

ESCUELA SUPERIOR POLITECNICA DEL LITORAL



Escuela de Diseño y Comunicación Visual

TÓPICO DE GRADUACIÓN

Previo a la obtención del título de:

Programador de Sistemas

Tema:

Universidad del Pacífico

Manual de Usuario y Configuración

Autores:

**Abad Anguisaca Jonathan
Baño Chano Gerardo David
Castillo Gonzáles Marcos**

Director

Anl. Fabián Barboza

Año 2006

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

TÓPICO DE GRADUACIÓN

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

**TEMA:
UNIVERSIDAD DEL PACÍFICO**

**MANUAL DE:
USUARIO Y CONFIGURACIÓN**

AUTORES

**ABAD ANGUISACA JONATHAN
BAÑO CHANO DAVID
CASTILLO GONZALES MARCOS**

DIRECTOR

ANL. FABIAN BARBOZA

AÑO

2006

AGRADECIMIENTO

A mi familia ya que gracias a ellos he podido superar varios obstáculos.

Al coordinador de la carrera quien me ha sabido guiar de manera correcta durante el transcurso de la misma

A mi director de t3pico que gracias a sus consejos y conocimientos hemos culminado con 3xito nuestros estudios.

Finalmente, a mis compa1eros de grupo quienes me han demostrado el verdadero significado de la palabra amistad.

DEDICATORIA

Dedico este triunfo a Dios, por darme salud, tolerancia y por sobre todas las cosas fuerzas para alcanzar lo que me propongo.

AGRADECIMIENTO

Principalmente a DIOS, que con su amor me impulsa día a día a seguir adelante.

A mí amada esposa que siempre creyó en mí y me alentó a seguir en momentos difíciles estando siempre junto a mí.

A mis padres y hermana ya que ellos son la piedra angular de mi vida y el mejor ejemplo de superación en tiempos de adversidad, son el impulso para alcanzar mis metas, siempre con la palabra precisa...

A mi director de tópicos que fue una excelente guía en el desarrollo de mi proyecto y que gracias a su apoyo hemos culminado exitosamente el mismo.

DEDICATORIA

Dedico este triunfo alcanzado principalmente a Dios, a mis padres Marlene Chano y David Baño Mena, mi hermana Gabriela Baño quienes supieron guiarme por el sendero del éxito con esfuerzo y dedicación.

A mi amada esposa Alisba Miranda por ser la inspiración en mi vida.

AGRADECIMIENTO

Principalmente a Dios por haberme permitido llegar hasta aquí.

A mis padres Joel Castillo y Gualquiria González por su gran esfuerzo diario para hacer de mí una persona de bien y ayudarme en mi formación profesional.

A mis maestros quienes me guiaron acertadamente en mi formación académica.

Y a mi Director de Tópico Anl. Fabián Barboza por compartir sus conocimientos con nosotros y guiarnos acertadamente a una exitosa culminación del mismo.

DEDICATORIA

Dedico este triunfo en especial a Dios quien guía mis pasos día a día por el sendero adecuado.

A mis padres por depositar su confianza en mí y apoyarme en cada uno de mis pasos.

A mi familia por siempre estar a mi lado y alentarme a seguir.

DECLARACIÓN EXPRESA

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

(Reglamento de Exámenes y Títulos Profesionales de la ESPOL).

**FIRMA DEL DIRECTOR
DEL TÓPICO DE GRADUACIÓN**



ANL. FARIAN BARBOZA

**FIRMA DEL AUTOR
DEL TÓPICO DE GRADUACIÓN**



JONATHAN ABAD



DAVID BAÑO



MARCOS CASTILLO

TABLA DE CONTENIDO

Pag.

CAPITULO 1

1	GENERALIDADES	1
1.1	OBJETIVO PARTICULAR	1
1.2	A QUIEN VA DIRIGIDO ESTE MANUAL	1
1.3	LO QUE DEBE CONOCER	1
1.4	ACERCA DE ESTE MANUAL	1
1.5	CONVENCIONES TIPOGRAFICAS	2
1.5.1	CONVENCIONES DE FORMATOS DE TEXTO	2
1.5.2	CONVENCIONES DEL MOUSE	2
1.5.3	CONVENCIONES DEL TECLADO	3

CAPITULO 2

2	ANTECEDENTES	1
2.1	MISION:	2
2.2	VISION:	2
2.3	LEVANTAMIENTO DE INFORMACION ORGANIZACIONAL	3
2.4	ANALISIS DE CABLEADO INTERNO	3
2.5	TENDIDO ELECTRICO	3
2.6	MATERIALES, MEDIOS Y DISPOSITIVOS DE NETWORKING	4
2.7	ESTACIONES DE TRABAJO Y LABORATORIO	5
2.8	SERVIDORES Y SUS RESPECTIVOS ROLES	5
2.9	RED	5
2.10	INTERNET Y DOMINIOS	5
2.11	PARTES O PIEZAS	6
2.12	EQUIPOS DE PROTECCIÓN: UPS - REGULADORES	6

CAPITULO 3

3	PROBLEMAS ACTUALES	1
3.1	SOLUCION PROPUESTA	2
3.2	ESTUDIO DE FACTIBILIDAD	3
3.2.1	ALTERNATIVA A	3
3.3	FACTIBILIDAD TECNICA:	3
3.4	FACTIBILIDAD OPERATIVA:	4
3.4.1	REQUERIMIENTOS OPERATIVOS:	4
3.5	FACTIBILIDAD ECONOMICA:	5
3.5.1	COSTOS OPERATIVOS:	5
3.5.2	COSTOS HARDWARE:	6
3.6	COSTO TOTAL DE LA ALTERNATIVA A:	6
3.7	VENTAJAS Y BENEFICIOS	7
3.7.1	VENTAJAS	7

3.7.2	BENEFICIOS	7
3.8	FORMA DE PAGO	7
3.9	PLAN DE TRABAJO A	8
3.10	ALTERNATIVA B	9
3.11	FACTIBILIDAD TECNICA:	9
3.12	FACTIBILIDAD ECONOMICA:	10
3.12.1	REQUERIMIENTOS DE SOFTWARE:	10
3.13	FACTIBILIDAD OPERATIVA:	11
3.13.1	REQUERIMIENTOS OPERATIVOS:	11
3.14	FACTIBILIDAD ECONOMICA:	12
3.14.1	COSTOS OPERATIVOS:	12
3.14.2	COSTOS HARDWARE:	13
3.15	COSTO TOTAL DE LA ALTERNATIVA B:	13
3.16	VENTAJAS Y BENEFICIOS	14
3.16.1	VENTAJAS	14
3.16.2	BENEFICIOS	14
3.17	FORMA DE PAGO	14
3.18	DIAGRAMA GANT	14

CAPITULO 4

4	INTRODUCCION A ROUTER	1
4.1	COMPONENTES INTERNOS DEL ROUTER	1
4.2	LA FUNCION DE UN ROUTER EN UNA RED WAN	2
4.3	CARACTERISTICAS FISICAS DE UN ROUTER	2
4.3.1	CONEXIONES EXTERNAS DE UN ROUTER	3
4.3.2	CONEXION DE PUERTO DE ADMINISTRACION	4
4.4	CONEXION DE LAS INTERFACES DEL ROUTER	4
4.4.1	¿SE CONECTA EL SISTEMA DE RED A UN DISPOSITIVO DE DTE O DCE?	5
4.4.2	ESTABLECIMIENTO DE UNA SESION HYPERTERMINAL	5
4.5	CONFIGURACION DE UN ROUTER	9
4.5.1	COMANDOS BASICOS DE ROUTER	10
4.6	GRAFICO A CONFIGURAR	11
4.7	ROUTER B	11
4.8	VLANS	14
4.8.1	TIPOS DE VLANS	14
4.8.2	VLANS POR PUERTO	15
4.8.3	VLANS POR DIRECCIONES MAC	15
4.8.4	VLANS POR PROTOCOLO	15
4.9	CONFIGURACION DE VLANS	15
4.9.1	ASIGNAR PUERTOS A UNA VLAN	15
4.9.2	ASIGNAR SWITCH DE TIPO SERVER	16
4.10	COMUNICACION ENTRE VLANS	16
4.10.1	ELIMINAR VLANS	17
4.10.2	SHOW VLANS	17
4.10.3	SH RUN	18

4.10.4	SH INTERFACES ROUTER B	19
4.10.5	SHOW IP ROUTE	21
4.11	ROUTER CORE	22
4.11.1	CONFIGURACION DE PROTOCOLOS DE ENRUTAMIENTO	24
4.12	VLANS	26
4.12.1	TIPOS DE VLANS	27
4.12.2	VLANS POR PUERTO	27
4.12.3	VLANS POR DIRECCIONES MAC	27
4.12.4	VLANS POR PROTOCOLO	27
4.13	CONFIGURACION DE VLANS	27
4.13.1	ASIGNAR PUERTOS A UNA VLAN	28
4.13.2	ASIGNAR SWITCH DE TIPO SERVER	28
4.14	COMUNICACION ENTRE VLANS	28
4.14.1	ELIMINAR VLANS	29
4.15	ROUTER D	34
4.15.1	USO DE LOS COMANDOS SHOW	36
4.16	LISTAS DE ACCESO	36
4.16.1	TIPOS DE ACLS	37
4.16.2	FUNCION DE LA WILCARD	37
4.16.3	DIRECCIONES DE TRAFICO	37
4.16.4	VERIFICACION DE LA ACL	38
4.17	SWITCHES	38
4.17.1	MODOS DE COMANDO DE LOS SWITCH	38
4.17.2	COMANDO SHOW MODO USUARIO	39
4.17.3	COMANDO SHOW MODO PRIVILEGIADO	39
4.17.4	CONFIGURACION DEL NOMBRE DEL SWITCH	39
4.17.5	CONFIGURACION DE CONTRASEÑAS DEL SWITCH	39
4.17.6	VLANS	40

CAPITULO 5

5	INTRODUCCION A LINUX	1
5.1	QUE ES LINUX	1
5.1.1	CARACTERISTICAS DE LINUX	1
5.1.2	COMANDOS BASICOS DE LINUX	2
5.2	DIRECTORIOS	3
5.3	INSTALACION DE LINUX FEDORA	4
5.3.1	REQUERIMIENTOS	4
5.3.2	LICENCIAS	5
5.3.3	OBTENER CD'S Y DVD DE FC	5
5.4	CREANDO LAS PARTICIONES	5
5.4.1	DEFRAGMENTAR NUESTRO DISCO	6
5.5	INSTALANDO FEDORA CORE.	12
5.6	INICIANDO LINUX	26
5.6.1	COMO INICIAR CON LINUX	26
5.6.2	INGRESO AL SISTEMA OPERATIVO LINUX FEDORA	27
5.7	SAMBA	30
5.7.1	REQUERIMIENTOS	30
5.7.2	CONFIGURACION	33
5.7.3	DESCRIPCION DE SAMBA	36
5.8	DNS (SISTEMA DE DOMINIO DE NOMBRE)	40

5.8.1	REQUERIMIENTOS	40
5.8.2	PRE-REQUISITOS:	40
5.8.3	CONFIGURACIONES:	41
5.9	WEBSERVER	48
5.9.1	REQUERIMIENTOS	48
5.9.2	PRE-REQUISITOS	48
5.10	PROXY	53
5.10.1	REQUERIMIENTOS	53
5.10.2	PRE-REQUISITOS	53
5.10.3	DENEGAR HORA	59
5.10.4	ACCESO CON AUTENTICACIÓN (PASSWORD)	59
5.11	SERVIDOR DE CORREO	61
5.11.1	REQUERIMIENTOS	61
5.11.2	PRE REQUISITOS	62
5.11.3	CONFIGURACION DE LOS CLIENTES	66
5.11.4	CONFIGURACION EN LA MAQUINA WINDOWS	67
5.12	DHCP	73
5.12.1	REQUERIMIENTOS	73
5.12.2	CONFIGURACION:	73
5.12.3	EN WINDOWS:	75
5.13	FIREWALL	78
5.13.1	ORDENES BASICAS:	79

TABLA DE FIGURAS

	Pag.
CAPITULO 3	
<i>Figura 3-1 Análisis de Piso Planta Baja</i>	16
<i>Figura 3-2 Análisis de Piso Primera Planta</i>	17
<i>Figura 3-3 Análisis de Piso Segunda Planta</i>	18
<i>Figura 3-3 Análisis del Laboratorio</i>	18
<i>Figura 3-4 Análisis del Piso del Edificio</i>	19
<i>Figura 3-5 Análisis de Piso</i>	20
<i>Figura 3-6 Comunicación a nivel WAN</i>	21
<i>Figura 4-1 Componentes externos de un router</i>	2
<i>Figura 4-2 Conexiones externas de un router</i>	3
<i>Figura 4-3 Conexión de un puerto de administración</i>	4
<i>Figura 4-4 Cable de datos entre Routers</i>	5
<i>Figura 4-5 Pasos para ingresar al Hyper Terminal</i>	6
<i>Figura 4-6 Ingreso del nombre de la conexión</i>	6
<i>Figura 4-7 Selección del puerto de conexión</i>	7
<i>Figura 4-8 Clic en el botón Aceptar para ingresar los cambios del puerto seleccionado</i>	7
<i>Figura 4-9 Selección de la velocidad del puerto del router</i>	8
<i>Figura 4-10 Clic en Aceptar para ingresar los cambios de la velocidad de conexión</i>	8
<i>Figura 4-11 Pantalla inicial del Hyper Terminal</i>	9
<i>Figura 4-12 Grafico de Configuración WAN</i>	11
<i>Figura 4-13 Arquitectura de las Vlans</i>	14
<i>Figura 4-14 Arquitectura de las Vlans</i>	26
<i>Figura 4-15 Arquitectura de las Vlans</i>	40
<i>Figura 5-2 Clic en Aceptar para empezar a redimensionar el Disco Duro</i>	7
<i>Figura 5-4 Indicamos el tamaño de la nueva partición</i>	8
<i>Figura 5-6 Creación de la Partición</i>	9
<i>Figura 5-7 Escogemos el tipo de Partición</i>	10
<i>Figura 5-8 Clic en Aceptar para empezar la configuración de la partición</i>	11
<i>Figura 5-9 Así es como debería quedar la pantalla después de las configuraciones realizadas</i>	11
<i>Figura 5-10 En el setup configuramos para que el computador encienda desde el Cd</i>	12
<i>Figura 5-11 Pantalla de inicio de Fedora</i>	13
<i>Figura 5-12 Opción para hacer un test al Cd</i>	13
<i>Figura 5-13 Pantalla de Bienvenida a la Instalación de Fedora</i>	14
<i>Figura 5-14 Selección del Lenguaje de la Instalación</i>	14
<i>Figura 5-15 Selección del Idioma del Teclado</i>	15
<i>Figura 5-16 Selección del tipo de instalación</i>	15
<i>Figura 5-17 Selección del particionamiento del disco</i>	16
<i>Figura 5-19 Selección del punto de montaje raíz (/)</i>	17
<i>Figura 5-20 Muestra las particiones existentes</i>	17
<i>Figura 5-21 Aviso de Formato</i>	18
<i>Figura 5-22 Ventana de Configuración del arranque</i>	18
<i>Figura 5-23 Configuración del Firewall (Cortafuegos)</i>	19
<i>Figura 5-24 Selección del país al cual se va a configurar</i>	19
<i>Figura 5-25 Ingreso de la contraseña</i>	20
<i>Figura 5-26 Instalación de paquetes</i>	20
<i>Figura 5-27 Pantalla en la que indica cuales Cd's se van a utilizar</i>	21
<i>Figura 5-28 Pantalla en la que indica que la instalación fue exitosa</i>	21
<i>Figura 5-29 Pantalla de inicio en la que permite seleccionar el sistema operativo de arranque</i>	22
<i>Figura 5-30 Pantalla de Bienvenida a Linux</i>	22
<i>Figura 5-31 Pantalla de Acuerdo de Licencia</i>	23
<i>Figura 5-32 Ventana de Configuración de la resolución de la pantalla</i>	23
<i>Figura 5-33 Ingreso de Nombre de Usuario</i>	24
<i>Figura 5-34 Configuración de la tarjeta de sonido</i>	24
<i>Figura 5-35 Pantalla de opción para la instalación de paquetes adicionales</i>	25
<i>Figura 5-36 Ingreso del Nombre de Usuario</i>	25
<i>Figura 5-37 Pantalla inicial de Linux Fedora</i>	26

Figura 5-39 Ingreso del Nombre de Usuario	28
Figura 5-42 Arquitectura de Samba	30
Figura 5-43 Salir al directorio raíz	30
Figura 5-48 Asignación de la dirección IP	33
Figura 5-51 Verificación de existencia del Localhost	35
Figura 5-52 Cambiando el grupo de trabajo en el archivo smb.conf	35
Figura 5-53 Crear la carpeta de trabajo en el archivo smb.conf	36
Figura 5-55 Creación y presentación del archivo deber.txt	37
Figura 5-56 Restaurar los servicios de Samba	38
Figura 5-57 Ingreso a la maquina Linux por medio de la dirección IP	38
Figura 5-58 Ingreso del usuario y Password	39
Figura 5-59 Carpetas de la maquina Linux	39
Figura 5-60 Arquitectura de DNS	40
Figura 5-61 Verificando si esta instalado el paquete bind	40
Figura 5-64 Se copia el archivo localhost.zone	42
Figura 5-66 Archivo upacifico.com editado	43
Figura 5-67 Reiniciar los servicios del DNS	43
Figura 5-68 Tiempos de respuestas	44
Figura 5-69 Editar el archivo resolv.conf	44
Figura 5-70 Ingreso al Menú propiedades del icono Mis sitios de Red	45
Figura 5-71 Ingresando al Menú Propiedades del icono Mis sitios de Red	45
Figura 5-72 Ingreso a las Propiedades del Protocolo Internet	46
Figura 5-73 Ingreso de la dirección IP de la maquina	47
Figura 5-74 Tiempos de respuestas a la maquina de Linux	47
Figura 5-75 Arquitectura de Web Server	48
Figura 5-76 Se verifica si esta instalado el paquete httpd	49
Figura 5-77 Se descomenta la línea Listen 80	49
Figura 5-78 Se descomenta la línea NamevirtualHost *:80	50
Figura 5-79 Se configura el párrafo <VirtualHost *:80>	50
Figura 5-80 Se crea la carpeta sitio y el archivo index.html	51
Figura 5-81 Se edita el archivo index.html	51
Figura 5-82 Se reinician los Servicios del Web Server	51
Figura 5-84 Arquitectura Proxy	53
Figura 5-85 Se verifica si esta instalado el paquete squid	54
Figura 5-86 Se comprueba la dirección IP de la maquina	54
Figura 5-87 Se descomenta y edita la línea http_port 8080	55
Figura 5-88 Se descomenta y edita la línea cache_mem	55
Figura 5-89 Se descomenta la línea cache_dir	55
Figura 5-90 Se edita la siguiente línea en la sección de las ACL	56
Figura 5-91 Se reinician los servicios del Proxy	56
Figura 5-92 Se ingresa al Sub Menú Opciones de Internet	57
Figura 5-93 Se ingresa a las configuraciones LAN dando clic en el botón (2)	57
Figura 5-94 Ingreso de la dirección IP y el puerto de comunicación	58
Figura 5-95 Pagina Universidad del Pacifico desde Windows	58
Figura 5-96 Ingreso de Usuario y Password	60
Figura 5-97 Arquitectura de Servidor de Correo	61
Figura 5-98 Se activa el paquete dovecot	62
Figura 5-99 Se edita el archivo Host	62
Figura 5-100 Se edita el archivo krb5-telnet	63
Figura 5-101 Se edita el archivo network	63
Figura 5-102 Se edita el archivo sendmail.cf	64
Figura 5-103 Se restauran los servicios de SendMail	64
Figura 5-104 Se edita el archivo dovecot.conf	65
Figura 5-105 Se restauran los servicios del dovecot	65
Figura 5-106 Se crea el usuario y password	66
Figura 5-107 Se reinician los servicios del dovecot y sendmail	66
Figura 5-108 Se ingresa el Outlook Express	67
Figura 5-109 Ingreso del Menú Cuentas...	67
Figura 5-110 Se crea una nueva cuenta	68
Figura 5-111 Se ingresa el nombre de usuario	68

<i>Figura 5-112 Se ingresa la dirección IP del servidor Linux</i>	69
<i>Figura 5-113 Si ingresa el nombre de la cuenta y password</i>	69
<i>Figura 5-114 Se finaliza para que las configuraciones tengan efecto</i>	70
<i>Figura 5-115 Ventana en la que se visualiza todas las cuentas existentes</i>	70
<i>Figura 5-116 Pantalla principal de Outlook Express</i>	71
<i>Figura 5-117 Ventana de transferencia de archivos</i>	71
<i>Figura 5-118 Ventana de recepción de correo en Windows</i>	72
<i>Figura 5-119 Pantalla de recepción de correo en Linux</i>	72
<i>Figura 5-120 Arquitectura de DHCP</i>	73
<i>Figura 5-121 Se edita el archivo dhcpd.conf</i>	74
<i>Figura 5-122 Se ingresa a las propiedades de mis sitios de red</i>	75
<i>Figura 5-123 Se ingresa a las propiedades de Conexión de área local</i>	75
<i>Figura 5-124 Se ingresa a las propiedades del Protocolo Internet</i>	76
<i>Figura 5-125 Se selecciona Obtener dirección IP automática</i>	76
<i>Figura 5-126 Se verifican las direcciones IP</i>	77
<i>Figura 5-127 Arquitectura de Firewall</i>	78
<i>Figura 5-128 Pantalla de bloqueo de servicios</i>	78

CONTENIDO DE TABLAS

<i>Tabla 1-1 Convenciones de Formato</i>	2
<i>Tabla 1-2 Convenciones del Mouse</i>	2
<i>Tabla 1-3 Convenciones del Teclado</i>	3
<i>Tabla 3-1 Problemas Actuales</i>	1
<i>Tabla 3-2 Solución Propuesta</i>	2
<i>Tabla 3-3 Factibilidad Técnica</i>	3
<i>Tabla 3-4 Requerimientos Operativos</i>	4
<i>Tabla 3-5 Costos Operativos</i>	5
<i>Tabla 3-6 Costos de Hardware</i>	6
<i>Tabla 3-7 Costo de la Alternativa A</i>	6
<i>Tabla 3-8 Factibilidad Técnica</i>	9
<i>Tabla 3-9 Factibilidad Económica</i>	10
<i>Tabla 3-10 Requerimientos de Software</i>	10
<i>Tabla 3-11 Requerimientos Operativos</i>	11
<i>Tabla 3-12 Costos Operativos</i>	12
<i>Tabla 3-13 Costos de Hardware</i>	13
<i>Tabla 3-14 Costo total de alternativa B</i>	13
<i>Tabla 4-1 Comandos Básicos de Router</i>	10
<i>Tabla 5-1 Comandos Básicos de Linux</i>	2
<i>Tabla 5-2 Descripción de SAMBA</i>	36



CAPÍTULO 1
GENERALIDADES

1 GENERALIDADES

Este manual es una guía de consulta para un usuario de cualquier nivel, ya que consta de distintos capítulos que contienen información clara y concisa acerca de cómo operar en Linux Fedora Core 3, Router y Switch basándose en un caso de estudio real de una empresa a nivel Lan y Wan.

Si usted no está familiarizado con Linux Fedora Core 3, Router y Switch Cisco es necesaria la lectura de este manual antes y/o durante la visualización de las páginas, ya que se indicará paso a paso el manejo del mismo.

1.1 OBJETIVO PARTICULAR

El objetivo de este manual es guiar a los usuarios interesados como al personal encargado del manejo y administración del sistema, entre los temas que detallaremos en los capítulos más adelante tenemos:

- Guía para conocer el entorno a Linux Fedora Core 3.
- Guía para conocer el entorno de Router y Switch.
- Cómo interactuar con los comandos.
- Guía para manejar cada una de las configuraciones.
- Conocer el alcance de los mismos.

1.2 A QUIEN VA DIRIGIDO ESTE MANUAL

Este manual está orientado a todos los usuarios finales involucrados en la etapa de operación de la Administración y Seguridades de Redes

1.3 LO QUE DEBE CONOCER

Los conocimientos mínimos que deben tener las personas que operarán este Sistema Operativo son:

1. Conocimientos básicos de Linux.
2. Conocimientos básicos de Windows.
3. Conocimientos básicos de Redes.

1.4 ACERCA DE ESTE MANUAL

Este manual contiene diversas ilustraciones e instrucciones que el Usuario debe seguir paso a paso para poder manejar correctamente el Sistema Operativo Linux Fedora Core 3, Router y Switch Cisco. Además incluye información adicional que servirá para orientar al Usuario sobre el correcto uso de la computadora.

Luego de leer este manual los usuarios que van a operar en el Linux estarán en capacidad de:

- Conocer las características del Sistema Operativo

- El usuario por medio de este manual de la aplicación podrá conocer más a fondo el funcionamiento de estas aplicaciones.
- Se especifica los requerimientos mínimos de hardware para poder instalar Linux Fedora Core 3.

1.5 CONVENCIONES TIPOGRAFICAS

Antes de comenzar a utilizar el Sistema Operativo Linux Fedora Core 3, es muy importante que entienda las convenciones tipográficas y los términos utilizados en el mismo.

1.5.1 CONVENCIONES DE FORMATOS DE TEXTO

Formato	Tipo de Información
Viñeta numérica 1	Numeración de procedimientos paso a paso.
	Términos a resaltar por su importancia.
	Secuencia de clic numeradas
	Resalta el lugar del cual se esta hablando en el texto

Tabla 1-1 Convenciones de Formato

1.5.2 CONVENCIONES DEL MOUSE

Término	Significado
“Señalar”	Se debe colocar el extremo superior del mouse sobre el elemento que se desea señalar.
“Hacer clic”	Se debe presionar el botón principal del mouse (generalmente el izquierdo) y soltarlo inmediatamente.

Tabla 1-2 Convenciones del Mouse

1.5.3 CONVENCIONES DEL TECLADO

Tecla	Significado
Teclas del método abreviado	Teclas que se utilizan como método abreviado para ejecutar un proceso. Por ejemplo F1 para mostrar la ayuda.
Tecla ENTER (ENTRAR - RETORNO)	Tecla utilizable para ejecutar un proceso. En el manual dirá “Presione ENTER”.
Teclas Direccionales → , ← , ↑ , ↓	Se puede utilizar las teclas direccionales para moverse (izquierda, derecha, arriba, abajo) en los diferentes elementos de un control de la pantalla, un elemento a la vez.
Teclas de avance de página INICIO, FIN, AV. PÁG, RE. PÁG.	Las teclas de avance de página son utilizadas para movilizarse entre varios elementos de un control de la pantalla.
Tecla TAB	Tecla utilizada para moverse entre los diferentes controles de la forma. Con la tecla TAB, se da el enfoque al primer control ubicado a la derecha, con SHIFT+TAB, se da el foco al primer control de la izquierda.
Otras teclas	Adicionalmente puede utilizar otros elementos del teclado. Por ejemplo: ✓ SHIFT+TECLA se utiliza para que se active la función que está graficada en la parte superior de TECLA. ✓ ALTGR+TECLA, es utilizada para que se active la tercera función de TECLA.

Tabla 1-3 Convenciones del Teclado

CAPÍTULO 2

SITUACION ACTUAL



2 ANTECEDENTES

El presente informe integral obedece a un requerimiento de la Junta Directiva Académica de establecer la Situación Actual de la infraestructura tecnológica de la Universidad del Pacífico (sede Guayaquil). Sin embargo hemos determinado necesario además, como segunda parte de este proyecto, presentar recomendaciones y mecanismos de reestructuración de esta infraestructura para conseguir una solución óptima e integral de las necesidades de la Universidad en un mediano plazo.

El objetivo principal de la Universidad del Pacífico es la formación integral de empresarios para el ejercicio eficiente de la carrera que han elegido, con énfasis en el desarrollo humanístico del individuo.

Las actividades académicas se basan en la búsqueda de la excelencia, a través de programas que consideran la investigación, la experimentación y el dominio de técnicas instrumentales; consolidando un proceso de enseñanza-aprendizaje de alto nivel

Actualmente la Universidad del Pacífico se compone de 3 sedes:

- Sede Guayaquil: Se encuentra ubicada en Kilómetro 7.5 vía a la Costa, sobre el desvío a Daule.
- Sede Quito: Se encuentra ubicada en El Pinar Alto calle B N48-177
- Sede Cuenca: Se encuentra ubicada en Av. Gran Colombia No. 23-116 y Av. de las Américas

Además tienen como proyecciones a futuro crear sedes en Esmeraldas, Galápagos y Manta, fortaleciendo de esta manera los vínculos académicos con la Asociación de Universidades de la cuenca del Pacífico.

2.1 MISION:

“Contribuir al desarrollo económico y social del país, mediante la preparación de hombres y mujeres de negocios, concientes de los procesos de transformación en que vive el mundo, dotados de una actitud emprendedora para fomentar sus propias iniciativas empresariales con valores éticos y morales, guiados por educadores comprometidos con la excelencia académica y la formación de las nuevas generaciones como agentes de cambio e impulsores del desarrollo sostenido”

2.2 VISION:

“Insertar a la Universidad del Pacífico Escuela de Negocios como institución especializada entre las mejores escuelas de negocios en el ámbito internacional”

2.6 MATERIALES, MEDIOS Y DISPOSITIVOS DE NETWORKING

Medios de Comunicación

- **Elementos :**
 - 1 Antena Satelital
 - Cable UTP categoría 5e

- **Dispositivos de Conmutación**
 - Existen 3 switches Principales 10/100 Mbps marca D-link
 - 1 Router Cisco modelo 2600 el cual distribuye el tráfico de red de los puntos de datos de la Universidad del Pacífico.

- **Materiales de Cableado**
 - Canalón metálico con conexión a Tierra.

 - **1 Rack de piso utilizado con los siguientes componentes:**
 - Soporte de los switches.

 - Soporte de los Patch Panels del cableado de los puntos de datos (3 en total).

 - Soporte de los Patch Panels del cableado de los puntos de voz (3 en total).

- **Distribución de puntos de datos y voz:**
 - Existe un cableado de voz y datos.
 - Existen 72 puntos de datos
 - Existen 60 puntos de datos habilitados de los cuales 40 se encuentran en uso
 - Existen 72 puntos de voz
 - Existen 50 puntos de voz habilitados de los cuales 30 se encuentran en uso.
 - Los puntos de red no se encuentran debidamente etiquetados tanto en el Rack de comunicaciones como en las áreas de trabajo.

- **Certificación del cableado:**
 - Cableado no certificado

2.7 ESTACIONES DE TRABAJO Y LABORATORIO

- **Hardware:**
 - Poseen 40 equipos Pentium IV con 512 de Memoria RAM y 40 GB de Disco Duro.
 - Todas las Estaciones de Trabajo poseen tarjetas de red integradas.
- **Software:**
 - Windows XP con sus respectivas licencias.
 - Symantec Norton Antivirus con sus respectivas licencias.

2.8 SERVIDORES Y SUS RESPECTIVOS ROLES

- **Hardware:**
 - 1 Servidor Marca Supermicro proporcionado por su proveedor de Internet (no poseen las características de hardware de este equipo)
 - 1 Servidor Clon Pentium IV con 2 Gb. de memoria RAM, 80 Gb. en Disco Duro para Aplicaciones y NIC 10/100.
 - 1 Servidor Clon Pentium IV con 2 Gb. de memoria RAM, Torre reproductora de CD y 80 Gb. en Disco Duro para Respaldo de Datos.
- **Software:**
 - El Sistema Operativo de los Servidores de Respaldo y de Aplicaciones es Windows 2000 Server.
 - Existe productos de Software Gratuito como el del Web Server con Sistema Operativo Linux en el cual se encuentran configuradas políticas Firewall.
 - Existe muy poca documentación de la infraestructura tecnológica actual.

2.9 RED

- **Estructura física de la red:**
 - Red de área local

2.10 INTERNET Y DOMINIOS

- **Enlaces con Proveedores de Servicio de Internet:**
 - Acceso a Internet con el Proveedor Hitelecom con un ancho de banda de 256 Kbps, por medio de Antena Satelital.
- **Dominios:** existen 3 Dominios (Administrativos, Docentes y Estudiantes).
- **Sitio WEB:**
 - Diseñado y administrado por Personal del Centro de Cómputo de la Universidad. www.udelpacifico.edu.ec

2.11 PARTES O PIEZAS

- **Partes y piezas de equipos informáticos fuera de uso que pueden ser reutilizados:**
 - Actualmente no poseen partes y piezas en el centro de cómputo.

2.12 EQUIPOS DE PROTECCIÓN: UPS - REGULADORES

- **Distribución de UPS y reguladores**
 - Todas las Estaciones de Trabajo, Laboratorios y las áreas administrativas poseen UPS y reguladores.

Faint, illegible text, possibly bleed-through from the reverse side of the page.

CAPÍTULO 3

PROPUESTA



3 PROBLEMAS ACTUALES

Luego de efectuar el estudio correspondiente y conocer el estado actual de la **Universidad**, se han detectado deficiencias existentes en el área de Información Técnica, los cuales impiden a la Universidad una mayor agilidad al ejecutar sus controles y procesos, y de acuerdo a esto poder elaborar el nivel de cada una de las soluciones a implementar con el propósito de alcanzar un funcional y completo aprovechamiento de las mismas.

Problema	Causas	Efectos
Congestionamiento en la navegación de Internet.	Descarga de archivos sin restricción de tamaño	Tiempos de respuestas muy altos.
No existe Administración a los dispositivos de comunicación.	Falta de dispositivos administrables.	Dificulta la administración de los recursos de la red.
Cableado no Estructurado.	<ul style="list-style-type: none"> • Canaletas en mal estado • Poca protección del cable • Puntos de red sin etiquetar • Rack de piso sin Gabinete Cerrado. 	<ul style="list-style-type: none"> • Daña la estética del lugar • El cable se puede dañar • Perdida de tiempo en soporte de la red • Tropiezo involuntario.
No poseen servidor Proxy propio	Falta personal capacitado para su administración.	Gasto excesivo de dinero en alquiler, configuración y mantenimiento.
Sedes no comunicadas	No se visualizo el crecimiento de la Universidad.	<ul style="list-style-type: none"> • Gasto de envío de información a las demás sedes (courrier) • No se puede intercambiar información de manera directa

Tabla 3-1 Problemas Actuales

3.1 SOLUCION PROPUESTA

Después de un exhaustivo trabajo de levantamiento de información llegamos a notar los principales problemas por lo que esta pasando en estos momentos La Universidad del Pacífico con respecto a su red LAN.

Problema	Solución	Alcance
Congestionamiento en la navegación de Internet.	Aumentar Ancho de banda Segmentar al ancho de banda.	Mayor velocidad en la red.
No existe Administración a los dispositivos de comunicación.	Adquisición de Switches administrables y Stakeables.	Nos permitirán administrar la red desde un punto central.
Cableado no Estructurado.	<ul style="list-style-type: none"> • Reestructuración del cableado • Adquirir gabinete cerrado de piso. 	<ul style="list-style-type: none"> • Resolver con rapidez problemas en la red • Seguridad de los diferentes puntos de red y Dispositivos
No poseen servidor Proxy propio	Adquirir 1 Servidor con Sistema Operativo Linux.	Administrar de forma directa las políticas de firewall.
Sedes no comunicadas	Implementar VPN.	Ayudará al intercambio de información entre Sedes.

Tabla 3-2 Solución Propuesta

Se permitirá a los administradores de red, distinguir los diversos conflictos comunes que se pueden presentar en una red con más facilidad y precisión

Con los cambios de los dispositivos respectivos y configuraciones propuestas se busca ampliar la efectividad de la red así como eliminar problemas existentes en la infraestructura.

3.2 ESTUDIO DE FACTIBILIDAD

3.2.1 ALTERNATIVA A

OBJETIVO:

El objetivo primordial de esta alternativa de solución es mantener a todas las sedes en constante comunicación a nivel WAN y a nivel LAN mejorar la seguridad, el tráfico y la administración de la red mediante la adquisición de equipos de conmutación y la reorganización del cableado.

3.3 FACTIBILIDAD TECNICA:

Cant.	Descripción	Características	Ubicación
1	Servidor	Server de 1 Gb. Ram, Disco Duro SCSI36, 2 NIC 10/100/1000 Mbps	Sistemas
2	Swieth Administrables	Switch D-Link XStack DXS-3326GSR, Stackeable	Sistemas
1	Minicenter Mc	Gabinete Metálico. Espacio interior de 35UR, Dimensión 196 x 62 x 101 cm.	Sistemas
1	Access Point D-Link Dwl-2100ap	D-link, 108 Mbps, 2.4GHz frecuencia flow control Servidor de DHCP incluido	Laboratorio
18	Pci D-Link G. Dwl-G520	Tarjeta de red Inalámbrica 108 Mbps velocidad de transmisión	Laboratorio
3	Canaletas	Canaleta Decorativa	
9	Jack	Categoría 5E	
9	Cajas	Sobrepuestas	
9	Face Plate	2 servicios	
2	Organizador	Organizador horizontal sencillo marca SMARTLINK	Sistemas
10	Artículos Varios	RJ45, botas, amarras, tornillos, etc.	Sistemas y áreas varias

Tabla 3-3 Factibilidad Técnica

3.4 FACTIBILIDAD OPERATIVA:**3.4.1 REQUERIMIENTOS OPERATIVOS:**

Cant.	Actividad	Días
Fase de Análisis Wan		
1	Ing. Telecomunicaciones.	9
1	Técnico de Redes	8
Fase Diseño WAN		
1	Ing. Telecomunicaciones.	3
1	Administrador de Redes	5
Fase Implementación WAN		
1	Ing. Telecomunicaciones.	8
1	Administrador de Redes	4
1	Técnico de Redes.	2
Fase de Documentación WAN		
1	Ing. Telecomunicaciones.	3
1	Administrador de Redes	3
Fase De Prueba WAN		
1	Administrador de Redes	6
1	Técnico de Redes.	6

Tabla 3-4 Requerimientos Operativos

3.5 FACTIBILIDAD ECONOMICA:**3.5.1 COSTOS OPERATIVOS:**

Cant.	Actividad	Semanas	Costo Semanal	Costo Total
Fase de Análisis Wan				
1	Ing. Telecomunicaciones.	2	\$ 180.00	\$ 300.00
1	Técnico de Redes	2	\$ 90.00	\$ 180.00
Fase Diseño WAN				
1	Ing. Telecomunicaciones.	6	\$ 150.00	\$ 900.00
1	Administrador de Redes	6	\$ 100.00	\$ 600.00
Fase Implementación WAN				
1	Ing. Telecomunicaciones.	3	\$ 150.00	\$ 450.00
1	Administrador de Redes	3	\$ 100.00	\$ 300.00
1	Técnico en Electricidad	3	\$ 80.00	\$ 240.00
2	Técnico de Redes.	3	\$ 90.00	\$ 270.00
Fase de Documentación WAN				
1	Administrador de Redes	3	\$ 150.00	\$ 450.00
1	Técnico de Redes	3	\$ 90.00	\$ 270.00
Fase De Prueba WAN				
1	Ing. Telecomunicaciones	2	\$150.00	\$300.00
1	Administrador de Redes	2	\$100.00	\$200.00
Total:			\$ 4.460.00	

Tabla 3-5Costos Operativos

3.5.2 COSTOS HARDWARE:

Cant.	Descripción	Precio Unitario	Precio Total
4	Server	\$1.050	\$4.200
4	Switch Administrables	\$431.20	\$862.40
1	Minicenter MC	\$3.250,00	\$3.250,00
5	MAX Modular Face Plate 2 Puertos Marfil	\$2.16	\$10.80
	VLAN (Configuración)	\$80.00	\$80.00
	VPN	\$250.00	\$250.00
9	Jack Modelo Plano Cat. 5E Simeón	\$5.00	\$45.00
1	Access Point D-Link DWL-2100 ap	\$110.88	\$110.88
18	PCI D-Link GDWL-G520	\$48.16	\$866.88
9	Patch Cord de 2mtr. Gris (PC)	\$1.80	\$16.20
4	Tarjetas de Red 10/100 Mbps	\$10.00	\$40.00
	Amarras, Tornillos, ángulos	\$25.00	\$25.00
	Subtotal		\$8.268,21
	IVA 12%		\$632.19
	Total		\$8.900,40

Tabla 3-6 Costos de Hardware

3.6 COSTO TOTAL DE LA ALTERNATIVA A:

Descripción	Costo
Costo Hardware	\$8,900.40
Costo Software	\$95.52
Costos Operativos	\$5,670.00
Imprevistos (8 %)	\$878.28
Costo Total de la Alternativa A:	\$15,544.20

Tabla 3-7 Costo de la Alternativa A

3.7 VENTAJAS Y BENEFICIOS

3.7.1 VENTAJAS

- Mejor Control del uso del Internet
- Se eliminaran falencias del cableado
- Detección de problemas con exactitud
- Se eliminaran tropiezos involuntarios con el cableado.
- Personalización de políticas de seguridad.
- Comunicación entre sedes.

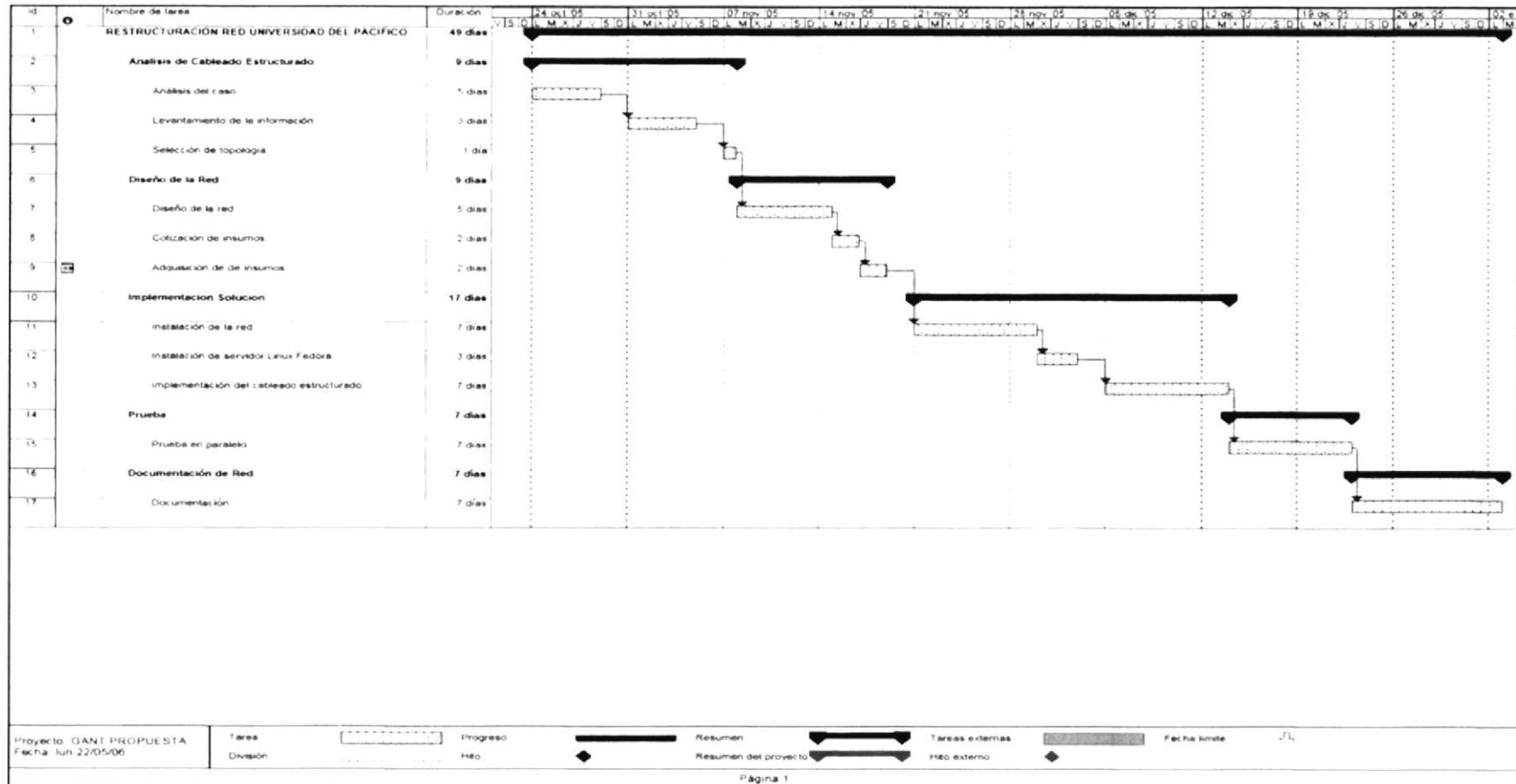
3.7.2 BENEFICIOS

- Mejor rendimiento de la red
- Mayor control de dispositivos de comunicación
- Mejor organización y presentación de los laboratorios
- Mejor soporte de red evitando perdida de tiempo
- Conservar el cableado en perfecto estado
- Mejor control del uso del Internet en toda la Universidad dividiendo el sector administrativo del sector alumnado
- Facilita una mejor comunicación de datos entre sedes.

3.8 FORMA DE PAGO

La forma de pago será en efectivo o cheque certificado, 60% al momento de la firma del contrato y 40% contra entrega del trabajo terminado, con una garantía de 1 año en infraestructura y configuración de equipos.

3.9 PLAN DE TRABAJO A



3.10 ALTERNATIVA B

OBJETIVO:

Como alternativa a la solución propuesta presentamos una segunda opción la cual va a permitir la corrección de problemas a un menor costo, pero no de una manera optima.

Cuarto de comunicaciones:

Se trabajara con Gabinete Cerrado pero añadiendo organizadores y etiquetando debidamente los puntos de red.

Laboratorio de Computación

Reestructuración del cableado dentro del laboratorio, verificación de los cables de red, colocación de canaletas, FACE plate, jack's y la correcta etiquetación de los puntos (18 en total) con una nomenclatura que sea identificada con facilidad en el cuarto de comunicaciones.

