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 MICROCOMPUTADORES
PROGRAMADOR DE SISTEMAS

TEMA

ADMINISTRACIÓN Y SEGURIDADES DE REDES ESPOLTEL S. A.

MANUAL DE USUARIO Y CONFIGURACIONES

AUTORES
JOHANNA HUACHISACA VERA
ERICK FUENTES PINCAY
IVAN PACHECO GUERRERO

DIRECTOR
ANL. FABIAN BARBOZA

AÑO
2006

AGRADECIMIENTO

Agradecemos a todas las personas que han contribuido con sus conocimientos y experiencia para que haya sido posible cumplir con este trabajo de manera optima. Pues, cada uno de sus aportes ha representado un avance y apoyo a nuestro esfuerzo. Constituyendo un apoyo académico para las futuras generaciones en la carrera.

Principalmente a Dios, porque nos lleno de esperanza y fortaleza para alcanzar nuestro objetivo y meta.

DEDICATORIA

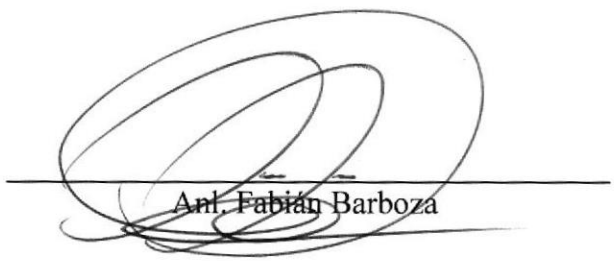
Este trabajo se lo dedicamos de manera especial, a nuestros padres, hermanos, hijos y amigos que de una u otra manera nos han apoyado y sirvieron de estímulo para siempre seguir adelante, ya que sin su ayuda no hubiera sido posible culminar la carrera.

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, a EDCOM ***(Escuela de Diseño y Comunicación Visual)*** de la Escuela Superior Politécnica del Litoral.

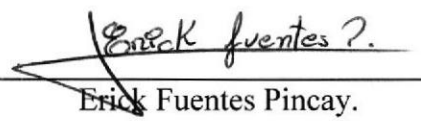
(Reglamento de exámenes y títulos profesionales de la ESPOL).

FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN



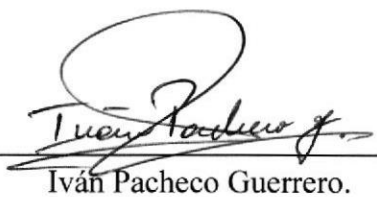
Anl. Fabián Barboza

FIRMA DE LOS AUTORES DEL TÓPICO DE GRADUACIÓN



Erick Fuentes Pincay.

Johanna Huachisaca Vera.



Iván Pacheco Guerrero.

TABLA DE CONTENIDO

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 6

TABLA DE FIGURAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 6

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 5

CAPÍTULO 1

GENERALIDADES

1. GENERALIDADES

1.1 INTRODUCCIÓN

Este manual fue elaborado con la finalidad de ayudar con una guía de consulta a los usuarios de redes y personal en general de la empresa, ya que contiene información de como manipular una red Lan y Wan.

1.2 OBJETIVOS DEL MANUAL

Guiar al personal en general y principalmente al de redes en lo que respecta a la administración de redes Lan y Wan, tanto en seguridades como en configuraciones de dispositivos de ruteo, conmutación y almacenamiento, por lo que se podrá despejar alguna inquietud.

1.3 ¿A QUIÉN VA DIRIGIDO ÉSTE MANUAL?

El manual está dirigido a todo el personal técnico y personas relacionadas con el manejo de las redes Lan y Wan de la empresa. Por tal razón, se especifican formas prácticas de como manipular los dispositivos de ruteo, conmutación y almacenamiento, además consta de instrucciones básicas para la resolución de inconvenientes físicos de las redes.

1.4 ¿POR QUÉ ÉSTE MANUAL?

Debido a los diferentes inconvenientes que suelen presentarse en la empresa y el tiempo que demoran en ubicar el mismo por la falta de información, se desarrolla este manual con una descripción detallada en configuraciones de dispositivos de enrutamiento, conmutación y almacenamiento. Éste manual se diseñó con la finalidad de otorgar recomendaciones útiles, en la estructura de la red Lan y Wan.

1.5 ORGANIZACIÓN DEL CONTENIDO DE ÉSTE MANUAL

El manual está dividido en 6 capítulos como se detalla a continuación:

- Capítulo 1. Generalidades
  Se detalla la introducción, objetivos, a quién se dirige, el por qué de este manual y su organización para que el usuario.

- Capítulo 2 . Situación Actual
  Presenta la situación actual de la empresa con la que se realizó el proyecto.

- Capítulo 3. Solución Propuesta
  Muestra una guía de las soluciones propuestas a los problemas que se encontraron en la empresa durante su estudio.

- Capítulo 4. Implementación
  En este capítulo se mostrarán gráficas de la estructura de la empresa tanto en la red Lan como en Wan.

- Capítulo 5. Configuraciones de Dispositivos.
  Se detalla como se debe realizar la manipulación de los dispositivos de ruteo y conmutación y sus configuraciones.

- Capítulo 6. Configuraciones de Linux Fedora Core 3
  El usuario podrá realizar configuraciones de servicio Samba, DNS, Web Server, Servidor de Correo, Proxy, Dhcp y Mrtg, así como también aplicar seguridades en Linux Fedora Core 3.

CAPÍTULO 2

SITUACIÓN ACTUAL

2. SITUACIÓN ACTUAL.

2.1 MISIÓN.

Buscar la perfección en el suministro de la comunicación de datos, a través del uso de la mejor tecnología disponible y la preparación continua de nuestros recursos humanos, en bien de la comunidad, clientes y empresas.

Promover convenios a largo plazo contribuyendo con el incremento de clientes y colaboradores, y al mismo tiempo al desarrollo de las telecomunicaciones y del país.

2.2 VISIÓN.

Ser reconocidos en el medio como la mejor compañía facilitadora del acceso a la información y conocimiento, líder en calidad de soluciones integrales en telecomunicaciones.

Asesorar y suministrar soluciones integrales en Telecomunicaciones e Internet; con un permanente mejoramiento de servicios, apoyados por un equipo humano especializado, íntegro y creativo, que hace posible la satisfacción de los clientes

2.3 ANTECEDENTES.

La ESPOL cuenta con amplia experiencia, tecnología e infraestructura de Servicios de Internet, estas ventajas tenían la necesidad de transmitirlas al mercado nacional y crean ESPOLTEL S.A., medio por el cual cubren estas expectativas. Aunque en la actualidad es una empresa independiente.

Su oficina matriz se encuentra ubicada en la ciudad de Guayaquil, en las calles Malecón #100 y Loja, específicamente en el Campus Las Peñas Bloque G Norte; además, consta con una sucursal operacional de telecomunicaciones en el Campus Prosperina.

ESPOLTEL S.A. cuenta con alrededor de 20 empleados distribuidos en sus diferentes áreas, sin contar con el personal que contratan esporádicamente para ciertos trabajos.

Su página web que es: www.espoltel.net

Figura 2.1 Oficinas de Espoltel S.A. Campus Peñas

Figura 2.2 Ubicación de Espoltel S.A. Campus Peñas

ESPOLTEL S.A., fue creada para el desarrollo y explotación de servicios de valor agregado, servicios finales y portadores de Telecomunicaciones, incluyendo tecnologías de manejo y administración de la información entre otros.

Está actualmente posicionada en el mercado como Proveedor de Servicios de Internet (ISP) gracias a su servicio personalizado.

Entre los servicios que Espoltel brinda a sus clientes tenemos los siguientes:

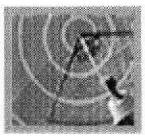
IMAGEN	SERVICIOS
	Conexiones dedicadas de Internet para empresas.
	Voz y Datos. Sistemas Telefónicos.
	Servicios de Videoconferencia y Multimedia.
	Diseño e implementación de redes digitales de transmisión de datos / Cableado Estructurado.
	Web Hosting Diseño de Páginas Web (websites).
	Telefonía sobre IP.

Tabla 2.1 Servicios de Espoltel S.A.

ESPOLTEL S.A. como objetivo principal tiene ampliar la cobertura en el mercado debido a la gran demanda de este, así aumentar el desarrollo y productividad de sus recursos a pesar de la situación económica del país y la competitividad entre otras organizaciones del medio ya que por el momento sus clientes son empresas grandes y medianas.

2.4 DESCRIPCIÓN DE LA RED WAN.

ESPOLTEL S.A. tiene implementada en su infraestructura principal enlace mediante fibra óptica monomodo de 8/125 micras con un ancho de banda de 2 mbps, la misma que es suministrada por proveedores como Telconet, Accessram y Transferdatos.

Tienen un nodo de concentración ubicado en el Edificio Plaza (9 de Octubre y García Moreno), el mismo que les sirve de enlace para Mapasingue lugar por el cual sale la señal para dar el servicio a sus clientes wireless. Esta señal tiene una velocidad de transmisión de 50 Kbps.

En Mapasingue, Cerro Azul y en el Edificio Finansur tienen BSU (Unidad de Estación Base) con el fin de formar celdas y cubrir esa área con su servicio WLL.

En cuanto a su infraestructura de respaldo esta se encuentra constituida por cuatro torres con antenas microondas tipo sectorial de 24 DBI que están legalizadas y con tecnología Spread Spectrum, ubicadas en:

- Campus Las Peñas, con una altura de 70 mts. y una frecuencia de 2.4 Ghrz.
- Campus Prosperina, con una altura de 45 mts. y una frecuencia de 2.4 Ghrz.
- Cerro Mapasingue con una altura de 45 mts. y una frecuencia de 3.5 Ghrz
- Salinas, con una altura de 30 mts. y una frecuencia de 2.4 Ghrz.

Figura 2.3 Torre del Campus Peñas Edificio Celex.

Para poder comunicarse mediante este medio de comunicación se ayudan de nodos contratados que se encuentran ubicados estratégicamente y entre los principales tenemos:

- Edificio Valco, Calles 9 de Octubre y Chile.
- Edificio Mi comisariato, calles Pedro Carbo y Roca.
- Cerro de Bellavista.

2.5 DIAGRAMA DE MEDIOS DE COMUNICACIÓN WAN

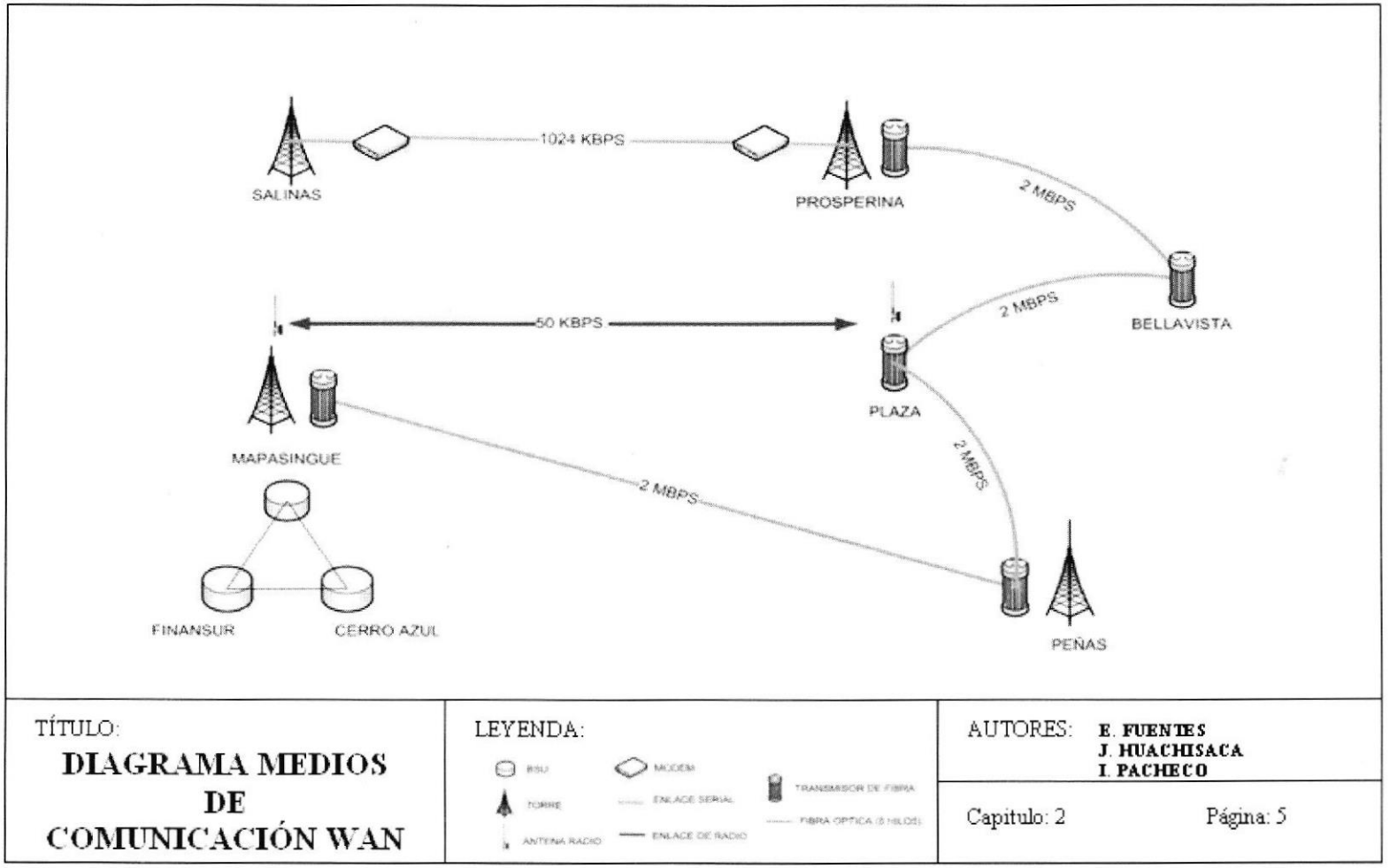


Figura 2.4 Diagrama de Medios de comunicación Wan.

2.6 DESCRIPCIÓN DE LOS MEDIOS DE COMUNICACIÓN WAN.

La línea principal de fibra es de tipo monomodo de 8/125 micras, se conecta desde el Océano Pacifico específicamente a 5 Km. de las costas de Punta Carnero – Salinas, desde este punto la señal llega a la Espol Prosperina (Guayaquil), por medio del servicio de Pacifictel cuya transmisión es de 1 Mbps (E1), mediante un módem.

Desde Prosperina hasta Las Peñas la señal es distribuida mediante fibra óptica monomodo de 8/125 micras por el carrier ubicado en el cerro de Bellavista y un nodo de concentración en el edificio Plaza, la velocidad entre cada punto es de 2 Mbps.

La conexión desde Peñas a Mapasingue también es fibra óptica monomodo de 8/125 micras con el mismo ancho de banda que las anteriores. Y de Mapasingue a Prosperina el enlace se realiza por radio hasta el Edificio Plaza y desde este hasta el punto de llegada se vuelve a conectar la fibra.0

Los nodos de concentración ubicados en el edificio Valco y de Mi Comisariato son propios de los proveedores que distribuyen el internet a la empresa y solo son usados como al momento de usar el enlace de respaldo.

Actualmente en Prosperina se forma un nodo de distribución de internet.

2.7 RESPALDO DE LA RED WAN

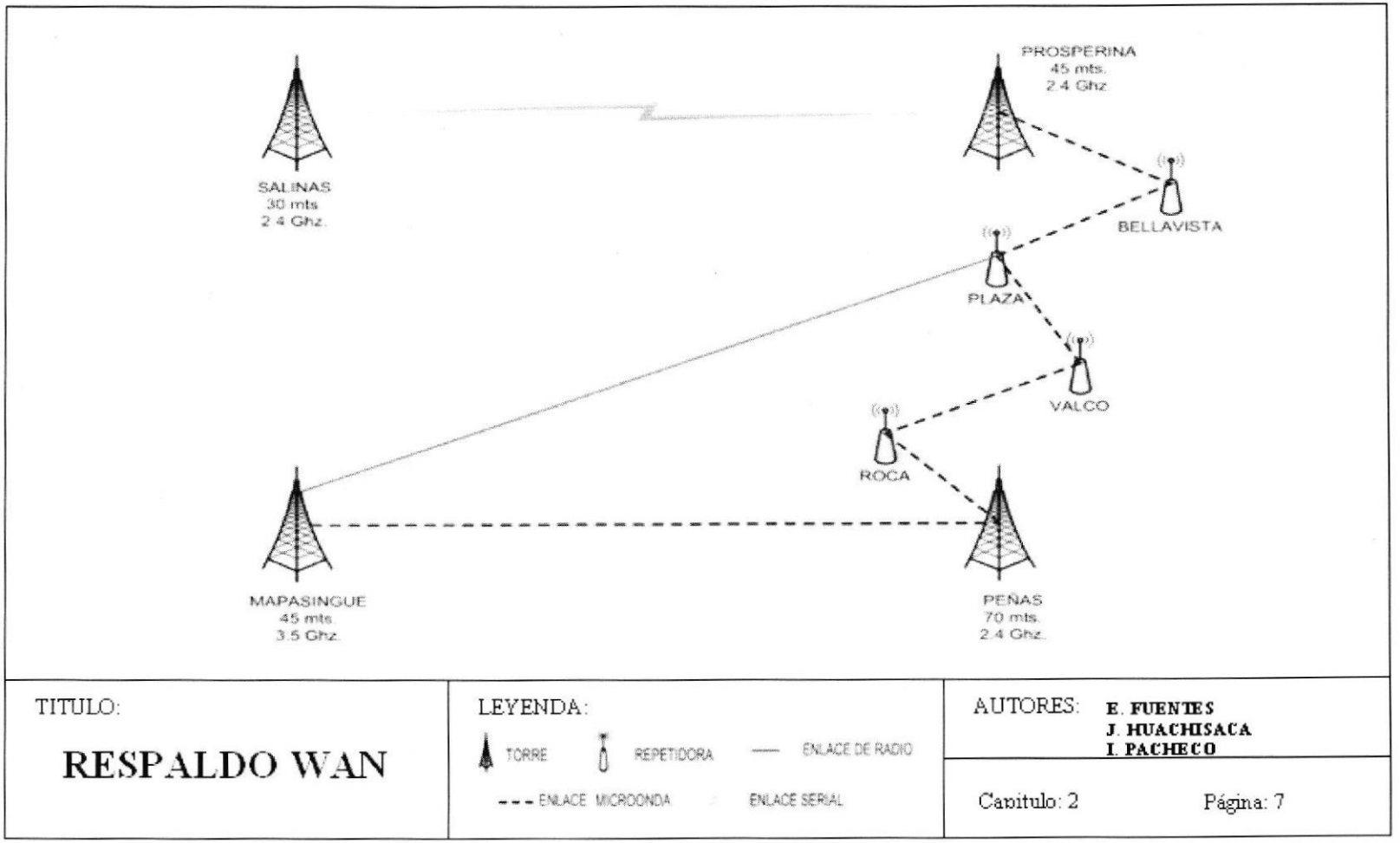


Figura 2.5 Diagrama de respaldo Wan.

2.8 DESCRIPCIÓN DE LOS EQUIPOS DE LA RED WAN.

Los equipos utilizados en la WAN con sus respectivas características, son los siguientes:

Router Cisco AS5850:

- Soporte completo del IOS para estándares H.232, SIP y MGCP.
- Ideal para arquitecturas distribuidas.
- Programables para servicios individualizados.
- Igual capacidad para cualquier CODEC sin ningún pre-aprovisionamiento.
- La escalabilidad permite tener hasta 3.360 usuarios concurrentes en un dispositivo de 14 unidades de rack.
- Hasta 3 Cisco As5850s por rack.
- Alto desempeño representado en la latencia de 5 milisegundos por paquete.
- Disponibilidad 99.999%. Soporte de ASAP.

Desde la torre del Campus Prosperina se forma un enlace vía microonda con la torre del Campus Peñas, cuya señal llega al cuarto de comunicaciones en la edificación de Espoltel, por medio de fibra a un transceiver de 10/100 Mbps, luego a un Patch Panel marca Unicom 110, el cual hace cascada con un Switch marca Dlink modelo Des 1024* y por último llegar al Servidor Proxy.

Además tiene un switch Cisco Catalyst 2950 y tres Routers, dos Cisco 2621 y uno Cisco 3600 cuyas características son:

Router Cisco 3600

- 2 Slots WAN.
- 1 Network Module Slot.
- 1 Advanced Integration Module (AIM) Slot.
- Opción de 1 ó 2 interfaces Ethernet o Fast Ethernet de fábrica.
- Opción de 1 interface Token Ring de fábrica.
- Módulos: 1 ó 4 puertos Ethernet, 4 u 8 puertos Seriales A/S, 1 ó 2 puertos de voz, ISDN BRI, ISDN PRI, 8 ó 16 módems análogos.

Router Cisco 2621

- 2 Wics de Ranuras de las tarjetas de interfaz Wan.
- 1 Ranura para modulo de red.
- 1 Ranura del modulo de integración avanzado.
- Corriente alterna (CA), de corriente continua (CC) o adaptador RPS en el sistema de alimentación interno.
- Rendimiento entre 15 y 25 Kbps.
- 115,2 Kbps con acceso telefónico activado, enrutamiento bajo demanda en puertos auxiliares y de consola.

Switch Cisco Catalyst 2950.

- Tecnología stack.
- Velocidad 10/100/1000 mbps.
- Tiene funciones básicas para voz, datos y video.
- Calidad de servicio avanzada (QoS), y la alta disponibilidad.

Switch Dlink Des 1024*.

- Velocidad 10/100/1000 mbps.
- No administrable.
- Capa 2 del modelo OSI.
- Tiene funciones básicas para voz, datos y video.

Espoltel cuenta con un cuarto de comunicaciones en el campus Prosperina tipo sucursal. Los equipos que se encuentran aquí no necesitan administrador.

2.9 DIAGRAMA DE DISPOSITIVOS WAN

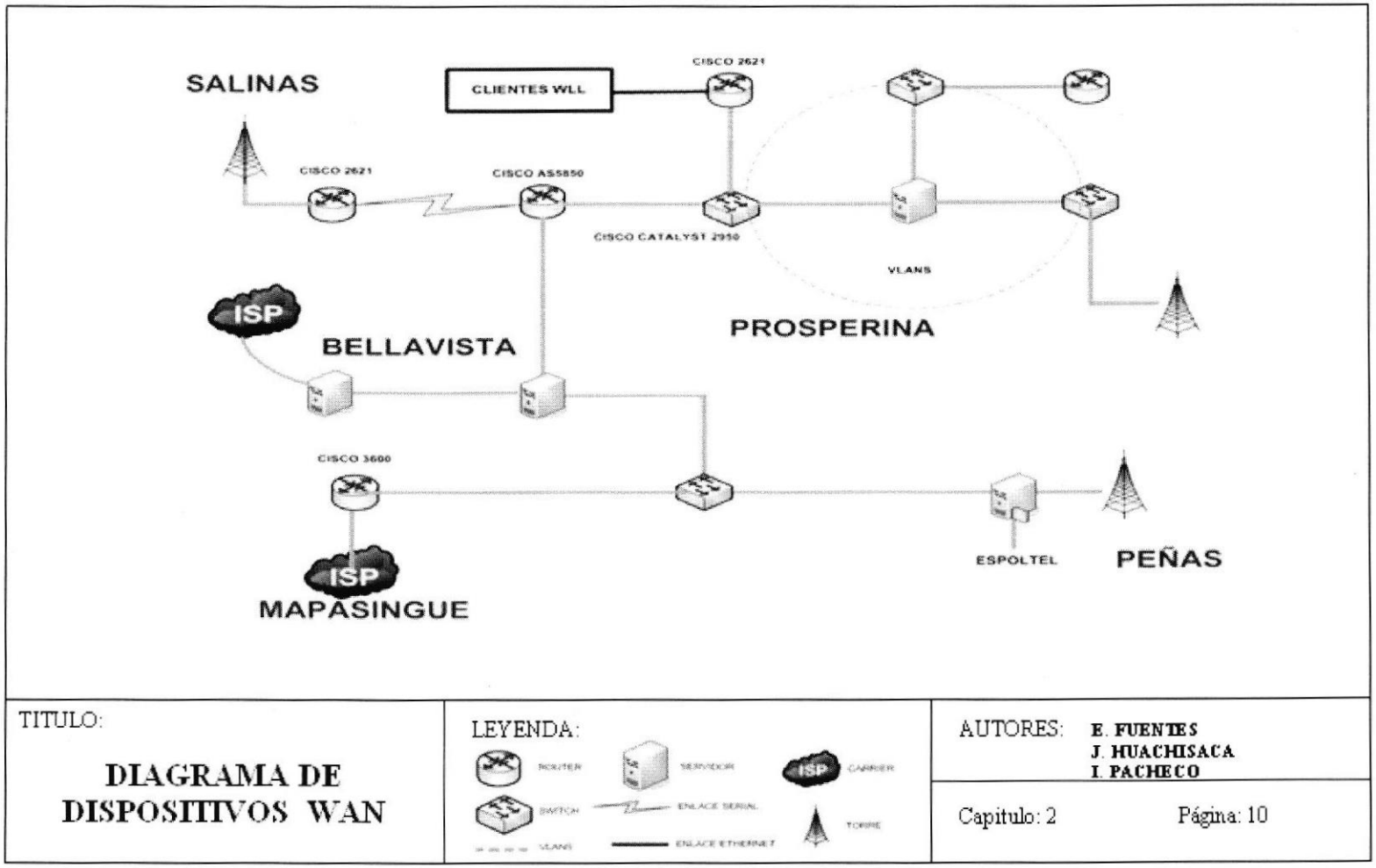


Figura 2.6 Diagrama de dispositivos Wan.

2.10 DESCRIPCIÓN DE LA RED LAN – CAMPUS PEÑAS.

Actualmente poseen los siguientes departamentos donde han distribuido 19 computadores según lo requerido en cada uno de ellos.

- Gerencial General
- Sala de Sesiones
- 1 Gerencia de Sistemas
- 1 Gerencia Comercial
- 1 Recepción
- 3 Finanzas
- 2 Caja
- 2 Ventas
- 1 Comunicaciones
- 8 Técnico o Monitoreo

La principal característica de estos computadores es su tarjeta de red pues son Marca Intel y de una velocidad 10/100 mbps. Además hay 3 impresoras distribuidas así:

- 1 Finanzas marca HP LaserJet 4
- 1 Caja marca Epson LX300
- 1 Recepción marca Canon 1000

Estos computadores son manejados con Sistema Operativo Windows XP.

2.11 DISTRIBUCIÓN DEL CABLEADO.

Figura 2.7 Instalaciones Eléctricas

En lo que respecta al backbone vertical, las instalaciones tanto eléctricas como de red que se encuentran en el tumbado de manera desordenada y en su minoría están protegidas por los tubos PVC. Mientras que el backbone horizontal siguen las normas de seguridades y los estándares correspondientes, debido a que sus instalaciones de red se encuentras recubiertas por unas canaletas y ángulos, la separación entre el punto de red y eléctrico es de 10 cm., los puntos de red se encuentra protegidos por face plate y a 50 centímetros del piso.

La construcción de la red esta hecha a base de cable UTP categoría 5E las de datos y las de voz con cable de categoría 3.

Para su red LAN no tienen definido un ancho de banda ya que se suministran según sus necesidades.

2.12 DIAGRAMA DE LA RED LAN

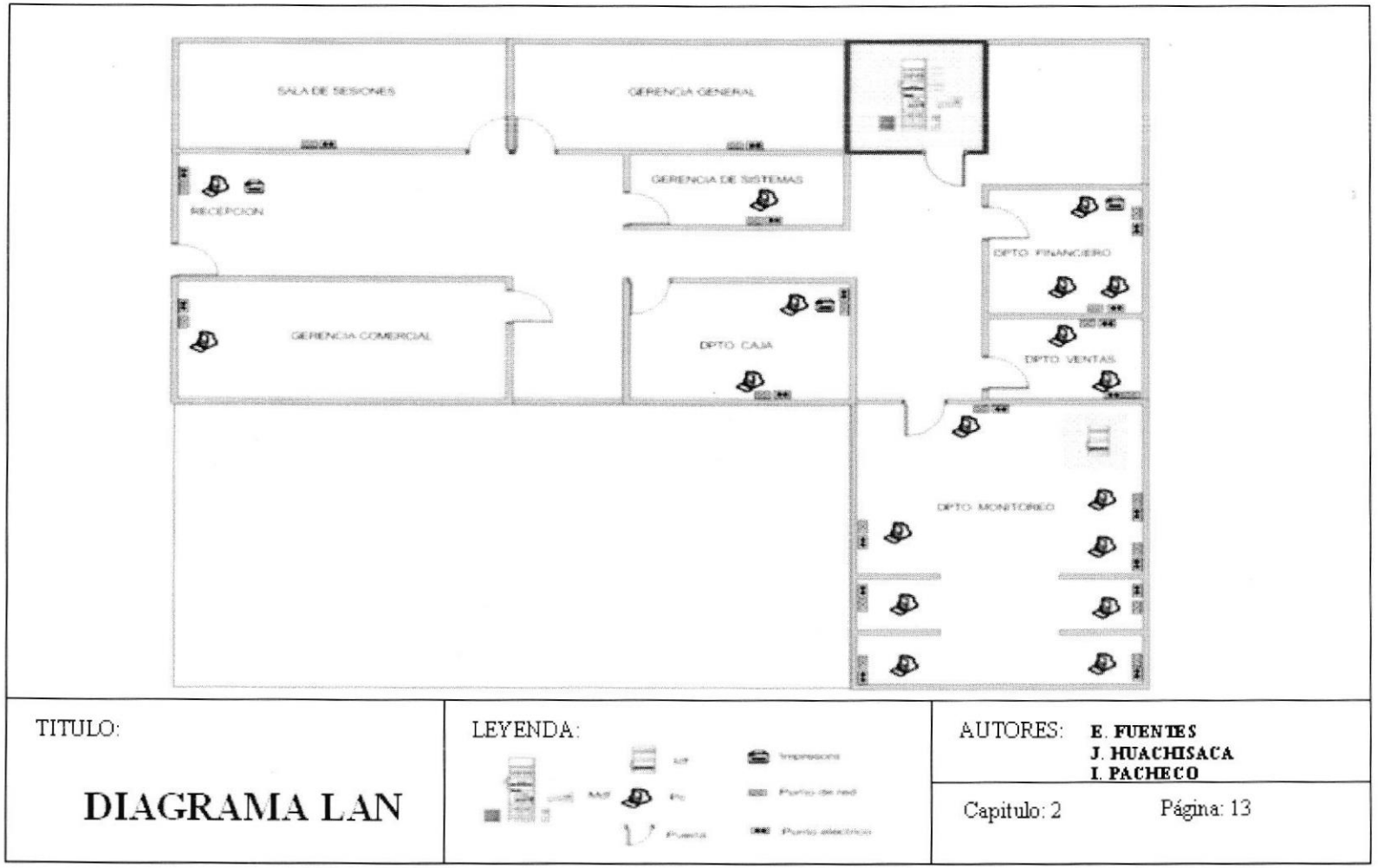


Figura 2.8 Diagrama de la red Lan

2.13 DEPARTAMENTO DE COMUNICACIONES – PEÑAS (MDF).

En este departamento encontramos los siguientes equipos:

- 1 Rack de servidores.

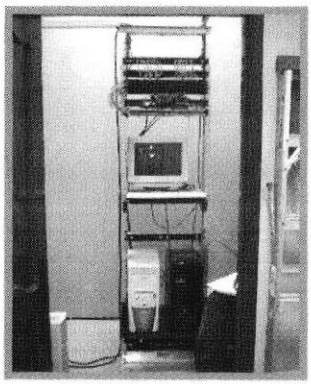


Figura 2.9 Rack de Servidores

- 1 Switch Capa 2 no admistrable marca Dlink modelo Des 1024*, con velocidad 10/100 mbps de 24 puertos para la red Lan.

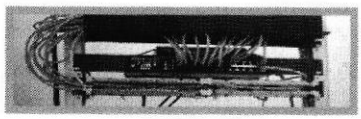


Figura 2.10 Switch Dlink Des 1024*

- 1 Switch VGA marca Dlink de 4 puertos que administra los servidores.

Figura 2.11 Switch Dlink VGA

- 1 Transceiver de 10/100 mbps en velocidad.

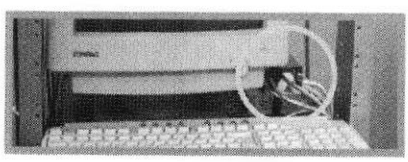


Figura 2.12 Transceiver

- 3 Patch Panel, uno de voz marca Dlink ,y 2 de datos, de los cuales uno es de marca Unicom 110 de 16 puertos y otro es marca Newlink de 12 puertos.

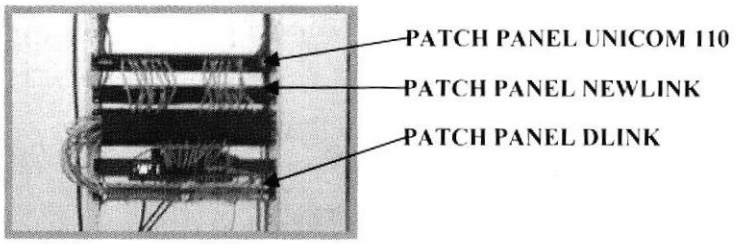


Figura 2.13 Patchs Panels

- 1 UPS marca SALICRU ELECTRONIC con duración de 12 a 24 horas el mismo que funciona con batería.

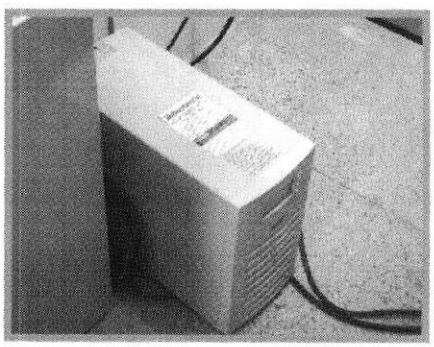


Figura 2.14 UPS Salicru Electronic

- 1 Cargador con 6 Baterías.

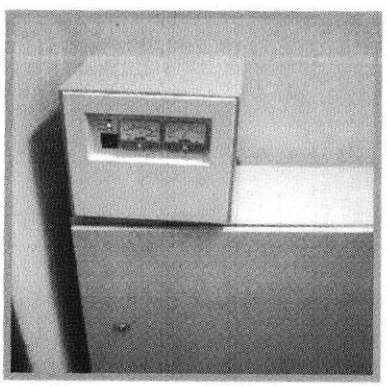


Figura 2.15 Cargador de Baterías

- 1 Central Telefónica (POP) marca Panasonic, modelo 4CO.

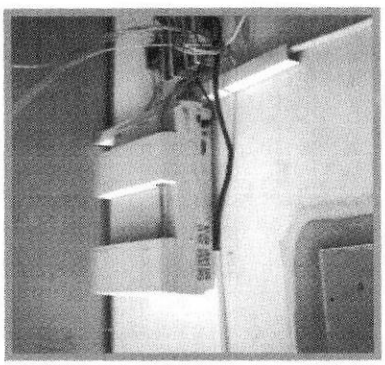


Figura 2.16 Pop Panasonic 4CO

- 1 Panel de breakers.
- 1 Servidor de Aplicaciones donde manejan base de datos con características tales como:
  - Intel Pentium 4.
  - Procesador de 3.0 Ghz.
  - Memoria RAM 512 Mb.
  - Disco Duro de 120 Gb.
  - Tarjeta de Red marca Intel de velocidad 10/100 Mbps.
  - Mainboard Intel.
- 1 Servidor Proxy de internet con características:
  - Intel Pentium 4.
  - Procesador de 3.0 Ghz.
  - Memoria RAM 512 Mb.
  - Disco Duro de 40 Gb.
  - 3 Tarjetas de Red marca Intel de velocidad 10/100 Mbps.
  - Mainboard Intel.

Ambos equipos son clones y trabajan bajo sistema operativo Linux Fedora Core 3.

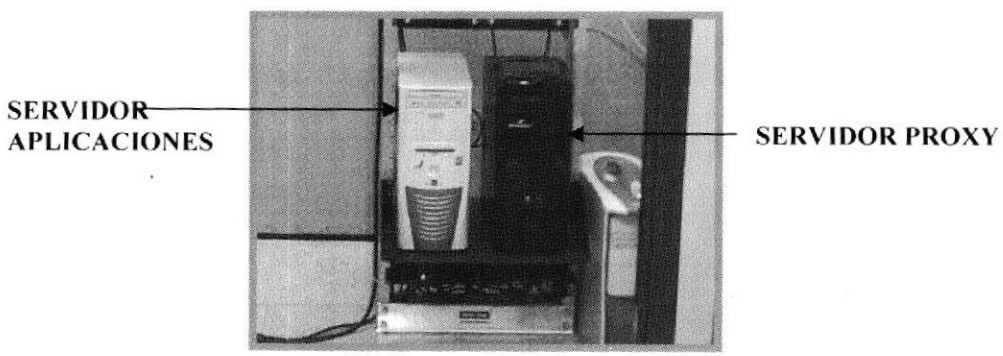


Figura 2.17 Servidores

2.14 DIAGRAMA DEL CUARTO DE COMUNICACIONES – CAMPUS PEÑAS

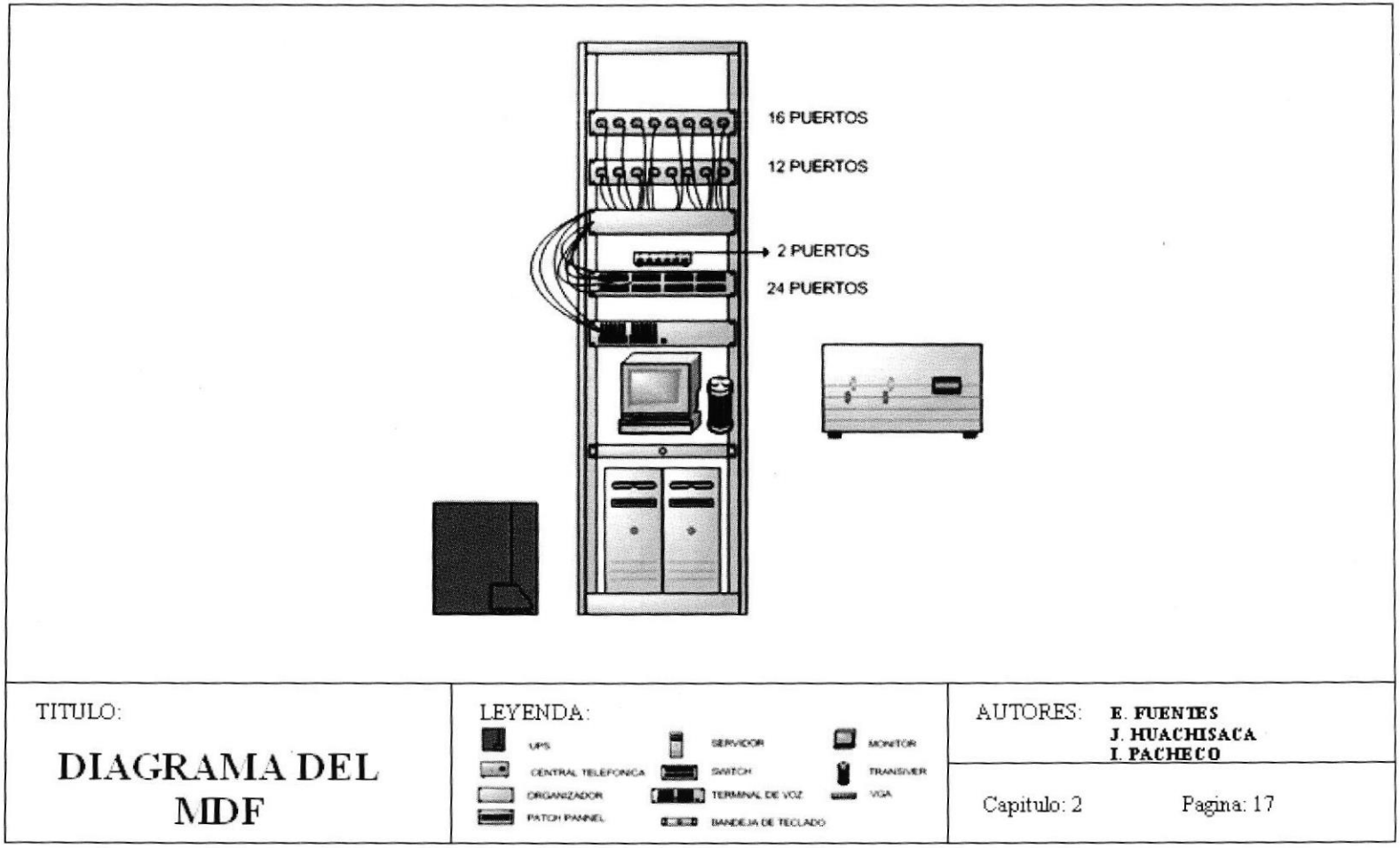


Figura 2.18 Diagrama de MDF - Peñas

2.15 DEPARTAMENTO TÉCNICO O DE MONITOREO (IDF).

Los equipos que se encuentran son:

- 1 Rack de pared abierto.
- 1 Switch no administrable de capa 2, de velocidad 10/100 mbps. marca DLINK. modelo DES -1024R* de 24 puertos.
- 1 Patch Panel Marca Smart Link de 24 puertos.
- 8 PC.

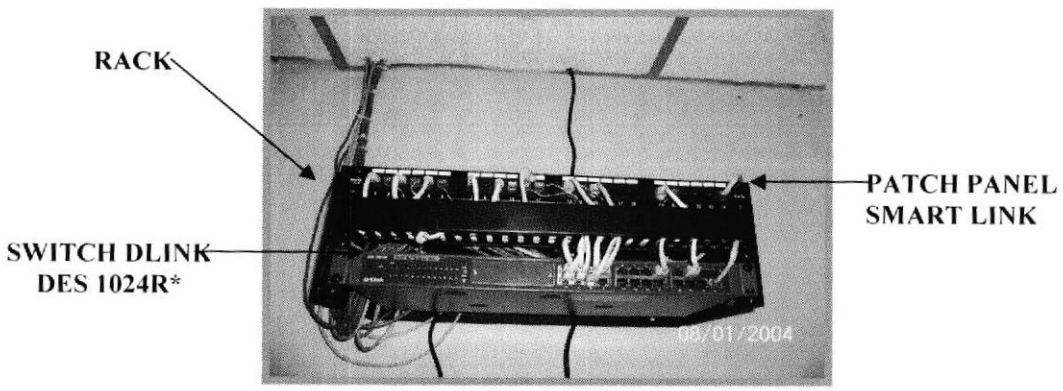


Figura 2.19 Rack de Pared y sus componentes.

CAPÍTULO 3

SOLUCIÓN PROPUESTA

3. SOLUCIÓN PROPUESTA.

3.1 TABLA: PROBLEMA, CAUSA, EFECTO.

PROBLEMA	CAUSA	EFECTO
No cumplen con normas y estándares de cableado estructurado interno (Peñas).	↓ No existe electro canaletas en el backbone vertical de la red Lan. ↓ No existe etiquetación de la red Lan. ↓ Espacio reducido en cuarto de comunicaciones.	↓ Mala distribución en el cableado del backbone vertical. ↓ Retraso al solucionar un problema en la comunicación interna. ↓ Difícil acceso a los dispositivos de comunicación en el MDF.
Dispositivos de ruteo, conmutación y almacenamiento, con bajo rendimiento.	No se ha invertido en infraestructura Wan.	Saturación de servidores clones por ejercer múltiples funciones.

Tabla 3.1 Problema, Causa, Efecto

3.2 TABLA: PROBLEMA, SOLUCIÓN, ALCANCE.

PROBLEMA	SOLUCIÓN	ALCANCE
No cumplen con normas y estándares de cableado estructurado interno (Peñas).	↓ Organizar el cableado del backbone vertical, usando electro - canaletas. ↓ Rotular tomas y etiquetar dispositivos. ↓ Reorganizar el cuarto de comunicaciones o adecuarlo en un área más amplia.	↓ Eliminar interferencias. ↓ Rápida solución a los problemas de comunicación. ↓ Facilidad al administrar dispositivos.
Dispositivos de ruteo, conmutación y almacenamiento, con bajo rendimiento.	Adquirir dispositivos con la tecnología necesaria para fortalecer los servicios que prestan.	Mejorar el rendimiento en servidores, dispositivos de ruteo y conmutación.

Tabla 3.2 Problema, Solución, Alcance

3.3 ESTUDIO DE FACTIBILIDAD.

Con el fin de contribuir con mejoras para y hacia la empresa se desarrollaron dos soluciones en base a los problemas encontrados, las mismas que se detallan a continuación.

3.3.1 ALTERNATIVA I.

Esta alternativa abarca mejoras en cableado, dispositivos de ruteo, conmutación y almacenamiento, para fortalecer la infraestructura Lan y Wan de Espoltel S. A.

3.3.1.1 OBJETIVO.

Fortalecer la infraestructura Wan y Lan invirtiendo en la compra de los dispositivos necesarios para alcanzar lo planteado.

3.3.1.2 FACTIBILIDAD TÉCNICA.

3.3.1.2.1 DISPOSITIVOS DE RUTEO, CONMUTACIÓN Y ALMACENAMIENTO.

CANTIDAD	EQUIPO	CARACTERÍSTICAS	UBICACIÓN
1	**Rack Server**	Procesador Intel® 3.00GHz/1MB Memoria estándar 1 GB Expandible hasta 12 GB 1 UR PCI-X Gigabit NIC (NC7782)	Cuarto de comunicaciones (Peñas)
2	**Router**	2 Puertos Fast Ethernet 10/100. 2 Puertos Gigabit Ethernet. Fuentes Redundantes.	Red Wan (Peñas, Prosperina)
1	**Router**	Interfaz 100BASETX 3 WIC Fast Ethernet Interfaz serial. Controladores Input Output Fast Ethernet	Red Wan (Mapasingue)
1	**Switch**	48 puertos 10/100. 2 Puertos 10/100/1000. Funciones básicas para voz, datos y video. Migración Gigabit.	Red Wan (Peñas)

Tabla 3.3 Dispositivos de ruteo, conmutación y almacenamiento de la Alternativa I

3.3.1.2.2 MATERIALES DE CABLEADO ESTRUCTURADO.

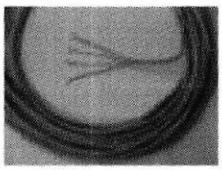
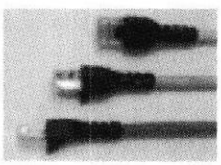
CANTIDAD	DESCRIPCIÓN	CARACTERÍSTICAS	UBICACIÓN
12	**Electro canaleta** 	Tamaño: tres metros Conexión a tierra	Red Lan (Peñas)
1	**Bobina cable UTP** 	Categoría 5e	Red Lan (Peñas)
40	**Conectores** 	RJ-45	Red Lan (Peñas)
20	**Patch Cord** 	Tamaño: 50 cm. 350 Mhrz marca: cp Technologies	Cuarto de comunicaciones (Peñas)

Tabla 3.4 Materiales de cableado estructurado de la Alternativa I

3.3.1.3 FACTIBILIDAD ECONÓMICA.

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
1	Rack server	2,350.88	2,350.88
1	Router	5,200.00	5,200.00
2	Router	4,615.00	9,230.00
1	Switch	1,520.40	1,520.40
8	Electro canaleta	50.00	400.00
1	Bobina cable UTP Cat 5e	48.00	48.00
40	Conectores RJ-45	0.45	18.00
20	Patch Cord 350 Mhrz	3.00	60.00
			$ 18,827.28

Tabla 3.5 Factibilidad Económica de la Alternativa I.

3.3.1.4 FACTIBILIDAD OPERATIVA.

CANTIDAD	ACTIVIDAD	SEMANAS	COSTO SEMANA	TOTAL
1	**Fase Análisis de la red Lan y Wan** Ingeniero en Telecomunicaciones	2	$ 150	$ 300.00
1	**Fase Diseño de la red Lan y Wan** Ingeniero en Telecomunicaciones	1	$ 150	$ 150.00
2 2	**Fase Implementación de la red Lan y Wan.** Ingeniero en Telecomunicaciones Técnico en redes	4	$ 150 $ 80	$ 1200.00 $ 640.00
1	**Fase Documentación de la Red Lan y Wan** Ingeniero en Telecomunicaciones	2	$ 150	$ 300.00
2 2	**Fase Prueba** Ingeniero en Telecomunicaciones Técnicos en redes.	4	$ 150 $ 80	$ 1200.00 $ 640.00
				$ 2,590.00

Tabla 3.6 Factibilidad Operativa de la Alternativa I.

Nota: Conforme avance la fase de implementación Wan y Lan, avanzará la Fase de prueba es por eso que el valor de la Fase de prueba no influye en el valor total de los costos operativos.

3.3.1.5 COSTOS DE INVERSIÓN.

Hardware	:	$	18,827.88
Operativos	:	$	2,590.00
Imprevistos (25%)	:	$	5,354.47
Total	**:**	**$**	**26,772.35**

Todos los precios incluyen iva.

3.3.1.6 VENTAJAS.

Cableado estructurado organizado y con acceso rápido a solucionar inconvenientes de la red Lan de Peñas.

3.3.1.7 BENEFICIOS.

Al ser dispositivos nuevos y con tecnología actual pueden abarcar futuras proyecciones de crecimiento de la empresa.

Establecer una mejor distribución del cableado estructurado del la red Lan cumpliendo con la norma EIA/TIA-568A y estándar IEEE 802.3 con el fin de obtener una certificación ISO.

Fortalecer los servicios que brindan a sus clientes debido a la actualización de tecnología en dispositivos de ruteo y conmutación.

3.3.1.8 TASA INTERNA DE RETORNO.

A continuación se muestra en detalle el tiempo en que la inversión será recuperada. Para esto se tomará en cuenta los costos que el trabajo va a tener en el tiempo incluyendo el valor total del mismo y los beneficios económicos año a año.

Datos generales:

- Se proyecta un aumento del 30% en el rubro de sueldos para el año 2006.
- El porcentaje de inflación es del 16,8% anual.
- Actualmente tienen una tasa de crecimiento anual del 11% en sus ingresos.
- Con los nuevos cambios se prevé el incremento de los ingresos en un 25%.

SITUACIÓN ACTUAL – INGRESOS			
No CLIENTES	**RUBRO**	**MENSUAL**	**ANUAL**
15	Corporativo	16,000.00	192,000.00
8	Enlace	13,500.00	162,500.00
1173	Dial Up	40,500.00	486,000.00
TOTAL INGRESOS			**$ 840,000.00**

Tabla 3.7 Ingresos actuales de Espoltel S.A.

SITUACIÓN ACTUAL – EGRESOS	
RUBRO	**ANUAL**
Sueldos	109,200.00
Suministros	2,400.00
Transporte	1,800.00
Servicios Básicos	19,200.00
TOTAL	**$ 132,600.00**

Tabla 3.8 Egresos actuales de Espoltel S.A.

SITUACIÓN ACTUAL		
Ingresos	$	840,000.00
Egresos	$	132,600.00
TOTAL	**$**	**707,400.00**

Tabla 3.9 Total de ganancias actuales de Espoltel S.A.

3.3.1.8.1 TASA DE CRECIMIENTO.

EGRESOS			
RUBRO	**ANUAL**	**PORCENTAJE**	**TOTAL**
Gasto de personal	$ 109,200.00	+ 30 %	$ 141,960.00
Costo de Vida	$ 23,400.00	+ 16,80 %	$ 27,331.20
TOTAL COSTOS AL AÑO 1			$ 169,291.20

Tabla 3.10 Egresos en el primer año luego de la implementación de la solución.

INGRESOS			
RUBRO	**ANUAL**	**PORCENTAJE**	**TOTAL DE COSTOS**
Corporativo	$ 192,000.00	+ 11%	$ 213,120.00
Enlace	$ 162,000.00	+ 11%	$ 179,820.00
Dial Up	$ 486,000.00	+ 11%	$ 539,460.00
TOTAL COSTOS AL AÑO 1			$ 932,400.00

Tabla 3.11 Ingresos en el primer año luego de la implementación de la solución.

SITUACIÓN ACTUAL		
Ingresos	$	932,400.00
Egresos	$	169,291.20
TOTAL	$	763,108.80

Tabla 3.12 Total de ganancia en el primer año de la implementación de la solución.

Diferencia = Año 1 – Año 0

Diferencia = $ 763,108.80 – $ 707,400.00

Diferencia = $ 55,708.80

Luego de obtener el resultado de la diferencia entre el total del año 1 y del año 0; por medio de una regla de tres se calcula el valor de la tasa de crecimiento.

$$\frac{707,400.00}{55,708.80} \rightarrow \frac{100\%}{X}$$

Tasa de crecimiento = 7.88%

3.3.1.8.2 COSTO DE MANTENIMIENTO.

MANTENIMIENTO		
TIPOS	**ANUAL**	
Mantenimiento preventivo	$	4,800.00
Mantenimiento correctivo	$	1,200.00
Suministros	$	100.00
TOTAL	**$**	**6,110.00**

Tabla 3.13 Costos de mantenimiento de la implementación de la solución.

3.3.1.8.3 PUNTO DE RETORNO.

AÑO	COSTOS	COSTOS ACUMULADOS	BENEFICIOS	BENEFICIOS ACUMULADOS
0	26,772.35	26,772.35	0	0
1	6,110,00	32,882.35	24.931,82	24.931,82
2	6,591,46	39,473,81	26.896.45	51.828,27
3	7,116,86	46,590.67	29.015,89	80.844,16

Tabla 3.14 Costos y Beneficios

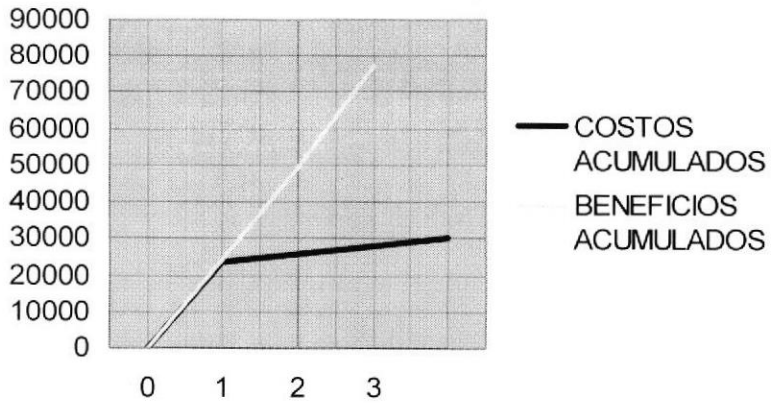


Figura 3.1 Punto de equilibrio de la inversión.

3.3.1.9 DIAGRAMA GANT ALTERNATIVA I

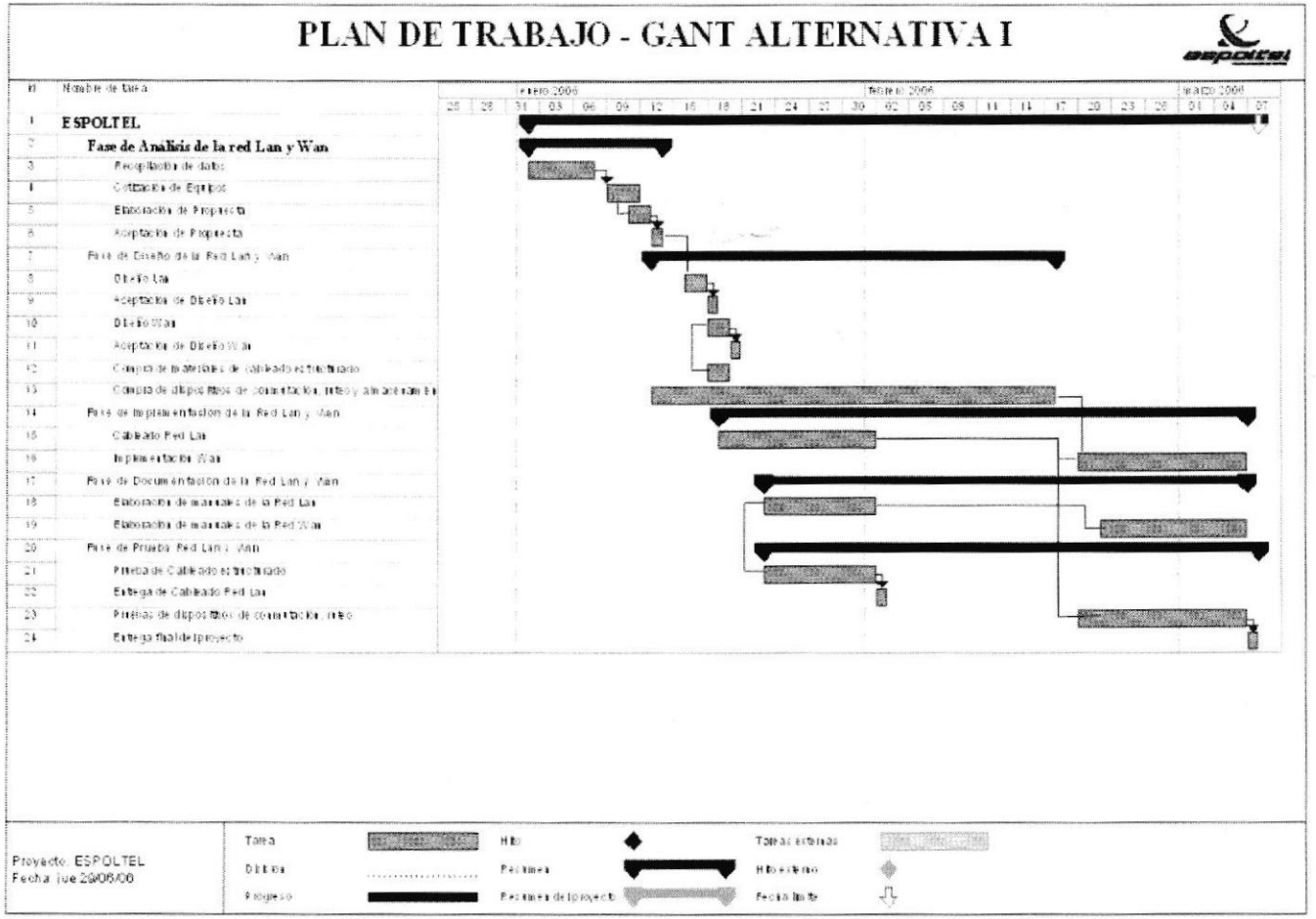


Figura 3.2 Diagrama Gant Alternativa I

3.3.2 ALTERNATIVA II.

A pesar de que esta alternativa no es la escogida, también abarca mejoras en cableado, dispositivos de ruteo, conmutación y almacenamiento aunque no con el mismo alcance.

3.3.2.1 OBJETIVO.

Mejorar y fortalecer la infraestructura Wan y Lan de la empresa para futuras proyecciones de crecimiento, pero con un costo de inversión inferior al de la Alternativa I, debido a que se invertirá en dispositivos con menor costo de adquisición, pero con un buen desempeño.

3.3.2.2 FACTIBILIDAD TÉCNICA.

3.3.2.2.1 DISPOSITIVOS DE RUTEO, CONMUTACIÓN Y ALMACENAMIENTO.

CANTIDAD	EQUIPO	CARACTERÍSTICAS	UBICACIÓN
1	**Servidor**	Intel P4 3.2 GHZ 256MB 4 GB. máximo DDR 80 GB Standard SATA Network adapter Ethernet, Fast Ethernet, Gigabit Ethernet (10/100/1000) Bus de datos 800 Mhz Hot Swap Bays 6 Tape Backup Interno (20-40 GB)	Cuarto de comunicaciones (Peñas)
3	**Router**	2 Puertos Fast Ethernet 10/100. 1 Slot de Modulo de Red. 3 Slot para tarjetas Wic de interfaz Wan. 2 Slot para modulo de integridad avanzada. Fuente redundante.	Red Wan (Peñas – Prosperina Mapasingue)
1	**Switch**	Transmisión: 10/100/1000 48 puertos Administrable Administrable Stack	Red Wan (Peñas)

Tabla 3.15 Dispositivos de ruteo, conmutación y almacenamiento de la Alternativa II.

3.3.2.2.2 MATERIALES DE CABLEADO ESTRUCTURADO.

CANTIDAD	EQUIPO	CARACTERÍSTICAS	UBICACIÓN
1	**Canalón**	Metálico Conexión a tierra	Toda la red (Peñas)
1	**Bobina cable UTP**	Categoría 5e	Toda la red (Peñas)
80	**Conectores**	RJ-45	Toda la red (Peñas)
20	**Patch Cord**	Tamaño: 50 cm. 350 Mhrz marca: cp Technologies	Cuarto de comunicaciones (Peñas

Tabla 3.16 Materiales de cableado de la Alternativa II.

3.3.2.3 FACTIBILIDAD ECONÓMICA.

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
1	Servidor Cybertron	1,300.00	1,300.00
3	Router Cisco 2691	4,615.00	13,845.00
1	Canalón metálico X 3 m.	200.00	200.00
1	Bobina cable UTP Cat 5e	48.00	48.00
80	Conectores RJ-45	0.45	36.00
20	Patch Cord	1.00	20.00
			$ 15,449.00

Tabla 3.17 Factibilidad Económica de la Alternativa II.

3.3.2.4 FACTIBILIDAD OPERATIVA.

CANTIDAD	ACTIVIDAD	SEMANAS	COSTO SEMANA	TOTAL
1	**Fase Análisis de la red Lan y Wan** Ingeniero en comunicaciones	2	$ 150	$ 300.00
1	**Fase Diseño de la red Lan y Wan** Ingeniero en comunicaciones	1	$ 150	$ 150.00
2 2	**Fase Implementación de la red Lan y Wan.** Ingeniero en comunicaciones Técnico en redes	4	$ 150 $ 80	$ 1200.00 $ 640.00
1	**Fase Documentación de la Red Lan y Wan** Ingeniero en comunicaciones	2	$ 150	$ 300.00
2 2	**Fase Prueba** Ingeniero en comunicaciones Técnicos en redes.	4	$ 150 $ 80	$ 1200.00 $ 640.00
				$ 2,590.00

Tabla 3.18 Factibilidad Operativa de la Alternativa II.

Nota: Conforme avance la fase de implementación Wan y Lan, avanzará la Fase de prueba es por eso que el valor de la Fase de prueba no influye en el valor total de los costos operativos.

3.3.2.5 COSTOS DE INVERSIÓN.

Hardware	:	$	15,449.00
Operativos	:	$	2,590.00
Imprevistos (25%)	:	$	4,509.75
Total	**:**	**$**	**22,548.75**

Todos los precios incluyen iva.

3.3.2.6 VENTAJAS.

Debido a la actualización de tecnología en sus dispositivos se puede ampliar la cobertura de la red wan.

Cableado estructurado organizado y con acceso rápido a solucionar inconvenientes de la red Lan.

3.3.2.7 BENEFICIOS.

Establecer una mejor distribución del cableado estructurado de la red Lan cumpliendo con la norma ANSI/TIA/EIA-568-A y el estándar IEEE 802.3, con el fin de obtener una certificación ISO.

Incrementar el nivel de velocidad y tiempo de respuesta en el tráfico de la red Lan.

Reducción de costos en los requerimientos técnicos.

Fortalecer los servicios que brindan a sus clientes debido a la actualización de tecnología en dispositivos de ruteo y conmutación.

3.3.2.8 TASA INTERNA DE RETORNO.

A continuación se demostrará al detalle el tiempo en que su inversión será recuperada. Para esto se tomará en cuenta los costos que el trabajo va a tener en el tiempo incluyendo el valor total del mismo y los beneficios económicos año a año.

Datos generales:

- Se proyecta un aumento del 30% en el rubro de sueldos para el año 2006.
- El porcentaje de inflación es del 16,8% anual.
- Actualmente tienen una taza de crecimiento anual del 11% en sus ingresos.
- Con los nuevos cambios se prevé el incremento de los ingresos en un 25%.

SITUACIÓN ACTUAL – INGRESOS			
No CLIENTES	**RUBRO**	**MENSUAL**	**ANUAL**
15	Corporativo	16,000.00	192,000.00
8	Enlace	13,500.00	162,500.00
1173	Dial Up	40,500.00	486,000.00
TOTAL INGRESOS			**$ 840,000.00**

Tabla 3.19 Ingresos actuales de Espoltel S.A. de la Alternativa II.

SITUACIÓN ACTUAL – EGRESOS	
RUBRO	**ANUAL**
Sueldos	109,200.00
Suministros	2,400.00
Transporte	1,800.00
Servicios Básicos	19,200.00
TOTAL	**$ 132,600.00**

Tabla 3.20 Egresos actuales de Espoltel S.A. de la Alternativa II.

SITUACIÓN ACTUAL		
Ingresos	$	840,000.00
Egresos	$	132,600.00
TOTAL	**$**	**707,400.00**

Tabla 3.21 Total de ganancia de Espoltel S.A. de la Alternativa II.

3.3.2.8.1 TASA DE CRECIMIENTO.

EGRESOS			
RUBRO	**ANUAL**	**PORCENTAJE**	**TOTAL**
Gasto de personal	$ 109,200.00	+ 30 %	$ 141,960.00
Costo de Vida	$ 23,400.00	+ 16,80 %	$ 27,331.20
TOTAL COSTOS AL AÑO 1			$ 169,291.20

Tabla 3.22 Egresos en el primer año luego de la implementación de la solución.

INGRESOS			
RUBRO	**ANUAL**	**PORCENTAJE**	**TOTAL DE COSTOS**
Corporativo	$ 192,000.00	+ 11%	$ 213,120.00
Enlace	$ 162,000.00	+ 11%	$ 179,820.00
Dial Up	$ 486,000.00	+ 11%	$ 539,460.00
TOTAL COSTOS AL AÑO 1			$ 932,400.00

Tabla 3.23 Ingresos en el primer año luego de la implementación de la solución.

SITUACIÓN ACTUAL		
Ingresos	$	932,400.00
Egresos	$	169,291.20
TOTAL	$	763,108.80

Tabla 3.24 Total de ganancias en el primer año luego de la implementación de la solución.

Diferencia = Año 1 – Año 0

Diferencia = $ 763,108.80 – $ 707,400.00

Diferencia = $ 55,708.80

Luego de obtener el resultado de la diferencia entre el total del año 1 y del año 0; por medio de una regla de tres se calcula el valor de la tasa de crecimiento.

$$\frac{707{,}400.00}{55{,}708.80} \rightarrow \frac{100\%}{X}$$

Tasa de crecimiento = 7.88%

3.3.2.8.2 COSTO DE MANTENIMIENTO.

MANTENIMIENTO		
TIPOS	**ANUAL**	
Mantenimiento preventivo	$	4,800.00
Mantenimiento correctivo	$	1,200.00
Suministros	$	100.00
TOTAL	**$**	**6,110.00**

Tabla 3.25 Costos de mantenimiento en el primer año luego de la implementación de la solución.

3.3.2.8.3 PUNTO DE RETORNO.

AÑO	COSTOS	COSTOS ACUMULADOS	BENEFICIOS	BENEFICIOS ACUMULADOS
0	22,548.75	22,548.75	0	0
1	6,110.00	28,658.75	24.931,82	24.931,82
2	6,591,46	35,250,21	26.896.45	51.828,27
3	7,116,86	42,367.07	29.015,89	80.844,16

Tabla 3.26 Costos y Beneficios.

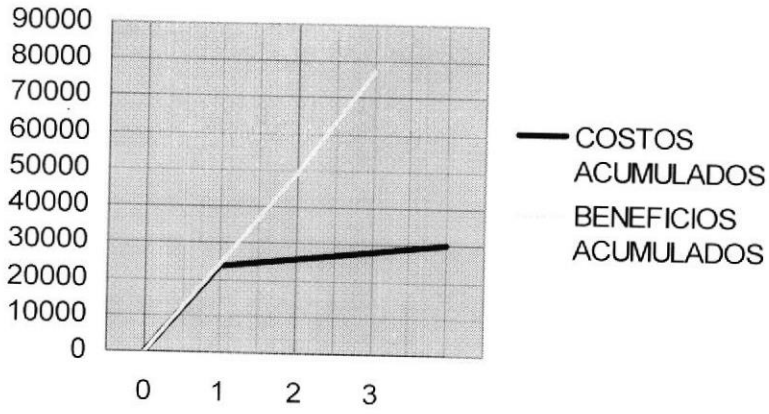


Figura 3.3 Punto de equilibrio de la inversión.

3.3.2.9 DIAGRAMA GANT ALTERNATIVA II

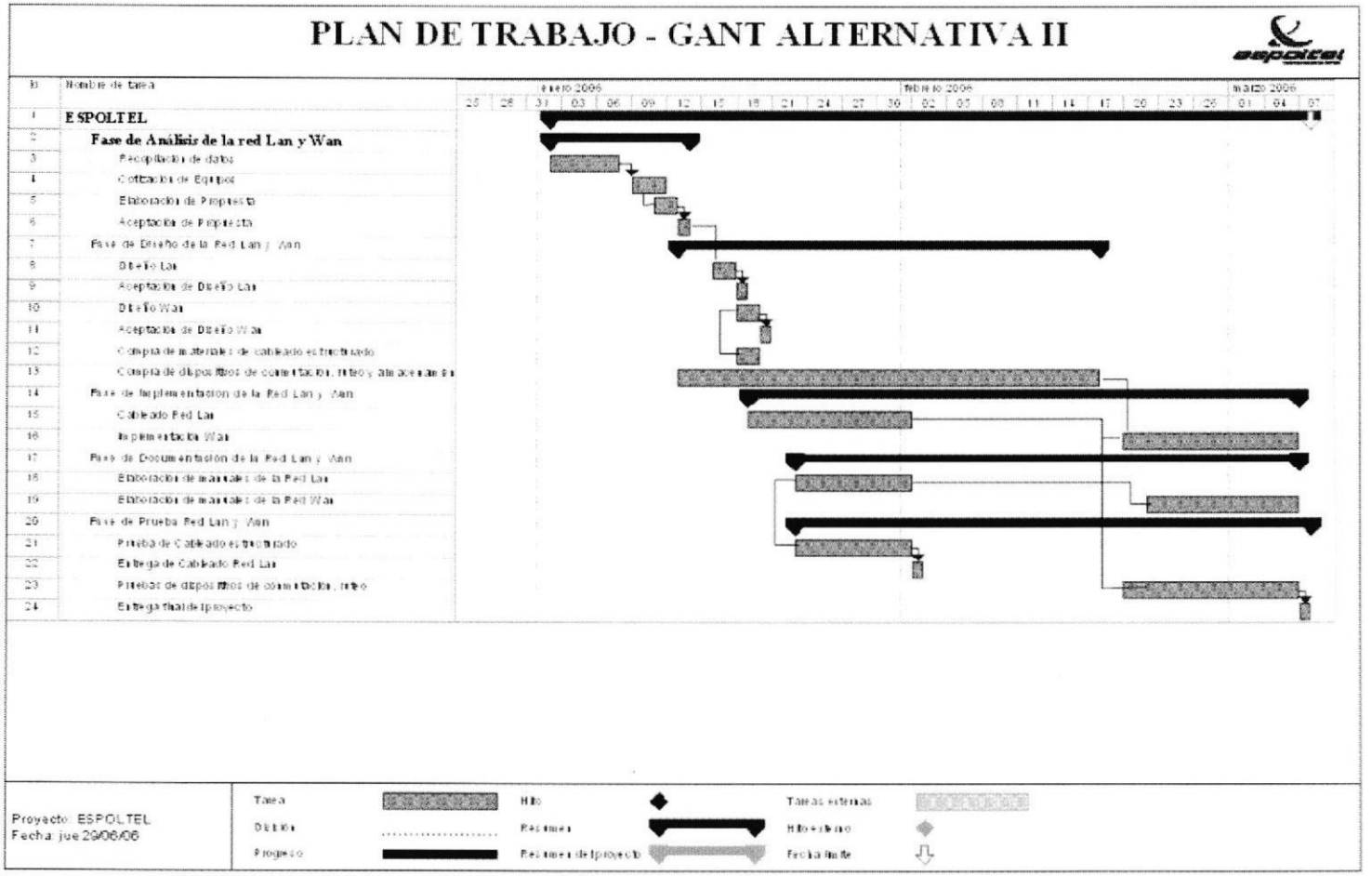


Figura 3.4 Diagrama Gant Alternativa II

3.4 FORMA DE PAGO.

A continuación se detallará la forma de pago establecida, para ambas alternativas.

75% Anticipo al cierre del contrato.
25% Contra entrega.

Duración del Trabajo: 9 semanas laborables.

El cliente se compromete a proveer las instalaciones y dar las facilidades respectivas para realizar el trabajo en el tiempo estimado, caso contrario, el sueldo por los días adicionales del personal involucrado, será cancelado por parte de ESPOLTEL.

