ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Escuela de Diseño y Comunicación Visual

TÓPICO DE GRADUACIÓN

Previo a la obtención del título de:

Analista de Soporte de Microcomputadores

Tema:

Administración y Seguridades de Redes Banco del Pacífico

MANUAL DE USUARIO Y CONFIGURACIONES

Autores:

Enzo Carrera

Ronald Soriano

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:

ANALISTA DE SOPORTE DE MICROCOMPUTADORAS

TEMA

ADMINISTRACIÓN Y SEGURIDADES DE REDES
BANCO DEL PACÍFICO

MANUAL DE USUARIO Y CONFIGURACIONES

AUTORES

ENZO CARRERA
RONALD SORIANO

DIRECTOR

ANL. FABIÁN BARBOZA

AÑO

2006

AGRADECIMIENTO

Queremos agradecer principalmente a Dios por darnos la sabiduría y a todas las personas que nos han ayudado a culminar nuestros objetivos: nuestros padres, profesores y amigos; ya que sin ustedes no hubiéramos podido lograrlo.

DEDICATORIA

Este trabajo va dedicado a mis padres todas las personas que nos han acompañado como son nuestros padres y hermanos que siempre han estado al tanto de la carrera y nos han apoyado en todo momento.

DECLARACIÓN EXPRESA

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

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

FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN

Arq. Fabián Barboza

FIRMA DE LOS AUTORES DEL TÓPICO DE GRADUACIÓN

Enzo Carrera Espinoza.

Ronald Soriano Bernabé

TABLA DE CONTENIDO

CAPÍTULO 1.
GENERALIDADES

CAPÍTULO 2.
SITUACIÓN ACTUAL

CAPÍTULO 3.
PROPUESTA

CAPÍTULO 4.
IMPLEMENTACIÓN DE CABLEADO

CAPÍTULO 5.
CONFIGURACIÓN DE DISPOSITIVOS

CAPÍTULO 6.
LINUX FEDORA CORE 3

TABLA DE ILUSTRACIONES

CAPÍTULO 2.- SITUACIÓN ACTUAL

CAPÍTULO 3.- PROPUESTA

CAPÍTULO 4.- IMPLEMENTACIÓN DE CABLEADO

CAPÍTULO 5.- CONFIGURACIÓN DE DISPOSITIVOS

CAPÍTULO 6.- LINUX FEDORA CORE 3

ÍNDICE DE TABLAS

CAPÍTULO 3.- PROPUESTA

CAPÍTULO 1

GENERALIDADES

1. GENERALIDADES

1.1 INTRODUCCIÓN

Este manual es una guía detallada de configuraciones básicas para configurar routers, switches, levantar un Proxy, Servidor de Correo, de Ficheros, y comandos básicos de LINUX.

Lo único que debes hacer es seguir paso a paso cada una de las indicaciones detalladas en este manual, que esperamos sea de ayuda para ti.

1.2 OBJETIVO DEL MANUAL

El objetivo del manual es servir de guía y consulta a los Administradores de Red, y a todos los relacionados en esta área.

1.3 ¿A QUIEN VA DIRIGIDO?

Este manual va dirigido al área de sistemas del Banco del Pacífico el mismo que servirá para ilustrar una mejor manera de administrar y dar soporte a las redes LAN y WAN de la empresa.

1.4 ¿LO QUE SE DEBE CONOCER?

El manual se ha elaborado con el objetivo de que un Administrador de redes pueda tener una guía para la correcta organización de la red, a la cual está a su cargo además de ayudar a las personas del área de redes en aspecto de configuraciones de servidores de red como dispositivos de comunicación a nivel LAN como WAN, se debe tener en cuenta que si se desea lograr un mejor rendimiento del mismo el usuario final tiene que conocer definiciones básicas de redes.

1.5 ORGANIZACIÓN DE ESTE MANUAL

Este manual esta dividido en 6 capítulos los cuales:

CAPÍTULO 1 GENERALIDADES

CAPÍTULO 2 SITUACIÓN ACTUAL

En este capítulo se detallará sobre la situación actual de la red de la empresa de una manera general.

CAPÍTULO 3 PROPUESTA

En este capítulo se detallará de las alternativas de solución para la empresa en aspecto de redes.

CAPÍTULO 4 IMPLEMENTACIÓN DE CABLEADO

En este capítulo se detallará la forma correcta para cablear un edificio.

CAPÍTULO 5 CONFIGURACIÓN DE DISPOSITIVOS

En este capítulo se detallará la configuración paso a paso de dispositivos como router y switches.

CAPÍTULO 6 LINUX FEDORA CORE 3

En este capítulo se detallará las configuraciones básicas de Linux como también las configuraciones de servidores.

CAPÍTULO 2

SITUACIÓN ACTUAL

2. SITUACIÓN ACTUAL

2.1 ANTECEDENTES

EL BANCO DEL PACÍFICO desde el 10 de octubre del 2000 somos el Nuevo Banco del Pacífico, institución flexible y moderna que hoy se proyecta con renovado optimismo hacia el futuro. Nuestra solidez y solvencia nos ubican como uno de los lideres de la banca ecuatoriana.

Contamos con una gran cobertura nacional, pues estamos presentes en 11 provincias, 28 cantones con 103 puntos de atención, 8 CIN (Centro Integral de Negocios) Principales, 56 CIN, 37 ventanillas, 2 autobancos y 161 cajeros Bancomáticos. Internacionalmente estamos al servicio de nuestros clientes en Miami y Panamá.

Actualmente somos manejados por una administración internacional, la misma que está especializada en el diseño e implementación de programas de asesoramiento al sector financiero. En especial, esta firma ofrece sus servicios de banca de inversión a reconocidas instituciones a nivel mundial.

La administración internacional tiene la finalidad de devolver con éxito nuestra institución a manos privadas. Mientras, hacemos lo que mejor sabemos: Servirle a usted con mayor eficiencia, poniendo una gama de productos y servicios a su completo alcance, reconociendo diariamente nuestro compromiso de trabajo con usted y el Ecuador.

2.2 MISIÓN Y VISIÓN

MISIÓN

Contribuir al desarrollo del país, mediante la oferta de servicios financieros de calidad; el compromiso ético y la excelencia; y el recurso humano capaz y motivado.

VISIÓN

Ser una organización rentable, flexible y moderna, líder en servicios financieros de calidad, basados en prácticas éticas y estándares internacionales de eficiencia.

VALORES

Nuestra reconocida cultura organizacional, tiene como base un conjunto de valores que identifican plenamente a cada uno de quienes conformamos el Nuevo Banco del Pacífico. Estos son:

- **El respeto a la persona humana**, que implica el reconocimiento objetivo de las capacidades propias y las de los demás para la realización de la tarea colectiva del Banco.
- **La honestidad** que se manifiesta en comportamientos de integridad y madurez que generan sentimientos de confianza en nuestros clientes, empleados y en la comunidad.
- **La excelencia en el servicio** se refiere a la orientación de nuestras acciones hacia la satisfacción del cliente mediante una cultura de servicio, asentada en la atención amable, oportuna y eficiente.
- **El mejoramiento continuo**, referido a la permanente adquisición de nuevos conocimientos y habilidades que permitan generar un valor agregado para los clientes y la Organización.
- **El trabajo en equipo o gestión participativa**, que permita a los empleados intervenir activamente en la vida de la organización, contribuyendo al logro de los objetivos institucionales.
- **La responsabilidad por los actos propios**, que promueva el ejercicio de acciones y decisiones maduras y nos lleve a asumir como propio el resultado de las mismas. Se refiere también a tomar una posición activa y responsable en las situaciones que requieran nuestra participación.

2.4 DISPOSITIVOS DE COMUNICACIÓN

2.4.1 DISPOSITIVOS DE RUTEO

2.4.1.1 ROUTER CISCO 7500

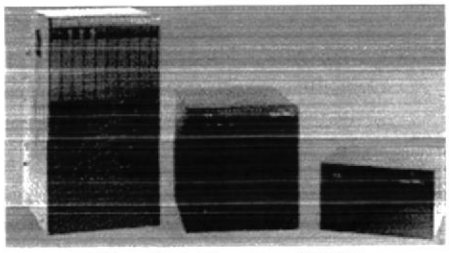

Fig. 2.1 Router 7500

ESPECIFICACIONES DEL EQUIPO

- La Serie Cisco 7500 es un router basado en un chasis que ha sido diseñado para ofrecer múltiples servicios, diversas interfaces y confiabilidad.
- La Serie Cisco 7500 del Procesador de Ruta Conmutada 16 (RSP 16) y el Procesador de Interfaz Versátil 6-80 (VIP- 6-80)
- Ofrece el mejor desempeño sobre una extensa gama de características de distribución para empresas y proveedores de servicio que necesitan alto rendimiento, interfaces de alta velocidad y aplicaciones.
- Los actuales clientes podrán ser capaces de aprovechar inmediatamente su base instalada de routers Serie 7500 y sus adaptadores de puerto utilizando el nuevo RSP16 y el VIP6-80 para conseguir escalabilidad y desempeño adicional en instalaciones ya existentes
- Admite interfaces dobles E1, T1 y PRI
- Admite un máximo de 60 llamadas de módem o de ISDN (RDSI).
- Equipado con dos puertos 10/100 Ethernet autosensing que son perfectos para redundancia y aplicaciones con firewalls.
- Dos puertos series de alta velocidad para poder dar servicios mediante lineas Frame Relay, PPP y HDLC.

2.4.1.2 ROUTER CISCO 2600

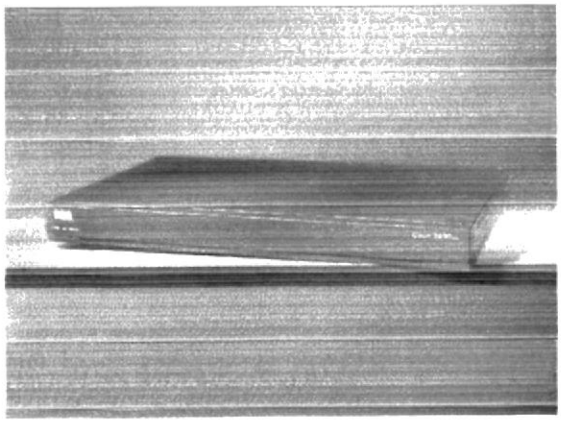

Fig. 2.2 Router 2600

ESPECIFICACIONES DEL EQUIPO

- La arquitectura modular de la serie Cisco 2600 permite actualizar los interfaces para ajustarlos a la expansión de la red o a los cambios tecnológicos que se producen cuando se instalan nuevos servicios y aplicaciones.
- Mediante la integración de las funciones de los distintos dispositivos independientes en una sola unidad compacta, la serie Cisco 2600 reduce la complejidad de gestionar la solución para redes remotas.
- Todos los modelos también tienen dos ranuras para tarjetas de interfaz WAN (WIC), una ranura para el módulo de red y una ranura para un módulo de integración avanzada (AIM).
- Esta serie comparte las interfaces modulares con las series Cisco 1600, 1700 y 3600, ofreciendo una solución rentable para satisfacer las necesidades actuales de las oficinas remotas.
- La serie Cisco 2600 refuerza el compromiso de Cisco para incorporar capacidades de integración multiservicio de voz y datos, lo que permite a los administradores de red ahorrar costos de llamadas entre oficinas que se encuentran a mucha distancia y habilitar futuras aplicaciones de activación por voz tales como la mensajería integrada y los centros de llamadas basados en Web.
- Utilizando los módulos de voz/fax, el router Cisco 2600 puede instalarse en redes de Voz sobre IP (VoIP) y Voz sobre Frame Relay (VoFR).

2.4.2 DISPOSITIVOS DE CONMUTACIÓN

2.4.2.1 HUB 3COM BASE LINE DUAL SPEED DE 48 PUERTOS

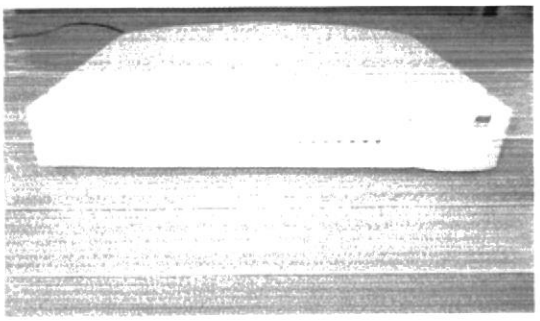

Fig. 2.3 Hub

ESPECIFICACIONES DEL EQUIPO

- Puertos LAN: 48 puertos 10BASE-T/100BASE-TX con auto-detección
- Interfaz de medios: RJ-45 Ethernet
- Indicadores LED: Potencia, tráfico de red, colisiones, segmento LAN
- Soporte de Protocolo y Funciones: ISO 8802-3, IEEE 802.3 (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.1d (puenteado)
- Direcciones MAC: 4,000
- Certificaciones de seguridad: UL 1950, EN 609 50, CSA 22.2 #950, IEC 60950
- Certificaciones de emisiones: EN 55022 Clase A, FCC Parte 15 Sub parte B Clase A, ICES-003 Clase A, VCCI Clase A, AS/NZS 3548 Clase A, CNS 13438 Clase A
- Certificaciones de inmunidades: EN 55024
- Especificaciones ambientales: Temperatura de operación: 0° a 50°C (32° a 122°F), Humedad: 10 a 90% (sin condensación), Estándar: EN 60068 (IEC 68)
- Dimensiones físicas: Ancho: 44 cm (17.3 pulgadas), Profundidad: 17.3 cm (6.8 pulgadas), Alto: 4.4 mm (1.7 pulgadas), Peso: 2.1 kg (5 lb)

2.4.2.2 SWITCH CISCO CATALYST 4500 GIGABIT ETHERNET MODULE 2-PORTS

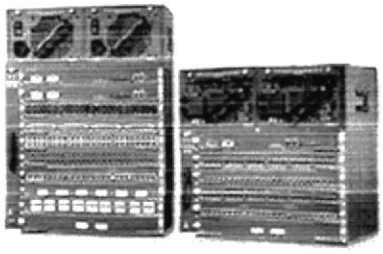

Fig. 2.4 Switch 4500

ESPECIFICACIONES DEL EQUIPO

- Factor de forma Módulo de inserción
- Tipo de dispositivo Módulo de expansión - 2 puertos
- Expansión / Conectividad
- Ranuras compatibles 1 x Ranura de expansión
- Total ranuras de expansión (libres) 2 (2) x GBIC
- Conexión de redes
- Tecnología de conectividad Cableado
- Protocolo de interconexión de datos Gigabit Ethernet
- Cumplimiento de normas IEEE 802.3x
- Velocidad de transferencia de datos 1 Gbpsc

2.4.3 RADIO PROXIM

Fig. 2.5 Radio Proxim

ESPECIFICACIONES DEL EQUIPO

- Proxim es líder en radios de espectro expandido T1/E1, exento de licencia.
- Los radios LYNX™ proveen de soluciones de interconexión inalámbrica exentas de licencia con una variedad de interfaces de telecomunicaciones de hasta DS-3.
- Los radios LYNX™ sin licencia operan en las bandas de 2.4 y 5.8 GHz ISM y en la banda 5.8 GHz UNII.

2.4.4 MODEM PARADYNE

Fig. 2.6 Modem Paradyne

ESPECIFICACIONES DEL EQUIPO

- Modem dial (conmutado) en alcanzar los 4,800 bps
- Primera familia de modems digitales LSI. Modem con diagnóstico remoto trabaja a 14.4 Kbps, con autorecocimiento a 9600/208B
- Primer modem en implementar compresión sincrónica.
- Además Paradyne a revolucionado la industria de la comunicación de datos con sus productos de acceso a redes de alta velocidad Hotwire implementado con tecnología RADSL, HDSL, SDSL y MSDSL

2.5 MEDIOS ALÁMBRICOS

2.5.1 CABLE UTP CATEGORIA 5.

Fig. 2.7 cable UTP Cat.5

2.6 MEDIOS INALÁMBRICOS

2.6.1 ANTENA MICROONDAS

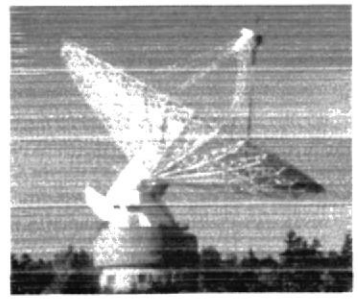

Fig. 2.8 Antena microondas

ESPECIFICACIONES DEL EQUIPO

- Modelo: ANTENA - ANDREW - ESC37T-2CPC-1
- Frecuencia: 2,4 GHZ, 24 DBI
- Homologación: Si

2.6.2 ANTENA DE RADIO

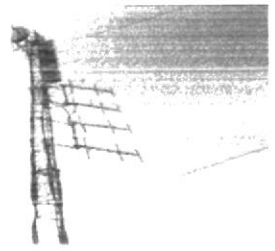

Fig. 2.9 Antena de Radio

ESPECIFICACIONES DEL EQUIPO

- Frecuencia: 2,4 GHZ, 24 DBI
- Homologación: Si

2.7 SERVIDORES

2.7.1 SERVIDORES WINDOWS 2000 (DATOS, FTP, DHCP)

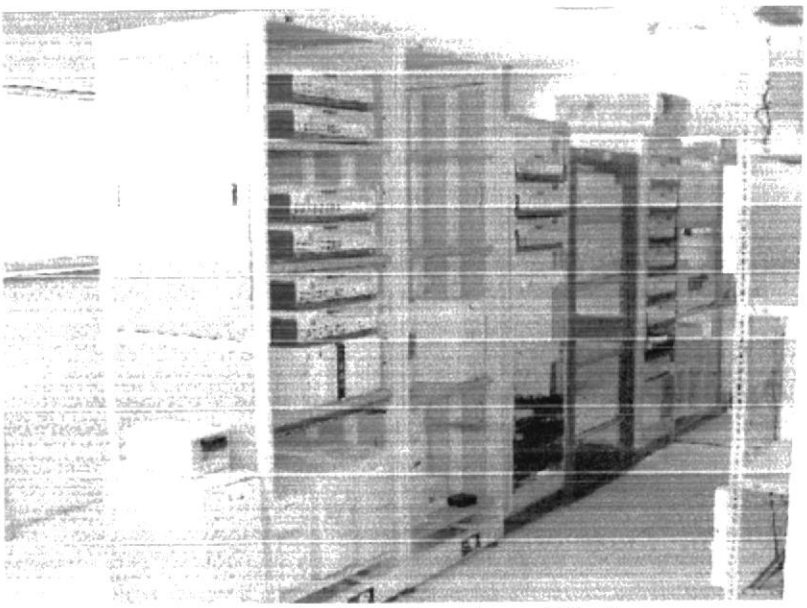

Fig. 2.10 Servidores Windows

2.7.2 SERVIDORES LINUX (PROXY, FIREWALL)

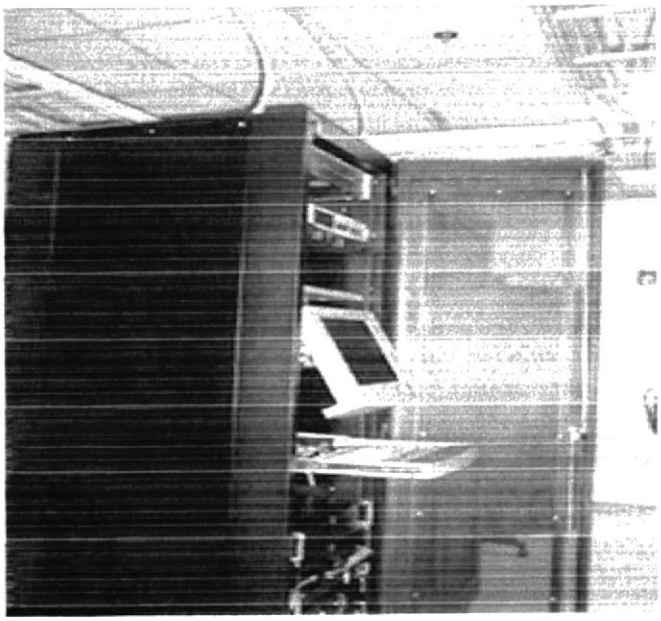

Fig. 2.11 Servidores Linux

2.8 ESTRUCTURA ACTUAL DE LA RED LAN

La matriz del Banco del Pacífico posee numerosos equipos de comunicaciones tanto para conexiones LAN como WAN.

2.8.1 RED LAN

La matriz posee 2 rack principales en el piso 9 (piso de comunicaciones), los cuales poseen 1 switch (cisco 4500), capa 3 que se encarga de comunicar todos los hubs de los pisos de la matriz.
Cada piso posee su IDF, con 2 o 4 hubs. La velocidad de transmisión es de 10mbps en todo el edificio.

2.8.2 IDF MATRIZ

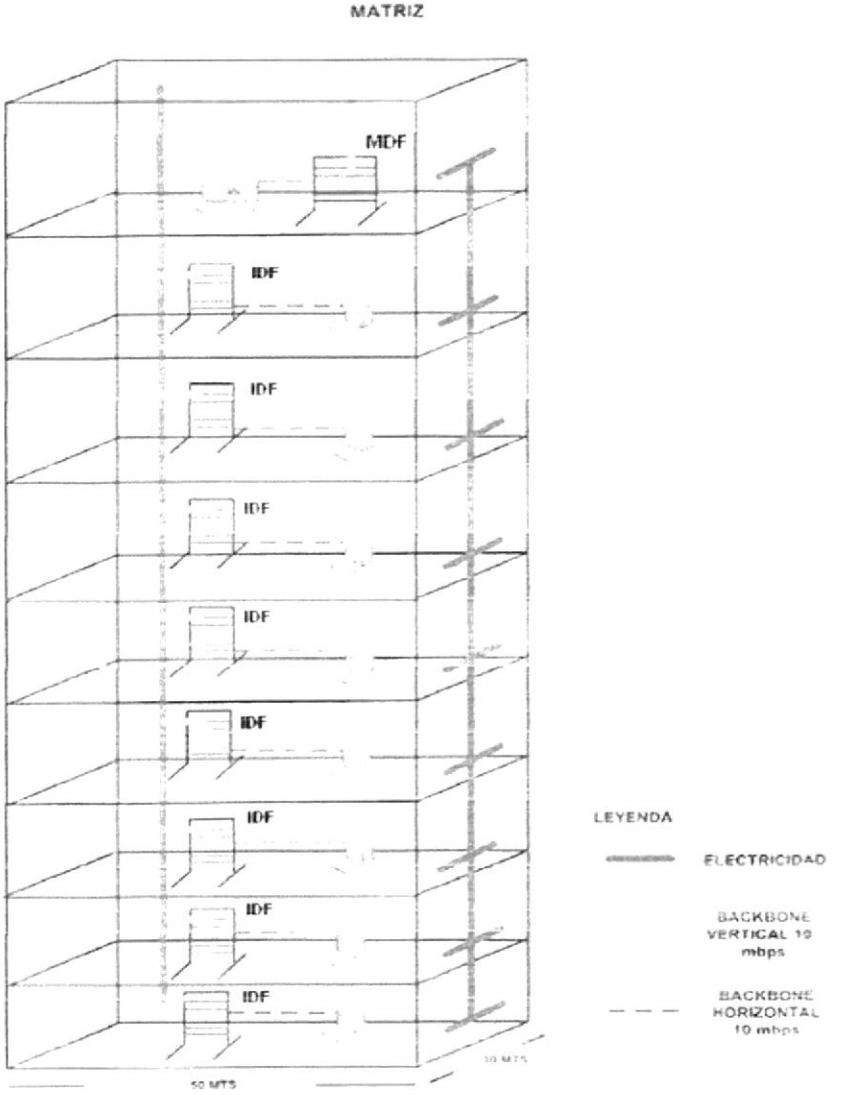

Fig. 2.12 Matriz

2.9 ESTRUCTURA ACTUAL DE LA RED WAN

2.9.1 ENLACE MICROONDAS DE AGENCIA-MATRIZ

El router principal Cisco 7500, va hacia un switch, que enlaza la conexión principal y la conexión de backup del Banco, como está en el diagrama tiene tres conexiones hacia el router, hacia la conexión principal y hacia el backup. Cuando estamos en la conexión principal entre ellos tengo un multiplexor que me divide el tráfico de datos y voz. En la conexión de backup o de contingencia vemos que no tenemos conexión de voz, solo datos, esta conexión usa la línea telefónica. Esto se repite del lado de la agencia o sucursal con equipos adecuados con menos características que el router principal pero con similar eficacia.

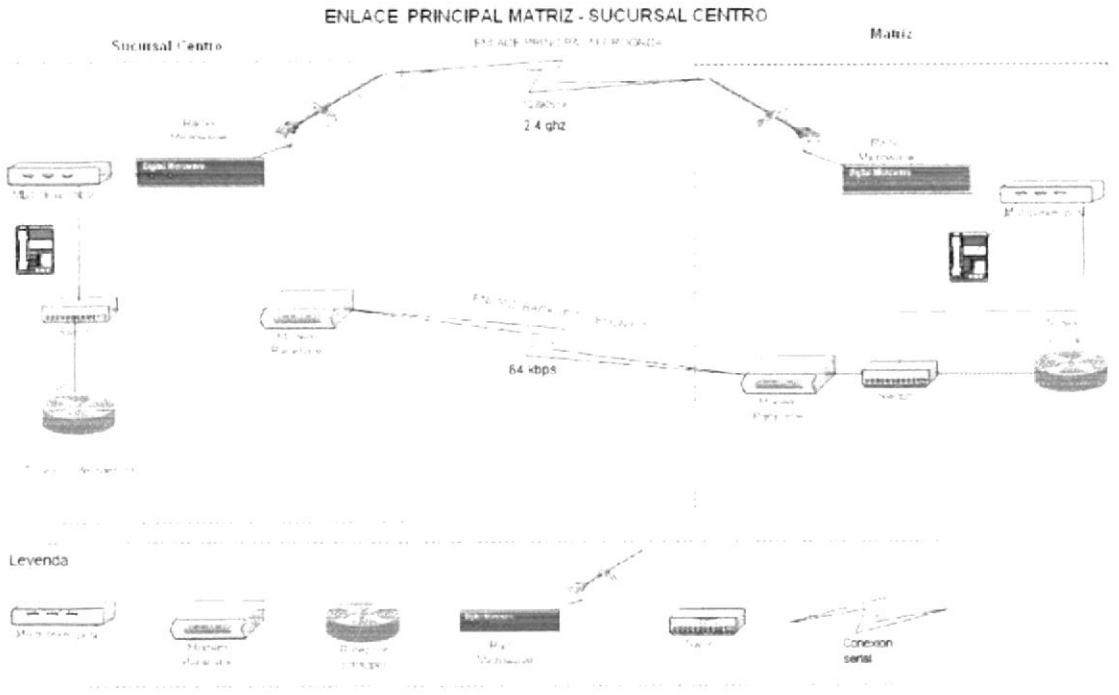

Fig. 2.13 Conexión Agencia Matriz

2.9.2 ENLACE SUCURSAL-AGENCIA

De la red Lan que es la ethernet del router principal va por una cable (RS232 o V35) hacia un modem (RAD ASM), de acuerdo al proveedor de última milla va hacia (cobre o radio) el otro par que es un modem rad, y va hacia el router de la agencia, por un cable rs232 o v35, y de ahí hacia la Lan por la interfaz ethernet del equipo.

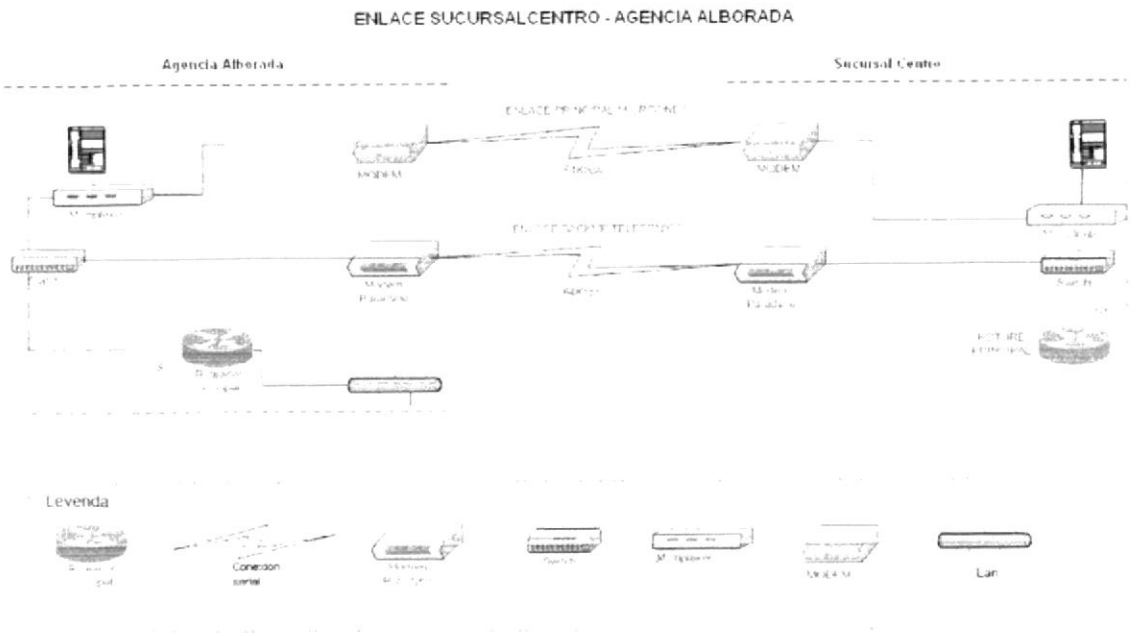

Fig. 2.14 Conexión Sucursal Agencia

2.9.3 ENLACE SATELITAL

De la red Lan que es la ethernet del router principal va por una cable (RS232 o V35) hacia un modem (comstream), que es un moden satelital intervienen otros equipos en la antena para que eleven la potencia de la señal y llega el otro par que es otro modem (comstream), y va hacia el router de la agencia, por un cable rs232 o v35, y de ahi hacia la LAN por la interfaz ethernet del equipo.

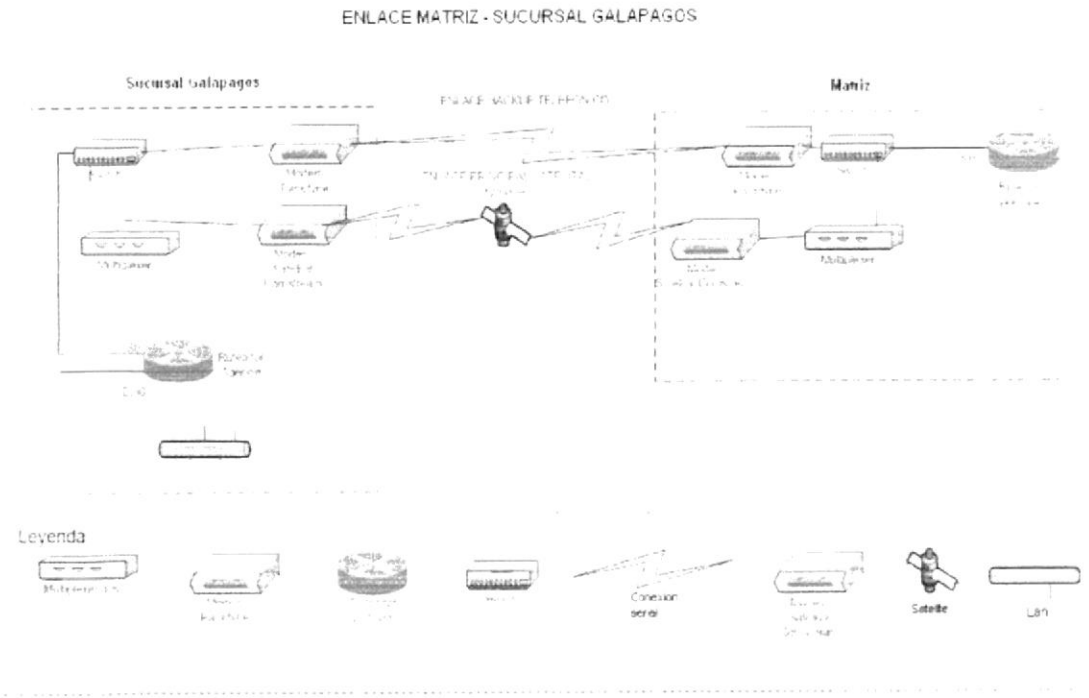

Fig. 2.15 Enlace Satelital

2.9.4 PROBLEMAS ENCONTRADOS

- No se cumple con todos las normas de cableado estructurado.
- Existen colisiones y propagación de broadcast en la red.
- Poco ancho de banda de datos entre Sucursal y Agencias.

CAPÍTULO 3

PROPUESTA

3. PROPUESTA

3.1 PROBLEMA - CAUSA - EFECTO

Después de un análisis exhaustivo de toda la red tanto LAN y parte de la WAN que se existe en EL BANCO DEL PACÍFICO se detectó algunos problemas los cuales se mostrará a continuación:

PROBLEMA	CAUSA	EFECTO
No se cumple con todos las normas de cableado estructurado.	No se encuentran etiquetados los puntos de red.	Perdida de tiempo en comprobación de puntos de red.
Existen colisiones y propagación de broadcast en la red.	Poseen Hubs.	Lentitud en la red, mayor de tiempo de respuesta.
Poco ancho de banda de datos entre Sucursal y Agencias.	Falta de presupuesto.	Demora en el proceso de las aplicaciones del Banco.

Tabla 3.1 Problema-Causa-Efecto

3.2 SOLUCIÓN PROPUESTA

PROBLEMA	SOLUCION	ALCANCE
No se cumple con todos las normas de cableado estructurado.	Etiquetar cada punto de red, y llevar un completo orden, para cumplir con las normas de cableado estructurado.	Con la respectiva etiquetación se ahorra tiempo al administrador en solucionar problemas de administración de red.
Existen colisiones y propagación de broadcast en la red.	Sustituir los hubs por switches de capa 2.	Mejor administración de la infraestructura Lan, y así se podrá ganar eficiencia en la red
Poco ancho de banda de datos entre Sucursal y Agencias.	Contratar los servicios de ISP para aumentar el ancho de banda y a su vez poder estandarizarlos a 128 kbps en todas las sucursales del país.	Con mayor ancho de banda a nivel Wan, se podrá agilitar los procesos del Banco y así ganar eficiencia en la red.

Tabla 3.2 Problema-Solución-Alcance

3.3 ESTUDIO DE FACTIBILIDAD: ALTERNATIVA "A"

3.3.1 OBJETIVOS

Mejorar el rendimiento en la comunicación de la red LAN, a través de la adquisición de dispositivos de conmutación indispensables para la empresa.

3.3.2 FACTIBILIDAD TÉCNICA

REQUERIMIENTOS DE HARDWARE

CANTIDAD	DESCRIPCION	UBICACION
19	SWITCH LAYER 2 poseen 48 puertos 10/100 +2 puertos Uplink de 10/100/1000BaseT.	Matriz
175	Rollos de cable UTP categoria 6	Matriz
3480	Conectores RJ45	Matriz
1	Contrato de ancho de banda a IMSAPT con 50% BIR	Sucursales

Tabla 3.3 Factibilidad Técnica

3.3.3 FACTIBILIDAD ECONÓMICA

REQUERIMIENTOS DE HARDWARE

CANT.	DESCRIPCION	UBICACION	PRECIO UNITARIO	SUBTOTAL
19	SWITCH LAYER 2 poseen 48 puertos 10/100 +2 puertos Uplink de 10/100/1000BaseT	Matriz	$1025.00	$19.475,00
175	Rollos de cable UTP categoria 6	Matriz	$80,00	$14.000,00
3480	Conectores RJ45	Matriz	$0,20	$696,00
1	Contrato de ancho de banda a IMSAPT con 50% BIR	Sucursales	$1250	$1250,00
			TOTAL:	35.421.00

Tabla 3.4 Factibilidad Económica

3.3.4 COSTO TOTAL DE PROPUESTA: ALTERNATIVA "A"

DESCRICPCION	VALOR TOTAL
Costos de hardware	35.421.00
Costos operativos	10.400.00
Subtotal	45.821.00
Imprevistos (15%)	6,873.15
Utilidades	11,455.25
TOTAL	$ 64,149.40

Tabla 3.5 Costo Total Alternativa "A"

3.3.5 FACTIBILIDAD OPERATIVA

ACTIVIDAD	CANTIDAD	DESCRIPCIÓN	TIEMPO SEMANAS
Fase Análisis de cableado estructurado	1	CCNA	3
	2	Técnico en red	3
Fase de Diseño del cableado LAN	1	CCNA	2
Fase de Implementación de red LAN	1	CCNA	7
	3	Técnico en red	7
Prueba de red LAN	1	CCNA	2
	1	Técnico de red	2
Documentación de la red de red LAN	1	CCNA	2

Tabla 3.6 Factibilidad Operativa

BANCO DEL PACIFICO

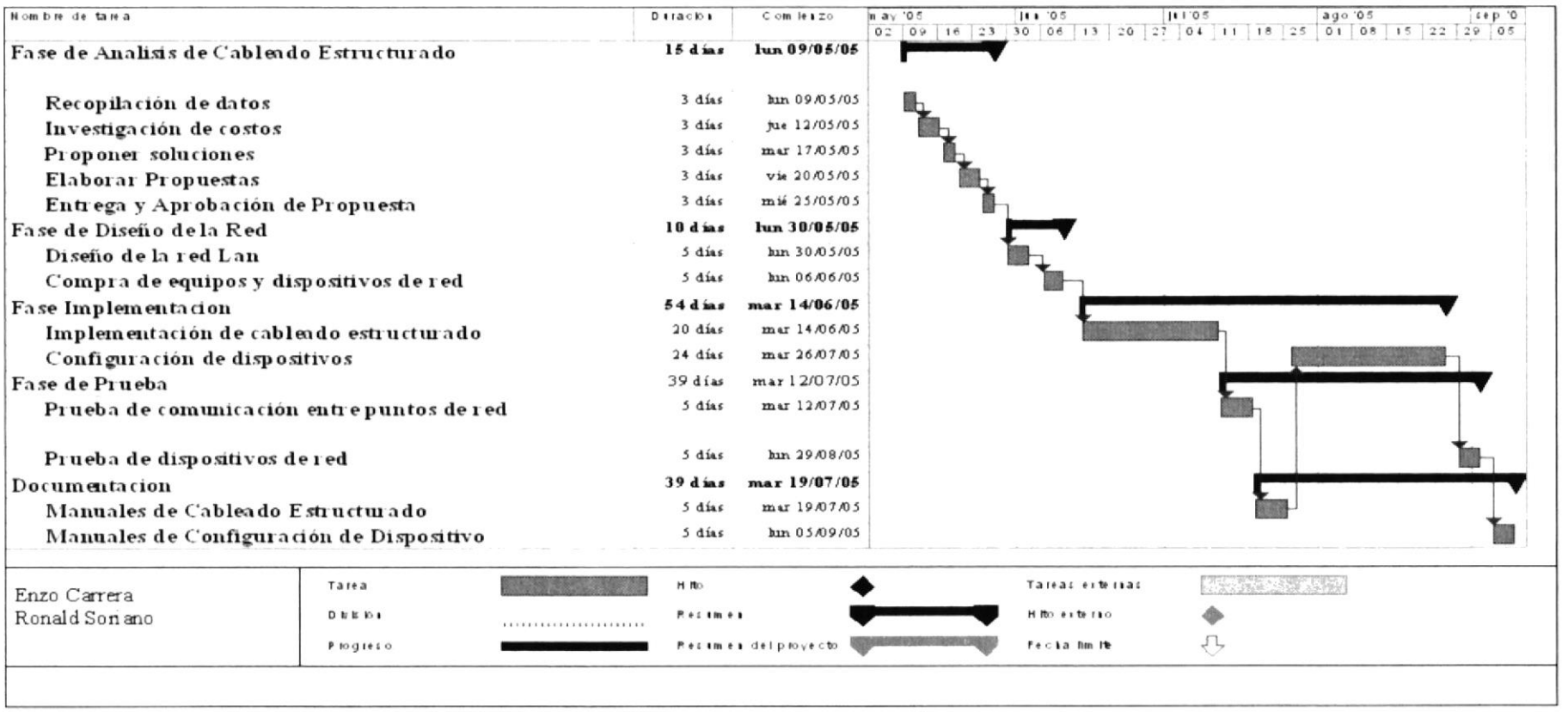

Fig 3.1 Diagrama Gant

3.3.7 VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA "A"

VENTAJAS

- Óptima actualización de datos entre matriz sucursales y agencias.
- Menor tiempo de respuestas, en la red Lan.
- fácil administración de la red Lan.
- Reducción de broadcast en la red.

BENEFICIOS

- Eficiencia en la realización de los procesos del Banco.
- La Empresa obtendrá un certificado por cumplir con los estándares de cableado estructurado.

3.4 ESTUDIO DE FACTIBILIDAD: ALTERNATIVA "B"

Mediante el estudio realizado a la empresa se estableció dos alternativas, de las cuales ésta a diferencia de la primera reduce costos debido a que los dispositivos y materiales de cableado utilizados son de menores caracteristicas.

3.4.1 OBJETIVOS

Mejorar el rendimiento en la comunicación de la red LAN, a través de la adquisición de dispositivos de conmutación indispensables para la empresa pero con rendimiento inferior a los ofrecidos en la alternativa anterior.

3.4.2 FACTIBILIDAD TÉCNICA

REQUERIMIENTOS DE HARDWARE

CANTIDAD	DESCRIPCION	UBICACION
19	Switch 48-PORT + 2 PRTS 10/100/1000	Matriz
175	Rollos de cable UTP categoria 5e	Matriz
3480	Conectores RJ45	Matriz
1	Contrato de ancho de banda a IMSAPT con 50% BIR	Sucursales

Tabla 3.7 Factibilidad Técnica

3.4.3 FACTIBILIDAD ECONÓMICA

REQUERIMIENTOS DE HARDWARE

CANT.	DESCRIPCIÓN	UBICACIÓN	PRECIO UNITARIO	COSTOS
19	Switch 48-PORT + 2 PRTS 10/100/1000	Matriz	631.57	$12.000,00
175	Rollos de cable UTP categoría 5e	Matriz	60.00	$10.500,00
3480	Conectores RJ45	Matriz	0.20	$696,00
1	Contrato de ancho de banda a IMSAPT con 50% BIR	Sucursales	1250.00	$1.250,00
			TOTAL:	24.446,00

Tabla 3.8 Factibilidad Económica

3.4.4 COSTO TOTAL DE PROPUESTA: ALTERNATIVA "B"

DESCRIPCION	VALOR TOTAL
Costos de hardware	24.446,00
Costos operativos	10.400.00
Subtotal	34.846.00
Imprevistos (15%)	5,226.00
Utilidades	8,711.00
TOTAL	$ 48,783.00

Tabla 3.9 Costo Total Alternativa "B"

3.4.5 FACTIBILIDAD OPERATIVA

ACTIVIDAD	CANTIDAD	DESCRIPCIÓN	TIEMPO SEMANAS
Fase Análisis de cableado estructurado	1	CCNA	3
	2	Técnico en red	3
Fase de Diseño del cableado LAN	1	CCNA	2
Fase de Implementación de red LAN	1	CCNA	7
	3	Técnico en red	7
Prueba de red LAN	1	CCNA	2
	1	Técnico de red	2
Documentación de la red LAN	1	CCNA	2

Tabla 3.9 Factibilidad Operativa

3.4.6 VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA "B"

VENTAJAS

- Óptima actualización de datos entre matriz sucursales y agencias.
- Menor tiempo de respuestas, en la red Lan.

