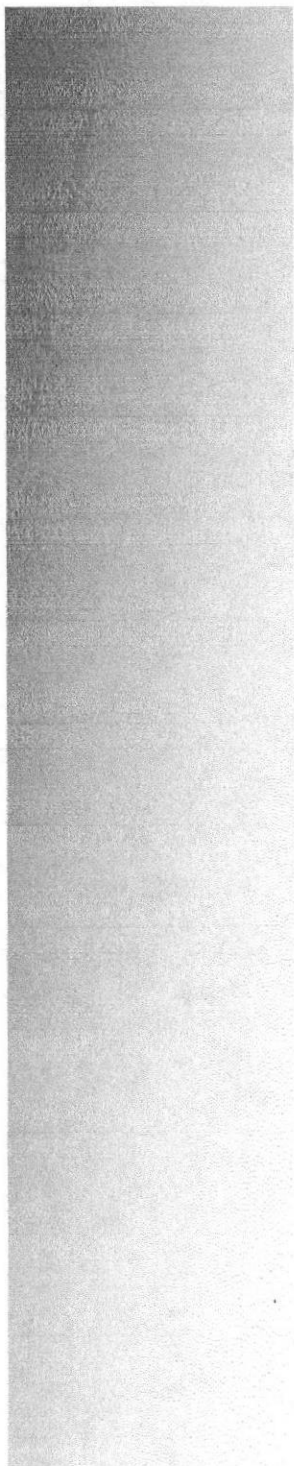


BIBLIOTECA  
CAMPUS  
PEÑAS

## **2.4.12.PROBLEMAS ENCONTRADOS**

Una vez realizado un análisis completa del estado de la red de comunicación a nivel WAN y LAN de los almacenes Estuardo Sánchez, hemos observado los siguientes problemas.

- ✓ Los accesos a la red Wan no cuenta con seguridad.
- ✓ No existen medios de comunicación wan entre la matriz y sucursal norte.
- ✓ La matriz y sucursales no tienen medios de respaldo en el enlace WAN.
- ✓ La sucursal norte no cuenta con ningún tipo de cableado de red.
- ✓ El departamento de contabilidad que se encuentra en la matriz no cuenta con ninguna clase de cableado de red.



# CAPÍTULO 3

PROPUESTA

### 3. PROPUESTA

#### 3.1. PROBLEMAS ENCONTRADOS

Una vez realizado un análisis completa del estado de la red de comunicación a nivel WAN y LAN de los almacenes Estuardo Sánchez, hemos observado los siguientes problemas.

PROBLEMA	CAUSA	EFEECTO
Los accesos a la red WAN no cuentan con ninguna clase de seguridad	Falta de asesoramiento al personal de sistemas, para recomendar medidas de seguridad	Libre acceso a la red WAN y LAN
No existe red ningún tipo de cableado de red en la sucursal norte	Falta de presupuesto	Procesos manuales e información actualizada
No existe comunicación WAN entre la matriz y sucursal norte	Falta de presupuesto, no se calculo el crecimiento de la empresa	Información no actualizada
Departamento de contabilidad en la matriz no cuenta con cableado estructurado	Resistencia al cambio por el encargado del departamento de contabilidad	Perdida de tiempo en procesos contables
No existe medios de respaldo en los enlaces WAN entre matriz y sucursales	Falta de presupuesto	Riesgo de pérdida de comunicación por siniestro que afecte la comunicación WAN

Tabla 3-1: PROBLEMA ENCONTRADOS

### 3.2. SOLUCIÓN PROPUESTA

De acuerdo al análisis realizado de la estructura y necesidades de la empresa y tomando en consideración su crecimiento, consideramos realizar la implementación de la red LAN con cable UTP categoría 6 y fibra óptica.

Para la implementación de la red WAN de respaldo usaremos fibra óptica, y para la protección de los accesos a la red WAN usaremos firewall de hardware.

En la comunicación entre la matriz y la sucursal que no se encuentra conectada usaremos el mismo esquema que tienen con sus demás sucursales en la actualidad.

La velocidad de transmisión con la que contara la empresa será de 1000 Mbps.

Todos los cambios que se efectuaran para la solución de los problemas nos brindaran un rendimiento óptimo y con proyección al futuro de la empresa en lo que se refiere a las redes WAN Y LAN.

Los costos invertidos en el sistema de cableado estructurado y de los dispositivos de red relacionados, aseguran un optimo funcionamiento de la organización a través de una comunicación de alto rendimiento, confiabilidad, integridad y seguridad de su información.

#### SOLUCIÓN PROPUESTA

PROBLEMA	SOLUCIÓN	ALCANCE
Acceso al WAN sin seguridad	Implementar hardware de protección Firewall	Mayor seguridad de acceso a la red WAN y LAN
No existe red LAN en la sucursal norte	Implementar cableado estructurado	Compartir recursos, periféricos e información
No existe comunicación WAN entre la matriz y sucursal norte	Implementar enlaces de comunicación matriz – sucursal norte	Comunicar la matriz con la sucursal norte y mantener la información actualizada
Departamento de contabilidad en la matriz no cuenta con cableado estructurado	Implementar cableado estructurado	Integrar el departamento de contabilidad a la red LAN de la empresa y procesos contables en línea
No existe respaldo en la comunicación WAN matriz - sucursales	Implementar enlaces de respaldo	La matriz y las sucursales estarán siempre comunicadas

Tabla 3-2: SOLUCIÓN PROPUESTA

### 3.3. ESTUDIO DE FACTIBILIDAD

#### 3.3.1. ALTERNATIVA 1

En este estudio detallamos las factibilidades técnica, operativa y económica el tiempo de consecución, costos y demás requerimientos así como también las ventajas, beneficios y forma de pagos.

##### 3.3.1.1. FACTIBILIDAD TÉCNICA

CANT	DESCRIPCIÓN	CARACTERÍSTICAS	UBICACIÓN
<b>HARDWARE</b>			
4	Antena	Microonda Tipo Grid 5.8Ghz	Sucursal norte
2	Router	PROXIM Modelo T sunami Mp 11 a puertos Ethernet	Dpto. comunicación matriz y sucursal norte
2	switch	3 COM Modelo 4500 Velocidad 10/100 Mbps Capa 2 administrable. 24 puertos	Sucursal norte
2	Transiver	10/100/1000 Mbps	Matriz sucursal alborada torre de transmisión
5	Tarjeta de red	D-Link 10/100/1000 Mbps	Sucursal Alborada
<b>RACK, PANELES Y GABINETES</b>			
1	Rack	Abierto de 5 UR	Dpto. comunicación Sucursal norte
1	Rack	Cerrado de 10 UR con ventilador	Oficinas de la sucursal norte
1	Gabinete	60*40	Sucursal norte
2	Patch panel	Modular de 24 puertos	Sucursal norte
<b>MATERIAL DE CABLEADO</b>			
3 rollos	cable	UTP categoría 6	Matriz y sucursal

			norte
74	Jack	Categoría 6	Matriz y sucursal norte
2	Bandeja par fibra óptica	Para 4 pares de hilos	Sucursal norte
9	Conectores para fibra óptica	Multimodo	Sucursal norte
2	patch cord de fibra	ST-SC DUPLEX MM	Sucursal norte
400 mts	Fibra óptica	Multimodo de 4 hilos	Sucursal norte
16	Cajas sobrepuestas	Categoría 6 rectangulares	Dpto. contabilidad matriz
25	Patch cord	3 pulgadas categoría 6	Matriz sucursal norte
20	FACE plate dobles	Tipo ejecutivo	Matriz y sucursal norte
18	Patch cord	10 pulgadas categoría 6	
30	Canaletas	Decorativas 40*25	Sucursal norte
4	Regletas eléctrica	Multitomas de 8 servicios	Sucursal norte
4	Bandeja metálica	estándar	Matriz y sucursal norte

Tabla 3-3: FACTIBILIDAD TÉCNICA ALTERNATIVA 1

## 3.3.1.2. FACTIBILIDAD OPERATIVA

CANT	FASES	SEMANAS
<b>ANÁLISIS DE CABLEADO LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	3
2	Técnicos de redes	3
<b>DISEÑO DE LA RED LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	3
<b>IMPLEMENTACIÓN DEL CABLEADO A NIVEL LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	8
3	Técnicos de redes	8
<b>FASE DE PRUEBA DE LA RED LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	8
2	Técnicos de redes	8
<b>FASE DE DOCUMENTACIÓN DE LA RED LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	2



Tabla 3-4: FACTIBILIDAD OPERATIVA ALTERNATIVA 1

**3.3.1.3. FACTIBILIDAD ECONÓMICA****3.3.1.3.1. COSTOS DE HARDWARE**

<b>CANT</b>	<b>DETALLE</b>	<b>PRECIO UNITARIO</b>	<b>TOTAL</b>
4	Antenas tipo grid de 5.8 GHz	\$ 390.00	\$ 1,560.00
2	Router modelo T sunami	\$ 357.00	\$ 714.00
4	Firewall DFL – 800	\$ 700.00	\$ 2,800.00
3	Switch 3COM 4500 16 puertos 10/100/1000 Mbps	\$ 490.50	\$ 490.50
5	Tarjetas de red D-Link 10/100/1000 Mbps	\$ 185.00	\$ 925.00
2	Rack abierto de pared modular de 5 ur	\$ 16.00	\$ 32.00
1	Rack cerrado de 10 ur con ventilador	\$ 150.00	\$ 150.00
2	Patch panel modular de 24 puertos	\$ 26	\$ 52.00
4	Organizadores horizontales 80 *80	\$ 9.00	\$ 36.00
2	Organizadores horizontales 60 * 40	\$ 9.00	\$ 18.00
4	Bandejas metálicas estándar	\$ 18.00	\$ 72.00
16	Cajas sobrepuesta rectangulares	\$ 1.24	\$ 19.84
2	Transiver 10/100/1000 Mbps	\$ 235.00	\$ 470.00
30	Canaletas decorativas	\$ 4.30	\$ 129.00
4	Regletas eléctricas multitomas de 8 servicio	\$ 32.00	\$128.00
20	FACE plate dobles de tipo ejecutivo	\$ 2.40	\$ 48.00
18	Patch cord 10' categoría 6	\$ 5.80	\$ 104.40
25	Patch cord 3' categoría 6	\$ 3.54	\$ 88.5
74	Jack categoría 6	\$ 4.10	\$ 303.00
3 rollos	Cable UTP categoría 6	\$ 267.00	\$ 801.00
2	Bandejas de fibra óptica 4 pares UNICOM	\$ 100.00	\$ 200.00
9	Conectores de fibra óptica multimodo	\$ 4.00	\$ 36.00

400 m	Fibra óptica multimodo 4 hilos	\$ 3.23	\$ 1,292.00
2	Match cord de fibra óptica ST-DUPLEX MM	\$ 29.00	\$ 58.00
<b>TOTAL</b>			<b>\$ 10,577.48</b>

Tabla 3-5: COSTOS DE HARDWARE ALTERNATIVA 1

## 3.3.1.3.2. COSTOS DE OPERATIVOS

CANT	FASES	SEMANAS	COSTO POR SEMANA	COSTO TOTAL
<b>ANÁLISIS DE CABLEADO LAN Y WAN</b>				
1	Ing. en Telecomunicaciones.	3	\$ 250.00	\$ 750.00
2	Técnicos de redes	3	\$ 75.00	\$ 450.00
<b>Total de la fase análisis de cableado LAN y WAN</b>				<b>\$ 1,200.00</b>
<b>DISEÑO DE LA RED LAN Y WAN</b>				
1	Ing. en Telecomunicaciones.	3	\$ 250.00	\$ 750.00
<b>Total de la fase de diseño LAN y WAN</b>				<b>\$ 750.00</b>
<b>IMPLEMENTACIÓN DEL CABLEADO</b>				
1	Ing. en Telecomunicaciones.	8	\$ 250.00	\$ 2,000.00
3	Técnicos de redes	8	\$ 75.00	\$ 1,800.00
<b>Total de la fase de implementación</b>				<b>\$ 3,800.00</b>
<b>FASE DE PRUEBA</b>				
1	Ing. en Telecomunicaciones.	8	\$ 250.00	\$ 2,000.00
2	Técnicos de redes	8	\$ 75.00	\$ 1,200.00
<b>Total de la fase de prueba</b>				<b>\$ 3,200.00</b>
<b>FASE DE DOCUMENTACIÓN</b>				
1	Ing. en Telecomunicaciones.	2	\$ 250.00	\$ 500.00
<b>Total de la fase de documentación</b>				<b>\$ 500.00</b>
<b>TOTAL</b>				<b>\$ 9,450.00</b>

Tabla 3-6: COSTOS OPERATIVOS ALTERNATIVA 1

## 3.3.1.4. COSTO DE FACTIBILIDAD ALTERNATIVA 1

<b>COSTOS DE HARDWARE</b>	<b>\$ 10,577.48</b>
<b>COSTOS OPERATIVOS</b>	<b>\$ 9,450.00</b>
<b>SUBTOTAL COSTOS</b>	<b>\$ 20,027.48</b>
<b>IVA 12%</b>	<b>\$ 2,403.30</b>
<b>COSTO TOTAL</b>	<b>\$ 22,430.78</b>

Tabla 3-7: COSTOS DE LA FACTIBILIDAD DE LA ALTERNATIVA 1



BIBLIOTECA  
CAMPUS  
PEÑAS

3.3.1.5. PLAN DE TRABAJO

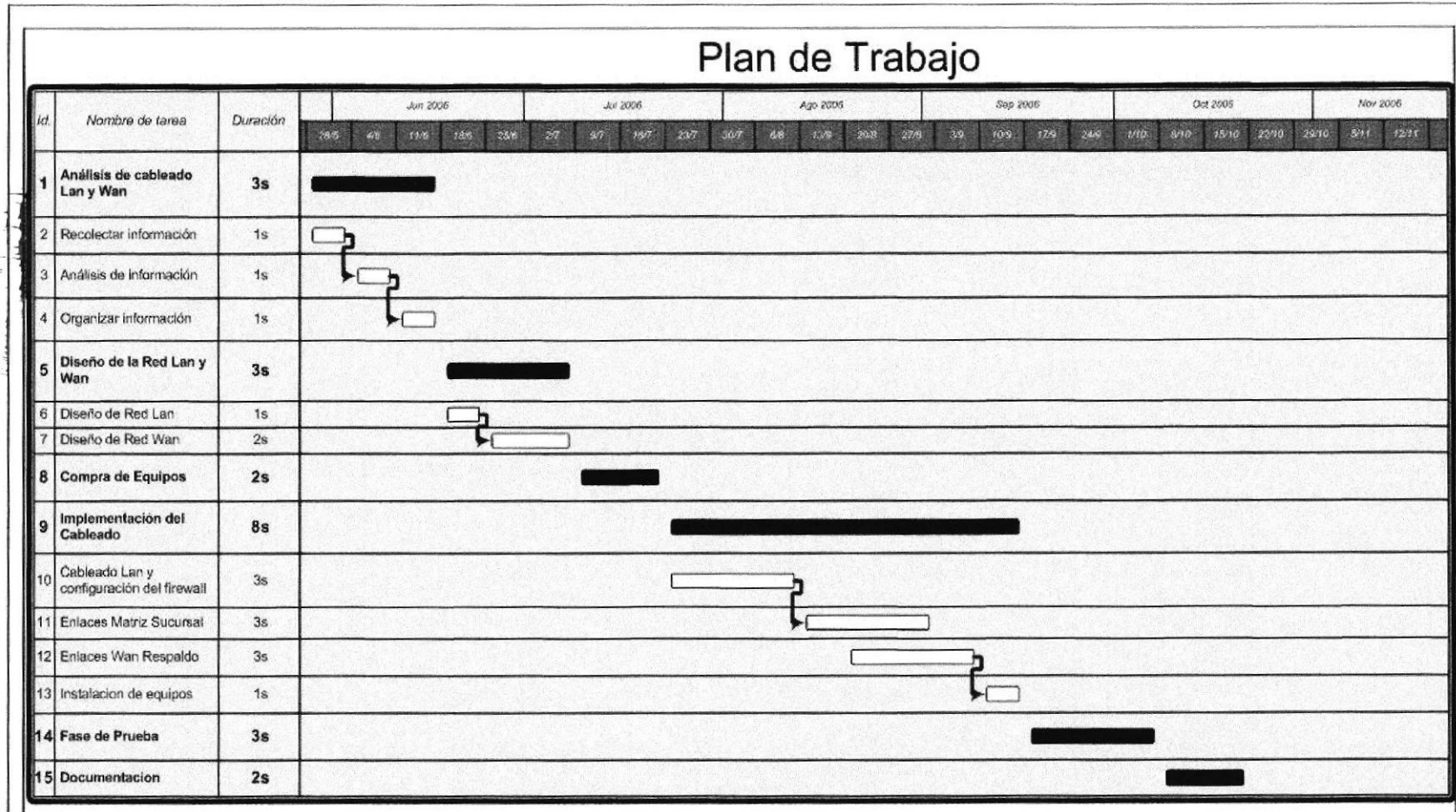


Figura 3-1: PLAN DE TRABAJO ALTERNATIVA 1

### 3.3.1.6. VENTAJAS

- ✓ Tendremos dispositivos de WAN y LAN enrutamiento y de conmutación seguros protegidos.
- ✓ Con la instalación de los enlaces de respaldo entre matriz y sucursales tendremos la seguridad de estar siempre conectados.
- ✓ Tener una red LAN en cada uno de los edificios mejorara la infraestructura.
- ✓ Con la implementación de la sucursal norte a la red WAN de la empresa, se ganara mayor agilidad y procesos en línea.

### 3.3.1.7. BENEFICIOS

- ✓ Seguridad en la red interna de la empresa.
- ✓ Seguridad a nivel de la red WAN.
- ✓ Organización en cada uno de los departamentos en el cableado estructurado.
- ✓ Mejor velocidad y tiempo de respuesta.



### 3.3.1.8. GARANTÍAS

Para esta alternativa nosotros damos un tiempo de garantía de 6 meses para cubrir cualquier tipo de inconvenientes en la red WAN, cabe mencionar que la garantía solo cubre algún desperfectos en los equipos y dispositivos.

### 3.3.1.9. FORMA DE PAGO

La forma de pago se realizara de la siguiente manera:

Se la hará en tres pagos:

El primer pago será del 50 % y se realizara el pago al momento de aceptar el contrato de la propuesta escogida.

El segundo pago será del 25 % y se realizara el pago 15 días después de haber firmado el contrato para cubrir gastos de materiales, equipos e imprevistos.

El tercer pago será del 25 % restante, se la efectuara al término la solución escogida.

Cabe recalcar que durante la implementación de la solución escogida, tendrán que ofrecer todas las garantías y facilidades que se requieran para el cumplimiento de la solución.

### 3.3.2. ALTERNATIVA 2

En este estudio detallamos las factibilidades técnica, operativa y económica el tiempo de consecución, costos y demás requerimientos así como también las ventajas, beneficios y forma de pagos.

#### 3.3.2.1. FACTIBILIDAD TÉCNICA

CANT	DESCRIPCIÓN	CARACTERÍSTICAS	UBICACIÓN
<b>HARDWARE</b>			
4	Antena	Microonda Tipo Grid 5.8Ghz	Sucursal norte
2	Router	PROXIM Modelo T sunami Mp 11 a puertos Ethernet	Dpto. comunicación matriz y sucursal norte
2	switch	3 D – LINK Velocidad 10/100/100 Mbps 16 puertos	Sucursal norte
2	Transiver	10/100/1000 Mbps	Matriz sucursal alborada torre de transmisión
5	Tarjeta de red	D-Link 10/100/1000 Mbps	Sucursal Alborada
<b>RACK, PANELES Y GABINETES</b>			
1	Rack	Abierto de 5 UR	Dpto. comunicación Sucursal norte
1	Rack	Cerrado de 10 UR con ventilador	Oficinas de la sucursal norte
1	Gabinete	60*40	Sucursal norte
2	Patch panel	Modular de 24 puertos	Sucursal norte
<b>MATERIAL DE CABLEADO</b>			
3 rollos	cable	UTP categoría 6	Matriz y sucursal

			norte
74	Jack	Categoría 6	Matriz y sucursal norte
2	Bandeja par fibra óptica	Para 4 pares de hilos	Sucursal norte
9	Conectores para fibra óptica	Multimodo	Sucursal norte
2	patch cord de fibra	ST-SC DUPLEX MM	Sucursal norte
400 mts	Fibra óptica	Multimodo de 4 hilos	Sucursal norte
16	Cajas sobrepuestas	Categoría 6 rectangulares	Dpto. contabilidad matriz
25	Patch cord	3 pulgadas categoría 6	Matriz sucursal norte
20	FACE plate dobles	Tipo ejecutivo	Matriz y sucursal norte
18	Patch cord	10 pulgadas categoría 6	
30	Canaletas	Decorativas 40*25	Sucursal norte
4	Regletas eléctrica	Multitomas de 8 servicios	Sucursal norte
4	Bandeja metálica	estándar	Matriz y sucursal norte



Tabla 3-8: FACTIBILIDAD TÉCNICA ALTERNATIVA 2

## 3.3.2.2. FACTIBILIDAD OPERATIVA

CANT	FASES	SEMANAS
<b>ANÁLISIS DE CABLEADO LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	3
2	Técnicos de redes	3
<b>DISEÑO DE LA RED LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	3
<b>IMPLEMENTACIÓN DEL CABLEADO A NIVEL LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	8
3	Técnicos de redes	8
<b>FASE DE PRUEBA DE LA RED LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	8
2	Técnicos de redes	8
<b>FASE DE DOCUMENTACIÓN DE LA RED LAN Y WAN</b>		
1	Ing. en Telecomunicaciones.	2

Tabla 3-9: FACTIBILIDAD OPERATIVA ALTERNATIVA 2

400 m	Fibra óptica multimodo 4 hilos	\$ 3.23	\$ 1,292.00
2	Match cord de fibra óptica ST-DUPLEX MM	\$ 29.00	\$ 58.00
<b>TOTAL</b>			<b>\$ 9,197.48</b>

Tabla 3-10: COSTOS DE HARDWARE ALTERNATIVA 2

## 3.3.2.3.2. COSTOS DE OPERATIVOS

CANT	FASES	SEMANAS	COSTO POR SEMANA	COSTO TOTAL
<b>ANÁLISIS DE CABLEADO LAN Y WAN</b>				
1	Ing. en Telecomunicaciones.	3	\$ 250.00	\$ 750.00
2	Técnicos de redes	3	\$ 75.00	\$ 450.00
<b>Total de la fase análisis de cableado LAN y WAN</b>				<b>\$ 1,200.00</b>
<b>DISEÑO DE LA RED LAN Y WAN</b>				
1	Ing. en Telecomunicaciones.	3	\$ 250.00	\$ 750.00
<b>Total de la fase de diseño LAN y WAN</b>				<b>\$ 750.00</b>
<b>IMPLEMENTACIÓN DEL CABLEADO</b>				
1	Ing. en Telecomunicaciones.	8	\$ 250.00	\$ 2,000.00
3	Técnicos de redes	8	\$ 75.00	\$ 1,800.00
<b>Total de la fase de implementación</b>				<b>\$ 3,800.00</b>
<b>FASE DE PRUEBA</b>				
1	Ing. en Telecomunicaciones.	8	\$ 250.00	\$ 2,000.00
2	Técnicos de redes	8	\$ 75.00	\$ 1,200.00
<b>Total de la fase de prueba</b>				<b>\$ 3,200.00</b>
<b>FASE DE DOCUMENTACIÓN</b>				
1	Ing. en Telecomunicaciones.	2	\$ 250.00	\$ 500.00
<b>Total de la fase de documentación</b>				<b>\$ 500.00</b>
<b>TOTAL</b>				<b>\$ 9,450.00</b>

Tabla 3-11: COSTOS OPERATIVOS ALTERNATIVA 2

## 3.3.2.4. COSTO DE FACTIBILIDAD ALTERNATIVA 1

<b>COSTOS DE HARDWARE</b>	<b>\$ 9,197.48</b>
<b>COSTOS OPERATIVOS</b>	<b>\$ 9,450.00</b>
<b>SUBTOTAL COSTOS</b>	<b>\$ 18,647.48</b>
<b>IVA 12%</b>	<b>\$ 2,237.70</b>
<b>COSTO TOTAL</b>	<b>\$ 20,885.18</b>

Tabla 3-12: COSTOS DE FACTIBILIDAD DE LA ALTERNATIVA 2



## 3.3.2.3. FACTIBILIDAD ECONÓMICA

## 3.3.2.3.1. COSTOS DE HARDWARE

BIBLIOTECA  
CAMPUS  
VEÑAS

CANT	DETALLE	PRECIO UNITARIO	TOTAL
4	Antenas tipo grid de 5.8 GHz	\$ 390.00	\$ 1,560.00
2	Router modelo T sunami	\$ 357.00	\$ 714.00
4	Firewall DFL – 800	\$ 700.00	\$ 2,800.00
3	Switch D – LINK 16 Puerto's 10/100/1000 Mbps	\$ 100.50	\$ 301.50
5	Tarjetas de red D-Link 10/100/1000 Mbps	\$ 185.00	\$ 925.00
2	Rack abierto de pared modular de 5 ur	\$ 12.00	\$ 24.00
1	Rack cerrado de 10 ur con ventilador	\$ 100.00	\$ 100.00
2	Patch panel modular de 24 puertos	\$ 26	\$ 52.00
4	Organizadores horizontales 80 *80	\$ 9.00	\$ 36.00
2	Organizadores horizontales 60 * 40	\$ 9.00	\$ 18.00
4	Bandejas metálicas estándar	\$ 10.00	\$ 40.00
16	Cajas sobrepuesta rectangulares	\$ 1.24	\$ 19.84
2	Transiver 10/100/1000 Mbps	\$ 200.00	\$ 400.00
30	Canaletas decorativas	\$ 4.30	\$ 129.00
4	Regletas eléctricas multitomas de 8 servicio	\$ 32.00	\$128.00
20	FACE plate dobles de tipo ejecutivo	\$ 2.40	\$ 48.00
18	Patch cord 10' categoría 6	\$ 5.80	\$ 104.40
25	Patch cord 3' categoría 6	\$ 3.54	\$ 88.5
74	Jack categoría 6	\$ 4.10	\$ 303.00
3 rollos	Cable UTP categoría 6	\$ 267.00	\$ 801.00
2	Bandejas de fibra óptica 4 pares UNICOM	\$ 100.00	\$ 200.00
9	Conectores de fibra óptica multimodo	\$ 4.00	\$ 36.00

3.3.2.5. PLAN DE TRABAJO

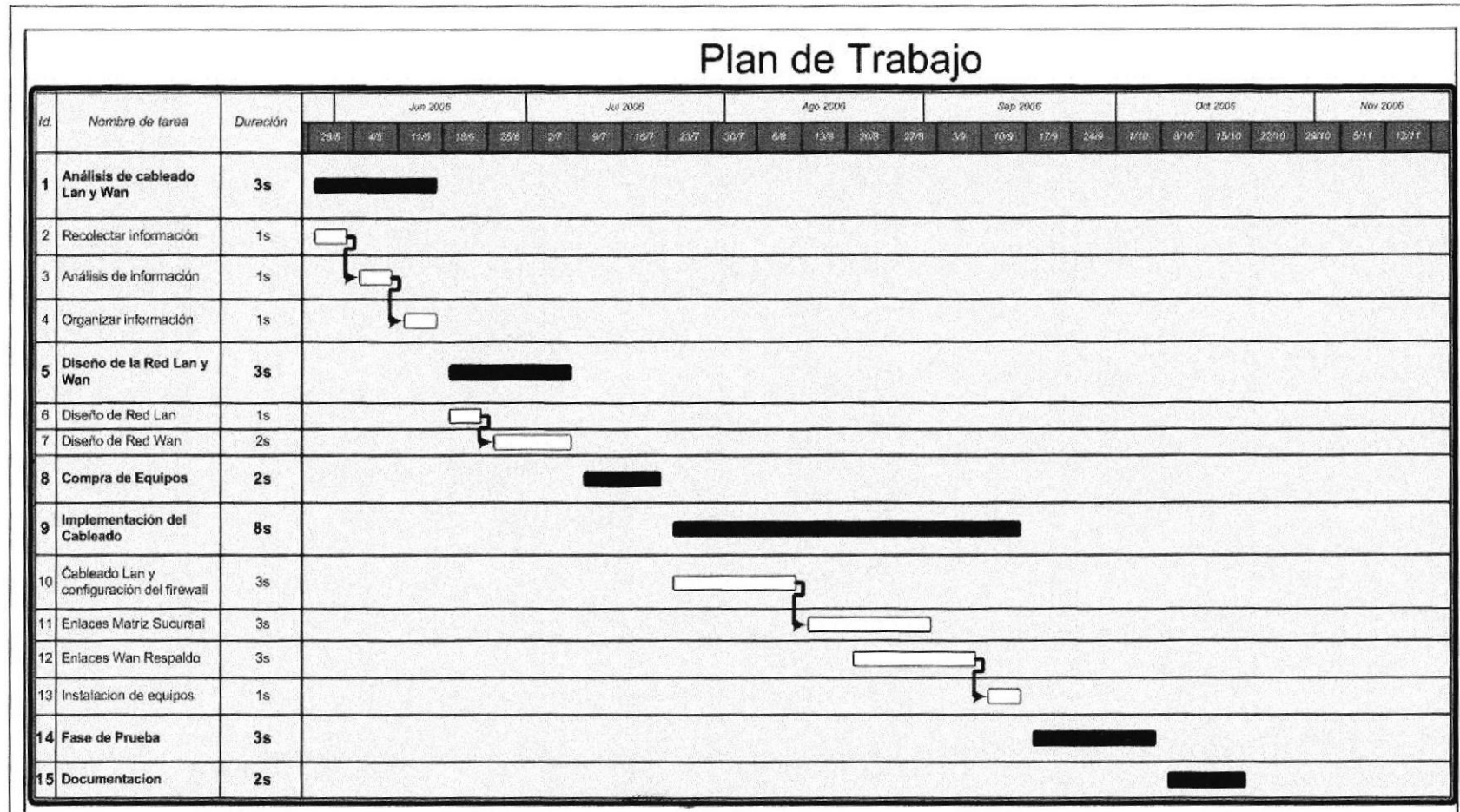


Figura 3-2: PLAN DE TRABAJO ALTERNATIVA 2

### **3.3.2.6. VENTAJAS**

- ✓ Tendremos dispositivos de WAN y LAN enrutamiento y de conmutación seguros protegidos.
- ✓ Con la instalación de los enlaces de respaldo entre matriz y sucursales tendremos la seguridad de estar siempre conectados.
- ✓ Tener una red LAN en cada uno de los edificios mejorara la infraestructura.
- ✓ Con la implementación de la sucursal norte a la red WAN de la empresa, se ganara mayor agilidad y procesos en línea.

### **3.3.2.7. BENEFICIOS**

- ✓ Seguridad en la red interna de la empresa.
- ✓ Seguridad a nivel de la red WAN.
- ✓ Organización en cada uno de los departamentos en el cableado estructurado.
- ✓ Mejor velocidad y tiempo de respuesta.

### **3.3.2.8. GARANTÍAS**

Para esta alternativa nosotros damos un tiempo de garantía de 6 meses para cubrir cualquier tipo de inconvenientes en la red WAN, cabe mencionar que la garantía solo cubre algún desperfectos en los equipos y dispositivos.

### **3.3.2.9. FORMA DE PAGO**

La forma de pago se realizara de la siguiente manera:

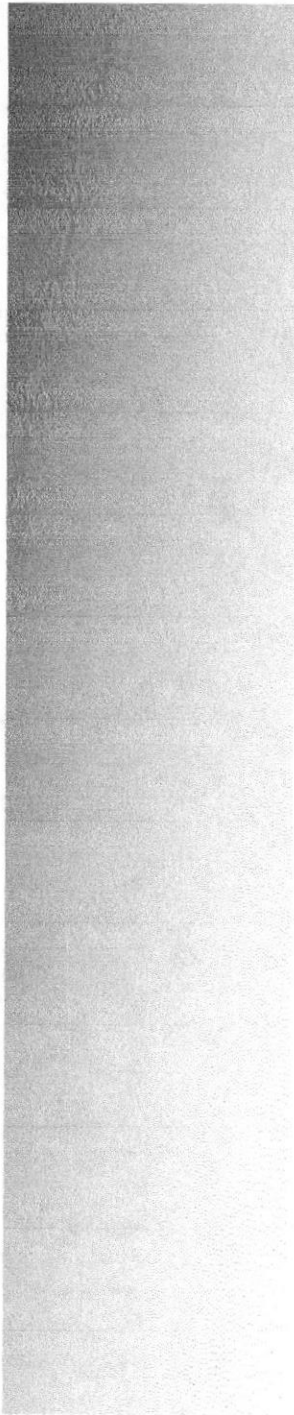
Se la hará en tres pagos:

El primer pago será del 50 % y se realizara el pago al momento de aceptar el contrato de la propuesta escogida.

El segundo pago será del 25 % y se realizara el pago 15 días después de haber firmado el contrato para cubrir gastos de materiales, equipos e imprevistos.

El tercer pago será del 25 % restante, se la efectuara al término la solución escogida.

Cabe recalcar que durante la implementación de la solución escogida, tendrán que ofrecer todas las garantías y facilidades que se requieran para el cumplimiento de la solución.



## CAPÍTULO 4

### IMPLEMENTACIÓN LAN Y WAN

## 4. IMPLEMENTACIÓN

### 4.1. IMPLEMENTACIÓN LAN

#### 4.1.1. DEPARTAMENTO DE CONTABILIDAD MATRIZ

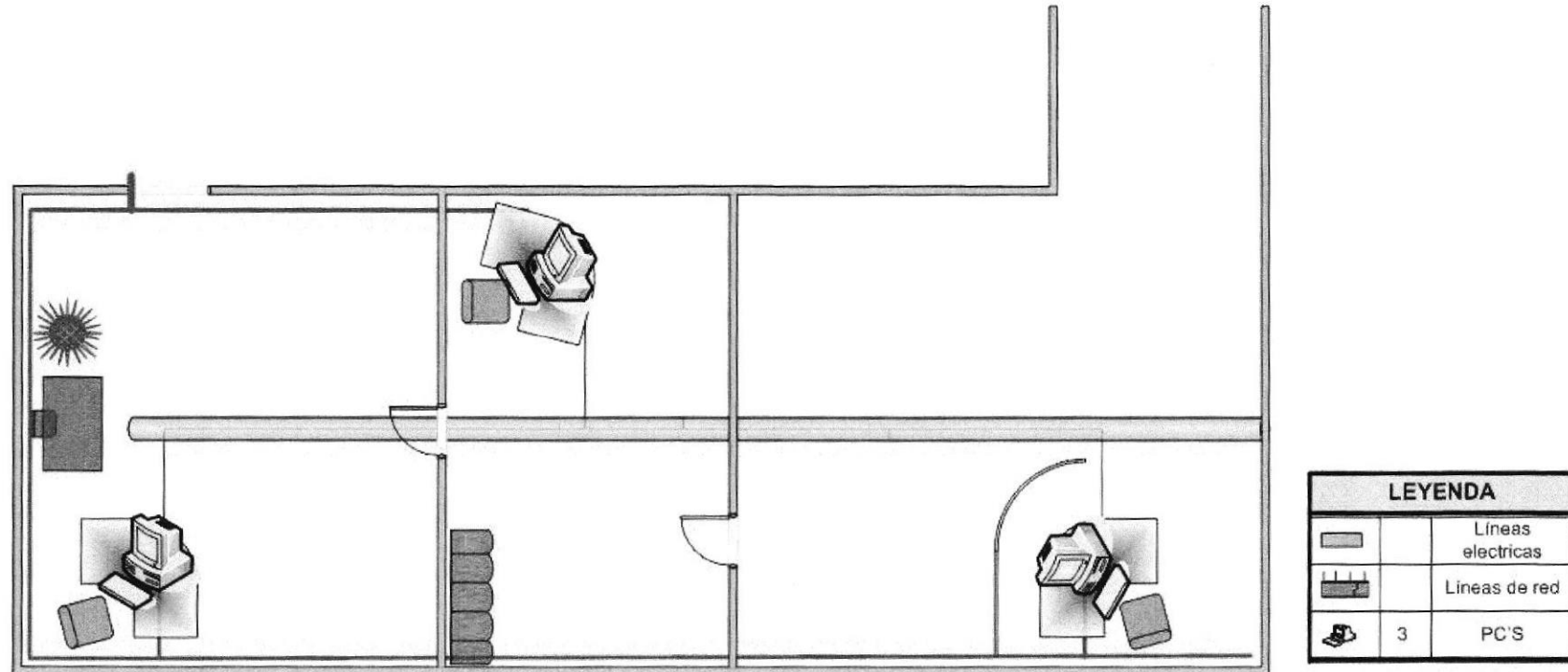


Figura 4-1: DEPARTAMENTO DE CONTABILIDAD MATRIZ



### 4.1.2. LAN SUCURSAL NORTE

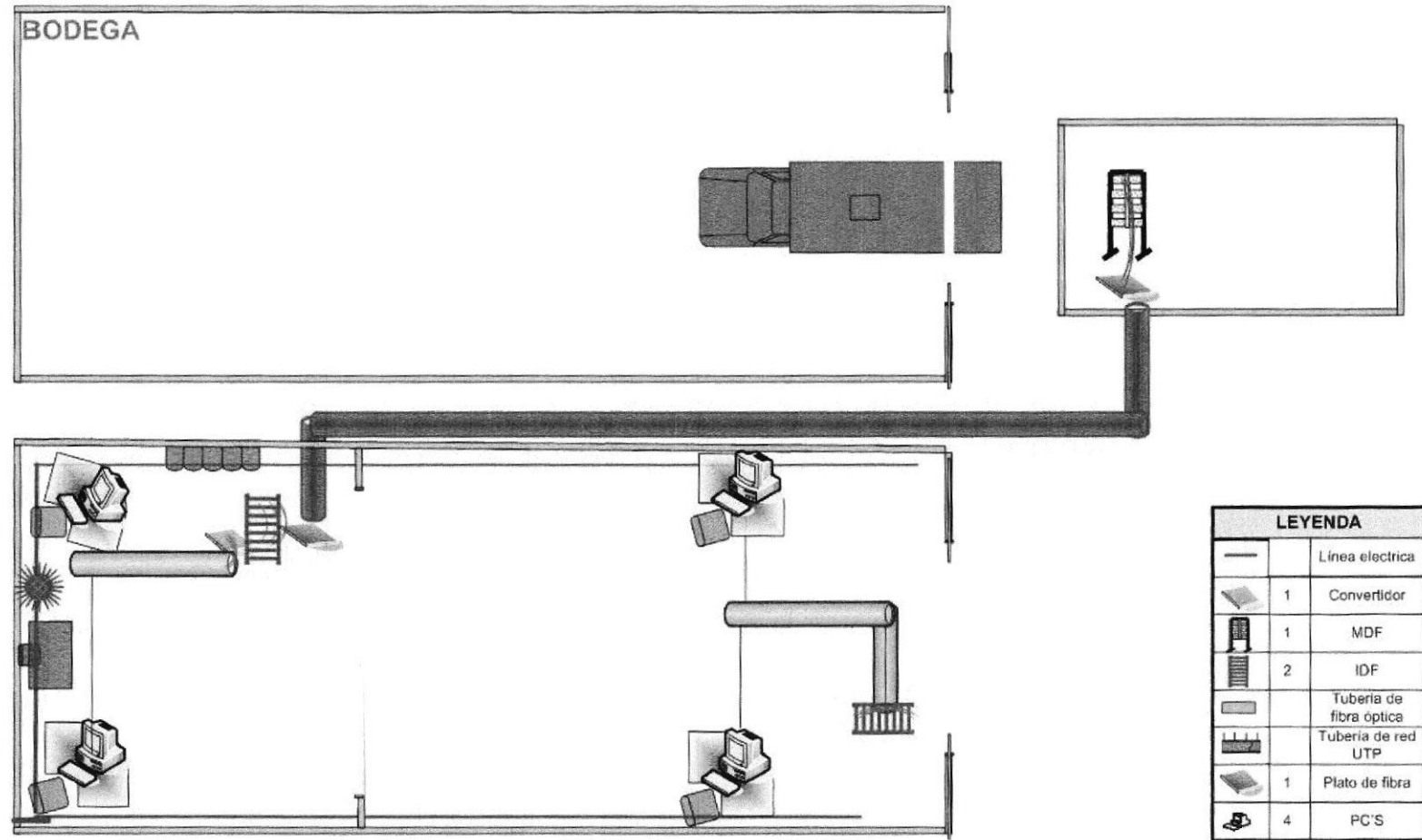


Figura 4-2: LAN SUCURSAL NORTE

## 4.2. IMPLEMENTACIÓN WAN

### 4.2.1. GRAFICO DE RESPALDO MEDIOS MATRIZ SUCURSAL

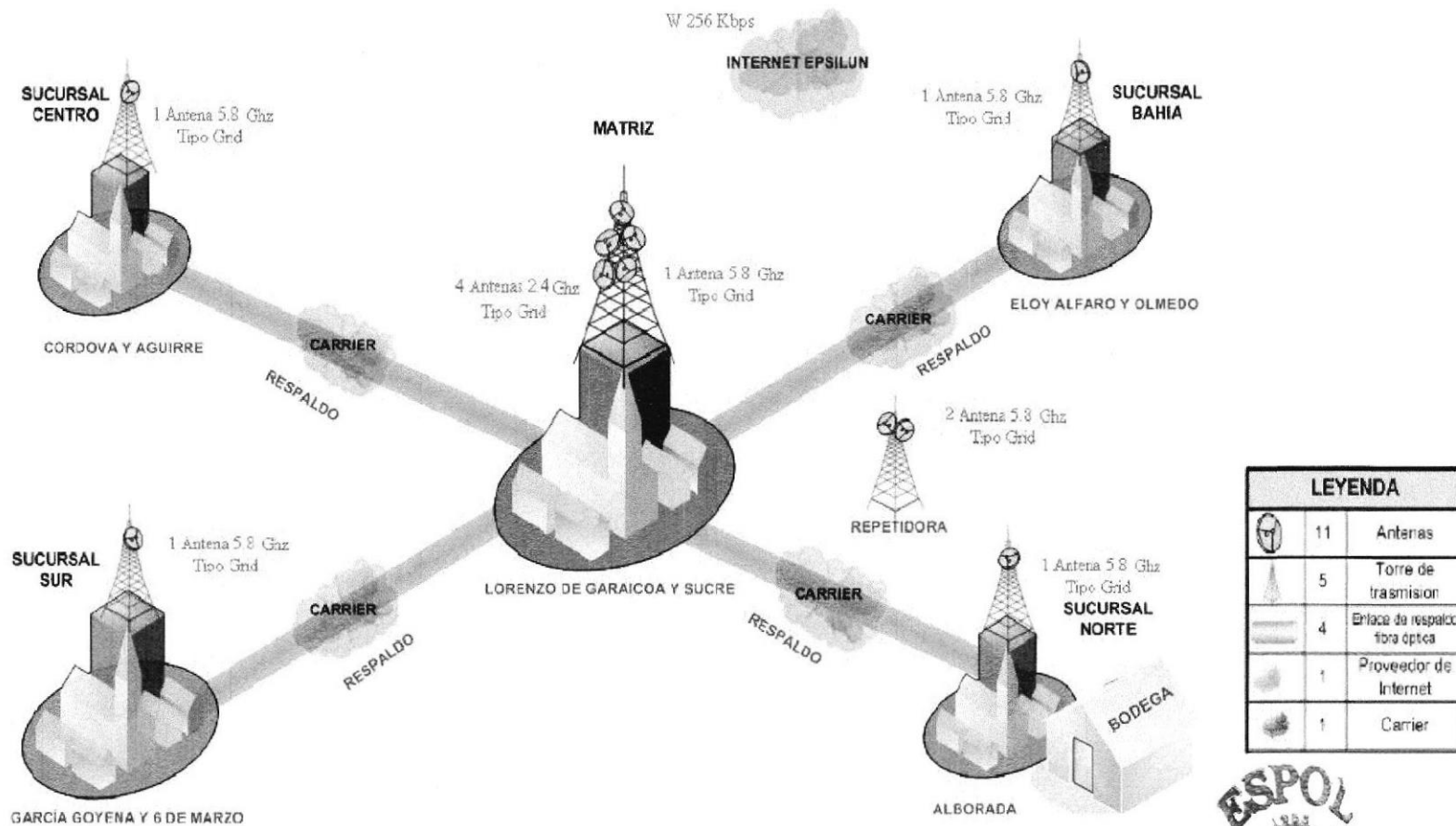


Figura 4-3: ENLACE DE RESPALDO MATRIZ – SUCURSALES

4.2.2. GRAFICO WAN DE COMUNICACIÓN MATRIZ - SUCURSAL NORTE

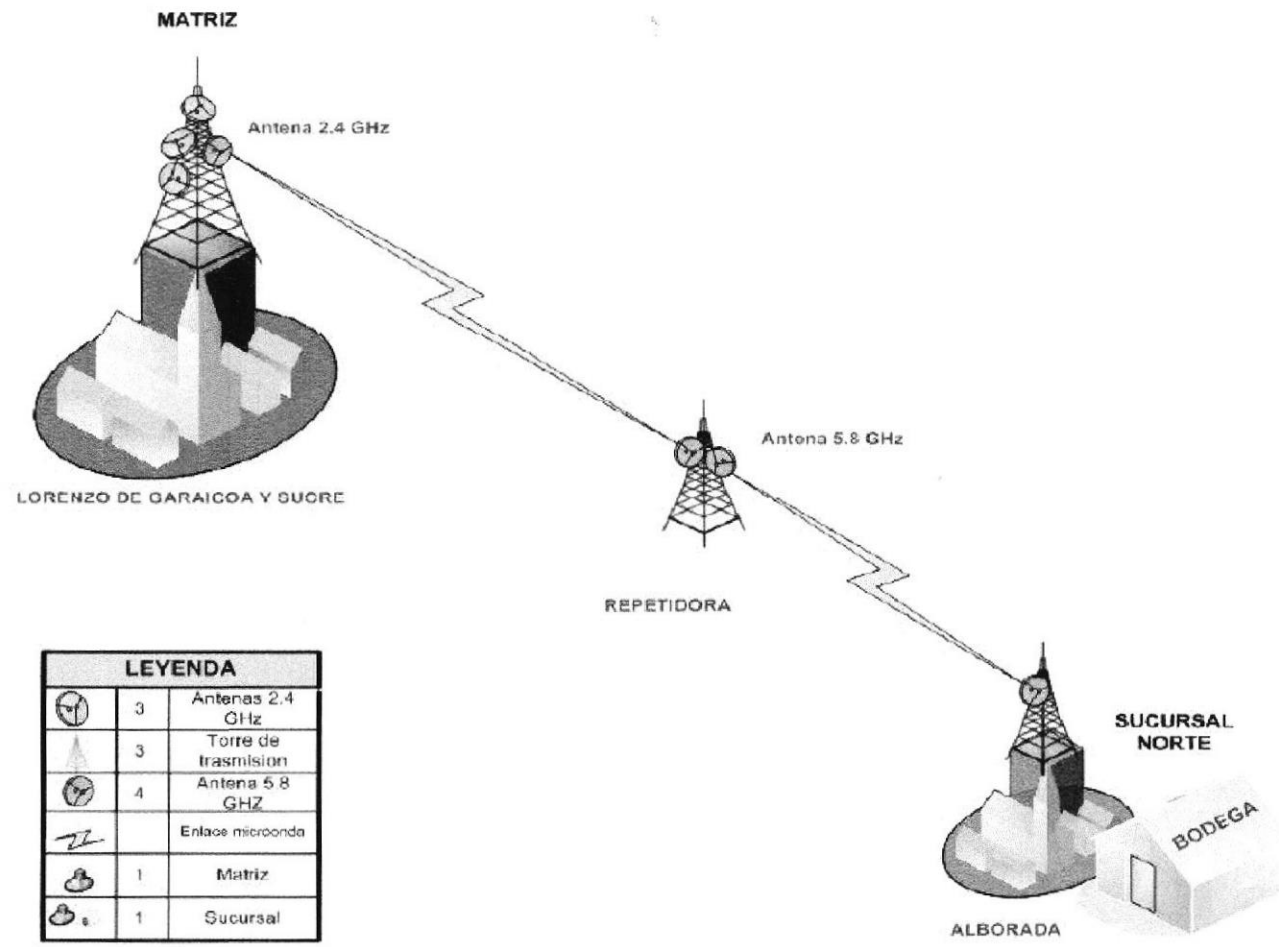


Figura 4-4: ENLACE DE COMUNICACIÓN MATRIZ - SUCURSAL NORTE

### 4.2.3. GRAFICO WAN DE SEGURIDAD MATRIZ – SUCURSALES

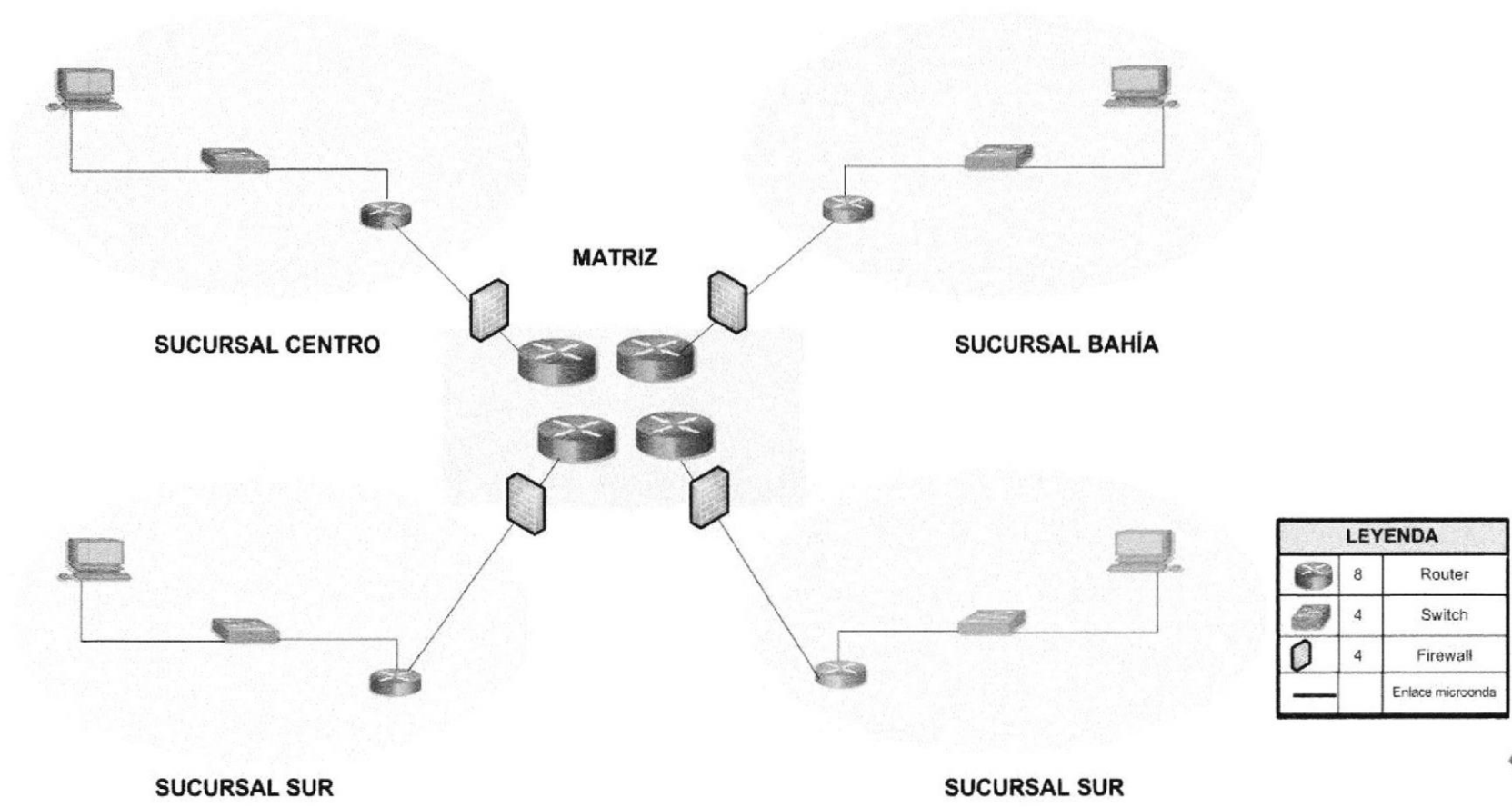
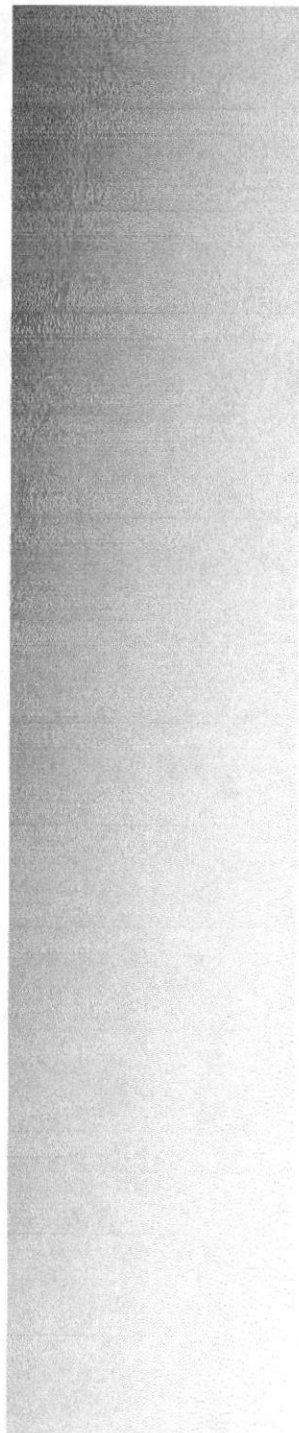


Figura 4-5: SEGURIDAD WAN MATRIZ – SUCURSALES





# CAPÍTULO 5

LINUX

## 5. LINUX

### 5.1. INTRODUCCIÓN.

### 5.2. ¿QUÉ ES LINUX?

Es un sistema operativo orientado a servidores, se distribuye en forma gratuita bajo una licencia de GNU poniéndolo a la disposición de cualquiera que lo desea usar.

Linux Fedora Core es completamente un Sistema operativo para escritorio o servidores, esta creado absolutamente en código abierto a diferencia de Windows que es un sistema operativo propietario (con derechos de autor).

Fedora Core Incluye software para un rango completo de servicios de red, para instalar un sistema con los servicios de red más comunes, también se puede seleccionar paquetes de programas individuales durante la instalación, o instalarlos después.

Fedora Project es el sistema libre de Red Hat, que aunque no da un soporte directo al mismo desde su lanzamiento, si se ha convertido en su patrocinador principal, aunque el código que lo forma está abierto y cualquiera puede incluir y/o ayudar a mejorarlo. Mejorar Linux no se trata de programar únicamente; si sabes inglés y español ya puedes ayudar a traducir información, manuales,... e incluso probar las nuevas aplicaciones es muy útil para comprobar su estabilidad.

Fedora Core (también conocida como Fedora Linux) es una distribución GNU/Linux desarrollada por la comunidad Fedora y promovida por la compañía estadounidense Red Hat.

El objetivo del proyecto Fedora es conseguir un sistema operativo de propósito general y basado exclusivamente en software libre con el apoyo de la comunidad Linux. Los ingenieros de Red Hat continúan participando en la construcción y desarrollo de este proyecto e invitan y fomentan la participación de miembros de la comunidad Linux.

Originalmente, Red Hat Linux fue desarrollado exclusivamente dentro de Red Hat, con la sola realimentación de informes de usuarios que recuperaban fallos y contribuciones a los paquetes de software incluidos; y no contribuciones a la distribución como tal. Esto cambió el 22 de septiembre de 2003, cuando Red Hat Linux se derivó dando origen al Proyecto Fedora que está orientado a la comunidad de usuarios y así mismo, sirve de base para que Red Hat Enterprise Linux se desarrolle con más efectividad y adopte las nuevas características que se añaden en el Proyecto Fedora.

Este modelo es similar a la relación entre Netscape Communicator y Mozilla Firefox, o entre StarOffice y OpenOffice.org, aunque en este caso, el producto comercial resultante es software libre.

### 5.3. CARACTERÍSTICAS DEL LINUX.

En líneas generales podemos decir que dispone de varios tipos de sistemas para poder acceder a ficheros en otras plataformas, Incluye un entorno grafico X Windows, que nada tiene que envidiar a los modernos y caros entornos comerciales.

El sistema Linux es compatible con ciertos estándares de UNIX a nivel de código fuente, incluyendo el IEEE POSIX.1, System V y BSD. Fue desarrollado buscando la portabilidad de las fuentes: encontrará que casi todo el software gratuito desarrollado para UNIX se compila en Linux sin problemas. Y todo lo que se hace para Linux (código del núcleo, drivers, librerías y programas de usuario) es de libre distribución.

Orientado al trabajo en red, con todo tipo de facilidades como correo electrónico por ejemplo, posee cada vez más software de libre distribución que desarrollan miles de personas a lo largo y ancho del planeta.

- ✓ Confiable.
- ✓ Seguro.
- ✓ Sistema multiusuario.
- ✓ Multitasking.
- ✓ Plug and play
- ✓ Alto porcentaje de servidores lo utilizan.
- ✓ El procesador trabajo de modo protegido.



## **5.4. REQUERIMIENTOS DE HARDWARE PARA INSTALACIÓN DE LINUX.**

### **REQUERIMIENTOS DE HARDWARE MÍNIMOS**

- ✓ Procesador Pentium II de 300 MHZ para modo grafico.
- ✓ Memoria 128 RAM.
- ✓ Capacidad de disco duro 6 GB.
- ✓ Unidad de CD – ROM.
- ✓ CDS o DVD para la instalación de Fedora core 3.

### **REQUERIMIENTOS DE HARDWARE RECOMENDADOS**

- ✓ Procesador Pentium III o superior para modo grafico.
- ✓ Memoria 256 RAM o superior.
- ✓ Capacidad de disco duro 20 GB o superior.
- ✓ Unidad de CD – ROM o DVD – ROM.
- ✓ CDS o DVD para la instalación de Fedora core 3.

### 5.5. CONFIGURACIÓN DE BIOS EN EL SERVIDOR LINUX

Debe verificar el sistema de buteo de su servidor en el cual va a instalar Linux. En el teclado presione la tecla Supr o la tecla del, para el cual le permitirá el ingreso al setup.

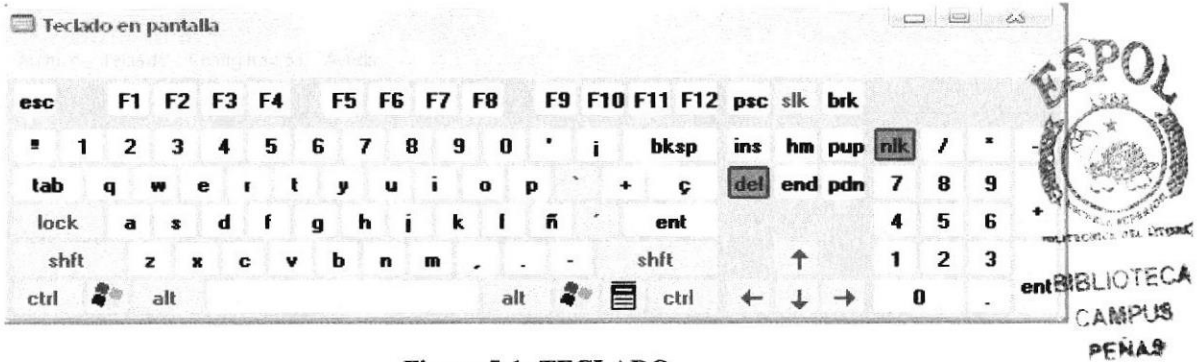


Figura 5-1: TECLADO

Bios, luego de esto aparecerá la pantalla del bios en el cual modificara el sistema.

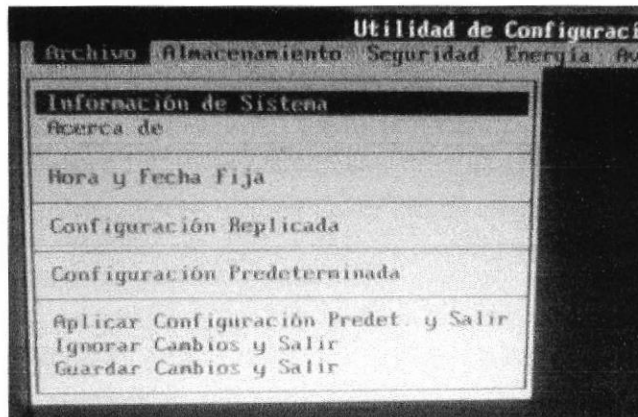


Figura 5-2: BIOS

Ahora elija la pestaña de almacenamiento, y con las teclas direccionales se ubica en orden de arranque, luego presione la tecla enter.

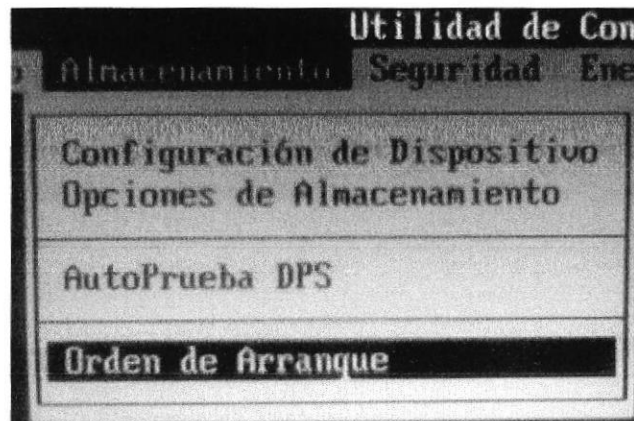


Figura 5-3: ORDEN DE ARRANQUE

Ahora se ubica con las teclas direccionales en la opción de unidad de CD-ROM IDE y presione la tecla enter.

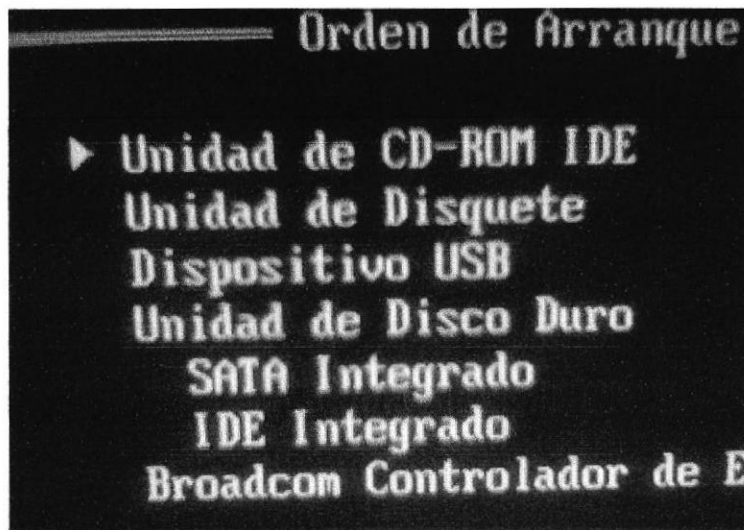


Figura 5-4: UNIDAD DE CD-ROM IDE

Luego se ubica en la opción de Guardar Cambios y Salir, y presione la tecla enter para y guardar los cambios y salir.

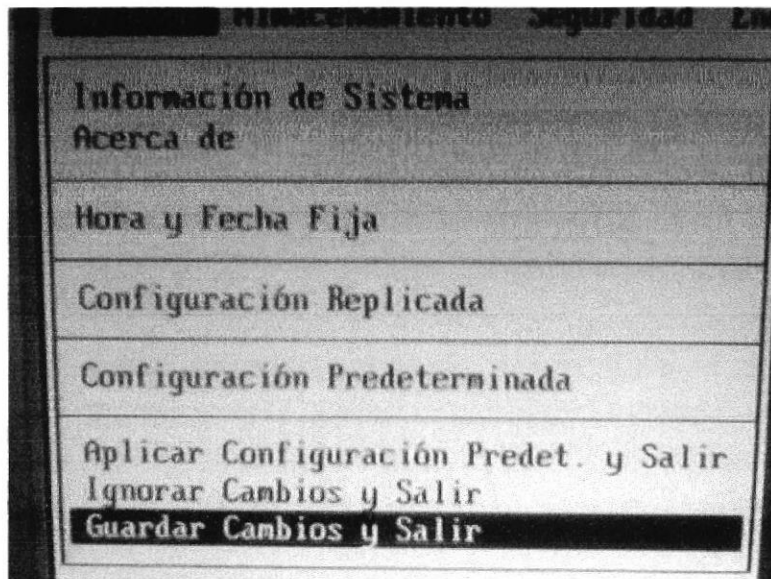


Figura 5-5: GUARDAR CAMBIOS Y SALIR DEL BIOS

## 5.6. EMPEZAR INSTALACIÓN DE LINUX FEDORA CORE 3

Iniciando boteo, si tiene los discos de instalación inserte el disco 1 de Fedora lo colocan en su lector de CD-ROM si esta configurado correctamente el BIOS para leer el CD-ROM al arrancar, debe aparecer es asistente que le ayudara en todo el proceso de la instalación como puede observar en la siguiente figura da un enter y sigue con la instalación.

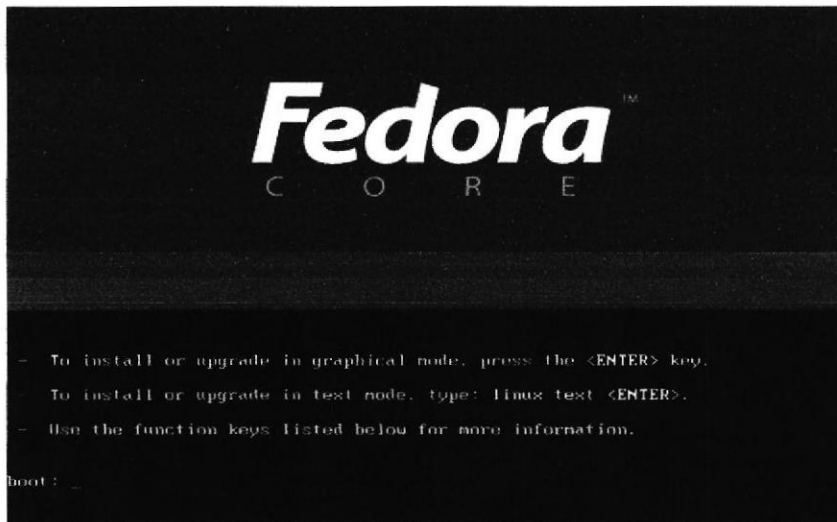


Figura 5-6: INICIANDO BOTEO.

Ahora se iniciará el proceso para detección de hardware y proceso de instalación a través de una consola gráfica, esta secuencia puede durar entre 10 o 15 segundos, mientras observa mensajes descriptivos sobre el sistema.

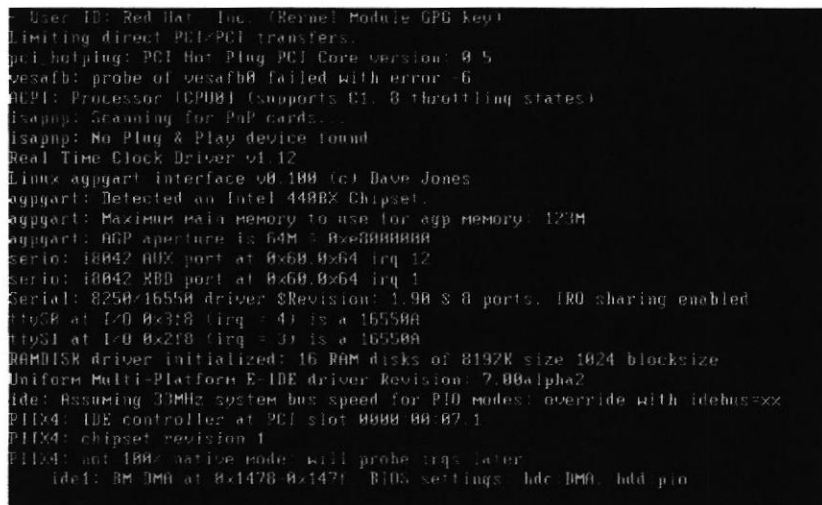


Figura 5-7: DETECTANDO HARDWARE.

Ahora hará la verificación de CDS, será presentado con la opción de realizar una prueba de integridad sobre los CDS de instalación Fedora, esta prueba dura entre 10 y 15 minutos para los 4 CDS de instalación, si no desea realizar esta prueba, seleccione la opción **Skip**, con la tecla tabulador se ubica en skip y de un enter.

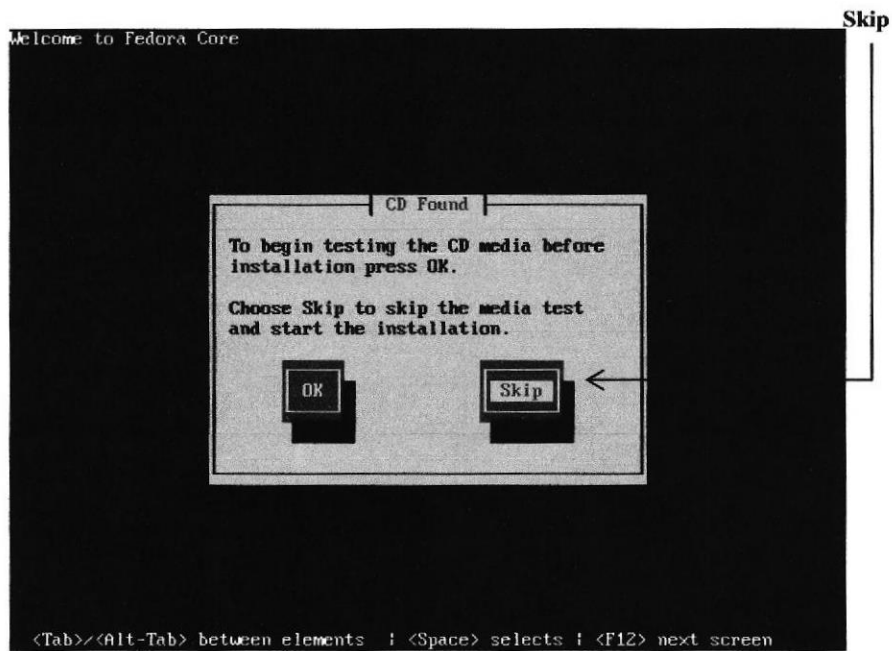


Figura 5-8: VERIFICACIÓN DE DISCOS.

Se despliega un mensaje de bienvenida que da el asistente de Linux con instrucciones de navegación aparece en ingles, simplemente de clic en **next** para continuar.

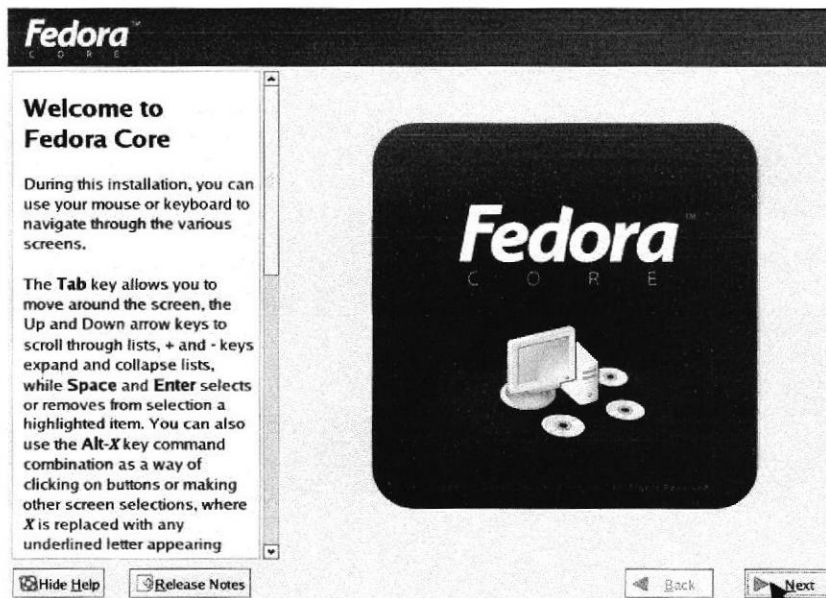


Figura 5-9: BIENVENIDO A FEDORA CORE

Lo siguiente es seleccionar el idioma que desea para su proceso de instalación y sistema, para este caso será castellano **Spanish (Español)**, ahora de clic en **next**.

