ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ANALISTA DE SOPORTE DE MICROCOMPUTADORES

TEMA:
ADMINISTRACIÓN Y SEGURIDADES DE REDES
"MOLINOS DEL ECUADOR"

MANUAL DE USUARIO

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

AUTORES:

JUAN ANDRÉS VERA VERGARA
JOSÉ FERNANDO CÁRDENAS CÁRDENAS

DIRECTOR:
ANL. FABIÁN BARBOZA

AÑO:
2007

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ANALISTA DE SOPORTE DE MICROCOMPUTADORES

TEMA:
ADMINISTRACIÓN Y SEGURIDADES DE REDES
"MOLINOS DEL ECUADOR"

MANUAL DE USUARIO

AUTORES:

JUAN ANDRÉS VERA VERGARA
JOSÉ FERNANDO CÁRDENAS CÁRDENAS

DIRECTOR:
ANL. FABIÁN BARBOZA

AÑO:
2007

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

AGRADECIMIENTO

Quiero dejar mi más profundo agradecimiento a la Escuela de Diseño y Comunicación Visual de la Escuela Superior Politécnica del Litoral (ESPOL) por la formación recibida para tomar y ejercer la profesión de Analistas de Soporte de Microcomputadoras.

Agradezco de forma especial al personal docente, administrativo, al departamento de Redes de la Escuela de Diseño y Comunicación Visual y a todas aquellas personas que trabajan internamente que de una u otra manera nos ayudaron en lo que respecta a nuestra formación académica.

Agradecezco a la empresa Molinos del Ecuador S.A por haber brindado información, la misma que nos sirvió para culminar nuestra tesis, al Ing. David Montenegro por su ayuda y colaboración para el desarrollo y entrega de tesis.

De la misma manera al Anl. Fabián Barboza Director del Tópico de Graduación que impartió en nosotros las autogestiones en el desarrollo y cuestionamiento de los aspectos dentro del entorno del Tópico de Administraciones & Seguridades de Redes.

Agradezco a Dios sobre todas las cosas, a mis Padres que me han apoyado en lo económico, en lo moral y en las situaciones más difíciles de nuestras vidas.

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Fernando Cárdenas

AGRADECIMIENTO

Agradezco a la Escuela de Diseño y Comunicación Visual de la Escuela Superior Politécnica del Litoral (ESPOL) por la formación recibida para tomar y ejercer la profesión de Analistas de Soporte de Microcomputadoras.

Agradezco de forma especial al personal docente, administrativo, al departamento de Redes de la Escuela de Diseño y Comunicación Visual y a todas aquellas personas que trabajan internamente que de una u otra manera nos ayudaron en lo que respecta a nuestra formación académica.

Agradezco a Dios sobre todas las cosas, a mis Padres que me han apoyado en el transcurso de toda mi carrera.

Andrés Vera

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

DEDICATORIA

Dedico este logro a Dios por brindarme fuerzas y sabiduría para la culminación de este proyecto, y a mí abnegada Madre: María Cárdenas porque fue su anhelo que me forme como profesional y culmine mi carrera.

A los seres que en todas las etapas de mi vida, me han dado mucho de sí, que siempre en los malos momentos me dieron el apoyo necesario para continuar luchando perseverantemente, haciendo de mí un hombre de bien.

Con mucho amor a todas aquellas personas, a quien ofrezco todo mi esfuerzo y sacrificio orientado a alcanzar mi bienestar y felicidad.

! Gracias ¡Padres, Tíos y Familia



Fernando Cárdenas.

DEDICATORIA

Dedicado este trabajo a mis padres por haber sido siempre mis más dignos ejemplos a seguir, quienes con mucho esfuerzo y bondad me han dirigido por el buen camino de la vida al cumplir las metas propuestas.

También dedico este trabajo a mi hermano, que con su paciencia supieron apoyar mis necesidades elementales por alcanzar el máximo nivel en mi carrera.

Finalmente un agradecimiento a aquellas personas que bien merecidamente ocupan un lugar muy importante en mi vida como mis más nobles amistades, que tomando un espacio de su tiempo lo dedicaron a mí.

! Gracias a todos



Andrés Vera.

DECLARACIÓN EXPRESA

La responsabilidad por los hecho, ideas y doctrinas expuestas en este Proyecto de Graduación / Tesis de Grado nos corresponden exclusivamente. Y el patrimonio intelectual de la misma a EDCOM (Escuela de Diseño y Comunicación Visual) de la Escuela Superior Politécnica del Litoral.

(Reglamento de Exámenes y Títulos profesionales de la ESPOL)



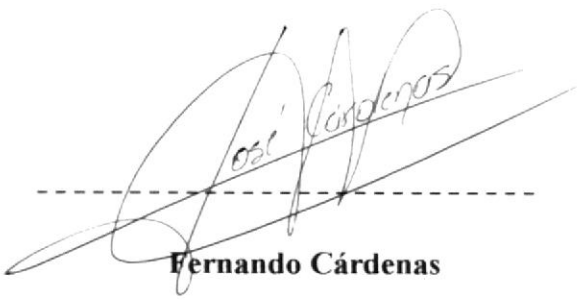


FIRMA DEL DIRECTOR DEL PROYECTO





Andrés Vera



Fernando Cárdenas

FIRMA DE LOS AUTORES DEL PROYECTO



INDICE DE CONTENIDO

CAPÍTULO 1 GENERALIDADES

1.1 INTRODUCCIÓN 1
1.2 OBJETIVO DE ESTE MANUAL 1
1.3 A QUIÉN VA DIRIGIDO ESTE MANUAL 1
1.4 QUÉ SE DEBE CONOCER 1
1.5 ACERCA DE ESTE MANUAL 1

CAPÍTULO 2 SITUACION ACTUAL

2. SITUACION ACTUAL 1
2.1. ANTECEDENTES 1
2.1.1. MISIÓN 1
2.1.2. VISIÓN 1
2.2. COMUNICACIÓN WAN MATRIZ Y SUCURSALES 2
2.3. INFRAESTRUCTURA LAN 3
2.3.1. ESTACIONES DE TRABAJO 3
2.3.1.1. MATRIZ 3
2.3.1.2. SUCURSALES QUITO, AMBATO, REYVENTAS, DIBSA 4
2.3.2. SOFTWARE INSTALADOS MATRIZ Y SUCURSALES 4
2.3.3. TOPOLOGÍA ESTRELLA DE MOLINOS 5
2.3.4. MEDIOS DE COMUNICACIÓN 5
2.3.4.1. ALÁMBRICOS 5
2.3.4.2. INALÁMBRICO 5
2.3.5. SERVIDORES 6
2.3.5.1. MATRIZ 6
2.3.5.2. SUCURSAL REYVENTAS 6
2.3.6. ESTRUCTURA DEL BACKBONE HORIZONTAL 7
2.3.6.1. MATRIZ 7
2.3.6.2. SUCURSAL QUITO 7
2.3.6.3. SUCURSAL AMBATO 8
2.3.6.4. SUCURSAL DIBSA 8
2.3.6.5. SUCURSAL REYVENTAS 9
2.3.7. ANÁLISIS DE PISO APLICATIVO 10
2.3.7.1. MATRIZ 10
2.3.7.2. SUCURSAL QUITO 10
2.3.7.3. SUCURSAL AMBATO 11
2.3.7.4. SUCURSAL DIBSA 11
2.3.7.5. SUCURSAL REYVENTAS 12
2.3.8. ANÁLISIS DE PISO LÓGICO 13
2.3.8.1. MATRIZ 13
2.3.8.2. SUCURSAL QUITO 13
2.3.8.3. SUCURSAL AMBATO 14
2.3.8.4. SUCURSAL DIBSA 14
2.3.8.5. SUCURSAL REYVENTAS 15
2.3.9. GRÁFICOS DEL MC 16
2.3.9.1. MC MATRIZ 16
2.3.9.2. MC QUITO 17
2.3.9.3. MC AMBATO 18
2.3.9.4. MC REYVENTAS 19

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.3.10. DISPOSITIVOS DE CONMUTACIÓN 20
2.3.10.1. MATRIZ, SUCURSALES QUITO Y AMBATO 20
2.4. INFRAESTRUCTURA WAN 21
2.4.1. DISPOSITIVOS DE ENRUTAMIENTO. 21
2.4.1.1. CARACTERÍSTICAS ROUTER CISCO 2500 (Quito) 21
2.4.1.2. CARACTERÍSTICAS ROUTER CISCO 2600 (MATRIZ) 21
2.4.1.3. CARACTERÍSTICAS ROUTER CISCO 1700 (Ambato) 21
2.4.2. ENLACE PRINCIPAL DE MOLINOS DEL ECUADOR 22
2.5. SEGURIDADES 23
2.5.1. CARACTERÍSTICAS DEL FIREWALL 23
2.6. RECEPCIÓN DE INTERNET 24
2.7. PROBLEMAS ENCONTRADOS 25

CAPÍTULO 3 SOLUCIÓN PROPUESTA

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 3
3.3.1.1.2. MATERIALES DE CABLEADO ESTRUCTURADO 3
3.3.1.2. FACTIBILIDAD OPERATIVA 4
3.3.1.3. FACTIBILIDAD ECONÓMICA 5
3.3.1.4. COSTO OPERATIVO 6
3.3.1.5. COSTO TOTAL DE PROPUESTA ALTERNATIVA "A" 6
3.3.1.6. VENTAJAS 7
3.3.1.7. BENEFICIOS 7
3.3.1.8. CONDICIONES COMERCIALES 7
3.3.1.8.1. FORMA DE PAGO 7
3.3.1.9. GARANTÍAS DE LA ALTERNATIVA "A" 7
3.3.1.10. DIAGRAMA DE GANT 8
3.3.2. ALTERNATIVA "B" 9
3.3.2.1. FACTIBILIDAD TÉCNICA 9
3.3.2.1.1. DISPOSITIVOS DE CONMUTACIÓN 9
3.3.2.1.2. MATERIALES DE CABLEADO ESTRUCTURADO 9
3.3.2.2. FACTIBILIDAD OPERATIVA 10
3.3.2.3. FACTIBILIDAD ECONÓMICA 11
3.3.2.4. COSTO OPERATIVA 12
3.3.2.5. COSTO TOTAL DE PROPUESTA ALTERNATIVA "B" 12
3.3.2.6. VENTAJAS 13
3.3.2.7. BENEFICIOS 13
3.3.2.8. CONDICIONES COMERCIALES 13
3.3.2.8.1. FORMA DE PAGO 13
3.3.2.9. GARANTÍAS DE LA ALTERNATIVA "B" 13
3.3.2.10. DIAGRAMA DE GANT 14

ESPOL
BIBLIOTECA
CAMPUS
PENAS

CAPÍTULO 4 IMPLEMENTACIÓN

4.1 ANÁLISIS DE PISO APLICATIVO 1
4.1.1 MATRIZ 1
4.1.2 BODEGA 3
4.1.3 SUCURSAL DIBSA 4
4.1.4 SUCURSAL REYVENTAS 5
4.2 ANÁLISIS DE PISO LÓGICO 6
4.2.1 MATRIZ 6
4.2.2 BODEGA 8
4.2.3 SUCURSAL DIBSA 9
4.2.4 SUCURSAL REYVENTAS 10
4.3 ESTRUCTURA DE MOLINOS 11
4.4 GRÁFICOS DEL MC 12
4.4.1 MC PRINCIPAL DE MOLINO 12
4.4.2 MC DE REYVENTAS 13
4.4.3 IC DE DIBSA 14
4.5 CÁLCULO DEL BACKBONE 15

CAPÍTULO 5 NORMATIVAS DE CERTIFICACIONES

NORMATIVAS DE CERTIFICACIONES 1
NORMATIVA 1 1
NORMATIVA 2 1
NORMATIVA 3 1
NORMATIVA 4 2
NORMATIVA 6 2
NORMATIVA 7 3
NORMATIVA 8 3
NORMATIVA 9 3
NORMATIVA 10 3
NORMATIVA 11 4
NORMATIVA 12 4
NORMATIVA 13 4
NORMATIVA 14 4
NORMATIVA 15 4
NORMATIVA 16 5
NORMATIVA 17 5
NORMATIVA 18 5
NORMATIVA 19 6
NORMATIVA 20 6
NORMATIVA 21 6
NORMATIVA 22 6
NORMATIVA 23 7
NORMATIVA 24 7
NORMATIVA 25 7
NORMATIVA 26 8
NORMATIVA 27 8
NORMATIVA 28 8
NORMATIVA 29 9
NORMATIVA 30 9

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

NORMATIVA 31 9
NORMATIVA 32 10
NORMATIVA 33 10
NORMATIVA 34 10
NORMATIVA 35 10
NORMATIVA 36 11
NORMATIVA 37 11
NORMATIVA 38 11
NORMATIVA 39 11
NORMATIVA 40 12
NORMATIVA 41 12
NORMATIVA 42 12
NORMATIVA 43 12
NORMATIVA 44 12
NORMATIVA 45 13
NORMATIVA 46 13
NORMATIVA 47 13
NORMATIVA 48 14
NORMATIVA 49 14
NORMATIVA 50 14
NORMATIVA 51 14
NORMATIVA 52 14
NORMATIVA 53 15
NORMATIVA 54..... 15
NORMATIVA 55 15
NORMATIVA 56 15
RECOMENDACIÓN DE CABLEADO ESTRUCTURADO 16
RECOMENDACIÓN 1 16
RECOMENDACIÓN 2 16
RECOMENDACIÓN 3 16
RECOMENDACIÓN 4 17
RECOMENDACIÓN 5 17
RECOMENDACIÓN 6 17
RECOMENDACIÓN 7 17
RECOMENDACIÓN 8 18
RECOMENDACIÓN 9 18
RECOMENDACIÓN 10 18
RECOMENDACIÓN 11 19
RECOMENDACIÓN 12 19
RECOMENDACIÓN 13 19

ESPOL
BIBLIOTECA
CAMPUS
PRENDAS

ESPOL
BIBLIOTECA
CAMPUS
PENAS

CAPÍTULO 6 LINUX

6.1 HISTORIA DE LINUX 1
6.1.2 ETIMOLOGÍA 1
6.1.3 ARQUITECTURA 2
6.1.4 LENGUAJES DE PROGRAMACIÓN 2
6.2 LINUX FEDORA CORE 3 3
6.2.1 CARACTERÍSTICAS DEL SISTEMA 3
6.2.2 REQUERIMIENTOS DE INSTALACIÓN 4
6.3 CONFIGURACIÓN DEL BIOS 5
6.4. INSTALACIÓN DE FEDORA CORE 3 8
6.4.1 CONFIGURACIÓN POST INSTALACIÓN DE LINUX FEDORA CORE 3 28
6.4.2 INICIO DE LINUX 32
6.4.2.1 MODO GRÁFICO 32
6.4.2.2 MODO TEXTO 34
6.5 COMANDOS BÁSICOS DE LINUX FEDORA CORE 3 35
6.6 SISTEMA DE ACHIVO DE LINUX 37
6.7 CONFIGURACIÓN DE LA TARJETA DE RED 38
6.7.1 CONFIGURACIÓN MODO TEXTO 38
6.7.2. CONFIGURACIÓN MODO GRÁFICO 39
6.8 SERVIDOR SAMBA 43
6.8.1. DISTRIBUCIÓN SAMBA 44
6.8.2. FUNCIONAMIENTO 45
6.8.3 VENTAJAS 45
6.8.4 DESVENTAJAS 45
6.8.5 REQUERIMIENTOS 46
6.8.6 CONFIGURACIÓN DEL SERVIDOR SAMBA 46
6.8.7 ACTIVACIÓN DEL SERVICIOS AMBA AUTOMATICAMENTE 54
6.8.8 CONFIGURACIÓN EN CLIENTE WINDOWS – SAMBA 56
6.9 SERVIDOR DNS 62
6.9.1 QUÉ ES UNA DIRECCIÓN IP 62
6.9.2 ESTRUCTURA 63
6.9.3 CARACTERÍSTICAS 63
6.9.4 FUNCIONAMIENTO 63
6.9.5 COMPONENTES 63
6.9.6 USOS DEL DNS 64
6.9.7 ZONAS 64
6.9.7.1 ZONAS ESTÁNDARES 64
6.9.7.1.1 ZONAS PRIMARIAS 64
6.9.7.1.2. ZONAS SECUNDARIAS 64
6.9.8. REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR DNS 64
6.9.9 CONFIGURACIÓN DEL SERVIDOR DNS 65
6.9.10. CONFIGURACIÓN EN CLIENTE WINDOWS –DNS 72
6.10 SERVIDOR WEB SERVER 75
6.10.1 REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR WEB 77
6.10.2 CONFIGURACIÓN DEL SERVIDOR WEB SERVER 77
6.10.3 CONFIRACIÓN EN CLIENTE WINDOWS – WEB SERVER 83
6.11 SERVIDOR SENDMAIL 86
6.11.1 CARACTERÍSTICAS PRINCIPALES 87
6.11.2 REQUERIMIENTOS 87

6.11.3 CONFIGURACIÓN DE SENDMAIL **88**
6.11.4 CONFIGURACIÓN EN CLIENTE WINDOWS - MAIL **95**
6.12 SERVIDOR PROXY **103**
6.12.1 VENTAJAS **104**
6.12.2 DESVENTAJAS **104**
6.12.3 FUNCIONAMIENTO **105**
6.12.4 REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR DE INTERNET **105**
6.12.5 CONFIGURACIÓN DE PROXY SERVER **106**
6.12.5.1 CONFIGURACIÓN EN CLIENTE WINDOWS - PROXY 112
6.12.6 RESTRICCIONES DE ACCESO A PÁGINAS ESPECÍFICAS. **115**
6.12.6.1 CONFIGURACIÓN EN CLIENTE WINDOWS RESTRICCIONES DE PÁGINAS ESPECÍFICAS 117
6.12.7 RESTRICCIONES A USUARIOS EL ACCESO A INTERNET **118**
6.12.7.1 CONFIGURACIÓN EN CLIENTE WINDOWS RESTRICCIONES A USUARIOS EL ACCESO A INTERNET 121
6.12.8 RESTRICCIONES POR HORARIO **122**
6.12.8.1 CONFIGURACIÓN EN CLIENTE WINDOWS - HORARIO 124
6.12.9 AUTENTICACIÓN POR USUARIOS **125**
6.12.9.1 CONFIGURACIÓN EN CLIENTE WINDOWS AUTENTICACIÓN POR USUARIOS 128
6.13 SERVIDOR DE FIREWALL **130**
6.13.1 TIPOS DE CORTAFUEGOS **131**
6.13.1.1 CORTAFUEGOS DE CAPA DE APLICACIÓN 131
6.13.1.2 CORTAFUEGOS PERSONALES 131
6.13.2 DIRECCIÓN DE ORIGEN **131**
6.13.3 DIRECCIÓN DE DESTINO **132**
6.13.4 PROTOCOLO **132**
6.13.5 INTERFAZ DE ENTRADA **132**
6.13.6 INTERFAZ DE SALIDA **132**
6.13.7 PUERTO ORIGEN **132**
6.13.8 PUERTO DESTINO **132**
6.13.9 DEFINICIÓN DE REGLAS **133**
6.13.10 IP TABLES **134**
6.13.11 REQUERIMIENTOS PARA CONFIGURAR FIREWALL **134**
6.13.12 CONFIGURACIÓN DE FIREWALL **135**
6.13.12.1 BLOQUEAR PING 135
6.13.12.2 HABILITAR TELNET 135
6.13.12.3 BLOQUEO DE TELNET 137
6.13.12.4 BLOQUEAR FTP 137
6.13.13 CONFIGURACIÓN EN CLIENTE WINDOWS - FIREWALL **138**
6.14 SERVIDOR DHCP **141**
6.14.1 CARACTERÍSTICAS **141**
6.14.2 ASIGNACIÓN DE DIRECCIONES IP **142**
6.14.3 ANATOMÍA DEL PROTOCOLO **142**
6.14.4 DHCP DISCOVER **143**
6.14.5 DHCP OFFER **143**
6.14.6 DHCP REQUEST **143**
6.14.7 DHCP ACKNOWLEDGE **143**
6.14.8 DHCP INFORM **143**

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

6.14.9 DHCP RELEASE....143
6.14.10 REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR DHCP....144
6.14.11 CONFIGURACIÓN DE DHCP....144
6.14.12 CONFIGURACION EN CLIENTE WINDOWS - DHCP....148

CAPÍTULO 7 ROUTER

7.1 INTRODUCCIÓN DE ROUTER. 1
7.1.1 VENTAJAS DE LOS ROUTERS.... 2
7.1.2 DESVENTAJAS DE LOS ROUTERS. 3
7.2 ESTRUCTURA DEL ROUTER. 3
7.3 LOS COMPONENTES BÁSICOS DE LA ARQUITECTURA INTERNA DE UN ROUTER. 4
7.4 CONEXIONES EXTERNAS DEL ROUTER. 6
7.5 CONEXIONES DEL PUERTO DE ADMINISTRACIÓN. 6
7.6 MEDIOS DE COMUNICACIÓN A USAR. 7
7.6.1 CABLE DTE. 7
7.6.2 CABLE DCE. 8
7.6.3 CABLE UTP (CAT 5E). 8
7.6.4 CONECTOR RJ45.... 9
7.6.5 PUERTO SERIAL (CONECTOR COM). 9
7.7 ENRUTAMIENTO. 10
7.7.1 ENRUTAMIENTO ESTÁTICO. 10
7.7.2 ENRUTAMIENTO DINÁMICO. 10
7.7.2.1 PROTOCOLOS DE ENRUTAMIENTO. 10
7.8 TIPOS DE PROTOCOLO. 11
7.8.1 PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP)..... 11
7.8.1.1 VERSIONES RIP.... 11
7.8.1.2 FUNCIONAMIENTO RIP. 12
7.8.1.3 VENTAJAS Y DESVENTAJAS. 13
7.8.1.4 MENSAJES RIP.... 13
7.8.1.4.1 TIPOS DE MENSAJES RIP.... 13
7.8.1.4.2 FORMATO DE LOS MENSAJES RIP.... 13
7.8.2 PROTOCOLO DE INTERIOR DE GATEWAY (IGRP). 14
7.8.3 EIGRP. 14
7.8.3.1 TABLA DE VECINOS. 15
7.8.3.2 TABLA DE TOPOLOGÍA. 15
7.8.3.3 TABLA DE ENCAMINAMIENTO.... 15
7.8.3.4 PROTOCOLOS QUE UTILIZA EIGRP. 16
7.8.4 OSPF.... 18
7.8.4.1 TIPOS DE ÁREA.... 19
7.8.4.1.1 ÁREA STUB.... 19
7.8.4.1.2 ÁREA NOT-SO-STUBBY. 19
7.8.4.1.3 ESTADOS DE OSPF. 19
7.8.4.1.4 ESTADO DESACTIVADO (DOWN STATE). 20
7.8.4.1.5 ESTADO DE INICIALIZACIÓN (INIT STATE).... 20
7.8.4.1.6 ESTADO DE DOS-VÍAS (TWO-WAY). 20
7.8.4.1.7 ESTADO EXSTART. 20
7.9 LISTAS DE CONTROL DE ACCESO (ACL'S). 21
7.9.1 FUNCIONAMIENTO DE LAS ACL.... 22
7.9.2 CREACIÓN DE LAS ACL.... 22
7.10 SWITCH. 26

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

7.10.1 INTERCONEXIÓN DE CONMUTADORES Y PUENTES. **28**
7.10.2 INTRODUCCIÓN AL FUNCIONAMIENTO DE LOS CONMUTADORES. **28**
7.10.3 BUCLES DE RED E INUNDACIONES DE TRÁFICO **28**
7.10.4 CONMUTADORES DE NIVEL 3. ..... **29**
7.10.5 DIFERENTES MODELOS DE SWITCH. **29**
7.10.6 ENCAPSULAMIENTO. **30**
7.10.7 SEGMENTACIÓN. **31**
7.10.8 COLISIÓN. **32**
7.11 VLAN. **34**
7.11.1 INTRODUCCIÓN A VLAN. **34**
7.11.2 TIPOS DE VLAN. **35**
7.11.2.1 VLAN DE PUERTO CENTRAL 35
7.11.2.2 VLAN ESTÁTICAS 35
7.11.2.3 VLAN POR PUERTO 35
7.11.2.3.1 VENTAJAS 35
7.11.2.3.2 DESVENTAJAS 36
7.11.2.4 POR DIRECCIÓN MAC 36
7.11.2.4.1 VENTAJAS 36
7.11.2.4.2 DESVENTAJAS 36
7.11.2.5 POR PROTOCOLO 37
7.11.2.5.1 VENTAJAS 37
7.11.2.5.2 DESVENTAJAS 37
7.11.2.6 POR DIRECCIONES IP 37
7.11.2.6.1 VENTAJAS 37
7.11.2.6.2 DESVENTAJAS 37
7.11.2.7 POR NOMBRE DE USUARIO 38
7.11.2.7.1 VENTAJAS 38
7.11.2.7.2 DESVENTAJAS 38
7.11.2.8 VLAN DINÁMICAS (DVLAN). **38**
7.12 TECNOLOGÍA. **39**
7.13 PRESTACIONES DE LAS VLAN. **41**
7.14 APLICACIONES. **42**
7.15 CASO DE ESTUDIO DE LA EMPRESA MOLINOS DEL ECUADOR. **43**
7.16 CONFIGURACIÓN EN EL HYPERTERMINAL **44**
7.17 COMANDOS BÁSICOS DE ROUTER. **47**
7.18 CONFIGURACIÓN DE ROUTER. **49**
7.18.1 ROUTER ISP. **49**
7.18.1.1 ASIGNACIÓN DE NOMBRE AL ROUTER ISP 49
7.18.1.2 ASIGNACIÓN DE CONTRASEÑA AL ROUTER ISP 50
7.18.1.3 CONFIGURACIÓN DE INTERFAZ SERIAL 0 51
7.18.1.4 CONFIGURACIÓN DEL PROTOCOLO RIP 52
7.18.1.5 SHOW PROTOCOLS ISP 53
7.18.1.6 SHOW RUN DEL ISP 54
7.18.1.7 SHOW IP ROUTE ISP 56
7.18.1.8 SHOW INTERFACE 58
7.18.2 MATRIZ (GUAYAQUIL). **60**
7.18.2.1 ASIGNACIÓN DE NOMBRE AL ROUTER MATRIZ 60
7.18.2.2 ASIGNACIÓN DE CONTRASEÑA AL ROUTER MATRIZ 61
7.18.2.3 CONFIGURACIÓN DE INTERFAZ SERIAL 1/0 62
7.18.2.4 CONFIGURACIÓN DE INTERFAZ SERIAL 1/1 63
7.18.2.5 CONFIGURACIÓN DE INTERFAZ SERIAL 1/2 64
7.18.2.6 CONFIGURACIÓN DE INTERFAZ FASTHERNET 0/0 65

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

7.18.2.7 CONFIGURACIÓN DE SUB-INTERFAZ FASTETHERNET 0/0. 66
7.18.2.7.1 ENRUTAMIENTO VLAN 10. 66
7.18.2.7.2 ENRUTAMIENTO VLAN 20. 67
7.18.2.7.3 ENRUTAMIENTO VLAN 30. 67
7.18.2.7.4 ENRUTAMIENTO VLAN 40. 68
7.18.2.8 CONFIGURACIÓN DEL PROTOCOLO OSPF 69
7.18.2.9 SHOW PROTOCOLS MATRIZ 70
7.18.2.10 SHOW IP ROUTE MATRIZ 71
7.18.2.11 SHOW RUN MATRIZ 73
7.18.2.12 SHOW INTERFACE MATRIZ 76
7.18.3 CONFIGURACIÓN DEL ROUTER SUCURSAL (AMBATO)..... 79
7.18.3.1 ASIGNAR EL NOMBRE AL ROUTER SUCURSAL 79
7.18.3.2 CREACIÓN DE CONTRASEÑAS 80
7.18.3.3 CONFIGURACIÓN DE INTERFAZ SERIAL 0 81
7.18.3.4 CONFIGURACIÓN DE INTERFAZ FASTETHERNET 0/0 82
7.18.3.5 CONFIGURACIÓN DE SUB-INTERFAZ FASTETHERNET 0/0 83
7.18.3.5.1 ENRUTAMIENTO DE LA VLAN 50. 83
7.18.3.5.2 ENRUTAMIENTO VLAN 60. 84
7.18.3.5.3 ENRUTAMIENTO VLAN 70. 84
7.18.3.6 CONFIGURACIÓN DEL PROTOCOLO OSPF 85
7.18.3.7 SHOW PROTOCOLS DE LA SUCURSAL AMBATO. 86
7.18.3.8 SHOW RUN DE LA SUCURSAL AMBATO. 87
7.18.3.9 SHOW IP ROUTE DE LA SUCURSAL AMBATO. 90
7.18.3.10 SHOW INTERFACE SUCURSAL AMBATO. 92
7.18.4 CONFIGURACIÓN DEL ROUTER SUCURSAL (QUITO). 95
7.18.4.1 ASIGNAR EL NOMBRE AL ROUTER SUCURSAL. 95
7.18.4.2 CREACIÓN DE CONTRASEÑAS 96
7.18.4.3 CONFIGURACIÓN DE INTERFAZ SERIAL 0 97
7.18.4.4 CONFIGURACIÓN DE FASTETHERNET 0/0. 98
7.18.4.5 CONFIGURACIÓN DE SUB-FASTETHERNET 0/0 99
7.18.4.5.1 ENRUTAMIENTO VLAN 80. 99
7.18.4.5.2 ENRUTAMIENTO VLAN 90. 100
7.18.4.5.3 ENRUTAMIENTO VLAN 100. 100
7.18.4.6 CONFIGURACIÓN DEL PROTOCOLO OSPF 101
7.18.4.7 SHOW PROTOCOLS DE LA SUCURSAL QUITO. 102
7.18.5. SHOW RUN DE LA SUCURSAL QUITO. 103
7.18.5.1 SHOW IP ROUTE DE LA SUCURSAL QUITO 105
7.18.5.2 SHOW INTERFACE SUCURSAL QUITO 107
7.19 CONFIGURACIÓN DE SWITCH MATRIZ.....110
7.19.1 CONFIGURACIÓN DE SWITCH MATRIZ. 110
7.19.1.1 ASIGNACIÓN DE NOMBRE AL SWITCH. 110
7.19.1.2 CREACIÓN DE VLAN'S. 110
7.19.1.3 ASIGNACIÓN DE PUERTO A LA VLAN 112
7.19.1.4 SHOW VLAN MATRIZ 114
7.19.1.5 SHOW RUN VLAN MATRIZ. 115
7.19.1.6 ASIGNACIÓN DE IP A LAS PC DE MATRIZ 117
7.19.2 CONFIGURACIÓN DEL SWITCH SUCURSAL AMBATO. 118
7.19.2.1 ASIGNACIÓN DE NOMBRES EN EL SWITCH AMBATO 118
7.19.2.2 CREACIÓN DE VLAN'S EN EL SWITCH AMBATO 119
7.19.2.3 ASIGNACIÓN DE VLAN'S A LOS PUERTOS. 120
7.19.2.4 SHOW VLAN AMBATO. 122
7.19.2.5 SHOW RUN AMBATO. 123
7.19.2.6 ASIGNACIÓN DE IP A LAS PC DE AMBATO 125
7.19.3 CONFIGURACIÓN DEL SWITCH EN LA SUCURSAL QUITO. 126

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

7.19.3.1 ASIGNACIÓN DE NOMBRES EN EL SWITCH AMBATO 126
7.19.3.2 CREACIÓN DE VLAN`S EN EL SWITCH QUITO. 127
7.19.3.3 ASIGNACIÓN DE VLAN`S A LOS PUERTOS 128
7.19.3.4 SHOW VLAN QUITO. 130
7.19.3.5 SHOW RUN QUITO 130
7.20 PRUEBAS DE COMUNICACIONES ENTRE ROUTER.....133
7.20.1 MATRIZ.....133
7.20.1.1 COMUNICACIÓN MATRIZ-AMBATO. 133
7.20.1.2 COMUNICACIÓN MATRIZ-QUITO 133
7.20.1.3 COMUNICACIÓN R:R:H:H-COBRANZAS 133
7.20.1.4 COMUNICACIÓN VENTAS–SISTEMAS. 134
7.20.1.5 COMUNICACIÓN COMPRAS–REDES. 134
7.20.2 AMBATO 135
7.20.2.1 COMUNICACIÓN AMBATO-MATRIZ 135
7.20.2.2 COMUNICACIÓN AMBATO-QUITO. 135
7.20.2.3 COMUNICACIÓN FINANZAS-SISTEMAS. 135
7.20.2.4 COMUNICACIÓN CONTABILIDAD-COBRANZAS. 136
7.20.3 QUITO.....136
7.20.3.1 COMUNICACIÓN QUITO-MATRIZ. 136
7.20.3.2 COMUNICACIÓN QUITO-AMBATO. 136
7.20.3.3 COMUNICACIÓN PRODUCCIÓN-REDES 137
7.20.3.4 COMUNICACIÓN REDES-SISTEMAS. 137
7.20.3.5 COMUNICACIÓN MARKETING-COBRANZAS. 137
7.21 ACL (EXTENDIDA).....138
7.21.1 BLOQUEO DE PING. 138
7.21.1.1 CONFIGURACIÓN DE IP ACCESS-GROUP. 138
7.21.1.2 ASIGNAR LAS ACL. 139
7.21.1.3 PRUEBA DE CONEXION SUCURSAL QUITO CON SERVIDOR. 140
7.21.1.4 PRUEBA DE CONEXION SUCURSAL AMBATO CON SERVIDOR. 140
7.21.1.5 SHOW ACCESS-LISTS 141
7.22. BLOQUEO DE TELNET. 142
7.22.1 CONFIGURACIÓN DE IP ACCESS-GROUP. 142
7.22.2 ASIGNAR LAS ACL. 143
7.22.3 SHOW ACCCESS-LIST.....144
7.22.4 PRUEBA DE TELNET SUCURSAL QUITO CON SERVIDOR.....145
7.22.5 PRUEBA DE TELNET SUCURSAL AMBATO CON SERVIDOR. 145



INDICE DE FIGURAS

CAPÍTULO 2 SITUACIÓN ACTUAL

FIGURA 2-1: COMUNICACIÓN WAN MATRIZ Y SUCURSALES 2
FIGURA 2-2: TOPOLOGÍA 5
FIGURA 2-3: SERVIDOR MATRIZ 6
FIGURA 2-4: ESTRUCTURA DEL BACKBONE MATRIZ 7
FIGURA 2-5: ESTRUCTURA DEL BACKBONE SUCURSAL QUITO 7
FIGURA 2-6: ESTRUCTURA DEL BACKBONE SUCURSAL AMBATO 8
FIGURA 2-7: ESTRUCTURA SUCURSAL DIBSA 8
FIGURA 2-8: ESTRUCTURA DEL BACKBONE SUCURSAL REYVENTAS 9
FIGURA 2-9: ANÁLISIS DE PISO APLICATIVO MATRIZ 10
FIGURA 2-10: ANÁLISIS DE PISO APLICATIVO SUCURSAL QUITO 10
FIGURA 2-11: ANÁLISIS DE PISO APLICATIVO SUCURSAL AMBATO 11
FIGURA 2-12: ANÁLISIS DE PISO APLICATIVO SUCURSAL DIBSA 11
FIGURA 2-13: ANÁLISIS DE PISO APLICATIVO DE SUCURSAL REYVENTAS 12
FIGURA 2-14: ANÁLISIS DE PISO LÓGICO MATRIZ 13
FIGURA 2-15: ANÁLISIS DE PISO LÓGICO SUCURSAL QUITO 13
FIGURA 2-16: ANÁLISIS DE PISO LÓGICO SUCURSAL AMBATO 14
FIGURA 2-17: ANÁLISIS DE PISO LÓGICO DE SUCURSAL DIBSA 14
FIGURA 2-18: ANÁLISIS DE PISO LÓGICO DE SUCURSAL REYVENTAS 15
FIGURA 2-19: MC PRINCIPAL MATRIZ 16
FIGURA 2-20: MC QUITO 17
FIGURA 2-21: MC AMBATO 18
FIGURA 2-22: MC REYVENTAS 19
FIGURA 2-23: ROUTER CISCO 2500 21
FIGURA 2-24: ROUTER CISCO 2600 21
FIGURA 2-25: ROUTER CISCO 1700 21
FIGURA 2-26: ENLACE PRINCIPAL DE MOLINOS 22
FIGURA 2-27: SEGURIDADES 23
FIGURA 2-28: RECEPCIÓN DE INTERNET 24

CAPÍTULO 4 IMPLEMENTACIÓN

FIGURA 4-1: ANÁLISIS DE PISO APLICATIVO MATRIZ 1
FIGURA 4-2: ANÁLISIS DE PISO APLICATIVO MATRIZ 2
FIGURA 4-3: ANÁLISIS DE PISO APLICATIVO BODEGA 3
FIGURA 4-4: ANÁLISIS DE PISO APLICATIVO SUCURSAL DIBSA 4
FIGURA 4-5: ANÁLISIS DE PISO APLICATIVO SUCURSAL REYVENTAS 5
FIGURA 4-6: ANÁLISIS DE PISO LÓGICO MATRIZ 6
FIGURA 4-7: ANÁLISIS DE PISO APLICATIVO MATRIZ 7
FIGURA 4-8: ANÁLISIS DE PISO LÓGICO BODEGA 8
FIGURA 4-9: ANÁLISIS DE PISO LÓGICO SUCURSAL DIBSA 9
FIGURA 4-10: ANÁLISIS DE PISO LÓGICO SUCURSAL REYVENTAS 10
FIGURA 4-11: GRÁFICO DE MOLINOS 11
FIGURA 4-12: MC MATRIZ 12
FIGURA 4-13: MC REYVENTAS 13
FIGURA 4-14: IC DIBSA 14

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 5 NORMATIVAS

FIGURA 5- 1 NORMATIVA 1 1
FIGURA 5- 2 NORMATIVA 2 1
FIGURA 5- 3 NORMATIVA 3 1
FIGURA 5- 4 NORMATIVA 4 2
FIGURA 5- 5 NORMATIVA 5 2
FIGURA 5- 6 NORMATIVA 6 2
FIGURA 5- 7 NORMATIVA 7 3
FIGURA 5- 8 NORMATIVA 8 3
FIGURA 5- 9 NORMATIVA 9 3
FIGURA 5- 10 NORMATIVA 10 3
FIGURA 5- 11 NORMATIVA 11 4
FIGURA 5- 12 NORMATIVA 12 4
FIGURA 5- 13 NORMATIVA 13 4
FIGURA 5- 14 NORMATIVA 14 4
FIGURA 5- 15 NORMATIVA 15 4
FIGURA 5- 16 NORMATIVA 16 5
FIGURA 5- 17 NORMATIVA 17 5
FIGURA 5- 18 NORMATIVA 18 5
FIGURA 5- 19 NORMATIVA 19 6
FIGURA 5- 20 NORMATIVA 20 6
FIGURA 5- 21 NORMATIVA 21 6
FIGURA 5- 22 NORMATIVA 22 6
FIGURA 5- 23 NORMATIVA 23 7
FIGURA 5- 24 NORMATIVA 24 7
FIGURA 5- 25 NORMATIVA 25 7
FIGURA 5- 26 NORMATIVA 26 8
FIGURA 5- 27 NORMATIVA 27 8
FIGURA 5- 28 NORMATIVA 28 8
FIGURA 5- 29 NORMATIVA 29 9
FIGURA 5- 30 NORMATIVA 30 9
FIGURA 5- 31 NORMATIVA 31 9
FIGURA 5- 32 NORMATIVA 32 10
FIGURA 5- 33 NORMATIVA 33 10
FIGURA 5- 34 NORMATIVA 34 10
FIGURA 5- 35 NORMATIVA 35 10
FIGURA 5- 36 NORMATIVA 36 11
FIGURA 5- 37 NORMATIVA 37 11
FIGURA 5- 38 NORMATIVA 38 11
FIGURA 5- 39 NORMATIVA 39 11
FIGURA 5- 40 NORMATIVA 40 12
FIGURA 5- 41 NORMATIVA 41 12
FIGURA 5- 42 NORMATIVA 42 12
FIGURA 5- 43 NORMATIVA 43 12
FIGURA 5- 44 NORMATIVA 44 12
FIGURA 5- 45 NORMATIVA 45 13
FIGURA 5- 46 NORMATIVA 46 13
FIGURA 5- 47 NORMATIVA 47 13
FIGURA 5- 48 NORMATIVA 48 14
FIGURA 5- 49 NORMATIVA 49 14
FIGURA 5- 50 NORMATIVA 50 14
FIGURA 5- 51 NORMATIVA 51 14
FIGURA 5- 52 NORMATIVA 52 14
FIGURA 5- 53 NORMATIVA 53 15

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

FIGURA 5- 54 NORMATIVA 54 15
FIGURA 5- 55 NORMATIVA 55 15
FIGURA 5- 56 NORMATIVA 56 15
FIGURA 5- 57 RECOMENDACIÓN 1 16
FIGURA 5- 58 RECOMENDACIÓN 2 16
FIGURA 5- 59 RECOMENDACIÓN 3 16
FIGURA 5- 60 RECOMENDACIÓN 4 17
FIGURA 5- 61 RECOMENDACIÓN 5 17
FIGURA 5- 62 RECOMENDACIÓN 6 17
FIGURA 5- 63 RECOMENDACIÓN 7 17
FIGURA 5- 64 RECOMENDACIÓN 8 18
FIGURA 5- 65 RECOMENDACIÓN 9 18
FIGURA 5- 66 RECOMENDACIÓN 10 18
FIGURA 5- 67 RECOMENDACIÓN 12 19

BIBLIOTECA CAMPUS PENAS

CAPÍTULO 6 LINUX

FIGURA 6-1: CD Y PC 4
FIGURA 6-2: TECLADO 5
FIGURA 6-3: PANTALLA DEL BIOS 5
FIGURA 6-4: TECLAS DIRECCIONALES 6
FIGURA 6-5: CONFIGURACIÓN DE BUTEO DEL SISTEMA 6
FIGURA 6-6: GUARDAR CAMBIOS Y SALIR DE CONFIGURACIONES DEL SETUP 7
FIGURA 6-7: REINICIACIÓN DEL COMPUTADOR 7
FIGURA 6-8: FEDORA BOOT 8
FIGURA 6-9: COMIENZO DE LA INSTALACIÓN 9
FIGURA 6-10: COMPROBACIÓN DE DISCOS 9
FIGURA 6-11: ELECCIÓN DE COMPROBACIÓN DE DISCO 10
FIGURA 6-12: CHEQUEO DE DISCOS 10
FIGURA 6-13: ACEPTACIÓN DE COMPROBACIÓN DE DISCOS 11
FIGURA 6-14: SELECCIÓN DEL PROCESO A INSTALARSE 11
FIGURA 6-15: PRESENTACIÓN INICIAL DE INSTALACIÓN 12
FIGURA 6-16: BIENVENIDA A FEDORA CORE 12
FIGURA 6-17: SELECCIÓN DE LENGUAJE 13
FIGURA 6-18: CONFIGURACIÓN DEL TECLADO 13
FIGURA 6-19: TIPO DE INSTALACIÓN 14
FIGURA 6-20: CONFIGURACIÓN DEL PARTICIONAMIENTO DEL DISCO 15
FIGURA 6-21: SELECCIÓN DEL PARTICIONAMIENTO DEL DISCO 16
FIGURA 6-22: CONFIGURACIÓN DEL DISCO 17
FIGURA 6-23: PUNTO DE MONTAJE RAÍZ 19
FIGURA 6-24: MODIFICAR PARTICIONES SWAP 19
FIGURA 6-25: PUNTO DE MONTAJE BOOT 20
FIGURA 6-26: CONFIGURACIÓN DEL GESTOR DE ARRANQUE 20
FIGURA 6-27: CONFIGURACIÓN DE RED 21
FIGURA 6-28: CONFIGURACIÓN DEL CORTAFUEGOS 21
FIGURA 6-29: SOPORTE ADICIONAL DEL IDIOMA 22
FIGURA 6-30: SELECCIÓN DEL HUSO HORARIO 22
FIGURA 6-31: CONFIGURACIÓN DE LA CONTRASEÑA DE ROOT 23
FIGURA 6-32: SELECCIÓN DE GRUPOS DE PAQUETES 23
FIGURA 6-33: ACEPTACIÓN DE GRUPOS DE PAQUETES 24
FIGURA 6-34: LISTO PARA LA INSTALACIÓN 24
FIGURA 6-35: MEDIO DE INSTALACIÓN REQUERIDO 25

FIGURA 6-36: FORMATEO DEL SISTEMA DE FICHEROS 25
FIGURA 6-37: FINALIZACIÓN DEL FORMATEO DE FICHEROS 26
FIGURA 6-38: INSTALACIÓN DE PAQUETES 26
FIGURA 6-39: FINALIZACIÓN DE LA INSTALACIÓN 27
FIGURA 6-40: INICIO DEL SISTEMA OPERATIVO INSTALADO 27
FIGURA 6-41: INICIALIZACIÓN DE LOS SERVICIOS DEL SISTEMA 28
FIGURA 6-42: BIENVENIDA AL SISTEMA 28
FIGURA 6-43: ACUERDO DE LICENCIA 29
FIGURA 6-44: CONFIGURACIÓN DE LA FECHA Y HORA 29
FIGURA 6-45: CONFIGURACIÓN DE LA RESOLUCIÓN DE LA PANTALLA 30
FIGURA 6-46: CONFIGURACIÓN DEL USUARIO DEL SISTEMA 30
FIGURA 6-47: CONFIGURACIÓN DE LA TARJETA DE SONIDO 31
FIGURA 6-48: CDS ADICIONALES 31
FIGURA 6-49: FINALIZAR LA CONFIGURACIÓN 32
FIGURA 6-50: INICIALIZACIÓN DEL SISTEMA LINUX 32
FIGURA 6-51: INGRESO DEL USUARIO 33
FIGURA 6-52: INGRESO DE LA CONTRASEÑA 33
FIGURA 6-53: ENTORNO GRÁFICO DE LINUX FEDORA CORE 3 34
FIGURA 6-54: ENTORNO MODO TEXTO DE LINUX 34
FIGURA 6-55: CONFIGURACIÓN DE LA TARJETA DE RED 38
FIGURA 6-56: VERIFICANDO IP 38
FIGURA 6-57: RESTAURAR LA TARJETA DE RED 39
FIGURA 6-58: INGRESO DEL COMANDO SETUP 39
FIGURA 6-59: CONFIGURACIÓN DE LA RED 40
FIGURA 6-60: ACEPTACIÓN DE LA CONFIGURACIÓN DE RED 40
FIGURA 6-61: CONFIGURACIÓN TCP/IP 41
FIGURA 6-62: REINICIAR EL SERVICIO DEL NETWORK 41
FIGURA 6-63: VERIFICANDO IP 42
FIGURA 6-64: SERVIDOR SAMBA 43
FIGURA 6-65: REVISIÓN DEL PAQUETE 46
FIGURA 6-66: INGRESO AL DIRECTORIO SAMBA 46
FIGURA 6-67: ARCHIVO DE SAMBA 47
FIGURA 6-68: CONFIGURACIÓN EN GLOBAL SETTING DE SAMBA 48
FIGURA 6-69: ESPECIFICAR VALORES DEL DIRECTORIO DEL SMB.CONF 49
FIGURA 6-70: CREA UN DIRECTORIO 49
FIGURA 6-71: INGRESO AL ARCHIVO PRUEBA.TXT 50
FIGURA 6-72: INGRESO DE DATOS EN EL ARCHIVO PRUEBA.TXT 50
FIGURA 6-73: PERMISOS DE LECTURA Y ESCRITURA AL ARCHIVO PRUEBA.TXT 51
FIGURA 6-74: PERMISOS DE LECTURA Y ESCRITURA A LA CARPETA 51
FIGURA 6-75: CREACIÓN DE USUARIO 52
FIGURA 6-76: CREACIÓN DE CONTRASEÑA 52
FIGURA 6-77: ASIGNACIÓN DE CONTRASEÑA AL SAMBA 53
FIGURA 6-78: RESTAURACIÓN DEL SERVICIO SAMBA 53
FIGURA 6-79: SETUP DE LINUX 54
FIGURA 6-80: SELECCIÓN DE SERVICIOS 54
FIGURA 6-81: SELECCIÓN CONFIGURACIÓN DEL FIREWALL 55
FIGURA 6-82: DESHABILITACIÓN DE LOS FIREWALL 55
FIGURA 6-83: PROPIEDADES DE MIS SITIOS DE RED 56
FIGURA 6-84: CONEXIONES DE RED 56
FIGURA 6-85: PROPIEDADES DE CONEXIÓN DE ÁREA LOCAL 57

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

FIGURA 6-86: PROPIEDADES DE PROTOCOLO INTERNET (TCP/IP) 57
FIGURA 6-87: SELECCIÓN BUSCAR EQUIPOS 58
FIGURA 6-88: BÚSQUEDA DE EQUIPOS 58
FIGURA 6-89: RESULTADO DE LA BÚSQUEDA DE EQUIPOS 59
FIGURA 6-90: INGRESO DE USUARIO Y CONTRASEÑA 59
FIGURA 6-91: RECURSOS COMPARTIDOS 60
FIGURA 6-92: ARCHIVO COMPARTIDO 60
FIGURA 6-93: INFORMACIÓN DEL ARCHIVO COMPARTIDO 61
FIGURA 6-94: SERVIDOR DNS 62
FIGURA 6-95: VERIFICAR PAQUETE DNS 65
FIGURA 6-96: ARCHIVO NAMED.CONF 66
FIGURA 6-97: LISTA DE ARCHIVOS DEL NAMED 67
FIGURA 6-98: COPIA DEL ARCHIVO LOCALHOST.ZONE 68
FIGURA 6-99: EDITAR FICHERO MOLINOSDELECUADOR.COM.ZONE 68
FIGURA 6-100: SETEO DE CAMPOS EN EL NAMED.CONF 69
FIGURA 6-101: COPIA DEL ARCHIVO A OTRO DIRECTORIO 69
FIGURA 6-102: INGRESO AL ARCHIVO RESOLV.CONF 70
FIGURA 6-103: EDITAR EL ARCHIVO RESOLV.CONF 70
FIGURA 6-104: INICIAR SERVICIOS NAMED 71
FIGURA 6-105: PING AL DOMINIO MOLINOSDELECUADOR.COM 71
FIGURA 6-106: SELECCIÓN DE PROPIEDADES DE MIS SITIOS DE RED 72
FIGURA 6-107: PROPIEDADES DE CONEXIONES DE RED 72
FIGURA 6-108: PROTOCOLO INTERNET TCP/IP 73
FIGURA 6-109: INGRESO DE IP Y DNS (SERVIDOR) 73
FIGURA 6-110: INGRESO AL CMD 74
FIGURA 6-111: PIN.G Y RESPUESTA DEL SERVIDOR 74
FIGURA 6-112: SERVIDOR WEB SERVER 75
FIGURA 6-113: VERIFICACIÓN DEL PAQUETE WEB SERVER 77
FIGURA 6-114: RUTA DE INGRESO A DIRECTORIO CONF 78
FIGURA 6-115: INGRESO AL ARCHIVO HTTPD.CONF 78
FIGURA 6-116: DESCOMENTAR PUERTO LISTEN 80 79
FIGURA 6-117: DIRECCIÓN DE ALMACENAMIENTO DEL SITIO WEB 79
FIGURA 6-118: DESCOMENTAR NAME VIRTUALHOST 80
FIGURA 6-119: CONFIGURACIÓN DEL VIRTUALHOST 80
FIGURA 6-120: RUTA DE INGRESO AL DIRECTORIO HTML 81
FIGURA 6-121: CREACIÓN DE LA CARPETA 81
FIGURA 6-122: CREACIÓN DEL ARCHIVO INDEX.HTML 82
FIGURA 6-123: INICIAR LOS SERVICIOS HTTPD 82
FIGURA 6-124: SELECCIÓN DE PROPIEDADES DE MIS SITIOS DE RED 83
FIGURA 6-125: PROPIEDADES DE CONEXIONES DE RED 83
FIGURA 6-126: PROTOCOLO INTERNET TCP/IP 84
FIGURA 6-127: INGRESO DE IP Y DNS (SERVIDOR) 84
FIGURA 6-128: INGRESO AL INTERNET EXPLORER 85
FIGURA 6-129: PRESENTACIÓN DE LA PÁGINA 85
FIGURA 6-130: SERVIDOR SENDMAIL 86
FIGURA 6-131: VERIFICAR PAQUETES SENDMAIL Y DOVECOT 88
FIGURA 6-132: CONFIGURACIÓN DE LOS PROTOCOLOS 88
FIGURA 6-133: LISTADO DE ARCHIVOS DEL DIRECTORIO MAIL 89
FIGURA 6-134: INGRESO AL ARCHIVO SENDMAIL.CF 89
FIGURA 6-135: SETEAR EL NOMBRE DEL DOMINIO 90

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

FIGURA 6-136:SMTP DAEMON OPTIONS 90
FIGURA 6-137: REINICIAR LOS SERVICIOS DEL SENDMAIL 91
FIGURA 6-138: VERIFICAR PUERTOS 110 Y 25 91
FIGURA 6-139: INGRESO AL ARCHIVO HOSTS 92
FIGURA 6-140: CONFIGURACIÓN DEL ARCHIVO HOSTS 92
FIGURA 6-141: CREACIÓN DE USUARIO Y CONTRASEÑA 93
FIGURA 6-142: RESTAURACIÓN DE LOS SERVICIOS DE DOVECOT Y SENDMAIL .. 93
FIGURA 6-143: ENVIÓ DE MAIL 94
FIGURA 6-144: SELECCIÓN DE OUTLOOK EXPRESS 95
FIGURA 6-145: PÁGINA PRINCIPAL DEL OUTLOOK EXPRESS 95
FIGURA 6-146: CONFIGURACIÓN DE CUENTAS 96
FIGURA 6-147: CUENTAS DE INTERNET 96
FIGURA 6-148: ASIGNACIÓN DE NOMBRE DE USUSARIO 97
FIGURA 6-149: DIRECCIÓN DE CORREO 97
FIGURA 6-150: ESPECIFICAR SERVIDOR DE CORREO ENTRANTE Y SALIENTE 98
FIGURA 6-151: INGRESO DE NOMBRE Y CONTRASEÑA 98
FIGURA 6-152: FINALIZAR CAMBIOS DEL ASISTENTE 99
FIGURA 6-153: FINALIZACIÓN DEL ASISTENTE 99
FIGURA 6-154: BANDEJA DE ENTRADA DE OUTLOOK 100
FIGURA 6-155: INGRESO AL MENSAJE 100
FIGURA 6-156: RESPUESTA AL MENSAJE 101
FIGURA 6-157: ENVIÓ DE MENSAJES 101
FIGURA 6-158: REVISIÓN DEL MENSAJE EN SERVIDOR 102
FIGURA 6-159: SERVIDOR PROXY 103
FIGURA 6-160: VERIFICACIÓN DEL PAQUETE SQUID 106
FIGURA 6-161: INGRESO AL DIRECTORIO DEL SQUID 106
FIGURA 6-162: INGRESO AL ARCHIVO SQUID.CONF 107
FIGURA 6-163: SETEO DEL PUERTO 8080 108
FIGURA 6-164: SETEO DE CACHE_MEM 108
FIGURA 6-165: SETEO DE CACHE_DIR 109
FIGURA 6-166: CONFIGURACIÓN CACHE_ACCESS_LOG 109
FIGURA 6-167: CONTROL DE ACCESO 110
FIGURA 6-168: APLICANDO REGLAS DE LISTA DE ACCESO 110
FIGURA 6-169: INICIAR SERVICIOS DEL SQUID 111
FIGURA 6-170: OPCIONES DE INTERNET 112
FIGURA 6-171: CONFIGURACIONES LAN 112
FIGURA 6-172: CONFIGURACIÓN DE LA RED DE ÁREA LOCAL (LAN) 113
FIGURA 6-173: CONFIGURACIÓN LA SECCIÓN SERVIDOR PROXY 113
FIGURA 6-174: PÁGINA HABILITADA DE MOLINOS 114
FIGURA 6-175:RESTRICCIONES DE PÁGINA 115
FIGURA 6-176: NEGACIÓN DE DIRECCIÓN 115
FIGURA 6-177: INICIO DEL SERVICIO SQUID 116
FIGURA 6-178: ENTORNO DE WINDOWS 117
FIGURA 6-179: PÁGINA BLOQUEADA 117
FIGURA 6-180: INGRESO AL ARCHIVO SQUID.CONF 118
FIGURA 6-181: RESTRICCIÓN A USUARIOS 118
FIGURA 6-182:NEGACIÓN A USUARIOS 119
FIGURA 6-183: CREACIÓN DE ARCHIVO CONTENEDORA DE USUARIOS 119
FIGURA 6-184: IP A NEGAR 120
FIGURA 6-185: INICIO DEL SERVICIO SQUID 120

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

FIGURA 6-186: ENTORNO DE WINDOWS 121
FIGURA 6-187: BLOQUEO DE PÁGINA 121
FIGURA 6-188: INGRESO AL ARCHIVO SQUID.CONF 122
FIGURA 6-189: LISTA DE CONTROL DE ACCESO 122
FIGURA 6-190: RESTRICCIÓN POR HORA 123
FIGURA 6-191: INICIAR SERVICIO SQUID 123
FIGURA 6-192: ENTORNO DE WINDOWS 124
FIGURA 6-193: RESTRICCIONES DE PÁGINA 124
FIGURA 6-194:INGRESO AL ARCHIVO SQUID.CONF 125
FIGURA 6-195: RUTA DE ALOJAMIENTO DE LAS CONTRASEÑAS 125
FIGURA 6-196: ACL PASSWORD 126
FIGURA 6-197: HTTP_ACCESS POR AUTENTICACIÓN 126
FIGURA 6-198: CREACIÓN DE ARCHIVO PASSWD 127
FIGURA 6-199: PERMISO PARA EL ARCHIVO PASSWD 127
FIGURA 6-200: CREACIÓN DE USUARIOS Y CONTRASEÑAS 128
FIGURA 6-201: ENTORNO DE WINDOWS 128
FIGURA 6-202: OPCIONES DE INTERNET EN INTERNET EXPLORER 129
FIGURA 6-203: PÁGINA HABILITADA 129
FIGURA 6-204: FIREWALL 130
FIGURA 6-205: BLOQUEO PING 135
FIGURA 6-206: INGRESO AL DIRECTORIO DEL XINETD.D 135
FIGURA 6-207: INGRESO AL ARCHIVO KRB5-TELNET 136
FIGURA 6-208: HABILITACIÓN DEL TELNET 136
FIGURA 6-209: BLOQUEO TELNET 137
FIGURA 6-210: BLOQUEO FTP 137
FIGURA 6-211: LIST DE IPTABLES 138
FIGURA 6-212 INGRESO AL CMD 138
FIGURA 6-213: PING AL SERVIDOR 139
FIGURA 6-214: BLOQUEO DE PING 139
FIGURA 6-215: TELNET AL SERVIDOR 140
FIGURA 6-216 BLOQUEO DE TELNET 140
FIGURA 6-217 SERVIDOR DHCP 141
FIGURA 6-218 VERIFICAR PAQUETE DHCP 144
FIGURA 6-219: BUSQUEDA DEL ARCHIVO DHCPD.CONF 144
FIGURA 6-210: COPIA DEL FICHERO DHCPD.CONF 145
FIGURA 6-221: INGRESO AL ARCHIVO DHCPD.CONF 145
FIGURA 6-222: CONFIGURACIÓN DHCP 146
FIGURA 6-223: CREACIÓN DEL ARCHIVO DHCP.LEASES 146
FIGURA 6-224: COMANDO DE ARRANQUE DEL SISTEMA 147
FIGURA 6-225: VERIFICACIÓN DEL ESTADO DE DHCPD 147
FIGURA 6-226: RESTAURAR LOS SERVICIO DHCPD 147
FIGURA 6-227: SELECCIÓN DE PROPIEDADES DE MIS SITIOS DE RED 148
FIGURA 6-228: PROPIEDADES DE CONEXIONES DE RED 148
FIGURA 6-229: PROTOCOLO INTERNET TCP/IP 149
FIGURA 6-230: OBTENER DIRECCIÓN IP AUTOMÁTICAMENTE 149
FIGURA 6-231: VERIFICACIÓN DE DIRECCIÓN ASIGNADA AUTOMÁTICAMENTE 150

BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 7 ROUTER

FIGURA 7-1: INTRODUCCIÓN A ROUTER. 1
FIGURA 7-2: VISTA FRONTAL DEL ROUTER. 2
FIGURA 7-3: VISTA POSTERIOR DEL ROUTER. 2
FIGURA 7-4: ESTRUCTURA DEL ROUTER. 3
FIGURA 7-5: COMPONENTES BÁSICOS DE UN ROUTER. 5
FIGURA 7-6: CONEXIONES EXTERNAS DEL ROUTER. 6
FIGURA 7-7: CONEXIÓN AL PUERTO DE ADMINISTRACIÓN. 7
FIGURA 7-8: CABLE DTC. 7
FIGURA 7-9: CABLE DCE. 8
FIGURA 7-10: CABLE UTP (CAT 5E). 8
FIGURA 7-11: CONECTOR RJ 45. 9
FIGURA 7-12: PUERTO SERIAL. 9
FIGURA 7-13: PROTOCOLO RIP. 12
FIGURA 7-14: PROTOCOLO IGRP. 14
FIGURA 7-15: PROTOCOLO OSPF. 18
FIGURA 7-16: LISTAS DE CONTROL DE ACCESO. 21
FIGURA 7-17: CREACIÓN DE ACL. 22
FIGURA 7-18: RED ESTRELLA. 27
FIGURA 7-19: FUNCIONAMIENTO DE LOS CONMUTADORES. 28
FIGURA 7-20: GRAFICO GENERAL DE COMUNICACIONES. 33
FIGURA 7-21: VLAN. 34
FIGURA 7-22: CASO DE ESTUDIO MOLINOS DEL ECUADOR. 43
FIGURA 7-23: CONFIGURACIÓN HYPERTERMINAL. 44
FIGURA 7-24: DESCRIPCIÓN DE LA CONEXIÓN. 44
FIGURA 7-25: CONFIGURACIÓN HYPERTERMINAL. 45
FIGURA 7-26: PROPIEDADES COM 1. 45
FIGURA 7-27: NOMBRE DE LA CONEXIÓN. 46
FIGURA 7-28: NOMBRE ROUTER ISP. 49
FIGURA 7-29: CONTRASEÑA AL ROUTER ISP. 50
FFIGURA 7-30: CONFIGURACIÓN INTERFAZ SERIAL 0. 51
FIGURA 7-31: CONFIGURACIÓN PROTOCOLO RIP. 52
FIGURA 7-32: SHOW PROTOCOLS ISP. 53
FIGURA 7-33: SHOW RUN ISP. 54
FIGURA 7-34: SHOW IP ROUTE ISP. 56
FIGURA 7-35: ASIGNACIÓN NOMBRE ROTER MATRIZ. 60
FIGURA 7-36: ASIGNACIÓN DE CONTRASEÑA ROUTER MATRIZ. 61
FIGURA 7-37: CONFIGURACIÓN INTERFAZ SERIAL 1/0. 62
FIGURA 7-38: CONFIGURACIÓN INTERFAZ SERIAL 1/1. 63
FIGURA 7-39: CONFIGURACIÓN INTERFAZ SERIAL 1/2. 64
FIGURA 7-40: CONFIGURACIÓN INTERFAZ FASTHERNET 0/0. 65
FIGURA 7-41: ENRUTAMIENTO VLAN 10. 66
FFIGURA 7-42: ENRUTAMIENTO VLAN 20. 67
FIGURA 7-43: ENRUTAMIENTO VLAN 30. 67
FIGURA 7-44: ENRUTAMIENTO VLAN 40. 68
FIGURA 7-45: PROTOCOLO OSPF. 69
FIGURA 7-46: SHOW PROTOCOLS MATRIZ. 70
FIGURA 7-47: SHOW IP ROUTE MATRIZ. 71
FIGURA 7-48: SHOW RUN MATRIZ. 73
FIGURA 7-49: ASIGNACIÓN DE NOMBRE ROUTER SUCURSAL AMBATO. 79

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

FIGURA 7-50: ASIGNACIÓN DE CONTRASEÑA ROUTER SUCURSAL AMBATO. 80
FIGURA 7-51: IP INTERFAZ SERIAL 0. 81
FIGURA 7-52: IP INTERFAZ FASTHERNET 0/0. 82
FIGURA 7-53: ENRUTAMIENTO VLAN 50. 83
FIGURA 7-54: ENRUTAMIENTO VLAN 60. 84
FIGURA 7-55: IP ENRUTAMIENTO VLAN 70. 84
FIGURA 7-56: CONFIGURACIÓN PROTOCOLO OSPF. 85
FIGURA 7-57: SHOW PROTOCOLS AMBATO. 86
FIGURA 7-58: SHOW RUN AMBATO. 87
FIGURA 7-59: SHOW IP ROUTE AMBATO. 90
FIGURA 7-60: NOMBRE ROUTER SUCURSAL QUITO. 95
FIGURA 7-61: CONTRASEÑA ROUTER QUITO. 96
FIGURA 7-62: IP INTERFAZ SERIAL 0. 97
FIGURA 7-63: CONFIGURACIÓN FASTHERNET 0/0. 98
FIGURA 7-64: ENRUTAMIENTO VLAN 80. 99
FIGURA 7-65: ENRUTAMIENTO VLAN 90. 100
FIGURA 7-66: ENRUTAMIENTO VLAN 100. 101
FIGURA 7-67: PROTOCOLO OSPF QUITO. 101
FIGURA 7-68: SHOW PROTOCOLS QUITO. 102
FIGURA 7-69: SHOW RUN QUITO. 103
FIGURA 7-70: SHOW IP ROUTE DE QUITO. 105
FIGURA 7-71: ASIGNACIÓN NOMBRE SWITCH MATRIZ. 110
FIGURA 7-72: CREACIÓN VLAN. 111
FIGURA 7-73: INTERFACE FASTHERNET 0/1. 112
FIGURA 7-74: INTERFACE FASTHERNET 0/2. 112
FIGURA 7-75: INTERFACE FASTHERNET 0/3. 112
FIGURA 7-76: INTERFACE FASTHERNET 0/4. 113
FIGURA 7-77: INTERFACE FASTHERNET 0/5. 113
FIGURA 7-78: SHOW VLAN MATRIZ. 114
FIGURA 7-79: ASIGNACIÓN DE IP MATRIZ. 117
FIGURA 7-81: CREACIÓN VLAN AMBATO. 119
FIGURA 7-82: INTERFCAE FASTHERNET 0/1. 120
FIGURA 7-83: INTERFCAE FASTHERNET 0/2. 120
FIGURA 7-84: INTERFCAE FASTHERNET 0/3. 121
FIGURA 7-85: INTERFCAE FASTHERNET 0/4. 121
FIGURA 7-86: SHOW VLAN AMBATO. 122
FIGURA 7-87: SHOW VLAN AMBATO. 125
FIGURA 7-88: ASIGNACIÓN NOMBRE SWITCH AMBATO. 126
FIGURA 7-89: CREACIÓN DE VLAN SWITCH AMBATO. 127
FIGURA 7-90: INTERFACE FASTHERNET 0/1. 128
FIGURA 7-91: INTERFACE FASTHERNET 0/2. 128
FIGURA 7-92: INTERFACE FASTHERNET 0/3. 129
FIGURA 7-93: INTERFACE FASTHERNET 0/4 129
FIGURA 7-94: SHOW VLAN QUITO. 130
FIGURA 7-95: ACCESS GROUP SERIAL 1/1. 138
FIGURA 7-98: PRUEBA DE CONEXIÓN QUITO. 140
FIGURA 7-100: ACCESS LISTS. 141
FIGURA 7-101: CONFIGURACIÓN ACCESS GOUP. 142
FIGURA 7-105: PRUEBAS DE TELNET QUITO. 145

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

FIGURA 7-106: PRUEBAS DE TELNET AMBATO 145

INDICE DE TABLAS

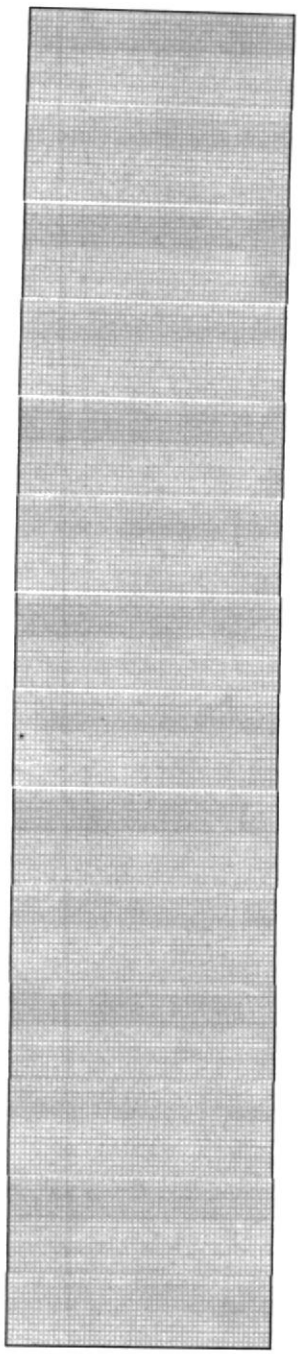
CAPITULO 2

TABLA 2-1: ESTACIONES DE TRABAJO (MATRIZ) 3
TABLA 2-2: ESTACIONES DE TRABAJO (SUCURSALES) 4
TABLA 2-3: SOFTWARE INSTALADOS (MATRIZ-SUCURSALES) 4
TABLA 2-4: SERVIDORES (MATRIZ) 6
TABLA 2-5: SERVIDOR REYVENTAS 6
TABLA 2-6: DISPOSITIVOS DE CONMUTACIÓN (MATRIZ-QUITO-AMBATO) 20
TABLA 2-7: CARACTERÍSTICAS DEL FIREWALL 23
TABLA 3-1: PROBLEMAS ENCONTRADOS 1
TABLA 3-2: SOLUCIÓN PROPUESTA 2
TABLA 3-3: DISPOSITIVOS DE CONMUTACIÓN 3
TABLA 3-4: MATERIALES DE CABLEADO ESTRUCTURADO 3
TABLA 3-5: FACTIBILIDAD OPERATIVA 4
TABLA 3-6: FACTIBILIDAD ECONÓMICA 5
TABLA 3-7: COSTO OPERATIVO 6
TABLA 3-8: COSTO TOTAL DE PROPUESTA ALTERNATIVA "A" 6
TABLA 3-9: DISPOSITIVOS DE CONMUTACIÓN ALTERNATIVA "B" 9
TABLA 3-10: MATERIALES DE CABLEADO ESTRUCTURADO ALTERNATIVA "B" 9
TABLA 3-11: FACTIBILIDAD OPERATIVA ALTERNATIVA "B" 10
TABLA 3-12: FACTIBILIDAD ECONÓMICA ALTERNATIVA "B" 11
TABLA 3-13: COSTO OPERATIVA ALTERNATIVA "B" 12
TABLA 3-14: COSTO TOTAL DE PROPUESTA ALTERNATIVA "B" 12

CAPITULO 3

TABLA 3-1: PROBLEMAS ENCONTRADOS 1
TABLA 3-2: SOLUCIÓN PROPUESTA 2
TABLA 3-3: DISPOSITIVOS DE CONMUTACIÓN 3
TABLA 3-4: MATERIALES DE CABLEADO ESTRUCTURADO 3
TABLA 3-5: FACTIBILIDAD OPERATIVA 4
TABLA 3-6: FACTIBILIDAD ECONÓMICA 5
TABLA 3-7: COSTO OPERATIVO 6
TABLA 3-8: COSTO TOTAL DE PROPUESTA ALTERNATIVA "A" 6
TABLA 3-9: DISPOSITIVOS DE CONMUTACIÓN ALTERNATIVA "B" 9
TABLA 3-10: MATERIALES DE CABLEADO ESTRUCTURADO ALTERNATIVA "B" 9
TABLA 3-11: FACTIBILIDAD OPERATIVA ALTERNATIVA "B" 10
TABLA 3-12: FACTIBILIDAD ECONÓMICA ALTERNATIVA "B" 11
TABLA 3-13: COSTO OPERATIVA ALTERNATIVA "B" 12
TABLA 3-14: COSTO TOTAL DE PROPUESTA ALTERNATIVA "B" 12

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 1

GENERALIDADES

1.1 INTRODUCCIÓN

Este manual es una guía de consulta para Usuario de cualquier nivel de informático.

1.2 OBJETIVO DE ESTE MANUAL

El objetivo de este manual es brindar una guía de consulta rápida y sencilla información acerca de la plataforma Linux en ambientes de redes empresariales con servicios de correo: Send Mail, Server Proxy, Autenticación e integración con clientes Microsoft, Configuración de Equipo de Comunicación Routers y Switchs, basado en un caso de estudio de empresa a nivel Lan y Wan.

1.3 A QUIÉN VA DIRIGIDO ESTE MANUAL

Este manual está orientado para usuarios finales involucrados en el Área de Redes, que requieren realizar configuraciones para la administración de una red con sus respectivas políticas de seguridad y permisos de acceso a PC y el uso de Internet en ambientes heterogéneo de plataformas de red.

1.4 QUÉ SE DEBE CONOCER

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

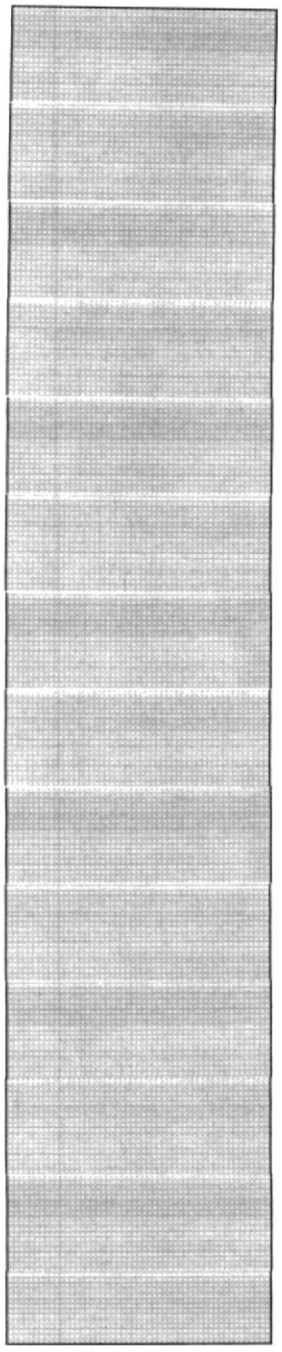
- Conceptos básicos de Redes y Sistemas Operativos de red.
- Conocimientos básicos de Información basados en el ambientes de Internet u Operacional.

1.5 ACERCA DE ESTE MANUAL

Este manual contiene diversas ilustraciones e instrucciones que el Usuario debe seguir paso a paso para poder manejar correctamente las configuraciones de Linux Fedora.

Además incluye información adicional que servirá para orientar al Usuario sobre Configuración de Equipo de Comunicación





ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 2

SITUACIÓN ACTUAL

2. SITUACION ACTUAL
2.1. ANTECEDENTES

La compañía fue fundada en 1952 y la construcción de sus instalaciones industriales estuvo a cargo de la famosa compañía inglesa CHRISTIAN NIELSEN, especializada en la construcción de modernos molinos de harina de trigo, utilizando para el efecto la mejor tecnología en la fabricación de harinas para consumo humano. Desde entonces, la compañía se ha mantenido a la vanguardia de la tecnología de Producción de Harinas y Subproductos.

El Grupo Molidor está compuesto por varias empresas dedicadas a actividades industriales, bioacuáticas, agropecuarias y comerciales en el área de alimentos Molidor. Son parte de la división industrial del grupo:

- La compañía **MOLINOS DEL ECUADOR** que es la matriz, se dedica a la fabricación de harinas para consumo humano, y para alimentos balanceados.
- **MOLINOS CHAMPION**, que se dedica a la fabricación de alimentos balanceados para animales.
- Interamericana **INTERAMA** de Tejidos, dedicada a la fabricación de sacos de polipropileno, zunchos y cabos plásticos y otros productos.
- Nuestra división local de COMERCIO EXTERIOR se dedica a la comercialización de granos de procedencia extranjera en el mercado nacional, particularmente entre los importadores de trigo (molineros) o entre los productores de alimento balanceado y consumidores de maíz, soya, sorgo y otros cereales.

La División bioacuática la componen:

- **DIBSA** (Desarrollo Industrial Bioacuático) que se dedica a la crianza de camarones en cautiverio y su empresa filial.
- **ACUATECSA** que se dedica a la producción de larva de camarones en laboratorio.
- **GRANPORSA** en la división agroindustrial se dedica a la crianza de cerdos.
- **REYVENTAS** la más joven de las empresas del grupo, dentro de la división comercial se dedica a la comercialización de los productos industriales del grupo y de algunos productos fabricados por otras empresas.

2.1.1. MISIÓN

Compromiso de producir servicios de calidad, eficientes y tecnológicamente adecuados a las necesidades de la comunidad y los socios.

2.1.2. VISIÓN

Contribuir al desarrollo del País y liderar los servicios en el ámbito nacional.

ESPOL BIBLIOTECA CAMPUS PEÑAS

2.2. COMUNICACIÓN WAN MATRIZ Y SUCURSALES

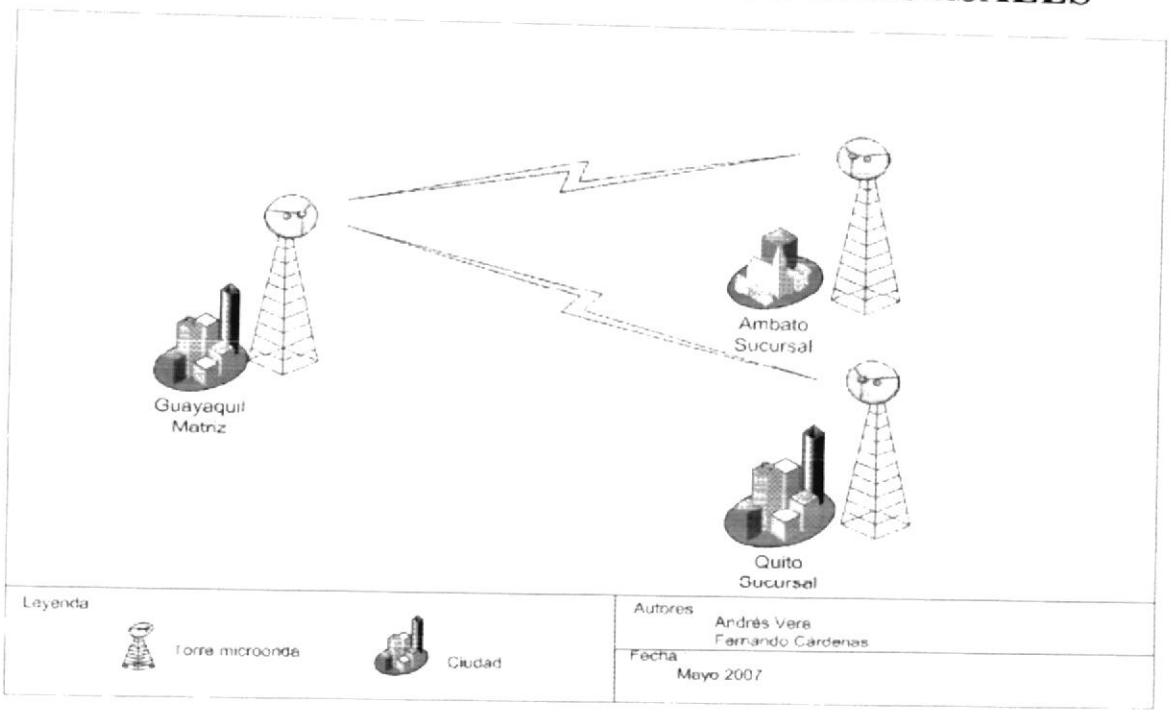


Figura 2-1: Comunicación Wan Matriz y Sucursales

Molinos del Ecuador está comprendida en 1 Matriz, 2 Sucursales y 2 empresas anexas (sub-empresas) las cuales se encuentran ubicadas de la siguiente manera:

- **MATRIZ:** Molinos del Ecuador (Guayaquil)
- **SUCURSAL 1:** Molinos del Ecuador (Quito)
- **SUCURSAL 2:** Molinos del Ecuador (Ambato)
- **SUCURSAL 3:** ReyVentas (Guayaquil)
- **SUCURSAL 4:** Dibsa (Guayaquil)

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.3. INFRAESTRUCTURA LAN

Molinos del Ecuador cuenta con una infraestructura a nivel LAN, la cual es implementada tanto en la matriz como en sus sucursales.

1. Se mantiene en Topología Estrella.
2. Posee ***Cable UTP Categoría 5***.
3. Maneja una velocidad de 10/100 Mbps en el Cableado Horizontal (HC).
4. Poseen una Central Telefónica de la Empresa (POP) que se encuentra ubicado en el Departamento de Sistemas.
5. La temperatura dentro del sitio del trabajo esta controlada mediante ductos de aire acondicionado.
6. El suministro de energía eléctrica del sitio de trabajo, esta dado por los transformadores debidamente polarizados con barras de cobre.

2.3.1. ESTACIONES DE TRABAJO

2.3.1.1. MATRIZ

BIBLIOTECA CAMPUS PEÑAS

Cantidad	Equipo	Características
120	PC	Procesador 933 Mhz Memoria RAM 256 Mb Disco duro de 40 GB Tarjeta de red 10/100
20	Impresora HP 825c	Entrada: 850 hojas Velocidad:52 Procesador:460 Mhz
10	Impresora EPSON LX-300 Matricial	Velocidad:15 PPM Semi-automática

Tabla 2-1: Estaciones de Trabajo (Matriz)

2.3.1.2. SUCURSALES QUITO, AMBATO, REYVENTAS, DIBSA

Cantidad	Equipo	Características
55	PC	Procesador Intel Pentium IV de 2.8GHz Motherboard 865 PERL 533-800 Mhz Disco Duro 80 GB Ide 7200 rpm Memoria RAM de 512 MB Tarjeta de red PCI 10/100 Mbps
20	Impresora HP 825c	Entrada: 850 hojas Velocidad:52 PPMProcesador:460 Mhz
10	Impresora EPSON LX-300 Matricial	Velocidad:15 PPM Semi-automática

Tabla 2-2: Estaciones de Trabajo (Sucursales)



2.3.2. SOFTWARE INSTALADOS MATRIZ Y SUCURSALES

Software	Características	Instalados
Windows Xp /Pack2	Sistema Operativo con Licencia	PC de Usuarios
Linux Red Hat	Sistema Operativo instalado en Servidor	Proxy Server, Mail Server, Dns
Microsoft Office 2003	Herramienta de Utilitarios Básico - No Actualizado	PC de Usuarios
Norton 2005	Antivirus	PC de Usuarios

Tabla 2-3: Software Instalados (Matriz-Sucursales)

2.3.3. TOPOLOGÍA ESTRELLA DE MOLINOS

La Topología Estrella cuenta con las siguientes características:

- Dispositivo principal switch.
- Velocidad 10/100 MBPS.
- Transmisión Full Duplex.
- Acceso múltiple a la red.
- Brinda soporte a la red.

ESPOL BIBLIOTECA CAMPUS PEÑAS

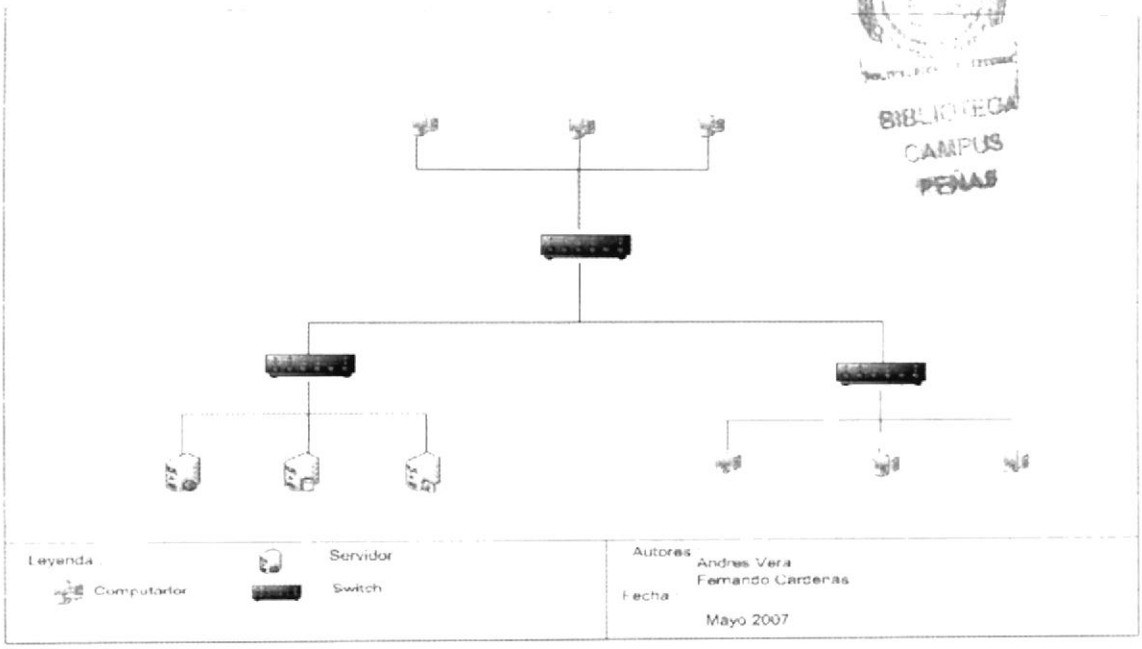


Figura 2-2: Topología

2.3.4. MEDIOS DE COMUNICACIÓN

2.3.4.1. ALÁMBRICOS

El medio utilizado en la empresa es cable UTP cat 5 con una velocidad de transmisión de 10/100 Mbps, tanto para el backbone horizontal como vertical.

- Matriz
- Quito
- Ambato

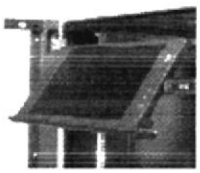
2.3.4.2. INALÁMBRICO

Molinos del Ecuador utiliza microondas como medio de transmisión. El protocolo que se utiliza es de IEEE 802.11b que transmite a 2.4 GHz con un ancho de banda de 532 KBPS.

El servicio utiliza una antena que se coloca en un área despejada sin obstáculos de edificios, árboles u otras cosas que pudieran entorpecer una buena recepción en el edificio o receptor y se coloca un módem que interconecta con la antena y la computadora. La comunicación entre el módem y la computadora se realiza a través de una tarjeta de red, que debe estar instalada en la computadora.

2.3.5. SERVIDORES

2.3.5.1. MATRIZ





ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 2-3: Servidor Matriz

Cantidad	Descripción	Características
1	Servidor de Aplicaciones	PowerEdge 28.50 marca Dell 1 Dual CORP 2.8 Ghz (2 Procesadores) Posee Memoria RAM de 4 GB. Sistema Operativo Windows 2003 Server Tarjeta de red de 10/100/1000 Mbps Posee 2 Disco Duro de 73 GB (arrays) Posee 4 Disco Duro de 146 GB (arrays)
1	Datos Impresión	Sistema Operativo Windows 2003 Server Procesador 1.2 Mhz Memoria RAM 1 GB Disco duro de 40 GB Tarjeta de Red 10/100 Mbps
1	Dns Dhcp Mail Web	Linux Read Hat 9.0 Pentium IV de 2.8 Mhz Memoria RAM 1 GB Disco duro de 40 GB Tarjeta de red 10/100 Mbps

Tabla 2-4: Servidores (Matriz)

2.3.5.2. SUCURSAL REYVENTAS

Cantidad	Descripción	Características
1	Servidor Aplicaciones	Posee Memoria RAM 512 MB Disco duro 80 GB Sistema Operativo Windows 2003 Server Tarjeta de red de 10/100/1000 Mbps

Tabla 2-5: Servidor Reyventas

2.3.6. ESTRUCTURA DEL BACKBONE HORIZONTAL

2.3.6.1. MATRIZ

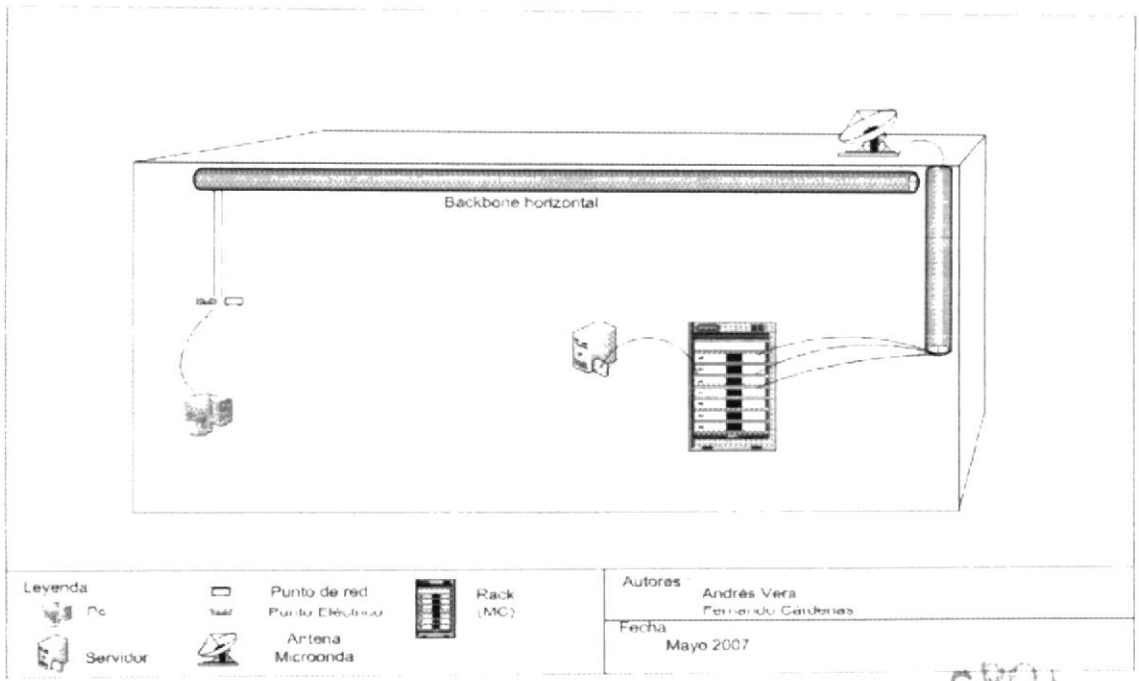


Figura 2-4: Estructura del Backbone Matriz

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.3.6.2. SUCURSAL QUITO

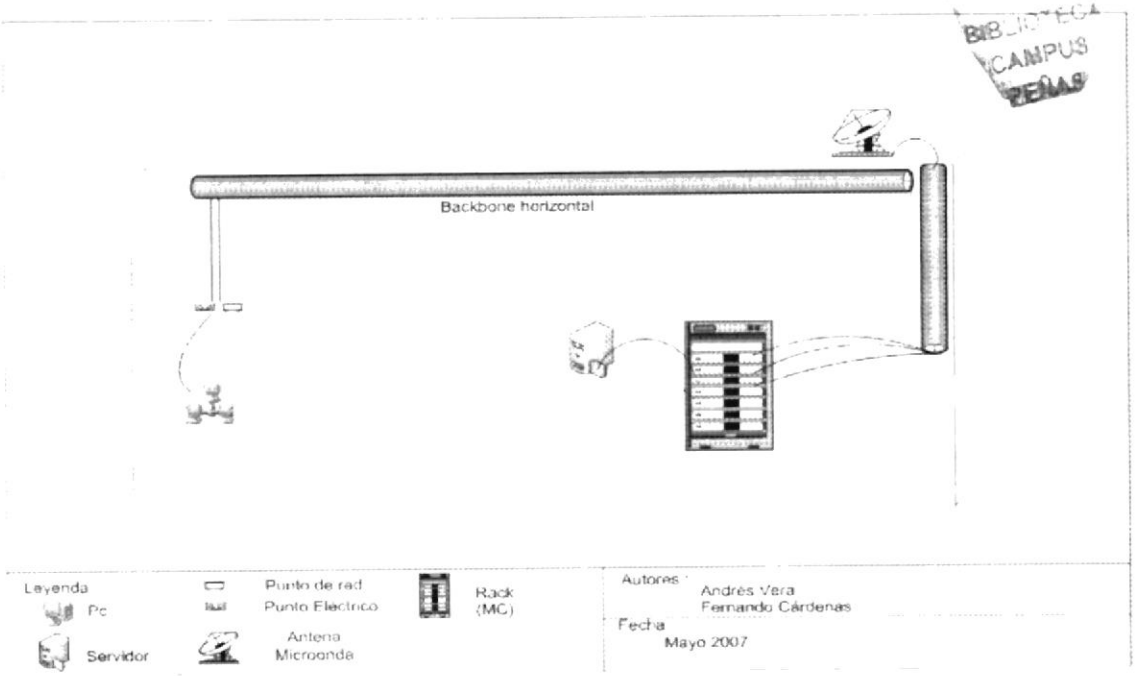


Figura 2-5: Estructura del Backbone Sucursal Quito

2.3.6.3. SUCURSAL AMBATO

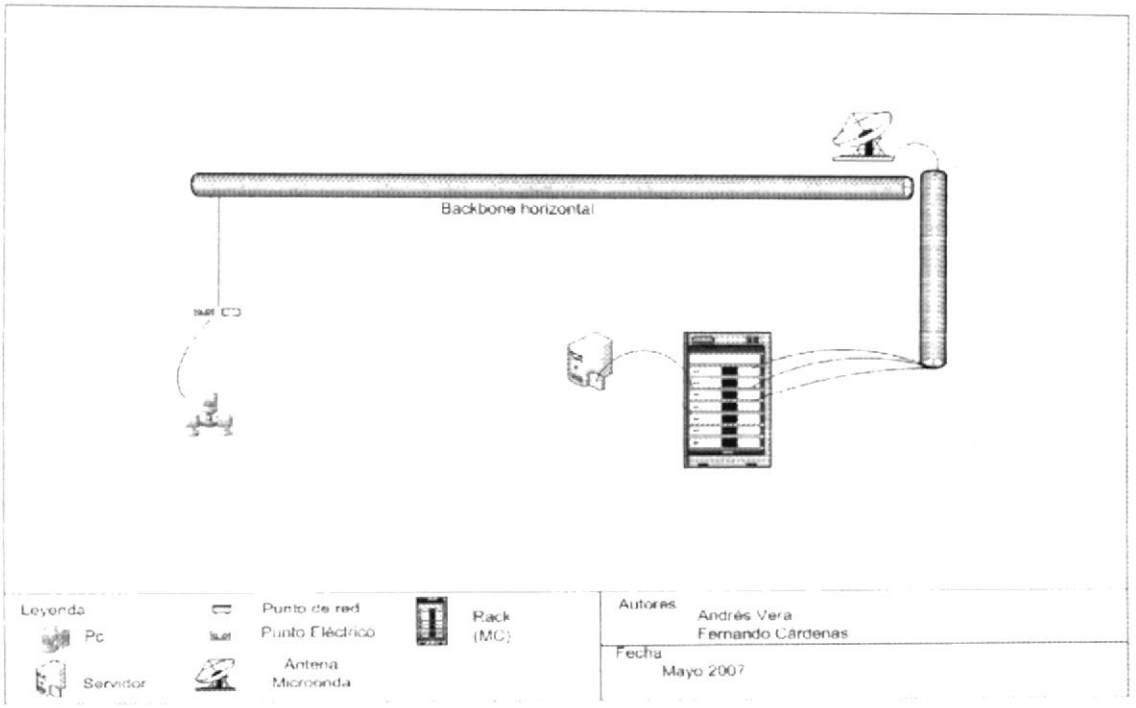


Figura 2-6: Estructura del Backbone Sucursal Ambato

ESPOL
BIBLIOTECA CAMPUS PEÑAS

2.3.6.4. SUCURSAL DIBSA

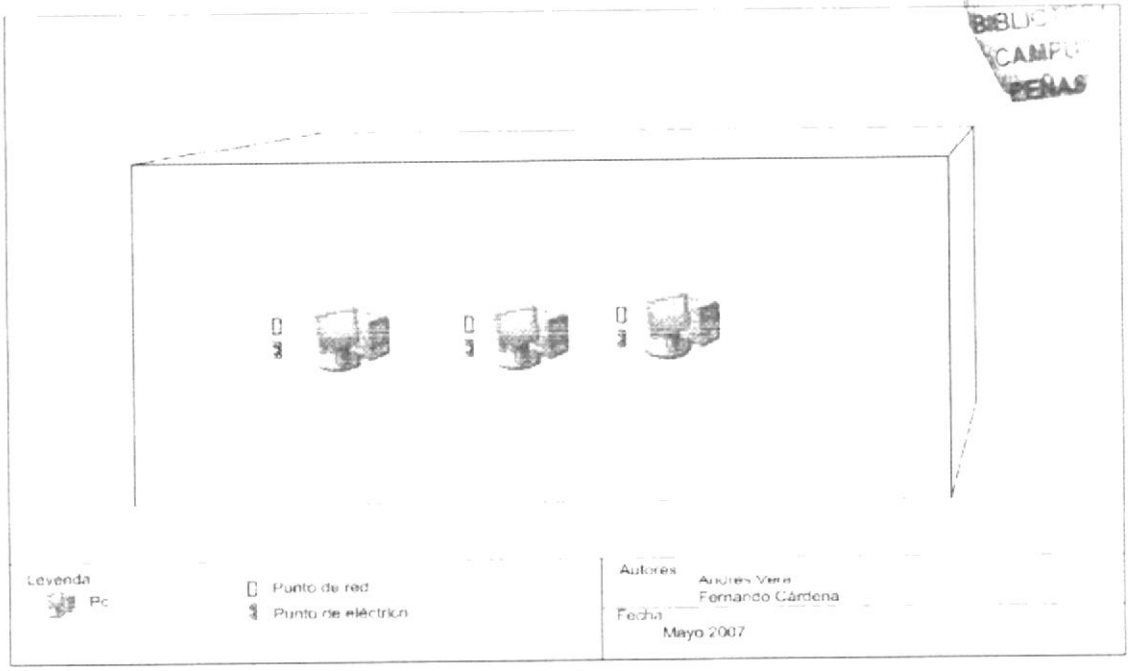


Figura 2-7: Estructura Sucursal Dibsa

2.3.6.5. SUCURSAL REYVENTAS

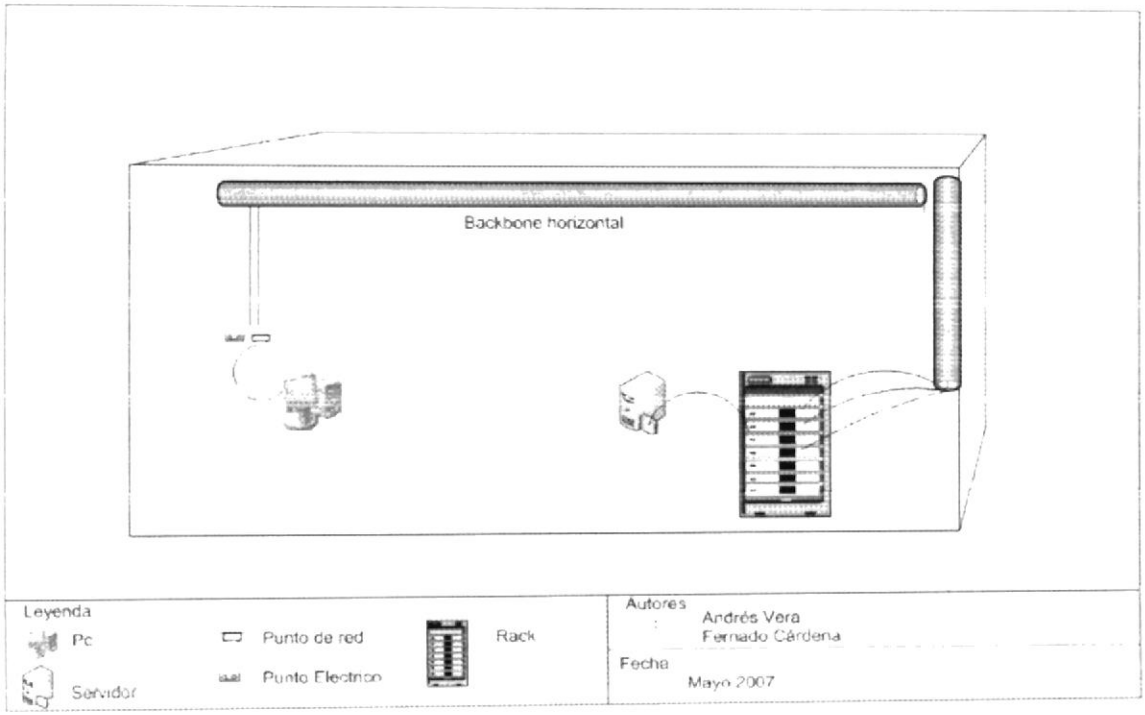


Figura 2-8: Estructura del Backbone Sucursal Reyventas

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.3.7. ANÁLISIS DE PISO APLICATIVO

2.3.7.1. MATRIZ

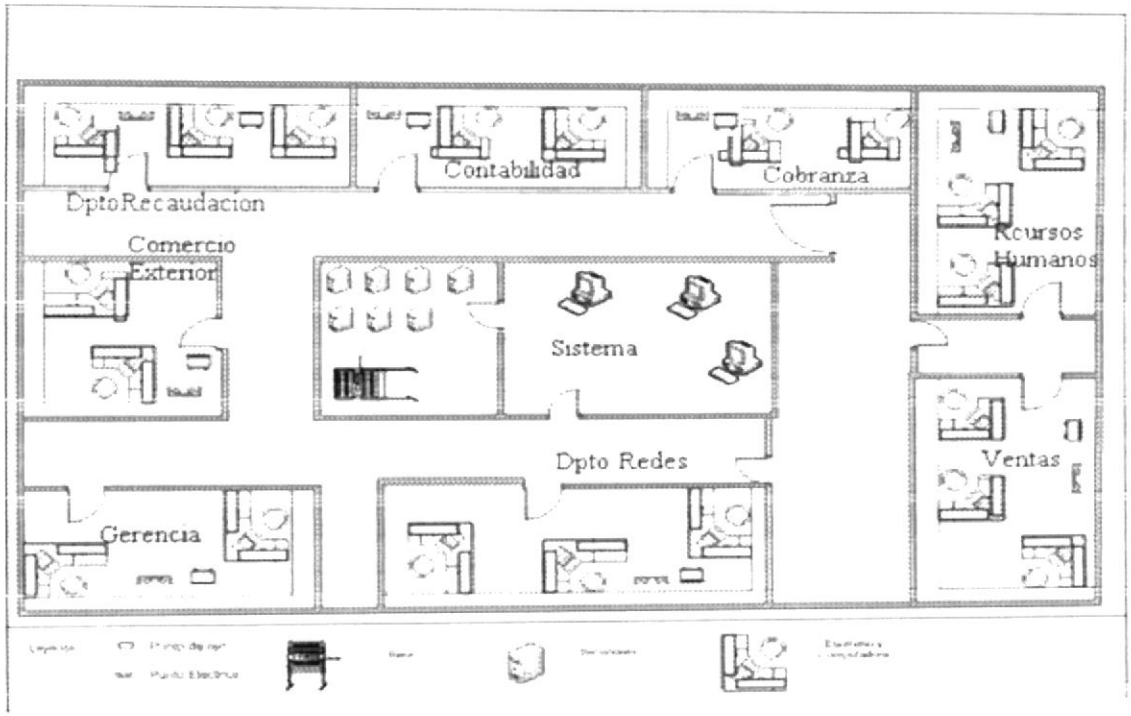


Figura 2-9: Análisis de Piso Aplicativo Matriz

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.3.7.2. SUCURSAL QUITO

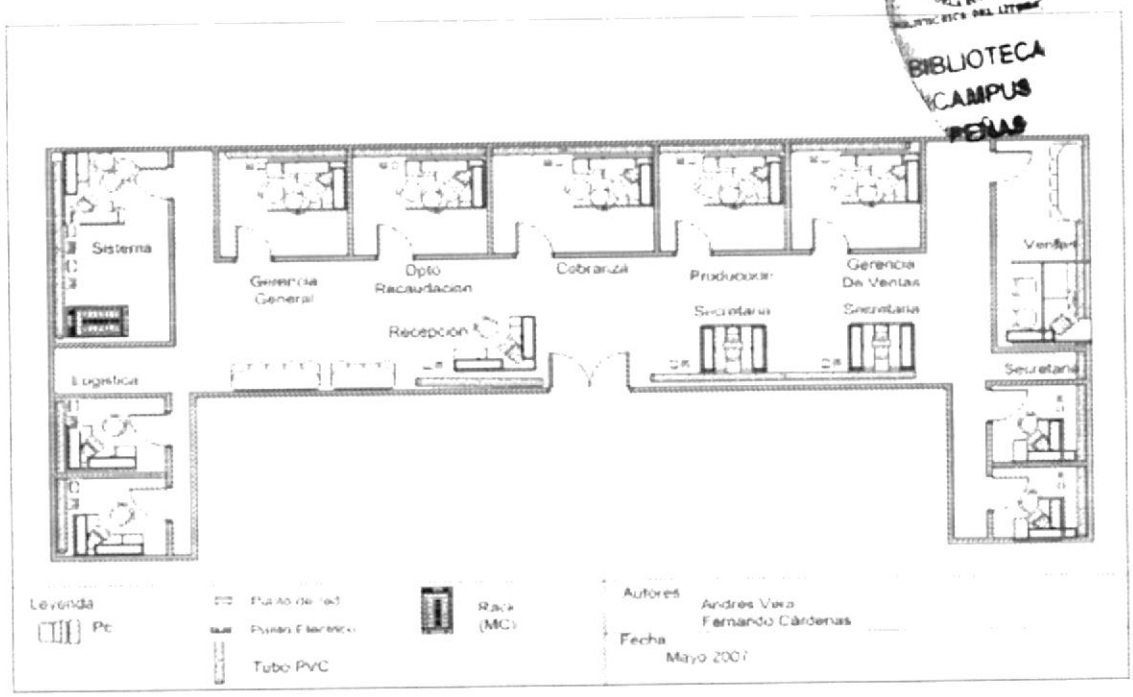


Figura 2-10: Análisis de Piso Aplicativo Sucursal Quito

2.3.7.3. SUCURSAL AMBATO

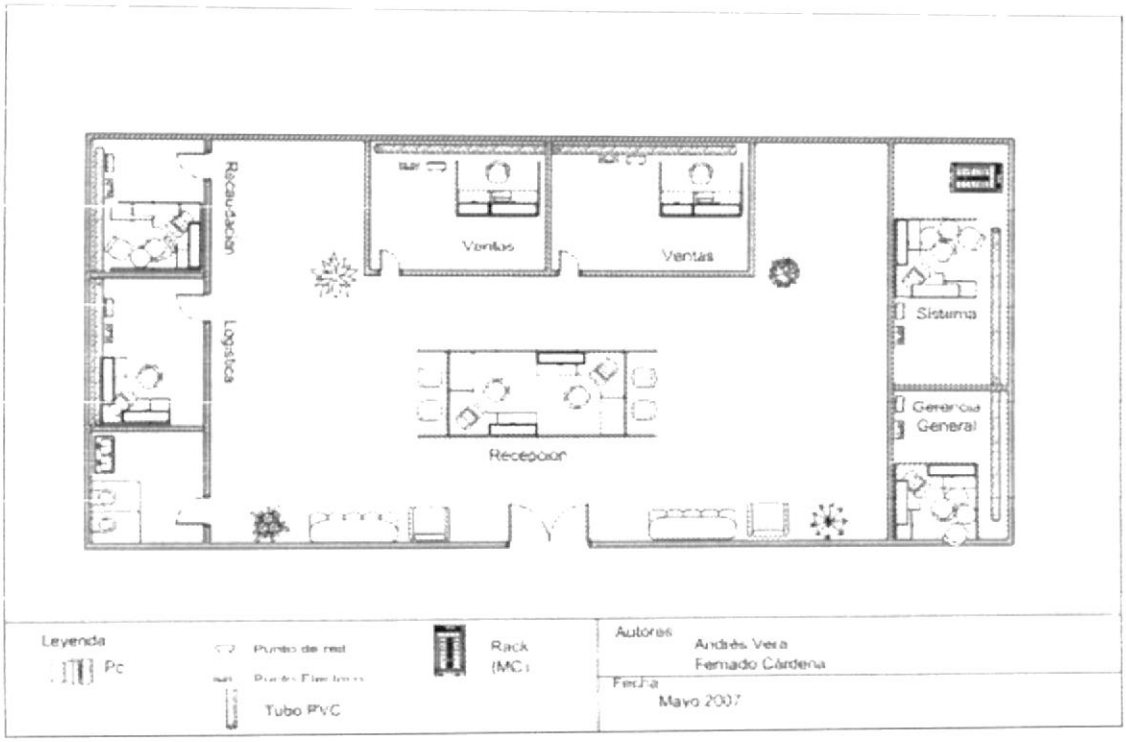
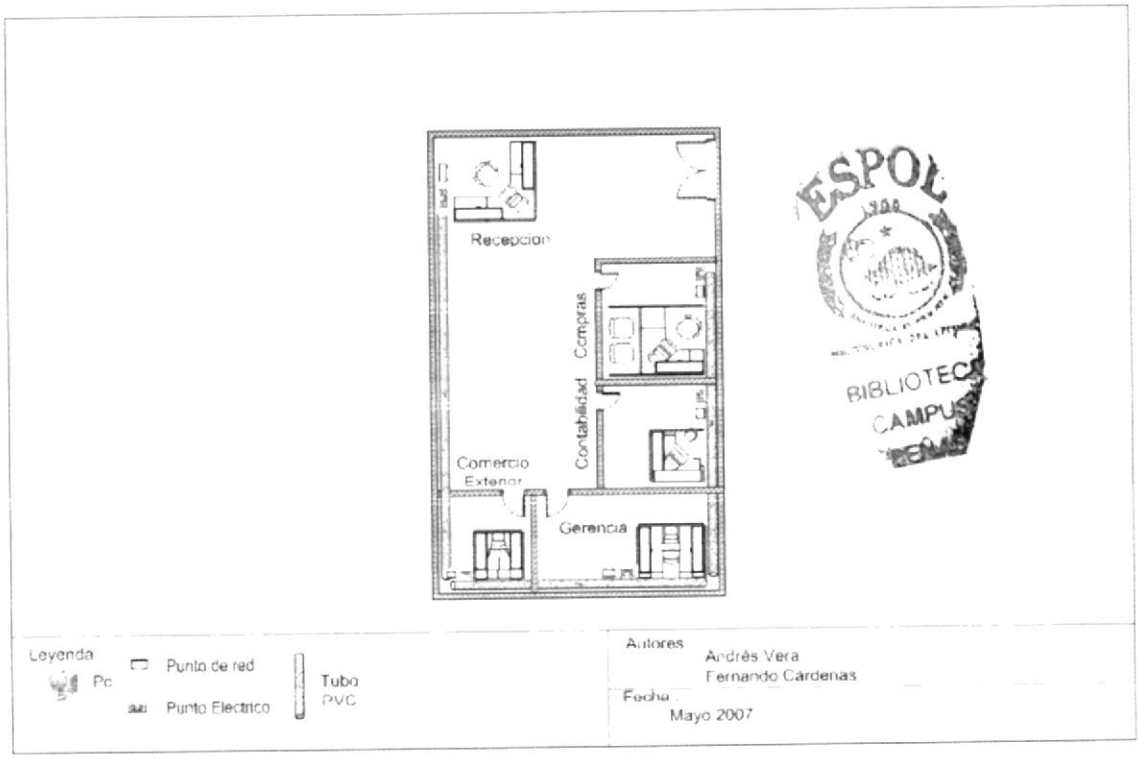


