

ESCUELA SUPERIO POLITÉCNICA DEL LITORAL



ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

## TÓPICO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ANALISTA DE SOPORTE DE  
MICROCOMPUTADORES

TEMA:

ADMINISTRACIÓN Y SEGURIDADES DE REDES  
EMPRESA TAME DEL ECUADOR

MANUAL DE USUARIO

AUTOR:

ARGELIO ROLANDO COROZO COROZO

DIRECTOR:

ANL. FABIÁN BARBOZA

AÑO:

2007

## **AGRADECIMIENTO**

Primeramente le agradezco a Dios a ser supremo en mi vida al que me da la fuerza y la valentía para conseguir mis metas y propósitos, gracias a Dios estoy consiguiendo ahora una muy importante que es graduarme, y también agradezco a todo mi familia en especial a mi Madre por todo lo que significa ella en mi vida y a mis amigos que ayudaron a pesar de tanta dificultades por estar ahí... **Gracias DIOS**

*Argelio Corozo Corozo*



## **DEDICATORIA**

Dedico este logro a Dios al ser supremo en mi vida, sin El esto no hubiera sido posible  
El es todo para mi, a mi madre la que a sido mi soporte en todo momento y a mi  
familia y a alguien en especial...

*Argelio Corozo Corozo*

## **DECLARACIÓN EXPRESA**

La responsabilidad por los hechos, ideas y doctrinas expuestas en este Tópico de Graduación nos corresponden exclusivamente; y el patrimonio intelectual del mismo al EDCOM (*Escuela de Diseño y Comunicación Visual*) de ESPOL (*Escuela Superior Politécnica del Litoral*).


(Reglamentos de Exámenes Y Títulos Profesionales de la ESPOL).

**FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN**



*Ant Fabian Barboza*

## **FIRMA DE AUTOR**

A handwritten signature in dark ink, appearing to read 'Argelio Corozo', is written over a horizontal line.

*Argelio Corozo Corozo*

# ÍNDICE GENERAL

## CAPÍTULO 1

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

## CAPÍTULO 2

<b>2.- SITUACIÓN ACTUAL.....</b>	<b>1</b>
2.1.- ANTECEDENTES.....	1
2.1.1.- <i>HISTORIA</i> .....	1
2.1.2.- <i>MISIÓN</i> .....	2
2.1.3.- <i>VISIÓN</i> .....	2
2.1.4.- <i>OBJETIVOS DEL NEGOCIO</i> .....	2
2.1.5.- <i>ESTRUCTURA ORGANIZACIONAL DE TAME MATRIZ</i> .....	3
2.2.- INFRATRUCTURA LAN.....	4
2.2.1.- <i>MATRIZ DE TAME</i> .....	4
2.3.- RED LAN MATRIZ TAME.....	5
2.4.- CARACTERÍSTICA DE LAS ESTACIONES DE TRABAJO-TAME .....	6
2.4.1.- <i>MATRIZ</i> .....	6
2.4.2.- <i>SUCURSALES</i> .....	7
2.4.2.1.- GERENCIA DE INFORMÁTICA .....	7
2.4.2.2.- GERENCIA DE RECURSOS HUMANOS .....	7
2.4.2.3.- GERENCIA DE PLANIFICACIÓN .....	7
2.4.2.4.- GERENCIA DE LOGÍSTICA .....	7
2.4.2.5.- GERENCIA DE FINANZAS .....	7
2.4.2.6.- PRESIDENCIA EJECUTIVA Y ASESORIA JURÍDICA .....	8
2.4.2.7.- GERENCIA COMERCIAL .....	8
2.4.2.8.- INGRESOS .....	8
2.4.2.9.- PENTHOUSE SALA DE REUNIONES Y CAPACITACIÓN .....	8
2.5.- CARACTERÍSTICA DE LOS SERVIDORES .....	9
2.5.1.- <i>MATRIZ TAME</i> .....	9
2.5.2.- <i>SUCURSALES GUAYAQUIL</i> .....	10
2.6.- ANÁLISIS DE PISO LÓGICO .....	11
2.6.1.- <i>MATRIZ Y SURCURSAL</i> .....	11
2.6.1.2.- GERENCIA DE INFORMÁTICA (PRIMER PISO).....	12
2.6.1.2.- GERENCIA DE RECURSOS HUMANOS (SEGUNDO PISO).....	13
2.6.1.3.- GERENCIA DE PLANIFICACIÓN (TERCER PISO).....	14
2.6.1.4.- GERENCIA DE LOGÍSTICA (CUARTO PISO).....	15
2.6.1.5.- GERENCIA DE FINANZAS (QUINTO PISO) .....	16
2.6.1.6.- PRESIDENCIA EJECUTIVA Y ASESORIA JURÍDICA (SEXTO PISO).....	17
2.6.1.7.- GERENCIA COMERCIAL (SÉPTIMO PISO) .....	18
2.6.1.8.- INGRESOS (OCTAVO PISO).....	19
2.6.1.9.- SALA DE CONFERENCIAS Y SALONES DE CAPACITACIÓN (NOVENO PISO).....	20
2.6.1.10.- GERENCIA DE INFORMÁTICA .....	21
2.6.1.11.- ÁREA DE VENTA DE PASAJES.....	22
2.6.1.12.- GERENCIA DE INFORMÁTICA .....	23
2.6.1.13.- ÁREA DE SISTEMAS .....	24
2.6.1.14.- ÁREA DE VENTAS DE PASAJES (PRIMER PISO).....	25
2.6.1.15.- ÁREA DE SISTEMAS (PRIMER PISO).....	26
2.6.1.16.- RESERVACIONES .....	26
2.7.- ANÁLISIS DE PISO APLICATIVO.....	27
2.7.1.- <i>MATRIZ Y SUCURSAL</i> .....	27
2.7.1.1.- GERENCIA DE INFORMÁTICA .....	27
2.7.1.2.- GERENCIA DE RECURSOS HUMANOS.....	28

2.7.1.3.- GERENCIA DE PLANIFICACIÓN .....	29
2.7.1.4.- GERENCIA DE LOGÍSTICA .....	30
2.7.1.5.- GERENCIA DE FINANZAS .....	31
2.7.1.6.- PRESIDENCIA EJECUTIVA Y ASESORÍA JURÍDICA .....	32
2.7.1.7.- GERENCIA COMERCIAL .....	33
2.7.1.8.- INGRESOS .....	34
2.7.1.9.- SALA DE CONFERENCIAS Y SALONES DE CAPACITACIÓN .....	35
2.7.1.10.- GERENCIA DE INFORMÁTICA .....	36
2.7.1.11.- ÁREA DE VENTA DE PASAJES .....	37
2.7.1.12.- GERENCIA DE INFORMÁTICA .....	38
2.7.1.13.- ÁREA DE SISTEMA .....	39
2.7.1.14.- ÁREA DE VENTAS DE PASAJES .....	40
2.7.1.15.- ÁREA DE SISTEMAS .....	41
2.7.1.16.- RESERVACIONES .....	42
2.8.- CUARTO DE COMUNICACIÓN (MATRIZ-TAME) .....	43
2.9.- MC MATRIZ TAME .....	44
2.10.- IC AGENCIA PRINCIPAL MATRIZ TAME .....	45
2.11.- MEDIOS DE COMUNICACIÓN .....	46
2.11.1.- MEDIOS ALÁMBRICOS .....	46
2.11.2.- TIPO/ ELEMENTOS NETWORKING UTILIZADOS .....	46
2.12.- CARACTERÍSTICAS DE LOS DISPOSITIVOS DE CONMUTACIÓN .....	47
2.12.1.- MATRIZ TAME .....	47
2.13.- INFRASTRUCTURA WAM .....	48
2.13.1.- RED WAN DE LA COMPAÑÍA TAME .....	48
2.14.2.- GRÁFICA DE COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS .....	49
2.15.- DISPOSITIVOS DE ENRUTAMIENTO .....	50
2.15.1.- GUAYAQUIL- JOSE JOAQUIN DE OLMEDO .....	50
2.16.2.- TERMINAL AEREA QUITO .....	50
2.17.- INFRAESTRUCTURA DE SEGURIDAD DE LA REDES WAN TAME .....	51
2.18.- INFRAESTRUCTURA DE COMUNICACIÓN DE INTERNET TAME .....	52
2.19.- PROBLEMAS ENCONTRADOS .....	53

## CAPÍTULO 3

### 3.- SOLUCIÓN PROPUESTA.....1

3.1.- PROBLEMAS ENCONTRADOS .....	1
3.2.- SOLUCIÓN PROPUESTA .....	2
3.3.- ESTUDIO DE FACTIBILIDAD .....	3
3.3.1.- ALTERNATIVA "A" .....	3
3.3.1.1.- FACTIBILIDAD TÉCNICA HARDWARE .....	3
3.3.1.2.- FACTIBILIDAD ECONÓMICA .....	4
3.3.1.2.1.- COSTO HARDWARE .....	4
3.3.1.2.2.- COSTO SOFTWARE .....	4
3.3.1.2.3.- COSTO DE LOS ENLACES .....	4
3.3.1.3.- COSTOS OPERATIVOS .....	5
3.3.1.4.- FACTIBILIDAD OPERATIVA .....	6
3.3.1.5.- VENTAJAS Y BENEFICIOS DE ALTERNATIVA "A" .....	7
3.3.1.5.1.- VENTAJAS .....	7
3.3.1.5.2.- BENEFICIOS .....	7
3.3.1.6.- FORMA DE PAGO Y LAPSO A DESARROLLARSE .....	8
3.3.1.7.- GARANTIA .....	8
3.3.1.8.- CRONOGRAMA DE TRABAJO .....	9
3.3.2.- ALTERNATIVA "B" .....	10
3.3.2.1.- FACTIBILIDAD TÉCNICA .....	10
3.3.2.1.2.- EQUIPOS CÓMPUTOS (PROPIO DE LA EMPRESA) .....	11
3.3.2.1.3.- DISPOSITIVOS DE ALQUILER CON EL ISP .....	11
3.3.2.2.- FACTIBILIDAD ECONÓMICA .....	11
3.3.2.2.1.- COSTO EQUIPOS CÓMPUTOS .....	11
3.3.2.2.2.- COSTO DE ALQUILER .....	11
3.3.2.2.3.- COSTO SOFTWARE .....	11
3.3.2.2.4.- COSTO DE LOS ENLACES PRINCIPALES (INTERPROVINCIAL Y LOCALES) .....	12
3.3.2.3.- COSTOS OPERATIVOS .....	13

3.3.2.4.- FACTIBILIDADES OPERATIVAS.....	14
3.3.2.5.- VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA "B" .....	15
3.3.2.5.1.- VENTAJAS .....	15
3.3.2.5.2.- BENEFICIOS .....	15
3.3.2.6.- FORMA DE PAGO Y LAPSO A DESARROLLARSE.....	16
3.3.2.7.- GARANTIA.....	16
3.3.2.8.- CRONOGRAMA DE TRABAJO .....	17

## CAPÍTULO 4

4.- IMPLEMENTACIÓN MAN .....	1
4.1.- COMUNICACIÓN QUITO GYE .....	1
4.2.- ENLACE MAN GUAYAQUIL Y SUS SUCURSALES.....	2
4.3.- COMUNICACIÓN DE PROTOCOLOS QUITO GYE .....	3

## CAPÍTULO 5

5.- NORMAS Y RECOMENDACIONES.....	1
5.1.- NORMAS.....	1
NORMATIVA 1 .....	1
NORMATIVA 2 .....	2
NORMATIVA 3.....	2
NORMATIVA 4.....	3
NORMATIVA 5 .....	3
NORMATIVA 6.....	4
NORMATIVA 7.....	4
NORMATIVA 8.....	5
NORMATIVA 10.....	6
NORMATIVA 11.....	6
NORMATIVA 12.....	7
NORMATIVA 13.....	7
NORMATIVA 14.....	8
NORMATIVA 15.....	8
NORMATIVA 16.....	9
NORMATIVA 17.....	9
NORMATIVA 18.....	10
NORMATIVA 19.....	10
NORMATIVA 20.....	11
NORMATIVA 21.....	11
NORMATIVA 22.....	12
NORMATIVA 24.....	13
NORMATIVA 25.....	14
NORMATIVA 26.....	14
NORMATIVA 27.....	15
NORMATIVA 29.....	16
NORMATIVA 30.....	16
NORMATIVA 31.....	17
NORMATIVA 33.....	18
NORMATIVA 34.....	18
NORMATIVA 35.....	19
NORMATIVA 36.....	19
NORMATIVA 37.....	20
NORMATIVA 38.....	20
NORMATIVA 39.....	21
NORMATIVA 40.....	22
NORMATIVA 41.....	23
NORMATIVA 42.....	23

NORMATIVA 43.....	24
NORMATIVA 45.....	25
NORMATIVA 46.....	26
NORMATIVA 47.....	26
NORMATIVA 48.....	27
NORMATIVA 49.....	27
NORMATIVA 50.....	28
NORMATIVA 51.....	28
NORMATIVA 52.....	29
NORMATIVA 56.....	31
5.2.- RECOMENDACIONES .....	32
RECOMENDACIÓN 1.....	32
RECOMENDACIÓN 2.....	32
RECOMENDACIÓN 3.....	33
RECOMENDACIÓN 4.....	34
RECOMENDACIÓN 5.....	34
RECOMENDACIÓN 6.....	35
RECOMENDACIÓN 7.....	35
RECOMENDACIÓN 8.....	35
RECOMENDACIÓN 9.....	36
RECOMENDACIÓN 10.....	37
RECOMENDACIÓN 11.....	37
RECOMENDACIÓN 12.....	39
RECOMENDACIÓN 13.....	40
RECOMENDACIÓN 14.....	40

## CAPÍTULO 6

### 6.- LINUX.....

6.1.- INTRODUCCIÓN A FEDORA CORE 3 .....	1
6.2.- CARACTERÍSTICAS DE LINUX FEDORA CORE 3 .....	2
6.3.- REQUERIMIENTOS DE HARDWARE PARA INSTALAR UN SERVIDOR LINUX .....	4
6.3.1.- REQUERIMIENTO HARDWARE MINIMO .....	4
6.3.2.- REQUERIMIENTO HARDWARE ÓPTIMO .....	4
6.4.- CONFIGURACION DESDE EL BIOS.....	5
6.5.- INSTALACIÓN DE LINUX FEDORA CORE 3 .....	9
6.5.1.- INICIO DE LA INSTALACIÓN.....	9
6.5.2.-INSTALACIÓN DE LOS PAQUETES DE SOFTWARE.....	21
6.5.3.- INSTALACIÓN TERMINADA CON ÉXITO.....	25
6.5.4.- CONFIGURACIÓN POST INSTALACIÓN.....	26
6.5.5.- INICIANDO EL SISTEMA OPERATIVO EN AMBIENTE GRÁFICO.....	30
6.5.6.- INICIANDO EL SISTEMA OPERATIVO EN AMBIENTE TEXTO.....	32
6.6.-COMANDOS BASICO DE LINUX CORE 3 .....	33
6.7.- CONFIGURACIÓN DE LA TARJETA DE RED MODO TEXTO .....	35
6.7.1.- CONFIGURACIÓN DE LA TARJETA DE RED MODO GRÁFICO.....	37
6.8.- SAMBA SERVER.....	39
6.8.1.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR SAMBA.....	40
6.8.2.- CONFIGURACIÓN SAMBA SERVER.....	41
6.9.- CONFIGURACIÓN EN EL CLIENTE WINDOWS .....	46
6.10.- CONFIGURACIÓN DNS SERVER.....	49
6.10.1.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR DNS.....	52
6.10.2.- CONFIGURACIÓN DEL SERVIDOR DNS.....	52
6.10.3.- CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	56
6.11.- CONFIGURACIÓN WEB SERVER .....	57
6.11.1.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR WEB .....	58
6.11.2.- CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	64
6.12.- CONFIGURACIÓN MAIL SERVER.....	66
6.12.2.- CONFIGURACIÓN DEL SERVIDOR SENDMAIL .....	68



6.12.3.- CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	72
6.12.4.- PRUEBA DEL CLIENTE AL SERVIDOR.....	79
6.13.- CONFIGURACIÓN DHCP SERVER.....	80
6.13.2.- CONFIGURACIÓN DE UN SERVIDOR DHCP.....	83
6.13.3.- CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	85
6.14.- CONFIGURACIÓN PROXY SERVER.....	88
6.14.1.- BENEFICIOS PROXY SERVER.....	88
6.14.2.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR PROXY.....	89
6.14.3.- CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	95
6.14.4.- RESTRICCIONES POR HORARIO.....	98
6.14.5.- RESTRICCIÓN POR PÁGINAS PROHIBIDAS.....	102
6.15.- CONFIGURACIÓN DE FIREWALL.....	106
6.15.1.- CARACTERÍSTICAS DE UN FIREWALL LINUX.....	107
6.15.2.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR FIREWALL.....	108
6.15.3.- COMO BLOQUEAR EL PING.....	109
6.15.4.- COMO BLOQUEAR FTP.....	109
6.15.5.- COMO BLOQUEAR TELNET.....	109
6.15.6.- HABILITAR TELNET.....	110
6.15.7.- CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	112

## CAPÍTULO 7

7.- ROUTER.....	1
7.1.-CONFIGURACIÓN DE DISPOSITIVOS INTRODUCCIÓN A LOS ROUTERS.....	1
7.1.1.-COMPONENTES INTERNOS DEL ROUTER 5232.....	5
7.2.-CONEXIONES EXTERNAS DEL ROUTER.....	6
7.3.-CONEXIONES DEL PUERTO DE ADMINISTRACIÓN.....	8
7.4.-ENRUTAMIENTO.....	8
7.4.1.-ENRUTAMIENTO ESTÁTICO.....	8
7.4.2.- ENRUTAMIENTO DINÁMICO.....	8
7.4.2.1.- PROTOCOLOS DE ENRUTAMIENTO.....	8
7.5.-CONFIGURACIÓN DEL HYPERTERMINAL.....	10
7.6.-CONFIGURACIONES EN EL ROUTER.....	14
7.6.1.-MODOS DE INTERFAZ DE USUARIO.....	14
7.6.2.- COMANDOS básicos.....	16
7.6.4.- GUARDAR CAMBIOS DEL ROUTER.....	17
7.6.5.- CONFIGURAR NOMBRE DE ROUTERS.....	18
7.6.6.- CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER.....	18
7.6.7.- Asignación DE IP'S A LAS INTERFACES.....	19
7.6.8.- CONFIGURACIÓN DE PROTOCOLOS.....	20
7.6.9.- VECTOR DISTANCIA:.....	20
7.6.10.- ESTADO ENLACE:.....	20
7.6.11.-COMANDOS SHOWS.....	20
7.7.- PROTOCOLOS DE ENRUTAMIENTOS.....	21
7.7.1.-PROTOCOLO DE ENRUTAMIENTO OSPF.....	21
7.7.1.1.-TIPOS DE REDES OSPF.....	22
7.7.1.2.-PROTOCOLO HELLO DE OSPF.....	23
7.8.- OSPF (PROTOCOLO ESTADO ENLACE):.....	24
7.9.- REDISTRIBUCIÓN DE RUTAS.....	25
7.10.-PROTOCOLOS RIP.....	26
7.10.1.-VERSIONES RIP.....	26
7.10.2.-CARACTERÍSTICAS.....	26
7.10.3.-MÁSCARA DE RED DE RIP.....	27
7.10.4.-VERSIÓN 1 DE RIP.....	27
7.10.5.-VERSIÓN 2 DE RIP.....	27
7.10.6.-VENTAJAS Y DESVENTAJAS DE RIP.....	27
7.10.7.-FUNCIONAMIENTO RIP.....	27
7.11.- REDISTRIBUCIÓN DE RUTAS.....	29
7.12.-LISTAS DE CONTROL DE ACCESO (ACL'S).....	30

7.12.1.-FUNCIONAMIENTO DE LAS ACL.....	31
7.12.2.- WILCARD.....	31
7.12.3.- TIPOS.....	32
7.12.3.1.- ACL ESTÁNDAR.....	32
7.12.3.2.- ACL EXTENDIDA.....	32
7.12.4.-CREACIÓN DE LAS ACL.....	34
7.12.5.-UBICACIÓN DE LA ACL.....	34

## 8.- SWITCHES..... 35

8.1.-TECNOLOGÍA.....	35
8.2.-SEGMENTACIÓN.....	36
8.2.1.-ASPECTOS BÁSICOS DE LAS VLAN.....	36
8.2.2.-COLISIÓN.....	37
8.2.3.- ENRUTAMIENTO ENTRE VLAN.....	38
8.2.4.- INTERFACES FÍSICAS Y LÓGICAS.....	39
8.3.- CONFIGURACIÓN DE SWITCH.....	40
8.3.1.- ACCESO A LA APLICACIÓN HYPERTERMINAL.....	40
8.3.1.1.-CONFIGURACIÓN DE VLAN POR DEFECTO.....	44
8.3.1.2.-CREACIÓN DE VLAN'S.....	44
8.3.1.3.- BORRADO DE VLAN'S.....	45
8.3.1.4.-ASIGNACIÓN DE VLAN'S A LOS PUERTOS.....	45
8.3.1.5.- CONFIGURACIÓN DE UN ENRUTAMIENTO DE VLAN.....	45
8.4.-CONFIGURACIÓN DE UN ENRUTAMIENTO ENTRE DISTINTAS VLAN.....	46
8.5.- CONFIGURACIÓN DETALLADAS DE LOS ROUTERS.....	48
8.6.-CONFIGURACIÓN DE LOS ROUTER Y SWICHT.....	49
8.6.1.-ASIGNACIÓN DE NOMBRE AL ROUTER.....	49
8.6.1.1.-ROUTER FRONTERA CORE GUAYAQUIL.....	49
8.6.1.2.-ROUTER MATRIZ GUAYAQUIL.....	49
8.6.1.3.-ROUTER MATRIZ QUITO.....	49
8.6.1.4.-ROUTER (MATRIZ) GUAYAQUIL.....	49
8.6.1.5.-ROUTER (PROVEEDOR DE INTERNET) ISP.....	50
8.6.1.6.-ROUTER (SUCURSAL) TAME CARGO.....	50
8.6.1.7.-ROUTER (SUCURSAL) BUEN DIA.....	50
8.6.1.8.-ROUTER (SUCURSAL) GRAN PASAJES.....	50
8.7.-CONFIGURACIÓN DE LAS INTERFAZ.....	51
8.7.1.-ROUTER FRONTERA GUAYAQUIL.....	51
8.7.2.-ROUTER MATRIZ GUAYAQUIL.....	52
8.7.3.-ROUTER MATRIZ QUITO.....	52
8.7.4.-ROUTER (MATRIZ) GUAYAQUIL.....	53
8.7.5.-ROUTER (PROVEEDOR DE INTERNET) ISP.....	54
8.7.6.-ROUTER (SUCURSAL) TAME CARGO.....	54
8.7.7.-ROUTER (SUCURSAL) BUEN DIA.....	55
8.7.8.-ROUTER (SUCURSAL) GRAN PASAJES.....	55
8.8.-LEVANTAMIENTO DE LAS INTERFACES SERIAL.....	56
8.8.1.-ROUTER FRONTERA GUAYAQUIL.....	56
8.8.2.-ROUTER MATRIZ GUAYAQUIL.....	56
8.8.3.-ROUTER MATRIZ QUITO.....	56
8.8.4.-ROUTER (MATRIZ) GUAYAQUIL.....	57
8.8.5.-ROUTER (PROVEEDOR DE INTERNET) ISP.....	57
8.8.6.-ROUTER (SUCURSAL) TAME CARGO.....	57
8.8.7.-ROUTER (SUCURSAL) BUEN DIA.....	58
8.8.8.-ROUTER (SUCURSAL) GRAN PASAJES.....	58
8.9.-CONFIGURAMOS LAS FASTETHERNET.....	59
8.9.1.-ROUTER (MATRIZ) GUAYAQUIL.....	59
8.9.2.-ROUTER (SUCURSAL) TAME CARGO.....	59
8.9.3.-ROUTER (SUCURSAL) BUEN DIA.....	60
8.9.4.-ROUTER (SUCURSAL) GRAN PASAJES.....	60
8.10.- CONFIGURAMOS TELNET.....	61
8.10.1.-ROUTER FRONTERA GUAYAQUIL.....	61
8.10.2.-ROUTER MATRIZ GUAYAQUIL.....	62

8.10.31.-ROUTER MATRIZ QUITO.....	62
8.10.4.-ROUTER (MATRIZ) GUAYAQUIL.....	63
8.10.5.-ROUTER (PROVEEDOR DE INTERNET) ISP.....	63
8.10.6.-ROUTER (SUCURSAL) TAME CARGO.....	64
8.10.7.-ROUTER (SUCURSAL) BUEN DIA.....	64
8.10.8.-ROUTER (SUCURSAL) GRAN PASAJES.....	65
8.11.-VERIFICACIÓN DE TELNET.....	66
8.11.1.-ROUTER FRONTERA GUAYAQUIL.....	66
8.12.-CONFIGURACIÓN DE LOS PROTOCOLOS ENRUTAMIENTO RIP V2 Y OSPF 1.....	67
8.12.1.-ROUTER FRONTERA GUAYAQUIL (RIP V2 Y OSPF 1).....	67
8.12.2.-ROUTER MATRIZ GUAYAQUIL (OSPF 1).....	68
8.12.3.-ROUTER MATRIZ QUITO (OSPF 1).....	68
8.12.4.-ROUTER (MATRIZ) GUAYAQUIL (OSPF 1).....	68
8.12.5.-ROUTER (PROVEEDOR DE INTERNET) ISP.....	69
8.12.6.-ROUTER (SUCURSAL) TAME CARGO (RIP V2).....	69
8.12.7.-ROUTER (SUCURSAL) BUEN DIA (RIP V2).....	69
8.12.8.-ROUTER (SUCURSAL) GRAN PASAJES (RIP V2).....	70
8.13.-SHOW IP ROUTER.....	71
8.13.1.-ROUTER FRONTERA GUAYAQUIL.....	71
8.13.2.-ROUTER MATRIZ GUAYAQUIL.....	72
8.13.3.-ROUTER MATRIZ QUITO.....	72
8.13.4.-ROUTER (MATRIZ) GUAYAQUIL.....	73
8.13.5.-ROUTER (PROVEEDOR DE INTERNET) ISP.....	73
8.13.6.-ROUTER (SUCURSAL) TAME CARGO.....	73
8.13.7.-ROUTER (SUCURSAL) BUEN DIA.....	74
8.13.8.-ROUTER (SUCURSAL) GRAN PASAJES.....	74
8.14.-PRUEBAS DE PING ENTRE MATRIZ Y SUCURSALES.....	75
8.14.1.-ROUTER FRONTERA GUAYAQUIL.....	75
8.14.2.-ROUTER MATRIZ GUAYAQUIL.....	76
8.14.3.-ROUTER MATRIZ QUITO.....	78
8.14.4.-ROUTER (MATRIZ) GUAYAQUIL.....	79
8.14.5.-ROUTER (PROVEEDOR DE INTERNET) ISP.....	80
8.14.6.-ROUTER (SUCURSAL) TAME CARGO.....	81
8.14.7.-ROUTER (SUCURSAL) BUEN DIA.....	82
8.14.8.-ROUTER (SUCURSAL) GRAN PASAJES.....	83
8.15.-CONFIGURACIÓN DE LAS VLANS.....	84
8.15.1.-CONFIGURACIÓN DE VLANS (SUCURSAL) TAME CARGO.....	84
8.15.1.1.-SWITCH TAME CARGO.....	84
8.15.1.2.-ROUTER (SUCURSAL) TAME CARGO.....	86
8.15.1.3.-HOST DE LA SUCURSALES TAME CARGO.....	86
8.15.2.-CONFIGURACIÓN DE LA VLANS (SUCURSAL) BUEN DIA.....	88
8.15.2.1.-SWITCH BUEN DIA.....	88
8.15.2.2.-ROUTER (SUCURSAL) BUEN DIA.....	90
8.15.2.3.-HOST DE LA SUCURSAL BUEN DIA.....	90
8.15.3.-CONFIGURACIÓN DE VLANS (SUCURSAL) GRAN PASAJES.....	92
8.15.3.1.-SWITCH GRAN PASAJES.....	92
8.15.3.2.-ROUTER (SUCURSAL) GRAN PASAJES.....	94
8.15.3.3.-HOST DE LA SUCURSAL GRAN PASAJES.....	95
8.15.4.-CONFIGURACIÓN DE VLANS MATRIZ GUAYAQUIL.....	96
8.15.4.1.-SWITCH 1 MATRIZ GUAYAQUIL.....	96
8.15.4.2.-SWITCH 2 MATRIZ GUAYAQUIL.....	98
8.15.4.4.-ROUTER MATRIZ GUAYAQUIL.....	102
8.15.4.5.-HOSTS DE LA MATRIZ GYE.....	103

## ÍNDICE DE FIGURA

### CAPÍTULO 2

FIGURA 2 - 1: COMUNICACIÓN MATRIZ-SUCURSALES.....	4
FIGURA 2 - 2: EDIFICIO MATRIZ.....	5
FIGURA 2 - 3: ANÁLISIS DE PISO LÓGICO-PRIMER PISO MATRIZ .....	11
FIGURA 2 - 4: ANÁLISIS DE PISO LÓGICO-SEGUNDO PISO MATRIZ .....	12
FIGURA 2 - 5: ANÁLISIS DE PISO LÓGICO-TERCER PISO MATRIZ .....	13
FIGURA 2 - 6: ANÁLISIS DE PISO LÓGICO-CUARTO PISO MATRIZ .....	14
FIGURA 2 - 7: ANÁLISIS DE PISO LÓGICO-QUINTO PISO LÓGICO MATRIZ .....	15
FIGURA 2 - 8: ANÁLISIS DE PISO LÓGICO-SEXTO PISO MATRIZ .....	16
FIGURA 2 - 9: ANÁLISIS DE PISO LÓGICO-SÉPTIMO PISO MATRIZ.....	17
FIGURA 2 - 10: ANÁLISIS DE PISO LÓGICO-OCTAVO PISO MATRIZ .....	18
FIGURA 2 - 11: ANÁLISIS DE PISO LÓGICO-NOVENO PISO MATRIZ.....	19
FIGURA 2 - 12: ANÁLISIS DE PISO LÓGICO-PRIMER PISO A JJO.....	20
FIGURA 2 - 13: ANÁLISIS DE PISO LÓGICO-SEGUNDO PISO A JJO .....	21
FIGURA 2 - 14: ANÁLISIS DE PISO LÓGICO-PRIMER PISO TAME CARGO.....	22
FIGURA 2 - 15: ANÁLISIS DE PISO LÓGICO-ÁREA DE SISTEMA TAME CARGO .....	23
FIGURA 2 - 16: ANÁLISIS DE PISO LÓGICO-PRIMER PISO BUEN DÍA.....	24
FIGURA 2 - 17: ANÁLISIS DE PISO LÓGICO-PRIMER PISO GRAN PASAJES .....	25
FIGURA 2 - 18: ANÁLISIS DE PISO LÓGICO-RESERVACIONES GRAN PASAJES .....	26
FIGURA 2 - 19: ANÁLISIS DE PISO APLICATIVO -PRIMER PISO MATRIZ.....	27
FIGURA 2 - 20: ANÁLISIS DE PISO APLICATIVO -SEGUNDO PISO MATRIZ .....	28
FIGURA 2 - 21: ANÁLISIS DE PISO APLICATIVO -TERCER PISO MATRIZ .....	29
FIGURA 2 - 21: ANÁLISIS DE PISO APLICATIVO -CUARTO PISO MATRIZ .....	30
FIGURA 2 - 23: ANÁLISIS DE PISO APLICATIVO -QUINTO PISO MATRIZ .....	31
FIGURA 2 - 24: ANÁLISIS DE PISO APLICATIVO -SEXTO PISO MATRIZ .....	32
FIGURA 2 - 25: ANÁLISIS DE PISO APLICATIVO -SÉPTIMO PISO MATRIZ .....	33
FIGURA 2 - 26: ANÁLISIS DE PISO APLICATIVO -OCTAVO PISO MATRIZ .....	34
FIGURA 2 - 27: ANÁLISIS DE PISO APLICATIVO-NOVENO PISO MATRIZ .....	35
FIGURA 2 - 28: ANÁLISIS DE PISO APLICATIVO-PRIMER PISO A JJO.....	36
FIGURA 2 - 29: ANÁLISIS DE PISO APLICATIVO-SEGUNDO PISO A JJO .....	37
FIGURA 2 - 30: ANÁLISIS DE PISO APLICATIVO-FREMIR PISO TAME CARGO.....	38
FIGURA 2 - 38: RED WAN DE LA COMPAÑÍA TAME .....	48
FIGURA 2 - 39: COMUNICACIÓN WAN DE LOS DISPOSITIVO.....	49
FIGURA 2 - 40: SEGURIDAD DE LA RED WAN DE TAME .....	51
FIGURA 2 - 41: COMUNICACIÓN DE INTERNET.....	52

### capítulo 4

FIGURA 4 - 1: COMUNICACIÓN QUITO GYE .....	1
FIGURA 4 - 2: ENLACE MAN GYE Y SUCURSALES .....	2
FIGURA 4 - 3: COMUNICACIÓN DE PROTOCOLOS QUITO GYE.....	3

### CAPÍTULO 5

FIGURA 5 - 1: NORMATIVA 1 .....	1
FIGURA 5 - 2: NORMATIVA 2.....	2
FIGURA 5 - 3: NORMATIVA 3.....	2
FIGURA 5 - 4: NORMATIVA 4.....	3
FIGURA 5 - 5: NORMATIVA 5.....	3
FIGURA 5 - 6: NORMATIVA 6.....	4
FIGURA 5 - 7: NORMATIVA 7.....	4
FIGURA 5 - 8: NORMATIVA 8.....	5
FIGURA 5 - 9: NORMATIVA 9.....	5
FIGURA 5 - 10: NORMATIVA 10 .....	6
FIGURA 5 - 11: NORMATIVA 11 .....	6
FIGURA 5 - 12: NORMATIVA 12 .....	7



FIGURA 5 - 13: NORMATIVA 13 .....	7
FIGURA 5 - 14: NORMATIVA 14 .....	8
FIGURA 5 - 15: NORMATIVA 15 .....	8
FIGURA 5 - 16: NORMATIVA 16 .....	9
FIGURA 5 - 17: NORMATIVA 17 .....	9
FIGURA 5 - 18: NORMATIVA 18 .....	10
FIGURA 5 - 19: NORMATIVA 19 .....	10
FIGURA 5 - 20: NORMATIVA 20 .....	11
FIGURA 5 - 21: NORMATIVA 21 .....	11
FIGURA 5 - 22: NORMATIVA 22 .....	12
FIGURA 5 - 23: NORMATIVA 23 .....	12
FIGURA 5 - 24: NORMATIVA 24 .....	13
FIGURA 5 - 25: NORMATIVA 25 .....	14
FIGURA 5 - 26: NORMATIVA 26 .....	14
FIGURA 5 - 27: NORMATIVA 27 .....	15
FIGURA 5 - 28: NORMATIVA 28 .....	15
FIGURA 5 - 29: NORMATIVA 29 .....	16
FIGURA 5 - 30: NORMATIVA 30 .....	16
FIGURA 5 - 31: NORMATIVA 31 .....	17
FIGURA 5 - 32: NORMATIVA 32 .....	17
FIGURA 5 - 33: NORMATIVA 33 .....	18
FIGURA 5 - 34: NORMATIVA 34 .....	18
FIGURA 5 - 35: NORMATIVA 35 .....	19
FIGURA 5 - 36: NORMATIVA 36 .....	19
FIGURA 5 - 37: NORMATIVA 37 .....	20
FIGURA 5 - 38: NORMATIVA 38 .....	20
FIGURA 5 - 39: NORMATIVA 39 .....	21
FIGURA 5 - 40: NORMATIVA 40 .....	22
FIGURA 5 - 41: NORMATIVA 41 .....	23
FIGURA 5 - 42: NORMATIVA 42 .....	23
FIGURA 5 - 43: NORMATIVA 43 .....	24
FIGURA 5 - 44: NORMATIVA 44 .....	25
FIGURA 5 - 45: NORMATIVA 45 .....	25
FIGURA 5 - 46: NORMATIVA 46 .....	26
FIGURA 5 - 47: NORMATIVA 47 .....	26
FIGURA 5 - 48: NORMATIVA 48 .....	27
FIGURA 5 - 49: NORMATIVA 49 .....	27
FIGURA 5 - 50: NORMATIVA 50 .....	28
FIGURA 5 - 51: NORMATIVA 51 .....	28
FIGURA 5 - 52: NORMATIVA 52 .....	29
FIGURA 5 - 67: NORMATIVA 53 .....	29
FIGURA 5 - 54: NORMATIVA 54 .....	30
FIGURA 5 - 55: NORMATIVA 55 .....	30
FIGURA 5 - 56: NORMATIVA 56 .....	31
FIGURA 5 - 57: NORMATIVA 57 .....	31
FIGURA 5 - 58: RECOMENDACIÓN 1 .....	32
FIGURA 5 - 59: RECOMENDACIÓN 2 .....	32
FIGURA 5 - 60: RECOMENDACIÓN 3 .....	33
FIGURA 5 - 61: RECOMENDACIÓN 4 .....	33
FIGURA 5 - 62: RECOMENDACIÓN 5 .....	34
FIGURA 5 - 63: RECOMENDACIÓN 6 .....	34
FIGURA 5 - 64: RECOMENDACIÓN 7 .....	35
FIGURA 5 - 65: RECOMENDACIÓN 8 .....	35
FIGURA 5 - 66: RECOMENDACIÓN 9 .....	36
FIGURA 5 - 68: RECOMENDACIÓN 10 .....	37
FIGURA 5 - 69: RECOMENDACIÓN 11 .....	38
FIGURA 5 - 70: RECOMENDACIÓN 12 .....	39
FIGURA 5 - 71: RECOMENDACIÓN 13 .....	40
FIGURA 5 - 72: RECOMENDACIÓN 14 .....	40

## CAPÍTULO 6

FIGURA 6 - 1: INTRODUCCIÓN A LINUX .....	1
FIGURA 6 - 2: CONFIGURACIÓN DEL BIOS (SETUP DEL COMPUTADOR).....	5
FIGURA 6 - 3: CONFIGURACIÓN DEL BIOS (FEATURES SETUP).....	6
FIGURA 6 - 4: CONFIGURACIÓN DEL BIOS (ARRANQUE DESDE EL CDROM).....	7
FIGURA 6 - 5: CONFIGURACIÓN DEL BIOS (SAVE & EXIT SETUP, PULSAMOS ENTER).....	8
FIGURA 6 - 6: ARRANQUE DE FEDORA CORE.....	9
FIGURA 6 - 7: PULSAR SKIP .....	10
FIGURA 6 - 8: PANTALLA DE BIENVENIDA A FEDORA .....	10
FIGURA 6 - 9: SELECCIONA EL IDIOMA .....	11
FIGURA 6 - 10: CONFIGURACIÓN DEL TECLADO SPANISH .....	11
FIGURA 6 - 11: TIPO DE INSTALACIÓN .....	12
FIGURA 6 - 12: CONFIGURACIONES DE LAS PARTICIONES .....	13
FIGURA 6 - 13: CONFIGURACIÓN DEL DISCO.....	13
FIGURA 6 - 14: PARTICIÓN BOOT .....	14
FIGURA 6 - 15: PARTICIÓN SWAP.....	14
FIGURA 6 - 16: PARTICIÓN RAÍZ .....	15
FIGURA 6 - 17: CONFIGURACIÓN DEL DISCO.....	16
FIGURA 6 - 18: CONFIGURACIÓN DEL GESTOR DE ARRANQUE .....	17
FIGURA 6 - 19: CONFIGURACIÓN DE LA RED.....	17
FIGURA 6 - 20: CONFIGURACIÓN DEL CORTAFUEGO .....	18
FIGURA 6 - 21: ADVERTENCIA SI HAY O NO CORTAFUEGO.....	18
FIGURA 6 - 22: SOPORTE ADICIONAL DEL IDIOMA .....	19
FIGURA 6 - 23: SELECCIÓN DEL USO DE HORARIO .....	19
FIGURA 6 - 24: CONFIGURACIÓN DE LA CONTRASEÑA ROOT .....	20
FIGURA 6 - 25: SELECCIÓN DE GRUPOS DE PAQUETES .....	1
FIGURA 6 - 26: SELECCIÓN DE PAQUETE DHCP .....	21
FIGURA 6 - 27: LISTO PARA LA INSTALACIÓN.....	22
FIGURA 6 - 28: CONTINUANDO LA INSTALACIÓN.....	22
FIGURA 6 - 29: INSTALACIÓN DE LOS PAQUETES .....	23
FIGURA 6 - 30: INSTALACIÓN DE LOS PAQUETES EN PROCESO.....	23
FIGURA 6 - 31: INSTALACIÓN FINALIZADA .....	24
FIGURA 6 - 32: REINICIO DEL SISTEMA .....	25
FIGURA 6 - 33: GESTOR DE ARRANQUE .....	25
FIGURA 6 - 34: PANTALLA BIENVENIDO .....	26
FIGURA 6 - 35: ACUERDO DE LICENCIA .....	26
FIGURA 6 - 36: CONFIGURACIÓN DE LA FECHA Y HORA .....	27
FIGURA 6 - 37: CONFIGURACIÓN DE LA PANTALLA .....	27
FIGURA 6 - 38: CONFIGURACIÓN DE USUARIO DEL SISTEMA.....	28
FIGURA 6 - 39: CONFIGURANDO TARJETA DE SONIDO .....	28
FIGURA 6 - 40: CDS ADICIONAL.....	29
FIGURA 6 - 41: FINALIZACIÓN DE LA CONFIGURACIÓN.....	29
FIGURA 6 - 42: INGRESANDO EL USUARIO .....	30
FIGURA 6 - 43: INGRESANDO LA CONTRASEÑA .....	30
FIGURA 6 - 44: MODO GRAFICO ESCRITORIO DE LINUX.....	31
FIGURA 6 - 45: MODO TEXTO DE LINUX.....	32
FIGURA 6 - 46: EDITAR EL COMANDO IFCONFIG .....	35
FIGURA 6 - 47: REINICIAR LOS SERVICIOS DE LA TARJETA RED .....	35
FIGURA 6 - 48: INFORMACIÓN DE LA TARJETA DE RED .....	36
FIGURA 6 - 49: CONFIGURACIÓN DE LA TARJETA DE RED .....	37
FIGURA 6 - 50: CONFIGURAR TCP/IP .....	37
FIGURA 6 - 51: LEVANTAR LOS SERVICIOS DE LA TARJETA DE RED .....	38
FIGURA 6 - 52: EDITAR IFCONFIG (VERIFICAR LA IP DEL SERVIDOR).....	38
FIGURA 6 - 53: SAMBA.....	39
FIGURA 6 - 54: PAQUETE SAMBA.....	41
FIGURA 6 - 55: IR AL FICHERO SAMBA.....	41
FIGURA 6 - 56: EDITANDO FICHERO SMB.CONF .....	42
FIGURA 6 - 57: ESPECIFICAR VALORES DEL DIRECTORIO.....	43
FIGURA 6 - 58: LEVANTANDO SERVICIO SAMBA .....	44

FIGURA 6 - 59: CREANDO EL RECURSO A COMPARTIR .....	44
FIGURA 6 - 60: CREAR EL USUARIO SAMBA .....	44
FIGURA 6 - 61: CAMBIANDO DE PROPIETARIO .....	45
FIGURA 6 - 62: LEVANTAR LOS SERVICIOS SAMBA .....	45
FIGURA 6 - 63: ASIGNAR DIRECCIÓN IP .....	46
FIGURA 6 - 64: BUSCANDO AL SERVIDOR .....	46
FIGURA 6 - 65: CONECTADO AL SERVIDOR .....	47
FIGURA 6 - 66: INGRESANDO AL DIRECTORIO.....	47
FIGURA 6 - 67: ABRIR ARCHIVO PRUEBA .....	48
FIGURA 6 - 68: VER EL ARCHIVO PRUEBA.....	48
FIGURA 6 - 69: SERVIDOR DNS .....	49
FIGURA 6 - 70: VERIFICANDO PAQUETES DNS.....	52
FIGURA 6 - 71: CREANDO LAS ZONAS.....	52
FIGURA 6 - 72: COPIAMOS EL ARCHIVO LOCALHOST.ZONE .....	53
FIGURA 6 - 73: INGRESAMOS A LA RUTA VI TAME.COM.ZONE .....	53
FIGURA 6 - 74: EDITAMOS LA ZONA .....	54
FIGURA 6 - 75: COPIANDO LAS ZONAS.....	54
FIGURA 6 - 76: LEVANTANDO SERVICIOS DNS .....	55
FIGURA 6 - 77: AGREGAR DIRECCIÓN AL NAME SERVER.....	55
FIGURA 6 - 78: PING A LA ZONA WWW.TAME.COM .....	55
FIGURA 6 - 79: ASIGNAR DIRECCIÓN DEL SERVIDOR DNS .....	56
FIGURA 6 - 80: HACER PING AL SERVIDOR DNS .....	56
FIGURA 6 - 81: SERVIDOR WEB .....	57
FIGURA 6 - 82: VERIFICAMOS PAQUETE HTTPD .....	59
FIGURA 6 - 83: EDITANDO HTTPD.CONF .....	59
FIGURA 6 - 84: HABILITANDO VARIAS ZONAS .....	60
FIGURA 6 - 85: RUTA DEL SITIO WEB .....	60
FIGURA 6 - 86: INGRESANDO AL DIRECTORIO HTML.....	61
FIGURA 6 - 87: CREANDO EL DIRECTORIO DE NUESTRA PÁGINA .....	61
FIGURA 6 - 88: INGRESANDO AL DIRECTORIO DE NUESTRA PÁGINA .....	61
FIGURA 6 - 89: CREANDO UN ARCHIVO DE PRUEBA .....	62
FIGURA 6 - 90: EDITANDO EL ARCHIVO DE PRUEBA HTML.....	62
FIGURA 6 - 91: CREANDO UN MENSAJE DE PRUEBA HTML .....	62
FIGURA 6 - 92: INICIANDO SERVICIOS HTTPD .....	63
FIGURA 6 - 93: VERIFICANDO LA IP DEL SERVIDOR DNS .....	64
FIGURA 6 - 94: ABRIR EL INTERNET EXPLORER .....	65
FIGURA 6 - 95: PRUEBA EXITOSA DEL WEB SERVER.....	65
FIGURA 6 - 96: SENDMAIL.....	66
FIGURA 6 - 97: VERIFICAMOS PAQUETE DE SENDMAIL .....	68
FIGURA 6 - 98: INGRESAMOS A LA RUTA VI /ETC/MAIL/SENDMAIL.CF .....	68
FIGURA 6 - 99: AGREGANDO LOS PARÁMETROS .....	68
FIGURA 6 - 101: INICIANDO SERVICIOS SENDMAIL .....	69
FIGURA 6 - 102: EDICIÓN ARCHIVO NETWORK .....	69
FIGURA 6 - 103: EDITANDO FICHERO NETWORK .....	70
FIGURA 6 - 104: INGRESANDO PARÁMETROS .....	70
FIGURA 6 - 105: INICIANDO SERVICIOS DOVECOT .....	70
FIGURA 6 - 106: CREAR CUENTAS DE USUARIOS .....	71
FIGURA 6 - 107: CREAMOS USUARIOS EN WINDOWS.....	72
FIGURA 6 - 108: CONFIGURAR UNA CUENTA DE CORREO ELECTRÓNICO.....	73
FIGURA 6 - 109: AGREGAR CORREO ELECTRÓNICO .....	73
FIGURA 6 - 110: ASIGNACIÓN DE NOMBRE A LA CUENTA DE CORREO.....	74
FIGURA 6 - 111: CONFIGURACIÓN DE UNA CUENTA DE CORREO ELECTRÓNICO .....	74
FIGURA 6 - 112: ESPECIFICAR DIRECCIÓN POP3 Y SMTP .....	75
FIGURA 6 - 113: ASIGNACIÓN DE USUARIO Y CONTRASEÑA .....	75
FIGURA 6 - 114: FINALIZACIÓN DE LA CONFIGURACIÓN DE UNA CUENTA DE CORREO.....	76
FIGURA 6 - 115: INGRESAR USUARIO Y CONTRASEÑA .....	76
FIGURA 6 - 116: ENVIADO UN MENSAJE AL SERVIDOR.....	77
FIGURA 6 - 117: MENSAJE DE PRUEBA RECEPTADO DESDE EL SERVIDOR.....	77
FIGURA 6 - 118: ENVIANDO UN MENSAJE AL USUARIO ROOT.....	78
FIGURA 6 - 119: RECIBIENDO UN MENSAJE DEL CLIENTE.....	79

FIGURA 6 - 120: SERVIDOR DHCP .....	80
FIGURA 6 - 121: VERIFICANDO PAQUETE DHCP .....	83
FIGURA 6 - 122: COPIANDO ARCHIVO DHCP .....	83
FIGURA 6 - 123: EDITANDO EL ARCHIVO DHCP.....	83
FIGURA 6 - 124: CONFIGURACIÓN DEL FICHERO DHCP .....	84
FIGURA 6 - 125: CREAMOS UN ARCHIVO LLAMADO DHCPD.LEASES .....	84
FIGURA 6 - 126: INICIAMOS SERVICIOS DHCP .....	84
FIGURA 6 - 127: PROPIEDADES INTERNET EXPLORER .....	85
FIGURA 6 - 128: PROTOCOLOS DE INTERNET (TCP/IP).....	85
FIGURA 6 - 129: CONFIGURACIÓN AUTOMÁTICA.....	86
FIGURA 6 - 130: INGRESANDO AL CMD.....	86
FIGURA 6 - 131: VERIFICACIÓN DE IP ASIGNADA POR EL SERVIDOR DHCP .....	87
FIGURA 6 - 132: SERVIDOR PROXY .....	88
FIGURA 6 - 133: VERIFICANDO PAQUETE SQUID .....	90
FIGURA 6 - 135: CONFIGURACIÓN DEL PUERTO DE SALIDA DEL PROXY .....	91
FIGURA 6 - 136: ASIGNANDO EL ESPACIO DEL DIRECTORIO.....	91
FIGURA 6 - 137: ASIGNANDO UN DIRECTORIO AL PROXY .....	92
FIGURA 6 - 138: PROGRAMA DE AUTENTICACIÓN PARA EL PROXY .....	92
FIGURA 6 - 139: CREANDO LISTA DE CONTROL DE ACCESO .....	93
FIGURA 6 - 140: APLICANDO REGLAS DE CONTROL DE ACCESO.....	93
FIGURA 6 - 141: INICIANDO SERVICIO SQUID.....	94
FIGURA 6 - 142: CREAMOS FICHERO PASSWD.....	94
FIGURA 6 - 143: CREANDO USUARIOS SQUID.....	94
FIGURA 6 - 144: INGRESAMOS A OPCIONES DE INTERNET .....	95
FIGURA 6 - 145: INGRESANDO A LA CONFIGURACIÓN LAN .....	95
FIGURA 6 - 146: INGRESANDO LA IP DEL SERVIDOR Y EL PUERTO DE SALIDA .....	96
FIGURA 6 - 147: INGRESAR USUARIO Y CONTRASEÑA .....	96
FIGURA 6 - 148: PRUEBA EXITOSA DE LA CONFIGURACIÓN PROXY.....	97
FIGURA 6 - 149: INGRESAMOS A LA CONFIGURACIÓN DEL SQUID .....	98
FIGURA 6 - 150: CREANDO LISTA DE CONTROL DE ACCESO .....	99
FIGURA 6 - 151: REGLAS DE CONTROL DE ACCESO POR HORARIO .....	100
FIGURA 6 - 152: RENICIANDO SERVICIO SQUID .....	100
FIGURA 6 - 153: PRUEBA EXITOSA DEL PROXY POR HORA .....	101
FIGURA 6 - 154: INGRESAMOS A LA CONFIGURACIÓN DEL SQUID .....	102
FIGURA 6 - 155: CREANDO LISTA DE CONTROL DE ACCESO .....	102
FIGURA 6 - 156: REGLAS DE CONTROL DE ACCESO POR SITIO DENEGADO .....	103
FIGURA 6 - 157: CREANDO ARCHIVO PARA LOS SITIOS DENEGADOS.....	103
FIGURA 6 - 158: EDITANDO ARCHIVO DE SITIOS DENEGADOS.....	104
FIGURA 6 - 160: REINICIAR SERVICIO SQUID .....	105
FIGURA 6 - 161: PRUEBA EXITOSA DE PÁGINAS PROHIBIDAS .....	105
FIGURA 6 - 162: SERVIDOR FIREWALL.....	106
FIGURA 6 - 163: BLOQUEO DEL PING .....	109
FIGURA 6 - 164: BLOQUEO DE FTP.....	109
FIGURA 6 - 165: BLOQUEO TELNET .....	109
FIGURA 6 - 166: VERIFICANDO EL ESTADO DE TELNET .....	110
FIGURA 6 - 167: INGRESAR AL DIRECTORIO CD /ETC .....	110
FIGURA 6 - 168: INGRESAR AL DIRECTORIO CD XINETD.D/ .....	110
FIGURA 6 - 169: INGRESAR A LA RUTA KBR5-TELNET .....	111
FIGURA 6 - 170: EDITANDO SERVICIOS TELNET .....	111
FIGURA 6 - 171: SESTEANDO EJECUTAR .....	112
FIGURA 6 - 172: INGRESANDO A CMD .....	113
FIGURA 6 - 173: BLOQUEO PING Y TELNET .....	113
FIGURA 6 - 175: HABILITADO PING .....	114
FIGURA 6 - 176: HABILITADO TELNET .....	114



## CAPÍTULO 7

FIGURA 7 - 1: ROUTER .....	1
FIGURA 7 - 2: PARTE INTERNA .....	2
FIGURA 7 - 3: PARTE EXTERNA.....	5
FIGURA 7 - 4: CONEXIÓN A LA TERMINAL .....	7
FIGURA 7 - 5: ESQUEMA DE COMUNICACIÓN .....	9
FIGURA 7 - 6: ABRIR HIPERTERMINAL .....	10
FIGURA 7 - 7: NUEVA CONEXIÓN.....	10
FIGURA 7 - 8: CONEXIÓN TAME.....	11
FIGURA 7 - 9: CONEXIÓN CABLE ROLLOVER.....	11
FIGURA 7 - 10: CONFIGURAR LOS BITS .....	12
FIGURA 7 - 11: CONFIGURAR LOS BITS .....	13
FIGURA 7 - 12: MONITOREANDO EL ROUTER .....	14
FIGURA 7 - 13: MODO PRIVILEGIADO .....	15
FIGURA 7 - 16: LISTA DE ACCESO.....	17
FIGURA 7 - 17: UBICACION DE LA ACL .....	20
FIGURA 7 - 18: SWITCHS .....	21
FIGURA 7 - 19: VLAN'S .....	22
FIGURA 7 - 20: ENRRUTAMIENTO.....	38
FIGURA 7 - 21: COMUNICACIÓN DE VLAN'S .....	38
FIGURA 7 - 22: INTERFACES FISICA Y LOGICAS .....	39
FIGURA 7 - 24: MENÚ INICIO.....	40
FIGURA 7 - 23: ENTORNO DE WINDOWS .....	40
FIGURA 7 - 25: SELECCIÓN DE PROGRAMA (HIPERTERMINAL) .....	41
FIGURA 7 - 26: NUEVA CONEXIÓN .....	41
FIGURA 7 - 27: CONEXIÓN CABLE ROLLOVER .....	42
FIGURA 7 - 28: PROPIEDADES DE COM 1 .....	43
FIGURA 7 - 29: CONEXIÓN AL SWITCH 1 .....	44
FIGURA 7 - 30: CONFIGURACIÓN DE ENRRUTAMIENTO.....	46
FIGURA 7 - 31: ENLACE QUITO GYE.....	46
FIGURA 7 - 32: CONFIGURACIÓN DEL HOST .....	86
FIGURA 7 - 33: PING A LA SUBINTERFACES .....	87
FIGURA 7 - 34: CONFIGURACIÓN DEL HOST .....	90
FIGURA 7 - 35: PING A LA SUBINTERFACES .....	91
FIGURA 7 - 36: CONFIGURACIÓN DEL HOST .....	95
FIGURA 7 - 37: PING A LA SUBINTERFACAS .....	96
FIGURA 7 - 38: CONFIGURAMOS EL HOST.....	104
FIGURA 7 - 39: CONFIGURAMOS EL HOST .....	105
FIGURA 7 - 40: CONFIGURAMOS EL HOST .....	106
FIGURA 7 - 41: PING A LAS SUBINTERFACES .....	106

## ÍNDICE DE TABLA

### CAPÍTULO 2

TABLA 2 - 1 CARACTERÍSTICA DE LAS ESTACIONES DE TRABAJO .....	6
TABLA 2 - 2 ESTACIONES DE TRABAJO (GERENCIA DE INFORMÁTICA).....	7
TABLA 2 - 3 ESTACIONES DE TRABAJO (GERENCIA DE RECURSOS HUMANOS) .....	7
TABLA 2 - 4 ESTACIONES DE TRABAJO (GERENCIA DE PLANIFICACIÓN) .....	7
TABLA 2 - 5 ESTACIONES DE TRABAJO (GERENCIA LOGISTICA).....	7
TABLA 2 - 6 ESTACIONES DE TRABAJO .....	7
TABLA 2 - 7 ESTACIONES DE TRABAJO (PRESIDENCIA EJECUTIVA Y ASESORIA JURÍDICA) .....	8
TABLA 2 - 8 ESTACIONES DE TRABAJO (GERENCIA COMERCIAL) .....	8
TABLA 2 - 9 ESTACIONES DE TRABAJO (INGRESOS) .....	8
TABLA 2 - 10 ESTACIONES DE TRABAJO (PENTHOUSE SALA DE REUNIONES Y CAPITACIONES) .....	8
TABLA 2 - 11 CARACTERISTICA DE LOS SERVIDORES .....	9
TABLA 2 - 12 MEDIOS DE COMUNICACIÓN.....	46
TABLA 2 - 13 DISPOSITIVO DE CONMUTACIÓN .....	47
TABLA 2 - 14 DISPOSITIVO DE ENRRUTAMIENTO.....	50
TABLA 2 - 15 DISPOSITIVO DE ENRUTAMIENTO.....	50

### CAPÍTULO 3

TABLA 3 - 16 PROBLEMAS ENCONTRADOS .....	1
TABLA 3 - 17 SOLUCIÓN PROPUESTA.....	2
TABLA 3 - 18 FACTIBILIDAD TÉCNICA.....	3
TABLA 3 - 19 COSTO DE HARDWARE .....	4
TABLA 3 - 20 COSTO DE SOFTWARE .....	4
TABLA 3 - 21 COSTO DE ENLACES .....	4
TABLA 3 - 22 COSTO OPERATIVO .....	5
TABLA 3 - 23 FACTIBILIDAD OPERATIVA.....	6
TABLA 3 - 24 COSTO TOTALES .....	7
TABLA 3 - 25 FACTIBILIDAD TÉCNICA .....	10
TABLA 3 - 26 ALQUILER DEL ROUTER PRINCIPAL .....	11
TABLA 3 - 27 COSTO DE EQUIPOS DE COMPUTO.....	11
TABLA 3 - 28 COSTO DE ALQUILER DE DISPOSITIVOS .....	11
TABLA 3 - 29 COSTO DE SOFTWARE .....	11
TABLA 3 - 30 COSTO DE ENLACES PRINCIPAL.....	12
TABLA3 - 31 COSTO OPERATIVO .....	13
TABLA3 - 32 FACTIBILIDAD OPERATIVAS.....	14
TABLA 3 - 33 COSTO TOTAL DE LA ALTERNATIVA B.....	15

### CAPÍTULO 5

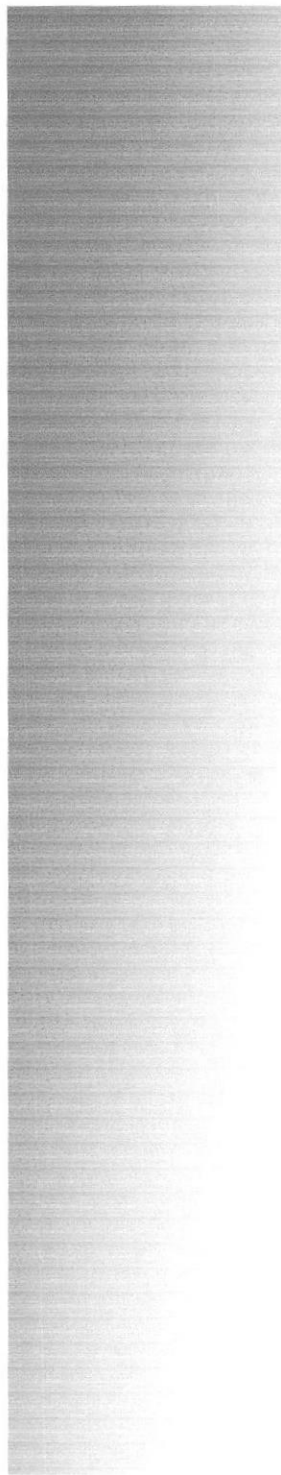
TABLA 5 - 1 LEYENDA.....	1
TABLA 5 - 2 ASIGNAR IDENTIFICACION .....	30
TABLA 5 - 3 PERIODO DE PLANIFICACIÓN DE LA FIBRA OPTICA .....	37

### CAPÍTULO 6

TABLA 6 - 1: REQUERIMIENTO DE HARDWARE MINIMO.....	4
TABLA 6 - 2: REQUERIMIENTO DE HARDWARE OPTIMO .....	4
TABLA 6 - 3: COMANDOS BÁSICOS DE LINUX .....	34
TABLA 6 - 4: DÍAS DETERMINADOS EN LETRAS .....	98

# CAPÍTULO 7

TABLA 7 - 1: COMANDOS BÁSICOS DE ROUTER.....	17
TABLA 7 - 2: COMANDOS SHOW.....	20
TABLA 7 - 3: RANGO ESPECIFICO DE ACL.....	33
TABLA 7 - 4: COMANDO PARA ASIGNAR NOMBRE .....	50
TABLA7 - 5: COMANDOS PARA CONFIGURA LAS INTERFACES.....	55
TABLA7 - 6: COMANDO PARA LEVANTAR LAS INTERFACES .....	58
TABLA 7 - 7: COMANDOS PARA LEVANTAR LAS INTERFACES .....	60
TABLA 7 - 8: COMANDO PARA LOS PROTOCOLOS DE ENRRUTAMIENTO .....	70



# CAPÍTULO 1

## GENERALIDADES

## **1.- GENERALIDADES**

### **1.1.- INTRODUCCIÓN**

En este topico de graduación, se realizo un estudio exhaustivo de las comunicaciones MAN y WAN la Empresa TAME, y este manual se detalla paso a poso.

- En el primer capítulo esta lo que son las generalidades de este manual
- En el segundo capítulo se describe la situación de la empresa TAME
- En el tercer capítulo se da solucionan a los problema ofreciendo una propuesta
- En el cuarto capítulo se presenta la implementacion MAN WAN que e realizado
- En el quinto capítulo se muestra las normativa y recomendaciones par una empresa
- En el sexto capítulo se puede apreciar las configuraciones realizadas en Linux fedora core 3 para manejo de Internet
- En séptimo capítulo se muestra las configuraciones realizadas en los router

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

EL objetivo de este manual es guiar a los usuarios interesados como al personal encargado del manejo y administración del área de redes, entre los temas que se detallaran en los capítulos más adelante tenemos:

- Conocer la realización de un estudio de Cableado Estructurado
- Conocer las configuraciones realizadas en los routers
- Guía para conocer el entorno de Linux.
- Guía para conocer los comandos de Linux.
- Conocer el alcance de todas las configuraciones en Linux, por medio de una explicación detallada e ilustrada de cada una que lo conforman.

### **1.3.- A QUIÉN VA DIRIGIDO ESTE MANUAL**

Este manual esta orientado a los Usuarios Finales involucrados en el Área de Redes que requieran hacer configuraciones para la navegación por Internet

## **1.4.- LO QUE DEBE CONOCER**

Los conocimientos mínimos que deben tener las personas que utilicen este manual deben ser:

- Conocimiento básico de windows
- Concepto básicos de redes y sistema operativos
- Conocimiento básicos de informática basados en el ambiente de internet



## CAPÍTULO 2

### SITUACIÓN ACTUAL



## **2.- SITUACIÓN ACTUAL**

### **2.1.- ANTECEDENTES**

#### **2.1.1.- HISTORIA**

TAME es una empresa de transporte aéreo de pasajeros y carga como una entidad adscrita a la Fuerza Aérea Ecuatoriana con autonomía administrativa y financiera. Se creó mediante Decreto Supremo N° 1020 publicado en el Registro Oficial N° 272 del 18 de junio de 1964. El 17 de diciembre de 1962 fue creada TAME, por iniciativa de la Fuerza Aérea, de ahí que el significado de su nombre era Transportes Aéreos Militares Ecuatorianos. En agosto de 1996 el Congreso Nacional aprueba un cambio en su razón social y se convierte en TAME, LINEA AEREA DEL ECUADOR, aspecto necesario para proyectar su imagen aerocomercial en el ámbito internacional.

La vinculación con esta importante rama de las Fuerzas Armadas, imprimió a su gestión empresarial, desde sus inicios, ciertas características fundamentales, como son la disciplina, seriedad y capacidad de servicio, aspectos que tornaron su personalidad y fueron factor decisivo en los éxitos alcanzados.

TAME es una empresa del sector público, adscrita a la Fuerza Aérea Ecuatoriana, con autonomía administrativa y financiera. La estrecha vinculación de TAME con la Fuerza Aérea Ecuatoriana ha favorecido para contar con personal técnicamente calificado, que provenía de las filas de la institución castrense, especialmente en los mandos directivos y los que han requerido de especialización. TAME nace con un equipo no superior a las 20 personas y con una estructura bien delineada en donde tenía prioridad la Dirección establecida en la capital de la República, Quito y la Subdirección en la ciudad más importante desde el punto de vista comercial, Guayaquil; además de las secciones: Administrativa, Operaciones, Auditoría, Aéreo expresos y atención al público.

Actualmente, la estructura de TAME tiene en sus más altos niveles de representatividad al Directorio, Presidente y Vicepresidente Ejecutivo; 5 Direcciones especializadas en el nivel Asesor que son: Legal, Auditoría Interna, Relaciones Públicas y Planificación; y 8 Gerencias que son: Financiera, Sistemas de Información, Recursos Humanos, Logística, Comercial, Operaciones, Mantenimiento y Regional. Además cuenta con oficinas en cada una de los destinos a los que opera a nivel nacional, esto es en 14 ciudades del Ecuador.

Considerando el avance tecnológico de la industria aeronáutica fue necesario revisar y actualizar el conjunto de normas y disposiciones administrativas y financieras vigentes, a fin de crear una administración autónoma y ágil para el mejoramiento del servicio aerocomercial, por este motivo el Congreso Nacional expidió la Ley constitutiva de la empresa de aviación TAME.



**2.1.2.- MISIÓN**

Proporcionar transporte aéreo –comercial Nacional e Internacional, con aviones modernos, garantizando a sus clientes altos estándares de calidad, eficiencia y seguridad.

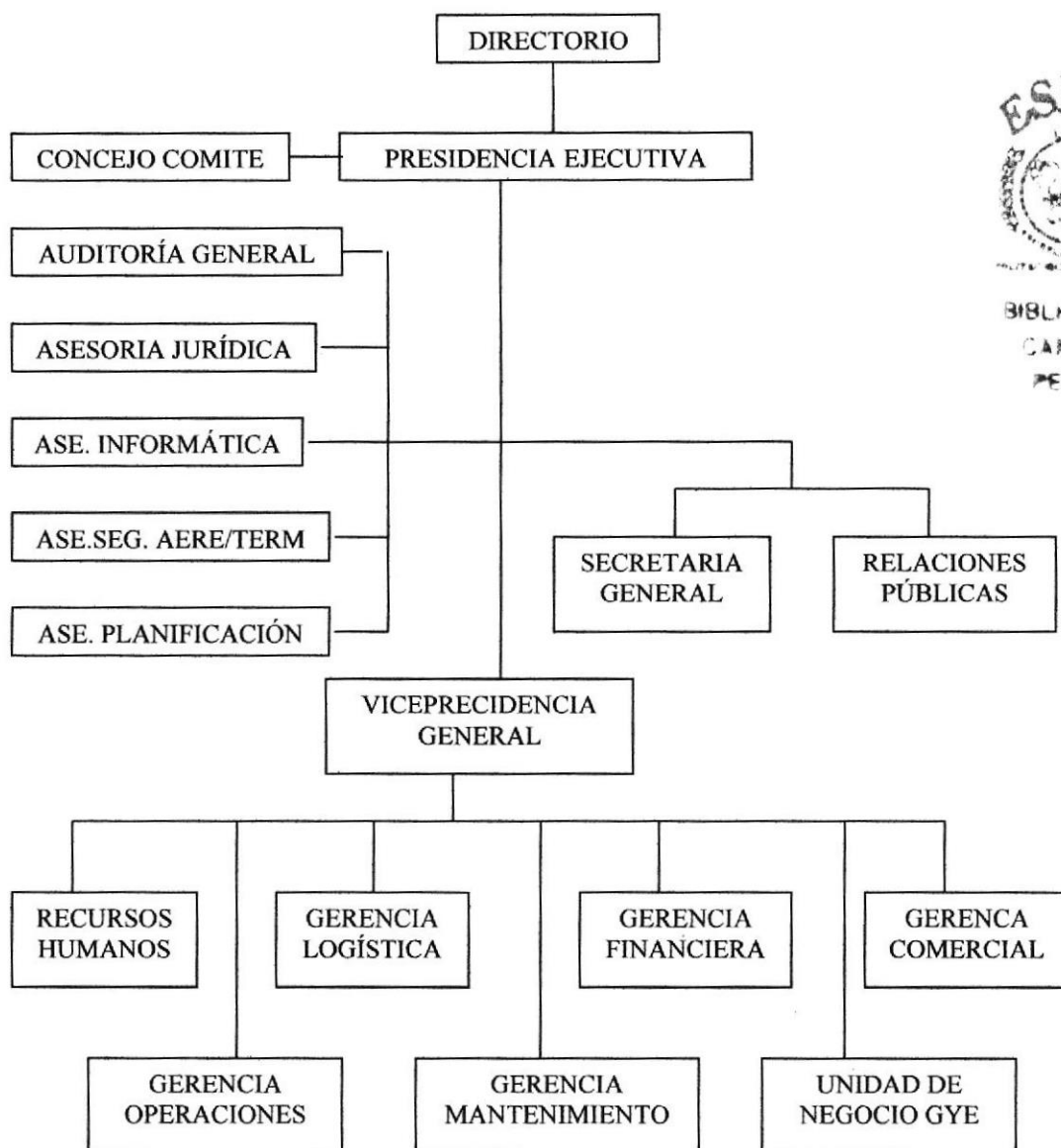
**2.1.3.- VISIÓN**

Mantener el liderazgo nacional, ser preferida por la calidad de su servicio y proyectarse internacionalmente.

**2.1.4.- OBJETIVOS DEL NEGOCIO**

Los objetivos de TAME son el operar con sus aeronaves en el transporte aerocomercial con las frecuencias y en las rutas autorizadas por las autoridades aeronáuticas, tanto en el país como en el exterior.

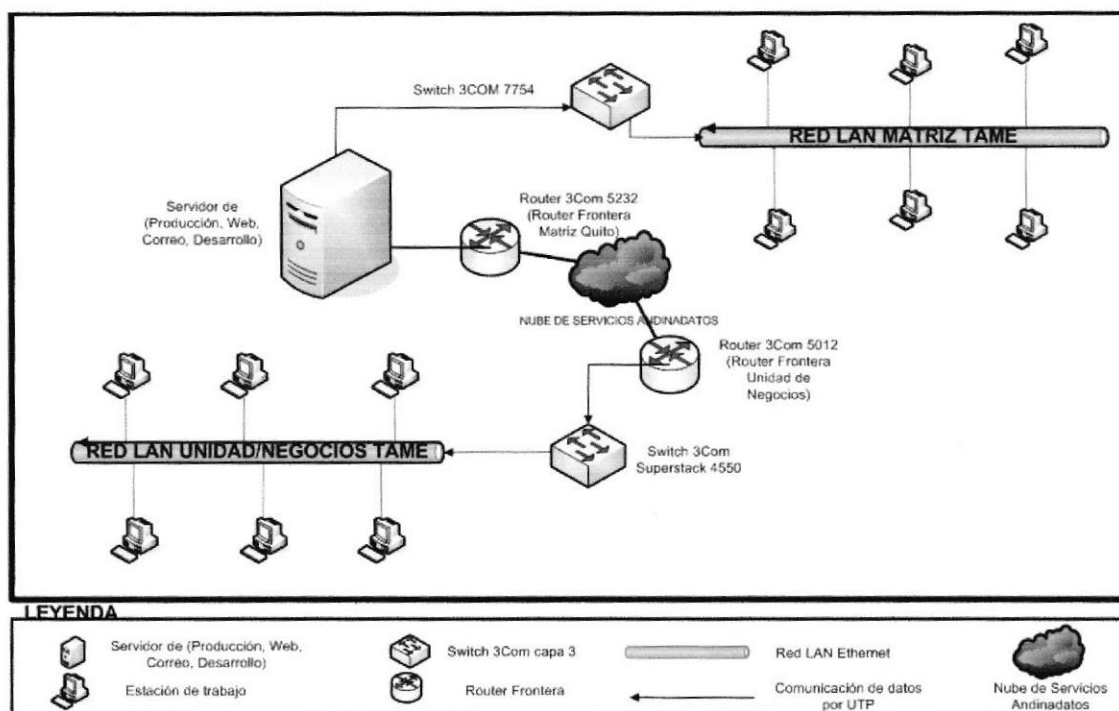
## 2.1.5.- ESTRUCTURA ORGANIZACIONAL DE TAME MATRIZ



## 2.2.- INFRASTRUCTURA LAN

### 2.2.1.- MATRIZ DE TAME

Para tener una idea clara de cómo es la comunicación entre la Matriz de TAME en la ciudad de Quito con las diferentes Agencias o Unidades de Negocios y Puntos de Ventas que se encuentran Ubicadas a Nivel Nacional, y a donde llega la Aerolínea, se utiliza una grafica sencilla, pero explicita de cuales son los principales dispositivos de telecomunicaciones que intervienen en dicho enlace y el medio que utilizan para ello



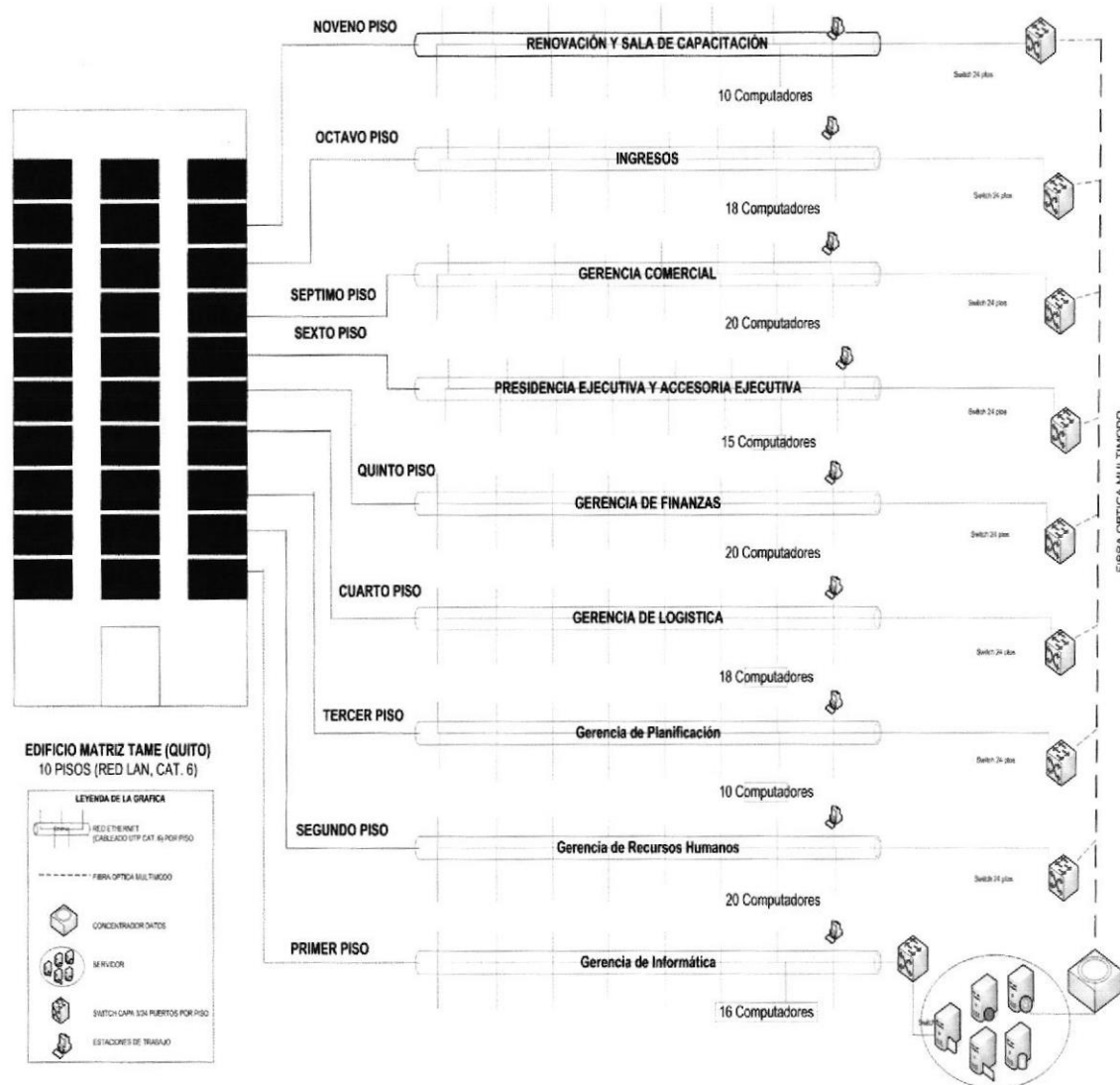
**FIGURA 2 - 1: Comunicación Matriz-Sucursales**

Cabe indicar que la Matriz de TAME esta ubicada en un edificio de 9 pisos, siendo el primer piso, en donde se encuentra ubicado la Gerencia de Informática que podría decirse es el Corazón de La RED WAN, conformadas las LAN instaladas en los diferentes pisos que conforman esta Matriz, las mismas que se comunican entre si por medio del uso de switch capa 3 marca 3com, utilizando como medio físico un cableado UTP categoría 6, manejando como esquema una topología tipo estrella, tanto a Nivel de WAN como LAN.

## 2.3.- RED LAN MATRIZ TAME

Actualmente la matriz de TAME, se encuentra ubicada en un edificio de 9 pisos, ubicado en las calles Amazonas y Colon, en la ciudad de Quito, cada piso de este edificio esta conformado por las diferentes Gerencias Administrativas de la Empresa.

Para tener una idea clara, de cómo se encuentra distribuida la red local de la Matriz de TAME, presentaremos el siguiente grafico:



**FIGURA 2 - 2: Edificio Matriz**

A continuación realizaremos un análisis de cada uno de los pisos que conforman esta MATRIZ, así como de las diferentes Agencias que conforman la Unidad de Negocio Guayaquil, para determinar los problemas a nivel comunicaciones (enlaces UIO - GYE) que existen actualmente.

## 2.4.- CARACTERÍSTICA DE LAS ESTACIONES DE TRABAJO-TAME

### 2.4.1.- MATRIZ

La estaciones de trabajo de la empresa TAME cuenta en todos los departamentos con las mismas características de sus PC

UBICACION	CANT / PC	TIPO/ MARCA	SISTEMA OPERATIVO	CARACTERISITICAS
GERENCIA	1	LAPTOP IBM	WINDOWS XP PRO.	PROCESADOR 2.8 GHZ., MEMORIA 512 MB, HD 80 GBytes DISCO DURO 40 GB T.RED 10/100 MBPS
AREA/ SOPORTE TECNICO,	3	PC CLONES PENTIUM 4	WINDOWS XP PRO.	PROCESADOR 2.4 GHZ., MEMORIA 256MB, HD 80 GBytes DISCO DURO 40 GB T.RED 10/100 MBPS
AREA/ DESARROLLO, OPERADOR/ RECEPCION AS400 AREA/VENTAS	21	PC HP/ PENTIUM 4	WINDOWS XP PRO.	

**Tabla 2 - 1** Característica de las estaciones de trabajo

**2.4.2.- SUCURSALES****2.4.2.1.- GERENCIA DE INFORMÁTICA**

UBICACIÓN	CANTIDAD
GERENCIA DE INFORMÁTICA	2
AREA DE SISTEMAS	5
AREA DE DESARROLLO	2
AREA DE VENTA DE PASAJES	8

**Tabla 2 - 2** Estaciones De Trabajo (Gerencia de Informática)**2.4.2.2.- GERENCIA DE RECURSOS HUMANOS**

UBICACIÓN	CANTIDAD
RECURSOS HUMANOS	2
JEFATURA ADMINISTRATIVA	1
DPTO. DE CAPACITACIÓN	2
AREA DE SERVICIOS SOCIALES	2
AREA DE ROLES DE PAGO	2

**Tabla 2 - 3** Estaciones De Trabajo (Gerencia de Recursos Humanos)**2.4.2.3.- GERENCIA DE PLANIFICACIÓN**

UBICACIÓN	CANTIDAD
GERENCIA LOGÍSTICA	15
GERENCIA	5

**Tabla 2 - 4** Estaciones De Trabajo (Gerencia de Planificación)**2.4.2.4.- GERENCIA DE LOGÍSTICA**

UBICACIÓN	CANTIDAD
GERENCIA DE PLANIFICACIÓN	18

**Tabla 2 - 5** Estaciones De Trabajo (Gerencia Logística)**2.4.2.5.- GERENCIA DE FINANZAS**

UBICACIÓN	CANTIDAD
GERENCIA DE FINANZAS	30

**Tabla 2 - 6** Estaciones De Trabajo

**2.4.2.6.- PRESIDENCIA EJECUTIVA Y ASESORIA JURÍDICA**

UBICACIÓN	CANTIDAD
ASESORÍA JURIDICA	18

**Tabla 2 - 7** Estaciones De Trabajo (Presidencia Ejecutiva y Asesoría Jurídica)**2.4.2.7.- GERENCIA COMERCIAL**

UBICACIÓN	CANTIDAD
GERENCIA COMERCIAL	5
RELACIONES PUBLICA	5
SERVICIO AL CLIENTE	5
MARKETING	5

**Tabla 2 - 8** Estaciones De Trabajo (Gerencia Comercial)**2.4.2.8.- INGRESOS**

UBICACIÓN	CANTIDAD
INGRESOS	18

**Tabla 2 - 9** Estaciones De Trabajo (Ingresos)**2.4.2.9.- PENTHOUSE SALA DE REUNIONES Y CAPACITACIÓN**

UBICACIÓN	CANTIDAD
SALONES DE CAPACITACIÓN	10
SALA DE CONFERNCIA	3

**Tabla 2 - 10** Estaciones De Trabajo (Penthouse Sala de Reuniones y Capitaciones)

## 2.5.- CARACTERÍSTICA DE LOS SERVIDORES

### 2.5.1.- MATRIZ TAME

A continuación se detalla los diferentes Servidores que se encuentran ubicados en la Gerencia de Informática

SERVIDOR MARCA Y MODELO	DISCO DURO	MEMORIA RAM	PROCESADOR	TARJETA RED	USO	SISTEMA OPERATIVOS	APLICACIONES
IBM-AS400 (9406825)	732 GB (18 DISCOS)	8 GB	2473 CPW3600	ETHERNET PCI 10/100 BITS	PRODUCCION	OS400 V5 R3	SISTEMA INTEGRADO CORPORATIVO
	356 GB (BACKUP)			MOD 287F-001			SIGETAME
	356 GB (APLICACIONES)						
IBM-AS400 (9402810)	350 GB( 10 DISCOS)	4 GB	2466 CPW1020	ETHERNET PCI 10/100 MBITS	DESARROLLO	OS400 V5 R2	DB2 (BASE/DATOS IBM)
	175 GB (BACKUP)			MOD 2849001			SNAP HERRAMIENTA DISEÑO PARA APLICACIONES)
	175 GB (APLICACIONES)						
IBM-AS400 (9402810)	210 GB(6 DISCOS)	1.5 GB	2466 CPW1020	ETHERNET PCI 10/100 MBITS	CORREO Y APLICACIONES WEB	OS400 V5 R2	DOMINIO (ADMINISTRADOR CORREO)
	105 GB (BACKUP) Y 105 GB (APLICACIONES)			MOD 2849001			INTERFAZ BAJO WINDOWS PARA ADMINISTRACION DE USUARIOS DE CORREO LOTUS NOTES
SERVIDOR INETSERVER (FIREWALL)	20 GB	256 MB		INCORPORADO	ADMINISTRADOR DE INTERNET		FIREWALL (CISCO PIX)
				PUERTO PARA RED LAN Y WAN			
SERVIDOR MULTIPLE	40 GB	1 GB	2,6 INTEL	TARJETA ETHERNET PCI 10/100 MBITS	ADMINISTRACION DE APLICACIONES WEB	WINDOW 2003	RESOL IT (HELPDESK), ISOMANAGER, BASE/DATOS SQL, CORREO LOTUS NOTES HOST ONDEMAN
SERVIDOR (PC_CLON)	10 GB (2 DISCOS)	1 GB	24 Ghz. INTEL XEON	TARJETA GENERICA ETHERNET PCI 10/100 MBITS	ADM. DEL DOMINIO DE TAME NET	WINDOW 2003 (SERVIPACK 1)	ADM. DE DOMINIO DE TAME NET(CREACION Y ADM. DE USUARIOS EN EL DOMINIO)
	40 GB Y 60 GB						ADM. ANTIVIRUS (SYMANTEC)

**Tabla 2 - 11** Característica de los Servidores



**2.5.2.- SUCURSALES GUAYAQUIL**

A Excepción del resto de agencias, la Ciudad de Guayaquil, cuenta con una Agencia Principal, sucursal o Unidad de Negocios, que se encuentra conformada por un numero de estaciones de trabajo mayor a 50 las mismas que componen 2 redes utilizadas tanto en el área Operativa como en el Área Administrativa, trabajando de manera independiente una de la otra y de la misma manera se comunican con los routers de la Matriz Quito, para poder usar los servicios que proveen ellos a través de sus diferentes aplicaciones; debido a esto procederemos a graficar como están compuestas estas 2 redes, así como su comunicación con la Matriz de TAME.

La unidad de Negocios Guayaquil, a nivel organizacional esta conformada de la siguiente manera:

Área Administrativa: Compuesta por una red local con 32 computadores, 3 switches de 24 puertos cada uno y un ruteador que provee un canal de comunicación con un ancho de banda de 256 kbps, el mismo que maneja el 50% para el uso de Internet es decir 128kbps y el otro 50% para el manejo de aplicaciones propias del sistema integrado que maneja la empresa, este canal de comunicaciones se encuentra entrelazado a través de una serie de nodos (ruteadores), interconectados por diferentes medios, tales como Cobre y Fibra Óptica; estos equipos actualmente se encuentran ubicados en diferentes oficinas tanto de pacifictel como de Andinadatos a nivel nacional, llegando hasta las oficinas de la Matriz de TAME en Quito, donde se encuentran los servidores.

Esta unidad de negocios se encuentra ubicada en el Centro de Guayaquil, en el Edificio Gran Pasaje (condominio Atahualpa 6to. piso) Atahualpa, 6to. Piso y Mezanine) y se encuentra integrada por los Dpto. de Jefe de la Unidad de Negocios y Secretaria, Contabilidad, Tesorería, Personal, Logística, Ventas, Comercial, Reservas e Informática, y es aquí, el lugar donde se encuentran ubicados los equipos de comunicación tanto de la red local (switches) como de la red Wan (ruteador).

La Adicional a esta red, podemos mencionar que dentro del perímetro de la antigua Terminal aérea, todavía se encuentra funcionando, la red local, que pertenece al área de carga y Servicios Aeroportuarios de la empresa, la cual se encuentra independizada de la red LAN del aeropuerto, por cuanto la distancia entre ambas oficinas tiene una distancia de 4 Km. por lo cual el área de Cargo tiene un router y un switch, de uso exclusivo

Jefatura de Aeropuerto, ubicada en la nueva Terminal aérea José Joaquín de Olmedo, esta conformada actualmente por una red local con 33 computadores, 3 switches de 24 puertos c/u. (1 TAME, 1 SITA, 1 TAGSA) y un ruteador con canal de comunicaciones de 256 kbps, el mismo que se comunica igual que la oficina centro con una serie de nodos o ruteadores de Pacifictel y Andinadatos, hasta llegar a un ruteador principal ubicado en la Matriz en Quito.