3.11 FACTIBILIDAD TECNICA:

Cantidad	Descripción	Fases	Características	Ubicación
1	Gabinete Cerrado	todas	24 U, 17", Seguro de 3 puntos, extractor de aire, regleta y foco interno	Sistemas
1	PC Clon	todas	Intel P4 3.2 Mb. 915GEVL Cd Rom, 120Gb SATA, 1 Gb DDR (2 512), 10/100 Mbps	Sistemas
4	Canaletas	todas	Canaleta Decorativa Acabado más cuidado, se utiliza para ocultar cableado.	Laboratorio
27	Jack	todas	Modelo plano blanco con tapa Categoría 5E	Laboratorio
27	Face plate	todas	Máx. modular 2 puertos marfil	Laboratorio
3	Organizador	todas	Organizador horizontal sencillo marca SMARTLINK	Sistemas
120	Conectores	todas	RJ45	Laboratorio
120	Botas	todas	Botas protectoras para cable UTP varios colores	Laboratorio

Tabla 3-8 Factibilidad Técnica

3.12 FACTIBILIDAD ECONOMICA:

Cant.	Descripción	P. Unitario	P. TOTAL
1	Pc Clon	\$712.00	\$712.00
3	Organizador Horizontal Sencillo	\$16.00	\$ 48.00
14	MAX Modular Face Plate 2 Puertos Marfil	\$2.16	\$30.24
27	Jack Modelo Plano Blanco Cat. 5E Simeón	\$5.00	\$135.00
54	Patch Cord de 2mtr. Gris (Pc)	\$1.80	\$97.20
	Artículos Varios		
	Amarras, Tornillos, Ángulos, Etc.	\$25.00	\$25.00
	Mano de Obra		
54	15,00 Por Punto de Red	\$810.00	\$810.00
	Organización de Rack de Comunicaciones	\$80.00	\$80.00
		Subtotal	\$1,937.44
		I.V.A. 12%	\$232.49
		Total	\$2,169.93

Tabla 3-9 Factibilidad Económica

3.12.1 REQUERIMIENTOS DE SOFTWARE:

Cantidad	Software	Costo Paquete	Costo Licencia	Cantidad Licencia	Costo Total Licencia	Costo Total
1	Linux Fedora (Core3)	\$95,52	\$0,00	1	\$0,00	\$95,52

Tabla 3-10 Requerimientos de Software

3.13 FACTIBILIDAD OPERATIVA:**3.13.1 REQUERIMIENTOS OPERATIVOS:**

Cant.	Actividad	Días
Fase de Análisis WAN		
1	Ing. Telecomunicaciones.	9
1	Técnico de Redes	8
Fase Diseño WAN		
1	Ing. Telecomunicaciones.	3
1	Administrador de Redes	5
Fase Implementación WAN		
1	Ing. Telecomunicaciones.	8
1	Administrador de Redes	4
1	Técnico de Redes.	2
Fase de Documentación WAN		
1	Ing. Telecomunicaciones.	3
1	Administrador de Redes	3
Fase de Prueba WAN		
1	Administrador de Redes	6
1	Técnico de Redes.	6

Tabla 3-11 Requerimientos Operativos

3.14 FACTIBILIDAD ECONOMICA:**3.14.1 COSTOS OPERATIVOS:**

Cant.	Actividad	Semanas	Costo Semanal	Costo Total
Fase de Análisis Wan				
1	Ing. Telecomunicaciones.	2	\$ 150.00	\$ 300.00
1	Técnico de Redes	2	\$ 90.00	\$ 180.00
Fase Diseño WAN				
1	Ing. Telecomunicaciones.	6	\$ 150.00	\$ 900.00
1	Administrador de Redes	6	\$ 100.00	\$ 600.00
Fase Implementación WAN				
1	Ing. Telecomunicaciones.	3	\$ 150.00	\$ 450.00
1	Administrador de Redes	3	\$ 100.00	\$ 300.00
1	Técnico en Electricidad	3	\$ 80.00	\$ 240.00
2	Técnico de Redes.	3	\$ 90.00	\$ 270.00
Fase de Documentación WAN				
1	Administrador de Redes	3	\$ 150.00	\$ 450.00
1	Técnico de Redes	3	\$ 90.00	\$ 270.00
Fase de Prueba WAN				
1	Ing. Telecomunicaciones	2	\$150.00	\$300.00
1	Administrador de Redes	2	\$100.00	\$200.00
			<u>Total:</u>	\$ 4.460.00

Tabla 3-12 Costos Operativos

3.14.2 COSTOS HARDWARE:

Cant.	Descripción	Precio Unitario	Precio Total
1	Pc Clon	712.00	712.00
3	Organizador Horizontal Sencillo	16.00	48.00
14	MAX Modular Face Plate 2 Puertos Marfil	2.16	30.24
27	Jack Modelo Plano Blanco Cat. 5E Simeón	5.00	135.00
54	Patch Cord de 2mtr. Gris	1.80	97.20
	Artículos Varios		
	Amarras, Tornillos, Ángulos, etc.	25.00	25.00
	Mano de Obra		
54	15.00 por punto de red	810.00	810.00
	Organización de Rack de Comunicaciones	80.00	80.00
		<u>Subtotal</u>	1,937.44
		<u>IVA 12%</u>	232.44
		<u>Total</u>	2,169.93

Tabla 3-13 Costos de Hardware

3.15 COSTO TOTAL DE LA ALTERNATIVA B:

Descripción	Costo
Costo Hardware	2,169.93 \$
Costo Software	95.52 \$
Costos Operativos	6,300.00 \$
Costo Total de la Alternativa B:	8,565.45 \$

Tabla 3-14 Costo total de alternativa B

3.16 VENTAJAS Y BENEFICIOS

3.16.1 VENTAJAS

- Mejor Control del uso del Internet
- Se eliminaran falencias del cableado
- Detección de problemas con exactitud
- Comunicación entre sedes.

3.16.2 BENEFICIOS

- Mejor rendimiento de la red
- Mejor organización y presentación de los laboratorios
- Conservar el cableado en perfecto estado
- Facilita una mejor comunicación de datos entre sedes.

3.17 FORMA DE PAGO

La forma de pago será en efectivo o cheque certificado, 60% al momento de la firma del contrato y 40% contra entrega del trabajo terminado, con una garantía de 1 año en infraestructura y configuración de equipos.

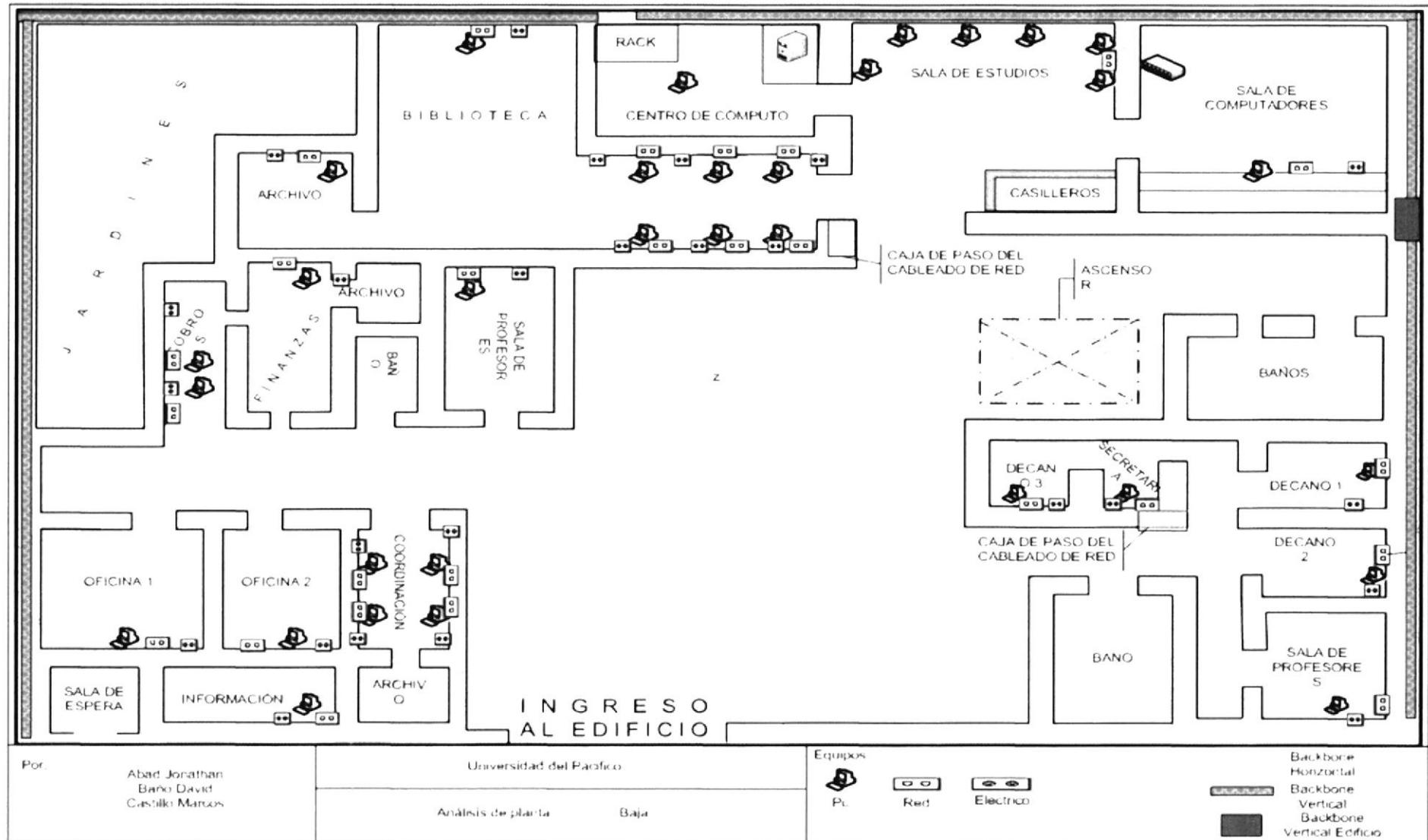


Figura 3-1 Análisis de Planta Baja

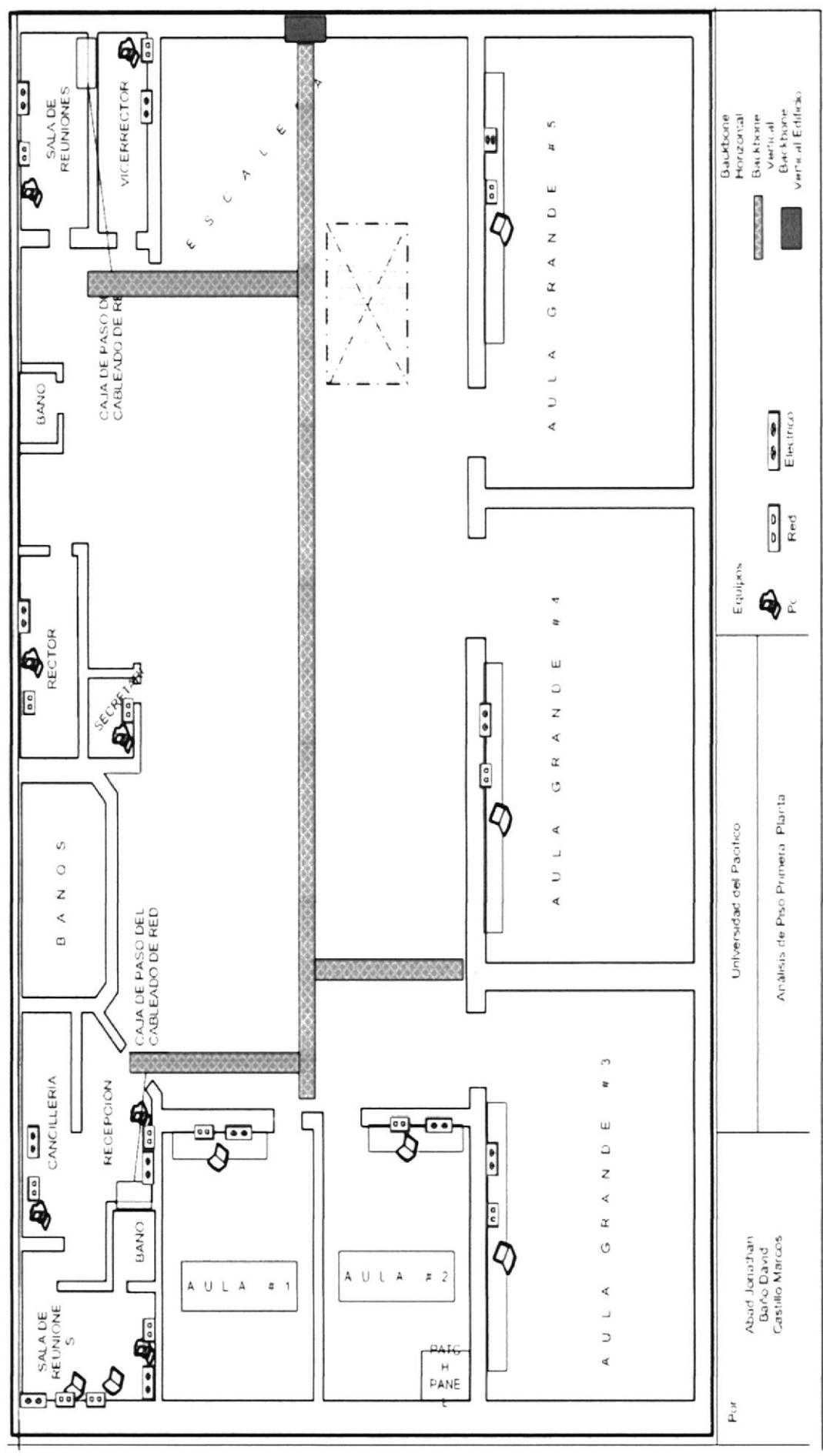


Figura 3-2 Análisis de Piso Primera Planta

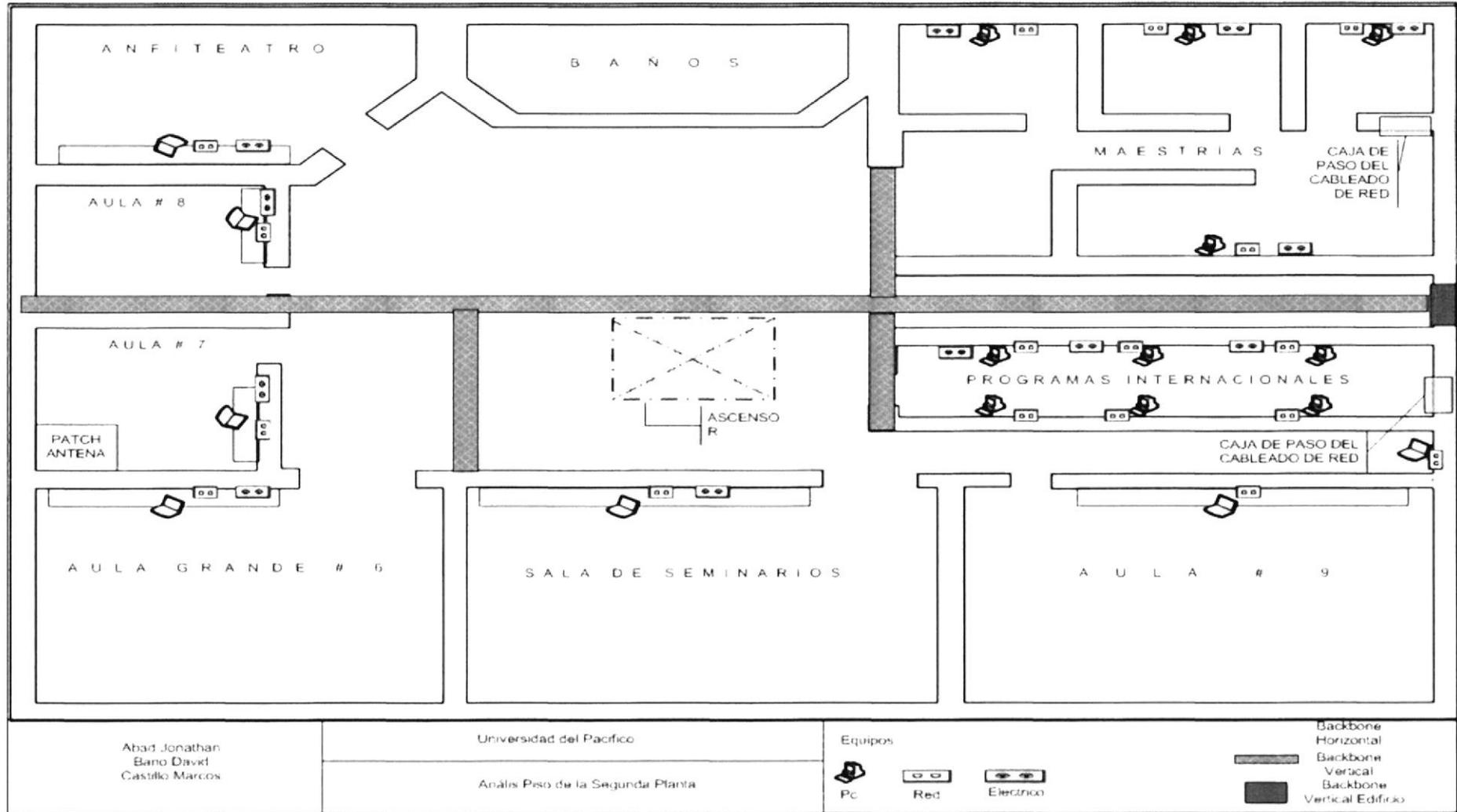


Figura 3-3 Análisis de Piso Segunda Planta

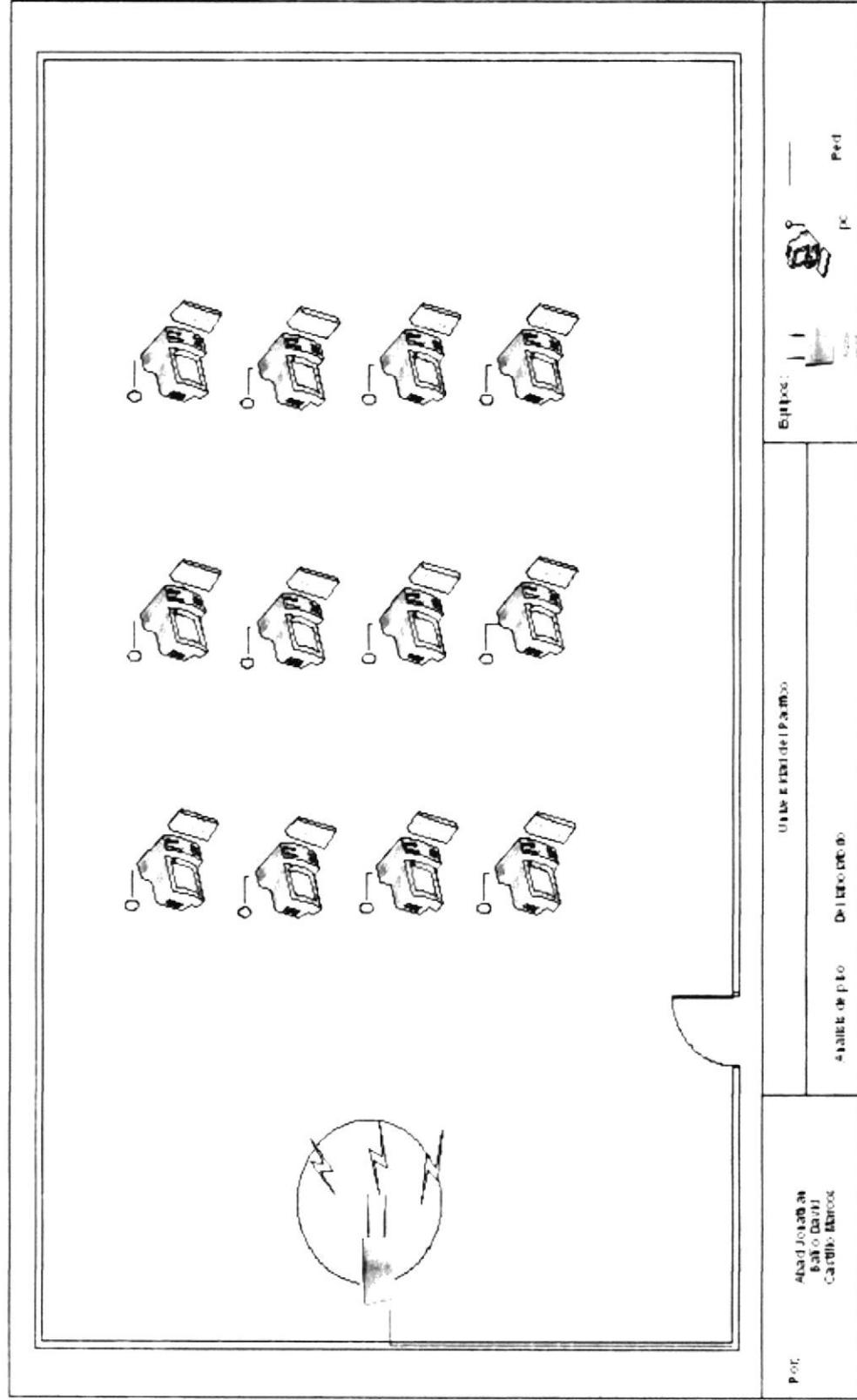
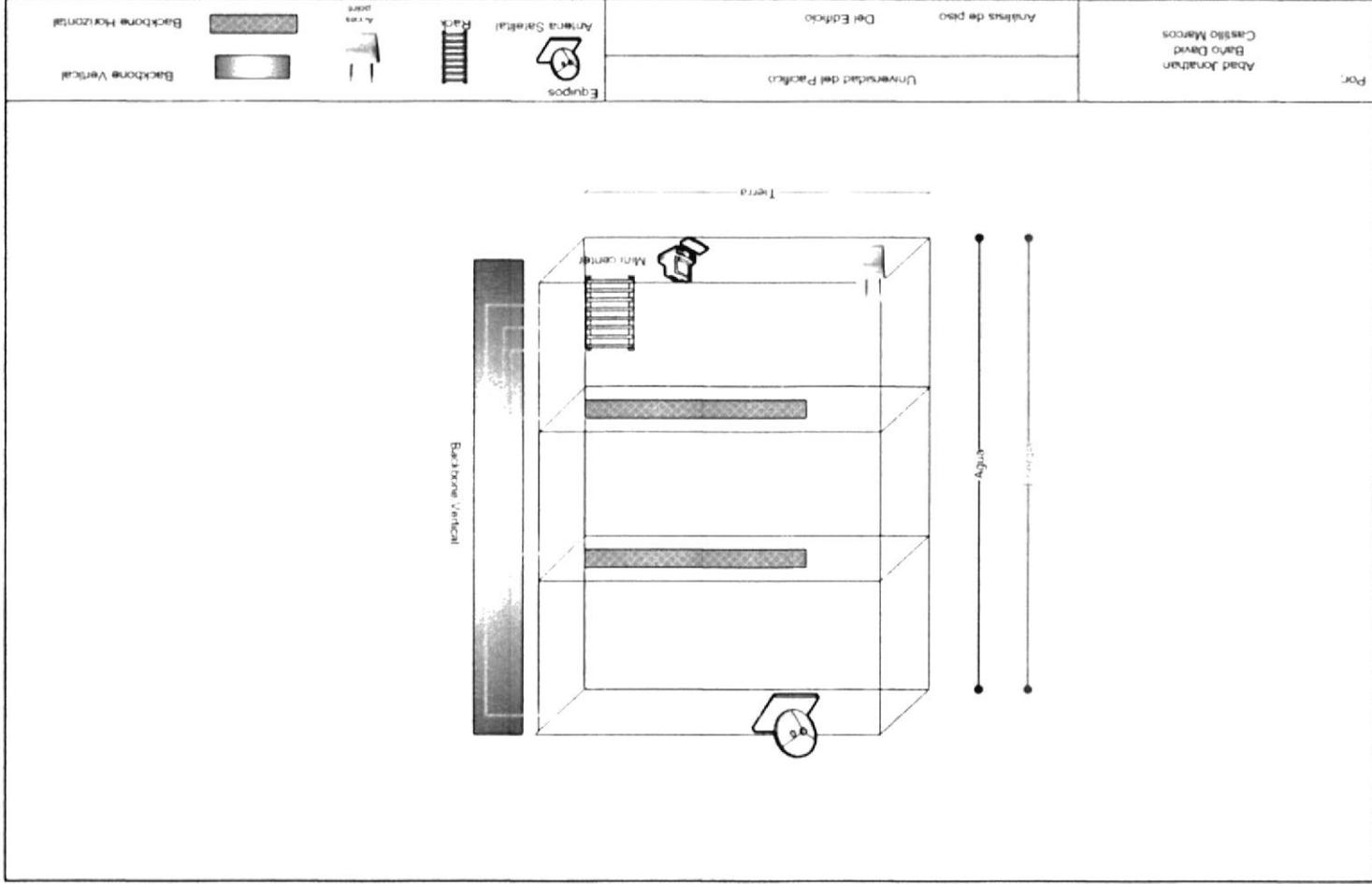


Figura 3-3 Análisis del Laboratorio

Figura 3-4 Análisis del Piso del Edificio



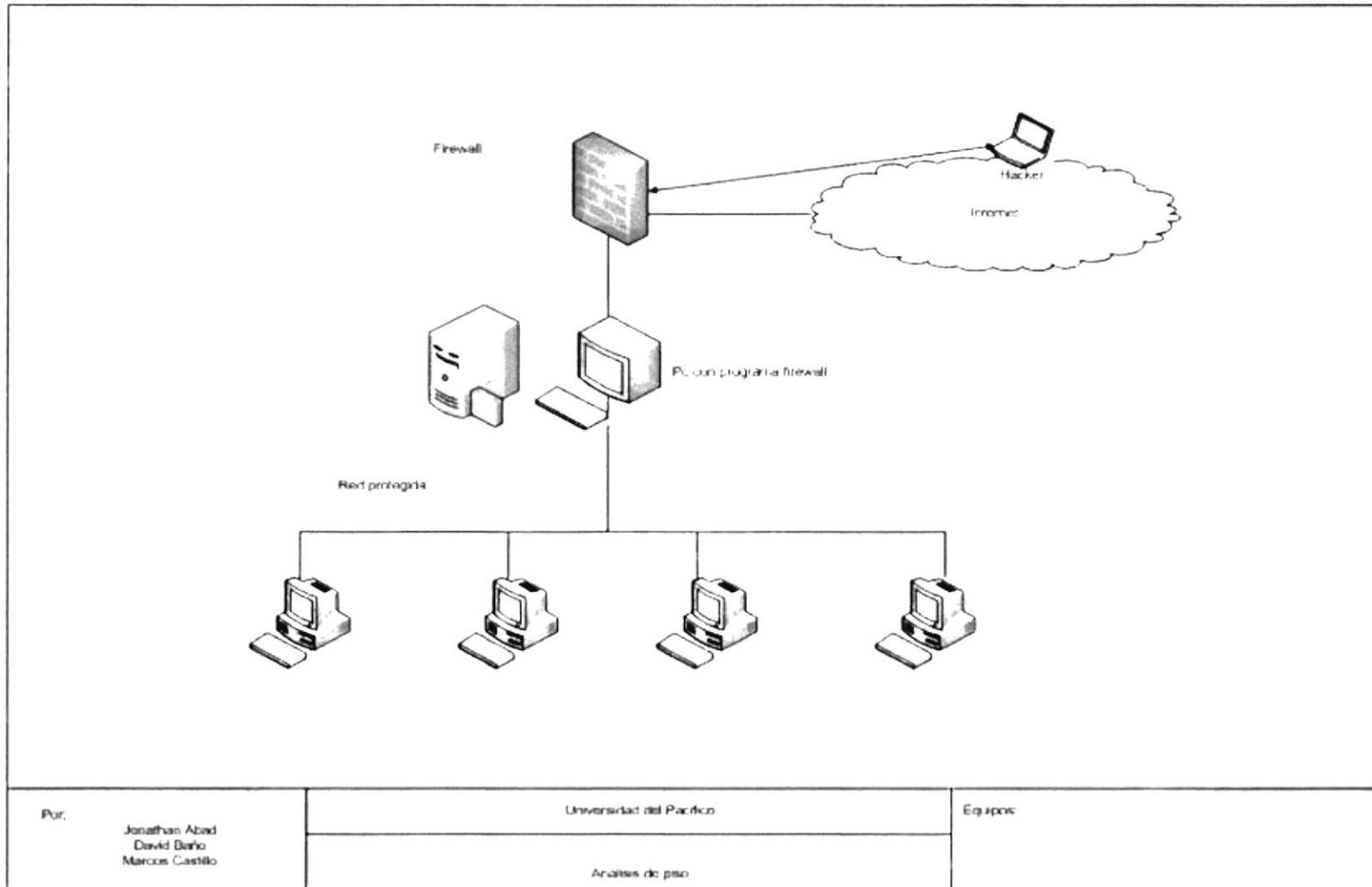


Figura 3-5 Análisis de Piso

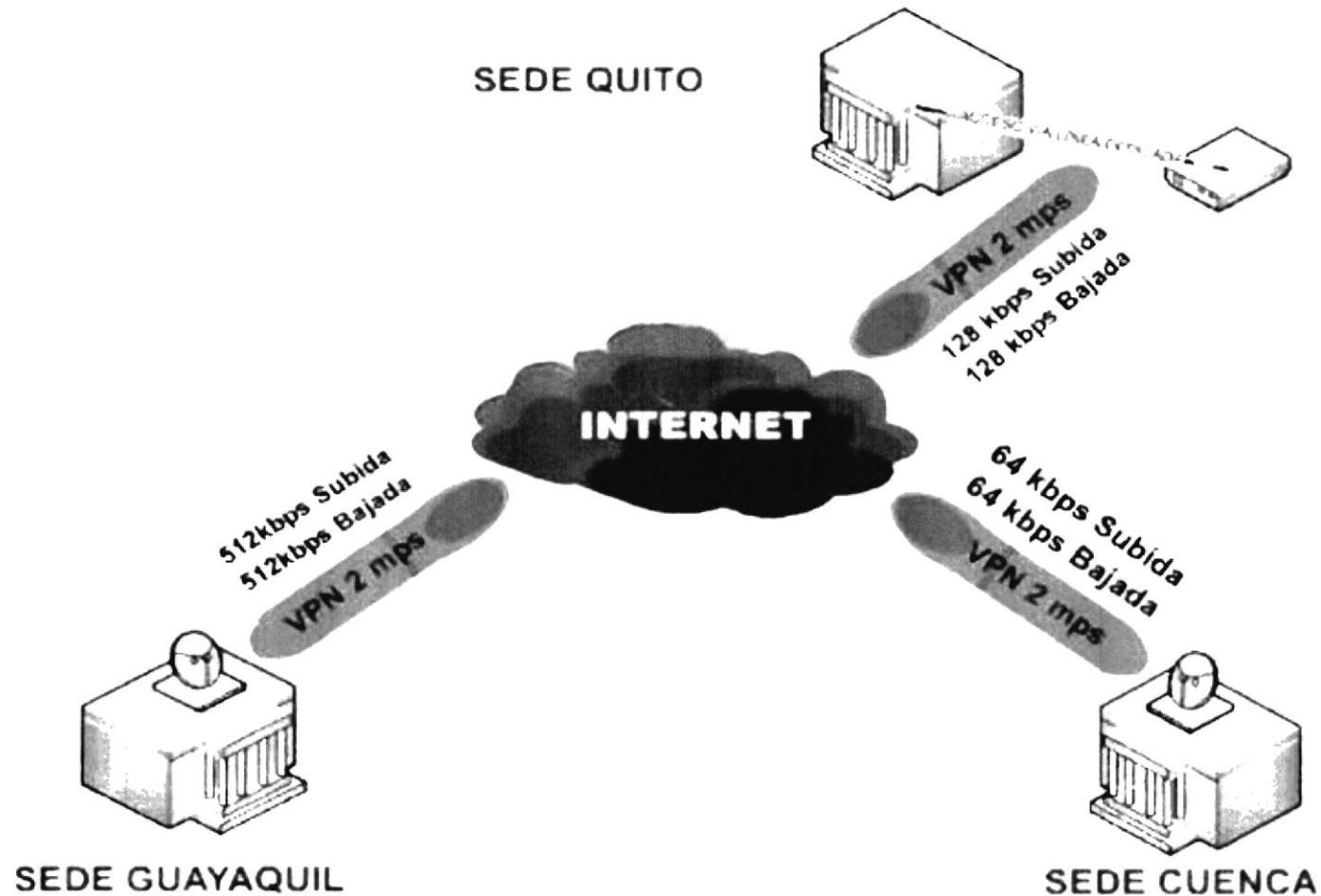


Figura 3-6 Comunicación a nivel WAN

Faint, illegible text, possibly bleed-through from the reverse side of the page.



CAPÍTULO 4

ROUTER

4 INTRODUCCION A ROUTER

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio. Cuenta con una CPU, memoria, bus de sistema y distintas interfaces de entrada/salida.

Sin embargo, los routers están diseñados para cumplir algunas funciones muy específicas que, en general, no realizan los computadores de escritorio. Por ejemplo, los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

Al igual que los computadores, que necesitan sistemas operativos para ejecutar aplicaciones de software, los routers necesitan el software denominado Sistema operativo de internetworking (IOS) para ejecutar los archivos de configuración. Estos archivos de configuración contienen las instrucciones y los parámetros que controlan el flujo del tráfico entrante y saliente de los routers. Específicamente, a través de los protocolos de enrutamiento, los routers toman decisiones sobre cuál es la mejor ruta para los paquetes. El archivo de configuración especifica toda la información necesaria para una correcta configuración y uso de los protocolos enrutados y de enrutamiento seleccionado, o habilitado, en el router

4.1 COMPONENTES INTERNOS DEL ROUTER

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

La **RAM**, también llamada RAM dinámica (DRAM), tiene las siguientes características y funciones:

- Almacena las tablas de enrutamiento.
- Guarda el caché ARP.
- Guarda el caché de conmutación rápida.
- Crea el buffer de los paquetes (RAM compartida).
- Mantiene las colas de espera de los paquetes.
- Brinda una memoria temporal para el archivo de configuración del router mientras está encendido.
- Pierde el contenido cuando se apaga o reinicia el router.

La **NVRAM** tiene las siguientes características y funciones:

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

La memoria flash tiene las siguientes características y funciones:

- Guarda la imagen del sistema operativo (IOS)

- Permite que el software se actualice sin retirar ni reemplazar chips en el procesador.
- Retiene el contenido cuando se apaga o reinicia el router.
- Puede almacenar varias versiones del software IOS.
- Es un tipo de ROM programable, que se puede borrar electrónicamente (**EEPROM**)

La memoria de sólo lectura (**ROM**) tiene las siguientes características y funciones:

- Guarda las instrucciones para el diagnóstico de la prueba al inicio (POST).
- Guarda el programa bootstrap y el software básico del sistema operativo.
- Requiere del reemplazo de chips que se pueden conectar en el motherboard para las actualizaciones del software.

Las interfaces tienen las siguientes características y funciones:

- Conectan el router a la red para permitir que las tramas entren y salgan.
- Pueden estar en el motherboard o en un módulo aparte.

4.2 LA FUNCION DE UN ROUTER EN UNA RED WAN

Una de las funciones de un router en una WAN es enrutar los paquetes en la capa 3, pero esta también es la función de un router en una LAN. Por lo tanto, el enrutamiento no es estrictamente una función de un router en la WAN. Cuando un router usa los protocolos y los estándares de la capa de enlace de datos y física asociados con las WAN, opera como dispositivo WAN. Las funciones principales de un router en una WAN, por lo tanto, no yacen en el enrutamiento sino en proporcionar las conexiones con y entre los diversos estándares de enlace de datos y físico WAN.

4.3 CARACTERISTICAS FISICAS DE UN ROUTER

No es necesario conocer la ubicación de los componentes físicos dentro del router para saber cómo utilizarlo. Sin embargo, en algunas situaciones, tales como agregar memoria, puede resultar muy útil.

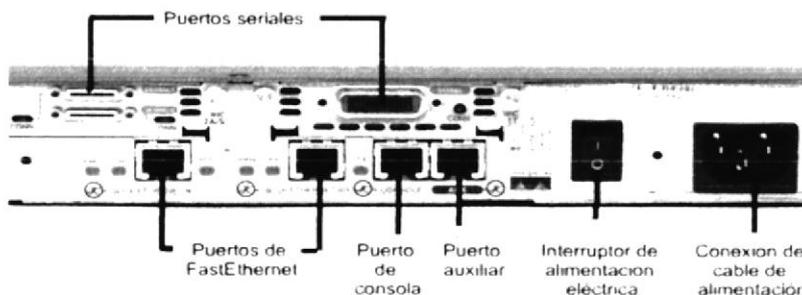


Figura 4-1 Componentes externos de un router

4.3.1 CONEXIONES EXTERNAS DE UN ROUTER

Los tres tipos de conexiones básicas de un router son las interfaces LAN, las interfaces WAN y los puertos de administración.

LAS INTERFACES LAN permiten que el router se conecte a los medios de la Red del área local. Por lo general, esta es una forma de Ethernet.

LAS CONEXIONES WAN proporcionan conexiones a través de un proveedor del servicio a un sitio lejano o a la Internet. Estas pueden ser conexiones seriales o cualquier número de otras interfaces WAN.

LA FUNCION DE LOS PUERTOS DE ADMINISTRACION 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

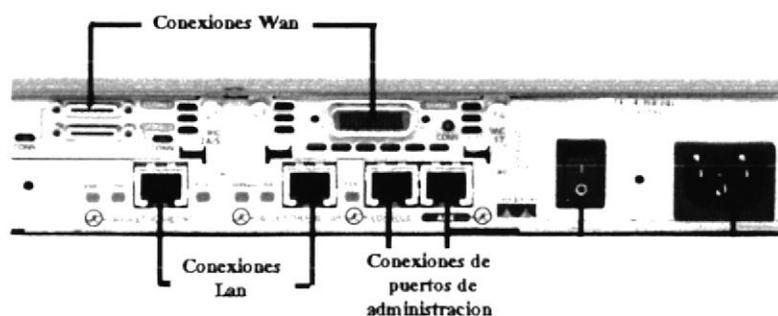


Figura 4-2 Conexiones externas de un router

4.3.2 CONEXION DE PUERTO DE ADMINISTRACION

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.

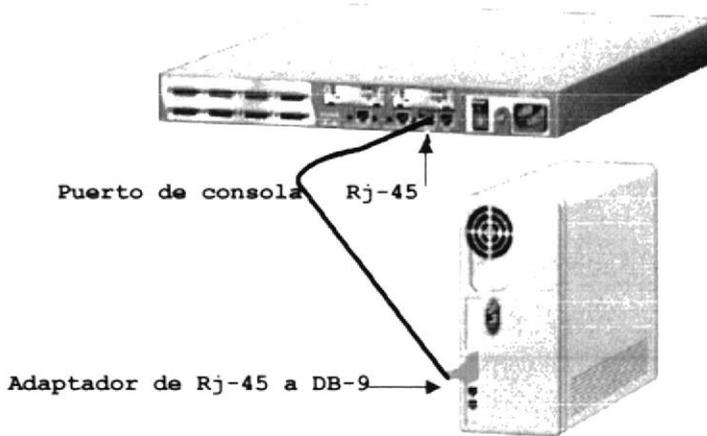


Figura 4-3 Conexión de un puerto de administración

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.

4.4 CONEXION DE LAS INTERFACES DEL ROUTER

Las interfaces de router que más se usan en los servicios WAN son las interfaces seriales. Seleccionar el cable serial adecuado es tan sencillo como conocer las respuestas a la siguiente pregunta:

4.4.1 ¿SE CONECTA EL SISTEMA DE RED A UN DISPOSITIVO DE DTE O DCE?

El DTE y el DCE son dos tipos de interfaces seriales que los dispositivos usan para comunicarse. La diferencia clave entre los dos es que el dispositivo DCE proporciona la señal reloj para las comunicaciones en el bus. La documentación del dispositivo debe especificar si es DTE o DCE.



Figura 4-4 Cable de datos entre Routers

4.4.2 ESTABLECIMIENTO DE UNA SESION HYPERTERMINAL

Se requiere cables y adaptadores para conectar una terminal de consola al puerto de consola. Una terminal de consola es una terminal ASCII o un PC que ejecuta un software de emulación de terminal como, por ejemplo, Hyper Terminal. Para conectar un PC que ejecuta un software de emulación de terminal al puerto de consola, use un cable transpuesto RJ-45 a RJ-45 con un adaptador hembra RJ-45 a DB-9.

- 1.- Primero se da clic al botón **Inicio** el mismo que desplegará un siguientes submenú de opciones como se observa en la figura a continuación.
- 2.- En el submenú se selecciona **Todos los Programas**
- 3.- Luego se selecciona el submenú **Accesorios**
- 4.- Ahora se da clic al submenú **Comunicaciones**
- 5.- Y finalmente se ingresa al programa **Hyper Terminal**

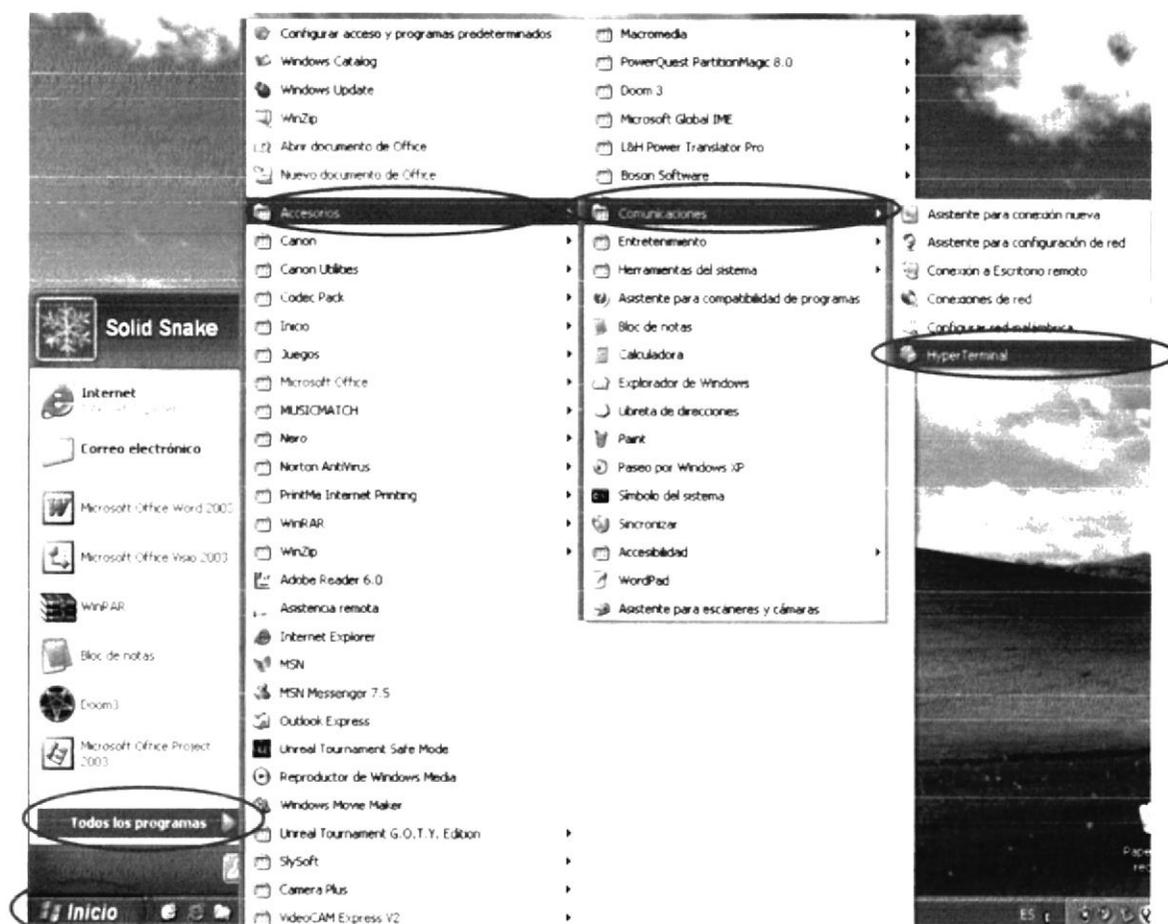


Figura 4-5 Pasos para ingresar al Hyper Terminal

6.- En esta ventana se escribe el nombre de la conexión



Figura 4-6 Ingreso del nombre de la conexión

7.- Aquí se selecciona el tipo de puerto que vamos a utilizar para la comunicación del computador y el router.



Figura 4-7 Selección del puerto de conexión

8.- Una vez seleccionado el puerto de conexión se da clic en el botón aceptar



Figura 4-8 Clic en el botón Aceptar para ingresar los cambios del puerto seleccionado

9.- En esta ventana se debe seleccionar la velocidad de conexión del router

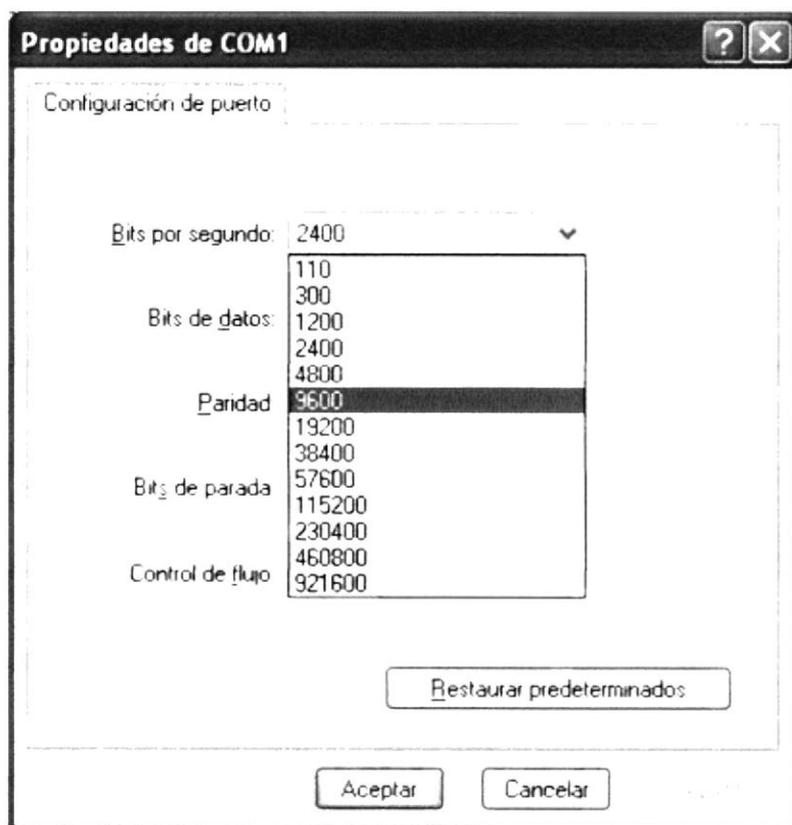


Figura 4-9 Selección de la velocidad del puerto del router

10.- Luego se da clic en el botón **Aceptar**

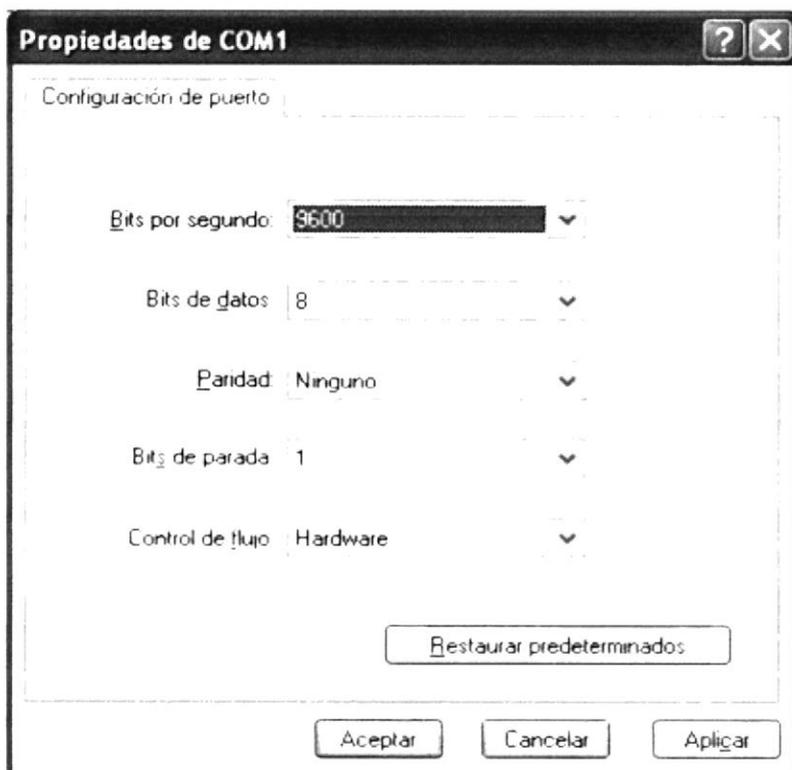


Figura 4-10 Clic en Aceptar para ingresar los cambios de la velocidad de conexión

11.- Finalmente aparece la pantalla en donde se va a realizar las configuraciones de todos los routers.