Figura 2-11: Análisis de Piso Aplicativo Sucursal Ambato

2.3.7.4. SUCURSAL DIBSA



ESPOL
BIBLIOTECA
CAMPUS

Figura 2-12: Análisis de Piso Aplicativo Sucursal Dibsa

2.3.7.5. SUCURSAL REYVENTAS

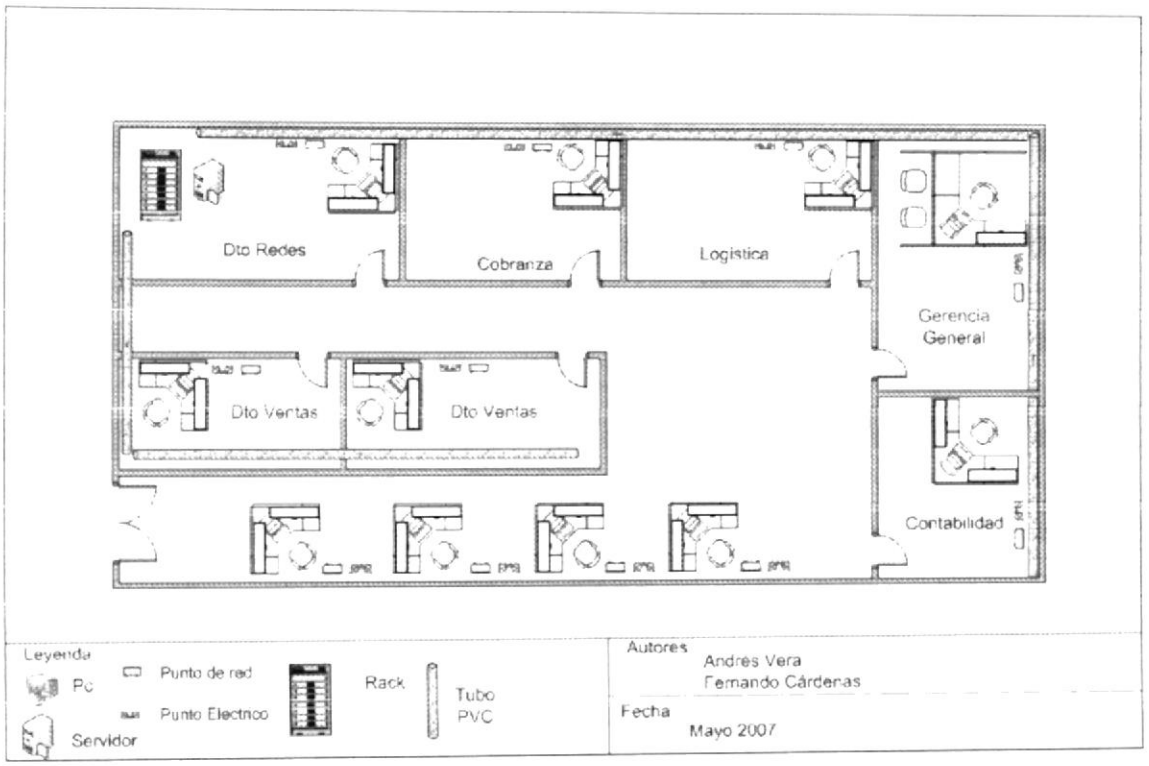


Figura 2-13: Análisis de Piso Aplicativo de Sucursal Reyventas

2.3.8. ANÁLISIS DE PISO LÓGICO

2.3.8.1. MATRIZ

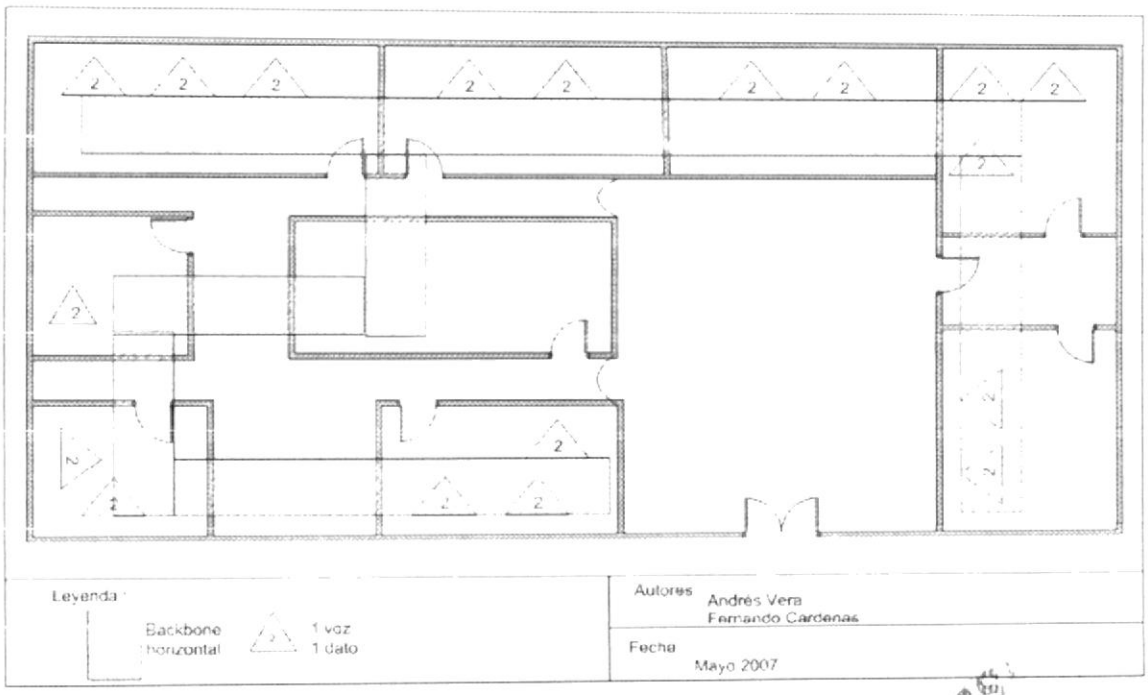


Figura 2-14: Análisis de Piso Lógico Matriz

2.3.8.2. SUCURSAL QUITO

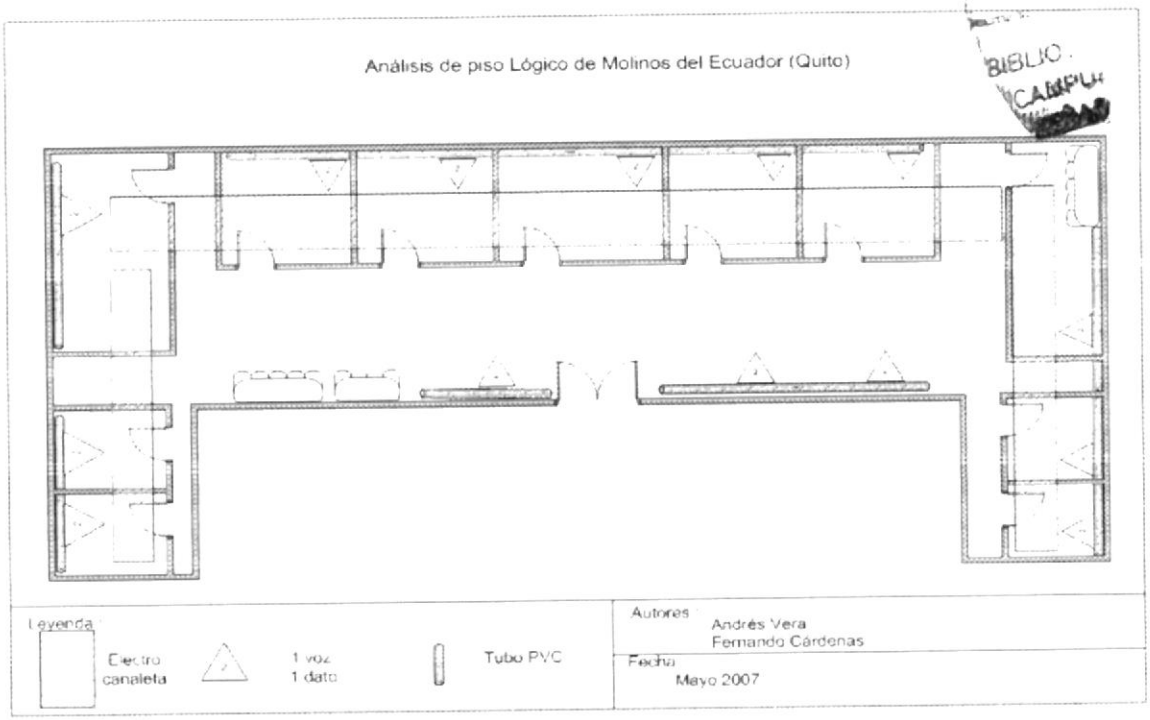


Figura 2-15: Análisis de Piso Lógico Sucursal Quito

2.3.8.3. SUCURSAL AMBATO

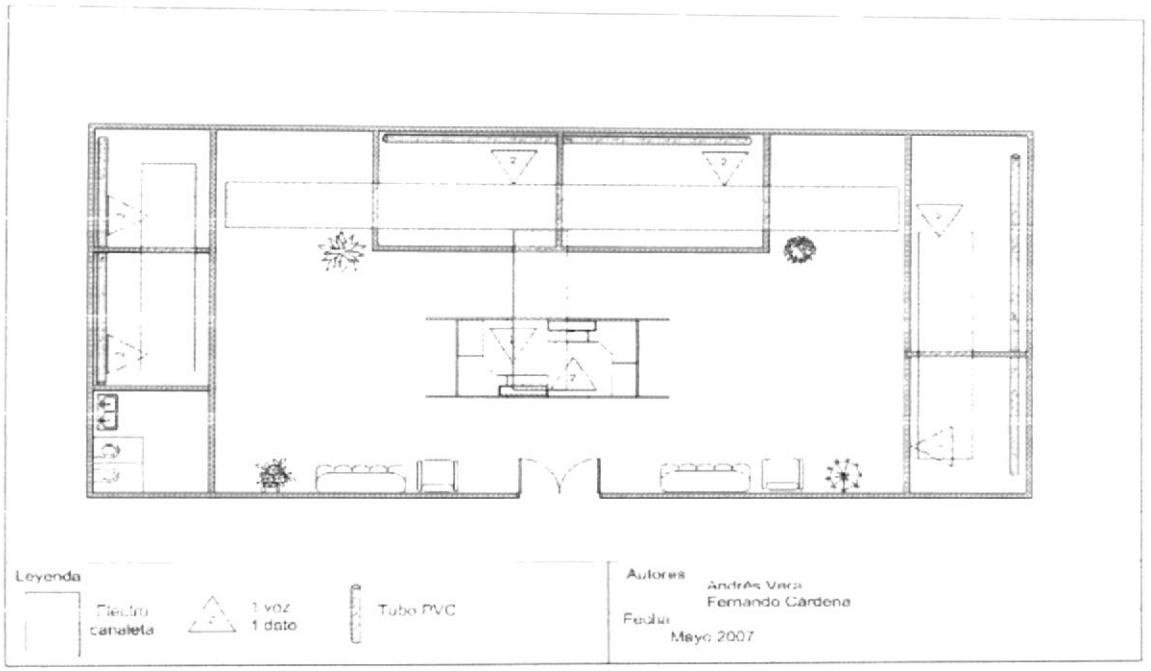


Figura 2-16: Análisis de Piso Lógico Sucursal Ambato

2.3.8.4. SUCURSAL DIBSA

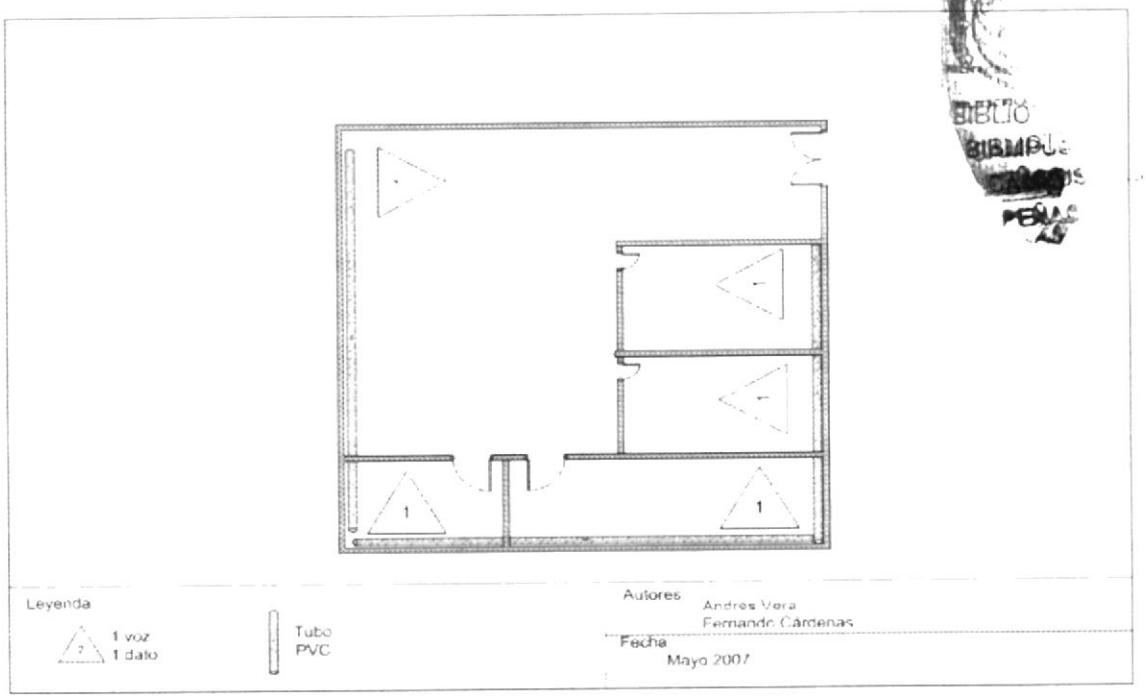


Figura 2-17: Análisis de Piso Lógico de Sucursal Dibsa

2.3.8.5. SUCURSAL REYVENTAS

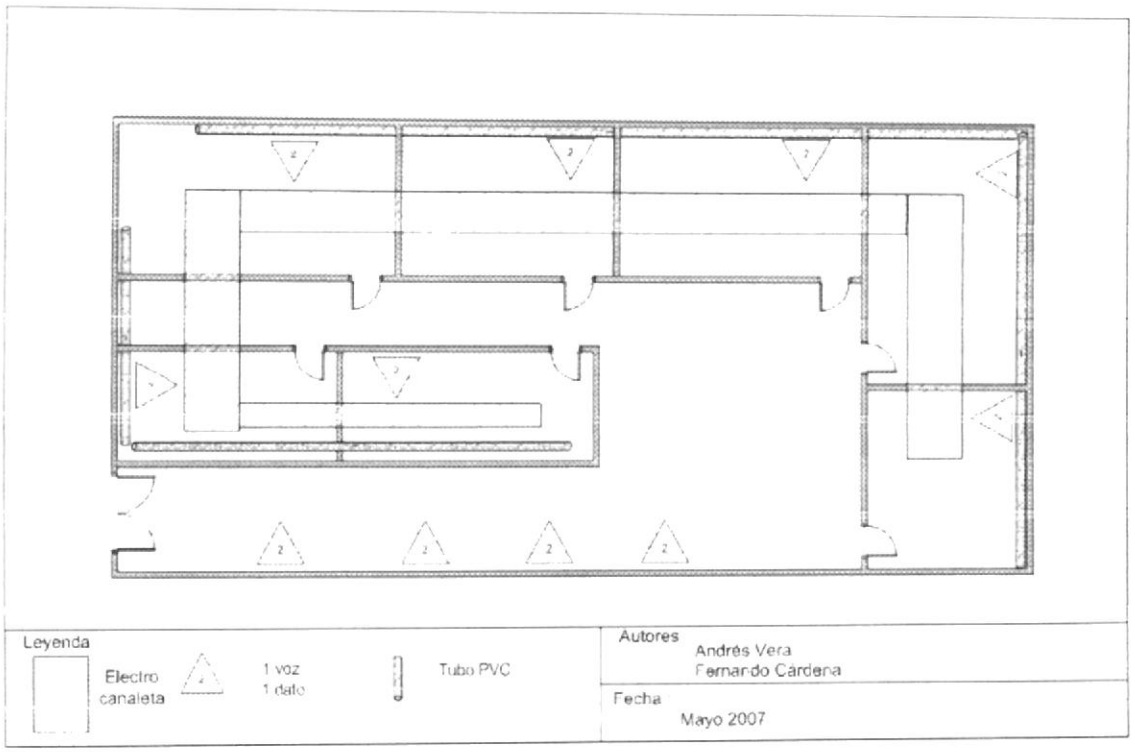


Figura 2-18: Análisis de Piso Lógico de Sucursal Reyventas

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.3.9. GRÁFICOS DEL MC

2.3.9.1. MC MATRIZ

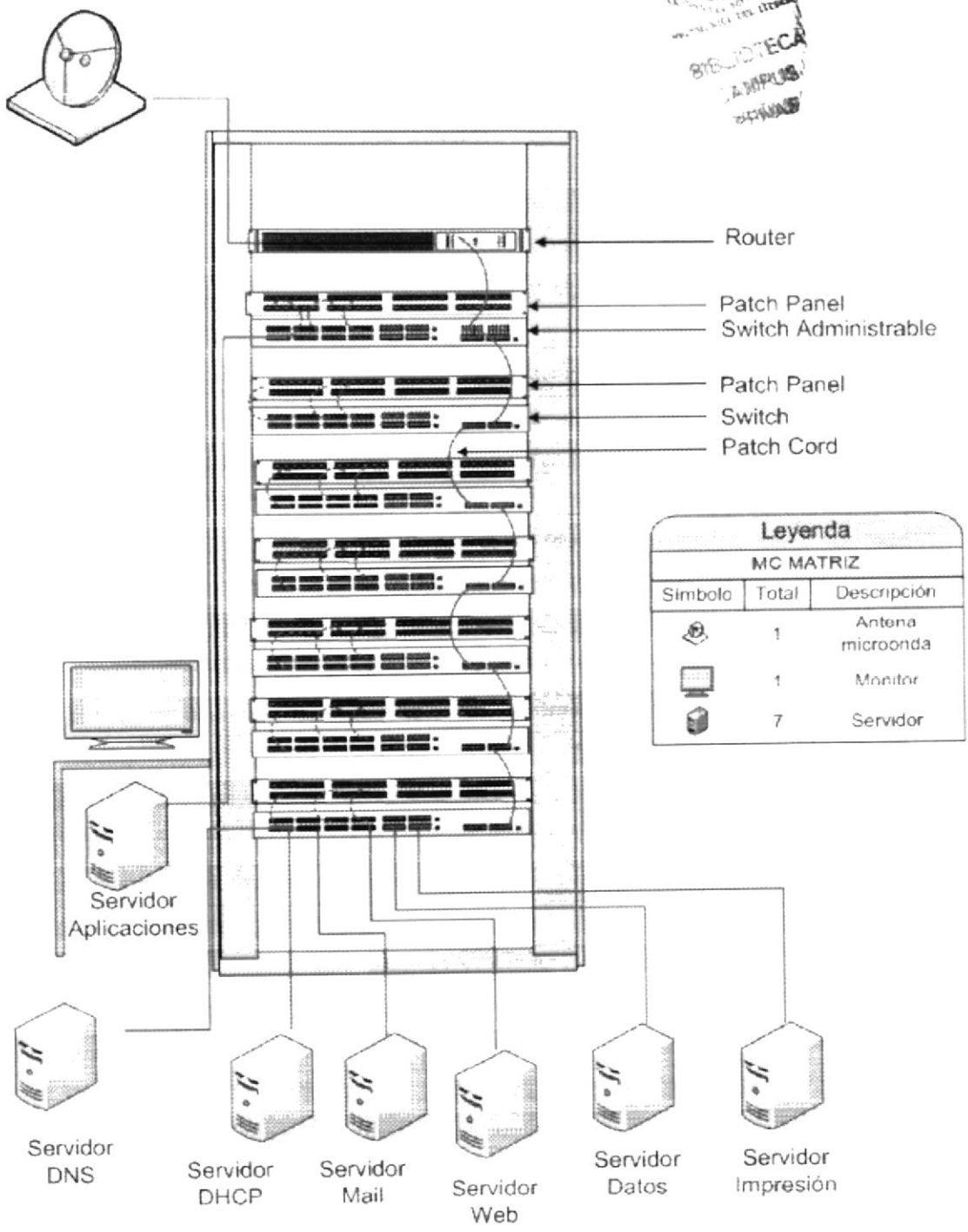
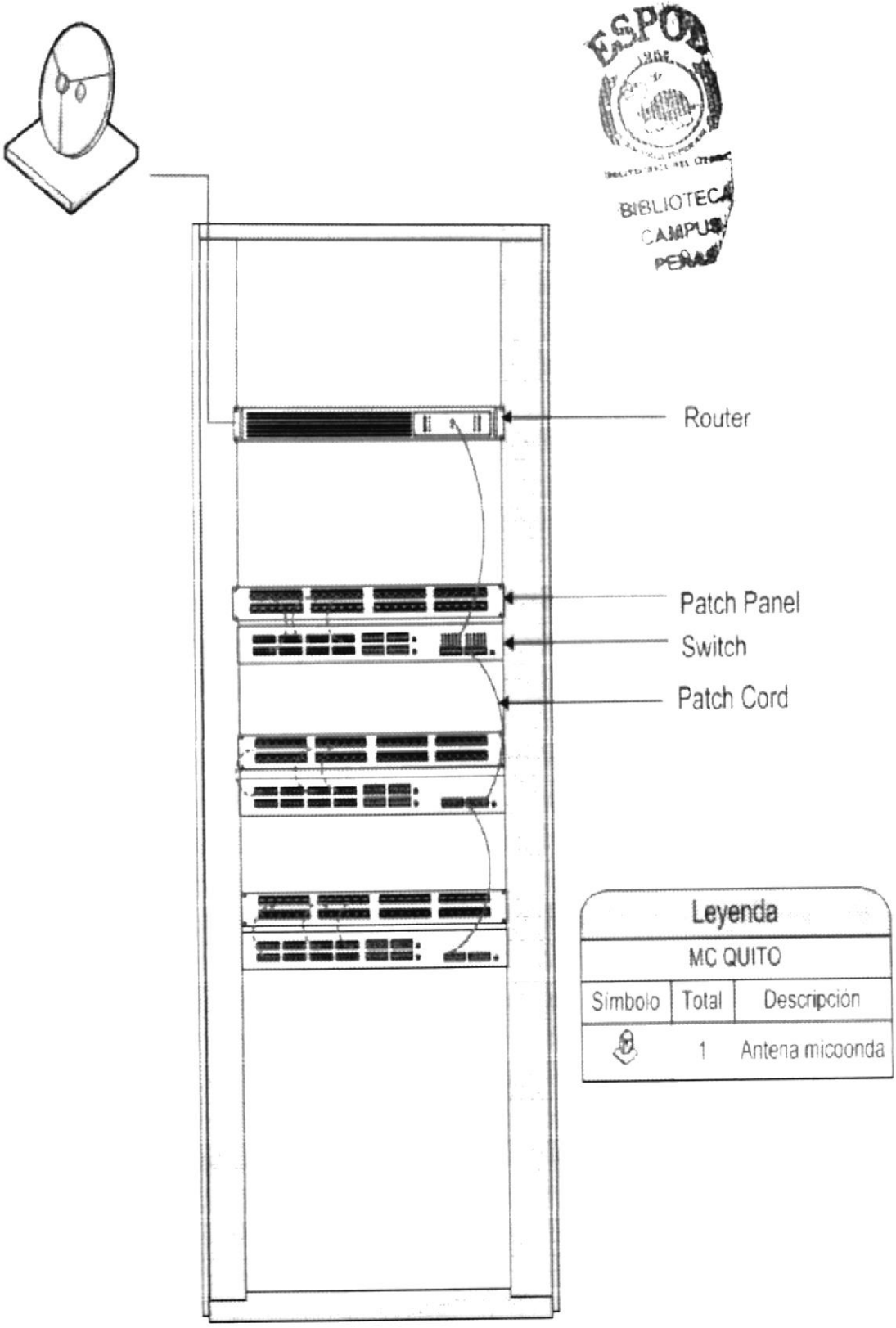


Figura 2-19: MC Principal Matriz

2.3.9.2. MC QUITO



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 2-20: MC Quito

2.3.9.3. MC AMBATO

ESPOL
BIBLIOTECA
CAMPUS

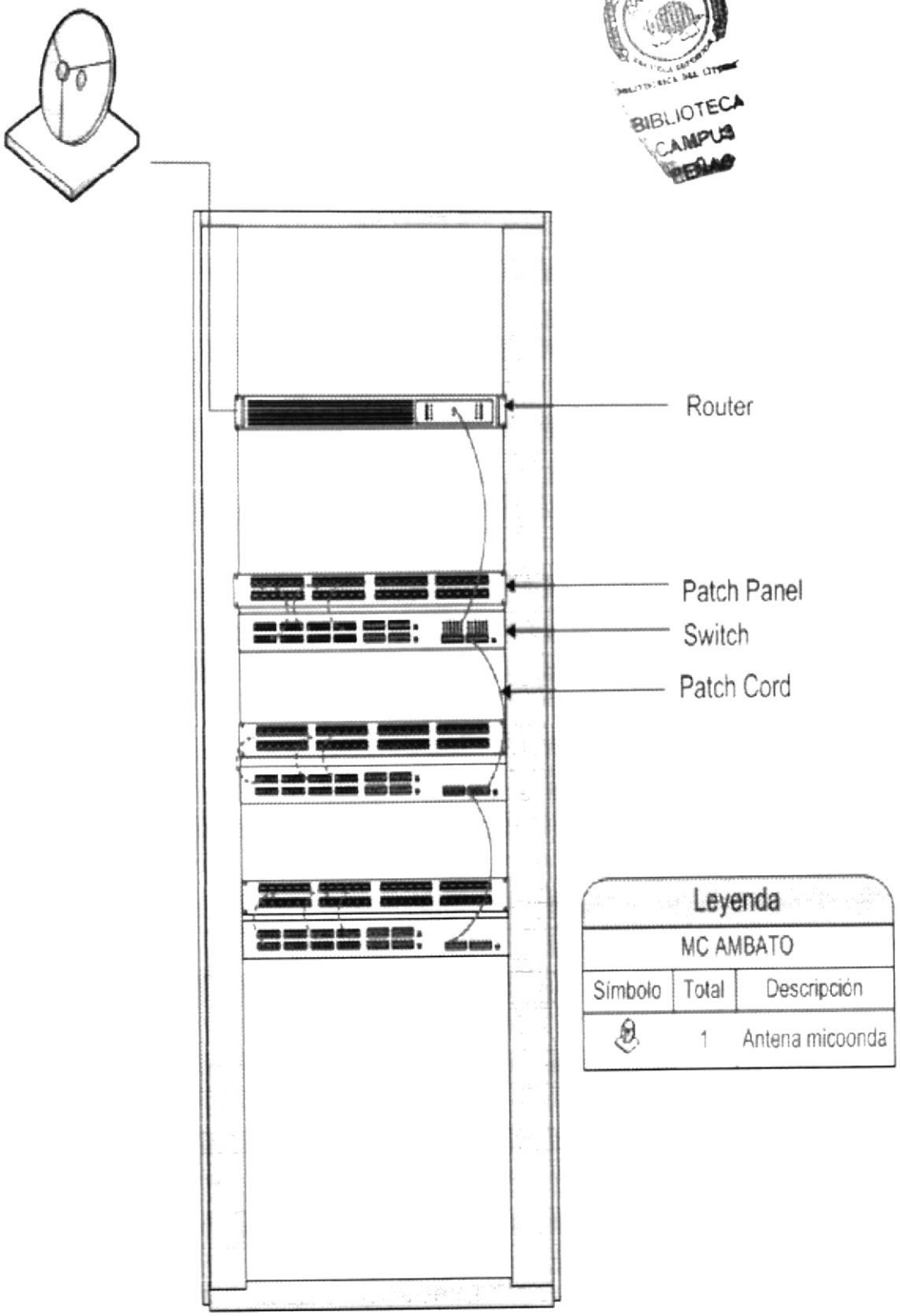


Figura 2-21: MC Ambato

2.3.9.4. MC REYVENTAS

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

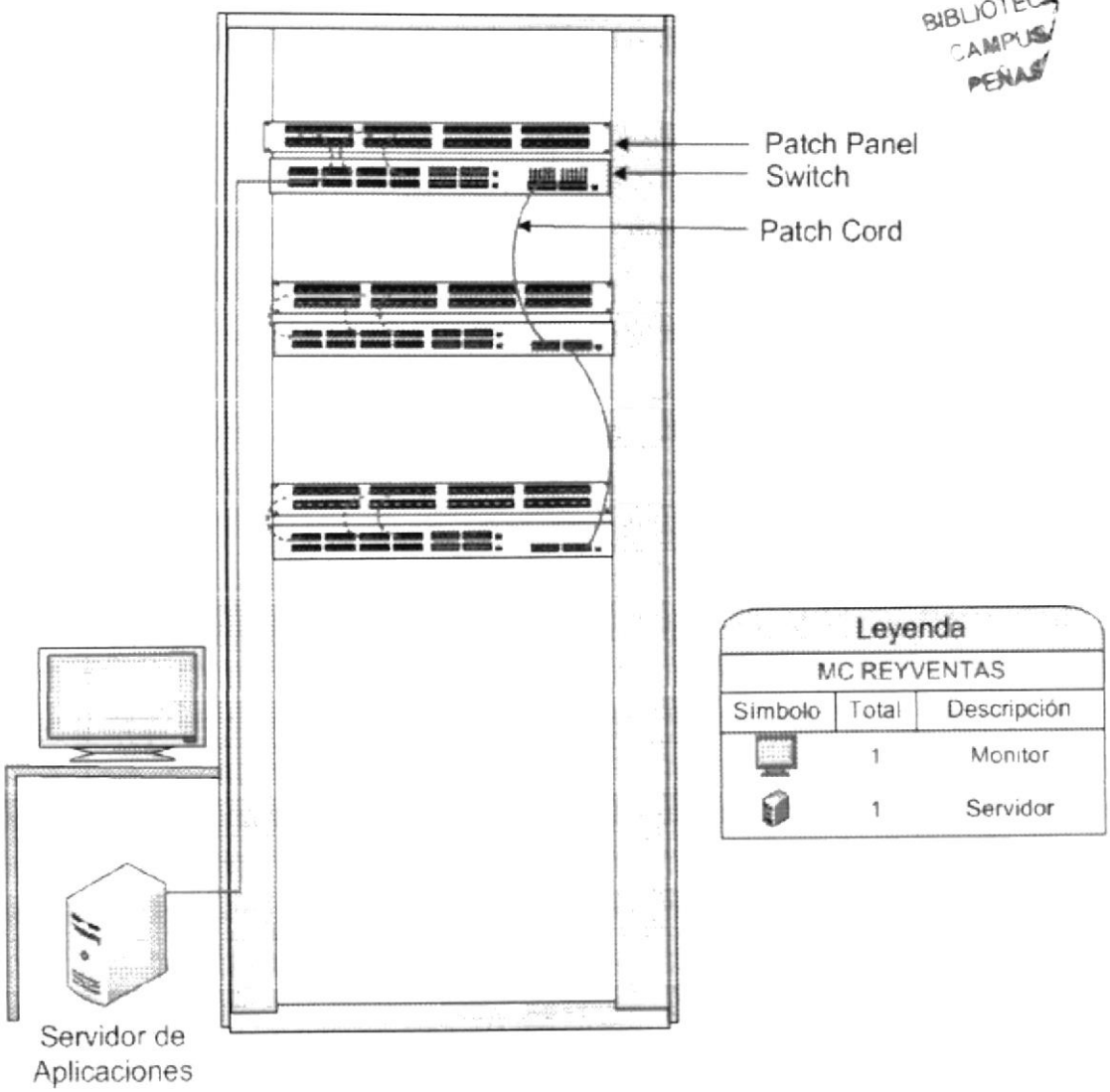


Figura 2-22: MC Reyventas

2.3.10. DISPOSITIVOS DE CONMUTACIÓN

2.3.10.1. MATRIZ, SUCURSALES QUITO Y AMBATO.

Cantidad	Características	Ubicación
16	• 3Com 4400. • Velocidad 10/100 Mbps. • Conexiones de alta velocidad • 24 x red - Ethernet – Stack • TX/10Base - TX/100 Base - RJ-45	Departamento De Sistemas

Tabla 2-6: Dispositivos de Conmutación (Matriz-Quito-Ambato).



2.4. INFRAESTRUCTURA WAN

2.4.1. DISPOSITIVOS DE ENRUTAMIENTO.

2.4.1.1. CARACTERÍSTICAS ROUTER CISCO 2500 (Quito)



Figura 2-23: Router Cisco 2500

- Mínimo de MB 8 de la memoria de destello.
- Posee dos tipos de memoria primario y compartido (paquete).

2.4.1.2. CARACTERÍSTICAS ROUTER CISCO 2600 (MATRIZ)



Figura 2-24: Router Cisco 2600

ESPOL BIBLIOTECA CAMPUS PEÑAS

- 10/100 Ethernet autosensing de Mbps.
- Token ring y Ethernet mezclados.
- Dial de soporte portuario auxiliar 115Kbps.
- Voz de Multiservice/datos/integración del fax.
- Servicios análogos y de Digital del dial.
- Acceso de la red (VPN) y protección privados virtuales del cortafuego.
- Concentración serial del dispositivo.
- Servicios WAN mezclados Servicios LAN-a-LAN.

2.4.1.3. CARACTERÍSTICAS ROUTER CISCO 1700 (Ambato)

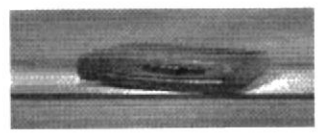


Figura 2-25: Router Cisco 1700

- Rápido, fiable y seguro acceso a Internet y a redes remotas a través de diferentes tecnologías de acceso WAN de alta velocidad.
- "Firewall", túneles VPN y detección de intrusos o "IDS".
- También proporcionan una vía de acceso a servicios como la Voz por IP o "Voice-over-IP" y telefónica IP a través de la convergencia de las redes de voz y datos.

2.4.2. ENLACE PRINCIPAL DE MOLINOS DEL ECUADOR

La comunicación entre la matriz y sus sucursales se da mediante el enlace de microonda de 2.4 Ghz.

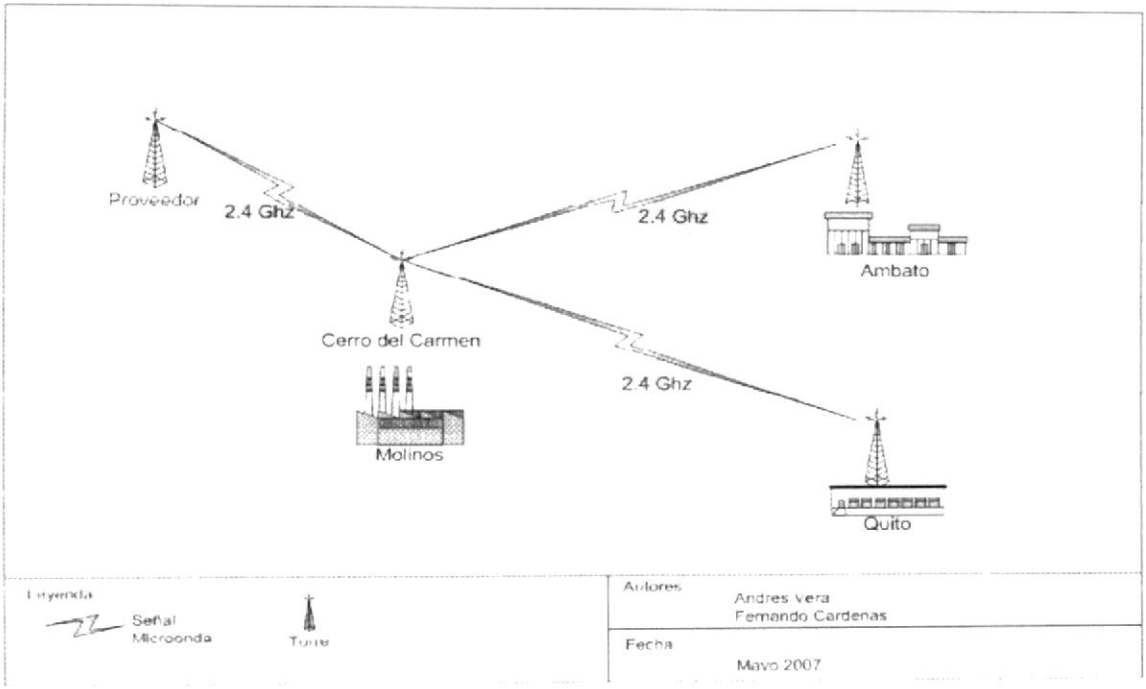


Figura 2-26: Enlace Principal de Molinos

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.5. SEGURIDADES

Esta empresa también posee un sistema de seguridad (Pix Firewall).

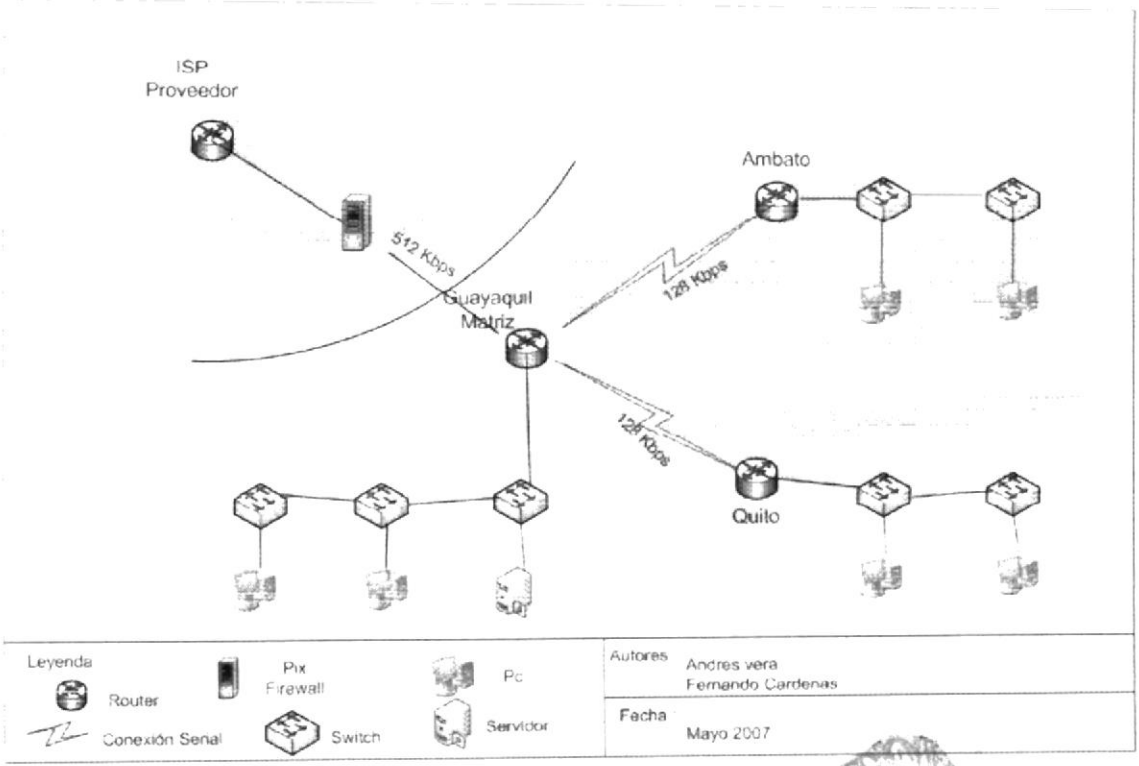


Figura 2-27: Seguridades

2.5.1. CARACTERÍSTICAS DEL FIREWALL

DISPOSITIVO	MODELO	CARACTERÍSTICAS	UBICACIÓN
Firewall Cisco	Pix 501	• Autentica a los usuarios utilizando Ftp, Telnet, o http. • Conector consola RJ-45. • Ethernet 10Base-T/10-100. • Puerto ethernet.	Matriz

Tabla 2-7: Características del Firewall

2.6. RECEPCIÓN DE INTERNET

La Empresa cuenta con un ISP (Proveedor de servicio de Internet) **Impsat** el cual es el encargado de brindar el servicio de Internet, tanto en la matriz como en sus sucursales, el mismo que recibe un ancho de banda de 512 Kbps el cual se distribuye 128 Kbps para la sucursal de Quito y Ambato.

Es importante señalar que tanto el router con el firewall frontera son propios de ISP.

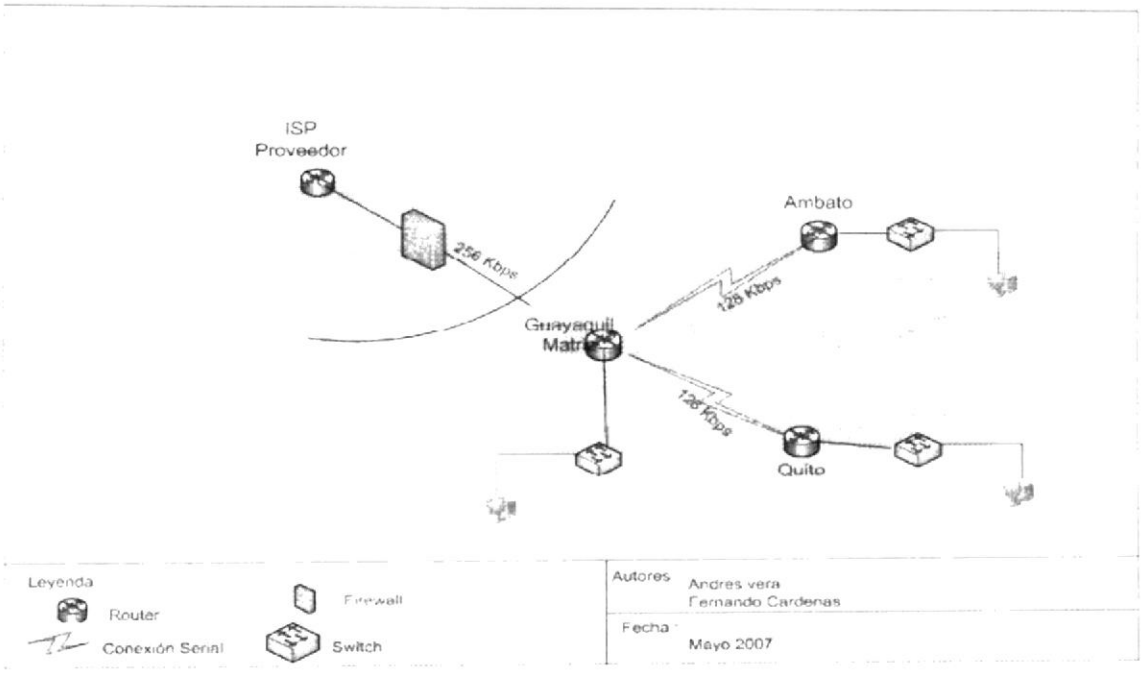


Figura 2-28: Recepción de Internet

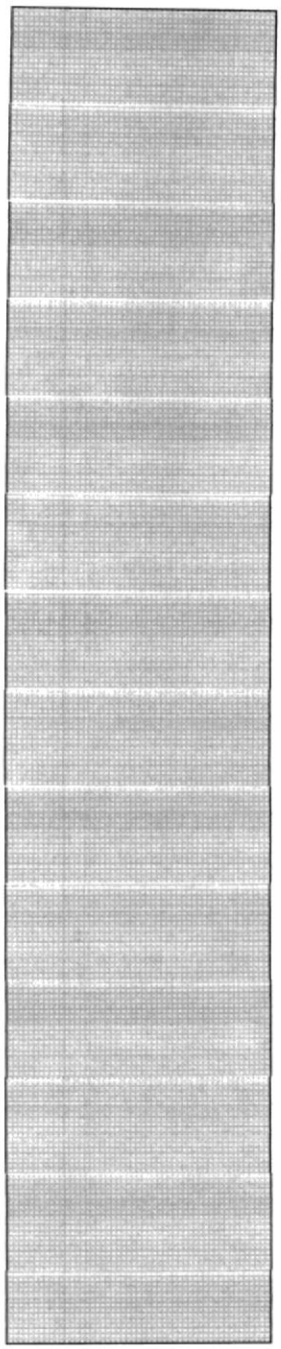
ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

2.7. PROBLEMAS ENCONTRADOS

En Molinos del Ecuador, Dibsa y Reyventas se realizó un estudio completo y minucioso del Cableado Estructurado en todas las áreas de trabajo de las mismas, se encontraron algunas anomalías las cuales se presentan en el siguiente cuadro:

- Documentación de la red no esta actualizada en el rack principal de Molinos.
- Cable UTP Cat5 expuesto a la visión publica en ciertas áreas en Molinos.
- No existe comunicación entre Molinos del Ecuador, Reyventas y Dibsa.
- La sucursal Dibsa no posee una comunicación interna entre usuarios.
- No existe comunicación entre Molinos y el Departamento de Bodega.
- En Reyventas el backbone principal no cubre todos los departamentos.





ESPOL
BIBLIOTECA
CAMPUS



CAPÍTULO 3
SOLUCIÓN PROPUESTA

3. SOLUCIÓN PROPUESTA

3.1. PROBLEMAS ENCONTRADOS

PROBLEMA	CAUSA	EFECTO
➢ No cumple con las normas y estándares de cableado estructurado interno en la Matriz.	➢ Falta de cableado backbon intra-edificio. ➢ Documentación no etiquetada por falta de tiempo. ➢ Red no etiquetada en el MC de Matriz.	➢ Dificultad para encontrar un punto deshabilitado de red.
➢ No existe comunicación de la Matriz con sus sucursales a nivel MAN.	➢ Falta de Presupuesto	➢ Gastos excesivos en materiales de oficina.
➢ Congestionamiento de la red interna LAN en ReyVentas.	➢ Red no segmentada. ➢ Existencia de Broadcast en la red Lan.	➢ Lentitud en la red tiempo de respuesta altos en los usuarios.
➢ La sucursal Dibsa no posee comunicación interna entre usuarios.	➢ Falta de implementación Lan en la sucursal Dibsa	➢ No existe comunicación entre usuarios.

TABLA 3-1: Problemas Encontrados

ESPOL BIBLIOTECA CAMPUS PEÑAS

3.2. SOLUCIÓN PROPUESTA

PROBLEMA	SOLUCIÓN	ALCANCE
➢ No cumple con las normas y estándares de cableado estructurado interno en la Matriz. ➢ Red no etiquetada en el MC de Matriz	➢ Implementar normativas de cableado estructurado en matriz.	➢ Rápida localización al usuario que se encuentre conectado a la red.
➢ No existe comunicación de la Matriz con sus sucursales a nivel MAN.	➢ Implementar fibra óptica y dispositivos de conmutación a nivel MAN en la Molinos y Reyventas.	➢ Optimización de materiales de oficina.
➢ Congestionamiento de la red interna LAN en ReyVentas	➢ Creación de Vlan. ➢ Reemplazar el cable UTP con Cat 6.	➢ Eliminación de Broadcast y mejoramiento de la transmisión de datos en la red interna de ReyVentas.
➢ La sucursal Dibsa no posee comunicación interna entre usuarios.	➢ Adquirir un IC. ➢ Implementar cableado estructurado. ➢ Adquirir dispositivos de conmutación (switch).	➢ Comunicación interna entre los departamentos

TABLA 3-2: Solución Propuesta

ESPOL BIBLIOTECA CAMPUS PEÑAS

3.3. ESTUDIO DE FACTIBILIDAD

3.3.1. ALTERNATIVA "A"

Esta alternativa abarca las mejoras a nivel de cableado estructurado para fortalecer la infraestructura a nivel LAN y MAN invirtiendo en medios de comunicación y dispositivos de conmutación, lo cual permitirá una mejora en la transmisión de datos y por tanto beneficiara el crecimiento de la empresa, para esto se debe:

- Reemplazar el cableado horizontal de categoría 5a a categoría 6 en Molinos, ReyVentas y Dibsa.
- Implementar un (1) switch administrable en ReyVentas y Dibsa para la distribución de salida de telecomunicaciones.
- Implementar IC en Dibsa.

3.3.1.1. FACTIBILIDAD TÉCNICA

3.3.1.1.1. DISPOSITIVOS DE CONMUTACIÓN.

Cantidad	Descripción	Características	Ubicación
2	Switch 3Com	Tecnología Snack administrable 24 puertos 10/100/1000	ReyVentas Dibsa

Tabla 3-3: Dispositivos de conmutación

3.3.1.1.2. MATERIALES DE CABLEADO ESTRUCTURADO

Cantidad	Descripción
3	Organizadores horizontales
10	Electrocanaletas
10	Cajas de cables UTP cat. 6
1	Gabinete de almacenamiento - Fuente redundante
1	Fibra óptica Monomodo núcleo 8,3/125 m (250 mts) de 6 hilos
2	Plato para fibra 4 pares (Unicom)
2	Transiver
2	Patch Panel / 24 Puertos Cat-6
20	Codos Plásticos Decorativas 90°
25	Amarras Plásticas
30	Cajas Plásticas Sobrepuestas
250	Face Plate 2 servicios – sin jack
30	Patch Cord Categoría 6
250	Jack Cat 6
250	Conectores RJ-45 Cat6
6	Canaletas decorativas
10	Canaleta plasticas ranurada
5	Paquetes de adecibos

ESPOL BIBLIOTECA CAMPUS PEÑAS

Tabla 3-4: Materiales de Cableado Estructurado

3.3.1.2. FACTIBILIDAD OPERATIVA

Cantidad	Actividad	Semanas
1 1	**Fase de análisis de la red LAN y MAN** • Ingeniero en Telecomunicaciones • Técnico en redes	3
1	**Fase de diseño de la red LAN y MAN** • Ingeniero en Telecomunicaciones	2
1 3	**Fase de Implementación LAN y MAN** • Ingeniero en telecomunicaciones • Técnico en redes	5 5
1 1	**Fase de Prueba LAN y MAN** • Ingeniero en telecomunicaciones • Técnico en redes	2 2
1 1	**Fase de Documentación LAN y MAN** • Ingeniero en telecomunicaciones • Técnico en redes	2 2

Tabla 3-5: Factibilidad Operativa

ESPOL BIBLIOTECA CAMPUS PEÑAS

3.3.1.3. FACTIBILIDAD ECONÓMICA

Descripción	Cantidad	Total
Organizadores horizontales	3	$ 135,00
Electrocanaletas	10	$ 300,00
Cajas de cables UTP cat. 6	10	$ 1.525,00
Switch administrable - Stack	2	$ 1.719,20
Gabinete de almacenamiento -	1	$ 1.200,00
Rollo de fibra óptica Monomodo	1	$ 495,00
Plato para fibra 4 pares (Unicom)	2	$ 260,00
Transiver	2	$ 307,00
Patch Panel / 24 Puertos Cat-6	2	$ 60,00
Codos Plásticos Decorativas 90°	20	$ 8,00
Amarras Plásticas	25	$ 67,50
Cajas Plásticas Sobrepuestas	30	$ 45,00
Face Plate 2 servicios – sin jack	250	$ 1.412,50
Patch Cord Categoría 6	30	$ 45,00
Jack Cat 6	250	$ 450,00
Conectores RJ-45 Cat6	250	$ 22,50
Canaletas decorativas	6	$ 37,50
Canaleta plasticas ranurada	10	$ 45,00
Paquetes de adhesivos	5	$ 25,00
	Total	**$ 8.159,20**

Tabla 3-6: Factibilidad Económica

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

3.3.1.4. COSTO OPERATIVO

Cant	Actividad	Sem.	Costos	Total
	Fase de diseño de la red LAN y MAN			
1	• Ingeniero en Telecomunicaciones	2	$ 200,oo	$ 400,oo
1	• Técnico en redes		$ 180,oo	$ 360,oo
	Fase de Implementación LAN y MAN			
1	• Ingeniero en telecomunicaciones	5	$ 220,oo	$ 1.100,oo
3	• Técnico en redes	5	$ 180,oo	$ 2.700,oo
	Fase de Prueba LAN y MAN			
1	• Ingeniero en telecomunicaciones	2	$ 200,oo	$ 400,oo
1	• Técnico en redes	2	$150,oo	$ 300,oo
	Fase de Documentación LAN y MAN			
1	• Ingeniero en telecomunicaciones	2	$ 200,oo	$ 400,oo
1	• Técnico en redes	2	$ 180,oo	$ 360.oo
			TOTAL	**$ 6.020,oo**

ESPOL BIBLIOTECA CAMPUS PEÑAS

Tabla 3-7: Costo Operativo

3.3.1.5. COSTO TOTAL DE PROPUESTA ALTERNATIVA "A"

Descripción	Total
Servicios profesionales	$ 6.020,00
Costo del hardware	$ 8.159,20
SUB-TOTAL	$ 14.179,20
IVA	$ 1.701,50
TOTAL	**$ 15.880,24**

Tabla 3-8: Costo Total de Propuesta Alternativa "A"

3.3.1.6. VENTAJAS

- Dispositivos que ofrecen la seguridad de sus datos.
- Mejora el tiempo de respuesta entre la comunicación de los usuarios.
- Optimización de enlaces de datos utilizando calidad de servicio.
- Mayor eficiencia, productividad y seguridad en la red.
- Los procesos se efectuarán de forma eficiente.
- Bajo Costo en Soporte Técnico.
- Mayor Soporte al Usuario.
- Mejorar el tráfico de la Red Lan.



3.3.1.7. BENEFICIOS

- Actualización en los procesos entre la matriz y sus sucursales.
- Comunicación en línea con las sucursales de Reyventas y Dibsa.
- Comunicación rápida y segura mediante dispositivos de última generación.

3.3.1.8. CONDICIONES COMERCIALES

3.3.1.8.1. FORMA DE PAGO

A continuación se detalla la forma de pago establecida:

- 60% A la firma del contrato.
- 20% Cuando comience la fase de Implementación Lan y Man (01 de Agosto del 2007).
- 20% una vez que la fase de prueba haya culminado.

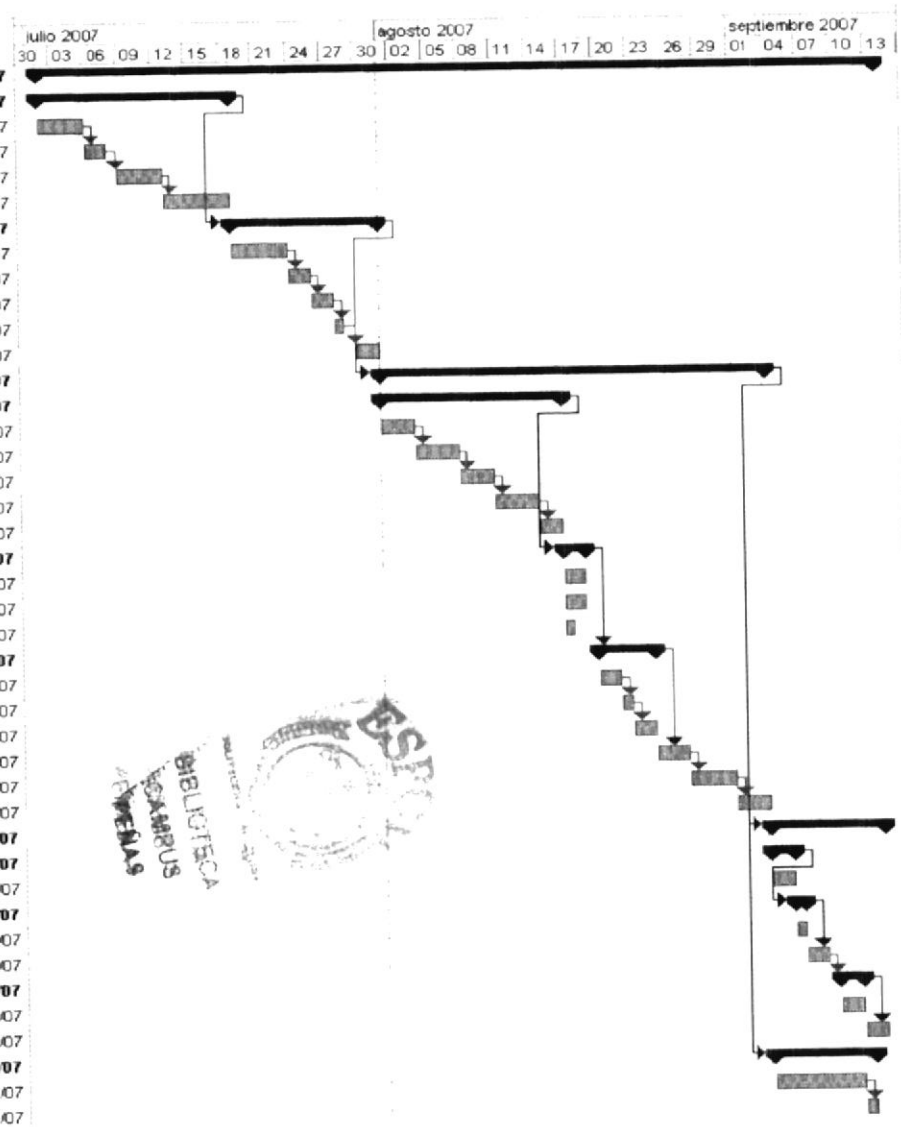
Duración del contrato: 11 semanas.

3.3.1.9. GARANTÍAS DE LA ALTERNATIVA "A"

- Soporte técnico por 3 meses en las configuraciones de los dispositivos.
- Garantía por 8 meses a los dispositivos de conmutación por parte de la empresa vendedora.
- Cabe indicar que todos nuestros servicios tanto de instalación del cableado estructurado como de configuración de dispositivos, le garantizamos un buen trabajo profesional, proyectando una garantía de 5 meses sin costo alguno.

3.3.1.10. DIAGRAMA DE GANT

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**TIEMPO DEL PROYECTO**	**64 días**	**lun 02/07/07**	**jue 13/09/07**
2	**FASE DE ANÁLISIS DE LA RED LAN Y MAN**	**15 días**	**lun 02/07/07**	**mié 18/07/07**
3	Estudio Lan y Man	4 días	lun 02/07/07	jue 05/07/07
4	Cotización de equipos y materiales	2 días	vie 06/07/07	sáb 07/07/07
5	Elaboración de la propuesta	4 días	lun 09/07/07	jue 12/07/07
6	Aceptación de la propuesta	5 días	vie 13/07/07	mié 18/07/07
7	**FASE DE DISEÑO LAN Y MAN**	**11 días**	**jue 19/07/07**	**mar 31/07/07**
8	Análisis de piso aplicativo de Molinos	4 días	jue 19/07/07	lun 23/07/07
9	Análisis de piso aplicativo de Dibsa	2 días	mar 24/07/07	mié 25/07/07
10	Análisis de piso aplicativo de ReyVentas	2 días	jue 26/07/07	vie 27/07/07
11	Compras de equipos de conmutación	1 día	sáb 28/07/07	sáb 28/07/07
12	Revisión de dispositivos	2 días	lun 30/07/07	mar 31/07/07
13	**IMPLEMENTACIÓN LAN Y MAN**	**29 días**	**mié 01/08/07**	**lun 03/09/07**
14	**Instalación del cableado de Molinos**	**14 días**	**mié 01/08/07**	**jue 16/08/07**
15	Dpto. de Sistema	3 días	mié 01/08/07	vie 03/08/07
16	Dpto. de Ventas	3 días	sáb 04/08/07	mar 07/08/07
17	Dpto. de RRHH	3 días	mié 08/08/07	vie 10/08/07
18	Dpto. de Contabilidad	3 días	sáb 11/08/07	mar 14/08/07
19	Dpto. de Marketing	2 días	mié 15/08/07	jue 16/08/07
20	**Instalación del cableado de Dibsa**	**2 días**	**vie 17/08/07**	**sáb 18/08/07**
21	Dpto. de Compras	2 días	vie 17/08/07	sáb 18/08/07
22	Dpto. de Comercio Exterio	2 días	vie 17/08/07	sáb 18/08/07
23	Contador	1 día	vie 17/08/07	vie 17/08/07
24	**Instalación del cableado de ReyVen**	**5 días**	**lun 20/08/07**	**vie 24/08/07**
25	Dpto. Tributario	2 días	lun 20/08/07	mar 21/08/07
26	Contador	1 día	mié 22/08/07	mié 22/08/07
27	Dpto de Crédito	2 días	jue 23/08/07	vie 24/08/07
28	Instalación del IC en Dibsa	2 días	sáb 25/08/07	lun 27/08/07
29	Instalación de fibra óptica	4 días	mar 28/08/07	vie 31/08/07
30	Configuración de vlan´s	2 días	sáb 01/09/07	lun 03/09/07
31	**FASE DE PRUEBA**	**9 días**	**mar 04/09/07**	**jue 13/09/07**
32	**Prueba de conexión de Molinos**	**2 días**	**mar 04/09/07**	**mié 05/09/07**
33	Prueba de comunicación entre depa	2 días	mar 04/09/07	mié 05/09/07
34	**Prueba de conexión de Dibsa**	**1 día**	**jue 06/09/07**	**jue 06/09/07**
35	Prueba de comunicación entre depa	1 día	jue 06/09/07	jue 06/09/07
36	Prueba de conexión de fibra óptica	2 días	vie 07/09/07	sáb 08/09/07
37	**Prueba de conexión de ReyVentas**	**2 días**	**lun 10/09/07**	**mar 11/09/07**
38	Prueba de comunicación entre depa	2 días	lun 10/09/07	mar 11/09/07
39	Prueba de vlan´s	2 días	mié 12/09/07	jue 13/09/07
40	**FASE DE DOCUMENTACIÓN**	**8 días**	**mar 04/09/07**	**mié 12/09/07**
41	Elaboración del manual de recl Lan y Mar	7 días	mar 04/09/07	mar 11/09/07
42	Entrega del manual de Usuario	1 día	mié 12/09/07	mié 12/09/07



BIBLIOTECA
ESPOL

3.3.2. ALTERNATIVA "B"

Esta alternativa abarca las mejoras a nivel de cableado estructurado para fortalecer la infraestructura a nivel LAN y MAN invirtiendo en medios de comunicación y dispositivos de conmutación, lo cual permitirá una mejora en la transmisión de datos y por tanto beneficiara el crecimiento de la empresa, para esto se debe:

- Reemplazar el cableado horizontal de categoría 5a a categoría 6 en Molinos, ReyVentas y Dibsa.
- Implementar un 1 switch administrable en ReyVentas y Dibsa para la distribución de salida de telecomunicaciones.
- Implementar un IC en Dibsa.



3.3.2.1. FACTIBILIDAD TÉCNICA

3.3.2.1.1. DISPOSITIVOS DE CONMUTACIÓN

Cantidad	Descripción	Características	Ubicación
2	Switch 3com	Tecnología Snack administrable 24 puertos 10/100/1000	ReyVentas y Dibsa

Tabla 3-9: Dispositivos de Conmutación Alternativa "B"

3.3.2.1.2. MATERIALES DE CABLEADO ESTRUCTURADO

Cantidad	Descripción
3	Organizadores horizontales
10	Electrocanaletas
10	Cajas de cables UTP cat. 6
1	Gabinete de almacenamiento - Fuente redundante
1	Fibra óptica Monomodo núcleo 8,3/125 m (250 mts) de 6 hilos
2	Plato para fibra 4 pares (Unicom)
2	Transiver
2	Patch Panel / 24 Puertos Cat-6
20	Codos Plásticos Decorativas 90°
25	Amarras Plásticas
30	Cajas Plásticas Sobrepuestas
250	Face Plate 2 servicios – sin jack
30	Patch Cord Categoría 6
250	Jack Cat 6
250	Conectores RJ-45 Cat6
6	Canaletas decorativas
10	Canaleta plasticas ranurada
5	Paquetes de adecibos

Tabla 3-10: Materiales de Cableado Estructurado Alternativa "B"

3.3.2.2. FACTIBILIDAD OPERATIVA

Cantidad	Actividad	Semanas
1 1	**Fase de análisis de la red LAN y MAN** • Ingeniero en Telecomunicaciones • Técnico de redes	3
1	**Fase de diseño LAN y MAN** • Ingeniero en Telecomunicaciones	2
1 3	**Fase de Implementación LAN y MAN** • Ingeniero en telecomunicaciones • Técnico en redes	5 5
1 1	**Fase de Prueba LAN y MAN** • Ingeniero en telecomunicaciones • Técnico en redes	2 2
1 1	**Fase de Documentación LAN y MAN** • Ingeniero en telecomunicaciones • Técnico en redes	2 2

Tabla 3-11: Factibilidad Operativa Alternativa "B"

ESPOL BIBLIOTECA CAMPUS PEÑAS

3.3.2.3. FACTIBILIDAD ECONÓMICA

Descripción	Cantidad	Total
Organizadores horizontales	3	$ 113,45
Electrocanaletas	5	$ 254,99
Cajas de cables UTP cat. 6	10	$ 1.243,21
Switch administrable - Stack	2	$ 1.119,56
Gabinete de almacenamiento - Fuente redundante	1	$ 953,69
Rollo de fibra óptica Multimodo núcleo 8,3/125	1	$ 495,00
Plato para fibra 4 pares (Unicom)	2	$ 250,00
Transiver	2	$ 300,00
Patch Panel / 24 Puertos Cat-6	2	$ 55,00
Codos Plásticos Decorativas 90°	15	$ 8,00
Amarras Plásticas	15	$ 67,00
Cajas Plásticas Sobrepuestas	20	$ 40,00
Face Plate 2 servicios – sin jack	196	$ 1.250,00
Patch Cord Categoría 6	25	$ 45,00
Jack Cat 6	196	$ 450,00
Conectores RJ-45 Cat6	196	$ 22,00
Canaletas decorativas	6	$ 37,00
Canaleta plasticas ranurada	8	$ 43,00
Paquetes de adhesivos	5	$ 22,00
	Total	**$ 6.768,90**

Tabla 3-12: Factibilidad Económica Alternativa "B"



3.3.2.4. COSTO OPERATIVA

Cant	Actividad	Sem	Costos	Total
	Fase de diseño de la red LAN y MAN			
1	• Ingeniero en Telecomunicaciones	2	$ 220,oo	$ 400,oo
1	• Técnico en redes	2	$ 180,oo	$ 360,oo
	Fase de Implementación LAN y MAN			
1	• Ingeniero en telecomunicaciones	5	220.oo	$ 1.100,oo
3	• Técnico en redes	5	$ 180.oo	$ 2.700,oo
	Fase de Prueba LAN y MAN			
1	• Ingeniero en telecomunicaciones	2	$ 200.oo	$ 400,oo
1	• Técnico en redes	2	$150,oo	$ 300,oo
	Fase de Documentación LAN y MAN			
1	• Ingeniero en telecomunicaciones	2	$ 200.oo	$ 400,oo
1	• Técnico en redes	2	$ 180,oo	$ 360.oo
			TOTAL	**$ 5.020,oo**

ESPOL BIBLIOTECA CAMPUS PEÑAS

Tabla 3-13: Costo Operativa Alternativa "B"

3.3.2.5. COSTO TOTAL DE PROPUESTA ALTERNATIVA "B"

Descripción	Total
Servicio Profesionales	$ 5,020,00
Costo del hardware	$ 6.768,90
Subtotal	$ 11,788.90
IVA	$ 1,414.66
TOTAL	**$ 13.203,56**

Tabla 3-14: Costo total de Propuesta Alternativa "B"

3.3.2.6. VENTAJAS

- Dispositivos que ofrecen la seguridad de sus datos.
- Mejora el tiempo de respuesta entre la comunicación de los usuarios.
- Optimización de enlaces de datos utilizando calidad de servicio.
- Mayor eficiencia, productividad y seguridad en la red.
- Los procesos se efectuarán de forma eficiente.
- Bajo Costo en Soporte Técnico.
- Mayor Soporte al Usuario.
- Mejorar el tráfico de la Red Lan.

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

3.3.2.7. BENEFICIOS

- Actualización en los procesos entre la matriz y sus sucursales.
- Comunicación en línea con las sucursales de Reyventas y Dibsa.
- Comunicación rápida y segura mediante dispositivos de última generación.

3.3.2.8. CONDICIONES COMERCIALES

3.3.2.8.1. FORMA DE PAGO

A continuación se detalla la forma de pago establecida:

- 60% A la firma del contrato.
- 20% Cuando comience la fase de Implementación Lan y Man (01 de Agosto del 2007).
- 20% una vez que la fase de prueba haya culminado.

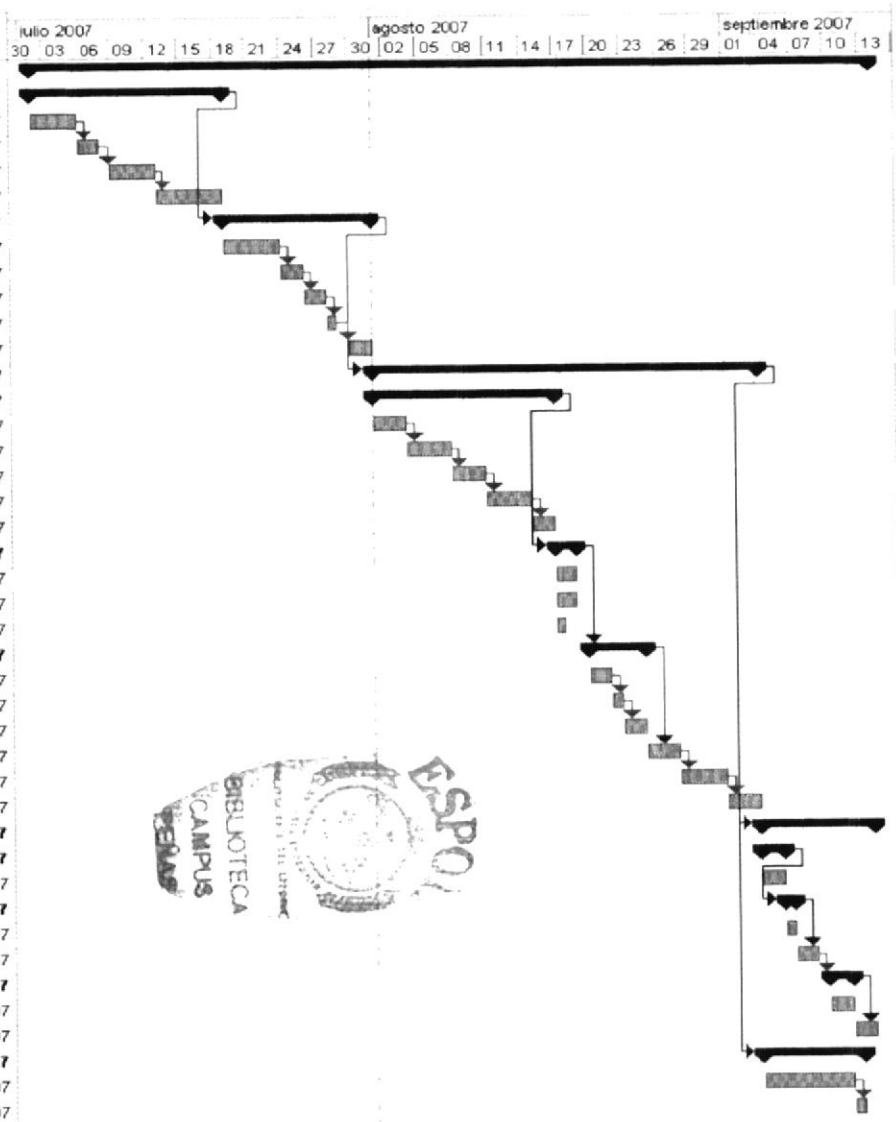
Duración del contrato: 11 semanas.

3.3.2.9. GARANTÍAS DE LA ALTERNATIVA "B"

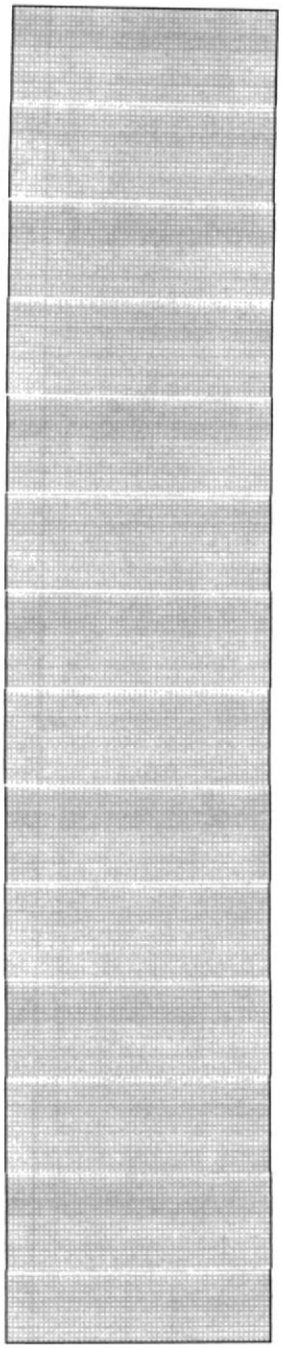
- Soporte técnico por 3 meses en las configuraciones de los dispositivos.
- Garantía por 8 meses a los dispositivos de conmutación por parte de la empresa vendedora.
- Cabe indicar que todos nuestros servicios tanto de instalación del cableado estructurado como de configuración de dispositivos, le garantizamos un buen trabajo profesional, proyectando una garantía de 5 meses sin costo alguno.

3.3.2.10. DIAGRAMA DE GANT

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**TIEMPO DEL PROYECTO**	**64 días**	**lun 02/07/07**	**jue 13/09/07**
2	**FASE DE ANÁLISIS DE LA RED LAN Y MAN**	**15 días**	**lun 02/07/07**	**mié 18/07/07**
3	Estudio Lan y Man	4 días	lun 02/07/07	jue 05/07/07
4	Cotización de equipos y materiales	2 días	vie 06/07/07	sáb 07/07/07
5	Elaboración de la propuesta	4 días	lun 09/07/07	jue 12/07/07
6	Aceptación de la propuesta	5 días	vie 13/07/07	mié 18/07/07
7	**FASE DE DISEÑO LAN Y MAN**	**11 días**	**jue 19/07/07**	**mar 31/07/07**
8	Análisis de piso aplicativo de Molinos	4 días	jue 19/07/07	lun 23/07/07
9	Análisis de piso aplicativo de Dibsa	2 días	mar 24/07/07	mié 25/07/07
10	Análisis de piso aplicativo de ReyVentas	2 días	jue 26/07/07	vie 27/07/07
11	Compras de equipos de conmutación	1 día	sáb 28/07/07	sáb 28/07/07
12	Revisión de dispostivos	2 días	lun 30/07/07	mar 31/07/07
13	**IMPLEMENTACIÓN LAN Y MAN**	**29 días**	**mié 01/08/07**	**lun 03/09/07**
14	**Instalación del cableado de Molinos**	**14 días**	**mié 01/08/07**	**jue 16/08/07**
15	Dpto. de Sistema	3 días	mié 01/08/07	vie 03/08/07
16	Dpto. de Ventas	3 días	sáb 04/08/07	mar 07/08/07
17	Dpto. de RRHH	3 días	mié 08/08/07	vie 10/08/07
18	Dpto. de Contabilidad	3 días	sáb 11/08/07	mar 14/08/07
19	Dpto. de Marketing	2 días	mié 15/08/07	jue 16/08/07
20	**Instalación del cableado de Dibsa**	**2 días**	**vie 17/08/07**	**sáb 18/08/07**
21	Dpto. de Compras	2 días	vie 17/08/07	sáb 18/08/07
22	Dpto. de Comercio Exterio	2 días	vie 17/08/07	sáb 18/08/07
23	Contador	1 día	vie 17/08/07	vie 17/08/07
24	**Instalación del cableado de ReyVen**	**5 días**	**lun 20/08/07**	**vie 24/08/07**
25	Dpto. Tributario	2 días	lun 20/08/07	mar 21/08/07
26	Contador	1 día	mié 22/08/07	mié 22/08/07
27	Dpto de Crédito	2 días	jue 23/08/07	vie 24/08/07
28	Instalación del IC en Dibsa	2 días	sáb 25/08/07	lun 27/08/07
29	Instalación de fibra óptica	4 días	mar 28/08/07	vie 31/08/07
30	Configuración de vlan's	2 días	sáb 01/09/07	lun 03/09/07
31	**FASE DE PRUEBA**	**9 días**	**mar 04/09/07**	**jue 13/09/07**
32	**Prueba de conexión de Molinos**	**2 días**	**mar 04/09/07**	**mié 05/09/07**
33	Prueba de comunicación entre depe	2 días	mar 04/09/07	mié 05/09/07
34	**Prueba de conexión de Dibsa**	**1 día**	**jue 06/09/07**	**jue 06/09/07**
35	Prueba de comunicación entre depe	1 día	jue 06/09/07	jue 06/09/07
36	Prueba de conexión de fibra óptica	2 días	vie 07/09/07	sáb 08/09/07
37	**Prueba de conexión de ReyVentas**	**2 días**	**lun 10/09/07**	**mar 11/09/07**
38	Prueba de comunicación entre depe	2 días	lun 10/09/07	mar 11/09/07
39	Prueba de vlan's	2 días	mié 12/09/07	jue 13/09/07
40	**FASE DE DOCUMENTACIÓN**	**8 días**	**mar 04/09/07**	**mié 12/09/07**
41	Elaboración del manual de recl Lan y Mar	7 días	mar 04/09/07	mar 11/09/07
42	Entrega del manual de Usuario	1 día	mié 12/09/07	mié 12/09/07



ESPOL BIBLIOTECA CAMPUS PEÑAS







CAPÍTULO 4

IMPLEMENTACIÓN WAN

4.1 ANÁLISIS DE PISO APLICATIVO

4.1.1 MATRIZ

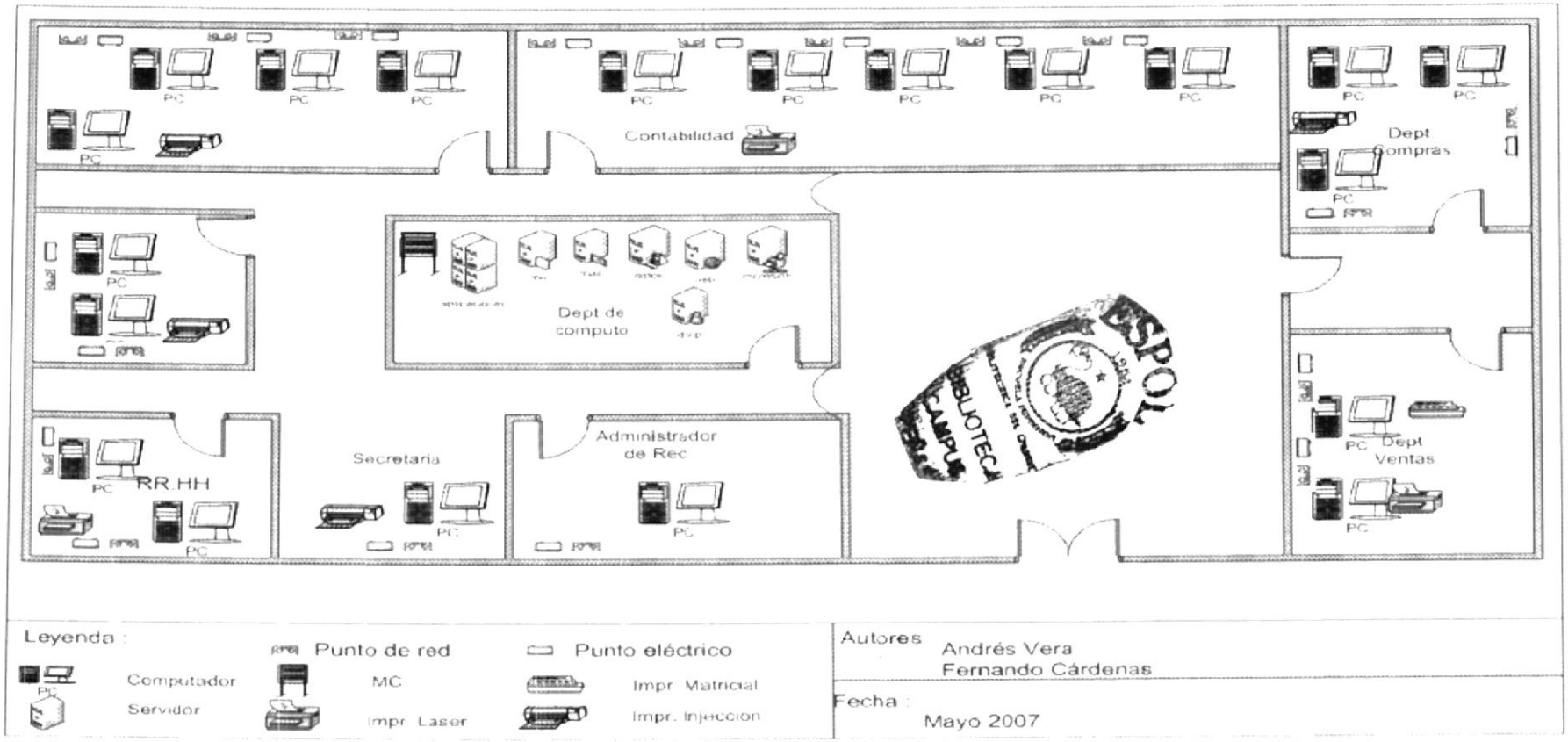


Figura 4-1: Análisis de Piso Aplicativo Matriz

MATRIZ

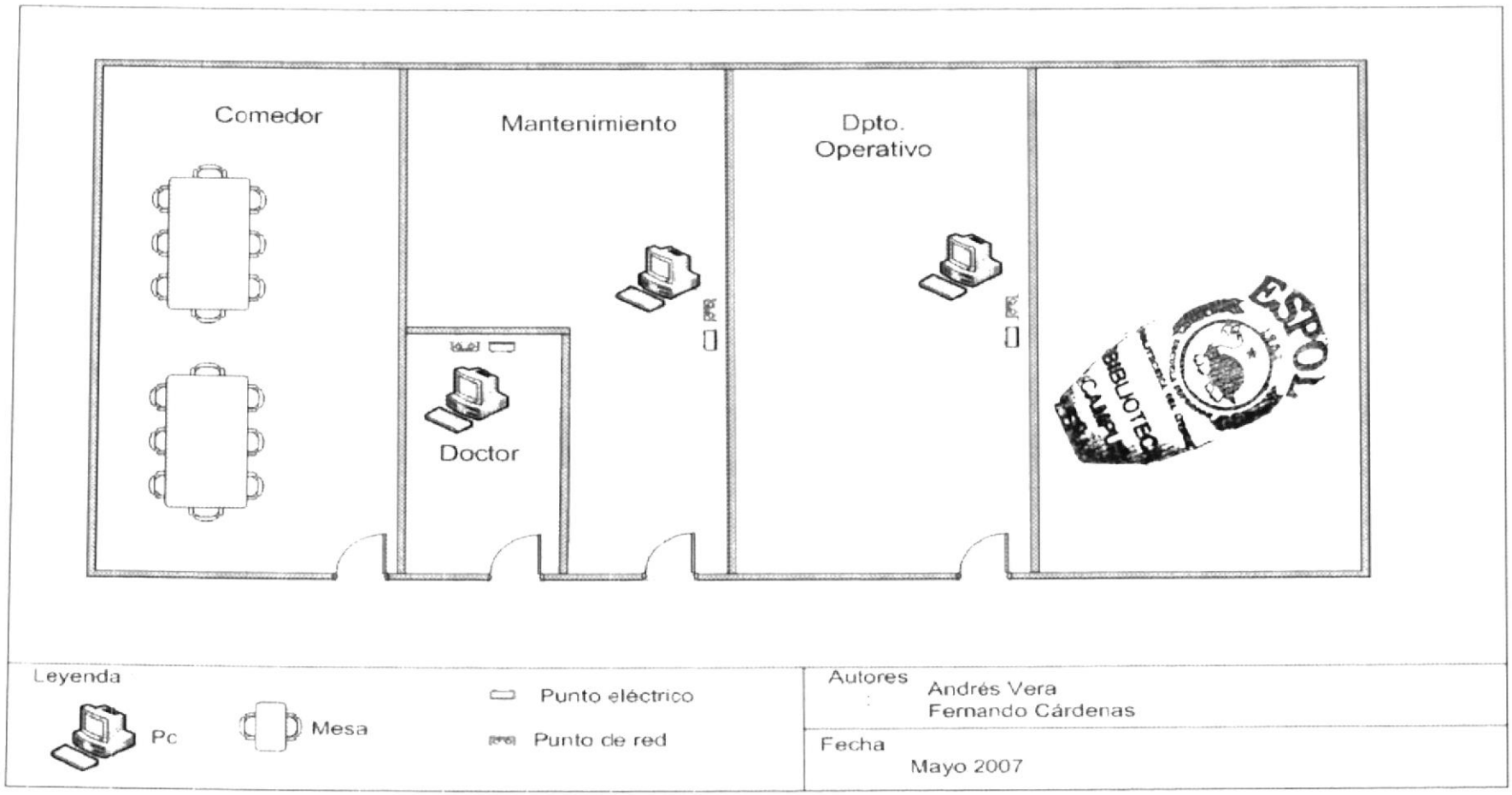


Figura 4-2: Análisis de Piso Aplicativo Matriz

4.1.2 BODEGA

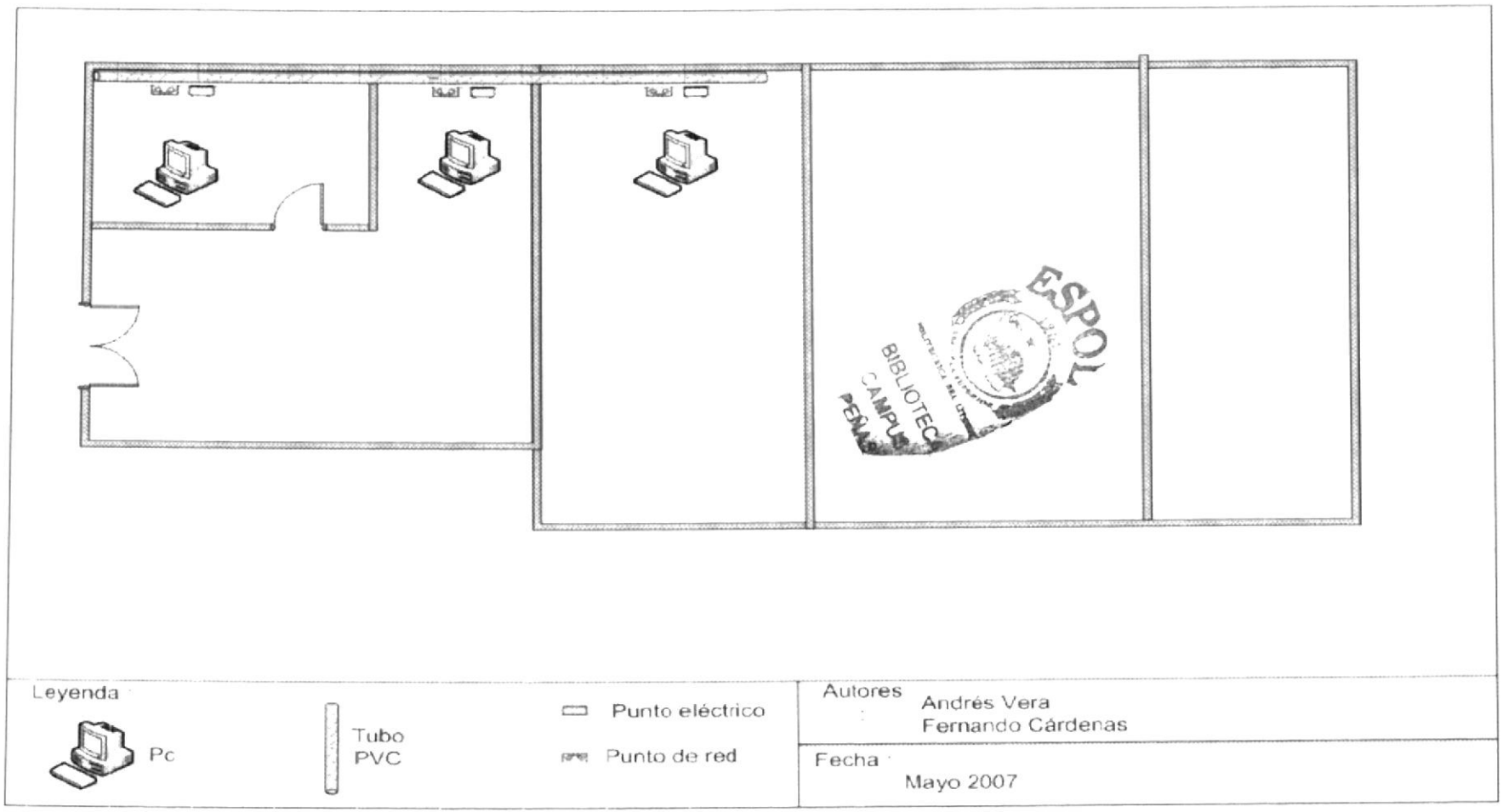


Figura 4-3: Análisis de Piso Aplicativo Bodega

4.1.3 SUCURSAL DIBSA

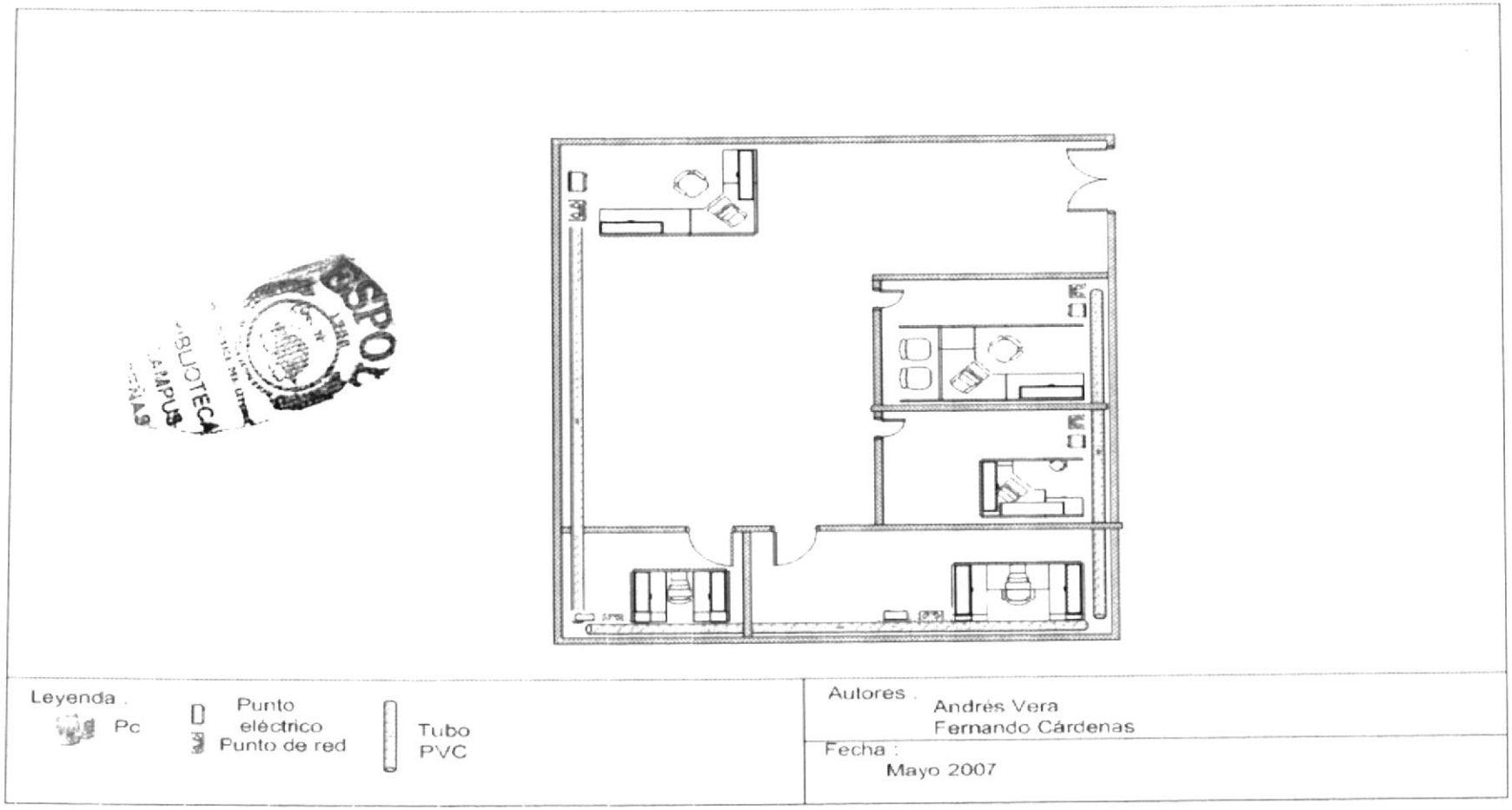


Figura 4-4: Análisis de Piso Aplicativo Sucursal Dibsa

4.1.4 SUCURSAL REYVENTAS

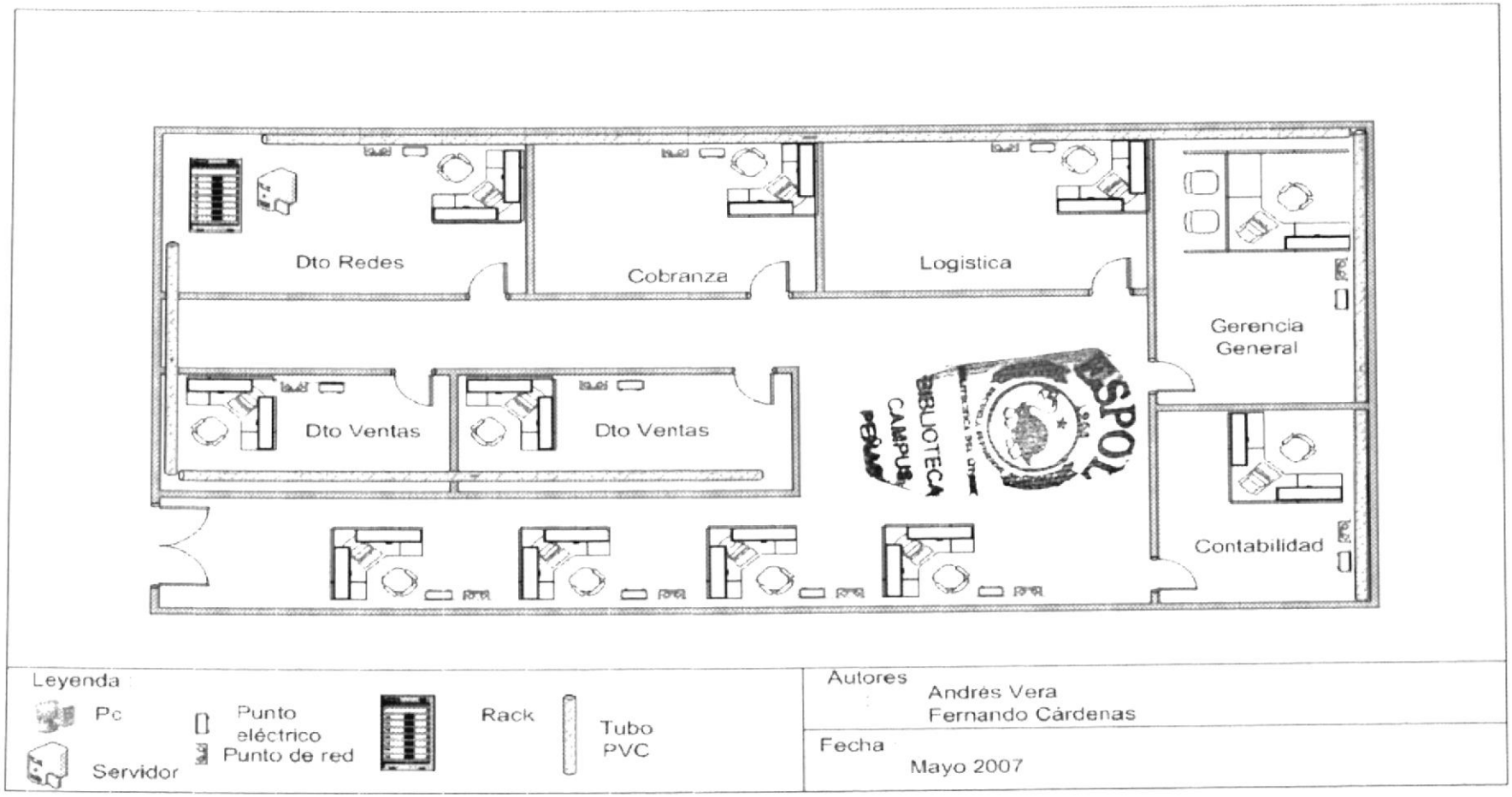


Figura 4-5: Análisis de Piso Aplicativo Sucursal ReyVentas

4.2 ANÁLISIS DE PISO LÓGICO

4.2.1 MATRIZ

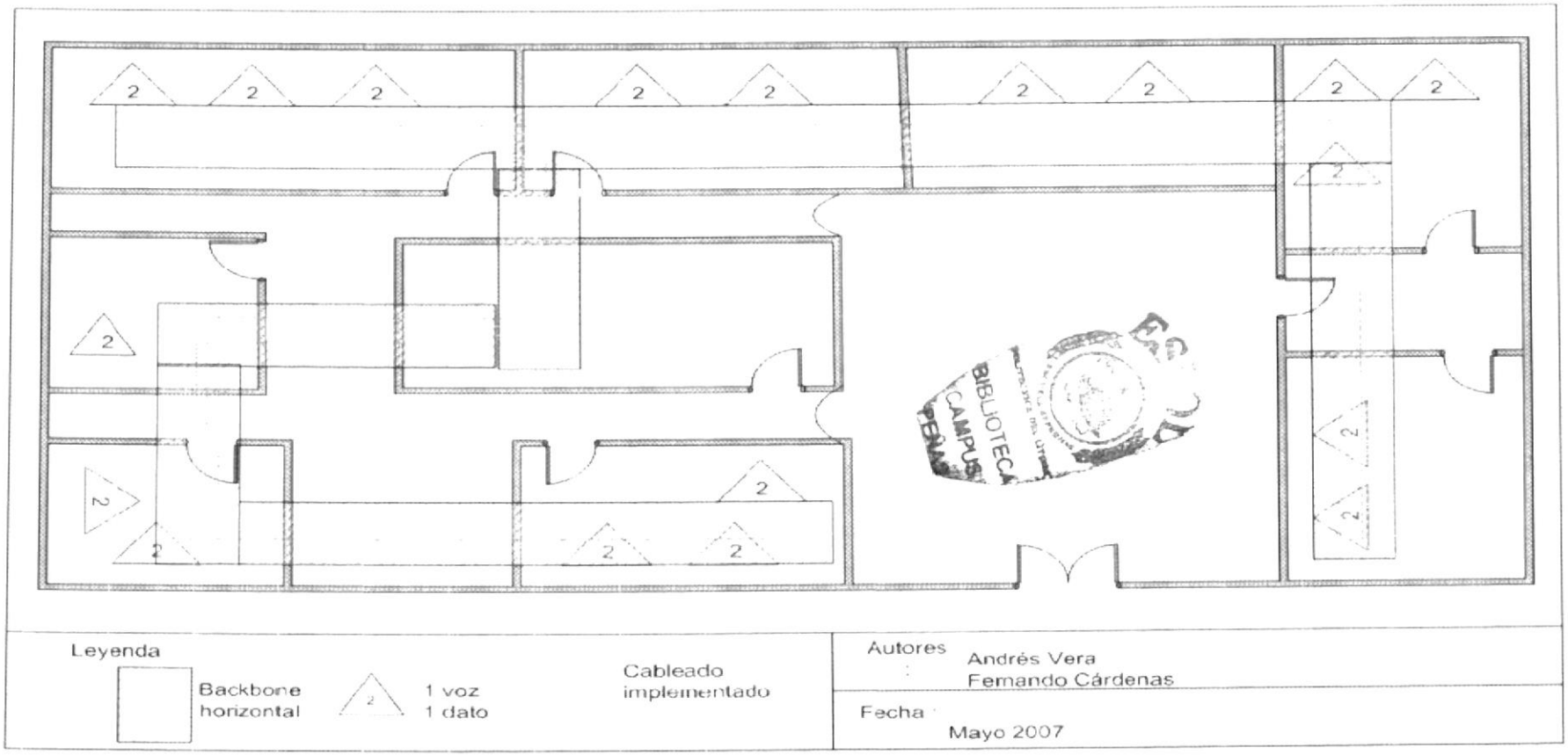


Figura 4-6: Análisis de Piso Lógico Matriz

MATRIZ

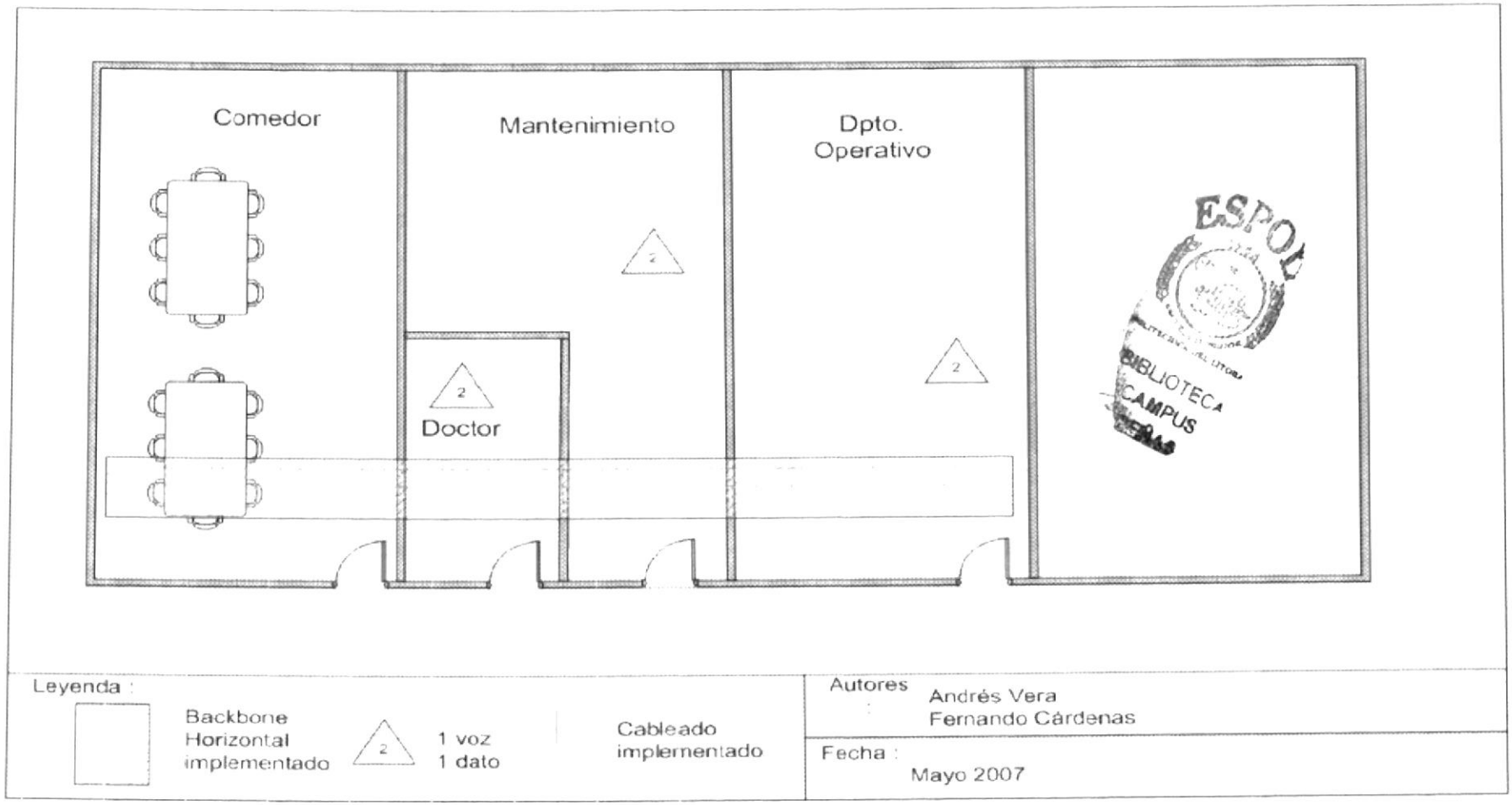


Figura 4-7: Análisis de Piso Aplicativo Matriz

4.2.2 BODEGA

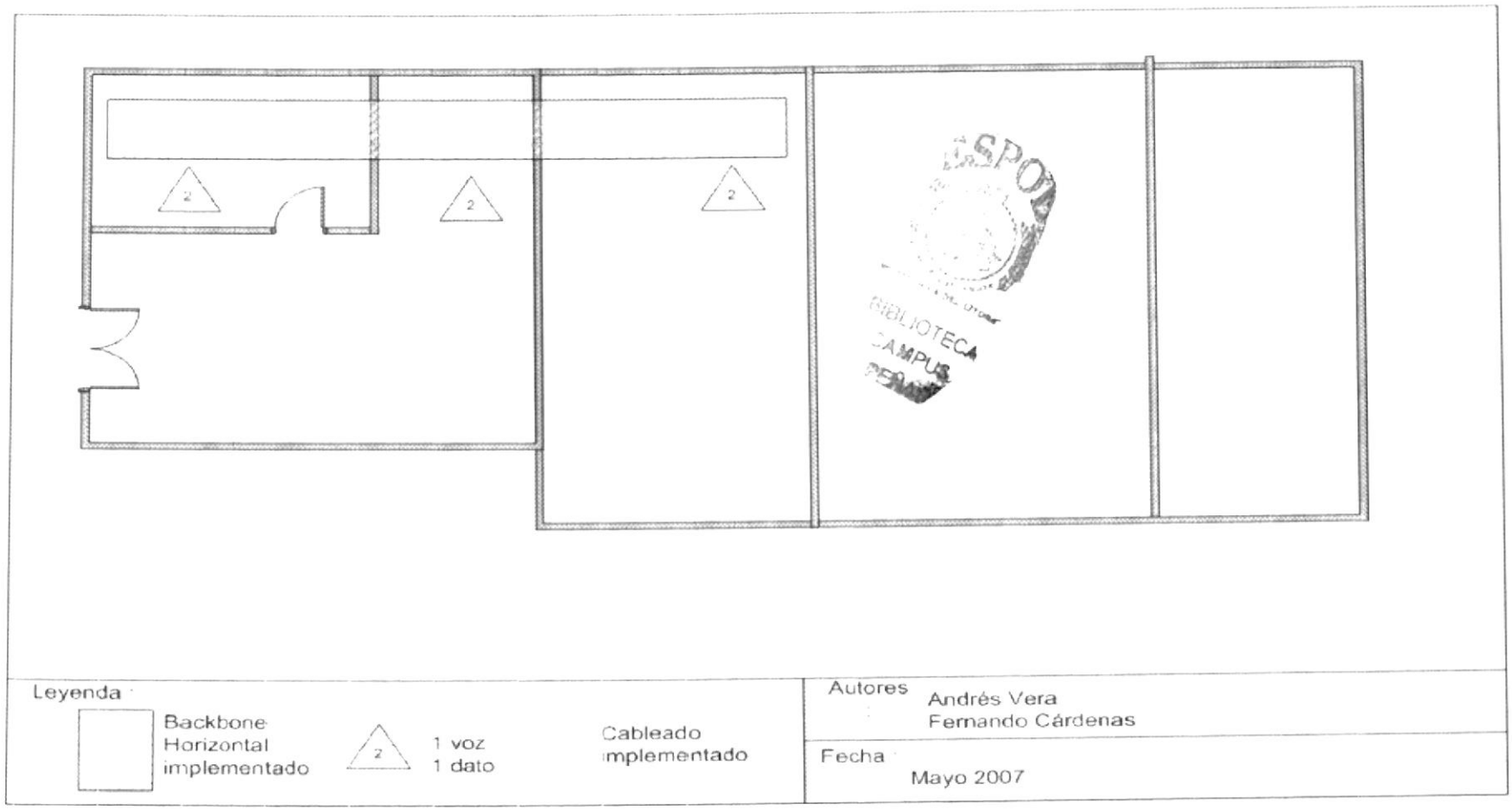


Figura 4-8: Análisis de Piso Lógico Bodega

4.2.3 SUCURSAL DIBSA

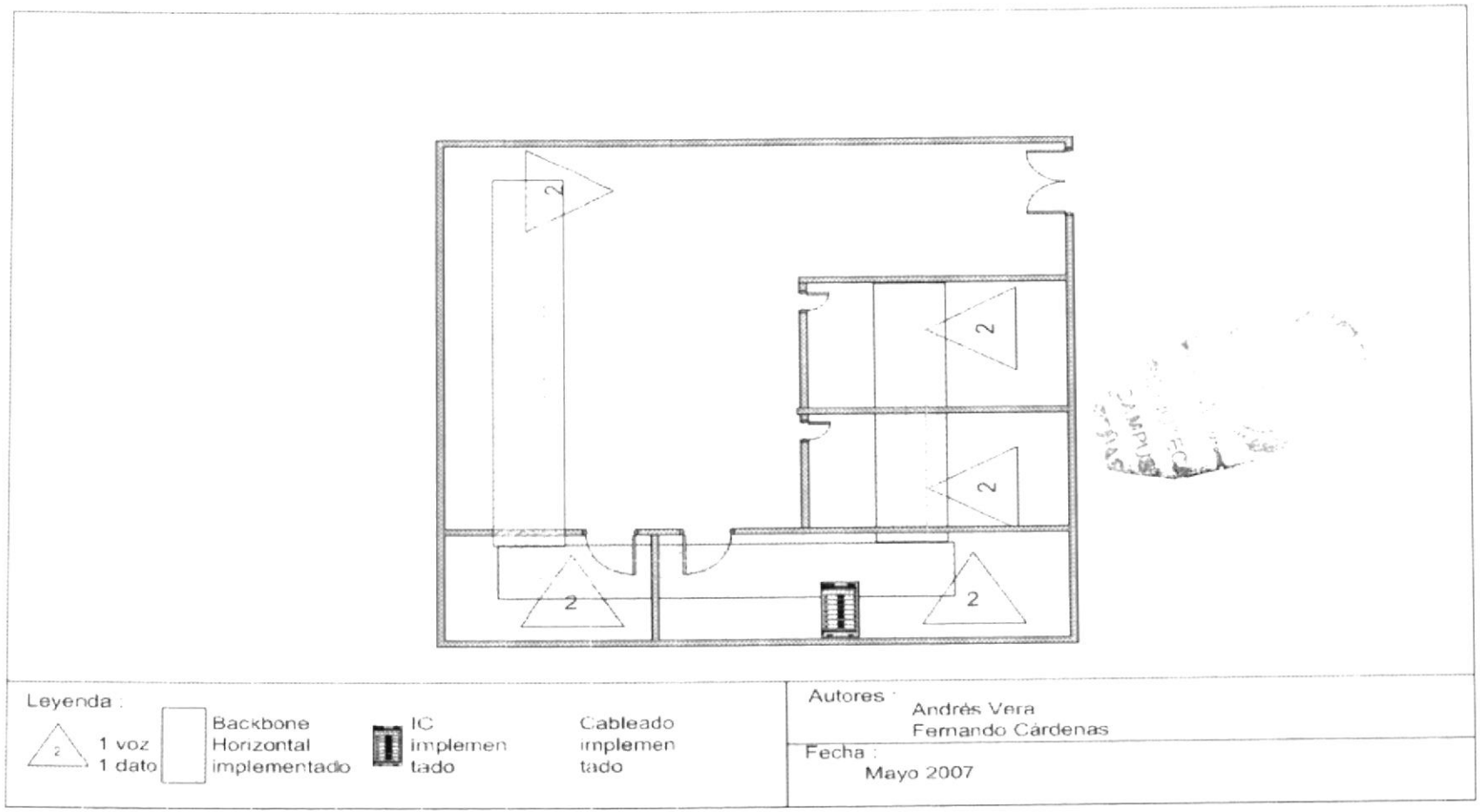


Figura 4-9: Análisis de Piso Lógico Sucursal Dibsa

4.2.4 SUCURSAL REYVENTAS

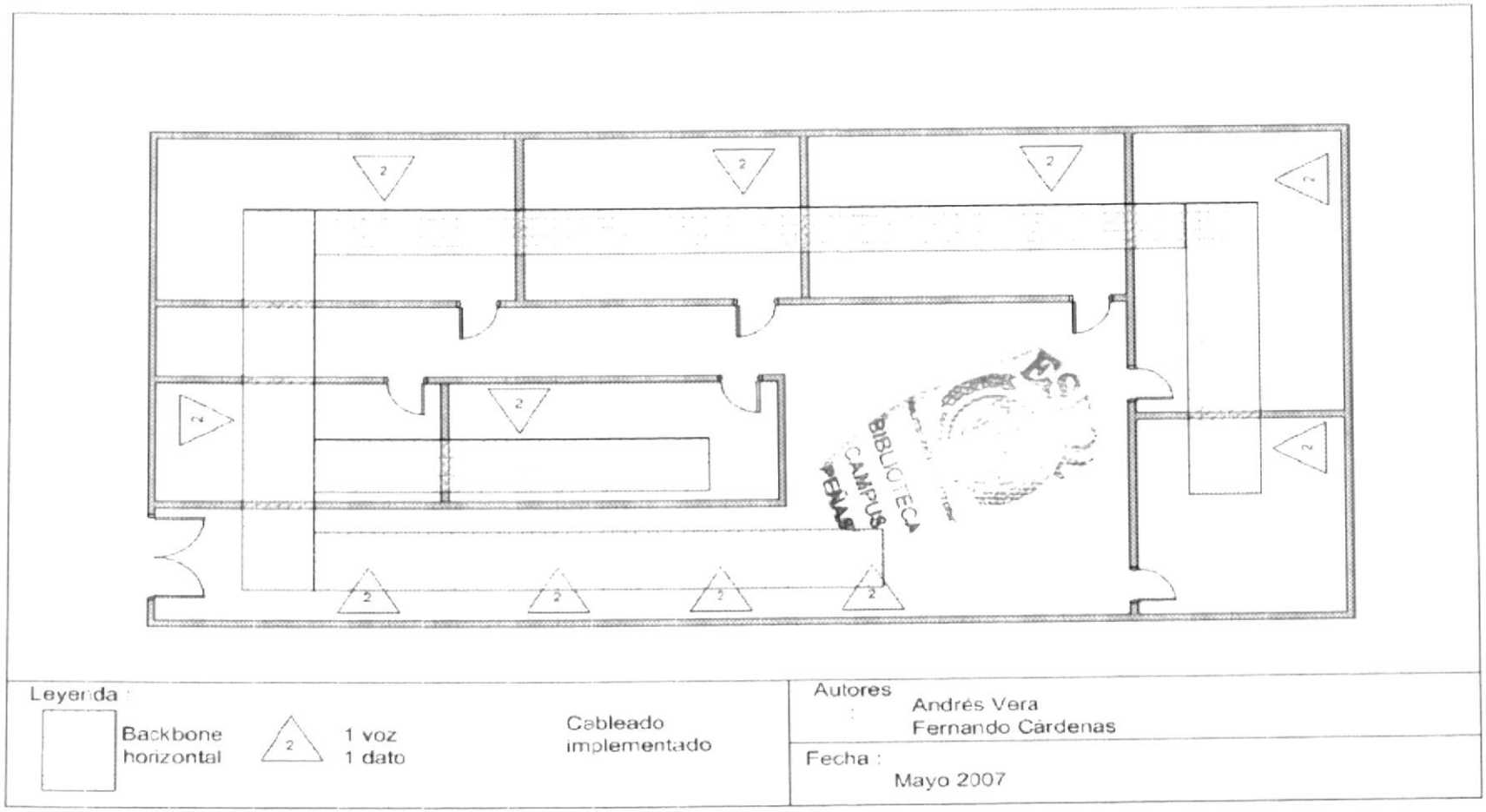


Figura 4-10: Análisis de Piso Lógico Sucursal ReyVentas

4.3 ESTRUCTURA DE MOLINOS

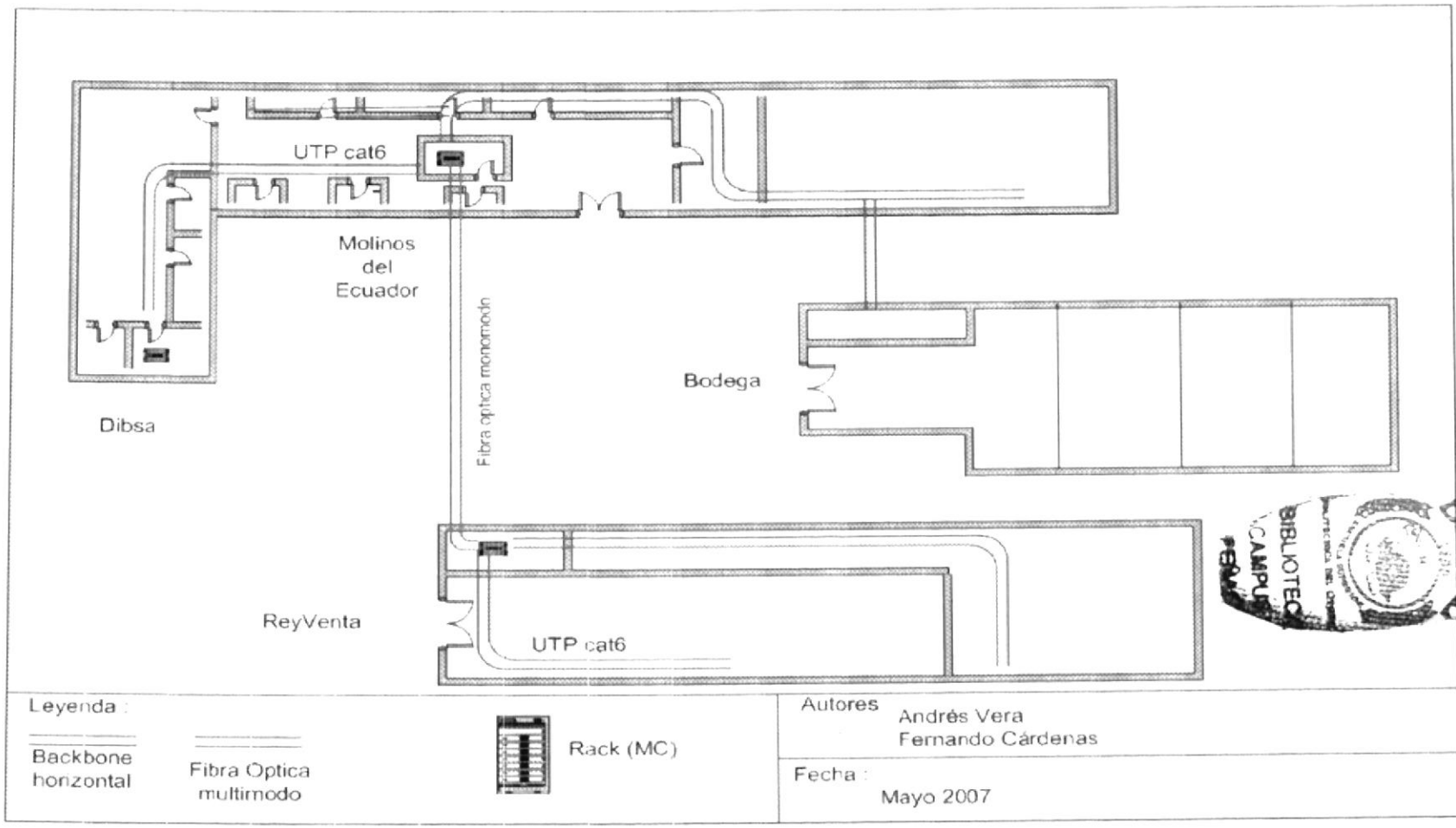


Figura 4-11: Gráfico de Molinos

4.4 GRÁFICOS DEL MC

4.4.1 MC PRINCIPAL DE MOLINO

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

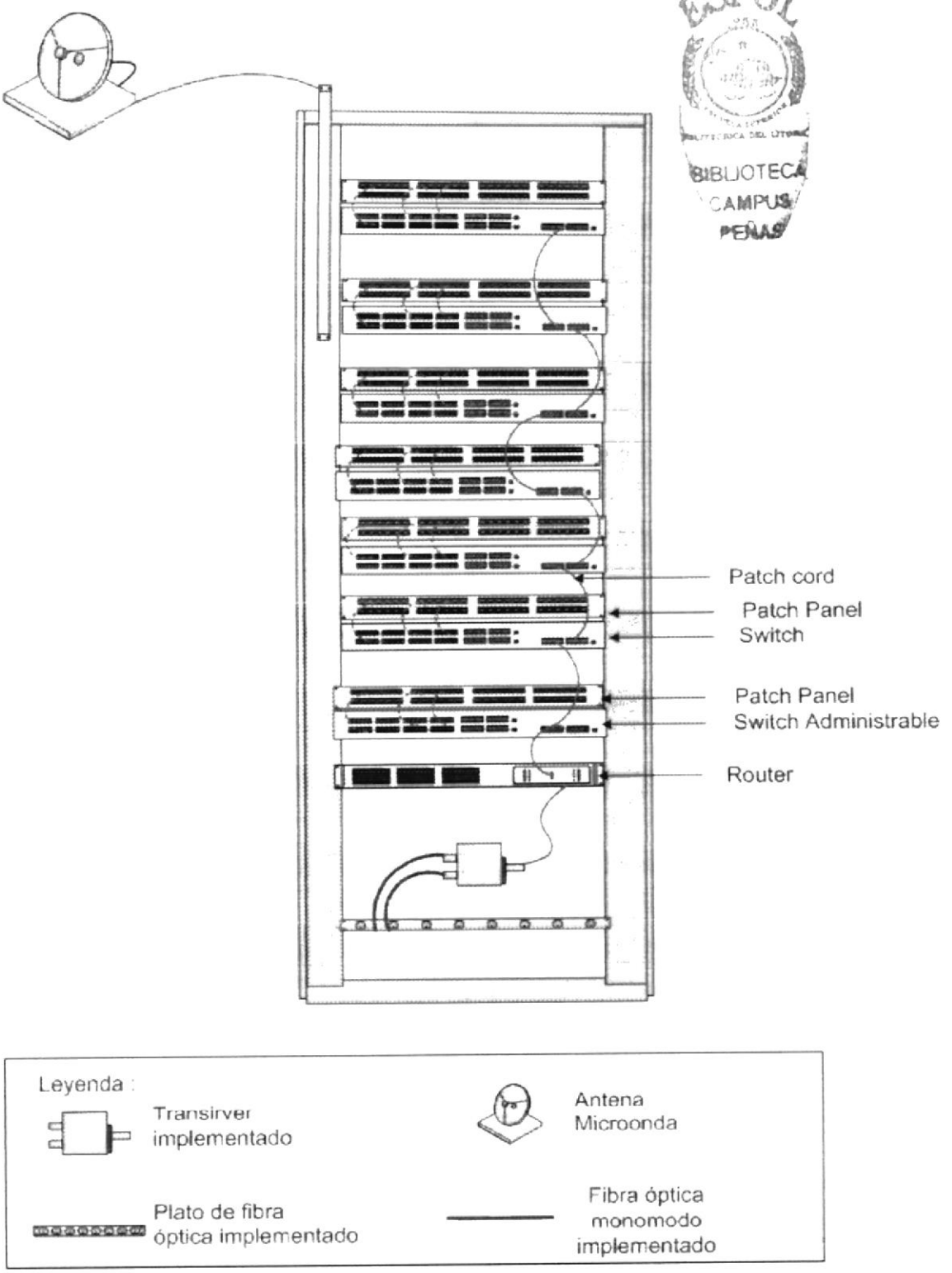


Figura 4-12: MC Matriz

4.4.2 MC DE REYVENTAS

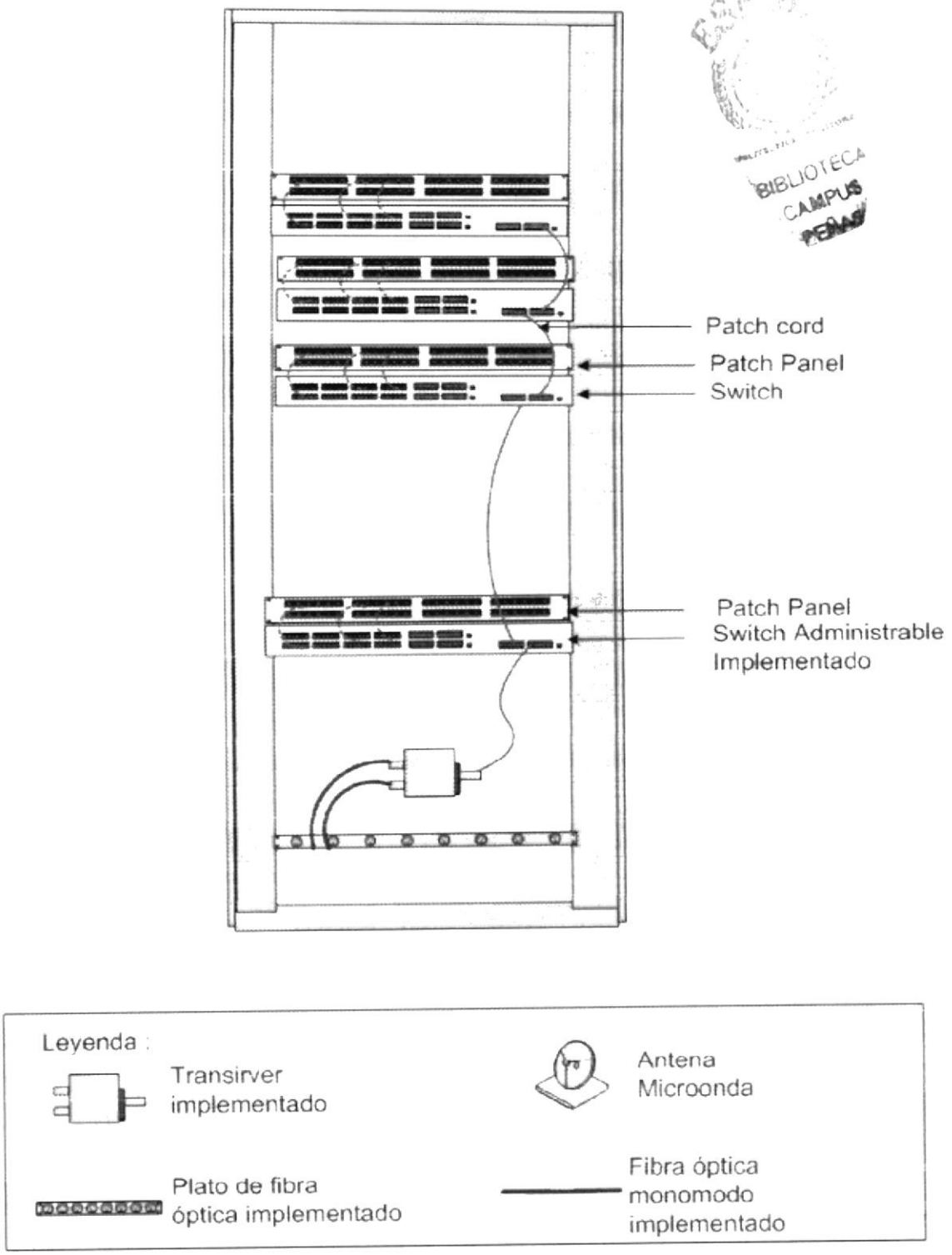
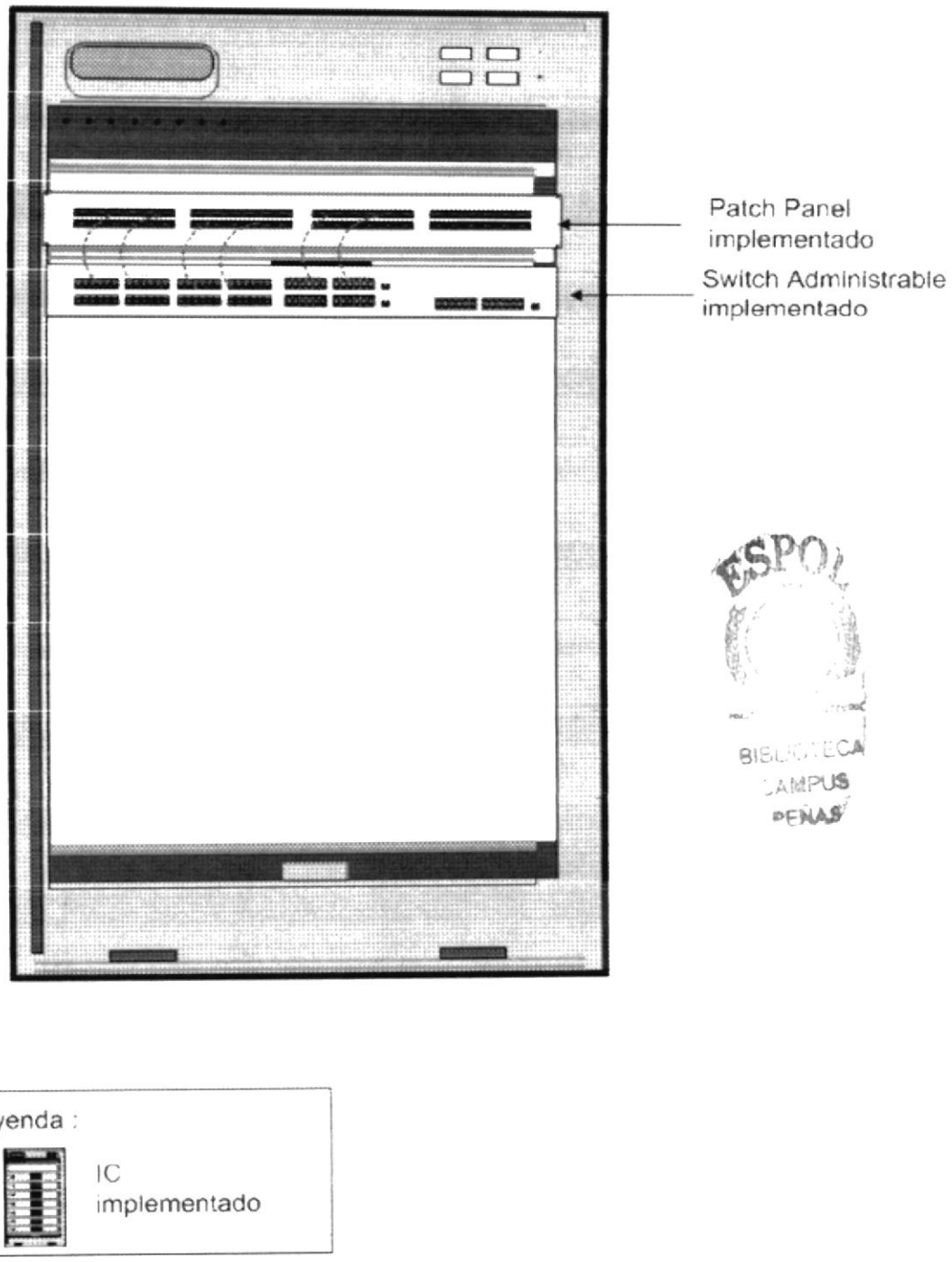


Figura 4-13: MC ReyVentas

4.4.3 IC DE DIBSA



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 4-14: IC Dibsa

4.5 CÁLCULO DEL BACKBONE

REYVENTAS										
cm	mts				4,5mt subida-bajada			1 video 1 dato		mts
1,50	*	1,92	=	2,88	+	9	=	11,88	* 2	23,76
5,00	*	1,92	=	9,60	+	9	=	18,60	* 2	37,20
7,50	*	1,92	=	14,40	+	9	=	23,40	* 2	46,80
10,50	*	1,92	=	20,16	+	9	=	29,16	* 2	58,32
15,00	*	1,92	=	28,80	+	9	=	37,80	* 2	75,60
16,50	*	1,92	=	31,68	+	9	=	40,68	* 2	81,36
17,50	*	1,92	=	33,60	+	9	=	42,60	* 2	85,20
18,30	*	1,92	=	35,14	+	9	=	44,14	* 2	88,27
19,00	*	1,92	=	36,48	+	9	=	45,48	* 2	90,96
10,50	*	1,92	=	20,16	+	9	=	29,16	* 2	58,32
16,00	*	1,92	=	30,72	+	9	=	39,72	* 2	79,44
									Total	725,23

Molinos										
Cm		Mts			4,5 subida-bajada			1 video- dato		mts
10,50	*	1,92	=	20,16	+	9	=	29,16	* 2	58,32
8,50	*	1,92	=	16,32	+	9	=	25,32	* 2	50,64
6,00	*	1,92	=	11,52	+	9	=	20,52	* 2	41,04
8,00	*	1,92	=	15,36	+	9	=	24,36	* 2	48,72
11,50	*	1,92	=	22,08	+	9	=	31,08	* 2	62,16
14,50	*	1,92	=	27,84	+	9	=	36,84	* 2	73,68
18,50	*	1,92	=	35,52	+	9	=	44,52	* 2	89,04
20,00	*	1,92	=	38,40	+	9	=	47,40	* 2	94,80
22,50	*	1,92	=	43,20	+	9	=	52,20	* 2	104,40
27,00	*	1,92	=	51,84	+	9	=	60,84	* 2	121,68
30,00	*	1,92	=	57,60	+	9	=	66,60	* 2	133,20
30,00	*	1,92	=	57,60	+	9	=	66,60	* 2	133,20
25,50	*	1,92	=	48,96	+	9	=	57,96	* 2	115,92
19,50	*	1,92	=	37,44	+	9	=	46,44	* 2	92,88
14,80	*	1,92	=	28,42	+	9	=	37,42	* 2	74,83
									Total	1,294.51

ESPOL BIBLIOTECA CAMPUS PEÑAS

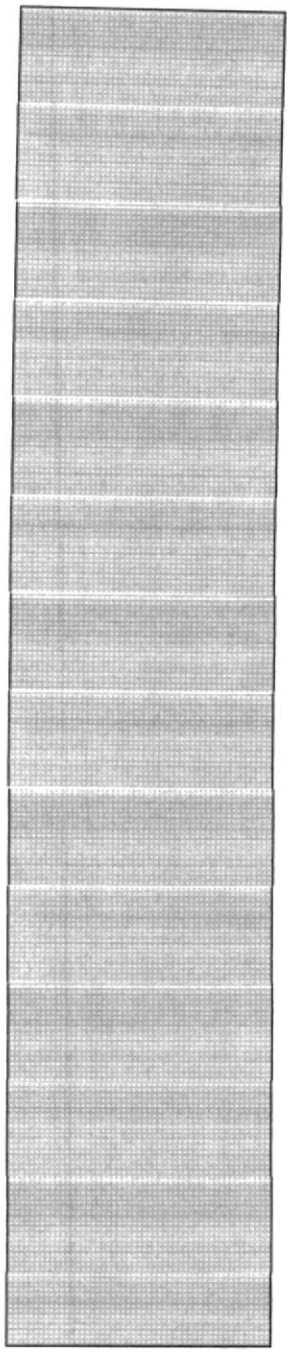
Dibsa										
Cm		Mts			4,5 subida-bajada			1 video-dato		mts
13	*	1,92	=	24,96	+	9	=	33,96	* 2	67,92
16	*	1,92	=	30,72	+	9	=	39,72	* 2	79,44
20	*	1,92	=	38,4	+	9	=	47,4	* 2	94,8
22	*	1,92	=	42,24	+	9	=	51,24	* 2	102,48
24	*	1,92	=	46,08	+	9	=	55,08	* 2	110,16
26	*	1,92	=	49,92	+	9	=	58,92	* 2	117,84
									Total	572,64

Bodega										
cm		mts			4,5mt subida 4,5 mt bajada				1 video 1 dato	mts
16	*	1,92	=	30,72	+	9	=	39,72	* 2	79,44
19	*	1,92	=	36,48	+	9	=	45,48	* 2	90,96
22	*	1,92	=	42,24	+	9	=	51,24	* 2	102,48
									Total	272,88

Suma de totales	
	mts
Rey Ventas	725,23
Molinos	1294,51
Dibsa	572,64
Bodega	272,88
Total	2.865,26



	bobina		
2,865,26	/	305	= 9,39
Total de bobinas	#	**10**	



ESCUELA SUPERIOR POLITECNICA DEL LITORAL
ESPOL

CAPÍTULO 5

NORMATIVAS

NORMATIVAS DE CERTIFICACIONES

NORMATIVA 1

Para evitar problemas causados por emisiones electromagnéticas pertenecientes a cables de potencia y otros equipos, todo sistema debe ser puesto y unido a tierra cumpliendo los reglamentos y normas aplicables.