## 2.6.- ANÁLISIS DE PISO LÓGICO

### 2.6.1.- MATRIZ Y SURCURSAL

#### 2.6.1.2.- GERENCIA DE INFORMÁTICA (PRIMER PISO)

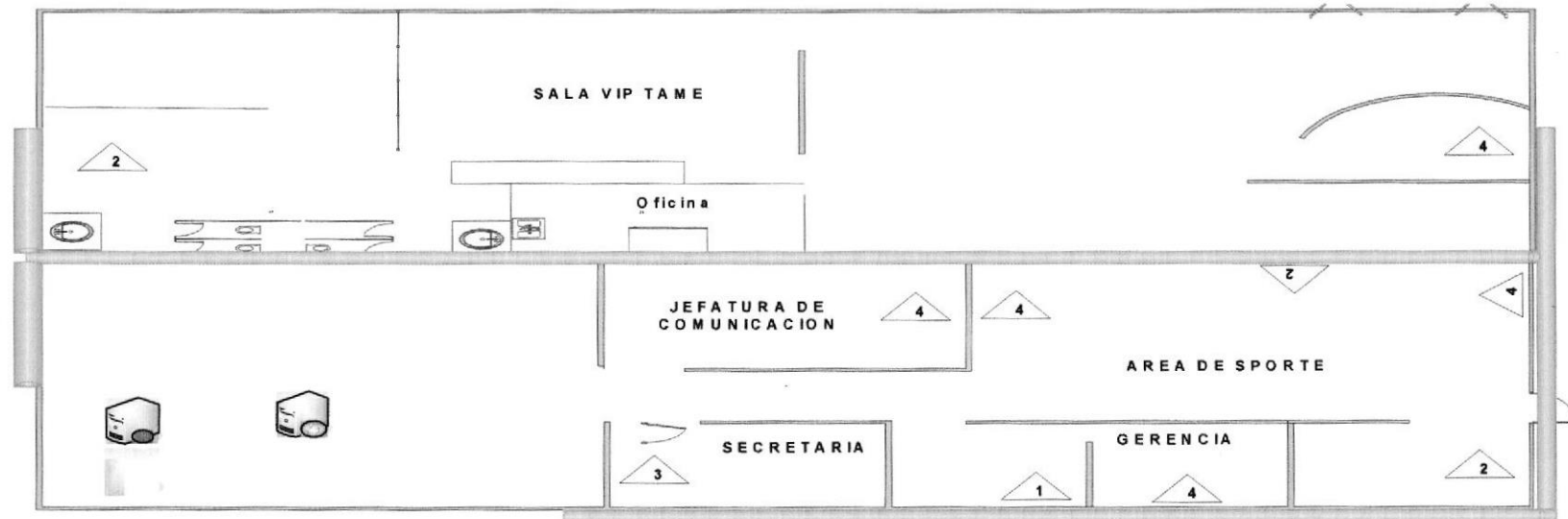


FIGURA 2 - 3: Análisis de piso lógico-Primer Piso Matriz



## 2.6.1.2.- GERENCIA DE RECURSOS HUMANOS (SEGUNDO PISO)

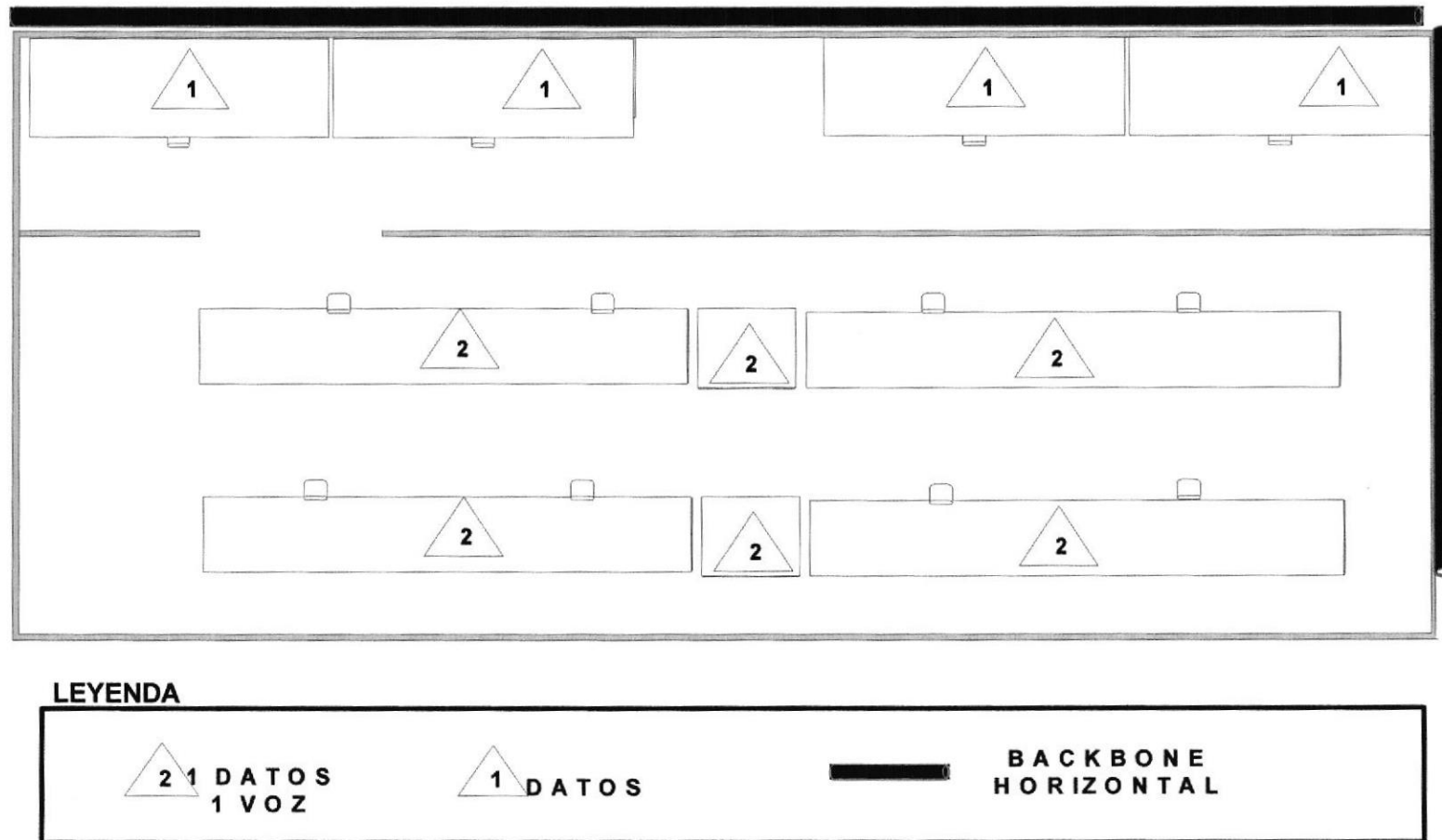


FIGURA 2 - 4: Análisis de piso lógico-Segundo Piso Matriz

## 2.6.1.3.- GERENCIA DE PLANIFICACIÓN (TERCER PISO)

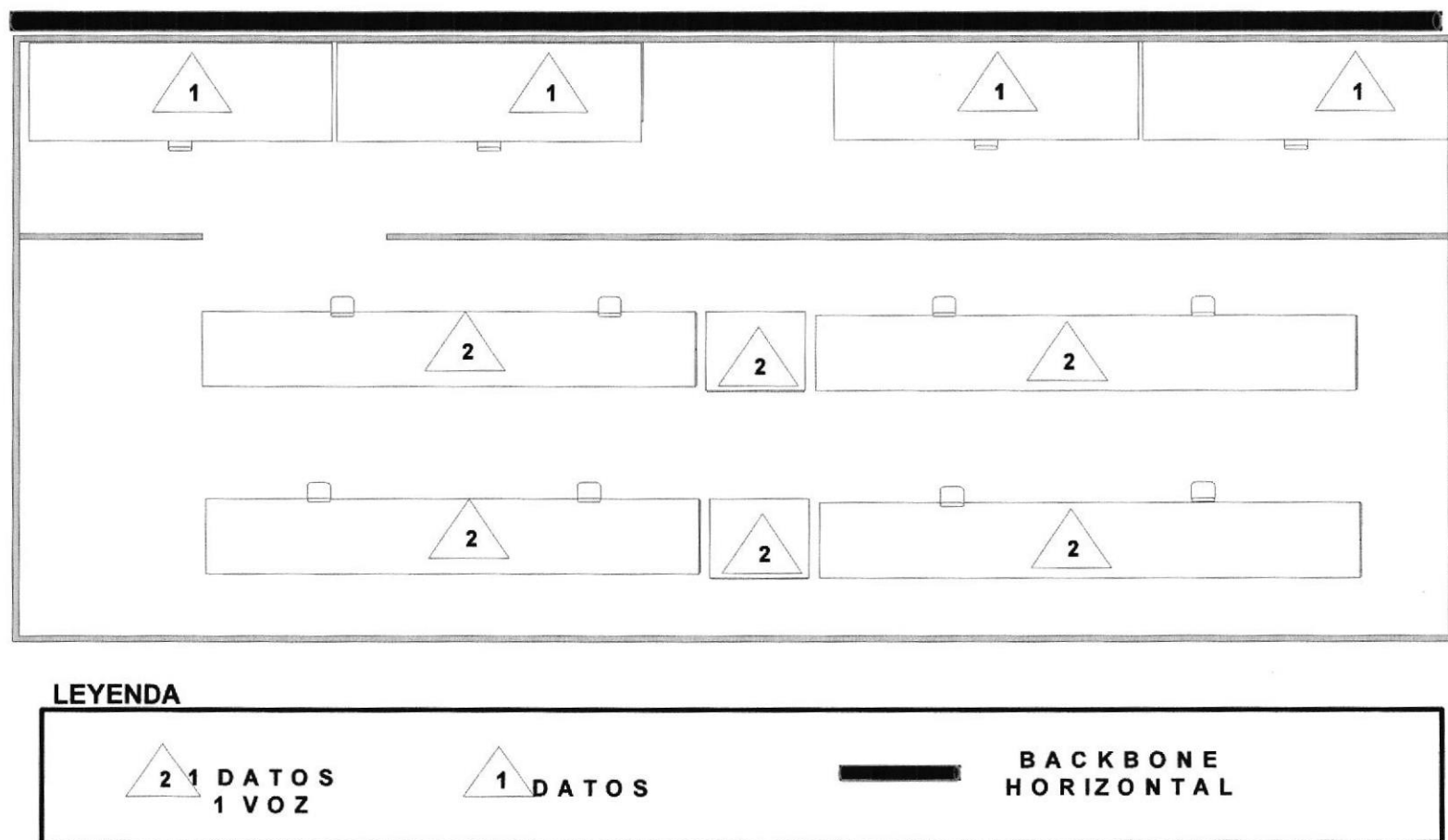


FIGURA 2 - 5: Análisis de piso lógico-Tercer Piso Matriz



## 2.6.1.4.- GERENCIA DE LOGÍSTICA (CUARTO PISO)

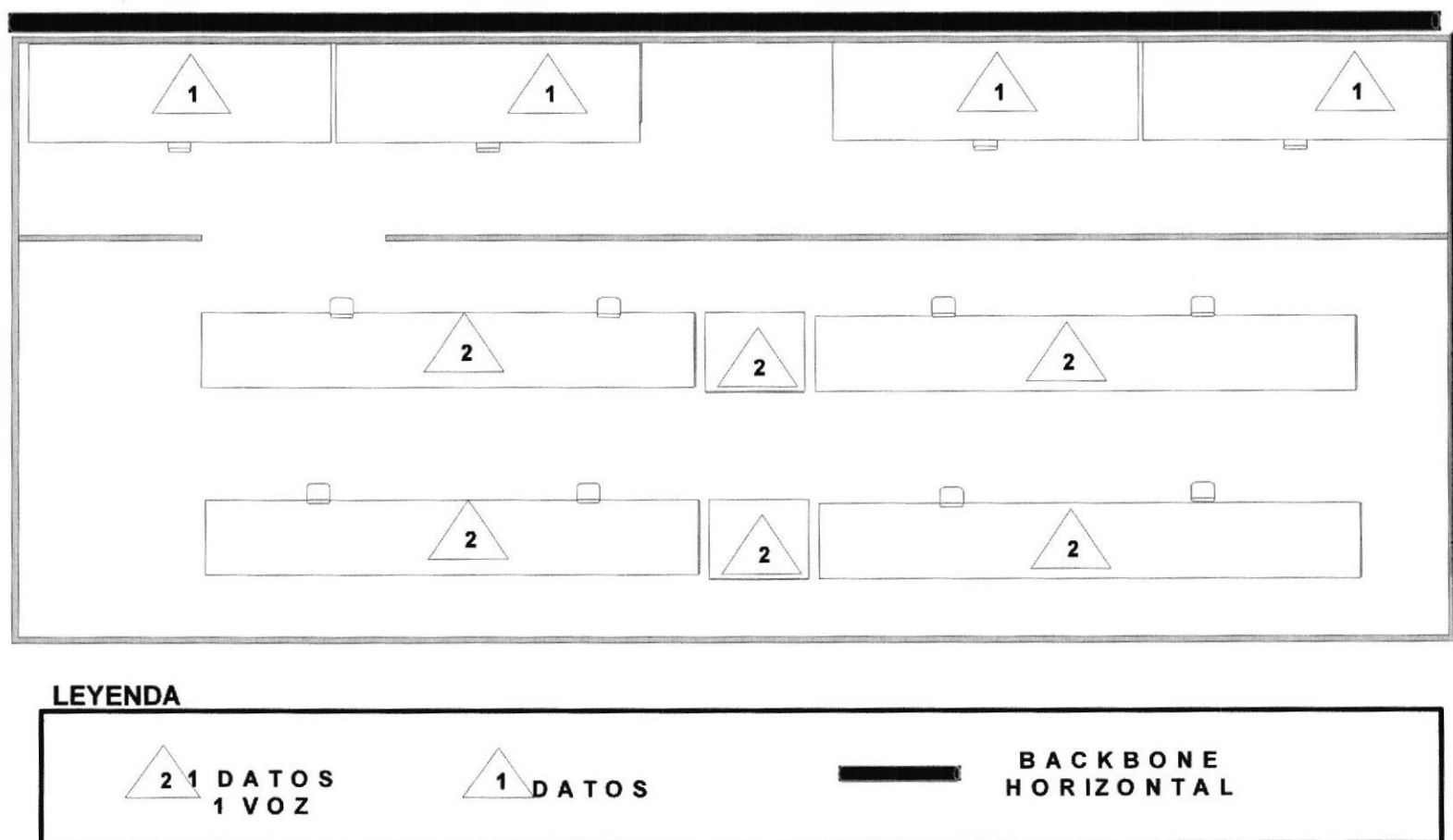


FIGURA 2 - 6: Análisis de piso lógico-Cuarto Piso Matriz

## 2.6.1.5.- GERENCIA DE FINANZAS (QUINTO PISO)

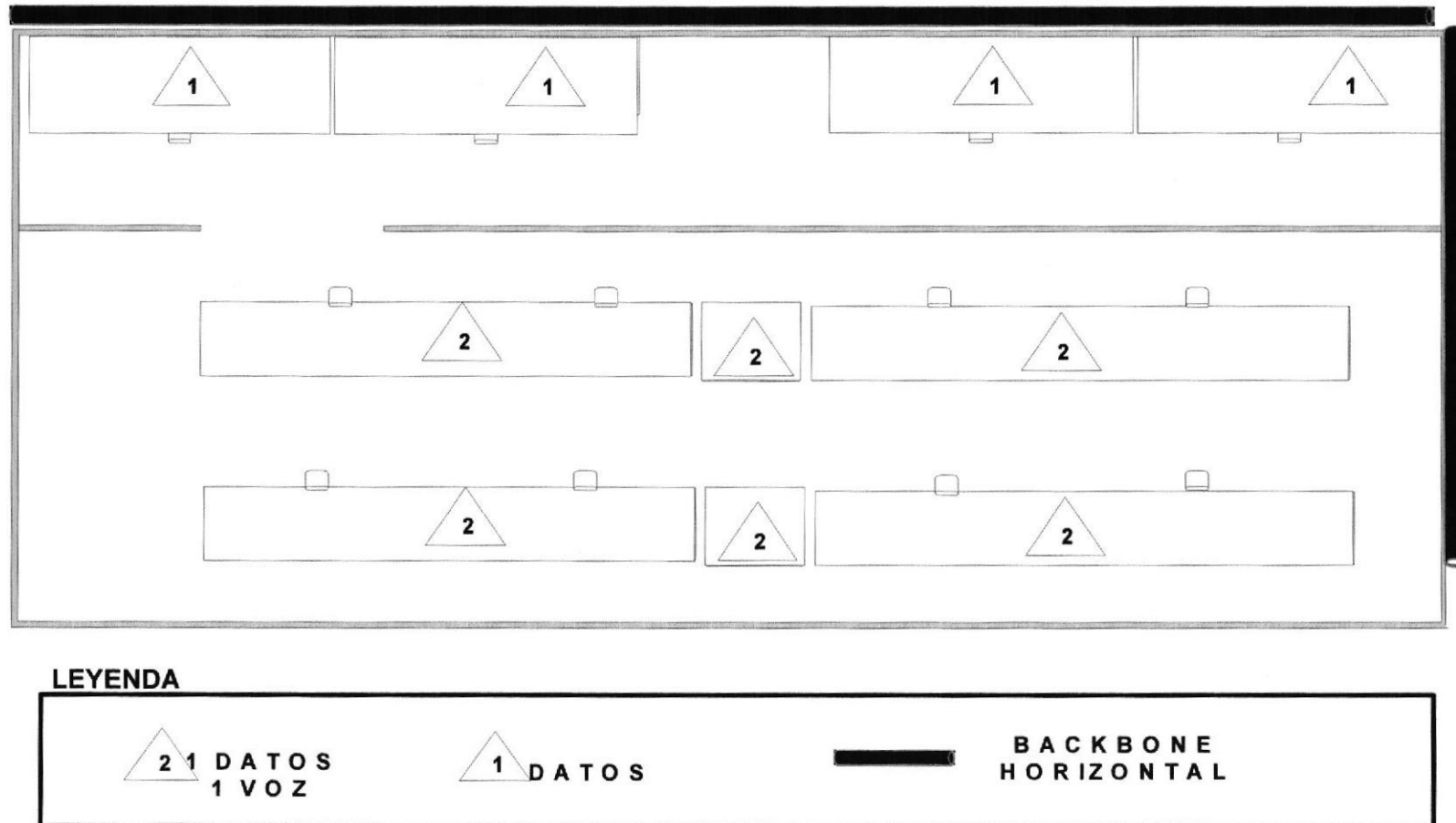


FIGURA 2 - 7: Análisis de piso lógico-Quinto Piso Lógico Matriz

## 2.6.1.6.- PRESIDENCIA EJECUTIVA Y ASESORÍA JURÍDICA (SEXTO PISO)

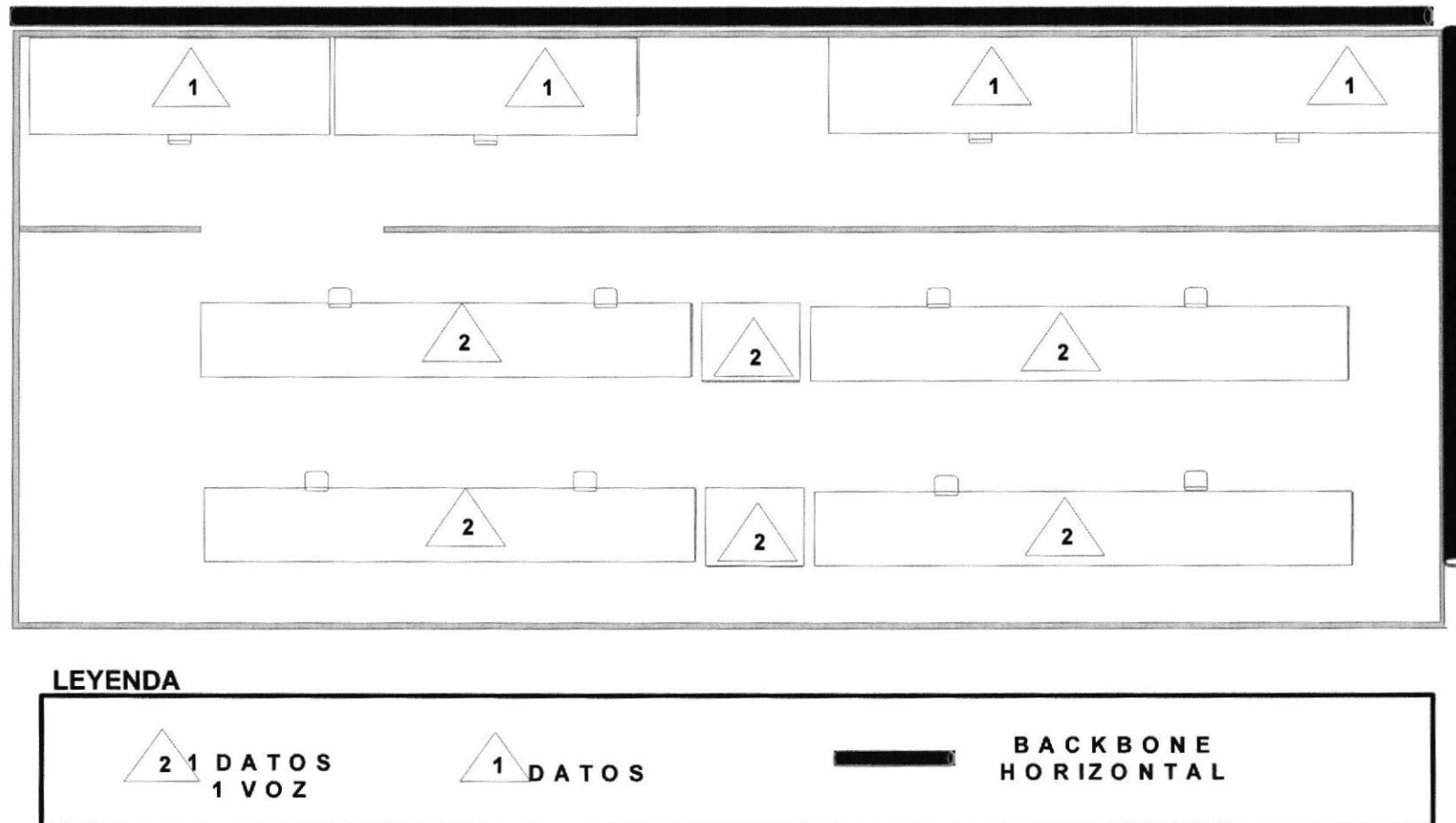


FIGURA 2 - 8: Análisis de piso lógico-Sexto Piso Matriz

## 2.6.1.7.- GERENCIA COMERCIAL (SÉPTIMO PISO)

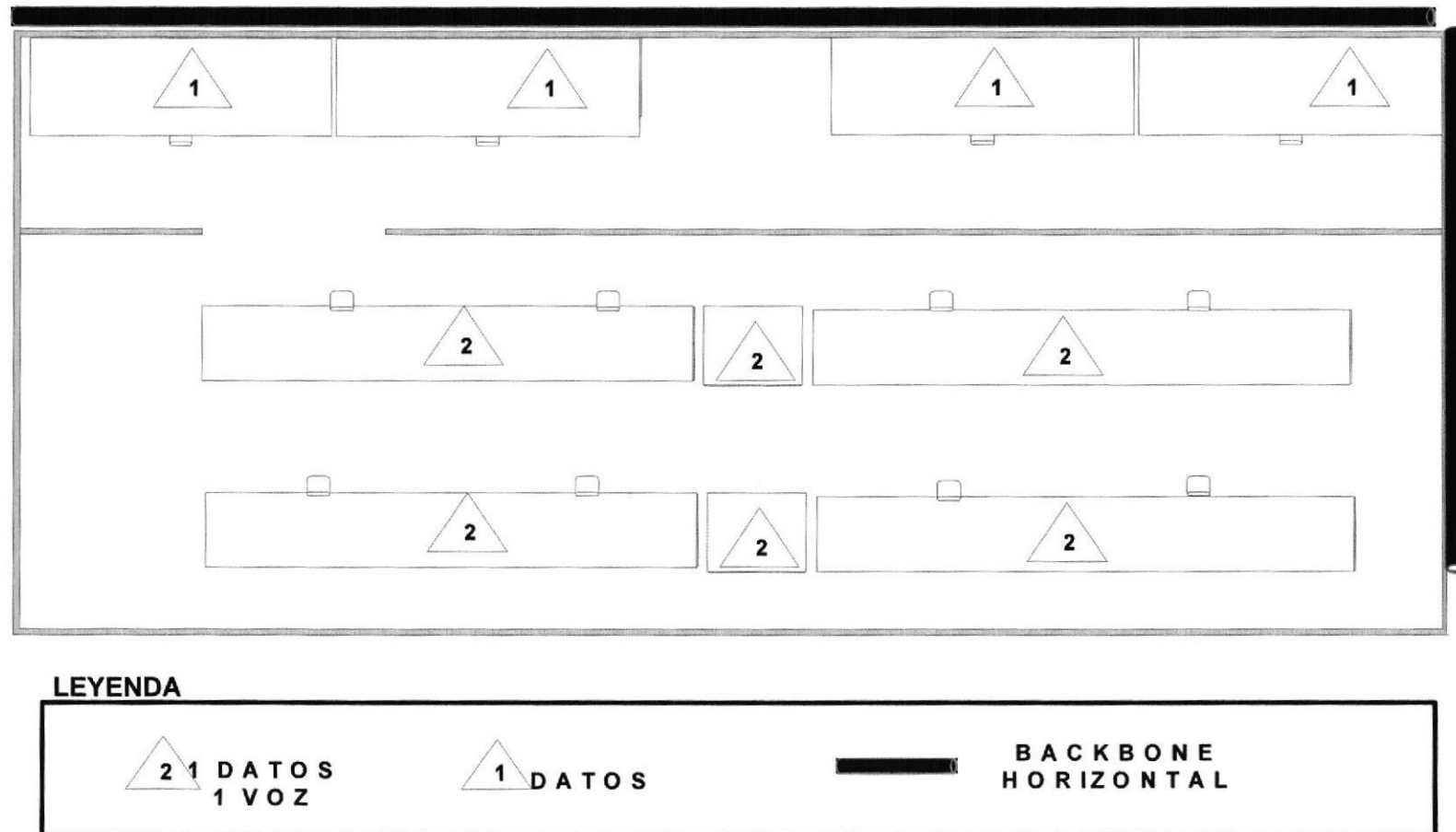


FIGURA 2 - 9: Análisis de piso lógico-Séptimo Piso Matriz



## 2.6.1.8.- INGRESOS (OCTAVO PISO)

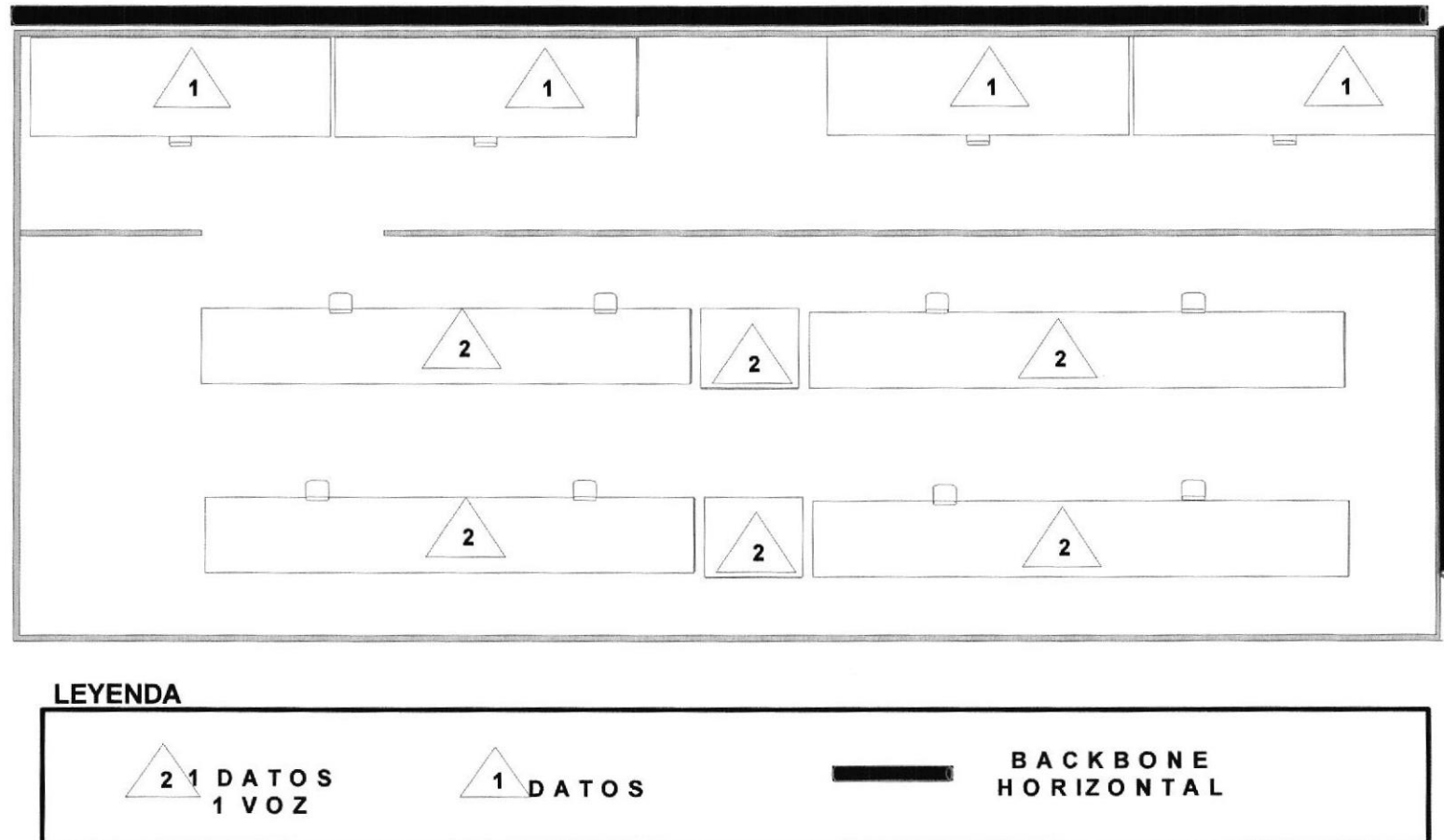


FIGURA 2 - 10: Análisis de piso lógico-Octavo Piso Matriz

## 2.6.1.9.- SALA DE CONFERENCIAS Y SALONES DE CAPACITACIÓN (NOVENO PISO)

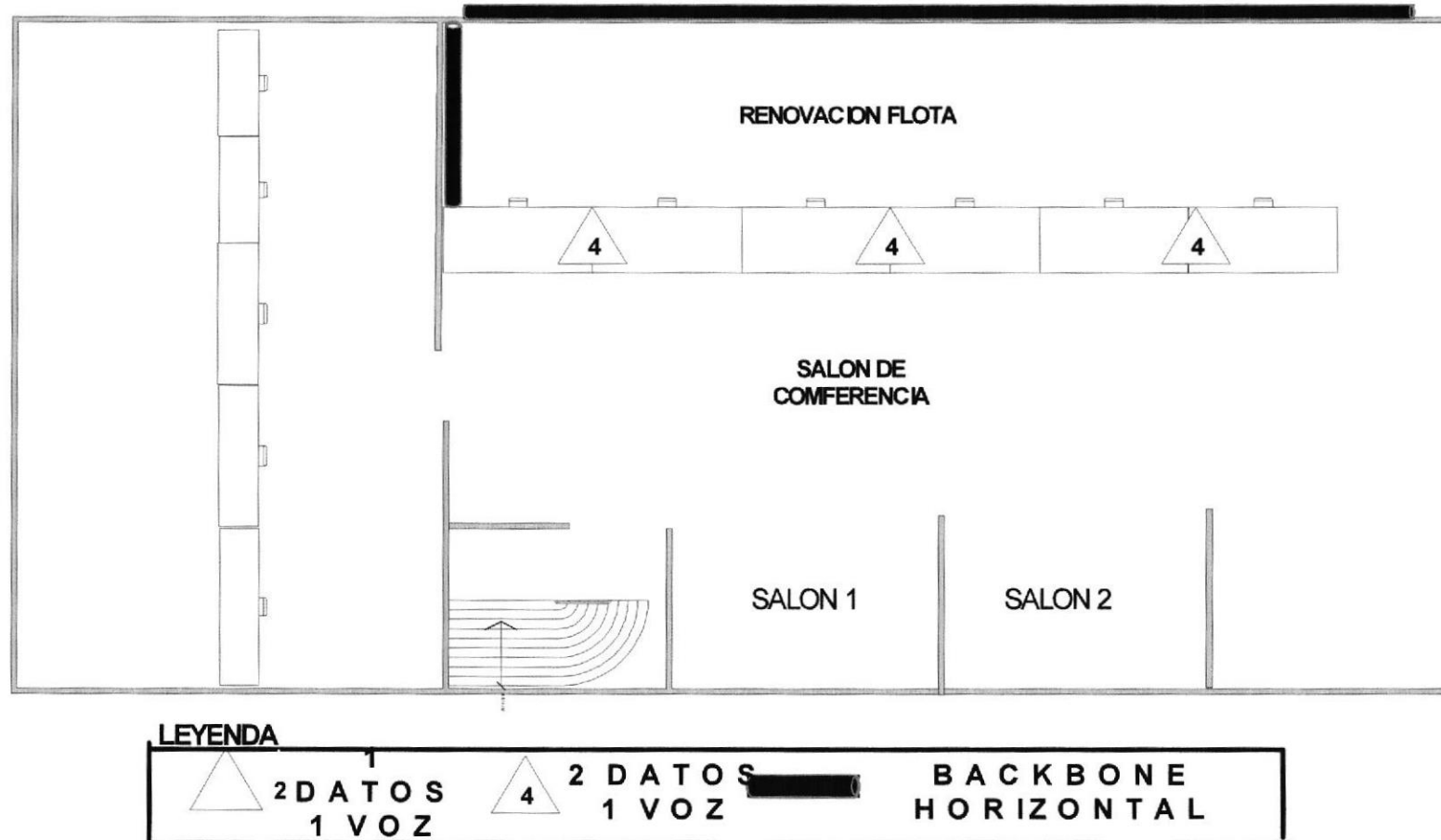


FIGURA 2 - 11: Análisis de piso lógico-Noveno Piso Matriz

## 2.6.1.10.- GERENCIA DE INFORMÁTICA

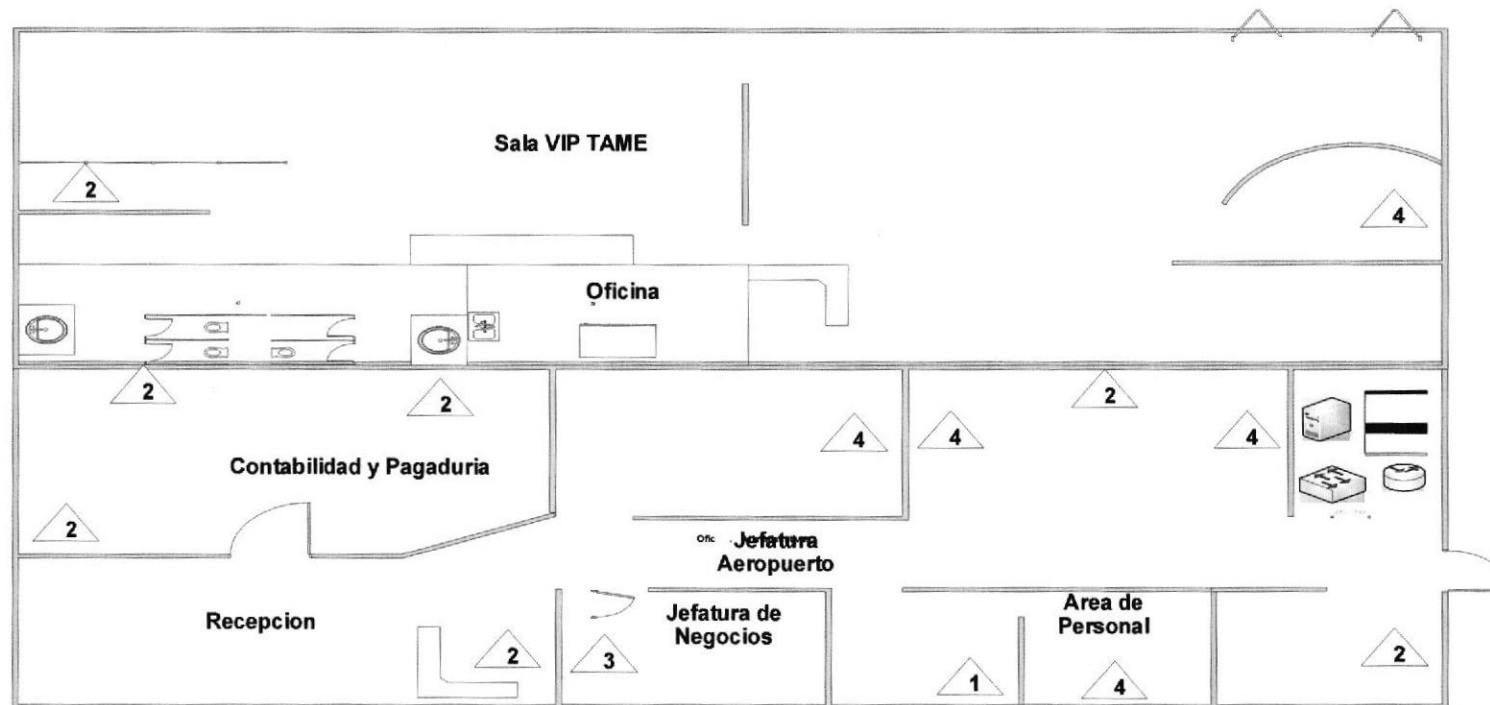


FIGURA 2 - 12: Análisis de piso lógico-Primer Piso A JJO

## 2.6.1.11.- ÁREA DE VENTA DE PASAJES.

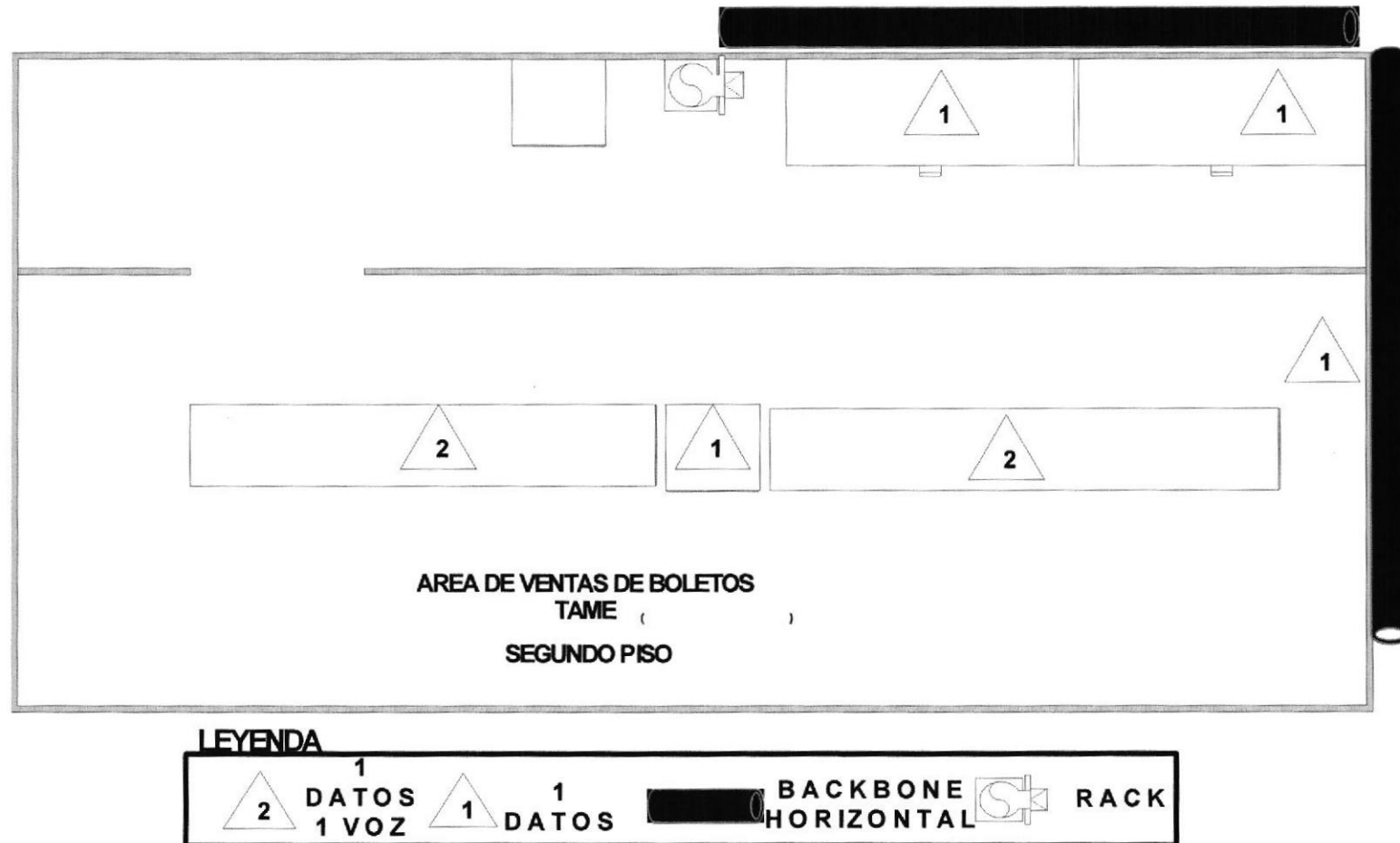


FIGURA 2 - 13: Análisis de piso lógico-Segundo Piso A JJO

## 2.6.1.12- GERENCIA DE INFORMÁTICA

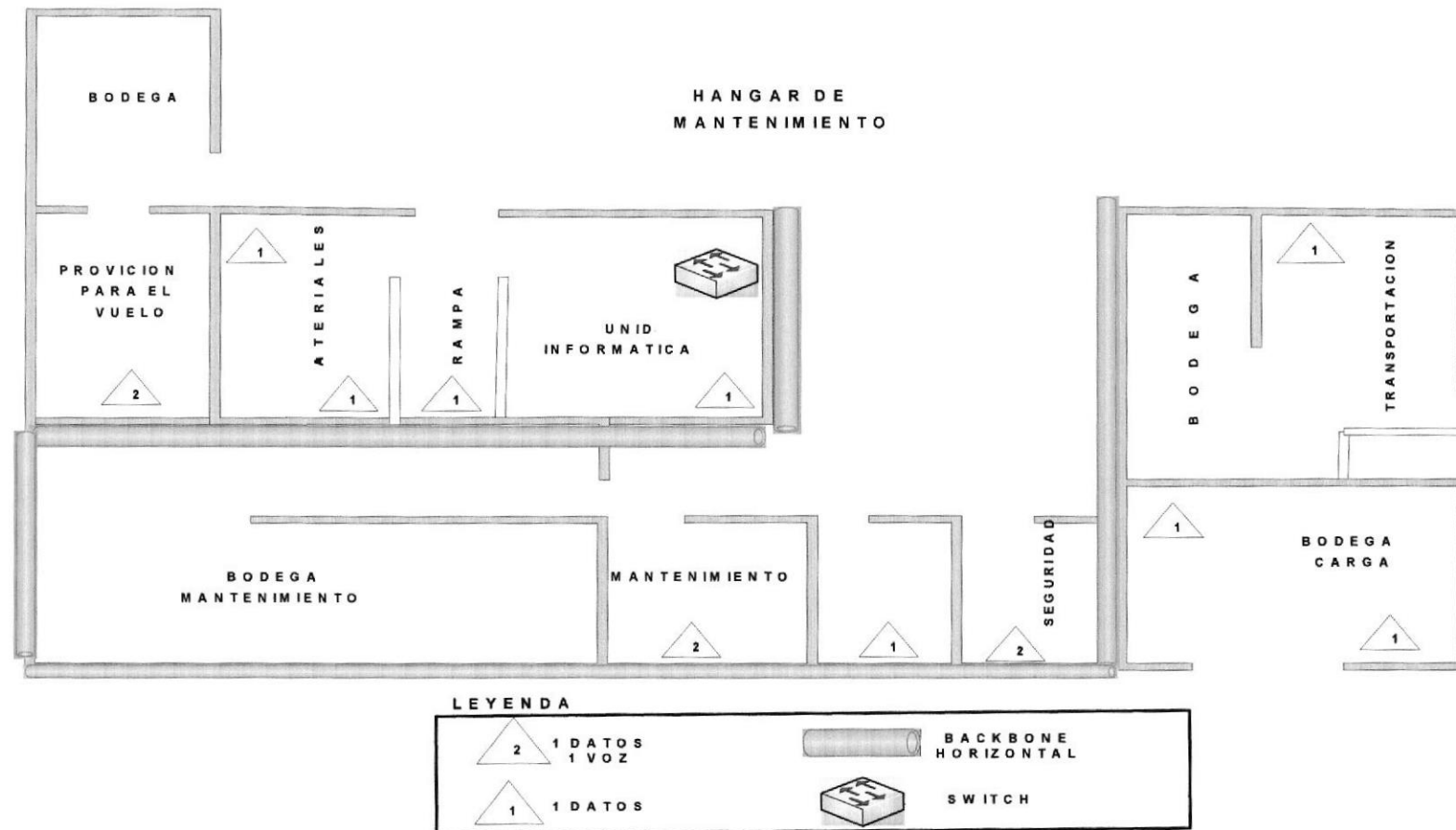


FIGURA 2 - 14: Análisis de piso lógico-Primer Piso TAME Cargo

## 2.6.1.13.- ÁREA DE SISTEMAS

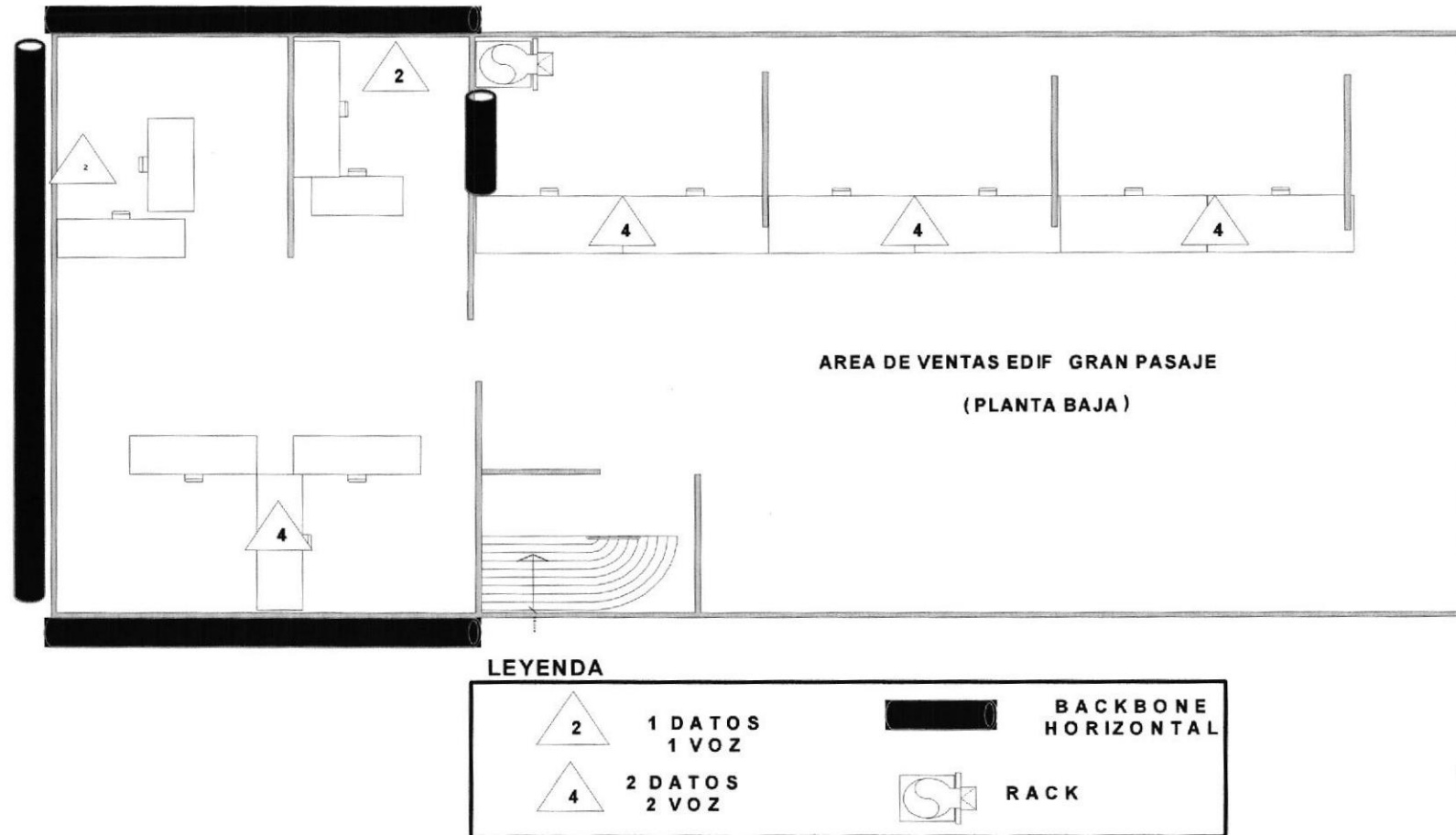


FIGURA 2 - 15: Análisis de piso lógico-Área de Sistema Tame Cargo



## 2.6.1.14.- ÁREA DE VENTAS DE PASAJES (PRIMER PISO)

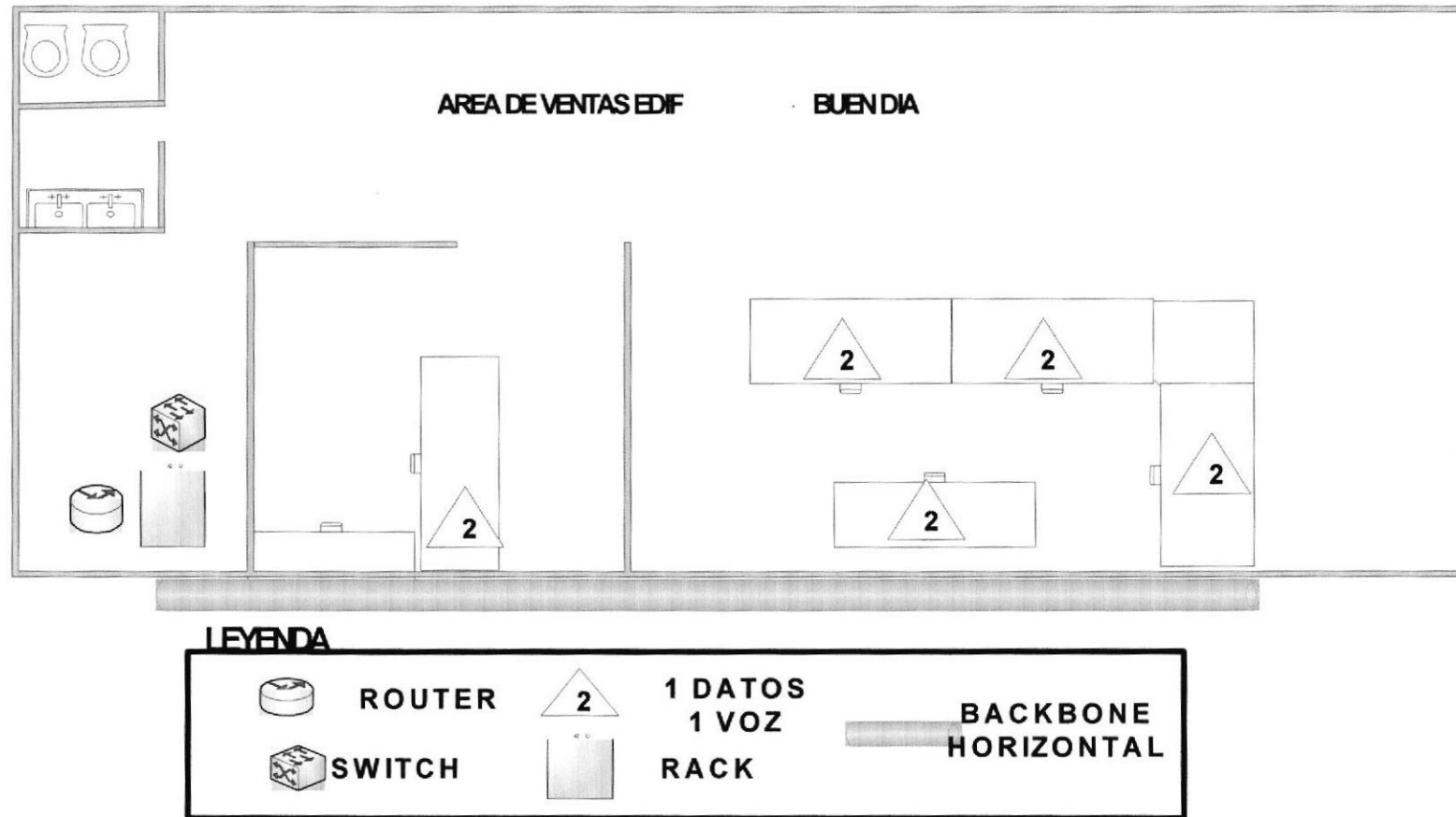


FIGURA 2 - 16: Análisis de piso lógico-Primer Piso Buen Día



## 2.6.1.15.- ÁREA DE SISTEMAS (PRIMER PISO)

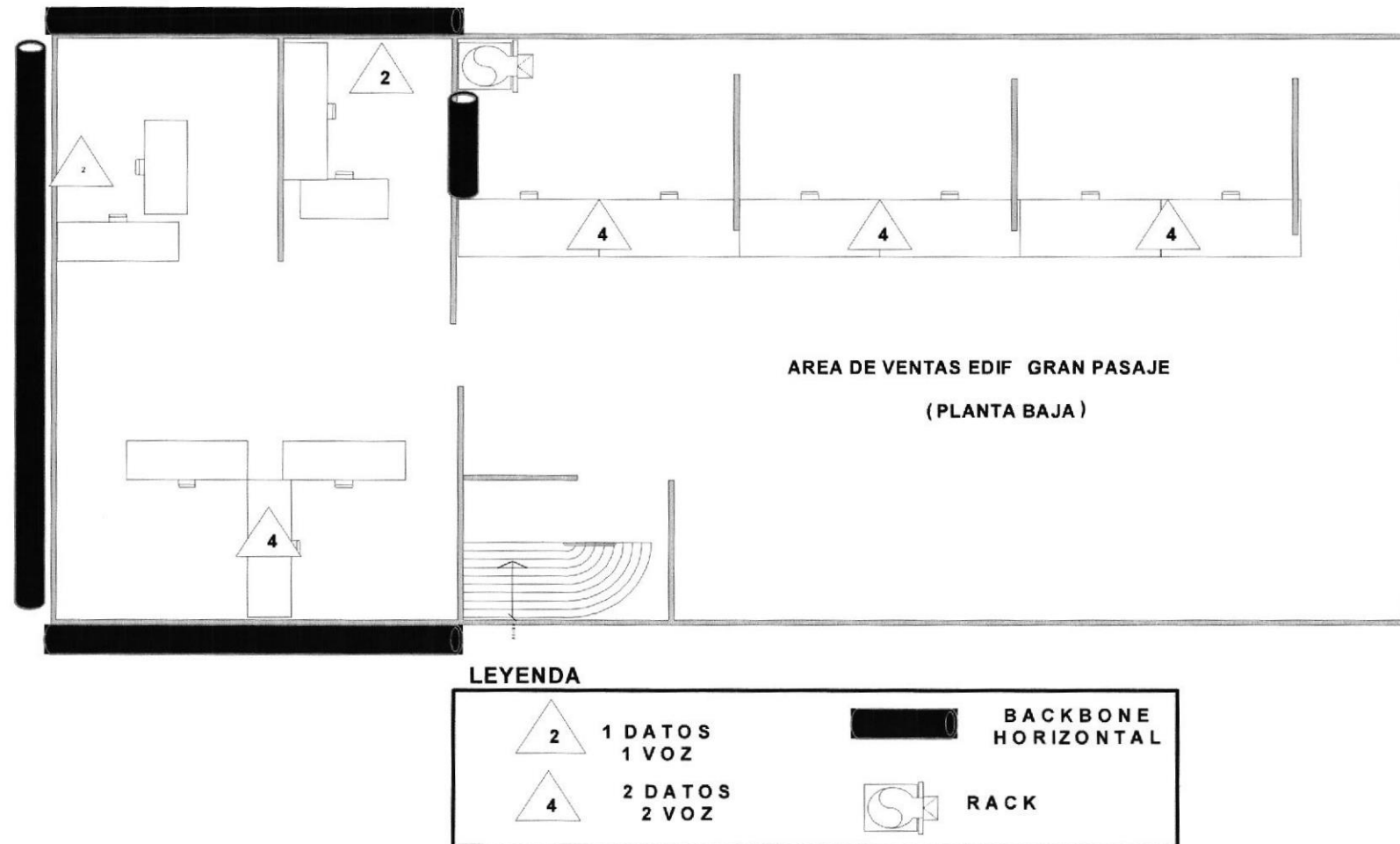


FIGURA 2 - 17: Análisis de piso lógico-Primer Piso Gran Pasajes

## 2.6.1.16.- RESERVACIONES

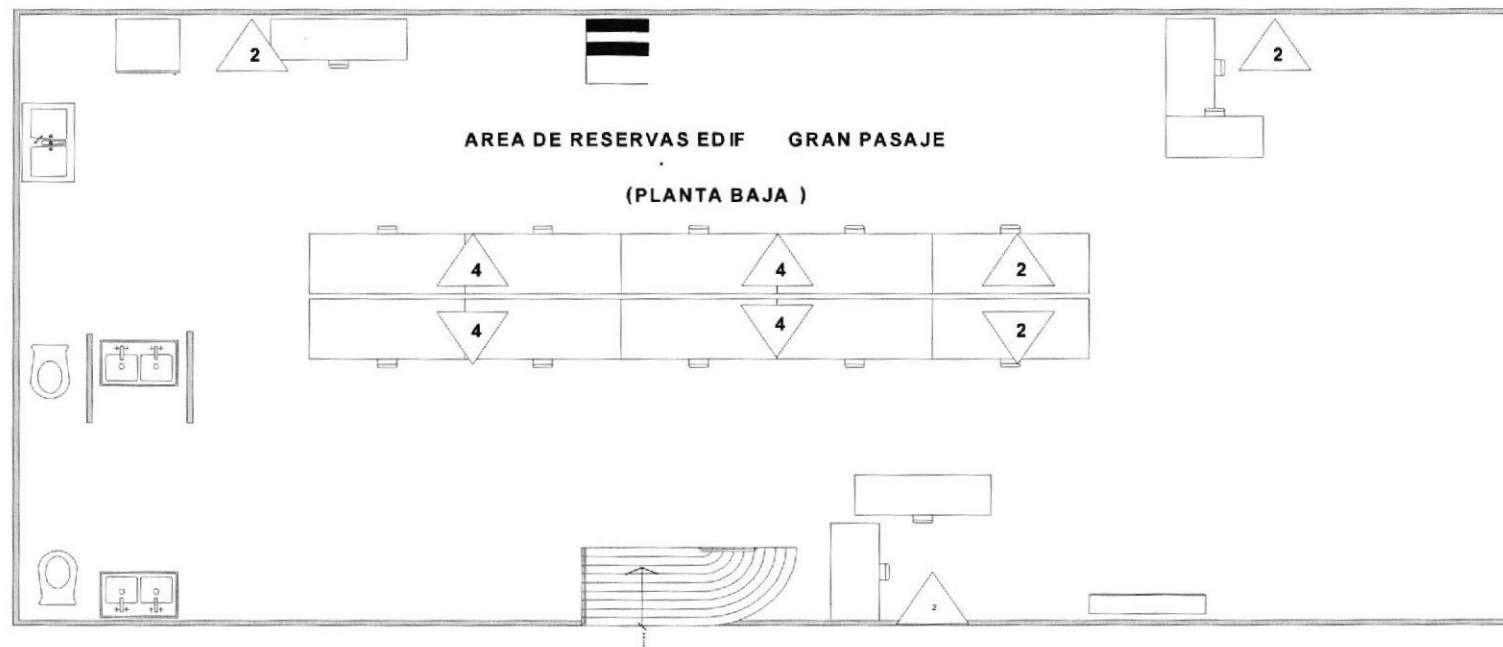
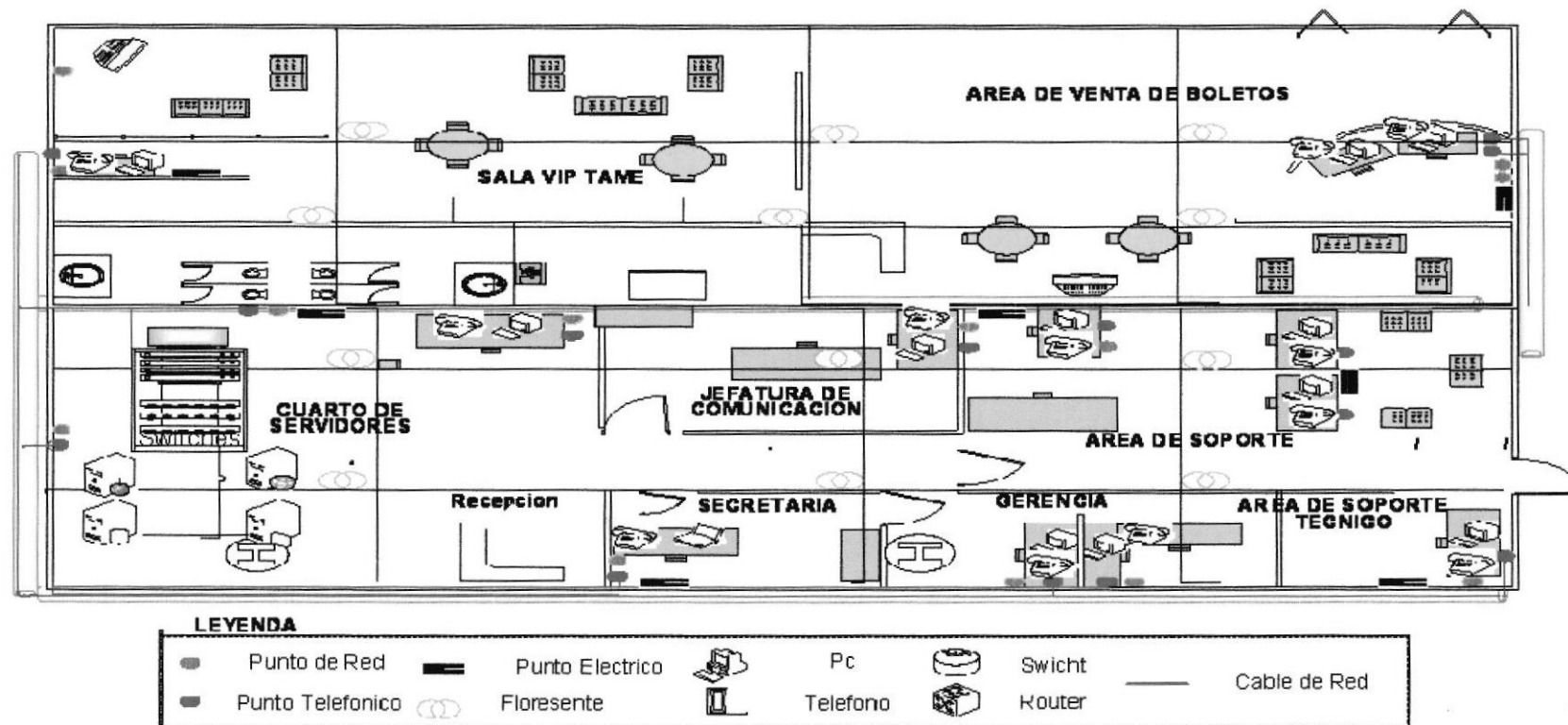


FIGURA 2 - 18: Análisis de piso lógico-Reservaciones Gran Pasajes

## 2.7.- ANÁLISIS DE PISO APLICATIVO

### 2.7.1.- MATRIZ Y SUCURSAL

#### 2.7.1.1.- GERENCIA DE INFORMÁTICA



**FIGURA 2 - 19:** Análisis de piso Aplicativo -Primer Piso Matriz

## 2.7.1.2.- GERENCIA DE RECURSOS HUMANOS

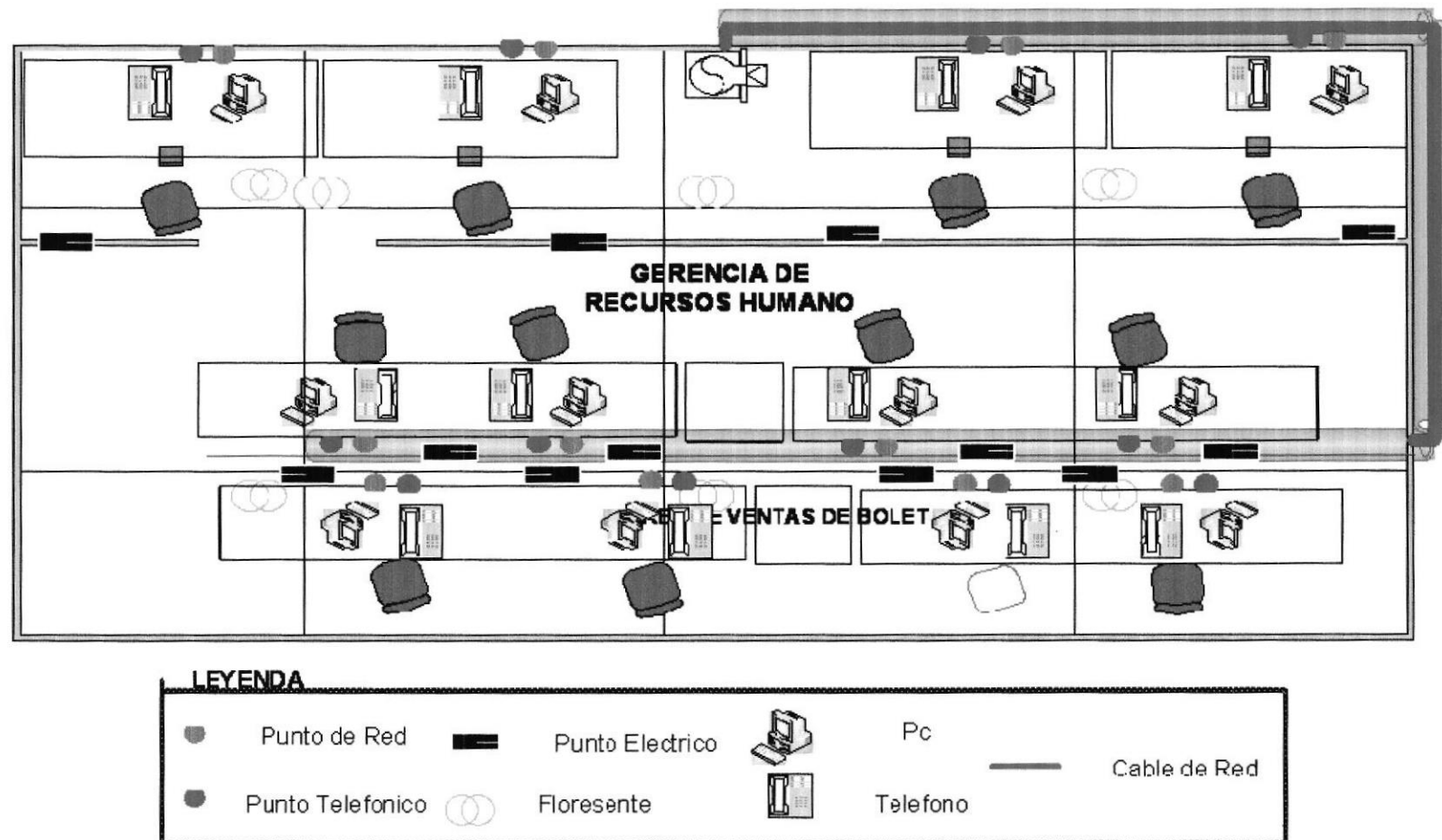


FIGURA 2 - 20: Análisis de piso Aplicativo -Segundo Piso Matriz

## 2.7.1.3.- GERENCIA DE PLANIFICACIÓN

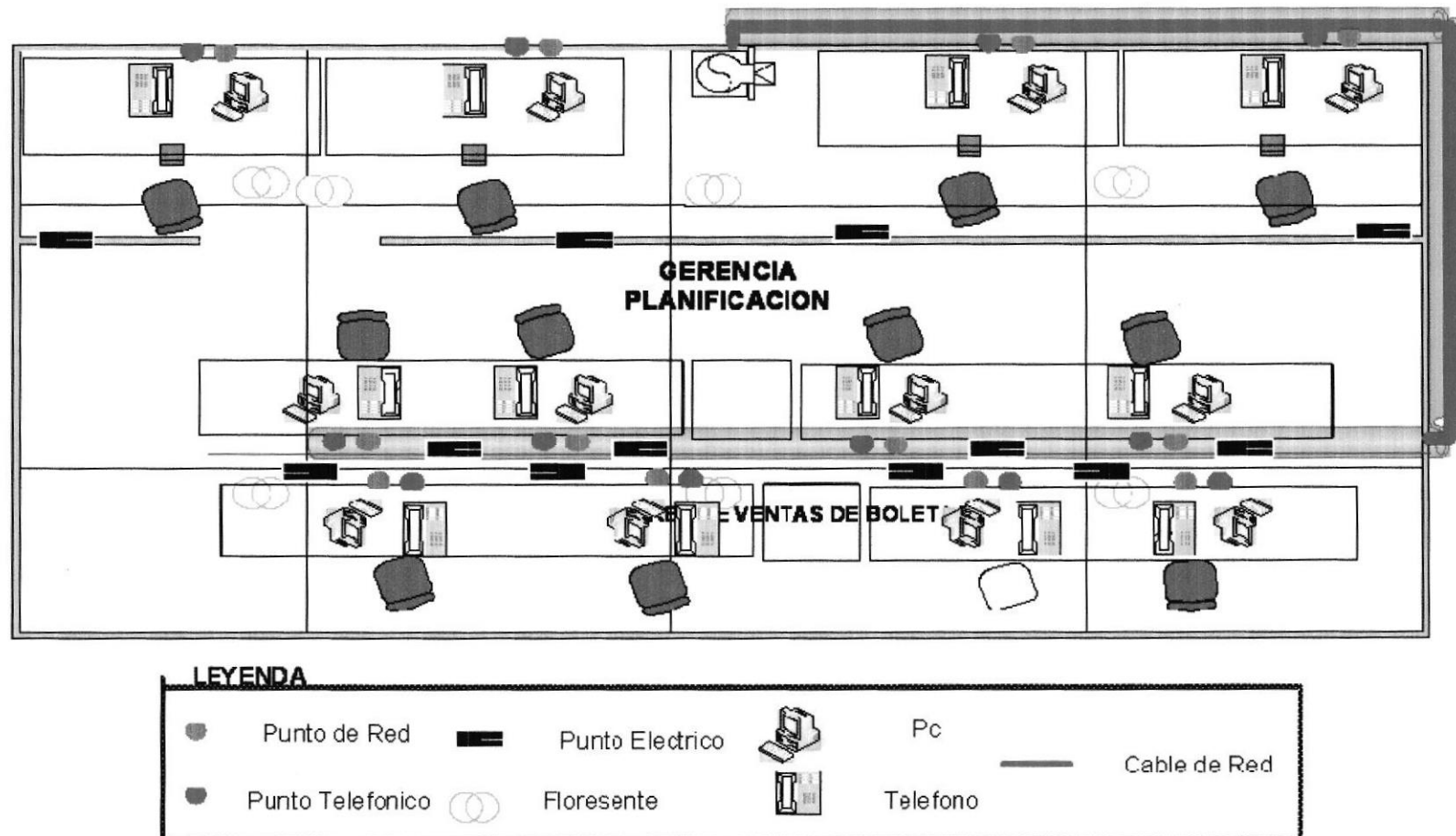


FIGURA 2 - 21: Análisis de piso Aplicativo -Tercer Piso Matriz

## 2.7.1.4.- GERENCIA DE LOGÍSTICA

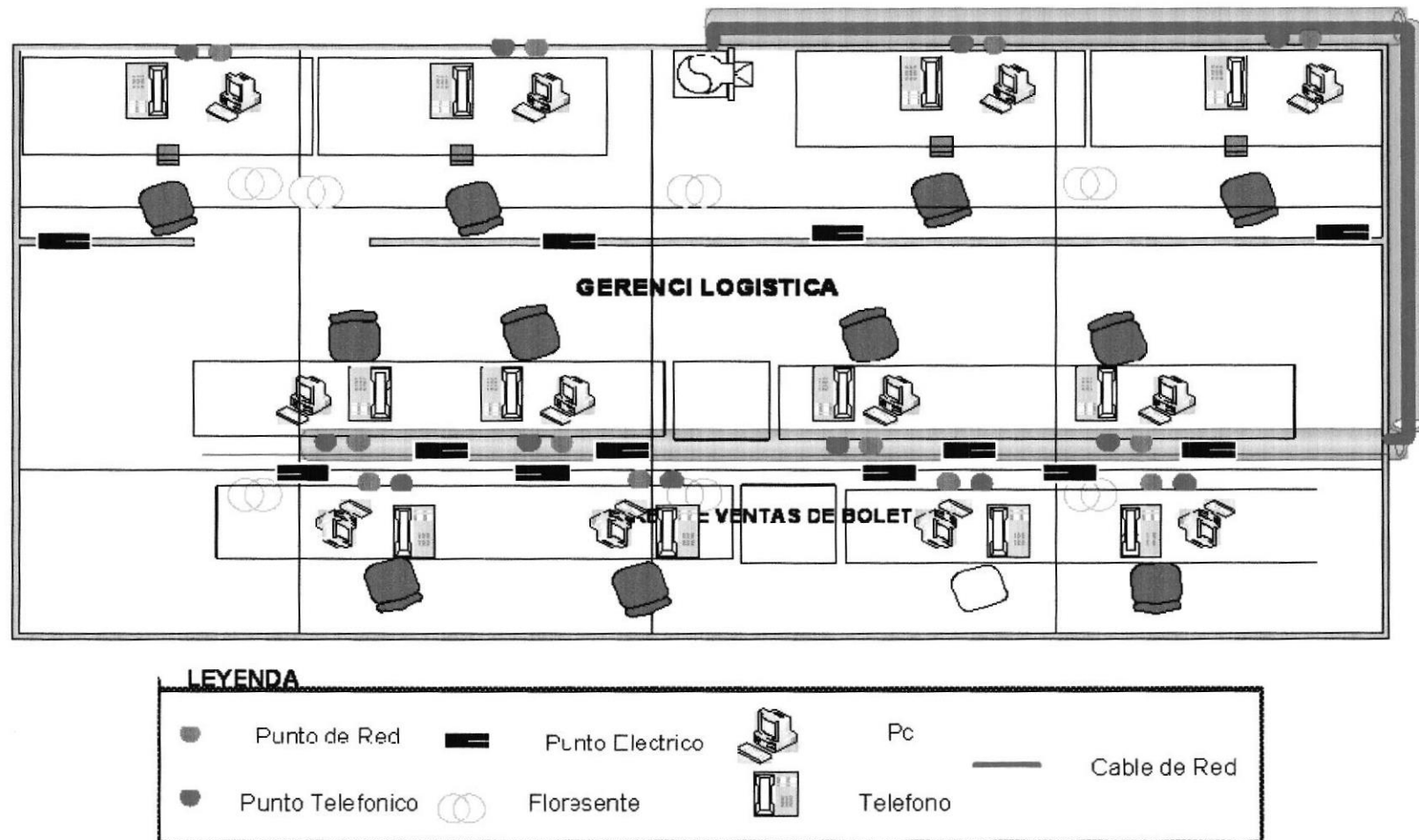


FIGURA 2 - 22: Análisis de piso Aplicativo -Cuarto Piso Matriz

## 2.7.1.5.- GERENCIA DE FINANZAS

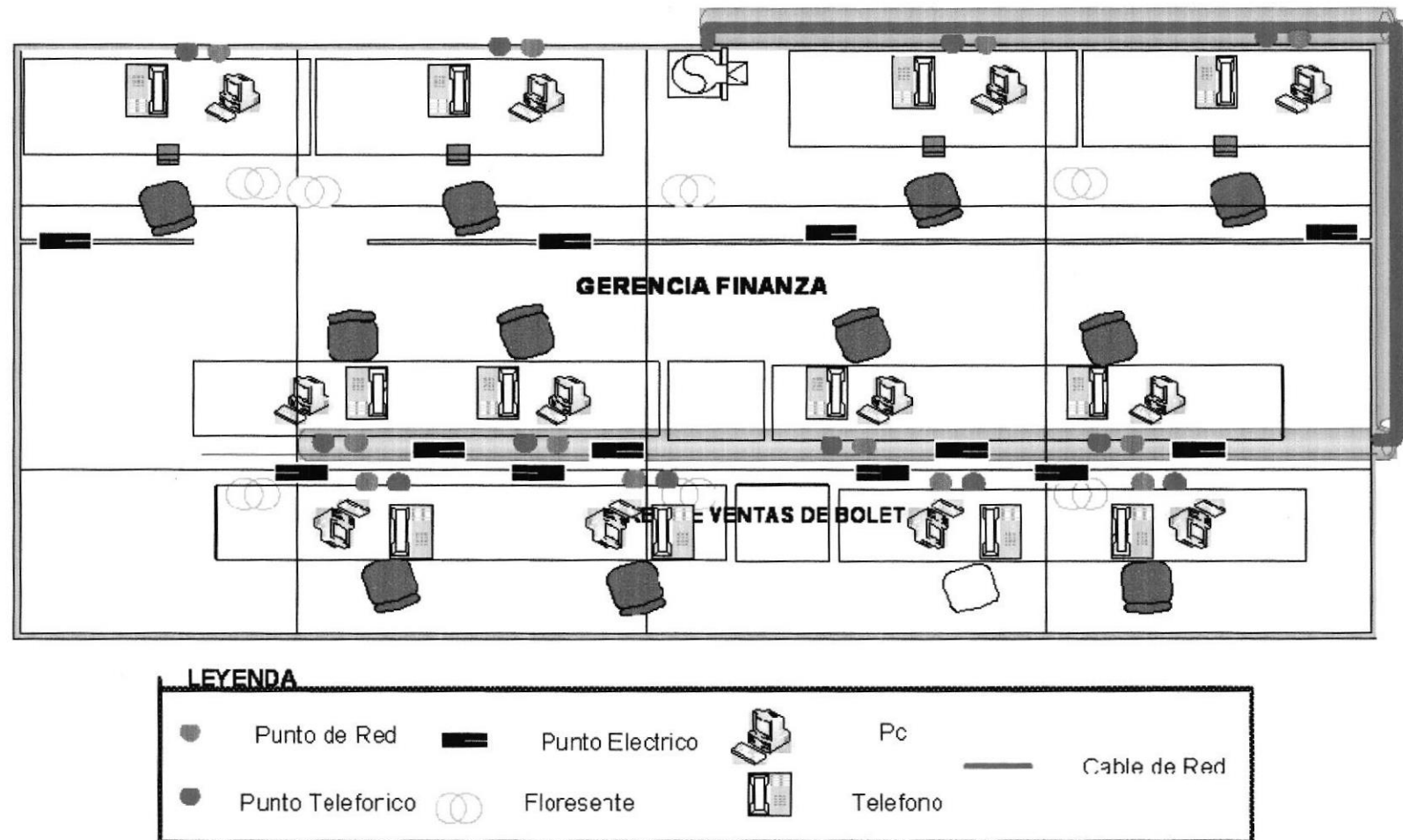


FIGURA 2 - 23: Análisis de piso Aplicativo -Quinto Piso Matriz



## 2.7.1.6.- PRESIDENCIA EJECUTIVA Y ASESORÍA JURÍDICA

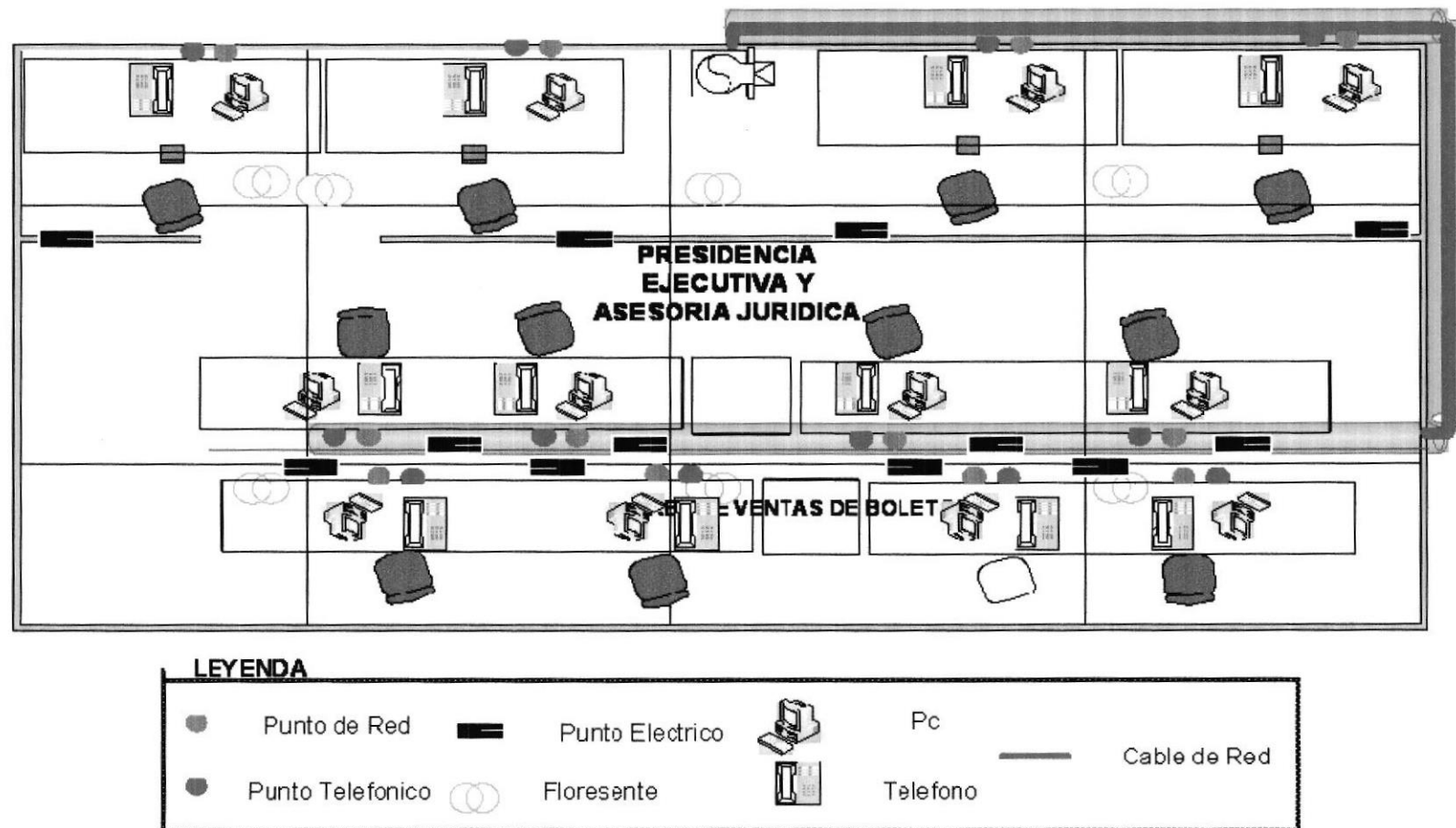


FIGURA 2 - 24: Análisis de piso Aplicativo -Sexto Piso Matriz

## 2.7.1.7.- GERENCIA COMERCIAL

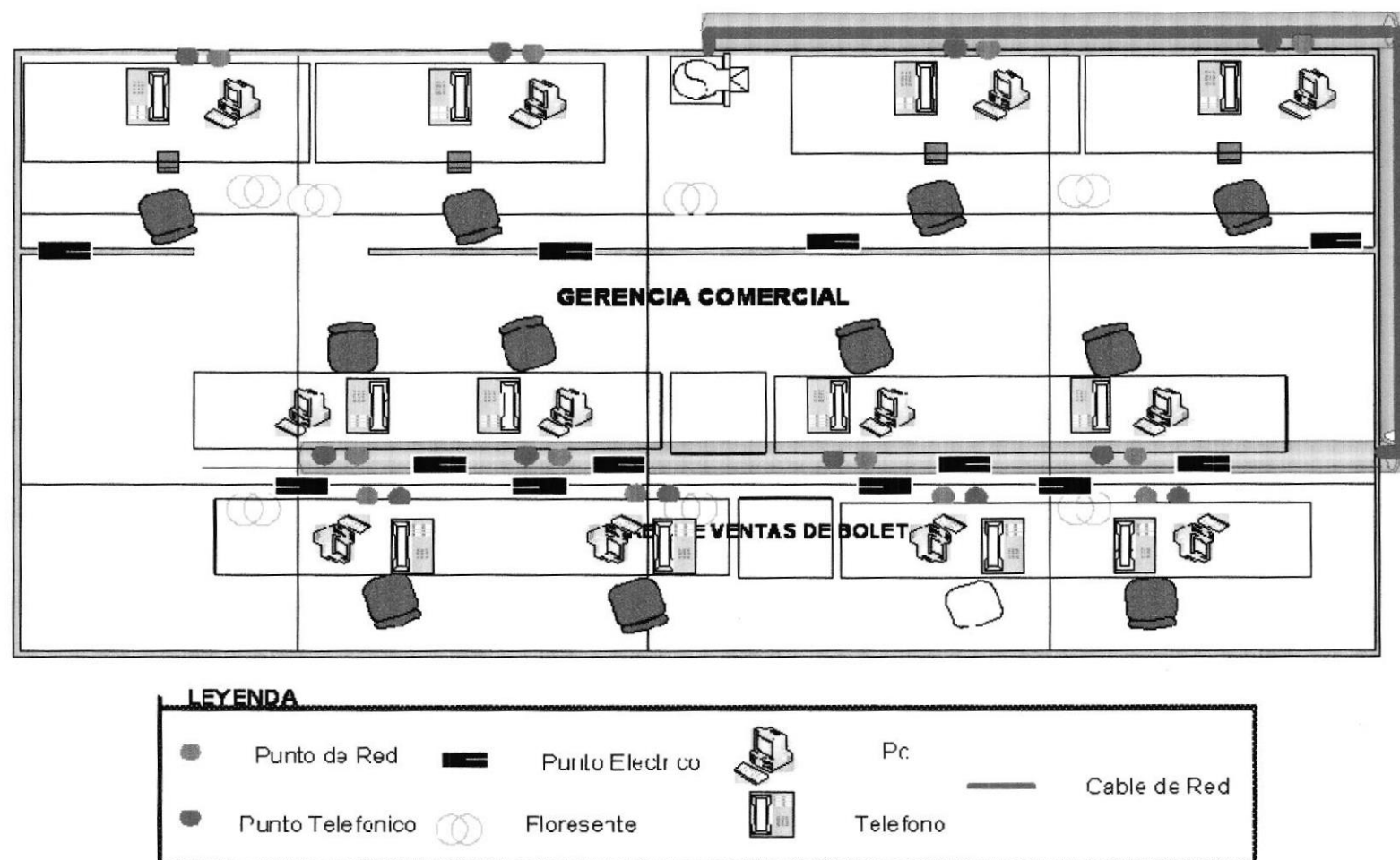


FIGURA 2 - 25: Análisis de piso Aplicativo -Séptimo Piso Matriz

## 2.7.1.8.- INGRESOS

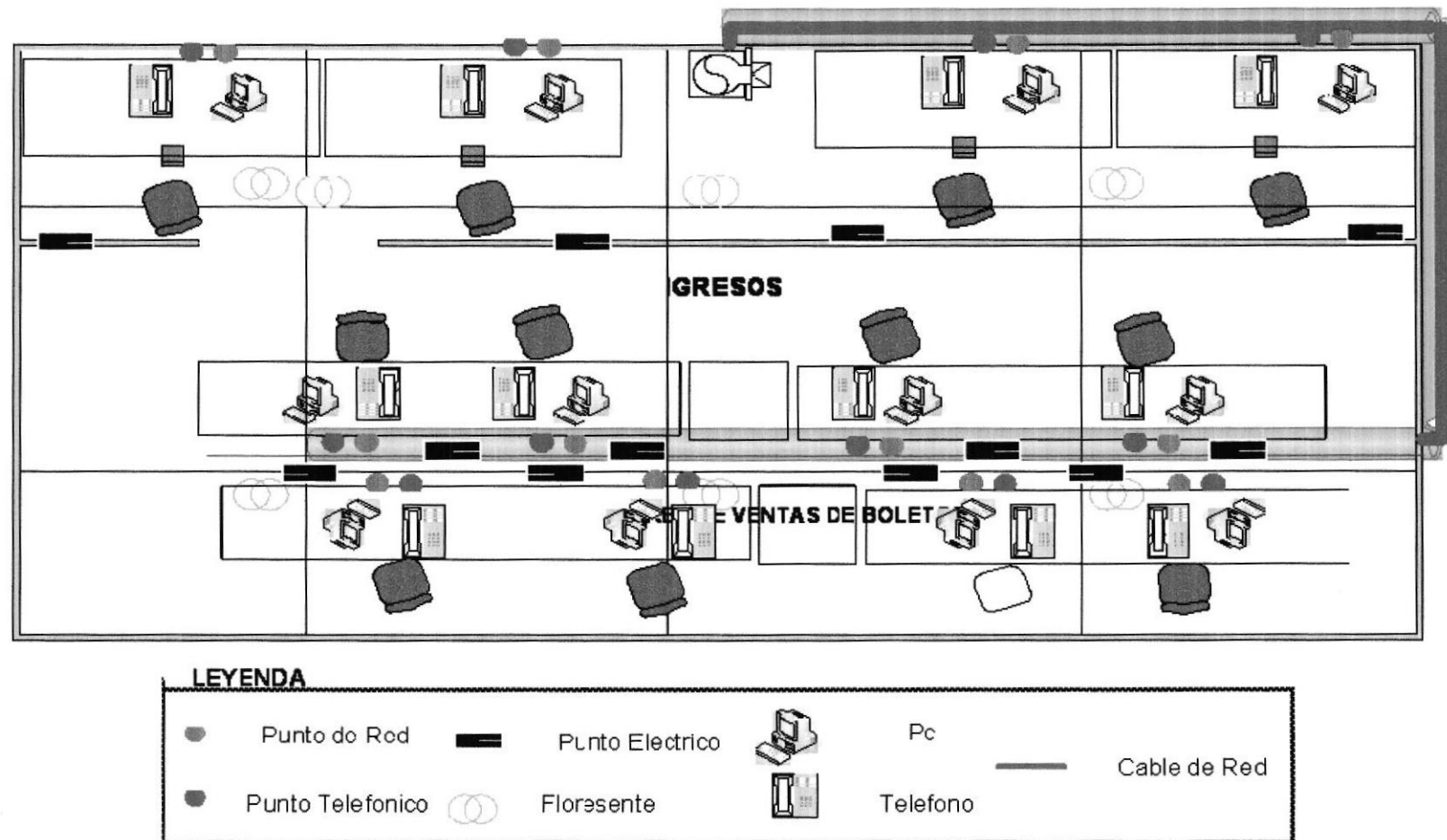


FIGURA 2 - 26: Análisis de piso Aplicative -Octavo Piso Matriz

## 2.7.1.9.- SALA DE CONFERENCIAS Y SALONES DE CAPACITACIÓN

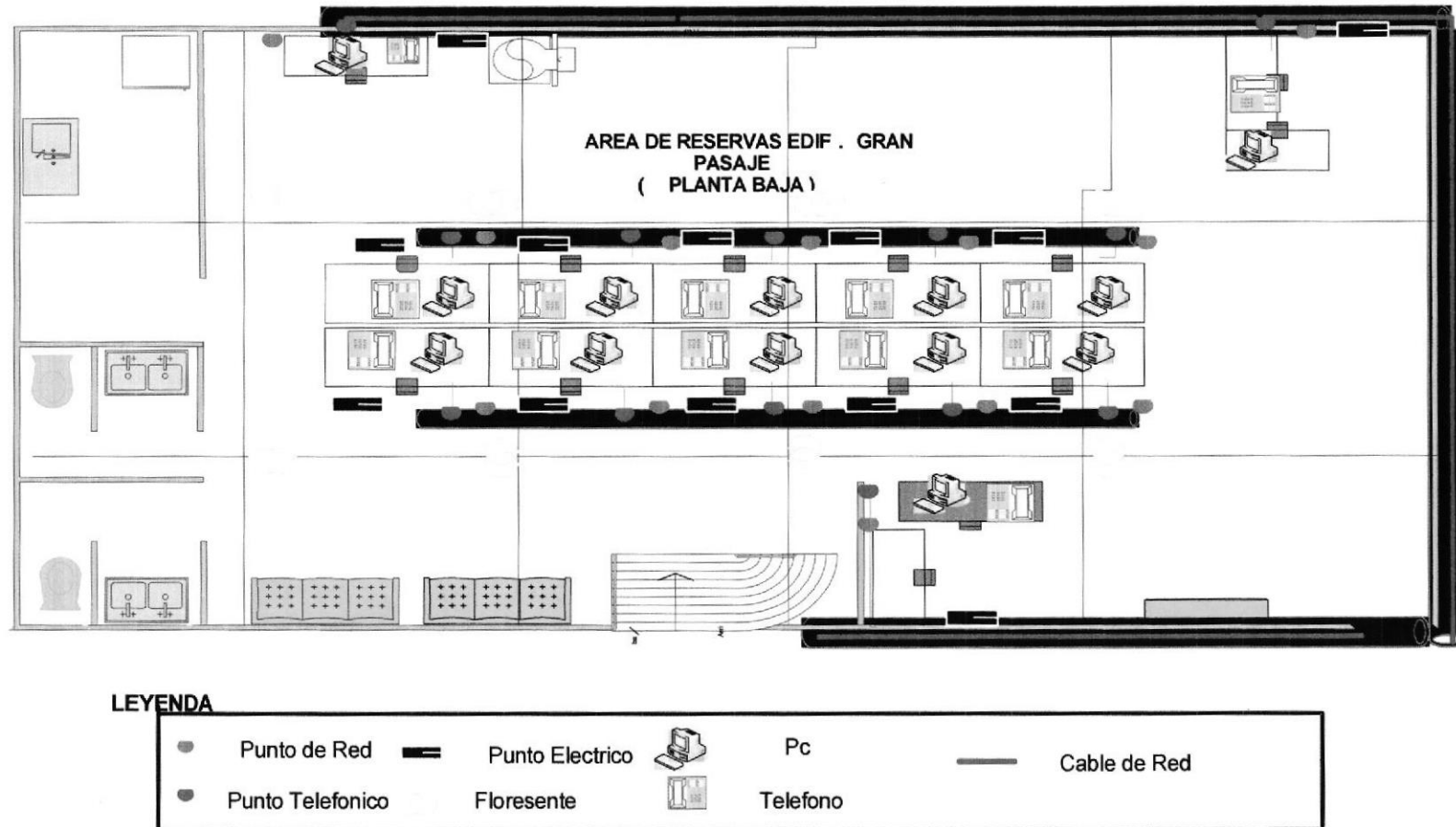


FIGURA 2 - 27: Análisis de piso Aplicativo-Noveno Piso Matriz



## 2.7.1.10.- GERENCIA DE INFORMÁTICA

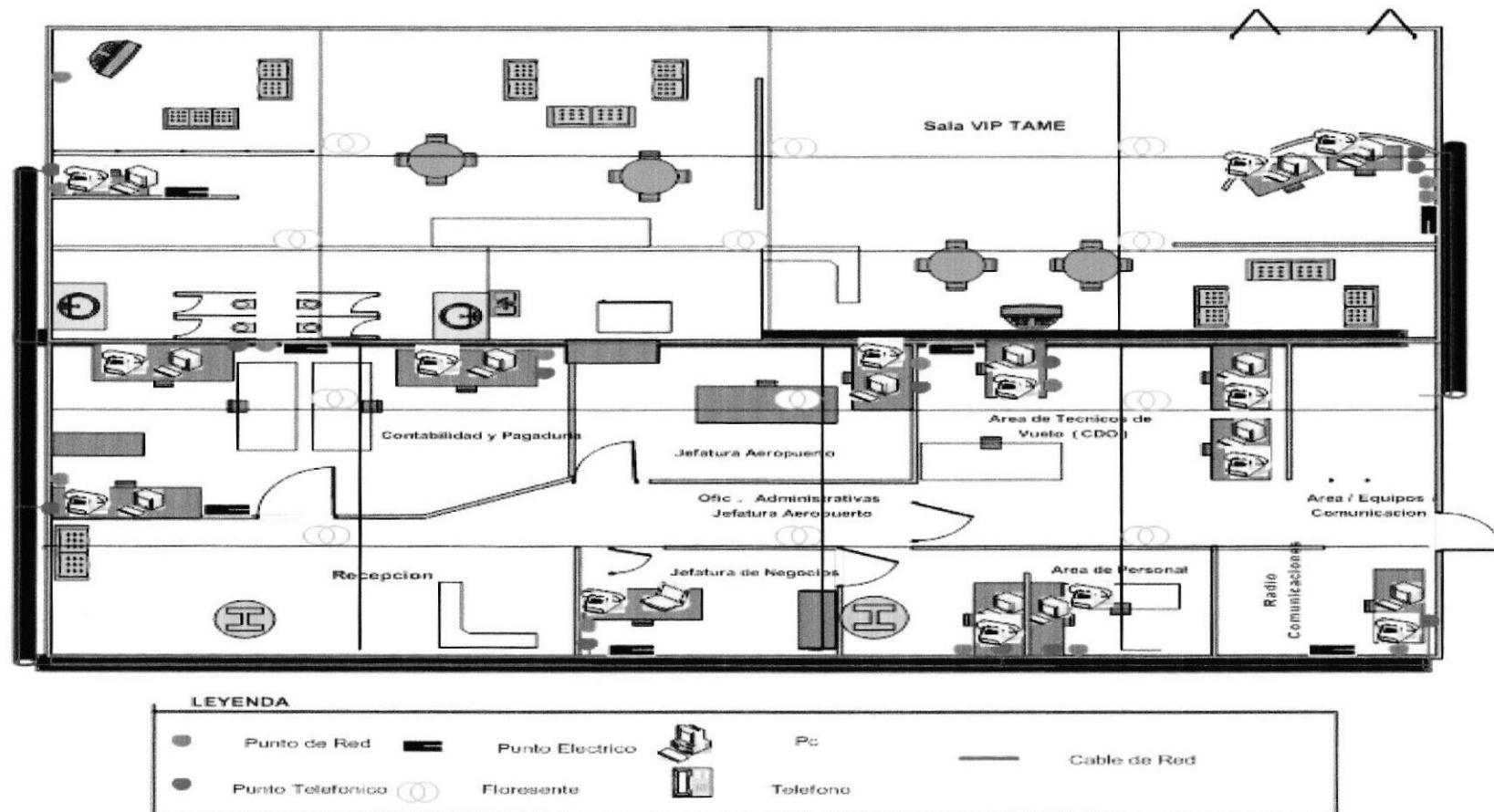


FIGURA 2 - 28: Análisis de piso Aplicativo-Primer Piso A JJO

## 2.7.1.11.- ÁREA DE VENTA DE PASAJES

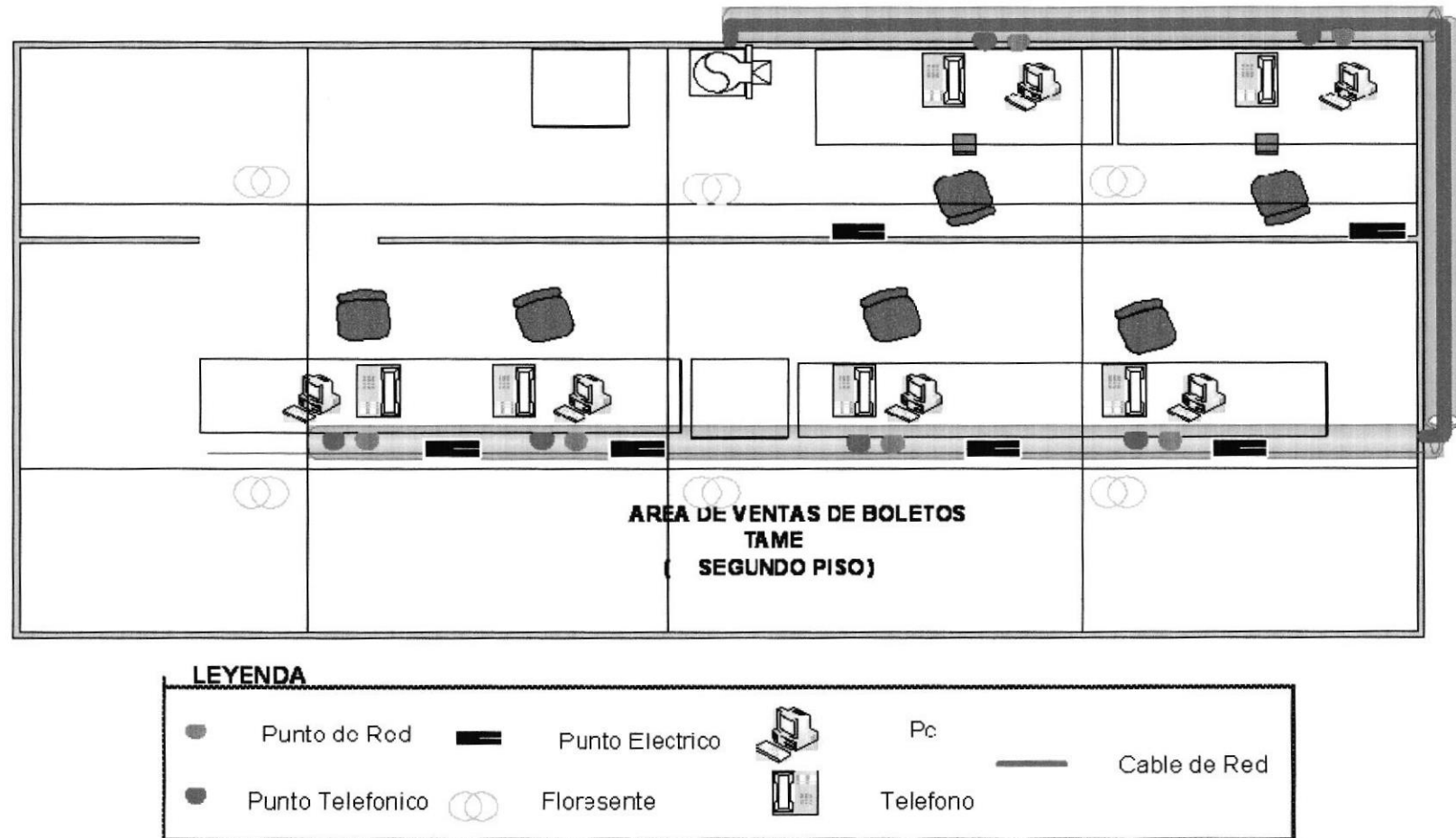


FIGURA 2 - 29: Análisis de piso Aplicativo-Segundo Piso A JJO

## 2.7.1.12.- GERENCIA DE INFORMÁTICA

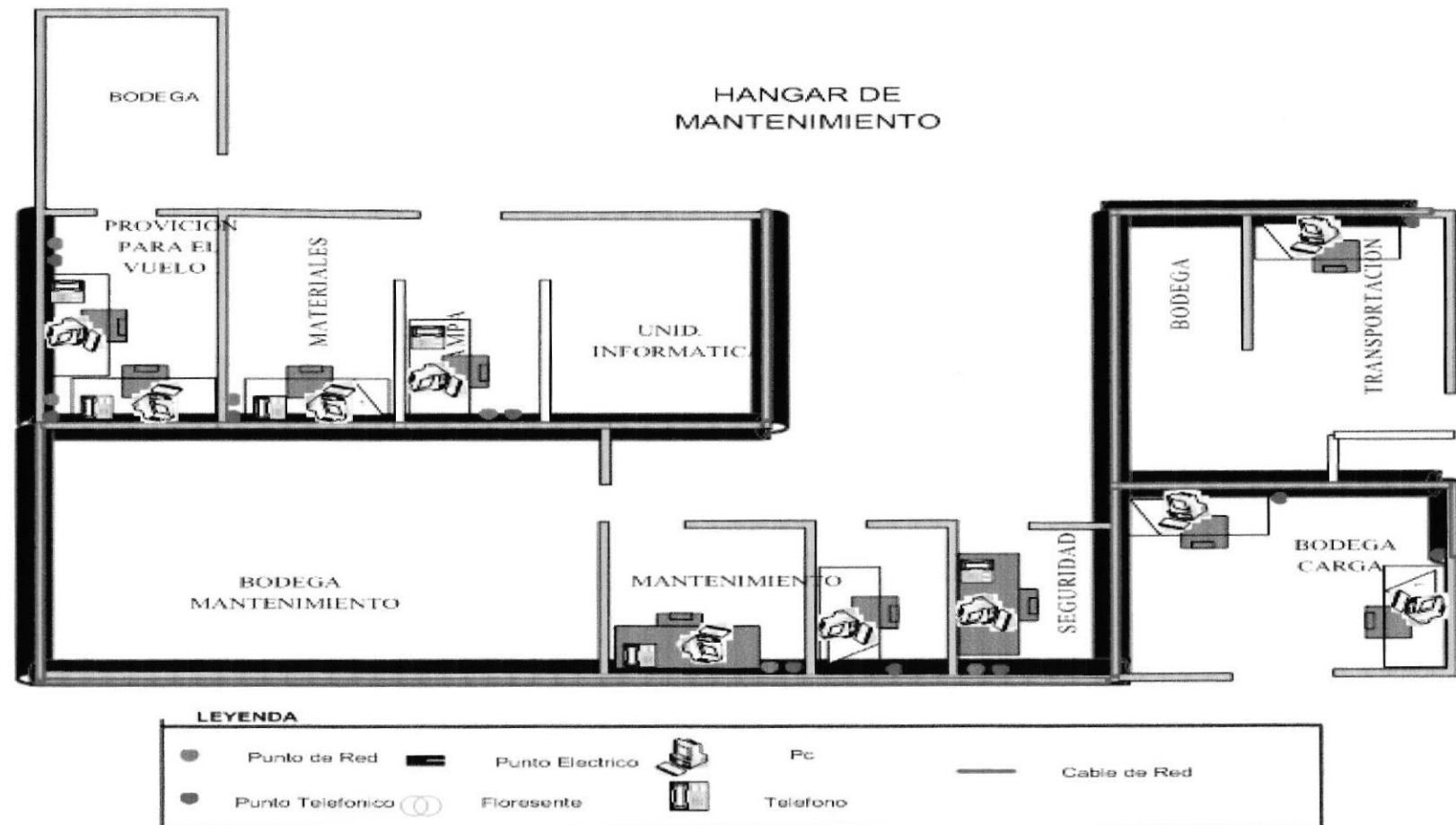


FIGURA 2 - 30: Análisis de piso Aplicativo-Fremir Piso TAME Cargo



## 2.7.1.13.- ÁREA DE SISTEMA

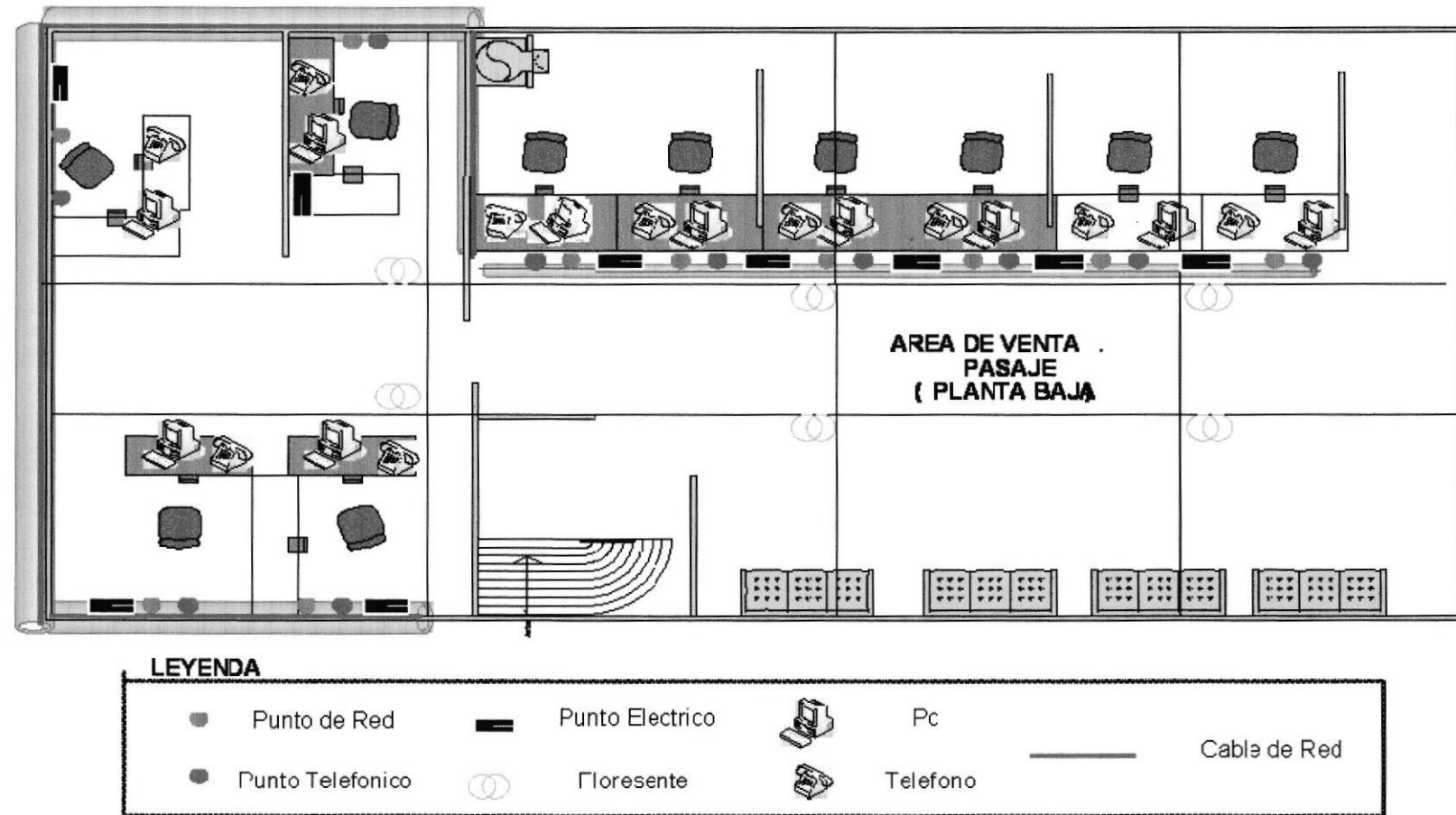


FIGURA 2 - 31: Análisis de piso Aplicativo-Área de Sistema TAME Cargo

## 2.7.1.14.- ÁREA DE VENTAS DE PASAJES

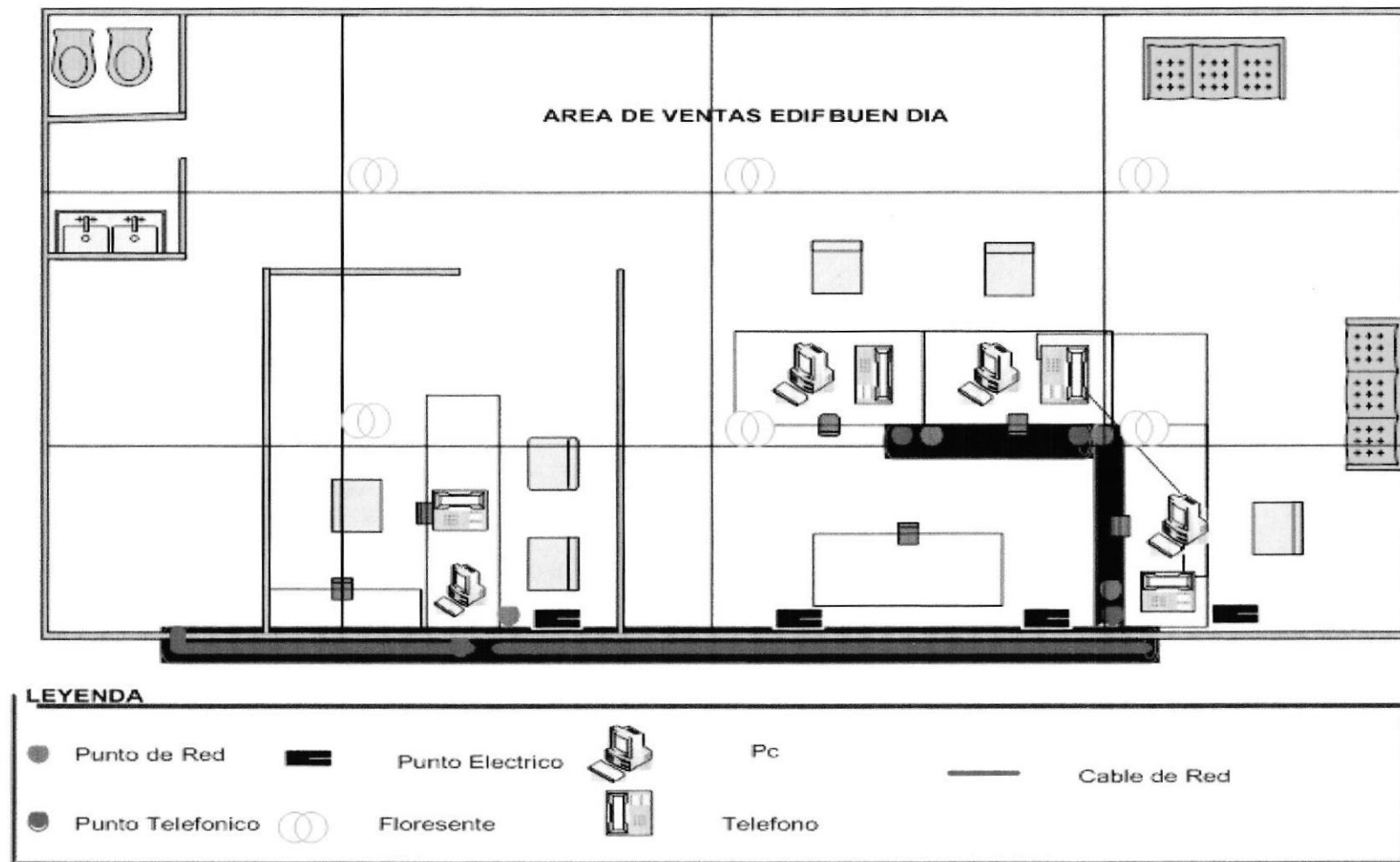


FIGURA 2 - 32: Análisis de piso Aplicativo-Fremir Piso Boina Dia

## 2.7.1.15- ÁREA DE SISTEMAS

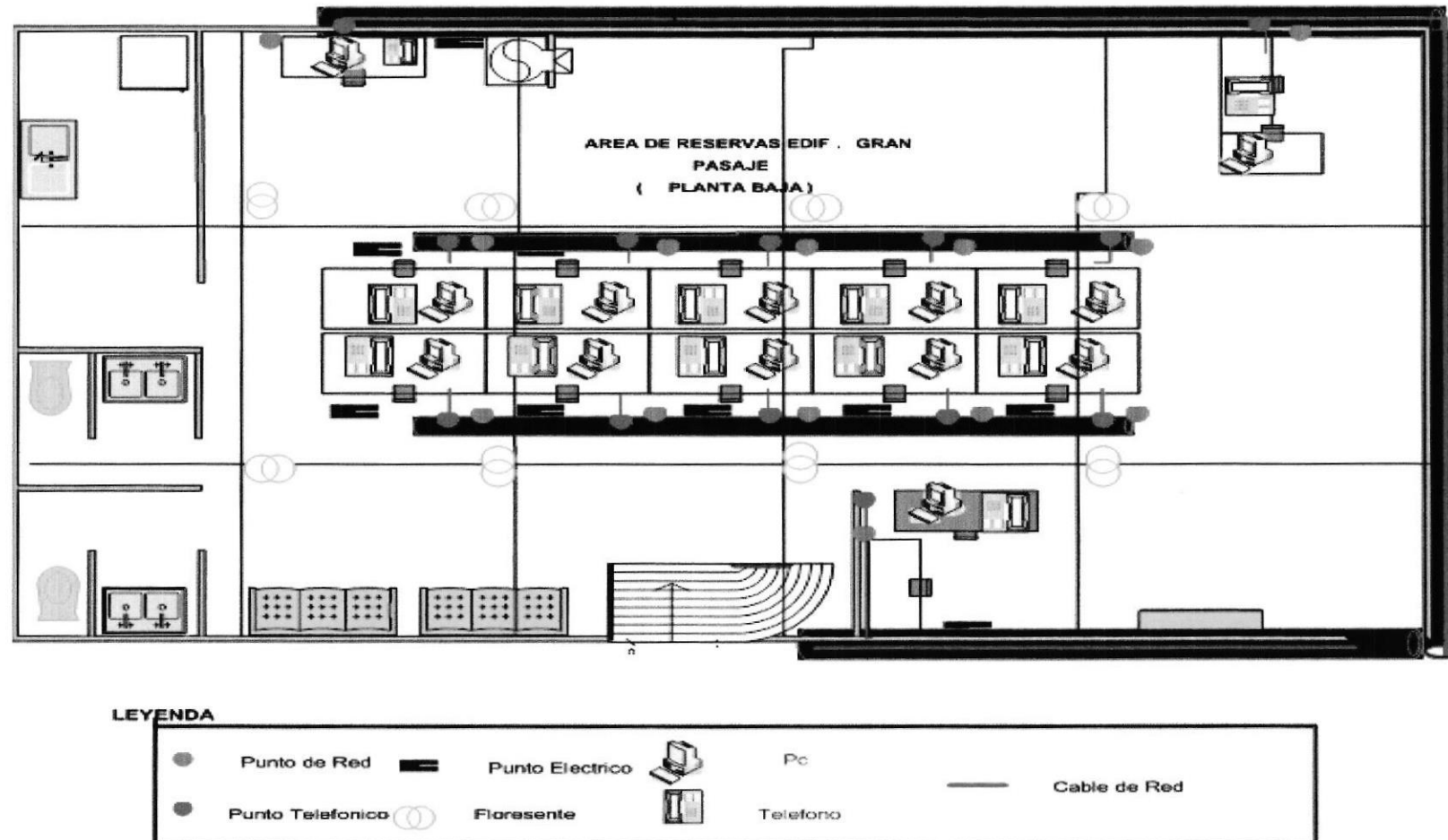


FIGURA 2 - 33: Análisis de piso Aplicativo-Primer Piso Gran Pasajes

## 2.7.1.16.- RESERVACIONES

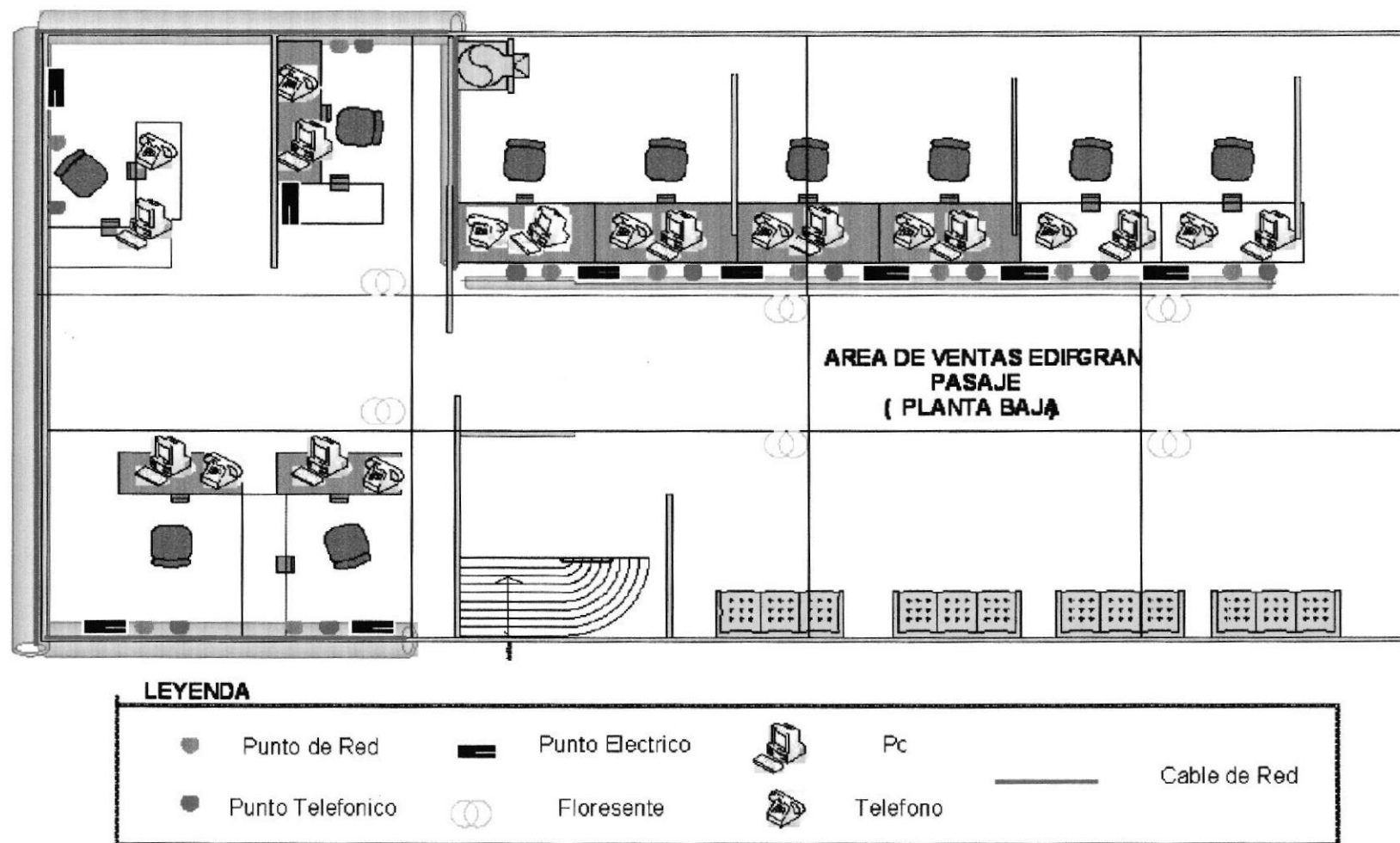
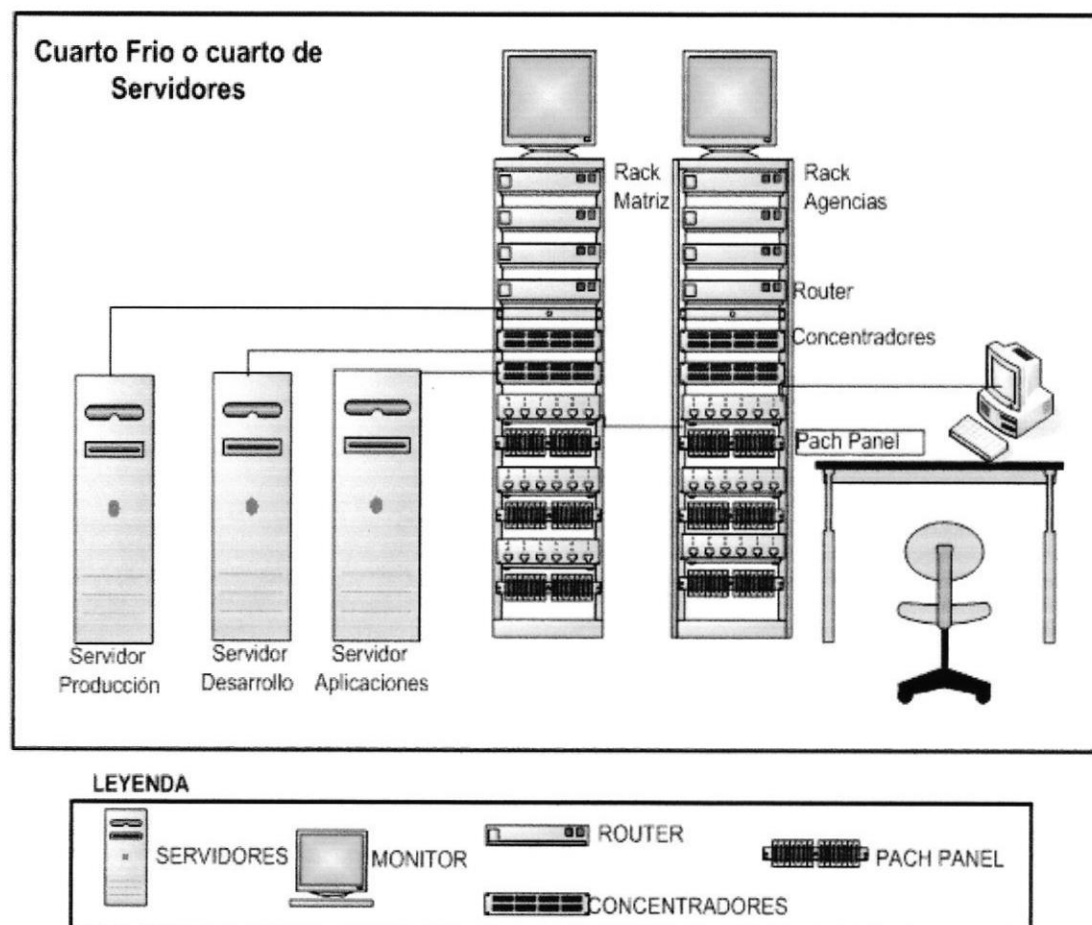


FIGURA 2 - 34: Análisis de piso Aplicative-Segundo Piso Gran Pasajes

## 2.8.- CUARTO DE COMUNICACIÓN (MATRIZ-TAME)



**FIGURA 2 - 35:** Cuarto de Servidores Matriz



## 2.9.- MC MATRIZ TAME

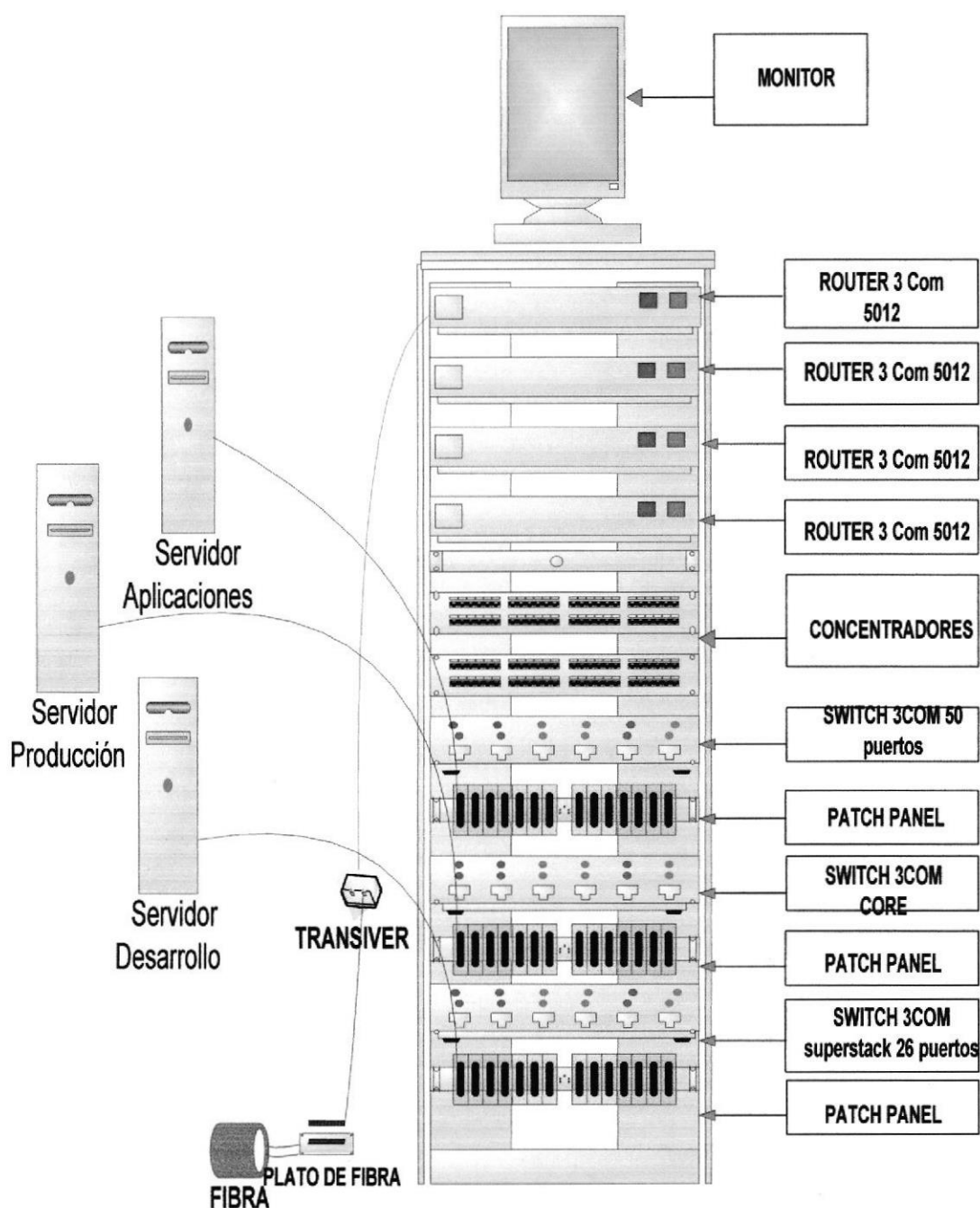


FIGURA 2 - 36: (MC) Rack Principal Matriz

## 2.10.- IC AGENCIA PRINCIPAL MATRIZ TAME

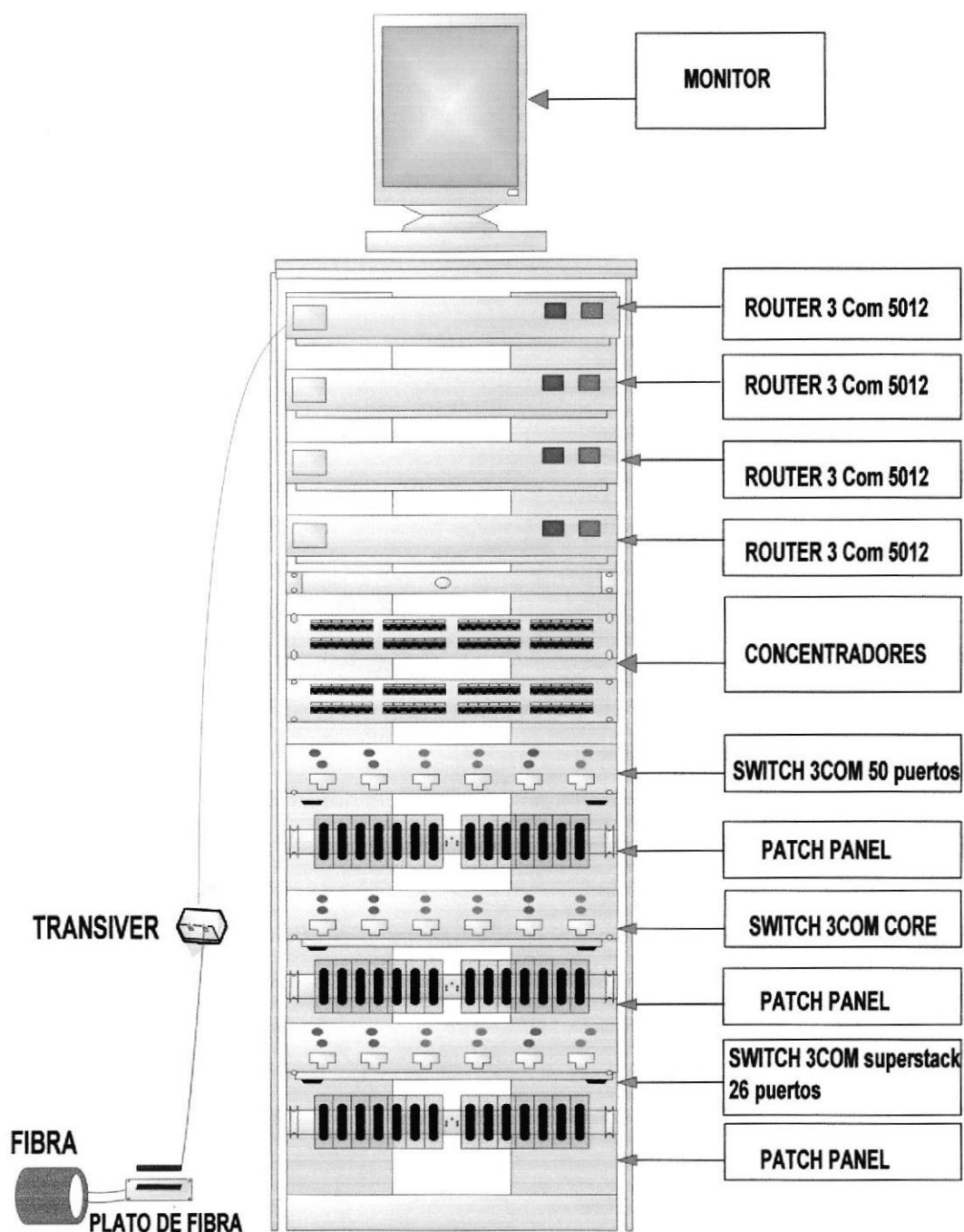


FIGURA 2 - 37: (IC) Rack Agencia Principal Matriz

## 2.11.- MEDIOS DE COMUNICACIÓN

### 2.11.1.- MEDIOS ALÁMBRICOS

Los medios alámbricos utilizados en la Matriz de TAME son marca BELDEN distribuidos de la siguiente manera.