Spanish

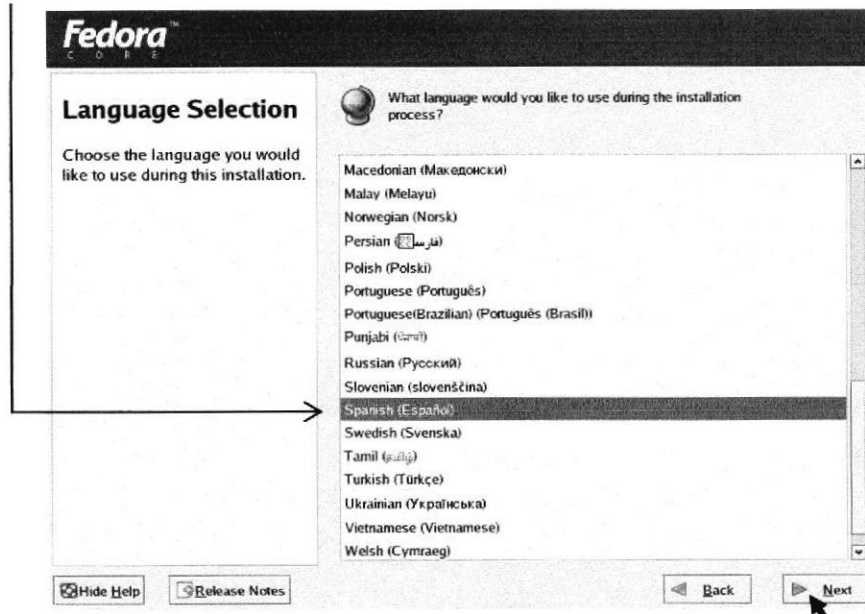


Figura 5-10: SELECCIÓN DE LENGUAJE.

Ahora configure el teclado, seleccione el tipo de teclado en base a su sistema, español si posee un teclado con tecla ñe y caracteres latinos, o bien, estadounidense de lo contrario y de clic en siguiente.

Spanish

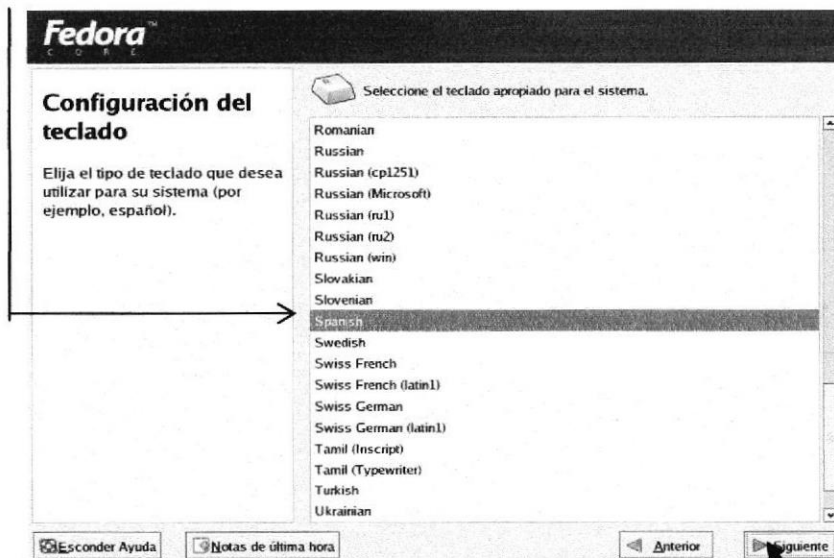


Figura 5-11: CONFIGURACIÓN DEL TECLADO.

Lo siguiente es seleccionar el **tipo de Instalación**, seguido será realizado un proceso de auto-detección para determinar si posee una instalación pre-existente de Fedora, de encontrarse será presentado con una opción de actualización, de lo contrario, podrá elegir entre cuatro modalidades, **escritorio personal**, **estación de trabajo**, **servidor** o

**personalizada**, cada una de éstas presenta una breve descripción de su funcionamiento para esta caso será configuración **personalizada** ahora de clic en **siguiente**.

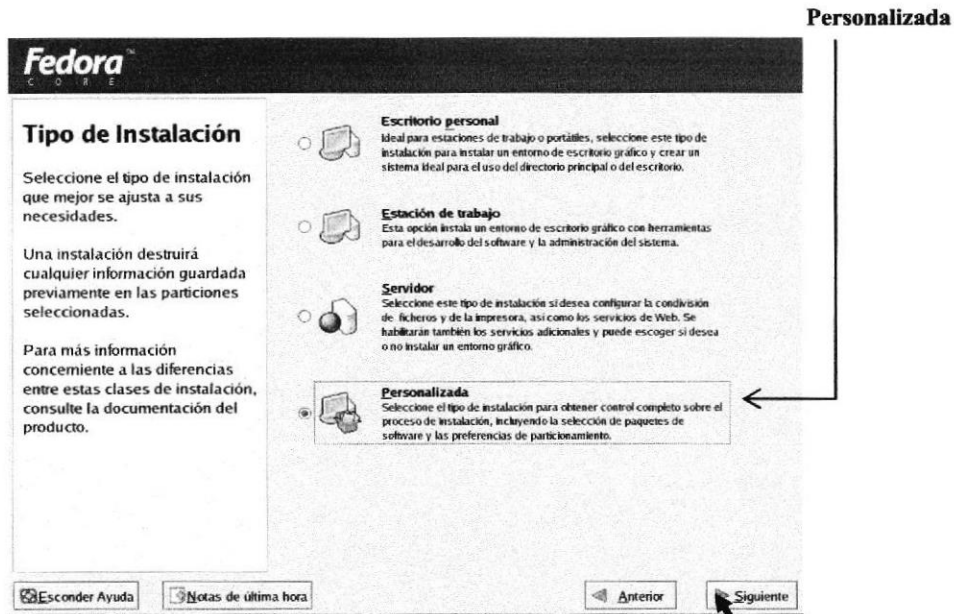


Figura 5-12: TIPO DE INSTALACIÓN.

Ahora seleccione el tipo de particionamiento que va a utilizar.

**Particionamiento automático.**- Como su nombre lo implica, Fedora realiza el particionamiento del disco duro a dimensiones pre-determinadas, sin embargo, esto implica generalmente que debe borrar toda la información existente en su disco duro.

**Partición manual con Disk Druid.**- Para usuarios con amplio conocimiento del proceso de partición, pueden optar por hacer su propia distribución de espacio con esta opción.

Para este caso debe usar **partición manual** y de clic en **siguiente**.

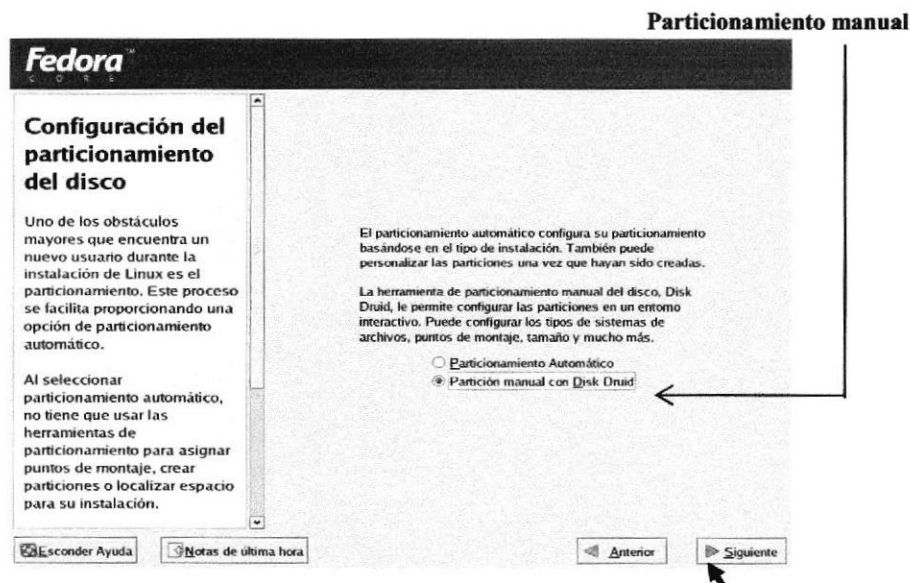


Figura 5-13: CONFIGURACIÓN DE PARTICIONAMIENTO DEL DISCO

Particiones que debe crear:

**Partición root (/).**- La partición root es donde se encuentra el directorio del root en esta configuración de las particiones, todos los ficheros (excepto los que residen en /boot) están en la partición de root por ello sería una buena elección hacer lo más grande posible el tamaño de su partición de root.

**Partición swap.**- Las particiones swap son utilizadas para soportar la memoria virtual con otras palabras, los datos son escritos en la swap cuando no hay bastante memoria disponible para contener los datos que su computador está procesando, el tamaño mínimo para una partición de swap tendría que ser el doble a la cantidad de memoria RAM presente en su computador.

**Una partición /boot.**- La partición boot que se crea en caso de que hubiera otro sistema operativo instalado en el mismo computador (que permite el arranque de su sistema con Linux Fedora Core 3).

Ya que ahora tiene conocimientos de las particiones que va a crear es hora de empezar, el asistente muestra el espacio con el que cuenta en el disco duro, para poder crear las particiones necesarias para la instalación, de clic en **nuevo**.

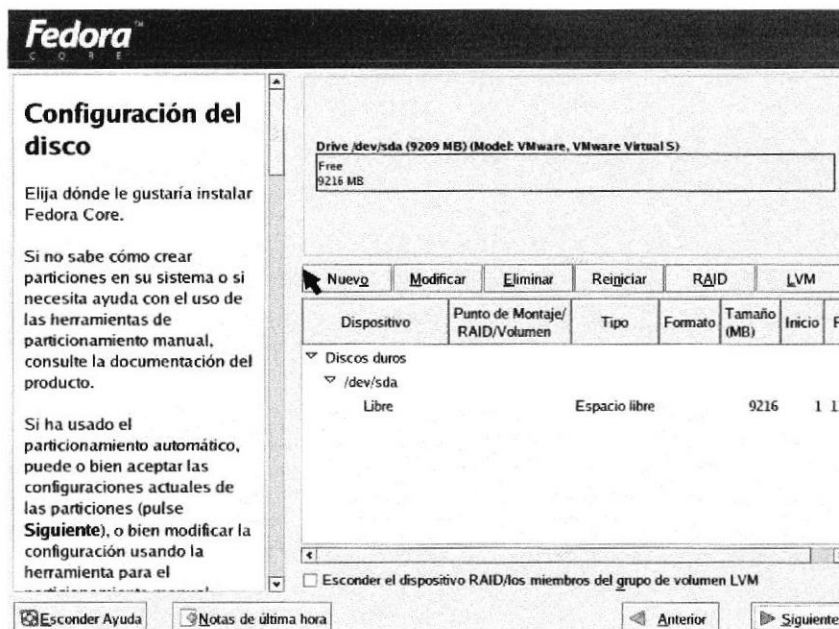


Figura 5-14: CONFIGURACIÓN DEL DISCO

Partición raíz (/), se abre la ventana añadir partición, elija el tipo de partición en este caso es la partición (raíz) / la cual debe seleccionar la casilla punto de montaje y asignar el tamaño en este caso es de 7000 MB la casilla tamaño (MB), de un clic en aceptar.

The screenshot shows the 'Añadir partición' dialog box with the following settings:

- Punto de montaje:** /
- Tipo de sistema de archivos:** ext3
- Unidades admisibles:** sda 9209 MB VMware, VMware Virtual S (checked)
- Tamaño (MB):** 7000
- Opciones de tamaño adicionales:**
  - Tamaño fijo
  - Complete todo el espacio hasta (MB): 1
  - Completar hasta el tamaño máximo permitido
- Forzar a partición primaria
- Buttons:** Cancelar, Aceptar

Figura 5-15: AÑADIR PARTICIÓN RAÍZ (/)

Partición swap, de clic en nuevo a continuación crea la partición swap la cual debe seleccionar en la casilla tipo de sistema de archivo y asignar el tamaño en este caso es el doble del tamaño de la memoria RAM 512 MB en la casilla tamaño (MB), de un clic en aceptar.

The screenshot shows the 'Añadir partición' dialog box with the following settings:

- Punto de montaje:** <Inaplicable>
- Tipo de sistema de archivos:** swap
- Unidades admisibles:** sda 9209 MB VMware, VMware Virtual S (checked)
- Tamaño (MB):** 512
- Opciones de tamaño adicionales:**
  - Tamaño fijo
  - Complete todo el espacio hasta (MB): 1
  - Completar hasta el tamaño máximo permitido
- Forzar a partición primaria
- Buttons:** Cancelar, Aceptar

Figura 5-16: AÑADIR PARTICIÓN SWAP

## LAS PARTICIONES CREADAS

Ahora aparece la siguiente pantalla y puede observar las particiones creadas y de clic en **siguiente** para continuar la instalación.

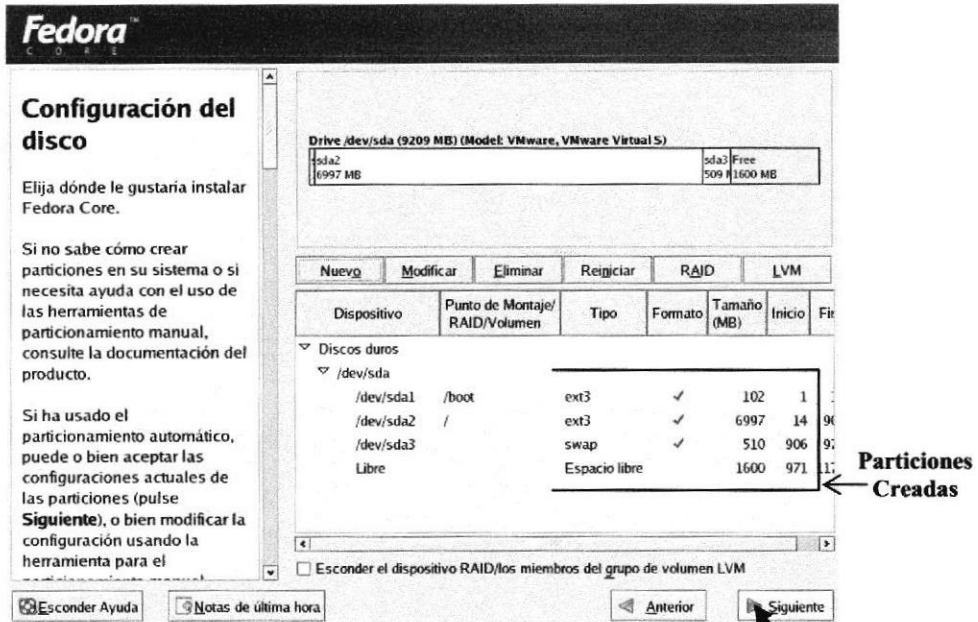


Figura 5-17: PARTICIONES CREADAS EN EL DISCO

Configuración del gestor de arranque, si Fedora será el único sistema operativo instalado en su equipo, este paso no debe ser de mayor trascendencia, pregunta con que sistema operativo desea iniciar la maquina cuando se la encienda, de clic en **siguiente**.

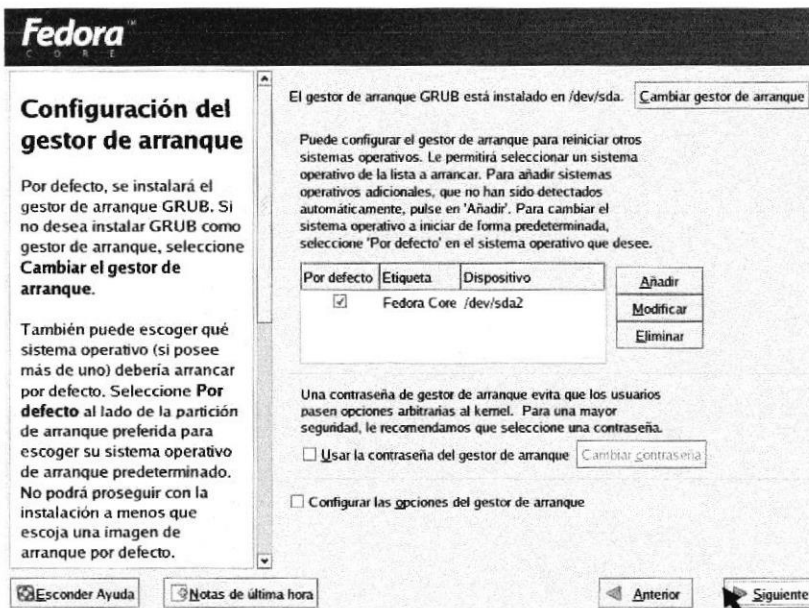


Figura 5-18: CONFIGURACIÓN GESTOR DE ARRANQUE.

Configuración de la red, el asistente le muestra la siguiente pantalla que le permite configurar los dispositivos de red que tenga el computador, Linux reconoce la tarjeta de red como eth0, en este caso no hará ningún tipo de configuración a la tarjeta de red, ya que la hará en modo de comando cuando tenga instalado el sistema operativo, de clic en **Siguiente**.

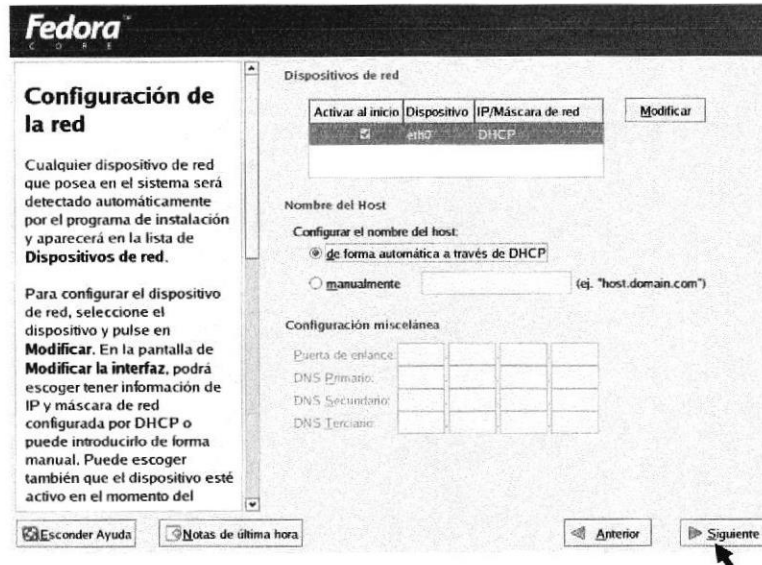


Figura 5-19: CONFIGURACIÓN DE LA RED

Configuración del cortafuegos ("Firewall"), aquí debe especificar si desea instalar un mecanismo de Firewall para proteger su sistema, de ser así, también tiene la opción de habilitar determinados servicios para que éstos no sean afectados por el "Firewall", tales como SSH, Servidores Web, Servidores de Correo y FTP, pero para este caso debe seleccionar ningún cortafuegos, ya que lo hará en modo de comando cuando tenga instalado el sistema operativo y da clic en **Siguiente** ahora aparece un mensaje de advertencia por no habilitar el cortafuego, de clic en **proceder** y siga con la instalación.

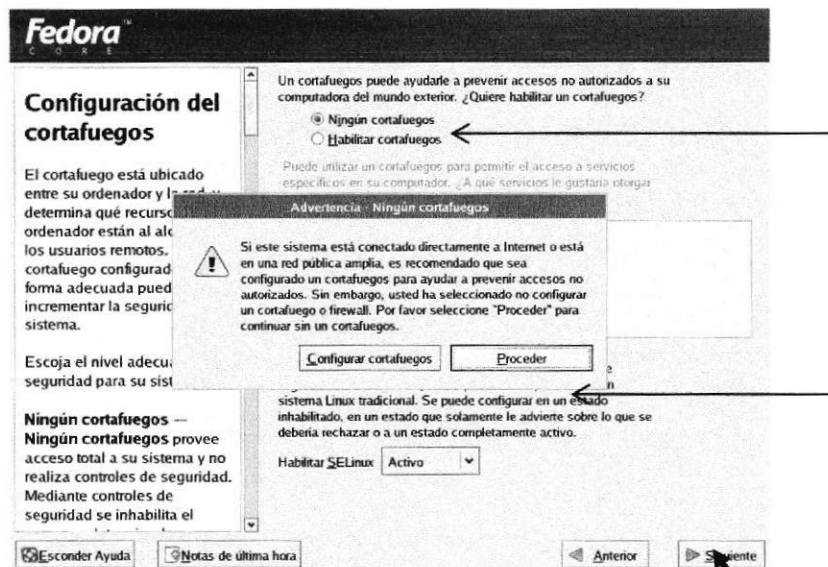


Figura 5-20: CONFIGURACIÓN DEL CORTAFUEGO.

A continuación, puede seleccionar un soporte de idioma, esto le permite instalar y utilizar varios idiomas en el sistema, después de la instalación, de clic en **siguiente** y siga con la instalación.

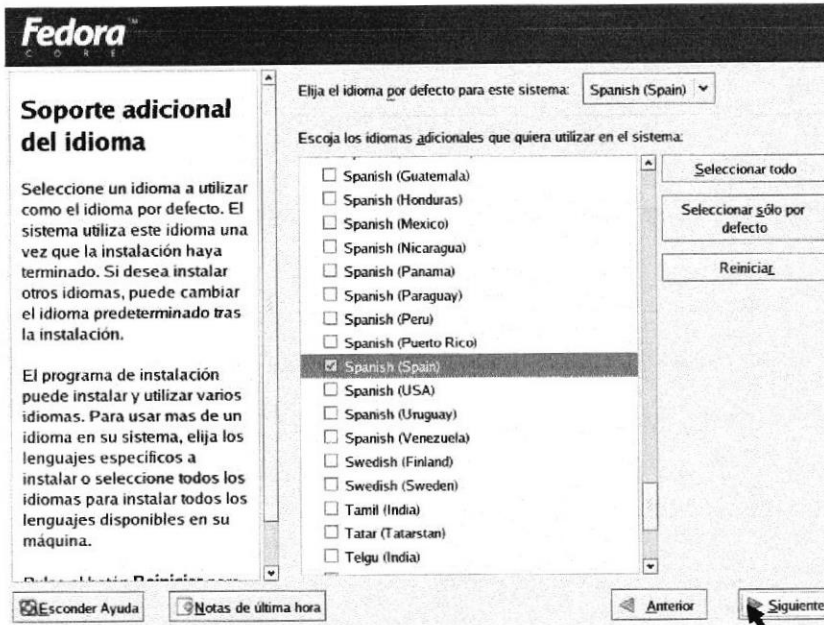


Figura 5-21: SOPORTE ADICIONAL DEL IDIOMA.

Aquí debe definir la zona horaria para su instalación debe configurarla, seleccione la ubicación geográfica de su computador, en el mapa interactivo pulse la zona horaria que se marca con una x roja y de clic en **siguiente**.



Figura 5-22: SELECCIÓN DEL HUSO HORARIO.

Ahora defina la contraseña al súper usuario **root**, éste es el usuario maestro de la instalación y tiene control absoluto de acceso sobre toda aplicación en Fedora, debe

asignar la contraseñas y la confirmación en las casillas respectivas, y de clic en siguiente.

Figura 5-23: CONFIGURAR CONTRASEÑA DEL ROOT

A continuación debe seleccionar aplicaciones y paquetes que desea instalar se selecciona la casilla del paquete o aplicación que se requiera para la instalación y de clic en siguiente.

Figura 5-24: SELECCIÓN DE GRUPOS PAQUETES.

Ahora aparece la pantalla, que indica que esta listo para la instalación, de clic en siguiente.

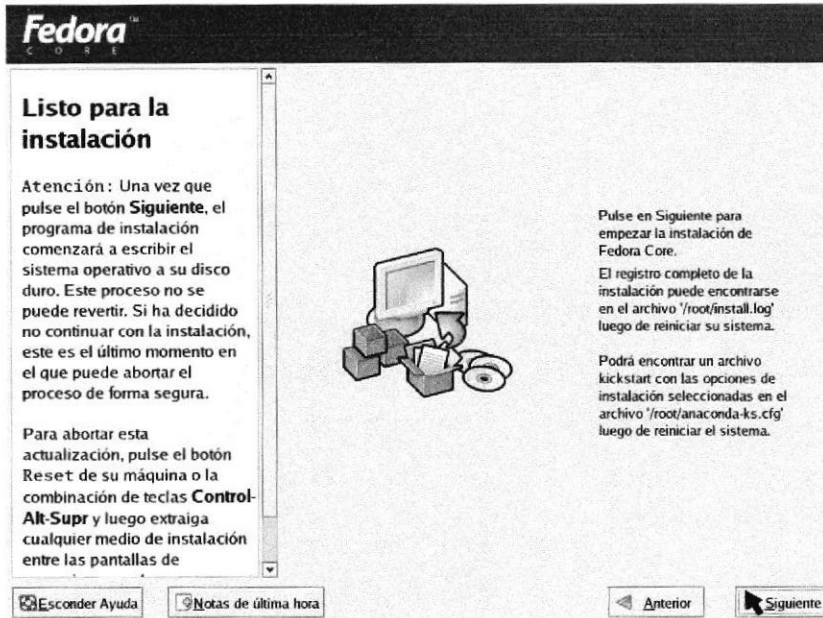


Figura 5-25: LISTO PARA LA INSTALACIÓN

Se inicia la instalación, dependiendo de su hardware, este paso puede demorar entre 20 o 40 minutos, asegúrese también de tener cerca de su computador los discos de instalación y no dejarla desatendida, ya que durante este proceso necesita colocar los distintos CDS conforme los requiera su instalación, pulse **continuar**.

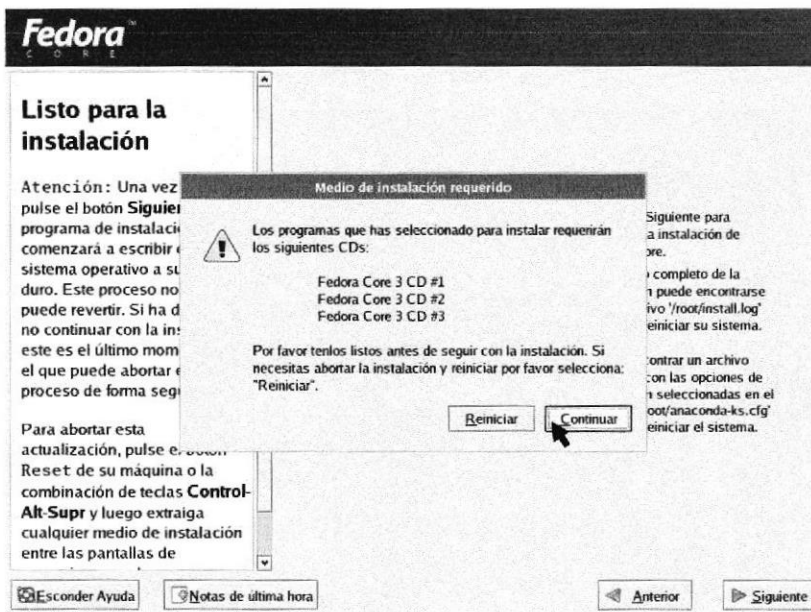


Figura 5-26: MEDIOS DE INSTALACIÓN REQUERIDOS

Ahora la instalación requiere el disco 2 para poder seguir con la misma, inserte el disco 2 y de clic en **aceptar** para continuar.

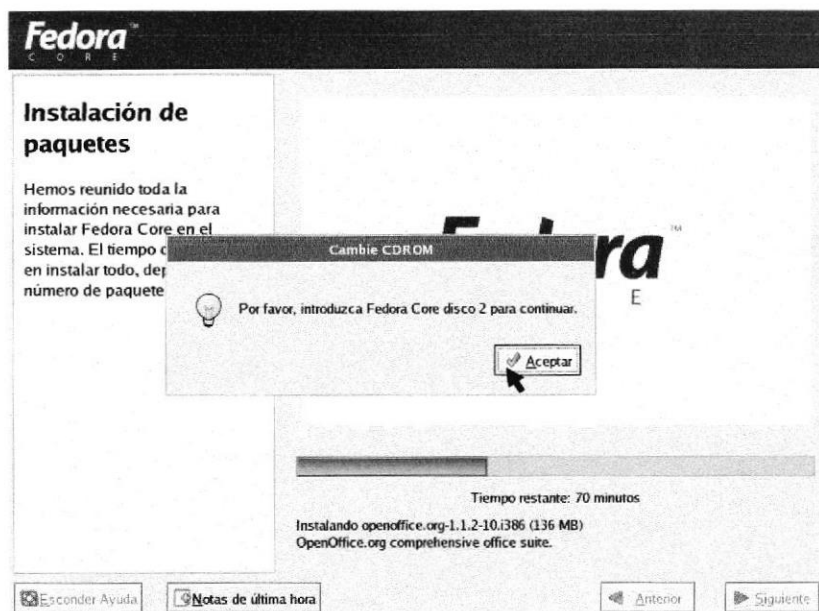


Figura 5-27: INSERTAR DISCO 2.

Ahora la instalación requiere el disco 3 para poder seguir con la misma, inserte el disco 3 y de clic en **aceptar** para continuar.

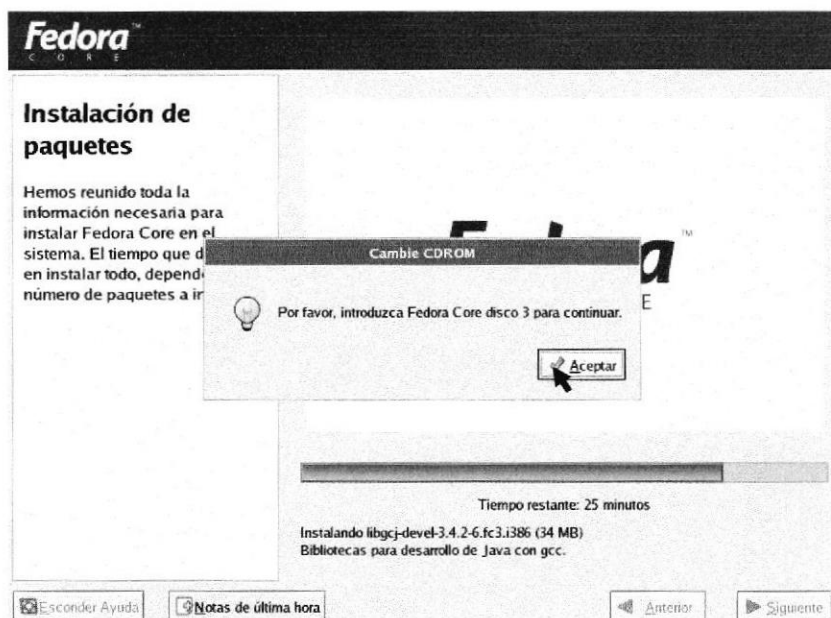


Figura 5-28: INSERTAR DISCO 3.

Ultimo paso, felicidades término de instalar satisfactoriamente Fedora Linux ahora sólo de clic en **reiniciar**.



**Figura 5-29: INSTALACIÓN COMPLETA.**

El sistema se reinicia y empieza a reconocer e iniciar el hardware y verificar ficheros, para cargar el sistema operativo.

```

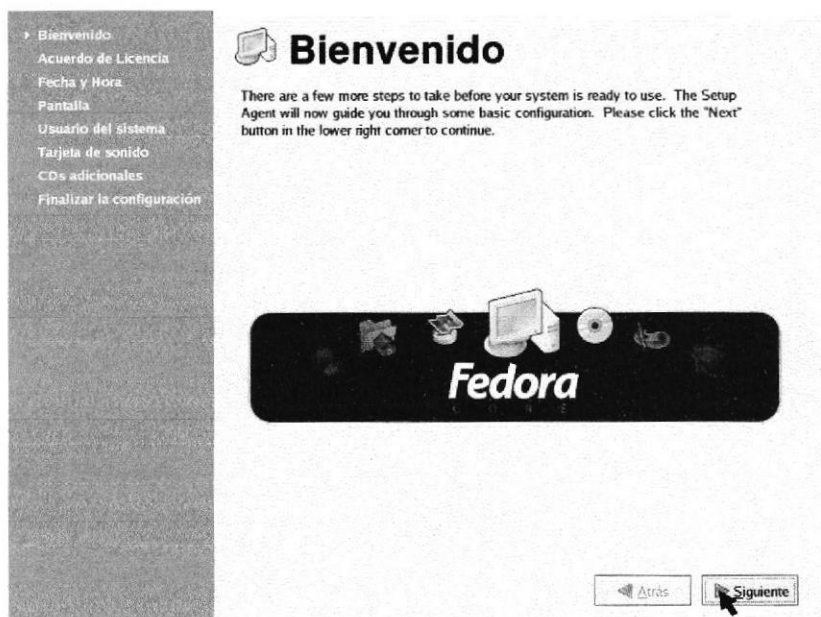
Press 'I' to enter interactive startup.
Iniciando udev: [ OK ]
Iniciando el hardware... almacenamientored audio hecho [ OK ]
Configurando parámetros del kernel: [ OK ]
Configuración del reloj (localtime): jue may 31 13:18:24 ET [ OK ]
Cargando mapa del teclado predeterminado (es): [ OK ]
Configuración del nombre de la máquina localhost.localdomain [ OK ]
Verificando el sistema de archivos raíz: [ OK ]
Remontando sistema de archivos raíz en modo de lectura y escritura [ OK ]
Configurando gestor de volúmenes lógicos: [ OK ]
Verificando sistema de archivos [ OK ]
Montando sistema de archivos local: [ OK ]
Activando cuotas del sistema de archivos local: [ OK ]
Activando espacio swap: [ OK ]

```

**Figura 5-30: CARGANDO SISTEMA.**

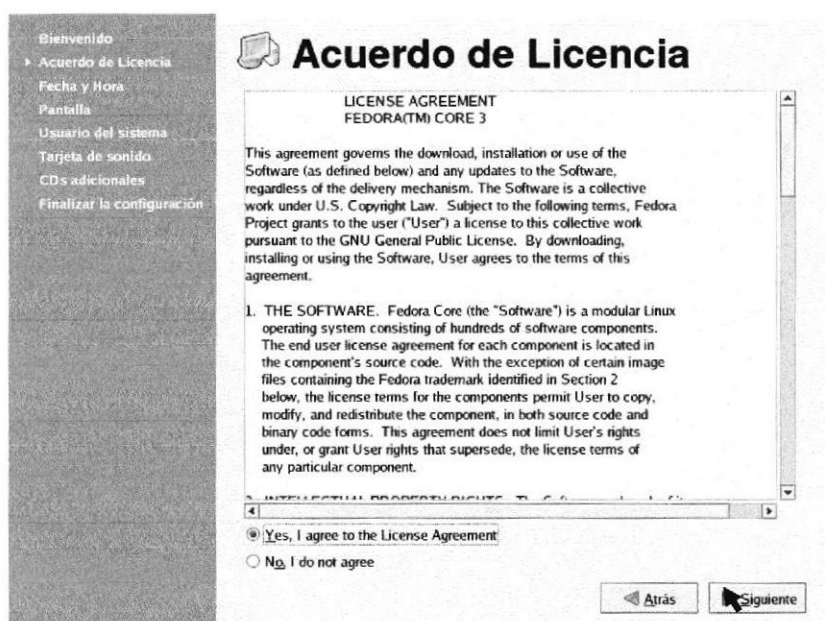
## 5.7. CONFIGURACIONES POST DE LINUX FEDORA CORE 3

Una vez que termina de reiniciar aparece una pantalla de bienvenida, un asistente para hacer configuraciones básicas y de clic en **siguiente** para continuar.



**Figura 5-31: BIENVENIDO AL SISTEMA**

Ahora, el asistente presenta el acuerdo de licencia del Linux seleccione **Yes**, para continuar y de clic en **siguiente**.



**Figura 5-32: ACUERDO DE LICENCIA.**

A continuación configure la fecha y hora del sistema y de clic en **siguiente**.

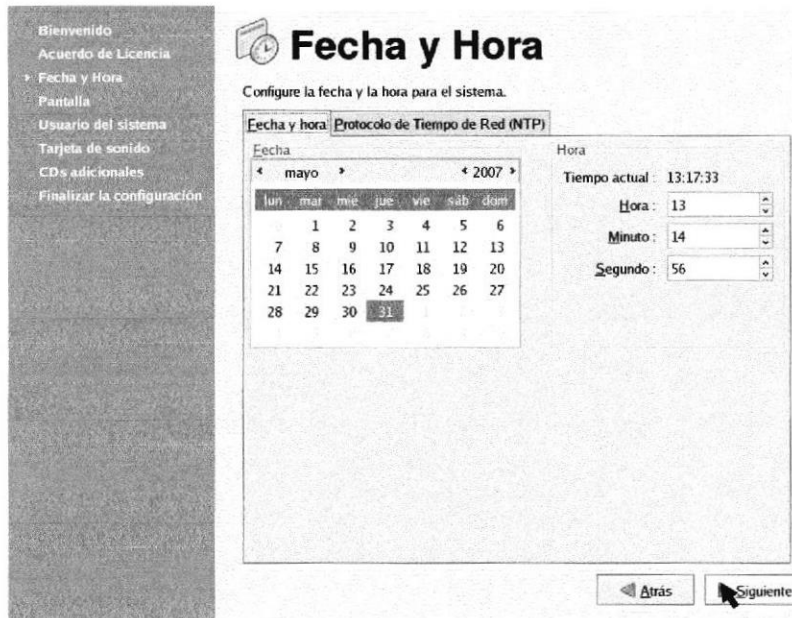


Figura 5-33: FECHA Y HORA.

Ahora seleccione la resolución de la pantalla y profundidad del color que desea utilizar y de clic en **siguiente**.

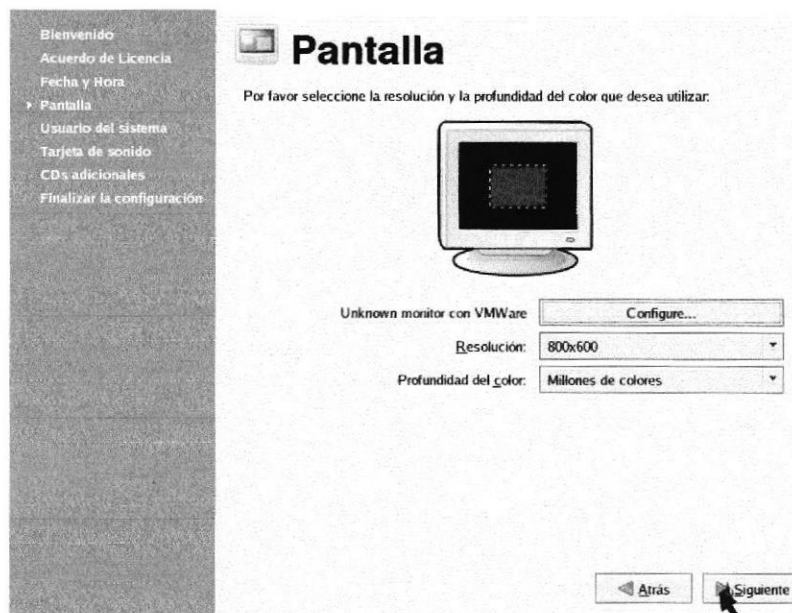


Figura 5-34: RESOLUCIÓN DEL MONITOR DE PANTALLA.

Ahora debe crear un usuario de sistema no administrativo **username** debe llenar las casillas requeridas y de clic en **siguiente**.

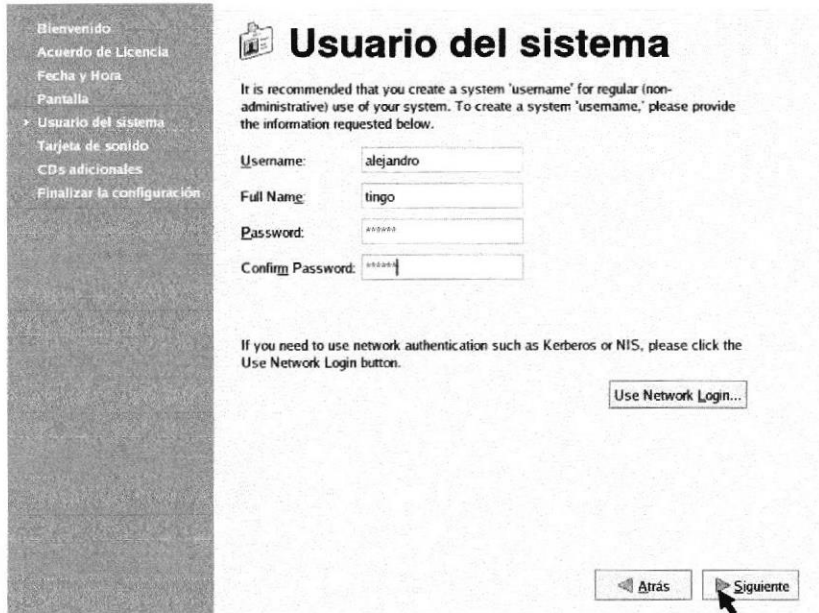


Figura 5-35: USUARIO DEL SISTEMA.

El sistema detecta una tarjeta de sonido en el computador mostrándole información de ella, si se desea puede realizar una prueba de sonido, y de clic en **siguiente**.

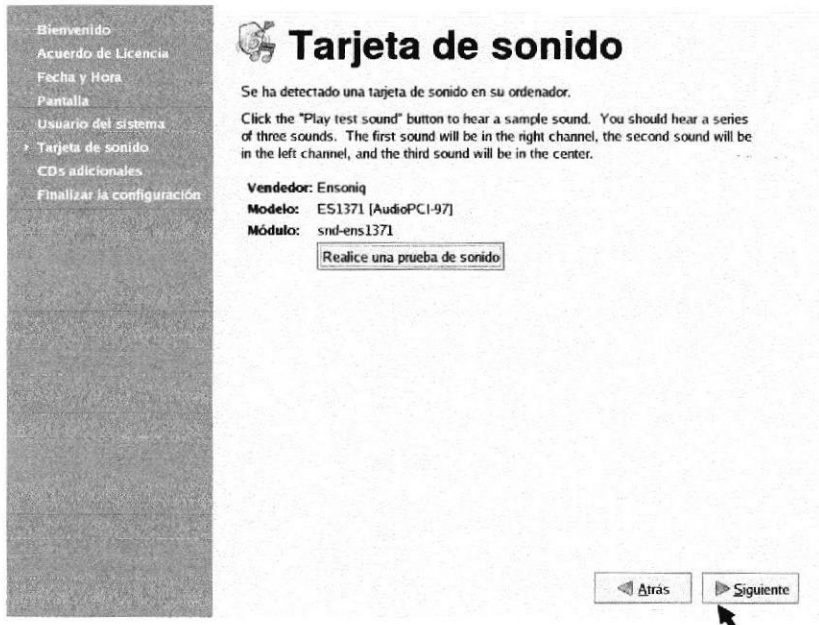


Figura 5-36: TARJETA DE SONIDO.

Ahora el asistente muestra un mensaje de finalizar la post configuración, le indica que el sistema esta listo para usarse de clic en **siguiente**.



Figura 5-37: FINALIZACIÓN DE CONFIGURACIÓN.

## 5.8. INICIANDO CON EL SISTEMA DE MODO GRAFICO.

Ahora debe ingresar el usuario con el cual desee entrar al sistema para este caso ingrese el súper usuario **root** y de **enter**.



Figura 5-38: INGRESO DE USUARIO.

Ahora debe ingresar la **contraseña** para autenticar el usuario si la contraseña es la correcta de un **enter** y listo ingrese al sistema.

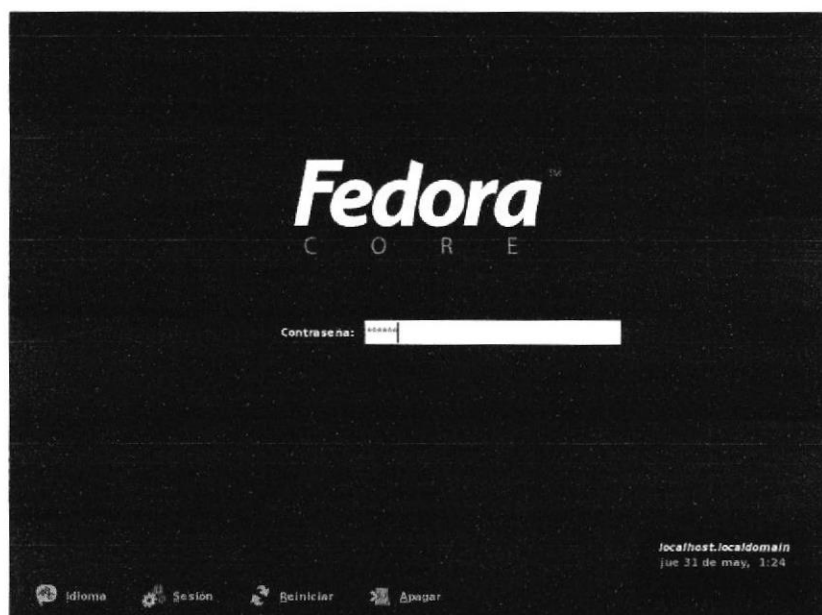


Figura 5-39: INGRESO DE CONTRASEÑA.

Listo Ahora muestra el entorno grafico, el escritorio de Linux.



Figura 5-40: ESCRITORIO DE LINUX

Para abrir un terminal, de clic en Aplicaciones, seleccione **herramientas de sistemas** y de clic en **Terminal**

**Nota:** El Terminal es donde hará las debidas configuraciones mas adelante.

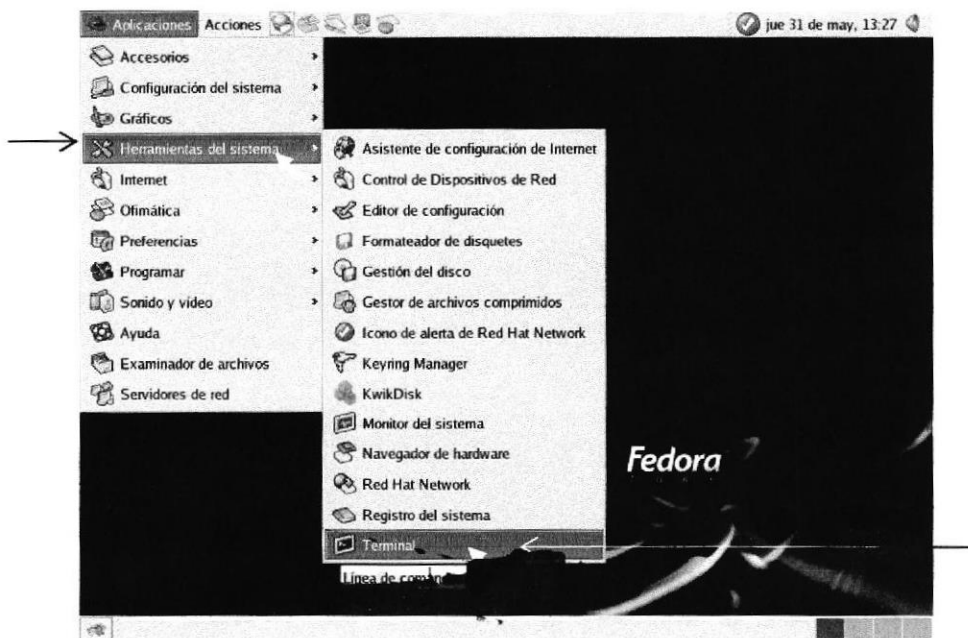


Figura 5-41: INGRESAR AL TERMINAL.

Listo ya esta en el terminal que realizara configuraciones mas adelante.

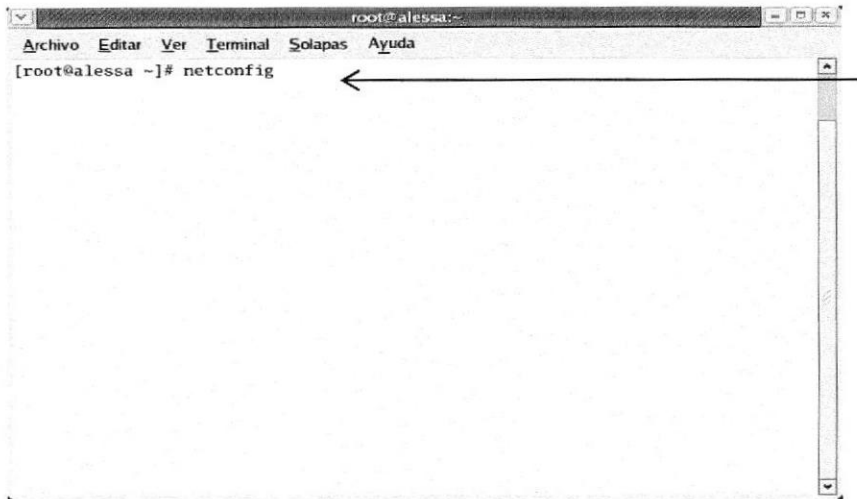


Figura 5-42: TERMINAL

## 5.9. COMANDOS BÁSICOS LINUX

Comando	Descripción	sintaxis
Cd	Ingresar a un directorio.	cd /deber
Cd	Para salir de un directorio.	cd..
chown	Cambia de usuario y grupo a un archivo.	chown squid:squid claves
Cp	Copia archivos de un directorio a otro.	cp deber /etc/
Mkdir	Crea un directorio.	mkdir topico
Mv	Mueve un archivo(s) a un directorio.	mv tarea.txt /topico
Adduser	Añadir usuario de sistema.	adduser administrador
Passwd	Asigna una clave a un usuario.	passwd administrador
Man	Ayuda del comando especificado.	man squid
Ls	Ver el contenido del directorio.	ls --

ls -a	Enlista archivos ocultos.	ls -a
Pwd	Muestra la ruta del directorio actual.	pwd
Rm	Borra un fichero.	rm borrador.doc
rm -r	Borra todo un directorio.	rm -r /topico
Rmdir	Borra un directorio vacío.	rmdir /nueva_carpeta
Vi	Edita un archivo.	vi deber.doc
Date	Muestra la fecha del sistema.	date
Gzip	Comprime un archivo.	gzip trabajo
Gunzip	Descomprime un archivo.	gunzip trabajo
ping	Herramienta de red para comprobar entre otras cosas si llegamos a un host remoto.	ping 200.168.41.1
ifconfig	Verifica si esta habilitada la ip del servidor.	ifconfig
chmod	Este comando da permisos de lectura, escritura a cualquier archivo.	chmod 600 /etc/squid/caves
mail	Sirve para revisar los correos de los usuarios.	mail
Slocate	Sirve para buscar directorios, archivo.	slocate dhcp
telnet	Permite una conexión de forma remota hacia el servidor por medio de la dirección IP.	telnet 200.168.41.1
Clear	Sirve para limpiar pantalla.	clear
rpm -q	Sirve para verificar si esta instalado un paquete	rpm -q samba
Rpm -i	Sirve para instalar un paquete.	rpm -i samba
rpm -e	Sirve para desinstalar un paquete.	rpm -e samba

mount	Montar unidades de disco duro, diskette, cdrom.	mount /media/cdrom
umount	Desmontar unidades de disco duro, diskette, cdrom.	umount /media/cdrom
Find	Busaca en todo el disco.	Find/
Slocate	Buscar ficheros específicamente.	Slocate< fichero>
Shutdown poweroff	Apagar sistema.	Shutdown poweroff
Exit Logout	Salir de una consola virtual.	Exit Logout
Startx	Reiniciar el modo gráfico.	Startx
Reboot	Reiniciar el sistema.	Reboot

Tabla 5-1 COMANDOS BÁSICOS DE LINUX

## 5.10. CONFIGURACIÓN DE TARJETA DE RED

Habrà el terminal

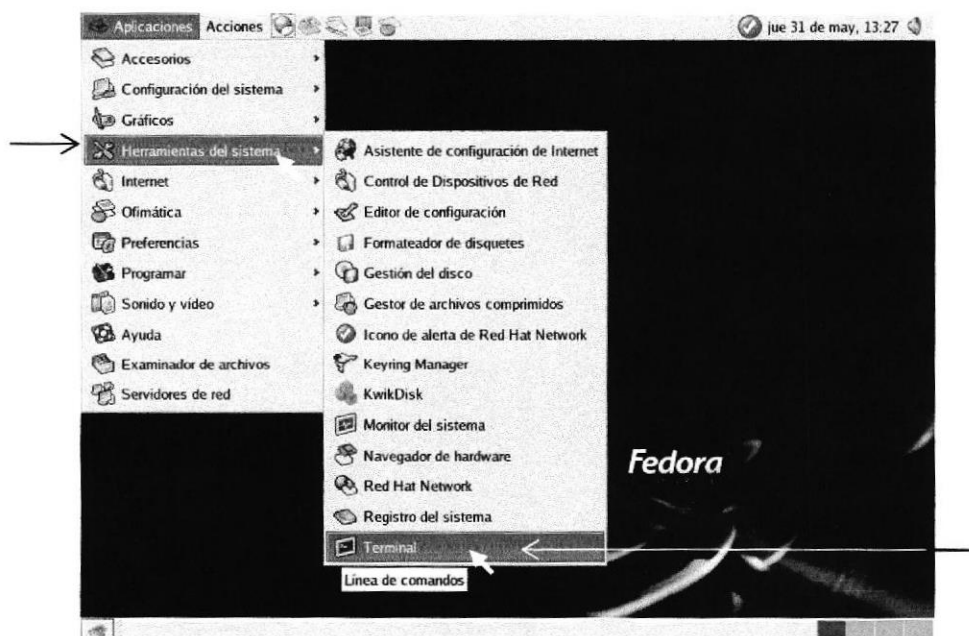
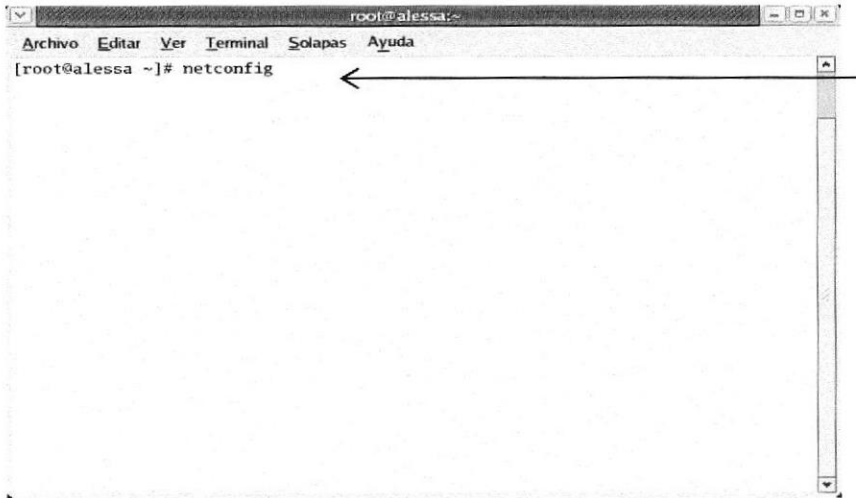


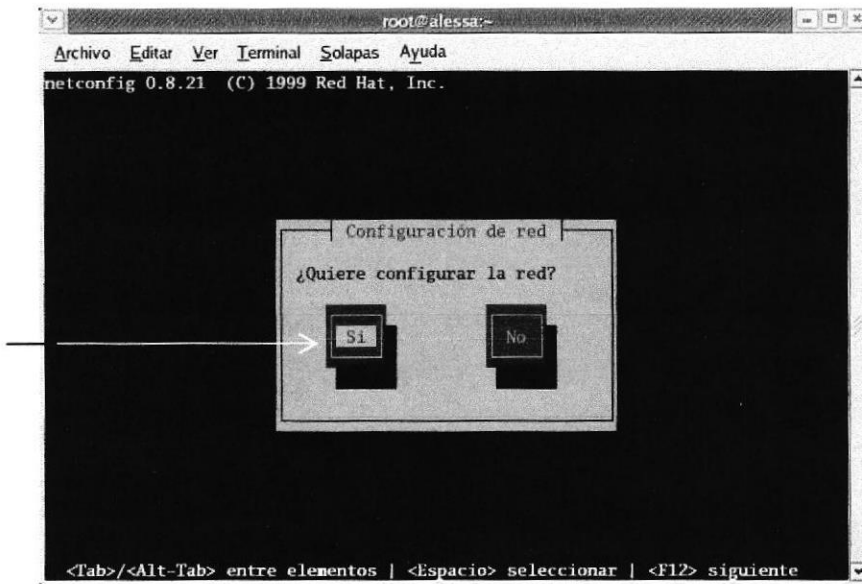
Figura 5-43: INGRESAR AL TERMINAL.

Ahora configure de forma grafica la tarjeta de red con el comando, **netconfig** y de enter.



**Figura 5-44: COMANDO NETCONFIG**

Ahora se muestra el asistente para la configuración, con la tecla tabulador marque la opción **si** y de enter.



**Figura 5-45: CONFIGURACIÓN DE RED**

A continuación aparece esta pantalla y con la tecla tabulador colóquese en el casillero de **Dirección IP** y agregue la dirección IP en su caso **192.168.12.1**, y apreté la tecla tabulador por todas las casillas que se llenen por default y colóquese en **OK**, de enter y ha configurado su tarjeta de red.

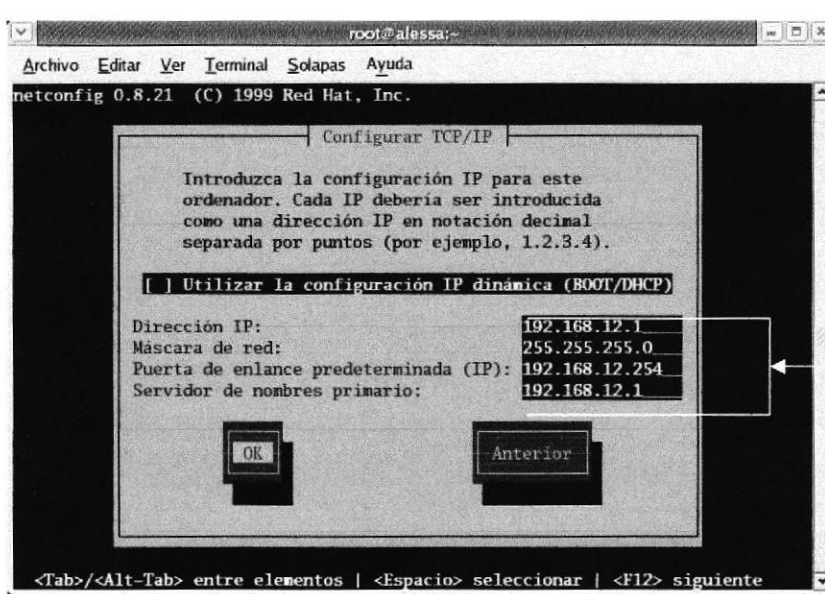


Figura 5-46: CONFIGURAR TCP/IP

Para aplicar los cambios efectuados en la configuración grafica ingrese el comando **service network start**, y de enter y revise si la configuración no tiene ningún error o problema si no tiene ningún error saldrán mensajes de **[OK]** indicándole que la configuración ha sido satisfactoria

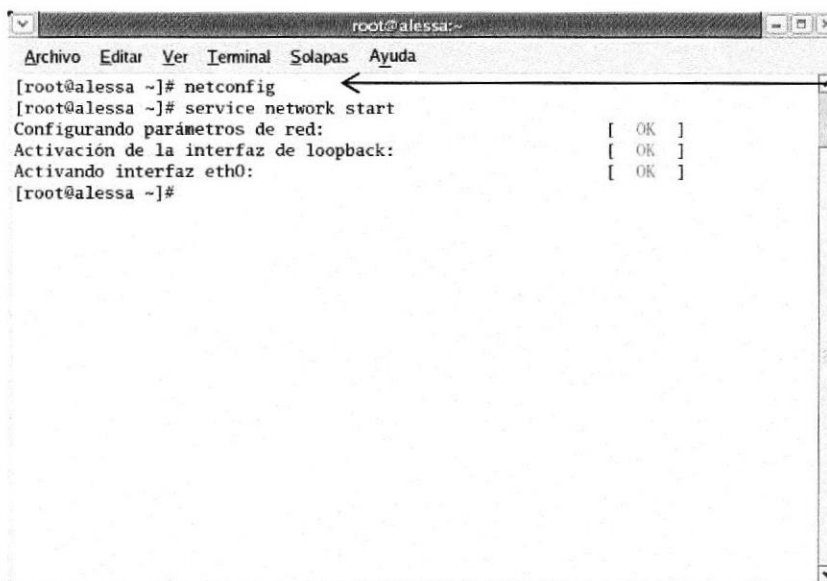


Figura 5-47: INICIAR LOS SERVICIOS

Verifique la configuración debe ingresando el comando **ifconfig**, luego de un enter y verifique la dirección IP, también puede observar la dirección mac address asignada por el fabricante **HWaddr 00:0C:29:B7:22:18**  
La mascara de subred **Mask: 255.255.255.0**

**Dirección IP**                      **Comando**                      **Mac address**                      **Mascara de sub red**

```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
i[root@localhost ~]# ifconfig
eth0  Link encap:Ethernet HWaddr 00:0C:29:B7:22:18
       inet addr:192.168.12.1 Bcast:192.168.12.255 Mask:255.255.255.0
       inet6 addr: fe80::20c:29ff:feb7:2218/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 b) TX bytes:4362 (4.2 KiB)
       Interrupt:10 Base address:0x1080

lo     Link encap:Local Loopback
       inet addr:127.0.0.1 Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING MTU:16436 Metric:1
       RX packets:6022 errors:0 dropped:0 overruns:0 frame:0
       TX packets:6022 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:7788376 (7.4 MiB) TX bytes:7788376 (7.4 MiB)

[root@localhost ~]#

```

ESPOL  
ESCUELA SUPERIOR  
MULTISUBICA DEL LITORAL  
BIBLIOTECA  
CAMPUS  
PEÑAS

Figura 5-48: VERIFICACIÓN DE DIRECCIÓN IP

### 5.10.1.CONFIGURAR FIREWALL

Ahora tendrá que deshabilitar el firewall, escribiendo el comando **setup** en el Terminal y de enter.

**Comando**

```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# setup

```

Figura 5-49: COMANDO SETUP

A continuación se abre el asistente para la configuración y con el teclado desplácese hacia la **opción configuración del firewall**, con las teclas de direcciones, ahora con la tecla tabulador colóquese en **ejecutar herramienta** y de un enter

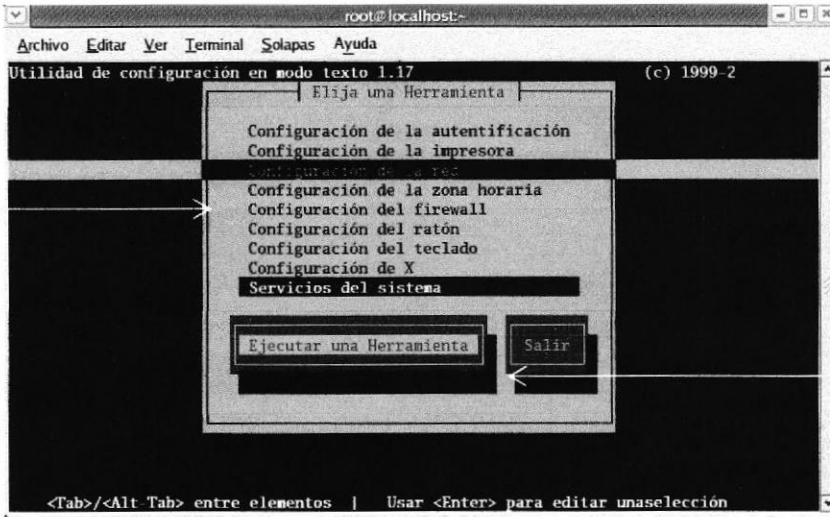


Figura 5-50: UTILIDAD DE CONFIGURACIÓN DE MODO GRAFICO

El asistente indica que debe seleccionar, si habilita o inhabilita el firewall, para este caso debe **inhabilitar** el firewall, para que más adelante realiza su respectivas configuraciones en el servidor, con la tecla tabulador colóquese en la casilla de inhabilitado si no se encuentra marcado, márkuela apretando la barra espaciador, luego con la tecla tabulador colóquese en **aceptar** y de un enter y listo ha configurado el firewall.

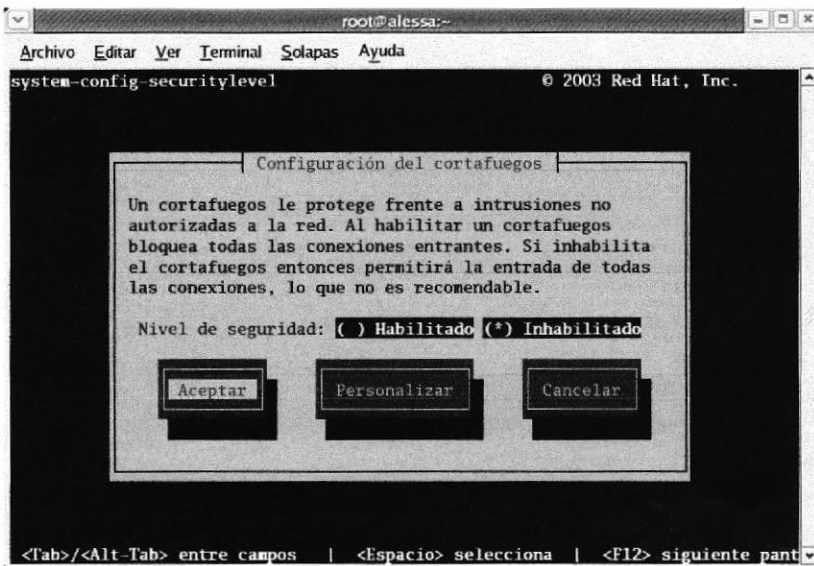


Figura 5-51: CONFIGURACIÓN DEL CORTAFUEGOS

## 5.11. SERVIDOR SAMBA

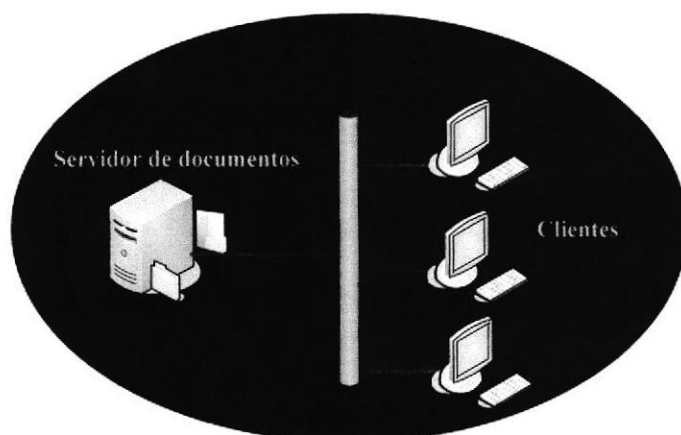


Figura 5-52: SAMBA

### 5.11.1. ¿QUÉ ES SAMBA O SMB?

SMB (acrónimo de Server Message Block) es un protocolo, del nivel de presentación del modelo OSI de TCP/IP, el ínter conectividad entre un equipo con Linux y el resto de los equipos de la red en una oficina con alguna versión de Windows es importante, ya que esto nos permitirá compartir ficheros e impresoras, este ínter conectividad se consigue exitosamente a través de SAMBA.

### 5.11.2. CARACTERÍSTICAS

Samba es una implementación de una docena de servicios y una docena de protocolos, entre los que están: NetBIOS sobre TCP/IP (NetBT), SMB (también conocido como CIFS), DCE/RPC o más concretamente, MSRPC, el servidor WINS también conocido como el servidor de nombres NetBIOS (NBNS), la suite de protocolos del dominio NT, con su Logon de entrada a dominio, la base de datos del gestor de cuentas seguras (SAM), el servicio Local Security Authority (LSA) o autoridad de seguridad local, el servicio de impresoras de NT y recientemente el Logon de entrada de Active Directory, que incluye una versión modificada de Kerberos y una versión modificada de LDAP. Todos estos servicios y protocolos son frecuentemente referidos de un modo incorrecto como NetBIOS o SMB.

Samba configura directorios Unix/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de Linux pueden montar en sus sistemas de archivos estas unidades de red como si fueran dispositivos locales, o utilizar la orden `smbclient` para conectarse a ellas muy al estilo del cliente de la línea de órdenes `ftp`. Cada directorio puede tener diferentes permisos de acceso sobrepuestos a las protecciones del sistema de archivos que se esté usando en Linux. Por ejemplo, las carpetas `home` pueden tener permisos de lectura y escritura para cada usuario, permitiendo que cada uno acceda a sus propios archivos; sin embargo, deberemos

cambiar los permisos de los archivos localmente para dejar al resto ver nuestros archivos, ya que con dar permisos de escritura en el recurso no será suficiente.

La configuración de Samba se consigue editando un solo archivo, accesible en `/etc/smb.conf` o en `/etc/samba/smb.conf`.

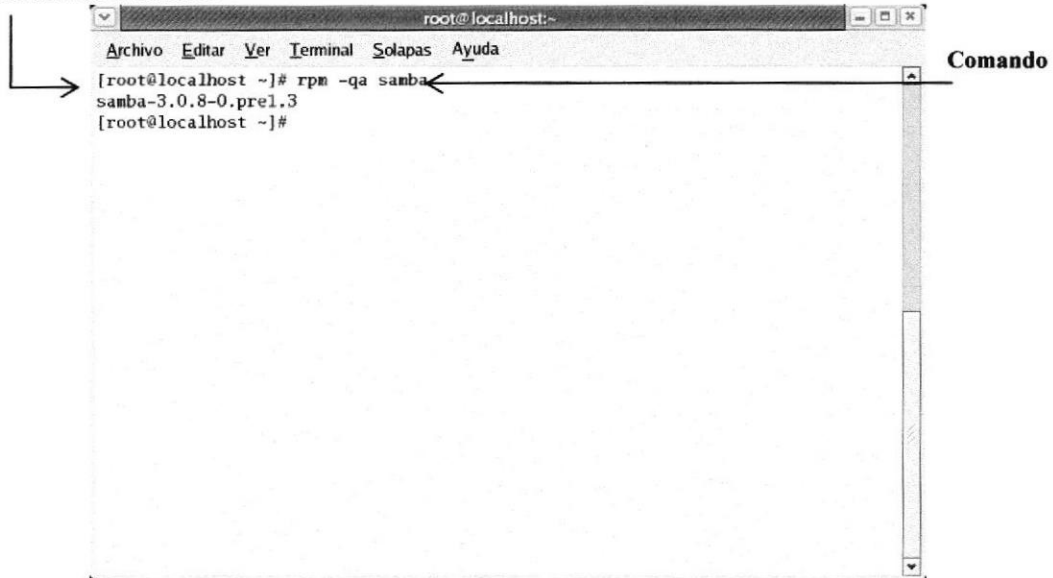
### 5.11.3. REQUISITOS PARA LEVANTAR UN SERVIDOR SAMBA

- ✓ Una equipo de trabajo con sistema operativo Linux.
- ✓ Tarjeta de red.
- ✓ Tener la tarjeta de red configurada.
- ✓ Paquete de samba instalado.
- ✓ Servicio samba habilitado.