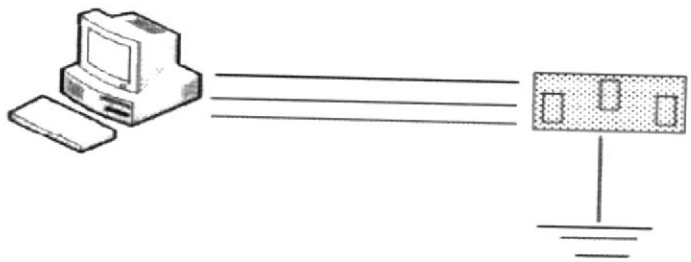


Figura 5- 1 Normativa 1

NORMATIVA 2

El cableado horizontal deberá estar configurado como topología estrella con cada salida de telecomunicaciones conectada a un HC o distribución de piso.

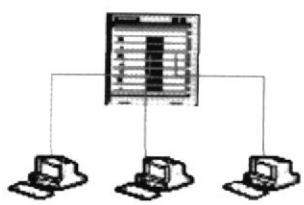


Figura 5- 2 Normativa 2

ESPOL
BIBLIOTECA
CAMPUS

NORMATIVA 3

Se empleara conexiones cruzadas para conexiones entre cableado horizontal y backbone y para conexiones entre cableado horizontal y equipos con salidas de puntos múltiples.

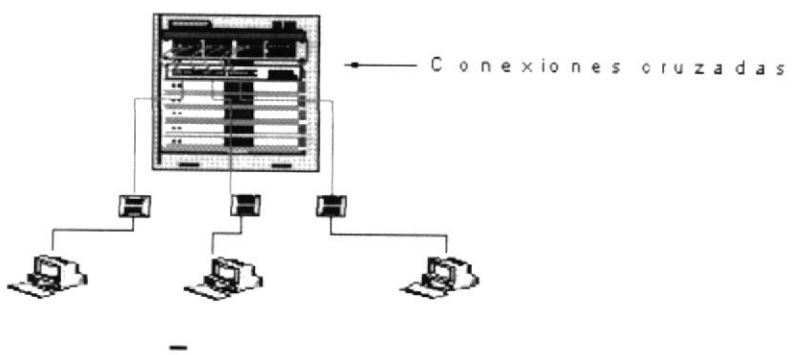


Figura 5- 3 Normativa 3

NORMATIVA 4

Cada área de trabajo será atendida por un HC *(cableado horizontal)* localizado en el mismo piso o adyacente.

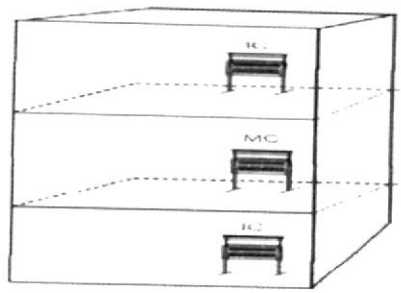


Figura 5- 4 Normativa 4

NORMATIVA 5

No se permite el uso de derivaciones punteados en el cableado horizontal.

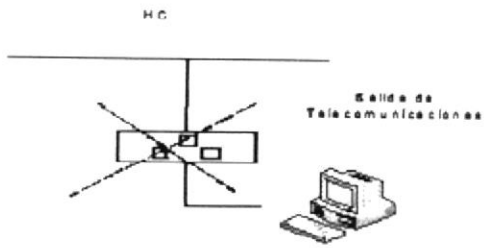


Figura 5- 5 Normativa 5

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

NORMATIVA 6

En la longitud del cable entre la salida de comunicación en el HC no exceda los 90 mts independiente del tipo del medio.

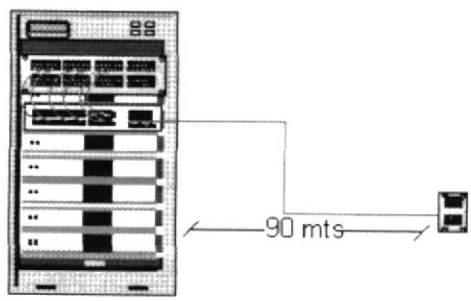


Figura 5- 6 Normativa 6

NORMATIVA 7

La longitud individual o combinada del pacht cord del par trenzado balanceado 24AWG (WG = cableado americano de alambre) o fibra óptica utilizada en el HC no excederá los 5mts.

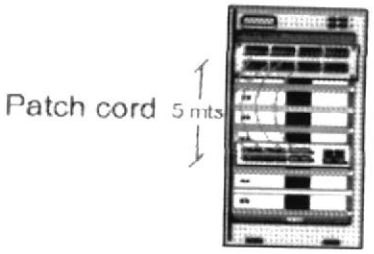


Figura 5- 7 Normativa 7

NORMATIVA 8

No se puede permitir más de 1 punto de consolidación dentro del mismo tendido del cableado horizontal.

- **Punto De Consolidación** es un hardware de conexiones que proporciona interconexión entre el cableado de oficina abierta y el cableado horizontal



Figura 5- 8 Normativa 8

ESPOL
BIBLIOTECA
CAMPUS
PENAS

NORMATIVA 9

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

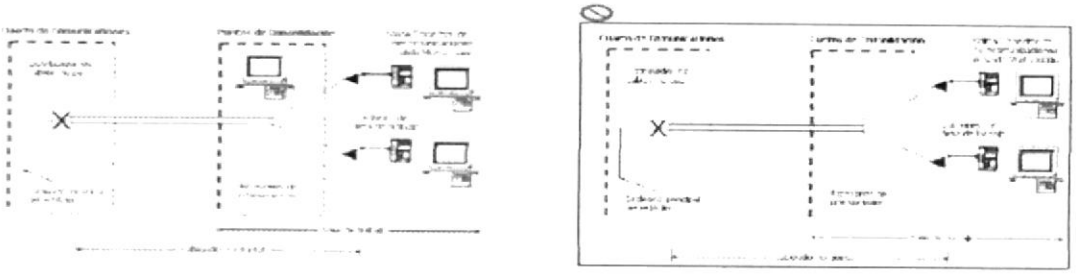


Figura 5- 9 Normativa 9

NORMATIVA 10

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

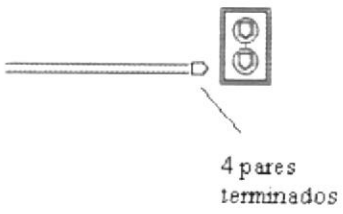


Figura 5- 10 Normativa 10

NORMATIVA 11

La distancia máxima entre el HC y la salida de comunicaciones será de 90mts.



Figura 5- 11 Normativa 11

NORMATIVA 12

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

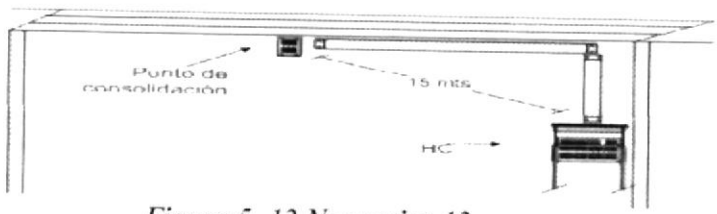
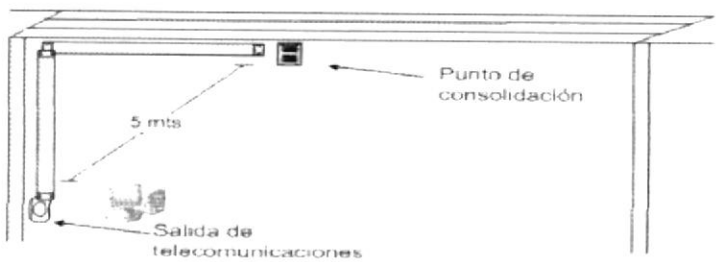


Figura 5- 12 Normativa 12

NORMATIVA 13

La distancia máxima entre el punto de consolidación y la salida de telecomunicaciones será de 5 mts.



ESPOL
BIBLIOTECA
CAMPUS

Figura 5- 13 Normativa 13

NORMATIVA 14

La distancia del canal del HC incluyendo el pacht cord y la salida de telecomunicaciones no excederá *los 100 mts.*

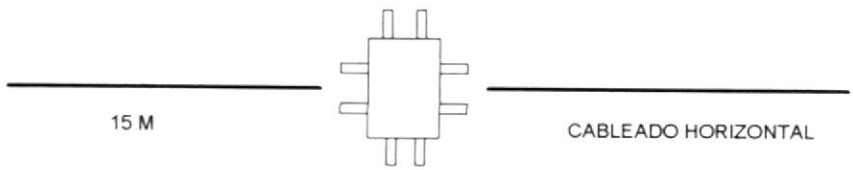


Figura 5- 14 Normativa 14

NORMATIVA 15

Todos los pares de cable estarán terminados en sus dos partes.

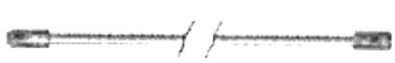


Figura 5- 15 Normativa 15

NORMATIVA 16

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

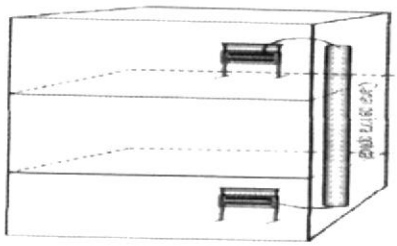


Figura 5- 16 Normativa 16

NORMATIVA 17

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



Figura 5- 17 Normativa 17

ESPOL
BIBLIOTECA
CAMPUS

NORMATIVA 18

Las canalizaciones horizontales se diseñarán e instalarán para cumplir los reglamentos eléctricos de construcciones locales, nacionales y de normas aplicables.

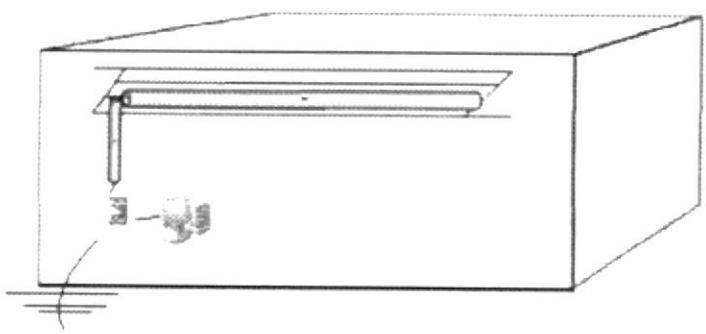


Figura 5- 18 Normativa 18

NORMATIVA 19

Las canalizaciones horizontales serán apropiadas para el ambiente en el cual se instalarán y no se obstaculizarán por ductos de ventilación, distribución de cableado eléctrico o estructura de edificio.

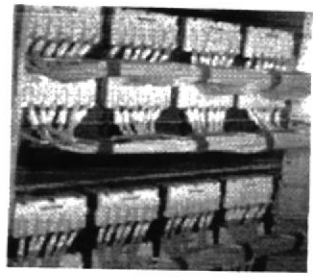


Figura 5- 19 Normativa 19

NORMATIVA 20

Las canalizaciones horizontales deberán tener un radio mínimo de curvatura del cable horizontal según las especificaciones del fabricante.



Figura 5- 20 Normativa 20

NORMATIVA 21

Todas las canalizaciones instaladas serán accesibles.

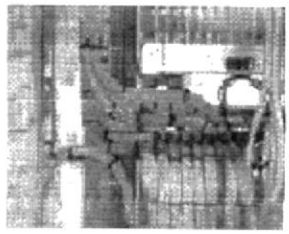


Figura 5- 21 Normativa 21

NORMATIVA 22

El backbone vertical utilizará una topología estrella jerárquica de cada MC a cada IC.

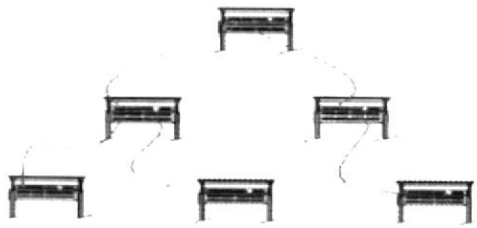


Figura 5- 22 Normativa 22

ESPOL
BIBLIOTECA
CAMPUS

NORMATIVA 23

Para cada tendido de backbond que sea mayor a 90mts de longitud debe tener cable de fibra óptica.

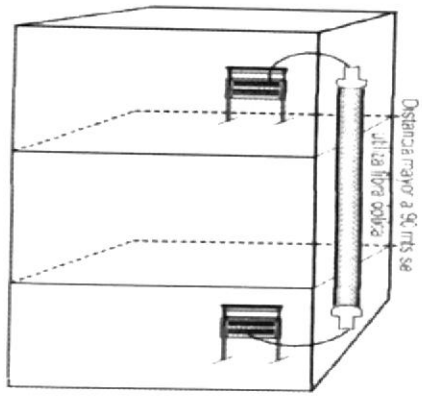


Figura 5- 23 Normativa 23

NORMATIVA 24

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

3 mil mts para fibra óptica monomodo.
2 mil mts para fibra óptica multimodo.
2 mil mts para par trenzado para aplicación PVX.

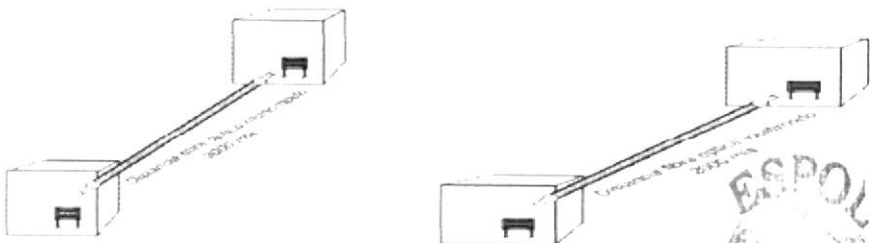


Figura 5- 24 Normativa 24

NORMATIVA 25

Las canalizaciones del edificio proveerán acceso a todos los cuartos de telecomunicaciones, cuarto de equipo y acometidas localizadas en el mismo edificio.

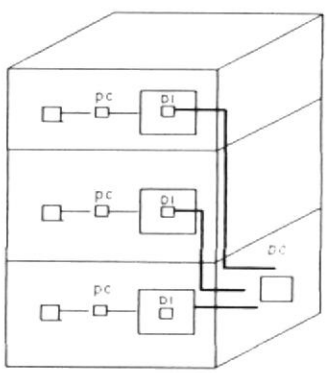


Figura 5- 25 Normativa 25

NORMATIVA 26

Las canalizaciones no ubicarán en ductos de ascensores.

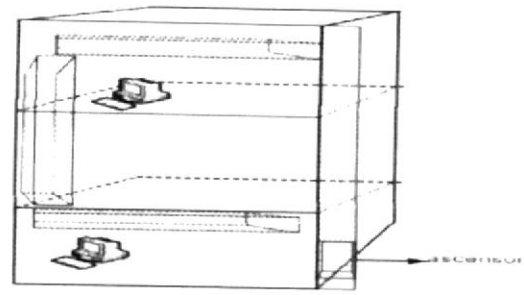


Figura 5- 26 Normativa 26

NORMATIVA 27

El cable que corre entre el cuarto de telecomunicaciones y la salida de telecomunicación no estará expuesto en el área de trabajo u otra parte de acceso público.

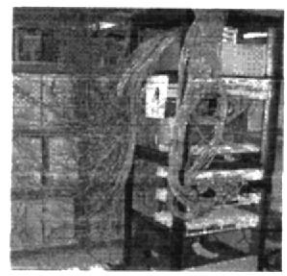


Figura 5- 27 Normativa 27

NORMATIVA 28

El cuarto de telecomunicaciones se diseñará y equipará para contener equipos de telecomunicaciones, terminales de cable y asociados.



BIBLIOTECA CAMPUS PEÑAS

Figura 5- 28 Normativa 28

NORMATIVA 29

El acceso a los cuartos de telecomunicaciones se restringirá al personal de servicio autorizado y no será compartido por servicio del edificio que puede interferir con el sistema de telecomunicaciones.

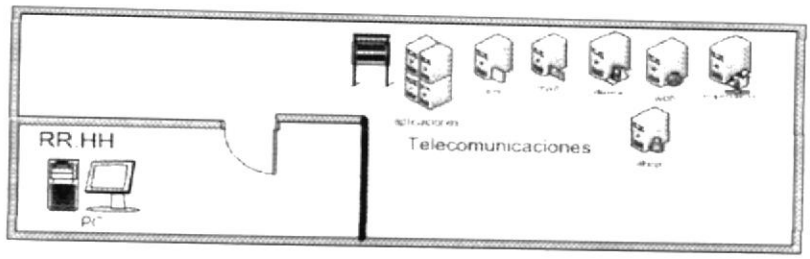


Figura 5- 29 Normativa 29

NORMATIVA 30

Las instalaciones unidas compuestas a tierra cumplirán los reglamentos y normas aplicables.

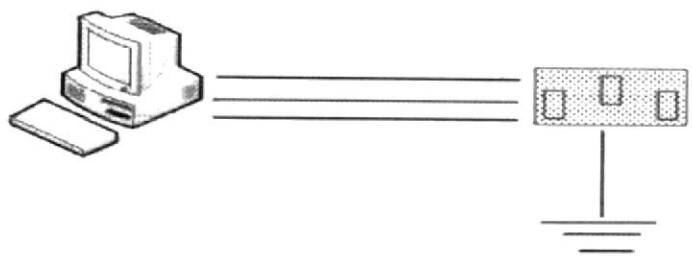


Figura 5- 30 Normativa 30

NORMATIVA 31

Los gabinetes usados como espacio alternativo cumplirán los requisitos de separación, tendrán una puerta con cerradura y se mantendrá en una ubicación fija.

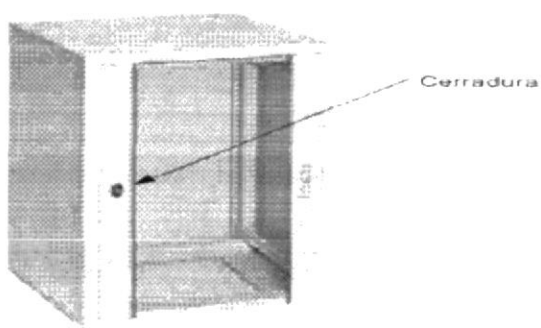


Figura 5- 31 Normativa 31

NORMATIVA 32

El cuarto de equipo no será compartido por servicio del edificio que puedan interferir con el sistema de telecomunicación o se utilicen para servicio de mantenimiento del edificio.

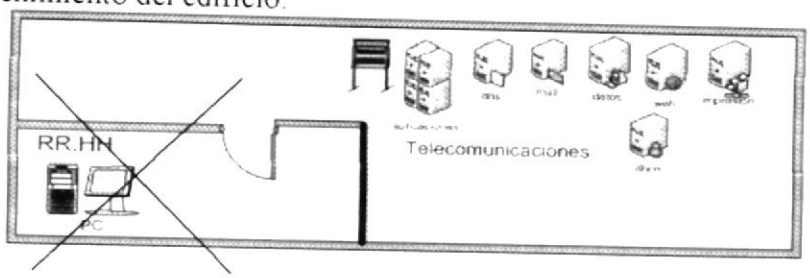


Figura 5- 32 Normativa 32

NORMATIVA 33

El cableado se instalará para facilitar el rotulado y la documentación y para permitir el código de colores de forma consistente.

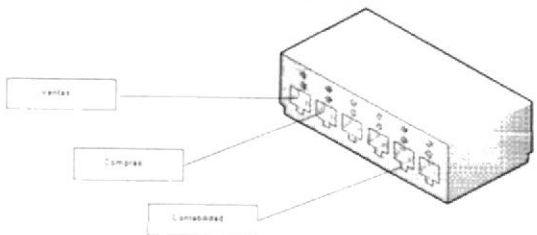


Figura 5- 33 Normativa 33

NORMATIVA 34

La instalación del gabinete y rack deberá promocionar las separaciones estipulada en los reglamentos y normas aplicables.

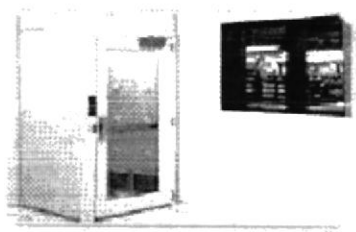


Figura 5- 34 Normativa 34

NORMATIVA 35

El cable de telecomunicaciones se soportará con los dispositivos diseñados para este fin y de forma independiente de cualquier otra infraestructura.





ESPOL
BIBLIOTECA
CAMPUS
PENAS

Figura 5- 35 Normativa 35

NORMATIVA 36

Los cables enrutados verticalmente, como backbone y horizontales enrutados entre pisos, se soportarán con abrazaderas. Se requiere un mínimo de dos soportes por piso.

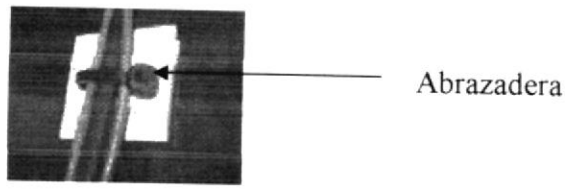


Figura 5- 36 Normativa 36

NORMATIVA 37

El número de cable horizontales (par tensado, balanceado o fibra óptica) colocada en un soporte en canalización se limitará a una cantidad que no altere forma geométrica del cable.

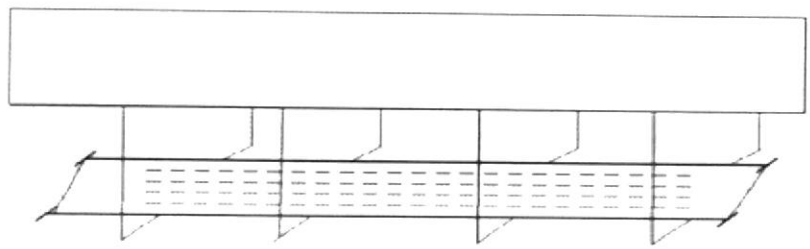


Figura 5- 37 Normativa 37

NORMATIVA 38

La canalizaciones de tipo bandeja o canal no excederá la capacidad máxima del 50% del llenado y una altura máxima de 6 pulgadas.

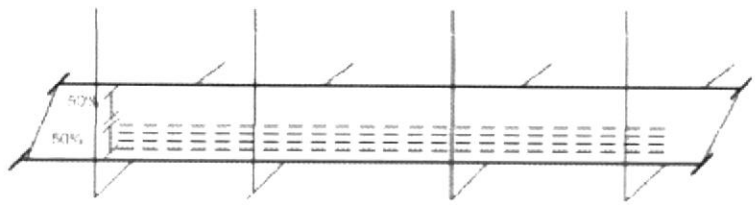
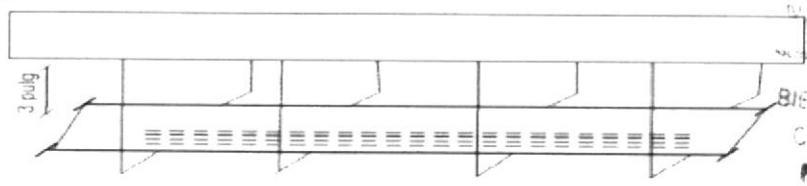


Figura 5- 38 Normativa 38

NORMATIVA 39

Para canalizaciones de techo falso los sistemas de soporte de cable se diseñarán e instalarán con un máximo 3 pulgadas por encina de loa rejilla del techo soportado.



BIBLIOTECA CAMPUS PEÑAS

Figura 5- 39 Normativa 39

NORMATIVA 40

La tensión máxima del jalado del cable con radio mínimo de cobertura no pasará de las especificaciones del fabricante.



Figura 5- 40 Normativa 40

NORMATIVA 41

No se permitirá el grapado de ningún tipo de cable.



Figura 5- 41 Normativa 41

NORMATIVA 42

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

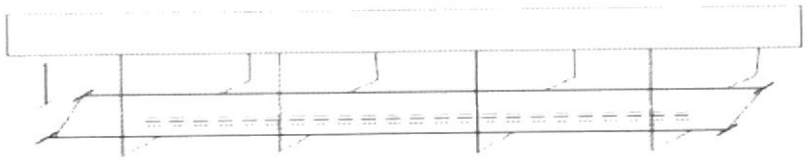


Figura 5- 42 Normativa 42

NORMATIVA 43

El radio mínimo de cobertura o condiciones de *no tensión* (cuando el cable es solo colocado) no jalado será de:

1 pulgada para SCTP o SFTP de diámetro es menor o igual a 6mm
2 pulgadas SCTP o SFTP de diámetro es menor a 6mm (0,25pulgadas)



Figura 5- 43 Normativa 43

NORMATIVA 44

El radio mínimo de cobertura para cable horizontal de 2 o 4 fibras será de 1pulgada bajo condiciones de *no tensión* y de 2 pulgadas bajo condiciones de *tensión;* en donde la tensión máxima de jalador será de 222 N (Newton = libras fuerzas).



Figura 5- 44 Normativa 44

NORMATIVA 45

El radio de cobertura para cable de backbone de fibras óptica de interiores no será menor a 10 veces el diámetro externo del cable bajo condiciones externa y no menor a 15 veces bajo condiciones de tensión.

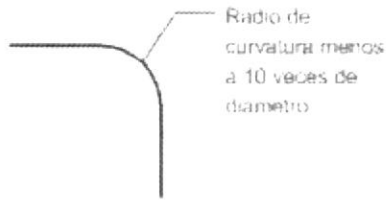


Figura 5- 45 Normativa 45

NORMATIVA 46

El radio de cobertura para cable de back bond de fibra óptica externa no será menor a 10 veces del diámetro externo de cable bajo condiciones *no tensión*, y no menor a 20 veces del diámetro externo del cable bajo condiciones de *tensión*, en donde la tensión de jalado es menor a 2.670 N (600 libras fuerza).

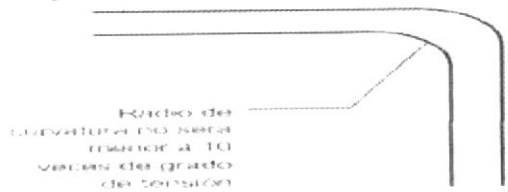


Figura 5- 46 Normativa 46

NORMATIVA 47

El cable que corre entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará expuesto en el área de trabajo ni en otro espacio exceso público.

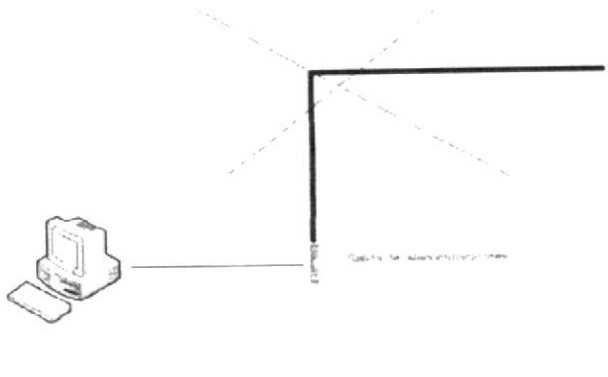


Figura 5- 47 Normativa 47

NORMATIVA 48

EL hardware de conexión se instalará de manera que brinde un control cable ordenado.

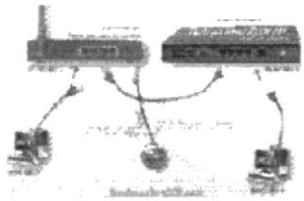


Figura 5- 48 Normativa 48

NORMATIVA 49

Con el fin de reducir el desentrezado de pares de cable, el instalador debe pelar solo aquella cantidad de forro que se requiera para terminar en el hardware de conexión para par tensado balanceado.

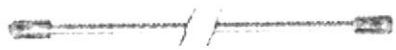


Figura 5- 49 Normativa 49

NORMATIVA 50

La cantidad máxima de desentrezado de cada par, resultante de la terminación en el hardware de conexión será de 13mm para cable de CAT 5 e o mayor y de 75mm para cable CAT 3.

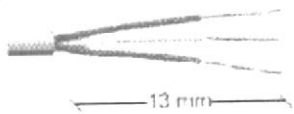


Figura 5- 50 Normativa 50

NORMATIVA 51

No se deberá terminar cable de diferente categoría de desempeño en el mismo hardware de conexión.

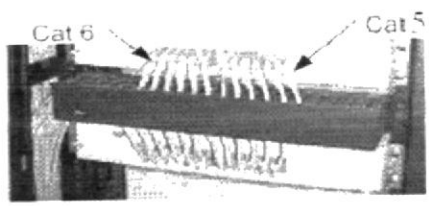


Figura 5- 51 Normativa 51

BIBLIOTECA
CAMPUS
PEÑAS

NORMATIVA 52

Los identificadores que se utilizan para accesar a grupos del mismo tipo deben ser únicos.



Figura 5- 52 Normativa 52

NORMATIVA 53

El rotulado deberá realizarse ya sea pagando o colocando firmemente una etiqueta, independiente al elemento que se va a administrar.

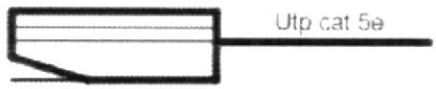


Figura 5- 53 Normativa 53

NORMATIVA 54

El rotulado debe ser legible y permanecer firmemente unido al elemento durante el periodo de garantia (5 años).

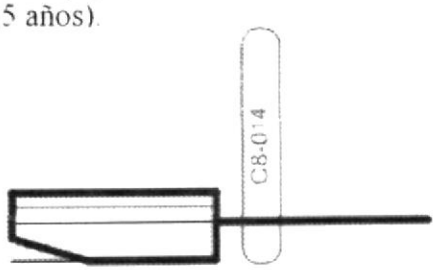


Figura 5- 54 Normativa 54

NORMATIVA 55

A cada cable se le asignarán un identificador único que sirva como referencia a su registro.

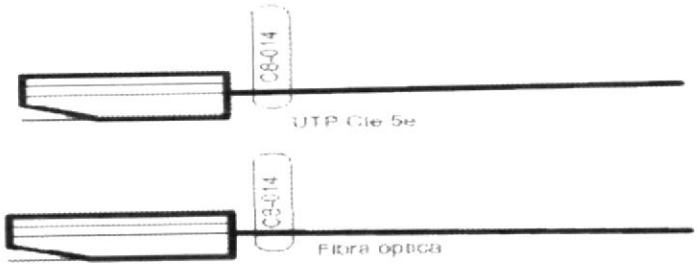


Figura 5- 55 Normativa 55

CAMPUS
PENAS

NORMATIVA 56

Los cable de los sistemas horizontales que de backbone deberán rotularse en cada extremo, la etique puede ser colocada 30 cm. del extremo del cable, esta marca deberá permanecer en cable después de terminar la instalación.

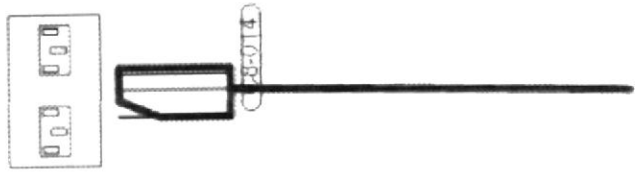


Figura 5- 56 Normativa 56

RECOMENDACIÓN DE CABLEADO ESTRUCTURADO

RECOMENDACIÓN 1

Se pueden emplear interconexiones para conexiones entre cableado horizontal y equipos compuestos individuales.

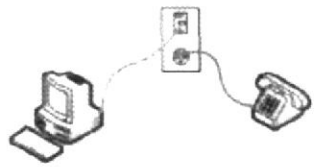


Figura 5- 57 Recomendación 1

RECOMENDACIÓN 2

Con el fin de proveer una infraestructura capaz, ubicar un buen ambiente se recomienda al menos *un cuarto de comunicación* por cada piso.

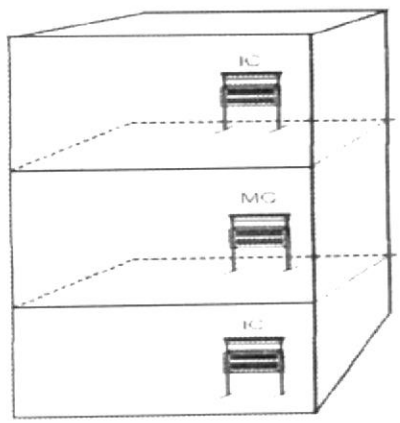


Figura 5- 58 Recomendación 2

RECOMENDACIÓN 3

El área que pueda atender efectivamente por un cuarto de comunicaciones debe tener un *radio máximo de 60 mts.*

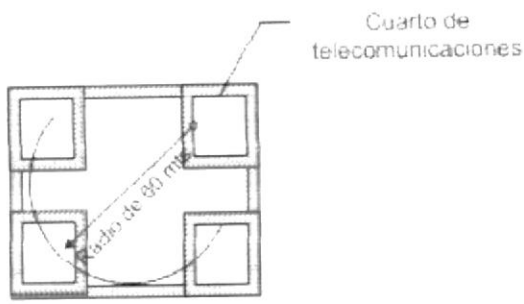


Figura 5- 59 Recomendación 3

RECOMENDACIÓN 4

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



Figura 5- 60 Recomendación 4

RECOMENDACIÓN 5

Se recomienda 2 salidas de categoría 6 por cada área de trabajo individual con el fin de soportar numerosas aplicaciones diseñadas para operar sobre cableado par trenzado.

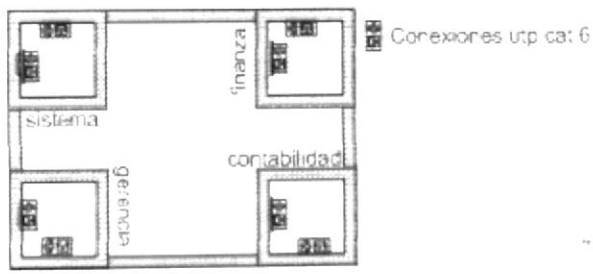


Figura 5- 61 Recomendación 5

RECOMENDACIÓN 6

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

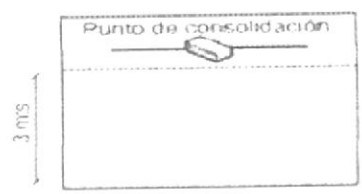


Figura 5- 62 Recomendación 6

RECOMENDACIÓN 7

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

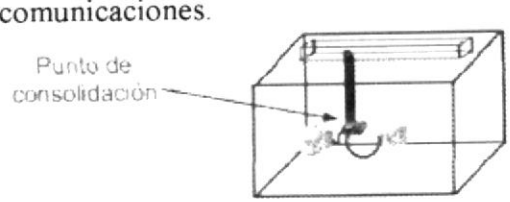


Figura 5- 63 Recomendación 7

RECOMENDACIÓN 8

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



Figura 5- 64 Recomendación 8

RECOMENDACIÓN 9

Se recomienda que se provea con mínimo de 2 hilos de fibra óptica para cada aplicación conocida, durante su periodo de planificación. Debe proveer un crecimiento del 100%.



Figura 5- 65 Recomendación 9

RECOMENDACIÓN 10

Para cada backbone se recomienda un mínimo de 3mts de reserva de cada extremo.

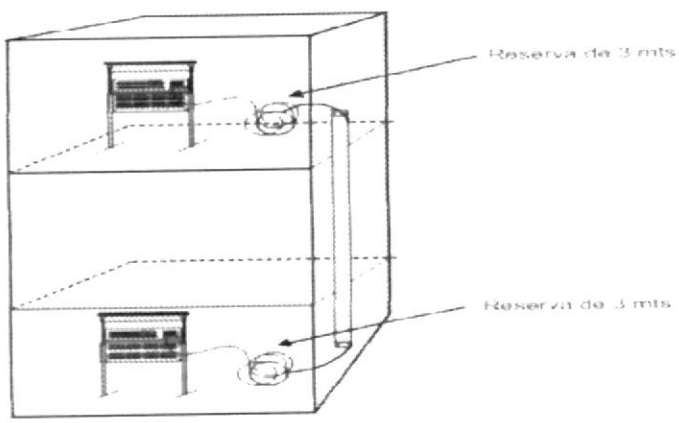


Figura 5- 66 Recomendación 10

RECOMENDACIÓN 11

Los acabados en el cuarto de telecomunicaciones deberán ser colores claros para mejorar la iluminación.

RECOMENDACIÓN 12

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

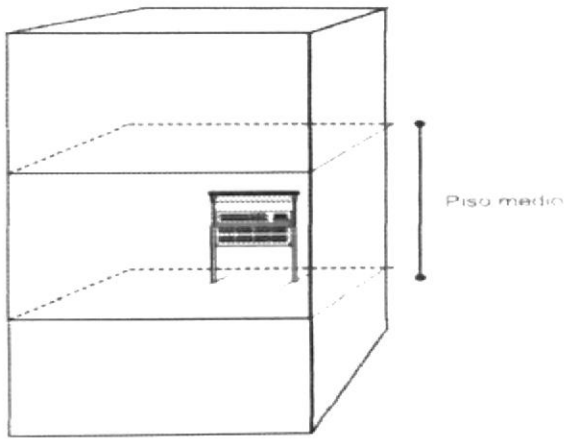


Figura 5- 67 Recomendación 12

ESPOL
BIBLIOTECA
CAMPUS
PENAS

RECOMENDACIÓN 13

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

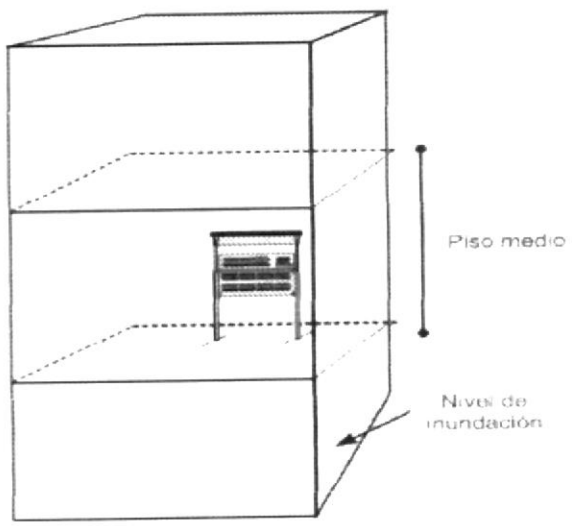
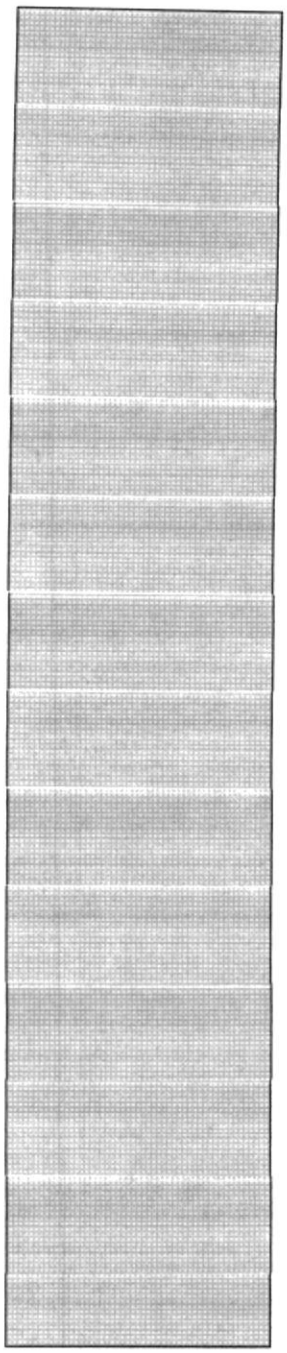


Figura 5- 68 Recomendación 13



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 6

LINUX

6.1 HISTORIA DE LINUX

Linux nació gracias a la idea de Linus Torvalds de crear un sistema basado en minix para máquinas i386; en más de una ocasión, Linus Torvalds ha afirmado que si hubiera sabido de la existencia de los sistemas BSD que ya cumplían lo que hacía Linux, no se habría molestado en modificar minix. La historia de Linux está fuertemente vinculada a la del proyecto GNU. El proyecto GNU, iniciado en 1983, tiene como objetivo el desarrollo de un sistema Unix completo compuesto enteramente de software libre. Hacia 1991, cuando la primera versión del núcleo Linux fue liberada, el proyecto GNU había producido varios de los componentes del sistema operativo, incluyendo un intérprete de comandos, una biblioteca C y un compilador, pero aún no contaba con el núcleo que permitiera completar el sistema operativo.
Entonces, el núcleo creado por Linus Torvalds, quien se encontraba por entonces estudiando en la Universidad de Helsinki, llenó el hueco final que el sistema operativo GNU exigía. Subsecuentemente, miles de programadores voluntarios alrededor del mundo han participado en el proyecto, mejorándolo continuamente. Torvalds y otros desarrolladores de los primeros días de Linux adaptaron los componentes de GNU y de BSD, así como de otros muchos proyectos como Perl, Apache, Python, etc. para trabajar con el núcleo Linux, creando un sistema operativo completamente funcional procedente de muchísimas fuentes diferentes, la mayoría libres.

6.1.2 ETIMOLOGÍA

Linux se refiere estrictamente al núcleo Linux, pero es comúnmente utilizado para describir al sistema operativo tipo Unix (que implementa el estándar POSIX), que utiliza primordialmente filosofía y metodologías libres (también conocido como GNU/Linux) y que está formado mediante la combinación del núcleo Linux con las bibliotecas y herramientas del proyecto GNU y de muchos otros proyectos/grupos de software (libre o no libre).
La expresión "Linux" es utilizada para referirse a las distribuciones GNU/Linux, colecciones de software que suelen contener grandes cantidades de paquetes además del núcleo. El software que suelen incluir consta de una enorme variedad de aplicaciones, como: entornos gráficos, suites ofimáticas, servidores web, servidores de correo, servidores FTP, etcétera. Coloquialmente se aplica el término "Linux" a éstas.



6.1.3 ARQUITECTURA

Linux es un núcleo monolítico híbrido. Los controladores de dispositivos y las extensiones del núcleo normalmente se ejecutan en un espacio privilegiado conocido como anillo 0 (ring 0), con acceso irrestricto al hardware, aunque algunos se ejecutan en espacio de usuario. A diferencia de los núcleos monolíticos tradicionales, los controladores de dispositivos y las extensiones al sistema operativo se pueden cargar y descargar fácilmente como módulos, mientras el sistema continúa funcionando sin interrupciones. También, a diferencia de los núcleos monolíticos tradicionales, los controladores pueden ser pre-volcados (detenidos momentáneamente por actividades más importantes) bajo ciertas condiciones. Esta habilidad fue agregada para manejar correctamente interrupciones de hardware, y para mejorar el soporte de Multiprocesamiento Simétrico.

El hecho de que Linux no fue desarrollado siguiendo el diseño de un microkernel (diseño que, en aquella época, era considerado el más apropiado para un núcleo por muchos teóricos informáticos) fue asunto de una famosa y acalorada discusión entre Linus Torvalds y Andy Tanenbaum.

A diferencia de los núcleos monolíticos tradicionales, los controladores de dispositivos son fácilmente configurables como Loadable Kernel Modules, y se pueden cargar o descargar mientras se está corriendo el sistema.

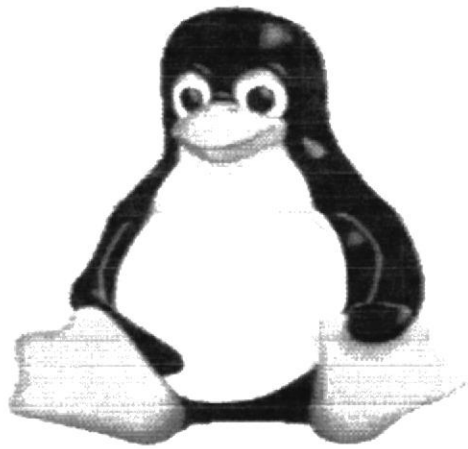
6.1.4 LENGUAJES DE PROGRAMACIÓN

Linux está escrito con una versión del lenguaje de programación C apoyado por GCC (que ha introducido un número de extensiones y cambios al C estándar), junto a unas pequeñas secciones de código escritas con el lenguaje ensamblador (assembly language). Por la extensión que soporta C, GCC fue durante mucho tiempo el único compilador capaz de construir correctamente Linux. Recientemente, Intel afirmó haber modificado su compilador C de forma de poder compilarlo correctamente.

Se usan muchos otros lenguajes en alguna forma, básicamente en la conexión con el proceso de construcción del kernel (el método a través del cual las bootable image son creadas desde la source). Estos incluyen a Perl, Python y varios lenguajes shell scripting. Algunos drivers también pueden ser escritos en C++, Fortran, u otros lenguajes, pero esto es altamente desaconsejable. El sistema de construcción de Linux oficialmente solo soporta GCC como kernel y compilador de driver.



6.2 LINUX FEDORA CORE 3



Fedora Core (también conocida como Fedora Linux) es una distribución de Linux desarrollada por la comunidad Fedora y promovida por la compañía estadounidense Red Hat.
El objetivo del proyecto Fedora es conseguir un sistema operativo de propósito general y basado exclusivamente en software libre con el apoyo de la comunidad Linux. Los ingenieros de Red Hat continúan participando en la construcción y desarrollo de este proyecto e invitan y fomentan la participación de miembros de la comunidad Linux.

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

ESPOL BIBLIOTECA CAMPUS PEÑAS

6.2.1 CARACTERÍSTICAS DEL SISTEMA

Fedora conserva el preciosismo y elegancia de los escritorios heredados de Red Hat, pero si hay alguna cosa que distingue el nuevo Fedora Core de otras distribuciones, es en el apartado de los asistentes.
Fiel a la tradicion de Red Hat de acercar Linux al usuario, Fedora Core 3 implementa asistentes para (casi) todas las funcionalidades que se requiera configurar en nuestro equipo, desde impresoras a escáners en red, dispositivos inalámbricos. Por supuesto, que los mas expertos siguen pudiendo abrir una Terminal y correr *vi* o *Emacs* para acceder a los archivos de configuración si asi lo desean. Esto sigue siendo Linux despues de todo. Otra de las caracteristicas más interesantes del nuevo Fedora es el que se refiere al apartado denominado *Stateless Linux*.
Bajo esta bastante oscura denominacion, se esconde un proyecto que hará las delicias de todo administrador de sistemas que tenga varias máquinas a su cargo y quiera mantener una instalación sincronizada e idéntica en cada una de ellas. Con las herramientas Stateless Linux proporcionadas por Fedora Core, un administrador de sistemas puede realizar una instalación en una maquina "maestra" y repetir esa misma instalación en tantas máquinas quiera con un mínimo esfuerzo. No solo eso, sino que las máquinas esclavo nunca tendrán que ser actualizadas o reconfiguradas individualmente.

En vez de eso, se actualiza el "maestro" y todos los cambios realizados en esta máquina se aplican automaticamente a las máquinas "esclavo".

Linux Core 3, incluye software para un rango completo de servicios de red. Para instalar un sistema con los servicios de red mas comunes, se puede seleccionar la instalación de servidor durante la instalación, también se puede escoger paquetes de programas individuales.

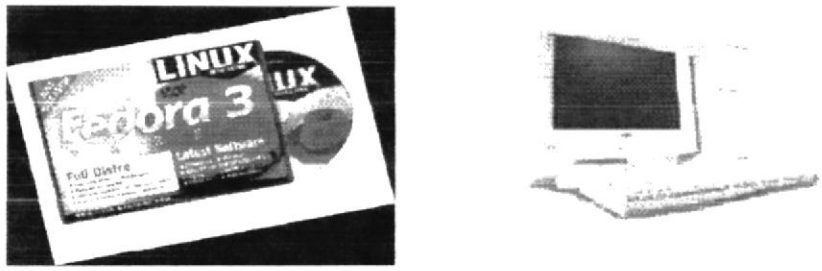


Figura 6-1: Cd y Pc

6.2.2 REQUERIMIENTOS DE INSTALACIÓN

Los requerimientos mínimos de hardware que el servidor Linux debe tener son los siguientes:

Mínimos	**Óptimos**
Procesador Pentium II 400 MHZ Memoria Ram 64 MB Espacio en Disco duro 5 GB Tarjeta de red 10 Mbps	Procesador Pentium IV 3.2 Ghz Memoria Ram 512 MB Espacio en Disco duro de 40 GB Tarjeta de red 10/100 Mbps

ESPOL

6.3 CONFIGURACIÓN DEL BIOS

Primero debe verificar que la primera unidad de buteo sea la de **CD ROM** esto lo hará entrando a las configuraciones del **SETUP**.

Cuando el equipo arranca se mostrará una pantalla igual al gráfico, aquí se debe mantener presionada la tecla **DEL** para ir a opciones del **SETUP**.

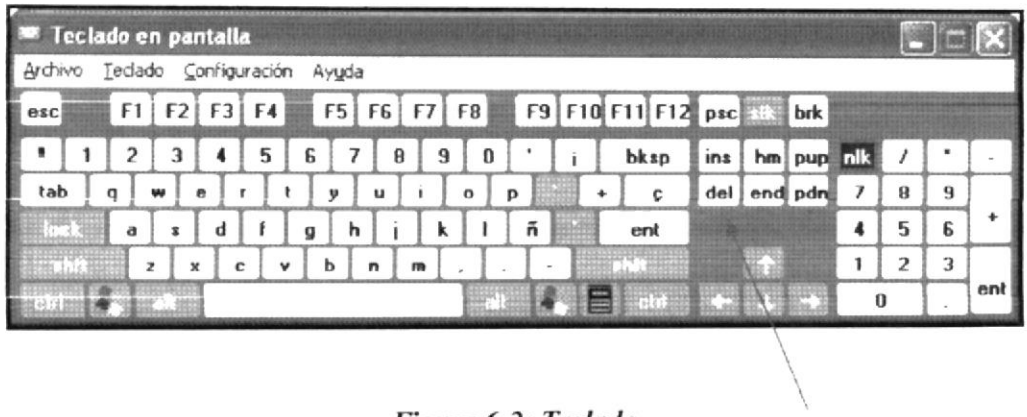


Figura 6-2: Teclado

Una vez que se ingrese a la pantalla de configuración del **BIOS** se selecciona la opción **ADVANCED BIOS FEATURES** en la cual se configura la secuencia de buteo.

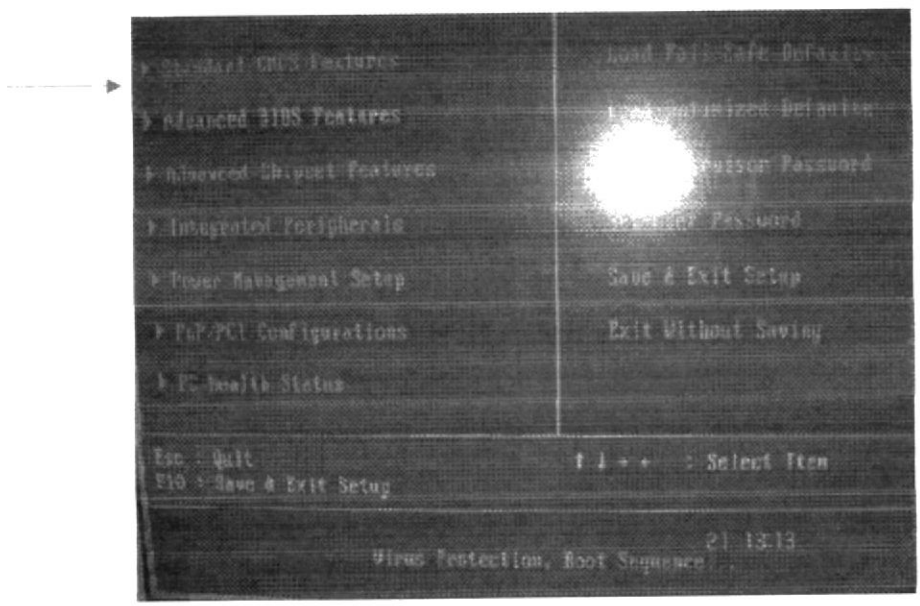


Figura 6-3: Pantalla del Bios

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

En esta pantalla se muestra las teclas direccionales del computador con las cuales se puede movilizar por las diferentes opciones que presenta el **SETUP.**



Figura 6-4: Teclas Direccionales

Se coloca el cursor en **FIRST BOOT DEVICE** y con Avpag seleccionar **CD-ROM,** para que el PC arranque desde el **CD-ROM** y en **SECOND BOOT DEVICE** se seleccione **HDD-0**.

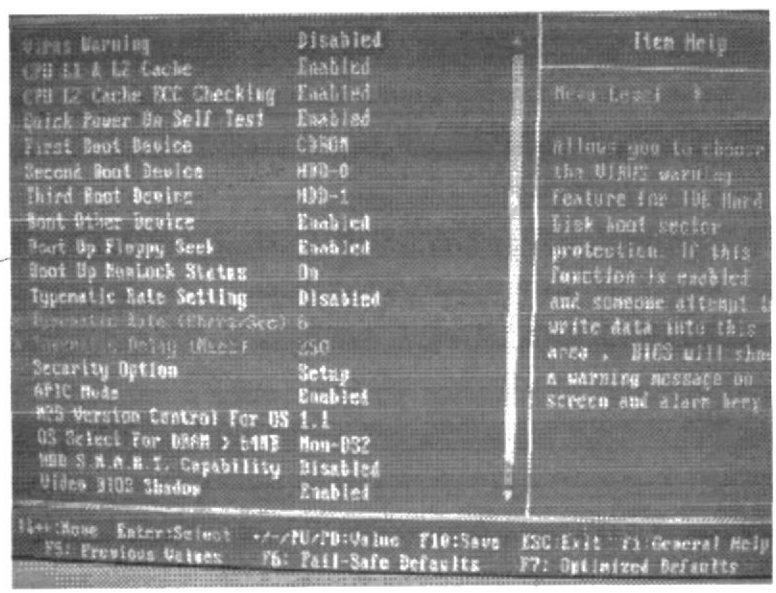


Figura 6-5: Configuración de Buteo del Sistema

BIBLIOTECA CAMPUS PEÑAS

Pulse **ESC** y se mostrará la siguiente pantalla, **Quit Without Saving (Y/N)** y se pulsa la letra **Y** para salir y grabar los cambios realizados.

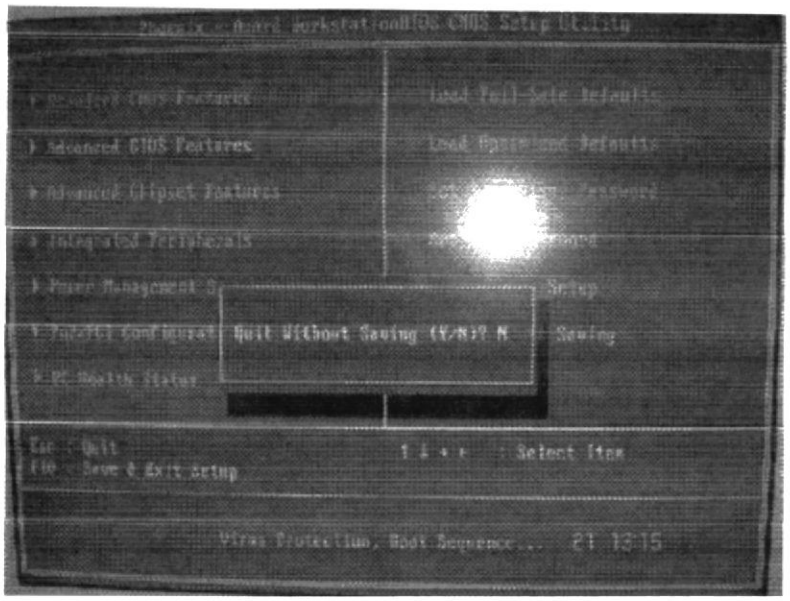
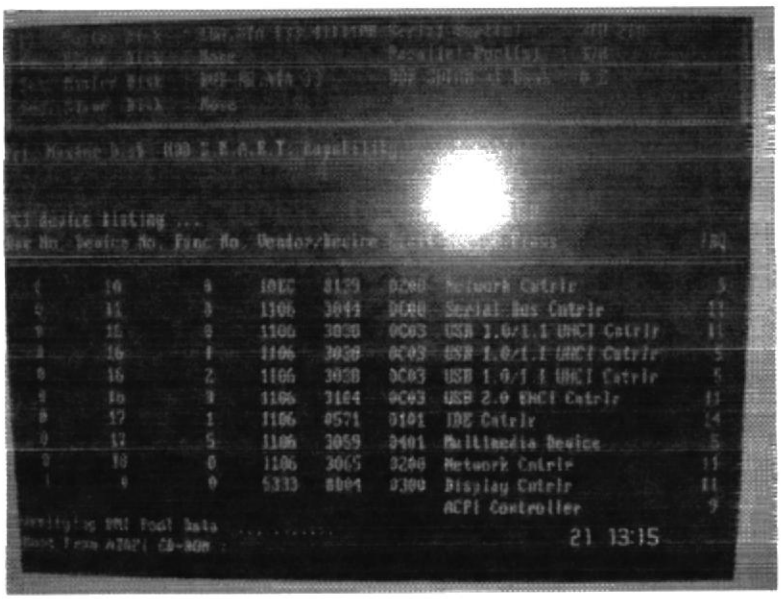


Figura 6-6: Guardar cambios y salir de la Configuración del Setup

Luego la computadora buteará desde el CD-ROM donde estará listos para instalar Linux.



ESPOL
BIBLIOTECA
CAMPUS

Figura 6-7: Reiniciación del Computador

6.4. INSTALACIÓN DE FEDORA CORE 3

1.- Como primer paso se ingresa el primer disco de instalación en la unidad de CD-ROM/DVD-ROM. Luego aparecerá la pantalla de booteo de Fedora Core 3, la misma que contiene **boot:** _ en la parte final.

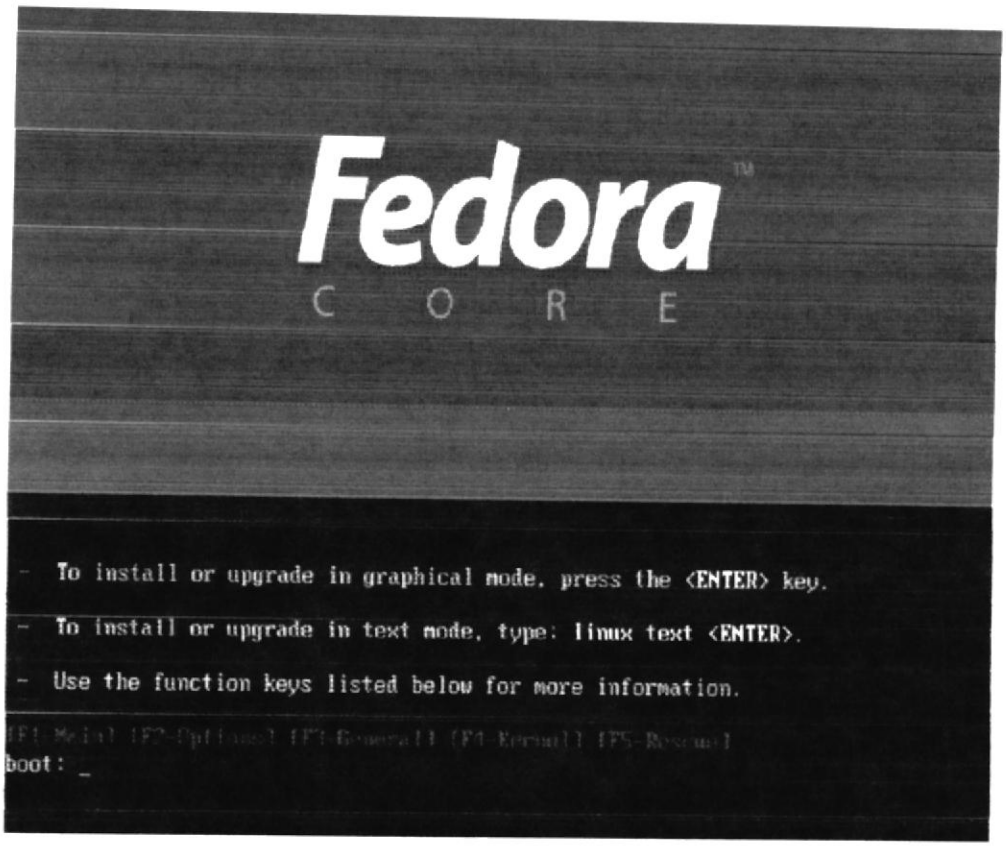
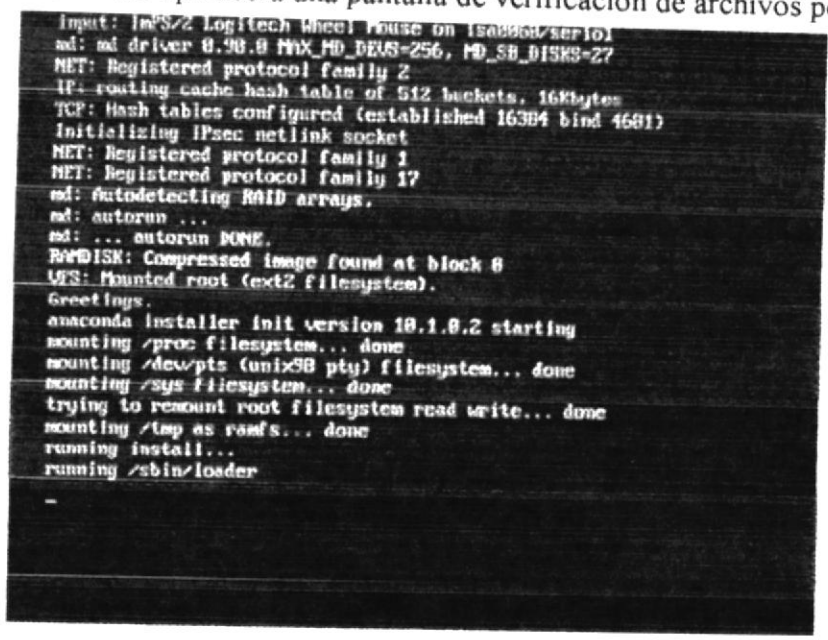


Figura 6-8: Fedora Boot

Presionar **Enter**, para comenzar la instalación por defecto, es decir en una interfaz gráfica ya que también se puede instalar Linux en interfaz de texto digitando al final donde se encontrará la palabra boot: _ Linux text.

ESPOL
BIBLIOTEC
CAMPUS
PEÑAS

Una vez pulsado **Enter** aparecerá una pantalla de verificación de archivos por defecto.



ESPOL BIBLIOTECA CAMPUS PENAS

Figura 6-9: Comienzo de la Instalación

2.- Después aparecerá la pantalla donde se encontrarán dos opciones:

- **OK.-** Que permitirá hacer la comprobación de los discos antes de la instalación.
- **Skip.-** Que evita la comprobación previa de los discos y empieza la instalación.

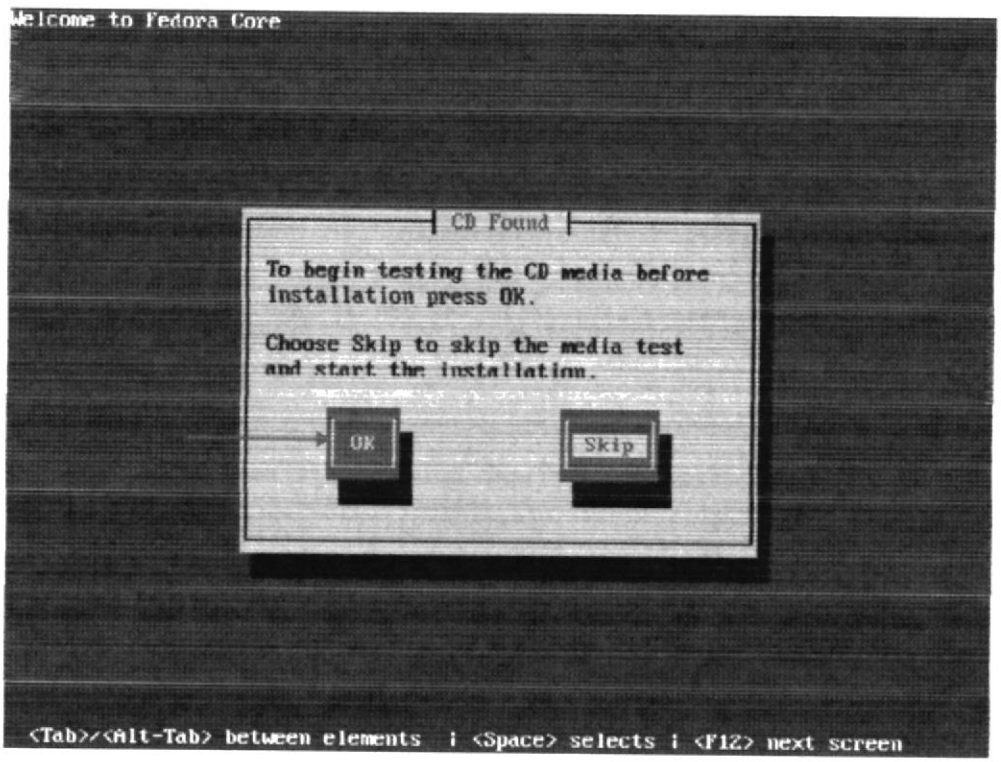


Figura 6-10: Comprobación de Discos

Al elegir la opción **OK** aparecerá la siguiente pantalla donde se encontrarán dos opciones:

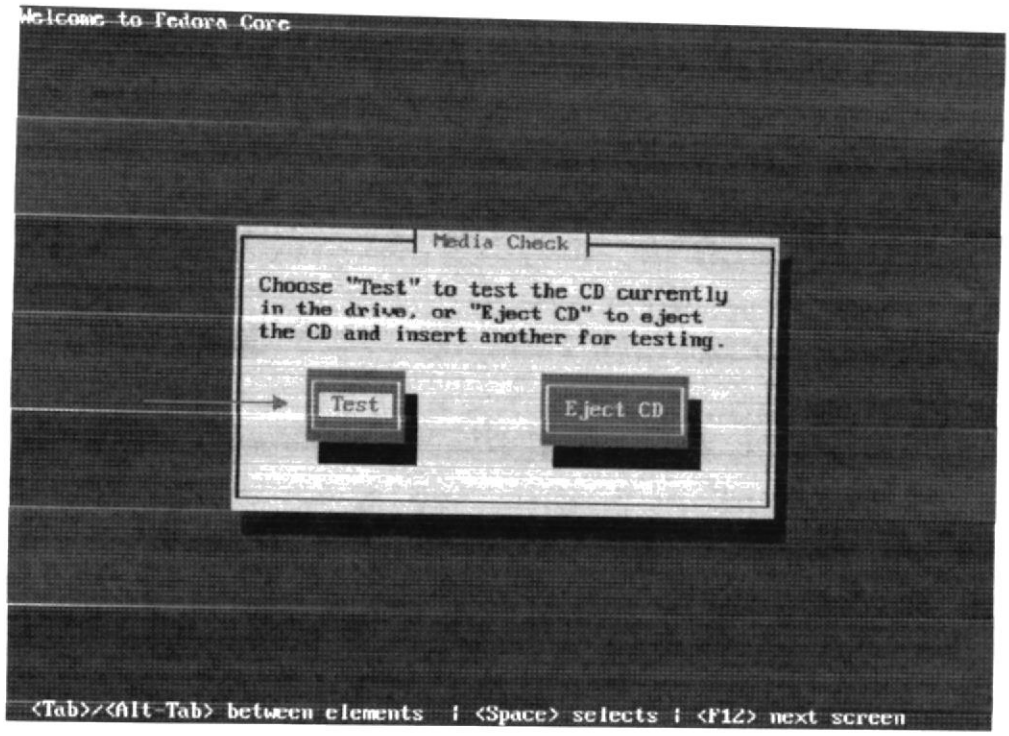


Figura 6-11: Elección de Comprobación de Disco

- **Test.-** La cual al seleccionarla comenzará la comprobación inmediata del disco del CD-ROM como se muestra en la siguiente pantalla.
- **Ejec. CD.-** La cual permite ingresar el otro disco de instalación si es que este no fuese el correcto.

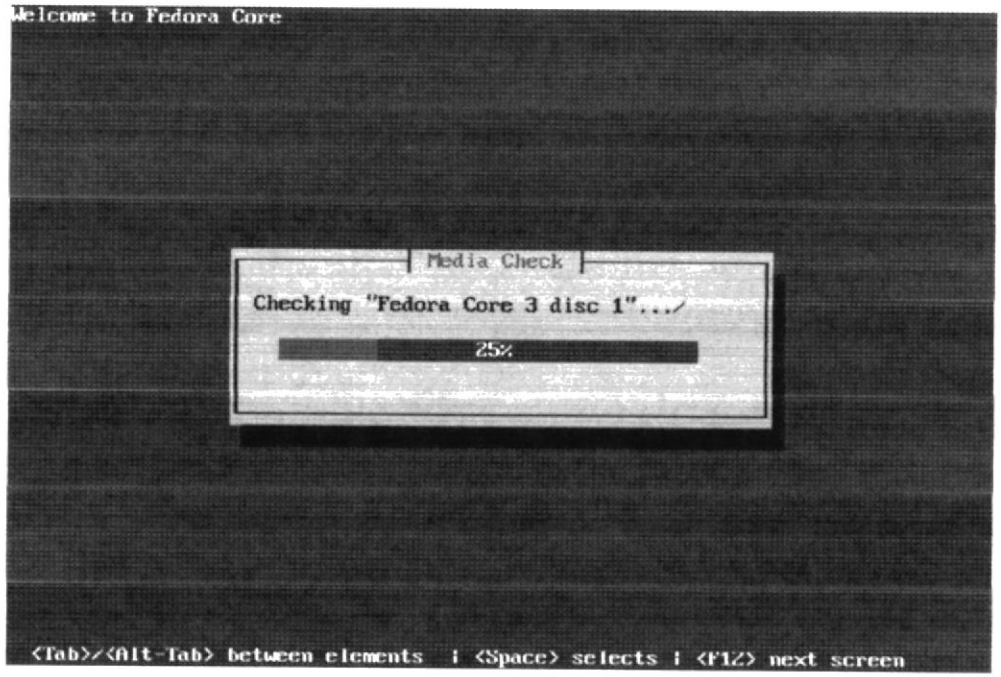
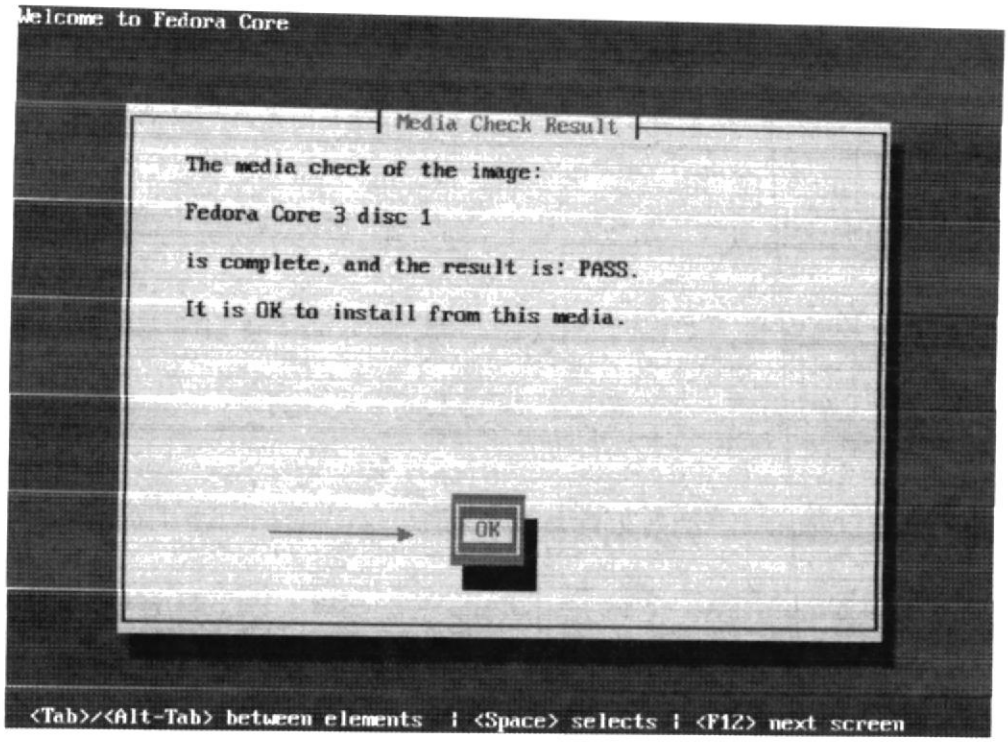


Figura 6-12: Chequeo de Discos

3.- Una vez que comprobado el disco y no a presentado ningún problema se mostrará la siguiente pantalla, y hacer clic en el botón **OK** para continuar con la instalación.



BIBLIOTECA CAMPUS PEÑAS

Figura 6-13: Aceptación de Comprobación de Discos

4.- En la siguiente pantalla aparecerán dos opciones:

- **Test.-** Permite hacer la comprobación del estado de los otros discos de Linux.
- **Continue.- P**ermite seguir con la instalación.

➢ Escoger la opción Continue.

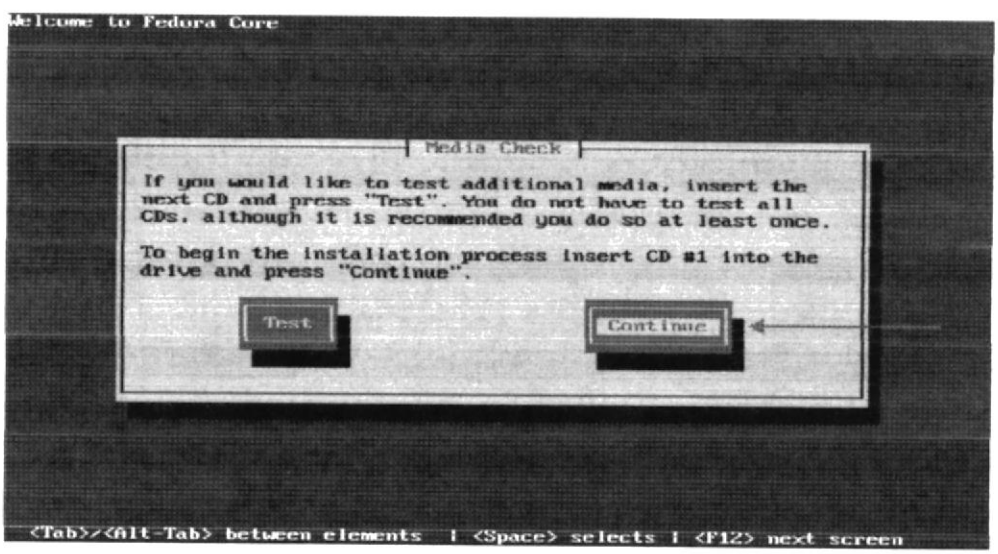
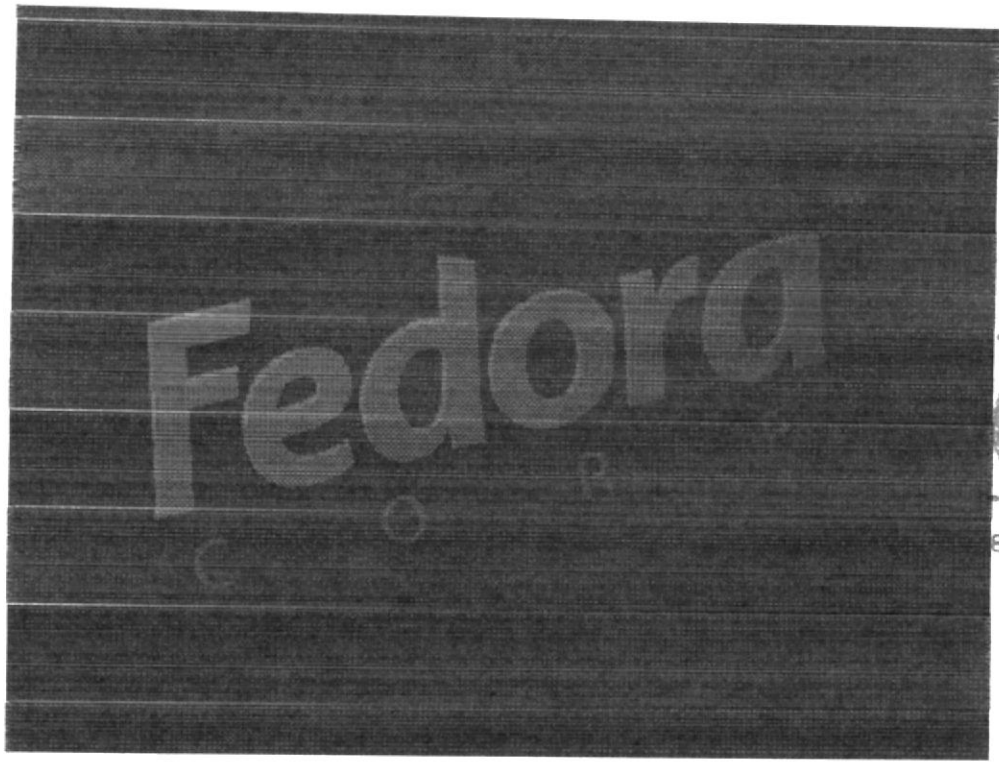


Figura 6-14: Selección del Proceso a Instalarse

- Una vez elegida la opción **CONTINUE** se mostrará la pantalla de bienvenida a Fedora Core 3.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 6-15: Presentación Inicial de Instalación

- En esta pantalla se pulsa el botón **next** para continuar con la instalación.

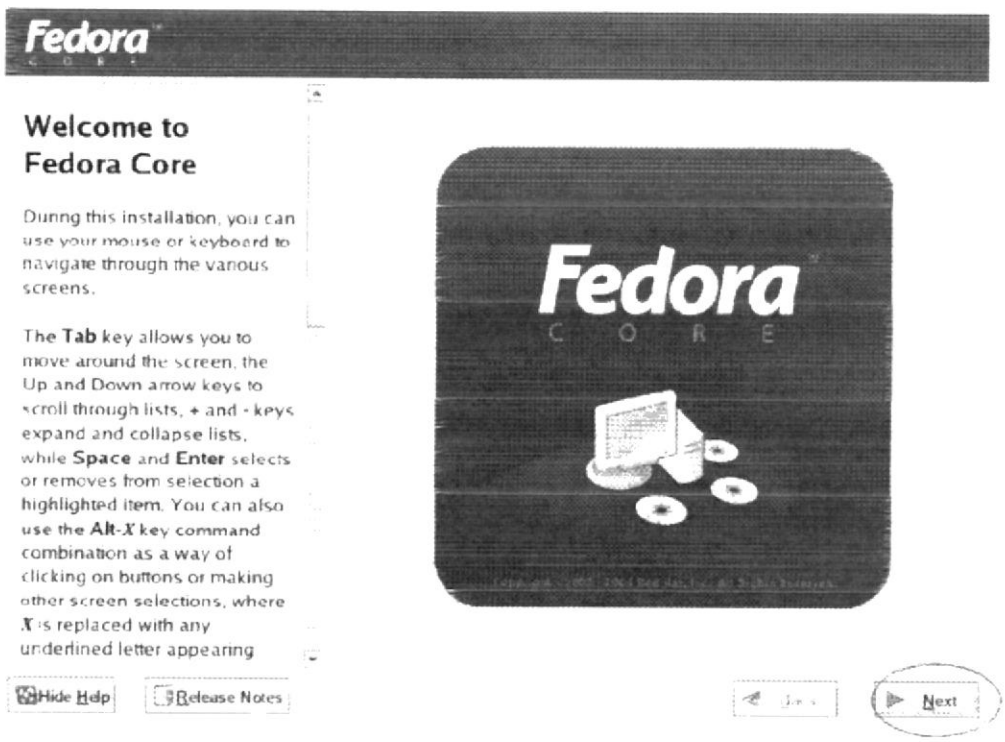


Figura 6-16: Bienvenida a Fedora Core

5.- Luego de la página de bienvenida aparecerá la pantalla que muestra la lista de idiomas que se utilizan durante la instalación Fedora Core 3.

- En esta pantalla se selecciona a seleccionar el idioma Español (Español) y se pulsa **NEXT**.

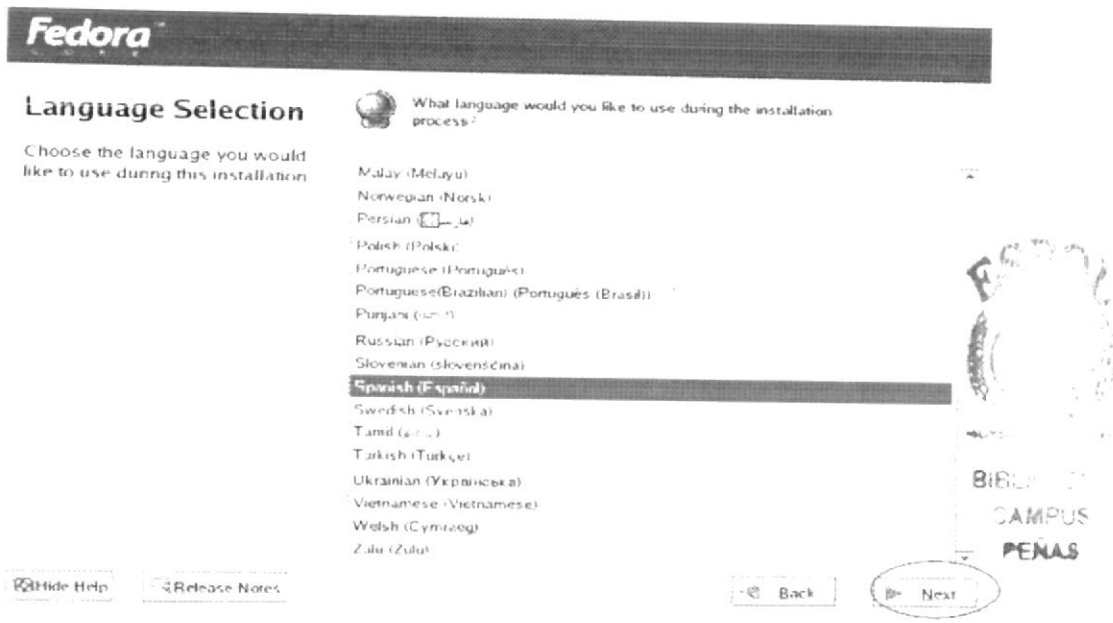


Figura 6-17: Selección de Lenguaje

En esta pantalla se muestra el tipo de teclado que desea utilizar para el sistema Fedora Core 3.

- En esta pantalla selecciona la opción **SPANISH**, y de clic en el botón **Siguiente.**

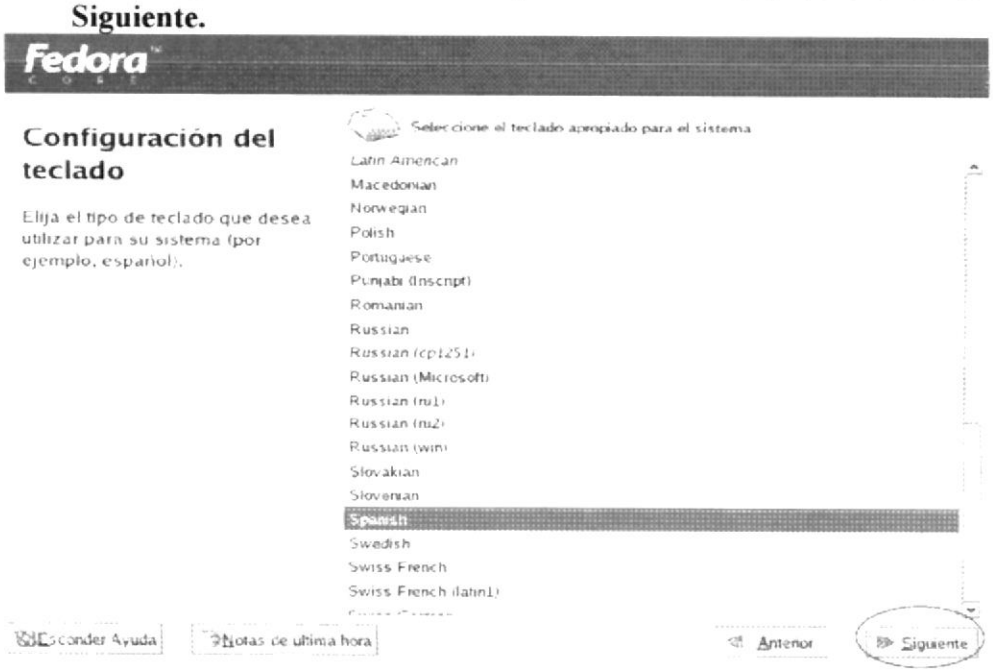


Figura 6-18: Configuración del Teclado

6.- En la siguiente pantalla se muestra el tipo de instalación que se va utilizar, cabe decir que esto dependerá de las necesidades que se desee cubrir.

Antes de escoger un tipo de instalación es necesario saber que ofrece cada una de las opciones.

- **ESCRITORIO PERSONAL**

  Este es el tipo de instalación por defecto. Esta instalación proporciona un ambiente de trabajo en forma gráfica con un paquete de utilitarios de oficina, aplicaciones de Internet y programas Multimedia.

- **ESTACIÓN DE TRABAJO**

  Este tipo de instalación incluye los programas que contiene el tipo de instalación de Escritorio Personal, y agrega programas para desarrollo y administración de sistemas. Escoja este tipo de instalación si usted necesita compilar programas desde el código fuente.

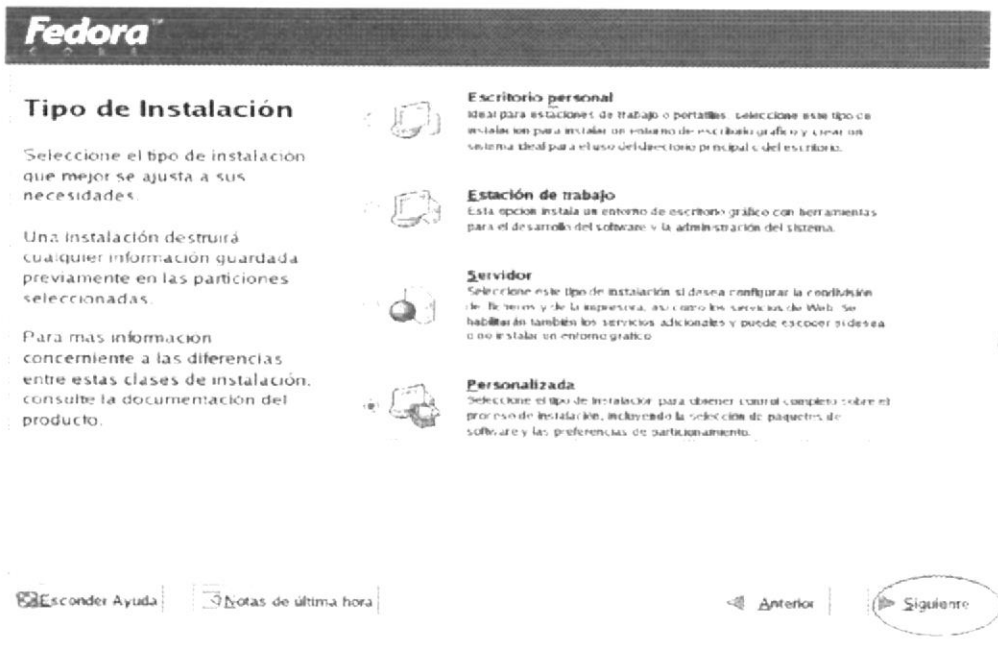
- **SERVIDOR**

  Este tipo de instalación provee de servidores de red como los servicios de Servidor Web Apache y el Servidor Samba, y herramientas de administración. Este tipo de instalación no suministra entorno gráfico por defecto.

- **PERSONALIZADO**

  Este tipo de instalación no abastece de ninguna partición en el disco. Este tampoco incluye ningún programa adicional que los que proporciona el tipo de instalación Escritorio Personal. Si usted elige la instalación personalizada, el programa de instalación mostrará diálogos para esas selecciones durante el proceso de instalación.

Con el fin de poder seleccionar los paquetes que se van a instalar, escoja el tipo de instalación Personalizado. Presione **Siguiente** una vez hecha la selección.

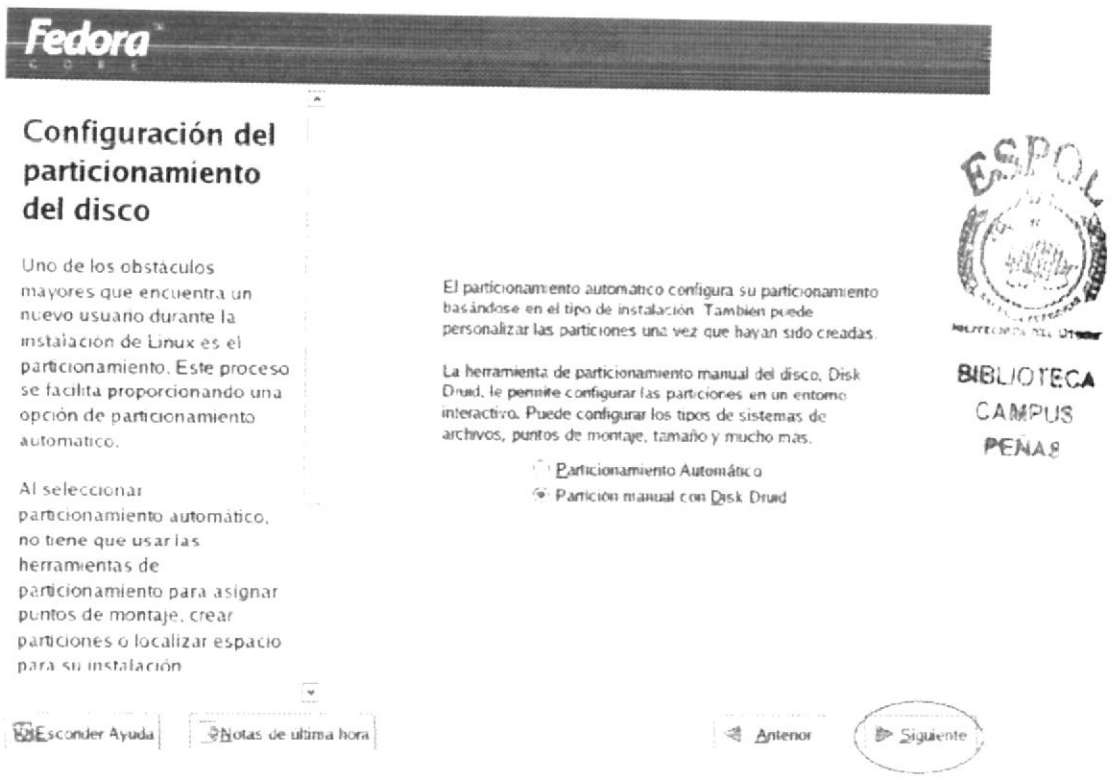


ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 6-19: Tipo de Instalación

7.- En la siguiente pantalla se muestra dos opciones de particionamiento las cuales son:

- Partición Automática.
- Partición manual.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 6-20: Configuración del Particionamiento del Disco

ELECCIÓN DE PARTICIÓN AUTOMÁTICA

Escoja Partición Automática en el menú de particiones para usar una partición Pre-configurada. Entonces Disk Fruid muestra opciones adicionales:

- **Retirar todas las particiones Linux en el sistema.-** Extrae todas las particiones de Linux ext2, ext3 y swap de todos los discos duros.

- **Retirar todas las particiones en este sistema.-** Es decir las particiones de todo el disco duro.

- **Mantener todas las particiones y usar el espacio libre.-** Usa solamente el espacio no particionado en los discos duros para instalar Fedora Core 3.

ELECCIÓN DE PARTICIÓN MANUAL

Para particionar el disco solamente, escoja Partición Manual con disk Druid. Elija este método si usted necesita una configuración de particiones especial.

Información General sobre las particiones
Un sistema Fedora Core 3 tiene tres particiones:

- Una partición de información montada /boot
- Una partición de información montada /
- Una partición swap

ESPOL BIBLIOTECA CAMPUS PEÑAS

Algunos sistemas tienen más particiones que las mínimas listadas anteriormente. Escoja particiones basadas particularmente en las necesidades de su sistema.

La información tiene un punto de montaje. El punto de montaje indica el contenido que se aloja en esa partición. Una partición sin punto de montaje no es accesible por los usuarios. Información no ubicada sobre alguna otra partición se aloja en al partición /o (root).

- Una vez que se elije la opción que se desea, aparecerá la siguiente pantalla. En este caso se elije la Partición Manual y hacer clic en **Siguiente**.

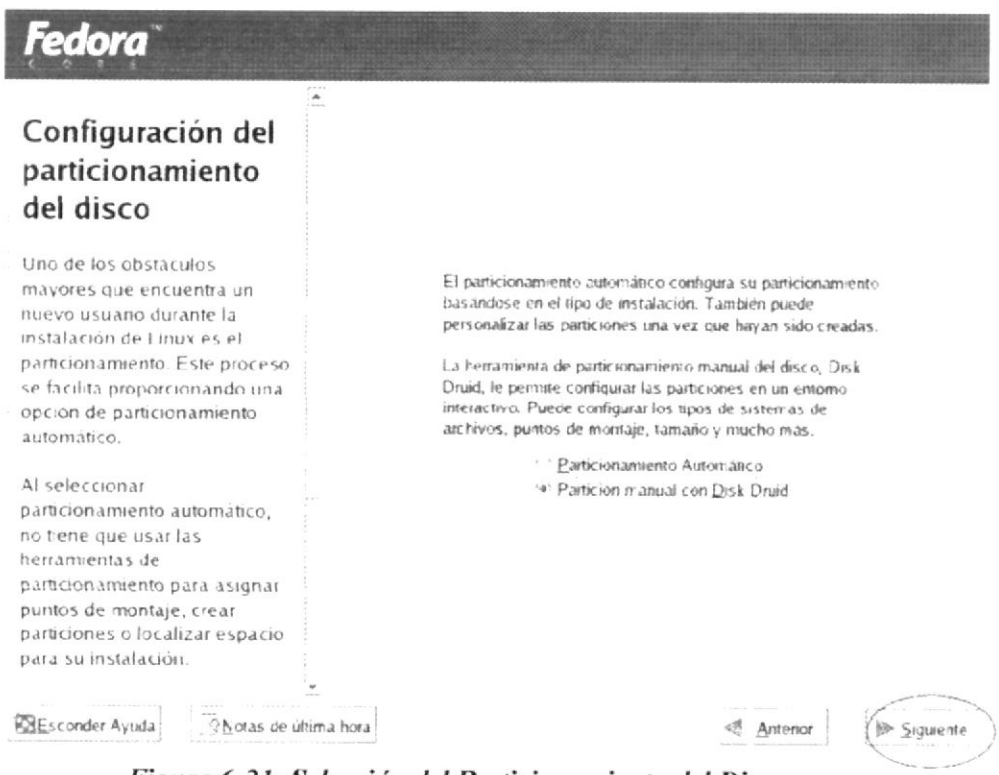


Figura 6-21: Selección del Particionamiento del Disco

8.- En esta pantalla de la instalación es donde se va a crear las particiones donde se va alojar el sistema operativo.

En esta pantalla se encuentran diferentes botones como los siguientes:

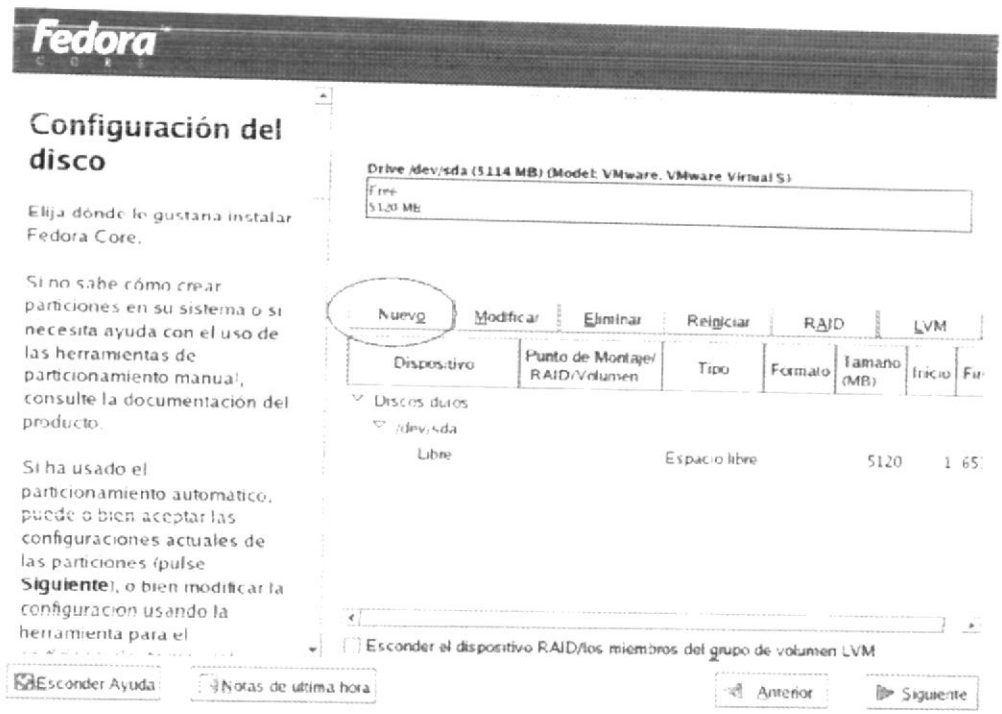


Figura 6-22: Configuración del Disco

a.- Nuevo

Seleccione esta opción para agregar una nueva partición o volumen fisico LVM al disco. En el dialogo de añadir partición elija un punto de montaje y un tipo de partición. Si usted tiene más de un disco en el sistema. Elija en cual de los discos la partición se creará. Indique un tamaño en megabytes para la partición.

ESPOL BIBLIOTECA CAMPUS PEÑAS

- **Tamaño fijo.-** Utiliza un tamaño fijo de acuerdo con su partición.
- **Complete hasta el tamaño máximo permitido.-** Incremente la partición hasta que llene los discos seleccionados.
- **Tamaño de las particiones.-** la partición actual sobre el disco puede ser levemente más pequeña o más grande que su elección. Las ediciones de la geometría del disco causan este efecto, no es un error o un bug

b.- Modificar

Seleccione esta opción para editar una partición existente, grupo de volumen LVM, o un volumen fisico LVM que todavía no es parte de un grupo de volumen.
Para cambiar el tamaño de una partición de volumen fisico LVM, primero retírelo de cualquier grupo de volumen.

- **Quitando volúmenes físicos de la LVM.-** si se remueve un volumen fisico del LVM desde un grupo de volumen, usted borrará cualquier volumen lógico que contenga.

Edite una partición para cambiar su tamaño, punto de montaje, o el tipo de sistema de archivos. Utilice esta función para:

1. Corrige errores en al configuración de las particiones.
2. Emigrar particiones Linux si usted esta actualizando o reinstalando Fedora Core 3.
3. Poporcione un punto de montaje para particiones que no son de Linux tales como las usadas en los sistemas Operativos Windows.

- **Particiones Windows.-** si no puede etiquetar las particiones Windows que utilizan el sistema de archivos NTFS con un punto de montaje en el instalador de Fedora Core 3. Usted puede etiquetar particiones VFAT (FAT16 o FAT32) con un punto de montaje.



Si su sistema contiene muchas particiones separadas para los datos del usuario del sistema, seria más fácil actualizar el sistema. El programa de instalación le permite borrar o conservar datos en particiones específicas. Si los datos de usuario están sobre una partición /home separada, usted puede conservar esos datos mientras elimina particiones del sistema como /boot.

c. **Eliminar**

Seleccione esta opción para borrar una partición existente o un volumen físico LVM. Para eliminar un volumen físico LVM, primero elimine cualquier grupo de volumen de la cual ese volumen físico es miembro.

Si usted comete un error, utilice la opción reiniciar para renunciar a todos los cambios que usted ha realizado.

d. **Reiniciar**

Seleccione esta opción para forzar a Disk Druid para reiniciar a todos los cambios realizados a las particiones del disco

e. **LVM**

Seleccione este botón para instalar LVM en su sistema Fedora Core. Primero cree por lo menos una partición o dispositivo de programa RAID como un volumen físico LVM, usando el nuevo dialogo.

Para asignar uno o más volúmenes físicos a un grupo de volumen, primero nombre el grupo de volumen. Entonces seleccione los volúmenes físicos para ser utilizados en el grupo de volumen. Finalmente, configure los volúmenes lógicos en cualquier grupo de volumen usando las opciones Agregar, Modificar y Borrar.

Una vez que ya se conoce las funciones de cada uno de los botones que aparecen en la pantalla de configuración de discos se procede a crear las particiones debidas.
La primera partición a crear es la raíz la cual se representa con un / y es la partición principal, donde se guardará todo el sistema de archivos. A esta partición se le asigna el valor por ejemplo **(4000MB)**, y hacer clic en el botón **Aceptar**.

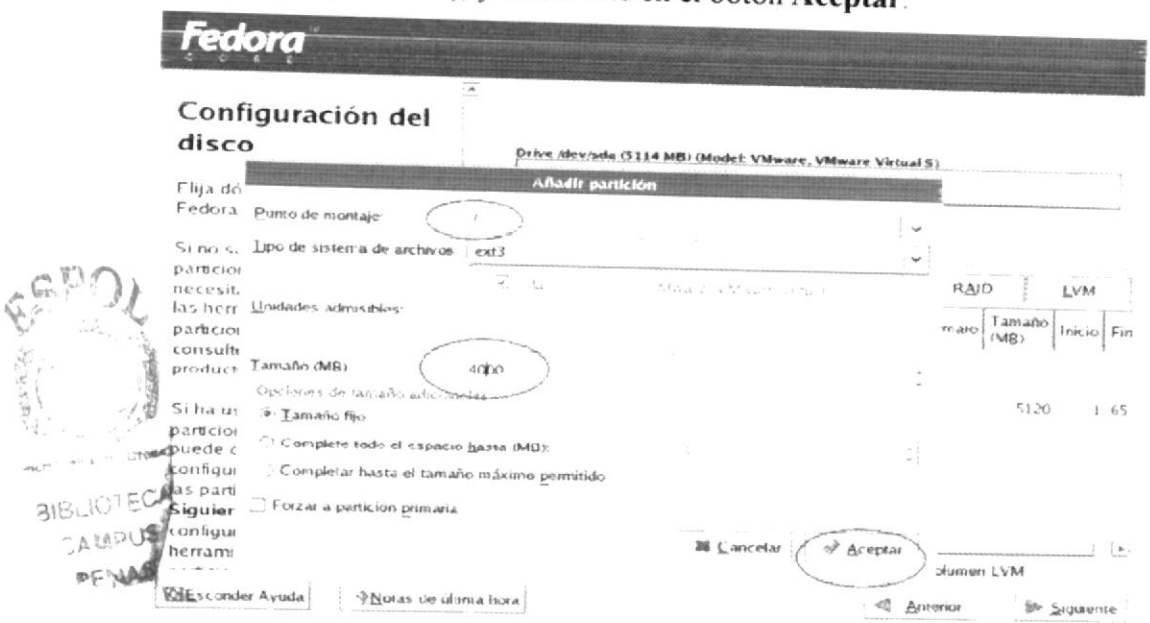


Figura 6-23: Punto de Montaje Raíz

La segunda partición que se crea es la **swap**, la cual sirve como una extensión de memoria virtual. Su tamaño duplica la cantidad de **memoria Ram** que tenga el computador. A esta partición se le asigna **512MB** que es el tamaño mínimo. Una vez introducido estos valores hacer clic en **Aceptar**.

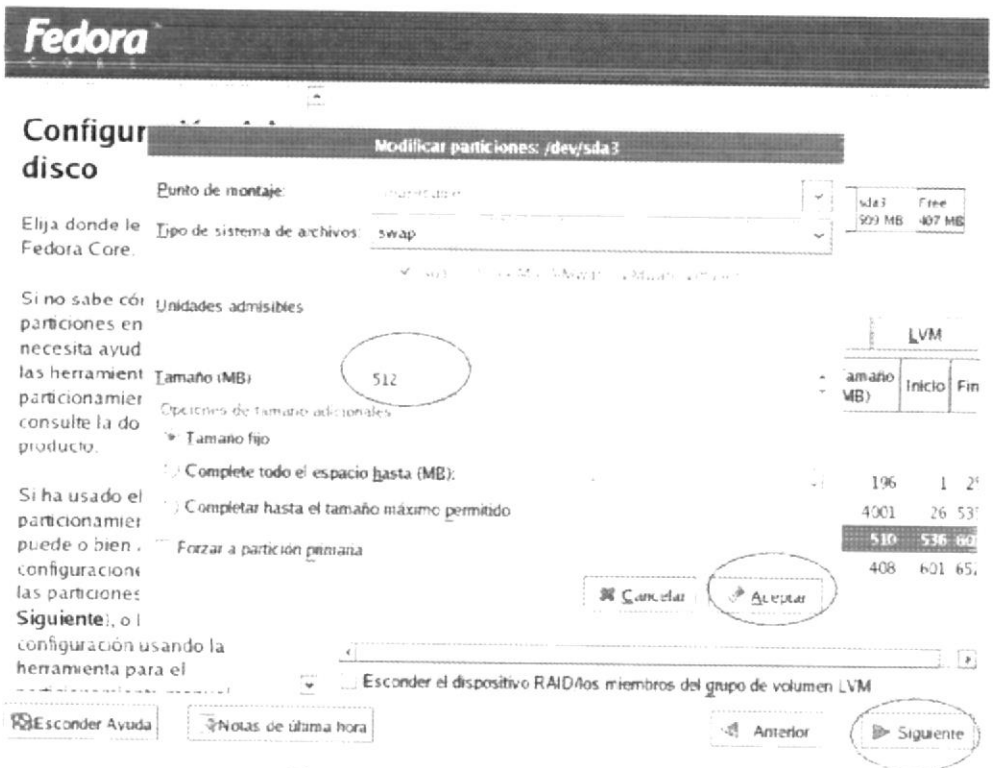


Figura 6-24: Modificar Particiones Swap

La última partición que se crea es la **/boot** la cual sirve de ayuda cuando se instala otro sistema operativo en la misma computadora. A esta partición se le asigna **200MB** que es el tamaño mínimo. Una vez introducido estos valores se debe hacer clic en **Aceptar**.

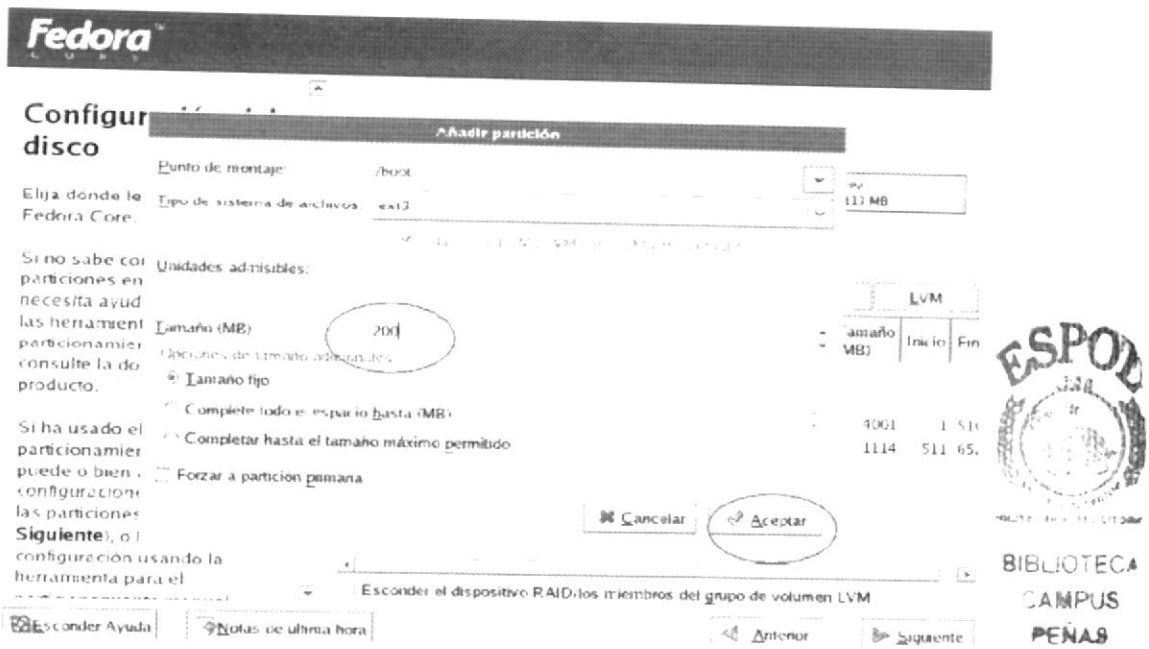


Figura 6-25: Punto de Montaje Boot

9.- Luego de crear las particiones en la siguiente pantalla se tiene una opción de configurar el gestor de arranque el cual se configura únicamente si se tiene instalado más de un sistema operativo en el mismo disco caso contrario se da clic en siguiente.

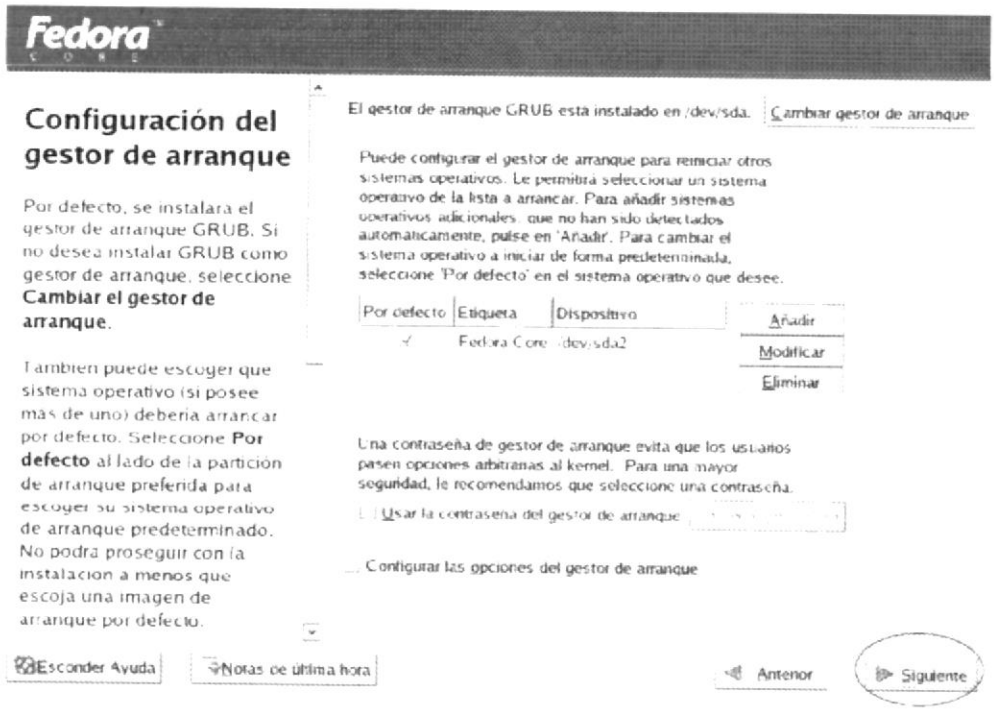


Figura 6-26: Configuración del Gestor de Arranque

10.- Después de configurar el gestor de arranque si el caso lo amerita, aparecerá la pantalla de configuración de dispositivos de red en la cual dejar todo por default y hacer clic en **Siguiente**.

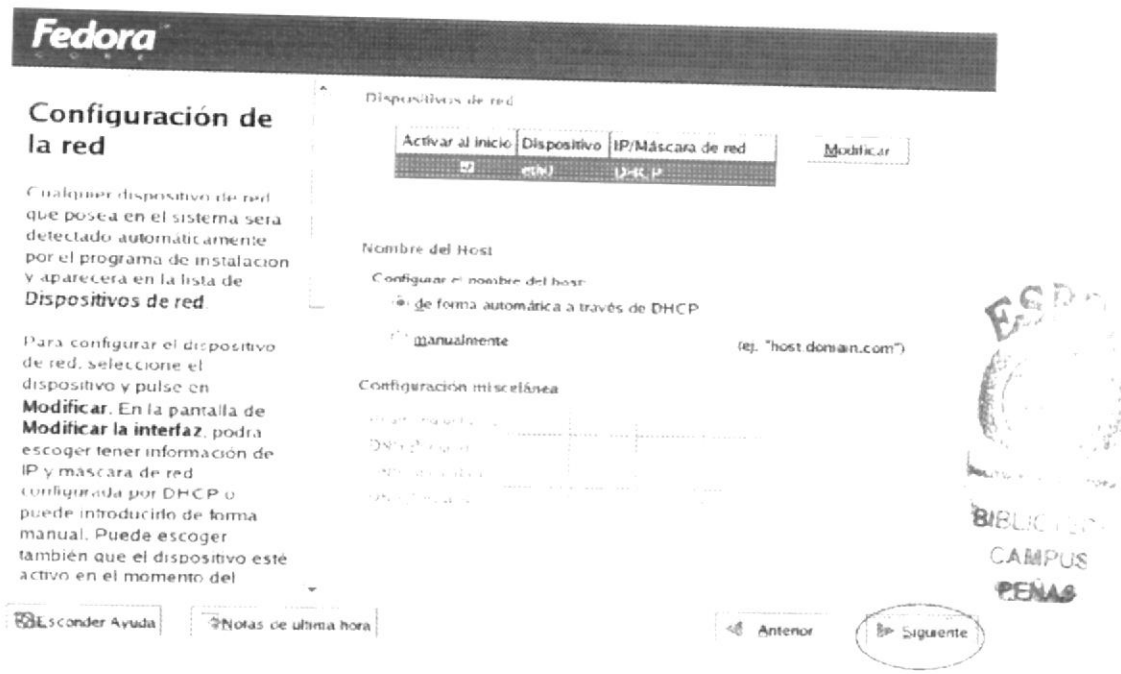


Figura 6-27: Configuración de Red

11.- En la siguiente pantalla se pueden configurar los firewalls. En este caso se deja deshabilitado los firewalls lo cual provee acceso total al sistema y no realiza controles de seguridad, luego pulsar **Siguiente.**

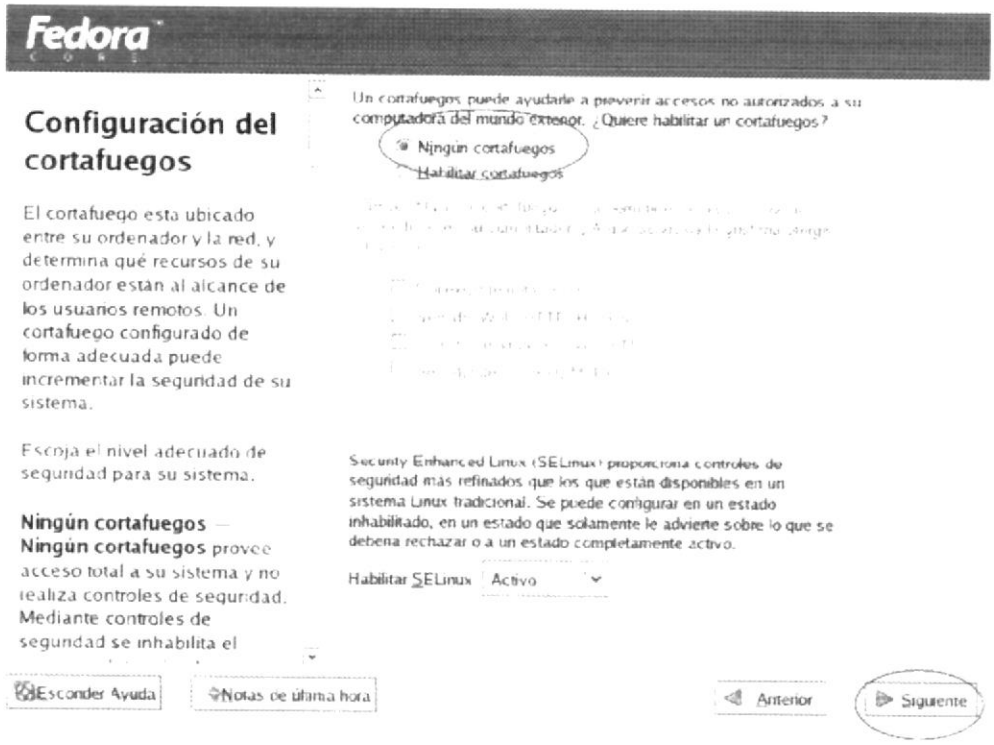
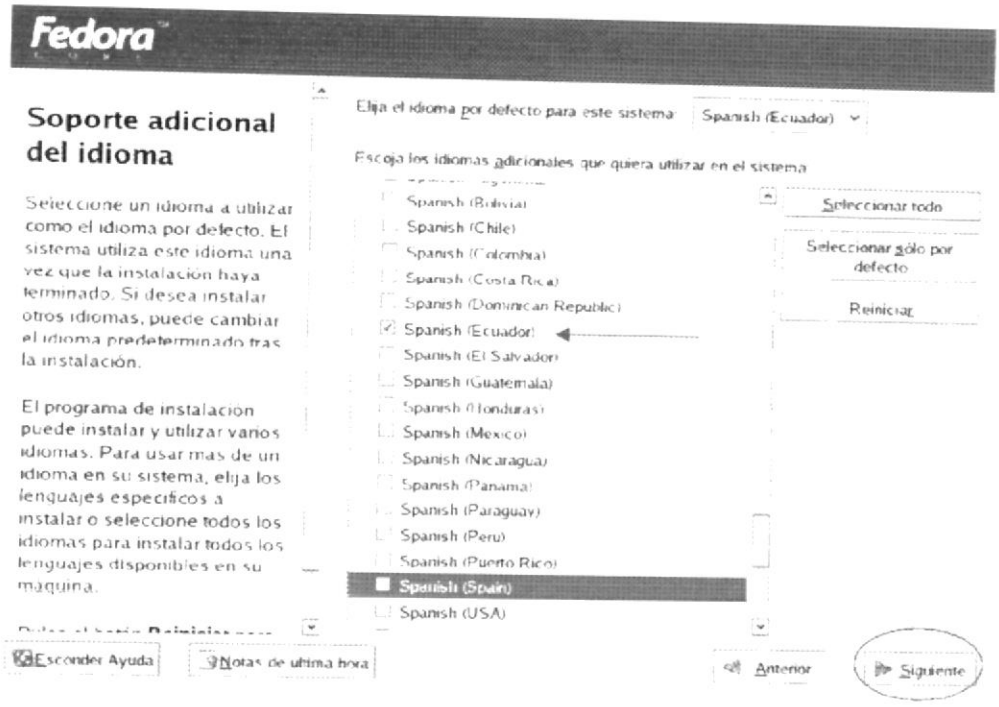


Figura 6-28: Configuración del Cortafuegos

12.- Una vez que a elegido la opción en la pantalla anterior en este caso ningún cortafuego, se procede a elegir la opción de soporte adicional de idioma donde se elige la opción de Spanish/Ecuador.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 6-29: Soporte Adicional del Idioma

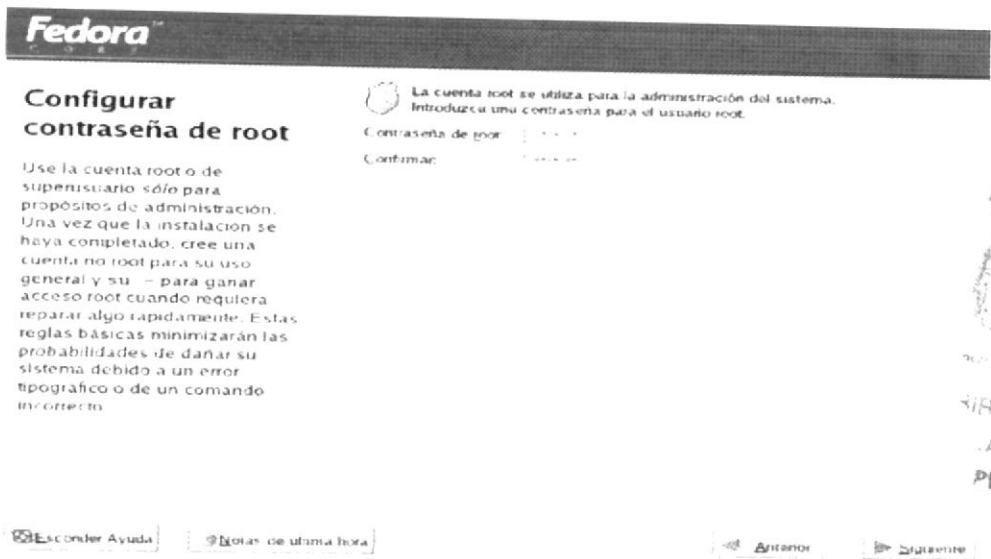
13.- Luego se elije la opción de soporte adicional del idioma, se configura la zona horaria en la cual se elije la opción América/Guayaquil y hacer clic en **Siguiente.**



Figura 6-30: Selección del Huso Horario

14.- Después de configurar la zona/horaria aparecerá la pantalla donde se va asignar la contraseña al usuario root, para seguir con la instalación.