BENEFICIOS

- Eficiencia en la realización de los procesos del Banco.
- La Empresa obtendrá un certificado por cumplir con los estándares de cableado estructurado.

3.5 FORMA DE PAGO

La forma de pago será en efectivo o cheque certificado, 75% al momento de la firma del contrato y 25% contra entrega del trabajo terminado, con una garantía de 1 año en infraestructura y configuración de equipos.

3.6 RECOMENDACIONES Y CONCLUSIONES

RECOMENDACIONES

Luego de haber realizado la identificación y análisis de los problemas que existen en la red LAN y WAN de la empresa, sugerimos optar por nuestra solución propuesta ya que se ajusta a las necesidades y requerimientos del Banco y le permitirá tener mayor velocidad de comunicación en la red interna del edificio.

Usted verá recuperada su inversión debido a los grandes beneficios que presta el nuevo CABLEADO ESTRUCTURADO que se ha presentado. Además cuenta con el soporte técnico necesario para el buen funcionamiento de la red.

CONCLUSIONES

La solución propuesta es la opción más acertada que usted pueda tomar, ya que le brinda velocidad y soporte en la red.

CAPÍTULO 4

IMPLEMENTACIÓN DE CABLEADO

4. IMPLEMENTACIÓN DE CABLEADO

4.1 MATRIZ

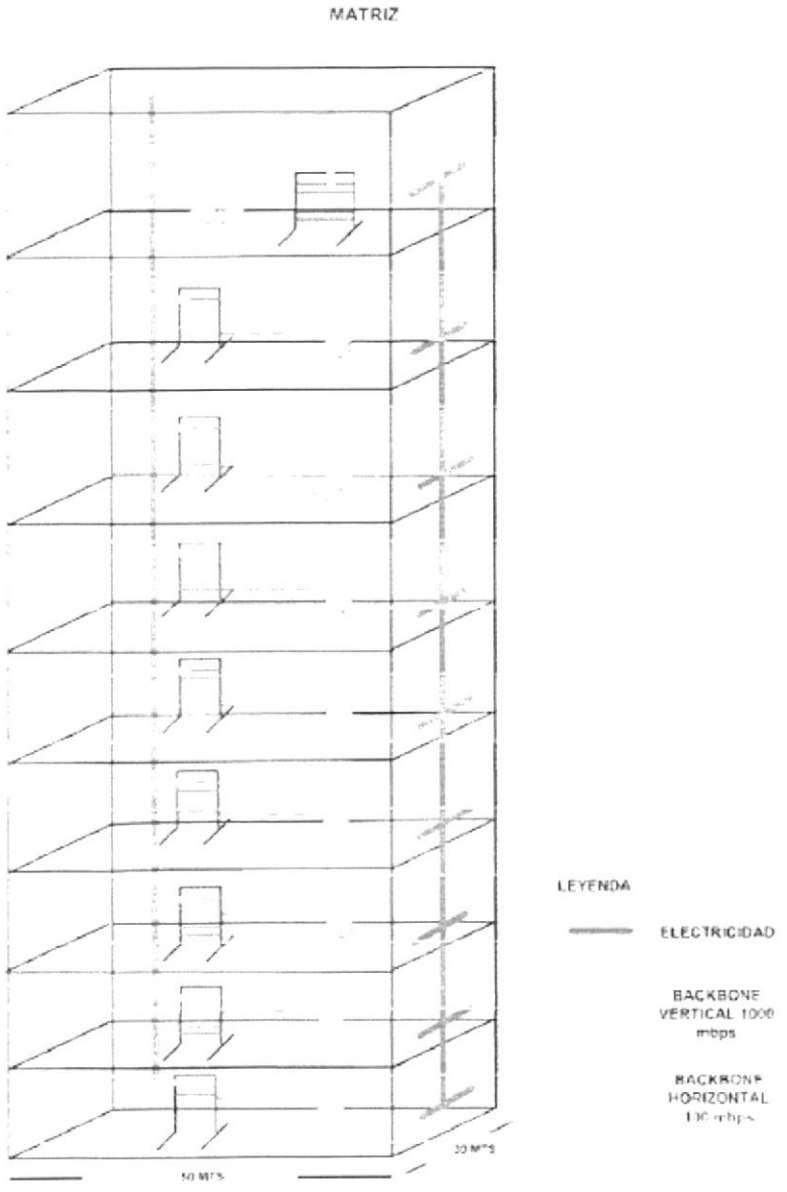

Fig 4.1 Matriz

4.1.1 PLANTA BAJA MATRIZ

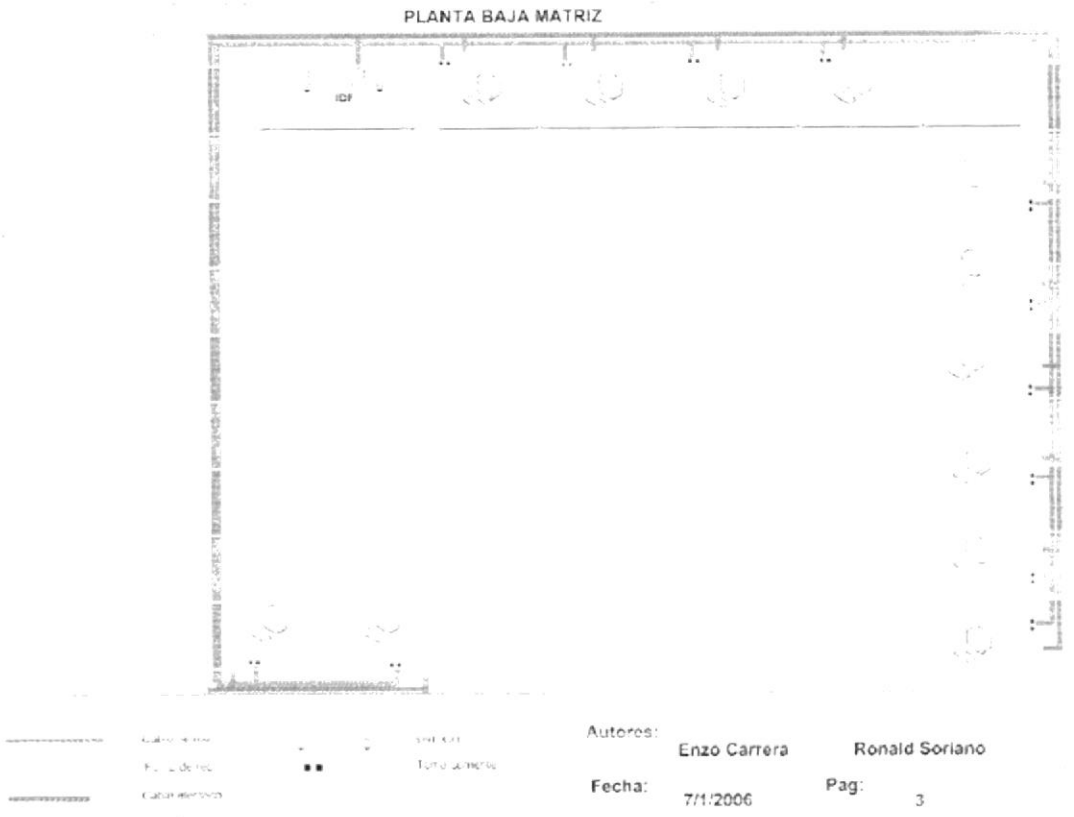

Fig 4.2 Planta Baja Matriz

4.1.2 PRIMER PISO MATRIZ

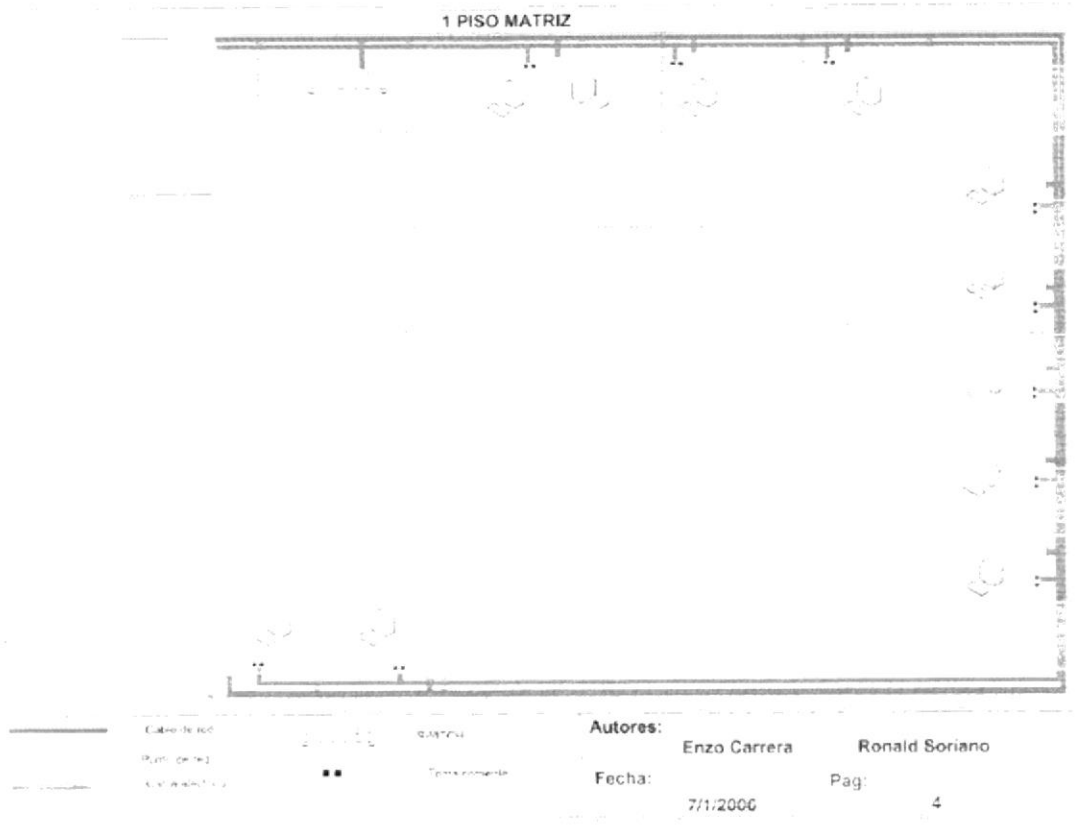

Fig 4.2 Primer Piso Matriz

4.1.3 SEGUNDO PISO MATRIZ

Fig 4.3 Segundo piso Matriz

4.1.4 TERCER PISO MATRIZ

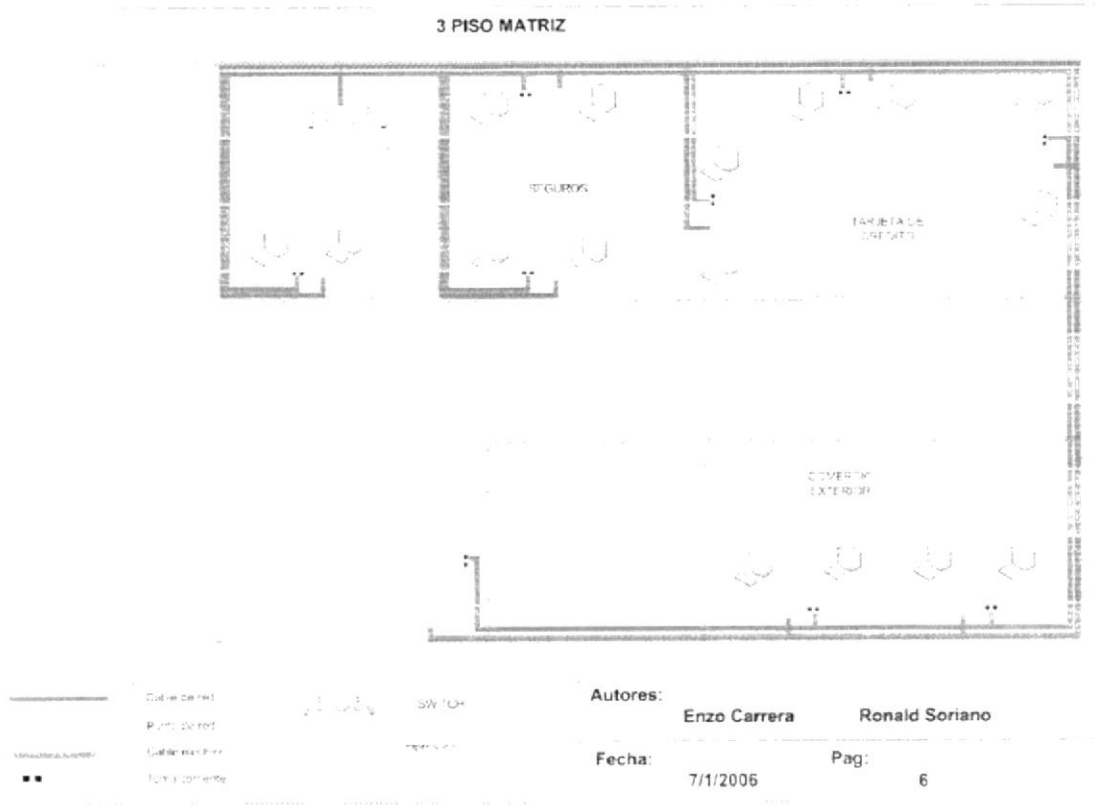

Fig 4.4 Tercer Piso Matriz

4.1.5 CUARTO PISO MATRIZ

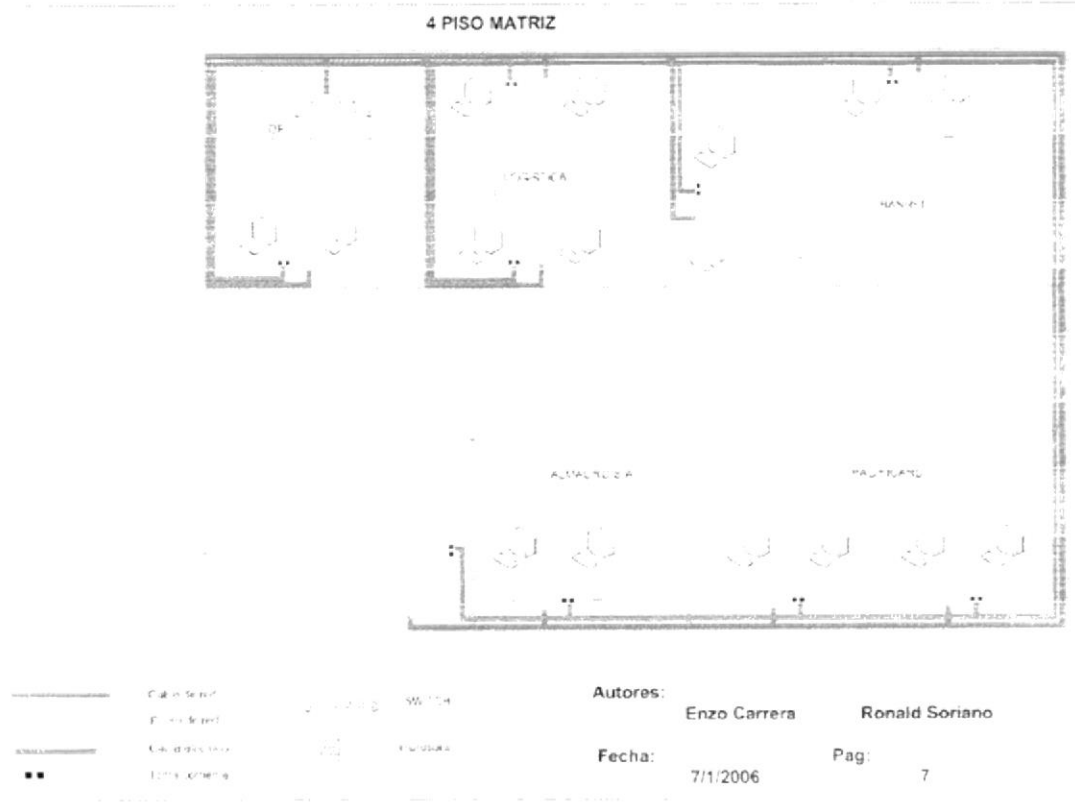

Fig 4.5 Cuarto piso Matriz

4.1.6 QUINTO PISO MATRIZ

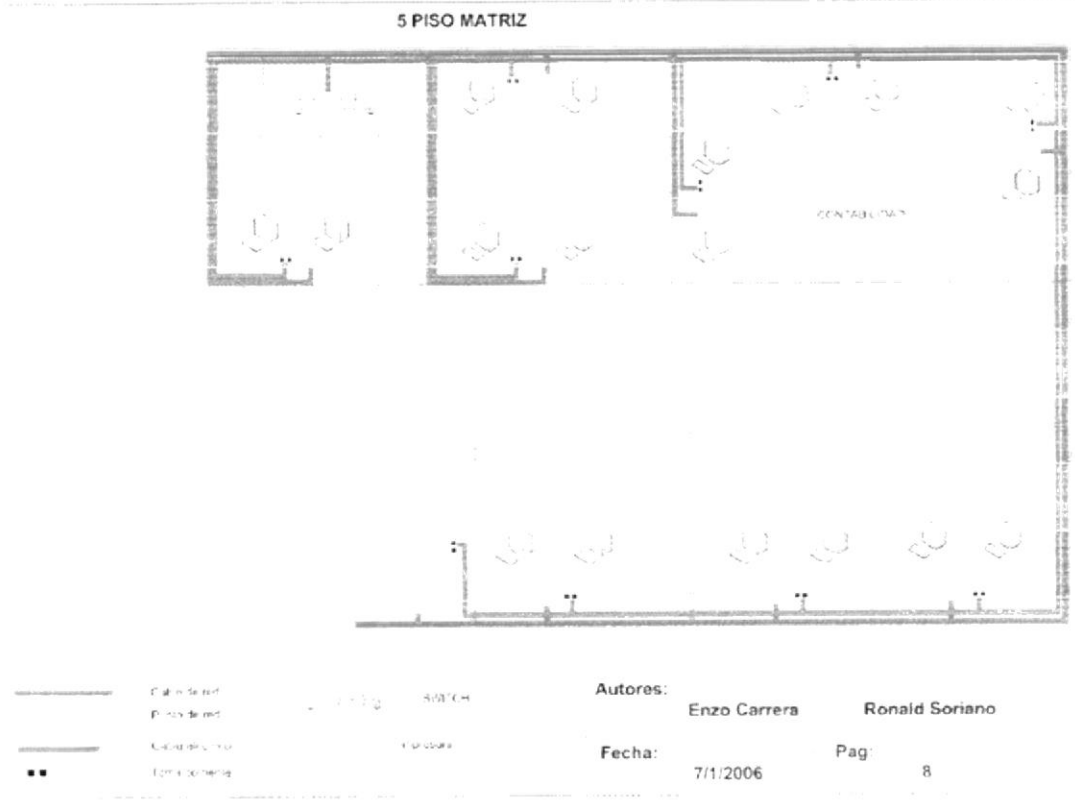

Fig 4.6 Quinto Piso Matriz

4.1.7 SEXTO PISO MATRIZ

Fig 4.7 Sexto Piso Matriz

4.1.8 SÉPTIMO PISO MATRIZ

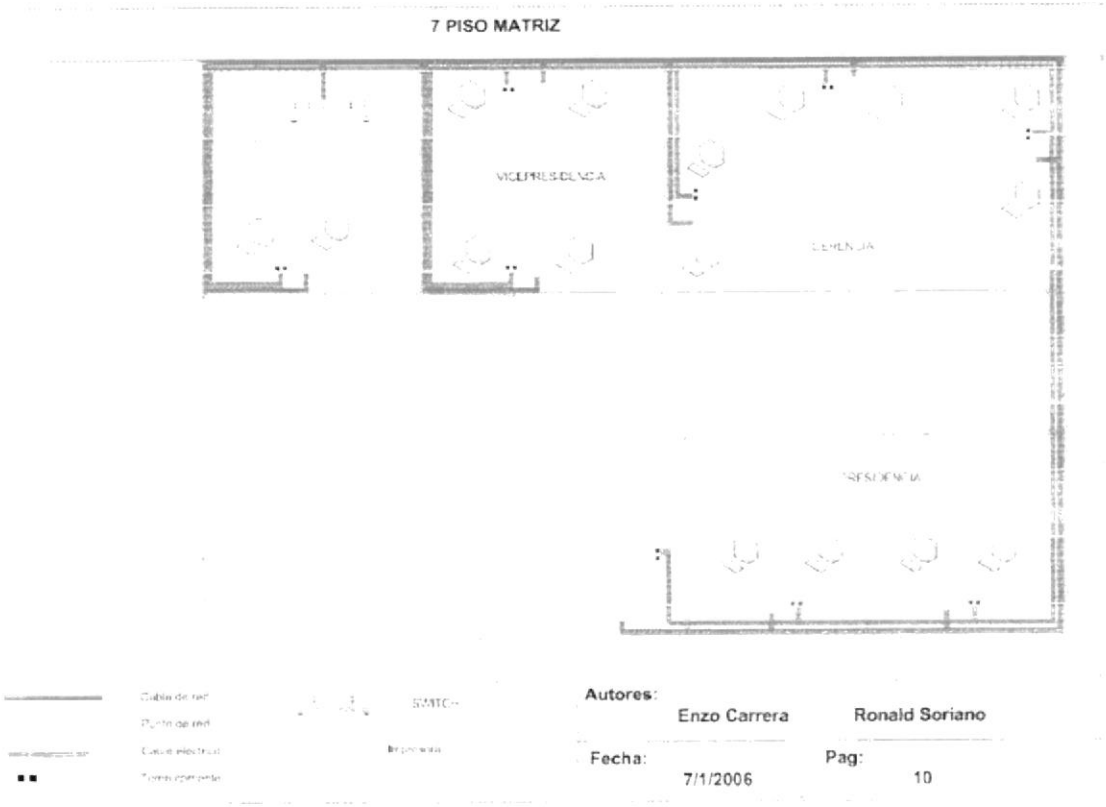

Fig 4.8 Séptimo Piso Matriz

4.1.9 OCTAVO PISO MATRIZ

Fig 4.9 Octavo Piso Matriz

4.2 SUCURSAL GALÁPAGOS

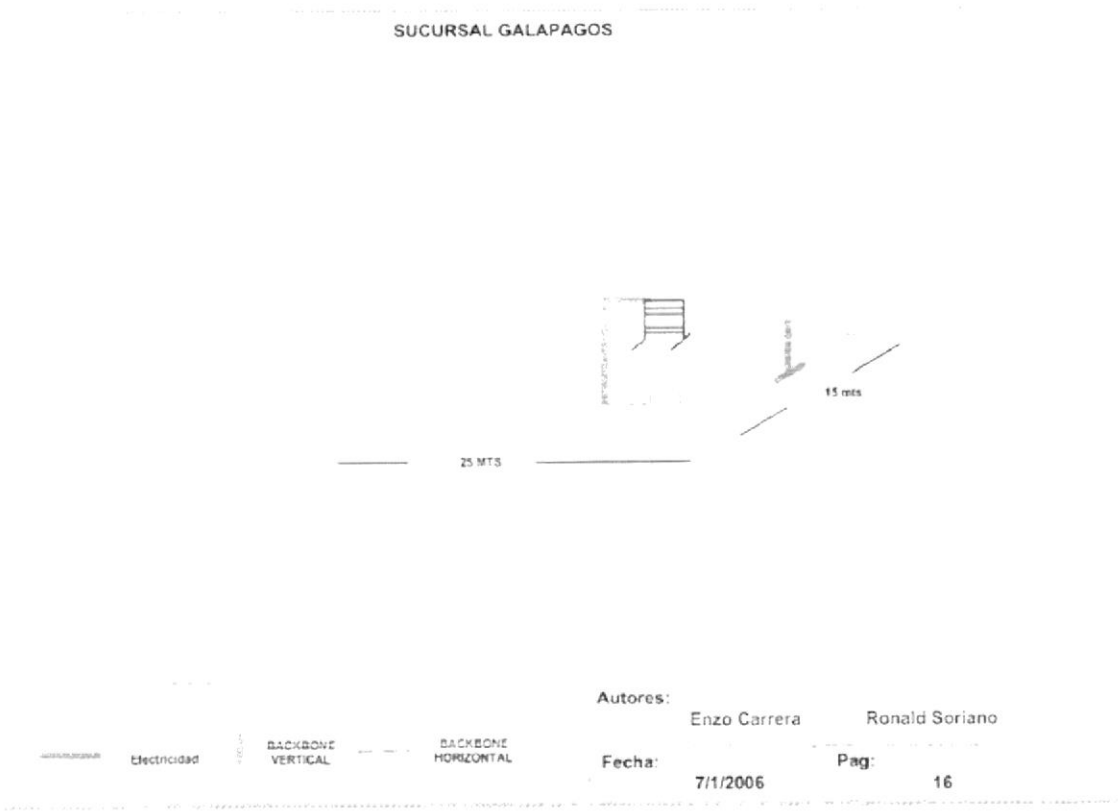

Fig 4.10 Sucursal Galápagos

4.2.1 PLANTA BAJA GALÁPAGOS

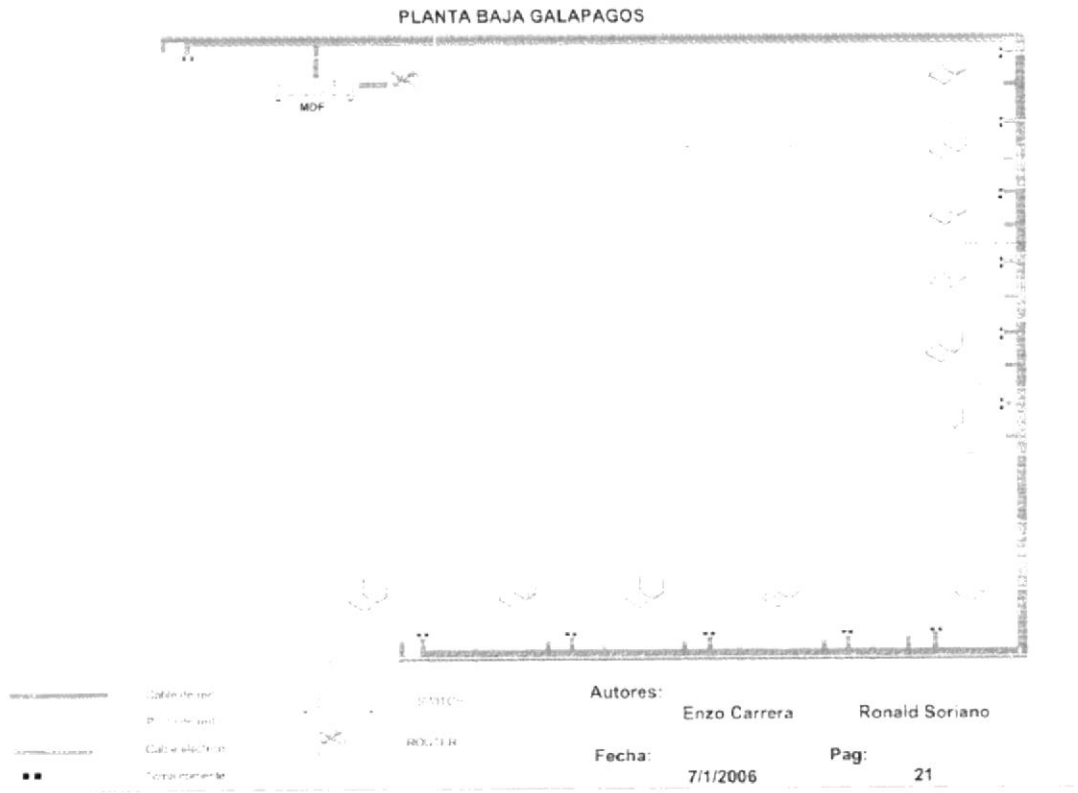

Fig 4.11 Planta Baja Galápagos

4.3 SUCURSAL CENTRO

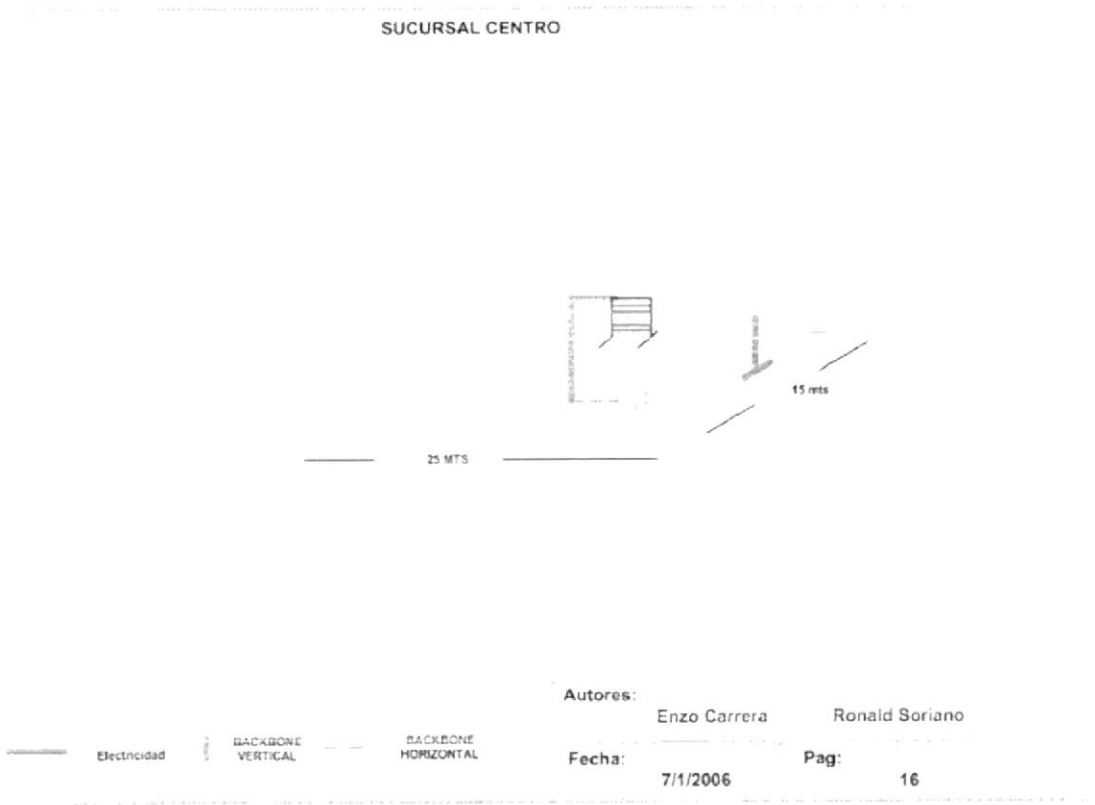

Fig 4.12 Sucursal Centro

4.3.1 PLANTA BAJA CENTRO

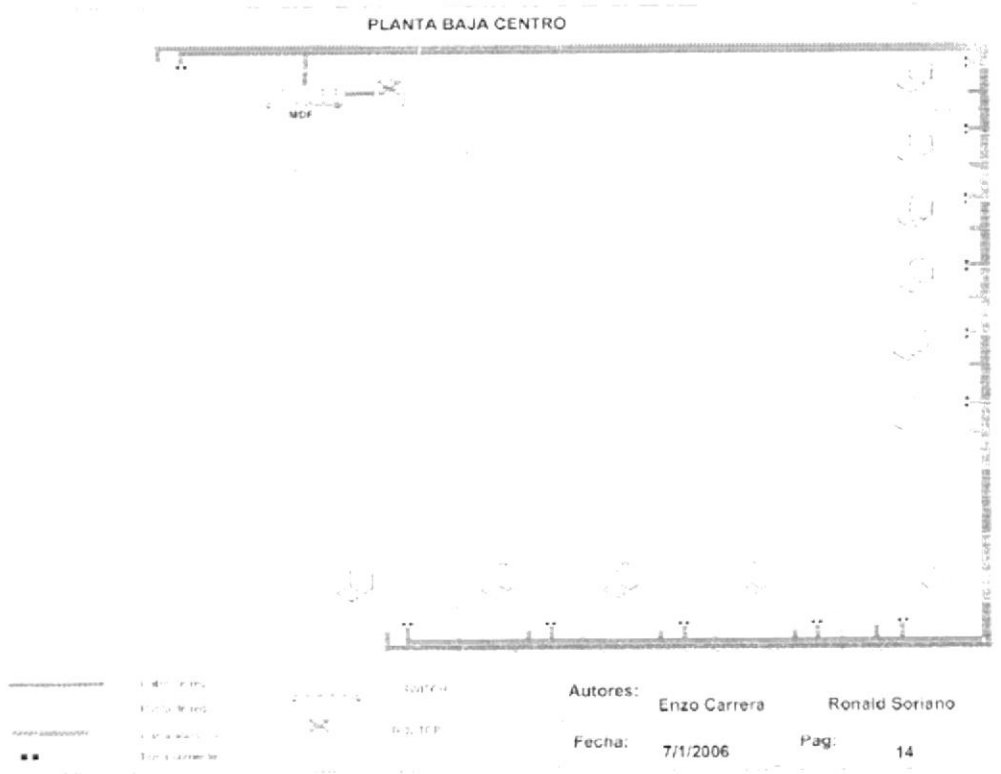

Fig 4.13 Planta baja Centro

4.4 AGENCIA ALBORADA

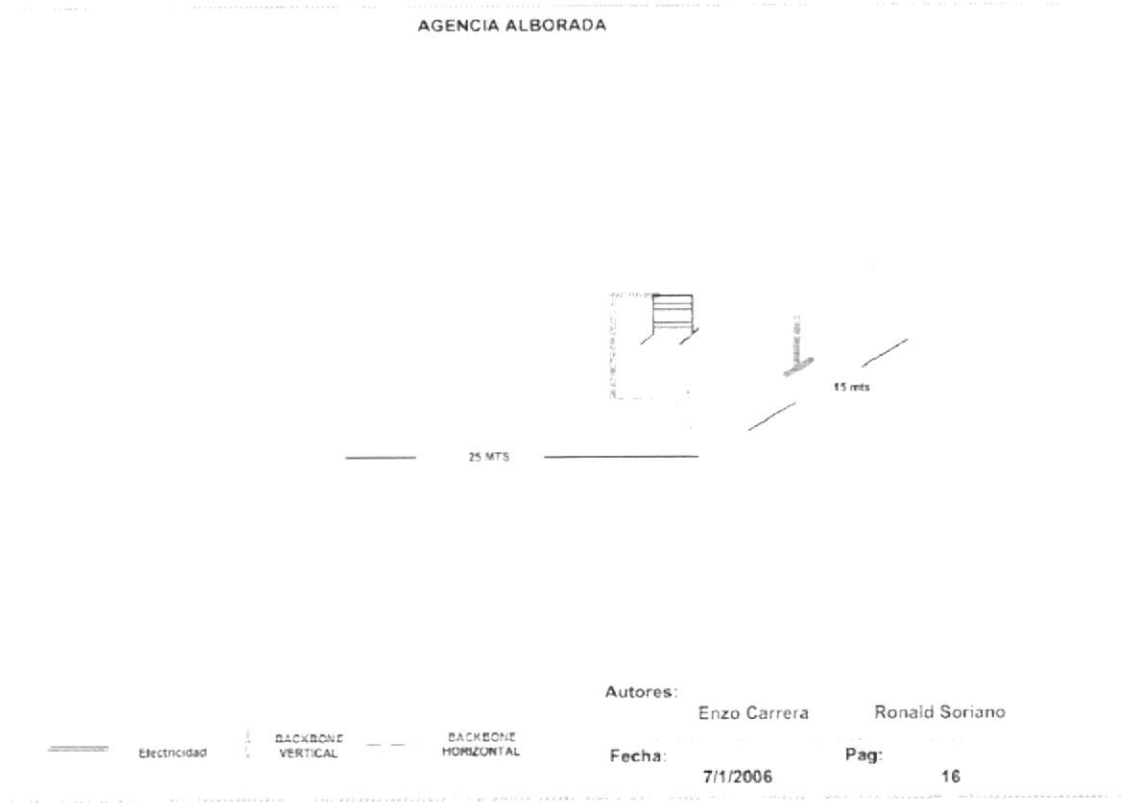

Fig 4.14 Sucursal Alborada

4.4.1 PLANTA BAJA ALBORADA

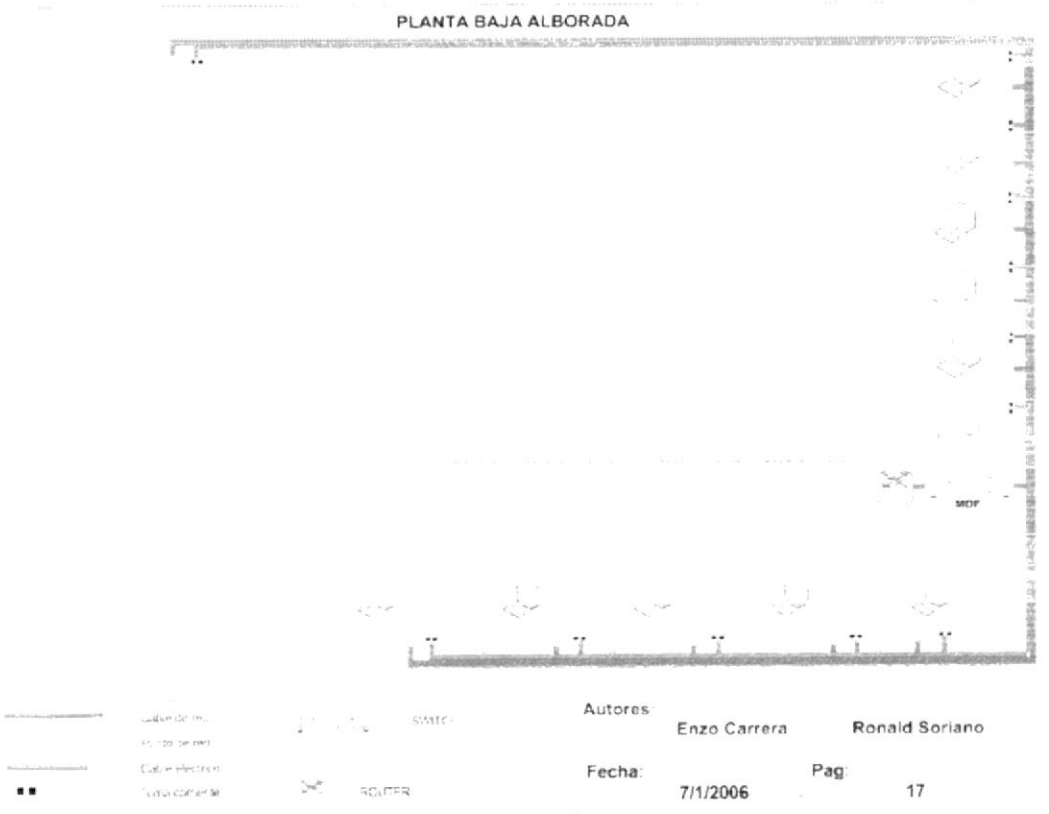

Fig 4.15 Planta Baja Alborada

CAPÍTULO 5

CONFIGURACIÓN DE DISPOSITIVOS

5. CONFIGURACIÓN DE DISPOSITIVOS

5.1 INTRODUCCIÓN A ROUTER

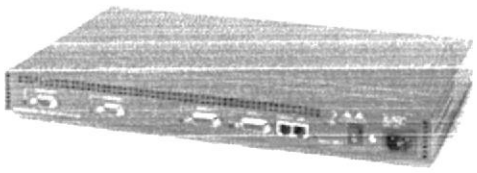

Figura 5.1 router

Un router es un dispositivo de red inteligente que funciona predominantemente en las tres primeras capas del modelo OSI. Los routers, al igual que los host son en realidad capaces de actuar en las siete capas del modelo de referencia OSI. Dependiendo de su configuración particular, se puede utilizar o no las siete capas de funcionabilidad, sin embargo, las necesidades de las tres primeras capas son virtualmente universales. La comunicación a través de las dos primeras capas permiten que los router se comuniquen directamente con las LAN (construcción de la capa de enlace datos) mas importante aún es que los router puedan identificar rutas a través de redes basándose en las direcciones de la capa 3. Esto permite que los routers interconecten múltiples redes utilizando el direccionamiento de la capa de red. Sin tener en cuenta lo cerca o lejos que puedan estar unos de otros.

Sus principales características son:

- Permiten interconectar tanto redes de área local como redes de área extensa.
- Proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP.
- Son capaces de rutear dinámicamente, es decir, son capaces de seleccionar el camino que debe seguir un paquete en el momento en el que les llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas, etc.

5.2 COMPONENTES INTERNOS DE CONFIGURACIÓN DE UN ROUTER

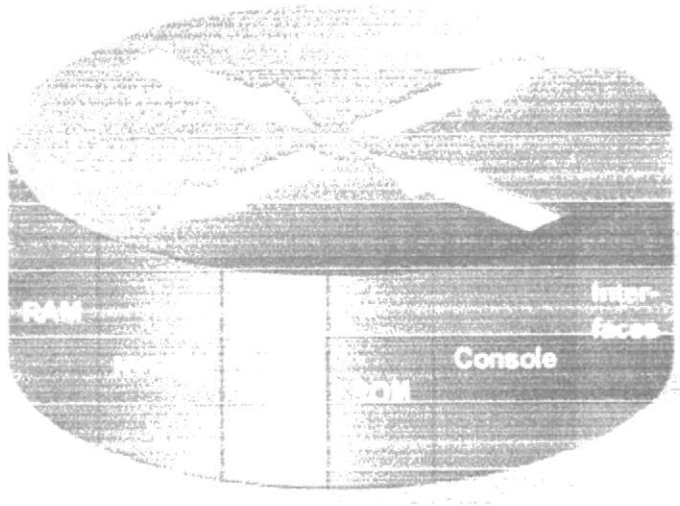

Figura 5.2 Componentes internos router

- **RAM/DRAM**
  Se utiliza para la información de la tabla de encaminamiento, caché de switching, configuración que se está ejecutando (running-config) y colas de paquetes.