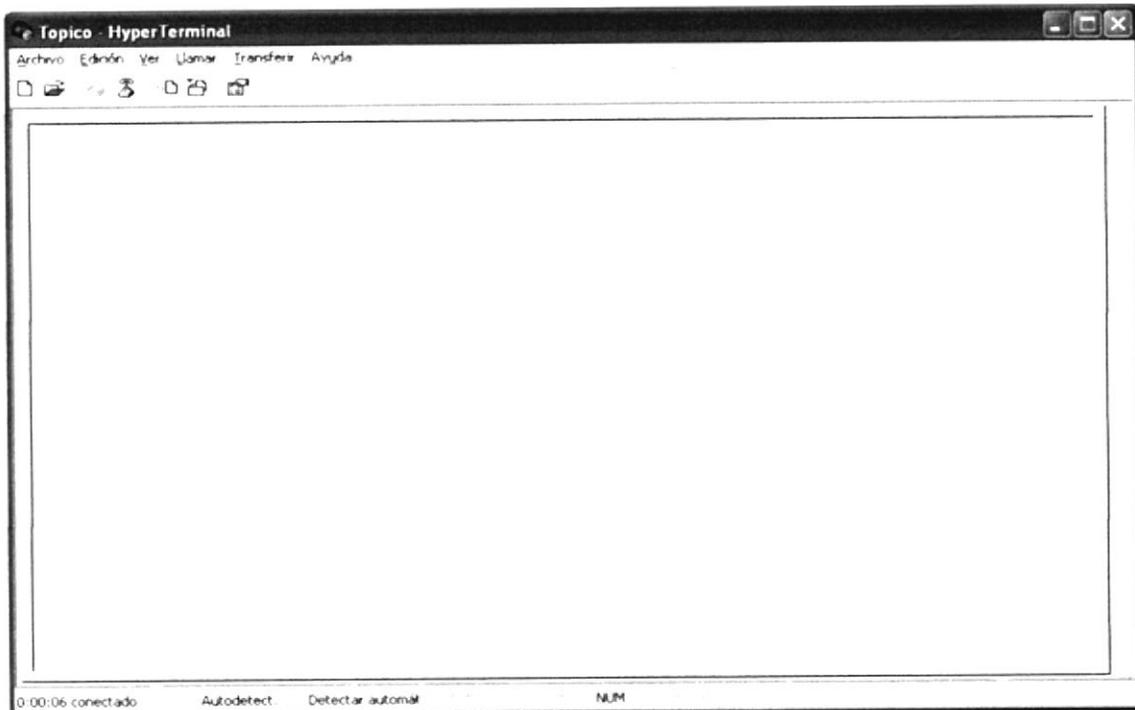


Figura 4-11 Pantalla inicial del Hyper Terminal

4.5 CONFIGURACION DE UN ROUTER

Para configurar los routers Cisco, se debe ingresar a la interfaz de usuario del router mediante una terminal o un acceso remoto. Al ingresar a un router, el usuario debe iniciar una sesión antes de ejecutar cualquier otro comando.

Por razones de seguridad, el router tiene dos niveles de acceso a los comandos:

- **Modo EXEC usuario:** Las tareas típicas incluyen la verificación del estado del router. En este modo no se permiten cambios en la configuración del router.
- **Modo EXEC privilegiado:** Las tareas típicas incluyen cambios a la configuración del router.

4.5.1 COMANDOS BASICOS DE ROUTER

Comando	Descripción
Enable	Modo privilegiado
Disable	Lo toma del modo privilegiado atrás al modo usuario
Config Terminal	Lo pone en modo de configuración global.
Interface	Lo pone en modo de configuraciones de interfaz
Line console 0	Lo pone en modo de configuración consola
Line vty	Lo pone en vty (telnet)el modo de configuración de interfaz
Enable password	
Enable secret	
Service password-encryption	Encripta el modo del usuario y habilita la contraseña
Interfase serial 0/0	Lo pone en modo de la configuración para la interfaz serial
Shutdown	Pone una interfaz en administrativamente abajo el modo.
No shutdown	Levantar la interfaz
Ip address	Dirección ip de una interfaz
Clock rate	Proporciona cronometrando en una interfaz de DCE de serie.
Bandwidth	
Hostname	Nombre de una fresadora
Description	Descripción de una interfaz
Copy run Star	Para copiar.
Show run	Muestra la configuración que corre actualmente en la fresadora
Show Star	Muestra la configuración auxiliar guardada en la NVRAM
Ping	Prueba de conectividad de ip
Traceroute	Prueba de conectividad de ip
Telnet	Prueba de conectividad de ip y configura una fresadora
Show controllers	Muestra el DTE o estado de DCE de una interfaz
Show version	Muestra las estadísticas de la fresadora
Show flash	Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí.
Show protocols	Muestra el estado global y por interfaces de cualquier protocolo de capa 3 que haya sido configurado.

Tabla 4-1 Comandos Básicos de Router

4.6 GRAFICO A CONFIGURAR

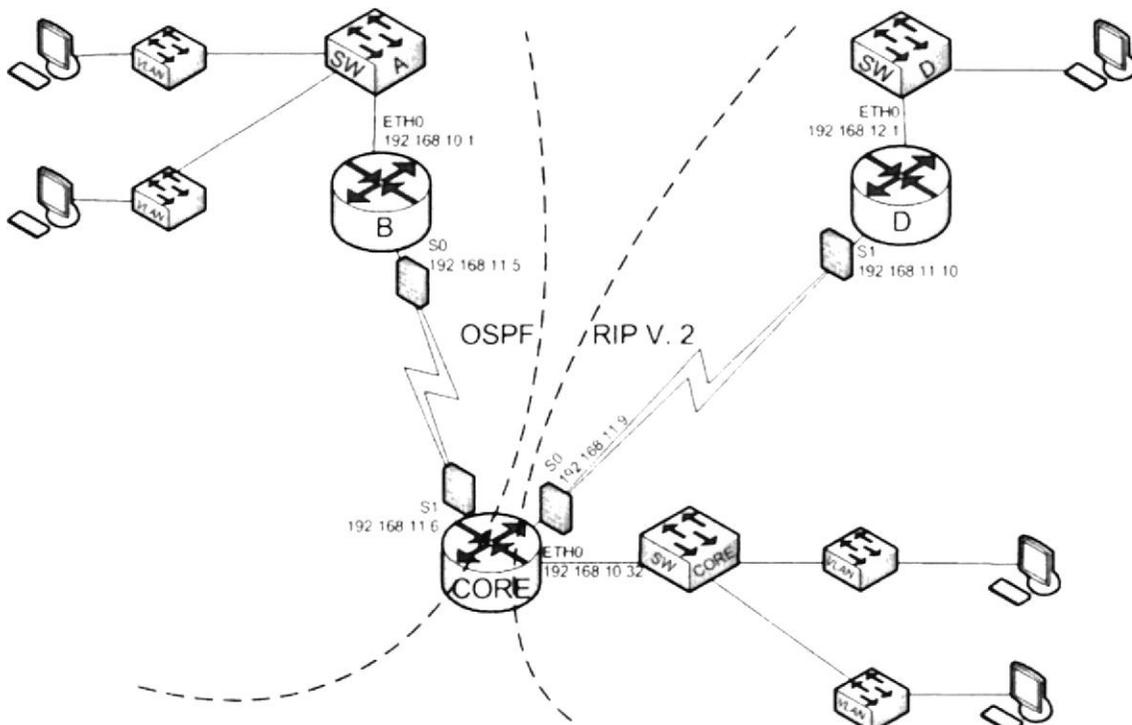


Figura 4-12 Grafico de Configuración WAN

4.7 ROUTER B

- 1.- Se debe ingresar al modo privilegiado para poder realizar todas las configuraciones

Press Enter to Start

Router> ← símbolo modo Exec usuario

Router>**ena**

- 2.- Debe ingresar al modo privilegiado

Router# ← simbolo modo Exec Privilegiado

- 3.- A continuación se ingresará al Modo de Configuración Global o CONFIGURE TERMINAL: el cual permitirá configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc.

Router#**configure terminal**

Router(config)#exit

Router#

4.- Aunque es opcional, se recomienda configurar una contraseña para la línea de comando. Los siguientes comandos se utilizan para fijar contraseña de modo privilegiado.

```
Router(config)#line console 0  
Router(config-line)#password cisco  
Router(config-line)#login  
Router(config-line)#exit
```

5.- Se fijan contraseñas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante Telnet. Normalmente, los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY.

```
Router(config)#line vty 0 4  
Router(config-line)#password cisco  
Router(config-line)#login  
Router(config-line)#exit
```

6.- El comando **enable password** se utiliza sólo si no se ha configurado previamente **enable secret**.

```
Router#conf terminal  
Router(config)# enable password cisco  
Router(config)#exit
```

7.- Para verificar los passwords creados debe salir totalmente de los routers digitando **exit** las veces que sean necesarias hasta que el router pida presionar una tecla para continuar.

```
Router(config)#exit  
Router#exit  
Press RETURN to get started.
```

8.- Para ingresar al modo usuario esta vez no va a pedir el password y se escribe lo siguiente:

```
Password: (nombre del password)  
Enter password:
```

9.- Y para ingresar al modo privilegiado se digita:

```
Router>ena  
Enter password: (nombre del password)
```

10.- Asignación de nombre al router esto se realiza en el modo de configuración global, mediante los siguientes comandos:

```
Router#configure terminal  
Router(config)#hostname R_B  
R_B(config)#
```

11.- Asignación de las direcciones IP a los puerto serial 0, cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

```
R_B#configure terminal  
R_B(config)#interface serial 0  
R_B(config-if)#ip address 192.168.11.5 255.255.255.252
```

Las interfaces seriales necesitan una señal de sincronización que controle la comunicación. En la mayoría de los entornos, un dispositivo DCE. Se activa la sincronización y se fija la velocidad mediante el comando **clock rate**. Las velocidades de sincronización disponibles (en bits por segundo) a tomar es de 56000.

```
R_B(config-if)#clock rate 56000
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se debe ingresar el comando **no shutdown**.

```
R_B(config-if)#no shutdown  
R_B(config-if)# exit  
R_B#wr  
Building configuration...  
[OK]
```

12.- Para configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual. A cada interfaz Ethernet activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

```
R_B#configure terminal  
R_B(config)#interface fastethernet 0.0  
R_B(config-subif)#ip address 192.168.10.1 255.255.255.240
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**.

```
R_B(config-subif)#no shutdown  
R_B(config-subif)# exit  
R_B#wr  
Building configuration...  
[OK]
```

4.8 VLANS

Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por función laboral o departamento, sin importar la ubicación física de los usuarios. El tráfico entre las VLAN está restringido.

Los switches y puentes envían tráfico unicast, multicast y broadcast sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. Los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN.

Los routers suministran conectividad entre diferentes VLAN. Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica.

Las VLAN simplifican las tareas cuando es necesario hacer agregados, mudanzas y modificaciones en una red. Las VLAN mejoran la seguridad de la red y ayudan a controlar los broadcasts de Capa 3.

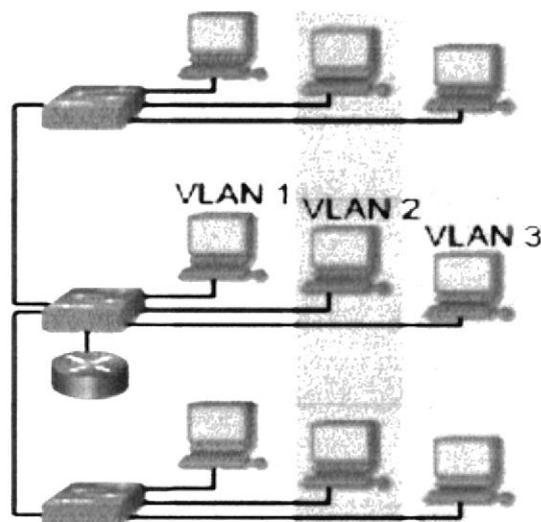


Figura 4-13 Arquitectura de las Vlan

4.8.1 TIPOS DE VLANS

Existen 3 tipos de vlans:

- Vlans por puerto
- Vlans por direcciones MAC
- Vlans por protocolos

4.8.2 VLANS POR PUERTO

El método de configuración es mas común, los puertos se asignan individualmente, en grupos, en filas o en 2 o mas switches. Se implementa a menudo donde el protocolo de control dinámico (DHCP).

4.8.3 VLANS POR DIRECCIONES MAC

Se implementa en escasa frecuencia hoy en día la administración es compleja y es necesario introducir y configurar cada dirección de forma individual.

4.8.4 VLANS POR PROTOCOLO

Se configuran como las direcciones MAC, pero usan una dirección lógica o IP pero ya no son comunes debido a que existe DHCP.

4.9 CONFIGURACION DE VLANS

Para configurar las vlans se debe ingresar en el MODO PRIVILIGED EXEC, luego ingresar al modo de configuración de vlan con el comando "**vlan database**" después ingresar la línea de comando "**vlan <numero de vlan> name <nombre>**" por ultimo salimos de la configuración con el comando "**exit**".

```
SW_B>enable
SW_B#
SW_B# vlan database
SW_B(vlan)#
SW_B(vlan)#vlan 20 name sistemas
SW_B(vlan)#exit
SW_B#
```

4.9.1 ASIGNAR PUERTOS A UNA VLAN

Las vlans pueden tener uno o varios puertos asignados, para asignar un puerto a la vlan debemos estar en el modo de configuración global e ingresar al puerto que se desee agregar a la vlan , una vez adentro digitar el comandos "**switchport mode access**" luego digitar el comando "**switchport access vlan <numero de vlan>**" y por ultimo salimos de modo de configuración global con el comando "**exit**".

```
SW_B>enable
SW_B#
SW_B(Config)#
SW_B(Config)#interface fastethernet 0/2
SW_B(config-if)#
SW_B(config-if)#switchport mode access
```

```
SW_B(config-if)#switchport access vlan 20
SW_B(config-if)#exit
SW_B#
```

4.9.2 ASIGNAR SWITCH DE TIPO SERVER

El rol de VTP es mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común. VTP es un protocolo de mensajería que usa tramas de enlace troncal de Capa 2 para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio. VTP también admite cambios centralizados que se comunican a todos los demás switches de la red. VTP mantiene su propia NVRAM.

13.- Para determinar un switch de tipo Server se debe estar en el MODO PRIVILEGED EXEC e ingresar al modo de configuración de vlans con el comando "**vlan database**", una vez adentro digitar la línea de comando "**vtp <Server o client>**" después se digita el comando "**vtp domain <nombre del dominio>**" y por ultimo salir de la configuración con el comando "**exit**".

```
SW_B>enable
SW_B#
SW_B# vlan database
SW_B(vlan)#vtp Server
SW_B(vlan)#vtp domain tópico
SW_B(vlan)#exit
SW_B#
```

4.10 COMUNICACION ENTRE VLANS

Por ultimo en el router principal se debe estar en el modo de configuración global para así ingresar a la interfaz ethernet con el comando "**interface ethernet<numero de interfaz>**", levantamos la interface con el comando "**no shutdown**" después ingresar a la sub interface ethernet con el comando "**interface ethernet<numero de interfaz. numero de subinterfaz>**" una vez a dentro se digita el protocolo de comunicación de vlans dot1q con el comando "**encapsulation dot1q <numero de vlan>**" luego la dirección ip de la vlan con su máscara con el comando "**ip address, mask**" y por ultimo salir del modo de configuración global con el comando "**exit**".

```
SW_B# configure terminal
SW_B(config)# interface Ethernet 0
SW_B(config-if)# no shutdown
SW_B(config-if)# interface Ethernet 0.1
SW_B(config-subif)# encapsulation dot1q 1
SW_B(config-subif)# ip address 192.168.1.1 255.255.255.240
SW_B(config-subif)# interface Ethernet0.2
SW_B(config-subif)# encapsulation dot1q 10
SW_B(config-subif)# ip address 192.168.1.17 255.255.255.240
SW_B(config-subif)# interface Ethernet0.3
SW_B(config-subif)# encapsulation dot1q 20
```

```

SW_Bconfig-subif)# ip address 192.168.1.33 255.255.255.240
SW_Bconfig-subif)# interface Ethernet0.4
SW_Bconfig-subif)# encapsulation dot1q 30
SW_Bconfig-subif)# ip address 192.168.1.49 255.255.255.240
SW_Bconfig-subif)# interface Ethernet0.5
SW_Bconfig-subif)# encapsulation dot1q 40
SW_Bconfig-subif)# ip address 192.168.1.65 255.255.255.240
SW_Bconfig-subif)# interface Ethernet0.6
SW_Bconfig-subif)# encapsulation dot1q 50
SW_Bconfig-subif)# ip address 192.168.1.81 255.255.255.240
SW_Bconfig-subif)# interface Ethernet0.7
SW_Bconfig-subif)# encapsulation dot1q 60
SW_Bconfig-subif)# ip address 192.168.1.97 255.255.255.240
SW_Bconfig-subif)# interface Ethernet0.8
SW_Bconfig-subif)# encapsulation dot1q 70
SW_Bconfig-subif)# ip address 192.168.1.113 255.255.255.240
SW_Bconfig-subif)# interface Ethernet0.9
SW_Bconfig-subif)# encapsulation dot1q 80
SW_Bconfig-subif)# ip address 192.168.1.129 255.255.255.240
SW_B(config-if)# exit
SW_B#

```

4.10.1 ELIMINAR VLANS

Para eliminar la información de VLAN actual, borre el archivo de la base de datos VLAN, denominado **vlan.database**, del directorio flash con el comando “**delete flash:vlan.database**”.

4.10.2 SHOW VLANS

Se muestra todas las vlans creadas con sus respectivos puertos asignados.

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/10, Fa0/11, Fa0/12
10 Sistemas	active	Fa0/2
20 Administración	active	Fa0/3
30 Laboratorio	active	Fa0/4
40 40	active	Fa0/5
50 50	active	Fa0/6
60 60	active	Fa0/7

```

70 70          active Fa0/8

80 80          active Fa0/9
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

```

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
60	enet	100060	1500	-	-	-	-	-	0	0
70	enet	100070	1500	-	-	-	-	-	0	0
80	enet	100080	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```
SW_CORE# delete flash:vlan.database.
```

4.10.3 SH RUN

```

B#sh run
Building configuration...
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname B
enable password cisco
!
ip subnet-zero
!
interface Serial0
ip address 192.168.11.5 255.255.255.252
no ip directed-broadcast
clock rate 56000
bandwidth 1544

interface Serial1
no ip address

```

```

no ip directed-broadcast
bandwidth 1544
shutdown
!
interface Ethernet0
ip address 192.168.10.1 255.255.255.240
no ip directed-broadcast
bandwidth 10000
ip ospf cost 100
!
router ospf 1
network 192.168.10.0 0.0.0.31 area 1
network 192.168.11.4 0.0.0.3 area 1
!
ip classless
no ip http server
!
line con 0
login
transport input none
password cisco
line aux 0
line vty 0 4
login
password cisco
!
no scheduler allocate
end

```

4.10.4 SH INTERFACES ROUTER B

```

B#sh interfaces
Serial0 is up, line protocol is up
  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 is administratively down, line protocol is down
Hardware is HD64570
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 000C.3782.8690 (bia 000C.3782.8690)
Internet address is 192.168.10.1/28
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

4.10.5 SHOW IP ROUTE

B#show ip route

El comando show ip route verifica la rutas en la tabla de enrutamiento.

B#show run

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 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, N2 - 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 inter 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

Subnetización con VLSM.

El segmento de red 192.168.12.0 posee dos subredes y dos máscaras.

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

El segmento de red 192.168.12.4 está directamente conectada a un enlace serial 0.

C 192.168.12.4/30 is directly connected, Serial0

El segmento de red 192.168.12.0 y la 192.168.13.0 están configuradas con protocolos de enrutamiento RIP versión 2 saliendo por la IP 192.168.2.5 en un enlace serial 0 con actualizaciones de 5 segundos, el **120** se refiere a la distancia, **10** el numero de saltos y vía es para indicar el rombo de los paquetes.

R 192.168.12.0/24 [120/1] vía 192.168.12.6, 00:00:05, Serial0

R 192.168.13.0/24 [120/10] vía 192.168.11.6, 00:00:05, Serial0

4.11 ROUTER CORE

- 1.- Ingresar al modo privilegiado para poder realizar todas las configuraciones

```
Router>ena Press Enter to Start
Router> ← simbolo modo Exec usuario
Router>ena
```

- 2.- A continuación se ingresara al modo privilegiado

```
Router# ← simbolo modo Exec Privilegiado
```

- 3.- Ingresar al Modo de Configuración Global que le permitirá configurar nombre el router, password, etc.

```
Router#configure terminal
```

Aunque es opcional, se recomienda configurar una contraseña para la línea de comando. Los siguientes comandos se utilizan para fijar dicha contraseña.

```
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
```

- 4.- Ahora se fijará contraseñas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante Telnet. Normalmente, los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY.

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable password cisco
```

- 5.- Para verificar los passwords creados salimos totalmente de los routers digitando exit las veces que sean necesarias hasta que el router pida presionar una tecla para continuar

```
Router(config)#exit
Router#exit
Press RETURN to get started.
```

- 6.- Para ingresar al modo usuario esta vez nos debe pedir el password y se digita la clave lo siguiente:

```
Password: (nombre del password)
Enter password:
```

- 7.- Y para ingresar al modo privilegiado digitamos:

```
Router>ena
Enter password: (nombre del password)
```

8.- Asignación de nombre del router

```
Router#configure terminal  
Router(config)#hostname CORE  
CORE (config)#
```

9.- Asignación de las direcciones IP a los puerto serial 0 , cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

```
CORE #configure terminal  
CORE (config)#interface serial 0  
CORE (config-if)#ip address 192.168.11.9 255.255.255.252
```

Las interfaces seriales necesitan una señal de sincronización que controle la comunicación. En la mayoría de los entornos, un dispositivo DCE. Se activa la sincronización y se fija la velocidad mediante el comando **clock rate**. Las velocidades de sincronización disponibles (en bits por segundo) a tomar es de 56000.

```
CORE (config-if)#clock rate 56000
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**.

```
CORE (config-if)#no shutdown  
CORE (config-if)#^Z  
CORE #wr  
Building configuration...  
[OK]
```

10.- Asignación de las direcciones IP a los puerto serial 1

```
CORE #configure terminal  
CORE (config)#interface serial 1  
CORE (config-if)#ip address 192.168.11.6 255.255.255.252
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**.

```
CORE (config-if)#no shutdown  
CORE (config-if)#^Z  
CORE #wr  
Building configuration...  
[OK]
```

11.- Para configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual. A cada interfaz Ethernet activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

```
CORE#configure terminal  
CORE (config)#interface fastethernet 0.0  
CORE (config-subif)#ip address 192.168.10.32 255.255.255.240
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**.

```
CORE (config-subif)#no shutdown
CORE (config-subif)#^Z
CORE #wr
Building configuration...
[OK]
```

12.- Se procede a configurar OSPF de manera global.

4.11.1 CONFIGURACION DE PROTOCOLOS DE ENRUTAMIENTO

4.11.1.1 ¿QUE ES UN PROTOCOLO DE ENRUTAMIENTO?

Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. Los ejemplos de protocolos de enrutamiento incluyen el IGRP, el OSPF y el RIP.

4.11.1.2 OSPF (PROTOCOLO ESTADO ENLACE)

Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. Mientras que el algoritmo de vector-distancia posee información no específica acerca de las redes distantes y ningún conocimiento acerca de los routers distantes, un algoritmo de enrutamiento del estado de enlace tiene pleno conocimiento de los routers distantes y la forma en que se interconectan.

Características:

- Usa la ruta mas corta
- Las actualizaciones son por eventos
- Tiene una vista común de la red
- Consume menos ancho de banda
- Converge rápidamente
- No susceptible a bucles de enrutamiento
- Requiere mas potencia y memoria

Para configurar este protocolo de enrutamiento OSPF, debemos cambiarnos al modo de configuración global, luego establecer el protocolo con el comando "**router ospf area**" luego se deberá establecer con una o más órdenes "**network**", las redes directamente conectadas al router, seguido de la máscara wildcard y el área. Finalmente salimos con el comando "**exit**". A continuación vamos a ver la configuración del router CORE con el protocolo OSPF:

```

CORE#configure terminal
CORE(config)#router ospf 1
CORE(config-router)#network 192.168.11.6 0.0.0.3 area 0
CORE(config-router)#redistribute rip subnets
CORE (config-if)#^Z

```

4.11.1.3 PROTOCOLO RIP (VECTOR DISTANCIA)

En el protocolo de vector-distancia, las actualizaciones de las tablas de enrutamiento se hacen periódicamente, o cuando cambia la topología de la red. Es importante que un protocolo de enrutamiento sea eficiente en su tarea de actualizar las tablas de enrutamiento. Utiliza el número de saltos como métrica para la selección de rutas. Si el número de saltos es superior a 15, el paquete es desechado. Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

Para configurar un protocolo de enrutamiento RIP, se debe cambiar al modo de configuración global, luego debemos establecer con una o más órdenes “**network**”, las redes directamente conectadas al router y finalmente salir con el comando “**exit**”.

A continuación se va a configurar el router CORE con el protocolo rip :

```

CORE#configure terminal
CORE(config)#router rip
CORE(config-router)#version 2
CORE(config-router)#network 192.168.11.0

```

4.11.1.4 REDISTRIBUCION DE RUTAS

Al tener zonas que usan protocolos de encaminamiento distintos. Por ejemplo OSPF y RIPv2. Hay que inyectar las rutas que se aprenden de un protocolo a otro, este proceso se la llama “**redistribución de rutas**”. Lo lógico es que en una red corra un único protocolo de encaminamiento, pero imaginar que se unen dos redes con protocolos distintos y tienen que convivir (pueden incluso estar administrados por distintos departamentos).

La métricas de los protocolos son distintas: RIPv2 usa saltos (“hops”) y OSPF usa “Bandwidth”. OSPF: su métrica es bandwidth y usa costos con la fórmula $108 / \text{bandwidth (bps)}$. OSPF pone como costo igual a 20 por defecto al protocolo redistribuido (excepto BGP que le pone costo igual a 1). Como anuncia redes principales hay que añadir el parámetro subset para indicar que la red este subneteada. RIPv2:

```

CORE(config-router)#redistribute ospf 1
CORE(config-router)#default-metric 10
CORE (config-if)# exit

```

13.- Una vez configurada de manera global se procede a configurar OSPF dentro de la interfase correspondiente.

```

CORE#configure terminal
CORE(config)#interface serial 1

```

```
CORE(config-if)#router ospf 1
CORE(config-router)#redistribute rip subnets
CORE (config-if)#^Z
```

14.- De igual modo se procede a configurar Rip dentro de la interfase correspondiente

```
CORE(config)#interface serial 0
CORE(config-if)#router rip
CORE(config-router)#version 2
CORE(config-router)#redistribute ospf 1
CORE (config-if)#^Z
```

4.12 VLANS

Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por función laboral o departamento, sin importar la ubicación física de los usuarios. El tráfico entre las VLAN está restringido.

Los switches y puentes envían tráfico unicast, multicast y broadcast sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. Los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN.

Los routers suministran conectividad entre diferentes VLAN. Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica.

Las VLAN simplifican las tareas cuando es necesario hacer agregados, mudanzas y modificaciones en una red. Las VLAN mejoran la seguridad de la red y ayudan a controlar los broadcasts de Capa 3.

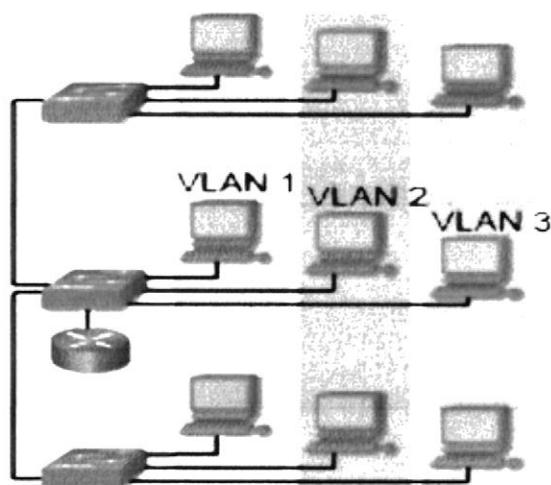


Figura 4-14 Arquitectura de las Vlan

4.12.1 TIPOS DE VLANS

Existen 3 tipos de vlans:

- Vlans por puerto
- Vlans por direcciones MAC
- Vlans por protocolos

4.12.2 VLANS POR PUERTO

El método de configuración es mas común, los puertos se asignan individualmente, en grupos, en filas o en 2 o mas switches. Se implementa a menudo donde el protocolo de control dinámico (DHCP).

4.12.3 VLANS POR DIRECCIONES MAC

Se implementa en escasa frecuencia hoy en día la administración es compleja y es necesario introducir y configurar cada dirección de forma individual.

4.12.4 VLANS POR PROTOCOLO

Se debe configurar como las direcciones MAC, pero usan una dirección lógica o IP pero ya no son comunes debido a que existe DHCP.

4.13 CONFIGURACION DE VLANS

Para configurar las vlans se debe ingresar en el MODO PRIVILIGED EXEC, luego ingresar al modo de configuración de vlan con el comando "**vlan database**" después ingresar la línea de comando "**vlan <numero de vlan> name <nombre>**" por ultimo salir de la configuración con el comando "**exit**".

```
SW_B>enable
SW_B#
SW_B# vlan database
SW_B(vlan)#
SW_B(vlan)#vlan 20 name sistemas
SW_B(vlan)#exit
SW_B#
```

4.13.1 ASIGNAR PUERTOS A UNA VLAN

Las vlans pueden tener uno o varios puertos asignados, para asignar un puerto a la vlan se debe ingresar en el modo de configuración global e ingresar al puerto que se desee agregar a la vlan , una vez adentro digitar el comando "**switchport mode access**" luego digitar el comando "**switchport access vlan <numero de vlan>** " y por ultimo salir de modo de configuración global con el comando "**exit**".

```
SW_B>enable
SW_B#
SW_B(Config)#
SW_B(Config)#interface fastethernet 0/2
SW_B(config-if)#
SW_B(config-if)#switchport mode access
SW_B(config-if)#switchport access vlan 20
SW_B(config-if)#exit
SW_B#
```

4.13.2 ASIGNAR SWITCH DE TIPO SERVER

El rol de VTP es mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común. VTP es un protocolo de mensajería que usa tramas de enlace troncal de Capa 2 para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio. VTP también admite cambios centralizados que se comunican a todos los demás switches de la red. VTP mantiene su propia NVRAM.

13.- Para determinar un switch de tipo Server debemos estar en el MODO PRIVILEGED EXEC e ingresar al modo de configuración de vlans con el comando "**vlan database**", una vez adentro digitar la línea de comando "**vtp <Server o client>**" después se digita el comando "**vtp domain <nombre del dominio>**" y por ultimo salir de la configuración con el comando "**exit**".

```
SW_B>enable
SW_B#
SW_B# vlan database
SW_B(vlan)#vtp Server
SW_B(vlan)#vtp domain tópico
SW_B(vlan)#exit
SW_B#
```

4.14 COMUNICACION ENTRE VLANS

Por ultimo en el router principal debera estar en el modo de configuración global para así ingresar a la interfaz ethernet con el comando "**interface ethernet<numero de interfaz>**", levantamos la interface con el comando "**no shutdown**" después ingresamos a la sub interface ethernet con el comando "**interface ethernet<numero de interfaz. número de subinterfaz>**" una vez a dentro digitamos el protocolo de comunicación de vlans dot1q con el comando "**encapsulation dot1q <número de**

vlan>” luego la dirección ip de la vlan con su máscara con el comando “**ip address, mask**” y por ultimo salimos del modo de configuración global con el comando “**exit**”.

```
SW_B# configure terminal
SW_B(config)# interface Ethernet 0
SW_B(config-if)# no shutdown
SW_B(config-if)# interface Ethernet 0.1
SW_B(config-subif)# encapsulation dot1q 1
SW_B(config-subif)# ip address 192.168.1.1 255.255.255.240
SW_B(config-subif)# interface Ethernet0.2
SW_B(config-subif)# encapsulation dot1q 10
SW_B(config-subif)# ip address 192.168.1.17 255.255.255.240
SW_B(config-subif)# interface Ethernet0.3
SW_B(config-subif)# encapsulation dot1q 20
SW_B(config-subif)# ip address 192.168.1.33 255.255.255.240
SW_B(config-subif)# interface Ethernet0.4
SW_B(config-subif)# encapsulation dot1q 30
SW_B(config-subif)# ip address 192.168.1.49 255.255.255.240
SW_B(config-subif)# interface Ethernet0.5
SW_B(config-subif)# encapsulation dot1q 40
SW_B(config-subif)# ip address 192.168.1.65 255.255.255.240
SW_B(config-subif)# interface Ethernet0.6
SW_B(config-subif)# encapsulation dot1q 50
SW_B(config-subif)# ip address 192.168.1.81 255.255.255.240
SW_B(config-subif)# interface Ethernet0.7
SW_B(config-subif)# encapsulation dot1q 60
SW_B(config-subif)# ip address 192.168.1.97 255.255.255.240
SW_B(config-subif)# interface Ethernet0.8
SW_B(config-subif)# encapsulation dot1q 70
SW_B(config-subif)# ip address 192.168.1.113 255.255.255.240
SW_B(config-subif)# interface Ethernet0.9
SW_B(config-subif)# encapsulation dot1q 80
SW_B(config-subif)# ip address 192.168.1.129 255.255.255.240
SW_B(config-if)# exit
SW_B#
```

4.14.1 ELIMINAR VLANS

Para eliminar la información de VLAN actual, borre el archivo de la base de datos VLAN, denominado **vlan.database**, del directorio flash con el comando “**delete flash:vlan.database**”.

4.14.1.1 SHOW VLANS CORE

Muestra todas las vlans creadas con sus respectivos puertos asignados.

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/10, Fa0/11, Fa0/12
10 Sistemas	active	Fa0/2
20 Administración	active	Fa0/3
30 Laboratorio	active	Fa0/4
40 40	active	Fa0/5
50 50	active	Fa0/6
60 60	active	Fa0/7
70 70	active	Fa0/8
80 80	active	Fa0/9
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
60	enet	100060	1500	-	-	-	-	-	0	0
70	enet	100070	1500	-	-	-	-	-	0	0
80	enet	100080	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

4.14.1.2 SHOW RUNNING CORE

Muestra el contenido del archivo de configuración activo, como las interfaces, nombre, y contraseñas.

```
CORE#sh run
Building configuration...
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CORE
enable password cisco
!
ip subnet-zero
!
interface Serial0
ip address 192.168.11.9 255.255.255.252
no ip directed-broadcast
clock rate 56000
bandwidth 1544
!
interface Serial1
ip address 192.168.11.6 255.255.255.252
no ip directed-broadcast
bandwidth 1544
!
interface Ethernet0
ip address 192.168.10.33 255.255.255.240
no ip directed-broadcast
bandwidth 10000
ip ospf cost 100
!
router rip

version 2
network 192.168.10.0
network 192.168.11.0
!
router ospf 1
network 192.168.11.4 0.0.0.3 area 1
!
ip classless
no ip http server
!
line con 0
login
transport input none
```

```

password cisco
line aux 0
line vty 0 4
login
password cisco
!
no scheduler allocate
end

```

4.14.1.3 SH IP ROUTE CORE

Muestra el contenido de una tabla de enrutamiento IP. Esta tabla contiene entradas para todas las redes y subredes conocidas, así como un código que indica como se aprendió la información, además muestra las interfaces por las que se llega a otras redes mediante los protocolos de enrutamiento Ej.: **O**: ospf, **R**: rip, **C**: directamente conectado, **[120/2]**: [dirección administrativa/ costo de la métrica], **vía a, b, c, d**: dirección de interfaz saliente **serial**: nombre de la interface saliente

```
CORE#sh ip route
```

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

```

```
Gateway of last resort is not set
```

```

192.168.10.0/28 is subnetted, 1 subnets
C    192.168.10.32 is directly connected, Ethernet0
192.168.11.0/30 is subnetted, 1 subnets
O    192.168.11.4 [110/64] via 192.168.11.6, 00:00:09, Ethernet0

```

4.14.1.4 SH INTERFACE CORE

Muestra la estadística completa de todas las interfaces del router.

```
CORE#sh interfaces
```

```

Serial0 is down, line protocol is down
  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
  Queuing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer

```

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

Serial1 is up, line protocol is up
Hardware is HD64570
Internet address is 192.168.11.6/30
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

Ethernet0 is up, line protocol is up
Hardware is Lance, address is 000C.2988.5967 (bia 000C.2988.5967)
Internet address is 192.168.10.33/28
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier

4.15 ROUTER D

- 1.- Ingresar al modo privilegiado para poder realizar todas las configuraciones

```
Router>ena Press Enter to Start
```

```
Router> ← simbolo modo Exec usuario
```

- 2.- Ingresar al modo privilegiado

```
Router# ← simbolo modo Exec Privilegiado
```

- 3.- Ingresar al modo de Configuración Global que nos permite configura nombre del router, password, etc.

```
Router#configure terminal
```

Aunque es opcional, se recomienda configurar una contraseña para la línea de comando. Los siguientes comandos se utilizan para fijar dicha contraseña.

```
Router(config)#line console 0
```

```
Router(config-line)#password cisco
```

```
Router(config-line)#login
```

```
Router(config-line)#exit
```

- 4.- Ahora fijamos contraseñas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante Telnet. Normalmente, los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY.

```
Router(config)#line vty 0 4
```

```
Router(config-line)#password cisco
```

```
Router(config-line)#login
```

```
Router(config-line)#exit
```

```
Router(config)#enable password cisco
```

- 5.- Para verificar los passwords creados salimos totalmente de los routers digitando exit las veces que sean necesarias hasta que el router pida presionar una tecla para continuar

```
Router(config)#exit
```

```
Router#exit
```

```
Press RETURN to get started.
```

- 6.- Para ingresar al modo usuario esta vez nos debe pedir el password y digita lo siguiente:

```
Password: (nombre del password)
```

```
Enter password:
```

- 7.- Y para ingresar al modo privilegiado digitamos:

```
Router>ena
```

```
Enter password: (nombre del password)
```

8.- Asignación del nombre al router

```
Router#configure terminal  
Router(config)#hostname R_D  
R_D(config)#
```

9.- Asignación de las direcciones IP al puerto serial 0 , cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

```
R_D#configure terminal  
R_D(config)#interface serial 1  
R_D(config-if)#ip address 192.168.11.10 255.255.255.252
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**.

```
R_D(config-if)#no shutdown  
R_D(config-if)#exit  
R_D#wr  
Building configuration...  
[OK]
```

10.- Como usted sabe que puerto es el que actúa de DCE, tiene que dar reloj. Está opción la tenemos que activar vía IOS con el comando “**clockrate Bw**”, donde **Bw** son los bps a los que queremos que trabaje la línea. En el puerto DTE no debe activar este comando.

```
R_D#configure terminal  
R_D(config)#interface fastethernet 0.0  
R_D(config-subif)#ip address 192.168.12.1 255.255.255.240
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**.

```
R_D(config-subif)#no shutdown  
R_D(config-subif)#exit  
R_D#wr  
Building configuration...  
[OK]
```

4.15.1 USO DE LOS COMANDOS SHOW

Los numerosos comandos **show** se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas. Tanto en el modo EXEC privilegiado como en el modo EXEC de usuario, el comando **show ?** muestra una lista de los comandos **show** disponibles.

- **show interfaces:** Muestra las estadísticas completas de todas las interfaces del router. Por ejemplo:

```
Router#show interfaces serial 0/1
```

- **show controllers serial:** muestra información específica de la interfaces de hardware. por ejemplo:

```
Router#show controllers serial 0/1
```

- **show clock:** Muestra la hora fijada en el router.
- **show hosts:** Muestra la lista en caché de los nombres de host y sus direcciones.
- **show users:** Muestra todos los usuarios conectados al router.
- **show history:** Muestra un historial de los comandos ingresados.
- **show flash:** Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí.
- **show version:** Despliega la información acerca del router y de la imagen de IOS que esté corriendo en al RAM.
- **show ARP:** Muestra la tabla ARP del router.
- **show protocols:** Muestra el estado global y por interfaces de cualquier protocolo de capa 3 que haya sido configurado.
- **show startup-configuration:** Muestra el archivo de configuración almacenado en la NVRAM.
- **show running-configuration:** Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica.

4.16 LISTAS DE ACCESO

Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior. Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router permitiendo la administración del tráfico.

Las ACL pueden aplicarse en Protocolos Enrutados:

- Protocolo de Internet (IP)
- Intercambio de paquetes de Internetwork (IPX)

Las ACL se definen según el protocolo

4.16.1 TIPOS DE ACLS

- Estándar (cerca del posible destino) del 1-99 o 1300,1999
- Extendidas (cerca del posible origen) de 100 1999 o 2000-2699

4.16.2 FUNCION DE LA WILCARD

Las máscaras de wildcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas.

La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros. La opción any reemplaza la dirección IP con 0.0.0.0 y la máscara wildcard por 255.255.255.255. Esta opción concuerda con cualquier dirección con la que se la compare.

4.16.3 DIRECCIONES DE TRAFICO

La dirección in o out (entrada o salida) determina si se va a permitir entrada o salida de tráfico en el router que se está configurando en el momento. El comando “**ip access group**” enlaza una ACL existente con una interfaz. Solo se permite una ACL por interfaz, por dirección, o por protocolo.

Las acls se crean en el modo de configuración global con el comando:

```
“Access-list <número de access list> <permit/deny> < test-conditions >”
“access-list number < permit/deny > <test-conditions>”.
```

Por último ingresamos a la interface ethernet en la cual se va a determinar si va permitir entrada o salida de tráfico:

```
“ip access-group access-list-number”
```

A continuación un ejemplo de ACL denegando el acceso al Servidor de las demás redes

```
R_D#configure terminal
R_D(config)# access-list 2 permit host 192.168.11.8
R_D(config)# access-list 2 deny any any
R_D(config)# interface Ethernet 0
R_D(config-if)# ip access-group 2 out
R_D(config-if)#exit
R_D(config)#exit
R_D# wr
```

4.16.4 VERIFICACION DE LA ACL

Existen varios comandos show que verifican el contenido y ubicación de las ACL en el router.

- El comando show ip interface muestra información de la interfaz IP e indica si se ha establecido alguna ACL.
- El comando show access-lists muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número ACL como opción a este comando.
- El comando show running-config también revela las listas de acceso en el router y la información de asignación de interfaz.

4.17 SWITCHES

Un switch es un dispositivo de red de Capa 2 que actúa como punto de concentración para la conexión de estaciones de trabajo, servidores, routers, hubs y otros switches. Los switches se pueden configurar y administrar desde una interfaz de línea de comando (CLI). Contienen una unidad de procesamiento central (CPU), memoria de acceso aleatorio (RAM), y un sistema operativo.

Una vez que se conecta el cable de energía eléctrica, el switch inicia una serie de pruebas denominadas Autocomprobación de Encendido (POST). El POST se ejecuta automáticamente para verificar que el switch funcione correctamente.

El LED del sistema indica el éxito o falla de la POST. Si el LED del sistema está apagado pero el switch está enchufado, entonces POST está funcionando. Si el LED del sistema está verde, entonces la POST fue exitosa.

Si el LED del sistema está ámbar, entonces la POST falló. La falla de la POST se considera como un error fatal. No se puede esperar que el switch funcione de forma confiable si la POST falla.

El switch tiene 2 modos de configuración USER EXEC y PRIVILEGED EXEC. Cuando estamos en modo USER EXEC el prompt que nos muestra el switch es ">". Cuando estamos en PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#

4.17.1 MODOS DE COMANDO DE LOS SWITCH

El modo por defecto es el modo EXEC usuario. El modo EXEC usuario se reconoce por su indicador, que termina en un carácter de "mayor que" (>). Los comandos disponibles en el modo EXEC usuario se limitan a los que cambian las configuraciones de terminal, realizan pruebas básicas y muestran información del sistema.

4.17.2 COMANDO SHOW MODO USUARIO

- **show flash:** Muestra información acerca del flash: sistema de archivos.
- **show version:** Despliega la información acerca de versión del software y hardware.
- **show controllers:** proporciona información acerca de tramas descartadas, errores, colisiones etc.

4.17.3 COMANDO SHOW MODO PRIVILEGIADO

- **show vlan:** Verifica la configuración de las Vlan.
- **show interfaces:** Muestra el estado y la configuración de la interfaz.
- **show running-configuration:** Muestra el contenido del archivo de configuración actual del switch.

4.17.4 CONFIGURACION DEL NOMBRE DEL SWITCH

Se debe asignar un nombre exclusivo al switch. Esto se realiza en el modo de configuración global, mediante los siguientes comandos:

```
Switch# configure terminal
```

```
switch(config)#hostname Sw_Core
```

```
Sw_Core(config)#exit
```

4.17.5 CONFIGURACION DE CONTRASEÑAS DEL SWITCH

Se debe siempre configurar contraseñas para las líneas de terminales virtuales y para la línea de consola. Las contraseñas también se usan para controlar el acceso al modo EXEC privilegiado, a fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración.

Contraseña de la consola

```
Sw_Core #configure terminal  
Sw_Core (config)# line console 0  
Sw_Core(config-line)# password  
Sw_Core(config-line) #login  
Sw_Core(config-line) #exit
```

Contraseña de la Terminal Virtual

```
Sw_Core #configure terminal  
Sw_Core (config)# line vty 0 15  
Sw_Core(config-line)# password  
Sw_Core(config-line) #login  
Sw_Core(config-line) #exit
```

Permita la Palabra de Acceso

Sw_Core (config)# enable password

4.17.6 VLANS

Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por función laboral o departamento, sin importar la ubicación física de los usuarios. El tráfico entre las VLAN está restringido.

Los switches y puentes envían tráfico unicast, multicast y broadcast sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. Los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN.

Los routers suministran conectividad entre diferentes VLAN. Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica.

Las VLAN simplifican las tareas cuando es necesario hacer agregados, mudanzas y modificaciones en una red. Las VLAN mejoran la seguridad de la red y ayudan a controlar los broadcast de Capa 3.

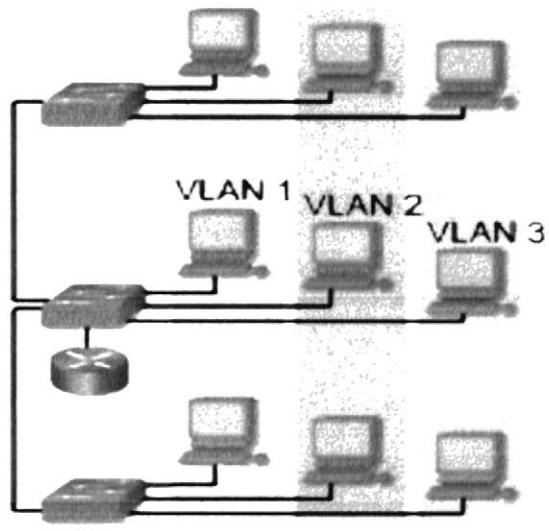


Figura 4-15 Arquitectura de las Vlan

4.17.6.1 TIPOS DE VLANS

Existen 3 tipos de vlans:

- Vlans por puerto
- Vlans por direcciones MAC
- Vlans por protocolos

4.17.6.2 VLANS POR PUERTO

El método de configuración es mas común, los puertos se asignan individualmente, en grupos, en filas o en 2 o mas switches. Se implementa a menudo donde el protocolo de control dinámico (DHCP).

Vlans por direcciones MAC

Se implementa en escasa frecuencia hoy en día la administración es compleja y es necesario introducir y configurar cada dirección de forma individual.

Vlans por protocolo

Se configuran como las direcciones MAC, pero usan una dirección lógica o IP pero ya no son comunes debido a que existe DHCP.

4.17.6.3 CONFIGURACION DE VLANS

11.- Para configurar las vlans se debe ingresar en el MODO PRIVILIGED EXEC, luego ingresar al modo de configuración de vlan con el comando "**vlan database**" después ingresar la línea de comando "**vlan <numero de vlan> name <nombre>**" por ultimo salir de la configuración con el comando "**exit**".