- Cat. 6 en los diferentes pisos administrativos del edificio de esta Matriz, así como de las oficinas Operativas Ubicadas en el Aeropuerto Mariscal Sucre.
- Conexión por Fibra óptica multimodo, conectada desde el backbone de 48 puertos, con terminación de un panel de 6 puertos por cada uno de los 8 pisos de la matriz, con un Ancho de Banda de: 1024 Kbps de los cuales se encuentran distribuidos 512 para los diferentes pisos de la Matriz, 256 para agencia remota del Aeropuerto y 256 agencia de Ventas de pasajes Av. Colon.
- Los medios alámbricos utilizados en las Unidades de Negocios, Sucursales y Agencias de Ventas, distribuidas a Nivel Nacional, son marca NEXXT distribuidos de la siguiente manera Cat. 6 tantos en las áreas administrativas y operativas.

### 2.11.2.- TIPO/ ELEMENTOS NETWORKING UTILIZADOS

Todos los medios alámbricos utilizados en la empresa TAME cuentan con las mismas certificaciones a nivel nacional en todas sus agencias

UBICACION	DESCRIPCION	CANTIDAD	OBSERVACIONES/ MARCAS
TODOS LOS PISOS	PATH PANEL PARA FIBRA	9 (1 POR PISO)	CON 6 PUERTOS
	CONECTORES TIPO ST PARA FIBRA	6 POR PISO	Con adaptadores, path cord de Fibra
PRIMER_PISO INFORMATICA	PANEL DE 48 PUERTOS	1	
	RACKS	4	2 PISO (120 UR) 2 ARMARIOS

**Tabla 2 - 12** Medios de comunicación





## 2.12.- CARACTERÍSTICAS DE LOS DISPOSITIVOS DE CONMUTACIÓN

### 2.12.1.- MATRIZ TAME

Todos los dispositivos de conmutación de la empresa TAME cuenta con la misma característica en todos los cuarto de comunicación

UBICACION	CANT.	TIPO/MARCA	MODELO	CARACTERISITICAS
CUARTO/ SERVIDORES (PRIMER PISO)	2	SWITCH 3COM CORE	7754	Soporta hasta 288 port fast ethernet, 292 port rj45 gb, 3 puertos de 10gb, 20 puertos 100base-x sfp, 20 puertos conexión gbit para fibra multimodo
	1	SWITCH 3COM 50 puertos	4550	48 puertos 10/100base-t autosensing, 2 puertos dual personality 10/100/1000 o puertos sfp gigabit
	1	Modulo de conexión Gigabit/switch		
AREA DE VENTAS	1	SWITCH 3COM superstack 26 puertos	4500	24 puertos 10/100 baset., 2 puertos 10/100/100 sfp gigabit

**Tabla 2 - 13** Dispositivo de Conmutación

## 2.13.- INFRASTRUCTURA WAM

### 2.13.1.- RED WAN DE LA COMPAÑÍA TAME

La red WAN de la Compañía TAME, se encuentra actualmente conformada por 15 redes LAN, cada una de ellas se encuentra instalada en las agencias o Unidades de Negocios que representan a la compañía a nivel Nacional, cabe indicar que para que cada una de estas LAN, puedan estar intercomunicadas con la Matriz de TAME, necesitan de dispositivos de comunicación tales como un router y un switch, para que de esta manera siempre exista la comunicación de datos entre la Matriz de TAME y sus diferentes agencias.

Para tener clara la idea de cómo están intercomunicadas la Matriz con sus agencias, les presentaremos a continuación 1 Grafica que representa del tipo de comunicación y sus características (velocidad, tipo de enlace, interfaz, equipo), axial como una grafica de cada uno de los diferentes equipos de comunicación que se utilizan para dicha transmisión.

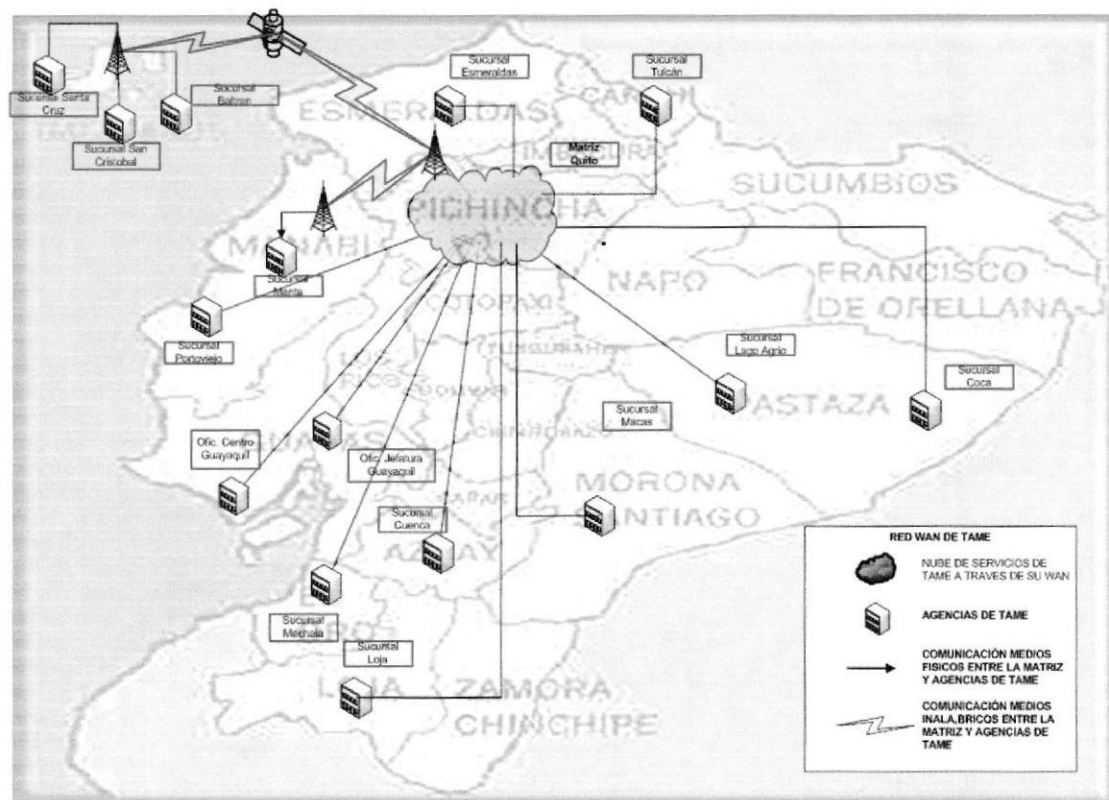


FIGURA 2 - 38: Red Wan de la Compañía TAME

## 2.14.2.- GRÁFICA DE COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS

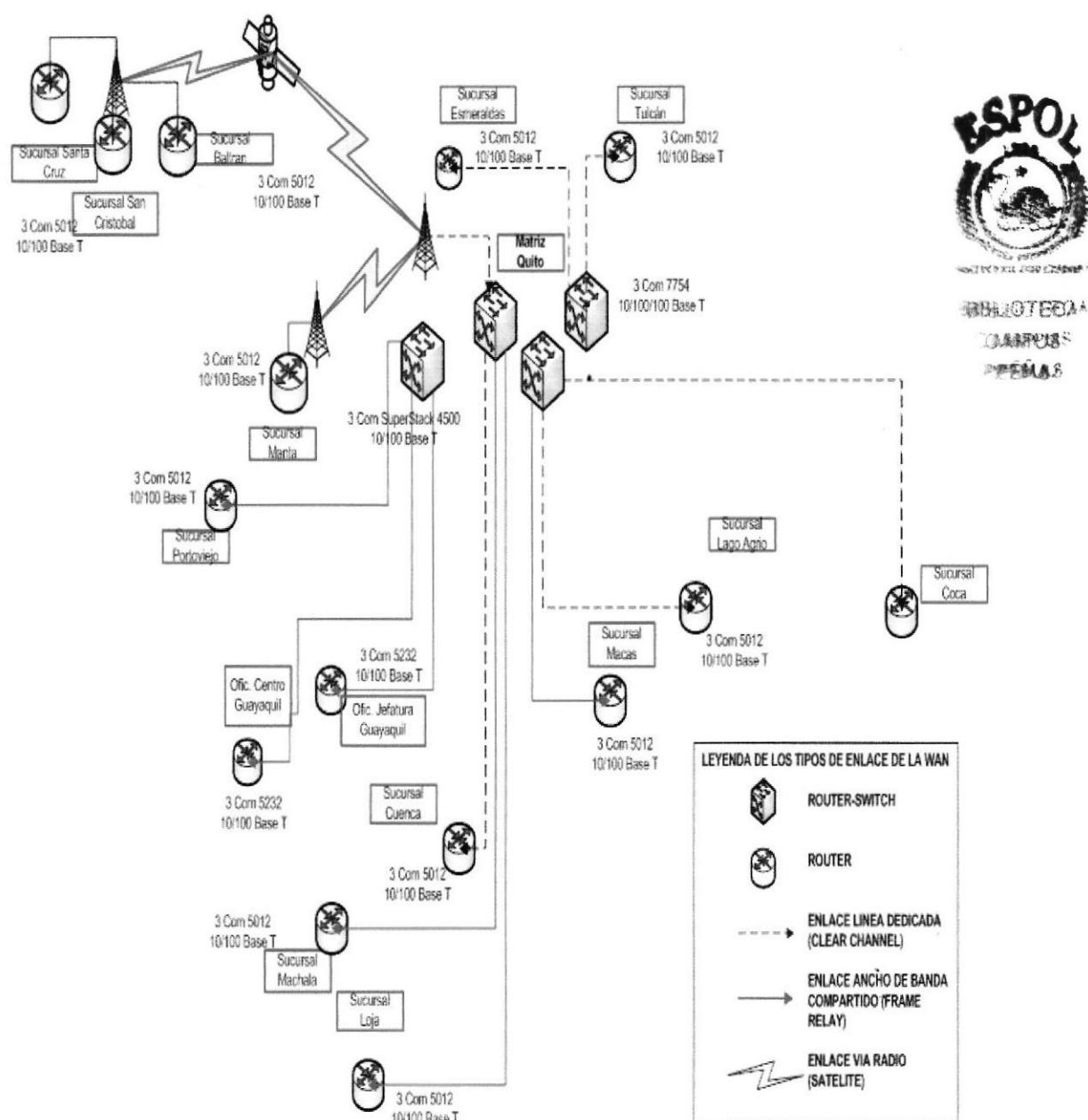


FIGURA 2 - 39: Comunicación Wan de los Dispositivo

## 2.15.- DISPOSITIVOS DE ENRUTAMIENTO

### 2.15.1.- GUAYAQUIL- JOSE JOAQUIN DE OLMEDO

Todos los dispositivos de enrutamiento de la empresa TAME cuenta con la misma característica en todos los cuarto de comunicación

ROUTERS DE LA WAN DE TAME (MATRIZ – UNIDADES DE NEGOCIOS)		
CANT	CARACTERÍSTICAS	VELOCIDAD
25	3 Com 5232 Dos puerto Un puerto serial de alta velocidad (Sync/Async), 2port channelized E/1PRI/MIM 4 port Serial MIM	10/100 base T

**Tabla 2 -14** Dispositivo de enrutamiento

### 2.16.2.- TERMINAL AEREA QUITO

UBICACION	CANTIDAD
Agencia Remota	15
Agencia de Paso	10

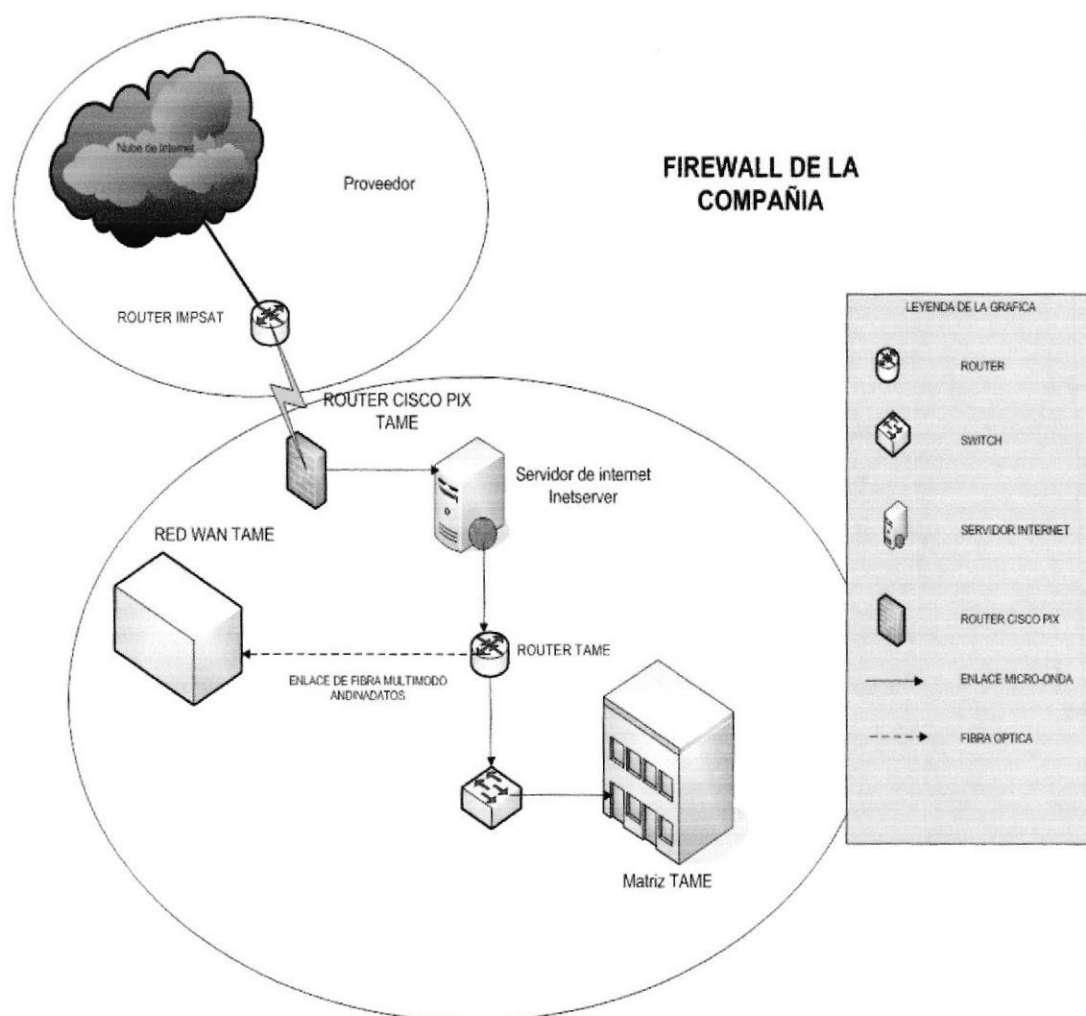
**Tabla 2 - 15** Dispositivo de enrutamiento

Características:

- Conecta Ethernet LANs a WANs via ISDN
- Conexión Serial Asíncrono y Serial Asíncrono
- Suporia Frame Relay, Línea Dedicada.
- 1024 Kbps para el resto de Agencias que conforman la WAN, dependiendo el consumo de datos a Nivel de ella.

## 2.17.- INFRAESTRUCTURA DE SEGURIDAD DE LA REDES WAN

La empresa TAME cuenta con un firewall de seguridad a nivel de hardware basado en un routers cisco PIX propio de la empresa obteniendo seguridad en la matriz. En las sucursales de guayaquil no cuenta con sus respectivos firewall



**FIGURA 2 - 40:** Seguridad de la red Wan de TAME

## 2.18.- INFRAESTRUCTURA DE COMUNICACIÓN DE INTERNET

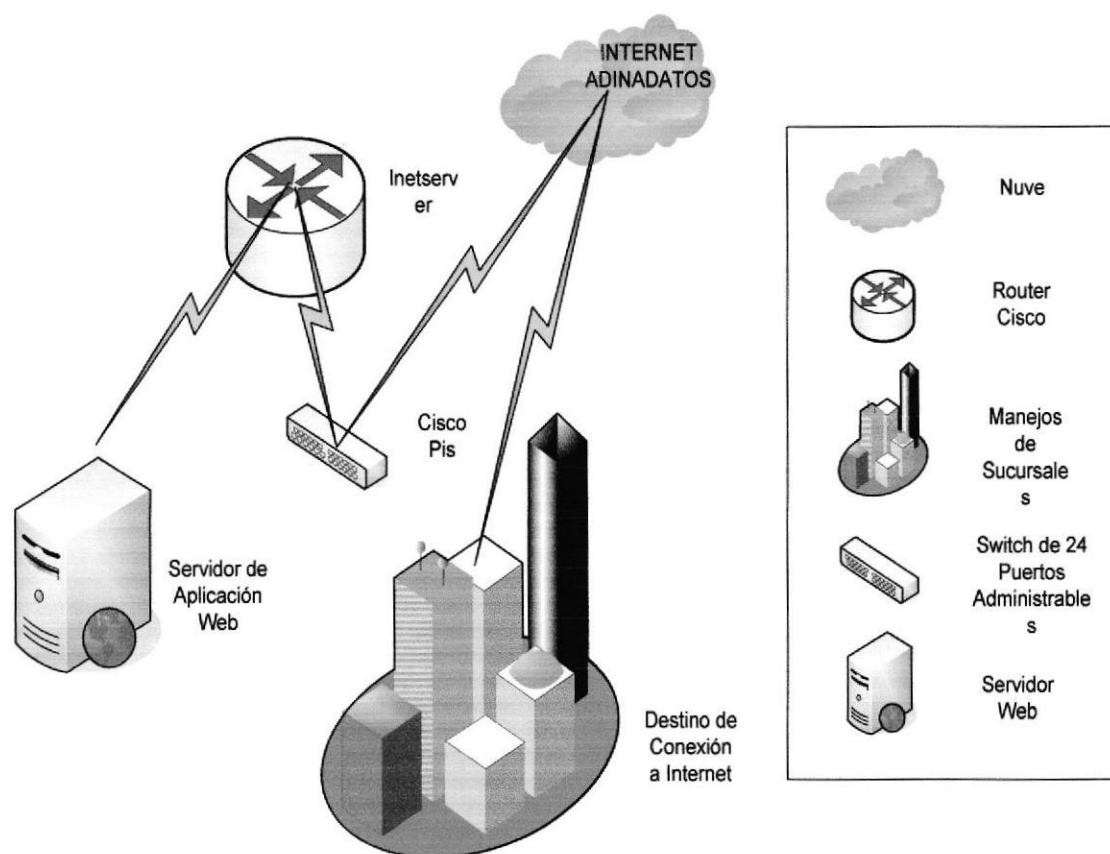


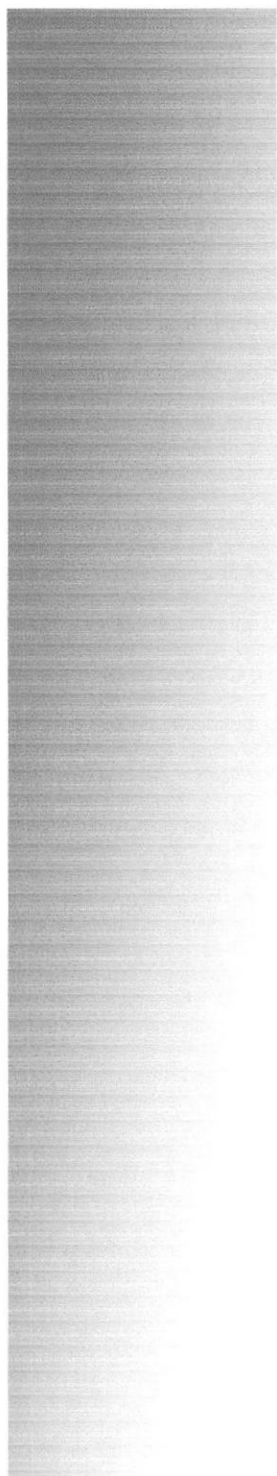
FIGURA 2 - 41: Comunicación de Internet

Guayaquil, actualmente este tiene un canal de comunicaciones total de 256Kbps, si queremos utilizar este servicio ocuparemos el 50% de la capacidad de este canal es decir 128 Kbps, para el uso de Internet y 128 Kbps, para el uso del resto de aplicaciones que se maneja en la WAN, tal es el caso del sistema Principal con que cuenta la empresa (SIGETAME), en otras palabras estamos usando de manera compartida el mismo canal de comunicaciones que conecta un nodo de la WAN a otro ubicado en la Matriz de TAME, pero con un ancho de banda exclusivamente para lo referente el servicio de Internet,, es decir por medio del uso de un ISP a través de una conexión RDSI, propio de la empresa, podemos administrar el uso de Internet, por un determinado grupo de usuarios que forman parte de la red WAN de TAME, con la finalidad de administrar y llevar un control de recursos en la WAN, no olvidando la implementación como medio de seguridad de un corta fuegos, el mismo que por medio de un Proxy establecido, se optimiza la seguridad con lo referente a conexiones a Internet o que no pertenezcan al Dominio de la Empresa.

## **2.19.- PROBLEMAS ENCONTRADOS**

- Lentitud en la comunicación WAN entre Matriz y Sucursales
- No existe políticas en la navegación de Internet en la red LAN Matriz
- A nivel de las LAN en las sucursales de Guayaquil constantemente llegan códigos maliciosos(virus informáticos)
- Frecuente congestionamiento en la red LAN





## CAPÍTULO 3

### PROPUESTA



### 3.- SOLUCIÓN PROPUESTA

#### 3.1.- PROBLEMAS ENCONTRADOS

PROBLEMA	CAUSA	EFEECTO
Lentitud en la comunicación WAN entre Matriz y Sucursales	La compañía no a implementado una comunicación directa entre Sucursales en Guayaquil	La comunicación de transmisión de datos entre sucursales es lenta
No existe políticas en la navegación de Internet en la red LAN Matriz	No hay un servidor Proxy LAN Matriz	Navegación sin restricción tanto a contenido como horario
A nivel de las LAN en las sucursales de Guayaquil constantemente llegan códigos maliciosos(virus informáticos)	No existe un Antivirus a nivel de software en las sucursales de la ciudad de Guayaquil.	Perdidas de información y daños de archivos en las PC
congestionamiento en la red LAN	No existe Segmentación en la red LAN	Broadcast y Trafico en la LAN

**Tabla 3 - 16** Problemas encontrados

**3.2.- SOLUCIÓN PROPUESTA**

<b>PROBLEMA</b>	<b>SOLUCION</b>	<b>ALCANCE</b>
Lentitud en la comunicación WAN entre Matriz y Sucursales	Implementar una MAN en la ciudad de Guayaquil en todas las sucursales.	No habrá pérdida de paquetes de datos Los paquetes de datos llegaran rápidamente a nivel de la MAN
No existe políticas en la navegación de Internet en la red LAN Matriz	Implementar un servidor Proxy a nivel de la Matriz	Mejor control de la navegación al nivel de la red Lan en Matriz
A nivel de las LAN en las sucursales de Guayaquil constantemente llegan códigos maliciosos(virus informáticos)	Implementar un antivirus a nivel de software	Mejora en la Seguridad de los datos a nivel de la Red LAN en las Sucursales.
congestionamiento en la red LAN	Creación de Vlan por departamentos	Reducir dominio de Broadcast en nuestra red LAN

**Tabla 3 - 17 Solución propuesta**

### 3.3.- ESTUDIO DE FACTIBILIDAD

#### 3.3.1.- ALTERNATIVA "A"

El objetivo de esta alternativa es la implementación de una red MAN, trabajo asignado a la Compañía Transferdatos, y además se realizarán la compra de los dispositivos por parte de la empresa.

##### 3.3.1.1.- FACTIBILIDAD TÉCNICA HARDWARE

CANT	DESCRIPCION	TIPO	UBICACION
1	<b>MARCA HP</b> Processor Intel Pentium Processor 640, 3.2 GHz/800MHz, Cache Memory 2MB L2 cache(2) GB RAM (2) Tarjetas de Red 100/1000, solo en un equipo Storage Controller Integrated 2 port embedded SATA RAID (RAID levels 0, (3) 80-GB NHP SATA	SERVIDOR PROXY	Cuarto de Servidores de matriz- Guayaquil En el Aeropuerto JJO.
2	<b>MARCA HP</b> MODELO ML110 G3 3.2- 2M/800 1GB NHP SATA2M/800 1GB NHP SATA	SERVIDOR CORREO/SER VIDOR WEB	
1	Router 3com 5232 con 2 puertos Canalizados E1/PR1/MIM1 y 4 puertos seriales MIM	ROUTER	
4	POWERWARE (1 6KVA, 3 2KVA)	UPS	

**Tabla 3 - 18** Factibilidad técnica

## 3.3.1.2.- FACTIBILIDA ECONÓMICA

## 3.3.1.2.1.- COSTO HARDWARE

CANT.	DESCRIPCIÓN	PRECIO UNIT.	TOTAL
1	SERVIDOR PROXY	\$1.500,00	\$1.500,00
1	SERVIDOR CORREO	\$1.100,00	\$1.100,00
1	SERVIDOR WEB	\$1.100,00	\$1.100,00
1	Router 3com 5232	\$3.000,00	\$3.000,00
4	UPS 2 KVA PowerWare	\$300,00	\$1.200,00
<b>Costo total adquisicion de hardware</b>			<b>\$7.900,00</b>

Tabla 3 - 19 Costo de hardware

## 3.3.1.2.2.- COSTO SOFTWARE

CANT.	DESCRIPCIÓN	PRECIO UNIT.	TOTAL
1	Software Linux Fedora 3	Gratis	
60	Licencias f-secure	\$20,00 * licencia	\$1.200,00
<b>Costo Total Adquisicion de Software</b>			<b>\$1.200,00</b>

Tabla 3 - 20 Costo de software

## 3.3.1.2.3.- COSTO DE LOS ENLACES

CANT.	DESCRIPCIÓN	PRECIO UNIT.	TOTAL
2	<b>Enlace microonda</b> Enlaces locales de 128Kbps, con una frecuencia de 2.4 Ghz y una ganancia 2.4 Dbi pago de servicio mensual	\$150,00	\$300,00
1	<b>Enlaces de fibra</b> Tendido de 3km de fibra Multimodo con ancho de banda 800 MHZ para enlace local entre Agencia Principal GYE en la Terminal José Joaquín de Olmedo y Áreas de Carga y Mantenimiento pago de servicio mensual	\$300,00	\$300,00
1	<b>Enlace Internet</b> Enlace dedicado con conexión no compartida, de 1 a 1, con 256Kbps de subida y bajada, usada para Internet (Servicio provisto por el carrier bajo Contrato, solo para Guayaquil), costo mensual	\$350,00	\$350,00
<b>Costo Mensual por alquiler de enlaces</b>			<b>\$ 950,00</b>
<b>COSTO TOTAL</b>			<b>\$ 950,00</b>

Tabla 3 - 21 Costo de enlaces



## 3.3.1.3.- COSTOS OPERATIVOS

No Semanas	Persona o Grupo Implicada	Costo Semanal	Costo Total	Total Fase
FASE DE DISEÑO LAN Y MAN				
1	1 Ing. en Telecomunicaciones	\$ 300	\$ 300	\$ 500
1	1 Técnico en Telecomunicaciones	\$ 200	\$ 200	
FASE DE IMPLEMENTACIÓN MAN				
1	1 Ing. en Telecomunicaciones	\$ 300	\$ 300	\$ 1,250
1	1 Maestro Electricista	\$ 150	\$ 150	
1	4 Técnico en Telecomunicaciones	\$ 200	\$ 800	
FASES DE PRUEBA MAN				
1	1 Ing. en Telecomunicaciones y 1 Asistente de Redes	\$ 470		
FASE DE DOCUMENTACIÓN LAN Y MAN				
1	1 Ing. en Telecomunicaciones	\$200		
Costo Total Operativo				\$2.370,00

Tabla 3 - 22 Costo operativo

## 3.3.1.4.- FACTIBILIDAD OPERATIVA

No.	Personal implicado	DESCRIPCION	Tiempo
FASE DE ANALISIS LAN			
1	Ing. en Telecomunicaciones	Análisis de falencias halladas en las redes	1 semana
2	Asistentes (técnicos en redes)	Verificación Cableado de las instalaciones	
FASE DE DISEÑO LAN Y MAN			
1	Ing. en Telecomunicaciones	Factibilidades Técnicas para los Enlaces	1 semana
FASE DE IMPLEMENTACION MAN			
1	Ing. Telecomunicaciones	Implementación enlace entre sucursales	1 semana
1	Técnico en Redes	Configuración Routers e Implementación enlace entre sucursales	
1	Maestro Electricista	Instalación de tomas eléctricas a Tierra e instalación de UPS	
1	Técnico en Redes	Instalación y configuración de Servidores	
FASE DE PRUEBA WAN Y LAN			
1	Ing. en Telecomunicaciones y Asistente en Redes	Pruebas de transmisión de paquetes de datos y tiempos de respuesta en enlaces principales. Verificación de Servidores y pruebas reales con Manejo de Correo Lotus Notes y Actualización de Antivirus	1 semana
FASE DOCUMENTACION LAN Y MAN			
1	Ing. en Telecomunicaciones	Entrega de Manuales sobre Red MAN, con diagramas y tablas de registros IP para nuevos equipos	1 semana

Tabla 3 - 23 Factibilidad operativa



**CUADRO DE COSTOS TOTALES DE LA ALTERNATIVA "A"**

DETALLE	PRECIO
➤ Costo Total Adquisición de Hardware	\$7.900,00
➤ Costo Total Adquisición de Software	\$1.200,00
➤ Costo Mensual por alquiler de enlaces	\$ 950,00
➤ Costo de Servicios Profesionales	\$2.370,00
Costo Total Factibilidad A	\$12.420,00
IVA 12%	\$1.490,40
<b>COSTO TOTAL</b>	<b>\$13.910,4</b>

Tabla 3 - 24 Costo totales

**COSTO TOTAL DE LA PROPUESTA "A": \$13.910,4****3.3.1.5.- VENTAJAS Y BENEFICIOS DE ALTERNATIVA "A"****3.3.1.5.1.- VENTAJAS**

- Mejora la seguridad a nivel de Hardware.
- Mejora la transmisión de datos.
- Mejora el tiempo de respuesta que pueda surgir con los dispositivos.
- Optimiza el tráfico de la red.
- Mejora la administración de la red.
- Mayor disponibilidad de las direcciones IP.
- Dominio de Colisión más pequeño.
- Mejora la administración remota de equipos.
- Mayor seguridad en la red.
- La transmisión de datos no se vera afectada por cortes de energía
- El Servicio al publico no se vera afectado por caída del Sistema por daño en el enlace de comunicaciones Principal, debido a su canal de backup implementado

**3.3.1.5.2.- BENEFICIOS**

La implementación de esta alternativa, la empresa TAME mejorara sus servicios y agilizará su atención a sus clientes, siendo así más competitiva con la demás aerolíneas del país

**3.3.1.6.- FORMA DE PAGO Y LAPSO A DESARROLLARSE**

Para la aplicación del proyecto se lo hará en 3 pagos:

- El 60% corresponderá al costo de validez de la propuesta incluye la etapa de análisis y diseño, martes 16 de julio de 2007.
- El 20% corresponderá a la etapa de implantación donde se adquiere todo el hardware y firma de contrato con el Carrier, martes 30 de julio de 2007.
- El 20% final corresponderá a la terminación de la etapa de prueba y documentación, viernes 24 de agosto de 2007.

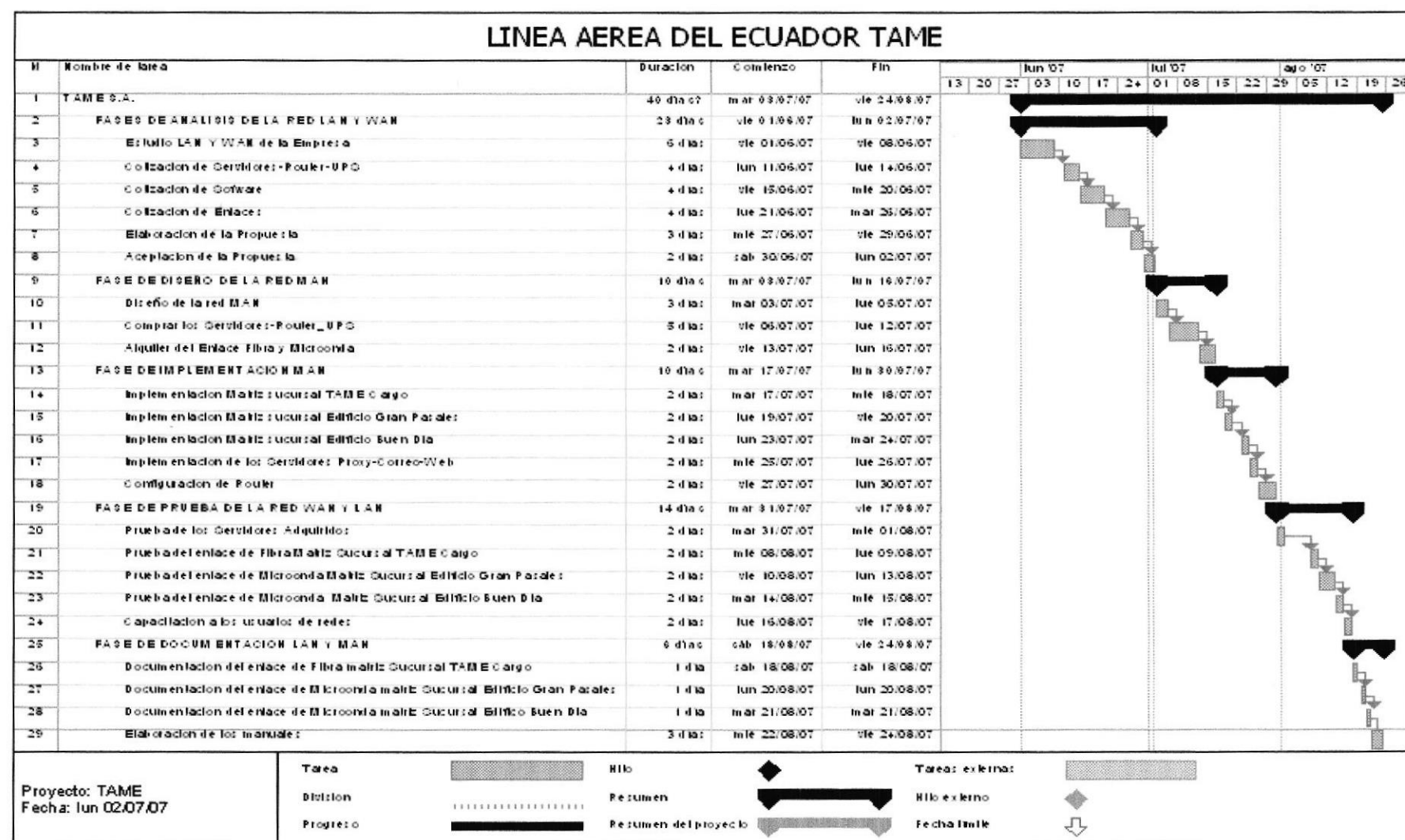
**3.3.1.7.- GARANTIA**

Teniendo como punto final la firma de conformidad entre el Cliente y la Empresa contratada para la aplicación del proyecto aquí aplicado, dando a conocer las garantías correspondientes del caso, como el soporte técnico en las correcciones futuras a implementar, con un costo a parte, de acuerdo al costo Hora de la mano de Obra.

- Para los equipos que van a funcionar como servidores, se dará un soporte técnico y una garantía de 3 meses.
- Para los dispositivos de comunicación se ofrecerá una garantía de 12 meses sin costo alguno.



## 3.3.1.8.- CRONOGRAMA DE TRABAJO



**3.3.2.- ALTERNATIVA "B"**

La diferencia con la alternativa A es que en esta alternativa voy a alquilar los dispositivos de comunicación (Modem y un Router Principal)

**3.3.2.1.- FACTIBILIDAD TÉCNICA****3.3.2.1.2.- EQUIPOS CÓMPUTOS (PROPIO DE LA EMPRESA)**

CANT	DESCRIPCION	TIPO	UBICACION
1	PC CLON Processor Intel Pentium Processor 640, 3.2 GHz/800MHz, Cache Memory 2MB L2 cache. (2) GB RAM (2) Tarjetas de Red 100/1000, solo en un equipo Storage Controller Integrated 2 port embedded SATA RAID (RAID levels 0, (3) 80-GB NHP SATA	SERVIDOR PROXY	Cuarto de Servidores de matriz- Guayaquil En el Aeropuerto JJO.
2	PC CLON MODELO ML110 G3 3.2- 2M/800 1GB NHP SATA2M/800 1GB NHP SATA	SERVIDOR CORREO/ SERVIDOR WEB	
4	POWERWARE (1 6KVA, 3 2KVA)	UPS	

**Tabla 3 - 25** Factibilidad técnica



## 3.3.2.1.3.- DISPOSITIVOS DE ALQUILER CON EL ISP

CANT.	Descripción	Ubicación
1	ROUTER ➤ 3com 5232 ➤ 2 puertos canalizados E1/PR1/MIM1 ➤ 4 puertos seriales MIM	Cuarto de Servidores de matriz-Guayaquil En el Aeropuerto JJO.

Tabla 3 - 26 Alquiler del Router principal

## 3.3.2.2.- FACTIBILIDAD ECONÓMICA

## 3.3.2.2.1.- COSTO EQUIPOS CÓMPUTOS

Cant.	Descripción	Precio Unit.	Total
3	PC CLONE PROCESADOR INTEL CORE 2 DUO	\$800,00	\$2.400,00
4	UPS 2 KVA PowerWare	\$300,00	\$1.200,00
<b>Costo Total Adquisición de Hardware</b>			<b>\$3.200,00</b>

Tabla 3 - 27 Costo de equipos de computo

## 3.3.2.2.2.- COSTO DE ALQUILER

Cant.	Descripción	Precio Unit.	Total
1	ROUTER	\$30,00	\$30,00
<b>Costo de alquiler del dispositivo</b>			<b>\$30,00</b>

Tabla 3 - 28 Costo de alquiler de dispositivos

## 3.3.2.2.3.- COSTO SOFTWARE

Cant.	Descripción	Precio Unit.	Total
1	Software Linux Fedora 5.0	Gratis	
60	Licencias Panda Interprice Business c/licencia	\$20,00	\$1.200,00
<b>Costo Total Adquisición de Software</b>			<b>\$1.200,00</b>

Tabla 3 - 29 Costo de software

## 3.3.2.2.4.- COSTO DE LOS ENLACES PRINCIPALES (INTERPROVINCIAL Y LOCALES)

Cant.	Descripción	Precio Unit.	Total
2	<b>Enlace microonda</b> Enlaces locales de 128Kbps, con una frecuencia de 2.4 Ghz y una ganancia 2.4 Dbi pago de servicio mensual	\$150,00	\$300,00
1	<b>Enlaces de fibra</b> Tendido de 3km de fibra Multimodo con ancho de banda 800 MHZ para enlace local entre Agencia Principal GYE en la Terminal José Joaquín de Olmedo y Áreas de Carga y Mantenimiento pago de servicio mensual	.\$300,00	\$300,00
1	<b>Enlace Internet</b> Enlace dedicado con conexión no compartida, de 1 a 1, con 256Kbps de subida y bajada, usada para Internet (Servicio provisto por el carrier bajo Contrato, solo para Guayaquil), costo mensual	\$350,00	\$350,00
<b>Costo Mensual por alquiler de enlaces</b>			<b>\$ 950,00</b>
<b>COSTO TOTAL</b>			<b>\$ 950,00</b>

Tabla 3 - 30 Costo de enlaces principal



## 3.3.2.3.- COSTOS OPERATIVOS

No Semanas	Persona o Grupo Implicada	Costo Semanal	Costo Total	Total Fase
FASE DE DISEÑO LAN Y MAN				
1	1 Ing. en Telecomunicaciones	\$300	\$300	\$450,00
1	1 Técnico en Telecomunicaciones	\$150	\$150	
FASE DE IMPLEMENTACIÓN MAN				
1	1 Ing. Telecomunicaciones	\$300	\$300	\$800,00
1	2 técnicos de Telecomunicaciones	\$200	\$400	
1	1 Maestro Electricista	\$100	\$100	
FASES DE PRUEBA MAN				
1	1 Ing. en Telecomunicaciones y 1 Asistente de Redes	\$450		
FASE DE DOCUMENTACIÓN LAN Y MAN				
1	1 Ing. en Telecomunicaciones	\$300		
Costo Total Operativo				\$2.000.00

Tabla3 - 31 Costo operativo



## 3.3.2.4.- FACTIBILIDADES OPERATIVAS

No.	Personal implicado	DESCRIPCION	Tiempo
FASE DE ANALISIS LAN Y WAN			
1	Ing. Telecomunicaciones	Análisis de falencias halladas en las redes actuales	1 semana
2	Asistentes (técnicos en redes)	Verificación instalaciones actuales	
FASE DE DISEÑO LAN Y MAN			
1	Ing. en Telecomunicaciones	Segmentación de Redes actuales	1 semana
1	Técnico en Telecomunicaciones	Factibilidades Técnicas para los Enlaces	
FASE DE IMPLEMENTACION LAN Y MAN			
1	Ing. en Telecomunicaciones	Aplicación de Segmentación y standardización de Nombres para PCS.	1 semana
1	Maestro Electricista	Instalación de tomas eléctricas a Tierra e instalación de UPS	
1	Técnicos en telecomunicaciones	Tendido de fibra óptica multimodo	
FASE DE PRUEBA LAN Y MAN			
1	Ing. Telecomunicaciones y Asistente	Pruebas de transmisión de paquetes de datos y tiempos de respuesta en enlaces principales (Interprovincial y locales) Verificación de Servidores y pruebas reales con Manejo de Servidores y Actualización de Antivirus	1 semana
FASE DOCUMENTACION LAN Y WAN			
1	Ing. en Telecomunicaciones	Entrega de Manuales sobre Red MAN, con diagramas y tablas de registros IP para nuevos equipos	1 semana

Tabla3 - 32 Factibilidad operativas

**CUADRO DE COSTOS TOTALES DE LA ALTERNATIVA B**

DETALLE	PRECIO
➤ Costo Equipos Cómputos	\$3.202,00
➤ Costo de Alquiler	\$30,00
➤ Costo Software	\$1.200,00
➤ Costo de los Enlaces	\$950,00
➤ Costos de Servicios Profesionales	\$2.000,00
<b>Costo Total Factibilidad B</b>	<b>\$7.382,00</b>
IVA 12%	\$885,84
<b>COSTO TOTAL</b>	<b>\$ 8.268,24</b>

Tabla 3 - 33 Costo total de la alternativa B

**COSTO TOTAL DE LA PROPUESTA "B": \$8.268,24****3.3.2.5.- VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA "B"**

Las ventajas de esta alternativa son similares a la alternativa "A", con la diferencia que para la implementación de la red MAN, se da la opción de abaratar costos en la compra del hardware utilizado en la instalación de los Servidores, así como el alquiler de los dispositivos al mismo carrier que nos brinda el Servicio de los enlaces, manteniéndose el la prioridad, de implementar Seguridades a la red MAN tanto a Nivel de Hardware como de Software, y la debida optimización en la distribución y uso del canal de comunicación principal con los enlaces locales.

**3.3.2.5.1.- VENTAJAS**

- Existe un ahorro de \$ 5.642.16 en el costo total de la propuesta dando solución a los principales problemas encontrados.
- Pese a los costos reducidos de los equipos recomendados, estos cumplen a cabalidad con su objetivo.
- Resultados eficientes en cuanto a la administración de los dispositivos.
- Reducidos costos por mantenimiento.
- Alto nivel de seguridad de hardware como software.
- Optimizar el tráfico en la red.
- Mayor disponibilidad de IP, dominio de colisión más pequeños.
- Mejora la administración y transmisión de datos.
- Mejora la seguridad a nivel de hardware

**3.3.2.5.2.- BENEFICIOS**

La implementación de esta alternativa, la empresa TAME mejorara sus servicios y agilizará su atención a sus clientes, siendo así más competitiva con la demás aerolíneas del país





**3.3.2.6.- FORMA DE PAGO Y LAPSO A DESARROLLARSE**

Para la aplicación del proyecto se lo hará en 3 pagos:

- El 60% corresponderá al costo de validez de la propuesta incluye la etapa de análisis y diseño, martes 16 de julio de 2007
- El 20% corresponderá a la etapa de implantación donde se adquiere todo el hardware y firma de contrato con el Carrier, martes 30 de julio de 2007
- El 20% final corresponderá a la terminación del etapa de prueba y documentación, viernes 24 de agosto de 2007

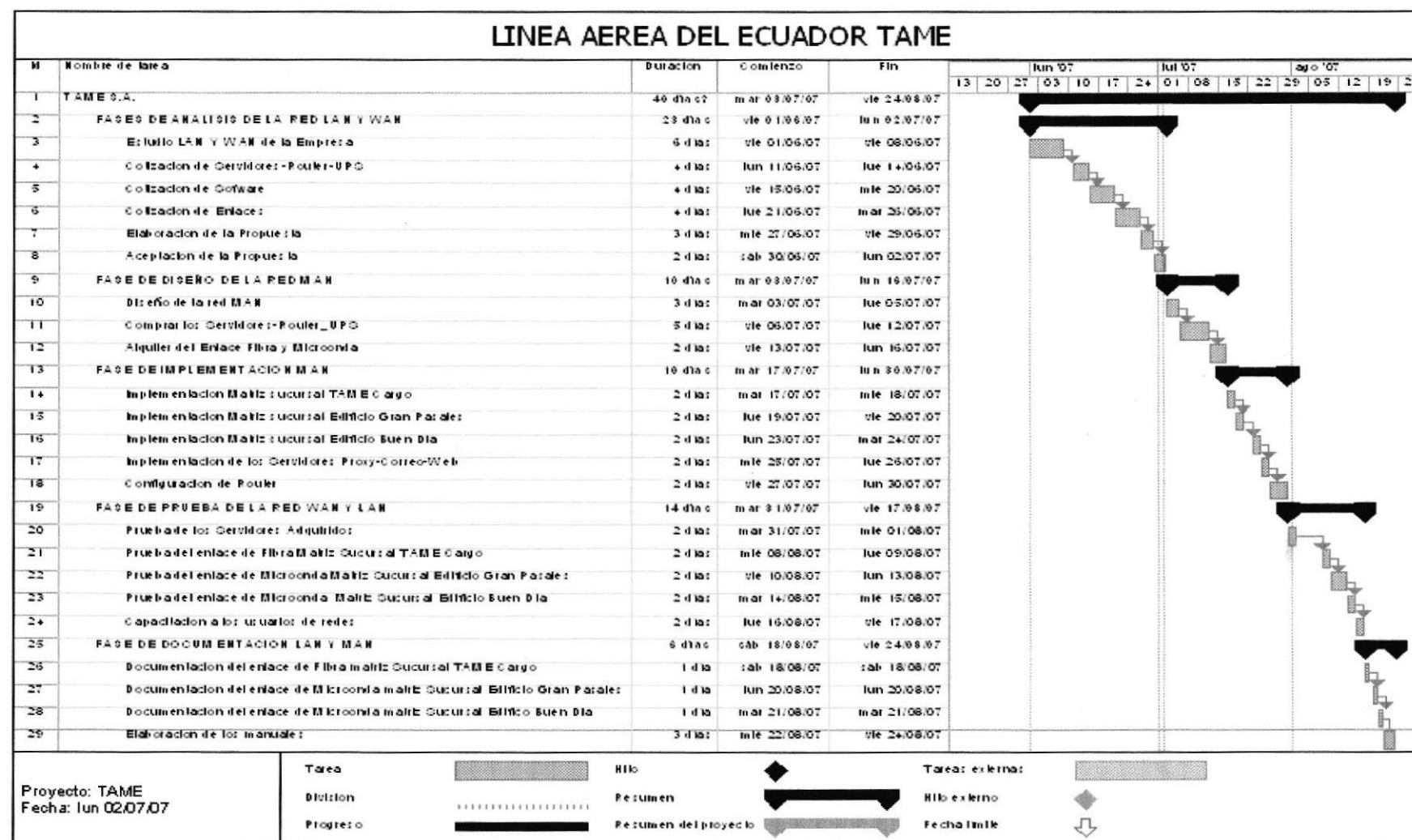
**3.3.2.7.- GARANTIA**

Teniendo como punto final la firma de conformidad entre el Cliente y la Empresa contratada para la aplicación del proyecto aquí aplicado, dando a conocer las garantías correspondientes del caso, como el soporte técnico en las correcciones futuras a implementar, con un costo a parte, de acuerdo al costo Hora de la mano de Obra.

- Para los equipos que van a funcionar como servidores, se dará un soporte técnico y una garantía de 3 meses
- Para los dispositivos de comunicación se ofrecerá una garantía de 12 meses sin costo alguno



## 3.3.2.8.- CRONOGRAMA DE TRABAJO



# CAPÍTULO 4 IMPLEMENTACIÓN



## 4.- IMPLEMENTACIÓN MAN

### 4.1.- COMUNICACIÓN QUITO GYE



FIGURA 4 - 1: Comunicación Quito Gye

## 4.2.- ENLACE MAN GUAYAQUIL Y SUS SUCURSALES

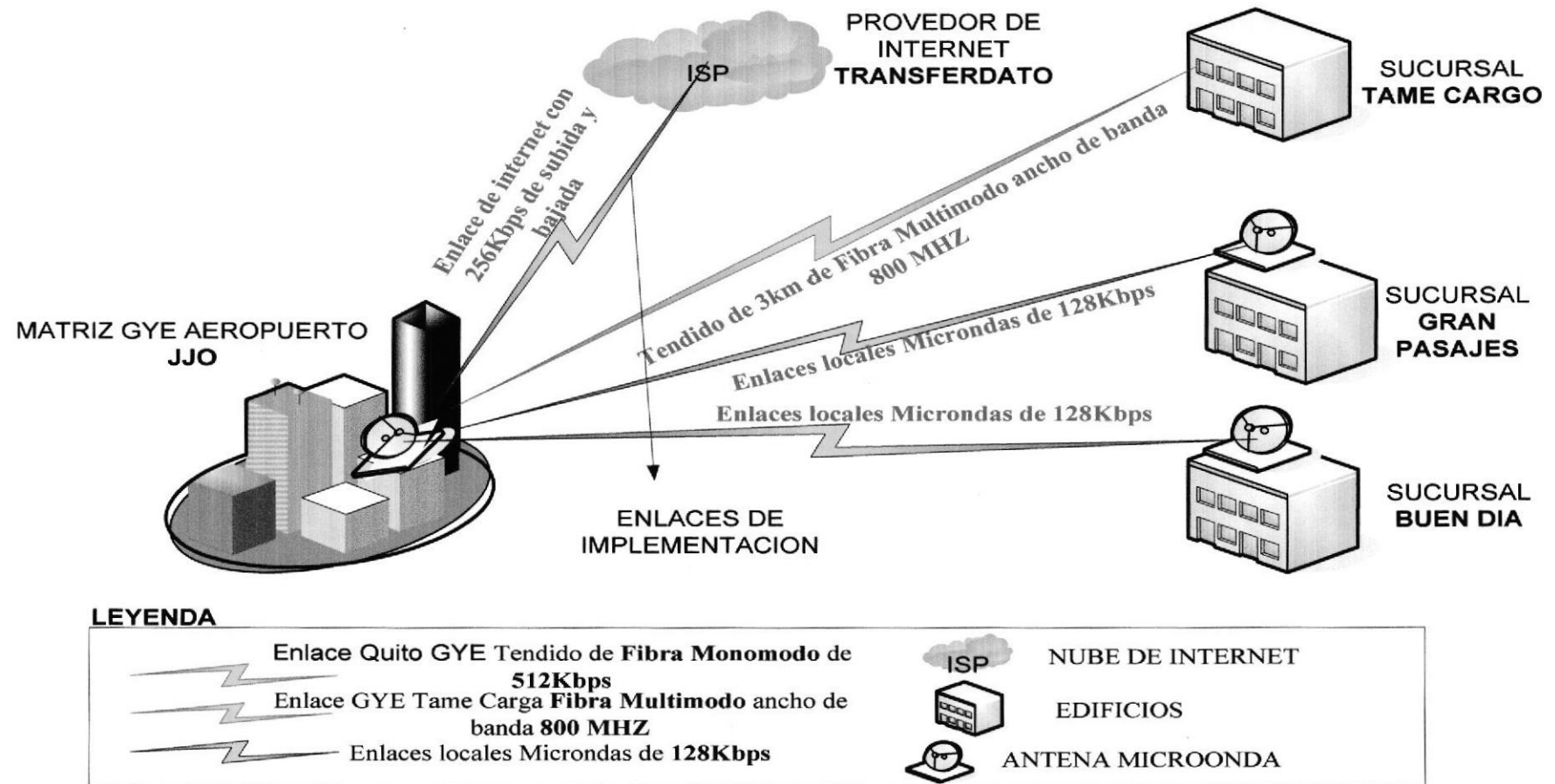


FIGURA 4 – 2: Enlace Man GYE y Sucursales

## 4.3.- COMUNICACIÓN DE PROTOCOLOS QUITO GYE

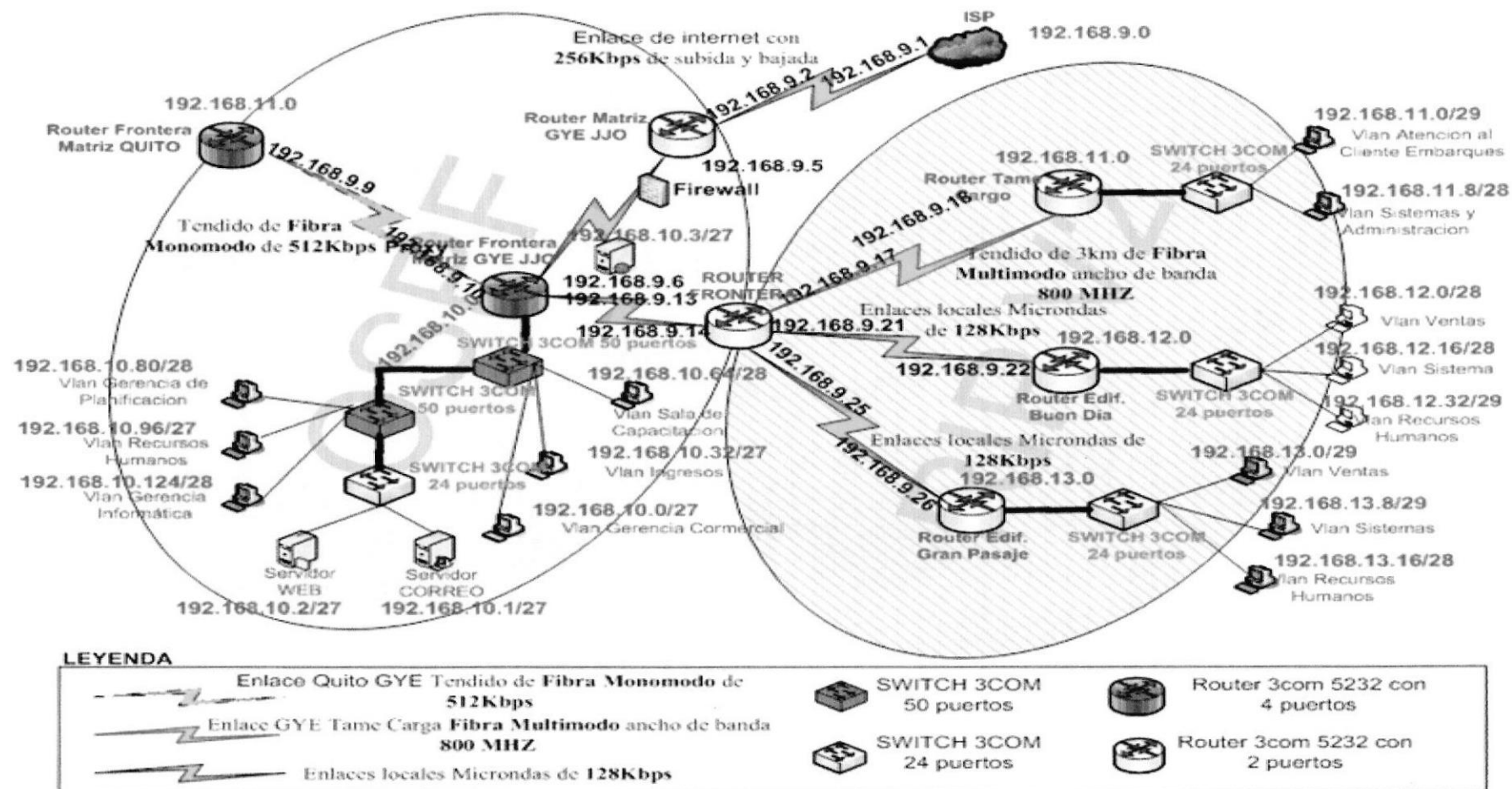


FIGURA 4 - 3: Comunicación De Protocolos Quito Gye

# CAPÍTULO 5 NORMATIVAS



## 5.- NORMAS Y RECOMENDACIONES

### LEYENDA



	RECOMENDACIONES
	OBLIGATORIEDAD

Tabla 5 - 1 Leyenda

### 5.1.- NORMAS

#### ▲NORMATIVA 1

Consideraciones de interferencia electromagnética

Para considerar problemas cuando por emisión electromagnética provenientes de cables de potencia y otros equipos se cubrirán.

Requisitos tales como:

- 1.- todo sistema deberán estar puesto y unidos a tierra
- 2.-deberán mantenerse una separación mínima de 50 mm (2 pulgadas) entre el cableado de telecomunicación de par trenzado sin blindaje (UTP) y los circuitos derivados menores a 3 KBA

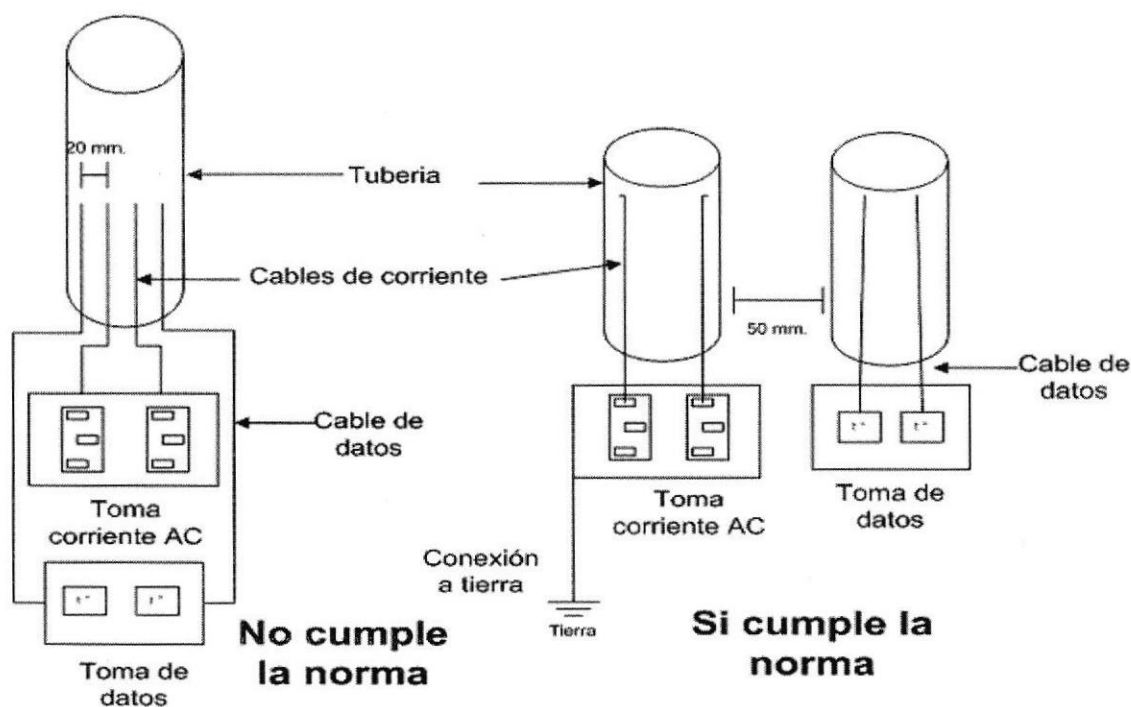


FIGURA 5 - 1: Normativa 1

## ▲ NORMATIVA 2

Aplicado a topología

El cableado horizontal deberá estar configurado como topología estrella, con cada salida de telecomunicación conectado a un cableado horizontal o distribuidor de piso.

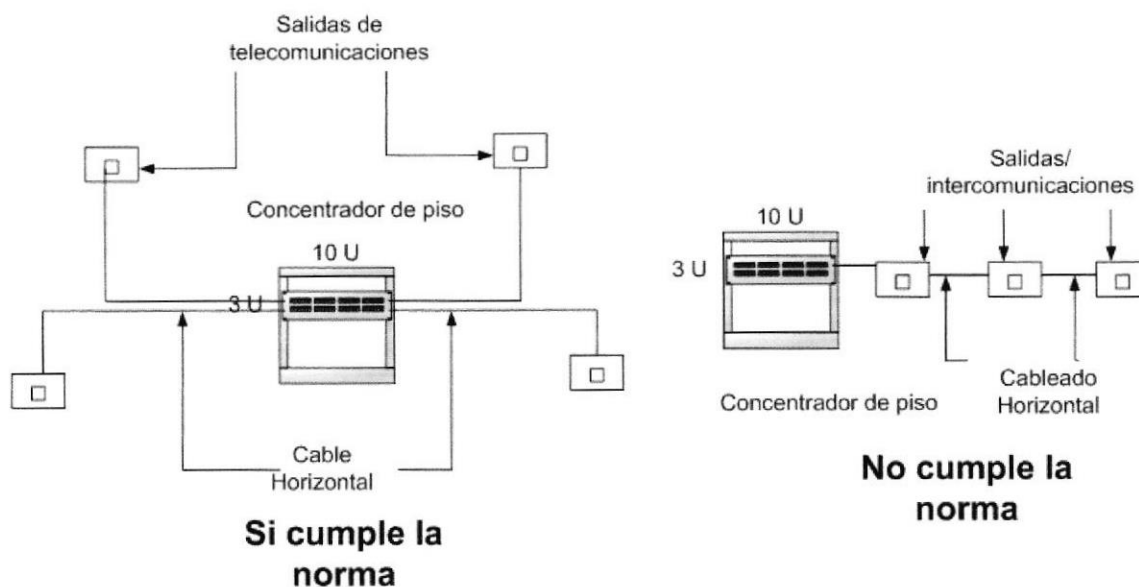


FIGURA 5 - 2: Normativa 2

## ▲ NORMATIVA 3

Se emplearan conexiones cruzadas para conexiones entre cableado horizontal y backbone y para conexiones de cableado horizontal y equipos de salida de punto múltiple

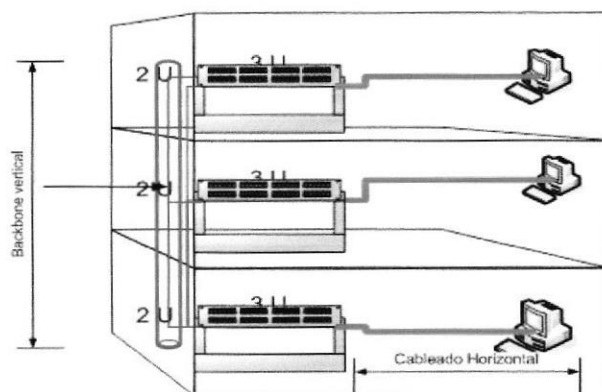
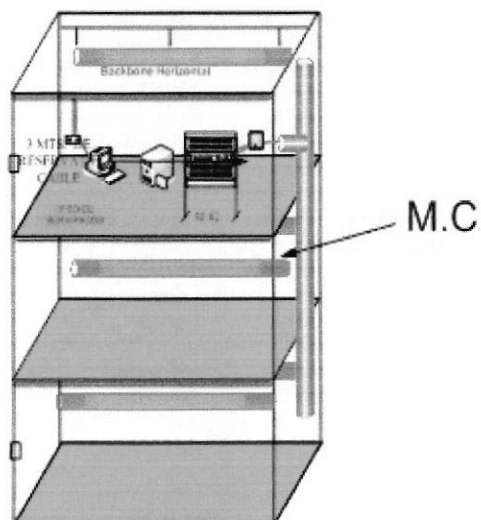


FIGURA 5 - 3: Normativa 3



**NORMATIVA 4**

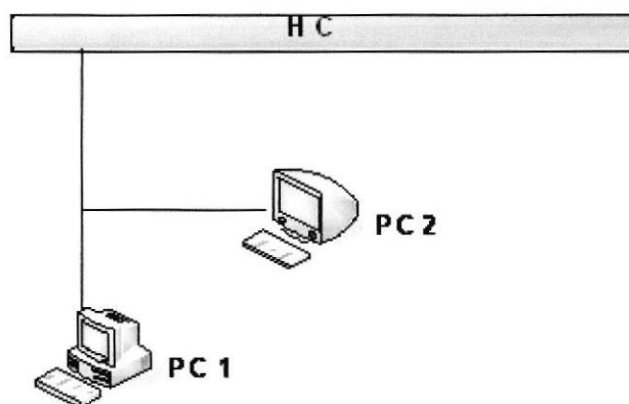
Cada área de trabajo estará extendida por un M.C. Localizado en el mismo piso o en un piso adyacente



**FIGURA 5 - 4:** Normativa 4

**NORMATIVA 5**

No se permití el uso de derivaciones puenteadas ampliada en el H.C.



**FIGURA 5 - 5:** Normativa 5

## ▲ NORMATIVA 6

La longitud del cable entre la salida de telecomunicación y el H.C. no excederá los 90mt. Independiente del tipo del medio

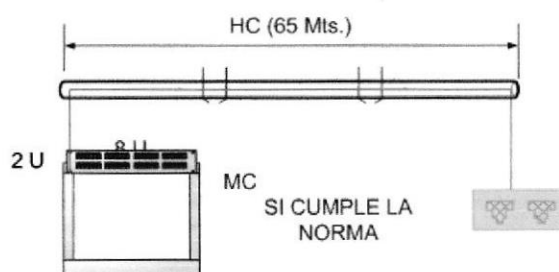


FIGURA 5 - 6: Normativa 6

## ▲ NORMATIVA 7

La longitud individual o combinada de patchcord de par trenzado balanceado 24 AWG (calibre americano de alambre) o fibra óptica utilizado en el H.C. No excederá los 5mt.

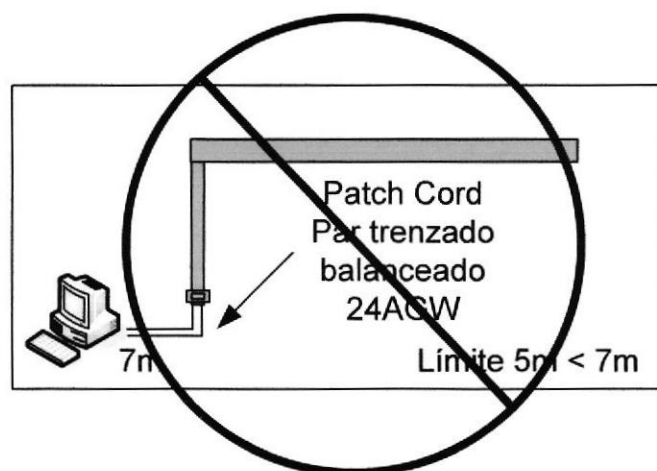


FIGURA 5 - 7: Normativa 7

## ▲ NORMATIVA 8

La longitud del canal del H.C incluyendo los patchcord de equipo en ambos extremo no excederá lo 100 mt independiente del medio

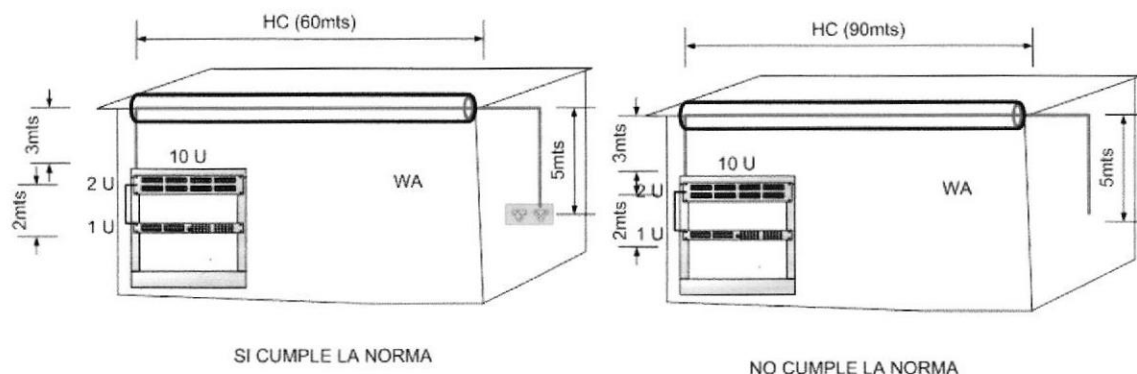


FIGURA 5 - 8: Normativa 8

## ▲ NORMATIVA 9

No se permitirá conexiones cruzados o equipo activo en el punto de consolidación

### Nota:

Punto de consolidación: es un hardware de conexión que proporciona interconexión entre cableado de oficina abierto y cableado horizontal

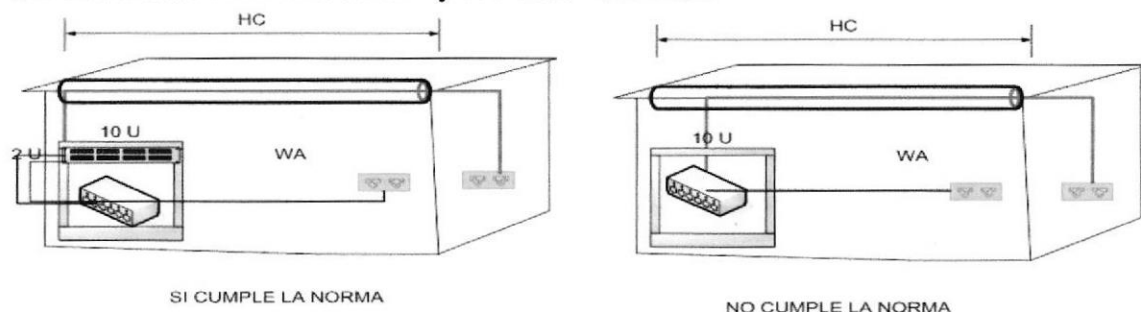
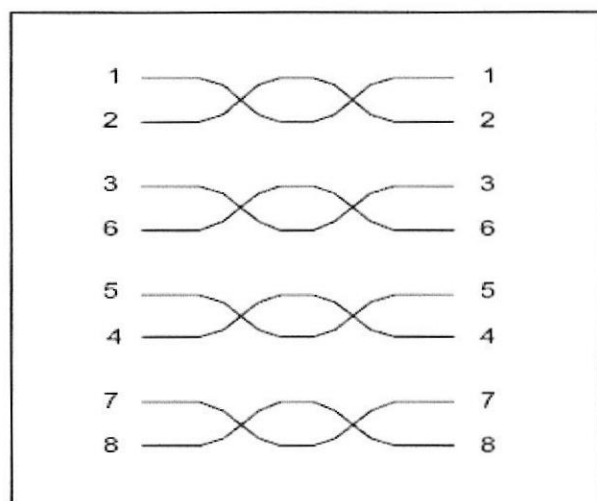


FIGURA 5 - 9: Normativa 9

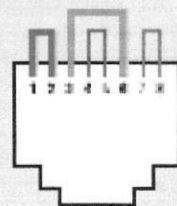


### ▲ **NORMATIVA 10**

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



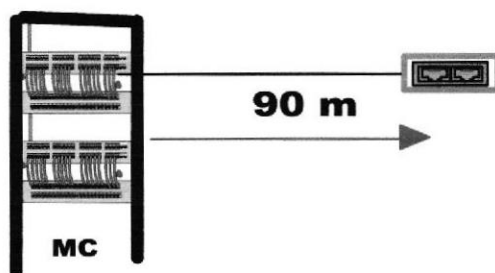
En el cableado VDI se conecta cada par pero sólo 2 pares son usados para propósitos de Ethernet: pares 1-2 y 3-6.



**FIGURA 5 - 10:** Normativa 10

### ▲ **NORMATIVA 11**

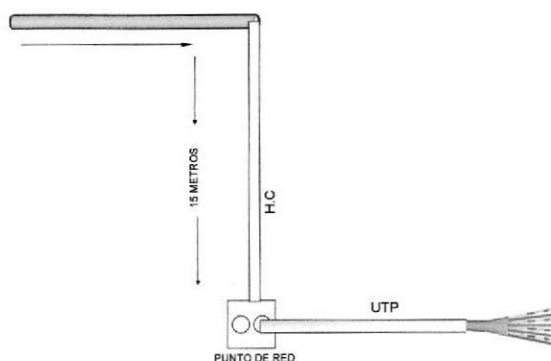
La distancia máxima entre el HC y la salida de telecomunicación será de 90mt.



**FIGURA 5 - 11:** Normativa 11

**▲ NORMATIVA 12**

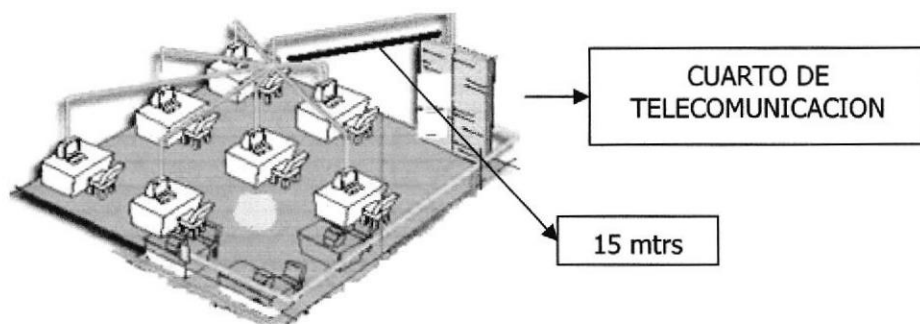
La distancia mínima entre el HC y el punto de consolidación será de 15m



**FIGURA 5 - 12:** Normativa 12

**▲ NORMATIVA 13**

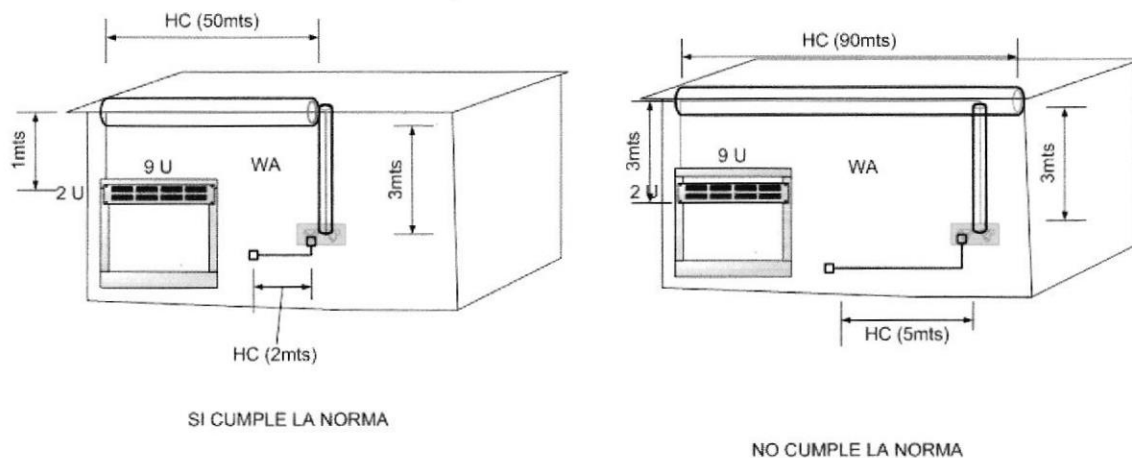
La distancia mínima Entre el punto consolidación y la salida de telecomunicación será de 15mt.



**FIGURA 5 - 13:** Normativa 13

### ▲ NORMATIVA 14

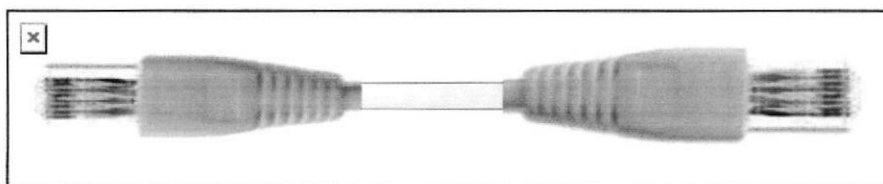
La distancia del canal del cableado horizontal incluyendo pachcord y salida de telecomunicación excederá a 100mts.



**FIGURA 5 - 14:** Normativa 14

### ▲ NORMATIVA 15

Todos los pares del cable estarán totalmente terminados en ambos extremos



**FIGURA 5 - 15:** Normativa 15

## ▲ NORMATIVA 16

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

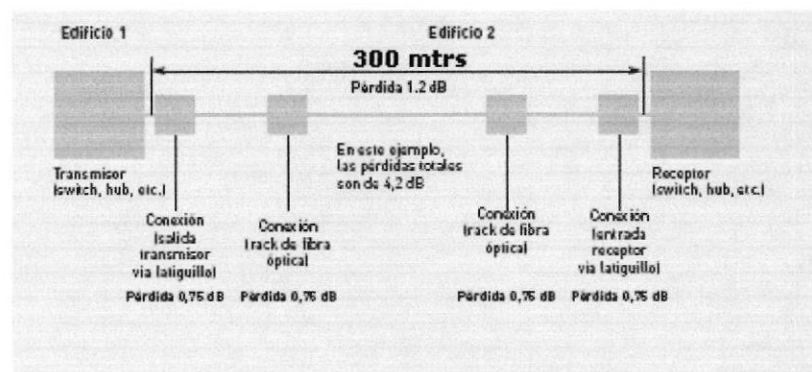


FIGURA 5 - 16: Normativa 16

## ▲ NORMATIVA 17

La longitud del cableado de fibra óptica y monomodo entre HC y la salida de telecomunicación no excede los 90mts.

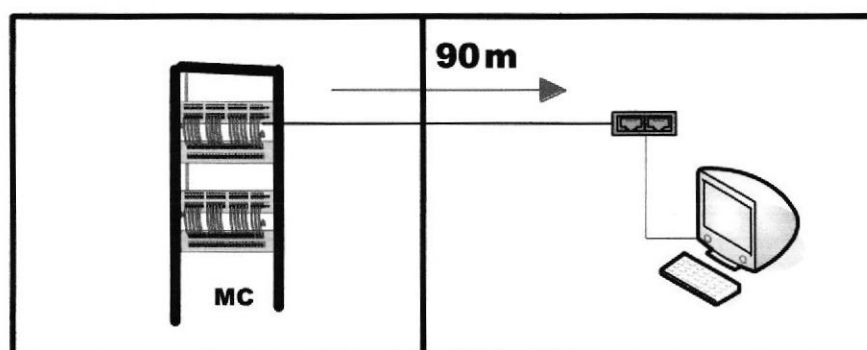
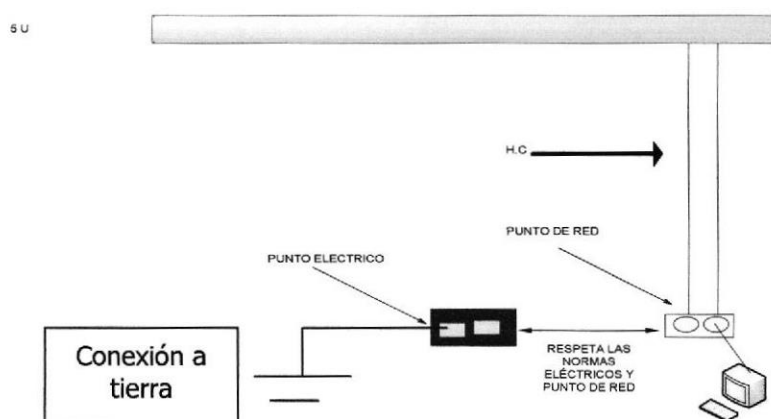


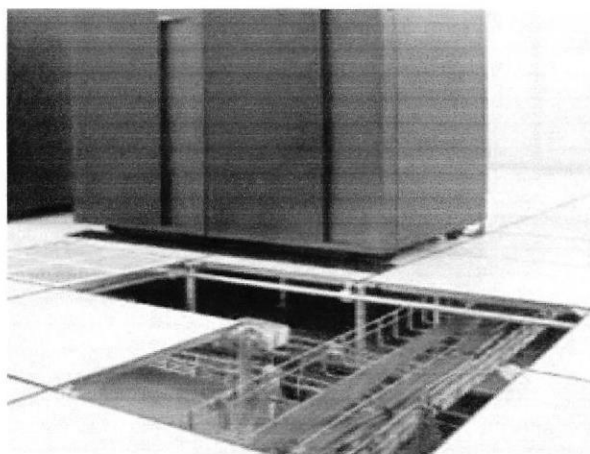
FIGURA 5 - 17: Normativa 17

**▲ NORMATIVA 18**

Las canalizaciones horizontales se diseñaran e instalara para cumplir los reglamentos eléctricos y de construcciones locales y nacionales y normas aplicables

**FIGURA 5 - 18: Normativa 18****▲ NORMATIVA 19**

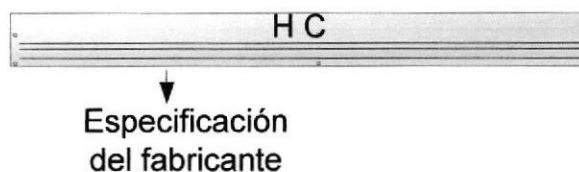
Las canalizaciones horizontales serán apropiados para el ambiente en el cual se instalara y no se obstaculizara por ductos de aires, ventilación y airé acondicionado distribución eléctrico o estructura del edificio

**FIGURA 5 - 19: Normativa 19**

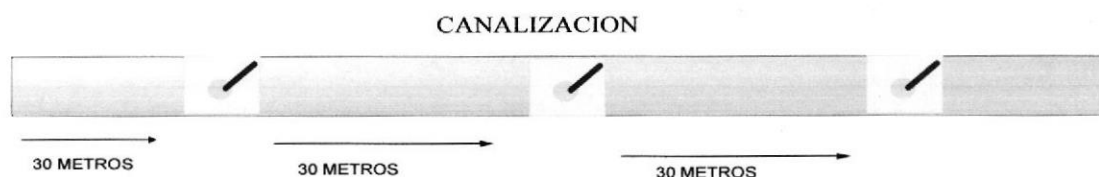


**▲ NORMATIVA 20**

Las canalización horizontal deberán mantener un radio min. De cobertura de cables horizontal según la especificación del fabricante

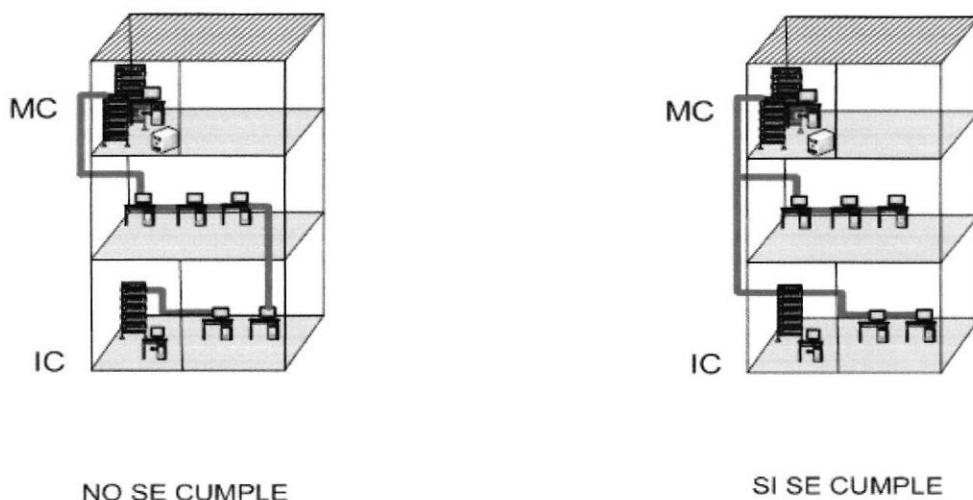
**FIGURA 5 - 20:** Normativa 20**▲ NORMATIVA 21**

Todas las canalizaciones instaladas serán accesibles con el fin de efectuar adiciones o retiro de cables. Las canalizaciones cerradas tendrán puntos de acceso espaciados como máximo cada 30m

**FIGURA 5 - 21:** Normativa 21

**▲ NORMATIVA 22**

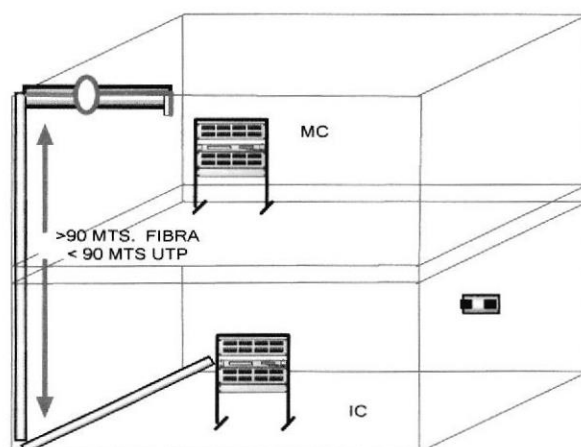
El backbone vertical deberá usar topología estrella jerárquica desde el MC hasta IC



**FIGURA 5 - 22:** Normativa 22

**▲ NORMATIVA 23**

Para cada tendido del backbone del edificio que sea mayor de 90mts. De longitud deberá proveer de cable de fibra óptica



**FIGURA 5 - 23:** Normativa 23

## **▲ NORMATIVA 24**

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

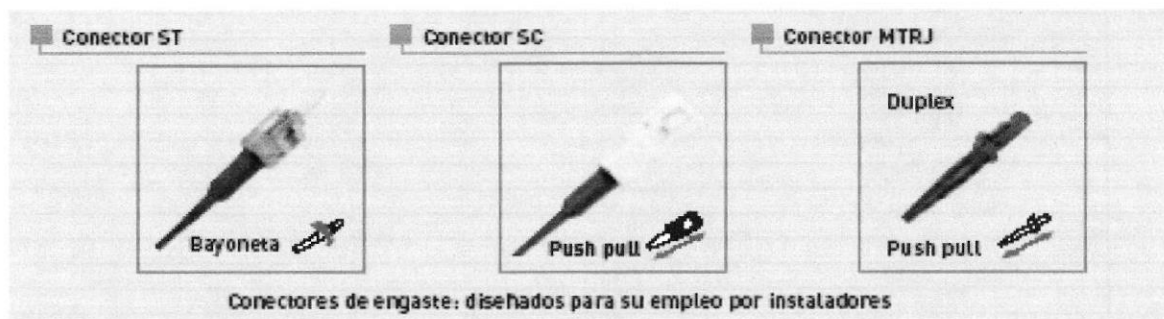
3000mts. Para Fibra Óptica monomodo

2000mts. Para Fibra Óptica multimodo

2000mts. Para par trenzado con aplicación PBX

### **Nota 1**

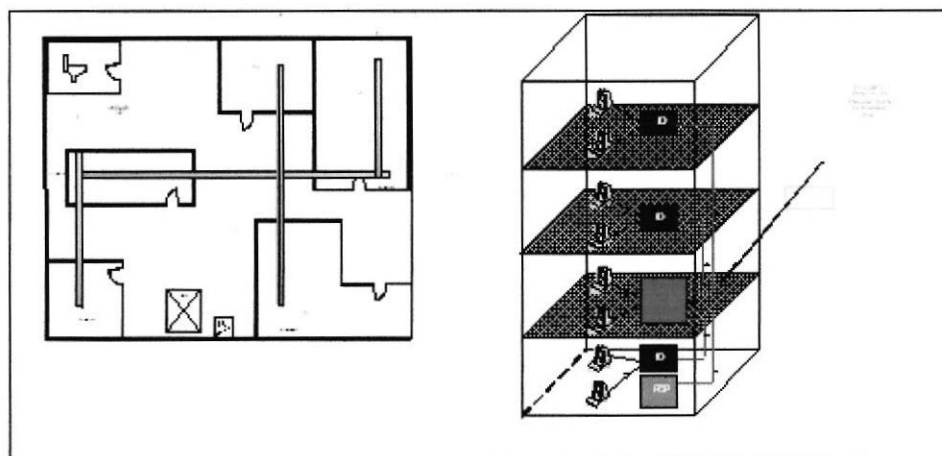
Si el backbone de par trenzado balanceado sobrepasa los 10mts. Su uso se restringe solo para soportar aplicaciones de voz



**FIGURA 5 - 24: Normativa 24**

**▲ NORMATIVA 25**

Las canalización del edificio proveerán acceso a todos los cuartos de comunicación, cuartos de equipos ya acometidos localizada en el mismo edificio



**FIGURA 5 - 25:** Normativa 25

**▲ NORMATIVA 26**

La canalización no se ubicara en ductos de ascensores



**FIGURA 5 - 26:** Normativa 26

**▲ NORMATIVA 27**

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

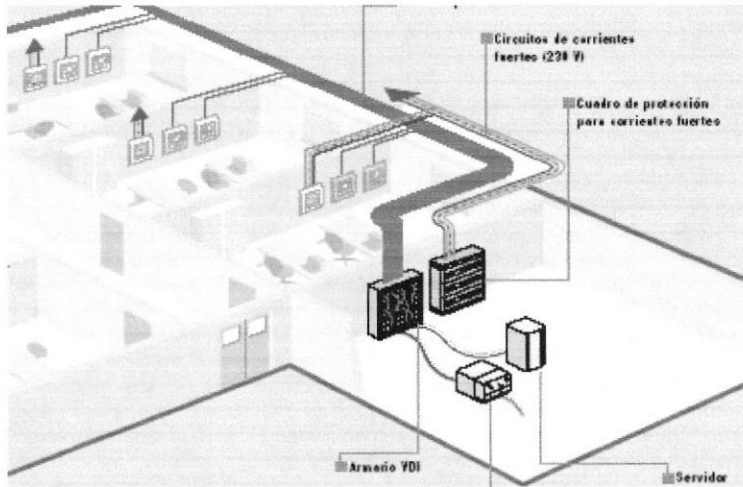


FIGURA 5 - 27: Normativa 27

**▲ NORMATIVA 28**

El cuarto de telecomunicaciones se diseñará y equipará el cuarto para contener equipos de telecomunicación terminaciones de cables y asociados.



FIGURA 5 - 28: Normativa 28

## ▲ NORMATIVA 29

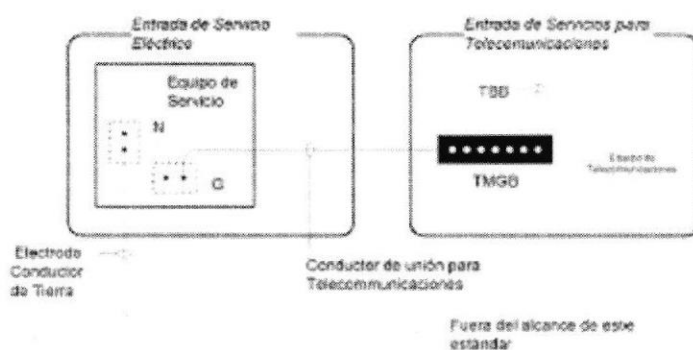
El acceso a los cuartos de telecomunicación se restringirá al personal de servicio autorizado y no será compartido por servicios del edificio que puedan interferir con los sistemas de telecomunicación



**FIGURA 5 - 29:** Normativa 29

## ▲ NORMATIVA 30

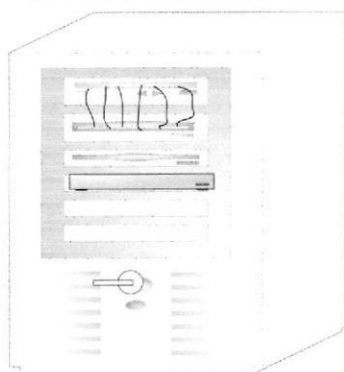
Las instalación separación de hilos a tierra, cumplirán las normas y reglas



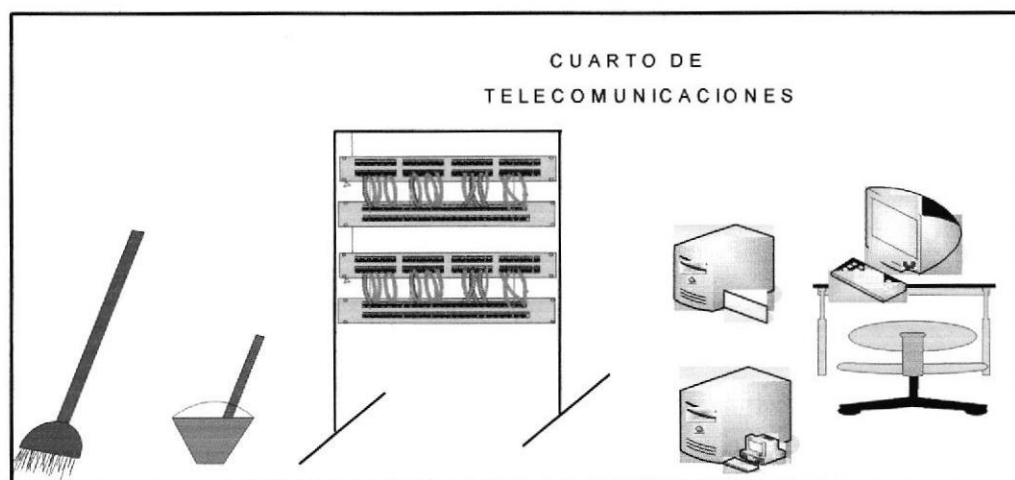
**FIGURA 5 - 30:** Normativa 30

**▲NORMATIVA 31**

Los gabinetes usados como espacio alternativos cumplirán los requisitos de telecomunicación que tendrán una puerta con cerradura y se montara en una ubicación fija

**GABINETE  
DEL RACK****FIGURA 5 - 31: Normativa 31****▲NORMATIVA 32**

El cuarto de equipo no será compartido con servicio del edificio que pueda interferir la telecomunicación o se utiliza mantenimiento del edificio

**FIGURA 5 - 32: Normativa 32**

### ▲ NORMATIVA 33

El cableado se instalara para facilitar el rotulado y la documentación para permitir el código de colores en forma consistente de los requisitos.

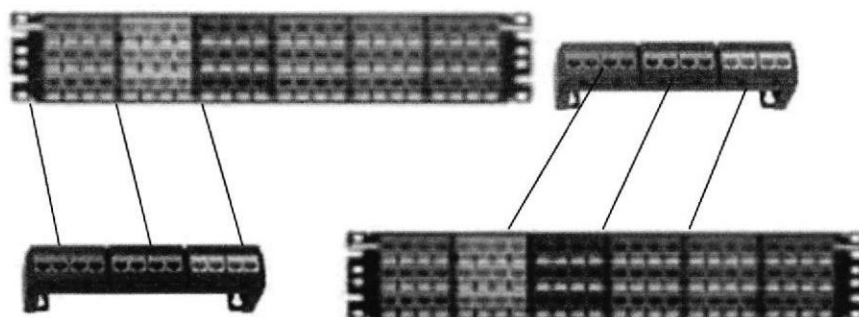


FIGURA 5 - 33: Normativa 33

### ▲ NORMATIVA 34

La instalación del gabinete en el rack deberá proporcionar la separación instalada en las normas y reglas necesaria

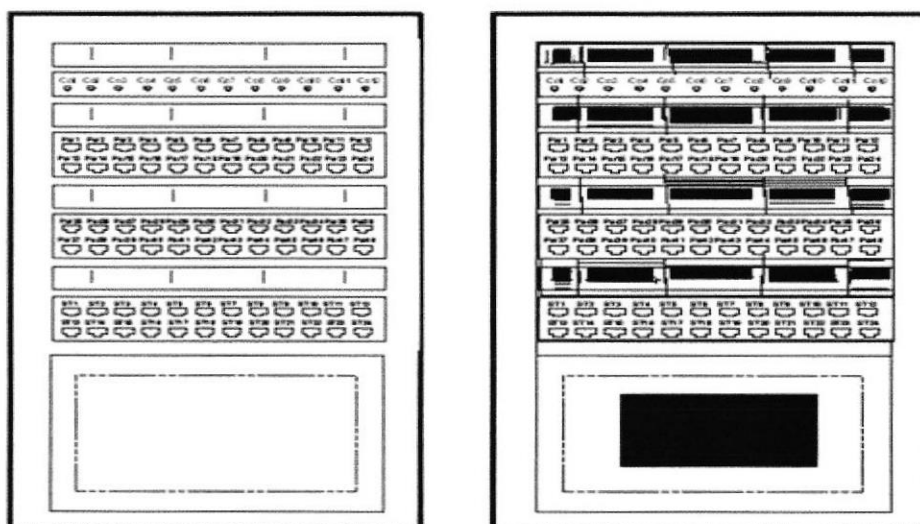


FIGURA 5 - 34: Normativa 34



### ▲ NORMATIVA 35

Los cables de telecomunicación se soportaran con dispositivos diseñados para este equipo y en forma independiente a cualquier otra estructura.

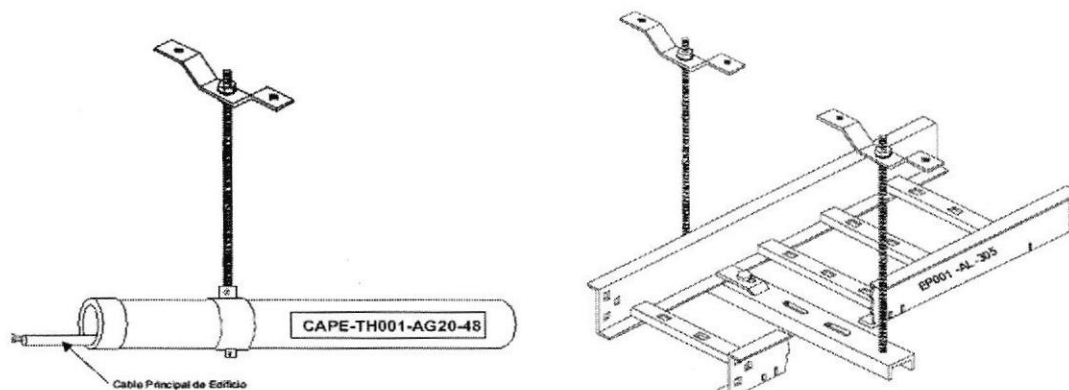


FIGURA 5 - 35: Normativa 35

### ▲ NORMATIVA 36

Los cables enrutados verticalmente, como en el caso del cable backbone u horizontal enrutados entre piso, se soportaran con abrazadera u otro mecanismo requiera un min. De 2 soportes por piso.

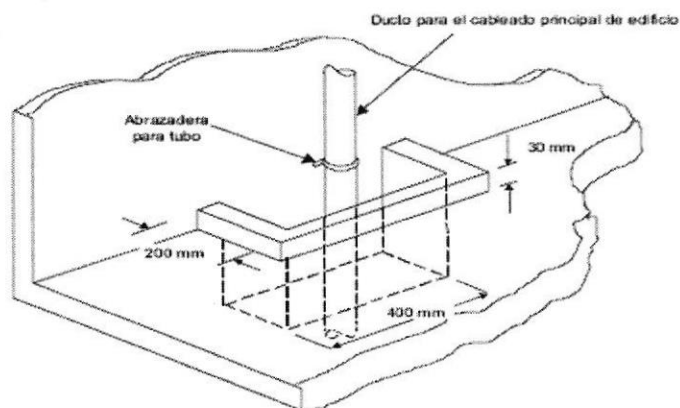


FIGURA 5 - 36: Normativa 36

### ▲ NORMATIVA 37

Los números de cables horizontales (par trenzado balanceado cable fibra óptica) colocado en un soporte de canalización, se extenderá a una cantidad que no altere el geométrico del cable

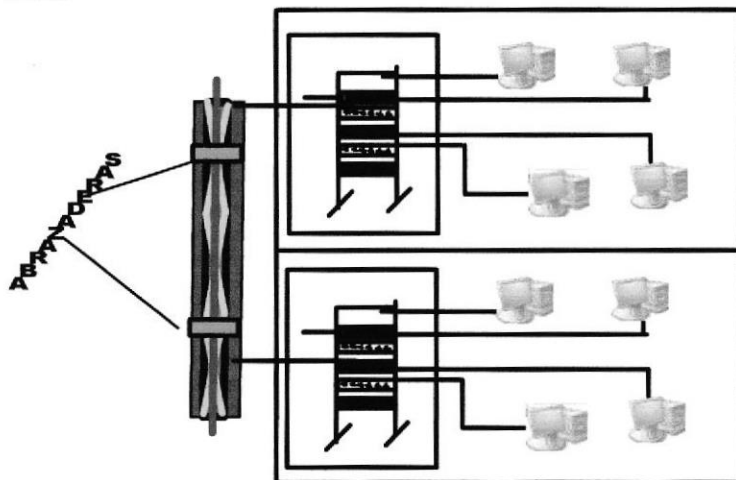


FIGURA 5 - 37: Normativa 37

### ▲ NORMATIVA 38

La canalización de tipo bandeja o canal no excede una capacidad máx. 50% de llenado y una altura máx. Interior de 6''

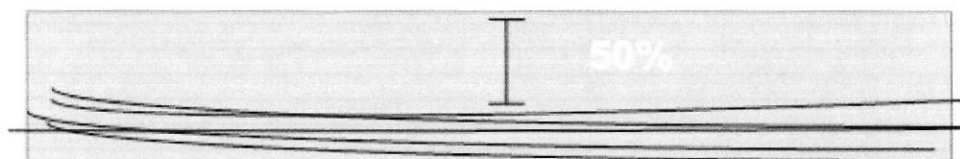
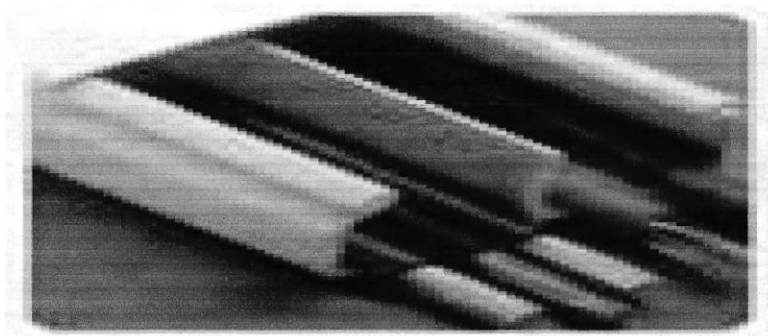


FIGURA 5 - 38: Normativa 38

▲ **NORMATIVA 39**

Para canalizar para espacio de techo falso, los sistemas de soporte de cable se diseñara e instalara un min. 3" por encima de la rejilla del techo soportado



**FIGURA 5 - 39:** Normativa 39

## ▲ NORMATIVA 40

Las tensiones máximas del jalado del cable o radio mínimo de curvatura no sobrepasaran las especificaciones del fabricante

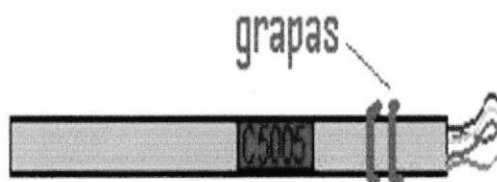


FIGURA 5 - 40: Normativa 40



**NORMATIVA 41**

No soportan engrampado de ningún tipo de cable reconocido

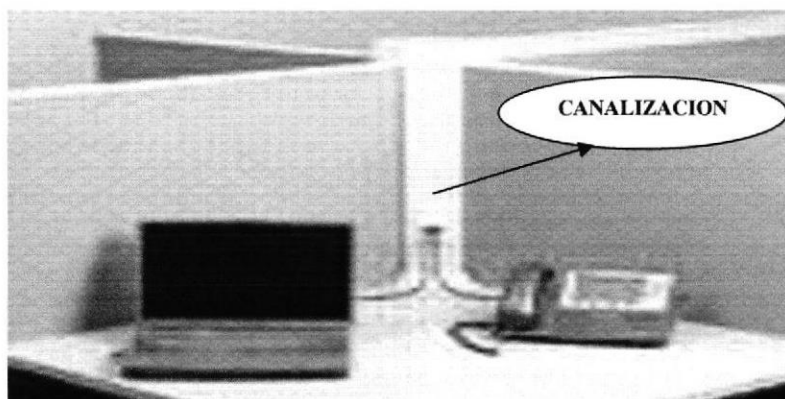


**FIGURA 5 - 41:** Normativa 41



**NORMATIVA 42**

Los cables se instalarán en canalizaciones y espacios que rinde protección adecuada contra la intemperie y demás riesgo del medio



**FIGURA 5 - 42:** Normativa 42

## ▲ NORMATIVA 43

El radio min. De cobertura, en coordinación de no tensión (cuando el cable es solo colocado no alojado) será de:

- 1'' para SCPP o SFTP de diámetro < igual 6 milímetro
- 2'' para SCPP o SFTP de diámetro > 6 milímetro (0.25'')

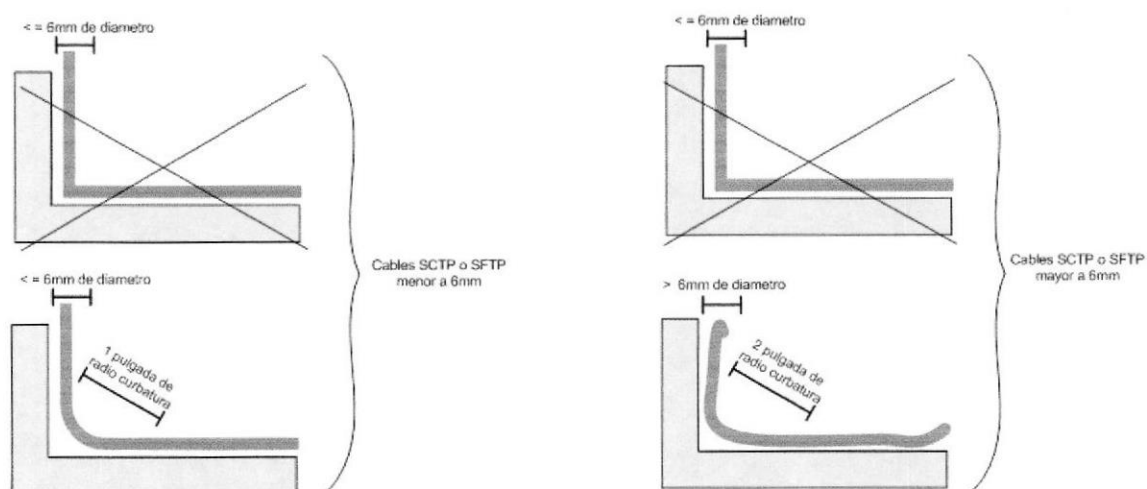


FIGURA 5 - 43: Normativa 43



## ▲ NORMATIVA 44

El radio min. De cobertura para cable horizontal de 2 y 4 fibras será de 1" bajo condición de no tensión y de 2" bajo condiciones de tensión; la tensión máx. De jalado permitida será de 222N ("Newton" (libras fuerzas))

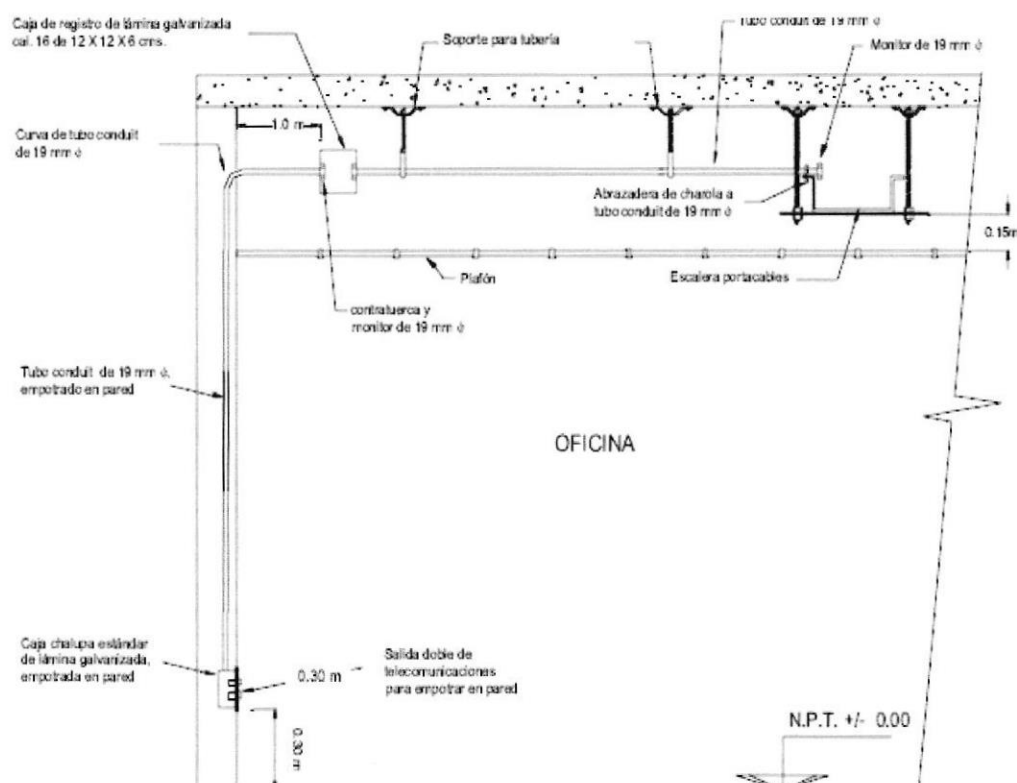


FIGURA 5 - 44: Normativa 44

## ▲ NORMATIVA 45

El radio de cobertura para cable backbone de fibra óptica de interiores no será < a 10 veces el diámetro externo del cable y no < a 15 veces bajo tensión.



FIGURA 5 - 45: Normativa 45

### ▲ NORMATIVA 46

El radio de cobertura para cable backbone de fibra externo no será  $< 10$  a veces el diámetro externo del cable bajo condiciones a no tensión, y no  $< a 20$  veces el diámetro de cable extremo bajo condición de tensión, en donde la tensión del cable extendida será  $< 2670$  N (600 libras de fuerza).