Fedora utiliza una cuenta especial nombrada root para la administración del sistema. La cuenta root sobre cada sistema Linux es limitada solamente para SELINUX. Este no esta sujeta a ninguna otra restricción normal. Como el propietario o administrador del sistema. En esos casos, utilice la cuenta root.



ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 6-31: Configuración de la Contraseña de Root

15.- Después de configurar la opción de la contraseña para al usuario root, en la pantalla que se muestra a continuación se selecciona los paquetes que se van a necesitar en nuestro servidor Linux y se pulsa el botón siguiente.

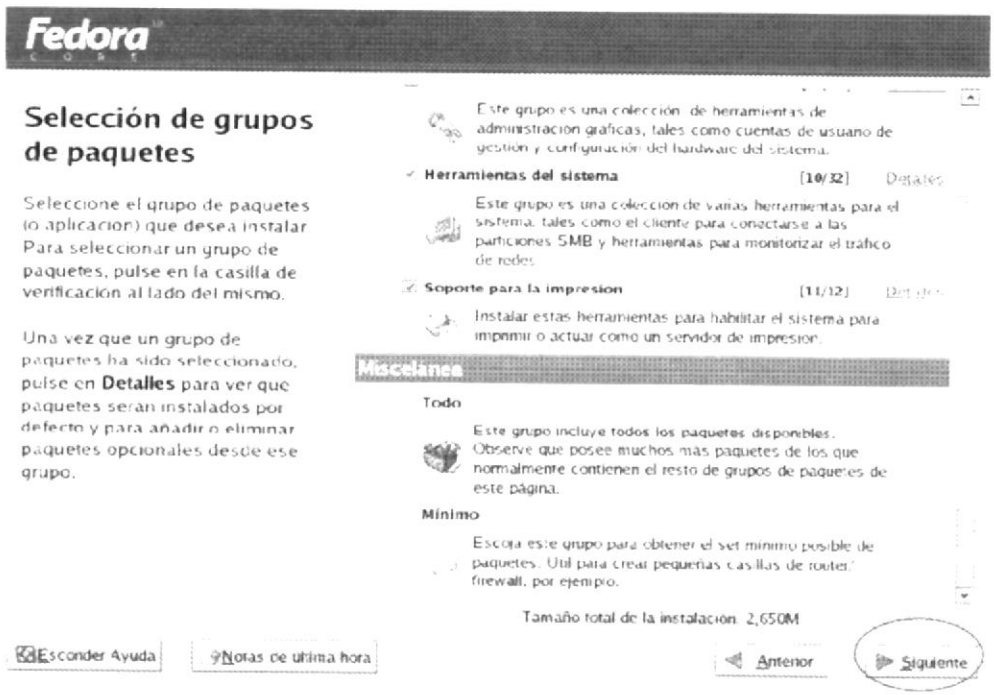


Figura 6-32: Selección de Grupos de Paquetes

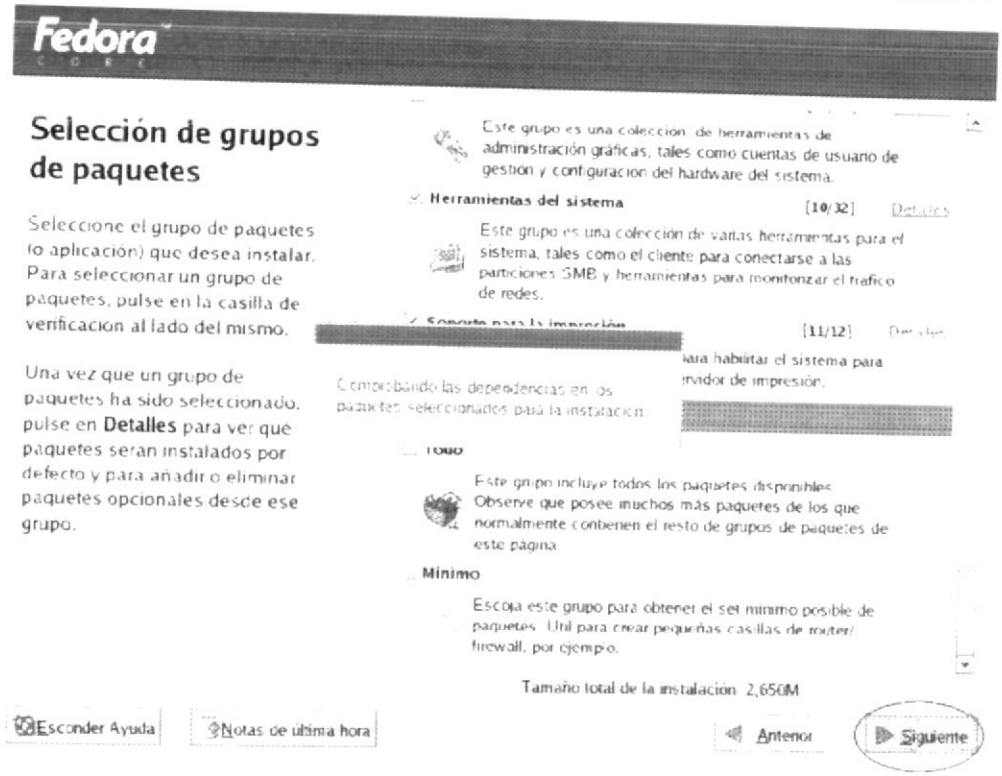
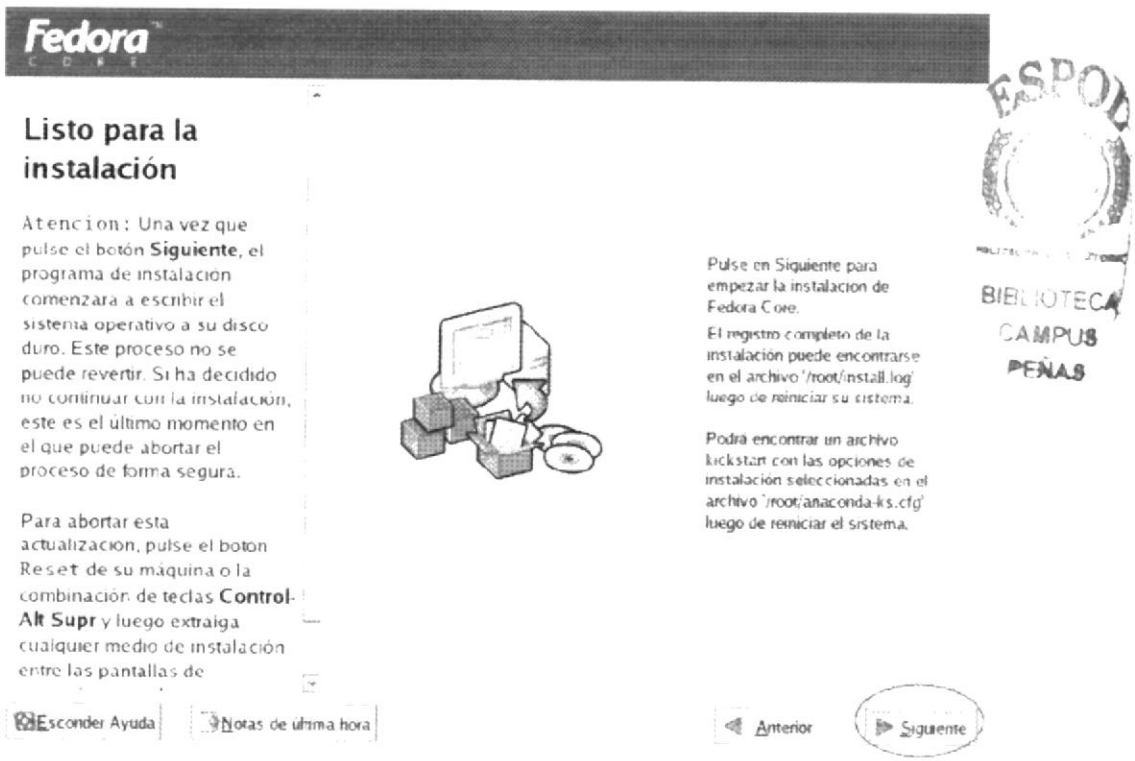


Figura 6-33: Aceptación de Grupos de Paquetes

16.- En la siguiente pantalla se muestra la pantalla de inicio de instalación la cual puede demorar dependiendo de los paquetes que se haya elegido para instalar. A continuación hacer un clic en **Siguiente**, para empezar la instalación.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 6-34: Listo para la Instalación

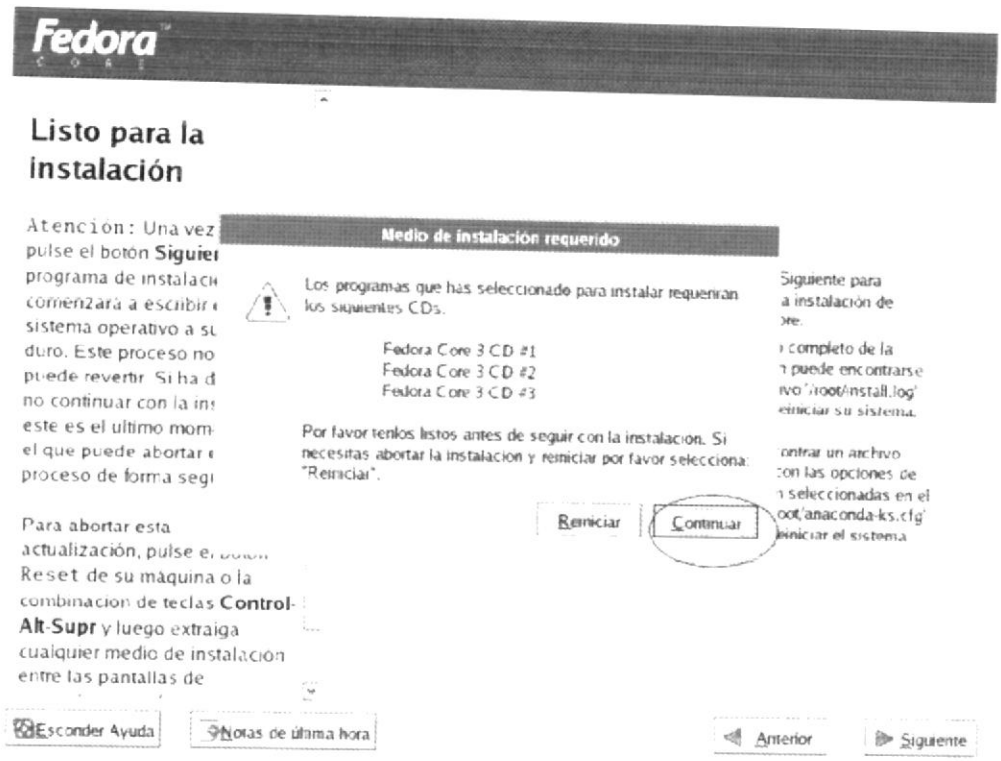
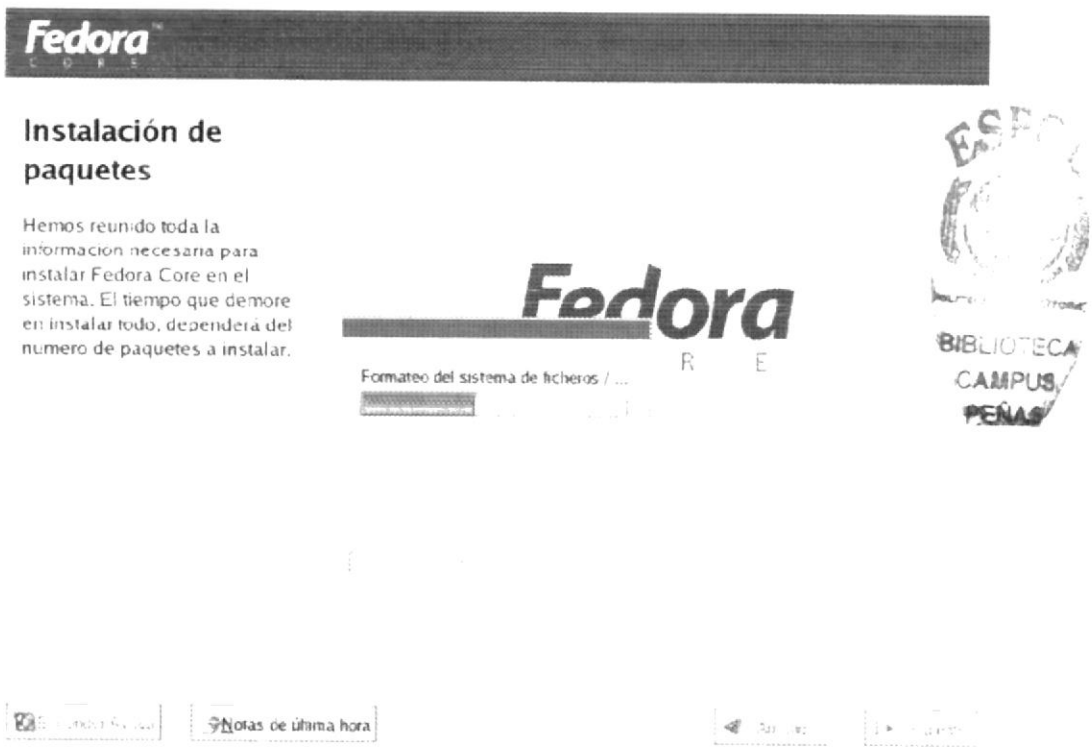


Figura 6-35: Medio de Instalación Requerido

17.- Ahora empezará la instalación de todos los paquetes elegidos conforme la instalación avance, el sistema de instalación, comenzará a pedir que se inserte en la bandeja de CR – ROM los CD siguientes para terminar la instalación con éxito.



BIBLIOTECA CAMPUS PEÑAS

Figura 6-36: Formateo del Sistema de Ficheros

La instalación de paquetes reune toda la información necesaria para instalar Fedora Core en el sistema.

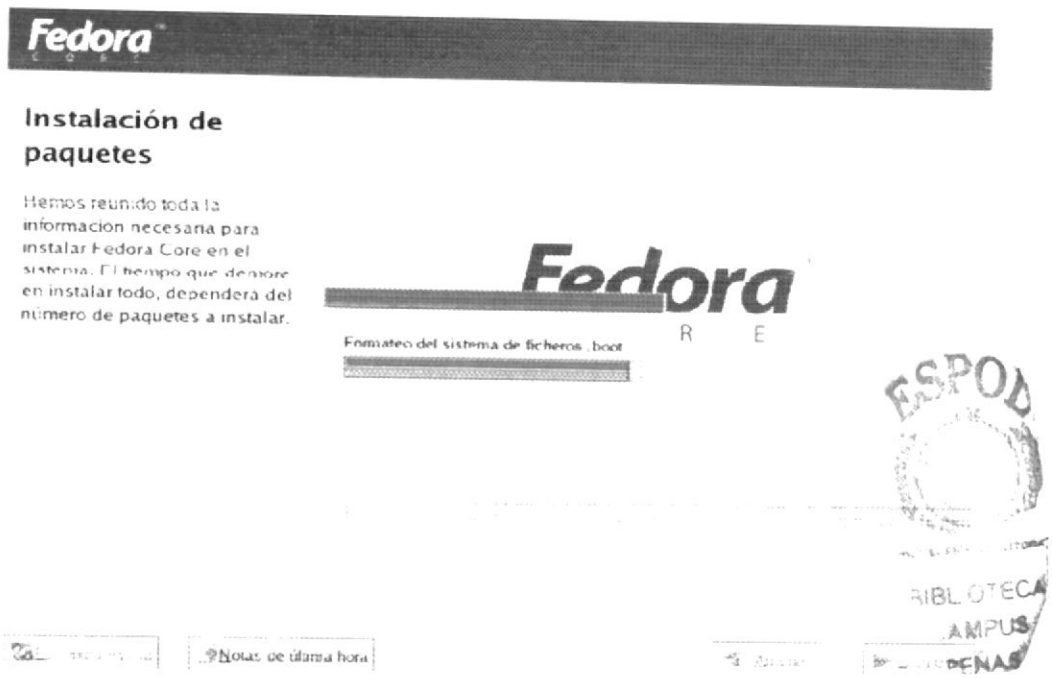


Figura 6-37: Finalización del Formateo de Ficheros

En esta pantalla se muestra la instalación de los paquetes y conforme se vayan grabando los paquetes, se irán pidiendo el ingreso de los demás CD de instalación.

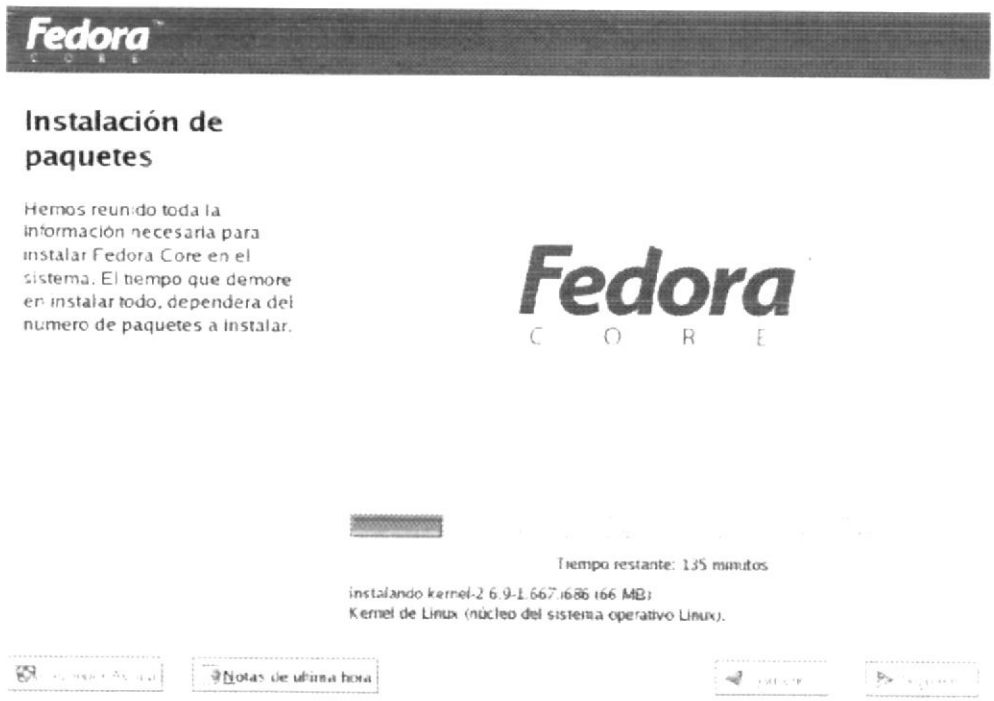


Figura 6-38: Instalación de Paquetes

Luego de que se haya completado la instalación, aparecerá la siguiente pantalla donde se va a elegir la opción de reiniciar para restaurar el equipo. Fedora Core expulsa cualquier disco cargado antes de que el computador se reinicie.

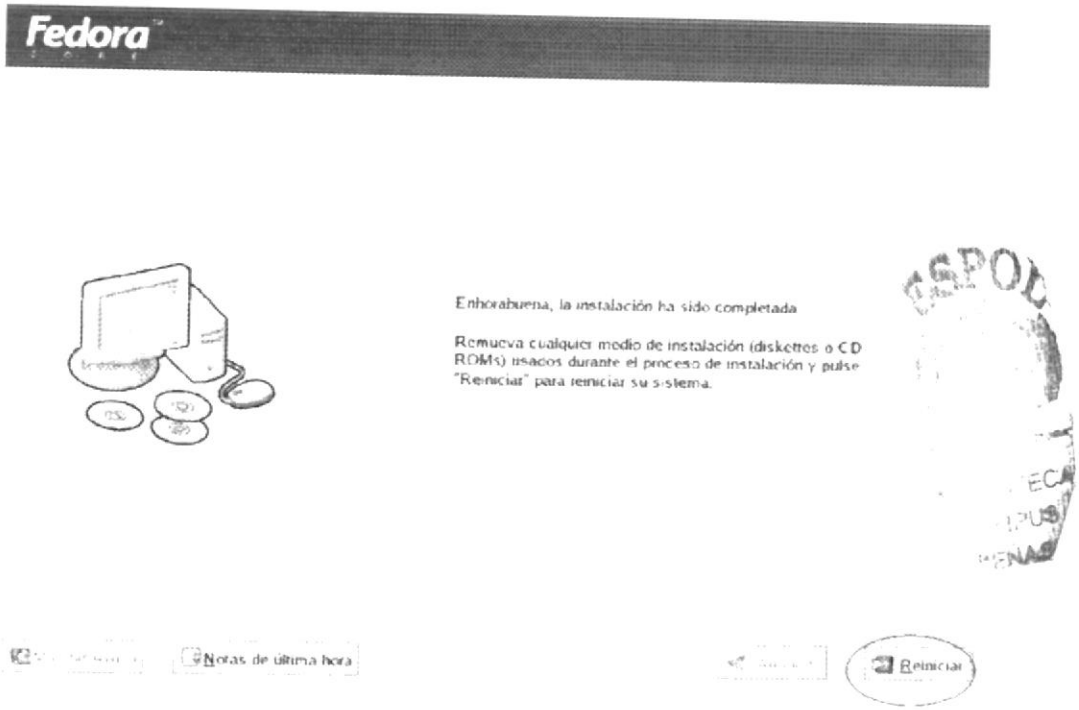


Figura 6-39: Finalización de la Instalación

En este momento se ha terminado la instalación de todos los paquetes de Linux. Ahora queda por configurar ciertos dispositivos. Luego de que cargue el sistema por primera vez aparecerá la pantalla donde se comienza a cargar Linux.

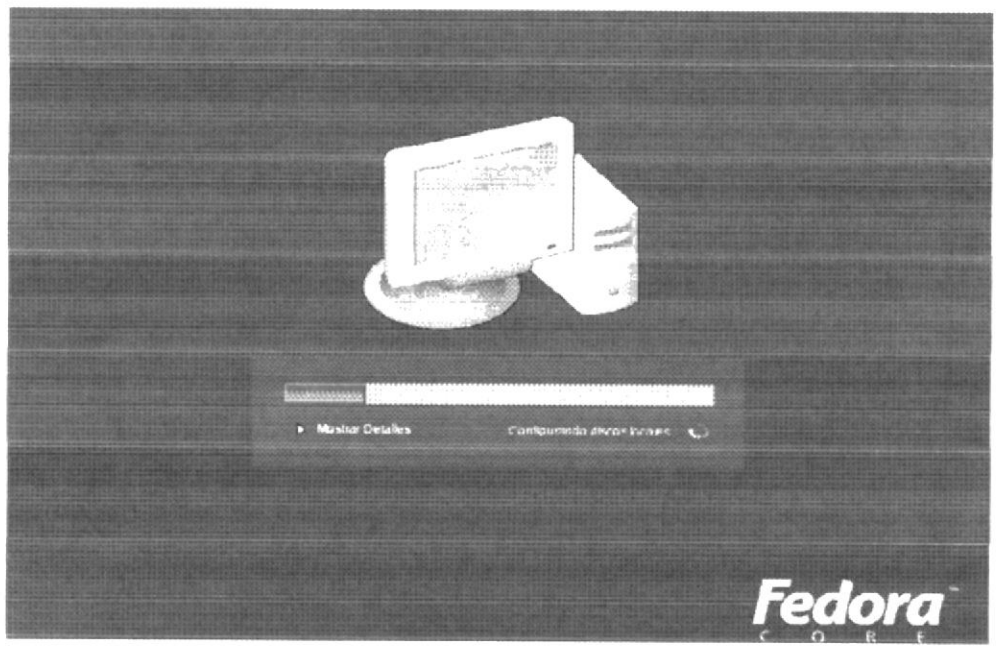


Figura 6-40: Inicio del Sistema Operativo Instalado

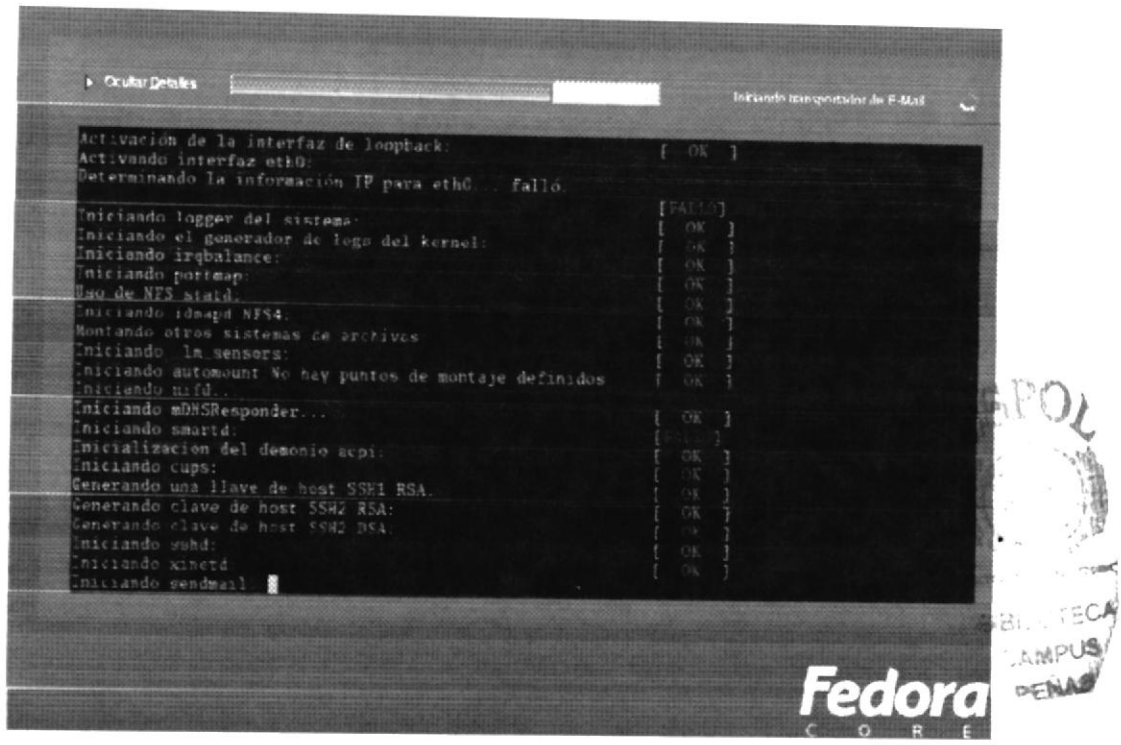


Figura 6-41: Inicialización de los Servicios del Sistema

6.4.1 CONFIGURACIÓN POST INSTALACIÓN DE LINUX FEDORA CORE 3

La siguiente pantalla muestra la bienvenida a una post-instalación de Linux.



Figura 6-42: Bienvenida al Sistema

En esta pantalla se muestra los términos de licencia que contiene Fedora Core, la cual se acepta y se pulsa **siguiente** para continuar con la configuración.

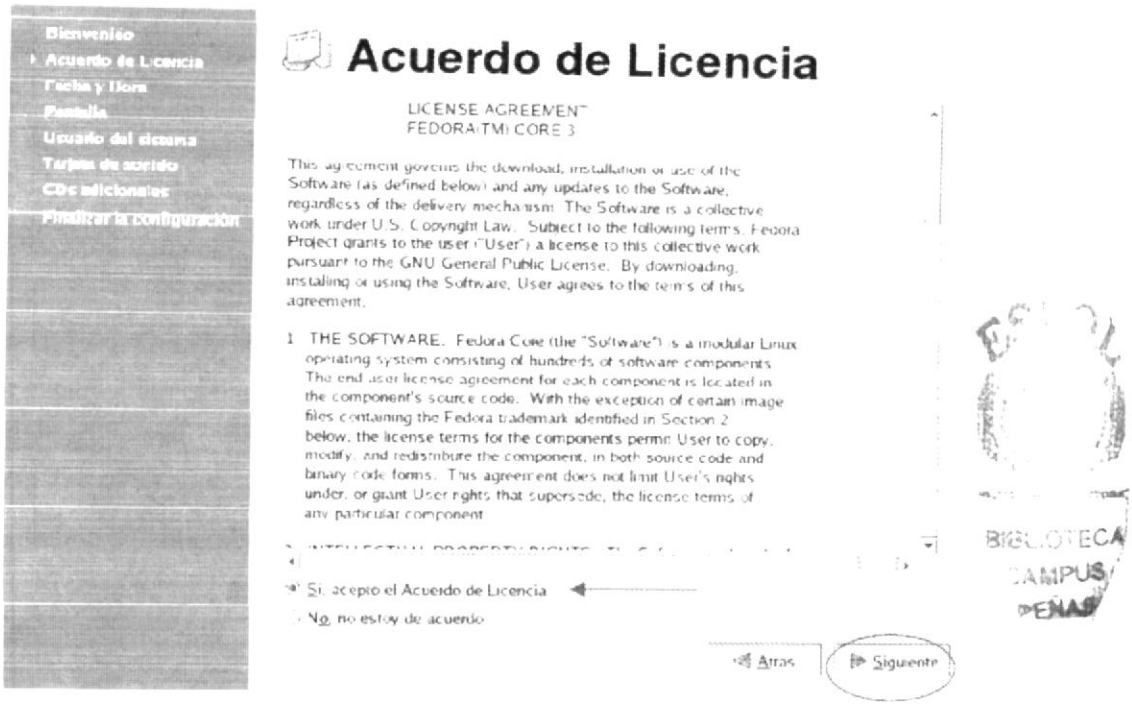


Figura 6-43: Acuerdo de Licencia

Luego que se configura la pantalla anterior, aparecerá la página de configuración de **fecha y hora** donde se configura la hora y la fecha exacta.

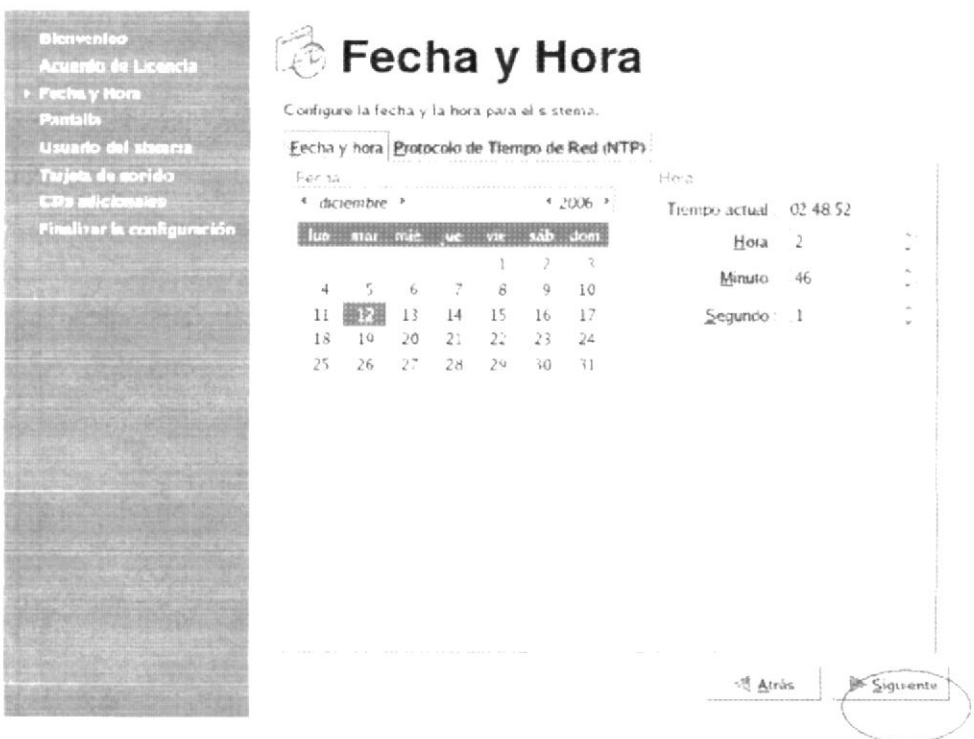
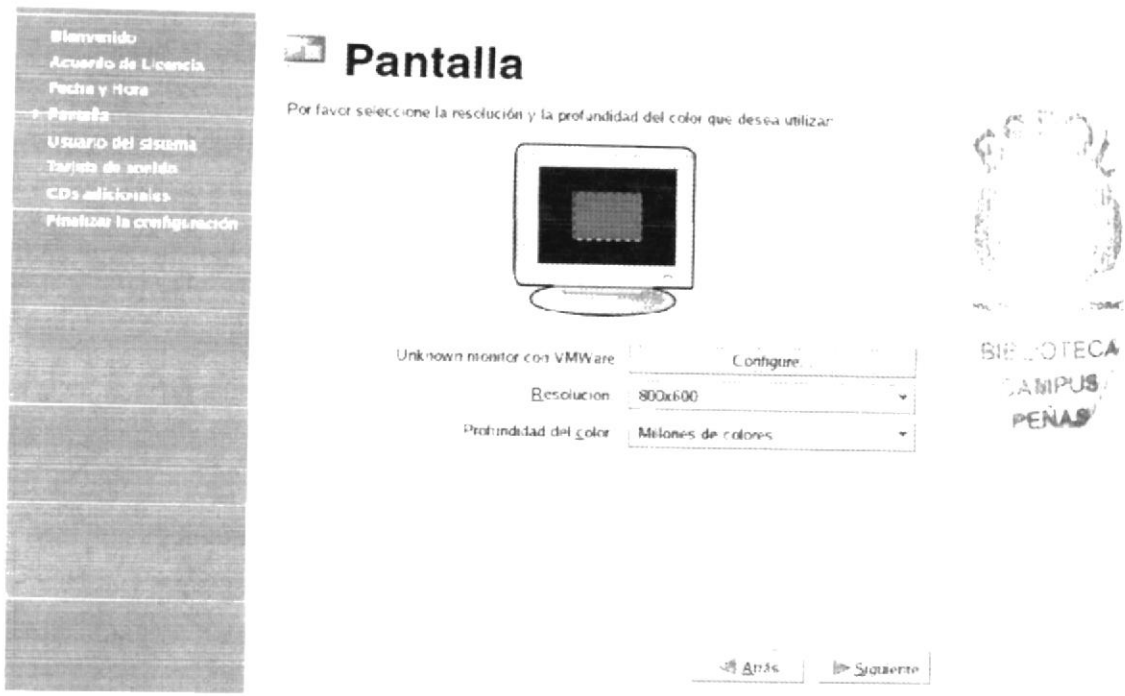


Figura 6-44: Configuración de la Fecha y Hora

En la página que se mostrará a continuación se configura la resolución y la definición del color.



BIBLIOTECA CAMPUS PEÑAS

Figura 6-45: Configuración de la Resolución de la Pantalla

En la siguiente página se crea una cuenta de usuario para así con esta cuenta poder iniciar sesión en el sistema Fedora Core3, una vez creado el usuario hacer clic en el botón **Siguiente**.

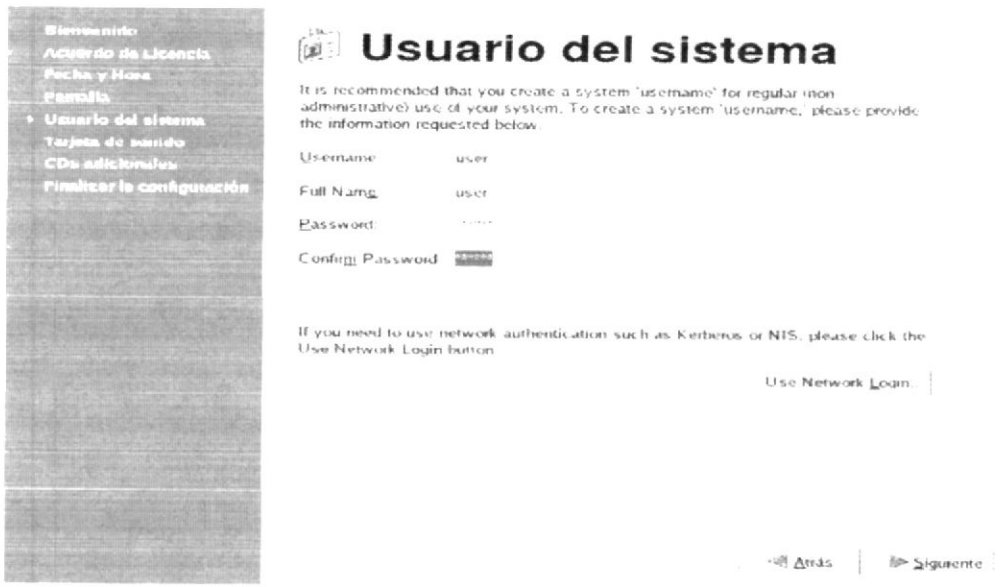


Figura 6-46: Configuración del Usuario del Sistema

Una vez configurado en la página anterior se procede a configurar la tarjeta de sonido, y a su vez se da clic en **Siguiente**.

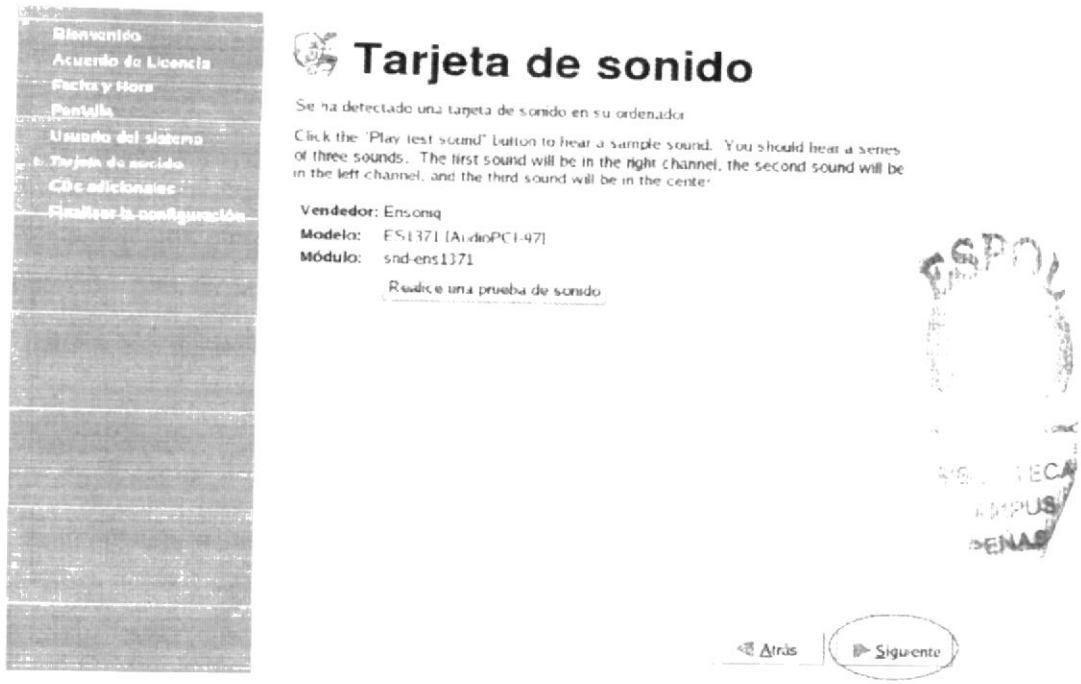


Figura 6-47: Configuración de la Tarjeta de Sonido

Esta pantalla permite cargar discos preparados para la instalación de programas en tercera persona. Sin embargo no se pueden utilizar para instalar paquetes adicionales desde los discos Fedora Core 3.

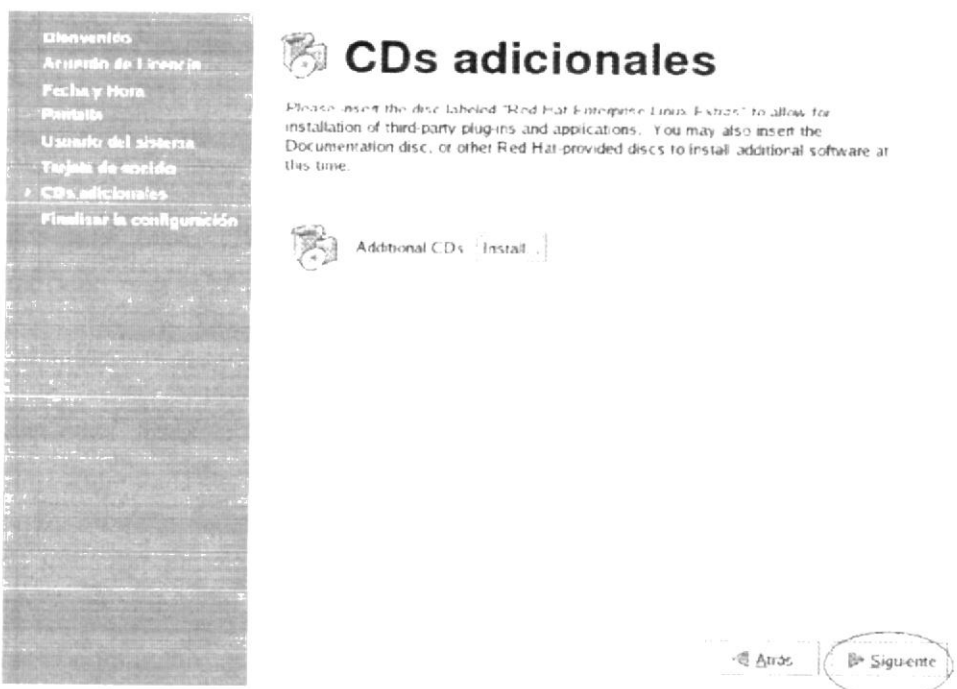
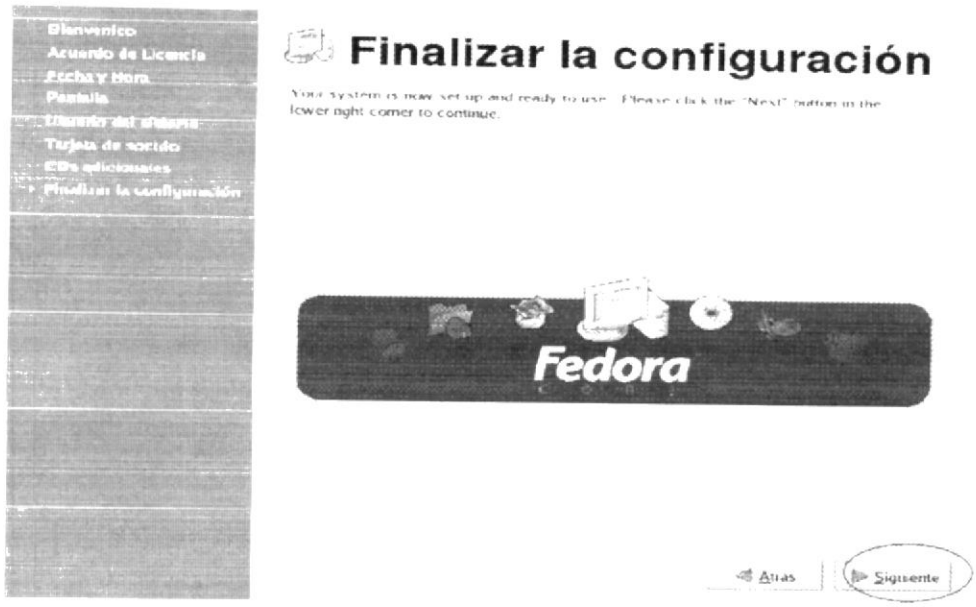


Figura 6-48: Cds Adicionales

Al terminar de configurar la página anterior aparecerá la **Siguiente** página con el mensaje de finalización de configuración, y se da clic en el botón **Siguiente**.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 6-49: Finalizar la Configuración

6.4.2 INICIO DE LINUX

6.4.2.1 MODO GRÁFICO

Una vez instalado Linux en la PC, cada vez que el sistema arranque mientras se cargue el sistema operativo se observará la siguiente pantalla.

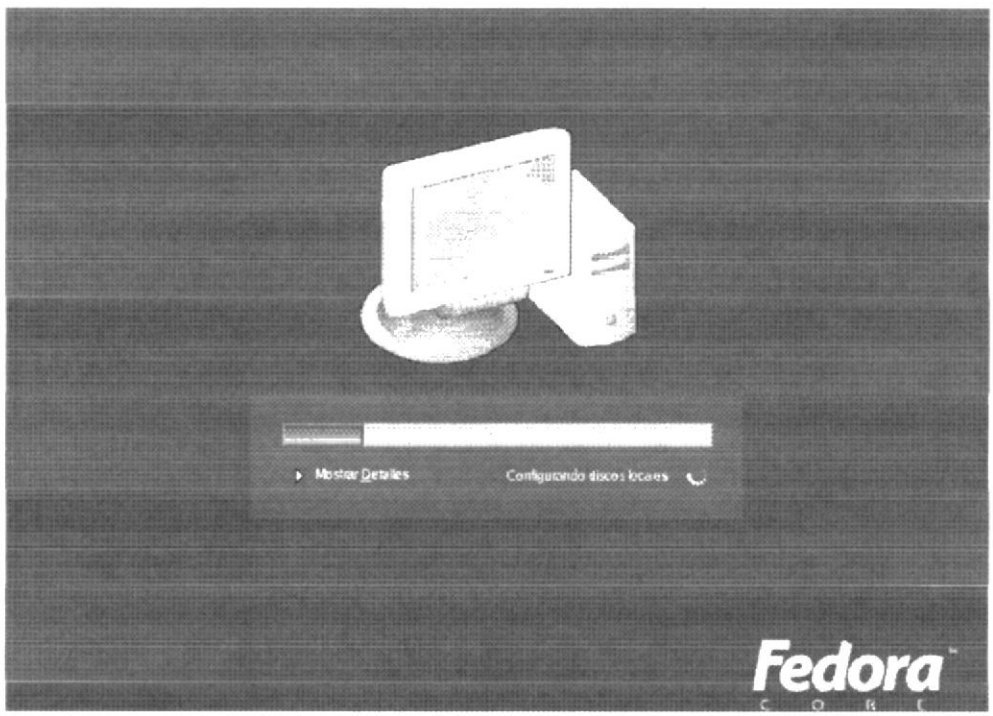


Figura 6-50: Inicialización del Sistema Linux

Luego de la página en la cual comienza a cargar el sistema operativo aparecerá la pantalla de ingreso de usuario, donde se digitará la palabra "**root**", la cual es la cuenta principal de Linux.

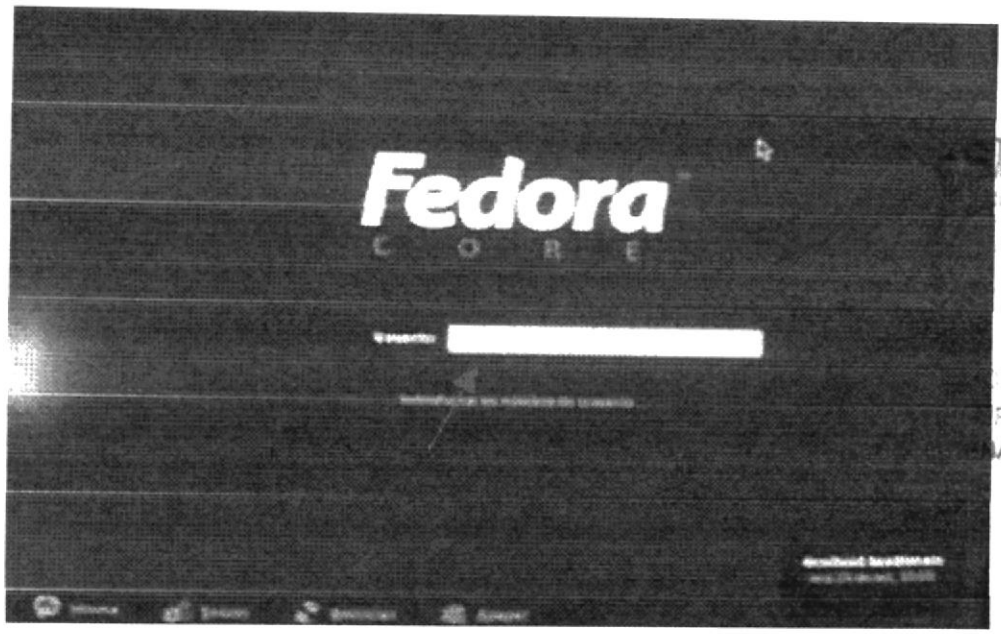


Figura 6-51: Ingreso del Usuario

Una vez ingresado el usuario, se solicita el ingreso de la contraseña al cual es la misma contraseña que se ingreso en el momento de la instalación.

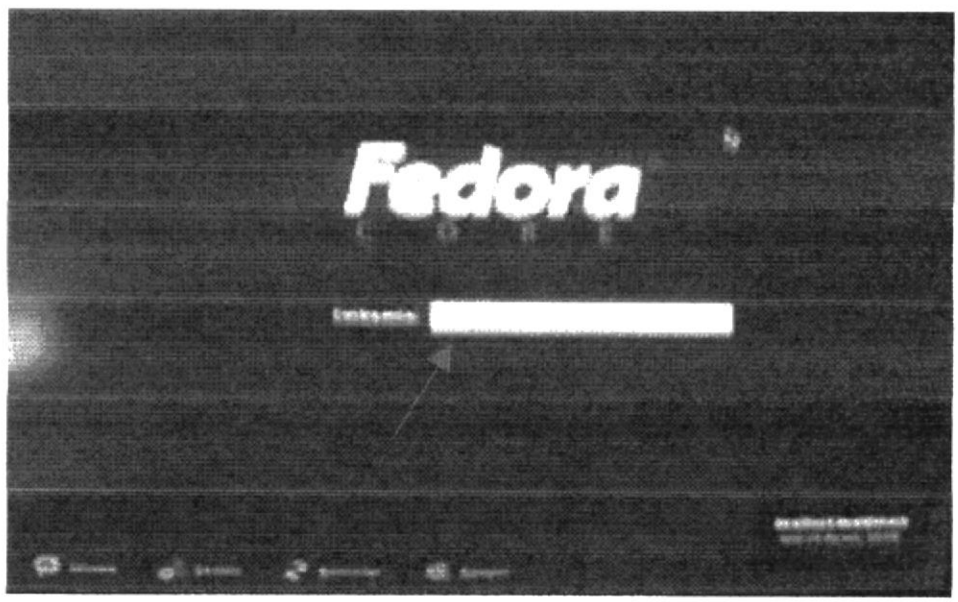


Figura 6-52: Ingreso de la Contraseña

Luego de haber ingresado correctamente el usuario y la contraseña respectivamente de Linux se procede a ingresar al entorno gráfico del servidor Linux como se muestra en el grafico anterior.



Figura 6-53: Entorno Gráfico de Linux Fedora Core 3

ESPOL
TECA
MPUS
ENAS

6.4.2.2 MODO TEXTO

Para ingresar al modo texto de Linux se presiona la tecla **shift** + **F1** y automáticamente ingresa, al iniciar en el modo texto aparecerá la siguiente pantalla en la que se deberá digitar el login y acto seguido digitar el password.

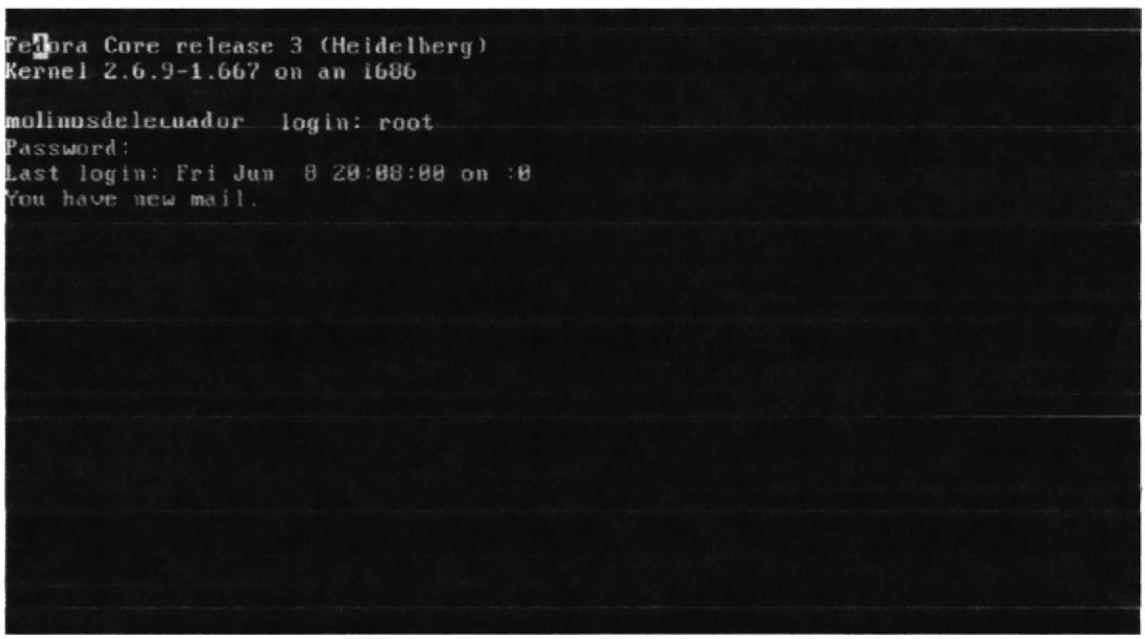


Figura 6-54: Entorno Modo Texto de Linux

6.5 COMANDOS BÁSICOS DE LINUX FEDORA CORE 3

cd
Ingresar a un directorio. **Sintaxis: cd /deber**

cd ..
Para salir de un directorio. **Sintaxis: cd..**

chown
Cambia de usuario y grupo a un archivo. **Sintaxis: chown squid:squid claves**

cp
Copia archivos de un directorio a otro. **Sintaxis: cp deber /etc/**

find
Encuentra archivos. **Sintaxis: find ejercicio.doc**

mkdir
Crea un directorio. **Sintaxis: mkdir topico**

mv
Mueve un archivo(s) a un directorio. **Sintaxis: mv deber.txt /topico**

adduser
Añadir usuario de sistema. **Sintaxis: adduser administrador**

passwd
Asigna una clave a un usuario. **Sintaxis: passwd administrador**

ls
Ver el contenido del directorio. **Sintaxis: Ls**

ls -a
Enlista archivos ocultos. **Sintaxis: ls –a**

pwd
Muestra la ruta del directorio actual. **Sintaxis: Pwd**

rm
Borra un fichero. **Sintaxis: rm borrador.doc**

rm -r
Borra todo un directorio. **Sintaxis: rm –r /topico**

rmdir
Borra un directorio vacío. **Sintaxis: rmdir /nueva_carpeta**

vi
Edita un archivo. **Sintaxis: vi examen.doc**

date
Muestra la fecha del sistema. **Sintaxis: Date**

gzip
Comprime un archivo. **Sintaxis: gzip trabajo.zip**

gunzip
Descomprime un archivo. **Sintaxis: gunzip trabajo**

ping
Herramienta de red para comprobar entre otras cosas si se llega a un host remoto. **Sintaxis: ping 192.168.12.1**

ifconfig
Verifica si esta habilitada la ip del servidor. **Sintaxis: Ifconfig**

ESPOL BIBLIOTECA CAMPUS PEÑAS

chmod

Este comando da permisos de lectura, escritura a cualquier archivo.
Sintaxis: chmod +777 prueba.txt

mail

Sirve para revisar los correos de los usuarios. **Sintaxis: Mail**

slocate

Sirve para buscar directorios, archivo. **Sintaxis: slocate d.C.**

Telnet

Permite una conexión de forma remota hacia el servidor por medio de la dirección IP. **Sintaxis: telnet 200.168.41.1**

clear

Sirve para limpiar pantalla. **Sintaxis: Clear**

rpm -q

Sirve para verificar si esta instalado un paquete **Sintaxis: rpm –q samba**

rpm -i

Sirve para instalar un paquete. **Sintaxis: rpm –i samba**

rpm -e

Sirve para desinstalar un paquete. **Sintaxis: rpm –e samba**



Touch

Permite crear un archivo en blanco. **Sintaxis: touch respaldo**

Updatedb

Actualiza la base de datos de archivos de Linux. **Sintaxis: updatedb**

Status

Muestra el estado actual de un servicio. **Sintaxis: service named status**

Stop

Permite detener un servicio. **Sintaxis: service named stop**

Service

Sirve para ver los estados de cualquier de los servicios, en conjunto con otros comandos. **Sintaxis: service httpd restart**

Start

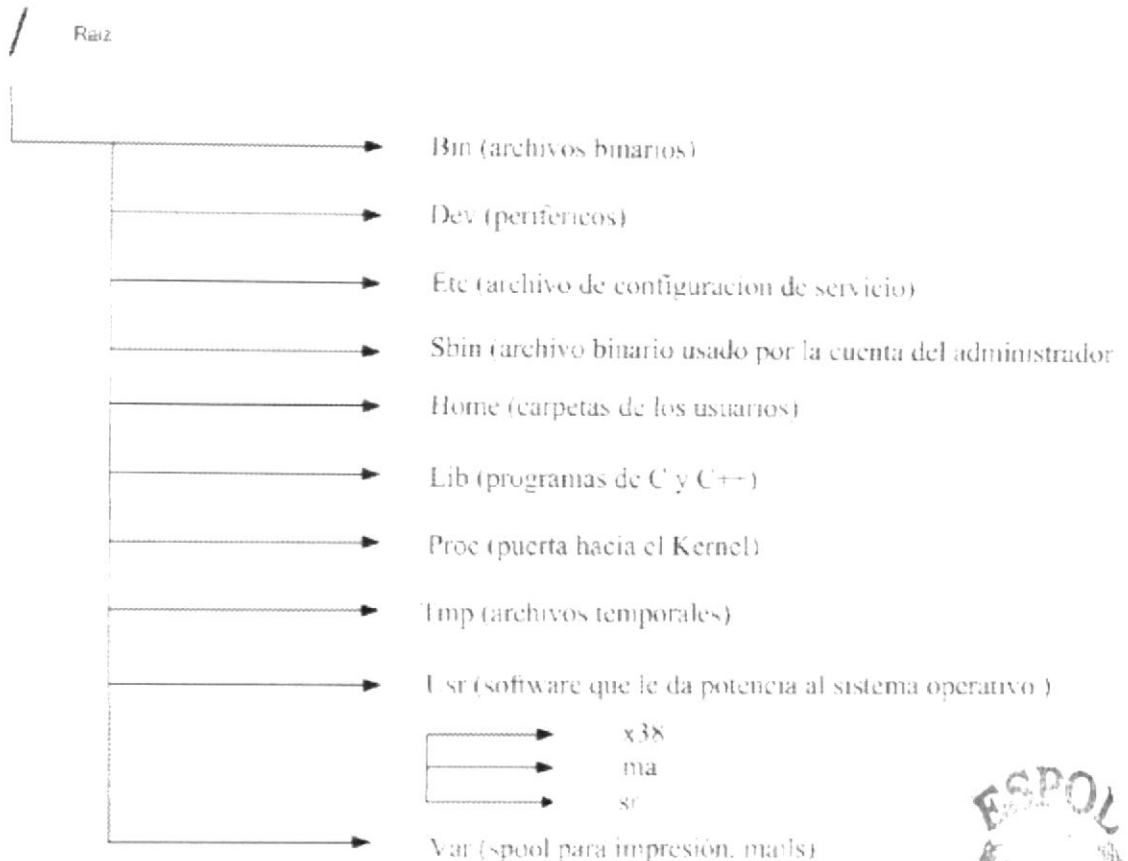
Permite iniciar un servicio **Sintaxis: service smb start**

Reload

Permite recargar un servicio sin detener su ejecución
Sintaxis:service smb reload

SISTEMA DE ARCHIVO DE LINUX

Todos los programas de Linux, las bibliotecas, los archivos del sistema y los archivos de usuario residen en el sistema de archivos.



ESPOL
BIBLIOTECA
CAMPUS
PENAS

6.7 CONFIGURACIÓN DE LA TARJETA DE RED

Para cualquier configuración de los servicios de Linux se necesita configurar la tarjeta de red.

6.7.1 CONFIGURACIÓN MODO TEXTO

1.- Se configura la tarjeta de red con el comando, **ifconfig eth0** (IP) up, y luego se verifica si se configuro correctamente con el comando **ifconfig**.

root@localhost /] # Ifconfig eth0 192.168.12.1 up

ifconfig: Es una palabra reservada de Linux.
eth0: Es como reconoce Linux a la tarjeta de red.
192.168.12.1: Es la dirección ip que se le asigna al servidor Linux.
up: Sirve para levantar la tarjeta de red.

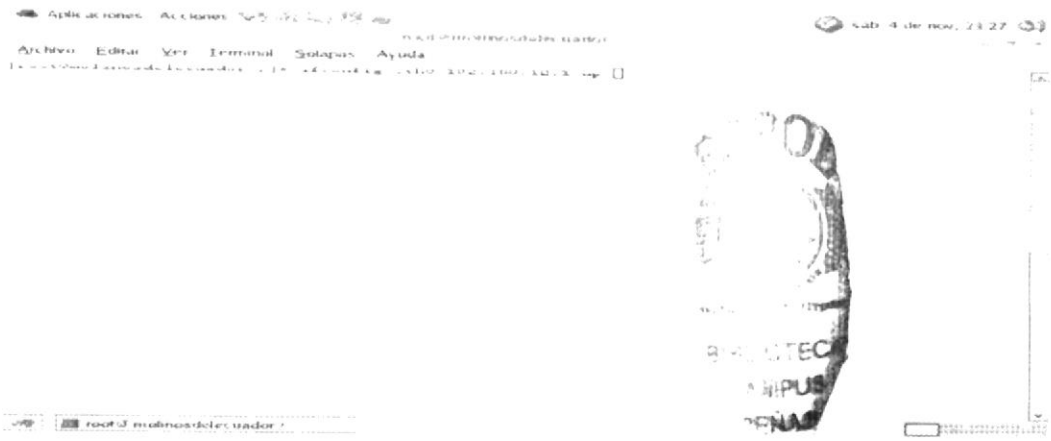


Figura 6-55: Configuración de la Tarjeta de Red

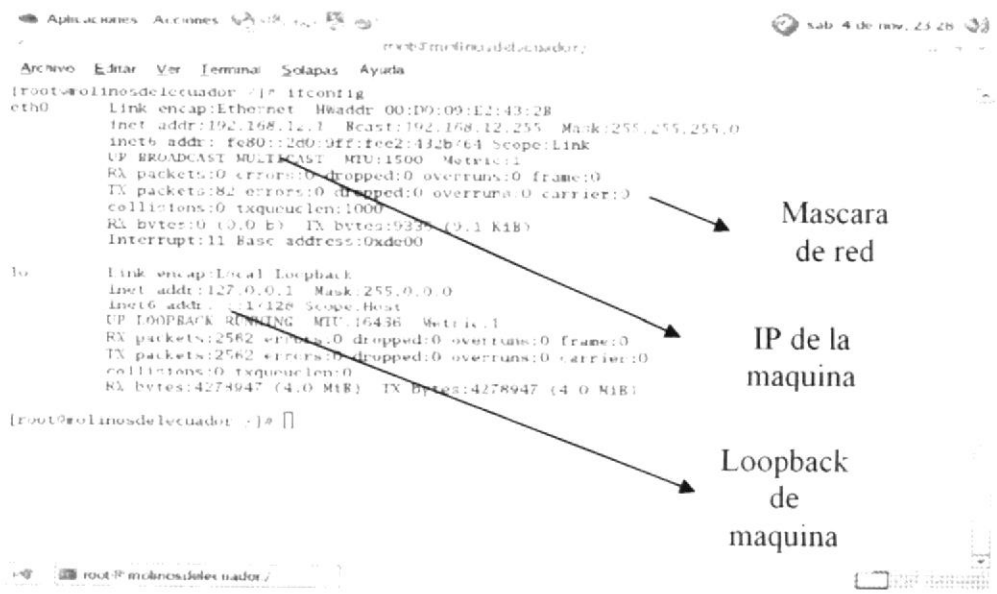


Figura 6-56: Verificando Ip

2.- Después de configurar la tarjeta de red restaurar la tarjeta de red con el siguiente comando.

root@localhost /] # Service network restart



Figura 6-57: Restaurar la Tarjeta de Red

BIBLIOTECA CAMPUS PEÑAS

6.7.2. CONFIGURACIÓN MODO GRÁFICO

1.- Se digita el comando **Setup** para configurar la tarjeta de red de modo gráfica.



Figura 6-58: Ingreso del Comando Setup

2.- Una vez en el **Setup** se procede a **Configuración de la red** y se presiona el botón **Ejecutar una herramienta.**

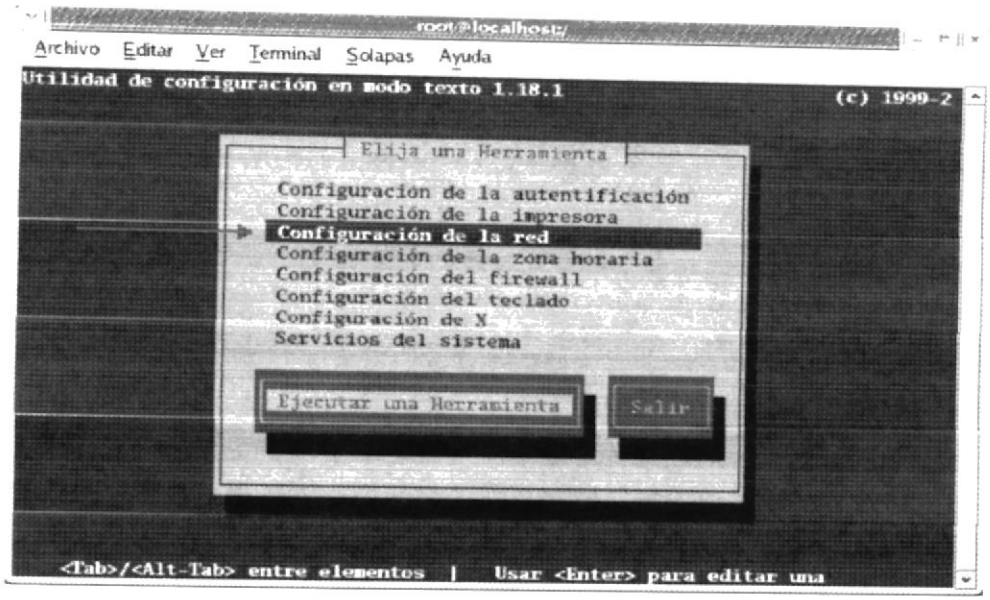


Figura 6-59: Configuración de la Red

En la pantalla siguiente aparecerá un mensaje el cual indica la opción de **Configurar la tarjeta de red** y seleccionar la opción **SI.**

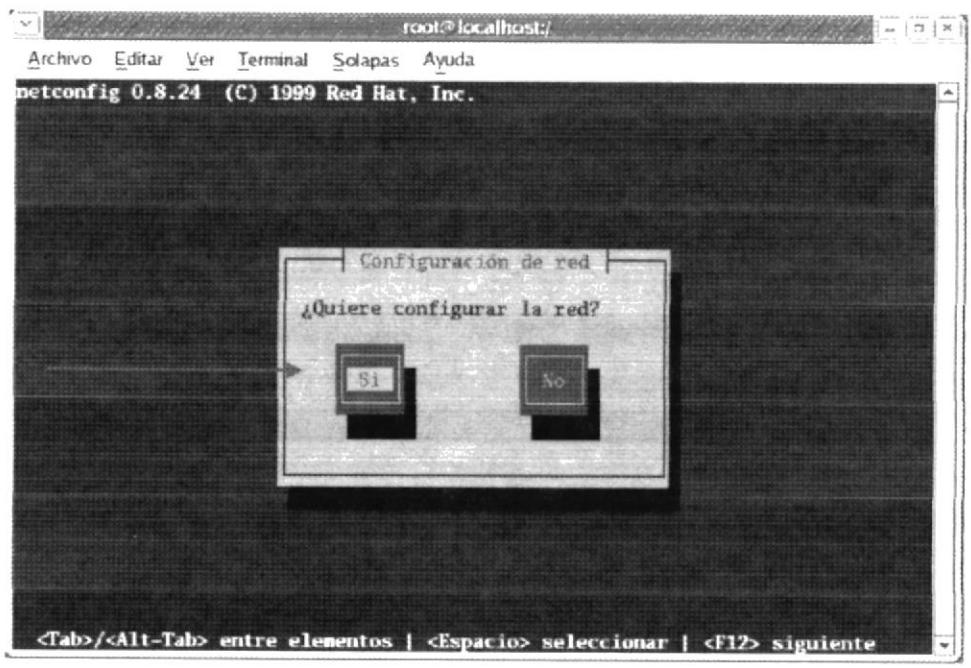


Figura 6-60: Aceptación de la Configuración de Red

3.- En la pantalla siguiente se digita la dirección **IP** y la **Máscara**.

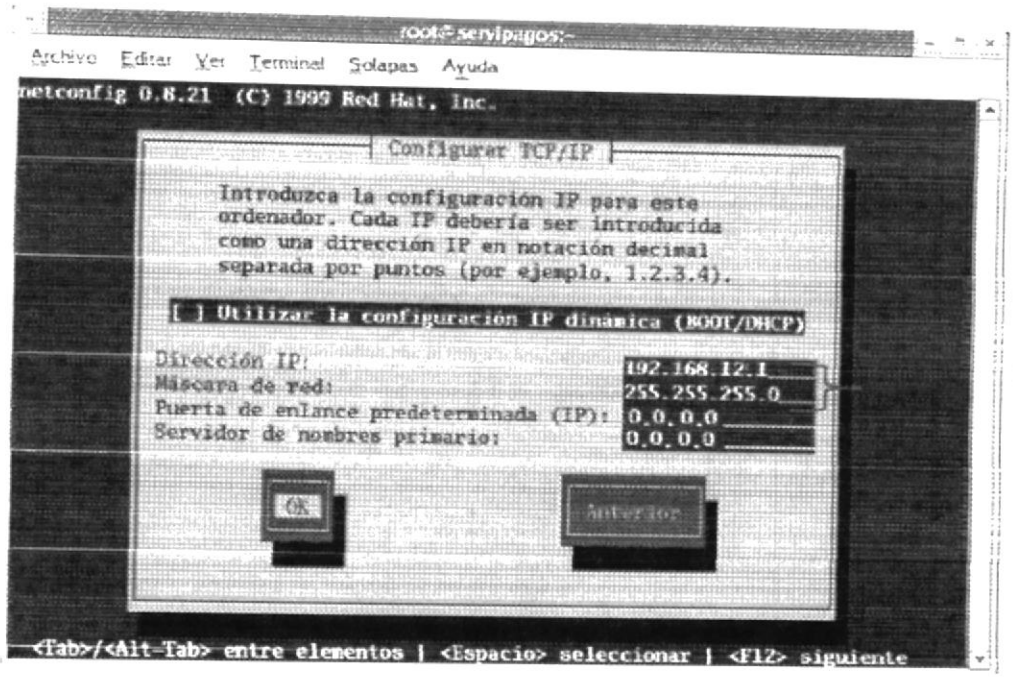


Figura 6-61: Configuración TCP/IP

4.- Después de configurar la tarjeta de red se restaura la tarjeta de red con el siguiente comando.

root@localhost /] # Service network restart



Figura 6-62: Reiniciar el servicio del Network

Una vez reiniciados los servicios de la tarjeta de red se verifica la respectiva asignación de la **IP.**

root@localhost /] # Ifconfig

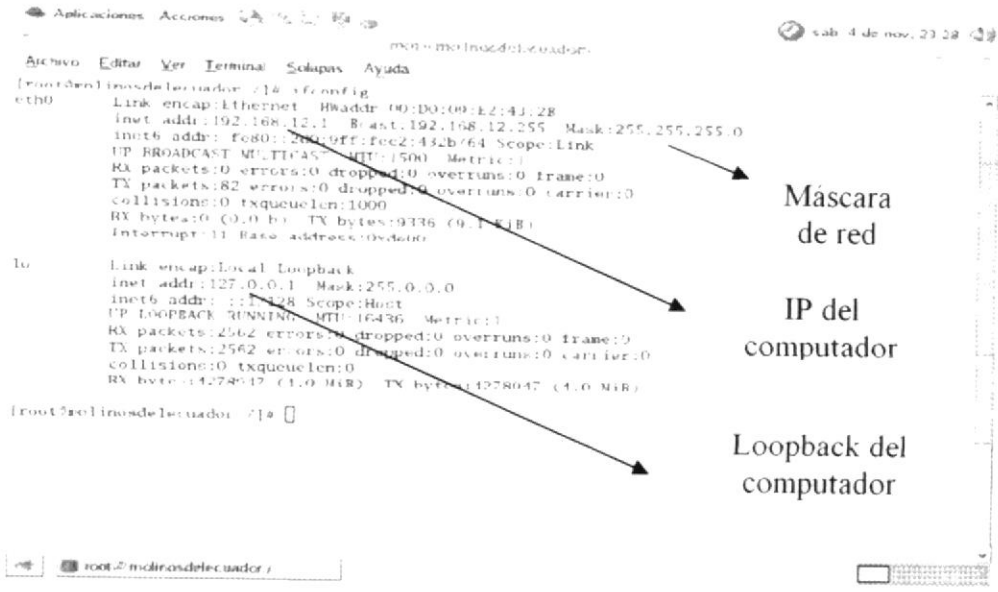


Figura 6-63: Verificando IP

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

6.8 SERVIDOR SAMBA

Samba es una implementación bajo los protocolos SMB y NETBIOS. Con Samba se puede hacer que el sistema Linux actué como servidor SMB dentro de la red, permitiendo a otros equipos (que por lo general serán otro computadors Windows) acceder a recursos compartidos como directorios e impresoras.
Samba proporciona a Linux soporte para estos protocolos, de forma que puede compartir discos e impresoras con Windows. Para ello utilizan los demonios "smbd" y "nmbd", que se ejecutan en un script de inicio o en /etc/xinetd.conf.. Estos demonios permiten:

- Compartir una unidad de Linux con máquinas Windows.
- Compartir una unidad de Windows con máquinas Linux.
- Compartir una impresora de Linux con máquinas Windows.
- Compartir una impresora de Windows con máquinas Linux.

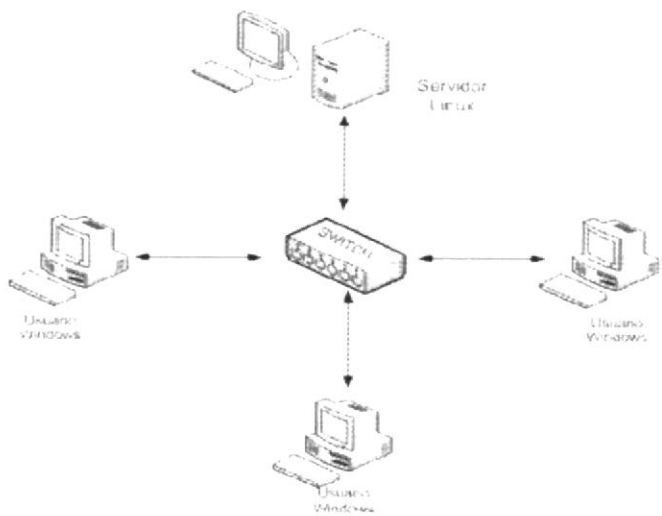


Figura 6-64: Servidor Samba

La configuración de *Samba* en un Linux (u otra máquina UNIX) es controlada por un solo fichero, /etc/smb.conf. Este fichero determina que recursos del sistema quieres compartir con el mundo exterior y que restricciones deseas poner en ellos.

Como las siguientes secciones 'direccionarán' la compartición de unidades e impresoras de Linux con máquinas Windows, el fichero **smb.conf** mostrado en esta sección es lo más simple posible, solo para propósitos introductorias.

No te preocupes por los detalles, aún. Otras secciones más adelante introducirán los conceptos más importantes.

Cada sección del fichero empieza con una cabecera como [global], [impresoras], etc.

La sección **[global]** define unas pocas variables que *Samba* usará para definir la compartición de todos los recursos.

La sección **[homes]** permite a los usuarios remotos acceder a sus respectivos directorios principales en la máquina Linux local (cada uno al suyo nada más). Esto es, si un usuario de Windows intenta conectar a este recurso desde su máquina Windows, será conectado a su directorio personal. A tener en cuenta que para hacer esto, tiene que tener una cuenta en la máquina Linux. ;-)

El fichero smb.conf que viene debajo como ejemplo permite a los usuarios remotos acceder a su directorio principal en la máquina local y escribir en un directorio temporal. Para que un usuario de Windows vea estos recursos, la máquina Linux debe estar en la red local. Entonces el usuario simplemente conecta una unidad de red desde el *Explorador de Windows* o el *Windows File Manager*.

Fíjate que en las siguientes secciones, se darán entradas adicionales a este fichero para permitir la compartición de más recursos.



6.8.1. DISTRIBUCIÓN SAMBA

Como se menciono antes, Samba actualmente contiene varios programas que sirven para diferentes propósitos. Introducir en cada uno de ellos brevemente y vera cómo funcionan. La mayoría de los programas que vienen con la distribución de Samba se centran en sus dos demonios. Echar un vistazo a las responsabilidades de cada demonio:

smbd
El demonio smbd es responsable de manejar los recursos compartidos entre la máquina servidora Samba y sus clientes. Proporciona servicios de archivos, impresión y visualización a los clientes SMB a través de una o más redes. smdb controla todas las notificaciones entre el servidor Samba y los clientes de red. En adición, es responsable de la autentificación de usuarios, bloqueo de recursos y la compartición de datos a través del protocolo SMB.

nmbd
El demonio nmbd es un sencillo servidor de nombres que imita la funcionalidad de los servidores WINS y de resolución de nombres NetBIOS. Este demonino está a la escucha de peticiones para el servidor de nombres y proporciona la información apropiada cuando se le llama. También proporciona listas de visualización del Entorno de Red y participa en las elecciones de los visualizadores.

La distribución de Samba también está acompañada por un pequeño grupo de herramientas tipo línea de comandos Unix:

smbclient
Un cliente tipo FTP Unix que puede ser usado para conectar a recursos compartidos por Samba.

smbtar
Un programa para realizar copias de seguridad de datos sitos en los recursos compartidos, similar al comando Unix "tar".

nmblookup
Un programa que proporciona búsquedas de nombres NetBIOS sobre TCP/IP.

smbpasswd
Un programa que permite a un administrador cambiar las passwords encriptadas usadas por Samba.

smbstatus
Un programa para reportar las conexiones de red actuales hacia los recursos compartidos por el servidor Samba.

testparm
Un simple programa para validar la sintaxis del fichero de configuración de Samba.

testprns
Un programa que testea si varias impresoras son reconocidas por el demonio smbd.



6.8.2. FUNCIONAMIENTO

Samba es en si un paquete muy complejo, que brinda a los usuarios un sin fin de posibilidades a la hora de interactuar con equipos Windows que estén coexistiendo en redes heterogéneas,

6.8.3 VENTAJAS

- Samba puede ayudar a las computadoras de s Windows y Linux a coexistir en la misma red.
- Proporciona un área común para datos o directorios de usuarios en orden a realizar una transición desde un servidor Windows hacia un Linux o viceversa.
- Compartir impresoras entre clientes Windows y Linux.
- Acceder a ficheros Windows desde un servidor Linux.

6.8.4 DESVENTAJAS

- Documentación.
- Formación del personal técnico y académico.
- Antes de realizar instalación del sistema operativo y cualquier aplicación se debe leer con detenimiento el HowTo, pues en ocasiones no funcionan debido a diferencias de versiones usadas en diferentes distribuciones de Linux. Algunas veces algún dispositivo no funciona adecuadamente y hay que recurrir a búsquedas de Internet para ubicar el driver necesario.

6.8.5 REQUERIMIENTOS

- Tener una computadora Linux
- Configuración IP Estática
- Tarjeta de red
- Paquete SMB instaldo
- Configurar la tarjeta de red

6.8.6 CONFIGURACIÓN DEL SERVIDOR SAMBA

1.- Como primer paso hay que verificar si esta instalado el paquete de samba, con el siguiente comando.

root@localhost /] # rpm –q samba

rpm –q	Verifica si está instalado un paquete
samba	Paquete



Figura 6-65: Revisión del Paquete

2.- Una vez verificado el paquete de Samba se procede a ingresar al directorio de **samba**.

root@localhost /] # cd /etc/samba

cd	Permite ingresar a un directorio
/etc/samba	Directorios



Figura 6-66: Ingreso al directorio Samba

3.- Una vez en el directorio de Samba se edita el archivo de **smb.conf.**

root@localhost samba] # vi smb.conf

vi	Edita un archivo
smb.conf	Archivo del Samba



Figura 6-67: Archivo de Samba

BIBLIOTECA CAMPUS PEÑAS

Secciones del smb.conf
Globals settings
El menú GLOBALS contiene variables generales que se aplican al total de los recursos puestos a disposición del servidor de SMB. Esta sección contiene también información de identificación del servidor dentro de la red NetBIOS: grupo de trabajo, nombre e identificador. Esta sección contiene también los modos de funcionamiento de Samba.

Identificar el servidor
Primero hay que elegir algunos parámetros de funcionamiento del servidor, para que se integre bien en la red.

El campo **workgroup,** permite elegir el grupo de trabajo del que el servidor Samba hace parte.

Workgroup = Cárdenas (Grupo de trabajo)

El campo **netbios name,** permite definir el nombre de la computadora, no como un nombre de DNS, sino como un nombre de resolución de nombres propio del protocolo NetBIOS.

Netbios name = Linux (Descripción del servidor)

El campo **Server string,** permite elegir las descripción que acompaña al nombre del servidor en la lista de recursos anunciados.

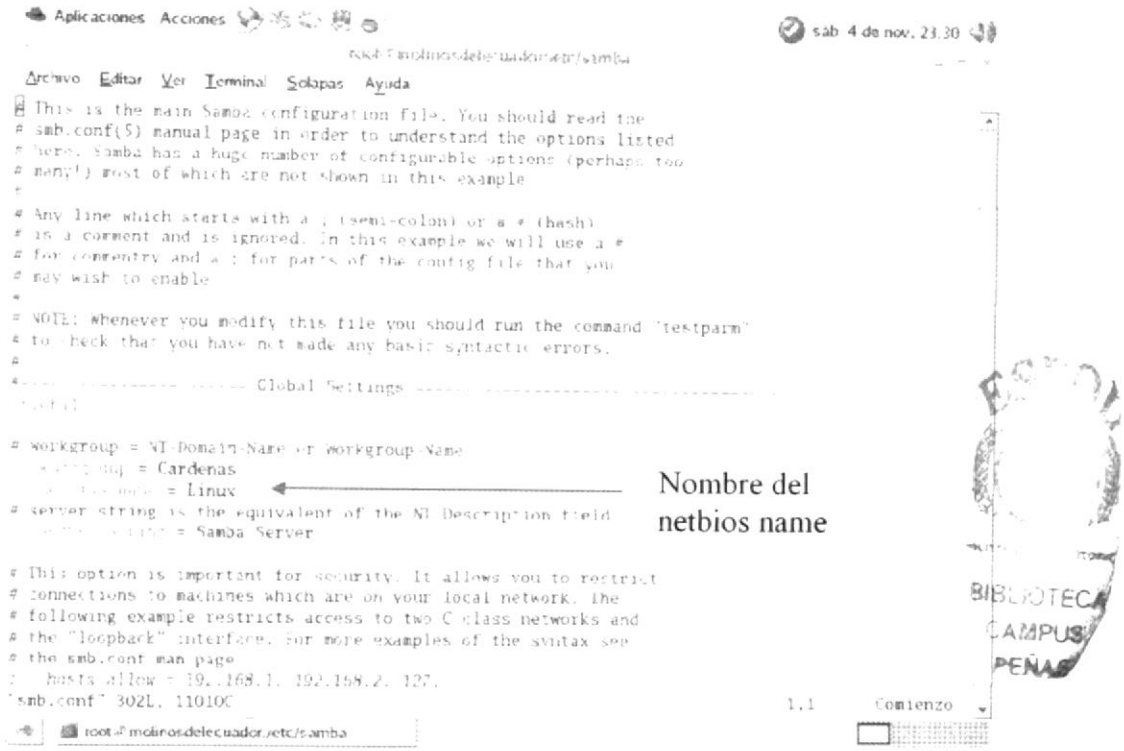


Figura 6-68: Configuración en Global Setting de Samba

Shares definitions

El menú Shares contiene la lista de comparticiones de disco efectuadas por la computadora. Se aconseja primero crear la partición compartida y después preci sar para cada partición sus propiedades particulares.

[home] (va el nombre_carpeta (molinosdelecuador))
Comment = Home Directories
Browsable = no
Valid users = fernando
Writable = yes
Path = /nombre_carpeta (molinosdelecuador)

El campo **comment** indica un comentario del recurso.

El campo **browsable** indica que este recurso debe ser anunciado por nmbd, y por lo tanto debe tener permiso de escritura para todos los usuarios.

El campo **writable** indica que este recurso debe ser anunciado por nmbd, y por lo tanto debe tener permiso de escritura para todos los usuarios.

El campo **valid users** limita el acceso a ciertos usuarios, ya que para cada recurso es posible restringir el acceso a ciertos usuarios. Para cada una de las líneas de recursos compartidos en /etc/smb.conf, puede añadir la línea:

Valid users = usuario1, usuario2

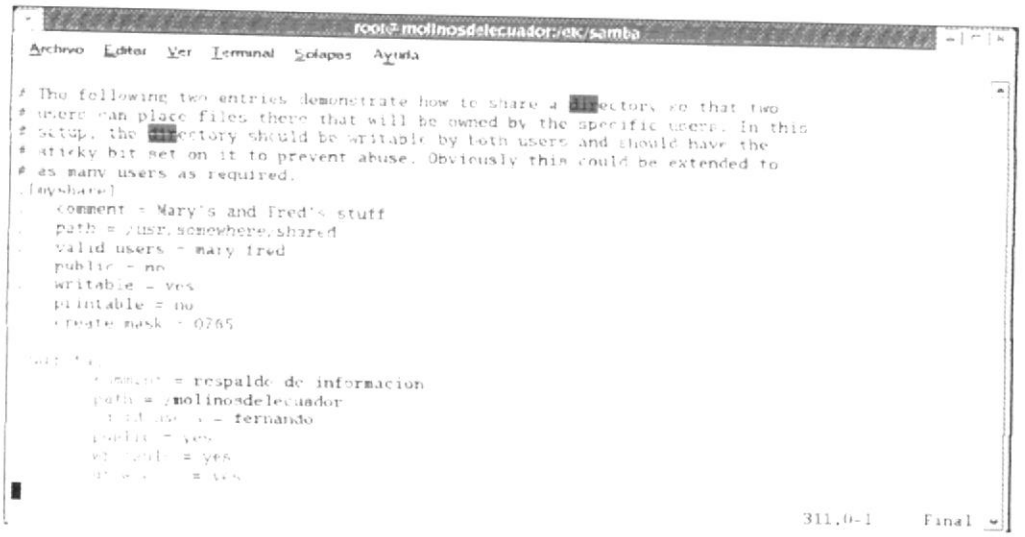


Figura 6-69: Especificar valores del Directorio del smb.conf

Al terminar de configurar el archivo **smb.conf** de *Samba* se sale del archivo guardando los cambios con el comando **wq.**

4.- Finalizada la configuración del archivo **smb.conf** de samba cambiarse al directorio raíz. Ya en el raíz se crea la carpeta a compartir con las computadoras Windows, que van a tener el mismo nombre que digitará en el archivo de samba.

root@localhost /] # mkdir molinosdelecuador

mkdir Crea un directorio



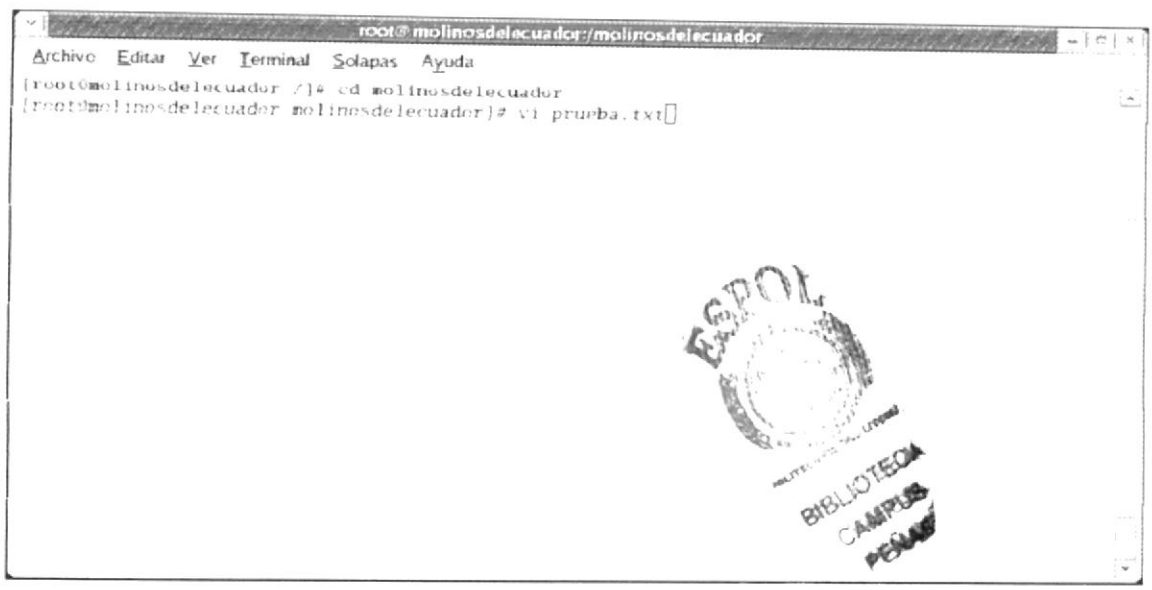
BIBLIOTECA CAMPUS PENAS

Figura 6-70: Crea un Directorio

5.- Se Ingresa a la carpeta que se creó (molinos del ecuador) para proceder a crear un archivo de texto para verificar su funcionamiento.

```
root@localhost /] # cd molinosdelecuador
root@localhost molinosdelecuador] # vi prueba.txt
```

cd	Ingresa a un directorio
vi	Crea y edita un archivo



ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 6-71: Ingreso al Archivo Prueba.txt

6.- En la siguiente pantalla se procede a ingresar información que se va a reflejar en el computador de Windows.

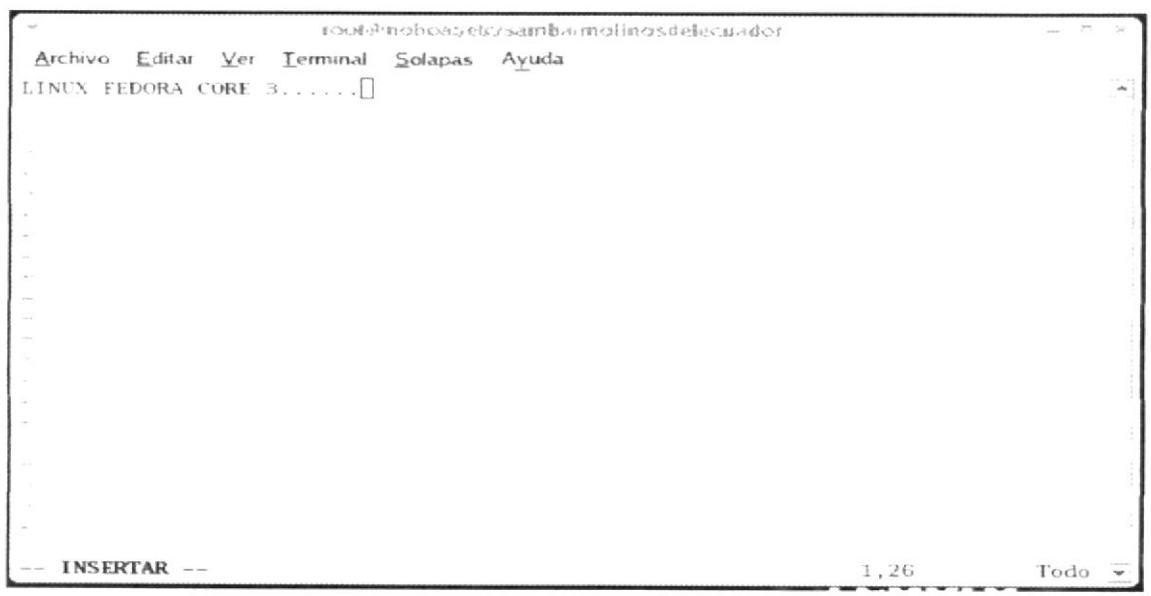
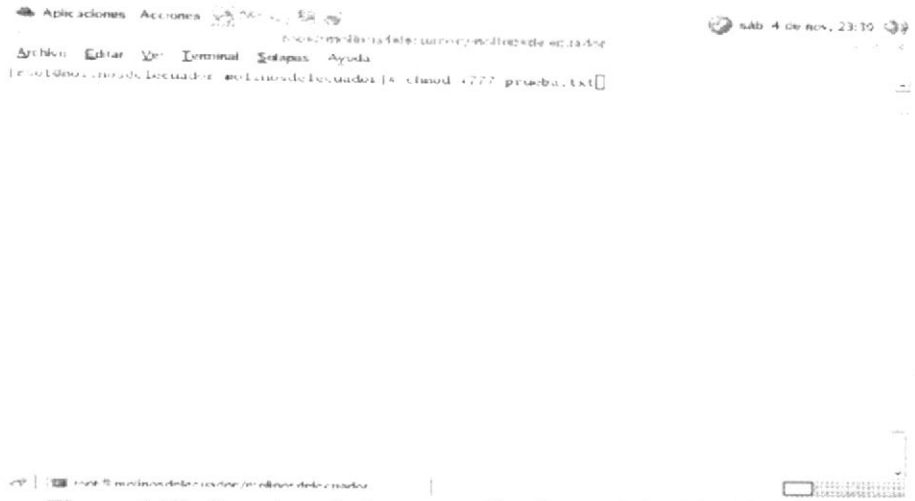


Figura 6-72: Ingreso de Datos en el Archivo Prueba.txt

7.- Una vez creado el archivo se dan los permisos de escritura, lectura y ejecución al archivo a compartir.

root@localhost molinosdelecuador] # chmod +777 prueba.txt

chmod + 777 Comando da permisos de lectura escritura a cualquier archivo



BIBLIOTECA
CAMPUS
PEÑAS

Figura 6-73: Permisos de Lectura y Escritura al Archivo Prueba.txt

8.- Se Asigna los permisos de lectura, escritura y ejecución a la carpeta. Con el siguiente comando.

root@localhost /] # chmod +777 molinosdelecuador

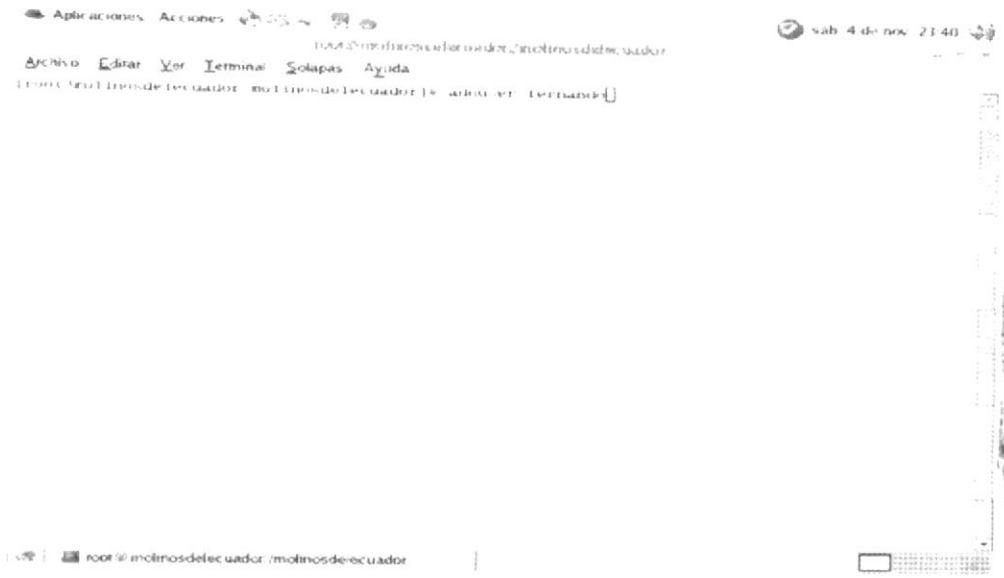


Figura 6-74: Permisos de Lectura y Escritura a la Carpeta

9.- Ya dado los permisos debidos a la carpeta y archivos a compartir, se procede a crear el usuario, el mismo usuario que se digitó en el directorio de samba.

root@localhost /] # adduser Fernando

adduser Comando que añade usuarios al sistema



BIBLIOTECA CAMPUS PEÑAS

Figura 6-75: Creación de Usuario

10.- Después de crear el usuario proceda a crear la contraseña para el usuario.

root@localhost /] # passwd (digitar la contraseña)

passwd Comando que asigna una clave o contraseña a un usuario



Figura 6-76: Creación de Contraseña

11.- Luego asigne una contraseña para los usuarios para hacer uso del servicio samba.

root@localhost /] # smbpasswd –a nombre_usuario

smbpasswd	Añade una contraseña a un usuario samba
-a	Añade un usuario

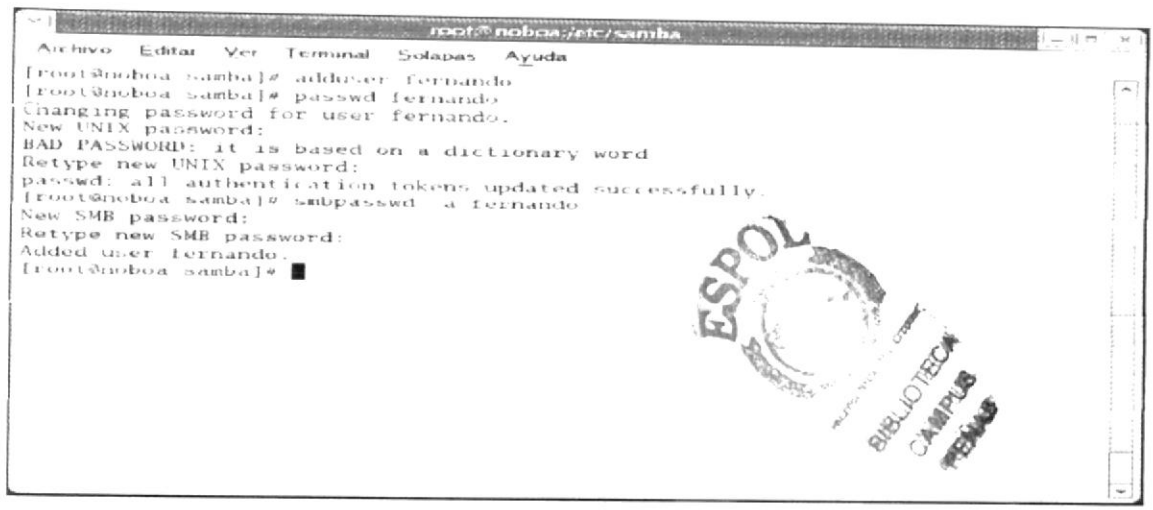


Figura 6-77: Asignación de Contraseña al Samba

12.- Ya creado el o los usuarios, proceda a levantar los servicios de samba y verifique el estado con el siguiente comando.

root@localhost /] # service smb start

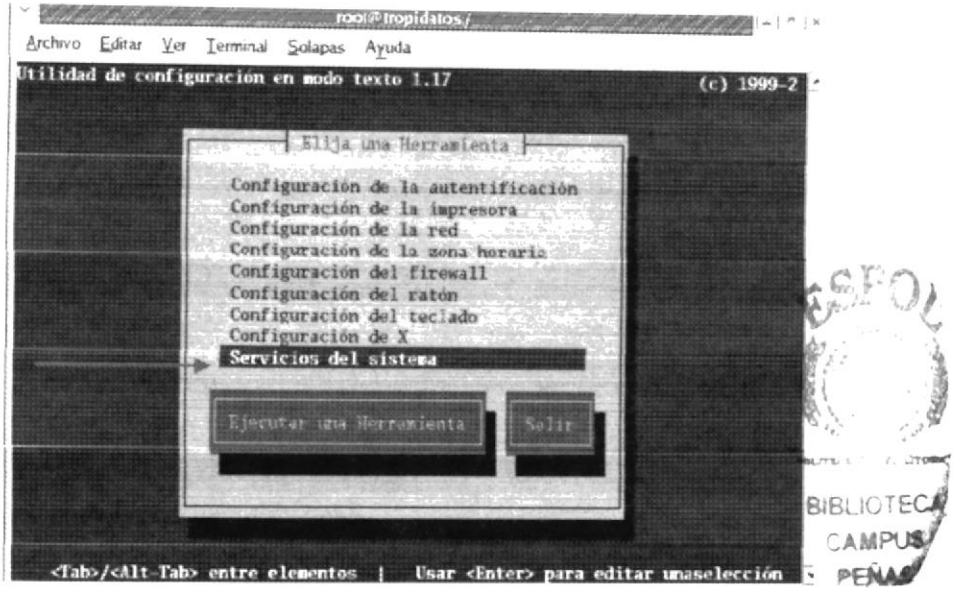


Figura 6-78: Restauración del Servicio Samba

6.8.7 ACTIVACIÓN DEL SERVICIOS SAMBA AUTOMÁTICAMENTE

Como sugerencia para que la configuración no presente ningún inconveniente se sugiere ingresar al SETUP con el comando:

root@localhost /] # setup



ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 6-79: Setup de Linux

Una vez en el setup proceda habilitar los servicios:

- Smb
- Xinetd
- Network

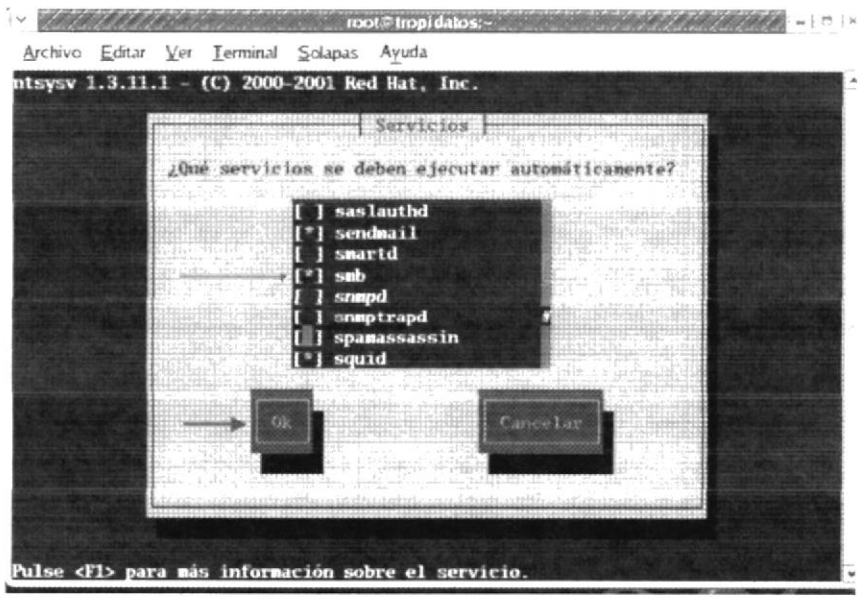


Figura 6-80: Selección de Servicios

Una vez activados los servicios de samba, ingrese a **Configuración del Firewall.**

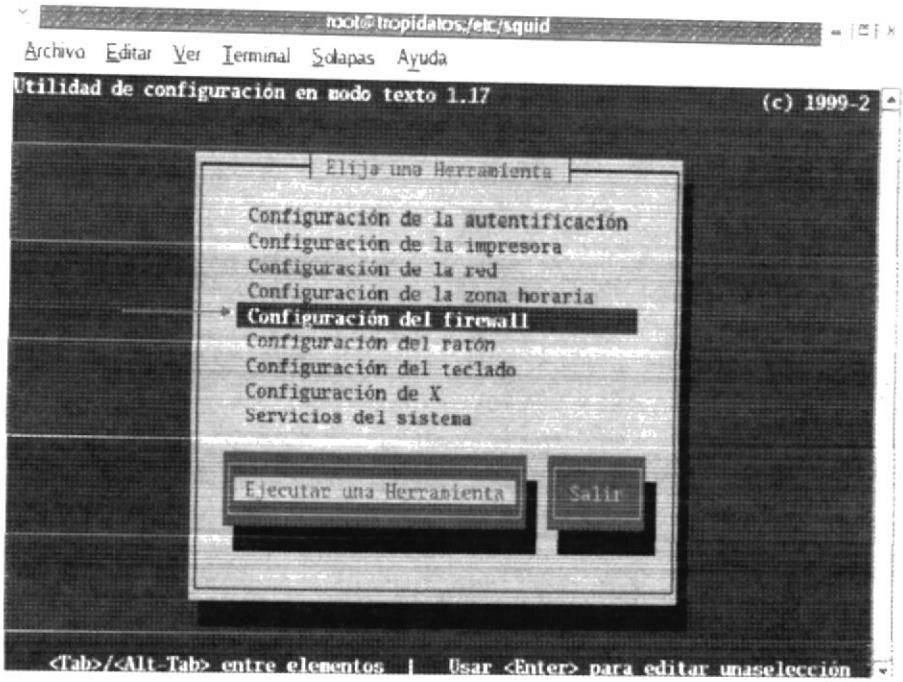


Figura 6-81: Selección Configuración del Firewall

Una vez en la **Configuración de firewall** proceda a **Inhabilitarlos**.

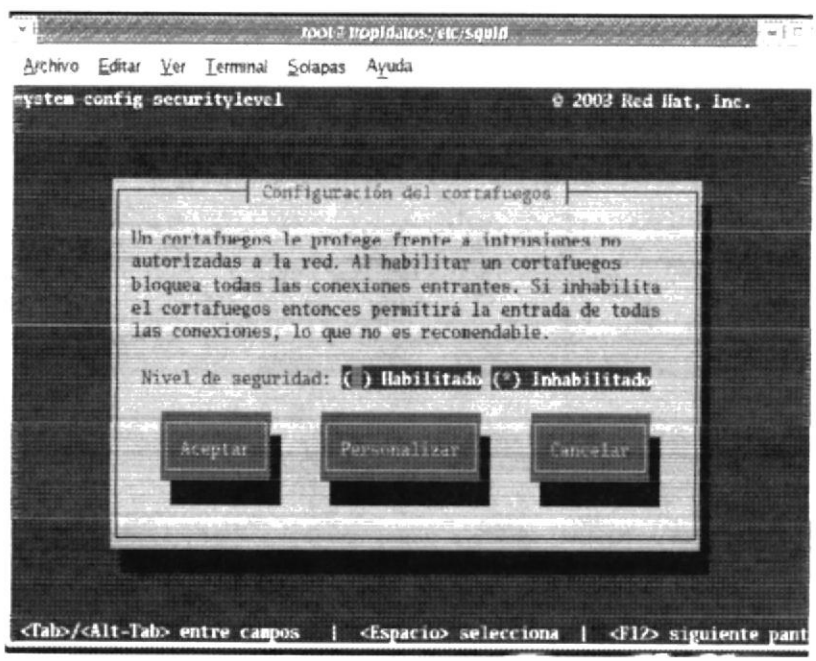


Figura 6-82: Deshabilitación de los Firewall

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

6.8.8 CONFIGURACIÓN EN CLIENTE WINDOWS – SAMBA

1.- Ir a **Mis Sitios de red** y hacer clic derecho y elegir la opción de **Propiedades.**

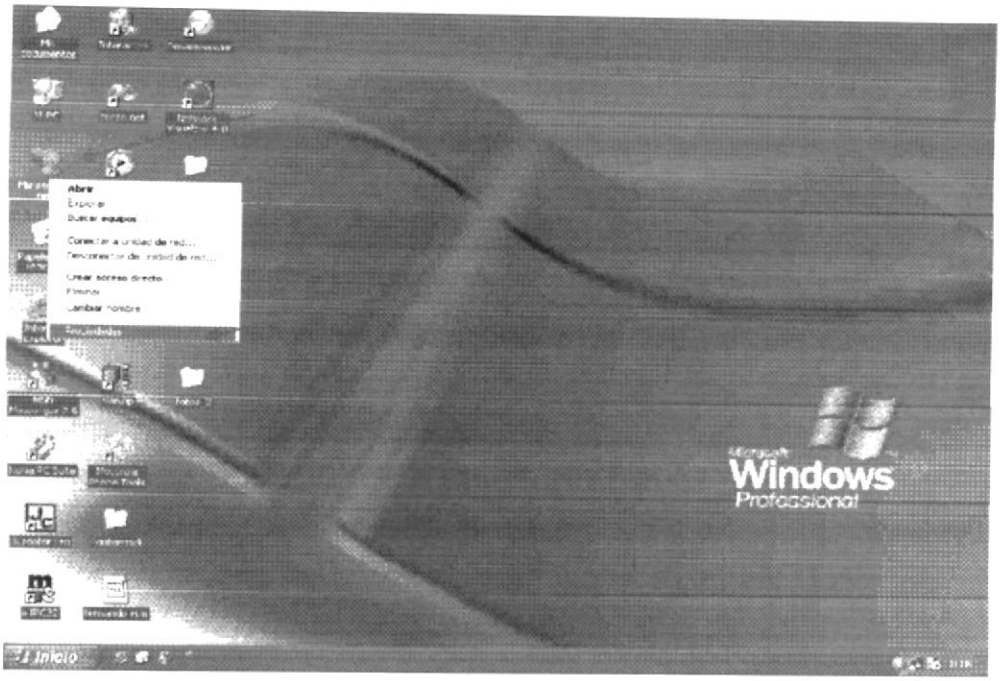


Figura 6-83: Propiedades de Mis Sitios de Red

BIBLIOTECA
CAMPUS

2.- Hacer clic derecho en la opción de **conexión de área local**, y elegir la opción de **Propiedades.**

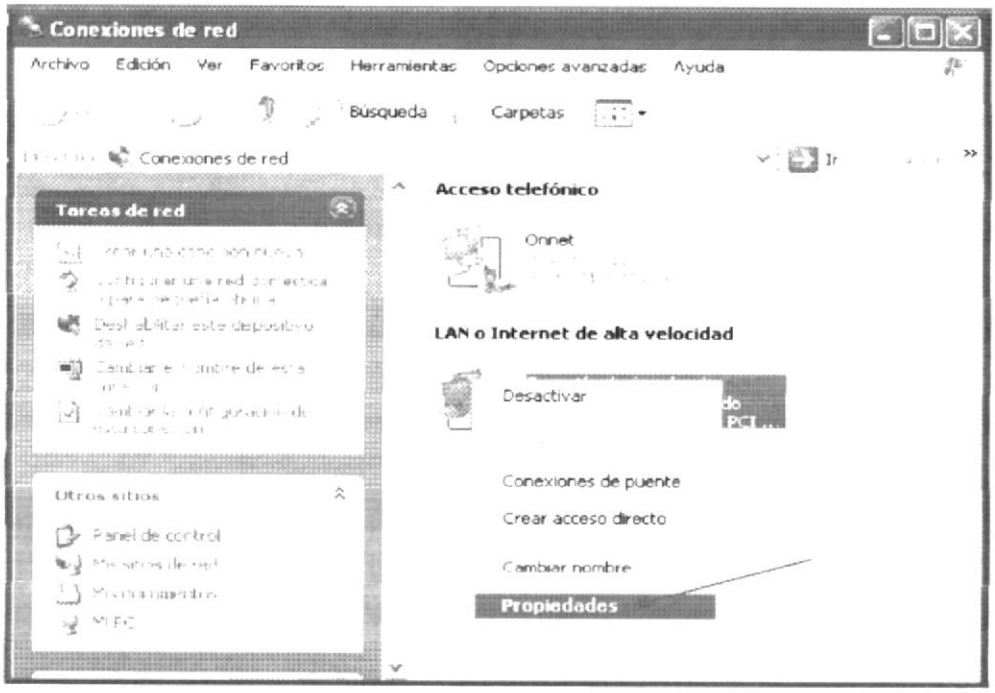


Figura 6-84: Conexiones de Red

3.- En esta ventana escoja la opción **TCP/IP** para configurar la tarjeta de red.

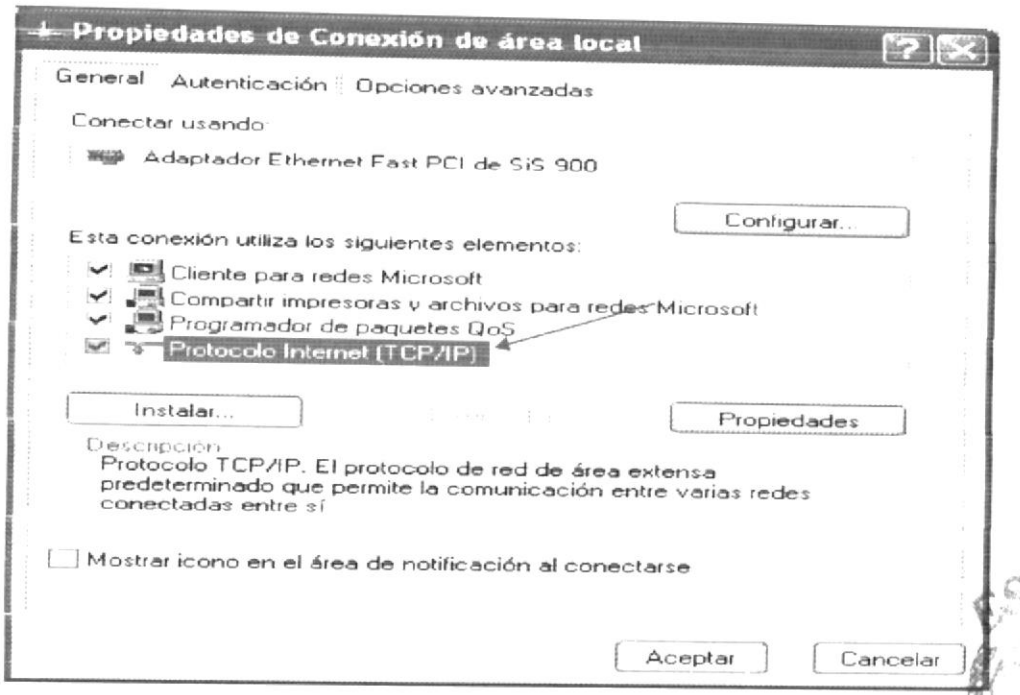


Figura 6-85: Propiedades de Conexión de Área Local

4.- Se procede a digitar la dirección IP al computador y hacer clic en **Aceptar.**

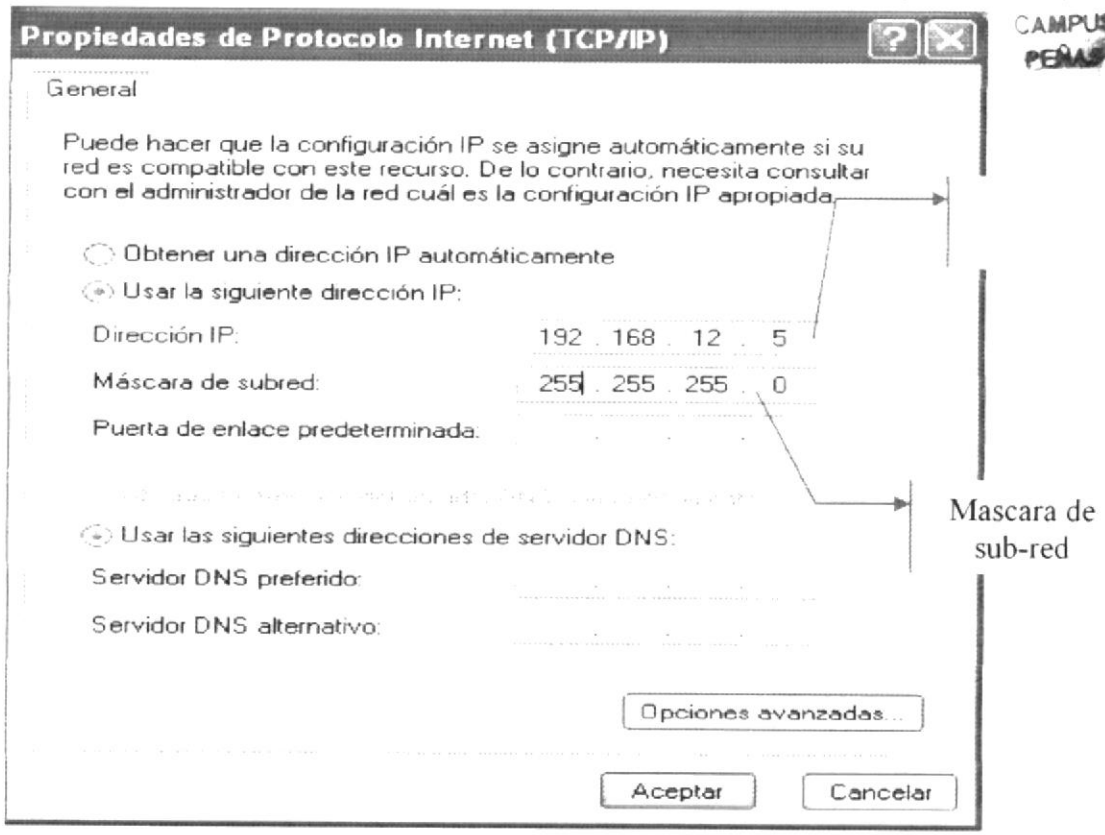


Figura 6-86: Propiedades de Protocolo Internet (Tcp/Ip)

BIBLIOTECA CAMPUS PEÑAS

5.- Una vez configurada la tarjeta de red hacer clic derecho en **Mis sitios de red**, y escoja la opción **Buscar equipos**.