- **NVRAM**
  Se utiliza para guardar el fichero de configuración (startup-config). Esta memoria NO es volátil.

- **Flash**
  Se utiliza para almacenar la imagen completa del software de Cisco IOS.

- **ROM**
  Contiene los códigos de diagnósticos de encendido almacenados de forma permanente.

- **Consola**
  El puerto de consola proporciona acceso físico para la configuración inicial.

- **Interfaces**
  Proporcionan conectividad LAN y WAN

5.3 CONEXIONES EXTERNAS DE UN ROUTER

Los tres tipos básicos de conexiones de un router son las interfaces LAN, las interfaces WAN y los puertos de administración. Las interfaces LAN permiten la conexión del router a un medio de la LAN; normalmente es una forma de ETHERNET, sin embargo podría ser alguna otra tecnología LAN, como la Token Ring o ATM.

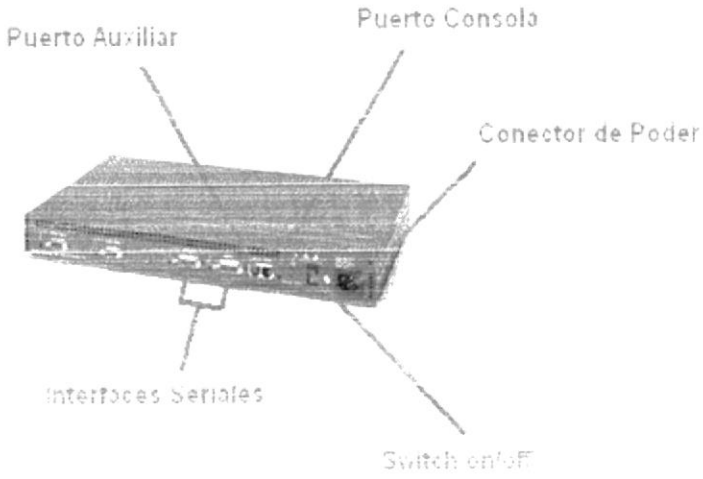

Figura 5.3 Conexiones externas router

Las conexiones WAN proporcionan conexiones, a través de un proveedor de servicios, con un lugar alejado o con Internet. Estas conexiones pueden ser serie o cualquier otra cantidad de interfaces WAN.

La función de los puertos de administración es diferente de la de otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red a través de las cuales se pasan los paquetes de trama. El puerto de administración ofrece una conexión basada en texto para la configuración y resolución de problemas del router. Las interfaces de administración más comunes son las de consola y auxiliares. Estos puertos están conectados a un puerto de comunicaciones en una computadora, esta ejecutará un programa de emulación de Terminal para proporcionar una sesión basada en texto con el router.

Cuando un router entra en servicio por primera vez, no hay parámetros de red configurados. Por tanto, el router no puede comunicarse con ninguna red. Para prepararse para el arranque y configuración iniciales, se debe conectar una computadora con un cable RS-232 emulando un Terminal ASCII, al puerto de consola del router. Entonces podrá introducir comandos de configuración para configurar un router.

5.4 INTERFACES

Una Interfaz es una conexión de red a traves de la cual los paquetes entran y salen de un router.

5.4.1 DCE (EQUIPO DE TERMINACIÓN DE CIRCUITO DE DATOS)

Proporciona una conexión física a la red, envía tráfico y proporciona una señal de sincronización utilizada para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE.

5.4.2 DTE (EQUIPO TERMINAL DE DATOS)

Dispositivo en el extremo del usuario de una interfaz de red de usuario que sirve como origen de datos, destino de datos o ambos. Se conecta a una red de datos a través de un dispositivo DCE. Y utiliza señales de sincronización generadas por el DCE. DTE incluye dispositivos como computadoras, traductores de protocolos y multiplexores.

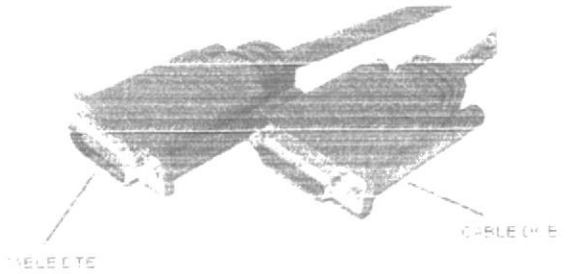

Figura 5.4 Tipos de cables

5.5 CONEXIÓN DE INTERFACES DE CONSOLA

5.5.1 PREPARACIÓN

Se necesita un cable de consola para establecer una sesión de consola y permitir la verificación o el cambio de la configuración del router. Serán necesarios los siguientes recursos:

- Estación de trabajo con una interfaz serial
- Router Cisco
- Cable transpuesto o de consola para conectar la estación de trabajo al router.

1.- Ubique el puerto consola del router

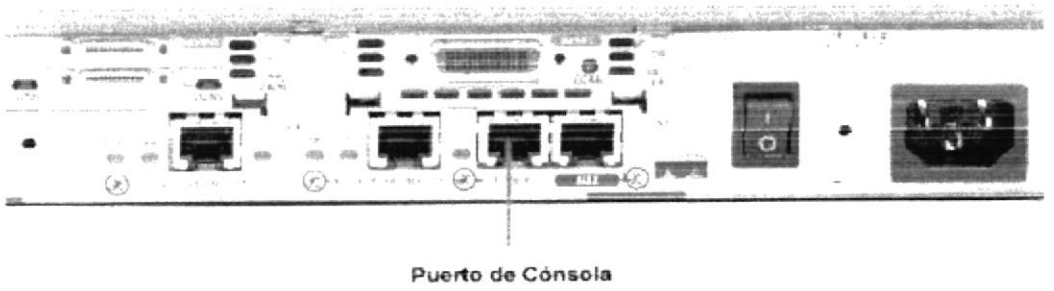

Figura 5.5 Parte posterior del router

2.- Ubicar el conector rj45 al Db9

Figura 5.6 Conector Db9

3.- Utilize el cable transpuesto

Use un cable de consola o transpuesto, elaborándolo si es necesario, de la longitud adecuada ara conectar el router a una de las estaciones de trabajo.

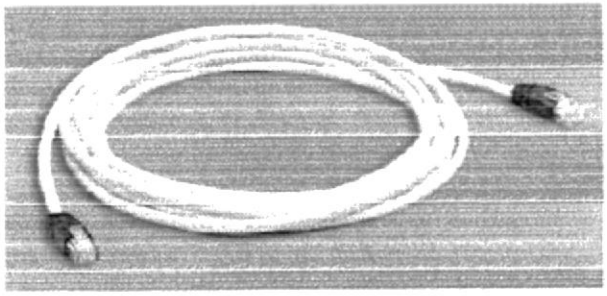

Figura 5.7 Cable transpuesto

4.- Conecte el cable transpuesto al conector RJ-45 que constituye el puerto de consola de router. A continuación, conecte el otro extremo del cable transpuesto al adaptador RJ-45 a DB-9. Por último, conecte el adaptador a un puerto serial del PC, ya sea DB-9 o DB-25, según el computador.

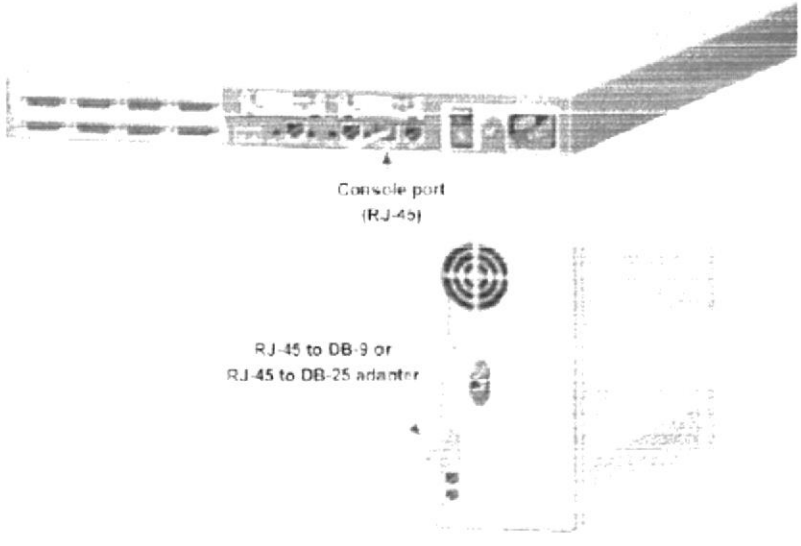

Figura 5.8 Conexión de router a Terminal

5.6 ESTABLECIMIENTO DE UNA SESIÓN EN HYPERTERMINAL

Para conectarse al router se debe utilizar la interfase de comandos en linea (CLI). Que es a través de una conexión por la linea serie conectada al puerto CONSOLE del router, usando por ejemplo la aplicación HYPERTERMINAL en Windows, MiniCOM en Linux, etc. Los parámetros necesarios para conectarse son los siguientes: Baud Rate 9600 bps, 8 bits/carácter, 1 bits de Stop, No paridad y No control de flujo Hardware.

A continuación se detalla los pasos a seguir:

1.- Abrir el Hyper Terminal con la siguiente ruta:

Menú inicio /programas /accesorios /comunicaciones /hyper Terminal

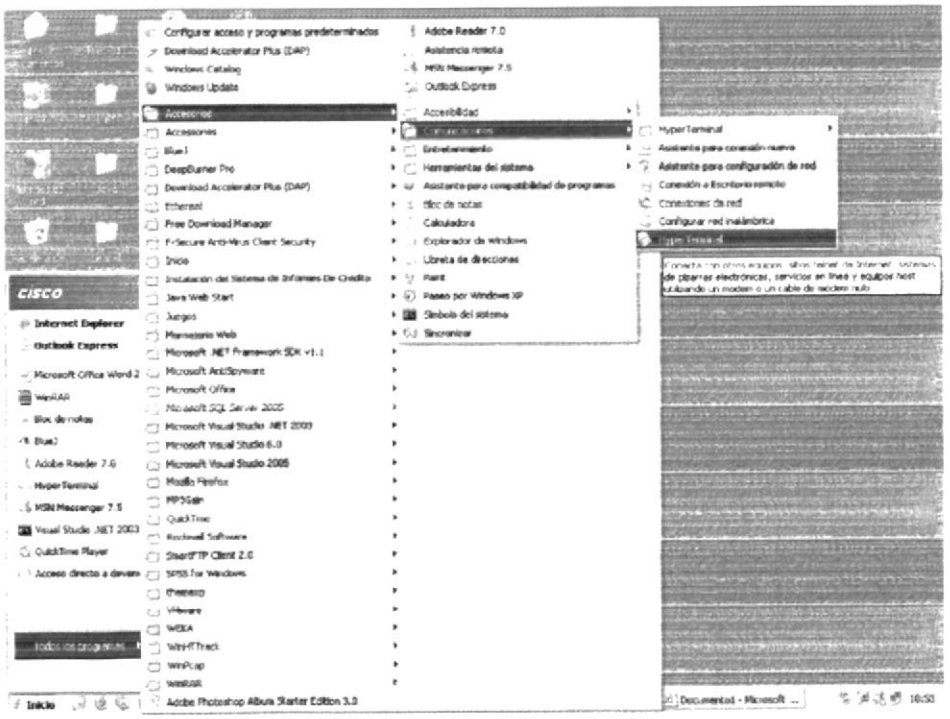

Figura 5.9 Ingresar al Hyperterminal

2.- Aparecerá un cuadro de dialogo en el cual tendrá que escribir el nombre de la conexión y elegir un icono, por último dar clic en aceptar:

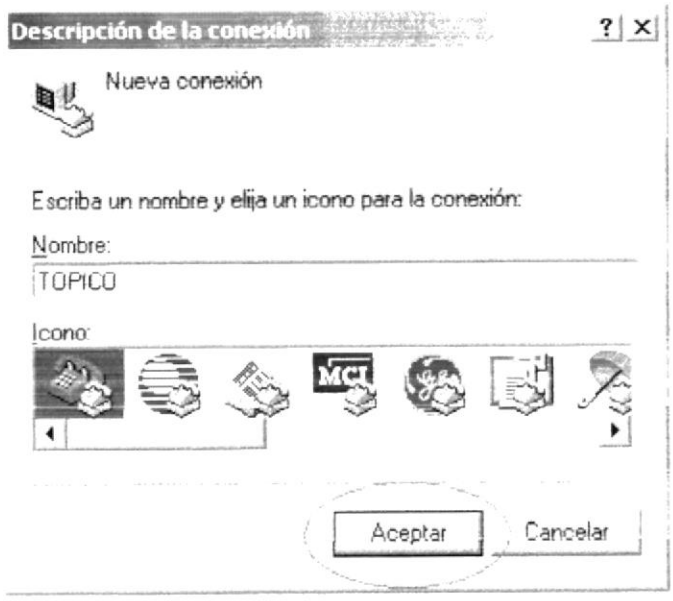

Figura 5.10 Descripción de conexión

3.- Elegir el puerto **COM** que va a utilizar para la conexión, y luego dar clic en aceptar:

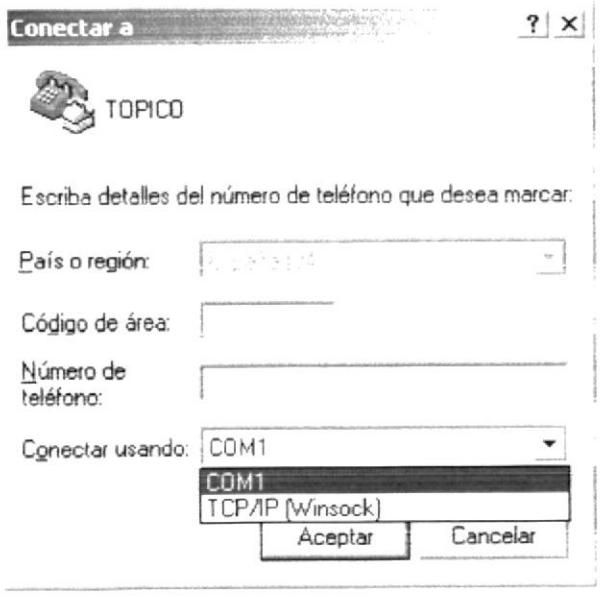

Figura 5.11 Conectar a

4.- Configurar el puerto **COM 1** de la siguiente manera y dar clic en aceptar:

- Bits por segundo: 96000
- Bits de datos: 8
- Paridad: ninguno
- Bits de parada: 1
- Control de flujo: ninguno

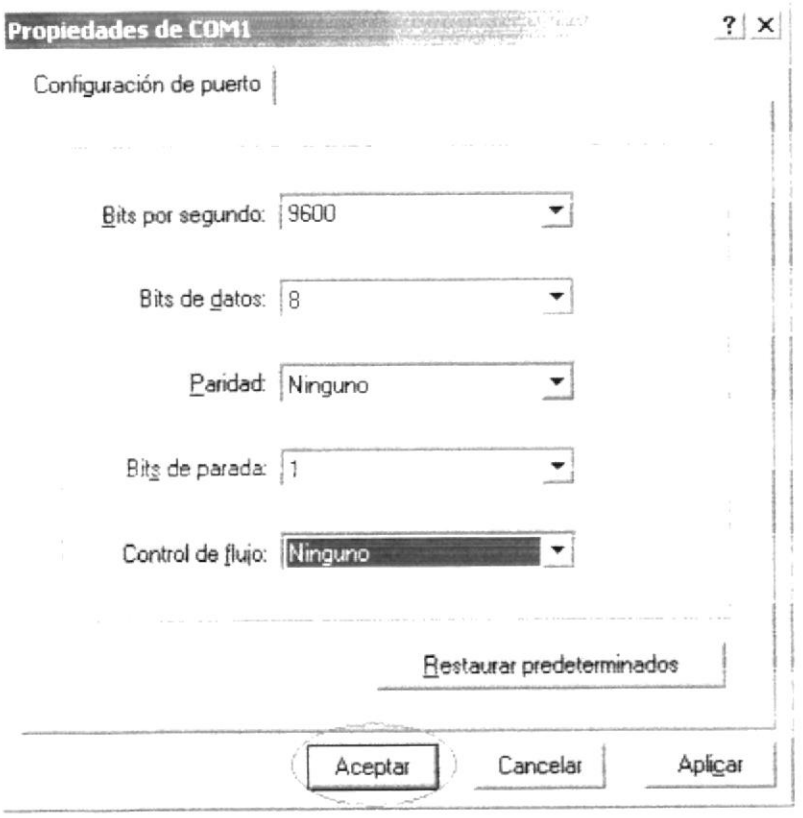

Figura 5.12 Propiedades de COM1

5.- Espere unos minutos y luego presionar la tecla **enter** para poder empezar a configurar el router desde nuestra Terminal en caso de presionar **cancelar** se cerrará la conexión:

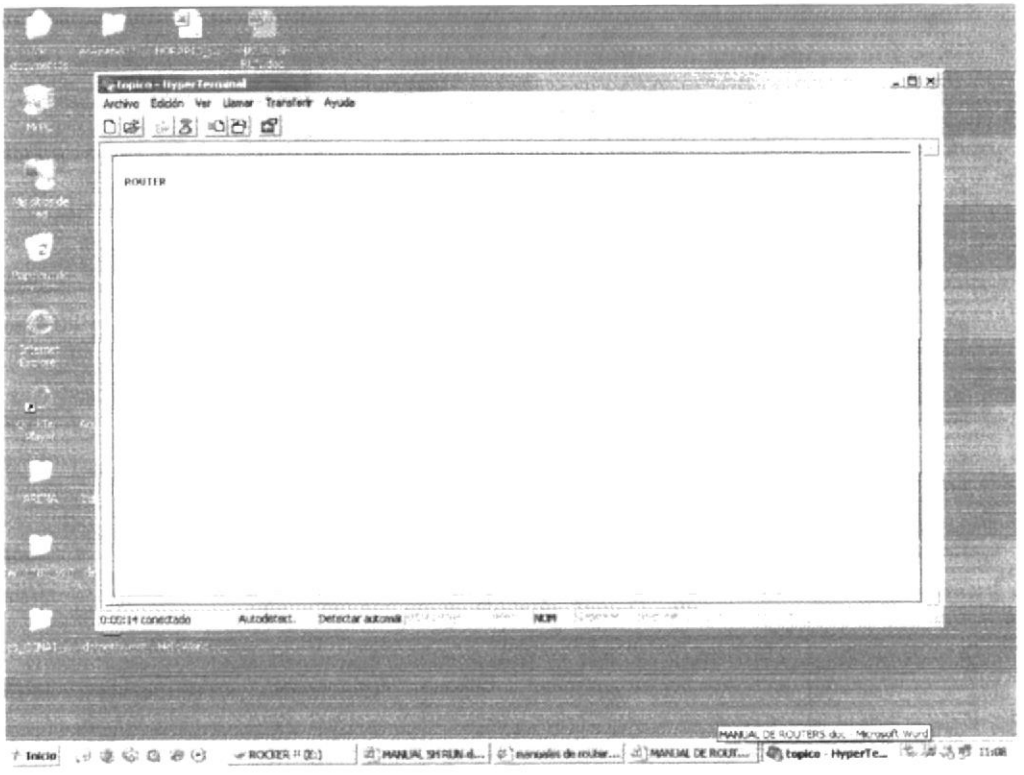

Figura 5.13 Hyperterminal

Al inicio el router preguntará si se desea arrancar con la configuración básica, se debe elegir no (si fuese el caso) y presionar **enter**.

Would you like to enter Basic management setup? [yes/no]: no

Después digitar el comando "**erase startup-config**" que sirve para borrar las configuraciones actuales en la NVRAM por último digitar el comando "**reload**" para recargar el router.

5.7 ESQUEMA WAN PROPUESTO

Aquí se mostrará el esquema WAN que representan a las diferentes sucursales que posee una empresa con su respectiva matriz la cual se va a configurar más adelante detallando paso a paso.

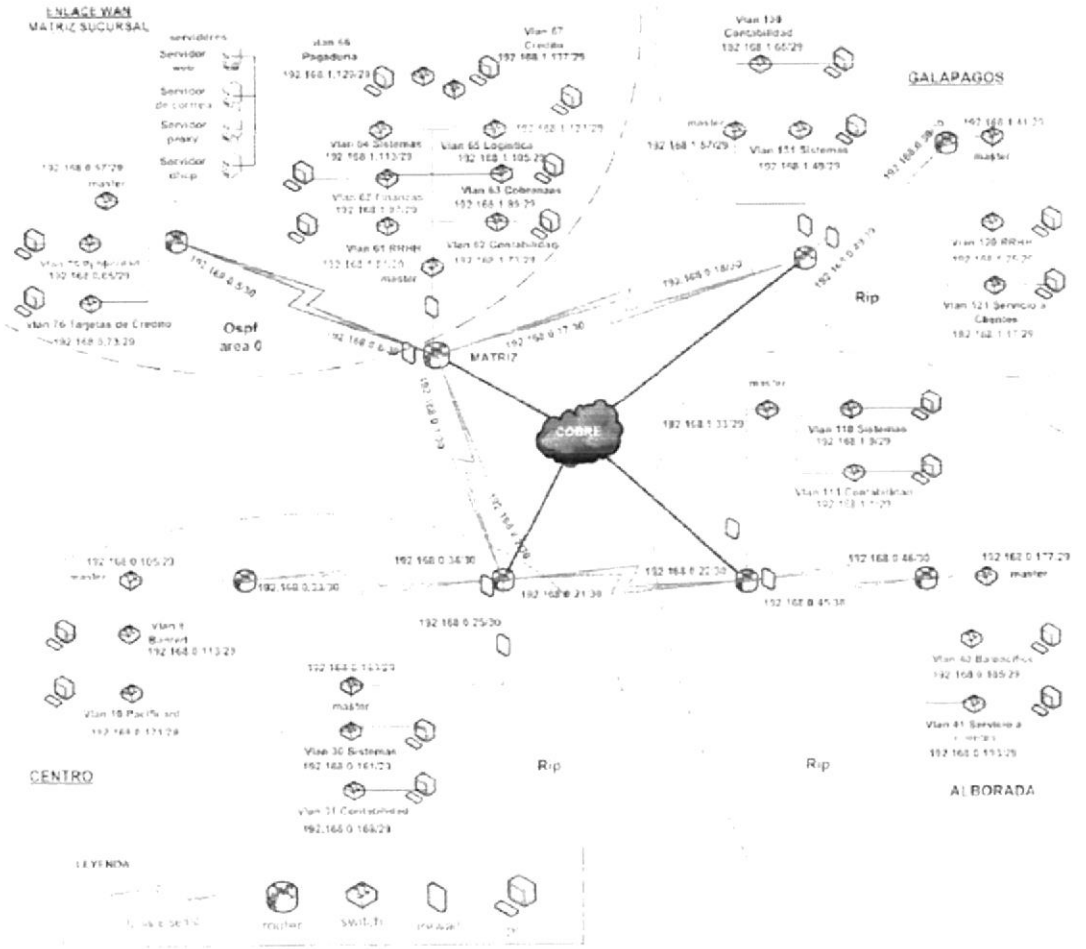

Figura 5.14 Esquema Wan

5.8 ROUTER MATRIZ

5.8.1 MODOS DE CONFIGURACIÓN DEL ROUTER

Al acceder al router por seguridad tiene dos niveles de acceso a los comandos:

- USER EXEC
- PRIVILEGED EXEC

En modo USER EXEC pueden consultar aspectos básicos de la configuración del router. Para consultar aspectos más críticos de la configuración del router se debe pasar a modo PRIVILEGED EXEC. Para pasar de modo USER EXEC a modo PRIVILEGED EXEC es necesario digitar el comando "**enable**".

En el modo USER EXEC el prompt que muestra el router es ">". En el modo PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#.

```
Router>                          modo usuario
Router> enable

Router#                          modo privilegiado
Router# exit
Router>
```

Desde los modos USER EXEC y PRIVILEGED EXEC no se puede modificar la configuración del router. Para hacerlo, se debe pasar del modo PRIVILEGED EXEC al modo de configuración global (CONFIGURE TERMINAL). Desde allí se puede configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc. y para salir de estos modos de configuración se debe digitar el comando "**exit**".

5.8.1.1 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc el prompt que aparece es "Router(config)#"

Router>
Router> enable

Router# configure Terminal  modo de configuración global

Una vez ingresado el comando" **configure Terminal**" aparecerá este msj. El cual se indicará que está dentro de la configuración global

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Router(config)#exit  modo privileged exec
Router#

5.8.1.2 MODO DE CONFIGURACIÓN ESPECÍFICOS

Permiten configurar protocolos, interfaces o en general aspectos más complejos del router. El prompt que aparece es R(config-if)#, R(config-route)#.

5.8.2 GUARDAR CAMBIOS EN EL ROUTER

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en la RAM del router llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el router se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

> Con el comando **copy running-config Startup-config** se guardan los cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN

MATRIZ# **copy running-config Startup-config**

> Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

Destinación filename [startup-config]? Yes

> El siguiente mensaje significa que se esta guardando la configuración

Building configuration...
[OK]

5.8.3 ASIGNAR NOMBRE A UN ROUTER

Una de las primeras tareas de configuración básica es asignar un nombre al router. El nombrado de un router ayuda a una mejor administración de la red al identificar univocamente cada uno de los router en la red.

Para configurar el nombre del router se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre >.Para salir del modo de configuración global con el comando "**exit**"

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

Router>**enable**
Router #

Entrar a la configuración global con el comando **configure Terminal**

Router # **configure Terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME** se cambia de nombre al router

Router # **hostname** MATRIZ
MATRIZ#

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

MATRIZ#

5.8.4 CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER

Un router puede ser asegurado mediante el uso de contraseñas para restringir el acceso. Las contraseñas pueden establecerse para las lineas de Terminal virtual y la linea de consola.
El modo de configuración **line console 0** puede utilizarse para establecer una contraseña de conexión en el Terminal de consola, lo que resulta útil en una red en la que hay muchas personas que tienen acceso al router.
El modo de configuración **line vty 0 4** sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

A NIVEL DE USUARIO

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

MATRIZ >**enable**
MATRIZ #

Entrar a la configuración global con el comando **configure terminal**:

MATRIZ # **configure Terminal**
MATRIZ (config)#

Digitar el comando **line console 0** para establecer una contraseña de conexión en el Terminal de consola.

MATRIZ (config)#**Line console** 0

Digitar el comando **password** seguido de la contraseña.

MATRIZ (config)#**Password** cisco

Después digitar el comando **login** el cual habilitará la petición de contraseña al usuario.

MATRIZ (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

MATRIZ#

A NIVEL DE USUARIO PRIVILEGIADO

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

MATRIZ >**enable**
MATRIZ #

Entrar a la configuración global con el comando **configure terminal**:

MATRIZ # **configure Terminal**
MATRIZ (config)#

Digitar el comando **line vty 0 4** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

MATRIZ (config)#**Line vty 0 4**

Digitar el comando **password** seguido de la contraseña.

MATRIZ (config)#**Password** cisco

Después digitar el comando **login** el cual habilitará la petición de contraseña al usuario.

MATRIZ (config)#**Login**

Digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la contraseña.

MATRIZ (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

MATRIZ#

5.8.5 CONFIGURACIÓN DE INTERFACES

Desde el modo de configuración global se puede pasar a configurar las interfaces. Para configurar una interfase siga los siguientes pasos:

- Entrar al modo de configuración global
- Entrar al modo de configuración de interfaz
- Especifique la dirección IP seguida de su máscara de subred
- Active la interfaz

Por ejemplo, para configurar una interfase ethernet se debe hacer de la siguiente manera:

Router# configure terminal

Router(config)# interface <eth0 > modo configuración de intefaz
Router(config-if)# ip address <IP MASK>
Router(config-if)# no shutdown
Router(config-if)# exit
Router#

El comando "**no shutdown**" es necesario para activar la interfaz. Por defecto, al arrancar el router todos los interfaces están desactivados. El comando "**shutdown**" en su defecto desactivaría administrativamente una interfaz.

Las interfaces serial están diseñadas para que en la situación más normal se conecten a una operadora de telecomunicaciones a través de un DCE (e.g.; un MODEM o una Terminación de Red, TR). El DCE es el que normalmente da reloj y por tanto fija la velocidad de modulación y por consiguiente de transmisión.

Si se conectan dos puertos serie de router (DTE-DTE) hay que usar un cable cruzado. Además uno de los dos puertos tiene que actuar como DCE dando reloj. En principio desde el punto de vista de router cualquiera de los dos puede actuar de DCE, así que lo importante es que conector del cable es el que marca que puerto es DCE.

5.8.5.1 INTERFACES SERIALES

Una vez que se sabe que puerto es el que actúa de DCE, tiene que dar reloj. Está opción la tendrá que activar vía IOS con el comando "**clockrate Bw**", donde **Bw** son los bps con los que va a trabajar la línea. En el puerto DTE no se deberá activar este comando.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

MATRIZ>**enable**
MATRIZ#

Entrar a la configuración global con el comando **configure terminal**:

MATRIZ # **configure Terminal**
MATRIZ (config)#

Ingresar al modo de configuración de interfaz con el comando **interface serial 0/0**:

MATRIZ(config)#**interface serial 0/0**

Especificar la dirección de la interfaz y la máscara de subred con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.0.17 255.255.255.252

Como esta interfaz es DCE entonces fijar la velocidad de sincronización en bips/seg. con el comando **clock rate.** Omita este paso si la interfaz es DTE:

MATRIZ (config-if)# **clockrate 56000**

Ahora digitar el comando **no shutdown** para levantar la interface:

MATRIZ (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

MATRIZ#(config)#

Ahora ingresar a la **interface serial 0/1**

MATRIZ (config)#**interface serial 0/1**

Especificar la dirección de la interfaz y la máscara de subred con el comando **ip address:**

MATRIZ (config-if)#**ip address** 192.168.0.1 255.255.255.252

Ahora digitar el comando **no shutdown** para levantar la interface:

MATRIZ (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

MATRIZ#(config)#

Ahora ingresar la **interface serial 0/3**

MATRIZ (config)#**interface serial 0/3**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

MATRIZ (config-if)#**ip address** 192.168.0. 255.255.255.252

Como esta interfaz es DCE entonces fijar la velocidad de sincronización en bips/seg. con el comando **clock rate.** Omita este paso si la interfaz es DTE:

MATRIZ (config-if)# **clockrate 56000**

Ahora digitar el comando **no shutdown** para levantar la interfase:

MATRIZ (config-if)# **no shutdown**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

MATRIZ#

5.8.5.2 INTERFACES ETHERNET

Un interfaz ethernet se configura desde en modo consola. Cada intefaz ethernet debe tener una dirección IP y una máscara de subred.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

MATRIZ>**enable**
MATRIZ#

Entrar a la configuración global con el comando **configure terminal**:

MATRIZ # **configure Terminal**
MATRIZ(config)#

Ingresar al modo de configuración de interfaz con el comando **interface ethernet 0/0**:

MATRIZ(config)#**interface ethernet 0/0**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address** pero en este caso solamente se va a levantar la interfase sin ponerle dirección ip.

Ahora digitar el comando **no shutdown** para levantar la interfase:

MATRIZ (config-if)# **no shutdown**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

MATRIZ#

5.8.6 CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO

El Protocolo de enrutamiento es aquel que suministra los mecanismos necesarios para compartir la información de enrutamiento. Los mensajes de un protocolo de enrutamiento se mueven entre los routers. Un protocolo de enrutamiento permite a los routers comunicarse con otros routers para actualizar y mantener sus tablas. A continuación mostrará diversos protocolos de enrutamiento:

- RIP (protocolo de información de enrutamiento)
- OSPF (primero la ruta libre mas corta)
- IGRP (protocolo de enrutamiento de gateway interior)

5.8.6.1 PROTOCOLO RIP VERSIÓN 2(VECTOR DISTANCIA)

Es un protocolo de enrutamiento por vector-distancia, que 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, primero se debe cambiar al modo de configuración global, luego se debe establecer con una o más órdenes "**network**", las redes directamente conectadas al router y finalmente para salir digitar el comando"**exit**" A continuación se mostrará la configuración del router MATRIZ con el protocolo rip:

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

MATRIZ>**enable**
MATRIZ#

Entrar a la configuración global con el comando **configure Terminal**:

MATRIZ # **configure Terminal**
MATRIZ (config)#

Ingresar a la configuración del protocolo Rip con el comando **router rip**:

MATRIZ (config)# **router rip**

Ingresar a la **versión 2**

MATRIZ (config-router)#**version 2**

Digitar la dirección de red que esta configurada con RIP con el comando **network**:

MATRIZ (config-router)# **network** 192.168.0.0
MATRIZ (config-router)# **network** 192.168.1.0

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

MATRIZ#

5.8.6.2 OSPF (PROTOCOLO ESTADO ENLACE)

Los protocolos de estado del enlace conocen los routers distantes y como se Interconectan.

Características:

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

Para configurar este protocolo de enrutamiento, primero se debe cambiar al modo de configuración global, luego establecer el protocolo con el comando"**router ospf area** "luego establecer con una o más órdenes "**network"**, las redes directamente conectadas al router, seguido de la máscara wilcard y el área. Finalmente para salir digitar el comando"**exit**" A continuación se presenta la configuración del router MATRIZ con el protocolo ospf:

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

MATRIZ>**enable**
MATRIZ#

- Entrar a la configuración global con el comando **configure Terminal**:

MATRIZ # **configure Terminal**
MATRIZ (config)#

- Ingresar a la configuración del protocolo OSPF con el comando **router ospf** seguido de un número entre el rango [1-65535]:

MATRIZ (config)#**router ospf 1**

- Ingresar la dirección de red que esta configurado con ospf con el comando **network** seguido de la **wildcard** y la **área.**

MATRIZ (config-router)# **network** 192.168.1.72 0.0.0.7 **area** 0
MATRIZ (config-router)# **network** 192.168.0.16 0.0.0.3 **area** 0
MATRIZ (config-router)# **network** 192.168.0.12 0.0.0.3 **area** 0
MATRIZ (config-router)# **network** 192.168.0.4 0.0.0.3 **area** 0

- Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global.

MATRIZ#

5.8.7 REDISTRIBUCIÓN DE RUTAS

Es posible tener zonas que usan protocolos de encaminamiento distintos. Por ejemplo OSPF y RIPv2. Hay que inyectar las rutas que se aprenden de un protocolo a otro. A este proceso se la llama "redistribución de rutas".

Para establecer comunicación entre dos protocolos distintos se debe utilizar el comando "**redistribute <protocolo>**" esta línea debe ir dentro de la configuración del protocolo.

A continuación se presenta un ejemplo de redistribución entre **Rip v2** y **Ospf:**

Entrar a la configuración global con el comando **configure Terminal**:

MATRIZ #**configure Terminal**

Entrar al modo de configuración protocolos con el comando **router ospf 1**

MATRIZ (config)# **router ospf 1**

Con el comando **redistribute** se establece comunicación entre protocolos distintos.

MATRIZ (config-router)# **redistribute** rip
MATRIZ (config-router)# exit
MATRIZ #

MATRIZ #configure terminal
MATRIZ (config)# router rip
MATRIZ (config)#version 2
MATRIZ (config-router)# redistribute ospf 1
MATRIZ (config-router)# exit
MATRIZ #

5.8.8 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 y asegurando el acceso hacia y desde una red.

Las ACL pueden aplicarse en Protocolos Enrutados:

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

Las ACL se definen según el protocolo, la dirección o el puerto además el orden en el que se ubican es muy importante.

5.8.8.1 TIPOS DE ACLS

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

5.8.8.2 FUNCIÓN 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.

5.8.8.3 DIRECCIONES DE TRÁFICO

La dirección in o out (entrada o salida) determina si se va a permitir entrada o salida de tráfico en el router que se esta 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 ingresar la interfaz ethernet en la cual se va a determinar si se va a permitir entrada o salida de tráfico:

"ip access-group access-list-number"

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

MATRIZ>**enable**
MATRIZ#

Entrar a la configuración global con el comando **configure Terminal**:

MATRIZ# configure Terminal

Digitar la siguiente Acl Estándar que permitirá denegar el acceso al servidor de las demás redes con el comando

MATRIZ (Config)#access-list 2 permit host 192.168.10.12
MATRIZ (Config)#access-list 2 deny any any

Ingresar a la interfaz ethernet en la cual se va a determinar si se va a permitir entrada o salida de tráfico.

MATRIZ (Config)#**interface Ethernet** 0
MATRIZ (Config-if)#**ip access-group** 2 **out**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

MATRIZ#

5.8.9 SWITCHES

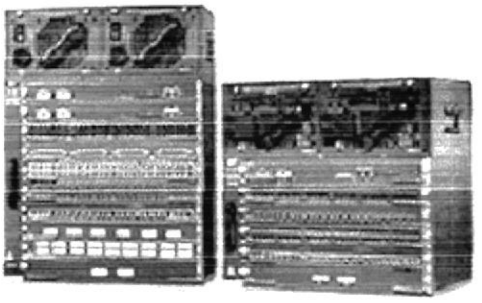

Figura 5.15 Switch

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. En el modo USER EXEC el prompt que muestra el switch es ">".En el PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#,

switch >
switch > enable

switch #
switch # exit
switch >

modo usuario

modo usuario privilegiado

5.8.10 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del switch como pueden ser la configuración del nombre del switch, passwords, etc (prompt R(config)#)

```
switch >
switch > enable

switch # configure terminal
switch (config)#exit
switch #
```

modo configuración global

5.8.11 GUARDAR CAMBIOS EN EL SWITCH

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en la RAM del switch llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el switch se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

Con el comando **copy running-config Startup-config** se guardan los cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN.

SWMATRIZ# **copy running-config Startup-config**

Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

Destinación filename [startup-config]? Yes

El siguiente mensaje significa que se esta guardando la configuración

```
Building configuration...
[OK]
```

5.8.12 HOSTNAME Y PASSWORD

Para configurar el nombre del router se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre >.Para salir del modo de configuración global con el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

Switch>**enable**
Switch #

Entrar a la configuración global con el comando **configure Terminal**:

Switch # **configure Terminal**

Una vez ingresado el comando" **configure Terminal**" aparecerá este msj. El cual dirá que está dentro de la configuración global y que para salir deberá presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME <nombre>** se cambia el nombre a nuestro router:

Switch # **hostname** SWMATRIZ
SWMATRIZ#

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

SWMATRIZ#

El router posee niveles de seguridad para que solo los administradores puedan configurar dichos dispositivos. Existen dos formas de colocar password en el router:

De modo USER EXEC con el comando "**line console 0**" seguido respectivo "**password**"<nombre del password> y "**login**"

De modo PRIVILEGED EXEC con el comando "**line vty 0 15**" seguido respectivo "**password**"<nombre del password> y "**login**".

A NIVEL DE USUARIO

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWMATRIZ >**enable**
SWMATRIZ #

Entrar a la configuración global con el comando **configure Terminal**:

SWMATRIZ # **configure Terminal**
SWMATRIZ (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z.

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line console 0** para establecer una contraseña de conexión en el Terminal de consola.

SWMATRIZ (config)#**Line console 0**

Digitar el comando **password** seguido de la contraseña

SWMATRIZ (config)#**Password** cisco

Después digitar el comando **login** el cual habilitara la petición de contraseña al usuario.

SWMATRIZ (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

SWMATRIZ#

A NIVEL DE USUARIO PRIVILEGIADO

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWMATRIZ >**enable**
SWMATRIZ #

Entrar a la configuración global con el comando **configure Terminal**:

SWMATRIZ # **configure Terminal**
SWMATRIZ (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line vty 0 15** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

SWMATRIZ (config)#**Line vty 0 15**

Digitar el comando **Password** seguido de la contraseña

SWMATRIZ (config)#**Password** cisco

Después digitar el comando **login** el cual habilitara la petición de contraseña al usuario.

SWMATRIZ (config)#**Login**

Digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la clave.

SWMATRIZ (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

SWMATRIZ#

5.8.13 IP ADRESS

Se le puede otorgar al switch una dirección IP para fines de administración. Esto se configura en la interfaz virtual, VLAN 1. Por defecto, el switch no tiene dirección IP.

Los puertos o interfaces del switch se establecen en modo automático y todos los puertos de switch están en VLAN 1. VLAN 1 se conoce como la VLAN de administración por defecto.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWMATRIZ> **enable**
SWMATRIZ#

Entrar a la configuración global con el comando **configure Terminal**:

SWMATRIZ # **configure Terminal**
SWMATRIZ(config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Ingresar al modo de configuración de interfaz con el comando **interface vlan 1**:

SWMATRIZ(config)#**interface vlan 1**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

SWMATRIZ(config)#**ip address** 192.168.1.2 255.255.255.240

Ahora digitar el comando **no shutdown** para levantar la interfase:

SWMATRIZ (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

SWMATRIZ#(config)#

5.8.14 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.

5.8.14.1 TIPOS DE VLANS

Existen 3 tipos de vlans:

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

5.8.14.2 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).

5.8.14.3 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.

5.8.14.4 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 d.C.

5.8.15 CONFIGURACIÓN DE VLANS

Para configurar las vlans se debe estar 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** <número de vlan> **name** <nombre>"por último para salir de la configuración se debe digitar el comando **"exit"**.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWMATRIZ>**enable**
SWMATRIZ #

Entrar a la configuración de vlan con el comando **vlan database**:

SWMATRIZ # **vlan database**
SWMATRIZ (vlan)#

Digitar el comando **vlan**<número> seguia de **name** y el nombre de la vlan:

SWMATRIZ (vlan)# **vlan 10** name **SISTEMAS**

Digitar **exit** para salir del modo de configuración de vlan.

SWMATRIZ (vlan)#**exit**
SWMATRIZ #

5.8.16 ASIGNAR PUERTOS A UNA VLAN

Las vlans pueden tener uno o varios puertos asignados, para asignar un puerto a la vlan se debe estar en el modo de configuración glogal 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 <número de vlan>** "y por último para salir de modo de configuración global digitar el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWMATRIZ >**enable**
SWMATRIZ #

Entrar a la configuración global con el comando **configure Terminal**:

SWMATRIZ # **configure Terminal**
SWMATRIZ (Config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Ingresar a la interfaz fastethernet a la cual va hacer asignada a la vlan con el comando **interface fastethernet 0/2**:

SWMATRIZ (Config)#**interface fastethernet 0/2**
SWMATRIZ (config-if)#

Asignar el puerto a la vlan con el siguiente comando **switchport access vlan 10**:

SWMATRIZ (config-if)#**switchport access vlan 10**

Digitar **exit** para salir del modo de configuración de vlan.

SWMATRIZ (config-if)#**exit**
SWMATRIZ #

5.8.17 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.