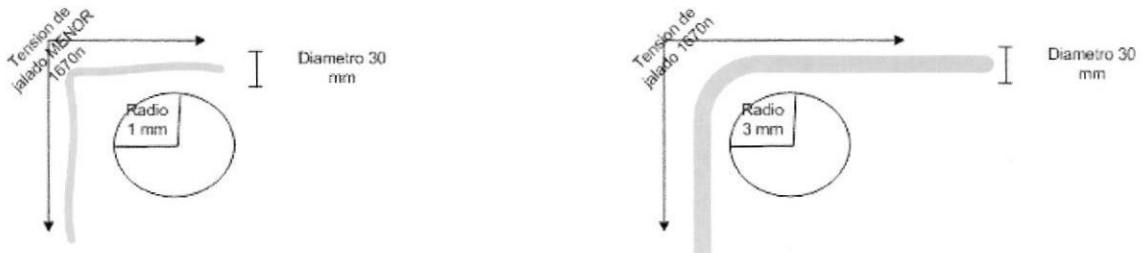


FIGURA 5 - 46: Normativa 46

### ▲ NORMATIVA 47

El cable que corra entre el cuarto de telecomunicación y salida de telecomunicación, no estará expuesto en el área de trabajo u otro espacio acceso al público

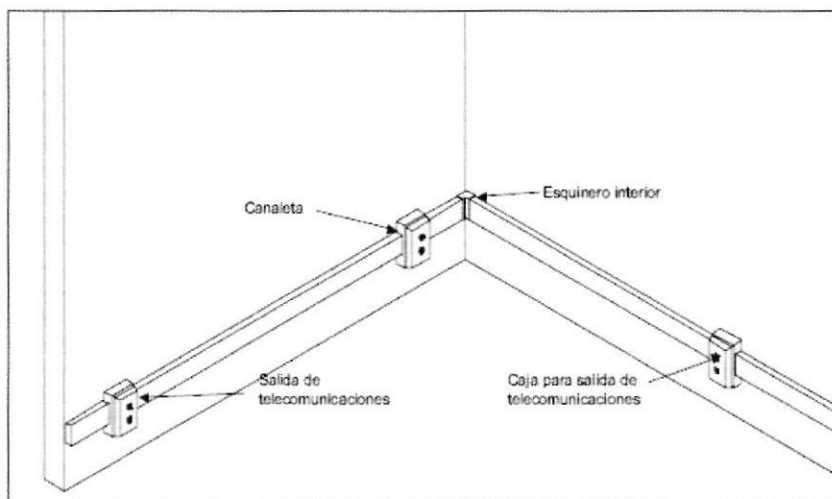
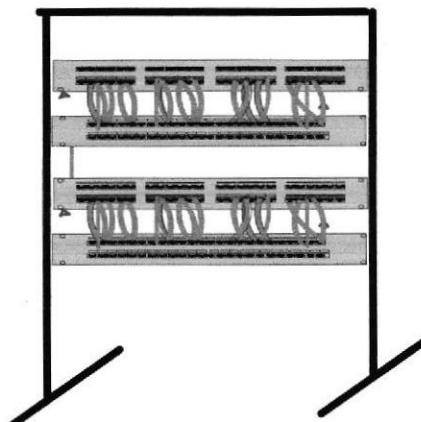


FIGURA 5 - 47: Normativa 47



### ▲ **NORMATIVA 48**

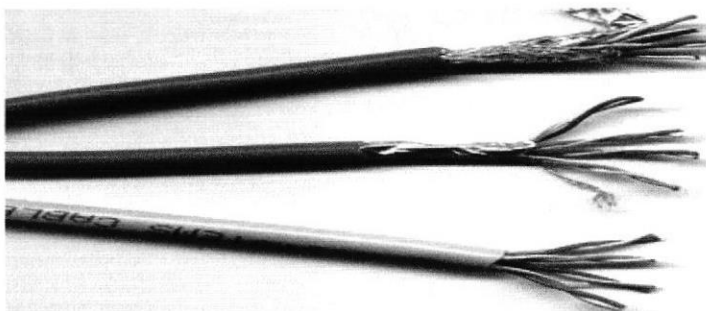
El hardware de conexión se instalara de una manera que evite un control de cables ordenados y bien organizados



**FIGURA 5 - 48:** Normativa 48

### ▲ **NORMATIVA 49**

Con el fin de reducir el Desentrezado de par trenzado instalador debe de pelar cantidad de forros que se requiera para determinar el hardware de comunicación



**FIGURA 5 - 49:** Normativa 49

## ▲ NORMATIVA 50

La cantidad máx. Del desenredado de cada par trenzado, resultante de comunicación del hardware de conexión, será de 13 milímetro, para cable de categoría 5e o > y de 75 milímetro para cables de cat 3

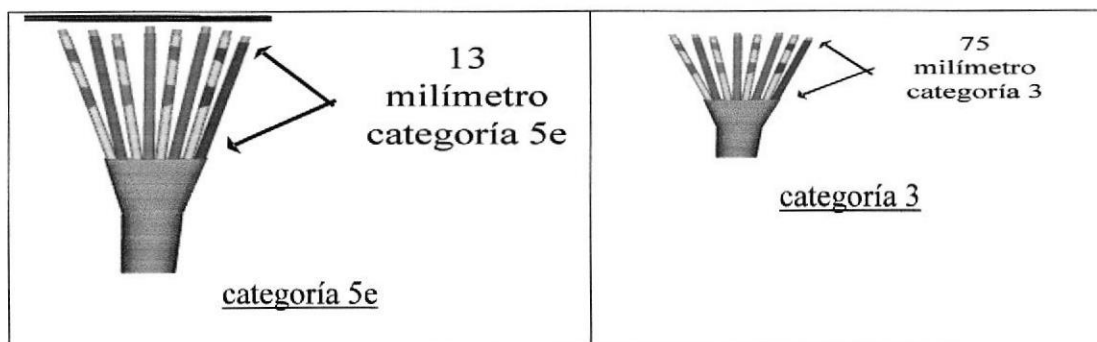


FIGURA 5 - 50: Normativa 50

## ▲ NORMATIVA 51

No se deberá terminar cables de diferente categoría de desempeño en el mismo hardware de telecomunicación

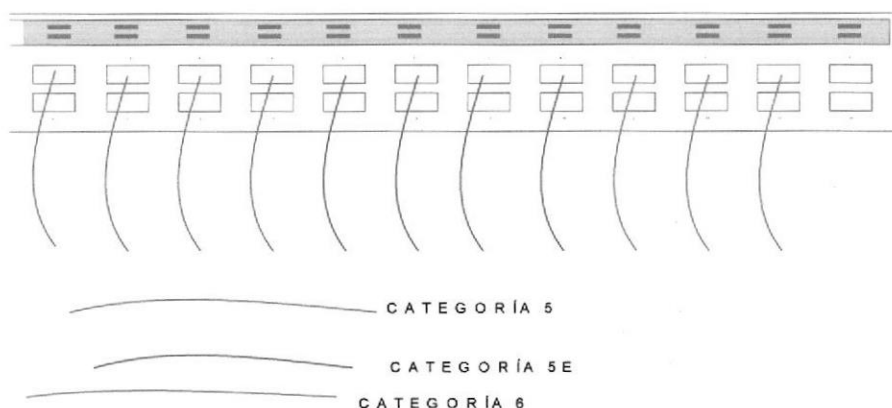


FIGURA 5 - 51: Normativa 51



## ▲ NORMATIVA 52

Los identificadores que se utiliza para acceder a grupos de registro del mismo equipo deben ser únicos

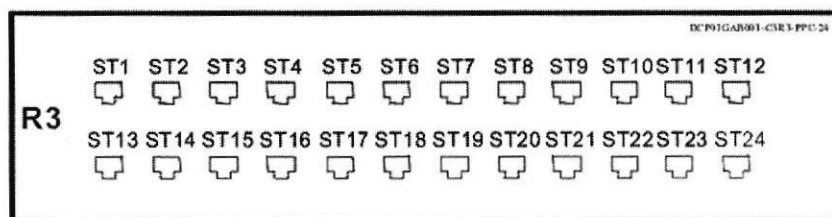


FIGURA 5 - 52: Normativa 52

## ▲ NORMATIVA 53

El rotulado se deberá realizar ya sea pegando o colocando firmemente una etiqueta independiente al elemento que se va a registrar o marcando el elemento directamente.

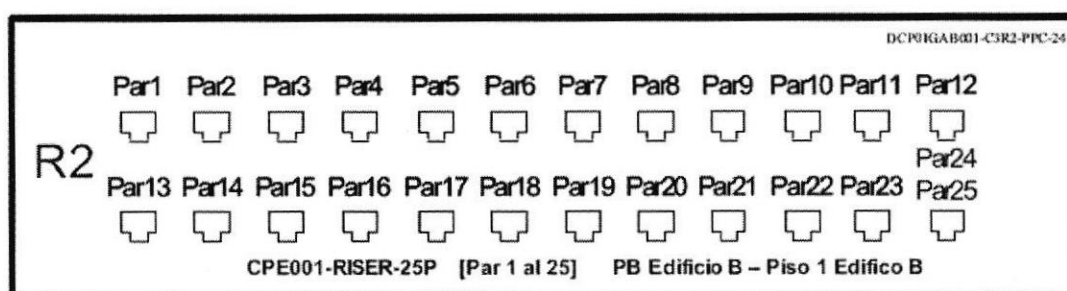
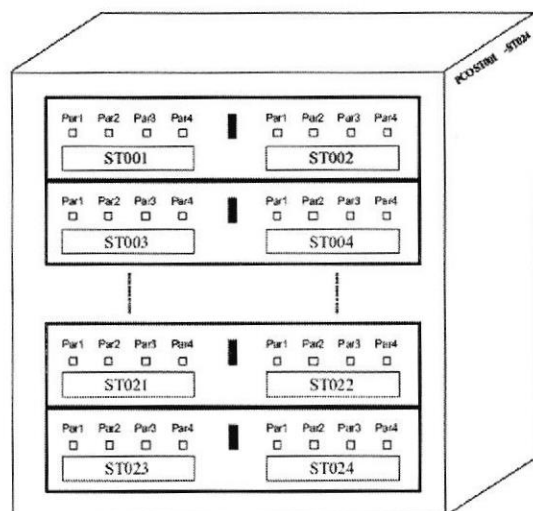


FIGURA 5 - 67: Normativa 53

## ▲ NORMATIVA 54

El rotulado deberá ser legible y permanecer firmemente unido al elemento durante el periodo de garantía (5 años de garantía según el fabricante)



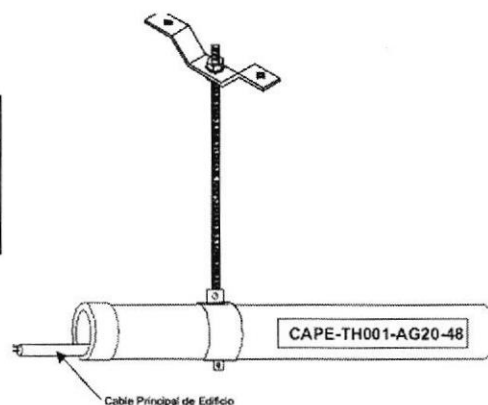
**FIGURA 5 - 54:** Normativa 54

## ▲ NORMATIVA 55

A cada cable se asignara un identificador único que sirva referencia a su respectivo ejemplo

Descripción	Identificador
Cable numero 9 de fibra óptica monómodo	FOM009
Cable numero 5 UTP cat 5E	C5005

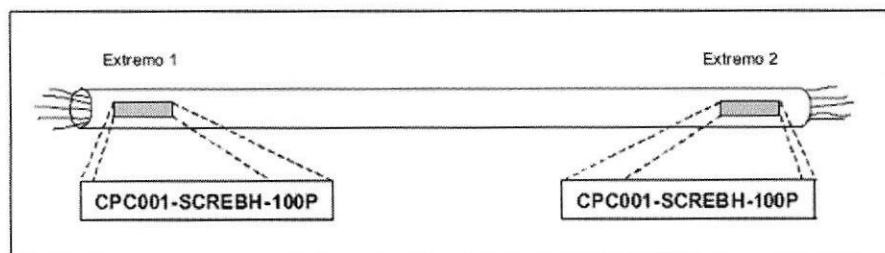
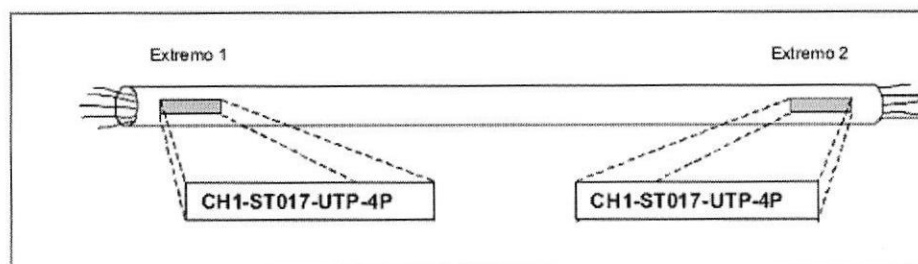
**Tabla 5 - 2** Asignar identificacion



**FIGURA 5 - 55:** Normativa 55

**NORMATIVA 56**

Los cables de subsistema horizontal y backbone deberán rotularse en cada extremo, la etiqueta puede ser colocada a 30cm del cable, esta marca deberá permanecer en el cable después de terminar la instalación

**FIGURA 5 - 56:** Normativa 56**FIGURA 5 - 57:** Normativa 57

## 5.2.- RECOMENDACIONES

### △ RECOMENDACIÓN 1

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

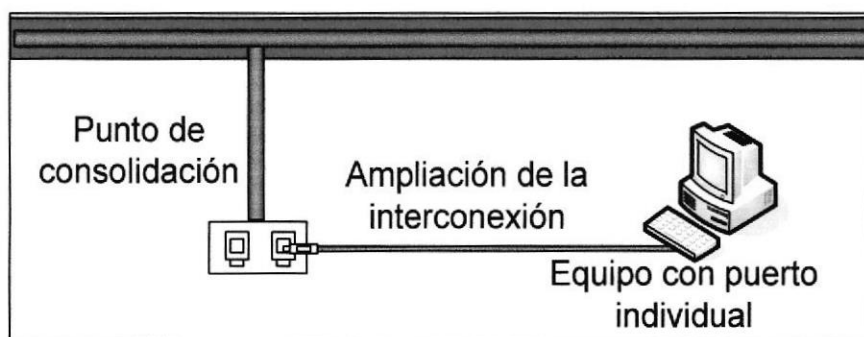


FIGURA 5 – 58: Recomendación 1

### △ RECOMENDACIÓN 2

Con el fin de proveer una infraestructura capas de crear un ambiente de oficina. Se recomendará un mínimo de un cuarto de telecomunicación por cada piso

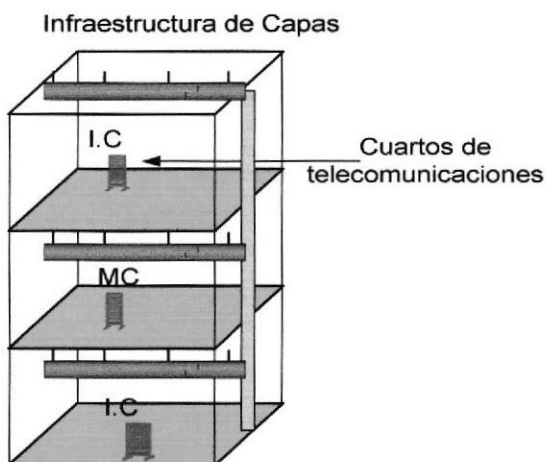


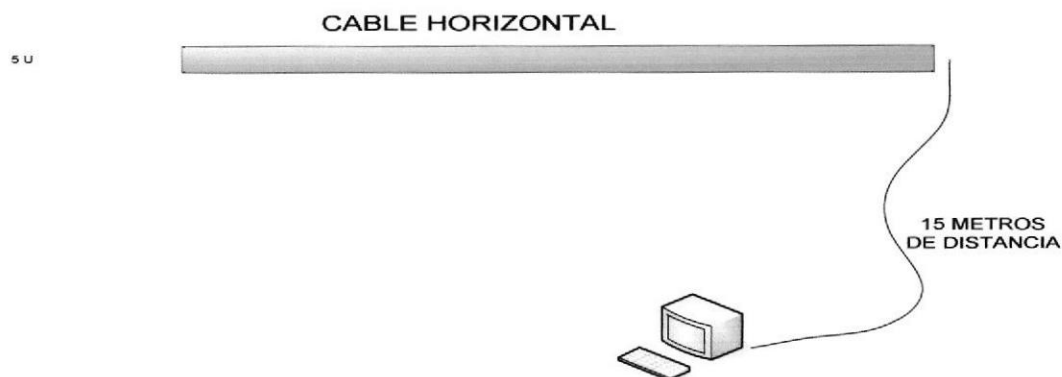
FIGURA 5 - 59: Recomendación 2

**RECOMENDACIÓN 3**

El área que puede atenderse efectivamente por un cuarto de telecomunicación abarca un radio máximo de 60mt.

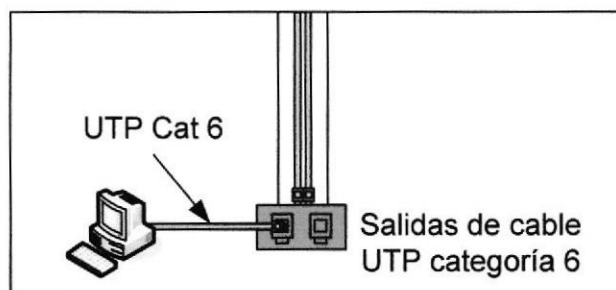
**FIGURA 5 - 60: Recomendación 3****RECOMENDACIÓN 4**

Se recomienda un min. De 15mt. Entre el H.C. y la salida de telecomunicación

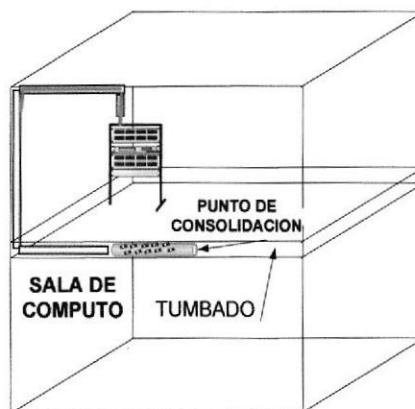
**FIGURA 5 - 61: Recomendación 4**

**RECOMENDACIÓN 5**

Se recomienda un mínimo de 2 salidas de cat. 6 por cada área de trabajo individual con el fin de soportar, numerosas aplicaciones diseñados para operar sobre el cableado de par trenzado

**FIGURA 5 - 62: Recomendación 5****RECOMENDACIÓN 6**

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

**FIGURA 5 - 63: Recomendación 6**



## RECOMENDACIÓN 7

El cableado backbone del edificio debe diseñar con la capacidad de reserva suficiente para tender salidas adicionales de telecomunicación desde el cuarto telecomunicación

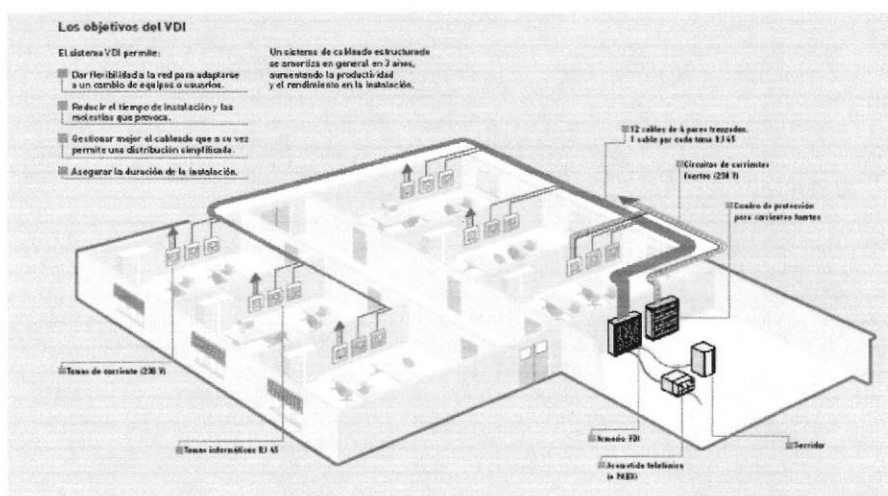


FIGURA 5 - 64: Recomendación 7

## RECOMENDACIÓN 8

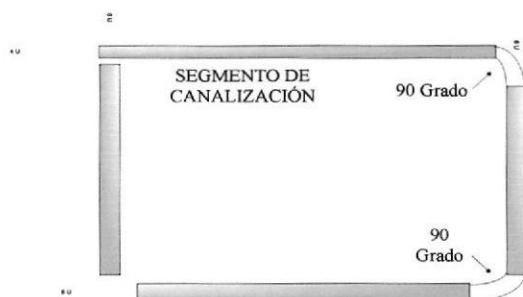
El radio de cobertura interior mín. De la canalización horizontal no debe ser inferior a 10 veces del mayor diámetro de los cables a instalarse



FIGURA 5 - 65: Recomendación 8

**RECOMENDACIÓN 9**

Ningún segmento de canalización contendrá más de 2 curvas de 90 o entre puntos de acceso



**FIGURA 5 - 66: Recomendación 9**

## RECOMENDACIÓN 10

Se recomienda que se proveer como min. 2 hilos de fibra óptica por cada aplicación conocida durante su periodo de planificación deben proveerse de una aplicación de 100%

Voz	2	2 hilos para voz de datos
Video	2	Mínimo fibra de 12 hilos
Lan	2	Desde un mismo cable utp de 8 hilos sacar 2 conectores
Crecimiento	6	Cable utp <90mts; >90 fibra óptica
TOTAL	12	

Tabla 5 - 3 Periodo de planificación de la fibra optica

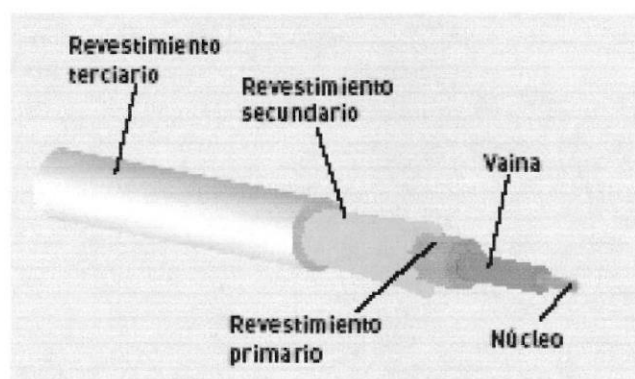
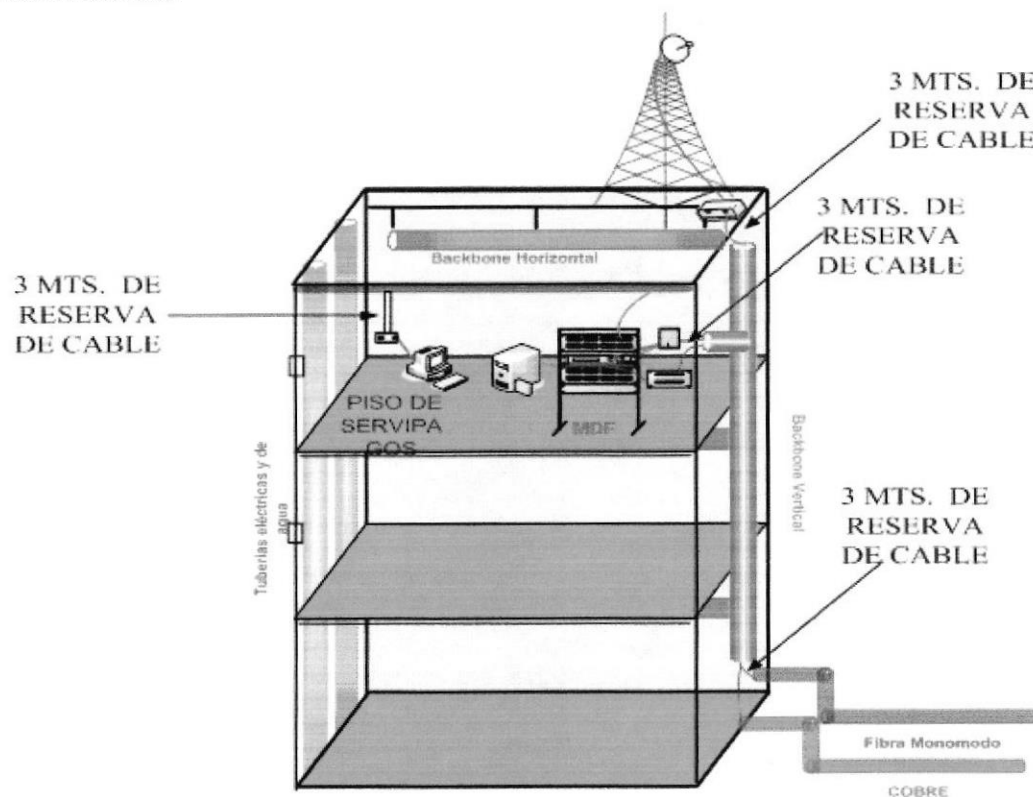


FIGURA 5 - 68: Recomendación 10

**RECOMENDACIÓN 11**

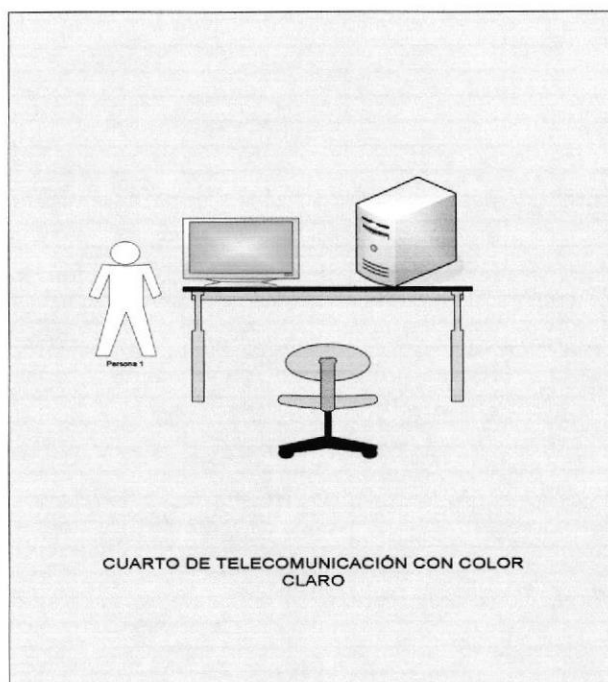
Para cables backbone se recomienda un mínimo de 3mts. De reserva de cable en cada lado o extremo



**FIGURA 5 - 69:** Recomendación 11

△ **RECOMENDACIÓN 12**

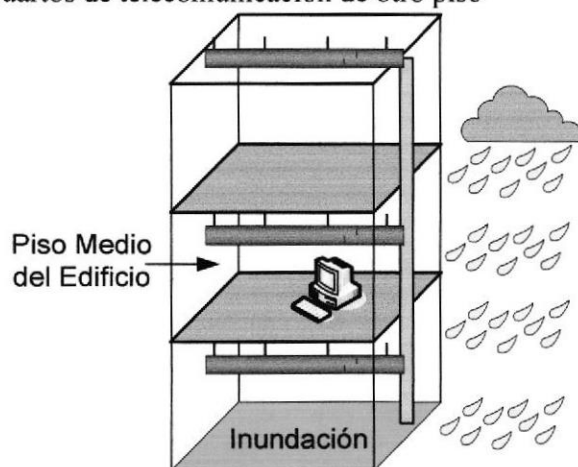
Los acabados en el cuarto de telecomunicación debe ser de color claro para mejorar la iluminación del mismo



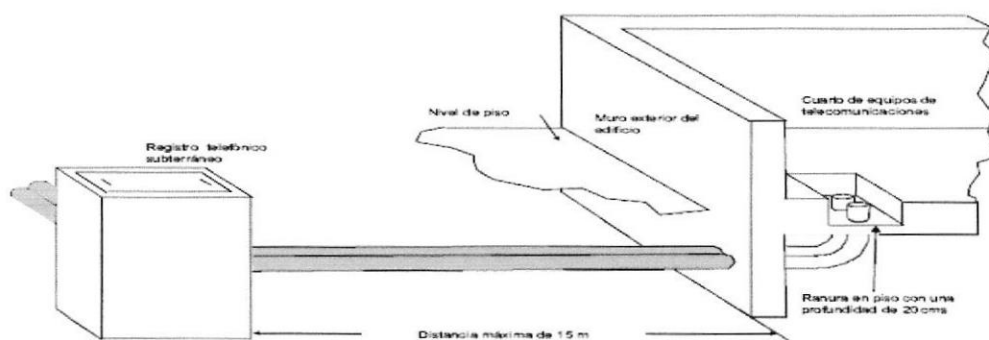
**FIGURA 5 - 70:** Recomendación 12

**RECOMENDACIÓN 13**

Cuando sea factible, en un edificio de varios pisos, se recomienda que el cuarto de equipo se localice en el piso de medio y una ubicación que facilite el acceso a canalización de los cuartos de telecomunicación de otro piso

**FIGURA 5 - 71: Recomendación 13****RECOMENDACIÓN 14**

Se recomienda que el cuarto de equipos se ubique por encima del nivel de inundación y este protegido con filtraciones de tuberías

**FIGURA 5 - 72: Recomendación 14**

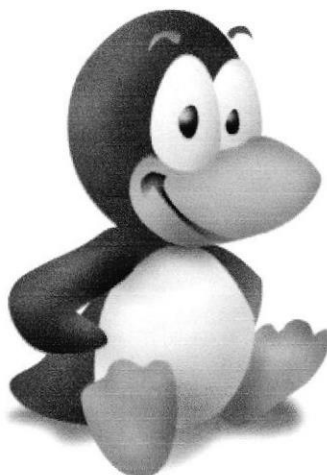
# CAPÍTULO 6

## LINUX



## **6.- LINUX**

### **6.1.- INTRODUCCIÓN A FEDORA CORE 3**



**FIGURA 6 - 1:** introducción a Linux

Entre los sistemas operativos que había hace una década estaba Minix, un sistema operativo tipo Unix, de fuentes publicas, que se había escrito a modo didáctico para los estudiantes de ingeniería informática. Funcionaba en un 8086, por lo que era un poco limitado.

Linux Tolvards un estudiante finlandés de informática que investigando y profundizando en los entresijos de los microprocesadores 386 decidió hacer, partiendo de cero, un sistema operativo, basado en Minix, pero que aprovecharse toda la potencia del 386, memoria virtual, multitarea y otras cosas.

Así que empezó a crearlo, las primeras versiones eran poco atractivas, apenas ejecutabas el GCC (un compilador de C creado según el estilo GNU) el bash (el equivalente al command com). Pero Linux, lo publico en Internet , con sus fuentes ,y un montón de gente se intereso en él, modificándolo, mejorándolo y añadiéndole cosas, a la vez que Linux lo mejoraba y coordinaba todo el trabajo que hacían el resto de la gente. Y así sigue siendo hoy, cientos de versiones después hasta convertirse en lo que tenemos delante.

La gente de GNU creó un montón de programas para su sistema operativo que gracias a que son software libre son también usados e Linux y por eso a Linux se le llama muchas veces GNU/Linux.

El núcleo de Linux, el kernel, se distribuye bajo la licencia GPL, es un tipo de licencia, dentro de lo que podríamos llamar el Open Source Software, básicamente dice que cojas el programa, lo uses, aprendas, lo mejores y compartas esas mejoras con el resto del mundo. Además la licencia GNU fija una serie de derechos a programador que le protegen, pero en resumidas cuentas:

Un Programa con Licencia GPL puede ser vendido, alquilado, prestado modificado, pero:



No se puede limitar el número de usuarios, copias o tiempo de uso.

No se puede cobrar por usar el programa (pero sí por distribuirlo)

No se puede impedir que otros lo vendan o distribuyan.

Tienes que dar las fuentes del programa de una manera pública

Puedes modificar el programa o aprovechar parte del código, pero el resultado tiene que seguir la misma filosofía.

Es básicamente lo que llamaríamos un programa Freeware, o Gratis. Linux sigue esta licencia. Por eso te encontraras a revistas que lo regalan a gente que cobra por él, a gente que lo coge de Internet, y lo encontraras en distribuciones, pero de esto hablaremos mas adelante.

Por su naturaleza Linux se distribuye libremente y puede ser obtenido y utilizado sin restricciones por cualquier persona, organización o empresa que así lo desee, sin necesidad de que tenga que firmar ningún documento ni inscribirse como usuario. Por todo ello, es muy difícil establecer quiénes son los principales usuarios de Linux. No obstante se sabe que actualmente Linux está siendo utilizado ampliamente en soportar servicios en Internet, lo utilizan Universidades alrededor del todo el mundo para sus redes y sus clases, lo utilizan empresas productoras de equipamiento industrial para vender como software de apoyo a su maquinaria, lo utilizan cadenas de supermercados, estaciones de servicio y muchas instituciones del gobierno y militares de varios países. Obviamente, también es utilizado por miles de usuarios en sus computadores personales.

El apoyo más grande, sin duda, ha sido Internet ya que a través de ella se ha podido demostrar que se puede crear un sistema operativo para todos los usuarios sin la necesidad de fines lucrativos.

Linux tiene una mascota oficial, el pingüino de Linux, que fue seleccionado por Linux Torvalds para representar la imagen que se asocia al sistema operativo que él creó.

## **6.2.- CARACTERÍSTICAS DE LINUX FEDORA CORE 3**

### **32 Bits**

Gracias a los 32 bits el sistema es rápido eficaz, seguro y fiable, sin que una aplicación pueda causar problemas a las otras, al no tener que guardar compatibilidad con los sistemas anteriores de 16 bits.

### **Multitarea**

El ordenador puede estar haciendo varias cosas a la vez, y que no tendrás que esperar a que acabe una para hacer otra, la multitarea esta controlada por el S.O. no por las aplicaciones, por lo que a diferencia de otros S.O. nunca se te quedara parado por culpa de una mala aplicación que consuma todos los recursos del ordenador Aquí si podrás bajar correo de Internet, formatear un disco, imprimir 100 hojas y jugar al Quake a la vez, y sin problemas.

### **Multiusuario**

Si has manejado antes un ordenador, seguramente usarías MAC OS o Windows, en estos S.O. tú eres el único que lo usas, en Linux, puede haber varias personas usando el ordenador, compartiendo el microprocesador, así puedes ponerle un par de pantallas y teclados y estar otra persona navegando por Internet, escribiendo una carta, jugando en

su pantalla, mientras tu estas en otra haciendo otra cosa completamente diferente, y estaréis ambos en el mismo ordenador. Además proporciona los elementos necesarios para garantizar la seguridad y la privacidad de los datos entre usuarios.

**POSIX**

Aunque para los usuarios normales esto importa poco, POSIX es un estándar de la industria, que asegura una calidad mínima en ciertas partes del S.O. y asegura su compatibilidad, a nivel de código, es decir, programas POSIX que funcionan en otros Unix, no tendrán problema para compilarse y ejecutarse en Linux, Para muchas empresas esto es muy importante, a la hora de decantarse por un S.O. u otro (por eso Windows NT es compatible POSIX).

**Estabilidad**

Linux es robusto, no se colgara (el S O. una aplicación si esta mal echa por supuesto que se colgara, pero no afectara al resto del sistema, nunca tendrás que reiniciar el ordenador por que un programa lo ha colgado),hay que notar que es posible bloquear el teclado o la pantalla, pero eso no significa que se cuelgue el ordenador, puedes entrar al ordenador por otro sitio (un terminal, por red)y desbloquearlo, y seguir usándolo, o si se te bloquea un programa mientras estabas conectado a Internet y cogiendo correo, quizás no puedas usar el ordenado, pero seguirá bajando el correo sin problemas.

**Es libre**

Es decir no te costara nada, no tendrás que pagar licencias, podrás copiarlo, venderlo, instalarlo donde quieras sin problemas, pero lo más importante es que dispones del código fuente, esto significa que si un día te encontrases con un problema del S.O. no tendrías que esperar inútilmente a que su creador decidiese que era un problema importante y crease un service pack para el S.O., tu mismo puedes solucionar el problema. o puedes indicarle a una 3 º personal el problema, y esta no tendrá que ser de la empresa que creo el S O. para poder solucionártelo.

### **6.3.- REQUERIMIENTOS DE HARDWARE PARA INSTALAR UN SERVIDOR LINUX**

#### **6.3.1.- REQUERIMIENTO HARDWARE MINIMO**

Memoria	64 MB
Espacio en el Disco Duro	5 GB
Procesador	Pentium II de 300 Mhz

**Tabla 6 - 1:** Requerimiento de hardware minimo

#### **6.3.2.- REQUERIMIENTO HARDWARE ÓPTIMO**

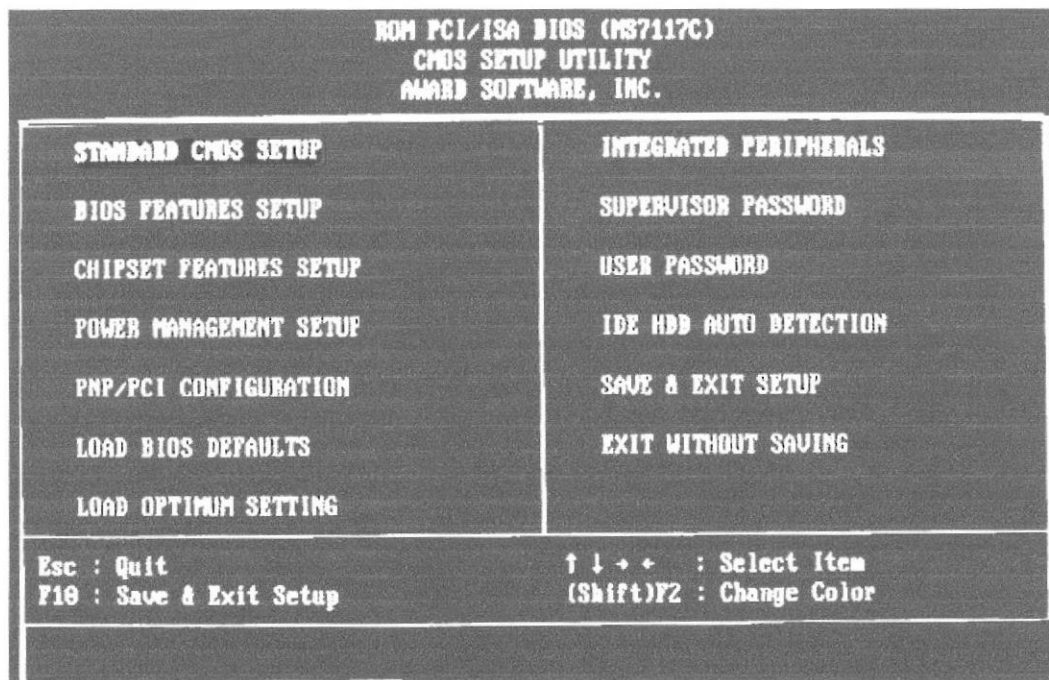
Memoria	512 MB
Espacio en el Disco Duro	10 GB
Procesador	Pentium D

**Tabla 6 - 2:** Requerimiento de hardware óptimo

#### 6.4.- CONFIGURACION DESDE EL BIOS

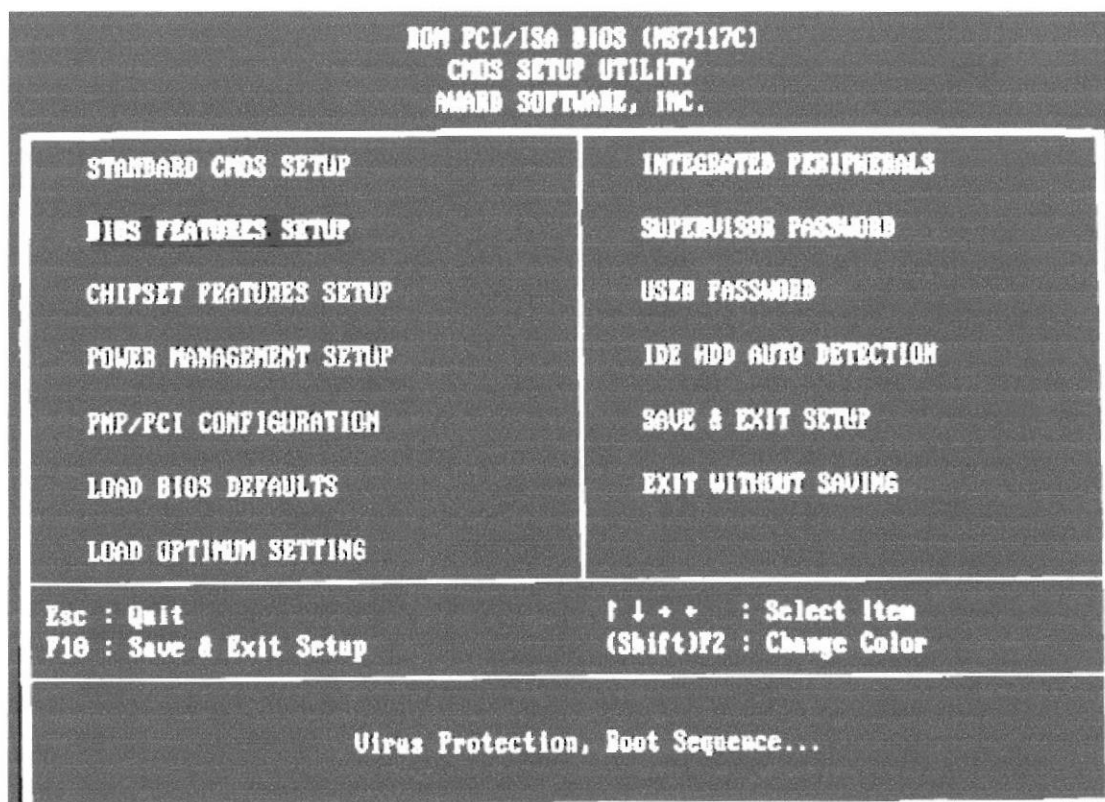
Para iniciar la instalación se debe ingresar al bios pulsar varias veces la tecla suprimir (Equipo Clon) o F2 (Equipo de Marca) dependiendo de la marca.

Una vez que ingrese al BIOS aparecerá una pantalla de configuración parecida a la que se muestra a continuación:



**FIGURA 6 - 2:** Configuración del bios (Setup del computador)

Y al pulsar ENTER, en la opción BIOS FEATURES SETUP, tal como se muestra en la grafica siguiente.



**FIGURA 6 - 3:** Configuración del bios (Features Setup)

Seleccionar el boot sequence para que el PC arranque desde el CDROM (además, hay que quitar la protección antivirus, para volverla a poner al acabar la instalación del sistema operativo).

ROM PCI/ISA BIOS (MS7117C) BIOS FEATURES SETUP AWARD SOFTWARE, INC.			
CPU Internal Core Speed	: Auto	OS Select For DRAM > 64MB	: Non-OS2
		HDD S.M.A.R.T. capability	: Enabled
		Report No FDD For WIN 95	: Yes
CPU clock failed reset	: Disabled	Video BIOS Shadow	: Enabled
CIM Buster Protection	: Enabled	C8000-CBFFF Shadow	: Disabled
Anti-Virus Protection	: Enabled	CC000-CFFFF Shadow	: Disabled
CPU Internal Cache	: Enabled	D0000-D3FFF Shadow	: Disabled
External Cache	: Enabled	D4000-D7FFF Shadow	: Disabled
CPU L2 Cache ECC Checking	: Enabled	D8000-DBFFF Shadow	: Disabled
Processor Number Feature	: Enabled	DC000-DFFFF Shadow	: Disabled
Quick Power On Self Test	: Enabled		
Boot From LAN First	: Disabled		
Boot Sequence	: CDROM,C,A		
Swap Floppy Drive	: Disabled		
Boot Up NumLock Status	: On		
Gate A20 Option	: Normal	ESC : Quit	F1++ : Select Item
Memory Parity/ECC Check	: Disabled	F1 : Help	F1/F2/+/=- : Modify
Security Option	: Setup	F5 : Old Values (Shift)	F2 : Color
PCI/UGA Palette Snoop	: Disabled	F6 : Load BIOS Defaults	
		F7 : Load Optimum Settings	

**FIGURA 6 - 4:** Configuración del bios (arranque desde el CDROM)



Pulsar ESC y se muestra la siguiente pantalla, donde se resalta SAVE & EXIT SETUP, y pulsar ENTER, y el PC arranca de nuevo.

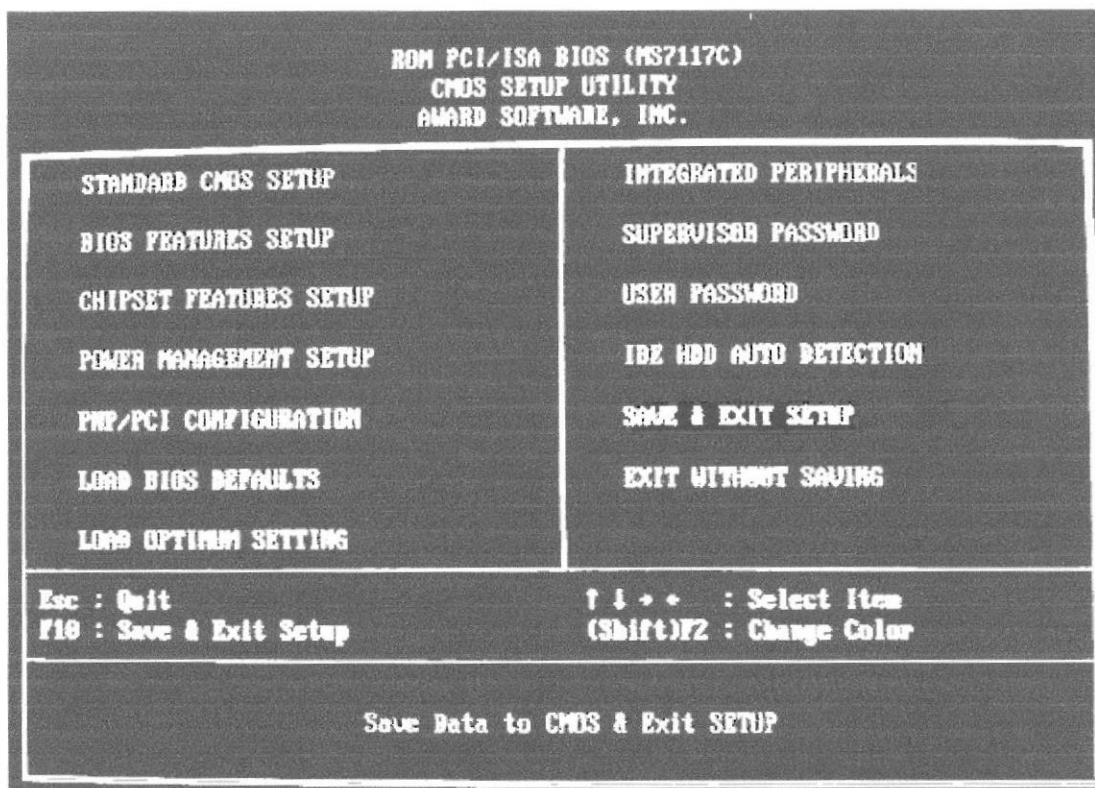


FIGURA 6 - 5: Configuración del bios (save & exit setup, pulsamos enter)



## 6.5.- INSTALACIÓN DE LINUX FEDORA CORE 3

Para la instalación de Linux es necesario un ordenador que tenga espacio en disco duro disponible, no basta con que desde otro S.O. de Windows aparezca el disco con espacio vacío, este espacio tiene que no pertenecer a ninguna partición.

Si se desea conservar el S.O. anterior para un arranque dual, y este ocupa todo el disco duro, habrá que recurrir a una herramienta de terceros, de particiones, para hacer espacio a Linux.

Si Linux va a ser el único S.O. del ese ordenador no importa el estado del disco duro. El proceso de instalación es muy parecido en todas las distribuciones, para ilustrar este capítulo utilizaremos Linux Fedora, la versión libre de Red Hat.

### 6.5.1.- INICIO DE LA INSTALACIÓN.

La mayoría de los CD de instalación de Linux son autoarrancables, en ocasiones puede ser necesario buscar en el programa de configuración de la BIOS del ordenador la opción para que arranque desde CD, así que metemos el CD y encendemos o reiniciamos el ordenador.

La primera pantalla Pertenece al BootLoader, suele estar en ingles, y además de unas pequeñas instrucciones, nos permite indicar algunos parámetros que pueden ser de ayuda en casos de PC poco compatibles y que den problemas al instalar.

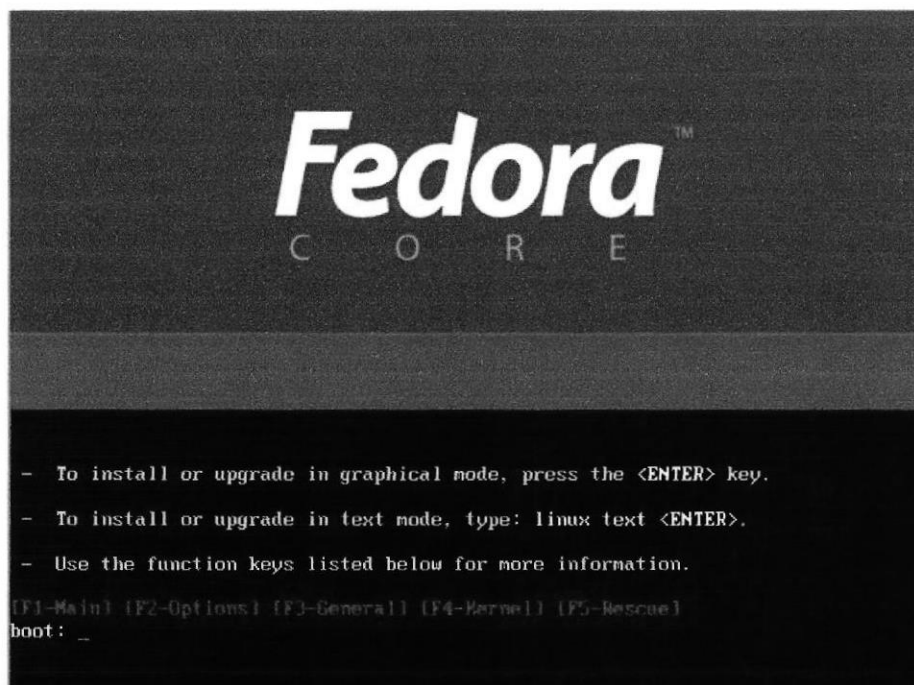


FIGURA 6 - 6: Arranque de fedora core



En la instalación de Fedora se permite comprobar la integridad de los CD, esto es, que no están rallados o mal grabados, lo que se asegurara un contratiempo menos durante la instalación. Una vez terminado este pasó, arranca el instalador grafico.

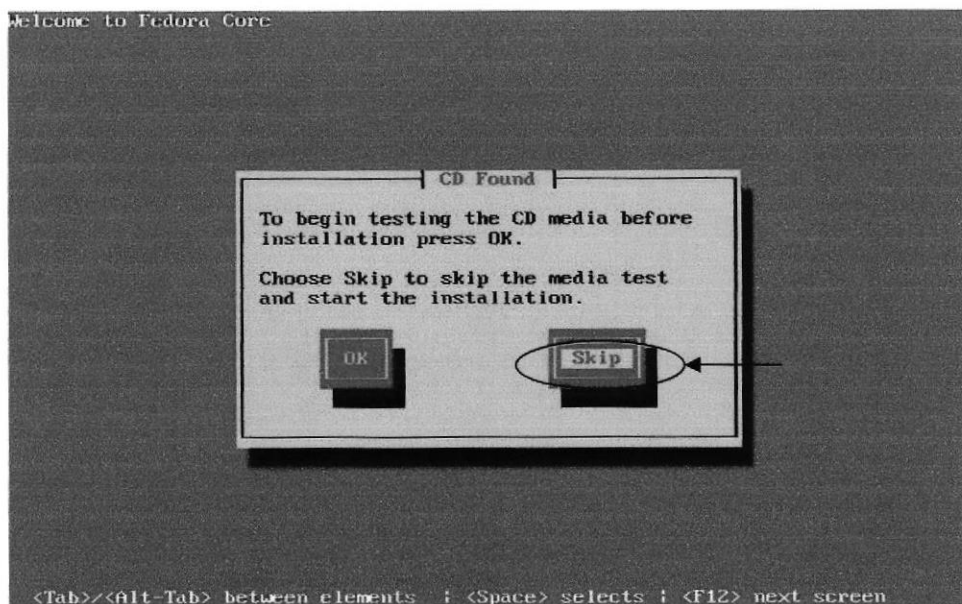


FIGURA 6 - 7: pulsar skip

Tras pulsar skip iniciara la instalación grafica por defecto, luego dar clic en Next.

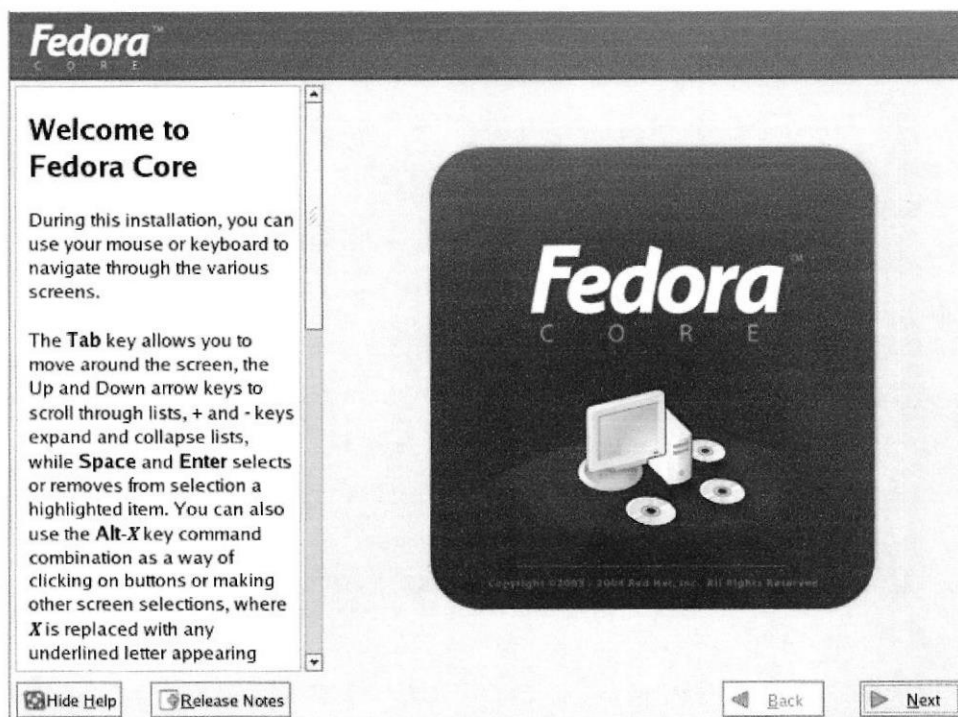


FIGURA 6 - 8: Pantalla de bienvenida a fedora

Nos pregunta el idioma en que se va a realizar la instalación (independiente del que luego utilice el usuario).

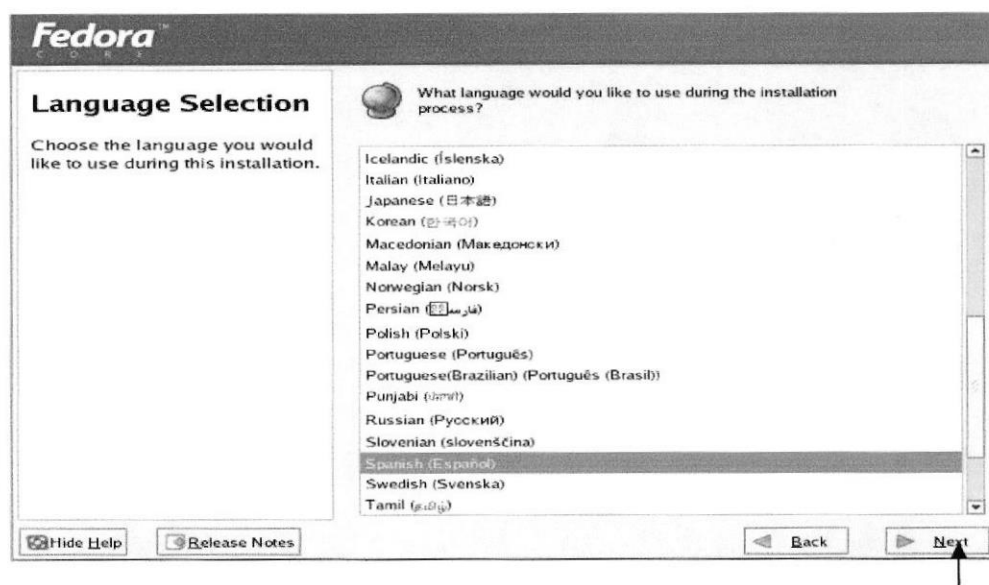


FIGURA 6 - 9: Selecciona el idioma

La configuración del teclado y del ratón, para asegurar que no hay problemas en los siguientes pasos.

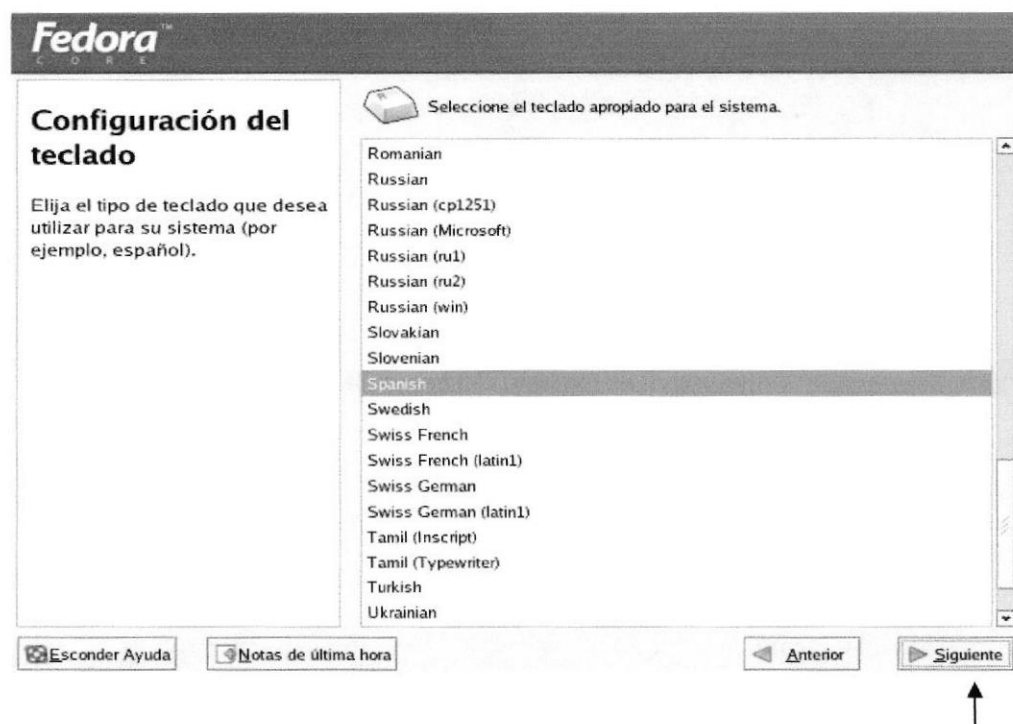


FIGURA 6 - 10: Configuración del teclado spanish

Tras esto se pregunta el tipo de instalación que desea, en caso de querer instalar ninguno de los roles predefinidos, la opción personalizada nos permitirá mas adelante decidir uno por uno que programas que lleve el sistema, para seguir con la instalación dar clic en siguiente.

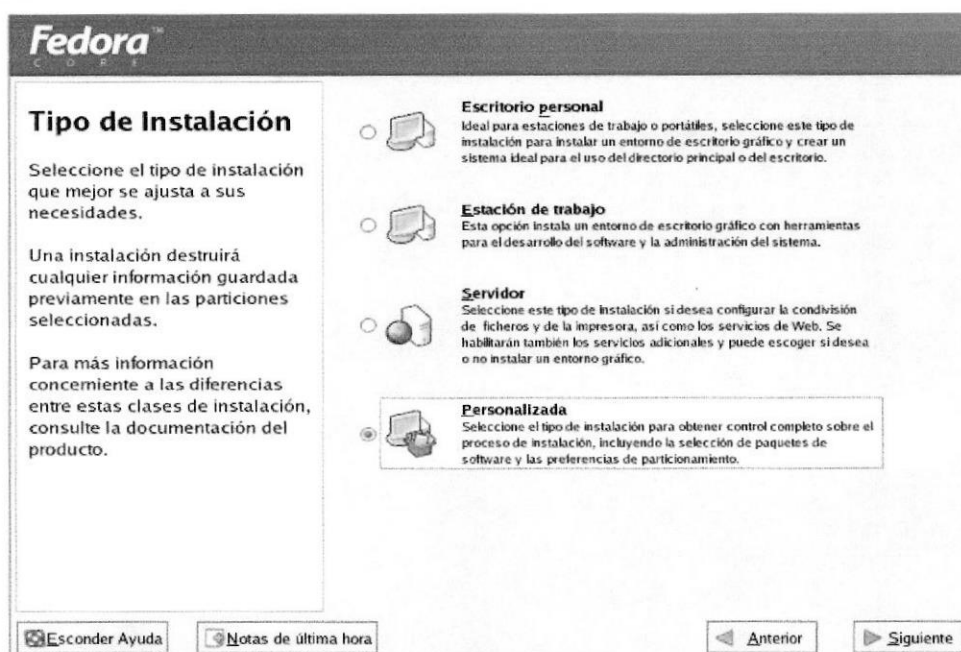
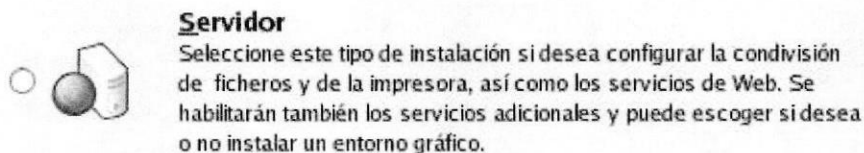
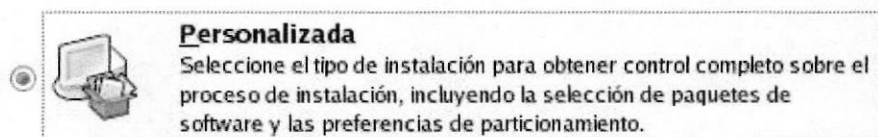


FIGURA 6 - 11: Tipo de instalación

Si al coger esta opción de Servidor, el asistente instalara todos los paquetes relacionados con un Servidor, incluyendo paquetes que el administrador no usara.



Esta opción permite elegir paso a paso las herramientas y paquetes que vallamos a instalar en nuestro Servidor.



1. Escoger la opción **Particionamiento manual con Disk Druid**
2. Dar clic en siguiente

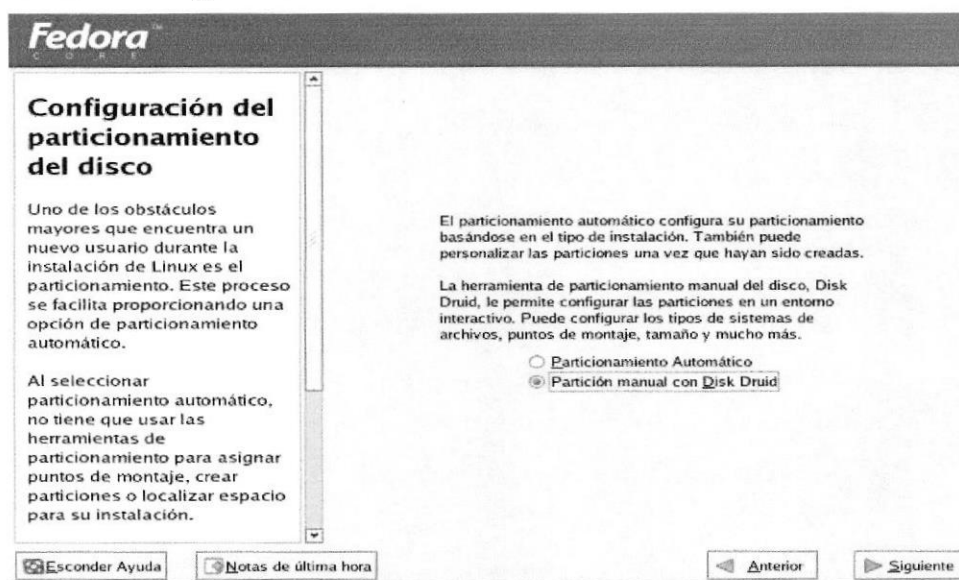


FIGURA 6 - 12: Configuraciones de las particiones

En esta pantalla el asistente permite asignar un **espacio en el disco duro** en el cual el sistema operativo va a ser instalado, dar clic en Nuevo para comenzar la creación de las particiones.

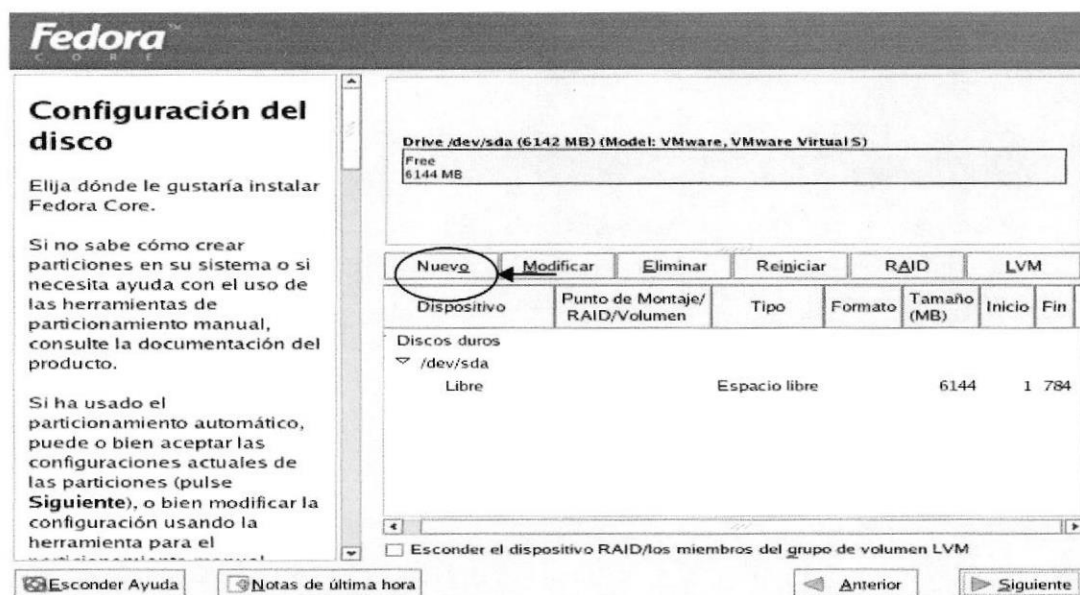


FIGURA 6 - 13: Configuración del disco

En esta pantalla se comenzara a crear la **partición Boot**, que es la que maneja el sistema de buteo de Linux, asignar el tamaño por defecto de 100 MB, dar clic en aceptar.

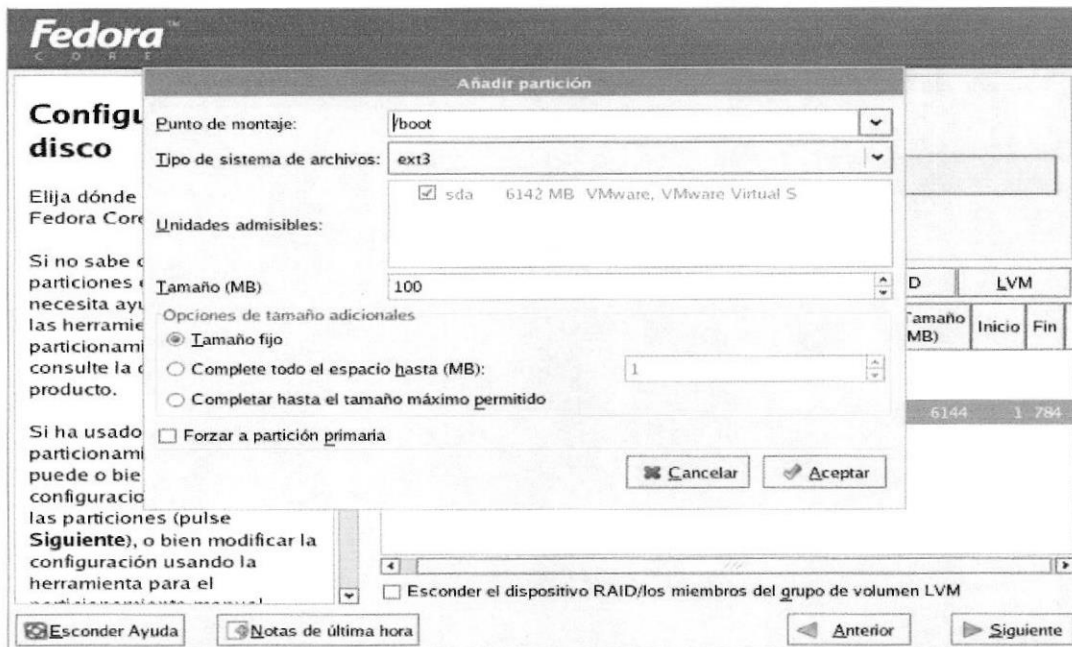


FIGURA 6 - 14: partición boot

En esta pantalla se comienza a crear la **partición Swap**, que es la partición que maneja la memoria virtual del sistema, se le asigna el tamaño dependiendo de la Memoria Ram que tenga el Servidor, para este caso le 512 MB, luego dar clic en aceptar.

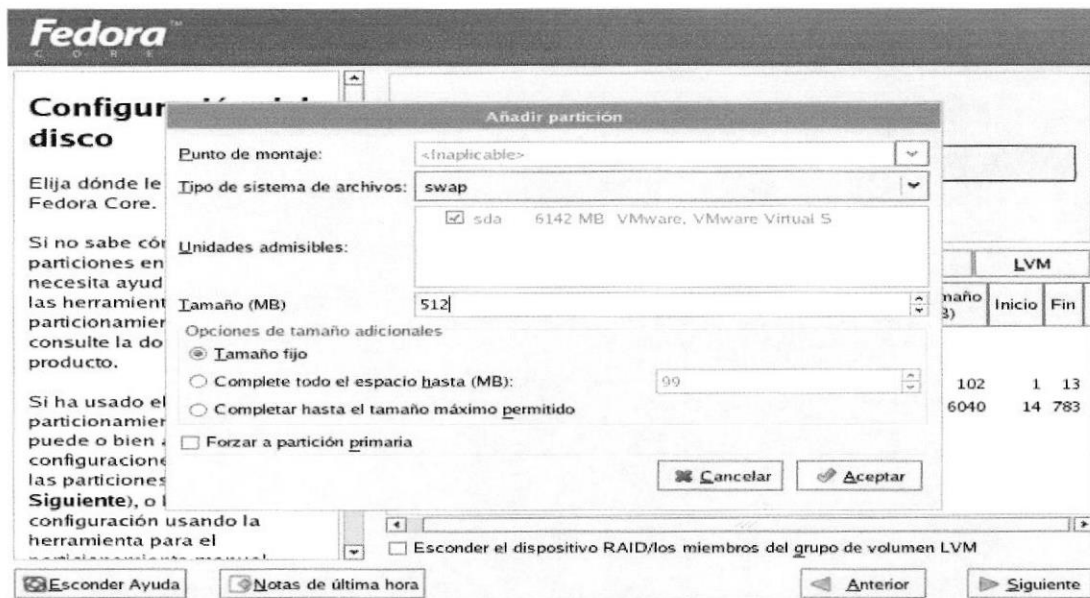


FIGURA 6 - 15: partición swap

En esta pantalla se comenzara a crear la **partición Raíz**, esta partición permite crear la estructura de directorios en Linux, se recomienda un espacio mínimo de 5 Gb, dar clic en aceptar.

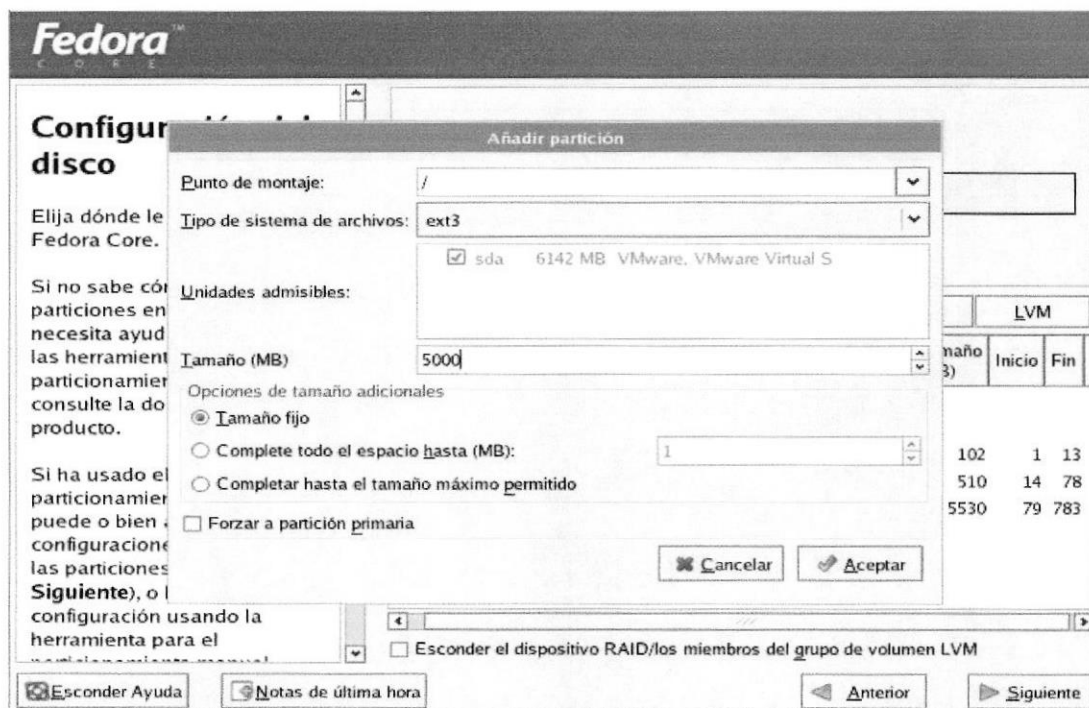


FIGURA 6 - 16: partición raíz



Tiene que haber al menos una partición de root, montada en / con espacio suficiente para el sistema, se deberá crear una partición swap y otra boot si se desea butear con otro sistema operativo.

**Partición /** es el espacio que se le va a dar en el disco duro al sistema.

**Partición boot** esta partición se crea en caso de que este instalado otro sistema como Windows.

**Partición swap**, idealmente del doble del tamaño de la memoria ram, y al menos 64Mb, para equipos con mucha ram, 256Mb o más, esto es opcional, aunque recomendable para mejorar su funcionamiento.

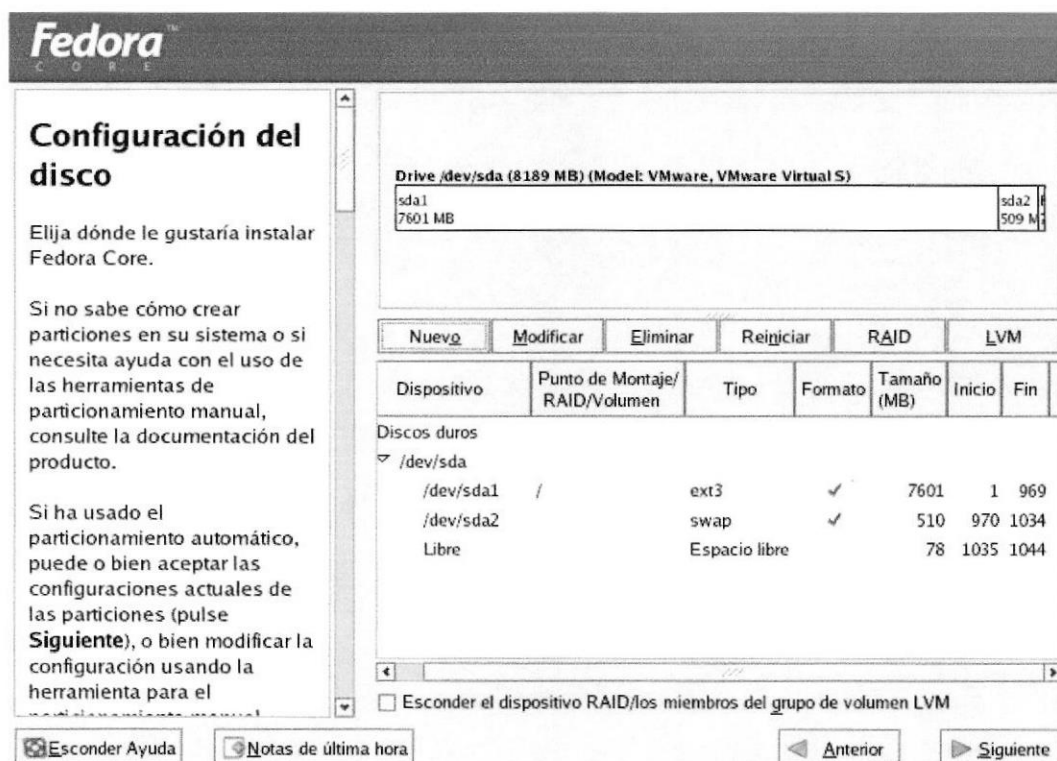


FIGURA 6 - 17: Configuración del disco



Se configurara el bootloader, permitiéndonos arrancar Linux u otro S.O. que estuviese en el ordenador.

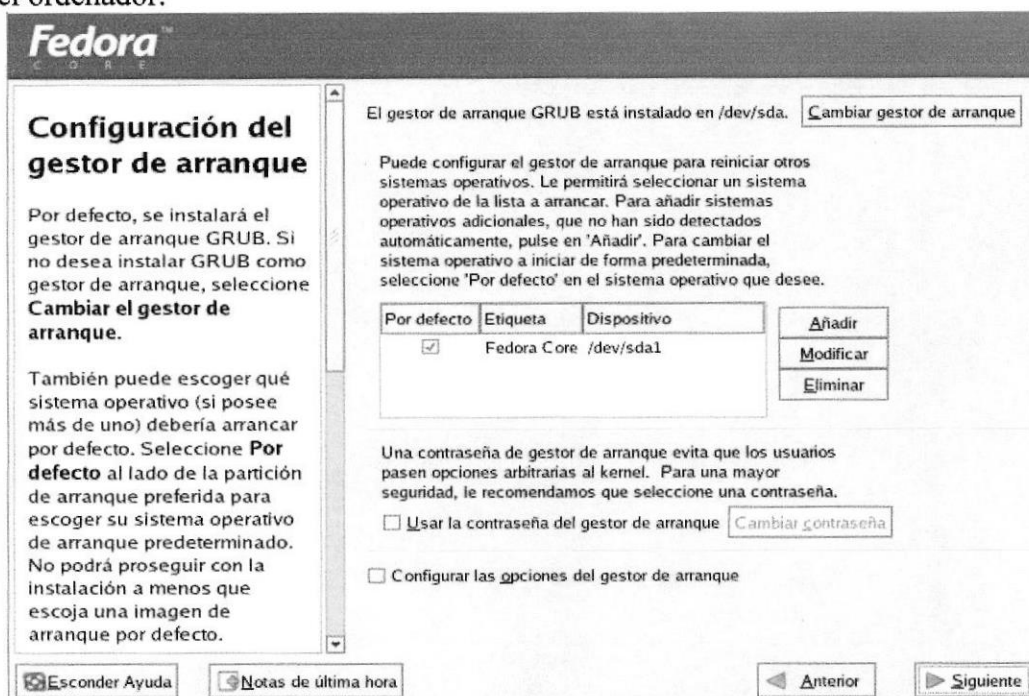


FIGURA 6 - 18: Configuración del gestor de arranque

Esta pantalla da la opción de configurar la tarjeta de red, ya sea una ip estática o por dhcp, para este caso de dar clic en siguiente.

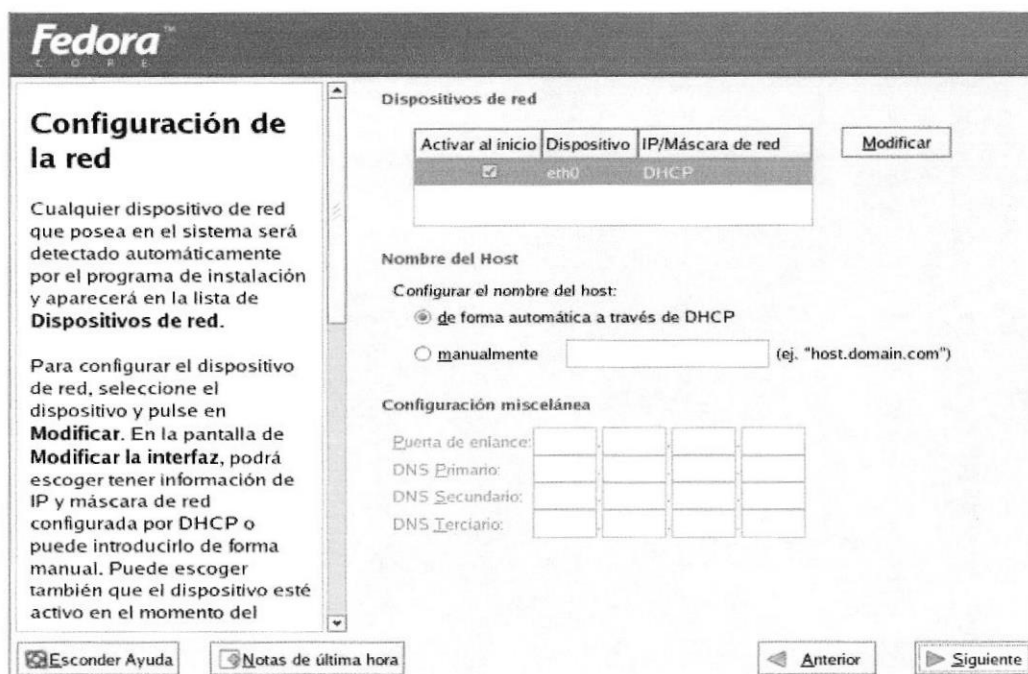


FIGURA 6 - 19: Configuración de la red



Se dará la opción de activar un Firewall en el servidor para aumentar la seguridad, para este caso de clic en siguiente ya que los firewall se los configurar después.

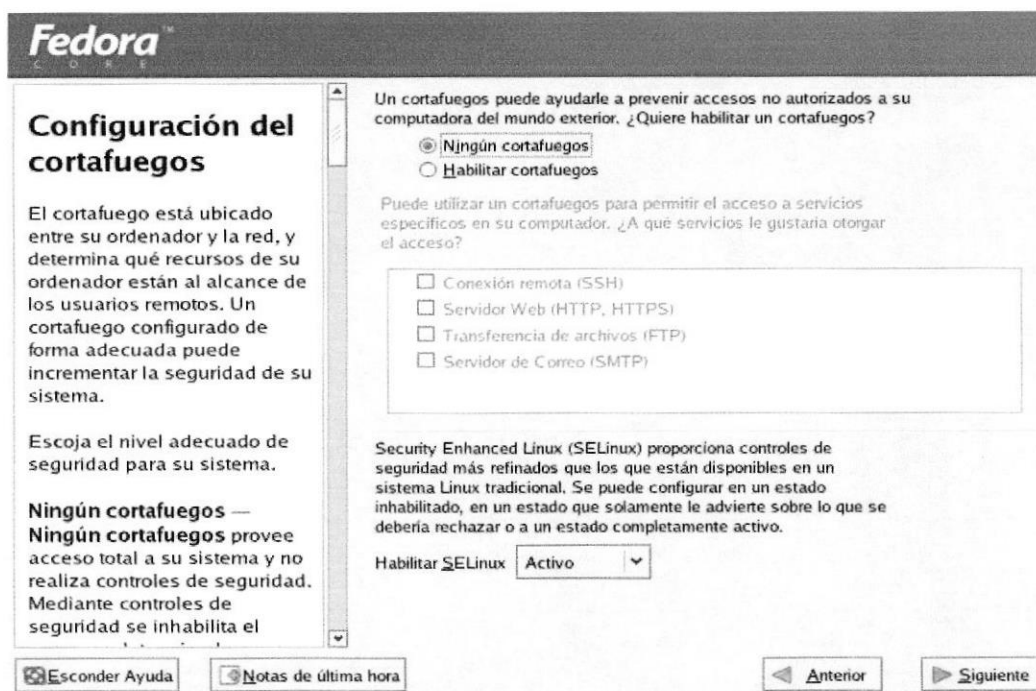


FIGURA 6 - 20: Configuración del cortafuego

En esta pantalla el asistente nos pregunta si se desea continuar con la instalación, para continuar con la instalación de clic en Proceder.

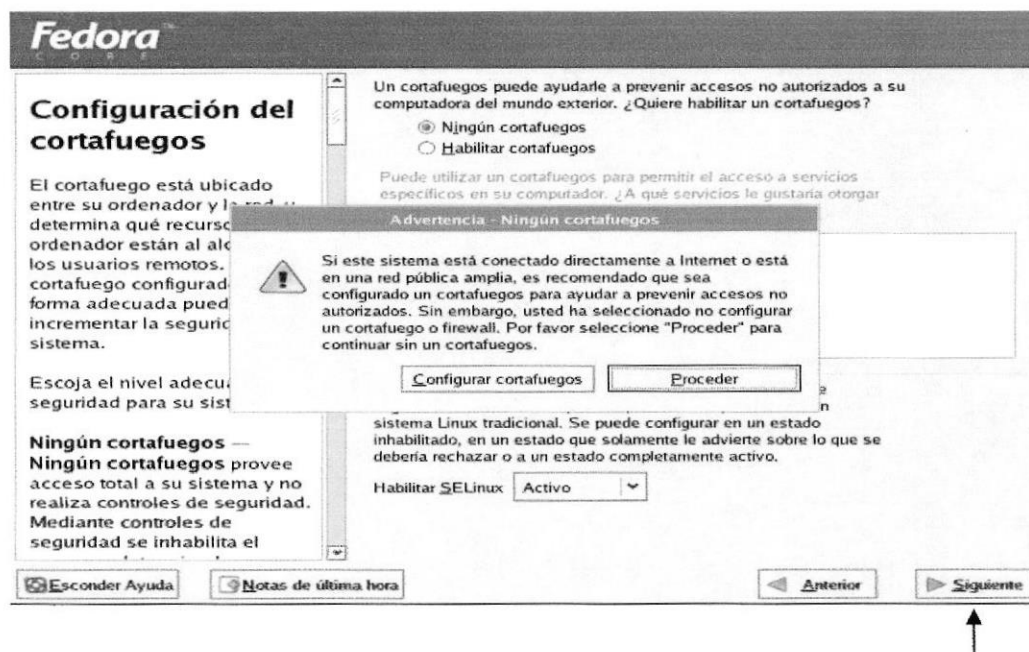


FIGURA 6 - 21: Advertencia si hay o no cortafuego

Se pedirá información sobre los idiomas que estarán disponibles en el ordenador.

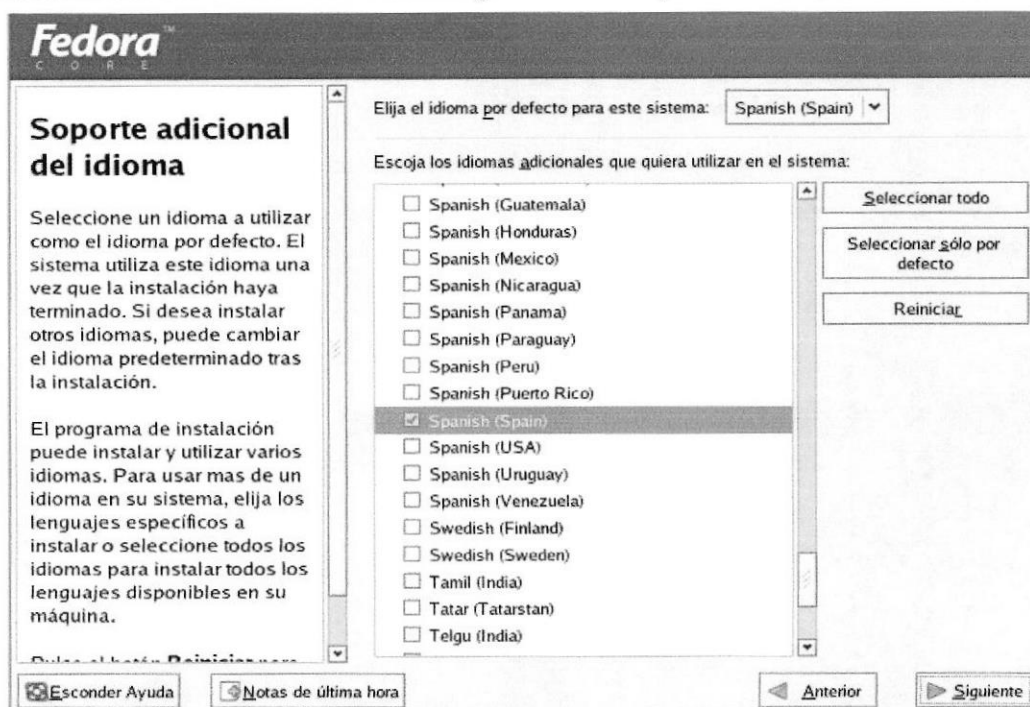


FIGURA 6 - 22: Soporte adicional del idioma

Aquí se dará la opción de configurar la zona horaria.

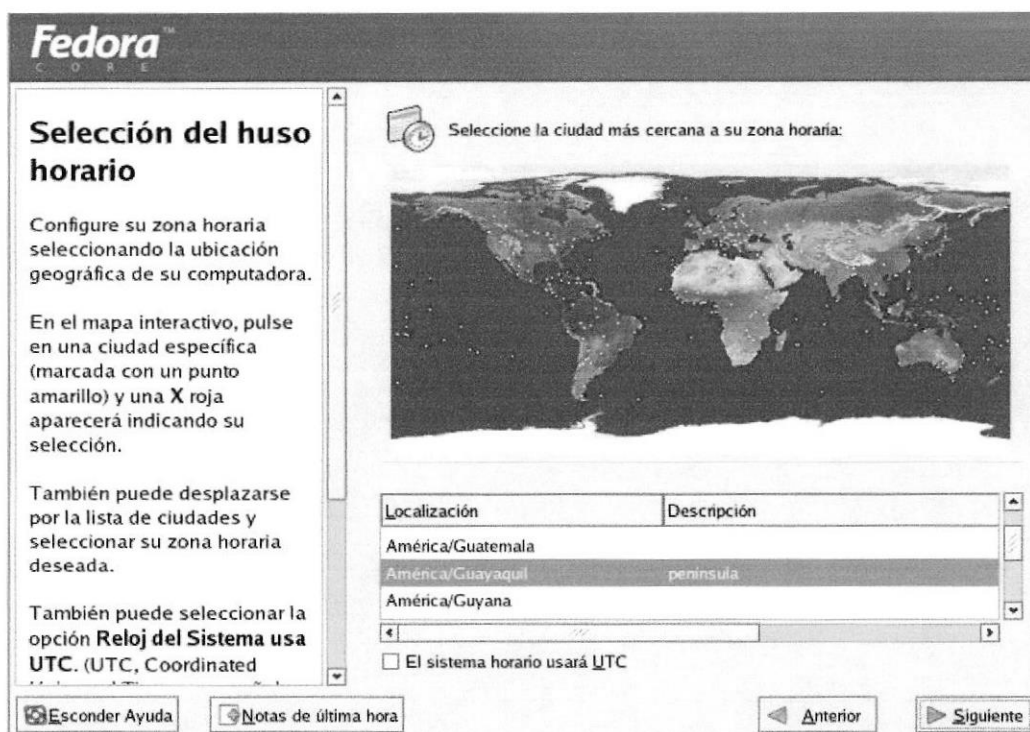
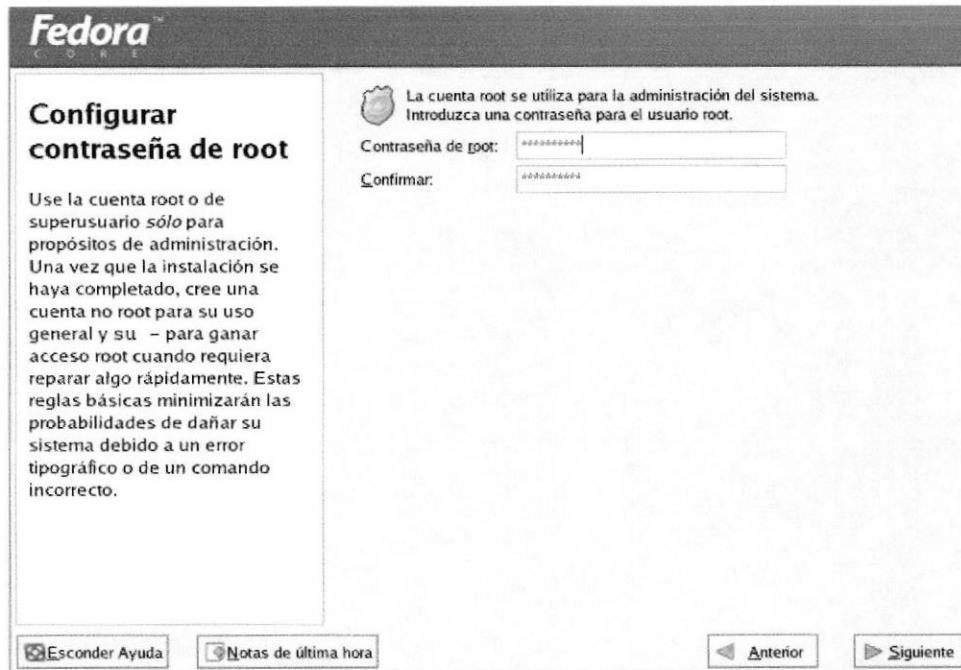


FIGURA 6 - 23: Selección del uso de horario

Se pedirá una contraseña para el Administrador del equipo (el root).



The screenshot shows the 'Fedora Core 3' logo at the top. The main window is titled 'Configurar contraseña de root'. On the left, there is a text box explaining the root account: 'Use la cuenta root o de superusuario sólo para propósitos de administración. Una vez que la instalación se haya completado, cree una cuenta no root para su uso general y su - para ganar acceso root cuando requiera reparar algo rápidamente. Estas reglas básicas minimizarán las probabilidades de dañar su sistema debido a un error tipográfico o de un comando incorrecto.' On the right, there is a shield icon and the text: 'La cuenta root se utiliza para la administración del sistema. Introduzca una contraseña para el usuario root.' Below this, there are two input fields: 'Contraseña de root:' and 'Confirmar:'. Both fields have a password mask (dots). At the bottom, there are four buttons: 'Esconder Ayuda', 'Notas de última hora', 'Anterior', and 'Siguiente'.

FIGURA 6 – 24: Configuración de la contraseña root



### 6.5.2.-INSTALACIÓN DE LOS PAQUETES DE SOFTWARE

En el caso de que al elegir la instalación personalizada, ahora aparecerá el listado de paquetes disponibles, deberá elegir los que se desea, así como sus dependencias, recordar que mas tarde siempre se puede volver a instalar software que en un primer momento

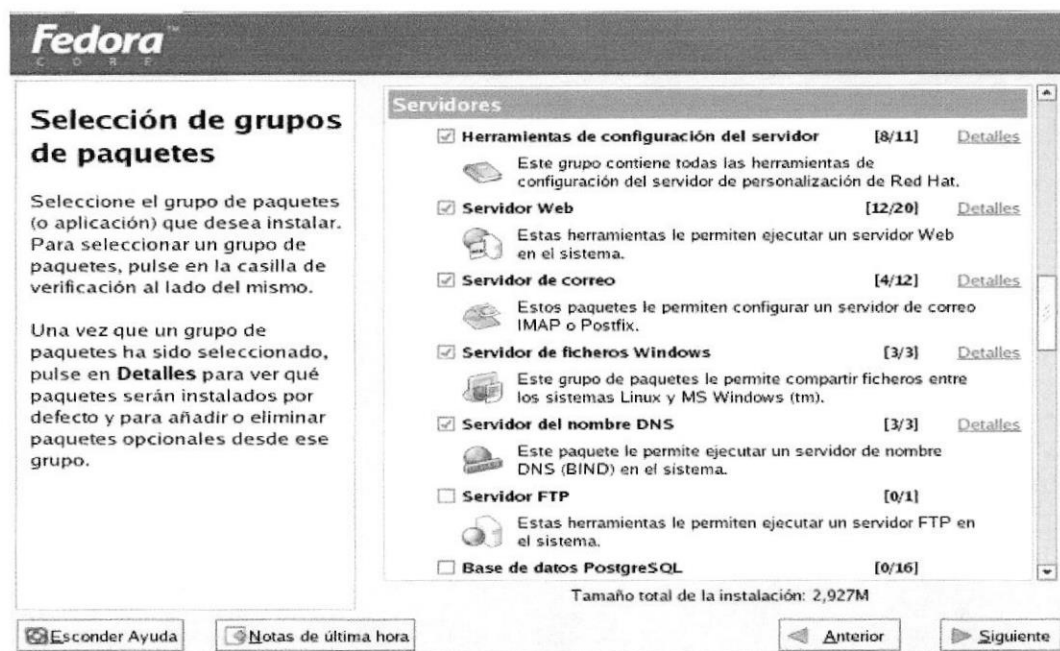


FIGURA 6 - 25: Selección de grupos de paquetes

Por defecto el servicio de DHCP no viene marcado en las opciones para instalarse, en esta pantalla al marcar la opción de dhcp Servidor y agente DHCP, para continuar con la instalación dar clic en Aceptar.

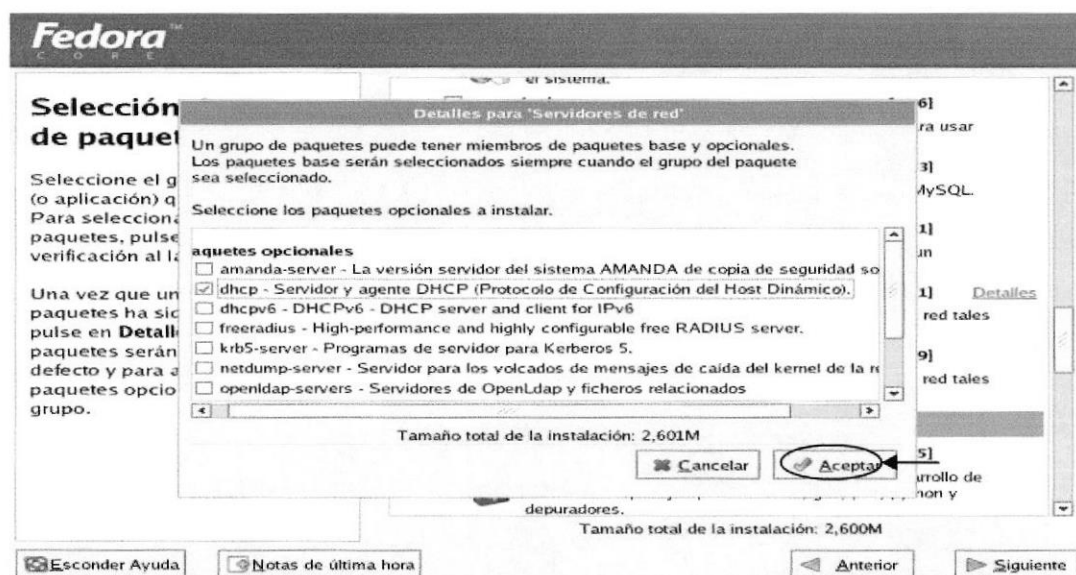


FIGURA 6 - 26: selección de paquete dhcp

Se procederá a formatear las particiones, y montarlas según la información que se proporcione antes.

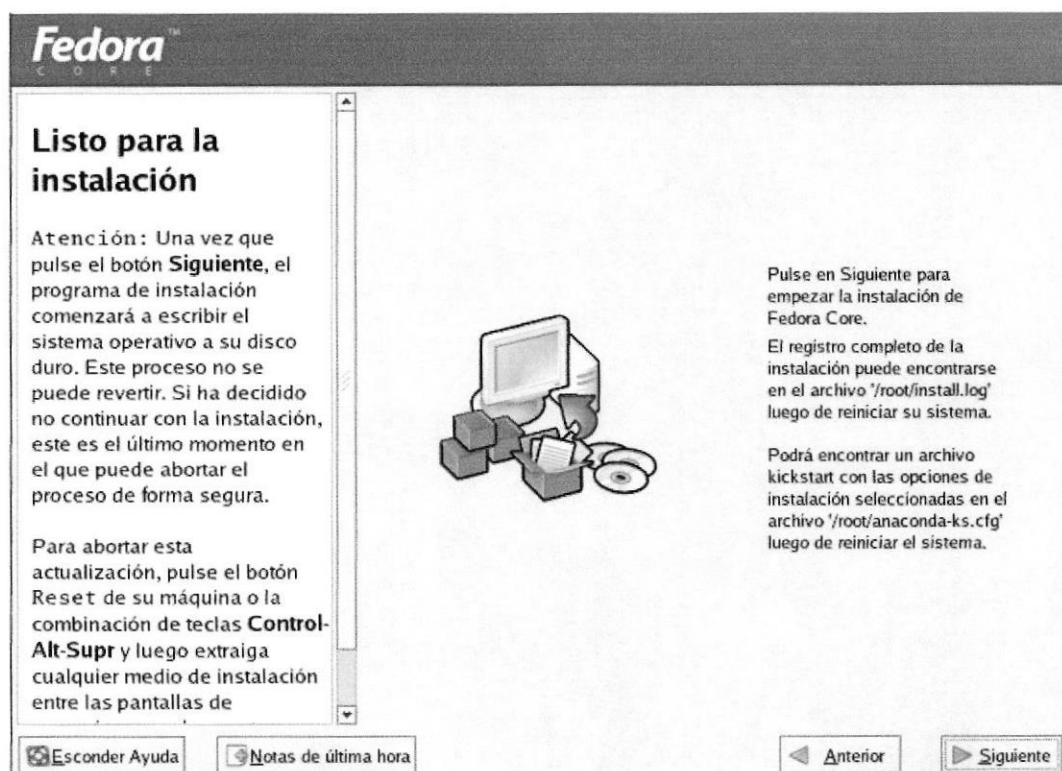


FIGURA 6 - 27: Listo para la instalación

Tras esto el programa de instalación procederá a instalar los programas, pidiendo los CDS en cada caso y configurando las partes que sean necesarias.

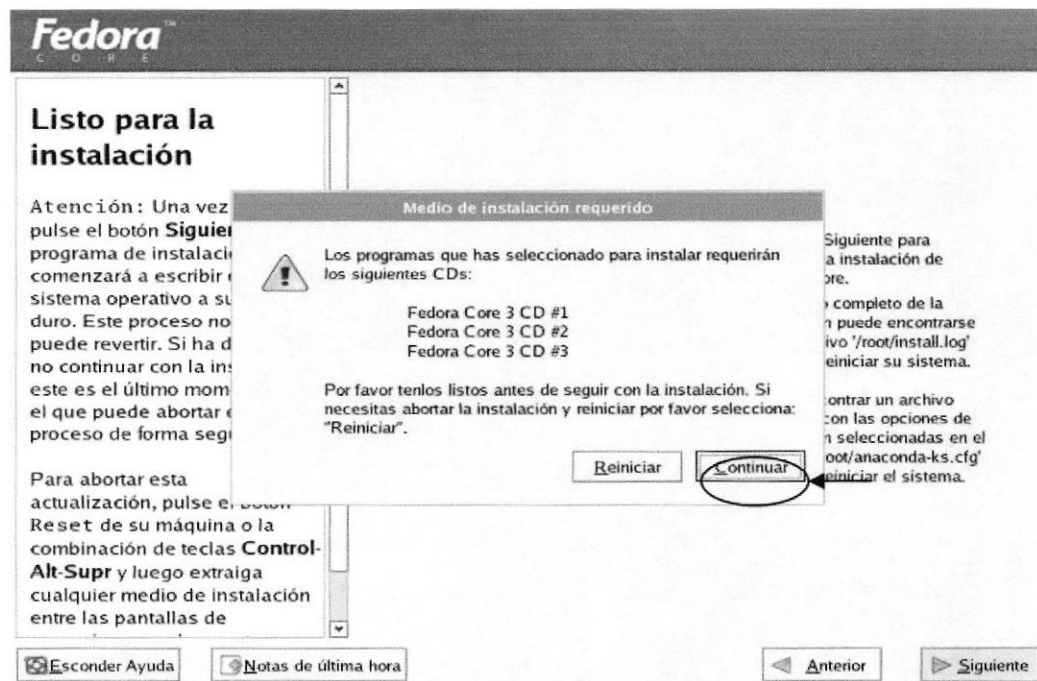


FIGURA 6 - 28: Continuando la instalación

En esta pantalla el asistente muestra la creación y formateo de nuestras particiones.

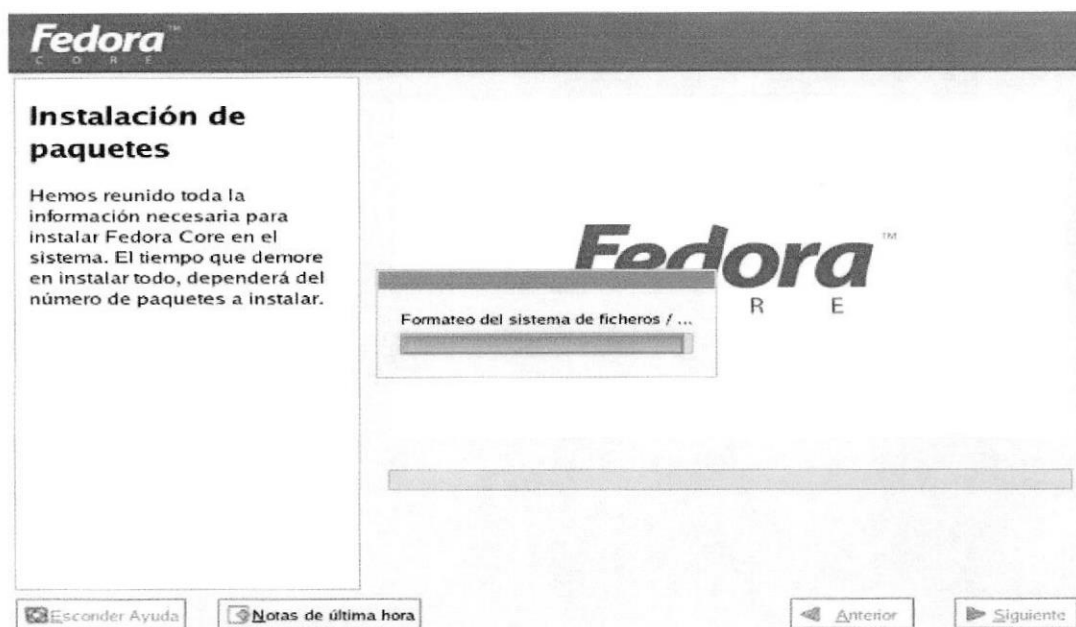


FIGURA 6 - 29: Instalación de los paquetes

Una vez reunido toda la información se procederá con la instalación de Linux.

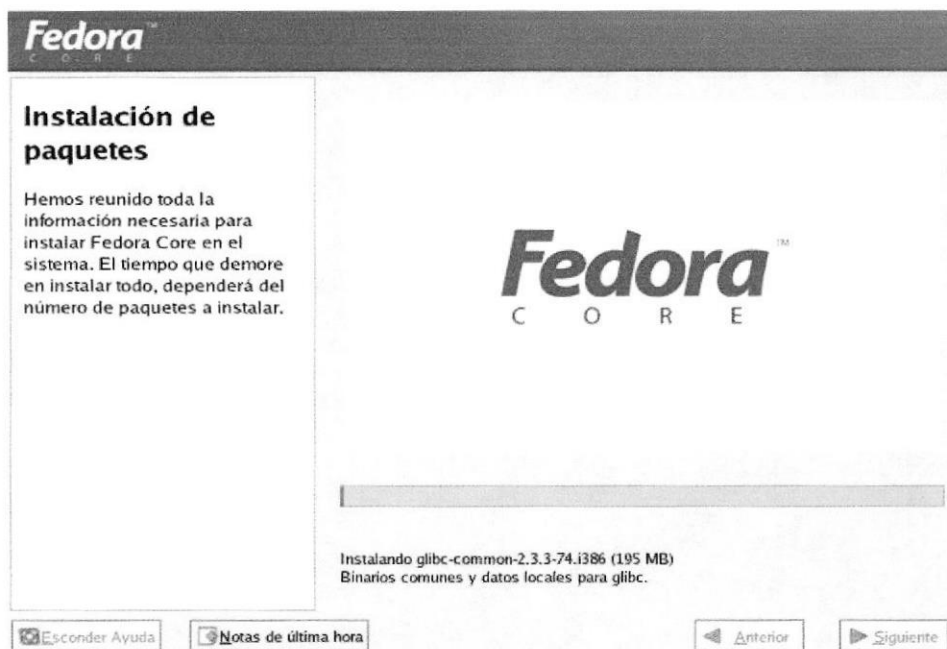
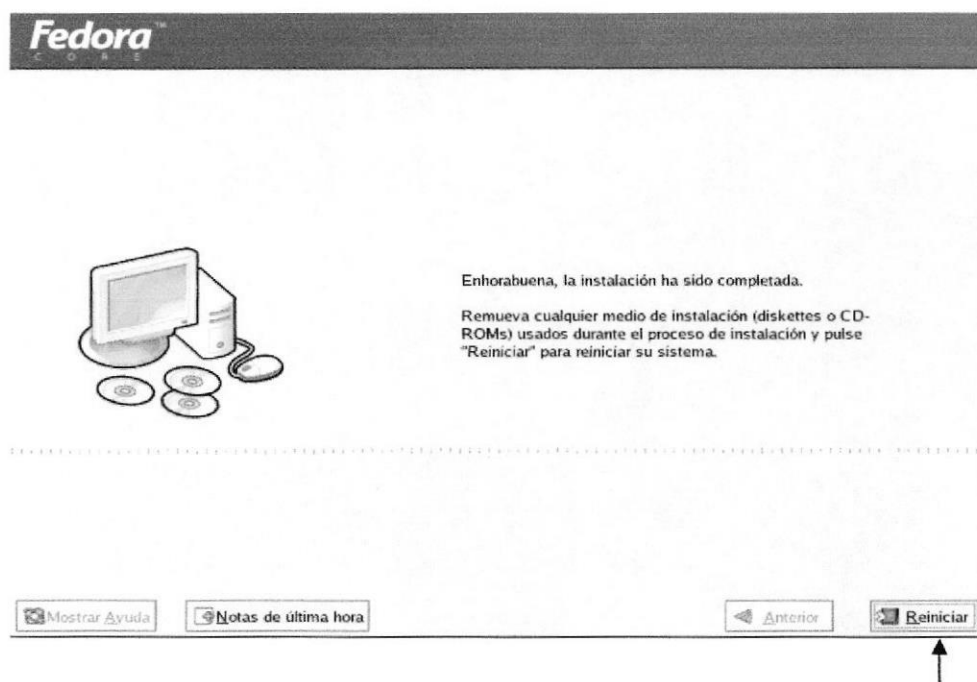


FIGURA 6 - 30: Instalación de los paquetes en proceso



Finalmente muestra la pantalla de una buena instalación y pide reiniciar el equipo, dar clic en reiniciar.



**FIGURA 6 - 31: Instalación Finalizada**

### 6.5.3.- INSTALACIÓN TERMINADA CON ÉXITO

En esta pantalla se muestra que la instalación fue terminada con éxito, y el sistema comienza a cargar y levantando los servicios.



FIGURA 6 - 32: Reinicio del sistema

Esta pantalla muestra el gestor de arranque.

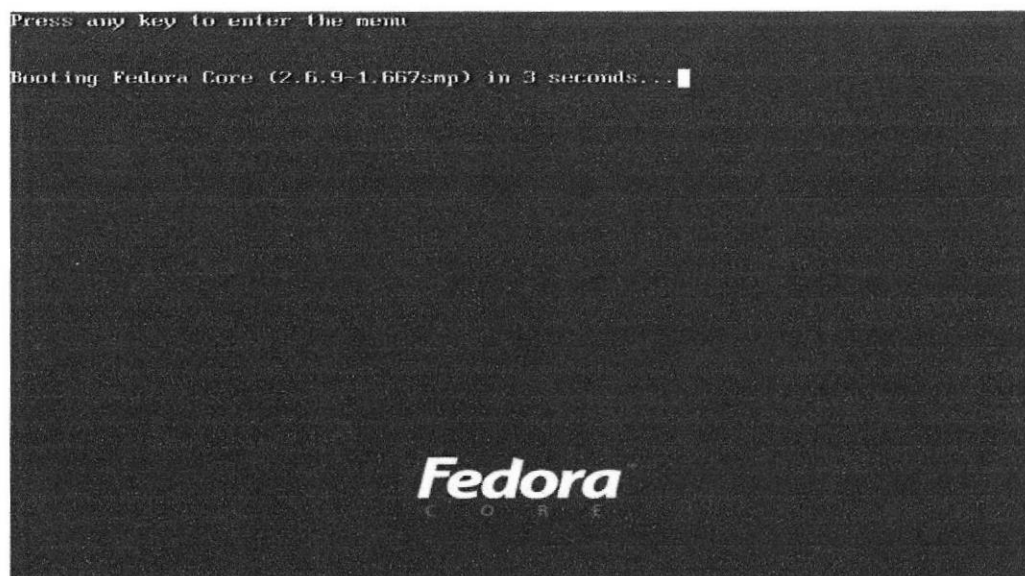


FIGURA 6 - 33: Gestor de Arranque



#### 6.5.4.- CONFIGURACIÓN POST INSTALACIÓN

Durante el primer inicio se configuraran aquellas partes del sistema. Que no pudieron o no debían ser configuradas durante la instalación.