### 5.11.4. CONFIGURACIÓN DE SAMBA

Ahora verifique si tiene instalado el paquete de samba, lo hace con el comando `rpm -qa samba`, luego de enter y revise.

Paquete samba instalado



```
root@localhost:~# rpm -qa samba
samba-3.0.8-0.pre1.3
root@localhost ~]#
```

The image shows a terminal window with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Terminal', 'Solapas', and 'Ayuda'. The terminal title is 'root@localhost:~'. The command 'rpm -qa samba' is entered and executed, resulting in the output 'samba-3.0.8-0.pre1.3'. A label 'Comando' with an arrow points to the command line, and another label 'Paquete samba instalado' with an arrow points to the output line.

Figura 5-53: VERIFICACIÓN DE PAQUETE DE SAMBA.

Verifique si esta habilitado el servicio samba, ingrese el comando setup en el Terminal y de enter.

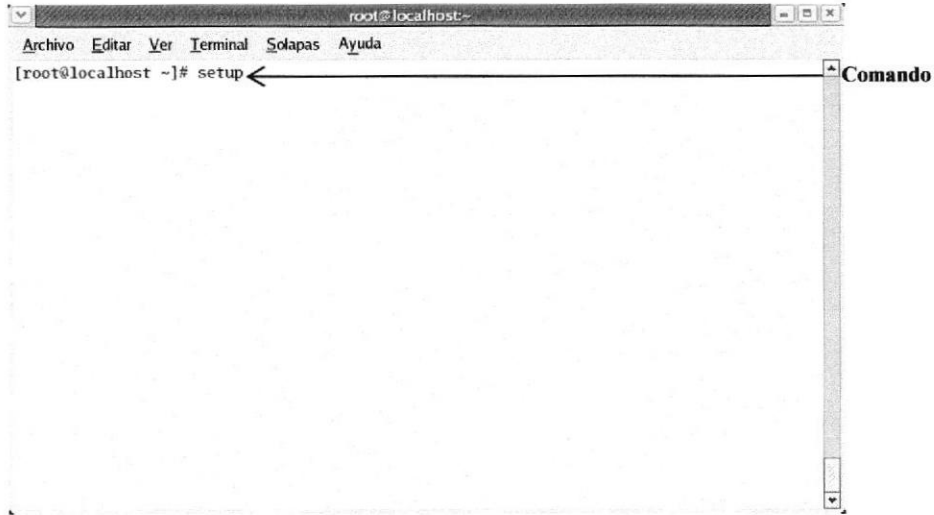


Figura 5-54: COMANDO SETUP

A continuación se abre esta la pantalla de utilidad de configuración de modo texto y con el teclado desplácese hacia la **opción servicios del sistema** con las teclas de direcciones, ahora con la tecla tabulador colóquese en **ejecutar herramienta** y de un enter

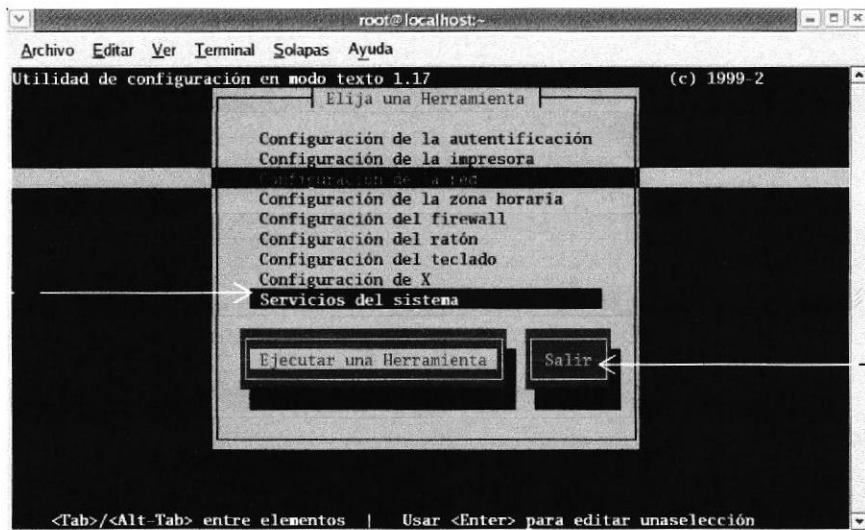


Figura 5-55: UTILIDAD DE CONFIGURACIÓN DE MODO TEXTO

Ahora se abre esta pantalla y con el teclado desplácese hacia la opción **smb** con las teclas direccionales y si esta opción no se encuentra marcada con un asterisco como lo muestra la imagen presione la tecla barra espaciadora [] para que se marque con el asterisco así esta habilitando el servicio samba, luego colóquese con la tecla tabulador en **OK** y de un enter.

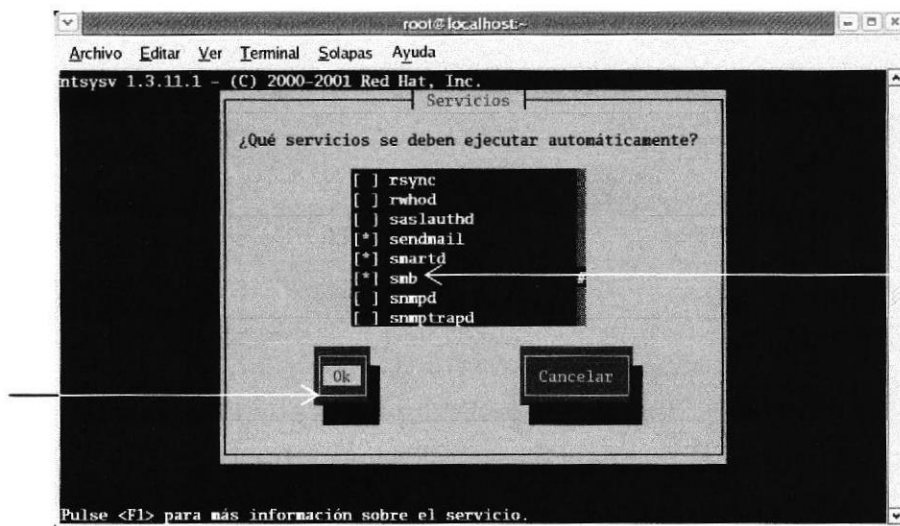


Figura 5-56: HABILITAR SERVICIO SMB

Continuación aparece esta pantalla y con la tecla tabulador colóquese en **salir** y de un enter, ya a ha habilitado el servicio samba.



Figura 5-57: SALIR UTILIDAD DE CONFIGURACIÓN DE MODO TEXTO

Ahora edite el fichero que se encuentra en el directorio etc/samba, para esto ingrese el comando vi, de la siguiente manera, **vi /etc/samba/smb.conf** y de un enter.

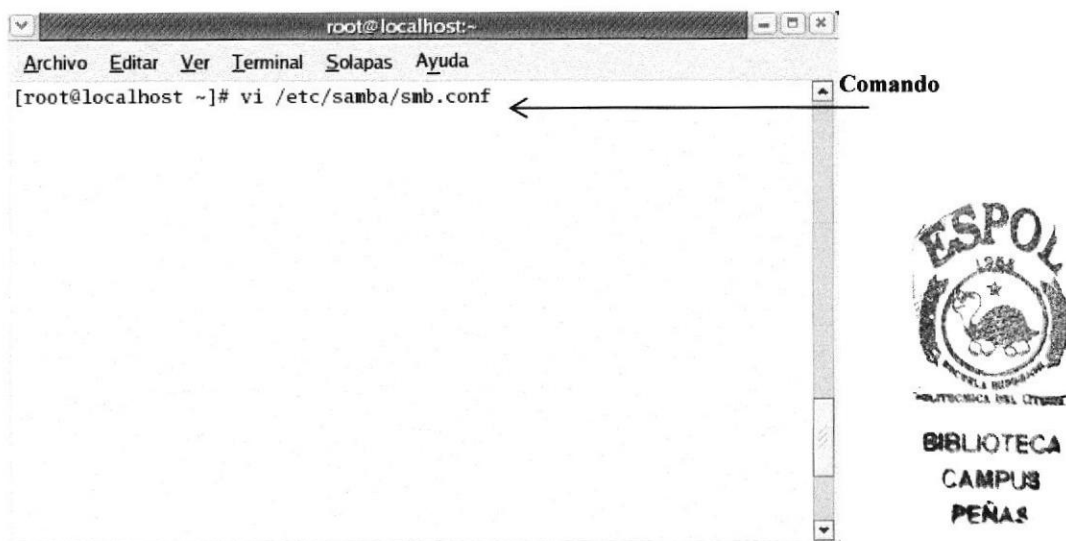


Figura 5-58: INGRESAR AL FICHERO SMB.CONF

Empiece editando, la sección **[global]**.

Workgroup, nos permite definir el grupo de trabajo en el cual el servidor samba va a trabajar.

Agregue la línea netbios name, que permite definir el nombre de la maquina, no como un nombre DNS, sino como un nombre de resolución de nombres propio del protocolo NetBios, es importante que recuerde que son dos cosas totalmente diferentes.

Para su caso la configuración será de la siguiente manera:

**Workgroup = ALESSA**

**netbiosname = Servidor samba**

**Server string = Servidor samba**

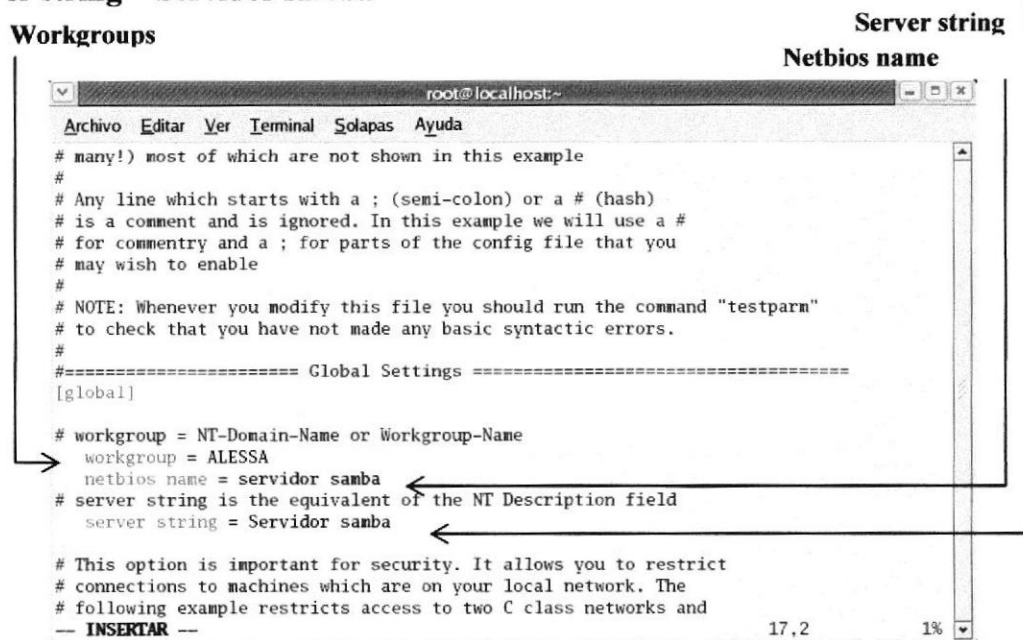


Figura 5-59: EDITAR FICHERO SMB.CONF SECCIÓN [GLOBAL]

Siga buscando las líneas que se encuentra en la sección **[share definitions]**

La línea **comment** permite agregar un comentario de su servidor Samba.

La línea **Path** permite definir cual es el directorio que va a compartir.

La línea **valid users** permite definir cuales son los usuarios que tendrán acceso al servidor Samba.

La línea **public** permite definir si el servidor será público o no para ciertos usuarios.

La línea **writable** permite definir si el servidor tendrá permisos de escritura para los usuarios.

La línea **browsable** permite definir si el servidor será visible para los usuarios.

Para nuestro su la configuración será de la siguiente manera:

#### [Alessa]

**Comen** = servidor configurado por Alejandro

**Pat.** = / archivos\_compartidos

**Valid user** = alejandro eduardo

**Public** = yes

**Writable** = yes

**Browsable** = yes



Una vez que ha realizado los cambios en el fichero **smb.conf** cierre y guarde los cambios de dicho fichero.

#### Líneas editadas

```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
# setup, the directory should be writable by both users and should have the
# sticky bit set on it to prevent abuse. Obviously this could be extended to
# as many users as required.
:[myshare]
; comment = Mary's and Fred's stuff
; path = /usr/somewhere/shared
; valid users = mary fred
; public = no
; writable = yes
; printable = no
; create mask = 0765

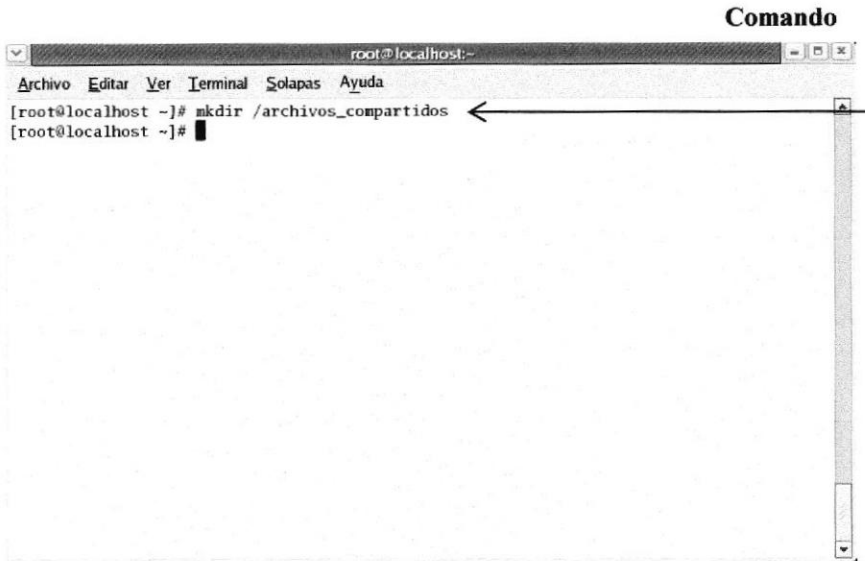
[alessa]
comment = servidor configurado por alejandro
path = /archivos_compartidos
valid users = alejandro eduardo
public = yes
writable = yes
browsable = yes

-- INSERTAR --                               303,1      Final
  
```

Figura 5-60: EDITAR FICHERO SMB.CONF SECCIÓN [SHARE DEFINITIONS]

Ahora debe crear el directorio que va a compartir, con el comando `mkdir` de la siguiente manera **`mkdir /archivos_compartidos`** y de un enter.

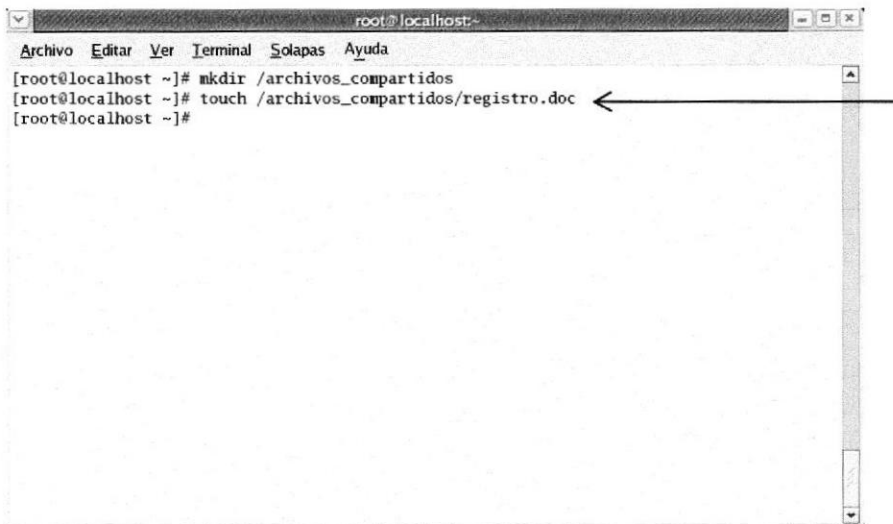
**Comando**

A terminal window titled "root@localhost:~" with a menu bar containing "Archivo", "Editar", "Ver", "Terminal", "Solapas", and "Ayuda". The terminal shows the command `mkdir /archivos_compartidos` being entered and executed. A black arrow points from the word "Comando" to the command line. The prompt `[root@localhost ~]#` is visible on both lines.

```
root@localhost:~  
[root@localhost ~]# mkdir /archivos_compartidos  
[root@localhost ~]#
```

**Figura 5-61: CREAR DIRECTORIO A COMPARTIR**

Entonces después de crear el directorio cree el fichero a compartir con el comando `touch` de la siguiente manera **`touch /archivos_compartidos/registro.doc`** y de un enter.

A terminal window titled "root@localhost:~" with a menu bar containing "Archivo", "Editar", "Ver", "Terminal", "Solapas", and "Ayuda". The terminal shows the command `touch /archivos_compartidos/registro.doc` being entered and executed. A black arrow points from the word "Comando" to the command line. The prompt `[root@localhost ~]#` is visible on both lines.

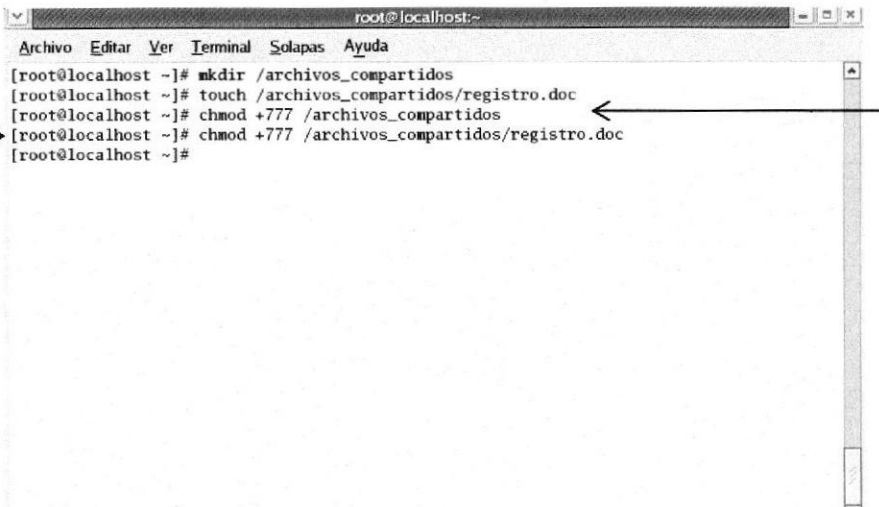
```
root@localhost:~  
[root@localhost ~]# mkdir /archivos_compartidos  
[root@localhost ~]# touch /archivos_compartidos/registro.doc  
[root@localhost ~]#
```

**Figura 5-62: CREAR FICHERO A COMPARTIR**

Una vez creados directorio y fichero déle los permisos respectivamente con el comando `chmod` de la siguiente manera, `chmod +777 /etc/archivos_compartidos` y para el fichero `chmod +777 /etc/archivos_compartidos/registro` y de un enter.

Permiso para directorio

Permiso para fichero



```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# mkdir /archivos_compartidos
[root@localhost ~]# touch /archivos_compartidos/registro.doc
[root@localhost ~]# chmod +777 /archivos_compartidos
[root@localhost ~]# chmod +777 /archivos_compartidos/registro.doc
[root@localhost ~]#
  
```




Figura 5-63: ASIGNAR PERMISO AL FICHERO CREADO

Ahora deben crear los usuarios samba, los usuarios se deben crear como usuarios del sistema, para luego crearlos como usuarios samba, continuación cree un usuario de sistema.

El usuario de sistema lo crea con el comando `adduser` y lo hace de la siguiente manera `adduser eduardo` y de un enter.

Comando

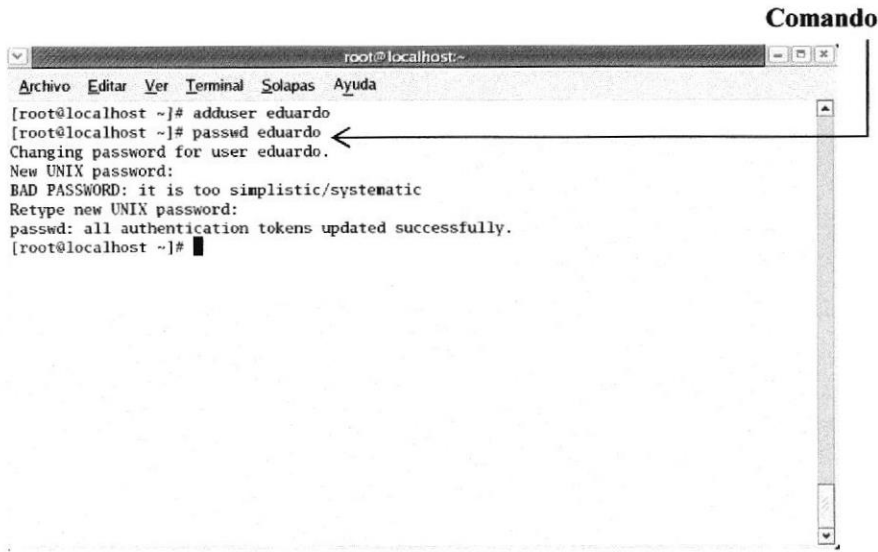


```

root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# adduser eduardo
[root@localhost ~]# █
  
```

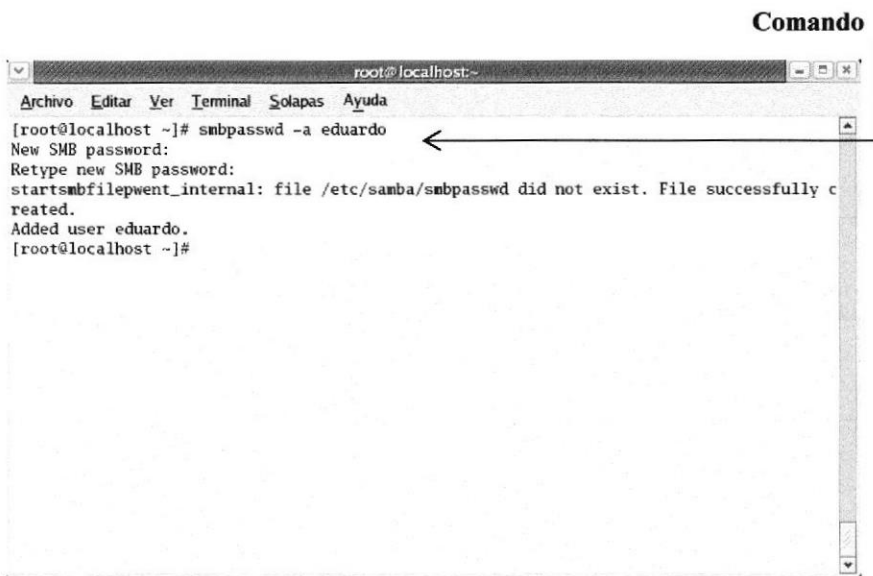
Figura 5-64: CREAR USUARIO DE SISTEMA.

Ahora asigne la contraseña al usuario creado en este caso **eduardo**, con el comando **passwd**, de la siguiente manera **passwd eduardo** luego de un enter y debe ingresar la contraseña dos veces para su autenticación sea satisfactoria.



**Figura 5-65: ASIGNAR CONTRASEÑA**

Después que el usuario de sistema se ha creado satisfactoriamente, continúe haciéndolo usuario samba, lo hace con el comando **smbpasswd -a Eduardo** déle un enter y debe ingresar una contraseña para entrar como usuario samba, la contraseña puede ser la misma que se usa para usuario del sistema si se lo desea luego de un enter y debe ingresar la contraseña dos veces para su autenticación sea satisfactoria.



**Figura 5-66: CREAR USUARIO SAMBA**

Después de haber terminado todas estas configuraciones, inicie el servicio samba con el comando `service smb start` de la siguiente manera **service smb start** y de un enter si la configuración no tiene ningún error o problema saldrán mensajes de **[OK]** indicándole que la configuración ha sido satisfactoria.

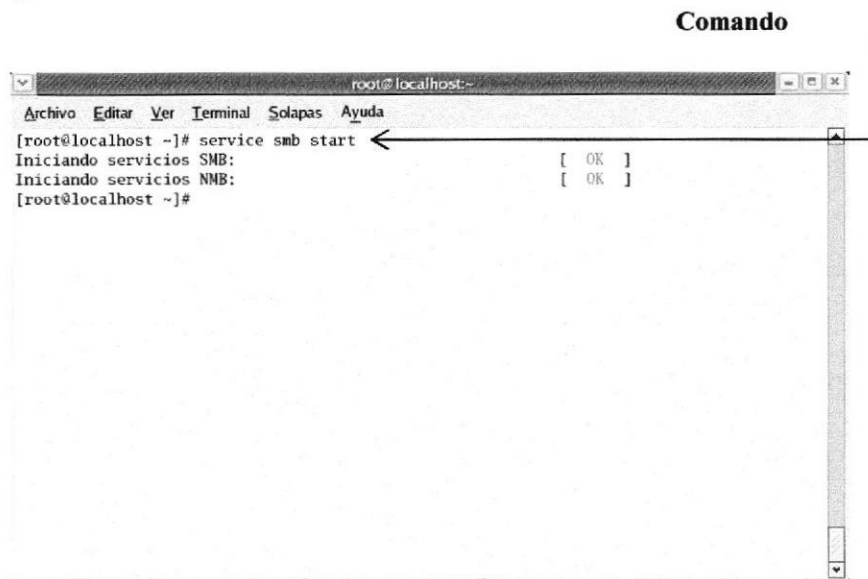


Figura 5-67: INICIAR SERVICIO SAMBA

### 5.11.4.1. CONFIGURACIÓN EN EL CLIENTE

Primero debe configurar la tarjeta de red dándole una dirección IP, lo hará de la siguiente manera de clic derecho sobre mis sitios de red y seleccione **propiedades**.



Figura 5-68: PROPIEDADES DE MIS SITIOS DE RED

Se habrá la ventana mis sitios de red seleccione conexión de área local y de clic derecho, seleccione **propiedades**.



Figura 5-69: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL

Entonces se habrá la ventana propiedades de conexión de área local seleccione **protocolo Internet [TCP/IP]**, y de clic en **propiedades**.

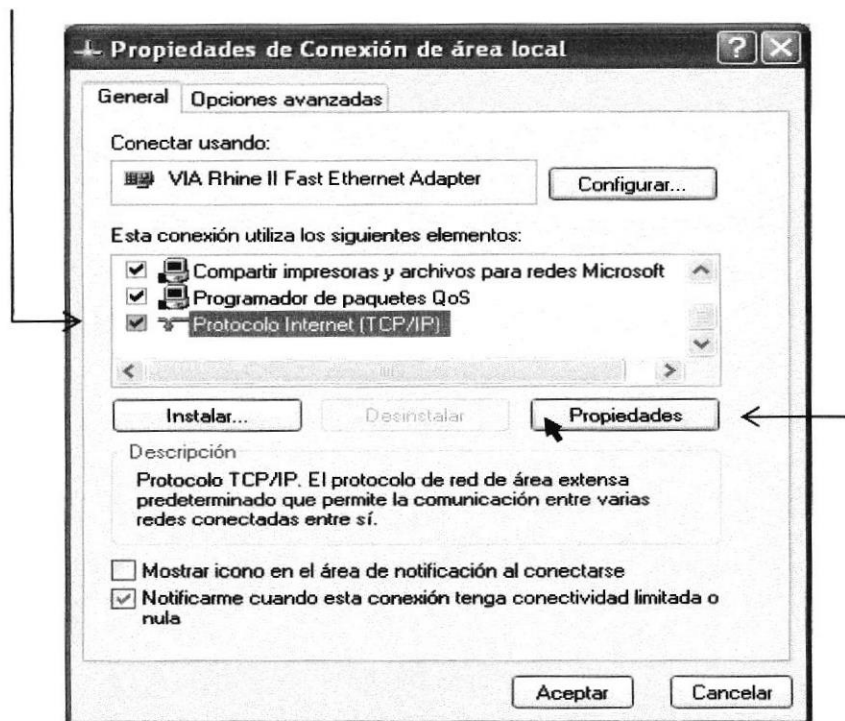


Figura 5-70: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL

Ahora en esta ventana debe seleccionar la casilla **usar la siguiente dirección IP** para poder asignar la dirección IP y la máscara de sub red por defecto en las casillas y de un clic en **aceptar** y listo ya tiene configurada la tarjeta de red del cliente.

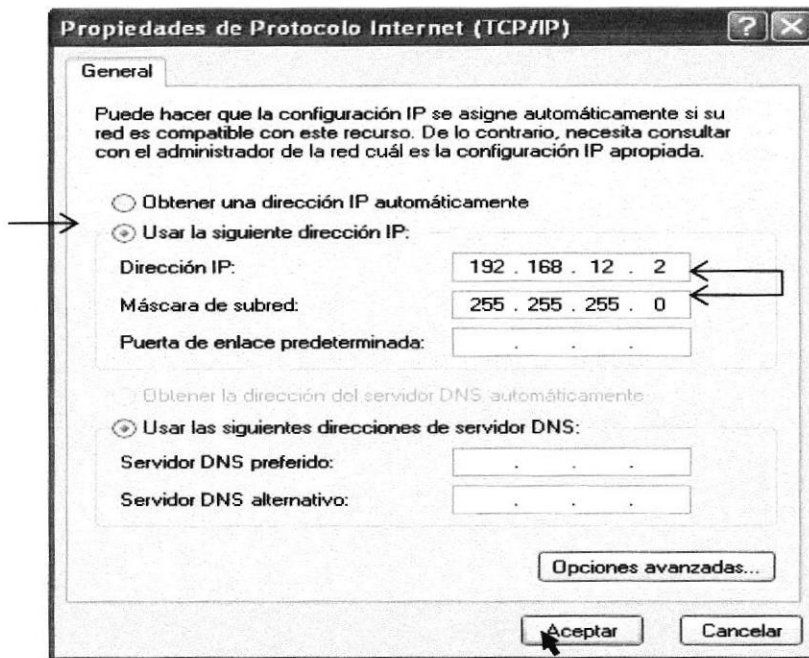


Figura 5-71: PROPIEDADES DE PROTOCOLO DE INTERNET (TCP/IP)

Una vez configurada la tarjeta de red, debe asignarle el grupo de trabajo al cliente en el que se encuentra el servidor Linux, lo hace de la siguiente manera de un clic derecho en **mi PC** y seleccionamos **propiedades**.



Figura 5-72: PROPIEDADES DE MI PC

En la ventana propiedades del sistema, seleccione la viñeta **nombre de equipo**.

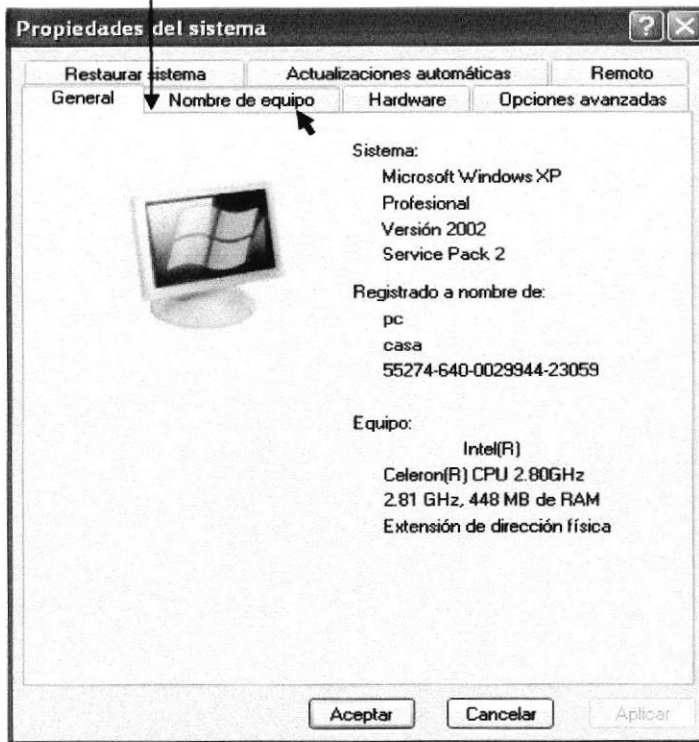


Figura 5-73: PROPIEDADES DEL SISTEMA – NOMBRE DE EQUIPO

En esta ventana de clic en **cambiar**.

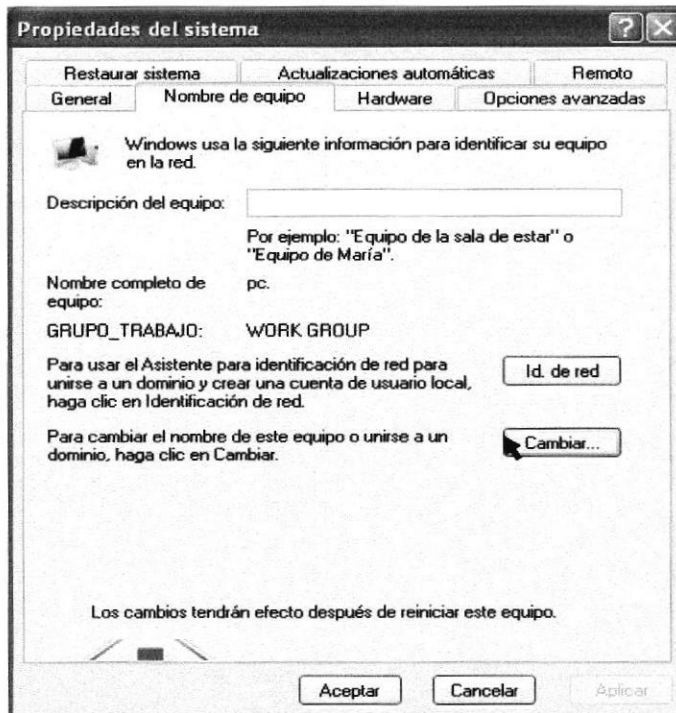


Figura 5-74: PROPIEDADES DEL SISTEMA – CAMBIAR

En esta ventana cambie el grupo de trabajo, por el que asigno en el servidor Linux, para este caso **ALESSA** y de clic en **aceptar**.

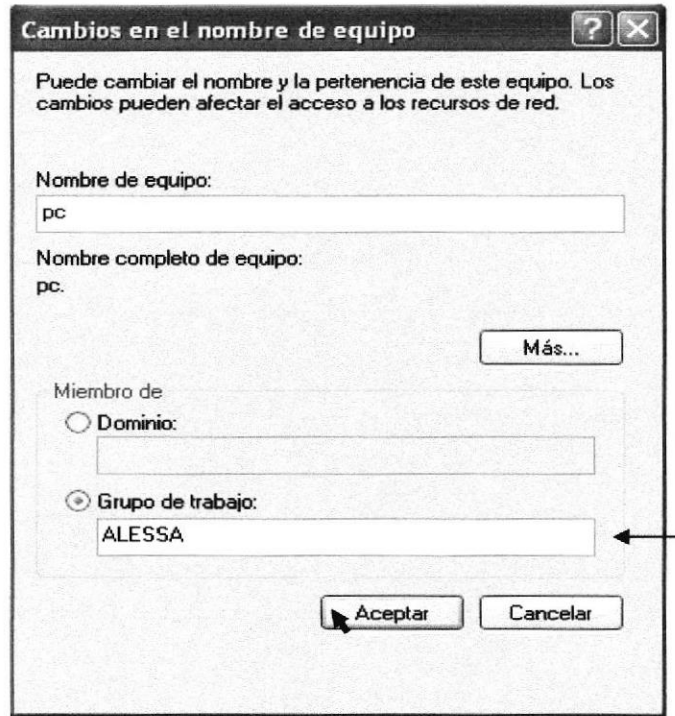


Figura 5-75: CAMBIOS EN EL NOMBRE DE EQUIPO

Después de esto aparece un mensaje de bienvenida al grupo de trabajo **ALESSA**, de clic en **aceptar** y ya termino de asignarle el grupo de trabajo, lo siguiente debe reiniciar el equipo para que se guarden los cambios efectuados.

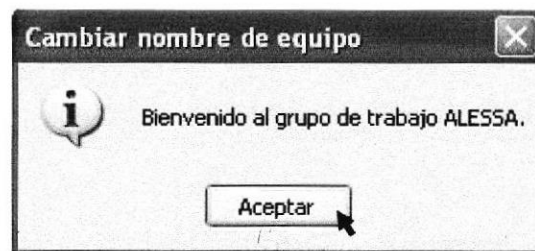


Figura 5-76: BIENVENIDO AL GRUPO DE TRABAJO

Ahora va a acceder del cliente en Windows al servidor Linux a la carpeta que comparte mediante el servicio samba.

Lo hace de la siguiente manera de clic en **inicio** y seleccione **ejecutar**.

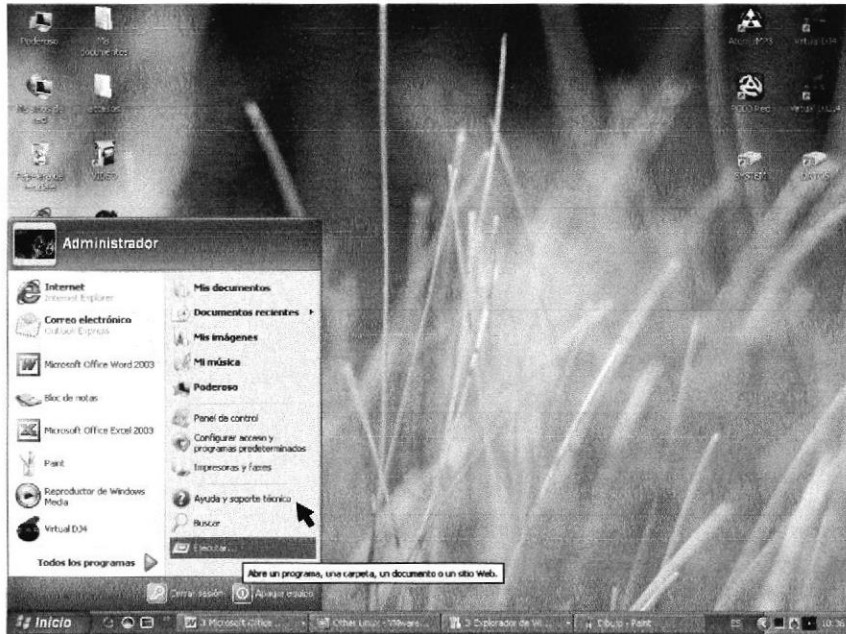


Figura 5-77: INICIO – EJECUTAR

Aparece la ventana de ejecutar y escriba la dirección IP del servidor Linux para poder acceder a la carpeta o directorio que creo en Linux.

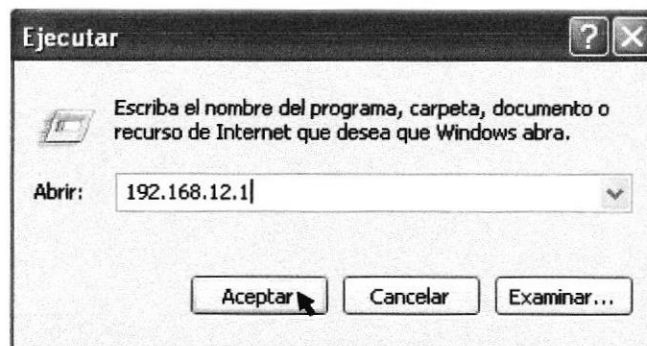


Figura 5-78: BUSCAR AL SERVIDOR POR IP

A continuación aparece una ventana en la cual debe ingresar el usuario y la contraseña creada en el Linux para poder acceder al servidor y de clic en aceptar.

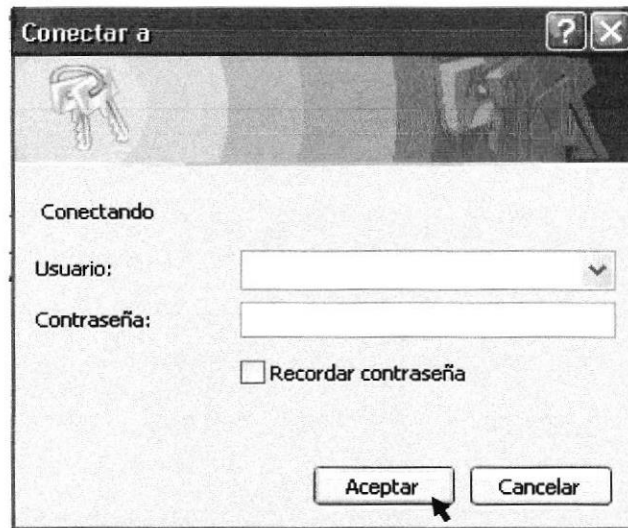


Figura 5-79: CONECTARSE AL SERVIDOR

Ahora que ya ingreso al servidor samba, revise que el servicio esta trabajando satisfactoriamente.

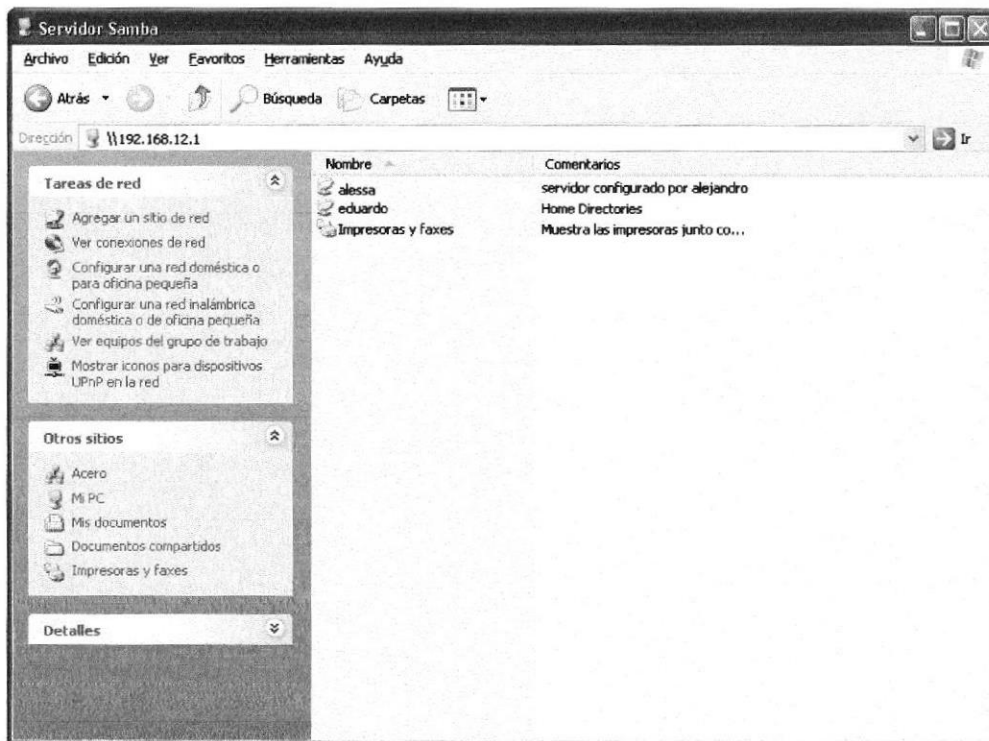


Figura 5-80: CARPETA COMPARTIDA

## 5.12.DNS

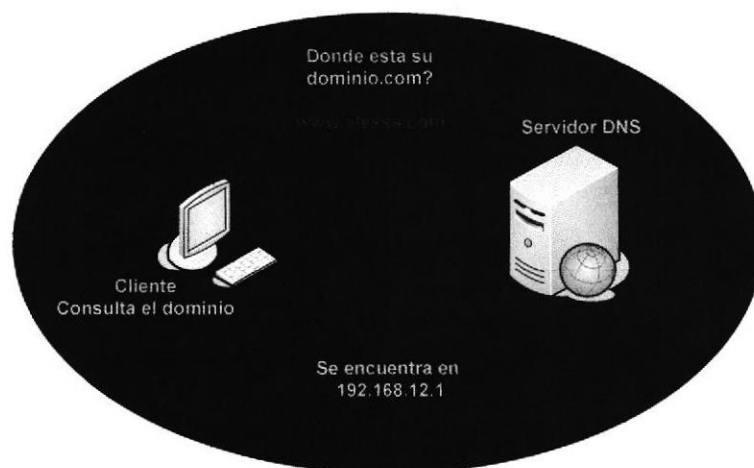


Figura 5-81: DNS

### 5.12.1.1. ¿QUÉ ES DNS?

DNS son las siglas de lo que se conoce como Domain Name System (sistema de dominio de nombres), es un servidor que nos permite convertir nombres a direcciones IP, para facilitar el uso de los recursos de red, los servicios de nombres como DNS proporcionan una forma de asignar estos nombres sencillos de los equipos o servicios a sus direcciones numéricas, si utilizó alguna vez un explorador Web, también utilizó DNS, también está catalogado como una base de datos distribuida jerárquicamente que es utilizado dentro de las redes IP para traducir o resolver nombres de computadores a su respectiva dirección IP.

#### COMPONENTES

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

Los Clientes DNS (resolvers), un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde a nombre del dominio?).

Los Servidores DNS (name servers), que contestan las peticiones de los clientes, los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

Y las Zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

#### USOS DEL DNS

El DNS se utiliza para distintos propósitos. Los más comunes son:

**Resolución de nombres:** Dado el nombre completo de un host (por ejemplo blog.smaldone.com.ar), obtener su dirección IP (en este caso, 208.97.175.41).

**Resolución inversa de direcciones:** Es el mecanismo inverso al anterior. Consiste en dada una *dirección IP*, obtener el nombre asociado a la misma.

**Resolución de servidores de correo:** Dado un nombre de dominio, obtener el servidor a través del cual debe realizarse la entrega del correo electrónico.



Por tratarse de un sistema muy flexible, es utilizado también para muchas otras funciones, tales como la obtención de claves públicas de cifrado asimétrico y la validación de envío de e-mails (a través de mecanismos como SPF).

### 5.12.1.2. ZONAS

Una zona es una porción continua de nombres de espacio de dominios configuradas dentro de un DNS Server y las cuales poseen autoridad para la resolución de consultas DNS.

Un DNS Server maneja 2 tipos de Zonas:

- Primarias
- Secundarias

#### 5.12.1.2.1.1 ZONAS ESTÁNDARES

#### 5.12.1.2.1.2 ZONAS PRIMARIAS

Contiene permisos de lectura/escritura sobre el archivo de la zona, cualquier cambio en la zona es reflejado en este archivo, cada vez que cree una zona la creará una zona primaria estándar

#### 5.12.1.2.1.3 ZONAS SECUNDARIAS

Contiene permisos de sólo lectura sobre el archivo de la zona. Cualquier cambio en la zona será registrado en el archivo de la zona primaria y luego replicado a la zona secundaria.

### 5.12.1.3. REQUISITOS PARA SU CONFIGURACIÓN

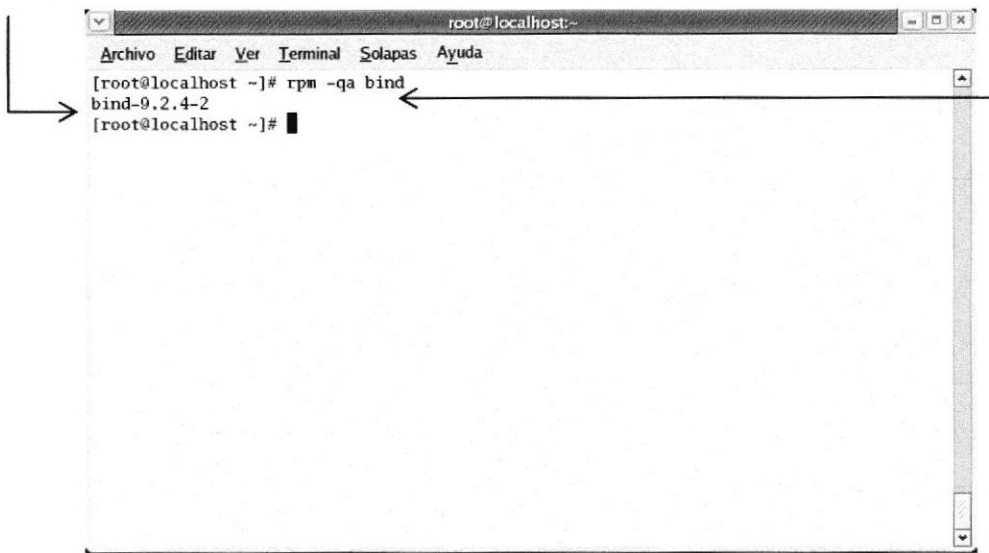
- ✓ Una equipo de trabajo con sistema operativo Linux.
- ✓ Tarjeta de red.
- ✓ Tener la tarjeta de red configurada
- ✓ Paquete bind instalado
- ✓ Servicio named habilitado

### 5.12.1.4. CONFIGURACIÓN DEL SERVICIO DNS

Ahora verifique si tiene instalado el paquete de samba, lo debe hacer con el comando **rpm -qa bind**, luego de enter y revise.

Paquete bind instalado

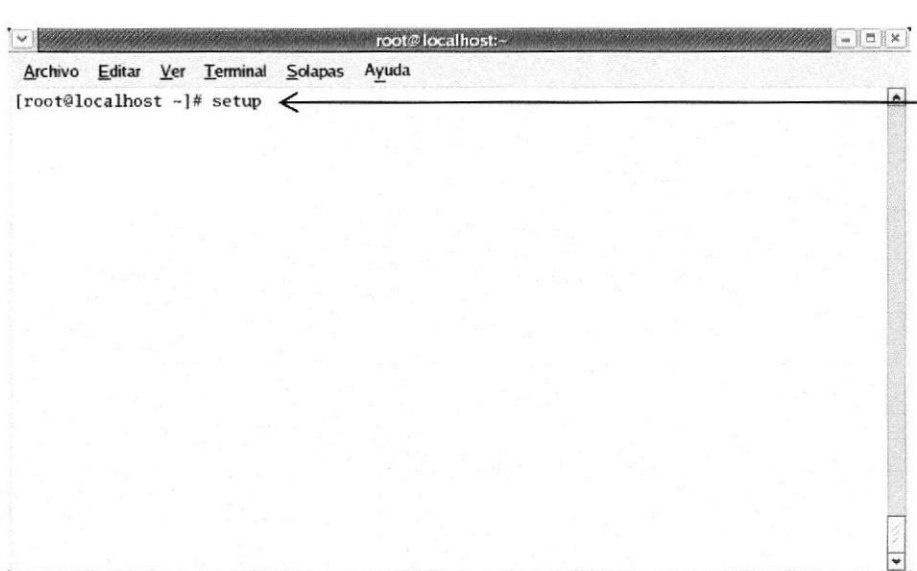
Comando



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# rpm -qa bind  
bind-9.2.4-2  
[root@localhost ~]#
```

Figura 5-82: VERIFICAR EL PAQUETE BIND

Ahora verifique si esta habilitado el servicio samba de no ser así habilítelo de la siguiente manera, en el terminal escriba el comando **setup** y de enter.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# setup
```

Figura 5-83: COMANDO SETUP

A continuación se abre la pantalla utilidad de configuración y con el teclado desplácese hacia la **opción servicios del sistema** con las teclas de direcciones, ahora con la tecla tabulador colóquese en **ejecutar herramienta** y de un enter

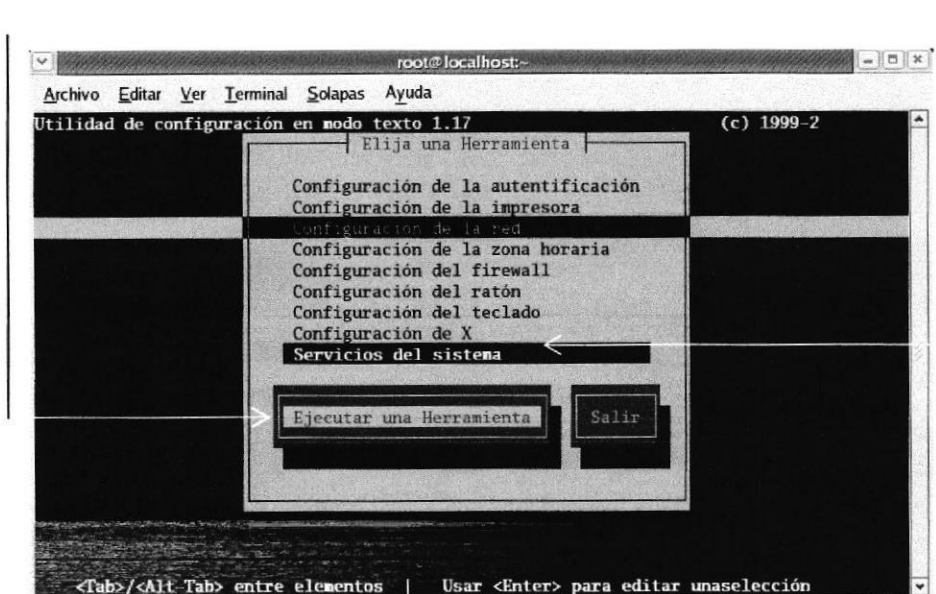


Figura 5-84: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora se abre esta pantalla y con el teclado desplácese hacia la opción **named** con las teclas direccionales y si esta opción no se encuentra marcada con un asterisco como lo muestra la imagen presione la tecla barra espaciadora [\*] para que se marque con el asterisco así estará habilitando el servicio dns, luego colóquese con la tecla tabulador **OK** y de un enter.



Figura 5-85: HABILITAR EL SERVICIO NAMED

A continuación aparece esta pantalla y con la tecla tabulador colóquese en salir y de un enter ya ha habilitado el servicio named.



Figura 5-86: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora edite el fichero named.conf que se encuentra en el directorio /etc, para esto ingrese el comando vi, de la siguiente manera, **vi /etc/named.conf** y de un enter.

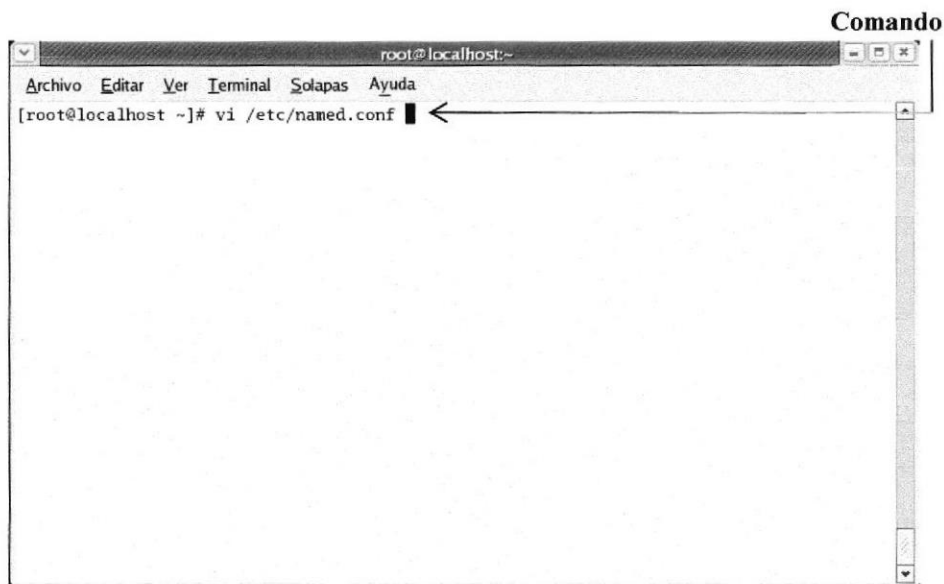


Figura 5-87: INGRESAR AL FICHERO NAMED.CONF

Entonces edite el fichero `named.conf`, busque las zonas creadas que se encuentran en la parte final del fichero, y agregue la zona **alessa.com**, el tipo de zona **master**, fichero **alessa.com.zone**.

## Zona creada

```

root@localhost:/var/named/chroot/var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
};
zone "255.in-addr.arpa" IN {
    type master;
    file "named.broadcast";
    allow-update { none; };
};
zone "0.in-addr.arpa" IN {
    type master;
    file "named.zero";
    allow-update { none; };
};
zone "alessa.com" IN {
    type master;
    file "alessa.com.zone";
    allow-update { none; };
};
include "/etc/rndc.key";
"/etc/named.conf" 74L, 1415C
70,2-9  Final

```

**Figura 5-88: EDITAR EL FICHERO NAMED.CONF**

Una vez editado el fichero del `named.conf` entre al siguiente directorio `/var/named` y copie el fichero del `localhost.zone` y lo hace de la siguiente manera, entre al directorio con el comando `cd /var/named` y de un enter, luego copie el fichero con el comando `cp localhost.zone alessa.com.zone`

## Comando

```

root@localhost:/var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# cd /var/named
[root@localhost named]# cp localhost.zone alessa.com.zone

```

**Figura 5-89: COPIAR EL FICHERO LOCALHOST.ZONE**

Ahora enliste el directorio para verificar si copio el fichero con el nombre de la zona, lo hace de la siguiente manera con el comando **ls**.

Fichero copiado

Comando



```

root@localhost:/var/named
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# cd /var/named
[root@localhost named]# cp localhost.zone alessa.com.zone
[root@localhost named]# ls
alessa.com.zone  localdomain.zone  named.ca          named.zero
chroot          localhost.zone    named.ip6.local  slaves
data            named.broadcast  named.local
[root@localhost named]#
  
```

Figura 5-90: VERIFICAR EL FICHERO ALESSA.COM.ZONE

A continuación edite el fichero que copio para este caso **alessa.com.zone** que se encuentra en el directorio que se encuentra actualmente, lo hace de la siguiente manera con el comando **vi alessa.com.zone**.

En este fichero encontrara varios parámetros que va a editar y otros que se mantienen fijos los cuales se explican a continuación.

**SOA** y **NS** son registros necesarios, como puede ver en el registro SOA, la persona de contacto es **root.alessa.com**, **NS** este registro de recursos indica los servidores de nombres (Name Servers NS) autorizados para la zona, se indican tanto los servidores principales como los secundarios, así como los servidores para cualquier zona delegada cada zona debe contener como mínimo, un registro NS, **CNAME** es el nombre canónico para un alias, el registro de recurso **A** es el tipo de registro que asigna un nombre de dominio completamente cualificado (FQDN) a una dirección IP, para que los clientes puedan solicitar la dirección IP de un nombre dado.

Cada zona contiene un registro de recursos Inicio de autoridad al comienzo de la zona los registros SOA (Start Of Authority) incluyen los siguientes campos:

**TTL:** tiempo de vida en segundos que un servidor DNS o un resolver debe guardar en caché esta entrada antes de descartarla.

**Persona responsable:** contiene la dirección de correo electrónico del responsable de la zona. Se utiliza un punto en el lugar del símbolo arroba **@**.

**Número de serie:** muestra cuantas veces se actualizo la zona. Cuando un servidor secundario de zona se pone en contacto con el servidor maestro para determinar si necesita iniciar una transferencia de zona, el secundario compara su número de serie con el del maestro. Si el número de serie del maestro es superior, el secundario inicia una transferencia de zona.



Una vez que edito el fichero de la zona debe hacer una copia en el directorio /var/named/chroot/var/named con el comando cp, lo hace de la siguiente manera **cp alessa.com.zone /var/named/chroot/var/named** y de un enter.

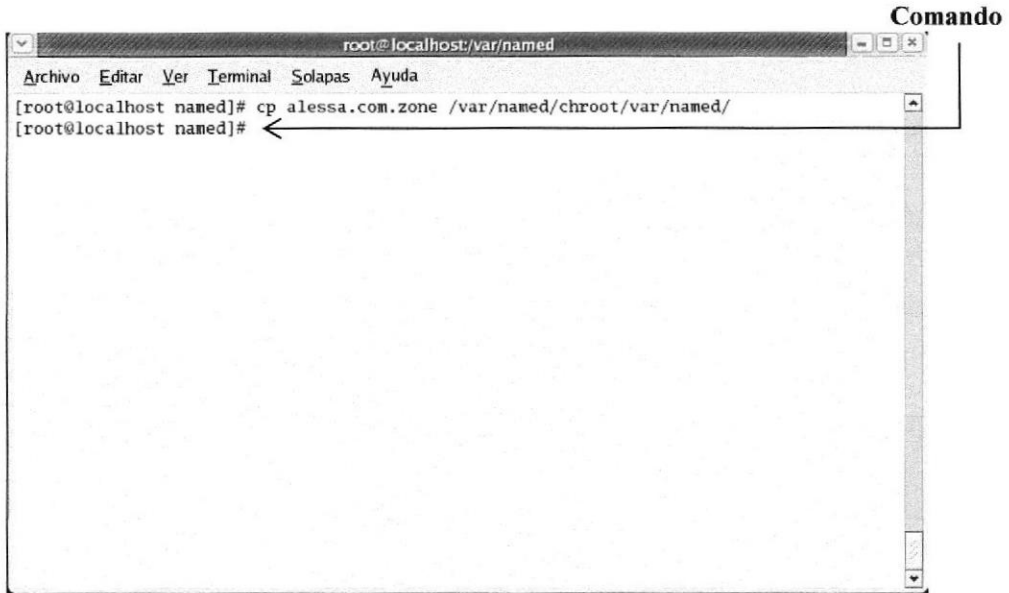


Figura 5-93: COPIAR FICHERO ALESSA.COM

Después de que terminado todas esas configuraciones, inicie el servicio named con el comando **service named start** de la siguiente manera **service named start** y déle un enter si la configuración no tiene ningún error o problema saldrán mensajes de **[OK]** indicándole que la configuración ha sido satisfactoria.

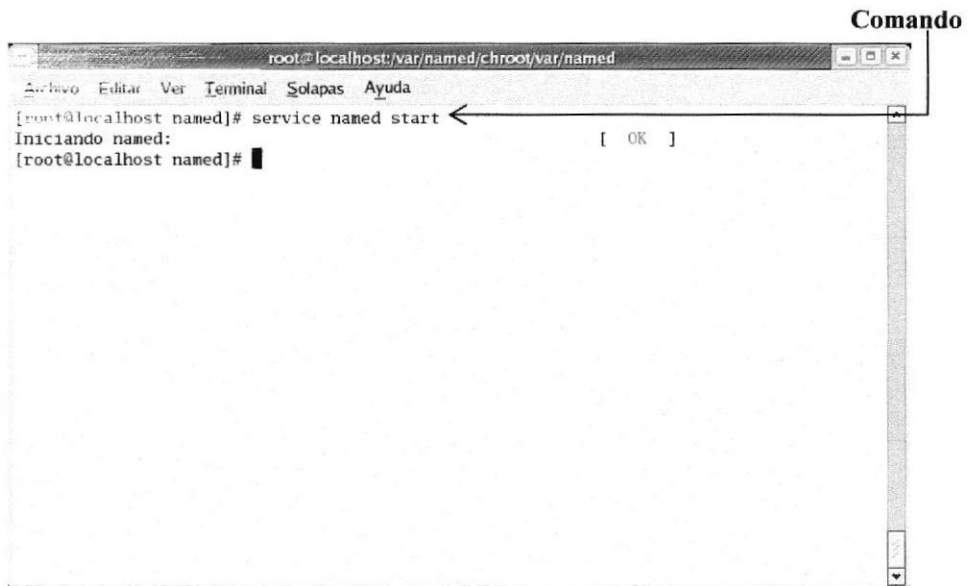
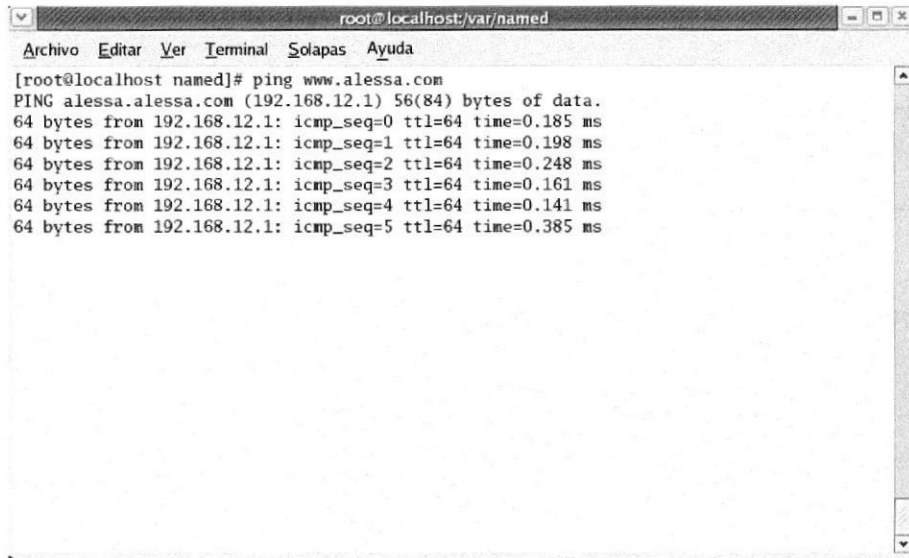


Figura 5-94: INICIAR SERVICIO BIND



Ahora compruebe que el DNS esta bien configurado y el dominio este levantado debe hacerle un ping a la dirección en este caso a [www.alessa.com](http://www.alessa.com) lo hará de la siguiente manera **ping www.alessa.com** y de enter, si le envía respuesta como se muestra en la figura el DNS ha sido configurado de manera satisfactoria.



```

root@localhost:/var/named
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost named]# ping www.alessa.com
PING alessa.alessa.com (192.168.12.1) 56(84) bytes of data:
64 bytes from 192.168.12.1: icmp_seq=0 ttl=64 time=0.185 ms
64 bytes from 192.168.12.1: icmp_seq=1 ttl=64 time=0.198 ms
64 bytes from 192.168.12.1: icmp_seq=2 ttl=64 time=0.248 ms
64 bytes from 192.168.12.1: icmp_seq=3 ttl=64 time=0.161 ms
64 bytes from 192.168.12.1: icmp_seq=4 ttl=64 time=0.141 ms
64 bytes from 192.168.12.1: icmp_seq=5 ttl=64 time=0.385 ms

```

Figura 5-97: HACER PING A LA ZONA CREADA [ WWW.ALESSA.COM ]

### 5.12.1.5. CONFIGURACIÓN EN EL CLIENTE

Primero configure la tarjeta de red dándole una dirección de servidor de DNS, lo haremos de la siguiente manera de clic derecho sobre mis sitios de red y seleccione **propiedades**.



Figura 5-98: PROPIEDADES DE MI SITIOS DE RÉD

Se habrá la ventana mis sitios de red seleccione conexión de área local y de clic derecho, seleccione **propiedades**.



Figura 5-99: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL

Entonces se habrá la ventana propiedades de conexión de área local seleccione **protocolo Internet [TCP/IP]**, y de clic en **propiedades**.

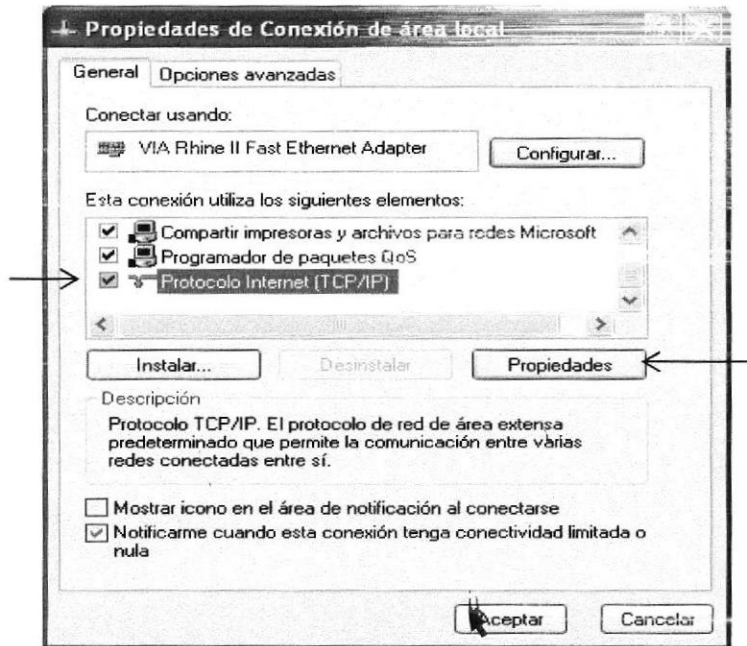


Figura 5-100: PROTOCOLO DE INTERNET PROPIEDADES

Ahora en esta ventana debe seleccionar la casilla **usar la siguiente dirección de servidor de DNS** colóquese en **servidor DNS preferido** y coloque la dirección IP del servidor Linux en la casillas y de un clic en **aceptar** y listo ya tiene el DNS configurado en la tarjeta de red del cliente.

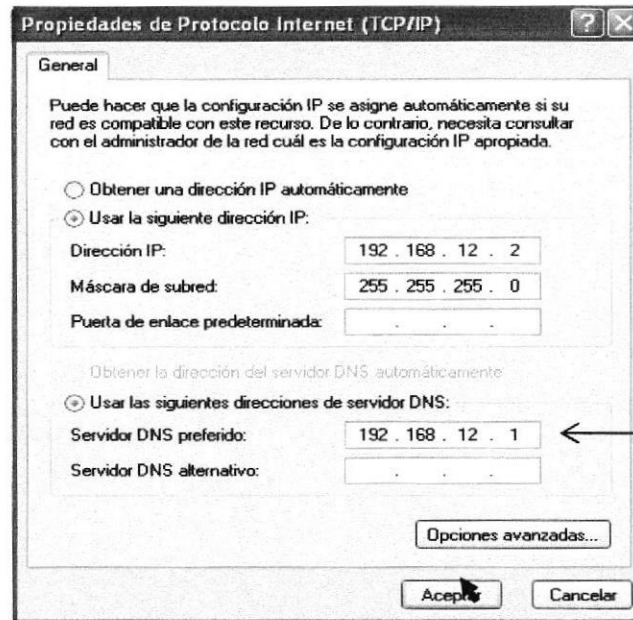


Figura 5-101: PROPIEDADES PROTOCOLO DE INTERNET (TCP/IP)

Ahora va a acceder al servicio DNS en Windows haciéndole un ping al servidor, lo hace de la siguiente manera de clic en **inicio** y seleccione **ejecutar**.

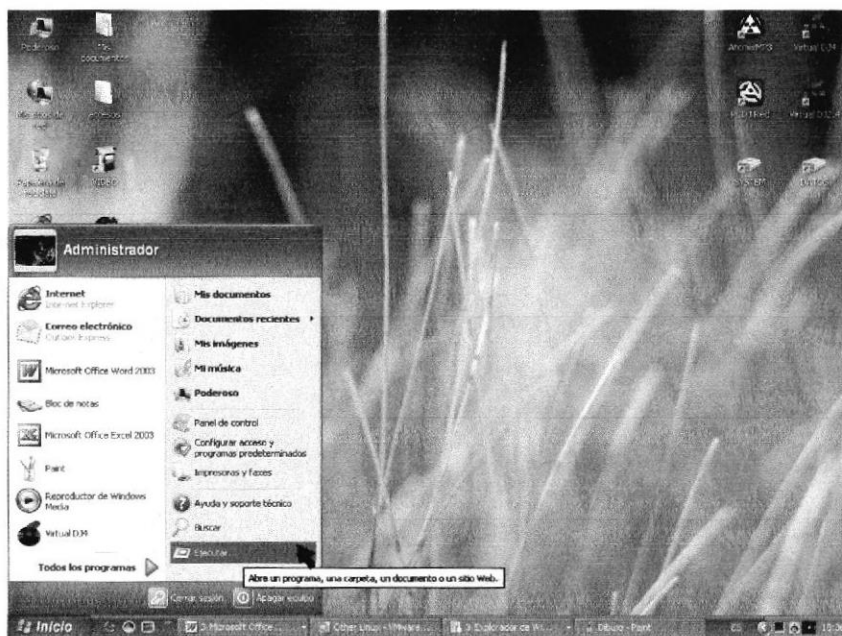


Figura 5-102: INICIO– EJECUTAR

Aparece la ventana de ejecutar pero ya no escriba la dirección IP del servidor Linux si no escriba el nombre que permitió convertir el servicio DNS, para este caso **www.alessa.com** y de un enter.