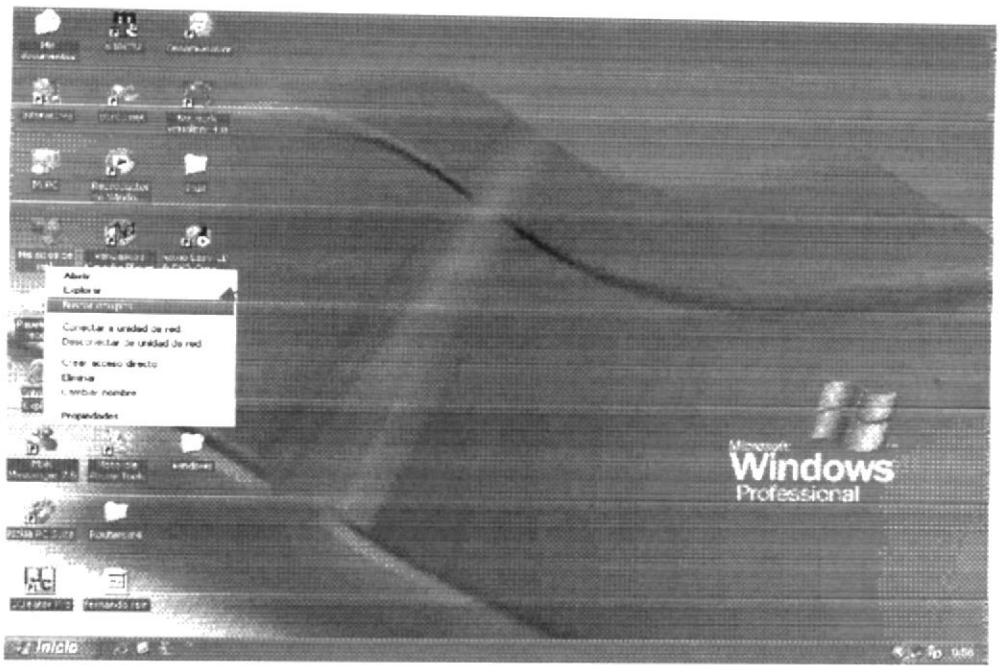


Figura 6-87: Selección Buscar Equipos

BIBLIOTECA CAMPUS PEÑAS

6.- En esta pantalla digite la dirección (IP) a buscar en la red en este caso la IP es del servidor.

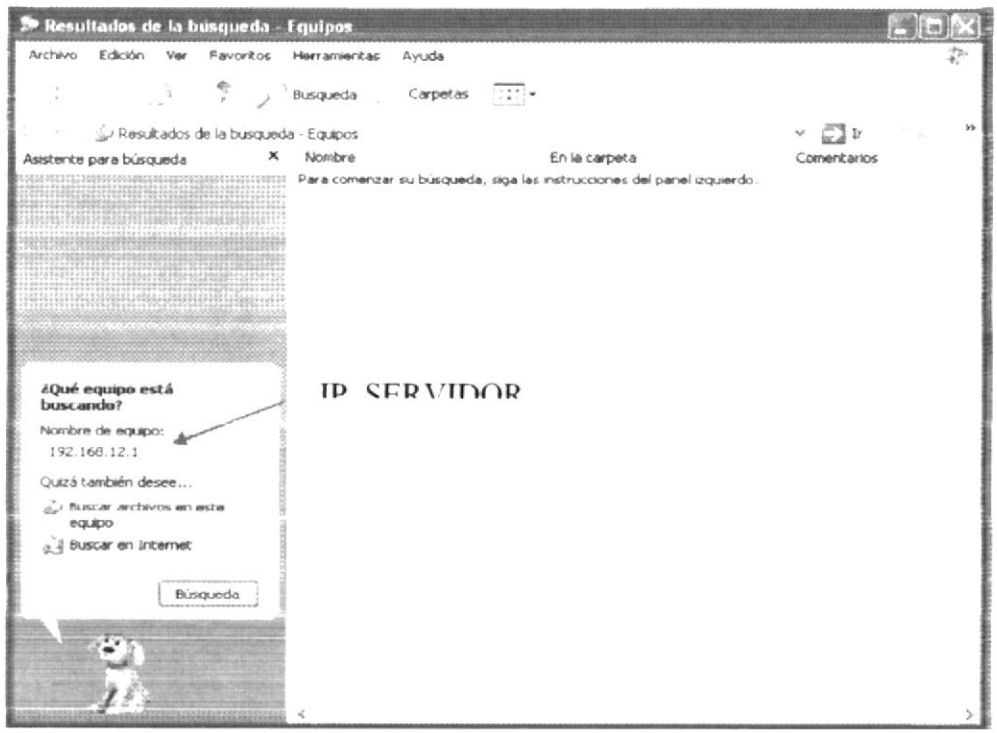


Figura 6-88: Búsqueda de Equipos

7.- En esta página se observa el resultado de la búsqueda.

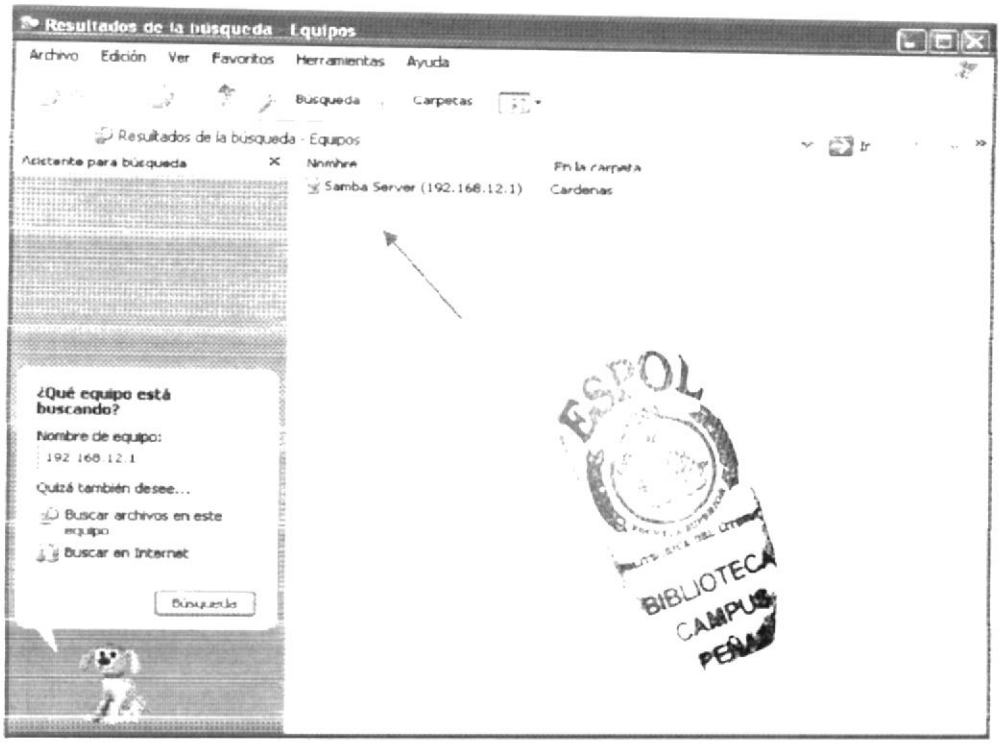


Figura 6-89: Resultado de la Búsqueda de Equipos

8.- Al proceder a ingresar al equipo aparecerá una pantalla en el cual se debe ingresar el usuario y la contraseña para poder acceder al servidor.



Figura 6-90: Ingreso de Usuario y Contraseña

9.- Ingrese a la carpeta creado en el servidor Linux.

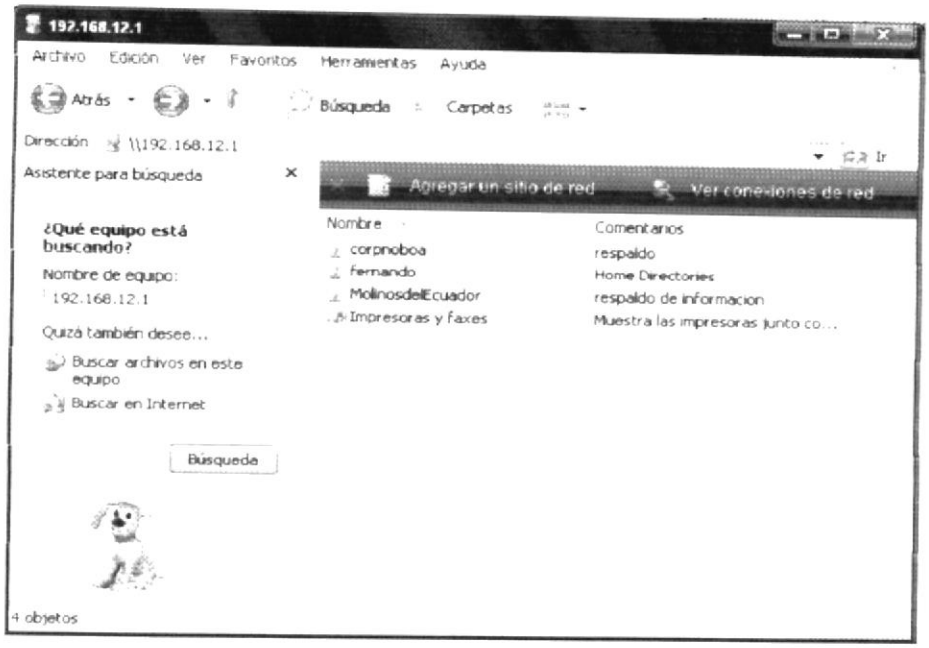


Figura 6-91: Recursos Compartidos

ESPOL
BIBLIOTECA
CAMPUS

10.- Se mostrará el archivo compartido por el **servidor de Linux.**

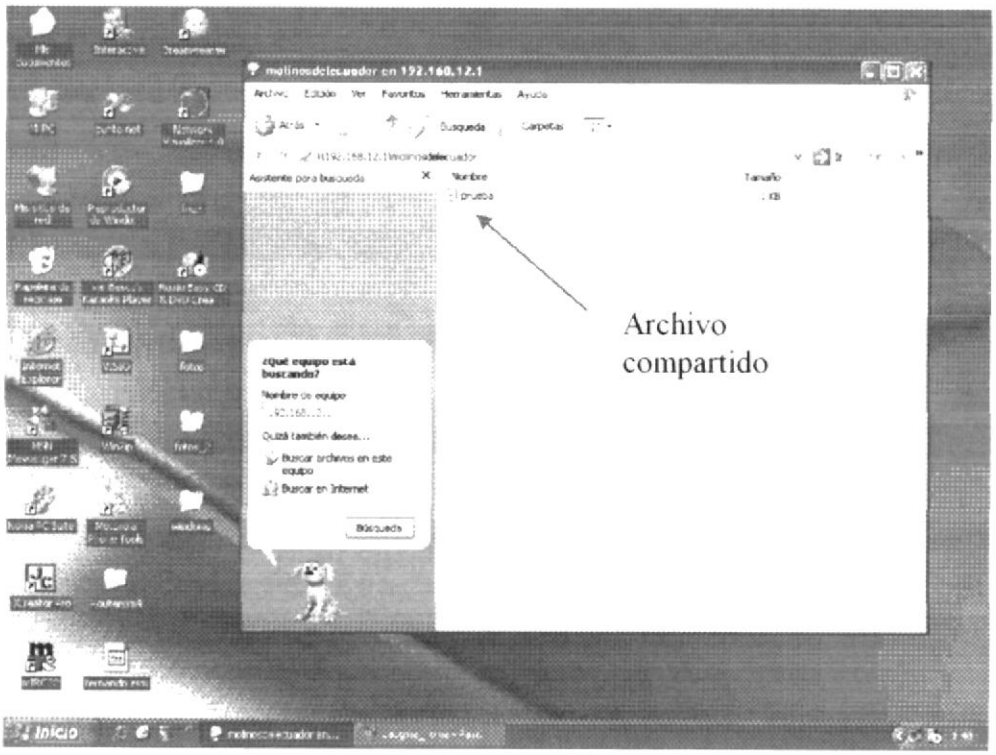


Figura 6-92: Archivo Compartido

11.- Ingrese archivo creado en Linux.

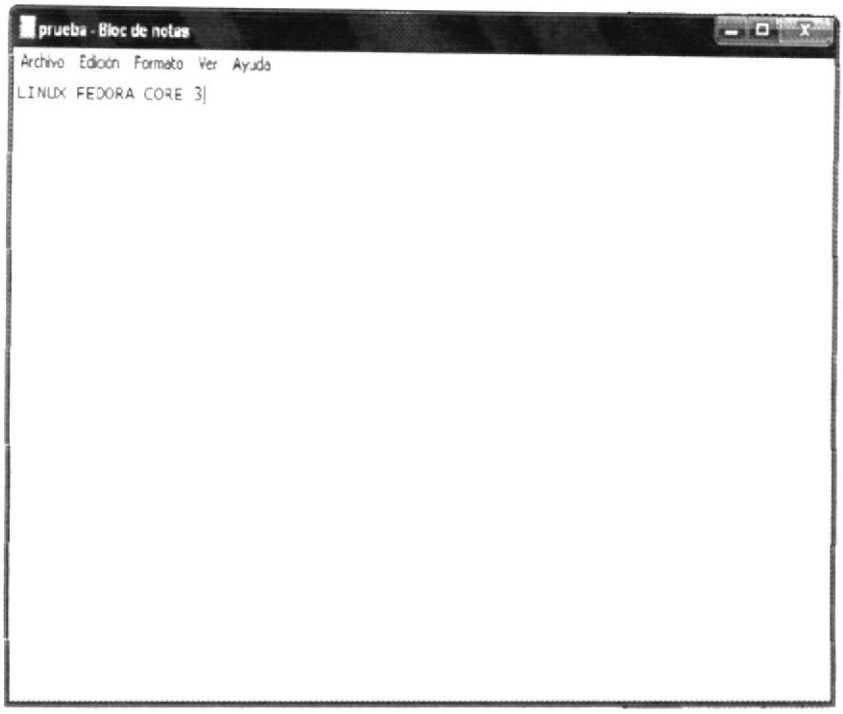


Figura 6-93: Información del Archivo Compartido

ESPOL
BIBLIOTECA
CAMPUS

6.9 SERVIDOR DNS

DNS ("Domain Name System") es otra herramienta primordial para el funcionamiento de Internet.
Es un conjunto de protocolos y servicios (base de datos distribuida) que permiten a los usuarios utilizar nombres en lugar de tener que recordar direcciones IP numéricas. Esta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP. A mas de ser más fácil de recordar las dirección es el nombre es el mas fiable.
Inicialmente los DNS nacieron de la necesidad de recordar fácilmente los sitios visitados o a visitar y sustituir el antiguo sistema de identificación de "host" en Internet que consistía en un gran archivo donde estaban almacenados los nombres y las direcciones IP de cada nodo de la red con el cual se podía establecer comunicación.
Desde un punto de vista técnico, un nombre de dominio es amas fácil de recordar, además cuando una empresa tiene su servidor DNS (y su propio nombre de dominio) se le puede localizar más fácilmente por Internet.

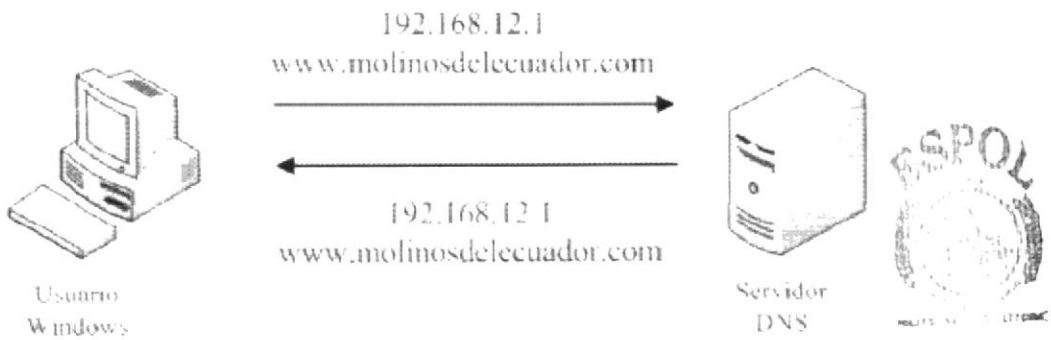


Figura 6-94: Servidor Dns

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

6.9.1 QUÉ ES UNA DIRECCIÓN IP

Para aquellos que no están muy familiarizados con Conectividad en Internet, en términos muy sencillos, las direcciones IP son la forma en que se localizan las computadoras. Para una computadora el manipular www.greenpeace.org o enviar un mail a usuarios@osmosislatina.com es sumamente ineficiente, por lo tanto utilizan direcciones IP.

DNS traduce el www.greenpeace.org a http://213.61.48.245 al igual que usuarios@osmosislatina.com es traducido a usuarios@216.230.213.71, como notará para un humano es mucho mas fácil recordar www.greenpeace.org que 213.61.48.245.Para quienes leyeron el documento : Como tener mi cuenta de Email @miempresa , se menciona un "apuntador", este es precisamente el "apuntador" al que se refiere el artículo.

6.9.2 ESTRUCTURA

- El sistema de nombres de dominio se implementa como una base de datos distribuida jerárquicamente que contiene diferentes tipos de datos, incluidos los nombres de host y de dominio.
- Los nombres de una base de datos DNS forman una estructura de árbol jerárquico denominada espacio de nombres de dominio.

6.9.3 CARACTERÍSTICAS

- Establece una correspondencia entre los nombres de direcciones IP.
- Consiste en una base de datos distribuidas por todo el Internet.
- Almacena información adicional.



6.9.4 FUNCIONAMIENTO

El sistema de DNS es una base de datos distribuida mantenida por miles de servidores DNS, cada uno de los cuales es responsable de una "zona" de Internet.
Cuando un programa cliente (por ejemplo, el navegador) hace una petición de una dirección de Internet, el servidor DNS del proveedor de acceso procesa la consulta, intentando buscar el dominio en su tabla de registro. Si no lo encuentra envía la petición a otro servidor DNS situado en un nivel superior de la jerarquía de nombres de dominios. Esta secuencia de peticiones se repite hasta que se obtiene la dirección IP del ordenador que corresponda al dominio consultado.

6.9.5 COMPONENTES

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

- Los Clientes DNS (resolvers), un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio?).
- Los Servidores DNS (name servers), que contestan las peticiones de los clientes, los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
- Y las Zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si este último no son delegados a otras zonas de autoridad.

6.9.6 USOS DEL DNS

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

- **Resolución de nombres:** Dado el nombre completo de un host (por ejemplo blog.smaldone.com.ar), obtener su dirección IP (en este caso, 208.97.175.41).
- **Resolución inversa de direcciones:** Es el mecanismo inverso al anterior. Consiste en, dada una dirección IP, obtener el nombre asociado a la misma.
- **Resolución de servidores de correo:** Dado un nombre de dominio (por ejemplo gmail.com) obtener el servidor a través del cual debe realizarse la entrega del correo electrónico (en este caso, gmail-smtp-in.l.google.com).

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

6.9.7 ZONAS

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

Un DNS Server maneja 2 tipos de Zonas:

Primarias

Secundarias



6.9.7.1 ZONAS ESTÁNDARES

6.9.7.1.1 ZONAS PRIMARIAS

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

6.9.7.1.2. ZONAS SECUNDARIAS

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

6.9.8. REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR DNS

- Un computador con Linux Fedora Core 3 instalado.
- Tarjeta de red.
- Configuración de IP Estática.
- Paquete de Bind instalado.

6.9.9 CONFIGURACIÓN DEL SERVIDOR DNS

1.- Verifique si se tiene el paquete de DNS instalado, e ingrese al directorio **etc** para configurar el archivo **named.conf**

```
root@localhost /] #  rpm –q bind
root@localhost /] # cd /etc
root@localhost etc] #  vi named.conf
```

rpm –q	Verifica si esta instalado un paquete
cd	Ingresa a un directorio
vi	Edita un archivo
named.conf	Archivo de l samba

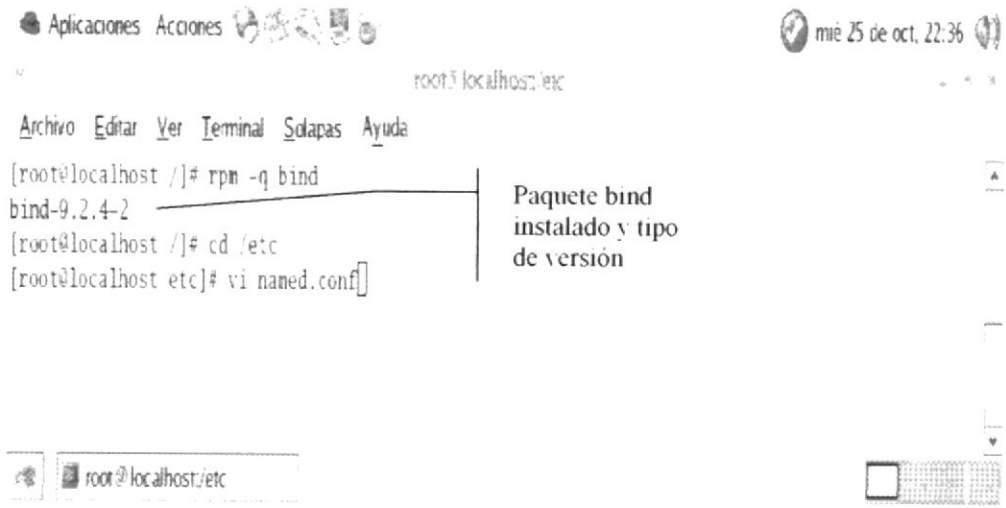


Figura 6-95: Verificar Paquete Dns

2.- Una vez que ha ingresado en el archivo **named.conf** proceda configurar el dominio que se va a utilizar.

zone "molinosdelecuador.com" IN {: Es el nombre del dominio.
type master: Tipo de la Zona, en este caso zona principal.
file "molinosdelecuador.com.zone": Es el nombre del archivo que se va a editar.
Allow-update { none; }: Es el que permite actualizar la zona.

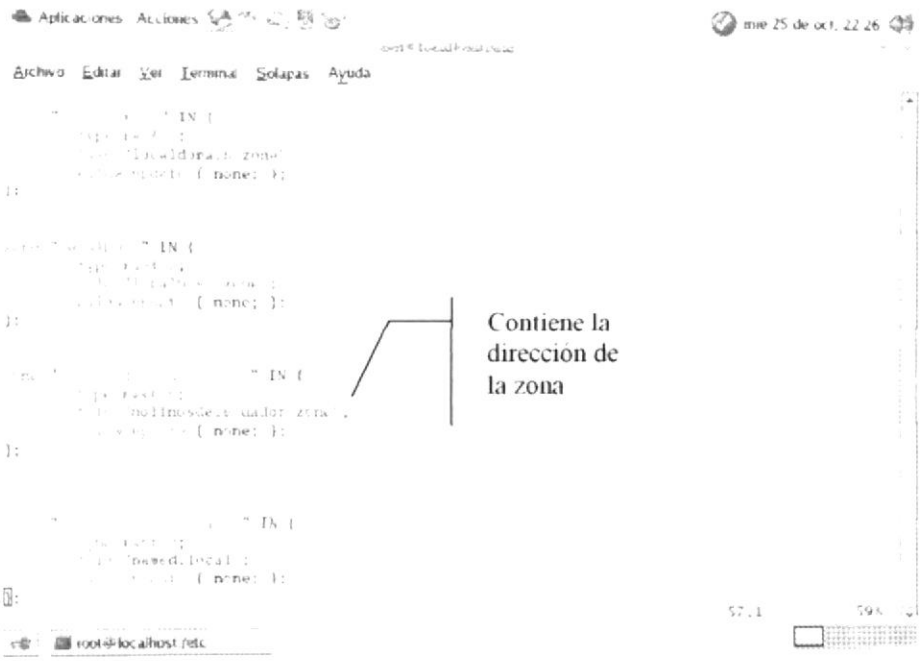


Figura 6-96: Archivo Named.Conf

- Como primer paso copiar las siguientes líneas

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

- Realizar los siguientes cambios

```
zone "molinosdelecuador.com" IN {
type master;
notify no;
file "molinosdelecuador.com.zone";
allow-update {none};
};
```

ESPOL BIBLIOTECA CAMPUS PEÑAS

Los parámetros en esta sección como **type**, indican si se tratará de un servidor principal (master) o secundario (slave) de la zona.

El parámetro **file**, indicará el fichero que almacenará la base de datos de resolución y es relativo al directorio de trabajo definido anteriormente.

Agregar el parámetro **notify** para que se notifiquen los cambios a los servidores secundarios.

- Salir guardando los cambios con el comando **wq**

3.- Ingresar al directorio del **named** y hacer un **ls** para listar el contenido del directorio **named** donde debe estar el archivo **localhost.zone**

```
root@localhost etc] #  cd /var
root@localhost var] #  cd named
root@localhost named] #  ls
```

cd	Ingresa a un directorio
ls	Lista el contenido del directorio

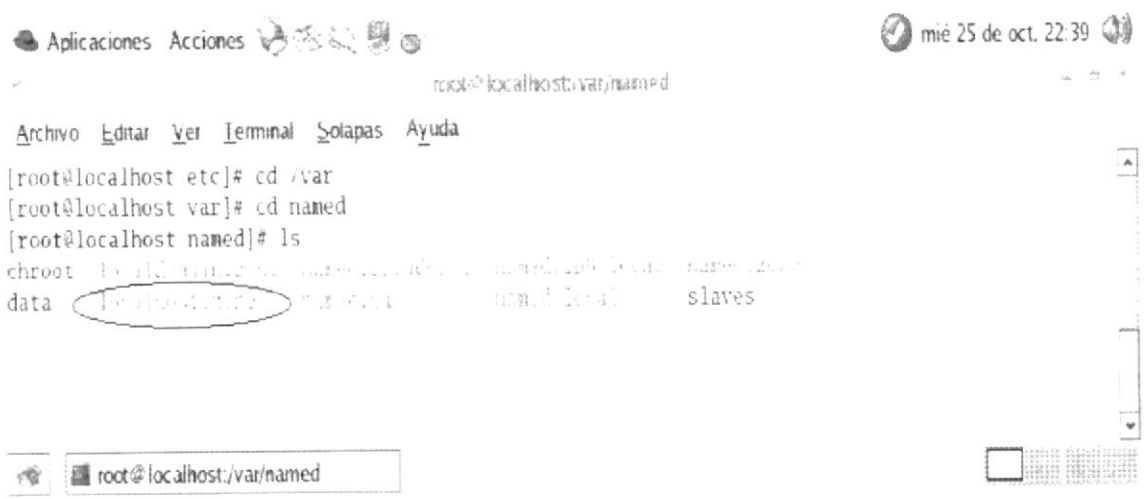


Figura 6-97: Lista de Archivos del Named

4.- Una vez que verificada la existencia del archivo **localhost.zone** realizar una copia del contenido del archivo y verificar su creación con el comando **ls**.

```
root@localhost named] # cp localhost.zone  molinosdelecuador.com.zone
root@localhost named] #  ls
```

cp	Copia archivos de un directorio a otro
localhost.zone	Archivo a copiar
ls	Lista el contenido del directorio



Figura 6-98: Copia del Archivo Localhost.Zone

5.- Modificar el archivo creado en este caso molinosdelecuador.com.zone.

```
root@localhost named] # vi molinosdelecuador.com.zone
```

vi	Edita un archivo

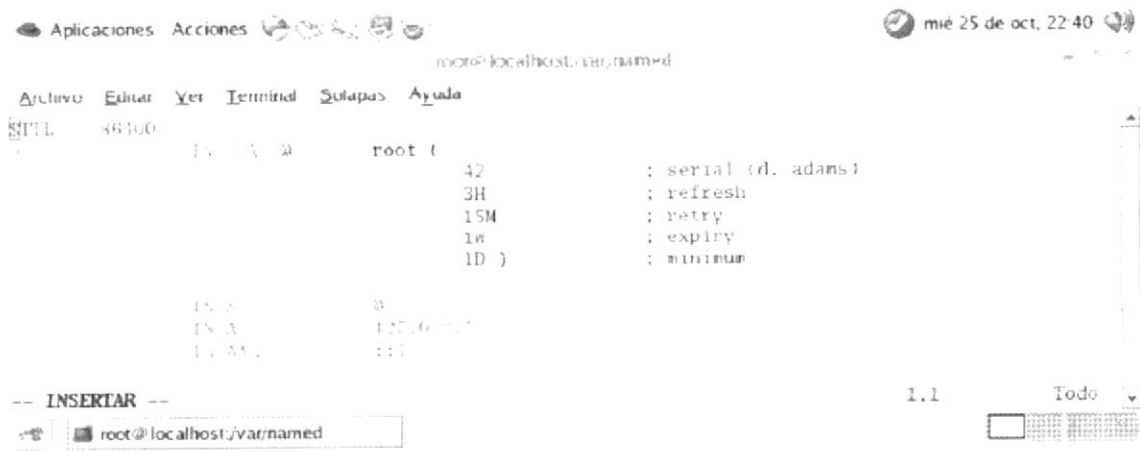


Figura 6-99: Editar Fichero molinosdelecuador.com.zone

Para entender mejor este fichero se detalla el significado de ciertas palabras que se encuentren en el mismo:

NS: Es el Name Server e indica que computadora es el servidor DNS
SOA: Es una abreviatura de Start Of Authority
@: Es una notación especial que simboliza el origen
CNAME: Registra nombre canónico, hace que un nombre sea un alias
REFRESH: Tiempo de RESTAURACIÓN de la página
RETRY: Tiempo de reintento de consulta
EXPIRY: Tiempo de expiración de la página
MINIMUM: Tiempo total de vida
:Wq Salir y grabar



- Esta pantalla muestra los cambios realizados.

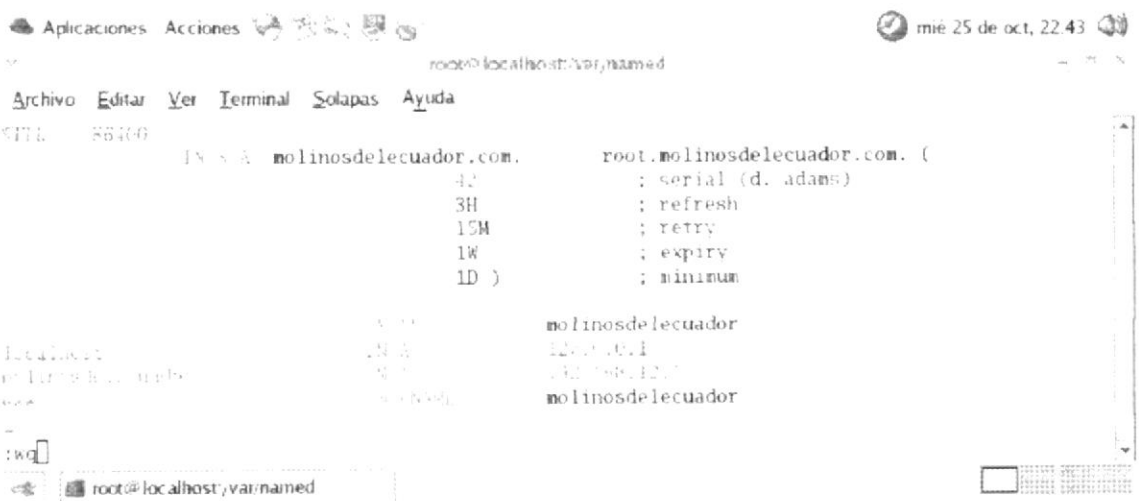


Figura 6-100: Seteo de Campos en el Named.Conf

6.- Copiar el archivo a la siguiente ruta.

/var/named/chroot/var/named



Figura 6-101: Copia del Archivo a Otro Directorio

7.- Ingresar al directorio **etc** y editar el archivo **resolv.conf**.

```
root@localhost named] #  cd /etc
root@localhost etc] #  vi resolv.conf
```

cd	Ingresa a un directorio
vi	Edita un archivo



Figura 6-102: Ingreso al Archivo Resolv.Conf

- Cabe indicar que en el **nameserver** debe de digitar la **IP** del **servidor**.



Figura 6-103: Editar el Archivo Resolv.conf

BIBLIOTECA CAMPUS PEÑAS

8.- Inicializar todos los servicios y ver el estado con los siguientes comandos.

root@localhost etc] # service named restart
root@localhost etc] # service named status



Figura 6-104: Iniciar Servicios Named

9.- Hacer **ping** a la dirección Web del servidor para verificar el funcionamiento.

root@localhost etc] # ping www.molinosdelecuador.com

Ping Comando que comprueba si se llega a un host remoto

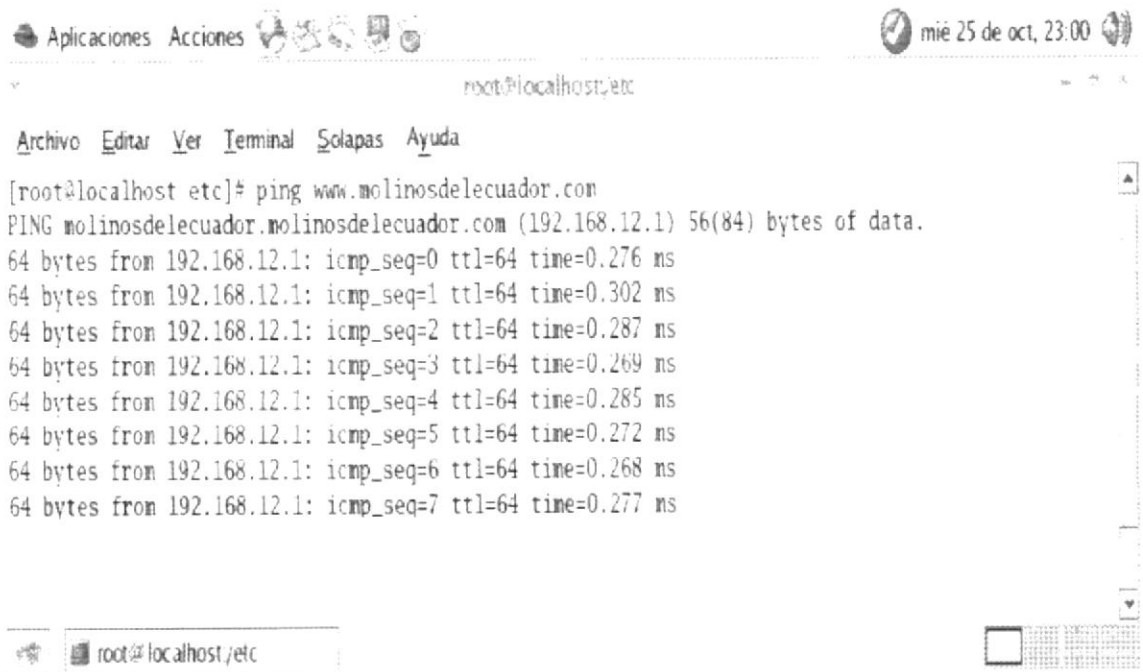


Figura 6-105: Ping al Dominio Molinos del Ecuador.com

6.9.10. CONFIGURACIÓN EN CLIENTE WINDOWS –DNS

1.- Vaya a **Mis Sitios de red** hacer clic derecho y elija la opción de **Propiedades.**

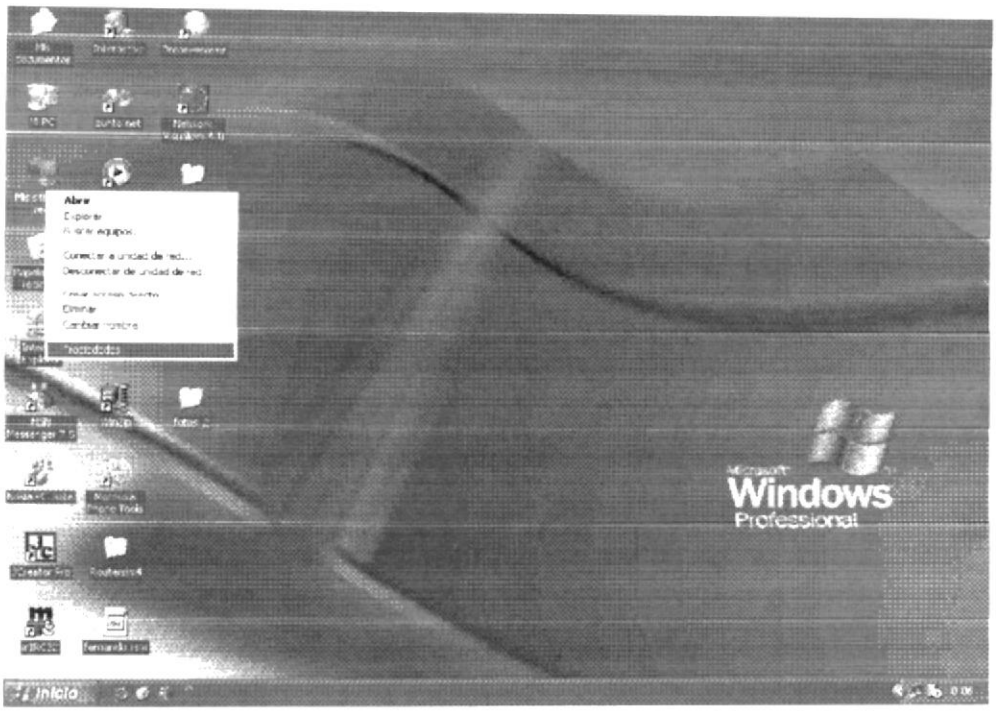


Figura 6-106: Selección de Propiedades de Mis Sitios de Red

BIBLIOTECA CAMPUS PEÑA

2.- Hacer clic derecho en la opción de **conexión de área local**, y elegir la opción de **Propiedades**.

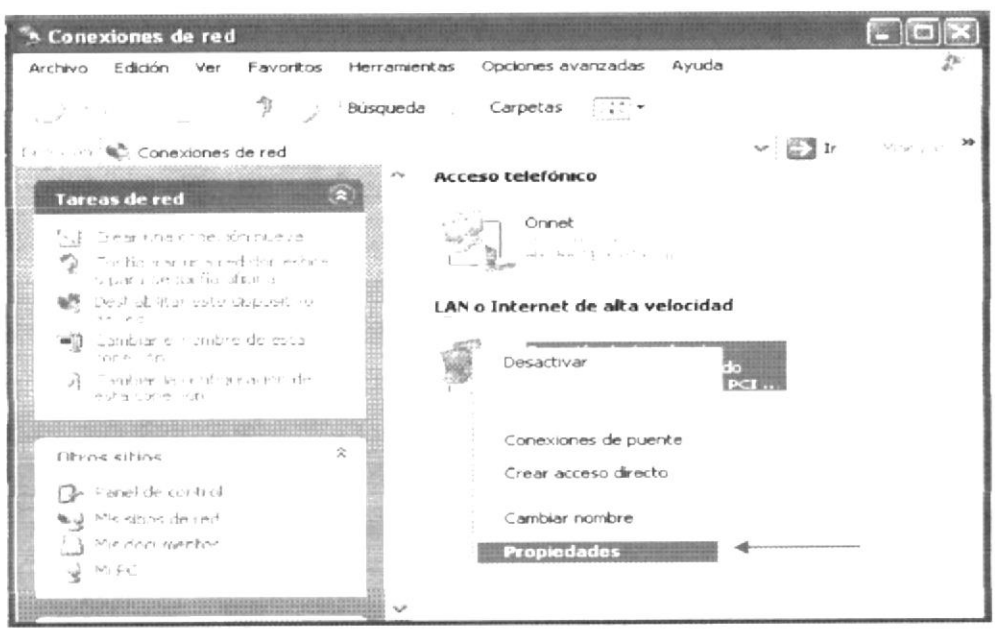


Figura 6-107: Propiedades de Conexiones de Red

3.- En esta ventana vaya a la opción TCP/IP para configurar la tarjeta de red.

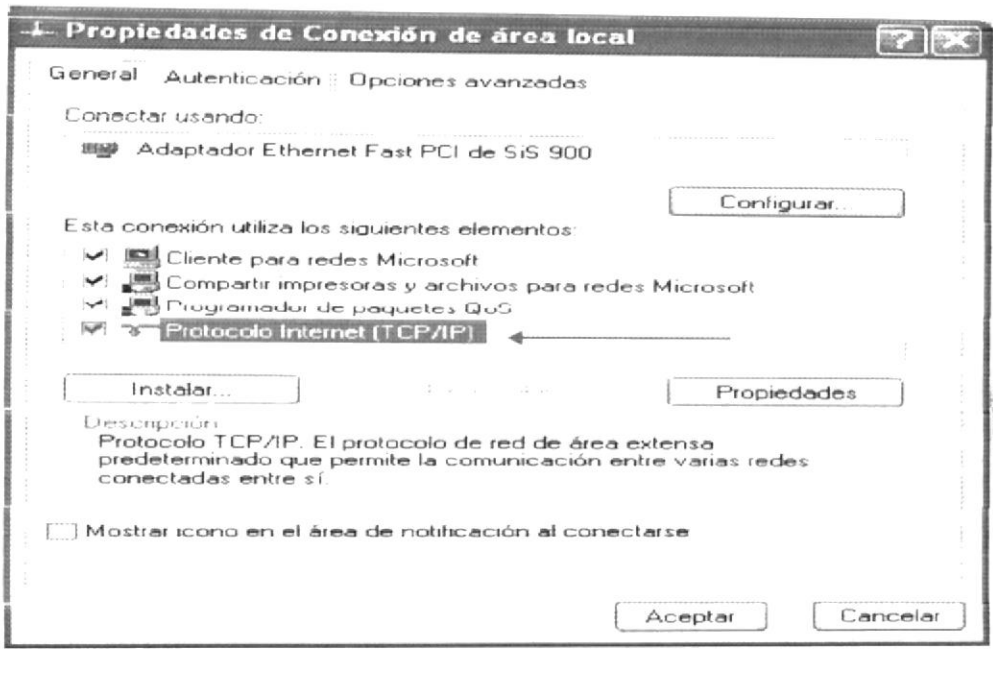


Figura 6-108: Protocolo Internet Tcp/Ip

4.- Proceda digitar una dirección al computador y digite nuestro DNS la IP del servidor y hacer clic en **Aceptar**.

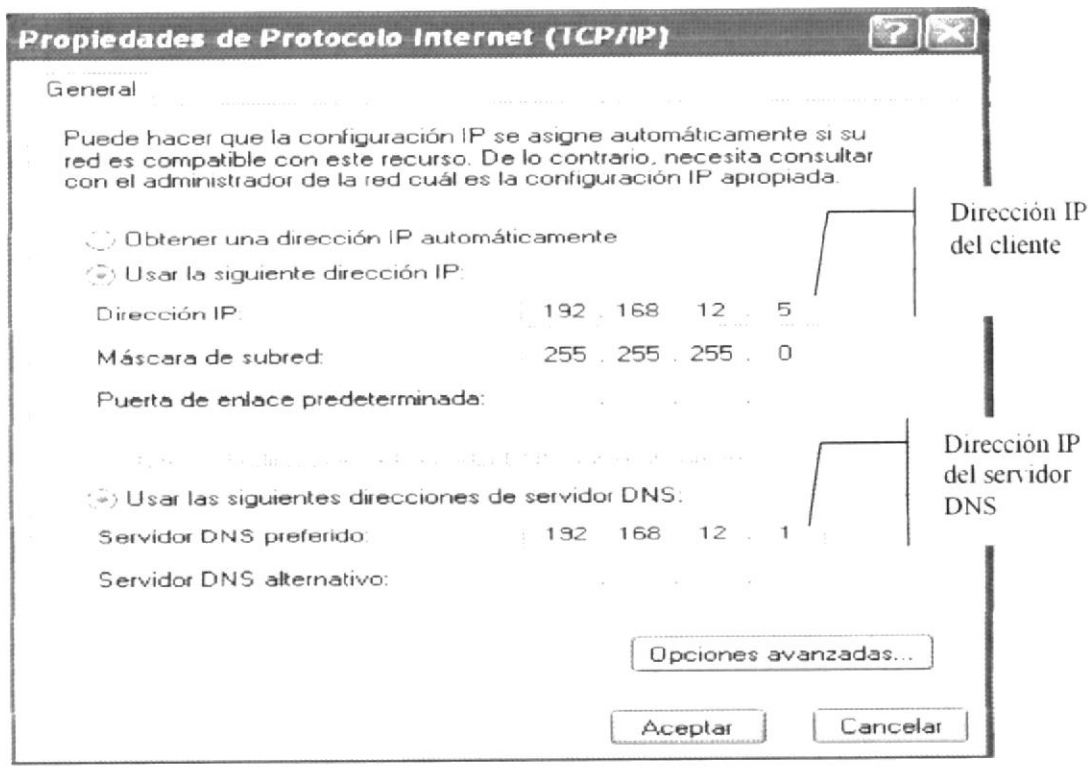


Figura 6-109: Ingreso de Ip y Dns (Servidor).

5.- Ingrese a **Inicio, Ejecutar** y digite **cmd**.

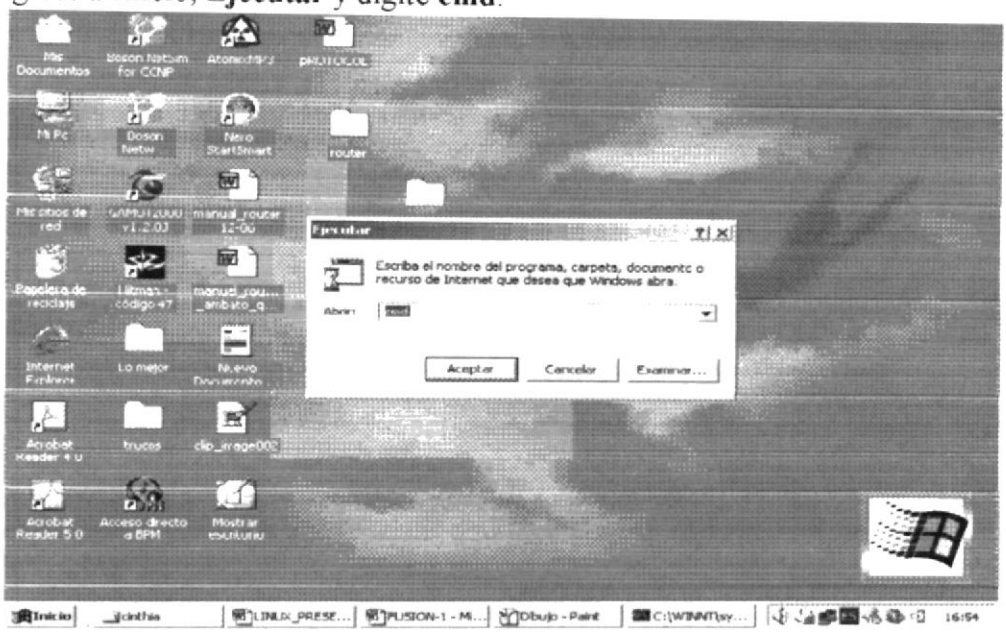


Figura 6-110: Ingreso al Cmd

Una vez en el cmd digite el dominio del servidor (www.molinosdelecuador.com) y mostrará respuesta por parte del servidor.

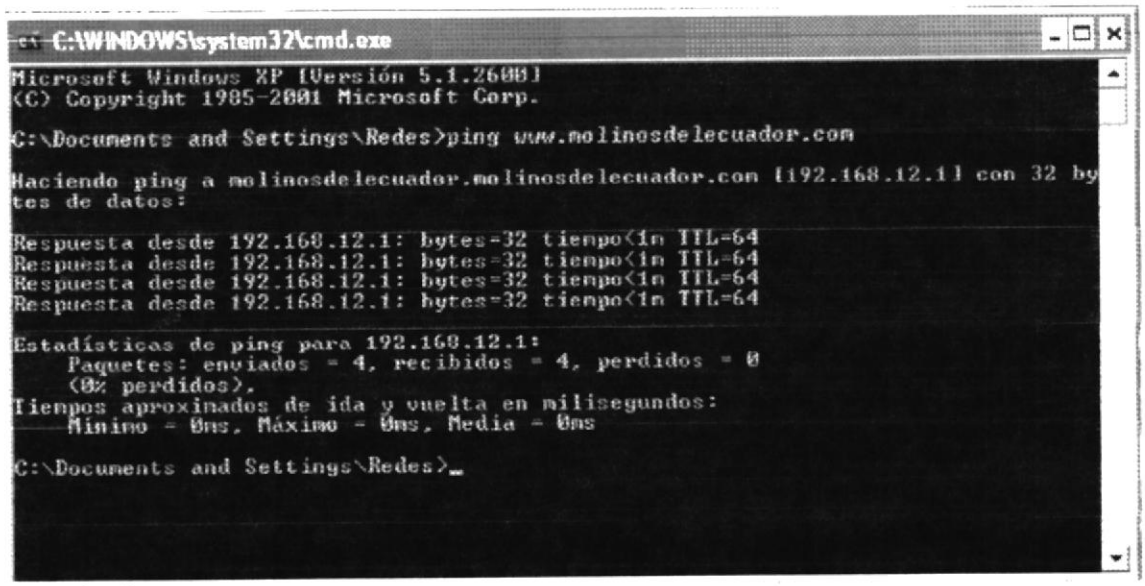


Figura 6-111: Pin.g y Respuesta del Servidor

ESPOL BIBLIOTECA CAMPUS PEÑAS

6.10 SERVIDOR WEB SERVER

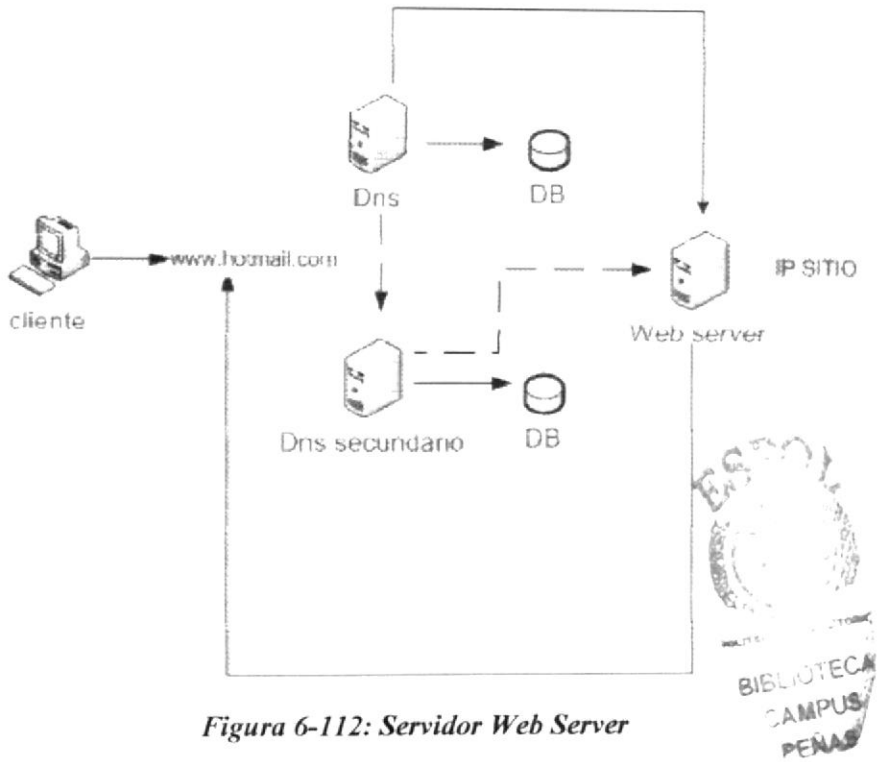


Figura 6-112: Servidor Web Server

Un servidor Web es una computadora conectada permanentemente al Internet (ha de tener asignada una dirección IP) que espera conexiones de clientes Web para que estos le soliciten datos, que normalmente son archivos como paginas de su sitio, además administra las cuentas de correo, bases de datos, etc. Es una computadora de alto rendimiento que lleva a cabo todo el procesamiento de datos e información.
Los servidores y los navegadores se comunican mediante el protocolo de transferencia de hipertexto (HTTP), un lenguaje creado para transferir documentos de hipertexto en la Web. o servicios Web a veces se llaman servidores HTTPD.
Un servidor Web es un programa de aplicación que satisface las solicitudes HTTP, FTP, SMTP, HTTPD realizadas por los navegadores. Para ello, el ordenador que la soporta debe estar conectado a la Internet o a la Intranet y por lo tanto, ha de tener asignada una dirección IP.
Una dirección de Internet o Web (a veces llamada dirección URL o Localizador de recursos universal) suele estar compuesta por cuatro partes:

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

Cabe destacar el hecho de que la palabra servidor identifica tanto al programa como a la máquina en la que dicho programa se ejecuta. Existe, por tanto, cierta ambigüedad en el término, aunque no será difícil diferenciar a cuál de los dos se refiere en cada caso. En este artículo se refiere siempre a la aplicación.
Un servidor web se encarga de mantenerse a la espera de peticiones HTTP llevada a cabo por un cliente HTTP que se suele conocer como navegador. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. A modo de ejemplo, al teclear www.wikipedia.org en nuestro navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo muestra en pantalla. Como se muestra con este ejemplo, el cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.
Sobre el servicio web clásico se puede disponer de aplicaciones web. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- **Aplicaciones en el lado del cliente:** el cliente web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java o Javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Normalmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje javascript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins.

- **Aplicaciones en el lado del servidor:** el servidor web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor suelen ser la opción por la que se opta en la mayoría de las ocasiones para realizar aplicaciones web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad adicional, como sí ocurre en el caso de querer ejecutar aplicaciones javascript o java. Así pues, cualquier cliente dotado de un navegador web básico puede utilizar este tipo de aplicaciones.

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).



6.10.1 REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR WEB

- Un computador con Linux Fedora Core 3 instalado.
- Configuración IP Estática
- Tarjeta de red.
- Configuración de la tarjeta de red.
- Paquete de Apache instalado.
- Haber configurado previamente el DNS (Bind).

6.10.2 CONFIGURACIÓN DEL SERVIDOR WEB SERVER

1.- Verificar si se tiene instalado el paquete del web Server.

```
root@localhost ~] #  rpm –q httpd
```



Figura 6-113: Verificación del Paquete Web Server

2.- Ingresar al directorio **conf** con la siguiente ruta.

root@localhost /] # cd /etc/httpd/conf

cd	Ingresa a un directorio
etc/httpd/conf	Directorios

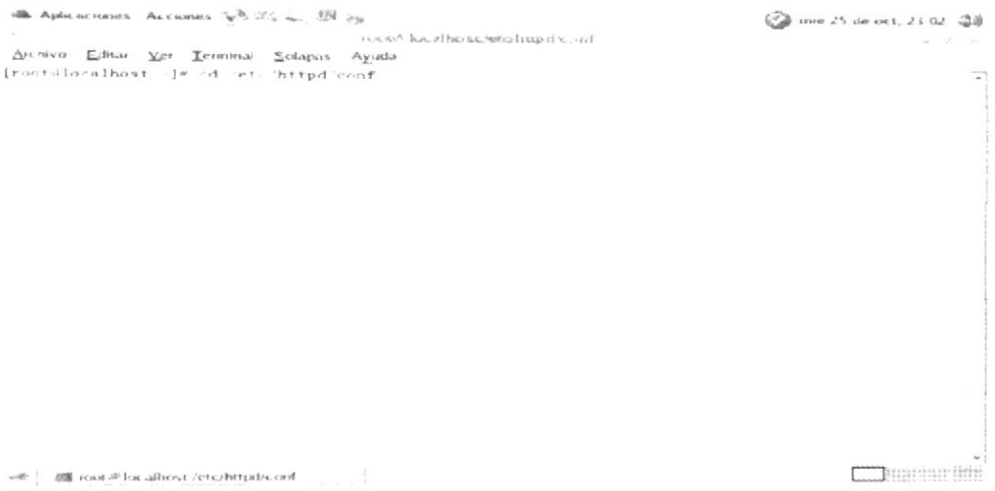


Figura 6-114: Ruta de Ingreso a Directorio Conf

3.- Editar el archivo **httpd.conf**

root@localhost conf] # vi httpd.conf

vi	Edita un archivo



Figura 6-115: Ingreso al Archivo Httpd.Conf

Descomentar las siguientes líneas

Listen 80 (puerto donde escucha el Web Server)



Figura 6-116: Descomentar Puerto listen 80

Document Root "var/www/html" (donde se va a guardar el sitio web)

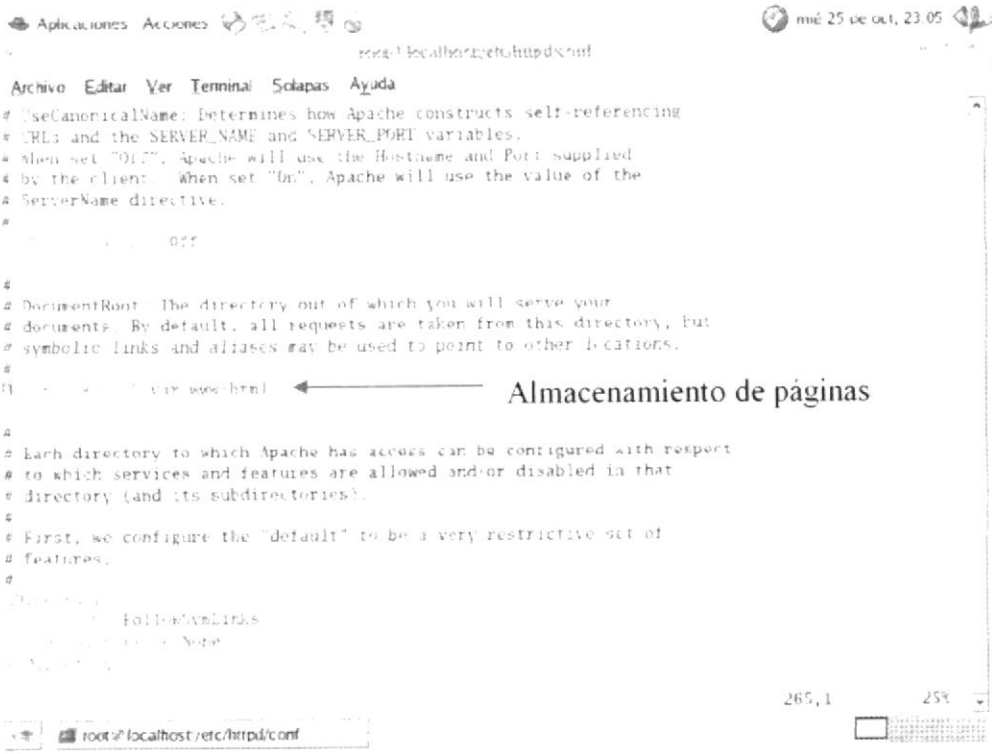


Figura 6-117: Dirección de Almacenamiento del Sitio Web

NameVirtualHost *:80 (Escucha a nivel de más páginas)

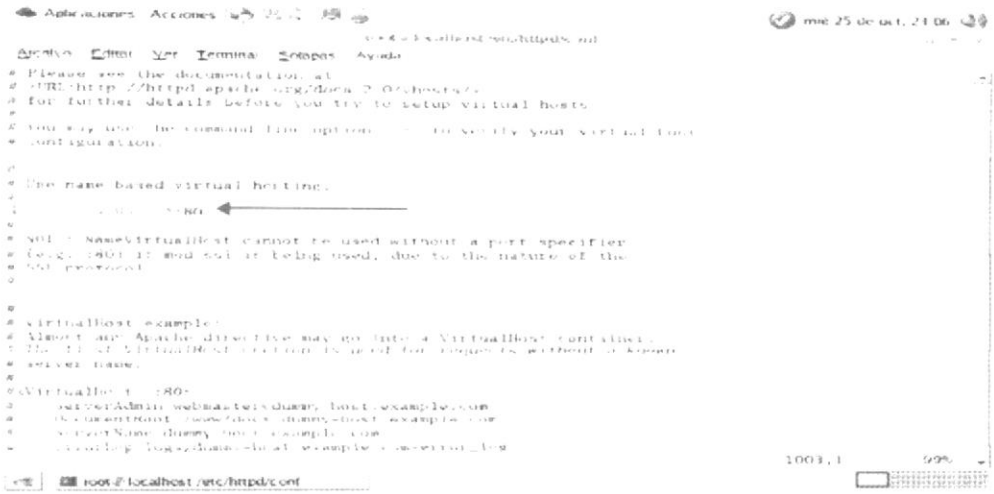


Figura 6-118: Descomentar Name Virtualhost

Copie el párrafo del <virtual host *:80>, descomente las líneas necesarias y realice los siguientes cambios.

<VirtualHost *:80>
ServerAdmin root@localhost
DocumentRoot /var/www/html/sitio
ServerName www.molinosdelecuador.com
</VirtualHost>

<VirtualHost *:80> Host virtual que escucha por el puerto 80
ServerAdmin Administrador Web de la computadora
DocumentRoot Ruta completa de donde se aloja la página.
ServerName Dirección del dominio



Figura 6-119: Configuración del Virtualhost

4.- Digitar el siguiente comando.

root@localhost conf] # cd /var/www/html

cd	Ingreso a directorio
/var/www/html	Directorios



Figura 6-120: Ruta de Ingreso al Directorio Html

5.- Crear una carpeta donde se alojará nuestro sitio Web, en este caso el nombre de la carpeta es el mismo que ingresará en el **DocumentRoot,** que es el sitio web.

root@localhost html] # mkdir sitio

mkdir	Crea un directorio

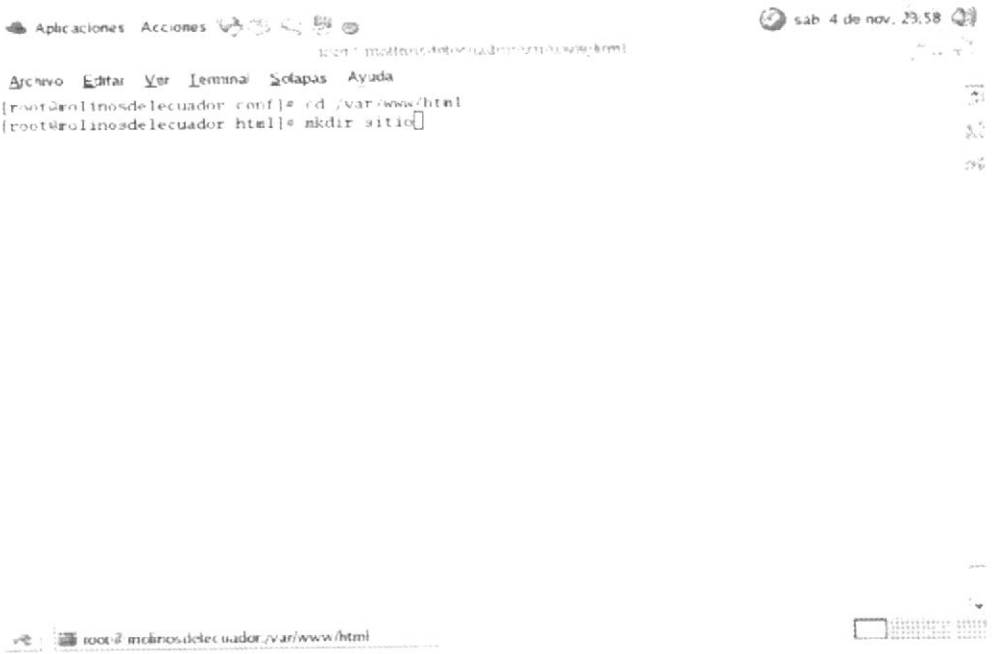


Figura 6-121: Creación de la Carpeta

6.- Ingresar al sitio y crear un archivo html.

root@localhost html] # cd sitio
root@localhost sitio] # vi index.html

cd	Ingreso a un directorio
vi	Edita un archivo



Figura 6-122: Creación del Archivo Index.html

7.- Levantar todos los servicios con los siguientes comandos.
root@localhost /] # service named restart
root@localhost /] # service httpd start

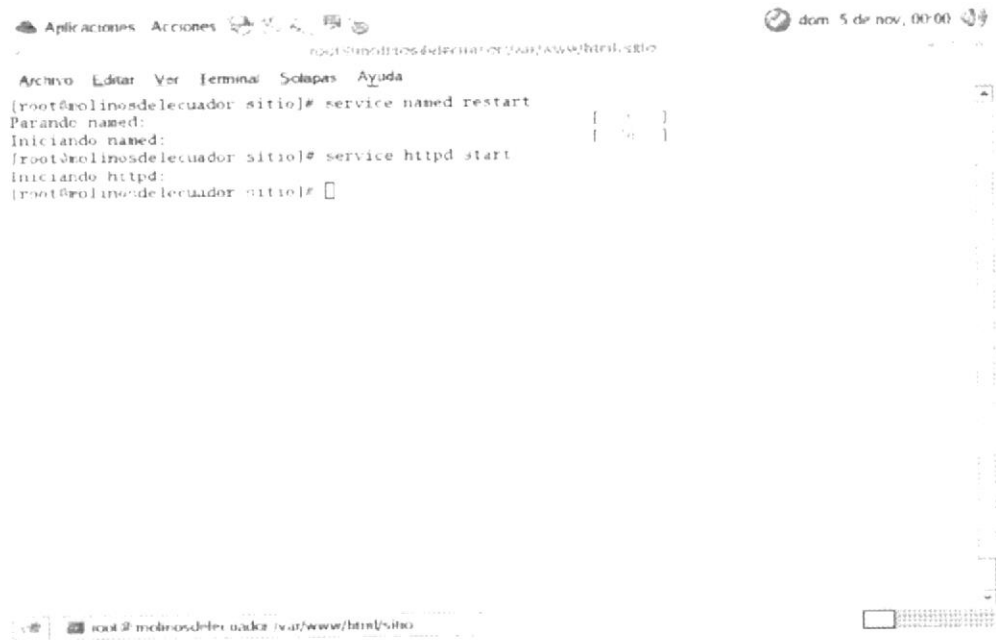


Figura 6-123: Iniciar los Servicios httpd

6.10.3 CONFIGURACIÓN EN CLIENTE WINDOWS – WEB SERVER

1.- Ir a **Mis Sitios de red** y hacer clic derecho y elegir la opción de **Propiedades**.

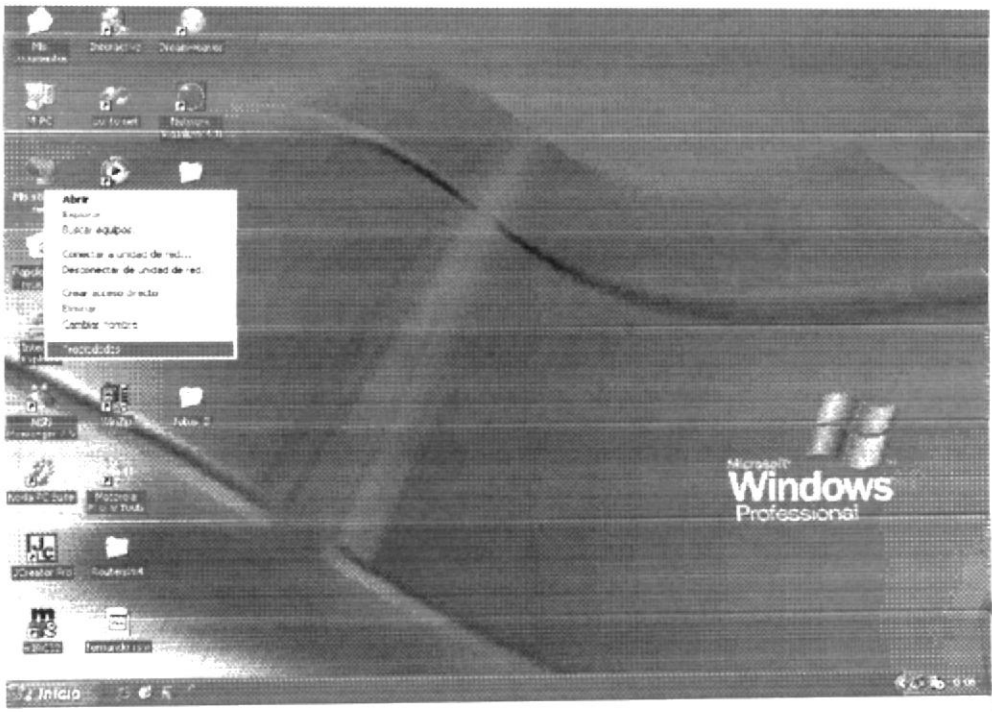


Figura 6-124: Selección de Propiedades de Mis Sitios de Red

BIBLIOTECA CAMPUS PEÑAS

2.- Hacer clic derecho en la opción de **Conexión De Área Local**, y elegir la opción de **Propiedades**.

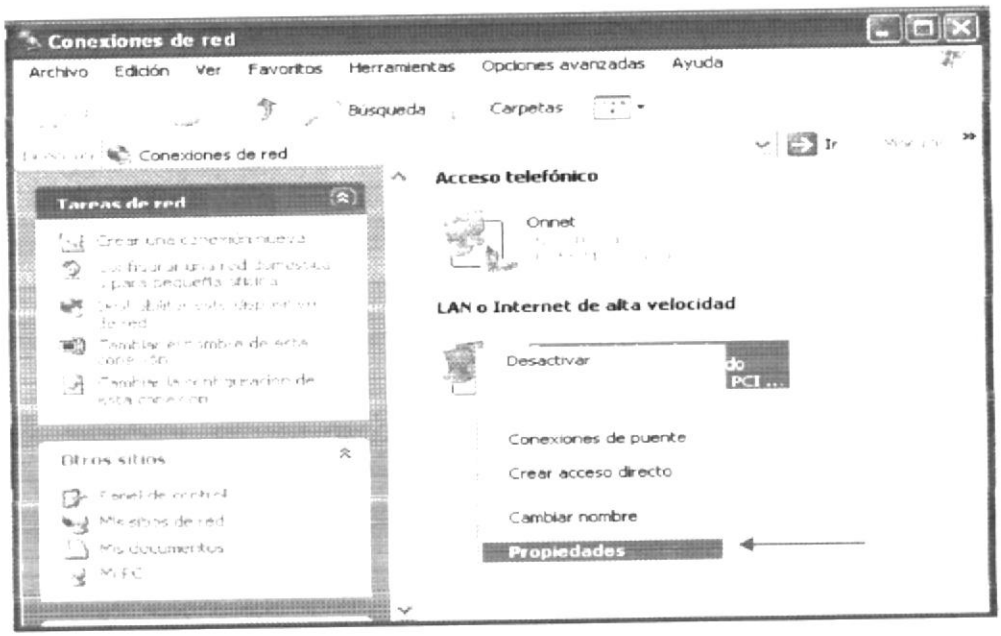


Figura 6-125: Propiedades de Conexiones de Red

3.- En esta ventana se muestra la opción TCP/IP para configurar la tarjeta de red.

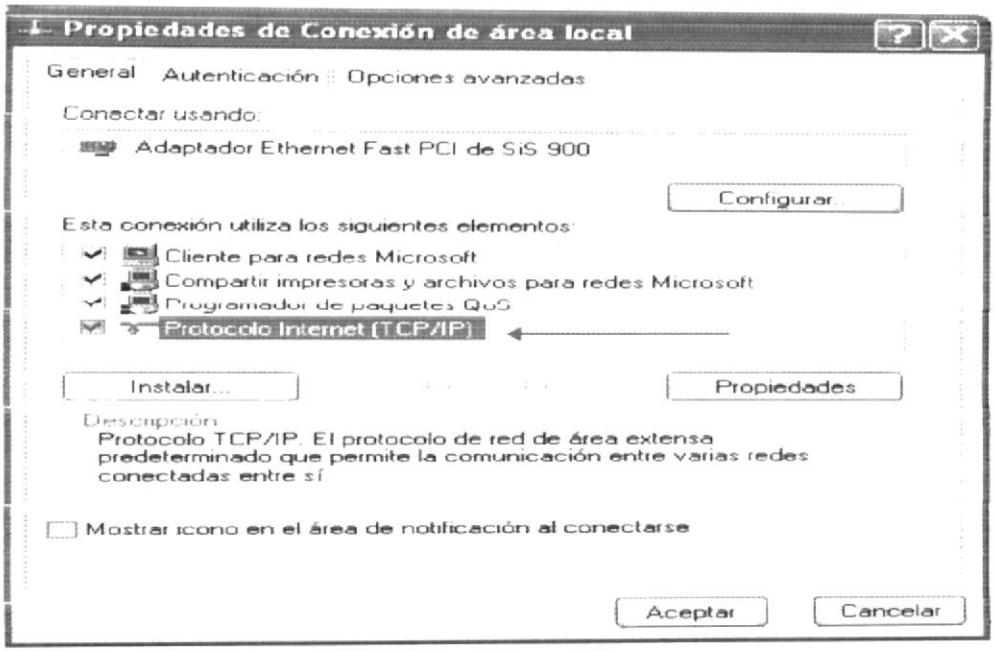


Figura 6-126: Protocolo Internet Tcp/Ip

4.- Proceder a digitar una dirección (IP) al computador y digitar como nuestro **DNS** la **IP** del **Servidor** y hacer clic en **Aceptar**.

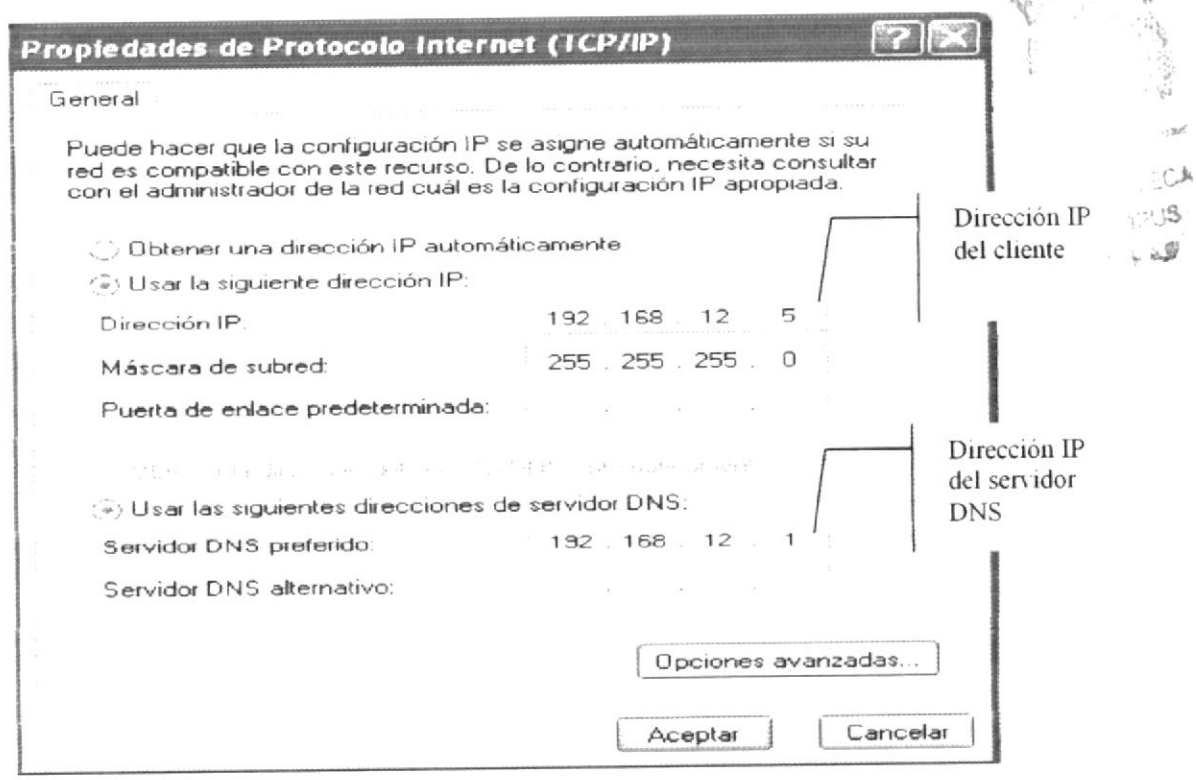


Figura 6-127: Ingreso de Ip y Dns (Servidor).

5.- En el icono **Internet Explorer**, hacer clic derecho y elegir la opción **Abrir la página principal**.

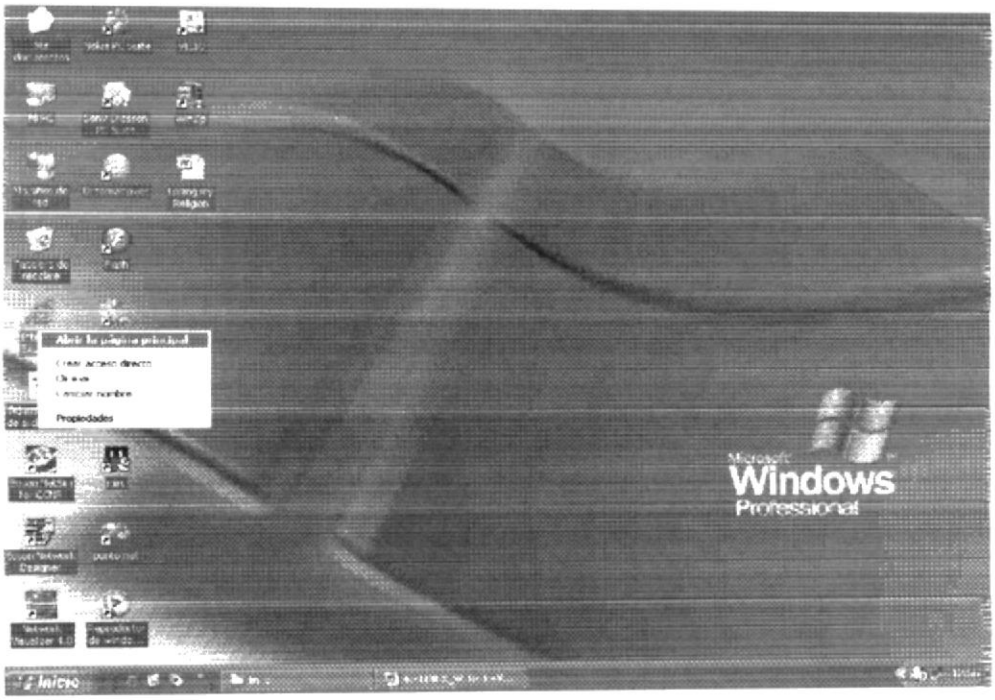


Figura 6-128: Ingreso al Internet Explorer

6.- En el **Internet Explorer** digitar la dirección de nuestra página.

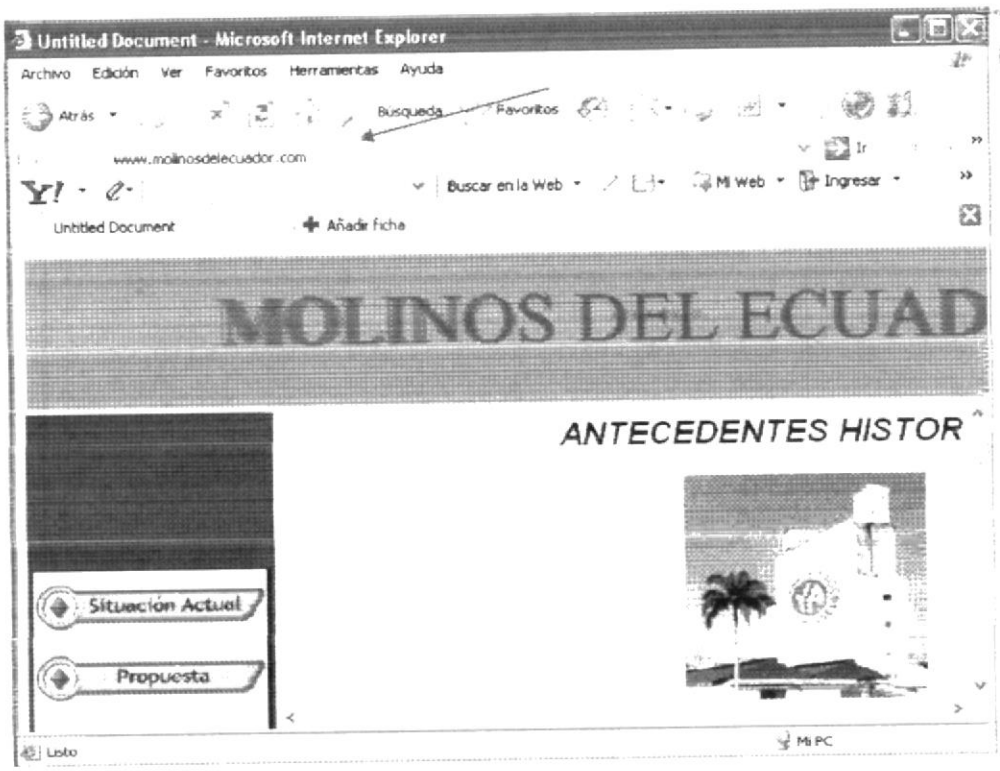


Figura 6-129: Presentación de la Página

6.11 SERVIDOR SENDMAIL

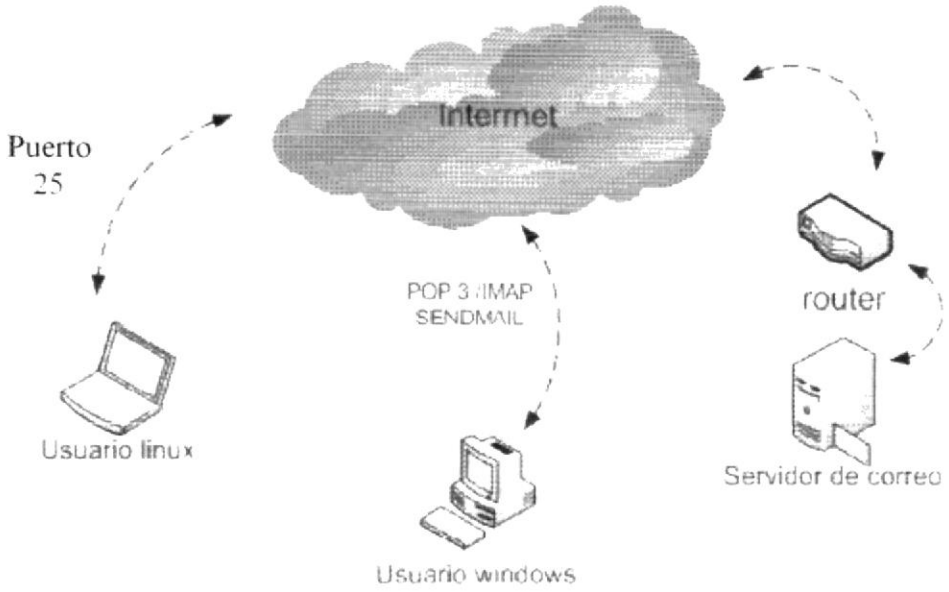


Figura 6-130: Servidor Sendmail

Al igual que los servidores de páginas, existen varios servidores de Mail (también llamados MTA "Mail Transfer Agent") uno de los más comunes es *Sendmail*, el archivo principal de configuración *sendmail.cf* es considerado uno de los archivos más complejos con los que trabaja un administrador.

Sendmail es el agente de transporte de correo mas común de Internet en los sistemas Linux.
Mail Server es un servidor de mail POP3 y SMTP que soporta un número ilimitado de dominios, casillas de mail, y listas de correo.
Mail Server es un programa chico, diseñado para manejar los servicios POP y SMTP para pequeñas empresas o para uso individual.
Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta;

SMTP simple Mail Tranfer 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 pasarselos al usuario.

IMAP (Internet Message Access Protocol): su finalidad es la misma que la del POP3, pero el funcionamiento y las funcionalidades son diferentes.
Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

6.11.1 CARACTERÍSTICAS PRINCIPALES

Existen una gran variedad de programas de correo electrónico que proveen al usuario de una aplicación para la creación y envió de mail. Estos programas son los llamados agentes de usuario o MUA (Mail User Agent), y su propósito es el aislar al usuario de los agentes de transporte o MTA (Mail Transport Agent), que son los encargados de transferir los mail a su correcto destino.

Sendmail es el agente de transporte de correo mas común de Internet en los sistemas Linux. Aunque actúa principalmente como MTA. Las misiones básicas de sendmail son las siguientes:

- Recogida de mails provenientes de un Mail Transport Agent (MTA)
- Elección de la estrategia de reparto de dos mails.
- Si el mail es local en el sistema, enviará el mails al programa de reparto local de mails.
- Si el mail no es local, sendmail utilizará el DNS del sistema para determinar el host al que se debe ser enviado el mail.

6.11.2 REQUERIMIENTOS



- Computador Linux
- Tarjeta de red
- Configuración IP Estática
- Paquete sendmail o Qmail
- Configurar tarjeta de red
- Levantar el puerto POP3 Y SMTP

6.11.3 CONFIGURACIÓN DE SENDMAIL

1.- Verificar si se tiene instalado el paquete de sendmail y dovecot.

root@localhost /] # rpm –q sendmail
root@localhost /] # rpm –q dovecot

rpm – q Verifica si esta instalados los paquetes

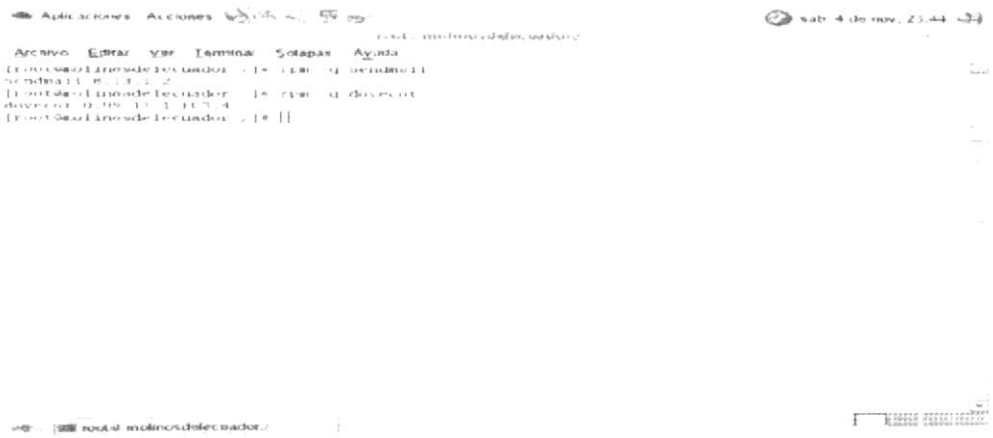


Figura 6-131: Verificar Paquetes Sendmail y Dovecot

2.- Ingresar al archivo **dovecot.conf**

root@localhost /] # cd /etc
root@localhost etc] # vi dovecot.conf

cd Ingresar a un directorio
vi Edita un archivo

- Descomentar la siguiente línea y agregar el fnal POP3.

#protocols = IMAP IMAPS POP3 (Permite levantar el puerto 110 para recibir correo electronico)

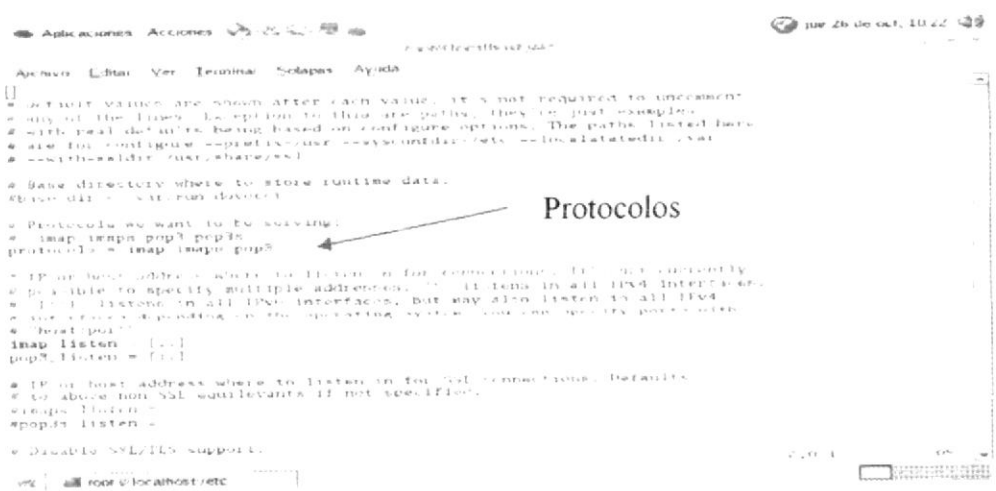


Figura 6-132: Configuración de los Protocolos

3.- Digitar el siguiente comando, y verificar si en el directorio se encuentra el archivo **sendmail.cf**.

root@localhost etc] # cd mail
root@localhost mail] # ls

cd	Ingresa a un directorio
ls	Lista contenido de un directorio



Figura 6-133: Listado de Archivos del Directorio Mail

4.- Ingresar al archivo del **sendmail.cf**

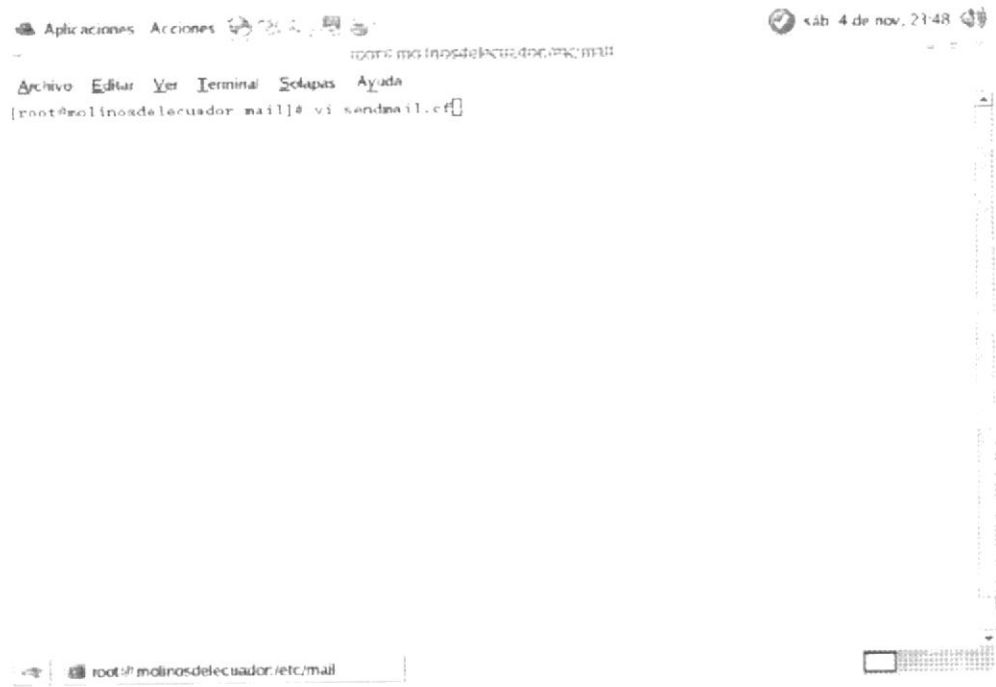


Figura 6-134: Ingreso alAarchivo Sendmail.cf

- Editar las siguientes líneas donde se edita el nombre del computador.

Cwlocalhost Cwmolinosdelecuador

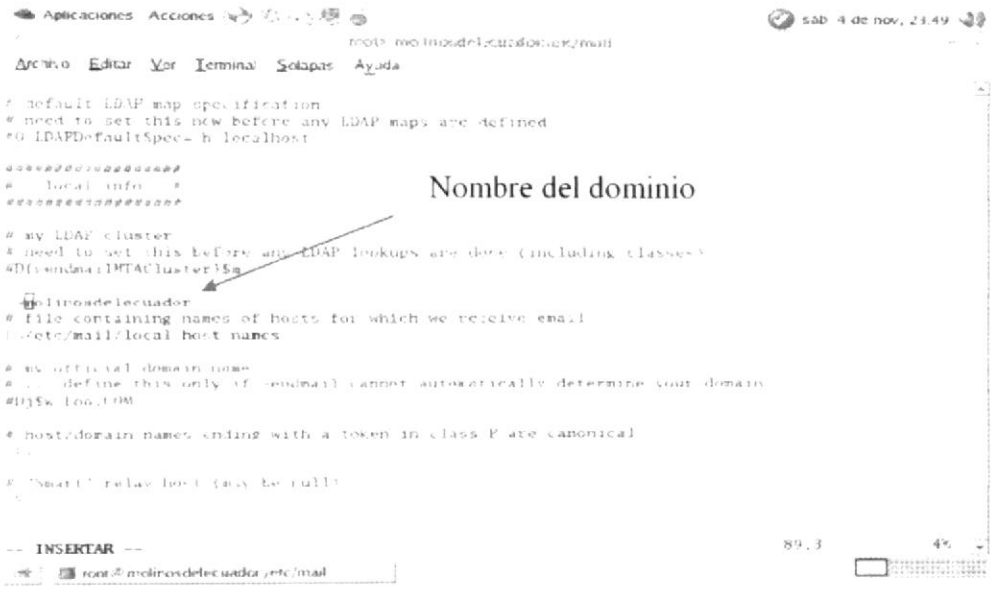


Figura 6-135: Setear el Nombre del Dominio

- Cambiar la dirección.

127.0.0.1 0.0.0.0

#SMTP daemon options
O DaemonPortOptions=Port=smtp, Addr=0.0.0.1, Name=MTA

Cualquier servidor pueda enviar el correo

SMTP client options
O ClientPortOptions=Family=inet, Addr=0.0.0.0

Cualquier cliente pueda enviar un correo

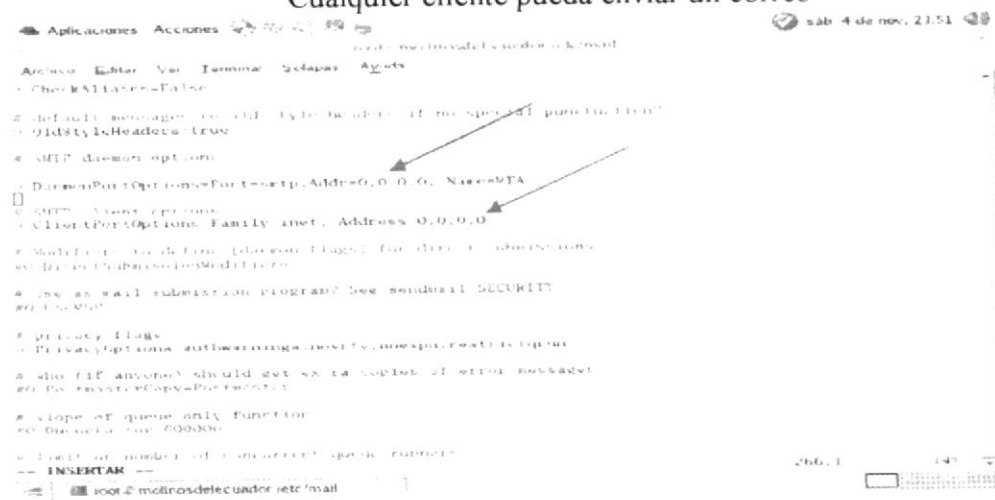


Figura 6-136:SMTP Daemon Options

5.- Luego proceder a iniciar los servicios del sendmail con el comando.

root@molinosdelecuador sysconfig] # service sendmail start.



Figura 6-137: Reiniciar los Servicios del Sendmail

6.- Luego verificar si los puertos 110 y 25 están habilitados.

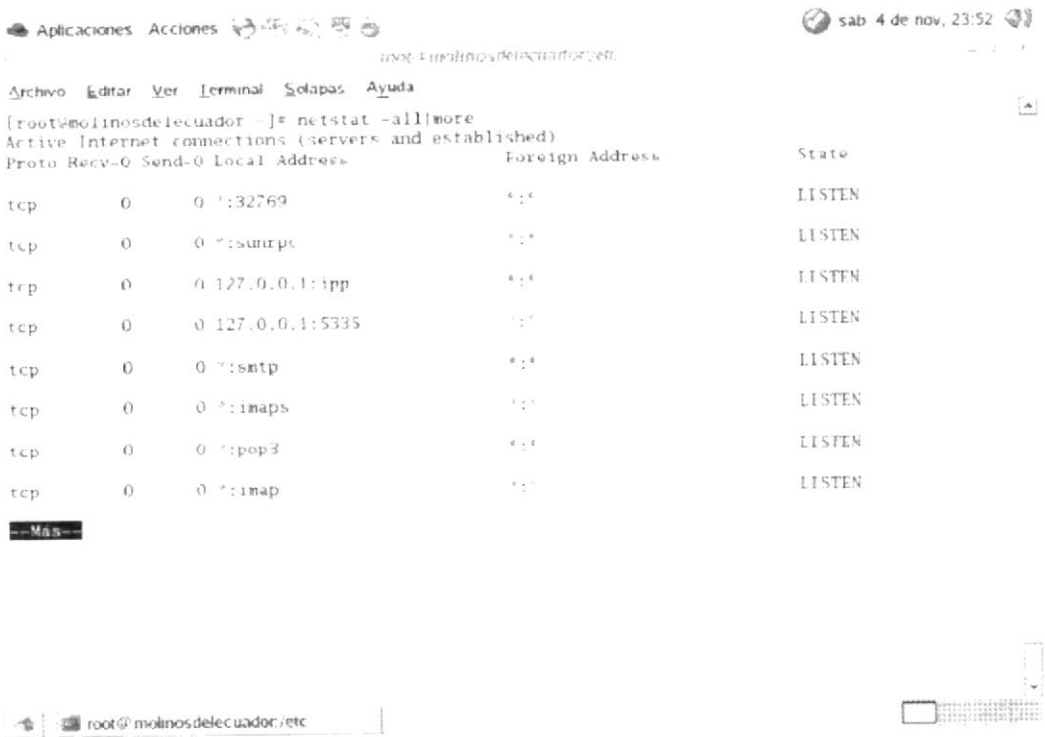


Figura 6-138: Verificar Puertos 110 y 25

7.- Ingresar al directorio de **etc** y editar el archivo del **hosts**.

root@localhost /] # cd /etc
root@localhost etc] # vi hosts

cd	Ingresa a un directorio
vi	Edita un archivo
hosts	Directorio

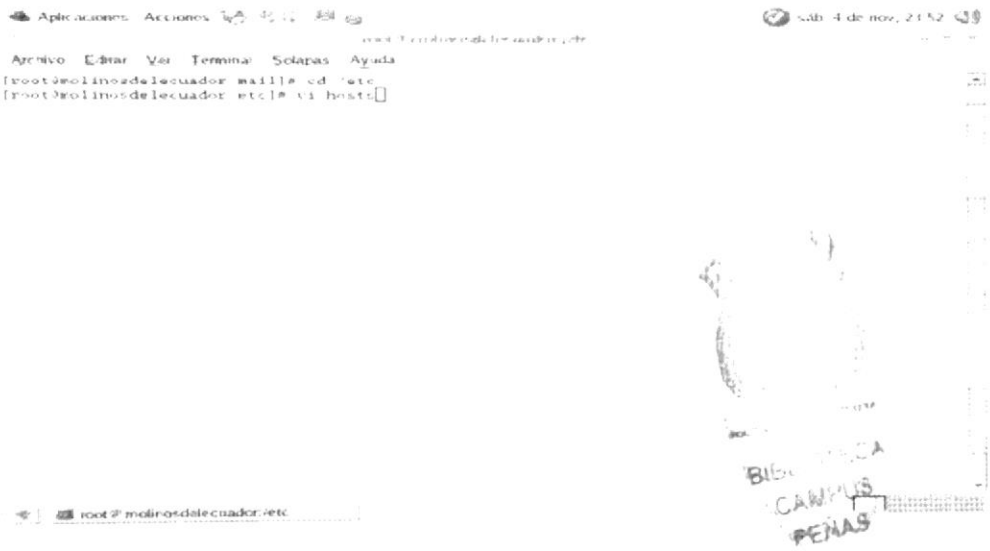


Figura 6-139: Ingreso al Archivo Hosts

- Aumentar estas dos líneas

127.0.0.1	molinosdelecuador.com	molinosdelecuador
192.168.12.1	molinosdelecuador.com	molinosdelecuador



Figura 6-140: Configuración del Archivo Hosts

8.- En la siguiente pantalla crear el usuario con su respectiva contraseña.

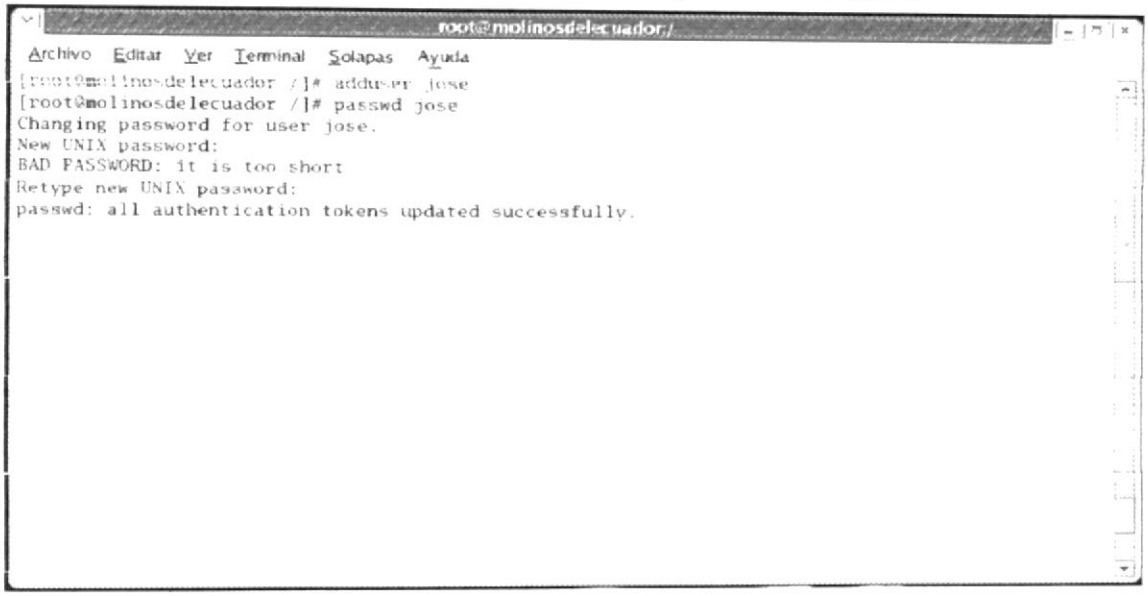


Figura 6-141: Creación de Usuario y Contraseña

9.- Levantar los siguientes servicios.

```
root@localhost /] # service dovecot restart
root@localhost /] # service sendmail restart
```



Figura 6-142: Restauración de los Servicios de Dovecot y Sendmail

10.- Una vez restaurados los servicios proceder a enviar un mensaje a un usuario en la red, como se muestra en la siguiente pantalla.

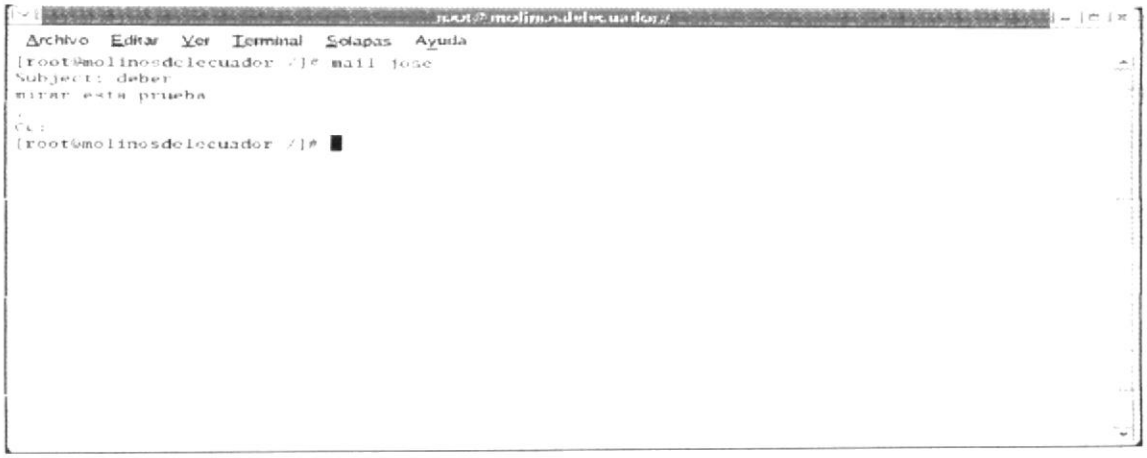


Figura 6-143: Envío de Mail

BIBLIOTECA
CAMPUS
PEÑAS

6.11.4 CONFIGURACIÓN EN CLIENTE WINDOWS - MAIL

1.- Como primer paso hacer clic en **Inicio, Programas, Outlook Express.**

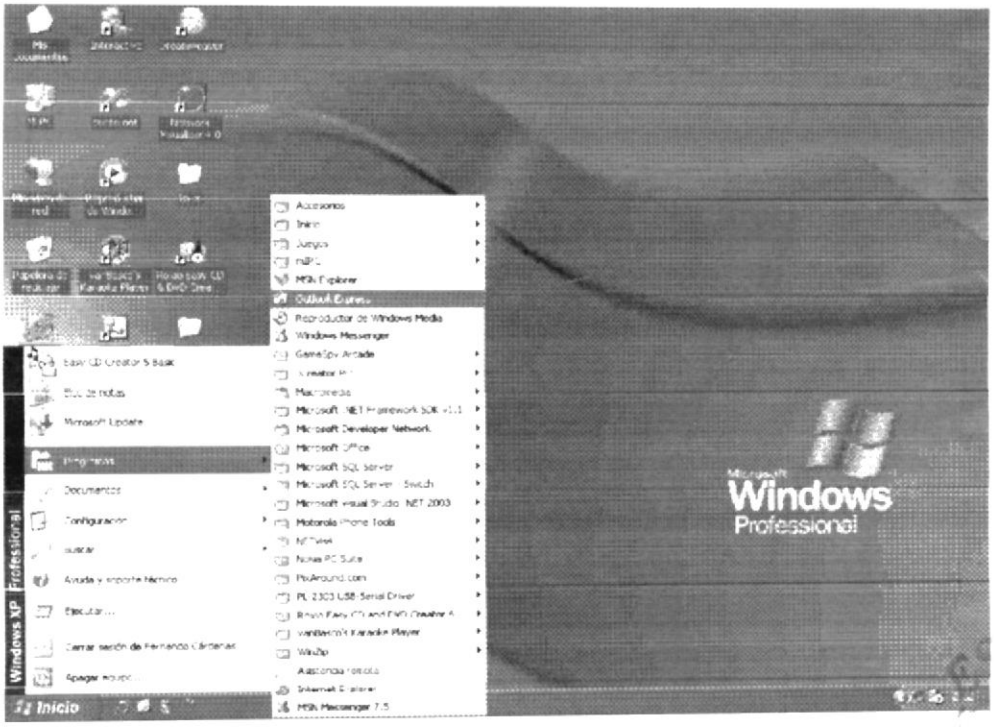


Figura 6-144: Selección de Outlook Express

2.- La siguiente pantalla muestra la página principal del **Outlook Express**.

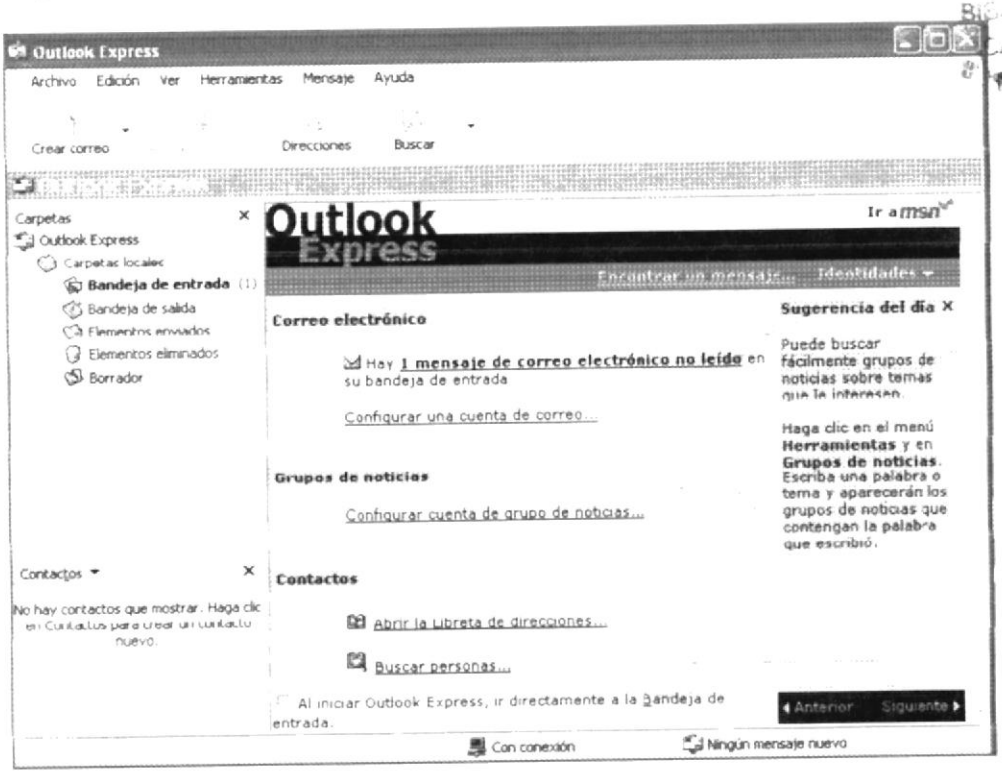


Figura 6-145: Página Principal del Outlook Express

3.- En el Outlook Express escoger la opción **Herramientas** y elegir **Cuentas**.

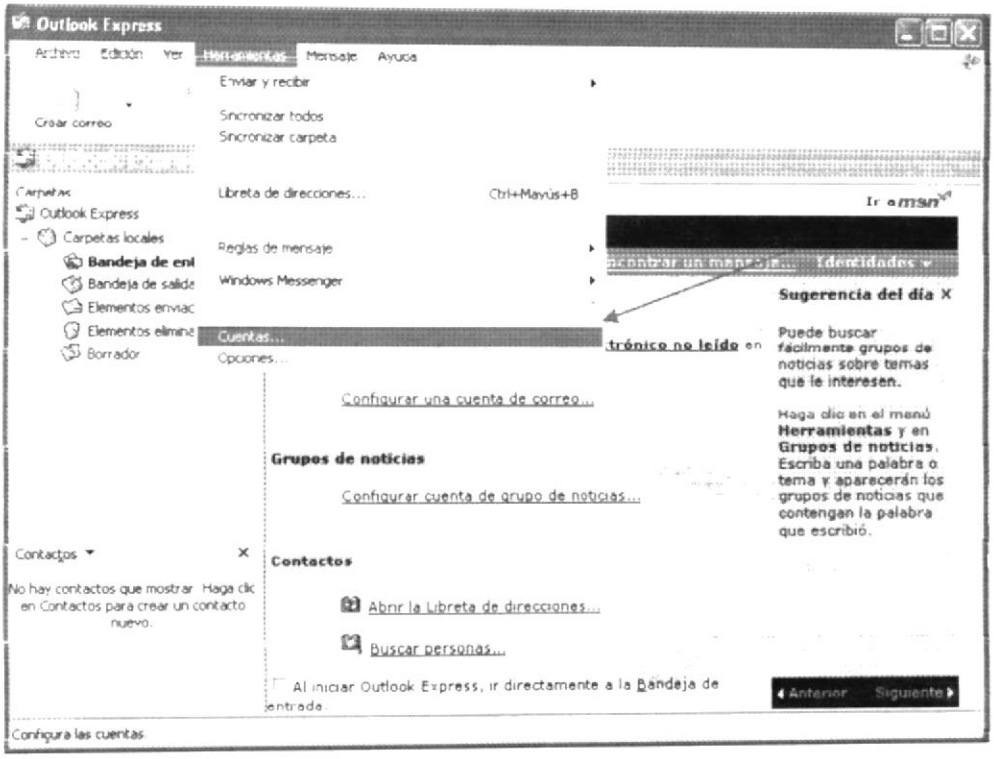


Figura 6-146: Configuración de Cuentas

4.- En esta pantalla elegir la opción **Agregar** y elegir **Correo**.

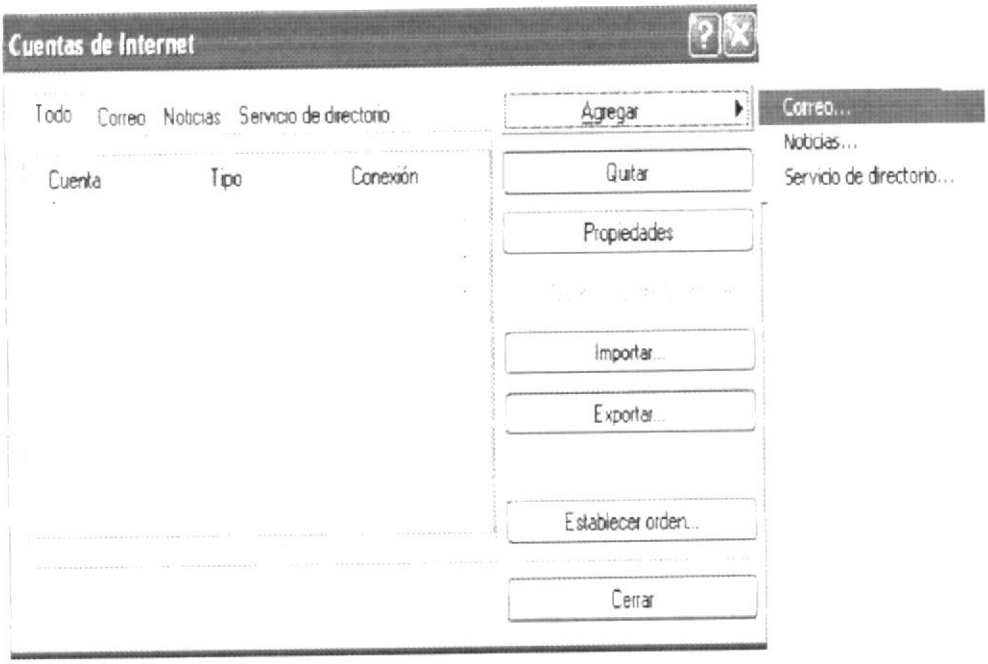


Figura 6-147: Cuentas de Internet

5.- En el siguiente cuadro ingresar nuestro nombre.

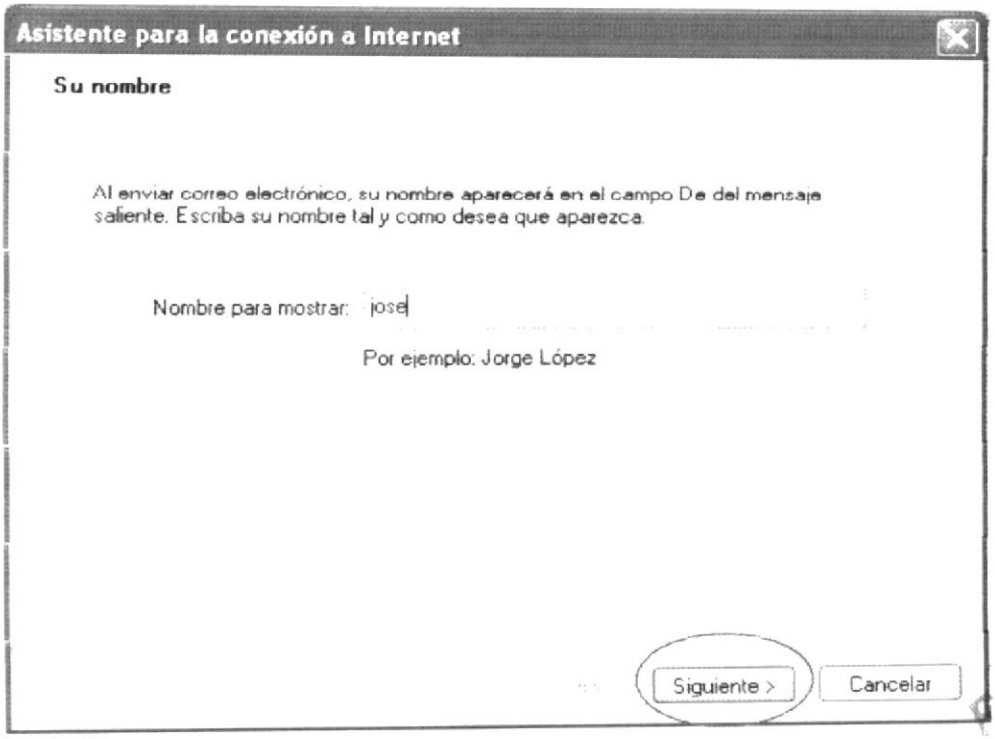


Figura 6-148: Asignación de Nombre de Ususario

6.- Ingresar nuestra dirección de correo electrónico como se muestra en la pantalla siguiente.

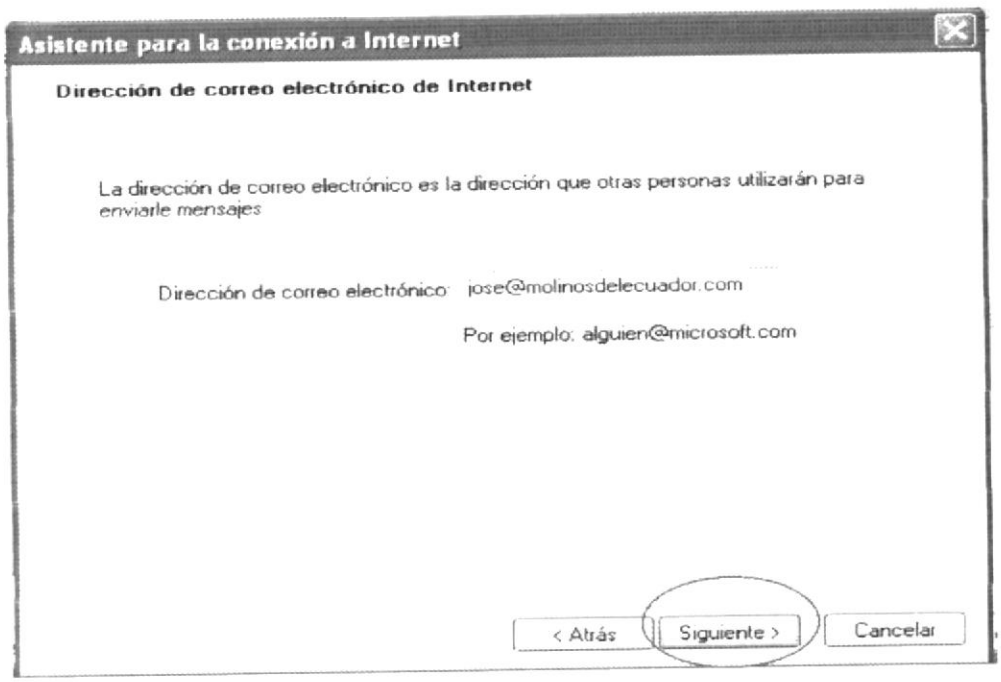


Figura 6-149: Dirección de Correo

7.- En esta pantalla especificar el servidor de correo entrante (POP3) y el servidor de correo saliente (SMTP), en este caso los dos son la misma dirección del servidor Linux, y hacer clic en **Siguiente**.

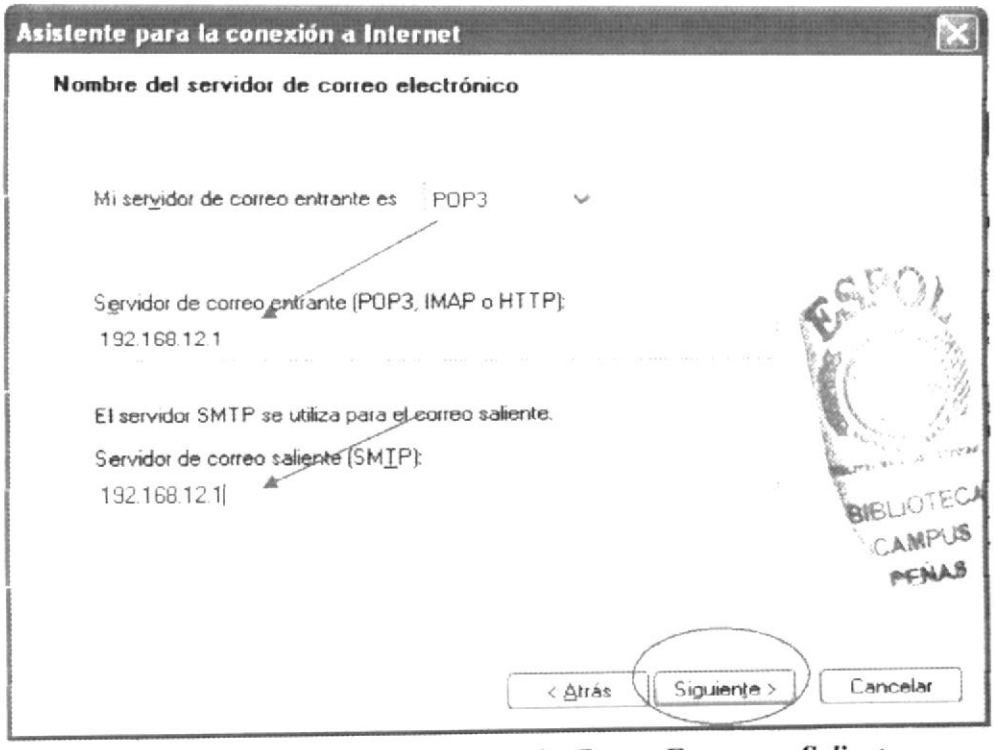


Figura 6-150: Especificar Servidor de Correo Entrante y Saliente

8.- En esta pantalla ingresar el nombre de usuario y la contraseña los mismos que fueron ya creados por el servidor de correo Linux, y hacer clic en **Siguiente**.