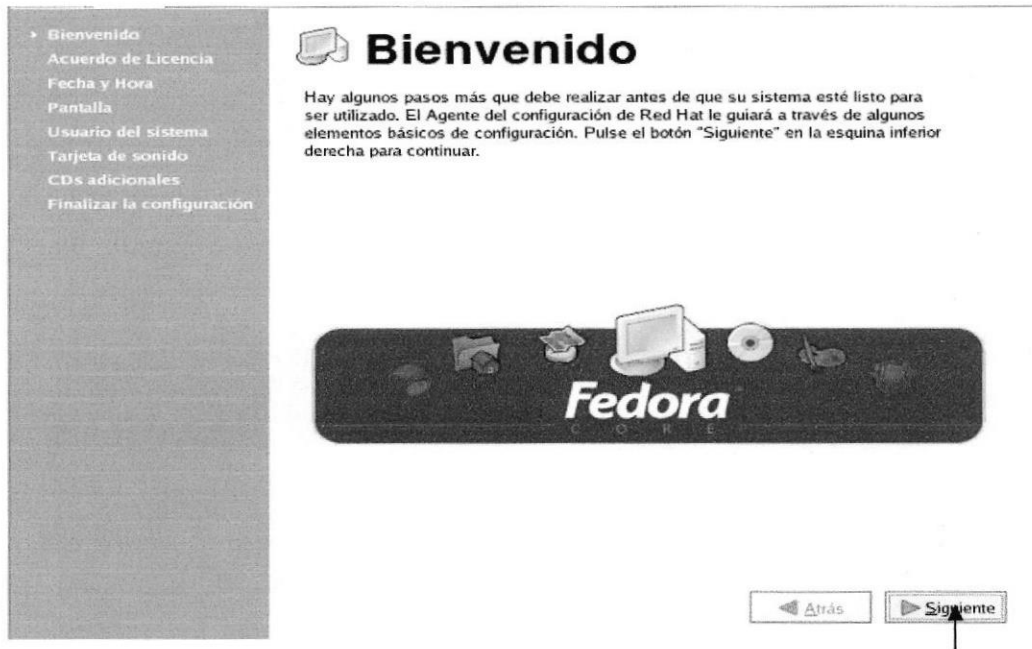


FIGURA 6 - 34: Pantalla Bienvenido

Ahora aparecerá el acuerdo de Licencia, que se debe aceptar si esta de acuerdo.

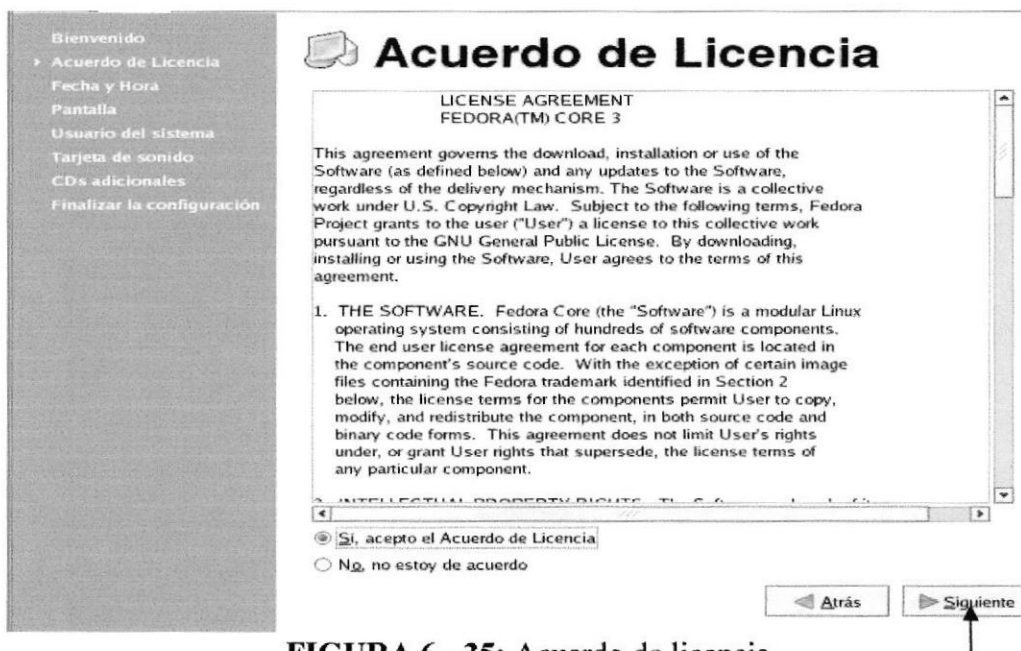


FIGURA 6 - 35: Acuerdo de licencia

También se configurara la Hora del sistema.

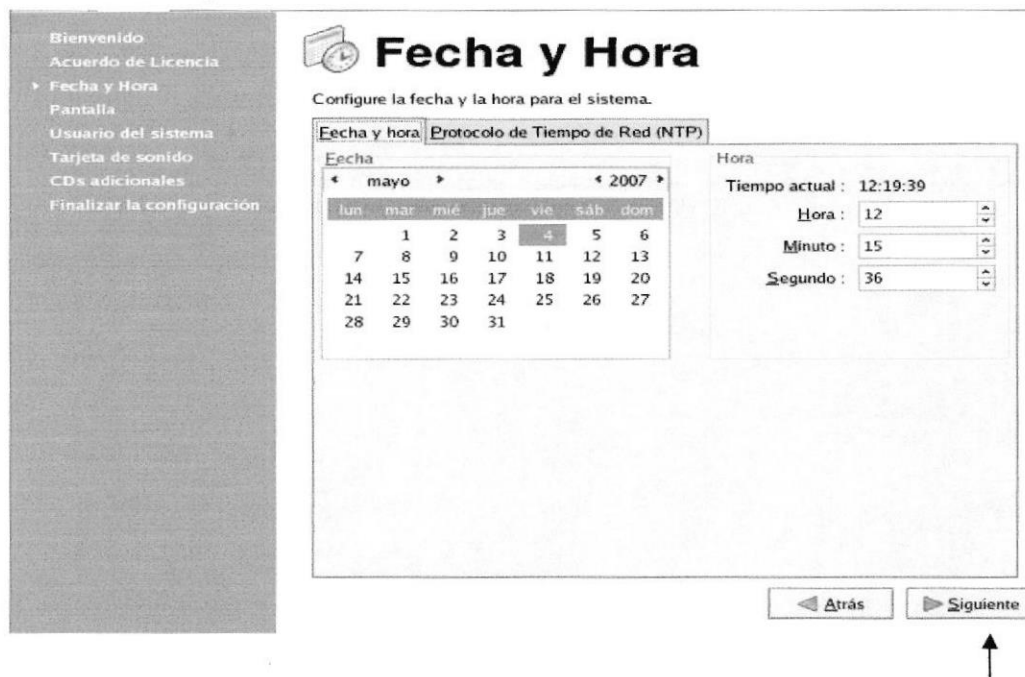


FIGURA 6 - 36: Configuración de la Fecha y Hora

Se configurara hardware de video para el correcto funcionamiento del ordenador.

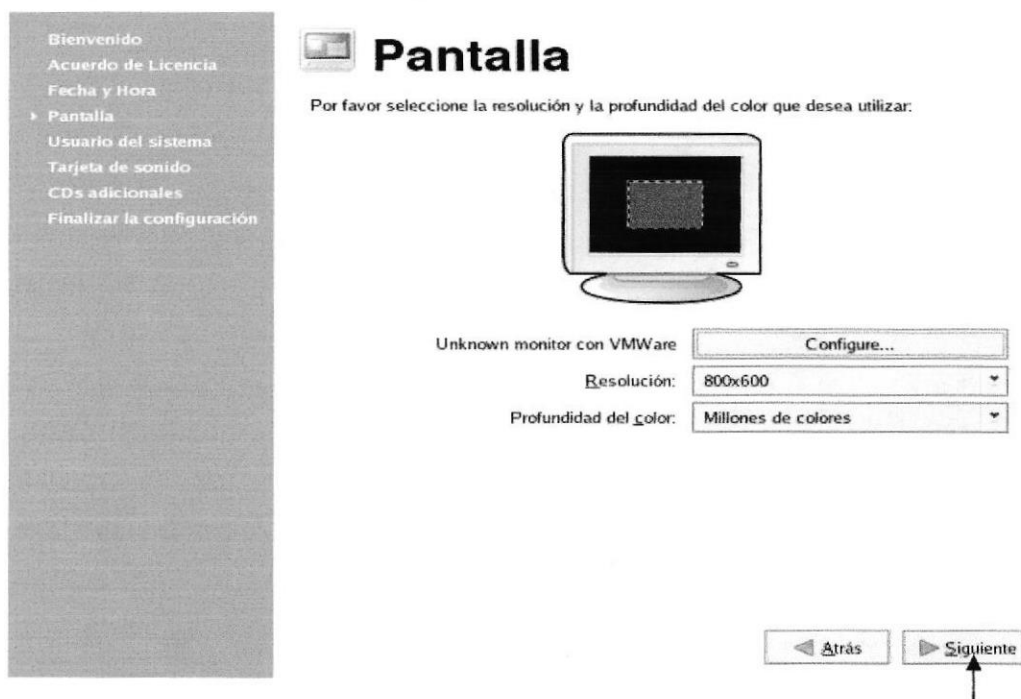


FIGURA 6 - 37: Configuración de la pantalla

Además se permite crear los usuarios (al menos uno, recordar la mala idea que es usar root siempre).

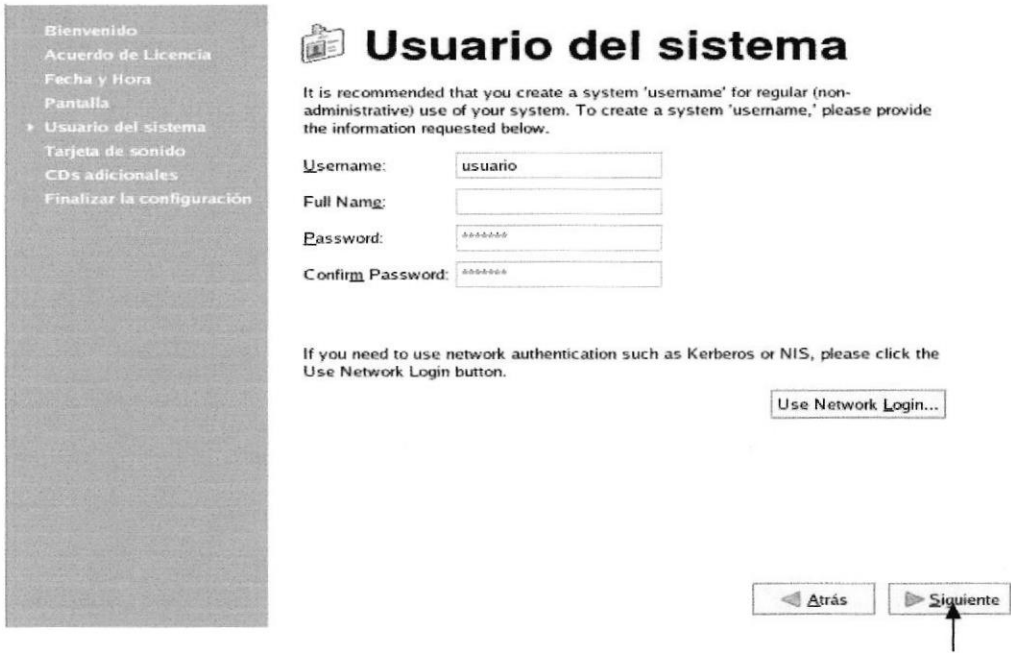


FIGURA 6 - 38: Configuración de usuario del sistema

Se configurara hardware de sonido para el correcto funcionamiento del mismo.

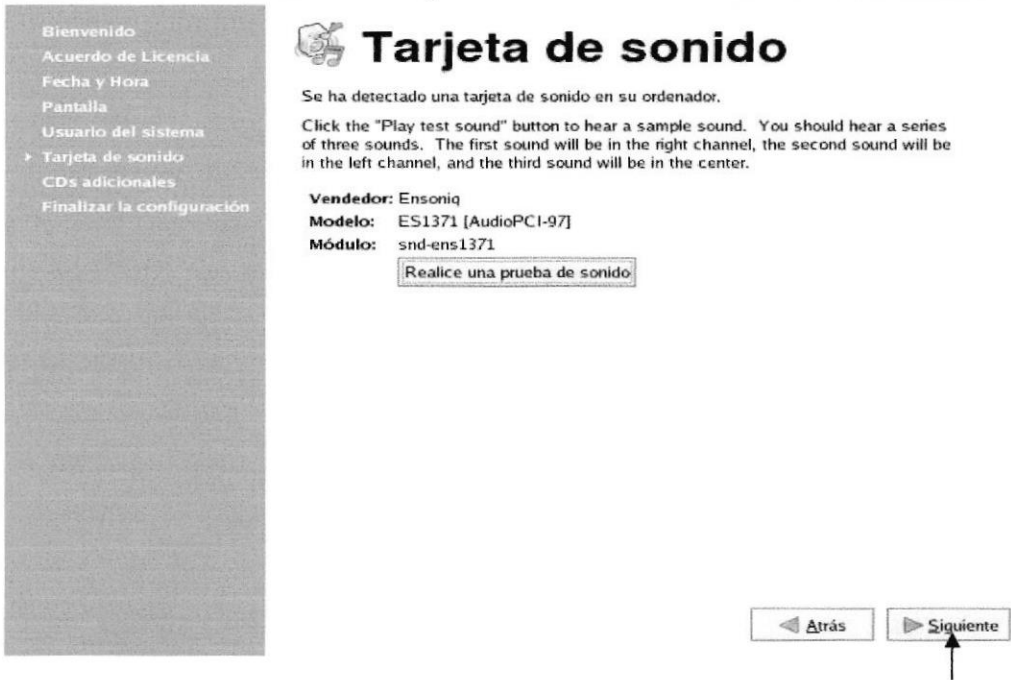


FIGURA 6 - 39: Configurando Tarjeta de sonido

Y por ultimo se preguntara si al tener el CD adicionales con software, para que el sistema sepa que están disponibles a la hora de listar los programas que se pueden instalar

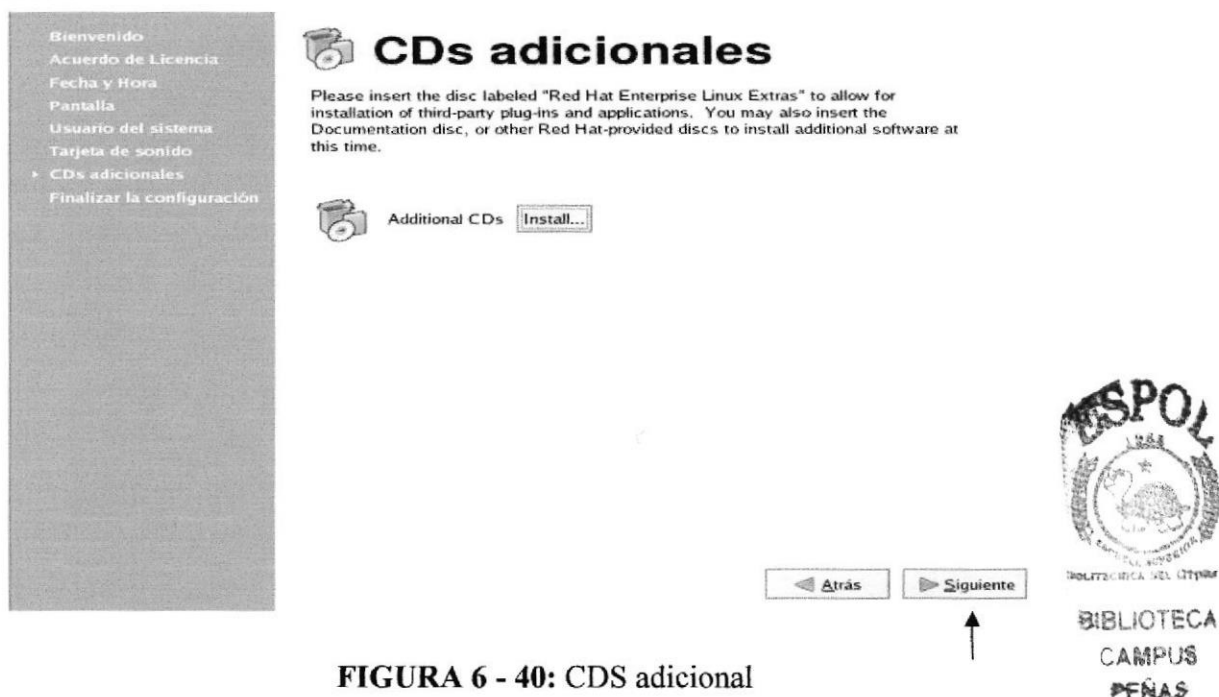


FIGURA 6 - 40: CDS adicional

Tras esto quedaría preparado para el uso, no siendo necesarios mas reinicio, excepto en el caso de Compilar un Kernel nuevo.

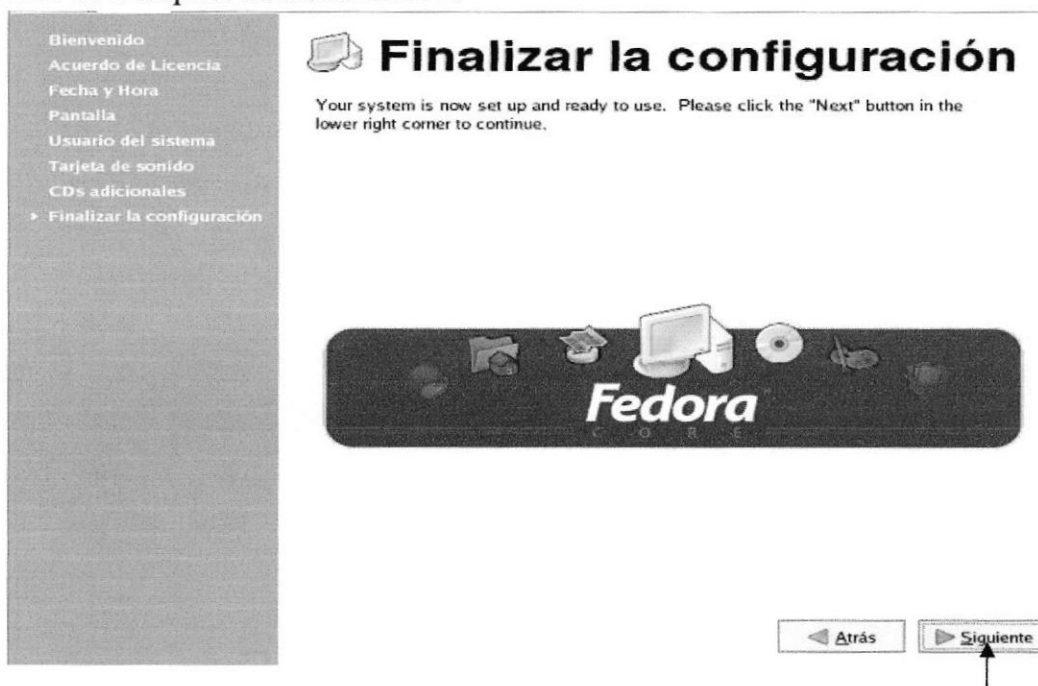
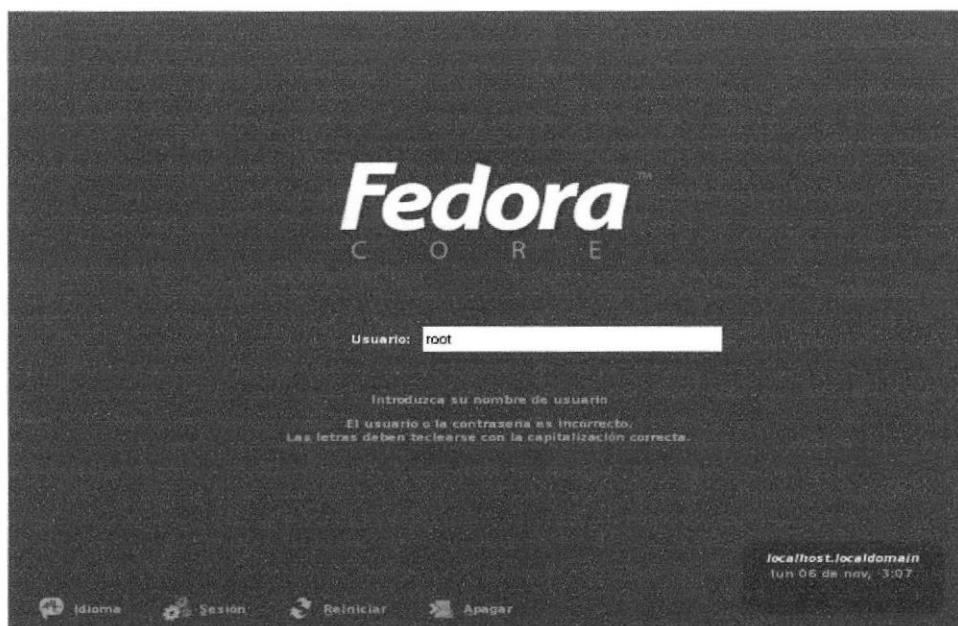


FIGURA 6 - 41: Finalización de la configuración

**6.5.5.- INICIANDO EL SISTEMA OPERATIVO EN AMBIENTE GRÁFICO**

Da la opción de ingresar el nombre del usuario root.



**FIGURA 6 - 42:** Ingresando el Usuario

Da la opción de ingresar la contraseña del usuario antes ingresado.



**FIGURA 6 - 43:** Ingresando la Contraseña

Esta pantalla indica q el sistema operativo ya esta iniciado y ya se podrá trabajar en el.



**FIGURA 6 - 44:** Modo grafico escritorio de Linux

**6.5.6.- INICIANDO EL SISTEMA OPERATIVO EN AMBIENTE TEXTO.**

Una vez estando en el modo gráfico se presionar las combinaciones de teclas CTRL + ALT + F2 al F6.



**FIGURA 6 - 45:** Modo texto de Linux



**6.6.-COMANDOS BASICO DE LINUX CORE 3**

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 tarea /etc/
find	Encuentra archivos.	find squid.conf
mkdir	Crea un directorio.	mkdir tame
mv	Mueve un archivo(s) a un directorio.	mv deber.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
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 200.10.148.1
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/claves
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 200.10.148.1
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
tar -cvf	<b>Tar--</b> Comando <b>c--</b> Crea un nuevo archivo tar <i>create</i> <b>v--</b> Da los nombres de los archivos procesados <b>f--</b> La información generada por el proceso se escribe en un archivo y no se muestra en la pantalla	tar -cvf /práctica.tar
tar -xvf	<b>Tar--</b> Comando <b>X---</b> ejecutar archivos o cambiar de directorio <b>v--</b> Da los nombres de los archivos procesados <b>f--</b> La información generada por el proceso se escribe en un archivo y no se muestra en la pantalla	tar -xvf /práctica.tar

Tabla 6 - 3: Comandos Básicos de Linux

Para efectuar el cambio o la introducción de un **password o contraseña** se utiliza el comando **passwd**.

El proceso a seguir es el siguiente:

**passwd**

**(current) UNIX password:** (se teclea la contraseña actual; no aparece en pantalla)

**New UNIX password:** (se teclea la nueva contraseña; no aparece en pantalla)

**Retype new UNIX password:** (se teclea de nuevo la nueva contraseña comprobando que se ha tecleado bien. Si no coincide no se cambia produce el cambio).

## 6.7.- CONFIGURACIÓN DE LA TARJETA DE RED MODO TEXTO

Para configurar la tarjeta de red se escribe el siguiente comando en la terminal.

**Ifconfig eth0 "IP del servidor" up.**

Donde **ifconfig** es el comando de Linux, **eth0** es como reconoce Linux a la tarjeta de red y **up** nos indica se le levantara la ip asignada.

Ejemplo: `ifconfig eth0 200.10.148.1 up`

<b>Ifconfig</b>	Palabra reservada
<b>eth0</b>	Red card via comando
<b>200.10.148.1</b>	Dirección del servidor
<b>Up</b>	Indicador levantamiento de la red card



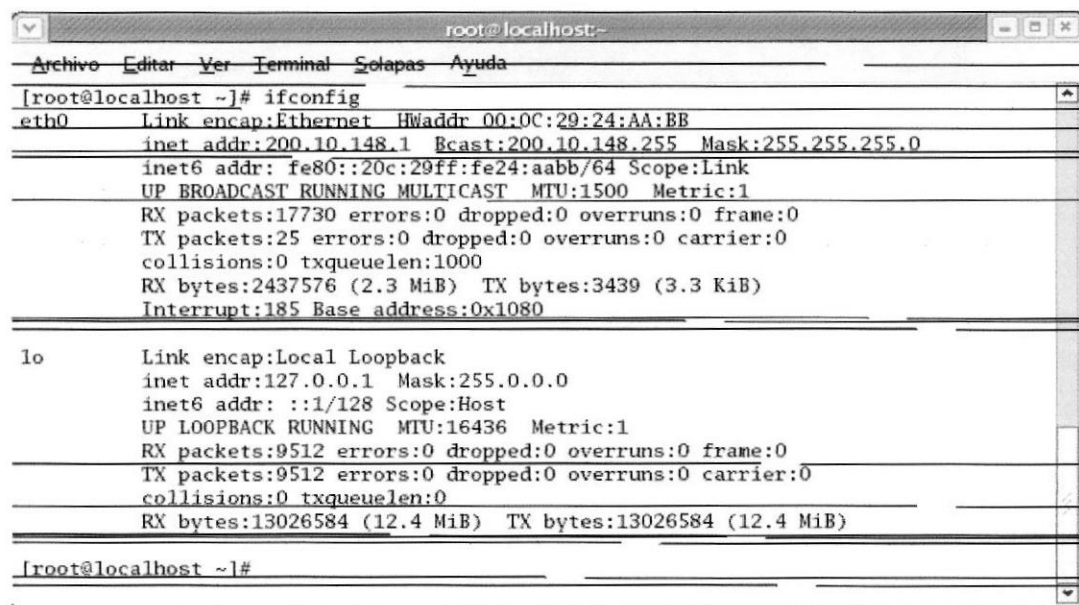
FIGURA 6 - 46: Editar el comando ifconfig

Se recomienda que una vez configurado la tarjeta de red, se deben reiniciar los servicios de red con el comando **service network restart**.



FIGURA 6 - 47: Reiniciar los servicios de la tarjeta red

Para verificar la ip en el servidor Linux se escribe el comando ifconfig el cual nos mostrara información de la tarjeta de red.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0C:29:24:AA:BB  
          inet addr:200.10.148.1  Bcast:200.10.148.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe24:aabb/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:17730 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:2437576 (2.3 MiB)  TX bytes:3439 (3.3 KiB)  
          Interrupt:185 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:9512 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:9512 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:13026584 (12.4 MiB)  TX bytes:13026584 (12.4 MiB)  
  
[root@localhost ~]#
```

FIGURA 6 - 48: Información de la tarjeta de red

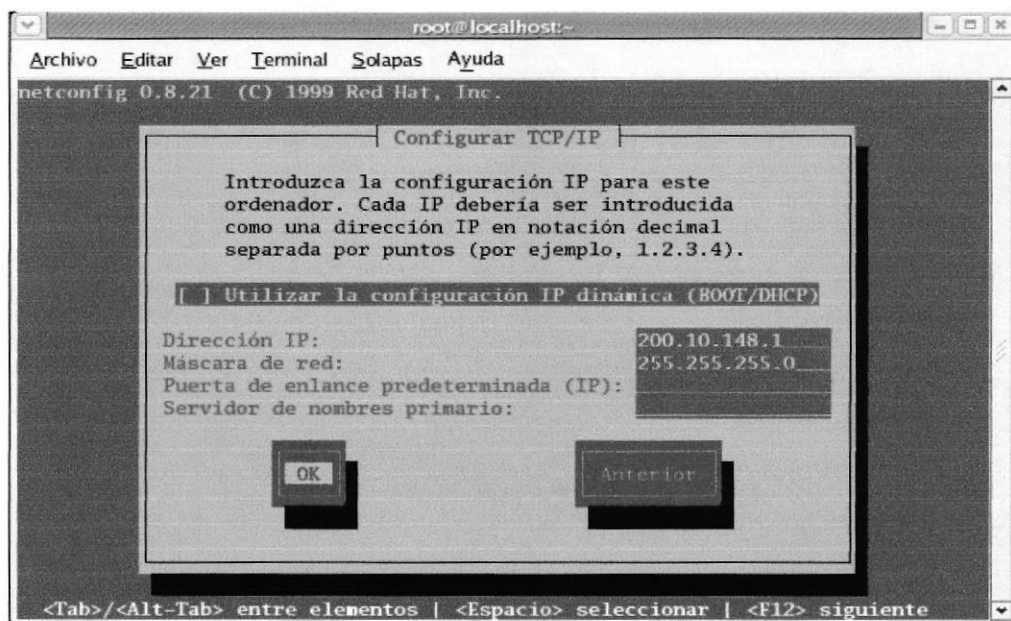
### 6.7.1.- CONFIGURACIÓN DE LA TARJETA DE RED MODO GRÁFICO

La segunda forma es escribiendo el comando netconfig, el cual mostrara una pantalla de confirmación para ingresar a configurar la tarjeta. En esta caso se selecciona el botón SI.



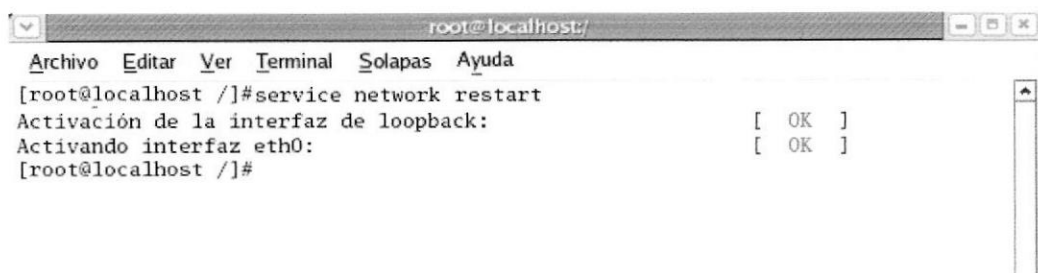
**FIGURA 6 - 49:** Configuración de la tarjeta de red

De esta manera se podrá asignar a la tarjeta de red una dirección IP, mascara de red, una puerta de enlace y un servidor DNS, para desplazarnos entre las opciones lo hara con la tecla Tab luego presiona el botón OK.



**FIGURA 6 – 50:** Configurar tcp/ip

Se recomienda que una vez configurado la tarjeta de red, se deben reiniciar los servicios de red con el comando **service network restart**.

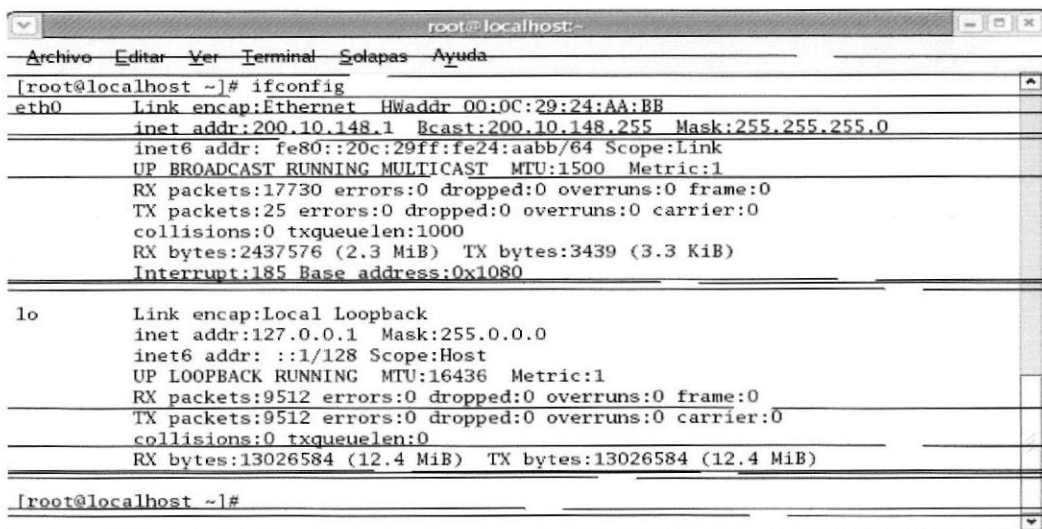


```

root@localhost:~# service network restart
Activación de la interfaz de loopback:      [ OK ]
Activando interfaz eth0:                    [ OK ]
root@localhost:~#
  
```

**FIGURA 6 – 51:** Levantar los servicios de la tarjeta de red

Para verificar la ip en el servidor Linux se escribe el comando **ifconfig** el cual mostrara información de la tarjeta de red.



```

root@localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:24:AA:BB
          inet addr:200.10.148.1  Bcast:200.10.148.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe24:aabb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17730 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2437576 (2.3 MiB)  TX bytes:3439 (3.3 KiB)
          Interrupt:185 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:9512 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9512 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:13026584 (12.4 MiB)  TX bytes:13026584 (12.4 MiB)

root@localhost:~#
  
```

**FIGURA 6 – 52:** Editar ifconfig (Verificar la ip del servidor)



## 6.8.- SAMBA SERVER

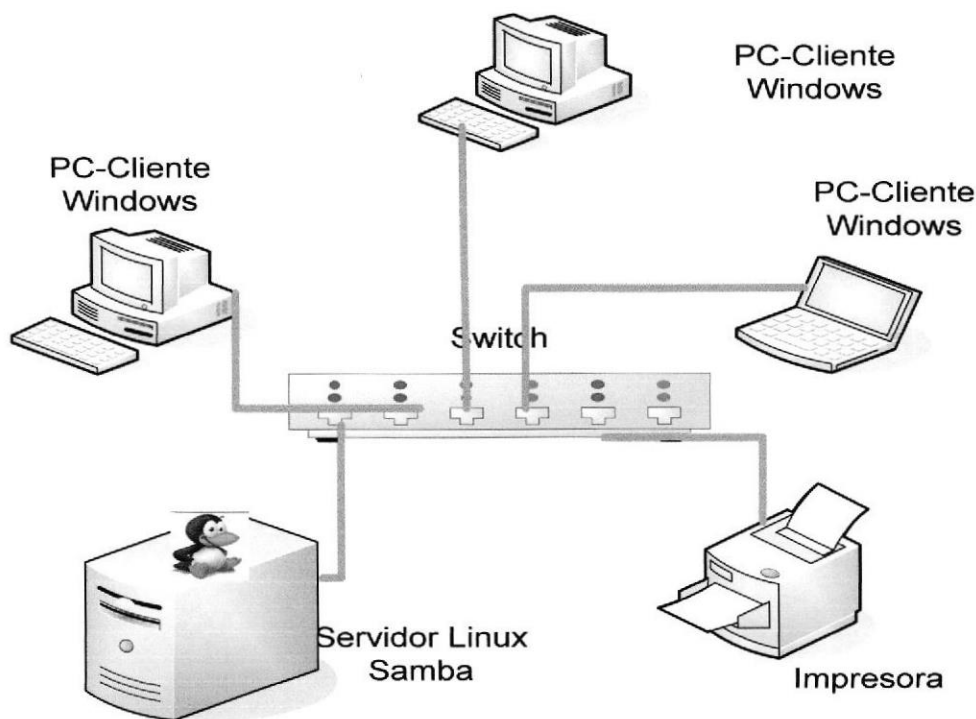


FIGURA 6 – 53: Samba

**Samba** son un conjunto de aplicaciones libres para Linux que implementan el protocolo de comunicación SMB utilizado por los sistemas operativos Microsoft Windows para compartir carpetas e impresoras.

Básicamente samba permite a PCs que utilizan Linux conectarse a carpetas compartidas en PCs con Windows y compartir carpetas como si de un Windows se tratara. Gracias a samba, en una red podemos tener PCs con Windows y PCs con Linux de forma que puedan intercambiar información en carpetas compartidas de la misma forma que se haría si todos los PCs fueran Windows.

Cuando en una misma red conviven sistemas Unix con equipos Windows, se utiliza samba para integrarlos y poder intercambiar información. Como alternativa, sería posible utilizar protocolos estándar como el ftp que es utilizado tanto equipos Windows como equipos Linux.'

Las funcionalidades de samba no se quedan solo en una simple compartición de archivos e impresoras sino que permite a un PC con Linux comportarse como un controlador de dominio de Windows para redes Microsoft con prestaciones superiores a las que nos ofrecería un servidor con Windows NT Server 4.0. En las páginas siguientes veremos como hacer que un PC con Linux haga las veces de controlador de dominio de nuestra red Windows.

**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`.

#### **6.8.1.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR SAMBA**

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener instalados los paquetes Samba
- Samba-2.2.1a
- Samba-client-2.2.1a



### 6.8.2.- CONFIGURACIÓN SAMBA SERVER

Para configurar un servidor samba se debe tener configurado la tarjeta de red y tener instalado el paquete del samba.

Se debe verificar si el paquete de Samba esta instalado, se lo verifica con el comando rpm -q samba.



```
root@localhost:/  
Archivo  Editar  Ver  Terminal  Solapas  Ayuda  
[root@localhost /]# rpm -q  samba  
samba-3.0.8-0.pre1.3_
```

**FIGURA 6 – 54:** Paquete Samba

Se controla desde el archivo /etc/samba/smb.conf y se edita el archivo de samba smb.conf



```
root@localhost:~  
Archivo  Editar  Ver  Terminal  Solapas  Ayuda  
[root@localhost ~]# vi /etc/samba/smb.conf
```

**FIGURA 6 – 55:** Ir al fichero samba



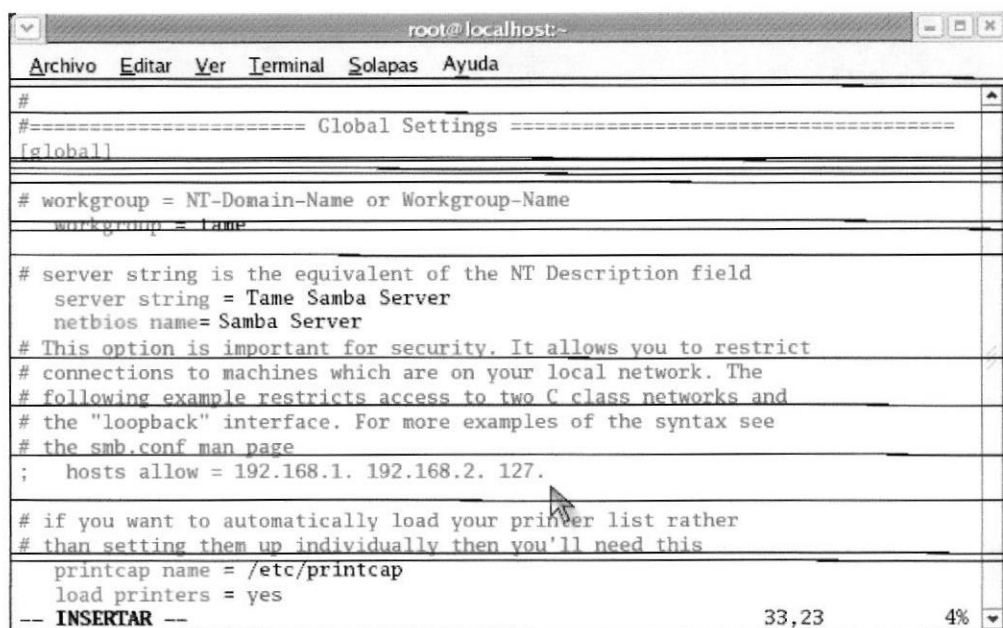
Una vez abierto el archivo de Samba se procede a editar las siguientes líneas:

### En la sección Global Settings.

Una vez dentro del archivo smb.conf, se ubicara en la sección de **GLOGAL SETTING** y se modifica las siguientes líneas.

**WORKGROUP:** Es aquel que nos permite elegir el tipo de grupo de trabajo vamos a trabajar en nuestro Servidor Samba.

**NETBIOSNAME:** Es aquel que nos permite definir el nombre de la maquina en este caso al momento de buscar la maquina lo se hará mediante el nombre que se agrega.



```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#
#===== Global Settings =====
[global]

# workgroup = NT-Domain-Name or Workgroup-Name
workgroup = Tame

# server string is the equivalent of the NT Description field
server string = Tame Samba Server
netbios name= Samba Server
# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
; hosts allow = 192.168.1. 192.168.2. 127.

# if you want to automatically load your printer list rather
# than setting them up individually then you'll need this
printcap name = /etc/printcap
load printers = yes
-- INSERTAR --                                     33,23      4%
```

FIGURA 6 – 56: Editando fichero smb.conf

**En la sección de Share Definitions**

Después de haber modificado la sección del GLOBAL SETTING, se ubicara en la última parte del archivo en la sección SHARE DEFINITION y se agrega las siguientes líneas tal como se muestra en la figura.

**PATH:** Es aquel que se permite definir en que directorio vamos a compartirlo.

**VALID USERS:** Es aquel que permite definir cual es el usuario que podrán acceder a nuestro servidor.

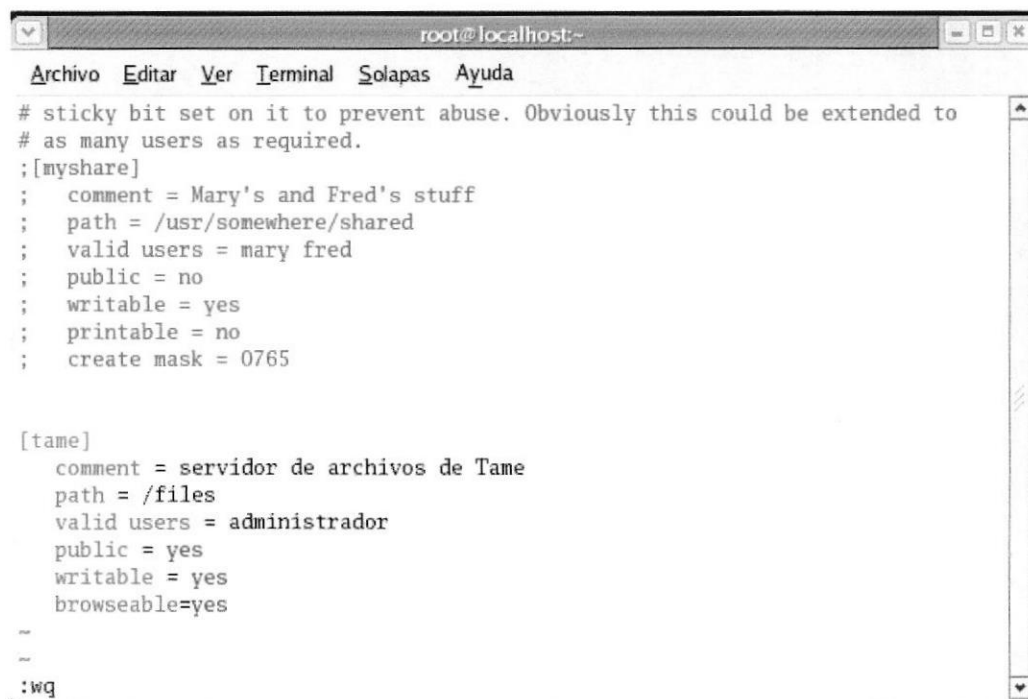
**WRITABLE:** Es aquel que permite que en el servidor podran tener acceso de escritura.

**COMMENT:** Nos permite agregar un comentario de nuestro Servidor en este caso Samba.

**PUBLIC:** Es aquel que permite que nuestro servidor sea publico.

**BROWSEABLE:** Es aquel que permite definir si el servidor sera visible para los usuarios, después de haber editado este archivo guardamos los cambios y salir con el comando: x

**ESC:** wq

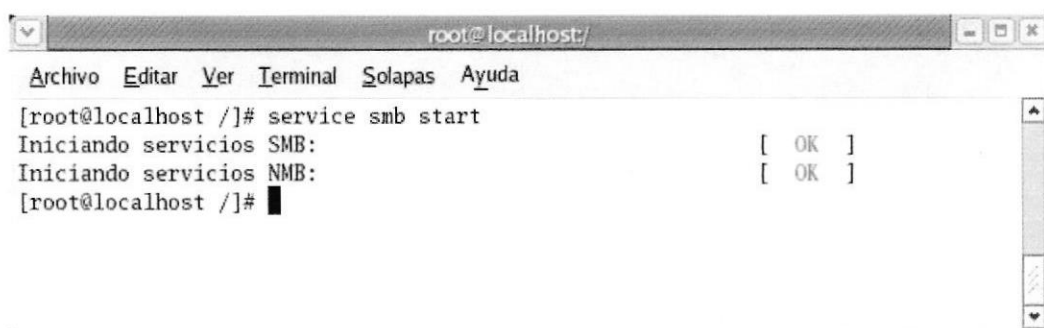


```
root@localhost:~
Archivo Editar Ver Terminal Solapas Ayuda
# sticky bit set on it to prevent abuse. Obviously this could be extended to
# as many users as required.
;[myshare]
;  comment = Mary's and Fred's stuff
;  path = /usr/somewhere/shared
;  valid users = mary fred
;  public = no
;  writable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

[tame]
  comment = servidor de archivos de Tame
  path = /files
  valid users = administrador
  public = yes
  writable = yes
  browseable=yes
~
:wq
```

**FIGURA 6 – 57:** Especificar valores Del directorio

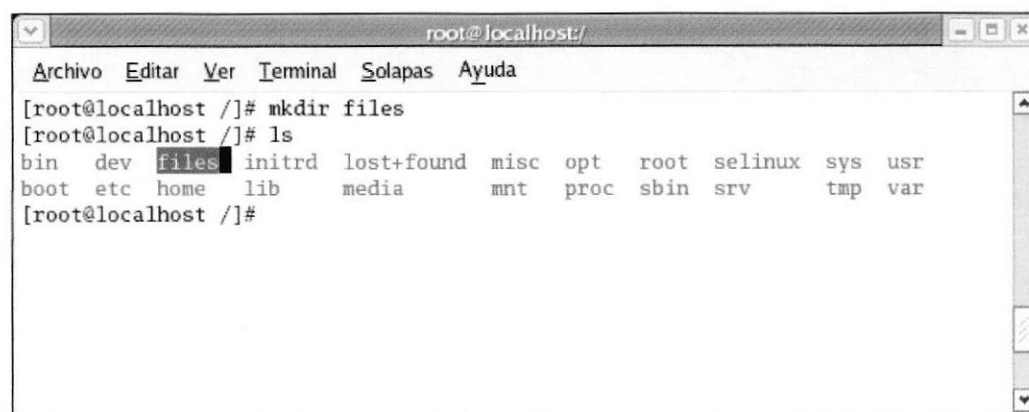
Para levantar el servicio de samba se hará con el comando `service smb start`.



```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# service smb start
Iniciando servicios SMB:                [ OK ]
Iniciando servicios NMB:                [ OK ]
[root@localhost /]#
```

FIGURA 6 – 58: Levantando servicio samba

Una vez guardados los cambios se procede a crear una carpeta la cual será compartida por el servidor samba.



```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# mkdir files
[root@localhost /]# ls
bin  dev  files  initrd  lost+found  misc  opt  root  selinux  sys  usr
boot  etc  home  lib    media      mnt   proc  sbin  srv    tmp  var
[root@localhost /]#
```

FIGURA 6 – 59: Creando el Recurso a Compartir

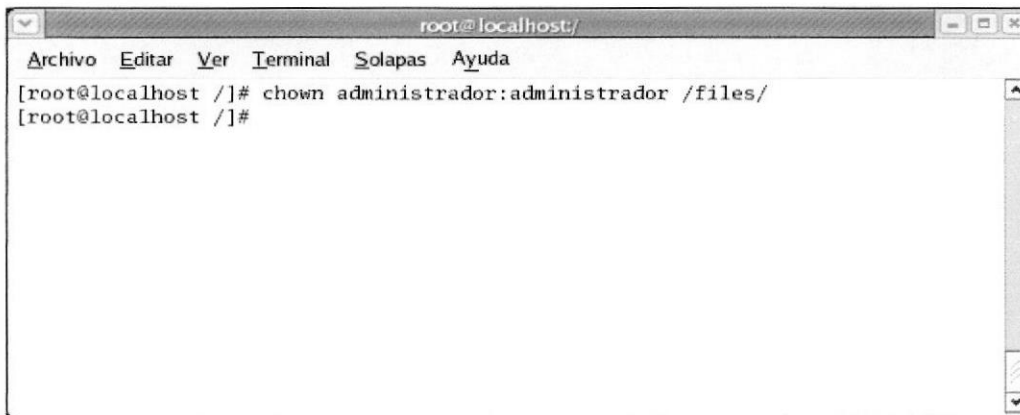
Luego se procederá a crear el usuario, el cual tendrá acceso al servidor samba, con el comando `adduser` para crear el **usuario** y `passwd` para dar la contraseña al usuario antes creado.



```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# adduser administrador
[root@localhost /]# passwd administrador
Changing password for user administrador.
New UNIX password:
BAD PASSWORD: it's WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@localhost /]#
```

FIGURA 6 – 60: Crear el usuario samba

Una vez creados los usuarios con sus respectivos password, se procede a cambiarlos de grupo y propietario.



**FIGURA 6 – 61:** Cambiando de Propietario

Después iniciar los servicios samba.



**FIGURA 6 - 62:** Levantar los servicios samba

6.9.- CONFIGURACIÓN EN EL CLIENTE WINDOWS

Se le asigna una dirección IP a la maquina Windows.

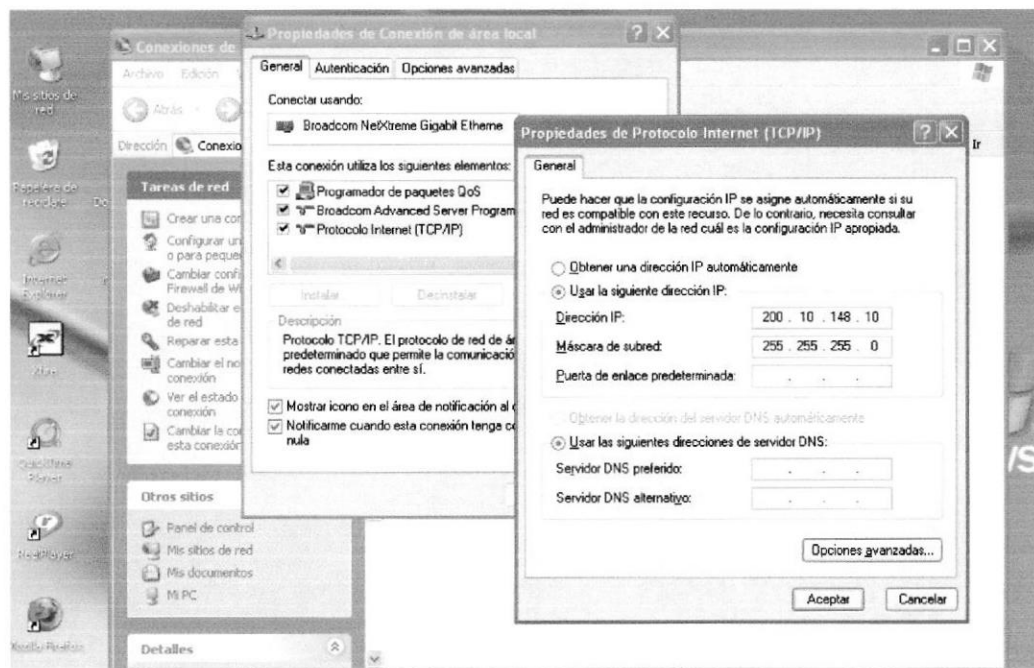


FIGURA 6 - 63: asignar dirección ip

Luego en el menú inicio, dar clic en ejecutar y se escribe la dirección IP del servidor samba.

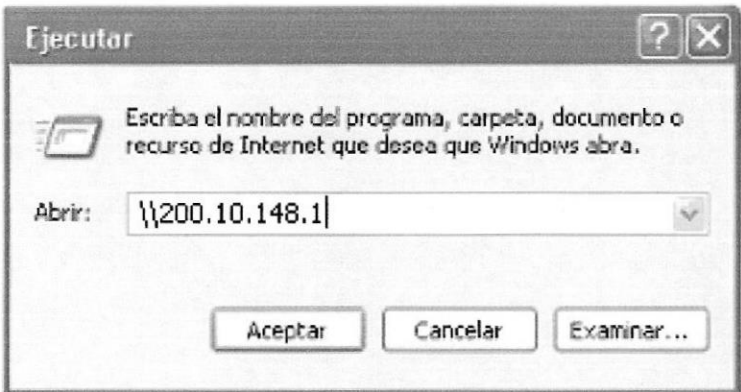
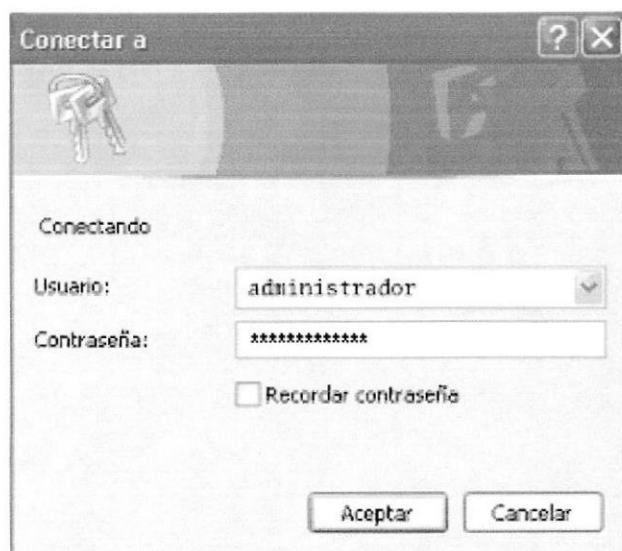


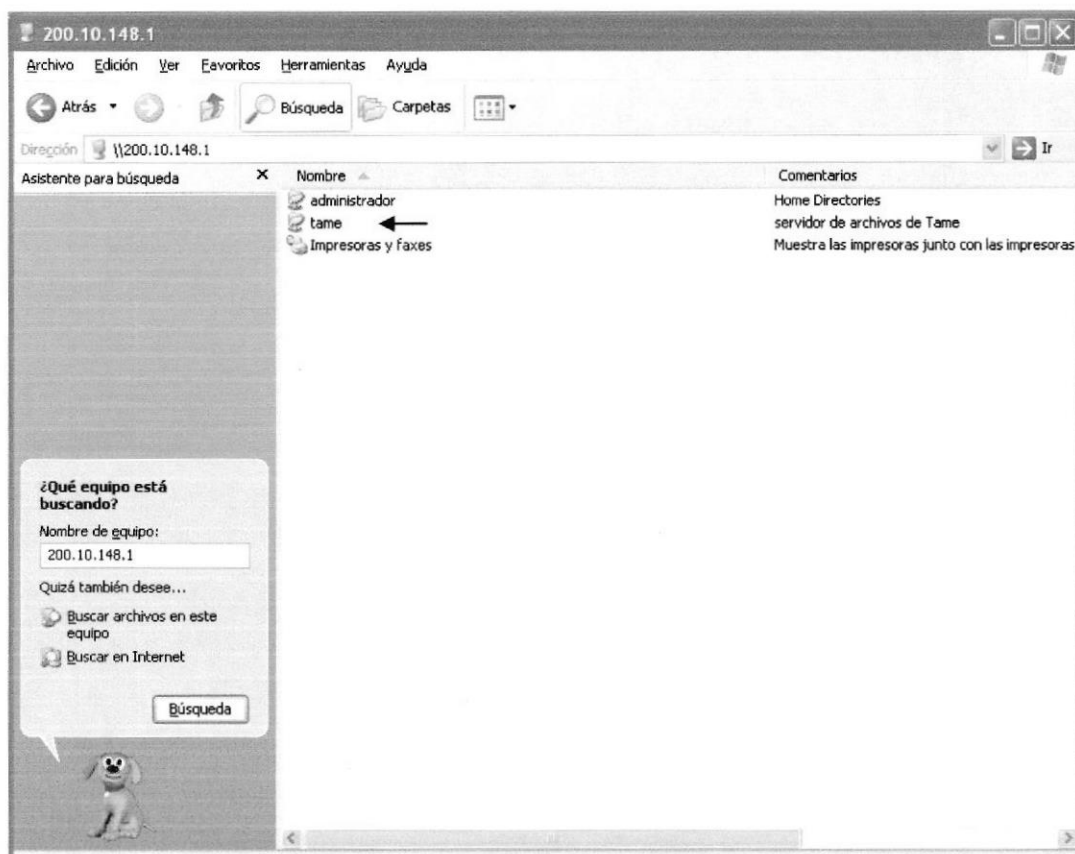
FIGURA 6 - 64: Buscando al servidor

Luego aparecerá una pantalla pidiendo el usuario y la contraseña del usuario que tendrán acceso al servidor, y se ingresa el usuario y la contraseña



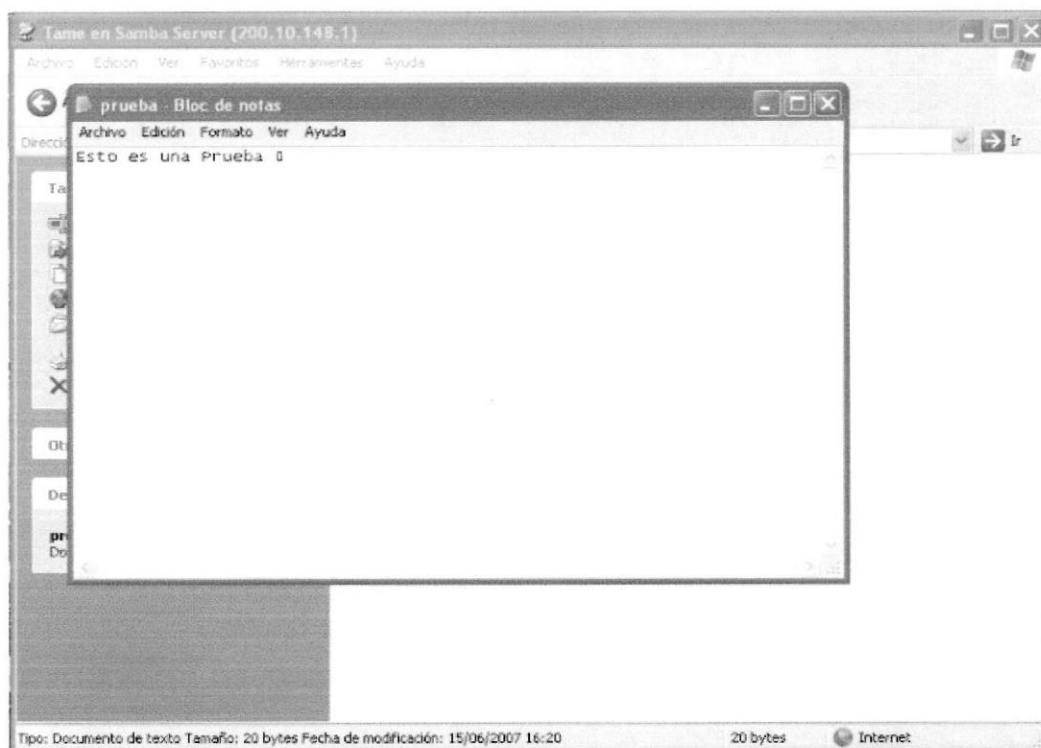
**FIGURA 6 - 65:** Conectado al servidor

Después se mostrara la carpeta compartida por el servidor samba.



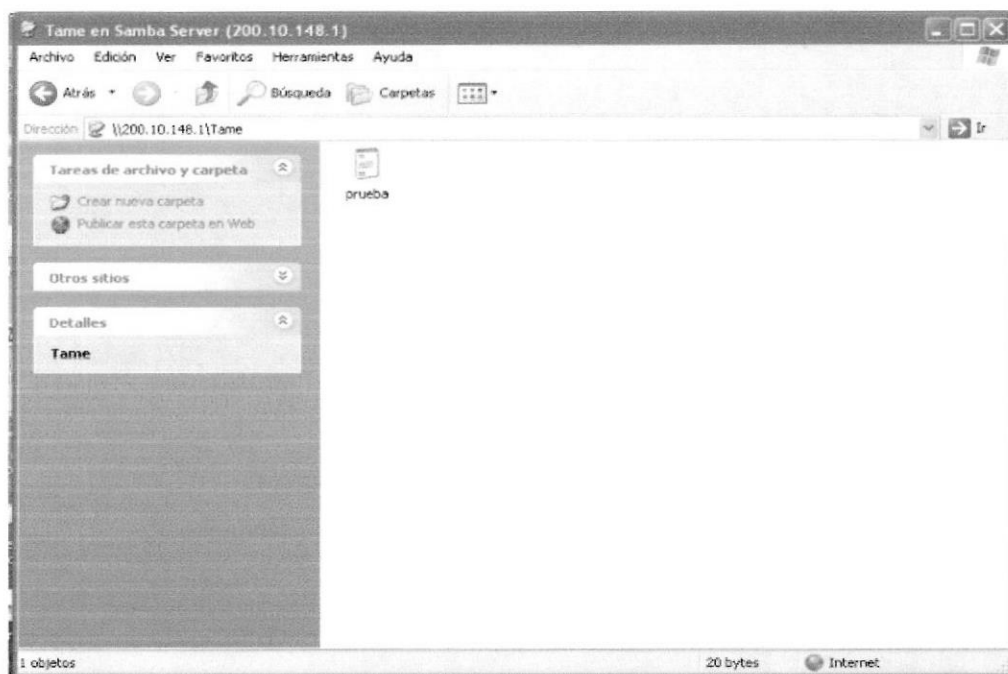
**FIGURA 6 - 66:** Ingresando al directorio

Luego se ingresará a la carpeta TAME compartida en el servidor samba



**FIGURA 6 - 67:** Abrir Archivo prueba

Después se ingresa a ver el archivo compartido en el servidor samba



**FIGURA 6 - 68:** Ver el archivo prueba

## 6.10.- CONFIGURACIÓN DNS SERVER

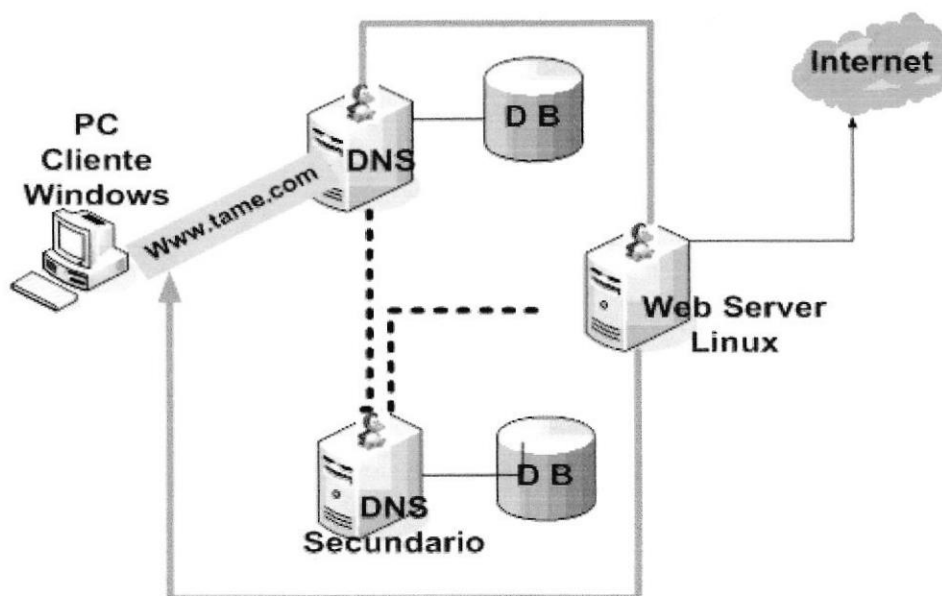


FIGURA 6 - 69: Servidor DNS

El DNS usa el concepto de espacio de nombres distribuido. Los nombres simbólicos se agrupan en zonas de autoridad, o más comúnmente, zonas. En cada una de estas zonas, uno o más hosts tienen la tarea de mantener una base de datos de nombres simbólicos y direcciones IP y de suministrar la función de servidor para los clientes que deseen traducir nombres simbólicos a direcciones IP. Estos servidores de nombres locales se interconectan lógicamente en un árbol jerárquico de dominios.

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

Un servidor de sistema de nombres de dominio (named).

Una biblioteca resolutoria de sistema de nombres de dominio.

Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

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

### DNS (Domain Name System).

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

Los Servidores DNS utilizan TCP y UDP en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud UDP desde un Cliente DNS seguida por una sola respuesta UDP del servidor. TCP interviene cuando el tamaño de



los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como transferencia de zonas.

**NIC (Network Information Center).**

**NIC** (acrónimo de Network Information Center o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genérico o por países, permitiendo personas o empresas montar sitios de Internet mediante a través de un ISP mediante un DNS. Técnicamente existe un NIC por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC MEXICO es la entidad encargada de gestionar todos los dominios con terminación .mx, la cual es la terminación correspondiente asignada a los dominios de México.

**FQDN (Fully Qualified Domain Name).**

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

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

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

Desde 2004, a solicitud de varios países de Europa, existe el estándar IDN (acrónimo de Internationalized Domain Name) que permite caracteres no-ASCII, codificando caracteres Unicode dentro de cadenas de bytes dentro del conjunto normal de caracteres de FQDN. Como resultado, los límites de longitud de los nombres de dominio IDN dependen directamente del contenido mismo del nombre.

**COMPONENTES DE UN DNS.**

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

**Cientes DNS.**

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

**Servidores DNS.**

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

**Servidor Maestro:** También denominado Primario. Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.

**Servidor Esclavo:** También denominado Secundario. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado transferencia de zona.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para la zona de DNS. De acuerdo al RFC 2182 el DNS requiere que al menos tres servidores existan para todos los dominios delegados (o zonas).

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

Contar con múltiples servidores también facilita la propagación de la zona y mejoran la eficiencia del sistema en general al brindar opciones a los Clientes DNS si acaso encontraran dificultades para realizar una consulta en un Servidor DNS. En otras palabras: tener múltiples servidores para una zona permite contar con redundancia y respaldo del servicio.

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

Los Servidores DNS responden dos tipos de consultas:

**Consultas Iterativas (no recursivas):** El cliente hace una consulta al Servidor DNS y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al Servidor DNS que tiene la Zona de Autoridad capaz de resolver la consulta.

**Consultas Recursivas:** El Servidor DNS asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el Cliente DNS. El Servidor DNS desarrolla entonces Consultas Iterativas separadas hacia otros Servidores DNS (en lugar de hacerlo el Cliente DNS) para obtener la respuesta solicitada.



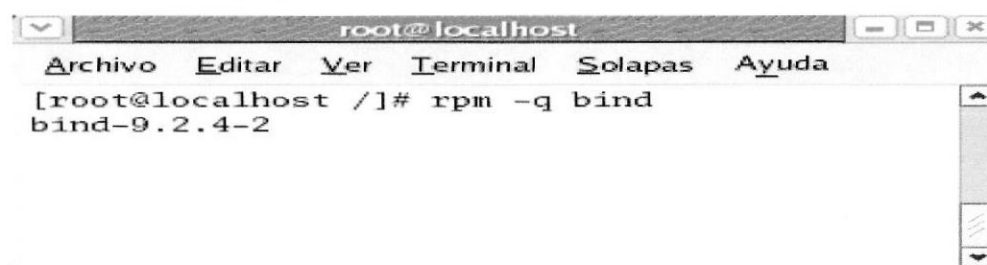
### 6.10.1.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR DNS

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener instalados los paquetes DNS
- -Bind
- -Bind-chroot

### 6.10.2.- CONFIGURACIÓN DEL SERVIDOR DNS

Para configurar un servidor DNS se debe tener configurado la tarjeta de red y tener instalado el paquete del bind.

Se debe verificar si el paquete del Bind esta instalado con el comando.



```
root@localhost
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost /]# rpm -q bind
bind-9.2.4-2
```

FIGURA 6 - 70: Verificando paquetes DNS

Una vez dentro del archivo del named.conf se agregara las siguientes líneas para levantar nuestro dominio.

**zone "TAME.com" IN {**: Es el nombre del dominio o la zona.

**TYPE MASTER:** Tipo de la Zona, en este caso zona principal.

**File "TAME.com.zone"**: Es el nombre del archivo que se va a editar.

**ALLOW-UPDATE {none;}**

: Es el que permite actualizar la zona.



```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda

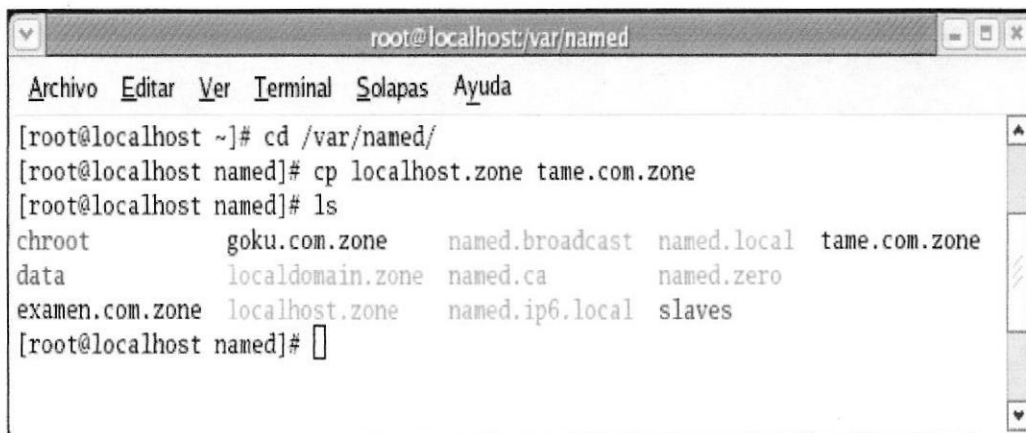
};

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

include "/etc/rndc.key";
~
~
~
80,1      Final
```

FIGURA 6 - 71: Creando las Zonas

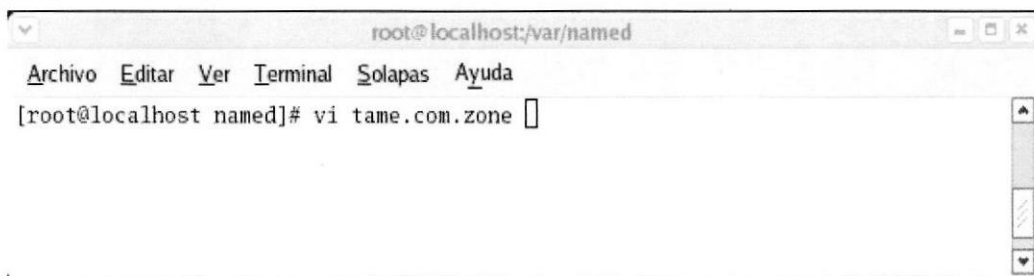
Cuando se termino de editar el archivo del bind, se procede a buscar y copiar el archivo del localhost.zone. Este archivo se lo renombra con el nombre de la zona creada en el bind.



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

**FIGURA 6 - 72:** Copiar el archivo localhost.zone

Una vez renombrado el archivo del localhost.zone, con nuestro dominio se procede a editar dicho archivo.



```
root@localhost:/var/named
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost named]# vi tame.com.zone
```

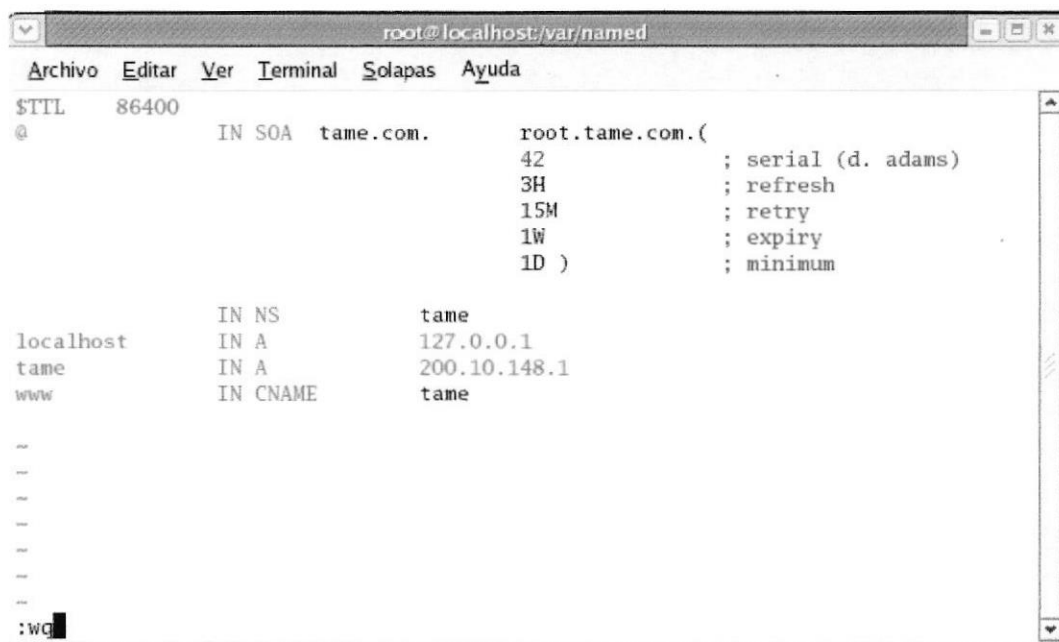
**FIGURA 6 - 73:** Ingresar a la ruta vi TAME.com.zone

**SOA (Start of Authority):** Registro de inicio de autoridad que especifica el Servidor DNS Maestro (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.

**NS (Name Server):** Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio.

**A (Address):** Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IP.

**CNAME (Canonical Name):** Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los sub-dominios y registros DNS del dominio original.



```


root@localhost:/var/named
Archivo Editar Ver Terminal Solapas Ayuda
$TTL      86400
@          IN SOA  tame.com.      root.tame.com. (
                        42          ; serial (d. adams)
                        3H          ; refresh
                        15M         ; retry
                        1W          ; expiry
                        1D )         ; minimum

localhost  IN NS   tame
localhost  IN A    127.0.0.1
tame       IN A    200.10.148.1
www        IN CNAME tame
:wg

```

**FIGURA 6 -74:** Editar la zona

Luego de haber editado este archivo y procedo a guardar los cambios y a copiarla en el siguiente directorio.



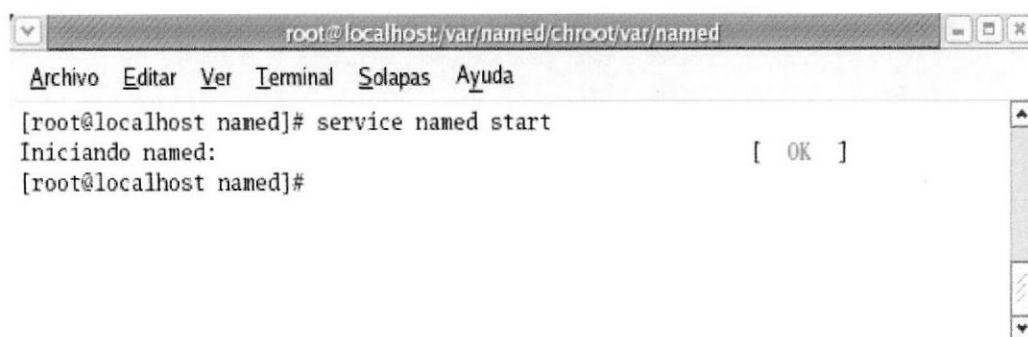
```

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

```

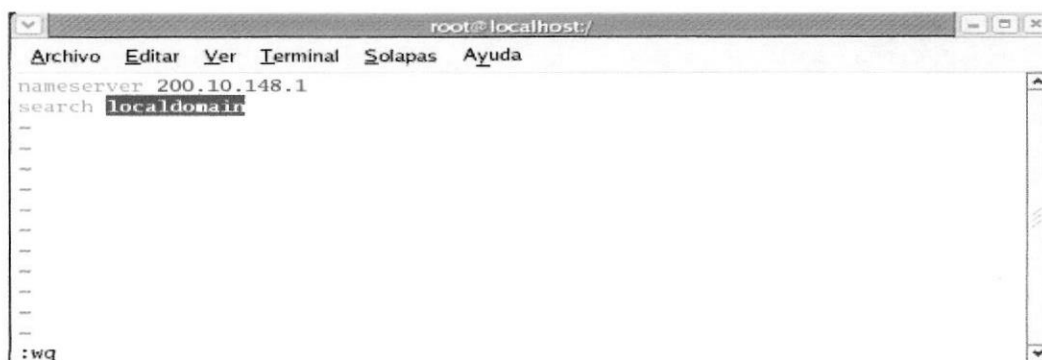
**FIGURA 6 - 75:** Copiando las zonas

Una vez hecho esto se procederá a levantar los servicios del bind con el siguiente comando.



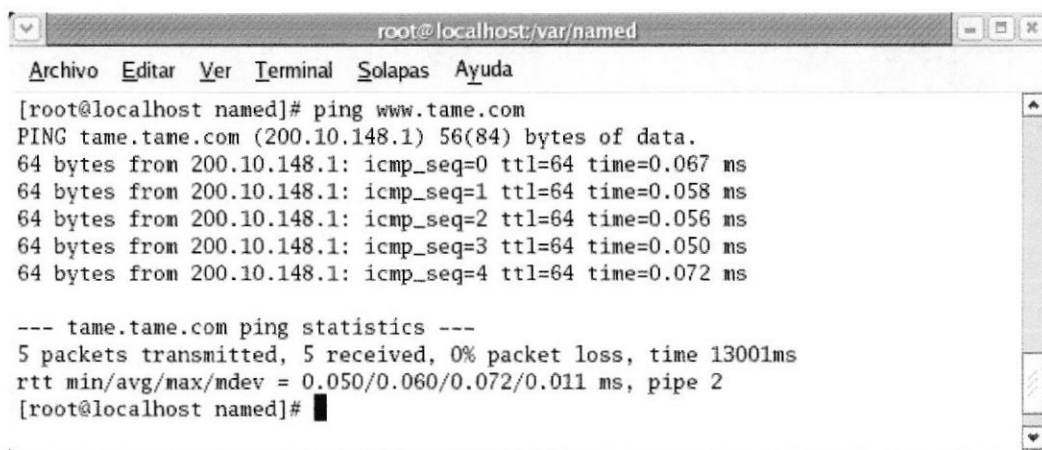
### FIGURA 6 - 76: Levantando servicios DNS

Se realizara en este archivo es una línea del HOSTNAME= localhost el cual lo se remplazara por HOSNAME= TAME.com



**FIGURA 6 - 77:** Agregar dirección al name server

Luego de esto se verificara que el nombre del dominio este bien levantado, haciéndole un ping a la dirección, ping [www.tame.com](http://www.tame.com).

**FIGURA 6 - 78:** Ping a la zona [www.tame.com](http://www.tame.com)

### 6.10.3.- CONFIGURACIÓN EN EL CLIENTE WINDOWS

Se le asigna una dirección IP y el DNS a la maquina Windows.

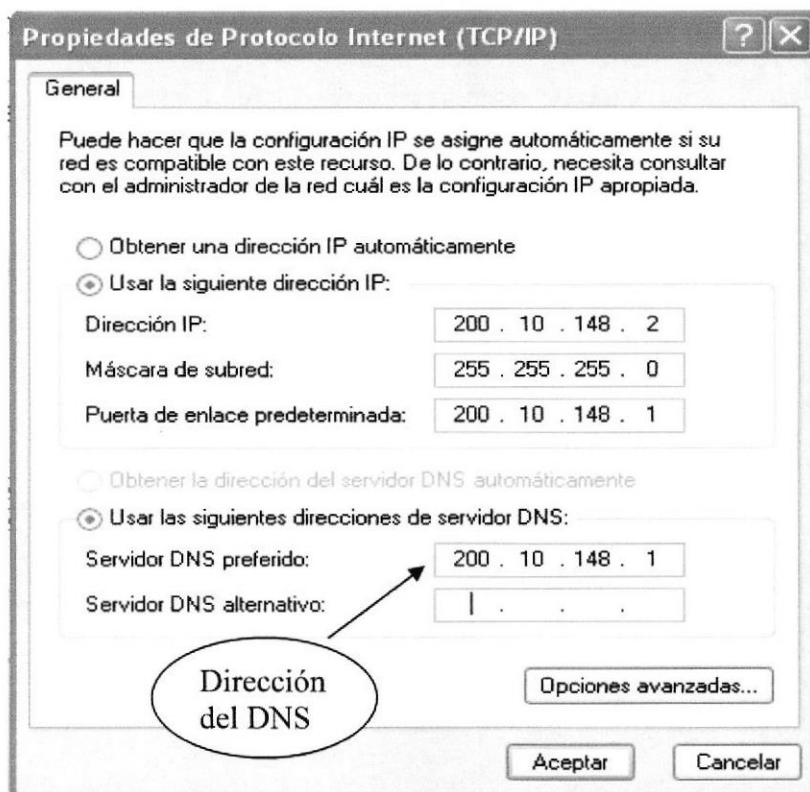


FIGURA 6 - 79: Asignar dirección del Servidor DNS

Hacer ping desde el cliente al servidor

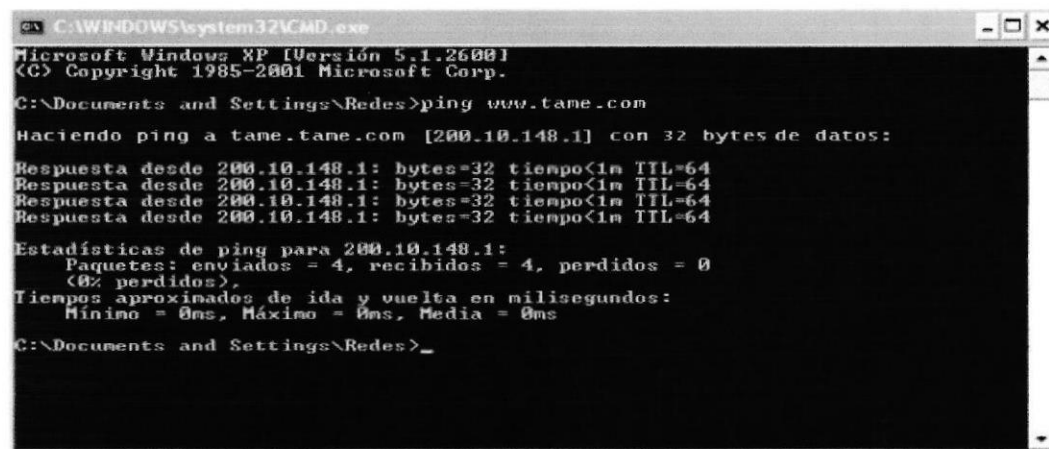
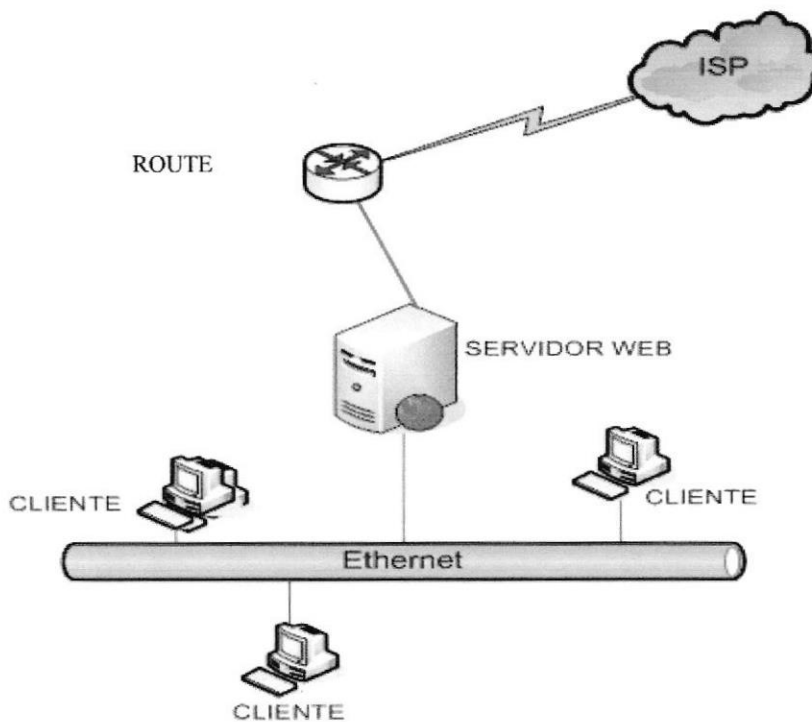


FIGURA 6 - 80: Hacer ping al servidor DNS



## 6.11.- CONFIGURACIÓN WEB SERVER



**FIGURA 6 - 81:** Servidor Web

Básicamente, un servidor Web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).

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).

**VERSATILIDAD En GNU/Linux**, no se está atado a un solo servidor Web. Desde el popular Apache (utilizado por más del 65 % de los servidores Web de todo el mundo) hasta servidores web basados en Java como Tomcat, pueden ser configurados dependiendo de la necesidad. Esto quiere decir que el servidor Web se adapta a su aplicación y necesidades y no al revés.

### CONFIABILIDAD

Un servidor Web bien programado y configurado, sobre una plataforma estable, conjugan para que la estabilidad y confiabilidad de un servidor Web Linux sean insuperables. Meses o años. Ese es el tiempo que puede llegar a estar corriendo el servidor sin necesidad de reiniciar y sin fallas.



**SEGURIDAD** La palabra clave en servidores Web, especialmente si corre sitios de e-commerce o maneja información valiosa. El servidor web Apache, a pesar de ser el más ampliamente utilizado, registra muchos menos incidentes de seguridad por año que su principal competidor propietario (IIS), el cual a pesar de poseer menor cuota de mercado registra las mayores fallos de seguridad.

### **ECONOMÍA**

Instalar un servidor Web Linux no sólo es más económico desde el punto de vista de la inversión inicial. El hecho de que requiera muy poco mantenimiento (si no es nulo) abarata costos y de que sea más seguro y confiable también ayuda a reducir el presupuesto, ya que el servidor nunca está off-line, evitando pérdidas de dinero. Además, al ser el rendimiento superior (y atender a más usuarios) se evitan actualizaciones de hardware y software.

### **ACERCA DE APACHE**

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

#### **6.11.1.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR WEB**

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener levantado previamente el dominio DNS.
- Tener habilitado los servicios necesarios (httpd).

Para configurar un servidor web se debe tener configurado la tarjeta de red y tener instalado el paquete del apache.

Se debe verificar si el paquete del apache esta instalado con el comando.



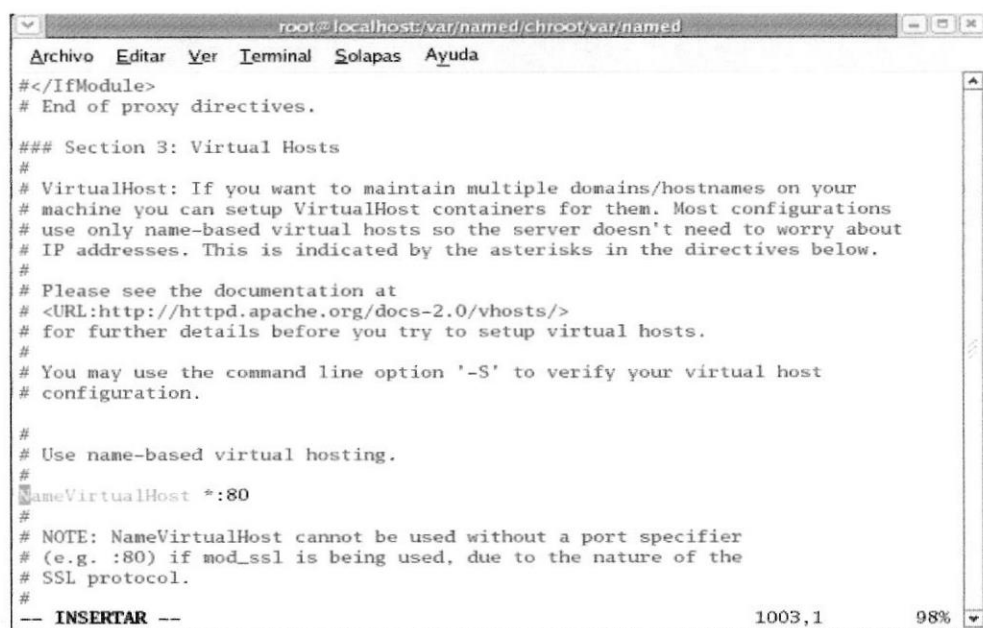
**FIGURA 6 - 82:** Verificamos paquete httpd

Se buscara el archivo de configuración del apache, que se encuentra en el directorio /etc/httpd/conf/httpd.conf. Y se editara las siguientes líneas.



**FIGURA 6 - 83:** Editando Httpd.conf

Una vez encontrado el archivo del apache, se procederá a buscar y descomentar la línea del NameVirtualHost \*:80.



```

root@localhost:/var/named/chroot/var/named
Archivo Editar Ver Terminal Solapas Ayuda
#</IfModule>
# End of proxy directives.

### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs-2.0/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
#
# 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.
#
-- INSERTAR --
1003,1 98%

```

FIGURA 6 - 84: Habilitando varias zonas

Luego de haber ingresado al archivo httpd.conf, se ubicara en la

En la sección del <VirtualHost \*:80> se debe cambiar la siguientes líneas.

Ultima parte del archivo y se procederá a agregar las siguientes líneas.

**ServerAdmin:** Es aquel donde se especifica el nombre del equipo y del usuario.

**DocumentRoot:** Es aquel donde se crea la carpeta en donde se va alojar nuestro sitio Web de prueba.

**ServerName:** En esta línea se especifica la dirección de dominio DNS.



```

root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
#<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/web
    ServerName www.tame.com
</VirtualHost>
~
:wq

```

FIGURA 6 - 85: Ruta del sitio Web

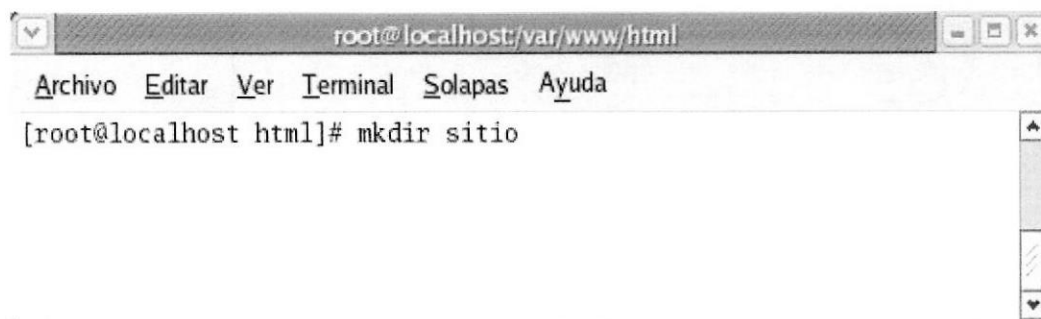


Después de haber agregado las líneas de configuración en el archivo httpd.conf, procedemos a crear el directorio al cual va a contener nuestro sitio Web en la siguiente ruta.



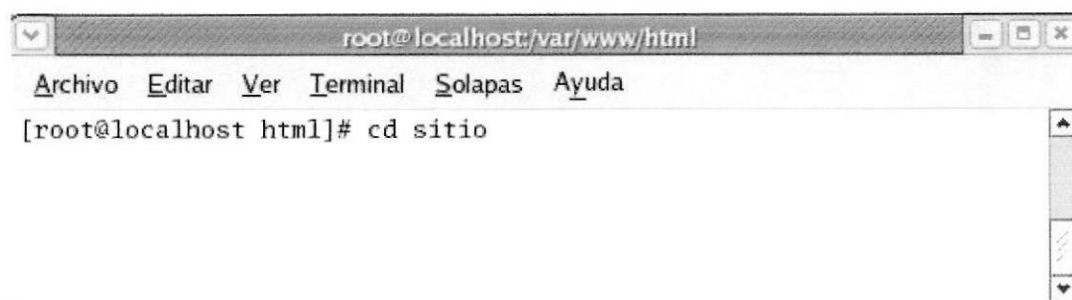
**FIGURA 6 - 86:** Ingresando al directorio html

Después de ingresar a la ruta donde se alojara nuestro sitio Web se crea un directorio con el comando mkdir.



**FIGURA 6 - 87:** Creando el directorio de nuestra página

Una vez creado nuestro directorio se procede a ingresar para crear nuestra página de prueba.



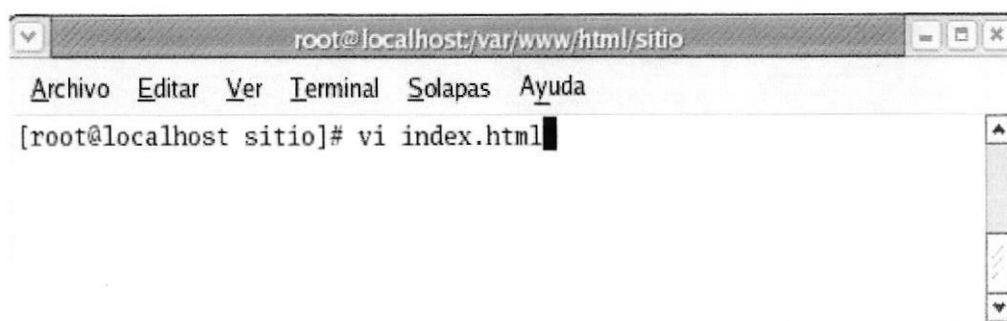
**FIGURA 6 - 88:** Ingresando al directorio de nuestra página

Luego se crea un archivo con el nombre index.html el cual será nuestra pagina de prueba.



**FIGURA 6 - 89:** Creando un archivo de prueba

Luego se procederá a editar dicho archivo con el comando vi.



**FIGURA 6 - 90:** Editando el archivo de prueba html

Después de haber hecho esto, se deberá editar el archivo index.html, y le se agrega algún mensaje para mostrar en el navegador web.



**FIGURA 6 - 91:** Creando un mensaje de prueba html

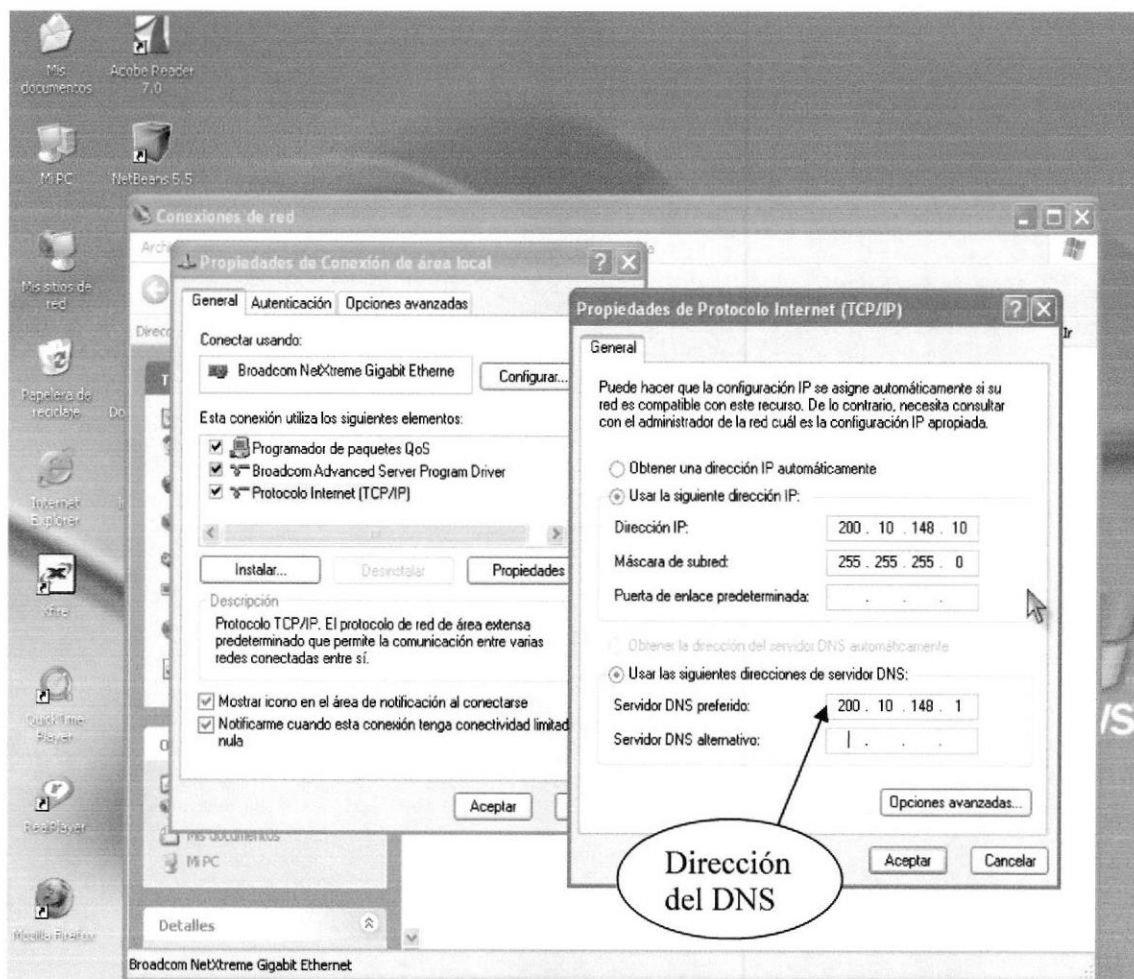
Para levantar el servicio apache con el comando `service httpd start`.



**FIGURA 6 - 92:** Iniciando servicios httpd

### 6.11.2.- CONFIGURACIÓN EN EL CLIENTE WINDOWS

Se le asigna una dirección IP a la maquina Windows y se le asigna la dirección del DNS preferido, el cual la dirección del DNS es la ip del servidor web.



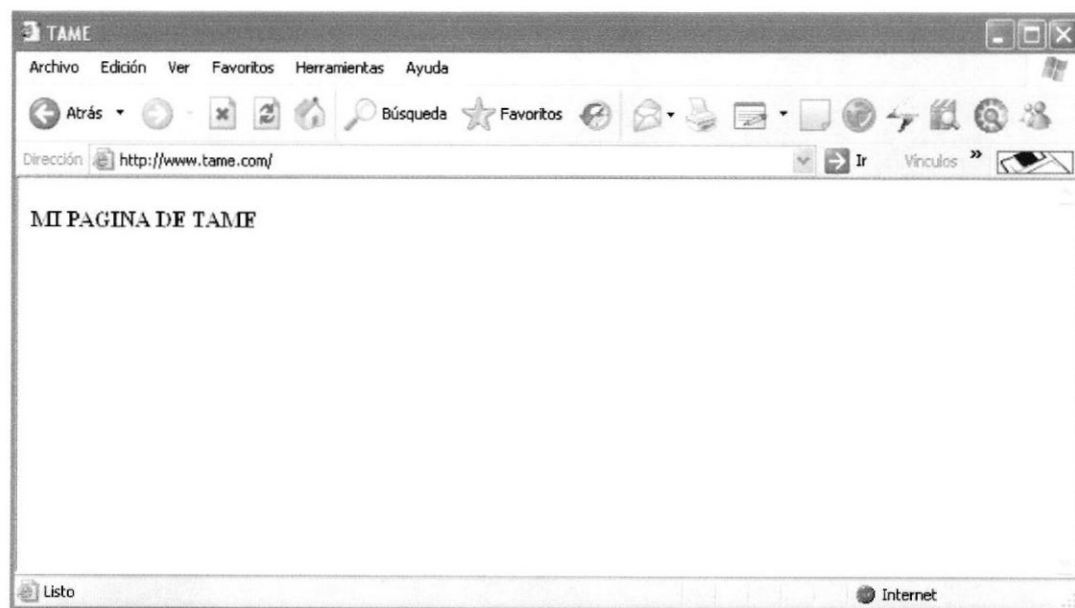
**FIGURA 6 - 93:** Verificando la ip del servidor DNS

Para realizar la prueba en el cliente Windows dar doble clic sobre el icono de Internet Explorer.



**FIGURA 6 - 94:** Abrir el Internet Explorer

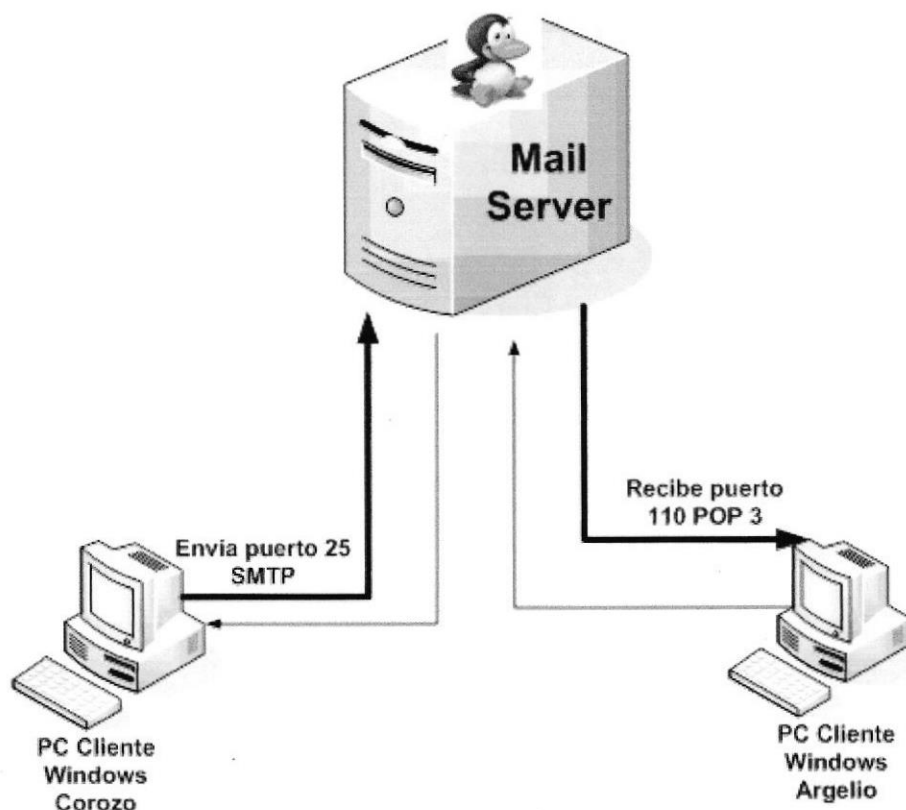
Luego de haber asignado una dirección IP y un DNS al cliente, abrir el navegador web y escribires el nombre de nuestro dominio.



**FIGURA 6 - 95:** Prueba exitosa del Web Server



## 6.12.- CONFIGURACIÓN MAIL SERVER



**FIGURA 6 - 96: Sendmail**

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.

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

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

**SMTP**, Simple Mail Transfer Protocol: Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

**POP**, Post Office Protocol: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

**IMAP**, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Mail Server es un servidor de mail POP3 y SMTP que soporta un número ilimitado de dominios, casillas de mail, y listas de correo.

**POP3** (Post Office Protocol versión 3) Es un protocolo estándar de Internet del Nivel de Aplicación que recupera el correo electrónico desde un servidor remoto a través de una conexión TCP/IP desde un cliente local. El diseño de POP3 y sus predecesores es

permitir a los usuarios recuperar el correo electrónico al estar conectado hacia una red y manipular los mensajes recuperados sin necesidad de permanecer conectados. A pesar de que muchos clientes de correo electrónico incluyen soporte para dejar el correo en el servidor, todos los clientes de POP3 recuperan todos los mensajes y los almacenan como mensajes nuevos en la computadora o anfitrión utilizado por el usuario, eliminan los mensajes en el servidor y terminan la conexión.

**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.

**Versatilidad** Desde pequeñas oficinas a grandes empresas, en GNU/Linux hay un servidor de correo para cada necesidad y presupuesto, manteniendo siempre una excelente calidad.

**Confiabilidad** "No se cae". Eso es lo que le responde un Administrador de Sistema satisfecho luego de unos pocos meses de probar un servidor de correo corriendo sobre GNU/Linux. Siendo usualmente éste uno de los servicios más castigados, la confiabilidad es fundamental.

**Seguridad** IMAP/POP con SSL, SMTP autenticado, claves encriptadas con CRAM-MD5, DIGEST-MD5, Kerberos, NT-Login o POP-before-SMTP.

Lo que quiera en materia de seguridad y control de relay puede ser realizado, siempre con el máximo rendimiento.

**Rapidez** En un servidor de correo, la rapidez es fundamental. Largas colas de mensajes pueden saturar hasta el más potente de los servidores. Por eso, los servidores de correo más grandes del mundo utilizan plataformas basadas en GNU/Linux.

**Economía** Menor costo de instalación, menor costo de mantenimiento y menor costo medio por usuario (debido a que atiende más usuarios por equipo) hacen de los servidores de correo basados en GNU/Linux la mejor opción.

### **6.12.1.- REQUERIMIENTOS PARA CONFIGURAR UN SENDMAIL**

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener habilitado los puertos 110 y 25

### 6.12.2.- CONFIGURACIÓN DEL SERVIDOR SENDMAIL

Para configurar un servidor de correos se deberá tener configurado la tarjeta de red y tener instalado el paquete del sendmail.

Se debe verificar si el paquete del sendmail esta instalado con el comando.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# rpm -q sendmail  
sendmail-8.13.1-2  
[root@localhost ~]#
```

FIGURA 6 - 97: Verificamos paquete de sendmail

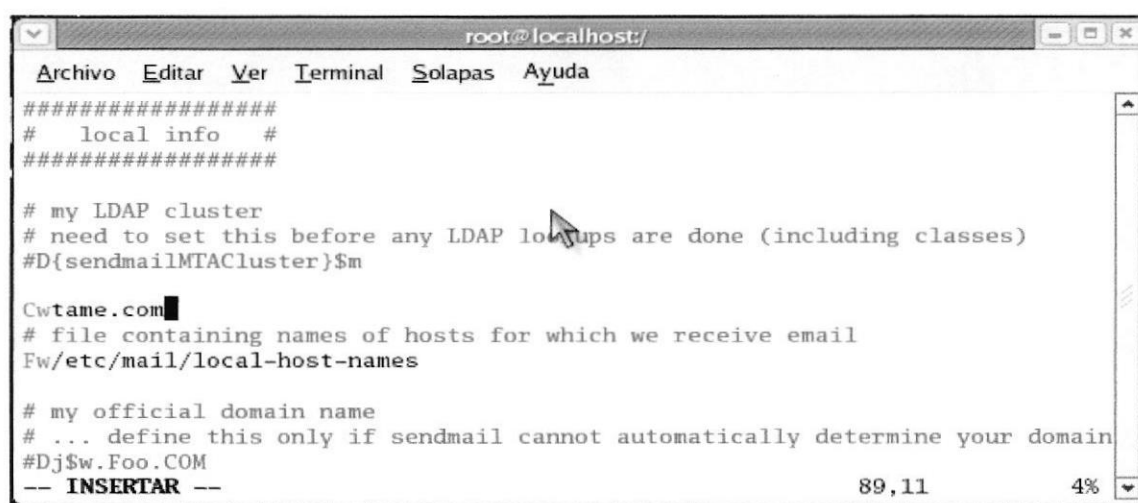
Se buscara el archivo de configuración del sendmail, que se encuentra en el directorio /etc/mail/sendmail.cf.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# vi /etc/mail/sendmail.cf
```

FIGURA 6 - 98: Ingresamos a la ruta vi /etc/mail/sendmail.cf

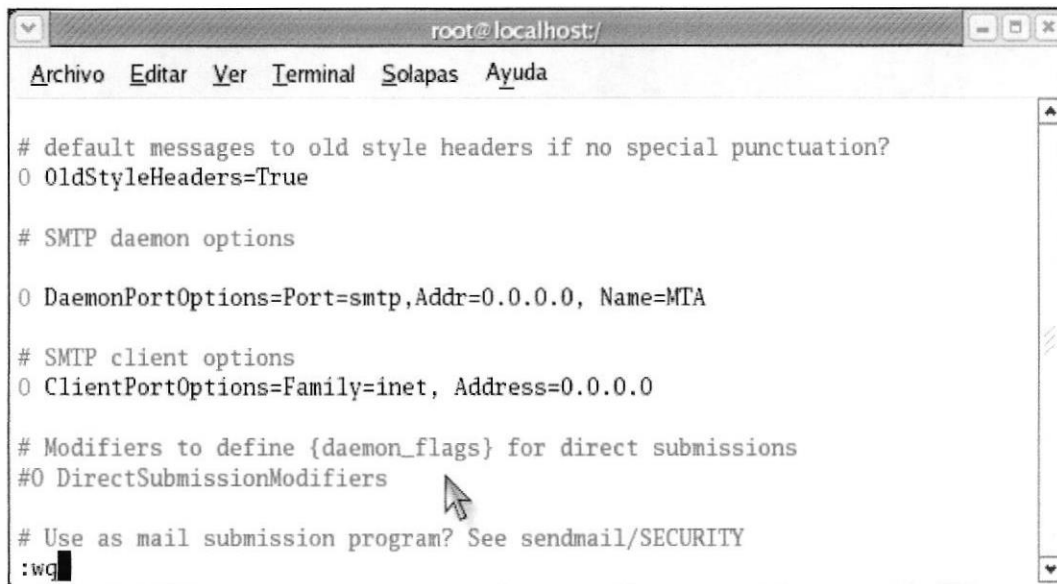
Luego de esto se edita la línea del Cw y le agrega el nombre de nuestro dominio.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
#####  
# local info #  
#####  
  
# my LDAP cluster  
# need to set this before any LDAP lookups are done (including classes)  
#D{sendmailMTACluster}$m  
  
Cwtame.com  
# file containing names of hosts for which we receive email  
Fw/etc/mail/local-host-names  
  
# my official domain name  
# ... define this only if sendmail cannot automatically determine your domain  
#Dj$w.Foo.COM  
-- INSERTAR --  
89,11 4%
```

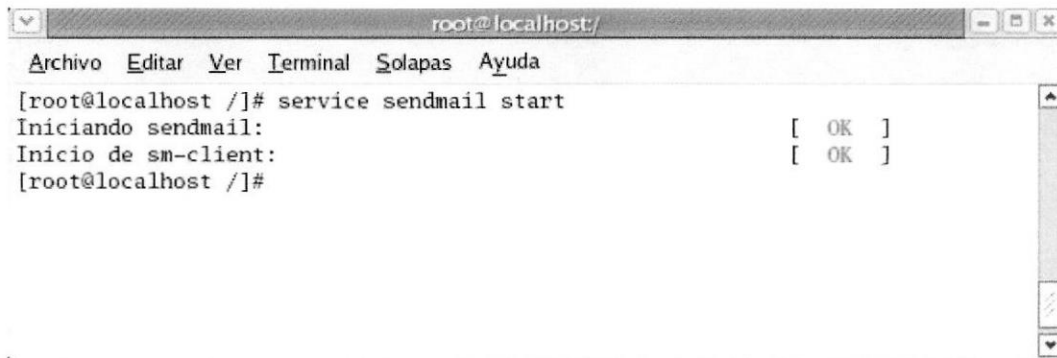
FIGURA 6 - 99: Agregando los parámetros

Luego en la sección del SMTP daemon options y SMTP client options se edita esas líneas como se muestra a continuación.