CAPÍTULO 4

IMPLEMENTACIÓN

4 CABLEADO ESTRUCTURADO.

4.1 RED WAN DE ESPOLTEL S.A.

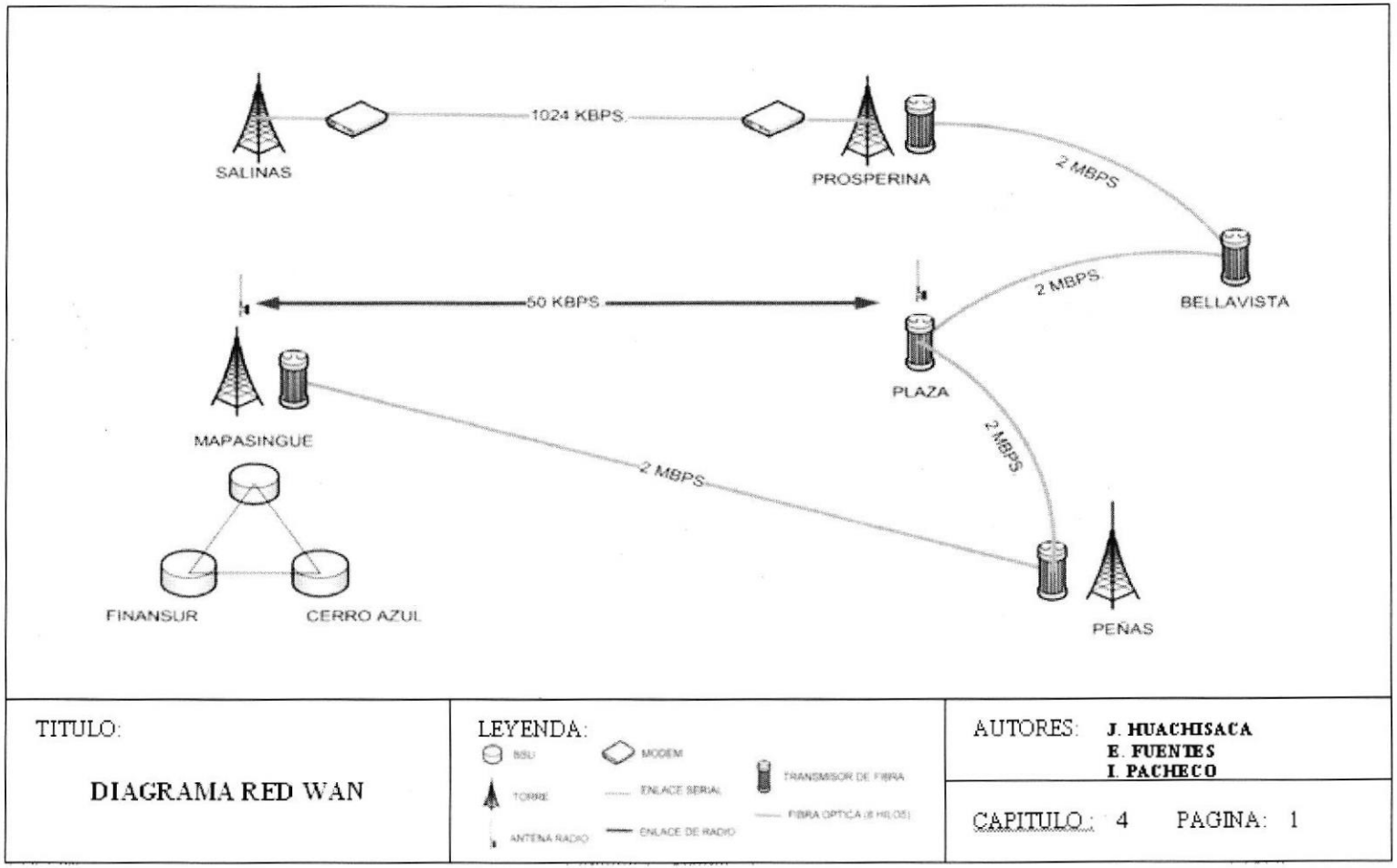


Figura 4.1 Diagrama de la red Wan

4.1.1 CONEXIÓN DE LA RED WAN SALINAS – PROSPERINA.

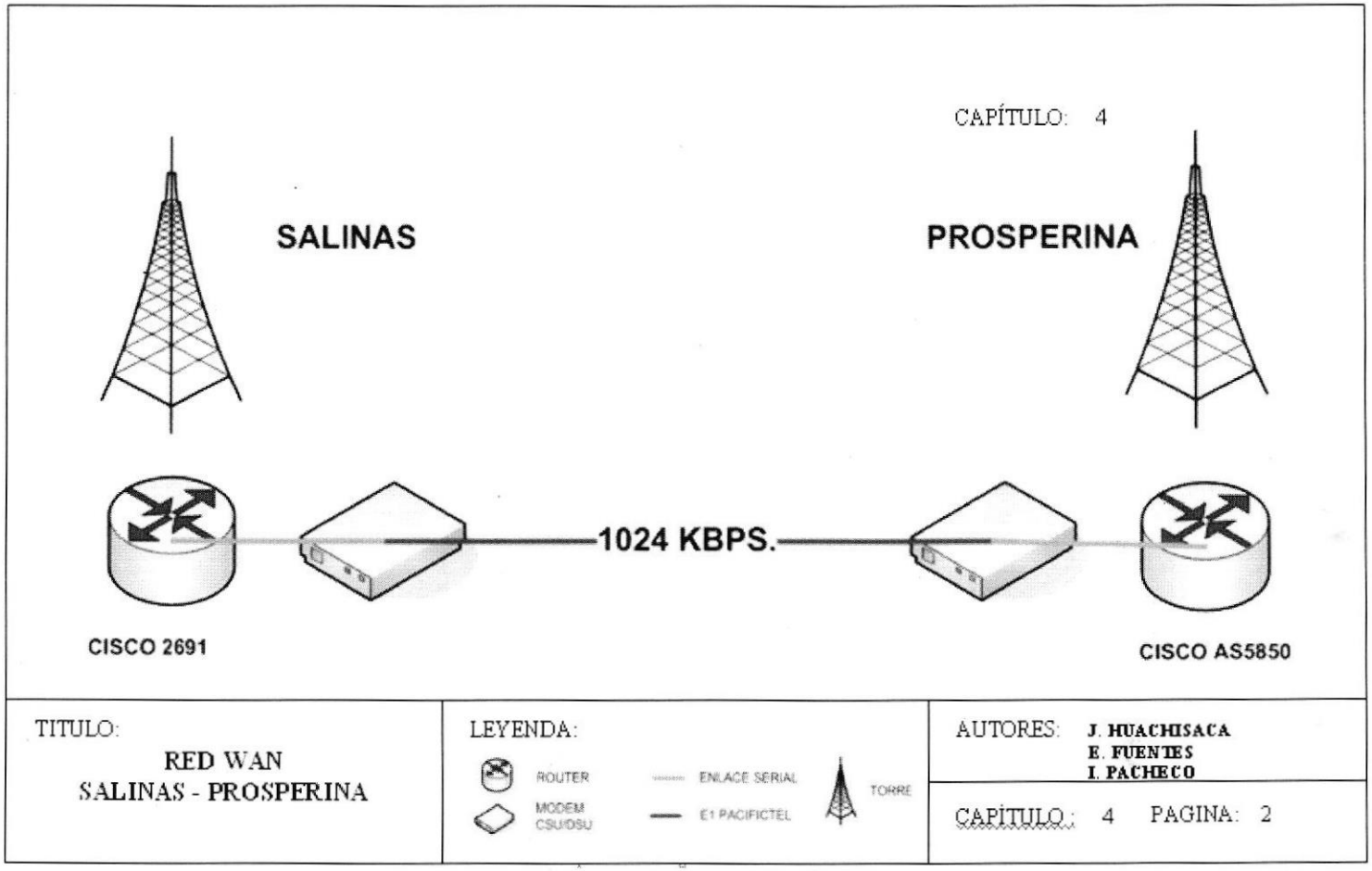


Figura 4.2 Conexión Salinas a Prosperina

4.1.2 CONEXIÓN DE LA RED WAN MAPASINGUE – PROSPERINA.

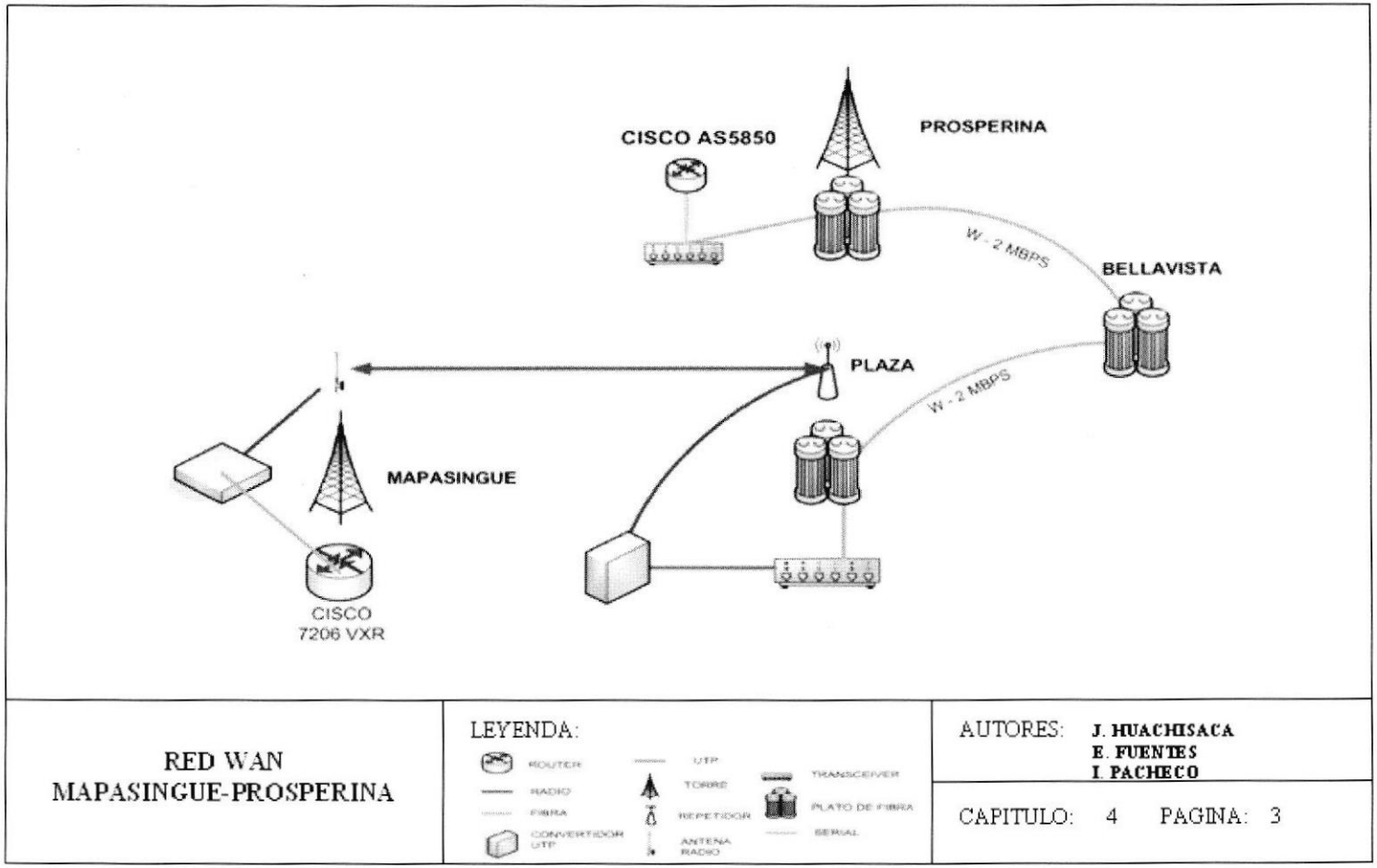


Figura 4.3 Conexión Mapasingue a Prosperina

4.1.3 CONEXIÓN DE LA RED WAN PROSPERINA – PEÑAS.

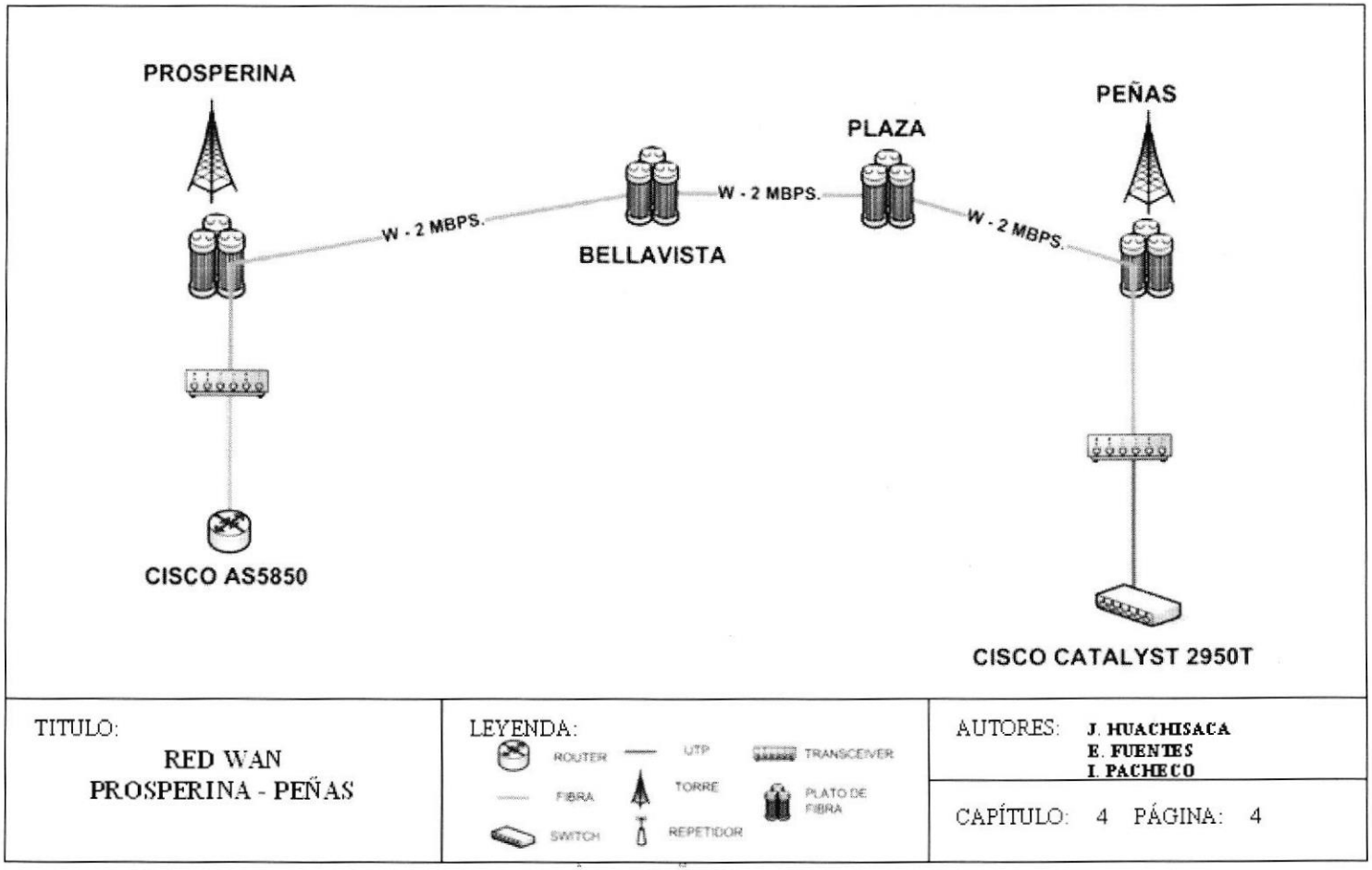


Figura 4.4 Conexión Prosperina a Peñas

4.1.4 CONEXIÓN DE LA RED WAN MAPASINGUE – PEÑAS.

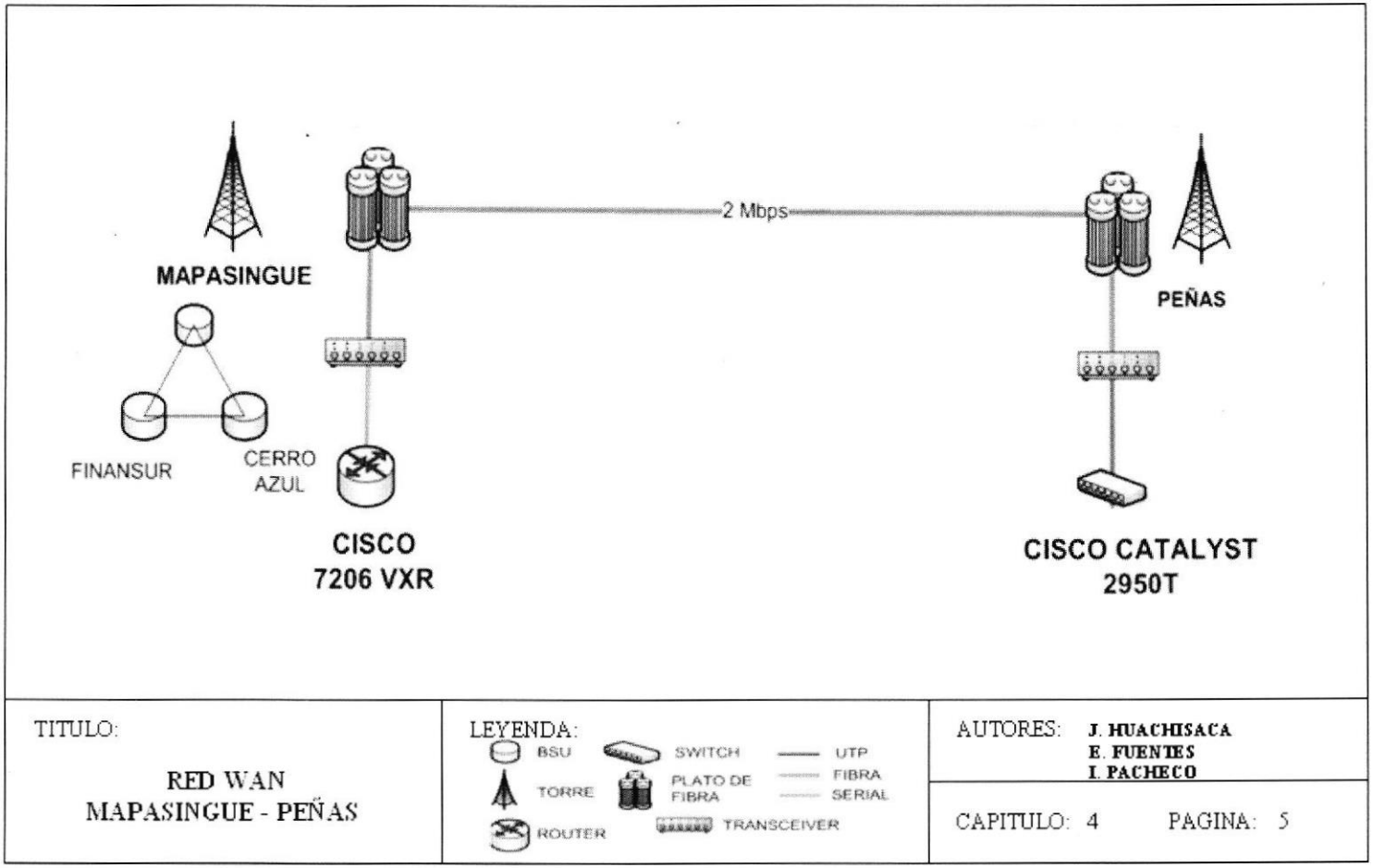


Figura 4.5 Conexión Mapasingue a Peñas

4.2 RESPALDO DE LA RED WAN DE ESPOLTEL S.A.

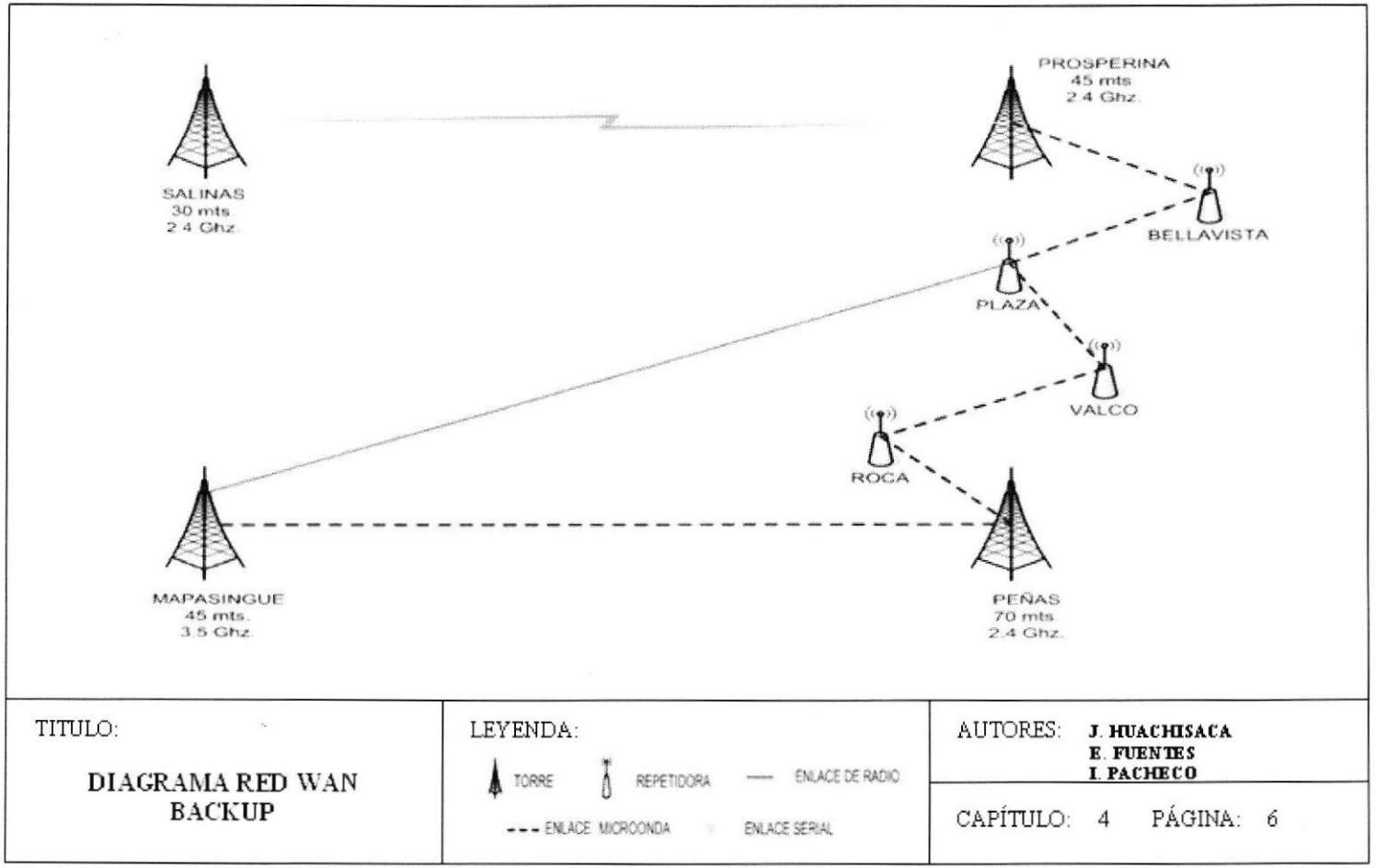


Figura 4.6 Diagrama red Wan Backup

4.2.1 RESPALDO DE LA CONEXIÓN MAPASINGUE – PROSPERINA.

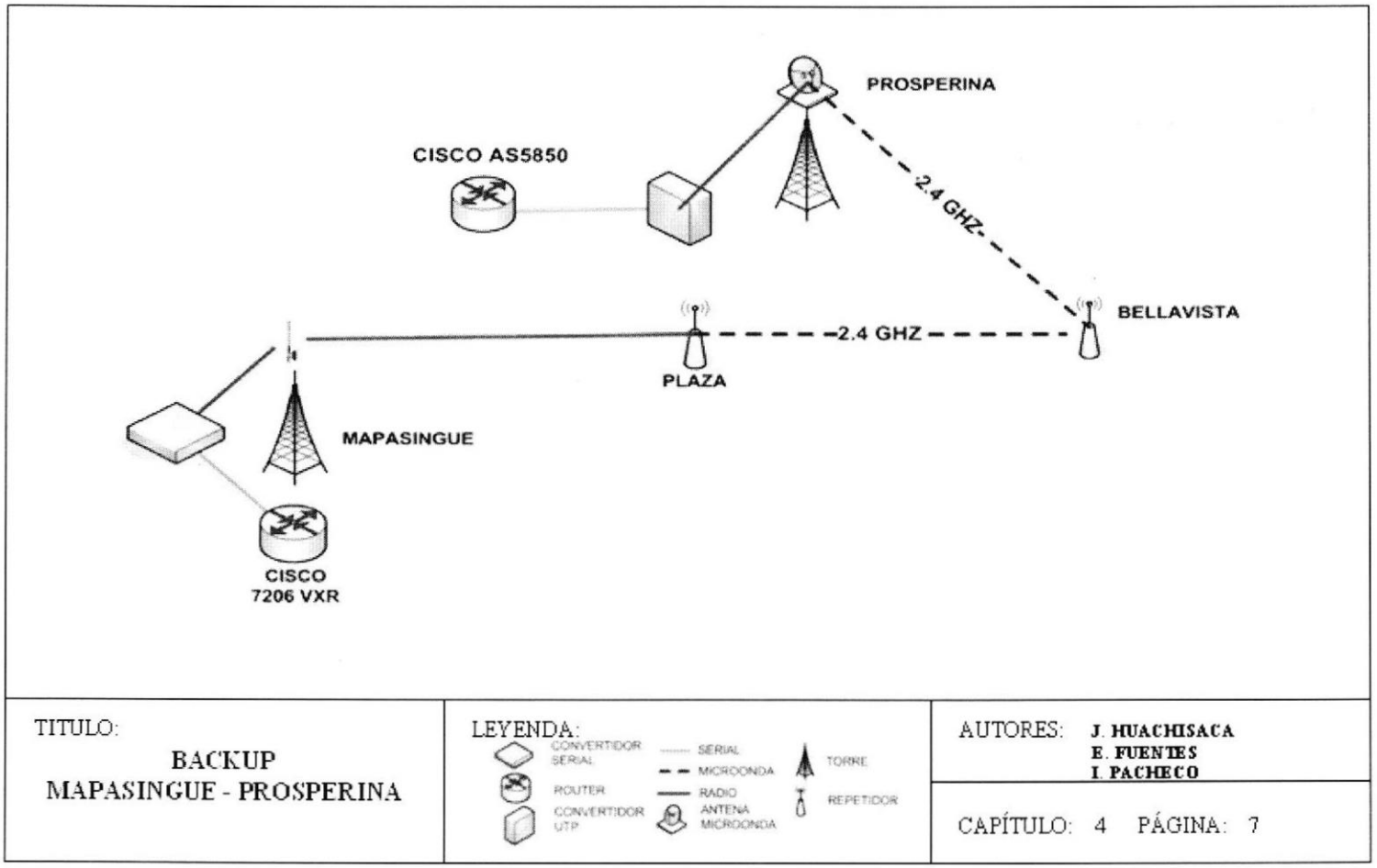


Figura 4.7 Conexión Backup Mapasingue a Prosperina

4.2.2 RESPALDO DE LA CONEXIÓN PROSPERINA – PEÑAS.

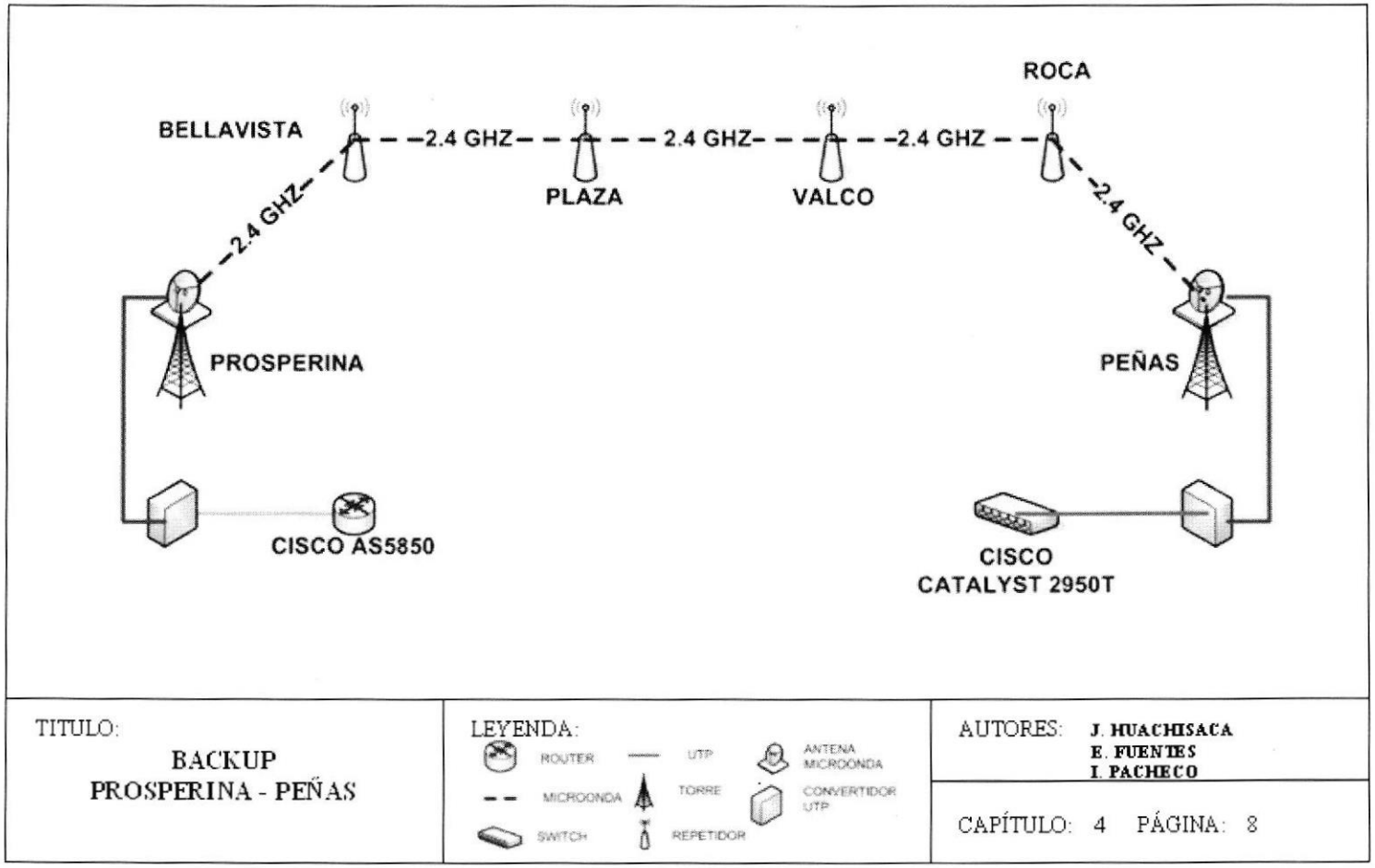


Figura 4.8 Conexión Backup Prosperina a Peñas

4.2.3 RESPALDO DE LA CONEXIÓN MAPASINGUE – PEÑAS.

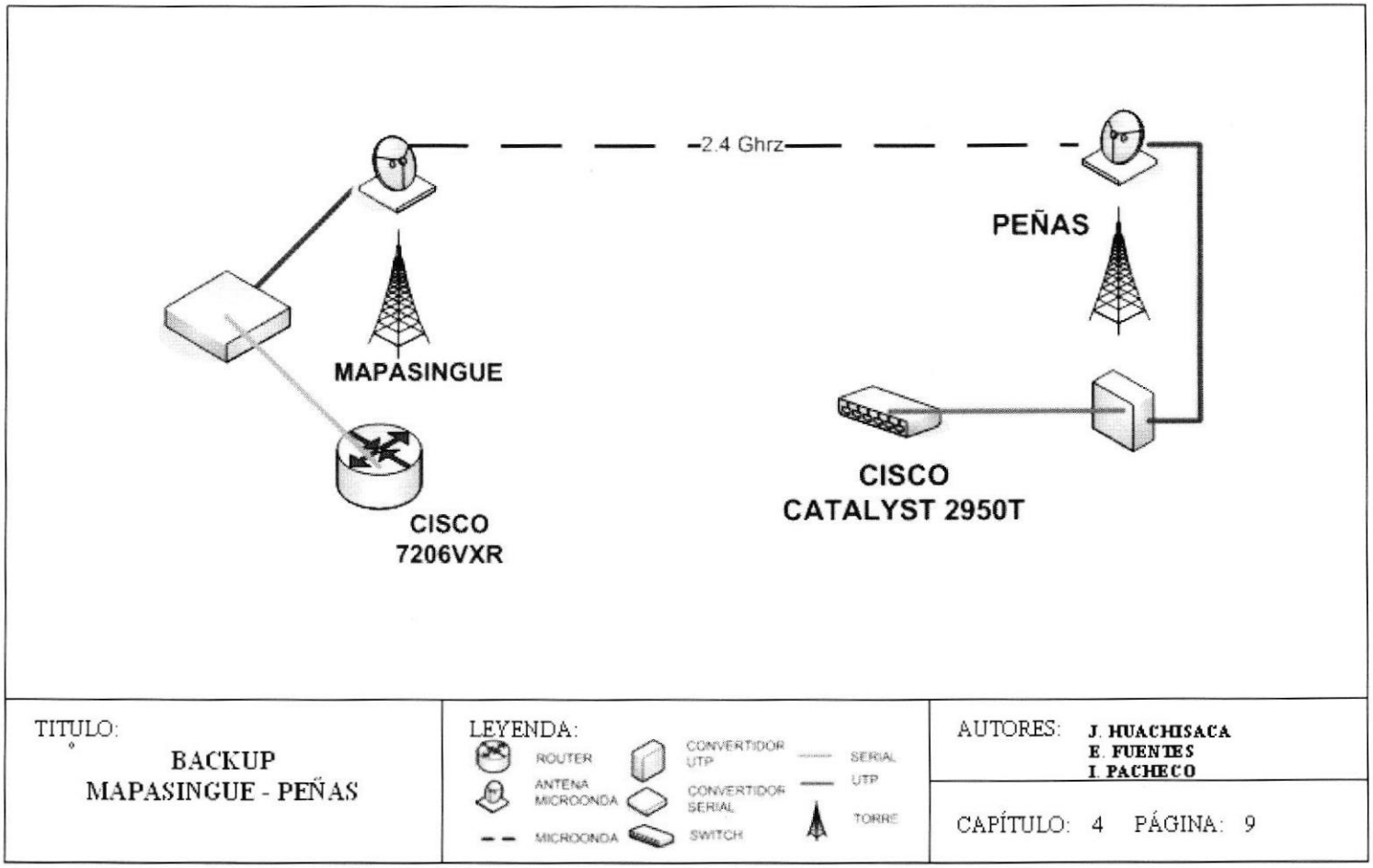


Figura 4.9 Conexión Backup Mapasingue a Peñas

4.3 ANÁLISIS DE PISO RED LAN DE ESPOLTEL S.A. – CAMPUS PEÑAS.

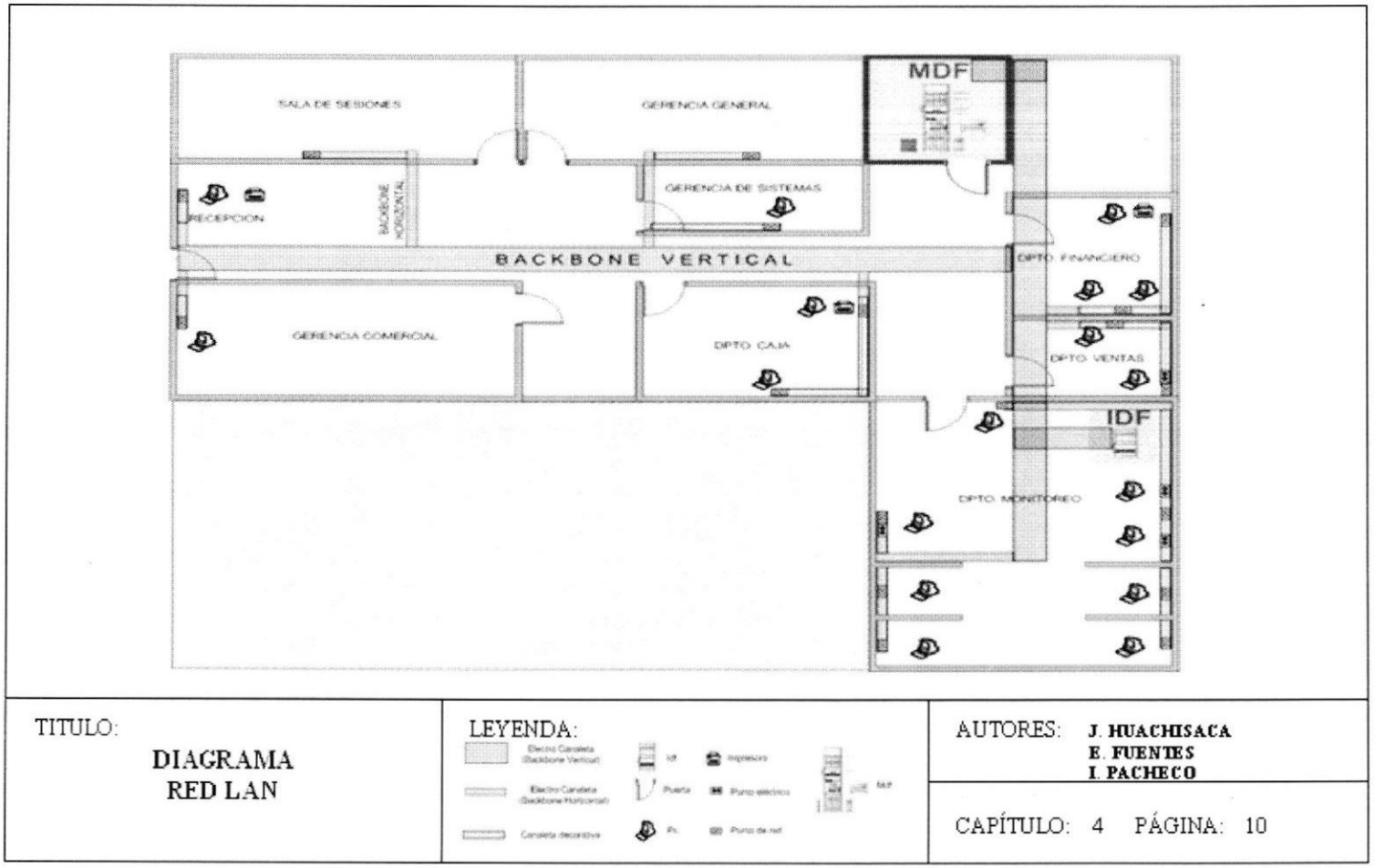


Figura 4.10 Diagrama red Lan

4.3.1 ANÁLISIS DE PISO DE LOS DPTOS. RECEPCIÓN SALA DE SESIONES, GERENCIAS Y CAJA.

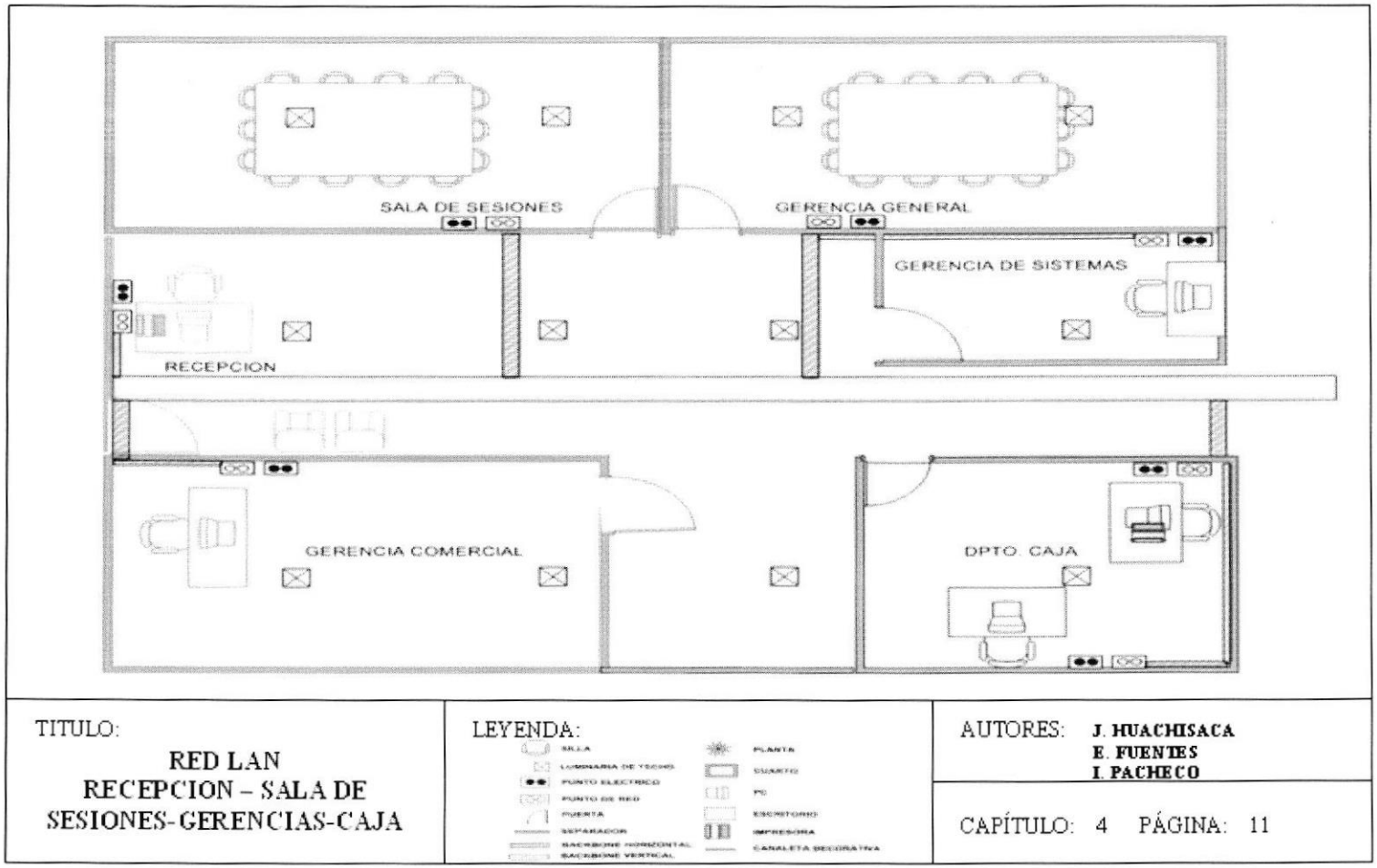


Figura 4.11 Diagrama red Lan Recepción, Sala de Sesiones, Gerencias y Caja.

4.3.2 ANÁLISIS DE PISO DEL DPTO. TÉCNICO O MONITOREO.

Figura 4.12 Diagrama red Lan Dpto. Técnico

4.3.3 ANÁLISIS DE PISO DE LOS DPTOS. FINANCIERO Y VENTAS.

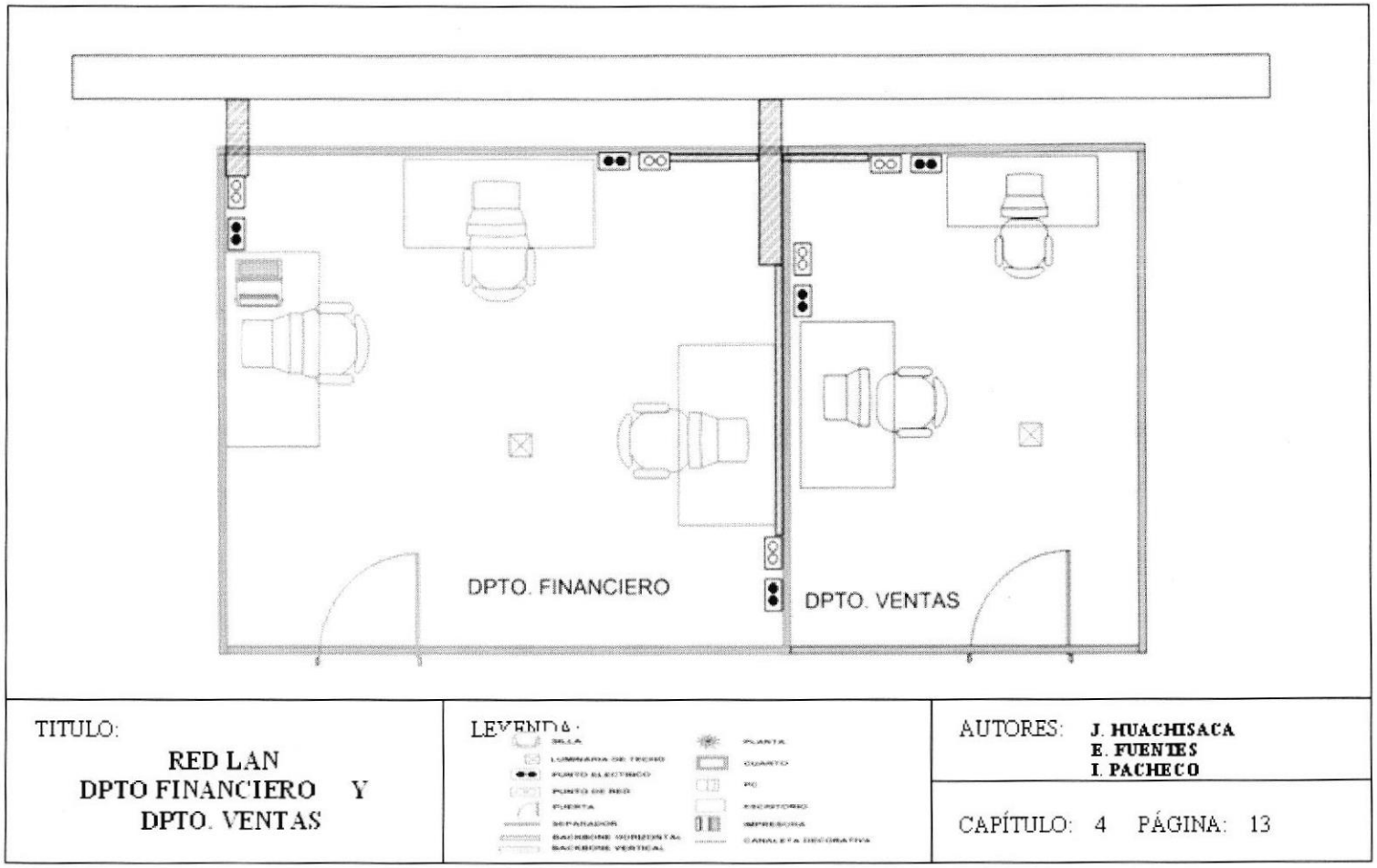


Figura 4.13 Diagrama red Lan Dpto. Financiero y Ventas.

4.3.4 CUARTO DE COMUNICACIONES (MDF) – CAMPUS PEÑAS.

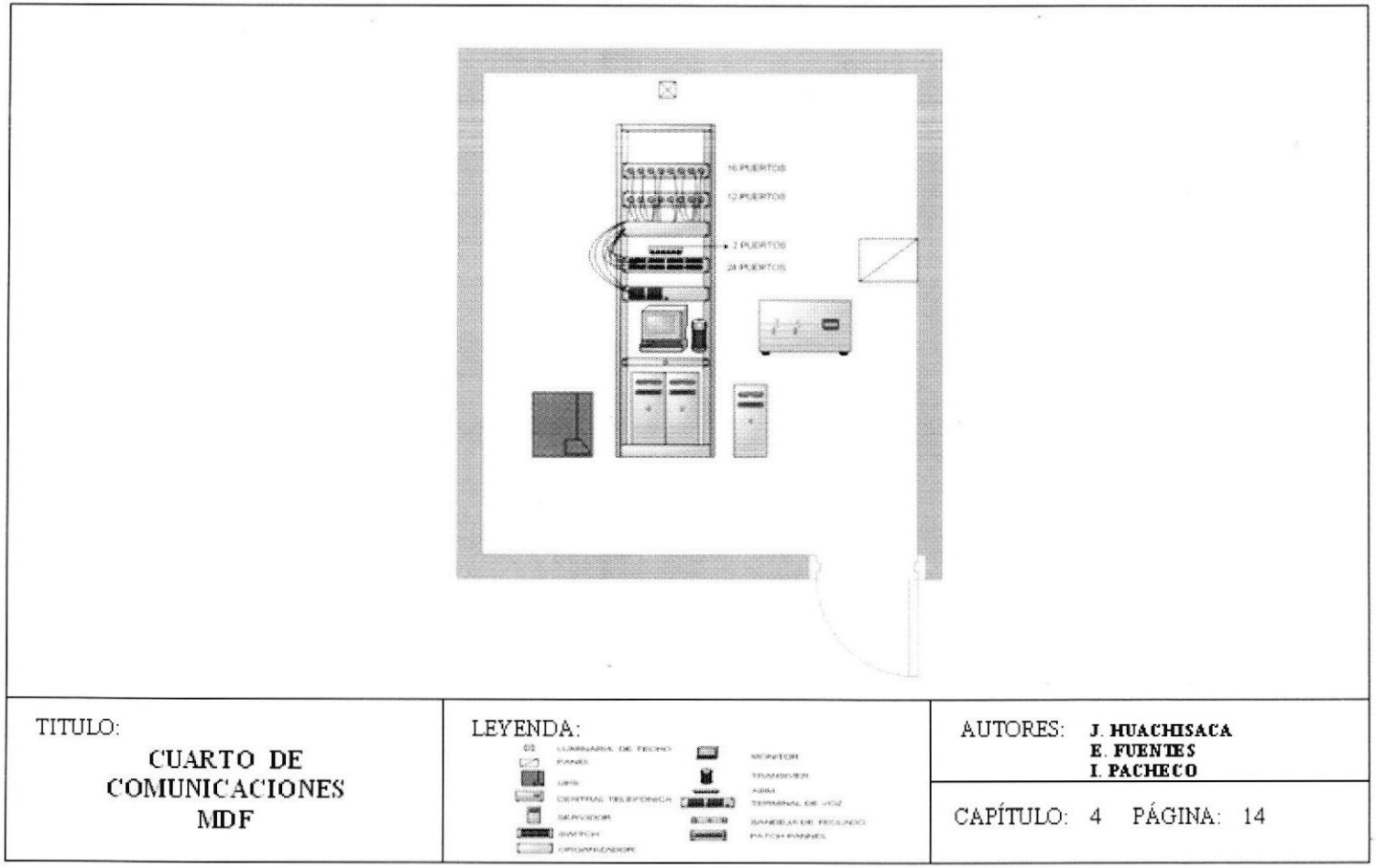


Figura 4.14 Diagrama del Cuarto de Comunicaciones (MDF)

CAPÍTULO 5

CONFIGURACIONES DE DISPOSITIVOS

5. CONFIGURACIÓN DE DISPOSITIVOS.

5.1 ROUTER.

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

5.1.1 FUNCIONES DEL ROUTER.

- La función principal de un router es enrutar.
- Un router es un dispositivo LAN y WAN.
- Proporciona conexiones con y entre los diversos estándares de enlace de datos y físico WAN.

5.1.2 TECNOLOGÍAS SOPORTADAS.

- Control de enlace de datos de alto nivel (HDLC).
- Frame Relay.
- Protocolo punto a punto (PPP).
- Control de enlace de datos síncrono (SDLC).
- Protocolo Internet de enlace serial (SLIP).
- X.25.
- ATM.

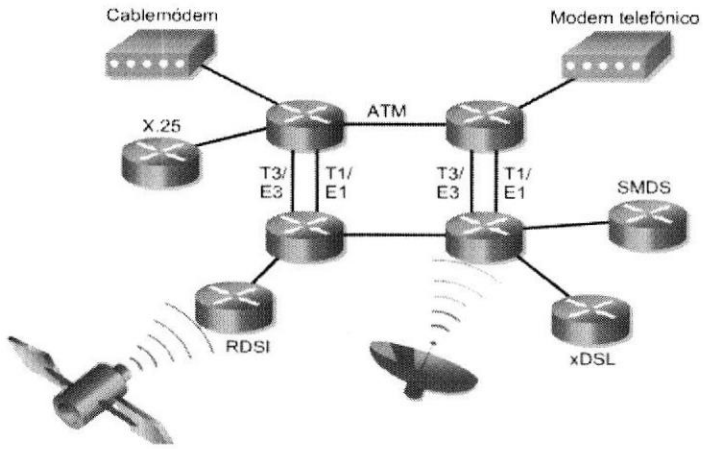


Figura 5.1 Tecnologías de router.

5.1.3 COMPONENTES INTERNOS DEL ROUTER.

Los principales componentes internos del router son:

- La memoria de acceso aleatorio (RAM).

- La memoria de acceso aleatorio no volátil (NVRAM).
- La memoria flash.
- La memoria de sólo lectura (ROM).

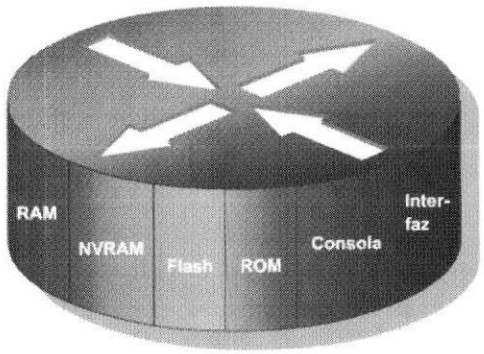


Figura 5.2 Componentes internos de un router.

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

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

Memoria flash: Se utiliza para almacenar una imagen completa del software IOS. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash, agregando o reemplazando los módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.

NVRAM: La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM).

Buses: La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces.

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

ROM: La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS, desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM en los tomas.

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

Los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

Los routers necesitan el software denominado Sistema Operativo de Internetworking (IOS) para ejecutar los archivos de configuración.

A través de los protocolos de enrutamiento, los routers toman decisiones sobre cuál es la mejor ruta para los paquetes.

Son dispositivos electrónicos complejos que permiten manejar comunicaciones entre redes que se encuentran a gran distancia, utilizando vínculos provistos por las empresas prestatarias del servicio telefónico (líneas punto a punto), líneas de datos (Arpac), enlaces vía satélite, etc.

Poseen avanzadas funciones de negociación del enlace y conversión de protocolos de transmisión. Se utilizan por lo general en empresas que manejan muchas sucursales, tales como Bancos, etc. Están relacionados con sistemas bajo Unix y TCP-IP.

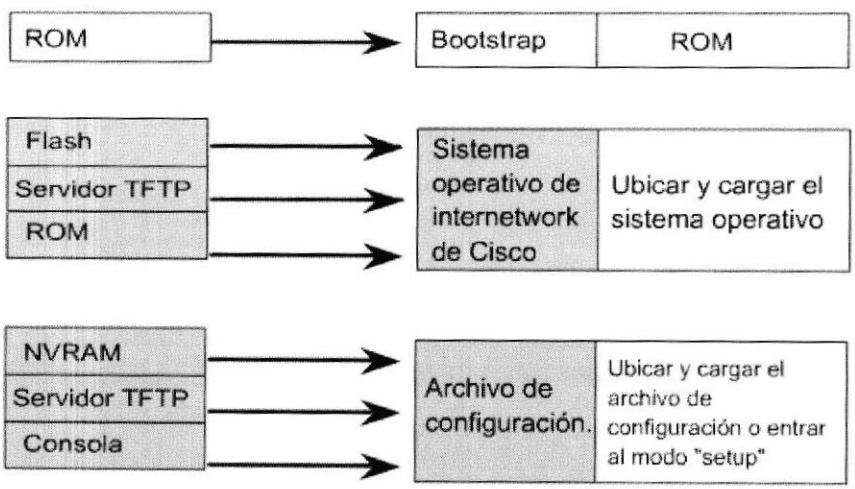


Figura 5.3 Secuencia de arranque.

5.1.4 COMPONENTES EXTERNOS DE UN ROUTER.

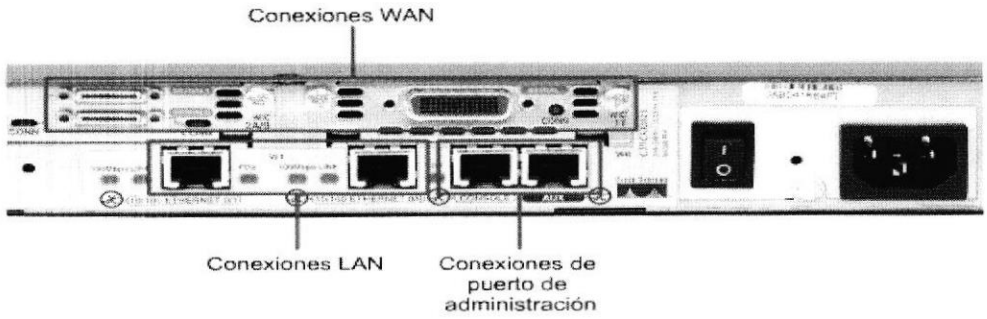


Figura 5.4 Componentes externos de un router.

Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring.

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

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

5.1.5 CONECCIÓN AL PUERTO DE CONSOLA.

5.1.5.1 REQUERIMIENTOS.

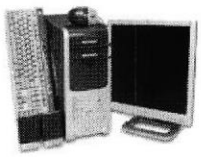
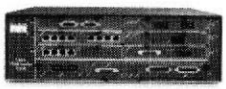
Imagen	Equipo
	Computador Tarjeta 10/100 Mbps Puerto Com disponible.
	Cable de consola
	Router

Tabla 5.1 Requerimientos para conectar un pc al router.

5.1.5.2 CONECCIÓN POR HARDWARE.

Para conectar un PC al Puerto de consola, se debe usar un cable Rollover RJ-45 a RJ-45, y cualquier adaptador DTE RJ-45 a DB-25 o RJ-45 a DB-9 hembra.

- Se debe conectar el extremo RJ-45 del cable de la consola al puerto **consola** del panel posterior del router, tal como se muestra en la Figura 5.7.

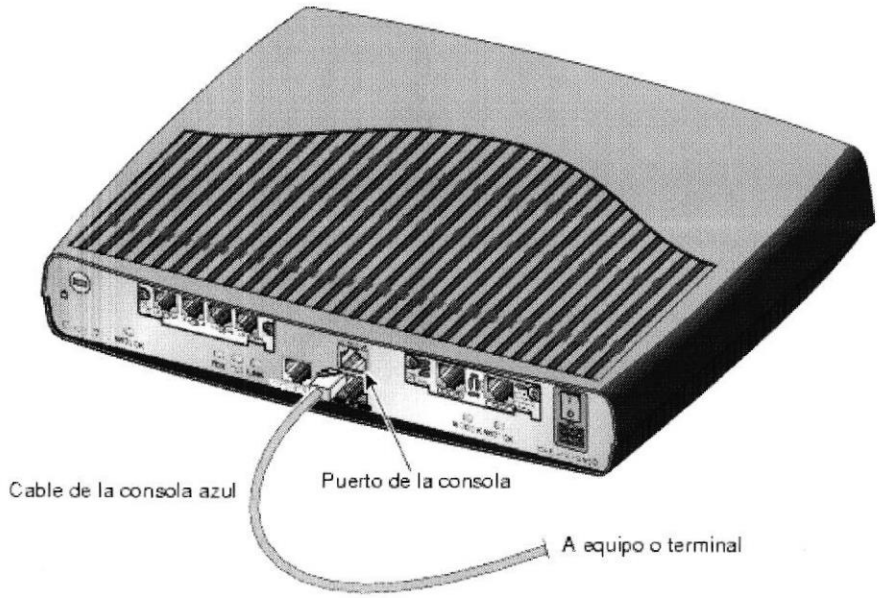


Figura 5.5 Conexión del cable de consola al router.

- Identifique el puerto serie, ubicado el parte posterior del computador.

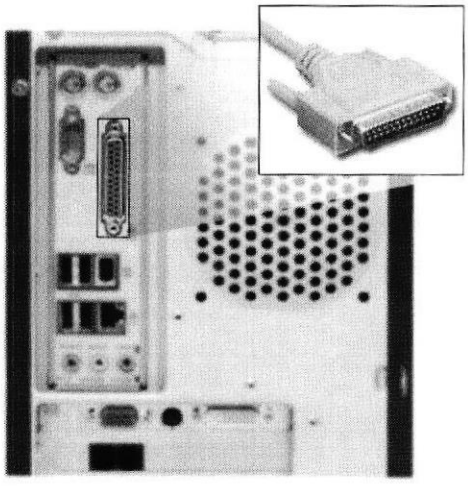


Figura 5.6 Puerto Serie del Computador.

- Conecte el extremo DB-9 del cable de la consola al puerto de la consola (también denominado *puerto serie*) del equipo. Si este adaptador no encaja, necesitará uno adecuado.

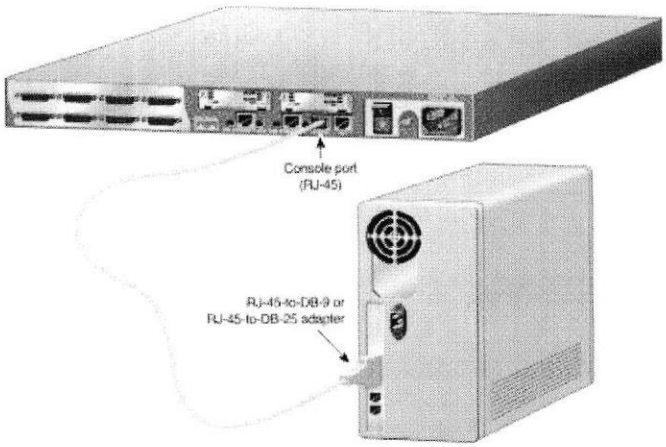


Figura 5.7 Esquema de conexión de un router a una terminal.

5.1.5.3 CONECCIÓN POR SOFTWARE (HYPER TERMINAL).

De clic en el menú Inicio, Opción Programas, luego elija Accesorios, Comunicaciones y por último Hyper Terminal.

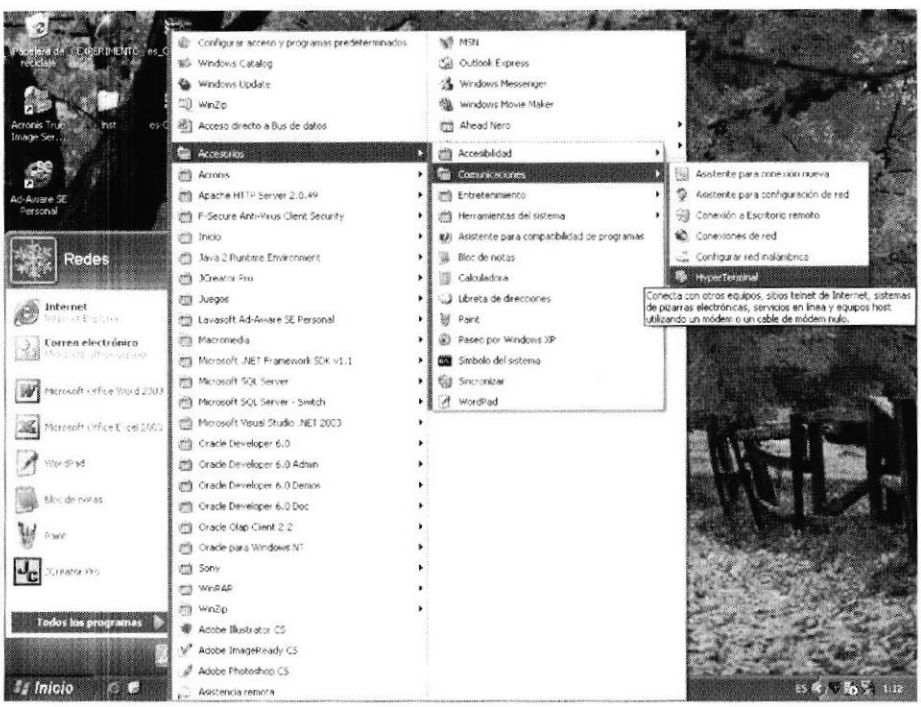


Figura 5.8 Pantalla para abrir una Hyper Terminal.

- Si es la primera vez que configura la Hyper Terminal le aparecerá un mensaje de confirmación, para hacer que el Hyper Terminal sea su programa predeterminado de telnet y además tendrá que configurar el modem.

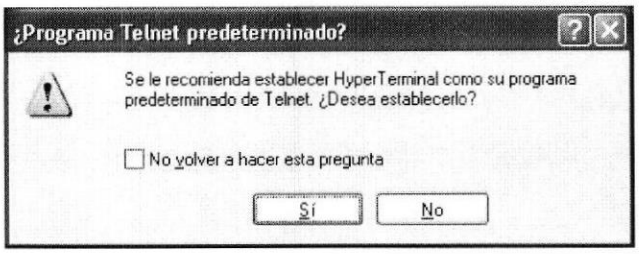


Figura 5.9 Pantalla para predeterminar telnet.

- Especifique el país en el que se encuentra, especifique el código de área, el número telefónico de acceso, dar clic en **Aceptar**.

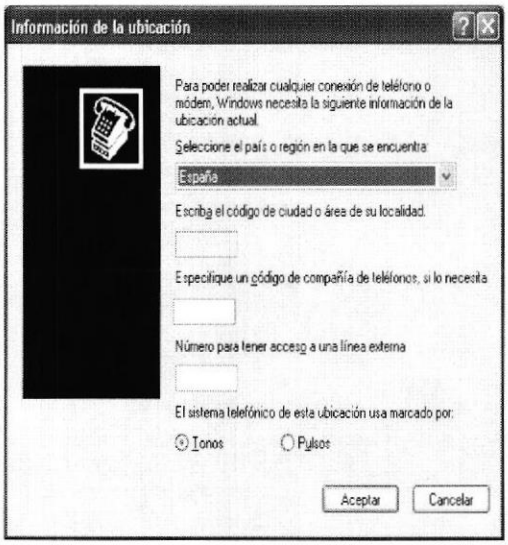


Figura 5.10 Pantalla de información de la ubicación.

- Al terminar la configuración del modem aparecerá una pantalla que muestra los datos anteriormente suministrados, dar clic en **Aceptar**.

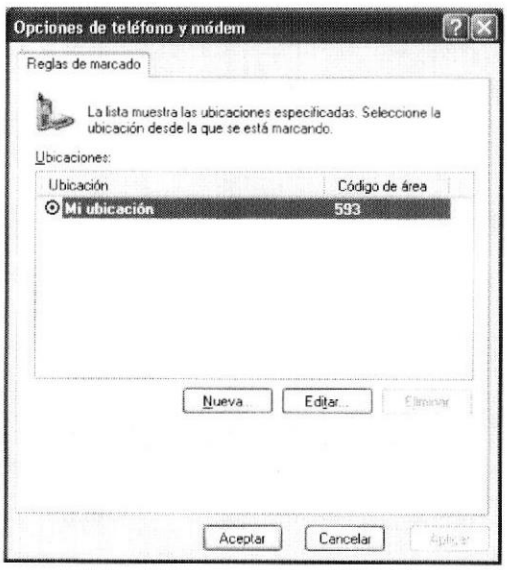


Figura 5.11 Pantalla de opciones de teléfono y modem.

- En el cuadro de dialogo siguiente, deberá especificar un nombre y un ícono para la conexión, luego, dar clic en **Aceptar**.

Figura 5.12 Pantalla de descripción de la conexión.

Nota Sino configura un nombre para la conexión, no podrá conectarse al router.

- A continuación se debe seleccionar el tipo de puerto por el cual se va a establecer la conexión.

Figura 5.13 Pantalla de conexión.

- Luego de esto se debe dar clic en **aceptar**.

Figura 5.14 Pantalla de conexión.

- Asignar los parámetros por defecto para el Puerto de consola y dar clic en **aceptar**.

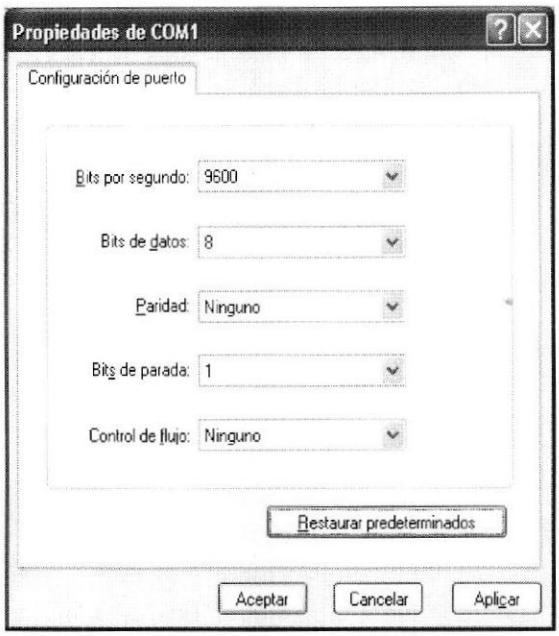


Figura 5.15 Pantalla de Propiedades del puerto Com1.

- **Bits por segundo**
  Número de bits transmitidos por segundo, que se usa como medida de la velocidad a la que un dispositivo, como un módem, puede transferir datos.

  Velocidad en la cual trabaja el cable serial para conectarse al puerto.

- **Bit de datos**
  Los bits de datos son el número de bits de una palabra. La mayoría de los sistemas usan ocho bits para representar un carácter de datos (ASCII

extendido). En raras ocasiones, algunos sistemas más antiguos utilizan siete bits.

Configuración del Procesamiento de datos al pasar al hyper terminal en bps.

- **Paridad**
  En comunicaciones asincrónicas, bit adicional utilizado para comprobar si hay errores en los grupos de bits de datos transferidos dentro de un equipo o entre equipos. En comunicaciones de módem a módem, se suele utilizar un bit de paridad para comprobar la exactitud con la que se transmite cada carácter.

  Método de trabajo, par, impar, ninguno, marca, espacio.

- **Bits de parada**
  Los bits de parada agrupan en tramas los paquetes de datos de las comunicaciones asincrónicas. Indican al módem de recepción que se ha enviado un byte. Los protocolos asincrónicos actuales no requieren nunca más de un bit de parada.

  Medida de transporte por la que se pasan datos al hyper Terminal.

- A continuación podrá proceder a configurar los router.

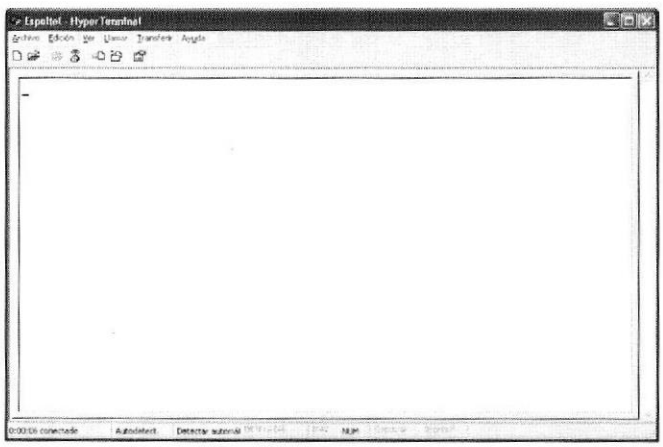


Figura 5.16 Pantalla de Hyper Terminal con conexión a router.

- Cuando se da clic en cerrar o en salir aparecerá la siguiente pantalla de confirmación para desconexión del dispositivo.

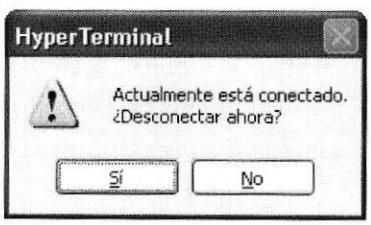


Figura 5.17 Pantalla para confirmar la desconexión del Hyper Terminal

- Si da clic en **Sí** aparecerá otra pantalla de confirmación para guardar los cambios.

- Si da clic en **No** regresará o si la opción escogida es **Cancelar** a la pantalla de configuraciones.