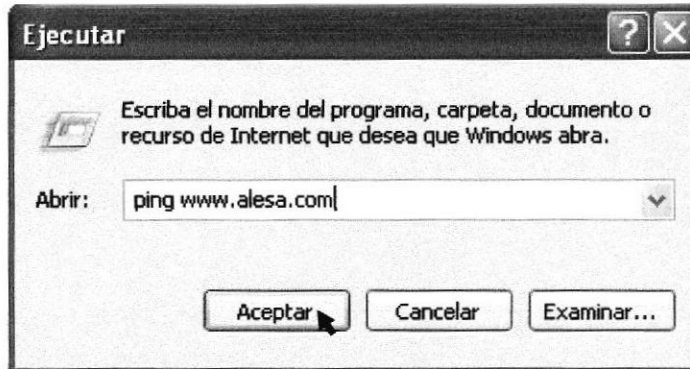


Figura 5-103: EJECUTAR

Ahora si la configuración fue satisfactoria, el ping tiene respuesta como lo muestra en la siguiente imagen.

```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>ping www.alessa.com

Haciendo ping a alessa.alessa.com[192.168.12.1] con 32 bytes de datos:

Respuesta desde 192.168.12.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.12.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.12.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.12.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.12.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Administrador>
```

Figura 5-104: PING AL DOMINIO

## 5.13. WEB SERVER

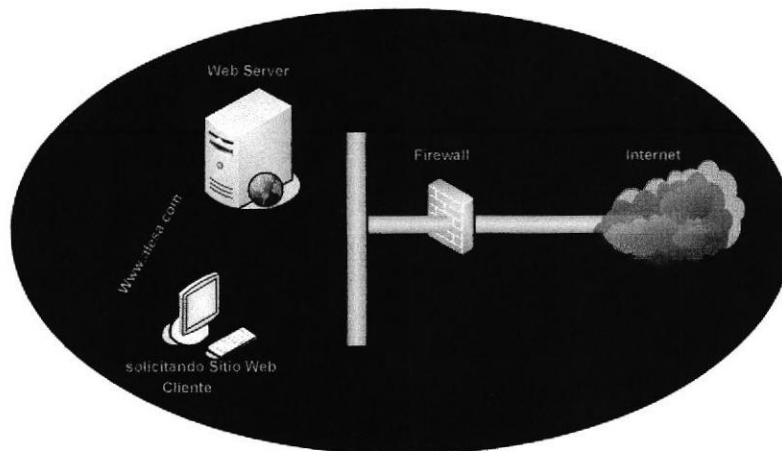


Figura 5-105: WEB SERVER

### 5.13.1. ¿QUÉ ES WEB SERVER?

Un servidor Web es un programa de aplicación que satisface las solicitudes HTTP, FTP, SMTP, HTTPD realizadas por los navegadores. Para ello, el ordenador que la soporta debe estar conectado a Internet o a Intranet y por lo tanto, debe tener asignada una dirección IP.

Una dirección de Internet o Web (a veces llamada dirección URL o Localizador de recursos universal) suele estar compuesta por cuatro partes:

- ✓ Un nombre de protocolo (un conjunto de reglas y estándares que permiten a los equipos intercambiar información).
- ✓ La ubicación del sitio.
- ✓ El nombre de la organización que mantiene el sitio.
- ✓ Un sufijo que identifica la clase de organización de que se trata (como **.com** en el caso de una organización comercial).

Los Servidores Web son aquéllos que permiten a los clientes compartir datos, documentos y multimedia en formato Web. Aunque es parte de la tecnología Cliente-Servidor, el servidor Web aporta algunas ventajas adicionales; como acceso más simple a la información (con un simple clic).

### 5.13.2. REQUISITOS PARA SU CONFIGURACIÓN

- ✓ Una equipo de trabajo con sistema operativo Linux.
- ✓ Tarjeta de red.
- ✓ Tener la tarjeta de red configurada.
- ✓ Paquete httpd instalado.
- ✓ Servicio httpd habilitado.
- ✓ Tener configurado DNS.

### 5.13.3.CONFIGURACIÓN DEL SERVICIO APACHE

Ahora verifique si tiene instalado el paquete de httpd, lo hará con el comando **rpm -qa httpd**, luego de enter y revise.

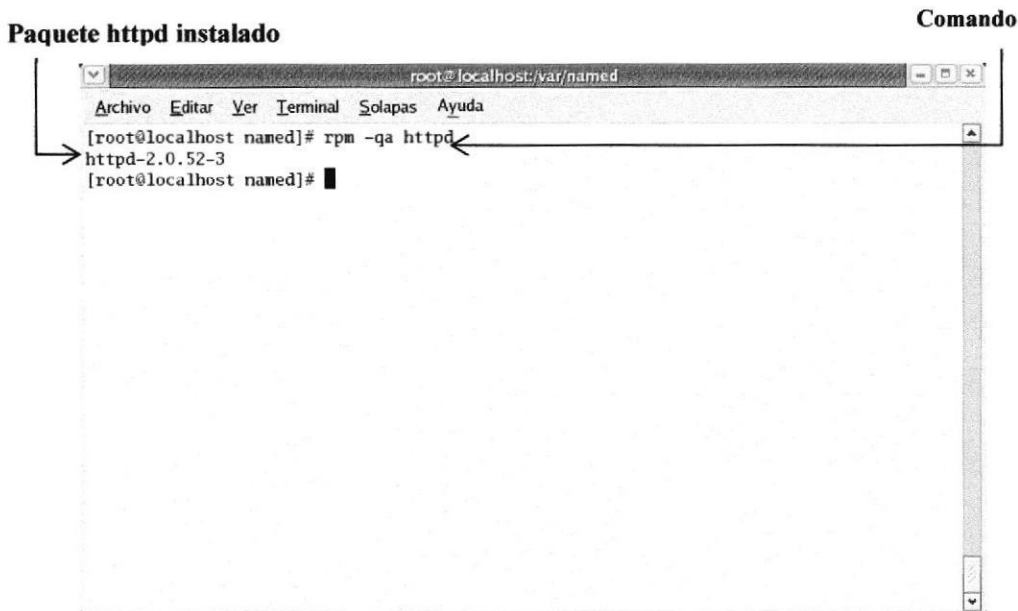


Figura 5-106: VERIFICAR PAQUETE HTTPD

Ahora verifique en el terminal si esta habilitado el servicio httpd de no ser así habilítelo de la siguiente manera, en el terminal escriba el comando **setup** y de enter.

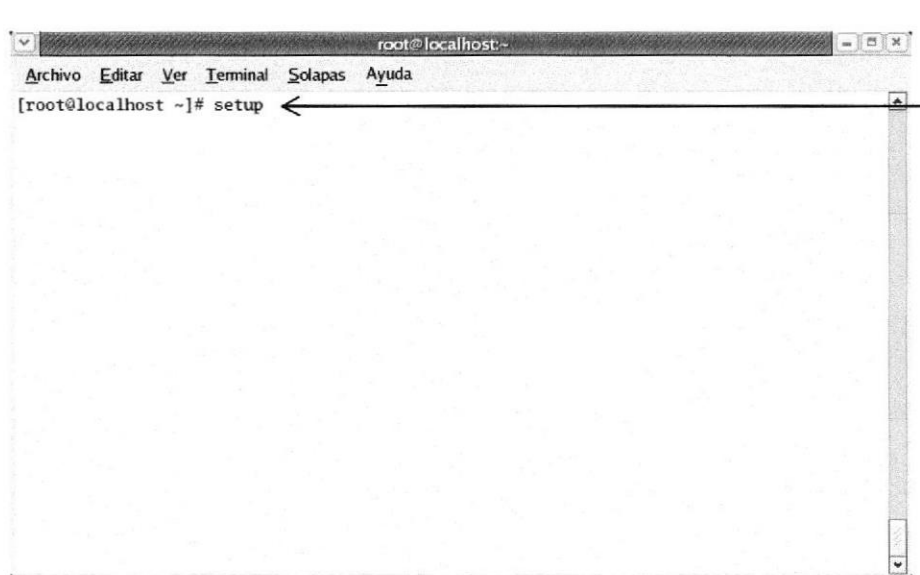


Figura 5-107: COMANDO SETUP

A continuación se abre esta pantalla y con el teclado desplácese hacia la **opción servicios del sistema** con las teclas de direcciones, ahora con la tecla tabulador colóquese en **ejecutar herramienta** y de un enter

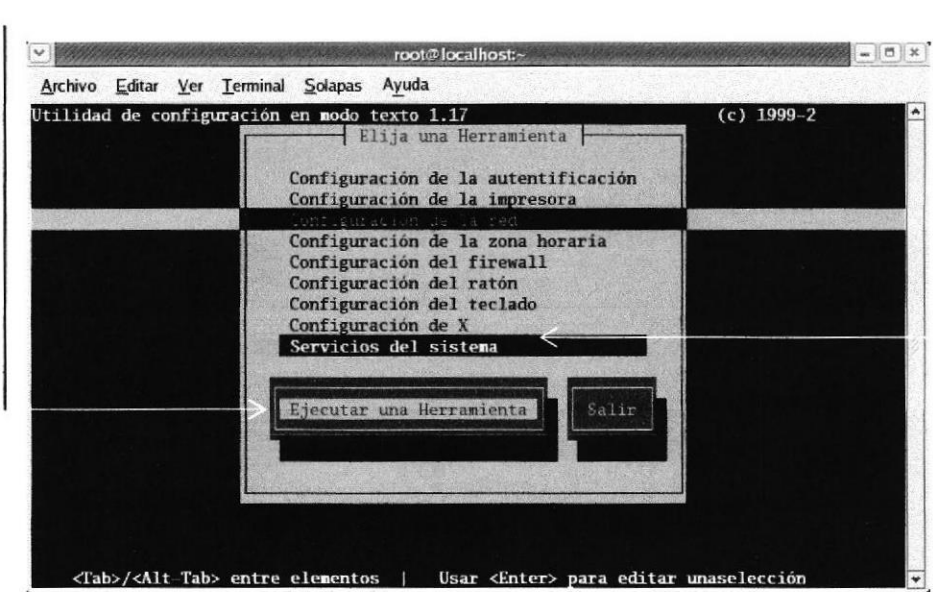


Figura 5-108: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora se abre esta pantalla y con el teclado desplácese hacia la opción **httpd** con las teclas direccionales y si esta opción no se encuentra marcada con un asterisco como lo muestra la imagen presione la tecla barra espaciadora [**\***] para que se marque con el asterisco así estará habilitando el servicio del apache, luego colóquese con la tecla tabulador **OK** y de un enter.

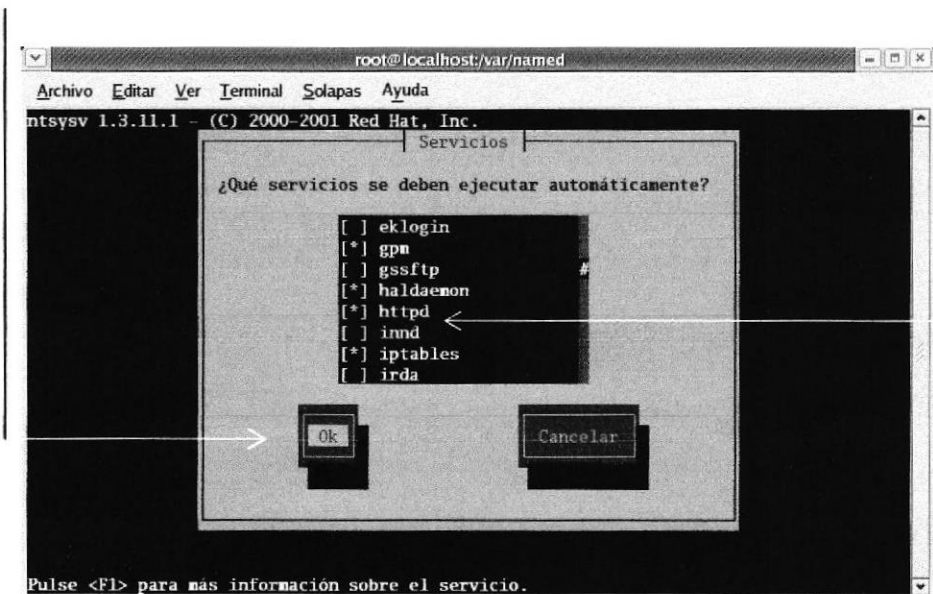
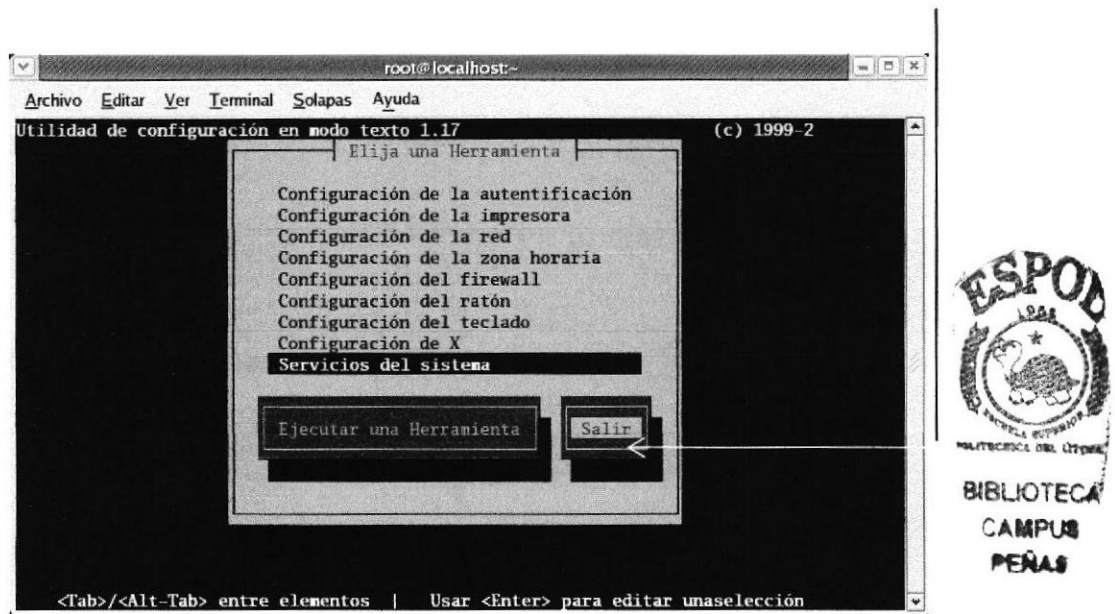


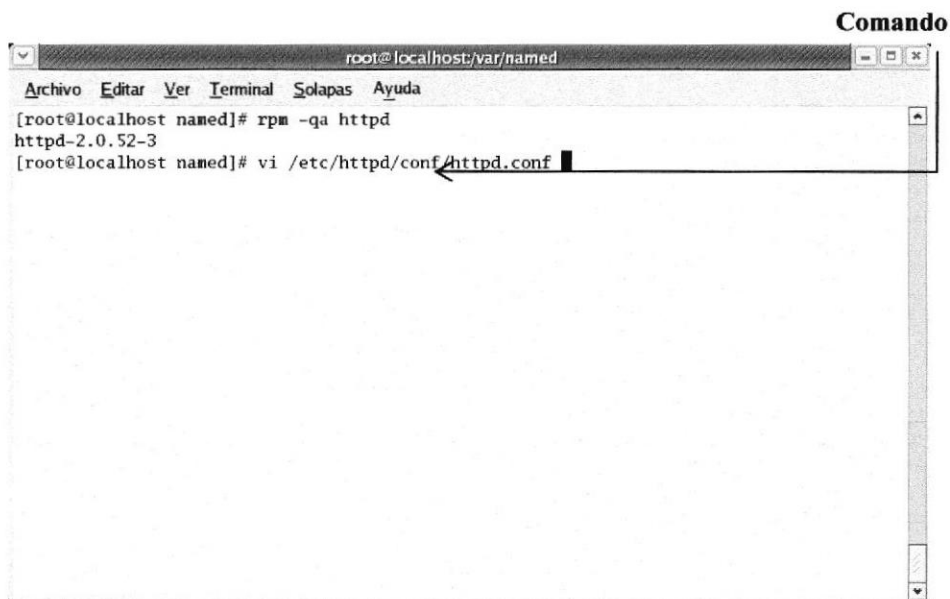
Figura 5-109: HABILITAR EL SERVICIO HTTPD

A continuación aparece esta pantalla y con la tecla tabulador colóquese en **salir** y de un enter y a ha habilitado el servicio httpd.



**Figura 5-110: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO**

Ahora edite el fichero `httpd.conf` que se encuentra en el directorio `/etc/httpd/conf`, para esto ingrese el comando `vi`, de la siguiente manera, `vi /etc/httpd/conf/httpd.conf` y de un enter.



**Figura 5-111: EDITAR EL FICHERO HTTPD.CONF**

Entonces edite el fichero `httpd.conf`, por lo general las líneas que va a buscar se encuentran descomentadas, de no ser así debe descomentarlas.

- ✓ **Listen 80** el puerto por donde va a escuchar, por donde va a llegar la Internet.
- ✓ **DocumentRoot var/www/html** esta línea indica la ruta en donde se va almacenar nuestro directorio con el sitio Web.
- ✓ **Directory Index index.html index.htm** esta línea indica los ficheros y las extensiones que se puede abrir, como en este caso una página Web por lo general son index.html.
- ✓ **NameVirtualHost\*:80** esta línea indica que puede levantar varias zonas.

**Listen 80**

```

root@localhost:var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#Listen 12.34.56.78:80
Listen 80
#
# Dynamic Shared Object (DSO) Support
#
LoadModule auth_ldap_module modules/mod_auth_ldap.so
133,1 13%

```

**Figura 5-112: FICHERO HTTPD.CONF [LISTEN 80]****DocumentRoot var/www/html**

```

root@localhost:var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# DocumentRoot "/var/www/html"
#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
# First, we configure the "default" to be a very restrictive set of
# features.
#
265,1 25%

```

**Figura 5-113: FICHERO HTTPD.CONF [DOCUMENTROOT]****Directory Index index.html index.htm**

```

root@localhost:var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# negotiated documents. The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.html index.html.var
#
# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives. See also the AllowOverride
# directive.
#
372,1 37%

```

**Figura 5-114: FICHERO HTTPD.CONF [DIRECTORY INDEX]****NameVirtualHost\*:8**

```

root@localhost:var/named
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# Use name-based virtual hosting.
#
NameVirtualHost *:80
#
# NOTE: NameVirtualHost cannot be used without a port specifier
# (e.g. :80) if mod_ssl is being used, due to the nature of the
# SSL protocol.
#
1003,1 Final

```

**Figura 5-115: FICHERO HTTPD.CONF [NAME VIRTUAL HOST]**

Ahora ubíquese en la parte final del fichero y agregue las siguientes líneas,

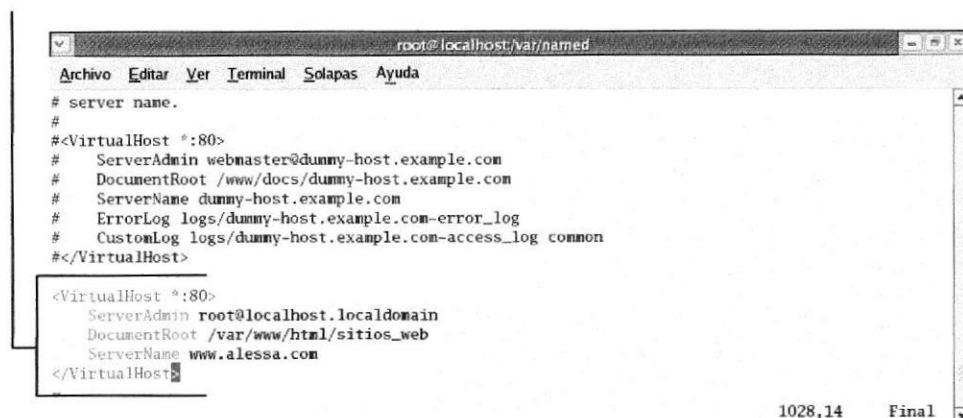
**<VirtualHost \*:80>**

**ServerAdmin** esta línea indica el nombre del equipo de trabajo y el usuario.

**DocumentRoot** esta línea indica la ruta en la cual se encuentra el directorio en donde tendrá alojado el sitio Web.

**ServerName** en esta línea debe especificar la dirección de la página.

**</VirtualHost \*:80>**



```

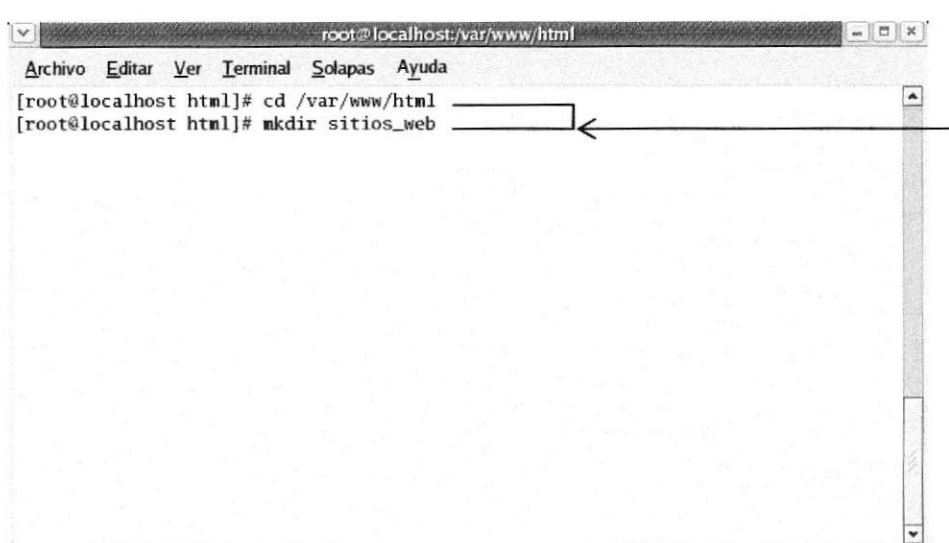
root@localhost:/var/named
Archivo Editar Ver Terminal Solapas Ayuda
# server name.
#
#<VirtualHost *:80>
#   ServerAdmin webmaster@dummy-host.example.com
#   DocumentRoot /www/docs/dummy-host.example.com
#   ServerName dummy-host.example.com
#   ErrorLog logs/dummy-host.example.com-error_log
#   CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>

<VirtualHost *:80>
  ServerAdmin root@localhost.localdomain
  DocumentRoot /var/www/html/sitios_web
  ServerName www.alessa.com
</VirtualHost>
1028,14 Final

```

Figura 5-116: FICHERO HTTPD.CONF [VIRTUAL HOST]

A continuación cree el directorio que contendrá el sitio Web en el directorio y la ruta que especifica en el Document Root, lo hará de la siguiente manera, **cd /var/www/html** para ubicarse en la ruta, paso siguiente cree el directorio **mkdir sitios\_web** listo ahora de un enter.



```

root@localhost:/var/www/html
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost html]# cd /var/www/html
[root@localhost html]# mkdir sitios_web

```

Figura 5-117: CREACIÓN DE DIRECTORIO SITIOS \_ WEB



Se habrá el Internet Explorer seleccione el menú **herramientas** y déle clic en **opciones de Internet**.

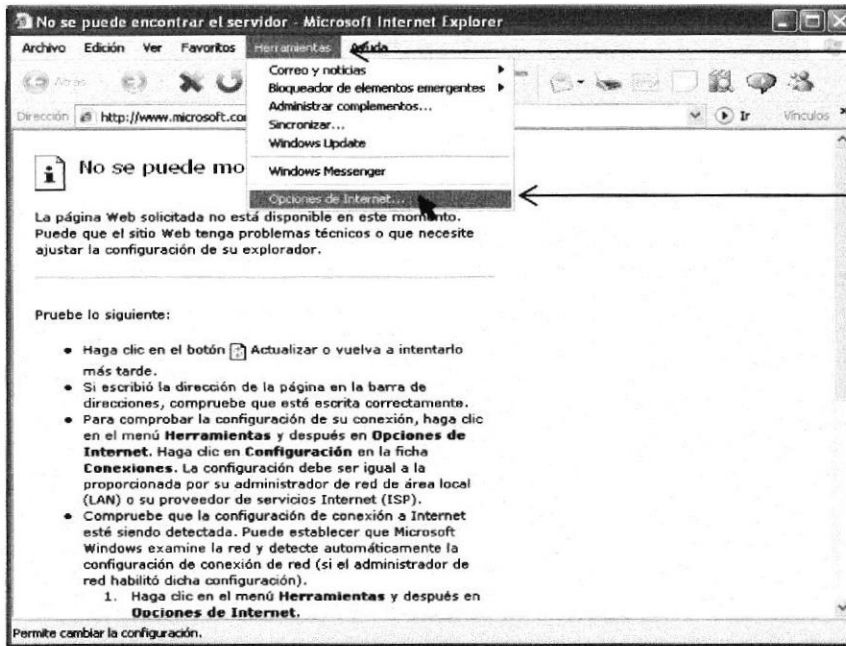


Figura 5-120: HERRAMIENTAS - OPCIONES DE INTERNET

Entonces se habrá la ventana opciones de Internet seleccione la pestaña **conexiones** y déle un clic en **configuración de LAN**.

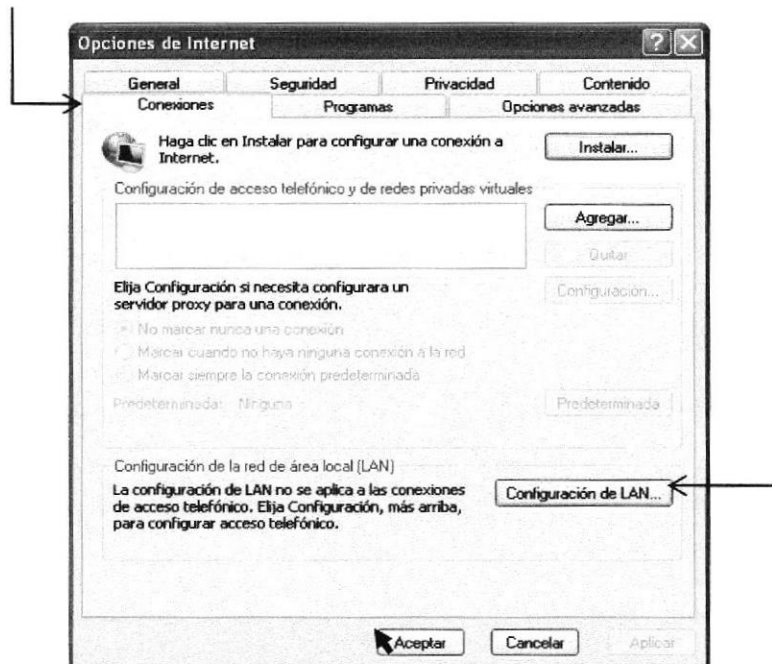


Figura 5-121: OPCIONES DE INTERNET

Ahora en esta ventana debe seleccionar la casilla **detectar la configuración automáticamente** déle clic en aceptar y listo esta configurado el cliente.

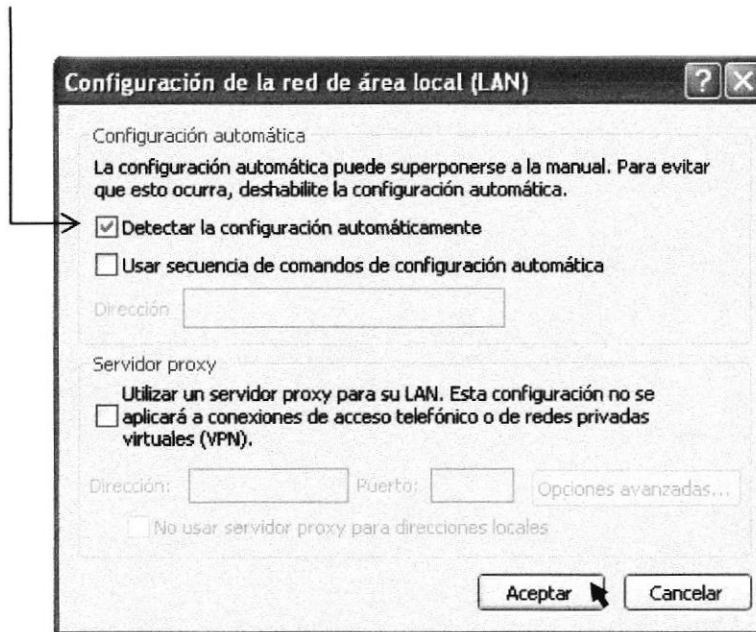


Figura 5-122: CONFIGURACIÓN DE LA RED DE ÁREA LOCAL (LAN)

Ahora va a acceder al sitio Web, para esto use el navegador en la casilla de **dirección** coloque la dirección de la pagina para este caso **www.alesa.com** damos un enter y la pagina requerida debe cargarse en su explorador esto indicara que las configuraciones realizadas han sido satisfactoria.

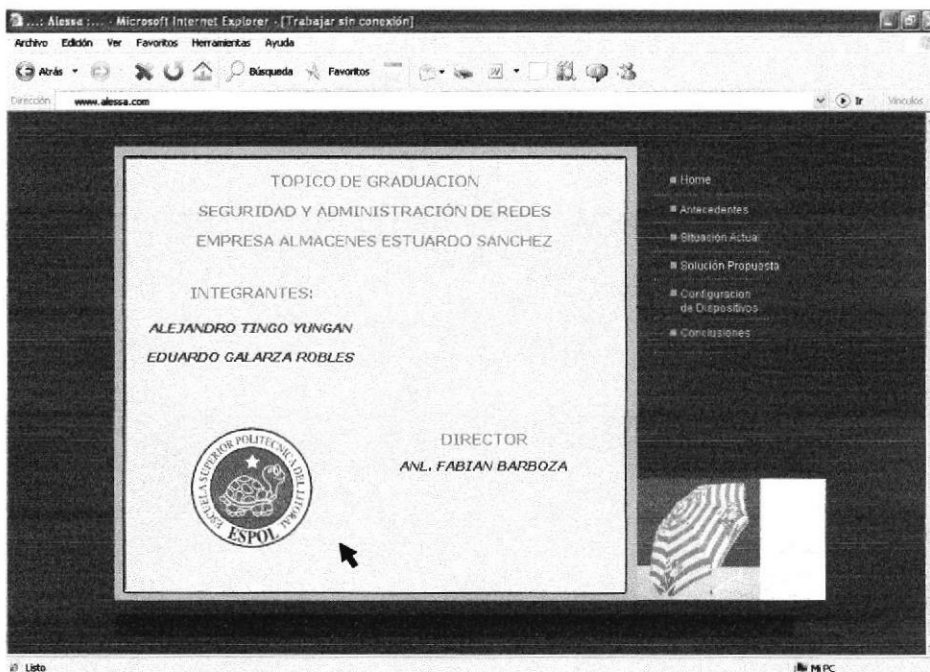


Figura -123: CARGANDO EL SITIO | WWW.ALESSA.COM |

## 5.14.SERVIDOR DE CORREO

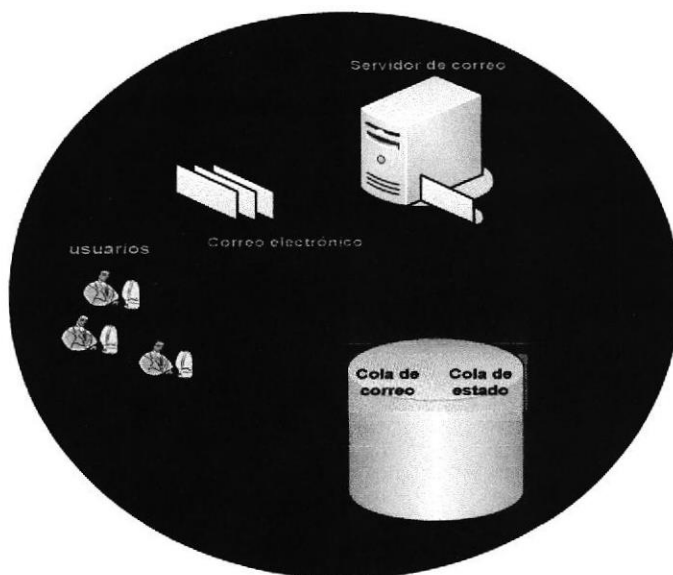


Figura 5-124: SERVIDOR DE CORREO

### 5.14.1.¿QUÉ ES EL SERVIDOR DE CORREO?

Sendmail es el agente de transporte de correo más común de Internet en los sistemas Linux, aunque actúa principalmente como MTA (Mail Transport Agent), que son los encargados de transferir los mail a su correcto destino.

En realidad, un servidor de correo consta 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.

- ✓ **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 pasarlos al usuario.
- ✓ **IMAP** (Internet Message Access Protocol), su finalidad es la misma que el pop, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

El servidor de correo permitirá a los usuarios revisar correos electrónicos, correos locales enviándose rápidamente y agilizando la comunicación, compartiendo la información de forma fácil y segura, también cuenta con filtros para rechazar archivos con posibles virus o por contenido que no sean de interés para su empresa, usando programas determinados como el Outlook.

### 5.14.2. REQUISITOS PARA SU CONFIGURACIÓN

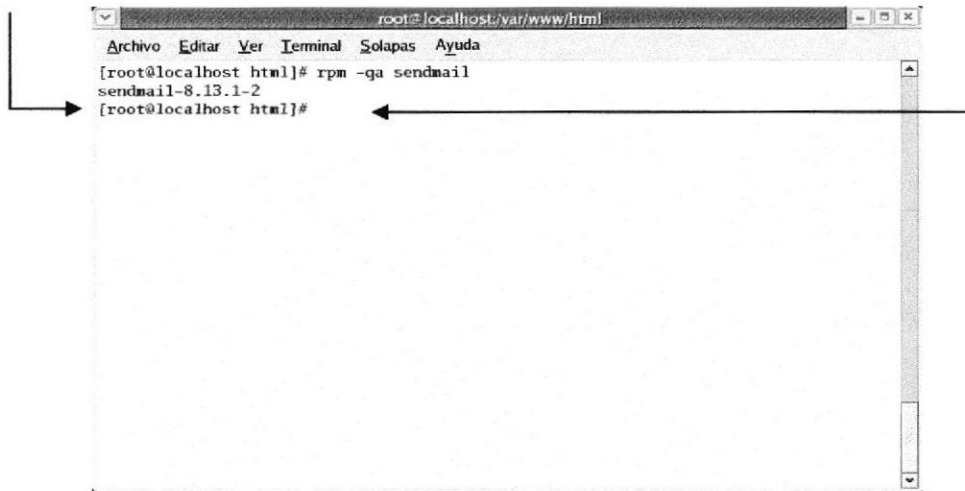
- ✓ Una equipo de trabajo con sistema operativo Linux.
- ✓ Tarjeta de red.
- ✓ Tener la tarjeta de red configurada.
- ✓ Paquete sendmail instalado.
- ✓ Servicio sendmail habilitado.
- ✓ Servicio dovecot habilitado.

### 5.14.3. CONFIGURACIÓN DEL SERVIDOR DE CORREO

Ahora verifique si tiene instalado el paquete sendmail, lo hará con el comando **rpm -qa sendmail**, luego de enter y revise.

Paquete sendmail instalado

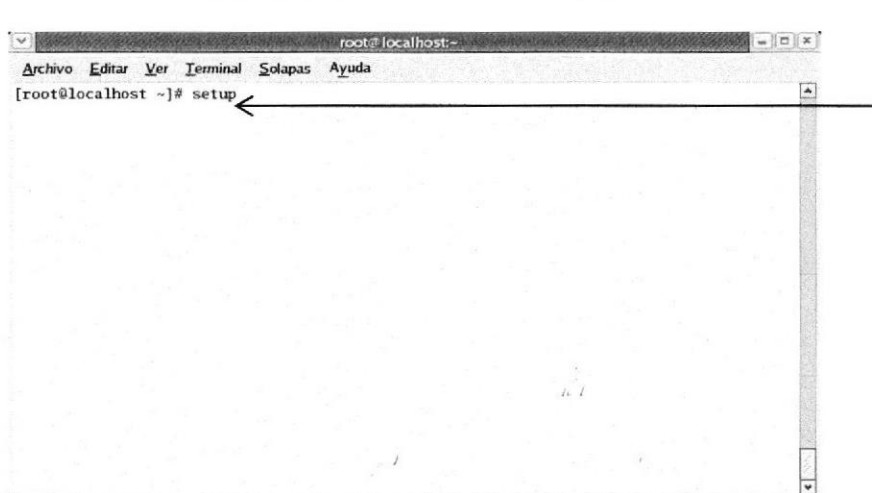
Comando



```
root@localhost:~/var/www/html
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost html]# rpm -qa sendmail
sendmail-8.13.1-2
[root@localhost html]#
```

Figura 5-125: VERIFICAR EL PAQUETE SENDMAIL

Ahora verifique si esta habilitado el servicio sendmail de no ser así lo habilítelo de la siguiente manera, en el terminal escriba el comando **setup** y déle enter.



```
root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# setup
```

Figura 5-126: COMANDO SETUP

A continuación se abre esta pantalla y con el teclado desplácese hacia la **opción servicios del sistema** con las teclas de direcciones, ahora con la tecla tabulador colóquese en **ejecutar herramienta** y déle un enter

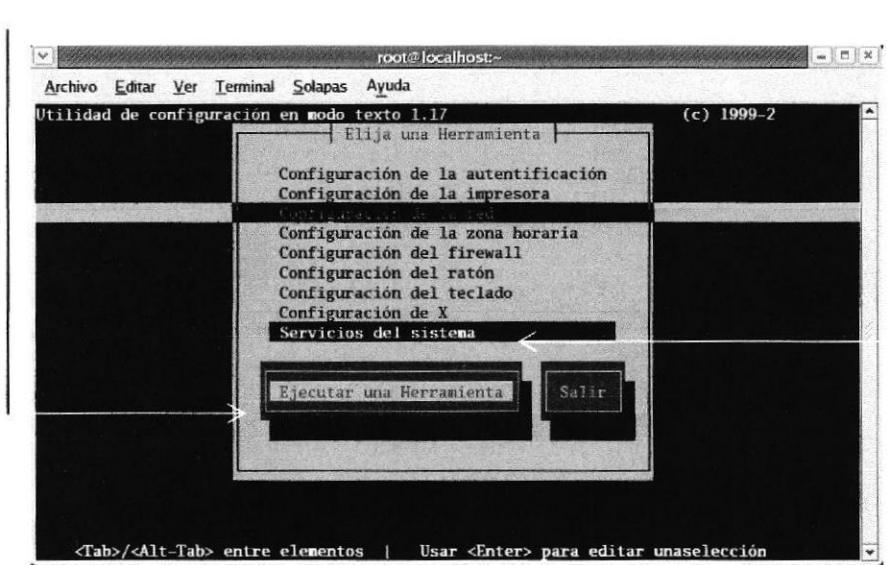


Figura 5-127: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora se abre esta pantalla con el teclado desplácese hacia la opciones **dovecot** y **sendmail** con las teclas direccionales y si esta opción no se encuentra marcada con un asterisco como lo muestra la imagen presione la tecla barra espaciadora, para que se marque [\*] con el asterisco así estará habilitando el servicio requerido, luego colóquese con la tecla tabulador **OK** y déle un enter.

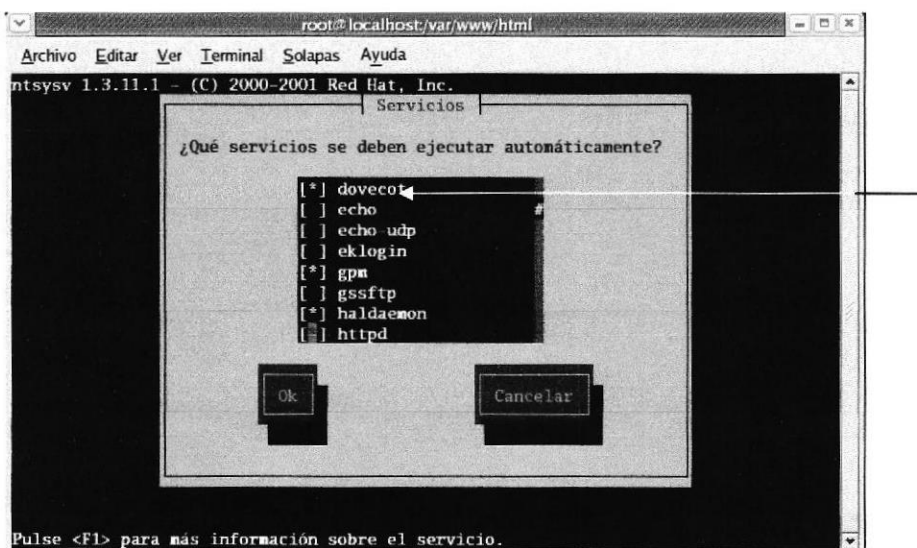


Figura 5-128: HABILITAR SERVICIO DOVECOT

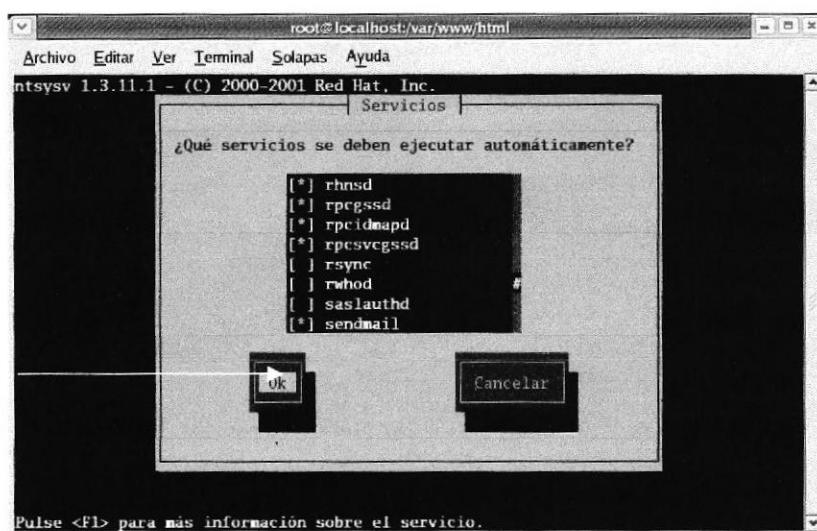


Figura 5-129: HABILITAR SERVICIO SENDMAIL

A continuación aparece esta pantalla y con la tecla tabulador colóquese en salir y de un enter y a ha habilitado el servicio requerido.



Figura 5-130: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora edite el fichero network que se encuentra en el directorio /etc/sysconfig, para esto ingrese el comando vi, de la siguiente manera, **vi /etc/sysconfig/network** y de un enter.

Comando

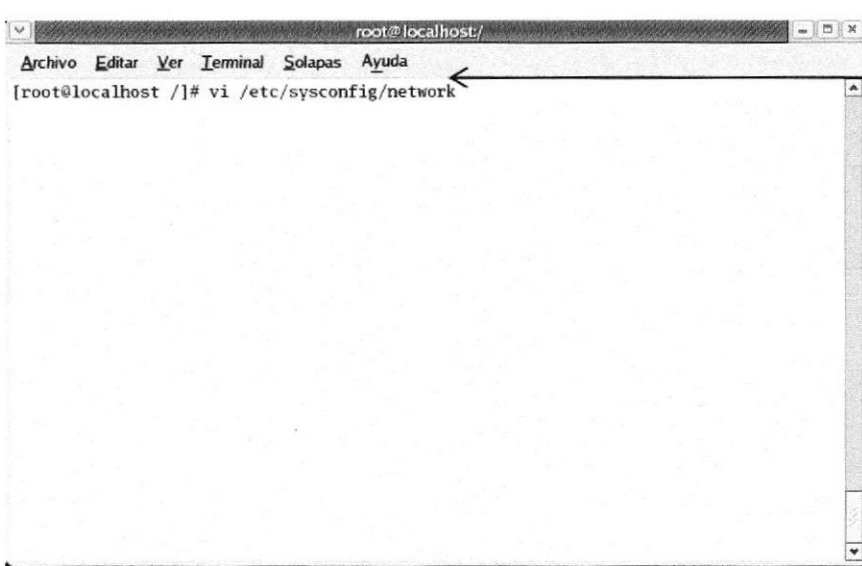


Figura 5-131: INGRESAR AL FICHERO NETWORK

Entonces edite el fichero network, debe agregar la línea **HOSTNAME=alessa.com**, guarde los cambios realizados y salga.

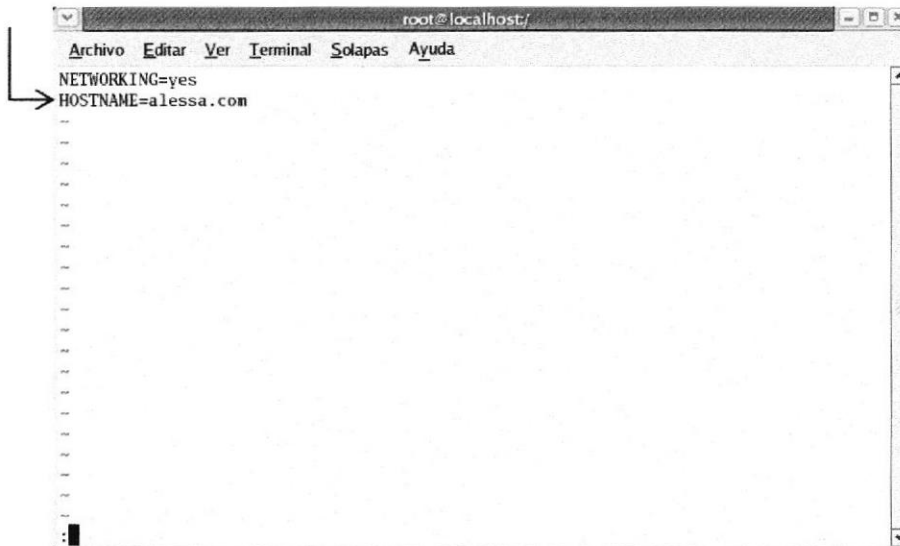
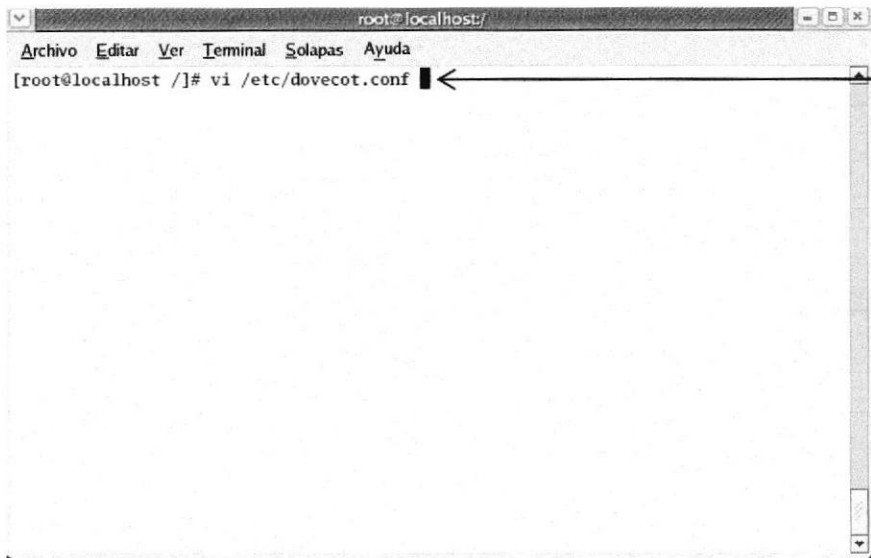


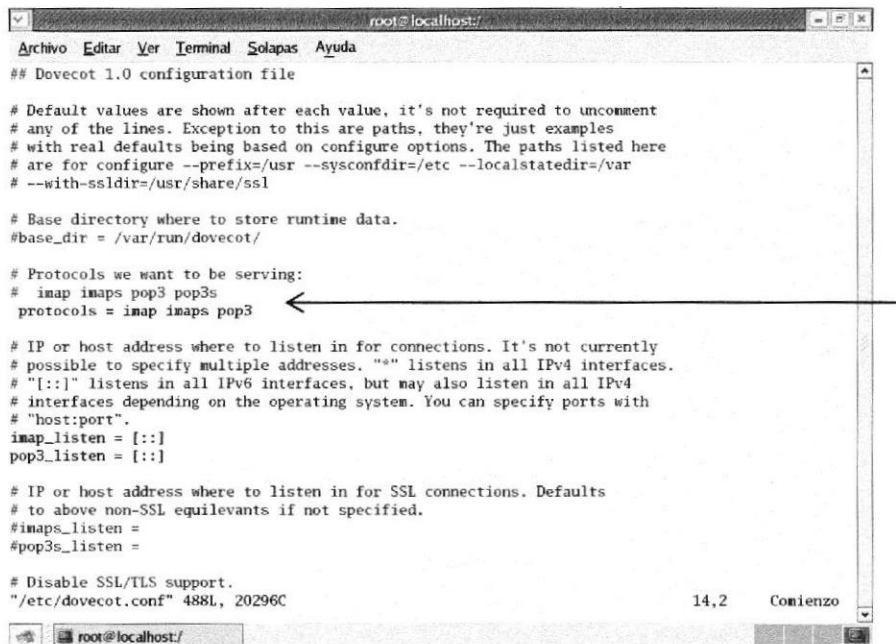
Figura 5-132: EDITAR EL FICHERO NETWORK

Ahora va a editar el fichero `dovecot.conf` que se encuentra en el directorio `/etc`, para esto ingrese el comando `vi` de la siguiente manera `vi /etc/dovecot.conf` y de un enter.



**Figura 5-133: INGRESAR AL FICHERO DOVECOT.CONF**

Ahora edite el fichero `dovecot.conf`, debe descomentar la línea de los protocolos y agregar el protocolo **pop3**.



**Figura 5-134: EDITAR FICHERO DOVECOT.CONF [PROTOCOLS]**

Debe iniciar el servicio dovecot y a la vez se levantara el puerto 110, con el comando `service dovecot start` de la siguiente manera **service dovecot start** y déle un enter si la configuración no tiene ningún error o problema saldrán mensajes de **[OK]** indicándole que la configuración ha sido satisfactoria.

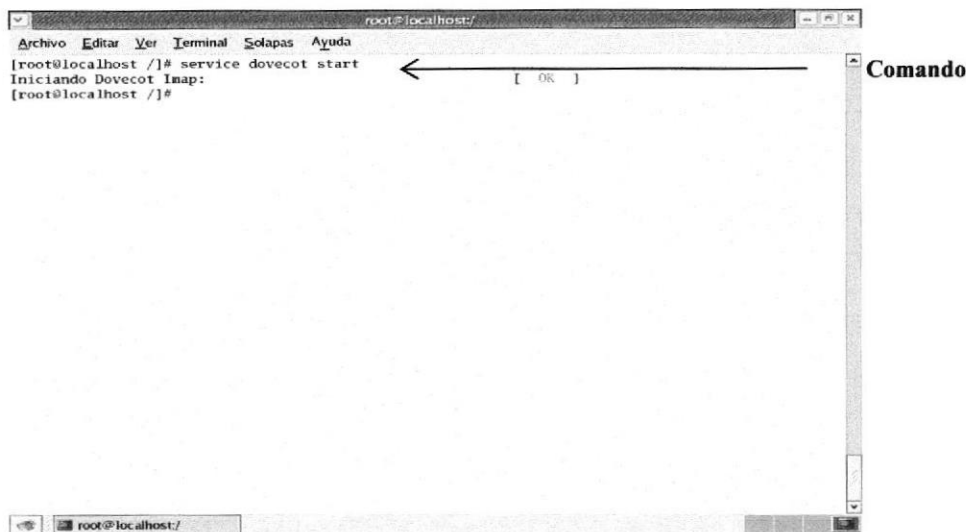


Figura 5-135: INICIAR SERVICIO DOVECOT

Ahora va ah editar el fichero `sendmail.cf` que se encuentra en el directorio `/etc/mail`, para esto ingrese el comando `vi /etc/mail/sendmail.cf` y déle un enter.

Comando

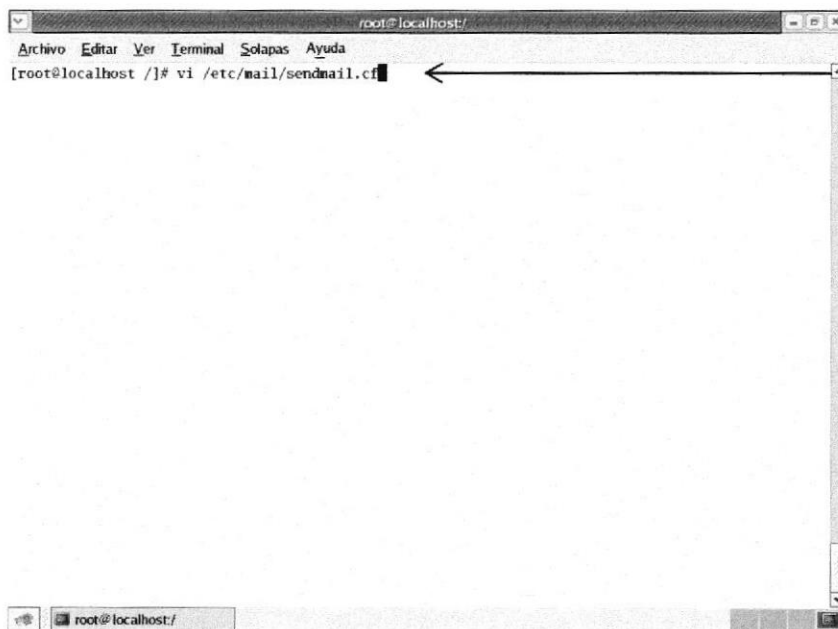
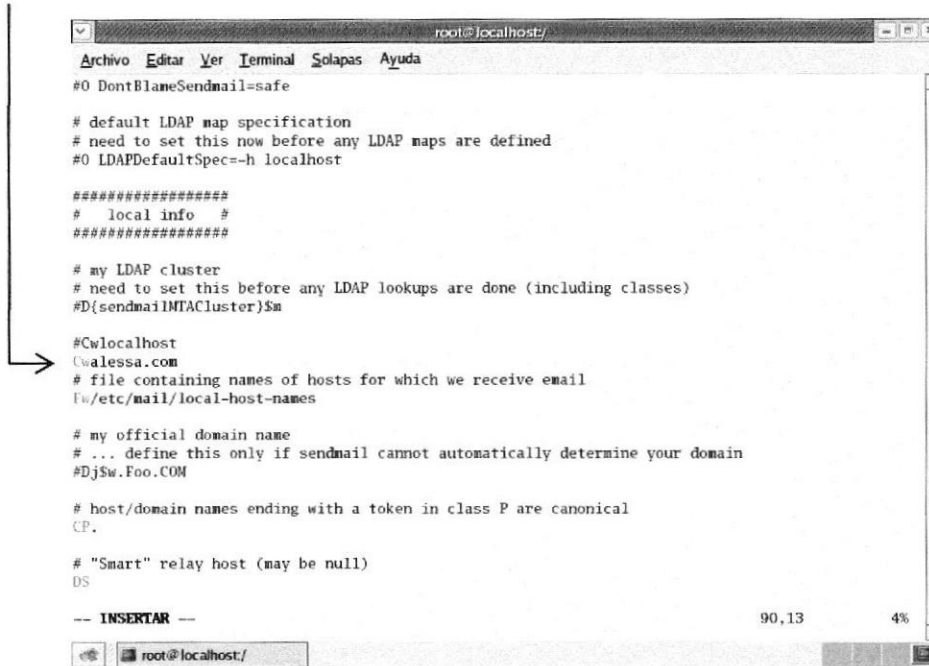


Figura 5-136: INGRESAR AL FICHERO SENDMAIL

Ahora entonces edite el fichero `sendmail.cf`, debe buscar la línea `Cwlocalhost` y es donde se especifica el dominio y rempácela por `Cwalesa.com`.



```

root@localhost/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#0 DontBlaneSendmail=safe

# default LDAP map specification
# need to set this now before any LDAP maps are defined
#0 LDAPDefaultSpec=-h localhost

#####
# local info #
#####

# my LDAP cluster
# need to set this before any LDAP lookups are done (including classes)
#D{sendmailMTACluster}$a

#Cwlocalhost
Cwalesa.com
# file containing names of hosts for which we receive email
f~/etc/mail/local-host-names

# my official domain name
# ... define this only if sendmail cannot automatically determine your domain
#Dj$w.Foo.COM

# host/domain names ending with a token in class P are canonical
CP.

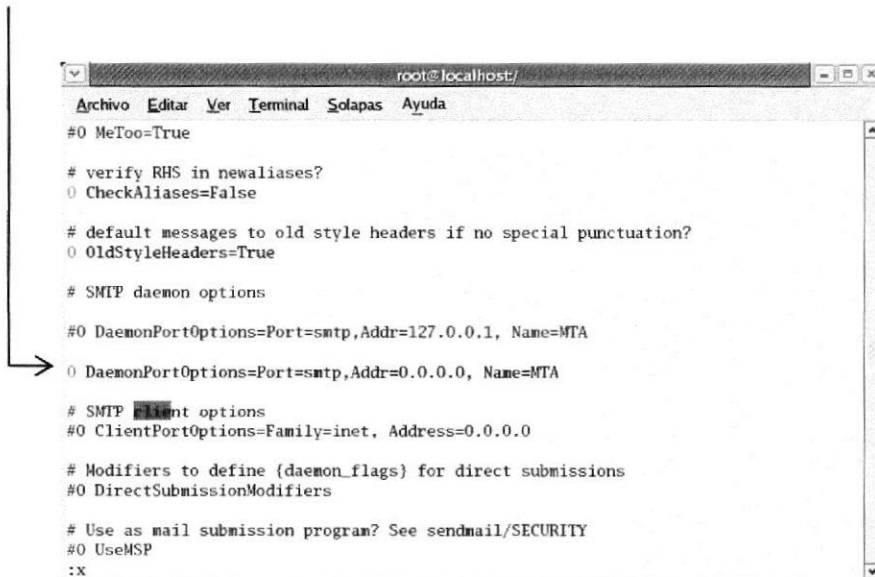
# "Smart" relay host (may be null)
DS

-- INSERTAR --                               90,13      4%
root@localhost/

```

Figura 5-137: EDITAR FICHERO SENDMAIL [CWLOCALHOST]

En el mismo directorio busque esta línea `DaemonPortOptions=Port=smtplib,Addr=127.0.0.1,Name=MTA`, y rempácela por `DaemonPortOptions=Port=smtplib,Addr=0.0.0.0,Name=MTA`, y guarde los cambios realizados y salga.



```

root@localhost/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#0 MeToo=True

# verify RHS in newaliases?
0 CheckAliases=False

# default messages to old style headers if no special punctuation?
0 OldStyleHeaders=True

# SMTP daemon options
#0 DaemonPortOptions=Port=smtplib,Addr=127.0.0.1,Name=MTA
0 DaemonPortOptions=Port=smtplib,Addr=0.0.0.0,Name=MTA

# SMTP client options
#0 ClientPortOptions=Family=inet,Address=0.0.0.0

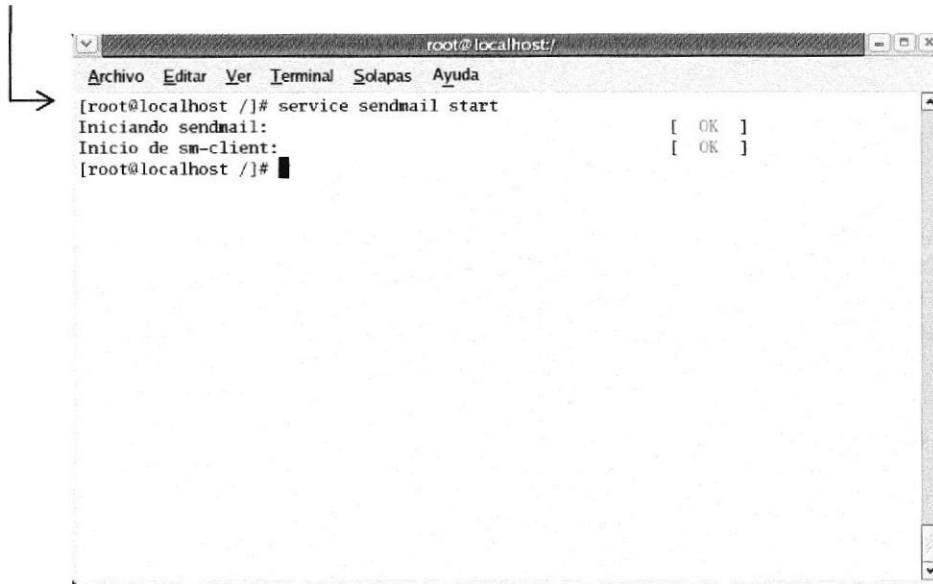
# Modifiers to define (daemon_flags) for direct submissions
#0 DirectSubmissionModifiers

# Use as mail submission program? See sendmail/SECURITY
#0 UseMSP
:x

```

Figura 5-138: EDITAR FICHERO SENDMAIL [DAEMONPORTOPTIONS]

Debe iniciar el servicio sendmail, con el comando `service sendmail start` de la siguiente manera **service sendmail start** y déle un enter si la configuración no tiene ningún error o problema saldrán mensajes de **[OK]** indicándole que la configuración ha sido satisfactoria.



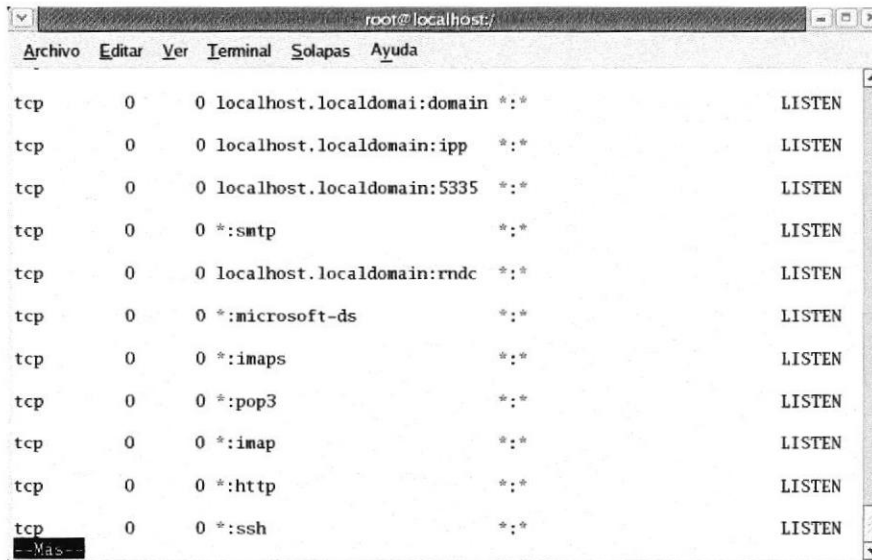
```

root@localhost/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# service sendmail start
Iniciando sendmail:           [ OK ]
Inicio de sm-client:         [ OK ]
[root@localhost /]#

```

**Figura 5-139: INICIAR SERVICIO SENDMAIL**

Ahora va a verificar si los puertos de descarga y de recibo 110 y 125 respectivamente están habilitados.



```

root@localhost/
Archivo Editar Ver Terminal Solapas Ayuda
tcp        0      0 localhost.localdomai:domain *.* LISTEN
tcp        0      0 localhost.localdomain:ipp *.* LISTEN
tcp        0      0 localhost.localdomain:5335 *.* LISTEN
tcp        0      0 *:smtp *.* LISTEN
tcp        0      0 localhost.localdomain:rndc *.* LISTEN
tcp        0      0 *:microsoft-ds *.* LISTEN
tcp        0      0 *:inaps *.* LISTEN
tcp        0      0 *:pop3 *.* LISTEN
tcp        0      0 *:inap *.* LISTEN
tcp        0      0 *:http *.* LISTEN
tcp        0      0 *:ssh *.* LISTEN

```

**Figura 5-140: VERIFICAR PUERTOS 110 Y 125**

### 5.14.3.1. CONFIGURACIÓN EN EL CLIENTE

Primero va a abrir el programa de correo electrónico para este caso Outlook de clic en inicio seleccione **todos los programas** y déle clic en **Outlook Express**.

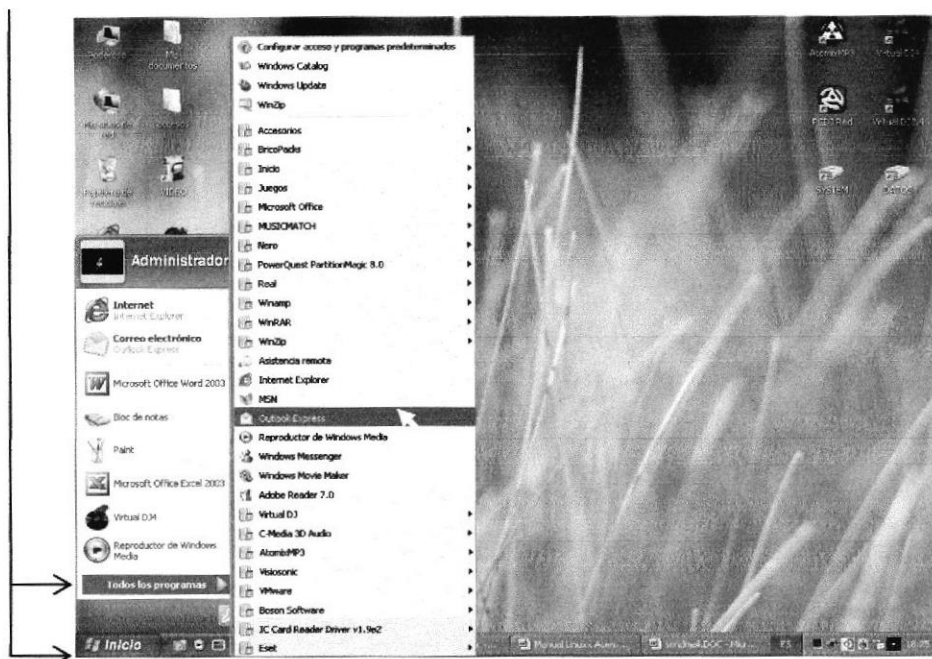


Figura 5-141: ABRIR OUTLOOK EXPRESS

Estando abierto el Outlook Express cree una cuenta, déle clic en el menú Herramientas y elija la opción **Cuentas** y el asistente se abrirá y siga las instrucciones.

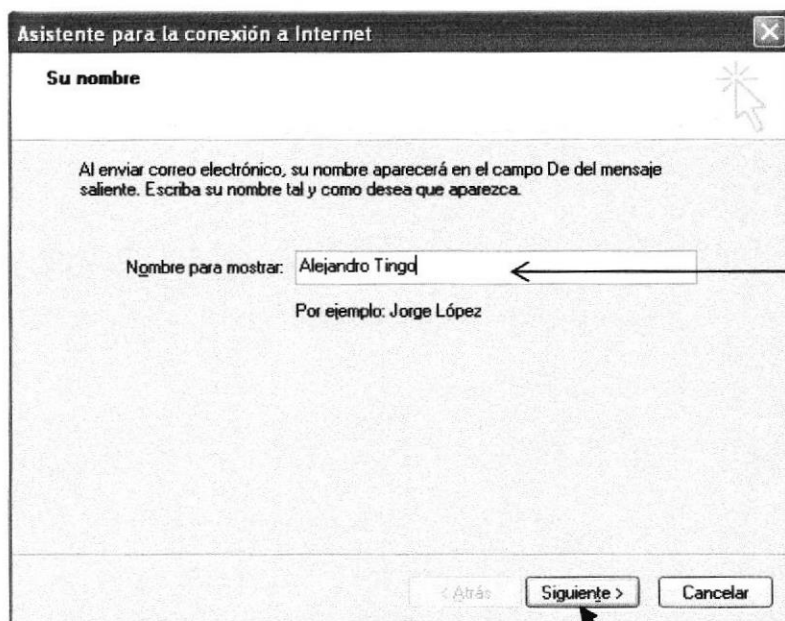


Figura 5-142: AGREGAR NOMBRE A LA CUENTA

El asistente indica que debe crear una dirección de correo asociada con la dirección que creo en Linux y de clic en **Siguiente**.

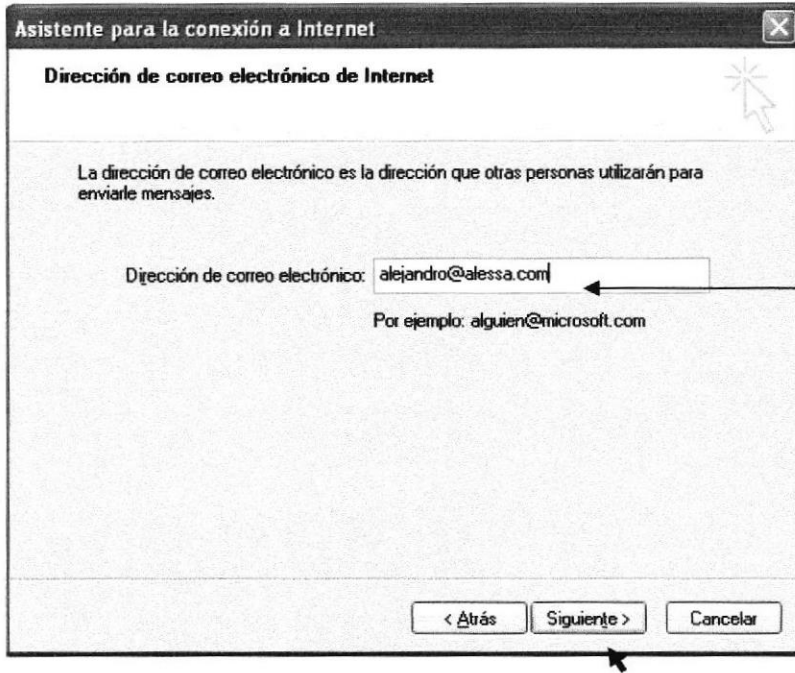


Figura 5-143: AGREGAR DIRECCIÓN DE CORREO ELECTRONICO

El asistente indica que debe especificar el servidor de correo entrante (POP3) y el servidor de correo saliente (SMTP), en este caso los dos son la misma dirección del servidor Linux, y de clic en **Siguiente**.