```
SW_CORE >enable
SW_CORE #
SW_CORE # vlan database
SW_CORE (vlan)#
SW_CORE (vlan)#vlan 20 name sistemas
SW_CORE (vlan)#exit
SW_CORE #
```

4.17.6.4 ASIGNAR PUERTOS A UNA VLAN

12.- Las vlans pueden tener uno o varios puertos asignados, para asignar un puerto a la vlan se debe ingresar en el modo de configuración global e ingresar al puerto que se desee agregar a la vlan , una vez adentro digitar el comandos "**switchport mode access**" luego digitar el comando "**switchport access vlan <numero de vlan>** " y por ultimo salir de modo de configuración global con el comando "**exit**".

```
SW_CORE >enable
SW_CORE #
```

```
SW_CORE (Config)#  
SW_CORE (Config)#interface fastethernet 0/2  
SW_CORE (config-if)#  
SW_CORE (config-if)#switchport mode access  
SW_CORE (config-if)#switchport access vlan 20  
SW_CORE (config-if)#exit  
SW_CORE #
```

4.17.6.5 ASIGNAR SWITCH DE TIPO SERVER

El rol de VTP es mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común. VTP es un protocolo de mensajería que usa tramas de enlace troncal de Capa 2 para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio. VTP también admite cambios centralizados que se comunican a todos los demás switches de la red. VTP mantiene su propia NVRAM.

13.- Para determinar un switch de tipo Server debemos estar en el MODO PRIVILEGED EXEC e ingresar al modo de configuración de vlans con el comando "**vlan database**", una vez dentro digitar la línea de comando "**vtp < Server o client>**" después digitamos el comando "**vtp domain <nombre del dominio>**" y por ultimo salimos de la configuración con el comando "**exit**".

```
SW_CORE >enable  
SW_CORE #  
SW_CORE # vlan database  
SW_CORE (vlan)#vtp Server  
SW_CORE (vlan)#vtp domain topico  
SW_CORE (vlan)#exit  
SW_CORE #
```

4.17.6.6 COMUNICACION ENTRE VLANS

14.- Por ultimo en el router principal se debe ingresar en el modo de configuración global para así ingresar a la interfaz ethernet con el comando "**interface ethernet<numero de interfaz>**", se levanta la interface con el comando "**no shutdown**" después ingresar a la sub interface ethernet con el comando "**interface ethernet<numero de interfaz numero de subinterfaz>**" una vez a dentro digitamos el protocolo de comunicación de vlans dot1q con el comando "**encapsulation dot1q <numero de vlan>**" luego la dirección ip de la vlan con su máscara con el comando "**ip address, mask**" y por ultimo salir del modo de configuración global con el comando "**exit**".

```
SW_CORE # configure terminal
SW_CORE (config)# interface Ethernet 0
SW_CORE (config-if)# no shutdown
SW_CORE config-if)# interface Ethernet 0.1
SW_CORE config-subif)# encapsulation dot1q 1
SW_CORE config-subif)# ip address 192.168.1.1 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.2
SW_CORE config-subif)# encapsulation dot1q 10
SW_CORE config-subif)# ip address 192.168.1.17 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.3
SW_CORE config-subif)# encapsulation dot1q 20
SW_CORE config-subif)# ip address 192.168.1.33 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.4
SW_CORE config-subif)# encapsulation dot1q 30
SW_CORE config-subif)# ip address 192.168.1.49 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.5
SW_CORE config-subif)# encapsulation dot1q 40
SW_CORE config-subif)# ip address 192.168.1.65 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.6
SW_CORE config-subif)# encapsulation dot1q 50
SW_CORE config-subif)# ip address 192.168.1.81 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.7
SW_CORE config-subif)# encapsulation dot1q 60
SW_CORE config-subif)# ip address 192.168.1.97 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.8
SW_CORE config-subif)# encapsulation dot1q 70
SW_CORE config-subif)# ip address 192.168.1.113 255.255.255.240
SW_CORE config-subif)# interface Ethernet0.9
SW_CORE config-subif)# encapsulation dot1q 80
SW_CORE config-subif)# ip address 192.168.1.129 255.255.255.240
SW_CORE (config-if)# exit
SW_CORE #
```

4.17.6.7 ELIMINAR VLANS

Para eliminar la información de VLAN actual, borre el archivo de la base de datos VLAN, denominado **vlan.database**, del directorio flash con el comando “**delete flash:vlan.database**”.

```
SW_CORE# delete flash:vlan.database.
```

4.17.6.8 SHOW VLANS D

Muestra todas las vlans creadas con sus respectivos puertos asignados.

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/10, Fa0/11, Fa0/12
10 Sistemas	active	Fa0/2
20 Administración	active	Fa0/3
30 Laboratorio	active	Fa0/4
40 40	active	Fa0/5
50 50	active	Fa0/6
60 60	active	Fa0/7
70 70	active	Fa0/8
80 80	active	Fa0/9
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
60	enet	100060	1500	-	-	-	-	-	0	0
70	enet	100070	1500	-	-	-	-	-	0	0
80	enet	100080	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	iecc	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

4.17.6.9 SHOW RUN

```
D#sh run
Building configuration...
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname D
enable password cisco
!
ip subnet-zero
!

interface Serial0
no ip address
no ip directed-broadcast
bandwidth 1544
shutdown
!
interface Serial1
ip address 192.168.11.10 255.255.255.252
no ip directed-broadcast
bandwidth 1544
!
interface Ethernet0
ip address 192.168.12.1 255.255.255.240
no ip directed-broadcast
bandwidth 10000
shutdown
!
router rip

version 2
network 192.168.11.0
network 192.168.12.0
!
ip classless
no ip http server
!
line con 0
login
transport input none
password cisco
line aux 0
line vty 0 4
password cisco
```

4.17.6.10 SH INTERFACE ROUTER D