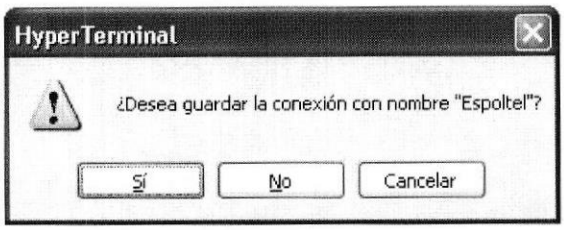


Figura 5.18 Pantalla para guardar la conexión creada

5.1.6 CONECTAR UN ROUTER A OTRO ROUTER.

5.1.6.1 REQUERIMIENTOS.

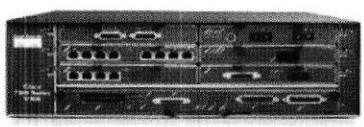
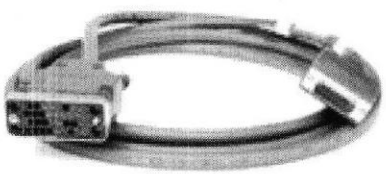
Imagen	Equipo
	Dos Router
	Cable DCE
	Cable DTE

Tabla 5.2 Requerimientos para conectar dos router.

5.1.6.2 CONECCIÓN DE CABLES.

Siga estos pasos para conectar dos router entre sí:

- Identifique el conector DCE y DTE de cada cable serial. (Figura 5.21).

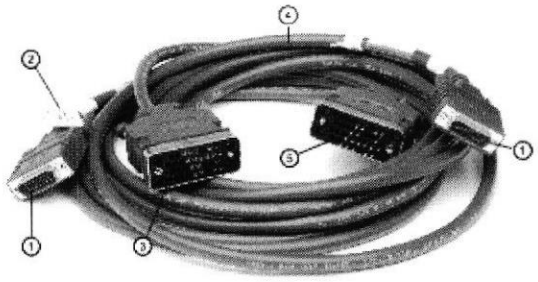


Figura 5.19 Componentes de los cables seriales.

1 Conector serial del Router	Conectado al Puerto serial del router.
2 Etiqueta	Información Provista acerca del cable.
3 Conector DCE DB-60	Es provisto con una interfaz para conectar el DTE.
5 Conector DTE DB-60	Conector que se une al del DCE.

- Conecte el extremo de los cables seriales DCE con DTE de manera que se forme un solo cable. (Figura 5.22).

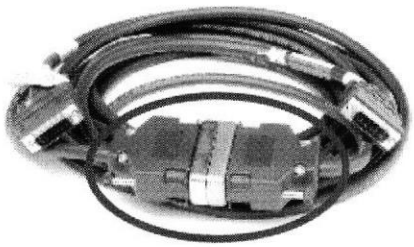


Figura 5.20 Cables seriales listos para conectarse a los routers.

- Identifique las interfaces seriales de cada router, por lo general se encuentran en la parte delantera del router.

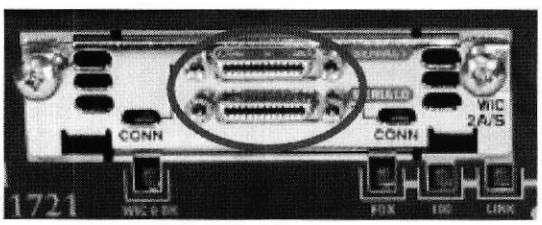


Figura 5.21 Vista frontal del router.

- Conecte los extremos de los cables a una de las interfaces seriales de cada router, de modo que quede un extremo conectado a un router y el otro extremo en el otro router.

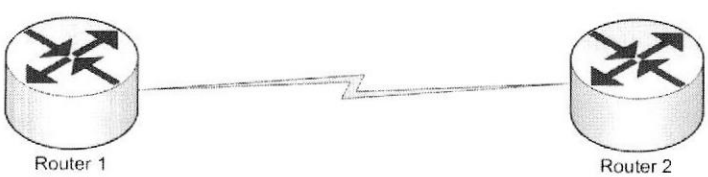


Figura 5.22 Esquema de conexión entre router.

5.1.7 MODOS DE INTERFAZ DE USUARIO.

La interfaz de línea de comando (CLI) de Cisco usa una estructura jerárquica, la misma que requiere el ingreso a distintos modos para realizar tareas particulares. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces. Desde el modo de configuración de interfaces, todo cambio de configuración que se realice, tendrá efecto únicamente en esa interfaz en particular.

Como característica de seguridad, el software Cisco IOS divide las sesiones EXEC en dos niveles de acceso, que son el modo EXEC usuario y el modo EXEC privilegiado, denominado también modo enable.

5.1.7.1 CARACTERÍSTICAS DEL MODO EXEC USUARIO.

El modo EXEC usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo "de visualización solamente". El nivel EXEC usuario no permite ningún comando que pueda cambiar la configuración del router. El modo EXEC usuario se puede reconocer por la petición de entrada: ">".

5.1.7.2 CARACTERÍSTICAS DEL MODO EXEC PRIVILEGIADO.

El modo EXEC privilegiado da acceso a todos los comandos del router. Se puede configurar este modo para que solicite una contraseña del usuario antes de dar acceso. Para ingresar al modo de configuración global y a todos los demás modos específicos, es necesario encontrarse en el modo EXEC privilegiado. El modo EXEC privilegiado se puede reconocer por la petición de entrada "#".

Para ingresar al nivel EXEC privilegiado desde el nivel EXEC usuario, ejecute el comando enable con la petición de entrada ">" en pantalla. Si se ha configurado una contraseña, el router solicitará la contraseña. Por razones de seguridad, los dispositivos de red de Cisco no muestran la contraseña al ser introducida. Una vez que se ha introducido la contraseña correcta, la petición de entrada del router cambia a "#", lo que indica que el usuario se encuentra ahora en el nivel EXEC privilegiado. Si se introduce un signo de interrogación (?) en el nivel EXEC privilegiado, se mostrarán muchas opciones de comando, adicionales a las disponibles en el nivel EXEC usuario.

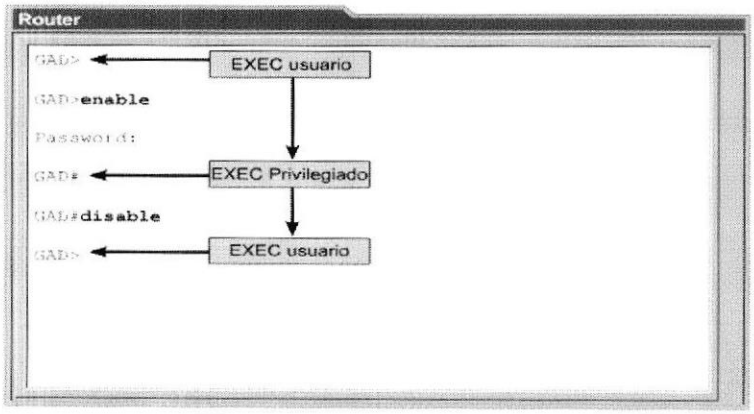


Figura 5.23 Cambio de modo Exec usuario a Exec Privilegiado.

Sólo se puede ingresar al modo de configuración global desde el modo EXEC privilegiado. A continuación los modos específicos a los que se tienen acceso desde el modo de configuración global:

- Interfaces
- Subinterfaces
- Línea
- Router
- Mapas de enrutamiento

Para regresar al modo EXEC usuario desde el modo EXEC privilegiado, se pueden ejecutar los comandos **disable** o **exit**.

Para regresar al modo EXEC privilegiado desde el modo de configuración global, ejecute **exit** o **Control-Z**.

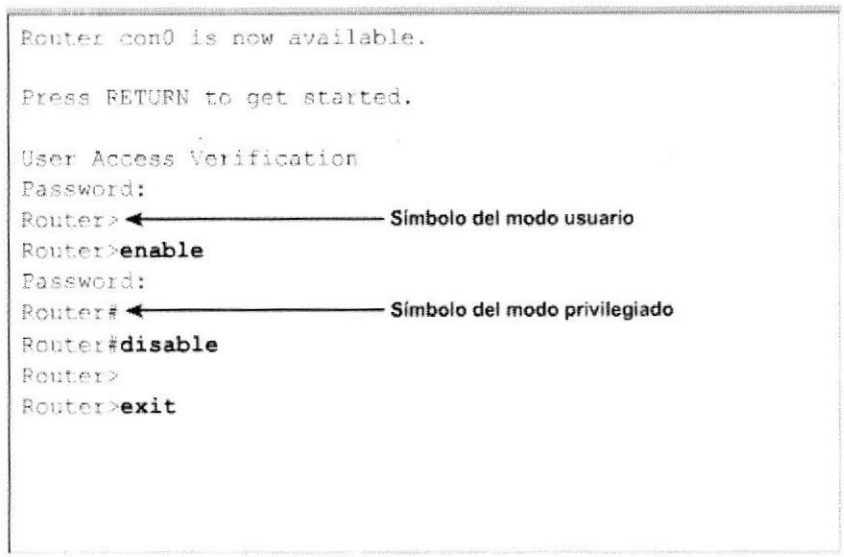


Figura 5.24 Símbolo de modo Exec Privilegiado y usuario.

Al utilizar **exit** desde alguno de estos modos de configuración específicos, el router regresa al modo de configuración global. Al presionar **Control-Z**, se sale por completo del modo de configuración y el router vuelve al modo EXEC privilegiado.

5.1.8 ASIGNAR NOMBRE AL ROUTER.

Antes de empezar la configuración de un router se debe establecer un nombre para el mismo, esta tarea se la realiza desde el modo de configuración global.

```
Router(config)#hostname Peñas
Peñas(config)#
```

Una vez presionada la tecla **Enter**, la petición de entrada ya no mostrará el nombre de host por defecto ('Router'), sino el nombre de host que se acaba de asignar, 'Peñas'

5.1.9 ASIGNAR CONTRASEÑAS AL ROUTER.

Las contraseñas sirven para restringir el acceso a los routers, estas deben configurarse para las líneas de terminales virtuales (line vty), para habilitar el acceso remoto de usuarios al router mediante Telnet. Normalmente y para la línea de consola (line console).

Aunque es opcional, se recomienda configurar una contraseña para la línea de comando.

Router(config)#**line console 0**
Router(config-line)#**password** <*password*>
Router(config-line)#**login**

Los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY.

Se suele usar la misma contraseña para todas las líneas, pero a veces se reserva una línea mediante una contraseña exclusiva, para que sea posible el acceso al router aunque haya demanda de más de cuatro conexiones.

Router(config)#**line vty 0 4**
Router(config-line)#**password** <*password*>
Router(config-line)#**login**

Los comandos **enable password** y **enable secret** (contraseña encriptada) se utilizan para restringir el acceso al modo EXEC privilegiado. El comando **enable password** se utiliza sólo si no se ha configurado previamente **enable secret**.

Router(config)#**enable password**<*password*>
Router(config)#**enable secret**<*password*>

En ocasiones es deseable evitar que las contraseñas se muestren en texto sin cifrar al ejecutar los comandos **show running-config** o **show startup-config**. Por tal razón se usa el comando service password-encryption para cifrar las contraseñas al mostrar los datos de configuración.

Router(config)#**service password-encryption**

El comando **service password-encryption** aplica un cifrado débil a todas las contraseñas sin cifrar. El comando **enable secret <password>** usa un fuerte algoritmo MD5 para cifrar.

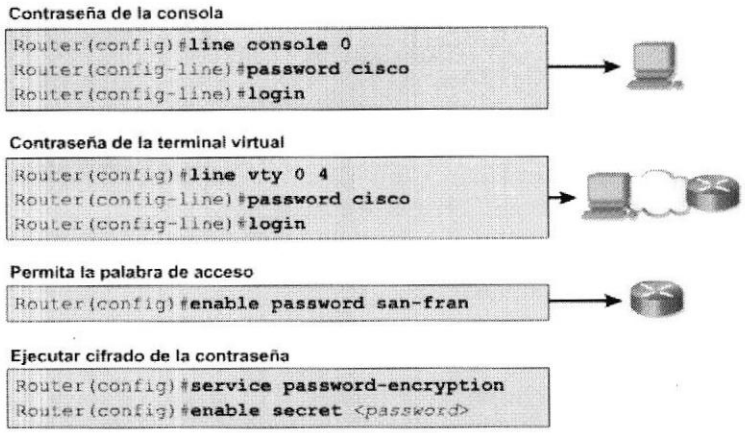


Figura 5.25 Configuración de contraseñas.

5.1.10 COMANDO DE AYUDA MEDIANTE TECLADO.

Al escribir un signo de interrogación (?) en la petición de entrada del modo usuario o del modo privilegiado, aparece una útil lista de los comandos disponibles.

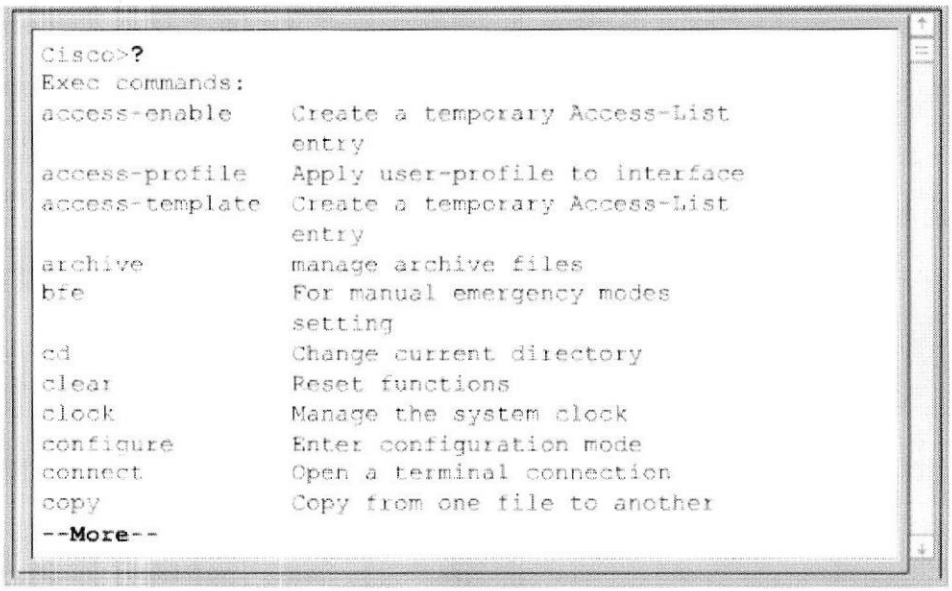


Figura 5.26 Ayuda mediante el teclado.

Es decir, que cuando no se conoce el comando adecuado a utilizar se puede usar el signo **?** para listar por pantalla los comandos con su respectiva sintaxis que el modo en uso contiene.

5.1.11 DIAGNÓSTICO DE FALLAS DE LOS ERRORES DE LÍNEA DE COMANDOS.

Los errores de línea de comandos se producen principalmente debido a errores de tecleado. Si un comando es escrito de forma incorrecta, la interfaz del usuario muestra el error mediante un indicador de error (^). El símbolo "^"aparece en el punto de la

cadena del comando donde este se introdujo, palabra clave o argumento incorrecto. El indicador de ubicación del error y el sistema de ayuda interactiva permiten al usuario localizar y corregir fácilmente los errores de sintaxis.

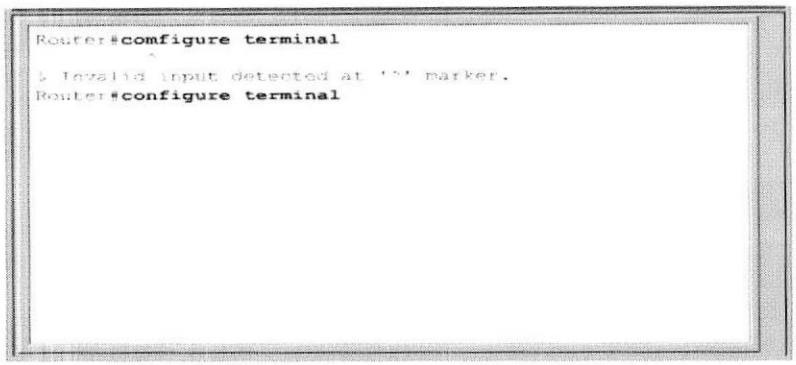


Figura 5.27 Errores de líneas de comando.

Si una línea de comando es escrita de forma incorrecta y se presiona la tecla Intro, se puede presionar la tecla flecha-arriba para reescribir el último comando. Use las teclas flecha-derecha e izquierda para mover el cursor hasta el lugar donde se cometió el error. Luego escriba la corrección necesaria. Si es necesario eliminar algo, use la tecla retroceso.

5.1.12 COMANDOS SHOW.

Los numerosos comandos **show** se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas. Tanto en el modo privilegiado como en el modo de usuario.

- **show interfaces:** Muestra las estadísticas completas de todas las interfaces del router. Para ver las estadísticas de una interfaz específica, ejecute el comando show interfaces seguido de la interfaz específica y el número de puerto.

- **show controllers serial:** muestra información específica de la interface de hardware. El comando debe incluir el número de puerto y/o de ranura de la interfaz.

- **show clock:** Muestra la hora fijada en el router.

- **show hosts:** Muestra la lista en caché de los nombres de host y sus direcciones.

- **show users:** Muestra todos los usuarios conectados al router.

- **show history:** Muestra un historial de los comandos ingresados.

- **show flash:** Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí.

- **show version:** Despliega la información acerca del router y de la imagen de IOS que esté corriendo en al RAM. Este comando también muestra el valor del registro de configuración del router.

- **show ARP:** Muestra la tabla ARP del router.
- **show protocols:** Muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.
- **show startup-configuration:** Muestra el archivo de configuración almacenado en la NVRAM.
- **show running-configuration:** Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

5.1.13 CONFIGURACIÓN DE UNA INTERFAZ SERIAL.

Es posible configurar una interfaz serial desde la consola o a través de una línea de terminal virtual.

- Ingrese al modo de configuración global.
- Ingrese al modo de configuración de interfaz.
- Especifique la dirección de la interfaz y la máscara de subred.
- Si el cable de conexión es DCE, fije la velocidad de sincronización. Omita este paso si el cable es DTE.
- Active la interfaz.

A cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP. Configure la dirección de IP mediante los siguientes comandos:

Router(config)#**interface serial 0/0**
Router(config-if)#**ip address** <*ip address*> <*netmask*>

Los routers Cisco pueden usar diferentes conectores para las interfaces seriales. La interfaz de la izquierda es una interfaz serial inteligente. La interfaz de la derecha es una conexión DB-60. Esto hace que la selección del cable serial que conecta el sistema de la red a los dispositivos seriales sea una parte fundamental de la configuración de una WAN.

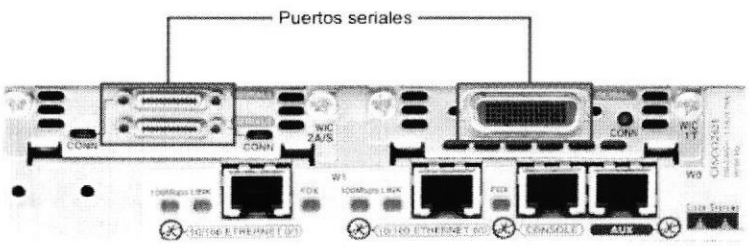


Figura 5.28 Puertos seriales.

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

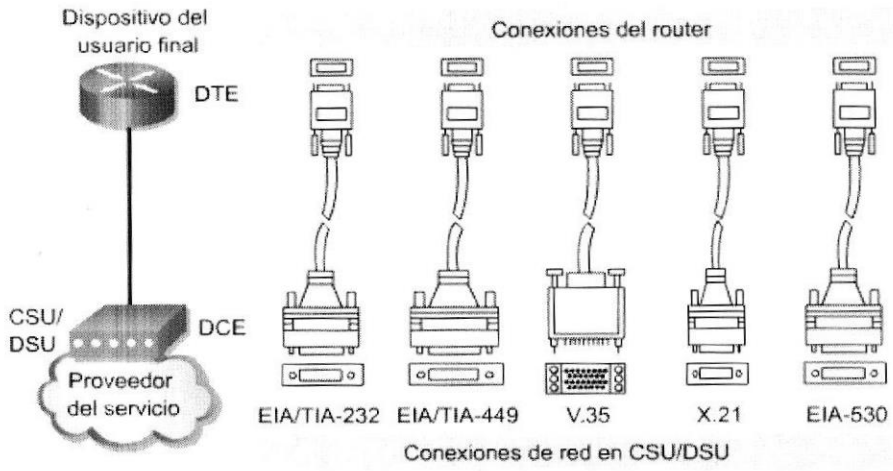


Figura 5.29 Conectores DCE y DTE.

- Cada dispositivo podría requerir un estándar serial diferente. Cada estándar define las señales del cable y especifica el conector del extremo del cable. Siempre se debe consultar la documentación del dispositivo para obtener información sobre el estándar de señalización.

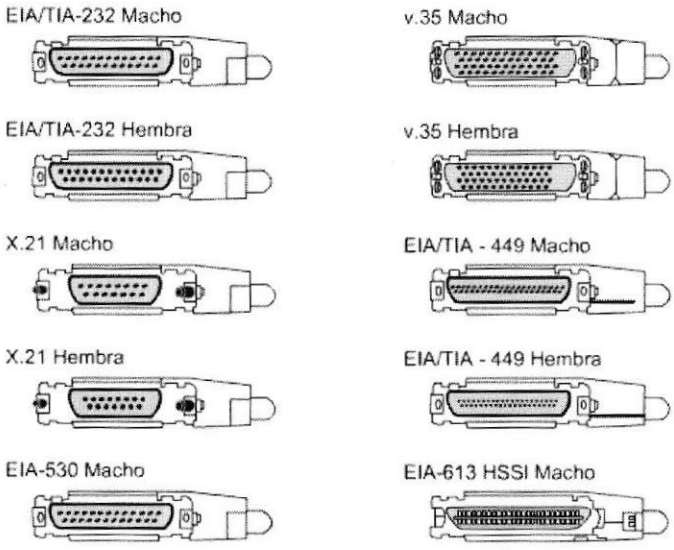


Figura 5.30 Conectores hembras y machos.

- Si el conector tiene ping salientes visibles, es macho. Si el conector tiene tomas para los ping salientes, es hembra.

En los enlaces seriales interconectados directamente, un extremo debe considerarse como un DCE y debe proporcionar la señal de sincronización. Se activa la sincronización y se fija la velocidad mediante el comando **clock rate**. Las velocidades de sincronización disponibles (en bits por segundo) son: 56000, 64000, 72000, etc... No obstante, es posible que algunas de estas velocidades no estén disponibles en algunas interfaces seriales, según su capacidad.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando **no shutdown**. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o de diagnóstico de fallas, se utiliza el comando **shutdown** para desactivarla.

Router(config)#**interface serial 0/0**
Router(config-if)#**clock rate 64000**
Router(config-if)#**no shutdown**

5.1.14 CONFIGURACIÓN DE UNA INTERFAZ ETHERNET.

Se puede configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual.

- Ingrese al modo de configuración global.
- Ingrese al modo de configuración de interfaz.
- Especifique la dirección de la interfaz y la máscara de subred.
- Active la interfaz.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ejecuta el comando **no shutdown**. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o diagnóstico de fallas, se utiliza el comando **shutdown** para desactivarla.

Router(config)#**interface ethernet 0**
Router(config-if)#**ip address 192.168.12.1 255.255.255.224**
Router(config-if)#**no shutdown**

5.1.15 DESCRIPCIÓN DE INTERFACES.

La descripción de las interfaces se emplea para indicar información importante, como puede ser la relativa a un router distante, el número de un circuito, o un segmento de red específico.

Router#**configure terminal**
Router(config)#**interface ethernet 0**
Router(config-if)#**ip address 192.168.12.1 255.255.255.224**
Router(config-if)# **description Lab_1**
Router(config-if)#**no shutdown**

5.1.16 CONFIGURACIÓN DEL MENSAJE DEL DÍA (MOTD).

Se puede configurar un mensaje del día (MOTD), para que sea mostrado en todas las terminales conectadas.

Ingrese al modo de configuración global para configurar un texto como mensaje del día (MOTD). Use el comando **banner motd**, seguido de un espacio y un delimitador, como por ejemplo el signo numeral (#).

Router#**configure terminal**
Router# **banner motd# No realizar cambios #.**
Router# **copy running-config startup-config**

5.1.17 CONFIGURACIÓN DE TABLAS DE HOST.

Para asignar nombres de host a direcciones, primero ingrese al modo de configuración global. Ejecute el comando **ip host** seguido del nombre de destino y todas las direcciones de IP con las que se puede llegar al dispositivo. Esto ayudará a acceder a un router por nombre y no siempre por dirección ip.

Router#**configure terminal**
Router(config)#**ip host PEÑAS 192.168.12.1**
Router(config)#**exit**
Router# **copy running-config startup-config**

5.1.18 TIPO DE ENRUTAMIENTO.

- Enrutamiento estático.
- Enrutamiento por defecto.
- Enrutamiento dinámico.

5.1.18.1 ENRUTAMIENTO ESTÁTICO.

Las operaciones con rutas estáticas pueden dividirse en tres partes:

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

Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando **ip route**, seguido de la dirección de red, máscara respectiva e interfaz saliente.

Router(config)#ip route 192.168.12.0 255.255.255.0 s0

La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. Un valor menor de distancia administrativa indica una ruta más confiable. La distancia administrativa por defecto cuando se usa una ruta estática es 1.

5.1.18.2 ENRUTAMIENTO POR DEFECTO.

Las rutas por defecto se usan para enviar paquetes a destinos que no coinciden con los de ninguna de las otras rutas en la tabla de enrutamiento. Generalmente, se las usa para el tráfico que se dirige a la Internet, ya que a menudo resulta poco práctico e innecesario mantener rutas hacia todas las redes de la Internet.

Router#**configure terminal**
Router(config)# **ip route 0.0.0.0 0.0.0.0 s0**
Router(config)# **exit**
Router# **copy running-config startup-config**

5.1.18.3 ENRUTAMIENTO DINÁMICO.

El enrutamiento dinámico significa que el router va averiguando las rutas para llegar al destino por medio de actualizaciones periódicas enviadas desde otros routers.

5.1.19 INTRODUCCIÓN A PROTOCOLOS DE ENRUTAMIENTO.

Los protocolos de enrutamiento son diferentes a los protocolos enrutados tanto en su función como en su tarea.

Un protocolo de enrutamiento es el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.

Ejemplos de protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP).
- Protocolo de enrutamiento de gateway interior (IGRP).
- Protocolo de enrutamiento de gateway interior mejorado (EIGRP).
- Protocolo "Primero la ruta más corta" (OSPF).
- Protocolo de enrutamiento exterior por vector-distancia(BGP).

Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

Ejemplos de protocolos enrutados:

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

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de

datos. Cuando todos los routers de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia.

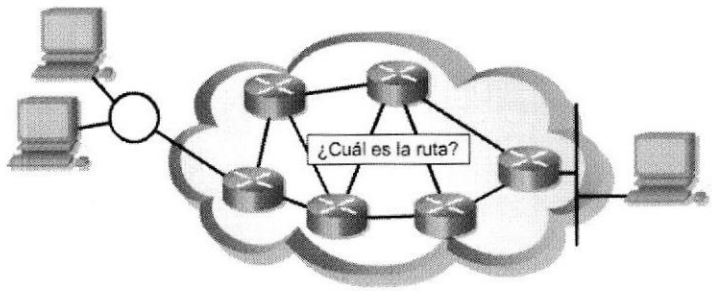


Figura 5.31 Determinación de rutas.

5.1.19.1 IGRP PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY.

Características:

- Es un protocolo de enrutamiento por vector-distancia.
- Se considera el ancho de banda, la carga, el retardo y la confiabilidad para crear una métrica compuesta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

5.1.19.2 EIGRP PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY MEJORADO.

Características:

- Es un protocolo mejorado de enrutamiento por vector-distancia.
- Utiliza balanceo de carga asimétrico.
- Utiliza una combinación de los algoritmos de vector-distancia y de estado del enlace.
- Utiliza el Algoritmo de actualización difusa (DUAL) para el cálculo de la ruta más corta.
- Las actualizaciones son mensajes de multicast a la dirección 224.0.0.10 generadas por cambios en la topología.

5.1.19.3 PROTOCOLO DE ENRUTAMIENTO POR VECTOR – DISTANCIA (RIP).

Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro. Estas actualizaciones periódicas entre routers informan de los cambios de topología. Los algoritmos de vector-distancia no permiten que un router conozca la topología exacta de una red, ya que cada router solo ve a sus routers vecinos.

Las actualizaciones de las tablas de enrutamiento se producen al haber cambios en la topología. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada una de las redes indicadas en la tabla.

La habilitación del enrutamiento de paquetes de IP, requiere fijar parámetros tanto globales como de enrutamiento. Las tareas globales incluyen la selección de un protocolo de enrutamiento, por ejemplo: RIP, IGRP, EIGRP o OSPF. La tarea principal del modo configuración de enrutamiento es indicar los números IP de la red. El enrutamiento dinámico utiliza comunicaciones broadcast y multicast con los otros routers. La métrica de enrutamiento ayuda a los routers a encontrar la mejor ruta hacia cada red o subred.

5.1.19.3.1 CARACTERÍSTICAS DEL PROTOCOLO RIP.

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete es desechado.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

5.1.19.3.2 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP.

El Protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento por vector-distancia, este protocolo se base en estándares abiertos y que sea de fácil implementación. Aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados.

RIP ha evolucionado desde el Protocolo de enrutamiento con definición de clases, RIP Versión 1 (RIP v1), hasta el Protocolo de enrutamiento sin clase, RIP Version 2 (RIP v2).

El comando **router** inicia el proceso de enrutamiento.

El comando **network** es necesario, ya que permite que el proceso de enrutamiento determine cuáles son las interfaces que participan en el envío y la recepción de las actualizaciones de enrutamiento.

router(config)#**router rip**
router(config-router)#**network 192.168.10.0**

5.1.19.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2.

Capacidad para transportar mayor información relativa al enrutamiento de paquetes. Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de las tablas. Soporta enmáscaramiento de subredes de longitud variable (VLSM).

router#**configure terminal**
router(config)#**router rip**
router(config-router)#**version 2**
router(config-router)#**network 192.168.10.0**

Entre las tareas opcionales se encuentran:

- Aplicar compensaciones a la métrica de enrutamiento.
- Ajustar los temporizadores.
- Especificar una versión de RIP.
- Habilitar la autenticación de RIP.
- Configurar el resumen de las rutas en una interfaz.
- Verificar el resumen de las rutas IP.
- Inhabilitar el resumen automático de rutas.

El comando **show ip route** se puede utilizar para verificar que las rutas recibidas por los routers RIP vecinos estén instaladas en la tabla de enrutamiento. Examine el resultado del comando y busque las rutas RIP que señaladas con "R". Recuerde que la red tardará algún tiempo en converger, de modo que puede que no aparezcan las rutas de forma inmediata.

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

Gateway of last resort is not set

192.168.20.0/30 is subnetted, 6 subnets
C 192.168.20.8 is directly connected, Serial0/0
C 192.168.20.4 is directly connected, Serial0/1
C 192.168.20.12 is directly connected, Serial0/2
C 192.168.20.0 is directly connected, Serial0/3
R 192.168.20.32 [120/1] via 192.168.20.14, 00:03:31, Serial0/2
R 192.168.20.36 [120/1] via 192.168.20.6, 00:09:40, Serial0/1

5.1.19.5 PROTOCOLO DE ENRUTAMIENTO ESTADO – ENLACE (OSPF).

Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. El algoritmo de enrutamiento de estado del enlace mantiene información completa sobre routers lejanos y su interconexión.

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). El término "libre" en "Primero la ruta libre más corta" significa que está abierto al público y no es propiedad de ninguna empresa.

OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes. Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento.

OSPF ofrece soluciones a los siguientes problemas:

- Velocidad de convergencia.
- Admite Máscara de subred de longitud variable (VLSM).
- Tamaño de la red.
- Selección de ruta.
- Agrupación de miembros

5.1.19.5.1 CARACTERÍSTICAS DE OSPF.

- Es un protocolo público conocido como "PRIMERO LA RUTA MÁS CORTA"
- Es un protocolo de enrutamiento de estado del enlace.
- Es un protocolo de enrutamiento público (open Standard).
- Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.
- Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

5.1.19.5.2 TIPOS DE RED OSPF.

Las interfaces OSPF reconocen tres tipos de redes:

- Multiacceso de broadcast como por ejemplo Ethernet.

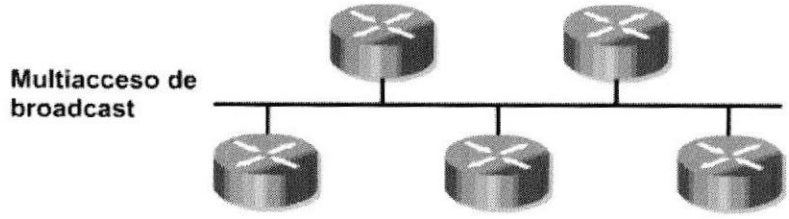


Figura 5.32 Red Ospf con multiacceso de broadcast.

- Redes punto a punto.

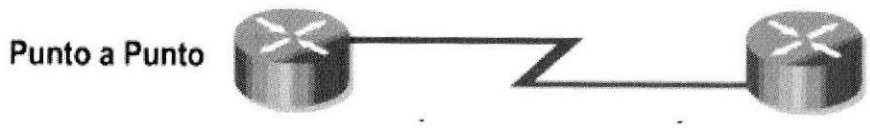


Figura 5.33 Red Ospf punto a punto.

- Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay.

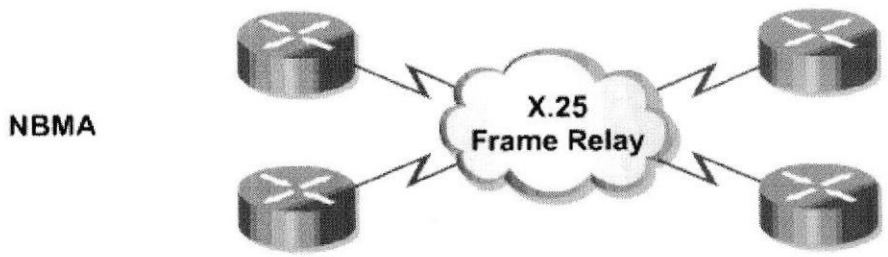


Figura 5.34 Red Ospf con munltiacceso sin broadcast.

5.1.19.5.3 PROTOCOLO HELLO DE OSPF.

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete hello y sigue enviando hellos a intervalos regulares. Las reglas de intercambio de paquetes hello de OSPF se denominan protocolo Hello.

En la capa 3 del modelo OSI, los paquetes hello se direccionan hacia la dirección multicast 224.0.0.5. Esta dirección equivale a "todos los routers OSPF". Los routers OSPF utilizan los paquetes hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los Hellos se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes NBMA, como por ejemplo Frame Relay, el tiempo por defecto es de 30 segundos.

En las redes multiacceso el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR).El paquete hello transmite información para la cual todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

La configuración de OSPF requiere que el proceso de enrutamiento OSPF esté activo en el router con las direcciones de red y la información de área especificadas.

Router(config)#**router ospf** *process-id*

El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en el router. Se pueden iniciar varios procesos OSPF en el mismo router. El número puede tener cualquier valor entre 1 y 65.535.

Se puede habilitar más de un proceso de ejecución de ospf al mismo tiempo en el mismo router si se requiere, este número puede ser el mismo en todos los router sobre la red, o puede ser diferente, esto no importa.

Las redes IP se publican de la siguiente manera en OSPF:

Router(config-router)#**network** *address wildcard-mask* **area** *area-id*

- **Dirección.-**Esta puede ser la dirección de red, subred o de la interfaz. Indica a los routers cuales son los enlaces en los que se deben escuchar publicaciones y que enlaces y redes se deben publicar.

- **Máscara de wildcard.-** Esta es una máscara inversa que se utiliza para determinar como se lee una dirección. La máscara tiene bits wildcard donde 0 representa coincidencia y 1 no es importante.

- **Id de área.-** Este valor indica el área que se debe asociar con una dirección. Puede ser un número o puede ser similar a una dirección ip. Para un área backbone, la id deber ser igual a 0.

  Ejemplo: **area 0**

  Contienen la misma información de red, todos los routers de una misma área se llaman internos, especifica el grupo de nodos o redes contiguos**, base de datos topológica por área**, invisible fuera del área, **reducción del tráfico de ruteo**.

5.1.19.5.4 MODIFICACIÓN DE LA MÉTRICA DE COSTOS DE OSPF.

OSPF utiliza el costo como métrica para determinar la mejor ruta. Un costo se asocia con el lado de salida de cada interfaz de router. Los costos también se asocian con datos de enrutamiento derivados en forma externa. Por lo general, el costo de ruta se calcula mediante la fórmula 10^8/ancho de banda, donde el ancho de banda se expresa en bps.

El ancho de banda por defecto para las interfaces seriales Cisco es 1,544 Mbps o 1544 kbps.

router(config)#**interface serial 0/0**
router(config-if)#**bandwidth 5000**

5.1.19.5.5 VERIFICACIÓN DE CONFIGURACIÓN OSPF.

Para verificar la configuración de OSPF existe una serie de comandos show.

Show ip protocol.-Esto muestra parámetros para temporizadores, filtros, métricas, redes y otra información acerca de todo el router.

Show ip route.- Ésta es una de las mejores maneras para determinar la conectividad entre el router local y el resto de la red.

Show ip ospf interface.- Esto verifica que las interfaces se hayan configurado en la áreas planificadas. Si no se especifica una dirección loopback, la interfaz con la dirección más alta se considera como el ID del router. Además proporciona los intervalos de temporización como el intervalo hello y muestra las adyacencias del router.

Show ip ospf.- Muestra la cantidad de veces en que se ha usado el algoritmo SPF. También muestra el intervalo de actualización de estado de enlace si no se han producido cambios topológicos.

Show ip ospf neighbor detail. - Este muestra un listado detallado de vecinos, sus prioridades y estados.

Show ip ospf database.- Esto muestra el contenido de la base de datos topológica que mantiene el router y el ID del proceso OSPF.

5.1.20 FIREWALLS.

Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos. En la mayoría de los casos, los intrusos provienen de la Internet mundial y de las miles de redes remotas que interconecta. Normalmente, un firewall de red se compone de varias máquinas diferentes que funcionan al mismo tiempo para impedir el acceso no deseado e ilegal.

Se deben utilizar ACL en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet. Esto permite el control del tráfico entrante o saliente de alguna parte específica de la red interna. El router firewall proporciona aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada.

Se necesita configurar las ACL en routers fronterizos, para brindar mayor seguridad. Esto proporciona protección básica contra la red externa u otra parte menos controlada de la red, en un área más privada de la red. En estos routers fronterizos, es posible crear ACLs para cada protocolo de red configurado en las interfaces del router.

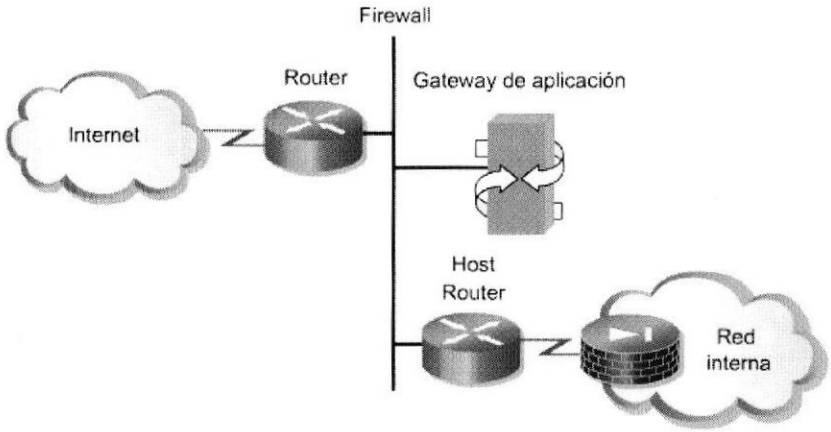


Figura 5.35 Funcionamiento de un Firewall.

5.1.20.1 LISTAS DE CONTROL DE ACCESO (ACL).

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos.

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACLs).

Una ACL es una lista secuencial de sentencias de permiso o rechazo, que se aplican a direcciones o protocolos de capa superior.

Las ACL pueden ser tan simples como una sola línea destinada a permitir paquetes desde un host específico o pueden ser un conjunto de reglas y condiciones extremadamente complejas que definan el tráfico de forma precisa y modelen el funcionamiento de los procesos de los routers.

Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX). Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

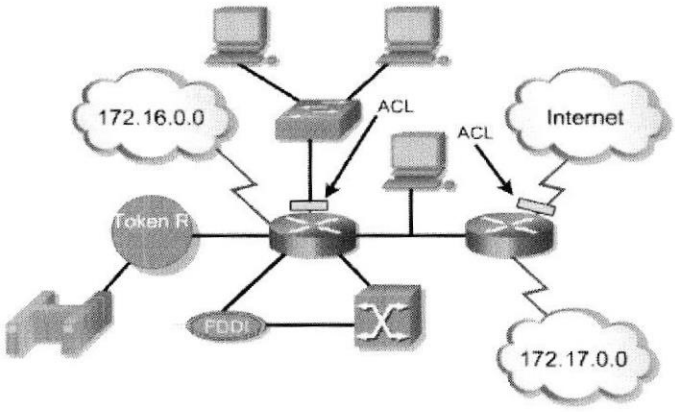


Figura 5.36 Listas de control de acceso.

5.1.20.2 FUNCIONAMIENTO DE LAS ACL.

El orden en el que se ubican las sentencias de la ACL es importante. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo. Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

5.1.20.3 CREACIÓN DE LAS ACL.

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

Cuando configure las ACL en el router, cada ACL debe identificarse de forma única, asignándole un número. Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista.

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

router#**configure terminal**
router(config)#**access-list 1 deny 172.20.12.1**
router(config)#**access-list 1 permit 172.20.12.0 0.0.0.255**
router(config)#**access-list 1 deny 172.20.0.0 0.0.255.255**
router(config)#**access-list 1 permit 172.0.0.0**
router(config)#**interface eth0**
router(config-if)#**ip access-group 2 in**

Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando **no access-list** seguido del número de la acl.

router(config)#**no access-list 1**

5.1.20.4 VERIFICACIÓN DE LAS ACL.

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

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Figura 5.37 Pantalla de verificación de la existencia de una acl.

5.1.20.5 ACL ESTÁNDAR.

Las ACL estándar se colocan cerca del destino del tráfico. Esto se debe a sus limitaciones: no se puede distinguir el destino. Usan los números de lista de acceso desde 1 - 99 y de la 1300 - 1999, su sintaxis es:

router(config)# **access-list** *access-list-number* {deny | permit | remark} source [*source-wildcard*] [**log**]

El uso de **remark** facilita el entendimiento de la lista de acceso. Cada **remark** está limitado a 100 caracteres. Por ejemplo, no es suficientemente claro cual es el propósito del siguiente comando: **access-list 1 permit 192.1.89.15.15**. Es mucho más fácil leer un comentario acerca de un comando para entender sus efectos, así como sigue:

access-list 1 remark Permit only karix workstation through
access-list 1 permit 192.168.15.1

La forma **no** de este comando se utiliza para eliminar una ACL estándar.

Router(config)#**no access-list***access-list-number*

El comando **ip access-group** relaciona una ACL existente a una interface:

Router(config)#**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

5.1.20.6 ACL EXTENDIDAS.

Las ACL extendidas se colocan cerca del origen del tráfico, por eficiencia - es decir, para evitar tráfico innecesario en el resto de la red. Utilizan el número de lista de acceso desde la 100 a la 199 y desde la 2000 a la 2699.

El comando **ip access-group** enlaza una ACL extendida existente a una interfaz. Recuerde que sólo se permite una ACL por interfaz por protocolo por dirección.

El formato del comando es:

router(config)#**interface eth1**
router(config-if)#**ip access-group 110 in**
router(config-if)#**exit**
router(config)#

5.1.20.7 UBICACIÓN DE LAS ACL.

Las ACL se utilizan para controlar el tráfico, filtrando paquetes y eliminando el tráfico no deseado de la red. Otra consideración importante a tener en cuenta al implementar la ACL es dónde se ubica la lista de acceso. Si las ACL se colocan en el lugar correcto, no sólo es posible filtrar el tráfico sino también toda la red se hace más eficiente. Si se tiene que filtrar el tráfico, la ACL se debe colocar en un lugar donde mejore la eficiencia de forma significativa.

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican las direcciones destino, de modo que se deben colocar lo más cerca posible del destino. Por ejemplo, una ACL estándar se debe colocar en Fa0/0 del Router D para evitar el tráfico desde el Router A.

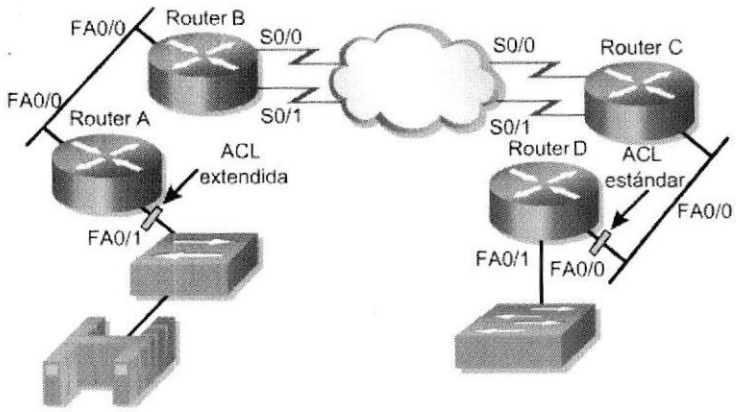


Figura 5.38 Ubicación de las ACL

5.1.21 GUARDANDO LA CONFIGURACIÓN.

Los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando **copy running-config startup-config** o abreviado **wr.**

Salinas(config-if)# copy running-config startup-config

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **startup-config** se almacena en memoria **NVRAM**, así, si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria **NVRAM (startup-config).**

5.2 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). Además 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).

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, pero 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.

5.2.1 CARACTERÍSTICAS.

- Existen administrables y no administrables
- No comparten velocidad de transmisión.
- El switch no administrable reemplazo al hub.
- Comunicación punto a punto.
- No existen colisiones.
- Los switches de capa 2 centran su administración en direcciones mac y los de capa 3 en direcciones ip.
- El ancho de banda no es compartido.
- Permite reducir el dominio de broadcast
- Controlan broadcast.
- No se puede hacer cascada en más de 8 switch.
- Existen switch con puerto de fibra.
- 10/100/1000 mbps.
- Existen switch:

ethernet	10
fast ethernet	100
gigabit ethernet	1000

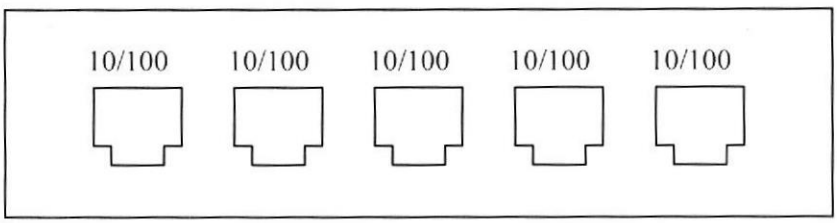


Figura 5.39 Vista frontal de un switch no administrable.

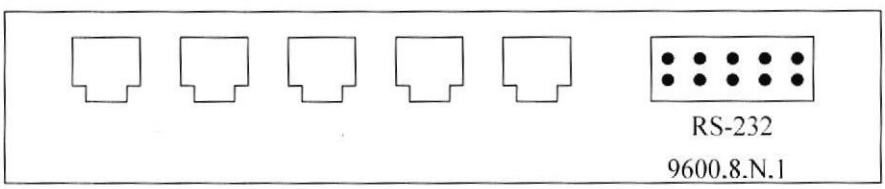


Figura 5.40 Vista frontal de un switch administrable.

5.2.2 NIVELES DE TRANSMISIÓN.

- Store and fordward
- Fragment free
- Cut trough

Por método de almacenamiento y envío (store-and-forward):

- Se recibe la trama entera antes de reenviarla.
- Latencia mayor.
- Se aplican filtros.

- Detección de errores.

Libre de fragmentos (fragment-free):

- Filtra los fragmentos de colisión.
- Después de 64 bytes, se considera válido.

Por método de corte (cut-through):

- Sólo se lee la dirección de destino de la trama.
- Latencia menor.
- Sin detección de errores.

5.2.3 TECNOLOGÍA STACK O STACKEABLE.

Permite administrar diferentes dispositivos fisicos con un solo dispositivo lógico. Tecnología con fines administrables.

5.2.4 TRUNKING PORT.

Permite disminuir el nivel de congestionamiento entre 2 dispositivos de comunicación.

Requerimientos: Es necesario que todos los switches sean truncados.
Fuente redundante: Si la fuente principal cae se activa la secundaria.

5.2.5 MODOS DE COMANDOS DEL SWITCH.

EXEC de usuario:

- Indicador: >
- Cambia parámetros de terminal.
- Pruebas básicas.
- Mostrar información de sistema.

EXEC privilegiado:

- Indicador: #
- Entrar a él con >enable.
- #configure nos lleva a otros modos de configuración.

5.2.6 CONFIGURACIÓN DE UN SWITCH.

5.2.6.1 INTRODUCCIÓN A LAS VLANS.

- Son grupos de servicios de red restringidos según puertos de switch o segmento.

- Son grupos de servicios de red restringidos según puertos de switch o segmento. Se configuran por software, para evitar movimientos físicos. Segmentan redes conmutadas lógicamente.

5.2.6.2 FUNCIONAMIENTO DE UNA VLAN.

Cuando un host se conecta a un puerto de una VLAN, se añade a esa VLAN. Se deben reasignar los puertos de la VLAN debido a que por defecto, están en la VLAN1.

La administración de una VLAN de puerto central sólo está sujeta a la configuración de los puertos, con lo que no hay que montar ni vigilar complejas bases de datos de VLAN. Tanto si la VLAN es dinámica como estática, el administrador debe configurarla.

5.2.6.3 VENTAJAS DE LAS VLANS.

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad.

5.2.6.4 CONFIGURACIÓN DE UNA VLAN.

Creación:

#vlan database
(vlan)#vlan número_de_VLAN

Añadir un puerto a una VLAN:

interface número_de_interfaz
(config-if)#switchport access VLAN número_de_VLAN.

Verificación:

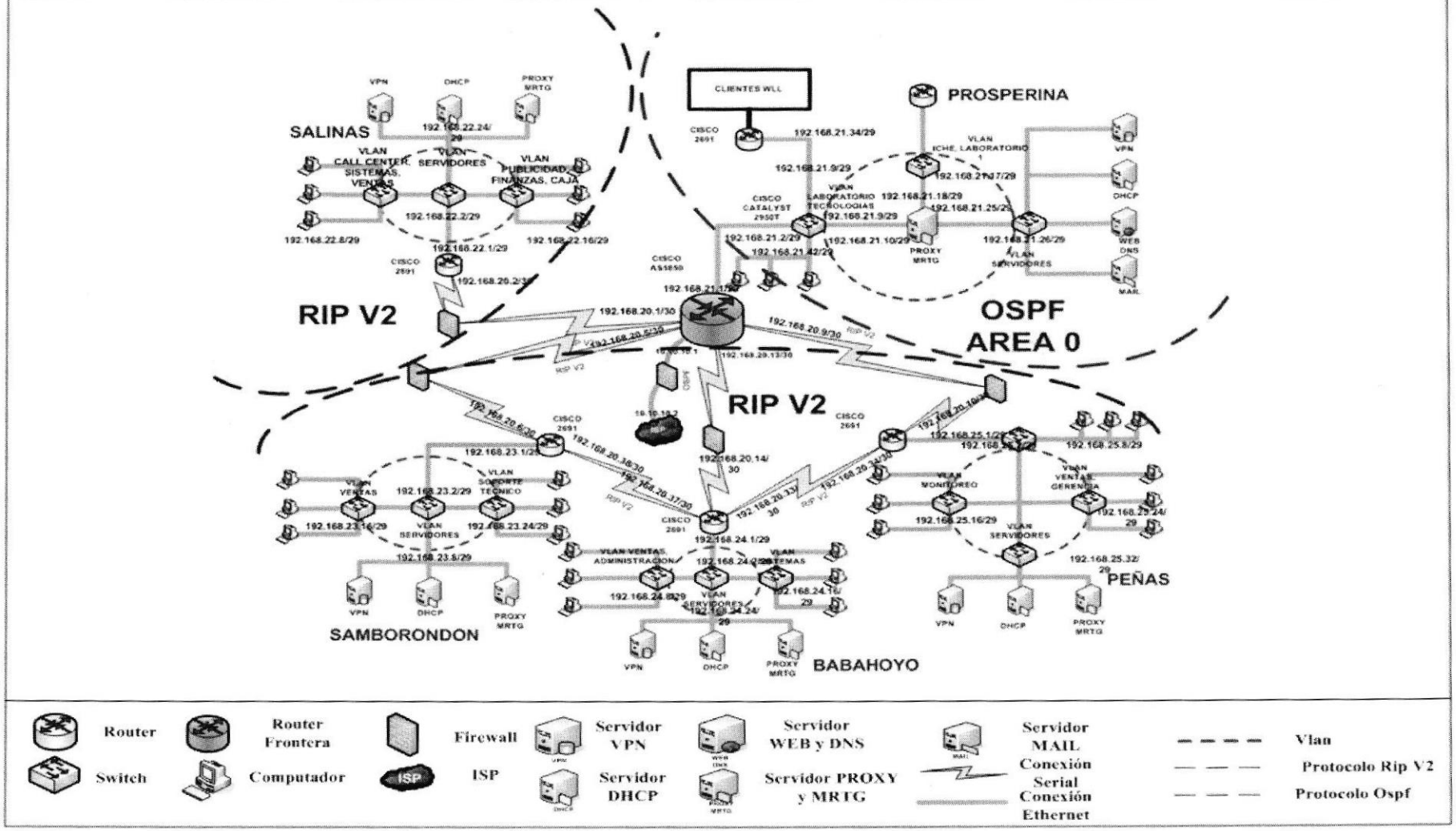
show vlan: muestra características de todas las VLAN

5.2.7 IMPLEMENTACIÓN.

Según la topología que encontramos en el estudio de la situación actual del proveedor de Internet Espoltel, se elaboró un nuevo diseñó de su comunicación Wan..

En este gráfico consta cada uno de los segmentos utilizados en los enlaces wan, la segmentación respectiva por cada sucursal y las vlan creadas para reducir el domino de broadcast.

DIAGRAMA DE DISPOSITIVOS WAN - ESPOLTEL



5.3 CONFIGURACIÓN DE ROUTERS.

5.3.1 CONFIGURACIÓN DEL ROUTER PROSPERINA.

5.3.1.1 ASIGNAR NOMBRE.

Router>**enable**

A nivel del modo usuario normal, se debe digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

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

Aparecerá un mensaje que le indica al usuario que debe ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname PROSPERINA**

En el modo de configuración general, digitar el comando anterior y a continuación un nombre para el dispositivo.

5.3.1.2 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

Para poder habilitar el acceso por consola y por terminal virtual, se debe entrar primeramente al modo de usuario privilegiado.

PROSPERINA(config)#**line vty 0 4**

Entrar al modo de configuración del acceso por terminal virtual.

PROSPERINA(config -line)#**password cisco**

Se debe ingresar la contraseña.

PROSPERINA(config -line)#**login**

Activar el inicio con contraseña.

PROSPERINA(config -line)#**exit**

Se debe salir de la configuración de la terminal virtual, para poder configurar el acceso a consola.

PROSPERINA(config)#**line console 0**

Habilita el acceso por consola.

PROSPERINA(config -line)#**password cisco**

Se debe ingresar la contraseña.

PROSPERINA(config -line)#**login**

Activar el inicio con contraseña.

Con el mismo procedimiento puede configurarse una password para acceder por el puerto auxiliar. Tanto el puerto de consola como el auxiliar, no requieren autenticación de password por defecto.

5.3.1.3 CONFIGURACIÓN DE INTERFACES SERIALES.

Para poder configurar una interfaz serial, se debe entrar primeramente al modo de usuario privilegiado.

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

Digite el comando anterior para entrar al modo de configuración de la interfaz serial 0/0.

PROSPERINA(config-if)#**description CONEXIÓN AL ROUTER PENAS**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

PROSPERINA(config-if)#**ip address** 192.168.20.9 255.255.255.252

Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

PROSPERINA(config-if)#**clock rate 56000**

Digite el comando anterior para indicar la velocidad del puerto en bps. Se necesita incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación. Figura 5.32.

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

Se debe ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparece el siguiente mensaje el cual realiza un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down,** quiere decir que existe algún tipo de problema en el enlace.

%LINEPROTO-5-UPDOWN: Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

PROSPERINA(config-if)#**interface serial 0/1**

Digite el comando anterior para ingresar al modo de configuración de la interfaz serial 0/1.

PROSPERINA(config-if)#**description CONEXIÓN AL ROUTER SAMBORONDON**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description**.

PROSPERINA(config-if)#**ip address** 192.168.20.5 255.255.255.252

Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

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

Se debe ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparece el siguiente mensaje el cual realiza un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down,** quiere decir que existe algún tipo de problema en el enlace.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/1, changed state to up
%LINK -3-UPDOWN: Interface serial0/1, changed state to up

PROSPERINA(config-if)#**interface serial 0/2**

Digite el comando anterior para configurar la interfaz serial 0/2.

PROSPERINA(config-if)#**description CONEXIÓN AL ROUTER BABAHOYO**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description**.

PROSPERINA(config-if)#**ip address** 192.168.20.13 255.255.255.252

Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

PROSPERINA(config-if)#**clock rate 56000**

Digite el comando anterior para indicar la velocidad del puerto en bps. Se necesita incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación. Figura 5.32.

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

Se debe ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparece el siguiente mensaje el cual realiza un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down,** quiere decir que existe algún tipo de problema en el enlace.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/2, changed state to up
%LINK -3-UPDOWN: Interface serial0/2, changed state to up

PROSPERINA(config-if)#**interface serial 0/3**

Digite el comando anterior para configurar la interfaz serial 0/3.

PROSPERINA(config-if)#**description CONEXIÓN AL ROUTER SALINAS**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description**.

PROSPERINA(config-if)#**ip address** 192.168.20.1 255.255.255.252

Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

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

Se debe ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparece el siguiente mensaje el cual realiza un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz **down,** quiere decir que existe algún problema en el enlace.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/3, changed state to up
%LINK -3-UPDOWN: Interface serial0/3, changed state to up

5.3.1.4 CONFIGURACIÓN DE SUB-INTERFACES.

Para poder configurar una sub-interfaz, se debe entrar primeramente al modo de usuario privilegiado.

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

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet1/0.1.

PROSPERINA(config-subif)#**description VLAN POR DEFECTO PROSPERINA**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

PROSPERINA(config-subif)#**encapsulation dot1q 1**

Se debe digitar el comando encapsulation dot1q para definir el tipo de encapsulamiento. Donde uno es el número de vlan.

PROSPERINA(config-subif)#**ip address** 192.168.21.1 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz interfaz.

PROSPERINA(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente el puerto.

PROSPERINA(config-subif)#**interface fastethernet1/0.2**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet1/0.2.

PROSPERINA(config-subif)#**description VLAN LAB_TECNOLOGIAS PROSPERINA**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

PROSPERINA(config-subif)#**encapsulation dot1q 2**

Se debe digitar el comando encapsulation dot1q y el número de la vlan, para definir el tipo de encapsulamiento. Donde dos es el número de la vlan.

PROSPERINA(config-subif)#**ip address** 192.168.21.9 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

PROSPERINA(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente el puerto.

PROSPERINA(config-subif)#**interface fastethernet1/0.3**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet1/0.3.

PROSPERINA(config-subif)#**description VLAN LAB1_ICHE PROSPERINA**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

PROSPERINA(config-subif)#**encapsulation dot1q 3**

Se debe digitar el comando encapsulation dot1q y el número de la vlan, para definir el tipo de encapsulamiento.

PROSPERINA(config-subif)#**ip address** 192.168.21.17 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

PROSPERINA(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente el puerto.

PROSPERINA(config-subif)#**interface fastethernet1/0.4**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet1/0.4.

PROSPERINA(config-subif)#**description VLAN SERVIDORES PROSPERINA**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

PROSPERINA(config-subif)#**encapsulation dot1q 4**

Se debe digitar el comando encapsulation dot1q y el número de la vlan, para definir el tipo de encapsulamiento.

PROSPERINA(config-subif)#**ip address** 192.168.21.25 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

PROSPERINA(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente el puerto.

PROSPERINA(config-subif)#**interface fastethernet1/0.5**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet1/0.4.

PROSPERINA(config-subif)#**description VLAN CLIENTES_WLL PROSPERINA**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

PROSPERINA(config-subif)#**encapsulation dot1q 5**

Se debe digitar el comando encapsulation dot1q y el número de la vlan, para definir el tipo de encapsulamiento.

PROSPERINA(config-subif)#**ip address** 192.168.21.33 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

PROSPERINA(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente el puerto.

PROSPERINA(config-if)#**interface fastethernet2/0**

Digite el comando anterior para ingresar al modo de configuración de la interfaz fastethernet 2/0.

PROSPERINA(config-if)#**description CONEXIÓN DE ÚLTIMA MILLA**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

PROSPERINA(config-if)#**ip address** 10.10.10.1 255.255.255.252

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

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

Se debe ingresar éste comando para habilitar administrativamente el puerto. Luego de digitar éste comando, aparece el siguiente mensaje el cual realiza un test para comprobar si hay conexión física y lógica. Si el estado de la interface es **down,** quiere decir que existe algún tipo de problema en el enlace.

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

5.3.1.5 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2.

Para poder configurar un protocolo de enrutamiento, se debe entrar primeramente al modo de usuario privilegiado.

PROSPERINA(config)#**router rip**

Con éste comando se habilita el protocolo de enrutamiento rip.

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

Se debe especificar la versión del protocolo de enrutamiento rip.

PROSPERINA (config -router)#**network 192.168.22.0**
PROSPERINA (config -router)#**network 192.168.20.0**
PROSPERINA (config -router)#**network 192.168.23.0**
PROSPERINA (config -router)#**network 192.168.24.0**
PROSPERINA (config -router)#**network 192.168.25.0**

Una vez activado el protocolo de enrutamiento es preciso indicar qué redes va ha enrutar.
Se debe asignar las redes que seguirá el protocolo.

PROSPERINA (config -router)#**default-metric 10**

Se debe especificar la métrica por defecto para que pueda transportar paquetes ospf.

PROSPERINA (config -router)#**redistribute ospf 1**

Éste comando permite redistribuir paquetes ospf por nuestra red rip.

5.3.1.6 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO OSPF.

Para poder configurar un protocolo de enrutamiento, se debe entrar primeramente al modo de usuario privilegiado.

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

Con éste comando se habilita el protocolo de enrutamiento ospf.

PROSPERINA(config -router)#**log-adjacency-changes**

Se debe ingresar el comando anterior para cargar los cambios de los routers adyacentes.

PROSPERINA(config -router)# **network** 192.168.21.0 0.0.0.255 area 0

Al activar el protocolo de enrutamiento se especifica la red con su respectiva wildcard y el área en la que va a trabajar.

PROSPERINA (config -router)#**redistribute rip subnets**

El comando anterior permite redistribuir paquetes rip v2, por nuestra red.

5.3.1.7 CONFIGURACIÓN DE LISTAS DE ACCESO.

Para poder crear las listas de acceso, se debe entrar primeramente al modo de usuario privilegiado.

PROSPERINA(config)#**access-list 1 permit host 192.168.21.10**
PROSPERINA(config)#**access-list 1 deny any any**
PROSPERINA(config)#**access-list 1 remark PERMITIR SOLO SERVIDOR ADMINISTRATIVO.**

Ingresar una lista de acceso standard, que permita únicamente al administrador enviar y recibir paquetes.

5.3.1.8 INCLUIR LA LISTA DE ACCESO A LA INTERFAZ DE SALIDA.

Para poder incluir la lista de acceso a la interfaz de salida, se debe entrar primeramente al modo de usuario privilegiado.

PROSPERINA(config)#**interface FastEthernet1/0.1**

Se debe ingresar a la interfaz que tendrá asignada la lista de acceso.

PROSPERINA(config-if)#**ip access-group** 1 **out**

Con éste comando se asigna la lista de acceso a la interfaz.

5.3.1.9 GUARDAR LAS CONFIGURACIONES.

Para poder guardar las configuraciones hechas en el router, se debe entrar primeramente al modo de usuario privilegiado.

PROSPERINA#**copy running-config startup-config**

Con éste comando se guarda desde la configuración actual a la configuración de inicio.

Building configuration...

Éste mensaje aparecerá cuando se está guardando la configuración.

[OK]

Luego aparece un mensaje de aprobación.

5.3.1.10 SHOW RUN ROUTER PROSPERINA.

PROSPERINA#sh run
Building configuration...
!
Version 12.11

Indica la versión del IOS.

service timestamps debug uptime
service timestamps log uptime
service password-encryption

Indica que el servicio de encriptación de contraseña se encuentra activo.

!
hostname PROSPERINA

Refleja el nombre asignado al router.

enable secret 5 sdf6978yhg$jnb76sd

Ésta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Ésta línea especifica la contraseña de ingreso al router, del usuario privilegiado.

!
ip subnet-zero
!
interface Serial0/0

Especifica la interfaz serial 0 slot 0.

description CONEXION AL ROUTER PENAS

Descripción de la interfaz.

ip address 192.168.20.9 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast

clock rate 56000

Muestra la velocidad del puerto en bps.

bandwidth 1544

Valor del ancho de banda del enlace.

interface Serial0/1

Especifica la interfaz serial 1 slot 0.

description CONEXION AL ROUTER SAMBORONDON

Descripción de la interfaz.

ip address 192.168.20.5 255.255.255.252

Dirección ip y máscara de sub-red de la interfaz.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda del enlace.

!
interface Serial0/2

Especifica interfaz serial 2 slot 0.

description CONEXION AL ROUTER BABAHOYO

Descripción de la interfaz.

ip address 192.168.20.13 255.255.255.252

Dirección ip y máscara de sub-red.

no ip directed-broadcast
clock rate 56000

Indica la velocidad del puerto en bps.

bandwidth 1544

Valor del ancho de banda del enlace.

!
interface Serial0/3

Especifica la interfaz serial 3 slot 0.

description CONEXION AL ROUTER SALINAS

Descripción de la interfaz.

ip address 192.168.20.1 255.255.255.252

Dirección ip y máscara de sub-red.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda del enlace.

!
interface FastEthernet0/0

Especifica la interfaz fastethernet 0 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace.

shutdown

Indica interfaz no levantada.

!
interface FastEthernet0/0.1

Especifica sub-interfaz fastethernet 0.1 slot 0.

description VLAN POR DEFECTO PROSPERINA

Descripción de la interfaz.

encapsulation dot1q 1

Define el tipo de encapsulamiento asignado a la VLAN 1.

ip address 192.168.21.1 255.255.255.248

Dirección ip y máscara de sub-red.

ip access-group 1 out

Define la lista de acceso a la interfaz de salida.

!
interface FastEthernet0/0.2

Especifica la sub-interfaz fastethernet 0.2.

description VLAN LAB_TECNOLOGIAS PROSPERINA

Descripción de la interfaz

encapsulation dot1q 2

Define el tipo de encapsulamiento asignado a la VLAN 2.

ip address 192.168.21.9 255.255.255.248

Dirección ip y máscara de sub-red.

!
interface FastEthernet0/0.3

Especifica sub-interfaz fastethernet 0.3 slot 0.

description VLAN LAB1_ICHE PROSPERINA

Descripción de la interfaz.

encapsulation dot1q 3

Define el tipo de encapsulamiento asignado a la VLAN 3.

ip address 192.168.21.17 255.255.255.248

Dirección ip y máscara de sub-red.

interface FastEthernet0/0.4

Especifica sub-interfaz fastethernet 0.4 slot 0.

description VLAN SERVIDORES PROSPERINA

Descripción de la interfaz.

encapsulation dot1q 4

Define el tipo de encapsulamiento asignado a la VLAN 4.

ip address 192.168.21.25 255.255.255.248

Dirección ip y máscara de sub-red.

interface FastEthernet0/0.5

Especifica sub-interfaz fastethernet 0.5 slot 0.

description VLAN CLIENTES_WLL PROSPERINA

Descripción de la interfaz.

encapsulation dot1q 5

Define el tipo de encapsulamiento asignado a la VLAN 5.

ip address 192.168.21.33 255.255.255.248

Dirección ip y máscara de sub-red.

!

interface FastEthernet0/1

Especifica la interfaz fastethernet 1 slot 0.

description CONEXIÓN DE ÚLTIMA MILLA

Descripción de la interfaz.

ip address 10.10.10.1 255.255.255.252

Dirección ip y máscara de sub-red.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace.

!

router rip

Indica que se ha configurado el protocolo de enrutamiento rip.

version 2

Versión del protocolo de enrutamiento.

redistribute OSPF 1

Se ha permitido redistribuir por nuestra red rip paquetes ospf.

default-metric 10

Especifica la métrica por defecto para que pueda transportar paquetes ospf.

network 192.168.22.0
network 192.168.20.0
network 192.168.23.0
network 192.168.24.0
network 192.168.25.0

Muestra las redes asignadas a nuestro protocolo de enrutamiento.

!
router ospf 1

Indica que se ha configurado el protocolo de enrutamiento ospf.

log-adjacency-changes

Esto indica que el router carga los cambios de los routers adyacentes.

redistribute RIP subnets

Permite redistribuir por nuestra red ospf paquetes rip.

network 192.168.21.0 0.0.0.255 area 0

Especifica la red con su respectiva wildcard y el área en la cual se desea trabajar trabajar.

!
ip classless

Indica el acceso a las redes no remotas con máscara de sub-red diferente.

no ip http server

Especifica que no existe un servidor http.

access-list 1 permit host 192.168.21.10 any
access-list 1 deny any any

Access-list asignadas al router.

access-list 1 remark PERMITIR SOLO SERVIDOR ADMINISTRATIVO

Descripción de la access-list ingresada en la configuración.

line con 0
login

Configuración Puerto de consola.

transport input none

Ningún transporte impuesto.

password cisco

Contraseña asignada.

line aux 0

Configuración Puerto auxiliar.

line vty 0 4
login

Configuración remota por telnet.

password cisco

Contraseña asignada.

!
no scheduler allocate
end-

Fin del reporte de la configuración actual.

5.3.1.11 SHOW IP ROUTE PROSPERINA.

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

Gateway of last resort is not set

192.168.20.0/30 is subnetted, 6 subnets
192.168.21.0/29 is subnetted, 5 subnets
192.168.22.0/29 is subnetted, 4 subnets
192.168.25.0/29 is subnetted, 4 subnets
192.168.24.0/29 is subnetted, 4 subnets
192.168.23.0/29 is subnetted, 4 subnets

192.168.x.x: Indica la red. **/x:** el nivel de segmentación. **x subnets:** el número de sub-redes en las cuales se encuentra dividida.

C 192.168.20.8 is directly connected, Serial0/0
C 192.168.20.4 is directly connected, Serial0/1
C 192.168.20.12 is directly connected, Serial0/2
C 192.168.20.0 is directly connected, Serial0/3
C 192.168.21.0 is directly connected, 192.168.21.1
C 192.168.21.8 is directly connected, 192.168.21.9
C 192.168.21.16 is directly connected, 192.168.21.17
C 192.168.21.24 is directly connected, 192.168.21.25

C 192.168.21.32 is directly connected, 192.168.21.33

C: Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectada y **Serialx:** la interfaz de salida por la cual se accede a la red de destino.

R 192.168.20.32 [120/1] via 192.168.20.14, 00:03:31, Serial0/2
R 192.168.20.36 [120/1] via 192.168.20.6, 00:09:40, Serial0/1
R 192.168.22.0 [120/1] via 192.168.20.2, 00:07:40, Serial0/3
R 192.168.22.8 [120/1] via 192.168.20.2, 00:07:21, Serial0/3
R 192.168.22.16 [120/1] via 192.168.20.2, 00:05:30, Serial0/3
R 192.168.22.24 [120/1] via 192.168.20.2, 00:05:39, Serial0/3
R 192.168.25.0 [120/1] via 192.168.20.10, 00:04:42, Serial0/0
R 192.168.25.8 [120/1] via 192.168.20.10, 00:01:13, Serial0/0
R 192.168.25.16 [120/1] via 192.168.20.10, 00:02:17, Serial0/0
R 192.168.25.24 [120/1] via 192.168.20.10, 00:05:29, Serial0/0
R 192.168.24.0 [120/1] via 192.168.20.14, 00:06:36, Serial0/2
R 192.168.24.8 [120/1] via 192.168.20.14, 00:09:44, Serial0/2
R 192.168.24.16 [120/1] via 192.168.20.14, 00:04:12, Serial0/2
R 192.168.24.24 [120/1] via 192.168.20.14, 00:01:28, Serial0/2
R 192.168.23.0 [120/1] via 192.168.20.6, 00:01:38, Serial0/1
R 192.168.23.8 [120/1] via 192.168.20.6, 00:01:27, Serial0/1
R 192.168.23.16 [120/1] via 192.168.20.6, 00:05:13, Serial0/1
R 192.168.23.24 [120/1] via 192.168.20.6, 00:05:19, Serial0/1

R: Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), 192.168.x.x la dirección de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **Serial x:** la interfaz de salida.