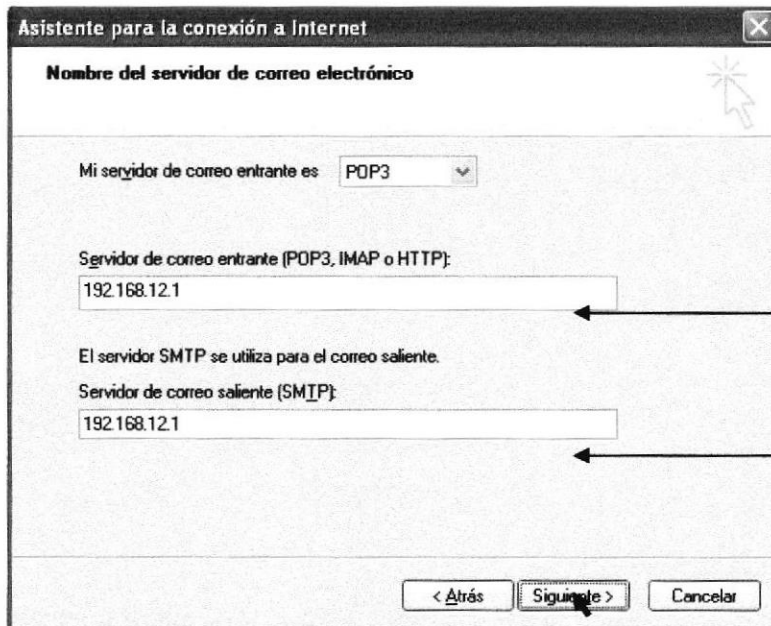


Figura 5-144: ESPECIFICAR SERVIDOR DE CORREO ENTRANTE Y SALIENTE

El asistente indica que debe ingresar el nombre de usuario y la contraseña los mismos que ya creo en el servidor de correo Linux, y de clic en **Siguiente**.

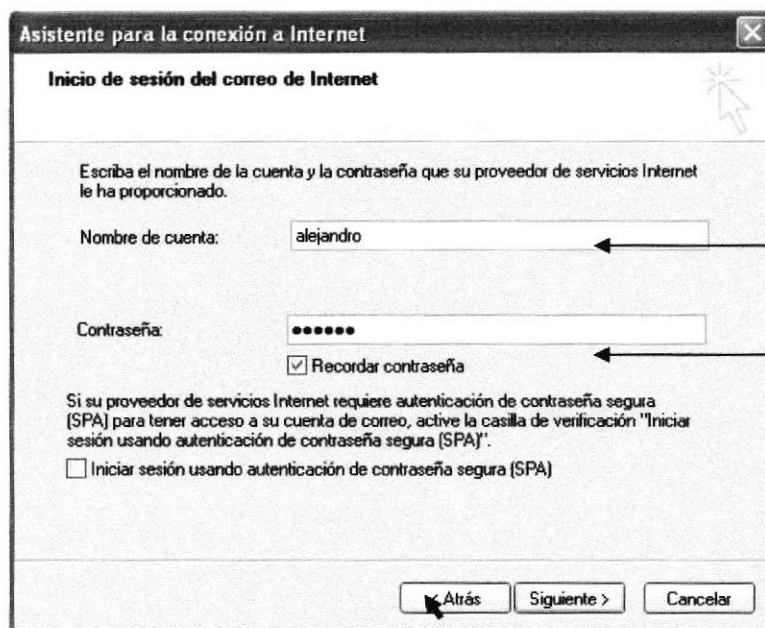


Figura 5-145: INGRESAR USUARIO Y CONTRASEÑA



El asistente le pregunta si toda la información ingresada es correcta, de ser así de clic en el botón **Finalizar**.

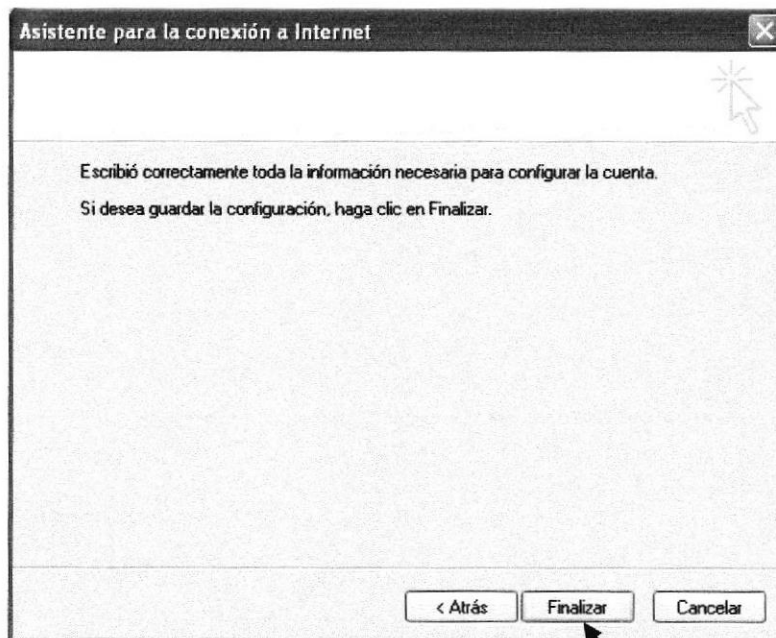


Figura 5-146: CREACIÓN DE CUENTA FINALIZADA

Ya creada la cuenta, estas listo para enviar y recibir mail.

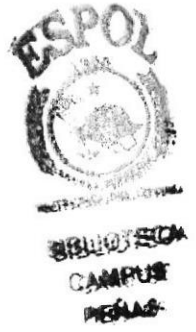
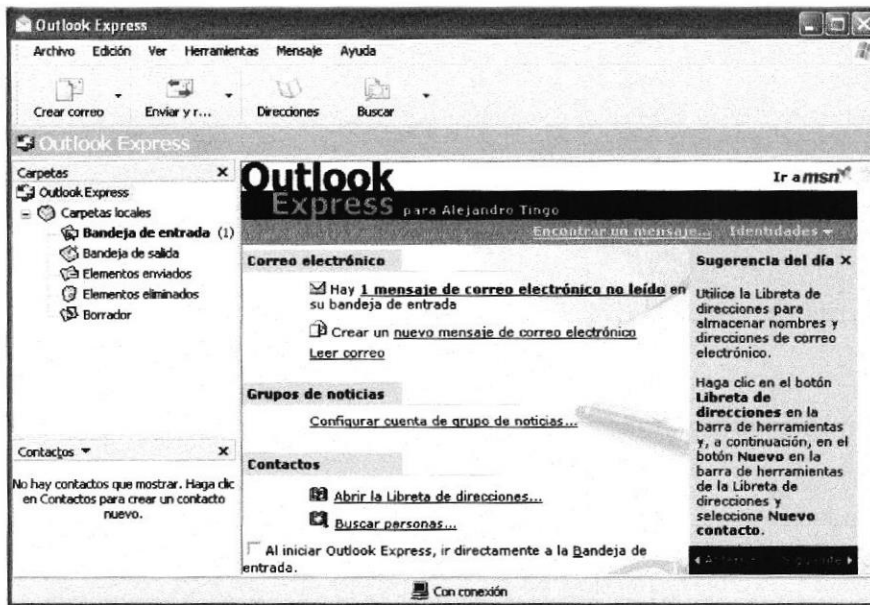


Figura 5-147: BANDEJA DE ENTRADA

A continuación realice una prueba de envío de correo del cliente al root al super usuario de Linux que se encuentra en el servidor, de clic en **crear correo**, aparecerá la ventana para crear el mensaje llene los casilleros con los datos requeridos, llene el casillero **para**, que es el mas importante **root@alessa.com**, es el que especifica el destinatario, finalmente de clic en enviar.

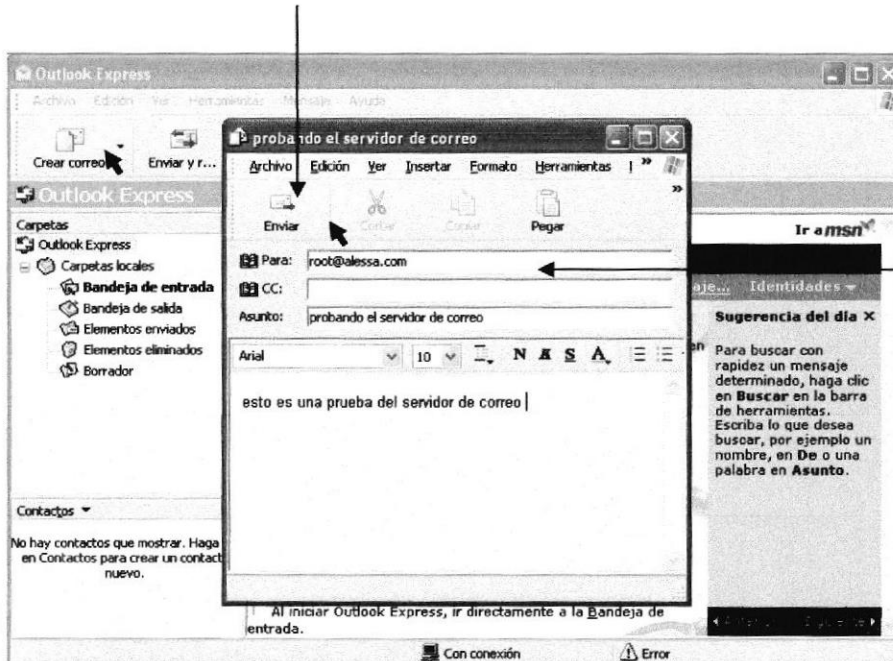


Figura 5-148: ENVIÓ DE CORREO

Ahora verifique si el correo fue enviado con éxito, déle clic en elementos enviados del Outlook Express y revise si se encuentra el mail que envió.

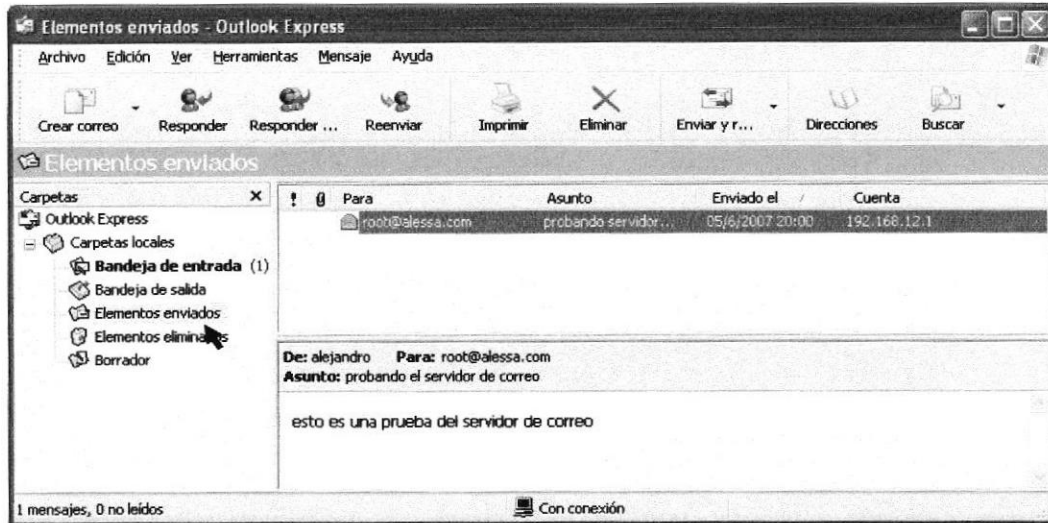


Figura 5-149: VERIFICAR MENSAJE ENVIADO

Revise si el correo llegó al servidor Linux, inicie sesión con el usuario root y luego escriba el comando mail.

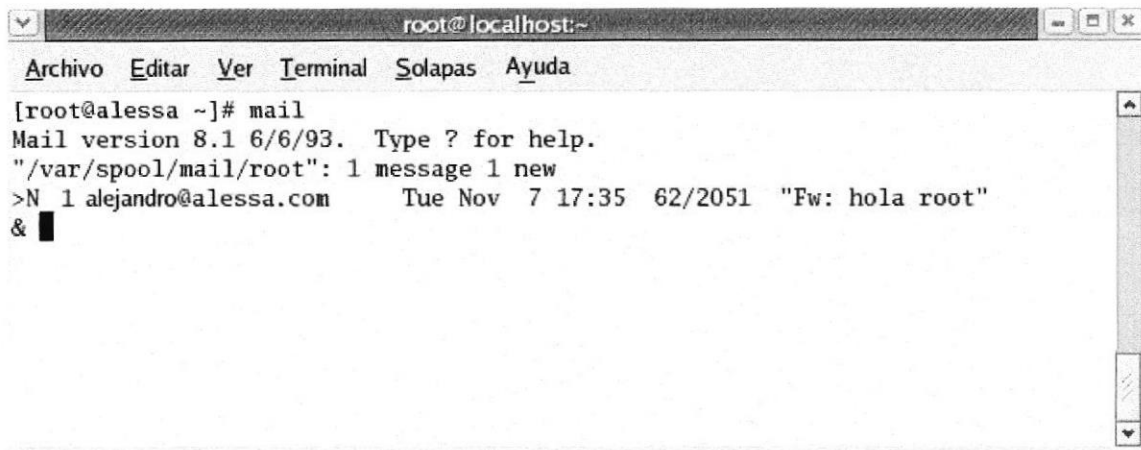


Figura 5-150: VERIFICACIÓN DE CORREO

## 5.15.PROXY

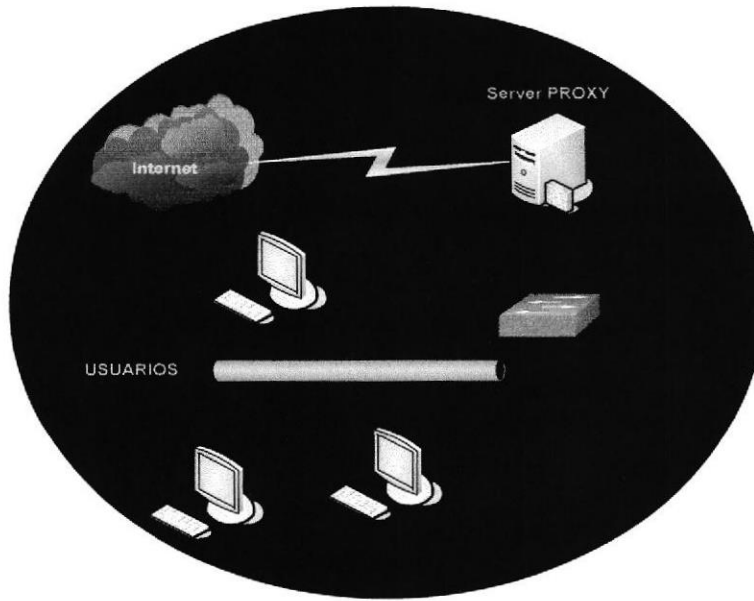


Figura 5-151: PROXY

### 5.15.1.¿QUÉ ES PROXY?

Existe una variedad de paquetes de software de Proxy para Linux. Algunos son a nivel de aplicación (como SQUID) y otros son a nivel de sesión (como SOCKS).

Squid es un Proxy a nivel de aplicación para HTTP, HTTPS y FTP. También puede ejecutar peticiones DNS bastante más rápido de lo que puede hacerlo la mayoría del software cliente. SQUID es ideal para acelerar el acceso a WWW, y para controlar el acceso a sitios Web (utilizando paquetes como squidGuard). Squid es el servidor Proxy más popular y extendido entre los sistemas operativos basados sobre UNIX®. Es muy confiable, robusto y versátil. Al ser *software libre*, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios. Entre otras cosas, Squid puede hacer Proxy y cache con los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, cache transparente, WWCP, aceleración HTTP, cache de consultas DNS y más.

El Servidor Proxy permitirá dar un acceso compartido y eficaz a todos los equipos de red local, permitiéndole controlar los contenidos visitados en Internet y asegurar que el uso que se hace es con fines laborales.

### 5.15.2.REQUISITOS PARA SU CONFIGURACIÓN

- ✓ Una equipo de trabajo con sistema operativo Linux.
- ✓ Tarjeta de red.
- ✓ Tener la tarjeta de red configurada
- ✓ Paquete SQUID, HTTPD instalado.
- ✓ Servicio SQUID, HTTPD habilitado

### 5.15.3.CONFIGURACIÓN DEL SQUID

Ahora verifique si tiene instalado el paquete squid, lo hace con el comando **rpm -q squid**, luego de enter y revise.

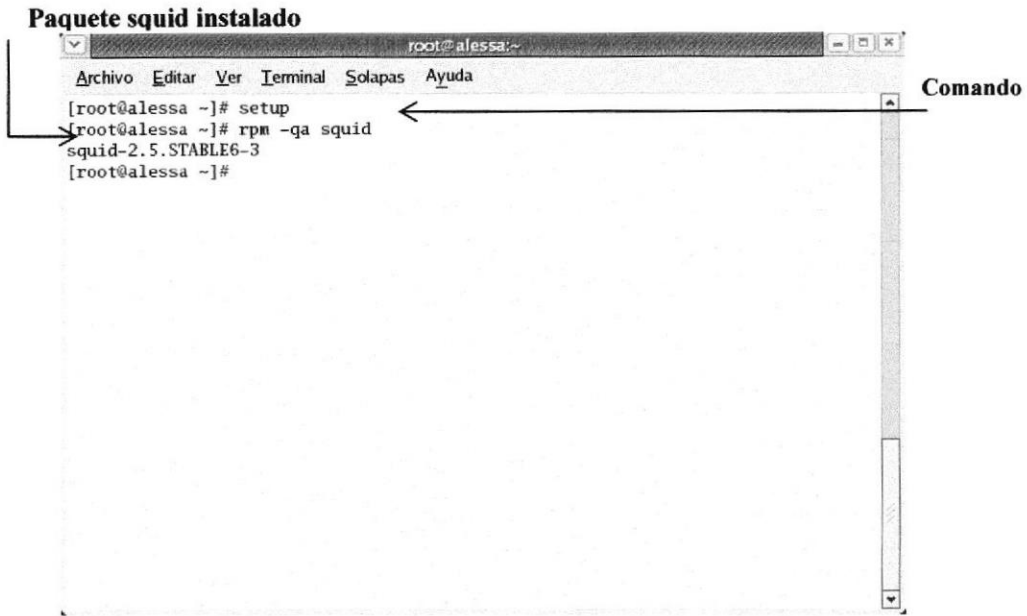


Figura 5-152: VERIFICACIÓN DEL PAQUETE SQUID.

Ingrese comando setup en el terminal y de un enter.

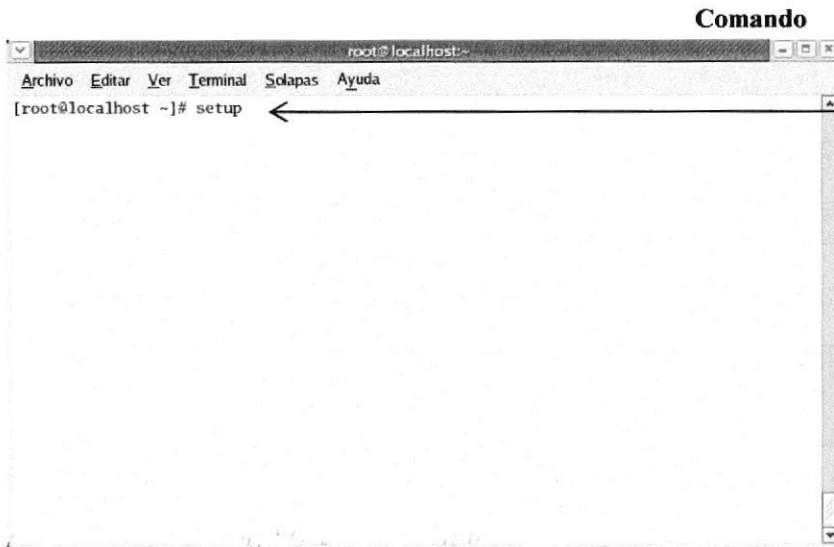


Figura 5-153: COMANDO SETUP.

A continuación se abre esta pantalla y con el teclado desplácese hacia la **opción servicios del sistema** con las teclas de direcciones, ahora con la tecla tabulador colóquese en **ejecutar herramienta** y déle un enter.

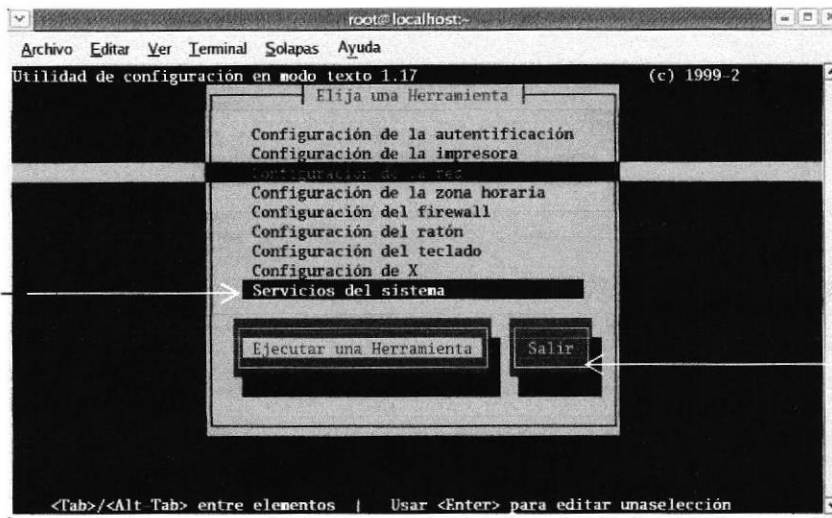


Figura 5-154: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora se abre esta pantalla y con el teclado desplácese hacia la opción **squid** con las teclas direccionales y si esta opción no se encuentra marcada con un asterisco como lo muestra la imagen presione la tecla barra espaciadora [\*] para que se marque con el asterisco así estará habilitando el servicio squid, luego colóquese con la tecla tabulador **OK** y déle un enter.

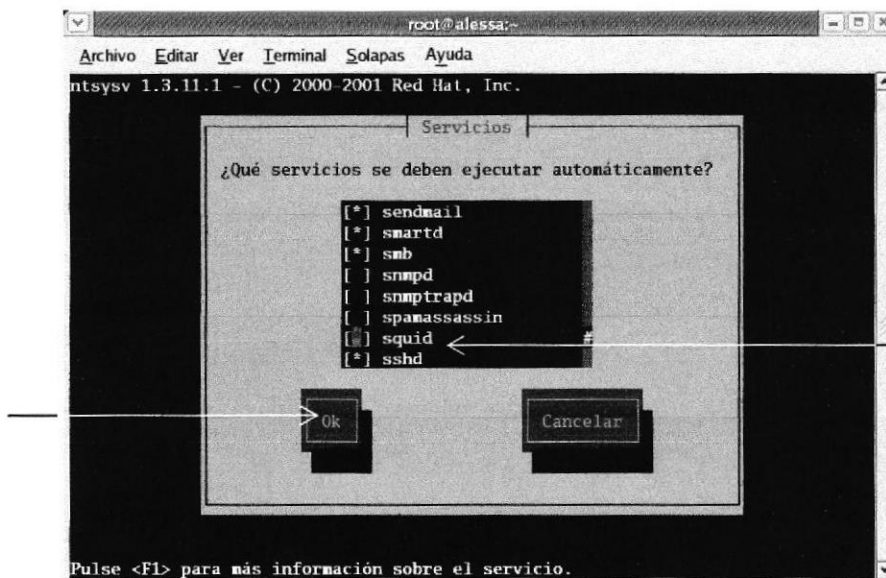


Figura 5-155: HABILITAR SERVICIO SQUID

A continuación aparece esta pantalla y con la tecla tabulador colóquese en **salir** y déle un enter y hemos habilitado el servicio squid.



Figura 5-156: SALIR UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora edite el fichero **squid.conf** que se encuentra en el directorio **etc/squid** para esto ingrese el comando **vi**, de la siguiente manera, **vi etc/squid/squid.conf** y déle un enter.

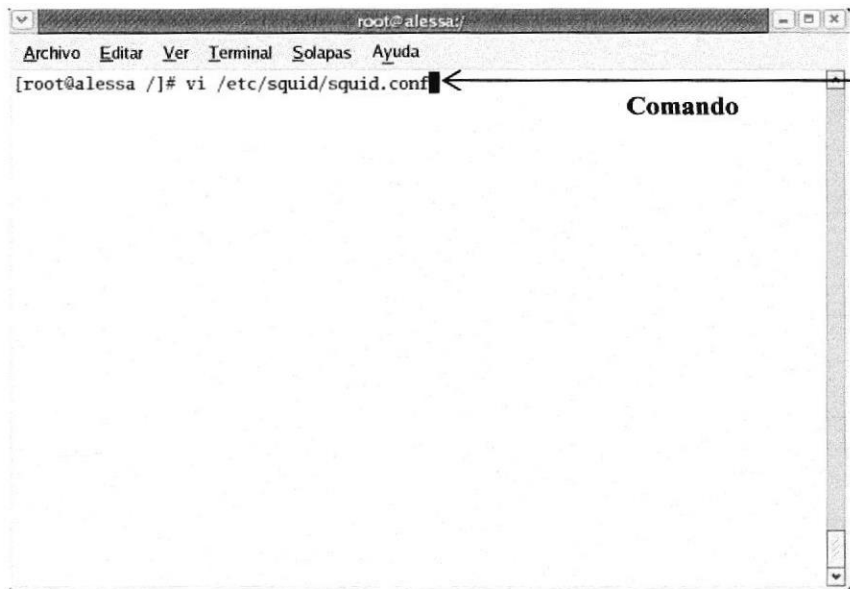
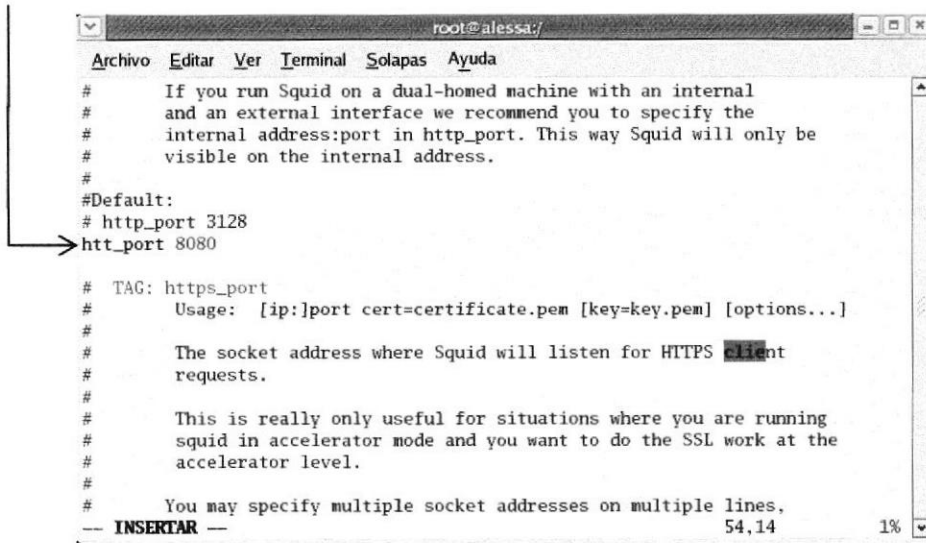


Figura 5-157: EDITAR EL FICHERO SQUID.CONF

El proxy por defecto utilizará el puerto 3128 para atender peticiones, sin embargo para este caso va a especificar que lo haga el puerto **8080**, busque la sección de **http\_port** en donde editara el puerto 3128 por el **8080**.



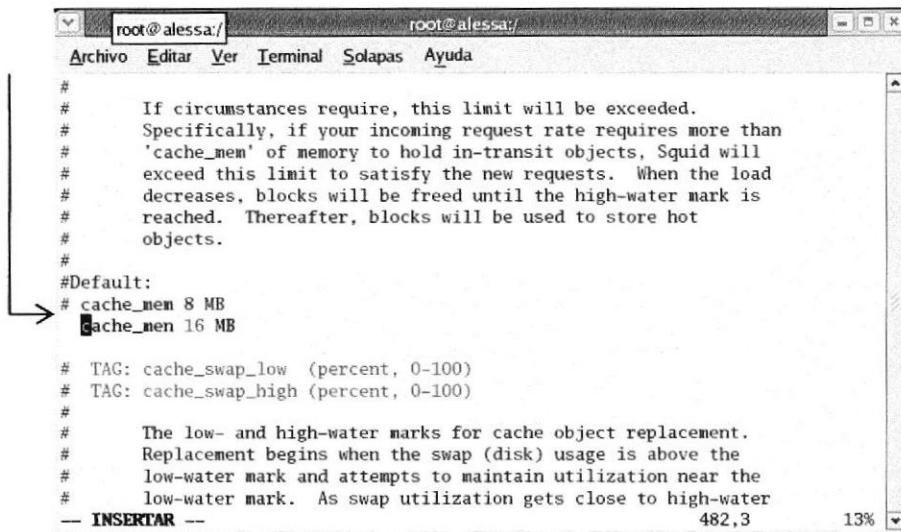
```

root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
#
#   If you run Squid on a dual-homed machine with an internal
#   and an external interface we recommend you to specify the
#   internal address:port in http_port. This way Squid will only be
#   visible on the internal address.
#
#Default:
# http_port 3128
htt_port 8080
#
# TAG: https_port
#   Usage: [ip:]port cert=certificate.pem [key=key.pem] [options...]
#
#   The socket address where Squid will listen for HTTPS client
#   requests.
#
#   This is really only useful for situations where you are running
#   squid in accelerator mode and you want to do the SSL work at the
#   accelerator level.
#
#   You may specify multiple socket addresses on multiple lines.
-- INSERTAR --                               54,14      1%

```

**Figura 5-158: EDITAR FICHERO SQUID.CONF [HTTPORT 8080]**

A continuación busque la sección de **cache\_mem**, en donde se establece la cantidad ideal de memoria cache, por defecto aparece 8 MB para este caso use **16 MB**.



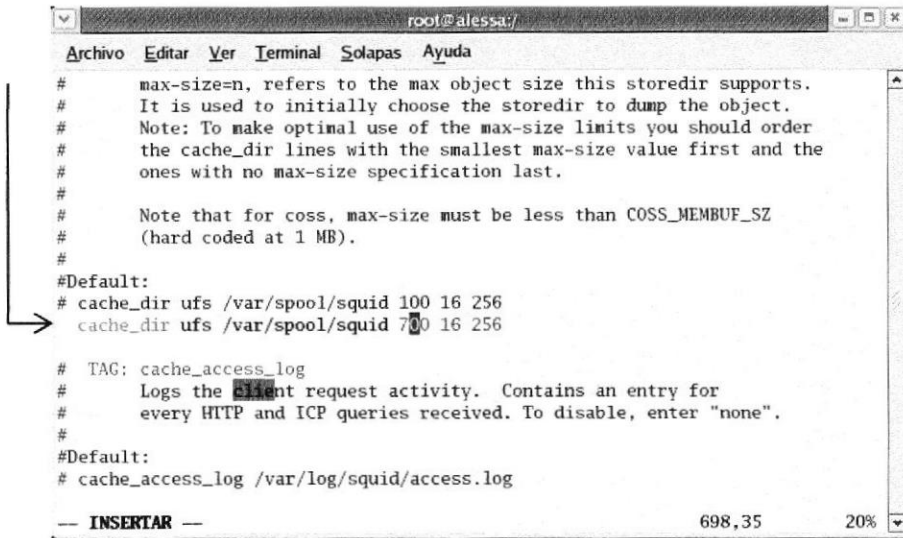
```

root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
#
#   If circumstances require, this limit will be exceeded.
#   Specifically, if your incoming request rate requires more than
#   'cache_mem' of memory to hold in-transit objects, Squid will
#   exceed this limit to satisfy the new requests. When the load
#   decreases, blocks will be freed until the high-water mark is
#   reached. Thereafter, blocks will be used to store hot
#   objects.
#
#Default:
# cache_mem 8 MB
cache_mem 16 MB
#
# TAG: cache_swap_low (percent, 0-100)
# TAG: cache_swap_high (percent, 0-100)
#
#   The low- and high-water marks for cache object replacement.
#   Replacement begins when the swap (disk) usage is above the
#   low-water mark and attempts to maintain utilization near the
#   low-water mark. As swap utilization gets close to high-water
-- INSERTAR --                               482,3      13%

```

**Figura 5-159: EDITAR FICHERO SQUID.CONF [CACHE MEN]**

Ahora busque la sección de **cache\_dir**, este parámetro se utiliza para establecer que tamaño desea que tenga el cache en el disco duro para el squid.

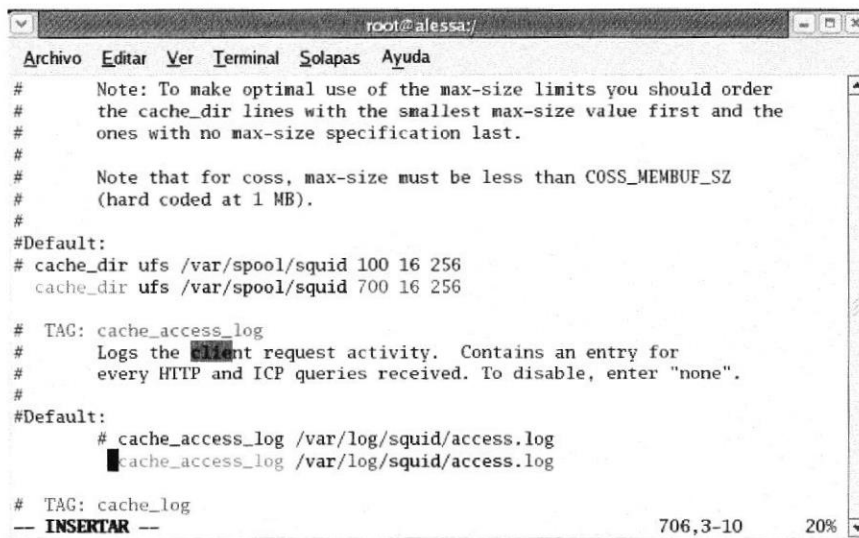


```
root@alessa/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# max-size=n, refers to the max object size this storedir supports.
# It is used to initially choose the storedir to dump the object.
# Note: To make optimal use of the max-size limits you should order
# the cache_dir lines with the smallest max-size value first and the
# ones with no max-size specification last.
#
# Note that for coss, max-size must be less than COSS_MEMBUF_SZ
# (hard coded at 1 MB).
#
#Default:
# cache_dir ufs /var/spool/squid 100 16 256
# cache_dir ufs /var/spool/squid 700 16 256
#
# TAG: cache_access_log
# Logs the client request activity. Contains an entry for
# every HTTP and ICP queries received. To disable, enter "none".
#
#Default:
# cache_access_log /var/log/squid/access.log
-- INSERTAR -- 698,35 20%
```



Figura 5-160: EDITAR FICHERO SQUID.CONF [CACHE DIR]

En el mismo fichero siga buscando la sección de **cache\_access\_log**, esta línea le sirve para monitorear la actividad de los host que tenga a cargo el Proxy, y proceda a descomentarla o agregarla.



```
root@alessa/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# Note: To make optimal use of the max-size limits you should order
# the cache_dir lines with the smallest max-size value first and the
# ones with no max-size specification last.
#
# Note that for coss, max-size must be less than COSS_MEMBUF_SZ
# (hard coded at 1 MB).
#
#Default:
# cache_dir ufs /var/spool/squid 100 16 256
# cache_dir ufs /var/spool/squid 700 16 256
#
# TAG: cache_access_log
# Logs the client request activity. Contains an entry for
# every HTTP and ICP queries received. To disable, enter "none".
#
#Default:
# cache_access_log /var/log/squid/access.log
# cache_access_log /var/log/squid/access.log
# TAG: cache_log
-- INSERTAR -- 706,3-10 20%
```

Figura 5-161: EDITAR FICHERO SQUID.CONF [CACHE ACESS LOG]

A continuación busque la sección de **ACCESS CONTROLS**, en esta sección va a definir todas nuestras listas de accesos para los usuarios, para este caso va a agregar lista de control de acceso (acl) para la red

**acl alessa myport 8080 (definimos que puerto vamos a utilizar).**

**acl red\_alessa src 192.168.12.1/255.255.255.0 (definimos el segmento de red).**

```

root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
#acl fileupload req_mime_type -i ^multipart/form-data$
#acl javascript rep_mime_type -i ^application/x-javascript$
#
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443 563    # https, snews
acl Safe_ports port 70        # gopher
acl Safe_ports port 210       # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280       # http-mgmt
acl Safe_ports port 488       # gss-http
acl Safe_ports port 591       # filemaker
acl Safe_ports port 777       # multiling http
acl CONNECT method CONNECT
acl alessa myport 8080
acl red_alessa src 192.168.12.1/255.255.255.0
-- INSERTAR --
1822,46 53%

```

Figura 5-162: ESTABLECER LISTA DE ACCESO PARA NUESTRA RED

Una vez creada la acl busque la sección de **http\_access**, en esta sección va a definir que lista de control de acceso tendrá el acceso a Internet, para este caso **http\_access allow red\_alessa**.

```

root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks
#
# And finally deny all other access to this proxy
#http_access allow localhost
#
# http_access allow red_alessa
#http_access deny all
#
# TAG: http_reply_access
# Allow replies to client requests. This is complementary to http_access.
# http_reply_access allow|deny [!] aclname ...
#
# NOTE: if there are no access lines present, the default is to allow
# all replies
#
# If none of the access lines cause a match the opposite of the
-- INSERTAR --
1873,28 55%

```

Figura 5-163: REGLA DE LISTA DE ACCESO PARA NUESTRA RED

En el mismo fichero busque la sección de **visible\_hostname**, luego proceda a editarla, en esta línea especifique el nombre del host, para este caso es localhost.

```

root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
# to the group (or GID) you want Squid to run as. When set
# all other group privileges of the effective user is ignored
# and only this GID is effective. If Squid is not started as
# root the user starting Squid must be member of the specified
# group.
#cache_effective_group squid
#
#Default:
# cache_effective_group squid

# TAG: visible_hostname
# If you want to present a special hostname in error messages, etc,
# define this. Otherwise, the return value of gethostname()
# will be used. If you have multiple caches in a cluster and
# get errors about IP-forwarding you must set them to have individual
# names with this setting.
#
#Default:
# none
visible_hostname localhost
# TAG: unique_hostname
# If you want to have multiple machines with the same
2094,27 61%

```

Figura 5-164: EDITAR FICHERO SQUID.CONF [VISIBLE\_HOSTNAME]

Autenticación, a continuación en el mismo fichero busque la sección de **auth\_param basic program**, en esta sección busque la línea **auth\_param basic program /usr/libexec/ncsa\_auth /usr/etc/passwd** y proceda a editarla o agregarla, esta línea le va a servir para especificar un programa de autenticación que utilizara.

**/usr/libexec/ncsa\_auth.-** Corresponde la localización del programa para autenticar.

**usr/etc/passwd.-** Este fichero contiene las cuentas y claves de acceso, para este caso la línea debe quedar de la siguiente manera **auth\_param basic program /usr/lib/squid/ncsa\_auth /etc/squid/claves**.

```

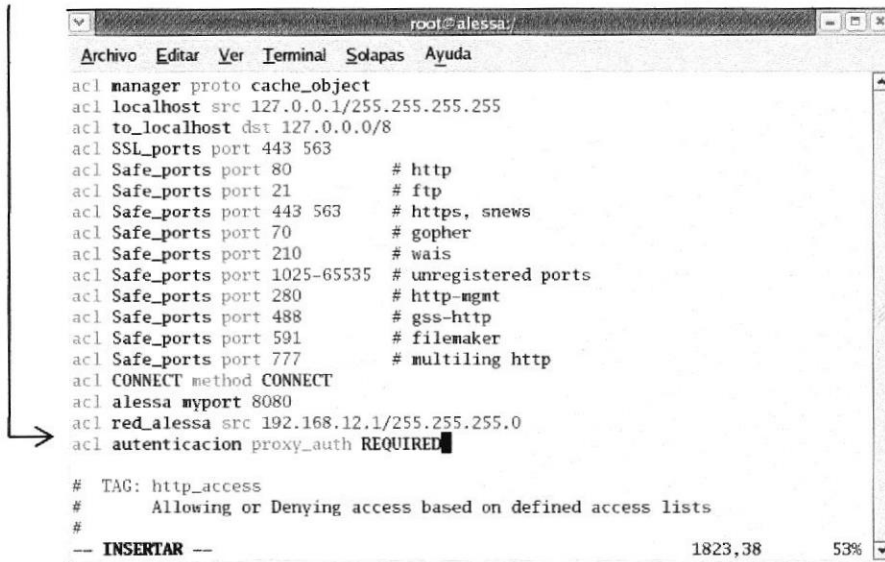
root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
# Specify the command for the external authenticator. Such a program
# reads a line containing "username password" and replies "OK" or
# "ERR" in an endless loop.
#
# By default, the basic authentication scheme is not used unless a
# program is specified.
#
# If you want to use the traditional proxy authentication, jump over to
# the helpers/basic_auth/NCSA directory and type:
# % make
# % make install
#
# Then, set this line to something like
#
auth_param basic program /usr/libexec/ncsa_auth /usr/etc/passwd
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves
#
# "children" numberofchildren
# The number of authenticator processes to spawn.
# If you start too few Squid will have to wait for them to process a
# backlog of usercode/password verifications, slowing it down. When
# password verifications are done via a (slow) network you are likely to
-- INSERTAR --
1102,53-59 32%

```

Figura 5-165: EDITAR FICHERO SQUID.CONF [AUTH\_PARAM]

A continuación busque la sección de **ACCESS CONTROLS**, en esta sección va a definir todas las listas de accesos para los usuarios, para este caso va a agregar la lista de control de acceso (acl) para autenticación de usuarios

**acl autenticación proxy\_auth REQUIRED (en esta línea definimos la autenticación para el Proxy).**



```

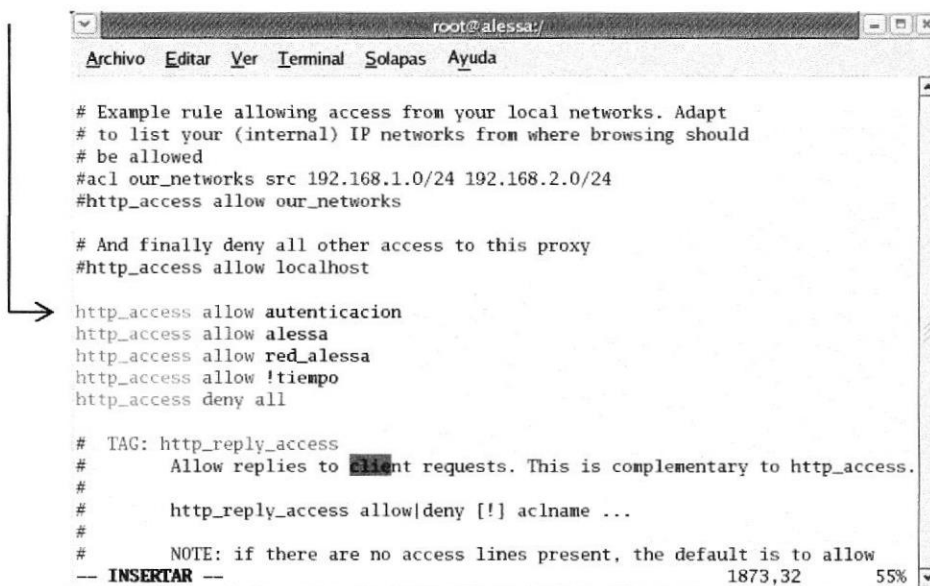
root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl alessa myport 8080
acl red_alessa src 192.168.12.1/255.255.255.0
acl autenticacion proxy_auth REQUIRED

# TAG: http_access
# Allowing or Denying access based on defined access lists
#
-- INSERTAR --                               1823,38      53%

```

Figura 5-166: ESTABLECER LISTA DE ACCESO DE AUTENTICACIÓN

Una vez creada la acl busque la sección de **http\_access**, en esta sección va a definir que lista de control de acceso tendrá para la autenticación de usuario, para este caso **http\_access allow autenticación**.



```

root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda

# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

# And finally deny all other access to this proxy
#http_access allow localhost

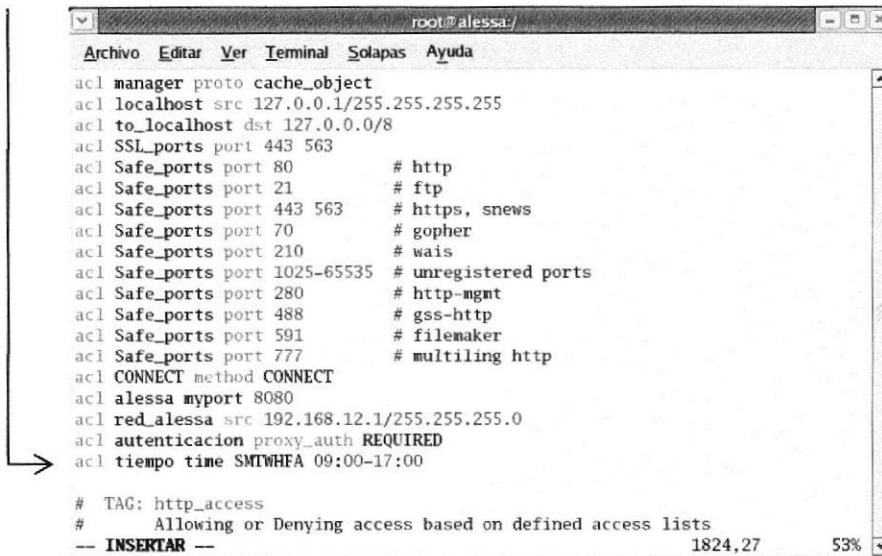
http_access allow autenticacion
http_access allow alessa
http_access allow red_alessa
http_access allow !tiempo
http_access deny all

# TAG: http_reply_access
# Allow replies to client requests. This is complementary to http_access.
#
# http_reply_access allow[deny [!] aclname ...
#
# NOTE: if there are no access lines present, the default is to allow
-- INSERTAR --                               1873,32      55%

```

Figura 5-167: REGLA DE LISTA DE ACCESO AUTENTICACIÓN.

Lista de acceso para el horario, a continuación busque la sección de **ACCESS CONTROLS**, en esta sección va a definir todas las listas de accesos para los usuarios, para este caso va a agregar lista de control de acceso (acl) para el horario **acl tiempo time SMTWHFA 09:00-17:00 (defina el horario de acceso si es el caso)**. Las letras **SMTWHFA** le indica el o los días que va a tener acceso a Internet si es el caso, estas letras son las iniciales de los días en ingles. El formato de hora es **00:00-24:00**.



```

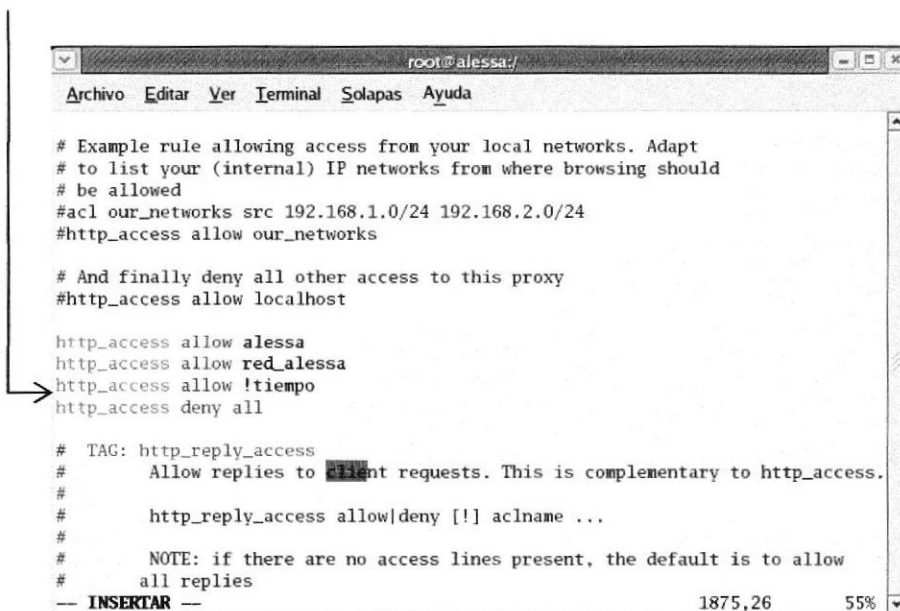
root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443 563    # https, snews
acl Safe_ports port 70        # gopher
acl Safe_ports port 210       # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280       # http-mgmt
acl Safe_ports port 488       # gss-http
acl Safe_ports port 591       # filemaker
acl Safe_ports port 777       # multiling http
acl CONNECT method CONNECT
acl alessa myport 8080
acl red_alessa src 192.168.12.1/255.255.255.0
acl autentificacion proxy_auth REQUIRED
acl tiempo time SMTWHFA 09:00-17:00

# TAG: http_access
#   Allowing or Denying access based on defined access lists
-- INSERTAR --                               1824,27      53%

```

Figura 5-168: ESTABLECER LISTA DE ACCESO PARA TIEMPO

Una vez creada la acl busque la sección de **http\_access**, en esta sección va a definir que lista de control de acceso tendrá para el horario el usuario, para este caso **http\_access allow ;tiempo o http\_access deny tiempo**, denegamos el servicio de Internet al usuario.



```

root@alessa:/
Archivo Editar Ver Terminal Solapas Ayuda

# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

# And finally deny all other access to this proxy
#http_access allow localhost

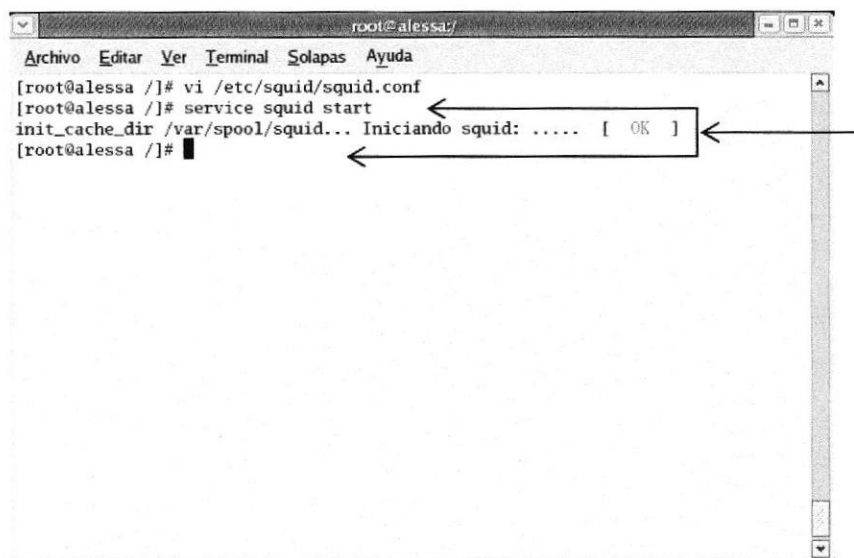
http_access allow alessa
http_access allow red_alessa
http_access allow !tiempo
http_access deny all

# TAG: http_reply_access
#   Allow replies to client requests. This is complementary to http_access.
#
#   http_reply_access allow|deny [!] aclname ...
#
#   NOTE: if there are no access lines present, the default is to allow
#   all replies
-- INSERTAR --                               1875,26      55%

```

Figura 5-169: REGLA DE LISTA DE ACCESO PARA TIEMPO

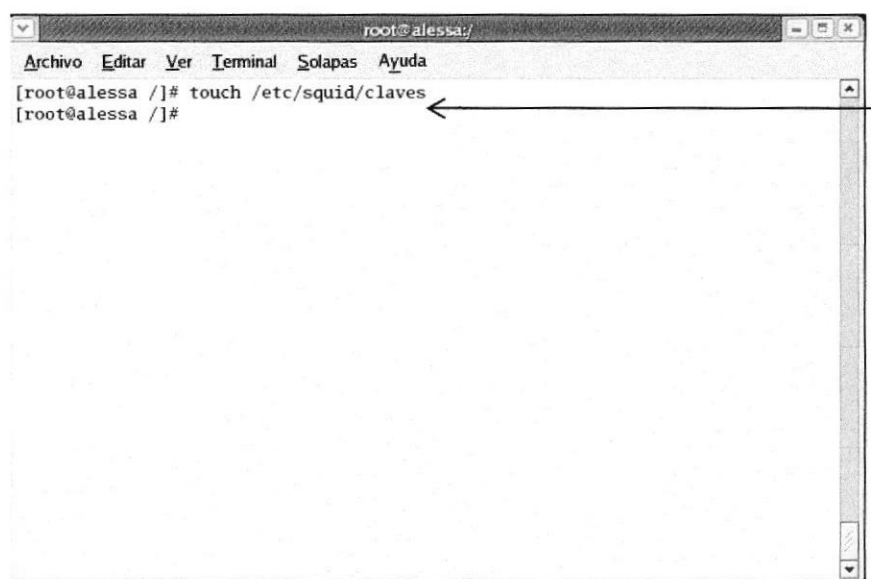
Debe iniciar el servicio squid, con el comando `service squid start` de la siguiente manera **service squid start** y le da un enter si la configuración no tiene ningún error o problema le saldrán mensajes de **[OK]** indicándole que la configuración ha sido satisfactoria.



```
root@alessa/
Archivo Editar Ver Terminal Solapas Ayuda
[root@alessa /]# vi /etc/squid/squid.conf
[root@alessa /]# service squid start
init_cache_dir /var/spool/squid... Iniciando squid: ..... [ OK ]
[root@alessa /]#
```

Figura 5-170: INICIANDO SERVICIO SQUID

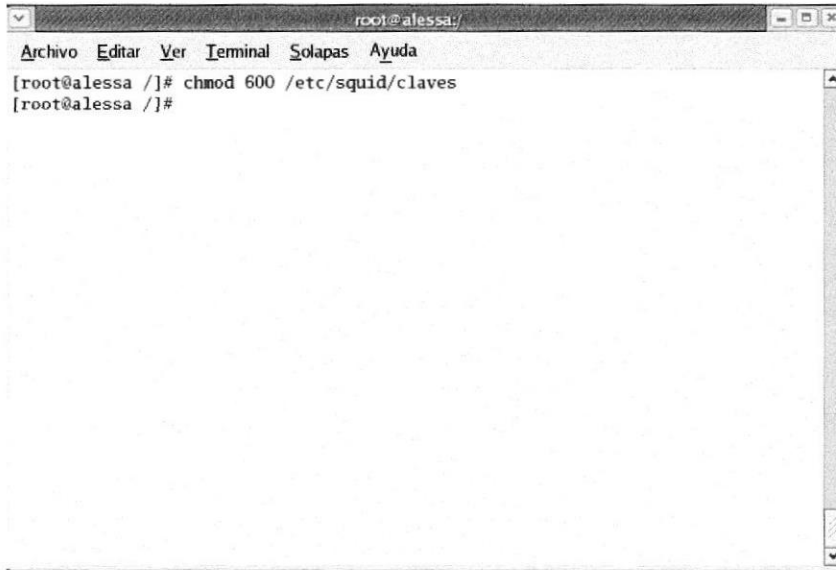
Ahora proceda a crear el fichero claves con el respectivo permiso, en el cual se van almacenar todas las contraseñas de los usuarios que pertenezcan al squid., lo debe crear de la siguiente manera **touch /etc/squid/claves**.



```
root@alessa/
Archivo Editar Ver Terminal Solapas Ayuda
[root@alessa /]# touch /etc/squid/claves
[root@alessa /]#
```

Figura 5-171: CREAR FICHERO CLAVES

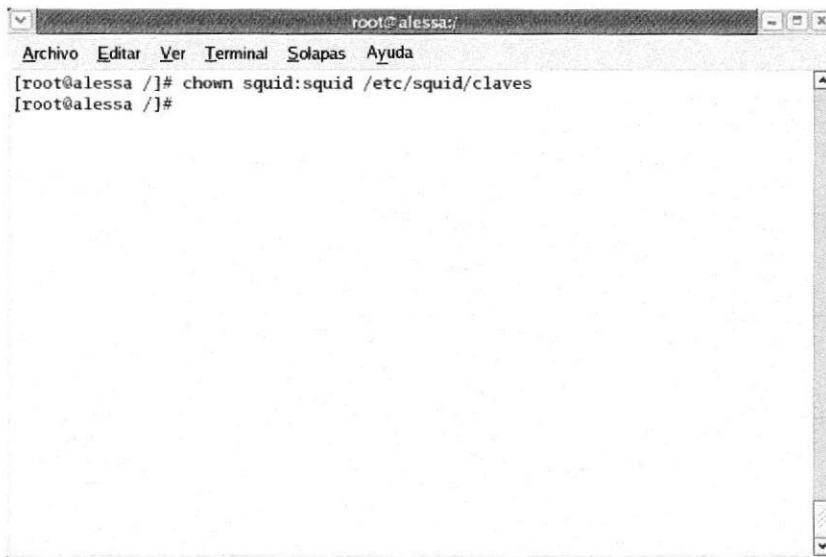
A continuación de los permisos al directorio claves, lo debe hacer de la siguiente manera, **chmod 600 /etc/squid/claves**.

A terminal window titled 'root@alessa:' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Terminal', 'Solapas', and 'Ayuda'. The terminal shows the command '[root@alessa /]# chmod 600 /etc/squid/claves' being entered and executed, followed by a new prompt '[root@alessa /]#'.

```
root@alessa:/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@alessa /]# chmod 600 /etc/squid/claves
[root@alessa /]#
```

Figura 5-172: PERMISO AL FICHERO CLAVES

Cambie de propietario fichero claves, lo debe hacer de la siguiente manera, **chown squid:squid /etc/squid/claves**.

A terminal window titled 'root@alessa:' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Terminal', 'Solapas', and 'Ayuda'. The terminal shows the command '[root@alessa /]# chown squid:squid /etc/squid/claves' being entered and executed, followed by a new prompt '[root@alessa /]#'.

```
root@alessa:/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@alessa /]# chown squid:squid /etc/squid/claves
[root@alessa /]#
```

Figura 5-173: CAMBIO DE PROPIETARIO FICHERO CLAVES



Se habrá el Internet Explorer seleccione el menú **herramientas** y haga clic en **opciones de Internet**.

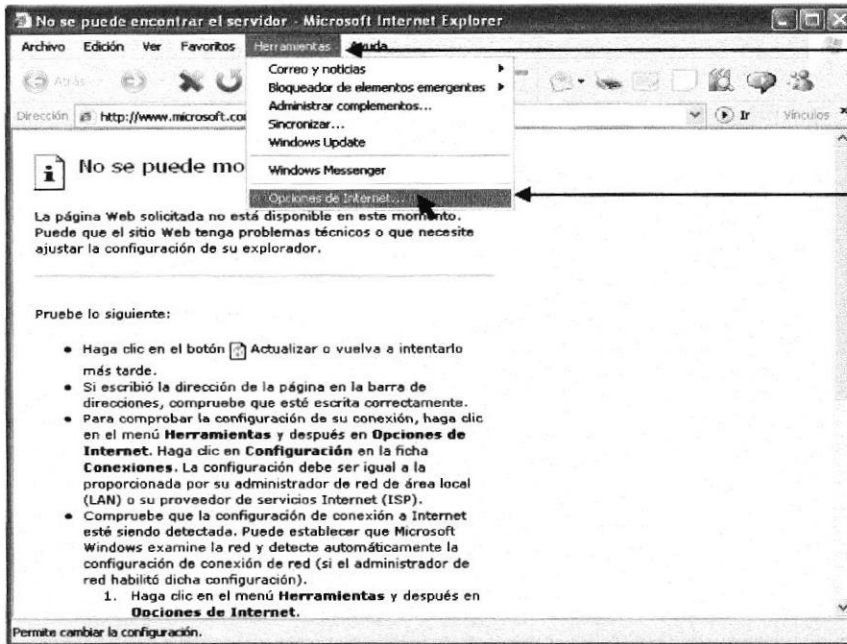


Figura 5-176: HERRAMIENTAS - OPCIONES DE INTERNET

Ahora habrá la ventana opciones de Internet seleccione la pestaña **conexiones** y de un clic en **configuración de LAN**.

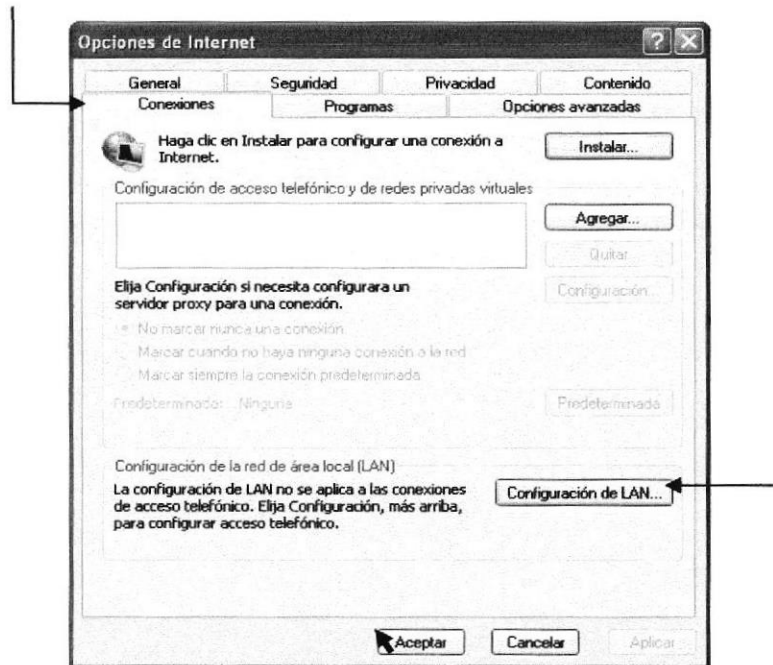


Figura 5-177: OPCIONES DE INTERNET

Ahora en esta ventana debe seleccionar la casilla **usar un servidor proxy** colóquese en la casilla dirección IP del servidor y en la casilla puerto asigne el puerto 8080, luego de clic en aceptar y listo ah configurado el cliente.

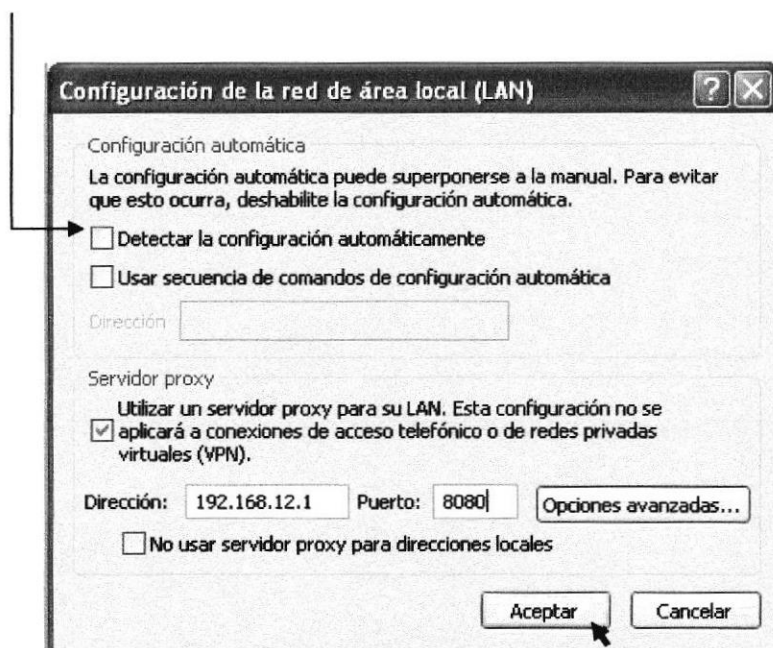


Figura 5-178: CONEXIÓN DE RED DE ÁREA LOCAL (LAN)

Ahora debe acceder al sitio Web, para esto use el navegador en la casilla de **dirección** colóquese la dirección de la pagina para este caso **www.alesa.com** de un enter y la pagina requerida debe cargarse en su explorador esto indica que las configuraciones realizadas han sido satisfactoria.

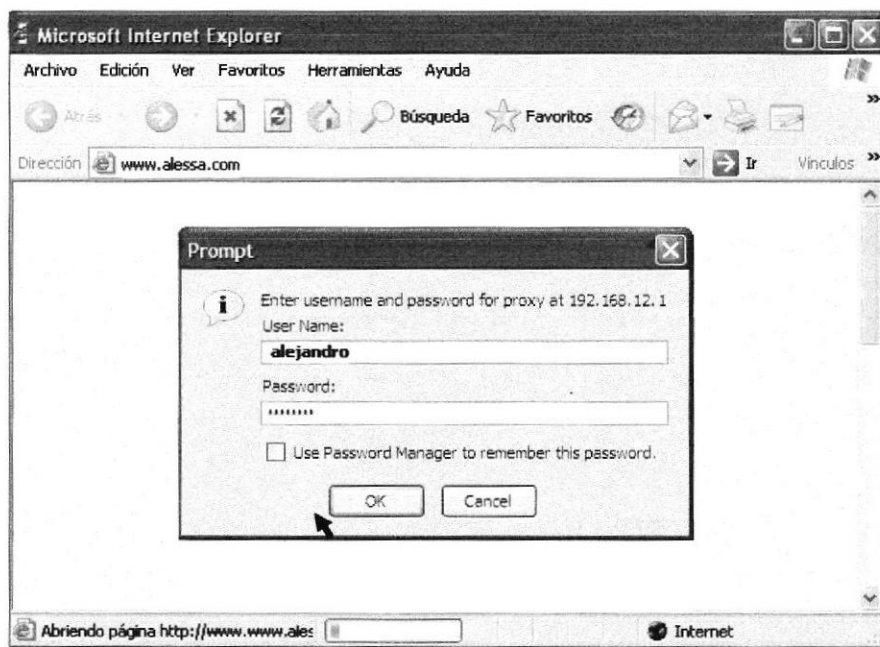


Figura 5-179: INGRESAR USUARIO Y CONTRASEÑA

Página Web solicitada cargada.

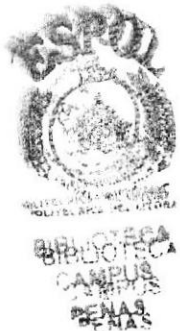
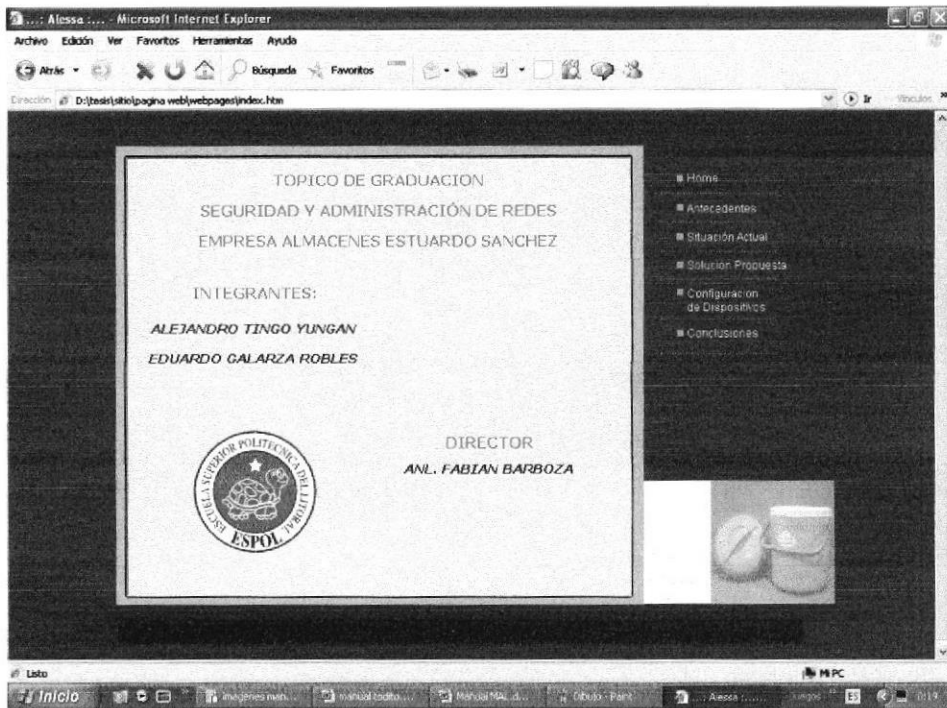


Figura 5-180: PÁGINA WEB CARGADA

## 5.16.DHCP

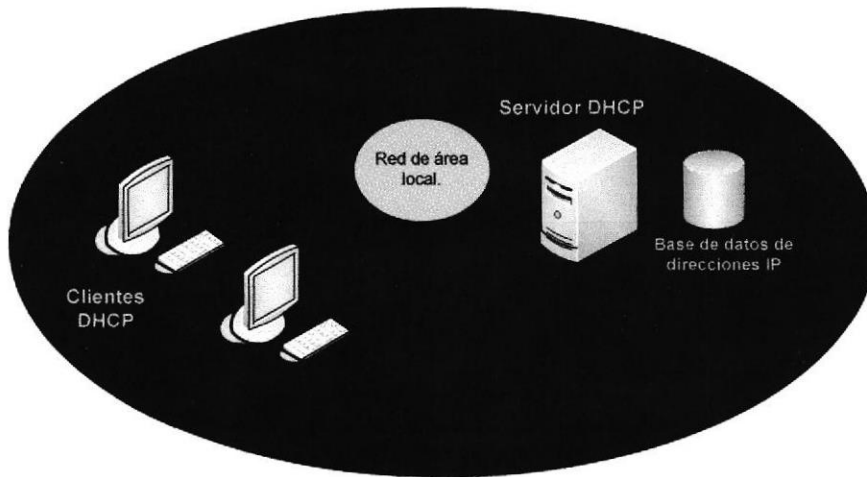


Figura 5-181: DHCP

### 5.16.1.¿QUÉ ES DHCP?

DHCP es un protocolo TCP/ IP que proporciona una asignación automática de las direcciones IP, (Es posible que el nombre Automatic IP Address Assignment sea más significativo que DHCP, pero (AIAA) parece más una llamada de auxilio de un administrador de redes que un acrónimo.)

Para utilizar TCP/ IP en la red, un administrador debe proporcionar por lo menos tres datos para cada ordenador, la dirección IP, la máscara del subred y la dirección IP de la puerta de enlace predeterminada, cada ordenador necesita una dirección IP única para usar TCP/ IP.

Las direcciones asignadas deben estar en la subred correcta, si usted se conecta a una red grande, se preguntará cómo determinar a qué subred se conecta, sin embargo, el DHCP sabe desde qué subred proviene la solicitud de la dirección IP, por lo que no tiene problemas al asignar una dirección apropiada. Si la red utiliza el servicio WINS (Windows Internet Naming Service) y el sistema DNS (Domain Name System), el administrador deberá configurar también los ordenadores cliente con las direcciones IP de los servidores WINS y DNS.

El administrador de la red puede configurar manualmente cada sistema, o puede proporcionar los valores correctos y pedirles a los usuarios que configuren sus sistemas, sin embargo, este último método es francamente arriesgado, el procedimiento más fácil y más seguro es configurar uno o más servidores DHCP para que asignen automáticamente direcciones IP y demás información necesaria a cada ordenador de la red.

Este proceso implica la configuración del servidor, indicándole el rango de las direcciones a utilizar, estableciendo algunos parámetros adicionales y revisando periódicamente el servidor.

### 5.16.2.REQUISITOS PARA SU CONFIGURACIÓN

- ✓ Una equipo de trabajo con sistema operativo Linux.
- ✓ Tarjeta de red.
- ✓ Tener la tarjeta de red configurada
- ✓ Paquete DHCP instalado.
- ✓ Servicio DHCP habilitado



### 5.16.3.CONFIGURACIÓN DE SERVICIO DHACP

**Verifique el paquete dhcp esta instalado.**

Ahora verifique si tiene instalado el paquete dhcp, lo debe hacer con el comando **rpm -q dhcp**, luego de un enter y revise.