```
D#sh interfaces
Serial0 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
Serial1 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
Ethernet0 is administratively down, line protocol is down
  Hardware is Lance, address is 000C.9596.5444 (bia 000C.9596.5444)
  Internet address is 192.168.12.1/28
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
```

Queueing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 1000 bits/sec, 2 packets/sec
 5 minute output rate 1000 bits/sec, 2 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 input packets with dribble condition detected
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out

D#

D#

D#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
 U - per-user static route

Gateway of last resort is not set

192.168.11.0/30 is subnetted, 2 subnets

C 192.168.11.8 is directly connected, Serial1

R 192.168.11.4 [120/1] via 192.168.11.9, 00:03:24, Serial1

192.168.10.0/28 is subnetted, 1 subnets

R 192.168.10.32 [120/1] via 192.168.11.9, 00:08:29, Serial1

4.17.6.11 SHOW IP ROUTE

D#show ip route

El comando show ip route verifica la rutas en la tabla de enrutamiento.

D#show run

- A continuación se le explicará con más detalle cada definición -

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 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, N2 - 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 inter 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

Subnetización con VLSM.

El segmento de red 192.168.14.0 posee dos subredes y dos máscaras.

192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks

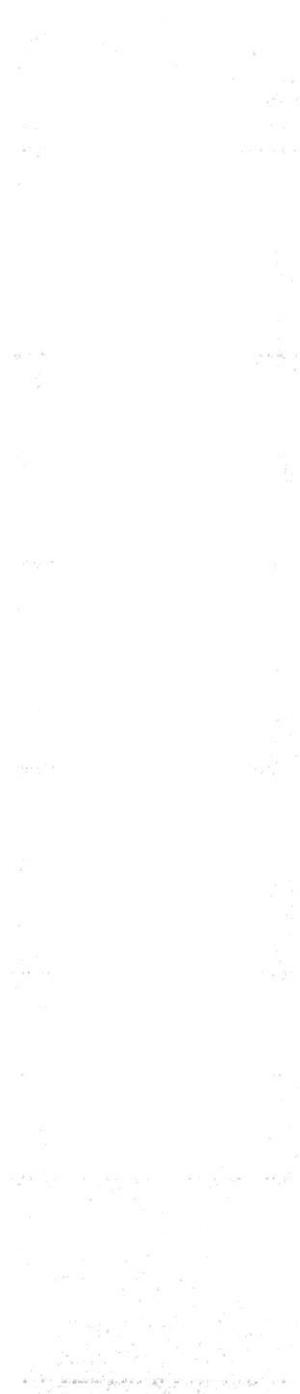
El segmento de red 192.168.14.4 está directamente conectada a un enlace serial 0.

C 192.168.14.4/30 is directly connected, Serial0

El segmento de red 192.168.14.0 y la 192.168.15.0 están configuradas con protocolos de enrutamiento RIP versión 2 saliendo por la IP 192.168.2.5 en un enlace serial 0 con actualizaciones de 5 segundos, el **120** se refiere a la distancia, **10** el numero de saltos y vía es para indicar el rombo de los paquetes.

R 192.168.14.0/24 [120/1] vía 192.168.14.6, 00:00:05, Serial0

R 192.168.15.0/24 [120/10] vía 192.168.13.6, 00:00:05, Serial0



CAPÍTULO 5

LINUX



5 INTRODUCCION A LINUX

Linux es un Unix libre, es decir, un sistema operativo, como el Windows o el MS-DOS (sin embargo, a diferencia de estos y otros sistemas operativos propietarios, ha sido desarrollado por miles de usuarios de computadores a través del mundo, y la desventaja de estos es que lo que te dan es lo que tu obtienes, dicho de otra forma no existe posibilidad de realizar modificaciones ni de saber como se realizó dicho sistema.), que fue creado inicialmente como un hobby por un estudiante joven, Linus Torvalds, en la universidad de Helsinki en Finlandia, con asistencia por un grupo de hackers a través de Internet. Linus tenía un interés en Minix, un sistema pequeño o abreviado del UNIX (desarrollado por Andy Tanenbaum); y decidido a desarrollar un sistema que excedió los estándares de Minix. Quería llevar a cabo un sistema operativo que aprovechara la arquitectura de 32 bits para multitarea y eliminar las barreras del direccionamiento de memoria.

Torvalds empezó escribiendo el núcleo del proyecto en ensamblador, y luego comenzó a añadir código en C, lo cual incrementó la velocidad de desarrollo, e hizo que empezara a tomarse en serio su idea.

Él comenzó su trabajo en 1991 cuando él realizó la versión 0,02, la cual no la dió a conocer porque ni siquiera tenía drivers de disquete, además de llevar un sistema de almacenamiento de archivos muy defectuoso.

Trabajó constantemente hasta 1994 en que la versión 1,0 del núcleo (KERNEL) de Linux se concretó. La versión completamente equipada actual es 2,2 (versión concluida el 25 de enero de 1999), y el desarrollo continúa.

5.1 QUE ES LINUX

Linux es un Sistema Operativo (conocida como núcleo o kernel) se distribuye a través de la Licencia Pública General GNU, lo que básicamente significa que puede ser copiado libremente, cambiado y distribuido, pero no es posible imponer restricciones adicionales a los productos obtenidos y, adicionalmente, se debe dejar el código fuente disponible, de la misma forma que está disponible el código de Linux.

5.1.1 CARACTERISTICAS DE LINUX

En líneas generales podemos decir que se dispone de varios tipos de sistema de archivos para poder acceder a archivos en otras plataformas. Incluye un entorno gráfico X Windows (Interfase gráfica standard para máquinas UNIX), que nada tiene que envidiar a los modernos y caros entornos comerciales. Está orientado al trabajo en red, con todo tipo de facilidades como correo electrónico por ejemplo. Posee cada vez más software de libre distribución, que desarrollan miles de personas a lo largo y ancho del planeta. Linux es ya el sistema operativo preferido por la mayoría de los informáticos.

Un ejemplo de la popularidad que ha alcanzado es sistema y la confianza que se puede depositar en él es que incluso la NASA ha encomendado misiones espaciales de control de experimentos a la seguridad y la eficacia de Linux.

5.1.2 COMANDOS BASICOS DE LINUX

Comandos Para Manipular Directorios y Archivos			
Comando	Sintaxis	Parámetros /opciones	Descripción
cd	cd <directorio>		Cambia de directorio activo
ls	ls <archivo1>...<archivoN>	-l -F -a	Muestra información sobre los archivos
cp	cp <archivo1>...<archivoN> <destino>		Copia archivo(s) en otro archivo o directorio
mv	mv <archivo1>...<archivoN> <destino>		Mueve archivo(s) en otro archivo o directorio
rm	rm <archivo1>...<archivoN>	-l -f -r	Borra archivo(s)
mkdir	mkdir <directorio1>...<directorioN>		Crea directorios
rmdir	rmdir <archivo1>...<archivoN>	-p	Borra borra directorios vacíos
man	man <comando>	-a	Muestra la página del manual del comando o recurso
more	more <archivo1>...<archivoN>		Muestra el contenido de los archivos indicados por pantallas
cat	cat <archivo1>...<archivoN>		Concatena archivos o muestra el contenido completo sin pausa
echo	echo <arg1> <arg2>...<argN>		Envía al terminal los argumentos pasados
grep	grep <patrón> <archivo1>...<archivoN>	e , i	Muestra todas las líneas de un fichero que coinciden con un patrón
pwd	Pwd		Muestra la ubicación actual del directorio (ruta)
clear	Clear		Limpiar pantalla
Comandos Para Reiniciar y Salir del Sistema			
Apagar Sistema	Shutdown Poweroff		
Salir De Una Consola Virtual	Exit Logout		
Reiniciar el Modo Grafico	Startx		
Reiniciar	Reboot		

Tabla 5-1 Comandos Básicos de Linux

5.2 DIRECTORIOS

Directorio Bin

Tiene programas ejecutables conocidos como binarios, y también shells.

Directorio Etc

Contiene muchos archivos de configuración del sistema, aquí se encuentra el archivo de contraseñas, el passwd.

Directorio Lib

Contiene las bibliotecas compartidas que utiliza los programas al ejecutarse permite la reutilización de código. El tamaño de los programas se reduce durante la ejecución.

Directorio Dev

Contiene archivos para control de dispositivos permiten acceder a los distintos tipos de hardware que hay en el sistema. Por ejemplo, /dev/mouse sirve para leer las entradas del ratón

Directorio Tmp

Se utiliza para almacenar los archivos temporales que crean los programas al ejecutarse. Si se tiene un programa que crea muchos archivos temporales muy grandes, es aconsejable que se monte este directorio como un sistema de archivos separado.

Directorio Home

Es el directorio base para los directorios iniciales de los usuarios.

Directorio Var

Contiene archivos que tienden a cambiar de tamaño con el tiempo, el directorio /var/spool y sus subdirectorios se utilizan para almacenar datos temporales, como mensajes y noticias.

Directorio Usr

Este directorio contiene varios subdirectorios que contienen paquetes de software que se instalan.

/usr/bin

- programas ejecutables del sistema Linux instalados

/usr/etc

- Contiene archivos misceláneos de configuración del sistema

/usr/man

- Contiene las diversas páginas de información para el comando man

5.3 INSTALACION DE LINUX FEDORA

5.3.1 REQUERIMIENTOS

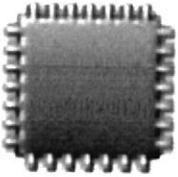
Para poder realizar la instalación vamos a requerir lo siguiente:

Un Computador

Los cd's de Fedora Core 3.

Partition Magic.

De seguro los puristas en software libre me criticaran por incluir un software como Partition Magic. Pero se los incluye por ser muy intuitivo y fácil para realizar particiones de disco duro sin tener mayores complicaciones.



CPU:

Como mínimo un procesador de tipo pentium, aunque Fedora Core 3 esta optimizado para Pentium 4 también es altamente compatible para otros procesadores como: Pentium I, II, III, Celeron y las variantes de AMD Duron, Semprom, Athlon. Recomendado para modo gráfico procesador de 400 Mhz. o superior.



MEMORIA:

Como mínimo 128 Mb, pero se recomienda 256 Mb de memoria ram.



ESPACIO EN DISCO DURO:

Se recomienda para el tipo de instalación que realizaremos "Escritorio Personal" tener como espacio libre en disco duro 2,7 Gb. Recuerde que para instalar Fedora se requiere además espacio para el sistema Swap, aproximadamente el doble de espacio de la memoria ram.



OTROS DISPOCITIVOS:

Fedora Core 3 reconoce la gran mayoría d e lectores de cd rom, grabadores de cd rom, DVD, Pendrive, etc.

5.3.2 LICENCIAS

Para obtener los cd's de Fedora Core puede hacerlos de distintas manera. Recuerde que Fedora Core como la gran mayoría de las distintas distribuciones de GNU/Linux son software libre y que posee licencia GPL:

- No se puede limitar el numero de usuarios, copias y tiempo de uso.
- No se puede cobrar por usar el programa (si por distribuirlos).
- No se puede impedir que otros vendan o distribuyan.
- Tiene que dar el código del programa en forma pública.
- Puede modificar el programa, copiar parte del código pero el resultado debe respetar las normas de licencias GPL.

En conclusión UD puede: Copiar cuantas veces id desee, instalar en cuantos equipos pueda, vender (cobrar por distribuir), regalar, modificar.

5.3.3 OBTENER CD'S Y DVD DE FC

Para obtener los cd's de Fedora Core puede hacerlos de distintas manera.

- Generalmente vienen en revistas especializadas en el tema y que generalmente las encuentra en los kioscos.
- Un amigo que posea los cd's y la buena voluntad para prestárselos
- En sitios de venta por Internet como Mercadolibre o Derremate.
- O descargar Directamente desde Internet (requerirá de una buena conexión y tiempo).

<http://www.linuxiso.org>

<http://fedora.redhat.com/download/>

Los archivos que se descargan son de la extensión "iso" que son imágenes de cd y que puede grabar utilizando cualquier programa de grabación por ejemplo: nero, easy cd creator, etc.

5.4 CREANDO LAS PARTICIONES

Las particiones en un disco duro son grupos sectores del disco duro, en el cual se engaña (por decirlo de cierta forma) al sistema operativo para que crea que existen varios de dispositivos de almacenamiento, dado que en realidad solo existe uno. Esto se utiliza no solo para instalar distintos sistemas operativos sino también para hacer respaldos de datos. Para poder instalar Fedora core o cualquier distribución de GNU/Linux, se requiere crear particiones.

Las particiones que se requiere realizar son como mínimo dos: una el la cual se alojara nuestro sistemas de archivos (/), y la partición de intercambio SWAP, que generalmente es del doble de tamaño de la capacidad de memoria ram.

El programa para realizar esta operación es el Partition Magic, el cual si bien es pagado es muy intuitivo y fácil de manejar UD puede descargar la versión de evaluación en:

- <ftp://download.axelero.hu/pub/seged/rendszer/enpm800retaildemo.zip>
- <http://www.softonic.com/>
- O también en Google.com otros programas que desee revisar:
- <http://www.partitionmanager.com/demo.htm>
- <http://www.7tools.com>
- <http://www.ranish.com/>

5.4.1 DEFRAGMENTAR NUESTRO DISCO

Es importante antes de particionar nuestro disco duro, realizar una defragmentación de este para ordenar la distribución física de los datos. Para realizar esto en Windows vaya a Mi PC luego con botón derecho del mouse debe seleccionar propiedades (imagen 1) después seleccionarla pestaña Herramientas y presione sobre defragmentar, aparecerá como en la imagen 2. Y espere que termine el proceso esto puede llevar varios minutos pero es lo mas recomendable.

Con el programa Partition Magic aparecerá lo siguiente:

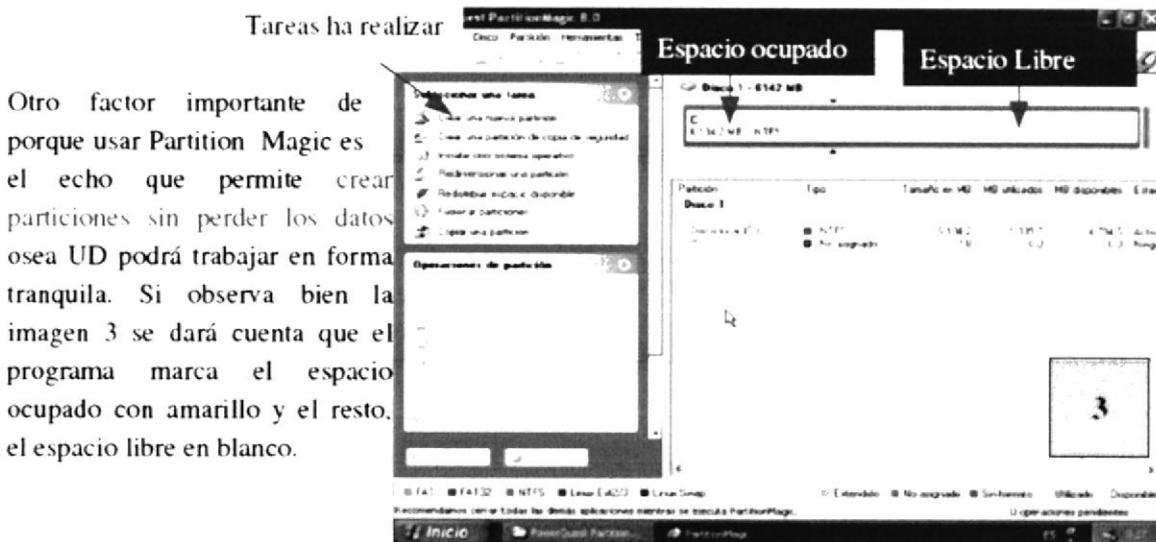


Figura 5-1 Formateando el Disco Duro desde Partición Magic

El siguiente paso es redimensionar particiones (imagen 4) para eso seleccione del menú de tareas esta opción o también haciendo clic con el botón derecho del mouse sobre la barra que indica el estado de nuestro disco duro en Partition Magic.

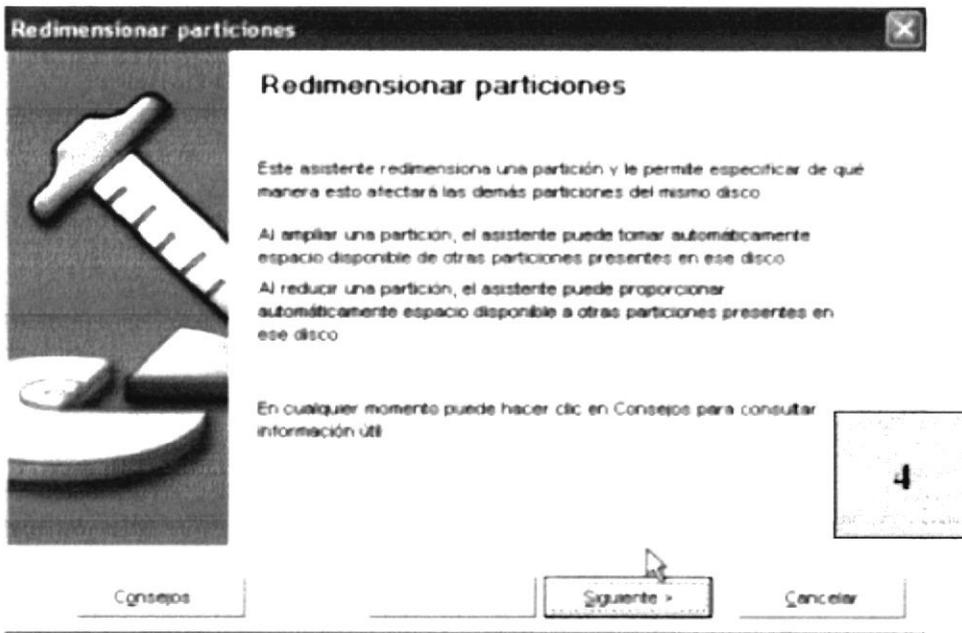


Figura 5-2 Clic en Aceptar para empezar a redimensionar el Disco Duro

Luego haga clic en el botón siguiente y aparecerá el siguiente cuadro (imagen 5), en nuestro caso como solo poseemos solo una partición elegimos el disco “C”, nótese que indica claramente el espacio utilizado y el libre que es en este ultimo donde haremos nuestra partición

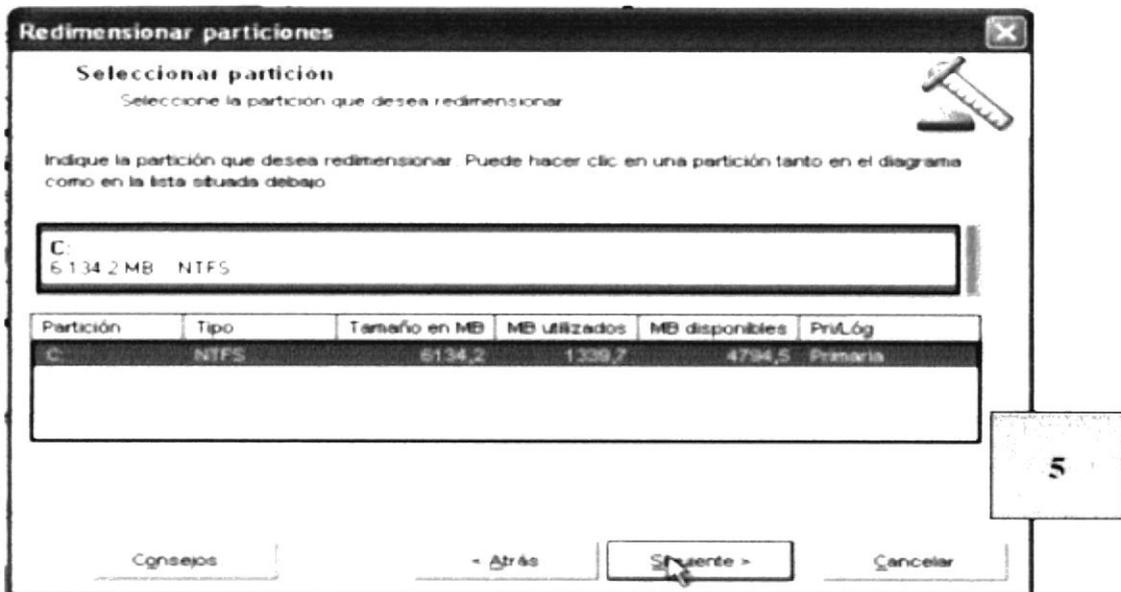


Figura 5-3 Seleccionar la partición que se desea redimensionar

Luego de hacer clic en el botón siguiente aparecerá esta parte Figura 6 aquí se debe seleccionar el tamaño de la partición que primeramente se crea y que pertenece a la partición que contendrá nuestro sistema windows, nótese que en este caso marca como tamaño actual 6134Mb y como tamaño mínimo 1474Mb que corresponde a los a nuestros datos, y como máximo los mismo 6134Mb, en este caso redimensionamos esta partición seleccionando 3000Mb.

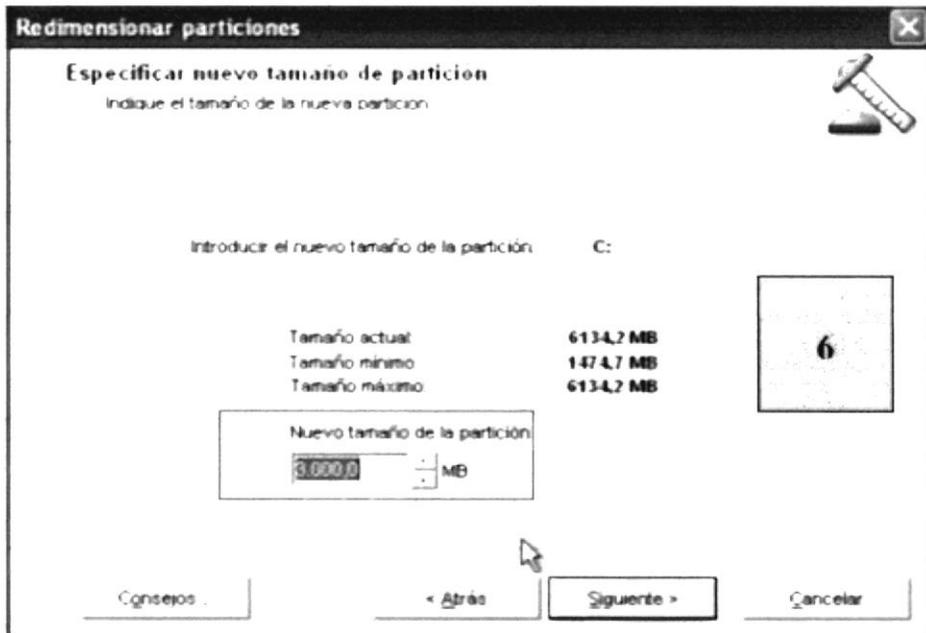


Figura 5-4 Indicamos el tamaño de la nueva partición

Si se observa en la figura 6 nos muestra como quedará ahora nuestra partición y también el espacio en color gris que esta no asignado y en la cual crearemos nuestras particiones de Linux. Luego solo hacemos clic en el boton terminar.



Figura 5-5 Clic en Aceptar para efectuar los cambios

Luego sobre el espacio en gris “No asignado” hacer clic con el botón derecho del mouse, seleccionar la opción “*crear partition*” y aparecerá el siguiente dialogo imagen 7, aquí hay varias cosas importantes como:

- Crear como seleccionar “partición primaria”
- Tipo de partición seleccionar “Linux Ext3”
- Tamaño colocar el espacio libre que UD dispone recuerde que debe ser mayor a 2,7 para “equipo de escritorio” en nuestro caso elegimos el resto disponible.

Luego de aceptar debería aparecer partition magic de esta forma (figura 9) ambas particiones definidas, pero aun nos falta una que es la partición swap de intercambio. Por lo tanto el paso a seguir es el siguiente: repetir el procedimiento de “redimensionar partición” como en la figura 4 o simplemente sobre la partición de linux hacer clic con el botón derecho y seleccionar “redimensionar/desplazar partición” como muestra la figura 9

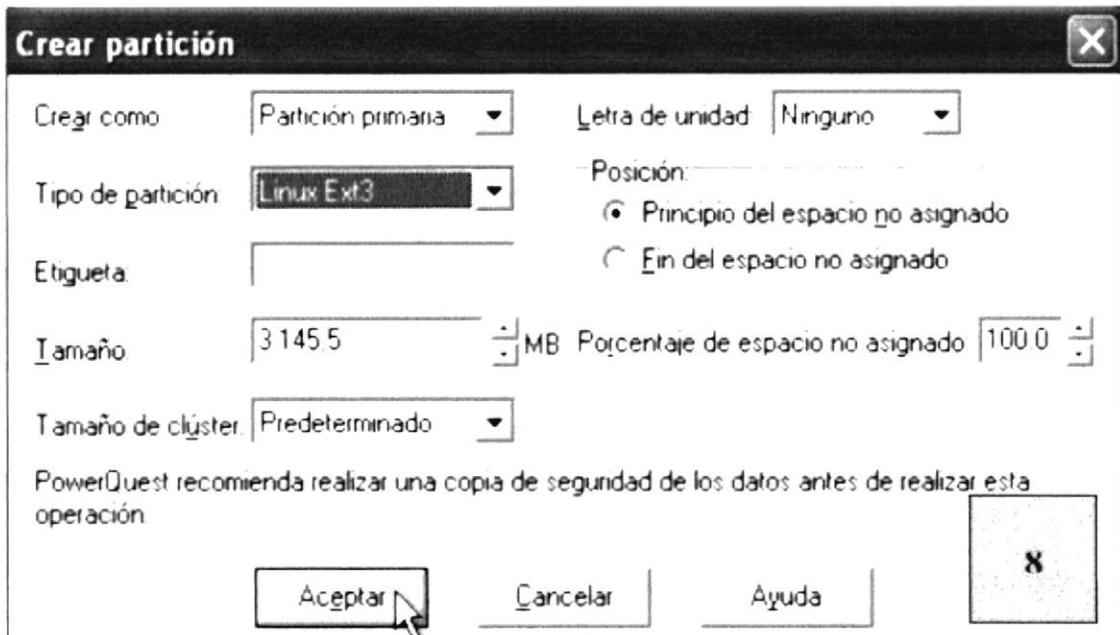


Figura 5-6 Creación de la Partición

Sobre el espacio en gris que corresponde a nuestra nueva partición swap hacer clic con el botón derecho del mouse y seleccionar la opción crear partición fíjense bien en la figura 10, en este caso:

- Partición como: elegir partición lógica.
- Tipo de Partición: elegir Linux Swap.
- Tamaño: elegir en este caso 250Mb recuerde que tiene que ser el doble de tamaño de la memoria RAM.

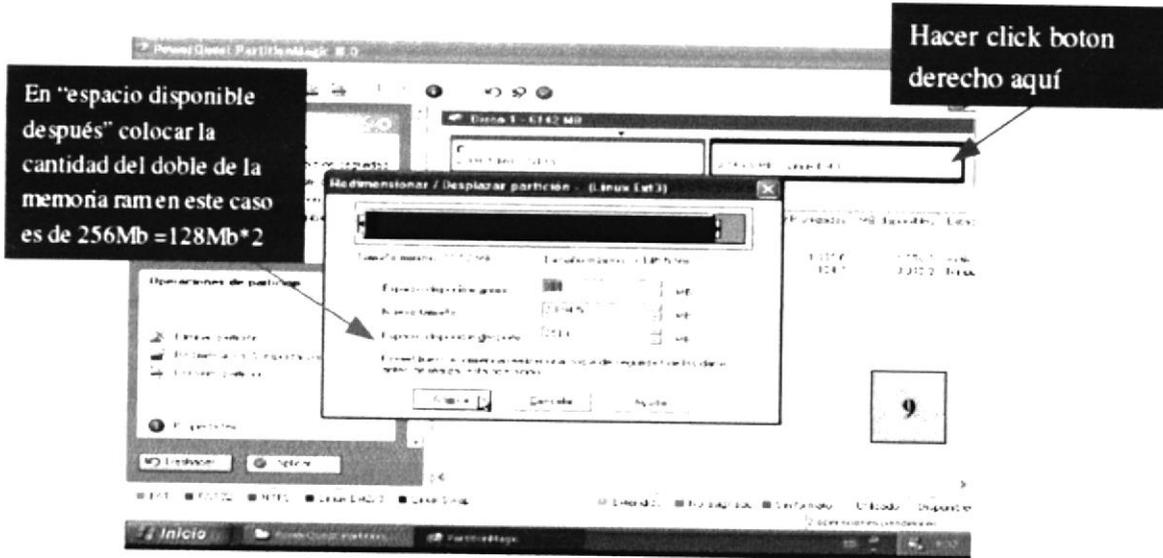


Figura 5-7 Escogemos el tipo de Partición

Terminado todo debería quedar como muestra la figura 11, ahora solo queda hacer clic en el botón aplicar y listo nos pedirá reiniciar para que los cambios surjan efecto. Al momento de reiniciar el equipo aplicara los cambios deje que su computador haga el trabajo al momento de reiniciar y estaríamos listos para instalar Fedora Core. No solamente puede crear particiones para instalar sistemas operativos sino también como seguridad al hacer respaldo de sus datos.

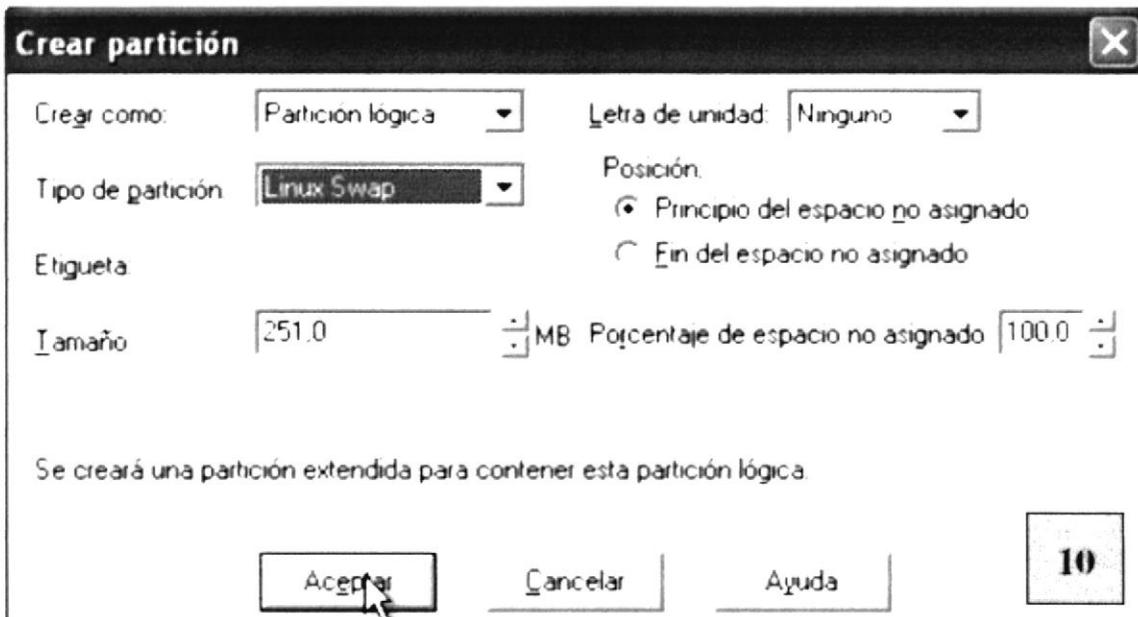


Figura 5-8 Clic en Aceptar para empezar la configuración de la partición

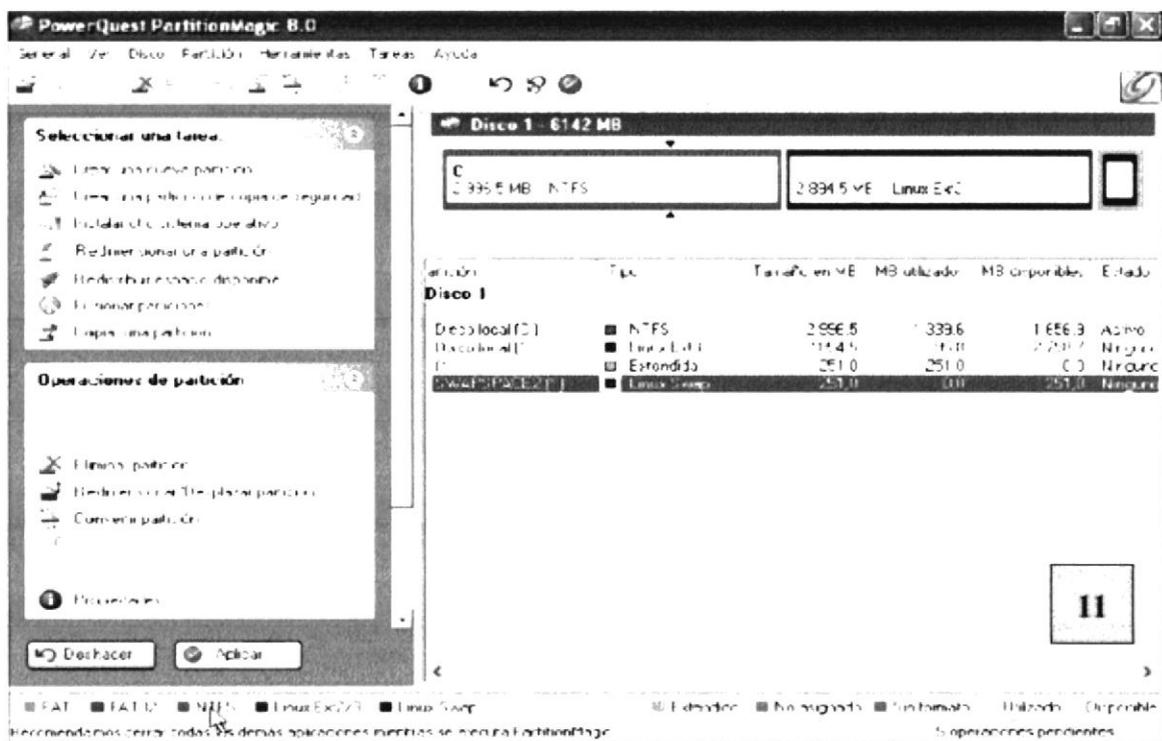


Figura 5-9 Así es como debería quedar la pantalla después de las configuraciones realizadas

5.5 INSTALANDO FEDORA CORE.

Para instalar Fedora Core debe iniciar el equipo por medio del cd rom. Actualmente la gran mayoría de los equipos tiene como primer arranque al cd rom.

En caso que no fuese así entre a la bios (es recomendable que esta operación lo realice con alguien con mayor conocimiento) para entrar a la bios generalmente es presionando la tecla supr en el primer momento del inicio, en alguna placas debe apretar F2 busque en la bios donde diga Boot sequence y elija el cd rom como primer dispositivo e arranque. Lea cuidadosamente y para guardar los cambios presione la tecla F10.

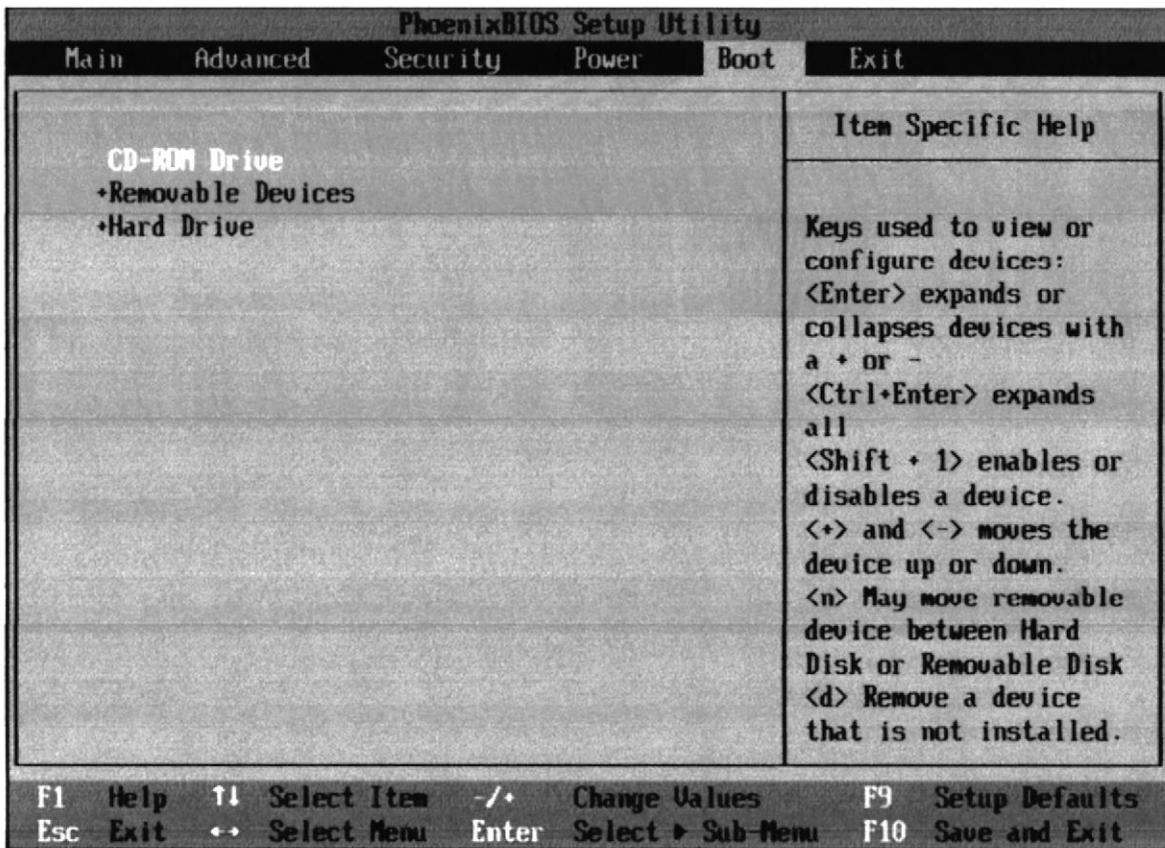


Figura 5-10 En el setup configuramos para que el computador encienda desde el Cd

Antes de reiniciar su Pc coloque el primer cd de instalación "Fedora Core cd1". Fedora Core 3 consta de 4 cd's mas el cd de rescate. Al arrancar el equipo deberá aparecer esta ventana, solo presione la tecla Enter.

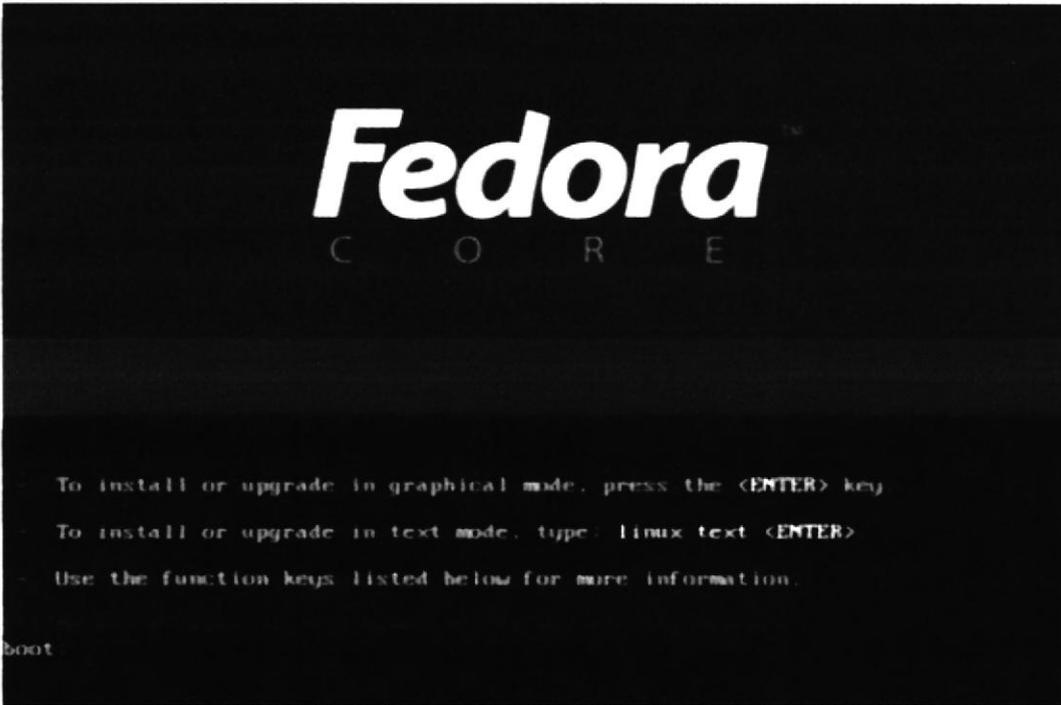


Figura 5-11 Pantalla de inicio de Fedora

Aparecerá este dialogo en el cual se le preguntara si desea realizar un test a los cd's de instalación Esto es opcional si desea realizar el test presione OK en caso contrario presione SKIP.



Figura 5-12 Opción para hacer un test al Cd

Seguramente el programa de instalación reconocerá el hardware de su equipo como el monitor, mouse, teclado, tarjeta de video, tarjeta de sonido, etc. si todo sale bien aparecerá esta pantalla solo debe hacer clic en el boton siguiente. (Next).

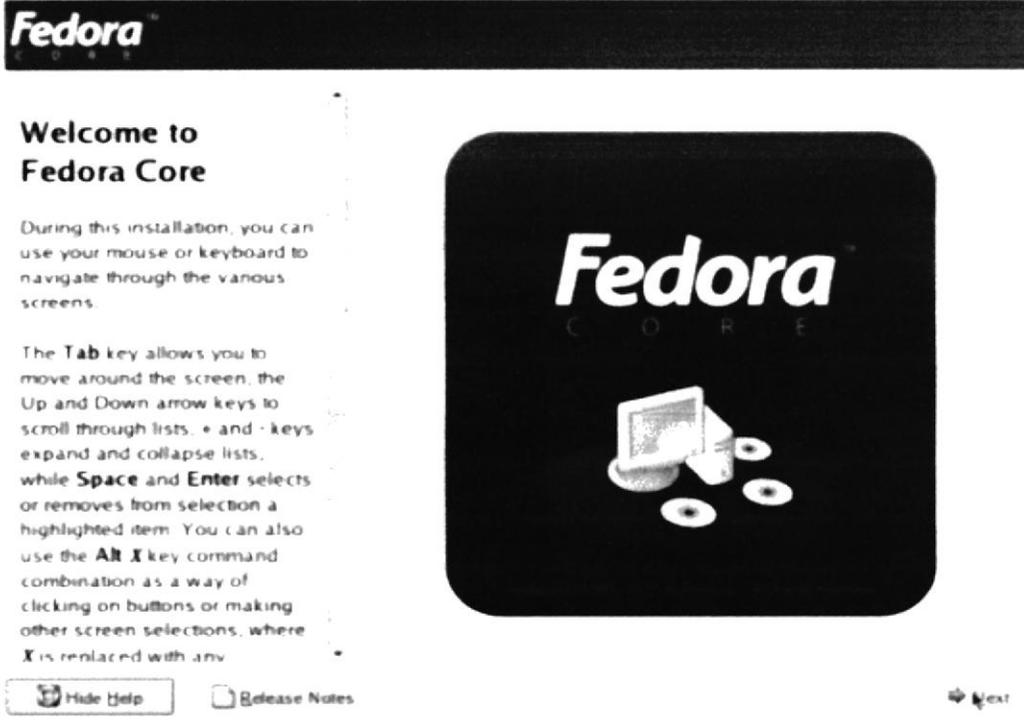


Figura 5-13 Pantalla de Bienvenida a la Instalación de Fedora

No hay mucho que decir solo seleccione el idioma en nuestro caso Español.



Figura 5-14 Selección del Lenguaje de la Instalación

Prácticamente igual que en el caso anterior debe seleccionar la opción Español

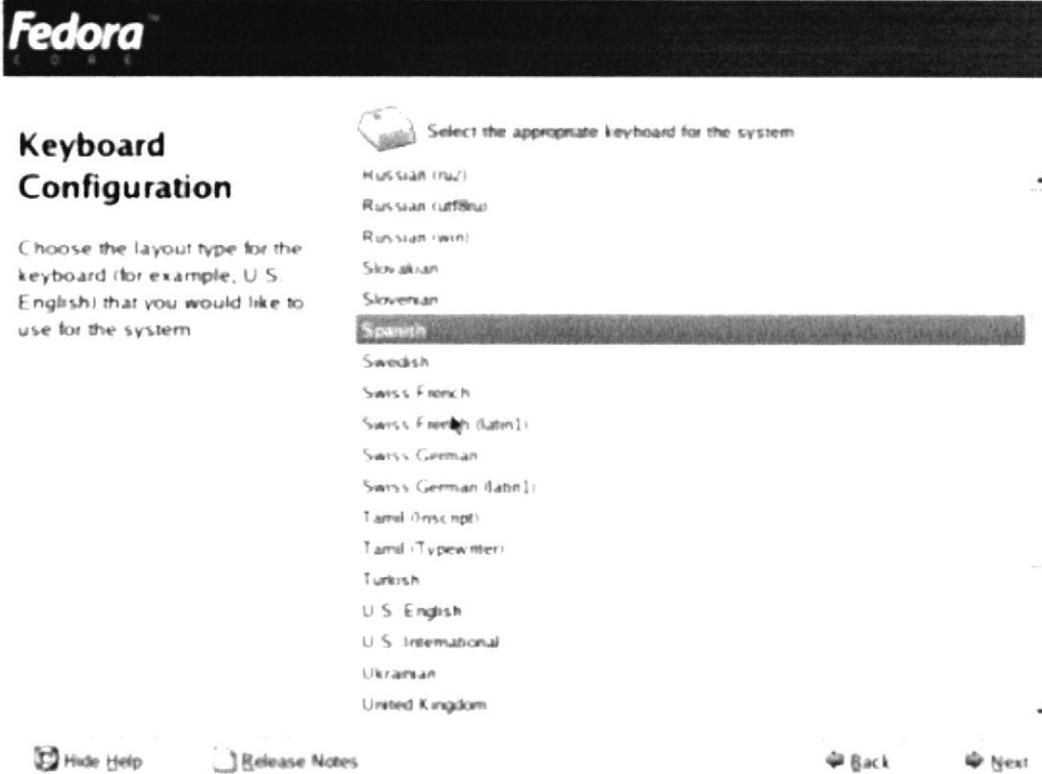


Figura 5-15 Selección del Idioma del Teclado

Luego aparecerá esta pantalla la cual le preguntará el tipo de instalación que desea realizar, el cual en nuestro caso recomiendo “Escritorio Personal”.

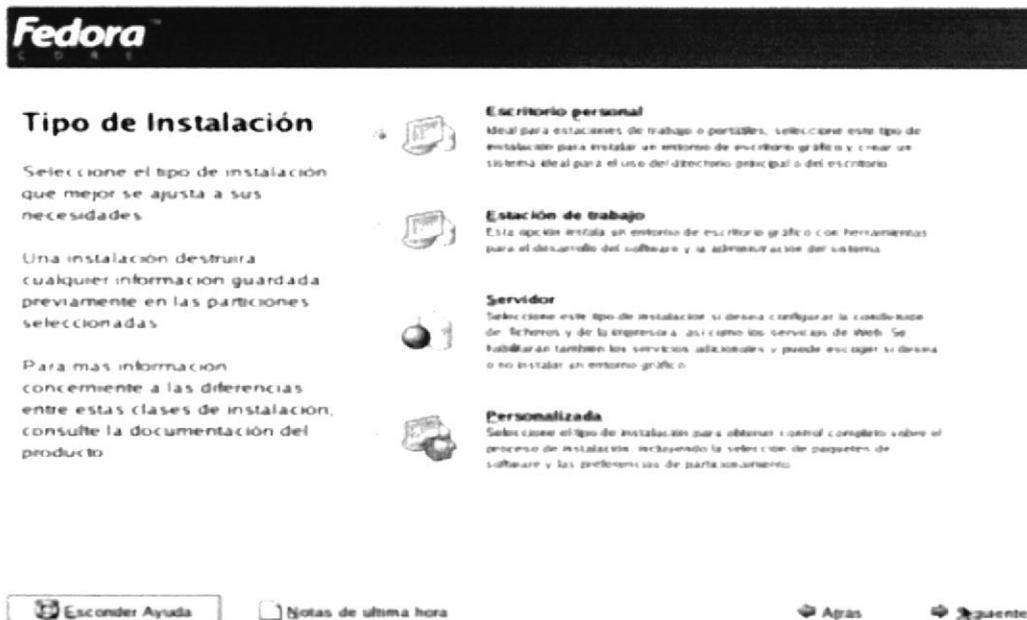


Figura 5-16 Selección del tipo de instalación

Ahora hay que indicar al programa de instalación cuales son las particiones en la cual se va instalar Fedora. En este paso debemos seleccionar *particionamiento manual con Disk Druid* y presionar siguiente.

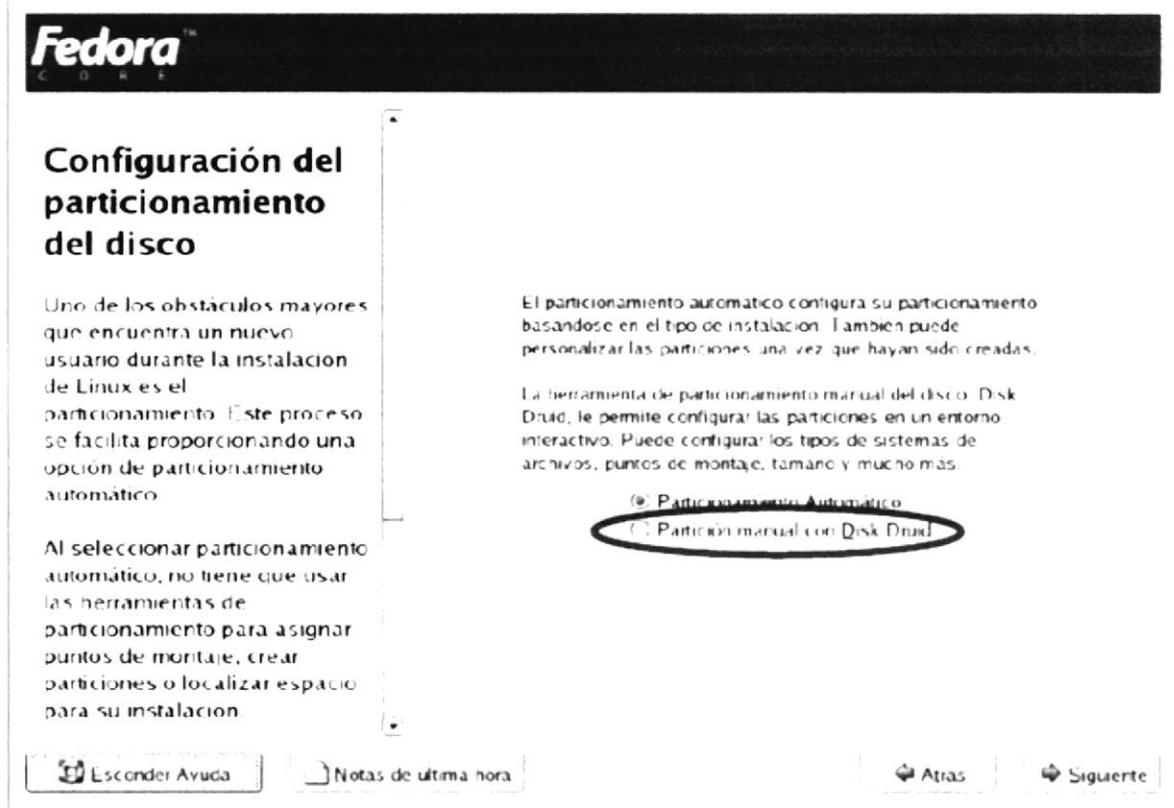


Figura 5-17 Selección del particionamiento del disco

Nótese que aparece una venta muy similar a Partition Magic. En la cual la partición llamada hda1 corresponde a la partición en la que se encuentra

Windows, Aparece hda2 y esta es la partición donde instalaremos el directorio raíz de Fedora Core y al final hda5 que corresponde a la partición de archivos de intercambio Swap.

Para mas información sobre la nomenclatura de discos y particiones en Linux ver aquí

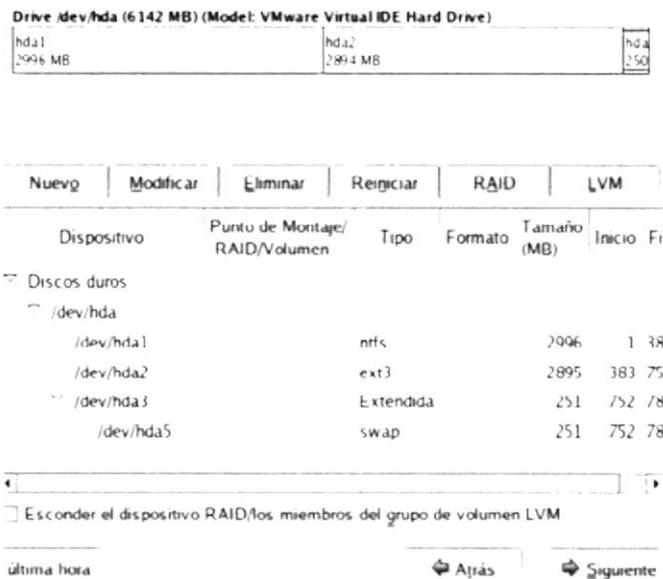


Figura 5-18 Particionamiento del Disco Duro

Seleccione la partición hda2 y hacemos clic en el botón modificar y aparecerá esta pantalla emergente. Donde aparece Punto de montaje seleccionar disco raíz osea (/) y después en formatear como elegir ext3 y aceptar.

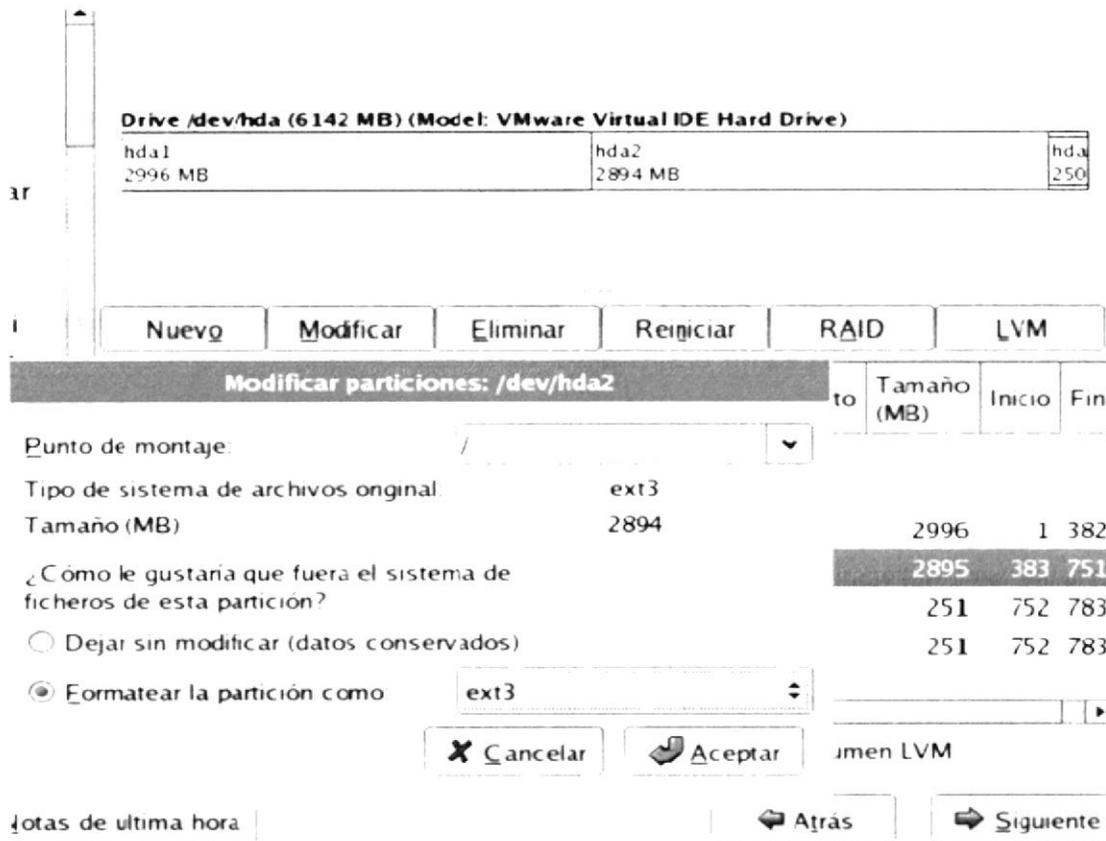


Figura 5-19 Selección del punto de montaje raíz (/)

Luego debería ver esto y ver que esta bien el punto de montaje ahora hacer clic en siguiente. No es necesario hacer el procedimiento para la partición swap debido a que se realizo cuando creamos la partición con partition magic.

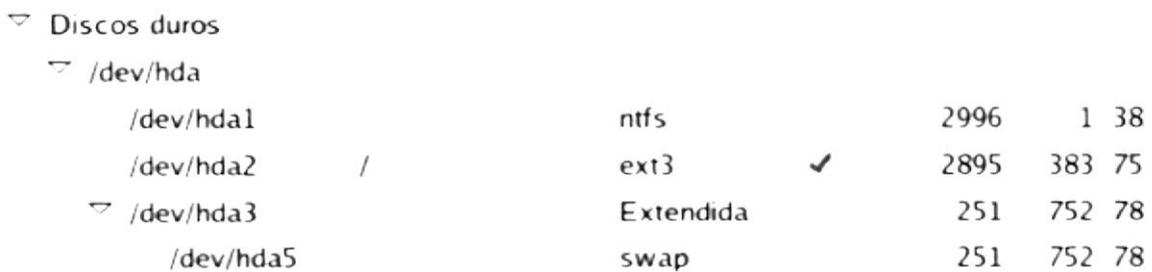


Figura 5-20 Muestra las particiones existentes

Aparecerá el siguiente cuadro en la cual nos avisará la (s) particiones a formatear si esta en lo correcto haga clic en el botón Formateo.



Figura 5-21 Aviso de Formato

La siguiente figura le preguntará sobre la instalación del gestor de arranque, este programa que se instala en el MBR sirve para seleccionar el sistema operativo que UD desee iniciar, es fundamental que sea instalado, en FC3 reconocerá el sistema Windows instalado y que lo nombra como “other” UD puede modificar el nombre “Etiqueta” presionando el botón Modificar, además de seleccionarlo por defecto.

IMPORTANTE:

No modifique la opción **Dispositivo**, si lo hace es posible que no podrá acceder a su sistema Windows

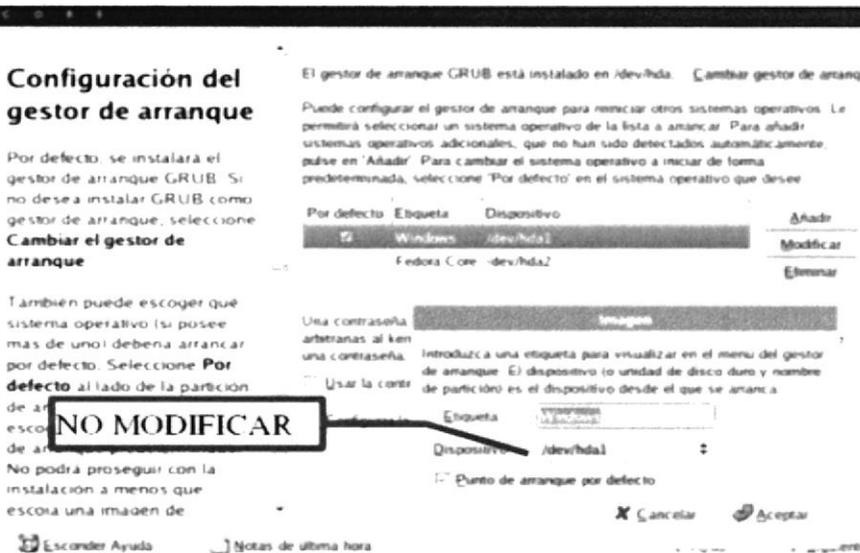


Figura 5-22 Ventana de Configuración del arranque

La siguiente figura corresponde a la instalación del Firewall si posee Internet es recomendable que lo habilite.



Figura 5-23 Configuración del Firewall (Cortafuegos)

Ahora debe seleccionar su zona horaria solo debe guiarse por la ubicación de los puntos amarillos.

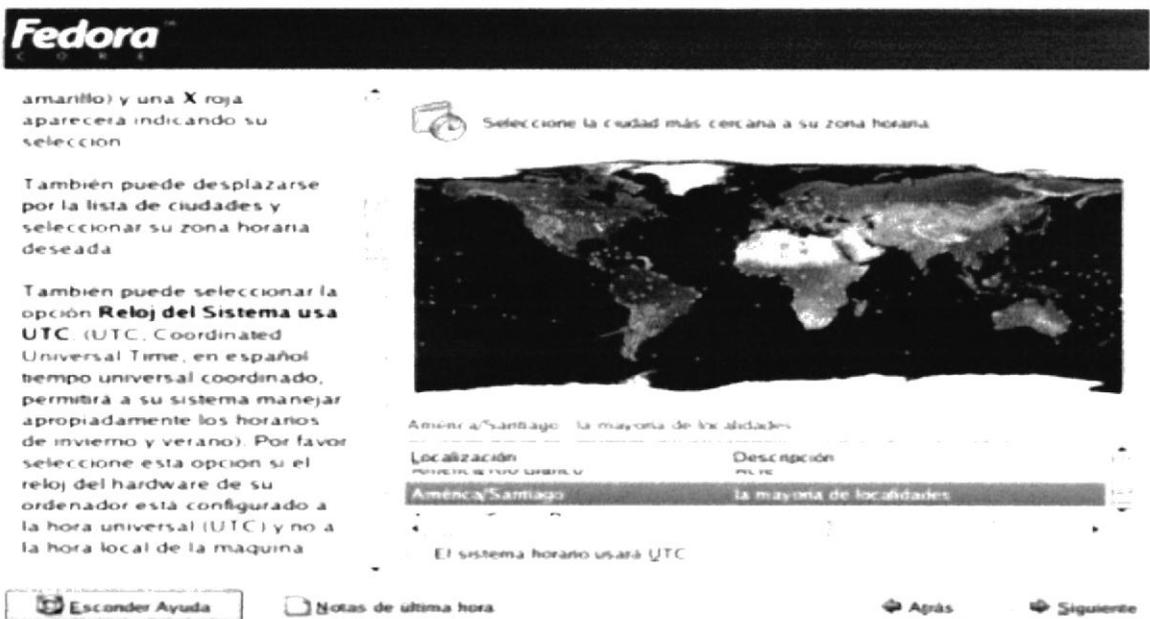


Figura 5-24 Selección del país al cual se va a configurar

Esta parte es muy importante, a diferencia de Windows XP en Linux existe un solo “administrador de sistema” el súper usuario llamado “ROOT”. Este usuario posee todos los privilegios sobre el sistema, por lo tanto es fundamental que recuerde la contraseña que va a instalar. Si olvida esta contraseña no podrá a futuro hacer alguna modificación al sistema.



Figura 5-25 Ingreso de la contraseña

Y ya estaría listo para instalar FC3 solo falta que verifique los paquetes que desea instalar, En este caso recomiendo “instalar paquetes de software por defecto”

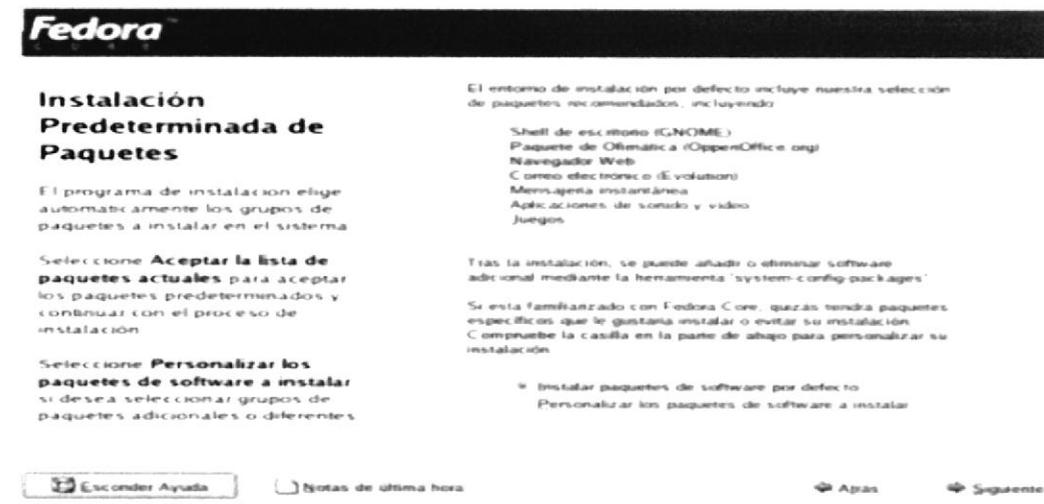


Figura 5-26 Instalación de paquetes

Verifique que posee los cd's requeridos para la instalación, si posee el DVD esto no será necesario. Solo en este tipo de instalación son requeridos estos cd's si ud agrega algún otro paquete de software es muy probable que a esta lista se agregue el cd #3. haga clic

en continuar y empezara el proceso de instalación la duración dependerá de la cantidad de paquetes a instalar como también del hardware que posea su PC.

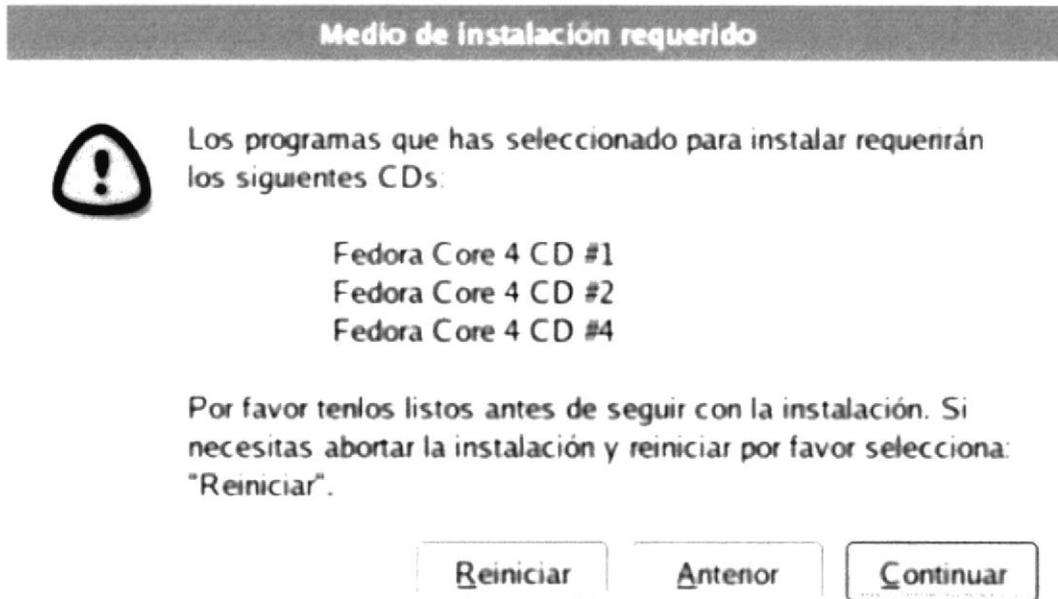


Figura 5-27 Pantalla en la que indica cuales Cd's se van a utilizar

Terminada la instalación de los archivos aparecerá este dialogo, debe quitar el cd de instalación de su lector de cd rom y reiniciar.

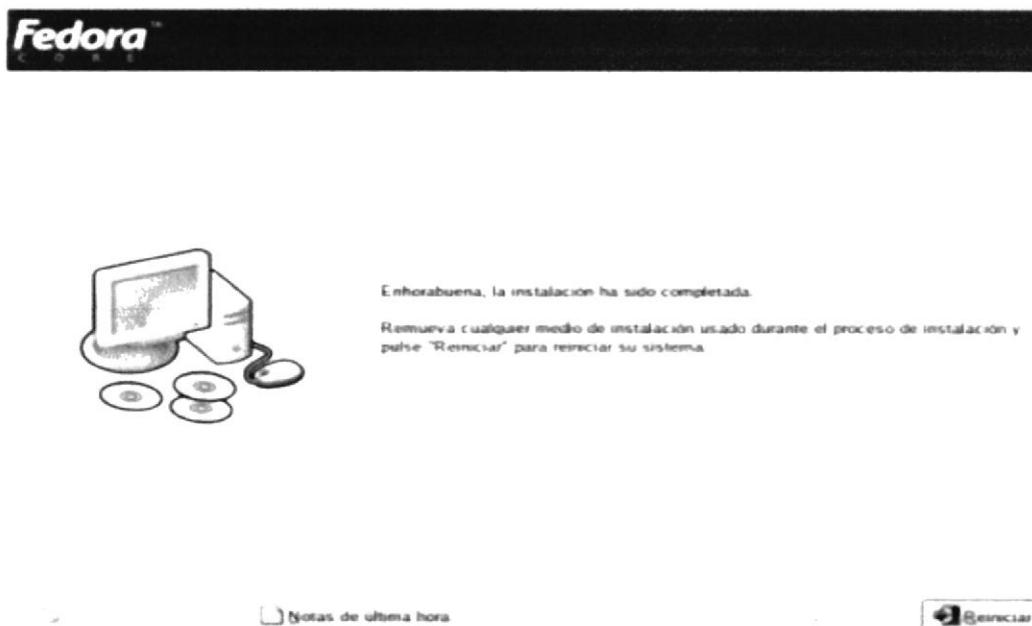


Figura 5-28 Pantalla en la que indica que la instalación fue exitosa

Al reiniciar aparecerá un conteo regresivo de 5 segundos, en ese tiempo UD debe apretar cualquier tecla, para acceder a este menú sino de lo contrario iniciara automáticamente su sistema Windows. Este es el gestor de arranque llamado GNU/Grub debe seleccionar Fedora Core tal como muestra la figura.

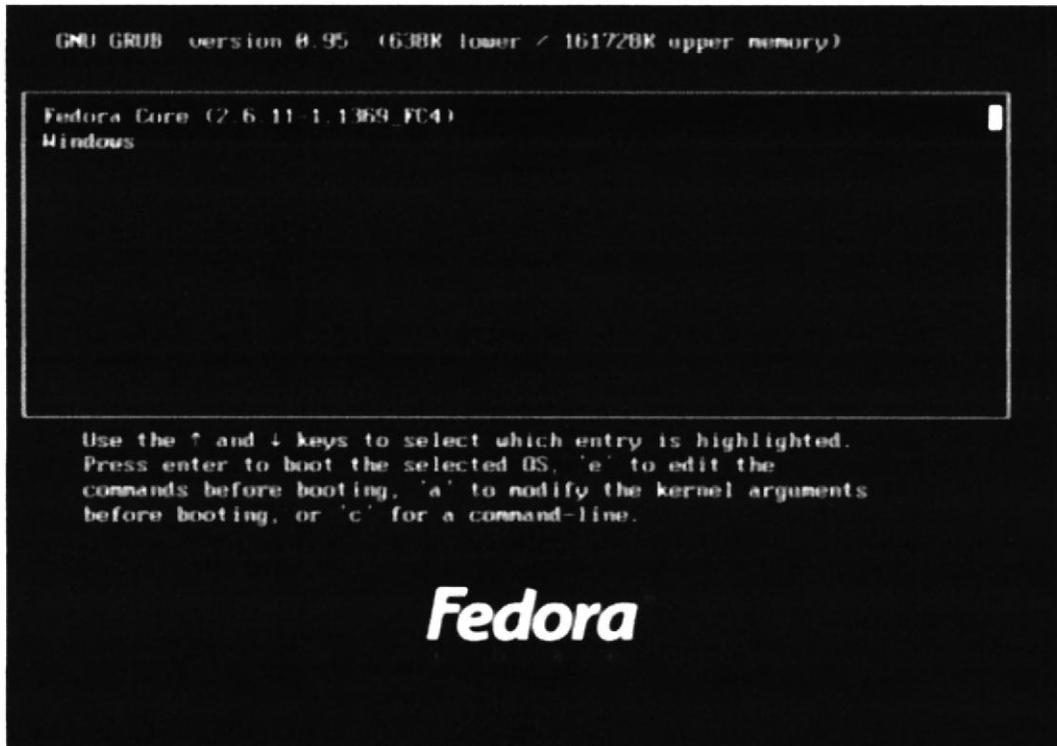


Figura 5-29 Pantalla de inicio en la que permite seleccionar el sistema operativo de arranque

Después de algunos segundos Ud deberá llegar a esta pantalla que le dará la bienvenida a la configuración post instalación (esto solo aparece en el primer inicio). Debe seguir los pasos a continuación.



Figura 5-30 Pantalla de Bienvenida a Linux

Debe aceptar el acuerdo de Licencia, mas que nada es acerca de la licencia GPL. Dependiendo de lugar de locación que UD seleccionó con anterioridad aparecerá este dialogo donde debe configura la hora y fecha.

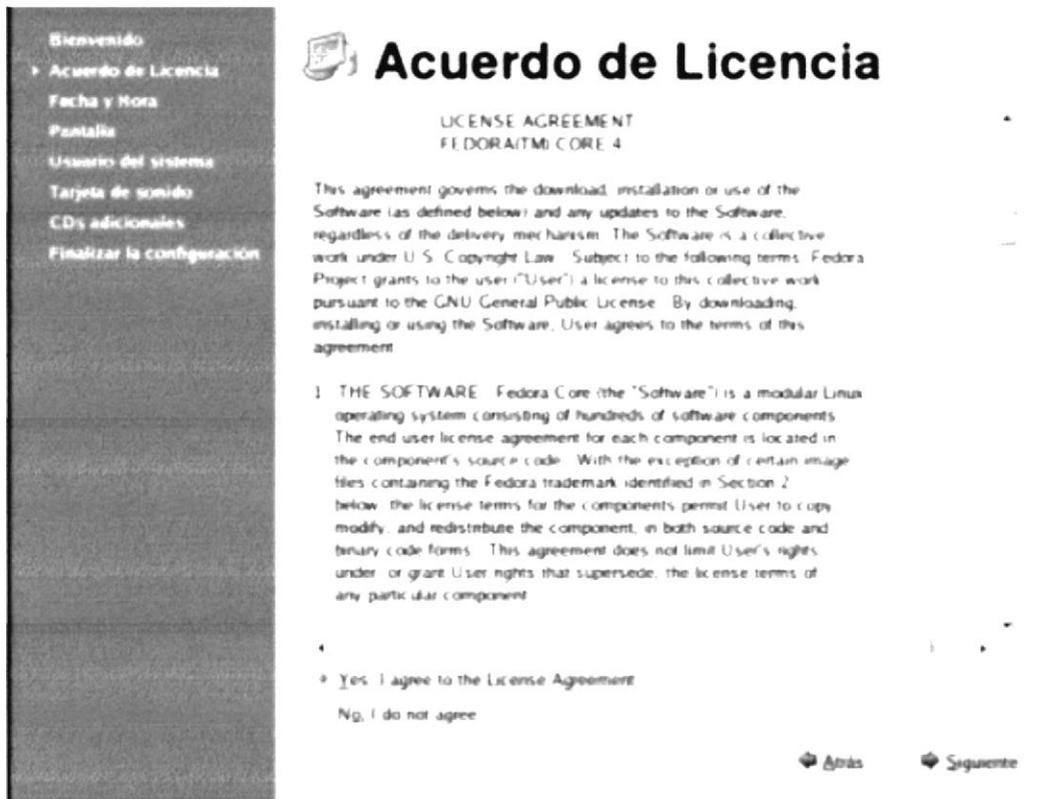


Figura 5-31 Pantalla de Acuerdo de Licencia

La configuración del monitor y resolución usted aquí debe especificar la resolución en este caso es de 800x600 pero también puede elegir valores mayores.

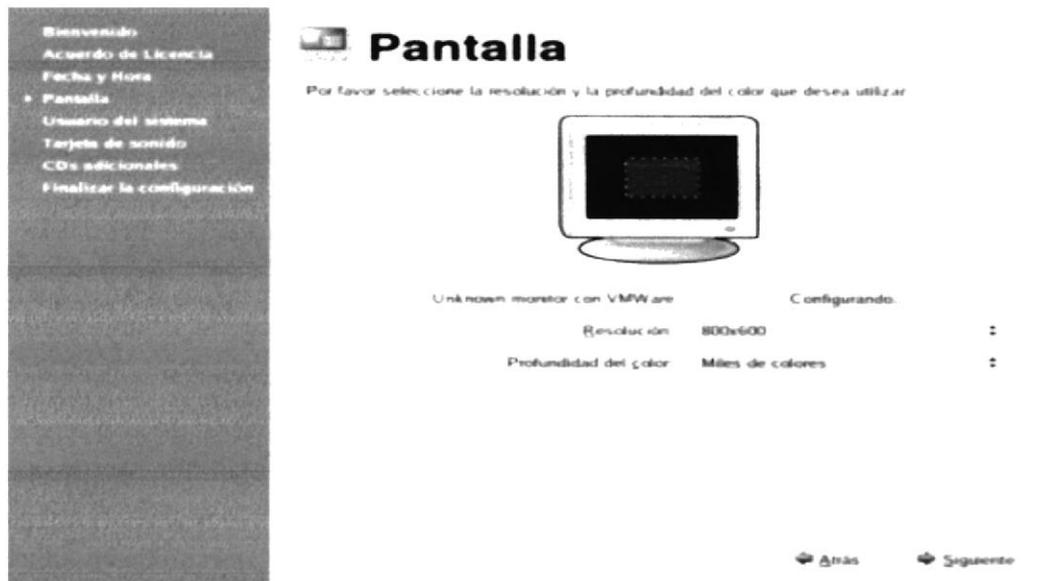


Figura 5-32 Ventana de Configuración de la resolución de la pantalla

Aquí debe colocar el usuario por el cual UD tendrá acceso al PC es algo muy parecido que en el caso de Windows XP solo que aquí no existe usuario del tipo administrador,

ya que el único con totales privilegios es el ROOT, ingrese tanto su Nombre de Usuario y Contraseña.

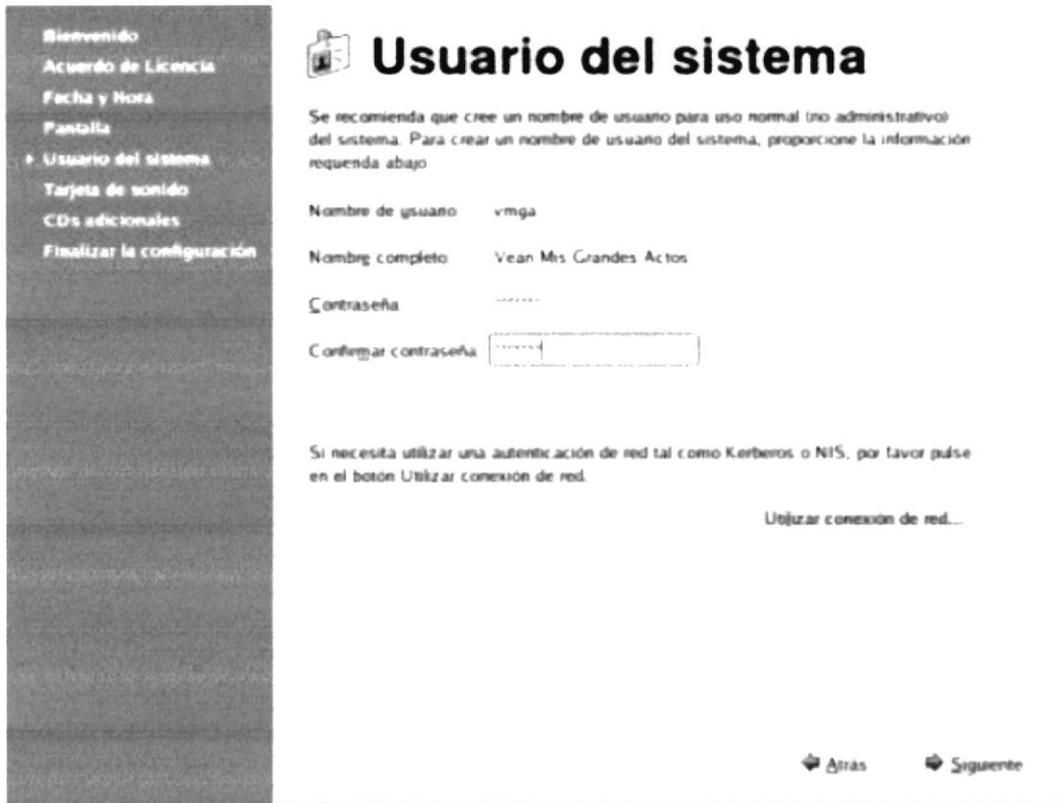


Figura 5-33 Ingreso de Nombre de Usuario

Verifique si funciona correctamente su tarjeta de sonido, seleccione “Realice una prueba de sonido”, si escucha bien el sonido de muestra entonces todo es ok.

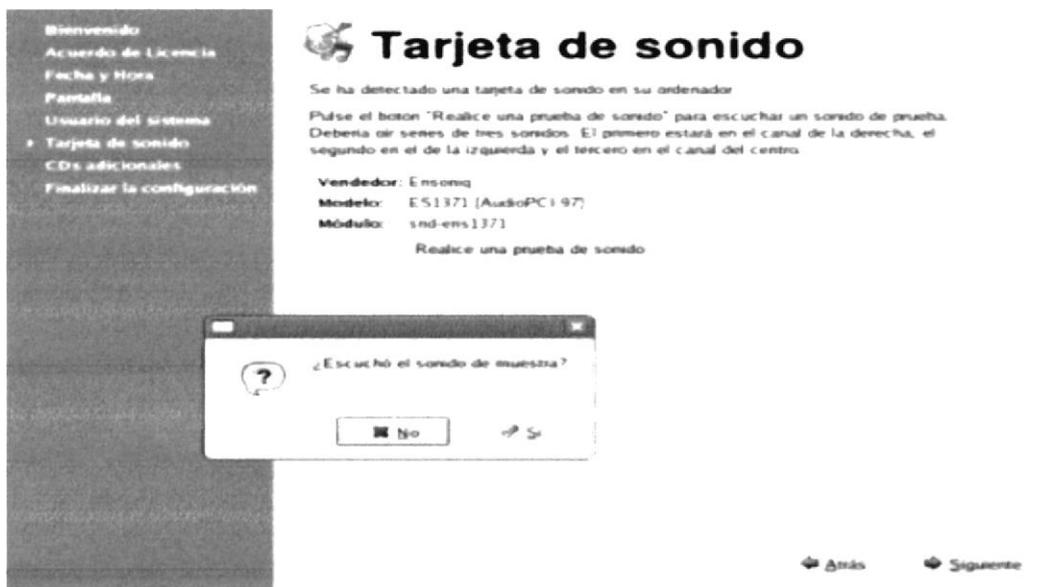


Figura 5-34 Configuración de la tarjeta de sonido

En esta etapa solo si posee cd's adicionales, en nuestro caso y seguramente el suyo solo haga clic en siguiente.

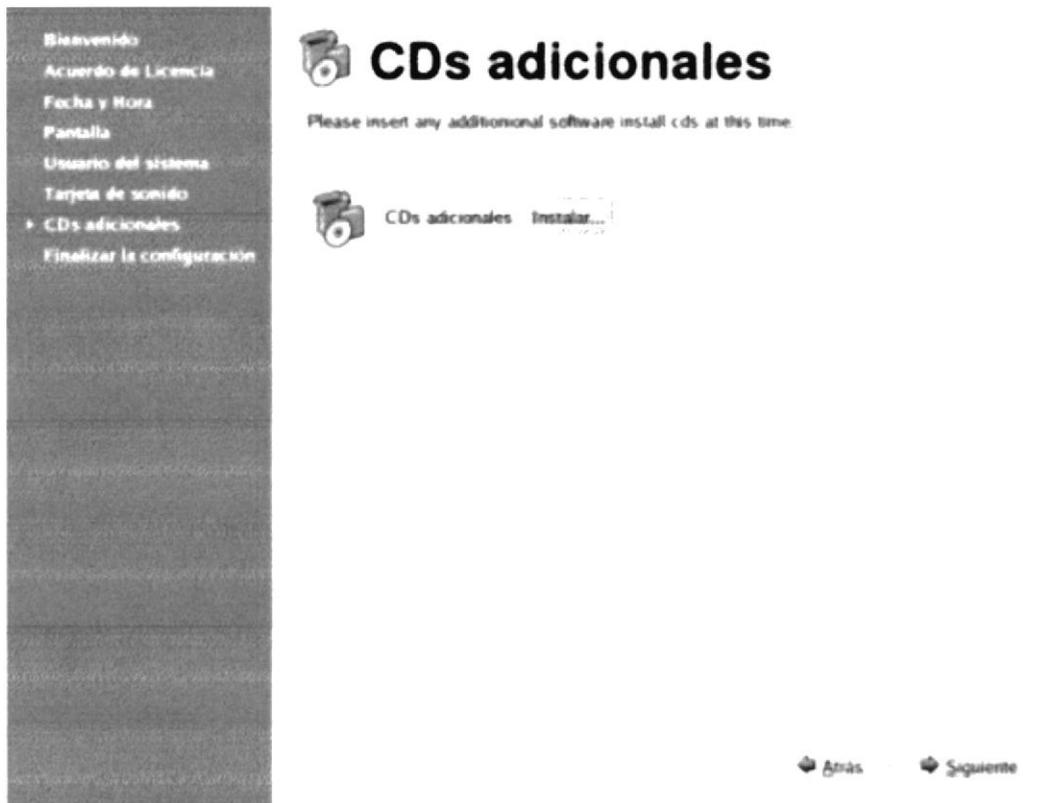


Figura 5-35 Pantalla de opción para la instalación de paquetes adicionales

Terminado el paso anterior estará listo para usar su nuevo sistema Fedora Core 3 ahora solo haga introduzca el nombre de usuario presione “enter” y luego su contraseña.

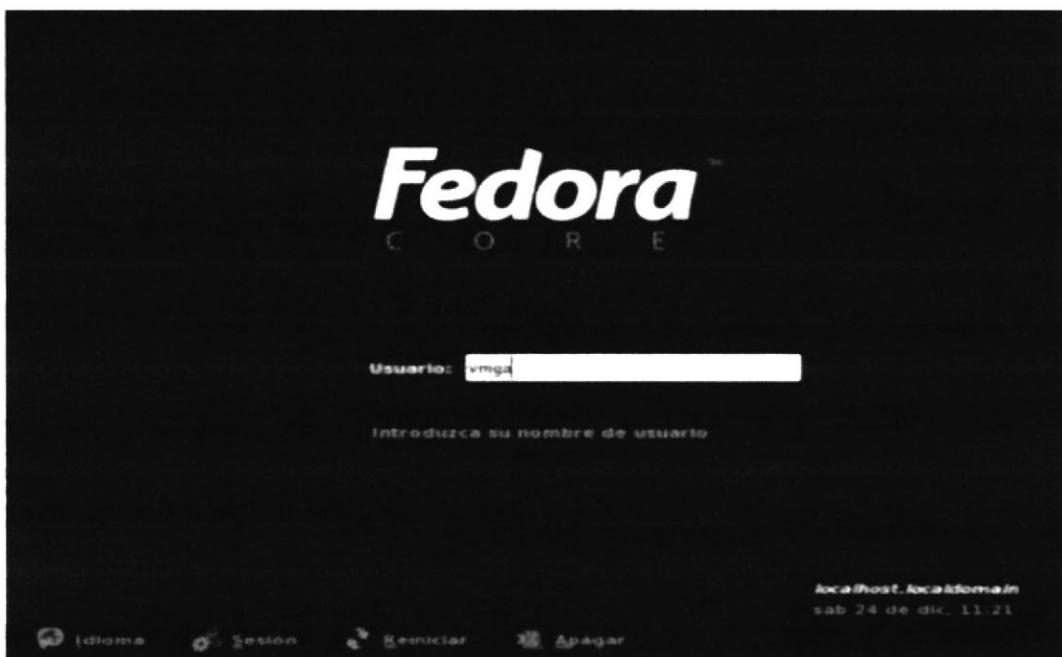


Figura 5-36 Ingreso del Nombre de Usuario

Y listo ya ha terminado de instalar su sistema, sin problemas ahora explore las distintas aplicaciones que posee FC3.



Figura 5-37 Pantalla inicial de Linux Fedora

5.6 INICIANDO LINUX

5.6.1 COMO INICIAR CON LINUX

Existen tres formas de acceder a un sistema *Linux*:

- A través de una consola de texto, el usuario se conecta directamente al ordenador que tiene instalado *Linux* y accede mediante un sistema no gráfico.
- Desde un gestor de sesiones gráfico (*X Window*), el usuario se conecta directamente al ordenador que tiene instalado *Linux* y accede al sistema mediante un programa gráfico.
- Desde un ordenador remoto mediante *telnet* o *secure shell*



PANTALLA DE ARRANQUE DEL SISTEMA OPERATIVO LINUX FEDORA

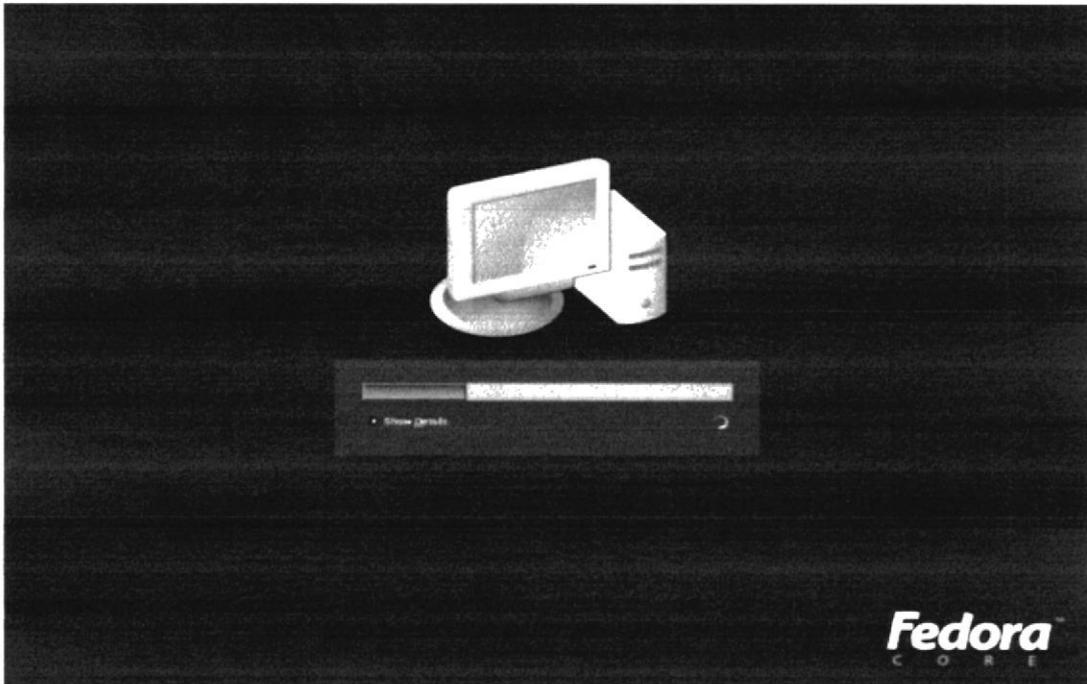


Figura 5-38 Iniciando el Sistema Operativo

5.6.2 INGRESO AL SISTEMA OPERATIVO LINUX FEDORA

En cualquiera de los casos en la pantalla aparecerá lo siguiente:

Login: (Se tecléa el nombre del usuario)

Password: (Se tecléa la contraseña, que no se ve en la pantalla)

Por motivos de seguridad la contraseña debe cumplir ciertas condiciones tales como:

- Contener al menos seis caracteres.
- Contener al menos un carácter numérico o especial y dos alfabéticos.
- Ser diferente del nombre de login.

La primera vez que se accede al sistema la contraseña empleada será la proporcionada por el administrador del sistema. Existen diversas formas para terminar la sesión de trabajo en **Linux**, dependiendo de si estamos en modo gráfico o de texto.

En modo texto:

Presionar las teclas <ctrl> d

*Escribir el comando **exit**.*



INICIALIZACION DE INGRESO A LINUX

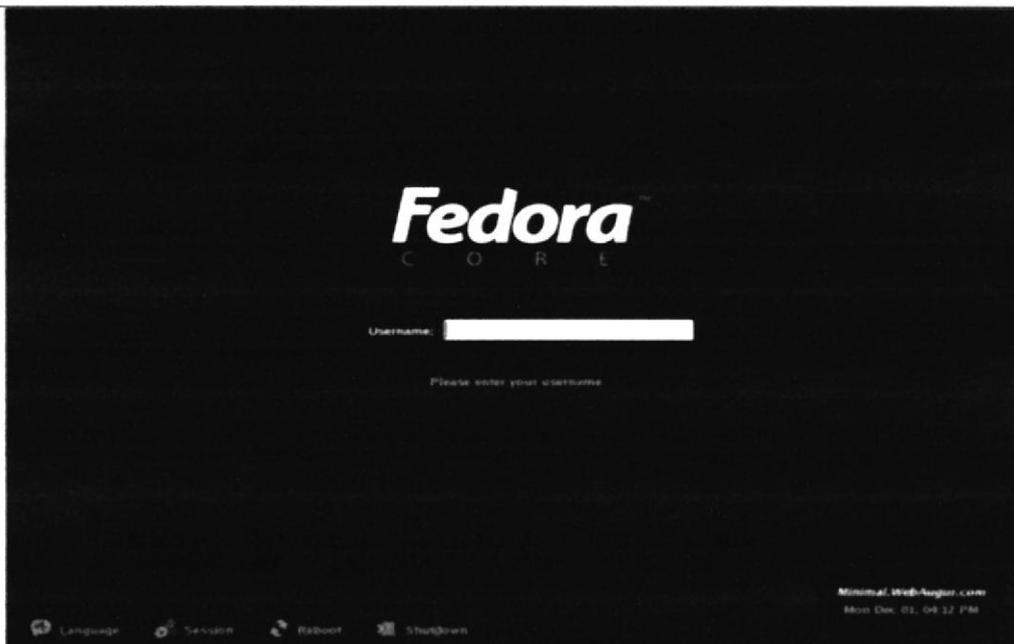


Figura 5-39 Ingreso del Nombre de Usuario



CONFIRMACION DE PASSWORD

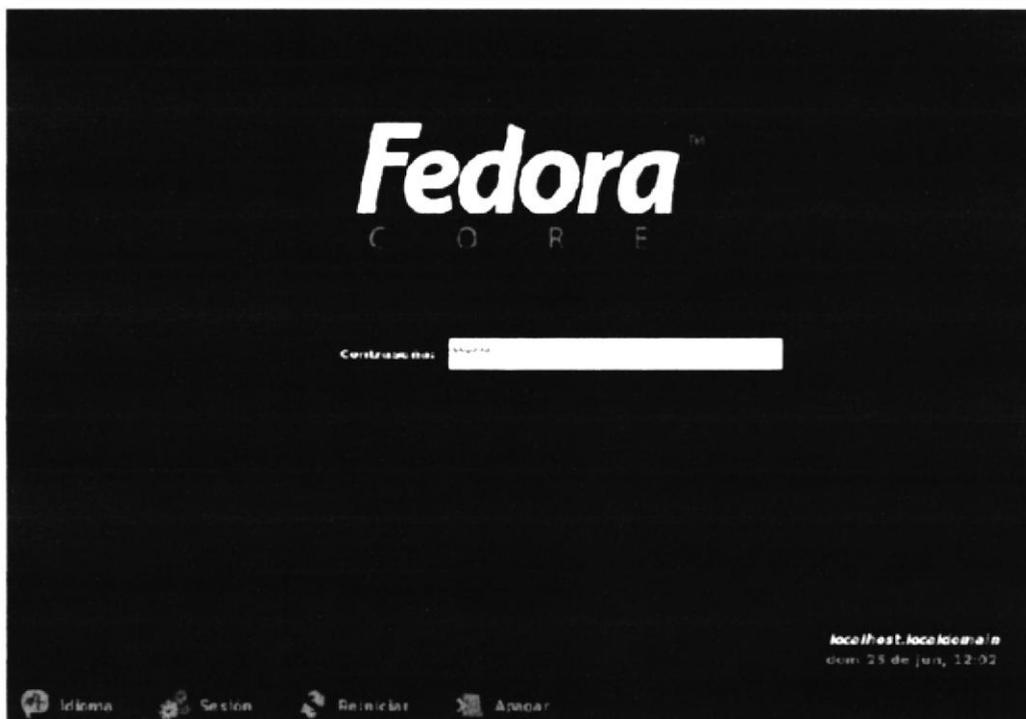


Figura 5-40 Ingreso del Password

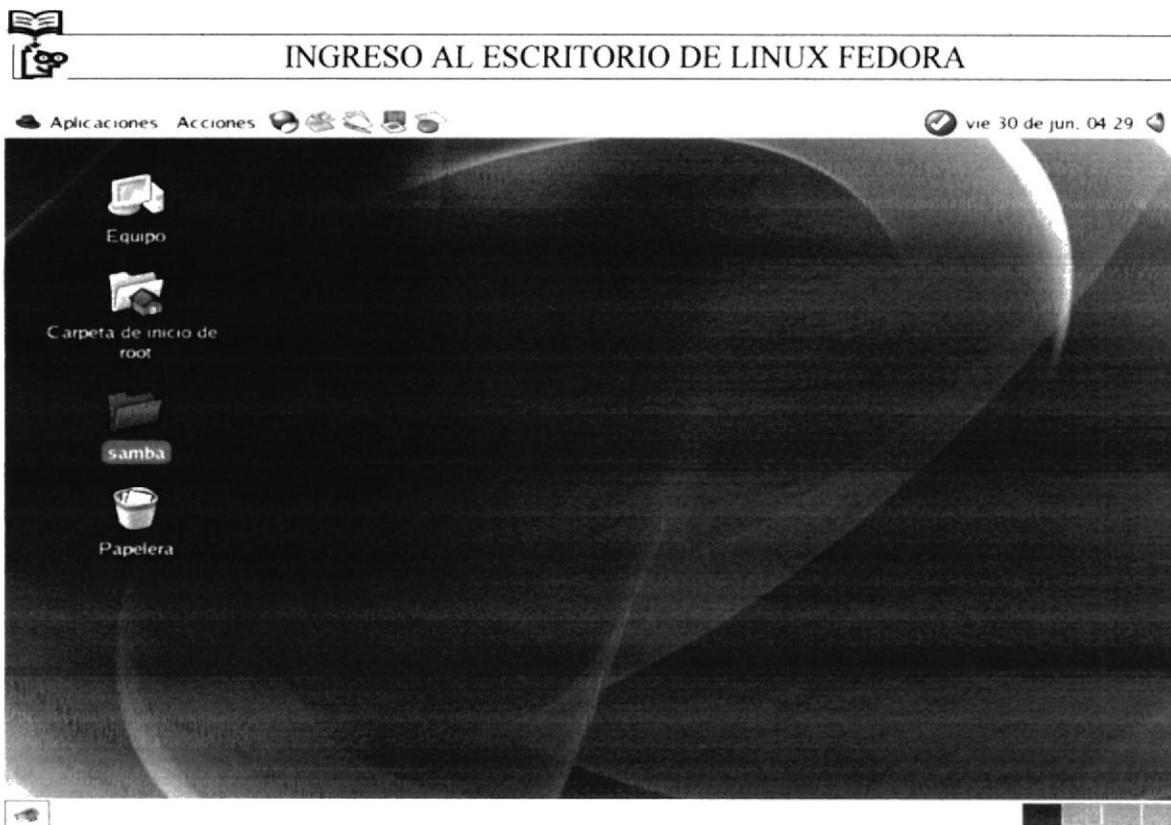


Figura 5-41 Escritorio de Linux

5.7 SAMBA

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

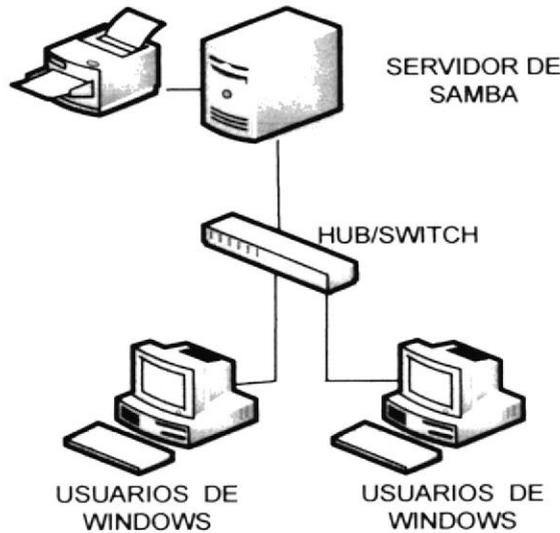


Figura 5-42 Arquitectura de Samba

5.7.1 REQUERIMIENTOS

Requerimientos

- Tener configurada la tarjeta de red tanto en nuestro pc con Linux como en el o los clientes
- Deshabilitar los firewalls en el pc con Linux y en los clientes

Abrir a la Terminal de Linux Fedora e ingresar a la raíz del sistema (**root**) con el comando "cd /".



Figura 5-43 Salir al directorio raíz

Una vez estando en la raíz ingresar el comando setup por teclado e inmediatamente una pantalla del modo grafico saldrá para así de deshabilitar el firewall del administrador.



Dentro del Setup deshabilitar el Firewall con ayuda de la tecla Tab podrá pasar a las siguientes opciones y damos enter en Configuración del Firewall



Figura 5-44 Selección del Menú Configuración de Firewall



Una vez que está dentro de firewall con ayuda de la barra espaciadora seleccione e **inhabilitado** el mismo que es representado con un asterisco y acepte.

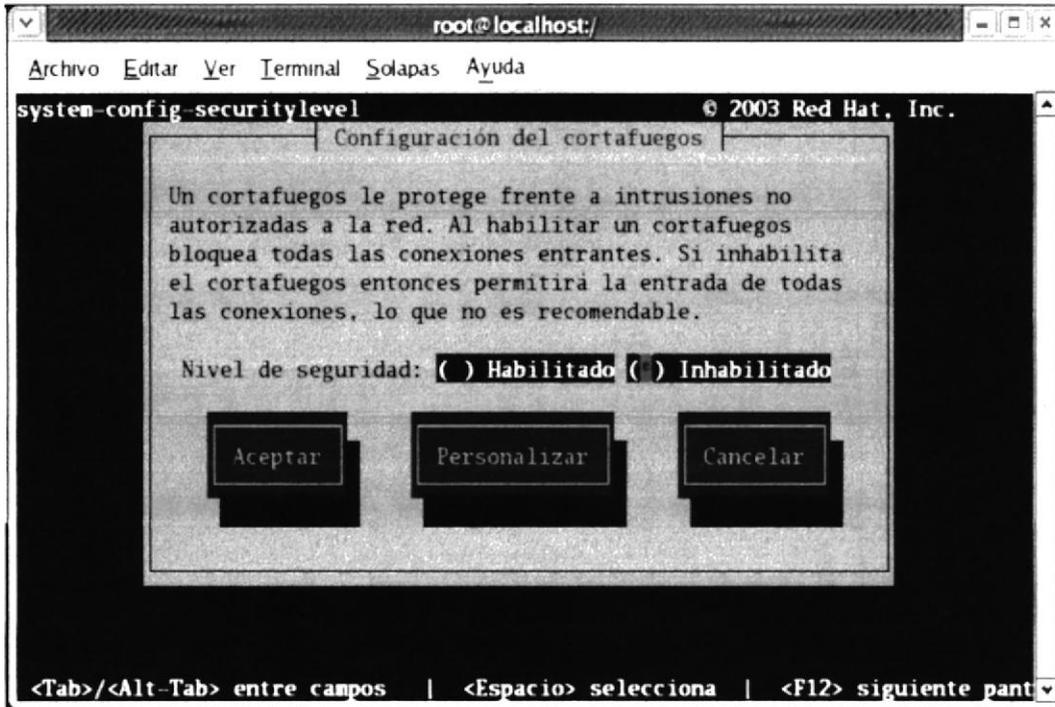


Figura 5-45 Selección del Menú Inhabilitado



Una vez que ingresó al setup diríjase a servicios del sistema y presione enter.



Figura 5-46 Ingreso del Menú Servicios del Sistema

 Estando dentro de servicios del sistema y habilite los servicios de samba (smb, xinetd, network)

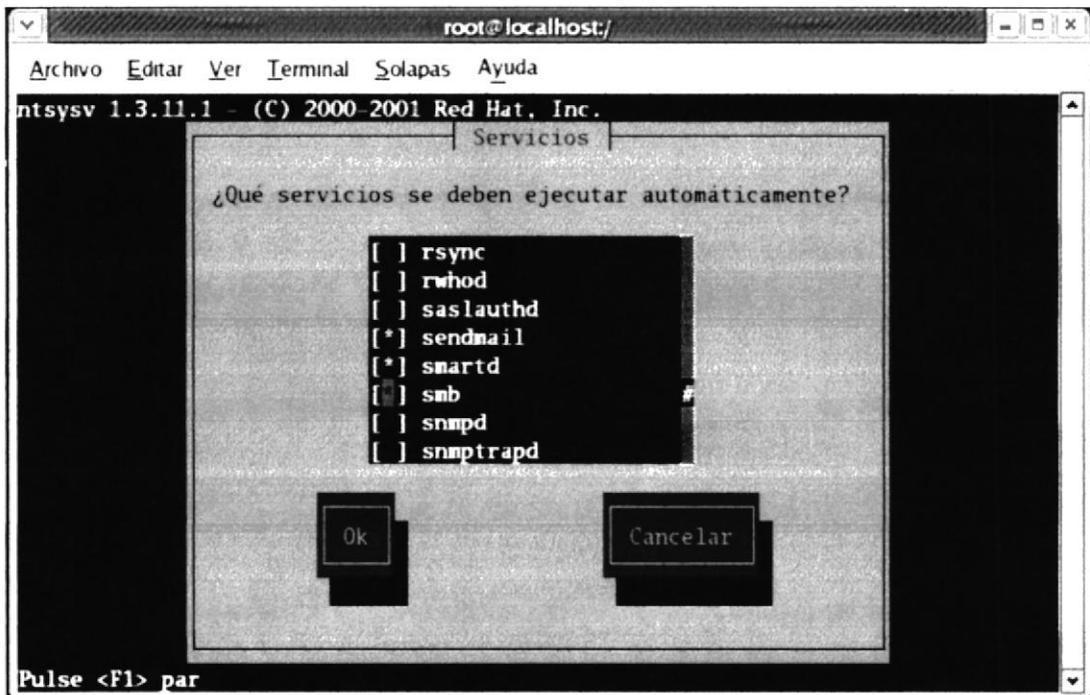


Figura 5-47 Habilitando el Comando smb

5.7.2 CONFIGURACION

1. Utilizar el comando ifconfig para ingresar la dirección IP de la máquina.

 Ifconfig eth0 192.168.12.1 up

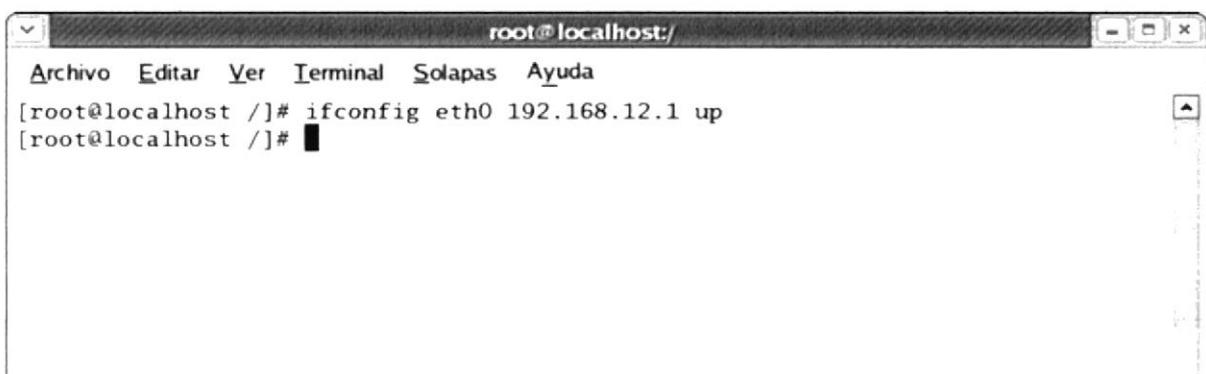


Figura 5-48 Asignación de la dirección IP



Verificar la configuración de la tarjeta de red