5.3.2 CONFIGURACIÓN DEL SWITCH PROSPERINA.

Switch>**enable**

A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#**configure terminal**

Estando en el modo de usuario privilegiado digitar el comando anterior para pasar al modo de configuración general.

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

Aparecerá un mensaje que indica que se debe ingresar los comandos de configuración, línea por línea.

Switch(config)#**hostname SW_PROSPERINA**

Digitar el comando anterior para establecer el nombre del dispositivo.

SW_PROSPERINA(config)#**ip default-gateway 192.168.21.1**

Asignar al switch esta ip como puerta de enlace por defecto.

5.3.2.1 CONFIGURACIÓN DE INTERFAZ VLAN 1 (INTERFAZ VLAN POR DEFECTO).

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

Se debe ingresar a la interfaz vlan por defecto.

SW_PROSPERINA(config-if)#**ip address 192.168.21.2 255.255.255.248**

Este comando sirve para asignar una dirección IP y máscara de sub-red a la sub-interfaz.

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

Permite habilitar administrativamente el puerto.

5.3.2.2 CREACIÓN DE VLAN.

SW_PROSPERINA#**vlan database**

Permite ingresar a la base de datos de las VLAN.

SW_PROSPERINA(vlan)#**vlan 2 name LAB_TECNOLOGIAS**

SW_PROSPERINA(vlan)#**vlan 3 name LAB1_ICHE**
SW_PROSPERINA(vlan)#**vlan 4 name SERVIDORES**
SW_PROSPERINA(vlan)#**vlan 5 name CLIENTES_WLL**

Con esta línea de comando se crearán las vlans con un número y nombre único.

5.3.2.3 CONFIGURACIÓN DE INTERFACES FASTETHERNET ASIGNANDO VLAN.

Para configurar las interfaces asignándoles vlan se debe acceder primeramente al nivel de usuario privilegiado.

SW_PROSPERINA(config)#**interface fastethernet 0/4**

Digite el comando anterior para configurar la interfaz fastethernet 0/4.

SW_PROSPERINA(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para poder asignarle una VLAN.

SW_PROSPERINA(config -if)#**switchport access vlan 2**

Agrega este puerto a la vlan especificada.

SW_PROSPERINA(config)#**interface fastethernet 0/5**

Digite el comando anterior para configurar la interfaz fastethernet 0/5

SW_PROSPERINA(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN

SW_PROSPERINA(config -if)#**switchport access vlan 3**

Agrega este puerto a la vlan especificada.

SW_PROSPERINA(config)#**interface fastethernet 0/6**

Digite el comando anterior para configurar la interfaz fastethernet 0/6

SW_PROSPERINA(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN

SW_PROSPERINA(config -if)#**switchport access vlan 4**

Agrega este puerto a la vlan especificada.

SW_PROSPERINA(config)#**interface fastethernet 0/7**

Digite el comando anterior para configurar la interfaz fastethernet 0/7

SW_PROSPERINA(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN

SW_PROSPERINA(config -if)#**switchport access vlan 5**

Agrega este puerto a la vlan especificada.

5.3.2.4 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

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

Este comando sirve para salir del modo configuración de interfaz a modo configuración general

SW_PROSPERINA(config)#**line vty 0 15**

Habilita el acceso por terminal virtual

SW_PROSPERINA(config -line)#**password cisco**

Se debe ingresar la contraseña

SW_PROSPERINA(config -line)#**login**

Activa el inicio por contraseña.

SW_PROSPERINA(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

SW_PROSPERINA(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual.

SW_PROSPERINA(config)#**line con 0**

Habilita el acceso por consola.

SW_PROSPERINA(config -line)#**password cisco**

Se debe ingresar la contraseña.

SW_PROSPERINA(config -line)#**login**

Activa al inicio de la contraseña.

5.3.2.5 GUARDAR CONFIGURACIONES HECHAS EN EL SWITCH.

SW_PROSPERINA(config -line)#**exit**

Digitar este comando para salir del modo configuración de consola a modo configuración general

SW_PROSPERINA(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado

%SYS-5-CONFIG_I: Configured from console by console

Cuando se hace este procedimiento aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

SW_PROSPERINA#**copy running-config startup-config**

Con el comando anterior se guarda la configuración actual a la configuración de inicio

Building configuration...

El siguiente mensaje significa que se esta guardando la configuración

[OK]

Ahora aparece un mensaje de aprobación.

5.3.2.6 SHOW RUN SWITCH PROSPERINA.

SW_PROSPERINA#sh run
!
Versión 12.1

Indica la versión del IOS.

service timestamps debug uptime
service timestamps log uptime
service password-encryption

Indica que el servicio de encriptación de contraseña esta activo.

!
hostname SW_PROSPERINA

Refleja el nombre que el administrador le ha asignado al router.

ip name-server 0.0.0.0
enable secret 5 sdf6978yhg$jnb76sd

Esta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Esta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
!
!
ip subnet-zero

!
!
!
!
!
!
spanning-tree extend system-id

Para usar red sin bucles, rutas cortas.

!
!
!
!
interface FastEthernet0/1

Especifica la interfaz. fastethernet0/1.

switchport mode dynamic desirable

Indica que no está configurado el modo tipo acceso.

bandwidth 100000

Indica el costo del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/2
```
Especifica interfaz fastethernet0/2.

```
switchport mode dynamic desirable
```
Indica que no está configurado el modo tipo acceso.

```
bandwidth 100000
```
Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/3
```
Especifica interfazfastethernet0/3.

```
switchport mode dynamic desirable
```
Indica que no está configurado el modo tipo acceso.

```
bandwidth 100000
```
Indica el costo del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/4
```
Especifica interfaz fastethernet0/4.

```
switchport mode dynamic
```
Indica que está configurado el modo tipo acceso a las VLAN.

```
switchport access vlan 2
```
Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
```
Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/5
```
Especifica interfazfastethernet0/5.

```
switchport mode dynamic
```
Indica que está configurado el modo tipo acceso a las VLAN.

```
switchport access vlan 3
```
Especifica que está interfaz es parte de la VLAN indicada.

```
bandwidth 100000
```

Valor del ancho de banda de la Interfaz.

```
!
interface FastEthernet0/6
```

Especifica interfazfastethernet0/6.

```
switchport mode dynamic
```

Indica que está configurado el modo tipo acceso para acceder a las VLAN.

```
switchport access vlan 4
```

Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
```

Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/7
```

Especifica interfazfastethernet0/7.

```
switchport mode dynamic
```

Indica que está configurado el modo tipo acceso para acceder a las VLAN.

```
switchport access vlan 5
```

Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
```

Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/8
```

Especifica interfaz fastethernet0/8.

```
switchport mode dynamic desirable
```

Indica que no está configurado el modo tipo acceso.

```
bandwidth 100000
```

Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/9
```

Especifica interfazfastethernet0/9.

```
switchport mode dynamic desirable
```

Indica que no está configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/10

Especifica interfazfastethernet0/10.

switchport mode dynamic desirable

Indica que no está configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/11

Especifica interfazfastethernet0/11.

switchport mode dynamic desirable

Indica que no está configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/12

Especifica interfazfastethernet0/12.

switchport mode dynamic desirable

Indica que no está configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface GigabitEthernet0/1

Especifica la interfaz Gigabithernet0/1.

switchport mode dynamic desirable

Indica que no está configurado el modo tipo acceso.

bandwidth 100000000

Valor del ancho de banda del enlace en la interfaz.

!
interface GigabitEthernet0/2

Especifica la interfaz Gigabithernet0/2.

switchport mode dynamic desirable

Indica que no está configurado el modo tipo acceso.

bandwidth 100000000

Valor del ancho de banda del enlace en la interfaz.

!

vtp domain bigdomain

Especifica el dominio del puerto truncado virtual.

interface Vlan 1

Especifica la VLAN 1 (vlan por defecto).

ip address 192.168.21.2 255.255.255.248

Dirección IP de la vlan por defecto.

no ip route-cache

No almacena ip en el cache de rutas.

shutdown

vlan 2 name lab_tecnologias

Indica VLAN configurada con su respectivo nombre.

vlan 3 name lab1_iche

Indica VLAN configurada con su respectivo nombre.

vlan 4 name servidores

Indica VLAN configurada con su respectivo nombre.

vlan 5 name clientes_wll

Indica VLAN configurada con su respectivo nombre.

!

ip classless

Indica acceso a las redes no remotas con máscara de sub-red diferente.

no ip http Server

Especifica que no existe un servidor http.

!

ip default-gateway 192.168.21.1

Indica interfaz de puerta de enlace para comunicar VLAN.

!

!

line con 0

Configuración Puerto de consola.

login

Activar configuración al inicio.

transport input none
Ningún transporte impuesto.

password cisco
Contraseña asignada.

line aux 0
Configuración Puerto auxiliar.

line vty 0 4
Configuración remota por telnet.

login
Activar configuración al inicio.

password cisco
Contraseña asignada.

!
no scheduler allocate

end
Fin del reporte de la configuración actual.

5.3.2.7 SHOW VLAN SWITCH PROSPERINA.

SW_PROSPERINA#sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14
2	lab_tecnologias	active	Fa0/4
3	lab1_iche	active	Fa0/5
4	servidores	active	Fa0/6
5	clientes wll	active	Fa0/7
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
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
4	enet	100004	1500	-	-	-	-	-	0	0
5	enet	100004	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

VLAN: Identificación vlan

Name: Nombre de vlan
Status: Estado
Ports: Puertos asignados a la vlan
Type: Tipo de interfaces
SIAD: Encabezado para identificar vlan
MTU: Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes

Parent: Parentela
RingNo: Número de anillo si hay
BridgeNO: Número de puente si hay
Stp: STP usado
BrdgMode: Modo de puente
Transx: TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

5.3.3 CONFIGURACIÓN DEL ROUTER SALINAS.

Router>**enable**

A nivel del modo usuario normal se debe digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

Digitar éste comando en el modo de usuario privilegiado para pasar al modo de configuración general.

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

Aparecerá un mensaje que le indica al usuario que debe ingresar los comandos de configuración, línea por línea.

Router(config)#**hostname SALINAS**

En el modo de configuración general digitar el comando anterior y a continuación un nombre para el dispositivo.

5.3.3.1 CONFIGURACIÓN DE INTERFACES SERIALES.

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

Digite el comando anterior para entrar al modo de configuración de la interfaz serial 0/0.

SALINAS(config-if)#**description CONEXIÓN AL ROUTER PROSPERINA**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

SALINAS(config-if)#**ip address** 192.168.20.2 255.255.255.252

Éste comando permite asignar una dirección IP con su respectiva máscara de sub-red, a la interfaz serial.

SALINAS(config-if)#**clock rate 56000**

Digite el comando anterior para indicar la velocidad de la interfaz en bps. Se necesita incluir éste comando ya que está definido como DCE. Según el gráfico de la implementación. Figura 5.32.

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

Se debe ingresar éste comando para habilitar administrativamente la interfaz. Luego de digitar éste comando, aparece el siguiente mensaje el cual realiza un test para comprobar si hay conexión física y lógica. Si el estado de la interfaz es **down,** quiere decir que existe algún tipo de problema en el enlace.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

5.3.3.2 CONFIGURACIÓN DE SUB-INTERFACES.

Para poder configurar una sub-interfaz, se debe entrar primeramente al modo de usuario privilegiado.

SALINAS(config)#**interface fastethernet0/0.1**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet1/0.1.

SALINAS(config-subif)#**description VLAN POR DEFECTO SALINAS**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

SALINAS(config-subif)#**encapsulation dot1q 1**

Se debe digitar el comando encapsulation dot1q para definir el tipo de encapsulamiento. Donde uno es el número de vlan.

SALINAS(config-subif)#**ip address** 192.168.22.1 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz interfaz.

SALINAS(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente el la interfaz.

SALINAS(config-subif)#**interface fastethernet0/0.2**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet0/0.2.

SALINAS(config-subif)#**description VLAN CALL_CENTER SALINAS**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

SALINAS(config-subif)#**encapsulation dot1q 2**

Se debe digitar el comando encapsulation dot1q y el número de la vlan, para definir el tipo de encapsulamiento. Donde dos es el número de la vlan.

SALINAS(config-subif)#**ip address 192.168.22.9 255.255.255.248**

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

SALINAS(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente la interfaz.

SALINAS(config-subif)#**interface fastethernet0/0.3**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet0/0.3.

SALINAS(config-subif)#**description VLAN SERVIDORES SALINAS**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

SALINAS(config-subif)#**encapsulation dot1q 3**

Se debe digitar el comando encapsulation dot1q y el número de la vlan, para definir el tipo de encapsulamiento.

SALINAS(config-subif)#**ip address** 192.168.22.17 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

SALINAS(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente la interfaz.

SALINAS(config-subif)#**interface fastethernet0/0.4**

Digite el comando anterior para entrar al modo de configuración de la sub-interfaz FastEthernet0/0.4.

SALINAS(config-subif)#**description VLAN FINANZAS_CAJA SALINAS**

Para agregar un comentario a la interfaz, se debe ingresar el comando **description.**

SALINAS(config-subif)#**encapsulation dot1q 4**

Se debe digitar el comando encapsulation dot1q y el número de la vlan, para definir el tipo de encapsulamiento.

SALINAS(config-subif)#**ip address** 192.168.22.25 255.255.255.248

Asignar una dirección IP con su respectiva máscara de sub-red, a la sub-interfaz.

SALINAS(config-subif)#**no shutdown**

Se debe ingresar éste comando para habilitar administrativamente la interfaz.

5.3.3.3 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2.

SALINAS# **configure Terminal**

A nivel de modo usuario privilegiado se debe digitar el comando anterior para pasar a modo de configuración general.

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

Aparece un mensaje que indica al usuario que ingrese los comandos de configuración, línea por línea.

SALINAS(config-if)#**router rip**

Se debe habilitar el protocolo de enrutamiento con el comando anterior.

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

Se debe especificar la versión del protocolo de enrutamiento.

SALINAS(config -router)#**network 192.168.20.0**
SALINAS(config -router)#**network 192.168.22.0**
SALINAS(config -router)#**network 192.168.23.0**
SALINAS(config -router)#**network 192.168.24.0**
SALINAS(config -router)#**network 192.168.25.0**

Una vez activado el protocolo de enrutamiento es preciso indicar qué redes se van a enrutar.
Asignando las redes que seguirán el protocolo.

5.3.3.4 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

SALINAS(config)#**line vty 0 4**

Habilitar el acceso por terminal virtual.

SALINAS(config -line)#**password cisco**

Se debe ingresar la contraseña.

SALINAS(config -line)#**login**

Activar el inicio con contraseña.

SALINAS(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

SALINAS(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual.

SALINAS(config)#**line con 0**

Habilitar el acceso por consola.

SALINAS(config -line)#**password cisco**

Se debe ingresar la contraseña.

SALINAS(config -line)#**login**

Activar el inicio con contraseña.

Con el mismo procedimiento puede configurarse una password para acceder por el puerto auxiliar. Tanto el puerto de consola como el auxiliar, no requieren autenticación de password por defecto.

5.3.3.5 GUARDANDO LA CONFIGURACIÓN DEL ROUTER.

SALINAS#**copy running-config startup-config**

Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

El siguiente mensaje indica que se está guardando la configuración.

[OK]

Ahora aparece un mensaje de aprobación.

5.3.3.6 SHOW RUN ROUTER SALINAS.

SALINAS#sh run
Building configuration...

!
Version 12.1

Indica la versión del IOS.

service timestamps debug uptime
service timestamps log uptime

service password-encryption

Indica que el servicio de encriptación de contraseña está activo.

!
hostname SALINAS

Refleja el nombre que el administrador le ha asignado al router

enable secret 5 sdf6978yhg$jnb76sd

Ésta línea especifica que la contraseña está encriptada por el protocolo md5.

enable password cisco

Ésta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
ip subnet-zero
!
interface Serial0

Especifica interfaz serial 0

description CONEXION PROSPERINA

Descripción de la interfaz

ip address 192.168.20.2 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
clock rate 56000

Indica la velocidad de la interfaz en bits por segundo. Se lo encuentra en interfaces DCE.

bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

!
interface Serial1
no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
interface FastEthernet0/0

Especifica interfaz fastethernet 0 slot 0

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
interface FastEthernet0/0.1

Especifica sub-interfaz fastetehrnet 0.1 slot 0.

description VLAN POR DEFECTO SALINAS

Descripción de la interfaz.

encapsulation dot1q 1

Define el tipo de encapsulamiento asignado a la VLAN 1.

ip address 192.168.22.1 255.255.255.248

Dirección ip y máscara de de sub-red de la sub-interfaz.

!
interface FastEthernet0/0.2

Especifica sub-interfaz fastetehrnet 0.2 slot 0.

description VLAN CALL_CENTER SALINAS

Descripción de la interfaz.

encapsulation dot1q 2

Define el tipo de encapsulamiento asignado a la VLAN 2.

ip address 192.168.22.9 255.255.255.248

Dirección ip y máscara de de sub-red de la sub-interfaz.

!
interface FastEthernet0/0.3

Especifica sub-interfaz fastetehrnet 0.3 slot 0.

description VLAN SERVIDORES SALINAS

Descripción de la interfaz.

encapsulation dot1q 3

Define el tipo de encapsulamiento asignado a la VLAN 3.

ip address 192.168.22.17 255.255.255.248

Dirección ip y máscara de de sub-red de la sub-interfaz.

!
interface FastEthernet0/0.4

Especifica sub-interfaz fastetehrnet 0.4 slot 0.

description VLAN FINANZAS_CAJA SALINAS

Descripción de la interfaz.

encapsulation dot1q 4

Define el tipo de encapsulamiento asignado a la VLAN 4.

ip address 192.168.22.25 255.255.255.248

Dirección ip y máscara de de sub-red de la sub-interfaz.

!
interface FastEthernet0/1

Especifica la interfaz fastethernet 1 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
router rip

Indica que se ha configurado el protocolo de enrutamiento rip.

version 2

Define la versión 2 del protocolo de enrutamiento.

network 192.168.20.0
network 192.168.22.0
network 192.168.23.0
network 192.168.24.0
network 192.168.25.0

Indica qué redes enruta nuestro protocolo de enrutamiento.

!
ip classless

Indica acceso a las redes no remotas con máscara de sub-red diferente.

no ip http Server

Especifica que no existe un servidor http.

!
line con 0

Configuración Puerto de consola.

Login

Activar el inicio con contraseña.

transport input none

Ningún transporte impuesto.

password cisco

Contraseña asignada.

line aux 0.

Configuración Puerto auxiliar.

line vty 0 4

Configuración remota por telnet.

Login

Activar el inicio con contraseña.

password cisco

Contraseña asignada.

!
no scheduler allocate

end

Fin del reporte de la configuración actual.

5.3.3.7 SHOW IP ROUTE SALINAS.

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

Gateway of last resort is not set

192.168.22.0/29 is subnetted, 4 subnets
192.168.0.0/30 is subnetted, 6 subnets
192.168.21.0/29 is subnetted, 5 subnets
192.168.25.0/29 is subnetted, 4 subnets
192.168.24.0/29 is subnetted, 4 subnets
192.168.23.0/29 is subnetted, 4 subnets

192.168.x.x: Indica la red / **x:** el nivel de segmentación y **x subnets:** el número de sub-redes en las cuales se encuentra dividida.

C 192.168.22.0 is directly connected, 192.168.22.1
C 192.168.22.8 is directly connected, 192.168.22.9
C 192.168.22.16 is directly connected, 192.168.22.17
C 192.168.22.24 is directly connected, 192.168.22.25
C 192.168.20.0 is directly connected, Serial0

C: Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serialx:** la interfaz de salida por la cual se accede a la red de destino.

R 192.168.20.8 [120/1] via 192.168.20.1, 00:05:32, Serial0
R 192.168.20.4 [120/1] via 192.168.20.1, 00:05:13, Serial0
R 192.168.20.12 [120/1] via 192.168.20.1, 00:06:22, Serial0
R 192.168.20.32 [120/2] via 192.168.20.1, 00:06:22, Serial0
R 192.168.20.36 [120/2] via 192.168.20.1, 00:07:26, Serial0
R 192.168.21.0 [120/10] via 192.168.20.1, 00:07:43, Serial0
R 192.168.21.8 [120/10] via 192.168.20.1, 00:09:42, Serial0
R 192.168.21.16 [120/10] via 192.168.20.1, 00:02:21, Serial0
R 192.168.21.24 [120/10] via 192.168.20.1, 00:04:28, Serial0
R 192.168.21.32 [120/10] via 192.168.20.1, 00:09:35, Serial0
R 192.168.25.0 [120/2] via 192.168.20.1, 00:02:17, Serial0
R 192.168.25.8 [120/2] via 192.168.20.1, 00:08:20, Serial0
R 192.168.25.16 [120/2] via 192.168.20.1, 00:03:30, Serial0
R 192.168.25.24 [120/2] via 192.168.20.1, 00:07:41, Serial0
R 192.168.24.0 [120/2] via 192.168.20.1, 00:02:20, Serial0
R 192.168.24.8 [120/2] via 192.168.20.1, 00:02:26, Serial0
R 192.168.24.16 [120/2] via 192.168.20.1, 00:07:39, Serial0
R 192.168.24.24 [120/2] via 192.168.20.1, 00:06:40, Serial0
R 192.168.23.0 [120/2] via 192.168.20.1, 00:05:15, Serial0
R 192.168.23.8 [120/2] via 192.168.20.1, 00:07:25, Serial0
R 192.168.23.16 [120/2] via 192.168.20.1, 00:06:41, Serial0
R 192.168.23.24 [120/2] via 192.168.20.1, 00:08:12, Serial0

R: Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), **192.168.x.x:** la dirección ip de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **Serialx:** la interfaz de salida.

5.3.4 CONFIGURACIÓN SWITCH SALINAS.

Switch>**enable**

A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando que se muestra para pasar a modo de configuración general.

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

Aparecerán unas líneas describiendo al usuario que ingrese los comandos de configuración, uno a uno.

Switch(config)#**hostname SW_SALINAS**

En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

SW_SALINAS(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado digitar el comando expuesto.

SW_SALINAS(config)#**enable secret cisco**

También para establecer puntos de seguridad se debe encriptar la contraseña con el protocolo de encriptación md5 mediante el comando señalado.

SW_SALINAS(config)#**ip default-gateway 192.168.22.1**

Asigna al switch esta ip como puerta de enlace por defecto

5.3.4.1 CONFIGURACIÓN DE INTERFAZ VLAN 1 (INTERFAZ VLAN POR DEFECTO).

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

Se debe ingresar a la interfaz vlan por defecto (vlan 1)

SW_SALINAS(config-if)#**ip address 192.168.22.2 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub-interfaz digitar lo anterior

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

5.3.4.2 CREACIÓN DE VLAN.

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general.

SW_SALINAS(config)#**exit**

Se debe ingresar el comando **exit** para salir del modo configuración general a modo de usuario privilegiado.

SW_SALINAS#**vlan database**

Permite ingresar a la base de datos de las VLAN.

SW_SALINAS(vlan)#**vlan 2 name CALLCENTER**

Crea la vlan número 2 con el nombre especificado.

SW_SALINAS(vlan)#**vlan 3 name SERVIDORES**

Crea la vlan 3 con el nombre especificado.

SW_SALINAS(vlan)#**vlan 4 name FINANZAS_CAJA**

Crea la vlan 4 con el nombre especificado.

5.3.4.3 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

SW_SALINAS(vlan)#**exit**

Para salir de la base de datos de las VLAN.

SW_SALINAS#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general

SW_SALINAS(config)#**interface fastethernet 0/4**

Digite el comando anterior para configurar la interfaz fastethernet 0/4.

SW_SALINAS(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_SALINAS(config -if)#**switchport access vlan 2**

Agrega este puerto a la vlan especificada..

SW_SALINAS(config)#**interface fastethernet 0/5**

Digite el comando anterior para configurar la interfaz fastethernet 0/5.

SW_SALINAS(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_SALINAS(config -if)#**switchport access vlan 3**

Agrega este puerto a la vlan especificada.

SW_SALINAS(config)#**interface fastethernet 0/6**

Digite el comando anterior para configurar la interfaz fastethernet 0/6.

SW_SALINAS(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_SALINAS(config -if)#**switchport access vlan 4**

Agrega este puerto a la vlan especificada.

5.3.4.4 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general.

SW_SALINAS(config)#**line vty 0 15**

Habilita el acceso por terminal virtual.

SW_SALINAS(config -line)#**password cisco**

Se debe de registrar una contraseña.

SW_SALINAS(config -line)#**login**

Activar al inicio.

SW_SALINAS(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

SW_SALINAS(config -line)#**exit**

Se debe salir de la configuración de la terminal virtual.

SW_SALINAS(config)#**line con 0**

Habilita el acceso por consola.

SW_SALINAS(config -line)#**password cisco**

Se debe registrar una contraseña.

SW_SALINAS(config -line)#**login**

Activar al inicio.

5.3.4.5 GUARDAR CONFIGURACIONES HECHAS EN EL SWITCH.

SW_SALINAS(config -line)#**exit**

Digitar lo anterior para salir del modo configuración de consola a modo configuración general

SW_SALINAS(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado

%SYS-5-CONFIG_I: Configured from console by console

Cuando se realiza este procedimiento aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

SW_SALINAS#**copy running-config startup-config**

Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

El siguiente mensaje significa que se esta guardando la configuración.

[OK]

Ahora aparece un mensaje de aprobación

5.3.4.6 SHOW RUN SWITCH SALINAS.

SW_SALINAS#sh run
!
Version 12.1

Indica la versión del IOS

service timestamps debug uptime
service timestamps log uptime
service password-encryption

Indica que el servicio de encriptación de contraseña esta activo.

!
hostname SW_SALINAS

Refleja el nombre que el administrador le ha asignado al router.

ip name-server 0.0.0.0
enable secret 5 sdf6978yhg$jnb76sd

Esta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Esta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
!
!
ip subnet-zero

!
!

```
!
!
!
!
spanning-tree extend system-id
                                Para usar red sin bucles, rutas cortas.
!
!
!
!
interface FastEthernet0/1
                                Especifica interfaz fastethernet0/1.

switchport mode dynamic desirable
                                Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
                                Valor del ancho de banda del enlace en la interfaz.
!
interface FastEthernet0/2
                                Especifica interfaz fastethernet0/2.

switchport mode dynamic
                                Indica que esta configurado el modo tipo acceso para
                                acceder a las VLAN.

switchport access vlan 2
                                Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000
                                Valor del ancho de banda del enlace en la interfaz.
!
interface FastEthernet0/3
                                Especifica interfaz fastethernet0/3.

switchport mode dynamic
                                Indica que esta configurado el modo tipo acceso para
                                acceder a las VLAN.

switchport access vlan 3
                                Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000
                                Valor del ancho de banda del enlace en la interfaz.
!
interface FastEthernet0/4
                                Especifica interfaz fastethernet0/4.

switchport mode dynamic
```

Indica que esta configurado el modo tipo acceso para acceder a las VLAN.

switchport access vlan 4

Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/5

Especifica interfaz fastethernet0/5.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/6

Especifica interfaz fastethernet0/6.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/7

Especifica interfaz fastethernet0/7.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/8

Especifica interfaz fastethernet0/8.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/9

Especifica interfaz fastethernet0/9.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/10
Especifica interfaz fastethernet0/10.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/11
Especifica interfaz fastethernet0/11.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/12
Especifica interfaz fastethernet0/12.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface GigabitEthernet0/1
Especifica la interfaz Gigabithernet0/1.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface GigabitEthernet0/2
Especifica la interfaz Gigabithernet0/2.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
vtp domain bigdomain
Especifica el dominio del puerto truncado virtual.

interface Vlan 1
Especifica la VLAN 1 (vlan por defecto).

ip address 192.168.22.2 255.255.255.248
Dirección IP de la vlan por defecto.

no ip route-cache
No almacena ip en el cache de rutas.

shutdown

vlan 2 name callcenter_sistemas
Indica VLAN configurada con su respectivo nombre.

vlan 3 name servidores
Indica VLAN configurada con su respectivo nombre.

vlan 4 name finanzas_caja
Indica VLAN configurada con su respectivo nombre.

!
ip classless
Indica acceso a las redes no remotas con mascara de sub-red diferente.

no ip http Server
Especifica que no existe un servidor http.

!
ip default-gateway 192.168.22.1
Indica interfaz de puerta de enlace para comunicar VLAN.

!
!
line con 0
Configuración Puerto de consola.

login
Activar configuración al inicio.

transport input none
Ningún transporte impuesto.

password cisco
Contraseña asignada.

line aux 0
Configuración Puerto auxiliar.

line vty 0 4
Configuración remota por telnet.

login
Activar configuración al inicio.

password cisco
Contraseña asignada.

!
no scheduler allocate

end
Fin del reporte de la configuración actual.

5.3.4.7 SHOW VLAN SWITCH SALINAS.

SW_SALINAS# sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14
2	callcenter	active	Fa0/4
3	servidores	active	Fa0/5
4	finanzas_caja	active	Fa0/6
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
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
4	enet	100004	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

VLAN: Identificación vlan.
Name: Nombre de vlan.
Status: Estado.
Ports: Puertos asignados a la vlan.
Type: Tipo de interfaces.
SIAD: Encabezado para identificar vlan.

MTU: Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes.

Parent: Parentela.
RingNo: Número de anillo si hay.
BridgeNO: Número de puente si hay.
Stp: STP usado
BrdgMode: Modo de puente.
Transx: TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

5.3.5 CONFIGURACIÓN ROUTER SAMBORONDÓN.

Router>**enable**

A nivel de modo usuario normal, digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

A nivel de modo usuario privilegiado, digitar el comando anterior para pasar a modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.
Aparece un mensaje que describe al usuario, que ingrese los comandos de configuración, línea por línea.

Router(config)#**hostname SAMBORONDON**

En el modo de configuración general, digitar el comando anterior para establecer el nombre del dispositivo.

SAMBORONDON(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado, digitar el comando anterior.

SAMBORONDON(config)#**enable secret cisco**

También para establecer puntos de seguridad se debe encriptar la contraseña con el protocolo de encriptación md5 con el comando anterior.

5.3.5.1 CONFIGURACIÓN DE INTERFACES SERIAL.

SAMBORONDON(config)#**interface serial 0**

Digite el comando anterior para configurar la interfaz serial 0.

SAMBORONDON(config-if)#**description CONEXIÓN AL ROUTER PROSPERINA**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

SAMBORONDON(config-if)#**ip address** 192.168.20.6 255.255.255.252

Para asignar una dirección IP y máscara de sub-red al puerto, se debe digitar el comando anterior.

SAMBORONDON(config-if)#**clock rate 56000**

Digitar éste comando para indicar la velocidad del puerto en bps. Se necesita incluir éste comando ya que está definido como DCE.

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

Para habilitar administrativamente el puerto, se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

SAMBORONDON(config)#**interface serial 1**

Digite el comando anterior para configurar la interfaz serial 0.

SAMBORONDON(config-if)#**description CONEXIÓN AL ROUTER BABAHOYO**

Para agregar un comentario como guía se debe ingresar el comando anterior.

SAMBORONDON(config-if)#**ip address** 192.168.20.38 255.255.255.252

Para asignar una dirección IP y máscara de sub-red al puerto se debe digitar el comando anterior.

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

Para habilitar administrativamente el puerto se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

5.3.5.2 GUARDAR LA CONFIGURACIÓN DEL ROUTER.

Se debe salir de la configuración de la interfaz a modo de usuario privilegiado para guardar los cambios hechos en la configuración del router.

SAMBORONDON#**copy running-config startup-config**

Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

El mensaje anterior significa que se está guardando la configuración.

[OK]

Luego aparece un mensaje de aprobación.

5.3.5.3 CONFIGURACIÓN DE SUB INTERFACES.

SAMBORONDON# **configure terminal**

A nivel de modo usuario privilegiado, digitar el comando anterior para pasar a modo de configuración general.

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

Aparece un mensaje que describe al usuario que ingrese los comandos de configuración, línea por línea.

SAMBORONDON(config)#**interface fastethernet0/0.1**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.1.

SAMBORONDON(config-subif)#**description VLAN POR DEFECTO SAMBORONDON**

Para agregar un comentario como guía se debe ingresar el comando anterior.

SAMBORONDON(config-subif)#**encapsulation dot1q 1**

Para definir el tipo de encapsulamiento se debe ingresar el comando anterior.

SAMBORONDON(config-subif)#**ip address** 192.168.23.1 255.255.255.248

Para asignar una dirección IP y máscara de sub-red a la sub interfaz, se debe digitar lo anterior.

SAMBORONDON(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto se debe ingresar lo anterior.

SAMBORONDON(config-subif)#**interface fastethernet0/0.2**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.2

SAMBORONDON(config-subif)#**description VLAN VENTAS SAMBORONDON**

Para agregar un comentario como guía se debe ingresar el comando anterior.

SAMBORONDON(config-subif)#**encapsulation dot1q 2**

Para definir el tipo de encapsulamiento se debe ingresar el comando anterior.

SAMBORONDON(config-subif)#**ip address** 192.168.23.9 255.255.255.248

Para asignar una dirección IP y máscara de sub-red a la sub interfaz, digite el comando anterior.

SAMBORONDON(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto se debe ingresar lo anterior.

SAMBORONDON(config-subif)#**interface fastethernet0/0.3**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.3.

SAMBORONDON(config-subif)#**description VLAN SOPORTE_T SAMBORONDON**

Para agregar un comentario como guía se debe ingresar el comando anterior.

SAMBORONDON(config-subif)#**encapsulation dot1q 3**

Para definir el tipo de encapsulamiento se debe ingresar el comando anterior.

SAMBORONDON(config-subif)#**ip address 192.168.23.17 255.255.255.248**

Para asignar una dirección IP y máscara de sub-red a la sub interfaz digite lo anterior.

SAMBORONDON(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

SAMBORONDON(config-subif)#**interface fastethernet0/0.4**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.4.

SAMBORONDON(config-subif)#**description VLAN SERVIDORES SAMBORONDON**

Para agregar un comentario como guía ingrese el comando anterior.

SAMBORONDON(config-subif)#**encapsulation dot1q 4**

Para definir el tipo de encapsulamiento se debe ingresar el comando anterior.

SAMBORONDON(config-subif)#**ip address 192.168.23.25 255.255.255.248**

Para asignar una dirección IP y máscara de sub-red a la sub interfaz digite lo anterior.

SAMBORONDON(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto se debe ingresar lo anterior.

5.3.5.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2.

SAMBORONDON(config-if)#**router rip**

Se debe habilitar el protocolo de enrutamiento con el comando anterior.

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

Se debe especificar la versión del protocolo de enrutamiento.

SAMBORONDON(config -router)#**network 192.168.20.0**
SAMBORONDON(config -router)#**network 192.168.22.0**
SAMBORONDON(config -router)#**network 192.168.23.0**
SAMBORONDON(config -router)#**network 192.168.24.0**
SAMBORONDON(config -router)#**network 192.168.25.0**

Una vez activado el protocolo de enrutamiento es preciso indicar qué redes enrutar.
Asigne las redes que seguirán el protocolo.

5.3.5.5 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

SAMBORONDON(config)#**line vty 0 4**

Habilitar el acceso por terminal virtual.

SAMBORONDON(config -line)#**password cisco**

Se debe ingresar la contraseña.

SAMBORONDON(config -line)#**login**

Activar al inicio.

SAMBORONDON(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

SAMBORONDON(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual.

SAMBORONDON(config)#**line con 0**

Habilitar del acceso por consola.

SAMBORONDON(config -line)#**password cisco**

Se debe ingresar la contraseña.

SAMBORONDON(config -line)#**login**

Activar al inicio.

Con el mismo procedimiento puede configurarse una password para acceder por el puerto auxiliar. Tanto el puerto de consola como el auxiliar, no requieren autenticación de password por defecto.

5.3.5.6 GUARDAR LA CONFIGURACIÓN DEL ROUTER.

%SYS-5-CONFIG_I: Configured from console by console

Cuando hace realiza éste procedimiento, aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

SAMBORONDON#**copy running-config startup-config**

Digitando el comando anterior, se guardará la configuración actual a la configuración de inicio.

Building configuration...

El siguiente mensaje significa que se está guardando la configuración.

[OK]

Ahora aparece un mensaje de aprobación.

5.3.5.7 SHOW RUN ROUTER SAMBORONDÓN.

SAMBORONDON#sh run
Building configuration...

!
Version 12.1

Indica la versión del IOS.

service timestamps debug uptime
service timestamps log uptime
service password-encryption

Indica que el servicio de encriptación de contraseña está activo.

!
hostname SAMBORONDON

Refleja el nombre que el administrador le ha asignado al router.

enable secret 5 sdf6978yhg$jnb76sd

Ésta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Ésta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
ip subnet-zero
!
interface Serial0

Especifica interfaz serial 0.

description CONEXION PROSPERINA

Descripción de la interfaz.

ip address 192.168.20.6 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
clock rate 56000

Indica la velocidad del puerto en bits por segundo.

bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

!
interface Serial1

Especifica interfaz serial 0.

description CONEXION BABAHOYO

Descripción de la interfaz.

ip address 192.168.20.38 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda del enlace.

!
interface FastEthernet0/0

Especifica interfaz fastethernet 0 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace.

Shutdown

Indica interfaz no levantada.

!
interface FastEthernet0/0.1

Especifica sub interfaz fastetehrnet 0.1 slot 0.

description VLAN POR DEFECTO

Descripción de la interfaz.

encapsulation dot1q 1

Define el tipo de encapsulamiento asignado a la VLAN 1.

ip address 192.168.23.1 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!
interface FastEthernet0/0.2

Especifica sub interfaz fastethernet 0.2 slot 0.

description VLAN VENTAS SAMBORONDON

Descripción de la interfaz.

encapsulation dot1q 2

Define el tipo de encapsulamiento asignado a la VLAN 2.

ip address 192.168.23.9 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!
interface FastEthernet0/0.3

Especifica sub interfaz fastetehrnet 0.3 slot 0.

description VLAN SOPORTE_T

Descripción de la interfaz

encapsulation dot1q 3

Define el tipo de encapsulamiento asignado a la VLAN 3.

ip address 192.168.23.17 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!
interface FastEthernet0/0.4

Especifica sub interfaz fastetehrnet 0.4 slot 0.

description VLAN SERVIDORES

Descripción de la interfaz.

encapsulation dot1q 4

Define el tipo de encapsulamiento asignado a la VLAN 4.

ip address 192.168.23.25 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!
interface FastEthernet0/1

Especifica interfaz fastethernet 1 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
router rip

Indica que se ha configurado el protocolo de enrutamiento rip.

version 2

Define la versión 2 del protocolo de enrutamiento.

network 192.168.20.0
network 192.168.22.0
network 192.168.23.0
network 192.168.24.0
network 192.168.25.0

Indica qué redes enruta nuestro protocolo de enrutamiento.

!
ip classless

Indica acceso a las redes no remotas con máscara de sub-red diferente.

no ip http Server

Especifica que no existe un servidor http.

!
line con 0

Configuración Puerto de consola.

Login

Activar configuración al inicio.

transport input none

Ningún transporte impuesto.

password cisco

Contraseña asignada.

line aux 0

Configuración Puerto auxiliar.

line vty 0 4

Configuración remota por telnet.

Login

Activar configuración al inicio.

password cisco

Contraseña asignada.

!
no scheduler allocate

end

Fin del reporte de la configuración actual.

5.3.5.8 SHOW IP ROUTE SAMBORONDÓN.

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

Gateway of last resort is not set

192.168.20.0/30 is subnetted, 6 subnets
192.168.23.0/29 is subnetted, 4 subnets
192.168.24.0/29 is subnetted, 4 subnets
192.168.22.0/29 is subnetted, 4 subnets
192.168.25.0/29 is subnetted, 4 subnets
192.168.21.0/29 is subnetted, 5 subnets

192.168.x.x: Indica la red. **/x:** el nivel de segmentación. **x subnets:** el número de sub-redes en las cuales se encuentra dividida.

C 192.168.20.36 is directly connected, Serial1
C 192.168.20.4 is directly connected, Serial0
C 192.168.23.0 is directly connected, 192.168.23.1
C 192.168.23.8 is directly connected, 192.168.23.9
C 192.168.23.16 is directly connected, 192.168.23.17
C 192.168.23.24 is directly connected, 192.168.23.25

C: Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectada y **Serialx:** la interfaz de salida por la cual accede a la red de destino.

```
R    192.168.20.32 [120/1] via 192.168.20.37, 00:02:24, Serial1
R    192.168.20.8 [120/1] via 192.168.20.5, 00:07:38, Serial0
R    192.168.20.12 [120/1] via 192.168.20.5, 00:08:25, Serial0
R    192.168.20.0 [120/1] via 192.168.20.5, 00:02:33, Serial0
R    192.168.24.0 [120/1] via 192.168.20.37, 00:06:35, Serial1
R    192.168.24.8 [120/1] via 192.168.20.37, 00:06:17, Serial1
R    192.168.24.16 [120/1] via 192.168.20.37, 00:01:25, Serial1
R    192.168.24.24 [120/1] via 192.168.20.37, 00:07:36, Serial1
R    192.168.22.0 [120/2] via 192.168.20.5, 00:05:41, Serial0
R    192.168.22.8 [120/2] via 192.168.20.5, 00:02:27, Serial0
R    192.168.22.16 [120/2] via 192.168.20.5, 00:09:27, Serial0
R    192.168.22.24 [120/2] via 192.168.20.5, 00:09:42, Serial0
R    192.168.25.0 [120/2] via 192.168.20.5, 00:07:17, Serial0
R    192.168.25.8 [120/2] via 192.168.20.5, 00:08:26, Serial0
R    192.168.25.16 [120/2] via 192.168.20.5, 00:06:30, Serial0
R    192.168.25.24 [120/2] via 192.168.20.5, 00:03:34, Serial0
R    192.168.21.0 [120/10] via 192.168.20.5, 00:04:37, Serial0
R    192.168.21.8 [120/10] via 192.168.20.5, 00:07:17, Serial0
R    192.168.21.16 [120/10] via 192.168.20.5, 00:08:23, Serial0
R    192.168.21.24 [120/10] via 192.168.20.5, 00:03:31, Serial0
R    192.168.21.32 [120/10] via 192.168.20.5, 00:06:33, Serial0
```

R: Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), 192.168.x.x la dirección de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **Serialx:** la interfaz de salida.

5.3.6 CONFIGURACIÓN SWITCH SAMBORONDÓN.

Switch>**enable**

A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado

Switch#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general

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

Aparecen unas líneas que describe al usuario que ingrese los comandos de configuración, uno a uno.

Switch(config)#**hostname SW_SAMBORONDON**

En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

SW_SAMBORONDON(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado digitar el comando anterior.

SW_SAMBORONDON(config)#**enable secret cisco**

También para establecer puntos de seguridad se encripta la contraseña con el protocolo de encriptación.

SW_SAMBORONDON(config)#**ip default-gateway 192.168.23.1**

Asigna al switch esta ip como puerta de enlace por defecto.

5.3.6.1 CONFIGURACIÓN DE INTERFAZ VLAN 1 (INTERFAZ VLAN POR DEFECTO).

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

Se debe ingresar a la interfaz vlan por defecto (vlan 1).

SW_SAMBORONDON(config-if)#**ip address 192.168.23.2 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub-interfaz digitar lo anterior.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

5.3.6.2 CREACIÓN DE VLAN.

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general.

SW_SAMBORONDON(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

SW_SAMBORONDON#**vlan database**

Permite ingresar a la base de datos de las VLAN.

SW_SAMBORONDON(vlan)#**vlan 2 name VENTAS**

Crea la vlan dos con el nombre especificado.

SW_SAMBORONDON(vlan)#**vlan 3 name SOPORTE_T**

Crea la vlan tres con el nombre especificado.

SW_SAMBORONDON(vlan)#**vlan 4 name SERVIDORES**

Crea la vlan cuatro con el nombre especificado.

5.3.6.3 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

SW_SAMBORONDON(vlan)#**exit**

Para salir de la base de datos de las VLAN.

SW_SAMBORONDON#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general.

SW_SAMBORONDON(config)#**interface fastethernet 0/4**

Digite el comando anterior para configurar la interfaz fastethernet 0/4.

SW_SAMBORONDON(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_SAMBORONDON(config -if)#**switchport access vlan 2**

Agrega este puerto a la vlan especificada..

SW_SAMBORONDON(config)#**interface fastethernet 0/5**

Digite el comando anterior para configurar la interfaz fastethernet 0/5.

SW_SAMBORONDON(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_SAMBORONDON(config -if)#**switchport access vlan 3**

Agrega este puerto a la vlan especificada.

SW_SAMBORONDON(config)#**interface fastethernet 0/6**

Digite el comando anterior para configurar la interfaz fastethernet 0/6.

SW_SAMBORONDON(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_SAMBORONDON(config -if)#**switchport access vlan 4**

Agrega este puerto a la vlan especificada.

5.3.6.4 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general.

SW_SAMBORONDON(config)#**line vty 0 15**
Habilita del acceso por terminal virtual.

SW_SAMBORONDON(config -line)#**password cisco**
Se registra la contraseña.

SW_SAMBORONDON(config -line)#**login**
Activar al inicio.

SW_SAMBORONDON(config -line)#**exec-timeout 5 0**
El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

SW_SAMBORONDON(config -line)#**exit**
Se debe salir de la configuración de la Terminal virtual.

SW_SAMBORONDON(config)#**line con 0**
Habilita el acceso por consola.

SW_SAMBORONDON(config -line)#**password cisco**
Se debe iregistrar la contraseña.

SW_SAMBORONDON(config -line)#**login**
Activar al inicio.

5.3.6.5 GUARDAR CONFIGURACIONES HECHAS EN EL SWITCH.

SW_SAMBORONDON(config -line)#**exit**
Digitar lo anterior para salir del modo configuración de consola a modo configuración general.

SW_SAMBORONDON(config)#**exit**
Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

%SYS-5-CONFIG_I: Configured from console by console
Cuando se hace este procedimiento aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

SW_SAMBORONDON#**copy running-config startup-config**
Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

El siguiente mensaje significa que se esta guardando la configuración.

[OK]

Ahora aparece un mensaje de aprobación.

5.3.6.6 SHOW RUN SWITCH SAMBORONDÓN.

SW_SAMBORONDON#sh run
!
Version 12.1

Indica la versión del IOS

service timestamps debug uptime
service timestamps log uptime
service password-encryption

Indica que el servicio de encriptación de contraseña esta activo.

!
hostname SW_SAMBORONDON

Refleja el nombre que el administrador le ha asignado al router.

ip name-server 0.0.0.0
enable secret 5 sdf6978yhg$jnb76sd

Esta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Esta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
!
!
ip subnet-zero

!
!
!
!
!
!
spanning-tree extend system-id

Para usar red sin bucles, rutas cortas.

!
!
!
!
interface FastEthernet0/1

Especifica interfaz fastethernet0/1.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface FastEthernet0/2

Especifica la interfaz fastethernet0/2.

switchport mode dynamic

Indica que esta configurado el modo tipo acceso para acceder a las VLAN.

switchport access vlan 2

Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface FastEthernet0/3

Especifica interfazfastethernet0/3.

switchport mode dynamic

Indica que esta configurado el modo tipo acceso para acceder a las VLAN.

switchport access vlan

Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface FastEthernet0/4

Especifica interfaz fastethernet0/4.

switchport mode dynamic

Indica que esta configurado el modo tipo acceso para acceder a las VLAN.

switchport access vlan 4

Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface FastEthernet0/5

Especifica interfaz fastethernet0/5.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/6
Especifica interfaz fastethernet0/6.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/7
Especifica interfaz fastethernet0/7.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/8
Especifica interfaz fastethernet0/8.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/9
Especifica interfaz fastethernet0/9.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/10
Especifica interfaz fastethernet0/10.

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface FastEthernet0/11

Especifica interfaz fastethernet0/11.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface FastEthernet0/12

Especifica interfaz fastethernet0/12.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface GigabitEthernet0/1

Especifica la interfaz Gigabithernet0/1.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

interface GigabitEthernet0/2

Especifica la interfaz Gigabithernet0/2.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!

vtp domain bigdomain

Especifica el dominio del puerto truncad virtual.

interface Vlan 1

Especifica la VLAN 1 (vlan por defecto).

ip address 192.168.23.2 255.255.255.248

Dirección IP de la vlan por defecto.

no ip route-cache No almacena ip en el cache de rutas..

shutdown

vlan 2 name ventas

Indica VLAN configurada con su respectivo nombre.

vlan 3 name soporte_t

Indica VLAN configurada con su respectivo nombre.

vlan 4 name servidores

Indica VLAN configurada con su respectivo nombre.

!
ip classless

Indica acceso a las redes no remotas con mascara de sub-red diferente.

no ip http Server

Especifica que no existe un servidor http.

!
!
!
line con 0

Configuración Puerto de consola.

login

Activar configuración al inicio.3

transport input none

Ningún transporte impuesto.

password cisco

Contraseña asignada.

line aux 0

Configuración Puerto auxiliar.

line vty 0 4

Configuración remota por telnet.

login

Activar configuración al inicio.

password cisco

Contraseña asignada.

!
no scheduler allocate

end

Fin del reporte de la configuración actual.

5.3.6.7 SHOW VLAN SWITCH SAMBORONDÓN.

SW_SAMBORONDON# sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14
2	ventas	active	Fa0/4
3	soporte_t	active	Fa0/5
4	servidores	active	Fa0/6
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
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
4	enet	100004	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

VLAN: Identificación vlan
Name: Nombre de vlan
Status: Estado
Ports: Puertos asignados a la vlan
Type: Tipo de interfaces
SIAD: Encabezado para identificar vlan
MTU: Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes.

Parent: Parentela
RingNo: Número de anillo si hay
BridgeNO: Número de puente si hay
Stp: STP usado
BrdgMode: Modo de puente
Transx: TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

5.3.7 CONFIGURACIÓN ROUTER BABAHOYO.

Router>**enable**

A nivel de modo usuario normal digite el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

A nivel de modo usuario privilegiado digite el comando anterior para pasar a modo de configuración general.

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

Aparece un comando que describe al usuario que ingrese los comandos de configuración, línea por línea.

Router(config)#**hostname SALINAS**

En el modo de configuración general, digitar el comando anterior para establecer el nombre del dispositivo.

BABAHOYO(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado digite el comando anterior.

BABAHOYO(config)#**enable secret cisco**

También para establecer puntos de seguridad encripte la contraseña con el protocolo de encriptación md5 con el comando anterior.

5.3.7.1 CONFIGURACIÓN DE INTERFACES SERIAL.

BABAHOYO(config)#**interface serial 0**

Digite el comando anterior para configurar la interfaz serial 0.

BABAHOYO(config-if)#**description CONEXIÓN AL ROUTER SAMBORONDON**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

BABAHOYO(config-if)#**ip address 192.168.20.37 255.255.255.252**

Para asignar una dirección IP y máscara de subred al puerto digite lo anterior.

BABAHOYO(config-if)#**clock rate 56000**

Digite el comando anterior para indicar la velocidad del puerto en bps. Se necesita incluir éste comando ya que está definido como DCE.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

BABAHOYO(config-if)#**interface serial 1**

Digite el comando anterior para configurar la interfaz serial 0.

BABAHOYO(config-if)#**description CONEXIÓN AL ROUTER PROSPERINA**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

BABAHOYO(config-if)#**ip address 192.168.20.14 255.255.255.252**

Para asignar una dirección IP y máscara de subred al puerto digite lo anterior.

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

Para habilitar administrativamente el puerto se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

BABAHOYO(config-if)#**interface serial 2**

Digite el comando anterior para configurar la interfaz serial 0.

BABAHOYO(config-if)#**description CONEXIÓN AL ROUTER PENAS**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

BABAHOYO(config-if)#**ip address 192.168.20.33 255.255.255.252**

Para asignar una dirección IP y máscara de subred al puerto digite lo anterior.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

5.3.7.2 GUARDAR LOS CAMBIOS HECHOS EN LA CONFIGURACIÓN DEL ROUTER.

luego Se debe salir de la configuración de la interfaz a modo de usuario privilegiado para guardar los cambios hechos en la configuración del router.

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

Digite lo anterior para salir del modo configuración de interfaz a modo configuración general.

BABAHOYO(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

%SYS-5-CONFIG_I: Configured from console by console

Cuando se realiza éste procedimiento, aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

BABAHOYO#**copy running-config startup-config**

Con el comando anterior guarde la configuración actual a la configuración de inicio.

Building configuration...

El mensaje anterior significa que se está guardando la configuración.

[OK]

Luego aparece un mensaje de aprobación.

5.3.7.3 CONFIGURACIÓN DE SUB INTERFACES.

BABAHOYO# **configure terminal**

A nivel de modo usuario privilegiado digite el comando anterior para pasar a modo de configuración general.

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

Aparece un mensaje que describe al usuario que ingrese los comandos de configuración, línea por línea.

BABAHOYO(config)#**interface fastethernet0/0.1**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.1.

BABAHOYO(config-subif)#**description VLAN POR DEFECTO BABAHOYO**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

BABAHOYO(config-subif)#**encapsulation dot1q 1**

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

BABAHOYO(config-subif)#**ip address 192.168.24.1 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub interfaz digite lo anterior.

BABAHOYO(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

BABAHOYO(config-subif)#**interface fastethernet0/0.2**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.2.

BABAHOYO(config-subif)#**description VLAN ADMINISTRACION BABAHOYO**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

BABAHOYO(config-subif)#**encapsulation dot1q 2**

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

BABAHOYO(config-subif)#**ip address 192.168.24.9 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub interfaz digite lo anterior.

BABAHOYO(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

BABAHOYO(config-subif)#**interface fastethernet0/0.3**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.3

BABAHOYO(config-subif)#**description VLAN SERVIDORES BABAHOYO**

Para agregar un comentario como guía Se debe ingresar el comando anterior

BABAHOYO(config-subif)#**encapsulation dot1q 3**

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

BABAHOYO(config-subif)#**ip address 192.168.24.17 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub interfaz digite lo anterior

BABAHOYO(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

BABAHOYO(config-subif)#**interface fastethernet0/0.4**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.4

BABAHOYO(config-subif)#**description VLAN SISTEMAS BABAHOYO**

Para agregar un comentario como guía Se debe ingresar el comando anterior

BABAHOYO(config-subif)#**encapsulation dot1q 4**

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

BABAHOYO(config-subif)#**ip address 192.168.24.25 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub interfaz digite lo anterior

BABAHOYO(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

5.3.7.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP V2.

BABAHOYO(config-subif)#**exit**

Digite lo anterior para salir del modo configuración de interfaz a modo configuración general

BABAHOYO# **configure Terminal**

A nivel de modo usuario privilegiado digite el comando anterior para pasar a modo de configuración general

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

Aparece un commando que describe al usuario que ingrese los comandos de configuración, línea por línea

BABAHOYO(config-if)#**router rip**

Se debe habilitar el protocolo de enrutamiento con el comando anterior

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

Se debe especificar la versión del protocolo de enrutamiento

BABAHOYO(config -router)#**network 192.168.20.0**
BABAHOYO(config -router)#**network 192.168.22.0**
BABAHOYO(config -router)#**network 192.168.23.0**
BABAHOYO(config -router)#**network 192.168.24.0**
BABAHOYO(config -router)#**network 192.168.25.0**

Una vez activado el protocolo de enrutamiento es preciso indicar qué redes enrutar.
Asigne las redes que seguirán el protocolo

5.3.7.5 HABILITAR EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

BABAHOYO(config -router)#**exit**

Se debe salir de modo de configuración de protocolo a modo de configuración general

BABAHOYO(config)#**line vty 0 4**

Habilitación del acceso por terminal virtual

BABAHOYO(config -line)#**password cisco**

Se debe ingresar la contraseña

BABAHOYO(config -line)#**login**

Activar al inicio

BABAHOYO(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

BABAHOYO(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual

BABAHOYO(config)#**line con 0**

Habilitación del acceso por consola

BABAHOYO(config -line)#**password cisco**

Se debe ingresar la contraseña

BABAHOYO(config -line)#**login**

Activar al inicio

Con el mismo procedimiento puede configurarse una password para acceder por el puerto auxiliar. Tanto el puerto consola como el auxiliar, no requieren autenticación de password por defecto.

5.3.7.6 GUARDAR LA CONFIGURACIÓN DEL ROUTER.

BABAHOYO(config -line)#**exit**

Digite lo anterior para salir del modo configuración de consola a modo configuración general

BABAHOYO(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado

%SYS-5-CONFIG_I: Configured from console by console

Cuando se realiza éste procedimiento, aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

BABAHOYO#**copy running-config startup-config**

Con el comando anterior guarde la configuración actual a la configuración de inicio

Building configuration...

El siguiente mensaje significa que se está guardando la configuración

[OK]

Ahora aparece un mensaje de aprobación

5.3.7.7 SHOW RUN ROUTER BABAHOYO.

BABAHOYO#sh run
Building configuration...

!
Version 12.1

Indica la versión del IOS.

service timestamps debug uptime
service timestamps log uptime

service password-encryption

Indica que el servicio de encriptación de contraseña está activo.

!
hostname BABAHOYO

Refleja el nombre que el administrador le ha asignado al router.

enable secret 5 sdf6978yhg$jnb76sd

Ésta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Ésta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
ip subnet-zero
!
!
interface Serial0

Especifica interfaz serial 0.

description CONEXIÓN SAMBORONDON

Descripción de la interfaz.

ip address 192.168.20.37 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
clock rate 56000

Indica la velocidad del puerto en bits por segundo.

bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

!
interface Serial1

Especifica interfaz serial 1.

description CONEXIÓN PROSPERINA

Descripción de la interfaz.

ip address 192.168.20.14 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
clock rate 56000

Indica la velocidad del puerto en bits por segundo.

bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

!
interface Serial2

Especifica interfaz serial 2.

description CONEXIÓN PENAS

Descripción de la interfaz.

ip address 192.168.20.33 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/0

Especifica interfaz fastethernet 0 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
interface FastEthernet0/0.1

Especifica la sub interfaz fastetehrnet 0.1 slot 0.

description VLAN POR DEFECTO BABAHO

Descripción de la interfaz.

encapsulation dot1q 1

Define el tipo de encapsulamiento asignado a la VLAN 1.

ip address 192.168.24.1 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!
interface FastEthernet0/0.2

Especifica sub interfaz fastetehrnet 0.2 slot 0.

description VLAN ADMINISTRACION BABA

Descripción de la interfaz.

encapsulation dot1q 2

Define el tipo de encapsulamiento asignado a la VLAN 2.

ip address 192.168.24.9 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!

interface FastEthernet0/0.3

Especifica sub interfaz fastetehrnet 0.3 slot 0.

description VLAN SERVIDORES BABAHOYO

Descripción de la interfaz

encapsulation dot1q 3

Define el tipo de encapsulamiento asignado a la VLAN 3.

ip address 192.168.24.17 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!

interface FastEthernet0/0.4

Especifica sub interfaz fastetehrnet 0.4 slot 0.

description VLAN SISTEMAS BABAHOYO

Descripción de la interfaz.

encapsulation dot1q 4

Define el tipo de encapsulamiento asignado a la VLAN 3.

ip address 192.168.24.25 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!

interface FastEthernet0/1

Especifica interfaz fastethernet 1 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda.

Shutdown	Indica interfaz no levantada.
!	
router rip	Indica que se ha configurado el protocolo de enrutamiento rip
version 2	Define la versión 2 del protocolo de enrutamiento
network 192.168.20.0 network 192.168.22.0 network 192.168.23.0 network 192.168.24.0 network 192.168.25.0	Indica qué redes enruta nuestro protocolo de enrutamiento.
!	
ip classless	Indica acceso a las redes no remotas con máscara de sub-red diferente.
no ip http Server	Especifica que no existe un servidor http.
! ! !	
line con 0	Configuración Puerto de consola.
Login	Activar configuración al inicio.
transport input none	Ningún transporte impuesto.
password cisco	Contraseña asignada.
line aux 0	Configuración Puerto auxiliar.
line vty 0 4	Configuración remota por telnet.
Login	Activar configuración al inicio.
password cisco	Contraseña asignada.
!	

no scheduler allocate

end

Fin del reporte de la configuración actual.

5.3.7.8 SHOW IP ROUTE BABAHOYO.

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

Gateway of last resort is not set

192.168.20.0/30 is subnetted, 6 subnets
192.168.24.0/29 is subnetted, 4 subnets
192.168.25.0/29 is subnetted, 4 subnets
192.168.21.0/29 is subnetted, 5 subnets
192.168.23.0/29 is subnetted, 4 subnets
192.168.22.0/29 is subnetted, 4 subnets

192.168.x.x: Indica la red / **x:** el nivel de segmentación y **x subnets:** el número de sub-redes en las cuales se encuentra dividida.

C 192.168.20.32 is directly connected, Serial2
C 192.168.20.36 is directly connected, Serial0
C 192.168.20.12 is directly connected, Serial1
C 192.168.24.0 is directly connected, 192.168.24.1
C 192.168.24.8 is directly connected, 192.168.24.9
C 192.168.24.16 is directly connected, 192.168.24.17
C 192.168.24.24 is directly connected, 192.168.24.25

C: Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serialx:** la interfaz de salida por la cual se accede a la red de destino.

R 192.168.20.8 [120/1] via 192.168.20.13, 00:05:16, Serial1
R 192.168.20.0 [120/1] via 192.168.20.13, 00:09:36, Serial1
R 192.168.20.4 [120/1] via 192.168.20.38, 00:06:14, Serial0
R 192.168.25.0 [120/1] via 192.168.20.34, 00:01:19, Serial2
R 192.168.25.8 [120/1] via 192.168.20.34, 00:04:24, Serial2
R 192.168.25.16 [120/1] via 192.168.20.34, 00:09:30, Serial2
R 192.168.25.24 [120/1] via 192.168.20.34, 00:09:30, Serial2
R 192.168.21.0 [120/10] via 192.168.20.13, 00:07:39, Serial1
R 192.168.21.8 [120/10] via 192.168.20.13, 00:07:15, Serial1

R 192.168.21.16 [120/10] via 192.168.20.13, 00:08:18, Serial1
R 192.168.21.24 [120/10] via 192.168.20.13, 00:02:36, Serial1
R 192.168.21.32 [120/10] via 192.168.20.13, 00:09:15, Serial1
R 192.168.23.0 [120/1] via 192.168.20.38, 00:03:14, Serial0
R 192.168.23.8 [120/1] via 192.168.20.38, 00:03:20, Serial0
R 192.168.23.16 [120/1] via 192.168.20.38, 00:09:20, Serial0
R 192.168.23.24 [120/1] via 192.168.20.38, 00:02:35, Serial0
R 192.168.22.0 [120/2] via 192.168.20.13, 00:07:37, Serial1
R 192.168.22.8 [120/2] via 192.168.20.13, 00:02:14, Serial1
R 192.168.22.16 [120/2] via 192.168.20.13, 00:08:25, Serial1
R 192.168.22.24 [120/2] via 192.168.20.13, 00:04:30, Serial1

R: Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), 192.168.x.x la dirección de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **Serialx:** la interfaz de salida.

5.3.8 CONFIGURACIÓN SWITCH BABAHOYO.

Switch>**enable**

A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general.

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

Aparece un comando que describe al usuario que ingrese los comandos de configuración, línea por línea.

Switch(config)#**hostname SW_BABAHOYO**

En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

SW_BABAHOYO(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado digitar el comando anterior.

SW_BABAHOYO(config)#**enable secret cisco**

También para establecer puntos de seguridad se encripta la contraseña con el protocolo de encriptación md5.

SW_BABAHOYO(config)#**ip default-gateway 192.168.24.1**

Asigna al switch esta ip como puerta de enlace por defecto.

5.3.8.1 CONFIGURACIÓN DE INTERFAZ VLAN 1 (INTERFAZ VLAN POR DEFECTO).

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

Se debe ingresar a la interfaz vlan por defecto (vlan 1).

SW_BABAHOYO(config-if)#**ip address 192.168.24.2 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub- interfaz digitar lo anterior.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

5.3.8.2 CREACIÓN DE VLAN.

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general

SW_BABAHOYO(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado

SW_BABAHOYO#**vlan database**

Permite ingresar a la base de datos de las VLAN

SW_BABAHOYO(vlan)#**vlan 2 name ADMINISTRACION**

Crea la vlan dos con el nombre especificado

SW_BABAHOYO(vlan)#**vlan 3 name SERVIDORES**

Crea la vlan tres con el nombre especificado

SW_BABAHOYO(vlan)#**vlan 4 name SISTEMAS**

Crea la vlan cuatro con el nombre especificado

5.3.8.3 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

SW_BABAHOYO(vlan)#**exit**

Para salir de la base de datos de las VLAN

SW_BABAHOYO#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general

SW_BABAHOYO(config)#**interface fastethernet 0/4**

Digite el comando anterior para configurar la interfaz fastethernet 0/4

SW_BABAHOYO(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN

SW_BABAHOYO(config -if)#**switchport access vlan 2**

Agrega este puerto a la vlan especificada.

SW_BABAHOYO(config)#**interface fastethernet 0/5**

Digite el comando anterior para configurar la interfaz fastethernet 0/5

SW_BABAHOYO(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN

SW_BABAHOYO(config -if)#**switchport access vlan 3**

Agrega este puerto a la vlan especificada.

SW_BABAHOYO(config)#**interface fastethernet 0/6**

Digite el comando anterior para configurar la interfaz fastethernet 0/6

SW_BABAHOYO(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN

SW_BABAHOYO(config -if)#**switchport access vlan 4**

Agrega este puerto a la vlan especificada.

5.3.8.4 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general

SW_BABAHOYO(config)#**line vty 0 15**

Habilita el acceso por terminal virtual

SW_BABAHOYO(config -line)#**password cisco**

Se debe ingresar la contraseña

SW_BABAHOYO(config -line)#**login**

Activar al inicio

SW_BABAHOYO(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

SW_BABAHOYO(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual

SW_BABAHOYO(config)#**line con 0**

Habilita el acceso por consola

SW_BABAHOYO(config -line)#**password cisco**

Se debe ingresar la contraseña

SW_BABAHOYO(config -line)#**login**

Activar al inicio

5.3.8.5 GUARDANDO LA CONFIGURACIÓN HECHA EN EL SWITCH.

SW_BABAHOYO(config -line)#**exit**

Digitar lo anterior para salir del modo configuración de consola a modo configuración general

SW_BABAHOYO(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado

%SYS-5-CONFIG_I: Configured from console by console

Cuando se hace este procedimiento aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

SW_BABAHOYO#**copy running-config startup-config**

Con el comando anterior se guarda la configuración actual a la configuración de inicio

Building configuration...

El siguiente mensaje significa que se esta guardando la configuración

[OK]

Ahora aparece un mensaje de aprobación

5.3.8.6 SHOW RUN SWITCH BABAHOYO.

SW_BABAHOYO#sh run
!
Version 12.1

Indica la versión del IOS

service timestamps debug uptime

service timestamps log uptime
service password-encryption
Indica que el servicio de encriptación de contraseña esta activo

!
hostname SW_BABAHOYO
Refleja el nombre que el administrador le ha asignado al router

ip name-server 0.0.0.0
enable secret 5 sdf6978yhg$jnb76sd
Esta línea especifica la contraseña encriptada por el protocolo md5

enable password cisco
Esta línea especifica una contraseña para ingreso al router en modo usuario privilegiado

!
!
!
ip subnet-zero

!
!
!
!
!
!
spanning-tree extend system-id
Para usar red sin bucles, rutas cortas
!
!
!
!
interface FastEthernet0/1
Especifica interfaz fastethernet0/1

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz

!
interface FastEthernet0/2
Especifica interfaz fastethernet0/2

switchport mode dynamic

Indica que esta configurado el modo tipo acceso para acceder a las VLAN

switchport access vlan 2

Especifica que esta interfaz es parte de la VLAN indicada

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz

!

interface FastEthernet0/3

Especifica interfaz fastethernet0/3

switchport mode dynamic

Indica que esta configurado el modo tipo acceso para acceder a las VLAN

switchport access vlan

Especifica que esta interfaz es parte de la VLAN indicada

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz

!

interface FastEthernet0/4

Especifica interfazfastethernet0/4

switchport mode dynamic

Indica que esta configurado el modo tipo acceso para acceder a las VLAN

switchport access vlan 4

Especifica que esta interfaz es parte de la VLAN indicada

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz

!

interface FastEthernet0/5

Especifica interfaz fastethernet0/5

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz

!

interface FastEthernet0/6

Especifica interfaz fastethernet0/6

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/7
Especifica interfaz fastethernet0/7

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/8
Especifica interfaz fastethernet0/8

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/9
Especifica interfaz fastethernet0/9

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/10
Especifica interfaz fastethernet0/10

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/11
Especifica interfaz fastethernet0/11

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/12
Especifica interfaz fastethernet0/12

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz

!
interface GigabitEthernet0/1
Especifica la interfaz Gigabithernet0/1

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz

!
interface GigabitEthernet0/2
Especifica la interfaz Gigabithernet0/2

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz

!
vtp domain bigdomain
Especifica el dominio del puerto truncado virtual

interface Vlan 1
Especifica la VLAN 1 (vlan por defecto)

ip address 192.168.24.2 255.255.255.248
Dirección IP de la vlan por defecto

no ip route-cache
No almacena ip en el cache de rutas

shutdown

vlan 2 name administración
Indica VLAN configurada con su respectivo nombre

vlan 3 name servidores
Indica VLAN configurada con su respectivo nombre

vlan 4 name sistemas
Indica VLAN configurada con su respectivo nombre

!
ip classless
Indica acceso a las redes no remotas con mascara de sub-red diferente

```
no ip http Server
                        Especifica que no existe un servidor http
!
ip default-gateway 192.168.24.1
                        Indica interfaz de puerta de enlace para comunicar VLAN
!
!

line con 0
                        Configuración Puerto de consola

login
                        Activar configuración al inicio

transport input none
                        Ningún transporte impuesto
password cisco
                        Contraseña asignada

line aux 0
                        Configuración Puerto auxiliar

line vty 0 4
                        Configuración remota por telnet

login
                        Activar configuración al inicio

password cisco
                        Contraseña asignada
!
no scheduler allocate

end
                        Fin del reporte de la configuración actual.
```

5.3.8.7 SHOW VLAN SWITCH BABAHOYO.

SW_BABAHOYO# sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14
2	administración	active	Fa0/4
3	servidores	active	Fa0/5
4	sistemas	active	Fa0/6

```
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
2    enet  100002     1500 -      -      -        -    -        0      0
3    enet  100003     1500 -      -      -        -    -        0      0
4    enet  100004     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
```

VLAN: Identificación vlan
Name: Nombre de vlan
Status: Estado
Ports: Puertos asignados a la vlan
Type: Tipo de interfaces
SIAD: Encabezado para identificar vlan
MTU: Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes

Parent: Parentela
RingNo: Número de anillo si hay
BridgeNO: Número de puente si hay
Stp: STP usado
BrdgMode: Modo de puente
Transx: TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

5.3.9 CONFIGURACIÓN ROUTER PEÑAS.

Router>**enable**

A nivel de modo usuario normal, digite el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

A nivel de modo usuario privilegiado, digite el comando anterior para pasar a modo de configuración general.

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

Aparece un comando que describe al usuario que ingrese los comandos de configuración, línea por línea.

Router(config)#**hostname PENAS**

En el modo de configuración general. digite el comando anterior para establecer el nombre del dispositivo.

PENAS(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado, digite el comando anterior.

PENAS(config)#**enable secret cisco**

También para establecer puntos de seguridad se debe encriptar la contraseña con el protocolo de encriptación md5 con el comando anterior.

5.3.9.1 CONFIGURACIÓN DE INTERFACES SERIAL.

PENAS(config)#**interface serial 0**

Digite el comando anterior para configurar la interfaz serial 0.

PENAS(config-if)#**description CONEXIÓN AL ROUTER BABAHOYO**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

PENAS(config-if)#**ip address 192.168.20.34 255.255.255.252**

Para asignar una dirección IP y máscara de sub-red al puerto, digite lo anterior.

PENAS(config-if)#**clock rate 56000**

Digite éste comando para indicar la velocidad del puerto en bps. Se necesita incluir éste comando ya que está definido como DCE.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

PENAS(config)#**interface serial 1**

Digite el comando anterior para configurar la interfaz serial 0.

PENAS(config-if)#**description CONEXIÓN AL ROUTER PROSPERINA**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

PENAS(config-if)#**ip address 192.168.20.10 255.255.255.252**

Para asignar una dirección IP y máscara de sub-red al puerto digite lo anterior.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

5.3.9.2 GUARDAR LA CONFIGURACIÓN DEL ROUTER.

luego Se debe salir de la configuración de la interfaz a modo de usuario privilegiado para guardar los cambios hechos en la configuración del router.