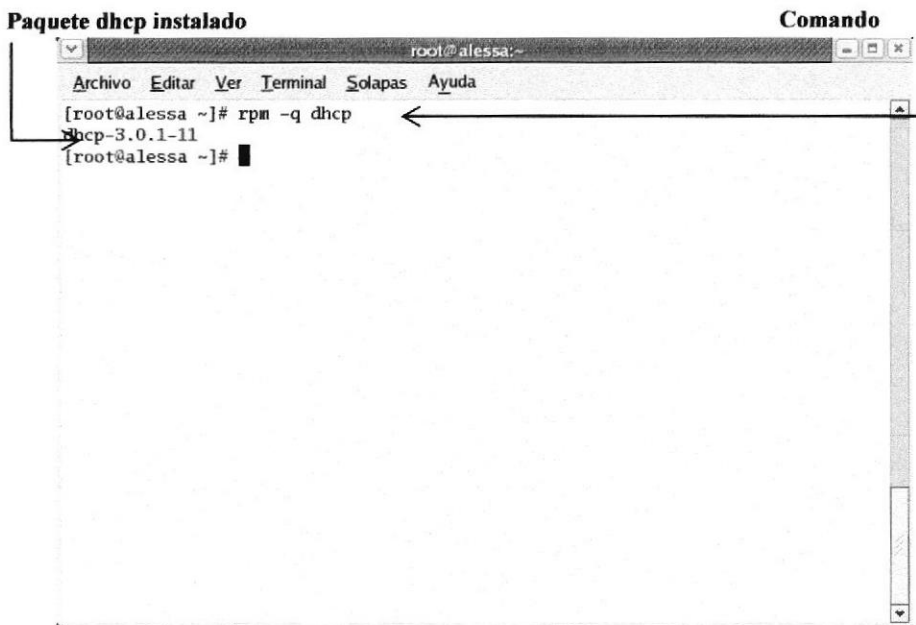


Figura 5-182: VERIFICAR PAQUETE DHCP.

Ingrese el comando setup en el terminal y de enter.

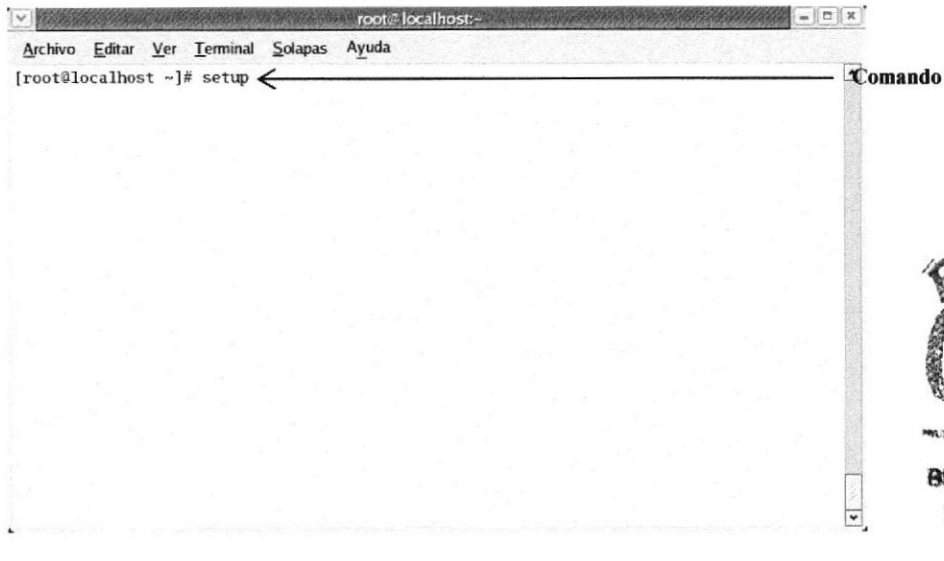


Figura 5-183: COMANDO SETUP

A continuación se abre esta pantalla y con el teclado desplácese hacia la **opción servicios del sistema** con las teclas de direcciones, ahora con la tecla tabulador colóquese en **ejecutar herramienta** y de un enter.

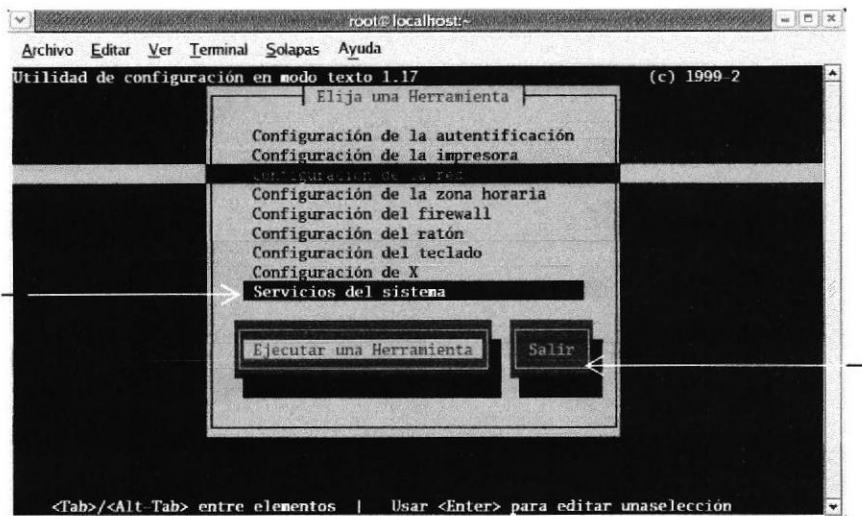


Figura 5-184: UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Se abre esta pantalla y con el teclado desplácese hacia la opción **dhcpcd** con las teclas direccionales y si esta opción no se encuentra marcada con un asterisco como lo muestra la imagen presione la tecla barra espaciadora [\*] para que se marque con el

asterisco así estará habilitando el servicio del DHCP, luego colóquese con la tecla tabulador en **OK** y de un enter.

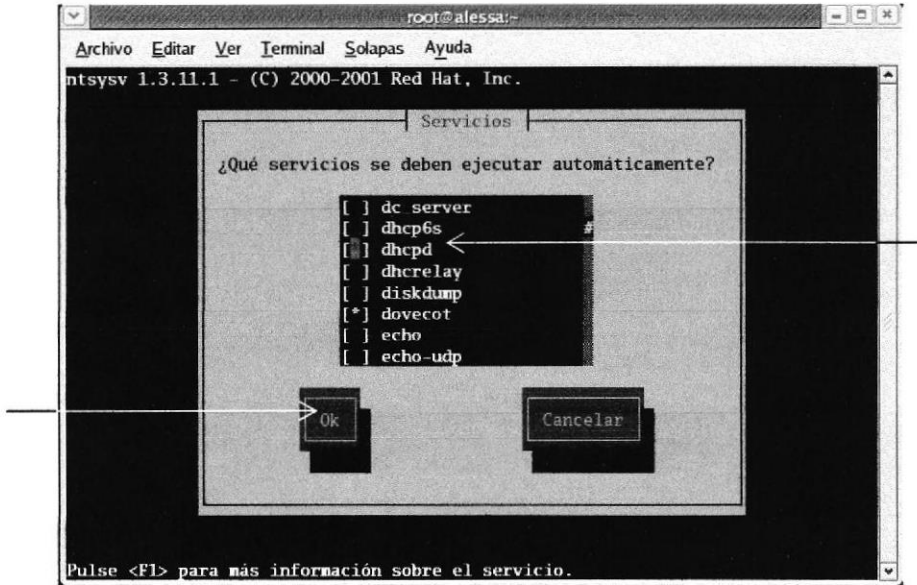


Figura 5-185: HABILITAR SERVICIO DHCPD

A continuación aparece esta pantalla y con la tecla tabulador colóquese en **salir** y de un enter.

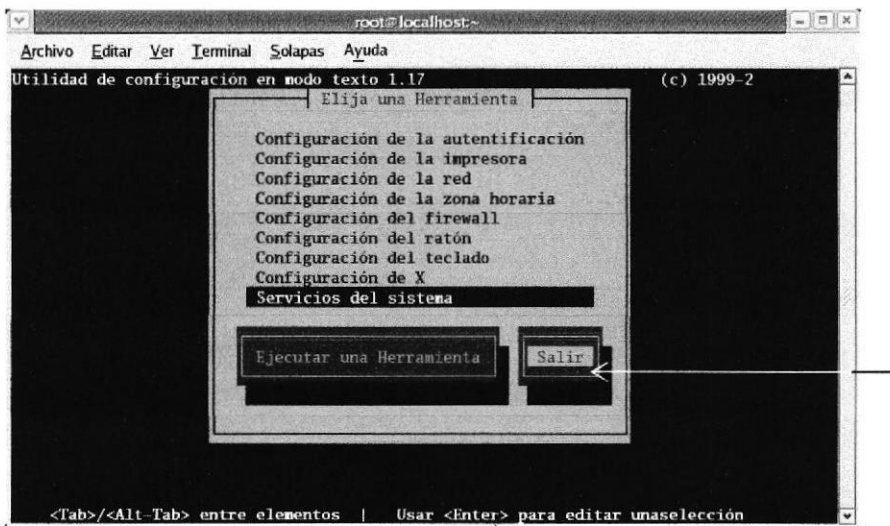


Figura 5-186: SALIR DE UTILIDAD DE CONFIGURACIÓN EN MODO TEXTO

Ahora debe copiar el fichero **dhcpd.conf** que se encuentra en el directorio **/usr/share/doc/dhcp-3.0.1/dhcpd.conf.sample** y cópielo en el directorio del **/etc**, con el comando **cp /usr/share/doc/dhcp-3.0.1/dhcpd.conf.sample /etc/dhcpd.conf**.

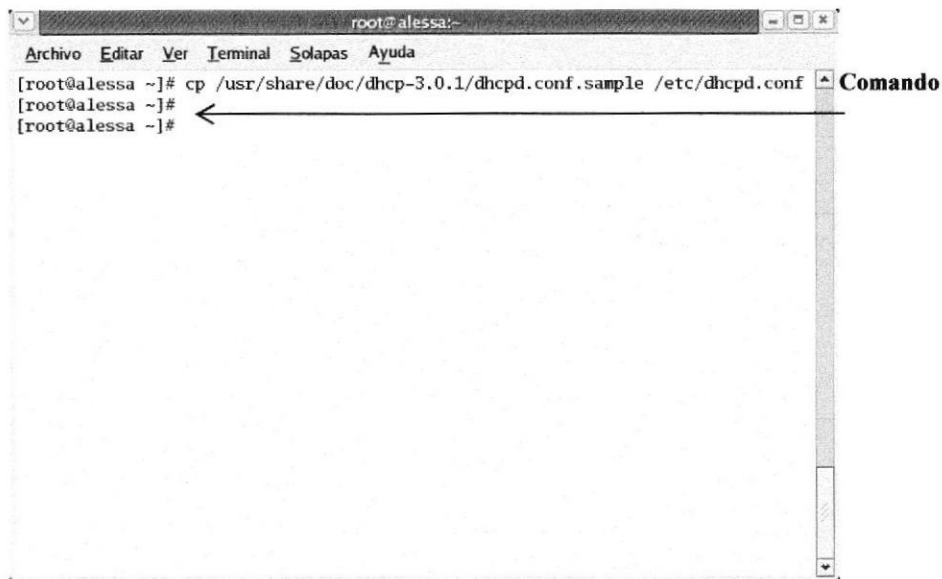


Figura 5-187: COPIAR FICHERO DHCPD.CONF

Ingrese el fichero de la siguiente manera, escriba el comando **vi /etc/dhcpd.conf** y de un enter.

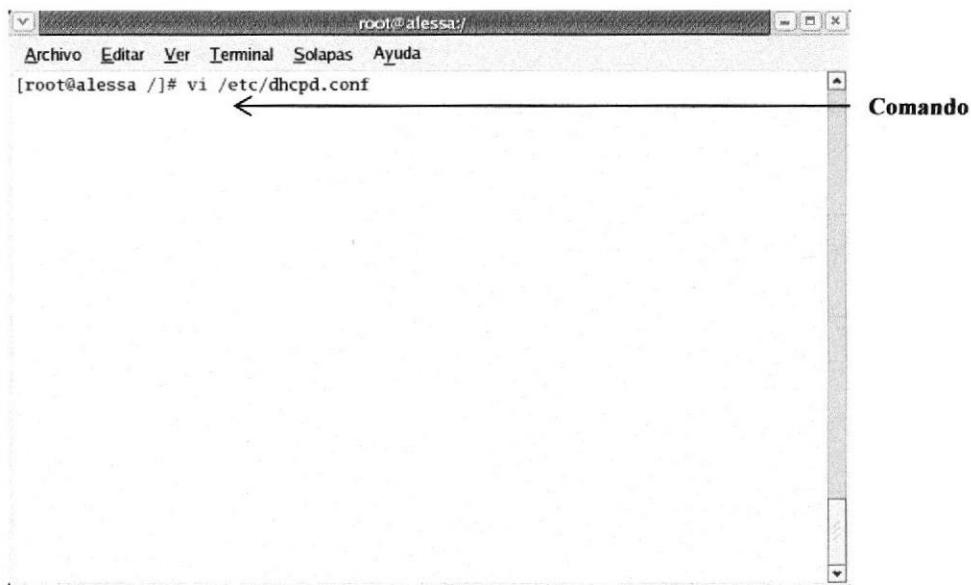


Figura 5-188: EDITAR FICHERO DHCPD.CONF

Edite el fichero dhcpd.conf que se encuentra en la ruta /etc/dhcpd.conf.  
Modifique las siguientes líneas.

**Subnet 192.168.11.0 netmask 255.255.255.0**

En esta línea debe asignar el segmento de red con su respectiva máscara.

**Option routers 192.168.12.1**

**Option subnet-mask 255.255.255.0**

**Option nis-domain "alessa.com";**

**Option domain-name "alessa.com";**

**Option domain-name-servers 192.168.12.1;**

Digite la dirección del DNS

**Option netbios-name-servers 192.168.0.1;**

**Range dynamic-bootp 192.168.11.66 192.168.11.80**

Defina el rango de IP desde - hasta

```

root@alessa/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
ddns-update-style interim;
ignore client-updates;

subnet 192.168.12.0 netmask 255.255.255.0 {
# --- default gateway
    option routers          192.168.12.1;
    option subnet-mask      255.255.255.0;

    option nis-domain       "alessa.com";
    option domain-name      "alessa.com";
    option domain-name-servers 192.168.12.1;
    option netbios-name-servers 192.168.0.1;

    option time-offset      -18000; # Eastern Standard Time
    option ntp-servers      192.168.1.1;
    option netbios-name-servers 192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#    option netbios-node-type 2;

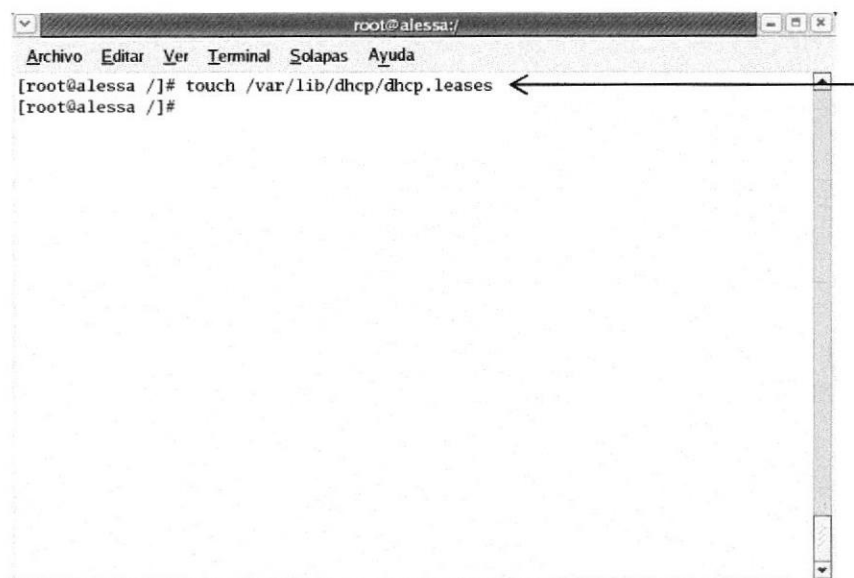
    range dynamic-bootp 192.168.12.8 192.168.12.16;
    default-lease-time 21600;
}

```

Figura 5-189: FICHERO DHCPD.CONF

Ahora debe crear un fichero **dhcpd.leases** en la ruta **var/lib/d.C./dhcpd.leases**, en este fichero se almacena las direcciones IP de las maquinas que tenga en en la red del servicio DHCP, lo debe crear de la siguiente manera **touch /var/lib/dhcp/dhcpd.leases**

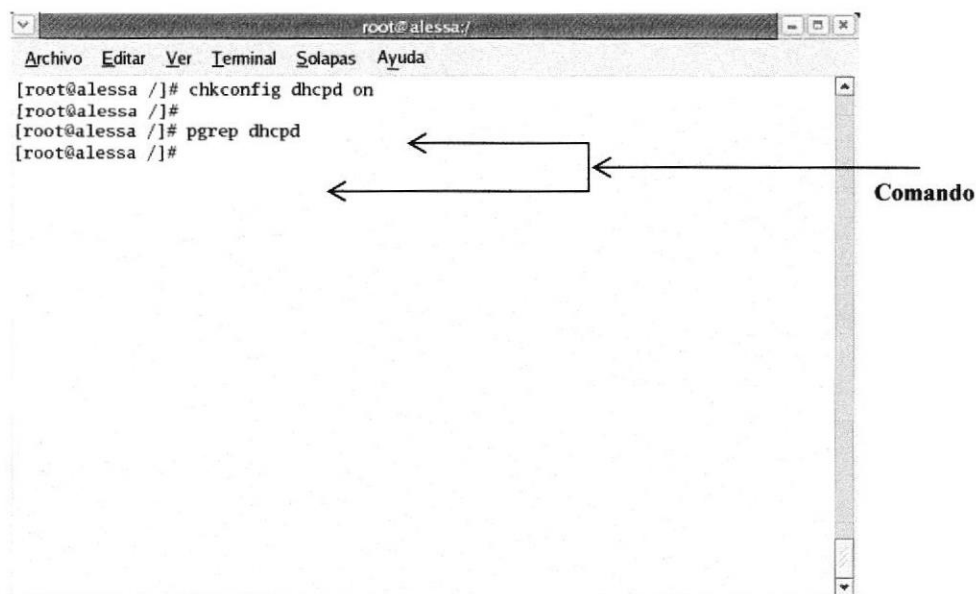
**Comando**



```
root@alessa:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@alessa /]# touch /var/lib/dhcp/dhcpd.leases  
[root@alessa /]#
```

**Figura 5-190: CREAR FICHERO DHCPD.LEASES**

Debe añadir el dhcp al arranque del sistema, lo debe hacer de la siguiente manera con el comando **chkconfig dhcpd on** y **pgrep dhcpd**.



```
root@alessa:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@alessa /]# chkconfig dhcpd on  
[root@alessa /]#  
[root@alessa /]# pgrep dhcpd  
[root@alessa /]#
```

**Comando**

**Figura 5-191: AÑADIR DHCP AL ARRANQUE DEL SISTEMA.**

Debe iniciar el servicio dhcp, con el comando `service dhcp start` de la siguiente manera **service dhcp start** y de un enter si la configuración no tiene ningún error o problema le saldrá un mensajes de **[OK]** indicándonos que la configuración ha sido satisfactoria.

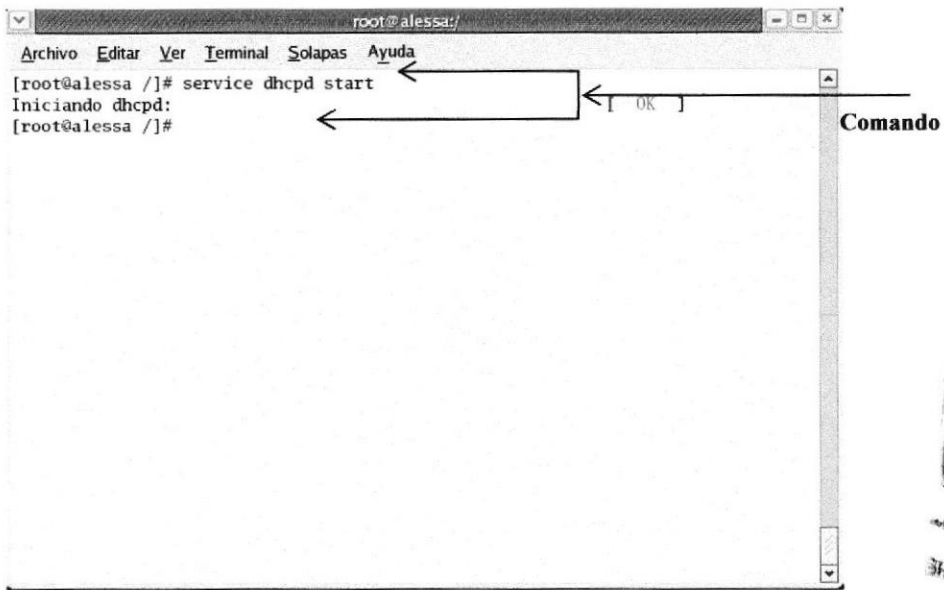


Figura 5-192: INICIAR SERVICIO DHCP



### 5.16.4. CONFIGURACIÓN EN EL CLIENTE

Primero debe configurar la tarjeta de red dándole una dirección IP automática, lo hará de la siguiente manera de clic derecho sobre mis sitios de red y seleccione **propiedades**.

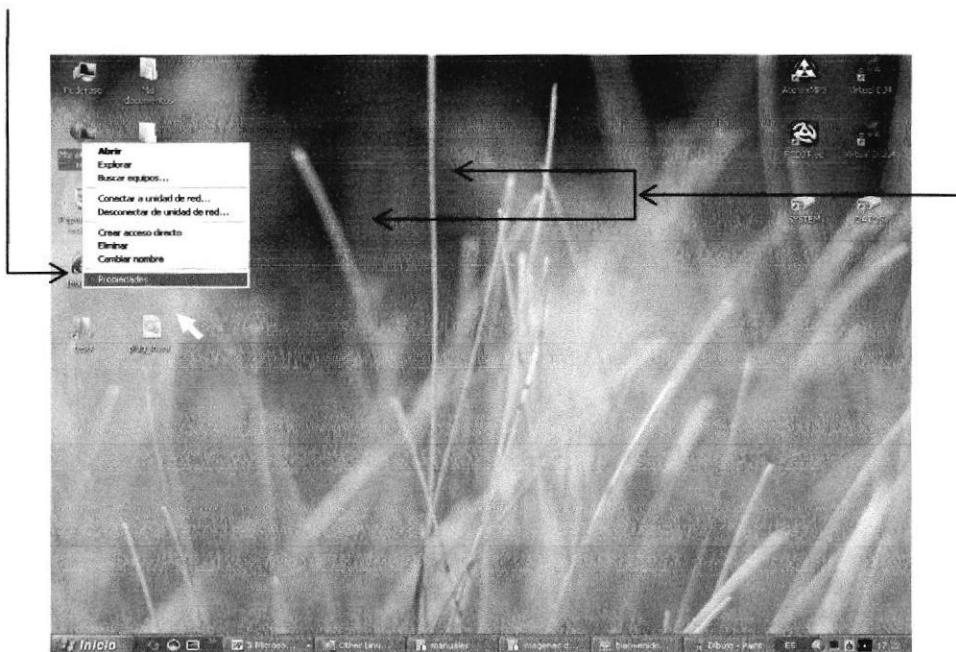


Figura 5-193: MIS SITIOS DE RED - PROPIEDADES.

Se habrá la ventana mis sitios de red seleccione conexión de área local y de clic derecho, seleccione **propiedades**.

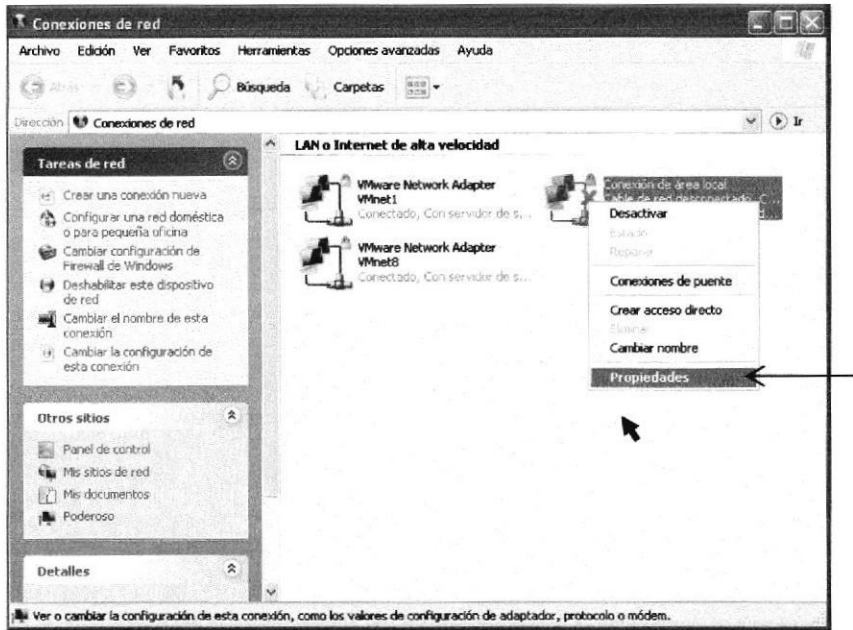


Figura 5-194: CONEXIÓN DE ÁREA LOCAL - PROPIEDADES.

Entonces se habrá la ventana propiedades de conexión de área local seleccione **protocolo Internet [TCP/IP]**, y de clic en **propiedades**.

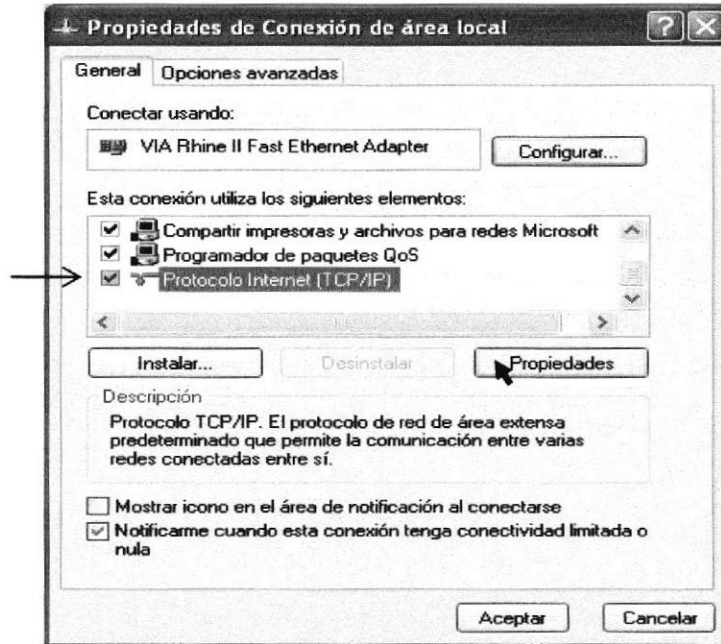


Figura 5-195: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL.

Ahora en esta ventana debe seleccionar la casilla **Obtener una dirección IP automáticamente** y de clic en **aceptar**.

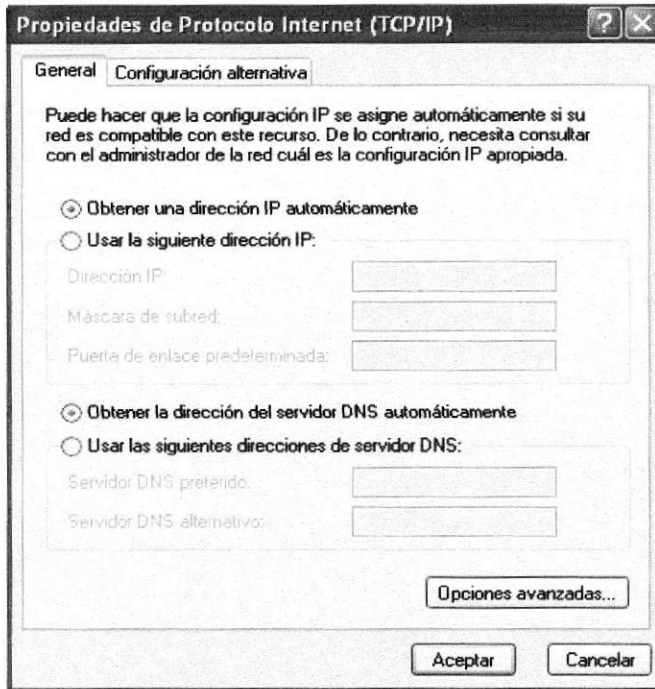


Figura 5-196: PROPIEDADES DE PROTOCOLO DE INTERNET.

Dar clic en inicio seleccione ejecutar.

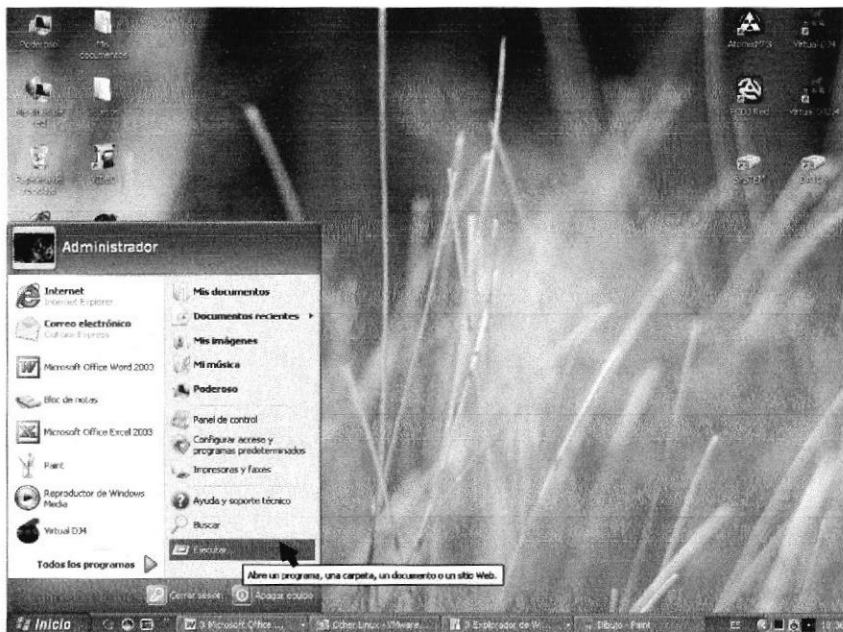


Figura 5-197: INGRESAR A EJECUTAR

Aparece la ventana de ejecutar y escriba el comando **cmd** par entrar a la consola DOS.

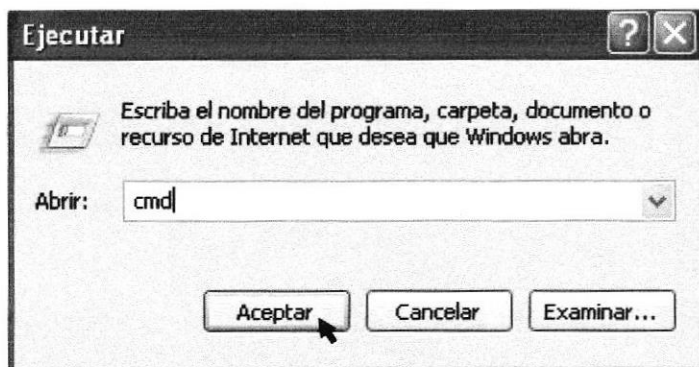


Figura 5-198: EJECUTAR

Ingrese el comando **ipconfig** y de un enter en la consola, le indicara la IP asignada automáticamente por el servidor DHCP.



Figura 5-199: CONSOLA DOS

## 5.17. FIREWALL

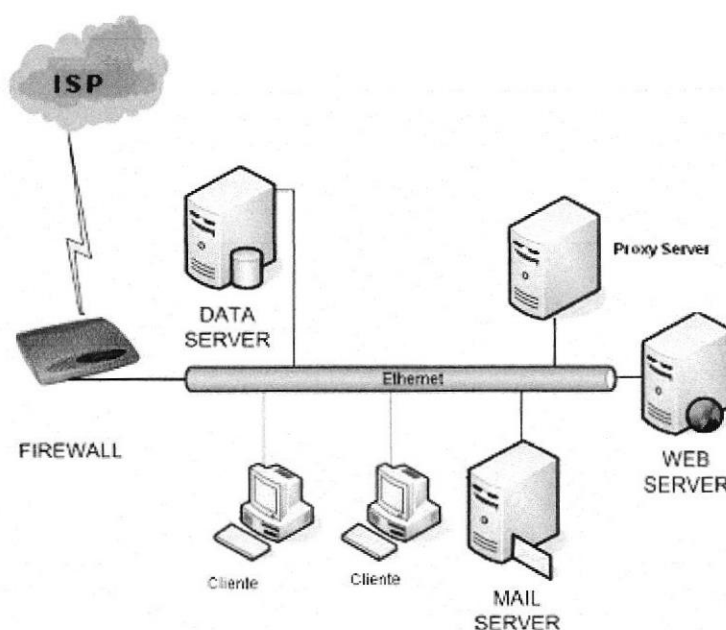


Figura 5-200: FIREWALL

### 5.17.1. ¿QUÉ ES FIREWALL?

Conocido también como muro de fuego, éste impedirá el acceso no autorizado a sus servicios e información, y/o controlar el acceso de los usuarios de su red a Internet. Es la interfaz entre el ordenador y la red. Determina qué recursos de su equipo están accesibles para los usuarios remotos de la red. Un Firewall bien configurado puede aumentar significativamente la seguridad de su sistema.

#### ¿Por qué un firewall?

Los hackers realizan sistemáticamente "barridos" de los ordenadores conectados a Internet, en busca de puertos de comunicaciones "abiertos" a través de los que puedan colarse en los equipos. Según datos de organismos como el FBI y el CSI (Computer Security Institute), aproximadamente un 85% de las grandes empresas han sufrido intrusiones en su red.

Los firewalls bloquean las entradas sin autorización a los ordenadores, además de restringir la salida de información de los mismos.

#### ¿Qué buscan los hackers en los ordenadores?

Por regla general, cuando un intruso accede a su ordenador, lo hace con intenciones poco amistosas:

Acceden a su información confidencial, pudiendo apropiarse por ejemplo de sus contraseñas de acceso a los servicios que use vía Internet (banca online o los propios servicios incluidos en su antivirus).

Se apropian del control de su ordenador, convirtiéndolo en un "zombie". Una vez hecho esto, el hacker podrá direccionar su ordenador, de forma simultánea a otros cientos o incluso miles de "zombies", contra un determinado sitios Web, provocando su colapso por sobrecarga. Esto es lo que se conoce como DoS (Denial of Service).

Después de hacerse con una parte del espacio de su disco duro, configuran su ordenador como una plataforma de descarga y distribución de software pirata a la que pueden acceder otros usuarios.

## IPTABLES

**Iptables:** Es un paquete de Linux que administra (inserta y borra) reglas de filtro de paquetes de la sección respectiva del kernel.

Esto significa que cuando el Server se re-inicie, cualquier cambio hecho se perderá, por lo que es necesario iniciar también el filtro de paquetes al iniciar el servidor.

Pero iptables también maneja conjuntamente enmascaramiento, pero no debe confundirse, ya que son dos conceptos distintos, también maneja re direccionamiento. El filtro de red kernel tiene tres tablas internas o listas de reglas. Son las siguientes:

**Filtro** => ésta es la tabla por defecto para manejar paquetes de red.

**Nat** => ésta tabla se usa para alterar paquetes que crean una nueva conexión.

**Mangle** => ésta tabla se usa tipos específicos de alteración de paquetes.

## ESTRUCTURA DE COMANDOS IPTABLES

Muchos comandos iptables tienen la siguiente estructura:

```
iptables [-t <table-name>]<command> <chain-name> <parameter> \ <option-1>
<parameter-n> <option-n>
```

En este ejemplo, la opción <table name> permite al usuario seleccionar una tabla diferente de la tabla filtro por defecto que se usa con el comando.

La opción <command> es el centro del comando, dictando cuál es la acción que específica a realizar. Como se pueda añadir o borrar una regla de una cadena particular, que es lo que se especifica en la opción <chain-name>.

Tras <chain-name> se encuentra los pares de parámetros y opciones que realmente definen la forma en la que la regla funcionará y que pasará cuando un paquete cumpla una regla.

Teclee iptables -h para ver una lista detallada de la estructura de los comandos iptables.

## ORDENES BÁSICAS DE FIREWALLS

Iptables -F: Borrado de reglas.

Iptables -L: Listado de reglas que se están aplicando.

Iptables -A: Añade una regla

Iptables -D: Borrar una regla.

Input : Entrada al servidor.

Output: Servidor hacia fuera.

Forward: Re direccionar

### 5.17.2. REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR FIREWALL

- ✓ Una maquina con Linux Fedora Core 3 instalado.
- ✓ Tarjeta de red.
- ✓ Tarjeta de red Configurada.

### 5.17.3. CONFIGURACIÓN DEL FIREWALL

#### 5.17.4. BLOQUEAR PING

**Iptables -A:** Añada una regla de firewall.

**INPUT:** Añadir una entrada al servidor.

**-s 192.168.12.2:** Es la dirección IP de origen.

**-d 192.168.12.1:** Es la dirección IP de destino.

**-p icmp :** Es el protocolo asignado.

**-j DROP:** Es la acción que se aplica para este caso es negar.

**dport 23:** Indica el Puerto que será bloqueado por Linux

```
Iptables -A INPUT -s 192.168.12.2 -d 192.168.12.1 -p icmp -j DROP
```

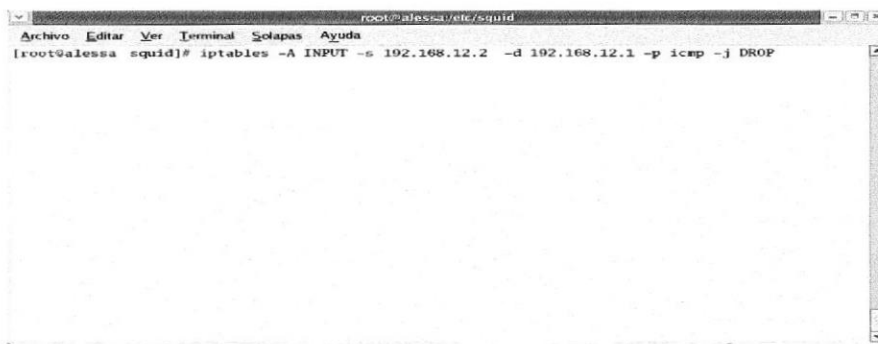


Figura 5-201: BLOQUEAR PING

#### 5.17.5. BLOQUEAR TELNET

```
Iptables -A INPUT -s 192.168.12.2 -d 192.168.12.1 -p tcp --dport 23 -j DROP
```

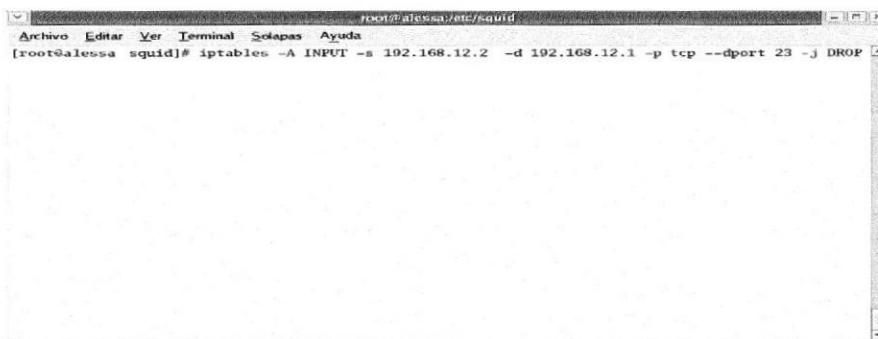
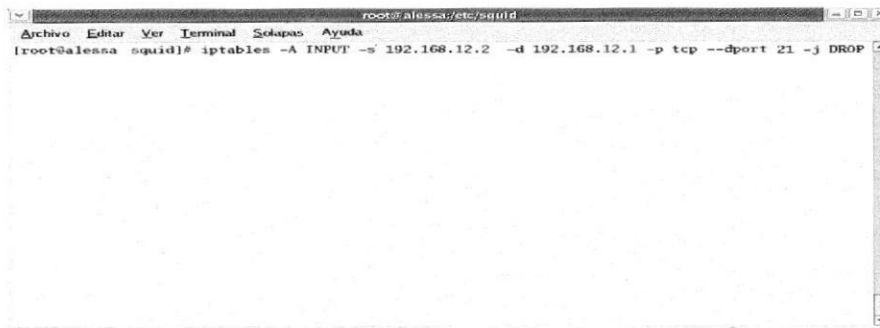


Figura 5-202: BLOQUEAR TELNET

### 5.17.6.BLOQUEAR FTP

Iptables -A INPUT -s 192.168.12.2 -d 192.168.12.1 -p tcp --dport 21 -j DROP

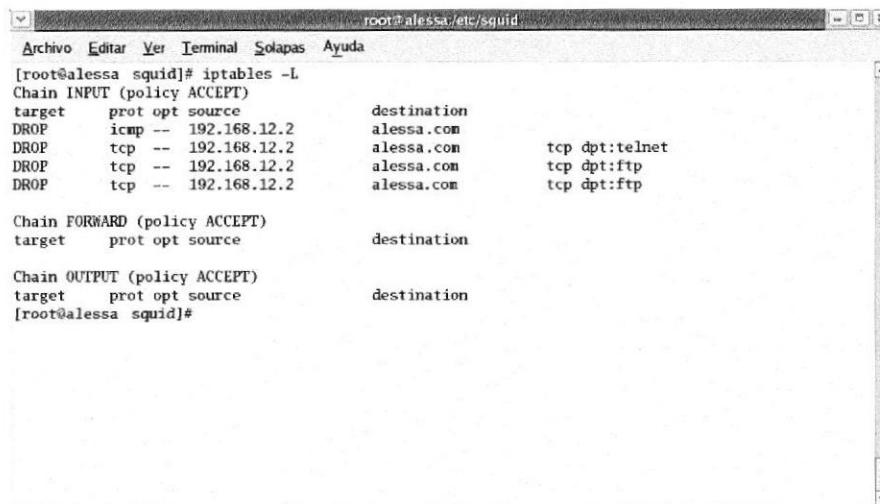


```

root@alessa/etc/squid
Archivo Editar Ver Terminal Solapas Ayuda
[root@alessa squid]# iptables -A INPUT -s 192.168.12.2 -d 192.168.12.1 -p tcp --dport 21 -j DROP
  
```

Figura 5-203: BLOQUEAR FTP

Para verificar si se habilitaron los Firewalls en el servidor Linux escriba el siguiente comando: Iptables -L



```

root@alessa/etc/squid
Archivo Editar Ver Terminal Solapas Ayuda
[root@alessa squid]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      icmp -- 192.168.12.2          alessa.com
DROP      tcp  -- 192.168.12.2          alessa.com          tcp dpt:telnet
DROP      tcp  -- 192.168.12.2          alessa.com          tcp dpt:ftp
DROP      tcp  -- 192.168.12.2          alessa.com          tcp dpt:ftp

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@alessa squid]#
  
```

Figura 5-204: VERIFICACIÓN DE LAS REGLAS DE FIREWALL

### 5.17.7. CONFIGURACIÓN DEL CLIENTE

En el cliente Windows de clic en inicio – ejecutar, y escriba el comando **cmd** para abrir el prompt del DOS.

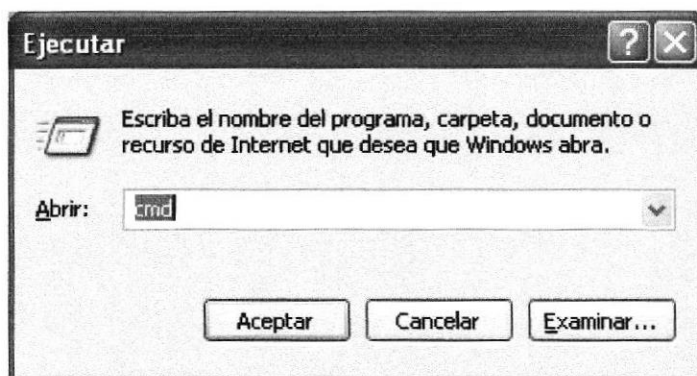


Figura 5-205: EJECUTAR

Esta pantalla le muestra que esta habilitado el ping hacia el servidor.

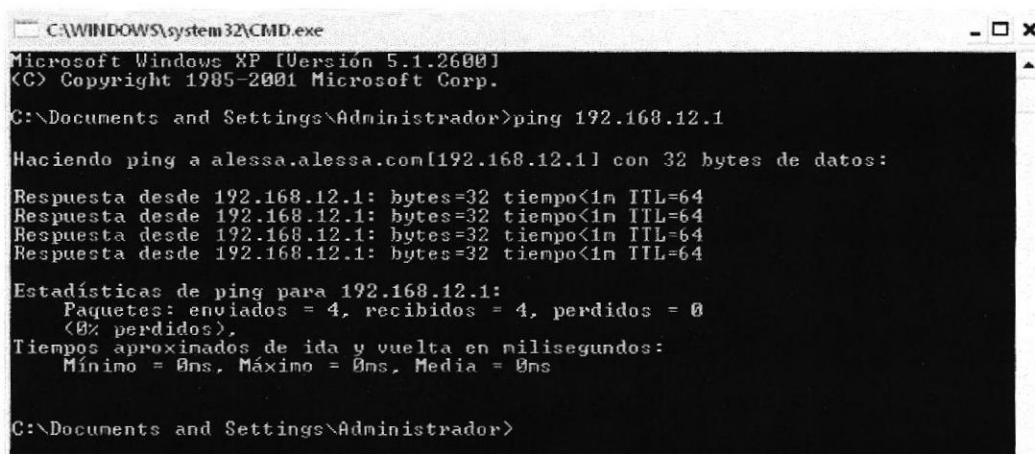


Figura 5-206: PING AL SERVIDOR

Esta pantalla le muestra que esta habilitado el telnet hacia el servidor. En el cual debe escribir un usuario y una contraseña para poder ingresar.

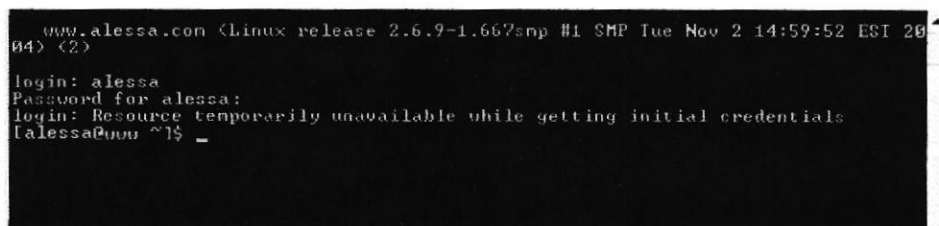
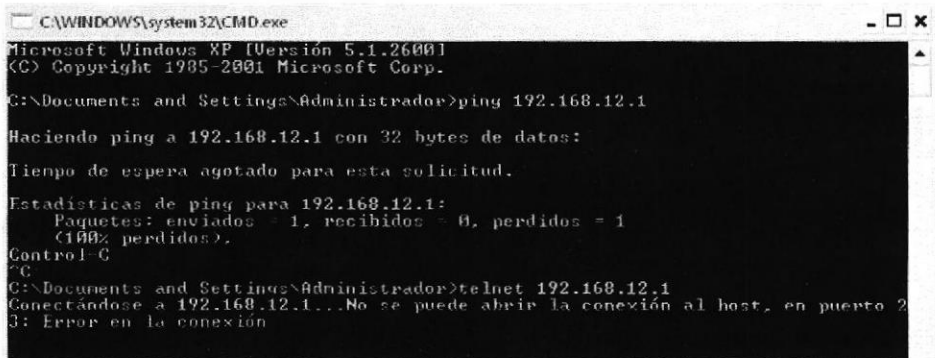


Figura 5-207: INGRESAR USUARIO Y CONTRASEÑA

### 5.17.8.BLOQUEO DEL PING Y DEL TELNET

Antes de realizar la prueba debe añadir las reglas del firewall, ya antes configurada en el servidor. En el cliente para verificar si esta levantado los Firewalls debe hacer ping al servidor, y luego un telnet y debe mostrarle de la siguiente manera.



```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

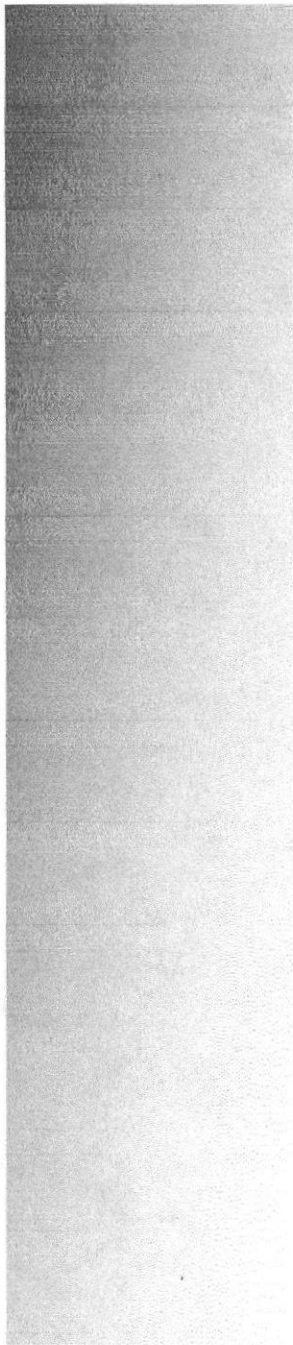
C:\Documents and Settings\Administrador>ping 192.168.12.1

Haciendo ping a 192.168.12.1 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.12.1:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
              (100% perdidos).
Control-C
^C
C:\Documents and Settings\Administrador>telnet 192.168.12.1
Conectándose a 192.168.12.1...No se puede abrir la conexión al host, en puerto 23:
3: Error en la conexión
```

Figura 5-208: BLOQUEO DEL PING Y DEL TELNET





## CAPÍTULO 6

# CONFIGURACIÓN DE ROUTERS Y SWITCHES

## 6. ROUTER

Un router es un dispositivo que acorde a su funcionalidad se puede ubicar en la capa 3 del modelo OSI. Su función básica es la de enrutar paquetes.

Específicamente, a través de los protocolos de enrutamiento, los routers toman decisiones sobre cuál 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.

### VISTA POSTERIOR DEL ROUTER

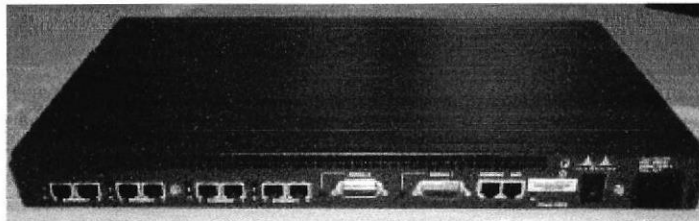


Figura 6-1: VISTA POSTERIOR DEL ROUTER

### VISTA FRONTAL DEL ROUTER

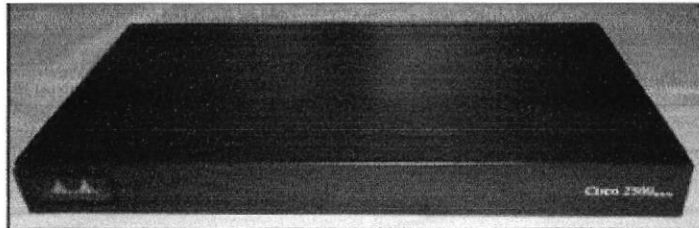


Figura 6-2: VISTA FRONTAL DEL ROUTER

### 6.1. ¿QUE ES UN ROUTER?

El **router** llamado también (**enrutador** o **encaminador**) es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa 3 (nivel de red) del modelo **OSI**. Este dispositivo interconecta segmentos de red o redes enteras, hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.



## VENTAJAS DE LOS ROUTERS

**Seguridad.** Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.

**Flexibilidad.** Las redes interconectadas con router no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con bridge.

**Soporte de Protocolos.** Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.

## DESVENTAJAS DE LOS ROUTERS

- ✓ Lentitud de proceso de paquetes respecto a los bridges.
- ✓ Necesidad de gestionar el sub direccionamiento en el Nivel de Enlace.
- ✓ Precio superior a los bridges.
- ✓ Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para una gran interconexión de redes con múltiples tipos de RALs, MANs, WANs y diferentes protocolos. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas.



## Características de los Routers

Un router es un conmutador de paquetes que opera en el nivel de red del modelo OSI. Sus principales características son:

- ✓ Permiten interconectar tanto redes de área local como redes de área extensa.
- ✓ Proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP.
- ✓ Son capaces de rutear dinámicamente, es decir, son capaces de seleccionar el camino que debe seguir un paquete en el momento en el que les llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas, etc.
- ✓ Los routers son más inteligentes que los switches, pues operan a un nivel mayor lo que los hace ser capaces de procesar una mayor cantidad de información, esta mayor inteligencia, sin embargo, requiere más procesador, lo que también los hará más caros a diferencia de los switches y bridges, que sólo leen la dirección MAC, los routers analizan la información contenida en un paquete de red leyendo la dirección de red. Los routers leen cada paquete y lo envían a través del camino más eficiente posible al destino apropiado, según una serie de reglas

recogidas en sus tablas, los routers se utilizan a menudo para conectar redes geográficamente separadas usando tecnologías WAN de relativa baja velocidad, como ISDN, una línea T1, Frame Relay, etc. El router es entonces la conexión vital entre una red y el resto de las redes. Un router también sabe cuándo mantener el tráfico de la red local dentro de ésta y cuándo conectarlo con otras LANs, es decir, permite filtrar los broadcasts de nivel de enlace. Esto es bueno, por ejemplo, si un router realiza una conexión WAN, así el tráfico de broadcast de nivel dos no es ruteado por el enlace WAN y se mantiene sólo en la red local. Eso es especialmente importante en conexiones conmutadas como RDSI. Un router dispondrá de una o más interfases de red local, las que le servirán para conectar múltiples redes locales usando protocolos de nivel de red.

## 6.2. MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER

### 6.2.1. CABLE DTE Y DCE

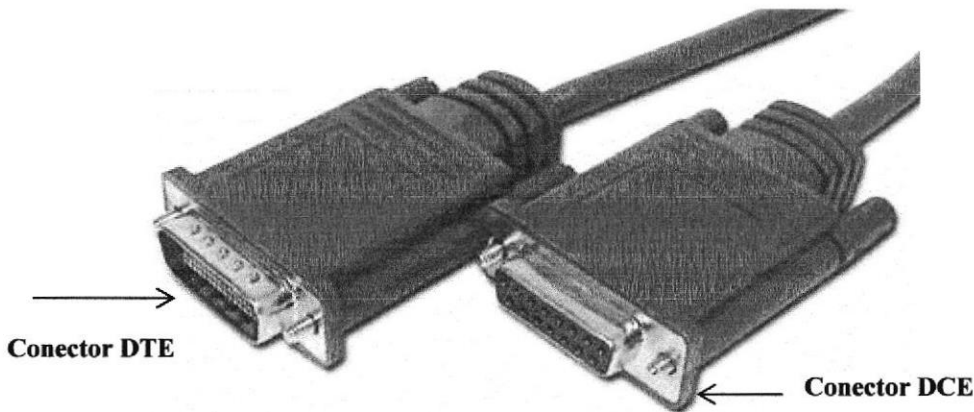


Figura 6-:3 CABLE DTE Y DCE

La conexión entre los cables DTE (Equipo de Terminación de Circuito de Datos) / DCE (Equipo Terminal de Datos), simulan los dispositivos que conforman la nube WAN.

#### Cable DCE (Data Circuit Equipment)

Es el cable que se conectara al equipo que realiza la función de DCE. Para simular la conexión serie con otro router, se utilizaran dos cables uno DCE-DTE. Siendo el DCE el que marcará el clock rate.

Es un conector hembra distinguible por tener el conector smartnet más pequeño.

#### CABLE DTE (Data Terminal Equipment)

Es el cable que se conectara al equipo que realiza la función de DTE. Generalmente será el cable que unirá un router a un MODEM CSU/DSU.

Es un conector macho distinguible por tener el conector smartnet más grande.

### 6.2.2. CABLE UTP

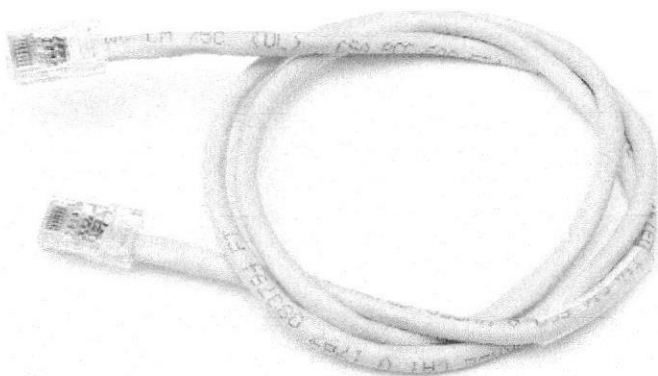


Figura 6-4: CABLE UTP

El cable Categoría 5 es el que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones, sin embargo, las predicciones de los analistas y sondeos independientes indican que el cable de Categoría 6 sobrepasará al cable Categoría 5 en instalaciones de red.

El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

### 6.2.3. CONECTOR RJ – 45

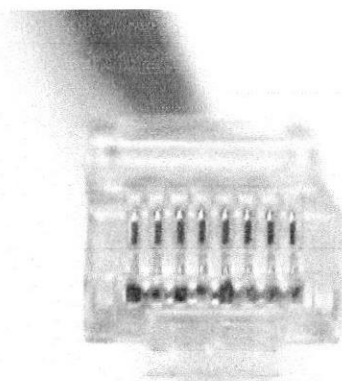


Figura 6-5: CONECTOR RJ 45

EIA/TIA especifica el uso de un conector RJ-45 para cables UTP, las letras RJ significan "registered jack" (jack registrado), y el número 45 se refiere a una secuencia específica de cableado.

El conector transparente RJ-45 muestra ocho hilos de distintos colores. Cuatro de estos hilos conducen el voltaje y se consideran "tip" (punta) (T1 a T4). Los otros cuatro hilos están conectados a tierra y se llaman "ring" (anillo) (R1 a R4).

Tip y ring son términos que surgieron a comienzos de la era de la telefonía. Hoy, estos términos se refieren al hilo positivo y negativo de un par. Los hilos del primer par de un cable o conector se llaman T1 y R1. El segundo par son T2 y R2, y así sucesivamente.

### 6.2.4. PUERTO SERIAL (CONECTOR COM)

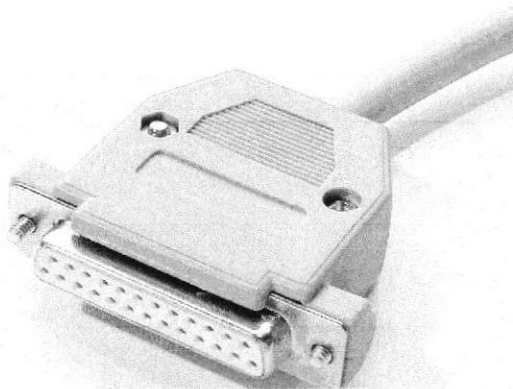


Figura 6-6: CONECTOR COM

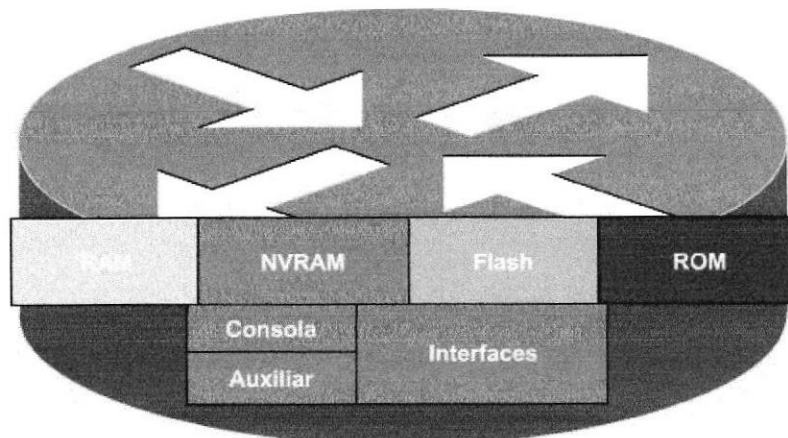
El cable Categoría 5 es el que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones, sin embargo, las predicciones de los analistas y sondeos independientes indican que el cable de Categoría 6 sobrepasará al cable Categoría 5 en instalaciones de red.

El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

La arquitectura interna del router Cisco soporta componentes que cumplen un papel fundamental en el proceso de inicio, como se indica.

El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

## 6.3. COMPONENTES DE CONFIGURACIÓN INTERNA DEL ROUTER



**Figura 6-7: COMPONENTES DE CONFIGURACIÓN INTERNA DEL ROUTER**

La arquitectura interna del router Cisco soporta componentes que cumplen un papel fundamental en el proceso de inicio, como se indica en la figura. Los componentes internos de la configuración del router son los siguientes:

### 6.3.1. RAM

También llamada (DRAM), es el área de almacenamiento de trabajo de un router, 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.

### 6.3.2. NVRAM

Tiene las siguientes características y funciones:

- ✓ Almacena el archivo de configuración inicial.
- ✓ Retiene el contenido cuando se apaga o reinicia el router.

### 6.3.3. 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 de ROM programable, que se puede borrar electrónicamente (EEPROM)

### 6.3.4. MEMORIA DE SÓLO LECTURA (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.

## 6.4. PARTES EXTERNAS DEL ROUTER

### 6.4.1. 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.

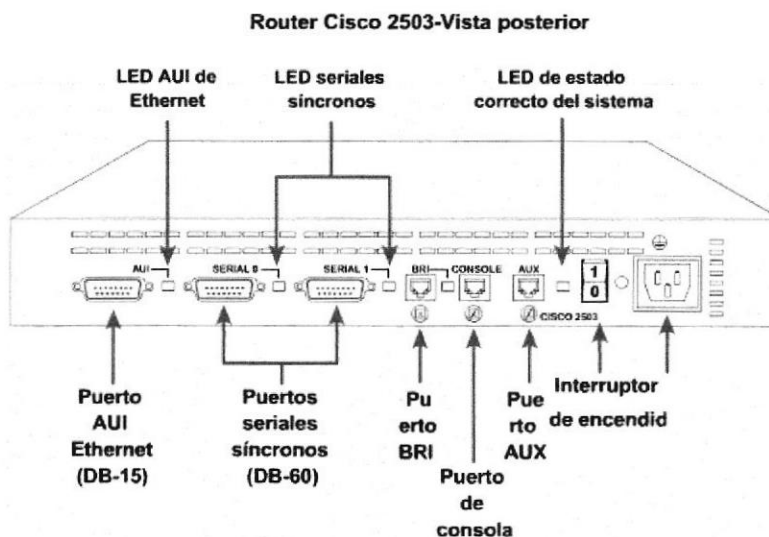


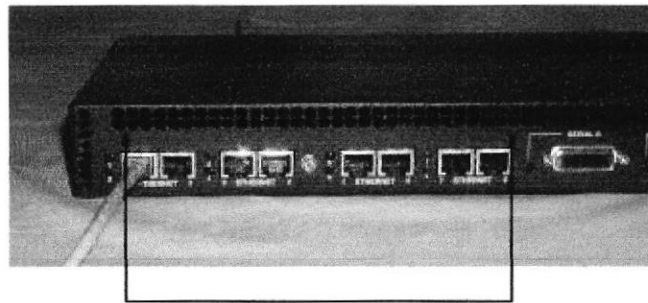
Figura 6-8: INTERFACES DEL ROUTER

Las interfaz de Cisco son a menudo llamadas puertos, y cada puerto se diseñará físicamente y apropiadamente para que se conecte al tipo de tecnología de la red que se supone a servir

Por ejemplo, una interfaz de LAN, como un puerto de Ethernet en el router consistirá en un conector de RJ-45.

### LAN INTERFACES

Las routers de Cisco soportan varias redes de LAN normalmente usadas, la mayoría de las LAN son interfaces comunes, Ethernet, Fast Ethernet, IBM Token Ring y (FDDI). Todos estos protocolos de LAN mencionados abarcan la misma capa de Enlace de Datos.



Conexiones LAN

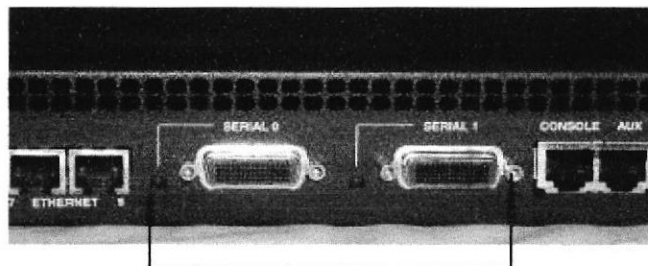
Figura 6-9: INTERFACES LAN

Dependiendo del tipo de router que se tenga, las conexiones LAN típicas son Ethernet o Token Ring.

### WAN INTERFACES

Las interfaces serial del router proporcionan una manera de conectar LANs que usa tecnología WAN. Los protocolos WAN mueven los datos por asíncrono y sincronas.

Algunos de los Datos WAN normalmente usados se unen que las tecnologías de la capa de enlace de datos, Frame Relay, los Servicios integrados la Red Digital (ISDN) y Punto a Punto el protocolo (PPP) todos los protocolos WAN discutidos se configuran adelante.



Conexiones WAN

Figura 6-10: INTERFACES WAN

Para las comunicaciones de larga distancia, las WAN utilizan transmisiones seriales, este es un proceso por el cual los bits de datos se envían por un solo canal, este proceso brinda comunicaciones de larga distancia confiables y el uso de un rango específico de frecuencias ópticas o electromagnéticas.

DTE (Equipo de Terminación de Circuito de Datos) / DCE (Equipo Terminal de Datos). Se conectan el puerto serial a los dispositivos WAN, como módems de gran velocidad o los dispositivos digitales.

Las líneas arrendadas consisten típicamente en un camino físico conectado al extremo del cliente a un Datos

El Elemento terminal (DTE). El proveedor de servicio tiene las Comunicaciones de los Datos típicamente

El equipo (DCE) eso se usa para conectar al DTE al sitio del cliente. El DTE

Las cuida de establecer y mantener la comunicación con el DCE al otro extremo.

Las velocidades del reloj y velocidades de transmisión de datos son controladas por el DCE.

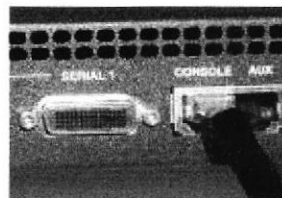
## **LAS INTERFACES LÓGICAS**

Antes de que nosotros concluyamos nuestra discusión de las interfaces del router, nosotros debemos fijar la mirada a las interfaces lógicas, una interfaz lógica es un software-only- interface - y se crea usando el IOS del router.

La interfaz lógica no existe como la interfaz del hardware real del router, usted puede pensar en la interfaz lógica como las interfaces virtuales que se ha creado con una serie de comandos de software del router.

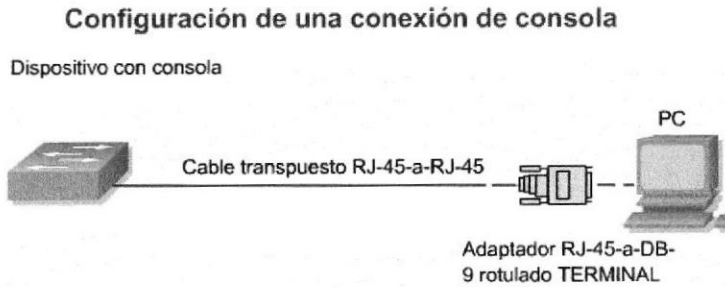
Esta interfaz virtual puede verse por los dispositivos en la red como la interfaz real, así como una interfaz del hardware como un puerto serial, usted puede configurar tipos diferentes de interfaz lógicas.

## **6.5. CONEXIÓN A CONSOLA**



**Figura 6-11: PUERTO DE CONSOLA**

Para configurar inicialmente un dispositivo Cisco, se debe conectar directamente una conexión para administración al dispositivo, para los equipos Cisco esta conexión para administración recibe el nombre de puerto de consola, este puerto de consola permite monitorear y configurar un hub, switch o router Cisco.



**Figura 6-12: CONFIGURACIÓN DE UNA CONEXIÓN DE CONSOLA**

El cable que se utiliza entre el terminal y el puerto de consola es el cable transpuesto, con conectores RJ-45, también conocido como cable de consola, tiene una disposición de pins diferente que la de los cables de conexión directa o conexión cruzada RJ-45 usados en Ethernet, la disposición de pins para un cable transpuesto es la siguiente:

- 1 a 8
- 2 a 7
- 3 a 6
- 4 a 5
- 5 a 4
- 6 a 3
- 7 a 2
- 8 a 1



## 6.6. SISTEMA DE ARRANQUE BOOTSTRAP

Como todo ordenador, un router necesita un sistema de arranque (bootstrap), encargado de realizar un chequeo del resto de los componentes antes de pasar el control a un sistema operativo (Cisco IOS, en el caso de los routers Cisco).

El sistema de arranque se almacena en una memoria ROM (Read Only Memory = Memoria de Solo Lectura), junto con una parte básica del sistema operativo, la que toma el control inicialmente, mientras que el cuerpo principal de éste se almacena en una memoria especial, de tipo FLASH, que se puede borrar y reprogramar, permitiendo con ello las actualizaciones necesarias, el contenido de la memoria Flash se conserva en caso de cortes de energía o durante los reinicio del router.

Por otra parte, las funcionalidades operativas de los routers son configurables mediante una serie de instrucciones escritas en un fichero de texto, denominado archivo de configuración, que se almacena en un módulo de memoria de tipo NVRAM (No Volatil RAM), cuyo contenido se conserva durante un corte de energía o si se reinicia el equipo.

Una vez inicializado un router, el fichero de configuración es cargado en una memoria RAM (Random Access Memory = Memoria de Acceso Aleatorio), desde la que se va ejecutando el conjunto de órdenes en él contenido. También se almacenan en esta memoria las tablas de enrutamiento, encargadas de almacenar los puertos del router por los que son accesibles las diferentes máquinas.

Por último, el router posee una serie de puertos o interfaces físicas, puntos de conexión del mismo con las diferentes redes a las que está unido, y a través de los cuales se produce la entrada y salida de datos al equipo.

## 6.7. ENRUTAMIENTO

### 6.7.1. ENRUTAMIENTO ESTÁTICO

Utiliza una ruta de protocolo que el administrador de red introduce en el router, las operaciones con rutas estáticas pueden dividirse en tres partes:

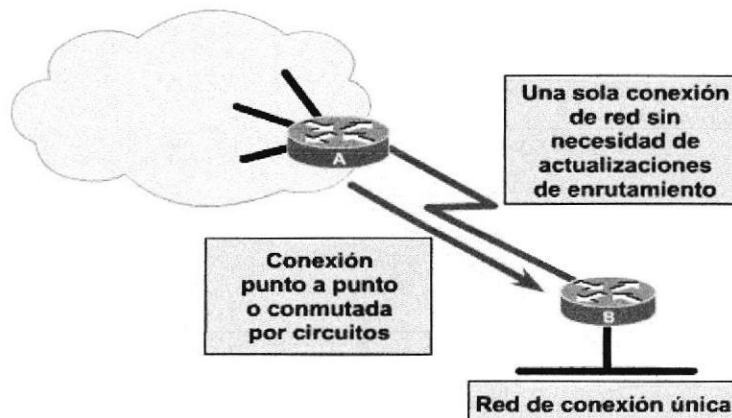
- ✓ El administrador de red configura la ruta.
- ✓ El router instala la ruta en la tabla de enrutamiento.
- ✓ Los paquetes se enrutan de acuerdo a la ruta estática.

Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando **IP route**.

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.

El enrutamiento estático posee varias aplicaciones útiles, mientras que el enrutamiento dinámico tiende a revelar todo lo que se conoce acerca de la internetwork, es posible que por razones de seguridad se desee ocultar parte de una internetwork, el enrutamiento estático le permite especificar la información que desea revelar acerca de redes restringidas.