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**", para digitar la linea de comando " **vtp < Server o client>**" después digtar el comando "**vtp domain <nombre del dominio>**" y para salir digitar el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWMATRIZ >**enable**
SWMATRIZ #

Entrar a la configuración de vlan con el comando **vlan database**:

SWMATRIZ # **vlan database**
SWMATRIZ (vlan)#

Para cambiar el tipo del switch a server se debe digitar el comando **vtp server** :

SWMATRIZ (vlan)# **vtp Server**

Digitar el comando **vtp domanin** para agregar al switch a un dominio.

SWMATRIZ (vlan)# **vtp domain topico**

Digitar **exit** para salir del modo de configuración de vlan.

SWMATRIZ (vlan)# **exit**
SWMATRIZ #

5.8.18 COMUNICACIÓN ENTRE VLANS

Por último en el router principal se debe ingresar al modo de configuración global para a su vez ingresar a la interfaz ethernet con el comando "**interface ethernet<número de interfaz>**", luego levantar la interface con el comando "**no shutdown**" después ingresar a la sub interface ethernet con el comando "**interface ethernet<número de interfaz. número de subinterfaz>**" para digitar 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, masc**" y por último para salir del modo de configuración global digitar el comando "**exit**".

Entrar al modo de configuración global con el comando **configure terminal**

MATRIZ# **configure terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z.

Digitar el comando **interface FastEthernet1/0.1** para configurar la sub interfaz

MATRIZ (config)#**interface fastethernet1/0.1**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **1** ya que es la vlan por defecto:

MATRIZ (config-if)#**encapsulation dot1q 1**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.1.1 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.2** para configurar la sub interfaz

MATRIZ (config)#**interface fastethernet1/0.2**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **10:**

MATRIZ (config-if)#**encapsulation dot1q 10**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ (config-if)#**ip address** 192.168.1.17 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.3** para configurar la sub interfaz

MATRIZ (config)#**interface fastethernet1/0.3**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **20:**

MATRIZ (config-if)#**encapsulation dot1q 20**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.1.33 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.4** para configurar la sub interfaz

MATRIZ (config)#**interface fastethernet1/0.4**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **30:**

MATRIZ (config-if)#**encapsulation dot1q 30**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ (config-if)#**ip address** 192.168.1.49 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.5** para configurar la sub interfaz

MATRIZ (config)#**interface fastethernet1/0.5**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **40:**

MATRIZ (config-if)#**encapsulation dot1q 40**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.1.65 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ(config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.6** para configurar la sub interfaz

MATRIZ(config)#**interface fastethernet1/0.6**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **50:**

MATRIZ (config-if)#**encapsulation dot1q 50**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.1.81 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ(config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.7** para configurar la sub interfaz

MATRIZ(config)#**interface fastethernet1/0.7**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **60:**

MATRIZ (config-if)#**encapsulation dot1q 60**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.1.97 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ(config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.8** para configurar la sub interfaz

MATRIZ(config)#**interface fastethernet1/0.8**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es 70:

MATRIZ (config-if)#**encapsulation dot1q 70**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.1.113 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ(config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.9** para configurar la sub interfaz

MATRIZ(config)#**interface fastethernet1/0.9**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **80:**

MATRIZ (config-if)#**encapsulation dot1q 80**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

MATRIZ(config-if)#**ip address** 192.168.1.129 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

MATRIZ(config-if)#**no shutdown**

Después de haber ingresado lo anterior aparecerá el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica, y detecta si el router adyacente esta en línea.

%LINEPROTO-5-UPDOWN: Line protocol on Interface fastethernet2/0, changed state to up
%LINK -3-UPDOWN: Interface fastethernet2/0, changed state to up

5.8.19 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**".

SWMATRIZ# delete flash: vlan.database.

5.8.20 COMANDO SHOW

Los numerosos comandos show se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas.

Show interfaces serial 0/1 .- muestra la estadística completa del router
Show controllers serial 0/1 .- muestra la información del hardware
Show clock .- muestra la hora fijada en el router
Show hosts .- muestra la lista en cache de los nombres de host y sus direcciones.
Show users .- muestra todos los usuario conectados al router.
Show version.- despliega la información acerca del router y de la versión del IOS que este corriendo en la RAM.
Show protocols. .- muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.
Show startup-configuartion .- muestra el archivo de configuración almacenado en la NVRAM.
Show running-configuration .- muestra el contenido del archivo de configuración activo.
Show ip route .- muestra las interfaces por las que se llega a otras redes mediantes los protocolos de enrutamiento ej: O:ospf, R:rip, C: directamente conectado
Show vlans.- muestra todas las vlans creadas con sus respectivos puertos asignados.

5.8.21 SHOW RUNNING

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

MATRIZ#show running-config
Building configuration...

Password:
Enter password:
Frontera1>enable
Enter password:
Version 12.1 ---------- Indica la versión del IOS
service timestamps debug uptime
service timestamps log uptime
service password-encryption
hostname MATRIZ---------- Refleja el nombre que el administrador le ha asigando a un router

enable secret 5 sdf6978yhg$jnb76sd ---- Este comando proporciona mayor seguridad Almacenando la contraseña con una función Criptográfica irreversible.
No se puede recuperar una contraseña perdida que ha sido cifrada por cualquier método.

Enable password CISCO ---------- Permite fijar una contraseña local para controlar el acceso a los varios niveles del privilegio, utilice el comando global de la configuración de la contraseña del permitir. Para quitar el requisito de la contraseña se antepone la palabra no al comando.

ip subnet-zero

Interface Serial0 ---------- Para fijar las direcciones IP de una interfaz utilice el comando IP Address. Para quitar las direcciones especificadas, utilice la forma negativa de este comando.

ip address 192.168.0.17 255.255.255.252--- Máscara de red del segmento utilizado
no ip directed-broadcast

```
 bandwidth 1544 ------------------------------
```

Para fijar un valor del ancho de banda de la Interfaz, se utiliza el comando Bandwitch en la configuración de la misma.
El valor mostrado es el que por defecto se le asigna a cada una de ellas.

```
!
interface Serial1
 ip address 192.168.0.1 255.255.255.252
 no ip directed-broadcast
 bandwidth 1544
!
interface Serial2
 no ip address
 no ip directed-broadcast
 bandwidth 1544
!
interface Serial3
 ip address 192.168.0.6 255.255.255.252
 no ip directed-broadcast
 clock rate 56000
 bandwidth 1544
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 ip access group 2 out
 bandwidth 10000
!
interface Ethernet0.1
encapsulation dot1q 1 -------------------------
```

IEEE 802.1Q es un protocolo estándar para interconectar los switches y routers y para definir topologías de VLAN.

```
 ip address 192.168.1.1 255.255.255.240
!
interface Ethernet0.2
 encapsulation dot1q 10
 ip address 192.168.1.17 255.255.255.240
!
interface Ethernet0.3
 encapsulation dot1q 20
 ip address 192.168.1.33 255.255.255.240
!
interface Ethernet0.4
 encapsulation dot1q 30
 ip address 192.168.1.49 255.255.255.240
!
interface Ethernet0.5
 encapsulation dot1q 40
 ip address 192.168.1.65 255.255.255.240
!
```

```
interface Ethernet0.6
 encapsulation dot1q 50

ip address 192.168.1.81 255.255.255.240
!
interface Ethernet0.7
 encapsulation dot1q 60
 ip address 192.168.1.97 255.255.255.240
!
interface Ethernet0.8
 encapsulation dot1q 70
 ip address 192.168.1.113 255.255.255.240
!
interface Ethernet0.9
 encapsulation dot1q 80
 ip address 192.168.1.129 255.255.255.240
!
!



router rip

 version 2
 redistribute OSPF 1
 default-metric 10
 network 192.168.0.0
 network 192.168.1.0
!
router ospf 1 ----------------------------------------
 redistribute RIP
 network 192.168.0.16 0.0.0.3 area 0
 network 192.168.0.0 0.0.0.3 area 0
 network 192.168.0.12 0.0.0.3 area 0
 network 192.168.0.4 0.0.0.3 area 0
!
ip classless
no ip http server
access-list 2 permit host 192.168.10.12
access-list 2 deny any any



!
line con 0
```

Para definir los interfaces con las cuales está trabajado OSPF y la identificación del área para esos interfaces, se utilizan estos comandos.
Area especifica el área para asociarse a la dirección de red.

```
login ----------------------------------------------
 transport input none
 password cisco

line aux 0


line vty 0 4
 login

 password cisco
!
no scheduler allocate
end
```

Para permitir la contraseña que comprueba la conexión, utilice el comando Login.En caso de querer inhabilitar la contraseña se antepone la negación al comando.

5.8.22 SHOW IP ROUTE

Muestra el contenido de una tabla d 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 metrica]
via a,b,c,d: dirección de interfaz a la que llega.
serial: nombre de la interface saliente.

MATRIZ # Show ip route

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

Gateway of last resort is not set

192.168.0.0/0 is variably subnetted, 12 subnets
C 192.168.0.16/30 is directly connected, Serial0
C 192.168.0.0/30 is directly connected, Serial1
C 192.168.0.12/30 is directly connected, Serial2
C 192.168.0.4/30 is directly connected, Serial3
O 192.168.0.20/30 [110/64] via 192.168.0.21, 00:49:41, Serial3
O 192.168.0.8/30 [110/64] via 192.168.0.5, 00:49:41, Serial3
R 192.168.0.48/30 [120/1] via 192.168.0.18, 00:05:24, Serial0
R 192.168.0.24/30 [120/1] via 192.168.0.2, 00:06:18, Serial1
R 192.168.0.32/30 [120/1] via 192.168.0.2, 00:09:30, Serial1
R 192.168.0.36/30 [120/2] via 192.168.0.2, 00:02:37, Serial1
is directly connected, is directly connected,

5.8.23 SHOW VLAN

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	10	active	Fa0/2
20	20	active	Fa0/3
30	30	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

5.9 ROUTER GALÁPAGOS

5.9.1 MODOS DE CONFIGURACIÓN DEL ROUTER

Al acceder al router por seguridad tiene dos niveles de acceso a los comandos:

- USER EXEC
- PRIVILEGED EXEC

En modo USER EXEC se puede consultar aspectos básicos de la configuración del router. Para consultar aspectos más críticos de la configuración del router se debe pasar a modo PRIVILEGED EXEC. Para pasar de modo USER EXEC a modo PRIVILEGED EXEC es necesario digitar el comando "**enable**".

En el modo USER EXEC el prompt que muestra el router es ">". En el modo PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#.

```
Router>                          modo configuración global
Router> enable

Router#                          modo usuario privilegiado
Router# exit
Router>
```

Desde los modos USER EXEC y PRIVILEGED EXEC no se puede modificar la configuración del router. Para hacerlo, se debe pasar del modo PRIVILEGED EXEC al modo de configuración global (CONFIGURE TERMINAL). Desde allí se puede configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc. y para salir de estos modos de configuración se debe digitar el comando "**exit**".

5.9.1.1 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc el prompt que muestra es "Router(config)#"

```
Router>
Router> enable

Router# configure terminal       modo configuración global
Router(config)#exit
Router#
```

5.9.1.2 MODO DE CONFIGURACIÓN ESPECÍFICOS

Permiten configurar protocolos, interfaces o en general aspectos más complejos del router. El prompt que aparece es R(config-if)#, R(config-route)#.

5.9.2 GUARDAR CAMBIOS EN EL ROUTER

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en la RAM del switch llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el switch se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

> Con el comando **copy running-config Startup-config** se guarda cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN.

Router # **copy running-config Startup-config**

> Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

Destination filename [startup-config]? Yes

> El siguiente mensaje significa que se esta guardando la configuración

Building configuration...
[OK]

5.9.3 ASIGNAR NOMBRE A UN ROUTER

Una de las primeras tareas de configuración basica es asignar un nombre al router. El nombrado de un router ayuda a una mejor administración de la red al identificar unívocamente cada uno de los router en la red.

Para configurar el nombre del router se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre >.Para salir del modo de configuración global con el comando "**exit**"

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

Router>**enable**
Router #

Entrar a la configuración global con el comando **configure Terminal**

Router # **configure Terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME GALÁPAGOS** se cambia el nombre al router.

Router # **hostname** GALÁPAGOS
GALÁPAGOS #

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

GALÁPAGOS #

5.9.4 CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER

Un router puede ser asegurado mediante el uso de contraseñas para restringir el acceso. Las contraseñas pueden establecerse para las líneas de Terminal virtual y la línea de consola.
El modo de configuración **line console 0** puede utilizarse para establecer una contraseña de conexión en el Terminal de consola, lo que resulta util en un red en la que hay muchas personas que tienen acceso al router.
El modo de configuración **line vty 0 4** sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

A NIVEL DE USUARIO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

GALÁPAGOS >**enable**
GALÁPAGOS #

Entrar a la configuración global con el comando **configure terminal**:

GALÁPAGOS # **configure Terminal**
GALÁPAGOS (config)#

Digitar el comando **line console 0** para establecer una contraseña de conexión en el Terminal de consola.

GALÁPAGOS (config)#**Line console 0**

Ahora proceder a digitar el comando **password** seguido de la contraseña

GALÁPAGOS (config)#**Password** cisco

Después digitar el comando **login** el cual habilitará la petición de contraseña al usuario

GALÁPAGOS (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

GALÁPAGOS #

A NIVEL DE USUARIO PRIVILEGIADO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

GALÁPAGOS >**enable**
GALÁPAGOS #

Entrar a la configuración global con el comando **configure terminal**:

GALÁPAGOS # **configure Terminal**
GALÁPAGOS (config)#

Digitar el comando **line vty 0 4** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

GALÁPAGOS (config)#**Line vty 0 4**

Ahora proceder a digitar el comando **Password** seguido de la contraseña

GALÁPAGOS (config)#**Password** cisco

Después digitar el comando **login** el cual permitirá aceptar nuestra clave.

GALÁPAGOS (config)#**Login**

Por último digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la contraseña.

GALÁPAGOS (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

GALÁPAGOS #

5.9.5 CONFIGURACIÓN DE INTERFACES

Desde el modo de configuración global se puede pasar a configurar las interfaces. Para configurar una interfase siga los siguientes pasos:

- Entrar al modo de configuración global
- Entrar al modo de configuración de interfaz
- Especifique la dirección ip seguida de su máscara de subred
- Active la interfaz

Por ejemplo, para configurar un interface ethernet se debe hacer de la siguiente manera:

```
Router# configure terminal
Router(config)# interface <eth0 >          modo configuración de intefaz
Router(config-if)# ip address <IP MASK>
Router(config-if)# no shutdown
Router(config-if)# exit
Router#
```

El commando "**no shutdown**" es necesario para activar la interfaz. Por defecto, al arrancar el router todos los interfaces están desactivados. El comando "**shutdown**" en su defecto desactivaría administrativamente una interfaz.

Las interfaces serial están diseñadas para que en la situación más normal se conecten a una operadora de telecomunicaciones a través de un DCE (e.g.; un MODEM o una Terminación de Red, TR). El DCE es el que normalmente da reloj y por tanto fija la velocidad de modulación y por consiguiente de transmisión.

Si se conectan dos puertos serie de router (DTE-DTE) hay que usar un cable cruzado. Además uno de los dos puertos tiene que actuar como DCE dando reloj. En principio desde el punto de vista de router cualquiera de los dos puede actuar de DCE, así que lo importante es que conector del cable es el que marca que puerto es DCE.

5.9.5.1 INTERFACES SERIALES

Una vez que se sabe que puerto es el que actúa de DCE, tiene que dar reloj. Está opción la tendrá que activar vía IOS con el comando "**clockrate Bw**", donde **Bw** son los bps con los que va a trabajar la línea. En el puerto DTE no se deberá activar este comando.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

```
GALAPAGOS>enable
GALAPAGOS #
```

Entrar a la configuración global con el comando **configure terminal**:

GALÁPAGOS # **configure Terminal**
GALÁPAGOS (config)#

Ingresar al modo de configuración de interfaz con el comando **interface serial 0/0**:

GALÁPAGOS (config)#**interface serial 0/0**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

GALÁPAGOS (config)#**ip address** 192.168.0.49 255.255.255.252

Ahora digitar el comando **no shutdown** para levantar la interface:

GALÁPAGOS (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

GALÁPAGOS #(config)#

Ahora ingresar a la **interface serial 0/1**

GALÁPAGOS (config)#**interface serial 0/1**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

GALÁPAGOS (config)#**ip address** 192.168.0.18 255.255.255.252

Como esta interfaz es DCE entonces fije la velocidad de sincronización en bips/seg 1con el comando **clock rate.** Omita este paso si la interfaz es DTE:

GALÁPAGOS (config-if)# **clockrate 56000**

Ahora digitar el comando **no shutdown** para levantar la interface:

GALÁPAGOS (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

GALÁPAGOS #(config)#

5.9.5.2 INTERFACES ETHERNET

Un interfaz ethernet se configura desde en modo consola. Cada intefaz ethernet debe tener una dirección IP y una máscara de subred.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

GALÁPAGOS>**enable**
GALÁPAGOS #

Entrar a la configuración global con el comando **configure terminal**:

GALÁPAGOS # **configure Terminal**
GALÁPAGOS (config)#

Ingresar al modo de configuración de interfaz con el comando **interface ethernet 0/0**:

GALÁPAGOS (config)#**interface ethernet 0/0**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address** pero en este caso solamente se levanta la interface sin ponerle dirección ip.

Ahora digitar el comando **no shutdown** para levantar la interface:

GALÁPAGOS (config-if)# **no shutdown**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

GALÁPAGOS #

5.9.6 CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO

El Protocolo de enrutamiento es aquel que suministra los mecanismos necesarios para compartir la información de enrutamiento. Los mensajes de un protocolo de enrutamiento se mueven entre los routers. Un protocolo de enrutamiento permite a los routers comunicarse con otros routers para actualizar y mantener sus tablas. A continuación se muestra diversos protocolos de enrutamiento:

- RIP (protocolo de información de enrutamiento)
- OSPF (primero la ruta libre mas corta)
- IGRP (protocolo de enrutamiento de gateway interior)

5.9.6.1 PROTOCOLO RIP VERSION 2(VECTOR DISTANCIA)

Es un protocolo de enrutamiento por vector-distancia, que 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, primero se debe cambiar al modo de configuración global, luego se debe establecer con una o más órdenes "**network**", las redes directamente conectadas al router.y finalmente para salir digitar el comando "**exit**".A continuación se mostrará la configurarción del router GALÁPAGOS con el protocolo rip vs 2:

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

GALÁPAGOS>**enable**
GALÁPAGOS #

Entrar a la configuración global con el comando **configure Terminal**:

GALÁPAGOS # **configure Terminal**
GALÁPAGOS (config)#

Ingresar la configuración del protocolo Rip con el comando **router rip**:

GALÁPAGOS (config)# **router rip**

Ingresar la **version 2**

GALÁPAGOS (config-router)#**version 2**

Ingresar la dirección de red que esta configurada con RIP con el comando **network**:

GALÁPAGOS (config-router)# **network** 192.168.0.0
GALÁPAGOS (config-router)# **network** 192.168.1.0

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

GALÁPAGOS #

5.9.7 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. En el modo USER EXEC el prompt que muestra el switch es ">".En el modo PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#,

```
switch >                          modo usuario
switch > enable

switch #                          modo usuario privilegiado
switch # exit
switch >
```

5.9.7.1 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del switch como pueden ser la configuración del nombre del switch, passwords, etc (prompt R(config)#)

```
switch >
switch > enable

switch # configure terminal       modo configuración global
switch (config)#exit
switch #
```

5.9.8 GUARDAR CAMBIOS EN EL SWITCH

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o especifico se guardan sobre un archivo de configuración residente en la RAM del switch llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el switch se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

Con el comando **copy running-config Startup-config** se guarda cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN.

Switch# **copy running-config Startup-config**

Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

Destination filename [startup-config]? Yes

El siguiente mensaje significa que se esta guardando la configuración

Building configuration...
[OK]

5.9.9 HOSTNAME Y PASSWORD

Para configurar el nombre del switch lo se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre > para salir del modo de configuración global digitar el comando "**exit**"

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

Switch>**enable**
Switch #

Entrar a la configuración global con el comando **configure terminal**:

Switch # **configure Terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME <nombre>** se cambia el nombre al router:

Switch # **hostname** SWGALÁPAGOS
SWGALÁPAGOS #

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

SWGALÁPAGOS #

El router posee niveles de seguridad para que solo los administradores puedan configurar dichos dispositivos. Existen dos formas de colocar password en el router:

De modo USER EXEC con el comando "**line console 0**" seguido respectivo "**password**"<nombre del password> y "**login**"

De modo PRIVILEGED EXEC con el comando "**line vty 0 15**" seguido respectivo "**password**"<nombre del password> y "**login**".

A NIVEL DE USUARIO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

SWGALÁPAGOS >**enable**
SWGALÁPAGOS #

Entrar a la configuración global con el comando **configure terminal**:

SWGALÁPAGOS # **configure Terminal**
SWGALÁPAGOS (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line console 0** para establecer una contraseña de conexión en el Terminal de consola.

SWGALÁPAGOS (config)#**Line console 0**

Ahora proceder a digitar el comando **password** seguido de la contraseña

SWGALÁPAGOS (config)#**Password** cisco

Después digitar el comando **login** el cual habilitará la petición de contraseña al usuario.

SWGALÁPAGOS (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global.

SWGALÁPAGOS #

A NIVEL DE USUARIO PRIVILEGIADO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

SWGALÁPAGOS >**enable**
SWGALÁPAGOS #

Entrar a la configuración global con el comando **configure terminal**:

SWGALÁPAGOS # **configure Terminal**
SWGALÁPAGOS (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line vty 0 15** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

SWGALÁPAGOS (config)#**Line vty 0 15**

Ahora proceder a digitar el comando **Password** seguido de la contraseña

SWGALÁPAGOS (config)#**Password** cisco

Después digitar el comando **login** el cual habilitará la petición de contraseña al usuario

SWGALÁPAGOS (config)#**Login**

Por último Digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la clave.

SWGALÁPAGOS (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

SWGALÁPAGOS #

5.9.10 IP ADRESS

Se le puede otorgar al switch una dirección IP para fines de administración. Esto se configura en la interfaz virtual, VLAN 1. Por defecto, el switch no tiene dirección IP.

Los puertos o interfaces del switch se establecen en modo automático y todos los puertos de switch están en VLAN 1. VLAN 1 se conoce como la VLAN de administración por defecto.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWGALÁPAGOS > **enable**
SWGALÁPAGOS #

Entrar a la configuración global con el comando **configure terminal**:

SWGALÁPAGOS # **configure Terminal**
SWGALÁPAGOS (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Ingresar al modo de configuración de interfaz con el comando **interface vlan 1**:

SWGALÁPAGOS (config)#**interface vlan 1**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

SWGALÁPAGOS (config-if)#**ip address** 192.168.11.2 255.255.255.240

Ahora Digitar el comando **no shutdown** para levantar la interface:

SWGALÁPAGOS (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

SWGALÁPAGOS#

5.9.11 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.

5.9.11.1 TIPOS DE VLANS

Existen 3 tipos de vlans:

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

5.9.11.2 VLANS POR PUERTO

El metodo 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 dimanico (DHCP).

5.9.11.3 VLANS POR DIRECCIONES MAC

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

5.9.11.4 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.

5.9.12 CONFIGURACIÓN DE VLANS

Para configurar las vlans se debe estar 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** <número de vlan> **name** <nombre>"por último para salir de la configuración se debe digitar el comando **"exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

```
SWGALAPAGOS >enable
SWGALAPAGOS #
```

Entrar a la configuración de vlan con el comando **vlan database**:

```
SWGALAPAGOS # vlan database
SWGALAPAGOS (vlan)#
```

Digitar el comando **vlan**<número> seguido de **name** y el nombre de la vlan:

```
SWGALAPAGOS (vlan)# vlan 20 name SISTEMAS
```

Digitar **exit** para salir del modo de configuración de vlan.

```
SWGALAPAGOS (vlan)#exit
SWGALAPAGOS #
```

5.9.13 ASIGNAR PUERTOS A UNA VLAN

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

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWGALÁPAGOS >**enable**
SWGALÁPAGOS #

Entrar a la configuración global con el comando **configure Terminal**:

SWGALÁPAGOS # **configure Terminal**
SWGALÁPAGOS (Config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z

Ingresar a la interfaz fastethernet a la cual va hacer asignada a la vlan con el comando **interface fastethernet 0/2**:

SWGALÁPAGOS (Config)#**interface fastethernet 0/2**
SWGALÁPAGOS (config-if)#

Asignar el puerto a la vlan con el siguiente comando **switchport access vlan 10**:

SWGALÁPAGOS (config-if)#**switchport access vlan 20**

Digitar **exit** para salir del modo de configuración de vlan.

SWGALÁPAGOS (config-if)#**exit**
SWGALÁPAGOS #

5.9.14 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.

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 linea de comando "**vtp < Server o client>**" después digtar el comando "**vtp domain <nombre del dominio>**" y por último para salir de la configuración digitar el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado.

SWGALAPAGOS >**enable**
SWGALAPAGOS #

Entrar a la configuración de vlan con el comando **vlan database**:

SWGALAPAGOS # **vlan database**
SWGALAPAGOS (vlan)#

Para cambiar el tipo del switch a server se debe digitar el comando **vtp server**:

SWGALAPAGOS (vlan)# **vtp Server**

Digitar el comando **vtp domanin** para agregar al switch a un dominio:

SWGALAPAGOS (vlan)# **vtp domain topico**

Digitar **exit** para salir del modo de configuración de vlan.

SWGALAPAGOS (vlan)# **exit**
SWGALAPAGOS #

5.9.15 COMUNICACIÓN ENTRE VLANS

Por último en el router principal se debe ingresar al modo de configuración global para a su vez ingresar a la interfaz ethernet con el comando "**interface ethernet<número de interfaz>**", luego levantar la interface con el comando "**no shutdown**" después ingresar a la sub interface ethernet con el comando "**interface ethernet<número de interfaz. número de subinterfaz>**" para digitar 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, masc**" y por último para salir del modo de configuración global digitar el comando "**exit**".

Entrar a la configuración global con el comando **configure Terminal**:

GALÁPAGOS# **configure terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z

Enter configuration commands, one per line. End with CNTL/Z.

Digitar el comando **interface FastEthernet1/0.1** para configurar la sub interfaz

GALÁPAGOS (config)#**interface fastethernet1/0.1**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **1** ya que es la vlan por defecto:

GALÁPAGOS (config-if)#**encapsulation dot1q 1**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

GALÁPAGOS (config-if)#**ip address** 192.168.11.1 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

GALÁPAGOS (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.2** para configurar la sub interfaz

GALÁPAGOS (config)#**interface fastethernet1/0.2**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **10:**

GALÁPAGOS (config-if)#**encapsulation dot1q 10**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

GALÁPAGOS (config-if)#**ip address** 192.168.11.17 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**.

GALÁPAGOS (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.3** para configurar la sub interfaz

GALÁPAGOS (config)#**interface fastethernet1/0.3**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **20:**

GALÁPAGOS (config-if)#**encapsulation dot1q 20**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

GALÁPAGOS (config-if)#**ip address** 192.168.11.33 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

GALÁPAGOS (config-if)#**no shutdown**

Después de haber ingresado lo anterior aparecerá el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica, y detecta si el router adyacente esta en línea.

%LINEPROTO-5-UPDOWN: Line protocol on Interface fastethernet2/0, changed state to up
%LINK -3-UPDOWN: Interface fastethernet2/0, changed state to up

5.9.16 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**".

SWGALÁPAGOS # delete flash: vlan.database.

5.9.17 COMANDO SHOW

Los numerosos comandos show se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas.

Show interfaces serial 0/1 .- muestra la estadística completa del router
Show controllers serial 0/1 .- muestra la información del hardware
Show clock .- muestra la hora fijada en el router
Show hosts .- muestra la lista en cache de los nombres de host y sus direcciones.
Show users .- muesra todos los usuario conectados al router.
Show version.- despliega la información acerca del router y de la versión del IOS que este corriendo en la RAM.
Show protocols. .- muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.
Show startup-configuartion .- muestra el archivo de configuración almacenado en la NVRAM.
Show running-configuration .- muestra el contenido del archivo de configuración activo.
Show ip route .- muestra las interfaces por las que se llega a otras redes mediantes los protocolos de enrutamiento ej: O:ospf, R:rip, C: directamente conectado
Show vlans.- muestra todas las vlans creadas con sus respectivos puertos asignados.

5.9.18 SHOW RUNNING GALÁPAGOS

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

Building configuration...

Password:
Enter password:
Frontera1>enable
Enter password:
Version 12.1 ---------- Indica la versión del IOS
service timestamps debug uptime
service timestamps log uptime
service password-encryption
hostname GALÁPAGOS---------- Refleja el nombre que el administrador le ha asigando a un router

enable secret 5 sdf6978yhg$jnb76sd ---- *Este comando proporciona mayor seguridad* Almacenando la contraseña con una función Criptográfica irreversible.
No se puede recuperar una contraseña perdida que ha sido cifrada por cualquier método.

Enable password CISCO ---------- Permite fijar una contraseña local para controlar el acceso a los varios niveles del privilegio, utilice el comando global de la configuración de la contraseña del permitir. Para quitar el requisito de la contraseña se antepone la palabra no al comando.

ip subnet-zero

interface Serial0 ---------- Para fijar las direcciones IP de una interfaz utilice el comando IP Address. Para quitar las direcciones especificadas, utilice la forma negativa de este comando.

ip address 192.168.0.49 255.255.255.252--- Máscara de red del segmento utilizado
no ip directed-broadcast
bandwidth 1544
!

interface Serial1

```
 ip address 192.168.0.18 255.255.255.252
 no ip directed-broadcast
 clock rate 56000
 bandwidth 1544 ------------------------------
!
interface Serial2
 no ip address
 no ip directed-broadcast
 bandwidth 1544
 shutdown
!
interface Serial3
 no ip address
 no ip directed-broadcast
 bandwidth 1544
 shutdown
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 bandwidth 10000
!
interface Ethernet0.1
 encapsulation dot1q 1------------------------
!
 ip address 192.168.11.1 255.255.255.240
!
interface Ethernet0.2
 encapsulation dot1q 10
 ip address 192.168.11.17 255.255.255.240
!
interface Ethernet0.3
 encapsulation dot1q 20
 ip address 192.168.11.33 255.255.255.240
!
!
```

Para fijar un valor del ancho de banda de la Interfaz, se utiliza el comando Bandwitch en la configuración de la misma.
El valor mostrado es el que por defecto se le asigna a cada una de ellas.

IEEE 802.1Q es un protocolo estándar para interconectar los switches y routers y para definir topologías de VLAN.

router rip ---------- Para definir los interfaces con las cuales está trabajado RIP y la identificación del área para esos interfaces, se utilizan estos comandos.

```
 version 2
 network 192.168.0.0
 network 192.168.1.0
!
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
```

Para permitir la contraseña que comprueba la conexión, utilice el comando Login.En caso de querer inhabilitar la contraseña se antepone la negación al comando.

5.9.19 SH IP ROUTE GALÁPAGOS

Muestra el contenido de una tabla d 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 metrica]
via a,b,c,d: dirección de interfaz a la que llega.
serial: nombre de la interface saliente

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

192.168.0.0/30 is subnetted, 6 subnets
R 192.168.0.48 [110/128] via 192.168.0.17, 00:51:17, Serial1
C 192.168.0.48 is directly connected, Serial0
C 192.168.0.16 is directly connected, Serial1
R 192.168.0.20 [110/192] via 192.168.0.17, 00:51:16, Serial1

5.9.20 SH VLANS GALÁPAGOS

Muestra todas las vlans creadas con sus respectivos puertos asignados

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
10	10	active	Fa0/2
20	20	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

5.10 ROUTER CENTRO

5.10.1 MODOS DE CONFIGURACIÓN DEL ROUTER

Al acceder al router por seguridad tiene dos niveles de acceso a los comandos:

- USER EXEC
- PRIVILEGED EXEC

En modo USER EXEC se puede consultar aspectos básicos de la configuración del router. Para consultar aspectos más críticos de la configuración del router se debe pasar a modo PRIVILEGED EXEC. Para pasar de modo USER EXEC a modo PRIVILEGED EXEC es necesario digitar el comando "**enable**".

En el modo USER EXEC el prompt que muestra el router es ">". En el modo PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#.

```
Router>                          modo usuario
Router> enable

Router#                          modo privilegiado
Router# exit
Router>
```

Desde los modos USER EXEC y PRIVILEGED EXEC no se puede modificar la configuración del router. Para hacerlo se debe pasar del modo PRIVILEGED EXEC al modo de configuración global (CONFIGURE TERMINAL). Desde allí se puede configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc. y para salir de estos modos de configuración se debe digitar el comando "**exit**"

5.10.1.1 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc el prompt que muestra es "Router(config)#"

```
Router>
Router> enable
Router# configure terminal       modo de configuración global
```

5.10.1.2 MODO DE CONFIGURACIÓN ESPECÍFICOS

Permiten configurar protocolos, interfaces o en general aspectos más complejos del router. El prompt que aparece es R(config-if)#, R(config-route)#.

5.10.2 GUARDAR CAMBIOS EN EL ROUTER

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o especifico se guardan sobre un archivo de configuración residente en la RAM del switch llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el router se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

> Con el comando **copy running-config Startup-config** se guarda cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN:

Router # **copy running-config Startup-config**

> Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

Destination filename [startup-config]? Yes

> El siguiente mensaje significa que se esta guardando la configuración:

Building configuration...
[OK]

5.10.3 ASIGNAR NOMBRE A UN ROUTER

Una de las primeras tareas de configuración básica es asignar un nombre al router. El nombrado de un router ayuda a una mejor administración de la red al identificar unívocamente cada uno de los router en la red.

Para configurar el nombre del router se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre >.Para salir del modo de configuración global con el comando "**exit**".

Cambiar de modo usuario a modo privilegiado con el comando **enable:**

Router>**enable**
Router #

Entrar a la configuración global con el comando **configure Terminal:**

Router # **configure Terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z.

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME <nombre>** se cambia el nombre al router:

Router # **hostname** CENTRO
CENTRO#

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

CENTRO#

5.10.4 CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER

Un router puede ser asegurado mediante el uso de contraseñas para restringir el acceso. Las contraseñas pueden establecerse para las líneas de Terminal virtual y la línea de consola.
El modo de configuración **line console 0** puede utilizarse para establecer una contraseña de conexión en el Terminal de consola, lo que resulta útil en un red en la que hay muchas personas que tienen acceso al router.
El modo de configuración **line vty 0 4** sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

A NIVEL DE USUARIO


Cambiar de modo usuario a modo privilegiado con el comando **enable**:

CENTRO >**enable**
CENTRO #


Entrar a la configuración global con el comando **configure terminal**:

CENTRO # **configure Terminal**
CENTRO (config)#


Digitar el comando **line console 0** para establecer una contraseña de conexión en el Terminal de consola:

CENTRO (config)#**Line console 0**


Ahora proceder a digitar el comando **password** seguido de la contraseña:

CENTRO (config)#**Password** cisco


Después digitar el comando **login** el permitirá aceptar nuestra clave:

CENTRO (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

CENTRO #

A NIVEL DE USUARIO PRIVILEGIADO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

CENTRO >**enable**
CENTRO #

Entrar a la configuración global con el comando **configure terminal**:

CENTRO # **configure Terminal**
CENTRO (config)#

Digitar el comando **line vty 0 4** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes:

CENTRO (config)#**Line vty 0 4**

Ahora proceder a digitar el comando **Password** seguido de la contraseña:

CENTRO (config)#**Password** cisco

Después Digitar el comando **login** el cual habilitara la petición de contraseña al usuario:

CENTRO (config)#**Login**

Por último digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la contraseña:

CENTRO (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

CENTRO #

5.10.5 CONFIGURACIÓN DE INTERFACES

Desde el modo de configuración global se puede pasar a configurar las interfaces. Para configurar una interface siga los siguientes pasos

- Entrar al modo de configuración global
- Entrar al modo de configuración de interfaz
- Especifique la dirección ip seguida de su máscara de subred
- *Active la interfaz*

Por ejemplo, para configurar un interface ethernet se debe hacer de la siguiente manera:

```
Router# configure terminal
Router(config)# interface <eth0 >          modo configuración de intefaz.
Router(config-if)# ip address <IP MASK>
Router(config-if)# no shutdown
Router(config-if)# exit
Router#
```

El commando "**no shutdown**" es necesario para activar la interfaz. Por defecto, al arrancar el router todos los interfaces están desactivados. El comando "**shutdown**" en su defecto desactivaría administrativamente una interfaz.

Las interfaces serial están diseñadas para que en la situación más normal se conecten a una operadora de telecomunicaciones a través de un DCE (e.g.; un MODEM o una Terminación de Red, TR). El DCE es el que normalmente da reloj y por tanto fija la velocidad de modulación y por consiguiente de transmisión.

Si se conectan dos puertos serie de router (DTE-DTE) hay que usar un cable cruzado. Además uno de los dos puertos tiene que actuar como DCE dando reloj. En principio desde el punto de vista de router cualquiera de los dos puede actuar de DCE, así que lo importante es que conector del cable es el que marca que puerto es DCE.

5.10.5.1 INTERFACES SERIALES

Una vez que se sabe que puerto es el que actúa de DCE, tiene que dar reloj. Está opción la tendrá que activar vía IOS con el comando "**clockrate Bw**", donde **Bw** son los bps con los que va a trabajar la línea. En el puerto DTE no se deberá activar este comando.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

CENTRO>**enable**
CENTRO #

Entrar a la configuración global con el comando **configure terminal**:

CENTRO # **configure Terminal**
CENTRO (config)#

Ingresar al modo de configuración de interfaz con el comando **interface serial 0/0**:

CENTRO (config)#**interface serial 0/0**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

CENTRO (config)#**ip address** 192.168.0.2 255.255.255.252

Como esta interfaz es DCE entonces fijar la velocidad de sincronización en bips/seg 1con el comando **clock rate.** Omita este paso si la interfaz es DTE:

CENTRO (config-if)# **clockrate 56000**

Ahora Digitar el comando **no shutdown** para levantar la interface:

CENTRO (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

CENTRO #(config)#

Ahora ingresar la **interface serial 0/1**

CENTRO (config)#**interface serial 0/1**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

CENTRO (config)#**ip address** 192.168.0.21 255.255.255.252

Ahora digitar el comando **no shutdown** para levantar la interface:

CENTRO (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

CENTRO #(config)#

Ahora ingresar la **interface serial 0/3**

CENTRO (config)#**interface serial 0/3**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

CENTRO (config)#**ip address** 192.168.0.34 255.255.255.252

Como esta interfaz es DCE entonces fijar la velocidad de sincronización en bips/seg con el comando **clock rate.** Omita este paso si la interfaz es DTE:

CENTRO (config-if)# **clockrate 56000**

Ahora digitar el comando **no shutdown** para levantar la interface:

CENTRO (config-if)# **no shutdown**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

CENTRO #

5.10.5.2 INTERFACES ETHERNET

Un interfaz ethernet se configura desde en modo consola. Cada intefaz ethernet debe tener una dirección IP y una máscara de subred.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

CENTRO >**enable**
CENTRO #

Entrar a la configuración global con el comando **configure terminal**:

CENTRO # **configure Terminal**
CENTRO (config)#

Ingresar al modo de configuración de interfaz con el comando **interface ethernet 0/0**:

CENTRO (config)#**interface ethernet 0/0**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address** pero en este caso solamente se levanta la interface sin ponerle dirección ip.

Ahora digitar el comando **no shutdown** para levantar la interface:

CENTRO (config-if)# **no shutdown**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

CENTRO#

5.10.6 CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO

El Protocolo de enrutamiento es aquel que suministra los mecanismos necesarios para compartir la información de enrutamiento. Los mensajes de un protocolo de enrutamiento se mueven entre los routers. Un protocolo de enrutamiento permite a los routers comunicarse con otros routers para actualizar y mantener sus tablas. A continuación se muestra diversos protocolos de enrutamiento:

- RIP (protocolo de información de enrutamiento)
- OSPF (primero la ruta libre mas corta)
- IGRP (protocolo de enrutamiento de gateway interior)

5.10.6.1 PROTOCOLO RIP VERSION 2(VECTOR DISTANCIA)

Es un protocolo de enrutamiento por vector-distancia, que 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, primero se debe cambiar al modo de configuración global, luego se debe establecer con una o más órdenes "**network**", las redes directamente conectadas al router.y finalmente para salir digitar el comando "**exit**" A continuación se muestra la configurarcion del router CENTRO con el protocolo rip vs 2:

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

CENTRO >**enable**
CENTRO #

Entrar a la configuración global con el comando **configure Terminal**:

CENTRO # **configure Terminal**
CENTRO (config)#

Ingresar a la configuración del protocolo Rip con el comando **router rip**:

CENTRO (config)# **router rip**

Ingresar la **version 2**

CENTRO (config-router)#**version 2**

Ingresar la dirección de red que esta configurada con RIP con el comando **network**:

CENTRO (config-router)# **network** 192.168.0.0
CENTRO (config-router)# **network** 192.168.1.0

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

CENTRO #

5.10.7 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. En el modo USER EXEC el prompt que muestra el switch es ">".En el modo PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#.

switch >
switch > enable

modo usuario.

switch #
switch # exit
switch >

modo usuario privilegiado.

5.10.8 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del switch como pueden ser la configuración del nombre del switch, passwords, etc (prompt R(config)#)

```
switch >
switch > enable
switch # configure terminal
switch (config)#exit
switch #
```

modo configuración global.

5.10.9 GUARDAR CAMBIOS EN EL SWITCH

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en la RAM del switch llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el switch se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

Con el comando **copy running-config Startup-config** se guarda cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN

Switch# **copy running-config Startup-config**

Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

```
Destination filename [startup-config]? Yes
```

El siguiente mensaje significa que se esta guardando la configuración

```
Building configuration...
[OK]
```

5.10.10 HOSTNAME Y PASSWORD

Para configurar el nombre del switch se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre >.Para salir del modo de configuración global con el comando "**exit**".

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

Switch>**enable**
Switch #

Entrar a la configuración global con el comando **configure terminal**:

Switch # **configure Terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME <nombre>** se cambia el nombre al switch:

Switch # **hostname** SWCENTRO
SWCENTRO #

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

SWCENTRO #

El router posee niveles de seguridad para que solo los administradores puedan configurar dichos dispositivos. Existen dos formas de colocar password en el router:

De modo USER EXEC con el comando "**line console 0**" seguido respectivo "**password**"<nombre del password> y "**login**"

De modo PRIVILEGED EXEC con el comando "**line vty 0 15**" seguido respectivo "**password**"<nombre del password> y "**login**".