```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:01:6C:B6:CF:4E
          inet addr:192.168.12.1  Bcast:192.168.12.255  Mask:255.255.255.0
          inet6 addr: fe80::201:6cff:feb6:cf4e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:987 (987.0 b)  TX bytes:7990 (7.8 KiB)
          Interrupt:11 Base address:0xe800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:7184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5741740 (5.4 MiB)  TX bytes:5741740 (5.4 MiB)

[root@localhost /]#
```

Figura 5-49 Verificación de la dirección IP actual de la maquina

- 2. También tendrá esta segunda opción para configurar la tarjeta de red que está utilizando el comando netconfig que sería en interfaz grafica.



Configuración de la tarjeta de red modo interfaz grafico.

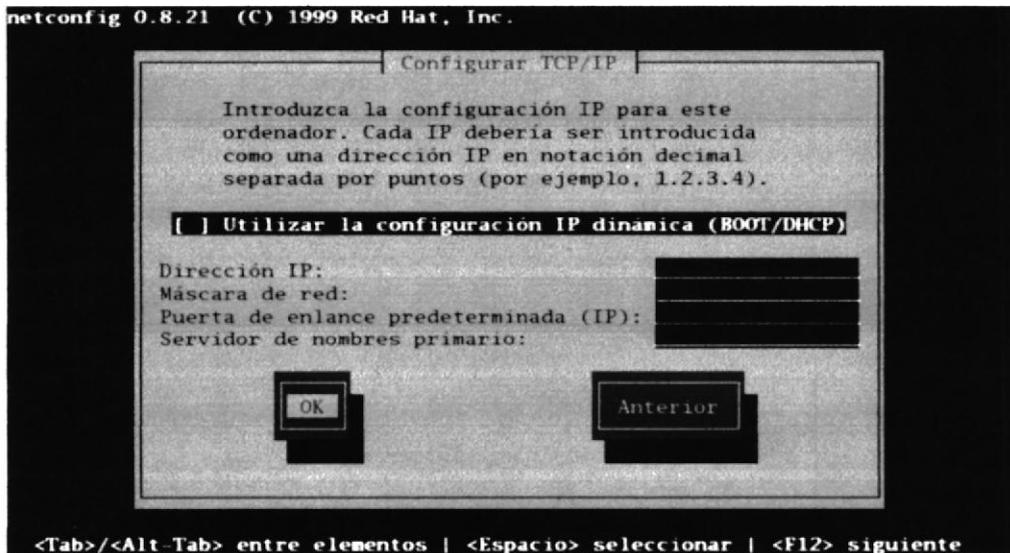


Figura 5-50 Configuración de la dirección IP dinámica

5.- Modificar el archivo en `vi/etc/samba/smb.conf`

Workgroups: permite elegir el grupo de trabajo del que el servidor Samba hace parte.
Netbios Name: permite definir el nombre de la maquina, no como un nombre de DNS, sino como un nombre de resolución de nombres propio del protocolo NetBIOS.



Dentro `vi /etc/samba/smb.conf` al final editamos

```

root@localhost:
Archivo  Editar  Ver  Terminal  Solapas  Ayuda

# The following two entries demonstrate how to share a directory so that two
# users can place files there that will be owned by the specific users. In this
# setup, the directory should be writable by both users and should have the
# sticky bit set on it to prevent abuse. Obviously this could be extended to
# as many users as required.
:[nyshare]
:   comment = Mary's and Fred's stuff
:   path = /usr/somewhere/shared
:   valid users = mary fred
:   public = no
:   writable = yes
:   printable = no
:   create mask = 0765

[topico]
path = /topico
valid users = upen
public = yes
writable = yes
browsable = yes

302.0-1  Final

```

Figura 5-53 Crear la carpeta de trabajo en el archivo `smb.conf`

5.7.3 DESCRIPCION DE SAMBA

El volumen puede utilizar cualquiera de las siguientes opciones:

Opción	Descripción
Path	Dirección de la ubicación de la carpeta a utilizar
public	Es un equivalente del parámetro guest ok , es decir define si se permitirá el acceso como usuario invitado. El valor puede ser Yes O No.
browseable	Define si se permitirá mostrar este recurso en las listas de recursos compartidos. El valor puede ser Yes O No.
writable	Define si se permitirá la escritura. Es el parámetro contrario de read only. El valor puede ser Yes O No. Ejemplos: «writable = Yes» es lo mismo que «read only = No». Obviamente «writable = No» es lo mismo que «read only = Yes»
valid users	Define que usuarios o grupos pueden acceder al recurso compartido. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo precedidos por una @. Ejemplo: Spiderman, Superman, Batman @administradores

Tabla 5-2 Descripción de SAMBA

6.- Crear un directorio (Tópico) como detallamos arriba.



Creación de un directorio dentro de la raíz del sistema

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

Figura 5-54 Creación del Directorio upacifico

7.- Crear un archivo en el directorio /Tópico/deber.txt



Creación de un archivo dentro del directorio creado anteriormente

```
root@localhost:/upacifico
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost upacifico]# touch deber.txt
[root@localhost upacifico]# ls
deber.txt
[root@localhost upacifico]#
```

Figura 5-55 Creación y presentación del archivo deber.txt

Crear un archivo en el directorio
touch /Topico/deber.txt

Asignar los permisos al directorio y al archivo

```
chmod +777 /Topico
chmod +777 /Topico/deber.txt
```

Crear los usuarios que anteriormente registramos en valid user.
adduser upacifico

Dar su respectiva contraseña.
passwd upacifico

Asigne contraseñas a los usuarios para hacer uso del servicio de samba
smb passwd -a upacifico

Restaurar los servicios de samba.



Restaurar de servicios de Smb “service smb restart”



Figura 5-56 Restaurar los servicios de Samba

8. Acceda a la maquina Linux por medio de la dirección ip, vamos a inicio. Ejecutar y ponemos la dirección de nuestro servidor en este caso 192.168.12.10 como detallamos abajo.

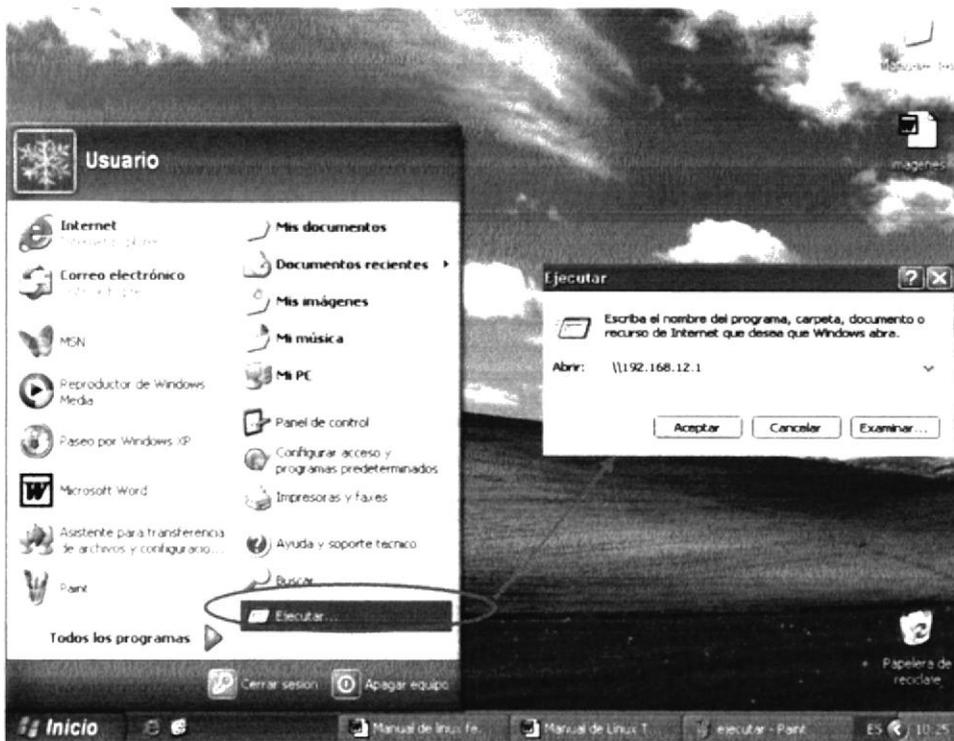


Figura 5-57 Ingreso a la maquina Linux por medio de la dirección IP

9. Ingresar su nombre de usuario al que se dio los permisos en la configuración de samba con su respectivo password (clave)

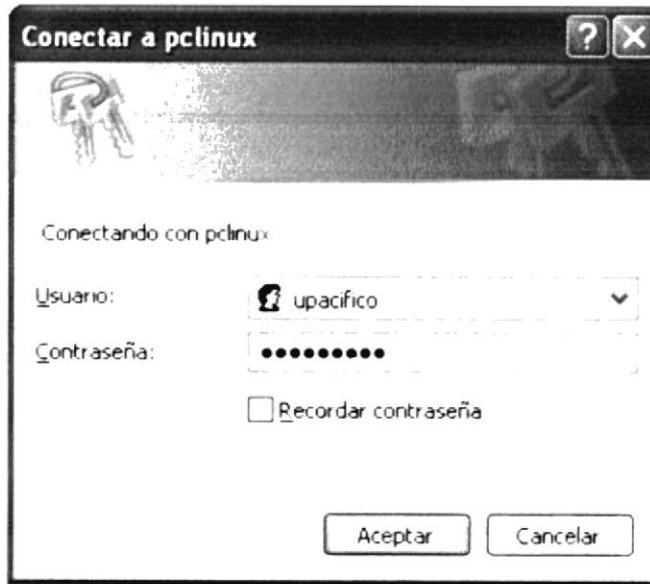


Figura 5-58 Ingreso del usuario y Password

10. Verificar que podemos acceder a nuestros recursos compartidos en nuestro servidor Samba

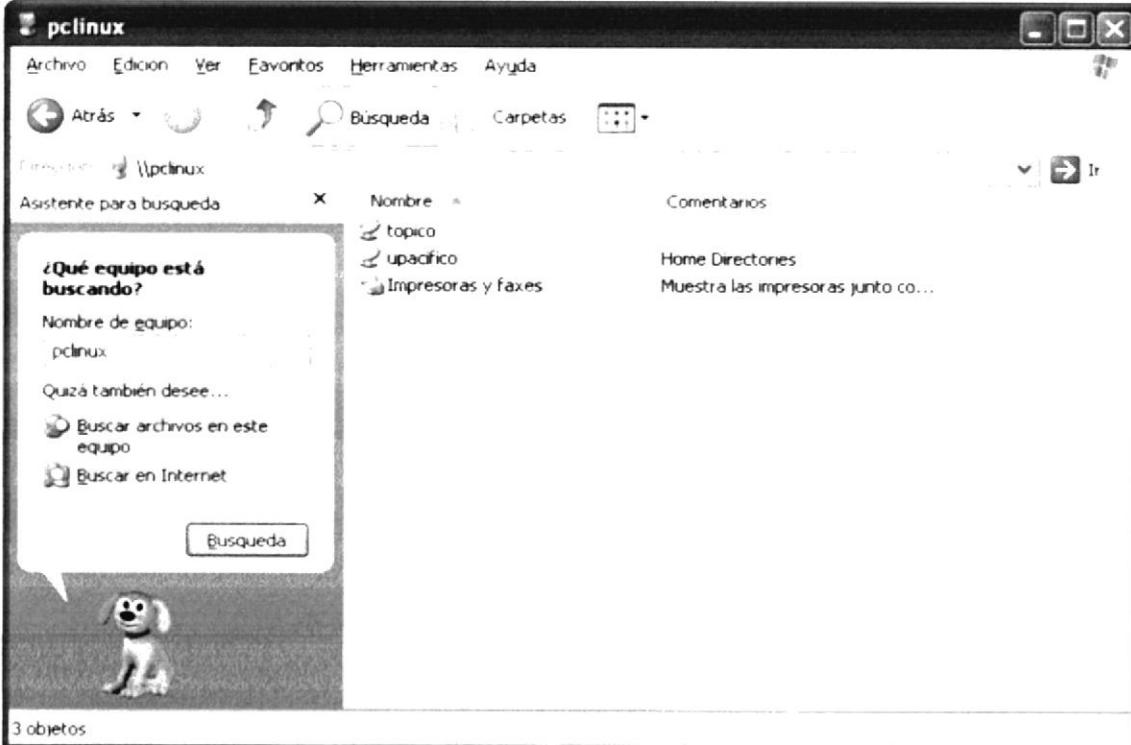


Figura 5-59 Carpetas de la maquina Linux

5.8 DNS (SISTEMA DE DOMINIO DE NOMBRE)

Domain Name System, esta configuración realizada es un servidor que le permite convertir Nombres a direcciones IP. La búsqueda de DNS es de forma recursiva, está basado en una estructura jerárquica. DNS se vale del FQDN (Full Qualified Domain Name que es la relación exacta con respecto a un dominio), para la resolución de nombres de host a su respectiva dirección IP.

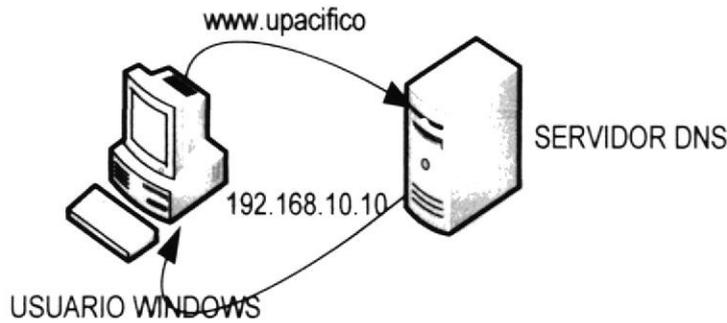


Figura 5-60 Arquitectura de DNS

5.8.1 REQUERIMIENTOS

- Tener configurada la tarjeta de red tanto en nuestro pc con Linux como en el o los clientes
- Deshabilitar los firewalls en el pc con Linux y en los clientes

5.8.2 PRE-REQUISITOS:

Revisar si se encuentra instalado el paquete de de Dns (bind) en nuestro sistema, dentro del setup habilitar los servicios de Dns (named).



Utilizar el comando `rpm -q bind`

```

root@localhost:~# rpm -q bind
bind-9.2.4-2
root@localhost:~#

```

Figura 5-61 Verificando si esta instalado el paquete bind

Verificar en el setup si esta activado el paquete named

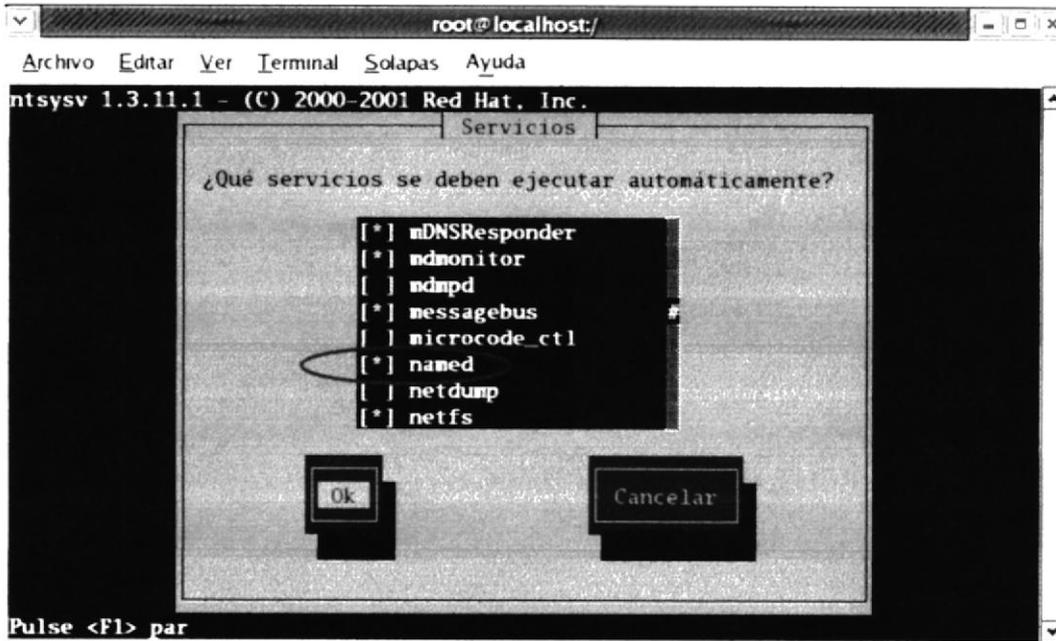


Figura 5-62 Verificación del paquete named

5.8.3 CONFIGURACIONES:

1.-Para la configuración de DNS, se empieza configurando el archivo named.conf encontrará todos los dominios ya existentes, podrá facilitar la escritura copiando uno de estos párrafos (con la tecla Y seguido del número de líneas que se desea copiar; y se lo pega con la letra P).



Ingresamos el archivo vi /etc/named.conf

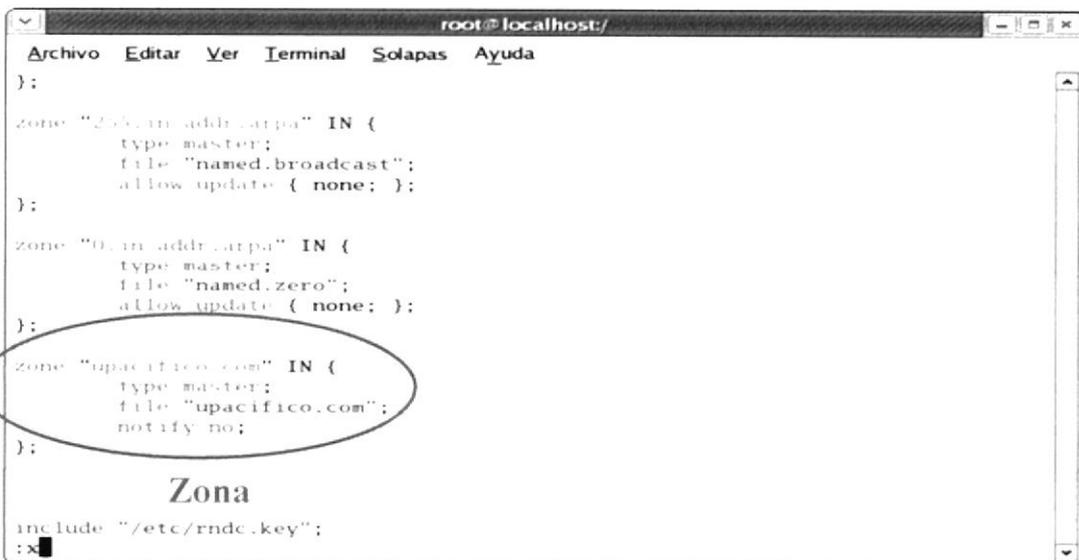
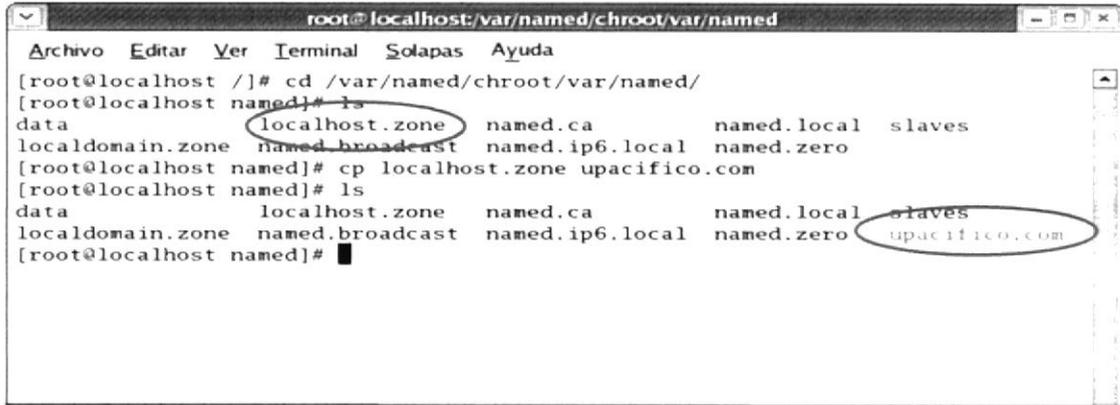


Figura 5-63 Configuración de la zona en el archivo named.conf

2.- Luego vaya a la ruta `cd /var/named/chroot/var/named/` procederá a copiar su dominio con el comando `cp` que permite copiar el contenido de un archivo existente (`localhost.zone`) a uno recién creado (`upacifico.com`).

 Ingresamos el comando `cd /var/named/chroot/var/named/`

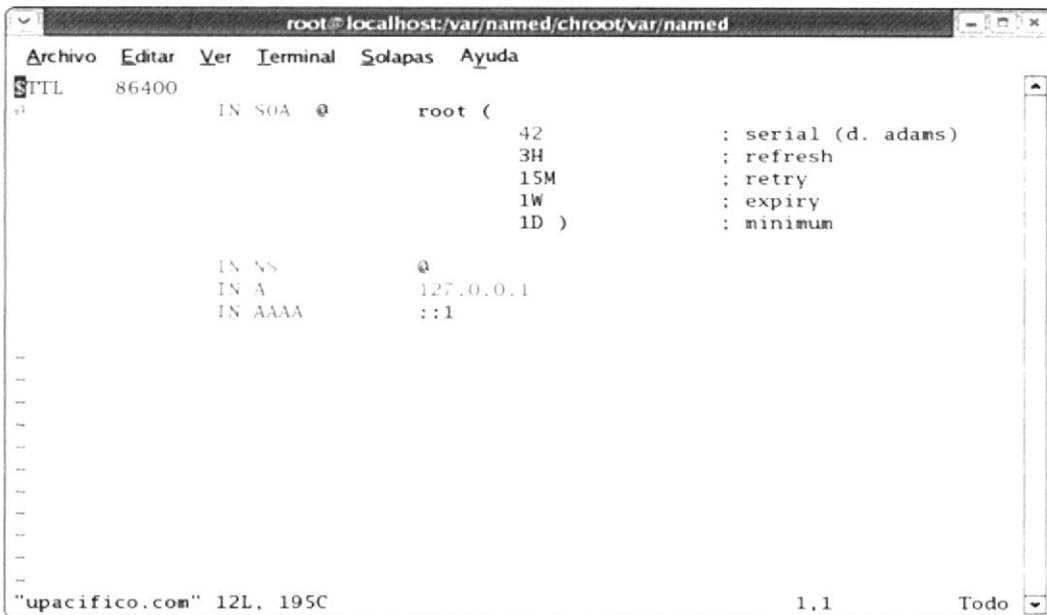


```
root@localhost:var/named/chroot/var/named
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# cd /var/named/chroot/var/named/
[root@localhost named]# ls
data          localhost.zone  named.ca       named.local    slaves
localdomain.zone named.broadcast named.ip6.local named.zero
[root@localhost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

Figura 5-64 Se copia el archivo `localhost.zone`

3.- Ahora modificara el archivo que copió en este caso `upacifico.com`

 Ingrese al archivo `vi upacifico.com`



```
root@localhost:var/named/chroot/var/named
Archivo Editar Ver Terminal Solapas Ayuda
STIL 86400
"upacifico.com" 12L, 195C
1,1 Todo
IN SOA @ root (
42 : serial (d. adams)
3H : refresh
15M : retry
1W : expiry
1D ) : minimum
IN NS @
IN A 127.0.0.1
IN AAAA ::1
```

Figura 5-65 Archivo `upacifico.com` sin editar



Una vez editado quedara de la siguiente forma a mostrar a continuación

```

root@localhost:/var/named/chroot/var/named
Archivo Editar Ver Terminal Solapas Ayuda
$TTL      86400
@          IN SOA  upacifico.com.  root.upacifico.com. (
; serial (d. adams)
; refresh
; retry
; expiry
; minimum

localhost IN NS   upacifico
upacifico IN A   127.0.0.1
www       IN A   192.168.12.1
;
;
;

```

Figura 5-66 Archivo upacifico.com editado

Comandos

Significado

SOA (Start of Authority)	Inicio de autoridad
@	Abreviatura del inicio del archivo de zona
IN	Dirección de Internet
NS	Indica los servidores DNS del sistema
CNAME	Especifica la resolución de <i>nombres textuales</i> a <i>nodos IP</i>

4.-Se reiniciará los servicios del named



Ingresar el comando service named restart

```

root@localhost:/var/named/chroot/var/named
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost named]# service named restart
Parando named:
Iniciando named:
[root@localhost named]# [ OK ]

```

Figura 5-67 Reiniciar los servicios del DNS

En la maquina de Windows se asigna la dirección de DNS siguiendo los siguientes pasos:

Primero acceder a mis sitios de red, damos clic derecho al icono Mis Sitios de Red que esta en el escritorio y elija la opción propiedades



Figura 5-70 Ingreso al Menú propiedades del icono Mis sitios de Red

A continuación verá la pantalla de conexiones de red, le damos clic derecho al icono de conexiones de área local y elija propiedades

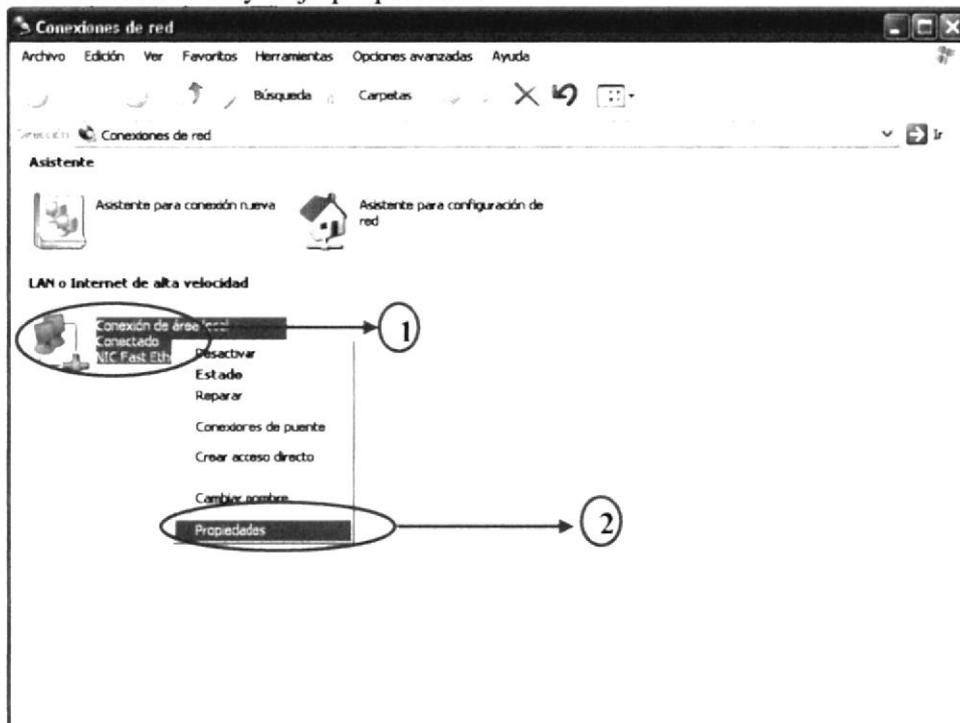


Figura 5-71 Ingresando al Menú Propiedades del icono Mis sitios de Red

Luego verá la pantalla de propiedades de conexión de área local, **1** le damos clic a protocolo Internet (TCP/IP), **2** clic en propiedades

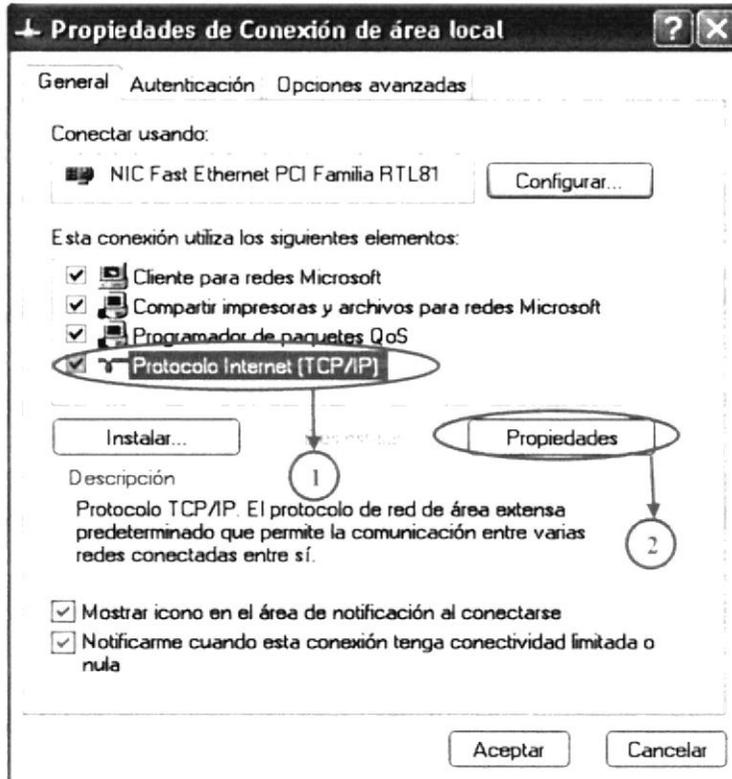


Figura 5-72 Ingreso a las Propiedades del Protocolo Internet

Configurar su tarjeta ingresando **1** la dirección IP, **2** la máscara de red **3** puerta de enlace, **4** la dirección de la maquina en Linux que sería nuestro DNS y **5 damos** clic en aceptar para que los cambios tengan efectos

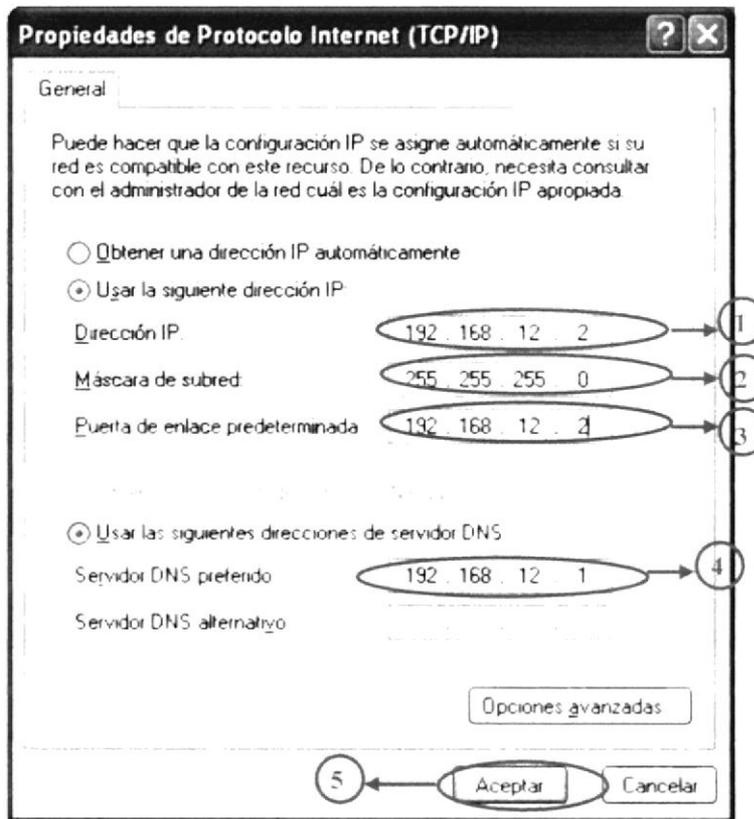


Figura 5-73 Ingreso de la dirección IP de la maquina

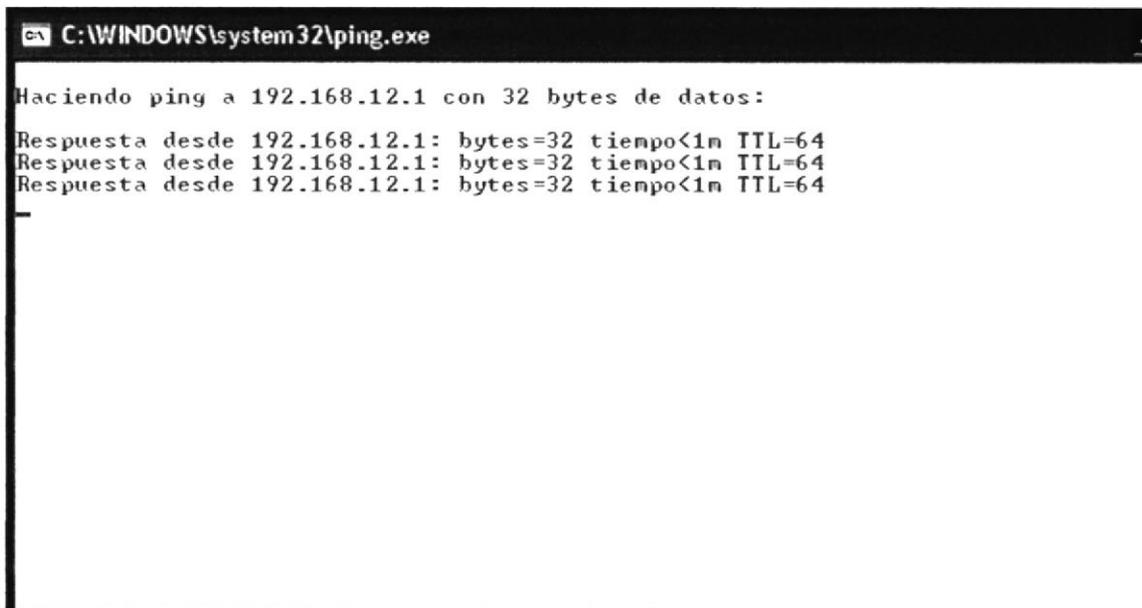


Figura 5-74 Tiempos de respuestas a la maquina de Linux

5.9 WEBSERVER

Un servidor Web Linux correctamente configurado es casi insuperable. Puede tener años que puede llegar a estar corriendo el servidor sin necesidad de reiniciarse y sin fallas.