PENAS#**copy running-config startup-config**

Con el comando anterior guarde la configuración actual a la configuración de inicio.

Building configuration...

El mensaje anterior significa que se está guardando la configuración.

[OK]

Luego, aparece un mensaje de aprobación.

5.3.9.3 CONFIGURACIÓN DE SUB INTERFACES.

PENAS# **configure terminal**

A nivel de modo usuario privilegiado digite el comando anterior para pasar a modo de configuración general.

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

Aparece un mensaje que describe al usuario que ingrese los comandos de configuración, línea por línea.

PENAS(config)#**interface fastethernet0/0.1**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.1.

PENAS(config-subif)#**description VLAN POR DEFECTO PENAS**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

PENAS(config-subif)#**encapsulation dot1q 1**

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

PENAS(config-subif)#**ip address 192.168.25.1 255.255.255.248**

Para asignar una dirección IP y máscara de sub-red a la sub interfaz digite lo anterior.

PENAS(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

PENAS(config-subif)#**interface fastethernet0/0.2**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.2.

PENAS(config-subif)#**description VLAN MONITORES PENAS**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

PENAS(config-subif)#**encapsulation dot1q 2**

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

PENAS(config-subif)#**ip address 192.168.25.9 255.255.255.248**

Para asignar una dirección IP y máscara de sub-red a la sub interfaz digite lo anterior.

PENAS(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

PENAS(config-subif)#**interface fastethernet0/0.3**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.3.

PENAS(config-subif)#**description VLAN SERVIDORES PENAS**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

PENAS(config-subif)#**encapsulation dot1q 3**

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

PENAS(config-subif)#**ip address 192.168.25.17 255.255.255.248**

Para asignar una dirección IP y máscara de sub-red a la sub interfaz digite lo anterior.

PENAS(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

PENAS(config-subif)#**interface fastethernet0/0.4**

Digite el comando anterior para configurar la sub interfaz FastEthernet0/0.4.

PENAS(config-subif)#**description VLAN SISTEMAS PENAS**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

PENAS(config-subif)#encapsulation dot1q 4

Para definir el tipo de encapsulamiento Se debe ingresar el comando anterior.

PENAS(config-subif)#**ip address 192.168.25.25 255.255.255.248**

Para asignar una dirección IP y máscara de sub-red a la sub interfaz digite lo anterior.

PENAS(config-subif)#**no shutdown**

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

5.3.9.4 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2.

PENAS(config-if)#**router rip**

Se debe habilitar el protocolo de enrutamiento con el comando anterior.

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

Se debe especificar la versión del protocolo de enrutamiento.

PENAS(config -router)#**network 192.168.20.0**
PENAS(config -router)#**network 192.168.22.0**
PENAS(config -router)#**network 192.168.23.0**
PENAS(config -router)#**network 192.168.24.0**
PENAS(config -router)#**network 192.168.25.0**

Una vez activado el protocolo de enrutamiento es preciso indicar qué redes enrutar.
Asigne las redes que seguirán el protocolo.

5.3.9.5 HABILITAR EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

PENAS(config -router)#**exit**

Se debe salir de modo de configuración de protocolo a modo de configuración general.

PENAS(config)#**line vty 0 4**

Habilitación del acceso por terminal virtual.

PENAS(config -line)#**password cisco**

Se debe ingresar la contraseña.

PENAS(config -line)#**login**

Activar al inicio.

PENAS(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

PENAS(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual.

PENAS(config)#**line con 0**

Habilitación del acceso por consola.

PENAS(config -line)#**password cisco**

Se debe ingresar la contraseña.

PENAS(config -line)#**login**

Activar al inicio.

Con el mismo procedimiento puede configurarse una password para acceder por el puerto auxiliar. Tanto el puerto de consola como el auxiliar, no requieren autenticación de password por defecto.

5.3.9.6 GUARDAR LA CONFIGURACIÓN DEL ROUTER.

PENAS#**copy running-config startup-config**

Con el comando anterior guarde la configuración actual a la configuración de inicio.

Building configuration...

El siguiente mensaje significa que se está guardando la configuración.

[OK]

Ahora aparece un mensaje de aprobación.

5.3.9.7 SHOW RUN ROUTER PEÑAS.

PENAS#sh run
Building configuration...

!
Version 12.1
Indica la versión del IOS

service timestamps debug uptime
service timestamps log uptime
service password-encryption
Indica que el servicio de encriptación de contraseña está activo.

!
hostname PENAS
Refleja el nombre que el administrador le ha asignado al router.

enable secret 5 sdf6978yhg$jnb76sd
Ésta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco
Ésta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
ip subnet-zero
!
interface Serial0
Especifica interfaz serial 0.

description CONEXIÓN BABAHOYO
Descripción de la interfaz.

ip address 192.168.20.34 255.255.255.252
Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
bandwidth 1544
Valor del ancho de banda del enlace en la interfaz.

!
interface Serial1
Especifica interfaz serial 1.

description CONEXIÓN PROSPERINA
Descripción de la interfaz.
ip address 192.168.20.10 255.255.255.252

Dirección ip y máscara de de sub-red de la interfaz.

```
 no ip directed-broadcast
 bandwidth 1544
```

Valor del ancho de banda de la Interfaz.

```
!
interface FastEthernet0/0
```

Especifica interfaz fastethernet 0 slot 0.

```
no ip address
```

Sin dirección ip asignada.

```
no ip directed-broadcast
bandwidth 100000
```

Valor del ancho de banda de la Interfaz.

```
Shutdown
```

Indica interfaz no levantada.

```
!
interface FastEthernet0/0.1
```

Especifica sub interfaz fastetehrnet 0.1 slot 0.

```
description VLAN POR DEFECTO PENAS
```

Descripción de la interfaz.

```
encapsulation dot1q 1
```

Define el tipo de encapsulamiento asignado a la VLAN 1.

```
ip address 192.168.25.1 255.255.255.248
```

Dirección ip y máscara de de sub-red de la sub interfaz.

```
!
interface FastEthernet0/0.2
```

Especifica la sub interfaz fastetehrnet 0.2 slot 0.

```
description VLAN MONITORES PENAS
```

Descripción de la interfaz.

```
encapsulation dot1q 2
```

Define el tipo de encapsulamiento asignado a la VLAN 2.

```
ip address 192.168.25.9 255.255.255.248
```

Dirección ip y máscara de de sub-red de la sub interfaz.

```
!
interface FastEthernet0/0.3
```

Especifica la sub interfaz fastetehrnet 0.3 slot 0.

description VLAN SERVIDORES PENAS

Descripción de la interfaz.

encapsulation dot1q 3

Define el tipo de encapsulamiento asignado a la VLAN 3.

ip address 192.168.25.17 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!
interface FastEthernet0/0.4

Especifica sub interfaz fastetehrnet 0.4 slot 0.

description VLAN SISTEMAS PENAS

Descripción de la interfaz.

encapsulation dot1q 4

Define el tipo de encapsulamiento asignado a la VLAN 4.

ip address 192.168.25.25 255.255.255.248

Dirección ip y máscara de de sub-red de la sub interfaz.

!
interface FastEthernet0/1

Especifica interfaz fastethernet 1 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
!
router rip

Indica que se ha configurado el protocolo de enrutamiento rip.

version 2

Define la versión 2 del protocolo de enrutamiento.

network 192.168.20.0
network 192.168.22.0
network 192.168.23.0

network 192.168.24.0
network 192.168.25.0

indica qué redes enruta nuestro protocolo de enrutamiento.

!
ip classless

Indica acceso a las redes no remotas con máscara de sub-red diferente.

no ip http server

Especifica que no existe un servidor http.

!
!
!
line con 0

Configuración Puerto de consola.

Login

Activar configuración al inicio.

transport input none

Ningún transporte impuesto.

password cisco

Contraseña asignada.

line aux 0

Configuración puerto auxiliar.

line vty 0 4

Configuración remota por telnet.

Login

Activar configuración al inicio.

password cisco

Contraseña asignada.

!
no scheduler allocate

end

Fin del reporte de la configuración actual.

5.3.9.8 SHOW IP ROUTE PEÑAS.

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

U - per-user static route

Gateway of last resort is not set

192.168.25.0/29 is subnetted, 3 subnets
192.168.20.0/30 is subnetted, 6 subnets
192.168.24.0/29 is subnetted, 4 subnets
192.168.21.0/29 is subnetted, 5 subnets
192.168.22.0/29 is subnetted, 4 subnets
192.168.23.0/29 is subnetted, 4 subnets

192.168.x.x: Indica la red / **x:** el nivel de segmentación y **x subnets:** el número de sub-redes en las cuales se encuentra dividida

C 192.168.25.8 is directly connected, 192.168.25.9
C 192.168.25.16 is directly connected, 192.168.25.17
C 192.168.25.24 is directly connected, 192.168.25.25
C 192.168.20.32 is directly connected, Serial0
C 192.168.20.8 is directly connected, Serial1

C: Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serialx:** la interfaz de salida por la cual se accede a la red de destino

R 192.168.20.36 [120/1] via 192.168.20.33, 00:09:36, Serial0
R 192.168.20.4 [120/1] via 192.168.20.9, 00:08:30, Serial1
R 192.168.20.12 [120/1] via 192.168.20.9, 00:08:37, Serial1
R 192.168.20.0 [120/1] via 192.168.20.9, 00:04:12, Serial1
R 192.168.24.0 [120/1] via 192.168.20.33, 00:07:41, Serial0
R 192.168.24.8 [120/1] via 192.168.20.33, 00:05:25, Serial0
R 192.168.24.16 [120/1] via 192.168.20.33, 00:08:29, Serial0
R 192.168.24.24 [120/1] via 192.168.20.33, 00:09:41, Serial0
R 192.168.21.0 [120/10] via 192.168.20.9, 00:03:20, Serial1
R 192.168.21.8 [120/10] via 192.168.20.9, 00:04:27, Serial1
R 192.168.21.16 [120/10] via 192.168.20.9, 00:07:34, Serial1
R 192.168.21.24 [120/10] via 192.168.20.9, 00:02:36, Serial1
R 192.168.21.32 [120/10] via 192.168.20.9, 00:02:19, Serial1
R 192.168.22.0 [120/2] via 192.168.20.9, 00:04:21, Serial1
R 192.168.22.8 [120/2] via 192.168.20.9, 00:03:18, Serial1
R 192.168.22.16 [120/2] via 192.168.20.9, 00:08:37, Serial1
R 192.168.22.24 [120/2] via 192.168.20.9, 00:05:42, Serial1
R 192.168.23.0 [120/2] via 192.168.20.9, 00:03:42, Serial1
R 192.168.23.8 [120/2] via 192.168.20.9, 00:03:24, Serial1
R 192.168.23.16 [120/2] via 192.168.20.9, 00:01:32, Serial1
R 192.168.23.24 [120/2] via 192.168.20.9, 00:01:41, Serial1

R: Especifica el protocolo de enrutamiento usado para conectarse a la red destino (RIP), 192.168.x.x la dirección de la sub-red, **[120/1]:** La distancia administrativa / el costo de la métrica, **vía**

192.168.x.x: la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **Serialx:** la interfaz de salida.

5.3.10 CONFIGURACIÓN SWITCH PEÑAS.

Switch>**enable**

A nivel de modo usuario normal digitar el comando anterior para pasar a modo de usuario privilegiado.

Switch#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general.

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

Aparece un comando que describe al usuario que ingrese los comandos de configuración, línea por línea.

Switch(config)#**hostname SW_PENAS**

En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

SW_PENAS(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado digitar el comando anterior.

SW_PENAS(config)#**enable secret cisco**

También para establecer puntos de seguridad se encripta la contraseña con el protocolo de encriptación md5.

SW_PENAS(config)#**ip default-gateway 192.168.25.1**

Asigna al switch esta ip como puerta de enlace por defecto.

5.3.10.1 CONFIGURACIÓN DE INTERFAZ VLAN 1 (INTERFAZ VLAN POR DEFECTO)

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

Se debe ingresar a la interfaz vlan por defecto (vlan 1).

SW_PENAS(config-if)#**ip address 192.168.25.2 255.255.255.248**

Para asignar una dirección IP y máscara de subred a la sub interfaz digitar lo anterior.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

5.3.10.2 CREACIÓN DE VLAN

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general.

SW_PENAS(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

SW_PENAS#**vlan database**

Permite ingresar a la base de datos de las VLAN.

SW_PENAS(vlan)#**vlan 2 name ADMINISTRACION**

Crea la vlan dos con el nombre especificado.

SW_PENAS(vlan)#**vlan 3 name SERVIDORES**

Crea la vlan tres con el nombre especificado.

SW_PENAS(vlan)#**vlan 4 name SISTEMAS**

Crea la vlan cuatro con el nombre especificado.

5.3.10.3 CONFIGURACIÓN DE PUERTOS ASIGNANDO VLAN.

SW_PENAS(vlan)#**exit**

Para salir de la base de datos de las VLAN.

SW_PENAS#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general.

SW_PENAS(config)#**interface fastethernet 0/4**

Digite el comando anterior para configurar la interfaz fastethernet 0/4.

SW_PENAS(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_PENAS(config -if)#**switchport access vlan 2**

Agrega este puerto a la vlan especificada..

SW_PENAS(config)#**interface fastethernet 0/5**

Digite el comando anterior para configurar la interfaz fastethernet 0/5.

SW_PENAS(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN..

SW_PENAS(config -if)#**switchport access vlan 3**

Agrega este puerto a la vlan especificada.

SW_PENAS(config)#**interface fastethernet 0/6**

Digite el comando anterior para configurar la interfaz fastethernet 0/6.

SW_PENAS(config -if)#**switchport mode access**

Permite configurar la interfaz con modo de tipo acceso para asignarle una VLAN.

SW_PENAS(config -if)#**switchport access vlan 4**

Agrega este puerto a la vlan especificada..

5.3.10.4 HABILITANDO EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

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

Digitar lo anterior para salir del modo configuración de interfaz a modo configuración general.

SW_PENAS(config)#**line vty 0 15**

Habilitación del acceso por terminal virtual .

SW_PENAS(config -line)#**password cisco**

Se debe ingresar la contraseña.

SW_PENAS(config -line)#**login**

Activar al inicio.

SW_PENAS(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos. .

SW_PENAS(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual.

SW_PENAS(config)#**line con 0**

Habilita el acceso por consola.

SW_PENAS(config -line)#**password cisco**

Se debe registrar la contraseña.

SW_PENAS(config -line)#**login**

Activar al inicio.

5.3.10.5 GUARDANDO LA CONFIGURACIÓN HECHA EN EL SWITCH.

SW_PENAS(config -line)#**exit**

Digitar lo anterior para salir del modo configuración de consola a modo configuración general.

SW_PENAS(config)#**exit**

Se debe ingresar lo anterior para salir del modo configuración general a modo de usuario privilegiado.

%SYS-5-CONFIG_I: Configured from console by console

Cuando se hace este procedimiento aparece el siguiente mensaje que significa que se ha configurado desde la interfaz de consola para la interfaz de consola.

SW_PENAS#**copy running-config startup-config**

Con el comando anterior se guarda la configuración actual a la configuración de inicio.

Building configuration...

El siguiente mensaje significa que se esta guardando la configuración.

[OK]

Ahora aparece un mensaje de aprobación.

5.3.10.6 SHOW RUN SWITCH PEÑAS.

SW_PENAS#sh run
!
Version 12.1

Indica la versión del IOS.

service timestamps debug uptime
service timestamps log uptime
service password-encryption

Indica que el servicio de encriptación de contraseña esta activo.

!
hostname SW_PENAS

Refleja el nombre que el administrador le ha asignado al router.

ip name-server 0.0.0.0
enable secret 5 sdf6978yhg$jnb76sd

Esta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Esta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

```
!
!
!
ip subnet-zero

!
!
!
!
!
!
spanning-tree extend system-id
```

Para usar red sin bucles, rutas cortas.

```
!
!
!
!
interface FastEthernet0/1
```

Especifica interfaz fastethernet0/1.

```
switchport mode dynamic desirable
```

Indica que no esta configurado el modo tipo acceso.

```
bandwidth 100000
```

Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/2
```

Especifica interfaz fastethernet0/2.

```
switchport mode dynamic
```

Indica que esta configurado el modo tipo acceso para acceder a las VLAN.

```
switchport access vlan 2
```

Especifica que esta interfaz es parte de la VLAN indicada.

```
bandwidth 100000
```

Valor del ancho de banda del enlace en la interfaz.

```
!
interface FastEthernet0/3
```

Especifica interfaz fastethernet0/3.

```
switchport mode dynamic
```

Indica que esta configurado el modo tipo acceso para acceder a las VLAN.

```
switchport access vlan
```

Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/4

Especifica interfazfastethernet0/4.

switchport mode dynamic

Indica que esta configurado el modo tipo acceso para acceder a las VLANs.

switchport access vlan 4

Especifica que esta interfaz es parte de la VLAN indicada.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/5

Especifica interfaz fastethernet0/5.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/6

Especifica interfaz fastethernet0/6.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/7

Especifica interfaz fastethernet0/7.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso.

bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

!
interface FastEthernet0/8

Especifica interfaz fastethernet0/8.

switchport mode dynamic desirable

Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/9
Especifica interfaz fastethernet0/9

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/10
Especifica interfaz fastethernet0/10

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/11
Especifica interfaz fastethernet0/11

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface FastEthernet0/12
Especifica interfaz fastethernet0/12

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface GigabitEthernet0/1
Especifica la interfaz Gigabithernet0/1

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz
!
interface GigabitEthernet0/2
Especifica la interfaz Gigabithernet0/2

switchport mode dynamic desirable
Indica que no esta configurado el modo tipo acceso

bandwidth 100000
Valor del ancho de banda del enlace en la interfaz

!
vtp domain bigdomain
Especifica el dominio del puerto truncado virtual

interface Vlan 1
Especifica la VLAN 1 (vlan por defecto)

ip address 192.168.25.2 255.255.255.248
Dirección IP de la vlan por defecto

no ip route-cache
No almacena ip en el cache de rutas

shutdown

vlan 2 name monitores
Indica VLAN configurada con su respectivo nombre

vlan 3 name servidores
Indica VLAN configurada con su respectivo nombre

vlan 4 name ventas_gerencia
Indica VLAN configurada con su respectivo nombre

!
ip classless
Indica acceso a las redes no remotas con mascara de sub-red diferente

no ip http Server
Especifica que no existe un servidor http

!
ip default-gateway 192.168.25.1
Indica interfaz de puerta de enlace para comunicar VLAN

!
!

line con 0
Configuración Puerto de consola

login
Activar configuración al inicio

transport input none
Ningún transporte impuesto

password cisco

```
                                Contraseña asignada

line aux 0
                                Configuración Puerto auxiliar

line vty 0 4
                                Configuración remota por telnet

 login
                                Activar configuración al inicio

 password cisco
                                Contraseña asignada
!
no scheduler allocate