A NIVEL DE USUARIO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

SWCENTRO >**enable**
SWCENTRO #

Entrar a la configuración global con el comando **configure terminal**:

SWCENTRO # **configure Terminal**
SWCENTRO (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line console** 0 para establecer una contraseña de conexión en el Terminal de consola.

SWCENTRO (config)#**Line console** 0

Ahora proceder a digitar el comando **password** seguido de la contraseña

SWCENTRO (config)#**Password** cisco

Después Digitar el comando **login** el cual habilitará la petición de contraseña al usuario:

SWCENTRO (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

SWCENTRO #

A NIVEL DE USUARIO PRIVILEGIADO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

SWCENTRO >**enable**
SWCENTRO #

Entrar a la configuración global con el comando **configure terminal**:

SWCENTRO # **configure Terminal**
SWCENTRO (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line vty 0 15** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes:

SWCENTRO (config)#**Line vty 0 15**

Ahora proceder a digitar el comando **Password** seguido de la contraseña:

SWCENTRO (config)#**Password** cisco

Después Digitar el comando **login** el cual habilitará la petición de contraseña al usuario:

SWCENTRO (config)#**Login**

Por úlimo Digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la contraseña:

SWCENTRO (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

SWCENTRO #

5.10.11 IP ADRESS

Se le puede otorgar al switch una dirección IP para fines de administración. Esto se configura en la interfaz virtual, VLAN 1. Por defecto, el switch no tiene dirección IP.

Los puertos o interfaces del switch se establecen en modo automático y todos los puertos de switch están en VLAN 1. VLAN 1 se conoce como la VLAN de administración por defecto.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWCENTRO > **enable**
SWCENTRO #

Entrar a la configuración global con el comando **configure terminal**:

SWCENTRO # **configure Terminal**
SWCENTRO (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Ingresar al modo de configuración de interfaz con el comando **interface vlan 1**:

SWCENTRO (config)#**interface vlan 1**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

SWCENTRO (config)#**ip address** 192.168.6.2 255.255.255.240

Ahora Digitar el comando **no shutdown** para levantar la interface:

SWCENTRO (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

SWCENTRO #

5.10.12 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.

5.10.12.1 TIPOS DE VLANS

Existen 3 tipos de vlans:

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

5.10.12.2 VLANS POR PUERTO

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

5.10.12.3 VLANS POR DIRECCIONES MAC

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

5.10.12.4 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.

5.10.13 CONFIGURACIÓN DE VLANS

Para configurar las vlans se debe estar 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** <número de vlan> **name** <nombre>"por último para salir de la configuración se debe digitar el comando **"exit"**.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWCENTRO >**enable**
SWCENTRO #

Entrar a la configuración de vlan con el comando **vlan database**:

SWCENTRO # **vlan database**
SWCENTRO (vlan)#

Digitar el comando **vlan**<número> seguido de **name** y el nombre de la vlan:

SWCENTRO (vlan)# **vlan 10** name **BANRED**

Digitar **exit** para salir del modo de configuración de vlan:

SWCENTRO (vlan)#**exit**
SWCENTRO #

5.10.14 ASIGNAR PUERTOS A UNA VLAN

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

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWCENTRO >**enable**
SWCENTRO #

Entrar a la configuración global con el comando **configure Terminal**:

SWCENTRO # **configure Terminal**
SWCENTRO (Config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Ingresar a la interfaz fastethernet a la cual va hacer asignada a la vlan con el comando **interface fastethernet 0/2**:

SWCENTRO (Config)#**interface fastethernet 0/2**
SWCENTRO (config-if)#

Asignar el puerto a la vlan con el siguiente comando **switchport access vlan 10**:

SWCENTRO (config-if)#**switchport access vlan 10**

Digitar **exit** para salir del modo de configuración de vlan:

SWCENTRO (config-if)#**exit**
SWCENTRO #

5.10.15 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.

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 linea de comando "**vtp < Server o client>**" después digitar el comando "**vtp domain <nombre del dominio>"** y por último para salir de la configuración digitar el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWCENTRO >**enable**
SWCENTRO #

Entrar a la configuración de vlan con el comando **vlan database**:

SWCENTRO # **vlan database**
SWCENTRO (vlan)#

Para cambiar el tipo del switch a server se debe digitar el comando **vtp server** :

SWCENTRO (vlan)# **vtp Server**

Digitar el comando **vtp domanin** para agregar al switch a un dominio:

SWCENTRO (vlan)# **vtp domain topico**

Digitar **exit** para salir del modo de configuración de vlan:

SWCENTRO (vlan)# **exit**
SWCENTRO #

5.10.16 COMUNICACIÓN ENTRE VLANS

Por último en el router principal se debe ingresar al modo de configuración global para a su vez ingresar a la interfaz ethernet con el comando "**interface ethernet<número de interfaz>**", luego levantar la interface con el comando "**no shutdown**" después ingresar a la sub interface ethernet con el comando "**interface ethernet<número de interfaz. número de subinterfaz>**" para digitar 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, masc**" y por último para salir del modo de configuración global digitar el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

CENTRO# **configure terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z.

Digitar el comando **interface FastEthernet1/0.1** para configurar la sub interfaz:

CENTRO (config)#**interface fastethernet1/0.1**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **1** ya que es la vlan por defecto:

CENTRO (config-if)#**encapsulation dot1q 1**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

CENTRO (config-if)#**ip address** 192.168.6.1 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

CENTRO (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.2** para configurar la sub interfaz:

CENTRO (config)#**interface fastethernet1/0.2**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **10:**

CENTRO (config-if)#**encapsulation dot1q 10**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

CENTRO (config-if)#**ip address** 192.168.6.17 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

CENTRO (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.3** para configurar la sub interfaz:

CENTRO (config)#**interface fastethernet1/0.3**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **20:**

CENTRO (config-if)#**encapsulation dot1q 20**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

CENTRO (config-if)#**ip address** 192.168.6.33 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

CENTRO (config-if)#**no shutdown**

Después de haber ingresado lo anterior aparecerá el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica, y detecta si el router adyacente esta en línea.

%LINEPROTO-5-UPDOWN: Line protocol on Interface fastethernet2/0, changed state to up
%LINK -3-UPDOWN: Interface fastethernet2/0, changed state to up

5.10.17 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**".

SWCENTRO # delete flash: vlan.database.

5.10.18 COMANDO SHOW

Los numerosos comandos show se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas.

Show interfaces serial 0/1 .- muestra la estadística completa del router
Show controllers serial 0/1 .- muestra la información del hardware
Show clock .- muestra la hora fijada en el router
Show hosts .- muestra la lista en cache de los nombres de host y sus direcciones.
Show users .- muesra todos los usuario conectados al router.
Show version.- despliega la información acerca del router y de la versión del IOS que este corriendo en la RAM.
Show protocols. .- muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.
Show startup-configuartion .- muestra el archivo de configuración almacenado en la NVRAM.
Show running-configuration .- muestra el contenido del archivo de configuración activo.
Show ip route .- muestra las interfaces por las que se llega a otras redes mediantes los protocolos de enrutamiento ej: O:ospf, R:rip, C: directamente conectado
Show vlans.- muestra todas las vlans creadas con sus respectivos puertos asignados.

5.10.19 SH RUN CENTRO

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

Building configuration...

Password:
Enter password:
Frontera1>enable
Enter password:
Version 12.1 ---------- Indica la versión del IOS
service timestamps debug uptime
service timestamps log uptime
service password-encryption
hostname CENTRO ---------- Refleja el nombre que el administrador le ha asigando a un router

enable secret 5 sdf6978yhg$jnb76sd ---- Este comando proporciona mayor seguridad Almacenando la contraseña con una función Criptográfica irreversible. No se puede recuperar una contraseña perdida que ha sido cifrada por cualquier método.

Enable password CISCO ---------- Permite fijar una contraseña local para controlar el acceso a los varios niveles del privilegio, utilice el comando global de la configuración de la contraseña del permitir. Para quitar el requisito de la contraseña se antepone la palabra no al comando.

ip subnet-zero

!
interface Serial0 ---------- Para fijar las direcciones IP de una interfaz utilice el comando IP Address. Para quitar las direcciones especificadas, utilice la forma negativa de este comando.

ip address 192.168.0.2 255.255.255.252--- Máscara de red del segmento utilizado
no ip directed-broadcast
clock rate 56000
bandwidth 1544
!

interface Serial1
ip address 192.168.0.21 255.255.255.252

```
 no ip directed-broadcast
 bandwidth 1544 ------------------------------ Para fijar un valor del ancho de banda de la
                                                Interfaz, se utiliza el comando Bandwitch en la
                                                configuración de la misma.
                                                El valor mostrado es el que por defecto se le
                                                asigna a cada una de ellas.
!
!
interface Serial2
 ip address 192.168.0.25 255.255.255.252
 no ip directed-broadcast
 bandwidth 1544
!

interface Serial3
 ip address 192.168.0.34 255.255.255.252
 no ip directed-broadcast
 clock rate 56000
 bandwidth 1544
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 bandwidth 10000
!
interface Ethernet0.1
 encapsulation dot1q 1------------------------ IEEE 802.1Q es un protocolo estándar para
                                                interconectar los switches y routers y para
                                                definir topologías de VLAN.
 ip address 192.168.6.1 255.255.255.240
!
interface Ethernet0.2
 encapsulation dot1q 10
 ip address 192.168.6.17 255.255.255.240
!
interface Ethernet0.3
 encapsulation dot1q 20
 ip address 192.168.6.33 255.255.255.240
!
!
router rip ------------------------------------ Para definir los interfaces con las cuales está
                                                trabajado RIP y la identificación del área
                                                para esos interfaces, se utilizan estos
                                                comandos.

 version 2
 network 192.168.0.0
 network 192.168.1.0
!
!
ip classless
```

```
no ip http server
line con 0
 login---------------------------------------------- Para permitir  la contraseña que comprueba la
                                                     conexión, utilice el comando Login.En caso de
                                                     querer inhabilitar la contraseña se antepone la
                                                     negación al comando.
 transport input none
 password cisco
line aux 0
line vty 0 4
 login
 password cisco
!
no scheduler allocate
end
```

5.10.20 SH IP ROUTE CENTRO

Muestra el contenido de una tabla d 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 metrica]
via a,b,c,d: dirección de interfaz a la que llega.
serial: nombre de la interface saliente

```
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

     192.168.0.0/30 is subnetted, 10 subnets
C       192.168.0.0 is directly connected, Serial0
C       192.168.0.20 is directly connected, Serial1
C       192.168.0.24 is directly connected, Serial2
C       192.168.0.32 is directly connected, Serial3
R       192.168.0.28 [120/1] via 192.168.0.26, 00:07:24, Serial3
R       192.168.0.36 [120/1] via 192.168.0.45, 00:03:33, Serial1
R       192.168.0.40 [120/2] via 192.168.0.45, 00:02:34, Serial1
```

5.10.21 SH VLAN CENTRO

Muestra todas las vlans creadas con sus respectivos puertos asignados

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
10	10	active	Fa0/2
20	20	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

5.11 ROUTER ALBORADA

5.11.1 MODOS DE CONFIGURACIÓN DEL ROUTER

Al acceder al router por seguridad tiene dos niveles de acceso a los comandos:

- USER EXEC
- PRIVILEGED EXEC

En modo USER EXEC se puede consultar aspectos básicos de la configuración del router. Para consultar aspectos más críticos de la configuración del router se debe pasar a modo PRIVILEGED EXEC. Para pasar de modo USER EXEC a modo PRIVILEGED EXEC es necesario digitar el comando "**enable**".

En el modo USER EXEC el prompt que muestra el router es ">".En el PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#.

```
Router>                          modo usuario
Router> enable

Router#                          modo privilegiado
Router# exit
Router>
```

Desde los modos USER EXEC y PRIVILEGED EXEC no se puede modificar la configuración del router. Para hacerlo se debe pasar del modo PRIVILEGED EXEC al modo de configuración global (CONFIGURE TERMINAL). Desde allí se puede configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc. y para salir de estos modos de configuración se debe digitar el comando "**exit**"

5.11.1.1 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc el prompt que aparece es "Router(config)#"

```
Router>
Router> enable
Router# configure terminal       modo de configuracion global.
Router# exit
Router>
```

5.11.1.2 MODO DE CONFIGURACIÓN ESPECÍFICOS

Permiten configurar protocolos, interfaces o en general aspectos más complejos del router.El prompt que aparece es R(config-if)#, R(config-route)#.

5.11.2 GUARDAR CAMBIOS EN EL ROUTER

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o especifico se guardan sobre un archivo de configuración residente en la RAM del switch llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el router se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

> Con el comando **copy running-config Startup-config** se guarda cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN

Router # **copy running-config Startup-config**

> Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

Destination filename [startup-config]? Yes

> El siguiente mensaje significa que se esta guardando la configuración

Building configuration...
[OK]

5.11.3 ASIGNAR NOMBRE A UN ROUTER

Una de las primeras tareas de configuración basica es asignar un nombre al router. El nombrado de un router ayuda a una mejor administración de la red al identificar univocamente cada uno de los router en la red.

Para configurar el nombre del router se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre >.Para salir del modo de configuración global con el comando "**exit**".

Cambiar de modo usuario a modo privilegiado con el comando **enable**

Router>**enable**
Router #

Entrar a la configuración global con el comando **configure Terminal**

Router # **configure Terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME <nombre>** se cambia el nombre al router:

Router # **hostname** ALBORADA
ALBORADA #

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

ALBORADA #

5.11.4 CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER

Un router puede ser asegurado mediante el uso de contraseñas para restringir el acceso. Las contraseñas pueden establecerse para las líneas de Terminal virtual y la línea de consola.
El modo de configuración **line console 0** puede utilizarse para establecer una contraseña de conexión en el Terminal de consola, lo que resulta util en un red en la que hay muchas personas que tienen acceso al router.
El modo de configuración **line vty 0 4** sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

A NIVEL DE USUARIO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

ALBORADA >**enable**
ALBORADA #

Entrar a la configuración global con el comando **configure terminal**:

ALBORADA # **configure Terminal**
ALBORADA (config)#

Digitar el comando **line console 0** para establecer una contraseña de conexión en el Terminal de consola:

ALBORADA (config)#**Line console 0**

Ahora proceder a digitar el comando **password** seguido de la contraseña:

ALBORADA (config)#**Password** cisco

Después digitar el comando **login** el cual habilitará la petición de contraseña al usuario:

ALBORADA (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

ALBORADA #

A NIVEL DE USUARIO PRIVILEGIADO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

ALBORADA >**enable**
ALBORADA

Entrar a la configuración global con el comando **configure terminal**:

ALBORADA # **configure Terminal**
ALBORADA (config)#

Digitar el comando **line vty 0 4** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes:

ALBORADA (config)#**Line vty 0 4**

Ahora proceder a digitar el comando **Password** seguido de la contraseña:

ALBORADA (config)#**Password** cisco

Después Digitar el comando **login** el cual habilitara la petición de contraseña al usuario:

ALBORADA (config)#**Login**

Por último digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la contraseña:

ALBORADA (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

ALBORADA #

5.11.5 CONFIGURACIÓN DE INTERFACES

Desde el modo de configuración global se puede pasar a configurar las interfaces. Para configurar una interface siga los siguientes pasos

- Entrar al modo de configuración global
- Entrar al modo de configuración de interfaz
- Especifique la dirección ip seguida de su máscara de subred
- *Active la interfaz*

Por ejemplo, para configurar un interface ethernet se debe hacer de la siguiente manera:

Router# configure terminal

Router(config)# interface <eth0 > modo configuración de intefaz
Router(config-if)# ip address <IP MASK>
Router(config-if)# no shutdown
Router(config-if)# exit
Router#

El commando "**no shutdown**" es necesario para activar la interfaz. Por defecto, al arrancar el router todos los interfaces están desactivados. El comando "**shutdown**" en su defecto desactivaría administrativamente una interfaz.

Las interfaces serial están diseñadas para que en la situación más normal se conecten a una operadora de telecomunicaciones a través de un DCE (e.g.; un MODEM o una Terminación de Red, TR). El DCE es el que normalmente da reloj y por tanto fija la velocidad de modulación y por consiguiente de transmisión.

Si se conectan dos puertos serie de router (DTE-DTE) hay que usar un cable cruzado. Además uno de los dos puertos tiene que actuar como DCE dando reloj. En principio desde el punto de vista de router cualquiera de los dos puede actuar de DCE, así que lo importante es que conector del cable es el que marca que puerto es DCE.

5.11.5.1 INTERFACES SERIALES

Una vez que se sabe que puerto es el que actúa de DCE, tiene que dar reloj. Está opción la tendrá que activar vía IOS con el comando "**clockrate Bw**", donde **Bw** son los bps con los que va a trabajar la línea. En el puerto DTE no se deberá activar este comando.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

ALBORADA >**enable**
ALBORADA #

Entrar a la configuración global con el comando **configure terminal**:

ALBORADA # **configure Terminal**
ALBORADA (config)#

Ingresar al modo de configuración de interfaz con el comando **interface serial 0/0**:

ALBORADA (config)#**interface serial 0/0**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

ALBORADA (config)#**ip address** 192.168.0.22 255.255.255.252

Ahora digitar el comando **no shutdown** para levantar la interface:

ALBORADA (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global:

ALBORADA #(config)#

Ahora ingresar la **interface serial 0/1:**

ALBORADA (config)#**interface serial 0/1**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

ALBORADA (config-if)#**ip address** 192.168.0.45 255.255.255.252

Ahora digitar el comando **no shutdown** para levantar la interface:

ALBORADA (config-if)# **no shutdown**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

ALBORADA #

5.11.5.2 INTERFACES ETHERNET

Un interfaz ethernet se configura desde en modo consola. Cada intefaz ethernet debe tener una dirección IP y una máscara de subred.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

ALBORADA >**enable**
ALBORADA #

Entrar a la configuración global con el comando **configure terminal**:

ALBORADA # **configure Terminal**
ALBORADA (config)#

Ingresar al modo de configuración de interfaz con el comando **interface ethernet** 0/0:

ALBORADA (config)#**interface ethernet 0/0**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address** pero en este caso solamente se va a levantar la interface sin ponerle dirección ip.

Ahora Digitar el comando **no shutdown** para levantar la interface:

ALBORADA (config-if)# **no shutdown**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

ALBORADA#

5.11.6 CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO

El Protocolo de enrutamiento es aquel que suministra los mecanismos necesarios para compartir la información de enrutamiento. Los mensajes de un protocolo de enrutamiento se mueven entre los routers. Un protocolo d enrutamiento permite a los routers comunicarse con otros routers para actualizar y mantener sus tablas. A continuación se mostrará diversos protocolos de enrutamiento:

- RIP (protocolo de información de enrutamiento)
- OSPF (primero la ruta libre mas corta)
- IGRP (protocolo de enrutamiento de gateway interior)

5.11.6.1 PROTOCOLO RIP VERSION 2(VECTOR DISTANCIA)

Es un protocolo de enrutamiento por vector-distancia, que 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, primero se debe cambiaral modo de configuración global, luego se debeestablecer con una o más órdenes "**network**", las redes directamente conectadas al router.y finalmente para salir digitar el comando "**exit**" A continuacion se muestra a ver la configurar el router ALBORADA con el protocolo rip vs 2 :

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

```
ALBORADA >enable
ALBORADA #
```

Entrar a la configuración global con el comando **configure Terminal**:

```
ALBORADA # configure Terminal
ALBORADA (config)#
```

Ingresar la configuración del protocolo Rip con el comando **router rip**:

```
ALBORADA (config)# router rip
```

Ingresar la **version 2**

ALBORADA (config-router)#**version 2**

Ingresar la dirección de red que esta configurada con RIP con el comando **network**:

ALBORADA (config-router)# **network** 192.168.0.0
ALBORADA (config-router)# **network** 192.168.1.0

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global

ALBORADA #

5.11.7 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. En el modo USER EXEC el prompt que muestra el switch es ">".En el PRIVILEGED EXEC el prompt es "#" y en el modo de configuración global el prompt es (config)#,

switch >
switch > enable

modo usuario.

switch #
switch # exit
switch >

modo usuario privilegiado.

5.11.8 MODO DE CONFIGURACIÓN GLOBAL O CONFIGURE TERMINAL

Permite configurar aspectos sencillos del switch como pueden ser la configuración del nombre del switch, passwords, etc (prompt R(config)#)

```
switch >
switch > enable
switch # configure terminal
switch (config)#exit
switch #
switch #
```

modo configuración global

5.11.9 GUARDAR CAMBIOS EN EL SWITCH

Como se ha mencionado, los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en la RAM del switch llamado"running-config". Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando "show running-config". Si el switch se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo "running-config" (RAM) en el archivo "startup-config"(NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando "**copy running-config startup-config**".

Con el comando **copy running-config Startup-config** se guarda cambios de configuración actual al archivo **startup-config** que se encuentra en la NVRAN:

Switch# **copy running-config Startup-config**

Luego de digitar este comando aparecerá un mensaje para la comprobación de la ruta destino para guardar el archivo **running-config** se debe digitar "**yes**":

Destination filename [startup-config]? Yes

El siguiente mensaje significa que se esta guardando la configuración:

Building configuration...
[OK]

5.11.10 HOSTNAME Y PASSWORD

Para configurar el nombre del switch se debe hacer en el modo de configuración global con el comando "**hostname**" <nombre >.Para salir del modo de configuración global con el comando "**exit**".

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

Switch>**enable**
Switch #

Entrar a la configuración global con el comando **configure terminal**:

Switch # **configure Terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Con el comando **HOSTNAME <nombre>** se cambia el nombre al router:

Switch # **hostname** SWALBORADA
SWALBORADA #

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

SWALBORADA #

El router posee niveles de seguridad para que solo los administradores puedan configurar dichos dispositivos. Existen dos formas de colocar password en el router:

De modo USER EXEC con el comando "**line console** 0" seguido respectivo "**password**"<nombre del password> y "**login**"

De modo PRIVILEGED EXEC con el comando "**line vty 0 4**" seguido respectivo "**password**"<nombre del password> y "**login**".

A NIVEL DE USUARIO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

SWALBORADA >**enable**
SWALBORADA #

Entrar a la configuración global con el comando **configure terminal**:

SWALBORADA # **configure Terminal**
SWALBORADA (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line console 0** para establecer una contraseña de conexión en el Terminal de consola:

SWALBORADA (config)#**Line console 0**

Ahora proceder a digitar el comando **password** seguido de la contraseña:

SWALBORADA (config)#**Password** cisco

Después Digitar el comando **login** el cual habilitará la petición de contraseña al usuario

SWALBORADA (config)#**Login**

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

SWALBORADA #

A NIVEL DE USUARIO PRIVILEGIADO

Cambiar de modo usuario a modo privilegiado con el comando **enable**:

SWALBORADA >**enable**
SWALBORADA #

Entrar a la configuración global con el comando **configure terminal**:

SWALBORADA # **configure Terminal**
SWALBORADA (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Digitar el comando **line vty 0 15** que sirve para establecer una contraseña de conexión en sesiones TELNET entrantes:

SWALBORADA (config)#**Line vty 0 15**

Ahora proceder a digitar el comando **Password** seguido de la contraseñ:

SWALBORADA (config)#**Password** cisco

Después Digitar el comando **login** el cual habilitará la petición de contraseña al usuario:

SWALBORADA (config)#**Login**

Por último Digitar el comando "**enable password**" para habilitar la contraseña a nivel privilegiado seguido de la contraseña:

SWALBORADA (config)#**enable password** cisco

Digitar la combinación de teclas **CRTL+Z** para salir de la configuración global:

SWALBORADA #

5.11.11 IP ADRESS

Se le puede otorgar al switch una dirección IP para fines de administración. Esto se configura en la interfaz virtual, VLAN 1. Por defecto, el switch no tiene dirección IP.

Los puertos o interfaces del switch se establecen en modo automático y todos los puertos de switch están en VLAN 1. VLAN 1 se conoce como la VLAN de administración por defecto.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWALBORADA > **enable**
SWALBORADA #

Entrar a la configuración global con el comando **configure terminal**:

SWALBORADA # **configure Terminal**
SWALBORADA (config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Ingresar al modo de configuración de interfaz con el comando **interface vlan 1**:

SWALBORADA (config)#**interface vlan 1**

Especifique la dirección de la interfaz y la máscara de subred con el comando **ip address:**

SWALBORADA (config-if)#**ip address** 192.168.9.2 255.255.255.240

Ahora digitar el comando **no shutdown** para levantar la interface:

SWALBORADA (config-if)# **no shutdown**

Digitar el comando **exit** para ir al modo de configuración global

SWALBORADA #

5.11.12 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.

5.11.12.1 TIPOS DE VLANS

Existen 3 tipos de vlans:

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

5.11.12.2 VLANS POR PUERTO

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

5.11.12.3 VLANS POR DIRECCIONES MAC

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

5.11.12.4 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.

5.11.13 CONFIGURACIÓN DE VLANS

Para configurar las vlans se debe estar en el MODO PRIVILIGED EXEC, luego ingresar al modo de configuración de vlan con el comando "**vlan database**" después ingresar la linea de comando "**vlan** <número de vlan> **name** <nombre>"por último para salir de la configuración digitar el comando **"exit"**.

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWALBORADA >**enable**
SWALBORADA #

Entrar a la configuración de vlan con el comando **vlan database**:

SWALBORADA # **vlan database**
SWALBORADA (vlan)#

Digitar el comando **vlan**<número> seguido de **name** y el nombre de la vlan:

SWALBORADA (vlan)# **vlan 20** name **SERVICIO_CLIENTES**

Digitar **exit** para salir del modo de configuración de vlan:

SWALBORADA (vlan)#**exit**
SWALBORADA #

5.11.14 ASIGNAR PUERTOS A UNA VLAN

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

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWALBORADA >**enable**
SWALBORADA #

Entrar a la configuración global con el comando **configure Terminal**:

SWALBORADA # **configure Terminal**
SWALBORADA (Config)#

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z

Ingresar a la interfaz fastethernet a la cual va hacer asignada a la vlan con el comando **interface fastethernet 0/2**:

SWALBORADA (Config)#**interface fastethernet 0/2**
SWALBORADA (config-if)#

Asignar el puerto a la vlan con el siguiente comando **switchport access vlan 20**:

SWALBORADA (config-if)#**switchport access vlan 20**

Digitar **exit** para salir del modo de configuración de vlan:

SWALBORADA (config-if)#**exit**
SWALBORADA #

5.11.15 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.

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 linea de comando " **vtp < Server o client>**" después digitar el comando "**vtp domain <nombre del dominio>"** y por último para salir de la configuración digitar el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

SWALBORADA >**enable**
SWALBORADA #

Entrar a la configuración de vlan con el comando **vlan database**:

SWALBORADA # **vlan database**
SWALBORADA (vlan)#

Para cambiar el tipo del switch a server se debe digitar el comando **vtp server** :

SWALBORADA (vlan)# **vtp Server**

Digitar el comando **vtp domanin** para agregar al switch a un dominio:

SWALBORADA (vlan)# **vtp domain topico**

Digitar **exit** para salir del modo de configuración de vlan:

SWALBORADA (vlan)# **exit**
SWALBORADA #

5.11.16 COMUNICACIÓN ENTRE VLANS

Por último en el router principal se debe ingresar al modo de configuración global para a su vez ingresar a la interfaz ethernet con el comando "**interface ethernet<número de interfaz>**", luego levantar la interface con el comando "**no shutdown**" después ingresar a la sub interface ethernet con el comando "**interface ethernet<número de interfaz. número de subinterfaz>**" para digitar 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, masc**" y por último para salir del modo de configuración global digitar el comando "**exit**".

Digitar el comando **enable** para cambiar de modo usuario a modo privilegiado:

ALBORADA # **configure terminal**

Después de ingresar el comando **configure Terminal** aparecerá un mensaje el cual dirá que está dentro de la configuración global y que para salir tendrá que presionar CNTL/Z:

Enter configuration commands, one per line. End with CNTL/Z.

Digitar el comando **interface FastEthernet1/0.1** para configurar la sub interfaz:

ALBORADA (config)#**interface fastethernet1/0.1**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **1** ya que es la vlan por defecto:

ALBORADA (config-if)#**encapsulation dot1q 1**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

ALBORADA (config-if)#**ip address** 192.168.9.1 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

ALBORADA (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.2** para configurar la sub interfaz:

ALBORADA (config)#**interface fastethernet1/0.2**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **10:**

ALBORADA (config-if)#**encapsulation dot1q 10**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

ALBORADA (config-if)#**ip address** 192.168.9.17 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**.

ALBORADA (config-if)#**no shutdown**

Digitar el comando **interface FastEthernet1/0.3** para configurar la sub interfaz:

ALBORADA (config)#**interface fastethernet1/0.3**

Ahora digitar el protocolo de comunicación entre el switch y router con el comando **encapsulation dotlq** y el **número de la vlan** en este caso es **20:**

ALBORADA (config-if)#**encapsulation dot1q 20**

Después asignar una dirección IP y máscara de subred a la sub interfaz con el comando **ip address:**

ALBORADA (config-if)#**ip address** 192.168.9.33 255.255.255.240

Por último levantar la interfaz con el comando **no shutdown:**

ALBORADA (config-if)#**no shutdown**

Después de haber ingresado lo anterior aparecerá el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica, y detecta si el router adyacente esta en línea.

%LINEPROTO-5-UPDOWN:Line protocol on Interface fastethernet2/0, changed state to up
%LINK -3-UPDOWN: Interface fastethernet2/0, changed state to up

5.11.17 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".**

SWALBORADA # delete flash: vlan.database.

5.11.18 COMANDO SHOW

Los numerosos comandos show se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas.

Show interfaces serial 0/1 .- muestra la estadística completa del router
Show controllers serial 0/1 .- muestra la información del hardware
Show clock .- muestra la hora fijada en el router
Show hosts .- muestra la lista en cache de los nombres de host y sus direcciones.
Show users .- muesra todos los usuario conectados al router.
Show version.- despliega la información acerca del router y de la versión del IOS que este corriendo en la RAM.
Show protocols. .- muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.
Show startup-configuartion .- muestra el archivo de configuración almacenado en la NVRAM.
Show running-configuration .- muestra el contenido del archivo de configuración activo.
Show ip route .- muestra las interfaces por las que se llega a otras redes mediantes los protocolos de enrutamiento ej: O:ospf, R:rip, C: directamente conectado
Show vlans.- muestra todas las vlans creadas con sus respectivos puertos asignados.

5.11.19 SH RUN ALBORADA

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

Building configuration...

Password:
Enter password:
Frontera1>enable
Enter password:
Version 12.1 ---------- Indica la versión del IOS
service timestamps debug uptime
service timestamps log uptime
service password-encryption
hostname ALBORADA ---------- Refleja el nombre que el administrador le ha asigando a un router

enable secret 5 sdf6978yhg$jnb76sd ---- Este comando proporciona mayor seguridad Almacenando la contraseña con una función Criptográfica irreversible. No se puede recuperar una contraseña perdida que ha sido cifrada por cualquier método.

Enable password CISCO ---------- Permite fijar una contraseña local para controlar el acceso a los varios niveles del privilegio, utilice el comando global de la configuración de la contraseña del permitir. Para quitar el requisito de la contraseña se antepone la palabra no al comando.

ip subnet-zero.

!
interface Serial0
ip address 192.168.0.22 255.255.255.252--- Máscara de red del segmento utilizado
no ip directed-broadcast
clock rate 56000
bandwidth 1544
!

interface Serial1
ip address 192.168.0.45 255.255.255.252
no ip directed-broadcast

```
 clock rate 56000
 bandwidth 1544---------- Para fijar un valor del ancho de banda de la
                          Interfaz, se utiliza el comando Bandwitch en la
                          configuración de la misma.
                          El valor mostrado es el que por defecto se le
                          asigna a cada una de ellas.

!
interface Serial2
 ip address 192.168.0.37 255.255.255.252
 no ip directed-broadcast
 clock rate 56000
 bandwidth 1544
!
interface Serial3
 no ip address
 no ip directed-broadcast
 bandwidth 1544
 shutdown
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 bandwidth 10000
!
interface Ethernet0.1
 encapsulation dot1q 1---------- IEEE 802.1Q es un protocolo estándar para
                                 interconectar los switches y routers y para
                                 definir topologías de VLAN.

 ip address 192.168.9.1 255.255.255.240
!
interface Ethernet0.2
 encapsulation dot1q 10
 ip address 192.168.9.17 255.255.255.240
!
interface Ethernet0.3
 encapsulation dot1q 20
 ip address 192.168.9.33 255.255.255.240
!
!
router rip ---------- ---------- Para definir los interfaces con las cuales está
                                 trabajado RIP y la identificación del área
                                 para esos interfaces, se utilizan estos
                                 comandos.

 version 2
 redistribute OSPF 1
 network 192.168.0.0
 network 192.168.1.0
ip classless
```

```
no ip http server
!
!
!
line con 0
 login
 transport input none
 password cisco
line aux 0
line vty 0 4
 login----------Para permitir la contraseña que comprueba
                la conexión, utilice el comando Login.En
                caso de  querer inhabilitar la contraseña
                se antepone la negación al comando.

 password cisco
!
no scheduler allocate
end
```

5.11.20 SH IP ROUTE ALBORADA

Muestra el contenido de una tabla d 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
[120/1]: [dirección administrativa/ costo de la metrica]
via a,b,c,d: dirección de interfaz a la que llega.
serial: nombre de la interface saliente

```
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

     192.168.0.0/0 is variably subnetted, 11 subnets
C       192.168.0.44/30 is directly connected, Serial1
C       192.168.0.20/30 is directly connected, Serial0
C       192.168.0.36/30 is directly connected, Serial2
R       192.168.0.24/30 [120/1] via 192.168.0.21, 00:08:42, Serial1
R       192.168.0.32/30 [120/1] via 192.168.0.21, 00:01:37, Serial1
R       192.168.0.40/30 [120/1] via 192.168.0.38, 00:09:21, Serial2
       is directly connected,
```

5.11.21 SH VLAN ALBORADA

Muestra todas las vlans creadas con sus respectivos puertos asignados

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
10	10	active	Fa0/2
20	20	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

CAPÍTULO 6

LINUX FEDORA CORE 3

6. LINUX FEDORA CORE 3

6.1 INTRODUCCIÓN

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 hobbie 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 aprovechase 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.
El comenzó su trabajo en 1991 cuando él realizó la versión 0,02, la cual no la dio 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.

Linux tiene todas las prestaciones que se pueden esperar de un Unix moderno y completamente desarrollado: multitarea real, memoria virtual, bibliotecas compartidas, carga de sistemas a-demanda, compartimiento, manejo de debido de la memoria y soporte de redes TCP/IP.

Linux corre principalmente en PC's basados en procesadores 386/486/586, usando las facilidades de proceso de la familia de procesadores 386 (segmentación TSS, etc.) para implementar las funciones nombradas.

La parte central de Linux (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. Aún cuando Linux tenga registro de Copyright, y no sea estrictamente de dominio público. La licencia tiene por objeto asegurar que Linux siga siendo gratuito y a la vez estándar.

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

Aunque existen muchas variaciones de la palabra Linux, es lo más a menudo posible pronunciada con un cortocircuito " i " y con la primera sílaba tensionada, como en LIH-nucks.

Básicamente se puede decir que hoy Linux es un sistema muy completo. El proyecto de Linux Torvalds aún no ha terminado, y se piensa que nunca se terminará por ésta continua evolución de la informática.

6.1.1 CARACTERÍSTICAS

- Confiable
- Seguro
- Sistema Multiusuario
- Multitasking
- Plug and play
- Alto porcentaje de servidores web lo utilizan
- Procesador trabaja de modo protegido
- Constantemente actualizado y refinado con últimas tecnologías

En líneas generales se puede decir que se dispone de varios tipos de sistema de archivos para poder acceder a archivos en otras plataformas. Incluye un entorno gráfico X window (Interfase gráfico estándar 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.

Por lo tanto, la gran popularidad de Linux incluye los siguientes puntos:

Se distribuye su código fuente, lo cual permite a cualquier persona que así lo desee hacer todos los cambios necesarios para resolver problemas que se puedan presentar, así como también agregar funcionalidad. El único requisito que esto conlleva es poner los cambios realizados a disposición del público.
Es desarrollado en forma abierta por cientos de usuarios distribuidos por todo el mundo, los cuales la red Internet como medio de comunicación y colaboración. Esto permite un rápido y eficiente ciclo de desarrollo.

Cuenta con un amplio y robusto soporte para comunicaciones y redes, lo cual hace que sea una opción atractiva tanto para empresas como para usuarios individuales.

Da soporte a una amplia variedad de hardware y se puede correr en una multitud de plataformas: PC's convencionales, computadoras Macintosh y Amiga, asi como costosas estaciones de trabajo.

6.1.2 VENTAJAS

La ventaja de Linux es que pertenece al desarrollo del software libre. El software libre, a diferencia del software propietario, es desarrollado bajo la premisa de que los programas son una forma de expresión de ideas y que las ideas, como en la ciencia, son propiedad de la humanidad y deben ser compartidas con todo el mundo (como ya se expuso en la licencia del público en general del GNU). Para lograr esto, el software libre expone el código fuente de sus programas a quien desee verlo, modificarlo o copiarlo.

6.1.3 KERNEL

Kernel (Núcleo) es el programa que tiene control total de la máquina y administra sus recursos. Linux. Desde un punto estricto es un kernel, no un sistema operativo. El sistema operativo es el kernel junto con todas las herramientas necesarias para que la computadora pueda operar.

El kernel es el encargado de que el software y el hardware de tu ordenador puedan trabajar juntos.
Las funciones más importantes del mismo, aunque no las únicas, son:
Administración de la memoria, para todos los programas en ejecución.
Administración del tiempo de procesador, que estos programas en ejecución utilizan.
Es el encargado de que se pueda acceder a los periféricos/elementos de nuestro ordenador de una manera cómoda.

6.1.4 COMANDOS BÁSICOS

Rm: borra ficheros.

Cd: cambia de directorio.

Mkdir: directorio crea un directorio.

Rmdir: directorio borra un directorio.

Date: muestra la fecha del sistema.

Man: muestra la página del manual del comando o recurso

Logout: sale de la actual sesión.

Login: sale de la actual sesión.

More: muestra el contenido de los archivos indicados por pantallas

Alt+F1: inicia una consola virtual (varias a la vez: F1, F2, F3...)

Cat: concatena archivos o muestra el contenido completo sin pausa

Echo: envía al terminal los argumentos pasados

Passwd: cambia el password del actual usuario.

^C: aborta programa en ejecución.

Mv: mueve archivos

Grep: muestra todas las líneas de un fichero que coinciden con un patrón

Who: lista los usuarios conectados.

Mail: visualiza tu correo, teclea? para ayuda.

Ls: lista directorios y ficheros.

Cp: copia ficheros.

Clear: limpia la pantalla

Wq: Este comando graba cambios realizados dentro de un fichero

Vi: Este comando ingresa al contenido de un fichero

Q!: Este comando sale de un fichero sin guardar cambios realizados

Reload: Recarga un servicio sin detener su ejecución

Service: Este comando sirve para ver los estados de cualquiera de los servicios

Q: Este comando detiene un proceso en ejecución.

Esc-y-# de líneas: Esta combinación de teclas copia un número de líneas

P: Esta tecla pega líneas copiadas con anterioridad

6.1.5 ESTRUCTURA DEL SISTEMA DE ARCHIVOS

/dev: Contiene ficheros del sistema representando los dispositivos que estén físicamente instalados en el ordenador

/etc: Este directorio esta reservado para los ficheros de configuración del sistema. En este directorio no debe aparecer ningún fichero binario (programas). Bajo este deben aparecer otros dos subdirectorios:

/etc/X11: Ficheros de configuración de X Window

/etc/skel: Ficheros de configuración básica que son copiados al directorio del usuario cuando se crea uno nuevo.

/lib: Contiene las librerías necesarias para que se ejecuten los programas que residen en

/bin: (no las librerías de los programas de los usuarios).

/proc: Contiene ficheros especiales que o bien reciben o envían información al kernel del sistema (Se recomienda no modificar el contenido de este directorio y sus ficheros).

/sbin: Contiene programas que son únicamente accesibles al súper usuario o root.

/usr: Este es uno de los directorios más importantes del sistema puesto que contiene los programas de uso común para todos los usuarios. Su estructura suele ser similar a la siguiente:

/usr/X11R6: Contiene los programas para ejecutar X Window.

/usr/bin: Programas de uso general, lo que incluye el compilador de C/C++.

/usr/doc: Documentación general del sistema.

/usr/etc: Ficheros de configuración generales.

/usr/incluye: Ficheros de cabecera de C/C++ (.h).

/usr/info: Ficheros de información de GNU.

/usr/lib: Librerías generales de los programas.

/usr/man: Manuales accesibles con el comando man (ver más adelante).

/usr/sbin: Programas de administración del sistema.

/usr/src: Código fuente de programas.
Existen además de los anteriores otros directorios que se suelen localizar en el directorio /usr, como por ejemplo las carpetas de los programas que se instalen en el sistema.

/var: Este directorio contiene información temporal de los programas (lo cual no implica que se pueda borrar su contenido, de hecho, ¡no se debe hacer!)

6.1.6 COMANDOS PARA REINICIAR Y SALIR DEL SISTEMA

Shutdown Poweroff: apagar el sistema.

Exit Logout: salir de una consola virtual

Startx: reiniciar el modo grafico.

Reboot: reiniciar

6.1.7 ARCHIVOS ESPECIALES

/etc/passwd Contiene todos los logins y passwords

/etc/motd Mensaje del día

/etc/profile Se ejecuta al introducir al entrar en el sistema

6.1.8 TERMINOLOGÍA

En Linux se utilizan términos a los cuales es fácil adaptarse si se conoce a que se refieren

Entre los más utilizados están:

Demonios: esto se refiere a algunos de los servicios como dovecot utilizado en la configuración del SENDMAIL.

Invocar: se refiere a levantar o cambiar el estado de ciertos servicios como Service smb reload utlizado para recargar el fichero de samba.

Logonear: se refiere a ingresar con un usuario a una de las consolas o a un PC de la red.

6.2 INSTALACIÓN DE LINUX

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

Fedora Core es un sistema operativo de evolución rápida que sigue las últimas técnicas de desarrollo.

Para instalar Linux Fedora Core 3 desde discos, se necesita 4 discos de instalación o el DVD de instalación. Existe un juego de discos por cada arquitectura soportada. Actualmente, Fedora Core soporta las arquitecturas i386, ppc y x86_64. Estas arquitecturas se las describe a continuación:

I386
Procesadores compatibles Intel x86, Incluyendo Intel Pentium and Pentium-MMX, Pentium Pro, Pentium-II, Pentium-III, Celeron, Pentium 4, y Xeon; VIA C3/C3-m y Eden/Eden-N; y AMD Athlon, AthlonXP, Duron, AthlonMP, y Sempron.