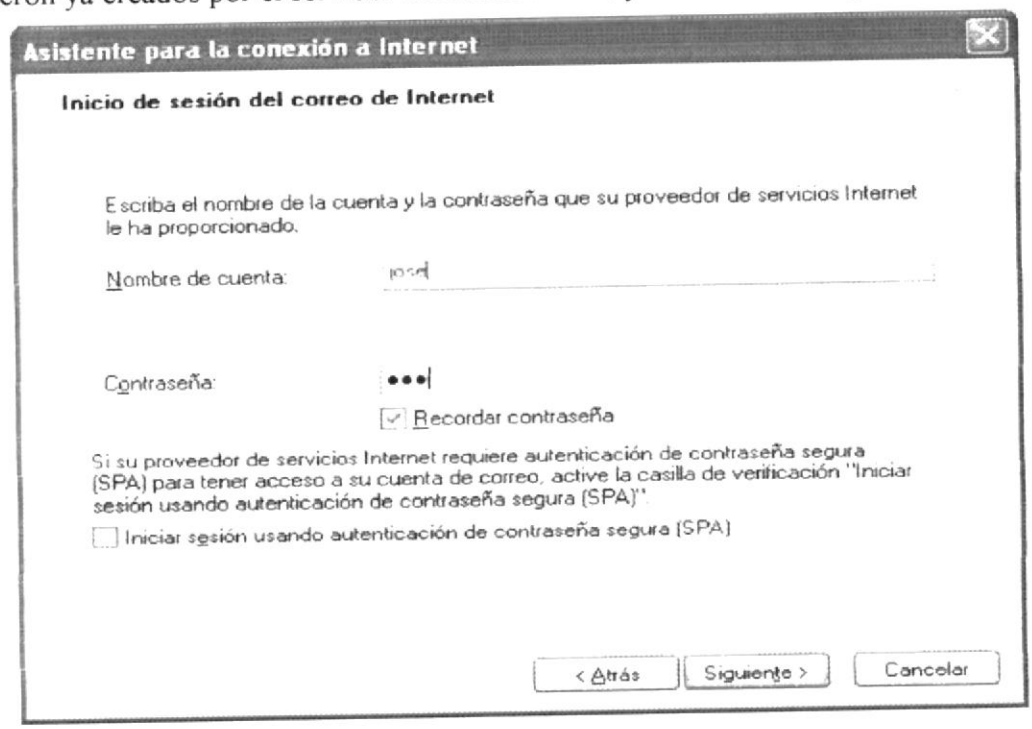


Figura 6-151: Ingreso de Nombre y Contraseña

9.- En esta pantalla el Asistente para la conexión a Internet pregunta si toda la información ingresada es correcta, de ser así hacer clic en el botón **Finalizar**.

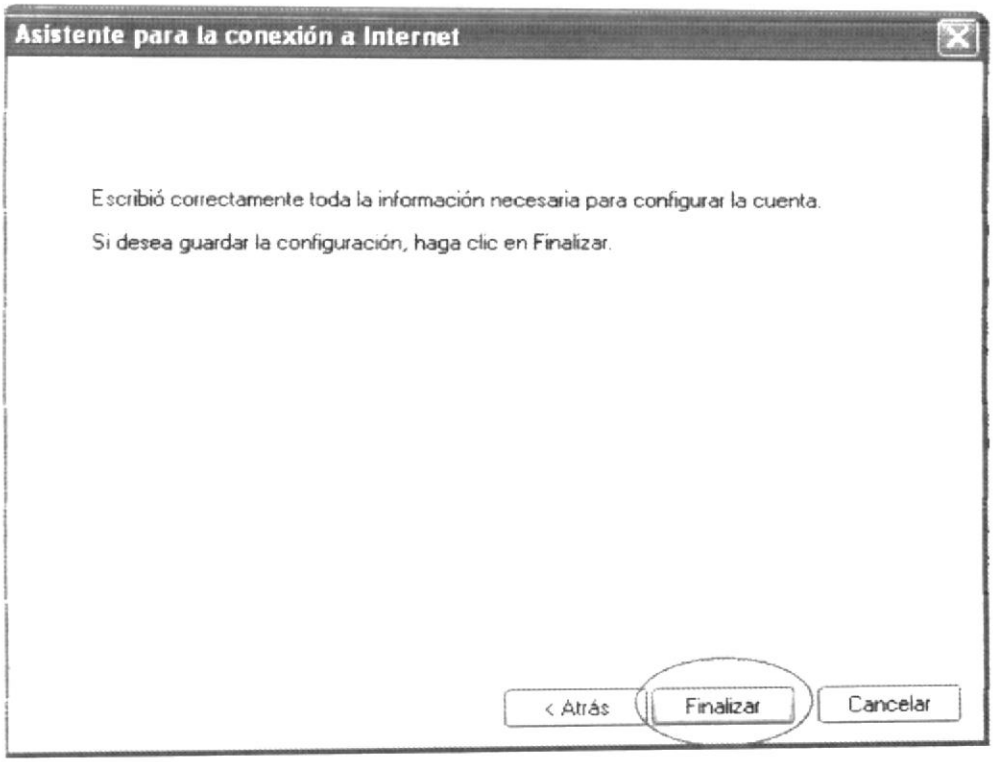


Figura 6-152: Finalizar Cambios del Asistente

10.- Como se muestra ya se tiene configurado el **Outlook Express**.

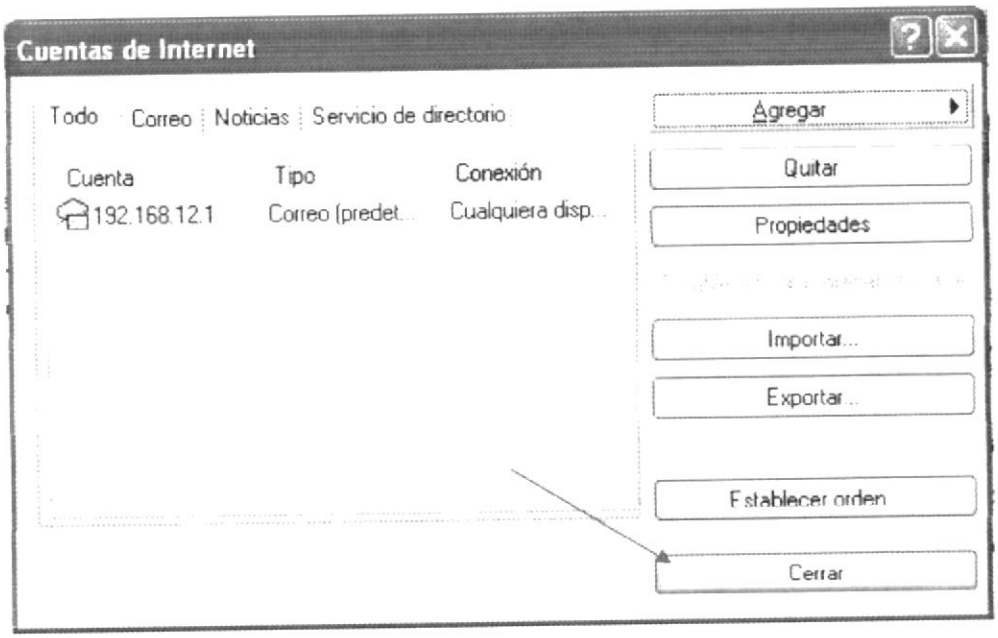


Figura 6-153: Finalización del Asistente

11.- Verificar en la bandeja de entrada el mensaje que se digitó por parte del servidor.

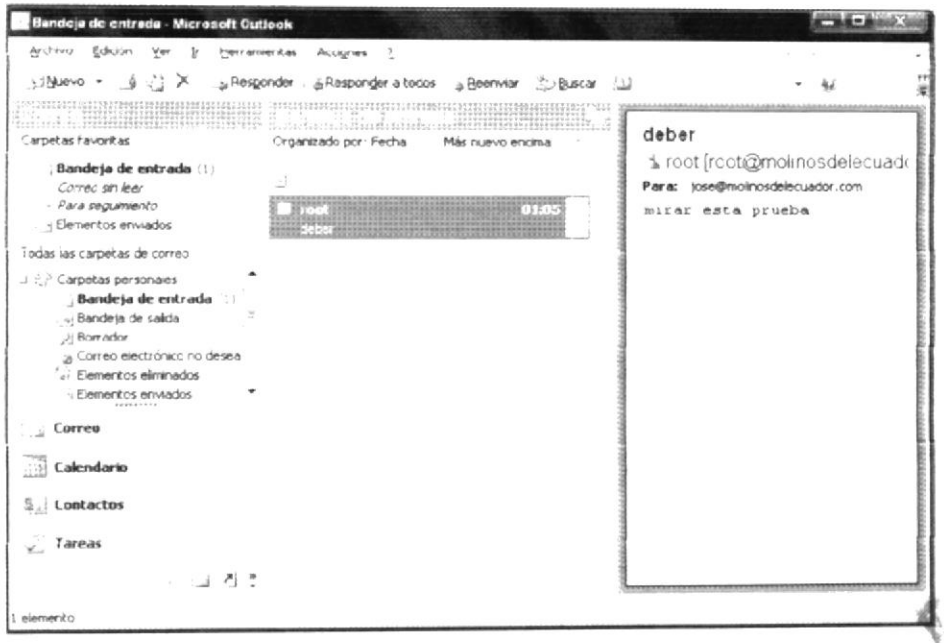


Figura 6-154: Bandeja de Entrada de OUTLOOK

Lectura de la información recibida del servidor de correo.

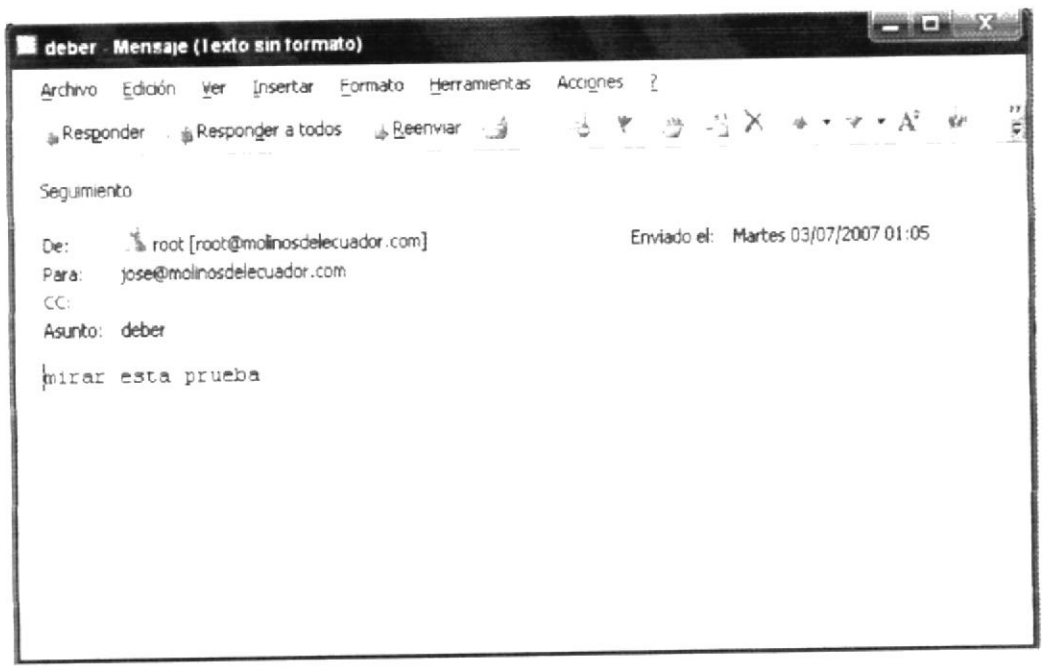


Figura 6-155: Ingreso al Mensaje

12.- En las siguientes pantallas se muestra el envío del mensaje.

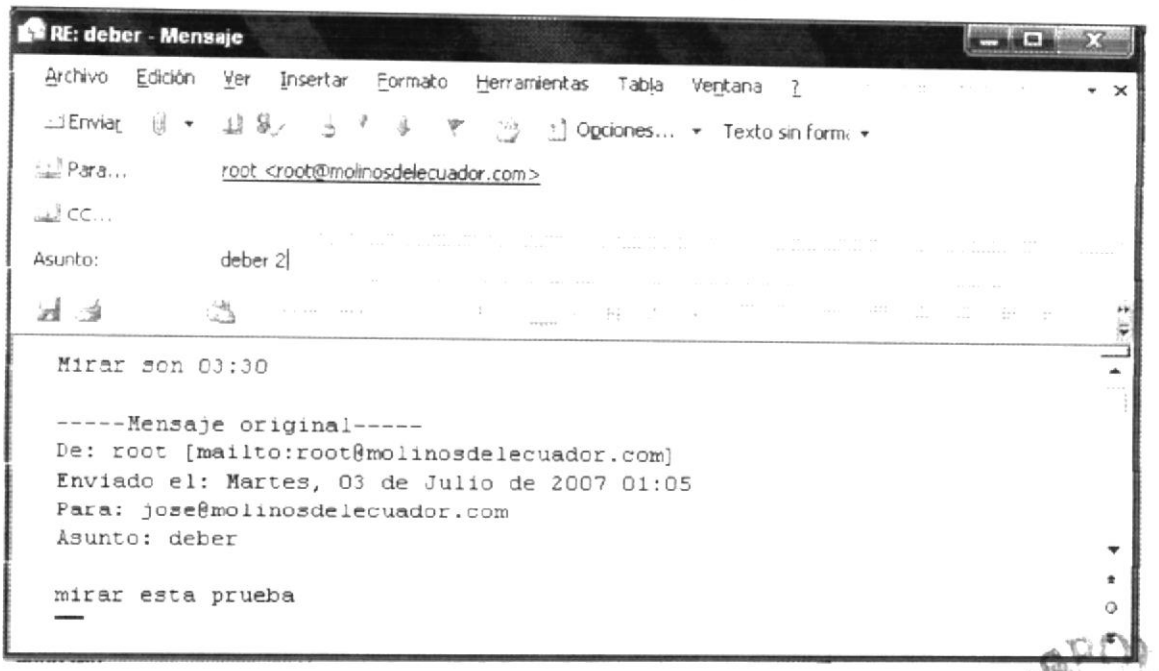


Figura 6-156: Respuesta al Mensaje

13.- Como se aprecia en la bandeja de salida el mensaje de respuesta por parte del cliente hacia el servidor.

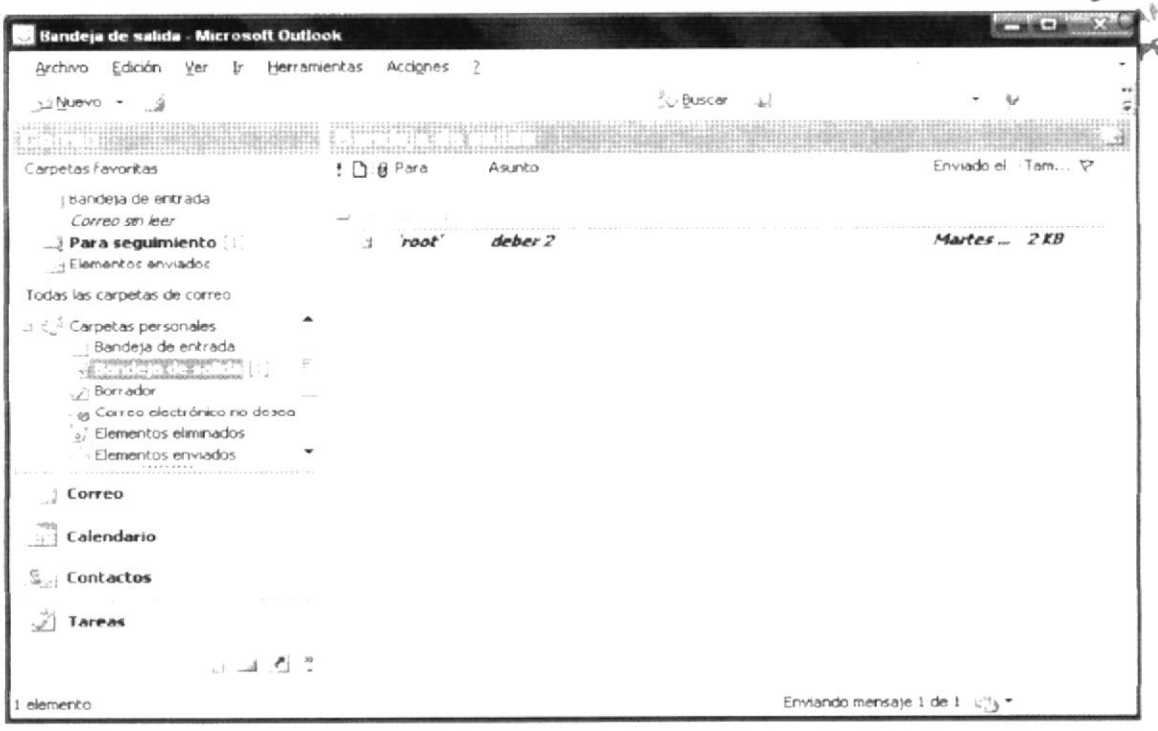


Figura 6-157: Envío de Mensajes

14.- Para revisar si el correo llegó al servidor Linux, iniciar sesión con el usuario root y luego digitar el comando **mail**.

[root@molinosdelecuador /]# mail

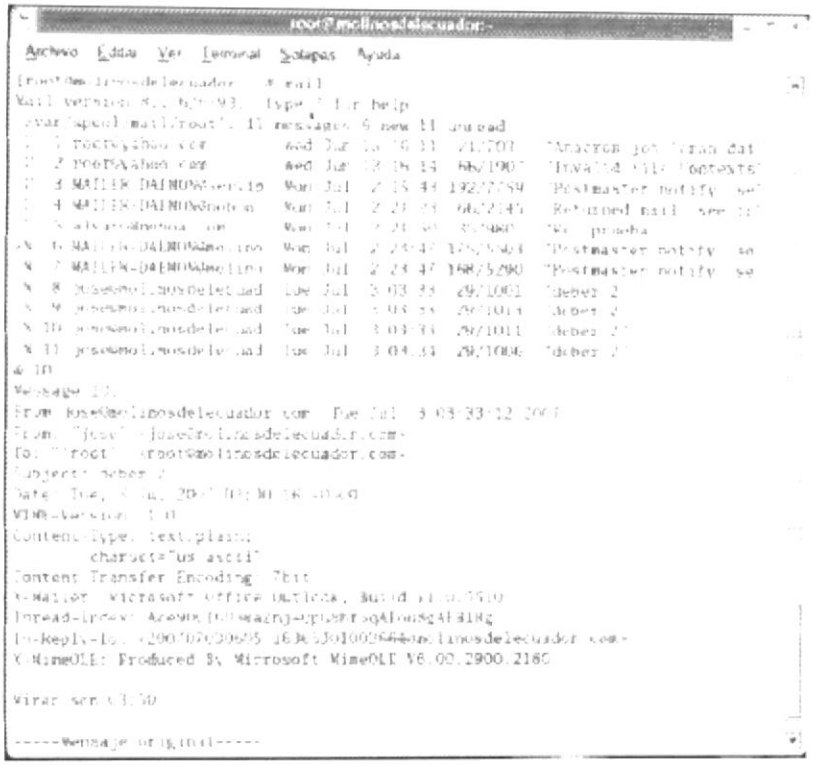


Figura 6-158: Revisión del Mensaje en Servidor

ESPOL
BIBLIOTECA
CAMPUS
PENAS

6.12 SERVIDOR PROXY

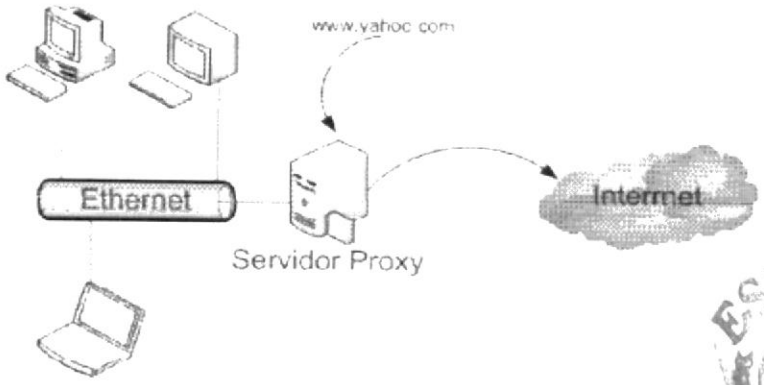


Figura 6-159: Servidor Proxy

ESPOL
BIBLIOTECA
CAMPUS

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

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

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

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

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

Cuando se recibe una petición para un recurso de Red especificado en un URL (Uniform Resource Locator) el Servidor Intermediario busca el resultado del URL dentro del caché. Si éste es encontrado, el Servidor Intermediario responde al cliente proporcionado inmediatamente el contenido solicitado.

Si el contenido solicitado no estuviera disponible en el caché, el Servidor Intermediario lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de respuestas a solicitudes (hits) (ejemplos: LRU, LFUDA y GDSF).

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

6.12.1 VENTAJAS

- Una ventaja importante del Proxy Server es que la memoria caché trabaja para todos los usuarios en conjunto, esto hace que las paginas que visita un usuario queden en caché para otros usuarios en caso en que otros usuarios decidan visitar la misma pagina.

- El Proxy Server también permite control administrativo de la conexión a internet, permite que los usuarios de la red interna tengan acceso solo a los servicios que se les definan.

- Descentralización del acceso a Internet.

- Configuraciones de seguridad

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

6.12.2 DESVENTAJAS

En general (no sólo en informática), el uso de un intermediario puede provocar:

- Abuso. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
- Carga. Un proxy ha de hacer el trabajo de muchos usuarios.
- Intromisión. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
- Incoherencia. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.
- Irregularidad. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

6.12.3 FUNCIONAMIENTO

Un Proxy Server trabaja de la siguiente manera:

- El Proxy Server recibe una solicitud de un usuario para un servicio de Internet.
- Si la solicitud pasa el proceso de filtrado, el Proxy Server busca el caché local las páginas previamente descargadas, si encuentra el documento y este es valido lo envía al usuario directamente sin tener que pasar la solicitud por el canal de Internet.
- Si la pagina no esta en el caché de Proxy Server se encargará de descargarlas de Internet por medio del canal de acceso externo y lo envía al usuario que la solicito una vez que obtenga.

6.12.4 REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR DE INTERNET

- Una computadora con Linux Fedora Core 3 instalado.
- Tarjeta de red.
- Configuración IP Estática, pública y privada.
- Paquete de squid



6.12.5 CONFIGURACIÓN DE PROXY SERVER

1.- Comprobar si esta instalado el paquete squid con el comando siguiente.

root@molinosdelecuador /] # rpm –q squid

rpm –q Verifica si están instalados los paquetes

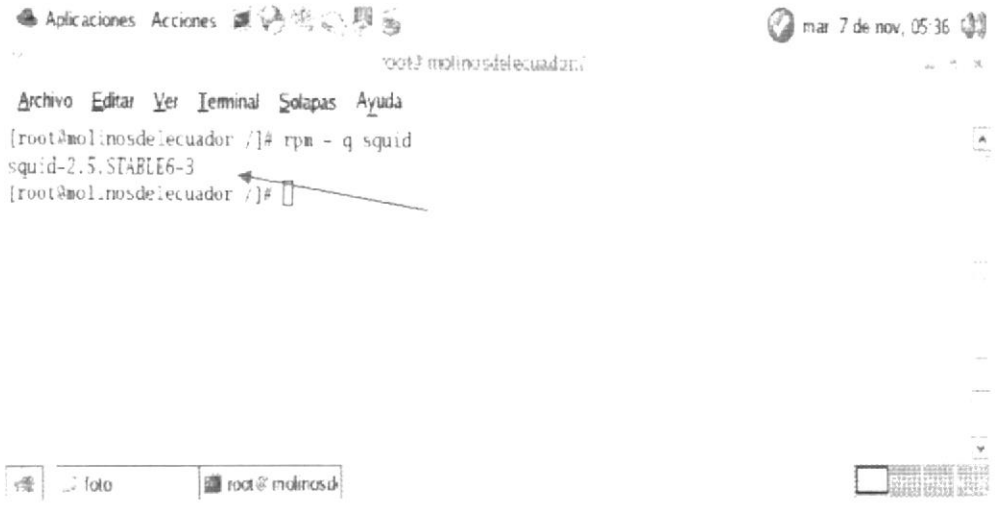


Figura 6-160: Verificación del Paquete Squid

2.- Ingresar al directorio **squid**.

root@molinosdelecuador /] # cd /etc/squid

cd Ingreso a directorios

/etc/squid Directorios



Figura 6-161: Ingreso Al directorio del Squid

3.- Editar el archivo **squid.conf**

root@molinosdelecuador squid] # vi squid.conf

vi Editar archivos



Figura 6-162: Ingreso al Archivo Squid.Conf

Proceder a realizar los siguientes cambios en las siguientes secciones:

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.

En el caso de un *Proxy Transparente*, regularmente se utilizará el puerto 80 y se valdrá del re-direccionamiento de peticiones de modo tal que no habrá necesidad alguna de modificar la configuración de los navegadores Web para utilizar el servidor Proxy. Bastará con utilizar como puerta de enlace al servidor.

Regularmente algunos programas utilizados comúnmente por los usuarios suelen traer por defecto el puerto 8080 -servicio *de cacheo WWW*- para utilizarse al configurar que servidor proxy utilizar. Si se quiere aprovechar esto en nuestro favor y ahorrarnos el tener que dar explicaciones innecesarias al usuario, se puede especificar que Squid escuche peticiones en dicho puerto también. Siendo así localice la sección de definición de http_port, y especifique:

- El parámetro http_port 3128 es el puerto por defecto y se lo utiliza para atender peticiones
- Proxy transparente utiliza el puerto 80 y redirecciona peticiones.
- Proxy convencional suele traer por defecto el puerto 8080

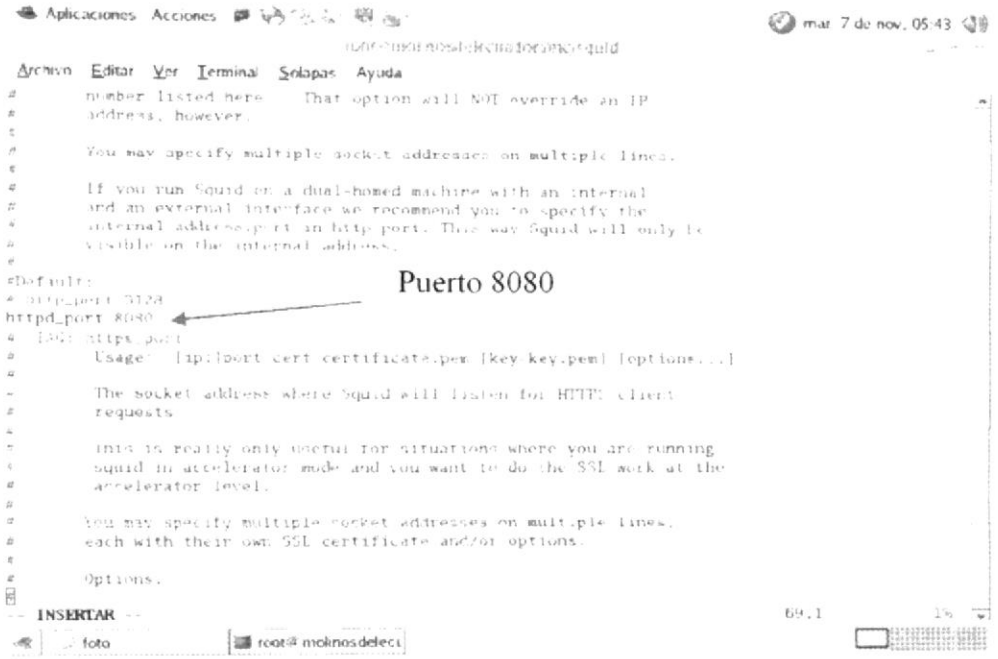


Figura 6-163: Seteo del Puerto 8080

- Cache_men 8 MB cambiar a cache_men 16 MB. El parámetro cache_men 16 MB establece la cantidad de memoria para los objetos en transito.



Figura 6-164: Seteo de Cache_Mem

- El parámetro cache_dir, debido a que entre más extensa la cache del disco mas objetos almacena este, y por lo tanto utilizará menos ancho de banda será por defecto 100MB.
  Descomentar **cache_dir**.



Figura 6-165: Seteo de Cache_Dir

- Descomentar **cache_access_log.** Sirve para monitorear la actividad de los host



Figura 6-166: Configuración Cache_Access_Log

4.- Configurar las listas de control de acceso.

acl puerto myport 8080 (definir el puerto a utilizar para nuestro Proxy).
acl red src 192.168.12.0/255.255.255.0(definir el segmento de red).

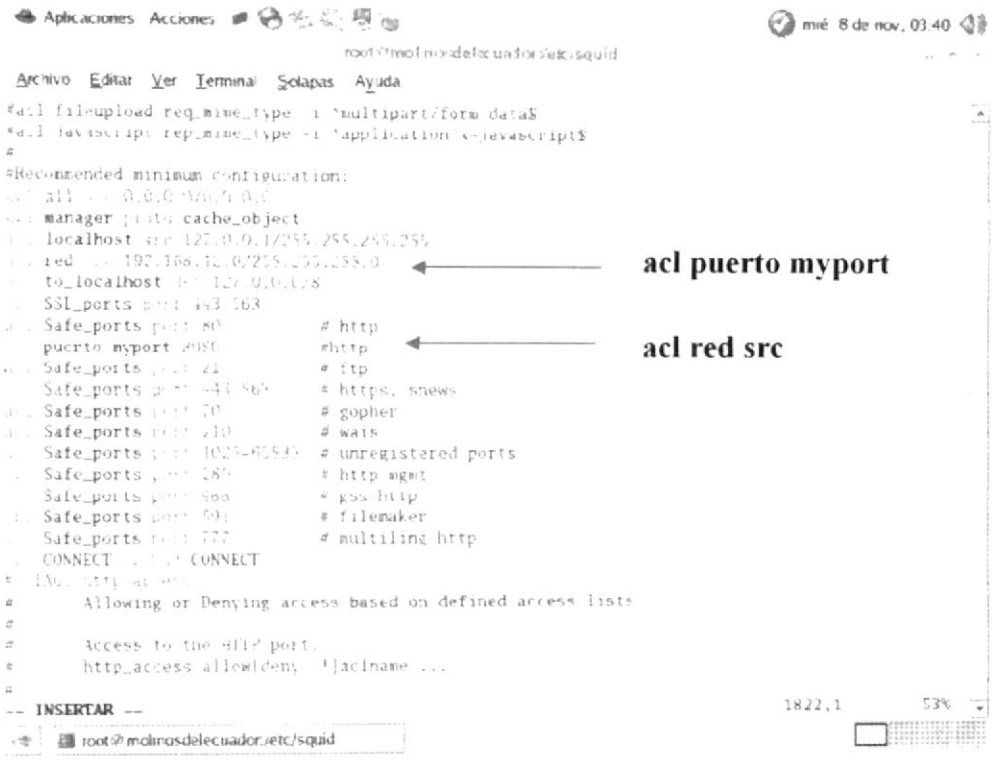


Figura 6-167: Control de Acceso

5.- Incluir las listas de control de acceso, la cual permitirá configurar el Proxy.

http_access allow red web



Figura 6-168: Aplicando reglas deLlista de Acceso

6.- Reiniciar los servicios del **squid.**

[root@molinosdelecuador /] # service squid start

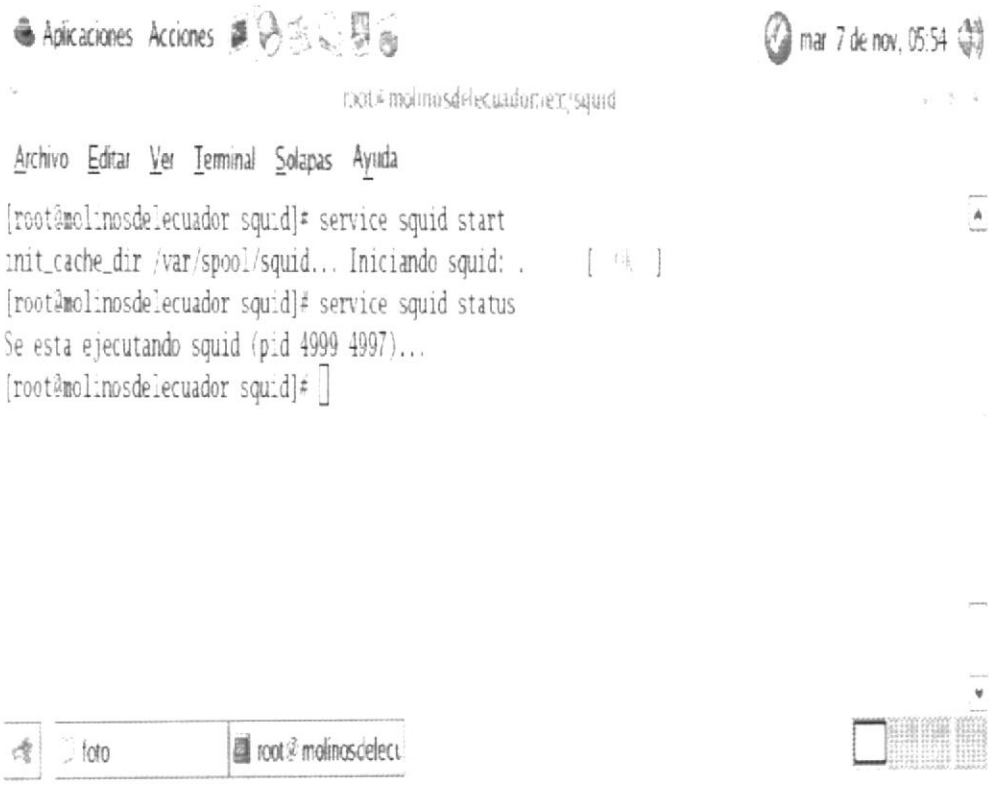


Figura 6-169: Iniciar Servicios del Squid

BIBLIOTECA CAMPUS PEÑAS

6.12.5.1 CONFIGURACIÓN EN CLIENTE WINDOWS - PROXY

1.- Ingresar al **Internet explorer**, escoger la opción **Herramientas** y elegir la **Opción De Internet.**

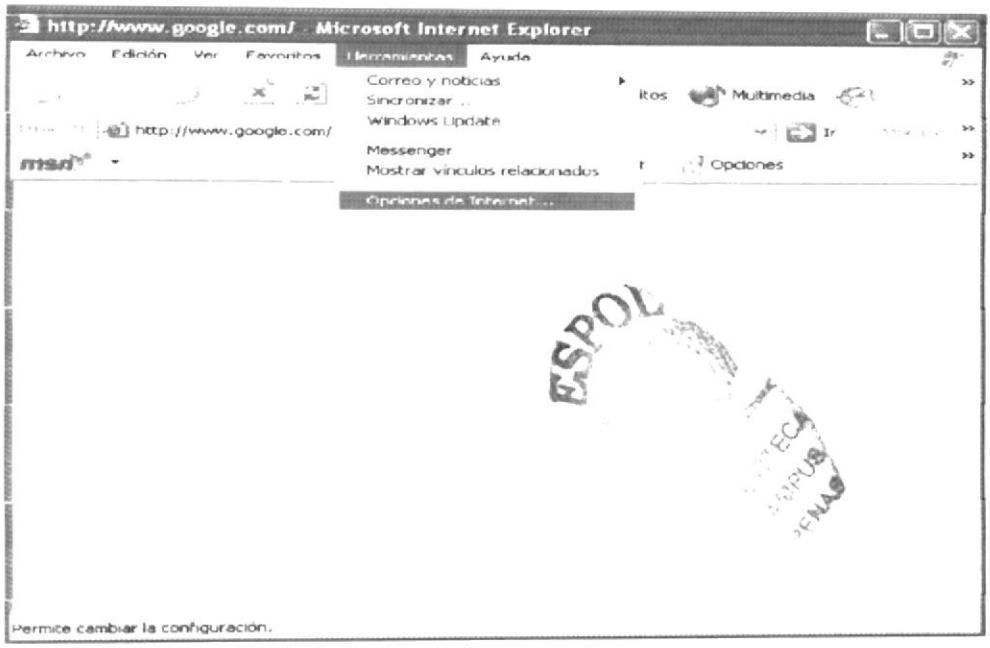


Figura 6-170: Opciones de Internet

2.- Hacer clic en **Configuración de Lan.**

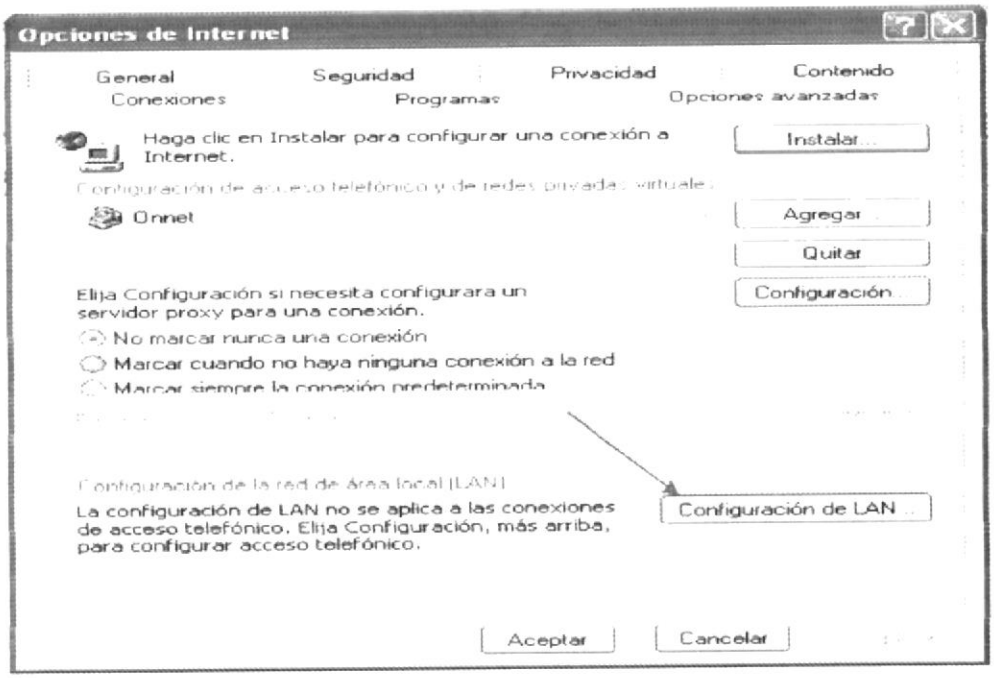


Figura 6-171: Configuraciones Lan

3.- Seleccionar la opcion **Servidor Proxy**.

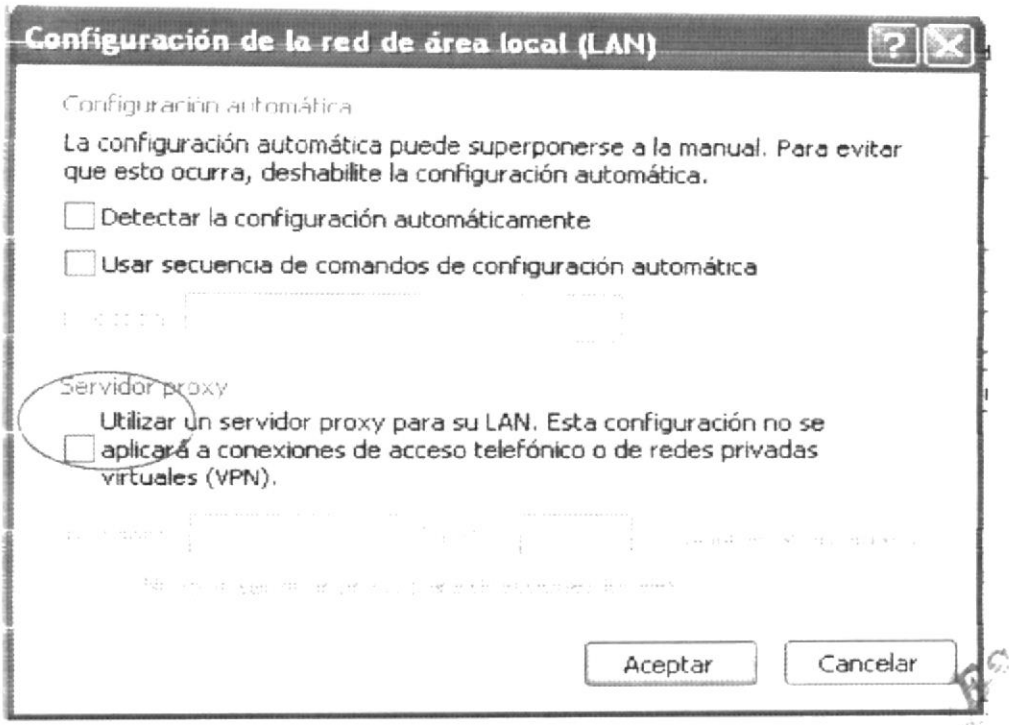


Figura 6-172: Configuración de la Red de Área Local (Lan)

En el cuadro de direccion digitar la IP del servidor, el puerto 8080 y hacer clic en **Aceptar**.

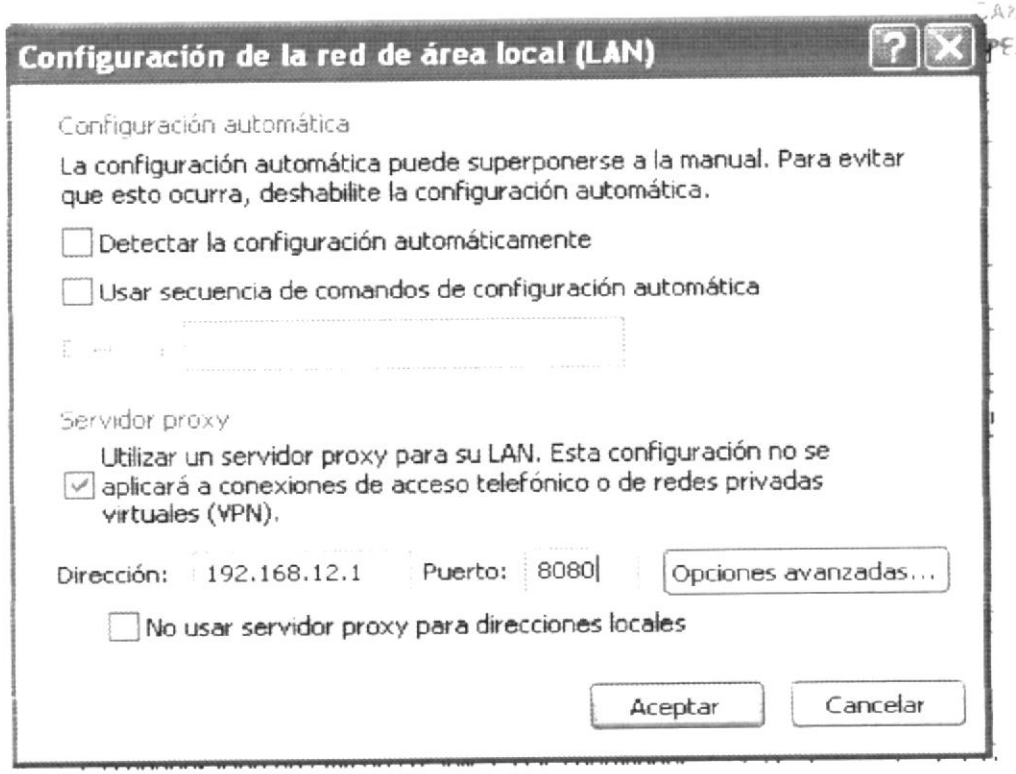


Figura 6-173: Configuración la Sección Servidor Proxy

4.- A continuación proceder a cargar el Internet Explorer y digitar una dirección Web para este caso será www.molinosdelecuador.com

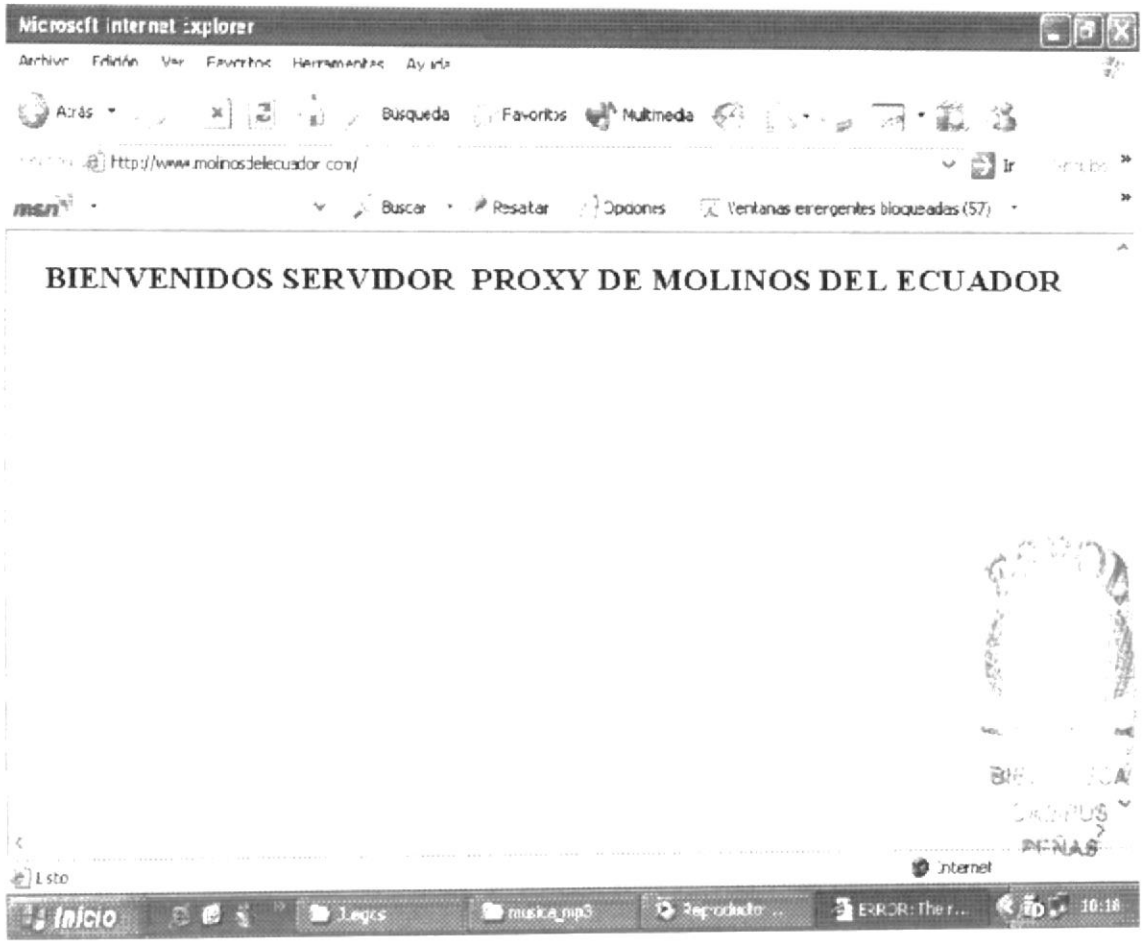


Figura 6-174: Página Habilitada de Molinos

6.12.6 RESTRICCIONES DE ACCESO A PÁGINAS ESPECÍFICAS.

Realizar los tres primeros pasos que se explico en la anterior configuracion.

1.- Configurar las listas de control de acceso.

Acl porno src "etc/squid/xxx"

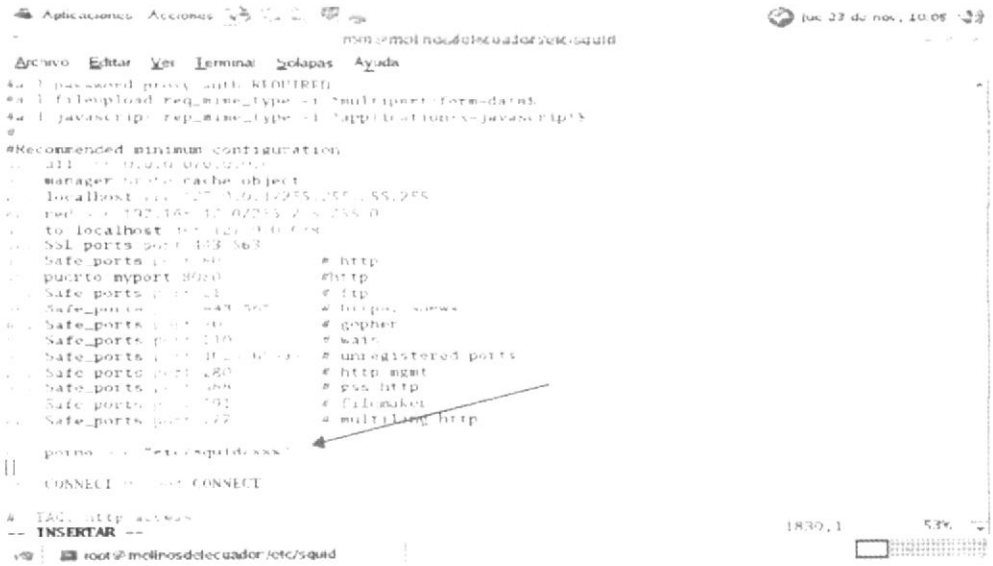


Figura 6-175:Restricciones de Página

2.- Incluir las listas de control de acceso donde se digita las políticas de no acceso a paginas en el internet.

http_access deny redpuerto porno

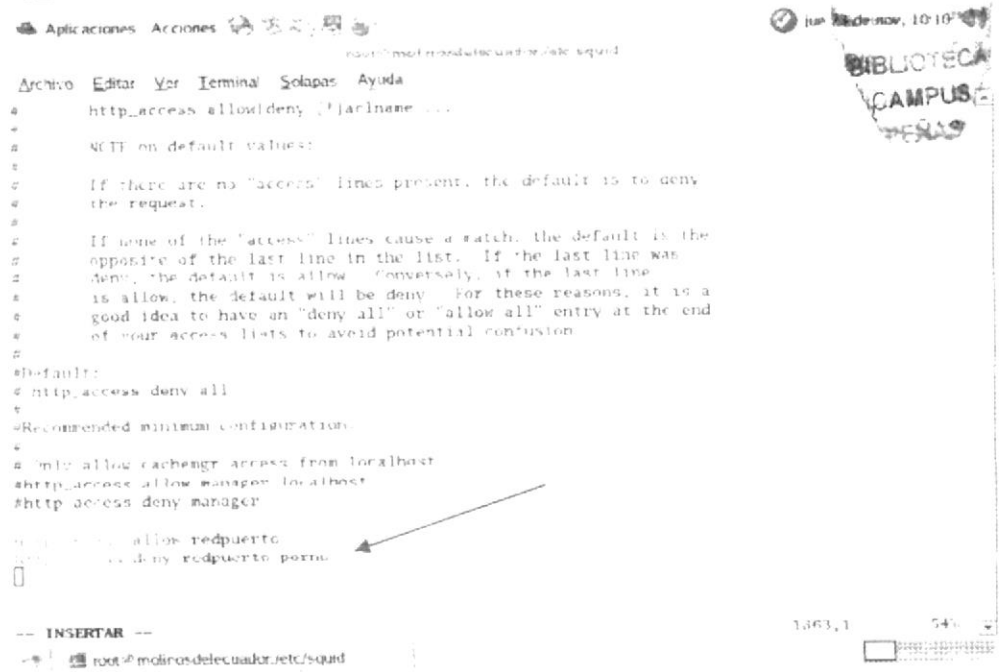


Figura 6-176: Negación de Dirección

3.- Reiniciar los servicios.

[root@molinosdelecuador /] # service squid start



Figura 6-177: Inicio del Servicio Squid

BIBLIOTECA
CAMPUS
PEÑAS

6.12.6.1 CONFIGURACIÓN EN CLIENTE WINDOWS RESTRICCIONES DE PÁGINAS ESPECÍFICAS

1.- Para comprobar los cambios hechos en el servidor hacer doble clic en el icono del **Internet Explorer**.

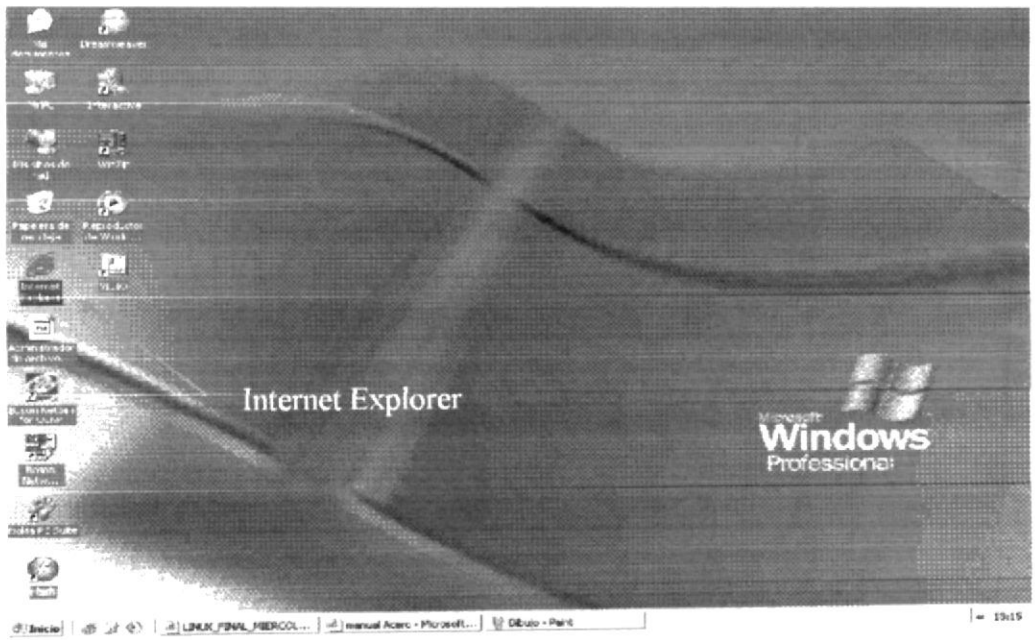


Figura 6-178: Entorno de Windows

2.- Luego debe mostrar algo parecido a esta pantalla. Esto indica que la restricción por horario en el servidor Proxy esta activa.

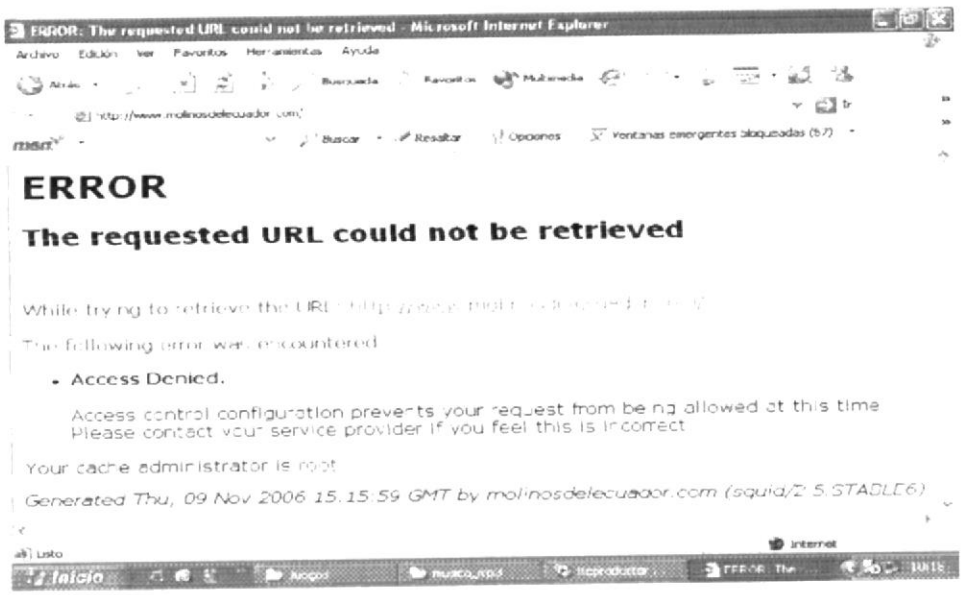


Figura 6-179: Página Bloqueada

6.12.7 RESTRICCIONES A USUARIOS EL ACCESO A INTERNET

1.- Ingresar al archivo **squid.conf** para hacer las respectivas modificaciones.



Figura 6-180: Ingreso al Archivo Squid.conf

2.- Configurar las listas de control de acceso donde se ingresa la ruta o dirección donde se quiere alojar las direcciones IP de los usuarios que va a restringir el uso del internet.

acl negar src "etc/squid/personas"

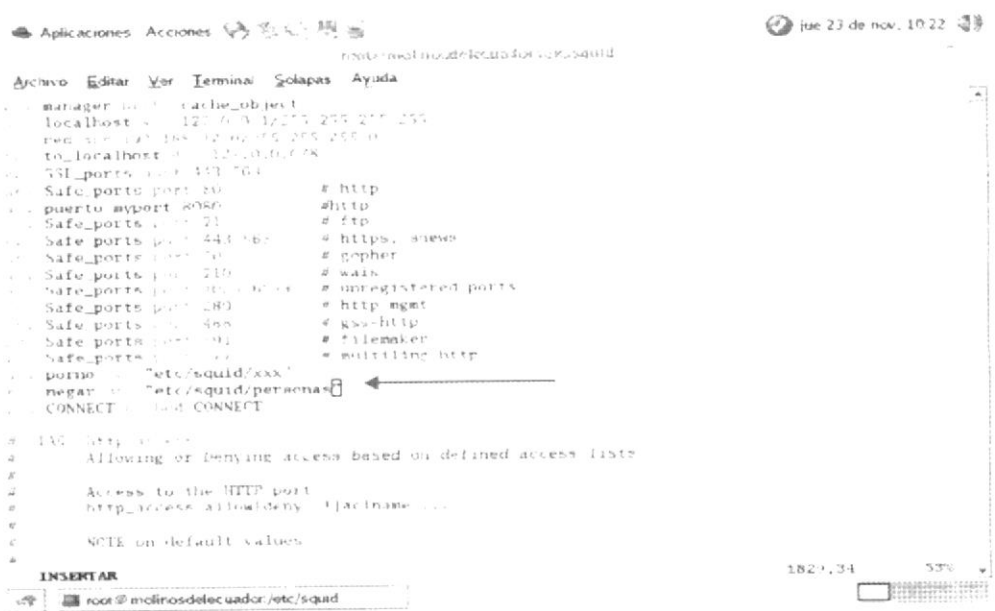


Figura 6-181: Restricción a Usuarios

BIBLIOTECA CAMPUS PEÑAS

3.- Incluir las listas de control de acceso donde se negará el acceso a intenet a ciertos usuarios.

http_access deny redpuerto negar

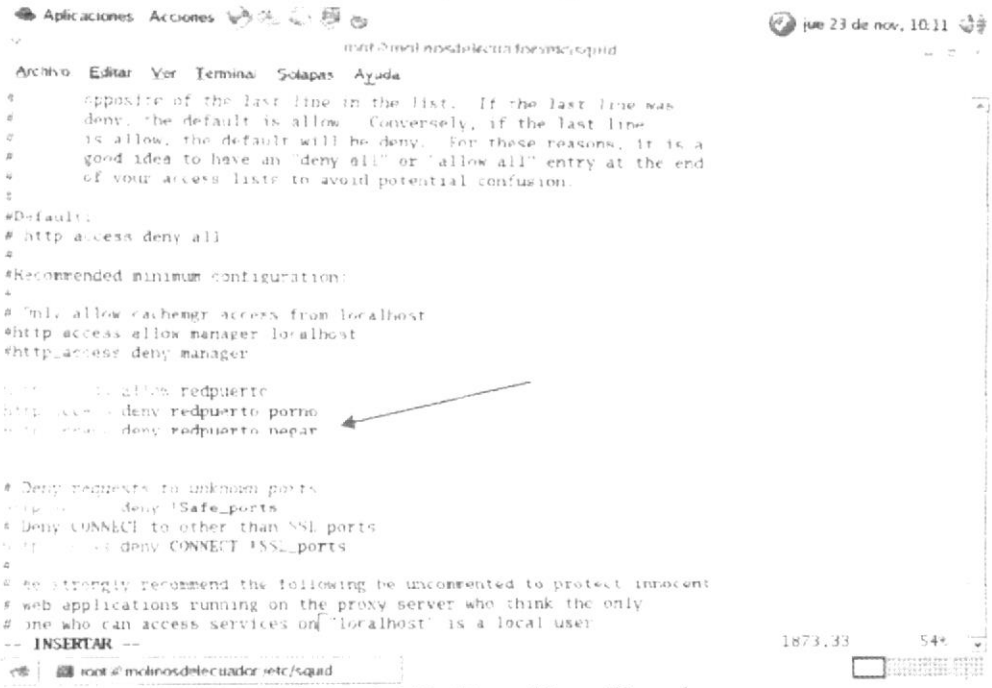


Figura 6-182: Negación a Usuarios

4.- Crear el archivo personas.

[root@molinosdelecuador /] # vi personas



Figura 6-183: Creación de Archivo Contenedora de Usuarios

5.- Digitar la IP de las computadoras de los usuarios que no le permitirá navegar en Internet.



Figura 6-184: Ip a Negar

6.- Reiniciar los servicios.

[root@molinosdelecuador /] # service squid start

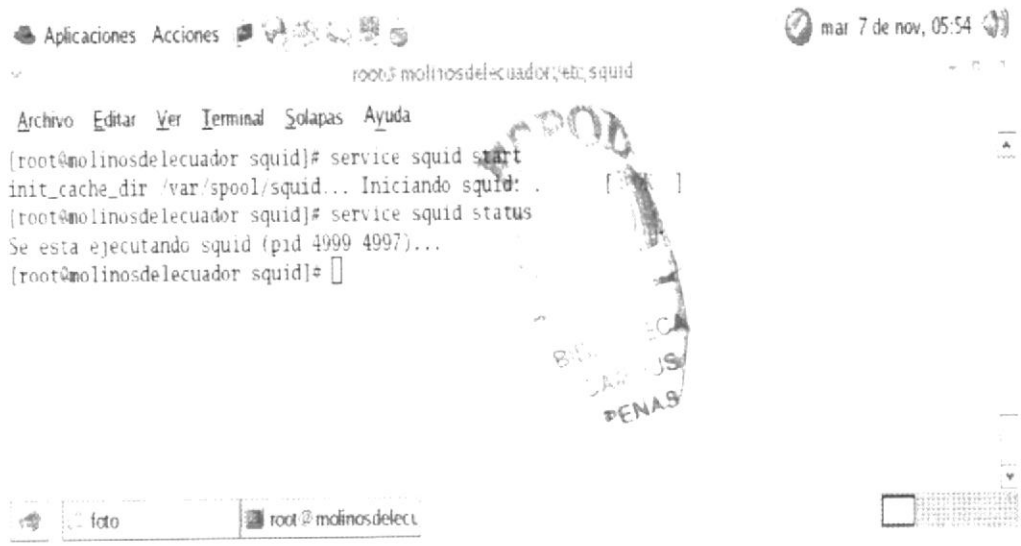


Figura 6-185: Inicio del Servicio Squid

6.12.7.1 CONFIGURACIÓN EN CLIENTE WINDOWS RESTRICCIONES A USUARIOS EL ACCESO A INTERNET

1.- Para comprobar los cambios hechos en el servidor hacer doble clic en el icono del **Internet Explorer.**

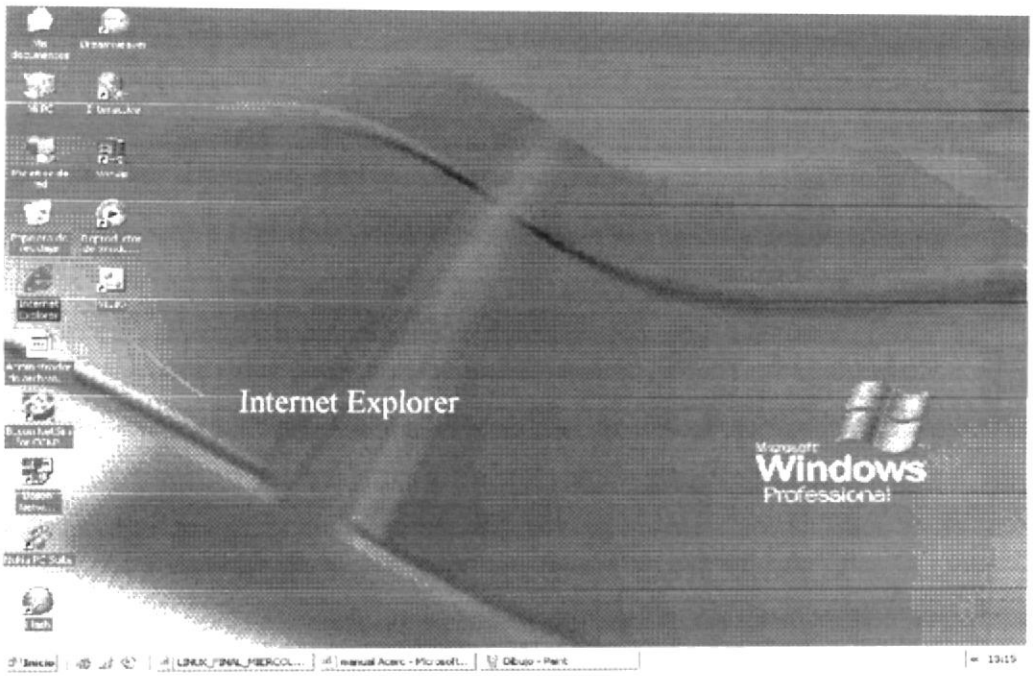


Figura 6-186: Entorno de Windows

2.- Luego debe mostrar algo parecido a esta pantalla. Esto indica que la restricción por horario en el servidor Proxy esta activa.

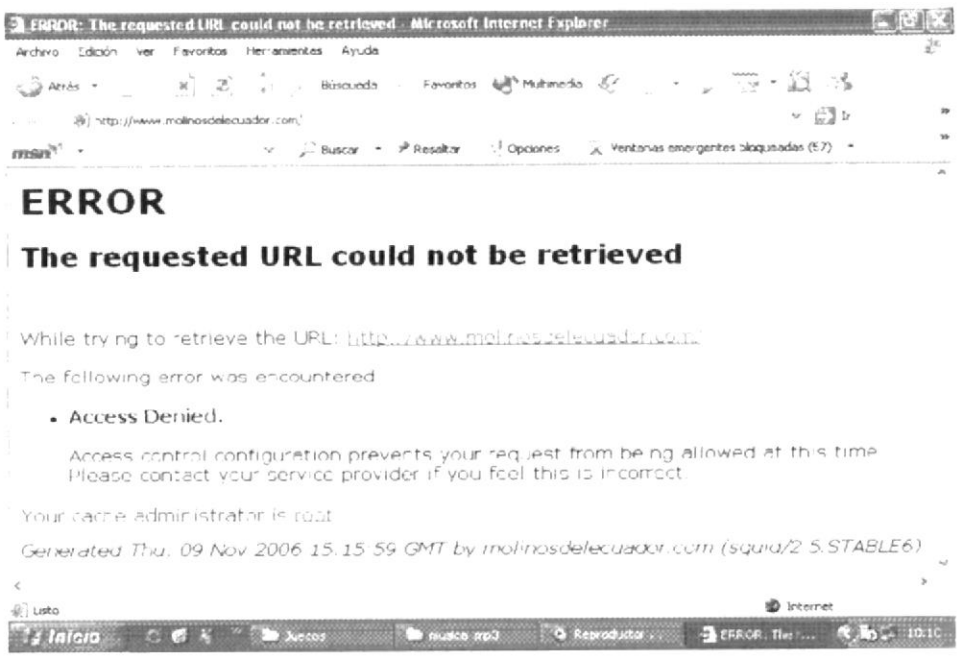


Figura 6-187: Bloqueo de Página

6.12.8 RESTRICCIONES POR HORARIO

1.- Como primer paso ingresar al archivo con el siguiente comando.
root@molinosdelecuador squid] # vi squid.conf

vi Editar archivos



Figura 6-188: Ingreso al Archivo Squid.Conf

2.- Configurar las listas de control de acceso donde se digitará el día y la hora de restricciones del Internet.

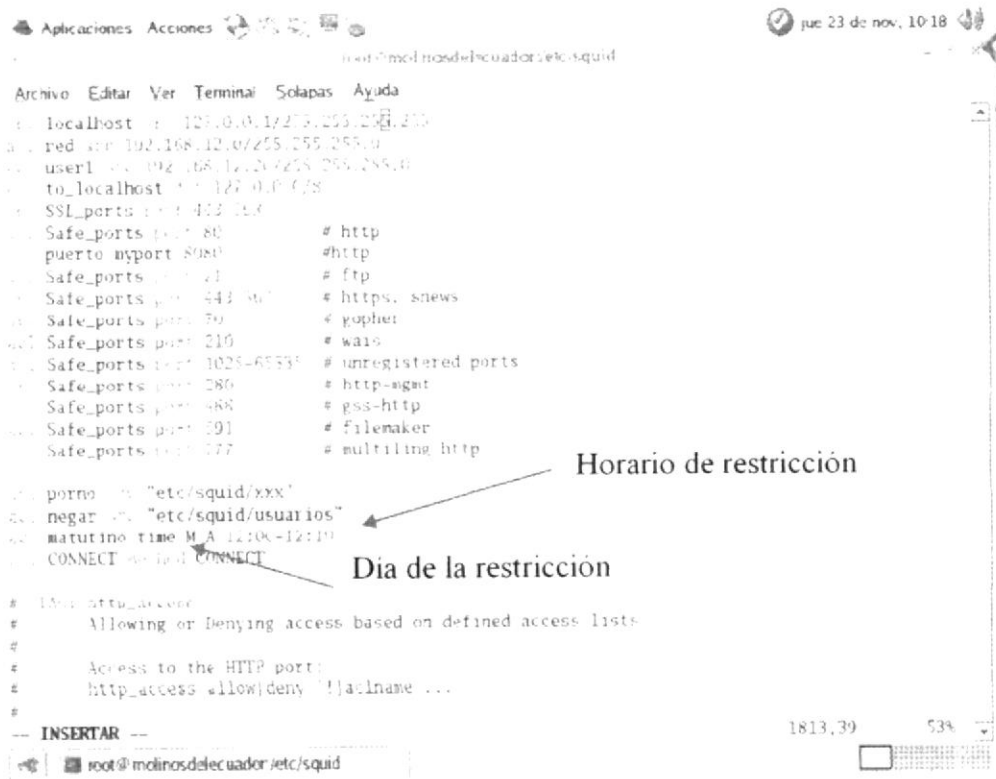


Figura 6-189: Lista de Control de Acceso

3.- Incluir las listas de control de acceso .

http_access deny redpuerto matutino

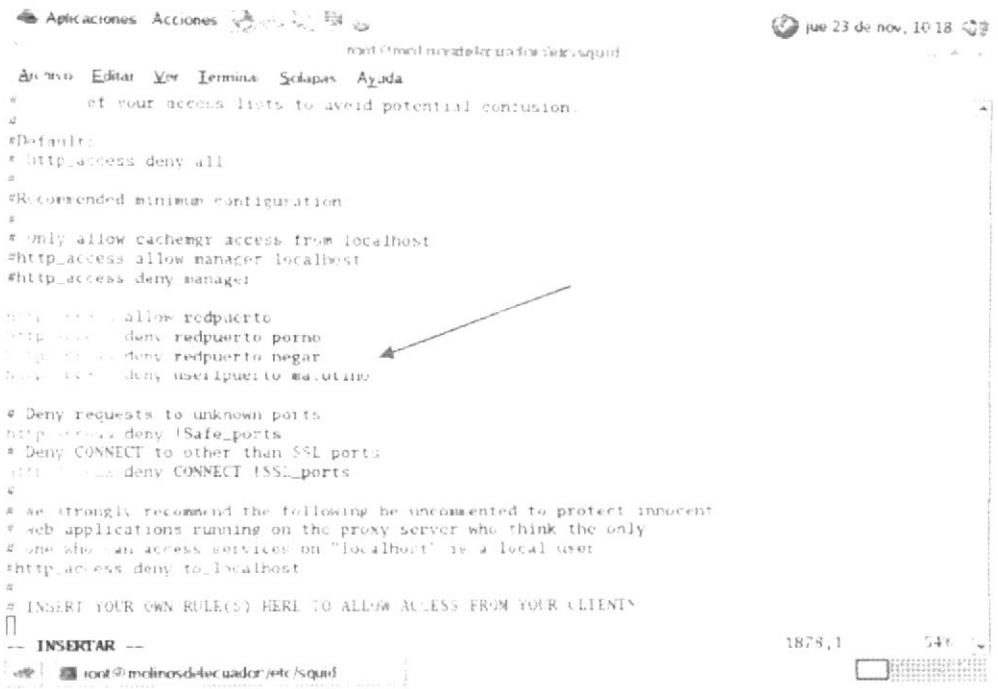


Figura 6-190: Restricción por Hora

4.- Reiniciar los servicios

[root@molinosdelecuador /] # service squid start

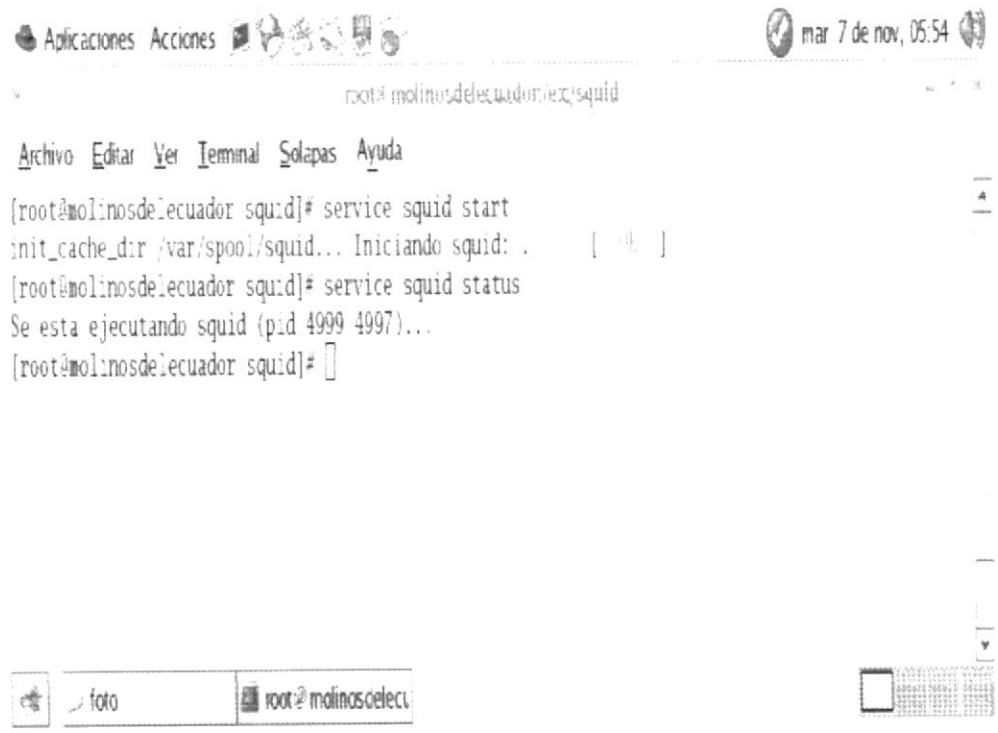


Figura 6-191: Iniciar Servicio Squid

6.12.8.1 CONFIGURACIÓN EN CLIENTE WINDOWS - HORARIO

1.- Para comprobar los cambios hechos en el servidor hacer doble clic en el icono del Internet Explorer.

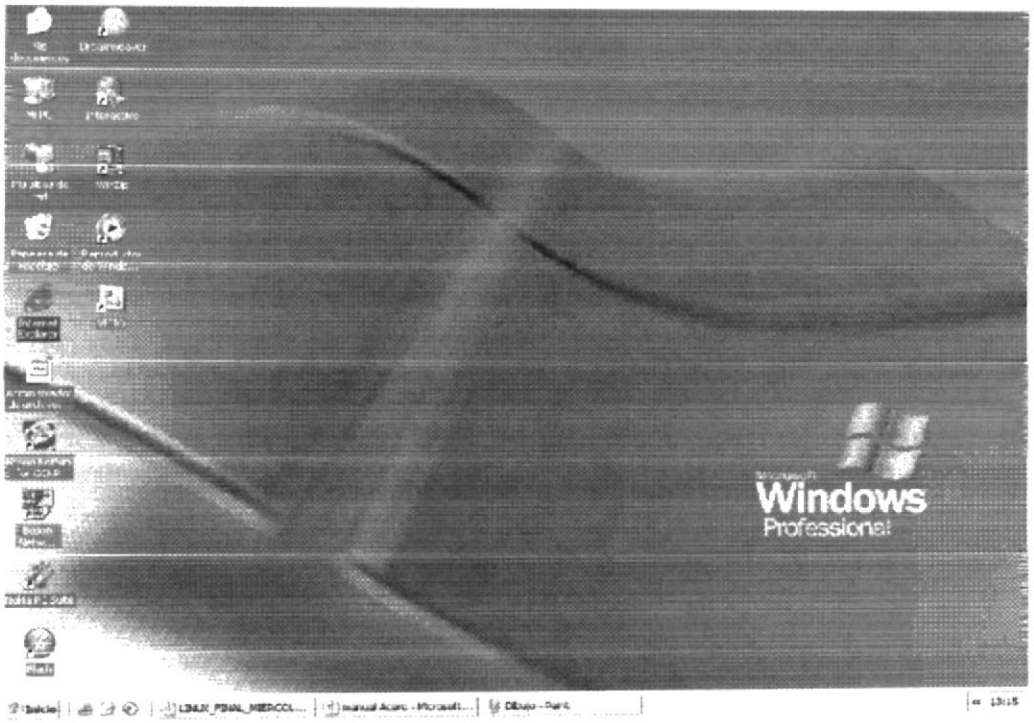
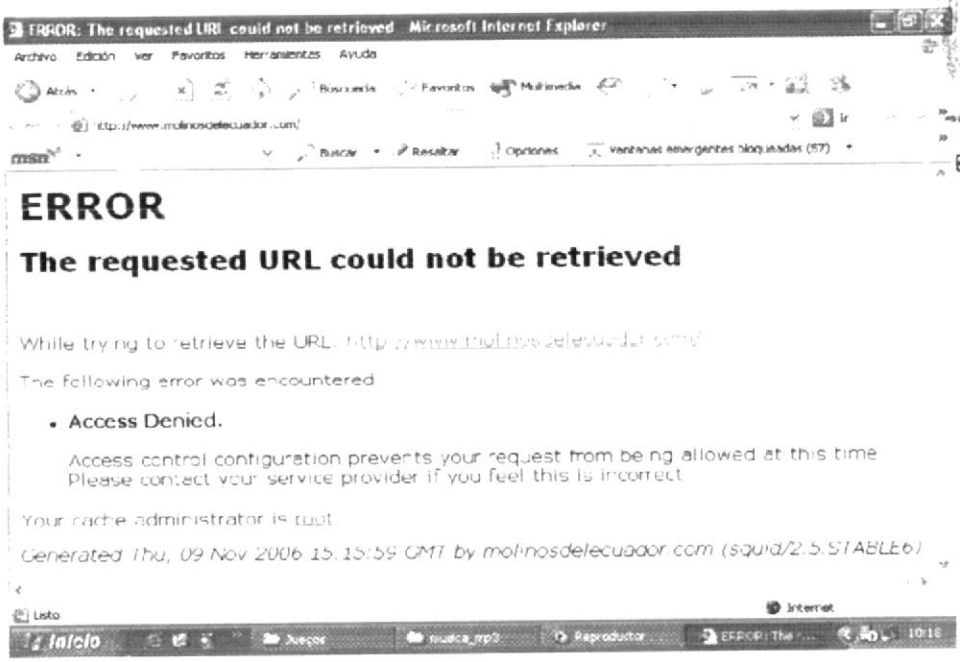


Figura 6-192: Entorno de Windows

2.- Luego debe mostrar algo parecido a esta pantalla. Esto indica que la restricción por horario en el servidor Proxy esta activa.



BIBLIOTECA CAMPUS PEÑAS

Figura 6-193: Restricciones de Página

6.12.9 AUTENTICACIÓN POR USUARIOS

1.- Como primer paso ingresar al archivo con el siguiente comando.
root@molinosdelecuador squid] # vi squid.conf



Figura 6-194:Ingreso al Archivo Squid.Conf

2.- En el archivo descomentar la siguiente línea:
auth_param basic program /usr/libexec/ncsa_auth /usr/etc/passwd
y proceder a editarla, esta línea sirve para especificar un programa de autenticación que se utilizará.

/usr/libexec/ncsa_auth.- Corresponde la localización del programa para autenticar.
usr/etc/passwd.- Este fichero contiene las cuentas y sus claves de acceso.
y digitar la dirección donde se quiere que este nuestra carpeta que va almacenar los password en nuestro caso se lo almacena en /etc/squid/passwd.

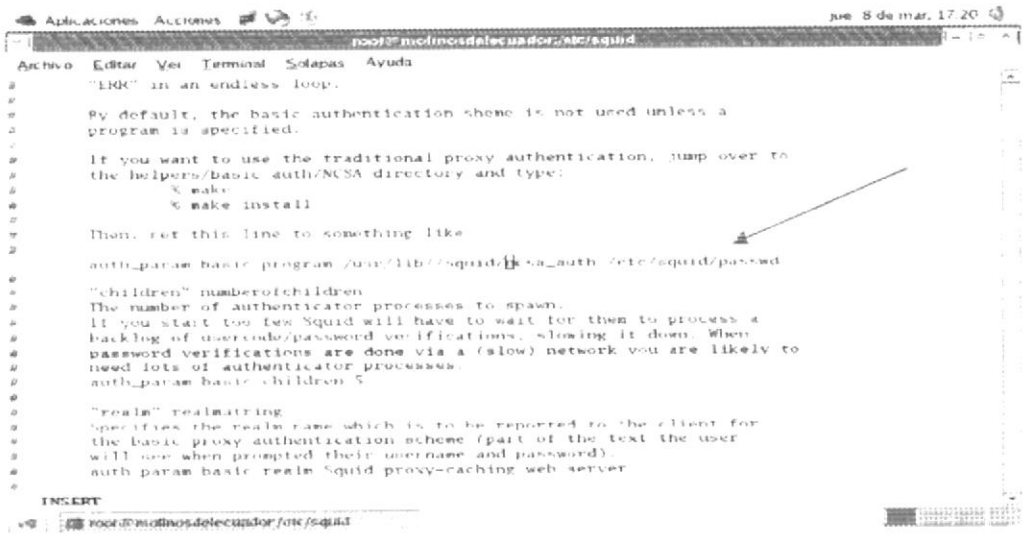


Figura 6-195: Ruta de Alojamiento de las Contraseñas

3.- Descomentar la siguiente línea.

Acl password proxy_auth REQUIRED

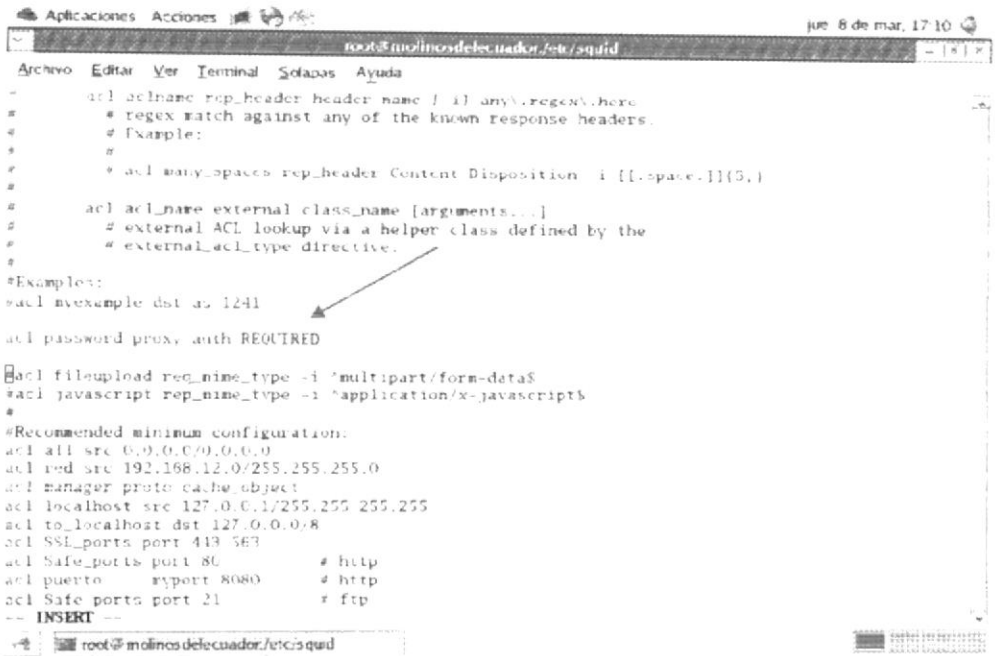


Figura 6-196: Acl Password

4.- Crear la lista de acceso.

http_access allow password red_puerto

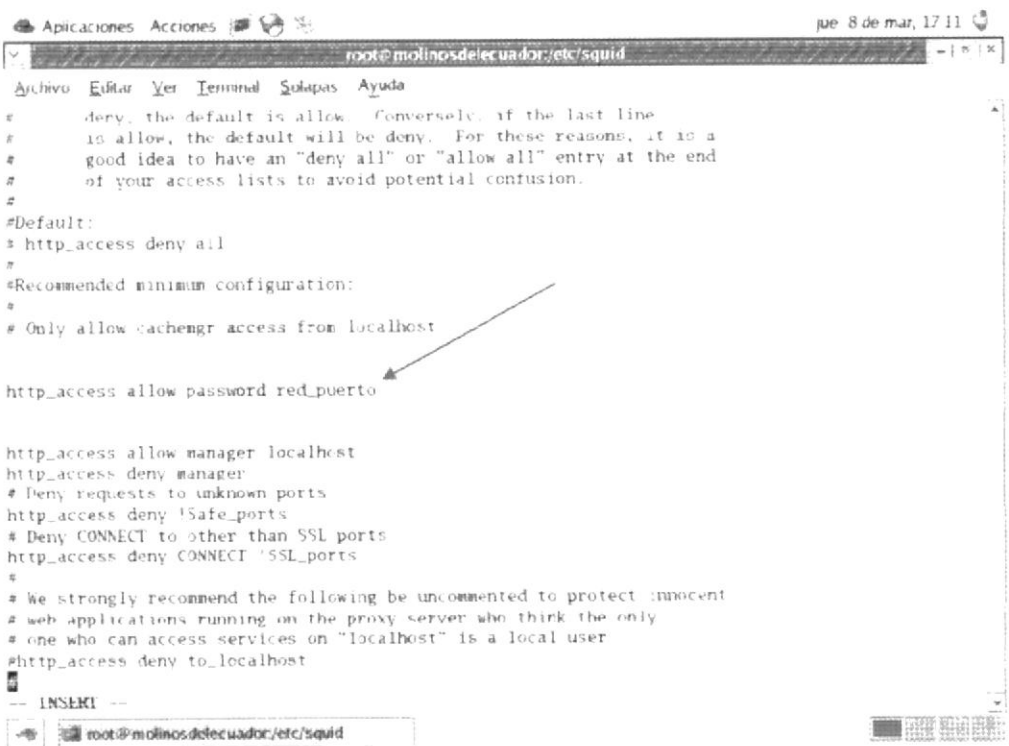


Figura 6-197: Http_Access por Autenticación

5.- Crear el archivo donde se va almacenar las contraseñas de los usuarios.

[root@molinosdelecuador squid]# touch passwd



Figura 6-198: Creación de Archivo Passwd

6.- Dar los respectivos permisos a la carpeta.

[root@molinosdelecuador squid]# chmood 600 passwd



ESPOL BIBLIOTECA

Figura 6-199: Permiso para el Archivo Passwd

7.- Crear los usuarios con sus respectivas contraseñas con el siguiente comando.

[root@molinosdelecuador squid]# httpasswd –b passwd fernando fernando



Figura 6-200: Creación de Usuarios y Contraseñas

6.12.9.1 CONFIGURACIÓN EN CLIENTE WINDOWS AUTENTICACIÓN POR USUARIOS

1.- Para comprobar los cambios hechos en el servidor hacer doble clic en el icono del **Internet Explorer.**

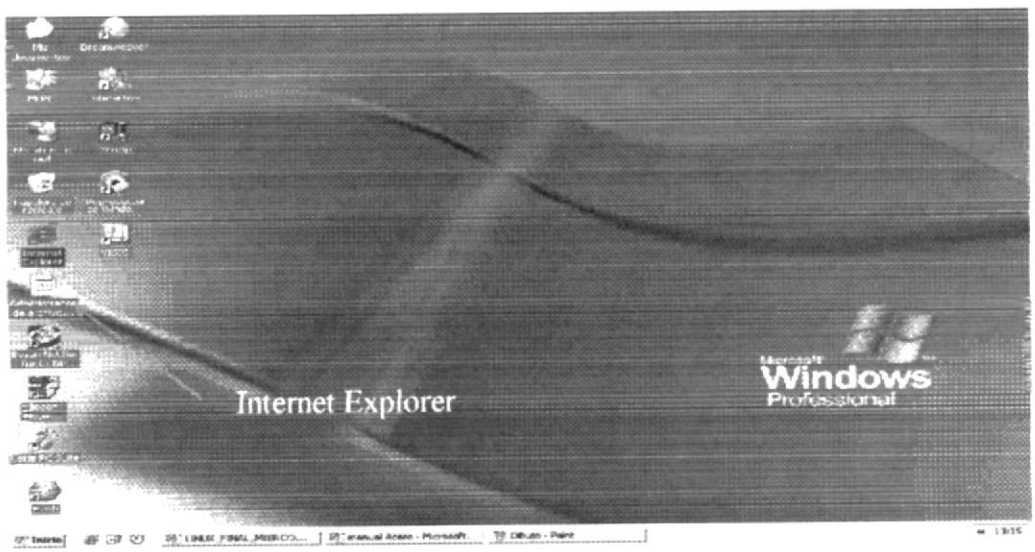


Figura 6-201: Entorno de Windows

2.- Luego aparecerá un recuadro, el cual pedirá un usuario y contraseña para tener acceso al Internet.

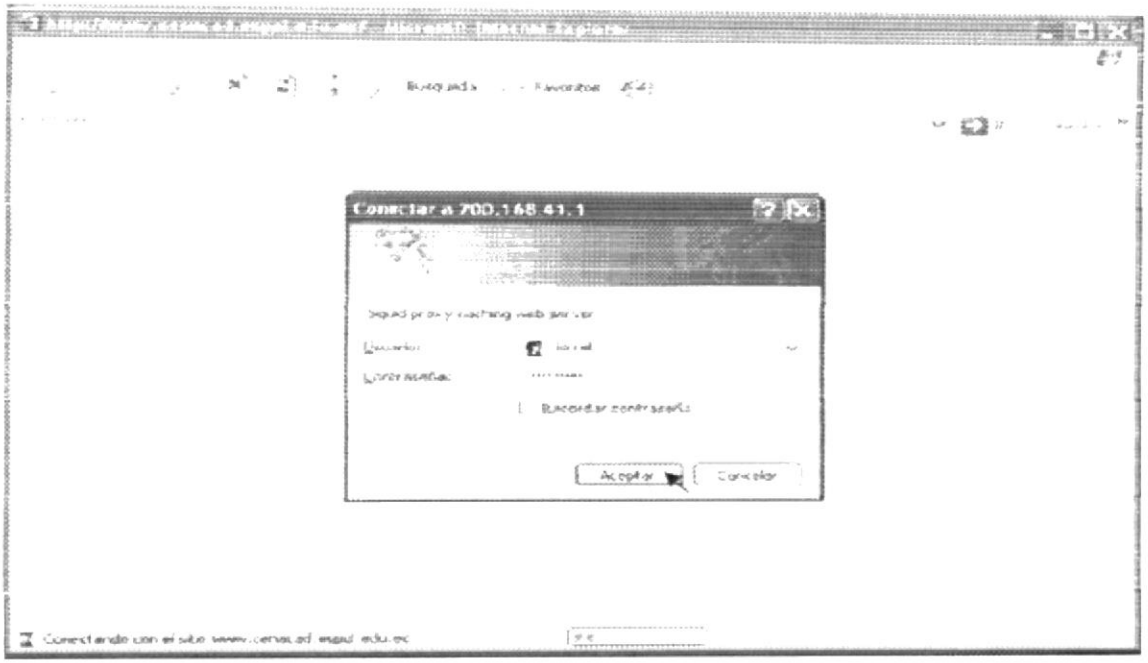


Figura 6-202: Opciones de Internet en Internet Explorer

3.- A continuación proceder a cargar el Internet Explorer y digitar una dirección Web para este caso será www.molinosdlecuador.com

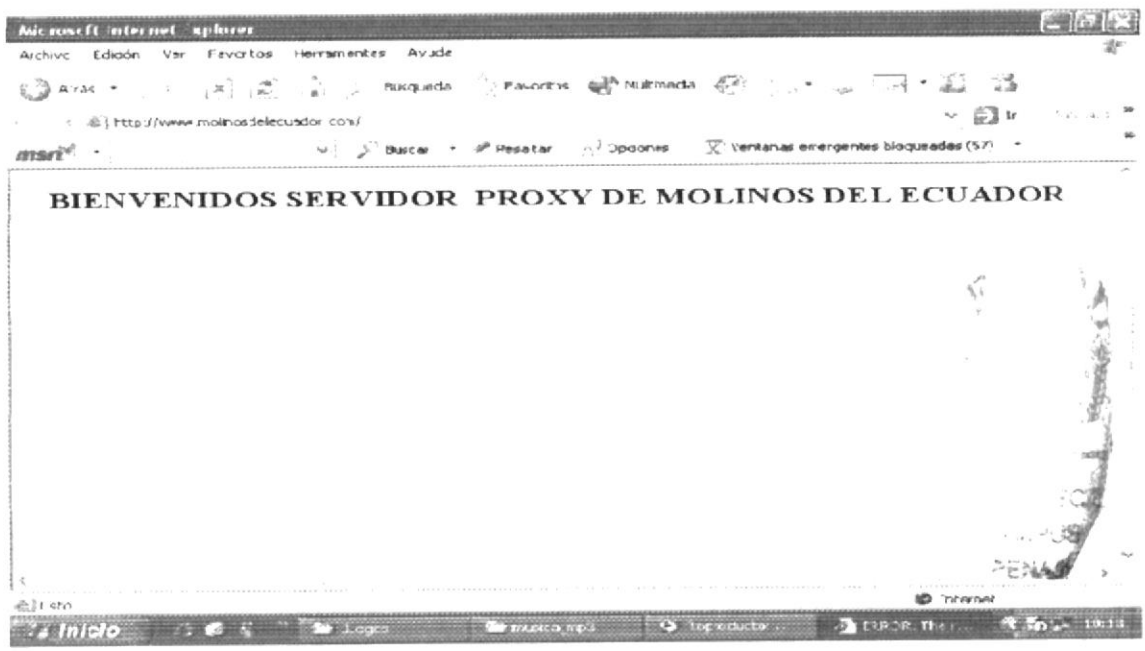


Figura 6-203: Página Habilitada

6.13 SERVIDOR DE FIREWALL

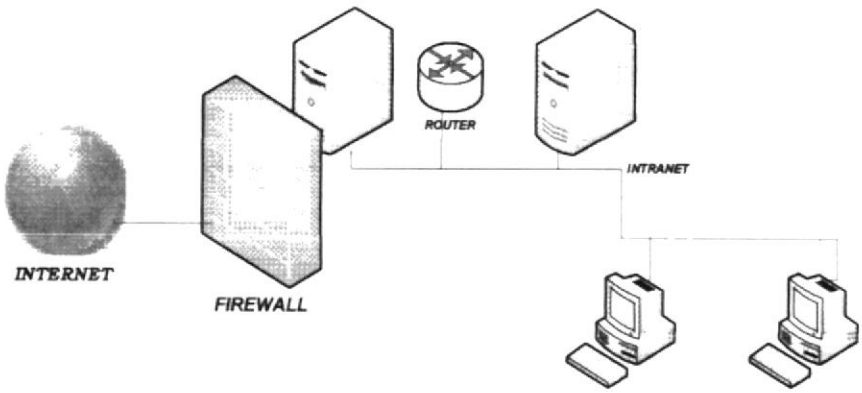


Figura 6-204: Firewall

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de Web, correo y FTP, pero no a IRC que puede ser innecesario para nuestro trabajo. También se puede configurar los accesos que se hagan desde Internet hacia la red local y también denegarlos todos o permitir algunos servicios como el de la Web, (si es que se posee un servidor Web y querer que accesible desde Internet). Dependiendo del firewall que se pesee también se puede permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un dispositivo que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el MODEM que conecta con Internet. Incluso poder encontrar ordenadores computadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes.

ESPOL
BIBLIOTECA
CAMPUS

6.13.1 TIPOS DE CORTAFUEGOS

Cortafuegos de capa de red o de filtrado de paquetes funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC.

6.13.1.1 CORTAFUEGOS DE CAPA DE APLICACIÓN

Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuegos a nivel 7 de tráfico HTTP es normalmente denominado Proxy y permite que los computadores de una organización entren a internet de una forma controlada.

6.13.1.2 CORTAFUEGOS PERSONALES

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

Ventajas de un cortafuego

- **Protege de intrusiones.** El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- **Protección de información privada.** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

BIBLIOTECA CAMPUS

6.13.2 DIRECCIÓN DE ORIGEN

Indica quien es el emisor del paquete, de qué ordenador viene. Se puede especificar con una dirección IP, un nombre de host o una dirección de red en formato CIDR (192.168.0.0/24) o en notación clasica (192.168.0.0/255.255.255.0). En iptables se puede especificar la dirección origen con la opción "-s". Si en una regla se omiti la dirección origen equivale a poner 0/0 es decir cualquier dirección. Por ejemplo "-s 192.168.0.0/24" indicaría cualquier dirección con origen en la red de clase C (24 bits de red) 192.168.0.0. Si delante de la dirección se añade "!" entonces se hace referencia a cualquier dirección salvo la especificada, es decir, que no sea esa dirección.

6.13.3 DIRECCIÓN DE DESTINO

Indica a quien va dirigido el paquete, a qué ordenador via. También se puede especificar con una dirección IP, un nombre de host o una dirección de red en formato CIDR (192.168.0.0/24) o en notación clasica (192.168.0.0/255.255.255.0). En iptables se podrá especificar la dirección destino con la opción "-d". Si en una regla se omite la dirección origen equivale a poner 0/0 es decir cualquier dirección. Por ejemplo "-s 192.168.0.0/24" indicaría cualquier dirección con destino a la red de clase C (24 bits de red) 192.168.0.0. Si delante de la dirección se añade "!" entonces se hace referencia a cualquier dirección salvo la especificada, es decir, que no sea esa dirección.

6.13.4 PROTOCOLO

Se Puede establecer filtros sobre protocolos concretos, será obligatorio si además se especifica algún puerto. La opción para especificar un protocolo es "-p" y los valores posibles son TDP, UDP e ICMP. El signo "!" antes del nombre del protocolo también se utiliza para negar.

6.13.5 INTERFAZ DE ENTRADA

Poder especificar un dispositivo de entrada de red concreto con la opción "-i". Por ejemplo "-i eth0" indicaría un paquete que proviene de eth0. Se puede usar un "!". Evidentemente no se podrá usar un interfaz de entrada con una regla de salida (OUTPUT).

6.13.6 INTERFAZ DE SALIDA

También se puede especificar un dispositivo de salida de red concreto con la opción "-o". Por ejemplo "-o eth0" indicaría un paquete que sale por eth0. Se puede usar un "!". Evidentemente no se podrá usar un interfaz de salida con una regla de entrada (INTPUT).

6.13.7 PUERTO ORIGEN

Mediante la opción "--sport" se podrá especificar un puerto o un rango de puertos si se separan por ":", por ejemplo [1024:65535] indicaría desde 1025 hasta 65535. Los puertos los se pueden especificar por su número o también por el nombre asociado en el fichero /etc/services. Es necesario especificar -p TCP o -p UDP para poder especificar un puerto origen.

6.13.8 PUERTO DESTINO

Mediente la opción "--dport" se podrá especificar un puerto o un rango de puertos. Las consideraciones son iguales que para el puerto origen.



6.13.9 DEFINICIÓN DE REGLAS

Para definir una nueva regla sólo se tiene que decirle a iptables si tiene que insertar la nueva regla en alguna posición (-I numero) o bien simplemente añadirla al final (-A) y la descripción de la regla. Ejemplos:

Ejemplo 1:

iptables -A INPUT -s 192.168.0.0/24 -d 192.168.5.0 -p tcp --dport 80 -j ACCEPT

Se añade (-A) una regla de entrada (INPUT) que indica que todos los paquetes originados en la red 192.168.0.0 (-s 192.168.0.0/24) y dirigidos a la la red 192.168.5.0 (-d 192.168.5.0) y dirigidos al puerto 80 (--dport 80) tienen que dejarse pasar (-j ACCEPT).

Ejemplo 2:

Iptables –A FORWARD -s 192.168.0.7 -j REJECT

Se añade (-A) una regla de reenvío (FORWARD) que indica que todo el tráfico proveniente del ordenador 192.168.0.7 (-s 192.168.0.7) se rechaza (-j REJECT). Es decir se está cortando a este equipo la salida fuera de la red.

Ejemplo 3:

iptables -A OUTPUT -o eth0 -j ACCEPT

Permitir cualquier salida por la interfaz de red eth0.

Conocido también como muro de fuego, este impedirá el acceso no autorizado a sus servicios e información, y/o controlar el acceso de los usuarios de su red a Internet.
Es la interfaz entre el ordenador y la red, determina que recursos de su equipo están accesibles para los usuarios remotos de la red, un firewall bien configurado puede aumentar significativamente la seguridad del sistema.
Existen tres tipos de reglas:

INPUT= entrada al servicio
OUTPUT = servidor hacia fuera
FORDWARD = redireccionar



6.13.10 IP TABLES

Es la herramienta que permite configurar las reglas del sistema de filtrado de paquetes del kernel de Linux
se debe especificar para cada regla una acción o target. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se recorren en orden hasta que las condiciones que pide una de ellas se cumplen en el paquete, y la regla se activa realizando sobre el paquete la acción que le haya sido especificada.

Estas acciones se plasman en los que se denominan targets, que indican lo que se debe hacer con el paquete. Los más usados son bastante explícitos: **ACCEPT, DROP** y **REJECT**

INPUT: Paquetes recibidos para nuestro sistema

FORWARD: Paquetes enrutados a través de nuestro sistema

OUTPUT: Paquetes generados en nuestro sistema y que son enviados

p [protocolo]: Protocolo al que pertenece el paquete.

-s [origen]: dirección de origen del paquete, puede ser un nombre de host, una dirección IP normal, o una dirección de red (con máscara, de forma dirección/máscara).

-d [destino]: Al igual que el anterior, puede ser un nombre de host, dirección de red o dirección IP singular.

-i [interfaz-entrada]: Especificación del interfaz por el que se recibe el paquete.

-o [interfaz-salida]: Interfaz por el que se va a enviar el paquete.

-j [target]: Permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.

Iptables –F: borrado de reglas
Iptables –L: listado de reglas que se están aplicando
Iptables –A: añadir regla
Iptables –D: borrar una regla especifica



6.13.11 REQUERIMIENTOS PARA CONFIGURAR FIREWALL

- Un computador con Linux Fedora Core 3 instalado.
- Tarjeta de red.
- Configuración de IP estática.

6.13.12 CONFIGURACIÓN DE FIREWALL

6.13.12.1 BLOQUEAR PING

Iptables -A: Añade una regla de firewall.
INPUT: Añadir una entrada al servidor.
-s192.168.12.0/24: Es la dirección ip de origen.
-d192.168.12.1/24: Es la dirección ip de destino.
-p icmp. :Es el protocolo asignado.
-j DROP : Es la acción que se aplica para este caso es negar.



Figura 6-205: Bloqueo Ping

ESPOL BIBLIOTECA CAMPUS PEÑAS

6.13.12.2 HABILITAR TELNET

Ingresar al directorio del etc/ xinetd.d

[root@molinosdelecuador etc]# cd xinetd.d

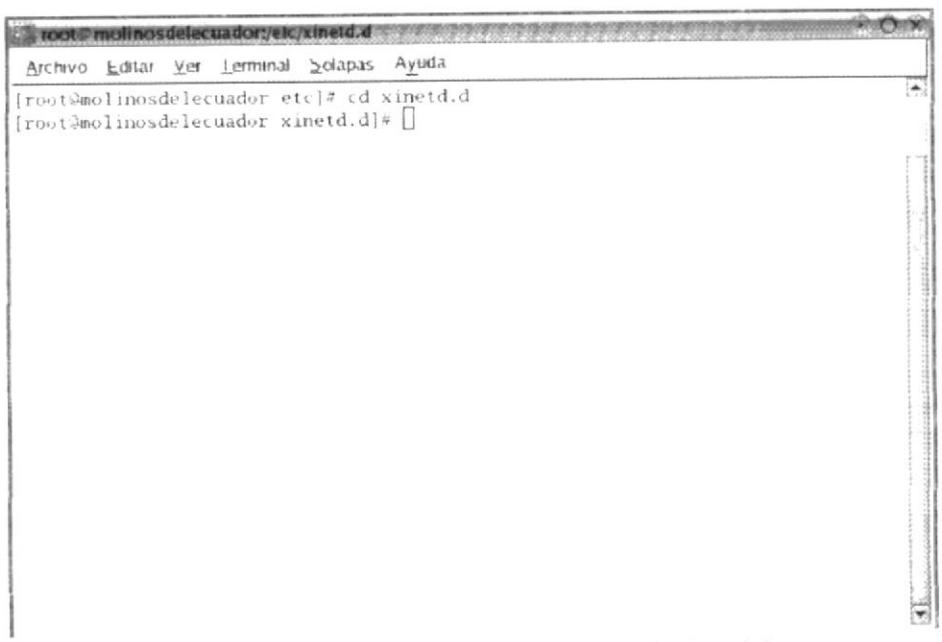


Figura 6-206: Ingreso al Directorio del Xinetd.d

Una vez en el directorio ingresar al archivo donde se habilita el telnet.

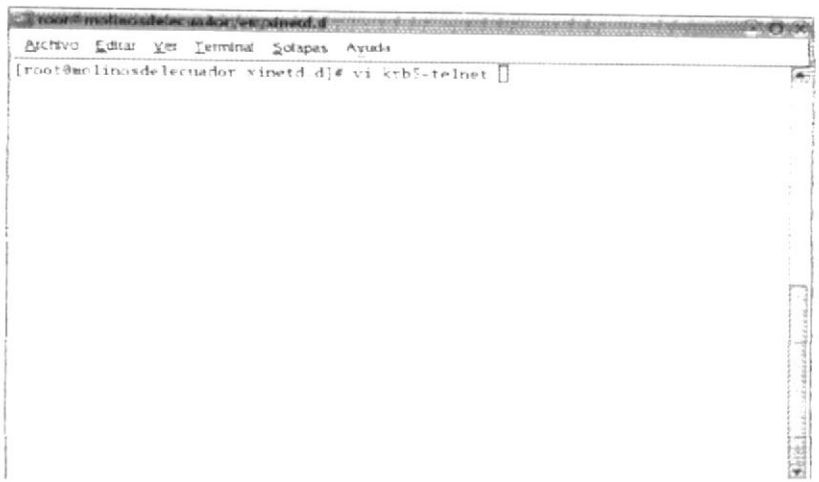


Figura 6-207: Ingreso al Archivo Krb5-telnet

En esta página se muestra la línea a cambiar para habilitar el firewall por default aparecerá **"wait = yes",** la cual cambiar por **"wait = no".**

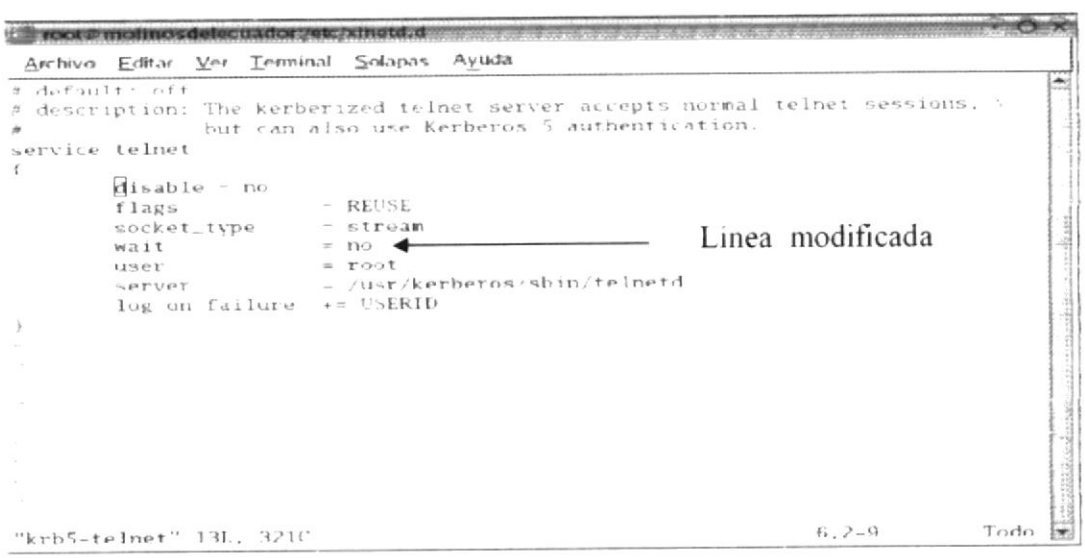


Figura 6-208: Habilitación del Telnet

ESPOL
BIBLIOTECA
CAMPUS
PENAS

6.13.12.3 BLOQUEO DE TELNET

Iptables -A: Añade una regla de firewall.
INPUT: Añadir una entrada al servidor.
-s192.168.12.0/24: Es la dirección ip de origen.
-d192.168.12.1/24: Es la dirección ip de destino.
-p tcp. :Es el protocolo asignado.
--dport 23: puerto
-j DROP : Es la acción que se aplica para este caso es negar.





Figura 6-209: Bloqueo Telnet

ESPOL BIBLIOTECA CAMPUS PEÑAS

6.13.12.4 BLOQUEAR FTP

Iptables -A: Añade una regla de firewall.
INPUT: Añadir una entrada al servidor.
-s192.168.12.0/24: Es la dirección ip de origen.
-d192.168.12.1/24: Es la dirección ip de destino.
-p tcp. :Es el protocolo asignado.
--dport 21: puerto
-j DROP : Es la acción que se aplica para este caso es negar.





Figura 6-210: Bloqueo FTP

Para verificar si se habilitaron los Firewalls en el servidor Linux digitar el siguiente comando: Iptables –L.



Figura 6-211: List de Iptables

6.13.13 CONFIGURACIÓN EN CLIENTE WINDOWS - FIREWALL

1.- Ingresar a **Inicio**, **Ejecutar** y digitar **cmd**.

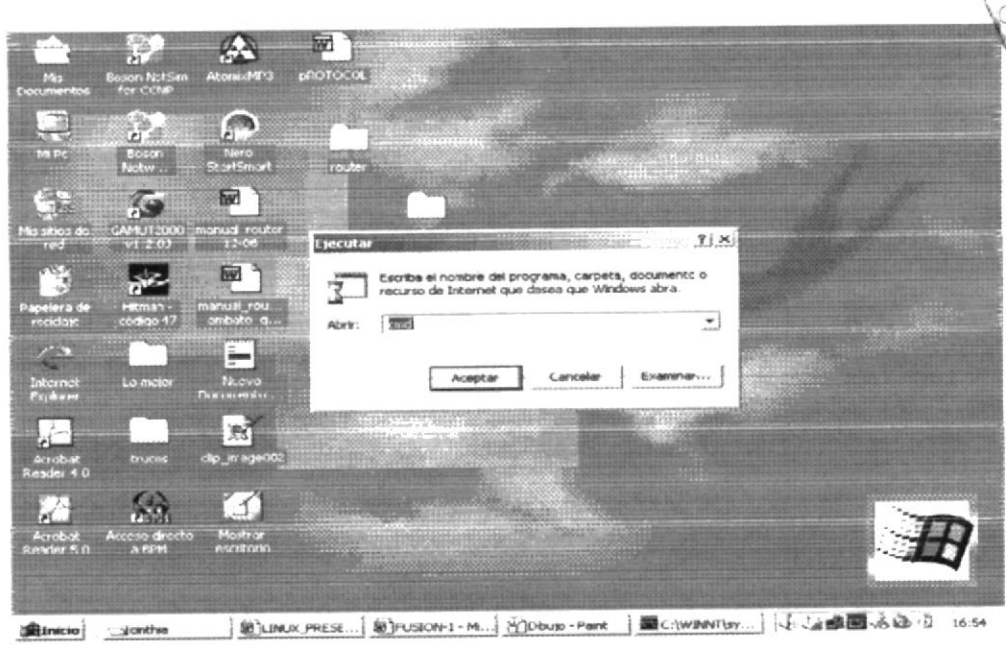


Figura 6-212 Ingreso al Cmd

2.- Una vez en el cmd digitar la dirección del servidor (ping 192.168.12.1) y mostrará respuesta por parte del servidor.

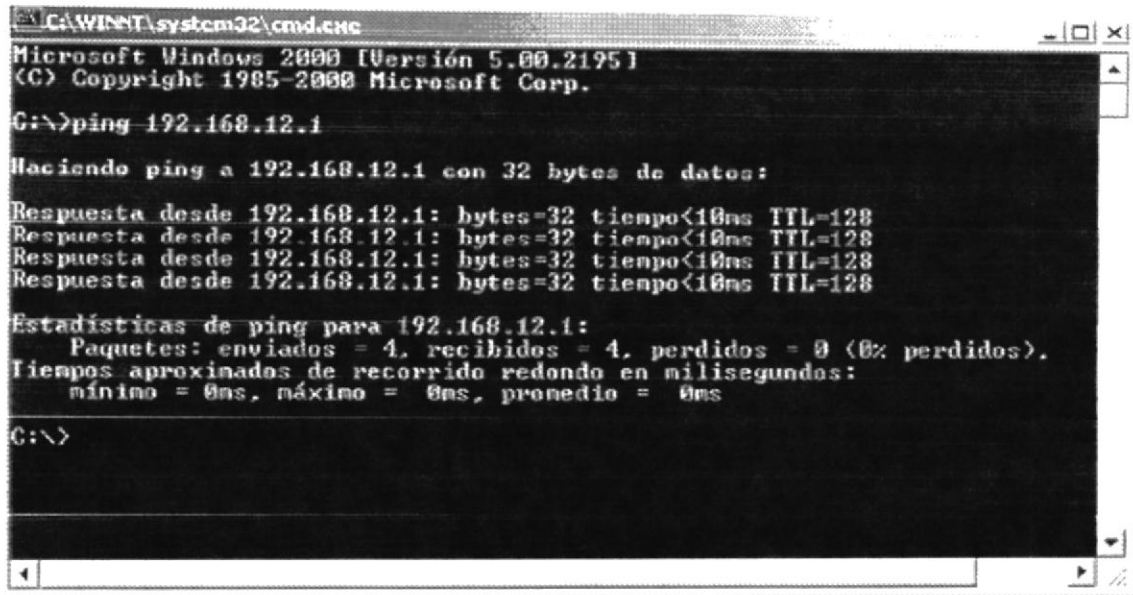


Figura 6-213: Ping al Servidor

En esta pantalla muestra el **bloqueo** del ping por parte del servidor.

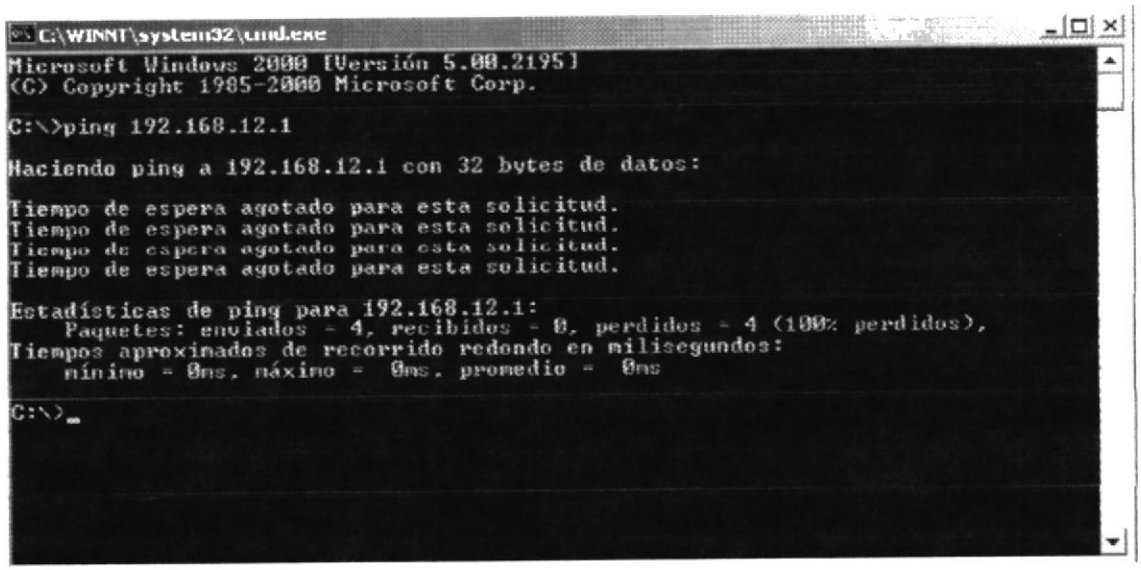


Figura 6-214: Bloqueo de Ping

3.- En esta pantalla muestra el **acceso** al servidor mediante telnet.

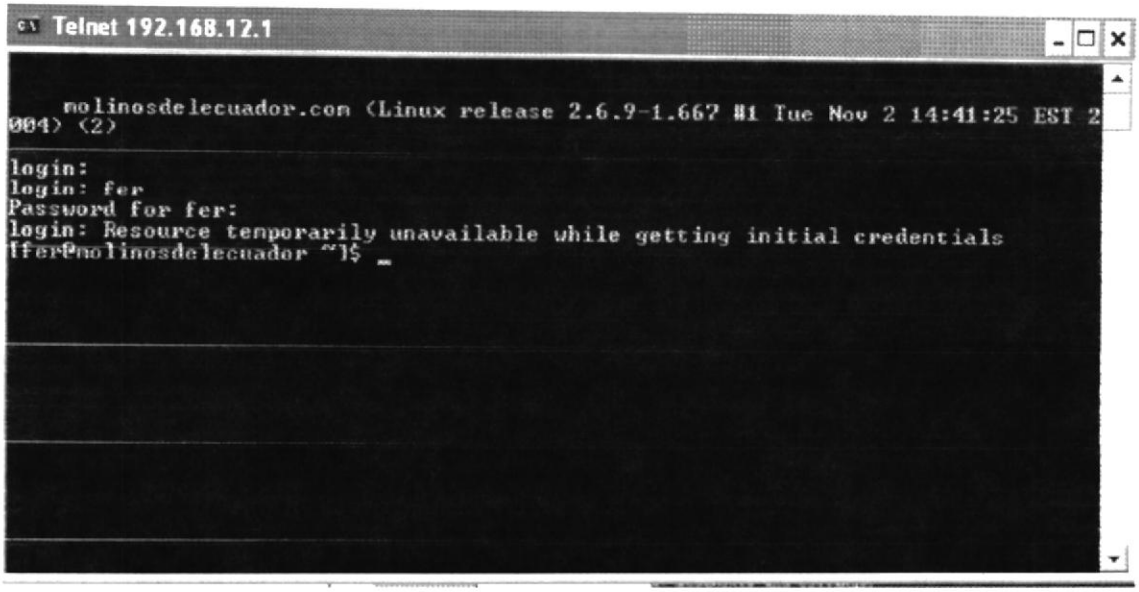


Figura 6-215: Telnet al Servidor

BIBLIOTECA CAMPUS PEÑAS

4.- En esta pantalla muestra el **bloqueo** de telnet.

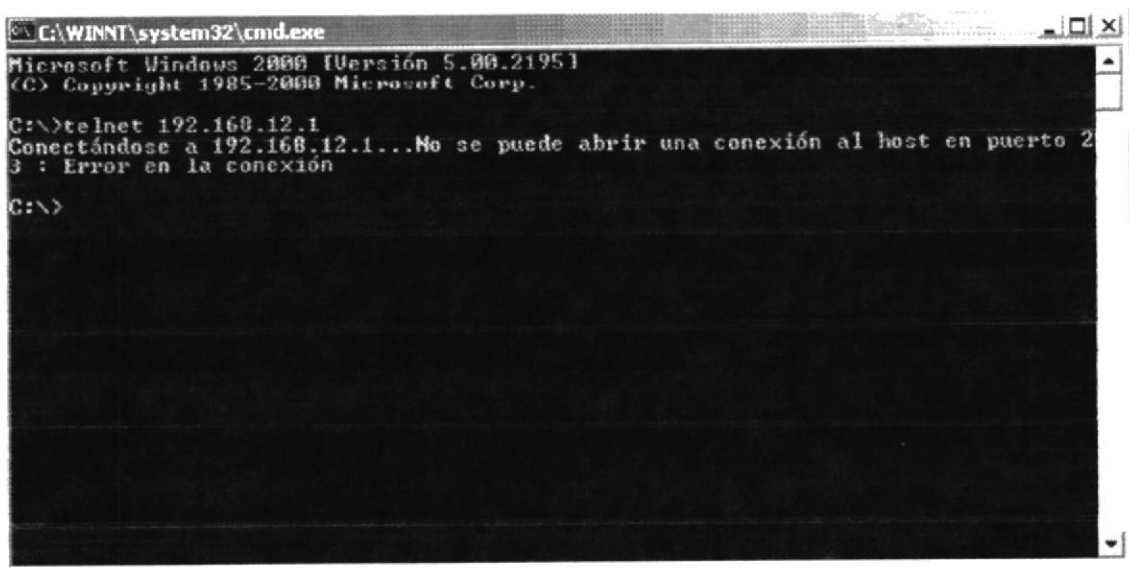


Figura 6-216 Bloqueo de Telnet

6.14 SERVIDOR DHCP

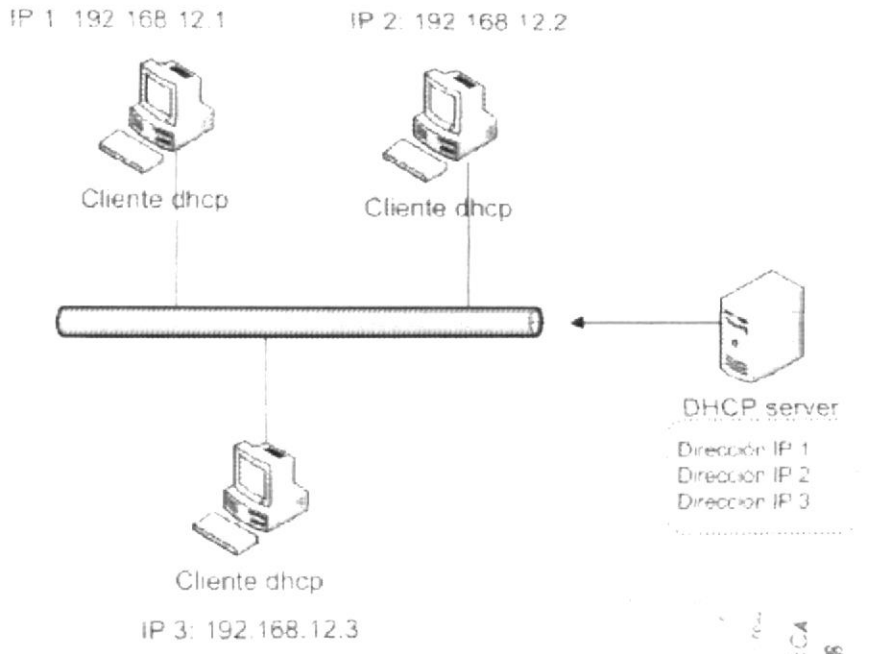


Figura 6-217 Servidor Dhcp

BIBLIOTECA CAMPUS PEÑAS

DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido, a quien se la ha asignado después.