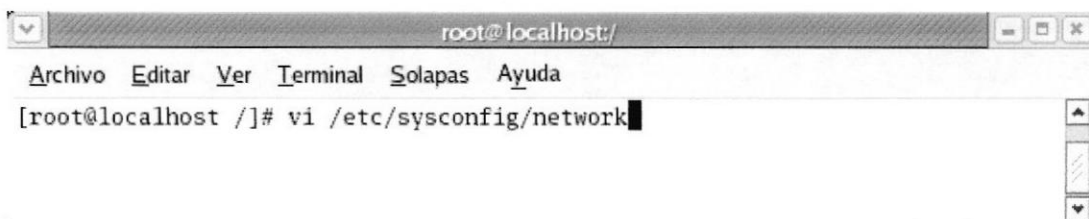
**FIGURA 6 - 100:** Modificando los SMTP

Una vez hecho esto se procede a levantar los servicios del sendmail con el siguiente comando.



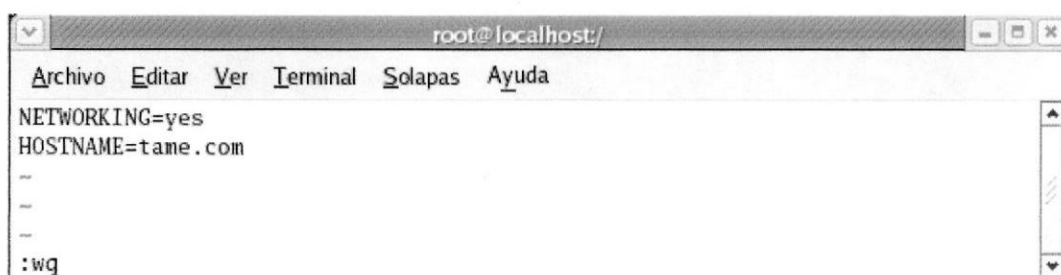
**FIGURA 6 - 101:** Iniciando servicios sendmail

Si todo salió bien, se procederá a buscar y editar el archivo del network



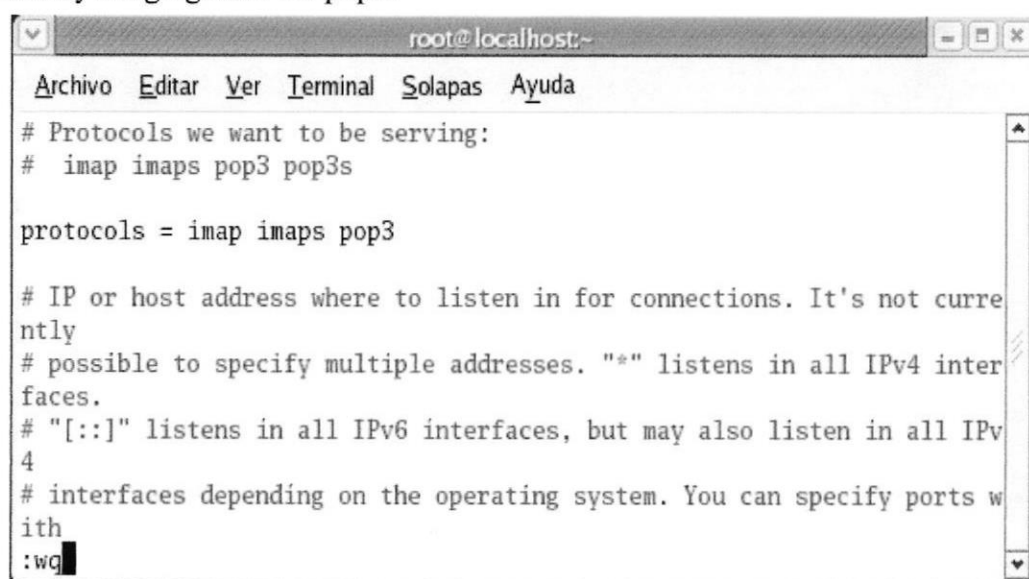
**FIGURA 6 - 102:** Edición Archivo Network

En este archivo se agrega la línea HOSTNAME y el nombre de nuestro dominio.



**FIGURA 6 - 103:** Editar Fichero Network

Luego, se procederá a buscar y editar el archivo del dovecot y se habilita la línea del protocols y la agregamos del pop3.



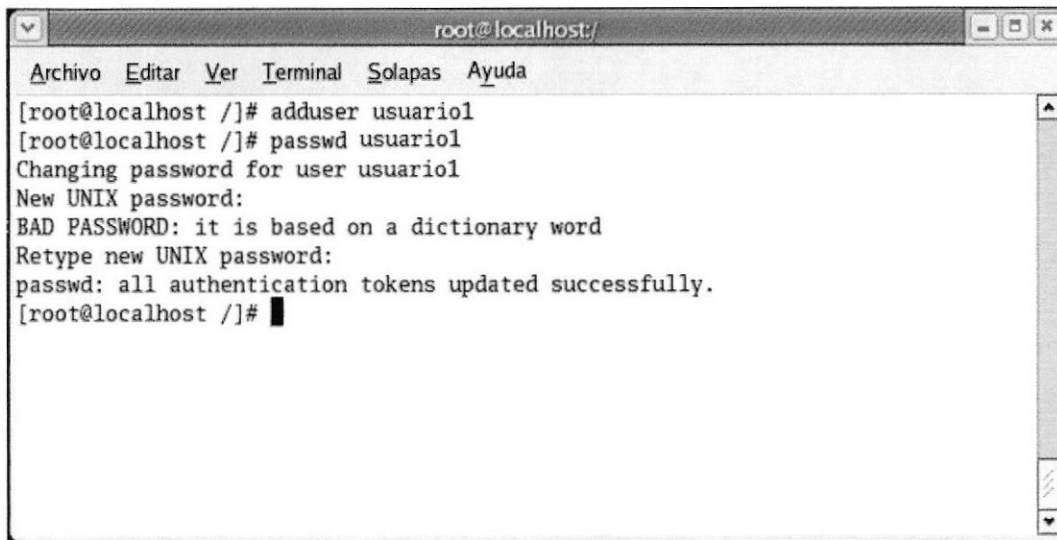
**FIGURA 6 - 104:** Ingresar parámetros

Una vez hecho esto se procede a levantar los servicios del dovecot con el siguiente comando.



**FIGURA 6 - 105:** Iniciar servicios dovecot

Para poder probar el sendmail deberás crear cuentas de usuarios.

A screenshot of a terminal window titled 'root@localhost:/' with standard window controls. The terminal shows the execution of the 'adduser' command to create a user named 'usuariol'. It then prompts for a password, which is rejected as being based on a dictionary word. After re-entering a password, it confirms that all authentication tokens have been updated successfully.

```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# adduser usuariol  
[root@localhost /]# passwd usuariol  
Changing password for user usuariol  
New UNIX password:  
BAD PASSWORD: it is based on a dictionary word  
Retype new UNIX password:  
passwd: all authentication tokens updated successfully.  
[root@localhost /]#
```

**FIGURA 6 - 106:** Crear cuentas de usuarios

### 6.12.3.- CONFIGURACIÓN EN EL CLIENTE WINDOWS

En nuestro cliente abrir el Outlook Express y luego aparecerá una ventana del mismo.

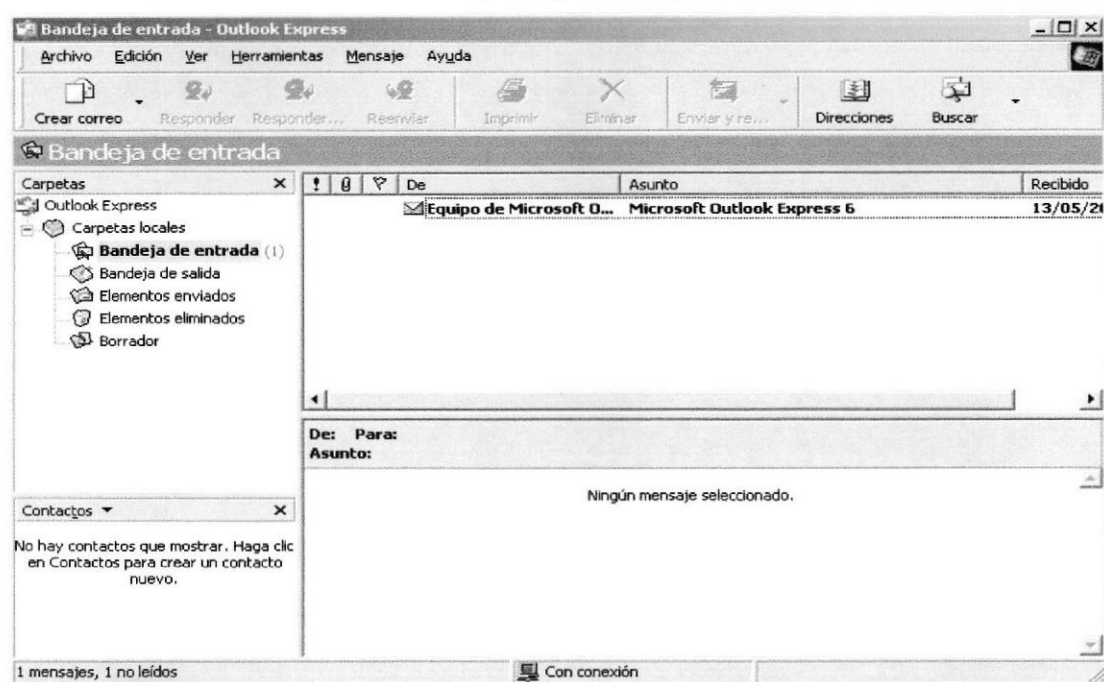
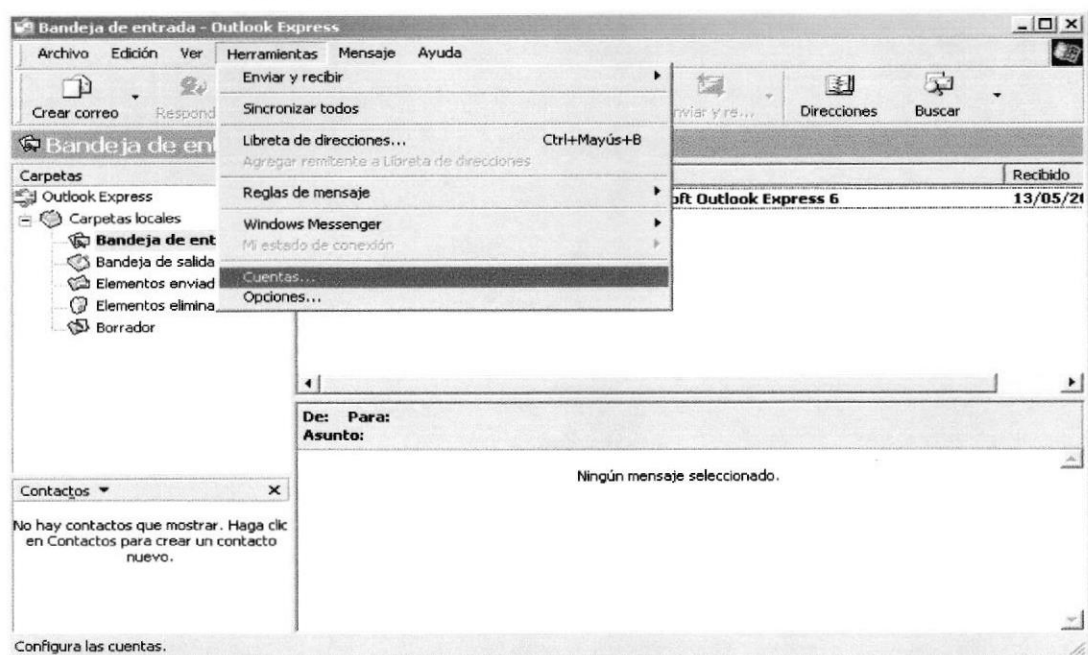


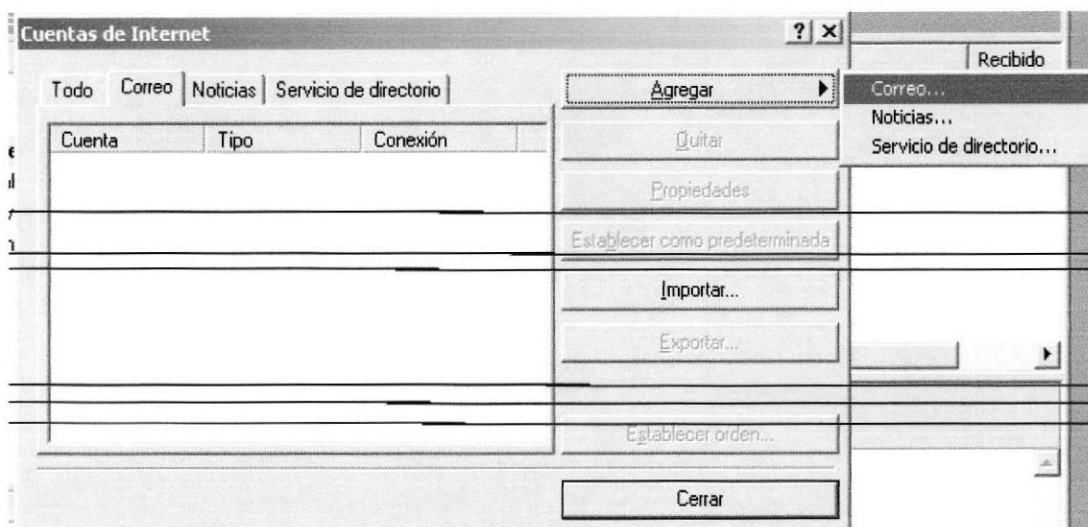
FIGURA 6 - 107: Crear usuarios en Windows

Cuando se ejecute el programa se dará clic en la opción Herramientas y clic en Cuentas.



**FIGURA 6 - 108:** Configurar una cuenta de correo electrónico

Luego aparecerá una ventana de Cuentas de Internet y elegimos la opción de agregar y se elige la opción de correo.



**FIGURA 6 - 109:** Agregar correo electrónico



Se mostrara un asistente para la conexión a Internet, y se escribe el nombre de nuestro usuario, se prece de la siguiente.manera

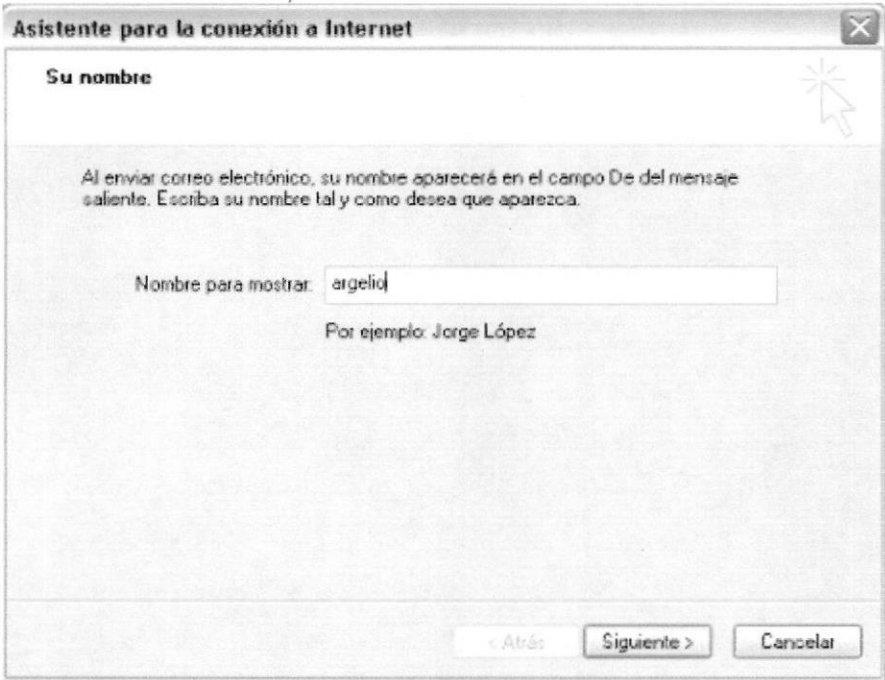


FIGURA 6 - 110: Asignación de nombre a la cuenta de correo

En esta pantalla se escribe el nombre del usuario con el nombre del dominio ya creado.

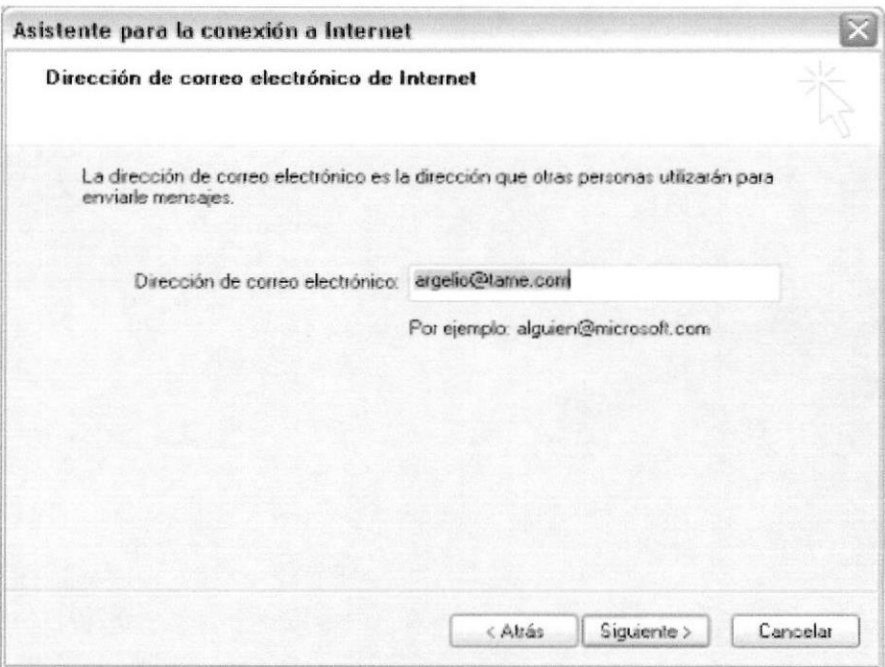
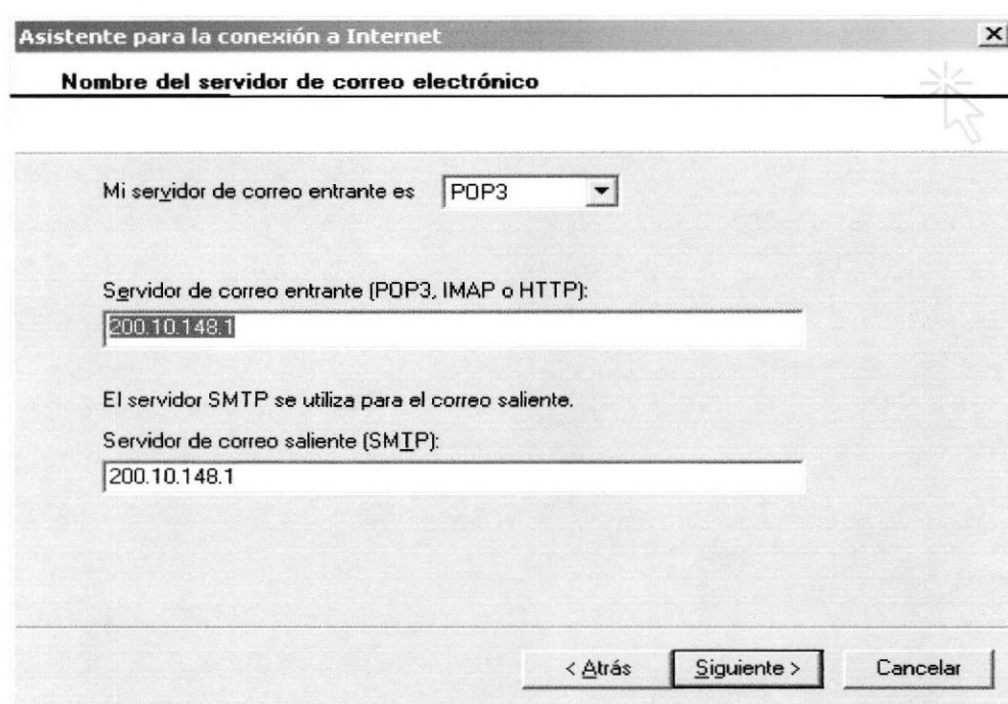


FIGURA 6 - 111: configuración de una cuenta de correo electrónico

A continuación el asistente nos pedirá el servidor de correo entrante y el servidor de correo saliente.



Asistente para la conexión a Internet

Nombre del servidor de correo electrónico

Mi servidor de correo entrante es: POP3

Servidor de correo entrante (POP3, IMAP o HTTP): 200.10.148.1

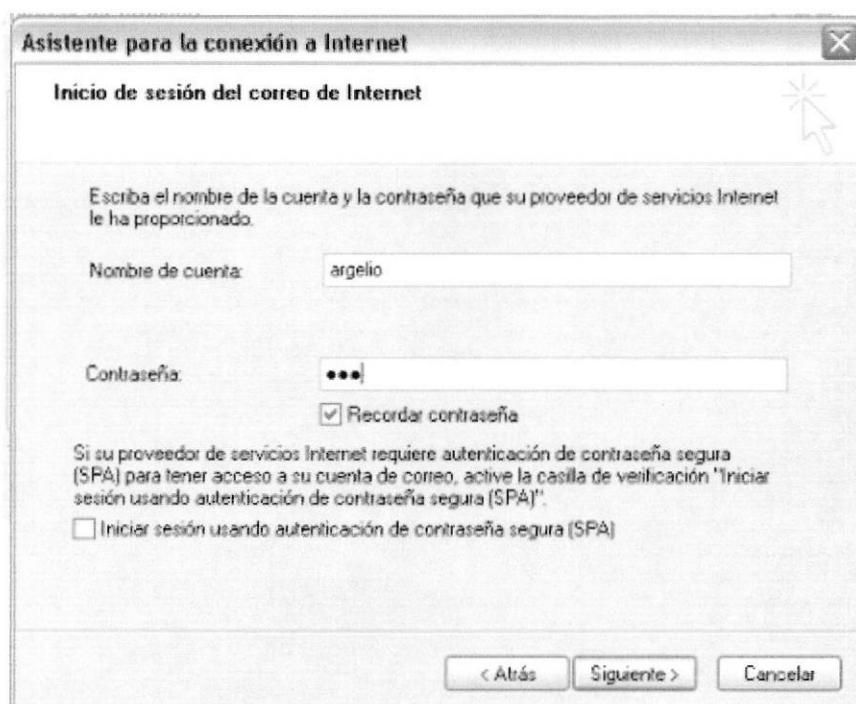
El servidor SMTP se utiliza para el correo saliente.

Servidor de correo saliente (SMTP): 200.10.148.1

< Atrás Siguiendo > Cancelar

**FIGURA 6 - 112:** Especificar Dirección POP3 y SMTP

A continuación el asistente le pide el nombre del usuario a crearse y la contraseña.



Asistente para la conexión a Internet

Inicio de sesión del correo de Internet

Escriba el nombre de la cuenta y la contraseña que su proveedor de servicios Internet le ha proporcionado.

Nombre de cuenta: argelio

Contraseña: ...

☒ Recordar contraseña

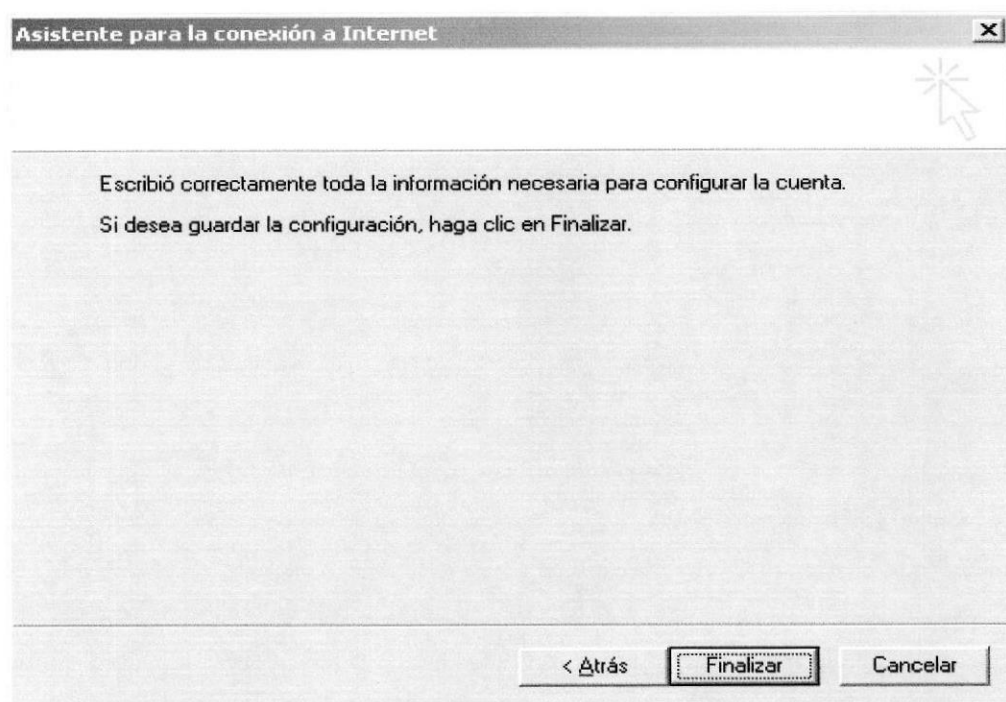
Si su proveedor de servicios Internet requiere autenticación de contraseña segura (SPA) para tener acceso a su cuenta de correo, active la casilla de verificación "Iniciar sesión usando autenticación de contraseña segura (SPA)".

☐ Iniciar sesión usando autenticación de contraseña segura (SPA)

< Atrás Siguiendo > Cancelar

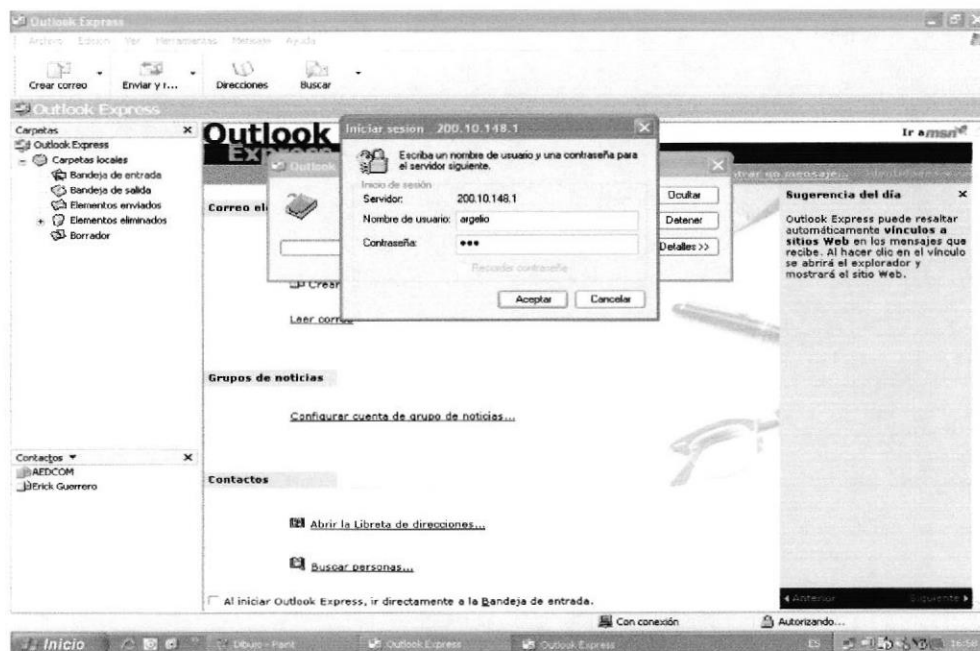
**FIGURA 6 - 113:** asignación de usuario y contraseña

Luego es asistente no dice si toda la información proporcionada es valida para finalizar el asistente.



**FIGURA 6 - 114:** finalización de la configuración de una cuenta de correo

Para saber si nuestro servidor de correos esta bien levantado, se realizara una prueba, enviando un correo de Windows a Linux.



**FIGURA 6 - 115:** Ingresar usuario y contraseña

Aquí se da cuenta que el mensaje enviado desde el servidor llega al cliente

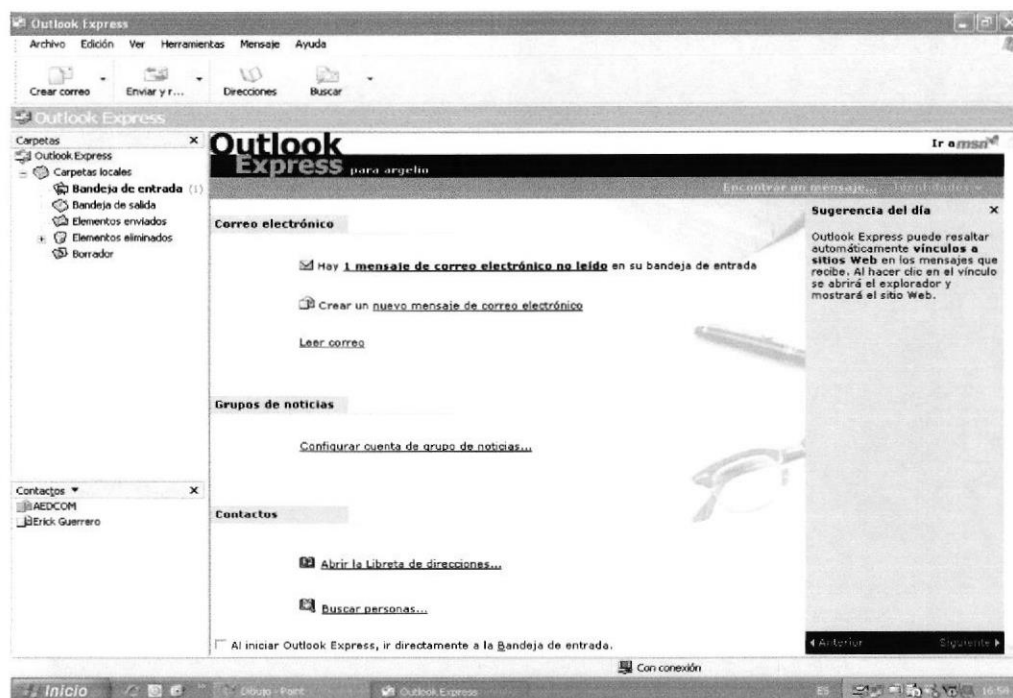


FIGURA 6 - 116: Enviado un mensaje al servidor

Para confirmar si el mensaje fue enviado a root, se revisara en la sección de elementos enviados.

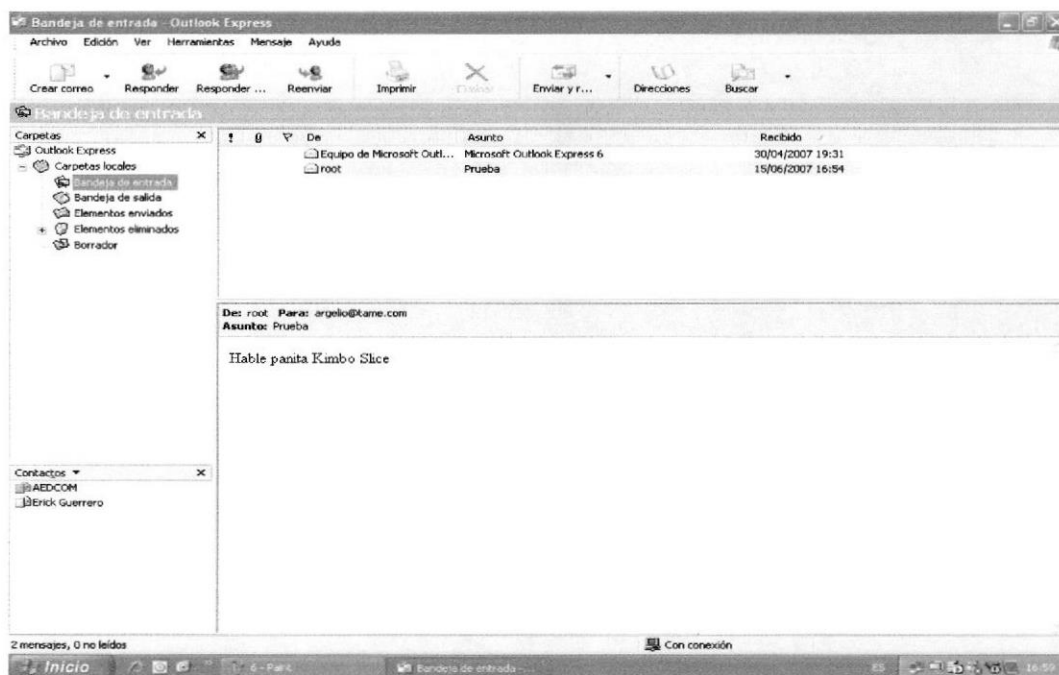


FIGURA 6 - 117: Mensaje de prueba receptado desde el servidor

Ahora se va a responderle al servidor enviándole un mensaje

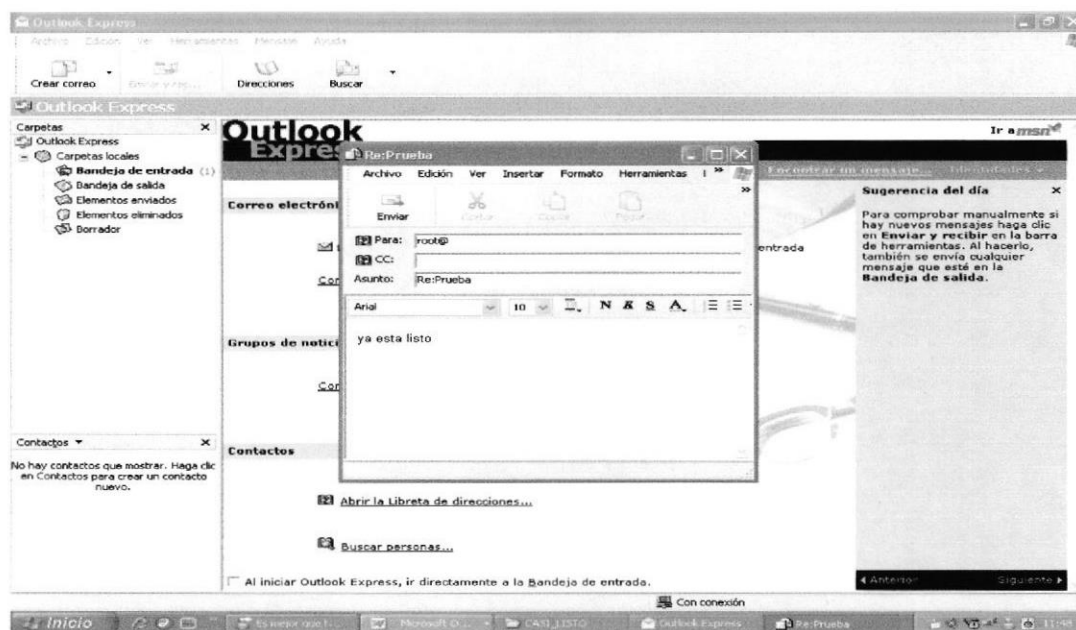
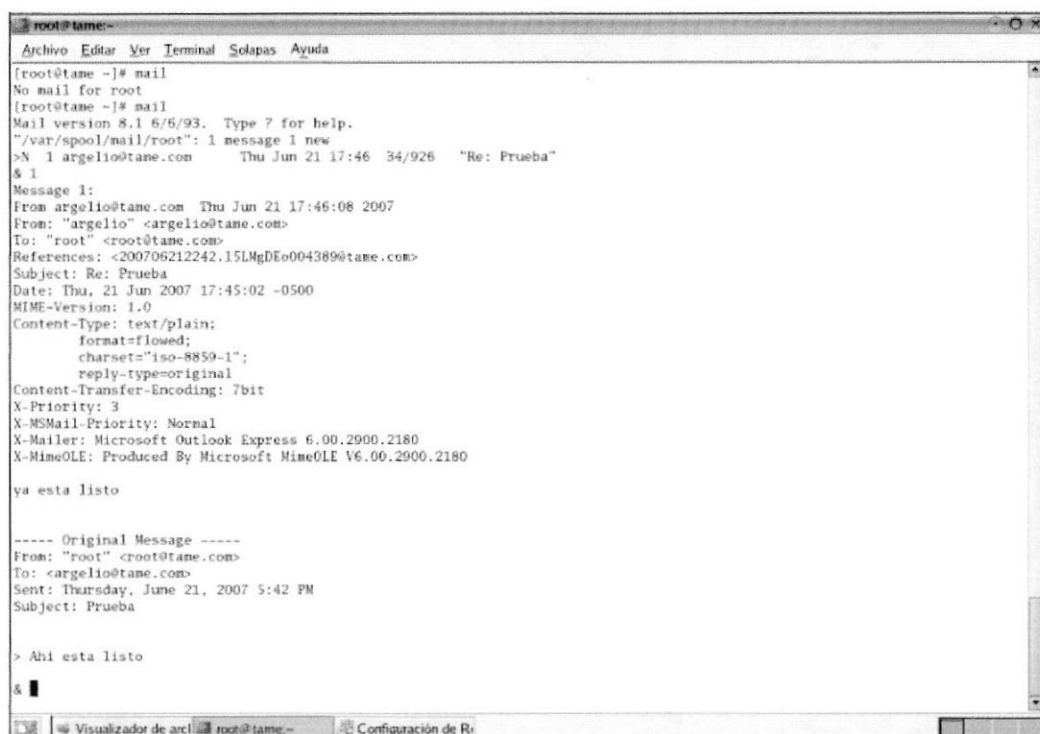


FIGURA 6 - 118: Enviando un mensaje al usuario root

#### 6.12.4.- PRUEBA DEL CLIENTE AL SERVIDOR

Aquí nos muestra el mail enviado por el cliente al servidor que fue recibido con éxito.



```
root@tame:~# mail
No mail for root
root@tame:~# mail
Mail version 8.1 6/6/93. Type ? for help.
"/var/spool/mail/root": 1 message 1 new
>N 1 argelio@tame.com Thu Jun 21 17:46 34/926 "Re: Prueba"
& 1
Message 1:
From: argelio@tame.com Thu Jun 21 17:46:08 2007
From: "argelio" <argelio@tame.com>
To: "root" <root@tame.com>
References: <200706212242.15LMgDEo004389@tame.com>
Subject: Re: Prueba
Date: Thu, 21 Jun 2007 17:45:02 -0500
MIME-Version: 1.0
Content-Type: text/plain;
      format=flowed;
      charset="iso-8859-1";
      reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

ya esta listo

----- Original Message -----
From: "root" <root@tame.com>
To: <argelio@tame.com>
Sent: Thursday, June 21, 2007 5:42 PM
Subject: Prueba

> Ahi esta listo
& 1
```

FIGURA 6 - 119: Recibiendo un mensaje del cliente



### 6.13.- CONFIGURACIÓN DHCP SERVER

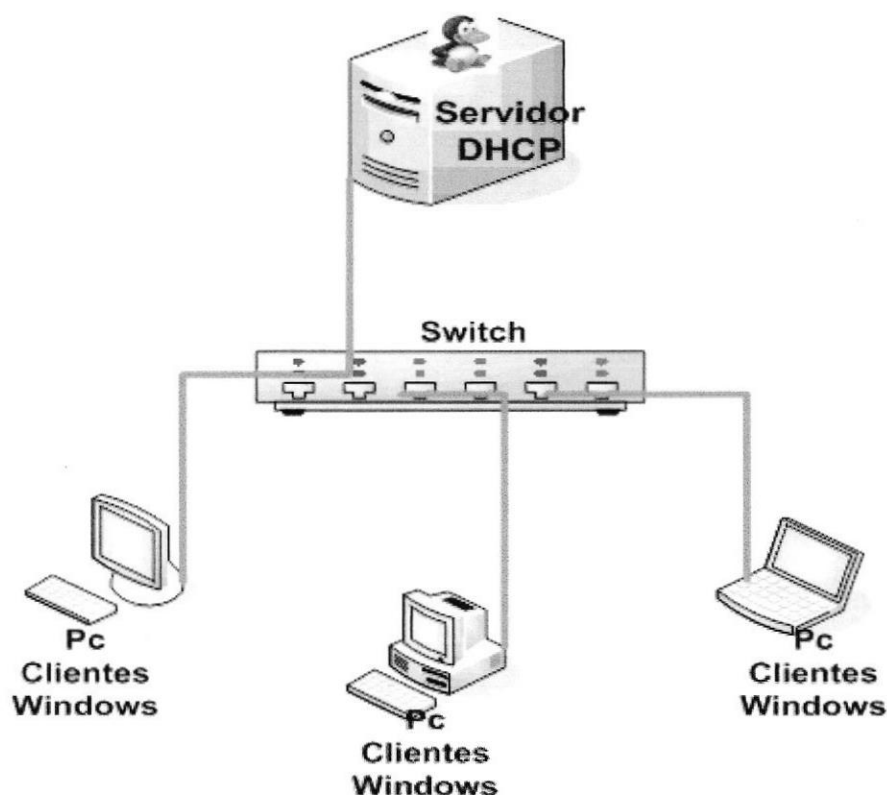


FIGURA 6 - 120: Servidor DHCP

**DHCP** son las siglas que identifican a un protocolo, empleado para que los hosts (clientes), en una red, puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS, entre otros. El servicio DHCP permite acelerar y facilitar la configuración de muchos ordenadores en una red, evitando en gran medida los posibles errores humanos.

Provee los parámetros de configuración a las computadoras conectadas a la red informática que lo requieran (Máscara de red, puerta de enlace y otros) y también incluyen mecanismo de asignación de direcciones de IP.

#### Asignación de direcciones IP

Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el ordenador es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

**Asignación manual o estática:** Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.



**Asignación automática:** Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.

**Asignación dinámica:** el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en RFC 2136 (Inglés).

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP (Bootstrap Protocol). DHCP es un protocolo más avanzado, pero ambos son los usados normalmente.

Cuando el DHCP es incapaz de asignar una dirección IP, se utiliza un proceso llamado "Automatic Private Internet Protocol Addressing".

Anatomía del protocolo

DHCP usa los mismos puertos asignados por el IANA (Autoridad de Números Asignados en Internet según siglas en inglés) en BOOTP: 67/UDP para las computadoras servidor y 68/UDP para los clientes.

### **DHCP Release**

Los clientes envían una petición al servidor DHCP para liberar su dirección DHCP. Como los clientes generalmente no saben cuándo los usuarios pueden desconectarlos de la red, el protocolo no define el envío del DHCP Release como obligatorio.

### **DHCP Discover**

Los clientes emiten peticiones masivamente en la subred local para encontrar un servidor disponible, mediante un paquete de broadcast. El router puede ser configurado para redireccionar los paquetes DHCP a un servidor DHCP en una subred diferente. La implementación cliente crea un paquete UDP (Protocolo de Datagramas de Usuario según siglas en inglés) con destino 255.255.255.255 y requiere también su última dirección IP conocida, aunque esto no es necesario y puede llegar a ser ignorado por el servidor.

### **DHCP Offer**

El servidor determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDRvbnv. El servidor especifica la dirección IP en el registro YIADDR. Como la cual se ha dado en los demás parámetros.

### **DHCP Request**

El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.



**DHCP Acknowledge**

El servidor confirma el pedido y lo publica masivamente en la subred. Se espera que el cliente configure su interface de red con las opciones que se le han otorgado.

**DHCP Nack**

El servidor envía al cliente un mensaje indicando que el contrato ha terminado o que la dirección IP asignada no es válida.

**DHCP Inform**

El cliente envía una petición al servidor de DHCP: para solicitar más información que la que el servidor ha enviado con el DHCPACK original; o para repetir los datos para un uso particular - por ejemplo, los browsers usan DHCP Inform para obtener la configuración de los proxies a través de WPAD. Dichas peticiones no hacen que el servidor de DHCP refresque el tiempo de vencimiento de IP en su base de datos.

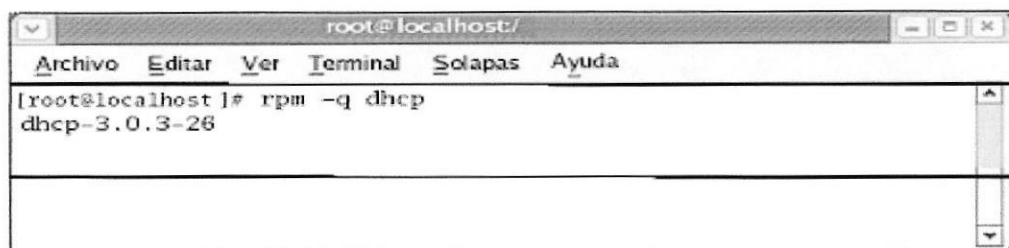
**6.13.1.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR DHCP**

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener habilitado los servicios necesarios (dhcpd).

### 6.13.2.- CONFIGURACIÓN DE UN SERVIDOR DHCP

Para configurar un servidor DHCP se debe tener configurado la tarjeta de red y tener instalado el paquete del DHCP.

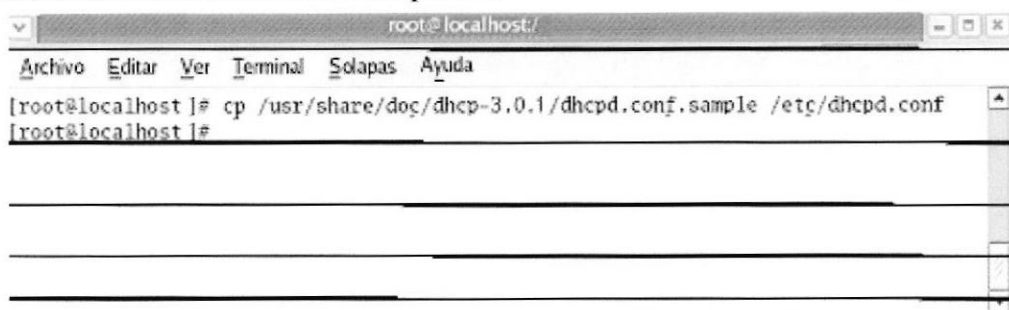
Se debe verificar si el paquete del DHCP esta instalado con el comando rpm -q.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost]# rpm -q dhcp  
dhcp-3.0.3-26
```

FIGURA 6 – 121: verificando paquete dhcp

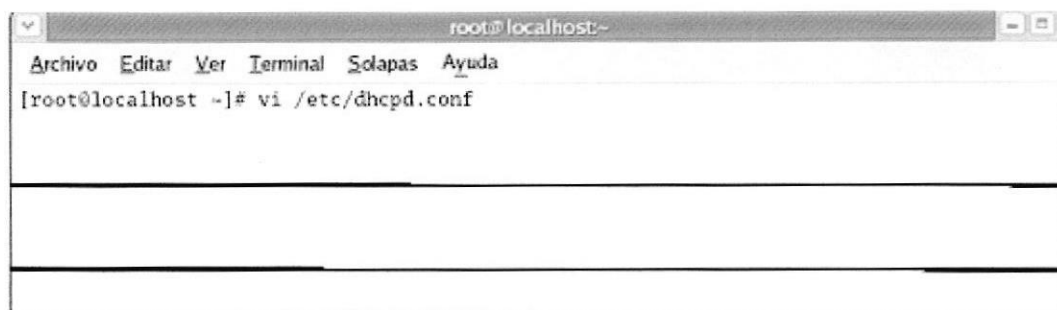
Luego se procede a buscar el directorio del dhcpd.conf.sample que se encuentra en **/usr/share/doc/dhcp-3.0.1/dhcpd.conf.sample**, y se copiara ese archivo al directorio /etc pero se lo renombrara con de dhcp.conf.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost]# cp /usr/share/doc/dhcp-3.0.1/dhcpd.conf.sample /etc/dhcpd.conf  
[root@localhost]#
```

FIGURA 6 - 122: Copiando archivo dhcp

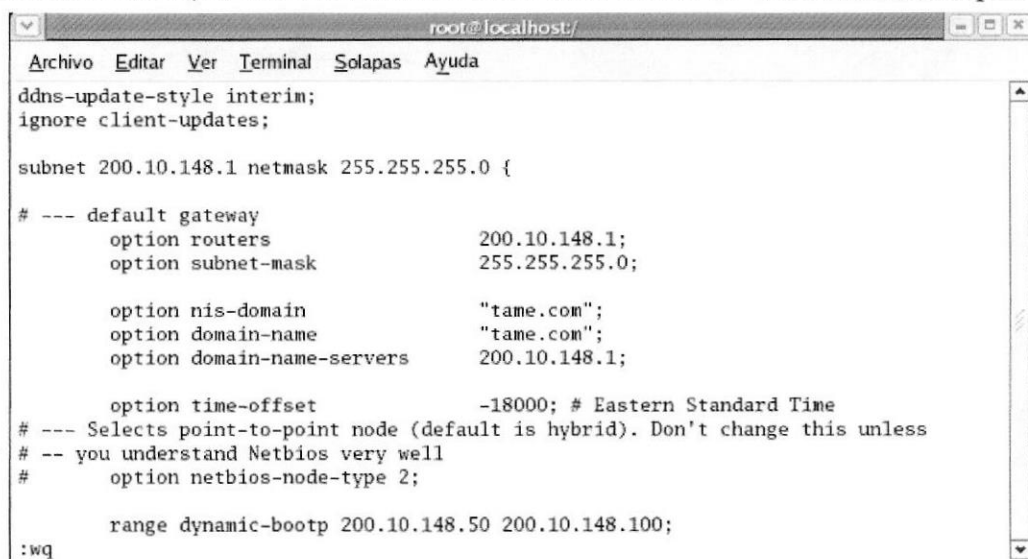
Una vez copiado el archivo del dhcp.conf, en el directoria /etc, procederá a editarlo.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# vi /etc/dhcpd.conf
```

FIGURA 6 - 123: Editando el archivo dhcp

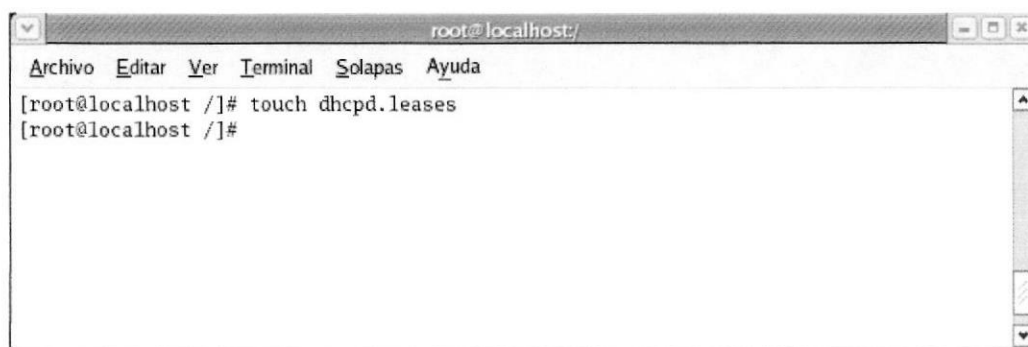
Dentro del archivo se editan las siguientes líneas para darle el rango de ip automática en el servidor DHCP, la dirección automática la da al cliente de la última hacia la primera:



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
ddns-update-style interim;  
ignore client-updates;  
  
subnet 200.10.148.1 netmask 255.255.255.0 {  
# --- default gateway  
    option routers                200.10.148.1;  
    option subnet-mask            255.255.255.0;  
  
    option nis-domain              "tame.com";  
    option domain-name            "tame.com";  
    option domain-name-servers    200.10.148.1;  
  
    option time-offset             -18000; # Eastern Standard Time  
# --- 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 200.10.148.50 200.10.148.100;  
:  
:wq
```

**FIGURA 6 - 124:** Configuración del fichero dhcp

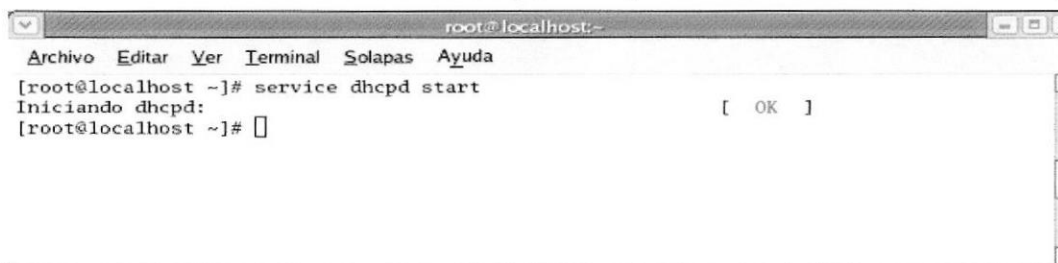
En el directorio / var/lib/dhcp/ creamos un archivo llamado dhcpd.leases el cual este archivo nos permitirá llevar un registro de las ip asignadas a los usuarios.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# touch dhcpd.leases  
[root@localhost /]#
```

**FIGURA 6 - 125:** creamos un archivo llamado dhcpd.leases

Cuando se halla creado el archivo del dhcpd.leases, se levantan los servicios del dhcp.

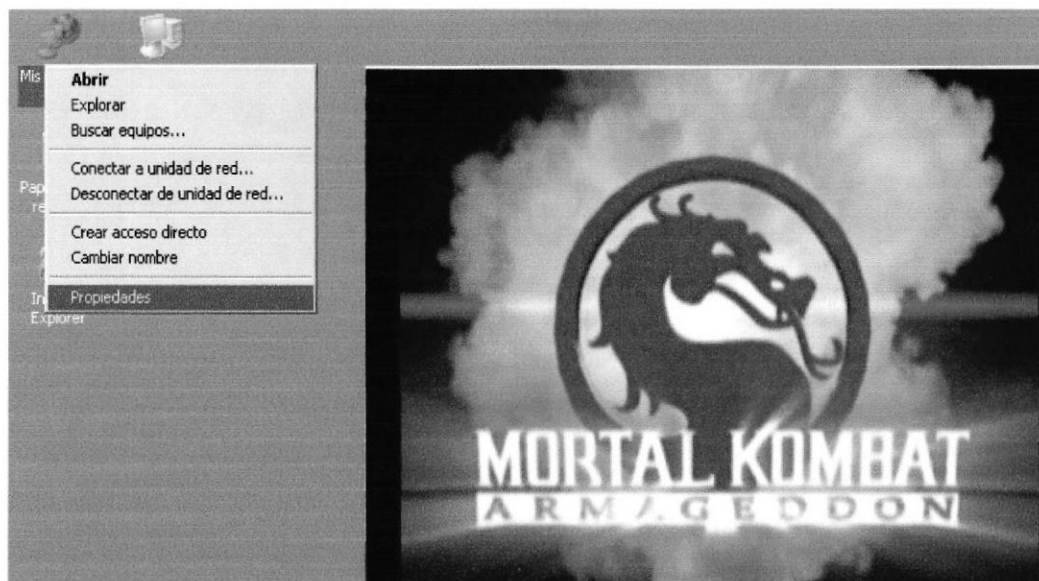


```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# service dhcpd start  
Iniciando dhcpd:  
[root@localhost ~]# [ OK ]
```

**FIGURA 6 - 126:** Iniciamos servicios dhcp

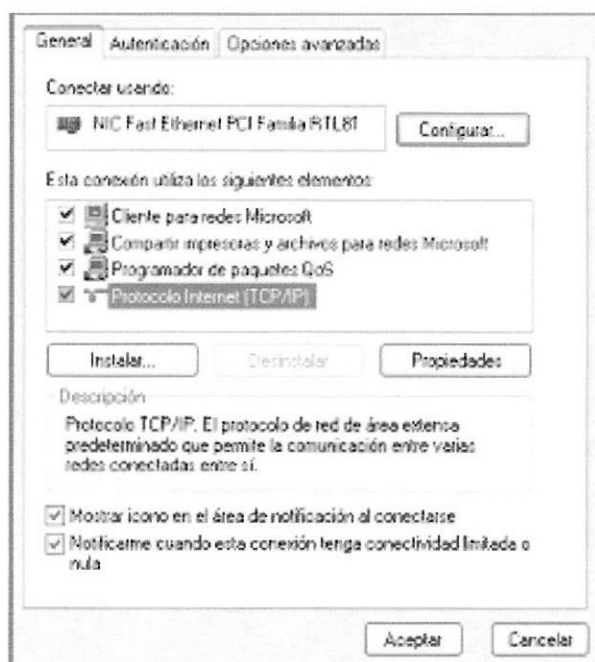
### 6.13.3.- CONFIGURACIÓN EN EL CLIENTE WINDOWS

En el icono de mis sitios de red se le dará clic derecho y se elige propiedades.



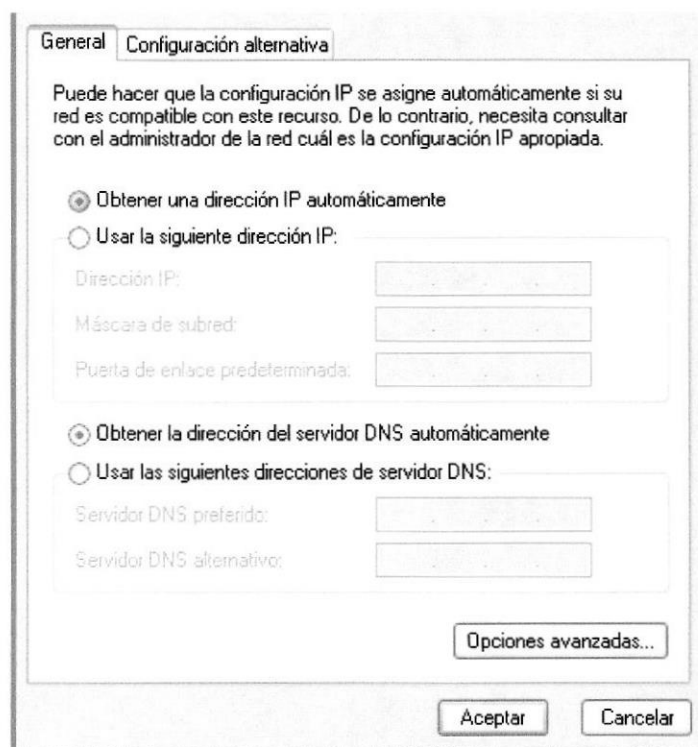
**FIGURA 6 - 127:** Propiedades Internet Explorer

En propiedades de red le da un clic en la opción de Protocolos de Internet (TCP/IP) y luego clic en el botón de propiedades.



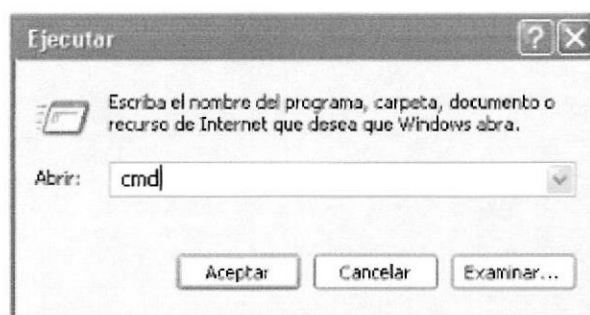
**FIGURA 6 - 128:** Protocolos de Internet (TCP/IP)

En esta ventana se da clic en la opción de Obtener una dirección IP automáticamente y otro clic en la opción de Obtener la dirección del servidor DNS automáticamente.



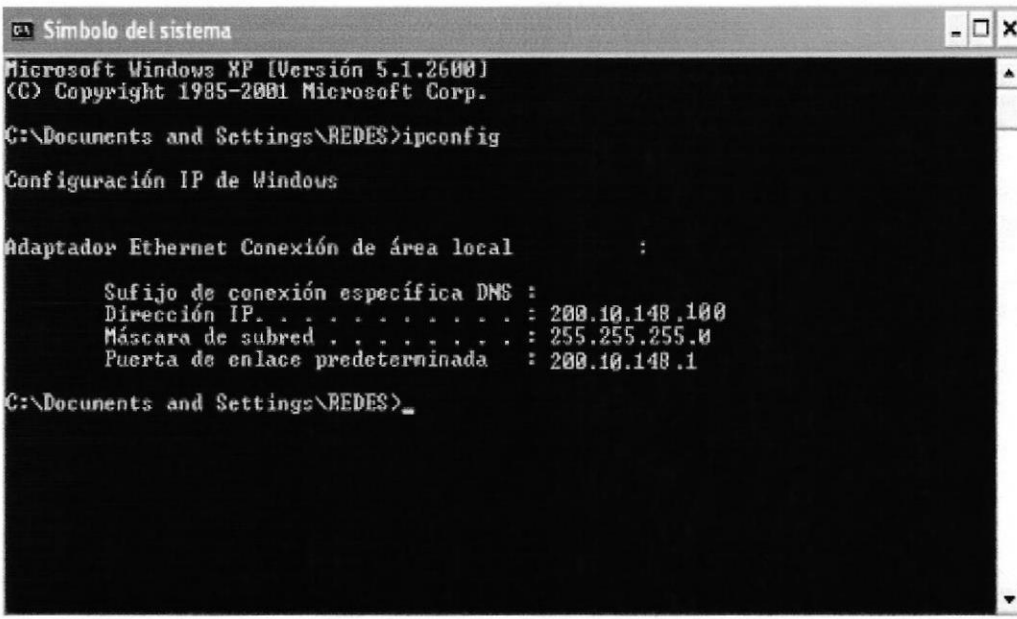
**FIGURA 6 - 129:** Configuración Automática

Luego dar clic en inicio, programas ejecutar y se escribe el comando cmd.



**FIGURA 6 - 130:** Ingresando al cmd

Para verificar la ip asignada por el servidor dhcp, se escribe el comando ifconfig.



```
Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\REDES>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local :

    Sufijo de conexión específica DNS :
    Dirección IP. . . . . : 200.10.148.100
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada : 200.10.148.1

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

**FIGURA 6 - 131:** Verificación de ip asignada por el servidor dhcp

## 6.14.- CONFIGURACIÓN PROXY SERVER

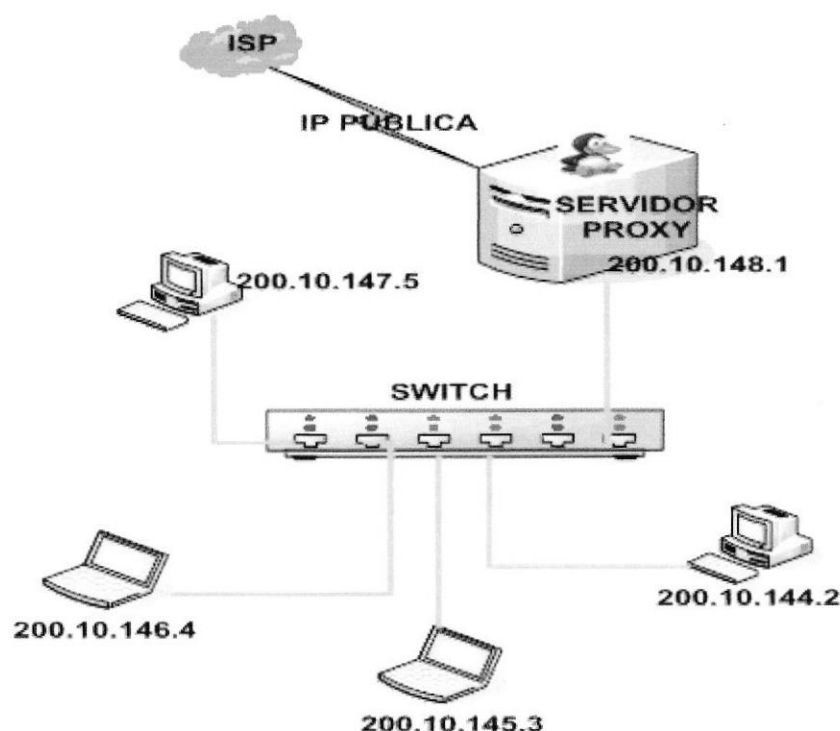


FIGURA 6 - 132: Servidor Proxy

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

Cliente se conecta hacia un Servidor Intermediario (**Proxy**).

Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto.

### 6.14.1.- BENEFICIOS PROXY SERVER

Servidor Intermediario (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.

En algunos casos el Servidor Intermediario (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

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

**Aplice políticas de seguridad**

Restrinja la navegación mediante la política que más le guste: combinación usuario/contraseña, restricción de horarios, listas de control de acceso o por dirección de máquina.

Obtenga mayor información

Genere reportes y gráficos de uso para determinar los sitios visitados, y la cantidad de tiempo en cada uno de ellos.

### **Administre eficientemente la navegación**

Puede administrar todo lo mencionado anteriormente desde cualquier navegador, a través de una herramienta web intuitiva y amigable. También puede hacerlo desde la línea de comandos si lo desea.

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

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

El Servidor Proxy Linux es una solución segura, robusta y versátil basada en Software Libre para una red local corporativa destinada a compartir la conexión a Internet. Este servidor le permite realizar distintos filtros de acceso, tanto por estaciones cliente como por listas de direcciones inapropiadas, o listas de palabras prohibidas, además de generar estadísticas y contabilizar un registro de conexiones.

El Servidor Proxy Linux ofrece grandes ventajas en el uso de la conexión a Internet como la optimización de la velocidad de conexión y mejora en la seguridad de la red local.

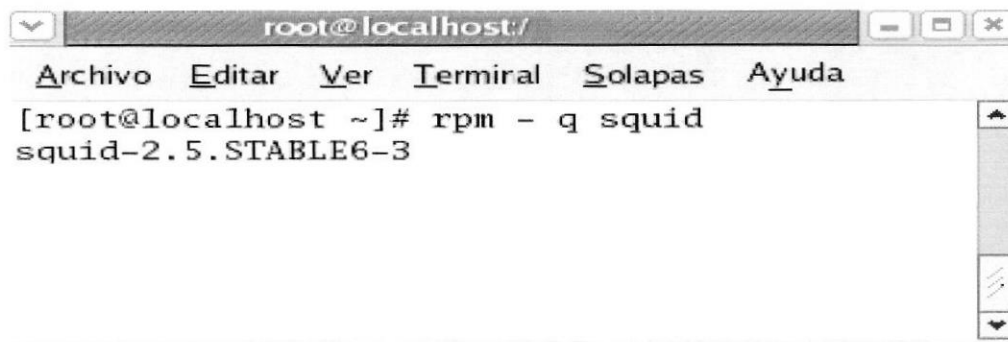
### **6.14.2.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR PROXY**

- 1 Pc con Linux Fedora Core 3
- 2 Tarjeta de Red
- Tener una IP Estática
- Tener habilitado los servicios.
- squid-2.5.STABLE1



Para configurar un servidor Proxy se debe tener configurado la tarjeta de red, tener configurado un DNS, un Web Server y tener instalado el paquete del Squid.

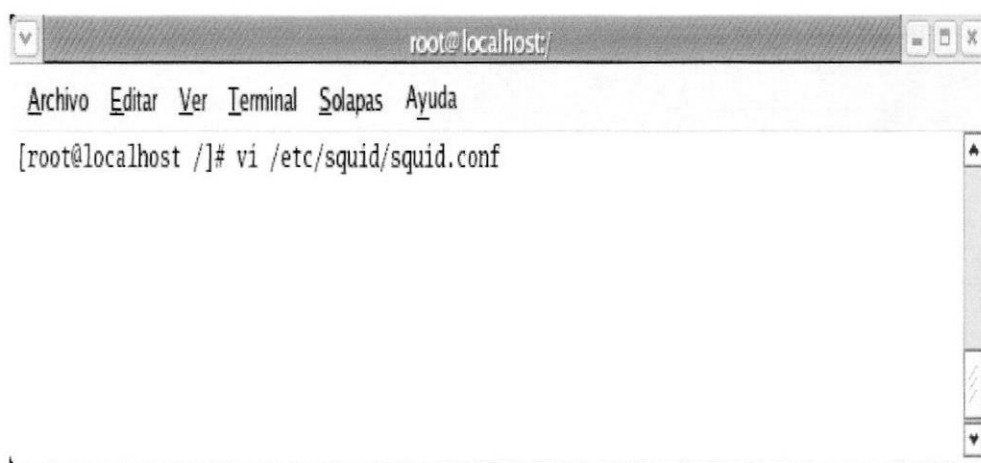
Se debe verificar si el paquete del Proxy esta instalado con el comando rpm -q.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# rpm -q squid  
squid-2.5.STABLE6-3
```

**FIGURA 6 - 133:** verificando paquete squid

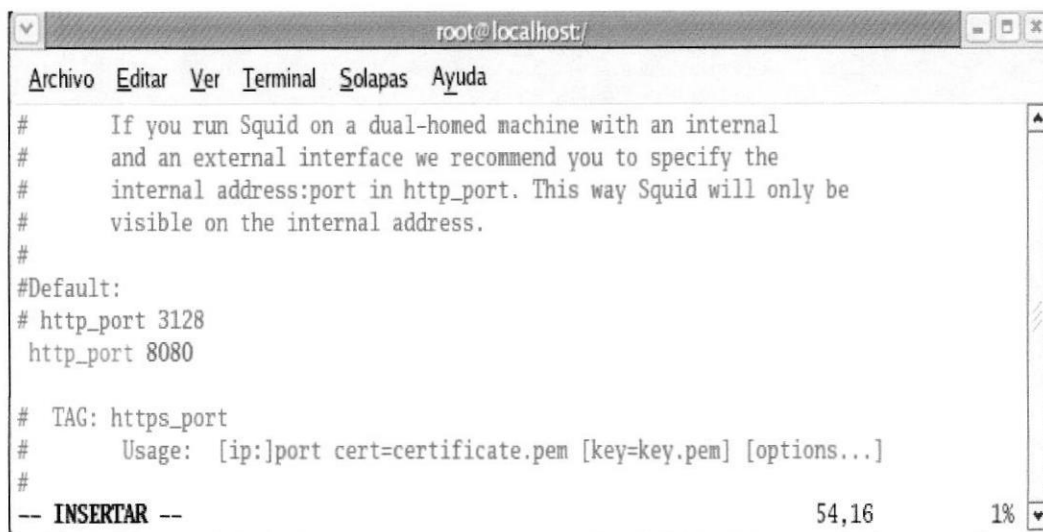
Luego de verificar si esta el paquete instalado, se edita el archivo que se encuentra en el directorio `/etc/squid/ squid.conf`.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# vi /etc/squid/squid.conf
```

**FIGURA 6 - 134:** Ingresamos a la configuración del squid

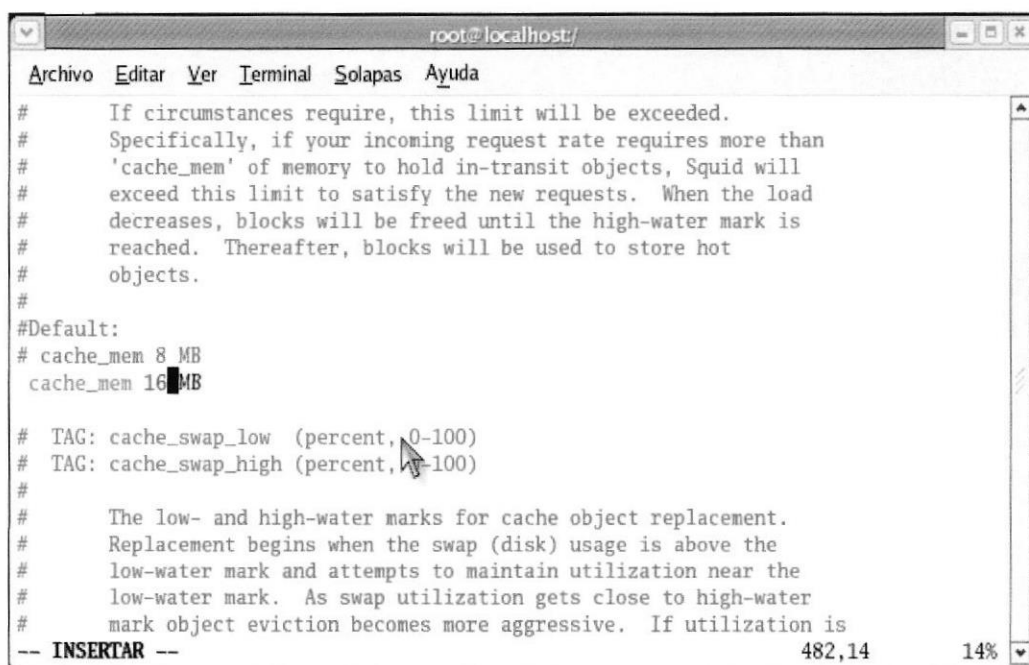
Squid por defecto utilizará el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto o bien que lo haga en varios puertos a la vez para este caso será el 8080.



```
root@localhost/
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
# http_port 8080
#
# TAG: https_port
#       Usage: [ip:]port cert=certificate.pem [key=key.pem] [options...]
#
-- INSERTAR --                                     54,16      1%
```

**FIGURA 6 - 135:** Configuración del puerto de salida del Proxy

Si se posee un servidor con al menos 128 MB de RAM establezca 16 MB como valor para este parámetro



```
root@localhost/
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
#       mark object eviction becomes more aggressive. If utilization is
#
-- INSERTAR --                                     482,14     14%
```

**FIGURA 6 - 136:** Asignando el espacio del directorio

Se guardara un historial de los acceso a la pagina, para esto se debe documentar la línea `cache_access_log /var/log/squid/access.log` recordar que este parámetro es opcional.

```

root@localhost:/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda

# 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

# 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

# TAG: cache_log
# Cache logging file. This is where general information about
-- INSERTAR --
698,1 20%

```

**FIGURA 6 - 137:** Asignando un directorio al Proxy

En la sección de las `auth_param basic` program es donde se establece el programa de autenticación para el Proxy.

```

root@localhost:/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda

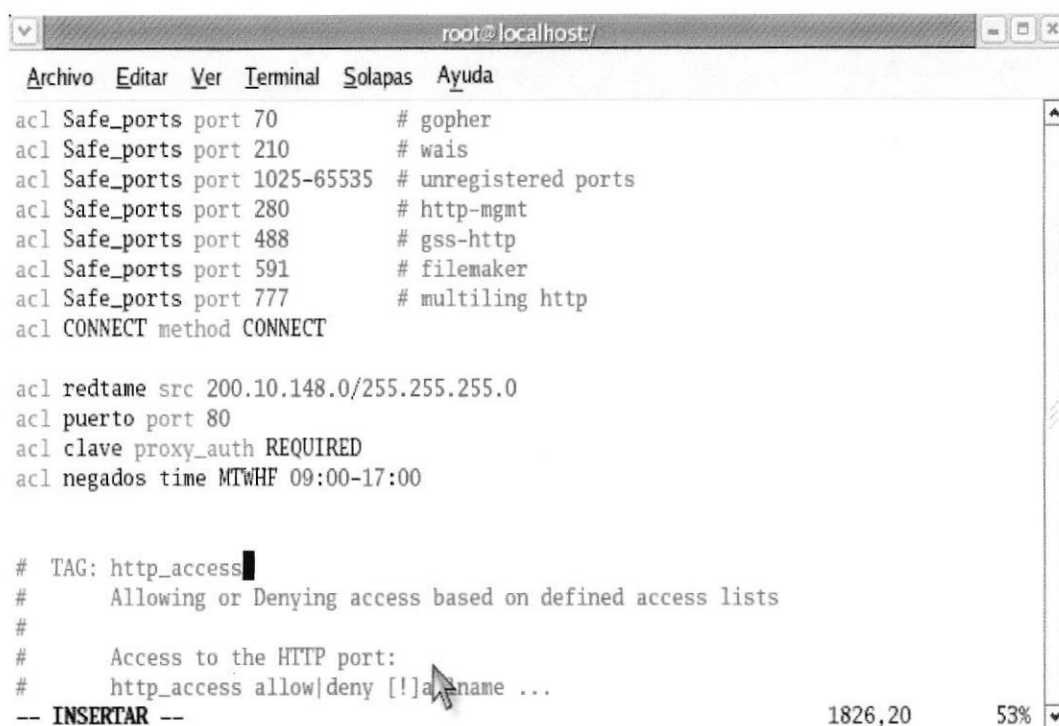
# reads a line containing "username password" and replies "OK" or
# "ERR" in an endless loop.
#
# By default, the basic authentication sheme is not used unless a
# program is specified.
#
# If you want to use the traditional proxy authentication, jump over to
# the helpers/basic_auth/NCSA directory and type:
#
# % make
# % make install
#
# Then, set this line to something like
#
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd

#
# "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 --
1093,62-69 32%

```

**FIGURA 6 - 138:** Programa de autenticación para el Proxy.

Luego de esto se busca la sección de la acl para definir nuestras reglas de acceso.



```

root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda

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

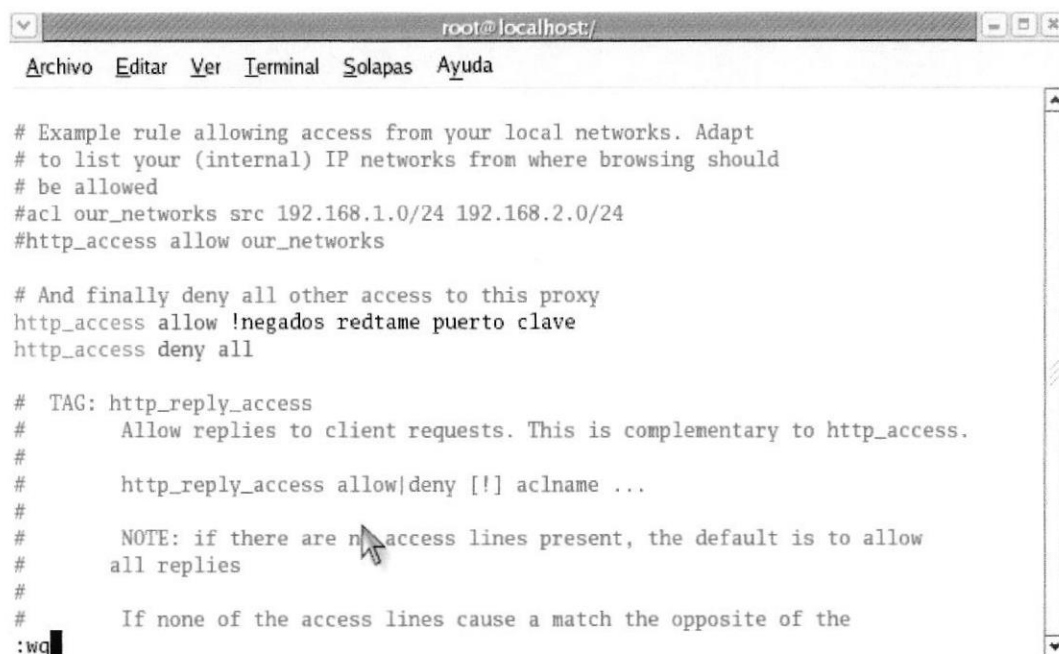
acl redtame src 200.10.148.0/255.255.255.0
acl puerto port 80
acl clave proxy_auth REQUIRED
acl negados time MTWHF 09:00-17:00

# TAG: http_access
#   Allowing or Denying access based on defined access lists
#
#   Access to the HTTP port:
#   http_access allow|deny [!]aclname ...
-- INSERTAR --                                     1826,20      53%

```

**FIGURA 6 - 139:** Creando Lista de control de acceso

Luego de esto se busca la sección de http\_access para definir nuestras reglas de acceso.



```

root@localhost:/
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

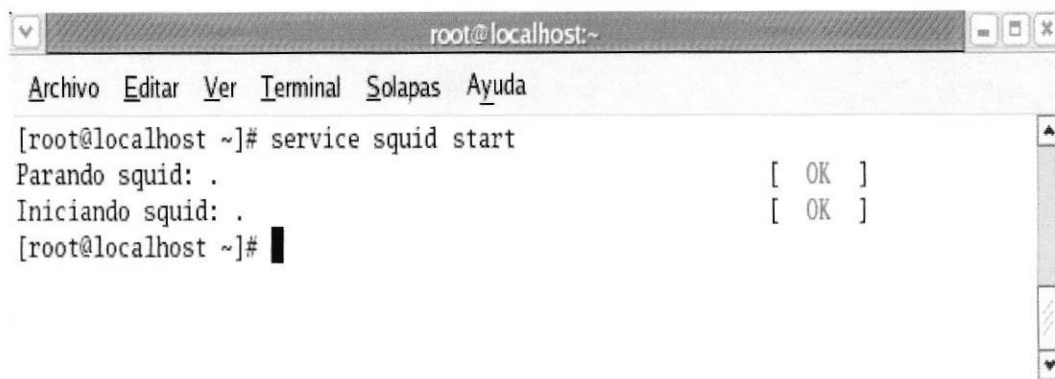
# And finally deny all other access to this proxy
http_access allow !negados redtame puerto clave
http_access deny all

# 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
:wg

```

**FIGURA 6 - 140:** Aplicando reglas de control de acceso

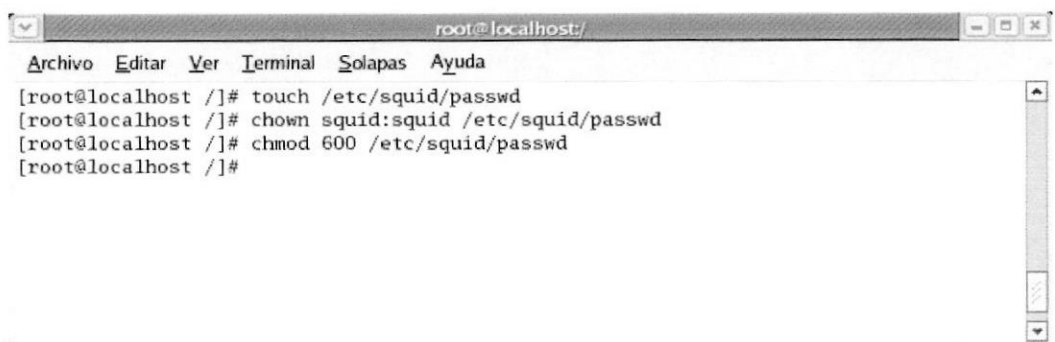
Una vez q se ha editado el archivo del squid se procederá a levantar los servicios del squid.



```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost ~]# service squid start  
Parando squid: . [ OK ]  
Iniciando squid: . [ OK ]  
[root@localhost ~]#
```

**FIGURA 6 - 141:** Iniciando servicio squid

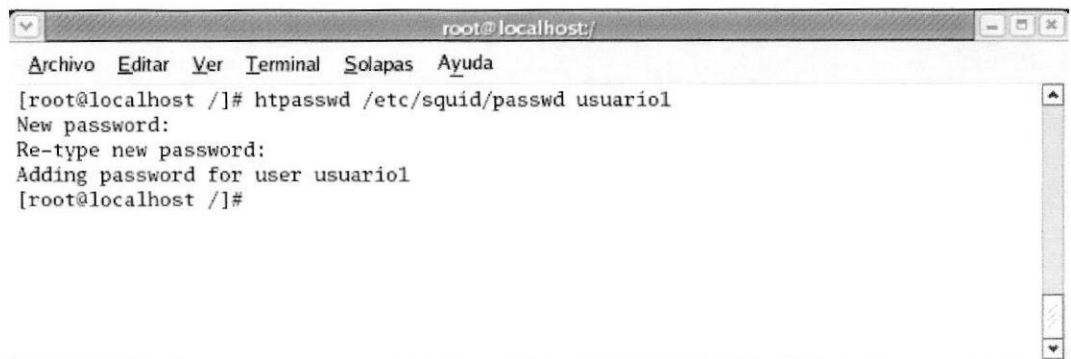
Luego de esto se crea el archivo en la ruta por defecto del squid, el cual contendrá todas las contraseñas del Proxy, le se cambia de grupo y usuario al archivo creado y se le da los respectivos permisos de lectura y escritura.



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# touch /etc/squid/passwd  
[root@localhost /]# chown squid:squid /etc/squid/passwd  
[root@localhost /]# chmod 600 /etc/squid/passwd  
[root@localhost /]#
```

**FIGURA 6 - 142:** Creamos fichero passwd

Para crear un usuario al cual tendrá acceso a Internet, se lo crea con el comando htpasswd.



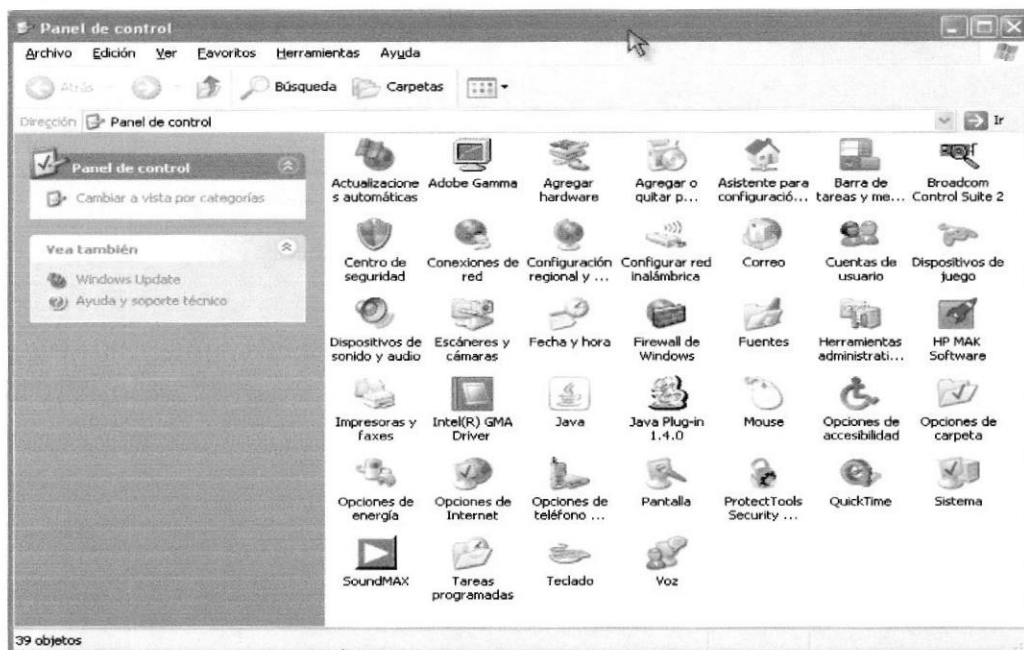
```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# htpasswd /etc/squid/passwd usuario1  
New password:  
Re-type new password:  
Adding password for user usuario1  
[root@localhost /]#
```

**FIGURA 6 - 143:** Creando usuarios squid

### 6.14.3- CONFIGURACIÓN EN EL CLIENTE WINDOWS

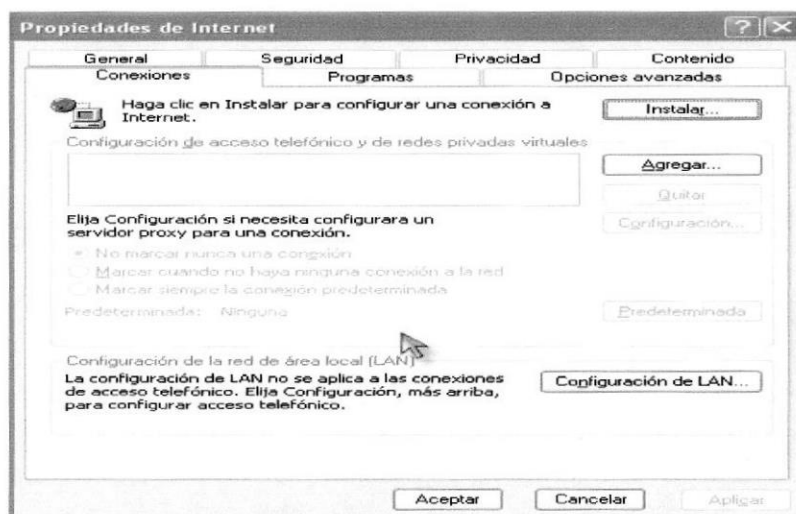
La configuración para los clientes con un sistema operativo Windows, que van a tener acceso al Proxy en sencilla, a continuación los pasos a seguir.

Dar clic en botón Inicio, Panel de Controles y doble clic sobre el icono de Opciones de Internet.



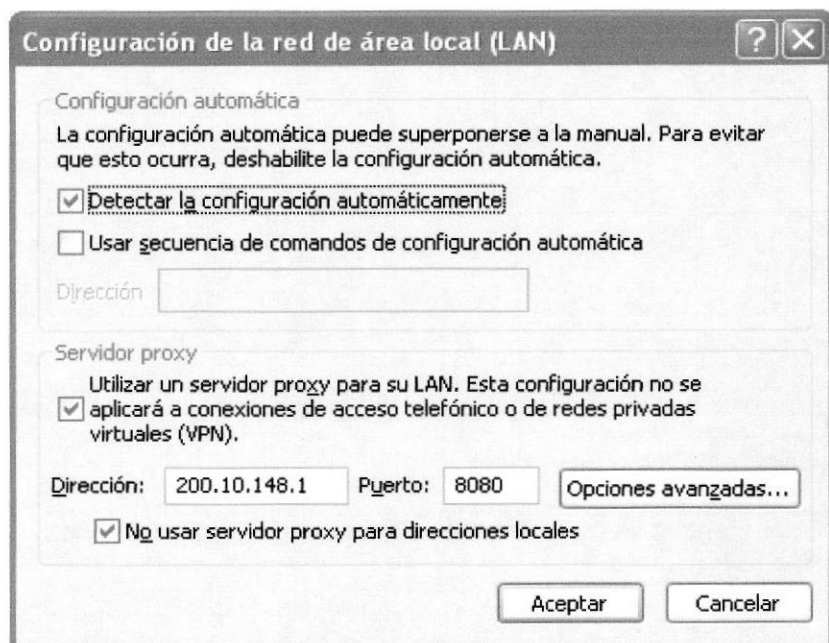
**FIGURA 6 - 144:** Ingresamos a opciones de Internet

A continuación se elige la opción Conexiones y se da click en el botón de Configuración de LAN.



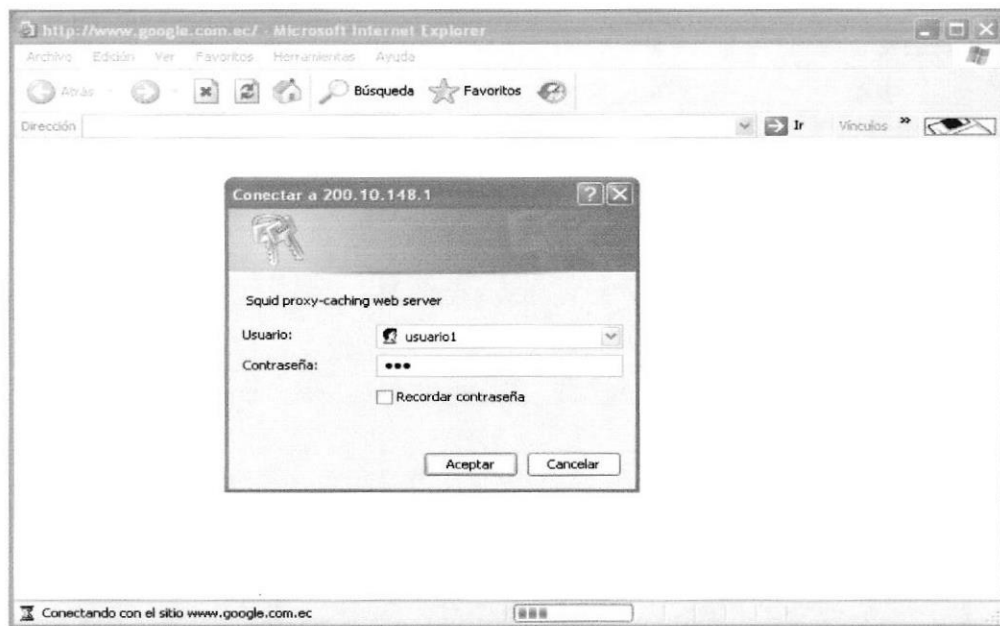
**FIGURA 6 - 145:** Ingresando a la configuración Lan

Luego le se da un visto a la opción Usar servidor Proxy, y escribimos la IP del servidor Proxy y el puerto que se va a utilizar el Proxy, y luego se dará clic en aceptar.



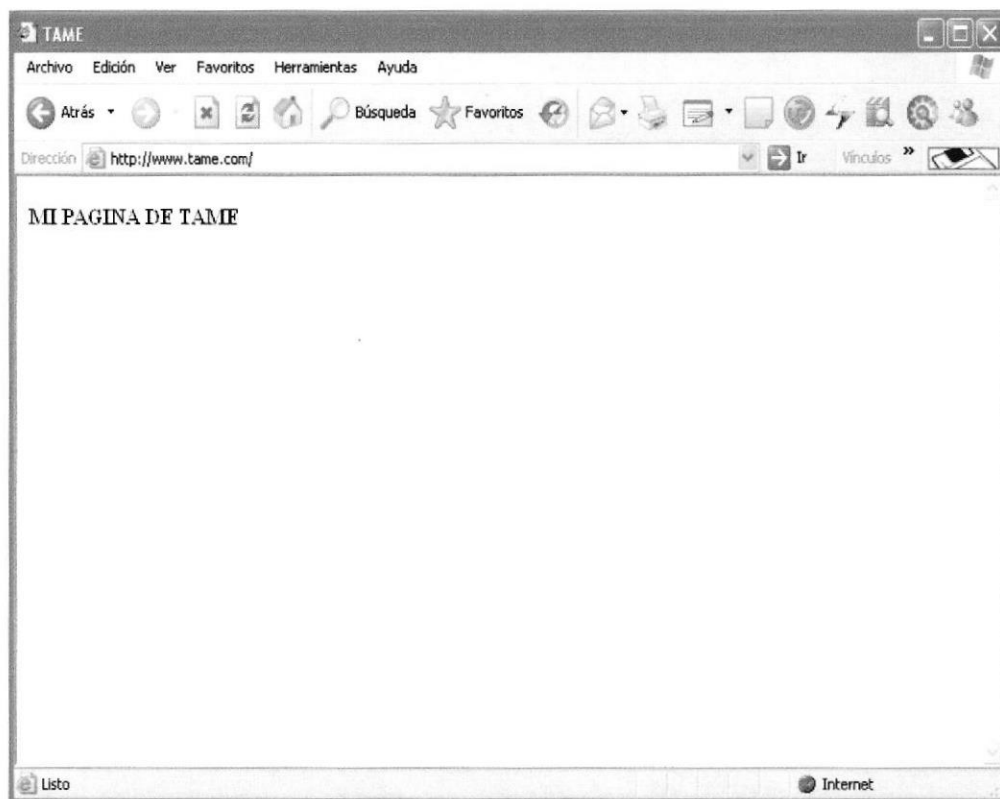
**FIGURA 6 - 146:** Ingresando la Ip del servidor y el puerto de salida

Después se abrirá una ventana del Internet Explorer el cual se pedirá un usuario y contraseña para poder navegar en Internet.



**FIGURA 6 - 147:** ingresar Usuario y contraseña

En la barra de direcciones se escribe nuestra dirección Web.



**FIGURA 6 - 148:** Prueba exitosa de la configuración Proxy



6.14.4.- RESTRINCIONES POR HORARIO

Los días están determinados por las letras los cuales son los siguientes:

LUNES	M
MARTES	T
MIÉRCOLES	W
JUEVES	H
VIERNES	F
SÁBADO	A
DOMINGO	A

Tabla 6 - 4: Días determinados en letras

Pueden combinarse los días

La hora inicio y hora fin debe ser asignados en formato 24:00

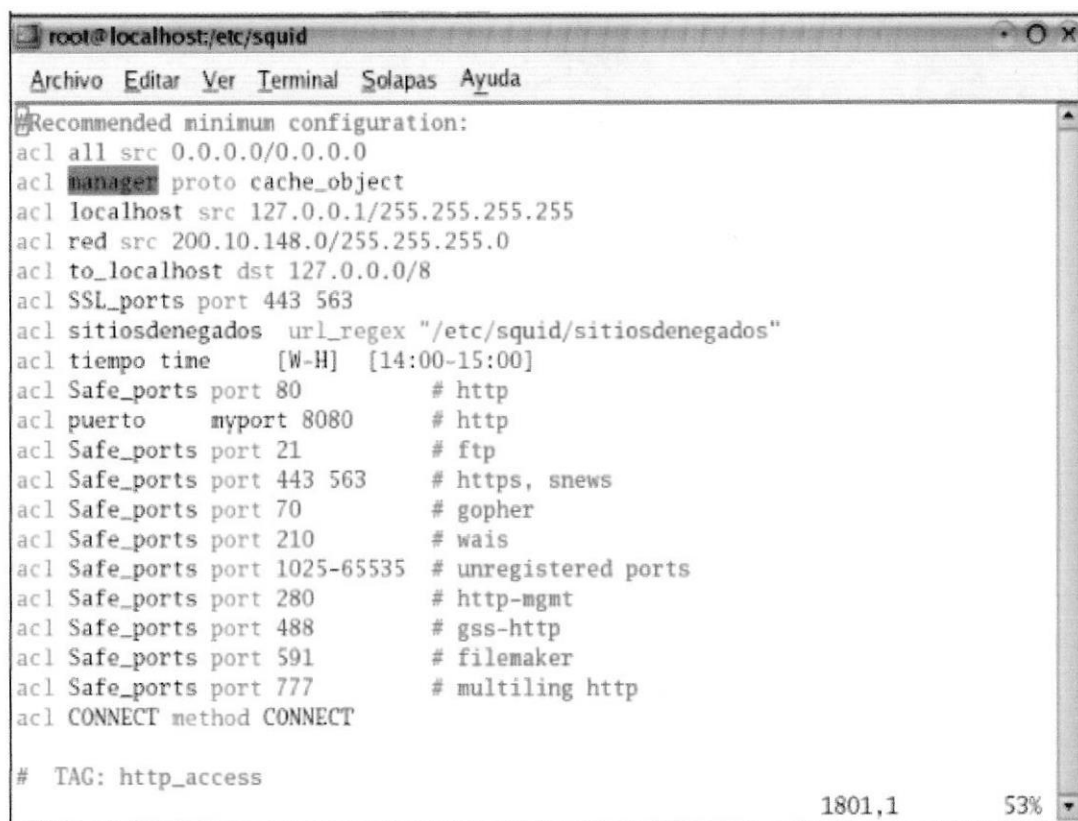
Para poder empezar a configurar por horario se debe digitar el archivo de configuración squid.conf,



FIGURA 6 - 149: Ingresamos a la configuración del squid

En la parte de las acl, se procederá a crear una línea donde se dará el rango de días y horas que se van a denegar.

**acl tiempo time [W-H] 14:00-15:00:** Esta línea permite denegar el acceso a Internet mediante la hora del Servidor.

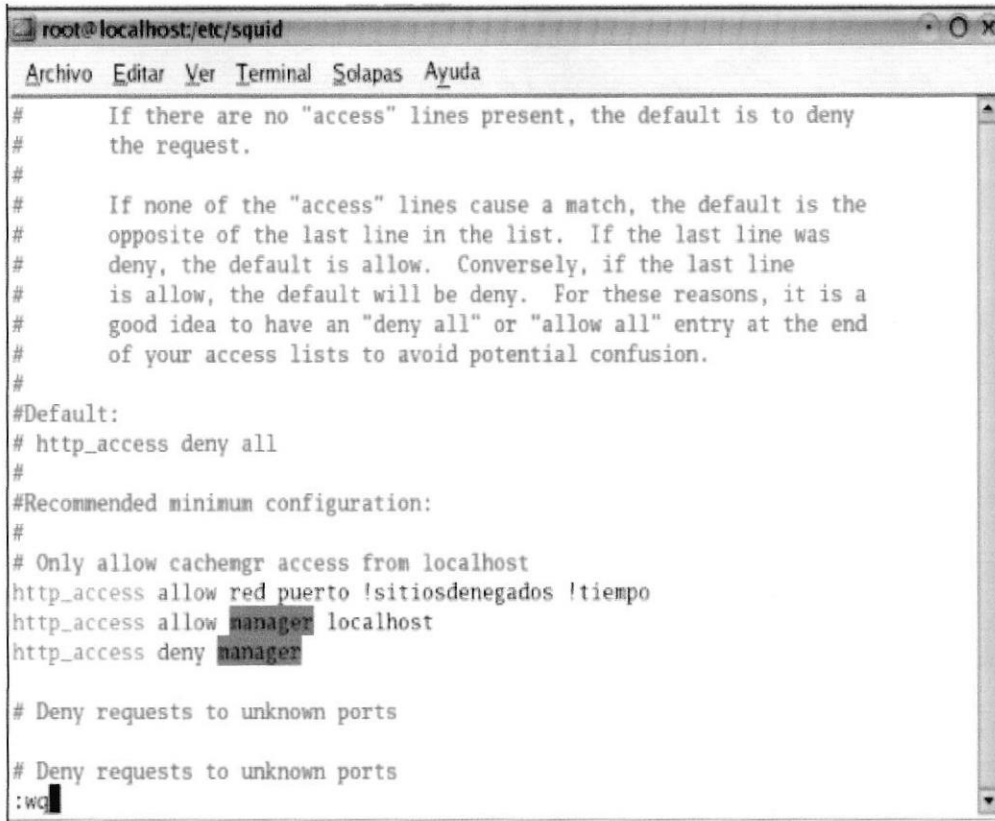


```
root@localhost:/etc/squid
Archivo Editar Ver Terminal Solapas Ayuda
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl red src 200.10.148.0/255.255.255.0
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
acl tiempo time [W-H] [14:00-15:00]
acl Safe_ports port 80 # http
acl puerto myport 8080 # 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

# TAG: http_access
1801,1 53%
```

**FIGURA 6 – 150:** Creando Lista de control de acceso

Luego de haber insertado la línea en las acl, se va a las http\_access donde se agregara el nombre de la acl creada, y luego se guarda los cambios y salimos.



```
root@localhost:/etc/squid
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#       If there are no "access" lines present, the default is to deny
#       the request.
#
#       If none of the "access" lines cause a match, the default is the
#       opposite of the last line in the list.  If the last line was
#       deny, the default is allow.  Conversely, if the last line
#       is allow, the default will be deny.  For these reasons, it is a
#       good idea to have an "deny all" or "allow all" entry at the end
#       of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachengr access from localhost
http_access allow red puerto !sitiosdenegados !tiempo
http_access allow manager localhost
http_access deny manager

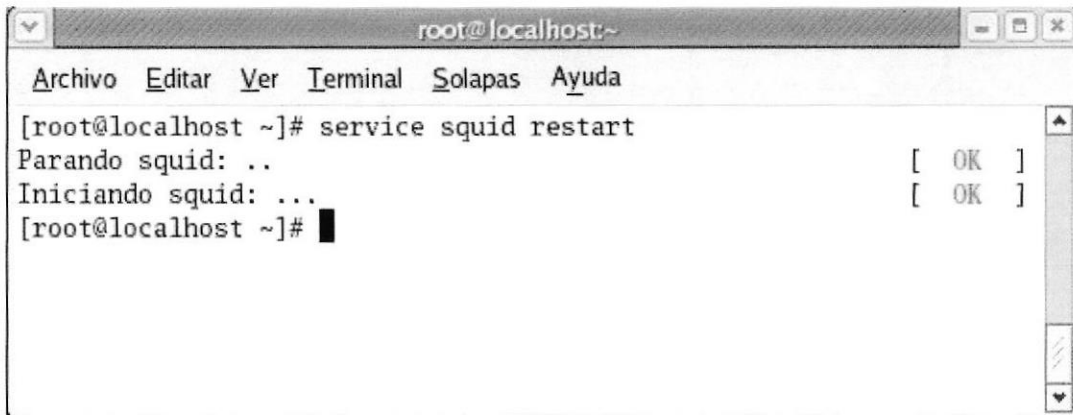
# Deny requests to unknown ports

# Deny requests to unknown ports
:wq
```



FIGURA 6 - 151: Reglas de control de acceso por horario

Luego de denegar por horario se restaurara el servicio squid, cabe indicar que cada configuración que se haga se deberá levantar el servicio para que tome efecto.



```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# service squid restart
Parando squid: .. [ OK ]
Iniciando squid: ... [ OK ]
[root@localhost ~]#
```

FIGURA 6 - 152: Reiniciando servicio squid

Luego de haber levantado el servicio, se va al equipo del cliente para verificar si esta bien hecha la configuración,

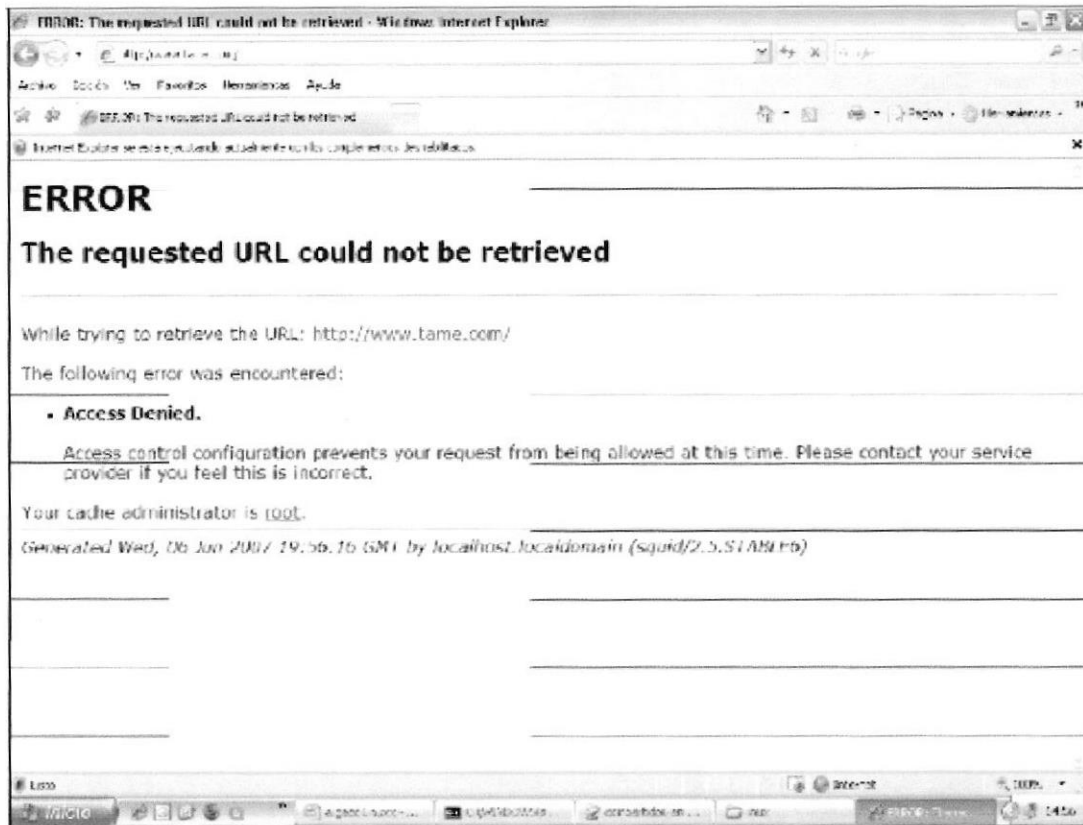


FIGURA 6 - 153: Prueba exitosa del Proxy por hora

### 6.14.5.- RESTRICCIÓN POR PÁGINAS PROHIBIDAS

Para poder empezar a configurar por bloqueo de página se deberá digitar el archivo de configuración squid.conf,



FIGURA 6 - 154: Ingresamos a la configuración del squid

Luego de haber ingresado a la configuración del squid se agrega la línea en la cual se agregara a una lista de páginas a las cuales no deben tener acceso los clientes.

**acl sitiosdenegados url\_regex "/etc/squid/sitiosdenegados"**: Esta línea se declarara una ruta donde se guardaran las direcciones Web que no se desea tener acceso.

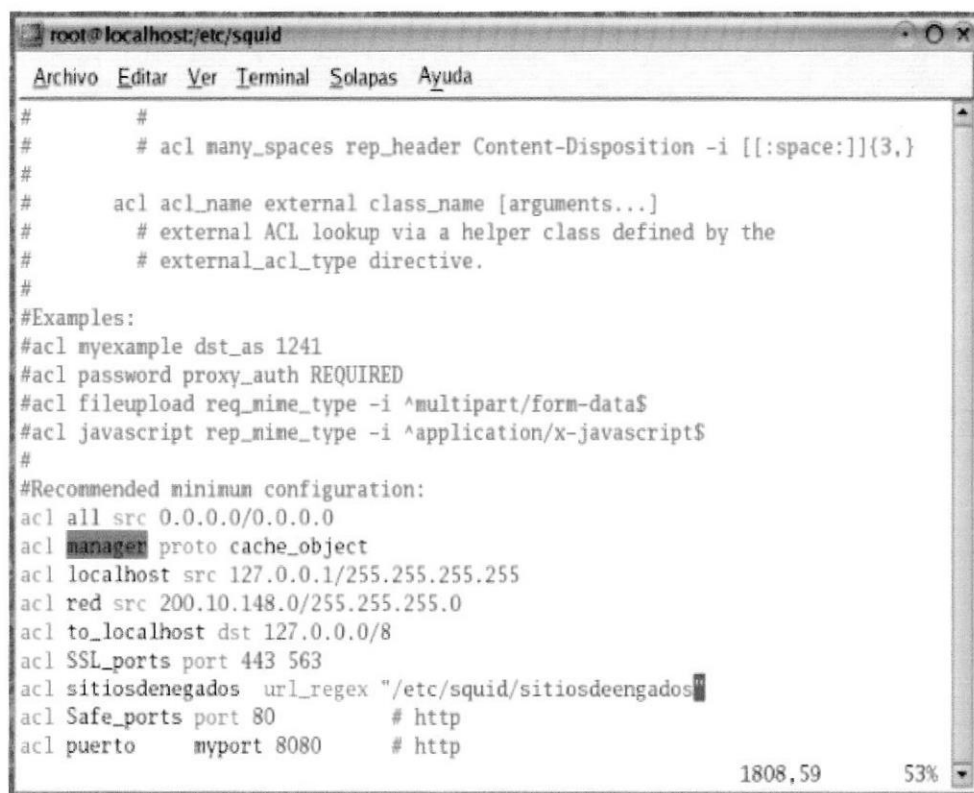
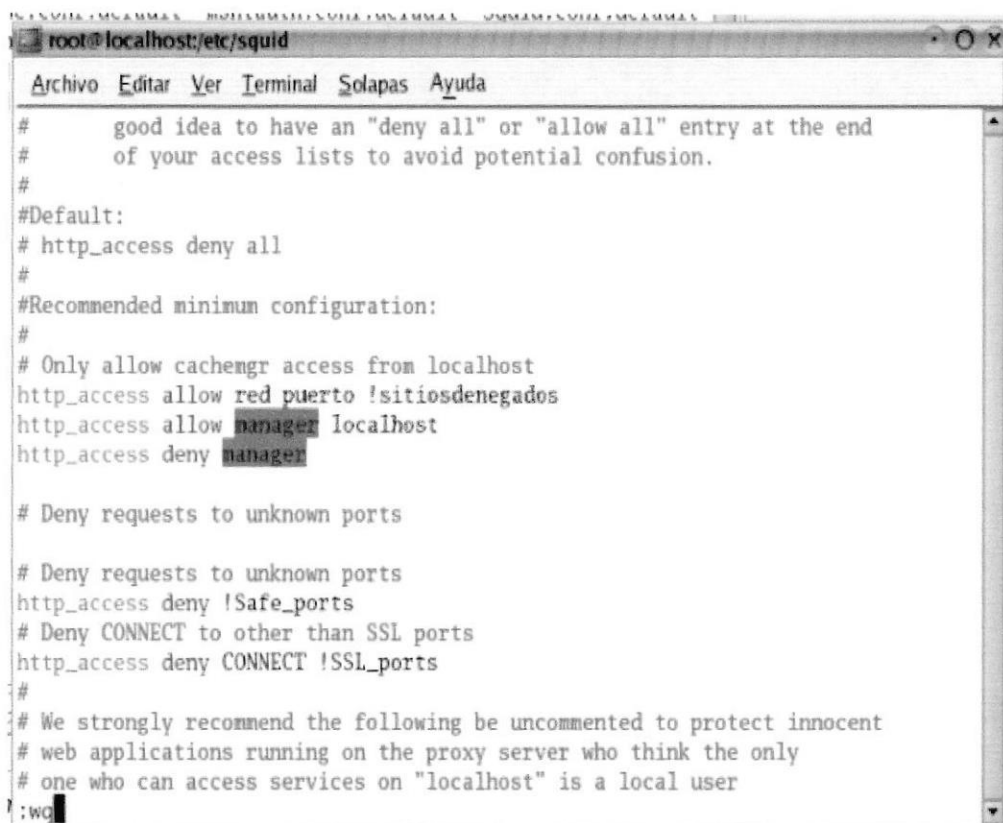


FIGURA 6 - 155: Creando Lista de control de acceso

Después de haber asignado en las acl la ruta se procede a denegar el nombre asignado en las acl, se guardara los cambios y salimos.