PPC
Procesadores PowerPC, como aquellos encontradonse Apple Power Macintosh, G3, G4, y G5, y sistemas IBM pSeries

X86_64
Procesadores 64-bit AMD como los Athlon64, Turion64, Opteron; y procesadores Intel 64-bit como el EM64T.

Instalando fedora core como un servidor, Fedora Core Incluye software para un rango completo de servicios de red. Para instalar un sistema con los servicios de red más comunes, se puede seleccionar la instalación de servidor durante la instalación. También se puede seleccionar paquetes de programas individuales durante la instalación, o instalarlos luego.

6.2.1 REQUERIMIENTOS PARA LA INSTALACIÓN

Para comenzar la instalación de Fedora Core, inicie el computador desde el disco. También se puede instalar desde memorias USB, Discos duros o servidores web, este manual especifica la instalación desde Discos.

El BIOS (Sistema básico de entrada y salida) del equipo debe soportar el inicio desde diferentes dispositivos. El BIOS controla el acceso a algunos dispositivos durante el inicio del equipo. Cualquier computador que coincide con la especificación mínima recomendada para Fedora Core puede ser iniciado desde un CD o un DVD con el primer disco.

Cancelar la instalación, para cancelar el proceso de instalación en cualquier momento antes de la pantalla de instalación de los paquetes, presione Ctrl-Alt-Del o apague el computador desde el botón. Fedora no realiza cambios en el computador antes de que comience a instalar los paquetes.

Arrancar desde el disco, Para arrancar el computador desde el disco:

- Encienda el computador.
- Inserte el primer disco en la unidad de CD o DVD.
- Una pantalla de inicio aparece, Con un boot: prompt al final.

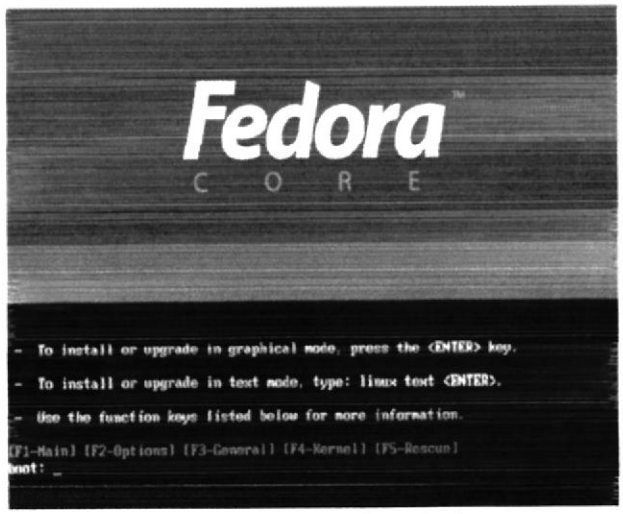

Fig. 6.1 Inicio de instalación

Si presiona **Enter**, la instalación es realizada en modo por defecto. En modo por defecto, la instalación usa una interfaz gráfica para la instalación. Para cambiar el modo de instalación en el `boot:` prompt, digite linux text para realizar la instalación en una interfaz de texto.

Cuando ingresas a la instalación ya sea por modo texto o modo comando, la primera fase del programa de instalación inicia, luego de su carga la siguiente pantalla aparece

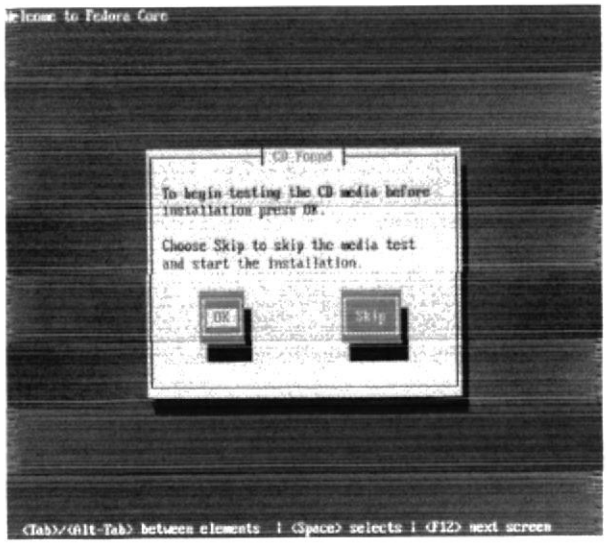

Fig. 6.2 Ingreso a la instalación

Seleccione **OK** para comprobar el disco, o seleccione **Skip** para proceder con la instalación sin probar el disco.

6.2.2 COMPROBAR DISCOS

Comprueba los discos que anteriormente no hayas comprobado. Un error de disco durante la instalación puede forzar a renovar el procedimiento completo

Después de que pruebas el primer disco, otra pantalla aparece y muestra el resultado.

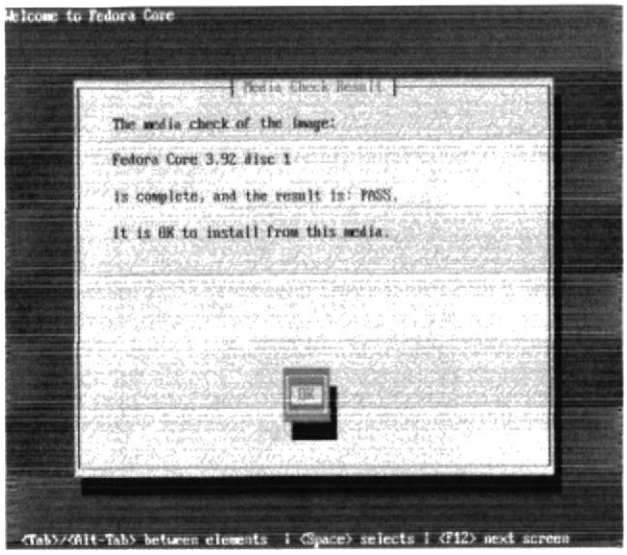

Fig. 6.3 Comprobar discos

Pulsa **OK**, la siguiente pantalla aparece

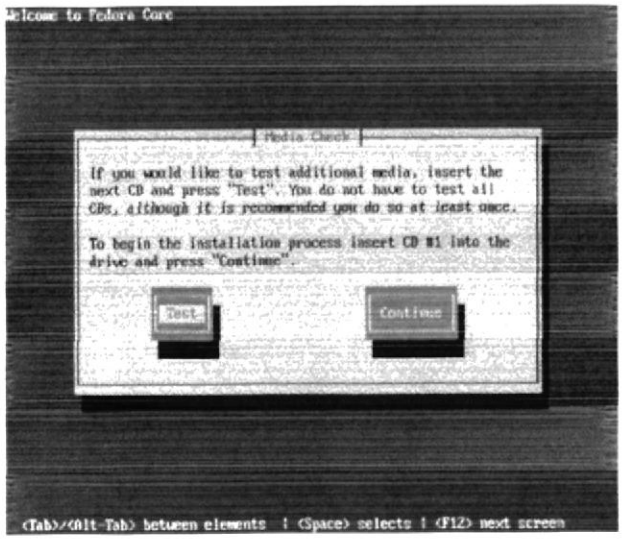

Fig. 6.4 Elección de comprobación

Selecciona **Test** para comprobar el siguiente disco del juego, o **Continue** para proceder con la instalación

Después de que comprabas los discos y seleccionas **Continue**, o si escoges skip testing, el programa principal de la instalación se carga.

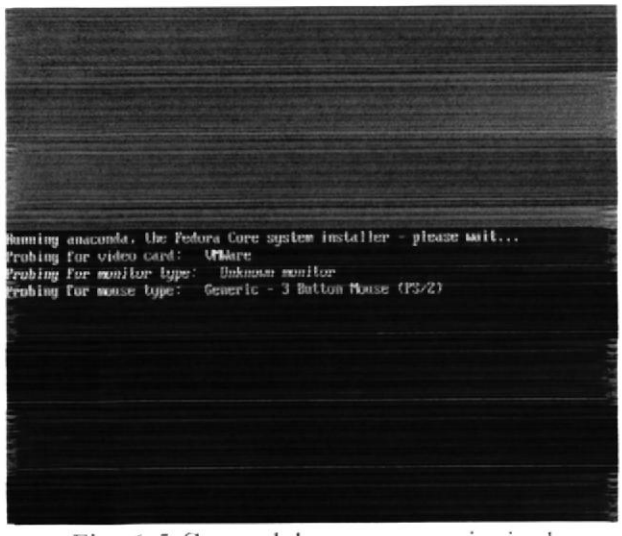

Fig. 6.5 Carga del programa principal

6.2.3 IDENTIFICAR EL AMBIENTE

Si el sistema de instalación falla la identificación del hardware en el computador, este mostraría pantallas de texto en vez de interfaces gráficas. Las pantallas de texto proporcionan la misma función que la interfaz gráfica. Luego en el proceso de instalación se puede especificar manualmente el hardware con el cual se cuenta.

Pantalla de bienvenida, el programa de instalación muestra una pantalla de bienvenida al terminar el proceso de identificación del hardware.

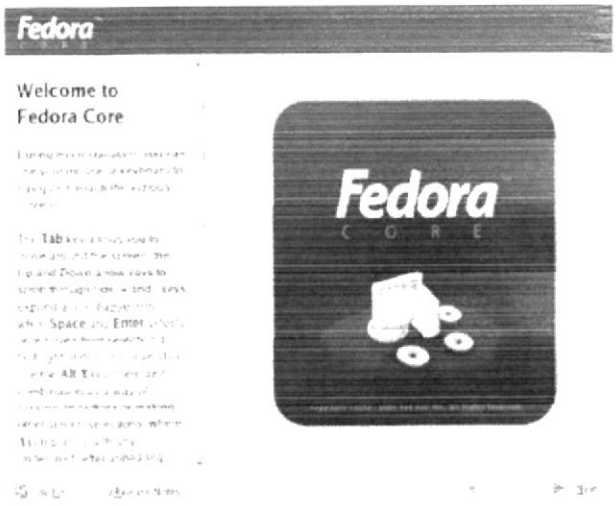

Fig. 6.6 Bienvenida

Pulse **Next** para continuar con la instalación

6.2.4 SELECCIONAR IDIOMA

El programa de instalación muestra una lista de idiomas soportados por Fedora Core

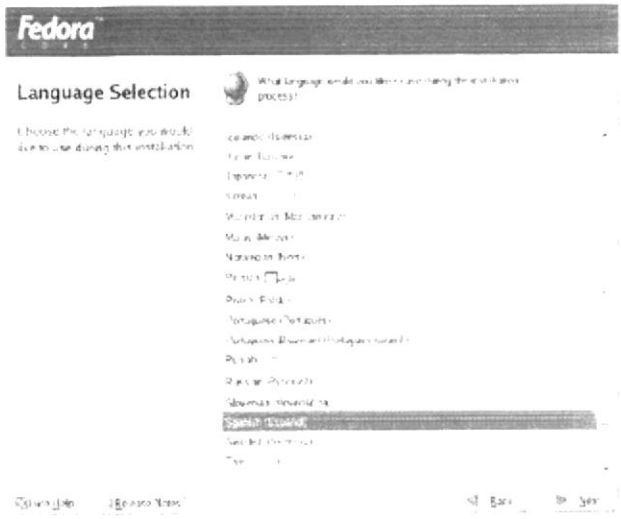

Fig. 6.7 Selección de idioma

Sombree el idioma correcto en la lista y seleccione **Next.**
Para obtener soporte para idiomas adicionales. Modifique la instalación en la fase de instalación de los paquetes. Para más información, pase a la sección 10.2

6.2.5 CONFIGURACIÓN DE TECLADO

La instalación muestra una lista de salidas de teclado soportados por Fedora.

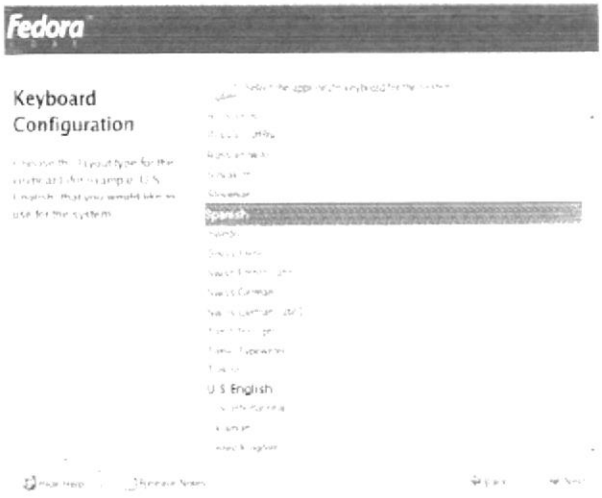

Fig. 6.8 Configuración de teclado

Sombree el idioma de salida de teclado correcta en la lista y seleccione **Next.**

6.2.6 CONFIGURACIÓN DE LA CARGA DE ARRANQUE

La instalación completa de Fedora Core debe ser registrada en la carga de arranque para arrancar apropiadamente. Una carga de arranque es un programa en el equipo que localiza y comienza el sistema operativo. Revise la sección 10.3 para mas información acerca de la carga de arranque.

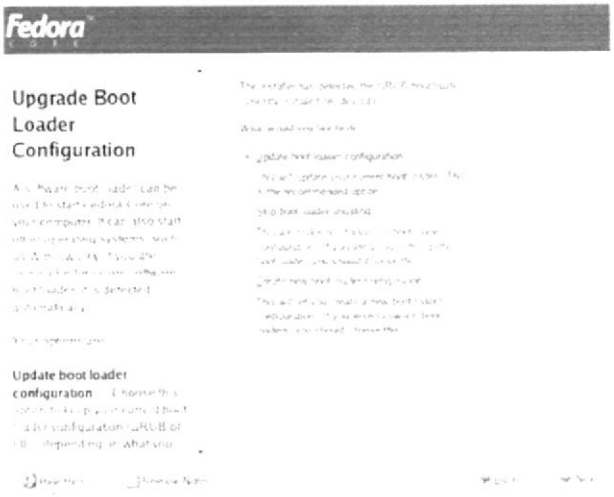

Fig. 6.9 Configurar carga de arranque

Si la carga de arranque fue instalada por una distribución de Linux, el programa de instalación puede modificarlo para cargar el nuevo programa de Fedora Core. Para actualizar la carga de arranque existente, seleccione Configuración de carga de arranque. Esta es la opción por defecto cuando se actualiza una instalación existente de Fedora Core o Red Hat Linux.

GRUB es el programa de carga de arranque que usa Fedora. Si su equipo usa otra carga de arranque, como BootMagic™, System Comander™, o el cargador de arranque instalado por Microsoft Windows, entonces el programa de instalación de Linux no podrá actualizarlo. En este caso, seleccione Saltar actualización de carga de arranque.

Instale una nueva carga de arranque como parte de un proceso de instalación solamente si esta seguro de que quiere reemplazar la carga de arranque existente. Si instala una nueva carga de arranque, Quizás no podrá cargar otro sistema operativo que tenga instalado en el equipo hasta que no haya configurado la nueva carga de arranque. Seleccione crear una nueva configuración de carga de arranque para quitar la carga de arranque existente e instalar GRUB

Después de que haya realizado su selección, presione **Next** para continuar

6.2.7 TIPO DE INSTALACIÓN

Un tipo de instalación es una etiqueta que aproximadamente describe como usará su sistema Fedora. Varios tipos de instalaciones están definidos en el programa de instalación de Fedora Core. Escoja el tipo de instalación apropiada para organizar el proceso de instalación si usted es un principiante.

El programa de instalación escoge algunas opciones basado en el tipo que usted selecciona. Estas elecciones incluyen particiones del disco duro, y paquetes de instalación a ser instalados. Todos los tipos de instalación le permiten al usuario realizar cambios en estas selecciones. Presione **Siguiente** una vez hecha la selección (personalizada).

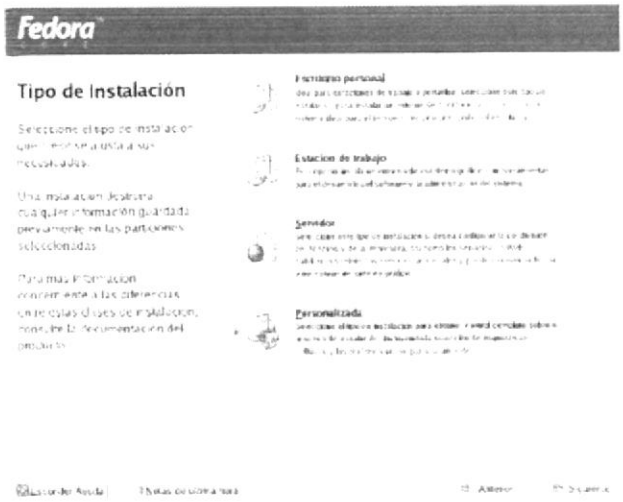

Fig. 6.10 Tipo de instalación

Escritorio Personal, este es el tipo de instalación por defecto. Esta instalación proporciona un ambiente de trabajo en forma gráfica con un paquete de utilitarios de oficina. *Multimedia de Internet y programas multimedia.*

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

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

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

Consideraciones especiales, todas las instalaciones de Fedora Core incluyen los siguientes servicios de red:

- Email a travez de SMTP (Simple Mail Transfer Protocol)
- Compartir archivos en red a travez de NFS (Network File System)
- Imprimir a travez de CUPS (Common UNIX Printing System)
- Acceso remoto a travez de SSH (Security Shell)

6.2.8 PARTICIÓN DEL DISCO

Si es nuevo en Linux, usted deberá querer usar el método de partición automática. Si es un usuario con más experiencia en Linux, use el método de partición manual para más control sobre la configuración del sistema, o seleccione y modifique las particiones definidas automáticamente. Presione **Continuar** una vez hecha la selección.

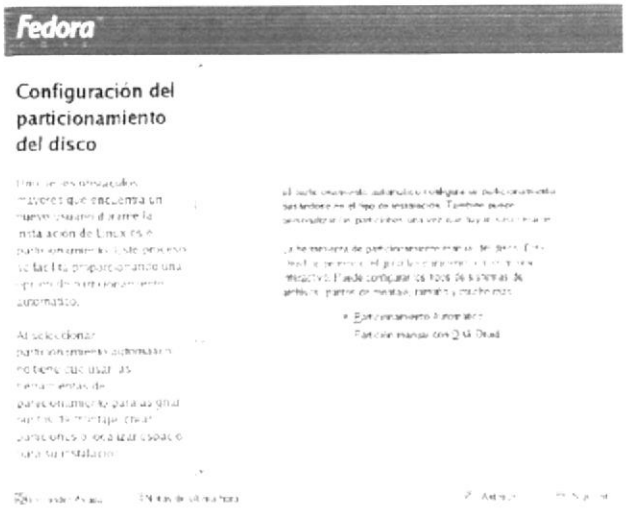

Fig. 6.11 Partición del disco

Elección de partición automática, escoja **Partición automática** en el menú opciones de particiones para usar una PRE-configurada. Entonces Disk Fruid muestra opciones adicionales. Presione **Next** una vez hecha la selección.

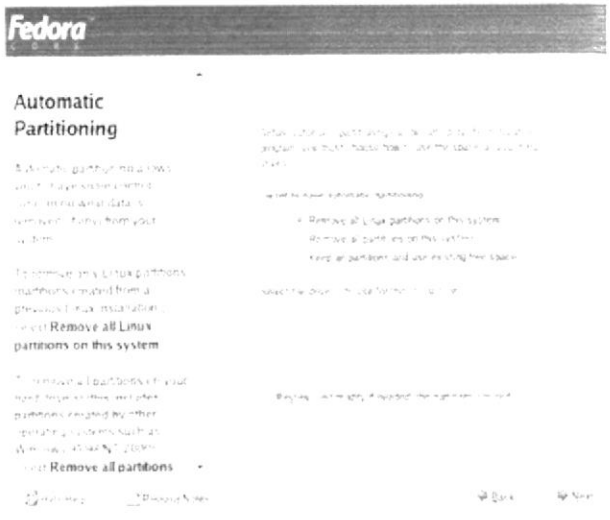

Fig. 6.12 Elección de partición

Seleccione la opción que desee, luego, elija algún disco donde desee crear las particiones para Linux. Si su sistema solo tiene un disco, ese disco es seleccionado automáticamente, Cualquier disco que seleccione es usado para las particiones de Linux de acuerdo con lo seleccionado anteriormente. La opción de selección es Global, y no requiere una diferente selección por cada disco.

Si quita alguna partición existente. El programa de instalación le pregunta para confirmar esta selección. Después de revisar y aprobar la configuración de partición, escoja **Next** para continuar con el siguiente paso de la instalación.

Un sistema Fedora Core tiene por lo menos 3 particiones:

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

Disk Fruid es un programa interactivo para editar las particiones de disco. Disk Fruid aguanta RAID y LVM para proveer almacenamiento más extenso y fiable.

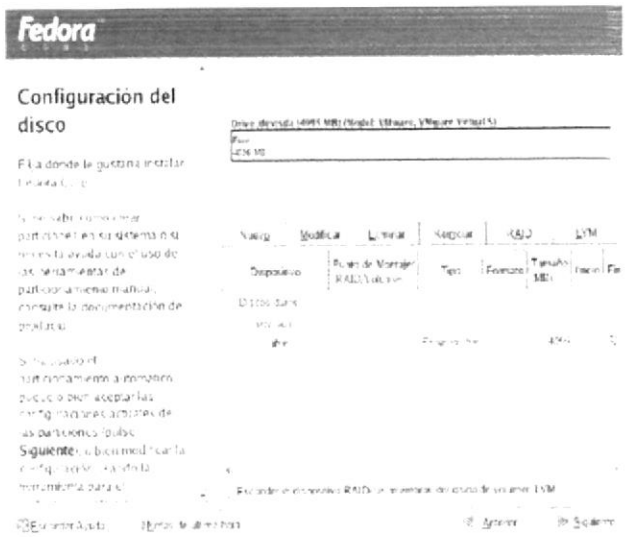

Fig. 6.13 Disk fruit

Seleccione la partición Boot. Le asignará 100 en "Tamaño (MB). Presione **Aceptar** una vez hecha la selección.

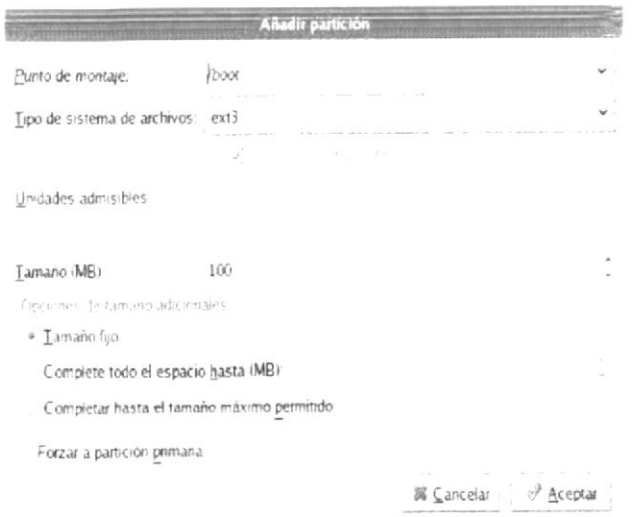

Fig. 6.14 Partición boot

Seleccione la partición Swap le asignará el doble el doble de lo que tenga en memoria para "Tamaño (MB)" pero solo hasta 512. Presione **Aceptar** una vez hecha la selección.

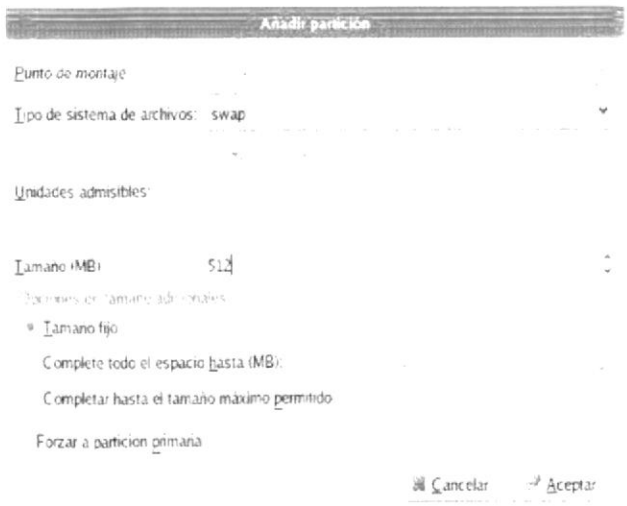

Fig. 6.15 Partición swap

Seleccione la partición Root (/) la cual será nuestro tamaño de almacenamiento. Presione **Aceptar** una vez hecha la selección.

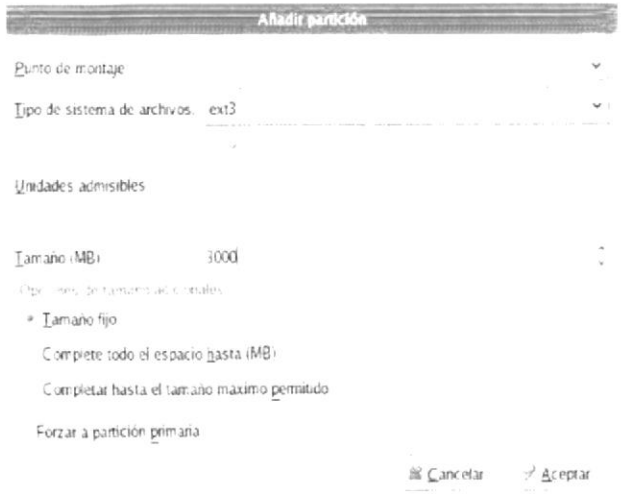

Fig. 6.16 Partición root

6.2.9 CONFIGURACIÓN DEL GESTOR DE ARRANQUE

La siguiente pantalla es la de configuración del gestor de arranque **GRUB** en donde se almacenara el sistema operativo para que inicie al encender la máquina. Presione **Siguiente**.

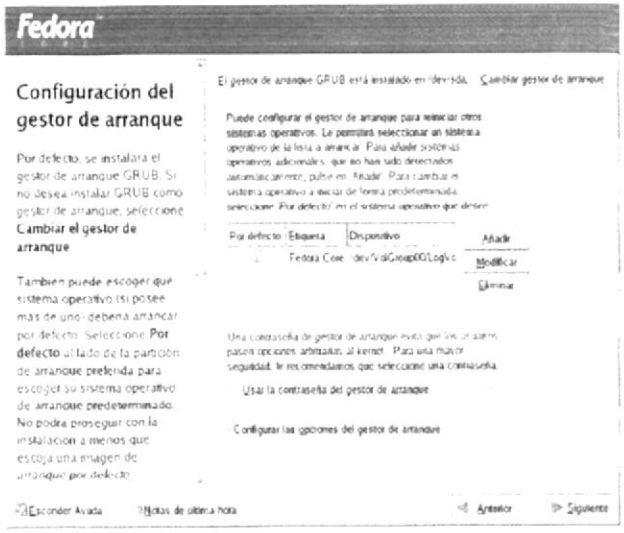

Fig. 6.17 Gestor de arranque (GRUB)

6.2.10 CONFIGURACIÓN DE LA TARJETA DE RED

Configure la tarjeta de red con su respectiva dirección IP, DNS primario, DNS secundario, una vez configurada todo presione **Siguiente** para continuar

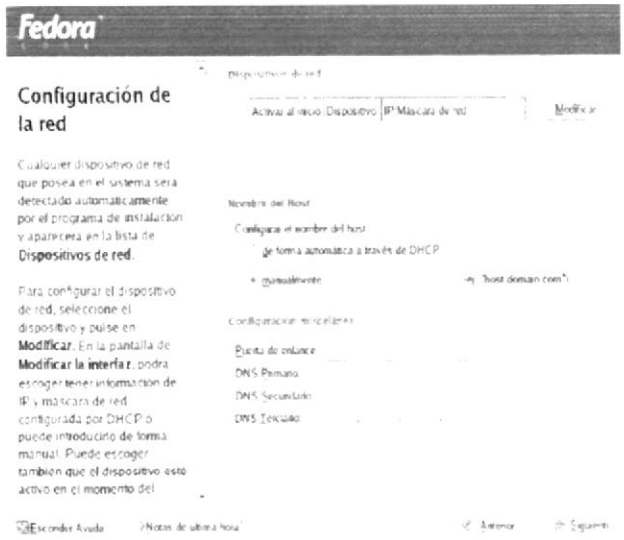

Fig. 6.18 Configurar tarjeta de red

6.2.11 CONFIGURACIÓN DE FIREWALL

En la configuración de cortafuegos seleccione ningún cortafuego, Presione **Siguiente** para continuar.

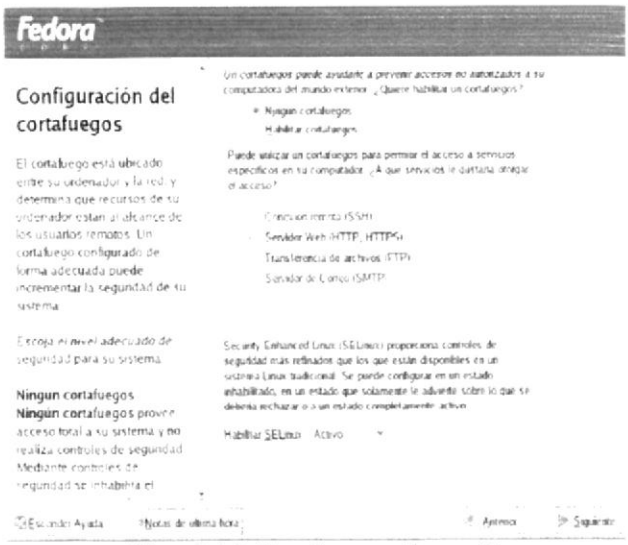

Fig. 6.19 Configurar firewall

6.2.12 SELECCIÓN DE IDIOMA

En la selección de idioma seleccione (español – Ecuador), Presione **Siguiente** para continuar.

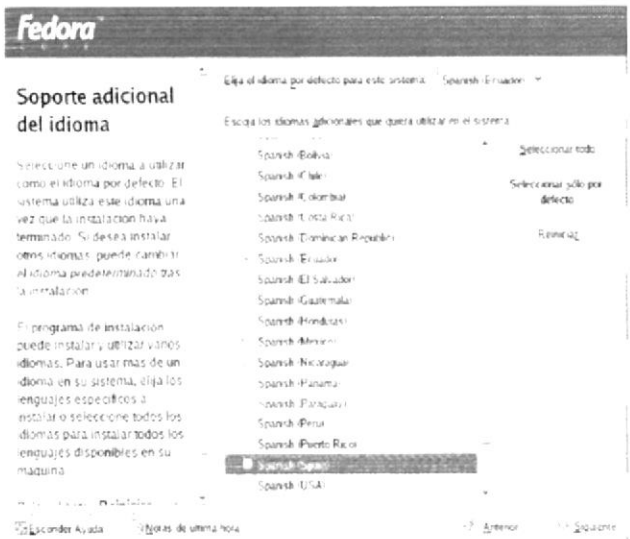

Fig. 6.20 Configurar idioma

6.2.13 SELECCIÓN DE ZONA HORARIA

Esta pantalla permite que usted especifique correctamente el uso horario de su ubicación actual en el computador. Especifique una zona aunque usted planea utilizar NTP (Network Time Protocol) para mantener la precisión del reloj del sistema.

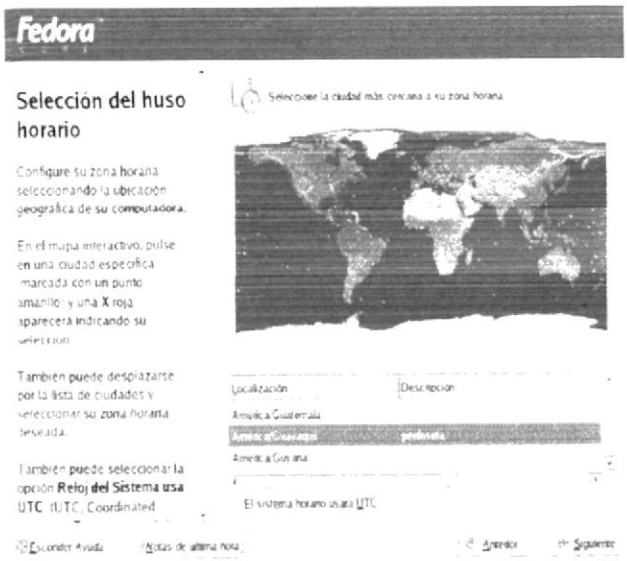

Fig. 6.21 Zona horaria

6.2.14 CONFIGURACIÓN DE LA CONTRASEÑA DEL ROOT

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

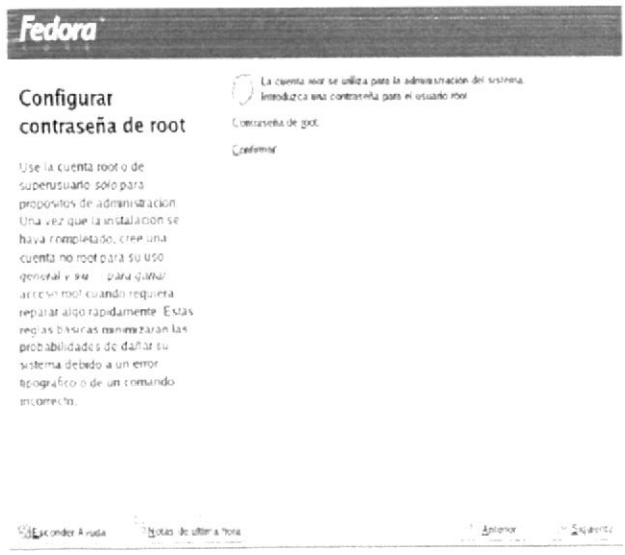

Fig. 6.22 Contraseña de root

6.2.15 SELECCIÓN DE PAQUETES

Fedora utiliza el tipo de instalación para seleccionar un juego de paquetes de programas para su sistema. Puede aceptar este juego de paquetes o elegirlo a su gusto para cumplir con sus preferencias. Si escoge el tipo de instalación personalizada, Fedora Core muestra la pantalla de Selección de grupo de paquetes automáticamente.

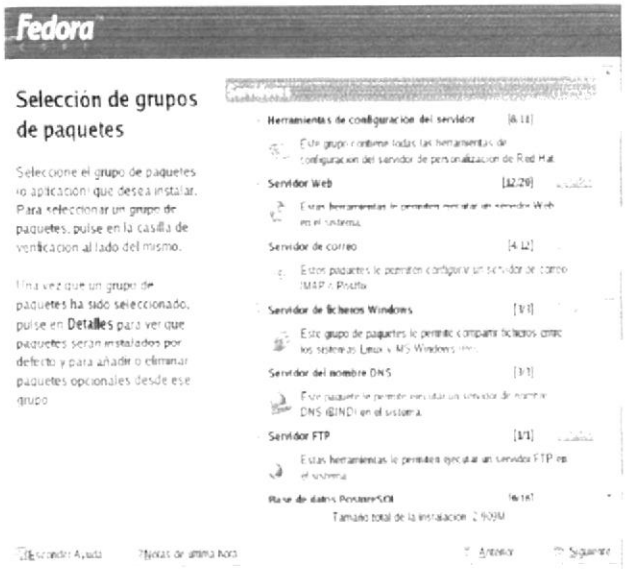

Fig. 6.23 Selección de paquetes

6.2.16 INSTALACIÓN DE PAQUETES

Fedora Core reporta el progreso de la instalación en la pantalla mientras que instala los paquetes seleccionados al sistema, seleccione **Siguiente** para continuar la instalación

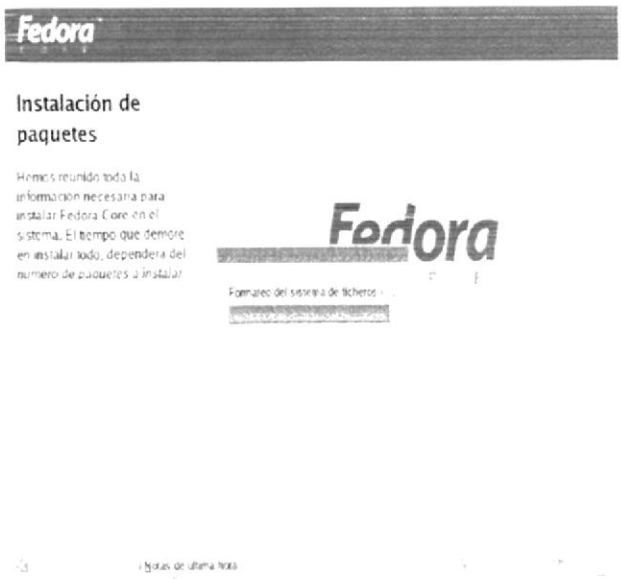

Fig. 6.24 Instalación de paquetes

Terminada la instalación del sistema operativo reinicie el equipo:

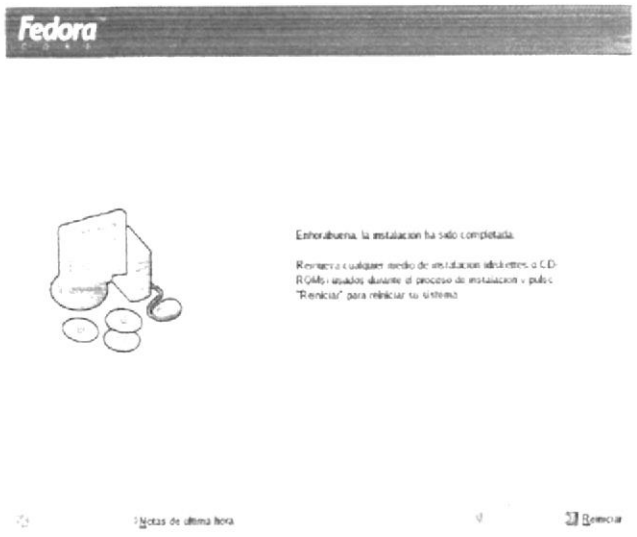

Fig. 6.25 Reiniciar el equipo

6.2.17 PRIMER ARRANQUE

El Agente de configuración se carga la primera vez que inicia un nuevo sistema de Fedora Core.
Use el agente de configuración para configurar el sistema para usarlo antes de que ingreses al sistema.

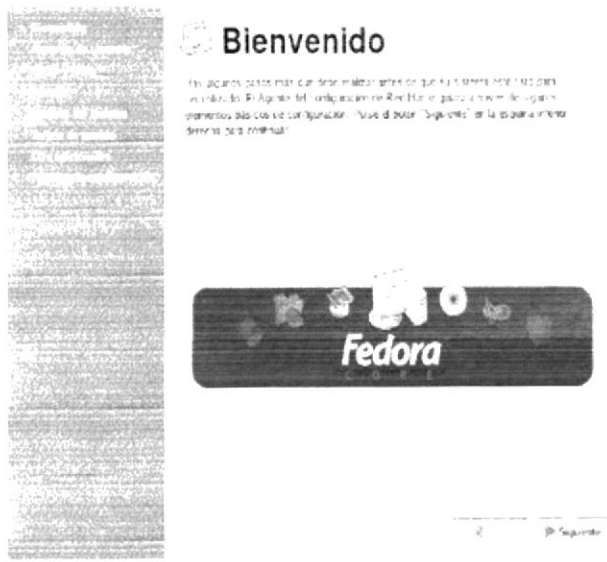

Fig. 6.26 Primer arranque

Seleccione **Siguiente** para comenzar el agente de configuración

6.2.18 ACUERDO DE LICENCIA

Esta pantalla exhibe los términos de licencia que contiene Fedora Core. Cada paquete de software en Fedora Core esta cubierto por su propia licencia que ha sido aprobada por la OSI Open Source Initiative (iniciativa de Código abierto)

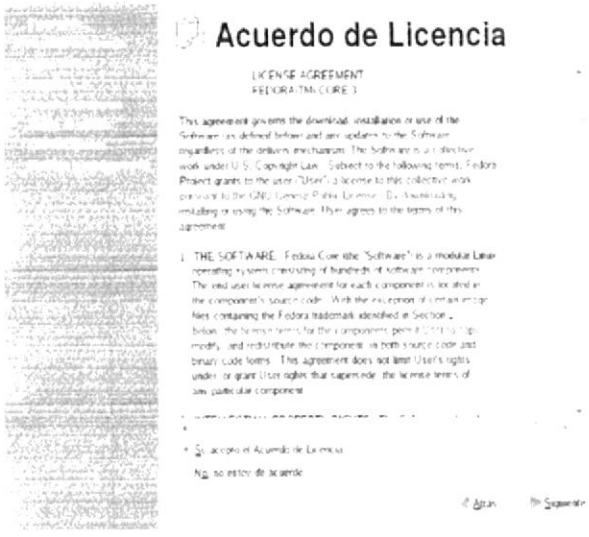

Fig. 6.27 Acuerdo de licencia

6.2.19 USUARIOS DEL SISTEMA

Cree una cuenta de usuario para usted con esta pantalla. Siempre use esta cuenta para iniciar sesión en su sistema Fedora Core, En el caso de administrar varios servicios puede usar la cuenta de root y saltar este paso, si lo desea, puede crear usuarios del sistema pero no tendrán privilegios administrativos como el super-usuario root

Fig. 6.28 Usuarios del sistema

Finalmente se da por terminada la configuración

Fig. 6.29 Fin de configuración

6.2.20 INICIALIZACIÓN DE LINUX FEDORA CORE 3

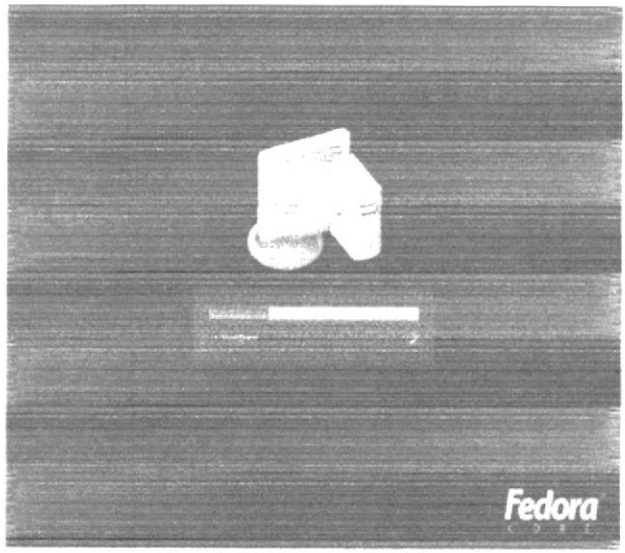

Fig. 6.30 Inicio de Linux

6.2.21 INICIO DE SESIÓN EN LINUX FEDORA CORE 3

Para iniciar sesión en una instalación de Linux normalmente existen dos opciones las cuales son:

- Modo texto y
- Modo Gráfico

La combinación de las teclas ctrl. + alt + F1 permite ingresar a un inicio de sesión en **Modo texto** aunque con la misma combinación terminada en F2, F3, F4, F5 y F6 también permiten iniciar sesión en modo texto cada una de estas combinaciones son terminales diferentes, de modo que puedo estar levantando configurando algún servicio en una Terminal y enviando un correo en otra.