Cuando se puede acceder a una red a través de un solo camino, una ruta estática hacia la red puede ser suficiente. Este tipo de red se denomina red de conexión única. La configuración del enrutamiento estático para una red de conexión única evita el gasto que implica el enrutamiento dinámico.



- ◆ Ruta fija a la dirección refleja el conocimiento del administrador

**Figura 6-13: ENRUTAMIENTO ESTÁTICO**



El enrutamiento estado-enlace (también denominado *primero la ruta libre más corta*) recrea la topología exacta de toda la internetwork (o por lo menos la porción en la que se ubica el router).

El enrutamiento híbrido balanceado combina aspectos de los algoritmos de estado-enlace y vector-distancia. En las páginas siguientes se hará referencia a los procedimientos y problemas para cada uno de estos algoritmos de enrutamiento y se presentan técnicas para reducir al mínimo los problemas.

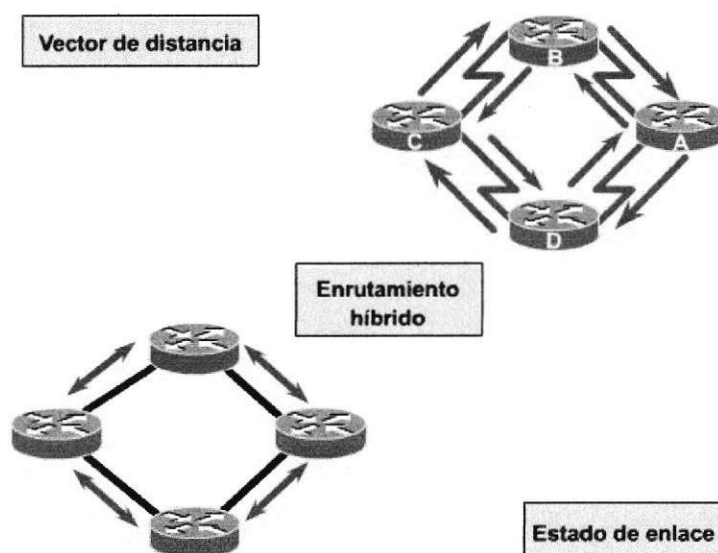


Figura 6-15: CLASES DE PROTOCOLO DE ENRUTAMIENTO

Ejemplos de protocolos de enrutamiento:

- ✓ Protocolo de información de enrutamiento (RIP).
- ✓ Protocolo de enrutamiento de gateway interior (IGRP).
- ✓ Protocolo de enrutamiento de gateway interior mejorado (EIGRP).
- ✓ Protocolo "Primero la ruta más corta" (OSPF).

### 6.7.3. TIPOS DE PROTOCOLOS

#### 6.7.3.1. 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 base 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.

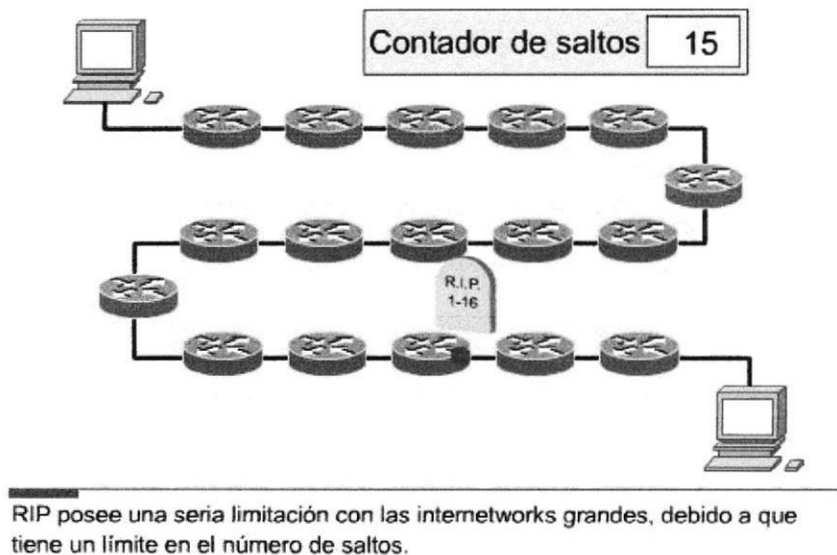
RIP ha evolucionado a lo largo de los años desde el Protocolo de enrutamiento con definición de clases, RIP Versión 1 (RIP v1), hasta el Protocolo de enrutamiento sin clase, RIP Versión 2 (RIP v2).

Las mejoras en RIP v2 incluyen:

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).

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.
- ✓ No siempre selecciona la ruta más rápida para los paquetes.
- ✓ Genera gran cantidad de tráfico de red con las actualizaciones.



RIP posee una seria limitación con las internetworks grandes, debido a que tiene un límite en el número de saltos.

**Figura 6-16: PROTOCOLO DE ENRUTAMIENTO RIP**

### 6.7.3.2. FUNCIONAMIENTO RIP

RIP utiliza UDP para enviar sus mensajes y el puerto bien conocido 520.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.

RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado)

RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).

La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino. Teniendo en cuenta el límite de 15 saltos mencionado anteriormente. Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.

Las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.

#### 6.7.3.2.1. VENTAJAS

En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar. Además, es un protocolo abierto, soportado por muchos fabricantes.

#### 6.7.3.2.2. DESVENTAJAS

Por otra parte, tiene la desventaja que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos (por cuántos routers o equipos similares pasa la información); no toma en cuenta otros criterios importantes, especialmente el ancho de banda, esto puede causar ineficiencias, ya que puede preferir una ruta de bajo ancho de banda.

#### 6.7.3.3. MENSAJES RIP

##### 6.7.3.3.1. TIPOS DE MENSAJES RIP

Los mensajes RIP pueden ser de dos tipos.

**Petición:** Enviados por algún enrutador recientemente iniciado que solicita información de los enrutadores vecinos.

**Respuesta:** mensajes con la actualización de las tablas de enrutamiento. Existen tres tipos:

Mensajes ordinarios: Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos.

Mensajes enviados como respuesta a mensajes de petición.

Mensajes enviados cuando cambia algún coste. Sólo se envían las rutas que han cambiado.

### **6.7.3.3.2. FORMATO DE LOS MENSAJES RIP**

Los mensajes tienen una cabecera que incluye el tipo de mensaje y la versión del protocolo RIP, y un máximo de 25 entradas RIP de 20 bytes.

Las entradas en RIPv1 contienen la dirección IP de la red de destino y la métrica.

Las entradas en RIPv2 contienen la dirección IP de la red de destino, su máscara, el siguiente enrutador y la métrica. La autenticación utiliza la primera entrada RIP.

### **6.7.4. EL PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY (IGRP)**

IGRP es un protocolo de enrutamiento basado en la tecnología vector-distancia. Utiliza una métrica compuesta para determinar la mejor ruta basándose en el ancho de banda, el retardo, la confiabilidad y la carga del enlace. El concepto es que cada router no necesita saber todas las relaciones de ruta/enlace para la red entera.

Cada router publica destinos con una distancia correspondiente. Cada router que recibe la información, ajusta la distancia y la propaga a los routers vecinos. La información de la distancia en IGRP se manifiesta de acuerdo a la métrica. Esto permite configurar adecuadamente el equipo para alcanzar las trayectorias más óptimas.

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.

### **6.7.5. EL PROTOCOLO EIGRP**

Es un protocolo de encaminamiento híbrido, propietario de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Sin embargo, EIGRP es más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP.

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.

Los routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos.

Las rutas reciben un estado y se pueden rotular para proporcionar información adicional de utilidad.

EIGRP mantiene las siguientes tres tablas:

#### **Tabla de vecinos.**

Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP.

#### **Tabla de topología.**

La tabla de topología se compone de todas las tablas de encaminamiento EIGRP recibidas de los vecinos. EIGRP toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino. EIGRP rastrea esta información para que los routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente. La información que el router recibe de los vecinos se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología. Los routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red (como IP, IPv6 o IPX). La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

#### **Tabla de encaminamiento**

La tabla de encaminamiento EIGRP contiene las mejores rutas hacia un destino. Esta información se recupera de la tabla de topología. Los routers EIGRP mantienen una tabla de encaminamiento por cada protocolo de red.

### **6.7.6. EL PROTOCOLO CONOCIDO COMO "PRIMERO LA RUTA MÁS CORTA" (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 internetworks grandes y 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

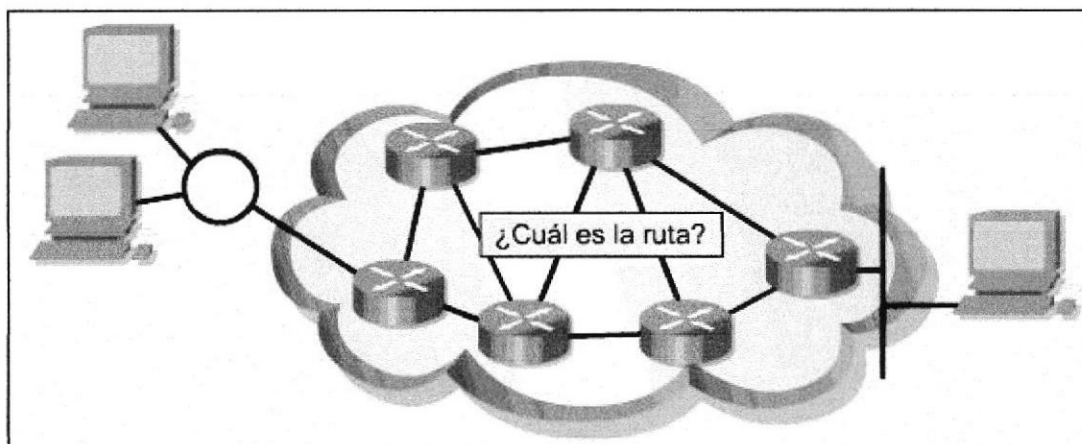


Figura 6-17: PROTOCOLO DE ENRUTAMIENTO OSPF

**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.**- Esta 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.**- Este 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 deber ser igual a 0.

## **TIPOS DE ÁREA**

Una red OSPF está dividida en áreas. Estas áreas son grupos lógicos de encaminadores cuya información se puede resumir para el resto de la red. Se pueden definir diferentes tipos de áreas "especiales":

### **ÁREA BACKBONE**

El área backbone (o área cero) forma el núcleo de una red OSPF. Todas las demás áreas y las rutas interiores de las áreas están conectadas a un encaminador conectado a una área backbone.

### **ÁREA STUB**

Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento. t-so-stubby

### **ÁREA NOT-SO-STUBBY**

También conocidas como NSSA se trata es un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

## **ESTADOS DE OSPF**

Las interfaces OSPF pueden encontrarse en uno de siete estados. Los vecinos OSPF progresan a través de estos estados, uno a la vez en el siguiente orden:

### **ESTADO DESACTIVADO (DOWN STATE)**

En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización).

### **ESTADO DE INICIALIZACIÓN (INIT STATE)**

Los encaminadores OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los encaminadores vecinos. Cuando una interfaz recibe su primer paquete Hello, el encaminador entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa.

Los dos tipos de relaciones son Dos-Vías y Adyacencia. Un encaminador debe recibir un Hello desde un vecino antes de establecer algún tipo de relación.

## ESTADO DE DOS-VÍAS (TWO-WAY)

Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de dos-vías, o comunicación vi direccional, con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un enrutador ingresa al estado de Dos-Vías cuando se ve a sí mismo en un paquete Hello proveniente de un vecino.

El estado de Dos-Vías es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos. Para aprender los estados de enlace de otros encaminadores y eventualmente construir una tabla de encaminamiento, cada encaminador OSPF debe formar a lo menos una adyacencia. Una adyacencia es una relación avanzada entre encaminadores OSPF que involucra una serie de estados progresivos que se basa no tan solo en paquetes Hello, si no que otros 4 paquetes OSPF. Aquellos encaminadores intentando volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.

## ESTADO EXSTART

Técnicamente, cuando un encaminador y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs. Los dos encaminadores vecinos emplean paquetes Hello para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos.

Aquel encaminador con el mayor router ID "gana" y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.

## ESTADO DE INTERCAMBIO (EXCHANGE)

En el estado de intercambio, los encaminadores vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los encaminadores se describen sus bases de datos de estado de enlace entre ellos. Los encaminadores comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace. Si alguno de los encaminadores recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.

## ESTADO CARGANDO (LOADING)

Después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un enrutador recibe un LSR este responde empleando un paquete de actualización de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace (LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados



BIOTECNA  
CAMPUS  
PENAS

empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

## ESTADO DE ADYACENCIA (ADJACENCY)

Cuando el estado de carga ha sido completado, los enrutadores se vuelven completamente adyacentes. Cada enrutador mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

## 6.8. LISTAS DE CONTROL DE ACCESO

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 especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

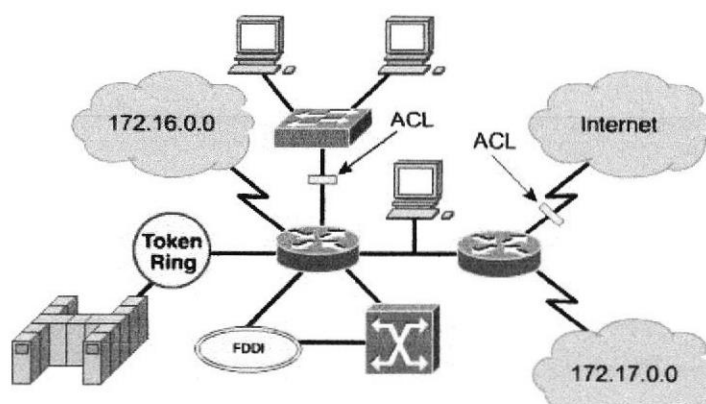
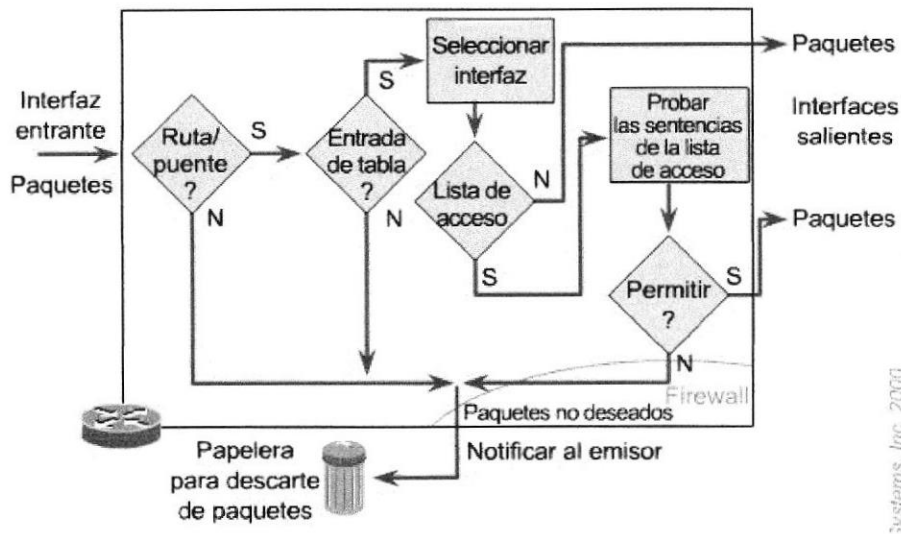


Figura 6-18: LISTAS DE CONTROL DE ACCESO

### 6.8.1. FUNCIONAMIENTO DE LAS ACL



**Figura 6-19: COMO FUNCIONAN 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.

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 cantidad 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 la 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 sea 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.

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 cantidad 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.

## 6.8.2. 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 configura las ACL en el router, cada ACL debe identificarse de forma única, asignándole 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
IP extendido	100-199
AppleTalk	600-699
IPX	800-899
IPX extendido	900-999
Protocolo de publicación de servicio IPX	1000-1099

**Figura 6-20: PROTOCOLOS CON ACL ESPECIFICADAS**

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.

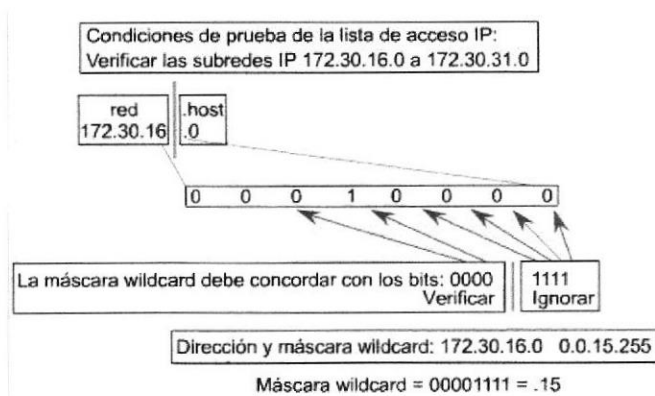
En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, usando el comando `ip access-group` en el modo de configuración de interfaz. Al asignar una ACL a una interfaz, se debe especificar la ubicación entrante o saliente. Después de crear una ACL numerada, se la debe asignar a una interfaz.

## 6.8.3. FUNCIÓN DE LA MÁSCARA WILDCARD EN UNA ACL

Una máscara wildcard es una cantidad de 32-bits que se divide en cuatro octetos. Una máscara wildcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar como tratar los bits de la dirección IP correspondiente. Las máscaras wildcard 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 wildcard 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 wildcard 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 wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.

Los números uno y cero en la máscara se usan para identificar como tratar los bits de la dirección IP correspondiente. Las máscaras wildcard 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 wildcard 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 wildcard 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 wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.



**Figura 6-21: BITS DE MASCARA WILDCARD**

Hay dos palabras clave 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 wildcard 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.

**Router(config)#access-list 1 permit 0.0.0.0 255. 255. 255. 255**

Agregar un número identificador a la acl, colocar la palabra reservada permit, la cual aceptará la condición a establecer y posteriormente el rango de direcciones a aceptar, en éste caso se acepta todas las direcciones ip's con todas sus máscaras.

Se la puede escribir como:

**Router(config)#access-list 1 permit any**

El ejemplo del párrafo anterior se lo puede resumir con la palabra reservada any, la cual es equivalente a 0.0.0.0 255.255.255.255

**Router(config)#access-list 1 permit 192.168.15.15 0.0.0.0**

Agregar un número identificador a la acl, colocar la palabra reservada permit, la cual aceptará la condición a establecer y posteriormente la dirección ip con su wildcard correspondiente, la misma que permitirá el acceso sólo a la ip específica.

Se la puede escribir como:

**Router(config)#access-list 1 permit host 192.168.15.15**

El ejemplo del párrafo anterior se lo puede resumir con la palabra reservada host, la cual es equivalente a una sola IP (192.168.15.15).

## 6.8.4. TIPOS DE ACL

### 6.8.4.1. ACL ESTÁNDAR

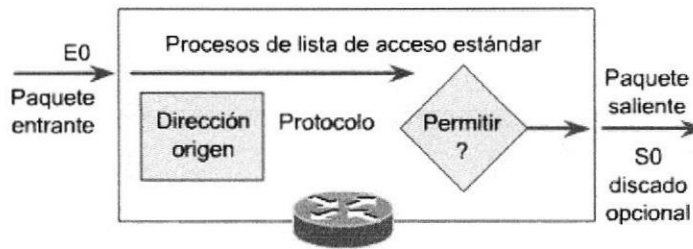


Figura 6-22: ACL ESTANDAR

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 ACL's estándar adicionales, a las cuales se les conoce como ACL's 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.

### 6.8.4.2. ACL EXTENDIDA



Figura 6-23: ACL EXTENDIDAS

Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos y números de puerto. Esto ofrece mayor flexibilidad para establecer que 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 datagrama del usuario (UDP).

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.

Número de puerto común (decimal)	Protocolo IP
20	Datos FTP
21	Programa FTP
23	Telnet
25	Protocolo simple de transferencia de correo (SMTP)
69	TFTP
53	DNS

Figura 6-24: NÚMERO DE PUERTO COMUNES DE LAS ACL EXTENDIDAS

### 6.8.5. UBICACIÓN DE UNA ACL

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.

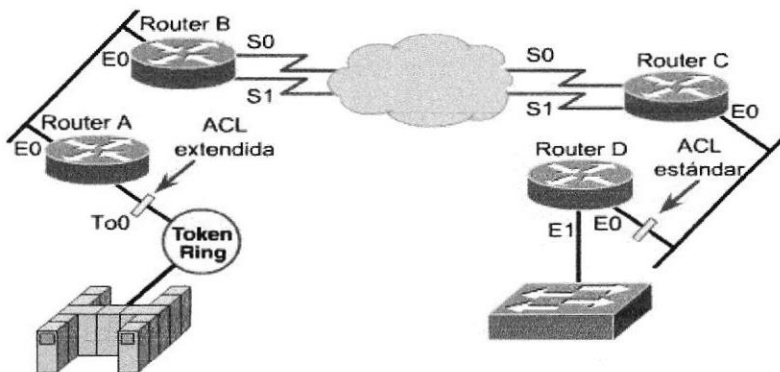


Figura 6-25: UBICACIÓN DE LAS ACL

### 6.8.6. PORQUE CREAR UNA ACL

- ✓ Brindar control de flujo de tráfico.
- ✓ Restringir el envío de las actualizaciones de enrutamiento.
- ✓ Proporcionar un nivel básico de seguridad para el acceso a la red.
- ✓ Tipos de tráfico que se envían o bloquean en las interfaces del router. Permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- ✓ Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- ✓ Analizar ciertos hosts para permitir o denegar acceso a partes de una red.
- ✓ Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

## 6.9. SWITCH

Un switch ("conmutador") es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconexión). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

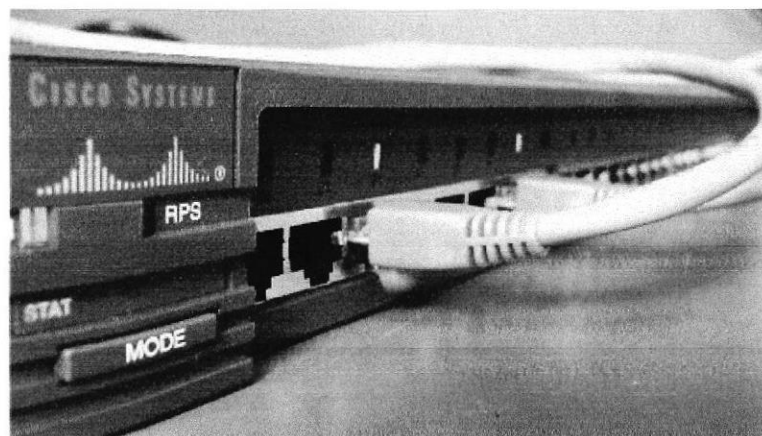


Figura 6-26: SWITCH

### 6.9.1. ENCAPSULAMIENTO

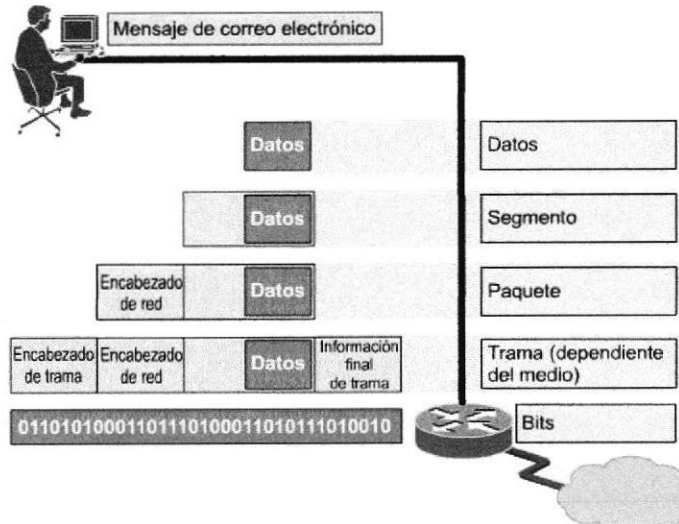


Figura 6-27: ENCAPSULAMIENTO

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión. La capa de transporte divide los datos en unidades de un tamaño que se pueda administrar, denominadas segmentos. También asigna números de secuencia a los segmentos para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego la capa de red encapsula el segmento creando un paquete.

En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física.

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino. Pero si se deben enviar los datos a otro host a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia. Esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos (el paquete).

Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet. La excepción principal a esto es un dispositivo denominado gateway. Este es un dispositivo que ha sido diseñado para convertir los datos desde un formato, creado por las capas de aplicación, presentación y sesión, en otro formato. De modo que el gateway utiliza las siete capas del modelo OSI para hacer esto.

Flujo de paquetes a través de los dispositivos de Capa 2: Es importante recordar que los paquetes se ubican dentro de tramas, de modo que para comprender la forma en que viajan los paquetes en los dispositivos de la Capa 2, es necesario trabajar con la forma en que se encapsulan los paquetes, que es la trama. Cualquier cosa que le suceda a la trama también le sucede al paquete. Las NIC, los puentes y los switches involucran el uso de la información de la dirección de enlace de datos (MAC) para dirigir las tramas. Las NIC son el lugar donde reside la dirección MAC exclusiva.

La dirección MAC se utiliza para crear la trama. Los puentes examinan la dirección MAC de las tramas entrantes. Si la trama es local (con una dirección MAC en el mismo segmento de red que el puerto de entrada del puente), entonces la trama no se envía a través del puente. Si la trama no es local (con una dirección MAC que no está en el puerto de entrada del puente), entonces se envía al segmento de red siguiente.

El puente toma una trama, la remueve, examina la dirección MAC y luego envía o no la trama, según lo que requiera la situación. El switch es como un hub con puertos individuales que actúan como puentes. El switch toma una trama de datos, la lee, examina las direcciones MAC de la Capa 2 y envía las tramas (las conmuta) a los puertos adecuados.

### 6.9.2. SEGMENTACIÓN

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina *microsegmentación*. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host. Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 de dirección MAC destino, los switches pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños. Si la LAN no se divide en segmentos, las LAN cuyo tamaño sea mayor que un grupo de trabajo pequeño se congestionarían rápidamente con tráfico y colisiones y virtualmente no ofrecerían ningún ancho de banda.

Al dividir redes de gran tamaño en unidades autónomas, los puentes y los switches ofrecen varias ventajas. Un puente, o switch, reduce el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo se envía un determinado porcentaje de tráfico. Los puentes y los switches amplían la longitud efectiva de una

LAN, permitiendo la conexión de estaciones distantes que anteriormente no estaban permitidas.

Aunque los puentes y los switches comparten los atributos más importantes, todavía existen varias diferencias entre ellos. Los switches son significativamente más veloces porque realizan la conmutación por hardware, mientras que los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda.

Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch. Estos pueden soportar densidades de puerto más altas que los puentes. Algunos switches soportan la conmutación por el método cut-through, que reduce la latencia y las demoras de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward). Por último, los switches reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

### **6.9.3. COLISIÓN**

Uno de los problemas que se puede producir, cuando dos bits se propagan al mismo tiempo en la misma red, es una colisión. En una red pequeña y de baja velocidad es posible implementar un sistema que permita que sólo dos computadores envíen mensajes, cada uno por turnos. Esto significa que ambas pueden mandar mensajes, pero sólo podría haber un bit en el sistema. El problema es que en las grandes redes hay muchos computadores conectados, cada uno de los cuales desea comunicar miles de millones de bits por segundo. Recordar que los "bits" en realidad son paquetes que contienen muchos bits.

Se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes como, por ejemplo, los repetidores, puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo. Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos.

El área dentro de la red donde los paquetes se originan y colisionan, se denomina dominio de colisión, e incluye todos los entornos de medios compartidos. Por ejemplo, un alambre puede estar conectado con otro a través de cables de conexión, transceptores, paneles de conexión, repetidores e incluso hubs. Todas estas interconexiones de la Capa 1 forman parte del dominio de colisión.

Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

Al igual que lo que ocurre con dos automóviles, que no pueden ocupar el mismo espacio, o la misma carretera, al mismo tiempo, tampoco es posible que dos señales ocupen el mismo medio simultáneamente. En general, se cree que las colisiones son malas ya que degradan el desempeño de la

red. Sin embargo, una cantidad determinada de colisiones es una función natural de un entorno de medios compartidos (es decir, un dominio de colisión) ya que una gran cantidad de computadores intentan comunicarse entre sí simultáneamente, usando el mismo cable.

Los repetidores regeneran y retemporizan los bits, pero no pueden filtrar el flujo de tráfico que pasa por ellos. Los datos (bits) que llegan a uno de los puertos del repetidor se envían a todos los demás puertos. El uso de repetidor extiende el dominio de colisión, por lo tanto, la red a ambos lados del repetidor es un dominio de colisión de mayor tamaño.

Se puede reducir el tamaño de los dominios de colisión utilizando dispositivos inteligentes de networking que pueden dividir los dominios. Los puentes, switches y routers son ejemplos de este tipo de dispositivo de networking. Este proceso se denomina segmentación.

Un puente puede eliminar el tráfico innecesario en una red con mucha actividad dividiendo la red en segmentos y filtrando el tráfico basándose en la dirección de la estación. El tráfico entre dispositivos en el mismo segmento no atraviesa el puente, y afecta otros segmentos. Esto funciona bien, siempre y cuando el tráfico entre segmentos no sea demasiado. En caso contrario, el puente se puede transformar en un cuello de botella, y de hecho puede reducir la velocidad de la comunicación.

#### 6.9.4. VLAN (REDES VIRTUALES)

Una VLAN (acrónimo de Virtual LAN, 'red de área local virtual') es una red de computadoras lógicamente independiente. Varias VLANs pueden coexistir en un único switch físico. Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente una computadora a otra ubicación: puede permanecer en la misma VLAN sin necesidad de ninguna re configuración hardware.

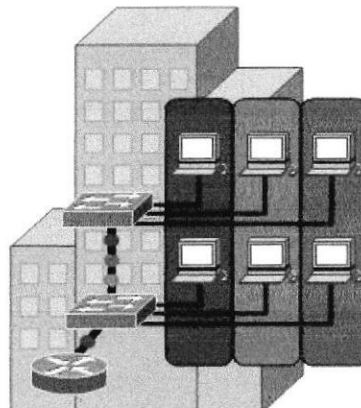


Figura 6-28: VLAN

## 6.9.5. TIPOS DE VLAN

### 6.9.5.1. VLAN DE PUERTO CENTRAL

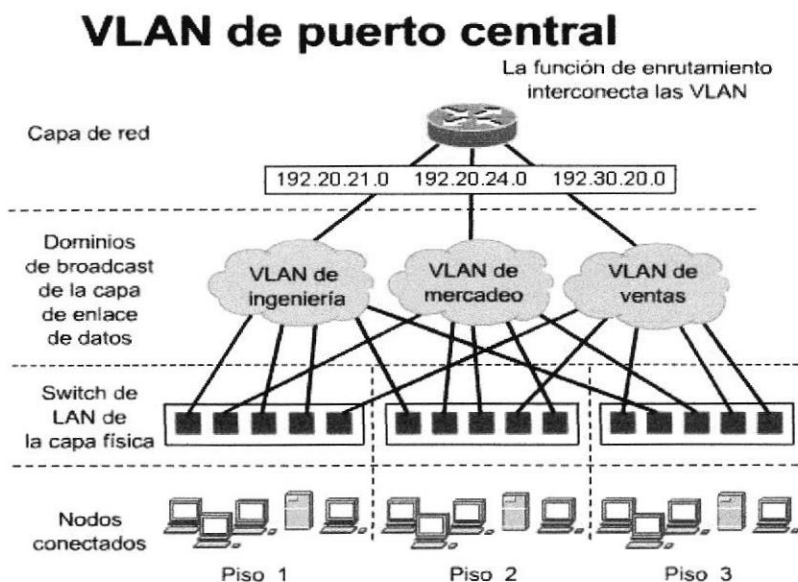


Figura 6-29: VLAN DE PUERTO CENTRAL

En las VLAN de puerto central, a todos los nodos conectados a puertos en la misma VLAN se les asigna el mismo identificador de VLAN, el gráfico muestra la pertenencia a la VLAN por puerto, lo que facilita el trabajo del administrador y hace que la red sea más eficiente porque:

- ✓ Los usuarios se asignan por puerto.
- ✓ Las VLAN son de fácil administración.
- ✓ Proporciona mayor seguridad entre las VLAN.
- ✓ Los paquetes no se "filtran" a otros dominios.

### 6.9.5.2. VLAN ESTÁTICAS



Figura 6-30: VLAN ESTÁTICAS

Las VLAN estáticas son puertos en un switch que se asignan estáticamente a una VLAN, estos puertos mantienen sus configuraciones de VLAN asignadas hasta que se cambien, aunque las VLAN estáticas requieren que el administrador haga los cambios, este tipo de red es segura, de fácil configuración y monitoreo, funcionan bien en las redes en las que el movimiento se encuentra controlado y administrado.

### 6.9.5.3. VLAN DINÁMICAS (DVLAN)



Figura 6-31: VLAN DINÁMICAS

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

### 6.9.5.4. VLAN POR PUERTO

Se configura por una cantidad "n" de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN. En esta figura tendríamos en el Switch 9 puertos de los cuales el 1,5 y 7 pertenecen a la VLAN 1, el 2, 3 y 8 a la VLAN 2 y los puertos 4, 6 y 9 a la VLAN 3 como la tabla lo indica.

**Ventajas:**

- ✓ Facilidad de movimientos y cambios.
- ✓ Micro segmentación y reducción del dominio de Broadcast.
- ✓ Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

**Desventajas:**

- ✓ Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que esta conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

**POR DIRECCIÓN MAC**

Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

**Ventajas:**

- ✓ Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la re configuración del switch.
- ✓ Multiprotocolo.
- ✓ Se pueden tener miembros en múltiples VLANs.

**Desventajas:**

- ✓ Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLANs.
- ✓ Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

**POR PROTOCOLO**

Asigna a un protocolo una VLAN. El switch se encarga de dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente.

**Ventajas:**

- ✓ Segmentación por protocolo.
- ✓ Asignación dinámica.



### Desventajas

- ✓ Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- ✓ No soporta protocolos de nivel 2 ni dinámicos.

### **POR DIRECCIONES IP**

Esta basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

#### Ventajas:

- ✓ Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el switch.

#### Desventajas:

- ✓ El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- ✓ Pérdida de tiempo en la lectura de las tablas.
- ✓ Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

### **POR NOMBRE DE USUARIO**

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

#### Ventajas:

- ✓ Facilidad de movimiento de los integrantes de la VLAN.
- ✓ Multiprotocolo.

#### Desventajas:

- ✓ En corporaciones muy dinámicas la administración de las tablas de usuarios.

## 6.10. ESTABLECER UNA SESIÓN HYPERTERMINAL

Para establecer una conexión entre la terminal y el puerto de consola de Cisco, hay que realizar dos pasos, primero conecte los dispositivos utilizando un cable transpuesto desde el puerto de consola del router hasta el puerto serial de la estación de trabajo es posible que se necesite un adaptador RJ-45-a-DB-9 o un RJ-45-a-DB-25 para la terminal o el PC, luego, configure la aplicación de emulación de terminal con los siguientes parámetros de puerto (COM) usuales para equipos. 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, y sin control de flujo.

El puerto AUX se utiliza para ofrecer administración fuera de banda a través de un módem debe ser configurado a través del puerto de consola antes de ser utilizado, el puerto AUX también utiliza los parámetros de 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, y sin control de flujo.

### ABRIR EL HYPERTERMINAL.

Entramos al HyperTerminal de la siguiente manera damos clic en **inicio**, seleccionamos **Todos los programas**, siguiente seleccionamos **Accesorios**, **Comunicaciones** y por ultimo damos clic en Hyperterminal.

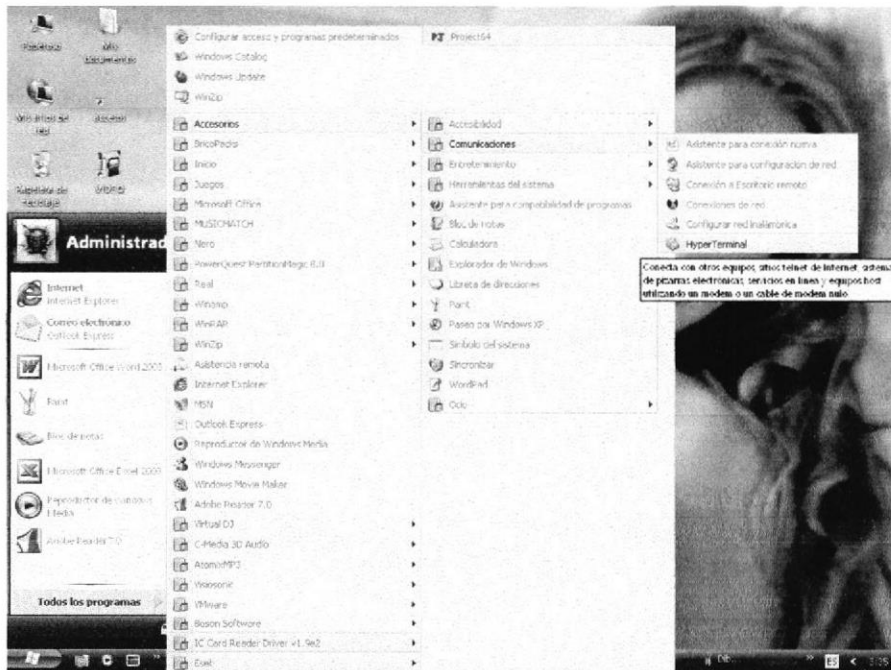


Figura 6-32: INGRESAR AL HYPERTERMINAL

Debemos dar un nombre a la conexión, para este caso le damos alessa y damos clic en **aceptar**.

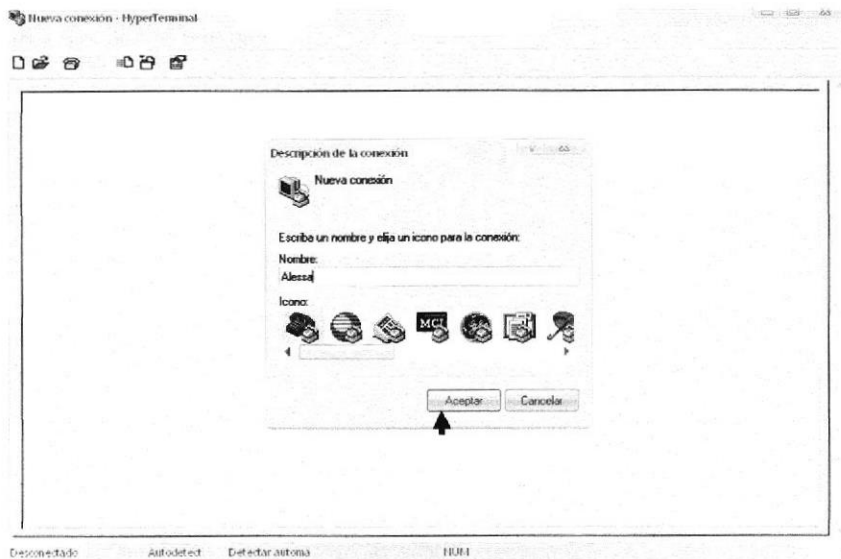


Figura 6-33: NUEVA CONEXIÓN

Elegimos el puerto **COM1** que vamos a establecer para la conexión y damos clic en **aceptar**.

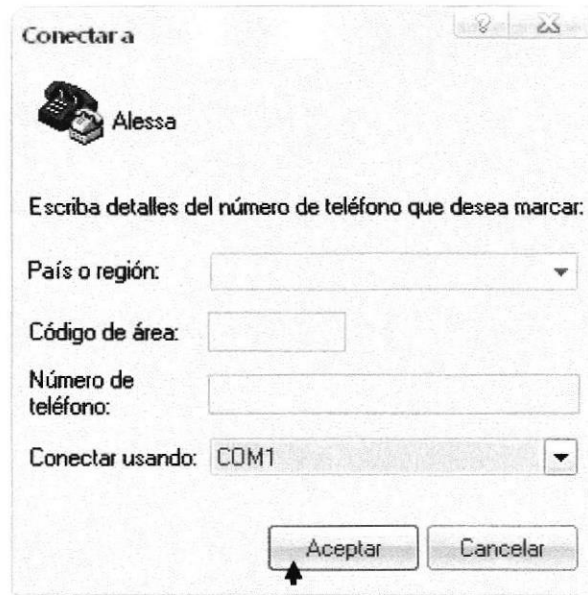


Figura 6-14: ELEGIR PUERTO COM

Configuramos el puerto con los siguientes parámetros de puerto (COM) usuales para equipos 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, y sin control de flujo y damos clic en **aceptar**.

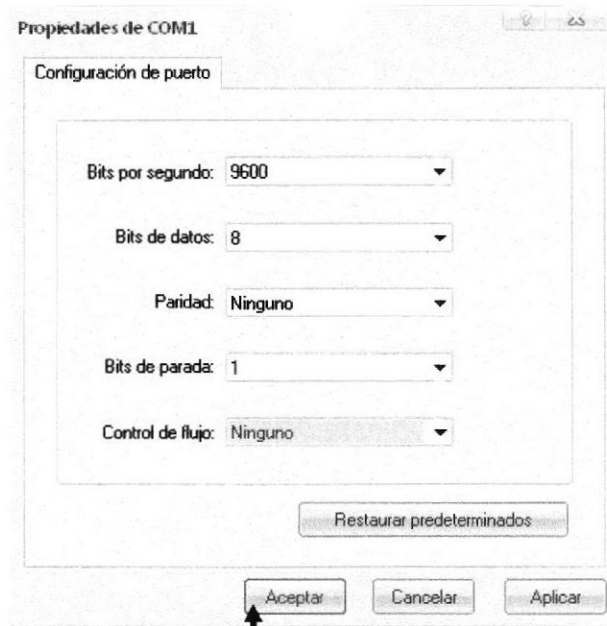


Figura 6-35: CONFIGURACIÓN DE PUERTO

### Hyperterminal

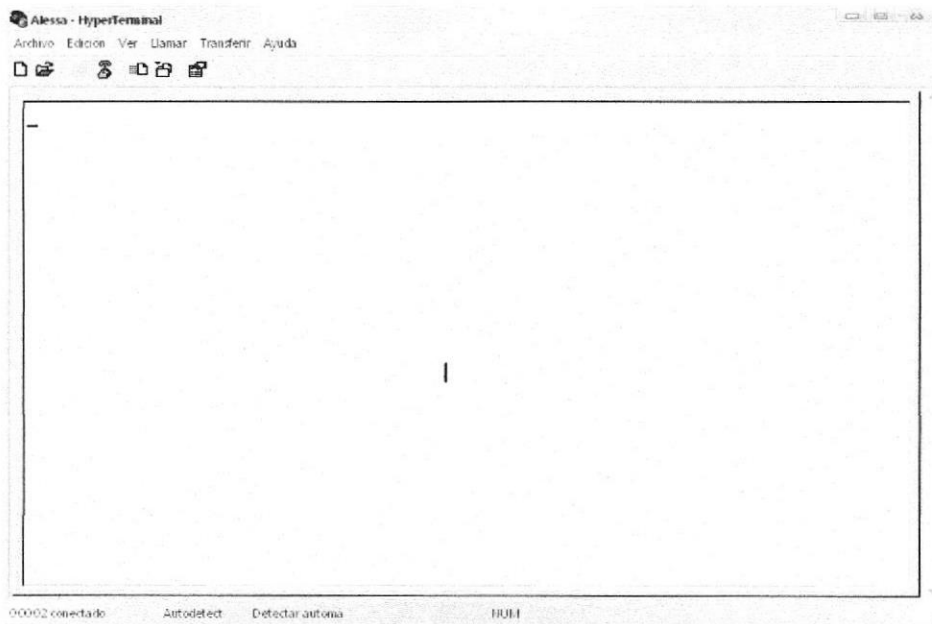
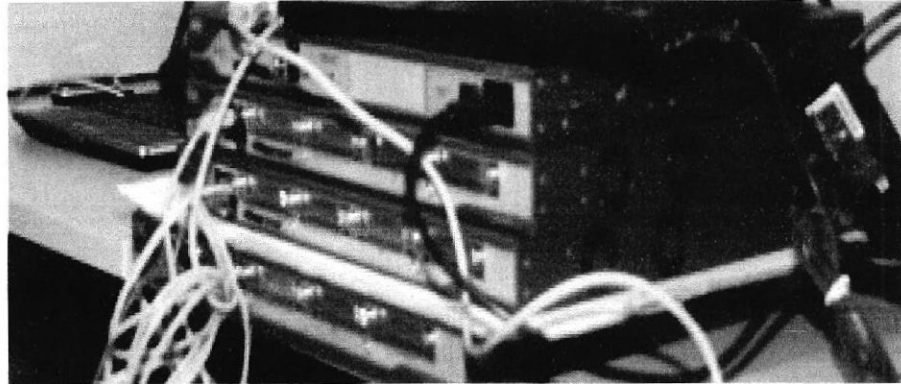


Figura 6-36: HYPERTERMINAL

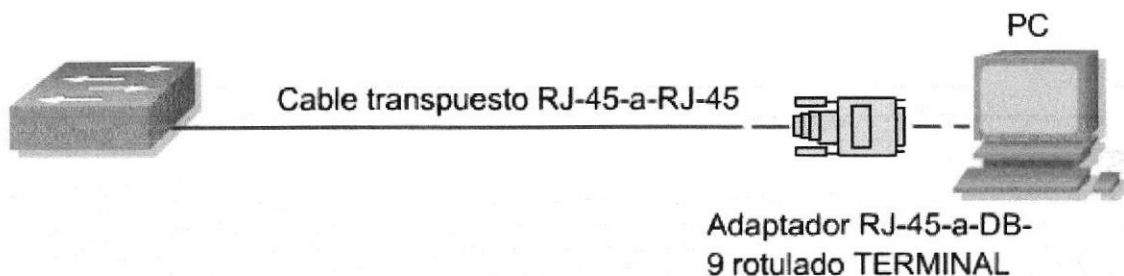
## 6.11. CONEXIONES DE LOS ROUTERS

Para empezar debemos tener conectados los routers y todos nuestros dispositivos en los cuales vamos a trabajar.



**Figura 6-37: CONEXIONES DE LOS ROUTERS**

Luego conectamos el cable en el puerto de la consola en la parte posterior del router, para comenzar la configuración.



- Los PC requieren un adaptador de RJ-45 a DB-9 o RJ-45 a DB-25.
- Las configuraciones de puerto COM son 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, sin control de flujo.
- Esto proporciona acceso de consola fuera de banda.
- El puerto de switch AUX se puede usar para una consola conectada por módem.

**Figura 6-38: PUERTO DE CONSOLA**

## 6.12.COMANDOS BÁSICOS DEL ROUTER

COMANDO	DESCRIPCIÓN
<b>Enable</b>	Comando para acceder al modo privilegiado.
<b>show history</b>	Muestra un historial de los comandos ingresados.
<b>Show version</b>	Muestra la configuración del hardware del sistema, la versión del software.
<b>Show processes</b>	Muestra información acerca de los procesos activos.
<b>Show protocols</b>	Muestra los protocolos configurados y el estado de los protocolos configurados de capa 3.
<b>Show memory</b>	Muestra estadísticas acerca de la memoria del router.
<b>Show stacks</b>	Monitorea el uso de la pila de proceso.
<b>Show buffers</b>	Suministra estadísticas sobre los grupos del búfer.
<b>Show flash</b>	Muestra información acerca de la memoria flash.
<b>show ip route</b>	Verifica la tabla de enrutamiento.
<b>show users</b>	Muestra los usuarios conectados al router.
<b>show interfaces</b>	Muestra las estadísticas completas de todas las interfaces del router.
<b>Show hosts</b>	Se utiliza para visualizar una lista de memoria cache de nombre y direcciones de host.
<b>show controllers</b>	Ver los enlaces DCE/DTE que usa el router.
<b>Show running-config</b>	Muestra el archivo de configuración activo.
<b>Show startup-config</b>	Muestra la copia de respaldo del archivo de configuración.
<b>Configure terminal</b>	Realiza la configuración desde el terminal de consola de forma manual.
<b>Configure memory</b>	Carga la información desde la NVRAM.
<b>Copy running-config startup-config</b>	Almacena la configuración actual desde la RAM a la NVRAM.
<b>Erase startup-config</b>	Borra el contenido de la NVRAM.
<b>Bandwidth</b>	Permite reemplazar el ancho de banda por defecto.
<b>clock rate</b>	Fija la velocidad de sincronización.
<b>Line console 0</b>	Establece una contraseña en la terminal de consola.

<b>Line vty 0 4</b>	Establece protección mediante contraseña en las sesiones Telnet entrantes.
<b>Enable password</b>	Restringe el acceso al modo EXEC privilegiado.
<b>Enable secret</b>	utiliza un proceso de cifrado propietario de Cisco para modificar la cadena de caracteres de la contraseña.
<b>ping</b>	Se utiliza para determinar si un computador esta conectado correctamente a los dispositivos o a Internet.
<b>tracert</b>	Rastrea la ruta que toma un paquete hacia el destino y se utiliza para depurar problemas de enrutamiento.
<b>ip address</b>	Para establecer la dirección lógica de una interfaz.
<b>ip host</b>	Asigna en forma estatica un nombre de host a una direccion ip.
<b>login</b>	Habilita la opción de introducir un usuario.

Tabla 6-1: COMANDOS BÁSICOS DEL ROUTER

### 6.13. MODOS DEL ROUTER

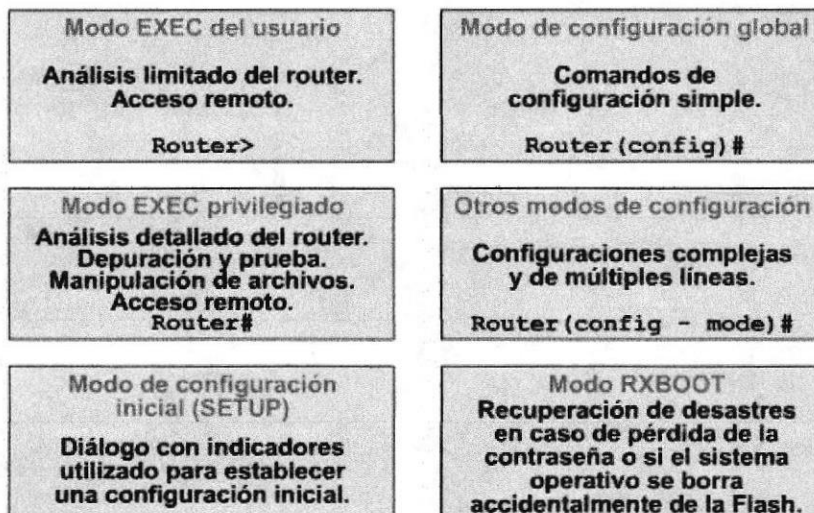


Figura 6-39: MODOS DEL ROUTER

Para configurar los routers de Cisco, debe acceder a la interfaz de usuario en el router con una terminal o acceder al router de forma remota, al acceder al router, debe conectarse al router antes de introducir cualquier otro comando.

Por razones de seguridad, el router tiene dos niveles de acceso a los comandos:

#### 6.13.1. MODO USUARIO

parámetros de configuración del router, sin embargo, no puede hacer algún cambio a la configuración del router.

Al modo usuario se accede automáticamente al conectarse al router.

**Router>**

### 6.13.2.MODO PRIVILEGIADO

Este modo se lo indica ‘#’ al lado del nombre del router, conocido como el modo habilitado, permite examinar mayormente al router y proporciona un conjunto más robusto de comandos que el modo usuario.

Después de que usted entra en el Modo privilegiado, debe ingresar el comando **enable** para ingresar al modo privilegiado que tiene permisos para poder modificar configuraciones y guardar los cambios.

**Router>**

**Router>enable**

**Router#**

Para desconectarse del router, escriba **exit** (salir).

```

Resultados de comandos
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router> ←————— Indicador de modo usuario
Router> enable
Password:
Router# ←————— Indicador de modo privilegiado
Router# disable
Router>
Router> exit
  
```

Figura 6-40: MODOS DEL USUARIO – MODO PRIVILEGIADO

### 6.13.3.MODO DE CONFIGURACIÓN INICIAL (SETUP)

Presenta en la consola un diálogo interactivo basado en indicadores que ayuda al nuevo usuario a crear una configuración básica inicial.

### 6.13.4.MODO DE CONFIGURACIÓN GLOBAL

Implementa poderosos comandos de una línea que ejecutan tareas simples de configuración. Otros modos de configuración: Permiten configuraciones más detalladas de múltiples líneas.



### 6.13.5.MODO RXBOOT

Modo de mantenimiento lo puede usar, entre otras cosas, para recuperar contraseñas perdidas.

### 6.13.6.DESCRIPCIÓN GENERAL DE LOS MODOS DEL ROUTER

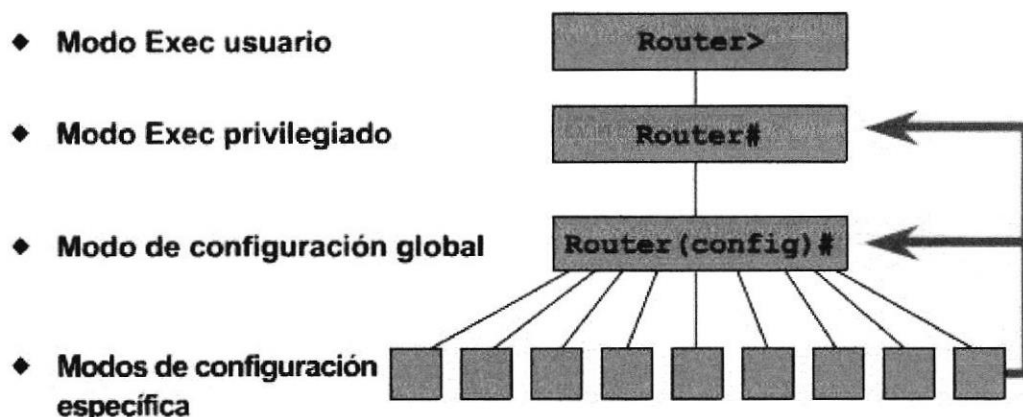


Figura 6-41: DESCRIPCIÓN GENERAL DE LOS MODOS DEL ROUTER

## 6.14.CONFIGURACIONES GENERAL DE UN ROUTER

### MODOS DE CONFIGURACIÓN DEL ROUTER

Al arrancar el router puede pasar al modo SETUP, que le permite dar una primera configuración al router cuando éste carece de una configuración preestablecida, o bien pasar al modo USER EXEC, cuando el router sí dispone de una configuración preestablecida.

En modo USER EXEC puede consultar aspectos básicos de la configuración del router. Para consultar aspectos más críticos de la configuración del router debe pasar a modo PRIVILEGED EXEC. Para pasar de modo USER EXEC a modo PRIVILEGED EXEC es necesario que digite el comando “enable”.

Desde los modos USER EXEC y PRIVILEGED EXEC no puede modificar la configuración del router. Para hacerlo debe pasar del modo PRIVILEGED EXEC al modo de configuración global (CONFIGURE TERMINAL). Desde allí puede configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc. y para salir de estos modos de configuración lo hace con el comando “Ext.”

Cuando esta en modo USER EXEC el prompt que le muestra el router es “>”. Cuando esta en PRIVILEGED EXEC el prompt es “#” y en el modo de configuración global el prompt es (config)#,

```
Router>
Router> enable
Router#
Router# exit
Router>
```

### 6.14.1.MODO DE CONFIGURACIÓN GLOBAL

Permite configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc (prompt R(config)#).

```
Router>
Router> enable
Router# configure terminal
Router(config)#exit
Router#
```

### 6.14.2.GUARDAR CAMBIOS EN EL ROUTER

Los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en la RAM del router llamado "running-config", este fichero lo puede visualizado desde el modo de configuración privilegiado con el comando "show running-config", si el router se apagase, estos cambios se perderían al estar almacenados en RAM.

Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM debe copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM), ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

```
Router# copy running-config startup-config
```

### 6.14.3.ASIGNAR NOMBRE AL ROUTER "HOSTNAME"

Para configurar el nombre del router debe hacer en el modo de configuración global con el comando "**hostname**" <nombre > una vez ingresado el nombre salga del modo de configuración global con el comando "**Ext.**"

```
Router>
Router> enable
Router# configure terminal
Router(config)#hostname MATRIZ
MATRIZ(config)#exit
MATRIZ#
```

#### 6.14.4. ASIGNAR CONTRASEÑA “PASSWORD”

El router posee niveles de seguridad para que solo los administradores puedan configurar dichos dispositivos, existen dos formas de colocar password en el router.

**Usuario no privilegiado:** De modo USER EXEC con el comando “**line console 0**” este designa la conexión de consola del router el **0** que le indica que asigna al usuario no privilegiado, seguido respectivo “**password**”<nombre del password> que establece una contraseña e ingrese nueva contraseña para este caso **topico** y siga con “**login**” .

**Usuario privilegiado:** De modo PRIVILEGED EXEC con el comando “**line vty 0 4**” este designa la conexión de consola del router el **0 4** le indica que asigne al usuario privilegiado y la configuración del servicio telnet, seguido respectivo “**password**”<nombre del password> que establece una contraseña e ingrese nuestra contraseña para este caso **topico** y siga con “**login**” .

```
MATRIZ(config)#
MATRIZ(config)#line console 0
MATRIZ(config-line)#password topico
MATRIZ(config-line)#LOGIN
MATRIZ(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

Cuando ha completado la configuración, presionamos ctrl.+z, esto guardara sus cambios en el router.

```
MATRIZ(config)#line vty 0 4
MATRIZ(config-line)#password topico
MATRIZ(config-line)#login
MATRIZ(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

#### 6.14.5. CONFIGURACIÓN DE INTERFACES

Desde el modo de configuración puede pasar a configurar los interfaces, por ejemplo, para configurar una interfase puede hacer:

```
Router# configure terminal
Router(config)# interface <eth0 ó serial0>
Router(config-if)# ip address <dirección IP y la mascara de sub red>
Router(config-if)# no shutdown
Router(config-if)# exit
Router#
```

El comando “**no shutdown**” es necesario para que active la interfaz, por defecto, al arrancar el router todos los interfaces están desactivados, el comando “**shutdown**” en su defecto desactivaría administrativamente una interfaz.

Las interfaces serial están diseñadas para que en la situación más normal se conecten a una operadora de telecomunicaciones a través de un DCE  
El DCE es el que normalmente da reloj y por tanto fija la velocidad de modulación y por consiguiente de transmisión.

Si se conectan dos puertos serie de router (DTE-DTE) hay que usar un cable cruzado, a demás uno de los dos puertos tiene que actuar como DCE dando reloj, en principio desde el punto de vista de router cualquiera de los dos puede actuar de DCE, así que lo importante es que conector del cable es el que marca que puerto es DCE.

#### 6.14.5.1. INTERFACES SERIALES / ETHERNET

**Serial 0:** Una vez que sabe que puerto es el que actúa de DCE, tiene que dar reloj, está opción la tiene que activar vía IOS con el comando "**clockrate Bw**", donde **Bw** son los bps a los que quiere que trabaje la línea.

**La serial 0** del router matriz es el actúa como DCE fijando una velocidad de transmisión de 56 Kbps.

```
MATRIZ#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MATRIZ(config)#interface s 0
MATRIZ(config-if)#ip address 192.168.12.5 255.255.255.252
MATRIZ(config-if)#clock rate 56000
MATRIZ(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
MATRIZ(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console#
MATRIZ#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

**Serial 1:** Una vez que sabe que puerto es el que actúa de DTE realice las configuraciones déle una dirección IP y la mascara de subred y levantando la interfaz.

```
MATRIZ#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MATRIZ(config)#interface s 1
MATRIZ(config-if)#ip address 192.168.11.6 255.255.255.252
MATRIZ(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial1, changed state to up
%LINK-3-UPDOWN: Interface Serial1, changed state to down
MATRIZ(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

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

**Ethernet 0**

```

MATRIZ#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MATRIZ(config)#interface ethernet 0
MATRIZ(config-if)#ip address 192.168.16.1 255.255.255.192
MATRIZ(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
MATRIZ(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

%LINK-3-UPDOWN: Interface Ethernet0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to
down
MATRIZ#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

**6.14.6.OSPF**

Los protocolos de estado del enlace conocen los routers distantes y cómo se Interconectan.

**Características:**

- ✓ Usa la ruta mas corta
- ✓ Las actualizaciones son por eventos
- ✓ Tiene una vista común de la red
- ✓ Consume menos ancho de banda
- ✓ Converge rápidamente
- ✓ No susceptible a bucles de enrutamiento
- ✓ Requiere mas potencia y memoria

Para configurar este protocolo de enrutamiento, primero debe cambiarse al modo de configuración global, luego establecer el protocolo con el comando “**router ospf area**” luego debe establecer con una o más órdenes “**network**”, las redes directamente conectadas al router, seguido de la mascara wilcard y el área, finalmente salga con el comando “**exit**” A continuacion va a observar la configuración del router MATRIZ con el protocolo ospf.

```

MATRIZ#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MATRIZ(config)#rout
MATRIZ(config)#router ospf 1
MATRIZ(config-router)#network 192.168.11.4 0.0.0.3 area 0
MATRIZ(config-router)#network 192.168.10.4 0.0.0.3 area 0

```

```
MATRIZ(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

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

### 6.14.7. REDISTRIBUCIÓN DE RUTAS

Es posible tener zonas que usan protocolos de encaminamiento distintos, por ejemplo OSPF y RIPv2. Hay que inyectar las rutas que se aprenden de un protocolo a otro, a este proceso se la llama “redistribución de rutas” Lo lógico es que en una red corra un único protocolo de encaminamiento, pero imaginar que se unen dos redes con protocolos distintos y tienen que convivir (pueden incluso estar administrados por distintos departamentos).

El punto más importante es que las métricas de los protocolos son distintas, RIPv2 usa saltos (“hops”) y OSPF usa “bandwidth” OSPF su métrica es bandwidth y usa costes con la fórmula  $108, \text{bandwidth (bps)}$ . OSPF pone como coste igual a 20 por defecto al protocolo redistribuido (excepto BGP que le pone coste igual a 1), Como anuncia redes principales hay que añadir el parámetro subset para indicar que la red está subneteada. RIPv2 como la métrica son los saltos se recomienda usar como métrica por defecto un valor bajo (1salto)

Para poder establecer comunicación entre dos protocolos distintos se debe utilizar el comando “**redistribute <protocol>**” esta línea debe ir dentro de la configuración del protocolo.

## 6.15. CASO DE ESTUDIO

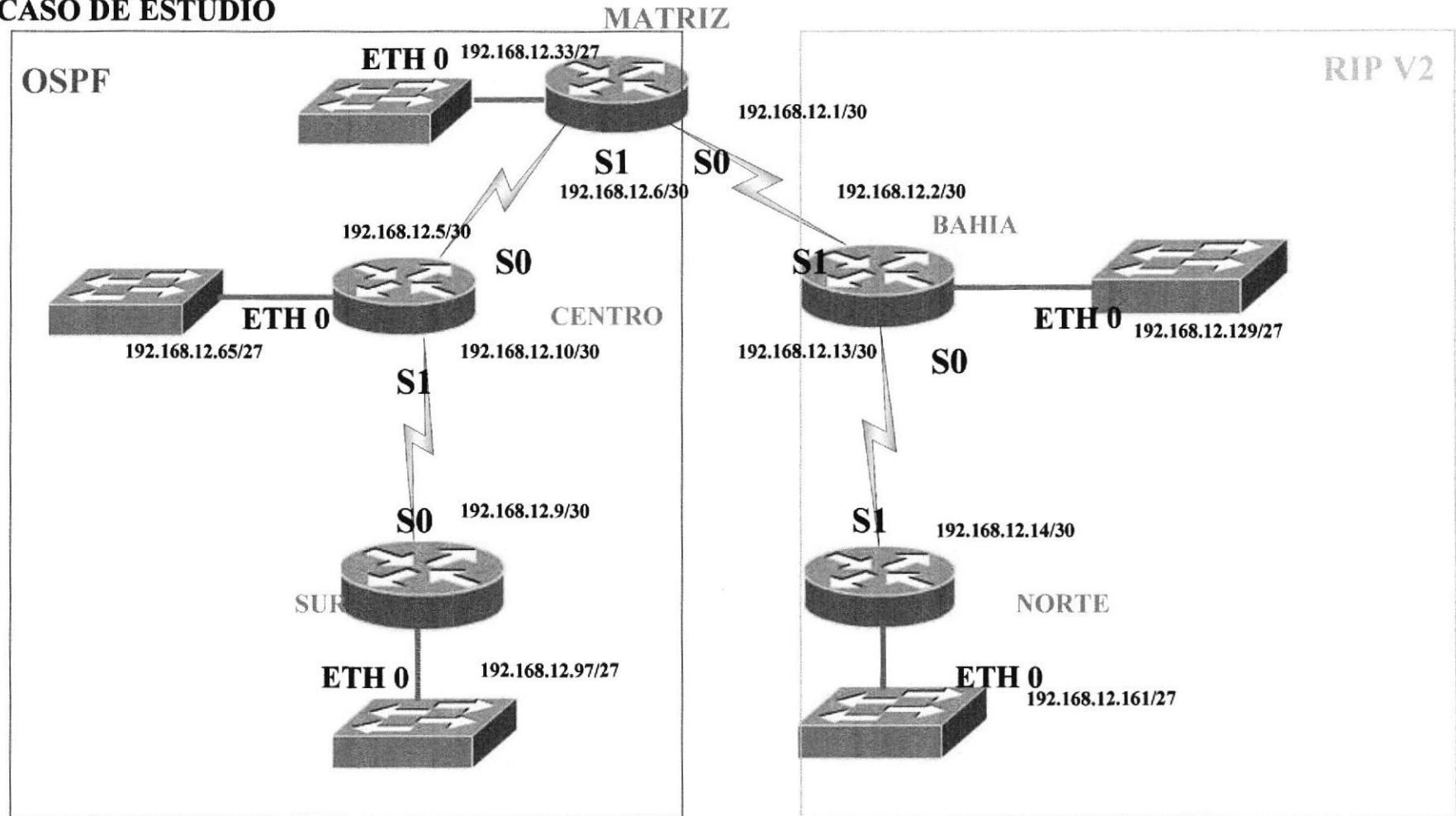


Figura 6-42: CASO DE ESTUDIO

## 6.16.CONFIGURACIÓN DE ROUTER DE LOS ALMACENES ESTUARDO SÁNCHEZ

### 6.16.1.ROUTER MATRIZ

#### 6.16.1.1.ASIGNAR NOMBRE AL ROUTER

**Esta en el modo usuario.**

Router>

**El comando enable le permite ingresar al modo privilegiado.**

Router> enable

**Ahora ingrese a configuración global con el comando configure terminal.**

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ahora asigne el nombre al router para este caso MATRIZ después del comando hostame.**

Router(config)#hostname MATRIZ

**Observe como cambio el nombre al router.**

MATRIZ(config)#

#### 6.16.1.2.ASIGNAR CONTRASEÑA

COSOLA DEL ROUTER

MATRIZ(config)#

**Ingrese el comando line console 0.**

MATRIZ(config)#line console 0

**Ingrese el comando password para asignar la contraseña.**

MATRIZ(config-line)#password topico

**Ahora ingrese el comando login.**

MATRIZ(config-line)#LOGIN

TERMINAL VIRTUAL DEL ROUTER

**Ingrese el comando line vty 0 4.**

MATRIZ(config)#line vty 0 4

**Ingrese el comando password para asignar la contraseña.**

MATRIZ(config-line)#password topico

**Ahora ingrese el comando login.**

MATRIZ(config-line)#login



### 6.16.1.3. ASIGNAR DIRECCIÓN IP AL ROUTER

#### 6.16.1.3.1. ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0

**Esta en el modo de configuración global.**

MATRIZ#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interfase S 0 para que configure dicha interfaz.**

MATRIZ(config)#interface s 0

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

MATRIZ(config-if)#ip address 192.168.12.1 255.255.255.252

**Con el comando clock rate fije la velocidad de sincronización del router.**

MATRIZ(config-if)#clock rate 56000

**Este comando le permite levantar la interfaz.**

MATRIZ(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Serial0, changed state to up

MATRIZ(config-if)#^Z

%SYS-5-CONFIG\_I: Configured from console by console#

**Este comando le permite guardar los cambios.**

MATRIZ#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

#### 6.16.1.3.2. ASIGNAR DIRECCIÓN IP INTERFAZ SERIAL 1

**Esta en el modo de configuración global.**

MATRIZ#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interfase S 1 para configurar dicha interfaz.**

MATRIZ(config)#interface s 1

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

MATRIZ(config-if)#ip address 192.168.12.6 255.255.255.252

**Este comando le permite levantar la interfaz.**

MATRIZ(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Serial1, changed state to up

MATRIZ(config-if)#^Z

%SYS-5-CONFIG\_I: Configured from console by console#

**Este comando le permite guardar los cambios.**

MATRIZ#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

### 6.16.1.3.3. ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET

**Esta en el modo de configuración global.**

MATRIZ#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interfaces ethernet 0 para configurar dicha interfaz.**

MATRIZ(config)#interface ethernet 0

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

MATRIZ(config-if)#ip address 192.168.12.33 255.255.255.192

**Este comando le permite levantar la interfaz.**

MATRIZ(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Ethernet0, changed state to up

MATRIZ(config-if)#^Z

%SYS-5-CONFIG\_I: Configured from console by console#

**Este comando le permite guardar los cambios.**

MATRIZ#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

### 6.16.1.4. DECLARAR EL PROTOCOLO OSPF

**Esta en el modo de configuración global.**

MATRIZ#configure terminal

**Este comando le permite declarar el protocolo OSPF.**

MATRIZ(config)#router ospf 1

**Declare todos los segmentos de las redes que estén directamente conectadas al Router con la willcard respectivamente y el área.**

MATRIZ(config-router)#network 192.168.12.0 0.0.0.3 area 0

MATRIZ(config-router)#network 192.168.12.32 0.0.0.31 area 0

MATRIZ(config-router)#network 192.168.12.4 0.0.0.3 area 0

**Este comando le permite hacer la redistribución en el router MATRIZ.**

MATRIZ(config-router)#redistribute rip

**Este comando le permite guardar los cambios.**

MATRIZ#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

### 6.16.1.5. ENRUTAMIENTO DE VLAN 10

**Este comando le permite declarar las sub-interfaces del router.**

MATRIZ(config)# interface fastethernet 0.1

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

MATRIZ(config-subif)# ip address 192.168.12.193 255.255.255.248

**Este comando le permite realizar el encapsulamiento de la vlan.**

MATRIZ(config-subif)# encapsulation dot1q 10  
**Este comando le permite levantar la sub-interfaces del router.**  
 MATRIZ(config-subif)# no shutdown

### 6.16.1.6. ENRUTAMIENTO DE LA VLAN 20

**Este comando le permite declarar las sub-interfaces del router.**  
 MATRIZ(config)# interface fastethernet 0.2  
**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**  
 MATRIZ(config-subif)# ip address 192.168.12.201 255.255.255.248  
**Este comando le permite realizar el encapsulamiento de la vlan.**  
 MATRIZ(config-subif)# encapsulation dot1q 20  
**Este comando le permite levantar la sub-interfaces del router.**  
 MATRIZ(config-subif)# no shutdown

### 6.16.1.7. SHOW RUN

```

MATRIZ#sh run
Building configuration...

!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname MATRIZ
!
!
!
ip subnet-zero
!
!
!
!
!
!
!
!
!
!
interface Serial0
ip address 192.168.12.1 255.255.255.252
no ip directed-broadcast
clock rate 56000
bandwidth 1544

```

**Version Del IOS**

**Nombre del router**

**IP asignada por el Administrador**

```

!
interface Serial1
ip address 192.168.12.6 255.255.255.252      IP asignada por el Administrador
no ip directed-broadcast
bandwidth 1544
!
interface Ethernet0
ip address 192.168.12.33 255.255.255.224   IP asignada por el Administrador
no ip directed-broadcast
bandwidth 10000
ip ospf cost 100
!
interface Ethernet0.1
encapsulation dot1q 10
ip address 192.168.12.193 255.255.255.248 IP asignada por el Administrador
!
interface Ethernet0.2
encapsulation dot1q 20
ip address 192.168.12.201 255.255.255.248 IP asignada por el Administrador
!
!
router rip                                  Protocolo rip

version 2
redistribute OSPF 1                         Redistribución OSPF
network 192.168.12.0
!
router ospf 1                               Protocolo OSPF
redistribute RIP                            Redistribución rip
network 192.168.12.0 0.0.0.3 area 0
network 192.168.12.32 0.0.0.31 area 0
network 192.168.12.4 0.0.0.3 area 0
!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

MATRIZ#

```

**6.16.1.8.SHOW IP ROUTE**

**C** Conectado.  
**S.** Estático.  
**I.** Protocolo IGRP.  
**R** Protocolo Rip.  
**B** Protocolo BGP.  
**D** Protocolo EIGRP.  
**EX** Protocolo EIGRP externo.  
**O** Protocolo OSPF.