end
                                Fin del reporte de la configuración actual
```

5.3.10.7 SHOW VLAN SWITCH PEÑAS.

SW_PENAS# sh vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14
2	monitores	active	Fa0/4
3	servidores	active	Fa0/5
4	ventas_gerencia	active	Fa0/6
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
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
4	enet	100004	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

VLAN: Identificación vlan

Name: Nombre de vlan
Status: Estado
Ports: Puertos asignados a la vlan
Type: Tipo de interfaces
SIAD: Encabezado para identificar vlan
MTU: Tamaño máximo de los paquetes transmitidos por el puerto expresado en bytes

Parent: Parentela
RingNo: Número de anillo si hay
BridgeNO: Número de puente si hay
Stp: STP usado
BrdgMode: Modo de puente
Transx: TRANS, o si es una VLAN que cambia de topología Token Ring / FDDI a Ethernet.

5.3.11 CONFIGURACIÓN ROUTER CLIENTES_WLL.

Router>**enable**

A nivel de modo usuario normal, digitar el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

A nivel de modo usuario privilegiado digitar el comando anterior para pasar a modo de configuración general.

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

Aparece un comando que describe al usuario que ingrese los comandos de configuración, línea por línea.

Router(config)#**hostname PENAS**

En el modo de configuración general digitar el comando anterior para establecer el nombre del dispositivo.

CLIENTES_WLL(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado digitar el comando anterior.

CLIENTES_WLL(config)#**enable secret cisco**

También para establecer puntos de seguridad se debe encriptar la contraseña con el protocolo de encriptación md5 con el comando anterior.

5.3.11.1 CONFIGURACIÓN DE INTERFAZ FASTETHERNET.

CLIENTES_WLL(config)#**interface fastethernet0/0**

Digite el comando anterior para configurar la interfaz serial 0.

CLIENTES_WLL(config-if)#**description CONEXIÓN AL ROUTER PROSPERINA**

Para agregar un comentario como guía Se debe ingresar el comando anterior.

CLIENTES_WLL(config-if)#**ip address 192.168.21.34 255.255.255.252**

Para asignar una dirección IP y máscara de sub-red al puerto digite lo anterior.

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

Para habilitar administrativamente el puerto Se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

5.3.11.2 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO OSPF.

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

Se debe habilitar el protocolo de enrutamiento con el comando anterior.

CLIENTES_WLL(config -router)#**log-adjacency-changes**

Se debe ingresar lo anterior para cargar los cambios de los routers adyacentes.

CLIENTES_WLL(config -router)# 192.168.21.0 0.0.0.255 area 0

Al activar el protocolo de enrutamiento se especifica la red con su respectiva wildcard y el área en la cual trabaje.

5.3.11.3 HABILITAR EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

CLIENTES_WLL(config)#**line vty 0 4**

Habilitación del acceso por terminal virtual.

CLIENTES_WLL(config -line)#**password cisco**

Se debe ingresar la contraseña.

CLIENTES_WLL(config -line)#**login**

Activar al inicio.

CLIENTES_WLL(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

CLIENTES_WLL(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual.

CLIENTES_WLL(config)#**line con 0**

Habilitación del acceso por consola.

CLIENTES_WLL(config -line)#**password cisco**

Se debe ingresar la contraseña.

CLIENTES_WLL(config -line)#**login**

Activar al inicio.

Con el mismo procedimiento puede configurarse una password para acceder por el puerto auxiliar. Tanto el puerto de consola como el auxiliar, no requieren autenticación de password por defecto.

5.3.11.4 GUARDAR LA CONFIGURACIÓN DEL ROUTER.

CLIENTES_WLL#**copy running-config startup-config**

Con el comando anterior guarde la configuración actual a la configuración de inicio.

Building configuration...

El siguiente mensaje significa que se está guardando la configuración.

[OK]

Ahora aparece un mensaje de aprobación.

5.3.11.5 SHOW RUN ROUTER CLIENTES_WLL.

CLIENTES_WLL#sh run
Building configuration...

!
Version 12.1

Indica la versión del IOS.

service timestamps debug uptime

service timestamps log uptime
service password-encryption

Indica que el servicio de encriptación de contraseña está activo.

!
hostname CLIENTES_WLL

Refleja el nombre que el administrador le ha asignado al router.

enable secret 5 sdf6978yhg$jnb76sd

Ésta línea especifica la contraseña encriptada por el protocolo md5.

enable password cisco

Ésta línea especifica una contraseña para ingreso al router en modo usuario privilegiado.

!
ip subnet-zero
!
interface Serial0

Especifica interfaz serial 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

shutdown

Indica interfaz no levantada.

!
interface Serial1
no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
interface FastEthernet0/0

Especifica interfaz fastethernet 0 slot 0.

description CONEXIÓN PROSPERINA

Descripción de la interfaz.

ip address 192.168.21.34 255.255.255.248

Dirección ip y máscara de de sub-red de la interfaz.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

ip ospf priority 0
!
interface FastEthernet0/1

Especifica interfaz fastethernet 1 slot 0.

no ip address

Sin dirección ip asignada.

no ip directed-broadcast
bandwidth 100000

Valor del ancho de banda del enlace en la interfaz.

Shutdown

Indica interfaz no levantada.

!
router ospf 1

Indica que se ha configurado el protocolo de enrutamiento ospf.

log-adjacency-changes

Esto indica que el router carga los cambios de los routers adyacentes.

network 192.168.21.0 0.0.0.255 area 0

Especifica la red con su respectiva wildcard y el área en la cual se va a trabajar.

!
ip classless

Indica acceso a las redes no remotas con máscara de sub-red diferente.

no ip http server

Especifica que no existe un servidor http.

!
line con 0

Configuración Puerto de consola.

Login

Activar configuración al inicio.

transport input none

Ningún transporte impuesto.

password cisco

Contraseña asignada.

line aux 0

Configuración Puerto auxiliary.

line vty 0 4

Configuración remota por telnet.

Login

Activar configuración al inicio.

password cisco

Contraseña asignada.

!
no scheduler allocate

end

Fin del reporte de la configuración actual.

5.3.11.6 SHOW IP ROUTE CLIENTES_WLL.

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

Gateway of last resort is not set

192.168.21.0/29 is subnetted, 5 subnets
192.168.23.0/29 is subnetted, 4 subnets
192.168.20.0/30 is subnetted, 5 subnets
192.168.24.0/29 is subnetted, 4 subnets
192.168.22.0/29 is subnetted, 4 subnets
192.168.25.0/29 is subnetted, 4 subnets

192.168.x.x: Indica la red / **x:** el nivel de segmentación y **x subnets:** el numero de sub-redes en las cuales se encuentra dividida.

C 192.168.21.32 is directly connected, FastEthernet0/0

C: Especifica que la interfaz está conectada directamente, **192.168.x.x:** la dirección de la sub-red a la cual está conectado y **Serialx:** la interfaz de salida por la cual accede a la red de destino.

O 192.168.21.8 [110/20] via 192.168.21.34, 00:00:43, FastEthernet0/0
O 192.168.21.16 [110/20] via 192.168.21.34, 00:00:43, FastEthernet0/0
O 192.168.21.24 [110/20] via 192.168.21.34, 00:00:43, FastEthernet0/0

O: Especifica el protocolo de enrutamiento usado para conectarse a la red destino (**OSPF**), **192.168.x.x:** la dirección de la sub-red, **[110/20]:** La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **FastEthernet0/0:** la interfaz de salida.

O E2 192.168.21.0 [120/11] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.23.0 [120/1] via 192.168.20.38, 00:00:33, FastEthernet0/0
O E2 192.168.23.8 [120/1] via 192.168.20.38, 00:00:33, FastEthernet0/0
O E2 192.168.23.16 [120/1] via 192.168.20.38, 00:00:33, FastEthernet0/0
O E2 192.168.23.24 [120/1] via 192.168.20.38, 00:00:33, FastEthernet0/0
O E2 192.168.20.4 [120/1] via 192.168.20.38, 00:00:33, FastEthernet0/0
O E2 192.168.20.36 [120/1] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.20.12 [120/1] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.20.8 [120/2] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.20.0 [120/2] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.24.0 [120/1] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.24.8 [120/1] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.24.16 [120/1] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.24.24 [120/1] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.22.0 [120/3] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.22.8 [120/3] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.22.16 [120/3] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.22.24 [120/3] via 192.168.20.33, 00:00:13, FastEthernet0/0
O E2 192.168.25.0 [120/3] via 192.168.20.38, 00:00:03, FastEthernet0/0
O E2 192.168.25.8 [120/3] via 192.168.20.38, 00:00:03, FastEthernet0/0
O E2 192.168.25.16 [120/3] via 192.168.20.38, 00:00:03, FastEthernet0/0
O E2 192.168.25.24 [120/3] via 192.168.20.38, 00:00:03, FastEthernet0/0

O: Especifica el protocolo de enrutamiento usado para conectarse a la red destino (**OSPF**), **E2:** el tipo, **192.168.x.x:** la dirección de la sub-red, **[110/20]**: La distancia administrativa / el costo de la métrica, **vía 192.168.x.x:** la interfaz adyacente para comunicarse con la sub-red, **hh:mm:ss:** la hora de la última actualización y **FastEthernet0/0:** la interfaz de salida.

5.3.12 CONFIGURACIÓN ROUTER PROSP_NORTE.

Router>**enable**

A nivel de modo usuario normal digite el comando anterior para pasar a modo de usuario privilegiado.

Router#**configure terminal**

A nivel de modo usuario privilegiado digite el comando anterior para pasar a modo de configuración general.

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

Aparece un comando que describe al usuario que ingrese los comandos de configuración, línea por línea.

Router(config)#**hostname PENAS**

En el modo de configuración general digite el comando anterior para establecer el nombre del dispositivo.

PROSP_NORTE(config)# **service password-encryption**

Permitir el uso de encriptación en el router.

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

Para configurar la contraseña de acceso al modo privilegiado digite el comando anterior.

PROSP_NORTE(config)#**enable secret cisco**

También para establecer puntos de seguridad se debe encriptar la contraseña con el protocolo de encriptación md5 con el comando anterior.

5.3.12.1 CONFIGURACIÓN DE INTERFAZ FASTETHERNET.

PROSP_NORTE(config)#**interface fastethernet0/0**

Digite el comando anterior para configurar la interfaz serial 0.

PROSP_NORTE(config-if)#**description CONEXIÓN AL ROUTER PROSPERINA**

Para agregar un comentario como guía se debe ingresar el comando anterior.

PROSP_NORTE(config-if)#**ip address 192.168.21.34 255.255.255.252**

Para asignar una dirección IP y máscara de sub-red al puerto digite lo anterior.

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

Para habilitar administrativamente el puerto se debe ingresar lo anterior.

%LINEPROTO-5-UPDOWN:Line protocol on Interface serial0/0, changed state to up
%LINK -3-UPDOWN: Interface serial0/0, changed state to up

Después de haber ingresado lo anterior, aparece el siguiente mensaje, que realiza un test para comprobar si hay conexión física y lógica.

5.3.12.2 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO OSPF.

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

Se debe habilitar el protocolo de enrutamiento con el comando anterior.

PROSP_NORTE(config -router)#**log-adjacency-changes**

Se debe ingresar lo anterior para cargar los cambios de los routers adyacentes.

PROSP_NORTE(config -router)# 192.168.21.0 0.0.0.255 area 0

Al activar el protocolo de enrutamiento se especifica la red con su respectiva wildcard y el área en la cual se va a trabajar.

5.3.12.3 HABILITAR EL ACCESO POR CONSOLA Y POR TERMINAL VIRTUAL.

PROSP_NORTE(config)#**line vty 0 4**

Habilitación del acceso por terminal virtual.

PROSP_NORTE(config -line)#**password cisco**

Se debe ingresar la contraseña.

PROSP_NORTE(config -line)#**login**

Activar al inicio.

PROSP_NORTE(config -line)#**exec-timeout 5 0**

El comando anterior limita el tiempo de disponibilidad del acceso por terminal virtual a 5 minutos, 0 segundos.

PROSP_NORTE(config -line)#**exit**

Se debe salir de la configuración de la Terminal virtual.

PROSP_NORTE(config)#**line con 0**

Habilitación del acceso por consola.

PROSP_NORTE(config -line)#**password cisco**

Se debe ingresar la contraseña.

PROSP_NORTE(config -line)#**login**

Activar al inicio.

Con el mismo procedimiento puede configurarse una password para acceder por el puerto auxiliar. Tanto el puerto de consola como el auxiliar, no requieren autenticación de password por defecto.

CAPÍTULO 6

LINUX FEDORA CORE 3

6. LINUX FEDORA CORE 3.

6.1 INTRODUCCIÓN.

Linux es un sistema operativo que puede convertir cualquier PC 386 o 486 en una estación de trabajo. Le pondrá todo el poder de UNIX en la punta de sus dedos. En los negocios ya se instala Linux en redes enteras, usando el sistema operativo para manejar registros financieros y de hospitales, un entorno de usuario distribuido, telecomunicaciones, etc. Universidades de todo el mundo usan Linux para dar cursos de programación y diseño de sistemas operativos. Y, por supuesto, entusiastas de los ordenadores de todo el mundo están usando Linux en casa, para programar, entretenerse, y conocerlo a fondo.

Lo que hace a Linux tan diferente es que es una implementación gratuita de UNIX. Fue y aún es desarrollado por un grupo de voluntarios, principalmente en Internet, intercambiando código, comentando fallos, y arreglando los problemas en un entorno abierto. Cualquiera es bienvenido a sumarse al esfuerzo de desarrollo de Linux: todo lo que se pide es interés en producir un clónico gratuito de UNIX y algunos conocimientos de programación.

Fue desarrollado buscando la portabilidad de los códigos fuentes: encontrará que casi todo el software gratuito desarrollado para UNIX se compila en Linux sin problemas. Y todo lo que se hace para Linux (código del núcleo, drivers, librerías y programas de usuario) es de libre distribución.

6.2 CARACTERÍSTICAS DEL SISTEMA.

Linux implementa la mayor parte de las características que se encuentran en otras implementaciones de UNIX, más algunas otras que no son habituales.

- **Multitarea:** La multitarea no consiste en hacer que el procesador realice más de un trabajo al mismo tiempo (un solo procesador no tiene esa capacidad), lo único que realiza es presentar las tareas de forma intercalada para que se ejecuten varias simultáneamente. Por lo tanto en Linux es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.

- **Multiusuario:** Para que pueda desarrollar esta labor (de compartir los recursos de un ordenador) es necesario un sistema operativo que permita a varios usuarios acceder al mismo tiempo a través de terminales, y que distribuya los recursos disponibles entre todos. Así mismo, el sistema debería proporcionar la posibilidad de que más de un usuario pudiera trabajar con la misma versión de un mismo programa al mismo tiempo, y actualizar inmediatamente cualquier cambio que se produjese en la base de datos, quedando reflejado para todos.

- **Multiplataforma:** Es decir que puede correr en muchas CPU distintas (Intel, AMD, motorola, sun, sparc, etc.)

- **Seguro:** Linux se autoprotege.
  Soporta consolas virtuales, lo que permite tener más de una sesión abierta en la consola de texto y conmutar entre ellas fácilmente.

- El núcleo es capaz de emular por su cuenta las instrucciones del coprocesador 387, con lo que en cualquier 386 con coprocesador o sin él se podrán ejecutar aplicaciones que lo requieran.

- Linux soporta diversos sistemas de ficheros para guardar los datos. Algunos de ellos, como el ext2fs, han sido desarrollados específicamente para Linux.

- Linux implementa todo lo necesario para trabajar en red con TCP/IP.

- Utiliza las características del modo protegido de los microprocesadores 80386 y 80486. En concreto, hace uso de la gestión de memoria avanzada del modo protegido y otras características avanzadas.

- Con el fin de incrementar la memoria disponible, Linux implementa la paginación con el disco. Cuando el sistema necesita más memoria, expulsará páginas inactivas al disco, permitiendo la ejecución de programas más grandes o aumentando el número de usuarios que puede atender a la vez. Sin embargo, el espacio de intercambio no puede suplir totalmente a la memoria RAM, ya que el primero es mucho más lento que ésta.

6.3 ESTRUCTURA.

En la estructura de Linux aparecen cuatro elementos situados en bloques diferentes, cada uno tiene encomendado una función:

- Núcleo o Kernel.

- Shell.

- Sistema de archivos.

- Utilidades.

El núcleo: es el programa medular que ejecuta programas y gestiona dispositivos de hardware tales como los discos y las impresoras.

El shell: proporciona una interfaz para el usuario. Recibe órdenes del usuario y las envía al núcleo para ser ejecutadas.

El sistema de archivos: organiza la forma en que se almacenan los archivos en dispositivos de almacenamiento tales como los discos. Los archivos están organizados en directorios. Cada directorio puede contener un número cualquiera de subdirectorios, cada uno de los cuales puede a su vez, contener otros archivos.

El núcleo, el shell y el sistema de archivos forman en conjunto la estructura básica del sistema operativo. Con estos tres elementos puede ejecutar programas, gestionar

archivos e interactuar con el sistema. Además, Linux cuenta con unos programas de software llamados utilidades que han pasado a ser considerados como características estándar del sistema.

Las utilidades: son programas especializados, tales como editores, compiladores y programas de comunicaciones, que realizan operaciones de computación estándar. Incluso uno mismo puede crear sus propias utilidades.

Linux contiene un gran número de utilidades. Algunas efectúan operaciones sencillas: otras son programas complejos con sus propios juegos de órdenes. Para empezar, muchas utilidades de pueden clasificar en tres amplias categorías: editores, filtros y programas de comunicaciones. También hay utilidades que efectúan operaciones con archivos y administración de programas.

6.4 INSTALANDO LINUX FEDORA CORE COMO SERVIDOR.

Fedora Core 3, 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 escoger paquetes de programas individuales, o instalarlos luego.

6.4.1 ANTES DE INSTALAR.

- Para instalar Linux Fedora Core 3 desde cds, se necesita 4 discos de instalación o el DVD de instalación.

Figura 6.1 Juego de discos de Fedora Core 3.

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

  - Procesador Pentium III o superior para modo gráfico.
  - Memoria RAM 256Mb o superior.
  - Disco Duro 4Gb.
  - Unidad de CD-ROM o DVD-ROM.
  - Tarjeta de red 10/100

6.4.2 ¿COMO 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.

6.4.3 COMENZANDO LA INSTALACIÓN.

Paso 1: Para comenzar la instalación de Fedora Core 3, 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 3 puede ser iniciado desde un CD o un DVD con el primer disco.

- Encienda el computador presionando el botón power del mismo. Tal como lo muestra la siguiente gráfica.

Figura 6.2 Encendido del botón Power.

- Cuando el equipo empiece el arranque, se debe mantener presionada la tecla **Supr.** para entrar a las opciones del setup.

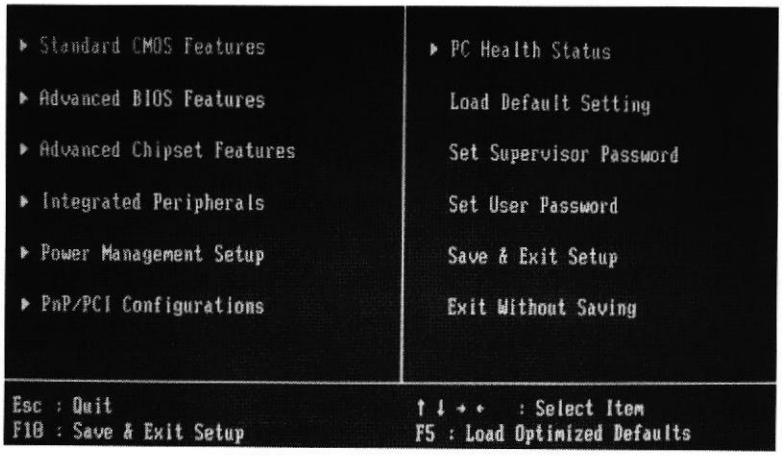


Figura 6.3 Captura de la pantalla del Setup.

Nota: No se puede ingresar al BIOS con la tecla suprimir en todos los computadores, esto dependerá mucho del fabricante del motherboard.

- Seleccione la opción **Advanced Bios Features** y presione la tecla **enter** para entrar a las opciones avanzadas del BIOS, como lo muestra la siguiente gráfica.

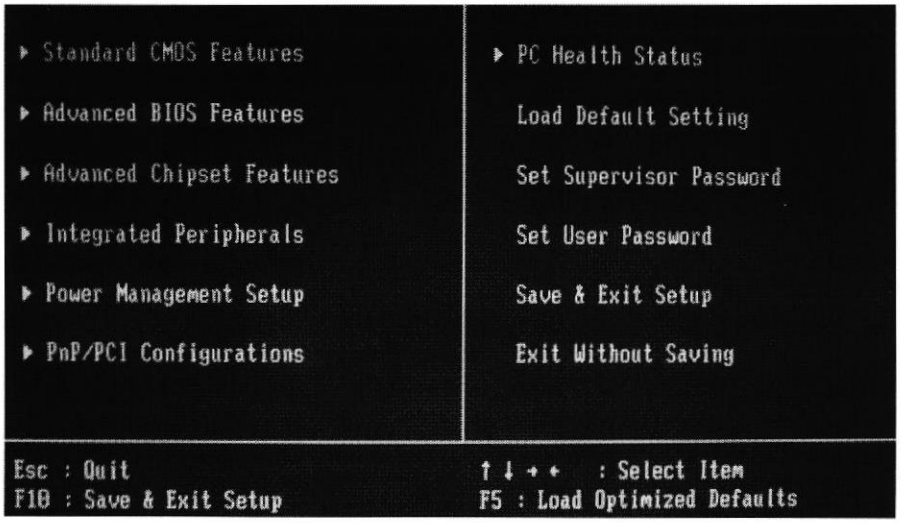


Figura 6.4 Opciones avanzadas del BIOS seleccionada en el menú principal.

Nota: Las opciones del BIOS varían según la versión. Y el fabricante del motherboard.

- A continuación debe seleccionar la opción **Boot Sequence** y presionar la tecla **enter,** para acceder a la configuración de la secuencia de buteo.

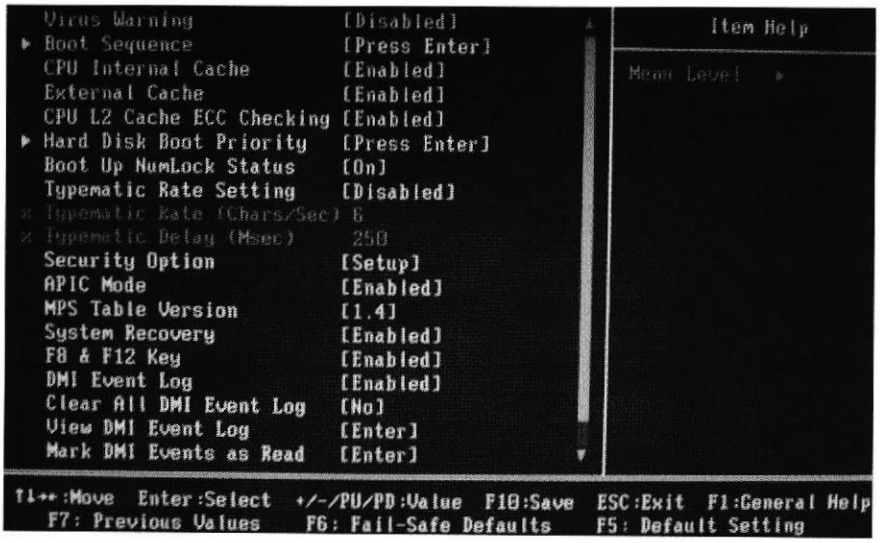


Figura 6.5 Opción secuencia de buteo seleccionada en el setup.

- En la siguiente gráfica se muestra como debe quedar configurado la opción **Boot Sequence** del BIOS, para que permita el buteo por medio del CDROM.

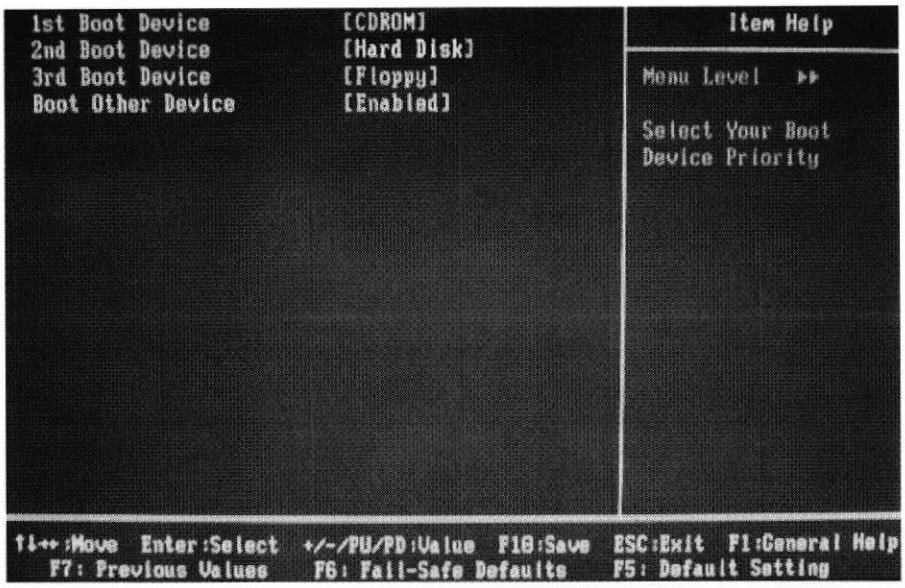


Figura 6.6 Opción secuencia de buteo seleccionada en el setup.

- Pulse la tecla **Esc** dos veces, para situarse en el menú principal del BIOS. Luego seleccione la opción **Save & Exit Setup** y presione la tecla enter, para que al salir de la configuración del Bios se guarden los cambios que hicieron.

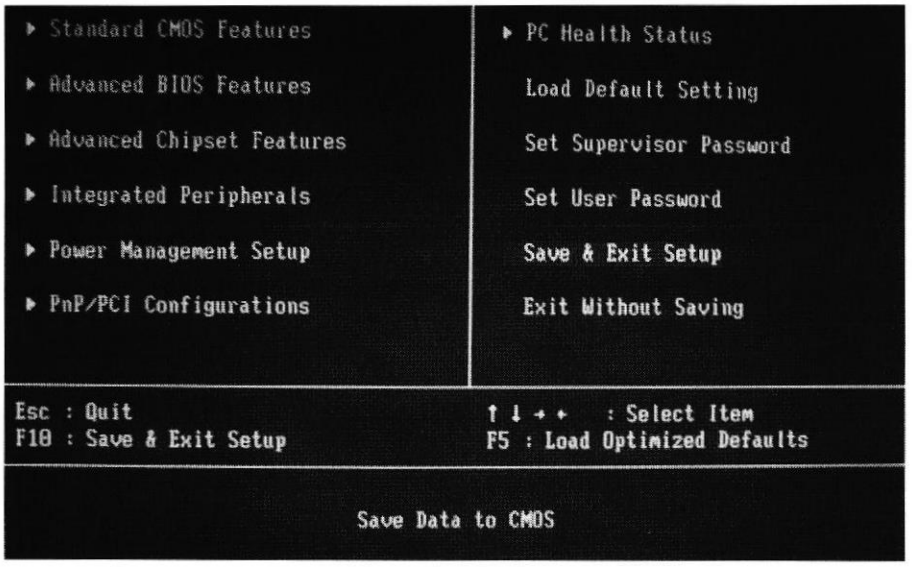


Figura 6.7 Opción Guardar y Salir del Setup

- Deberá aparecer una pantalla de confirmación, digite la tecla **Y** para que los cambios surtan efecto. Si presiona la tecla N no se guardaran los cambios hechos en la configuración del Bios. Luego de esto el computador reiniciará el sistema.

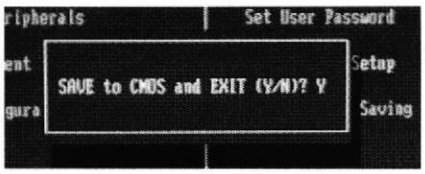


Figura 6.8 Ventana de confirmación para la configuración del BIOS.

- Ingrese el primer disco en la unidad de CD o DVD, para empezar la instalación.

Figura 6.9 Muestra la inserción del disco 1 en la unidad de CD del pc.

- Luego, aparecerá la pantalla de boteo de Fedora Core 3, la misma que contiene boot: _ en la parte final.

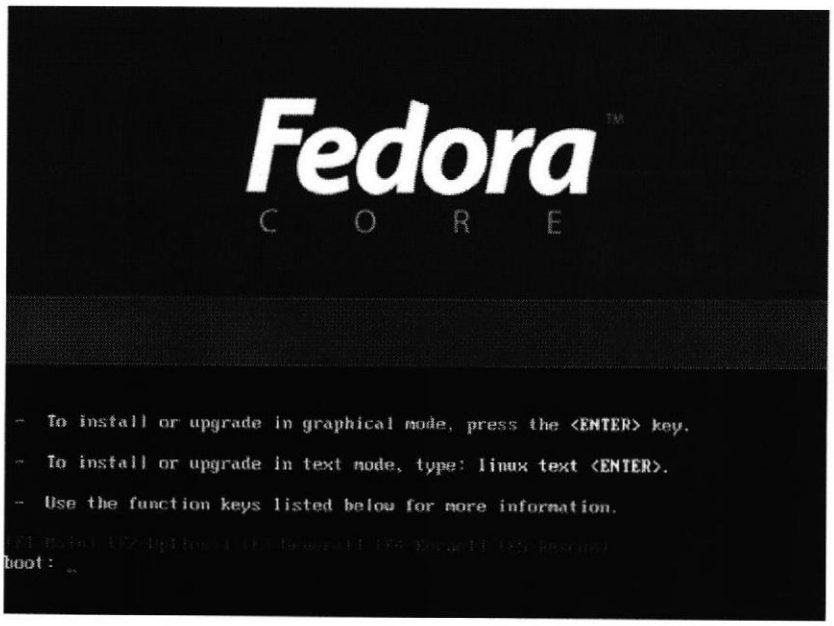


Figura 6.10 Pantalla de arranque

Si presiona **Enter**, la instalación es realizada en el modo por defecto. Es decir, la instalación usa una interfaz gráfica. Para cambiar el modo de instalación, en el boot:_ digite linux text para realizar la instalación en una interfaz de texto.

Paso 2: Cuando se ingresa a la instalación ya sea por modo texto o modo comando, la primera fase del programa de instalación inicia, por lo que pedirá comprobar el funcionamiento de los discos de instalación.

- Seleccione **OK** para comprobar el primer disco de instalación, o seleccione **Skip** para proceder con la instalación sin probar el disco.

Figura 6.11 Pantalla de comprobación de discos.

Nota: Se recomienda realizar la comprobación de los discos de instalación porque un error de disco durante la instalación puede forzar a renovar el procedimiento completo.

- Después de que se realizó el test del primer disco, otra pantalla aparece y muestra el resultado, donde deberá presionar **OK.**

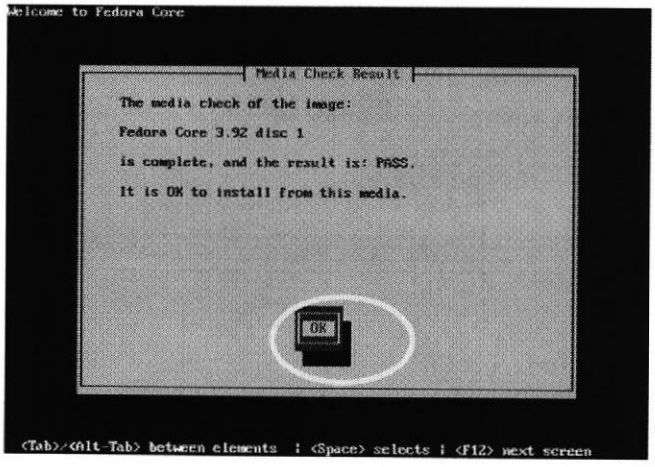


Figura 6.12 Resultado de comprobación de discos.

- A continuación aparecerá una pantalla para seguir comprobando los discos. Seleccione **Test** para comprobar el siguiente disco del juego, o **Continue** para proceder con la instalación

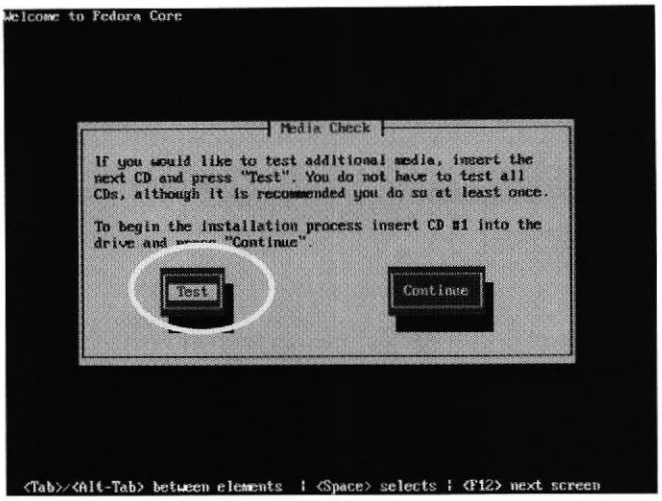


Figura 6.13 Pantalla de próximo disco.

- Después de que se han comprobado los discos y seleccionar **Continue**, o si escoge **Skip Testing**, el programa principal de la instalación se carga.

Figura 6.14 Carga de instalación gráfica.

Nota: Si en la instalación falla la identificación del hardware, 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.

- Después que termina el proceso de identificación del hardware, el programa de instalación muestra una pantalla de bienvenida. Pulse **Siguiente** para continuar con la instalación.

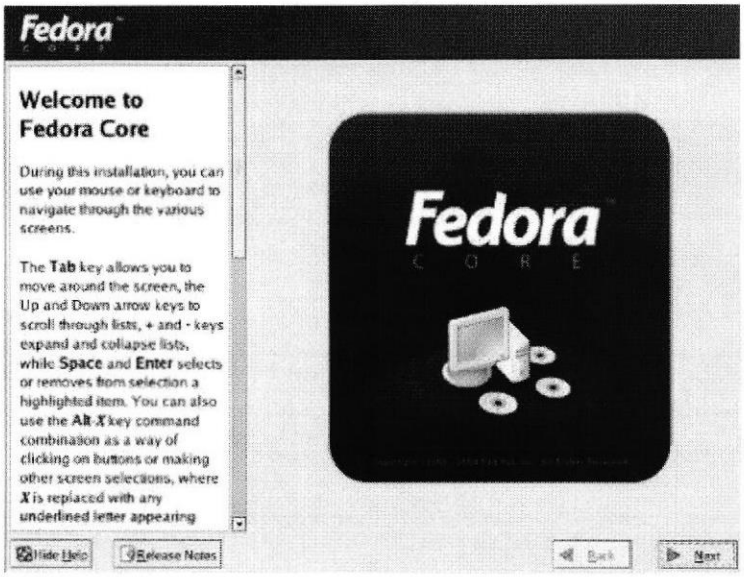


Figura 6.15 Pantalla de Bienvenida.

Paso 3: A continuación aparecerá una pantalla que muestra la lista de idiomas que se utilizan durante la instalación Fedora Core 3.

- Sombree el idioma de su elección en la lista y de clic en **Siguiente.**

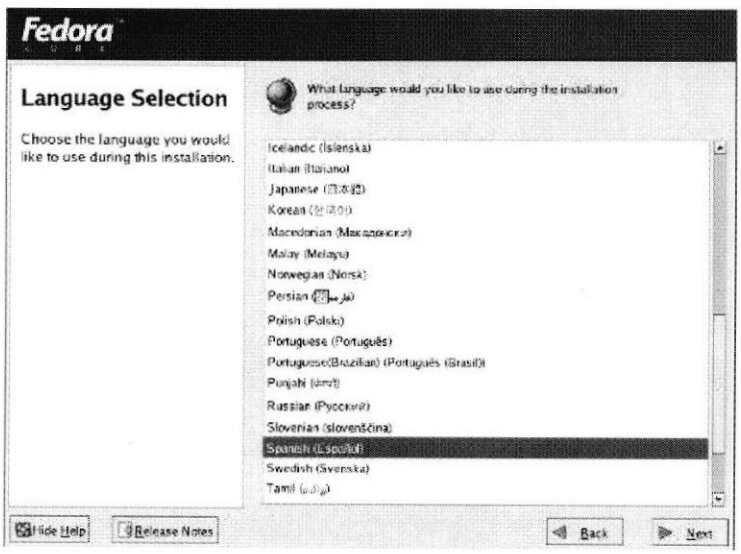


Figura 6.16 Pantalla de selección del idioma.

Nota: Para obtener soporte para idiomas adicionales. Modifique la instalación en la fase de instalación de los paquetes.

Paso 4: El programa de instalación muestra una lista de salidas de teclado soportados por Fedora Core 3.

- Sombree el idioma apropiado para su teclado de la lista mostrada y seleccione **Siguiente.**

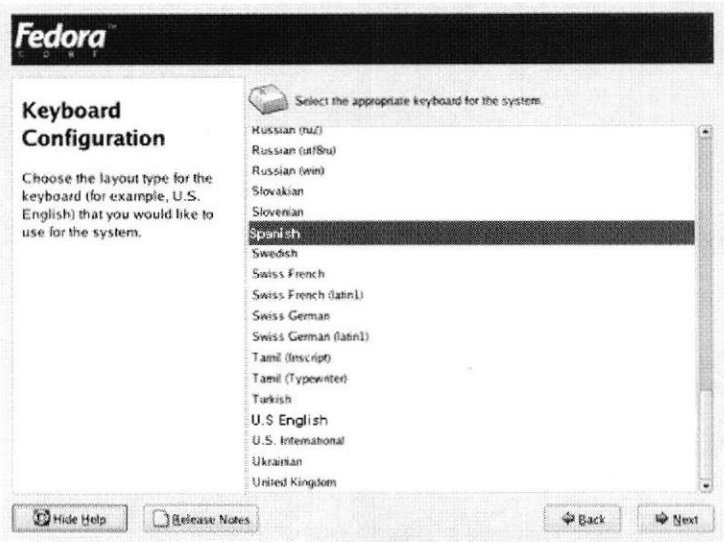


Figura 6.17 Pantalla de selección de teclado.

Paso 5: Luego de haber configurado el idioma, tanto para el sistema como para el teclado, aparecerá una pantalla con dos opciones, de la que se debe escoger entre un nueva instalación o una actualización de una instalación existentes, pero no ambas a la vez.

- Escoja la opción de Instalación que más se ajuste a sus necesidades. En este caso se procede a escoger la opción de **Instalar Fedora Core 3,** porque el computador no tiene instalado sistema operativo alguno.

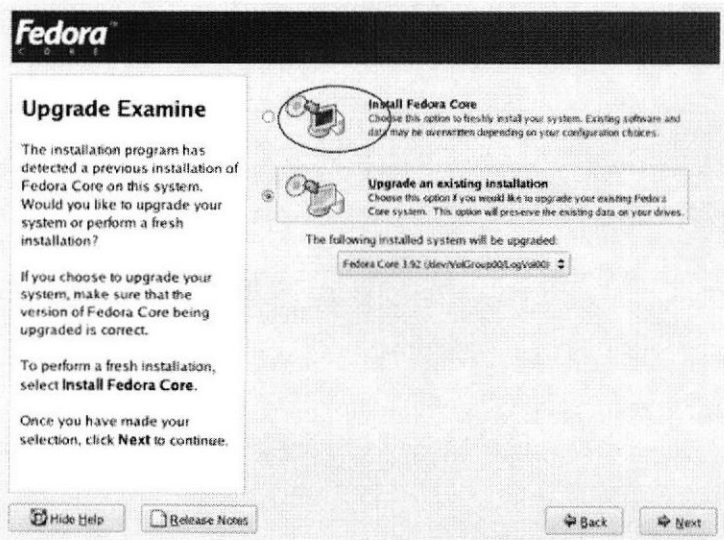


Figura 6.18 Pantalla de reconocimiento de actualización.

Paso 6: Ahora tendrá que escoger que tipo de instalación va a utilizar, esto dependerá de las necesidades que desee cubrir. Antes de escoger un tipo de instalación es necesario saber que ofrece cada una de ellas.

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 3. 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.

- **ESCRITORIO PERSONAL**
  Este es el tipo de instalación por defecto. Esta instalación proporciona un ambiente de trabajo en forma gráfica con un paquete de utilitarios de oficina. Aplicaciones de Internet y programas multimedia.

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

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

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

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

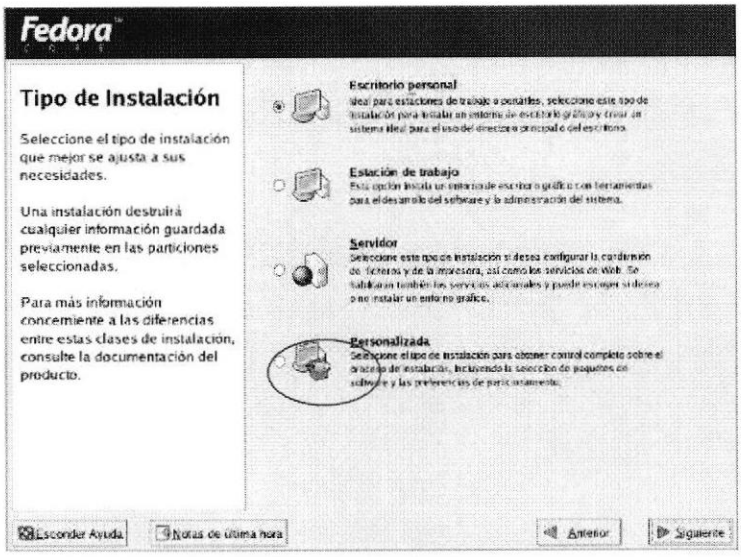


Figura 6.19 Pantalla de tipo de instalación.

- **Consideraciones especiales:** Todas las instalaciones de Fedora Core 3, incluyen los siguientes servicios de red:

  - Email a través de SMTP (Simple Mail Transfer Protocol)
  - Compartir archivos en red a través de NFS (Network File System)
  - Imprimir a través de CUPS (Common UNIX Printing System)
  - Acceso remoto a través de SSH (Security Shell)

  Algunos procesos automatizados sobre su sistema en Fedora usan el servicio de email para enviar reportes y mensajes al administrador del sistema. Por defecto, los servicios de email e impresión no aceptan conexiones desde otros sistemas. Aunque Fedora se vincula a los servicios de NFS sobre otros sistemas, el componente de compartir con el servicio NFS esta deshabilitado por defecto. Usted deberá configurar su sistema Fedora después de la instalación para entregar email, NFS, o servicios de impresión. El servicio SSH esta habilitado por defecto.

- **Instalación mínima:** Para instalar lo mas mínimo en software, escoja el tipo instalación **Personalizada**. En la pantalla de **Selección de grupo de paquetes,** seleccione el grupo de paquetes mínimo. Los únicos servicios incluidos en la instalación mínima son email, impresión, NFS, y SSH. Este tipo de instalación puede ser útil para firewalls u otros sistemas especializados en los cuales los servicios limitados son una ventaja.

Paso 7: En esta pantalla se necesita elegir que tipo de partición se va a utilizar. Si usted es nuevo en Linux, usted necesitará usar el método de partición automática. Si usted 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. Antes de escoger un tipo de partición es necesario saber que ofrece cada una de ellas.

- **ELECCIÓN DE PARTICIÓN AUTOMÁTICA**

Escoja **Partición automática** en el menú opciones de particiones para usar una pre-configurada. Entonces Disk Fruid muestra opciones adicionales.

- **Retirar todas las particiones linux en el sistema,** extrae todas las particiones de Linux ext2, ext3, y swap de todos los discos duros.
- **Retirar todas las particiones en este sistema,** es decir, las particiones de todos los discos duros.
- **Mantener todas las particiones y usar el espacio libre**, usa solamente el espacio no particionado en los discos duros para instalar Fedora Core.

Seleccione la opción que desee, y 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.

Para revisar la configuración de la partición automática, seleccione el chekbox **Revisar.**

- **ELECCIÓN DE PARTICIÓN MANUAL**

Para particionar el disco manualmente, escoja **Partición manual con Disk Fruid.** Elija este método si usted necesita una configuración de particiones especial.

- **Información General sobre las particiones:** Un sistema Fedora Core 3 tiene por lo menos 3 particiones:
  - Una partición de información montada en /boot
  - Una partición de información montada en /
  - Una partición swap

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

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

- Una vez que se sabe en que consiste el particionamiento automático y el particionamiento manual con Disk Druid. Elija **Partición manual con Disk Druid,** debido a que esta opción permite asignar un tamaño determinado a cada partición de una forma interactiva.

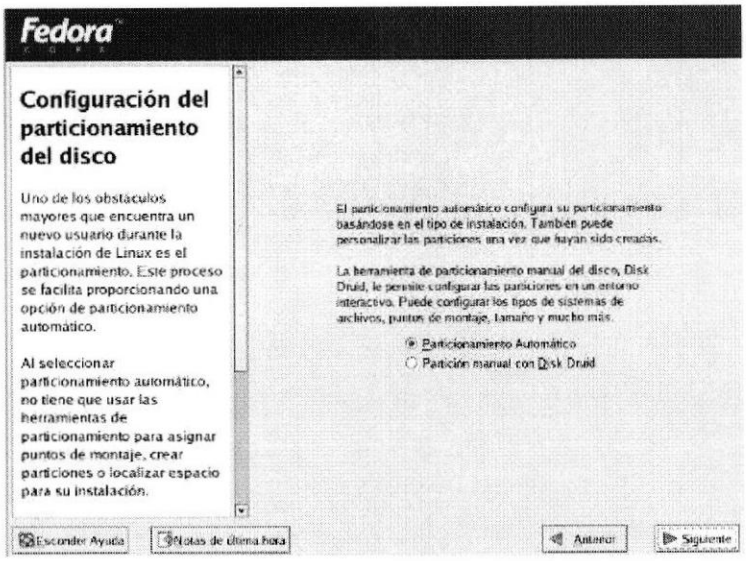


Figura 6.20 Pantalla de configuración de particionamiento del disco.

Paso 8: En este paso de la instalación se deben crear las particiones donde se va a alojar el sistema operativo, en esta pantalla se muestra el detalle de las particiones creadas, cuanto espacio se tiene ocupado y cuanto espacio se tiene libre en el disco duro. Recuerde que Fedora Core 3 debe tener mínimo tres particiones.

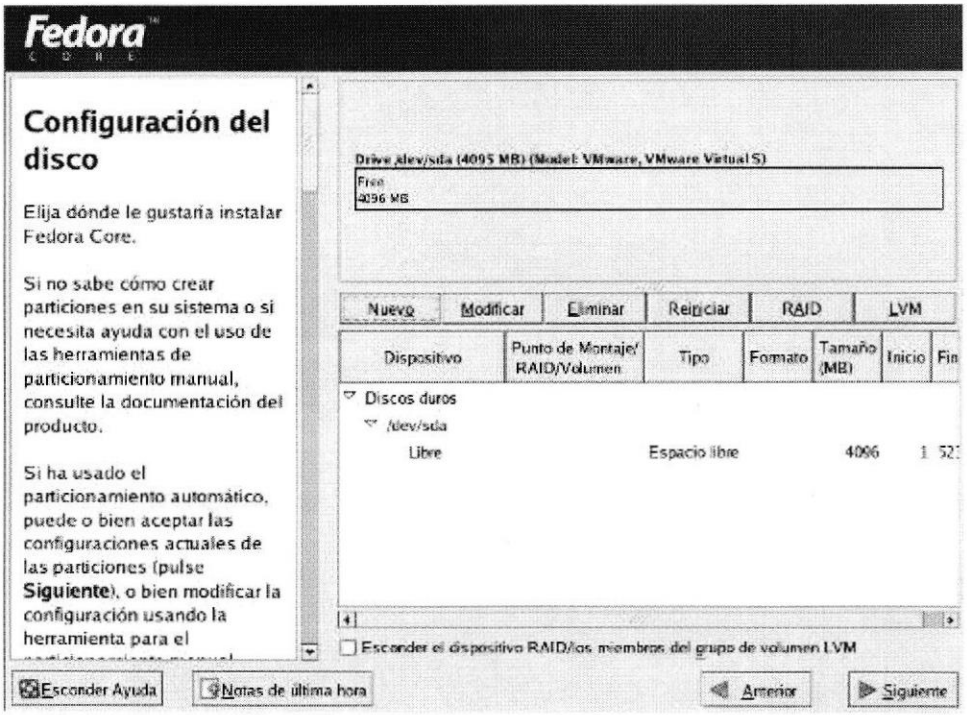


Figura 6.21 Pantalla de Configuración del disco.

Disk Druid muestra las siguientes acciones en el programa de la instalación:

- **Nuevo**
  Seleccione esta opción para agregar una partición o volumen físico LVM al disco. En el diálogo de añadir partición elija un punto de montaje y un tipo de

partición. Si usted tiene más de un disco en el sistema, Elija en cual de los discos la partición se creará. Indique un tamaño en megabytes para la partición.

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

Después que de ingresar los detalles para la partición, seleccione **ACEPTAR** para continuar.

Modificar

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

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

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

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

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

  Si usted necesita realizar cambios drásticos para la configuración de la partición, Usted quisiera borrar las particiones y empezar de nuevo. Si su disco contiene los datos que usted necesita guardar, Respáldelos

antes de que edite alguna partición, Si usted corrige el tamaño de una partición, usted podría perder todos los datos sobre este.

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

Eliminar

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

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

Reiniciar

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

Raid

Seleccione este botón para instalar el programa RAID sobre su sistema Fedora.

- **Crear un programa de partición RAID,** elija esta opción para agregar una partición para programas RAID. Esta opción es la única elección disponible si su disco no contiene programas para particiones RAID.

- **Crear un dispositivo RAID,** escoja esta opción para construir un dispositivo RAID a partir de dos o mas programas existentes de particiones RAID. Esta opción está disponible si se han configurado dos o más programas de las particiones RAID.

- **Clone un dispositivo para crear un dispositivo RAID,** elija esta opción para instalar un espejo RAID de un disco existente. Esta opción esta disponible si dos o más discos se unen al sistema.

LVM

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

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

Usted no debería quitar un volumen físico de un grupo de volumen haciendo esto podría dejar espacio insuficiente para los grupos de volúmenes lógicos.

Por ejemplo, si un grupo de volumen se compone de dos particiones de volumen físicas de 5GB. LVM, entonces contiene un volumen lógico de 8 GB. El instalador no permitiría que usted remueva luego de los componentes de volúmenes físicos, eso dejaría solamente 5 GB en el grupo para un volumen lógico de 8 GB.

Si usted reduce el tamaño total de cualquier volumen lógico apropiadamente, usted puede entonces quitar un volumen físico a partir de un grupo de volumen. En el ejemplo, la reducción del tamaño del volumen lógico a 4 GB. Permitiría que usted quitara uno de los volúmenes físicos de 5 GB.

- Como ya se conoce la función de cada uno de los botones que aparecen en la pantalla de **Configuración de Discos** se procede a crear las particiones debidas.

La primera partición a crear es la **raíz** la cual se representa con un / y es partición principal, donde se guardará todo el sistema de archivo. A esta partición se le asigna 5000mb. Una vez introducido estos valores dar clic en **Aceptar.**

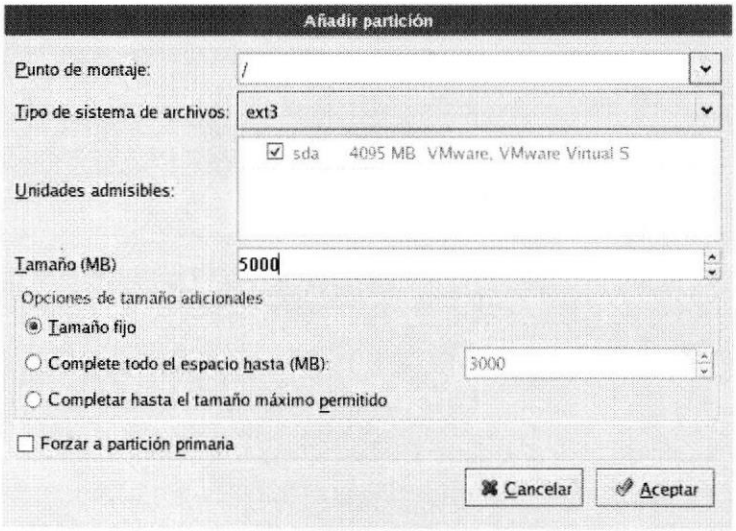


Figura 6.22 Creación de la partición raíz.

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

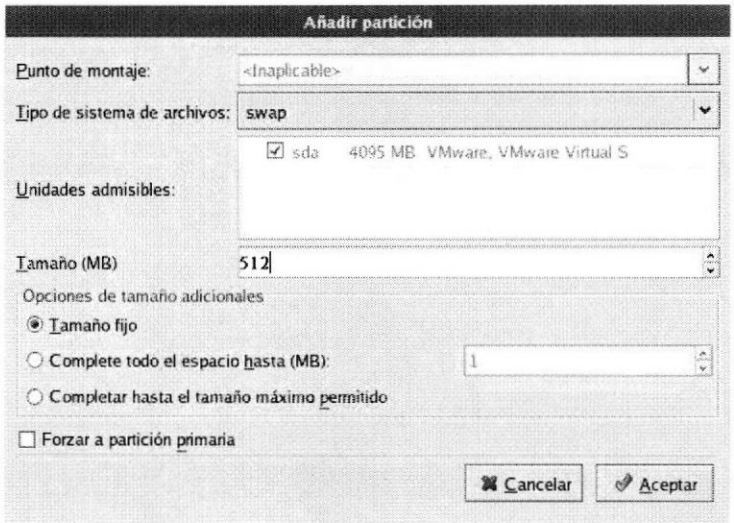


Figura 6.23 Creación de la partición swap.

La última partición que se crea es la **/boot** la cual sirve de ayuda cuando se instala otro sistema operativo en la misma computadora. A esta partición se le asigna 100 mb que es el tamaño mínimo. Una vez introducido estos valores se debe dar clic en **Aceptar**.

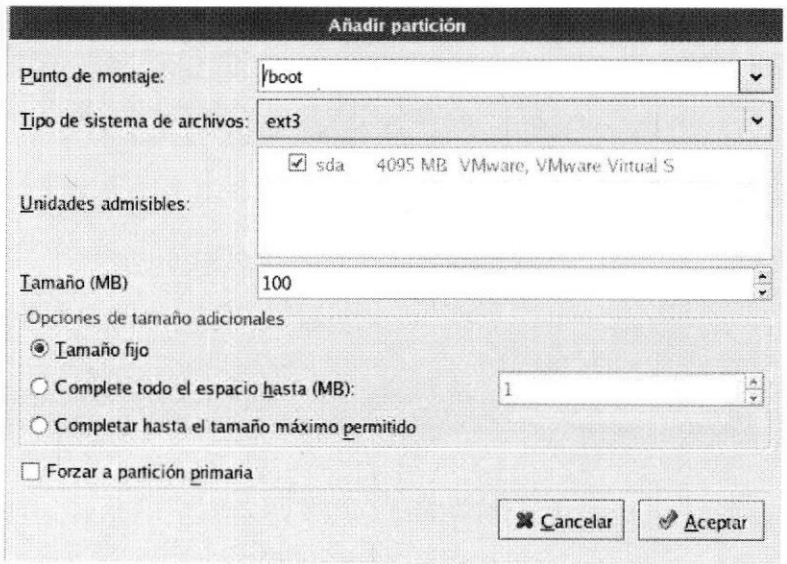


Figura 6.24 Creación de la partición /boot.

Nota: Sino se crea esta partición no habría ningún inconveniente porque Linux es el único sistema operativo instalado.

- Después de que se crean todas las particiones y se revisan las configuraciones de partición, hay que seleccionar **Siguiente** para continuar con el proceso de instalación.

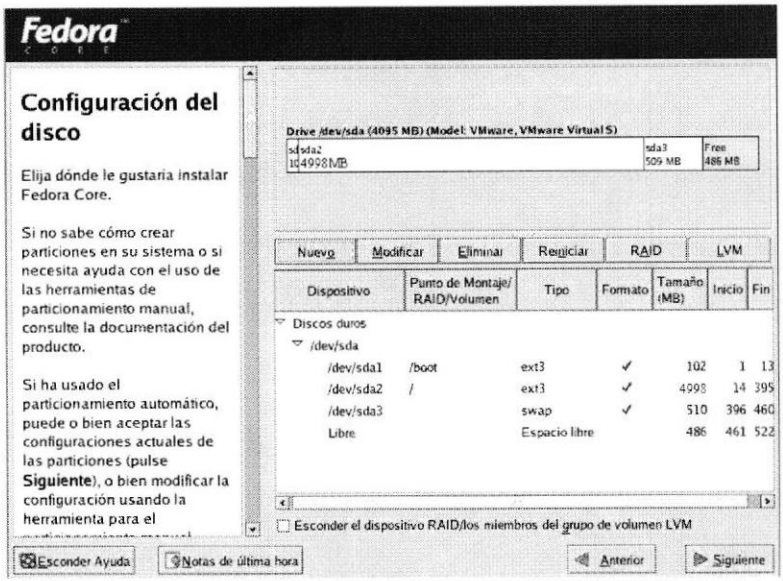


Figura 6.25 Detalle de las particiones creadas.

Paso 9: Luego de crear las particiones necesarias, se debe configurar el gestor de arranque.

- **Gestor de Arranque:** Un gestor de arranque es un pequeño programa que lee y principia el sistema operativo. Fedora Core 3 utiliza el gestor de arranque **GRUB** por defecto. Si usted tiene múltiples sistemas operativos, el gestor de arranque determina con cual arrancar, generalmente mostrando un menú.

  Usted deberá tener instalado un gestor de arranque en su sistema. Un sistema operativo puede instalar su gestor de arranque preferido, o usted pudo haber instalado una tercera persona del gestor de arranque. Si su gestor de arranque no reconoce las particiones Linux, Usted no podrá arrancar Fedora Core 3. Utilice **GRUB** como su gestor de arranque para arrancar Linux y otros sistemas operativos más. Siga las instrucciones en esta sección para instalar **GRUB.**

- Seleccione el Sistema operativo que se va a iniciar de manera predeterminada cada vez que encienda el computador, en este caso Fedora es el único sistema operativo instalado en la máquina, por lo cual se dará clic en **siguiente**.

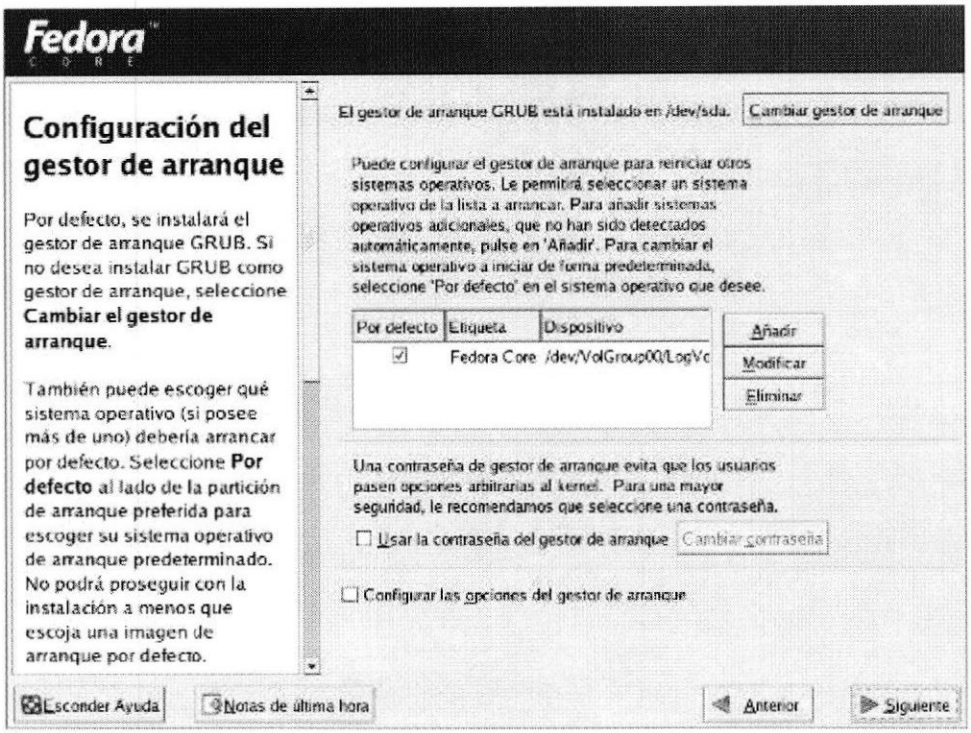


Figura 6.26 Pantalla de configuración del gestor de arranque.

Nota: Si usted instala GRUB, este se sobre escribirá en su gestor de arranque actual ya que este se ubica en el MBR (Master Boot Records) y como es de conocimiento solamente puede existir un gestor de arranque en el sistema.

Arranque de sistemas operativos adicionales: Si usted tiene otros sistemas operativos ya instalados, Fedora Core 3 apunta a detectarlos automáticamente y configurar el **GRUB** para arrancar desde ellos.

Para agregar, quitar o cambiar la configuración de los sistemas operativos detectados, utilice las opciones proporcionadas.

- **Agregar,** presione el botón agregar para incluir un sistema operativo adicional en el GRUB.

  Seleccione la partición del disco duro la cual contiene el sistema operativo a partir de la lista e ingresa una etiqueta. **GRUB** muestra esta etiqueta en su menú de arranque.

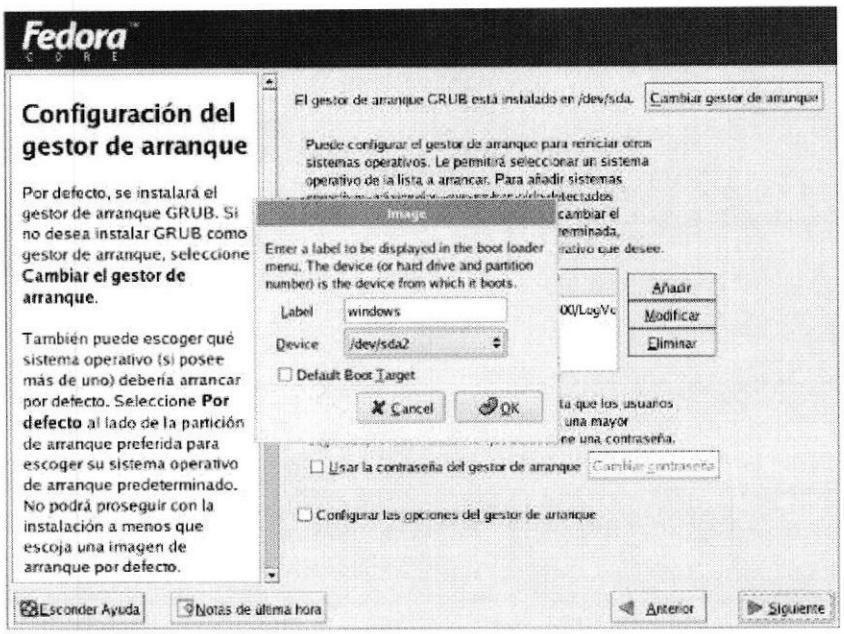


Figura 6.27 Agregar sistemas operativos en e menú de arranque.

- **Modificar,** para cambiar una entrada en el menú de arranque del GRUB, seleccione la entrada y luego seleccione **modificar.**

- **Eliminar,** para quitar una entrada del menú de arranque del GRUB, seleccione la entrada y luego presione **Eliminar.**

Paso 10: Después de asignar el orden de buteo de los sistemas operativos instalados en la computadoras, aparecerá una pantalla para configurar dispositivos de red.

Utilice esta pantalla para modificar los ajustes de la red de su sistema Fedora. La configuración de red manual de un sistema Fedora Core 3 no se requiere a menudo.

Muchas redes tienen el servicio de DHCP (Dynamic Host Configuration Protocol) que proporciona automáticamente sistemas conectados con datos configurados.

Por defecto, Fedora Core 3 activa todas las interfaces de red sobre el computador y los configura para usar DHCP.

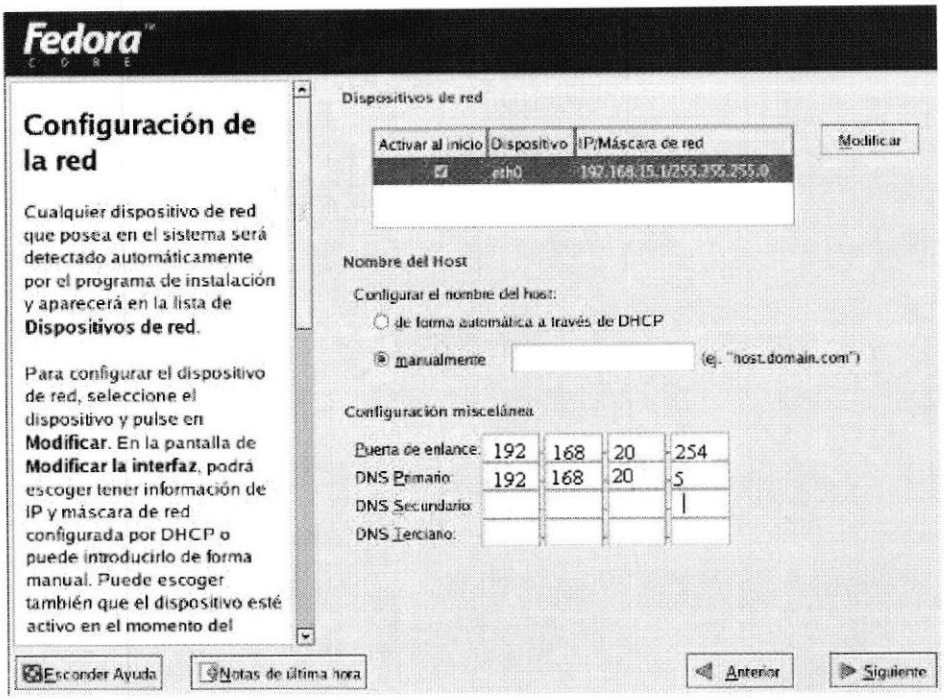


Figura 6.28 Pantalla de configuración de la red.

- **Dispositivos de red:** Fedora muestra una lista de interfaces de red en su computador. Cada interfaz debe tener una dirección IP única en la red a la cual pertenecen. La interfaz debe recibir esta dirección desde la red por el servicio DHCP si este esta seleccionado.

  Para asignar una dirección IP manualmente, sombree la interfaz en la lista de **Dispositivo de red** y seleccione **Modificar.** Entonces Fedora muestra un dialogo de configuración de red. Deseleccione la opción **Configurar usando DHCP,** entonces una vez que aparece en blanco, Ingrese la **dirección IP** y **máscara de sub red** apropiada para la interfaz. Luego presione **Aceptar**

  Si su computador será un servidor, no utilice DHCP. Configure la red manualmente en vez de eso. Configuraciones de red manuales permiten a su servidor ingresar a la red local aunque el proveedor de DHCP este caído.

  Especifique si una interfaz debe activarse automáticamente a la hora de arrancar con el checkbox **Activar al inicio** seleccionado para ese dispositivo. Usted puede activar manualmente una interfaz de red en cualquier momento después de que el sistema haya cargado.

- **Nombre del computador:** En algunas redes, el servidor DHCP también suministra el nombre del computador, o hostname. Para especificar el hostname, seleccione **manualmente** e ingrese el nombre completo del equipo en el campo.

  El hostname completo incluye el nombre del equipo y el nombre del dominio del cual es miembro, como por ejemplo maquina1.topico.com. El nombre del equipo (o "hostname corto") es maquina1, y el nombre del dominio es topico.com.

Usted puede dar a su sistema cualquier nombre asegurando que el hostname completo es único. El hostname puede incluir, letras, números y guiones.

- **Ajustes diversos:** Para configurar manualmente una interfaz de red, usted también puede proporcionar otros ajustes de red para su computador. Todos estos ajustes son direcciones IP de otros sistemas en la red.

  Una puerta de enlace es un dispositivo que proporciona conectividad a otras redes. Puertas de enlace también son representadas como routers. Si su sistema se conecta a otras redes a través de una puerta de enlace, ingrese su dirección IP in la casilla de **Puerta de enlace.**

  La mayoría de programas confían en el proveedor del servicio DNS (Domain Name System) para localizar equipos y servicios en la red. DNS convierte hostname en direcciones IP y viceversa. Un sistema Fedora Core debería usar más de un servidor DNS. Si el servidor DNS primaria no responde, el computador envía una consulta al servidor DNS secundario. Para asignar servidores DNS, ingrese sus direcciones IP dentro de las casillas de servidor DNS Primario, Secundario, o Terciario.

  Seleccione **Siguiente** una vez que se encuentre satisfecho con los ajustes de la red para su sistema.

Paso 11: En esta pantalla podrá habilitar las configuraciones de seguridad por defecto de Linux Fedora Core 3.

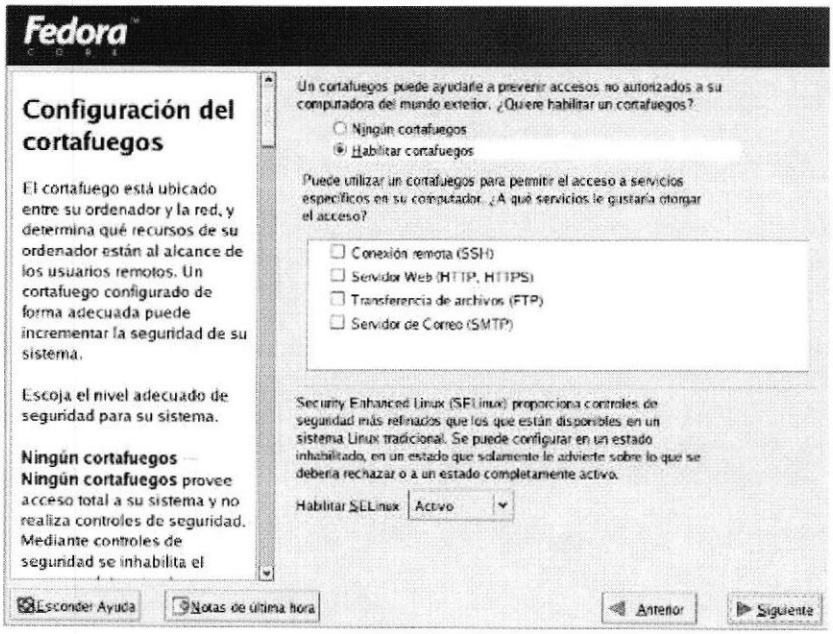


Figura 6.29 Pantalla de configuración de seguridad.

Seleccione **Siguiente** luego de revisar la configuración de seguridad y realizar algún cambio necesario.

Paso 12: Luego es necesario seleccionar la 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.

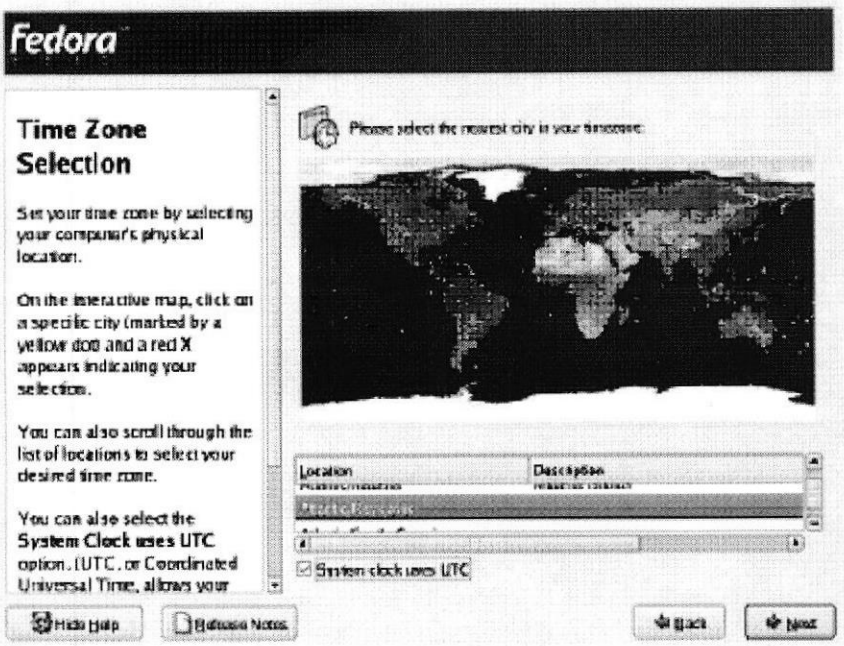


Figura 6.30 Pantalla de configuración de zona horaria.

Para seleccionar una zona horaria usando el mapa, seleccione el punto amarillo que representa la ciudad más cercana a su ubicación. Cunado usted se ubica la flecha en un punto, Fedora muestra el nombre de la ciudad abajo del mapa.

Una vez seleccionado un punto, este se convierte en una **X** roja para indicar su selección.

Para seleccionar una zona horaria usando la lista, seleccione el nombre de la ciudad más cercana a su ubicación. Las ciudades están listadas en orden alfabético.

Paso 13: Debe asignarle una contraseña al usuario root, para poder seguir adelante con la instalación.

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

- **Usando la cuenta root:** Evite ingresar en el sistema Fedora Core 3 como root cuando sea posible, cualquier herramienta de administración necesita de privilegios de root y preguntará por la contraseña.

  El programa de instalación de Fedora requiere la contraseña del usuario root que debe de ser por lo menos de seis caracteres. Por que la cuenta root puede

controlar potencialmente cualquier parte del sistema, use las siguientes pautas para crear una buena contraseña.

- Utilice una combinación de letras mayúsculas, letras minúsculas, números, signos de puntuación y otros caracteres.
- No utilice la misma contraseña para más de un sistema.

Los siguientes son ejemplos de contraseñas seguras:

- f9*@1Ls99A
- HL8$391%%rb

Ingrese la contraseña del usuario root en el campo **Contraseña del root**. Fedora muestra los caracteres como asteriscos por seguridad. Ingrese la misma clave en el campo confirmar para confirmar que esta correcta.

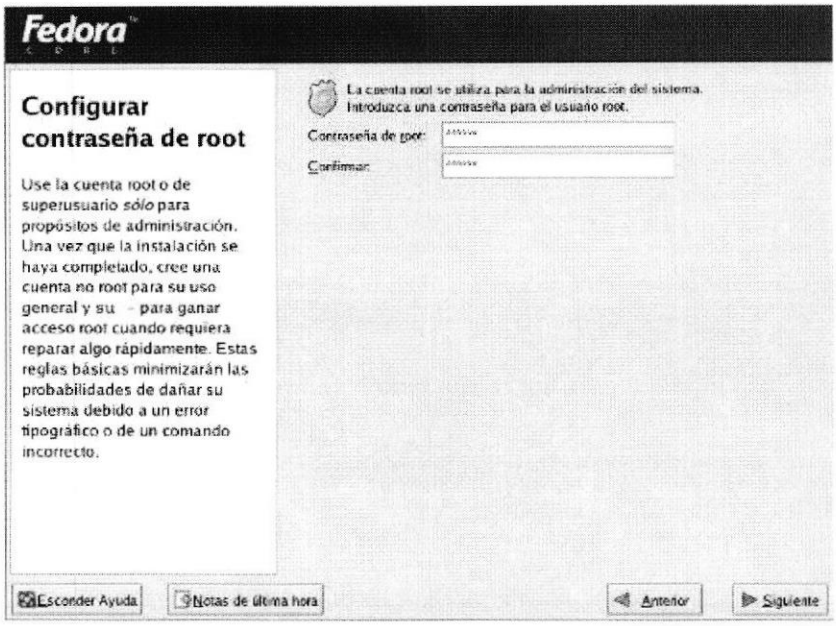


Figura 6.31 Pantalla de configuración de la contraseña de root.

Después de que ingresa la contraseña para el root, presione siguiente para continuar.

Paso 14: Ahora debe seleccionar el grupo de paquetes a instalar.

- **Selección de paquetes:** Fedora utiliza el tipo de instalación para seleccionar un juego de paquetes de programas para su sistema. Usted puede aceptar este juego de paquetes o Elegirlo a su gusto para cumplir con sus preferencias.

  Si usted escoge el tipo de instalación personalizada, Fedora Core 3 muestra la pantalla de **Selección de grupo de paquetes** automáticamente.

El tipo de instalación y los paquetes que usted selecciona no son permanentes. Después de que arranca el sistema, utilice la herramienta de manejo de paquetes para seleccionar programas diferentes para su sistema.

Para ejecutar esta herramienta, desde el menú principal, seleccione **Escritorio->Configuración del sistema->Agregar o quitar aplicaciones.**

- **Paquetes de instalación por defecto:** Para aceptar la selección de paquetes por defecto, seleccione **Instalar los paquetes de software por defecto**. Seleccione **Siguiente** para continuar.

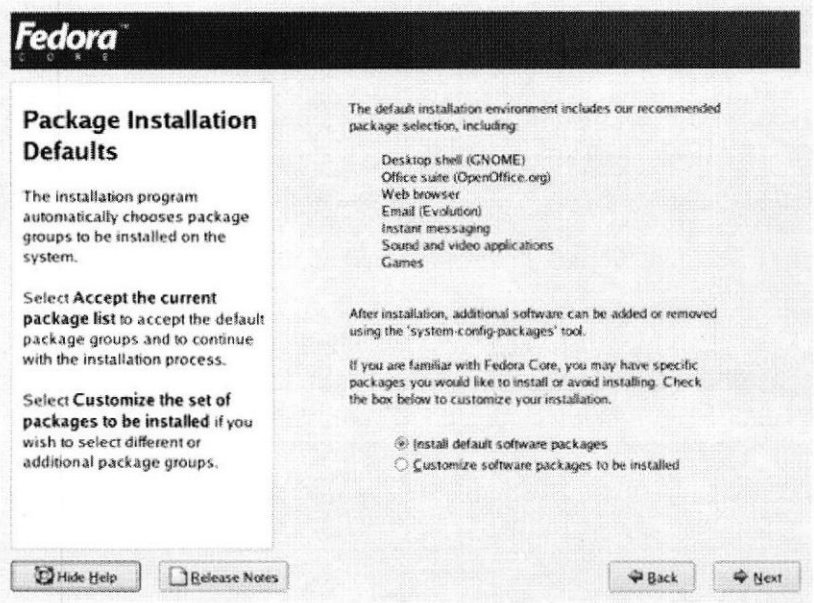


Figura 6.32 Pantalla de instalación de paquetes por defecto.

Para ver o cambiar los paquetes, seleccione **Personalizar los paquetes de software que será instalado**. Presione **Siguiente** para continuar.

- **Selección del grupo de paquetes:** Fedora Core 3 divide el software en grupos de paquetes que hacen la selección más fácil.

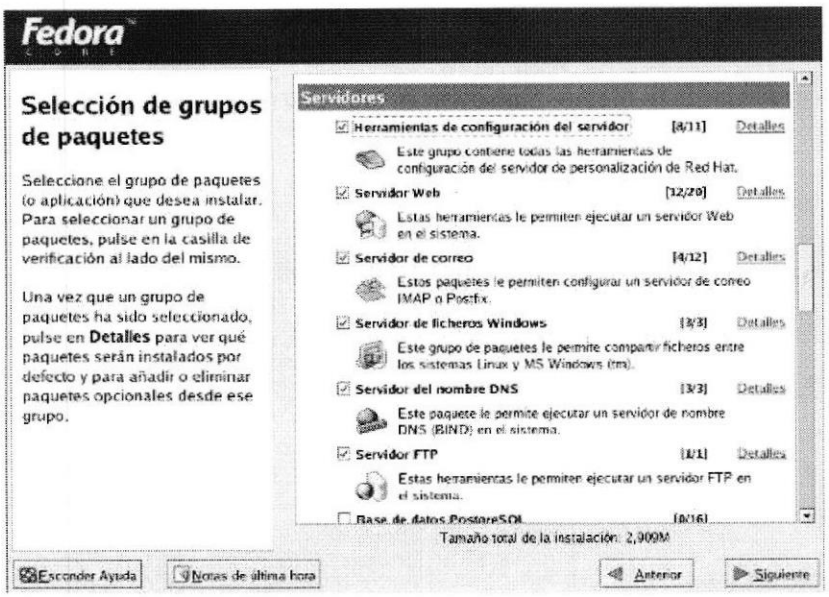


Figura 6.33 Pantalla de selección de grupos de paquetes.

Los grupos por defecto para el tipo de instalación escogida están todavía seleccionados. Seleccione o quite cualquier grupo de paquetes según lo deseado. No se instalará ninguno de los paquetes de un grupo a menos de que la casilla a lado del grupo este seleccionada.

Para cambiar cuales paquetes sin un grupo seleccionado será instalado, seleccione el link de **Detalles** al lado del nombre del grupo. Fedora Core 3 instala automáticamente los **Paquetes Base** de un grupo si el grupo es seleccionado. Cambie la opción de **Paquetes opcionales** usando la casilla a lado del nombre de los paquetes individuales.

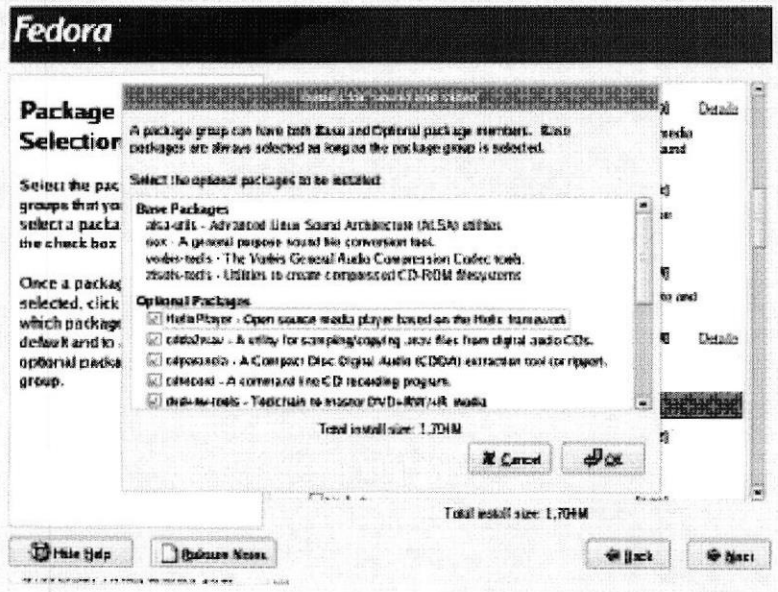


Figura 6.34 Dialogo del detalle de grupo de paquetes.

Paso 15: Luego de haber seleccionado el grupo de paquetes necesario para la instalación, proceda a dar clic en siguiente y debe aparecer un a pantalla con información acerca de la instalación.

- **Acerca de la instalación:** No se realiza ningún cambio a su computador hasta que usted presiona el botón **Siguiente**. Si usted interrumpe el proceso de instalación después de este punto, el sistema Fedora Core estará incompleto e inutilizable.

  Para volver a las pantallas anteriores para realizar diferentes selecciones, seleccione **Regresar** para interrumpir la instalación, apague el computador.

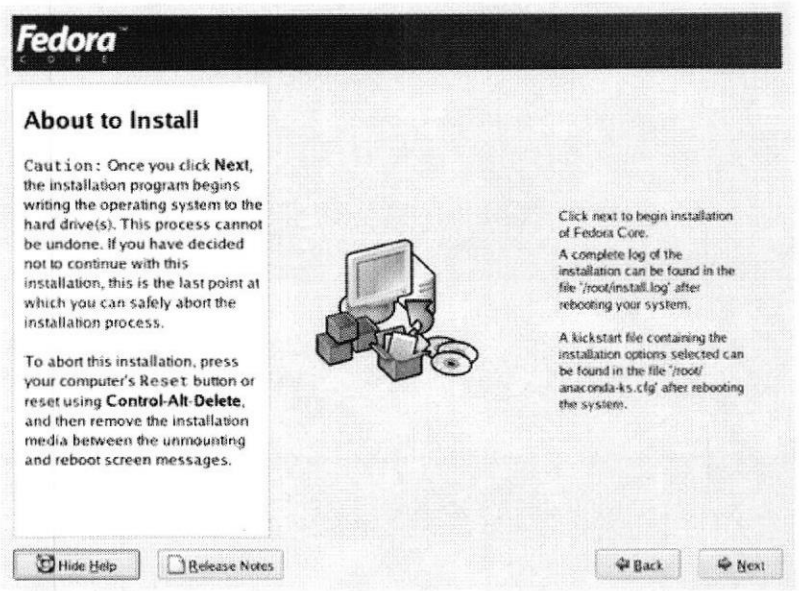


Figura 6.35 Pantalla de acerca de la instalación.

Presione **siguiente** para comenzar la instalación

Si su instalación requiere más de un disco, Fedora Core 3 muestra una lista de todos los discos requeridos para completar el proceso. Si usted no tiene todos los discos necesarios, seleccione **Reiniciar** para interrumpir la instalación. Si no, escoja **Continuar** para procedes con la instalación.

Paso 16: Ahora comenzará la instalación de los paquetes. Conforme la instalación avance, el sistema de instalación, pedirá que se inserte en la bandeja de CD-ROM los CD necesarios para llevar cabo con éxito la instalación.

- **Instalando paquetes:** Fedora Core 3 reporta el progreso de la instalación en la pantalla mientras que instala los paquetes seleccionados al sistema, seleccione **Siguiente** para continuar la instalación.

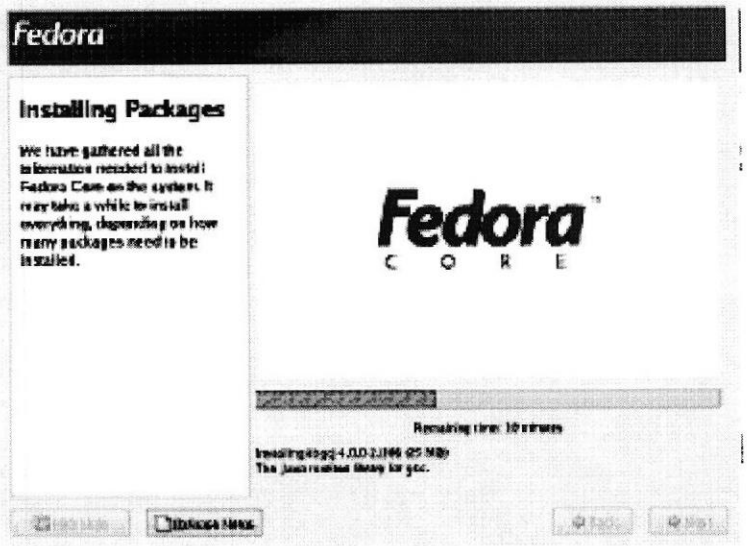


Figura 6.36 Pantalla de instalación del paquete.

Luego de que se complete la instalación, seleccione **Reiniciar** para restaurar el equipo. Fedora Core expulsa cualquier disco cargado antes de que el computador se reinicie. (Figura 6.28)

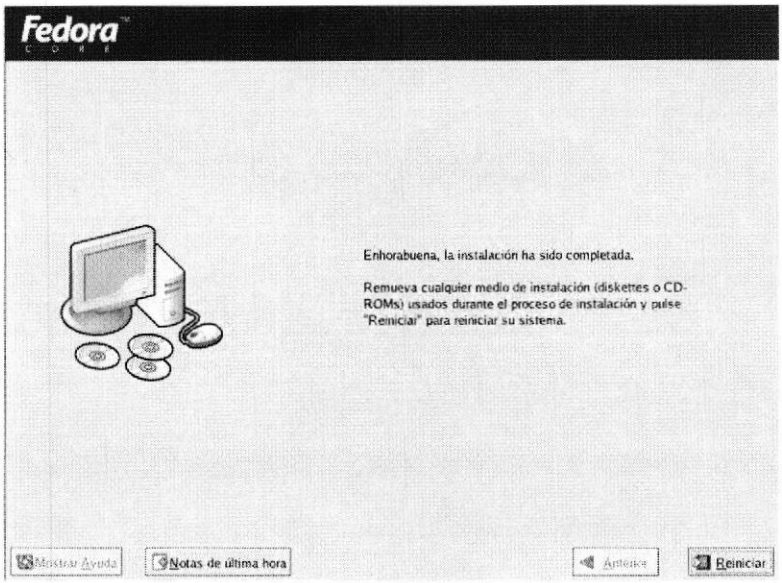


Figura 6.37 Pantalla de instalación terminada.

Paso 17: En este momento ya se puede decir que ha acabado la instalación, aunque aún quede por configurar ciertos dispositivos. Luego de que se cargue el sistema por primera vez aparecerá una pantalla de bienvenida.

- **Primer arranque:** El Agente de configuración se carga la primera vez que usted inicia un nuevo sistema de Fedora Core.

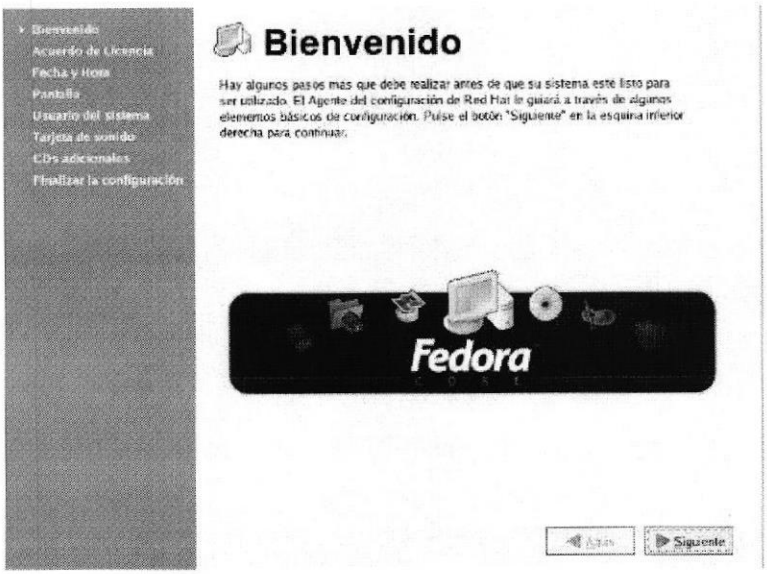


Figura 6.38 Pantalla de bienvenida.

Seleccione **Siguiente** para comenzar el agente de configuración

- **Acepte el acuerdo de licencia:** Esta pantalla exhibe los términos de licencia que contiene Fedora Core 3. Cada paquete de software en Fedora Core 3 está cubierto por su propia licencia que ha sido aprobada por la OSI Open Source Initiative (iniciativa de Código abierto).

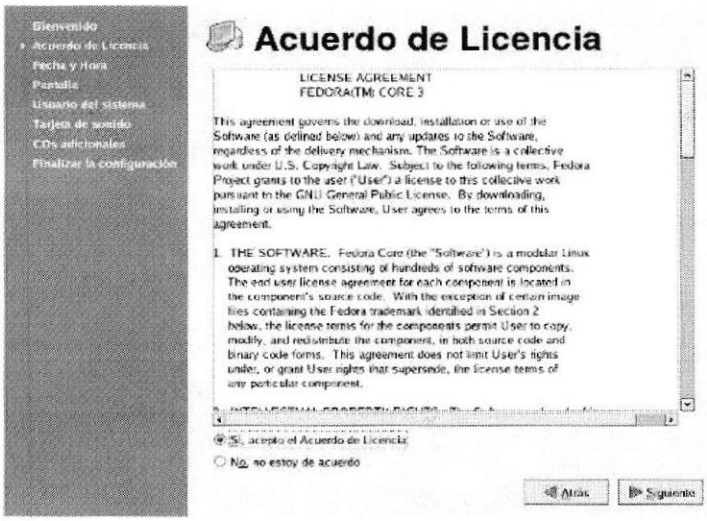


Figura 6.39 Pantalla de acuerdo de Licencia.

Para proceder, seleccione **Si, acepto el Acuerdo de Licencia** y después seleccionar **Siguiente.**

- **Fecha y hora:** Si su sistema no tiene el acceso a Internet o un servidor de tiempo en la red, Fije manualmente la fecha y la hora para su sistema en esta pantalla. Si no, utilice los servidores NTP (Network Time Protocol) para mantener la exactitud del reloj. El NTP proporciona servicio de sincronización a los computadores en la misma red.

El Internet contiene muchas computadoras que ofrecen servicios públicos NTP.

La exhibición inicial le permite fijar la fecha y la hora de su sistema manualmente.

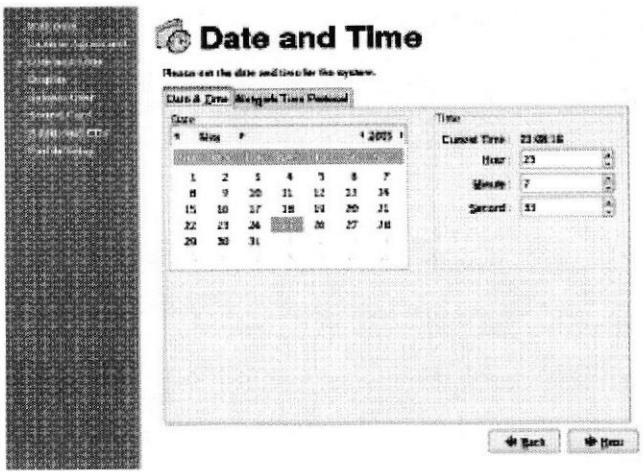


Figura 6.40 Pantalla de Fecha y Hora.

- **Resolución:** El agente de configuración automáticamente procura identificar la tarjeta gráfica y el monitor para su computador. Este usa esta información para calcular la **Resolución** y la **Definición del Color.**

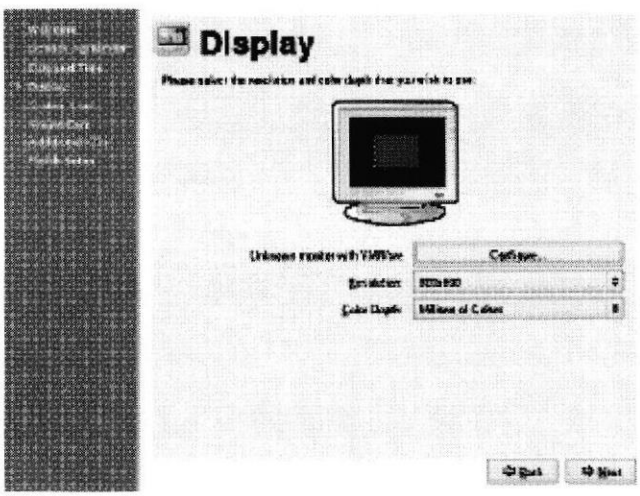


Figura 6.41 Pantalla de resolución.

Si usted necesita cambiar el monitor, seleccione **Configurar** para mostrar una lista de fabricantes. Seleccione el fabricante de su monitor en la lista, y presione la tecla + o seleccione el triángulo a lado del nombre para ver modelos soportados. Elija el modelo correcto de la lista y seleccione **OK**. Si ninguno de la lista coincide con su monitor, seleccione el más cercano de la lista, la lista **Generic CRT Display** o la lista **Generis LCD Display.**

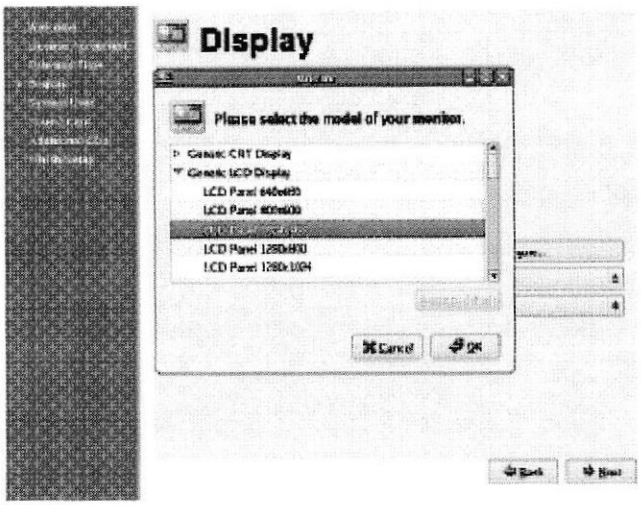


Figura 6.42 Diálogo de Monitor.

- **Usuario del sistema:** Cree una cuenta de usuario para usted con esta pantalla. Siempre use esta cuenta para iniciar sesión en su sistema Fedora Core 3, En el caso de administrar varios servicios puede usar la cuenta de root y saltar este paso.

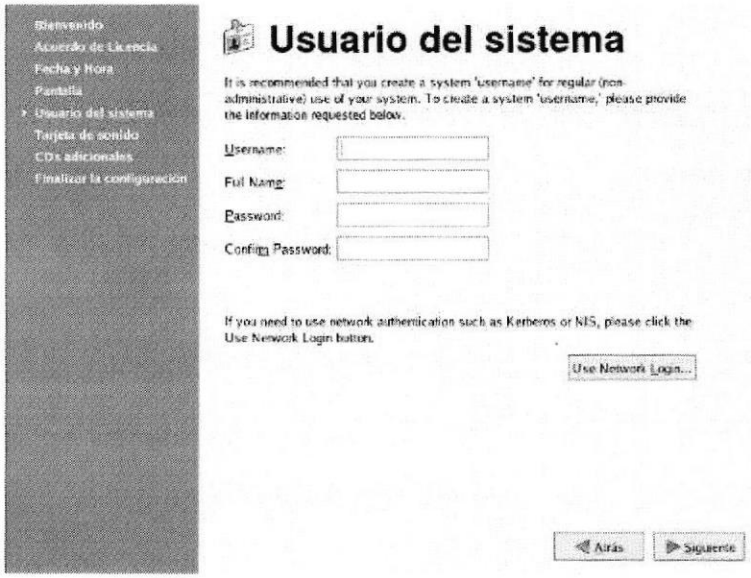


Figura 6.43 Pantalla de usuarios del sistema.

Ingrese un nombre usuario y su nombre completo, y luego una clave escogida. Ingrese la clave una vez más in el campo **Confirmar contraseña** para asegurar de que esta correcta

- **Tarjeta de sonido:** El agente de configuración automáticamente procura identificar la tarjeta de sonido en su computador.

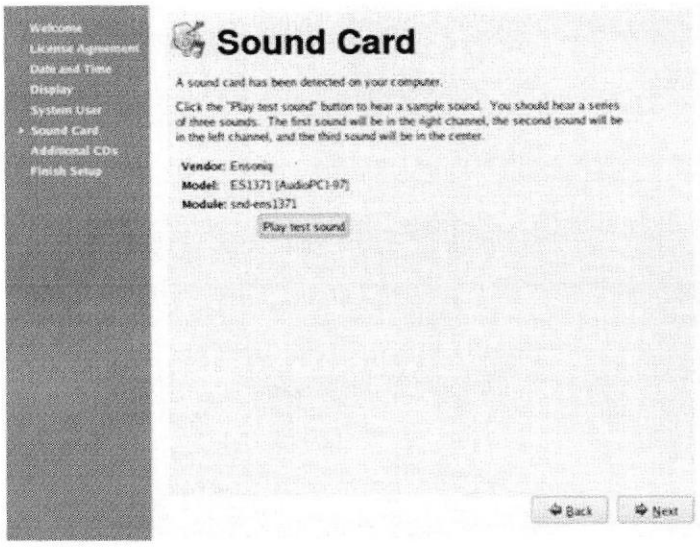


Figura 6.44 Pantalla de Tarjeta de sonido.

Presione **Realice una prueba de sonido** para comprobar la configuración de la tarjeta de sonido. Si esta configuración es correcta, Fedora Core 3 carga una secuencia de sonido. Si la tarjeta de sonido es identificada, pero usted no escucha el volumen, Verifique los speakers e intente de nuevo.

Usted puede configurar manualmente el sistema Fedora Core 3 para utilizar tarjetas de sonido.

- **Discos adicionales:** Esta pantalla te permite cargar discos preparados para la instalación programas en tercera persona. Sin embargo, usted no puede usarlo para instalar paquetes adicionales desde los discos de Fedora Core 3.

- **Agregar Software:** Para agregar paquetes de programas desde los discos de Fedora Core 3, use la herramienta **Administración de paquetes** después de que inicia sesión.

  Desde el menú principal, seleccione **Escritorio->Configuración del sistema-> Añadir/Eliminar aplicaciones.**

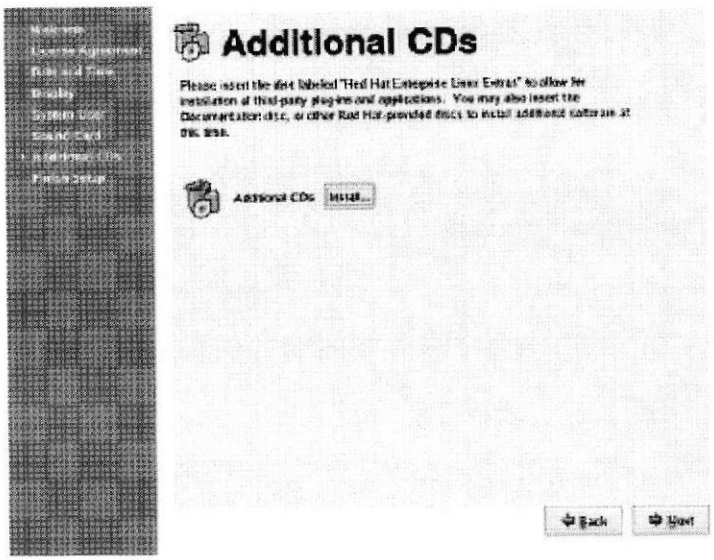


Figura 6.45 Pantalla de discos adicionales.

Seleccione **Siguiente** para continuar con la pantalla final.

Figura 6.46 Pantalla de configuración final.

Presione **Siguiente** para proceder con la pantalla de inicio de sesión. Su sistema Fedora Core 3 ahora esta listo para que lo utilice.

6.5 INICIANDO LINUX.

Una vez instalado linux en la pc, cada vez que este arranque mientras se cargue el sistema operativo se observará la siguiente pantalla.

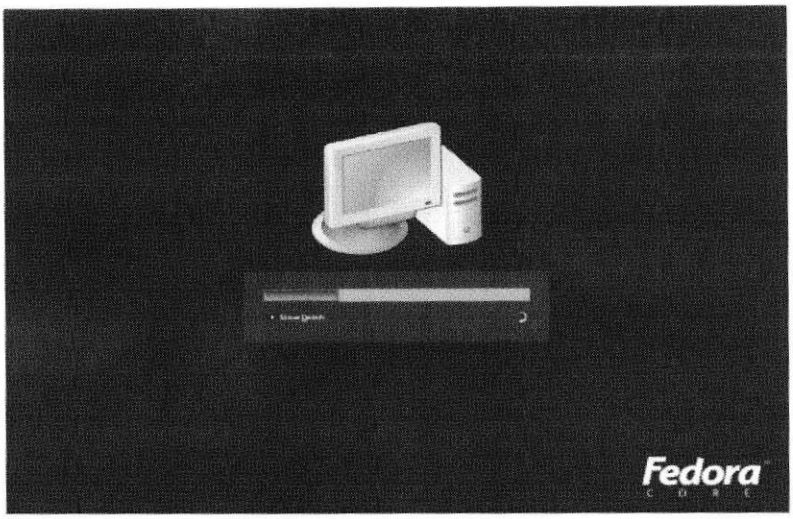


Figura 6.47 Pantalla de inicio de Linux.

6.5.1 INICIO DE SESIÓN EN LINUX.

Para iniciar sesión en una instalación de Linux normalmente existen dos opciones las cuales son:

- Modo texto y
- Modo Gráfico

6.5.1.1 INICIO DE SESIÓN EN LINUX (MODO TEXTO).

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.

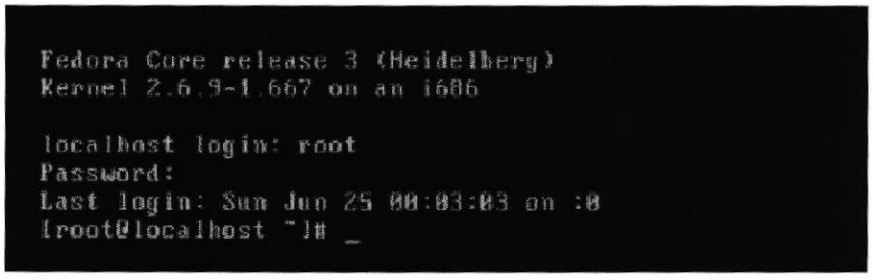


Figura 6.48 Pantalla de inicio de sesión en modo texto.

Cuando usted ha realizado una instalación de Linux agregando el modo gráfico este se cargará por defecto

6.5.1.2 INICIO DE SESIÓN EN LINUX (MODO GRÁFICO).

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

Este procederá primeramente a solicitar el ingreso del 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.

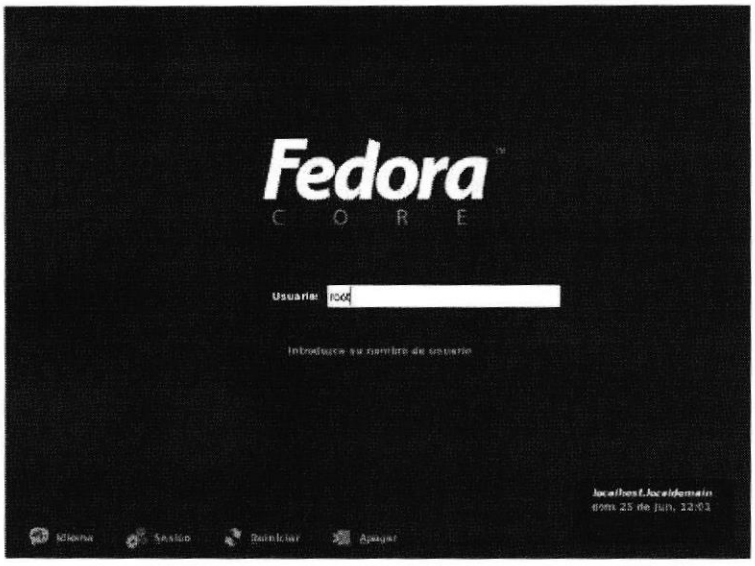


Figura 6.49 Pantalla de inicio de sesión en modo gráfico usuario.

Una vez que se ingresa el usuario, solicitará ingresar la clave o password para poder acceder al sistema operativo con todos los privilegios que el mismo ofrece.

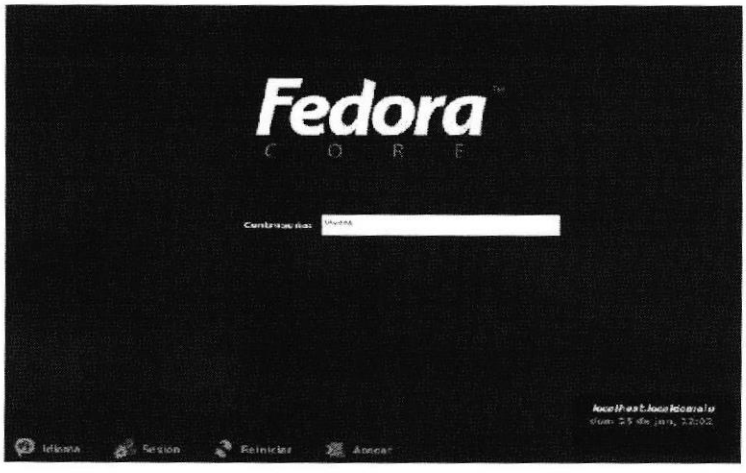


Figura 6.50 Pantalla de inicio de sesión en modo gráfico contraseña.

A continuación se observará el entorno de Linux (escritorio), el mismo que tiene similitud con el sistema operativo de Windows.

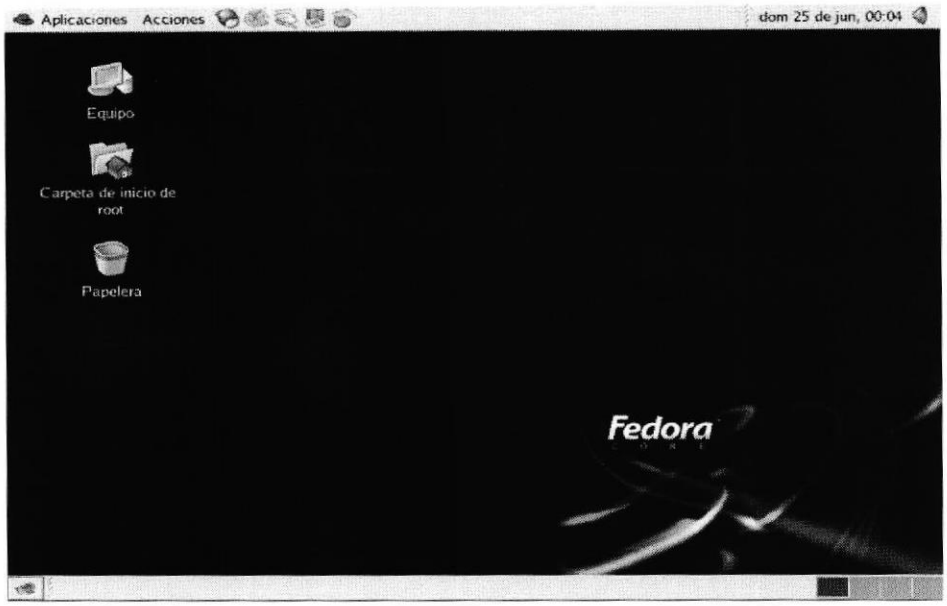


Figura 6.51 Entorno Linux.

6.6 COMANDOS EN LINUX.

- ls

  Para ver el listado de archivos disponibles en el computador remoto.

- cd

  Este comando permite cambiarse de directorio.
  Ejemplo: [root@localhost] **cd** /etc
  [root@localhost etc] _

  Si le agrega a este comando un espacio y dos puntos seguidos (..), permite salir del directorio actual.
  Ejemplo: [root@localhost etc]**cd ..**
  [root@localhost /] _

- cp [-rf] fuente destino

  Copia del archivo fuente al destino especificado. Si se usa la opción –rf también se copiaran subdirectorios.

- chmod

  Este comando modifica los permisos de un archivo o directorio.

- delete

  Para borrar un archivo del computador remoto.

- pwd

  Para examinar el directorio en el que está en el computador remoto.

- man

  Este comando muestra la página del manual del comando o recurso .

- ifconfig

  Este comando verifica la configuración de una tarjeta de red

- ping

  Este comando muestra las respuestas de una tarjeta de red.

  Ejemplo: **ping** 192.168.20.5

- more

  Este comando muestra el contenido de los ficheros indicados por pantallas, puede usarse en combinación con otros comandos.

- adduser

  Este comando agrega usuarios al sistema

- passwd

  Este comando agrega contraseñas a usuarios al sistema, y cuando se le agrega el parámetro –a permite agregar una contraseña para que el usuario tenga permiso de acceder al servicio samba.

- service

  Este comando sirve para ver los estados de cualquiera de los servicios de Linux y su sintaxis es: **service** <nombre del servicio> **estado**

status	Muestra el estado actual del servicio
stop	Detiene un servicio
start	Inicia un servicio
restart	Detiene la ejecución de un servicio y lo vuelve a arrancar.
reload	Recarga un servicio sin detener su ejecución

  Ejemplo

  service network status

- chmod

  Este comando modifica los permisos de un archivo o directorio, basándose en los siguientes valores:

Id	**significado**
w	escritura
r	lectura
x	ejecución

  Ejemplo

  chmod 777 vistazo

- touch

  Este comando crea archivos

- q

  Este comando detiene un proceso en ejecución.

- ctrl+c

  Esta combinación de teclas detiene un proceso en ejecución.

- Vi

Este comando sirve para editar texto. Para editar un texto con el editor vi, teclee desde un intérprete de comandos:

[root@localhost etc] `vi` espoltel.txt

Vi es un editor con dos modos: edición y comandos. En el modo de edición el texto que ingrese será agregado al texto, en modo de comandos las teclas que oprima pueden representar algún comando de vi. Cuando comience a editar un texto estará en modo para dar comandos el comando para salir es**:** seguido de **q** y **ENTER** --con ese comando saldrá si no ha hecho cambios al archivo o los cambios ya están salvados, para salir ignorando cambios **:q!** seguido de **ENTER**.

Teclas en vi para salir ignorando cambios.

Puede insertar texto (pasar a modo edición) con varias teclas:

- i

Inserta texto antes del carácter sobre el que está el cursor.

- a

Inserta texto después del carácter sobre el que está el cursor.

- I

Inserta texto al comienzo de la línea en la que está el cursor.

- A

Inserta texto al final de la línea en la que está el cursor.

- o

Abre espacio para una nueva línea después de la línea en la que está el cursor y permite insertar texto en la nueva línea.

- O

Análogo al anterior, pero abre espacio en la línea anterior.

- i.e.

Esta combinación de teclas copia un número de líneas, especificado con anterioridad. Para que este comando funcione a la perfección hay que ubicarse al inicio de las líneas a copiar, presionar y, y a continuación el numero de líneas que se van a copiar.

- p

Esta tecla permite tener en memoria las líneas que han sido copiadas con anterioridad y pegarlas en el momento que el usuario así lo desee.

- q!

Este comando permite salir de un fichero sin guardar cambios realizados.

- wq

Este comando guarda los cambios realizados dentro de un archivo, y sale del mismo.

Para pasar de modo edición a modo de comandos se emplea la tecla **ESC**, para desplazarse sobre el archivo puede emplear las flechas, PgUp, PgDn[1]. Para ir a una línea específica puede emplear **:** seguido del número de línea y **ENTER**, para ir al final de la línea en la que está el cursor **$**,para ir al comienzo **0**. Para buscar un texto **/** seguido del texto que desea buscar y **ENTER**. Después de hacer cambios puede salvarlos con **:w** o para salvar y salir puede emplear **ZZ**. Para ejecutar un comando del interprete de comandos puede emplear **:!** seguido del comando y **ENTER** (e.g `:!ls`).

6.7 CONFIGURACIÓN DE SERVICIOS LINUX.

Para poder hacer uso de los diferentes servicios que Linux ofrece, se debe tener dos computadores como mínimo, además hay que cumplir con ciertos requerimientos (hardware y software) esenciales para su funcionamiento, tanto del computador que va ha cumplir la función de servidor, como la del computador que ejercerá la función de cliente.

6.7.1 REQUERIMIENTOS BÁSICOS.

- Se necesita como mínimo dos computadores.

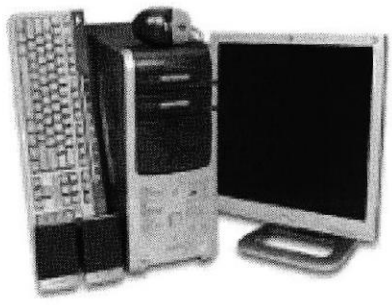


Figura 6.52 Computador de escritorio.

- El servidor debe tener instalado el Sistema Operativo **Fedora Core 3**. Mientras que el cliente el Sistema Operativo **Windows** en cualquiera de sus versiones para clientes.

Figura 6.53 Sistema Operativo para el servidor.

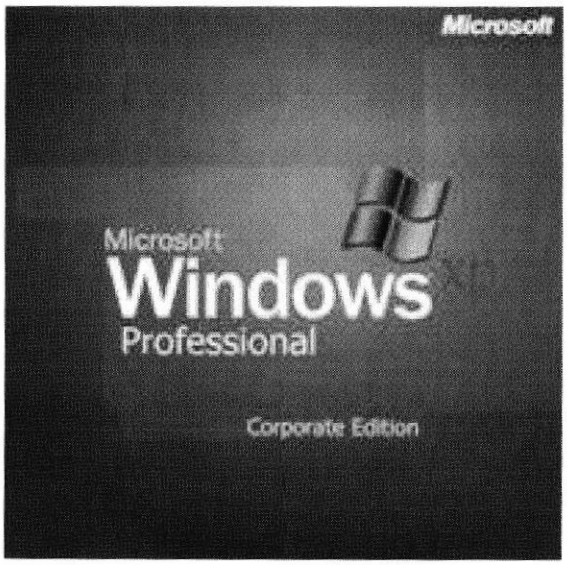


Figura 6.54 Sistema Operativo para el cliente.

- Una tarjeta de red 10/100 Mbps. **Como mínimo.** El servidor Linux puede tener más de una tarjeta de red.

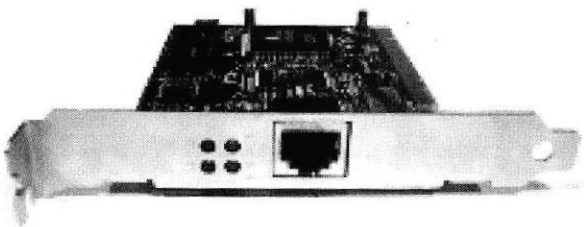


Figura 6.55 Tarjeta de red 10/100 Mbps.

- Ambos computadores deben estar conectados en red.

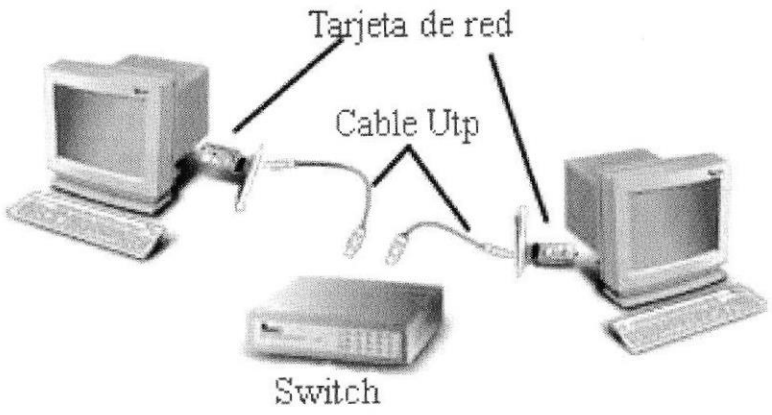


Figura 6.56 Esquema de conexión entre el servidor y el cliente.

6.7.2 CONFIGURACIÓN BÁSICA DE LA TARJETA DE RED.

Es necesario tener configurada la tarjeta de red para poder utilizar los servicios de Linux, porque esta es la que permite el enlace con la red.

6.7.2.1 CONFIGURACIÓN EN LINUX.

Antes de proceder con la configuración de la tarjeta se debe verificar si esta se encuentra configurada. Existen varias formas para comprobar si la tarjeta está o no deshabilitada. Entre estas existen:

- Digitando el comando **ifconfig** y presionando la tecla **enter.** Este comando muestra por pantalla la configuración de la tarjeta de red.

- Digitando el comando **service network status** y luego se presiona **enter.** Este comando permite saber el estado de la tarjeta de red.

Si al utilizar los métodos anteriores se verifica que la tarjeta no está habilitada o no se encuentra configurada de la manera que se necesita, se puede seguir cualquiera de estos tres métodos para configurarla:

Método 1. Ingrese a una terminal, estando en modo gráfico o texto, y digite la siguiente línea de comando:

[root@localhost]# **ifconfig** eth0 192.168.20.5 **netmask** 255.255.255.248 **up**

Sintaxis:

```
ifconfig <interface> <address> netmask up/down
```

Figura 6.57 Se muestra la sintaxis del comando ifconfig.

COMANDOS / OPCIONES	DESCRIPCION	EJEMPLO
ifconfig	Palabra reservada. Comando que permite configurar una interfaz de red.	
interface	Nombre de la interfaz ethernet.	eth0. Donde 0 indica la primera tarjeta de red.
address	Determina la ip que va a ser asignada a la tarjeta de red.	192.168.20.5
netmask	Palabra reservada. Determina la clase de la ip asignada.	255.255.255.224
Up/down	Palabra reservada. Esta opción es utilizada para que la interfaz sea activada UP o desactivada DOWN.	

Tabla 6-1 Comando, descripción y ejemplos.

Método 2. Ingrese a una terminal, estando en modo gráfico o texto, y digite el siguiente comando:

[root@localhost]# **netconfig**

- A continuación de este comando presione la tecla enter.
- Deberá aparecer la pantalla de configuración de red, dé clic en el botón **Si** para acceder a la configuración del protocolo TCP/IP.

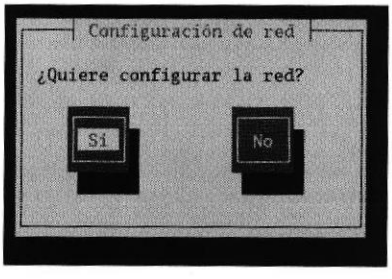


Figura 6.58 Pantalla de configuración de red.

- En esta ventana se puede asignar a la tarjeta de red: la dirección ip con su respectiva máscara de red, la puerta de enlace, la ip del servidor DNS.

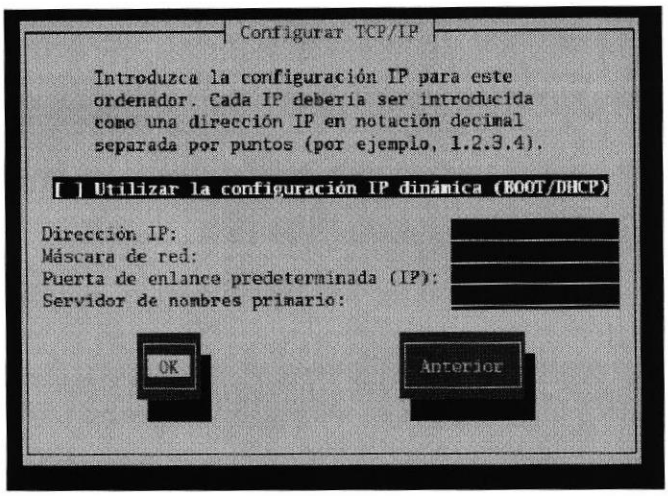


Figura 6.59 Pantalla sin la configuración del TCP/IP

- Para que el Servidor Samba funcione, es de vital importancia que estén configuradas por lo menos la Dirección IP y la Máscara de red.

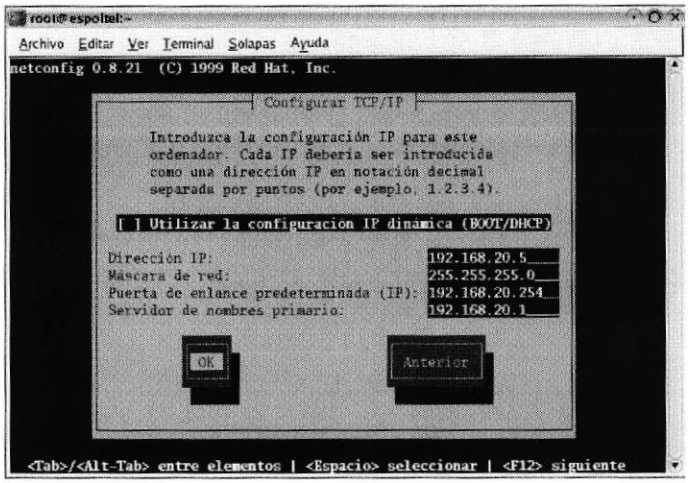


Figura 6.60 Pantalla de configuración del TCP/IP.

Nota: Es importante que la opción de "Utilizar la configuración IP dinámica" no este habilitada, por que si está habilitada no se podrá configurar de manera manual. Pero, si se desea utilizar un servidor DHCP para asignar automáticamente la dirección ip de la tarjeta de red, esta opción debe estar habilitada.

Método 3. Esta es la opción más recomendable de utilizar, porque se edita directamente el archivo que contiene la configuración de la tarjeta de Red. Se ingresa a una Terminal, estando en modo gráfico o texto, y se procede a digitar la siguiente línea de comando que contiene el archivo a editar:

[root@localhost]# **vi /etc/sysconfig/network-scripts/ifcfg-eth0**

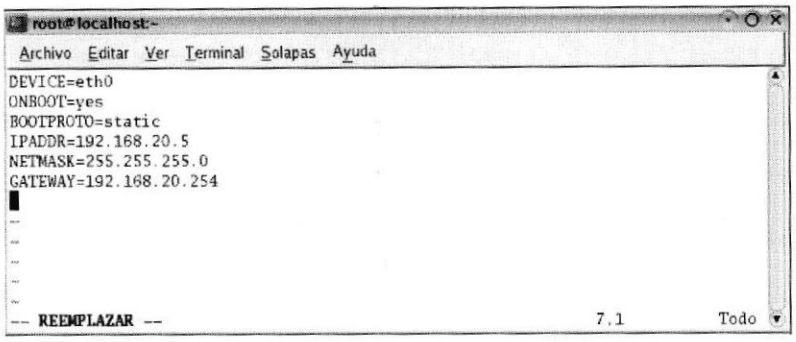


Figura 6.61 Captura de la salida por pantalla del archivo.

A continuación hay que inicializar el servicio de red, con el comando service parámetro start.

[root@localhost]# **service network start**

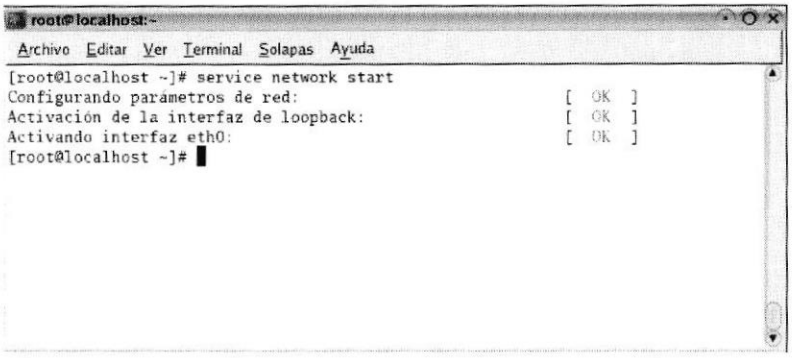


Figura 6.62 Captura de la salida por pantalla de la habilitación de la tarjeta de red.

Para comprobar que la tarjeta de red está habilitada, se debe abrir una Terminal y le hacer ping a la dirección ip de la tarjeta de red o digitar el comando ifconfig.

Si hay respuesta del ping realizado a la tarjeta, se puede decir que desde ese momento el servidor estará en red.

6.7.2.2 CONFIGURACIÓN EN WINDOWS.

- Existen dos métodos para acceder a la configuración de la tarjeta de red:

  Método 1. Clic en **Inicio/Todos los programas/Accesorios/Comunicaciones/ Conexiones de red.**

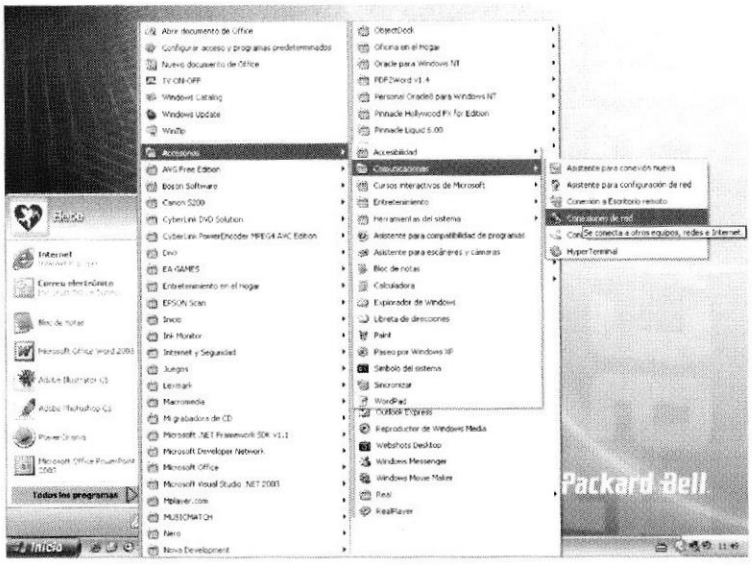


Figura 6.63 Entorno Windows.

Método 2. En la barra de tareas, del lado inferior derecho encontrará el icono de conexiones de área local. Dé clic sobre ese icono.

Figura 6.64 Icono de conexiones de área local.

El icono se encuentra en modo desconectado porque no tiene el cable de red conectado a la tarjeta de red.

- Ahora puede dar clic derecho y seleccionar **Propiedades** o dar doble clic sobre el icono.

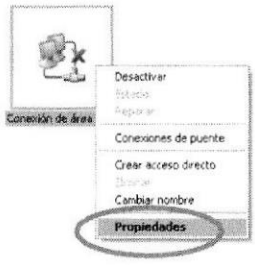


Figura 6.65 Opción Propiedades de la ventana de conexión de red local.

- Tendrá que aparecer la pantalla de **Propiedades de Conexión de área local.** Seleccione **Protocolo Internet TCP/IP** y dé clic en **Propiedades.**

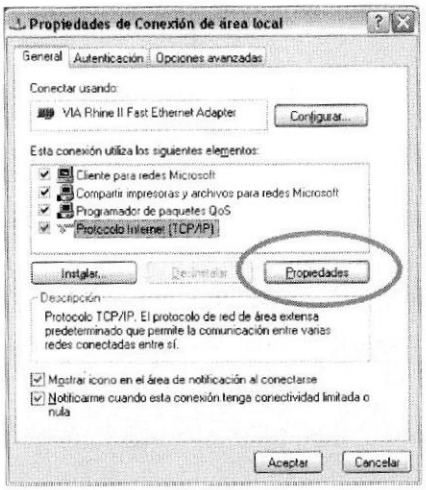


Figura 6.66 Pantalla de Propiedades de Conexión.

- En la pantalla siguiente usted puede observar las **Propiedades del Protocolo Internet (TCP/IP)** y puede asignar las direcciones ip correspondientes a la tarjeta que está configurando. Luego de verificar que las direcciones han sido ingresadas correctamente dé clic en **Aceptar**.

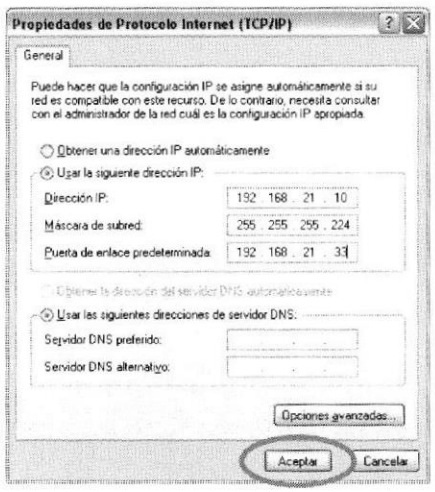


Figura 6.67 Propiedades del protocolo de Internet (TCP/IP)

- Al dar clic en aceptar notará que el icono de la parte inferior derecha de la barra de tareas cambia.

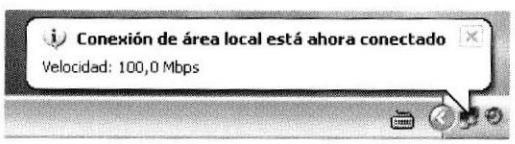


Figura 6.68 Icono en la parte inferior de la barra de tareas.

- Esto indica que el computador desde este momento se encuentra en red.
  Para comprobar que existe comunicación entre el servidor y el cliente haga ping a las respectivas direcciones ip de sus tarjetas de red.

6.7.3 CONFIGURACIONES DEL SERVIDOR SAMBA.

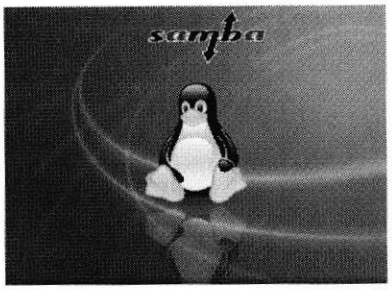


Figura 6.69 Configurando Samba

Samba es una implementación bajo los protocolos SMB y NetBIOS. Con Samba se puede hacer que el sistema Linux actúe como servidor SMB dentro de la red, permitiendo a otros equipos (que por lo general serán otras máquinas Windows) acceder a recursos compartidos como directorios e impresora.

Es necesario anotar que Microsoft Windows utiliza los siguientes protocolos:

- El Protocolo SMB ("Server Message Block") para compartir discos e impresoras. Permite la interconectividad entre un equipo con Linux instalado y el resto de los equipos en la red con alguna versión de Windows. Esta interconectividad se consigue exitosamente a través de SAMBA.

- El Protocolo NetBIOS (Network Basic Input /Output System) para proporcionar a los programas de aplicación un conjunto de comandos que solicitan los servicios de bajo nivel necesarios para establecer sesiones entre nodos de una red, para transmitir información en ambos sentidos y resolver nombres e IPs.

Samba proporciona a Linux soporte para estos protocolos, de forma que puede compartir discos e impresoras con Windows. Para ello se utilizan dos demonios "smbd" y "nmbd", que se ejecutan en un script de inicio o en /etc/xinetd.conf. Estos demonios permiten:

- **Smbd:** Permite la compartición de archivos e impresoras sobre una red SMB y proporciona autentificación y autorización de acceso para clientes SMB.

- **Nmbd:** Permite la búsqueda a través del Windows Internet Name Service (WINS), y ayuda mediante un visualizador.

6.7.3.1 FUNCIONAMIENTO.

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

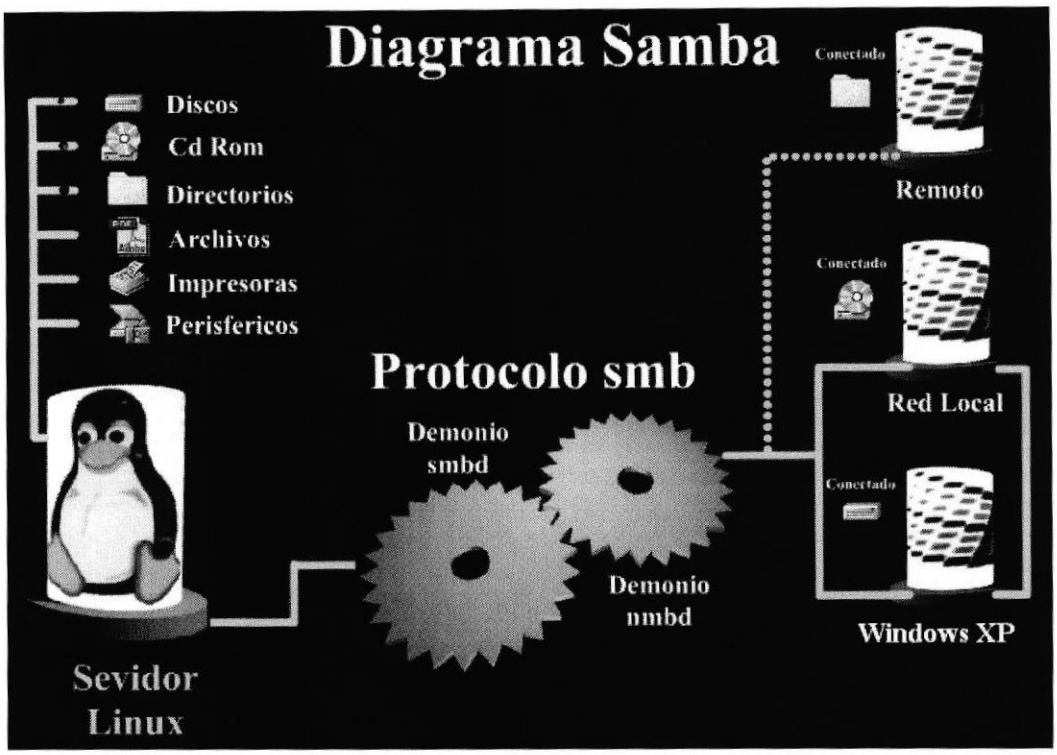


Figura 6.70 Esquema de red, incluyendo un Servidor Samba.

6.7.3.2 VENTAJAS.

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

6.7.3.3 DESVENTAJAS.

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

6.7.3.4 REQUERIMIENTOS.

- Para poder probar el servicio Samba se necesita mínimo dos computadores, uno con el sistema operativo Linux para el Servidor Linux y otro con cualquier sistema operativo Windows para ejercer la función de cliente, ambos computadores deben tener por lo menos una tarjeta de red. (Figura 40)

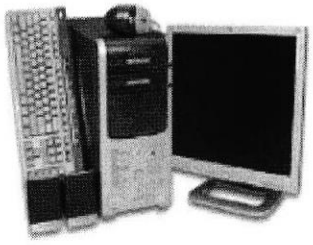


Figura 6.71 Pc de escritorio.

- Los computadores deben estar conectados en red, ya sea por la utilización de un switch o cable cruzado.

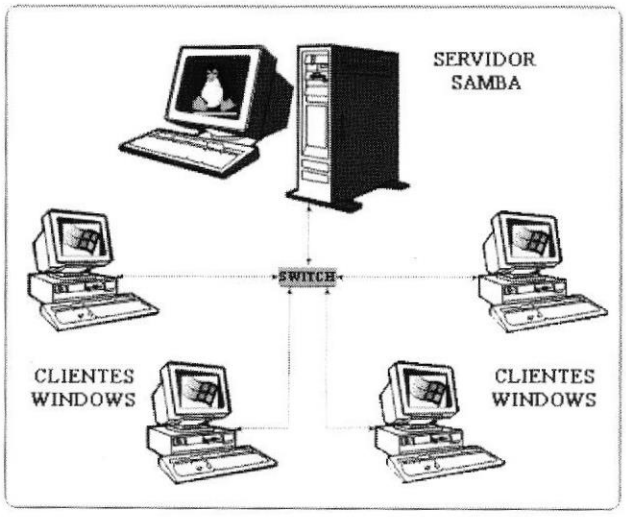


Figura 6.72 Esquema de conexión entre el Servidor y sus Clientes.

- Tener instalados los paquetes correspondientes a Samba.

  - Samba-2.2. 1 a
  - Samba-client -2.2. 1a
  - Samba-commont -2.2. 1a
  - Samba-swat -2.2. 1 a
  - Xinetd – 2.3.3.

6.7.3.5 CONFIGURACIÓN DE SAMBA.

1. Verifique si el paquete de samba esta instalado.

root@localhost /]# rpm –q samba

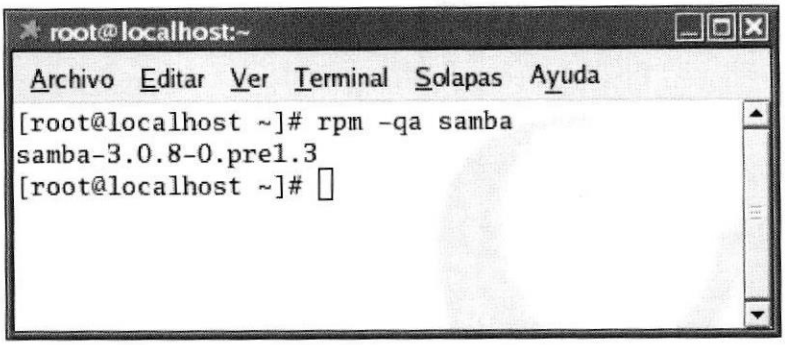


Figura 6.73 Pantalla de verificación del paquete samba.

2. Editar con el comando **vi** y configurar el archivo smb.conf que se encuentra en el directorio de samba, el mismo que esta contenido por etc.

root@localhost /]# vi /etc/samba/smb.conf

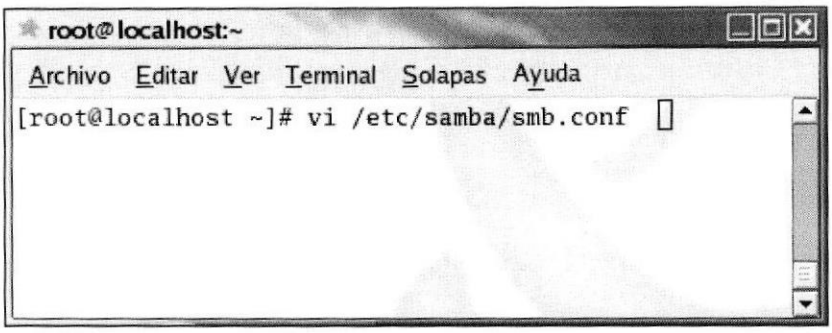


Figura 6.74 Pantalla de ingreso al archivo smb.conf.

En las secciones del smb.conf

Los menús GLOBALS, SHARES, PRINTERS son parecidos a los de las secciones existentes en el fichero /etc/smb.conf, que se presenta como un fichero inhabitual del mundo Windows.

Globals Settings

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

- **Identificar el servidor**

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

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

workgroup = ESPOLGROUP (Grupo de trabajo)

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.

netbios name = LINUX SERVER (Descripción del servidor)

Los menús **hosts allow** y **host deny** permiten controlar el acceso a los recursos de ciertas maquinas.

host allow= registrar las ip de las pc.

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

El campo **interfaces** permite identificar la o las tarjetas de red que enlazan el servidor con el grupo de trabajo.

El control de acceso

El campo **security** permite elegir el método de autentificación, puede elegir uno de los vistos anteriormente.

Las configuraciones hechas en esta sección se aplican a la totalidad de los recursos compartidos, independientemente de la configuración especifica.

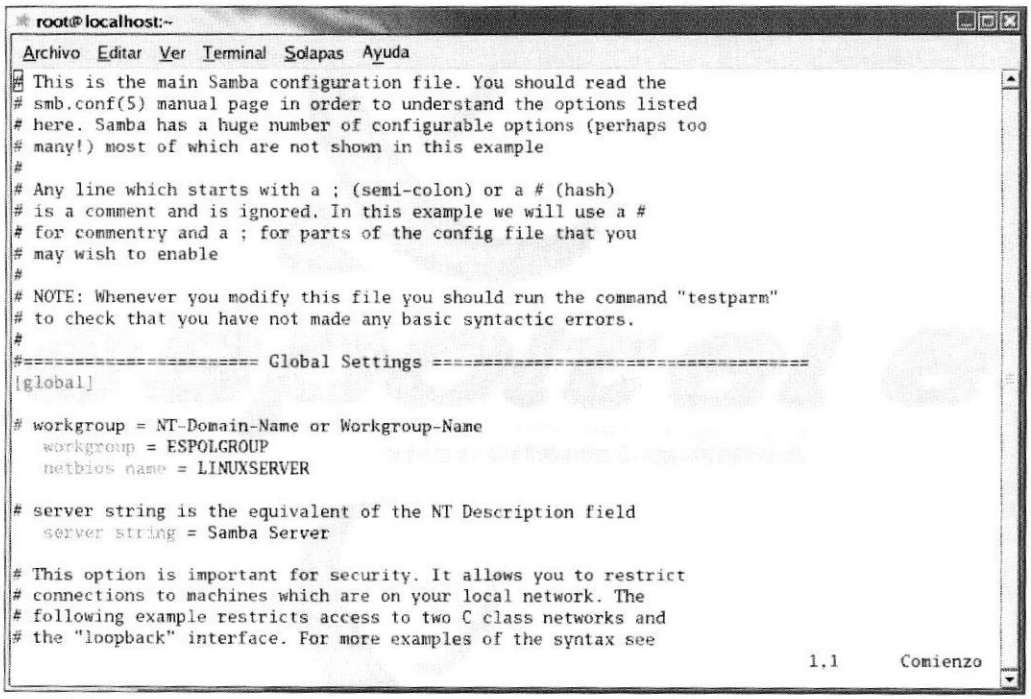


Figura 6.75 Pantalla de la sección Global Settings.

Shares Definitions

El menú SHARES contiene la lista de comparticiones de disco efectuadas por la máquina. Se aconseja primero crear la partición compartida y después precisar para cada partición sus propiedades particulares.

[home]
coment = Home Directories
browseable = no
writable = yes
path = /nombre_carpeta (adicionar)

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

El campo **browseable** indica que este recurso debe ser anunciado por nmbd, y por tanto ser visible para todos los usuarios.

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

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

valid users = usuario1, usuario2

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.

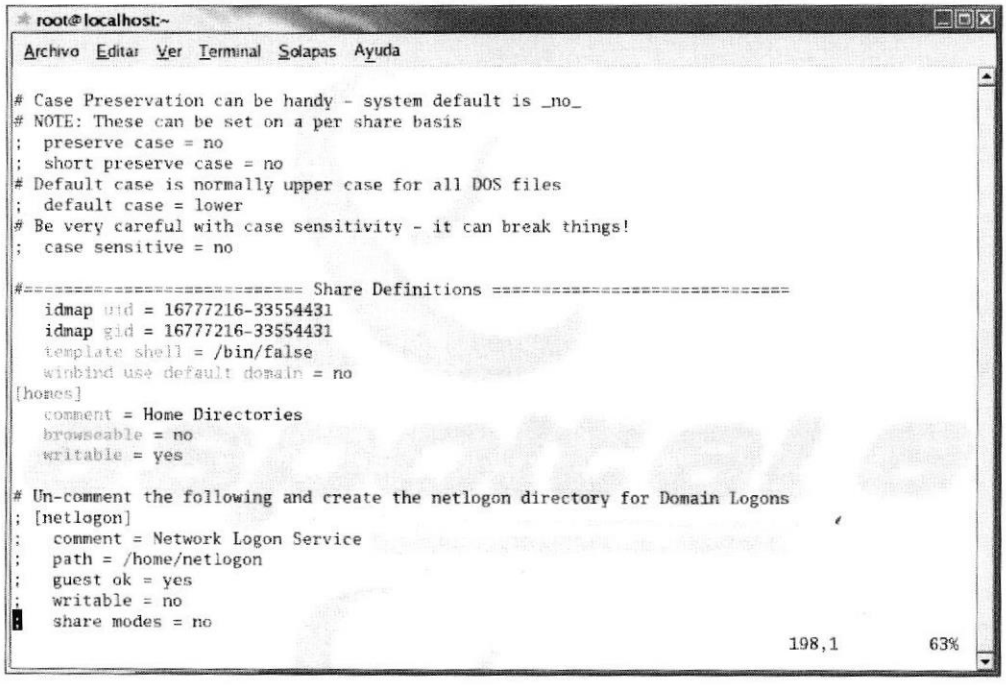


Figura 6.76 Pantalla de la sección Shares Definitions.

Otros Menús

El menú **PRINTERS** es casi idéntico al anterior, pero permite compartir impresoras en lugar de particiones de disco.

El menú **HOME** permite acceder a la versión HTML de la documentación de Samba. Faltan talvez algunas opciones, en particular la ayuda sobre el propio SWAT deja algo que desear. Se trata a menudo de una ayuda relativa a las opciones de los ficheros en modo texto.

A menudo más configurables que la herramienta gráfica. De un modo u otro toda esta documentación es en el fondo muy usable.

Es decir, en este caso, la configuración del menú Home de esta sección quedaría tal como se muestra a continuación.

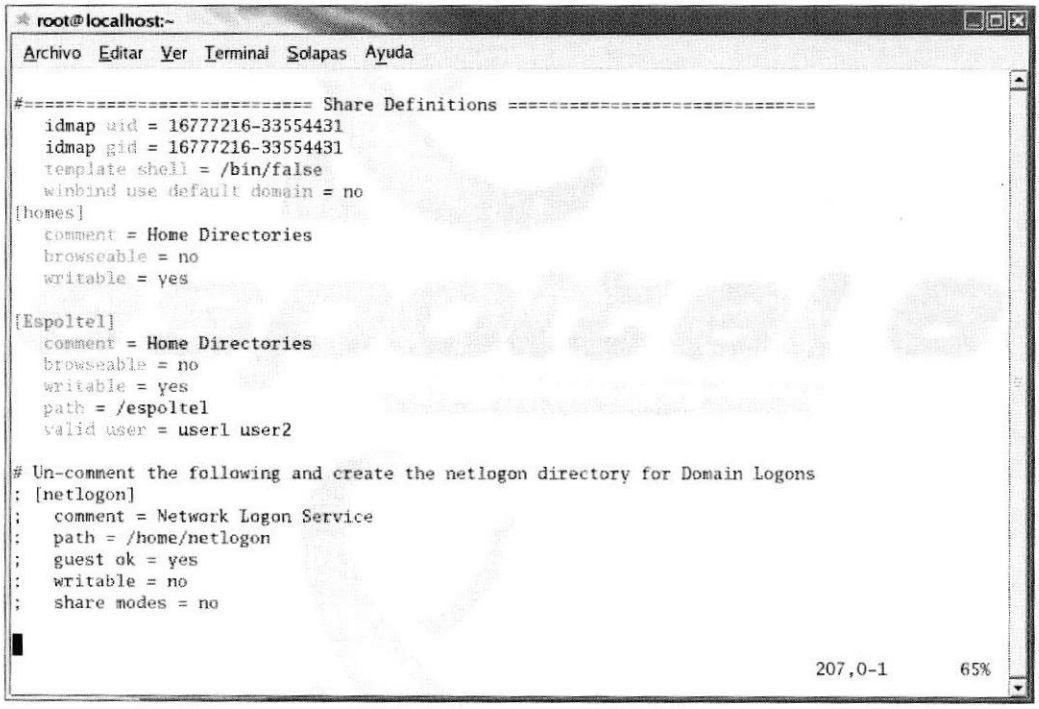


Figura 6.77 Pantalla de configuración Home.

El menú **VIEW** permite ver el fichero **smb.conf** tal cual ha sido redactado por SWAT. Es posible ver también la totalidad de las opciones posibles, incluso las que SWAT no ha cambiado, pero que tienen un valor por defecto.

El menú **PASSWORD** permite al usuario cambiar su contraseña. Se trata de un interfaz gráfico para el programa smbpasswd. Sirve también al administrador para añadir nuevos usuarios.

- Salir con :wq para guardar los cambios.

3. Cree el directorio que contendrá los archivos a compartir.

root@localhost /]# mkdir <nombre_directorio>

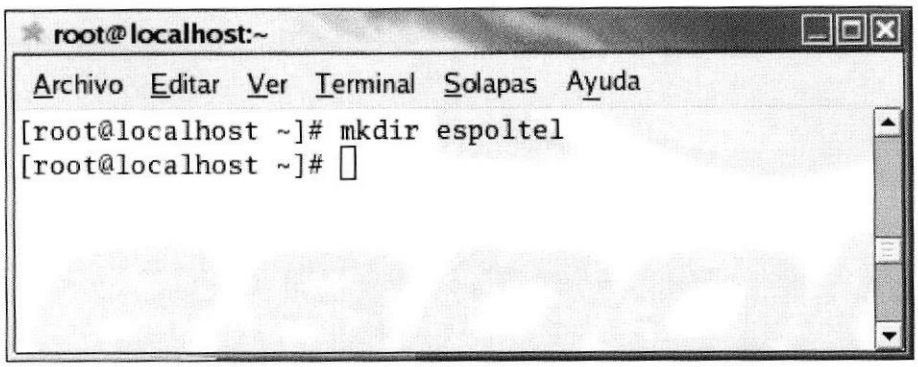


Figura 6.78 Pantalla de creación de directorio.

4. Ingresar al directorio que se creo y para proceder a crear un archivo de texto para la verificación de su funcionamiento.

root@localhost /]# cd <nombre _directorio>
root@localhost /]# touch prueba.txt

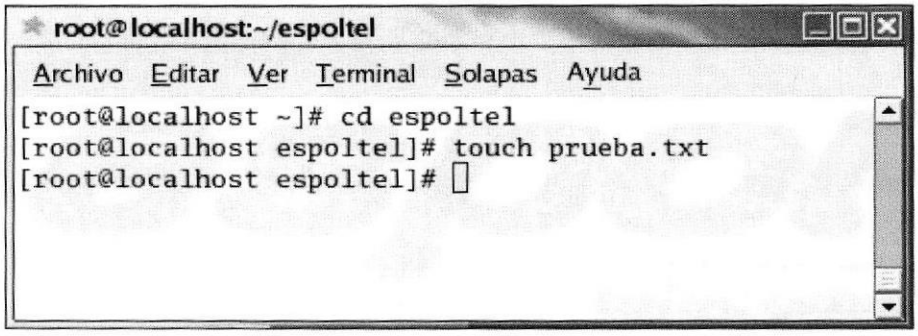


Figura 6.79 Pantalla de cambio de directorio y creación de archivo.

5. Dar todos los permisos de escritura, lectura y ejecución (+777) para el archivo a compartir.

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

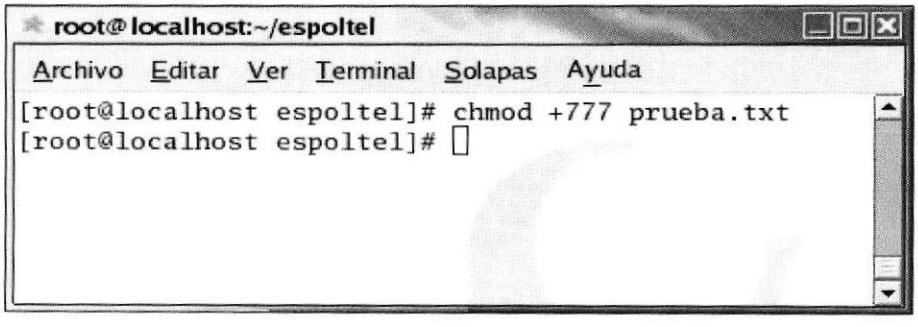


Figura 6.80 Pantalla para otorgar permisos al archivo.

6. Salir del directorio a compartir, en este caso espoltel y asignar todos los permisos de escritura, lectura y ejecución.

root@localhost /]# chmod +777 nombre_carpeta

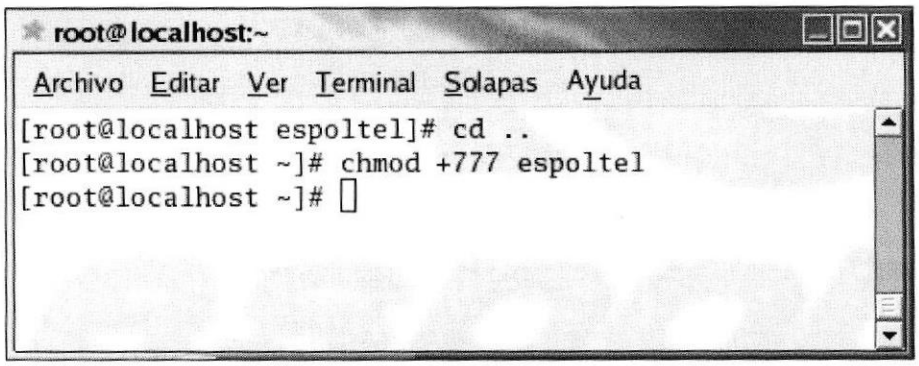


Figura 6.81 Pantalla para otorgar permisos al directorio.

7. Debe crear los usuarios que anteriormente registró en valid user.

root@localhost /]# adduser user1

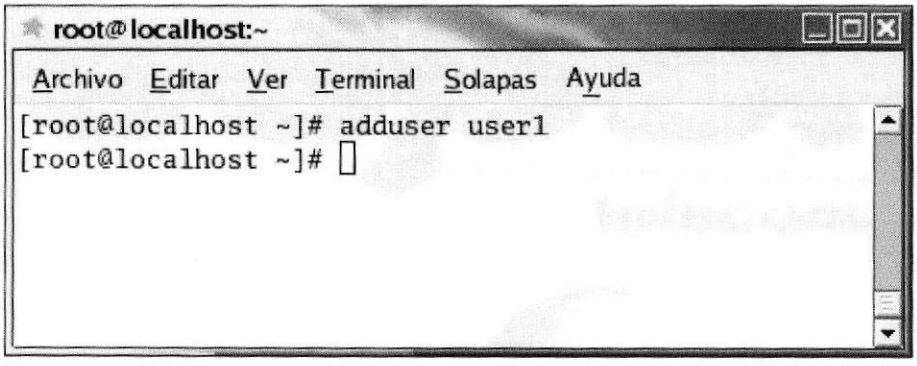


Figura 6.82 Pantalla donde se crea un usuario.

8. Proceda a crear las contraseñas para el usuario.

root@localhost /]# passwd user1

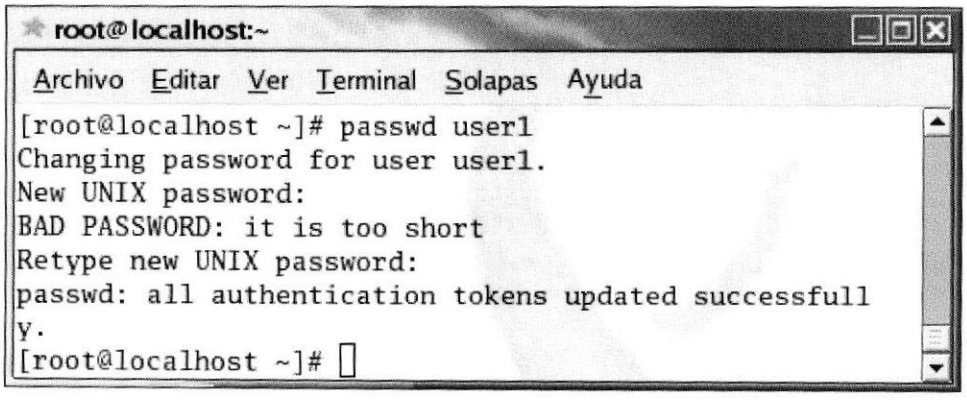


Figura 6.83 Pantalla para crear contraseña.

9. Asignar una contraseña para los usuarios para hacer uso del servicio de samba.

root@localhost /]# smbpasswd –a nombre_usuario

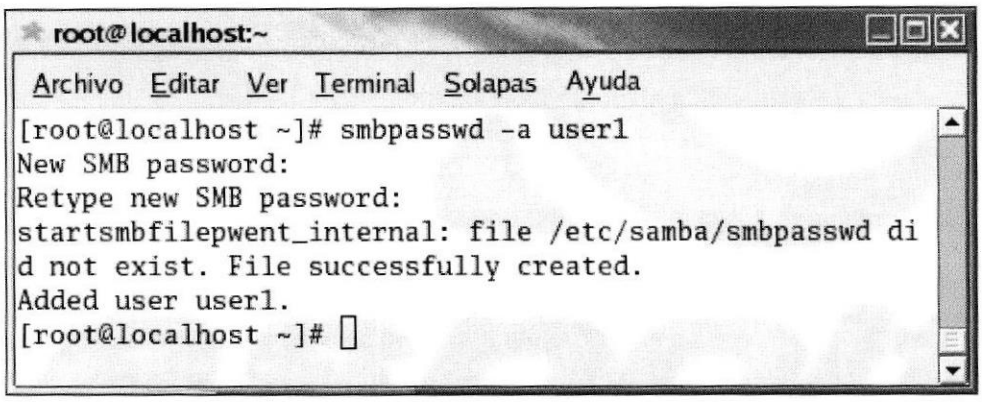


Figura 6.84 Pantalla para crear usuarios y contraseñas en samba.

10. Inicialice los servicios de samba.

root@localhost /]# service smb start

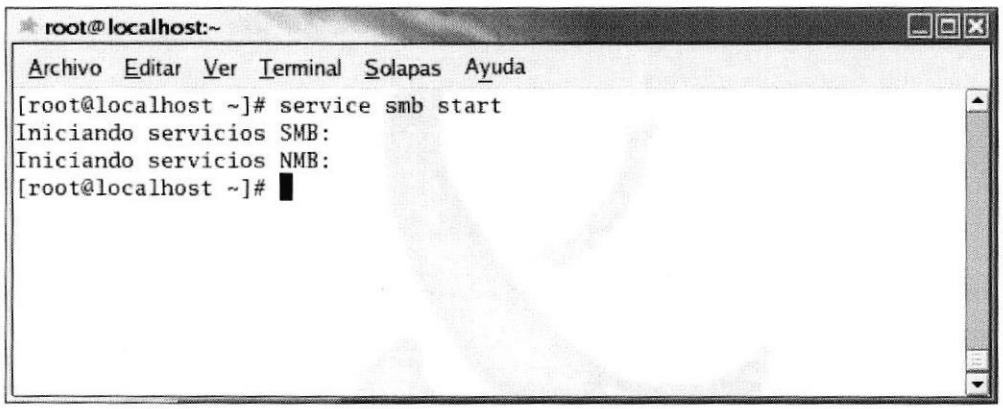


Figura 6.85 Pantalla para inicializar los servicios de samba.

En caso de reiniciar el servidor, los servicios no se inician, por lo tanto deberá activarlos con el comando Setup.

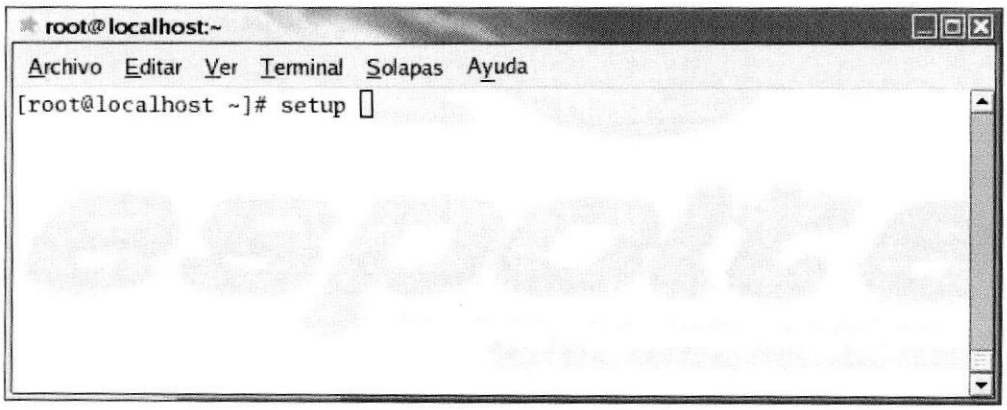


Figura 6.86 Pantalla para ingresar al setup.

A continuación aparecerá una pantalla, la misma que contiene el menú "Elija una Herramienta", donde deberá escoger la opción Servicios del Sistema y luego Ejecutar una Herramienta.

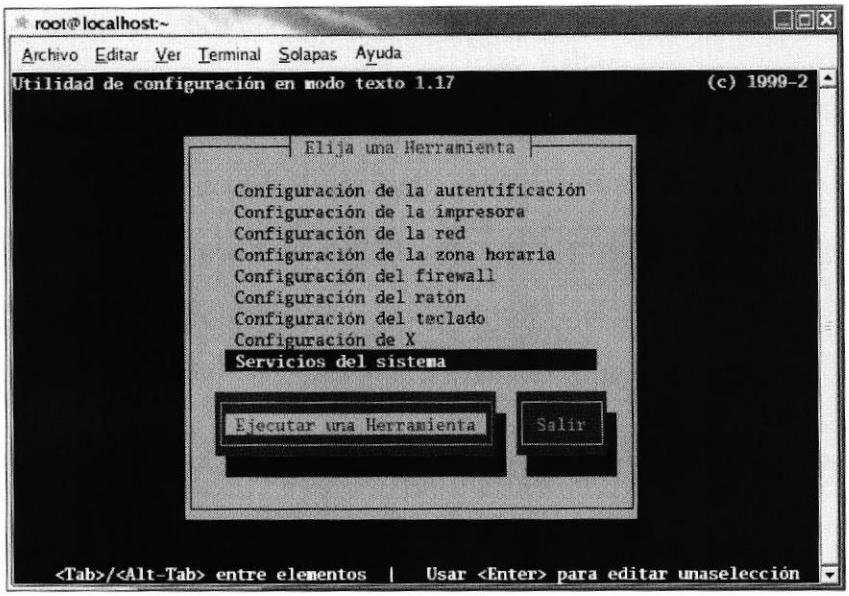


Figura 6.87 Pantalla para escoger Servicios del Sistema.

Aparece la ventana de Servicios donde se debe habilitar smb, posteriormente elegir Ok.

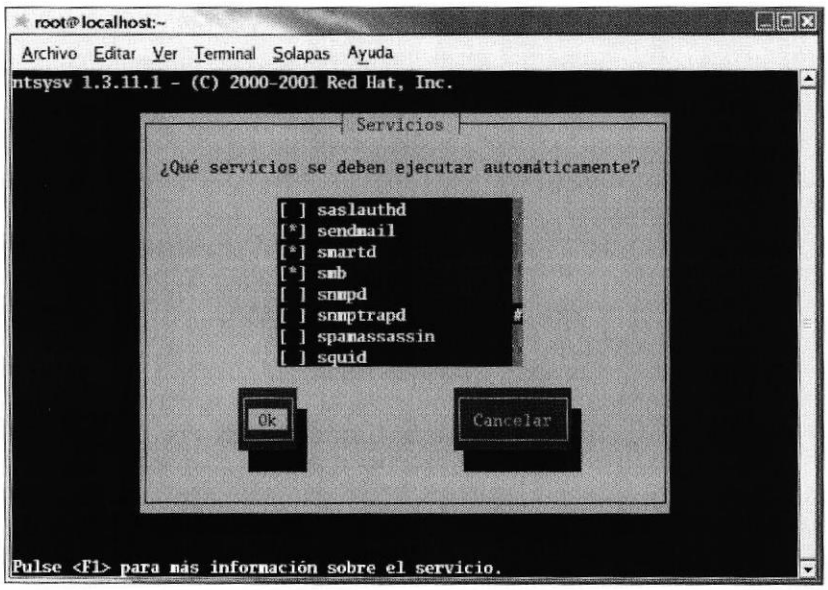


Figura 6.88 Pantalla para escoger la opción del servicio de SMB

6.7.3.6 CONFIGURACIÓN EN EL CLIENTE WINDOWS EN SAMBA.

Pasos a seguir en la estación de trabajo con sistema operativo Windows:

1. Acceder al servidor Linux por dirección ip, Dé clic en el botón Inicio, opción Ejecutar, en el recuadro que aparece colocar la dirección del servidor en este caso 192.168.20.5.

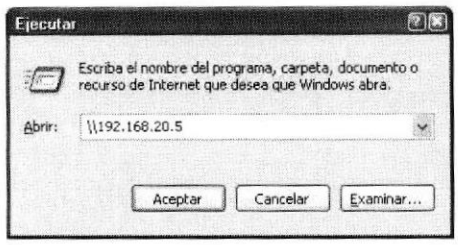


Figura 6.89 Pantalla para acceder al servidor Linux.

2. Aparecerá la siguiente pantalla solicitando clave y usuario.

Figura 6.90 Pantalla de petición de usuario y contraseña.

3. Ingrese su usuario samba con su clave respectiva, recuerde que deberá ser el utilizado en la configuración de samba.

Figura 6.91 Pantalla para conectarse al servidor Linux.

4. Ingrese y verifique recursos compartidos en el servidor Samba Linux.

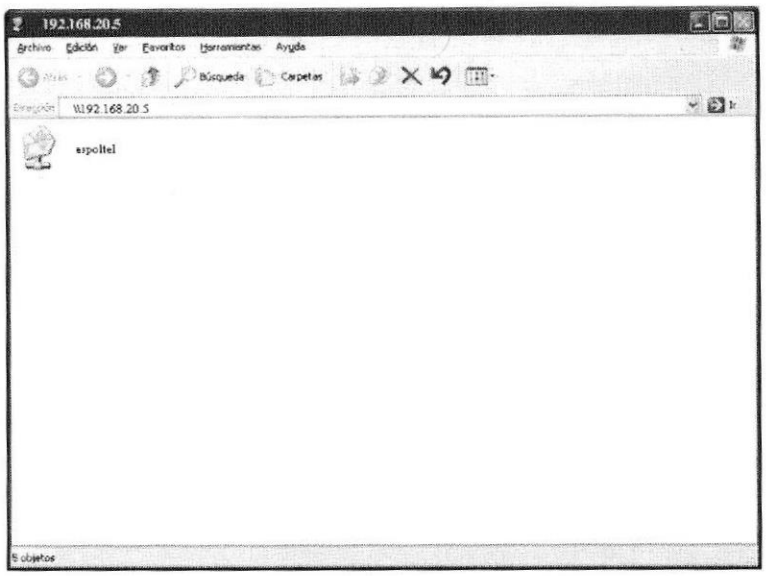


Figura 6.92 Pantalla para verificar el servidor Samba este en funcionamiento.

6.7.4 CONFIGURACIONES DEL SERVIDOR DNS.

Un **DNS** (Domain Name System) es un conjunto de protocolos y servicios (base de datos distribuida) que permiten a los usuarios utilizar nombres en lugar de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP. Por ejemplo, si la dirección IP del sitio FTP de prox.ve es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.ve y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente los DNS nacieron de la necesidad de recordar fácilmente los sitios visitados o a visitar y sustituir el antiguo sistema de identificación de "host" en internet que consistía en un gran archivo donde estaban almacenados los nombres y las direcciones ips de cada nodo de la red con el cual se podía establecer comunicación.

Desde un punto de vista técnico, un nombre de dominio es más fácil de recordar, además cuando una empresa tiene un servidor DNS (y su propio nombre de dominio) se le puede localizar más fácilmente por Internet.

6.7.4.1 ESTRUCTURA.

- El sistema de nombres de dominio se implementa como una base de datos distribuida jerárquicamente que contiene diferentes tipos de datos, incluidos los nombres de host y de dominio.

- Los nombres de una base de datos DNS forman una estructura de árbol jerárquico denominada espacio de nombres de dominio.

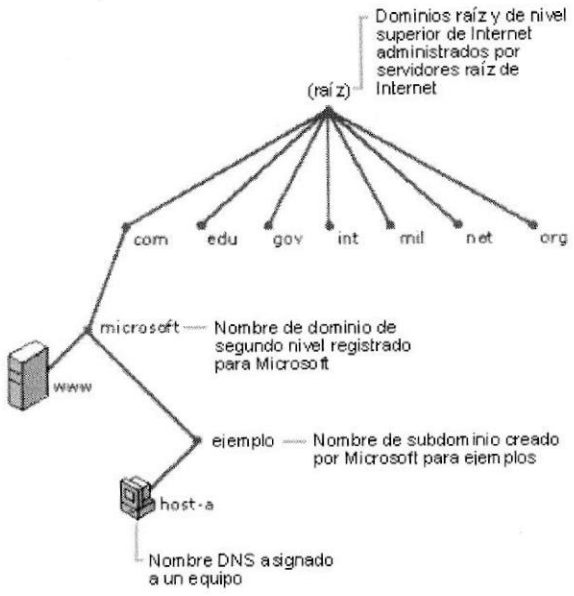


Figura 6.93 Estructura DNS.

6.7.4.2 CARACTERÍSTICAS.

- Establece una correspondencia entre nombres direcciones IP.
- Consiste en una base de datos distribuida por todo el internet.
  - Se gestiona de forma descentralizada.
  - El esquema de distribución es jerárquico.
  - Fácil de usar en las aplicaciones.
  - Espacio de nombres es global.
- Almacena información adicional.
  - Se puede utilizar para otros fines.
  - Almacenamiento de características de máquinas.
  - Configuración de servicios.

6.7.4.3 FUNCIONAMIENTO.

El sistema DNS es una base de datos distribuida mantenida por miles de servidores DNS, cada uno de los cuales es responsable de una "zona" de internet.

Cuando un programa cliente (por ejemplo, el navegador) hace una petición de una dirección internet, el servidor DNS del proveedor de acceso procesa la consulta, intentando buscar el dominio en su tabla de registros. Si no lo encuentra envía la petición a otro servidor DNS situado en un nivel superior de la jerarquía de nombres de dominios. Esta secuencia de peticiones se repite hasta que se obtiene la dirección IP del ordenador que corresponde al dominio consultado.

El servicio que registra tu dominio es el responsable de asociar tu nombre de dominio con el servidor DNS correspondiente, de manera que siempre queda asegurada su "visibilidad".

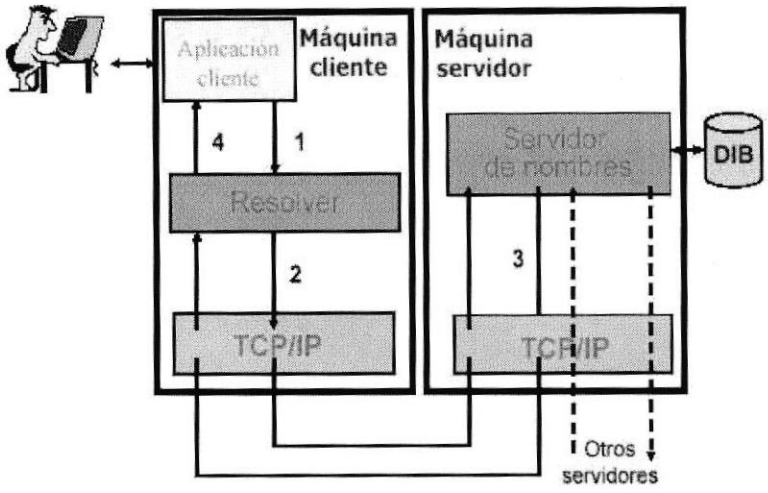


Figura 6.94 Esquema de resolución de nombres.

6.7.4.4 BENEFICIOS.

- **Conveniencia:**
  Nombres conocidos por el usuario son más fácil de recordar que sus respectivas direcciones IP.

- **Consistencia:**
  Las direcciones IP pueden cambiar pero los nombres permanecen constantes.

- **Simplicidad:**
  Usuarios necesitan aprender solo un nombre para encontrar recursos ya sea en internet o en una Intranet.

6.7.4.5 REQUERIMIENTOS.

- Para poder probar el servicio DNS se necesita mínimo dos computadores, uno con el sistema operativo Linux para el Servidor Linux y otro con cualquier sistema operativo Windows para ejercer la función de cliente, ambos computadores deben tener por lo menos una tarjeta de red.

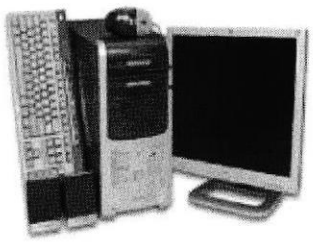


Figura 6.95 Pc de escritorio.

- Los computadores deben estar conectados en red, ya sea por la utilización de un switch o cable cruzado.

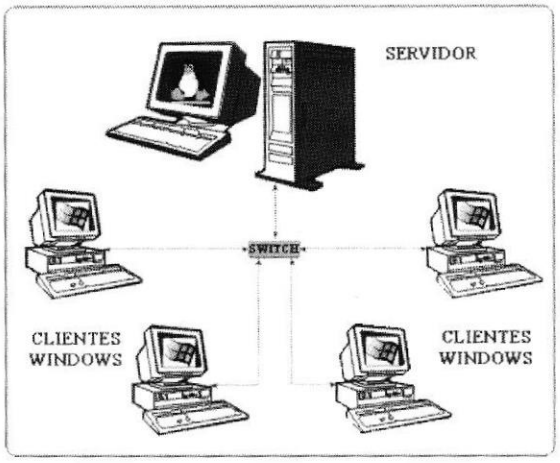


Figura 6.96 Esquema de conexión entre el servidor y sus clientes.

- Tener instalados los paquetes correspondientes a DNS.
  - Bind
  - Bind-chroot
  - Bind-utils
  - Caching-nameserver

6.7.4.6 CONFIGURACIÓN DE DNS.

1. Verifique la instalación del paquete del DNS.

[root@localhost /]# rpm –qa bind

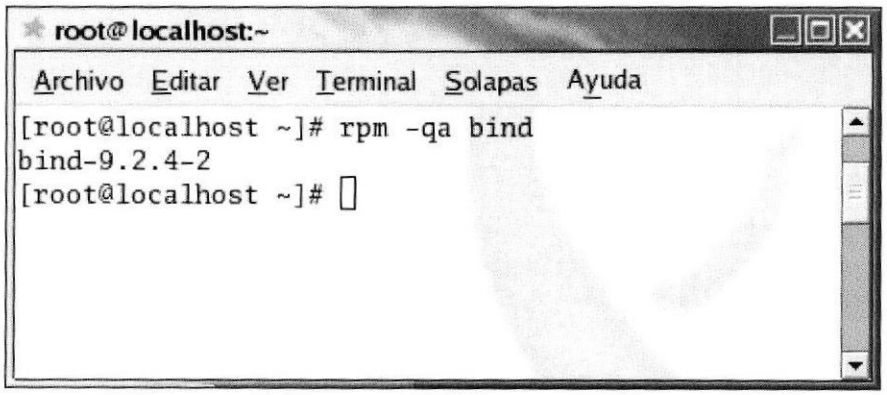


Figura 6.97 Pantalla de verificación del paquete bind.

2. Configurar el archivo named.conf que se encuentra en el directorio etc.

[root@localhost /etc]# vi /etc/ named.conf

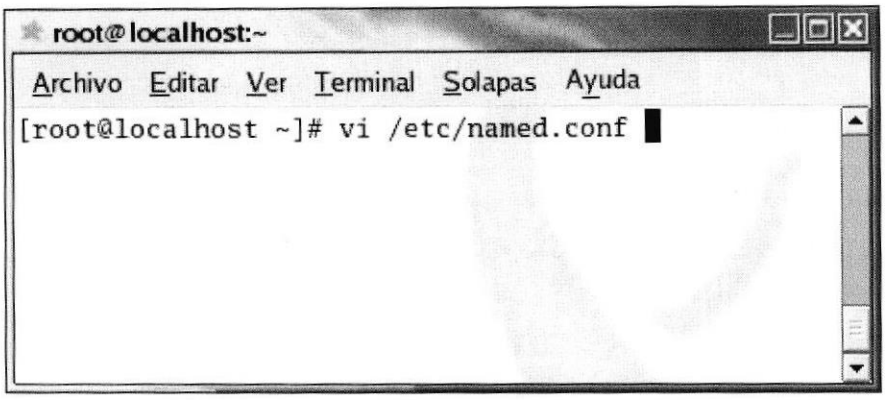


Figura 6.98 Pantalla de ingreso al archivo named.conf.

Zona de Búsqueda Directa

Las zonas de búsqueda directa contienen la información necesaria para resolver nombres en el dominio DNS. Deben incluir registros SOA y NS, y pueden incluir cualquier tipo de registros de recurso, excepto el registro de recursos PTR.

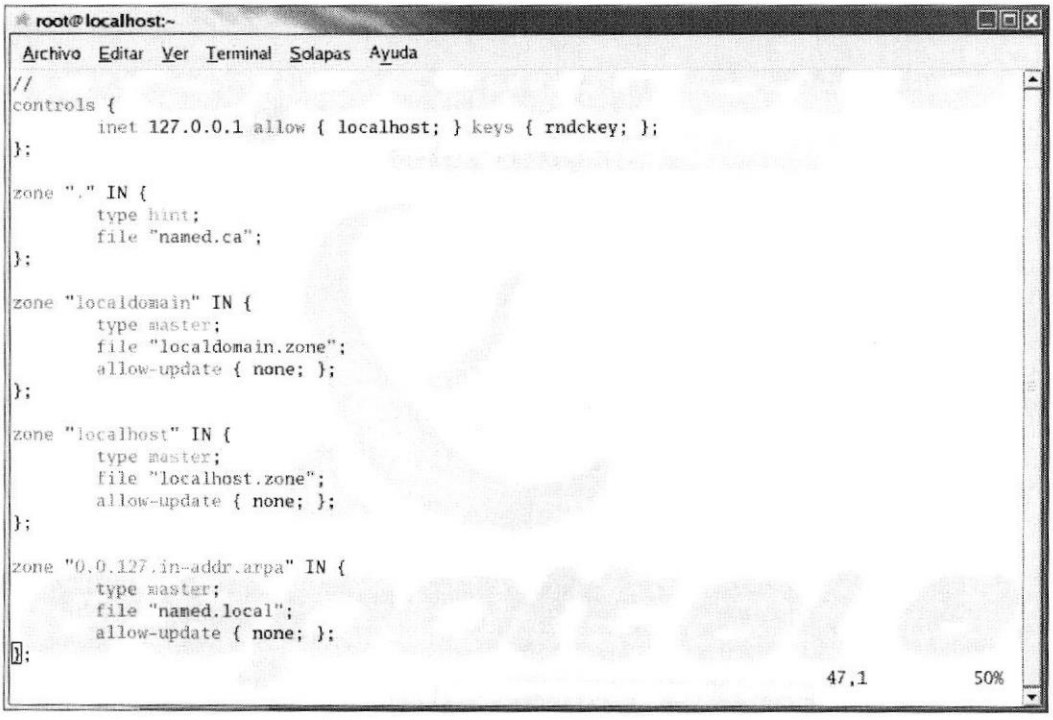


Figura 6.99 Pantalla de edición del archivo named.conf.

Realizar los siguientes pasos:

1. Copiar estas líneas

```
zone "localhost" IN {
type master;
file "localhost.zone";
allow-update {nome};
};
```

2. Realizar los siguientes cambios

```
zone "espoltel.net"{
type master;
notify no;
file "espoltel.net";
allow-update{nome};
};
```

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.

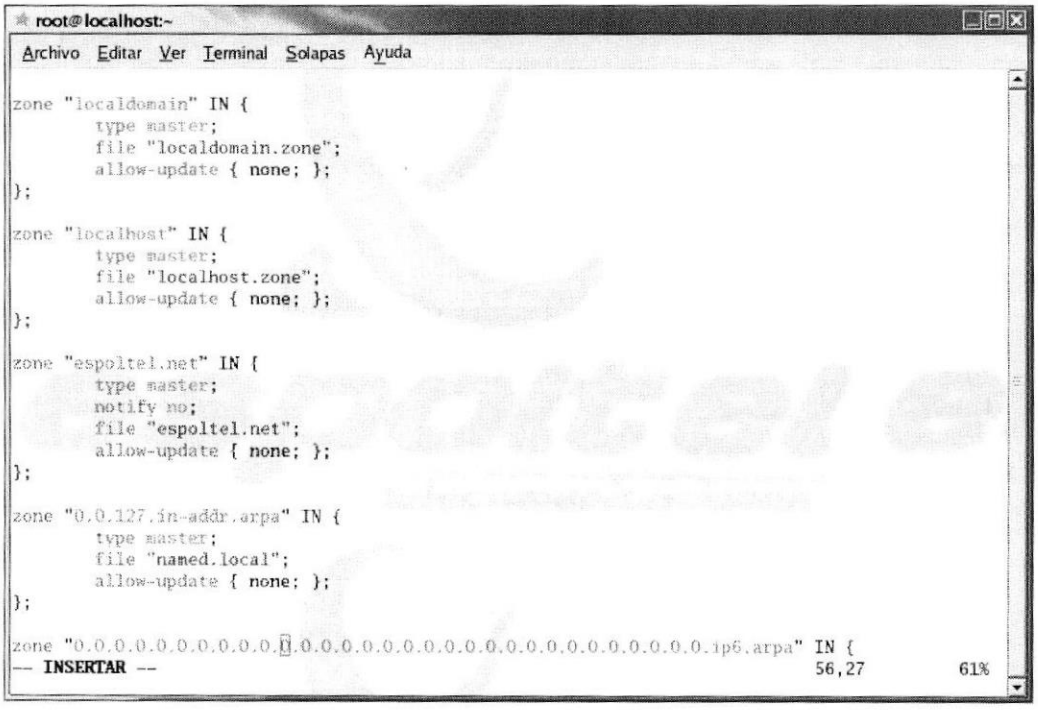


Figura 6.100 Pantalla con los cambios en zone.

- Salir con :wq para guardar los cambios.

3. Ingresar al directorio var/named/chroot/var/named/ y listar el contenido con el comando **ls**, donde deberá aparecer el archivo localhost.zone.