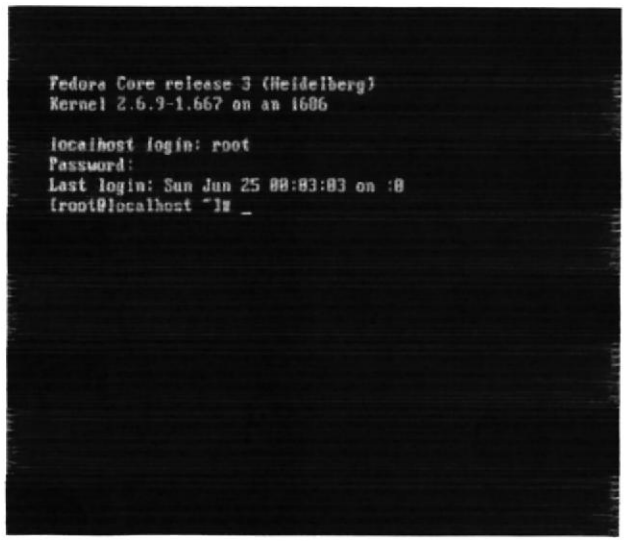

Fig. 6.31 Inicio Modo Texto

Pantalla de inicio de sesión en modo texto, la combinación de las teclas ctrl. + alt + F7 permite ingresar a un inicio de sesión en Modo gráfico, aunque desde el modo gráfico puedo abrir Terminales en forma de ventanas
Cuando usted ha realizado una instalación de Linux agregando el modo gráfico este se cargará por defecto

Se ingresa el username del administrador en este caso se utiliza root (viene por default desde la instalación de Linux), en caso de que el usuario tenga otro username con su respectivo password también podrá ingresar al sistema operativo pero no con los mismos privilegios del administrador

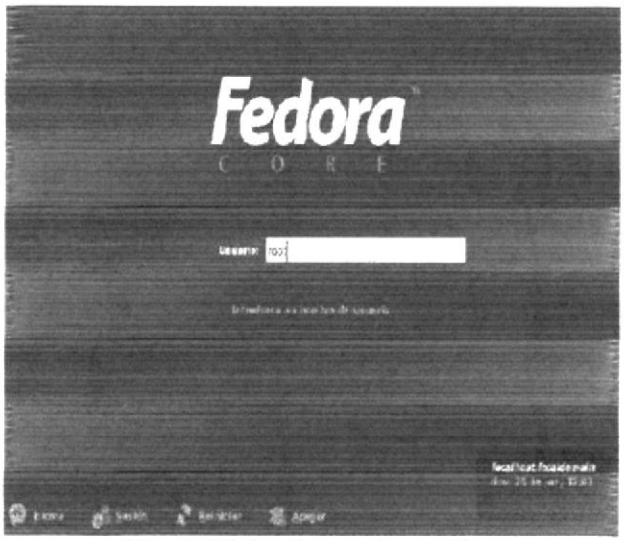

Fig. 6.32 Inicio modo gráfico

La primera vez que se accede al sistema la contraseña empleada será la proporcionada por el administrador del sistema
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

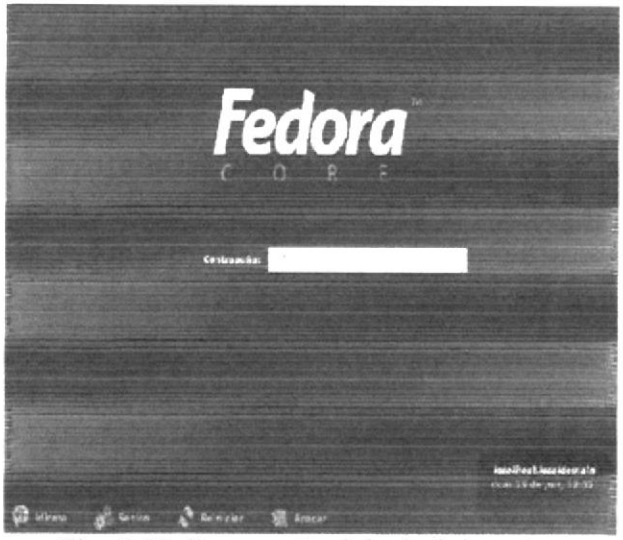

Fig. 6.33 Contraseña del administrador

6.2.22 ENTORNO DE LINUX FEDORA CORE 3

La primera vez que se accede al sistema operativo se podrá ver el entorno de Linux (escritorio), podrá notar que es muy parecido a Windows.

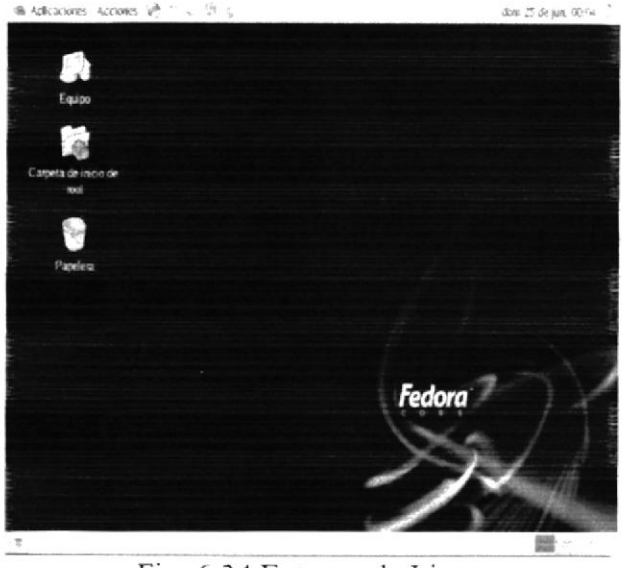

Fig. 6.34 Entorno de Linux

6.2.23 AGREGAR O QUITAR PAQUETES

Si necesita agregar o quitar algún paquete de instalación se hará siguiente:
Dar clic en aplicaciones elige configuración del sistema y dar clic en Añadir/Eliminar aplicaciones

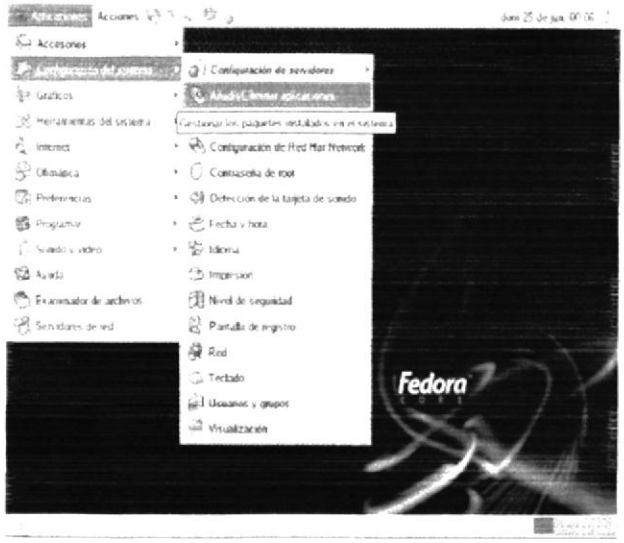

Fig. 6.35 Agregar o quitar paquetes

6.3 INGRESAR A UNA TERMINAL

Hay dos opciones de acceder a una Terminal:

- Dar clic en aplicaciones, herramientas del sistema y elegir abrir una Terminal,
- Clic derecho en el escritorio, elegir abrir una Terminal.

Cualquiera de las dos opciones llevara a la siguiente pantalla en la cual se podrá realizar las configuraciones tanto de la tarjeta de red como de los servidores.

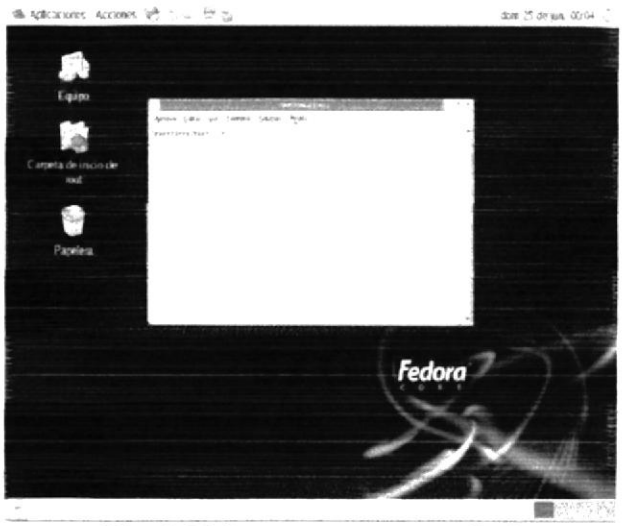

Fig. 6.36 Ingresar a una terminal

6.4 CONFIGURAR LA TARJETA DE RED

Verifique si la tarjeta de red esta configurada, esto lo hace con el comando ifconfig

Fig. 6.37 Configurar tarjeta de red

En caso de que no esté configurada la tarjeta de red, tiene dos opciones a seguir:

- Utilizando el comando ifconfig, como esta detallado a continuación

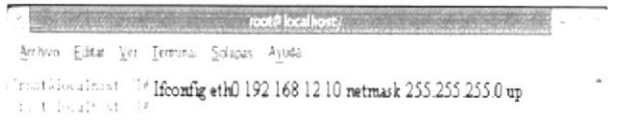

Fig. 6.38 Ifconfig

- Utilizando el comando netconfig que seria en interfaz gráfica

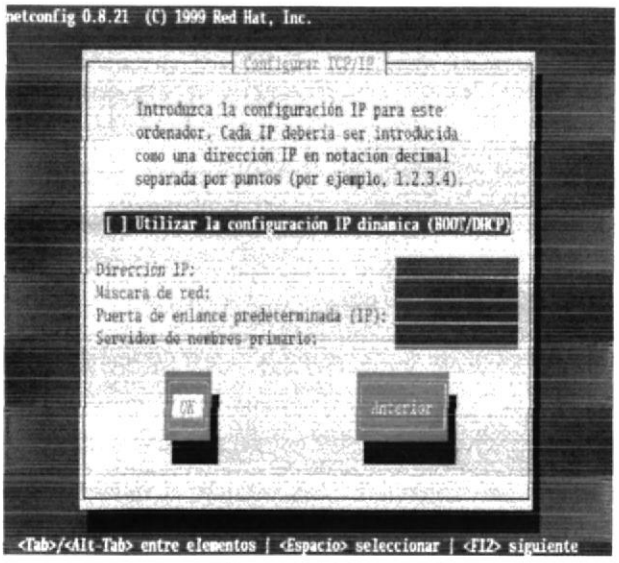

Fig. 6.39 Netconfig

Una vez que configura la tarjeta de red digite el comando ifconfig para verificar si esta se configuro.

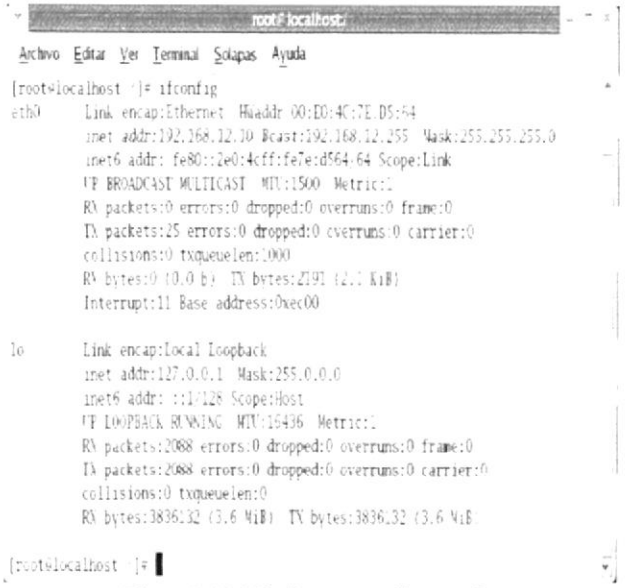

Fig. 6.40 Tarjeta configurada

6.5 SAMBA

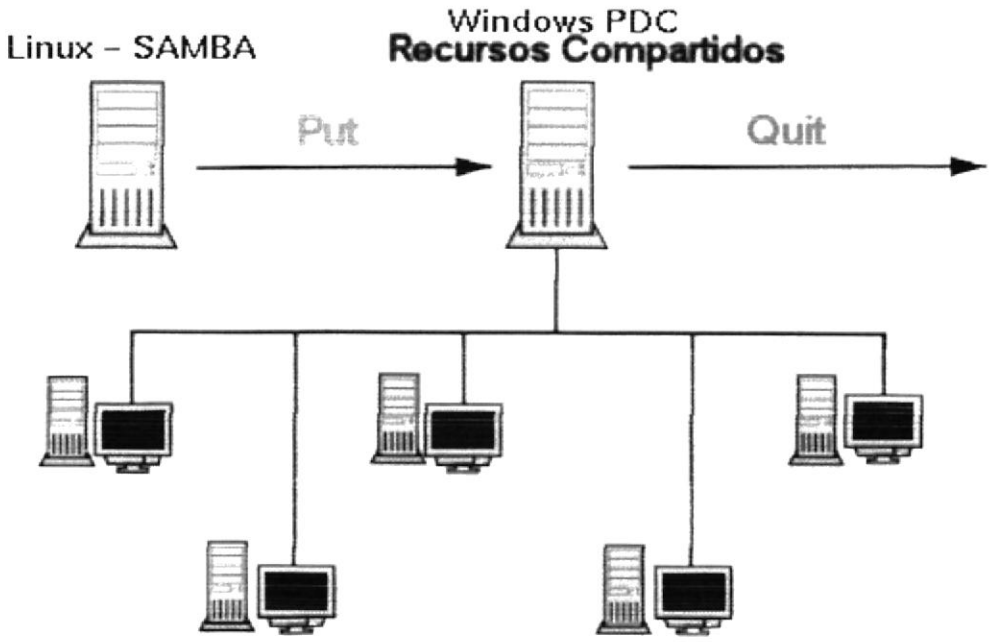

Fig. 6.41 Samba

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.

Los ficheros relacionados con la configuración del servidor Samba se agrupan en el directorio /etc/samba/. El fichero de configuración principal es smb.conf. Básicamente smb.conf solo consta de varias secciones que se identifican a través de una cadena encerrada entre corchetes. Existen tres secciones especiales:
[global] : agrupa los aspectos generales del servidor Samba.
[homes] : reúne los aspectos relacionados con la forma en que se compartirán los directorios de todos los usuarios.
[printers] : agrupa los aspectos relacionados con las impresoras a compartir.

5.5.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Tener deshabilitado los firewall (cortafuegos), esto se verifica al digitar el comando setup, se elige la opción configuración de firewall y se podrá verificar el estado

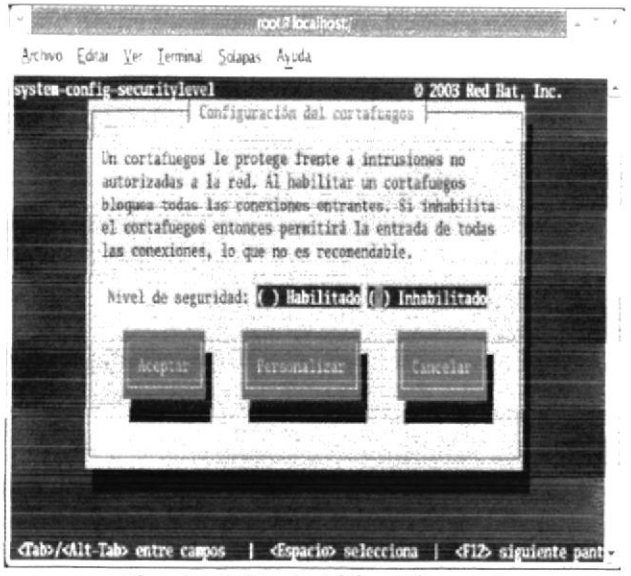

Fig. 6.42 Deshabilitar firewall

5.5.2 CONFIGURACIÓN

Verificar si el paquete de samba esta instalado, caso contrario digitar el comando setup, se elige la opción Servicios del Sistema y habilitar network, smb y xinetd.

[root@localhost /] rpm –q samba
[root@localhost /] rpm –q network
[root@localhost /] rpm –q xinetd

Editar el archivo de configuración de samba

[root@localhost /] vi /etc/samba/smb.conf

En los párrafos Global Settings y Share Definitions se realizan ciertas modificaciones las cuales se detallaran mas adelante

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

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

NetBIOS. Es importante entender que son dos cosas totalmente diferentes.

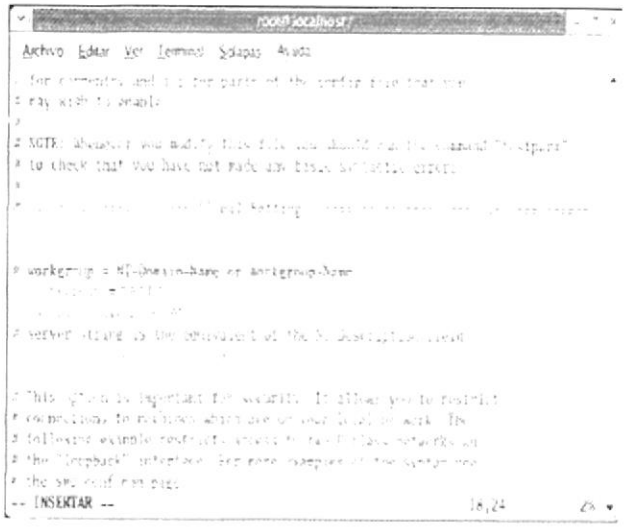

Fig. 6.43 Global settings

El menú **Browseable** indica que este recurso debe ser anunciado por nmbd, y por tanto ser visible para todos los usuarios.
El menú **Writable** indica que este recurso debe ser anunciado por nmbd, y por tanto debe tener permiso de escritura para todos los usuarios.
Public para que sea publica.
Para cada recurso es posible restringir el acceso a ciertos usuarios. Para cada una de las líneas de recursos compartidos en /etc/smb.conf, se puede añadir la línea: **Valid Users.**
En su ausencia, el recurso es accesible por todos los usuarios del servidor Samba. Si esta línea esta presente el acceso esta reservado únicamente a los usuarios mencionados.

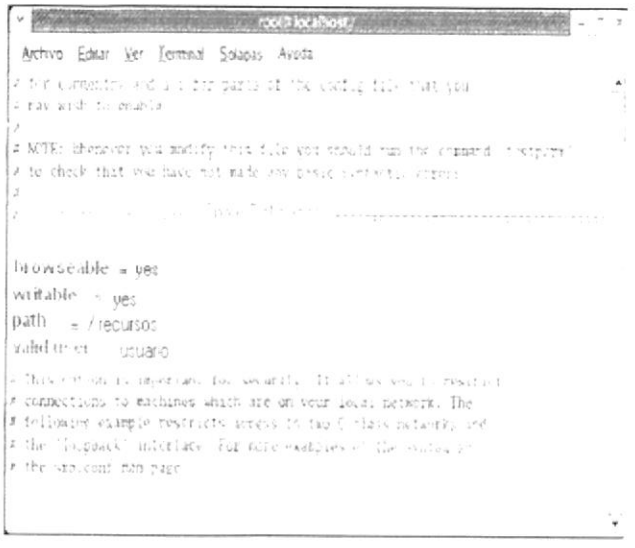

Fig. 6.44 Share definitions

Salir con esc: wq para guardar los cambios.

Las configuraciones hechas en esta sección se aplican a la totalidad de los recursos compartidos, independientemente de la configuración especifica.

Crear directorio (Tópico) con el comando mkdir.

Fig. 6.45 Mkdir (crear directorio)

Crear el archivo en el directorio, esto se hace con el comando touch.

Fig. 6.46 Touch (crear archivo)

Asignar los respectivos permisos al directorio y al archivo.

Fig. 6.47 Chmod (permisos)

Crear los usuarios que anteriormente se registraron en el campo valid user y darle su respectiva contraseña.

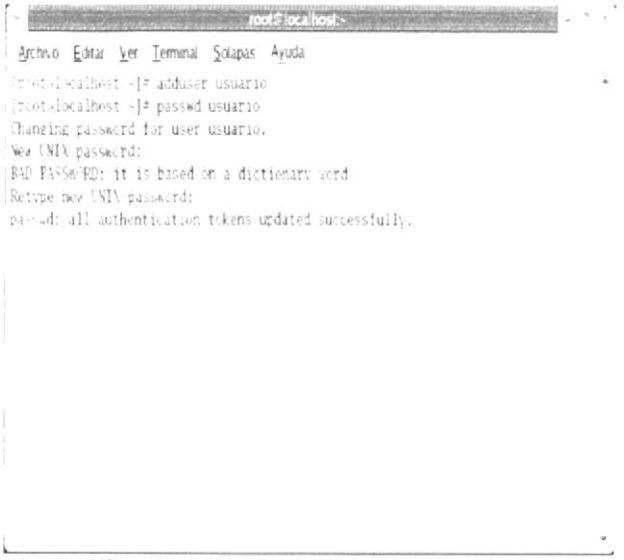

Fig. 6.48 Adduser (crear usuarios)

Asignar contraseñas a los usuarios para hacer uso del servicio de samba, es decir para poder acceder a los recursos de Linux desde windows.

Fig. 6.49 Asignar contraseñas

Restaurar los servicios de samba.

Fig. 6.50 Restaurar los servicios samba

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS DE SAMBA

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mensionados,
- Verificar si los firewall estan deshabilitados, ya que es un requerimiento para que samba funcione
- Verificar en los servicios del sistema si estan instalados los paquetes smb, network y xinetd
- Verificar si están asignados los permisos a los usuarios para poder acceder a los recursos Linux desde Windows

5.5.3 CONFIGURACIÓN EN WINDOWS

Acceder a la máquina Linux por medio de la dirección IP, esto se hace en inicio. Ejecutar y poner la dirección del servidor en este caso 192.168.12.10.

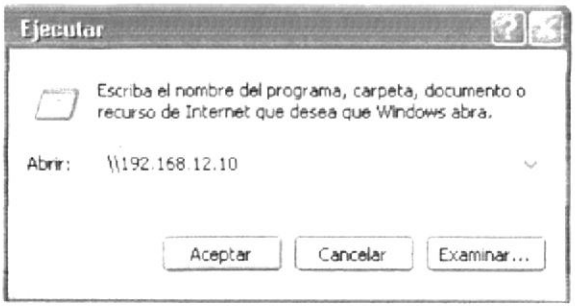

Fig. 6.51 Ejecutar

Ingresar el usuario al que se dio los respectivos permisos en la configuración de samba con su respectivo password.

Fig. 6.52 Usuario y passwd

Verificar que puede acceder a los recursos compartidos del servidor Samba

Fig. 6.53 Recursos samba

5.6 DNS

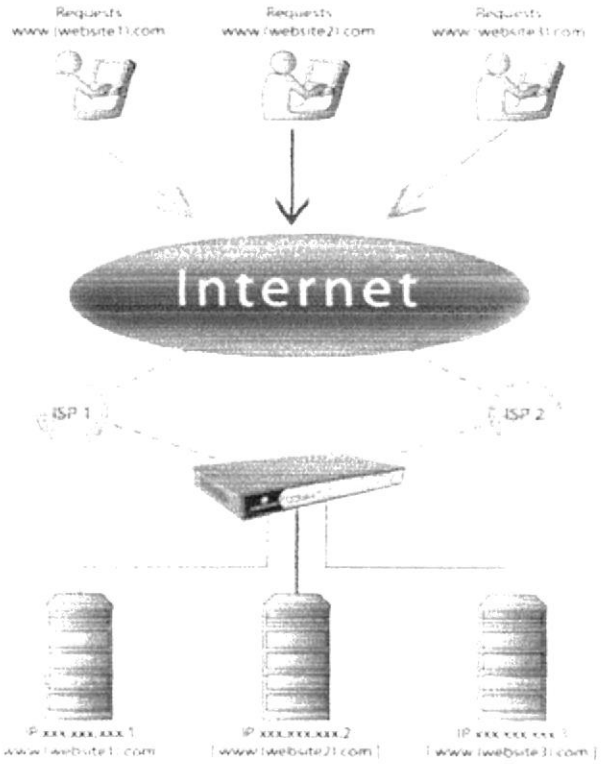

Fig. 6.54 DNS

Domain Name System (Sistema de Dominio de Nombre), esta configuración realizada en un servidor me 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.

Antes de empezar, debe configurar su sistema convenientemente, de forma que pueda hacer telnet desde y hacia su máquina, efectuando satisfactoriamente toda clase de conexiones de red, especialmente telnet 127.0.0.1 entrando en su propia máquina (compruébelo ahora). También necesita que los archivos /etc/host.conf (o /etc/nsswitch.conf), /etc/resolv.conf y /etc/hosts sean correctos como punto de partida.

6.6.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.

- Tener deshabilitado los firewall (cortafuegos), esto se verifica al digitar el comando setup, se elige la opción configuración de firewall y se podrá verificar el estado

6.6.2 CONFIGURACIÓN

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

[root@localhost /] rpm –q bind

Para empezar se debe editar el archivo de configuración de DNS que es named.conf el mismo que esta ubicado en la siguiente ruta:

[root@localhost /] vi /etc/ named.conf

Observarán todos los dominios ya existentes, aquí puede facilitar la escritura copiando uno de estos párrafos (con la tecla Y seguido del número de líneas que se desea copiar; y se pega con la letra P), vale recalcar que estas Líneas se las agrega.

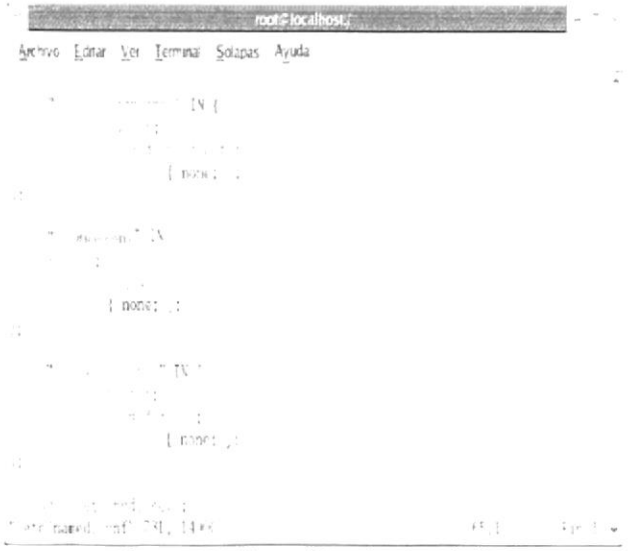

Fig. 6.55 Creación de dominios

Salir con esc: wq para guardar los cambios.

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

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

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

Una vez que se modifica el archivo de configuración named.conf, se ingresa a la siguiente ruta.

Fig. 6.56 var/named/chroot/var/named

Proceder a copiar el dominio

[root@localhost /] cp localhost.zone pacifico.com

El comando cp permite copiar el contenido de un archivo existente (localhost.zone) a uno recién creado (pacifico.com).

Ahora se modificará el archivo que se copio en este caso pacifico.com

[root@localhost /] vi pacifico.com

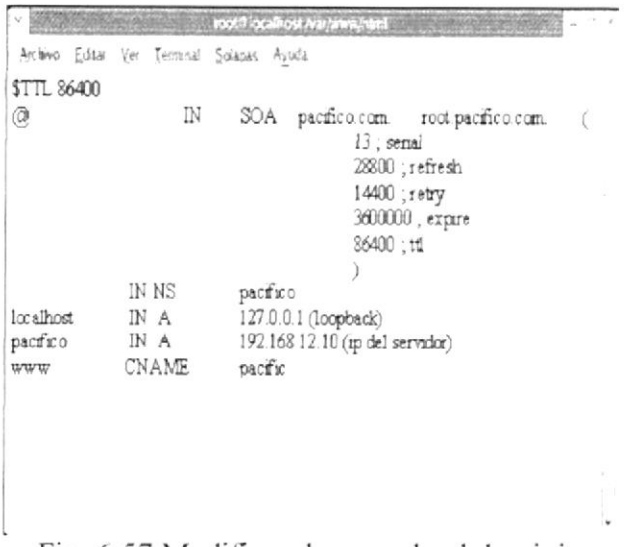

Fig. 6.57 Modificar de acuerdo al dominio

Salir con esc: wq para guardar los cambios.

A especifica la dirección real IP
NS apunta a una posición específica del servidor de nombres
CNAME el nombre canónico para un alias
SOA marca el principio de la zona de autoridad (dominio, dirección del responsable de zona, número de serie)
TTL: tiempo de vida en segundos que un servidor DNS o un resolver debe guardar en caché esta entrada antes de descartarla.

Restaurar los servicios del named

Fig. 6.58 Restaurar los servicios named

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS BIND

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mensionados,
- Verificar en los servicios del sistema si esta instalado el paquete bind

Probar que funciona haciéndole ping al DNS creado.

[root@localhost /] ping www.pacífico.com

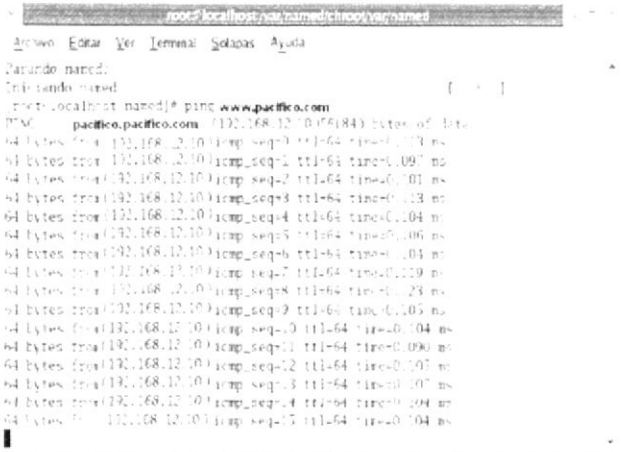

Fig. 6.59 Ping de verificación

En caso de que el ping no funcione se deberá ir a la ruta vi /etc/resolv.conf

Ahí se encontrará el NameServer, y se debe confirmar que la IP sea la misma que de tarjeta de red (192.168.12.10)

Fig. 6.60 vi /etc/resolv.conf

6.6.3 CONFIGURACIÓN EN WINDOWS

Existen varias opciones de acceder a mis sitios de red, el icono esta en el escritorio pero en caso de no estar, la mas usual es: clic derecho en inicio, elegir explorar y elegir mis sitio de red, se da clic derecho y elegir propiedades

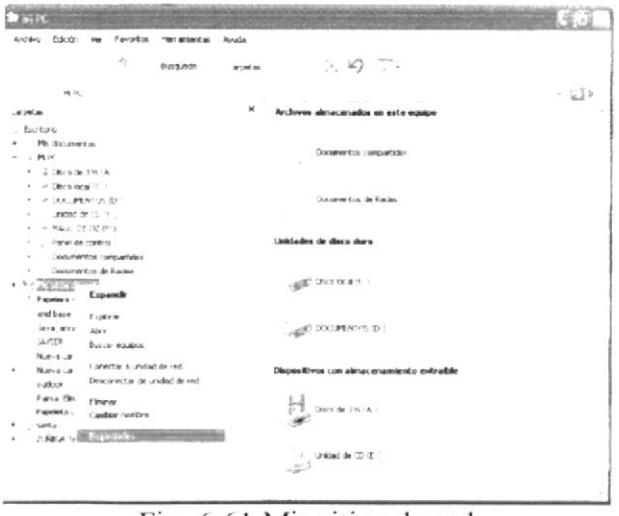

Fig. 6.61 Mis sitios de red

Se observará la pantalla de conexiones de red, se da clic derecho al icono de conexiones de área local y se elige propiedades.

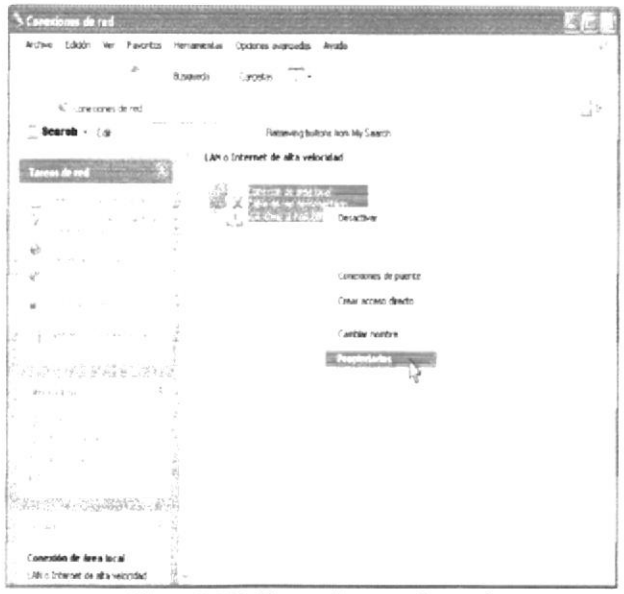

Fig. 6.62 Conexiones de red

Aparecerá la pantalla de propiedades de conexión de área local, se le dará doble clic en protocolo Internet (TCP/IP) o se sombrea y se elige la pestaña de propiedades.

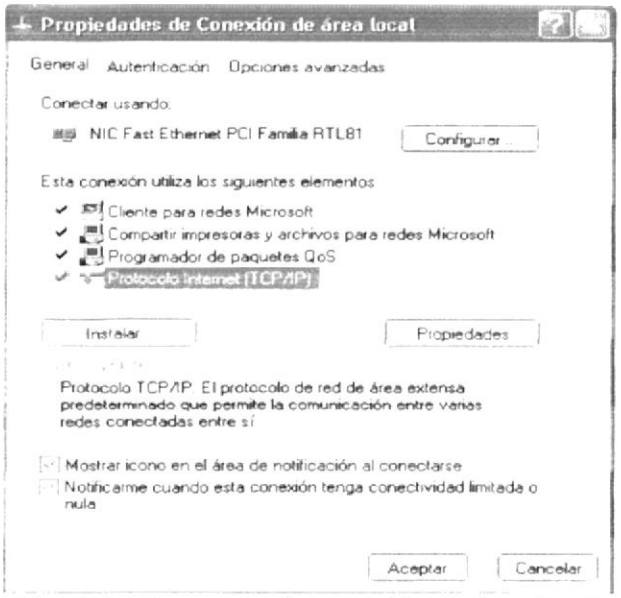

Fig. 6.63 Protocolo de conexión de área local

Configurar la tarjeta de red, se debe asignar su respectiva dirección como también se le dará la dirección del servidor DNS.

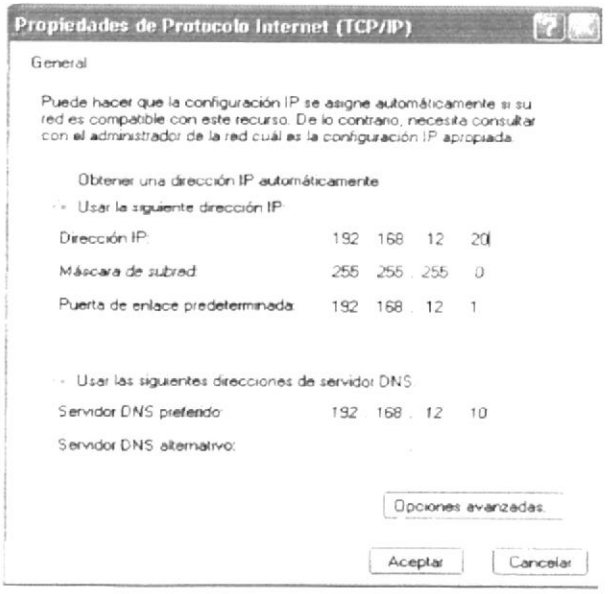

Fig. 6.64 Propiedades de protocolo de Internet

Verificar DNS, esto se hará al dar clic en inicio elegir accesorios, símbolos del sistema o, dar clic en inicio se elige ejecutar y procederá hacer el ping a www.pacifico.com.

6.7 WEB SERVER

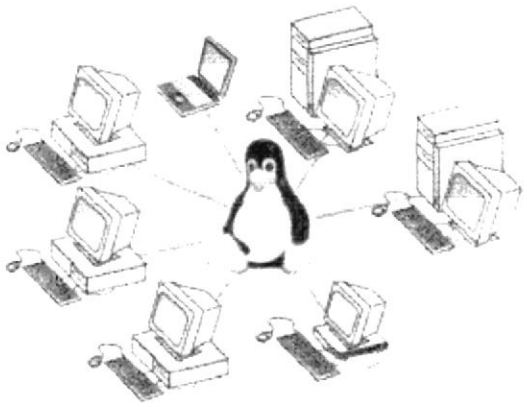

Fig. 6.65 Servidor web

6.7.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Tener deshabilitado los firewall (cortafuegos), esto se verifica al digitar el comando setup, se elige la opción configuración de firewall y se podrá verificar el estado

6.7.2 CONFIGURACIÓN

Para empezar la configuración de Web Server (Servidor Web) se necesita como requisito tener levantado DNS y contar con el paquete httpd.

[root@localhost /]rpm –q httpd

Una vez que verifica si esta el paquete instalado configurar el archivo httpd.conf

Fig. 6.66 Vi /etc/httpd/conf/httpd.conf

Buscar las siguientes líneas (Puede hacerlo por secciones o por líneas) y descomentarlas

En el parámetro **directory index** se agrega el nombre y la extensión del archivo que se va a crear en el caso que no se encuentra especificado

En el párrafo del ***<virtual host *:80>*** tendrá que realizar los siguientes cambios, facilitando 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).

Fig. 6.67 Virtual host

En la siguiente ruta crear la carpeta que alojará al sitio Web.

/var/www/html/

Ingresar a la ruta especificada y cree la carpeta web.

cd /var/www/html/
mkdir web

Una vez creada la carpeta, ingrese a ella y editar el sitio index (en donde se encontrará el sitio web.

cd web
touch index.html
vi index.html
(Agregar cualquier texto)

Restaurar los servicios httpd

Fig. 6.68 Restaurar servicios de httpd

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS HTTPD

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mensionados,
- Verificar en los servicios del sistema si esta instalado el paquete httpd

Ir al navegador y cargar la página, en este caso:

www.pacífico.com

Acceder al sitio web mediante el navegador. Recordar que tendrá que haber asignado la dirección DNS en el equipo con sistema operativo windows.

Fig. 6.69 Cargar la página

6.7.3 CONFIGURACIÓN EN WINDOWS

Ingresar al explorador de windows, herramientas, opciones de Internet

Fig. 6.70 Explorador de windows

Dentro de opciones de Internet elegir la pestaña conexiones, dar clic en configuración de la red LAN

Fig. 6.71 Opciones de Internet

Digitar la dirección del servidor y el Puerto de comunicación en este caso para web server es el 80, se da clic en aceptar y se da por terminada la configuración.

Fig. 6.72 Configuración de la red de área local

Verificar la página cargada desde windows.

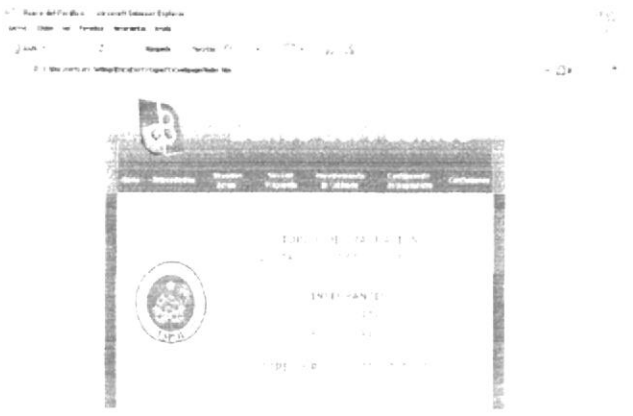

Fig. 6.73 Página Cargada desde windows

6.8 PROXY

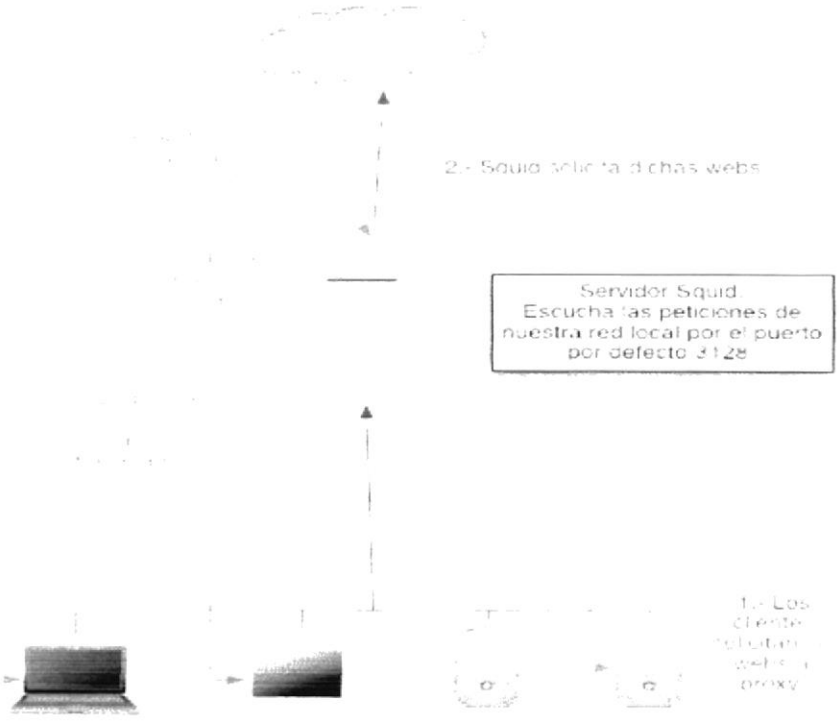

Fig. 6.74 Servidor proxy

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.

Squid

Software para servidor Proxy más popular y extendido.
Es muy confiable, robusto y versátil. Hace de Proxy y caché con los protocolos HTTP, FTP, GOPHER y protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y de consultas DNS y otras.

6.8.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.

- Tener deshabilitado los firewall (cortafuegos), esto se verifica digitando el comando setup, elegir la opción configuración de firewall y se podrá verificar el estado

Para realizar la configuración de un servidor Proxy, se 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.

[root@localhost /] rpm –q squid

6.8.2 CONFIGURACIÓN

Comprobar la IP del servidor
[root@localhost /] ifconfig

Para configurar el archivo squid se debe editarlo en la ruta que se muestra a continuación.