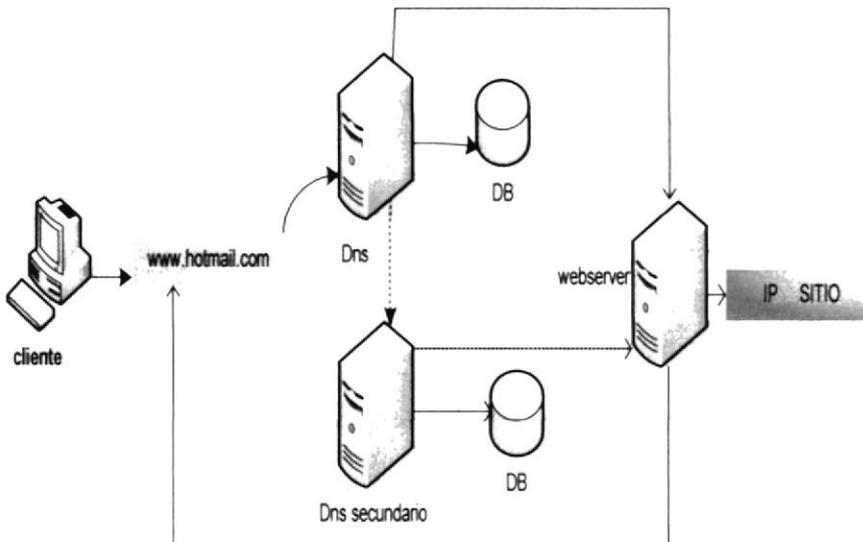


Figura 5-75 Arquitectura de Web Server

5.9.1 REQUERIMIENTOS

- Tener configurada la tarjeta de red tanto en su pc con Linux como en el o los clientes
- Deshabilitar los firewalls en el pc con Linux y en los clientes
- Tener configurado DNS

5.9.2 PRE-REQUISITOS

Para empezar la configuración de Web Server (Servidor Web) necesitará como pre-requisito tener levantado DNS y contar con el paquete httpd, lo que verificará de la siguiente manera:



Ingrese el comando `rpm -q httpd`

```

root@localhost:~/var/named/chroot/var/named
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost named]# rpm -q httpd
httpd-2.0.52-3
[root@localhost named]#
  
```

Figura 5-76 Se verifica si está instalado el paquete httpd

1.-Configure el archivo `httpd.conf` que se encuentra en la siguiente ruta tiene que editar el siguiente fichero y buscar las siguientes líneas (Puede hacerlo por secciones o por líneas) y descomentarlas:



Ingrese el comando `vi /etc/httpd/conf/httpd.conf`

- * Listen 80
- * DocumentRoot "/var/www/html"
- * Directory Index index.html index.htm

```

root@localhost:~/var/named/chroot/var/named
Archivo Editar Ver Terminal Solapas Ayuda
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 80
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as
a DSO you
  
```

Figura 5-77 Se descomenta la línea Listen 80

* NameVirtualHost *:80

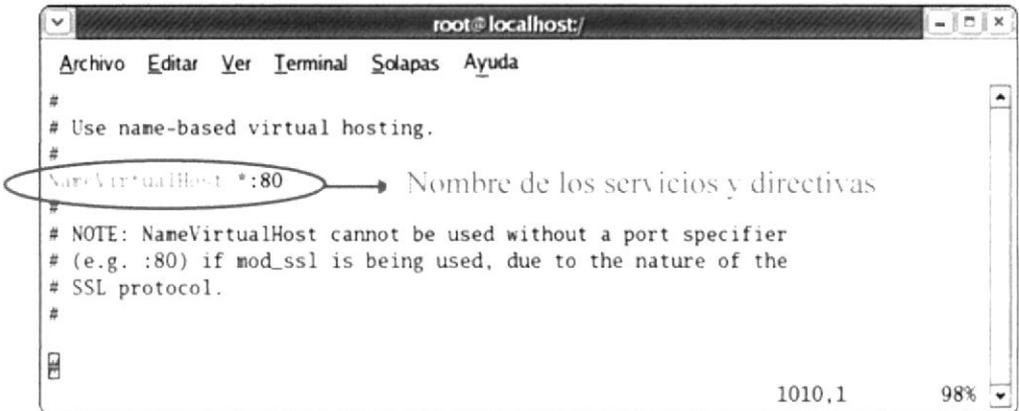


Figura 5-78 Se descomenta la línea NamevirtualHost *:80

En el párrafo del <virtual host *:80> deberá realizar los siguientes cambios, podrá facilitar la escritura copiando uno de estos párrafos (primero digitamos la tecla Esc para habilitar los comandos luego presionar la tecla Y seguido del número de líneas que se desea copiar; luego se dirige al lugar donde se quiere el texto y se lo pega con la letra P).

<VirtualHost *:80>

ServerAdmin root@localhost.localdomain

DocumentRoot /var/www/html/web/ (sitio es la carpeta donde se va a guardar el sitio)

ServerName www.pacifico.com (nuestro servidor DNS)

</VirtualHost>

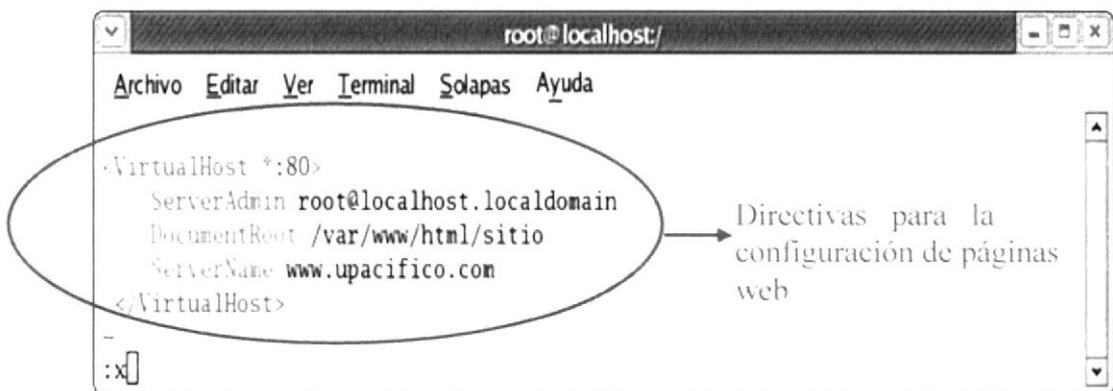


Figura 5-79 Se configura el párrafo <VirtualHost *:80>

2.-Ingrese a la ruta especificada creará la carpeta Web donde se alojada nuestro sitio Web ya creada la carpeta, ingrese a ella y edite el sitio index (en donde se encontrará el sitio Web).

5.-Una vez realizado los pasos anteriormente dicho podrá ir al navegador y cargar la página, en este caso: www.upacifico.com

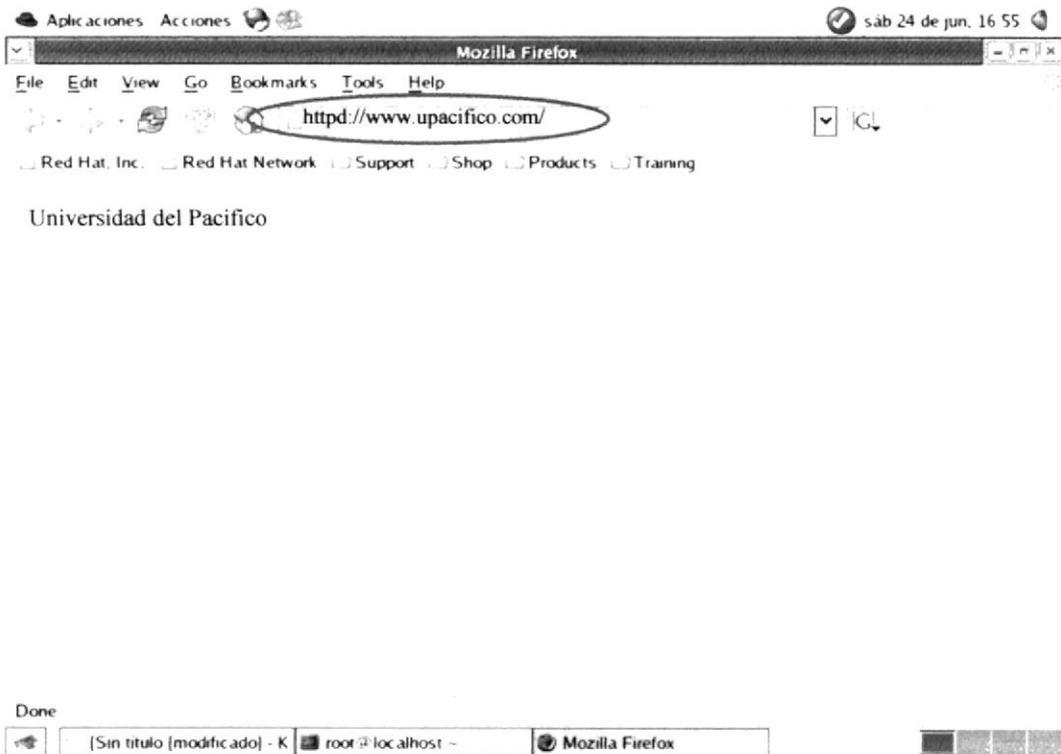


Figura 5-83 Se levanta la página web upacifico

5.10 PROXY

El Servidor Proxy Linux es una solución segura, robusta y versátil basada en Software Libre para una red local corporativa, es el que se encarga de la distribución de Internet y accesos o restricciones de determinados usuarios a ciertos servicios. El Servidor Proxy Linux ofrece grandes ventajas en el uso de la conexión a Internet como la optimización de la velocidad de conexión y mejora en la seguridad de la red local.

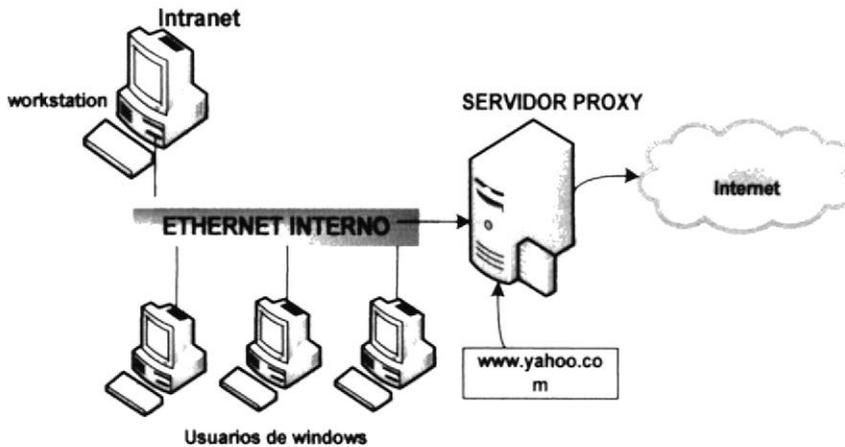


Figura 5-84 Arquitectura Proxy

5.10.1 REQUERIMIENTOS

- Tener configurada la tarjeta de red tanto en su nuestro pc con Linux como en el de los clientes
- Deshabilitar los firewall en el pc con Linux y en los clientes
- Tener configurado Webserver

5.10.2 PRE-REQUISITOS

Para realizar la configuración de un servidor Proxy, requiere que previamente se hayan configurado Servidores DNS y Web Server.

Verificar si el paquete de squid esta instalado, caso contrario digitar el comando setup y elija la opción Servicios del Sistema y habilitar squid.



Ingrese el comando rpm -q squid

```
root@localhost:~# rpm -q squid
squid-2.5.STABLE6-3
[root@localhost ~]#
```

Figura 5-85 Se verifica si esta instalado el paquete squid



Ingrese el comando ifconfig para comprobar la dirección ip

```
root@localhost:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:01:6C:B6:CF:4E
          inet addr:192.168.12.1  Bcast:192.168.12.255  Mask:255.255.255.0
          inet6 addr: fe80::201:6cff:feb6:cf4e/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4  errors:0  dropped:0  overruns:0  frame:0
          TX packets:53  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:987 (987.0 b)  TX bytes:7990 (7.8 KiB)
          Interrupt:11  Base address:0xe800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:7184  errors:0  dropped:0  overruns:0  frame:0
          TX packets:7184  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:5741740 (5.4 MiB)  TX bytes:5741740 (5.4 MiB)

[root@localhost /]#
```

Figura 5-86 Se comprueba la dirección IP de la maquina

1.-Para configurar el archivo squid deberá editar en la ruta que a continuación mostraremos:



Ingrese al directorio `vi /etc/squid/squid.conf`

```

root@localhost:var/www/html/sitio
Archivo Editar Ver Terminal Solapas Ayuda
#
#Default:
# http_port 3128
http_port 8080
-- INSERTAR --                               57,1      1%

```

Figura 5-87 Se descomenta y edita la línea `http_port 8080`

En esta sección se debe editar ciertas líneas, como es el puerto 8080, el cual nos permitirá “escuchar”. `http_port 8080`

Aquí se asigna la memoria cache, en este caso se ha asignado 16MB

`Cache_dir ufs /var/spool/squid 700 16 256`

`Cache_access_log /var/log/squid/access_log`

```

root@localhost:var/www/html/sitio
Archivo Editar Ver Terminal Solapas Ayuda
#
#
#Default:
# cache_mem 8 MB
cache_mem 16 MB
-- INSERTAR --                               487,1     14%

```

Figura 5-88 Se descomenta y edita la línea `cache_mem`

```

root@localhost:var/www/html/sitio
Archivo Editar Ver Terminal Solapas Ayuda
#
#Default:
# cache_dir ufs /var/spool/squid 100 16 256
cache_dir ufs /var/spool/squid 100 16 256
#
#
-- INSERTAR --                               706,1     20%

```

Figura 5-89 Se descomenta la línea `cache_dir`

2.-Luego diríjase a las listas de acceso donde editaremos la siguiente:
Acl red src 192.168.1.10/255.255.255.0



```

root@localhost:/var/www/html/sitio
Archivo Editar Ver Terminal Solapas Ayuda
acl all src 0.0.0.0/0.0.0.0
acl red src 192.168.12.1/255.255.255.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443 563    # https, snews
acl Safe_ports port 70         # gopher
acl Safe_ports port 210        # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280        # http-mgmt
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
acl CONNECT method CONNECT
-- INSERTAR --
1812,39 53%

```

Figura 5-90 Se edita la siguiente línea en la sección de las ACL

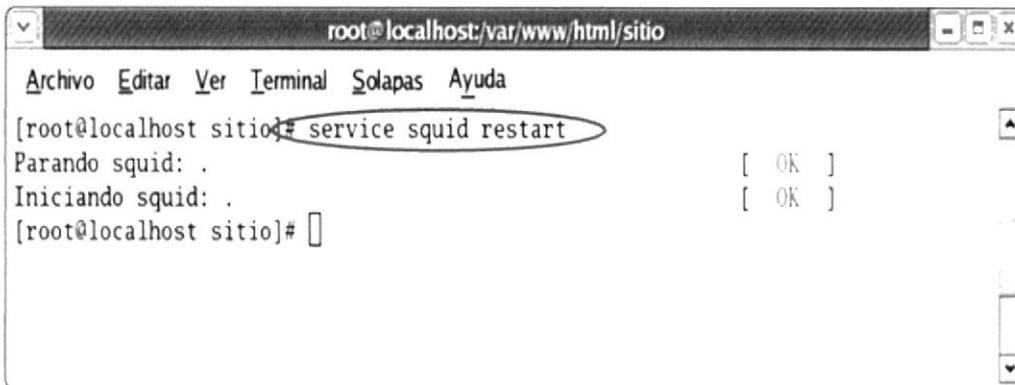
3.-A continuación aquí permitirá que a la red que haya especificado en la ACL pueda tener acceso a navegar:

http_access allow red

4.-Reinicie servicio del squid



Reinicie los servicios del squid: `service squid restart`



```

root@localhost:/var/www/html/sitio
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost sitio]# service squid restart
Parando squid: . [ OK ]
Iniciando squid: . [ OK ]
[root@localhost sitio]#

```

Figura 5-91 Se reinician los servicios del Proxy

5.-Ingrese al explorador de windows, herramientas, opciones de Internet como vemos en la siguiente grafica:

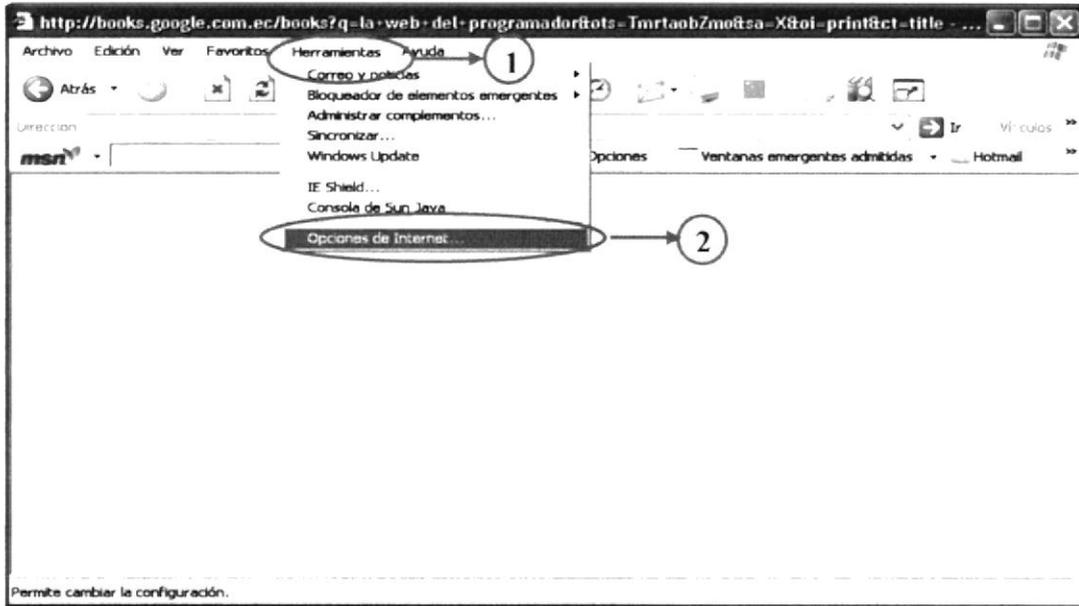


Figura 5-92 Se ingresa al Sub Menú Opciones de Internet

6.-Dentro de opciones de Internet escoja la pestaña conexiones, configuración de la red LAN como vera a continuación:

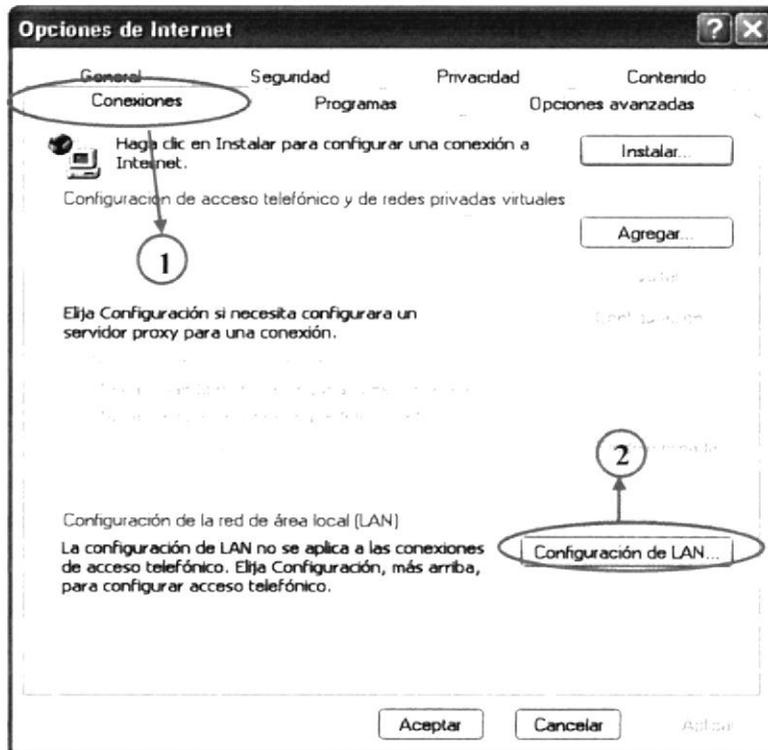


Figura 5-93 Se ingresa a las configuraciones LAN dando clic en el botón (2)

7.-Aquí pondrá la dirección del servidor y el Puerto de comunicación en este caso para proxy es el 8080

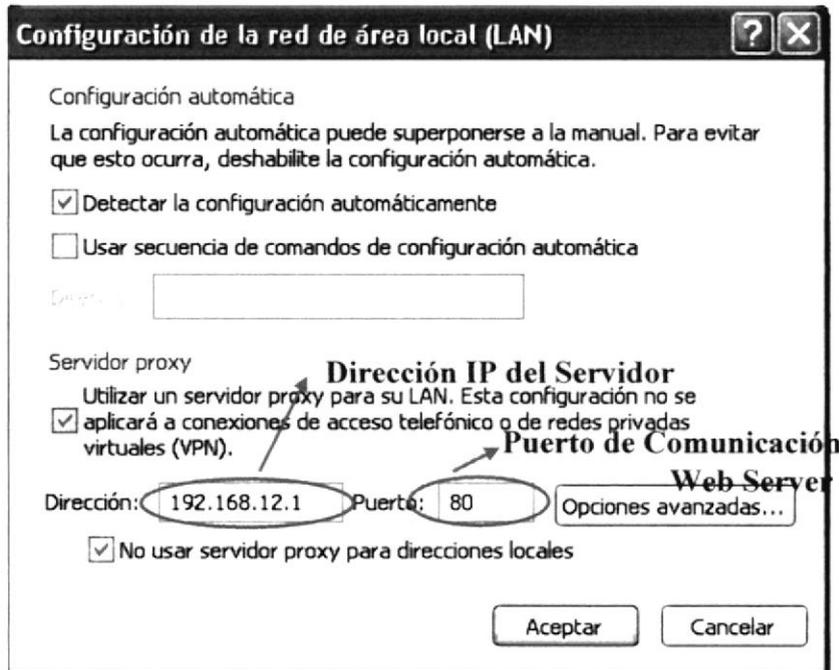


Figura 5-94 Ingreso de la dirección IP y el puerto de comunicación

8.-A continuación cargara la página www.upacifico.com



Figura 5-95 Pagina Universidad del Pacifico desde Windows

5.10.3 DENEGAR HORA

Incluir las listas de control de acceso (ACL)

acl (nombre de la lista) time (día) (hora inicio)-(hora fin)

Ej.: acl matutino time A 12:00-12:10

acl (nombre de la regla) src (IP de la red o la maquina a restringir)/

Ej.: acl cliente src 192.168.12.2/

Los días están determinados por las letras

Lunes M

Martes T

Miércoles W

Jueves H

Viernes F

Sábado A

Domingo S

Pueden combinarse los días

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

Incluir las listas en las reglas de control de acceso

http_acces deny cliente matutino

Reinicie el servicio.

service squid restart

5.10.4 ACCESO CON AUTENTICACIÓN (PASSWORD)

Crear el archivo clave.

touch /etc/squid/claves

Levantar permisos al archivo.

chmod 600 /etc/squid/claves

Cambiar de propietario al archivo.

chown squid:squid /etc/squid/claves

Asignar contraseña

htpasswd /etc/squid/claves (usuario existente)

Configurar el archivo squid.

Especificar ruta del programa básico de parámetros de autenticación y ruta de contraseñas.

La línea donde dice auth_param descomentarla y ponerla así:

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

Incluir lista de control de acceso.
acl password proxy_auth REQUIRED

Incluir regla de control de acceso
http_access allow cliente password

Salir con: wq para guardar los cambios.

Reiniciar el servicio.
service squid restart

Una vez configurado el proxy con acceso de autenticación abra el explorador de windows cargue el sitio web, en este caso www.pacifico.com verá que le pedirá usuario y clave que fueron creados en Linux.

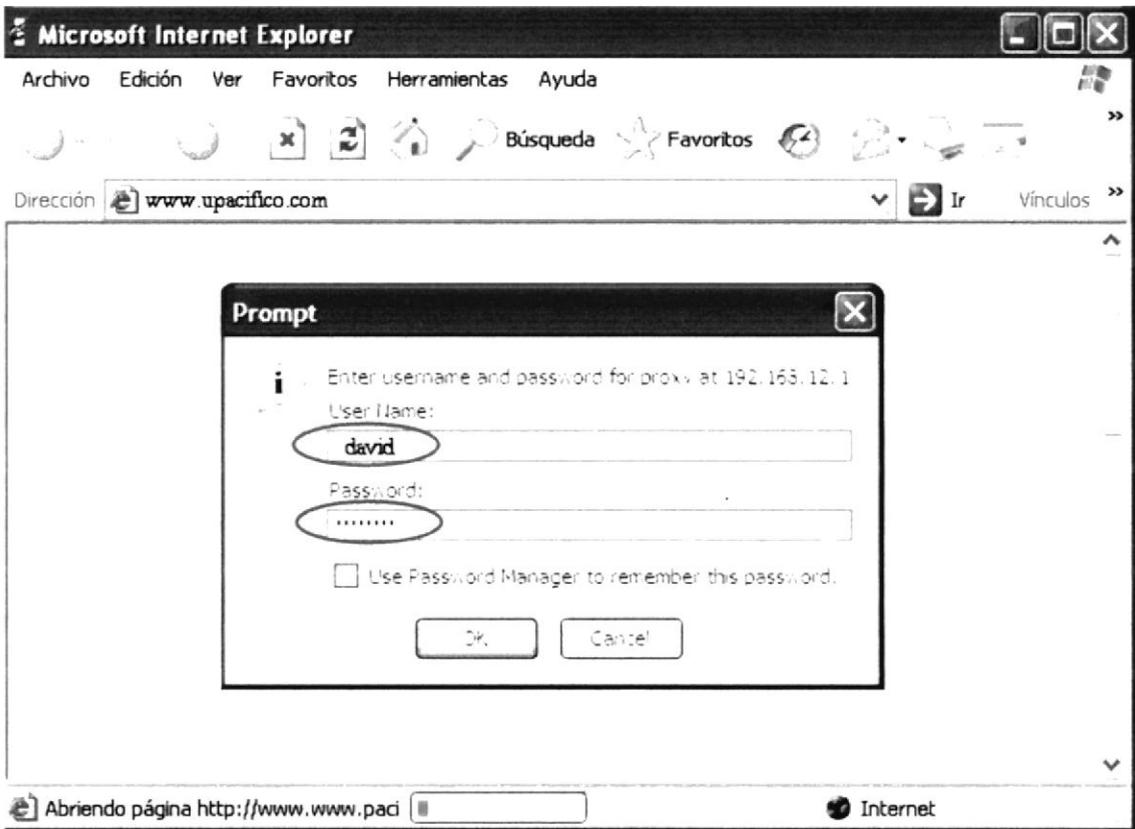


Figura 5-96 Ingreso de Usuario y Password

5.11 SERVIDOR DE CORREO

Sendmail es el agente de transporte de correo más común de Internet en los sistemas Linux. Aunque actúa principalmente como MTA (Mail Transport Agent), que son los encargados de transferir los mail a su correcto destino. Un servidor de correo es una aplicación que nos permite enviar mensajes de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

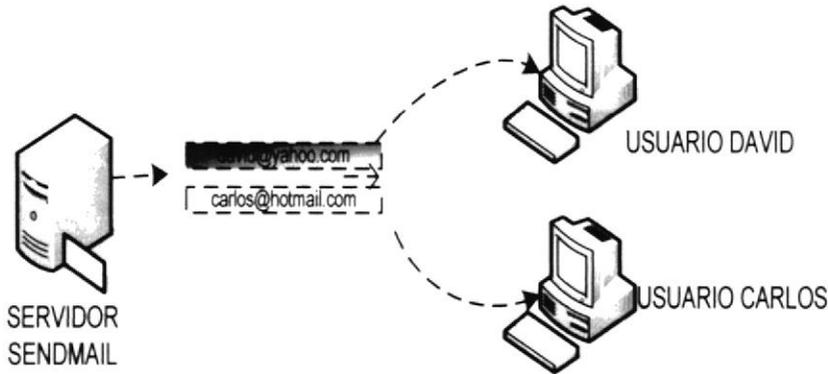


Figura 5-97 Arquitectura de Servidor de Correo

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

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

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

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

5.11.1 REQUERIMIENTOS

- Tener configurada la tarjeta de red tanto en nuestro pc con Linux como en el o los clientes
- Deshabilitar los firewalls en el pc con Linux y en los clientes
- Tener configurado DNS

5.11.2 PRE REQUISITOS

Para poder configurar Servidor de Correo (Send Mail) como pre-requisito se necesitara que su maquina Linux tenga configurado DNS, Web Server, Proxy y la tarjeta de red configurada

Ingresar al Setup y habilitar los servicios de sendmail (dovecot , sendmail)



Editar en el setup dovecot y sendmail



Figura 5-98 Se activa el paquete dovecot

1.-Editar el fichero donde podrá ver si su PC esta en un dominio con la siguiente ruta:



Editar el fichero **vi /etc/hosts**

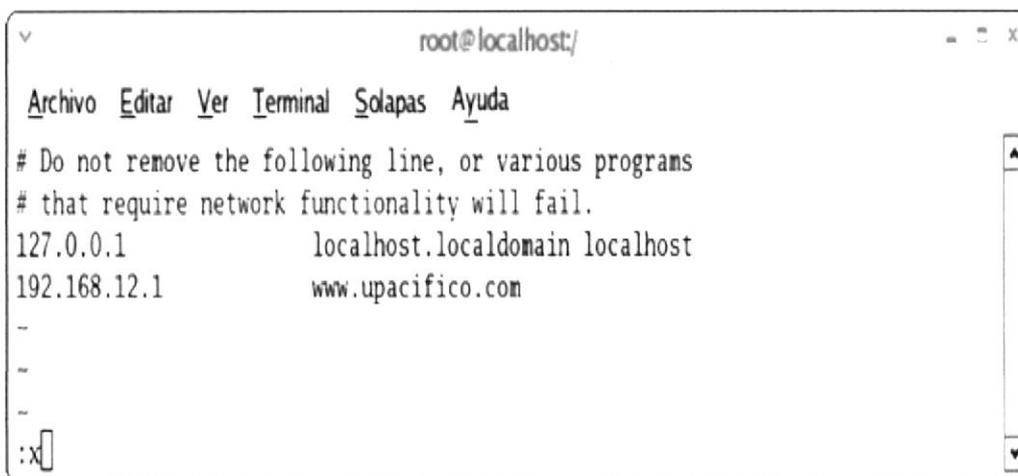


Figura 5-99 Se edita el archivo Host



Edite el fichero vi/etc/mail/sendmail.cf

```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
#D(sendmailMTACluster)$m
localhost
# file containing names of hosts for which we receive email
-- INSERTAR -- 92,1 4%
```

localhost

```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
#D(sendmailMTACluster)$m
cupacifico.com
# file containing names of hosts for which we receive email
-- INSERTAR -- 90,16 4%
```

cupacifico.com

Figura 5-102 Se edita el archivo sendmail.cf



Restauración de servicios de Sendmail “service sendmail restart”

```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /] service sendmail restart
Apagando sendmail: [ OK ]
Desactivación de sn-client: [ OK ]
Iniciando sendmail: [ OK ]
Inicio de sn-client: [ OK ]
[root@localhost /]#
```

Figura 5-103 Se restauran los servicios de SendMail



Editar el fichero vi/etc/dovecot.conf

```

root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Protocols we want to be serving:
# imap imap3 pop3
protocols = imap imap3 pop3

# IP or host address where to listen in for connections. It's not currently
# possible to specify multiple addresses. "*" listens in all IPv4 interfaces.
:x
  
```

Figura 5-104 Se edita el archivo dovecot.conf



Restauración de servicios de dovecot "service dovecot restart"

```

root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost /]# service dovecot restart
Parando Dovecot Imap:           [ OK ]
Iniciando Dovecot Imap:        [ OK ]
[root@localhost /]#
  
```

Figura 5-105 Se restauran los servicios del dovecot

Revise los puertos de descarga.

```
netstat -pelan | grep 110
```

Comprobar los puertos abiertos

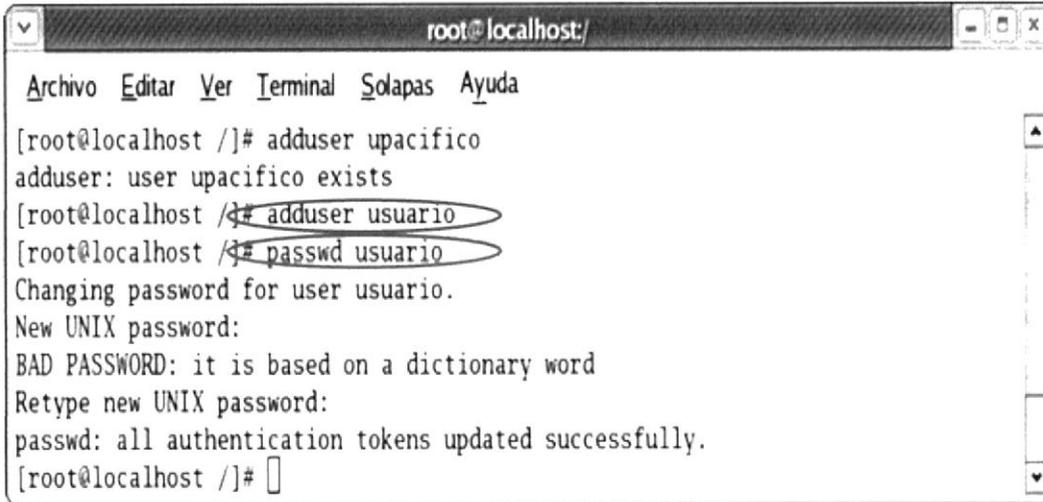
```
Netstat -an | more, o netstat -plan | more
```

Deben estar escuchando los puertos 25 (SMTP) y el 110 (POP3)

5.11.3 CONFIGURACION DE LOS CLIENTES

Creación de los Usuario con su respectiva contraseña.

 Crear los username con sus respectivos password

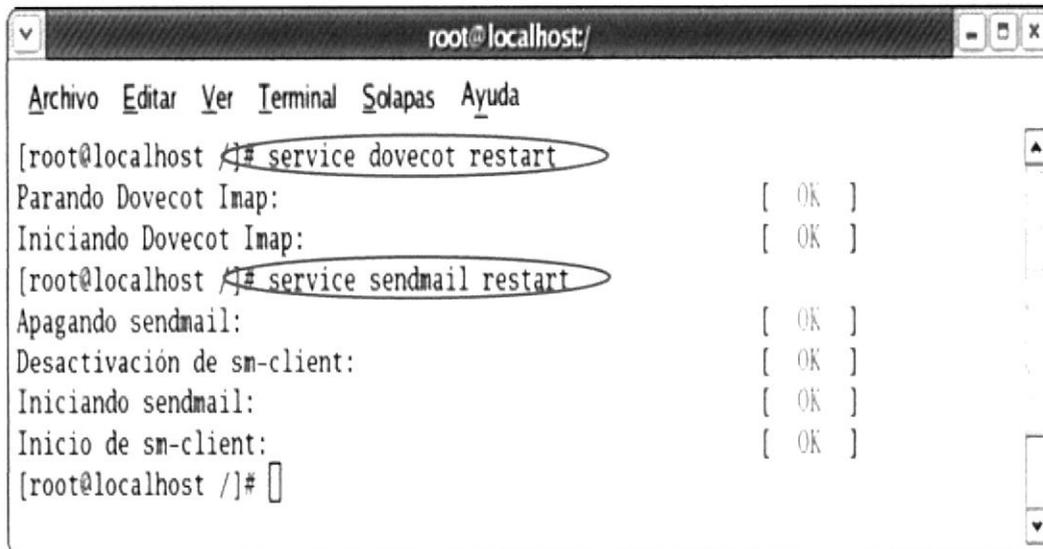


```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# adduser upacifico
adduser: user upacifico exists
[root@localhost ~]# adduser usuario
[root@localhost ~]# passwd usuario
Changing password for user usuario.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word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

Figura 5-106 Se crea el usuario y password

Reinicie los servicios del Dovecot y Sendmail.

 Reiniciar los servicios Dovecot y Sendmail