```
root@localhost:/etc/squid
# good idea to have an "deny all" or "allow all" entry at the end
# of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachengr access from localhost
http_access allow red puerto !sitiosdenegados
http_access allow nanager localhost
http_access deny nanager

# Deny requests to unknown ports

# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
#
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
:wg
```

FIGURA 6 – 156: Reglas de control de acceso por sitio denegado

Digitar el archivo de configuración squid.conf,



```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# touch / sitiosdenegados
[root@localhost /]#
```

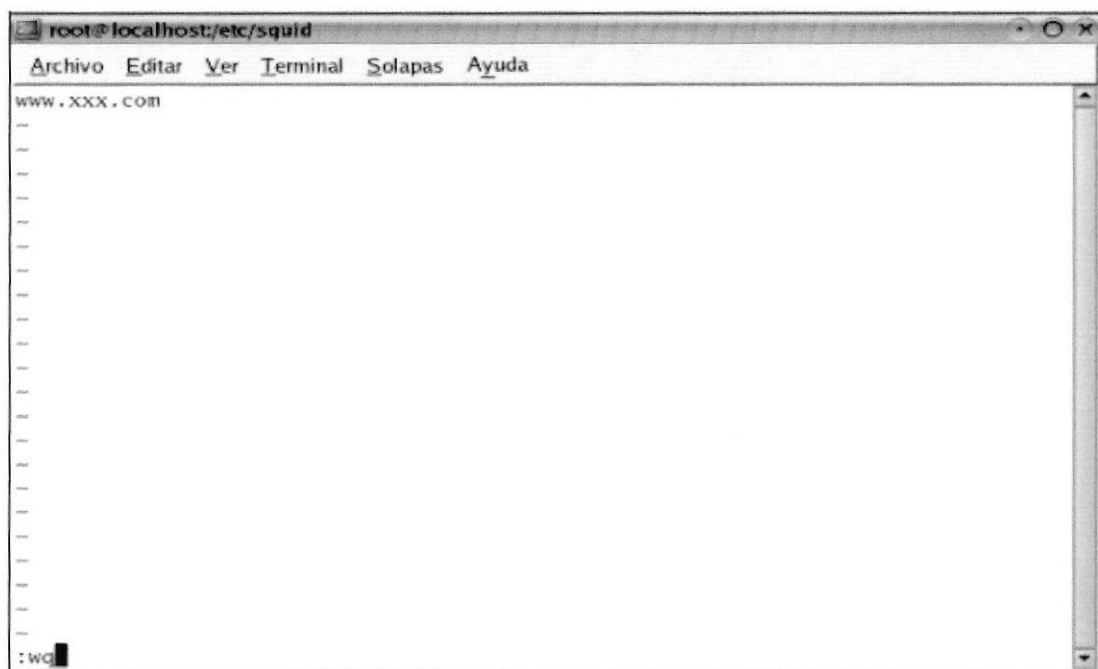
FIGURA 6 - 157: Creando archivo para los sitios denegados

Luego se procederá a editar el archivo, en el cual se pondrá la lista de direcciones web que no se deben cargar.



**FIGURA 6 - 158:** Editando archivo de sitios denegados

Agregar la lista de direcciones web a la cual no debe el cliente tener acceso.



**FIGURA 6 - 159:** Agregar la lista de direcciones web

Luego de haber editado el archivo donde se alojaran las paginas negadas, se reiniciara el servicio squid.

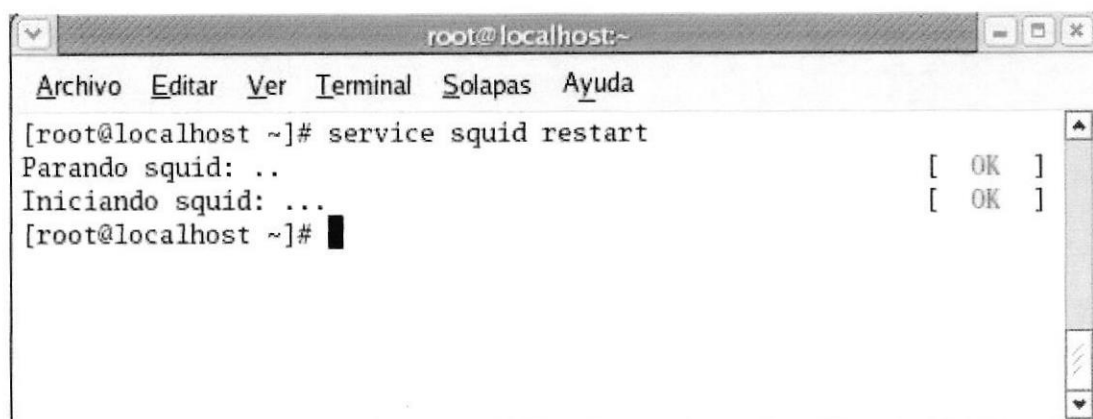


FIGURA 6 - 160: Reiniciar servicio squid

Luego de haber levantado el servicio squid, se procedera a abrir el explorador de Windows para cargar la pagina.

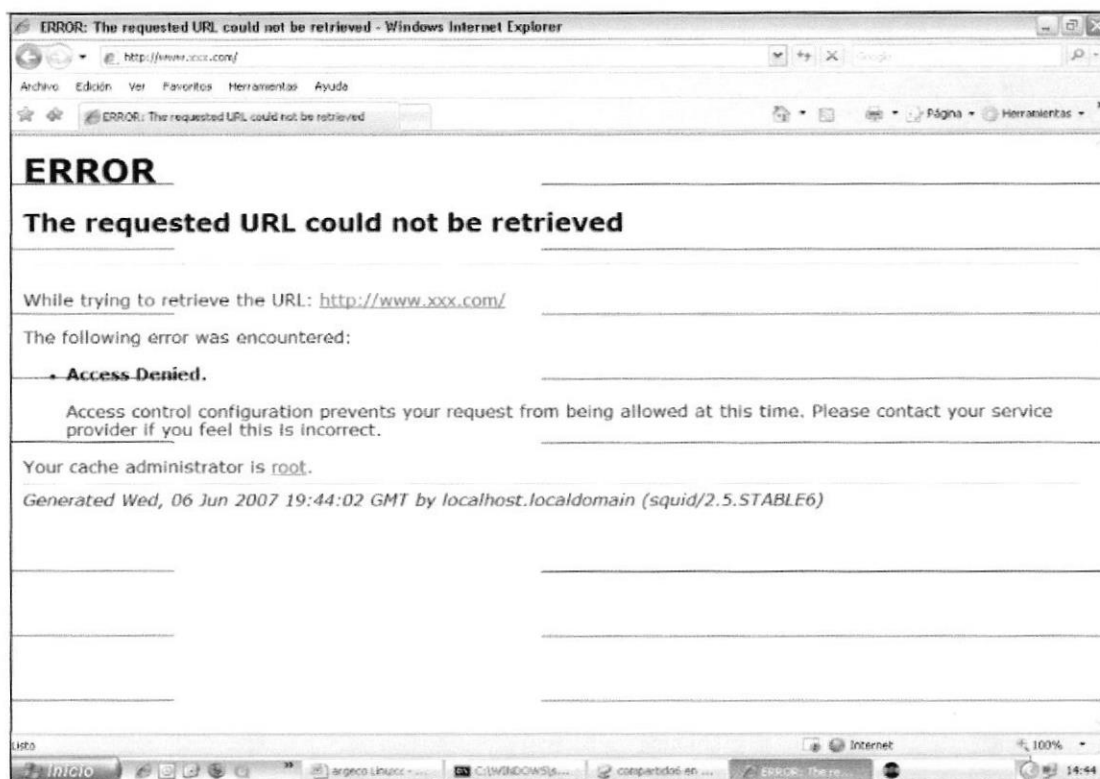
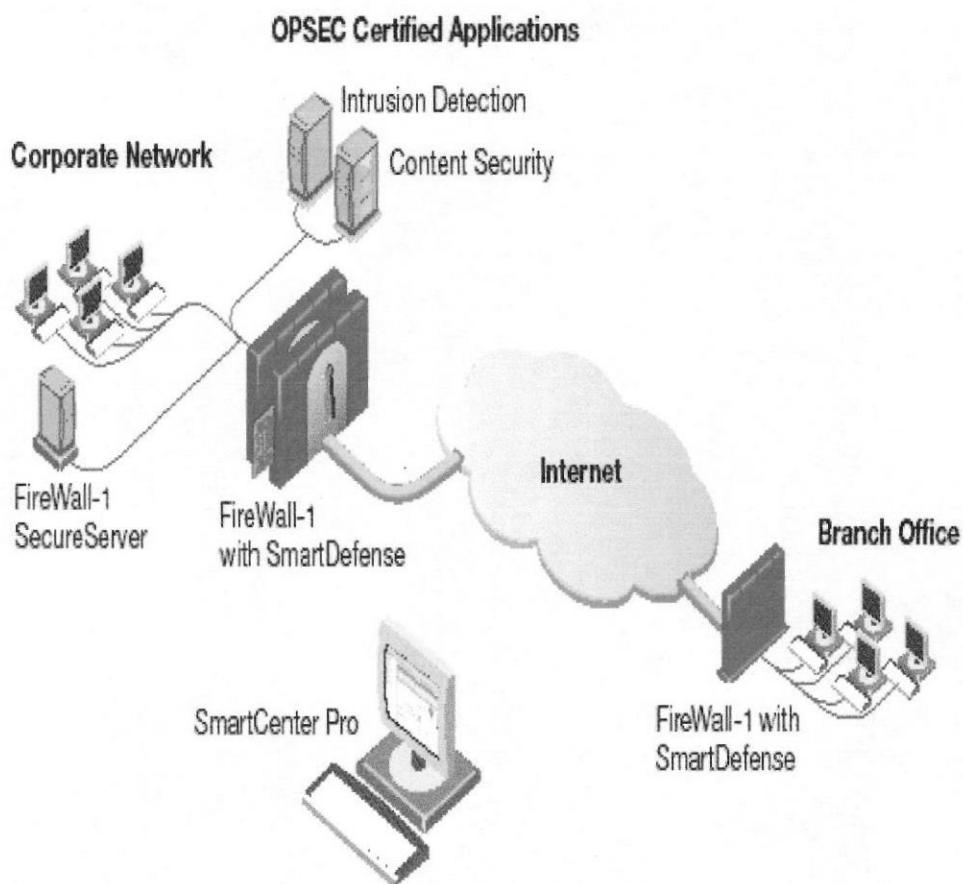


FIGURA 6 - 161: Prueba exitosa de páginas prohibidas



## 6.15.- CONFIGURACIÓN DE FIREWALL



**FIGURA 6 - 162:** Servidor Firewall

Un firewall se utiliza primariamente para separar y controlar la actividad entre redes, como por ejemplo entre su red interna e Internet.

Puede querer tener control sobre los servicios de su red que pueden ser vistos desde afuera, así como también ser notificado si alguna máquina de su red local empieza a enviar paquetes innecesarios al exterior.

Por otro lado, con un firewall Linux entre dos redes tiene la posibilidad de gerenciar el ancho de banda de una forma eficiente en una etapa posterior, mejorando los tiempos de respuesta de sus servicios.

Por último vale aclarar que si bien muchos ataques a su servidor puede ser originados en Internet, la estadística demuestra que muchos de estos ataques provienen de la red interna de la empresa. Un firewall ayuda minimizar estos riesgos.

### **6.15.1.- CARACTERÍSTICAS DE UN FIREWALL LINUX**

#### **Filtrado a nivel de Núcleo**

El filtrado de paquetes en Linux se hace a nivel de núcleo. No es una aplicación corriendo sobre él como en otras plataformas. Esto de por sí ya le da una cualidad de seguridad sobresaliente respecto a otras opciones, así como un elevado rendimiento.

#### **Requerimientos de Hardware**

Los requerimientos de hardware para realizar esta tarea son mínimos. El límite está en el throughput del bus.

#### **Flexibilidad**

Los firewalls comerciales, denominados "por hardware", usualmente son vistos como cajas negras por sus propietarios. Un firewall Linux es totalmente flexible y adaptable a las necesidades particulares de cada situación.

#### **Economía**

No hay forma más económica y confiable para filtrar paquetes. El costo de instalar un firewall Linux puede ser hasta 10 veces más económico que comprar un firewall por hardware o paquetes de software comerciales.

#### **Herramientas de Administración**

**El filtrado** de paquetes del kernel Linux es realizado mediante el código NetFilter del mismo. Como herramienta de administración se puede utilizar la herramienta IPTables de línea de comandos, o algún front-end gráfico como FWBuilder.

**Logic** no sólo asesora en la instalación y personalización del firewall, sino que además capacita al cliente en las herramientas necesarias (consola o entorno gráfico, según elección) para su posterior administración.

### **6.15.2.- REQUERIMIENTOS PARA CONFIGURAR UN SERVIDOR FIREWALL**

- 1 Pc con Linux Fedora Core 3
- 1 Tarjeta de Red
- Tener una IP Estática
- Tener habilitado los servicios necesarios (iptables).

**filter:** Tabla por defecto, para los paquetes que se refieran a nuestra máquina

**INPUT:** Paquetes recibidos para nuestro sistema

**FORWARD:** Paquetes enrutados a través de nuestro sistema

**OUTPUT:** Paquetes generados en nuestro sistema y que son enviados.

**nat:** Tabla referida a los paquetes enrutados en un sistema con Masquerading .

**PREROUTING:** Para alterar los paquetes según entren

**OUTPUT:** Para alterar paquetes generados localmente antes de enrutar.

**POSTROUTING:** Para alterar los paquetes cuando están a punto para salir.

**mangle:** Alteraciones más especiales de paquetes

**PREROUTING:** Para alterar los paquetes entrantes antes de enrutar.

**OUTPUT:** Para alterar los paquetes generados localmente antes de enrutar.

Para configurar un firewall debemos tener configurado la tarjeta de red en el servidor.

```
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 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 qué pasará cuando un paquete cumpla una regla.

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

### 6.15.3.- COMO BLOQUEAR EL PING

**Iptables -A INPUT -s 200.10.148.0/24 -d 200.10.148.1 -p icmp -j DROP**

**iptables** → Palabra reservada

**-A INPUT** → Agregar

**-s** → Red Origen

**200.10.148.0/24** → Red origen

**-d** → Red Destino

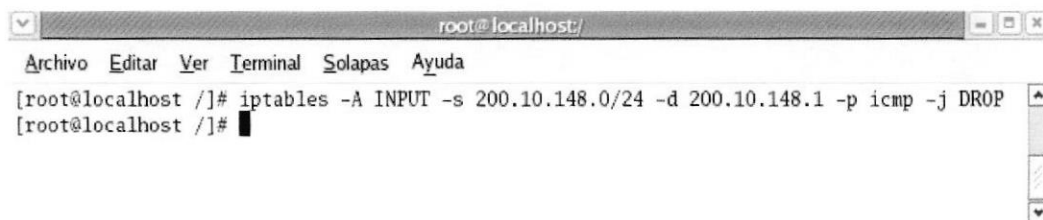
**200.10.148.1** → IP Servidor

**-p** → Protocolo

**icmp** →

**-j** → Acción a aplicar

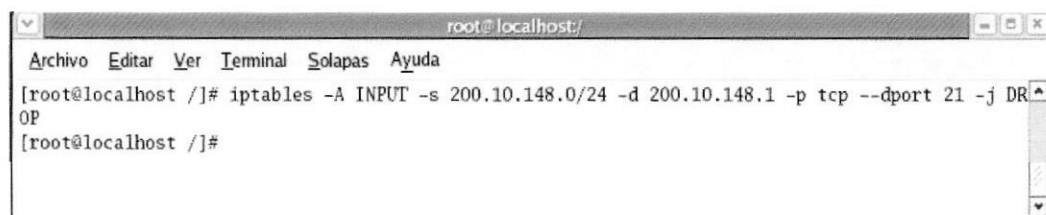
**DROP** → Denegar



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# iptables -A INPUT -s 200.10.148.0/24 -d 200.10.148.1 -p icmp -j DROP  
[root@localhost /]#
```

**FIGURA 6 – 163:** Bloqueo del ping

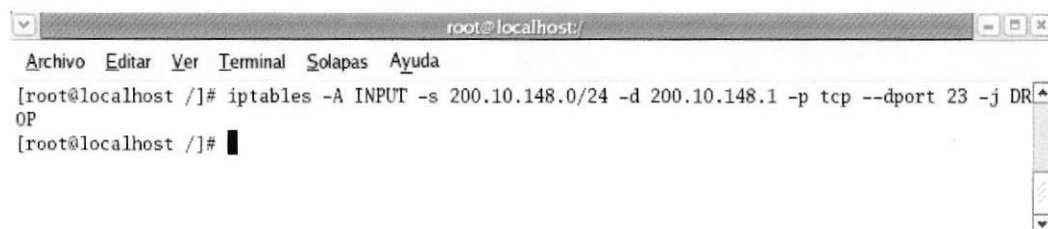
### 6.15.4.- COMO BLOQUEAR FTP



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# iptables -A INPUT -s 200.10.148.0/24 -d 200.10.148.1 -p tcp --dport 21 -j DROP  
[root@localhost /]#
```

**FIGURA 6 – 164:** Bloqueo de ftp

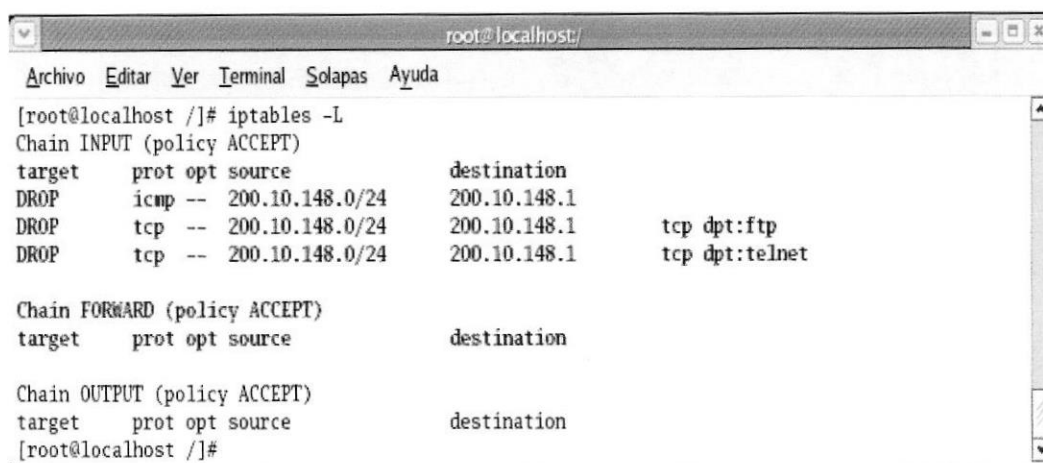
### 6.15.5.- COMO BLOQUEAR TELNET



```
root@localhost:/  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@localhost /]# iptables -A INPUT -s 200.10.148.0/24 -d 200.10.148.1 -p tcp --dport 23 -j DROP  
[root@localhost /]#
```

**FIGURA 6 – 165:** Bloqueo telnet

Para ver si Linux acepto los iptables, en la terminal se escribe el comando iptables -L.



```
root@localhost:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP       icmp -- 200.10.148.0/24        200.10.148.1
DROP       tcp  -- 200.10.148.0/24        200.10.148.1      tcp dpt:ftp
DROP       tcp  -- 200.10.148.0/24        200.10.148.1      tcp dpt:telnet

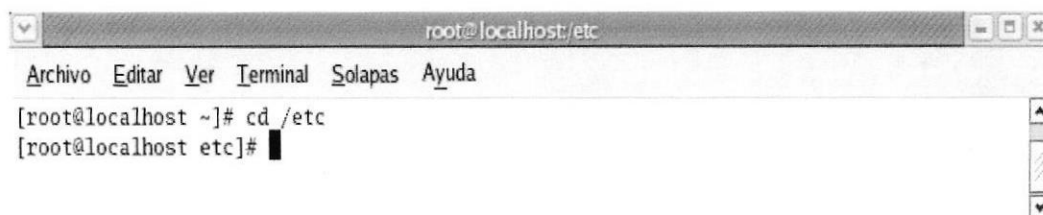
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@localhost /#
```

**FIGURA 6 – 166:** Verificando el estado de Telnet

#### 6.15.6.- HABILITAR TELNET

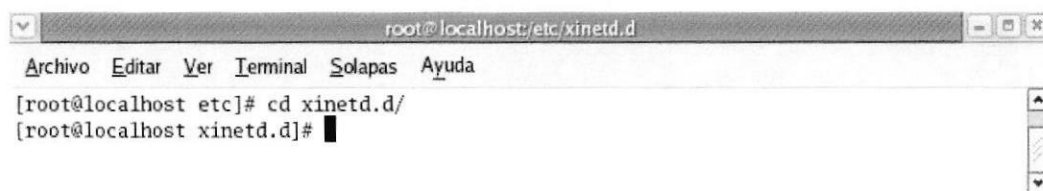
Para poder habilitar el telnet, se entrara al directorio /etc/ de la siguiente manera.



```
root@localhost/etc
[root@localhost ~]# cd /etc
[root@localhost etc]#
```

**FIGURA 6 – 167:** Ingresar al directorio cd /etc

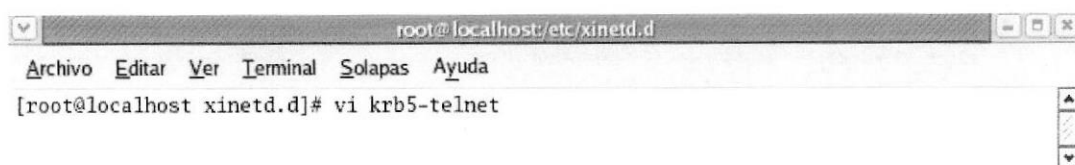
Luego dentro del directorio etc, se procederá a ingresar al directorio xinetd.d para editar el archivo krb5-telnet.



```
root@localhost/etc/xinetd.d
[root@localhost etc]# cd xinetd.d/
[root@localhost xinetd.d]#
```

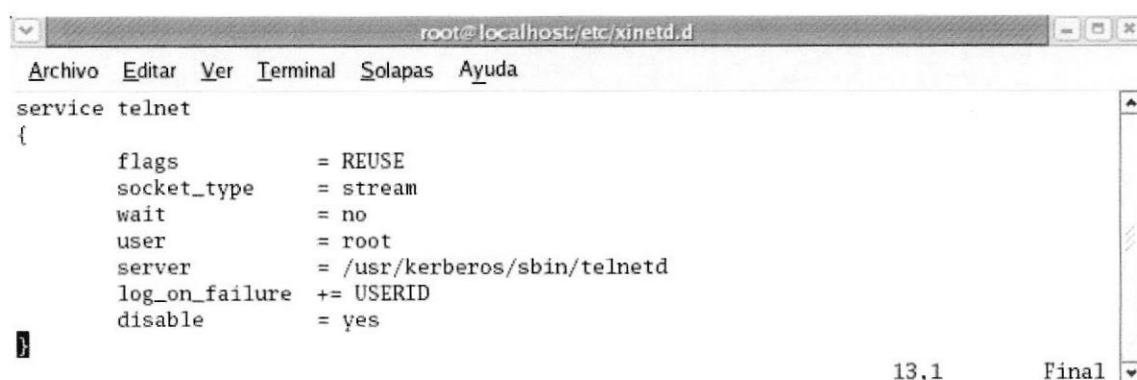
**FIGURA 6 - 168:** ingresar al directorio cd xinetd.d/

En este caso de editara el archivo krb5-telnet con el comando vi.



**FIGURA 6 - 169:** Ingresar a la ruta kbr5-telnet

Después de haber ingresado al archivo de configuración de telnet se procederá a editar este archivo.



**FIGURA 6 - 170:** Editando servicios telnet



### 6.15.7.- CONFIGURACIÓN EN EL CLIENTE WINDOWS

Dar clic en inicio, luego en ejecutar, nos aparecerá un recuadro del ejecutar



FIGURA 6 - 171: Sesteando ejecutar

En este recuadro escribimos el comando cmd.

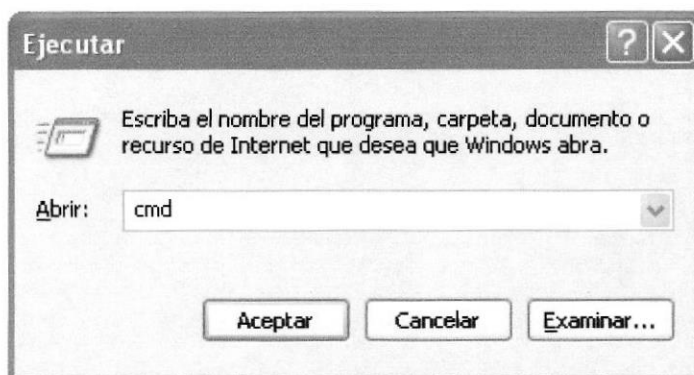


FIGURA 6 – 172: Ingresando a cmd

En el prompt de Windows probar si el cliente puede hacerle ping y telnet al servidor.

**Ping 200.10.148.1**

**Telnet 200.10.148.1**

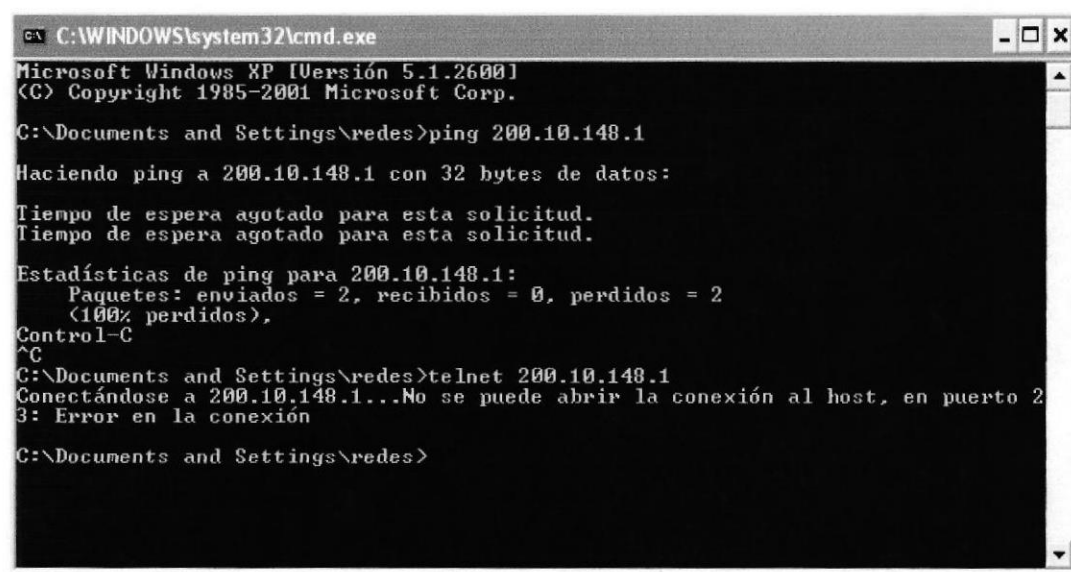


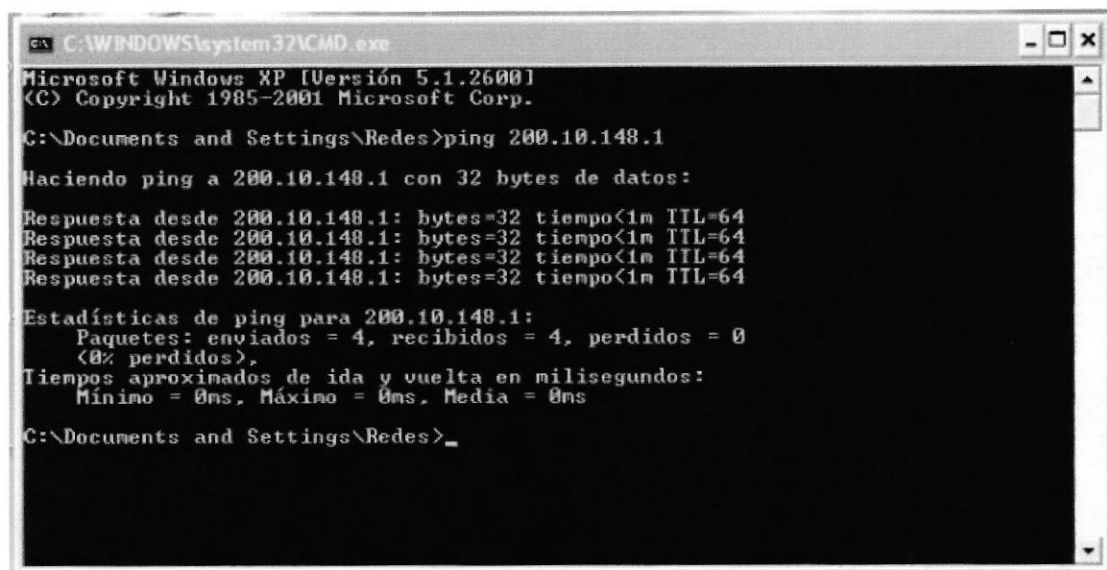
FIGURA 6 - 173: Bloqueo ping y telnet



Acá se puede ingresar al servidor haciendo ping y telnet

**Ping 200.10.148.1**

**Telnet 200.10.148.1**



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

C:\Documents and Settings\Redes>ping 200.10.148.1

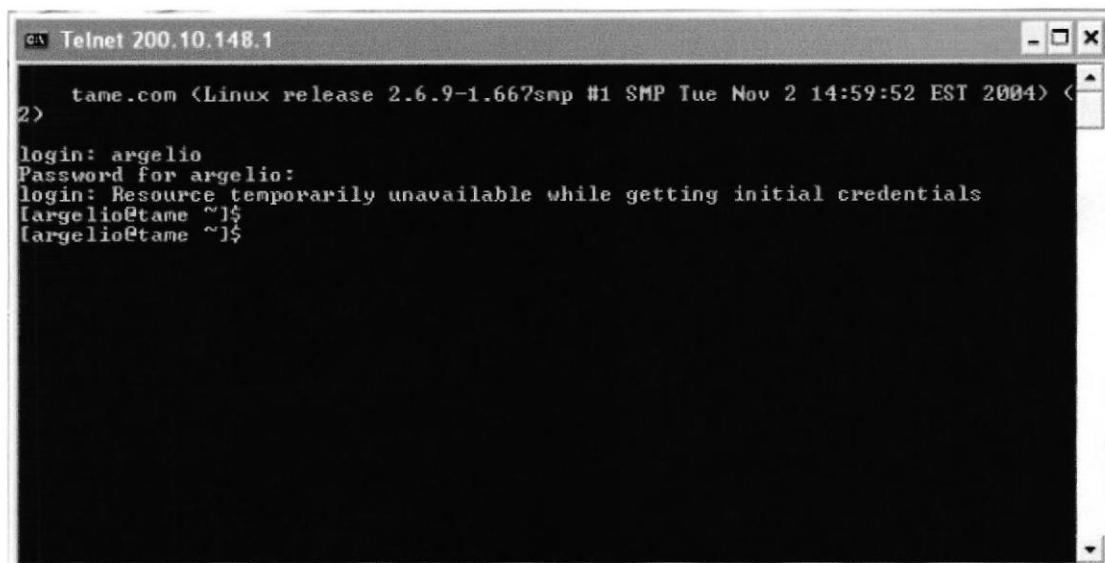
Haciendo ping a 200.10.148.1 con 32 bytes de datos:

Respuesta desde 200.10.148.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 200.10.148.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 200.10.148.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 200.10.148.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 200.10.148.1:
    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\Redes>_
```

**FIGURA 6 - 175:** Habilitado ping



```
Telnet 200.10.148.1

tane.com (Linux release 2.6.9-1.667smp #1 SMP Tue Nov 2 14:59:52 EST 2004) <
2)
login: argelio
Password for argelio:
login: Resource temporarily unavailable while getting initial credentials
[argelio@tane ~]#
[argelio@tane ~]#
```

**FIGURA 6 - 176:** Habilitado telnet

# CAPÍTULO 7

## ROUTERS



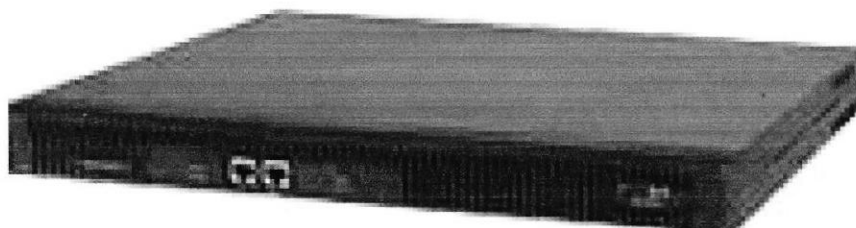
## **7.- ROUTER**

### **7.1.-CONFIGURACIÓN DE DISPOSITIVOS INTRODUCCIÓN A LOS ROUTERS**

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio. Cuenta con un CPU, memoria, bus de sistema y distintas interfaces de entrada/salida. Sin embargo, los routers están diseñados para cumplir algunas funciones muy específicas que, en general, no realizan los computadores de escritorio. Por ejemplo, los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

Al igual que los computadores, que necesitan sistemas operativos para ejecutar aplicaciones de software, los routers necesitan el software denominado Sistema operativo de internetworking (IOS) para ejecutar los archivos de configuración. Estos archivos de configuración contienen las instrucciones y los parámetros que controlan el flujo del tráfico entrante y saliente de los routers. Específicamente, a través de los protocolos de enrutamiento, los routers toman decisiones sobre 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.

#### **7.1.1.-COMPONENTES INTERNOS DEL ROUTER 5232**



**FIGURA 7 - 1: Router**

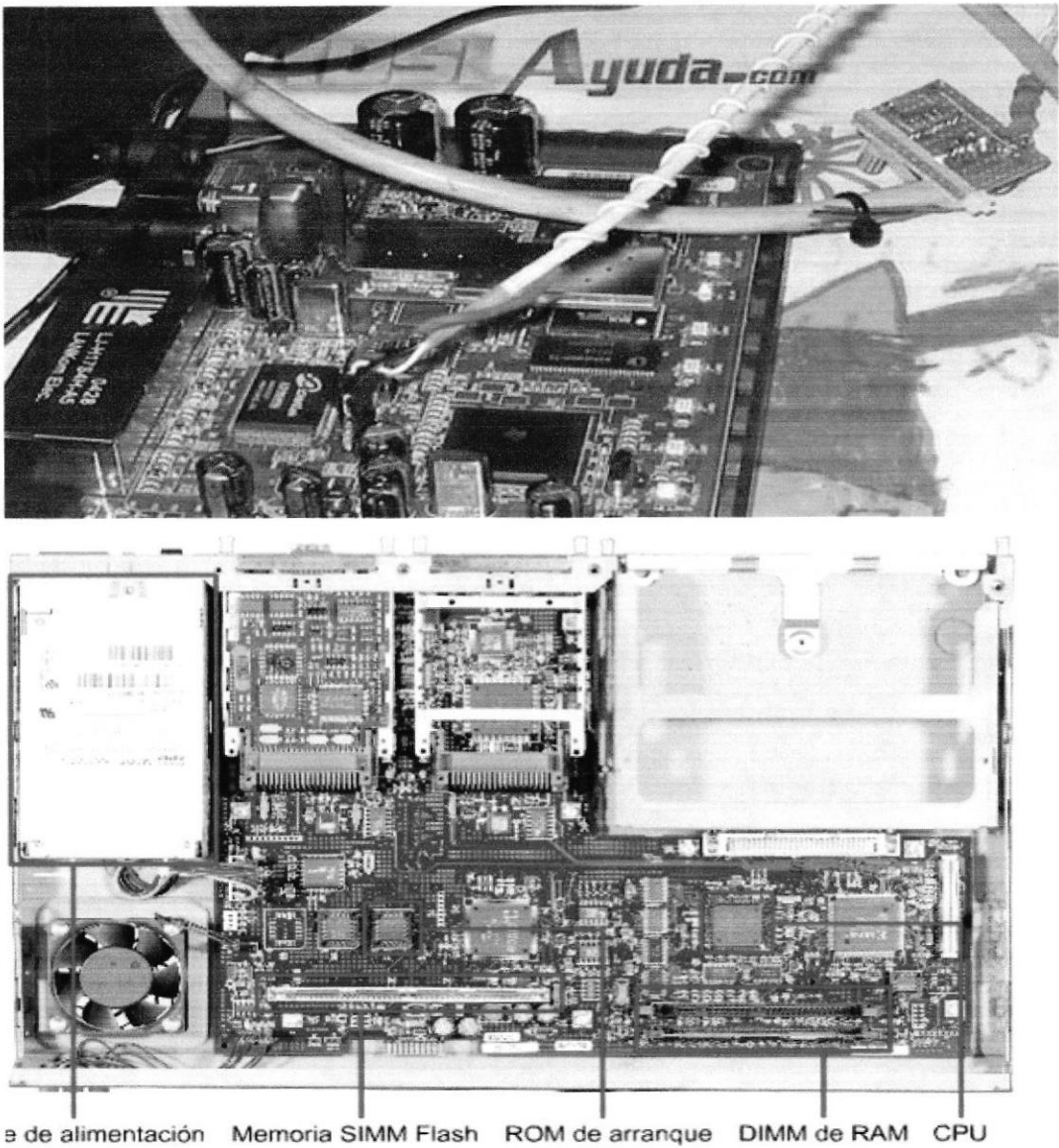


FIGURA 7 - 2: Parte interna

Los principales componentes internos del router son: CPU, la memoria de acceso aleatorio (RAM), la memoria de acceso aleatorio no volátil (NVRAM), la memoria flash, la memoria de sólo lectura (ROM) y las interfaces.

**CPU:** La unidad central de procesamiento. (CPU) ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varias CPU.

**RAM:** La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Por lo general, la RAM se divide de forma lógica en memoria del procesador principal y memoria compartida de entrada/salida (I/O). Las interfaces de almacenamiento temporal de los paquetes comparten la memoria de I/O compartida. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica

Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring. Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser configuraciones fijas o modulares.

Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de configuraciones fijas o modulares.

Las interfaces tienen las siguientes características y funciones:

Conectan el router a la red para permitir que las tramas entren y salgan.

Pueden estar en el motherboard o en un módulo aparte.

**BUSES:** La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces.

**FUENTE DE ALIMENTACIÓN:** La fuente de alimentación brinda la energía necesaria para operar los componentes internos. Los routers de mayor tamaño pueden contar con varias fuentes de alimentación o fuentes modulares. En algunos de los routers de menor tamaño, la fuente de alimentación puede ser externa al router.

o

**(DRAM)** y puede actualizarse agregando más Módulos de memoria en línea doble **(DIMM)**.

Tiene las siguientes características y funciones:

Almacena las tablas de enrutamiento.

Guarda el caché ARP.

Guarda el caché de conmutación rápida.

Crea el buffer de los paquetes (RAM compartida).

Mantiene las colas de espera de los paquetes.

Brinda una memoria temporal para el archivo de configuración del router mientras está encendido.

Pierde el contenido cuando se apaga o reinicia el router.

**NVRAM:** La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

La NVRAM tiene las siguientes características y funciones:

Almacena el archivo de configuración inicial.

Retiene el contenido cuando se apaga o reinicia el router.

**MEMORIA FLASH:** La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los Módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de 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).

**ROM:** La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM en los tomas.

La 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.

**INTERFACES:** Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la



## 7.2.-CONEXIONES EXTERNAS DEL ROUTER

La función de los puertos de administración es diferente a la de las otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red por donde se transmiten los paquetes. El puerto de administración proporciona una conexión basada en texto para la configuración y diagnóstico de fallas del router. Los puertos auxiliares y de consola constituyen las interfaces de administración comunes. Estos son puertos seriales asíncronos EIA-232. Están conectados a un puerto de comunicaciones de un computador. El computador debe ejecutar un programa de emulación de Terminal para iniciar la sesión basada en texto con el router. A lo largo de esta sesión, el administrador de la red puede administrar el dispositivo.

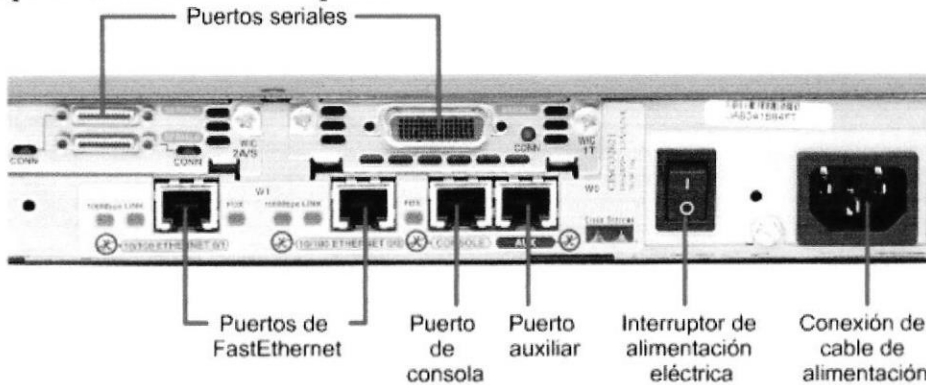


FIGURA 7 - 3: Parte Externa

### **7.3.- CONEXIONES DEL PUERTO DE ADMINISTRACIÓN**

El puerto de consola y el puerto auxiliar (AUX) son puertos de administración. Estos puertos seriales asíncronos no se diseñaron como puertos de networking.

Uno de estos dos puertos es necesario para la configuración inicial del router. Se recomienda el puerto de consola para esta configuración inicial. No todos los routers cuentan con un puerto auxiliar.

Cuando el router entra en servicio por primera vez, los parámetros de networking no están configurados.

Por lo tanto, el router no puede comunicarse con ninguna red. Para prepararlo para la puesta en marcha y configuración iniciales, conecte una Terminal ASCII RS-232 o un computador que emule una

Terminal ASCII Terminal al puerto de consola del sistema. Entonces, se podrán ingresar los comandos de configuración para poner en marcha el router.

Una vez que la configuración inicial se ha introducido en el router a través del puerto de consola o auxiliar, entonces, se puede conectar el router a la red para realizar un diagnóstico de fallas o monitoreo.

Además, el router puede configurarse desde un lugar remoto haciendo telnet a una línea de Terminal virtual o marcando el número de un módem conectado al puerto de consola o auxiliar del router.

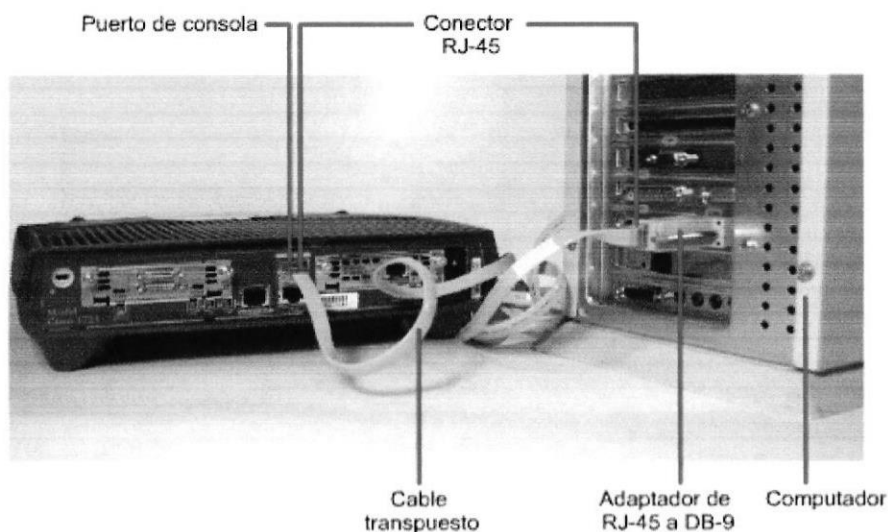
El puerto de consola es un puerto de administración que se utiliza para proveer acceso al router fuera de banda.

Se usa para la configuración inicial de router, el monitoreo y los procedimientos de recuperación de desastres.

Para realizar la conexión al puerto de consola, se usa un cable transpuesto o de consola y un adaptador **RJ-45 a DB-9** para conectarse al PC.

Para conectar una Terminal al puerto de consola del router, conecte la Terminal mediante un cable transpuesto **RJ-45 a RJ-45** y un adaptador **RJ-45 a DB-9 o RJ-45 a DB-25**.





**FIGURA 7 - 4:** Conexión a la Terminal

Generalmente para que se pueda configurar un router el administrador del equipo debe ingresar a una interfaz de usuario, el acceso a ésta puede ser mediante una Terminal o accensando remotamente.

## **7.4.-ENRUTAMIENTO**

### **7.4.1.-ENRUTAMIENTO ESTÁTICO**

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.

Para verificar la distancia administrativa de una ruta en particular use el comando `show ip route address`, donde la dirección ip de dicha ruta se inserta en la opción `address`. Si se desea una distancia administrativa diferente a la distancia por defecto, se introduce un valor entre 0 y 255 después de la interfaz de salida.

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta. A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

◦

## 7.4.2.- ENRUTAMIENTO DINÁMICO

### 7.4.2.1.- PROTOCOLOS DE ENRUTAMIENTO

Un protocolo de enrutamiento es el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.

Ejemplos de protocolos de enrutamiento:

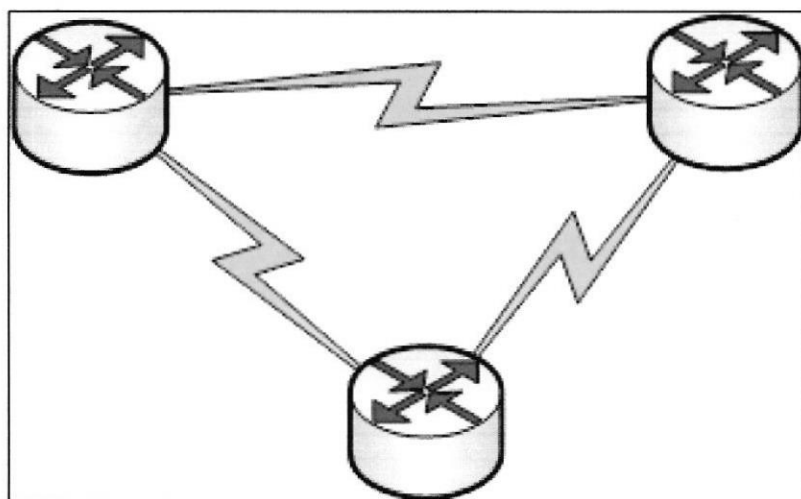
Protocolo de información de enrutamiento (RIP).

Protocolo de enrutamiento de gateway interior (IGRP).

Protocolo de enrutamiento de gateway interior mejorado (EIGRP).

Protocolo "Primero la ruta más corta" (OSPF).

Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.



**FIGURA 7 - 5:** Esquema De Comunicación

7.5.-CONFIGURACIÓN DEL HYPERTERMINAL

Se lo explica con los siguientes PASOS:

1.- Abrir el Hyperterminal de la siguiente manera



FIGURA 7 - 6: Abrir hiperterminal

2.- Hacer clic en inicio--Escoger la opción accesorios-- Luego hacer click en comunicación—luego hacer click en Hyperterminal, nueva conexión HyperTerminal



FIGURA 7 - 7: Nueva conexión

3.- Al abrir el hyperterminal, se dará la opciones de crear una nueva conexión, le poner un nombre que identifique la BBS, por ejemplo 'TAME' y elegir el icono que le guste.



FIGURA 7 - 8: Conexión TAME

4.- En esta pantalla elegimos el puerto para conectar el router con el cable rollover, cabe indicar que puede conectarse mediante el com1, com2, com3 dependiendo el tipo de conexión que tenga la PC.

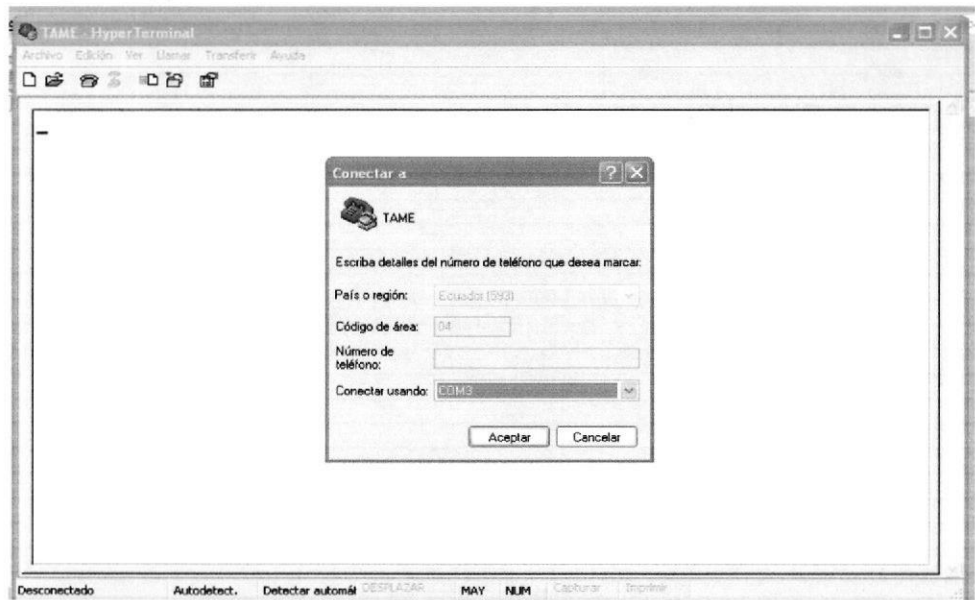


FIGURA 7 - 9: Conexión cable rollover

5.- A continuación deberá configurar los bits, pero tiene que restablecer la tabla.

En la siguiente pantalla encontrara algunos parámetros de conexión de los cuales deberá establecer y dar clic en el botón Aceptar.

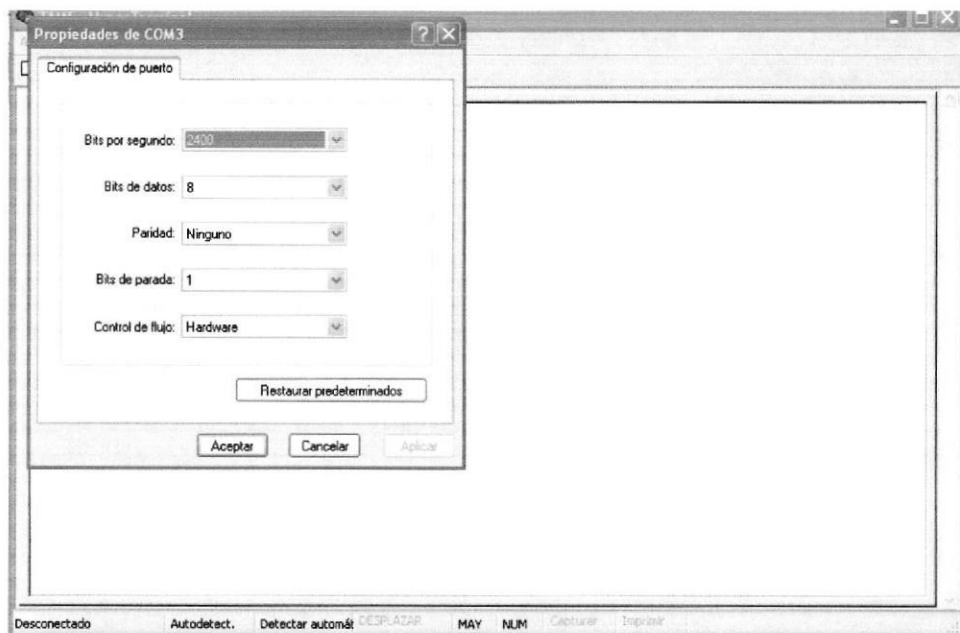
9600 bps. (Velocidad de transmisión del cable serial de conexión

8 bits de Datos (configuración de los procesamientos de datos al pasar al Hyperterminal en bits por segundo)

Ninguno (paridad) (utilizado para comprobar errores en el grupo de bits de datos transferidos entre uno o varios equipos)

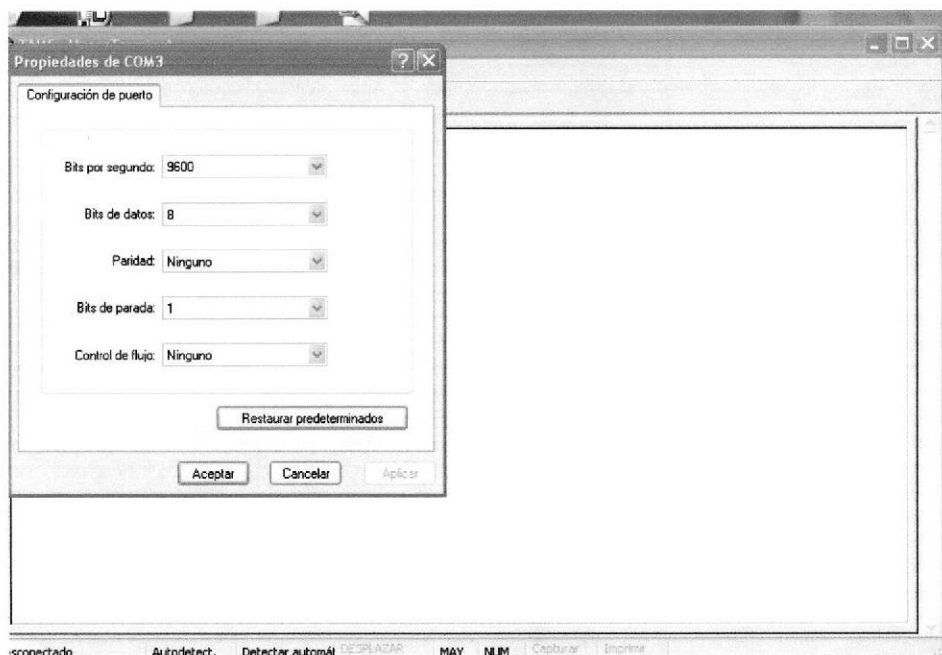
1 (bit de parada) (medida de transporte por la que pasan datos al Hyperterminal)

Ninguno control del flujo (se refiere a la información que viaja)



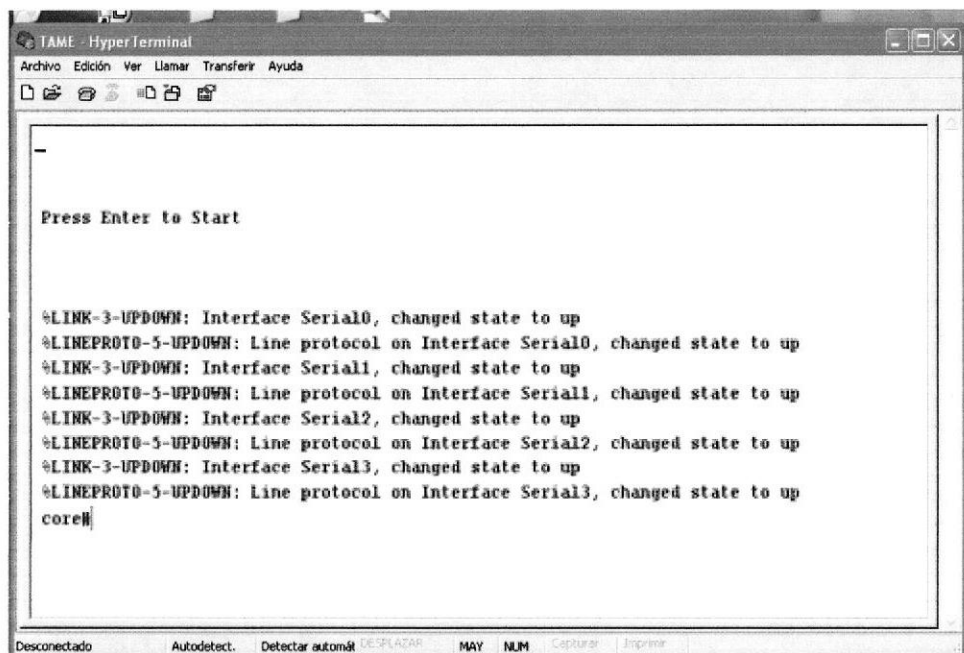
**FIGURA 7 - 10:** Configurar los bits

6.- Después haber restablecido configuramos los bits



**FIGURA 7 - 11:** Configurar los bits

7.- Una vez configurado el HYPERTERMINAL nos aparecerá una ventana donde allí poder configurar y monitorear los router; en el siguiente grafico nos dará una idea de cómo sería la pantalla de inicio del HYPERTERMINAL.



**FIGURA 7 - 12:** Monitoreando el router

## 7.6.-CONFIGURACIONES EN EL ROUTER

### 7.6.1.-MODOS DE INTERFAZ DE USUARIO

La interfaz de línea de comando (CLI) de Cisco usa una estructura jerárquica. Esta estructura requiere el ingreso a distintos modos para realizar tareas particulares. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces. Desde el modo de configuración de interfaces, todo cambio de configuración que se realice, tendrá efecto únicamente en esa interfaz en particular.

El IOS suministra un servicio de intérprete de comandos, denominado comando ejecutivo (EXEC). Luego de ingresar un comando, el EXEC lo valida y ejecuta.

Como característica de seguridad, el software Cisco IOS divide las sesiones EXEC en dos niveles de acceso. Estos niveles son el modo EXEC usuario y el modo EXEC privilegiado. El modo EXEC privilegiado también se denomina el modo enable. Las siguientes son las características resaltantes del modo EXEC usuario y del modo EXEC privilegiado:

El modo EXEC usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo "de visualización solamente". El nivel EXEC usuario no permite ningún comando que pueda cambiar la configuración del router. El modo EXEC usuario se puede reconocer por la petición de entrada: ">".

El modo EXEC privilegiado da acceso a todos los comandos del router. Se puede configurar este modo para que solicite una contraseña del usuario antes de dar acceso. Para ingresar al modo de configuración global y a todos los demás modos específicos, es necesario encontrarse en el modo EXEC privilegiado. El modo EXEC privilegiado se puede reconocer por la petición de entrada "#".

Para ingresar al nivel EXEC privilegiado desde el nivel EXEC usuario, ejecute el comando enable con la petición de entrada ">" en pantalla. Si se ha configurado una contraseña, el router solicitará la contraseña. Por razones de seguridad, los dispositivos de red de Cisco no muestran la contraseña al ser introducida. Una vez que se ha introducido la contraseña correcta, la petición de entrada del router cambia a "#", lo que indica que el usuario se encuentra ahora en el nivel EXEC privilegiado. Si se introduce un signo de interrogación (?) en el nivel EXEC privilegiado, se mostrarán muchas opciones de comando, adicionales a las disponibles en el nivel EXEC usuario.

A continuación veremos un esquema de los diferentes usuarios y los permisos que tiene cada uno:

o



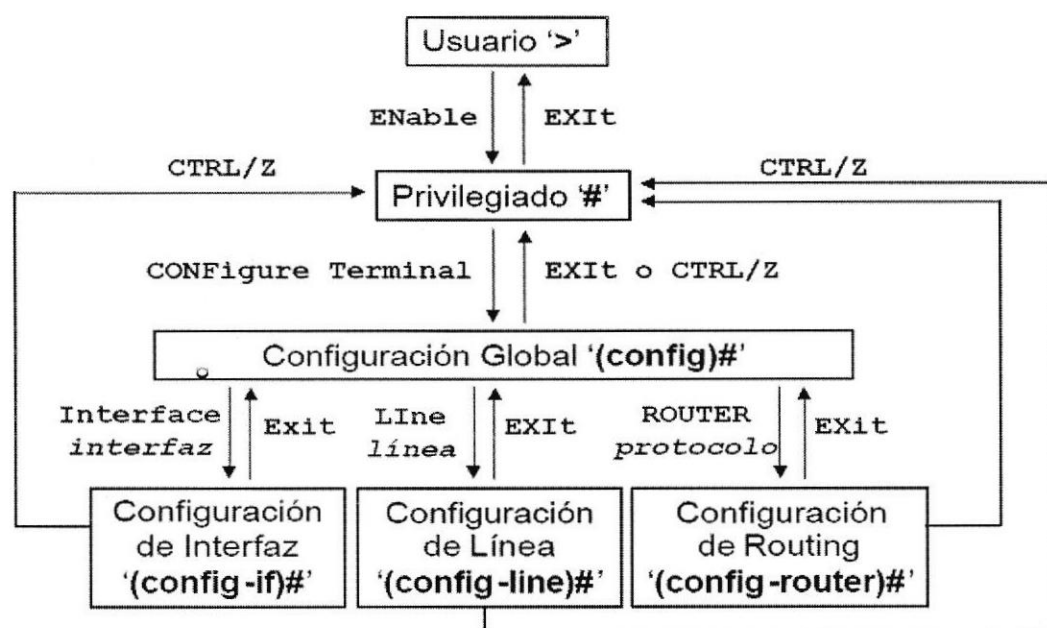


FIGURA 7 - 13: Modo privilegiado

Sólo se puede ingresar al modo de configuración global desde el modo EXEC privilegiado. Los siguientes son modos específicos a los que también se puede ingresar desde el modo de configuración global:

Interfaces

Sub-interfaces

Línea

Router

Mapas de enrutamiento

Para regresar al modo EXEC usuario desde el modo EXEC privilegiado, se pueden ejecutar los comandos disable o exit. Para regresar al modo EXEC privilegiado desde el modo de configuración global, ejecute exit o Control-Z. Control-Z también se puede usar para regresar directamente al modo EXEC privilegiado desde cualquier modo de configuración global secundario.

Para ingresar al modo EXEC privilegiado, escriba enable o su abreviatura ena. Esto puede hacer que el router pida al usuario una contraseña, que se haya fijado con anterioridad.

o

**7.6.2.- COMANDOS BASICAS**

show history	Muestra un historial de los comandos ingresados.
show flash	Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados
show interfaces	Muestra las estadísticas completas de todas las interfaces del router.
show controllers	Ver los enlaces DCE/DTE que usa el router.
show users	Muestra los usuarios conectados al router.
show ip route	Verifica la tabla de enrutamiento.
show version	Despliega la información acerca del router de la imagen de IOS que esté corriendo en la RAM
show ARP	Muestra la tabla ARP del router
show protocols	Muestra el estado global de las interfaces.
show startup-configuration	Muestra el archivo de configuración almacenado en la NVRAM.
show running-configuration	Muestra el contenido del archivo de configuración activo.
configure terminal	Ingreso al modo de configuración global
interface serial	Ingreso al modo de configuración de interfaz serial.
interface fastethernet	Ingreso al modo de configuración de interfaz fastethernet.
ip address	Especifique la dirección de la interfaz y la máscara de subred.
no ip address	Dar de baja a la dirección ip asignada.
clock rate	Fija la velocidad de sincronización.
enable secret	Habilitar la clave en forma encriptada. No se muestra en el show run
enable password	Habilita la clave en forma cifrada.
shutdown	Dar de baja a la interfaz
exit	Salir en forma progresiva.
Ctrl.Z	Salir del modo privilegiado de forma rápida.
wr	Guardar los cambios en la NVRAM de forma rápida.
erase running startup -config	Borrar la configuración activa.
no shutdown	Levanta la interfaz.
line console 0	Comando para ingresar al modo de configuración del puerto consola.
login	Habilita la opción de introducir un

	usuario.
password [xxx]	Configura el password de acceso.
line vty 0 4	Comando para ingresar al modo de configuración de las terminales virtuales (sesiones telnet).
bandwidth	Configura el parámetro ancho de banda (en Kb) que utilizan los protocolos de enrutamiento en el cálculo de la métrica. No tiene relación real con el.

**Tabla 7 - 1:** Comandos básicos de Router

Ahora se les va a explicar como realizar configuraciones usando los comandos anteriormente explicados.

#### 7.6.4.- GUARDAR CAMBIOS DEL 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 a RAM del router llamado **running – config**.

Para poder ver su contenido se debe ejecutar el comando **show running-config**.

Si se tuviese que reiniciar el router por A o B motivos lo que estaba guardado en el **running-config** se perdería, para evitar eso se hace una copia del running-config al startup-config. Ello se puede hacer desde el modo Privilegiado con el siguiente comando:

Router#copy running-config startup-config

Copia de la configuración actual al archivo de arranque

Destination filename [startup-config]?

Archivo de destino

Building configuration ...

Guardando configuración

[OK]

### 7.6.5.- CONFIGURAR NOMBRE DE ROUTERS

Una de las configuraciones mas básicas es asignar un nombre al router lo cual ayuda a una mejor administración de la red al identificar de manera única los routers dentro de nuestra red.

Esta configuración se la realiza en el modo de configuración Global con el **comando hostname** de la siguiente manera

Router>

**Router> enable**

Acceso al modo privilegiado.

**Router# configure terminal**

Entra al modo de configuración global.

Router(config)#hostname TAME

Asigna el nombre del Router

TAME(config)#exit

Sale de la configuración global.

TAME#

### 7.6.6.- CONFIGURACION DE CONTRASEÑAS EN EL ROUTER

Se puede restringir el acceso al router estableciendo contraseñas tanto para la consola como para la terminal.

El **line console 0** debe utilizarse para establecer una contraseña de conexión en el terminal de consola.

El modo de configuración **line vty 0 4** sirve para establecer una contraseña de conexión en sesiones **TELNET** entrantes.

Router# configure terminal

Entra al modo de configuración global.

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

**Router#conf ter**

Enter configuration commands, one per line. End with CNTL/Z.

**Router(config)#line console 0** consola

**Router(config-line)#password cisco** contraseña

**Router(config-line)#login** login para la contraseña

**Router(config)#line vty 0 4** terminal virtual

**Router(config-line)#password cisco** contraseña

**Router(config-line)#login** login para la contraseña

**Router(config-line)#enable password cisco** habilitar contraseña

Sugerencia:

Cada password debe tener un mínimo de cuatro caracteres y máximo de ocho caracteres

### 7.6.7.- ASIGNACION DE IP'S A LAS INTERFACES

La Asignación de las **IP'S** es uno de los pasos primordiales junto con la asignación de los protocolos para establecer comunicación.

La forma de asignar las IP es la misma tanto en routers como en switches, se aplica el comando **interface serial / interface ethernet /interface fastethernet(A)**, en donde **A es el numero de la interfaz**, entramos a la interface y con el comando **ip address (dir) (mask)** asignamos la dirección donde dir es la dirección IP y mask es la mascara de subred.

Después de asignar la IP se asigna un Clock rate dependiendo si es DCE o DTE, para después ejecutar el comando **no shutdown** para que la interfaz se levante.

Router# configure terminal

Entra al modo de configuracion global.

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuracion global y que se presiona CTRL+Z para salir.

Router(config)#interface serial 0/0

Se ingresa a la interfaz a configurar

o

Router(config-if)#ip address 192.168.9.9 255.255.255.252

Se asigna la dirección IP y la mascara de subred que es 252 ya que es la dirección de un router

Router(config-if)#clock rate 64000

Velocidad de sincronización con los demas router

Router(config-if)#no shutdown

Comando para levantar la interfaz

%LINK-3-UPDOWN: Interface Serial0/0, changed state to up

Indica la interfaz que se ha levantado

Router(config-if)#

o

### 7.6.8.- CONFIGURACION DE PROTOCOLOS

Un protocolo de enrutamiento define el conjunto de reglas utilizadas por un router cuando este se comunica con los routers vecinos. Existen dos tipos:

#### 7.6.9.- VECTOR DISTANCIA:

Aprende la mejor ruta a la red de destino basándose en la acumulación de la métricas de cada vecino.

#### 7.6.10.- ESTADO ENLACE:

Aprende la Topología exacta de la red entera. Mantiene una compleja información de la Topología. Es utilizado para crear una imagen común de la red entera. Utiliza notificaciones del "Vecindario".

#### 7.6.11.-COMADOS SHOWS

Los numerosos comandos show se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas.

Show interfaces serial	Muestra la estadística completa del router
Show controllers serial	Muestra la información del hardware
Show clock	Muestra la hora fijada en el router.
Show hosts.	Muestra la lista en cache de los nombres de host y sus direcciones.
Show users.	Muestra a todos los usuarios conectados al router.
Show versión.	Despliega la información acerca del router y de la versión del IOS que este corriendo en la RAM.
Show protocols.	Muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.
Show running	Muestra el archivo de configuración almacenado en la NVRAM.
Show ip route.	Muestra las interfaces por las que se llega a otras redes mediante los protocolos de enrutamiento ej: O:ospf, R:rip, C: directamente conectado
Show vlans.	Muestra todas las vlans creadas con sus respectivos puertos asignados.

**Tabla 7 - 2:** Comandos Show

## 7.7.- PROTOCOLOS DE ENRUTAMIENTOS

Un aspecto fundamental en las redes de conmutación de paquetes es el encaminamiento y los algoritmos que para él se emplean. A lo largo de las clases teóricas, se han diferenciado dos técnicas para los mismos (por vector distancia y por estado del enlace) y se han analizado dos de los posibles algoritmos de camino más corto. En este manual, observaremos cómo funcionan dos de los protocolos de enrutamiento que se utilizan en IP (**R.I.P.** y **O.S.P.F.**).

El primero de ellos será un protocolo de vector distancia

El segundo lo será de estado del enlace. Que no nos permitirá observar cómo se crean las tablas de rutas de los routers de la red, ni cuál es la información intercambiada entre los mismos, pero sí se podrá comprobar como es posible encaminar los paquetes en función de distintos criterios.

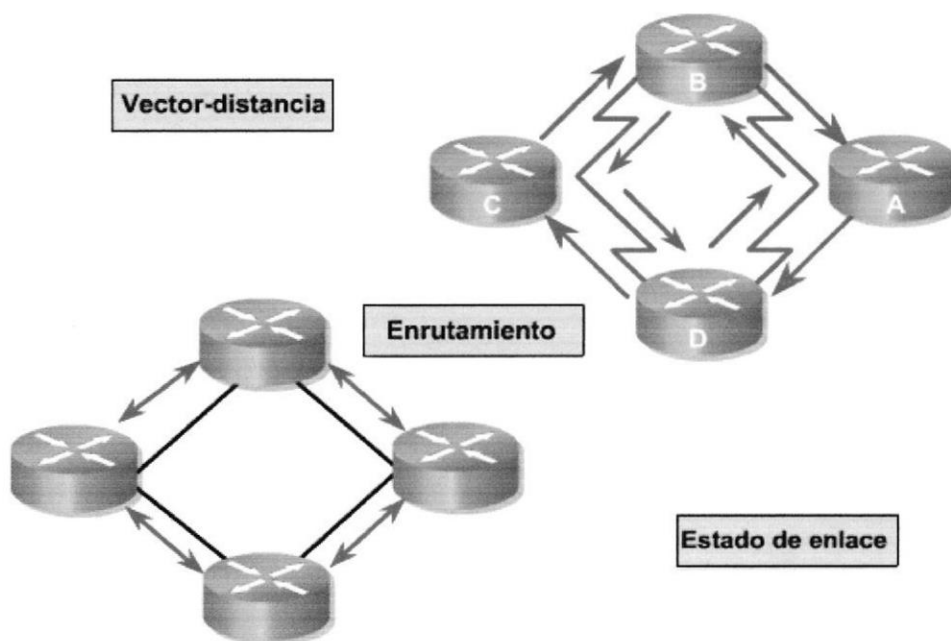


FIGURA 7 - 14: Ospf

### 7.7.1.-PROTOCOLO DE ENRUTAMIENTO OSPF

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). El término "libre" en "Primero la ruta libre más corta" significa que está abierto al público y no es propiedad de ninguna empresa.

OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes. Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento.



- 1.1 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.
- 1.2 OSPF ofrece soluciones a los siguientes problemas:

Velocidad de convergencia.

Admite la Máscara de subred de longitud variable (VLSM).

Tamaño de la red.

Selección de ruta.

Agrupación de miembros

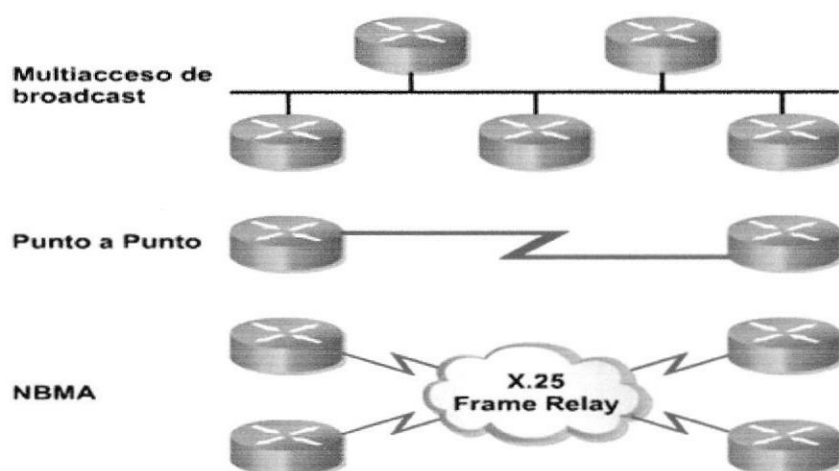
#### 7.7.1.1.-TIPOS DE REDES OSPF

- 1.3 Las interfaces OSPF reconocen tres tipos de redes:

Multiacceso de broadcast como por ejemplo Ethernet.

Redes punto a punto.

Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay.



**FIGURA 7 - 15:** Ospf



### 7.7.1.2.- PROTOCOLO HELLO DE OSPF

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete hello y sigue enviando hellos a intervalos regulares. Las reglas de intercambio de paquetes hello de OSPF se denominan protocolo Hello.

En la capa 3 del modelo OSI, los paquetes hello se direccionan hacia la dirección multicast 224.0.0.5. Esta dirección equivale a "todos los routers OSPF". Los routers OSPF utilizan los paquetes hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los Hellos se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes NBMA, como por ejemplo Frame Relay, el tiempo por defecto es de 30 segundos.

En las redes multiacceso el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR). El paquete hello transmite información para la cual todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

La configuración de OSPF requiere que el proceso de enrutamiento OSPF esté activo en el router con las direcciones de red y la información de área especificadas.

- 1.4 Para habilitar el enrutamiento OSPF, utilice la sintaxis de comando de configuración global:

```
Router (config) #router ospf 1
```

El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en el router. Se pueden iniciar varios procesos OSPF en el mismo router. El número puede tener cualquier valor entre 1 y 65.535.

Las redes IP se publican de la siguiente manera en OSPF:

```
Router (config-router) #network address wildcard-mask area area-0
```

**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.

## 7.8.- OSPF (PROTOCOLO ESTADO ENLACE):

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

Router# configure terminal

    Entra al modo de configuración global.

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router(config)# router ospf 1

    Protocolo a configurar

Router(config-router)#network 192.168.9.12 0.0.0.3 area 0

    Red que aprende con la respectiva wildcard y el área en que se encuentran

Router(config-router)#

◦

## 7.9.- REDISTRIBUCION DE RUTAS

En los esquemas Wan es muy probable tener áreas con protocolos diferentes, en estos casos se aplica lo que se conoce como redistribución de rutas de un protocolo como por ejemplo RIP versión 2 hacia un protocolo diferente como OSPF.

Para poder realizar este proceso se debe ejecutar el comando redistribuye protocolo donde protocolo es el protocolo que vamos a inyectar dentro del que estamos configurando

Router# configure terminal

Entra al modo de configuración global.

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router(config)# router ospf 1

Protocolo a configurar

Router(config-router)#network 192.168.9.12 0.0.0.3 area 0

Red que aprende con la respectiva wildcard y el área en que se encuentran

Router(config-router)#network 192.168.9.20 0.0.0.3 area 0

Red que aprende con la respectiva wildcard y el área en que se encuentran

Router(config-router)#redistribute rip

Redistribución de protocolos

Router(config-router)#exit

Sale de modo configuración global

Router# configure terminal

Entra al modo de configuración global.

Router(config)#

Router(config)# router rip

Protocolo a configurar

Router(config-router)#version 2

Version del Protocolo

Router(config-router)#network 192.168.9.8

Red que aprende

Router(config-router)#redistribute ospf 1

Redistribución de protocolos

Router(config-router)#exit

Sale de modo configuración global

## 7.10.-PROTOCOLOS RIP

Uno de los protocolos de routing más antiguos es el Routing Information Protocol o más comúnmente llamado RIP. Utiliza algoritmos de vector distancia para calcular sus rutas. Este tipo de algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

Los protocolos vector distancia fueron descritos académicamente por: R.E. Bellman, L.R. Ford Jr y D.R. Fulkerson.

La primera organización que implementó un protocolo de vector distancia fue la compañía Xerox en su protocolo GIP (Gateway Information Protocol), este protocolo estaba incluido dentro de la arquitectura XNS (Xerox Network Systems). GIP se utilizaba para intercambiar información de routing entre redes o sistemas autónomos no adyacentes. Pero claro, Xerox había implementado su propio protocolo propietario.

Poco después la University of California en Berkeley creo una variante llamada "routed", esta variante del GIP introdujo novedades como modificación del campo de direccionamiento, que se consiguió más flexible, también se añadió un temporizador que limitaba a 30 segundos el tiempo máximo de actualización, es decir, el tiempo máximo permitido sin saber la información de los vecinos, y por supuesto se integró dentro de UNIX, con lo cual pasó a ser abierto.

RIP es un protocolo de routing de vector distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies. RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto. RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace

### 7.10.1.-VERSIONES RIP

**RIP v1.-** No soporta subredes ni CIDR. Tampoco incluye ningún mecanismo de autenticación de los mensajes. No se usa actualmente. Su especificación está recogida en el RFC 1058

**RIP v2.-** Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes mecanismos: no autenticación mediante contraseña autenticación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). Su especificación está recogida en el RFC 1723-2453.

**RIP ng.-** RIP para IPv6. Su especificación está recogida en el RFC 2080

También existe un RIP para IPX; casualmente lleva el mismo acrónimo, pero no está directamente relacionado con el RIP para redes IP, ad-hoc.

### 7.10.2.-CARACTERÍSTICAS

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).

### 7.10.3.-MÁSCARA DE RED DE RIP

La característica de máscara de red de rip está soportada para ambas versiones, la 1 y la 2.

### 7.10.4.-VERSIÓN 1 DE RIP

Originalmente no contenía información de la máscara. En la versión 1 de RIP, las clases eran utilizadas originalmente para determinar el tamaño de la máscara. Las redes de Clase A utilizaban 8 bits para la máscara, las redes de Clase B utilizaban 16 bits para la máscara, mientras que las redes de Clase C utilizaban 24 bits para la máscara. Actualmente, el método más utilizado para el tamaño de la máscara de un paquete consiste en asignar al paquete la máscara en base al interfaz que recibió el paquete.

### 7.10.5.-VERSIÓN 2 DE RIP

Soporta la máscara de subred de tamaño variable length subnet mask (VLSM). Extendiendo la submáscara de red, la máscara puede ser dividida y puede reusarse. Cada subred puede usarse para propósitos diferentes como grandes o medianas LANs y enlaces WAN. El demonio *ripd* de Quagga no soporta las máscaras nosecuenciales, las cuales están incluidas en la especificación de RIP versión 2.

En caso de existir información similar con el mismo prefijo y métrica, la información antigua será eliminada. Rip actualmente no soporta rutas multipath con el mismo coste.

### 7.10.6.-VENTAJAS Y DESVENTAJAS DE RIP

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

**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

### 7.10.7.-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.

El Protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento por vector-distancia. Cuenta el numero de "Saltos" (routers que debe atravesar en la ruta hasta el destino), para determinar la mejor ruta. Se encuentra más de un enlace a la misma red de destino con la misma métrica, automáticamente realiza balanceo de carga. RIP puede realizar balanceo de carga en hasta 6 enlaces de igual métrica

Capacidad para transportar mayor información relativa al enrutamiento de paquetes. Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de las tablas. Soporta enmascaramiento de subredes de longitud variable (VLSM).

Entre las tareas opcionales se encuentran:

Aplicar compensaciones a la métrica de enrutamiento.

Ajustar los temporizadores.

Especificar una versión de RIP.

Habilitar la autenticación de RIP.

Configurar el resumen de las rutas en una interfaz.

Verificar el resumen de las rutas IP.

Inhabilitar el resumen automático de rutas.

Router# configure terminal

Entra al modo de configuracion global.

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuracion global y que se presiona CTRL+Z para salir.

o

Router(config)# router rip

Protocolo a configurar

Router(config-router)#version 2

Version del Protocolo

Router(config-router)#network 192.168.9.8

Red que aprende

## 7.11.- REDISTRIBUCION DE RUTAS

En los esquemas Wan es muy probable tener áreas con protocolos diferentes, en estos casos se aplica lo que se conoce como redistribución de rutas de un protocolo como por ejemplo RIP versión 2 hacia un protocolo diferente como OSPF.

Para poder realizar este proceso se debe ejecutar el comando redistribuye protocolo donde protocolo es el protocolo que vamos a inyectar dentro del que estamos configurando

Router# configure terminal

Entra al modo de configuracion global.

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuracion global y que se presiona CTRL+Z para salir.

Router(config)# router ospf 1

Protocolo a configurar

Router(config-router)#network 192.168.9.12 0.0.0.3 area 0

Red que aprende con la respectiva wilcard y el área en que se encuentran

Router(config-router)#network 192.168.9.20 0.0.0.3 area 0

Red que aprende con la respectiva wilcard y el área en que se encuentran

Router(config-router)#redistribute rip

Redistribución de protocolos

Router(config-router)#exit

Sale de modo configuración global

Router#

Router# configure terminal

Entra al modo de configuracion global.

Enter configuration commands, one per line. End with CNTL/Z.

Con este comando se comprueba que se ha ingresado al modo de configuracion global y que se presiona CTRL+Z para salir.

Router(config)# router rip

Protocolo a configurar

Router(config-router)#version 2

Version del Protocolo

Router(config-router)#network 192.168.9.8

Red que aprende

Router(config-router)#redistribute ospf 1

Redistribución de protocolos

Router(config-router)#exit

Sale de modo configuración global

Router#

## 7.12.-LISTAS DE CONTROL DE ACCESO (ACL'S)

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos.

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACL's). Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior.

Las ACL pueden ser tan simples como una sola línea destinada a permitir paquetes desde un host específico o pueden ser un conjunto de reglas y condiciones extremadamente complejas que definan el tráfico de forma precisa y modelen el funcionamiento de los procesos de los routers.

Es posible crear ACL en todos los protocolos de red enrutados por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX). Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones 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.

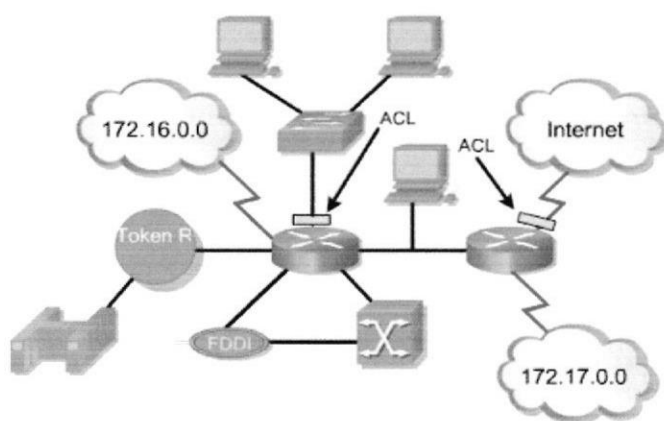


FIGURA 7 - 16: Lista de acceso





### 7.12.1.-FUNCIONAMIENTO DE LAS ACL

El orden en el que se ubican las sentencias de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL.

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.

### 7.12.2.- WILCARD

Las mascarar de wilcard usan números binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso según el valor de las mismas.

La única similitud entre la mascara wilcard y la subred es que ambas tienen 32 bits de longitud. La opción any reemplaza la dirección IP con 0.0.0.0 y la mascara Wilcard por 255.255.255.255. Esta dirección concuerda con cualquier dirección que se la compare

Para especificar un nodo:

192.168.12.0.5 0.0.0.0

Para especificar una red pequeña:

192.168.12.0-200.10.148.7 (seria una /29)

### 7.12.3.-TIPOS

#### 7.12.3.1.-ACL ESTÁNDAR

En la versión 12.0.1 del IOS de Cisco, se usaron por primera vez números adicionales (1300 al 1999) para las ACL's estándar pudiendo así proveer un máximo posible de 798 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.

La sintaxis completa del comando ACL estándar es:

Router (config)#access-list access-list-number {deny | permit | remark} source [source-wildcard] [log]

El uso de remark facilita el entendimiento de la lista de acceso. Cada remark está limitado a 100 caracteres. Por ejemplo, no es suficientemente claro cual es el propósito

del siguiente comando: `access-list 1 permit 192.168.15.15`. Es mucho más fácil leer un comentario acerca de un comando para entender sus efectos, así como sigue:

La forma no de este comando, se utiliza para eliminar una ACL estándar. Ésta es la sintaxis:

Router (config) #no access-list access-list-number

El comando `ip access-group` relaciona una ACL existente a una interface:

Router (config)#ip access-group {access-list-number | access-list-name} {in | out}

### **7.12.3.2.-ACL EXTENDIDA**

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).

Las operaciones lógicas pueden especificarse como igual (`eq`), desigual (`neq`), mayor a (`gt`) y menor a (`lt`) aquéllas que efectuarán las ACL extendidas en protocolos específicos. Las ACL extendidas utilizan el número de lista de acceso entre 100 y 199.

El comando `ip access-group` enlaza una ACL extendida existente a una interfaz. Recuerde que sólo se permite una ACL por interfaz, por protocolo, por dirección.

7.12.4.-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, 1300-1999
IP extendido	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX extendido	900-999
Protocolo de publicación de servicio IPX	1000-1099

Tabla 7 - 3: Rango específico de ACL

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

7.12.5.-UBICACIÓN DE LA ACL

Las ACL se utilizan para controlar el tráfico, filtrando paquetes y eliminando el tráfico no deseado de la red. Otra consideración importante a tener en cuenta al implementar la ACL es donde se ubica la lista de acceso. Si las ACL se colocan en el lugar correcto, no sólo es posible filtrar el tráfico sino también toda la red se hace más eficiente.

Si se tiene que filtrar el tráfico, la ACL se debe colocar en un lugar donde mejore la eficiencia de forma significativa.

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican las direcciones destino, de modo que se deben colocar lo más cerca posible del destino. Por ejemplo, una ACL estándar se debe colocar en Fa0/0 del Router D para evitar el tráfico desde el Router A.

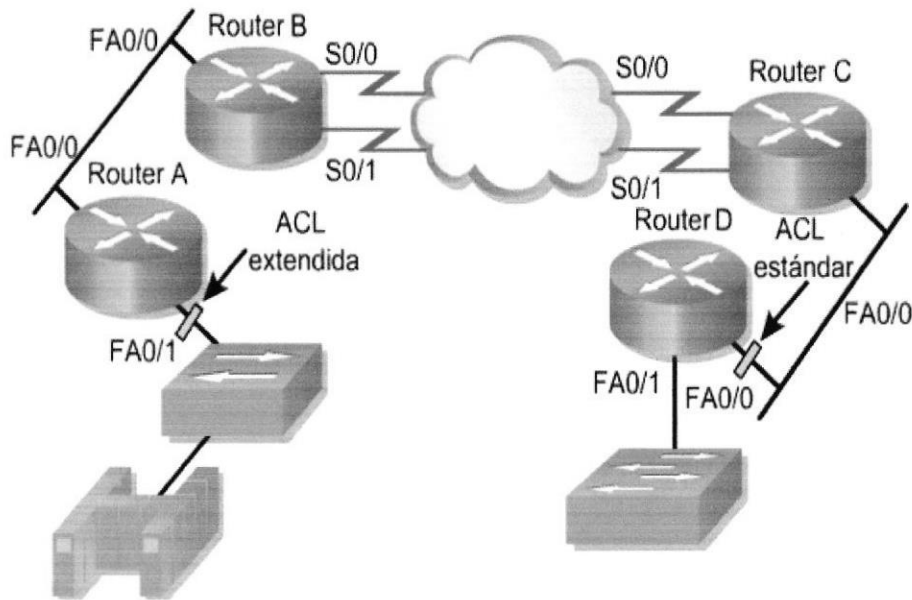
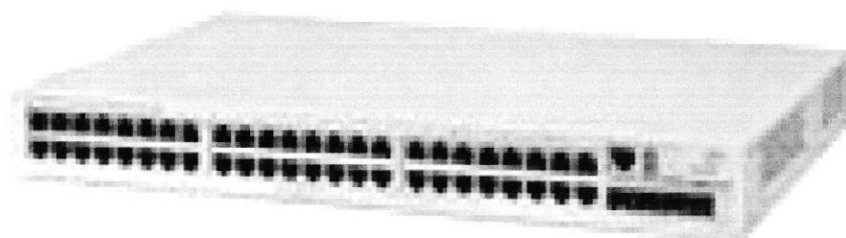


FIGURA 7 - 17: Ubicacion de la Acl

## 8.- SWITCHES

Un switch denominado en el idioma castellano se la llama también "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 Interconnection). Un conmutador o switch se 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.

3COM SWITCH 4500 48



3COM SWITCH 5500G-EI 48

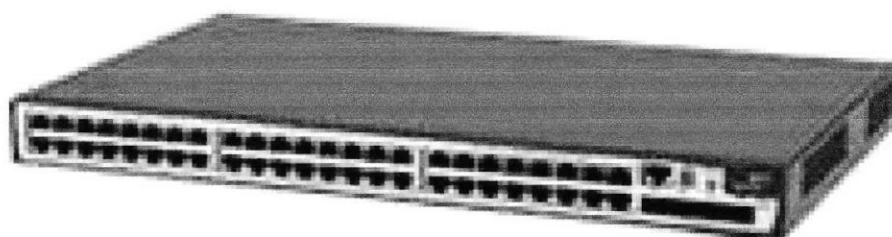


FIGURA 7 - 18: Switchs

### 8.1.-TECNOLOGÍA

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

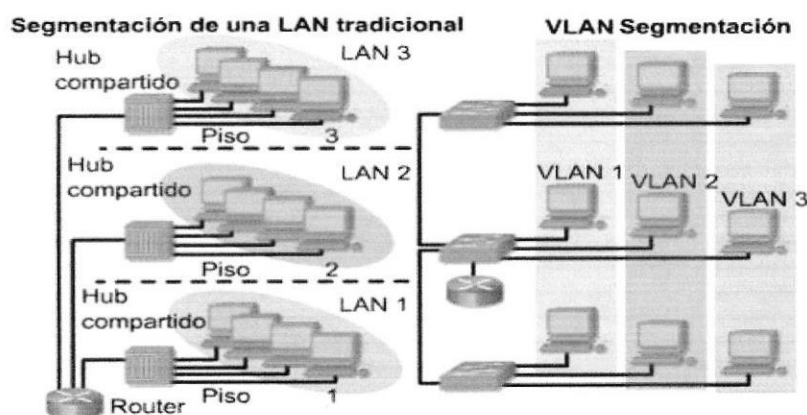
El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

## 8.2.-SEGMENTACIÓN

La segmentación se trata de dividir un segmento de red en varias direcciones o sea direcciones IP con la finalidad que estas IP se han utilizado en varias máquinas que se encuentran conectadas en la red, esta dirección IP no se puede repetir en la red ya que produce problemas de dirección de IP en la red.

### 8.2.1.-ASPECTOS BÁSICOS DE LAS VLAN



**FIGURA 7 - 19: VLAN'S**

Una VLAN es una agrupación lógica de dispositivos o usuarios que se pueden agrupar por función, departamento o aplicación, sin importar su ubicación física.

Las VLAN se configuran en el switch a través del software. Debido a la cantidad de implementaciones de VLAN que compiten entre sí es posible que deba requerirse el uso de un software propietario por parte del fabricante del switch. La agrupación de puertos y usuarios en comunidades de interés, conocidos como organizaciones VLAN, puede obtenerse mediante el uso de un solo switch o una conexión más potente entre los switches ya conectados dentro de la empresa. Al agrupar puertos y usuarios en varios switches, las VLAN pueden abarcar infraestructuras contenidas en un solo edificio o en edificios interconectados. Las VLAN ayudan a utilizar con efectividad el ancho de banda dado que comparten el mismo dominio de broadcast o la misma red de Capa 3. Las VLAN optimizan la acumulación y uso del ancho de banda. Las VLAN se disputan el mismo ancho de banda aunque los requisitos del ancho de banda pueden variar considerablemente según el grupo de trabajo o el departamento.

A continuación, presentamos algunos de los temas de configuración de las VLAN:

Un switch crea un dominio de broadcast

Las VLAN ayudan a administrar los dominios de broadcast

Las VLAN se pueden definir en grupos de puerto, usuarios o protocolos

Los switches LAN y el software de administración de red suministran un mecanismo para crear las VLAN

Las VLAN ayudan a controlar el tamaño de los dominios de broadcast y a ubicar el tráfico. Las VLAN se asocian con redes individuales. Por lo tanto, los dispositivos de red en las distintas VLAN no se pueden comunicar directamente entre sí sin la intervención de un dispositivo de enrutamiento de Capa 3.



### **8.2.2.-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 retiemprizan 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.

8.2.3.-ENRUTAMIENTO ENTRE VLAN

Cuando el host en un dominio de broadcast desea comunicarse con un host en otro dominio de broadcast, debe utilizarse un router.

El puerto 1 en un switch forma parte de la VLAN 1 y el puerto 2 forma parte de la VLAN 200.



FIGURA 7 - 20: Enrutamiento

Si todos los puertos de switch formaran parte de la VLAN 1, es posible que los hosts conectados a estos puertos puedan comunicarse entre sí. Sin embargo, en este caso, los puertos forman parte de distintas VLAN, la VLAN 1 y la VLAN 200. Se debe utilizar un router si los hosts de las distintas VLAN necesitan comunicarse entre sí.

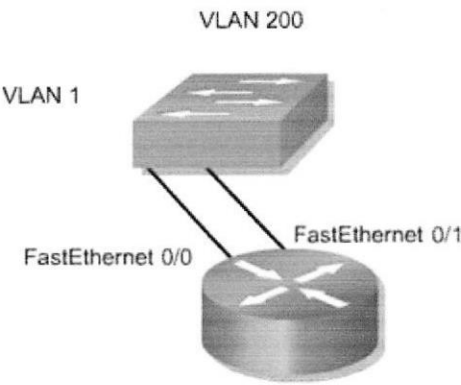


FIGURA 7 - 21: Comunicación de Vlan's



Dado que los routers evitan la propagación de broadcast y utilizan algoritmos de envío más inteligentes que los switches, los routers ofrecen un uso más eficiente del ancho de banda. Esto da como resultado simultáneamente una selección de ruta flexible y óptima. Si una VLAN abarca varios dispositivos, se utiliza un enlace troncal para interconectar los dispositivos. El enlace troncal transporta el tráfico para varias VLAN.

Recuerde que cuando un host en una VLAN desea comunicarse con un host de otra VLAN, se debe utilizar un router.

#### 8.2.4.-INTERFACES FÍSICAS Y LÓGICAS

En una situación tradicional, una red con cuatro VLAN requeriría cuatro conexiones físicas entre el switch y el router externo.

A medida que las tecnologías como por ejemplo el Enlace inter-switch (ISL) se vuelven más comunes, los diseñadores de red empiezan a utilizar enlaces troncales para conectar los routers a los switches. A pesar de que se puede utilizar cualquier tecnología de enlace troncal como por ejemplo ISL, 802.1Q, 802.10 o la emulación LAN (LANE), los enfoques basados en Ethernet como por ejemplo ISL y 802.1Q son más comunes.

A medida que aumenta la cantidad de VLAN en una red, el enfoque físico de tener una interfaz de router por VLAN se vuelve rápidamente no escalable. Las redes con muchas VLAN deben utilizar el enlace troncal de VLAN para asignar varias VLAN a una interfaz de router única.

El router puede admitir varias interfaces lógicas en enlaces físicos individuales. Por ejemplo, la interfaz de FastEthernet 0/0 puede admitir tres interfaces virtuales numeradas como FastEthernet 0/0.1, 0/0.2 y 0/0.3.

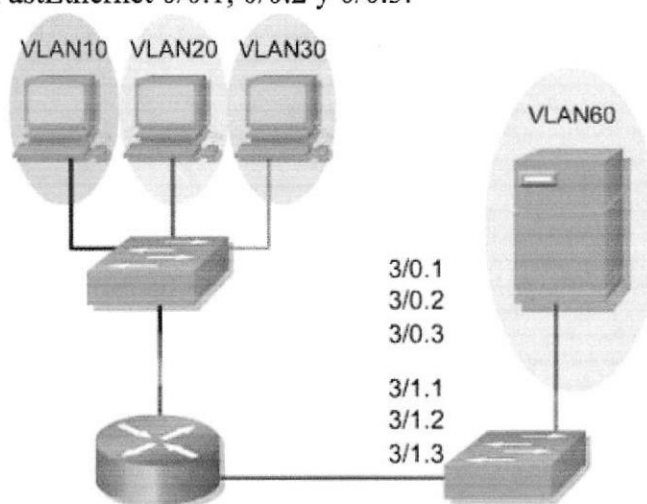


FIGURA 7 - 22: Interfaces física y lógicas

La ventaja principal del uso del enlace troncal es una reducción en la cantidad de puertos de router y switch que se utiliza. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de router conectado a un enlace troncal puede ampliarse hasta un número mucho más alto de VLAN que el diseño de "un enlace por VLAN".

## 8.3.- CONFIGURACIÓN DE SWITCH

Ahora pasaremos a configurar paso a paso los diferentes Switch de la red Corporación Noboa

### 8.3.1.- ACCESO A LA APLICACIÓN HYPERTERMINAL

En la barra de tareas de Windows seleccionar con el Mouse la opción Inicio

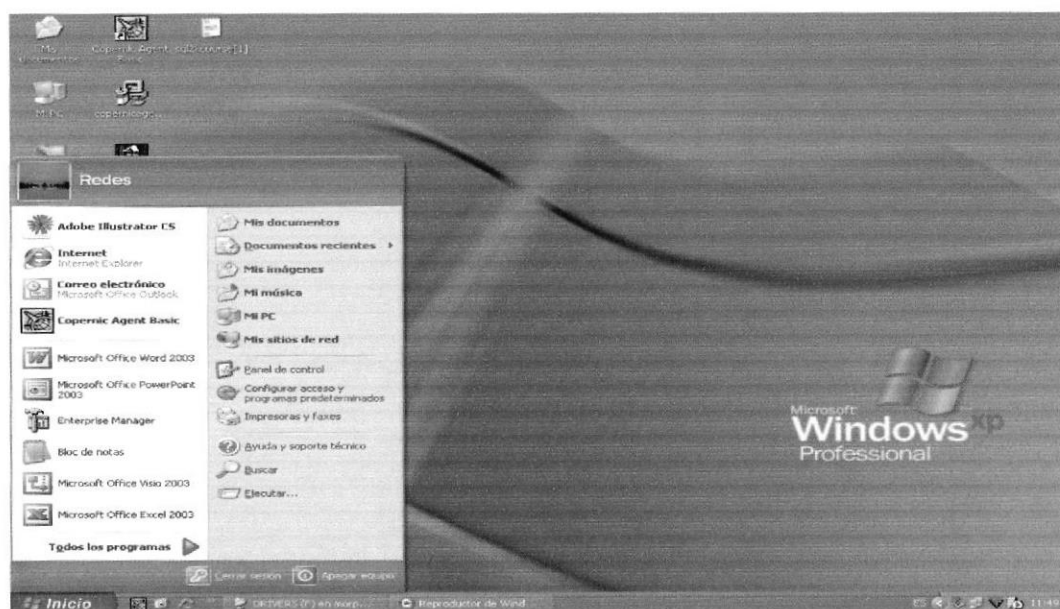


Figura 7 – 23: Entorno de Windows

Abrirá un menú donde seleccionara la opción todos los programas.

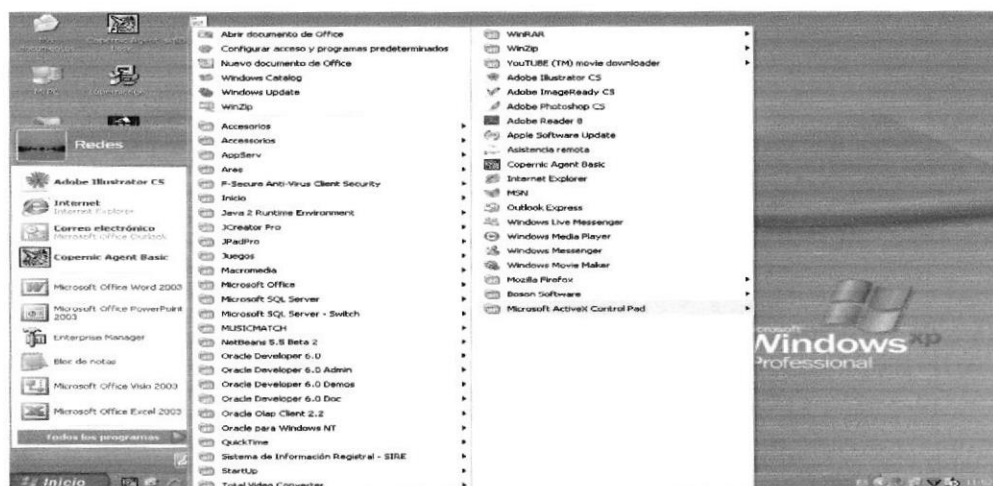


Figura 7 – 24: Menú inicio

Aquí encontraremos un acceso directo llamado HyperTerminal, al cual le dará clic y nos mostrara la siguiente pantalla

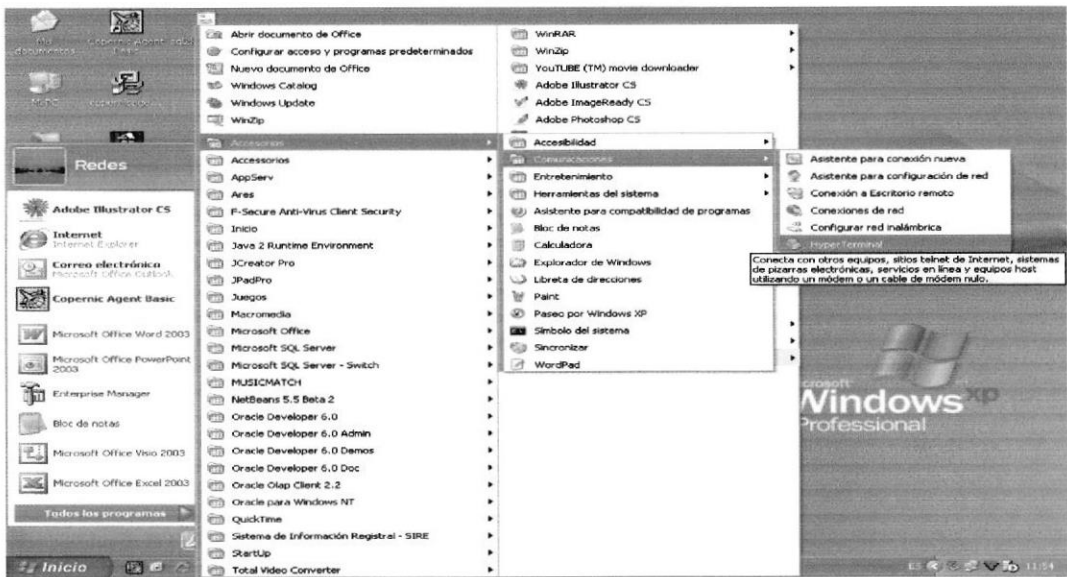


Figura 7 – 25: Selección de programa (hiperterminal)

En el cuadro de texto denominado Nombre se colocara un identificador a la conexión en este caso será Corporación Noboa y dará Aceptar, si da clic en el botón Cancelar no existirá ninguna conexión



Figura 7 – 26: Nueva conexión



En la siguiente pantalla se pedirá ingresar algunos detalles de conexión como País o región, Código de área, Numero de teléfono y conectar usando. Las tres primeras no son obligatorias son opcionales mientras que la ultima opción deberá escoger el puerto del computador al cual se va conectar el router en este caso va ser el puerto COM 1 y da clic en el botón Aceptar

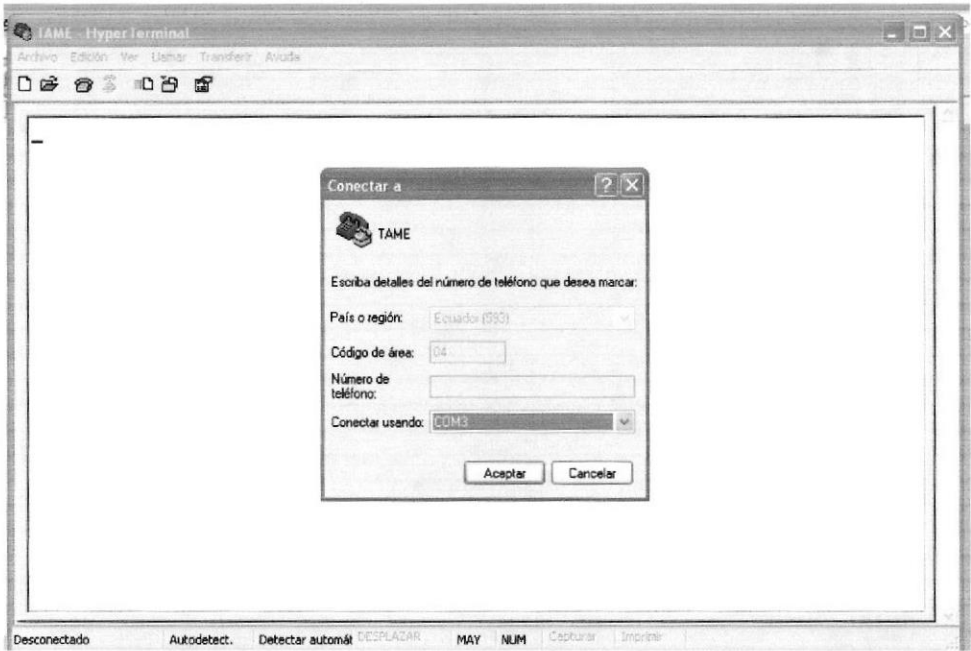


Figura 7 – 27: Conexión cable rollover

En la siguiente pantalla encontrara algunos parámetros de conexión de los cuales deberá establecer y dar clic en el botón Aceptar.

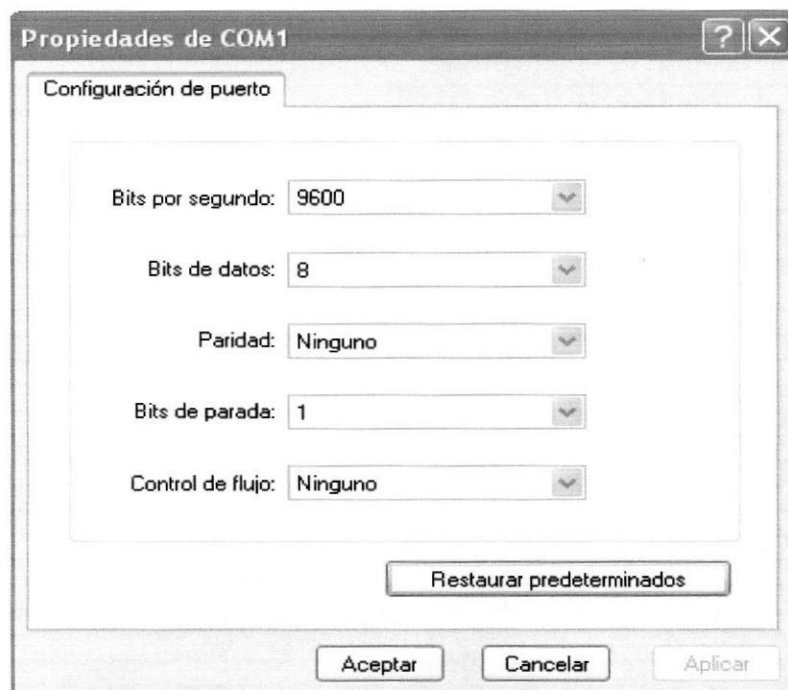
9600 bps. (Velocidad de transmisión del cable serial de conexión

8 bits de Datos (configuración del procesamiento de datos al pasar al Hyperterminal en bits por segundo)

Ninguno (paridad) (utilizado para comprobar errores en el grupo de bits de datos transferidos entre uno o varios equipos)

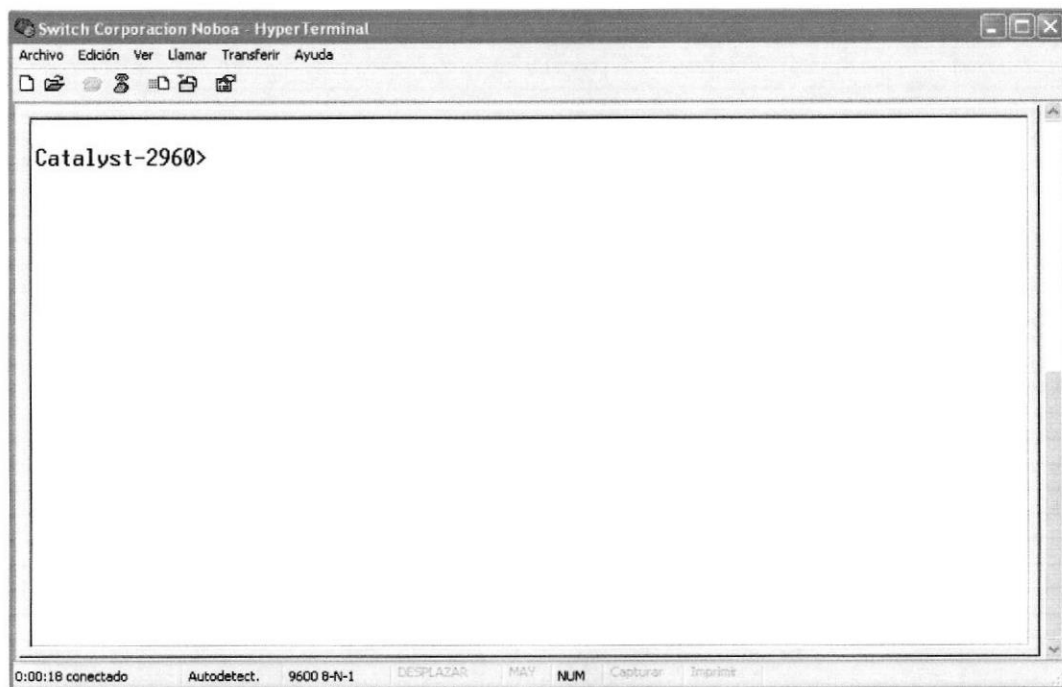
1 (bit de parada) (medida de transporte por la que pasan datos al Hyperterminal)

Ninguno control del flujo (se refiere a la información que viaja)



**Figura 7 – 28:** Propiedades de com 1

Una vez colocado los parámetros dará clic en el botón Aceptar y podrá empezar con la configuración del Swicht a través de la consola Hyperterminal.



**Figura 7 – 29:** Conexión al switch 1

#### 8.3.1.1.-CONFIGURACIÓN DE VLAN POR DEFECTO

Para permitir que Telnet y otras aplicaciones TCP/IP puedan acceder al switch, se deberán establecer direcciones IP y un gateway por defecto. Por defecto, la VLAN 1 es la VLAN de administración. En una red basada en switch, todos los dispositivos de red deberían estar en la VLAN de administración. Esto permite que una sola estación de trabajo de administración acceda, configura y administre todos los dispositivos de red. Acceso al modo de Configuración principal.

Switch>enable

    Ingresar al modo EXEC privilegiado

Switch#configure terminal

    Ingresar al modo de configuración global

Switch(config)#exit

    Salir un nivel

#### 8.3.1.2.-CREACIÓN DE VLAN'S

Las VLAN se configuran en el switch a través del software.

Ingrese al modo de configuración de Vlan con el comando Vlan database.

Asigne un número y un nombre con el comando **Vlan number name** nombre.

Switch\_Principal>enable

Ingresar al modo de configuración global

Switch\_Principal#vlan database

Ingresar al modo de configuración de vlan's

Switch\_Principal(Vlan )#Vlan 5 name Sistemas

Asignar un número referencial y un nombre a la Vlan que se va a crear

### 8.3.1.3.-BORRADO DE VLAN'S

Los siguientes pasos permitirán que una nueva configuración se sobrescriba completamente a la configuración actual:

Para eliminar la información de VLAN actual, borre el archivo de la base de datos VLAN, denominados **vlan.dat**, del directorio **flash**

Borre el archivo de configuración de respaldo con el nombre **startup-config**

Reinicie el switch con el comando **reload**

```
Switch>enable
```

```
Switch#delete flash:vlan.dat
```

```
Switch#erase startup-config
```

```
Switch#reload
```

### 8.3.1.4.-ASIGNACIÓN DE VLAN'S A LOS PUERTOS

Switch\_Principal>enable

Ingresar al modo EXEC privilegiado

Switch\_Principal#configure terminal

Ingresar al modo de configuración global

Switch\_Principal(config)#

Switch\_Principal(config)#interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

### 8.3.1.5.- CONFIGURACIÓN DE UN ENRUTAMIENTO DE VLAN

Matriz\_Guayaquil>enable

Ingresar al modo EXEC privilegiado

Matriz\_TAME#configure terminal

Ingresar al modo de configuración global

Matriz\_TAME (config)#interface FastEthernet 1/0.2

Ingresar a la sub-interfaz que se va a configurar

Matriz\_TAME (config-subif)#encapsulation dot1q 5

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 10

Matriz\_TAME(config-subif)#ip address 192.168.10.1 255.255.255.224

Asignar una dirección ip con su respectiva máscara

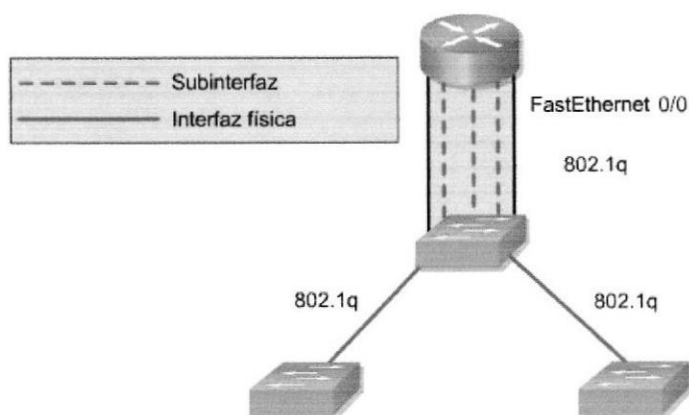
Matriz\_TAME(config-subif)#exit

Salir de la configuración de la sub-interfaz



## 8.4.-CONFIGURACIÓN DE UN ENRUTAMIENTO ENTRE DISTINTAS VLAN

Para que el enrutamiento entre VLAN funcione correctamente, todos los routers y switches involucrados deben admitir el mismo encapsulamiento.



**FIGURA 7 - 30:** Configuración de enrutamiento

En un router, una interfaz se puede dividir lógicamente en varias subinterfaces virtuales. Las subinterfaces ofrecen una solución flexible para el enrutamiento de varias corrientes de datos a través de una interfaz física única.

Para definir las subinterfaces en una interfaz física, realice las siguientes tareas:

Identifique la interfaz.

Defina el encapsulamiento de la VLAN.

Asigne una dirección IP a la interfaz.

Para identificar la interfaz utilice el comando `interface` en el modo de configuración global.

Router (config)#`interface fastethernet port-number. Subinterface-number`

Port-number identifica la interfaz física y subinterface-number identifica la interfaz virtual (Vlan ).

El router debe poder comunicarse con el switch utilizando un protocolo de enlace troncal estandarizado. Esto significa que ambos dispositivos conectados entre sí deben comprenderse. Para definir el encapsulamiento de la VLAN, introduzca el comando `encapsulation` en el modo de configuración de interfaz.

Router (config-if) #`encapsulation dot1q Vlan -number`

Vlan-number identifica la VLAN para la cual la subinterfaz transportará el tráfico. Se agrega un ID de VLAN a la trama sólo cuando la trama está destinada a una red no local. Cada paquete de VLAN transporta el ID de VLAN dentro del encabezado del paquete.

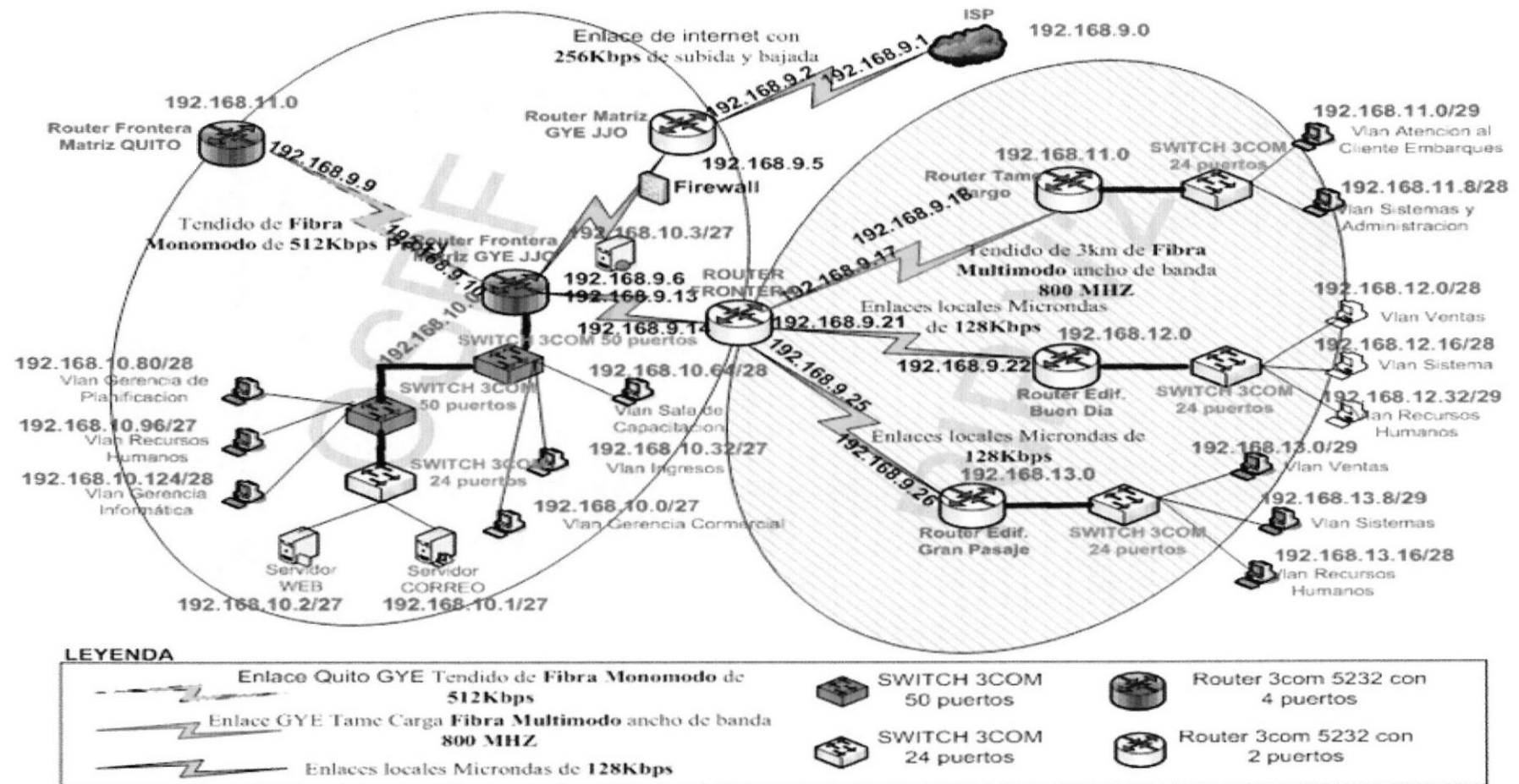


Para asignar una dirección IP a la interfaz, introduzca el siguiente comando en el modo de configuración de interfaz.

Router (config-if) #ip address ip-address subnet-mask

IP-address y subnet-mask son las direcciones y la máscara de red de 32 bits de la interfaz específica.

## 8.5.- CONFIGURACION DETALLADAS DE LOS ROUTERS



**FIGURA 7 - 31:** Enlace quito GYE

## 8.6.-CONFIGURACION DE LOS ROUTER Y SWICHT

### 8.6.1.-ASIGNACIÓN DE NOMBRE AL ROUTER

#### 8.6.1.1.-ROUTER FRONTERA CORE GUAYAQUIL

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CORE_GYE
CORE_GYE(config)#
```

Router> Enable  
En esta línea permite ingresar al modo privilegiado  
Router# configure terminal  
En esta línea permite ingresar al modo global  
Router(config)# hostname CORE\_GYE  
Esta línea permite cambiar el nombre al router

#### 8.6.1.2.-ROUTER MATRIZ GUAYAQUIL

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname MATRIZ_GYE
MATRIZ_GYE(config)#
```

#### 8.6.1.3.-ROUTER MATRIZ QUITO

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname QUITO
QUITO(config)#
```

#### 8.6.1.4.-ROUTER (MATRIZ) GUAYAQUIL

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hops
Router(config)#hostname GYE
GYE(config)#
```

8.6.1.5.-ROUTER (PROVEEDOR DE INTERNET) ISP

```
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#
```

8.6.1.6.-ROUTER (SUCURSAL) TAME CARGO

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TAME_CARGO
TAME_CARGO(config)#
```

8.6.1.7.-ROUTER (SUCURSAL) BUEN DIA

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUEN_DIA
BUEN_DIA(config)#
```

8.6.1.8.-ROUTER (SUCURSAL) GRAN PASAJES

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname GRAN_PASAJES
GRAN_PASAJES(config)#
```

COMANDOS	DETALLE
Router>	Modo usuario
Enable	Modo exe privilegiado
Router #	Modo privilegiado
Configure terminal	Modo de configuración global
Hostname	Comando para asignar nombre a un router
(control) z	Retrocedo a modo privilegiado
Wr	Permite guardar el cambio efectuado

Tabla 7 - 4: Comando para asignar nombre

## 8.7.-CONFIGURACIÓN DE LAS INTERFAZ

### 8.7.1.-ROUTER FRONTERA GUAYAQUIL

```
CORE_GYE(config)#interface serial 0/0
CORE_GYE(config-if)#ip address 192.168.9.14 255.255.255.252
CORE_GYE(config-if)#clock rate 56000
CORE_GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up
CORE_GYE(config-if)#exit
%LINK-3-UPDOWN: Interface Serial0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
```

#### .Configuración De La Serial 0/0 Core GYE

CORE\_GYE(config)# interface serial 0

En esta línea entrar en la serial 0 del router

Matriz(config-if)#ip address 192.168.9.14 255.255.255.252

Esta línea nos permite asignar una Ip al router con la mascara de subred.