[root@localhost /] vi /etc/squid/squid.conf

En esta sección se debe descomentar ciertas líneas, como es el caso del puerto 8080, el cual nos permitirá "escuchar".

http_port
(Si Ud. tiene http_port 3128, cámbiela por http_port 8080)

cache_men 16 MB
(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
(linea para monitorear la actividad de los hosts que tenga a cargo el proxy)

Ahora a las listas de acceso:

acl red src 192.168.12.10/255.255.255.0
(ip del servidor y máscara)

http_access allow red
(Aquí se permite que la red que se ha especificado en la ACL pueda tener acceso a navegar)

Restaurar el servicio del SQUID

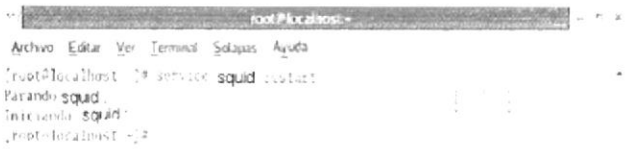

Fig. 6.75 Restaurar los servicios squid

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS SQUID

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mencionados,
- Verificar en los servicios del sistema si esta instalado el paquete squid.

6.8.3 CONFIGURACIÓN EN WINDOWS

Ingresar al explorador de windows, herramientas, opciones de Internet

Fig. 6.76 Explorador de windows

Dentro de opciones de Internet elegir la pestaña conexiones, dar clic en configuración de la red LAN

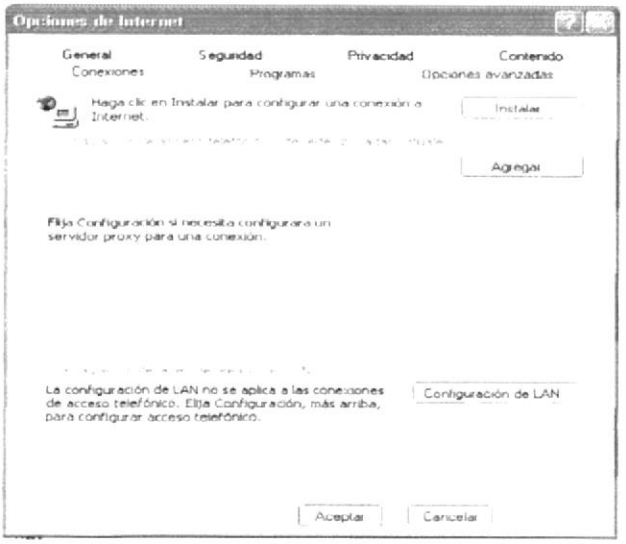

Fig. 6.77 Opciones de Internet

Digitar la dirección del servidor y el Puerto de comunicación en este caso para proxy es el 8080, se da clic en aceptar y se da por terminada la configuración.

Fig. 6.78 Configuración de red de área local

Verificar la página cargada desde windows.

Fig. 6.79 Página Cargada desde windows

6.8.4 DENEGAR ACCESOS POR 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 máquina 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
SábadoA	
Domingo	S

Pueden combinarse los días

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

Incluir las listas en las reglas de control de acceso
http_acces deny cliente matutino

Restaurar el servicio del SQUID

Fig. 6.80 Restaurar los servicios squid

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS SQUID

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mencionados,
- Verificar en los servicios del sistema si esta instalado el paquete squid

6.8.5 ACCESO CON AUTENTICACIÓN

Crear el archivo claves.
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 autentificación 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.

Restaurar el servicio del SQUID

Fig. 6.81 Restaurar los servicios squid

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS SQUID

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mencionados,
- Verificar en los servicios del sistema si esta instalado el paquete squid

Una vez configurado el proxy con acceso de autenticación, se debe abrir el explorador de windows para cargar el sitio web, en este caso www.pacifico.com. Pedirá usuario y clave que fueron creados en Linux.

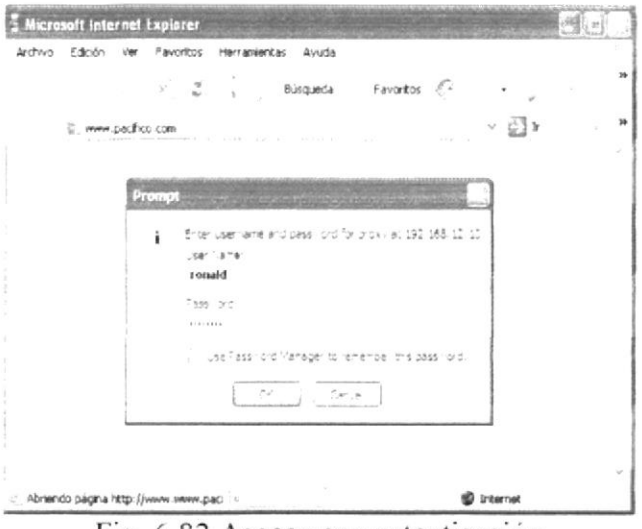

Fig. 6.82 Acceso son autenticación

6.8.6 DENEGAR PÁGINAS PROHIBIDA

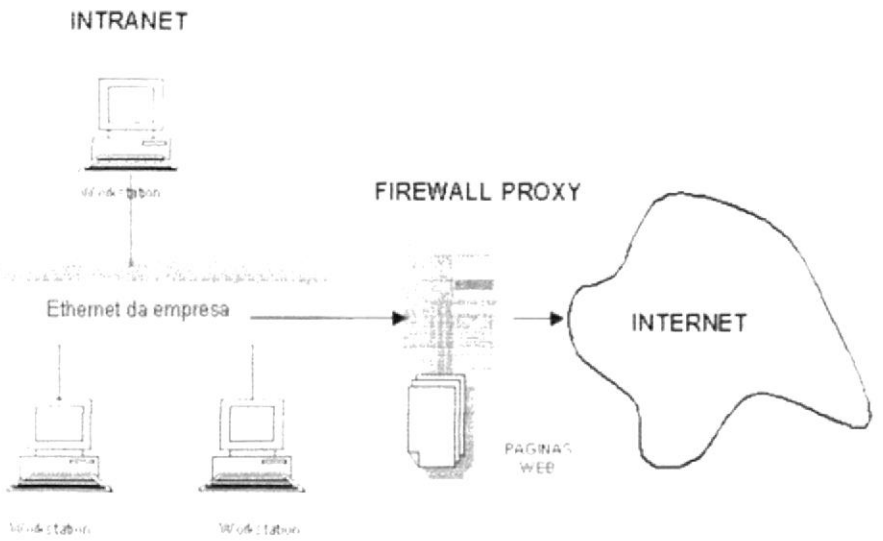

Fig. 6.83 Denegar páginas prohibidas

Configurar el archivo squid

Incluir lista de control de acceso
acl prohibidos src "/sitios/denegados"

Incluir regla de control de acceso
http_access deny red prohibidos

Crear directorio y archivo de sitios prohibidos

[root@localhost /] mkdir /sitios

[root@localhost /] cd /sitios (ingresa al directorio)

[root@localhost /] touch denegados (crea al archivo)

Editar archivo de páginas prohibidas

[root@localhost /] vi /sitios/denegados

www.hardcore.com
www.playboy.com
www.triplex.com

Salir con: wq para guardar los cambios del archivo

Restaurar el servicio del SQUID

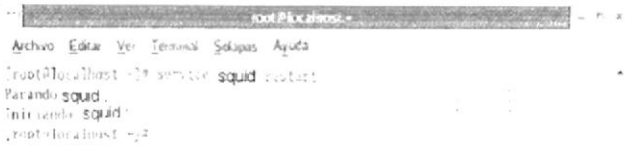

Fig. 6.84 Restaurar los servicios squid

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS SQUID

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mencionados.
- Verificar en los servicios del sistema si esta instalado el paquete squid

6.9 SEND MAIL

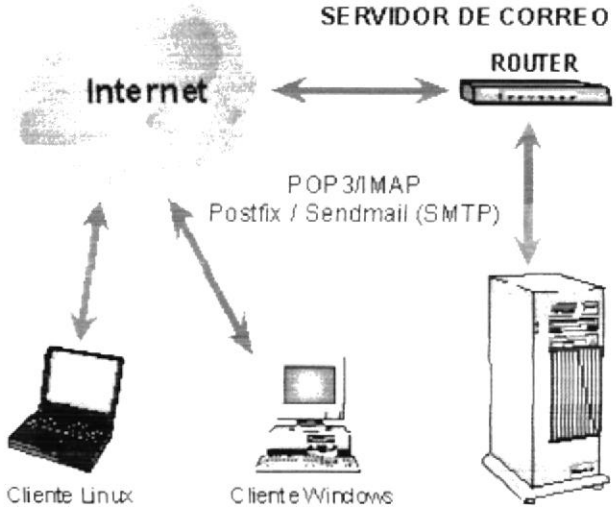

Fig. 6.85 Servidor de correo

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.

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

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

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

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

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

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

6.9.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.

- Tener deshabilitado los firewall (cortafuegos), esto se verifica digitando el comando setup, se elige la opción configuración de firewall y se podrá verificar el estado

6.9.2 CONFIGURACIÓN

Verificar si los paquetes sendmail y dovecot se encuentran instalados

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

Comprobar la IP del servidor

[root@localhost /] ifconfig

Editar el fichero donde se podrá ver si su PC esta en un dominio con la siguiente ruta

[root@localhost /] vi /etc/hosts

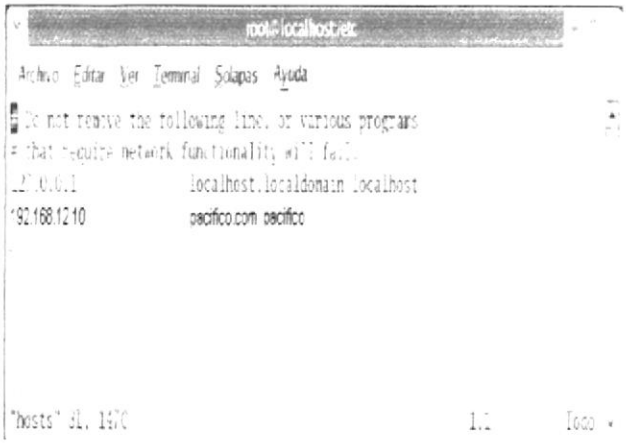

Fig. 6.86 Fichero hosts

Salir con esc: wq para guardar los cambios.

Es decir, se debe poner tanto el la dirección loopback y la IP del servidor

Ingresar al archivo krb5-telnet

[root@localhost /] vi krb5-telnet

Modificar este archivo

Fig. 6.87 Fichero krb5-telnet

Salir con esc: wq para guardar los cambios.

Editar el fichero que permitirá dar nombre al servidor. :

[root@localhost /] vi /etc/sysconfig/network

Fig. 88 Fichero network

Salir con esc: wq para guardar los cambios.

Editar el fichero SENDMAIL, con la siguiente ruta:

[root@localhost /] vi /etc/mail/sendmail.cf

En Cwlocalhost cambiar por el nombre del dominio que se creo

Fig. 89 Fichero sendmail

Donde 0.0.0.0 permite enviar y recibir e-mail's desde cualquier dirección.

Fig. 90 Permitir enviar y recibir mail

Salir con esc: wq para guardar los cambios.

Editar el fichero Dovecot con la siguiente ruta:

[root@localhost /] vi /etc/dovecot.conf

Buscar la linea, descomentar y agregar lo siguiente
protocols = imap imaps pop3

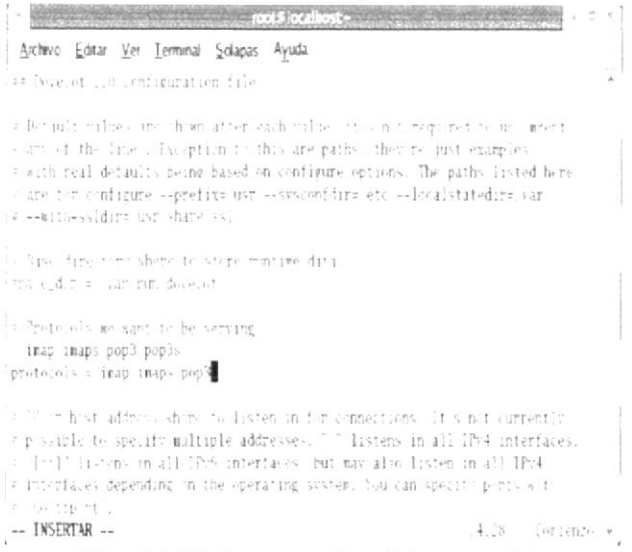

Fig. 91 Fichero sendmail(protocols)

Salir con esc: wq para guardar los cambios.

Revisar los puertos de descarga.

[root@localhost /] netstat –pelan | grep 110

Comprobar los puertos abiertos

[root@localhost /] netstat –an | more, o netstat –plan | more

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

6.9.3 CONFIGURACIÓN DE CLIENTES

Crear un usuario y darle su respectiva contraseña

[root@localhost /] adduser usuario (el que le proporcionen)
[root@localhost /] passwd usuario

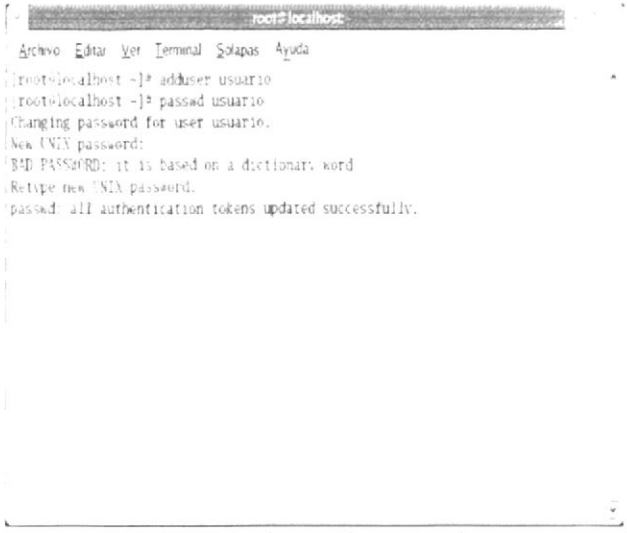

Fig. 92 Configuración de clientes

Reinicie los servicios del Dovecot Network y Sendmail

Fig. 93 Restaurar servicios

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS DE SEND MAIL, DOVECOT Y NETWORK

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mensionados,
- Verificar en los servicios del sistema si esta instalado el paquete sendmail, network, xinetd, dovecot que son indispensables para que el servidor de correo funcione
- Verificar si esta bien configurada la cuenta de correo en el Outlook Express tomando en cuenta los pasos que se detallará en las configuraciones de windows.

6.9.4 ENVÍO DE CORREO

Para verificar si se envia un mail

[root@localhost /] mail root@pacifico.com

Subject: nombre_usuario
Finalizar el mensaje con punto

Cc:/nombre_usuario

Para verificar un mail

[root@localhost /] mail

Para verificar correos de otros usuarios.

[root@localhost /] mail –u root (nombre_usuario)

Fig. 94 Enviar correo

6.9.5 CONFIGURACIÓN EN WINDOWS

Configurar el Outlook Express, dar clic en inicio y elegir la pestaña de correo electrónico (Outlook Express)

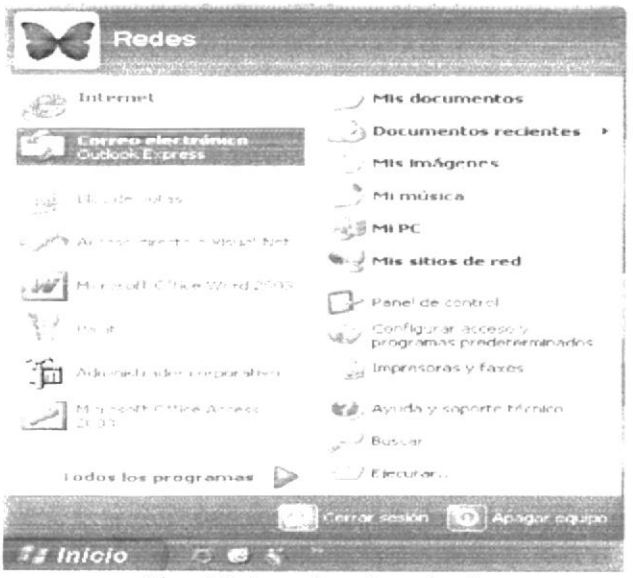

Fig. 95 Acceder al outlook

Se abrirá la pantalla principal del Outlook Express en la cual se va empezar la configuración, dar clic en herramientas y seleccionar cuentas de correos como se detalla a continuación:

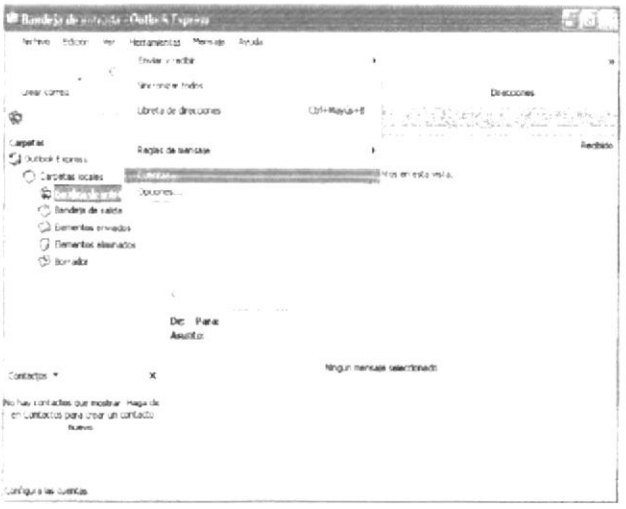

Fig. 96 Outlook Express

Aparecerá el asistente para poder configurar la nueva cuenta de correo electrónico, se da clic en agregar y elegir la opción correo.

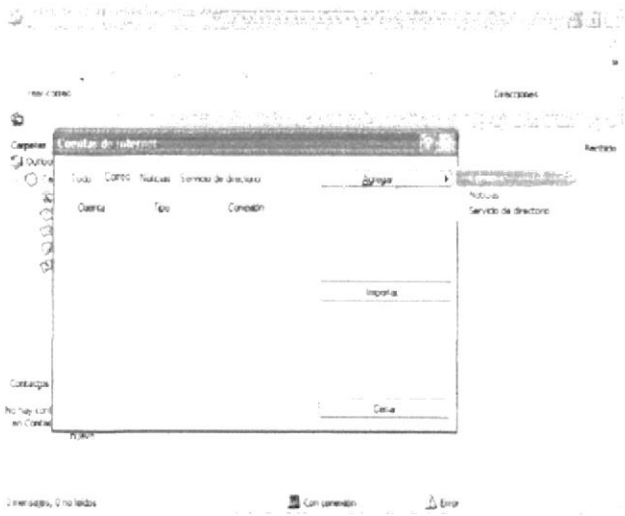

Fig. 97 Cuentas de Internet

Aparecerá la pantalla para configurar el nombre que aparecerá en el campo del mensaje saliente (nombre que el usuario desee)

Fig. 98 Conexiones a Internet

Configurar la dirección del correo (dirección que utilizan las demás personas para poder enviarle mensajes)

Fig. 99 Dirección de correo

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

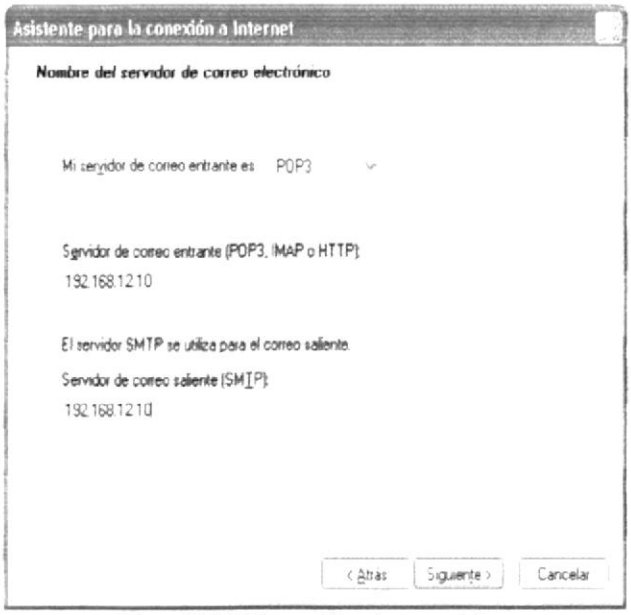

Fig. 100 Dirección de servidor

Configurar 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)

Fig. 101 Usuario y contraseña

Terminado los anteriores pasos saldrá la pantalla finalizar para concluir la configuración del nuestra cuenta de correo

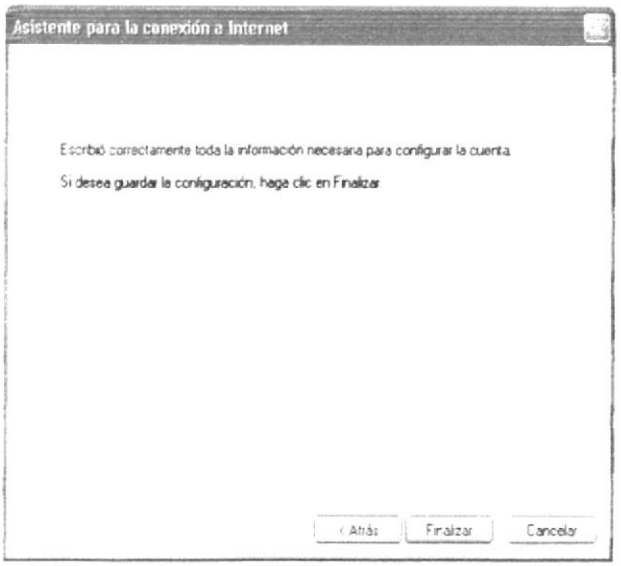

Fig. 102 Finalizar

Para verificar el envío y recepción de mensajes de correo en el Outlook Express presionar la pestaña enviar y recibir mensajes en la barra de herramientas y saldrá una pantalla como se detalla a continuación:

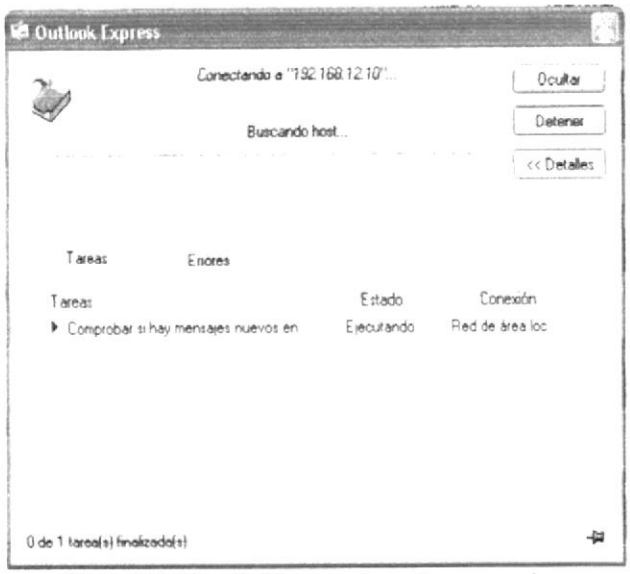

Fig. 105 Envio/Recepcion de mensajes

De esta manera se verifica en el Outlook Express cuando envía un mensaje el root de nuestro servidor Linux

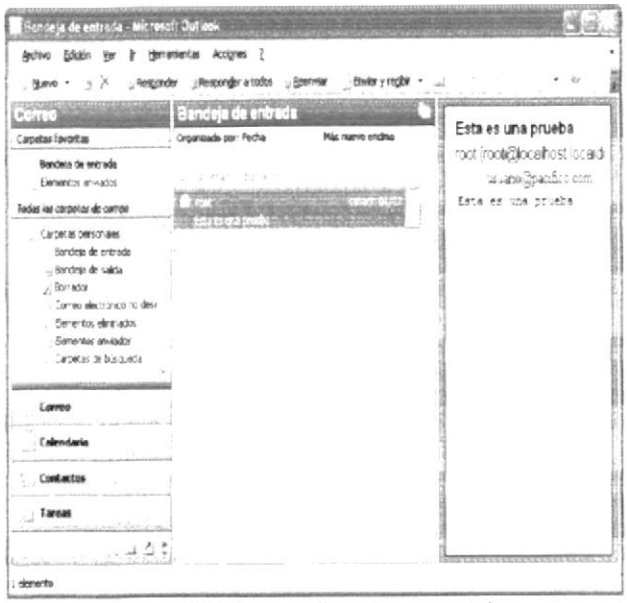

Fig. 106 Recepción de mensajes

Terminada la configuración se visualizará 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

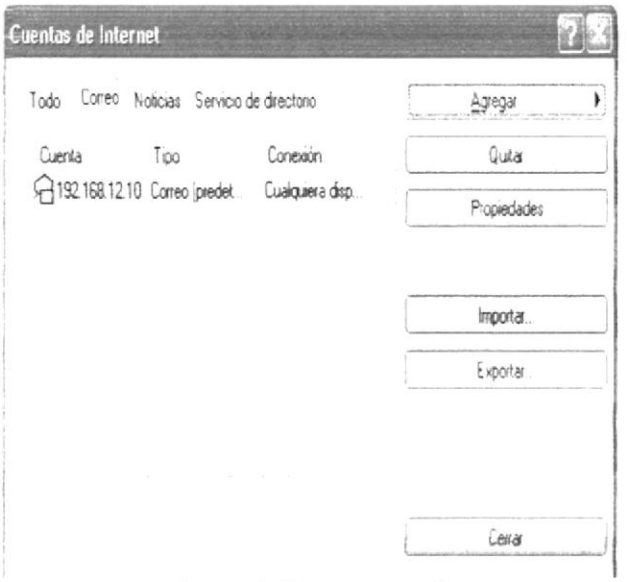

Fig. 103 Cuenta creada

Terminada la configuración se podrá enviar y recibir mensajes de correos de los usuarios creados en el servidor Linux.

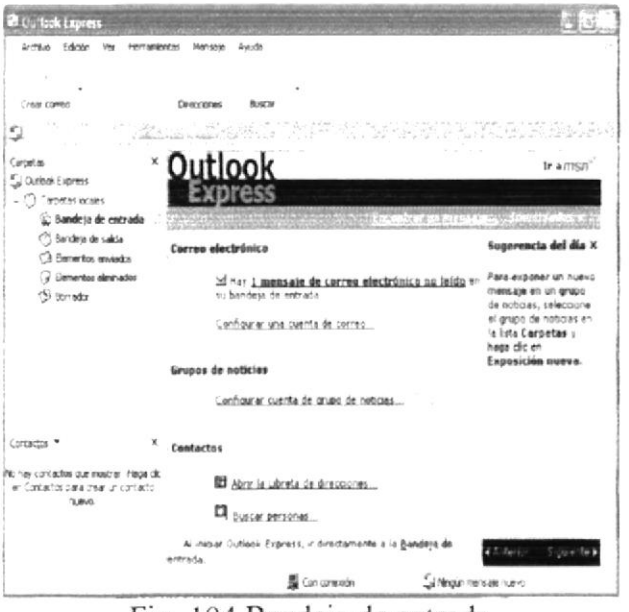

Fig. 104 Bandeja de entrada

6.10 DHCP

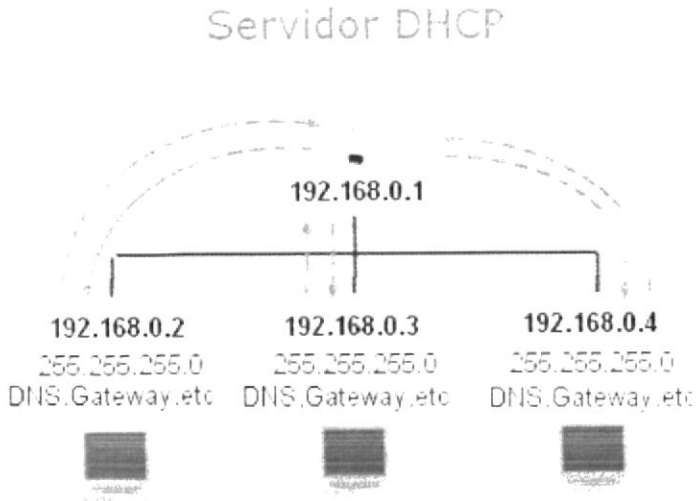

Fig. 107 Servidor DHCP

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

6.10.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Tener deshabilitado los firewall (cortafuegos), esto se verifica digitando el comando setup, se elige la opción configuración de firewall y se podrá verificar el estado.

6.10.2 CONFIGURACIÓN

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

[root@localhost /] rpm -q dhcp

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

[root@localhost /] cp /usr/share/doc/dhcp-3.01/dhcpd.conf.sample /etc/dhcpd.conf

Configurar el archivo dhcpd.conf el cual ha sido creado en la ruta /etc/dhcpd.conf (realizar las siguientes modificaciones)

[root@localhost /] vi /etc/dhcpd.conf

Fig. 108 Fichero dhcp

Subnet 192.168.11.0 netmask 255.255.255.0
En esta línea se asigna el segmento de red con su respectiva máscara.

Option routers 192.168.11.8
Opcional colocar la línea del gateway

Option subset-mask 255.255.255.0
Máscara de subred

Option nis-domain "pacifico.com" ;
Nombre del dominio

Option domain-name "pacifico.com" ;

Option domain-name-servers 192.168.12.10
Digitar la dirección del DNS

option netbios –name – servers 192.168.12.10;

Range dynamic-bootp 192.168.11.66 192.168.11.80
Definir el rango de IP desde - hasta

Salir con esc: wq para guardar los cambios.

En este caso, el servidor DHCP otorgaría una dirección IP al cliente en el rango 192.168.11.66 - 192.168.11.80, y concedería la dirección. Además configurará el cliente para que use la máscara de red 255.255.255.0, la dirección de difusión 192.168.12.10, el gateway 192.168.11.8, y el nombre de dominio pacifico.com

Crear un archivo en la ruta que se dará a continuación, en este archivo se almacenarán las direcciones ip de las máquinas que estén en el servicio DHCP

[root@localhost /] touch /var/lib/dhcp/dhcpd.leases

Para añadir dhcp al arranque del sistema, ejecute:

[root@localhost /] chkconfig dhcpd on

[root@localhost /] pgrep dhcp

Restaurar el servicio del dhcpd

Fig. 109 Restaurar servicios

EN CASO DE ERRORES AL RESTAURAR LOS SERVICIOS DHCPD

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mencionados,
- Verificar en los servicios del sistema si esta instalado el paquete dhcpd

6.10.3 CONFIGURACIÓN EN WINDOWS

Acceder a mis sitios de red, el icono esta en el escritorio pero en caso de no estar, la mas usual es: clic derecho en inicio, elegir explorar y aparecerá la pantalla en la cual esta mis sitio de red, se da clic derecho y elegir propiedades.

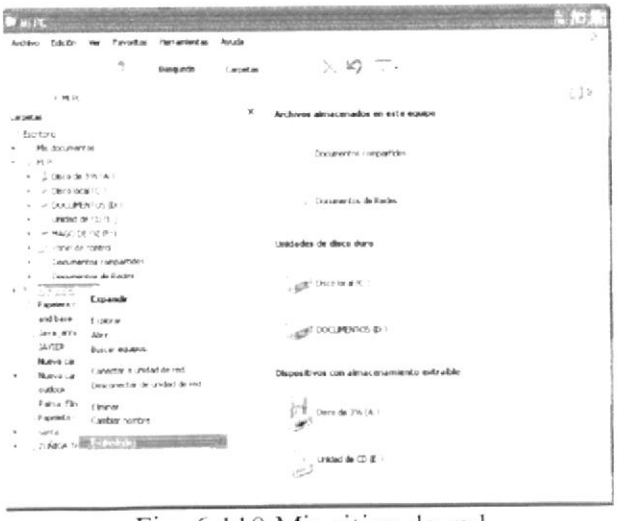

Fig. 6.110 Mis sitios de red

Se observará la pantalla de conexiones de red, se da clic derecho al icono de conexiones de área local y se elige propiedades

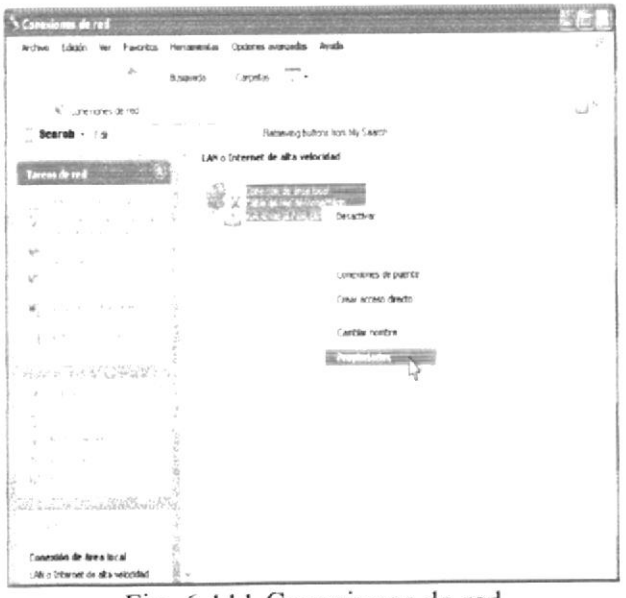

Fig. 6.111 Conexiones de red

Aparecerá la pantalla de propiedades de conexión de área local, se le dará doble clic en protocolo Internet (TCP/IP) o se sombrea y se elige la pestaña de propiedades.

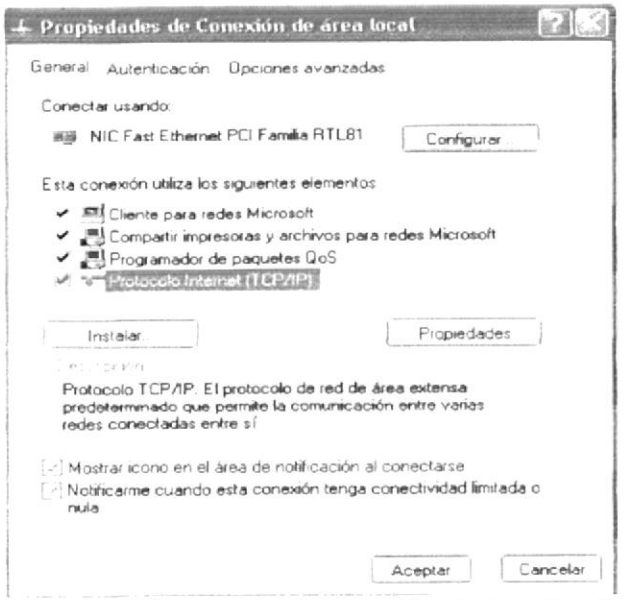

Fig. 6.112 Protocolo de conexión de área local

Configurar la tarjeta de red de manera dinámica, en este caso poner las opciones obtener una dirección IP automáticamente y obtener la dirección del servidor DNS automáticamente como se detalla a continuación:

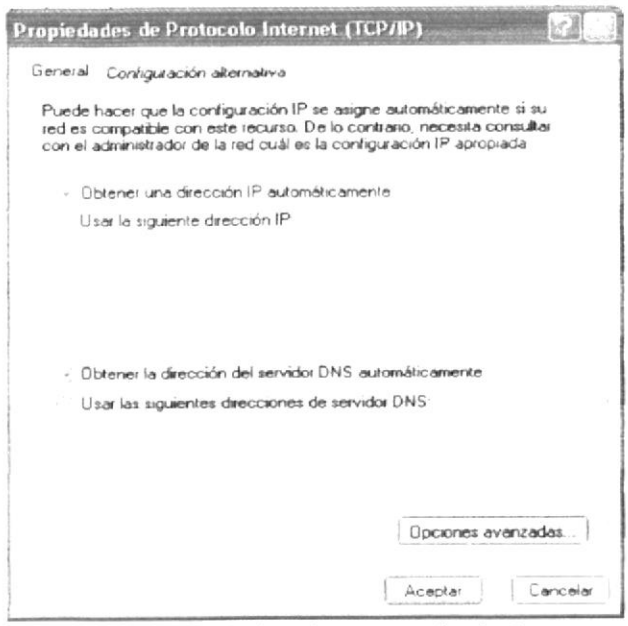

Fig. 6.113 Propiedades de protocolo de Internet

Verificar en Windows que la conexión sea dada por el servidor DHCP, dar doble clic en conexiones de área local en la barra inicio

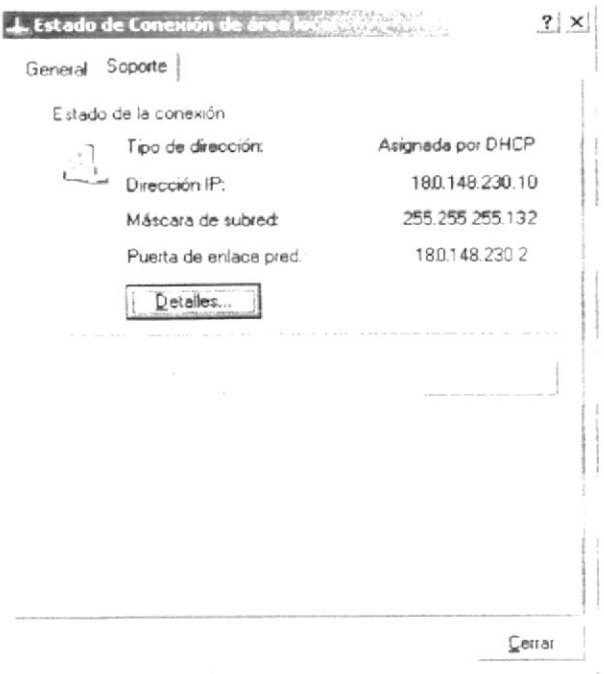

Fig. 114 Dirección IP asignada DHCP

6.11 FIREWALL

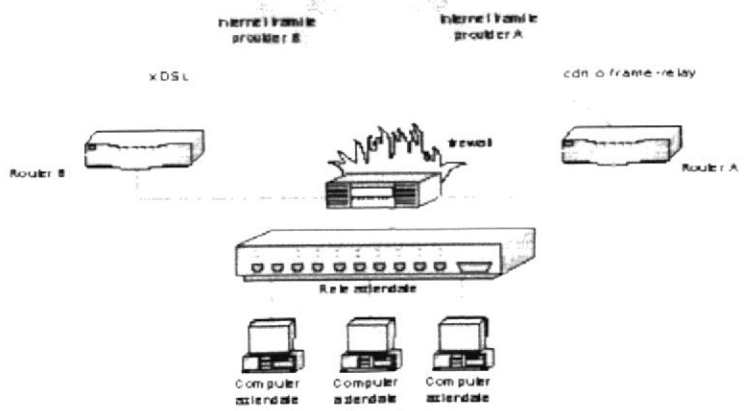

Fig. 115 Firewall

El firewall puede ser un dispositivo fisico o un software sobre un sistema operativo. Es un hardware especifico 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

En definitiva lo que se hace es:

Habilita el acceso a puertos de administración a determinadas IP's privilegiadas En máscara el tráfico de la red local hacia el exterior (NAT, una petición de un pc de la LAN sale al exterior con la ip pública), para poder salir a Internet
Deniega el acceso desde el exterior a puertos de administración y a todo lo que este entre 1 y 1024.

Hay dos maneras de implementar un firewall:

Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.
Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

¿Que es un IPtable?:

IPtables es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que inicia o que se pueda caer por un error de programación (esto es una pequeña mentira, ha tenido alguna vulnerabilidad que permite DOS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): iptables esta integrado con el kernel, es parte del sistema operativo.

¿Cómo se pone en marcha?
Realmente lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añade, borra, o crea reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.

6.11.1 DIAGRAMA IPTABLE

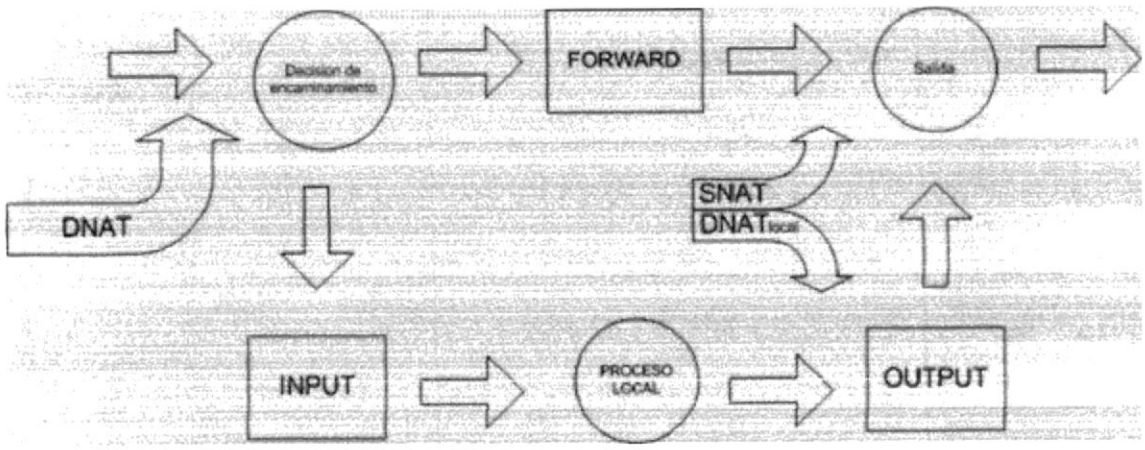

Fig. 116 Diagrama IPTABLE

6.11.2 ORDENES BÁSICOS

Iptables -F : Borrado de reglas

Iptables -L : Listado de reglas que se están aplicando

Iptables -A : Append, añadir regla

Iptables -D : Borrar una regla

6.11.3 CONFIGURACIÓN

Bloqueo TELNET

Iptables –A INPUT –s 0.0.0.0/24 –d 192.168.12.x/32 –p tcp --dport 23 –j DROP
Esta linea se utiliza para el bloqueo del telnet

Fig. 117 Bloqueo telnet

Bloqueo PING

Iptables –A INPUT –s 192.168.12.x –d 192.168.12.x –p icmp –j DROP
Esta linea se utiliza para el bloqueo del ping

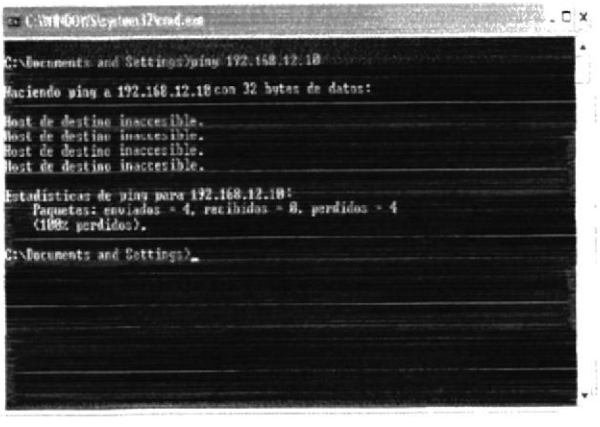

Fig. 118 Bloqueo ping