```
root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# service dovecot restart
Parando Dovecot Inap: [ OK ]
Iniciando Dovecot Inap: [ OK ]
[root@localhost ~]# service sendmail restart
Apagando sendmail: [ OK ]
Desactivación de sm-client: [ OK ]
Iniciando sendmail: [ OK ]
Inicio de sm-client: [ OK ]
[root@localhost ~]#
```

Figura 5-107 Se reinician los servicios del dovecot y sendmail

5.11.4 CONFIGURACION EN LA MAQUINA WINDOWS

1.-Proceder a configurar el Outlook Express, damos clic en inicio y elegimos la pestaña de correo electrónico (Outlook Express)

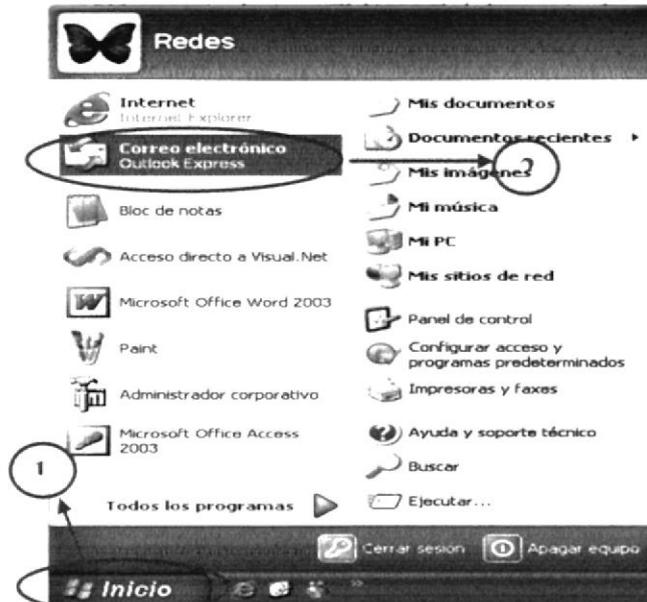


Figura 5-108 Se ingresa el Outlook Express

2.-Se abrirá la pantalla principal del Outlook Express en la cual vamos a empezar la configuración, damos clic en herramientas y seleccionar cuentas de correos como lo detallamos a continuación.

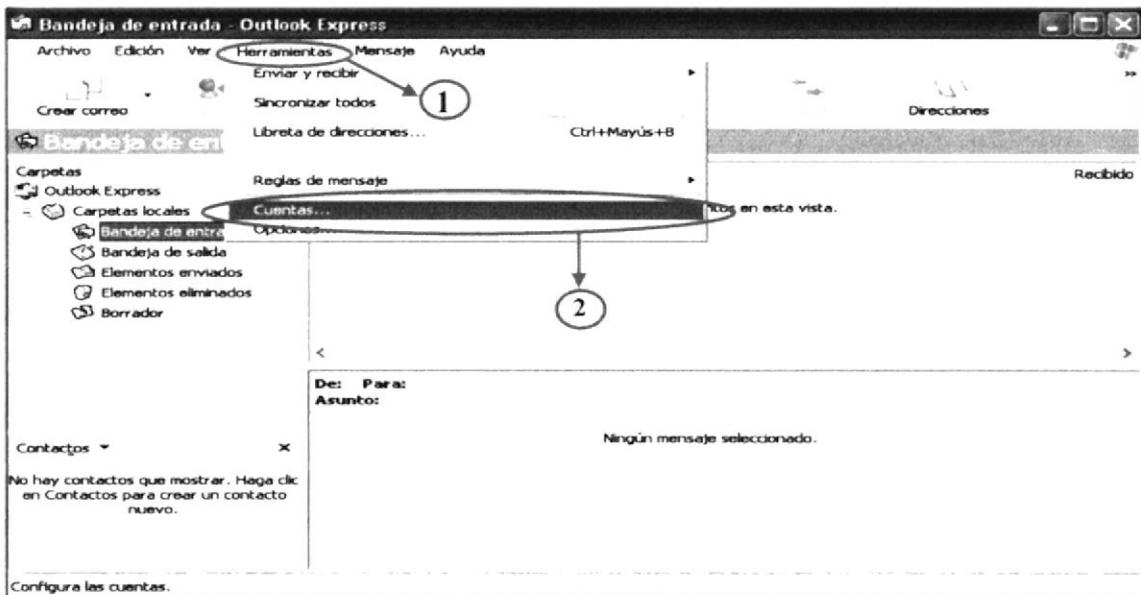


Figura 5-109 Ingreso del Menú Cuentas...

3.-Le aparecerá la siguiente pantalla a manera de un asistente para poder configurar la nueva cuenta de correo electrónico, en la cual da clic en agregar y elija la opción correo

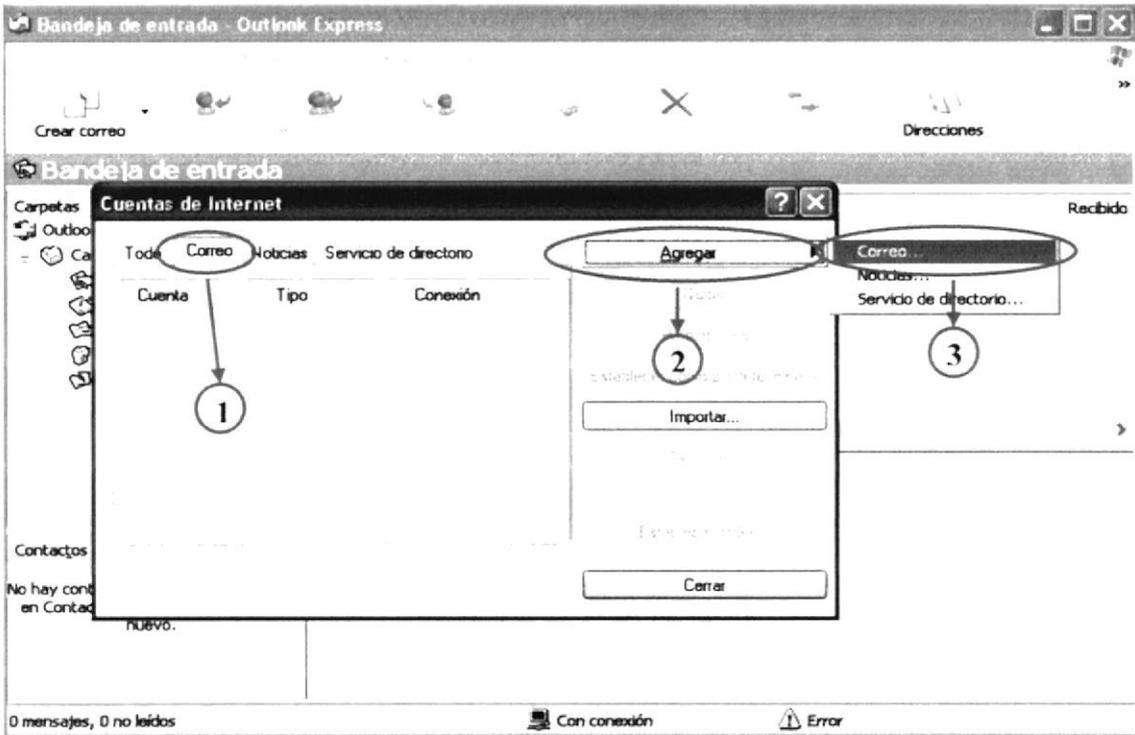


Figura 5-110 Se crea una nueva cuenta

Ahora le aparecerá la pantalla para configurar el nombre que aparecerá en el campo De del mensaje saliente (nombre que el usuario desea)

Luego configurar la dirección del correo (dirección que utilizan las demás personas para poder enviarle mensajes) como detallaremos a continuación



Figura 5-111 Se ingresa el nombre de usuario

A continuación saldrá la pantalla para configurar el servidor del correo electrónico (entrante POP3 y saliente SMTP) en ambas opciones va la dirección de nuestro servidor Linux en este caso 192.168.12.10

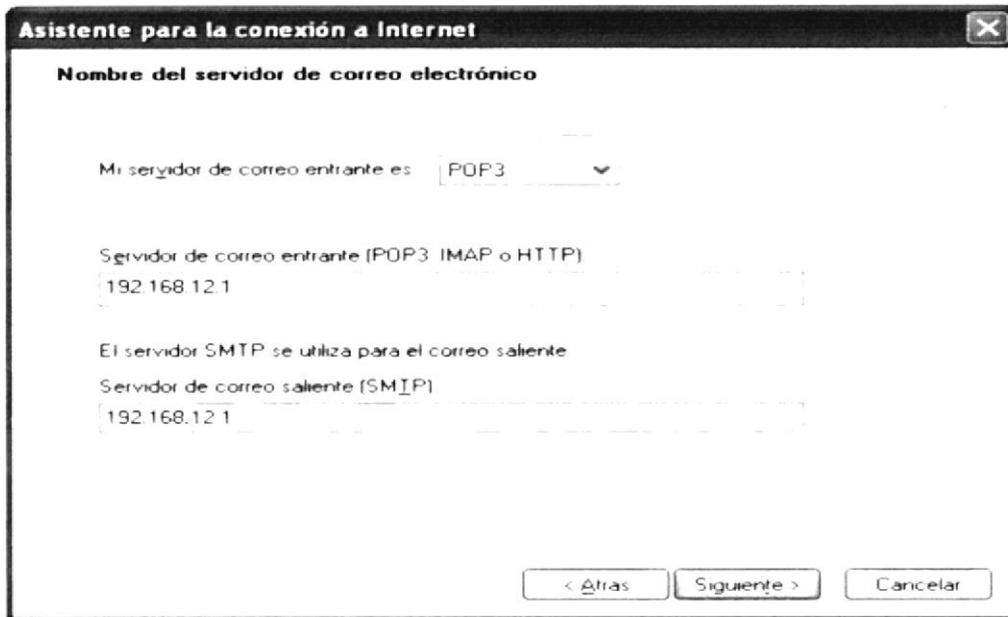


Figura 5-112 Se ingresa la dirección IP del servidor Linux

En esta pantalla configurara el nombre de la cuenta y su respectiva contraseña (para Internet el proveedor le proporciona, en este caso el usuario puede poner la contraseña que le convenga) como detallaremos a continuación

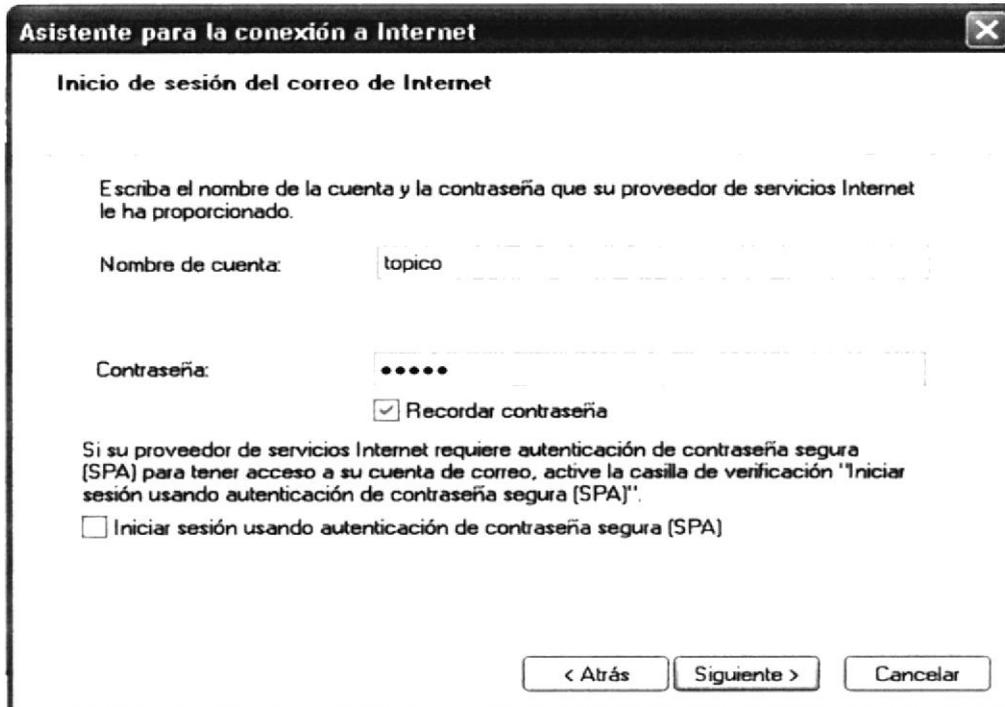


Figura 5-113 Si ingresa el nombre de la cuenta y password

Una vez terminado los anteriores pasos le saldrá la siguiente pantalla donde ponemos finalizar para concluir la configuración del nuestra cuenta de correo

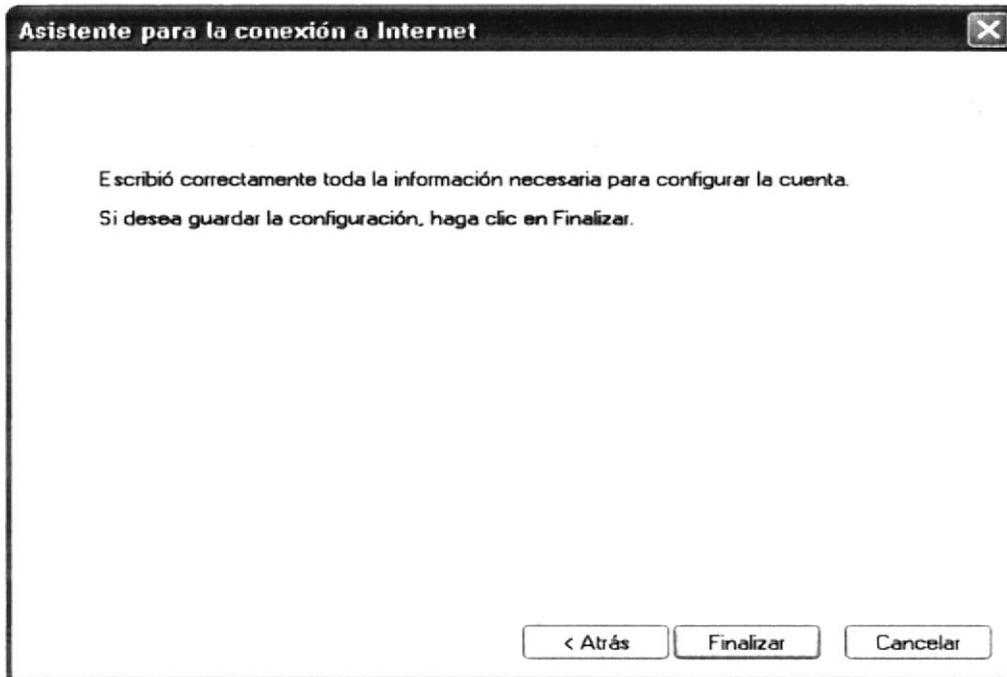


Figura 5-114 Se finaliza para que las configuraciones tengan efecto

Terminada la configuración visualizara una pantalla con las cuentas de correo que existen, a la vez la cuenta que esta como predeterminada en este caso 192.168.12.10 como detallaremos a continuación

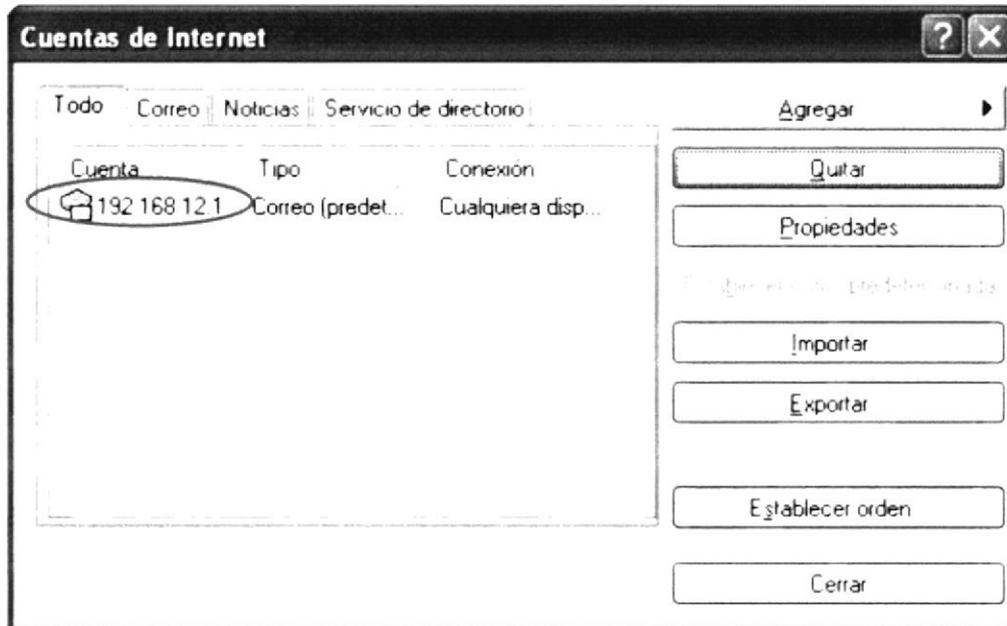


Figura 5-115 Ventana en la que se visualiza todas las cuentas existentes

Ahora podrá enviar y recibir mensajes de correos de los usuarios creados en su servidor Linux como vera a continuación:

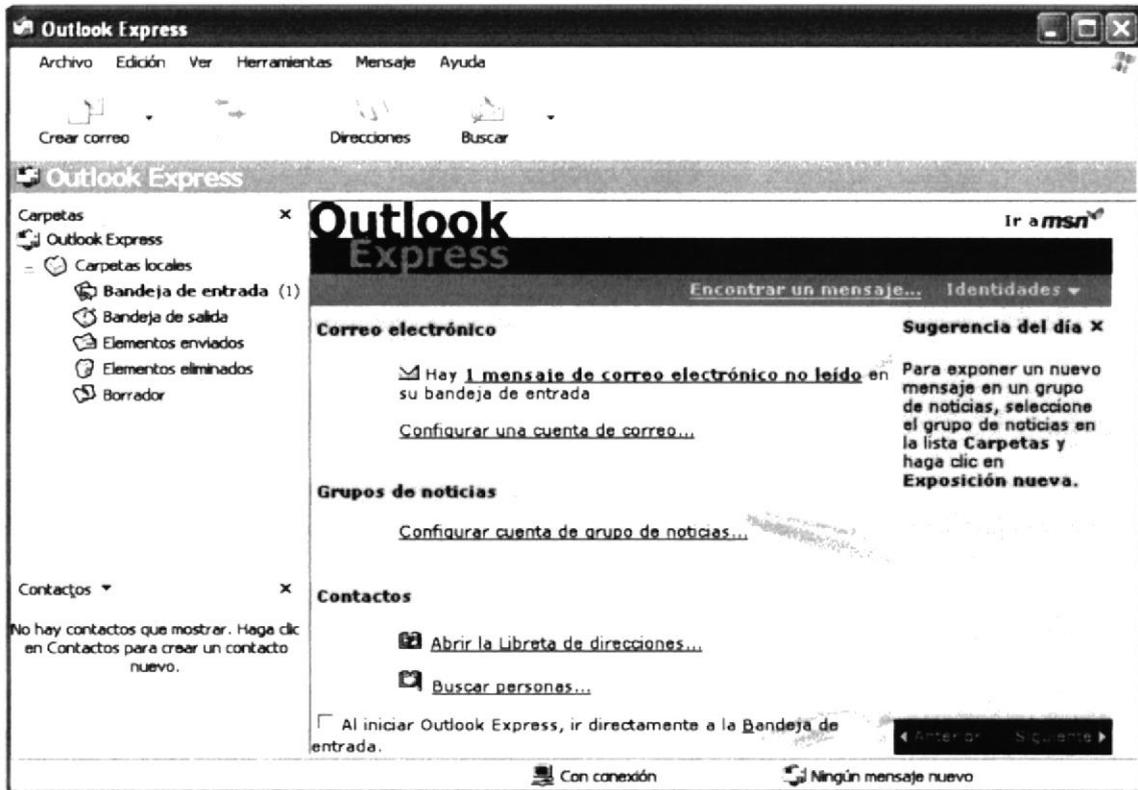


Figura 5-116 Pantalla principal de Outlook Express

Para realizar la prueba de envío y recepción de mensajes de correo en el Outlook Express presione la pestaña enviar y recibir mensajes que esta en la barra de herramientas y nos saldrá una pantalla como se detallara a continuación (busca mensajes que son enviados y recibidos)

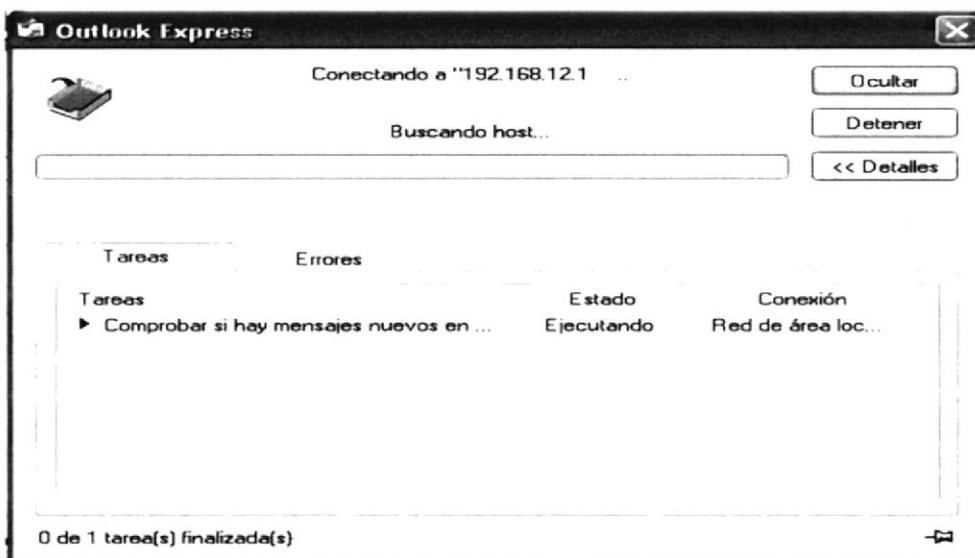


Figura 5-117 Ventana de transferencia de archivos

Recepción de correo en la maquina Windows, revise en la bandeja de entrada

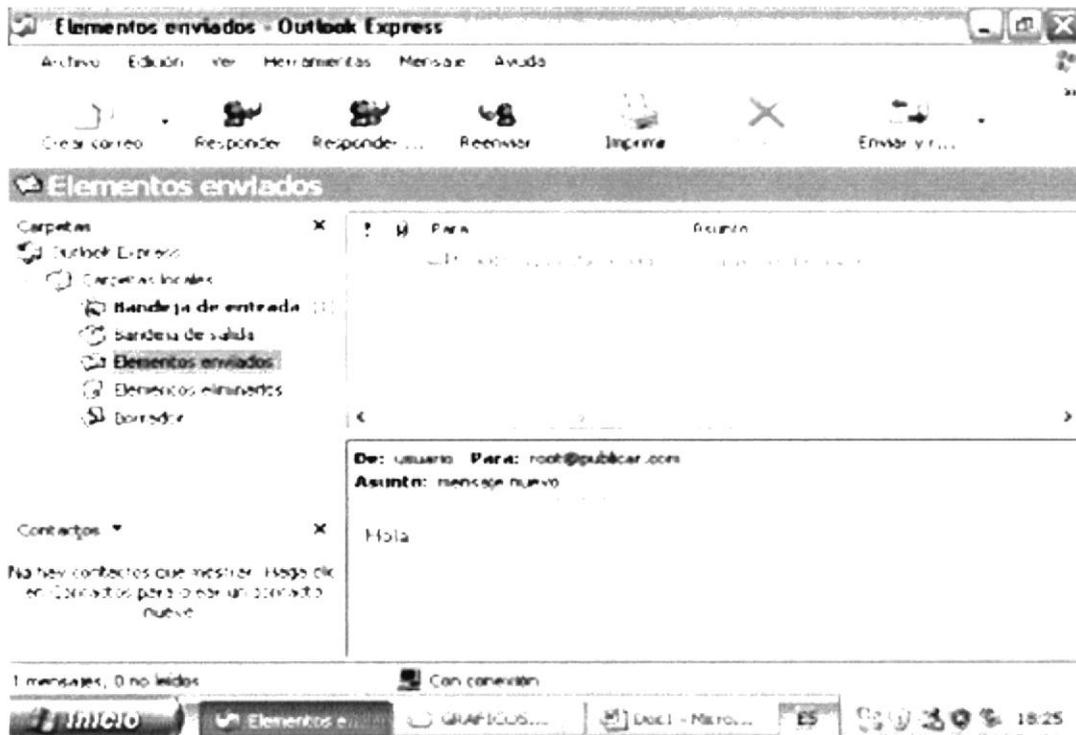


Figura 5-118 Ventana de recepción de correo en Windows

Recepción de correo en la pc_linux, digite Mail --u

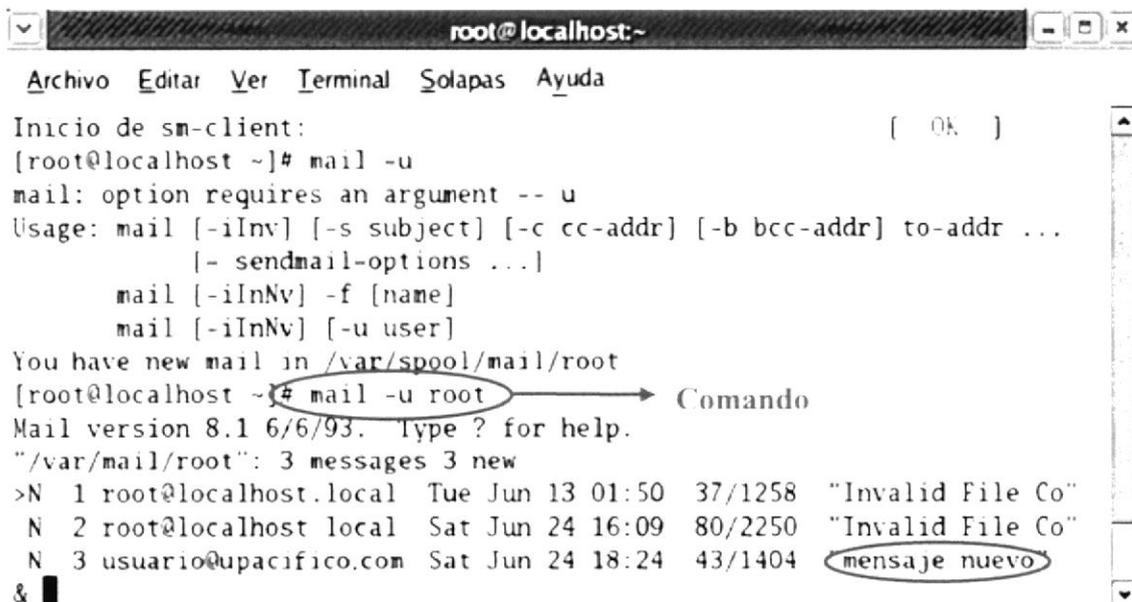


Figura 5-119 Pantalla de recepción de correo en Linux

5.12 DHCP

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

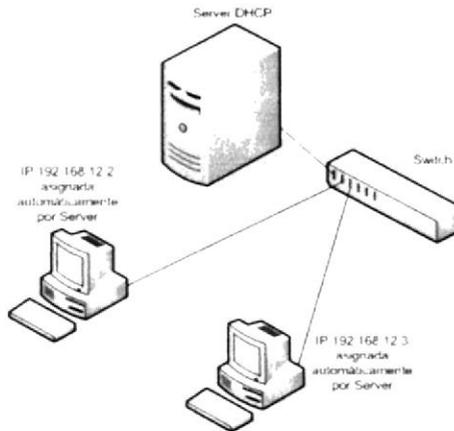


Figura 5-120 Arquitectura de DHCP

5.12.1 REQUERIMIENTOS

- Tener configurada la tarjeta de red tanto en su pc con Linux como en el o los clientes
- Deshabilite los firewalls en el pc con Linux y en los clientes

5.12.2 CONFIGURACION:

Para realizar esta configuración necesita verificar si el paquete dhcpd, esta instalado y se lo hace de la siguiente manera:

```
rpm -q dhcp
```

Una vez verificado que el paquete esta instalado se procederá a crear el archivo dhcpd.conf , y lo haremos de la siguiente manera:

```
cp /usr/share/doc/dhcp-3.01/dhcpd.conf.sample /etc/dhcpd.conf
```

Ahora configure el archivo dhcpd.conf (realice las siguientes modificaciones) el cual ha sido creado en la ruta /etc/dhcpd.conf

```
vi /etc/dhcpd.conf
```

```

root@localhost:/
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# cd /
Subset 192.168.11.0 netmask 255.255.255.0
#---default gateway
Option routers 192.168.11.8
Option subset-mask 255.255.255.0
Option nis-domain "upacifico.com" ;
Option domain-name "upacifico.com" ;
Option domain-name-servers 192.168.12.10
option netbios -name - servers 192.168.12.10;
Range dynamic-bootp 192.168.11.66 192.168.11.80

```

Figura 5-121 Se edita el archivo dhcpd.conf

- ① En esta línea se asigna el segmento de red con su respectiva máscara.
- ② Opcional colocar la línea del gateway
- ③ Digitar la dirección del DNS
- ④ Definir el rango de IP desde - hasta

Salir con esc :wq para guardar los cambios.

Proceda a crear un archivo en la ruta que dará a continuación, en este archivo se almacenaran las direcciones ip de las maquinas que tendrá en su servicio DHCP

Touch /var/lib/dhcp/dhcpd.leases

Para añadir dhcp al arranque del sistema, ejecute:

chconfig dhcpd on

pgrep dhcp

Restaurar el servicio del dhcpd
service dhcpd restart

5.12.3 EN WINDOWS:

Realice lo siguiente:

Como lo dijimos anteriormente hay varias maneras de acceder a mis sitios de red, el icono esta en el escritorio pero en caso de no estar tiene muchas mas opciones, la que mas se usa es: clic derecho en botón inicio, busque explorar y lo llevara a esta pantalla en la cual esta mis sitio de red, le damos clic derecho y elija propiedades

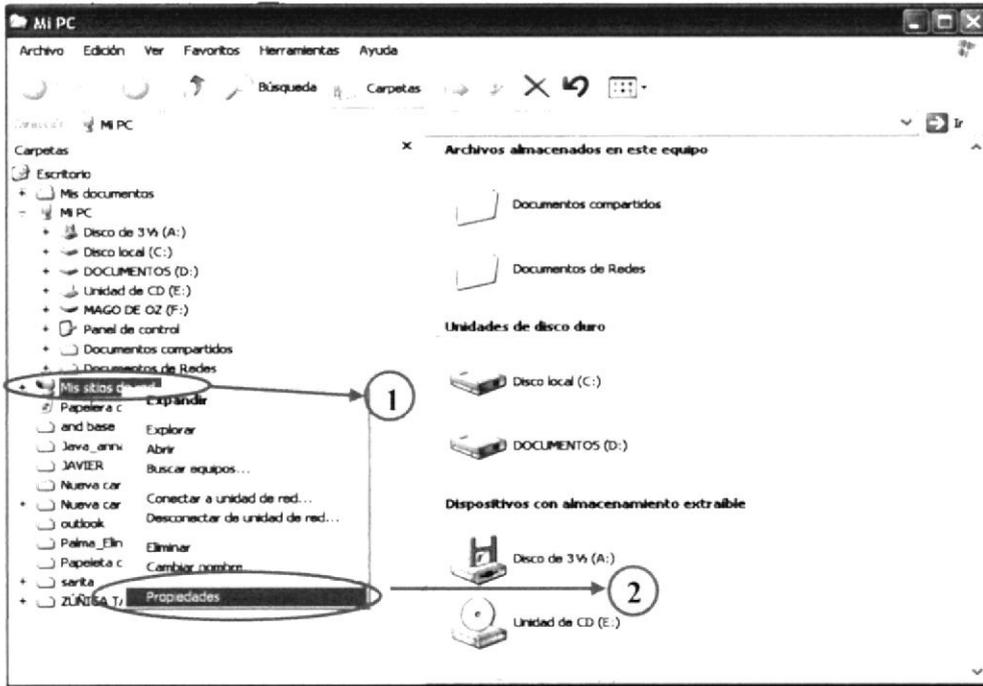


Figura 5-122 Se ingresa a las propiedades de mis sitios de red

A continuación vera la pantalla de conexiones de red, le damos clic derecho al icono de conexiones de área local y elija propiedades

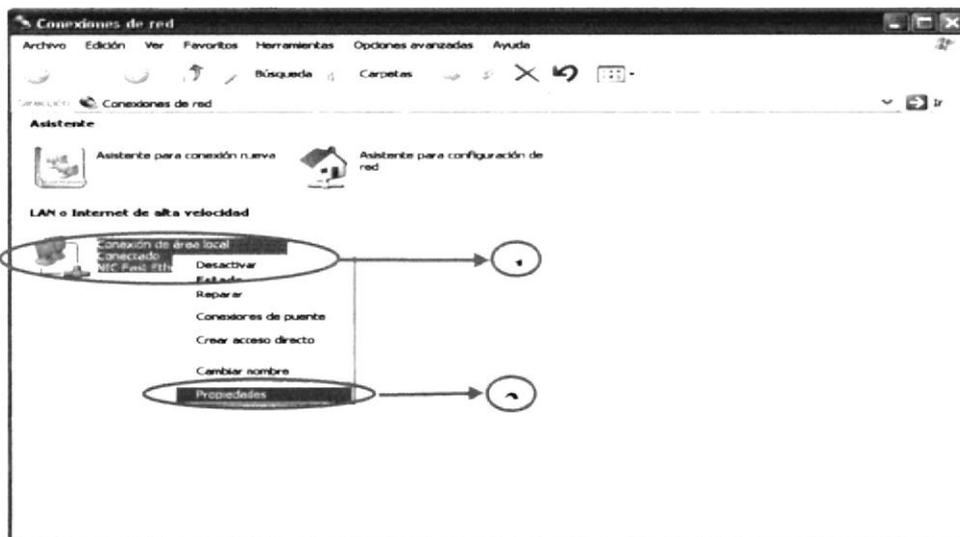


Figura 5-123 Se ingresa a las propiedades de Conexión de área local

Luego verá la pantalla de propiedades de conexión de área local, 1 le damos clic a protocolo Internet (TCP/IP), 2 clic en propiedades

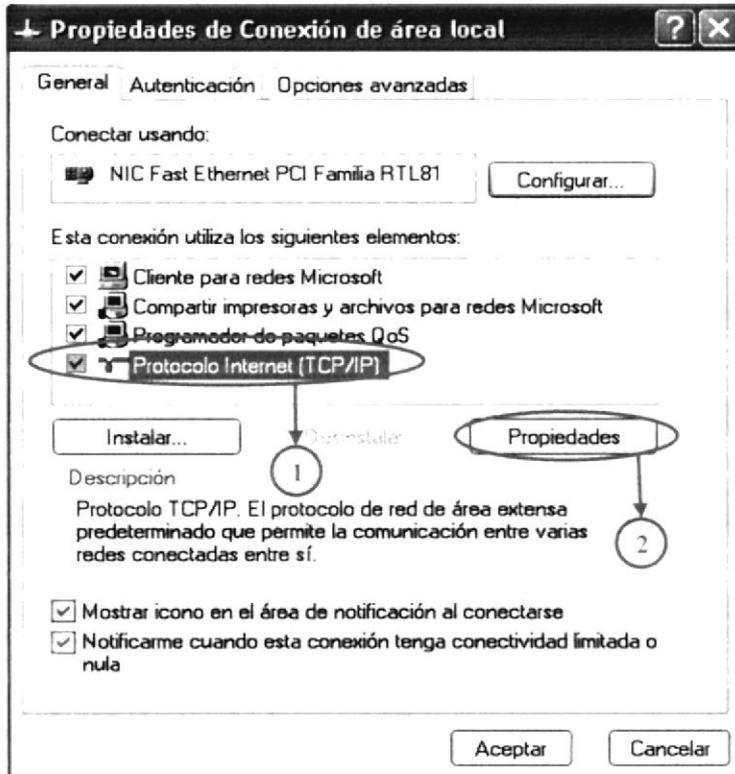


Figura 5-124 Se ingresa a las propiedades del Protocolo Internet

Configurar su tarjeta de red de manera dinámica, en este caso pondremos las opciones obtener una dirección IP automáticamente y obtener la dirección del servidor DNS automáticamente como lo detallara a continuación

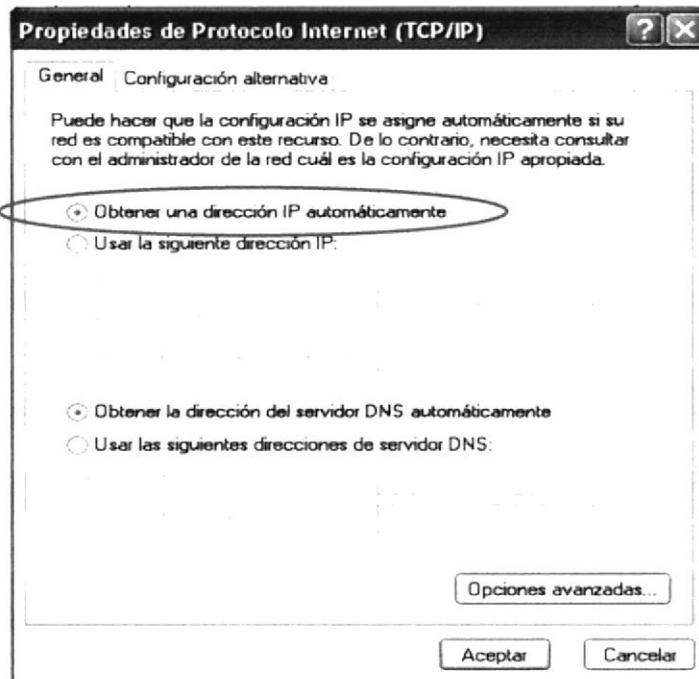


Figura 5-125 Se selecciona Obtener dirección IP automática

En el Símbolo de Sistema digite el comando ipconfig / all

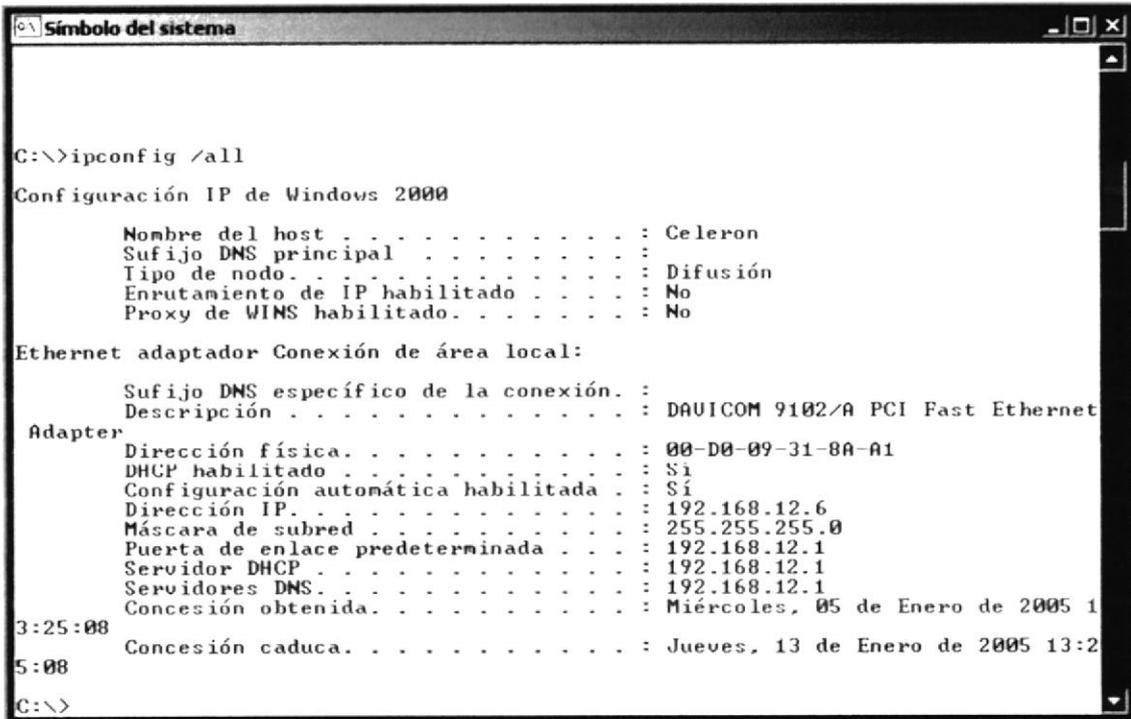


Figura 5-126 Se verifican las direcciones IP

5.13 FIREWALL

El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. Es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/.../IP y decide si un paquete pasa, se modifica, se convierte o se descarta.

Un firewall es un dispositivo que filtra el tráfico entre redes

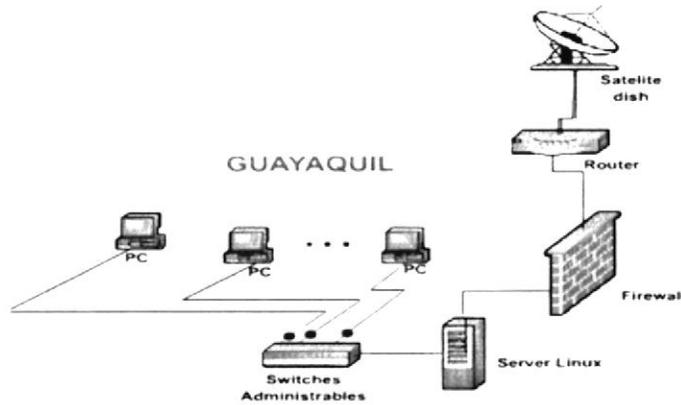


Figura 5-127 Arquitectura de Firewall

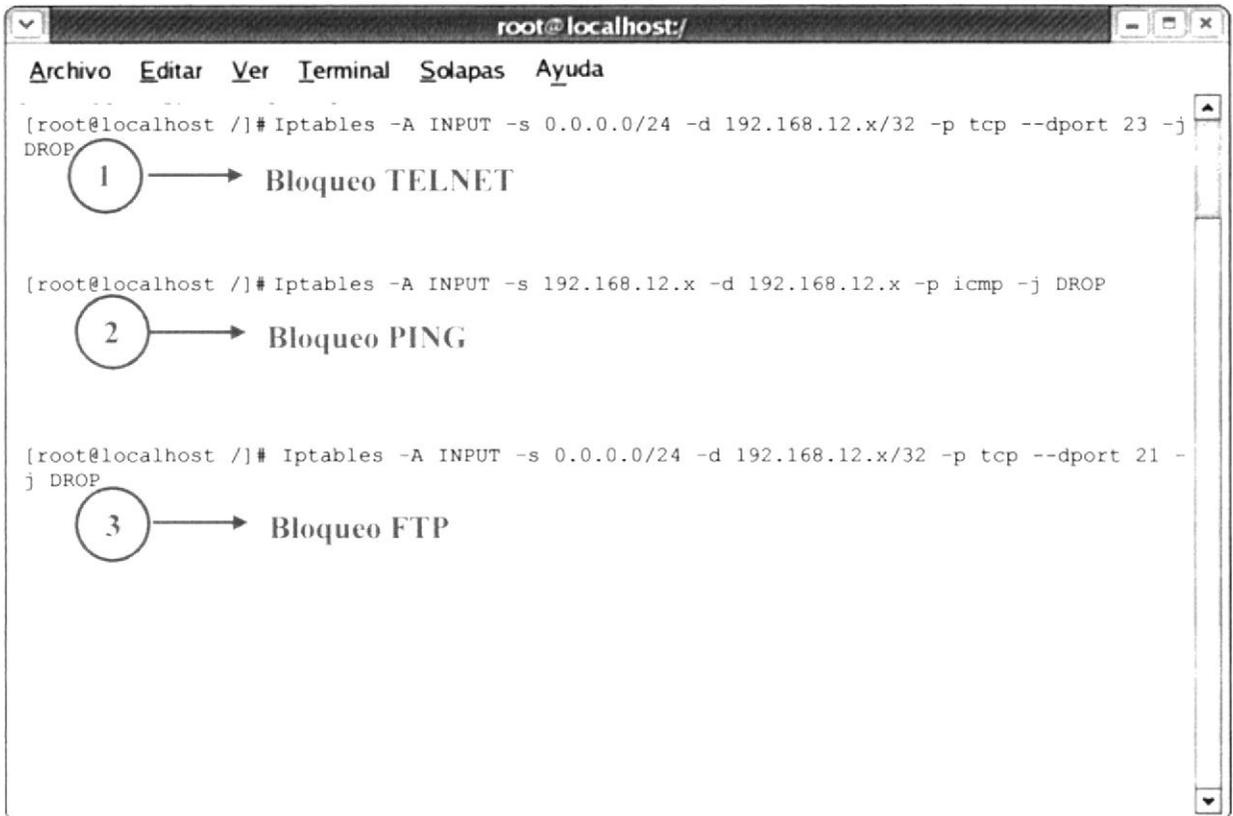


Figura 5-128 Pantalla de bloqueo de servicios

5.13.1 ORDENES BASICAS:

Iptables -F : Borrado de reglas

Iptables -L : Listado de reglas que se están aplicando

Iptables -A : Append, añadir regla

Iptables -D : Borrar una regla



ANEXO

APENDICE A



APENDICE A

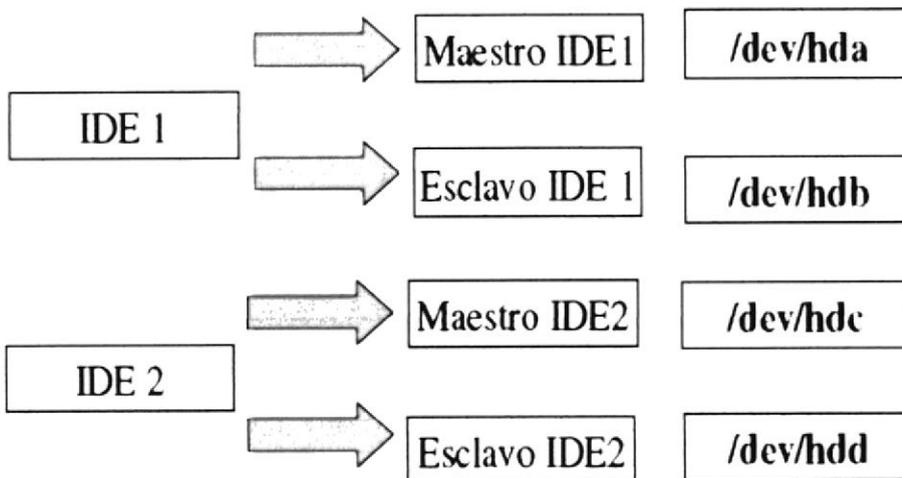
Convenciones para nombrar disco y particiones en GNU/Linux

GNU/Linux posee una forma distinta y más ordenada de nombrar discos rígidos y particiones que en Windows. Las ventajas de manejar particiones o “discos virtuales” dentro de su disco duro son:

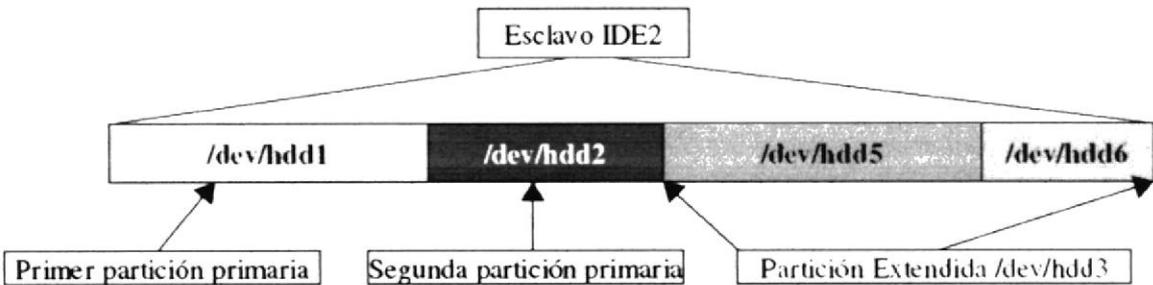
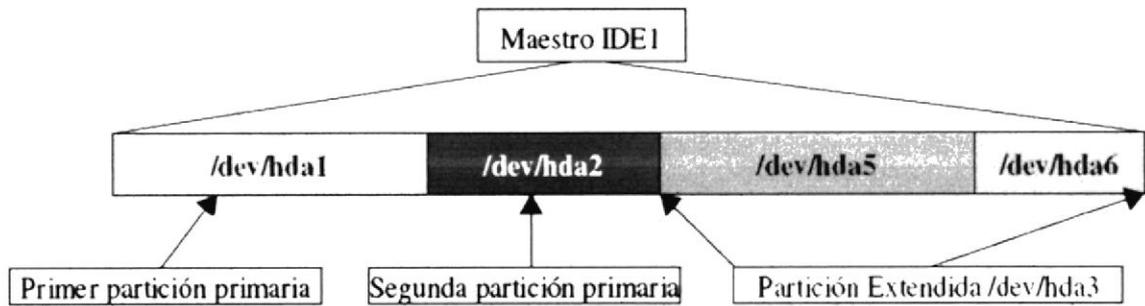
- Tener distintos sistemas operativos ya ellos poseen distintos sistemas de archivo, por ejemplo. Windows ocupa Fat y NTFS en cambio GNU/Linux ocupa ext3, ext2(caducado), reiserfs, xfs.
- Por razones de desempeño un único sistema operativo puede preferir unidades distintas que contengan sistemas de archivos distintos, por ejemplo GNU/Linux utiliza una segunda partición llamada Swap que se usa como memoria virtual.
- Por seguridad de respaldar sus datos ante cualquier imprevisto. Mantener una partición solo para sus datos y archivos que Ud. haya generado aparte de los archivos de sistema de su sistema operativo.
- Los errores físicos de un disco duro generalmente se ubican en sectores adyacentes, por lo tanto al distribuir sus datos en distintas particiones limitará las perdidas de datos en caso de daños físicos en su disco duro.

La estructura de nombrar los discos y particiones es la siguiente:

En su placa madre (Motherboard) UD posee generalmente 2 interfaces IDE y por cada una de ellas UD puede colocar como máximo 2 dispositivos uno maestro y uno esclavo entonces de esta forma la estructura de nombramiento es la siguiente independiente si es disco duro o unidades de cd rom:



Si su computador posee otras interfaces IDE los dispositivos se denominaran /dev/hde, /dev/hdf, etc, los discos SCSI se denominan /dev/sda, /dev/sdb, etc, en cuanto a su dispositivo de diskette de denomina /dev/fd0. Para las particiones un disco duro solo puede tener 4 particiones “Primarias”(o extendidas) y 64 particiones lógicas. Las particiones primarias son aquellas en las cuales UD puede albergas sistemas operativos y grupos de particiones lógicas. En el caso de las particiones la convención es la siguiente: particiones primarias o extendidas(para el maestro IDE 1) /dev/hda1 a /dev/hda4, en cuanto a las particiones lógicas /dev/hda5, /dev/hda6, /dev/hda7, etc dependiendo del orden de las particiones lógicas, para entender mejor el concepto vea la siguientes figuras:





ANEXO

APENDICE B

APENDICE B

Sistemas de Archivos

El sistema de archivos de GNU/Linux

Al igual que Windows con sistemas de archivos FAT, FAT32 y NTFS, GNU/Linux posee sistemas de archivos aquí se explicará algunos de ellos:

Ext2FS(Second Extended File system)

Fue el estándar de GNU/Linux por muchos años es el reemplazo del Sistema de archivos extendido (Extended FileSystem). Aunque ya en la actualidad ya no es muy frecuente.

Ext3(Third Extended File System)

Es el sucesor de Ext2FS es compatible con este último aunque con algunas mejoras, Las transacciones. Una de las fallas de los sistemas de archivos tradicionales como Ext2FS es la baja tolerancia a caídas del sistemas en forma abrupta (fallas de energía o programas que se cuelgan) y para tales eventos implican un examen prolongados de la estructura del sistema de archivo.

Las transacciones para simplificar es la grabación de las acciones antes de llevarlas a cabo en forma efectiva. El resultado es un sistema de archivos coherente siempre y si ocurren problemas su verificación es mucho mas rápida.

ReiserFS

Es un sistema de archivo que se creo desde cero y también es un sistema Transaccional.

JFS

Es un sistema de archivo tradicional y diseñado por IBM, su estructura interna es muy parecida a la ReiserFS.

	EXT2FS	EXT3	REISERFS	JFS
Estabilidad	Excelente	Buena	Buena	Mediana
Herramienta para recupera archivos borrados	Sí (complejas)	Sí (complejas)	No	No
Tiempo de re-arranque después de una caída	Largo	Corto	Muy corto	Muy corto
Cantidad de datos después de una caída	Bueno, pero con alto riesgo de perdidas	N/D	Muy buena	Muy buena



ANEXO

GLOSARIO



GLOSARIO

G

Gnu: Gnu is Not Unix. Proyecto de la FSF (Free Software Foundation) para crear un sistema UNIX libre.

GNU/Linux: Sistema operativo compuesto de las herramientas GNU de la FSF y el núcleo desarrollado por Linus Torvalds y sus colaboradores.

GPL: General Public License. Una de las mejores aportaciones de la FSF. Es una licencia que protege la creación y distribución de software libre.

P

Partición: La partición de un disco, como su propio nombre indica es un fraccionamiento lógico (que se utilizan programas para hacerlo, no físico) donde se puede guardar información, o son requeridas dependiendo del S.O. Utilizado.

R

Root: Superusuario. Es el administrador del sistema, con todos los derechos sobre el mismo. Es el único usuario con permiso sobre el sistema, **TENGA MUCHO CUIDADO SI VA INGRESAR COMO TAL.**(Procura sus accesos los menos posibles..., crear usuarios, borrarlos, montar unidades...)

S

Swap :El *Espacio swap* en Linux, como en otros sistemas operativos, es usado cuando la cantidad de memoria física (RAM) está llena. Si el sistema necesita más recursos de memoria y la memoria física está llena, las páginas inactivas de la memoria se mueven al espacio swap. Mientras que el espacio swap puede ser de ayuda para las máquinas con poca memoria RAM, no debería considerarse como algo que pueda sustituir a más RAM. El espacio Swap se encuentra en discos duros, que tienen un tiempo de acceso más lento que la memoria física.

El espacio Swap puede ser una partición swap dedicada (recomendable), un archivo swap o una combinación de particiones y archivos swap.

El tamaño de su espacio swap debería ser igual o dos veces mayor que la memoria RAM de su ordenador, o 32 MB, la cantidad que sea más grande de estas dos, pero no más de 2048 MB (o 2 GB).

A contrario de GNU/Linux Ud. en MS Windows encontrará seguramente un archivo win386.swp que aumentara o disminuirá de tamaño dependiendo de la cantidad de trabajo que realiza el computador y que cumple la misma función que la partición Swap.