6.14.1 CARACTERÍSTICAS

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

Este protocolo se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131 . Los últimos esfuerzos describiendo DHCP v6, DHCP en una red IPv6, fueron publicados como RFC 3315.

6.14.2 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**: donde la asignación se basa en una tabla con direcciones MAC (pares de direcciones IP ingresados manualmente por el administrador). Sólo las computadoras con una dirección MAC que figure en dicha tabla recibirá el IP que le asigna dicha tabla.

- **Asignación automática**: donde una dirección de IP libre obtenida de un rango determinado por el administrador se le asigna permanentemente a la computadora que la requiere.

- **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 RESTAURACIÓN 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".

BIBLIOTECA CAMPUS PEÑAS

6.14.3 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 las computadoras cliente.

6.14.4 DHCP DISCOVER

La computadora cliente emite 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.

6.14.5 DHCP OFFER

El servidor determina la configuración basándose en la dirección del soporte fisico 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.



6.14.6 DHCP REQUEST

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

6.14.7 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.

6.14.8 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.

6.14.9 DHCP RELEASE

El cliente envía una petición al servidor DHCP para liberar su dirección DHCP. Como los clientes generalmente no saben cuándo los usuarios pueden desconectarles de la red, el protocolo no define el envío del *DHCP Release* como obligatorio.

6.14.10 REQUERIMIENTOS PARA LEVANTAR UN SERVIDOR DHCP

- Un computador con Linux Fedora Core 3 instalado
- Tarjeta de red
- Configuración de IP ESTÁTICA
- Paquete DHCP instalado

6.14.11 CONFIGURACIÓN DE DHCP

1.- Verificar si el paquete del d.C. si esta instalado:

[root@molinosdelecuador /]# rpm –q dhcp

rpm –q Verifica si estan instalados los paquetes



Figura 6-218 Verificar Paquete Dhcp

2.- Buscar la localización de archivo que se editará de la siguiente manera:

[root@molinosdelecuador etc]# slocate dhpd.conf

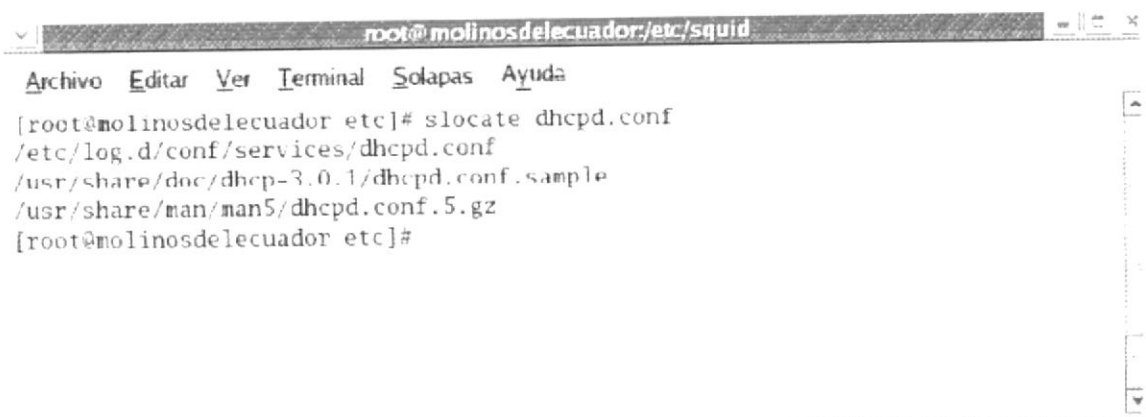


Figura 6-219: Busqueda del Archivo Dhcpd.conf

3.- Copiar el archivo dhcp-3.0.1 a la ruta donde quiere que se se aloje el archivo del d.C. para poder configurarlo, a continuación se indica la ruta.

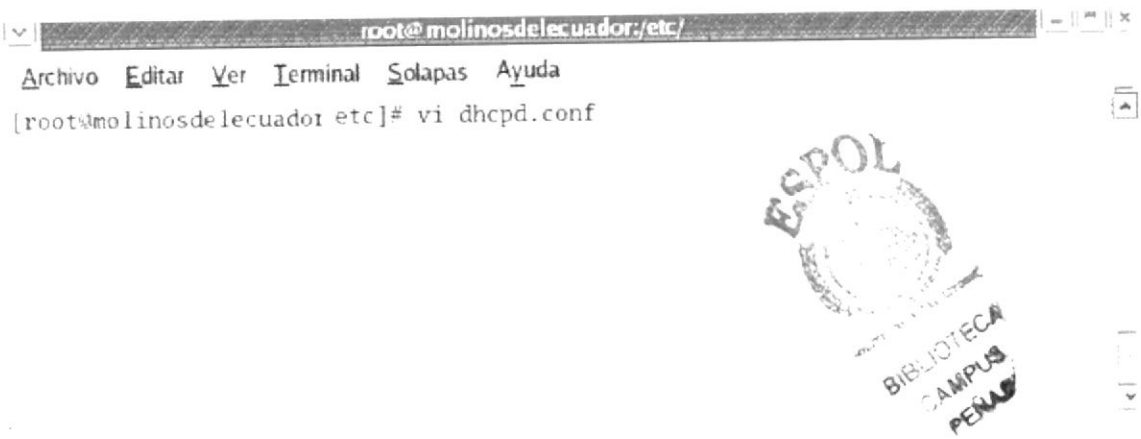
[root@molinosdelecuador /]# cp /usr/share/doc/dhcp-3.0.1/dhcpd.conf.sample/ etc/dhcpd.conf



Figura 6-210: Copia del Fichero Dhcpd.Conf

4.- Editar el archivo ***dhcp.conf*** con el comando **vi** de la siguiente manera:
[root@molinosdelecuador etc] **# vi dhcpd.conf**

Vi Editar archivo



ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 6-221: Ingreso al Archivo Dhcpd.Conf

5.- Configurar el archivo ***dhcpd.conf***

En la linea subnet se asigna el segmento de red con su respectiva máscara.
Subnet 192.168.12.0 **netmask** 255.255.255.0
Opcional colocar la linea del **gateway**
Option routers 192.168.12.1
Option subnet – mask 255.255.255.0
Digitar la direccion del DNS

Option Domain –name-servers 192.168.12.1
Definir el rango de ip desde – hasta
Range dynamic – boota 192.168.120.10 192.168.20.20
Salir con **:wq** para guardar los cambios.

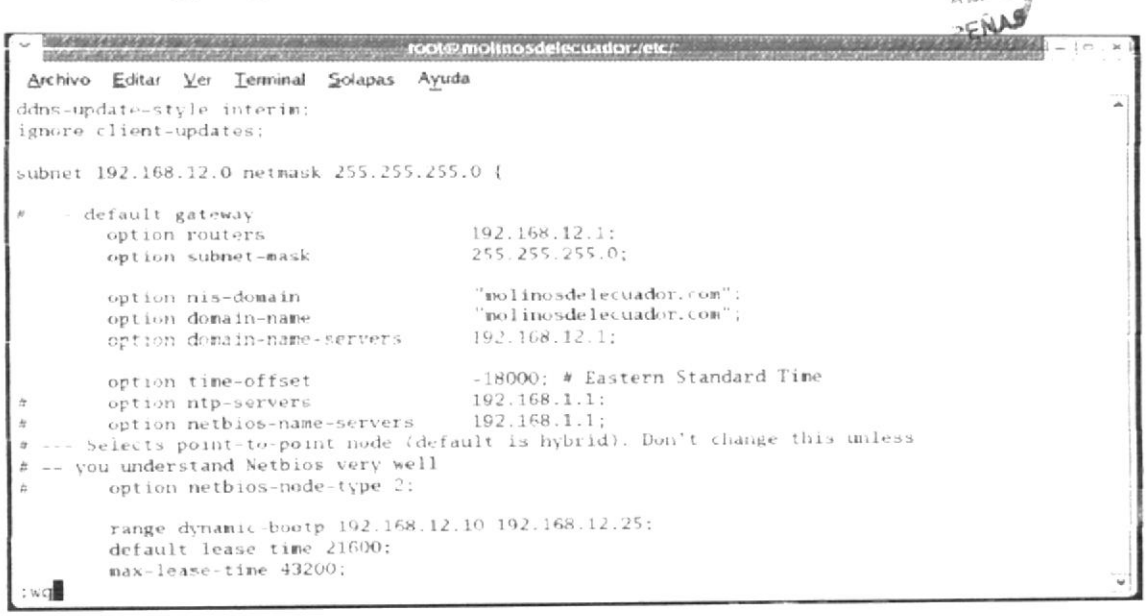


Figura 6-222: Configuración Dhcp

6.- Se debe crear un archivo en la siguiente ruta que es donde se guardan todas las direcciones ip asignadas por dhcp :

[root@molinosdelecuador etc] # touch/var/lib/dhcp/dhcpd.leases

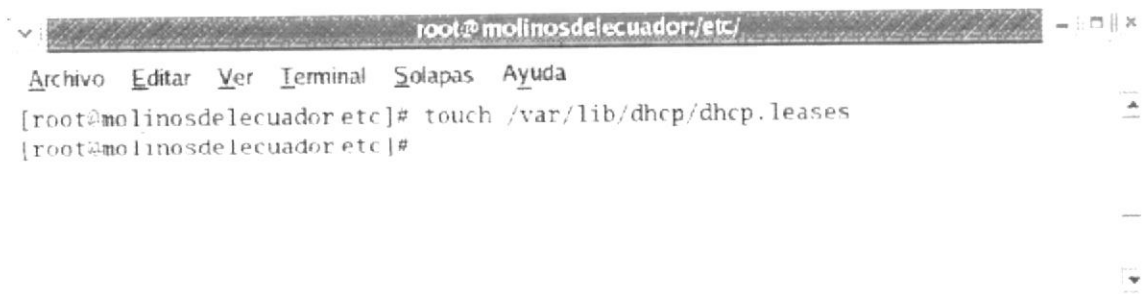


Figura 6-223: Creación delAarchivo Dhcp.leases

7.- Para añadir dhcp al arranque del sistema se ejecuta.

[root@molinosdelecuador etc] # chkconfig dhcpd on

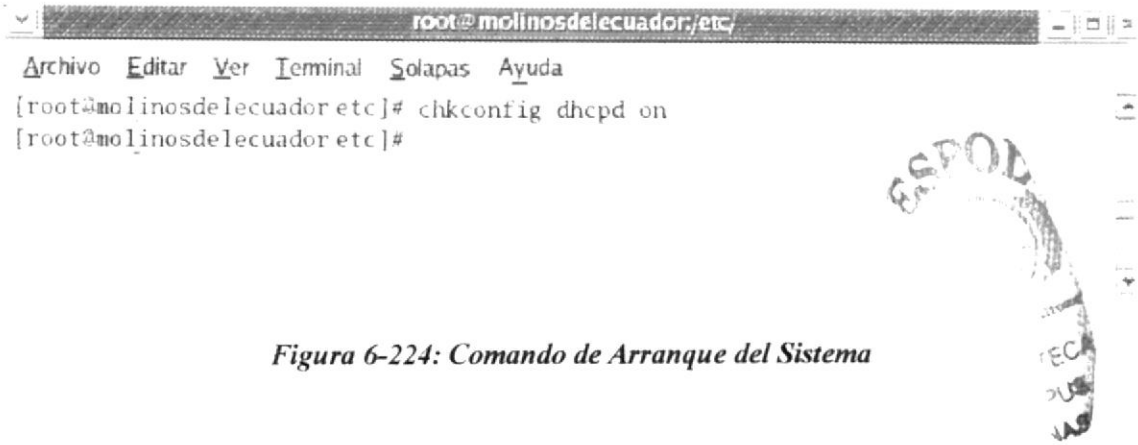


Figura 6-224: Comando de Arranque del Sistema

8.- Verificar el estado del proceso de dhcpd cada vez que se realice un cambio.
[root@molinosdelecuador etc] # pgrep dhcpd

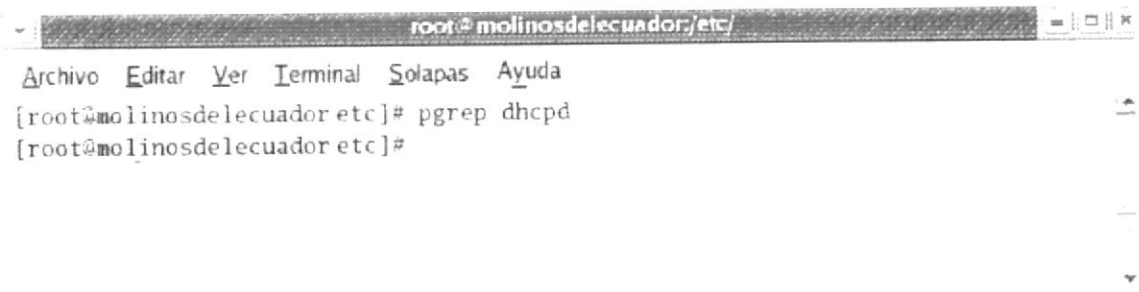


Figura 6-225: Verificación del Estado del Dhcpd

9.- Restaurar los servicios del dhcpd

[root@molinosdelecuador **etc]** service dhcpd restart (Iniciar el servicio del dhcpd)

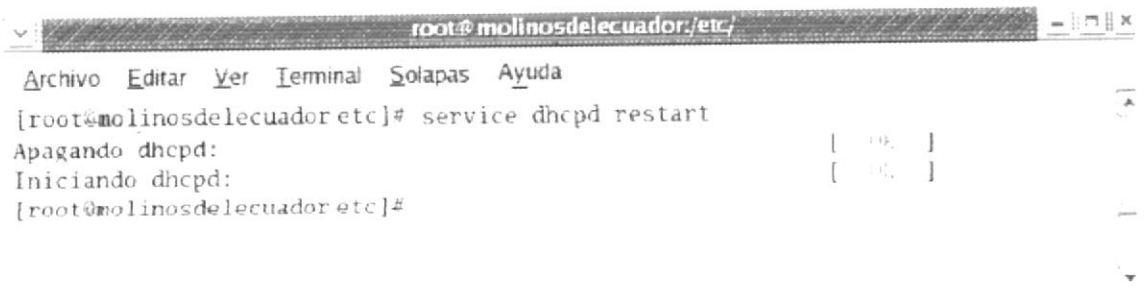


Figura 6-226: Restaurar los Servicio Dhcpd

6.14.12 CONFIGURACION EN CLIENTE WINDOWS - DHCP

Ir a **Mis Sitios de red** y hacer clic derecho y elegir la opción de **Propiedades**.

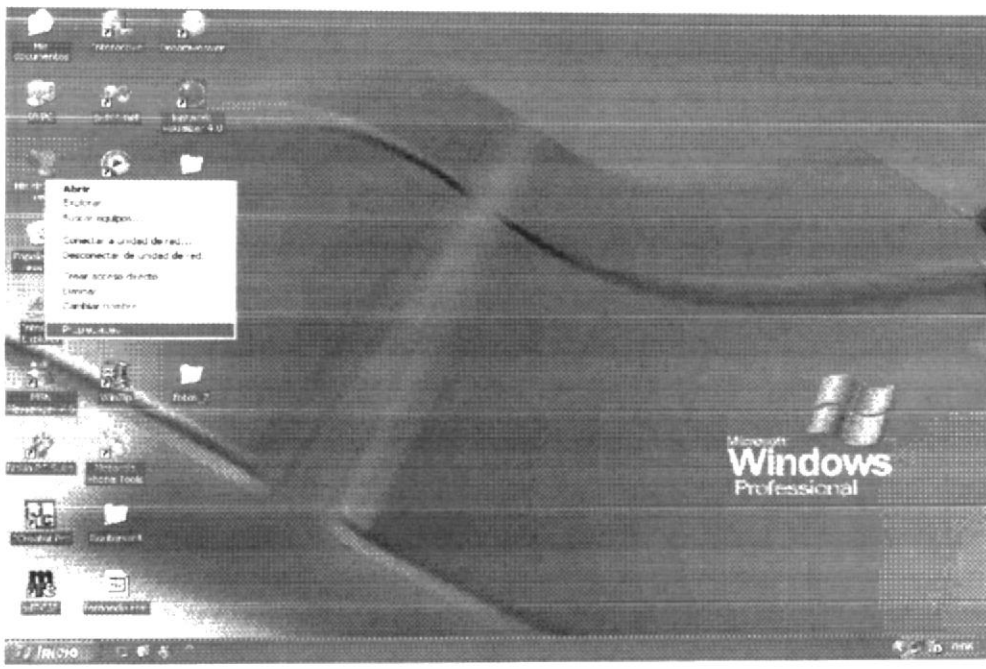


Figura 6-227: Selección de Propiedades de Mis Sitios de Red

Hacer clic derecho en la opción de **Conexión De Área Local**, y elegir la opción de **Propiedades**.

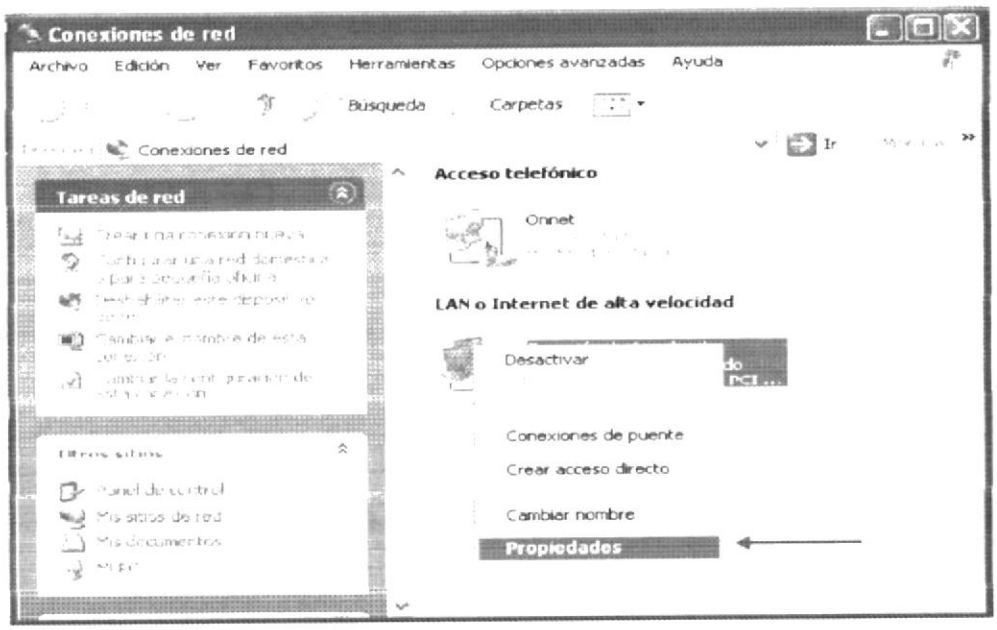


Figura 6-228: Propiedades de Conexiones de Red

En esta ventana escoger a la opción TCP/IP para configurar la tarjeta de red.

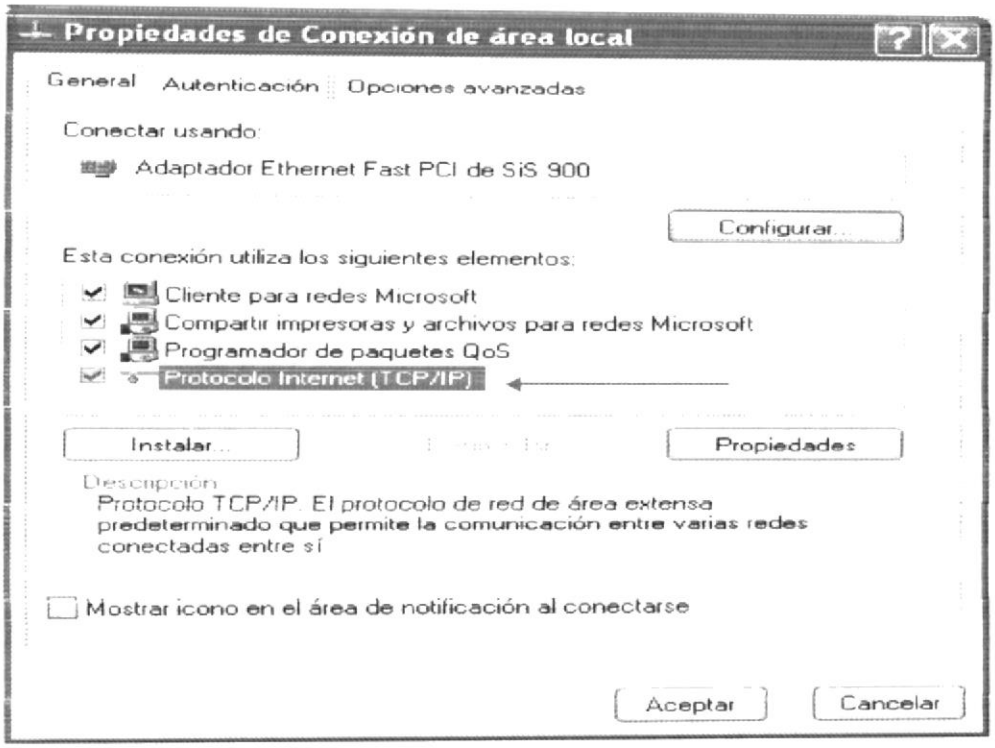


Figura 6-229: Protocolo Internet Tcp/Ip

ESPOL
BIBLIOTECA
CAMPUS

Una vez realizado el proceso, configure la tarjeta de red de manera automática y luego presiones OK.

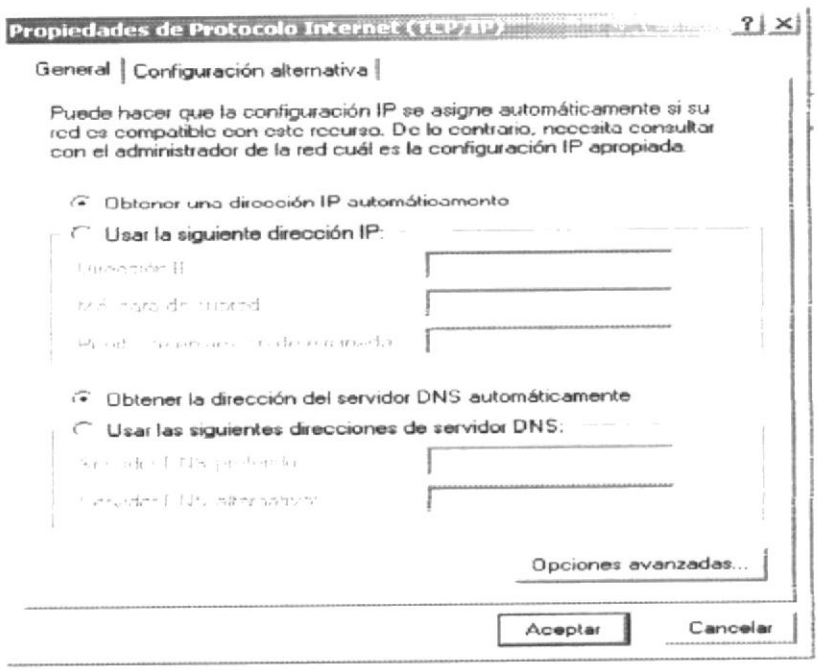


Figura 6-230: Obtener Dirección IP Automáticamente

A continuación la red de área local comenzará a buscar una ip.

Ahora comprobar si ya se configuró la tarjeta de red por dhcp:
Inicio
Ejecutar
Digitar: cmd →→→ para entrar a la consola ms-dos
Y con el comando: ipconfig →→→ aparecerá la ip que se le asigno por medio de dhcp

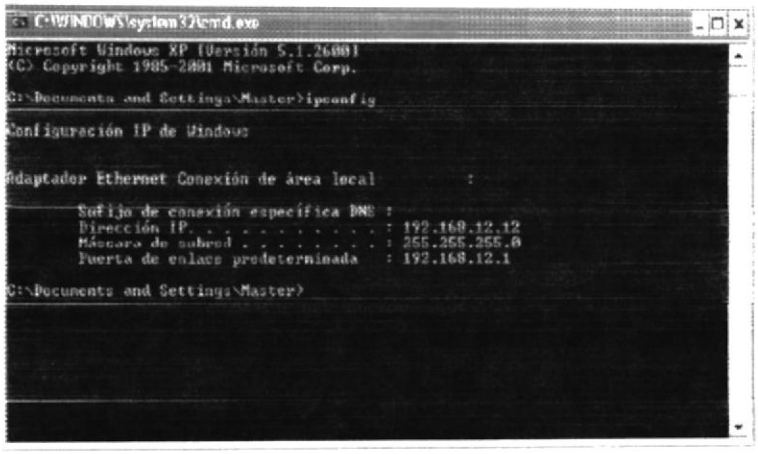
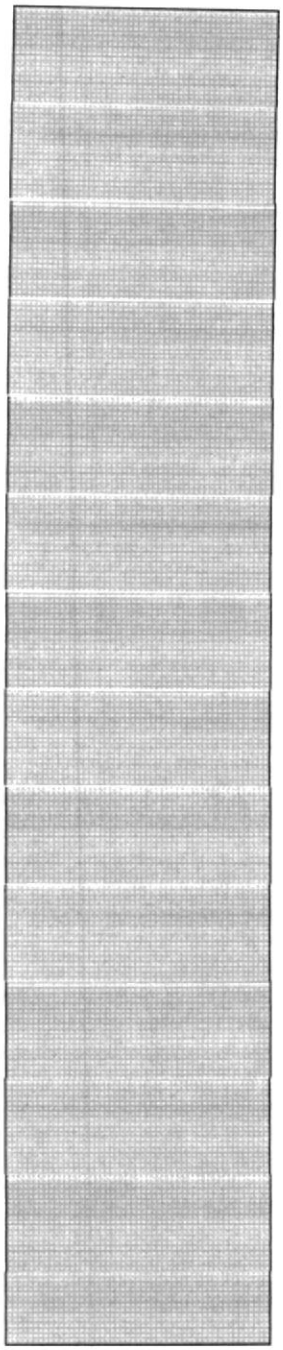


Figura 6-231: Verificación de Dirección Asignada Automáticamente



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 7

ROUTER

7.1 INTRODUCCIÓN DE ROUTER

Enrutador, encaminador. Dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red) del modelo OSI.

El router interconecta segmentos de red, o algunas veces hasta redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

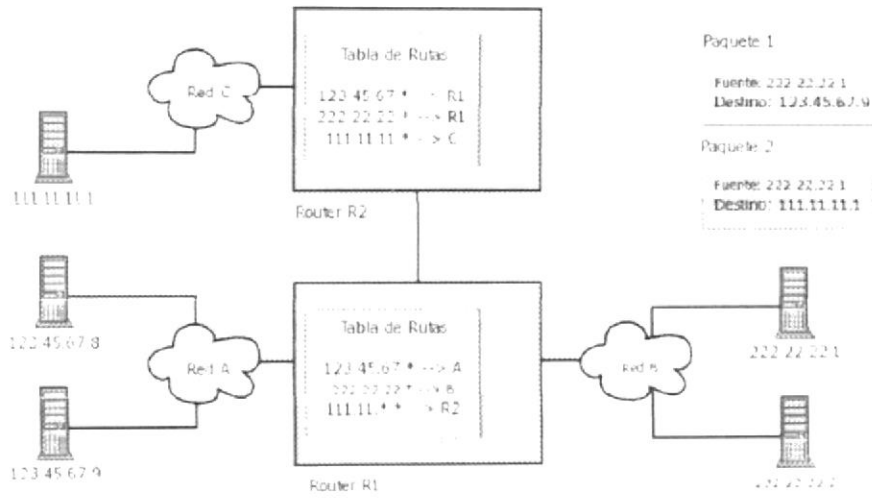


Figura 7-1: Introducción A Router.

En el ejemplo del diagrama, se muestran 3 redes IP interconectadas por 2 router. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configurados previamente, los router pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete.

Los broadcast, o difusiones, se producen cuando una fuente envía datos a todos los dispositivos de una red.

En el caso del protocolo IP, una dirección de broadcast es una dirección compuesta exclusivamente por números unos (1) en el campo del host (para la dirección ip en formato binario de modo que para una máscara de red 255.255.255.0 la dirección de broadcast para la dirección 192.168.0.1 seria la 192.168.0.255.

Los protocolos de enrutamiento son aquellos protocolos que utilizan los router o encaminadores para comunicarse entre sí y compartir información que les permita tomar la decisión de cual es la ruta más adecuada en cada momento para enviar un paquete.

Los protocolos más usados son RIP (v1 y v2), OSPF (v1, v2 y v3), y BGP (v4), que se encargan de gestionar las rutas de una forma dinámica, aunque no es estrictamente necesario que un router haga uso de estos protocolos, pudiéndosele indicar de forma estática las rutas (caminos a seguir) para las distintas subredes que estén conectadas al dispositivo.

Comúnmente los router se implementan también como puertas de acceso a Internet (por ejemplo un router ADSL), usándose normalmente en casas y oficinas pequeñas. Es correcto utilizar el término router en este caso, ya que estos dispositivos unen dos redes (una red de área local con Internet).

VISTA FRONTAL DEL ROUTER

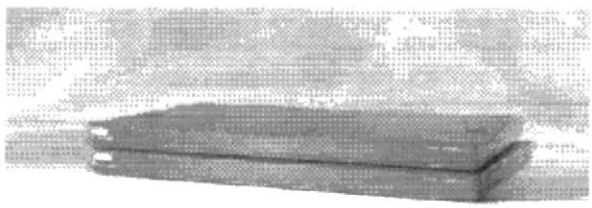
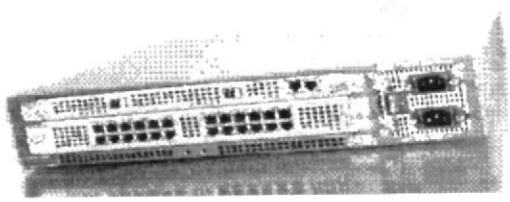


Figura 7-2: Vista frontal del Router.

VISTA POSTERIOR DEL ROUTER



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 7-3: Vista Posterior del Router.

7.1.1 VENTAJAS DE LOS ROUTERS

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

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

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

7.1.2 DESVENTAJAS DE LOS ROUTERS

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

7.2 ESTRUCTURA DEL ROUTER

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.

ESPOL BIBLIOTECA CAMPUS PENAS

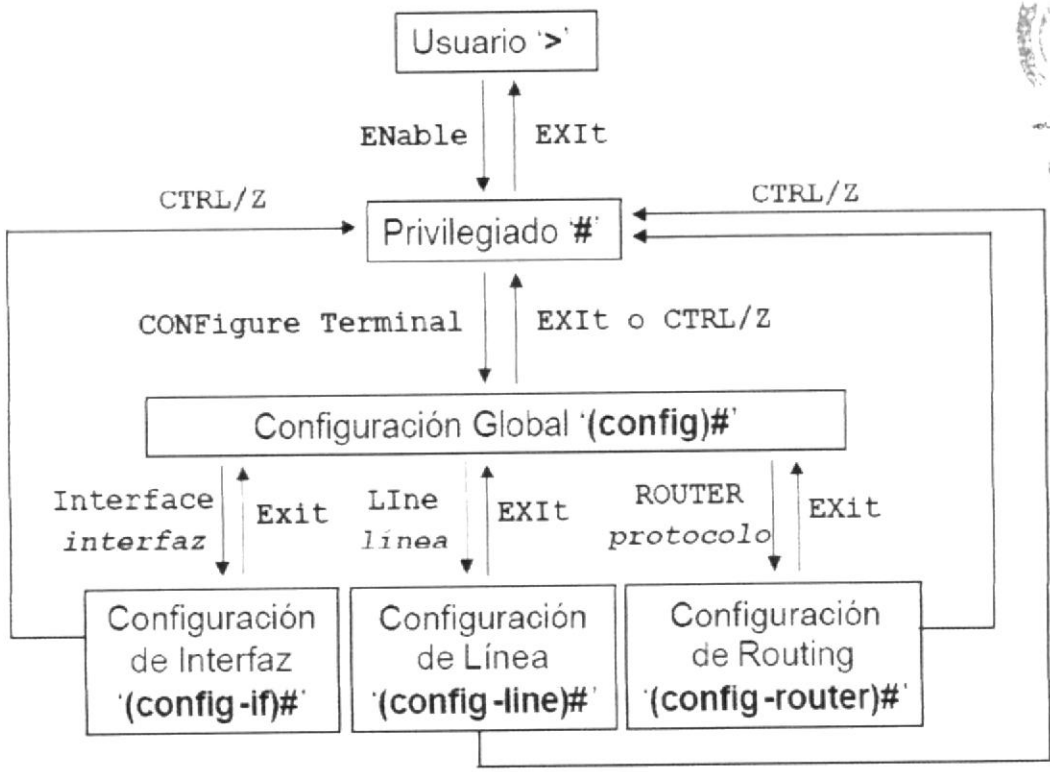


Figura 7-4: Estructura del Router.

7.3 LOS COMPONENTES BÁSICOS DE LA ARQUITECTURA INTERNA DE UN ROUTER

- **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 router, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más Módulos de memoria en línea doble (DIMM).

- **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.

- **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.

ESPC
BIBLIOTE
AMPUS
PEÑAS

- **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. El CPU usa el bus para tener acceso a los componentes desde el almacenamiento del router. Este bus transfiere las instrucciones y los datos hacia o desde las direcciones de memoria especificadas.

- **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.

- **INTERFACES:** Las interfaces son las conexiones de los router con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring. Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser configuraciones fijas o modulares.

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

  Los puertos de Consola/AUX son puertos seriales que se utilizan principalmente para la configuración inicial del router. Estos puertos no son puertos de networking. Se usan para realizar sesiones terminales desde los puertos de comunicación del computador o a través de un módem.

- **Fuente de alimentación:** La fuente de alimentación brinda la energía necesaria para operar los componentes internos. Los router de mayor tamaño pueden contar con varias fuentes de alimentación o fuentes modulares. En algunos de los router de menor tamaño, la fuente de alimentación puede ser externa al router.

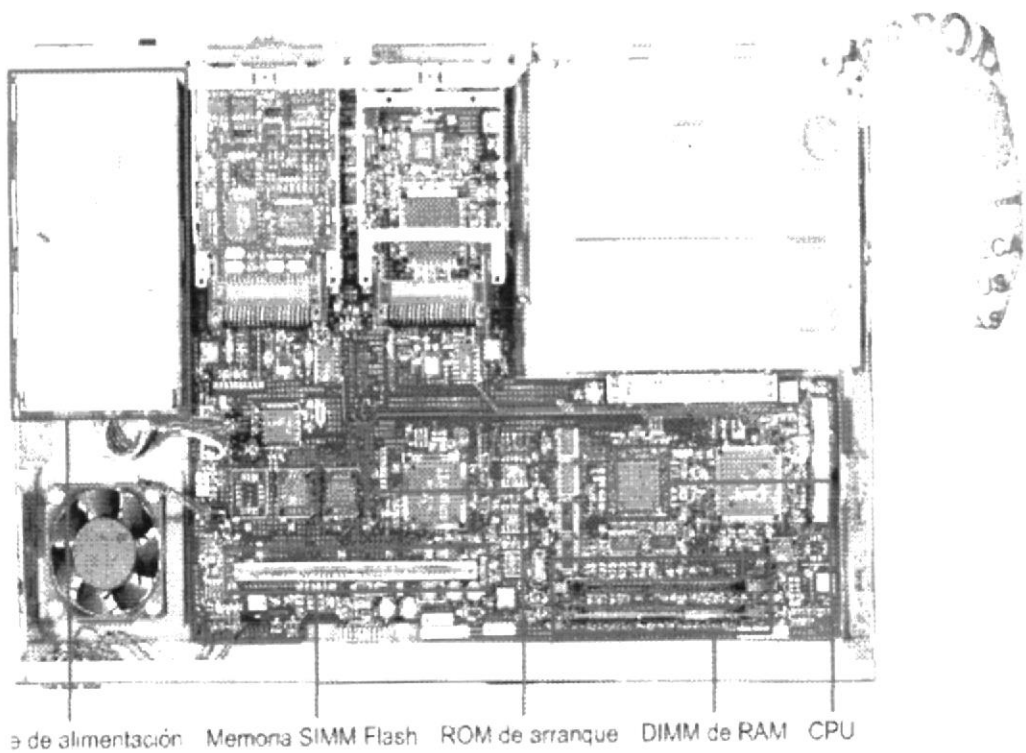
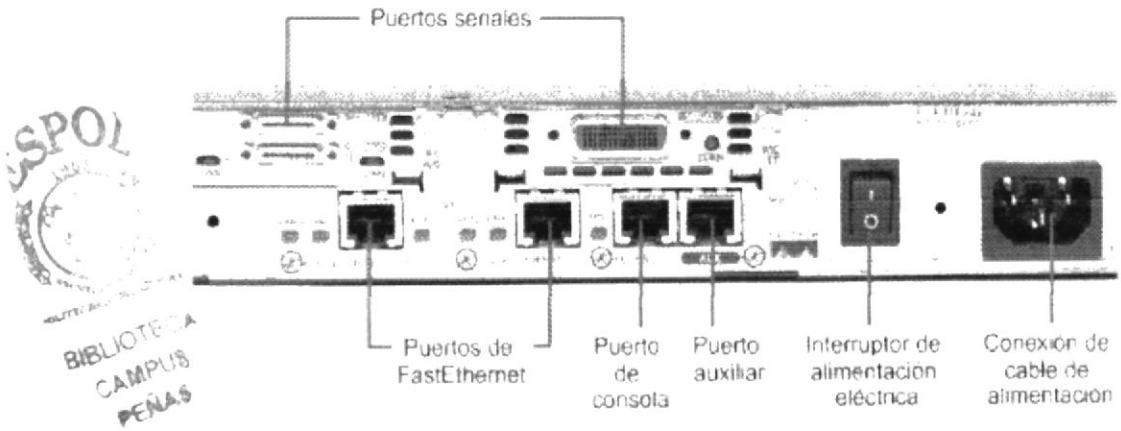


Figura 7-5: Componentes Básicos de un Router.

7.4 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.



ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 7-6: Conexiones Externas del Router.

7.5 CONEXIONES DEL PUERTO DE ADMINISTRACIÓN

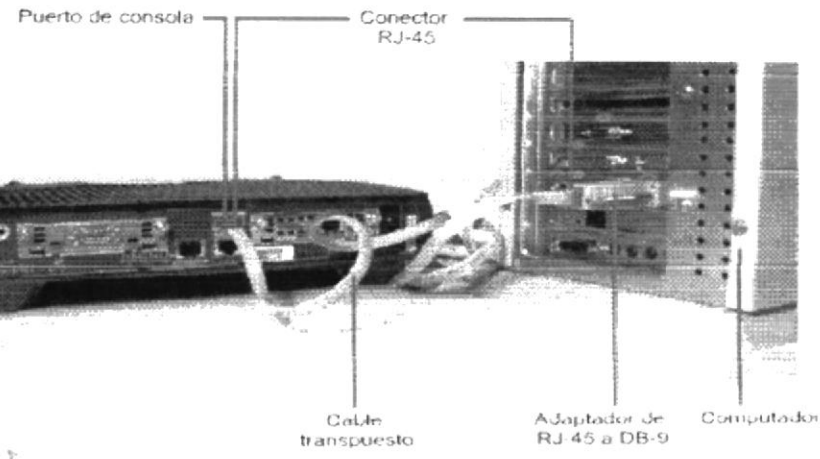
El puerto de consola y el puerto auxiliar (AUX) son puertos de administración. Estos puertos seriales asíncronos no se diseñaron como puertos de networking. Uno de estos dos puertos es necesario para la configuración inicial del router. Se recomienda el puerto de consola para esta configuración inicial. No todos los router 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**.



ESPOL BIBLIOTECA CAMPUS PENAS

Figura 7-7: Conexión al Puerto de Administración.

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 accesando remotamente.

7.6 MEDIOS DE COMUNICACIÓN A USAR

7.6.1 CABLE DTE

Un DTE, por sus siglas en ingles Data Terminal Equipment, se encarga de receptar datos. En otras palabras se considera al DTE al Usuario Final.

Como característica principal este medio de comunicación DTE en uno de sus extremos tiene pines, por lo que es llamado "macho".



Figura 7-8: Cable Dtc.

7.6.2 CABLE DCE

Un DCE, por sus siglas en ingles Data Circuit Equipment, es el originado o proveedor de datos. Como características principales este medio de comunicación DCE en uno de sus extremos tiene hoyitos listos para recibir los pines del cable DTE, por lo que es llamado "hembra".



Figura 7-9: Cable Dce.

7.6.3 CABLE UTP (CAT 5E)

Es el cable más usado y provee una infraestructura a través de la cual la mayoría de los productos pueden ser conectados.

El diseño de un Sistema de cableado UTP tiene una configuración de estrella, están conectados a un Patch Panel Central y los HUB's o Switch son utilizados para conectar a un servicio. Para la conexión entre el Gabinete y la roseta de conexión el largo máximo aceptado es de 100 metros.

El cable consiste en 4 pares torcidos y existen 5 categorías siendo las tres más importantes (3, 4 y 5) utilizadas en transmisión de datos. El cable Categoría 5 soporta transmisión de datos hasta 100 Megabytes por segundo.



Figura 7-10: Cable UTP (CAT 5E).

BIBLIOTECA
CAMPUS
PEÑAS

7.6.4 CONECTOR RJ45

El conector RJ-45, es similar al telefónico, pero algo más grande y con capacidad para ocho contactos o hilos.

El conector RJ-45, debe existir en cada extremo del cable de par trenzado. Para conectar el cable a la tarjeta, colocar el conector de forma que la patilla de plástico quede en línea con la ranura de la hembra y empuje el conector hasta escuchar un clic (el conector es similar al enchufe de plástico que se utiliza para conectar un cordón telefónico con un enchufe telefónico de pared).

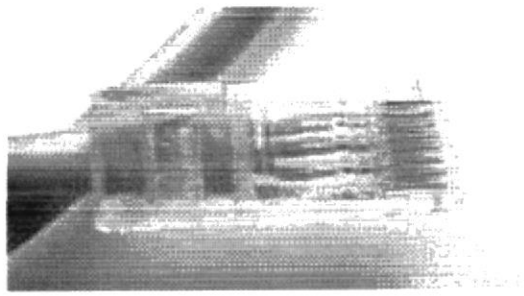


Figura 7-11: Conector RJ 45.

7.6.5 PUERTO SERIAL (CONECTOR COM)

El puerto serie usa conectores tipo D-9.Estos puertos hacen transferencia de datos en serie; o sea comunican la información de un bit en una línea. Estos puertos son compatibles con dispositivos como módems externos y los mouse.

La mayoría de los software utilizan el término COM (derivado de comunicaciones) seguido de un número para designar un puerto serie (por ejemplo, COM1 ó COM2).





Figura 7-12: Puerto Serial.

7.7 ENRUTAMIENTO

7.7.1 ENRUTAMIENTO ESTÁTICO

Las operaciones con rutas estáticas pueden dividirse en tres partes:

1. El administrador de red configura la ruta.
2. El router instala la ruta en la tabla de enrutamiento.
3. 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.

7.7.2 ENRUTAMIENTO DINÁMICO

7.7.2.1 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.

7.8 TIPOS DE PROTOCOLO

7.8.1 PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP)

RIP son las siglas de Routing Information Protocol (Protocolo de información de enrutamiento)

Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los router (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

7.8.1.1 VERSIONES RIP

En la actualidad existen tres versiones diferentes de RIP las cuales son:

- **RIPv1:** No soporta subredes ni CIDR. Tampoco incluye ningún mecanismo de autentificación de los mensajes. No se usa actualmente. Su especificación está recogida en el RFC 1058.
- **RIPv2:** Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, autentificación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). Su especificación está recogida en el RFC 1723-2453.



- **RIPng:** 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.

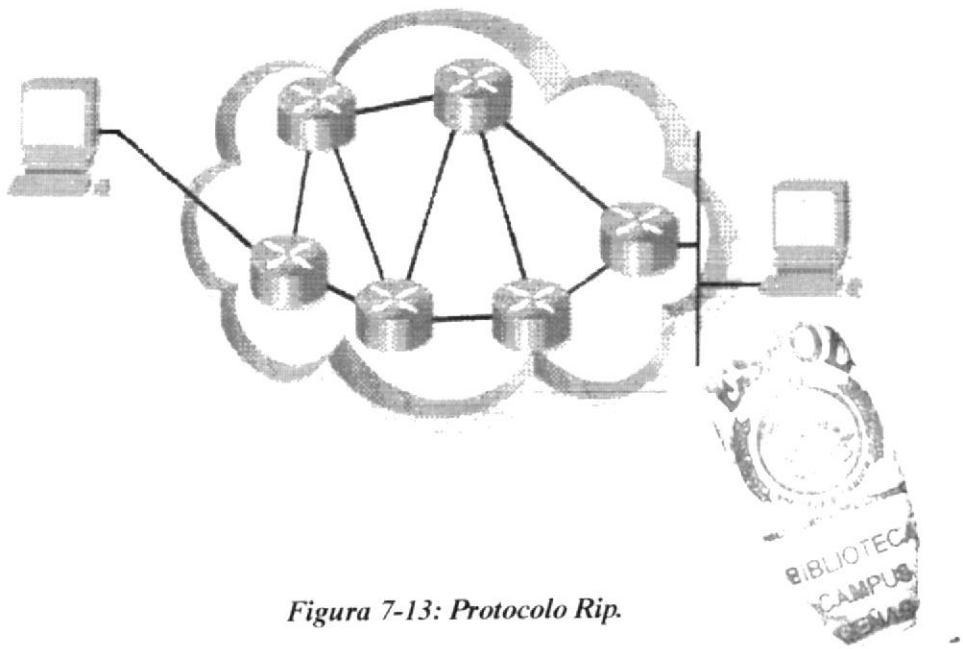


Figura 7-13: Protocolo Rip.

7.8.1.2 FUNCIONAMIENTO RIP

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

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

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

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

La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino. Teniendo en cuenta el límite de 15 saltos mencionado anteriormente.

Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del Enrutador que anunció esa ruta.

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

7.8.1.3 VENTAJAS Y DESVENTAJAS

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

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.



7.8.1.4 MENSAJES RIP

7.8.1.4.1 TIPOS DE MENSAJES RIP

Los mensajes RIP pueden ser de dos tipos.

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

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

- **Mensajes ordinarios:** Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos.
  Mensajes enviados como respuesta a mensajes de petición.
  Mensajes enviados cuando cambia algún coste. Sólo se envían las rutas que han cambiado.

7.8.1.4.2 FORMATO DE LOS MENSAJES RIP

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

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

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

Otros protocolos de enrutamiento:

- **IGRP**
- **EIGRP**
- **OSPF**

7.8.2 PROTOCOLO DE INTERIOR DE GATEWAY (IGRP)

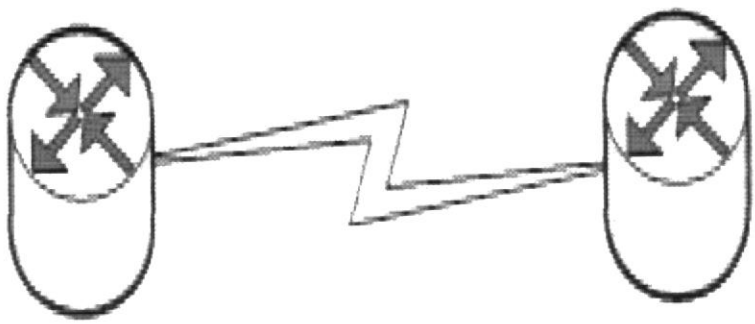
(***Interior Gateway Routing Protocol***, o *Protocolo de enrutamiento de gateway interior*) es un protocolo patentado y desarrollado por CISCO que se emplea con el protocolo TCP/IP según el modelo (OSI) Internet.

La versión original del IP fue diseñada y desplegada con éxito en 1986. Se utiliza comúnmente como IGP pero también se ha utilizado extensivamente como Exterior Gateway Protocol (EGP) para el enrutamiento inter-dominio.

IGRP es un protocolo de enrutamiento basado en la tecnología vector-distancia. Utiliza una métrica compuesta para determinar la mejor ruta basándose en el ancho de banda, el retardo, la confiabilidad y la carga del enlace.

El concepto es que cada router no necesita saber todas las relaciones de ruta/enlace para la red entera. Cada router publica destinos con una distancia correspondiente. Cada router que recibe la información, ajusta la distancia y la propaga a los router vecinos.

La información de la distancia en IGRP se manifiesta de acuerdo a la métrica. Esto permite configurar adecuadamente el equipo para alcanzar las trayectorias más óptimas.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 7-14: Protocolo IGRP.

7.8.3 EIGRP

EIGRP es un protocolo de encaminamiento híbrido, propietario de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Sin embargo, EIGRP es más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP.

Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP.

EIGRP al igual que IGRP usa el siguiente cálculo de métrica:

Métrica= [K1 * ancho de banda + ((K2 * ancho de banda)/ (256-carga))+ (K3 * retardo)]*[K5/ (confiabilidad + K4)]. (Nota: Debido a que EIGRP utiliza un campo de métrica de 32 bits, a diferencia de IGRP que es de 24, multiplica este valor por 256).

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

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

EIGRP mantiene las siguientes tablas:



7.8.3.1 TABLA DE VECINOS

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

7.8.3.2 TABLA DE TOPOLOGÍA

La tabla de topología se compone de todas las tablas de encaminamiento EIGRP recibidas de los vecinos. EIGRP toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino.

EIGRP rastrea esta información para que los router EIGRP puedan identificar y conmutar a rutas alternativas rápidamente. La información que el router recibe de los vecinos se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor.

Esta información también se introduce a la tabla de topología. Los router EIGRP mantienen una tabla de topología por cada protocolo configurado de red (como IP, IPv6 o IPX). La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

7.8.3.3 TABLA DE ENCAMINAMIENTO

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

A continuación se muestran los campos que conforman la tabla de encaminamiento:

- **Distancia factible (FD):** Ésta es la métrica calculada más baja hacia cada destino. Por ejemplo, la distancia factible a 32.0.0.0 es 2195456. La distancia de la ruta que está en la tabla de encaminamiento.

- **Origen de la ruta:** Número de identificación del router que publicó esa ruta en primer lugar. Este campo se llena sólo para las rutas que se aprenden de una fuente externa a la red EIGRP. El rotulado de rutas puede resultar particularmente útil con el encaminamiento basado en políticas. Por ejemplo, el origen de la ruta a 32.0.0.0 es 200.10.10.10.

- **Distancia informada (RD):** La distancia informada (RD) de la ruta es la distancia informada por un vecino adyacente hacia un destino específico. Por ejemplo, la distancia informada a 32.0.0.0 por el vecino 200.10.10.10 es 281600 tal como lo indica (2195456/281600).

- **Información de interfaz:** La interfaz a través de la cual se puede alcanzar el destino.

- **Estado de ruta:** El estado de una ruta. Una ruta se puede identificar como pasiva, lo que significa que la ruta es estable y está lista para usar, o activa, lo que significa que la ruta se encuentra en el proceso de recálculo por parte de DUAL.

7.8.3.4 PROTOCOLOS QUE UTILIZA EIGRP



Uno de los Protocolos que utiliza EIGRP es el Protocolo de Transporte Confiable (RTP, no confundir con el Real-time Transport Protocol), que es un protocolo de capa de transporte que garantiza la entrega ordenada de paquetes EIGRP a todos los vecinos.

En una red IP, los hosts usan TCP para secuenciar los paquetes y asegurarse de que se entreguen de manera oportuna. Sin embargo, EIGRP es independiente de los protocolos.

Esto significa que no se basa en TCP/IP para intercambiar información de encaminamiento de la forma en que lo hacen RIP, IGRP y OSPF. Para mantenerse independiente de IP, EIGRP usa RTP como su protocolo de capa de transporte propietario para garantizar la entrega de información de encaminamiento. EIGRP puede hacer una llamada a RTP para que proporcione un servicio confiable o no confiable, según lo requiera la situación.

Por ejemplo, los paquetes hello no requieren el gasto de la entrega confiable porque se envían con frecuencia y se deben mantener pequeños. La entrega confiable de otra información de encaminamiento puede realmente acelerar la convergencia porque entonces los routers EIGRP no tienen que esperar a que un temporizador expire antes de retransmitir.

Con RTP, EIGRP puede realizar envíos en multicast y en unicast a diferentes pares de forma simultánea. Esto maximiza la eficiencia.

Cuando un router detecta que un vecino no está disponible, intenta encontrar rutas alternativas para todas aquellas que en la tabla de encaminamiento están dirigidas a ese vecino.

El heurístico que se emplea para saber si utilizar una ruta de un vecino o no es comparar la distancia factible de la ruta (la que tenía el router antes de perder la conectividad con el vecino) con la distancia informada por cada vecino alternativo.

Si un vecino alternativo tiene una distancia informada menor que la distancia factible, significa que está más cerca que el router que calcula del destino y por tanto no puede dar origen a un bucle porque no puede volver al router que recalcula. En este caso se puede usar como encaminamiento alternativo.

Si un vecino tiene una distancia informada mayor que la factible, es posible que su camino hacia el destino pase por el router que hace el recálculo, por lo que no es conveniente utilizarla ya que hay la posibilidad de que de lugar a un bucle de encaminamiento

Cuando no se encuentra un camino alternativo con la información disponible localmente (en terminología EIGRP, no se encuentra un sucesor factible), se desencadena el algoritmo DUAL (Diffusing Update ALgorithm), que es el proceso de búsqueda de rutas alternativas de EIGRP.

El proceso simplificado funciona de la siguiente manera:
El router que ha detectado la caída marca la ruta como parte del proceso de recálculo (la marca como activa, o perteneciente a un proceso de activo de recálculo, como opuesto al proceso pasivo de recibir las tablas de encaminamiento de los vecinos, el proceso estándar). A continuación, pregunta a todos sus vecinos (menos al que está caído) por una ruta alternativa para llegar a ese destino.



BIBLIOT
CAMPU
PEÑAS

Cada vecino que recibe una pregunta por una ruta, mira en su tabla de encaminamiento si tiene alguna ruta para llegar a ese destino que no sea el vecino que pregunta. Si la encuentra, contesta al vecino con ese dato y el proceso se acaba.

Si no la encuentra, marca a su vez la ruta como activa y pregunta a su vez a todos los vecinos menos el que originó la pregunta por una ruta alternativa. Si no tiene vecinos, responde que no encuentra una ruta. Así, la pregunta se va difundiendo (lo que da origen al nombre del algoritmo) por toda la parte de la red que sigue accesible, hasta que se encuentra una ruta alternativa o se determina que la ruta no está accesible porque todos los vecinos responden negativamente.

Una de las mejores características de EIGRP es su diseño modular. Se ha demostrado que los diseños modulares o en capas son los más escalables y adaptables. EIRGP logra la compatibilidad con los protocolos enrutados, como IP, IPX y AppleTalk, mediante los PDM.

En teoría, EIGRP puede agregar PDM para adaptarse fácilmente a los protocolos enrutados nuevos o revisados como IPv6. Cada PDM es responsable de todas las funciones relacionadas con su protocolo encaminado específico.

El módulo IP-EIGRP es responsable de las siguientes funciones:

- Enviar y recibir paquetes EIGRP que contengan datos IP.
- Avisar a DUAL una vez que se recibe la nueva información de encaminamiento IP.
- Mantener de los resultados de las decisiones de encaminamiento DUAL en la tabla de encaminamiento IP.
- Redistribuir la información de encaminamiento que se aprendió de otros protocolos de encaminamiento capacitados para IP

7.8.4 OSPF

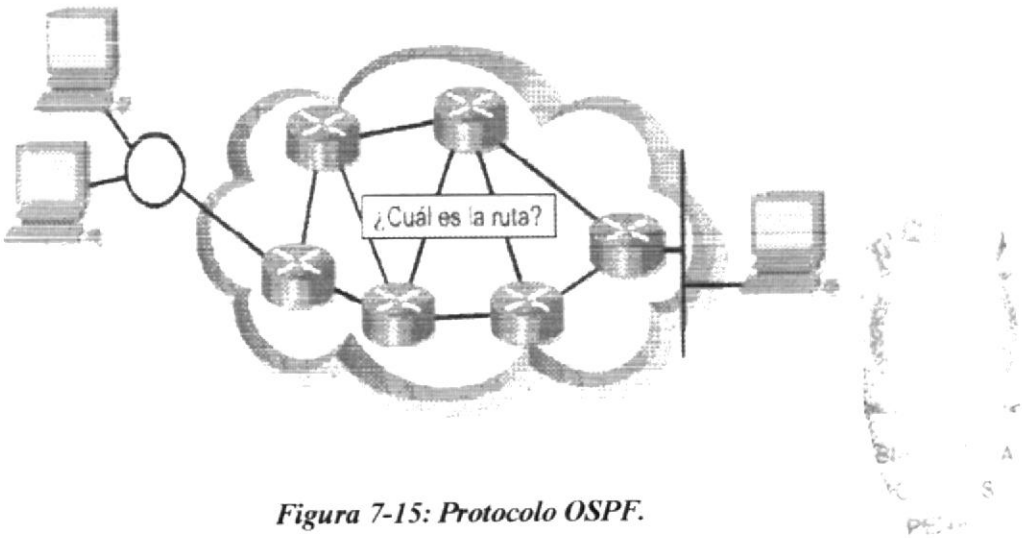


Figura 7-15: Protocolo OSPF.

Open Shortest Path First (frecuentemente abreviado OSPF).

Es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado idéntica en todos los encaminadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en redes grandes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.

Como sucesor natural a RIP, es VLSM o sin clases desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que también soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas.

OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas. Una red OSPF se puede descomponer en redes más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red y donde hay otras áreas conectadas a ella.

Las rutas entre diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

Los encaminadores en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. Los encaminadores eligen a un encaminador designado' (DR) y un encaminador designado secundario (BDR) que actúan como hubs para reducir el tráfico entre los diferentes encaminadores. OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado.

Las direcciones de multidifusiones usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa IP directamente, mediante el IP protocolo 89.

7.8.4.1 TIPOS DE ÁREA

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

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.8.4.1.1 ÁREA BACKBONE

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

7.8.4.1.1 ÁREA STUB

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

7.8.4.1.2 ÁREA NOT-SO-STUBBY

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

7.8.4.1.3 ESTADOS DE OSPF

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

7.8.4.1.4 ESTADO DESACTIVADO (DOWN STATE)

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

7.8.4.1.5 ESTADO DE INICIALIZACIÓN (INIT STATE)

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

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

7.8.4.1.6 ESTADO DE DOS-VÍAS (TWO-WAY)

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

ESPOL
BIBLIOTECA CAMPUS PEÑAS

El estado de Dos-Vías es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos.

Para aprender los estados de enlace de otros encaminadores y eventualmente construir una tabla de encaminamiento, cada encaminador OSPF debe formar a lo menos una adyacencia.

Una adyacencia es una relación avanzada entre encaminadores OSPF que involucra una serie de estados progresivos que se basa no tan solo en paquetes Hello, si no que otros 4 paquetes OSPF.

Aquellos encaminadores intentando volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.

7.8.4.1.7 ESTADO EXSTART

Técnicamente, cuando un encaminador y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs.

Los dos encaminadores vecinos emplean paquetes Hello para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos.

Aquel encaminador con el mayor router ID "gana" y se convierte en el maestro.

Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.

7.9 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.

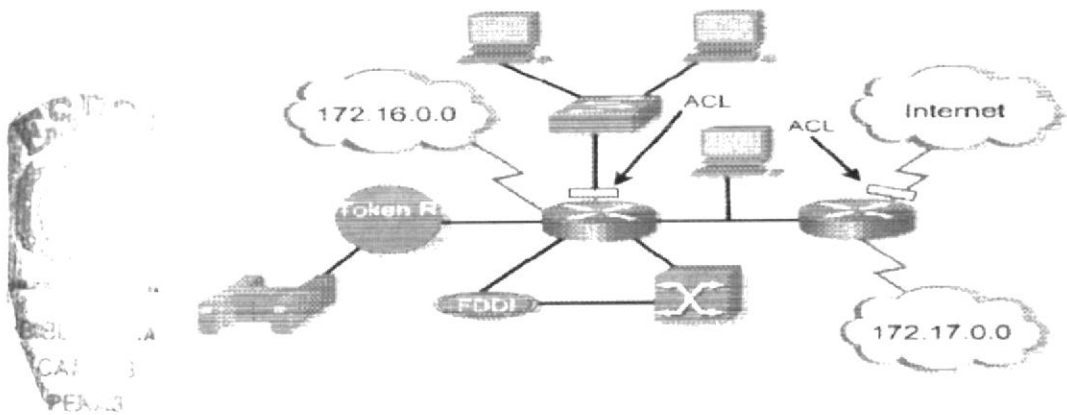


Figura 7-16: Listas de Control de Acceso.

7.9.1 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.

7.9.2 CREACIÓN DE LAS ACL

Las ACL se crean en el modo de configuración global. Existen varias clases diferentes de ACL`s: estándar, extendidas, IPX, AppleTalk, entre otras.

Cuando configura las ACL en el router, cada ACL debe identificarse de forma única, asignándole un número.

Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista.

Protocolo	Intervalo
IP	1-99, 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



Figura 7-17: Creación de ACL.

7.9.3 PROPÓSITO DE LAS ACL

Las ACL permiten un control del tráfico de red, a nivel de los routers. Pueden ser parte de una solución de seguridad (junton con otros componentes, como antivirus, anti-espías, firewall, proxy, etc.).

7.9.4 PUNTOS VARIOS, QUE SE DEBEN RECORDAR

- Una ACL es una lista de una o más instrucciones.
- Se asigna una lista a una o más interfaces.
- Cada instrucción permite o rechaza tráfico, usando uno o más de los siguientes criterios: el origen del tráfico; el destino del tráfico; el protocolo usado.
- El router analiza cada paquete, comparándolo con la ACL correspondiente.
- El router compara la ACL línea por línea. Si encuentra una coincidencia, toma la acción correspondiente (aceptar o rechazar), y ya no revisa los restantes renglones.
- Es por eso que hay que listar los comandos desde los casos más específicos, hasta los más generales. ¡Las excepciones tienen que estar antes de la regla general!
- Si no encuentra una coincidencia en ninguno de los renglones, rechaza automáticamente el tráfico. Consideren que hay un "deny any" implícito, al final de cada ACL.
- Cualquier línea agregada a una ACL se agrega al final. Para cualquier otro tipo de modificación, se tiene que borrar toda la lista y escribirla de nuevo. Se recomienda copiar al Bloc de Notas y editar allí.
- Las ACL estándar (1-99) sólo permiten controlar en base a la dirección de origen.
- Las ACL extendidas (100-199) permiten controlar el tráfico en base a la dirección de origen; la dirección de destino; y el protocolo utilizado.
- También se pueden usar ACL nombradas en vez de usar un rango de números. El darles un nombre facilita entender la configuración (y por lo tanto, también facilita hacer correcciones). No trataré las listas nombradas en este resumen.
- Si se considera sólo el tráfico de tipo TCP/IP, para cada interface puede haber sólo una ACL para tráfico entrante, y una ACL para tráfico saliente.

Sugerencia para el examen: Se deben conocer los rangos de números de las ACL, incluso para protocolos que normalmente no nos interesan.

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.9.5 WILDCARDS

- "Wildcard" significa "comodín", como el joker en el juego de naipes.
- Tanto en la dirección de origen, como (en el caso de las ACL extendidas) en la dirección de destino, se especifican las direcciones como dos grupos de números: un número IP, y una máscara wildcard.
- Si se traduce a binario, los "1" en la máscara wildcard significan que en la dirección IP correspondiente puede ir cualquier valor.
- Para permitir o denegar una red o subred, la máscara wildcard es igual a la máscara de subred, cambiando los "0" por "1" y los "1" por "0" (en binario).

- Sin embargo, las máscaras wildcard también permiten más; por ejemplo, se pueden denegar todas las máquinas con números IP impares, o permitir el rango de IP 1-31, en varias subredes a la vez.

Ejemplos:

- Permitir o denegar un IP específico: **172.16.0.1 0.0.0.0**. Se puede abreviar como **host 172.16.0.1**.
- Permitir o denegar una subred: **172.16.0.0 0.0.0.255**. (El ejemplo corresponde a una subred /24, es decir, máscara de subred = 255.255.255.0.)
- Permitir o denegar a todos: **0.0.0.0 255.255.255.255**. Se puede abreviar como **any**.

7.9.6 COLOCACIÓN DE LAS ACL

- Las ACL estándar se colocan cerca del destino del tráfico. Esto se debe a sus limitaciones: no se puede distinguir el destino.
- Las ACL extendidas se colocan cerca del origen del tráfico, por eficiencia - es decir, para evitar tráfico innecesario en el resto de la red.

7.9.7 DIRECCIÓN DEL TRÁFICO

El tema "in" vs. "out" suele causar confusiones, por eso es conveniente la siguiente explicación.

La dirección in u out (entrada o salida) se refiere al router que están configurando en ese momento. Por ejemplo, con la siguiente configuración de routers (A, B, C son routers; X, Y son hosts (o redes)):

X ------ A ------ B ------ C ------- Y

Se puede controlar el tráfico de X a Y en el router A, B o C.



Por ejemplo, el en router A, se puede controlar el tráfico entrante (in), en la interface que está a su izquierda. En el mismo router, también es posible controlar el tráfico saliente (out), en la interface que está a su derecha.

De la misma manera, se puede controlar el tráfico en el router B: entrante, a la izquierda; o saliente, por la derecha; o de igual manera en el router C.

(Lo más recomendable en este caso es usar una lista extendida, en el router A, y aplicarla a la interface a su izquierda, dirección "in" - entrante.).También se debe recordar que normalmente el tráfico fluye en dos direcciones. Por ejemplo, si "Y" es un servidor Web, teóricamente, en el router C, interface a la derecha, se podría bloquear la solicitud al servidor (out), o también la respuesta del servidor (in).

7.9.8 ACL ESTÁNDAR

Sintaxis para un renglón (se escribe en el modo de configuración global):

access-list (número) (deny | permit) (ip origen) (wildcard origen)

Ejemplo: Bloquear toda la subred 172.17.3.0/24, excepto la máquina 172.17.3.10.

```
access-list 1 permit host 172.17.3.10
access-list 1 deny 172.17.3.0 0.0.0.255
access-list 1 permit any
```

Para asignarlo a una interface:

interface F0

ip access-group 1 out



7.9.9 ACL EXTENDIDAS

Sintaxis para cada renglón:

access-list (número) (deny | permit) (protocolo) (IP origen) (wildcard origen) (IP destino) (wildcard destino)
[(operador) (operando)]

El "protocolo" puede ser (entre otros) IP (todo tráfico de tipo TCP/IP), TCP, UDP, ICMP.

El "operando" puede ser un número de puerto (por ejemplo 21), o una sigla conocida, por ejemplo, "ftp".

Ejemplo 1:

Repetir el ejemplo de la ACL estándar, pero se especifica que se quiere permitir o denegar el tráfico con destino al servidor, que está en 172.16.0.1:

```
access-list 101 permit ip host 172.17.3.10 host 172.16.0.1
access-list 101 deny ip 172.17.3.0 0.0.0.255 host 172.16.0.1
access-list 101 permit ip any any
```

Ejemplo 2:

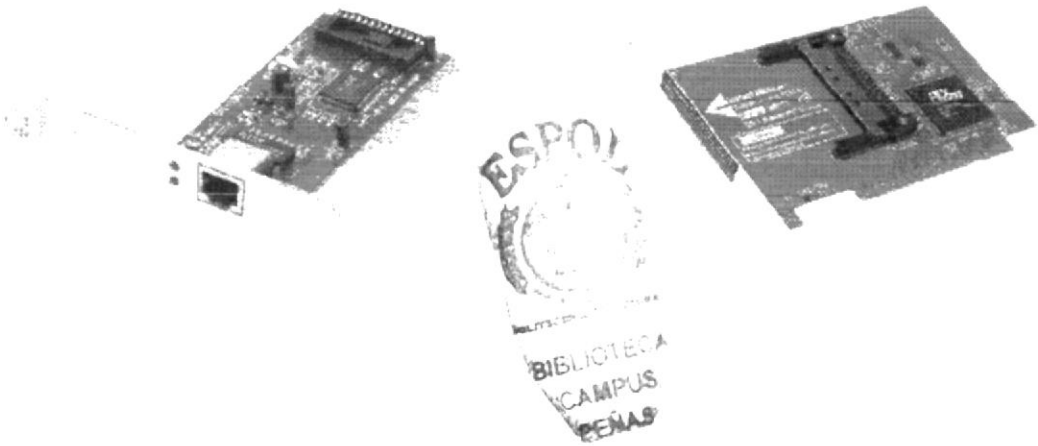
Permitir tráfico HTTP y "ping" (ICMP) al servidor 172.16.0.1, para todos. Denegar todo lo demás.

```
access-list 102 permit icmp any host 172.16.0.1
access-list 102 permit tcp any host 172.16.0.1 eq www.
```

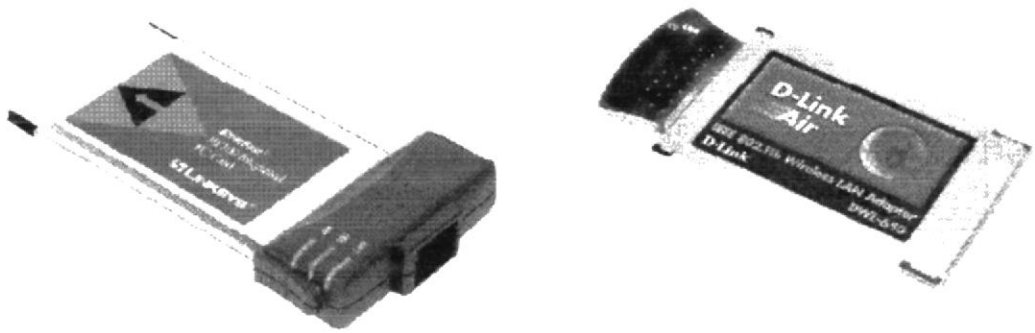
7.10 SWITCH

Un switch (en castellano "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 Interconection).

Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.En esta capa además se encuentran las NIC (Netwok Interface Card; Placa de Red) pueden ser inalámbricas y los Bridges (Puentes).


ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Comunes (PCI) Para conexión con medios fisicos (cables) e inalámbricas.



Placas para puerto PMCIA (Para computadoras portátiles), para medios fisicos e inalámbricos

La capa 2 del modelo de referencia OSI es la capa de Enlace de datos, esta capa proporciona un tránsito de datos confiable a través de un enlace fisico.

Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento fisico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de trama de control de flujo.

Un switch, al igual que un puente, es un dispositivo de la capa 2. De hecho, el switch se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto.

La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión.

Como los switches son capaces de tomar decisiones, así hacen que la LAN sea mucho más eficiente. Los switches hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente.

A diferencia de esto, el hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos.

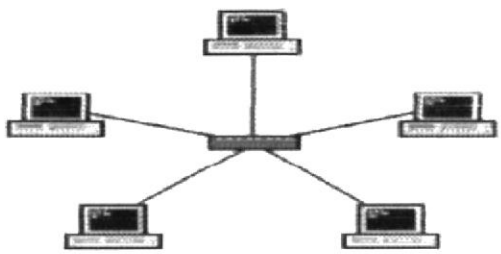
Esto hace que la LAN sea más lenta.

A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión (pueden ser de 8, 12, 24 o 48, o conectando 2 de 24 en serie), dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red).

La diferencia entre un hub y un switch está dada por lo que sucede dentro de cada dispositivo.

El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto.

El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total. Básicamente un Switch es un administrador inteligente del ancho de banda.



BIBLIOTECA CAMPUS PEÑAS

Figura 7-18: Red Estrella.

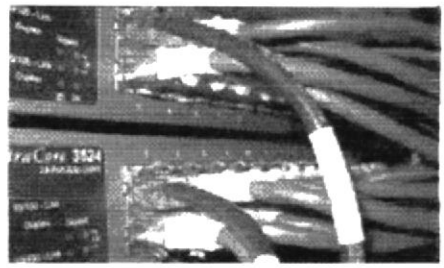
Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un *filtro* en la red, mejoran el rendimiento y la seguridad de las LANs (*Local Area Network*- Red de Área Local).

7.10.1 INTERCONEXIÓN DE CONMUTADORES Y PUENTES

Los puentes (bridges) y conmutadores (switches) pueden ser conectados unos a los otros, pero existe una regla que dice que sólo puede existir **un único camino** entre dos puntos de la red. En caso de que no se siga esta regla, se forma un bucle en la red, que produce la transmisión infinita de datagramas de una red a otra.

Sin embargo, esos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

7.10.2 INTRODUCCIÓN AL FUNCIONAMIENTO DE LOS CONMUTADORES



ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 7-19: Funcionamiento de los Conmutadores.

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos.

Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo vaya desde el puerto origen al puerto de destino.

En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

7.10.3 BUCLES DE RED E INUNDACIONES DE TRÁFICO

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores.

Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo.

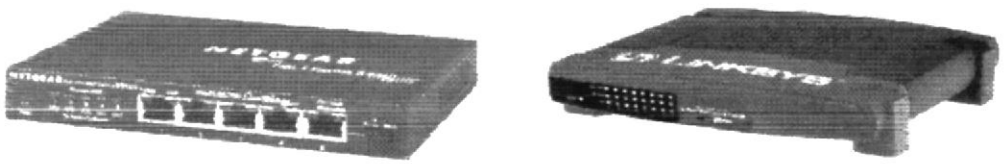
Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Como se ha comentado se emplea el protocolo spanning tree para evitar este tipo de fallos.

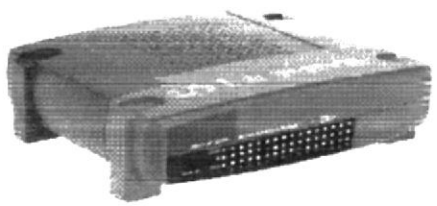
7.10.4 CONMUTADORES DE NIVEL 3

Aunque los conmutadores o switches son los elementos que fundamentalmente se encargan de encaminar las tramas de nivel 2 entre los diferentes puertos, existen los denominados conmutadores de nivel 3 o superior, que permiten crear en un mismo dispositivo múltiples redes de nivel 3 (ver VLANs) y encaminar los paquetes (de nivel 3) entre las redes, realizado por tanto las funciones de encaminamiento o routing.

7.10.5 DIFERENTES MODELOS DE SWITCH

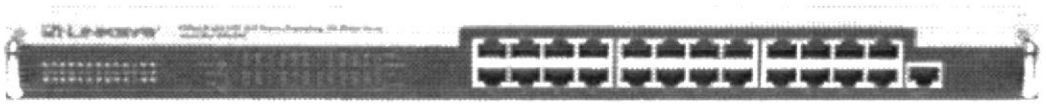


Diferentes Switchs Netgear de 4 puertos y Linksys de 8 puertos

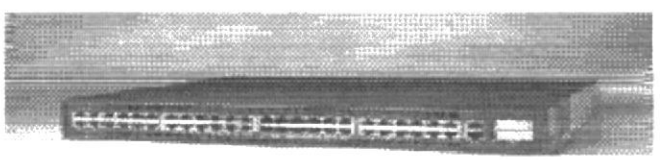


BIBLIOTECA CAMPUS PEÑAS

Cisco de 8 puertos y Linksys de 16 puertos



Linksys de 24 puertos.



Cisco de 48 puertos.

7.10.6 ENCAPSULAMIENTO

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

La capa de transporte divide los datos en unidades de un tamaño que se pueda administrar, denominadas segmentos. También asigna números de secuencia a los segmentos para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego la capa de red encapsula el segmento creando un paquete. Le agrega al paquete una dirección de red destino y origen, por lo general IP.

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

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino.

Pero si se deben enviar los datos a otro host a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia. Esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos (el paquete).

Las tres capas inferiores (red, enlace de datos, física) del modelos OSI son las capas principales de transporte de los datos a través de una red interna o de Internet. La excepción principal a esto es un dispositivo denominado gateway.



Este es un dispositivo que ha sido diseñado para convertir los datos desde un formato, creado por las capas de aplicación, presentación y sesión, en otro formato. De modo que el gateway utiliza las siete capas del modelo OSI para hacer esto.

Flujo de paquetes a través de los dispositivos de Capa 2. Es importante recordar que los paquetes se ubican dentro de tramas, de modo que para comprender la forma en que viajan los paquetes en los dispositivos de la Capa 2, es necesario trabajar con la forma en que se encapsulan los paquetes, que es la trama.

Cualquier cosa que le suceda a la trama también le sucede al paquete. Las NIC, los puentes y los switches involucran el uso de la información de la dirección de enlace de datos (MAC) para dirigir las tramas. Las NIC son el lugar donde reside la dirección MAC exclusiva. La dirección MAC se utiliza para crear la trama.

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

Si la trama no es local (con una dirección MAC que no está en el puerto de entrada del puente), entonces se envía al segmento de red siguiente.

El puente toma una trama, la remueve, examina la dirección MAC y luego envía o no la trama, según lo que requiera la situación.

El switch es como un hub con puertos individuales que actúan como puentes. El switch toma una trama de datos, la lee, examina las direcciones MAC de la Capa 2 y envía las tramas (las conmuta) a los puertos adecuados.

7.10.7 SEGMENTACIÓN

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño.

De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz.

Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host.

Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino.

ESPOL
BIBLIOTECA
CAMPUS PEÑAS

Al leer la información de Capa 2 de dirección MAC destino, los switches pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch.

Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños.

Si la LAN no se divide en segmentos, las LAN cuyo tamaño sea mayor que un grupo de trabajo pequeño se congestionarían rápidamente con tráfico y colisiones y virtualmente no ofrecerían ningún ancho de banda.

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

Los puentes y los switches amplían la longitud efectiva de una LAN, permitiendo la conexión de estaciones distantes que anteriormente no estaban permitidas.

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

Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch. Estos pueden soportar densidades de puerto más altas que los puentes.

Algunos switches soportan la conmutación por el método cut- through, que reduce la latencia y las demoras de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward).

Por último, los switches reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.



7.10.8 COLISIÓN

Uno de los problemas que se puede producir, cuando dos bits se propagan al mismo tiempo en la misma red, es una colisión. En una red pequeña y de baja velocidad es posible implementar un sistema que permita que sólo dos computadores envíen mensajes, cada uno por turnos.

Esto significa que ambas pueden mandar mensajes, pero sólo podría haber un bit en el sistema. El problema es que en las grandes redes hay muchos computadores conectados, cada uno de los cuales desea comunicar miles de millones de bits por segundo. Recordar que los "bits" en realidad son paquetes que contienen muchos bits.

Se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes como, por ejemplo, los repetidores, puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo.

Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos.

El área dentro de la red donde los paquetes se originan y colisionan, se denomina dominio de colisión, e incluye todos los entornos de medios compartidos.

Por ejemplo, un alambre puede estar conectado con otro a través de cables de conexión, transceptores, paneles de conexión, repetidores e incluso hubs. Todas estas interconexiones de la Capa 1 forman parte del dominio de colisión.

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

Al igual que lo que ocurre con dos automóviles, que no pueden ocupar el mismo espacio, o la misma carretera, al mismo tiempo, tampoco es posible que dos señales ocupen el mismo medio simultáneamente.

En general, se cree que las colisiones son malas ya que degradan el desempeño de la red. Sin embargo, una cantidad determinada de colisiones es una función natural de un entorno de medios compartidos (es decir, un dominio de colisión) ya que una gran cantidad de computadores intentan comunicarse entre sí simultáneamente, usando el mismo cable.

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

Se puede reducir el tamaño de los dominios de colisión utilizando dispositivos inteligentes de networking que pueden dividir los dominios.

Los puentes, switches y routers son ejemplos de este tipo de dispositivo de networking. Este proceso se denomina segmentación.

Un puente puede eliminar el tráfico innecesario en una red con mucha actividad dividiendo la red en segmentos y filtrando el tráfico basándose en la dirección de la estación. El tráfico entre dispositivos en el mismo segmento no atraviesa el puente, y afecta otros segmentos.

Esto funciona bien, siempre y cuando el tráfico entre segmentos no sea demasiado. En caso contrario, el puente se puede transformar en un cuello de botella, y de hecho puede reducir la velocidad de la comunicación. La mejor solución para este problema es la utilización de switches para la correcta segmentación de una LAN

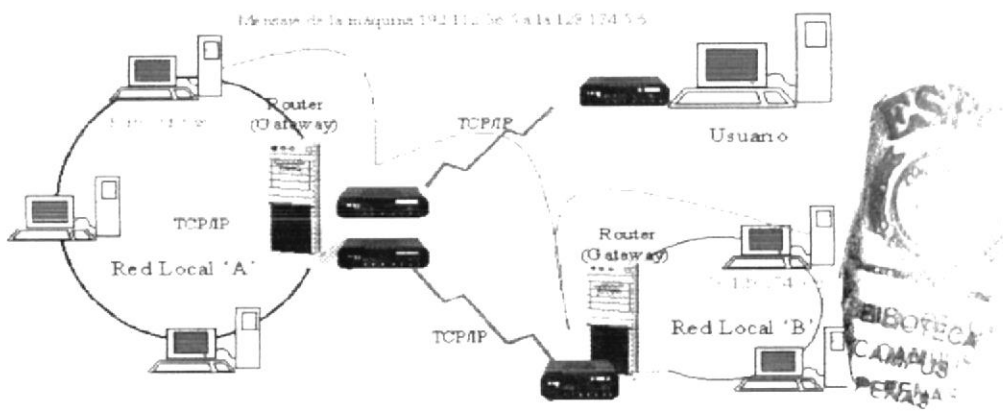
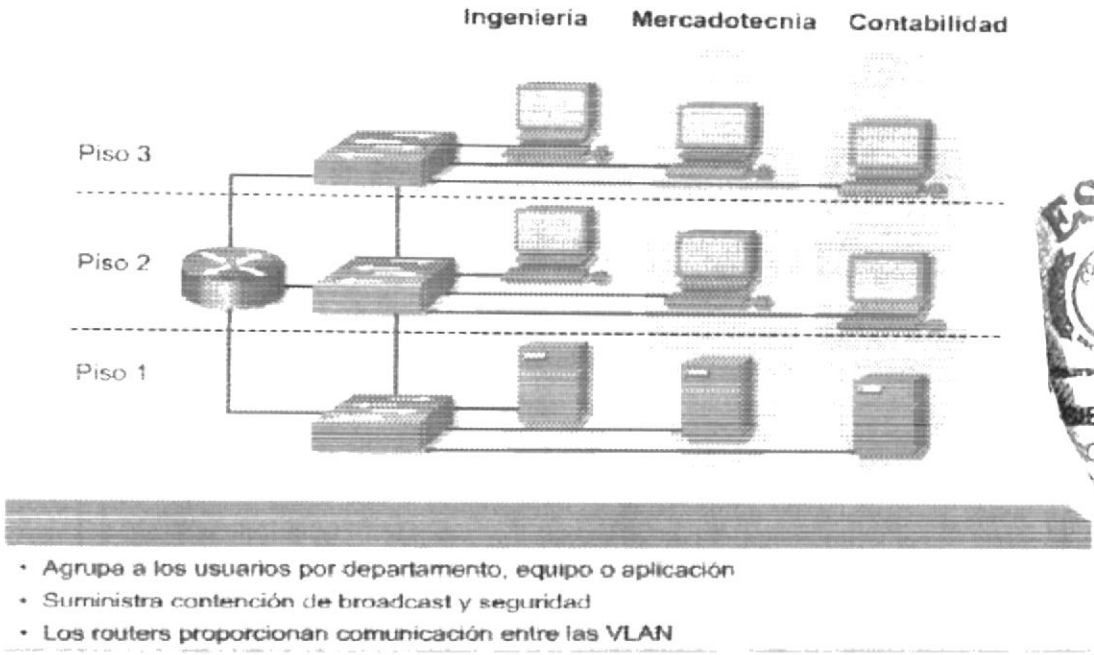


Figura 7-20: Grafico General de Comunicaciones.

7.11 VLAN



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 7-21: Vlan.

7.11.1 INTRODUCCIÓN A VLAN

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub.

Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual LAN o red virtual), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.

Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma.

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico.

Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

Además, al poder distribuir a los usuarios en diferentes segmentos de la red, se puede situar puentes y encaminadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo.

Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde/hacia otras redes.

Pero aún se puede llegar más lejos. Las redes virtuales nos permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.



7.11.2 TIPOS DE VLAN

7.11.2.1 VLAN DE PUERTO CENTRAL

Es en la que todos los nodos de una VLAN se conectan al mismo puerto del switch.

7.11.2.2 VLAN ESTÁTICAS

Los puertos del switch están ya preasignados a las estaciones de trabajo.

7.11.2.3 VLAN POR PUERTO

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

7.11.2.3.1 VENTAJAS

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

7.11.2.3.2 DESVENTAJAS

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

7.11.2.4 POR DIRECCIÓN MAC

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

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1



7.11.2.4.1 VENTAJAS

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

7.11.2.4.2 DESVENTAJAS

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

7.11.2.5 POR PROTOCOLO

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

7.11.2.5.1 VENTAJAS

- Segmentación por protocolo.
- Asignación dinámica.



7.11.2.5.2 DESVENTAJAS

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

7.11.2.6 POR DIRECCIONES IP

Esta basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados.

No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

7.11.2.6.1 VENTAJAS

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

7.11.2.6.2 DESVENTAJAS

- El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- Perdida de tiempo en la lectura de las tablas.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

7.11.2.7 POR NOMBRE DE USUARIO

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

7.11.2.7.1 VENTAJAS

- Facilidad de movimiento de los integrantes de la VLAN.
- Multiprotocolo.



7.11.2.7.2 DESVENTAJAS

En corporaciones muy dinámicas la administración de las tablas de usuarios.

7.11.2.8 VLAN DINÁMICAS (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo.

El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados.

Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN.

El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

7.12 TECNOLOGÍA

Existen tres aproximaciones diferentes que pueden ser empleadas como soluciones válidas para proporcionar redes virtuales: conmutación de puertos, conmutación de segmentos con funciones de bridging, y conmutación de segmentos con funciones de bridging/routing.

Todas las soluciones están basadas en arquitecturas de red que emplean concentradores/conmutadores. Aunque las tres son soluciones válidas, sólo la última, con funciones de bridge/router, ofrece todos las ventajas a las VLAN.

- **Conmutadores de puertos**

Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se diferencian de los conmutadores tradicionales en que sus puertos pueden ser dinámicamente asociados a cualquiera de los segmentos, mediante comandos software.

Cada segmento se asocia a un "backplane", el cual a su vez, equivale a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden asignadas y reasignadas a diferentes grupos de trabajo o redes virtuales.

Definir a los conmutadores de puertos como "software patch panels", y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo; sin embargo, tienen graves limitaciones.

Dado que están diseñados como dispositivos compartiendo un backplane físico, las reconfiguraciones de grupo de trabajo están limitadas al entorno de un único concentrador, y por tanto, todos los miembros del grupo deben de estar físicamente próximos.

Las redes virtuales con conmutadores de puertos, padecen de conectividad con el resto de la red. Al segmentar sus propios backplanes, no proporcionan conectividad integrada entre sus propios backplanes, y por tanto están "separados" de la comunicación con el resto de la red. Para ello requieren un bridge/router externo.

Ello implica mayores costes, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red.

Por último, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o backplane, y por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.



- **Conmutadores de segmentos con bridging**

A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Para ello, se emplean los algoritmos tradicionales de los puentes (bridges), o subconjuntos de los mismos, para proporcionar conectividad entre varios segmentos a la "velocidad del cable" o velocidad máxima que permite la topología y protocolos de dicha red.

Mediante estos dispositivos, las VLAN no son grupos de trabajo conectados a un solo segmento o backplane, sino grupos lógicos de nodos que pueden ser conectados a cualquier número de segmentos de red físicos.

Estas VLAN son dominios de broadcast lógicos: conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, mediante comandos software se puede reconfigurar y modificar la estructura de la VLAN, con la ventaja añadida del ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aún manteniendo el concepto de grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Aún así, comparten el mismo problema con los conmutadores de puertos en cuanto a su comunicación fuera del grupo.

Al estar aislados, para su comunicación con el resto de la red precisan de routers (encaminadores), con las consecuencias de las que ya se a hablado en el caso anterior respecto del coste y la reconfiguración de la red.



- **Conmutadores de segmentos con bridging/routing**

Son la solución evidente tras la atenta lectura de las dos soluciones anteriores. Dispositivos que comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además, con funciones añadidas de routing (encaminamiento), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de red.
Además, sus funciones de routing facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales, se puede crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador.

Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiéndoños así asignar el ancho de banda requerido por el nuevo grupo de trabajo sin afectar a las aplicaciones de red existentes.

En las VLAN con funciones de routing, la comunicación con el resto de la red se puede realizar de dos modos diferentes: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las funciones de routing multiprotocolo integradas, que facilitan el tráfico incluso entre varias VLAN's.

7.13 PRESTACIONES DE LAS VLAN

Los dispositivos con funciones VLAN ofrecen unas prestaciones de "valor añadido", suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las VLAN.

Al igual que en el caso de los grupos de trabajo "físicos", las VLAN permiten a un grupo de trabajo lógico compartir un dominio de broadcast.

Ello significa que los sistemas dentro de una determinada VLAN reciben mensajes de broadcast desde el resto, independientemente de que residan o no en la misma red física.

Por ello, las aplicaciones que requieren tráfico broadcast siguen funcionando en este tipo de redes virtuales. Al mismo tiempo, estos broadcast no son recibidos por otras estaciones situadas en otras VLAN.

Las VLAN no se limitan solo a un conmutador, sino que pueden extenderse a través de varios, estén o no físicamente en la misma localización geográfica.

Además las redes virtuales pueden solaparse, permitiendo que varias de ellas compartan determinados recursos, como backbones (troncales) de altas prestaciones o conexiones a servidores.



Uno de los mayores problemas a los que se enfrentan los administradores de las redes actuales, es la administración de las redes y subredes. Las VLAN tienen la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos de la red sin preocuparse de colisiones de direcciones.

Las soluciones tradicionales de internetworking, empleando concentradores y routers, requieren que cada segmento sea una única subred; por el contrario, en un dispositivo con facilidades VLAN, una subred puede expandirse a través de múltiples segmentos físicos, y un solo segmento físico puede soportar varias subredes.

Asimismo, hay que tener en cuenta que los modelos más avanzados de conmutadores con funciones VLAN, soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que permiten determinar con gran precisión las características del tráfico y de la seguridad que se desea en cada dominio, segmento, red o conjunto de redes.

Todo ello se realiza en función de algoritmos de bridging, y routing multiprotocolo.

7.14 APLICACIONES

A intentar esquematizar los puntos en que las redes virtuales pueden beneficiar a las redes actuales:

- **Movilidad**: Como a visto, el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.
  Dominios lógicos: Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos, o en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.

  Control y conservación del ancho de banda: Las redes virtuales pueden restringir los broadcast a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.

- **Conectividad:** Los modelos con funciones de routing permiten interconectar diferentes conmutadores y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos.

- **Seguridad:** Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad.

- **Protección de la inversión:** Las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costes adicionales.

  El primer suministrador de conmutadores con soporte VLAN fue ALANTEC (familia de concentradores/conmutadores multimedia inteligentes PowerHub), pero actualmente son muchos los fabricantes que ofrecen equipos con soluciones VLAN: Bytex (concentrador inteligente 7700), Cabletron (ESX-MIM), Chipcom (OnLine), Lannet (MultiNet Hub), Synoptics (Lattis System 5000), UB (Hub Access/One) y 3Com (LinkBuilder).



7.15 CASO DE ESTUDIO DE LA EMPRESA MOLINOS DEL ECUADOR

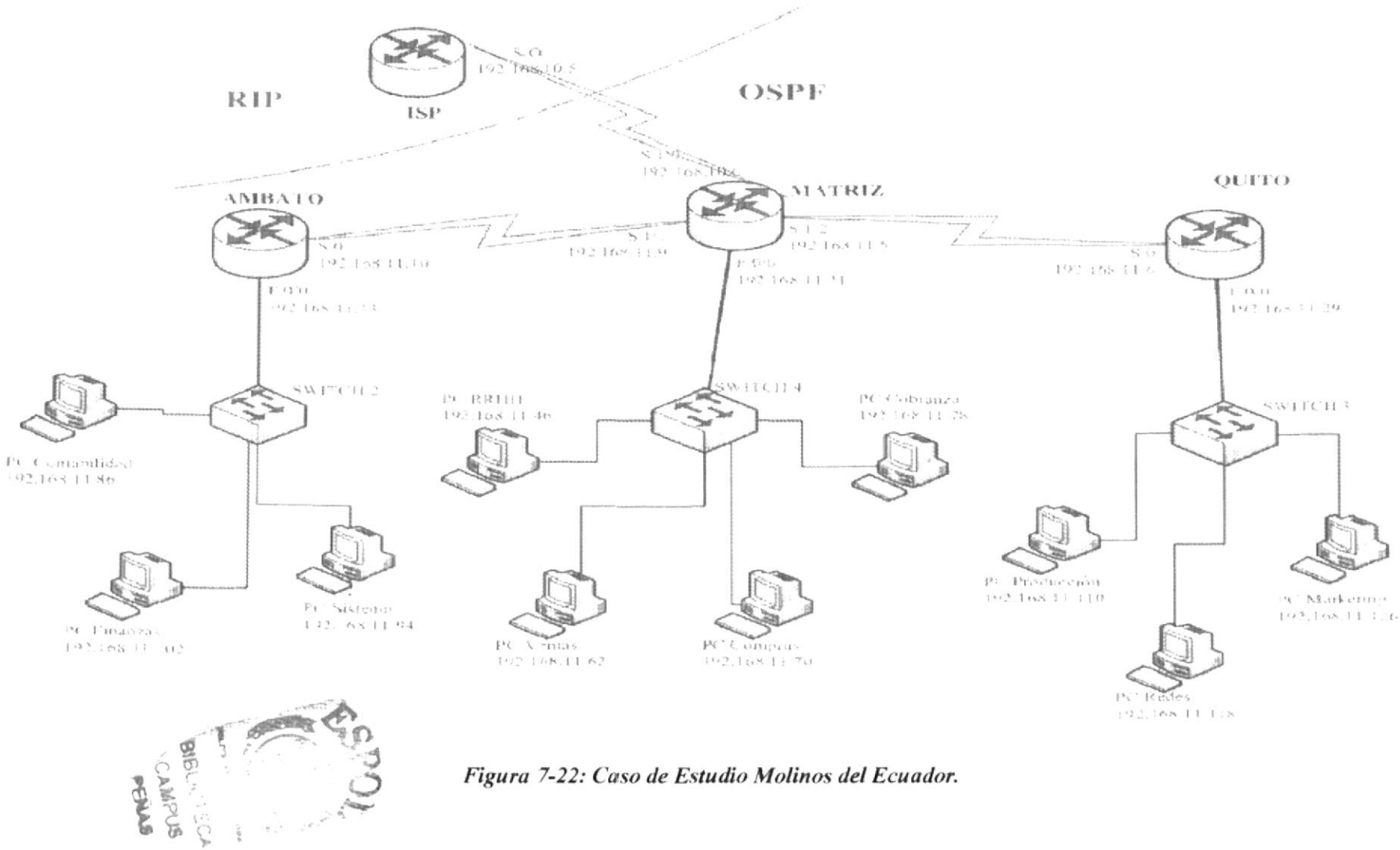


Figura 7-22: Caso de Estudio Molinos del Ecuador.

7.16 CONFIGURACIÓN EN EL HYPERTERMINAL

Ingrese a Inicio, Programas, Accesorios, Comunicaciones, HyperTerminal.

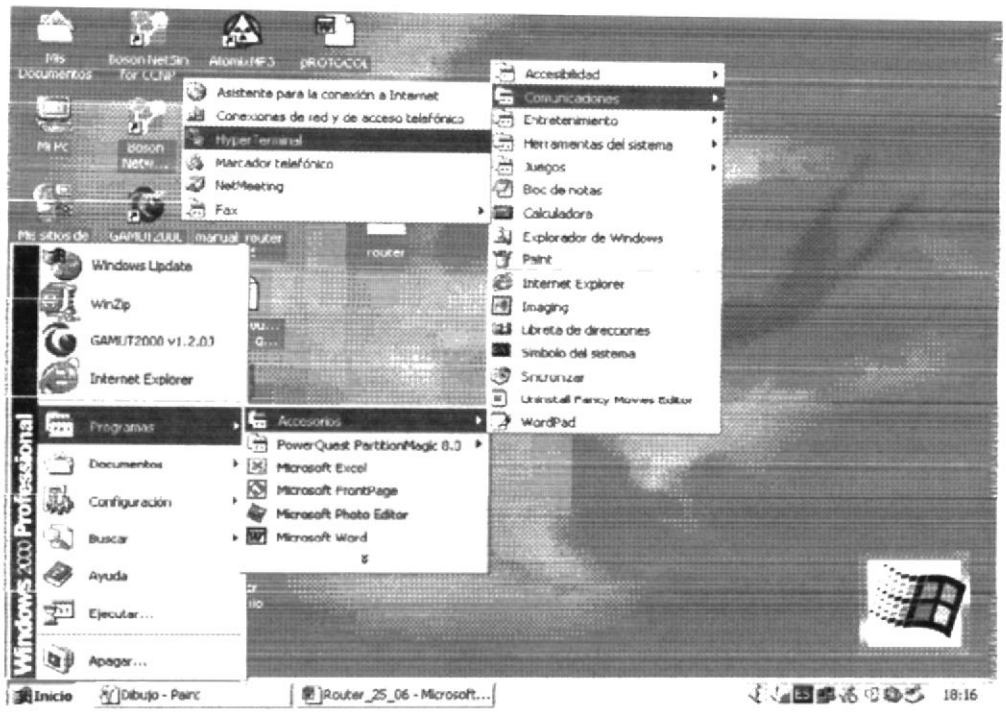
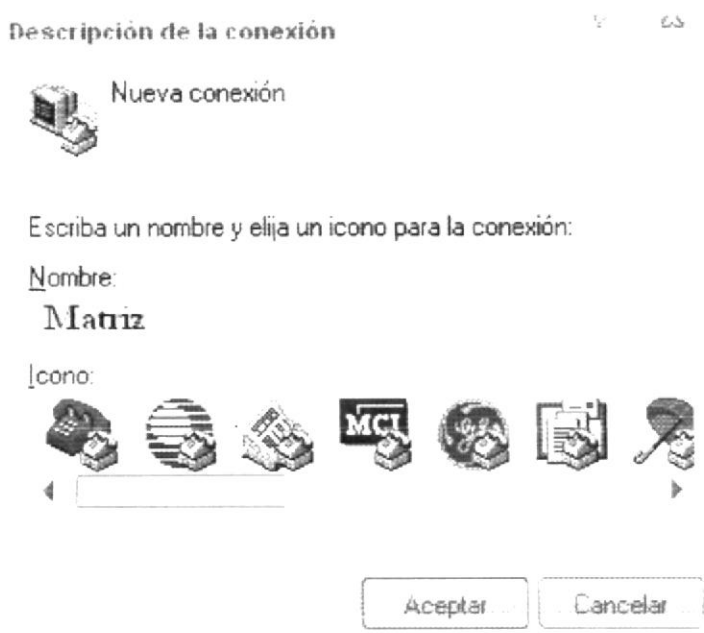


Figura 7-23: Configuración Hyperterminal.

En esta pantalla se muestra el cuadro de asignación del nombre del router que se va a configurar.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Figura 7-24: Descripción de la Conexión.

En esta pantalla se muestra el puerto en el cual esta conectado el router.

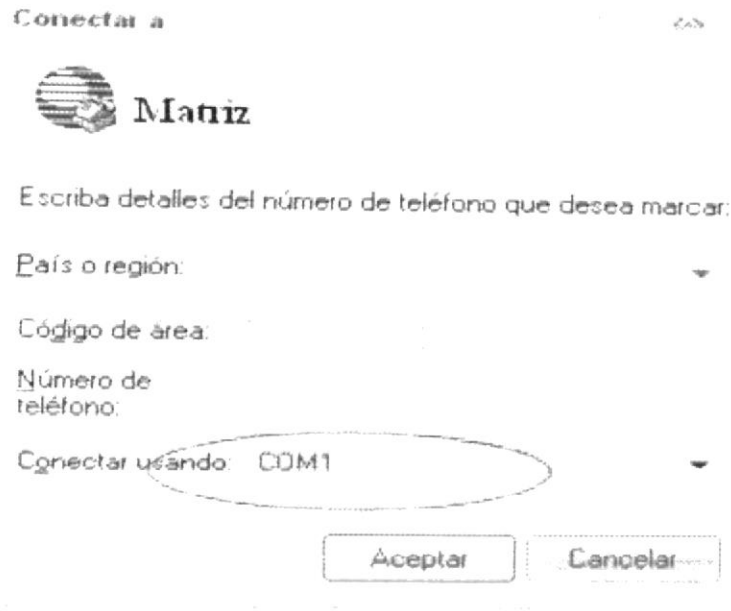
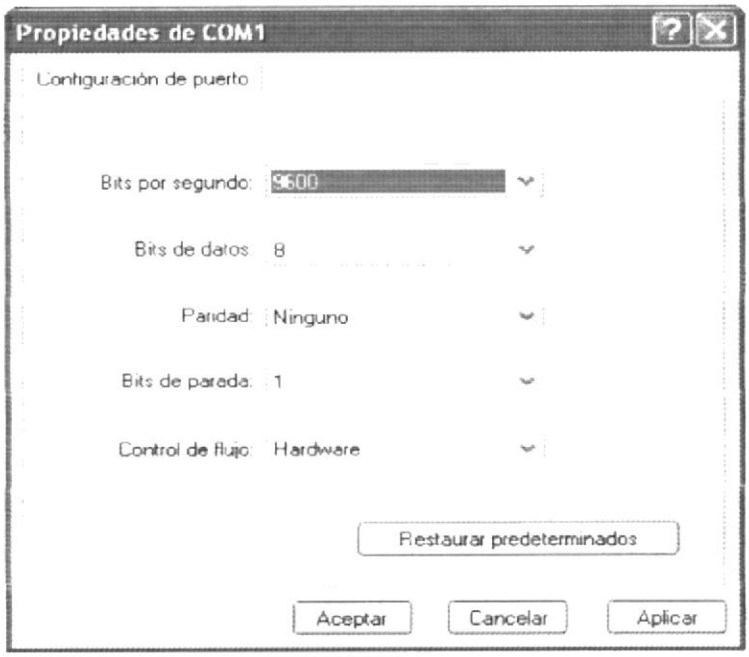


Figura 7-25: Configuración Hyperterminal.

Luego aparecerá una pantalla en la cual se mostrará las propiedades del COM1, y elija las siguientes opciones:

Bits por segundos: 9600
Bits de datos: 8
Paridad: ninguno
Bits de parada: 1
Control de flujo: Hardware



ESPOL
BIBLIOTECA
CAMPUS
PENAS

Figura 7-26: Propiedades COM 1.

Luego en esta pantalla ya se puede ver el nombre de la conexión.

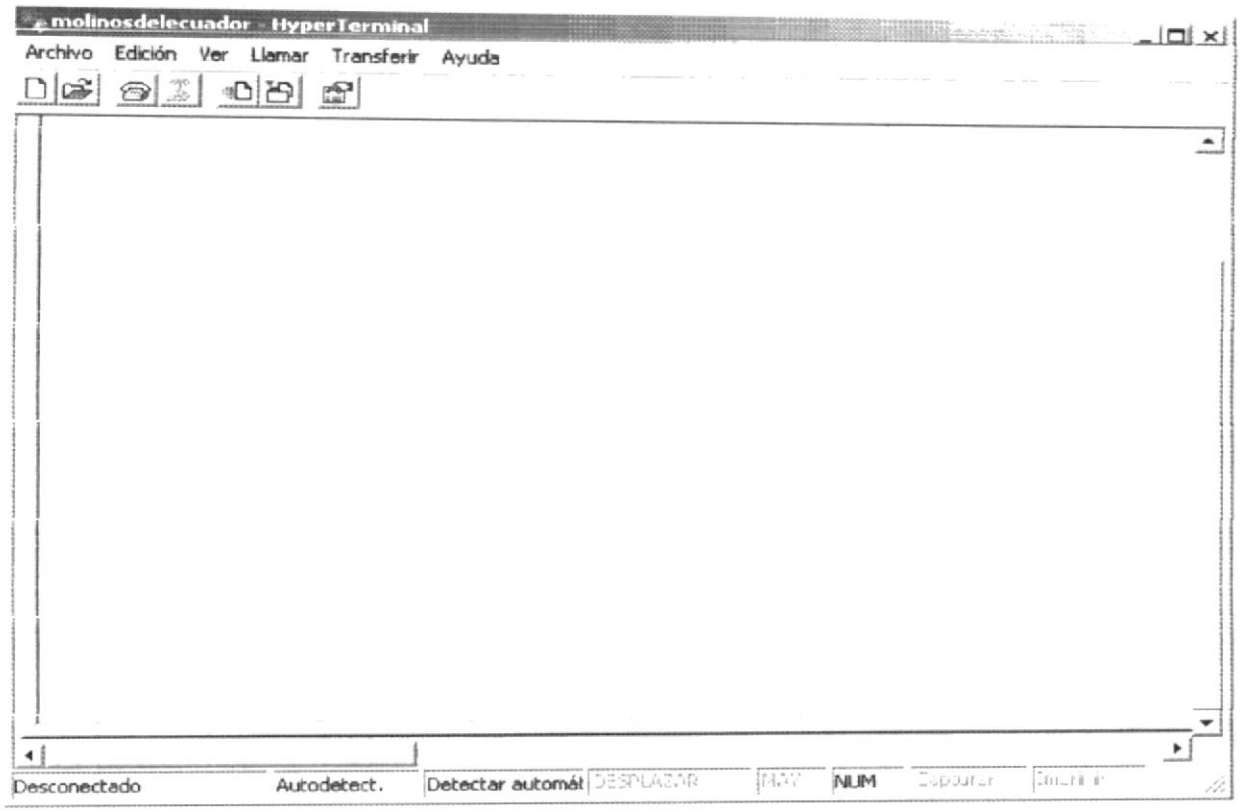
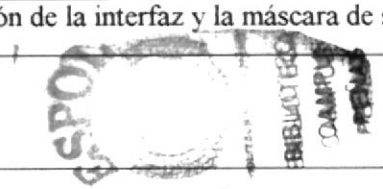


Figura 7-27: Nombre de la Conexión.

BIBLIOTECA
CAMPUS
PEÑAS

7.17 COMANDOS BÁSICOS DE ROUTER

COMANDO	DESCRIPCIÓN
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.



COMANDO	DESCRIPCIÓN
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.
Enable	Ingreso al modo privilegiado
Hostname	Comando que permite asignar un nombre a los dispositivos
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.



7.18 CONFIGURACIÓN DE ROUTER

7.18.1 ROUTER ISP

7.18.1.1 ASIGNACIÓN DE NOMBRE AL ROUTER ISP

Router> Enable
Ingresar al modo privilegiado
Router# configure terminal
Modo Global
Router(config)# hostname isp
Cambiar el nombre al route

Hostname	Comando
isp	Nombre del Router

BIBLIOTECA CAMPUS

isp(config)# ^Z
isp# wr
Grabar los cambios

```
Router>ena
Router#config ter
Router(config)#hostname isp
isp(config)#exit
isp#wr
Building configuration...
[OK]

isp#
```

Figura 7-28: Nombre Router ISP.

7.18.1.2 ASIGNACIÓN DE CONTRASEÑA AL ROUTER ISP

Isp> Enable

Ingresar al modo privilegiado

Isp# configure terminal

Ingresar al modo global

Isp (config)# line console 0

Ingresar a configurar la consola

isp (config-line)# password isp

Asignar una contraseña a la consola

Isp (config-line)# login

Ingresar de contraseña

Isp (config-line)# exit

Salir de la configuración de la consola

Isp(config)# line vty 0 4

Para ingresar una contraseña en modo telnet

Isp(config-line)# password isp

Permite asignar una contraseña

Isp(config-line)# login

Permite hacer petición de la contraseña

Isp(config-line)# exit

Comando para salir de la consola

Isp(config)# enable password isp

Permite habilitar la contraseña en el router

Isp (config)# enable secret isp

Contraseña encriptada para ingresar al router

Isp(config)# exit

Salir del config modo global

Isp# wr

Comando para grabar los cambios




```
isp#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
isp(config)#line console 0
isp(config-line)#password isp
isp(config-line)#login
isp(config-line)#exit
isp(config)#line vty 0 4
isp(config-line)#password isp
isp(config-line)#login
isp(config-line)#exit
isp(config)#enable password isp
isp(config)#enable secret isp
isp(config)#exit
isp#wr
Building configuration...
[OK]


isp#
```

Figura 7-29: Contraseña al Router ISP.

7.18.1.3 CONFIGURACIÓN DE INTERFAZ SERIAL 0.

isp > enable

Ingresar al modo privilegiado

isp #configure terminal

Ingresar al modo de configuración global

isp (config)# inter serial 0

Ingresar a la serial a configurar

isp (config-if)# ip address 192.168.10.5 255.255.255.252

Digitar la dirección IP con su respectiva máscara

192.168.10.5	DCE Serial 0
255.255.255.252	Máscara de Red

isp (config-if)# clock rate 64000

Asignar el valor para el sincronizador del reloj

isp (config-if)# no shutdown

Levantar la dirección IP

isp (config-if)# exit

Salir de la interfaz serial

isp# wr

Grabar los cambios

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

```
isp>ena
isp#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
isp(config)#interface serial 0
isp(config-if)#ip
isp(config-if)#ip address 192.168.10.5 255.255.255.252
isp(config-if)#clock rate 64000
isp(config-if)#no shutdown
isp(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

isp#wr
Building configuration...
[OK]


isp#
```

Figura 7-30: Configuración Interfaz Serial 0.

7.18.1.4 CONFIGURACIÓN DEL PROTOCOLO RIP

isp > enable

Ingresar al modo privilegiado

isp #configure terminal

Ingresar al modo de configuración global

isp (config)# router rip

Habilitar el protocolo de enrutamiento a configurar

isp (config-router)# network 192.168.10.0

Asignar la dirección de la red, wildcard y área respectiva

Network	Comando
192.168.10.0	Red

Al mismo tiempo configurar la distribución del protocolo de enrutamiento RIP.

isp (config-router)# redistribute ospf

Distribuir OSPF hacia las redes de OSPF

isp (config-if)# ^Z

Salir de la interfaz serial

isp# wr

Grabar los cambios

BIBLIOTECA CAMPUS PEÑAS

```
isp#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
isp(config)#router rip
isp(config-router)#network 192.168.10.0
isp(config-router)#redistribute ospf 1
isp(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

isp#wr
Building configuration...
[OK]


isp#
```

Figura 7-31: ConfiguraciónProtocolo RIP.

7.18.1.5 SHOW PROTOCOLS ISP

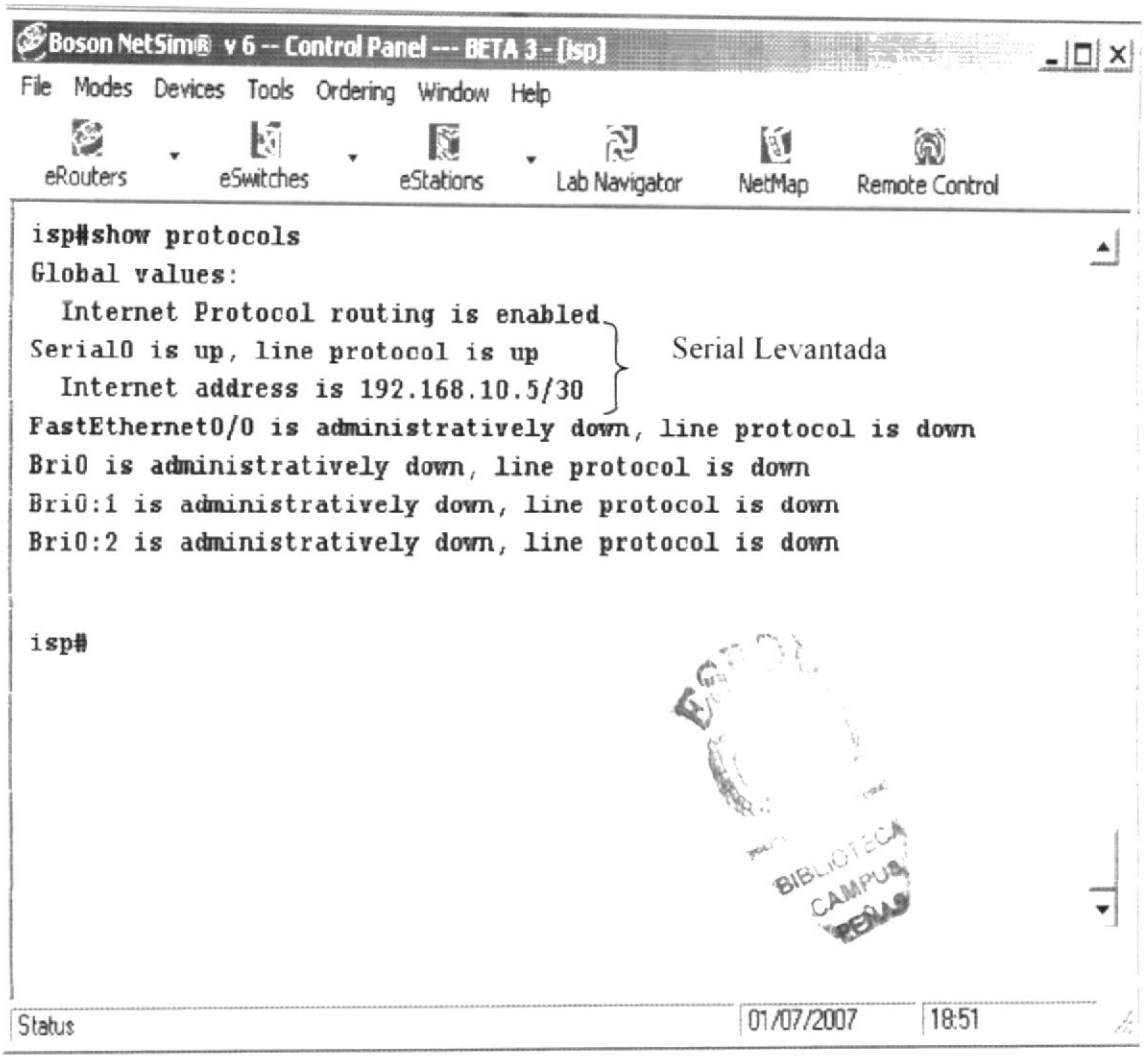


Figura 7-32: Show Protocols ISP.

Serial 0 is up, Line protocol is up
Indica la serial levantado
Internet address is 192.168.10.5/30
IP asignada al puerto serial del router.

Fasthernet 0/0 is administratively down, Line protocol is down
Indica que no se a asignado ninguna IP al puerto serial

7.18.1.6 SHOW RUN DEL ISP

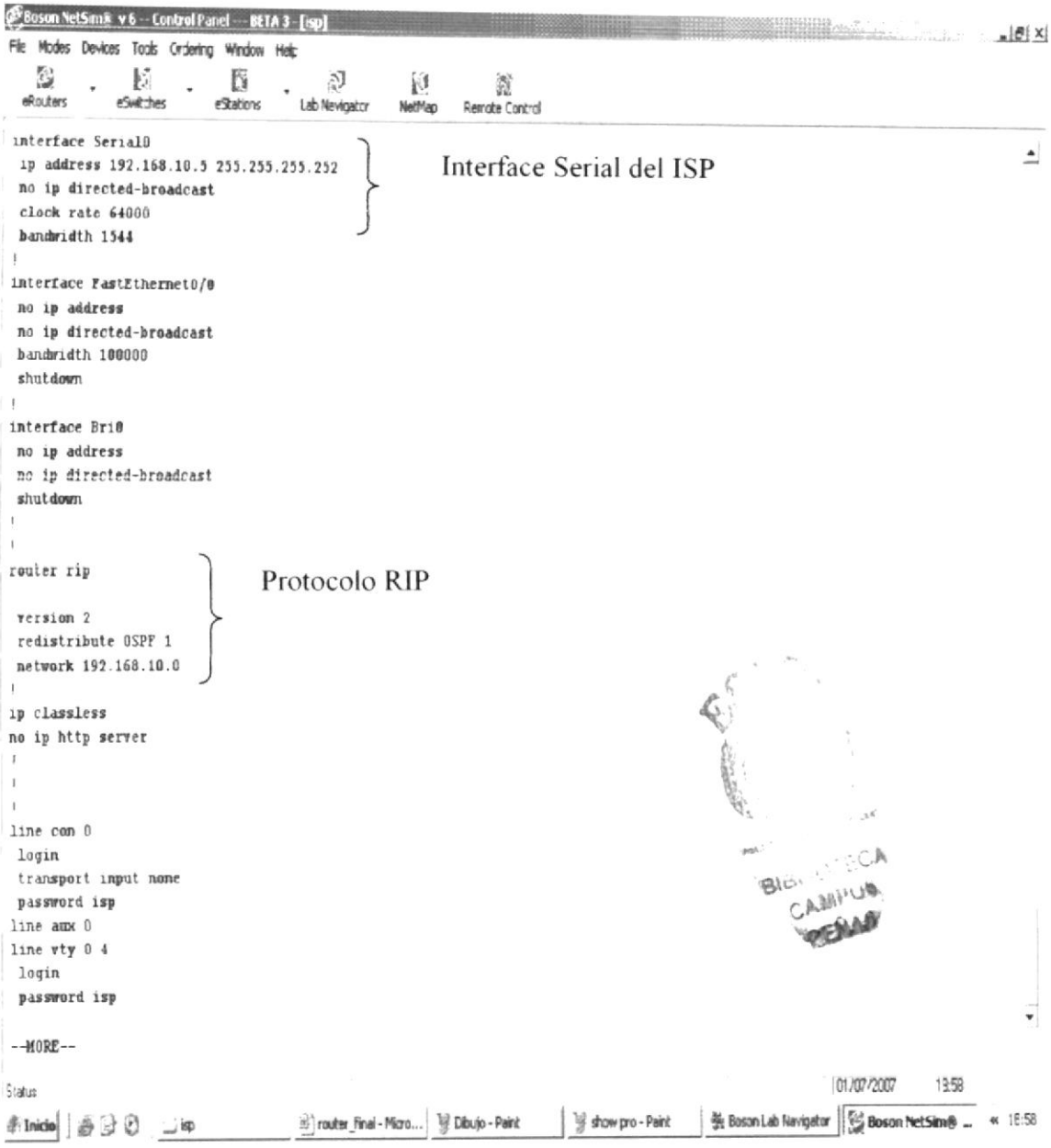


Figura 7-33: Show Run ISP.

```
ISP#show running-config
```

Mostrará el estado de todo el router con sus serials e interfaces

```
Building configuration...

!
Version 12.1
```

Version del Bios

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

Servicio de encriptción de contraseña no esta activo

```
!
hostname ISP
```

Nombre del router

```
enable secret 5 $sdf$6978yhg$jnb76sd
```

Indica que la contraseña de ingreso al switch se encuentra encriptada

```
enable password isp
!
!
!
ip subnet-zero
!
!
interface Serial0
```

Tipo de serial

```
 ip address 192.168.10.5 255.255.255.252
```

dirección IP y máscara de sub-red de la serial

```
 no ip directed-broadcast
 clock rate 64000
 bandwidth 1544
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 bandwidth 100000
 shutdown
!
interface Bri0
 no ip address
 no ip directed-broadcast
 shutdown
!
!
router rip

 version 2
 redistribute OSPF 1
 network 192.168.10.0
!
ip classless
```

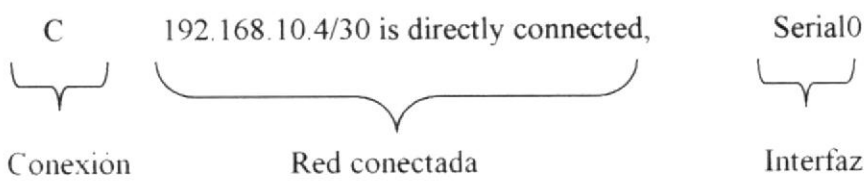
Protocolo RIP con su respectiva redistribución en este caso OSPF

```
no ip http server
!
line con 0
 login
 transport input none
 password matriz
line aux 0
line vty 0 4
 login
 password matriz
!
no scheduler allocate
endBri0:2 is administratively down, line protocol is down
end.
```

7.18.1.7 SHOW IP ROUTE ISP



Figura 7-34: Show IP Route ISP.



Codes: C- connected, S – static, I – IGRP, R RIP, M – mobile, B - BGP

Comandos:

C – enlace conectado.

S – ruta estática.

I – protocolo de enrutamiento IGRP.