Matriz(config-if)# Clock rate 56000

En esta línea fijar la velocidad de sincronización del router.

Matriz (config-if) # no shutdown

En esta línea permite levantar la interfaces del router.

```
CORE_GYE(config)#interface serial 0/1
CORE_GYE(config-if)#ip address 192.168.9.17 255.255.255.252
CORE_GYE(config-if)#clock rate 56000
CORE_GYE(config-if)#no shu8
CORE_GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/1, changed state to up
CORE_GYE(config-if)#exit
%LINK-3-UPDOWN: Interface Serial0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down
```

#### Configuración De La Serial 0/1 Core GYE

```
CORE_GYE(config)#interface serial 0/2
CORE_GYE(config-if)#ip address 192.168.9.21 255.255.255.252
CORE_GYE(config-if)#clock rate 56000
CORE_GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/2, changed state to up
CORE_GYE(config-if)#exit
%LINK-3-UPDOWN: Interface Serial0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down
```

#### Configuración De La Serial 0/2 Core GYE

```
CORE_GYE(config)#interface serial 0/3
CORE_GYE(config-if)#ip address 192.168.9.25 255.255.255.252
CORE_GYE(config-if)#clock rate 56000
CORE_GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/3, changed state to up
%LINK-3-UPDOWN: Interface Serial0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3, changed state to down
```

#### Configuración De La Serial 0/2 Core GYE

## 8.7.2.-ROUTER MATRIZ GUAYAQUIL

```
MATRIZ_GYE(config)#interface serial 0/0
MATRIZ_GYE(config-if)#ip address 192.168.9.9 255.255.255.252
MATRIZ_GYE(config-if)#clock rate 56000
MATRIZ_GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up
```

### Configuración De La Serial 0/0 Matriz GYE

```
MATRIZ_GYE(config)#interface serial 0/1
MATRIZ_GYE(config-if)#ip address 192.168.9.13 255.255.255.252
MATRIZ_GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/1, changed state to up
MATRIZ_GYE(config-if)#exit
```

### Configuración De La Serial 0/1 Matriz GYE

```
MATRIZ_GYE(config-if)#clock rate 56000
MATRIZ_GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/2, changed state to up
%LINK-3-UPDOWN: Interface Serial0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down
MATRIZ_GYE(config-if)#exit ^Z
%SYS-5-CONFIG_I: Configured from console by console

MATRIZ_GYE#wr
Building configuration...
[OK]
```

### Configuración De La Serial 0/2 Matriz GYE

## 8.7.3.-ROUTER MATRIZ QUITO

```
QUITO(config)#interface serial 0
QUITO(config-if)#ip address 192.168.9.10 255.255.255.252
QUITO(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
QUITO(config-if)#exit
QUITO(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
QUITO#wr
Building configuration...
[OK]
```

### Configuración De La Serial 0 Quito



BIBLIOTECA  
CAMPUS  
PEÑAS

#### 8.7.4.-ROUTER (MATRIZ) GUAYAQUIL

```
GYE(config)#interface serial 0
GYE(config-if)#ip address 192.168.9.6 255.255.255.252
GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
GYE(config-if)#exit
```

##### Configuración De La Serial 0 GYE

CORE\_GYE(config)# interface serial 0  
En esta línea entrar en la serial 0 del router  
Matriz(config-if)#ip address 192.168.9.6 255.255.255.252  
Esta línea permite asignar una Ip al router con la mascara de subred.  
Matriz (config-if) # no shutdown  
En esta línea permite levantar la interfaces del router.

```
GYE(config)#interface serial 1
GYE(config-if)#ip address 192.168.9.2 255.255.255.252
GYE(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial1, changed state to up
GYE(config-if)#exit
GYE(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

%LINK-3-UPDOWN: Interface Serial1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to down
GYE#wr
Building configuration...
[OK]
```

##### Configuración De La Serial 1 GYE

### 8.7.5.-ROUTER (PROVEEDOR DE INTERNET) ISP

```
Router(config)#hostname ISP
ISP(config)#interface serial 0
ISP(config-if)#ip address 192.168.9.1 255.255.255.252
ISP(config-if)#clock rate 56000
ISP(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
```

#### Configuración De La Serial 0 ISP

CORE\_GYE(config)# interface serial 0  
En esta línea entrar en la serial 0 del router  
Matriz(config-if)#ip address 192.168.9.1 255.255.255.252  
Esta línea permite asignar una Ip al router con la mascara de subred.  
Matriz(config-if)# Clock rate 56000  
En esta línea fijamos la velocidad de sincronización del router.  
Matriz (config-if) # no shutdown  
En esta línea permite levantar la interfaces del router.

### 8.7.6.-ROUTER (SUCURSAL) TAME CARGO

```
TAME_CARGO(config)#interface serial 0
TAME_CARGO(config-if)#ip address 192.168.9.18 255.255.255.252
TAME_CARGO(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
```

#### Configuración De La Serial 0 TAME Cargo

CORE\_GYE(config)# interface serial 0  
En esta línea entrar en la serial 0 del router  
Matriz(config-if)#ip address 192.168.9.18 255.255.255.252  
Esta línea permite asignar una Ip al router con la mascara de subred.  
Matriz (config-if) # no shutdown  
En esta línea permite levantar la interfaces del router



**8.7.7.-ROUTER (SUCURSAL) BUEN DIA**

```

BUEN_DIA(config)#interface serial 0
BUEN_DIA(config-if)#ip address 192.168.9.22 255.255.255.252
BUEN_DIA(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up

```

Configuración De La Serial 0 Buen Dia

**8.7.8.-ROUTER (SUCURSAL) GRAN PASAJES**

```

GRAN_PASAJES(config)#interface serial 0
GRAN_PASAJES(config-if)#ip address 192.168.9.26 255.255.255.252
GRAN_PASAJES(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up

```

Configuración De La Serial 0 Gran Pasajes

COMANDOS	DETALLE
Configure Terminal	Modo de configuración Global
Interface serial 0/0 o 0/1	Comando que permite ingresar al modo de configuración interfaz serial
Ip address	Permite colocar la dirección IP y la mascara al router
No shutdown	Permite activar la interfaz
Clock rate 5600° o 64000	Establece la velocidad del reloj se aplica solo DCE
(Control) Z	Retrocedo a modo privilegiado
Wr	Permite guardar el cambio efectuado

**Tabla 7 - 5:** Comandos para configura las interfaces

## 8.8.-LEVANTAMIENTO DE LAS INTERFACES SERIAL

### 8.8.1.-ROUTER FRONTERA GUAYAQUIL

```
CORE_MATRIZ#show protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled
```

```
Serial0/0 is up, line protocol is up
```

```
Internet address is 192.168.9.14/30
```

```
Serial0/1 is up, line protocol is up
```

```
Internet address is 192.168.9.17/30
```

```
Serial0/2 is up, line protocol is up
```

```
Internet address is 192.168.9.21/30
```

```
Serial0/3 is up, line protocol is up
```

```
Internet address is 192.168.9.25/30
```

```
Bri1/0 is administratively down, line protocol is down
```

```
Bri1/0:1 is administratively down, line protocol is down
```

```
Bri1/0:2 is administratively down, line protocol is down
```

Levantamiento de las interfaces serial  
0/0, 0/1, 0/2, 0/3

Conexión Bri del  
Administrador se  
encuentra bajo sus  
protocolos

### 8.8.2.-ROUTER MATRIZ GUAYAQUIL

```
GYE#show protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled
```

```
Serial0 is up, line protocol is up
```

```
Internet address is 192.168.9.6/30
```

```
Serial1 is up, line protocol is up
```

```
Internet address is 192.168.9.2/30
```

```
FastEthernet0/0 is administratively down, line protocol is down
```

```
Bri0 is administratively down, line protocol is down
```

```
Bri0:1 is administratively down, line protocol is down
```

```
Bri0:2 is administratively down, line protocol is down
```

### 8.8.3.-ROUTER MATRIZ QUITO

```
QUITO#show protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled
```

```
Serial0 is up, line protocol is up
```

```
Internet address is 192.168.9.10/30
```

```
Serial1 is administratively down, line protocol is down
```

```
FastEthernet0/0 is administratively down, line protocol is down
```

```
Bri0 is administratively down, line protocol is down
```

```
Bri0:1 is administratively down, line protocol is down
```

```
Bri0:2 is administratively down, line protocol is down
```

#### 8.8.4.-ROUTER (MATRIZ) GUAYAQUIL

```
MATRIZ_GYE#show protocols
Global values:
  Internet Protocol routing is enabled
Serial0/0 is up, line protocol is up
  Internet address is 192.168.9.9/30
Serial0/1 is up, line protocol is up
  Internet address is 192.168.9.13/30
Serial0/2 is up, line protocol is up
  Internet address is 192.168.9.5/30
Serial0/3 is administratively down, line protocol is down
FastEthernet1/0 is up, line protocol is up
  Internet address is 192.168.10.1/27
Bri1/0 is administratively down, line protocol is down
Bri1/0:1 is administratively down, line protocol is down
Bri1/0:2 is administratively down, line protocol is down
```

#### 8.8.5.-ROUTER (PROVEEDOR DE INTERNET) ISP

```
ISP#show protocols
Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.9.1/30
Serial1 is administratively down, line protocol is down
FastEthernet0/0 is administratively down, line protocol is down
Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down
```

#### 8.8.6.-ROUTER (SUCURSAL) TAME CARGO

```
TAME_CARGO#show protocols
Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.9.18/30
Serial1 is administratively down, line protocol is down
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.11.1/27
Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down
```

8.8.7.-ROUTER (SUCURSAL) BUEN DIA

Levantamiento de las interfaces serial 0/0 192.168.9.22/30

```
BUEN_DIA#show protocols
Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.9.22/30
Serial1 is administratively down, line protocol is down
FastEthernet0/0 is up, line protocol is up
```

8.8.8.-ROUTER (SUCURSAL) GRAN PASAJES

```
GRAN_PASAJE#show protocols
Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.9.26/30
Serial1 is administratively down, line protocol is down
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.13.1/27
Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down
```

COMADOS	DETALLE
UP	La interfaz están levantada
DOWN	La interfaz no están levantadas

Tabla 7 - 6: Comando para levantar las interfaces

## 8.9.-CONFIGURAMOS LAS FASTETHERNET

### 8.9.1.-ROUTER (MATRIZ) GUAYAQUIL

Levantamiento de las interfaces Fastethernet 1/0 192.168.10.1/27

```
MATRIZ_GYE(config)#interface fastethernet 1/0
MATRIZ_GYE(config-if)#ip address 192.168.10.1 255.255.255.224
MATRIZ_GYE(config-if)#no shutdown
MATRIZ_GYE(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
MATRIZ_GYE#wr
Building configuration...
[OK]
```

```
MATRIZ_GYE#
```

MATRIZ\_GYE(config)# interface fastethernet 0/0  
configuración de la fastethernetMATRIZ\_GYE (config-if)# ip address 192.168.10.1  
255.255.255.248

Dar una ip a la interfaz fastethernet del router con la mascara de subred

MATRIZ\_GYE (config-if)# no shutdown

para levantar las interfaces

MATRIZ\_GYE (config-if)# Ctrl. Z

Salir del Modo Global

MATRIZ\_GYE # wr

Para guardar los cambios

### 8.9.2.-ROUTER (SUCURSAL) TAME CARGO

Levantamiento de las interfaces Fastethernet 0/0 192.168.11.1/27

```
TAME_CARGO(config)#interface fastethernet 0/0
TAME_CARGO(config-if)#ip address 192.168.11.1 255.255.255.224
TAME_CARGO(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
TAME_CARGO(config-if)#exi
TAME_CARGO(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

### 8.9.3.-ROUTER (SUCURSAL) BUEN DIA

Levantamiento de las interfaces Fastethernet 0/0 192.168.12.1/27

```
BUEN_DIA(config)#interface fastethernet 0/0
BUEN_DIA(config-if)#ip address 192.168.12.1 255.255.255.224
BUEN_DIA(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
BUEN_DIA(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

8.9.4.-ROUTER (SUCURSAL) GRAN PASAJES

Levantamiento de las interfaces Fastethernet 0/0 192.168.13.1/27

```
GRAN_PASAJES(config)#interface fastethernet 0/0
GRAN_PASAJES(config-if)#ip address 192.168.13.1 255.255.255.224
GRAN_PASAJES(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
GRAN_PASAJES(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

COMANDOS	DETALLE
Configure Terminal	Modo de configuración Global
Interface fastethernet 0/0 o 1/0	Comando que permite ingresar al modo de configuración interfaz fastethernet
Ip address	Permite colocar la dirección IP y la mascara al router
No shutdown	Permite activar la interfaz
(Control) Z	Retrocedo a modo privilegiado
Wr	Permite guardar el cambio efectuado

Tabla 7 - 7: Comandos para levantar las interfaces

## 8.10.- CONFIGURAMOS TELNET

### 8.10.1.-ROUTER FRONTERA GUAYAQUIL

```
CORE_MATRIZ#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE_MATRIZ(config)#line console 0
CORE_MATRIZ(config-line)#password cisco
CORE_MATRIZ(config-line)#login
CORE_MATRIZ(config-line)#line vty 0 4
CORE_MATRIZ(config-line)#password tame
CORE_MATRIZ(config-line)#login
CORE_MATRIZ(config-line)#en
CORE_MATRIZ(config-line)#exit
CORE_MATRIZ(config)#en
CORE_MATRIZ(config)#enable password cisco
CORE_MATRIZ(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
CORE_MATRIZ#wr
Building configuration...
[OK]
```

```
CORE_MATRIZ # configure terminal
Modo Global
CORE_MATRIZ(config)# line console 0
Configuración del puerto consola.
CORE_MATRIZ(config)# password cisco
password de acceso
CORE_MATRIZ(config)#login
Introducir n usuario.
CORE_MATRIZ (config)# line vty 0 4
Para ingresar una contraseña en modo telnet
CORE_MATRIZ (config-line)# password tame
Asignar una contraseña
CORE_MATRIZ(config-line)# login
Para hacer petición de la contraseña
CORE_MATRIZ (config-line)# exit
Para salir de la consola
CORE_MATRIZ (config)# enable password cisco
Para habilitar la contraseña en el router
CORE_MATRIZ (config)#
```

### 8.10.2.-ROUTER MATRIZ GUAYAQUIL

```
MATRIZ_GYE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MATRIZ_GYE(config)#line console 0
MATRIZ_GYE(config-line)#password cisco
MATRIZ_GYE(config-line)#login
MATRIZ_GYE(config-line)#line vty 0 4
MATRIZ_GYE(config-line)#password tame
MATRIZ_GYE(config-line)#login
MATRIZ_GYE(config-line)#exi
MATRIZ_GYE(config)#enable password cisco
MATRIZ_GYE(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

MATRIZ_GYE#wr
Building configuration...
[OK]
```

### 8.10.31.-ROUTER MATRIZ QUITO

```
QUITO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
QUITO(config)#line console 0
QUITO(config-line)#password cisco
QUITO(config-line)#login
QUITO(config-line)#line
QUITO(config-line)#line vty 0 4
QUITO(config-line)#password tame
QUITO(config-line)#login
QUITO(config-line)#exit
QUITO(config)#enable password cisco
QUITO(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

QUITO#wr
Building configuration...
[OK]
```



#### 8.10.4.-ROUTER (MATRIZ) GUAYAQUIL

```
GYE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GYE(config)#line console 0
GYE(config-line)#password cisco
GYE(config-line)#login
GYE(config-line)#line vty 0 4
GYE(config-line)#password tame
GYE(config-line)#login
GYE(config-line)#exi
GYE(config)#enable password cisco
GYE(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

GYE#wr
Building configuration...
[OK]
```

#### 8.10.5.-ROUTER (PROVEEDOR DE INTERNET) ISP

```
ISP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#login
ISP(config-line)#exi
ISP(config)#enable password cisco
ISP(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

ISP#wr
Building configuration...
[OK]

ISP#
```

### 8.10.6.-ROUTER (SUCURSAL) TAME CARGO

```
TAME_CARGO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TAME_CARGO(config)#line console 0
TAME_CARGO(config-line)#password cisco
TAME_CARGO(config-line)#login
TAME_CARGO(config-line)#line vty 0 4
TAME_CARGO(config-line)#login
TAME_CARGO(config-line)#exit
TAME_CARGO(config)#line vty 0 4
TAME_CARGO(config-line)#password tame
TAME_CARGO(config-line)#en
TAME_CARGO(config-line)#ena
TAME_CARGO(config-line)#exi
TAME_CARGO(config)#en
TAME_CARGO(config)#enable password cisco
TAME_CARGO(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

TAME_CARGO#wr
Building configuration...
[OK]

TAME_CARGO#
```

### 8.10.7.-ROUTER (SUCURSAL) BUEN DIA

```
BUEN_DIA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BUEN_DIA(config)#line console 0
BUEN_DIA(config-line)#password cisco
BUEN_DIA(config-line)#login
BUEN_DIA(config-line)#exi
BUEN_DIA(config)#line vty 0 4
BUEN_DIA(config-line)#password tame
BUEN_DIA(config-line)#login
BUEN_DIA(config-line)#exit
BUEN_DIA(config)#enable password cisco
BUEN_DIA(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

BUEN_DIA#wr
Building configuration...
[OK]

BUEN_DIA#
```

### 8.10.8.-ROUTER (SUCURSAL) GRAN PASAJES

```
GRAN_PASAJE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GRAN_PASAJE(config)#line console 0
GRAN_PASAJE(config-line)#password cisco
GRAN_PASAJE(config-line)#login
GRAN_PASAJE(config-line)#exit
GRAN_PASAJE(config)#line vty 0 4
GRAN_PASAJE(config-line)#password tame
GRAN_PASAJE(config-line)#login
GRAN_PASAJE(config-line)#exi
GRAN_PASAJE(config)#enable password cisco
GRAN_PASAJE(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

GRAN_PASAJE#wr
Building configuration...
[OK]

GRAN_PASAJE#
```



## 8.11.-VERIFICACIÓN DE TELNET

### 8.11.1.-ROUTER FRONTERA GUAYAQUIL

Prueba Telnet a la Matriz GYE por la interfaz conectada directamente al router Frontera  
GYE 192.168.9.13

```
CORE_MATRIZ#telnet 192.168.9.13
```

```
MATRIZ_GYE#show protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled  
Serial0/0 is down, line protocol is down  
Internet address is 192.168.9.9/30  
Serial0/1 is up, line protocol is up  
Internet address is 192.168.9.13/30  
Serial0/2 is down, line protocol is down  
Internet address is 192.168.9.5/30  
Serial0/3 is administratively down, line protocol is down  
FastEthernet1/0 is up, line protocol is up  
Internet address is 192.168.10.1/27  
Br11/0 is administratively down, line protocol is down  
Br11/0:1 is administratively down, line protocol is down  
Br11/0:2 is administratively down, line protocol is down
```

```
MATRIZ_GYE#
```

```
CORE_MATRIZ#telnet 192.168.9.13
```

Hacien telnet para poder ingresar a un router vecino

```
CORE_MATRIZ# show protocolo
```

Muestra el estado global de las interfaces.



## 8.12.-CONFIGURACIÓN DE LOS PROTOCOLOS ENRUTAMIENTO RIP V2 Y OSPF 1

### 8.12.1.-ROUTER FRONTERA GUAYAQUIL (RIP V2 Y OSPF 1)

```

CORE_GYE#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CORE_GYE(config)#router rip
CORE_GYE(config-router)#version 2
CORE_GYE(config-router)#network 192.168.9.16
CORE_GYE(config-router)#network 192.168.9.20
CORE_GYE(config-router)#network 192.168.9.24
CORE_GYE(config-router)#rede
CORE_GYE(config-router)#redistribute ospf 1
CORE_GYE(config-router)#exi
CORE_GYE(config)#router ospf 1
CORE_GYE(config-router)#network 192.168.9.12 0.0.0.3 area
%Incomplete command.

CORE_GYE(config-router)#network 192.168.9.12 0.0.0.3 area 0
CORE_GYE(config-router)#redistribute rip
CORE_GYE(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

CORE_GYE#wr
Building configuration...
[OK]

CORE_GYE#

```

CORE\_GYE # configure terminal

(terminal (Modo Global))

CORE\_GYE (config)# router ospf 2

redes que estén directamente conectadas al router

**CORE\_GYE (config-router)# network 192.168.9.16 0.0.0.3 area 0**Declaramos los segmentos de las redes que estén directamente conectadas al router con la willcard y el área

**CORE\_GYE (config-router)# network 192.168.9.20 0.0.0.3 area 0**Declaramos los segmentos de las redes que estén directamente conectadas al router con la willcard y el área

**CORE\_GYE (config-router)# network 192.168.9.24 0.0.0.3 area 0**Declaramos los segmentos de las redes que estén directamente conectadas al router con la willcard y el área

CORE\_GYE (config-router)# Ctrl. Z

Salir del Modo Global

CORE\_GYE #wr

Para guardar los cambios

### 8.12.2.-ROUTER MATRIZ GUAYAQUIL (OSPF 1)

```
MATRIZ_GYE#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.

MATRIZ_GYE(config)#router ospf 1
MATRIZ_GYE(config-router)#network 192.168.9.4 0.0.0.3 area 0
MATRIZ_GYE(config-router)#network 192.168.9.4 0.0.0.8 area 0
MATRIZ_GYE(config-router)#network 192.168.9.4 0.0.0.12 area 0
MATRIZ_GYE(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

MATRIZ_GYE#wr
Building configuration...
[OK]

MATRIZ_GYE#
```

### 8.12.3.-ROUTER MATRIZ QUITO (OSPF 1)

```
QUITO#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
QUITO(config)#router ospf 1
QUITO(config-router)#network 192.168.9.8 0.0.0.3 area 0
QUITO(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

QUITO#wr
Building configuration...
[OK]

QUITO#
```

### 8.12.4.-ROUTER (MATRIZ) GUAYAQUIL (OSPF 1)

```
GYE(config)#router ospf 1
GYE(config-router)#network 192.168.9.0 0.0.0.3 area 0
GYE(config-router)#network 192.168.9.4 0.0.0.3 area 0
GYE(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

GYE#wr
Building configuration...
[OK]
```

### 8.12.5.-ROUTER (PROVEEDOR DE INTERNET) ISP

```
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#router ospf 1
ISP(config-router)#network 192.168.9.0 0.0.0.3 area 0
ISP(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

ISP#wr
Building configuration...
[OK]

ISP#|
```

### 8.12.6.-ROUTER (SUCURSAL) TAME CARGO (RIP V2)

```
TAME_CARGO#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TAME_CARGO(config)#route
TAME_CARGO(config)#router rip
TAME_CARGO(config-router)#version 2
TAME_CARGO(config-router)#network 192.168.9.16
TAME_CARGO(config-router)#network 192.168.11.0
TAME_CARGO(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

TAME_CARGO#wr
Building configuration...
[OK]

TAME_CARGO#|
```

### 8.12.7.-ROUTER (SUCURSAL) BUEN DIA (RIP V2)

```
BUEN_DIA#inter
BUEN_DIA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUEN_DIA(config)#router rip
BUEN_DIA(config-router)#version 2
BUEN_DIA(config-router)#network 192.168.9.20
BUEN_DIA(config-router)#network 192.168.12.0
BUEN_DIA(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

BUEN_DIA#wr
Building configuration...
[OK]

BUEN_DIA#|
```

8.12.8.-ROUTER (SUCURSAL) GRAN PASAJES (RIP V2)

```
GRAN_PASAJES#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GRAN_PASAJES(config)#router rip
GRAN_PASAJES(config-router)#version 2
GRAN_PASAJES(config-router)#network 192.168.9.24
GRAN_PASAJES(config-router)#network 192.168.13.0
GRAN_PASAJES(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

GRAN_PASAJES#wr
Building configuration...
[OK]
```

```
GRAN_PASAJES#|
```

COMANDOS	DETALLE
Configure Terminal	Modo de configuración Global
Router rip	Asigna el tipo de protocolos de que va a trabajar
Versión 2	Asigna el tipo de versión de rip que van a atrabajar
Network (direccion red)	Asignas las redes de origen que pertenecerán a un protocolo enrutamiento
Redistribuye ospf 1	Redistribuye los diferentes protocolos del uno con el otro protocolo diferente
(Control) Z	Retrocedo a modo privilegiado
Wr	Permite guardar el cambio efectuado

Tabla 7 - 8: Comando para los protocolos de enrutamiento



## 8.13.-SHOW IP ROUTER

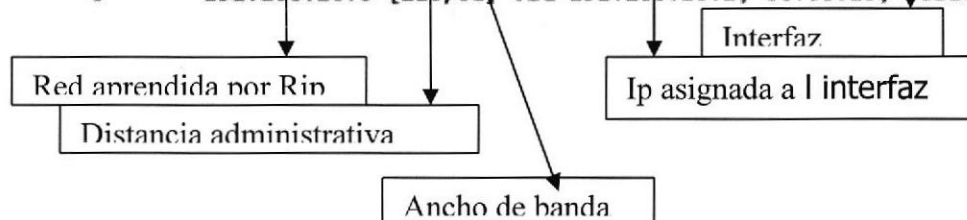
Como ya le tenemos detallado en la parte conceptual el comando Show Ip Route nos permitirá ver la tabla de ruteo de los diferente Router

### 8.13.1.-ROUTER FRONTERA GUAYAQUIL

```
CORE_MATRIZ#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route
```

Gateway of last resort is not set

```
192.168.9.0/30 is subnetted, 6 subnets
C    192.168.9.16 is directly connected, Serial0/1
C    192.168.9.20 is directly connected, Serial0/2
C    192.168.9.24 is directly connected, Serial0/3
C    192.168.9.12 is directly connected, Serial0/0
O    192.168.9.8 [110/128] via 192.168.9.13, 00:00:14, Serial0/0
O    192.168.9.4 [110/128] via 192.168.9.13, 00:00:14, Serial0/0
192.168.12.0/27 is subnetted, 1 subnets
R    192.168.12.0 [120/1] via 192.168.9.22, 00:07:41, Serial0/2
192.168.13.0/27 is subnetted, 1 subnets
R    192.168.13.0 [120/1] via 192.168.9.26, 00:08:24, Serial0/3
192.168.11.0/27 is subnetted, 1 subnets
R    192.168.11.0 [120/1] via 192.168.9.18, 00:02:31, Serial0/1
192.168.10.0/27 is subnetted, 1 subnets
O    192.168.10.0 [110/64] via 192.168.10.1, 00:00:10, Serial0/3
```



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.

### 8.13.2.-ROUTER MATRIZ GUAYAQUIL

```
MATRIZ_GYE#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route
```

```
Gateway of last resort is not set
```

```
192.168.9.0/30 is subnetted, 4 subnets
C      192.168.9.12 is directly connected, Serial0/1
C      192.168.9.8 is directly connected, Serial0/0
C      192.168.9.4 is directly connected, Serial0/2
O      192.168.9.0 [110/128] via 192.168.9.6, 00:12:46, Serial0/2
192.168.10.0/27 is subnetted, 1 subnets
C      192.168.10.0 is directly connected, FastEthernet1/0
```

```
MATRIZ_GYE#
```

```
MATRIZ_GYE#show running-config
Building configuration...
```

```
--MORE--
```

### 8.13.3.-ROUTER MATRIZ QUITO

```
QUITO#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route
```

```
Gateway of last resort is not set
```

```
192.168.9.0/30 is subnetted, 6 subnets
C      192.168.9.8 is directly connected, Serial0
O      192.168.9.4 [110/128] via 192.168.9.9, 00:09:23, Serial0
O      192.168.9.12 [110/64] via 192.168.9.13, 00:09:18, Serial0
O E2   192.168.9.20 [120/1] via 192.168.12.1, 00:00:58, Serial0
O E2   192.168.9.16 [120/2] via 192.168.12.1, 00:00:58, Serial0
O E2   192.168.9.24 [120/2] via 192.168.12.1, 00:00:58, Serial0
192.168.13.0/27 is subnetted, 1 subnets
O E2   192.168.13.0 [120/3] via 192.168.12.1, 00:00:58, Serial0
```

## 8.13.4.-ROUTER (MATRIZ) GUAYAQUIL

```

MATRIZ_GYE#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route

Gateway of last resort is not set

    192.168.9.0/30 is subnetted, 4 subnets
C       192.168.9.12 is directly connected, Serial0/1
C       192.168.9.8 is directly connected, Serial0/0
C       192.168.9.4 is directly connected, Serial0/2
O       192.168.9.0 [110/128] via 192.168.9.6, 00:12:46, Serial0/2
    192.168.10.0/27 is subnetted, 1 subnets
C       192.168.10.0 is directly connected, FastEthernet1/0

```

## 8.13.5.-ROUTER (PROVEEDOR DE INTERNET) ISP

```

ISP#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route

Gateway of last resort is not set

    192.168.9.0/30 is subnetted, 4 subnets
C       192.168.9.0 is directly connected, Serial0
O       192.168.9.4 [110/64] via 192.168.9.6, 00:42:40, Serial0
O       192.168.9.8 [110/256] via 192.168.9.2, 00:40:20, Serial0
O       192.168.9.12 [110/192] via 192.168.9.2, 00:40:10, Serial0
    192.168.10.0/27 is subnetted, 1 subnets
O       192.168.10.0 [110/192] via 192.168.9.2, 00:24:38, Serial0

ISP#

```

## 8.13.6.-ROUTER (SUCURSAL) TAME CARGO

TAME\_CARGO#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
 U - per-user static route

Gateway of last resort is not set

```

192.168.9.0/30 is subnetted, 4 subnets
C    192.168.9.16 is directly connected, Serial0
R    192.168.9.20 [120/1] via 192.168.9.17, 00:01:32, Serial0
R    192.168.9.24 [120/1] via 192.168.9.17, 00:07:33, Serial0
R    192.168.9.12 [120/1] via 192.168.9.17, 00:02:38, Serial0
192.168.11.0/27 is subnetted, 1 subnets
C    192.168.11.0 is directly connected, FastEthernet0/0
192.168.12.0/27 is subnetted, 1 subnets
R    192.168.12.0 [120/2] via 192.168.9.17, 00:02:44, Serial0
192.168.13.0/27 is subnetted, 1 subnets
R    192.168.13.0 [120/2] via 192.168.9.17, 00:09:25, Serial0

```

## 8.13.7.-ROUTER (SUCURSAL) BUEN DIA

BUEN\_DIA#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
 U - per-user static route

Gateway of last resort is not set

```

192.168.9.0/30 is subnetted, 4 subnets
C    192.168.9.20 is directly connected, Serial0
R    192.168.9.16 [120/1] via 192.168.9.21, 00:05:24, Serial0
R    192.168.9.24 [120/1] via 192.168.9.21, 00:06:20, Serial0
R    192.168.9.12 [120/1] via 192.168.9.21, 00:03:22, Serial0
192.168.12.0/27 is subnetted, 1 subnets
C    192.168.12.0 is directly connected, FastEthernet0/0

```



### 8.13.8.-ROUTER (SUCURSAL) GRAN PASAJES

GRAN\_PASAJE#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default  
U - per-user static route

Gateway of last resort is not set

192.168.9.0/30 is subnetted, 4 subnets  
C 192.168.9.24 is directly connected, Serial0  
R 192.168.9.16 [120/1] via 192.168.9.25, 00:05:35, Serial0  
R 192.168.9.20 [120/1] via 192.168.9.25, 00:07:24, Serial0  
R 192.168.9.12 [120/1] via 192.168.9.25, 00:03:30, Serial0  
192.168.13.0/27 is subnetted, 1 subnets  
C 192.168.13.0 is directly connected, FastEthernet0/0

## 8.14.-PRUEBAS DE PING ENTRE MATRIZ Y SUCURSALES

Ya se configurados las interfaces de cada uno de los router levantándola y verificándolas ahora se a probar haciéndole ping para ver si hay comunicación entre la Matriz y sus sucursales

### 8.14.1.-ROUTER FRONTERA GUAYAQUIL

Hacer ping a las interfaces conectada con el router matriz que son los router de matriz GYE las sucursales TAME Cargo Buen Día Gran Pasajes

```
CORE_MATRIZ#ping 192.168.9.13
```

Señal de interfaces conectadas

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.13, timeout is 2 seconds:  
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
CORE_MATRIZ#ping 192.168.9.18
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.18, timeout is 2 seconds:  
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
CORE_MATRIZ#ping 192.168.9.22
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.22, timeout is 2 seconds:  
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
CORE_MATRIZ#ping 192.168.9.26
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.26, timeout is 2 seconds:  
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
CORE_MATRIZ#
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento rip v2 y ospf 1

```
CORE_MATRIZ#ping 192.168.9.9
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.9, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
CORE_MATRIZ#ping 192.168.9.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
CORE_MATRIZ#
```

### 8.14.2.-ROUTER MATRIZ GUAYAQUIL

Hacer ping a las interfaces conectada con el router de matriz GYE

```
MATRIZ_GYE#ping 192.168.9.6
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
MATRIZ_GYE#ping 192.168.9.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.10, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
MATRIZ_GYE#ping 192.168.9.14
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.14, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
MATRIZ_GYE#
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento ospf  
1

```
MATRIZ_GYE#ping 192.168.9.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
MATRIZ_GYE#
```

### 8.14.3.-ROUTER MATRIZ QUITO

Hacer ping a las interfaces conectada con el router de matriz Quito

```
QUITO#ping 192.168.9.9
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.9, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
QUITO#
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento ospf  
1

```
QUITO#ping 192.168.9.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
QUITO#ping 192.168.9.13
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.13, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
QUITO#ping 192.168.9.14
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.14, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
QUITO#ping 192.168.9.6
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
QUITO#
```



#### 8.14.4.-ROUTER (MATRIZ) GUAYAQUIL

Hacer ping a las interfaces conectada con el router de GYE

```
GYE#ping 192.168.9.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GYE#ping 192.168.9.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento ospf  
1

```
GYE#ping 192.168.9.9
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.9, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GYE#ping 192.168.9.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.10, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GYE#ping 192.168.9.13
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.13, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GYE#ping 192.168.9.14
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.14, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

### 8.14.5.-ROUTER (PROVEEDOR DE INTERNET) ISP

Hacer ping a las interfaces conectada con el router del ISP

```
ISP#ping 192.168.9.2
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
ISP#
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento ospf  
1

```
ISP#ping 192.168.9.6
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
ISP#ping 192.168.9.5
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
ISP#ping 192.168.9.13
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.9.13, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
ISP#ping 192.168.9.9
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.9.9, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
ISP#ping 192.168.9.10
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.9.10, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
ISP#ping 192.168.9.14
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.9.14, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
ISP#
```

#### 8.14.6.-ROUTER (SUCURSAL) TAME CARGO

Hacer ping a las interfaces conectada con el router sucursales TAME Cargo

```
TAME_CARGO#ping 192.168.9.17
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.17, timeout is 2 seconds:
```

```
!!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
TAME_CARGO#
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento rip v2

```
TAME_CARGO#ping 192.168.9.14
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.14, timeout is 2 seconds:
```

```
!!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
TAME_CARGO#ping 192.168.12.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
```

```
!!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
TAME_CARGO#ping 192.168.13.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.13.1, timeout is 2 seconds:
```

```
!!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
TAME_CARGO#
```

### 8.14.7.-ROUTER (SUCURSAL) BUEN DIA

Hacer ping a las interfaces conectada con el router sucursales Buen Día

```
BUEN_DIA#ping 192.168.9.21
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.21, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
BUEN_DIA#
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento rip v2

```
BUEN_DIA#ping 192.168.9.14
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.14, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
BUEN_DIA#ping 192.168.11.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
BUEN_DIA#ping 192.168.13.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.13.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
BUEN_DIA#
```

### 8.14.8.-ROUTER (SUCURSAL) GRAN PASAJES

Hacer ping a las interfaces conectada con el router sucursales Gran Pasajes

```
GRAN_PASAJE#ping 192.168.9.25
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.25, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GRAN_PASAJE#
```

Luego hacer ping a las interfaces que aprendió por los protocolos de enrutamiento rip v2

```
GRAN_PASAJE#ping 192.168.9.14
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.9.14, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GRAN_PASAJE#ping 192.168.11.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GRAN_PASAJE#ping 192.168.12.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
GRAN_PASAJE#
```

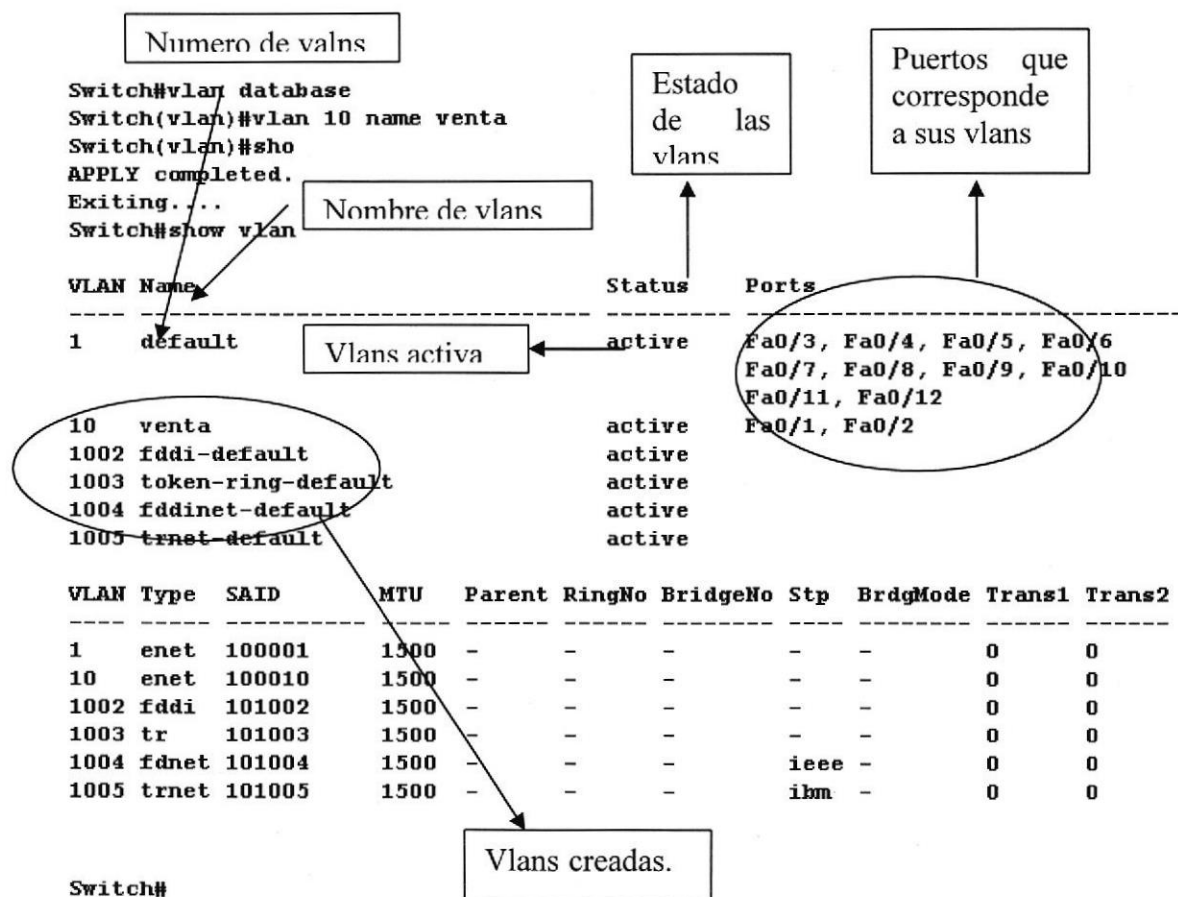
## 8.15.-CONFIGURACIÓN DE LAS VLANS

Para comenzar a configurar las Vlan's debe haber segmentado bien las diferentes redes por departamentos como mas conocido el Subneteo para los departamentos

### 8.15.1.-CONFIGURACIÓN DE VLANS (SUCURSAL) TAME CARGO

#### 8.15.1.1.-SWITCH TAME CARGO

Comenzar A Declara las Vlan's a darle sus respectivo nombres y verificar



**VLAN.-** Es el numero de la vlan.

**Name.-** Es el nombre asignado a la vlan.

**Status.-** Es el estado en que se encuentra la vlan.

**Ports.-** Son los puertos asignados a la vlan.

Comenzar habilitar las subinterfaces del switch en sus respectivos puertos y luego verificar

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show 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
10	venta	active	Fa0/1, 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
10	enet	100010	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

```
Switch#
```

### 8.15.1.2.-ROUTER (SUCURSAL) TAME CARGO

Ya configurado los puerto del switch ahora debe configurar en le router asignándole sus respectiva ip a cada subinterfaz

```
TAME_CARGO(config)#interface fastethernet 0/0.1
TAME_CARGO(config-subif)#encapsulation dot1q 10
TAME_CARGO(config-subif)#interface fastethernet 0/0.2
TAME_CARGO(config-subif)#encapsulation dot1q 10
TAME_CARGO(config-subif)#ip address 192.168.11.33 255.255.255.224
TAME_CARGO(config-subif)#no shutdown
TAME_CARGO(config-subif)#^Z
%SYS-5-CONFIG_I: Configured from console by console

TAME_CARGO#wr
Building configuration...
[OK]

TAME_CARGO#
```

### 8.15.1.3.-HOST DE LA SUCURSALES TAME CARGO

Le configurar la ip correspondiente

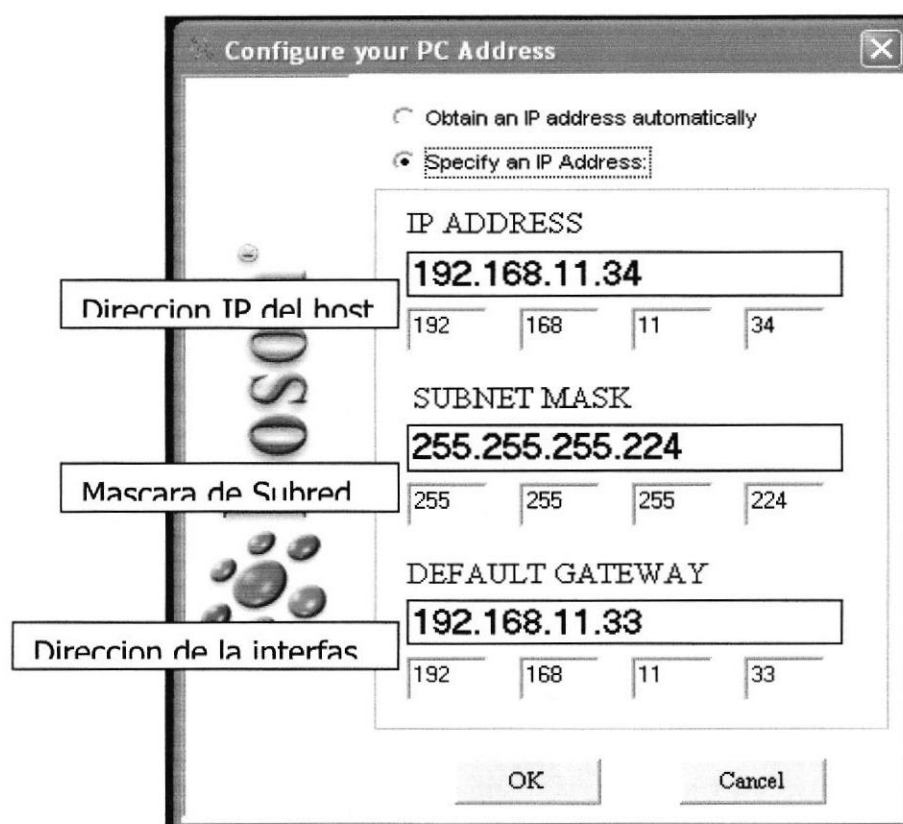


FIGURA 7 - 32: Configuración del Host



Luego hacer ping a la subinterfaces y al router de la sucursal

```
C:\#ping 192.168.11.33
Pinging 192.168.11.33 with 32 bytes of data:

Reply from 192.168.11.33: bytes=32 time=60ms TTL=241
Reply from 192.168.11.33: bytes=32 time=60ms TTL=241
Reply from 192.168.11.33: bytes=32 time=60ms TTL=241
Reply from 192.168.11.33: bytes=32 time=60ms TTL=241
Reply from 192.168.11.33: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.33:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms

C:\#ping 192.168.9.18
Pinging 192.168.9.18 with 32 bytes of data:

Reply from 192.168.9.18: bytes=32 time=60ms TTL=241
Reply from 192.168.9.18: bytes=32 time=60ms TTL=241
Reply from 192.168.9.18: bytes=32 time=60ms TTL=241
Reply from 192.168.9.18: bytes=32 time=60ms TTL=241
Reply from 192.168.9.18: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.9.18:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms

C:\#|
```

FIGURA 7 - 33: Ping a la subinterfaces

## 8.15.2.-CONFIGURACIÓN DE LA VLANS (SUCURSAL) BUEN DIA

### 8.15.2.1.-SWITCH BUEN DIA

Comenzara Declara las Vlan`s a darle sus respectivo nombres y verificar

```
Switch#vlan database
Switch(vlan)#vlan 20 name gerencia
APPLY completed.
Exiting....
Switch#show 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
20	gerencia	active	Fa0/1, 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
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

```
Switch#
```

Comenzar habilitar las subinterfaces del switch en sus respectivos puertos y luego verificar

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
Switch(config-if)#switchport access vlan 20
Switch(config-if)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show 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
20	gerencia	active	Fa0/1, 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
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

```
Switch#
```

### 8.15.2.2.-ROUTER (SUCURSAL) BUEN DIA

Ya configurado los puerto del switch ahora debe configurar en le router asignándole sus respectiva ip a cada subinterfaz

```
BUEN_DIA#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.

BUEN_DIA(config)#interface fastethernet 0/0.1
BUEN_DIA(config-subif)#encapsulation dot1q 20
BUEN_DIA(config-subif)#interface fastethernet 0/0.2
BUEN_DIA(config-subif)#encapsulation dot1q 20
BUEN_DIA(config-subif)#ip address 192.168.12.33 255.255.255.224
BUEN_DIA(config-subif)#no shutdown
BUEN_DIA(config-subif)#^Z
%SYS-5-CONFIG_I: Configured from console by console

BUEN_DIA#wr
Building configuration...
[OK]
```

BUEN\_DIA#

### 8.15.2.3.-HOST DE LA SUCURSAL BUEN DIA

Le configurar la ip correspondiente

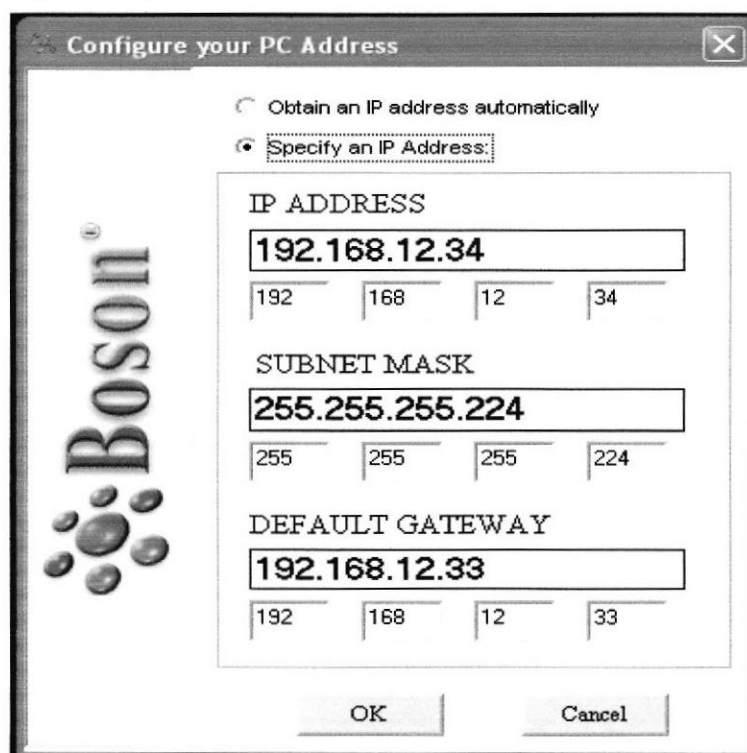


FIGURA 7 – 34: configuración del Host

Luego hacer ping a la subinterfaces y al router de la sucursal

```
C:#ping 192.168.12.33
Pinging 192.168.12.33 with 32 bytes of data:

Reply from 192.168.12.33: bytes=32 time=60ms TTL=241
Reply from 192.168.12.33: bytes=32 time=60ms TTL=241
Reply from 192.168.12.33: bytes=32 time=60ms TTL=241
Reply from 192.168.12.33: bytes=32 time=60ms TTL=241
Reply from 192.168.12.33: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.12.33:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms

C:#ping 192.168.9.22
Pinging 192.168.9.22 with 32 bytes of data:

Reply from 192.168.9.22: bytes=32 time=60ms TTL=241
Reply from 192.168.9.22: bytes=32 time=60ms TTL=241
Reply from 192.168.9.22: bytes=32 time=60ms TTL=241
Reply from 192.168.9.22: bytes=32 time=60ms TTL=241
Reply from 192.168.9.22: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.9.22:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms

C:#
```

**FIGURA 7 - 35:** Ping a la subinterfaces

### 8.15.3.-CONFIGURACIÓN DE VLANS (SUCURSAL) GRAN PASAJES

#### 8.15.3.1.-SWITCH GRAN PASAJES

Comenzar A Declara las Vlan`s a darle sus respectivo nombres y verificar

```
Switch#vlan database
Switch(vlan)#vlan 30 name presidencia
APPLY completed.
Exiting....
Switch#show v
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
300	300	active	Fa0/1, Fa0/2
30	presidencia	active	Fa0/3, Fa0/4
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
300	enet	100300	1500	-	-	-	-	-	0	0
30	enet	100030	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	-	-	-	ihm	-	0	0

Switch# |

Comenzar habilitar las subinterfaces del switch en sus respectivos puertos y luego verificar

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 30
Switch(config-if)#interface fastethernet 0/4
Switch(config-if)#switchport access vlan 30
Switch(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
300	300	active	Fa0/1, Fa0/2
30	presidencia	active	Fa0/3, Fa0/4
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
300	enet	100300	1500	-	-	-	-	-	0	0
30	enet	100030	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

```
Switch# |
```

### 8.15.3.2.-ROUTER (SUCURSAL) GRAN PASAJES

Ya configurado los puerto del switch ahora debe configurar en le router asignándole sus respectiva ip a cada subinterfaz

```
GRAN_PASAJE#
GRAN_PASAJE#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
GRAN_PASAJE(config)#interface fastethernet 0/0.3
GRAN_PASAJE(config-subif)#sw
GRAN_PASAJE(config-subif)#encapsulation dot1q 30
GRAN_PASAJE(config-subif)#interface fastethernet 0/0.4
GRAN_PASAJE(config-subif)#encapsulation dot1q 30
GRAN_PASAJE(config-subif)#ip address 192.168.13.65 255.255.255.224
GRAN_PASAJE(config-subif)#no shutdown
GRAN_PASAJE(config-subif)#^Z
%SYS-5-CONFIG_I: Configured from console by console

GRAN_PASAJE#wr
Building configuration...
[OK]

GRAN_PASAJE#|
```

GRAN\_PASAJES(config-subif)interface fasteternet 0/0.3

Esta línea indica como declarar las sub-interfaces del router.

GRAN\_PASAJES (config-subif)# ip address 192.168.13.65 255.255.255.224

Esta línea permite asignar una dirección Ip a la sub-interfaces del router con la mascara de subred.

GRAN\_PASAJES (config-subif)# encapsulation dot1q 30

En esta línea mostramos el encapsulamiento de la vlan.

GRAN\_PASAJES (config- subif)# no shutdown

En esta línea permite levantar la sub-interfaces del router.



### 8.15.3.3.-HOST DE LA SUCURSAL GRAN PASAJES

Le configurar la ip correspondiente

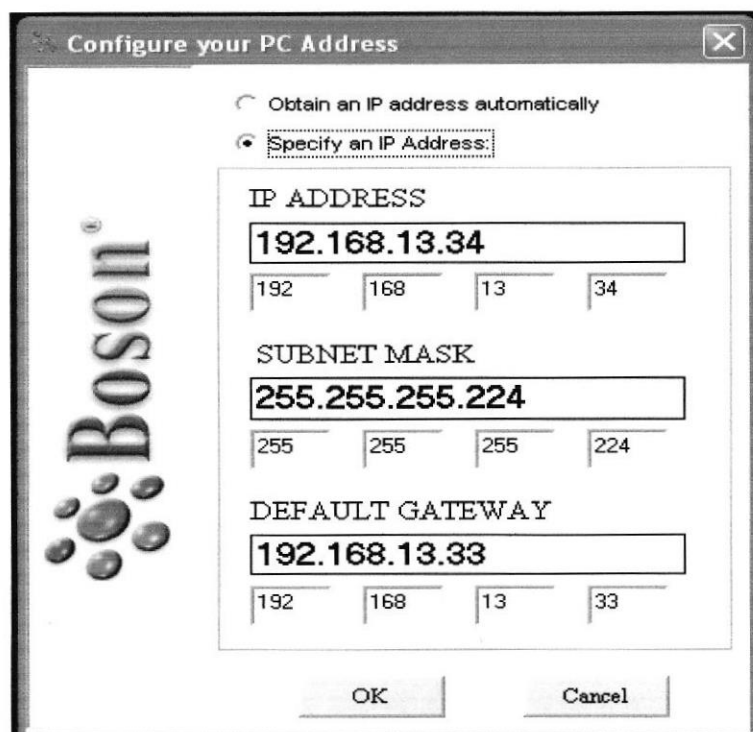


FIGURA 7 - 36: Configuración del Host

Luego hacer ping a la subinterfaces y al router de la sucursal

```
C:\#ping 192.168.13.33
Pinging 192.168.13.33 with 32 bytes of data:

Reply from 192.168.13.33: bytes=32 time=60ms TTL=241
Reply from 192.168.13.33: bytes=32 time=60ms TTL=241
Reply from 192.168.13.33: bytes=32 time=60ms TTL=241
Reply from 192.168.13.33: bytes=32 time=60ms TTL=241
Reply from 192.168.13.33: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.13.33:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 60ms, Average = 55ms

C:\#ping 192.168.9.26
Pinging 192.168.9.26 with 32 bytes of data:

Reply from 192.168.9.26: bytes=32 time=60ms TTL=241
Reply from 192.168.9.26: bytes=32 time=60ms TTL=241
Reply from 192.168.9.26: bytes=32 time=60ms TTL=241
Reply from 192.168.9.26: bytes=32 time=60ms TTL=241
Reply from 192.168.9.26: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.9.26:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 60ms, Average = 55ms

C:\#|
```

FIGURA 7 - 37: Ping a la subinterfaces

## 8.15.4.-CONFIGURACIÓN DE VLANS MATRIZ GUAYAQUIL

### 8.15.4.1.-SWITCH 1 MATRIZ GUAYAQUIL

Comenzara A Declara las Vlan`s a darle sus respectivo nombres y verificar

```
Switch#vlan database
Switch(vlan)#vlan 40 name gerencia
VLAN 40 added:
    Name:gerencia
APPLY completed.
Exiting....
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
40	gerencia	active	
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
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	-	-	-	ihm	-	0	0

Switch#

Switch#vlan database

En esta línea mostramos como crear una vlan.

Switch(vlan)# vlan 40 name gerencia

En esta línea mostramos como crear una vlan con su nombre.

Name: gerencia

Comenzar habilitar las subinterfaces del switch en sus respectivos puertos y luego verificar

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#inet
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 40
Switch(config-if)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 40
Switch(config-if)#interface fastethernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 40
Switch(config-if)#interface fastethernet 0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 40
Switch(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
40	gerencia	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
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
40	enet	100040	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0

```
Switch# |
```

Switch # configure terminal

Esta línea permite ingresar al modo global.

Switch (config)# interface fastethernet 0/1

En esta línea entrar a al interfaz del switch.

Switch (config)#switchport mode trunk

En esta línea Definir un puerto en modo truncado

Switch (config)#switchport access vlan 40

En esta línea asignar a la vlan una o más interfaces:

Switch (config)# interface fastethernet 0/2

En esta línea entrar a al interfaz del switch.

Switch (config)#switchport access vlan 40

En esta línea asignar a la vlan una o más interfaces:

Switch (config)# interface fastethernet 0/3

En esta línea entrar a al interfaz del switch.

Switch (config)#switchport access vlan 40

En esta línea asignara la vlan una o más interfaces

Switch (config)# interface fastethernet 0/4

En esta línea entrar a al interfaz del switch.

Switch (config)#switchport access vlan 40

En esta línea asignar a la vlan una o más interfaces:

#### 8.15.4.2.-SWITCH 2 MATRIZ GUAYAQUIL

Comenzar A Declara las Vlan`s a darle sus respectivo nombres y verificar

```
Switch#vlan database
Switch(vlan)#vlan 50 name sistema
VLAN 50 added:
  Name:sistema
APPLY completed.
Exiting....
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
50	sistema	active	
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
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

Switch#

Comenzar habilitar las subinterfaces del switch en sus respectivos puertos y luego verificar

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 50
Switch(config-if)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 50
Switch(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show 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
50	sistema	active	Fa0/1, 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
50	enet	100050	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	-	-	-	ikm	-	0	0

```
Switch#
```

## 8.15.4.3.-SWITCH 3 MATRIZ GUAYAQUIL

Comenzar A Declara las Vlan's a darle sus respectivo nombres y verificar

```
Switch#vlan database
Switch(vlan)#vlan 60 name venta
VLAN 60 added:
  Name:venta
Switch(vlan)#sho
APPLY completed.
Exiting....
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
60	venta	active	
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
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

```
Switch#|
```

Comenzar habilitar las subinterfaces del switch en sus respectivo puertos y luego Verificar

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 60
Switch(config-if)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 60
Switch(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show 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
60	venta	active	Fa0/1, 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
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

```
Switch#
```

#### 8.15.4.4.-ROUTER MATRIZ GUAYAQUIL

Ya configurado los puerto del switch ahora debemos configurar en le router asignándole sus respectiva ip a cada subinterfaz

```
MATRIZ_GYE#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.

MATRIZ_GYE(config)#interface fastethernet 1/0.1
MATRIZ_GYE(config-subif)#encapsulation dot1q 40
MATRIZ_GYE(config-subif)#
MATRIZ_GYE(config-subif)#interface fastethernet 1/0.2
MATRIZ_GYE(config-subif)#encapsulation dot1q 40
MATRIZ_GYE(config-subif)#ip address 192.168.10.33 255.255.255.224
MATRIZ_GYE(config-subif)#interface fastethernet 1/0.3
MATRIZ_GYE(config-subif)#encapsulation dot1q 40
MATRIZ_GYE(config-subif)#interface fastethernet 1/0.4
MATRIZ_GYE(config-subif)#encapsulation dot1q 40
MATRIZ_GYE(config-subif)#ip address 192.168.10.65 255.255.255.224
MATRIZ_GYE(config-subif)#interface fastethernet 1/0.5
MATRIZ_GYE(config-subif)#encapsulation dot1q 40
MATRIZ_GYE(config-subif)#interface fastethernet 1/0.6
MATRIZ_GYE(config-subif)#encapsulation dot1q 40
MATRIZ_GYE(config-subif)#ip address 192.168.10.97 255.255.255.224
MATRIZ_GYE(config-subif)#no shutdown
MATRIZ_GYE(config-subif)#^Z
%SYS-5-CONFIG_I: Configured from console by console

MATRIZ_GYE#wr
Building configuration...
[OK]

MATRIZ_GYE#|
```



#### 8.15.4.5.-HOSTS DE LA MATRIZ GYE

Le configuramos la ip correspondiente

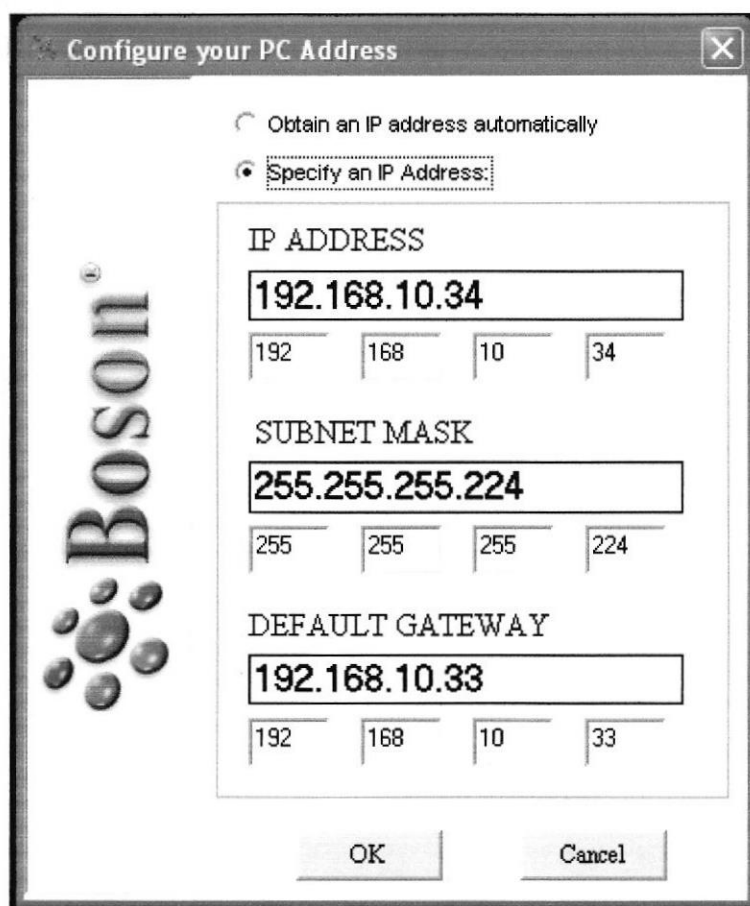


FIGURA 7 – 38: Configurar el Host

Le configuramos la ip correspondiente

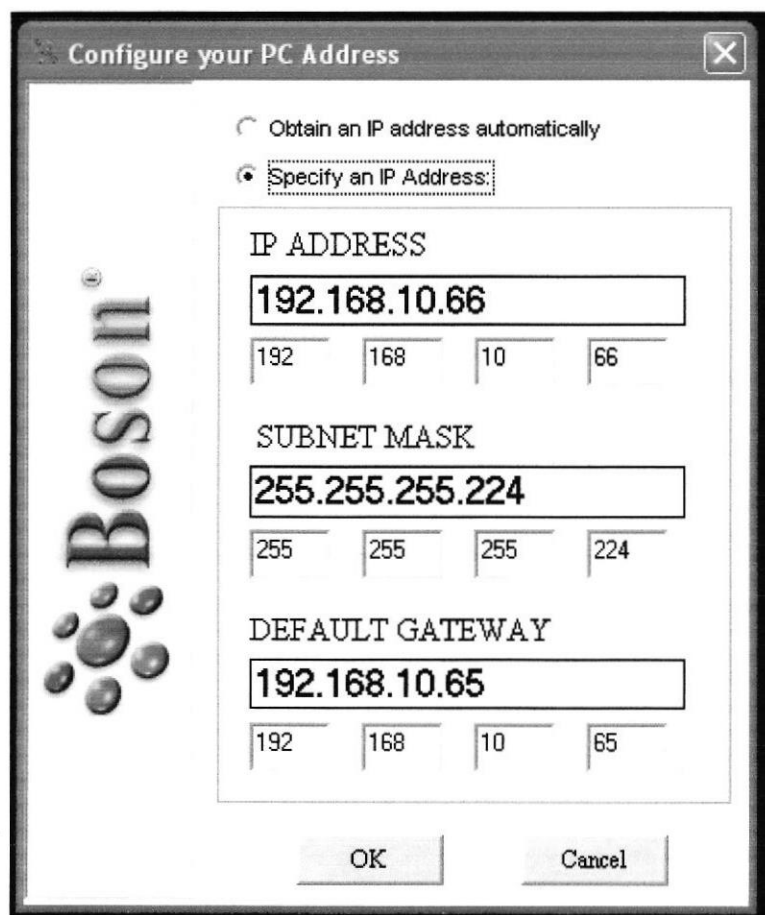


FIGURA 7 - 39: Configurar el Host

Le configurarla ip correspondiente

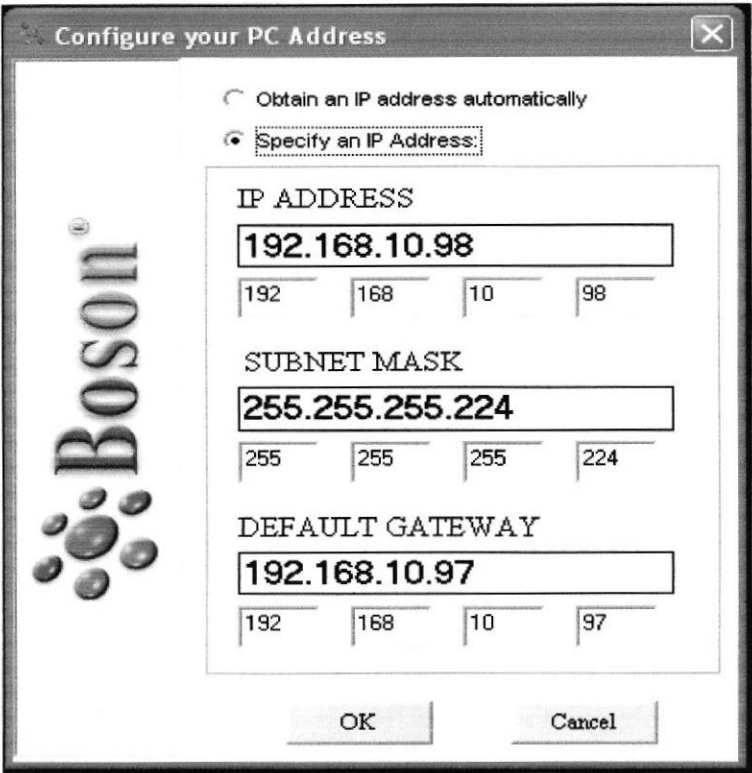


FIGURA 7 - 40: Configurar el Host

Luego hacer ping a la subinterfaces y al router de la sucursal

```
C:\#ping 192.168.10.33
Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=60ms TTL=241
Reply from 192.168.10.33: bytes=32 time=60ms TTL=241
Reply from 192.168.10.33: bytes=32 time=60ms TTL=241
Reply from 192.168.10.33: bytes=32 time=60ms TTL=241
Reply from 192.168.10.33: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.10.33:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms

C:\#ping 192.168.10.65
Pinging 192.168.10.65 with 32 bytes of data:

Reply from 192.168.10.65: bytes=32 time=60ms TTL=241
Reply from 192.168.10.65: bytes=32 time=60ms TTL=241
Reply from 192.168.10.65: bytes=32 time=60ms TTL=241
Reply from 192.168.10.65: bytes=32 time=60ms TTL=241
Reply from 192.168.10.65: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.10.65:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms
```

FIGURA 7 - 41: Ping a las Subinterfaces



# ANEXO

## GLOSARIO DE TÉRMINOS

## GLOSARIO DE TÉRMINOS

### A

**Ancho de Banda:** La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también se usa para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

**Arp:** Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Comparar con RARP.

**Asignación de direcciones:** Técnica que permite que distintos protocolos interoperen traduciendo direcciones desde un formato a otro. Por ejemplo, al enrutar IP a través de una red Frame Relay, las direcciones IP se deben mapear a las direcciones Frame Relay de modo que los paquetes IP se puedan transmitir por la red. Ver también resolución de direcciones.

### B

**Banda Ancha:** Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica. Comparar con banda ancha.

**Broadcast:** Envío de información en cualquier formato a más de un lugar de destino

**Banda Base:** Característica de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha. Ver la diferencia con banda ancha. Término utilizado en la WWW.

**Bps:** (Bits per Second). Medida que representa la rapidez con que los bits de datos se transmiten a través de un medio de comunicaciones. Por ejemplo: un módem de 28.8 Kbps es capaz de transferir 28.800 bits por segundo.

**Bit:** (Binary Digit ó Dígito Binario). Es un dígito en base 2, es decir, 0 ó 1. Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

**Byte:** Unidad de medida de la cantidad de información en formato digital. Usualmente un byte consiste de 8 bits. Un bit es un cero (0) o un uno (1). Esa secuencia de números (byte) pueden simbolizar una letra o un espacio (un carácter). Un kilobyte (Kb) son 1024 bytes y un Megabyte (Mb) son 1024 Kilobytes.

**Bloqueo:** En un sistema de conmutación, una condición en el que no hay ninguna ruta disponible para completar un circuito. El término también se usa para describir una situación en la que no se puede iniciar una actividad hasta que la otra no se haya completado.

# C

**Cable blindado:** Cable que posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

**Cable coaxial:** Cable compuesto por un conductor cilíndrico exterior hueco que rodea un conductor de alambre interno-único. En la actualidad se usan dos tipos de cable coaxial en la LAN: cable de 50 ohmios, que se usa para la señalización digital, y cable de 75 ohmios que se usa para señales analógicas y señalización digital de alta velocidad.

**Cable de fibra óptica:** Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro, sin embargo no es susceptible a la interferencia electromagnética y es capaz de brindar velocidades de datos más altas.

**Cable neutro:** Cable de circuito que se conecta a la conexión a tierra en la central de energía y en el transformador.

**Cableado backbone:** Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN. Ver cableado vertical.

**Cableado de Categoría 1:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 1 se usa para comunicaciones telefónicas y no es adecuado para transmitir datos. Comparar con cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

**Cableado de Categoría 2:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

**Cableado de Categoría 3:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 3 se usa en las redes 10BASE-T y puede transmitir datos a velocidades de hasta 10 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

**Cableado de Categoría 4:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 4 se usa en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

**Cableado de Categoría 5:** Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 4. Ver también EIA/TIA-568B y UTP.

**Caché:** Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso más rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los accesos a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

**Canaleta decorativa:** Tipo de canal montado en la pared que tiene una cubierta removible que se usa para admitir el cableado horizontal. La canaleta decorativa es lo suficientemente grande como para contener dos cables.

**Canaleta:** Un tipo de canal adosado a la pared que tiene una cubierta removible para dar apoyo al cableado horizontal. La canaleta es lo suficientemente grande como para contener varios cables.

**Capa física:** La Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

**Capa de control de enlace de datos:** La Capa 2 del modelo de arquitectura SNA. Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

**Capa de red:** La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

**Capa de transporte:** La Capa 4 del modelo de referencia OSI. Esta capa es responsable de la comunicación confiable de red entre nodos finales. La capa de transporte suministra mecanismos para establecer, mantener y terminar los circuitos virtuales, detección y recuperación de errores de transporte y control del flujo de información.

**Capa de sesión:** La Capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de capa de presentación.



**Capa de servicios de presentación:** La Capa 6 del modelo de arquitectura SNA. Esta capa suministra administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Corresponde aproximadamente a la capa de presentación del modelo OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control física, capa de servicios de transacción y capa de control de transmisión.

**Capa de aplicación:** La Capa 7 del modelo de referencia OSI. Esta capa suministra servicios a los procesos de aplicación (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de terminal) que están fuera del modelo OSI. La capa de aplicación identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos que se requieren para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos. Corresponde aproximadamente a la capa de servicios de transacción del modelo SNA. Ver también capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

**Cliente:** Nodo que solicita servicios a un servidor.

**Colisión:** En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

**Cola:** Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

**Conector RJ:** Conector macho registrado. Conectores estándar que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ.

**Costo:** Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.

**Consola:** DTE a través del cual se introducen los comandos en un host.

**Correo electrónico:** Aplicación de red utilizada ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.



**CSMA/CD:** Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

**Clic:** Acción de presionar y soltar rápidamente el botón del mouse (ratón).

**Cliente:** Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

**Computador:** Es un dispositivo electrónico compuesto básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

**Contraseña ó Password:** Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los Sistemas y recursos de la computadora.

**CPU;** (Central Processing Unit ó Unidad central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

**Cuadro de Diálogo:** Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

**Cuadro de Texto:** Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de diálogo, el cuadro de texto puede estar en blanco o contener texto.

**Cursor:** Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo carácter a visualizar cuando se pulse una tecla.

**CSU:** Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con el loop telefónico digital local. A menudo se denomina, de forma conjunta con DSU, como CSU/DSU.

# D

**Db:** Decibelios

**Dominio:** En Internet, una parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía

**DCE:** Equipo de comunicación de datos. Equipo de comunicación de datos (expansión EIA) o equipo de terminación de circuito de datos (expansión ITU-T). El dispositivo y las conexiones de una red de comunicaciones que abarca el extremo de la red de la interfaz usuario a red. El DCE proporciona una conexión física con la red, envía tráfico y suministra una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE. Comparar con DTE.

**Descifrado:** La aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando por lo tanto los datos a su estado original, no cifrado.

**Dato:** Son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

**DTE:** Equipo de terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario-red que actúa como origen de datos, destino de datos o ambas. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y por lo general usa señales de temporización generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadores, traductores de protocolo y multiplexores.

**Directorio:** En D.O.S., una lista de nombres de archivo que contiene toda la información de los archivos almacenados. A partir de Windows 95 este término se reemplazó por CARPETA.

**Dirección:** Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico" (emáil address); "IP" y (direccion de Internet) y "dirección hardware".

**Dirección del Protocolo de Internet (dirección IP):** Dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red con Protocolo de control de transmisión/Protocolo Internet (TCP/IP). Número único que consta de 4 partes separadas por puntos. Una dirección IP se suele representar en una notación decimal con puntos que indica cada octeto (ocho bits o un byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 172.16.255.255.

Cada computadora conectada a Internet tiene un único número de IP. Si la máquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem).

**Disco Rígido:** Unidad de almacenamiento permanente de información. Éste es el que guarda la información cuando apagamos la computadora. Aquí se guardan la mayoría de los programas y el sistema operativo. Su capacidad de almacenamiento se mide en Megabytes (Mb) o Gigabytes (Gb), en donde 1024 Mb = 1Gb.

**Disquete:** Dispositivo que puede insertarse y extraerse en una unidad de disco.

**DNS:** (Domain Name System ó Sistema de Nombres de Dominio). El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de éstos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes son: .COM (comercial - empresas), .EDU (educación, centros docentes), .ORG (organización sin ánimo de lucro), .NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejército USA). La mayoría de los países tienen un dominio propio. Por ejemplo, AR (Argentina) .PY (Paraguay), .US (Estados Unidos de América), .ES (España), ..AU (Australia), etc.

**Dominio:** (Domain Name). Nombre único que identifica a un sitio de Internet. Los nombres de dominio tienen 2 o más secciones, separadas por puntos. La sección de la izquierda es la más específica, y la de la derecha, la más general. Una computadora particular puede tener más de un nombre de dominio, pero un nombre de dominio se refiere únicamente a una PC.

**Download ó descargar:** En Internet es el proceso de transferir información desde un servidor de información a la propia PC.

**Documentación:** Manual escrito que detalla el manejo de un sistema o pieza de hardware.

**Doble Clic:** Acción de presionar y soltar rápidamente el botón del mouse (ratón) dos veces, sin desplazarlo. Esta acción sirve para ejecutar una determinada aplicación, como por ejemplo: inicializarla.

**DSU:** Unidad de servicio de datos. Dispositivo que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión como, por ejemplo, TI y El.

**DVD:** (Digital Versatile Disc ó Disco Versátil Digital). Disco que sirve para almacenar más datos de contenido digital, como música o video, que un CD. Un DVD guarda un mínimo de 4.7 Gigabytes (el tamaño de una película de cine).

# E

**EI:** Estándar Europeo equivalente al americano TI. Los circuitos EI y TI. Los dos usan canales de 64 Kbps, pero el TI tiene 24 mientras que el EI tiene 32 canales.

**EIA/TIA-568:** Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

**Encapsulamiento:** El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

**Emulación de terminal:** Aplicación de red en la que un computador ejecuta software que la hace aparecer ante un host remoto como una terminal conectada directamente.

**Enrutamiento:** Proceso para encontrar una ruta hacia un host destino. El enrutamiento en redes de gran tamaño es muy complejo dada la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

**Ethernet:** Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3. Ver también 10BASE2, 10BASE5, 10BASE-F, 10BASE-T, 10Broad36 e IEEE 802.3.

**Elemento de Pantalla:** Partes que constituyen una ventana o cuadro de diálogo como por ejemplo: la barra de título, los botones de "Maximizar" y "Minimizar", los bordes de las ventanas y las barras de desplazamiento.

**Escritorio:** Fondo de la pantalla sobre la cual aparecen ventanas, iconos y cuadros de diálogo.

**Estación de trabajo:** Computador de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. Llamadas así para distinguirlas de los que se conocen como servidores.

**Expandir:** Mostrar los niveles de directorio ocultos del árbol de directorios. Con el administrador de archivos es posible expandir un solo nivel de directorio, una rama del árbol de directorio o todas las ramas a la vez.

**Explorador:** Llamado también explorador Web. Interfaz cliente que permite al usuario ver documentos HTML en el World Wide Web, en otra red o en su propio equipo; seguir los hipervínculos y transferir archivos. Un ejemplo es Microsoft Internet Explorer.

**Extensión:** Está compuesto por un punto y un sufijo de hasta tres caracteres situados al final de un nombre de archivo. La extensión suele indicar el tipo de archivo o directorio.

# F

**Fibra monomodo:** Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único. Ver también fibra multimodo.

**Fibra multimodo:** Fibra óptica que permite la propagación de múltiples frecuencias de luz.

**Firewall:** Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

**Fluctuación de fase:** Distorsión analógica de la línea de comunicación provocada por la variación de una señal de sus posiciones de temporización de referencia. La fluctuación de fase puede provocar la pérdida de datos, especialmente a altas velocidades.

**Flujo de datos:** Todos los datos que se transmiten a través de la línea de comunicaciones en una sola operación de lectura o escritura.

**Frecuencia:** Cantidad de ciclos, medidos en hercios, de una señal de corriente alterna por unidad de tiempo.

**FTP:** Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP, que se usa para transferir archivos entre nodos de la red. El FTP se define en la RFC 959.

**Full dúplex:** Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora.

# G

**Gateway:** En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función, y gateway se refiere a un dispositivo con fines especiales que ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra.

**Sateway fronterizo:** Router que se comunica con routers de otros sistemas autónomos.

**Giga:** Prefijo que indica un múltiplo de 1.000 millones, o sea 10<sup>9</sup>. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 1.073.741.824.



**Grupo de trabajo:** Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

# H

**Hardware:** Son todos los componentes físicos que componen una PC.

**Hercio:** Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

**Hexadecimal:** Base 16. Representación numérica que usa los dígitos 0 a 9, con su significado habitual, y las letras A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, luego  $16A_2=256$ , etc. ;-.-;

**Host:** Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

**HTML:** (HyperText Markup Language). Lenguaje utilizado para crear los documentos de hipertexto que se emplean en la WWW. Los documentos HTML son simples archivos de texto que contienen instrucciones (llamadas tags) entendibles por el Navegador (Browser).

**HTTP:** (HyperText Transport Protocol). Protocolo utilizado para transferir archivos de hipertexto a través de Internet. Requiere de un programa "cliente" de HTTP en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la WWW.

**Hub:** Dispositivo de hardware o software que contiene módulos de red y equipo de internetwork múltiples, independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen, las señales que se envían a través de ellos).

# I

**IEEE:** Instituto de ingenieros eléctricos y electrónicos. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN del IEEE son los estándares de LAN predominantes en el mundo actual

**IEEE 802.1:** Especificación del IEEE que describe un algoritmo que evita los loops de capa dos mediante la creación de un spanning tree. El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo de Digital y el algoritmo IEEE 802.1 no son exactamente los mismos, ni tampoco son compatibles.

**IEEE 802.12:** Estándar LAN del IEEE que especifica la capa física y la subcapa MAC de la capa de enlace de datos. El IEEE 802.12 usa el esquema de acceso a los medios de prioridad de demanda a 100 Mbps a través de una diversidad de medios físicos. Ver también IEEE 802.3-Any LAN.

**IEEE 802.2:** Protocolo LAN del IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 administra errores, entramado, control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se usa en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

**IEEE 802.3:** Protocolo LAN del IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 usa acceso CSMA/CD a diversas velocidades sobre diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican las implementaciones de Fast Ethernet. Las variantes físicas de la especificación IEEE 802.3 original incluyen 10BASE2, 10BASE5, 10BASE-F, 10BASE-T y 10Broad36. Las variantes físicas de Fast Ethernet incluyen 100BASE-T, 100BASE-T4 y 100BASE-X.

**Icono:** Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc.

**IDF:** Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

**Impresora:** Dispositivo de salida, cuya funcionalidad es transcribir/pasar un documento (imagen y/o texto) desde el ordenador (procesador de textos, bloc de notas, visor de imágenes, etc.) a un medio físico, generalmente papel, mediante el uso de cinta, cartuchos de tinta o también con tecnología láser.

**Impresora de Inyección a tinta:** Crean imágenes directamente sobre el papel al rociar tinta a través de una pequeñas boquillas, su calidad de impresión es bastante alta.

**Impresora Predeterminada:** Impresora que se utiliza si se elige el comando Imprimir, no habiendo especificado antes la impresora que se desea utilizar. Sólo puede haber una impresora predeterminada, que debe ser la que se utilice con mayor frecuencia.

**Información:** Es lo que se obtiene del procesamiento de datos, es el resultado final.

**Informática cliente-servidor:** Término que se usa para describir los sistemas de red informáticos distribuidos (de procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: cliente (front end) y servidor (back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos actuales.

**Internetwork:** Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red.

**IP:** Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de

direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad. Documentado en la RFC 791.

**IP access-group:** Comando que enlaza una lista de acceso existente con una interfaz de salida.

**IP host:** Comando que se usa para crear una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.

**IP multicast:** Técnica de enrutamiento que permite que el tráfico IP se propague desde un origen hacia un número de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, se envía un paquete a un grupo de multicast que se identifica mediante una sola dirección de grupo de destino IP.

**IPX:** Intercambio de paquetes de internetworking. Protocolo de capa de red (Capa 3) de NetWare que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

**Interfaz:** Una conexión e interacción entre hardware, software y usuario, es decir, como la plataforma o medio de comunicación entre usuario o programa.

**Internet:** Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

**Intranet:** Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno.

**ISO:** Organización Internacional de Normalización. Organización internacional que es responsable por una amplia gama de estándares, incluyendo aquellos relevantes para el networking. ISO desarrolló el modelo de referencia OSI, un modelo de referencia de networking sumamente popular.

## J

**Jumper:** Término que se usa para los cables de interconexión que se encuentran en el armario de cableado.

## K

**Kbps:** (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit esta formado por mil bits.

**Kilobyte:** Es el equivalente a 1024 bytes.



# L

**LAN:** Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido. Comparar con MAN y WAN.

**Latencia:** Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir también sucede en el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

**LED:** Diodo emisor de luz. Dispositivo semiconductor que emite luz producida por la conversión de energía eléctrica. Las lámparas de estado en los dispositivos de hardware generalmente son LED.

**Línea de acceso telefónico:** Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

**Línea de comunicación:** Enlace físico (como, por ejemplo, un cable o circuito de teléfono) que conecta uno o más dispositivos con uno o más dispositivos.

**Línea de mira:** Característica de determinados sistemas de transmisión como, por ejemplo, los sistemas láser, de microondas e infrarrojos, en los que no puede existir ninguna obstrucción en la ruta directa entre el transmisor y el receptor.

**Línea dedicada:** Línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir. Ver también línea arrendada.

**Lista de acceso:** Lista que mantienen los routers Cisco para controlar el acceso hacia o desde el router para diversos servicios (por ejemplo, para evitar que los paquetes que tienen una determinada dirección IP salgan de una interfaz específica del router).

**LSA:** Publicación de estado de enlace. Paquete de broadcast que usan los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de la ruta. Los routers receptores usan las LSA para mantener sus tablas de enrutamiento

**Login:** Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del password, el login no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

# M

**MAC:** Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

**MICIP:** Protocolo de capa de red que encapsula paquetes IP en DDS o transmisión a través de AppleTalk.

**Malla:** Topología de red en la que los dispositivos se organizan de una manera administrable, segmentada, con varias interconexiones, a menudo redundantes, ubicadas estratégicamente entre nodos de la red. Ver también malla completa y malla parcial.

**Malla completa:** Término que describe a una red en la que los dispositivos están organizados en una topología de malla, en la que cada nodo de la red tiene un circuito físico o un circuito virtual que lo conecta a todos los otros nodos de la red. Una malla completa brinda una gran cantidad de redundancia pero, dado que su implementación puede resultar excesivamente cara, generalmente se la reserva para los backbones de la red. Ver también malla y malla parcial.

**MAN:** Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

**MAP:** Protocolo de automatización de fabricación. Arquitectura de red creada por General Motors para satisfacer las necesidades específicas las instalaciones fabriles. El MAP especifica una LAN de transmisión de tokens similar a IEEE 802.4. Ver también IEEE 802.4.

**Mapa de cableado:** Característica suministrada por la mayoría de los analizadores de cable. Se usa para probar las instalaciones de cableado de par trenzado, y muestra cuáles hilos están conectados a cuáles pines, en conectores macho y hembra.

**Mapa de topología:** Herramienta para administrar un switch ATM LightStream 2020 que examina una red y muestra el estado de sus nodos y enlaces troncales. El mapa de topología es una aplicación basada en HP OpenView que se ejecuta en un NMS.

**Máscara de red:** Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

**Máscara wildcard:** Cantidad de 32 bits que se usan de forma conjunta con una

dirección IP para determinar cuáles son los bits de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

**MDF:** Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

**Megabyte (MB):** 1.048.576 bytes; 1.024 Kilobytes.

**Megahertz:** Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

**Memoria RAM:** Memoria de acceso aleatorio cuyo contenido permanecerá presente mientras el computador permanezca encendido.

**Memoria ROM:** Memoria de sólo lectura. Chip de memoria que sólo almacena permanentemente instrucciones y datos de los fabricantes.

**Microonda:** este enlace esta constituido por dos transceptores de radio provistos de antenas parabólicas que se apuntan directamente entre si. La radio puede transportar transmisiones punto a punto de muchos anchos de banda. Su alcance varia según el tamaño de la antena, el clima en la zona y la magnitud de la potencia emitida contemplando todos estos conjuntos la señal puede llegar hasta 80 Km.

**Módem:** (Modulator, Demodulator). Dispositivo que se conecta a la computadora y a la línea telefónica y que permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

**Mouse:** Permite convertir el movimiento de la mano en desplazamiento de un cursor sobre la pantalla.

**Multicast:** la multidifusión (multicast) permite que grupos de usuarios seleccionados reciban la misma transmisión de datos en una red los cuales están identificados por una única dirección de grupo de destino IP.

## N

**Navegador de Web:** Aplicación de cliente de hipertexto basada en GUI como, por ejemplo, Mosaic, que se usa para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a través de la WWW e Internet. Ver también hipertexto, Internet, Mosaic y WWW.

**NBP:** Protocolo de enlace de denominación. Protocolo AppleTalk de nivel de transporte que convierte un nombre dado en forma de una cadena de caracteres en una dirección de internetwork.

**NET:** Título de entidad de red. Direcciones de red, definidas por la arquitectura de red ISO.

**NetBIOS:** Sistema básico de entrada/salida de red. API que usan las aplicaciones de una LAN IBM para solicitar servicios de procesos de red de nivel inferior. Estos servicios pueden incluir establecimiento y terminación de sesión y transferencia de información.

**NetWare:** NOS distribuido de uso generalizado desarrollado por Novell. Suministra acceso remoto transparente a archivos, y muchos otros servicios de red distribuida.

**Networking:** Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

**NIC:** Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

**NOS:** Sistema operativo de red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos. Los ejemplos de NOS incluyen LAN Manager, NetWare, NFS y VINES.

**Número de host:** Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

**Número de red:** Parte de una dirección IP que especifica la red a la que pertenece el host.

**Número de saltos:** Métrica de enrutamiento que se usa para medir la distancia entre un origen y un destino. El RIP usa el número de saltos como su única métrica.

**NVRAM:** RAM no volátil. RAM que retiene su contenido cuando una unidad se apaga. En los productos Cisco, la NVRAM se usa para guardar la información de configuración.

**Nodo:** En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma.

**Nombre de usuario:** La secuencia de caracteres que lo identifica. Al conectarse a una computadora, generalmente necesita proporcionar su nombre y contraseña de usuario. Esta información se usa para verificar que la persona está autorizada para usar el Sistema.

## O

**Operador de red:** Persona que monitorea y controla una red de forma continua, ejecutando tareas como

**Oscilación:** Señal secundaria superpuesta a la onda de 60 Hz. Tiene una magnitud que

varía entre el 15% y el 100% del voltaje normal de la línea de alimentación. Ver sobrevoltaje, pico y baja de voltaje. :

**OSI:** Interconexión de sistemas abiertos. Programa internacional de normalización creado por la ISO y la UIT-T para desarrollar estándares de interconexión que faciliten la interoperabilidad de equipos de múltiples proveedores.

**OSINET:** Asociación internacional diseñada para promover OSI en las arquitecturas de los proveedores. ::

**OSPF:** Versión abierta del algoritmo "Primero la ruta libre más corta". Algoritmo de enrutamiento IGP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad Internet. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga. El OSPF deriva de una versión inicial del protocolo ISIS.

## P

**PAD:** Ensamblador/desensamblador de paquetes. Dispositivo que se usa para conectar dispositivos simples (como terminales de modo de carácter) a una red, los cuales no admiten toda la funcionalidad de un protocolo específico. Los PAD almacenan los datos en el búfer de los PAD y ensamblan y desensamblan los paquetes que se envían a dichos dispositivos finales.

**Panel de conexión:** Conjunto de ubicaciones de pin y puertos que se puede montar en un bastidor o una consola de pared en el armario de cableado. Los paneles de conexión actúan como conmutadores que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

**Paquete:** Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

**Paquete de choque:** Paquete que se envía al transmisor para informarle que hay congestión y que debe reducir su velocidad de envío.

**Par trenzado:** Medio de transmisión de relativa baja velocidad compuesto por dos cables aislados dispuestos en un patrón en espiral regular. Los cables pueden ser blindados o no blindados. El uso del par trenzado es común en aplicaciones de telefonía y es cada vez más común en las redes de datos. Ver también STP y UTP.

**Paradiafonía:** Energía de interferencia transferida de un circuito a otro.

**PBX:** Central telefónica privada. Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas



y públicas.

**PCI:** Información de control de protocolo. Información de control que se agrega a los datos del usuario para formar un paquete OSI.

**Pila de protocolo:** Conjunto de protocolos de comunicación relacionados que operan de forma conjunta y, como un grupo, cumplen con la comunicación en alguna o en las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo y, a menudo, un solo protocolo de la pila se dirige a una cantidad de capas a la vez. El TCP/IP es un protocolo de pila típico.

**Ping:** Abreviatura para Packet Internet Groper o Packet Inter-network Groper, una utilidad que se usa para determinar si una dirección IP en particular está disponible. Funciona enviando un paquete a la dirección especificada y esperando una respuesta. El PING se usa principalmente para diagnosticar las fallas de las conexiones de Internet.

**Plan de distribución:** Diagrama simple que indica dónde están ubicados los tendidos de cable y la cantidad de habitaciones hacia las que se dirigen.

**POP:** Punto de presencia. Punto de presencia es el punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y el servicio de distribución principal del edificio.

**Portadora:** Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos. Ver también modulación.

**POST:** Autocomprobación de encendido. Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando ese dispositivo se enciende.

**Protocolo de enrutamiento:** Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. Los ejemplos de protocolos de enrutamiento incluyen el IGRP, el OSPF y el RIP.

**Puerto:** Interfaz de un dispositivo de internetworking (como, por ejemplo, un router) En terminología ip, un proceso de capa superior que recibe información de las capas Inferiores. Un conector hembra de un panel de conexión el cual acepta el mismo tamaño de conector que el de un rj45. Los cables de conexión se usan en estos puertos para realizar interconexiones entre los computadores conectados al panel. Es esta interconexión conexión la que permite la operación de la lan.

**Página Web:** Documento de World Wide Web. Una página Web suele consistir en un archivo HTML, con sus archivos asociados de gráficos y secuencias de comandos, en un directorio determinado de un equipo concreto (y, por tanto, identificable mediante una dirección URL).

**Periféricos:** Cualquier dispositivo de hardware conectado a una computadora.

**Pixel:** (PIcture cELL). Es la parte más pequeña de una pantalla de video, constituido por uno o más puntos que se consideran como una unidad. Es por tanto, el bloque de construcción de imágenes.

**Protocolo:** Método por el que los equipos se comunican en Internet. El protocolo más común en el World Wide Web es HTTP. Otros protocolos de Internet incluyen FTP, Gopher y telnet. El protocolo forma parte de la dirección URL completa de un recurso.

**Proveedor:** Institución o empresa que provee acceso a uno o varios servicios de Internet.

## R

**RAM:** Memoria de acceso directo aleatorio. Memoria volátil que puede ser leída y escrita por un microprocesador.

**Red:** Conjunto de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

**Red de conexión única:** Red que tiene una sola conexión con un router

**Redireccionar:** Parte de los protocolos ICMP y ES-IS que permiten que un router le indique a un host que puede ser más efectivo usar otro router.

**Redistribución:** Permitir que la información de enrutamiento detectada a través de un protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento. A veces denominada redistribución de ruta.

**Redundancia:** En internetworking, la duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan ejecutar el trabajo de aquellos que han fallado. Ver también sistema redundante.

**Rendimiento:** Velocidad de la información que llega a, y posiblemente atraviesa, un punto particular de un sistema de red.

**Repetidor:** Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red.

**Retardo:** El tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. También, el tiempo que se requiere para mover un paquete desde el origen hacia el destino a través de una ruta específica.

**RF:** Radiofrecuencia. Término genérico que se usa para referirse a frecuencias que corresponden a transmisiones radioeléctricas. Las redes de televisión por cable y de banda ancha usan tecnología RF.

**Router:** Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

**RIP:** Protocolo de información de enrutamiento. IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet.

**RMON:** Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitoreo remoto de los dispositivos conectados a la red.

**ROM:** Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.

**Ruta estática:** Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

**Ruta por defecto:** Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

## S

**Segmento:** La sección de una red limitada por puentes, routers o switches. Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

**SMTP:** Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico

**Sondeo:** Método de acceso en el que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

**Switch:** Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI:

**Switch LAN:** Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches LAN envían tráfico basándose en las direcciones MAC. Esta variedad de switch LAN a veces se denomina switch de trama. Los switches LAN a menudo se clasifican de acuerdo con el método que usan para enviar tráfico: conmutación de paquetes por método de corte y conmutación de paquetes por almacenamiento y envío. Los switches multicapas son un subconjunto inteligente de los switches LAN.

**Servidor:** Computadora o programa que brinda un servicio específico al "cliente", que se ejecuta en otras computadoras. El término puede referirse tanto a un equipo de una red que envía archivos o ejecuta aplicaciones para otros equipos de la red; el software que se ejecuta en el equipo servidor y que efectúa la tarea de servir archivos y ejecutar aplicaciones; o bien, en la programación orientada a objetos, un fragmento de código que intercambia información con otro fragmento de código cuando se pide.

**SO:** (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.



**Software:** Todos los componentes no físicos de una PC (Programas).

**T**

**TI:** Servicio de portadora de WAN digital. TI transmite datos con formato DS-1 a 1.544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o B8ZS. Comparar con El. Ver también AMI, B8ZS y DS-1.

**Tabla de enrutamiento:** Tabla que se guarda en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas hacia destinos de red en particular y, en algunos casos, las métricas asociadas con esas rutas.

**TFTP:** Protocolo de Transferencia de Archivos Trivial. Versión simplificada del FTP que permite que los archivos se transfieran desde un computador a otra a través de una red.

**Terminal:** Dispositivo simple en el que los datos se pueden introducir o recuperar desde una red. Generalmente, las terminales tienen un monitor y un teclado pero no tienen ningún procesador ni unidad de disco local.

**Topología:** Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

**Topología de anillo:** Topología de red que consta de un conjunto de repetidores conectados entre sí mediante enlaces de transmisiones unidireccionales para formar un solo bucle cerrado. Cada estación de la red se conecta a la red en el repetidor. Aunque lógicamente están organizadas en anillo, las topologías de anillo a menudo están organizadas en una estrella de bucle cerrado.

**Topología de bus:** Arquitectura LAN lineal en la que las transmisiones de las estaciones de red se propagan a lo largo del medio y son recibidas por todas las otras estaciones.

**Topología en árbol:** Topología LAN similar a la topología bus, salvo que las redes en árbol pueden tener ramificaciones con múltiples nodos. Las transmisiones desde una estación atraviesan la longitud del medio y son recibidas por todas las otras estaciones.

**Topología en estrella:** Topología LAN en la que los puntos de terminación de una red se conectan a un switch central común mediante enlaces punto a punto. Una topología de anillo que está organizada como estrella implementa una estrella de loop cerrado unidireccional en lugar de enlaces punto a punto.

**Topología en estrella jerárquica:** Topología en estrella extendida en la que un hub central se conecta a través de cableado vertical con otros hubs que dependen del mismo.

**Transceiver:** Unidad de conexión al medio. Dispositivo que se usa en las redes Ethernet e IEEE 802.3 que suministra la interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que se puede incorporar a una estación o puede ser un dispositivo individual, ejecuta funciones de capa física, incluyendo la conversión de datos digitales desde la interfaz Ethernet, detección de colisiones e inyección de bits

en la red.

**Tunneling:** Arquitectura que está diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.

**Tarjeta de Interfaz de Red:** (NIC). Dispositivo a través del cual computadoras de una red transmiten y reciben datos.

**TCP/IP:** (Transmisor Control Protocol/Internet Protocol). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

**Telnet:** Protocolo que permite al usuario de Internet conectarse y escribir comandos en un equipo remoto vinculado a Internet como si el usuario estuviera utilizando un terminal de texto conectado directamente al equipo. Forma parte del conjunto de protocolos TCP/IP.

**Tiempo Real:** Método para procesar la información en cuanto se recibe.

## U

**Unicast:** En redes conmutadas ethernet, transferencia de archivos/paquetes entre dos entidades. Una difusión única puede iniciarla un servidor a una estación de trabajo, una estación a un servidor, una estación a una impresora o cualquier otra unidad única hacia otra entidad

**UPS:** (Uninterruptible Power Supply ó Suministro de Energía Ininterrumpida). Es un estabilizador electrónico que está preparado para suplir al computador cuando se presenten caídas de energía o cambios de voltaje.

**URL:** (Universal Resource Locator ó Localizador de Recursos Universal). Identifica de manera única la ubicación de un equipo, directorio o archivo en Internet. La dirección URL también indica el protocolo de Internet apropiado, como HTTP o FTP. Por ejemplo: <http://www.microsoft.com>.

**USB:** Tecnología que facilita la conexión de periféricos a la computadora. Esta reconoce automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo, ya que se conecta a la parte trasera de la PC a un enchufe especial (puerto USB). La tarjeta madre debe tener esta tecnología en su CHIPSET para poder conectar dispositivos de este tipo.

**UTP:** Cable de para trenzado no apantallado, lo que significa que no tiene envoltura alrededor del grupo de conductores. Estos cables se usan principalmente en redes de voz y datos

**Usuario:** Cualquier individuo que interactúa con el computador a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con el computador a nivel profesional. :

# V

**Vector:** Segmento de datos de un mensaje SNA. Un vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

**Virtualización:** Proceso que se usa para implementar una red basada en segmentos de red virtuales. Los dispositivos se conectan a segmentos virtuales independientemente de su ubicación física y de su conexión física con la red.

**VLAN:** LAN virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.

**VLSM:** Máscara de subred de longitud variable. Capacidad de especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

**VTP:** Protocolo de terminal virtual. Aplicación ISO para establecer una conexión de terminal virtual a través de una red.

**Virus:** Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan, se propagan a través de cualquier medio de almacenamiento, o a través de la LAN, o de la misma Internet.

# W

**WAN:** Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

**WorkGroup Director:** Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroup Director se ejecuta en estaciones de trabajo UNIX, ya sea como una aplicación independiente o integrada con otra plataforma de administración de red basada en SNMP, brindando un sistema de gestión poderoso y transparente para los productos de grupo de trabajo de Cisco.

**WWW:** World Wide Web. Gran red de servidores de Internet la cual suministra servicios de hipertexto y otros a terminales que ejecutan aplicaciones de clientes como, por ejemplo, un navegador de Web. Ver también navegador de Web.

# X

**X Windows:** Protocolo que interconecta estaciones de trabajo de interfaz gráfica de usuario con programas servidores de aplicaciones que utiliza TCP/IP.

# Z

**Zona de autoridad:** Asociada con DNS, la zona de autoridad es una sección del árbol del nombre de