**IA** El número de las rutas recibidas de otras áreas del OSPF.

**E1** Rutas recibidas de otras áreas del OSPF tipo externo 1.

**E2** Rutas recibidas de otras áreas del OSPF tipo externo 2.

**I** Son las rutas recibidas de los anuncios del protocolo del IS-IS.

<b>C</b>	192.168.12.32/27 is directly connected,	Ethernet0
<b>Conectada directamente</b>	<b>Red con la que se conecta</b>	<b>Interfaz</b>

**O**

**Protocolo OSPF**

192.168.12.64/27

**Red aprendida ospf**

Via [110/64]

**Distancia administrativa y ancho de banda**

192.168.12.65

**Ip asignada a la interfaz**

Ethernet0

**Interfaz**

**R**

**Protocolo OSPF**

192.168.12.128/27

**Red aprendida RIP**

[120/1] via

**Distancia administrativa y ancho de banda**

192.168.12.2

**Ip asignada a la interfaz**

Serial0

**Interfaz**

MATRIZ#sh 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

192.168.12.0/0 is variably subnetted, 9 subnets

C 192.168.12.32/27 is directly connected, Ethernet0  
 C 192.168.12.4/30 is directly connected, Serial1  
 O 192.168.12.64/27 [110/64] via 192.168.12.65, 00:57:46, Ethernet0  
 O 192.168.12.8/30 [110/64] via 192.168.12.10, 00:57:36, Ethernet0  
 C 192.168.12.0/30 is directly connected, Serial0  
 R 192.168.12.128/27 [120/1] via 192.168.12.2, 00:04:19, Serial0  
 R 192.168.12.12/30 [120/1] via 192.168.12.2, 00:04:17, Serial0  
 R 192.168.12.160/27 [120/2] via 192.168.12.2, 00:06:15, Serial0  
 O 192.168.12.96/27 [110/192] via 192.168.12.5, 00:40:42, Ethernet0

### 6.16.1.9.SHOW INTERFACES

MATRIZ#show interfaces

Serial0 is up, line protocol is up

Hardware is HD64570

Internet address is 192.168.12.1/30

MTU 1500 bytes, BW 1544 Kbit, 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
Serial1 is up, line protocol is up
Hardware is HD64570
Internet address is 192.168.12.6/30
MTU 1500 bytes, BW 1544 Kbit, 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
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 000C.3782.8690 (bia 000C.3782.8690)
Internet address is 192.168.12.33/27
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
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
Ethernet0.1 is down, line protocol is down
```

```

Hardware is AmdFE, address is 000C.3782.8691 (bia 000C.3782.8691)
Internet address is 192.168.12.193/29
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Ethernet0.2 is down, line protocol is down
Hardware is AmdFE, address is 000C.3782.8691 (bia 000C.3782.8691)
Internet address is 192.168.12.201/29
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00

```

MATRIZ#

### 6.16.1.10. SWITCH MATRIZ

**Este comando le permite crear una vlan.**

```
Switch#vlan database
```

**Este comando le asigna un nombre a la vlan**

```
Switch(vlan)#vlan 10 name sistemas
```

```
VLAN 10 added:
```

```
  Name:sistemas
```

```
Switch(vlan)#vlan 20 name contabilidad
```

```
VLAN 20 added:
```

```
  Name:contabilidad
```

### 6.16.1.11. CREACIÓN DE UNA VLAN

**Ingrese al modo de configuración global.**

```
Switch#conf ter
```

Enter configuration commands, one per line. End with CNTL/Z.

**Con este comando ingresamos a la interfaz del switch.**

```
S_MATRIZ(config)#interface fastethernet 0/1
```

**Este comando le permite crear el Puerto truncado.**

```
S_MATRIZ(config-if)#switchport mode trunk
```

**Este comando le permite asignar a la vlan una o varias interfaces.**

```
S_MATRIZ(config-if)#switchport access vlan 10
```

**Con este comando ingrese a la interfaz del switch.**

```
S_MATRIZ(config-if)#interface fastethernet 0/2
```

**Con este comando asigne la vlan a una o varias interfaces.**

```
S_MATRIZ(config-if)#switchport access vlan 10
```

**Con este comando ingrese a la interfaz del switch.**

```
S_MATRIZ(config-if)#interface fastethernet 0/3
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_MATRIZ(config-if)#switchport access vlan 20
```

**6.16.1.12. SHOW VLAN**

<b>VLAN</b>	Es el numero de la vlan.
<b>Name</b>	Es el nombre asignado a la vlan.
<b>Status</b>	Es el estado en que se encuentra la vlan.
<b>Ports</b>	Son los puertos asignados a la vlan.

S\_MATRIZ#sh vlan

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12
10 sistemas	active	Fa0/1, Fa0/2
20 contabilidad	active	Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	-	0	0
10 enet	100010	1500	-	-	-	-	-	0	0
20 enet	100020	1500	-	-	-	-	-	0	0
1002 fddi	101002	1500	-	-	-	-	-	0	0
1003 tr	101003	1500	-	-	-	-	-	0	0
1004 fdnet	101004	1500	-	-	-	ieee	-	0	0
1005 trnet	101005	1500	-	-	-	ibm	-	0	0

**6.16.1.13. SHOW INTERFACES**

S\_MATRIZ#sh interfaces

Vlan 1 is administratively down, line protocol is down  
 Hardware is CPU Interface, address is 000C.2487.827-1 (bia 000C.2487.827-1)  
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is up, line protocol is up  
Hardware is Fast Ethernet, address is 000C.2487.8270 (bia 000C.2487.8270)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/2 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.2532.2354 (bia 000C.2532.2354)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/3 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.2750.5910 (bia 000C.2750.5910)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/4 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.7574.4587 (bia 000C.7574.4587)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/5 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.9220.3246 (bia 000C.9220.3246)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec  
 5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/6 is down, line protocol is down  
 Hardware is Fast Ethernet, address is 000C.3582.9773 (bia 000C.3582.9773)  
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec  
 5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/7 is down, line protocol is down  
 Hardware is Fast Ethernet, address is 000C.7288.6416 (bia 000C.7288.6416)  
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec



5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/8 is down, line protocol is down  
 Hardware is Fast Ethernet, address is 000C.4198.6794 (bia 000C.4198.6794)  
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec  
 5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/9 is down, line protocol is down  
 Hardware is Fast Ethernet, address is 000C.3869.1988 (bia 000C.3869.1988)  
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec  
 5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/10 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.9785.6374 (bia 000C.9785.6374)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.3357.2095 (bia 000C.3357.2095)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/12 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.7004.6342 (bia 000C.7004.6342)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec  
 5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

## 6.16.2. ROUTER CENTRO

### 6.16.2.1. ASIGNAR NOMBRE AL ROUTER

**Esta en el modo usuario.**

Router>

**El comando enable le permite ingresar al modo privilegiado.**

Router> enable

**Ahora ingrese a configuración global con el comando configure terminal.**

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ahora asígnele el nombre al router para este caso CENTRO después del comando hostame.**

Router(config)#hostname CENTRO

**Observe como cambio el nombre al router.**

CENTRO(config)#

### 6.16.2.2. ASIGNAR CONTRASEÑA

COSOLA DEL ROUTER

CENTRO(config)#

**Ingrese el comando line console 0.**

CENTRO(config)#line console 0

**Ingrese el comando password para asignar la contraseña.**

CENTRO(config)#password topico

**Ahora ingrese el comando login.**

CENTRO(config-line)#LOGIN

TERMINAL VIRTUAL DEL ROUTER

**Ingrese el comando line vty 0 4.**

CENTRO(config)#line vty 0 4

**Ingrese el comando password para asignar la contraseña.**

```
CENTRO(config-line)#password topico
Ahora ingrese el commando login.
CENTRO(config-line)#login
```

### 6.16.2.3. ASIGNAR DIRECCIÓN IP AL ROUTER

#### 6.16.2.3.1. ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0

**Esta en el modo de configuración global.**

```
CENTRO#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface S 0 para configurar dicha interfaz.**

```
CENTRO(config)#interface s 0
```

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

```
CENTRO(config-if)#ip address 192.168.12.5 255.255.255.252
```

**Con el comando clock rate fije la velocidad de sincronización del router.**

```
CENTRO(config-if)#clock rate 56000
```

**Este comando le permite levantar la interfaz.**

```
CENTRO(config-if)#no shutdown
```

```
%LINK-3-UPDOWN: Interface Serial0, changed state to up
```

```
CENTRO(config-if)#^Z
```

```
%SYS-5-CONFIG_I: Configured from console by console#
```

**Este comando le permite guardar los cambios.**

```
CENTRO#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

#### 6.16.2.3.2. ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 1

**Esta en el modo de configuración global.**

```
CENTRO#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface S1 para configurar dicha interfaz.**

```
CENTRO(config)#interface s 1
```

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

```
CENTRO(config-if)#ip address 192.168.12.10 255.255.255.252
```

**Este comando le permite levantar la interfaz.**

```
CENTRO(config-if)#no shutdown
```

```
%LINK-3-UPDOWN: Interface Serial1, changed state to up
```

```
CENTRO(config-if)#^Z
```

```
%SYS-5-CONFIG_I: Configured from console by console#
```

**Este comando le permite guardar los cambios.**

```
CENTRO#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

### 6.16.2.3.3. ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET

**Esta en el modo de configuración global.**

```
CENTRO#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface ethernet 0 para configurar dicha interfaz.**

```
CENTRO(config)#interface ethernet 0
```

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

```
CENTRO(config-if)#ip address 192.168.12.65 255.255.255.224
```

**Este comando le permite levantar la interfaz.**

```
CENTRO(config-if)#no shutdown
```

```
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
```

```
CENTRO(config-if)#^Z
```

```
%SYS-5-CONFIG_1: Configured from console by console#
```

**Este comando le permite guardar los cambios.**

```
CENTRO#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

### DECLARAR EL PROTOCOLO OSPF

**Esta en el modo de configuración global.**

```
CENTRO#configure terminal
```

**Este comando le permite declarar el protocolo OSPF.**

```
CENTRO(config)#router ospf 1
```

**Declare todos los segmentos de las redes que estén directamente conectadas al router con la willcard respectivamente y el área.**

```
CENTRO(config-router)#network 192.168.12.8 0.0.0.3 area 0
```

```
CENTRO(config-router)#network 192.168.12.64 0.0.0.31 area 0
```

```
CENTRO(config-router)#network 192.168.12.4 0.0.0.3 area 0
```

```
CENTRO#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

### 6.16.2.4. ENRUTAMIENTO DE LA VLAN 30

**Este comando le permite declarar las sub-interfaces del router.**

```
CENTRO(config)# interface fastethernet 0.1
```

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

```
CENTRO(config-subif)# ip address 192.168.12.209 255.255.255.248
```

**Este comando le permite realizar el encapsulamiento de la vlan.**

```
CENTRO(config-subif)# encapsulation dot1q 30
```

**Este comando le permite levantar la sub-interfaces del router.**

```
CENTRO(config- subif)# no shutdown
```

## ENRUTAMIENTO DE LA VLAN 40

**Este comando le permite declarar las sub-interfaces del router.**

```
CENTRO(config)# interface fastethernet 0.2
```

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

```
CENTRO(config-subif)# ip address 192.168.12.217 255.255.255.248
```

**Este comando le permite realizar el encapsulamiento de la vlan.**

```
CENTRO(config-subif)# encapsulation dot1q 40
```

**Este comando le permite levantar la sub-interfaces del router.**

```
CENTRO(config-subif)# no shutdown
```

## 6.16.2.5.SHOW RUN

```
CENTRO#sh run
```

```
Building configuration...
```

```
!
```

```
Version 12.1
```

**Version Del IOS**

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
no service password-encryption
```

```
!
```

```
hostname CENTRO
```

**Nombre del router**

```
!
```

```
!
```

```
!
```

```
ip subnet-zero
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
interface Serial0
```

```
ip address 192.168.12.5 255.255.255.252
```

**IP asignada por el administrador**

```
no ip directed-broadcast
```

```
clock rate 56000
```

```
bandwidth 1544
```

```
!
```

```
interface Serial1
```

```
ip address 192.168.12.10 255.255.255.252
```

**IP asignada por el administrador**

```
no ip directed-broadcast
```

```
bandwidth 1544
```

```

!
interface Ethernet0
ip address 192.168.12.65 255.255.255.224      IP asignada por el administrador
no ip directed-broadcast
bandwidth 10000
ip ospf cost 100
!
interface Ethernet0.1
encapsulation dot1q 30
ip address 192.168.12.209 255.255.255.248  IP asignada por el administrador
!
interface Ethernet0.2
encapsulation dot1q 40
ip address 192.168.12.217 255.255.255.248  IP asignada por el administrador
!
!
router ospf 1                               Protocolo ospf
network 192.168.12.4 0.0.0.3 area 0
network 192.168.12.8 0.0.0.3 area 0
network 192.168.12.64 0.0.0.31 area 0
!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

```

#### 6.16.2.6. SHOW IP ROUTE

- C** Conectado.
  - S.** Estático.
  - I.** Protocolo IGRP.
  - R** Protocolo Rip.
  - B** Protocolo BGP.
  - D** Protocolo EIGRP.
  - EX** Protocolo EIGRP externo.
  - O** Protocolo OSPF.
- 
- IA** El número de las rutas recibidas de otras áreas del OSPF.
  - E1** Rutas recibidas de otras áreas del OSPF tipo externo 1.
  - E2** Rutas recibidas de otras áreas del OSPF tipo externo 2.

**I** Son las rutas recibidas de los anuncios del protocolo del IS-IS.

<b>C</b>	192.168.12.32/27 is directly connected,	Ethernet0
<b>Conectada directamente</b>	<b>Red con la que se conecta</b>	<b>Interfaz</b>

**O**

**Protocolo OSPF**

192.168.12.64/27

**Red aprendida ospf**

Via [110/64]

**Distancia administrativa y ancho de banda**

192.168.12.65

**Ip asignada a la interfaz**

Ethernet0

**Interfaz**

**R**

**Protocolo OSPF**

192.168.12.128/27

**Red aprendida RIP**

[120/1] via

**Distancia administrativa y ancho de banda**

192.168.12.2

**Ip asignada a la interfaz**

Serial0

**Interfaz**

CENTRO#sh 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

```

192.168.12.0/0 is variably subnetted, 7 subnets
C    192.168.12.4/30 is directly connected, Serial0
C    192.168.12.64/27 is directly connected, Ethernet0
O    192.168.12.0/30 [110/64] via 192.168.12.1, 01:00:08, Ethernet0
O    192.168.12.32/27 [110/64] via 192.168.12.1, 01:00:08, Ethernet0
C    192.168.12.8/30 is directly connected, Serial1
O    192.168.12.96/27 [110/64] via 192.168.12.9, 00:43:46, Ethernet0
R    192.168.12.128/27 [120/2] via 192.168.12.6, 00:07:28, Serial0

```

#### 6.16.2.7.SHOW INTERFACES

CENTRO#sh inter

Serial0 is down, line protocol is down

Hardware is HD64570

Internet address is 192.168.12.5/30

MTU 1500 bytes, BW 1544 Kbit, 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

Serial1 is down, line protocol is down

Hardware is HD64570

Internet address is 192.168.12.10/30

MTU 1500 bytes, BW 1544 Kbit, 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
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 000C.8131.5600 (bia 000C.8131.5600)
  Internet address is 192.168.12.65/27
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  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
Ethernet0.1 is down, line protocol is down
  Hardware is AmdFE, address is 000C.8131.5601 (bia 000C.8131.5601)
  Internet address is 192.168.12.209/29
  MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
Ethernet0.2 is down, line protocol is down
  Hardware is AmdFE, address is 000C.8131.5601 (bia 000C.8131.5601)
  Internet address is 192.168.12.217/29
  MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
```

CENTRO#

### 6.16.2.8. SWITCH CENTRO

**Este comando le permite crear una vlan.**

```
Switch#vlan database
```

**Este comando le permite asignar un nombre a la vlan**

```
Switch(vlan)#vlan 30 name ventas
```

```
VLAN 20 added:
```

```
  Name:ventas
```

```
Switch(vlan)#vlan 40 name computacion
```

```
VLAN 40 added:
```

```
  Name:computacion
```

### 6.16.2.9. CREACIÓN DE UNA VLAN

**Ingrese al modo de configuración global.**

```
Switch#conf ter
```

Enter configuration commands, one per line. End with CNTL/Z.

**Con este comando ingrese a la interfaz del switch.**

```
S_CENTRO(config)#interface fastethernet 0/1
```

**Con este comando cree el puerto truncado.**

```
S_CENTRO(config-if)#switchport mode trunk
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_CENTRO(config-if)#switchport access vlan 30
```

**Con este comando ingrese a la interfaz del switch.**

```
S_CENTRO(config-if)#interface fastethernet 0/2
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_CENTRO(config-if)#switchport access vlan 30
```

**Con este comando ingrese a la interfaz del switch.**

```
S_CENTRO(config-if)#interface fastethernet 0/3
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_CENTRO(config-if)#switchport access vlan 40
```

### 6.16.2.10. SHOW VLAN

<b>VLAN</b>	Es el numero de la vlan.
<b>Name</b>	Es el nombre asignado a la vlan.
<b>Status</b>	Es el estado en que se encuentra la vlan.
<b>Ports</b>	Son los puertos asignados a la vlan.

S\_CENTRO#sh vlan

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
30 ventas	active	Fa0/1
40 computacion	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	-	0	0
30 enet	100030	1500	-	-	-	-	-	0	0
40 enet	100040	1500	-	-	-	-	-	0	0
1002 fddi	101002	1500	-	-	-	-	-	0	0
1003 tr	101003	1500	-	-	-	-	-	0	0
1004 fdnet	101004	1500	-	-	-	ieee	-	0	0
1005 trnet	101005	1500	-	-	-	ibm	-	0	0

S\_CENTRO#

### 6.16.2.11. SHOW INTERFACES

S\_CENTRO#sh interfaces

```
Vlan 1 is administratively down, line protocol is down
Hardware is CPU Interface, address is 000C.3722.3717 (bia 000C.3722.3717)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Auto-duplex, Auto-speed
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 02:29:44, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
269 packets input, 71059 bytes, 0 no buffer
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```

7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is up, line protocol is up

Hardware is Fast Ethernet, address is 000C.3722.3718 (bia 000C.3722.3718)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/2 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.6353.3518 (bia 000C.6353.3518)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/3 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.3003.4040 (bia 000C.3003.4040)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/4 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.4143.7135 (bia 000C.4143.7135)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/5 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.3439.7120 (bia 000C.3439.7120)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/6 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.1989.3587 (bia 000C.1989.3587)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/7 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.1359.8784 (bia 000C.1359.8784)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/8 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.3977.5931 (bia 000C.3977.5931)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/9 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.7655.6168 (bia 000C.7655.6168)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/10 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.1264.3009 (bia 000C.1264.3009)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.6860.3482 (bia 000C.6860.3482)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/12 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.8779.2341 (bia 000C.8779.2341)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer

```
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
7290 packets output, 429075 bytes, 0 underruns
0 output errors, 3 interface resets
0 output buffer failures, 0 output buffers swapped out
```

S\_CENTRO#

### 6.16.3.ROUTER SUR

#### 6.16.3.1.ASIGNAR NOMBRE AL ROUTER

**Esta en el modo usuario.**

```
Router>
```

**El comando enable le permite ingresar al modo privilegiado.**

```
Router>enable
```

**Ahora ingrese a configuración global con el comando configure terminal.**

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Ahora asigne el nombre al router para este caso SUR después del comando hostame.**

```
Router(config)#hostname SUR
```

**Observe como cambio el nombre al router.**

```
SUR(config)#
```

#### 6.16.3.2.ASIGNAR CONTRASEÑA

COSOLA DEL ROUTER

```
SUR(config)#
```

**Ingrese el comando line console 0.**

```
SUR(config)#line console 0
```

**Ingrese el comando password para asignar la contraseña.**

```
SUR(config)#password topico
```

**Ahora ingrese el comando login.**

```
SUR(config-line)#LOGIN
```

TERMINAL VIRTUAL DEL ROUTER

**Ingrese el comando line vty 0 4.**

```
SUR(config)#line vty 0 4
```

**Ingrese el comando password para asignar la contraseña.**

```
SUR(config-line)#password topico
```

**Ahora ingrese el comando login.**

```
SUR(config-line)#login
```

### 6.16.3.3. ASIGNAR DIRECCIÓN IP AL ROUTER

#### 6.16.3.3.1. ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0

**Esta en el modo de configuración global.**

SUR#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface s 0 para configurar dicha interfaz.**

SUR(config)#interface s 0

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

SUR(config-if)#ip address 192.168.12.9 255.255.255.252

**Con el comando clock rate fije la velocidad de sincronización del router.**

SUR(config-if)#clock rate 56000

**Este comando le permite levantar la interfaz.**

SUR(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Serial0, changed state to up

SUR(config-if)#^Z

%SYS-5-CONFIG\_I: Configured from console by console#

**Este comando le permite guardar los cambios.**

SUR#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

#### 6.16.3.3.2. ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET

**Esta en el modo de configuración global.**

SUR#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface ethernet 0 para configurar dicha interfaz.**

SUR(config)#interface ethernet 0

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

SUR(config-if)#ip address 192.168.12.97 255.255.255.224

**Este comando le permite levantar la interfaz.**

SUR(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Ethernet0, changed state to up

SUR(config-if)#^Z

%SYS-5-CONFIG\_I: Configured from console by console#

**Este comando le permite guardar los cambios.**

SUR#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

#### 6.16.3.4. DECLARAR EL PROTOCOLO OSPF

**Esta en el modo de configuración global.**

```
SUR#configure terminal
```

**Este comando le permite declarar el protocolo OSPF.**

```
SUR(config)#router ospf 1
```

**Declare todos los segmentos de las redes que estén directamente conectadas al router con la willcard respectiva y el área.**

```
SUR(config-router)#network 192.168.12.8 0.0.0.3 area 0
```

```
SUR(config-router)#network 192.168.12.96 0.0.0.31 area 0
```

```
SUR#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

#### 6.16.3.5. ENRUTAMIENTO DE LA VLAN 50

**Este comando le permite declarar las sub-interfaces del router.**

```
SUR(config)# interface fastethernet 0.1
```

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

```
SUR(config-subif)# ip address 192.168.12.225 255.255.255.248
```

**Este comando le permite realizar el encapsulamiento de la vlan.**

```
SUR(config-subif)# encapsulation dot1q 50
```

**Este comando le permite levantar la sub-interfaces del router.**

```
SUR(config- subif)# no shutdown
```

#### ENRUTAMIENTO DE LA VLAN 60

**Este comando le permite declarar las sub-interfaces del router.**

```
SUR(config)# interface fastethernet 0.2
```

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

```
SUR(config-subif)# ip address 192.168.12.233 255.255.255.248
```

**Este comando le permite realizar el encapsulamiento de la vlan.**

```
SUR(config-subif)# encapsulation dot1q 60
```

**Este comando le permite levantar la sub-interfaces del router.**

```
SUR(config- subif)# no shutdown
```

**6.16.3.6. SHOW RUN**

SUR#sh run  
Building configuration...

```

!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SUR
!
!
!
ip subnet-zero
!
!
!
!
!
!
!
!
!
!
interface Serial0
 ip address 192.168.12.9 255.255.255.252
 no ip directed-broadcast
 clock rate 56000
 bandwidth 1544
!
interface Serial1
 no ip address
 no ip directed-broadcast
 bandwidth 1544
 shutdown
!
interface Ethernet0
 ip address 192.168.12.97 255.255.255.224

no ip directed-broadcast
 bandwidth 10000
 ip ospf cost 100
!
interface Ethernet0.1
 encapsulation dot1q 50
 ip address 192.168.12.225 255.255.255.248
!
interface Ethernet0.2

```

**Versión Del IOS****IP asignada por el Administrador****IP asignada por el Administrador****IP asignada por el Administrador****IP asignada por el Administrador**

```

encapsulation dot1q 60
ip address 192.168.12.233 255.255.255.248      IP asignada por el Administrador
!
!
router ospf 1                                Protocolo OSPF
network 192.168.12.96 0.0.0.31 area 0
network 192.168.12.8 0.0.0.3 area 0
!
ip classless
no ip http server
!
!
!
line con 0
  transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

SUR#

```

### 6.16.3.7.SHOW IP ROUTE

- C** Conectado.
  - S.** Estático.
  - I.** Protocolo IGRP.
  - R** Protocolo Rip.
  - B** Protocolo BGP.
  - D** Protocolo EIGRP.
  - EX** Protocolo EIGRP externo.
  - O** Protocolo OSPF.
- IA** El número de las rutas recibidas de otras áreas del OSPF.
  - E1** Rutas recibidas de otras áreas del OSPF tipo externo 1.
  - E2** Rutas recibidas de otras áreas del OSPF tipo externo 2.
  - I** Son las rutas recibidas de los anuncios del protocolo del IS-IS.

```

C          192.168.12.32/27 is directly connected,    Ethernet0
Conectada directamente      Red con la que se conecta      Interfaz

O

Protocolo OSPF

```

192.168.12.64/27

Red aprendida ospf

Via [110/64]

Distancia administrativa y ancho de banda

192.168.12.65

IP asignada a la interfaz

Ethernet0

Interfaz

R

Protocolo OSPF

192.168.12.128/27

Red aprendida RIP

[120/1] via

Distancia administrativa y ancho de banda

192.168.12.2

Ip asignada a la interfaz

Serial0

Interfaz

SUR#sh 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

192.168.12.0/0 is variably subnetted, 9 subnets

C 192.168.12.8/30 is directly connected, Serial0

C 192.168.12.96/27 is directly connected, Ethernet0

O 192.168.12.4/30 [110/256] via 192.168.12.10, 01:00:30, Ethernet0

- O 192.168.12.0/30 [110/192] via 192.168.12.10, 01:00:30, Ethernet0
- O 192.168.12.32/27 [110/192] via 192.168.12.10, 01:00:30, Ethernet0
- O 192.168.12.64/27 [110/64] via 192.168.12.10, 00:48:16, Ethernet0
- O 192.168.12.12/30 [120/10] via 192.168.12.97, 00:18:05, Ethernet0
- O 192.168.12.160/27 [120/10] via 192.168.12.97, 00:18:05, Ethernet0
- R 192.168.12.128/27 [120/3] via 192.168.12.10, 00:04:41, Serial0

### 6.16.3.8.SHOW INTERFACES

SUR#sh interfaces

Serial0 is up, line protocol is up

Hardware is HD64570

Internet address is 192.168.12.9/30

MTU 1500 bytes, BW 3000 Kbit, 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

Serial1 is administratively down, line protocol is down

Hardware is HD64570

MTU 1500 bytes, BW 1544 Kbit, 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  
Serial2 is administratively down, line protocol is down  
Hardware is HD64570  
MTU 1500 bytes, BW 1544 Kbit, 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  
Ethernet0 is up, line protocol is up  
Hardware is Lance, address is 000C.9596.5444 (bia 000C.9596.5444)  
Internet address is 192.168.12.97/27  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255  
Encapsulation ARPA, loopback not set, keepalive set (10 sec)  
ARP type: ARPA, ARP Timeout 04:00:00  
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  
Ethernet0.1 is down, line protocol is down  
Hardware is AmdFE, address is 000C.9596.5445 (bia 000C.9596.5445)  
Internet address is 192.168.12.225/29  
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255  
Encapsulation ARPA, loopback not set, keepalive set (10 sec)  
ARP type: ARPA, ARP Timeout 04:00:00  
Ethernet0.2 is down, line protocol is down  
Hardware is AmdFE, address is 000C.9596.5445 (bia 000C.9596.5445)  
Internet address is 192.168.12.233/29

MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255  
 Encapsulation ARPA, loopback not set, keepalive set (10 sec)  
 ARP type: ARPA, ARP Timeout 04:00:00

SUR#

#### 6.16.4.SWITCH SUR

**Con este comando le permite crear una vlan.**

Switch#vlan database

**Este commando le permite asignar un nombre a la vlan**

Switch(vlan)#vlan 50 name gerencia

VLAN 50 added:

Name:gerencia

Switch(vlan)#vlan 60 name RRHH

VLAN 60 added:

Name:RRHH

##### 6.16.4.1.CREACIÓN DE UNA VLAN

**Ingrese al modo de configuración global.**

Switch#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

**Con este comando le permite ingresar a la interfaz del switch.**

S\_SUR(config)#interface fastethernet 0/1

**Con este comando cree el Puerto truncado.**

S\_SUR(config-if)#switchport mode trunk

**Con este comando asigne la vlan una o varias interfaces.**

S\_SUR(config-if)#switchport access vlan 50

**Con este comando ingrese a la interfaz del switch.**

S\_SUR(config-if)#interface fastehernet 0/2

**Con este comando asigne la vlan una o varias interfaces.**

S\_SUR(config-if)#switchport access vlan 50

**Con este comando ingrese a la interfaz del switch.**

S\_SUR(config-if)#interface fastethernet 0/3

**Con este comando asigne a la vlan una o varias interfaces.**

S\_SUR(config-if)#switchport access vlan 60

##### 6.16.4.2.SHOW VLAN

<b>VLAN</b>	Es el numero de la vlan.
<b>Name</b>	Es el nombre que le asigno a la vlan.
<b>Status</b>	Es el estado en que se encuentra la vlan.
<b>Ports</b>	Son los puertos asignados a la vlan.

S\_SUR#sh vlan

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12
50 gerencia	active	Fa0/1, Fa0/2
60 RRHH	active	Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	-	0	0
50 enet	100050	1500	-	-	-	-	-	0	0
60 enet	100060	1500	-	-	-	-	-	0	0
1002 fddi	101002	1500	-	-	-	-	-	0	0
1003 tr	101003	1500	-	-	-	-	-	0	0
1004 fdnet	101004	1500	-	-	-	ieee	-	0	0
1005 trnet	101005	1500	-	-	-	ibm	-	0	0

## SHOW INTERFACES

S\_SUR#sh interfaces

Vlan 1 is administratively down, line protocol is down  
 Hardware is CPU Interface, address is 000C.1801.2896 (bia 000C.1801.2896)  
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec  
 5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is up, line protocol is up

Hardware is Fast Ethernet, address is 000C.1801.2897 (bia 000C.1801.2897)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/2 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.7202.6944 (bia 000C.7202.6944)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/3 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.7432.1762 (bia 000C.7432.1762)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/4 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.1573.8180 (bia 000C.1573.8180)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/5 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.7925.7924 (bia 000C.7925.7924)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/6 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.7418.9903 (bia 000C.7418.9903)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/7 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.1229.7843 (bia 000C.1229.7843)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/8 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.7418.3886 (bia 000C.7418.3886)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/9 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.3585.5109 (bia 000C.3585.5109)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/10 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.4861.1072 (bia 000C.4861.1072)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.9727.4836 (bia 000C.9727.4836)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/12 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.7477.8089 (bia 000C.7477.8089)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

S\_SUR#

## 6.17.ROUTER BAHÍA.

### 6.17.1.ASIGNAR NOMBRE AL ROUTER

**Esta en el modo usuario.**

Router>

**El comando enable le permite ingresar al modo privilegiado.**

Router>enable

**Ahora ingrese a configuración global con el comando configure terminal.**

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ahora asigne el nombre al router para este caso BAHÍA después del comando hostame.**

Router(config)#hostname BAHIA

**Observe como cambio el nombre al router.**

BAHIA(config)#

### 6.17.2.ASIGNAR CONTRASEÑA

BAHIA(config)#

**Ingrese el comando line console 0.**

BAHIA(config)#line console 0

**Ingrese el comando password para asignar la contraseña.**

BAHIA(config)#password topico

**Ahora ingrese el comando login.**

BAHIA(config-line)#LOGIN

TERMINAL VIRTUAL DEL ROUTER

**Ingrese el comando line vty 0 4.**

BAHIA(config)#line vty 0 4

**Ingrese el comando password para asignar la contraseña.**

BAHIA(config-line)#password topico

**Ahora ingrese el comando login.**

BAHIA(config-line)#login

### 6.17.3. ASIGNAR DIRECCIÓN IP AL ROUTER

#### 6.17.3.1. ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 0

**Esta en el modo de configuración global.**

```
BAHIA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface s 0 para configurar dicha interfaz.**

```
BAHIA(config)#interface s 0
```

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

```
BAHIA(config-if)#ip address 192.168.12.13 255.255.255.252
```

**Con el comando clock rate fije la velocidad de sincronización del router.**

```
BAHIA(config-if)#clock rate 56000
```

**Este comando le permite levantar la interfaz.**

```
BAHIA(config-if)#no shutdown
```

```
%LINK-3-UPDOWN: Interface Serial0, changed state to up
```

```
BAHIA(config-if)#^Z
```

```
%SYS-5-CONFIG_I: Configured from console by console#
```

**Este comando le permite guardar los cambios.**

```
BAHIA#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

#### 6.17.3.2. ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 1

**Esta en el modo de configuración global.**

```
BAHIA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface s 1 para configurar dicha interfaz.**

```
BAHIA(config)#interface s 1
```

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

```
BAHIA(config-if)#ip address 192.168.12.2 255.255.255.252
```

**Este comando le permite levantar la interfaz.**

```
BAHIA(config-if)#no shutdown
```

```
%LINK-3-UPDOWN: Interface Serial1, changed state to up
```

```
BAHIA(config-if)#^Z
```

```
%SYS-5-CONFIG_I: Configured from console by console#
```

**Este comando le permite guardar los cambios.**

```
BAHIA#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

### 6.17.3.3.ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET

**Esta en el modo de configuración global.**

BAHIA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface ethernet 0 para configurar dicha interfaz.**

BAHIA(config)#interface ethernet 0

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

BAHIA(config-if)#ip address 192.168.12.129 255.255.255.224

**Este comando le permite levantar la interfaz.**

BAHIA(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Ethernet0, changed state to up

BAHIA(config-if)#^Z

%SYS-5-CONFIG\_I: Configured from console by console#

**Este comando le permite guardar los cambios.**

BAHIA#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

### 6.17.4.DECLARAR EL PROTOCOLO RIP

**Esta en el modo de configuración global.**

BAHIA#configure terminal

**Este comando le permite declarar el protocolo RIP VERSION 2.**

BAHIA(config)#router rip

Ingresamos la version del protocolo

BAHIA(config-router)# version 2

**Declare el segmento de red en el que esta trabajando.**

BAHIA(config-router)#network 192.168.12.0

BAHIA#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

### 6.17.5.ENRUTAMIENTO DE LA VLAN 70

**Este comando le permite declarar las sub-interfaces del router.**

BAHIA(config)# interface fastethernet 0.1

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

BAHIA(config-subif)# ip address 192.168.12.226 255.255.255.248

**Este comando le permite realizar el encapsulamiento de la vlan.**

BAHIA(config-subif)# encapsulation dot1q 70

**Este comando le permite levantar la sub-interfaces del router.**

BAHIA(config- subif)# no shutdown

ENRUTAMIENTO DE LA VLAN 80

**Este comando le permite declarar las sub-interfaces del router.**

BAHIA(config)# interface fastethernet 0.2

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

BAHIA(config-subif)# ip address 192.168.12.234 255.255.255.248

**Este comando le permite realizar el encapsulamiento de la vlan.**

BAHIA(config-subif)# encapsulation dot1q 80

**Este comando le permite levantar la sub-interfaces del router.**

BAHIA(config-subif)# no shutdown

6.17.6.SHOW RUN

BAHIA#sh run

Building configuration...

!

Version 12.1

**Versión Del IOS**

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname BAHIA

**Nombre del Router**

!

!

!

ip subnet-zero

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Serial0

ip address 192.168.12.13 255.255.255.252

**IP asignada por el Administrador**

no ip directed-broadcast

clock rate 56000

bandwidth 3000

!

interface Serial1

ip address 192.168.12.2 255.255.255.252

**IP asignada por el Administrador**

no ip directed-broadcast

```

bandwidth 1544
!
interface Serial2
no ip address
no ip directed-broadcast
bandwidth 1544
shutdown
!
interface Ethernet0
ip address 192.168.12.129 255.255.255.224      IP asignada por el Administrador
no ip directed-broadcast
bandwidth 10000
!
interface Ethernet0.1
encapsulation dot1q 70
ip address 192.168.12.226 255.255.255.248    IP asignada por el Administrador
!
interface Ethernet0.2
encapsulation dot1q 80
ip address 192.168.12.234 255.255.255.248    IP asignada por el Administrador
!
!
router rip                                     Protocolo rip

version 2
network 192.168.12.0
!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

BAHIA#

```

### 6.17.7.SHOW IP ROUTE

**C** Conectado.  
**S**. Estático.  
**I**. Protocolo IGRP.  
**R** Protocolo Rip.

- B** Protocolo BGP.
- D** Protocolo EIGRP.
- EX** Protocolo EIGRP externo.
- O** Protocolo OSPF.

**IA** El número de las rutas recibidas de otras áreas del OSPF.

**E1** Rutas recibidas de otras áreas del OSPF tipo externo 1.

**E2** Rutas recibidas de otras áreas del OSPF tipo externo 2.

**I** Son las rutas recibidas de los anuncios del protocolo del IS-IS.

<b>C</b>	192.168.12.32/27 is directly connected,	Ethernet0
<b>Conectada directamente</b>	<b>Red con la que se conecta</b>	<b>Interfaz</b>

**O**

**Protocolo OSPF**

192.168.12.64/27

**Red aprendida ospf**

Via [110/64]

**Distancia administrativa y ancho de banda**

192.168.12.65

**Ip asignada a la interfaz**

Ethernet0

**Interfaz**

**R**

**Protocolo OSPF**

192.168.12.128/27

**Red aprendida RIP**

[120/1] via

**Distancia administrativa y ancho de banda**

192.168.12.2

**Ip asignada a la interfaz**

Serial0

**Interfaz**

BAHIA#sh 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

192.168.12.0/0 is variably subnetted, 9 subnets  
C 192.168.12.0/30 is directly connected, Serial1  
C 192.168.12.128/27 is directly connected, Ethernet0  
R 192.168.12.32/27 [120/1] via 192.168.12.1, 00:08:26, Serial1  
R 192.168.12.4/30 [120/1] via 192.168.12.1, 00:07:16, Serial1  
C 192.168.12.12/30 is directly connected, Serial0  
R 192.168.12.160/27 [120/1] via 192.168.12.14, 00:06:37, Serial0  
R 192.168.12.64/27 [120/10] via 192.168.12.1, 00:08:13, Serial1  
R 192.168.12.8/30 [120/10] via 192.168.12.1, 00:06:30, Serial1  
R 192.168.12.96/27 [120/10] via 192.168.12.1, 00:09:34, Serial1

**6.17.8.SHOW INTERFACES**

BAHIA#sh interfaces

Serial0 is up, line protocol is up  
Hardware is HD64570  
Internet address is 192.168.12.13/30  
MTU 1500 bytes, BW 3000 Kbit, 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  
Serial1 is up, line protocol is up  
Hardware is HD64570  
Internet address is 192.168.12.2/30  
MTU 1500 bytes, BW 1544 Kbit, 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  
Serial2 is administratively down, line protocol is down  
Hardware is HD64570  
MTU 1500 bytes, BW 1544 Kbit, 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  
Ethernet0 is up, line protocol is up  
Hardware is Lance, address is 000C.8385.5044 (bia 000C.8385.5044)  
Internet address is 192.168.12.129/27  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255  
Encapsulation ARPA, loopback not set, keepalive set (10 sec)  
ARP type: ARPA, ARP Timeout 04:00:00  
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
Ethernet0.1 is down, line protocol is down
  Hardware is AmdFE, address is 000C.8385.5045 (bia 000C.8385.5045)
  Internet address is 192.168.12.226/29
  MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
Ethernet0.2 is down, line protocol is down
  Hardware is AmdFE, address is 000C.8385.5045 (bia 000C.8385.5045)
  Internet address is 192.168.12.234/29
  MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00

```

BAHIA#

### 6.17.9.SWITCH BAHÍA

**Este comando le permite crear una vlan.**

Switch#vlan database

**Con este comando asigne un nombre a la vlan**

Switch(vlan)#vlan 70 name diseño

VLAN 70 added:

Name:diseño

Switch(vlan)#vlan 80 name produccion

VLAN 80 added:

Name:produccion

#### 6.17.9.1.CREACIÓN DE UNA VLAN

**Ingrese al modo de configuración global.**

Switch#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

**Con este comando ingrese a la interfaz del switch.**

```
S_BAHIA(config)#interface fastethernet 0/1
```

**Con este comando cree el puerto truncado.**

```
S_BAHIA(config-if)#switchport mode trunk
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_BAHIA(config-if)#switchport access vlan 70
```

**Con este comando ingrese a la interfaz del switch.**

```
S_BAHIA(config-if)#interface fastethernet 0/2
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_BAHIA(config-if)#switchport access vlan 70
```

**Con este comando ingrese a la interfaz del switch.**

```
S_BAHIA(config-if)#interface fastethernet 0/3
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_BAHIA(config-if)#switchport access vlan 80
```

### 6.17.9.2. SHOW VLAN

Muestra la lista de vlan configuradas y que puertos son miembros de cada ID

**VLAN** el número de la vlan

**Name** el nombre asignado a la vlan.

**Status** el estado en que se encuentra la vlan.

**Ports** Son los puertos asignados a la vlan

```
S_BAHIA#sh vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12
70 diseño	active	Fa0/1, Fa0/2
80 produccion	active	Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	0	0	
70	enet	100070	1500	-	-	-	-	0	0	
80	enet	100080	1500	-	-	-	-	0	0	
1002	fddi	101002	1500	-	-	-	-	0	0	
1003	tr	101003	1500	-	-	-	-	0	0	
1004	fdnet	101004	1500	-	-	-	ieee	0	0	
1005	trnet	101005	1500	-	-	-	ibm	0	0	

### 6.17.9.3.SHOW INTERFACES

S\_BAHIA#sh interfaces

Vlan 1 is administratively down, line protocol is down  
Hardware is CPU Interface, address is 000C.9335.9293 (bia 000C.9335.9293)  
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is up, line protocol is up  
Hardware is Fast Ethernet, address is 000C.9335.9294 (bia 000C.9335.9294)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/2 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.4511.6013 (bia 000C.4511.6013)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/3 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.5737.6809 (bia 000C.5737.6809)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/4 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.9051.3389 (bia 000C.9051.3389)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/5 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.9866.7896 (bia 000C.9866.7896)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/6 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.3611.1492 (bia 000C.3611.1492)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/7 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.9460.2656 (bia 000C.9460.2656)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/8 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.4954.6844 (bia 000C.4954.6844)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/9 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.3516.1412 (bia 000C.3516.1412)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/10 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.5172.9979 (bia 000C.5172.9979)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.2990.5602 (bia 000C.2990.5602)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/12 is down, line protocol is down  
 Hardware is Fast Ethernet, address is 000C.5016.2460 (bia 000C.5016.2460)  
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never  
 Last clearing of "show interface" counters never  
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
 Queueing strategy: fifo  
 Output queue :0/40 (size/max)  
 5 minute input rate 0 bits/sec, 0 packets/sec  
 5 minute output rate 0 bits/sec, 0 packets/sec  
 269 packets input, 71059 bytes, 0 no buffer  
 Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
 7290 packets output, 429075 bytes, 0 underruns  
 0 output errors, 3 interface resets  
 0 output buffer failures, 0 output buffers swapped out

S\_BAHIA#

## 6.18.ROUTER NORTE

### 6.18.1.ASIGNAR NOMBRE AL ROUTER

**Esta en el modo usuario.**

Router>

**El comando enable le permite ingresar al modo privilegiado.**

Router>enable

**Ahora ingrese a configuración global con el comando configure terminal.**

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ahora asigne el nombre al router para este caso NORTE después del comando hostame.**

Router(config)#hostname NORTE

**Observe como cambio el nombre al router.**

NORTE(config)#

## 6.18.2. ASIGNAR CONTRASEÑA

NORTE(config)#

**Ingrese el comando line console 0.**

NORTE(config)#line console 0

**Ingrese el comando password para asignar la contraseña.**

NORTE(config)#password topico

**Ahora ingrese el comando login.**

NORTE(config-line)#LOGIN

TERMINAL VIRTUAL DEL ROUTER

**Ingrese el comando line vty 0 4.**

NORTE(config)#line vty 0 4

**Ingrese el comando password para asignar la contraseña.**

NORTE(config-line)#password topico

**Ahora ingrese el comando login.**

NORTE(config-line)#login

## 6.18.3. ASIGNAR DIRECCIÓN IP AL ROUTER

### 6.18.3.1. ASIGNAR DIRECCIÓN IP A INTERFAZ SERIAL 1

**Esta en el modo de configuración global.**

NORTE#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface s 1 para configurar dicha interfaz.**

NORTE(config)#interface s 1

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

NORTE(config-if)#ip address 192.168.12.14 255.255.255.252

**Este comando le permite levantar la interfaz.**

NORTE(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Serial1, changed state to up

NORTE(config-if)#^Z

%SYS-5-CONFIG\_I: Configured from console by console#

**Este comando le permite guardar los cambios.**

NORTE#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

### 6.18.3.2. ASIGNAR DIRECCIÓN IP A INTERFAZ ETHERNET

**Esta en el modo de configuración global.**

NORTE#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Ingrese el comando interface ethernet 0 para configurar dicha interfaz.**

```
NORTE(config)#interface ethernet 0
```

**Con el comando IP address asigne la dirección IP con su respectiva mascara.**

```
NORTE(config-if)#ip address 192.168.12.161 255.255.255.224
```

**Este comando le permite levantar la interfaz.**

```
NORTE(config-if)#no shutdown
```

```
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
```

```
NORTE(config-if)#^Z
```

```
%SYS-5-CONFIG_I: Configured from console by console#
```

**Este comando le permite guardar los cambios.**

```
NORTE#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

#### 6.18.4.DECLARAR EL PROTOCOLO RIP

**Esta en el modo de configuración global.**

```
NORTE#configure terminal
```

**Este comando le permite declarar el protocolo RIP VERSION 2.**

```
NORTE(config)#router rip
```

```
Ingresamos la version del protocolo
```

```
NORTE(config-router)# version 2
```

**Declare el segmento de red en el que esta trabajando.**

```
NORTE(config-router)#network 192.168.12.0
```

```
NORTE#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

#### 6.18.5.ENRUTAMIENTO DE LA VLAN 90

**Este comando le permite declarar las sub-interfaces del router.**

```
NORTE(config)# interface fastethernet 0.1
```

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

```
NORTE(config-subif)# ip address 192.168.12.227 255.255.255.248
```

**Este comando le permite realizar el encapsulamiento de la vlan.**

```
NORTE(config-subif)# encapsulation dot1q 90
```

**Este comando le permite levantar la sub-interfaces del router.**

```
NORTE(config- subif)# no shutdown
```

#### ENRUTAMIENTO DE LA VLAN 100

**Este comando le permite declarar las sub-interfaces del router.**

```
NORTE(config)# interface fastethernet 0.2
```

**Este comando le permite asignar una dirección IP a la sub-interfaces del router con la mascara de subred.**

```
NORTE(config-subif)# ip address 192.168.12.235 255.255.255.248
```

**Este comando le permite realizar el encapsulamiento de la vlan.**

NORTE(config-subif)# encapsulation dot1q 100

**Este comando permite levantar la sub-interfaces del router.**

NORTE(config-subif)# no shutdown

### 6.18.6.SHOW RUN

NORTE#sh run

Building configuration...

!

Version 12.1

**Versión Del IOS**

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname NORTE

**Nombre del Router**

!

!

!

ip subnet-zero

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

```

interface Ethernet0
ip address 192.168.12.161 255.255.255.224      IP asignada por el Administrador
no ip directed-broadcast
bandwidth 10000
!
interface Ethernet0.1
encapsulation dot1q 90
ip address 192.168.12.227 255.255.255.248
!
interface Ethernet0.2
encapsulation dot1q 100
ip address 192.168.12.235 255.255.255.248    IP asignada por el Administrador
!
!
router rip                                     Protocolo rip

version 2
network 192.168.12.0
!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

NORTE#

```

### 6.18.7.SHOW IP ROUTE

- C** Conectado.
  - S.** Estático.
  - I.** Protocolo IGRP.
  - R** Protocolo Rip.
  - B** Protocolo BGP.
  - D** Protocolo EIGRP.
  - EX** Protocolo EIGRP externo.
  - O** Protocolo OSPF.
- IA** El número de las rutas recibidas de otras áreas del OSPF.

- E1 Rutas recibidas de otras áreas del OSPF tipo externo 1.
- E2 Rutas recibidas de otras áreas del OSPF tipo externo 2.
- I Son las rutas recibidas de los anuncios del protocolo del IS-IS.

C	192.168.12.32/27 is directly connected,	Ethernet0
<b>Conectada directamente</b>	<b>Red con la que se conecta</b>	<b>Interfaz</b>

O

**Protocolo OSPF**

192.168.12.64/27

**Red aprendida ospf**

Via [110/64]

**Distancia administrativa y ancho de banda**

192.168.12.65

**Ip asignada a la interfaz**

Ethernet0

**Interfaz**

R

**Protocolo OSPF**

192.168.12.128/27

**Red aprendida RIP**

[120/1] via

**Distancia administrativa y ancho de banda**

192.168.12.2

**Ip asignada a la interfaz**

Serial0

**Interfaz**

NORTE#sh 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

```

192.168.12.0/0 is variably subnetted, 9 subnets
C   192.168.12.12/30 is directly connected, Serial1
C   192.168.12.160/27 is directly connected, Ethernet0
R   192.168.12.0/30 [120/1] via 192.168.12.13, 00:07:13, Serial1
R   192.168.12.128/27 [120/1] via 192.168.12.13, 00:01:34, Serial1
R   192.168.12.32/27 [120/2] via 192.168.12.13, 00:07:41, Serial1
R   192.168.12.4/30 [120/2] via 192.168.12.13, 00:03:42, Serial1
R   192.168.12.64/27 [120/11] via 192.168.12.13, 00:05:25, Serial1
R   192.168.12.8/30 [120/11] via 192.168.12.13, 00:02:27, Serial1
R   192.168.12.96/27 [120/11] via 192.168.12.13, 00:06:37, Serial1

```

NORTE#

### 6.18.8.SHOW INTERFACES

NORTE#sh interfaces

Serial0 is administratively down, line protocol is down

Hardware is HD64570

MTU 1500 bytes, BW 3000 Kbit, 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

Serial1 is up, line protocol is up

Hardware is HD64570

Internet address is 192.168.12.14/30

MTU 1500 bytes, BW 1544 Kbit, 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
Serial2 is administratively down, line protocol is down
Hardware is HD64570
MTU 1500 bytes, BW 1544 Kbit, 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
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 000C.4809.8723 (bia 000C.4809.8723)
Internet address is 192.168.12.161/27
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
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
Ethernet0.1 is down, line protocol is down
Hardware is AmdFE, address is 000C.4809.8724 (bia 000C.4809.8724)
Internet address is 192.168.12.227/29
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Ethernet0.2 is down, line protocol is down
Hardware is AmdFE, address is 000C.4809.8724 (bia 000C.4809.8724)
Internet address is 192.168.12.235/29
MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00

```

### 6.18.9.SWITCH NORTE

**Con este comando le permite crear una vlan.**

```
Switch#vlan database
```

**Con este comando asigne un nombre a la vlan**

```
Switch(vlan)#vlan 90 name administracion
```

```
VLAN 90 added:
```

```
Name:administracion
```

```
Switch(vlan)#vlan 100 name pagaduria
```

```
VLAN 100 added:
```

```
Name:pagaduria
```

#### 6.18.9.1.CREACIÓN DE UNA VLAN

**Ingrese al modo de configuración global.**

```
Switch#conf ter
```

Enter configuration commands, one per line. End with CNTL/Z.

**Con este comando ingrese a la interfaz del switch.**

```
S_NORTE(config)#interface fastethernet 0/1
```

**Con este comando cree el Puerto truncado.**

```
S_NORTE(config-if)#switchport mode trunk
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_NORTE(config-if)#switchport access vlan 90
```

**Con este comando ingrese a la interfaz del switch.**

```
S_NORTE(config-if)#interface fastethernet 0/2
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_NORTE(config-if)#switchport access vlan 90
```

**Con este comando ingrese a la interfaz del switch.**

```
S_NORTE(config-if)#interface fastethernet 0/3
```

**Con este comando asigne a la vlan una o varias interfaces.**

```
S_NORTE(config-if)#switchport access vlan 100
```

**6.18.9.2.SHOW VLAN**

Muestra la lista de vlan configuradas y que puertos son miembros de cada ID

**VLAN** el número de la vlan

**Name** el nombre asignado a la vlan.

**Status** el estado en que se encuentra la vlan.

**Ports** Son los puertos asignados a la vlan

S\_NORTE#sh vlan

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12
90 administracion	active	Fa0/1, Fa0/2
100 pagaduria	active	Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	-	0	0
90 enet	100090	1500	-	-	-	-	-	0	0
100 enet	100100	1500	-	-	-	-	-	0	0
1002 fddi	101002	1500	-	-	-	-	-	0	0
1003 tr	101003	1500	-	-	-	-	-	0	0
1004 fdnet	101004	1500	-	-	-	ieee	-	0	0
1005 trnet	101005	1500	-	-	-	ibm	-	0	0

S\_NORTE#

**6.18.9.3.SHOW INTERFACES**

S\_NORTE#sh interfaces

Vlan 1 is administratively down, line protocol is down  
 Hardware is CPU Interface, address is 000C.6757.7916 (bia 000C.6757.7916)  
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,  
 reliability 255/255, txload 1/255, rxload 1/255  
 Auto-duplex, Auto-speed  
 Encapsulation ARPA, loopback not set  
 ARP type: ARPA, ARP Timeout 04:00:00  
 Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is up, line protocol is up  
Hardware is Fast Ethernet, address is 000C.6757.7917 (bia 000C.6757.7917)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/2 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.4470.5145 (bia 000C.4470.5145)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/3 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.6808.3697 (bia 000C.6808.3697)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/4 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.4584.8700 (bia 000C.4584.8700)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/5 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.4706.4564 (bia 000C.4706.4564)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/6 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.2547.6366 (bia 000C.2547.6366)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/7 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.3289.9320 (bia 000C.3289.9320)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo

Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/8 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.7020.1977 (bia 000C.7020.1977)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/9 is down, line protocol is down  
Hardware is Fast Ethernet, address is 000C.9620.4083 (bia 000C.9620.4083)  
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Auto-duplex, Auto-speed  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/10 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.1710.2222 (bia 000C.1710.2222)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.4196.9679 (bia 000C.4196.9679)

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 02:29:44, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

269 packets input, 71059 bytes, 0 no buffer

Received 6 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

7290 packets output, 429075 bytes, 0 underruns

0 output errors, 3 interface resets

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/12 is down, line protocol is down

Hardware is Fast Ethernet, address is 000C.1200.2161 (bia 000C.1200.2161)

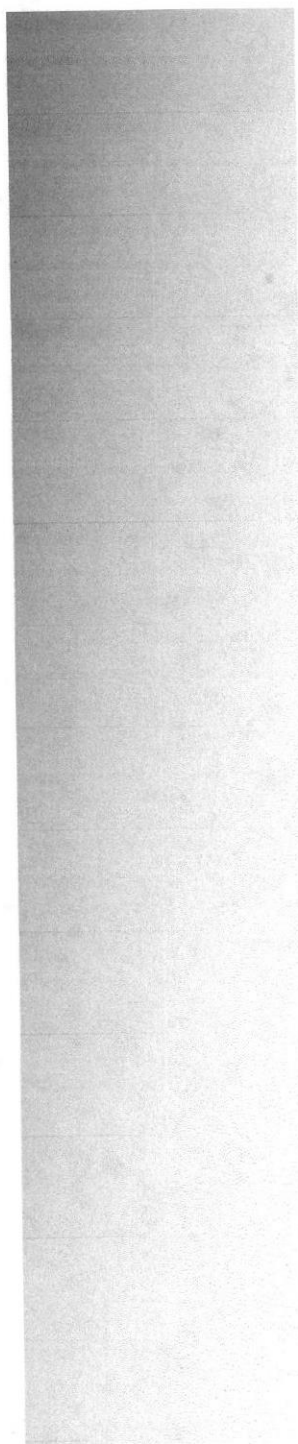
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Auto-duplex, Auto-speed

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00  
Last input 02:29:44, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
269 packets input, 71059 bytes, 0 no buffer  
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
7290 packets output, 429075 bytes, 0 underruns  
0 output errors, 3 interface resets  
0 output buffer failures, 0 output buffers swapped out



## **Anexo A** **Glosario**

## A. GLOSARIO GENERAL

### A

#### **Administración:**

Proceso por el cual se mantiene un sistema a punto y operativo. Es una tarea de la que se encarga el administrador o root y sus posibles colaboradores. Abarca acciones tales como: configurar nuevos dispositivos, administrar cuentas, seguridad del sistema.

#### **Adduser:**

El comando adduser lo utiliza root, o alguien que tenga autoridad para ello, con el fin de crear un nuevo usuario. Al comando adduser le sigue el nombre de cuenta que se va a crear. Cabe destacar que en algunas distribuciones este comando a cambiado su nombre por useradd. La sintaxis de este comando vendría a ser por ejemplo: **adduser nombre\_usuario**.

#### **ADSL: Asymmetric Digital Subscriber Line**

Línea de abonado asimétrica digital. Tecnología DSL que permite al cableado de cobre telefónico convencional transportar hasta 9 Mbps hacia el usuario y hasta 800 Kbps desde el usuario. Cuando se instala un módem ADSL en cada extremo de una línea telefónica, se crean tres canales de información: un canal de alta velocidad en el sentido red-usuario, un canal dúplex de menor velocidad y un canal ordinario telefónico. Para ello, utiliza tecnología de división de frecuencia, permitiendo separar los canales telefónicos de los otros dos canales.

#### **Ancho de banda:**

Corresponde a la cantidad de datos que se pueden enviar a través de una conexión. Por lo general se mide en bits por segundo. Una página completa de texto en español puede contener cerca de 16,000 bits. Un buen módem puede mover alrededor de 15,000 bits en un segundo. El video en pantalla y movimiento completo requeriría aproximadamente 10,000,000 bits-por-segundo, dependiendo del tipo de compresión.

#### **Autenticación:**

Proceso mediante el cual se comprueba la identidad de un usuario en la red.

## **Apache:**

Servidor de páginas web. Hoy por hoy líder del mercado de servidores, por delante de soluciones propietarias.

## **Arranque:**

Proceso por el cual un ordenador comienza a ejecutar un sistema operativo cuando se le aplica la energía de alimentación. En inglés: «bootstrap» o más comúnmente «boot».

## **B**

### **Bind:**

Berkeley Internet Name Domain. Servidor de nombres de dominio.

### **BIOS:**

Sigla de Basic Input/Output System (sistema de entrada/salida básico). Se utiliza para realizar todas las funciones necesarias para colocar en estado inicial el hardware del sistema cuando se conecta a la alimentación de energía. El BIOS controla el proceso de arranque, proporciona rutinas de entrada/salida de bajo nivel (de aquí su nombre) y (usualmente) permite que el usuario modifique los detalles de la configuración del hardware del sistema.

### **Boot:**

Proceso de arranque en un sistema informático.

### **Buffer:**

Según el diccionario, "memoria intermedia". Es una memoria que ciertos programas usan para diversas funciones, normalmente para guardar datos en memoria para su uso en un plazo corto de tiempo.

## **C**

### **Caché:**

Cuando se descarga una página Web, el dato es "ocultado", lo que significa que es almacenado temporalmente en el ordenador. La próxima vez que se desea esa página, en lugar de pedir el fichero al servidor, el navegador accede a ella a partir del caché, de manera que la página aparezca rápidamente. Pero si la página es actualizada frecuentemente, como lo son las páginas de noticias, de resultados deportivos o de datos

financieros, no se verán las informaciones más recientes. Se ha de usar el botón de Recargar del navegador para descargar del servidor los datos más recientes.

### **Conexión por módem:**

Es un tipo de cuenta para conectarse a Internet. Con este tipo de cuenta, se tiene un sobrenombre o login name y una contraseña que permite acceder a algunos lugares del sistema informático. A través de un proveedor de Internet, ISP, la cuenta permite usar un módem para establecer una conexión con el sistema del proveedor. Una vez que se ha marcado el número del proveedor y que se está conectado, el proveedor conecta al usuario a Internet. Ya se pueden visitar sitios web por medio de un navegador, como si se tuviera una conexión directa a Internet.

### **Consola:**

Una consola la forman el teclado y el monitor del equipo donde tenemos instalado Linux. No confundir con terminal.

### **Contraseña:**

Una contraseña es un código o una palabra que se utiliza para acceder a datos restringidos de un ordenador. Mientras que las contraseñas crean una seguridad contra los usuarios no autorizados, el sistema de seguridad sólo puede confirmar que la contraseña es válida, y no si el usuario está autorizado a utilizar esa contraseña. Esa es la razón por la que es tan importante salvaguardar la contraseña:

- No revelar la contraseña.
- Diseñar una contraseña que consista de letras, números y símbolos.
- Cambiar a menudo de contraseña.

### **Cortafuegos:**

Un cortafuegos es un equipamiento, combinación de hardware y software que muchas empresas u organizaciones instalan entre sus redes internas y el Internet. Un cortafuegos permite que sólo un tipo específico de mensajes pueda entrar y/o salir de la red interna. Esto protege a la red interna de los piratas o hackers que intentan entrar en redes internas a través del Internet.

### **Correo electrónico:**

También conocido como E-mail, abreviación de electronic mail. Consiste en mensajes, a menudo sólo con texto, enviados de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

## **Cuenta:**

Una cuenta en un sistema Linux puede ser algo así como la llave de un taller comunitario. Es decir, tenemos una llave personal que nos permite acceder a ese taller y utilizar algunas de las herramientas del mismo. Donde además tenemos que atenernos a las normas que rijan en ese taller.

## **D**

### **Dirección IP:**

Las direcciones IP son el método mediante el cual se identifican los ordenadores individuales (o, en una interpretación más estricta, las interfaces de red de dichos ordenadores) dentro de un red TCP/IP. Todas las direcciones IP consisten en cuatro números separados por puntos, donde cada número está entre 0 y 255.

### **DNS:**

Domain Name Server. Servidor de nombres de dominio. Servicio de red que nos facilita la búsqueda de ordenadores por su nombre de dominio. Se encarga tanto de traducir nombres a direcciones IP como del paso contrario.

### **Dominios:**

Los dominios son las direcciones de Internet que utilizan las entidades proveedoras de contenidos en la red. Estas direcciones empiezan por www. (world wide web) y tienen finalizaciones genéricas (.com,.org,.net, etc.) o de país (.es, .uk, .de, etc.).

Un dominio es el componente principal de una dirección de Internet (sitio web o e-mail). Identifica la dirección a la empresa o usuario al que pertenece. Para tener presencia constante y permanente en la Red su Empresa o Actividad debe contar con un nombre exclusivo o dominio propio que los reconozca Ej. : www.mi\_empresa.com. La posesión del mismo es fundamental para identificarse en la Web prestigiando su Empresa.

Es la forma más sencilla de localizar una dirección en Internet y garantiza la propia identidad del sitio.

## **E**

### **Ext3:**

Sistema de ficheros utilizado en Linux. Permite el uso de permisos para los ficheros y directorios, y tiende a fragmentarse mucho menos que los de otros sistemas operativos.

## **F**

### **Firewall:**

Es un elemento, que interponemos entre nuestra máquina y la red y que sirve para filtrar a voluntad el tráfico de datos que pueden circular, tanto de la red hacia nuestra maquina, como de esta hacia la red.

## **G**

### **Grupo:**

El grupo es la manera de asignar derechos de acceso específicos a ciertas clases de usuarios. Por ejemplo, todos los usuarios que trabajan en el Proyecto X pueden agregarse al grupo Proxy. Los recursos del sistema (como por ejemplo espacio en disco) que se dedican al Proyecto X se pueden configurar entonces para permitir su acceso total sólo a los miembros de Proxy. En inglés: «group».

## **H**

### **Hardware:**

El hardware es el soporte físico de una computadora, se compone de diferentes dispositivos de hardware que pueden estar dentro o fuera de la caja de la computadora. Dentro del hardware entran la placa base, la cpu, la memoria, el teclado, el ratón...

### **Host:**

Nombre de un ordenador en una red.

### **Http:**

HyperText Transfer Protocol. Protocolo de red para la transferencia de páginas de hipertexto, o lo que es lo mismo, páginas web como esta.

**Hub:**

Dispositivo que sirve para conectar entre sí dos o más ordenadores.

**I****ISP:**

Siglas de Internet Service Provider. Empresa u organización que ofrece acceso a Internet a usuarios finales y corporativos.

**L****LAN (Local Area Network):**

Red de Area Local, relativo a la conexión física y lógica de dos o más computadoras en una pequeña o no tan pequeña área de trabajo como un edificio. De esta manera se pueden compartir programas, datos, impresoras, discos duros y a veces hasta capacidad de procesamiento. Existen muchos tipos de redes, en cuanto a interconexión lógica, física. Se necesita un sistema operativo especial que permita el establecimiento de una red de este tipo.

**Linux:**

Sistema operativo completo, robusto, disponible libremente, que fue desarrollado originalmente por Linus Torvalds.

**Login:**

Programa encargado de la validación de un usuario a la entrada al sistema. Primero pide el nombre del usuario y después comprueba que el password sea el asignado a este.

**Loopback:**

Sistema de trabajo en red en modo local. Con este sistema podemos trabajar en red con nuestro propio ordenador, su utilidad radica en probar programas de seguridad, leer las noticias o el correo de los servidores instalados en nuestro ordenador o simplemente poder ejecutar Xwindow.

**M**

**Multitarea:**

Capacidad de un sistema para el trabajo con varias aplicaciones al mismo tiempo.

**Multiusuario:**

Capacidad de algunos sistemas para ofrecer sus recursos a diversos usuarios conectados a través de terminales.

**Máscara de red:**

Una máscara de red es un conjunto de cuatro números separados por puntos. Cada número se representa normalmente como el equivalente decimal de un número binario de 8 bits, lo que significa que cada número puede tomar valores entre 0 (todos los bits en cero) y 255 (todos los bits en uno). Cada dirección IP consiste de dos partes (la dirección de red y el número de máquina). La máscara de red se usa para determinar el tamaño de cada una de estas partes. Las posiciones de los bits en uno de la máscara se consideran parte del espacio reservado para la dirección de red, mientras que los bits que están puestos a cero se consideran parte del espacio apartado para el número de máquina.

**Memoria:**

Cuando se refiere a ordenadores, la memoria (en general) es cualquier hardware capaz de almacenar datos para recuperarlos posteriormente. En este contexto, la memoria en general se refiere específicamente a la RAM.

**Módem:**

Mode-Demod. Dispositivo que convierte señales analógicas a digitales y viceversa posibilitando la comunicación con las computadoras vía telefónica.

**N****Nombre de dominio:**

El nombre de dominio se utiliza para expresar que las computadoras pertenecen a una determinada organización. Los nombres de dominio son jerárquicos por naturaleza, y cada nivel de la jerarquía se separa de los otros niveles mediante un punto.

## **P**

### **Paquete:**

Fichero que contiene software; está escrito en un cierto formato que permite la fácil instalación y borrado del software.

### **Partición:**

El segmento del espacio de almacenamiento de una unidad de disco que puede accederse como si fuese un disco entero.

### **Password:**

Palabra clave personal, que nos permite el acceso al sistema una vez autenticada con la que posee el sistema en el fichero passwd.

### **Path:**

Variable del entorno, cuyo valor contiene los directorios donde el sistema buscara cuando intente encontrar un comando o aplicación.

### **Permisos:**

El conjunto de identificadores que controlan el acceso a los ficheros. Los permisos constan de tres campos: usuario, grupo y mundo. El campo de usuario controla el acceso del propietario del fichero, y el campo de grupo controla el acceso de cualquiera que concuerda con la especificación de grupo del fichero. Como el nombre implica, el campo mundo controla el acceso de cualquier otro usuario. Cada campo contiene el mismo conjunto de bits que especifican las operaciones que pueden o no realizarse, tales como lectura, escritura y ejecución.

### **Protocolo:**

Un protocolo es una serie de reglas que utilizan dos ordenadores para comunicar entre sí. Cualquier producto que utilice un protocolo dado debería poder funcionar con otros productos que utilicen el mismo protocolo.

**Proxy:**

Servidor que canaliza el acceso a Internet de varios usuarios conectados en red local (en lugar de conectarse cada usuario a Internet por su cuenta se canaliza la conexión de un ordenador)

**R****RAM:**

Sigla de Random Access Memory (Memoria de acceso directo). La RAM se usa para mantener los programas mientras se están ejecutando, y los datos mientras se los procesa. La RAM es volátil, lo que significa que la información escrita en la RAM desaparecerá cuando se apague la alimentación de energía del ordenador.

**RPM:**

Sigla de Red Hat Package Manager (Gestionador de paquetes de Red Hat). Rpm es también el nombre del programa que permite la instalación, actualización y eliminación de paquetes.

**Router:**

Un dispositivo (o programa de software) que maneja la conexión entre dos o más redes. Los ruteadores se encargan de buscar la dirección de destino de los paquetes que pasan por ellos y deciden hacia cual ruta enviarlos.

**Root:**

Persona o personas encargadas de la administración del sistema Tiene TODO el privilegio para hacer y deshacer, por lo que su uso para tareas que no sean absolutamente necesarias es muy peligroso.

**S****Servidor:**

Empresa o puesto al que se conecta nuestro ordenador y que permite el acceso a Internet.

**Switch:**

Dispositivo utilizado para conectar varios equipos informáticos, en redes locales. Más seguro y fiable que el Hub.

**SMB:**

Sigla de Server Message Block (Bloque de mensajes de servidor), SMB es el protocolo de comunicación que usan los sistemas operativos basados en MS-Windows para permitir los recursos compartidos a través de la red.

**Software:**

Programa de ordenador.

**Swap:**

Memoria virtual. Espacio de disco duro que utiliza el kernel en caso de necesitar más memoria de la que tengamos instalada en nuestro ordenador.

**T****TCP/IP(Transmission Control Protocol) / Internet Protocol).**

Familia de protocolos en los que se basan Internet y la mayoría de redes locales.

**Telnet:**

Servicio que nos permite la conexión a otro ordenador de la red, pasando nuestro sistema a ser una terminal de ese ordenador.

**W****WAN (Wide Area Network).**

Red de Área Amplia. Es una red de computadoras que puede estar localizada en un área geográfica muy extensa y puede contener varios miles de computadoras interconectadas por medio de canales de comunicación de alta velocidad. Utilizadas por organizaciones muy grandes.