R – protocolo de enrutamiento RIP.

M – enlace con un teléfono móvil.

D – eigrp, ex – EIGRP external, O OSPF, IA – OSPF, IA – OSPF inter área.

D – protocolo de enrutamiento EIGRP.

EX – protocolo de enrutamiento EIGRP externo

O – protocolo de enrutamiento OSPF.

IA - área interna del protocolo de enrutamiento OSPF.

N1 OSPF NSSA external type 1, N" – OSPF NSSA external type 2.

N1 - protocolo de enrutamiento OSPF externo de Tipo 1 NSSA.

N2 - protocolo de enrutamiento OSPF externo de Tipo 2 NSSA.

E1 OSPF external type 1, E2 – OSPF external type 2, E – EGP.

E1 - protocolo de enrutamiento OSPF externo de Tipo 1.

E2 - protocolo de enrutamiento OSPF externo de Tipo 2.

I – IS-IS, su – IS-IS summary, L1 – IS-IS level – 1, L2 – IS – IS level – 2 ia – IS-IS area, * -candidate default, U – per-user static route o – ODR, P – periodic downloaded static route.

Puerta de enlace no seteada o grabada.

Gateway of last resort is not set

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.18.1.8 SHOW INTERFACE

Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.10.5/30 → **Serial levantada**
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is Lance, address is 000C.3782.8690 (bia 000C.3782.8690)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Bri0 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never

ESPOL BIBLIOTECA CAMPUS PEÑAS

```
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Bri0:1 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Bri0:2 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
```



0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out.

7.18.2 MATRIZ (GUAYAQUIL)

7.18.2.1 ASIGNACIÓN DE NOMBRE AL ROUTER MATRIZ

Router> Enable
Ingresar al modo privilegiado
Router# configure terminal
Modo Global
Router(config)# hostname Matriz
Cambiar el nombre al route

Hostname	Comando
Matriz	Nombre del Router

Matriz(config)# ^Z
Matriz# wr
Grabar los cambios




```
Router>
Router>ena
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname matriz
matriz(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]

matriz#
```

Figura 7-35: Asignación Nombre Router Matriz

7.18.2.2 ASIGNACIÓN DE CONTRASEÑA AL ROUTER MATRIZ

Matriz> Enable

Ingresar al modo privilegiado

Matriz# configure terminal

Ingresar al modo global

Matriz (config)# line console 0

Ingresar a configurar la consola

Matriz (config-line)# password matriz

Asignar una contraseña a la consola

Matriz (config-line)# login

Ingresar de contraseña

Matriz (config-line)# exit

Salir de la configuración de la consola

Matriz(config)# line vty 0 4

Para ingresar una contraseña en modo telnet

Matriz(config-line)# password matriz

Permite asignar una contraseña

Matriz(config-line)# login

Permite hacer petición de la contraseña

Matriz(config-line)# exit

Comando para salir de la consola

Matriz(config)# enable password matriz

Permite habilitar la contraseña en el router

Matriz (config)# enable secret matriz

Contraseña encriptada para ingresar al router

Matriz(config)# ^Z

Matriz# wr

Grabar los cambios

ESPOL BIBLIOTECA CAMPUS PEÑAS

```
matriz>ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#line console 0
matriz(config-line)#password matriz
matriz(config-line)#login
matriz(config-line)#exit
matriz(config)#line vty 0 4
matriz(config-line)#password matriz
matriz(config-line)#login
matriz(config-line)#exit
matriz(config)#enable password matriz
matriz(config)#enable secret matriz
matriz(config)#exit
matriz#wr
Building configuration...
[OK]

matriz#
```

Figura 7-36: Asignación de Contraseña Router Matriz.

7.18.2.3 CONFIGURACIÓN DE INTERFAZ SERIAL 1/0.

matriz > enable

Ingresar al modo privilegiado

matriz #configure terminal

Ingresar al modo de configuración global

matriz (config)# inter serial 1/0

Ingresar a la serial que se va a configurar

matriz (config-if)# ip address 192.168.10.6 255.255.255.252

Digitar la dirección IP con su respectiva máscara

192.168.10.6	DTE Serial 1/0
255.255.255.252	Máscara de Red

ESPOL BIBLIOTECA CAMPUS PEÑAS

matriz (config-if)# clock rate 64000

Asignar el valor para el sincronizador del reloj

matriz (config-if)# no shutdown

Levantar la dirección IP

matriz (config-if)# exit

Salir de la interfaz serial

matriz# wr

Grabar los cambios

```
matriz>ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#inter serial 1/0
matriz(config-if)#ip address 192.168.10.6 255.255.255.252
matriz(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial1/0, changed state to up
matriz(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]

matriz#
```

Figura 7-37: Configuración Interfaz Serial 1/0.

7.18.2.4 CONFIGURACIÓN DE INTERFAZ SERIAL 1/1

matriz > enable

Ingresar al modo privilegiado

matriz #configure terminal

Ingresar al modo de configuración global

matriz (config)# inter serial 1/1

Ingresar a la serial quese va a configura

matriz (config-if)# ip address 192.168.11.9 255.255.255.252

Ingresar la dirección IP con su respectiva máscara

192.168.11.9	DCE Serial 1/1
255.255.255.252	Máscara de Red

matriz (config-if)# clock rate 64000

Asignar el valor para el sincronizador del reloj

matriz (config-if)# no shutdown

Levantar la dirección IP

matriz (config-if)# exit

Salir de la interfaz serial

matriz# wr

Grabar los cambios

ESPOL
BIBLIOTECA
AMPUS
PEÑAS

```
matriz>ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#interface serial 1/1
matriz(config-if)#ip address 192.168.11.9 255.255.255.252
matriz(config-if)#clock rate 64000
matriz(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial1/1, changed state to up
matriz(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]

matriz#
```

Figura 7-38: Configuración Interfaz Serial 1/1.

7.18.2.5 CONFIGURACIÓN DE INTERFAZ SERIAL 1/2

matriz > enable
Ingresar al modo privilegiado
matriz #configure terminal
Ingresar al modo de configuración global
matriz (config)# inter serial 1/2
Ingresar a la serial que se va a configurar
matriz (config-if)# ip address 192.168.11.5 255.255.255.252
Ingresar la dirección IP con su respectiva máscara

192.168.11.5	DCE Serial 1/2
255.255.255.252	Máscara de Red

matriz (config-if)# clock rate 64000
Asignar el valor para el sincronizador del reloj
matriz (config-if)# no shutdown
Levantar la dirección IP
matriz (config-if)# exit
Salir de la interfaz serial
matriz# wr
Grabar los cambios




```
matriz>ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#inter serial 1/2
matriz(config-if)#ip address 192.168.11.5 255.255.255.252
matriz(config-if)#clock rate 64000
matriz(config-if)#no shu
%LINK-3-UPDOWN: Interface Serial1/2, changed state to up
matriz(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]

matriz#
```

Figura 7-39: Configuración Interfaz Serial 1/2.

7.18.2.6 CONFIGURACIÓN DE INTERFAZ FASTHERNET 0/0

matriz > enable

Ingresar al modo privilegiado

matriz #configure terminal

Ingresar al modo de configuración global

matriz (config)# interface fastethernet 0/0

Ingresar a la fastethernet

matriz (config-if)# ip address 192.168.11.21 255.255.255.248

Ingresar la dirección IP con su respectiva máscara

192.168.11.5	Dirección del puerto Fasthernet
255.255.255.248	Máscara de Red

matriz (config-if)# no shutdown

Levantar la dirección IP

matriz (config-if)# exit

Salir de la interfaz serial

matriz# wr

Grabar los cambios



```
matriz>ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#interface fastethernet 0/0
matriz(config-if)#ip address 192.168.11.21 255.255.255.248
matriz(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
matriz(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]
```

Figura 7-40: Configuración Interfaz Fasthernet 0/0.

7.18.2.7 CONFIGURACIÓN DE SUB-INTERFAZ FASTETHERNET 0/0

matriz > enable
Ingresar al modo privilegiado
matriz #configure terminal
Ingresar al modo de configuración global
matriz (config)# interface fastethernet 0/0.1
Ingresar a la sub-fastethernet
matriz (config-subif)# ip address 192.168.11.45 255.255.255.240
Ingresar la dirección IP con su respectiva máscara

192.168.11.45	IP
255.255.255.240	Máscara de Red



7.18.2.7.1 ENRUTAMIENTO VLAN 10

matriz (config-subif)# encapsulation dot1q 10
Encapsular el número de la vlan a crear
matriz (config-subif)# no shutdown
Levantar la dirección IP
matriz (config-subif)# exit
Salir de la interfaz serial

```
matriz#>ena
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#interface fastethernet 0/0.1
matriz(config-subif)#ip address 192.168.11.45 255.255.255.240
matriz(config-subif)#encapsulation dot1q 10
matriz(config-subif)#no shutdown
matriz(config-subif)#exit
```

Figura 7-41: Enrutamiento Vlan 10.

7.18.2.7.2 ENRUTAMIENTO VLAN 20

matriz (config)# interface fastethernet 0/0.2

Ingresar a la sub- fastethernet

matriz (config-subif)# ip address 192.168.11.61 255.255.255.240

Ingresar la dirección IP con su respectiva máscara

192.168.11.61	IP
255.255.255.240	Máscara de Red

matriz (config-subif)# encapsulation dot1q 20

Encapsular el número de la vlan a crear

matriz (config-subif)# no shutdown

Levantar la dirección IP

matriz (config-subif)# exit

Salir de la interface Fasthernet 0/0.2

```
matriz(config)#interface fastethernet 0/0.2
matriz(config-subif)#ip address 192.168.11.61 255.255.255.240
matriz(config-subif)#encapsulation dot1q 20
matriz(config-subif)#no shutdown
matriz(config-subif)#exit
```

Figura 7-42: Enrutamiento Vlan 20.

7.18.2.7.3 ENRUTAMIENTO VLAN 30

matriz (config)# interface fastethernet 0/0.3

Ingresar a la sub- fastethernet

matriz (config-subif)# ip address 192.168.11.69 255.255.255.248

Ingresar la dirección IP con su respectiva máscara

192.168.11.69	IP
255.255.255.248	Máscara de Red

matriz (config-subif)# encapsulation dot1q 30

Encapsular el número de la vlan a crear

matriz (config-subif)# no shutdown

Levantar la dirección IP

matriz (config-subif)# exit

matriz# wr

Grabar los cambios

```
matriz(config)#interface fastethernet 0/0.3
matriz(config-subif)#ip address 192.168.11.69 255.255.255.248
matriz(config-subif)#encapsulation dot1q 30
matriz(config-subif)#no shutdown
matriz(config-subif)#exit
```

Figura 7-43: Enrutamiento Vlan 30.

7.18.2.7.4 ENRUTAMIENTO VLAN 40

matriz (config)# interface fastethernet 0/0.4
Ingresar a la sub- fastethernet
matriz (config-subif)# ip address 192.168.11.77 255.255.255.248
Ingresar la dirección IP con su respectiva máscara

192.168.11.77	IP
255.255.255.248	Máscara de Red

matriz (config-subif)# encapsulation dot1q 40
Encapsular el número de la vlan a crear
matriz (config-subif)# no shutdown
Levantar la dirección IP
matriz (config-subif)# exit
Salir de la interfaz serial)
matriz# wr
Grabar los cambios

```
matriz(config)#interface fastethernet 0/0.4
matriz(config-subif)#ip address 192.168.11.77 255.255.255.248
matriz(config-subif)#encapsulation dot1q 40
matriz(config-subif)#no shutdown
matriz(config-subif)#exit
```

Figura 7-44: Enrutamiento Vlan 40.

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

7.18.2.8 CONFIGURACIÓN DEL PROTOCOLO OSPF

matriz > enable

Ingresar al modo privilegiado

matriz #configure terminal

Ingresar al modo de configuración global

matriz (config)# router ospf 1

Habilitar el protocolo de enrutamiento a configurar

matriz (config-router)# network 192.168.11.4 0.0.0.3 area 0

matriz (config-router)# network 192.168.11.8 0.0.0.3 area 0

Asignar la dirección de la red, wildcard y área respectiva

Network	Comando
192.168.11.4	Red
0.0.0.3	Willcard
Área 0	Tipo de área

Al mismo tiempo se configurará la distribución del protocolo de enrutamiento RIP.

matriz (config-router)# redistribute rip

Distribuir OSPF hacia las redes de RIP

matriz (config-if)# ^Z

Salir de la interfaz serial

matriz# wr

Grabar los cambios



```
matriz>ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#router ospf 1
matriz(config-router)#network 192.168.11.4 0.0.0.3 area  0
matriz(config-router)#network 192.168.11.8 0.0.0.3 area  0
matriz(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]
```

Figura 7-45: Protocolo OSPF.

7.18.2.9 SHOW PROTOCOLS MATRIZ

matriz > enable

Ingresar al modo privilegiado

matriz # show protocols

Este comando mostrará las IP levantadas o activas

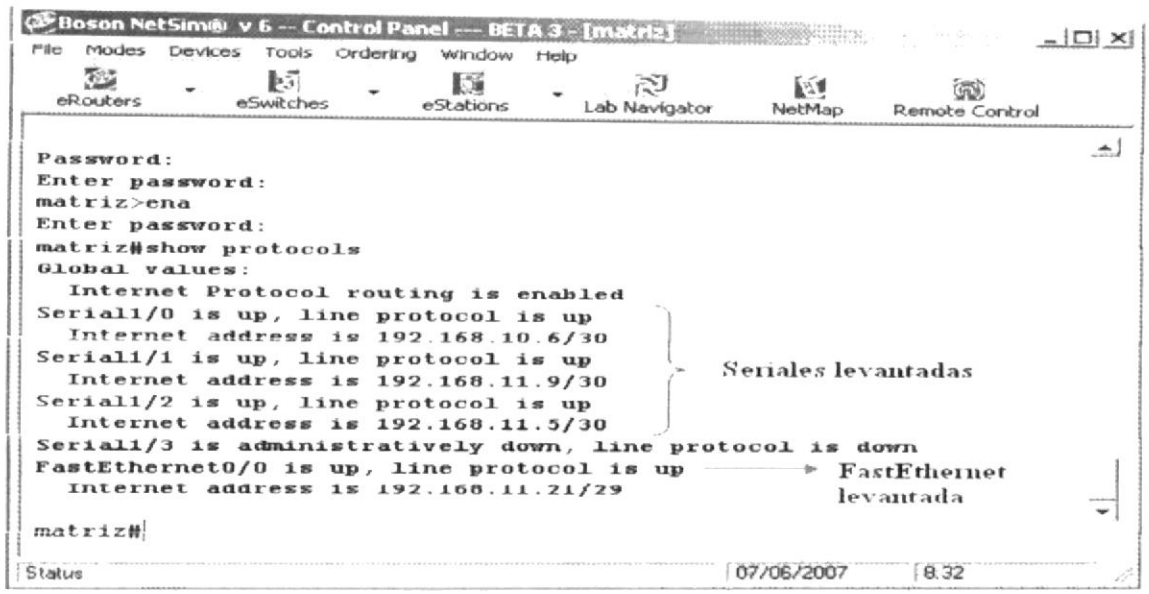


Figura 7-46: Show Protocols Matriz

Serial 1/0 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.10.6/30

IP asignada al puerto serial del router.

Serial 1/1 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.11.9/30

IP asignada al puerto serial del router.

Serial 1/2 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.11.5/30

IP asignada al puerto serial del router.

Serial 1/3 is administratively down, Line protocol is down

Indica que no se a asignado ninguna IP al puerto serial

Fasthernet 0/0 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.11.21/29

IP asignada al puerto del Switch.

7.18.2.10 SHOW IP ROUTE MATRIZ

matriz > enable

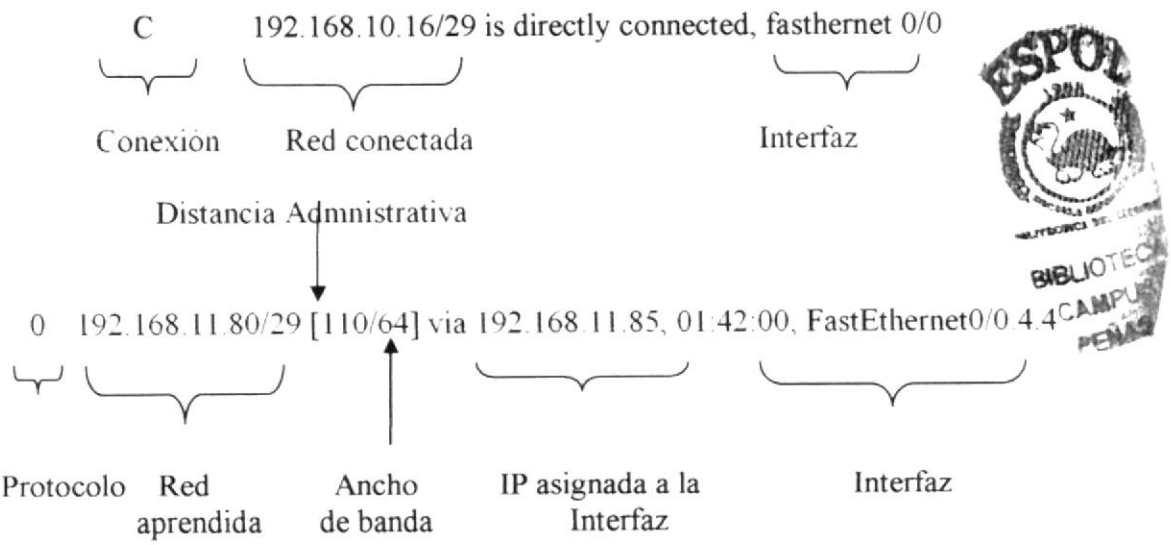
Ingresar al modo privilegiado

matriz # show ip route

Muestra la tabla de ruteo en la cual se verifica los seriales de los puertos conectados y el o los protocolos aprendidos en el router.



Figura 7-47: Show IP Route Matriz



Codes: C- connected, S – static, I – IGRP, R RIP, M – mobile, B - BGP

Comandos:

C – enlace conectado.

S – ruta estática.

I – protocolo de enrutamiento IGRP

R – protocolo de enrutamiento RIP.

M – enlace con un teléfono móvil.

D – eigrp, ex – EIGRP external, O OSPF, IA – OSPF, IA – OSPF inter área.

D – protocolo de enrutamiento EIGRP.

EX – protocolo de enrutamiento EIGRP externo.

O – protocolo de enrutamiento OSPF.

IA - área interna del protocolo de enrutamiento OSPF.

N1 OSPF NSSA external type 1, N" – OSPF NSSA external type 2.

N1 - protocolo de enrutamiento OSPF externo de Tipo 1 NSSA.

N2 - protocolo de enrutamiento OSPF externo de Tipo 2 NSSA.

E1 OSPF external type 1, E2 – OSPF external type 2, E – EGP.

E1 - protocolo de enrutamiento OSPF externo de Tipo 1.

E2 - protocolo de enrutamiento OSPF externo de Tipo 2.

I – IS-IS, su – IS-IS summary, L1 – IS-IS level – 1, L2 – IS – IS level – 2 ia – IS-IS area, * -candidate default, U – per-user static route o – ODR, P – periodic downloaded static route.

Puerta de enlace no seteada o grabada.

Gateway of last resort is not set



7.18.2.11 SHOW RUN MATRIZ

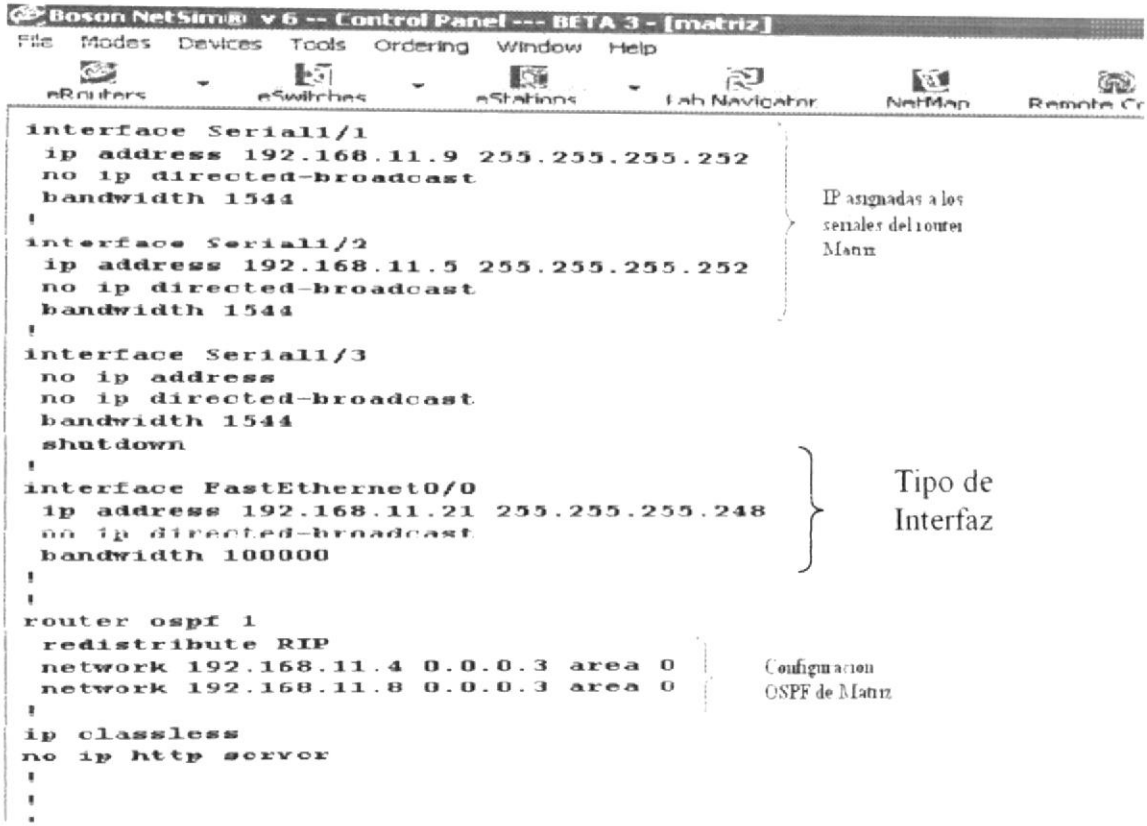


Figura 7-48: Show Run Matriz.

matriz #show running-config

Mostrará el estado de todo el router con sus seriales e interfaces

Building configuration...

!

Version 12.1

Versión del Bios

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

Servicio de encriptación de contraseña no esta activo

!

hostname matriz

Nombre del router

enable secret 5 sdf6978yhg$jnb76sd

Indica que la contraseña de ingreso al switch se encuentra encriptada

enable password matriz

!

ip subnet-zero

!

interface Serial1/0

ESPOL BIBLIOTECA CAMPUS

Tipo de Serial
ip address 192.168.10.6 255.255.255.252
Dirección IP y máscara de sub-red de la serial
no ip directed-broadcast
bandwidth 1544
!
interface Serial1/1

Tipo de Serial
ip address 192.168.11.9 255.255.255.252
Dirección IP y máscara de sub-red de la serial
no ip directed-broadcast
bandwidth 1544
!
interface Serial1/2

Tipo de Serial
ip address 192.168.11.5 255.255.255.252
Dirección IP y máscara de sub-red de la serial
no ip directed-broadcast
bandwidth 1544
!
interface Serial1/3
no ip address
no ip directed-broadcast
bandwidth 1544
shutdown
!
interface FastEthernet0/0

Tipo de Interfaz
ip address 192.168.11.21 255.255.255.248

Dirección IP y máscara de interfaz.
no ip directed-broadcast
bandwidth 100000
!
interface FastEthernet0/0.2

Tipo de Sub-Interfaz
encapsulation dot1q 20
Sub-interfaz
ip address 192.168.11.61 255.255.255.240
! **Dirección IP y máscara de la interfaz**
interface FastEthernet0/0.1

Tipo de Sub-interfaz
encapsulation dot1q 10
Sub-interfaz



```
ip address 192.168.11.45 255.255.255.240
!       Dirección IP y máscara de la interfaz
interface FastEthernet0/0.3
        Tipo de Sub-Interfaz
 encapsulation dot1q 30
        Sub-interfaz
 ip address 192.168.11.69 255.255.255.248
!       Dirección IP y máscara de la interfaz
interface FastEthernet0/0.4

        Tipo de Sub-Interfaz
 encapsulation dot1q 40
        Sub-interfaz
 ip address 192.168.11.77 255.255.255.248
!       Dirección IP y máscara de la interfaz
!
router ospf 1

        Tipo de Protocolo
 redistribute RIP
        Redistribulle el protocolo Rip
 network 192.168.11.4 0.0.0.3 area 0
 network 192.168.11.8 0.0.0.3 area 0
 !      Red con su respectiva Willcard
ip classless
no ip http server
!
!
line con 0
 login
 transport input none
 password matriz
line aux 0
line vty 0 4
 login
 password matriz
!
no scheduler allocate
end.
```



7.18.2.12 SHOW INTERFACE MATRIZ

matriz#
matriz#show interfaces
Serial1/0 is up, line protocol is up
Hardware is HD64570 **Serial 1/0 levantada**
Internet address is 192.168.10.6/30
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Serial1/1 is up, line protocol is up **Serial 1/1 levantada**
Hardware is HD64570
Internet address is 192.168.11.9/30
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Serial1/2 is up, line protocol is up **Serial 1/2 levantada**
Hardware is HD64570
Internet address is 192.168.11.5/30
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255



```
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never.
Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Serial1/3 is administratively down, line protocol is down
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0 is up, line protocol is up
  Hardware is Lance, address is 000C.2988.5967 (bia 000C.2988.5967)
  Internet address is 192.168.11.21/29
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
```

Fastethernet 0/0 levantada



```
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.2 is up, line protocol is up
  Hardware is AmdFE, address is 000C.2988.5968 (bia 000C.2988.5968)
  Internet address is 192.168.11.61/28
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/0.1 is up, line protocol is up
  Hardware is AmdFE, address is 000C.2988.5968 (bia 000C.2988.5968)
  Internet address is 192.168.11.45/28
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/0.3 is up, line protocol is up
  Hardware is AmdFE, address is 000C.2988.5968 (bia 000C.2988.5968)
  Internet address is 192.168.11.69/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/0.4 is up, line protocol is up
  Hardware is AmdFE, address is 000C.2988.5968 (bia 000C.2988.5968)
  Internet address is 192.168.11.77/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00.
```

Fastehernet 0/0.2 levantada

Fastehernet 0/0.1 levantada

Fastehernet 0/0.3 levantada

Fastehernet 0/0.4 levantada



7.18.3 CONFIGURACIÓN DEL ROUTER SUCURSAL (AMBATO)

7.18.3.1 ASIGNAR EL NOMBRE AL ROUTER SUCURSAL

Router>ena

Ingresar al modo privilegiado

Router>config terminal

Ingresar al modo de configuración global

Router(config) # hostname Ambato

Asignar el nombre al router sucursal ambato

Hostname	Comando
Ambato	Nombre del router de la sucursal

ambato (config) # ^Z

Salir del modo global

ambato(config) # wr

Grabar los cambios

```
Router>ena
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ambato
ambato(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

ambato#wr
Building configuration...
[OK]

ambato#
```

Figura 7-49: Asignación de Nombre Router Sucursal Ambato.



7.18.3.2 CREACIÓN DE CONTRASEÑAS

ambato > enable

Ingresar al modo privilegiado

ambato #configure terminal

Ingresar al modo de configuración global

ambato (config)# line console 0

Ingresar a configurar la consola

ambato (config-line)# password Ambato

Asignar una contraseña a la consola

ambato (config-line)# login

Ingresar de contraseña

ambato (config-line)# exit

Salir de la configuración de la consola

ambato (config)# line vty 0 4

Ingresar a configurar la Terminal Virtual

ambato (config-line)# password Ambato

Ingresar la contraseña a la Terminal Virtual

ambato (config-line)# login

Petición de contraseña

ambato (config-line)# exit

Salir de la configuración de la Terminal Virtual

ambato (config)# enable password cisco

Agregar una contraseña para ingresar al router

ambato (config)# enable secret cisco

Agregar una contraseña encriptada para ingresar al router

ambato (config)# exit

Salir del config Terminal

ambato# wr

Grabar los cambios asignados

```
ambato>ena
ambato#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
ambato(config)#line console 0
ambato(config-line)#password ambato
ambato(config-line)#login
ambato(config-line)#exit
ambato(config)#line vty 0 4
ambato(config-line)#password ambato
ambato(config-line)#login
ambato(config-line)#exit
ambato(config)#enable password ambato
ambato(config)#enable secret ambato
ambato(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

ambato#wr
Building configuration...
[OK]
ambato#
```



Figura 7-50: Asignación de Contraseña Router Sucursal Ambato.

7.18.3.3 CONFIGURACIÓN DE INTERFAZ SERIAL 0

ambato > enable
Ingresar al modo privilegiado
ambato #configure terminal
Ingresar al modo de configuración global
ambato (config)# inter serial 0
Ingresar a la serial que se va a configurar
ambato (config-if)# ip address 192.168.11.10 255.255.255.252
Ingresar la dirección IP con su respectiva máscara

192.168.11.10	DTE IP Serial 0
255.255.255.252	Máscara de Red

ambato (config-if)# no shutdown
Levantar la dirección IP
ambato (config-if)# exit
Salir de la interfaz serial
ambato(config) # ^Z
Salir del modo global
ambato# wr
Grabar los cambios

```
ambato>ena
Enter configuration commands, one per line.  End with CNTL/Z.
ambato(config)#inter serial 0
ambato(config-if)#ip address 192.168.11.10 255.255.255.252
ambato(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
ambato(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

ambato#wr
Building configuration...
[OK]

ambato#
```

F

igura 7-51: IPlinterfaz Serial 0.

7.18.3.4 CONFIGURACIÓN DE INTERFAZ FASTETHERNET 0/0

ambato > enable

Ingresar al modo privilegiado

ambato #configure terminal

Ingresar al modo de configuración global

ambato (config)# interface fastethernet 0/0

Ingresar a la fastethernet

ambato (config-if)# ip address 192.168.11.13 255.255.255.248

Ingresar la dirección IP con su respectiva máscara

192.168.11.13	IP Fasthernet 0/0
255.255.255.248	Máscara de Red



ambato (config-if)# no shutdown

Levantar la dirección IP

ambato (config-if)# exit

Salir de la interfaz serial

ambato# wr

Grabar los cambios

```
ambato>ena
ambato#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
ambato(config)#interface fastethernet 0/0
ambato(config-if)#ip address 192.168.11.13 255.255.255.248
ambato(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
ambato(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

ambato#wr
```

Figura 7-52: IP Interfaz Fasthernet 0/0.

7.18.3.5 CONFIGURACIÓN DE SUB-INTERFAZ FASTETHERNET 0/0

ambato > enable
Ingresar al modo privilegiado
ambato #configure terminal
Ingresar al modo de configuración global
ambato (config)# interface fastethernet 0/0.1
Ingresar a la sub- fastethernet
ambato (config-subif)# ip address 192.168.11.85 255.255.255.248
Ingresar la dirección IP con su respectiva máscara

192.168.11.85	IP
255.255.255.248	Máscara de red

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.18.3.5.1 ENRUTAMIENTO DE LA VLAN 50

ambato (config-subif)# encapsulation dot1q 50
Encapsular el número de la vlan a crear
ambato (config-subif)# no shutdown
Levantar la dirección IP
ambato (config-subif)# exit
Salir de la interfaz Fasthernet 0/0.1

```
ambato>ena
ambato#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
ambato(config)#inter fastethernet 0/0.1
ambato(config-subif)#ip address 192.168.11.85 255.255.255.248
ambato(config-subif)#encapsulation dot1q 50
ambato(config-subif)#no shutdown
ambato(config-subif)#exit
```

Figura 7-53: Enrutamiento VLAN 50.

7.18.3.5.2 ENRUTAMIENTO VLAN 60

ambato (config)# interface fastethernet 0/0.2

Ingresar a la sub- fastethernet

ambato (config-subif)# ip address 192.168.11.93 255.255.255.248

Ingresar la dirección IP con su respectiva máscara

192.168.11.93	IP
255.255.255.248	Máscara de red



ambato (config-subif)# encapsulation dot1q 60

Encapsular el número de la vlan a crear

ambato (config-subif)# no shutdown

Levantar la dirección IP

ambato (config-subif)# exit

Salir de la interface Fasthernet 0/0.2

```
ambato(config)#inter fastethernet 0/0.2
ambato(config-subif)#ip address 192.160.11.93 255.255.255.240
ambato(config-subif)#encapsulation dot1q 60
ambato(config-subif)#no shutdown
ambato(config-subif)#EXIT
```

Figura 7-54: Enrutamiento VLAN 60.

7.18.3.5.3 ENRUTAMIENTO VLAN 70

ambato (config)# interface fastethernet 0/0.3

Ingresar a la sub- fastethernet

ambato (config-subif)# ip address 192.168.11.101 255.255.255.248

Ingresar la dirección IP con su respectiva máscara

192.168.11.101	IP
255.255.255.248	Máscara de red

ambato (config-subif)# encapsulation dot1q 70

Encapsular el número de la vlan a crear

ambato (config-subif)# no shutdown

Levantar la dirección IP

ambato (config-subif)# exit

ambato# wr

Grabar los cambios

```
ambato(config)#inter fastethernet 0/0.3
ambato(config-subif)#ip address 192.168.11.101 255.255.255.248
ambato(config-subif)#encapsulation dot1q 70
ambato(config-subif)#no shutdown
ambato#wr
```

Figura 7-55: IP Enrutamiento VLAN 70.

7.18.3.6 CONFIGURACIÓN DEL PROTOCOLO OSPF

ambato > enable

Ingresar al modo privilegiado

ambato #configure terminal

Ingresar al modo de configuración global

ambato (config)# router ospf 1

Habilitar el protocolo de enrutamiento a configurar

ambato (config-router)# network 192.168.11.8 0.0.0.3 área 0

Asignar la dirección de la red, wildcard y área respectiva

Network	Comando
192.168.11.8	Red
0.0.0.3	Willcard
Área 0	Tipo de área



Al mismo tiempo configurar la distribución del protocolo de enrutamiento RIP.

ambato (config-router)# redistribute rip

Distribuir OSPF hacia las redes de RIP

ambato (config-if)# ^Z

Salir de la interfaz serial

ambato# wr

Grabar los cambios

```
ambato>ena
ambato#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
ambato(config)#router ospf 1
ambato(config-router)#network 192.168.11.8 0.0.0.3 area 0
ambato(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

ambato#wr
Building configuration...
[OK]

ambato#
```

Figura 7-56: Configuración Protocolo OSPF.

7.18.3.7 SHOW PROTOCOLS DE LA SUCURSAL AMBATO



ambato > enable

Ingresar al modo privilegiado

ambato # show protocols

Permite ver el estado de los puertos.

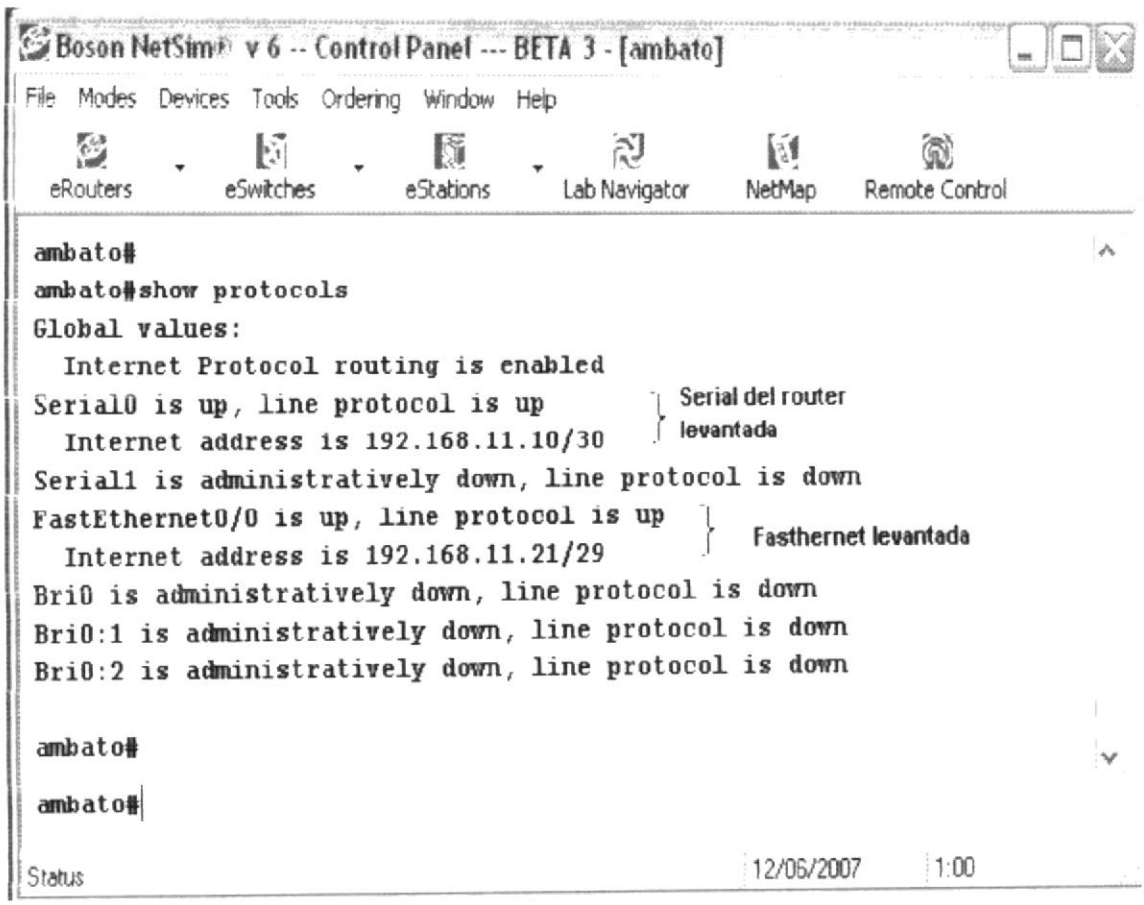


Figura 7-57: Show Protocols Ambato.

Serial 0 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.11.10/30

IP asignada al puerto serial del router

Serial 1 is administratively down, Line protocol is down

Indica que no se asignado ninguna IP al puerto serial

Fasthernet 0/0 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.11.21/29

IP asignada al puerto del Switch

7.18.3.8 SHOW RUN DE LA SUCURSAL AMBATO

ambato > enable

Ingresar al modo privilegiado

ambato # show running-config

Permite ver todas las configuraciones IP y protocolos utilizados en el router.

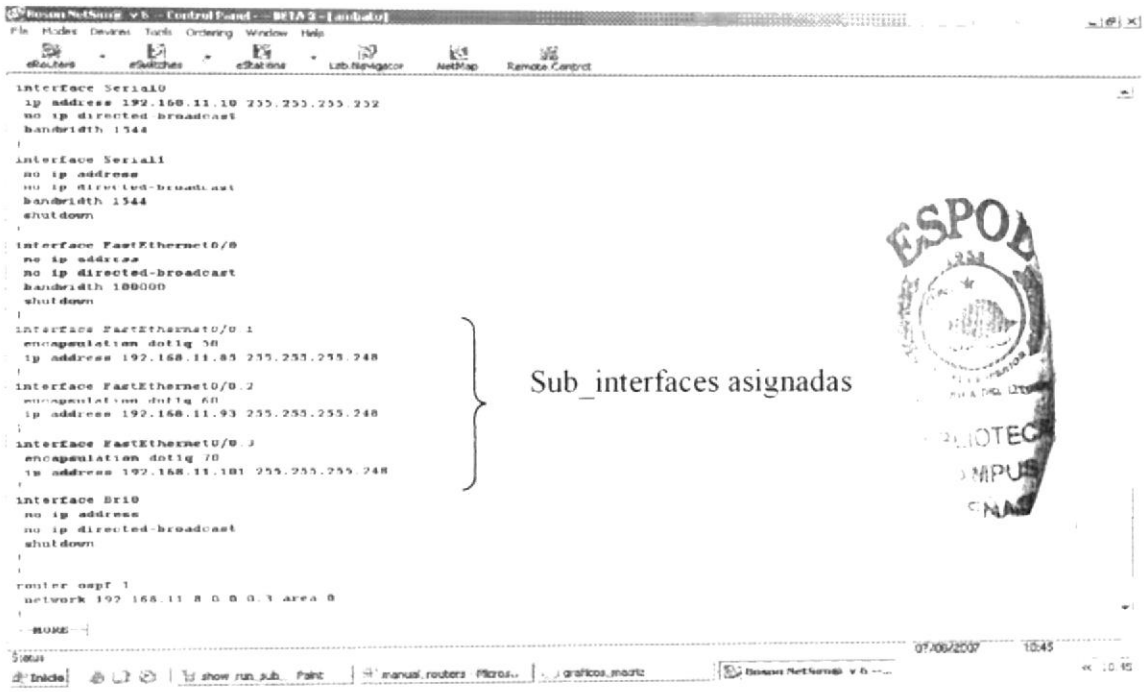


Figura 7-58: Show Run Ambato.

Ambato #show running-config

Mostrará el estado de todo el router con sus seriales e interfaces

Building configuration...

!

Version 12.1

Versión del Bios

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

Servicio de encriptación de contraseña no esta activo

!

hostname ambato

Nombre del router

enable secret 5 sdf6978yhg$jnb76sd

Indica que la contraseña de ingreso al switch se encuentra encriptada

enable password ambato

!

ip subnet-zero

!

interface Serial 0

Tipo de Serial

ip address 192.168.11.10 255.255.255.252

Dirección IP y máscara de sub-red de la serial

no ip directed-broadcast

bandwidth 1544

!

interface Serial 1

Tipo de Serial

ip address 192.168.11.9 255.255.255.252

Dirección IP y máscara de la serial

no ip directed-broadcast

bandwidth 1544

!

interface FastEthernet0/0

Tipo de Interfaz

ip address 192.168.11.13 255.255.255.248

Dirección IP y máscara de interfaz

no ip directed-broadcast

bandwidth 100000

!

interface FastEthernet0/0.1

Tipo de Sub-interfaz

encapsulation dot1q 50

Sub-interfaz

ip address 192.168.11.86 255.255.255.240

Dirección IP y máscara de la interfaz

!

interface FastEthernet0/0.2



Tipo de Sub-Interfaz

encapsulation dot1q 60

Sub-interfaz

ip address 192.168.11.94 255.255.255.240

Dirección IP y máscara de la interfaz

interface FastEthernet0/0.3

Tipo de Sub-Interfaz

encapsulation dot1q 70

Sub-interfaz

ip address 192.168.11.102 255.255.255.248

! **Dirección IP y máscara de la interfaz**

router ospf 1

Tipo de Protocolo

```
redistribute RIP
        Redistribulle el protocolo Rip
 network 192.168.11.8 0.0.0.3 area 0
!       Red y Willcard
ip classless
no ip http server
!
line con 0
 login
 transport input none
 password ambato
line aux 0
line vty 0 4
 login
 password ambato
!
no scheduler allocate
end.
```



7.18.3.9 SHOW IP ROUTE DE LA SUCURSAL AMBATO

ambato > enable

Ingresar al modo privilegiado

ambato # show ip route

Permite ver las conexiones del router.

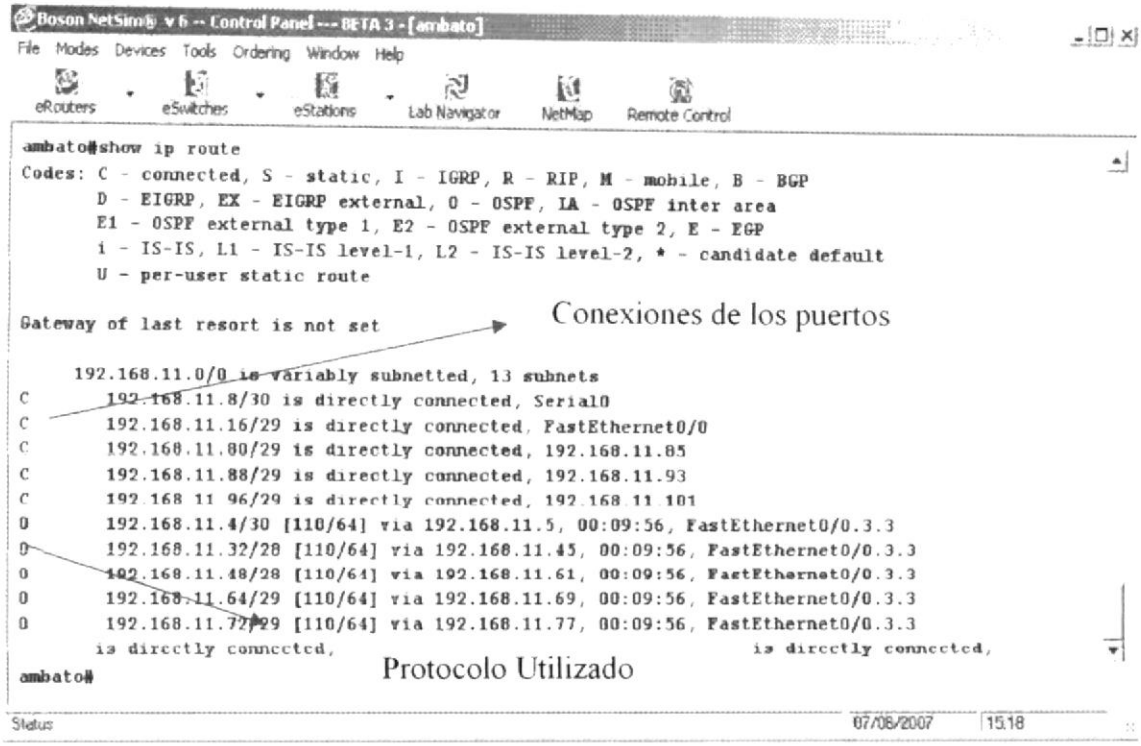
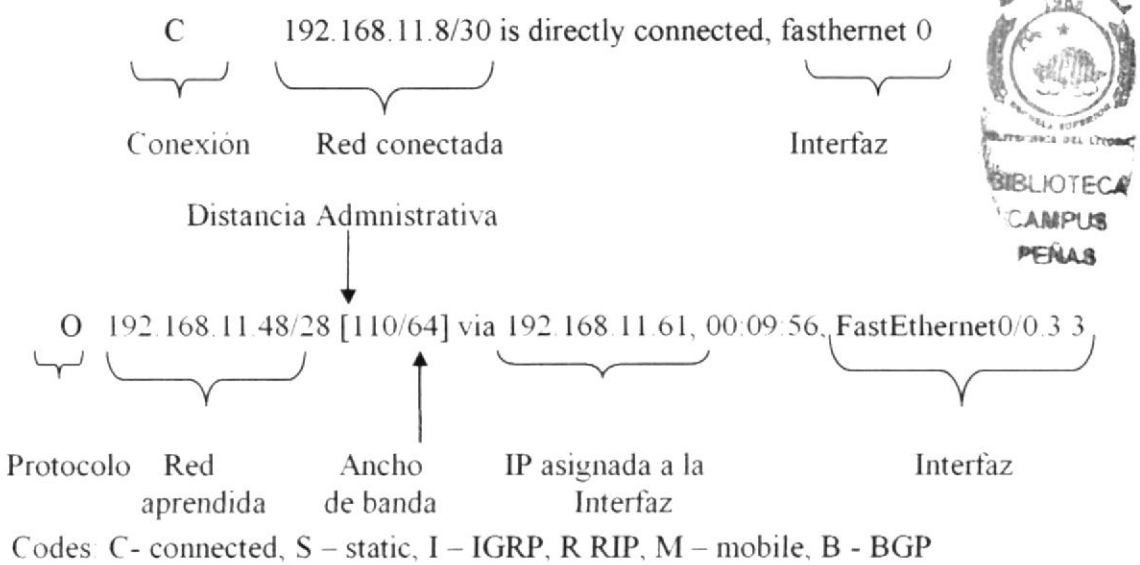


Figura 7-59: Show Ip Route Ambato.



ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

Comandos:

C – enlace conectado.

S – ruta estática.

I – protocolo de enrutamiento IGRP.

R – protocolo de enrutamiento RIP.

M – enlace con un teléfono móvil.

D – eigrp, ex – EIGRP external, O OSPF, IA – OSPF, IA – OSPF inter área.

D – protocolo de enrutamiento EIGRP.

EX – protocolo de enrutamiento EIGRP externo.

O – protocolo de enrutamiento OSPF.

IA - área interna del protocolo de enrutamiento OSPF.

ESPOL
BIBLIOTECA
CAMPUS

N1 OSPF NSSA external type 1, N" – OSPF NSSA external type 2.

N1 - protocolo de enrutamiento OSPF externo de Tipo 1 NSSA.

N2 - protocolo de enrutamiento OSPF externo de Tipo 2 NSSA.

E1 OSPF external type 1, E2 – OSPF external type 2, E – EGP.

E1 - protocolo de enrutamiento OSPF externo de Tipo 1.
E2 - protocolo de enrutamiento OSPF externo de Tipo 2.

I – IS-IS, su – IS-IS summary, L1 – IS-IS level – 1, L2 – IS – IS level – 2 ia – IS-IS area, * -candidate default, U – per-user static route o – ODR, P – periodic downloaded static route.

Puerta de enlace no seteada o grabada.

Gateway of last resort is not set.

7.18.3.10 SHOW INTERFACE SUCURSAL AMBATO

Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 192.168.11.10/30
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Serial1 is administratively down, line protocol is down
Hardware is HD64570
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0 is up, line protocol is up
Hardware is Lance, address is 000C.9596.5444 (bia 000C.9596.5444)
Internet address is 192.168.11.21/29
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
Auto-duplex, Auto Speed, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00

Fastethernet 0/0 levantada

BIBLIOTECA CAMPUS

```
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never.
Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.1 is up, line protocol is up
  Hardware is AmdFE, address is 000C.9596.5445 (bia 000C.9596.5445)
  Internet address is 192.168.11.85/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/0.2 is up, line protocol is up
  Hardware is AmdFE, address is 000C.9596.5445 (bia 000C.9596.5445)
  Internet address is 192.168.11.93/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/0.3 is up, line protocol is up
  Hardware is AmdFE, address is 000C.9596.5445 (bia 000C.9596.5445)
  Internet address is 192.168.11.101/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Time out 04:00:00
Bri0 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

Fastethernet 0/0.1 levantada

Fastethernet 0/0.2 levantada

Fastethernet 0/0.3 levantada



```
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets.
  0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Bri0:1 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Bri0:2 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out.
```



7.18.4 CONFIGURACIÓN DEL ROUTER SUCURSAL (QUITO)

7.18.4.1 ASIGNAR EL NOMBRE AL ROUTER SUCURSAL

Router>ena

Ingresar al modo privilegiado

Router>config terminal

Ingresar al config terminal

Router(config) # hostname quito

Asignar el nombre al router quito

quito (config) # ^Z

Salir del modo global

quito(config) # wr

Grabar los cambios

```
Router>ena
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname quito
quito(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

quito#wr
Building configuration...
[OK]

quito#
```

Figura 7-60: Nombre Router Sucursal Quito.



7.18.4.2 CREACIÓN DE CONTRASEÑAS

quito > enable

Ingresar al modo privilegiado

quito #configure terminal

Ingresar al modo de configuración global

quito (config)# line console 0

Ingresar a configurar la consola

quito (config-line)# password quito

Asignar una contraseña a la consola

quito (config-line)# login

Ingresar de contraseña

quito (config-line)# exit

Salir de la configuración de la consola

quito (config)# line vty 0 4

Ingresar a configurar la Terminal Virtual

quito (config-line)# password quito

Ingresar la contraseña a la Terminal Virtual

quito (config-line)# login

Petición de contraseña

quito (config)# enable password quito

Agregar una contraseña para ingresar al router

quito (config)# enable secret quito

Agregar una contraseña encriptada para ingresar al router

quito (config)# exit

Salir de la configuración global

quito # wr

Guardar los cambios

```
quito>ena
quito#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
quito(config)#line console 0
quito(config-line)#password quito
quito(config-line)#login
quito(config-line)#exit
quito(config)#line vty 0 4
quito(config-line)#password quito
quito(config-line)#login
quito(config-line)#exit
quito(config)#enable password quito
quito(config)#enable secret quito
quito(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

quito#wr
Building configuration...
[OK]


quito#
```

ESPOL BIBLIOTECA CAMPUS PEÑAS

Figura 7-61: Contraseña Router Quito.

7.18.4.3 CONFIGURACIÓN DE INTERFAZ SERIAL 0

quito > enable

Ingresar al modo privilegiado

quito #configure terminal

Ingresar al modo de configuración global

quito (config)# inter serial 0

Ingresar a la serial que se va a configurar

quito (config-if)# ip address 192.168.11.6 255.255.255.252

Ingresar la dirección IP con su respectiva máscara

192.168.11.6	DTE Serial 0
255.255.255.252	Máscara de Red



quito (config-if)# no shutdown

Levantar la dirección IP

quito (config-if)# exit

Salir de la interfaz serial

quito # wr

Grabar los cambios

```
quito>ena
quito#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
quito(config)#inter serial 0
quito(config-if)#ip address 192.168.11.6 255.255.255.252
quito(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
quito(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

quito#wr
Building configuration...
[OK]


quito#
```

Figura 7-62: IP interfaz Serial 0.

7.18.4.4 CONFIGURACIÓN DE FASTETHERNET 0/0

quito > enable

Ingresar al modo privilegiado

quito #configure terminal

Ingresar al modo de configuración global

quito (config)# interface fastethernet 0/0

Ingresar a la fastethernet

quito (config-if)# ip address 192.168.11.29 255.255.255.248

Ingresar la dirección IP con su respectiva máscara

192.168.11.29	IP Interfaz Serial 0
255.255.255.248	Máscara de Red



quito (config-if)# no shutdown

Levantar la dirección IP

quito (config-if)# exit

Salir de la interfaz serial

quito # wr

Grabar los cambios

```
quito>ena
quito#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
quito(config)#inter fastethernet 0/0
quito(config-if)#ip address 192.168.11.29 255.255.255.248
quito(config-if)#no shu
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
quito(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

quito#wr
Building configuration...
[OK]


quito#
```

Figura 7-63: Configuración Fasthernet 0/0.

7.18.4.5 CONFIGURACIÓN DE SUB-FASTETHERNET 0/0

quito > enable
Ingresar al modo privilegiado
quito #configure terminal
Ingresar al modo de configuración global
quito (config)# interface fastethernet 0/0.1
Ingresar a la sub- fastethernet
quito (config-subif)# ip address 192.168.11.109 255.255.255.248
Ingresar la dirección IP con su respectiva máscara

192.168.11.109	IP
255.255.255.248	Máscara de red

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

7.18.4.5.1 ENRUTAMIENTO VLAN 80.

quito (config-subif)# encapsulation dot1q 80
Encapsular el número de la vlan a crear
quito (config-subif)# no shutdown
Levantar la dirección IP
quito (config-subif)# exit
Salir de la sub- interfaz serial

```
quito>ena
quito#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
quito(config)#interface fastethernet 0/0.1
quito(config-subif)#ip address 192.168.11.109 255.255.255.248
quito(config-subif)#encapsulation dot1q 80
quito(config-subif)#no shutdown
quito(config-subif)#exit
```

Figura 7-64: Enrutamiento VLAN 80.

7.18.4.5.2 ENRUTAMIENTO VLAN 90

quito (config)# interface fastethernet 0/0.2
Ingresar a la sub- fastethernet
quito (config-subif)# ip address 192.168.11.117 255.255.255.248
Ingresar la dirección IP con su respectiva máscara

192.168.11.117	IP
255.255.255.248	Máscara de red

quito (config-subif)# encapsulation dot1q 90
Encapsular el número de la vlan a crear
quito (config-subif)# no shutdown
Levantar la dirección IP
quito (config-subif)# exit
Salir de la sub- interfaz serial

```
quito(config)#inter fastethernet 0/0.2
quito(config-subif)#ip address 192.168.11.117 255.255.255.248
quito(config-subif)#encapsulation dot1q 90
quito(config-subif)#no shutdown
quito(config-subif)#exit
```

Figura 7-65: Enrutamiento VLAN 90.

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.18.4.5.3 ENRUTAMIENTO VLAN 100

quito (config)# interface fastethernet 0/0.3
Ingresar a la sub- fastethernet
quito (config-subif)# ip address 192.168.11.125 255.255.255.248
Ingresar la dirección IP con su respectiva máscara

192.168.11.125	IP
255.255.255.248	Máscara de red
255.255.255.249	

quito (config-subif)# encapsulation dot1q 100
Encapsular el número de la vlan a crear
quito (config-subif)# no shutdown
Levantar la dirección IP
quito (config-subif)# exit
Salir de la interfaz serial

quito # wr

Grabar los cambios

```
quito(config)#inter fastethernet 0/0.3
quito(config-subif)#ip address 192.168.11.125 255.255.255.248
quito(config-subif)#encapsulation dot1q 100
quito(config-subif)#no shutdown
quito(config-subif)#exit
```

Figura 7-66: Enrutamiento VLAN 100.

7.18.4.6 CONFIGURACIÓN DEL PROTOCOLO OSPF

quito > enable

Ingresar al modo privilegiado

quito #configure terminal

Ingresar al modo de configuración global

quito (config)# router ospf 1

Habilitar el protocolo de enrutamiento a configurar

quito (config-router)# network 192.168.11.4 0.0.0.3 area 0

Asignar la dirección de la red, wildcard y área respectiva

Network	Comando
192.168.11.4	Red
0.0.0.3	Willcard
Área 0	Tipo de área

Al mismo tiempo configurar la distribución del protocolo de enrutamiento RIP

quito (config-router)# redistribute rip

Distribuir OSPF hacia las redes de RIP

quito (config-if)# ^Z

quito # wr

Grabar los cambios




```
quito>ena
quito#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
quito(config)#router ospf 1
quito(config-router)#network 192.168.11.4 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#
```

Figura 7-67: Protocolo OSPF QUITO.

7.18.4.7 SHOW PROTOCOLS DE LA SUCURSAL QUITO

quito > enable

Ingresar al modo privilegiado

quito # show protocols

Permite ver el estado de los puertos.

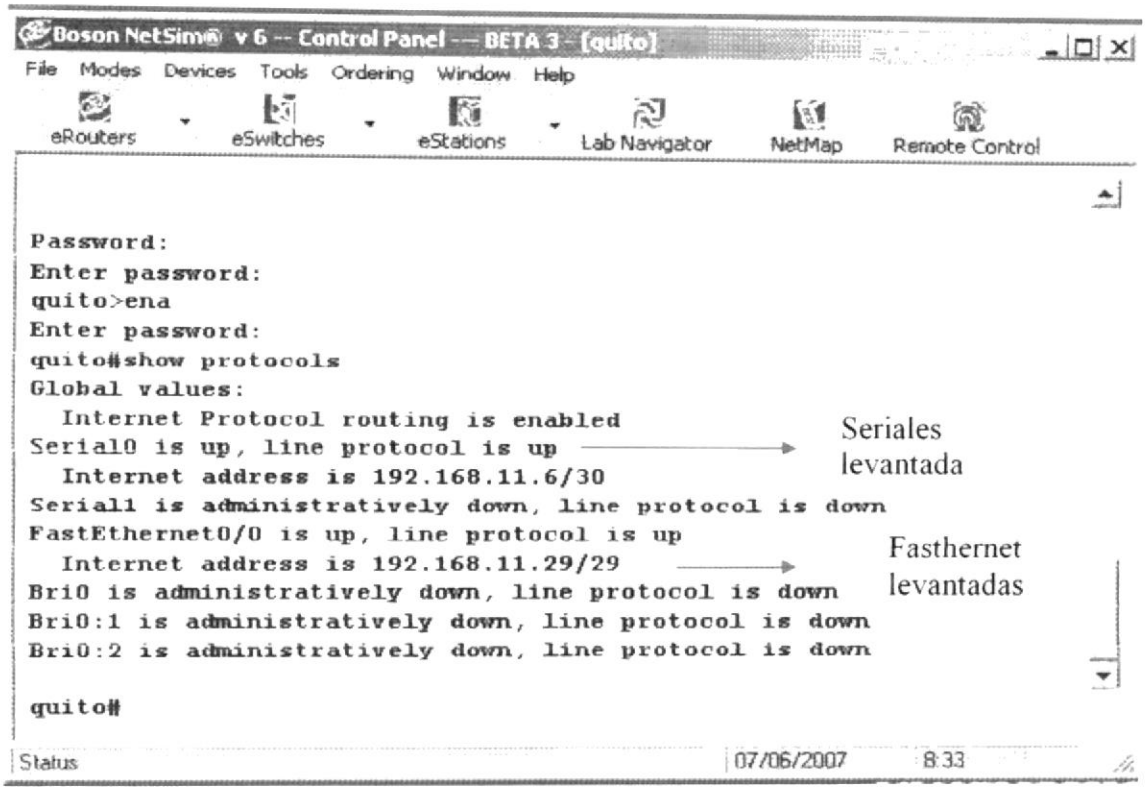


Figura 7-68: Show Protocols Quito.

Serial 0 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.11.6/30

IP asignada al puerto serial del router

Serial 1 is administratively down, Line protocol is down

Indica que no se asignado ninguna IP al puerto serial

Fasthernet 0/0 is up, Line protocol is up

Indica el serial levantado

Internet address is 192.168.11.29/29

IP asignada al puerto del Switch

7.18.5. SHOW RUN DE LA SUCURSAL QUITO

quito > enable

Ingresar al modo privilegiado

quito # show running-config

Permite ver todas las configuraciones IP y protocolos utilizados en el router.

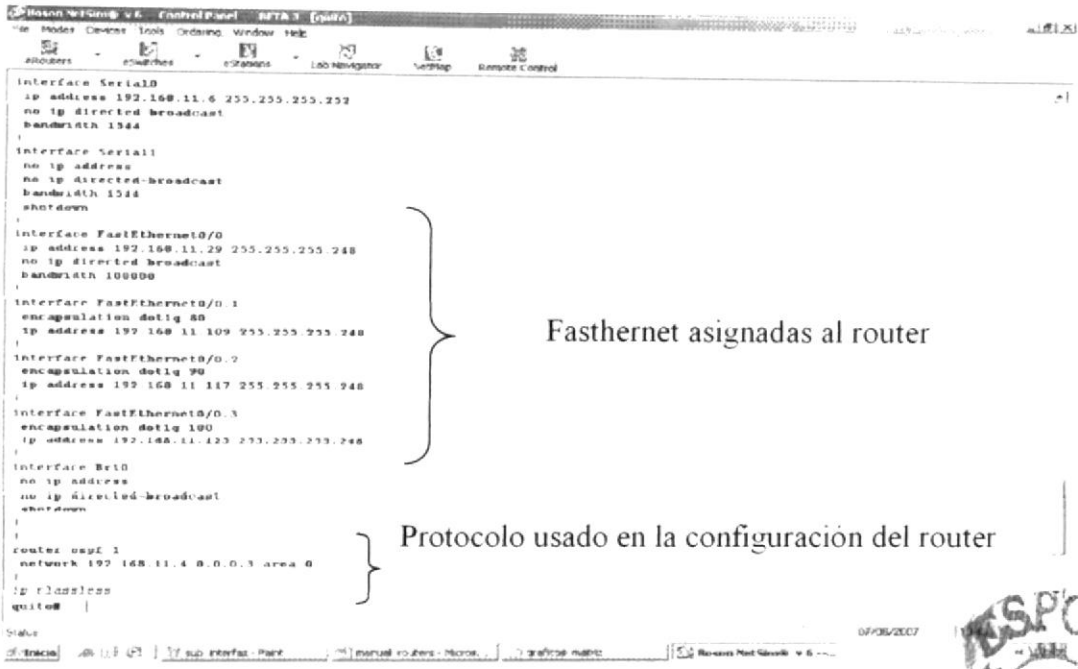


Figura 7-69: Show Run Quito.

ESPOL BIBLIOTECA CAMPUS PEÑAS

Quito #show running-config

Mostrará el estado de todo el router con sus seriales e interfaces

Building configuration...

!

Version 12.1

Versión del Bios

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

Servicio de encriptación de contraseña no esta activo

hostname quito

Nombre del router

enable secret 5 sdf6978yhg$jnb76sd

Indica que la contraseña de ingreso al switch se encuentra encriptada

enable password quito

!

```
ip subnet-zero
!
interface Serial 0
```

Tipo de Serial

```
ip address 192.168.11.6 255.255.255.252
```

Dirección IP y máscara de sub-red de la serial

```
 no ip directed-broadcast
 bandwidth 1544
!
interface FastEthernet0/0
```

Tipo de Interfaz

```
 ip address 192.168.11.29 255.255.255.248
```

Dirección IP y máscara de interfaz

```
 no ip directed-broadcast
 bandwidth 100000
!
interface FastEthernet0/0.1
```

Tipo de Sub-Interfaz

```
 encapsulation dot1q 80
```

Sub-interfaz

```
 ip address 192.168.11.110 255.255.255.240
!
```

Dirección IP y máscara de la interfaz

```
interface FastEthernet0/0.2
```

Tipo de Sub-interfaz

```
 encapsulation dot1q 90
```

Sub-interfaz

```
 ip address 192.168.11.118 255.255.255.240
!
```

Dirección IP y máscara de la interfaz

```
interface FastEthernet0/0.3
```



Tipo de Sub-Interfaz

```
 encapsulation dot1q 100
```

Sub-interfaz

```
 ip address 192.168.11.126 255.255.255.248
!
```

Dirección IP y máscara de la interfaz

```
router ospf 1
```

Tipo de Protocolo

```
 redistribute RIP
```

Redistribulle el protocolo Rip

```
 network 192.168.11.4 0.0.0.3 area 0
!
```

Red y Willcard

```
ip classless
no ip http server
!
```

```
line con 0
 login
 transport input none
 password quito
line aux 0
line vty 0 4
 login
 password quito
!
no scheduler allocate
end
```



7.18.5.1 SHOW IP ROUTE DE LA SUCURSAL QUITO

quito > enable

Ingresar al modo privilegiado

quito # show ip route

Permite ver las conexiones del router.

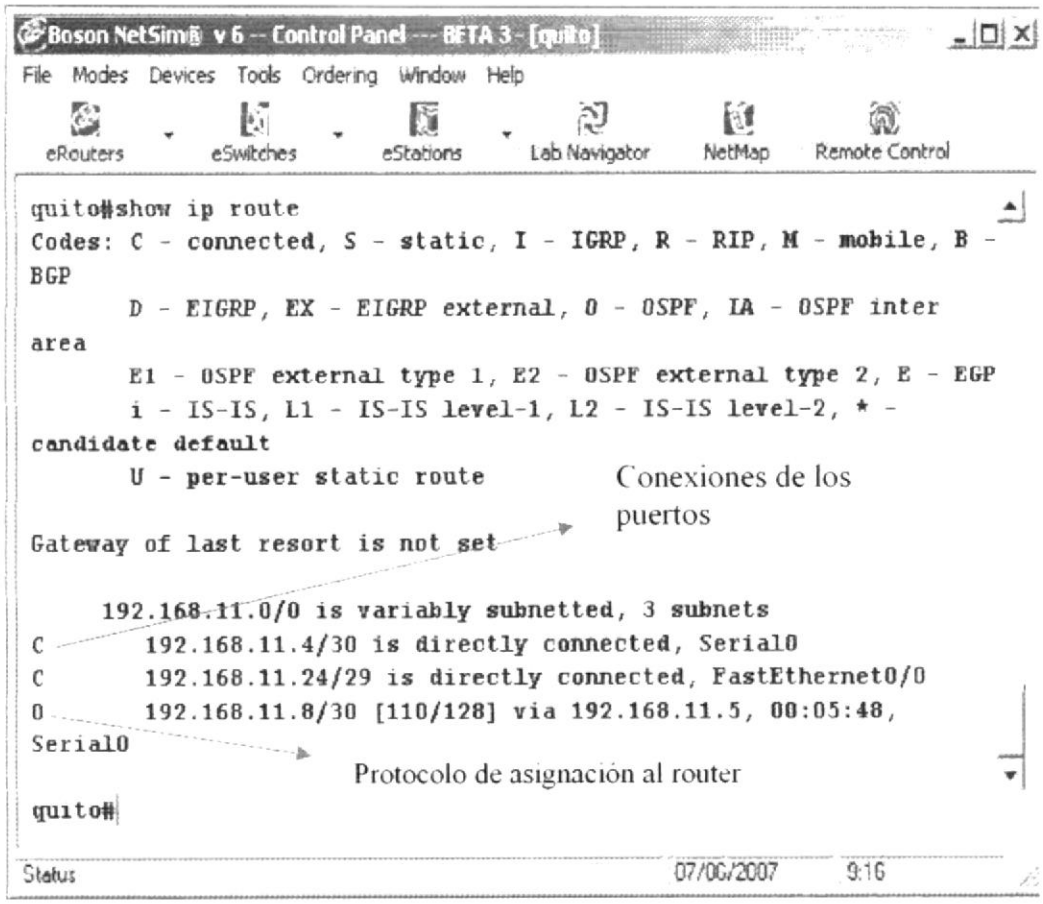
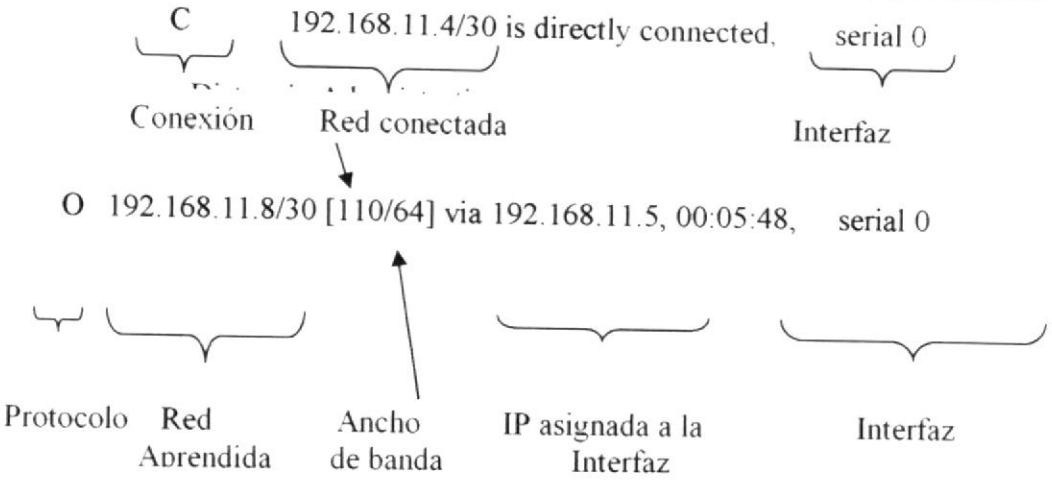


Figura 7-70: Show Ip Route de Quito.



Codes: C- connected, S – static, I – IGRP, R RIP, M – mobile, B - BGP

Comandos:

C – enlace conectado. Distancia Admnistrativa

S – ruta estática.

I – protocolo de enrutamiento IGRP.

R – protocolo de enrutamiento RIP.

M – enlace con un teléfono móvil.



D – eigrp, ex – EIGRP external, O OSPF, IA – OSPF, IA – OSPF inter área.

D – protocolo de enrutamiento EIGRP.

EX – protocolo de enrutamiento EIGRP externo.

O – protocolo de enrutamiento OSPF.

IA - área interna del protocolo de enrutamiento OSPF.

N1 OSPF NSSA external type 1, N" – OSPF NSSA external type 2.

N1 - protocolo de enrutamiento OSPF externo de Tipo 1 NSSA.

N2 - protocolo de enrutamiento OSPF externo de Tipo 2 NSSA.

E1 OSPF external type 1, E2 – OSPF external type 2, E – EGP.

E1 - protocolo de enrutamiento OSPF externo de Tipo 1.

E2 - protocolo de enrutamiento OSPF externo de Tipo 2.

I – IS-IS, su – IS-IS summary, L1 – IS-IS level – 1, L2 – IS – IS level – 2 ia – IS-IS area, * -candidate default, U – per-user static route o – ODR, P – periodic downloaded static route.

Puerta de enlace no seteada o grabada.

Gateway of last resort is not set

7.18.5.2 SHOW INTERFACE SUCURSAL QUITO

Serial 0 levantada

```
quito#
quito#show interfaces
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.11.6/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial1 is administratively down, line protocol is down
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
```

ESPOL BIBLIOTECA CAMPUS PEÑAS

```
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0 is up, line protocol is up
  Hardware is Lance, address is 000C.8385.5044 (bia 000C.8385.5044)
  Internet address is 192.168.11.29/29
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.1 is up, line protocol is up
  Hardware is AmdFE, address is 000C.8385.5045 (bia 000C.8385.5045)
  Internet address is 192.168.11.109/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec).
Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/0.2 is up, line protocol is up
  Hardware is AmdFE, address is 000C.8385.5045 (bia 000C.8385.5045)
  Internet address is 192.168.11.117/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
FastEthernet0/0.3 is up, line protocol is up
  Hardware is AmdFE, address is 000C.8385.5045 (bia 000C.8385.5045)
  Internet address is 192.168.11.125/29
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
Bri0 is administratively down, line protocol is down
```

Fastethernet 0/0 levantada

Fastethernet 0/0.1 levantada

Fastethernet 0/0.3 levantada



```
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Bri0:1 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns.
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Bri0:2 is administratively down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW  Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```



0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

quito#
quito#

7.19 CONFIGURACIÓN DE SWITCH MATRIZ

7.19.1 CONFIGURACIÓN DE SWITCH MATRIZ

7.19.1.1 ASIGNACIÓN DE NOMBRE AL SWITCH



Switch>ena
Ingresar al modo privilegiado
Switch#>config terminal
Ingresar al config terminal
Switch (config) # hostname matriz
Asignar el nombre al router matriz
matriz(config) # copy r startup-config
Grabar los cambios

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname matriz
matriz(config)#exit
matriz#copy r startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

matriz#
```

Figura 7-71: Asignación Nombre Switch Matriz

7.19.1.2 CREACIÓN DE VLAN´S.

matriz # vlan database
Ingresar a la base de datos del switch
matriz (vlan) # vlan 10 name RR.HH
Asignación un número referencial y un nombre a la Vlan's que se va a crear

matriz (vlan) # vlan 20 name cobranza

Asignación un número referencial y un nombre a la Vlan's que se va a crear

matriz (vlan) # vlan 30 name ventas

Asignación un número referencial y un nombre a la Vlan's que se va a crear

matriz (vlan) # vlan 40 name compras

Asignación un número referencial y un nombre a la Vlan's que se va a crear

matriz (vlan) #exit

Salir del vlan database

matriz #copy r startup-config

Guardar los cambios en el switch

Vlan	Comando
10	Número de Vlan
Name	Parámetro
Cobranza	Dpto. Matriz




```
matriz#vlan database
matriz(vlan)#vlan 10 name R.R.H.H
VLAN 10 added:
    Name:R.R.H.H
matriz(vlan)# vlan 20 name cobranzas
VLAN 20 added:
    Name:cobranzas
matriz(vlan)# vlan 30 name ventas
VLAN 30 added:
    Name:ventas
matriz(vlan)#vlan 40 name compras
VLAN 40 added:
    Name:compras
matriz(vlan)#exit
APPLY completed.
Exiting....
matriz#copy r startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

matriz#
```

Figura 7-72: Creación VLAN.

7.19.1.3 ASIGNACIÓN DE PUERTO A LA VLAN

matriz # config terminal
Ingresar a la Configuración global
matriz (config) # interface fastethernet 0/1
matriz (config-if) # switchport mode trunk
Truncar el puerto
matriz (config-if) # exit

```
Switch#config ter
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)#exit
```

Figura 7-73: Interface Fasthernet 0/1.

matriz (config) # interface fastethernet 0/2
Ingresar a fastethernet
matriz (config-if) # switchport access vlan 10
Asignar la vlan 10 al puerto 0/2
matriz (config-if) # exit

ESPOL BIBLIOTECA CAMPUS PEÑAS

```
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

Figura 7-74: Interface Fasthernet 0/2.

matriz (config) # interface fastethernet 0/3
Ingresar a fastethernet
matriz (config-if) # switchport access vlan 20
Asignar la vlan 10 al puerto 0/3
matriz (config-if) # exit

```
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

Figura 7-75: Interface Fasthernet 0/3.

matriz (config) # interface fastethernet 0/4
Ingresar a fastethernet
matriz (config-if) # switchport access vlan 30
Asignar la vlan 10 al puerto 0/4
matriz (config-if) # exit

```
Switch(config)#interface fastethernet 0/4
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
```

Figura 7-76: Interface Fasthernet 0/4.

matriz (config) # interface fastethernet 0/5
Ingresar a fastethernet
matriz (config-if) # switchport access vlan 40
Asignar la vlan 10 al puerto 0/5
matriz (config-if) # exit

```
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport access vlan 40
Switch(config-if)#exit
```

Figura 7-77: Interface Fasthernet 0/5.

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.19.1.4 SHOW VLAN MATRIZ

matriz # show vlan

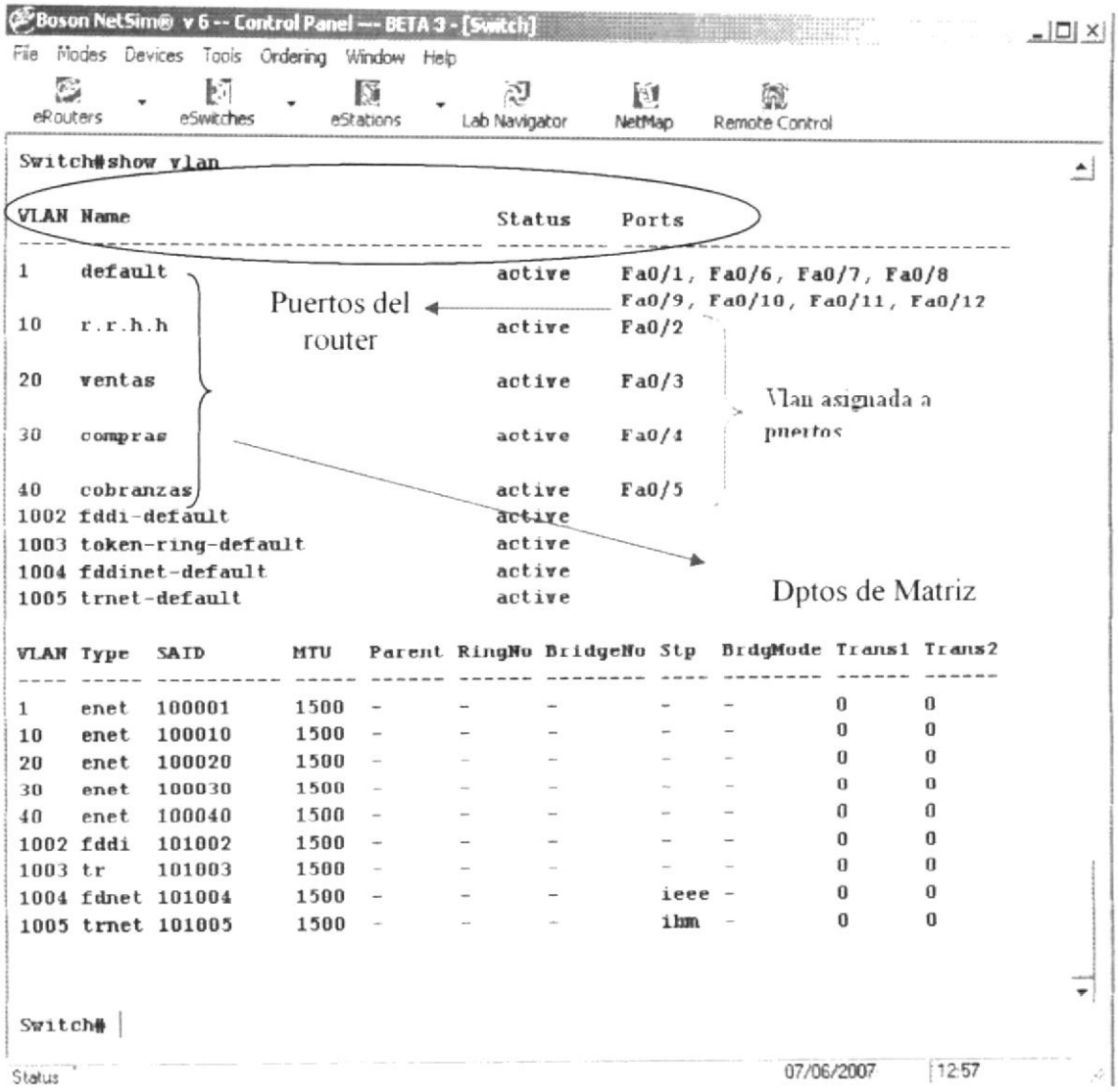


Figura 7-78: Show Vlan Matriz

VLAN.- Es el número 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

ESPOL
BIBLIOTECA
CAMPUS
PEÑAS

7.19.1.5 SHOW RUN VLAN MATRIZ

```
matriz#show run
!
Version 12.1
```

Version del Bios

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname matriz
```

Nombre del switch

```
ip name-server 0.0.0.0
!
!
!
ip subnet-zero
!
!
!
!
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
 switchport mode trunk
 bandwidth 100000
!
interface FastEthernet0/2
 switchport access vlan 10
 bandwidth 100000
!
interface FastEthernet0/3
 switchport mode access
 switchport access vlan 20
 bandwidth 100000
!
interface FastEthernet0/4
 switchport mode access
 switchport access vlan 30
 bandwidth 100000
!
interface FastEthernet0/5
 switchport mode access
 switchport access vlan 40
 bandwidth 100000
```

Vlan asignadas a los puertos

ESPOL BIBLIOTECA CAMPUS PEÑAS

```
interface FastEthernet0/6
 bandwidth 100000
!
interface FastEthernet0/7
 bandwidth 100000
!
interface FastEthernet0/8
 bandwidth 100000
!
interface FastEthernet0/9
 bandwidth 100000
!
interface FastEthernet0/10
 bandwidth 100000
!
interface FastEthernet0/11
 bandwidth 100000
!
interface FastEthernet0/12
 bandwidth 100000
!
 vtp Server
 vtp domain bigdomain
interface Vlan 1
 no ip address
 no ip route-cache
 shutdown

vlan 10 name R.R.H.H

vlan 20 name cobranzas

vlan 30 name ventas

vlan 40 name compras
!
ip classless
no ip http server
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end.
```

Vlan Creadas con sus respectivos números y nombres



7.19.1.6 ASIGNACIÓN DE IP A LAS PC DE MATRIZ

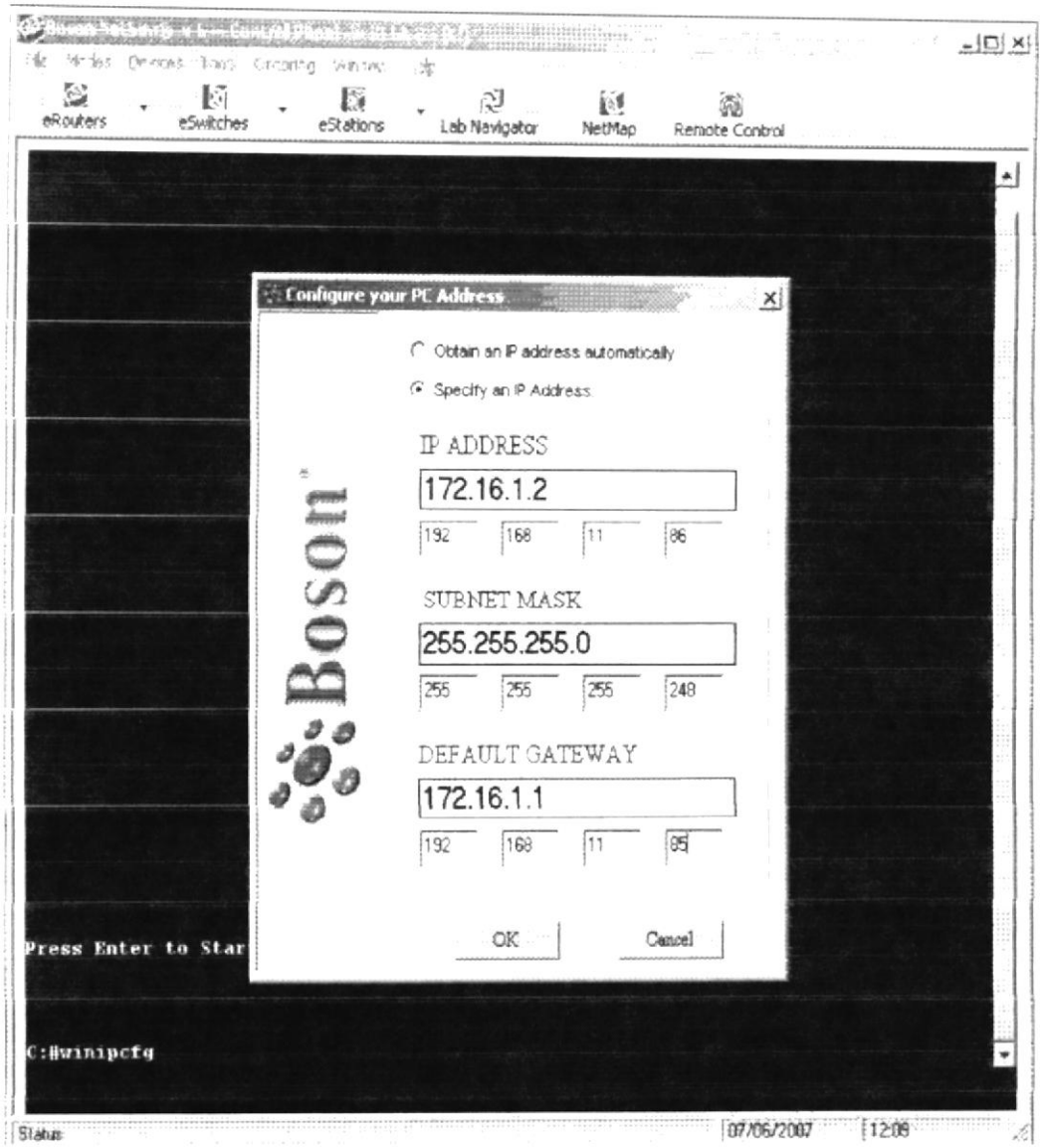


Figura 7-79: Asignación de Ip Matriz

ESPOL
BIBLIOTECA
CAMPUS

7.19.2 CONFIGURACIÓN DEL SWITCH SUCURSAL AMBATO

7.19.2.1 ASIGNACIÓN DE NOMBRES EN EL SWITCH AMBATO

Switch#configure terminal

Ingresar al modo de configuración global

Switch (config)#hostname ambato_2

Sirve para asignarle un nombre al Peñas_1 (Peñas1)

ambato_2(config)# ^ Z

Salir de la configuración global del router.

ambato_2(config)# copy r startup-config

Grabar los cambios hechos en el router.

```
Switch#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname ambato
ambato(config)#exit
ambato#copy r startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

ambato#
```

Figura 7-80: Asignación Nombre Switch Ambato.

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.19.2.2 CREACIÓN DE VLAN'S EN EL SWITCH AMBATO

ambato_2(config)# vlan database

Ingresar al modo de configuración de vlan's

ambato_2(config)#Vlan 50 name contabilidad

Asignación un número referencial y un nombre a la Vlan's que se va a crear

ambato_2(config)# (Vlan)#Vlan 60 name finanzas

Asignación un número referencial y un nombre a la Vlan's que se va a crear

ambato_2(config)# (Vlan)#Vlan 70 name sistemas.

Asignación un número referencial y un nombre a la Vlan's que se va a crear

ambato_2# copy r startup-config

Grabar los cambios hechos en el router.

Vlan	Comando
10	Número de Vlan
Name	Parámetro
Sistemas	Dpto. Ambato

```
ambato#vlan database
ambato(vlan)#vlan 50 name contabilidad
VLAN 50 added:
    Name:contabilidad
ambato(vlan)# vlan 60 name finanzas
VLAN 60 added:
    Name:finanzas
ambato(vlan)#vlan 70 name sistemas
VLAN 70 added:
    Name:sistemas
APPLY completed.
Exiting....
ambato#copy r startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figura 7-81: Creación VLAN Ambato.

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.19.2.3 ASIGNACIÓN DE VLAN'S A LOS PUERTOS

ambato_2#configure terminal

Ingresar al modo de configuración global

ambato_2 (config)#interface fastethernet 0/1

Ingresar a la interfaz puerto que se va a configurar

ambato_2 (config-if)#switchport mode trunk

Truncar el puerto de conexión con el router.

ambato_2 (config-if)# exit

Salir de la configuración de la fasthernet del switch

```
Switch#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#inter fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Figura 7-82: Interfcae Fasthernet 0/1.

ambato_2 (config)#interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

ambato_2 (config-if)#switchport access Vlan 50

Asignar el puerto a la Vlan 50

ambato_2 (config-if)#exit

Salir de la configuración de la fasthernet del switch

```
Switch(config)#inter fastethernet 0/2
Switch(config-if)#switchport access vlan 50
Switch(config-if)#exit
```

Figura 7-83:Interfcae Fasthernet 0/2.

ESPOL BIBLIOTECA CAMPUS PEÑAS

ambato_2 (config)#interface fastethernet 0/3

Ingresar a la interfaz puerto que se va a configurar

ambato_2 (config-if)#switchport access vlan 60

Asignar el puerto a la Vlan 60

ambato_2 (config-if)# exit

Salir de la configuración de la fasthernet del switch

```
Switch(config)#inter fastethernet 0/3
Switch(config-if)#switchport access vlan 60
Switch(config-if)#exit
```

Figura 7-84: Interfcae Fasthernet 0/3.

ambato_2 (config)#interface fastethernet 0/4

Ingresar a la interfaz puerto que se va a configurar

ambato_2 (config-if)#switchport access vlan 70

Asignar el puerto a la Vlan 70

ambato_2 (config-if)# exit

Salir de la configuración global.

ambato_2# copy r Startup-config

Guardar la configuración realizada en el switch.

```
Switch(config)#inter fastethernet 0/4
Switch(config-if)#switchport access vlan 70
Switch(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy r startup-config
Destination filename [startup-config]?
Building configuration...
[OK]


Switch#
```

Figura 7-85:Interfcae Fasthernet 0/4.



7.19.2.4 SHOW VLAN AMBATO

ambato_2>enable

Ingresar al modo privilegiado

ambato_2# show vlan

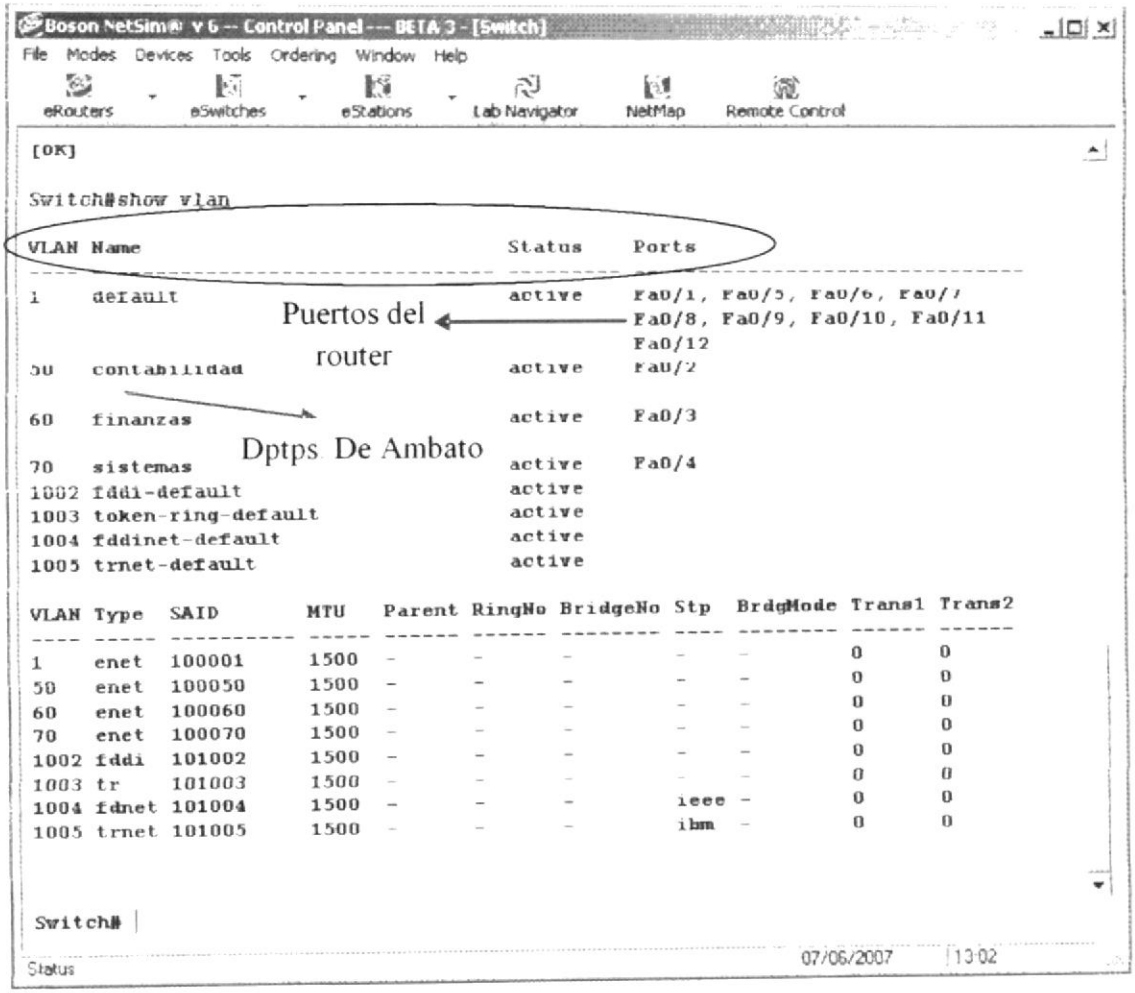


Figura 7-86: Show Vlan Ambato.

VLAN.- Es el número 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

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.19.2.5 SHOW RUN AMBATO

```
ambato#show run
!
Version 12.1
```

Versión del Bios

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ambato
```

Nombre del switch

```
ip name-server 0.0.0.0
!
!
!
ip subnet-zero
!
!
!
!
!
!
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
 switchport mode trunk
 bandwidth 100000
!
interface FastEthernet0/2
 switchport access vlan 50
 bandwidth 100000
!
interface FastEthernet0/3
 switchport access vlan 60
 bandwidth 100000
!
interface FastEthernet0/4
 switchport access vlan 70
 bandwidth 100000
!
interface FastEthernet0/5
 bandwidth 100000
!
interface FastEthernet0/6
```

Vlan asignadas a los puertos

ESPOL BIBLIOTECA CAMPUS PEÑAS

```
 bandwidth 100000
!
interface FastEthernet0/7
 bandwidth 100000
!
interface FastEthernet0/8
 bandwidth 100000
!
interface FastEthernet0/9
 bandwidth 100000
!
interface FastEthernet0/10
 bandwidth 100000
!
interface FastEthernet0/11
 bandwidth 100000
!
interface FastEthernet0/12
 bandwidth 100000
!
 vtp Server
 vtp domain bigdomain
interface Vlan 1
 no ip address
 no ip route-cache
 shutdown

vlan 50 name contabilidad

vlan 60 name finanzas

vlan 70 name sistemas
!
ip classless
no ip http server
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end.
```



Vlan Creadas con sus respectivos números y nombres

7.19.2.6 ASIGNACIÓN DE IP A LAS PC DE AMBATO

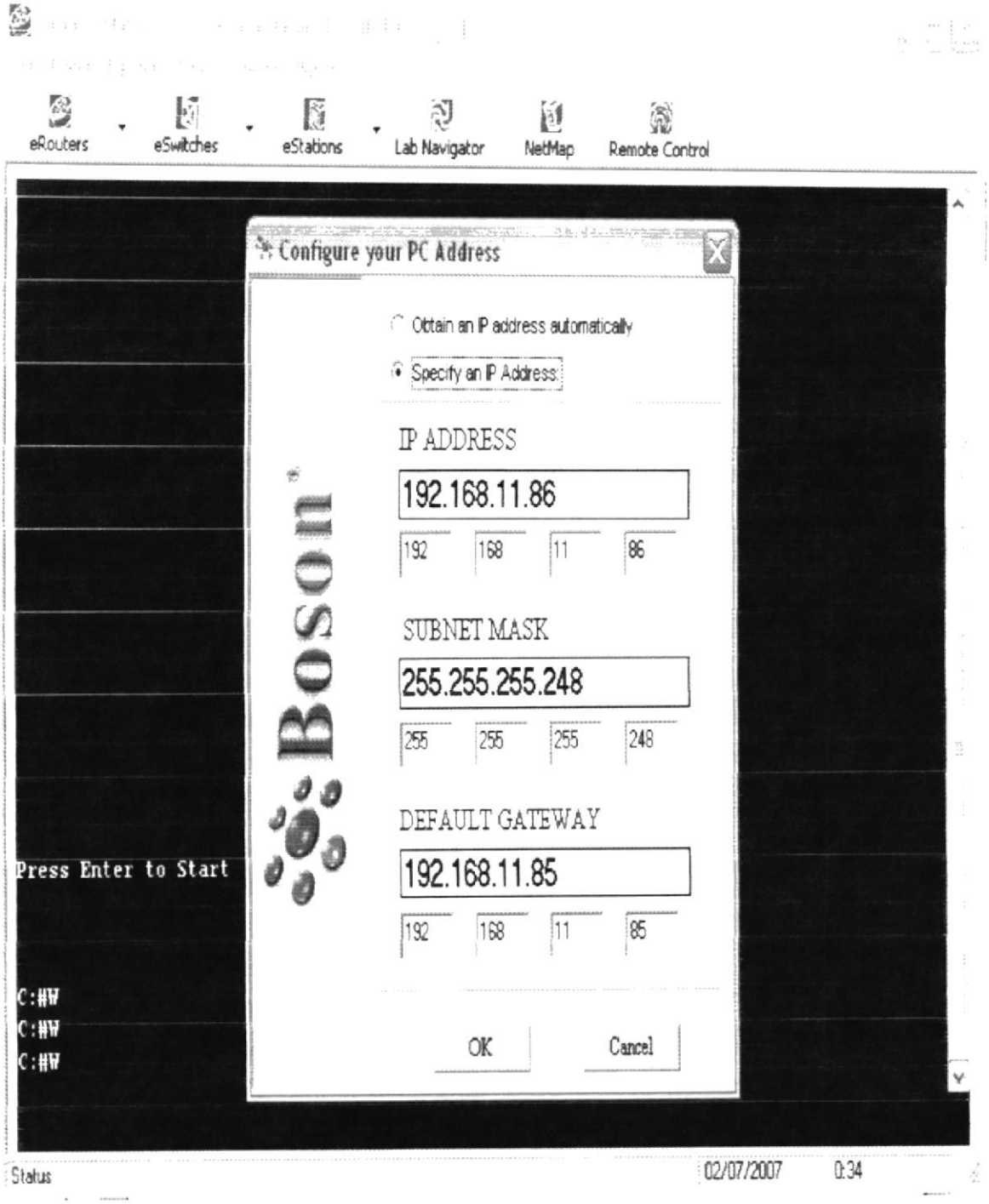


Figura 7-87: Show Vlan Ambato.

ESPOL BIBLIOTECA CAMPUS

7.19.3 CONFIGURACIÓN DEL SWITCH EN LA SUCURSAL QUITO

7.19.3.1 ASIGNACIÓN DE NOMBRES EN EL SWITCH AMBATO

Switch>enable

Ingresar al modo privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch (config)#hostname quito

Sirve para asignarle un nombre al Peñas_1 (Peñas1)

quito (config)# ^ Z

Salir de la configuración global del router.

quito (config)# copy r startup-config

Grabar los cambios hechos en el router.

```
Switch#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname quito
quito(config)#exit
quito#copy r startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

quito#
```

Figura 7-88: Asignación Nombre Switch Ambato.



7.19.3.2 CREACIÓN DE VLAN'S EN EL SWITCH QUITO

quito (config)# vlan database
Ingresar al modo de configuración de vlan's

quito (config)#Vlan 80 name marketing
Asignar un número referencial y un nombre a la Vlan's que se va a crear.

quito (Vlan)#Vlan 90 name produccion
Asignar un número referencial y un nombre a la Vlan's que se va a crear.

quito (Vlan)#Vlan 100 name redes
Asignar un número referencial y un nombre a la Vlan's que se va a crear

quito (Vlan)# ^ Z
Salir de la configuración global del router.

quito# copy r startup-config
Grabar los cambios hechos en el router.

Vlan	Comando
10	Número de Vlan
Name	Parámetro
Sistemas	Dpto. Quito

```
quito#vlan database
quito(vlan)#vlan 80 name produccion
VLAN 80 added:
    Name:produccion
quito(vlan)#vlan 90 name redes
VLAN 90 added:
    Name:redes
quito(vlan)#vlan 100 name marketing
VLAN 100 added:
    Name:marketing
APPLY completed.
Exiting....
```

Figura 7-89: Creación de VLAN Switch Ambato.

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.19.3.3 ASIGNACIÓN DE VLAN'S A LOS PUERTOS

quito >enable

Ingresar al modo privilegiado

quito #configure terminal

Ingresar al modo de configuración global

quito (config)#interface fastethernet 0/1

Ingresar a la interfaz puerto que se va a configurar

quito (config-if)#switchport mode trunk

Truncar el puerto de conexión con el router.

quito (config-if)# exit

Salir de la configuración de la fasthernet del switch

```
quito#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
quito(config)#inter fastethernet 0/1
quito(config-if)#switchport mode trunk
quito(config-if)#exit
```

Figura 7-90: Interface Fasthernet 0/1.

quito (config)#interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

quito (config-if)#switchport access Vlan 80

Asignar el puerto a la Vlan 80

quito (config-if)#exit

Salir de la configuración de la fasthernet del switch

```
quito(config)#inter fastethernet 0/2
quito(config-if)#switchport access vlan 80
quito(config-if)#exit
```

BIBLIOTECA CAMPUS PEÑAS

Figura 7-91: Interface Fasthernet 0/2..

quito (config)#interface fastethernet 0/3
Ingresar a la interfaz puerto que se va a configurar

quito (config-if)#switchport access vlan 90
Asignar el puerto a la Vlan 90

quito (config-if)# exit
Salir de la configuración de la fasthernet del switch

```
quito(config)#inter fastethernet 0/3
quito(config-if)#switchport access vlan 90
quito(config-if)#exit
```

Figura 7-92: Interface Fasthernet 0/3.

quito (config)#interface fastethernet 0/4
Ingresar a la interfaz puerto que se va a configurar

quito (config-if)#switchport access vlan 100
Asignar el puerto a la Vlan 100

quito (config-if)# exit
Salir de la configuración del puerto

quito (config-)# exit
Salir del modo global
quito # copy r Startup-config
Guardar la configuración realizada en el switch.

```
quito(config)#inter fastethernet 0/4
quito(config-if)#switchport access vlan 100
quito(config-if)#exit
quito(config)#exit
quito#copy r startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

quito#
```

ESPOL
BIBLIOTECA
CAMPUS
PENAS

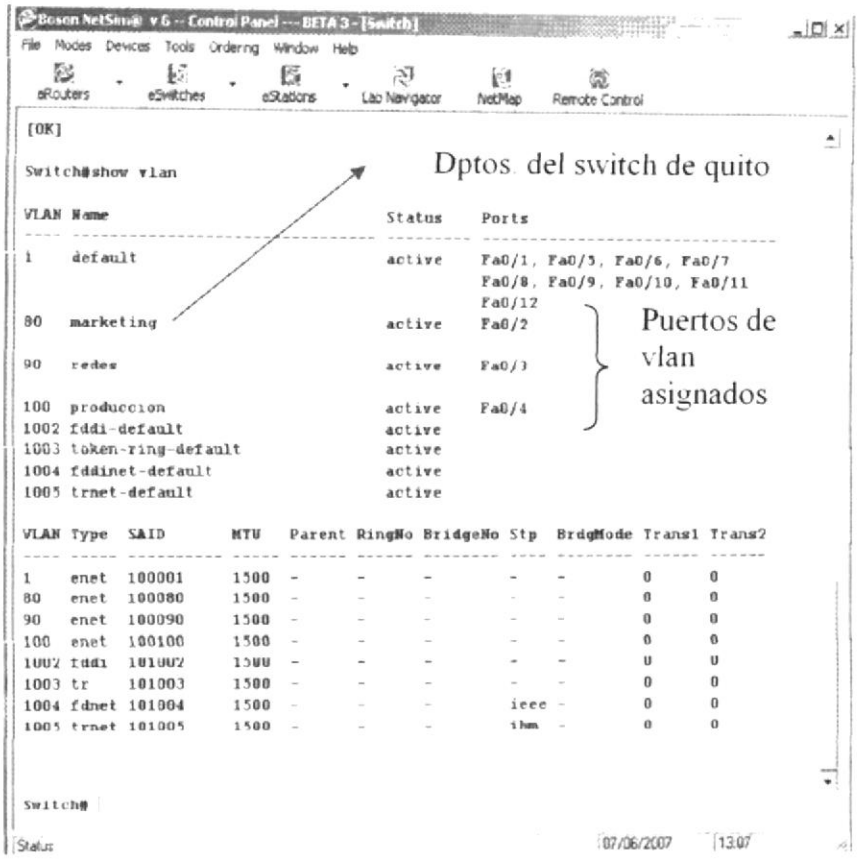
Figura 7-93: Interface Fasthernet 0/4

7.19.3.4 SHOW VLAN QUITO

quito >enable

Ingresar al modo privilegiado

quito # show vlan




```
[OK]

Switch#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                                   Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                   Fa0/12
80   marketing                           active    Fa0/2
90   redes                               active    Fa0/3
100  produccion                          active    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
80   enet  100080     1500  -      -      -        -    -        0      0
90   enet  100090     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Switch#
```

Figura 7-94: Show VLAN Quito.

7.19.3.5 SHOW RUN QUITO.

Name:marketing
APPLY completed.
Exiting....
quito#SHOW RUN
!
Version 12.1
Versión del Bios
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!

```
hostname quito
```

Nombre del switch

```
ip name-server 0.0.0.0
!
!
!
ip subnet-zero
!
!
!
!
!
!
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
 switchport mode trunk
 bandwidth 100000
!
interface FastEthernet0/2
 switchport access vlan 80
 bandwidth 100000
!
interface FastEthernet0/3
 switchport access vlan 90
 bandwidth 100000
!
interface FastEthernet0/4
 switchport access vlan 100
 bandwidth 100000
!
interface FastEthernet0/5
        bandwidth 100000

!
interface FastEthernet0/6
 bandwidth 100000
!
interface FastEthernet0/7
 bandwidth 100000
!
interface FastEthernet0/8
 bandwidth 100000
!
interface FastEthernet0/9
```

Vlan asignadas a los puertos

ESPOL BIBLIOTECA CAMPUS PEÑAS

```
 bandwidth 100000
!
interface FastEthernet0/10
 bandwidth 100000
!
interface FastEthernet0/11
 bandwidth 100000
!
interface FastEthernet0/12
 bandwidth 100000
!
 vtp Server
 vtp domain bigdomain
interface Vlan 1
 no ip address
 no ip route-cache
 shutdown

vlan 80 name produccion

vlan 90 name redes

vlan 100 name marketing
!
ip classless
no ip http server
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end
```

Vlan Creadas con sus respectivos números y nombres

ESPOL BIBLIOTECA CAMPUS

7.20 PRUEBAS DE COMUNICACIONES ENTRE ROUTER

7.20.1 MATRIZ

7.20.1.1 COMUNICACIÓN MATRIZ-AMBATO

Press Enter to Start



matriz#
matriz#ping 192.168.11.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
matriz#

7.20.1.2 COMUNICACIÓN MATRIZ-QUITO

Press Enter to Start

matriz#
matriz#ping 192.168.11.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
matriz#

7.20.1.3 COMUNICACIÓN R:R:H:H-COBRANZAS

Press Enter to Start

C:#ping 192.168.11.78
Pinging 192.168.11.78 with 32 bytes of data:

Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.78: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.20.1.4 COMUNICACIÓN VENTAS–SISTEMAS

Press Enter to Start

C:#
C:#ping 192.168.11.102
Pinging 192.168.11.102 with 32 bytes of data:

Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.102: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.20.1.5 COMUNICACIÓN COMPRAS–REDES



Press Enter to Start

C:#
C:#ping 192.168.11.118
Pinging 192.168.11.118 with 32 bytes of data:

Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.118: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.20.2 AMBATO

7.20.2.1 COMUNICACIÓN AMBATO-MATRIZ

matriz#
matriz#ping 192.168.11.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
matriz#



7.20.2.2 COMUNICACIÓN AMBATO-QUITO

Press Enter to Start

matriz#
matriz#ping 192.168.11.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
matriz#

7.20.2.3 COMUNICACIÓN FINANZAS-SISTEMAS

C:#
C:#ping 192.168.11.102
Pinging 192.168.11.102 with 32 bytes of data:

Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.102: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.20.2.4 COMUNICACIÓN CONTABILIDAD-COBRANZAS

Press Enter to Start
C:#
C:#ping 192.168.11.78
Pinging 192.168.11.78 with 32 bytes of data:

Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.78: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.20.3 QUITO

7.20.3.1 COMUNICACIÓN QUITO-MATRIZ



Press Enter to Start

matriz#ping 192.168.11.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
matriz#

7.20.3.2 COMUNICACIÓN QUITO-AMBATO

Press Enter to Start

matriz#
matriz#ping 192.168.11.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
matriz#

7.20.3.3 COMUNICACIÓN PRODUCCIÓN-REDES

Press Enter to Start

C:#ping 192.168.11.118
Pinging 192.168.11.118 with 32 bytes of data:
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241
Reply from 192.168.11.118: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.118: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.20.3.4 COMUNICACIÓN REDES-SISTEMAS



Press Enter to Start
C:#ping 192.168.11.102
Pinging 192.168.11.102 with 32 bytes of data:
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241
Reply from 192.168.11.102: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.102: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.20.3.5 COMUNICACIÓN MARKETING-COBRANZAS

C:#ping 192.168.11.78
Pinging 192.168.11.78 with 32 bytes of data:

Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241
Reply from 192.168.11.78: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.11.78: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

7.21 ACL (EXTENDIDA)

7.21.1 BLOQUEO DE PING

7.21.1.1 CONFIGURACIÓN DE IP ACCESS-GROUP

matriz > enable

Ingresar al modo privilegiado

matriz # configure terminal

Ingresar al modo de configuración global

matriz(config)#interface serial 1/1

Ingresar al serial donde quiere bloquear el puerto

matriz(config-if)#ip access-group 102 in

Crear el grupo de trabajo el cual permite verificar la clase de acl.

Matriz(config-if))#exit

Salir de la interface del serial




```
matriz#ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#interface serial 1/1
matriz(config-if)#ip access-group 102 in
matriz(config-if)#exit
```

Figura 7-95: Access Group Serial 1/1.

matriz(config)#interface serial 1/2

Ingresar al serial donde quiere bloquear el puerto

matriz(config-if)#ip access-group 103 in

Crear el grupo de trabajo el cual permite verificar la clase de acl.

Matriz(config-if)#^Z

matriz#wr

Grabar los cambios hechos.

```
matriz#ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#inter serial 1/2
matriz(config-if)#ip access-group 103 in
matriz(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]
```

Figura 7-96: Access Group Serial 1/2.

7.21.1.2 ASIGNAR LAS ACL

matriz > enable

Ingresar al modo privilegiado

matriz # configure terminal

Ingresar al modo de configuración global

matriz(config)#access-list 102 deny icmp host 192.168.11.9 host 192.168.11.10 echo
matriz(config)#access-list 103 deny icmp host 192.168.11.5 host 192.168.11.6 echo

Línea de comandos que se va a digitar para el bloqueo de ping al matriz.

Access.list	Comando
103	Número de access.group
Deny	Especifica paquetes de bloqueo.
Icmp	Internet control message protocol
Host	Reemplaza la willcard
192.168.11.6	IP origen
Host	Reemplaza la wilcard
192.168.11.5	IP destino
Echo	Ping



Matriz(config)#^Z

matriz#wr

Grabar los cambios hechos.

```
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#
matriz(config)#access-list 102 deny icmp host 192.168.11.9 host 192.168.11.10 echo
matriz(config)#access-list 103 deny icmp host 192.168.11.5 host 192.168.11.6 echo
matriz(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]
```

Figura 7-97: Asignaciòn de las ACL.

7.21.1.3 PRUEBA DE CONEXION SUCURSAL QUITO CON SERVIDOR



Ping Comando
192.168.11.5 Ip servidor

```
quito#ping 192.168.11.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.5, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5), round-trip min/avg/max = 1/2/4 ms
```

Figura 7-98: Prueba de Conexión Quito.

7.21.1.4 PRUEBA DE CONEXION SUCURSAL AMBATO CON SERVIDOR

Ping Comando
192.168.11.5 Ip servidor

```
ambato#ping 192.168.11.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.5, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5), round-trip min/avg/max = 1/2/4 ms
```

Figura 7-99: Prueba de Conexión Quito.

7.21.1.5 SHOW ACCESS-LISTS

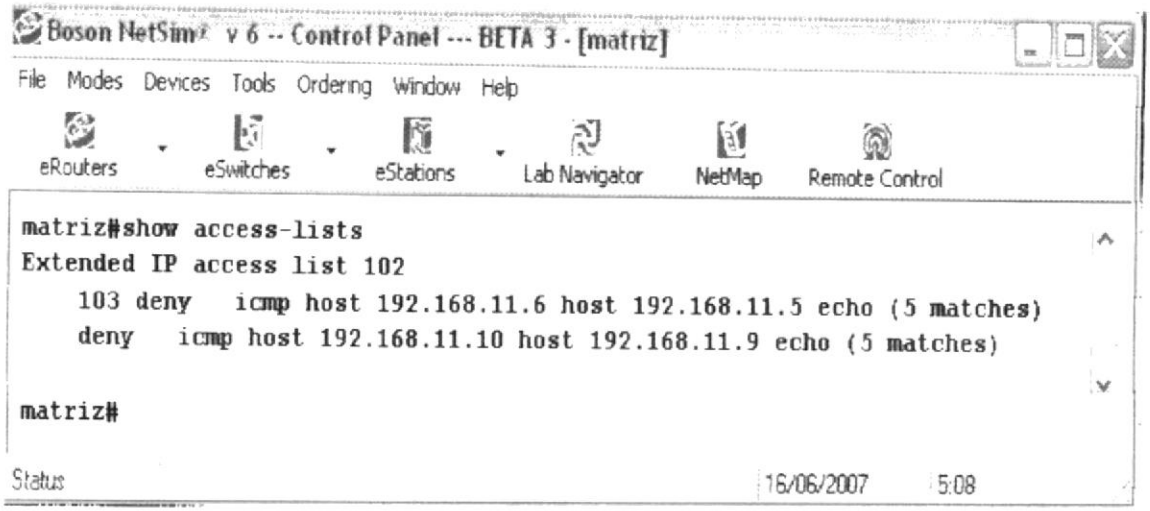


Figura 7-100: Access Lists.

Extended IP access list 102.

Indica el tipo de access list a usar y el número de access group en este caso (102).

103

Número de access group a utilizar

Deny

Especifica paquetes de bloqueo.

Icmp

Internet control message protocol

Host

Reemplaza la willcard

192.168.11.6

IP origen

Host

Reemplaza la wilcard

192.168.11.5

IP destino

Echo

Ping

ESPOL BIBLIOTECA CAMPUS PEÑAS

7.22. BLOQUEO DE TELNET

7.22.1 CONFIGURACIÓN DE IP ACCESS-GROUP

matriz > enable

Ingresar al modo privilegiado

matriz # configure terminal

Ingresar al modo de configuración global

matriz(config)#interface serial 1/1

Ingresar al serial donde quiere bloquear el puerto

matriz(config-if)#ip access-group 102 in

Crear el grupo de trabajo el cual permite verificar la clase de acl

Matriz(config-if))#exit

Salir de la interface del serial

```
matriz#ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#interface serial 1/1
matriz(config-if)#ip access-group 102 in
matriz(config-if)#exit
```

Figura 7-101: Configuración Access Group.



matriz(config)#interface serial 1/2

Ingresar al serial donde quiere bloquear el puerto

matriz(config-if)#ip access-group 103 in

Crear el grupo de trabajo el cual permite verificar la clase de acl.

Matriz(config-if)#^Z

matriz#wr

Grabar los cambios hechos.

```
matriz#ena
matriz#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
matriz(config)#inter serial 1/2
matriz(config-if)#ip access-group 103 in
matriz(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]
```

Figura 7-102: Access-Group 103.

7.22.2 ASIGNAR LAS ACL

matriz > enable

Ingresar al modo privilegiado

matriz # configure terminal

Ingresar al modo de configuración global

matriz(config)#access-list 102 deny tcp host 192.168.11.9 host 192.168.11.10 eq telnet
matriz(config)#access-list 103 deny tcp host 192.168.11.5 host 192.168.11.6 eq telnet

línea de comandos que se va a digitar para el bloqueo el telnet al matriz.

Access.list	Comando
103	Número de access.group
Deny	Especifica paquetes de bloqueo.
Tcp	Control de transmission de Protocolos
Host	Reemplaza la willcard
192.168.11.6	IP origen
Host	Reemplaza la wilcard
192.168.11.5	IP destino
Echo	Ping



Matriz(config)#^Z

matriz#wr

Grabar los cambios hechos.

```
matriz#config ter
matriz(config)#access-list 102 deny tcp host 192.168.11.9 host 192.168.11.10 eq telnet
matriz(config)#access-list 103 deny tcp host 192.168.11.5 host 192.168.11.6 eq telnet
matriz(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

matriz#wr
Building configuration...
[OK]

matriz#
```

Figura 7-103: Asignaiòn ACL.

7.22.3 SHOW ACCCESS-LIST

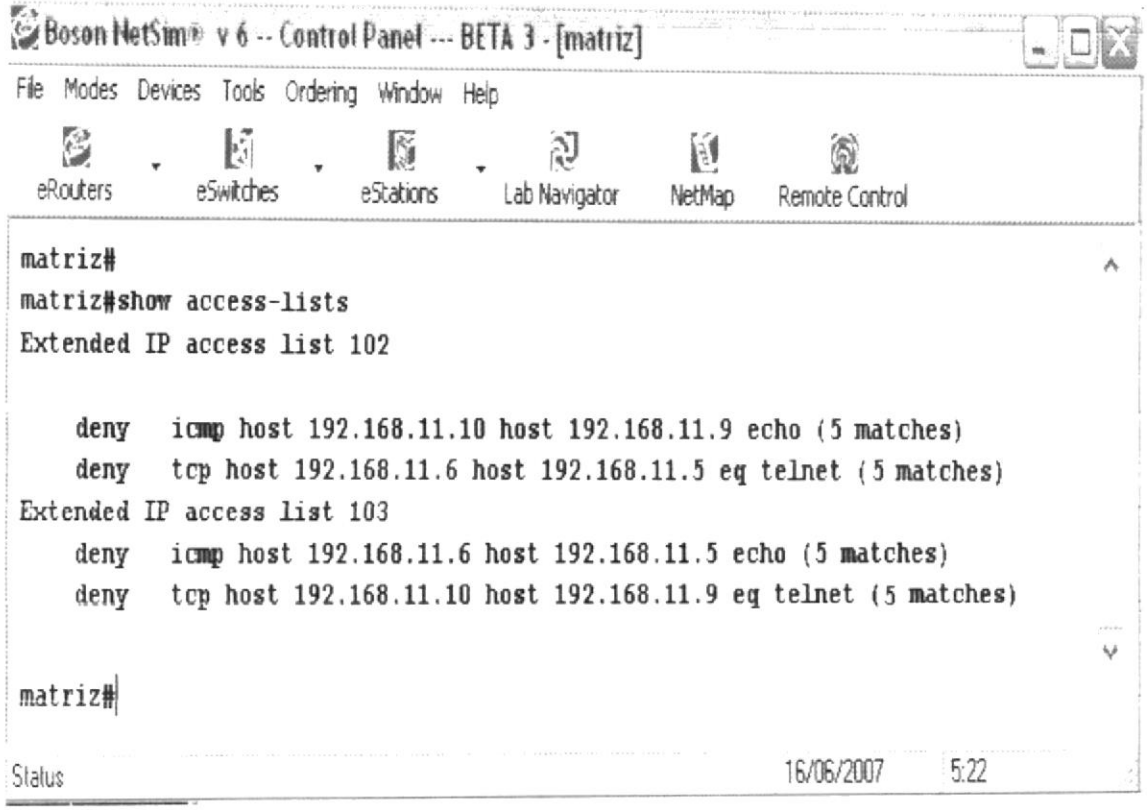


Figura 7-104: Show Access List.

Extended IP access list 102

Indica el tipo de access list a usar y el número de access group en este caso (102).

103

Número de access group a utilizar

Deny

Especifica paquetes de bloqueo.

Tcp

Transmisión del control del protocolo

Host

Reemplaza la willcard

192.168.11.6

IP origen

Host

Reemplaza la wilcard

ESPOL BIBLIOTECA CAMPUS PEÑAS

192.168.11.5

IP destino

Echo

Ping

Eq

Equipo solo de paquetes que dan el número del puerto.

Telnet

Manipulación y control de diferentes router.

7.22.4 PRUEBA DE TELNET SUCURSAL QUITO CON SERVIDOR

Telnet	Comando
192.168.11.5	Ip servidor



```
quito#telnet 192.168.11.5
Trying 192.168.11.5 ...
% Destination unreachable; gateway or host down
quito#
```

Figura 7-105: Pruebas de Telnet Quito.

7.22.5 PRUEBA DE TELNET SUCURSAL AMBATO CON SERVIDOR

Telnet	Comando
192.168.11.5	Ip servidor

```
ambato#telnet 192.168.11.5
Trying 192.168.11.5 ...
% Destination unreachable; gateway or host down
ambato#
```

Figura 7-106: Pruebas de Telnet Ambato.

ESPOL
BIBLIOTECA
CAMPUS
PERIMETRAL