```
[root@localhost /]# cd /var/named/chroot/var/named/
```

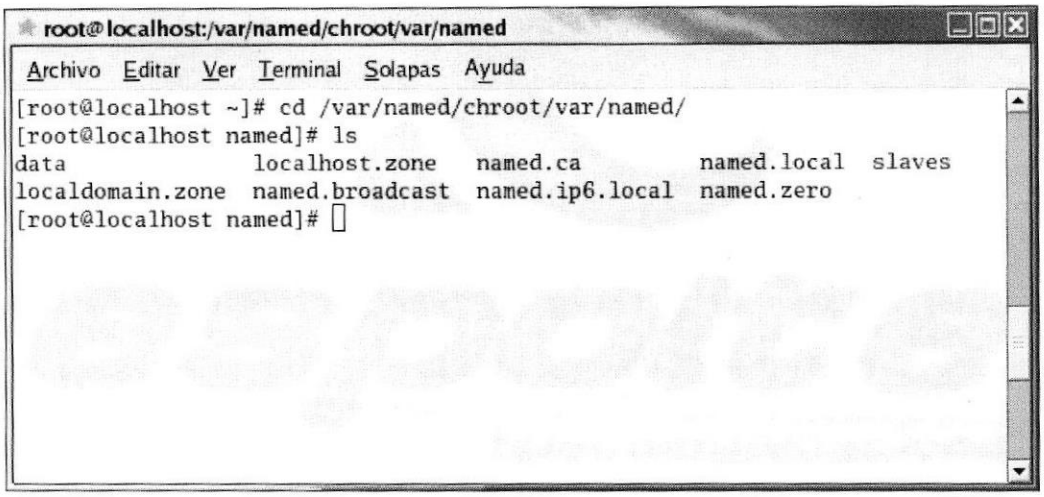


Figura 6.101 Pantalla de ingreso al directorio named.

4. Realizar una copia del contenido del archivo localhost.zone al nombre.com, en este caso topico.com

[root@localhost named]# cp localhost.zone espoltel.net

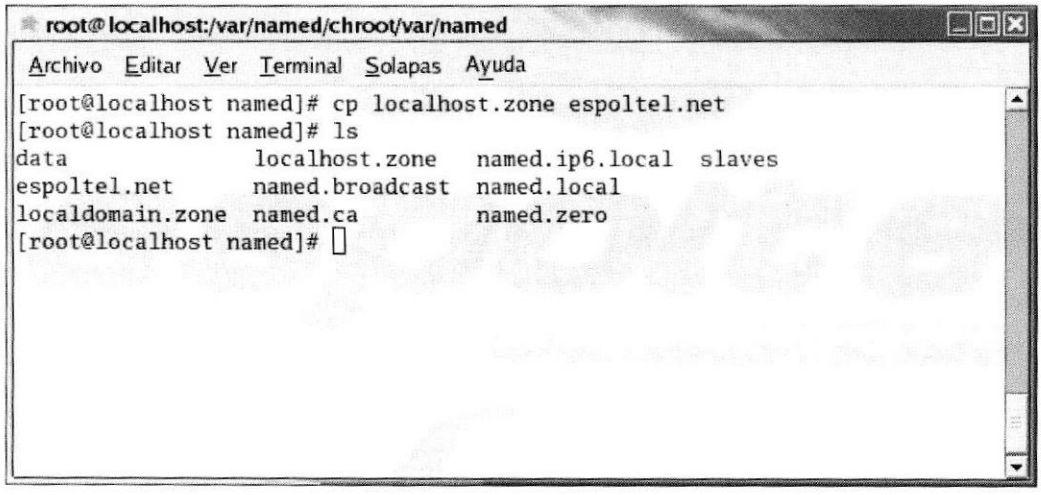


Figura 6.102 Pantalla para copiar el archivo localhost.zone a espoltel.net.

5. Editar el archivo espoltel.net

[root@localhost named /]# vi espoltel.net

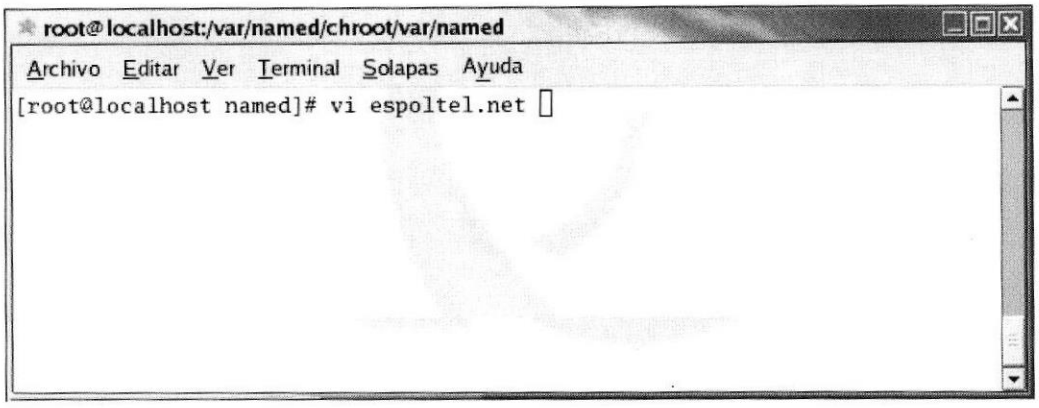


Figura 6.103 Pantalla para ingresar al ar4chivo espoltel.net.

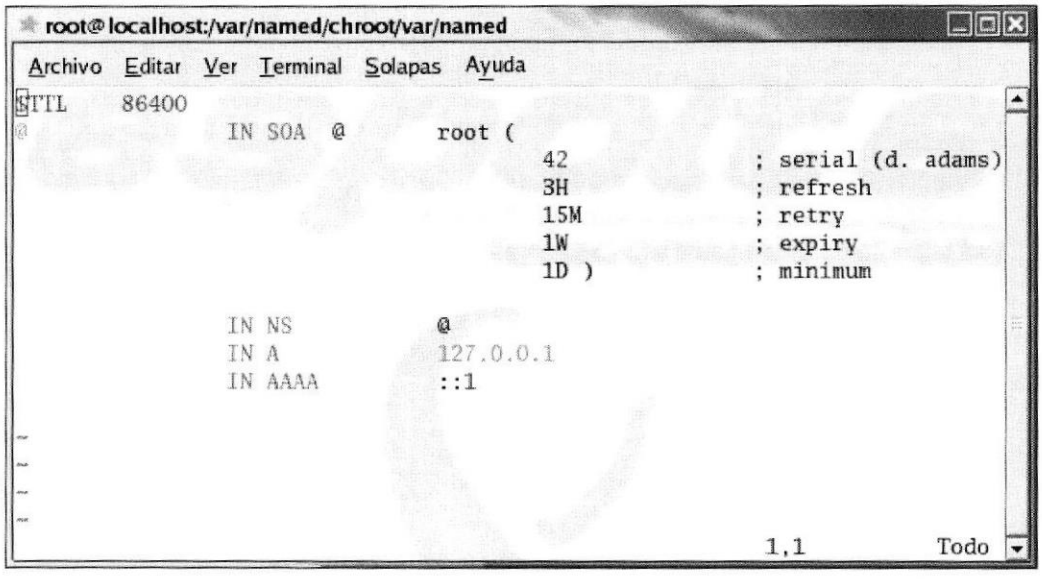


Figura 6.104 Pantalla de edición del archivo espoltel.net.

Registros de recursos

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 .....).

@ al principio de línea de los archivos de zona indica que no se necesita nombre.

Los registros **SOA (Start Of Authority)** incluyen los siguientes campos:

• Propietario: nombre de host o del dominio DNS al que pertenece este RR

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

• Clase: define la familia de protocolos en uso.

• Tipo: identifica el tipo de RR.

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

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

• Actualización: muestra las veces que el servidor secundario de la zona comprueba si hay cambios en la zona.

• Reintentos: define el tiempo que el servidor secundario, después de enviar una solicitud de transferencia de zona, espera para obtener una respuesta del servidor maestro antes de volverlo a intentar.

• Caducidad: define el tiempo que el servidor secundario de la zona, después de la transferencia de zona anterior, responderá a las consultas de la zona antes de descartar la suya propia como no válida.

• TTL mínimo: este campo se aplica a todos los registros siempre que no se especifique un valor de tiempo de vida en un registro de recursos.

Al realizar los cambios el archivo deberá de quedar de la siguiente manera.

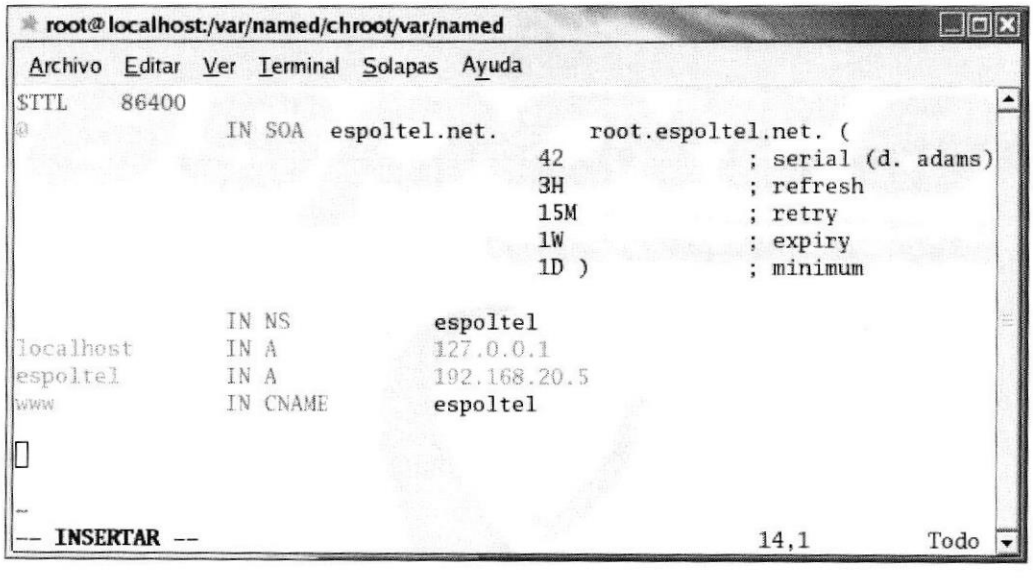


Figura 6.105 Pantalla con los cambios del archivo espoltel.net.

6. Inicialice los servicios del named .

[root@localhost /]# service named start

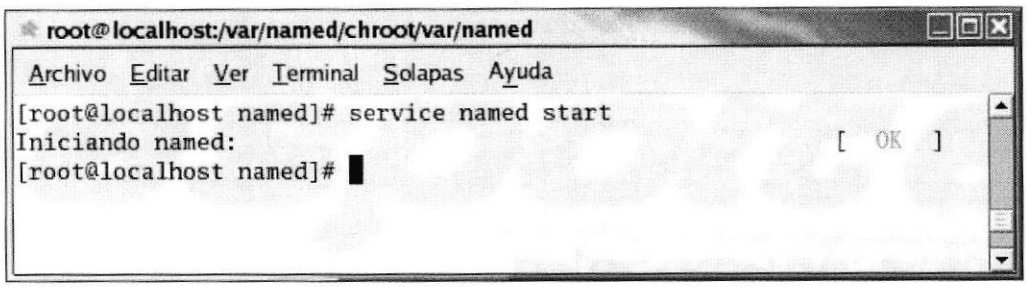


Figura 6.106 Pantalla de inicialización del servicio named.

7. Haga ping a la dirección web del servidor para verificar su funcionamiento.

[root@localhost named /]# ping www.espoltel.net

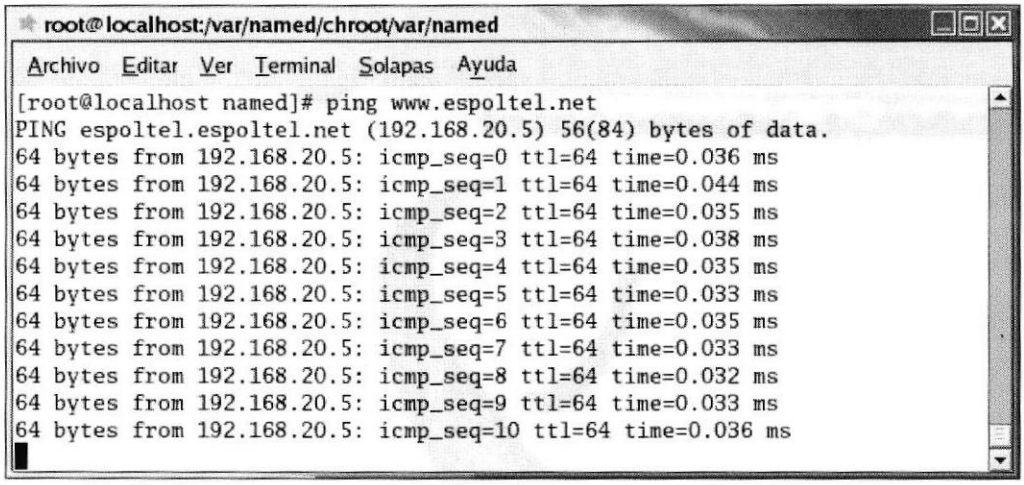


Figura 6.107 Pantalla de verificación del ping a la dirección

Si da respuesta es porque su configuración esta bien realizada, caso contrario uno de los inconvenientes puede ser la ip del servidor por lo que deberá ingresar al directorio etc y editar el archivo resolv.conf para proceder a configurar la dirección ip del servidor DNS.

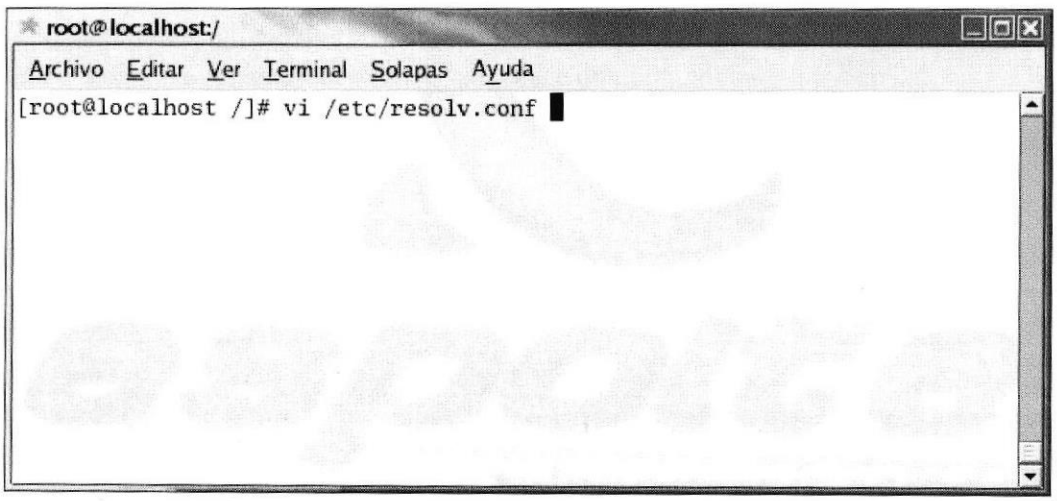


Figura 6.108 Pantalla de edición del archivo resolv.conf.

En este archivo aparecerá NameServer, y deberá confirmar que la ip sea la misma de la tarjeta de red del servidor DNS.

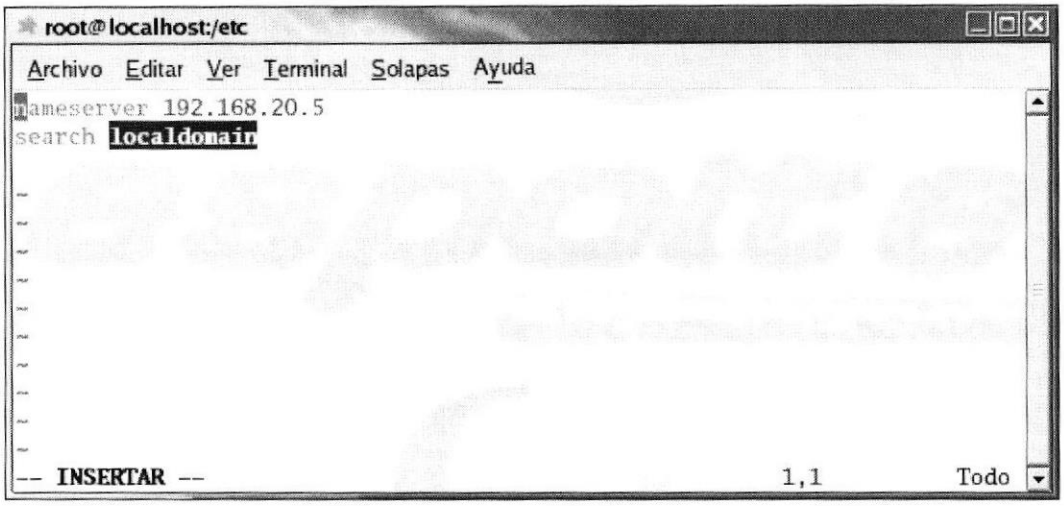


Figura 6.109 Pantalla de configuración de la ip del servidor DNS:

En caso de reiniciar el servidor, los servicios no se inician, por lo tanto deberá activarlos con el comando Setup.

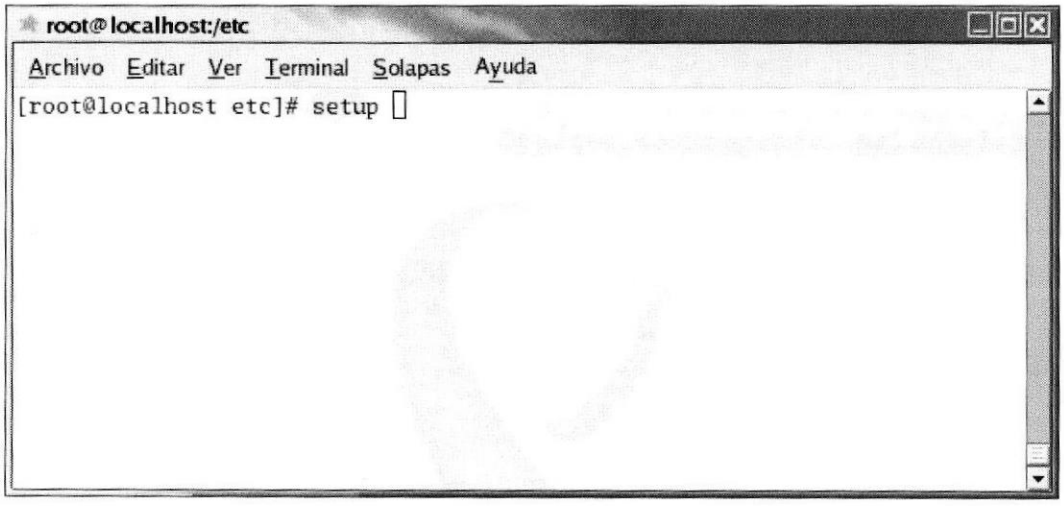


Figura 6.110 Pantalla de ingreso al setup.

A continuación aparecerá una pantalla, la misma que contiene el menú "Elija una Herramienta", donde debe escoger la opción Servicios del Sistema y luego Ejecutar una Herramienta.

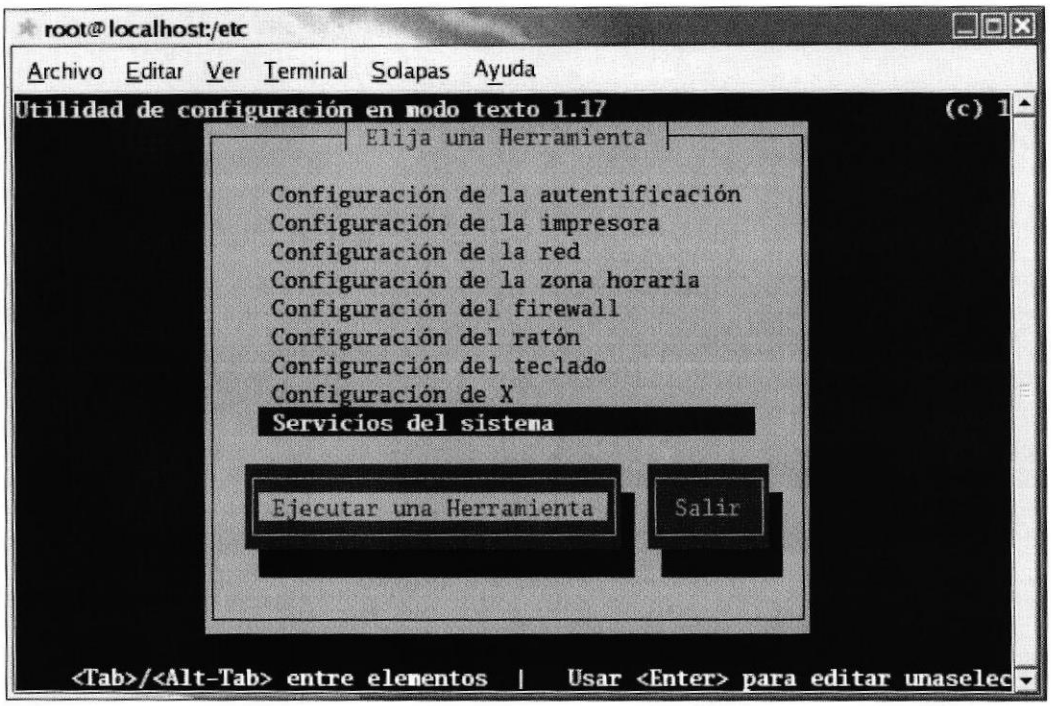


Figura 6.111 Pantalla de ingreso a Servicios del Sistema.

Aparece la ventana de Servicios donde se debe habilitar named y elija Ok.

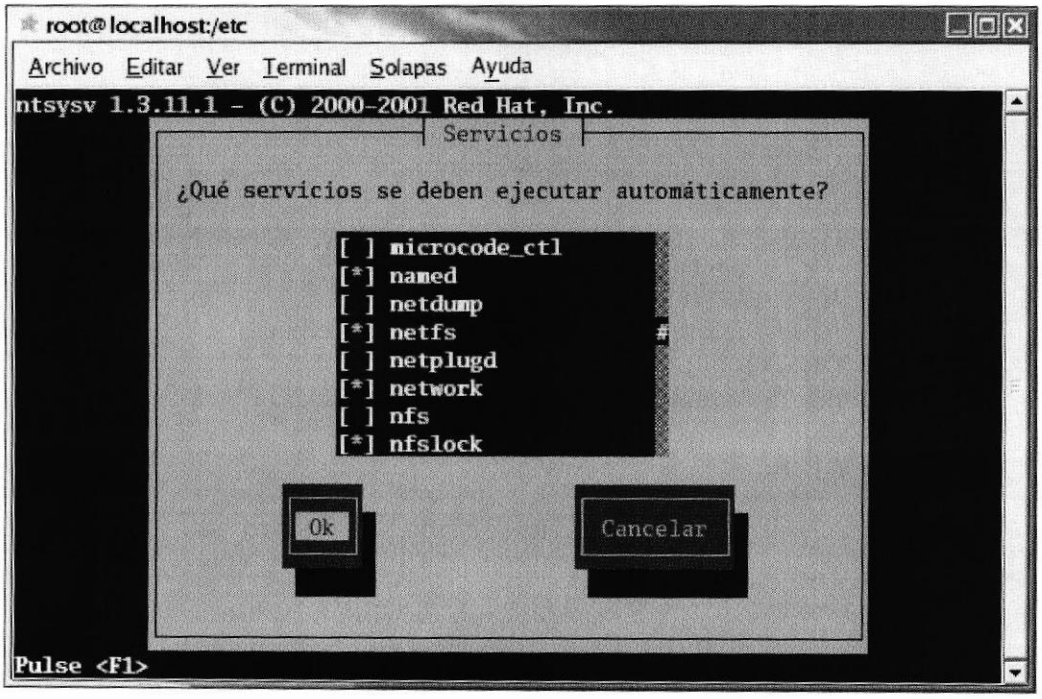


Figura 6.112 Pantalla para habilitar el servicio de named.

6.7.4.7 CONFIGURACIÓN EN EL CLIENTE WINDOWS EN DNS.

Se debe ingresar a mis sitios de red, este icono se encuentra en el escritorio de Windows.

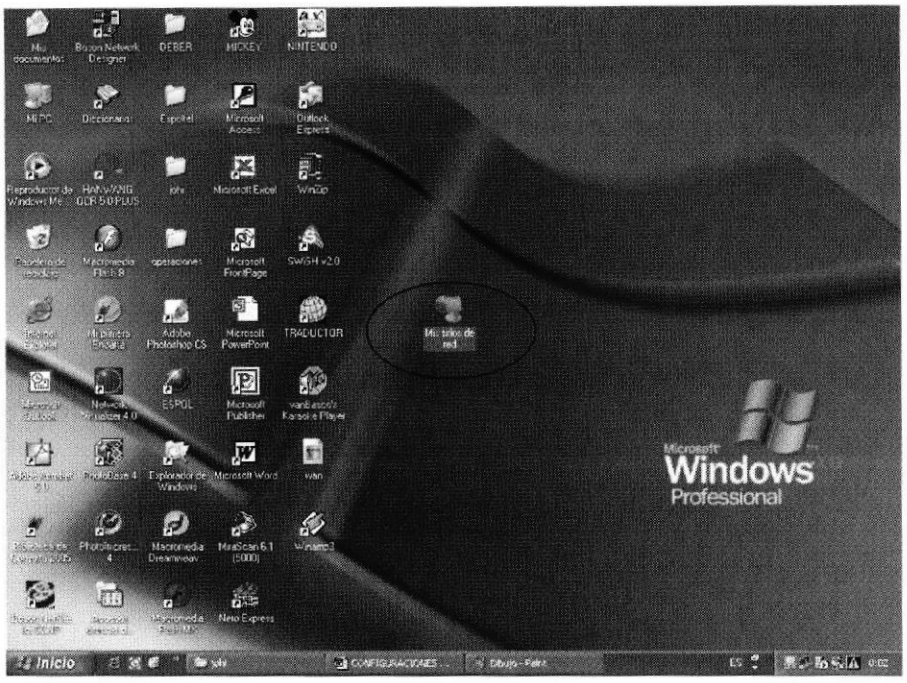


Figura 6.113 Pantalla del entorno Windows.

Si el icono, no apareciera, debe ir al explorador de Windows; donde deberá escoger mis sitios de red y proceder a dar clic derecho opción propiedades.

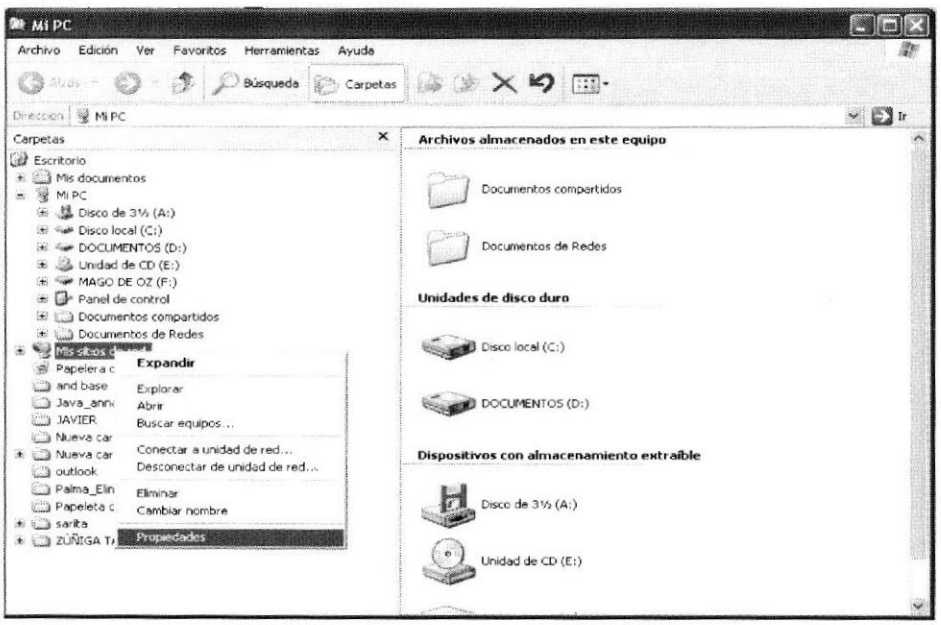


Figura 6.114 Pantalla del explorador de Windows.

Tanto en la primera opción, como en la segunda se mostrará la ventana de conexiones de red, dé clic derecho al icono de conexiones de área local y elija propiedades.

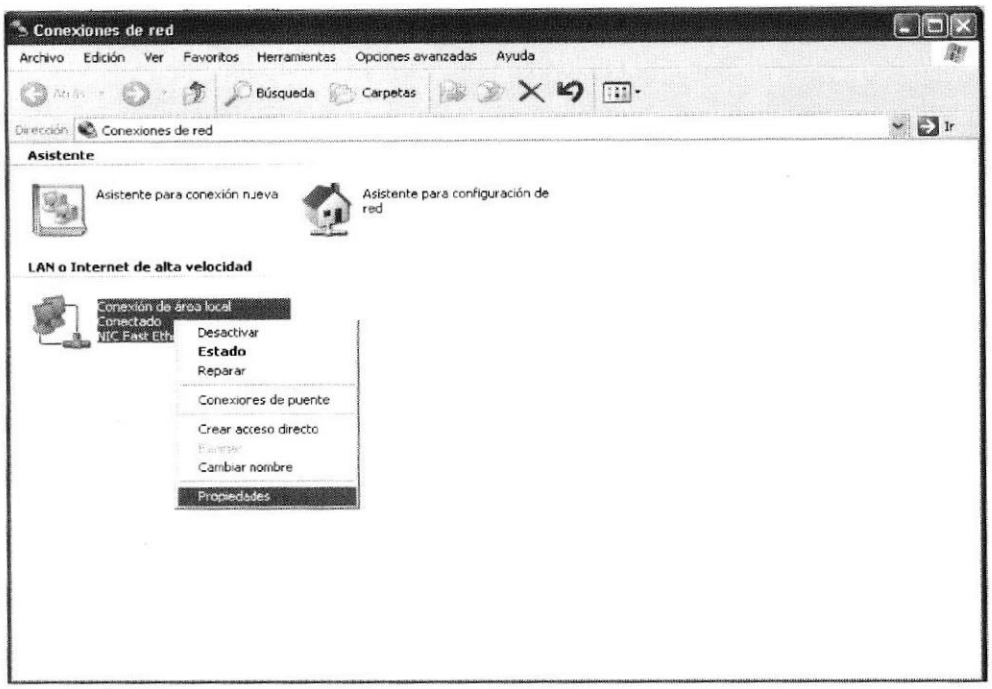


Figura 6.115 Pantalla de conexión de red.

De la ventana que se muestra en propiedades de conexiones de área local, proceda a dar doble clic sobre Protocolo Internet (TCP/IP).

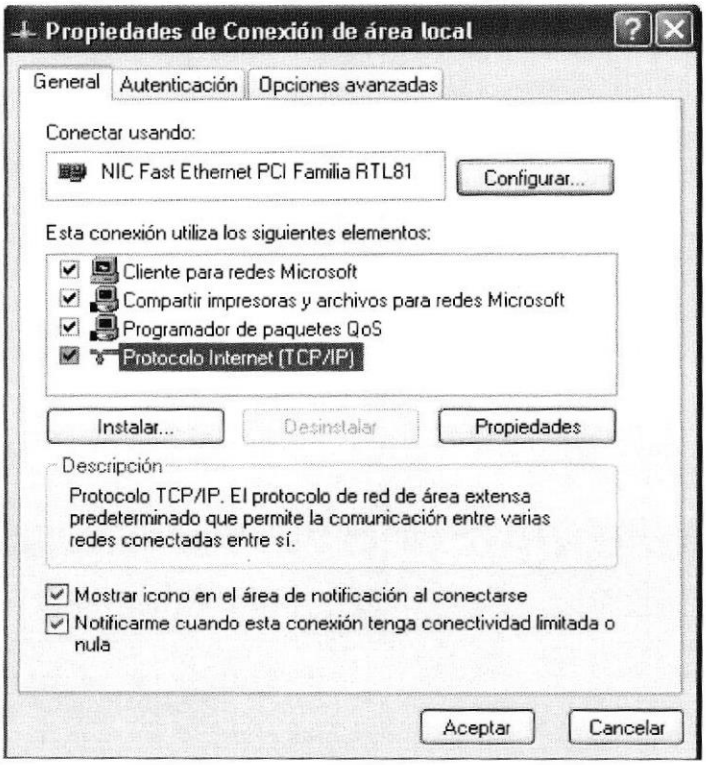


Figura 6.116 Pantalla de propiedades de conexión de área local.

Una vez realizado el proceso, configure la tarjeta de red, asignándole su respectiva dirección ip, máscara de subred, puerta de enlace y dirección del servidor DNS, y presione Ok..

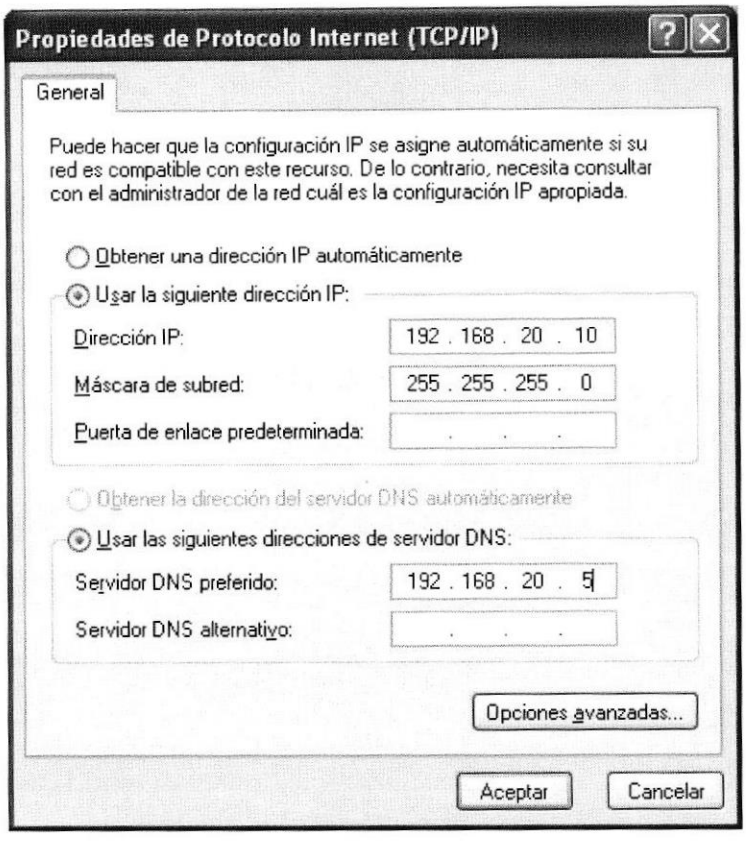


Figura 6.117 Pantalla de propiedades (TCP/IP)

6.7.5 CONFIGURACIONES DEL SERVIDOR WEB.

Un servidor Web es una computadora conectada permanentemente al internet (ha de tener asignada una dirección IP) que espera conexiones de clientes Web (por ejemplo, Netscape Navigator o MS Internet Explorer) para que éstos le soliciten datos, que normalmente son archivos como páginas de su sitio, además administra las cuentas de correo, bases de datos, etc. Es una computadora de alto rendimiento que lleva a cabo todo el procesamiento de datos e información.

Los servidores y los navegadores se comunican mediante el Protocolo de transferencia de hipertexto (HTTP), un lenguaje creado para transferir documentos de hipertexto en la Web. Los servidores Web a veces se llaman servidores HTTPD.

Nota: La "D" de HTTPD es la inicial de 'daemon' (vigilante). Un vigilante es el término empleado en UNIX (sistema operativo) para denominar a un programa que está en segundo plano en espera de solicitudes. No hace falta ejecutar UNIX para que el programa se comporte como un vigilante, por lo que los servidores Web de cualquier plataforma también se llaman servidores HTTPD o sencillamente servidores HTTP.

Un servidor web debe soportar los protocolos estándar en la Internet como el HTTP (protocolo de transferencia de hipertexto) que facilita el intercambio de datos entre el servidor web y el navegador. Los navegadores, por su parte, pueden recibir archivos

mediante HTTP y FTP y poseer capacidad para interpretar scripts en los lenguajes con Java y Javascript, PHP y otros comunes, y ofrecer soporte a scripts. Finalmente, debe contener algunos elementos de seguridad. Los programas de aplicación más difundidos para organizar un servidor web son: Apache y IIS de Microsoft.

6.7.5.1 FUNCIONAMIENTO.

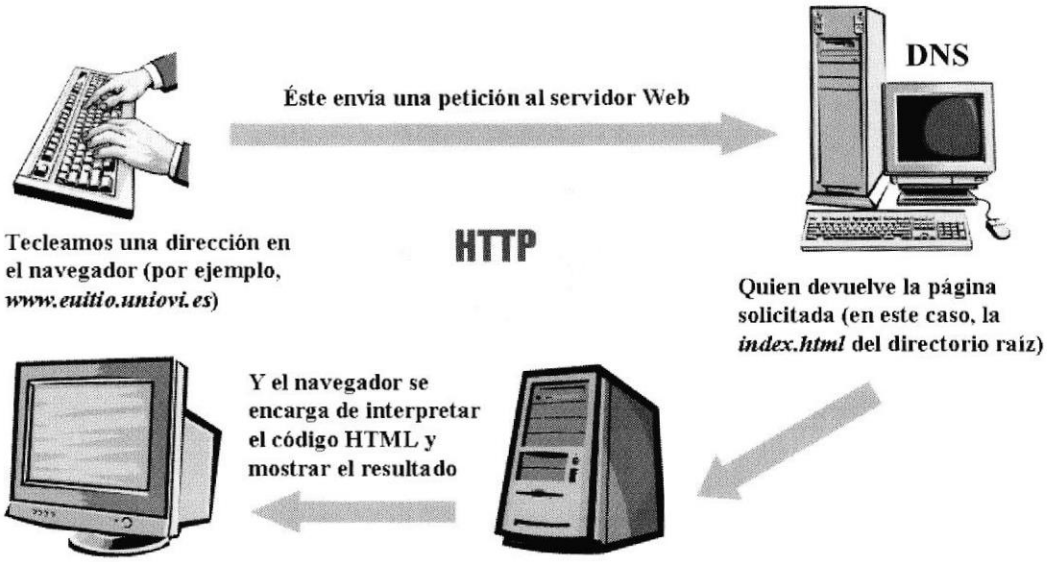


Figura 6.118 Esquema de red, incluyendo un servidor DNS

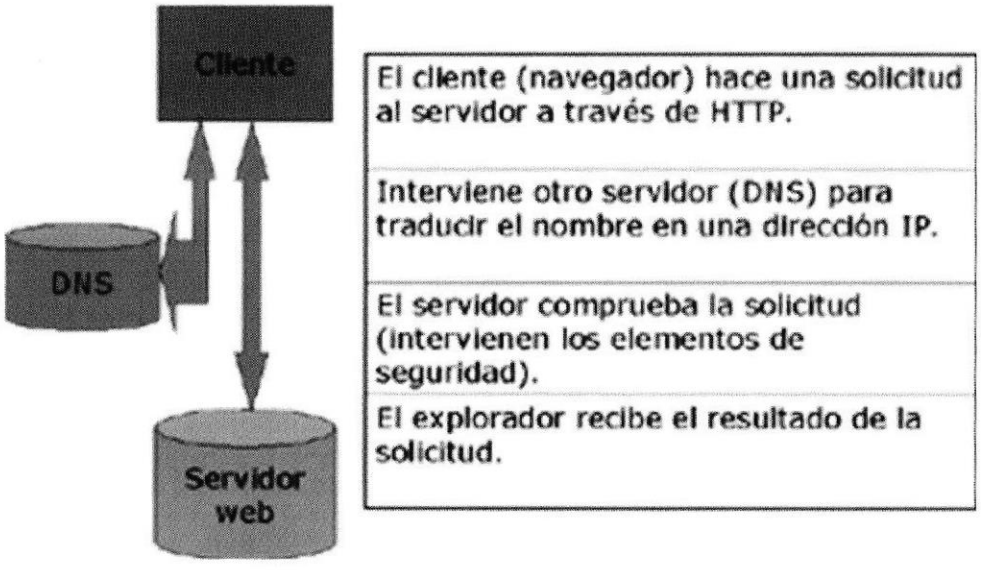


Figura 6.119 Esquema de conexión entre DNS – CLIENTE – WEB SERVER

6.7.5.2 REQUERIMIENTOS.

- Tener previamente configurado el Servidor de Nombres de Dominio.

6.7.5.3 CONFIGURACIÓN de WEB SERVER.

1. Verifique la instalación del paquete de web Server.

[root@localhost /]# rpm –qa httpd

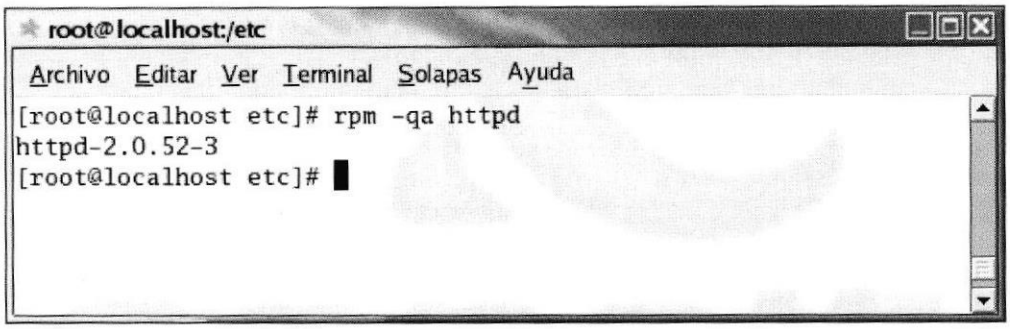


Figura 6.120 Verificación del paquete httpd.

3. Ingresar al archivo httpd.conf que se encuentra en el directorio conf.

[root@localhost /]# vi /etc/httpd/conf/httpd.conf

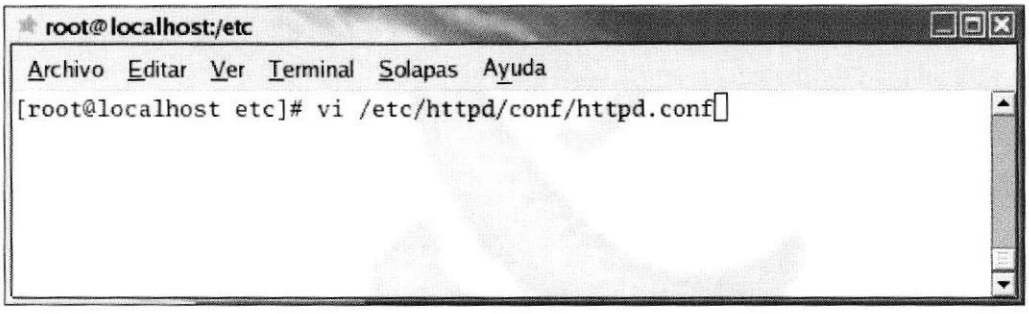


Figura 6.121 Pantalla de ingreso al archivo httpd.conf

4. Una vez editado el archivo se procede a configurarlo, buscando las siguientes líneas y descomentándolas.

Listen 80, este es el puerto por el que escucha web Server.

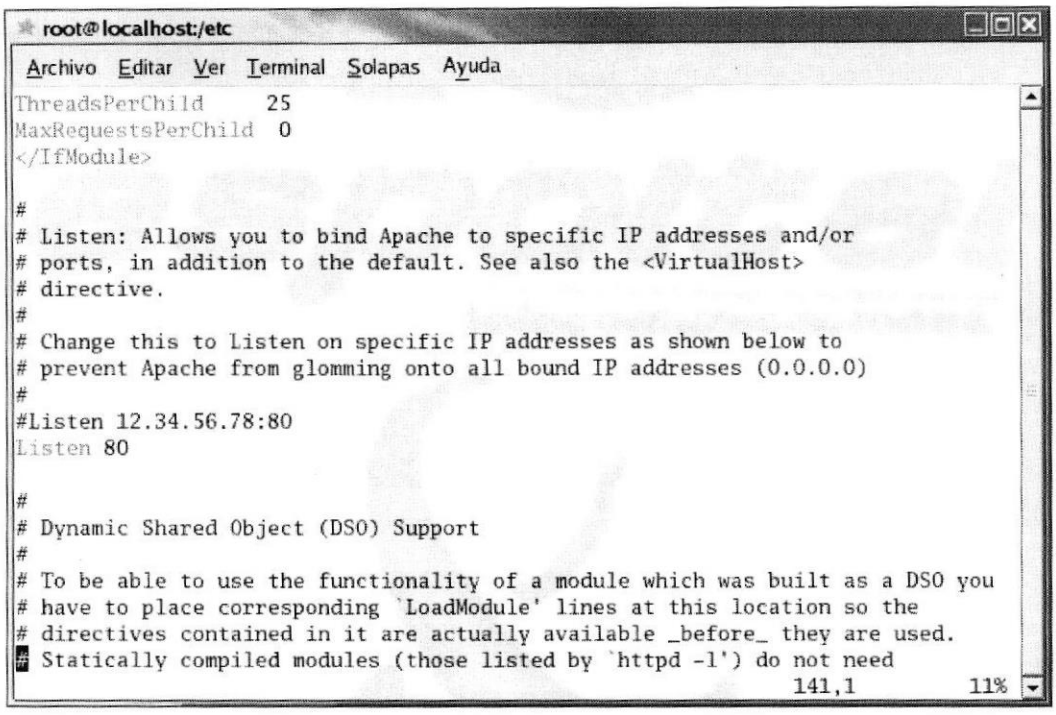


Figura 6.122 Pantalla del archivo httpd.conf sección Listen 80.

DocumentRoot "/var/www/html", indica la ruta donde se guardarán las páginas web.

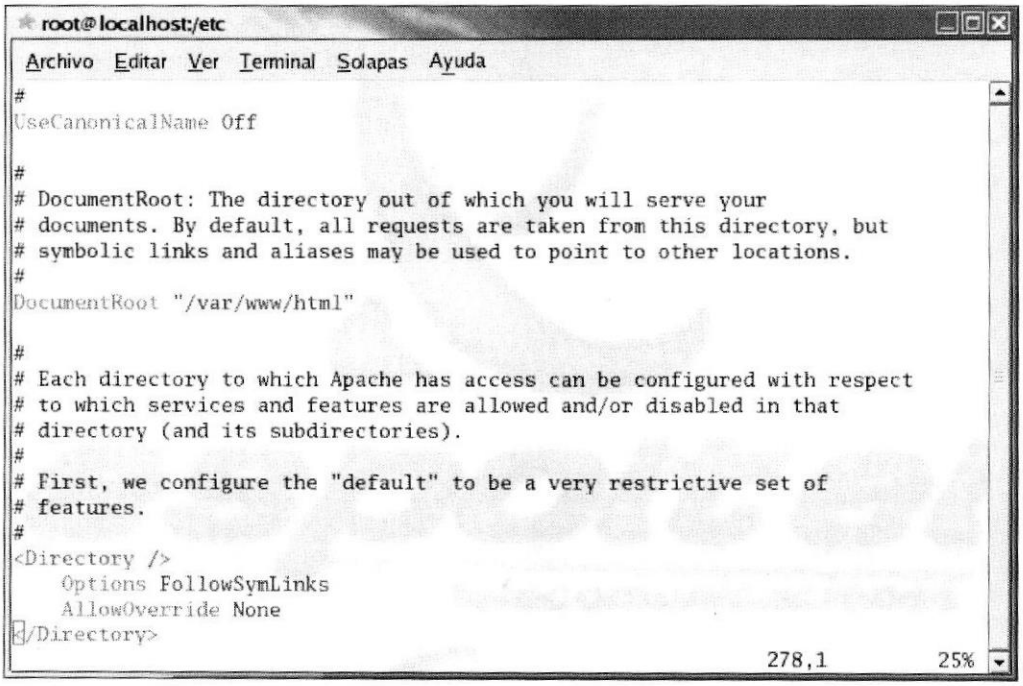


Figura 6.123 Pantalla del archivo httpd.conf sección Document Root

Directory Index index.html index.doc, especifica si el servidor esta apto para usar las extensiones de los tipos de páginas del servidor web.

En este parámetro se agrega el nombre y la extensión del archivo que se va a crear en el caso que no se encuentra especificado

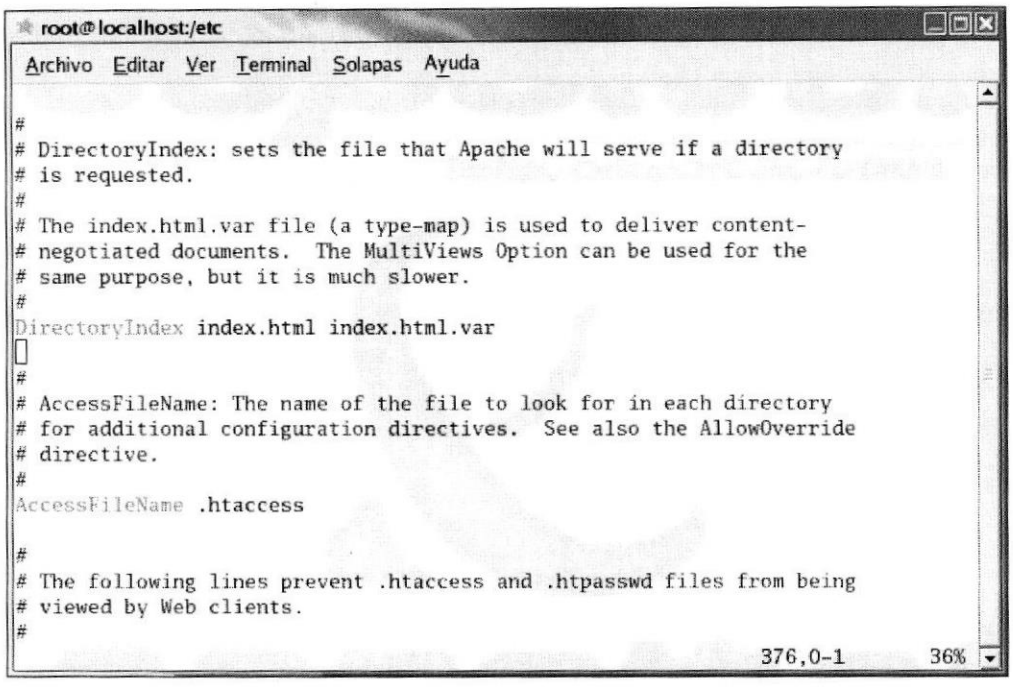


Figura 6.124 Pantalla del archivo httpd.conf sección Directory Index.

NameVirtualHost *:80, es para que escuche a nivel de más páginas (se transforma en servidor virtual).

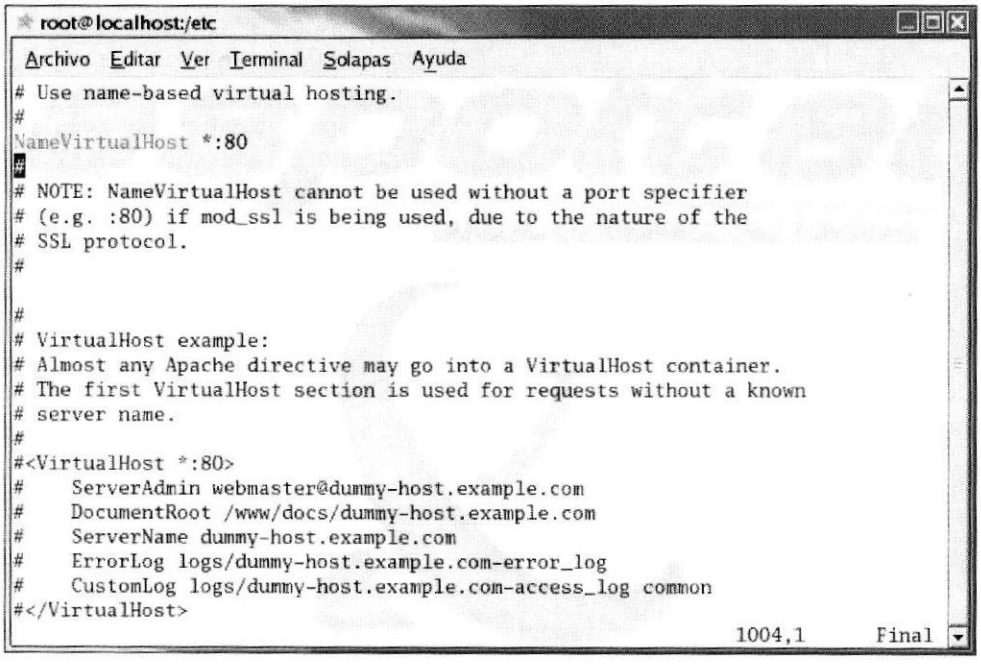


Figura 6.125 Pantalla del archivo httpd.conf sección NameVirtualHost.

5. Copiar el párrafo del <virtual host *:80> -- <virtual host >, descomentar las líneas necesarias y realizar los siguientes cambios:

<virtual host * :80>
server admin root@ localhost.localdomain
document root /var/www/html/sitio

server name www.espoltel.net
</virtual host>

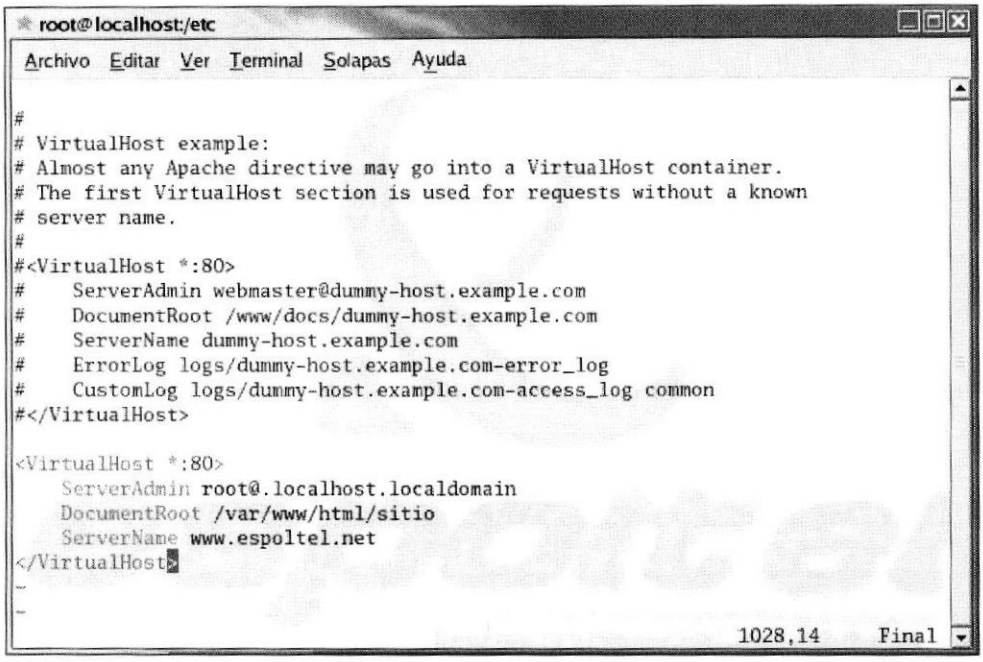


Figura 6.126 Pantalla de edición del archivo httpd.conf sección Virtual Host.

Server Admin, se especifica quien administra.
Document Root, se detalla la ruta donde se guardarán las páginas.
Server Name, especifica la unión entre el sitio web y el servidor web.

6. Ingresar a la ruta especificada en el document root y listar su contenido digitando el comando **ls**, para verificar las carpetas que han sido creadas

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

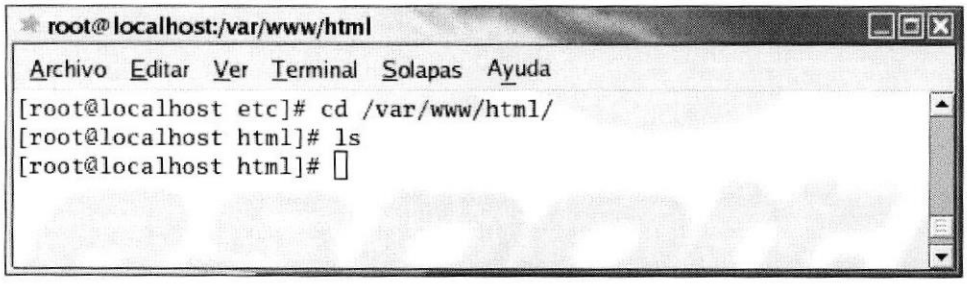


Figura 6.127 Pantalla de ingreso al directorio html.

7. Crear la carpeta donde será ubicada la página.

[root@localhost conf]# mkdir sitio

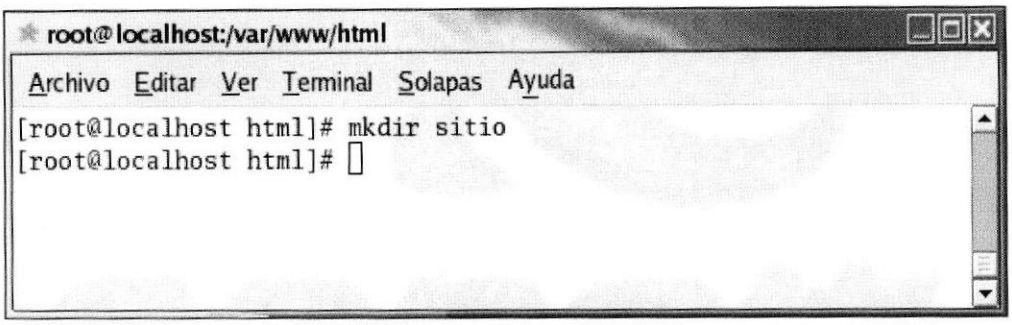


Figura 6.128 Pantalla de creación del directorio sitio.

8. Ingresar al directorio sitio y crear un archivo con extensión .html para verificar funcionamiento.

[root@localhost /]# vi index.html

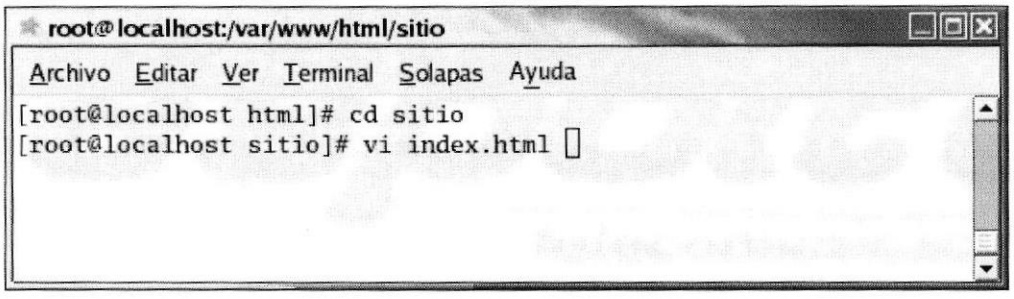


Figura 6.129 Pantalla de creación del archivo index.html.

9. Edite el archivo index.html con un texto cualquier solo para prueba.

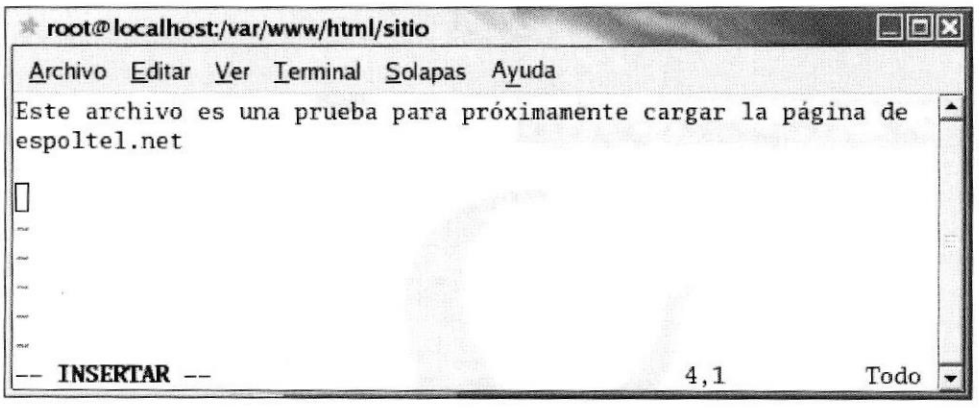


Figura 6.130 Pantalla de creación del archivo index.html.

10. Inicialice los servicios del httpd

[root@localhost /]# service httpd start

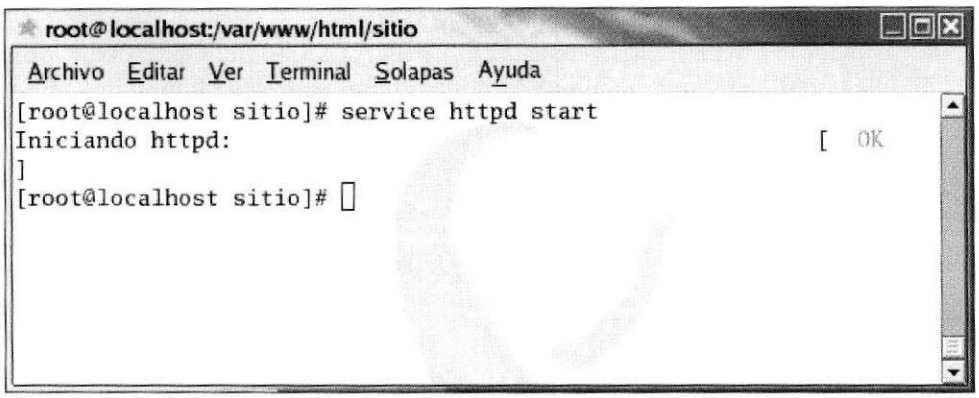


Figura 6.131 Pantalla de inicio del servicio de httpd.

11. Para la verificación de la funcionalidad de este proceso deberá ir al navegador de linux y cargar la dirección www.espoltel.net, esta deberá aparecer con el contenido del archivo de la index.html.

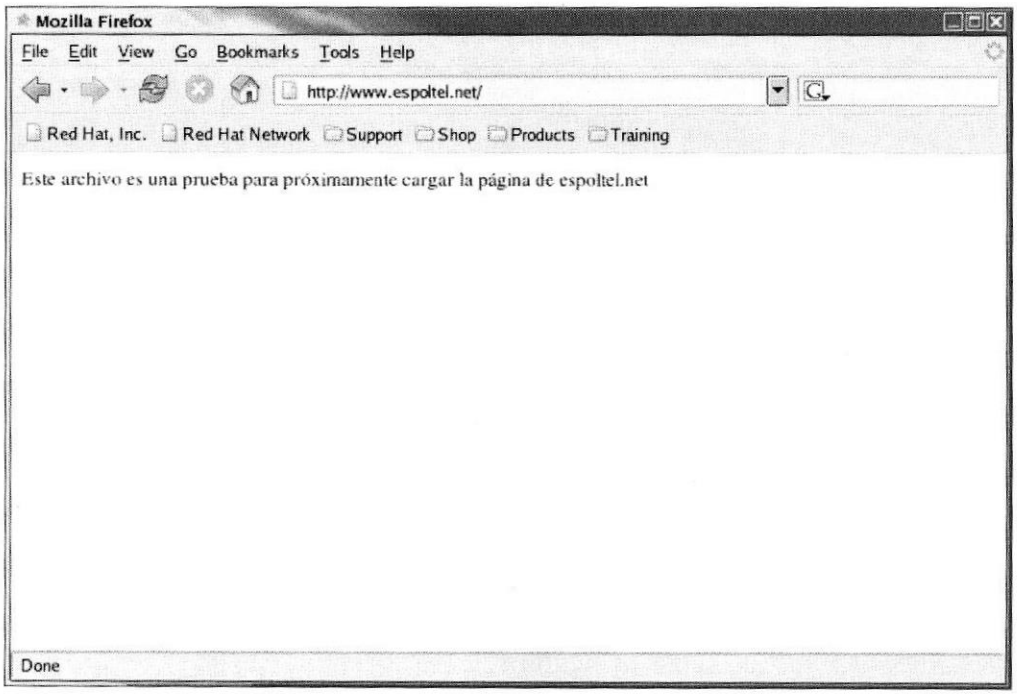


Figura 6.132 Pantalla del navegador de linux cargando www.espoltel.net.

En caso de reiniciar el servidor los servicios no se inician, por lo tanto deberá activarlos con el comando Setup.

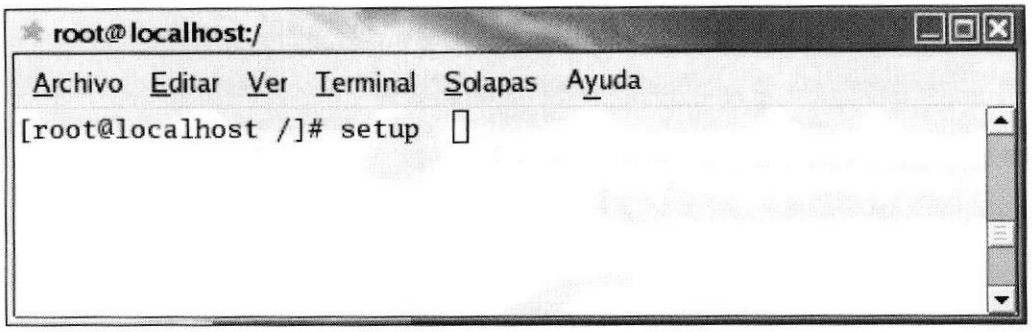


Figura 6.133 Pantalla de ingreso a setup.

A continuación aparecerá una pantalla, la misma que contiene el menú "Elija una Herramienta", donde deberá escoger la opción Servicios del Sistema y luego Ejecutar una Herramienta.

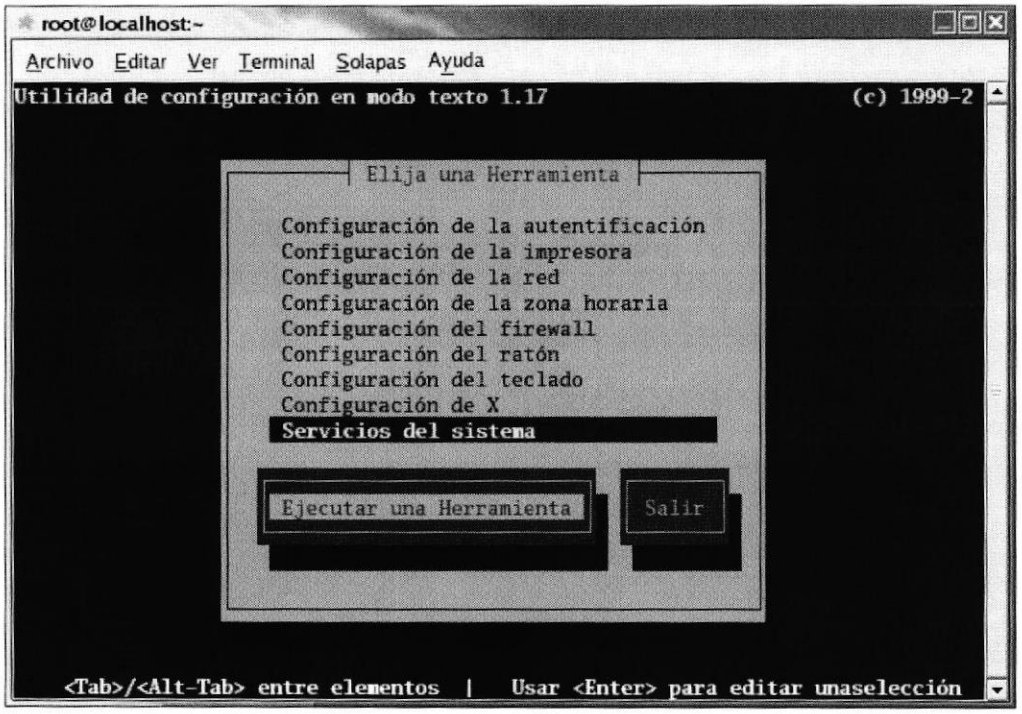


Figura 6.134 Pantalla de ingreso a servicios del sistema.

Aparece la ventana de Servicios donde se habilitará el httpd y elija Ok.

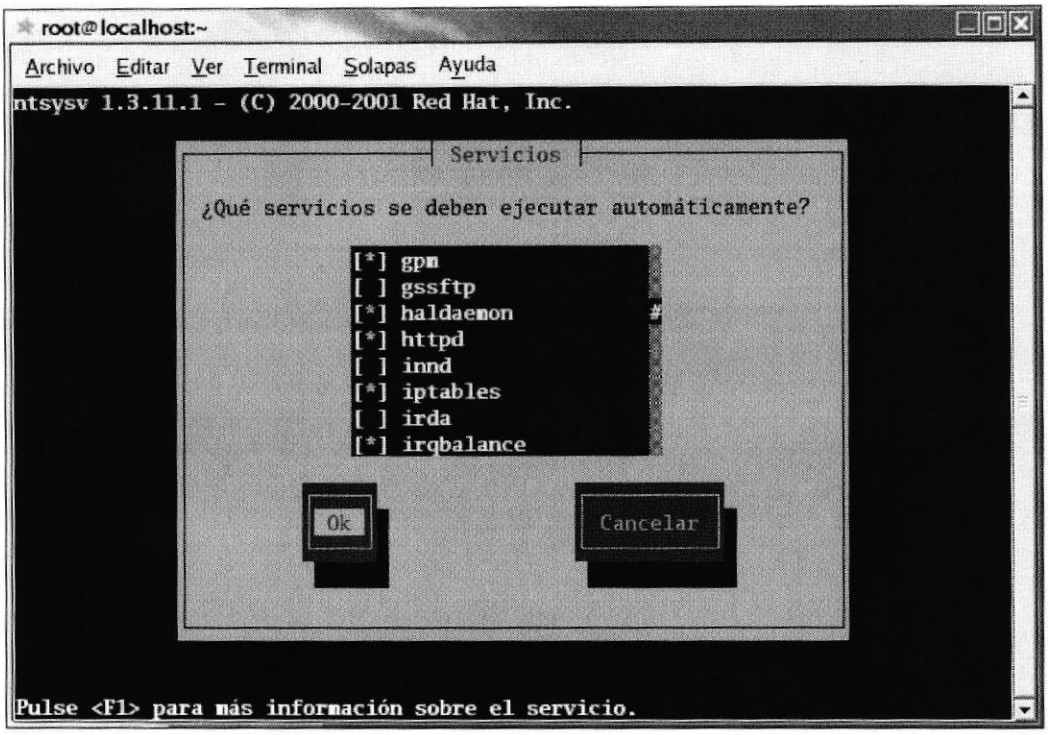


Figura 6.135 Pantalla de selección del paquete httpd.

6.7.5.4 CONFIGURACIÓN EN EL CLIENTE WINDOWS EN WEB SERVER.

1. Ingrese al explorador de Windows, menú Herramientas y elegir Opciones de Internet

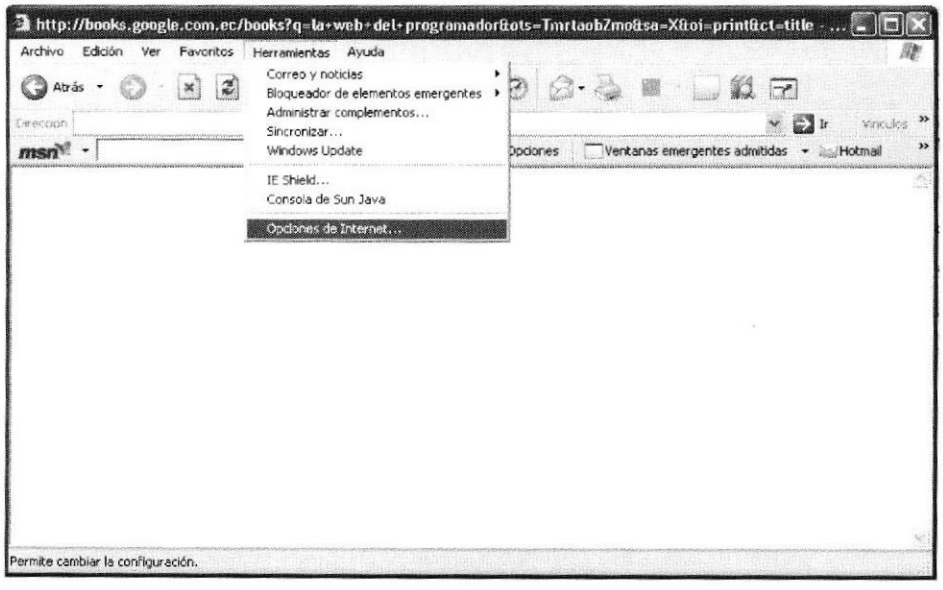


Figura 6.136 Pantalla del Internet Explorer.

2. Dentro de opciones de Internet escoja la opción Conexiones, configuración de la red LAN.

Figura 6.137 Pantalla de Opciones de internet.

3. Señalar Detectar la configuración automática.

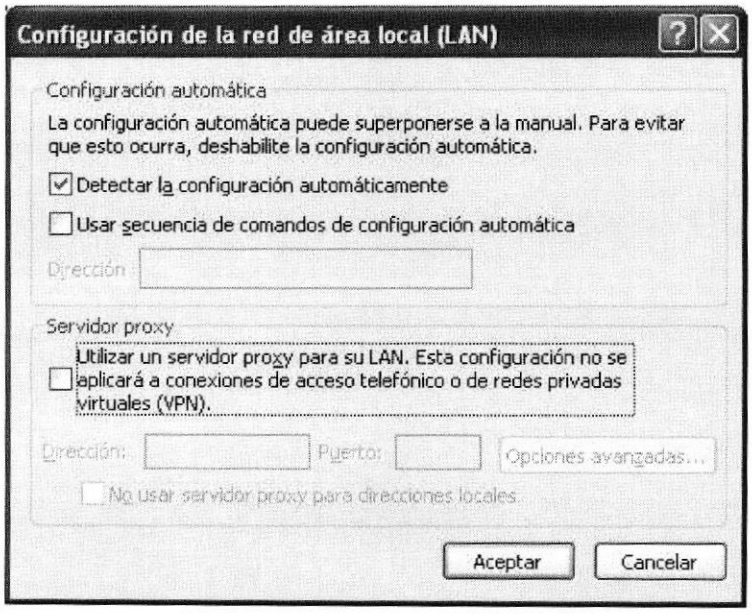


Figura 6.138 Pantalla de configuración de la red de área local.

4. Acceda al sitio web mediante el navegador.

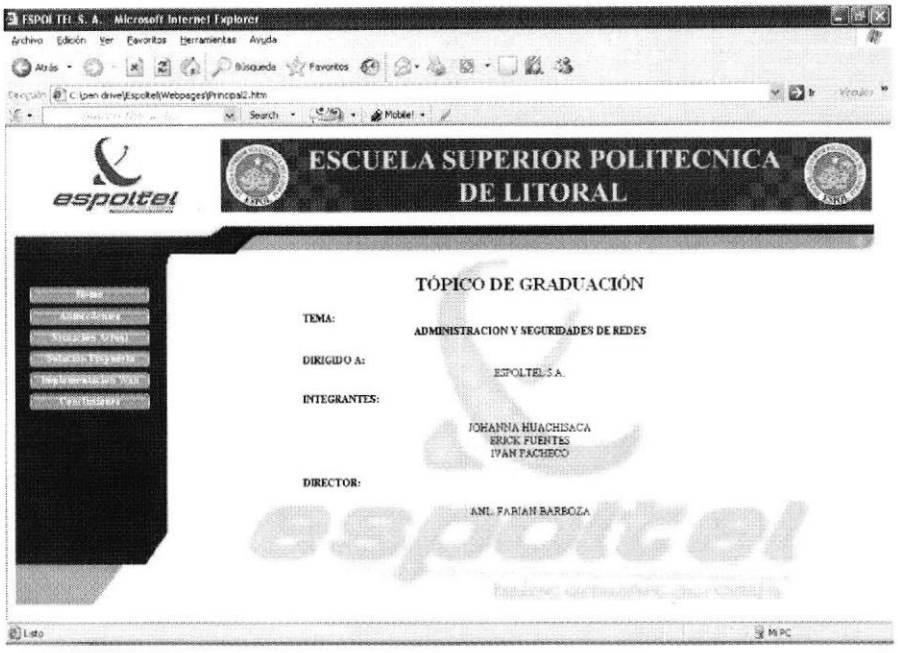


Figura 6.139 Pantalla del internet Explorer cargada la página web de espoltel .net

6.7.6 CONFIGURACIONES DEL SERVIDOR PROXY.

Un Proxy Server es un servidor intermediario entre las computadoras de la red local e Internet, con esto se garantiza seguridad, control administrativo y servicio de caché.

Además de esto puede ser un servidor de caché que hace que los accesos a Internet sean más rápidos y que el canal de acceso a Internet se libere de forma significativa.

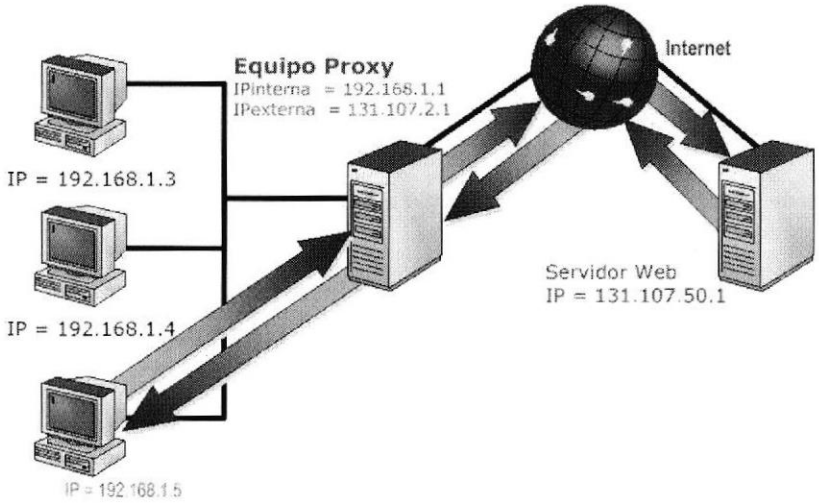


Figura 6.140 Esquema de Proxy.

6.7.6.1 FUNCIONAMIENTO.

Un Proxy Server trabaja de la siguiente manera:

- El Proxy Server recibe una solicitud de un usuario para un servicio de Internet.

- Si la solicitud pasa el proceso de filtrado, el Proxy Server busca en el caché local las páginas previamente descargadas, si encuentra el documento y este es válido lo envía al usuario directamente sin tener que pasar la solicitud por el canal de Internet.

- Si la página no está en caché el Proxy Server se encarga de descargarla de Internet por medio del canal de acceso externo y la envía al usuario que la solicitó una vez que la tenga.

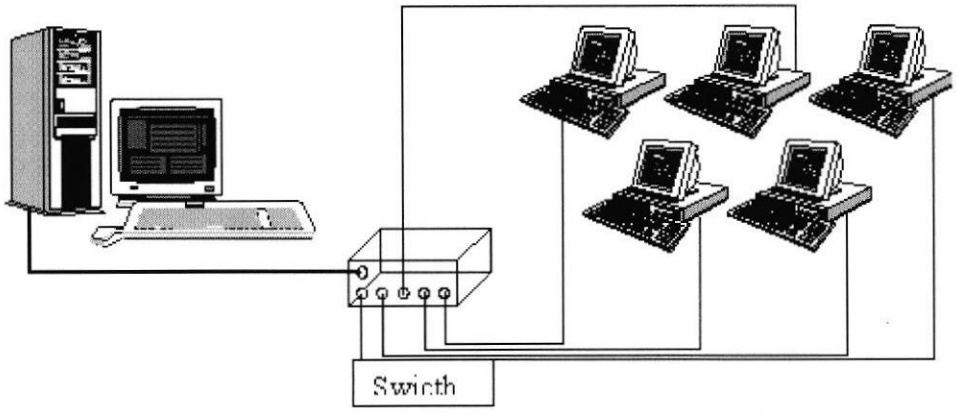


Figura 6.141 Esquema de funcionalidad de Proxy.

6.7.6.2 VENTAJAS.

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

- Un Proxy Server concentra el punto de entrada a Internet en un sólo nodo de la red local, dada su funcionalidad de firewall se encarga de verificar todo el tráfico y permite el ingreso y salida de sólo la información autorizada, de esta forma le provee una gran protección contra intrusos a la red interna.

- El Proxy Server también permite control administrativo de la conexión a Internet, permite hacer que los usuarios de la red Interna tengan acceso sólo a los servicios que se les definan.

- Menor coste de equipo.

- Una sola línea telefónica.

- Uso de un sólo MÓDEM.

- Descentralización del acceso a Internet.

- Personalización de configuraciones en el software de Internet.

- Configuraciones de seguridad.

- Conexión y desconexión automática, cada estación establece la conexión individualmente y sin interferir con otra estación.

- Estación de salida no dedicada.

6.7.6.3 DESVENTAJAS.

- Las páginas mostradas pueden no estar actualizadas si estas han sido modificadas desde la última carga que realizó el proxy caché.

- Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona para un Proxy (a menos que se utilicen lenguajes como PHP).

- El hecho de acceder a Internet a través de un Proxy, por conexión directa, impide realizar operaciones avanzadas mediante algunos puertos o protocolos.

- Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la privacidad para algunas personas.

6.7.6.4 REQUERIMIENTOS.

- Debe tener previamente configurados el Servidor de Nombre de Dominios y el Servidor Web.

Para poder llevar a cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos lo siguiente:

- squid-2.4.STABLE1
- kernel-2.4.9
- apache 1.3.22

Tómese en consideración que, de ser posible, se debe utilizar la versión estable más reciente de todo el software que vaya a instalar al realizar los procedimientos descritos en este manual, a fin de contar con los parches de seguridad necesarios. Ninguna versión de Squid anterior a la 2.4.STABLE1 se considera como apropiada debido a fallas de seguridad de gran importancia, y ningún administrador competente utilizaría una versión inferior a la 2.4.STABLE1.

6.7.6.5 CONFIGURACIÓN DE PROXY.

1. Comprobar si esta instalado el servicio squid

```
[root@localhost /]#rpm -q squid
```

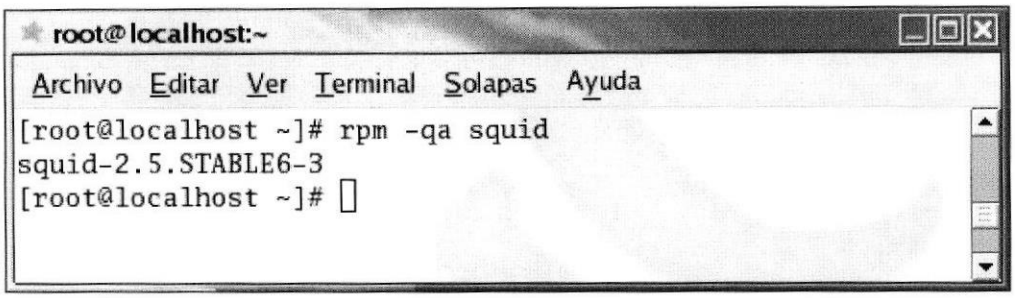


Figura 6.142 Pantalla de verificación del paquete squid.

2. Ingresar al directorio squid para editar el archivo squid.conf

[root@localhost /]# vi /etc/squid/squid.conf

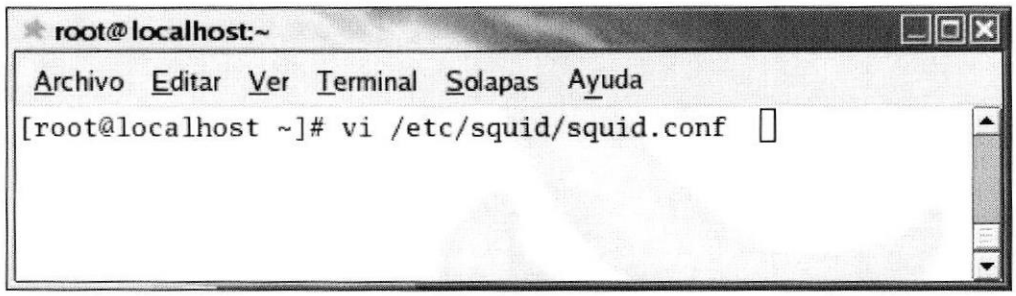


Figura 6.143 Pantalla de ingreso al archivo squid.conf-

3. Una vez editado el archivo proceda a realizar los siguientes cambios en las secciones:

   El parámetro **http_port**, en squid el puerto por defecto es el 3128 para atender peticiones pero puede especificarse otro, o más de uno.

   - Proxy Transparente utiliza el puerto 80 y redirecciona peticiones.
   - Proxy Convencional suele traer por defecto el puerto 8080 (Servicio de Cacheo de www).

   http_port 8080, cambiar el puerto 3128 por el 8080.

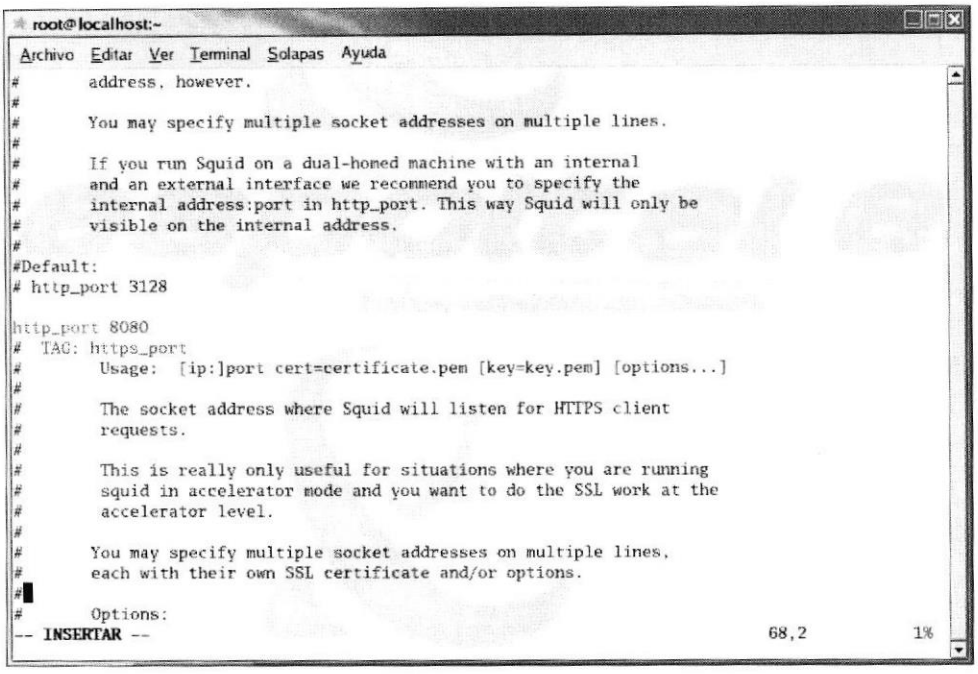


Figura 6.144 Pantalla de configuración del http_port 8080.

El parámetro **cache_men,** establece la cantidad de memoria para Objetos en Tránsito, Objetos Hot y Objetos navegantes almacenados en caché. Debido a que los datos se almacenan en bloques de 4 kb por defecto se asignan 8 MB.

cache_men 16 MB, cambiar 8 MB por 16 MB

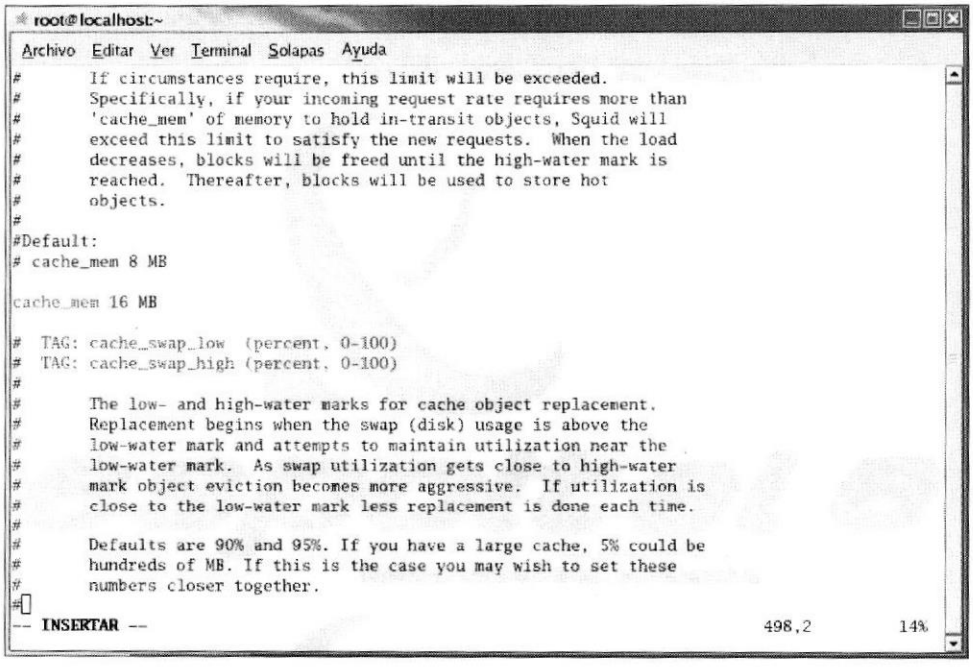


Figura 6.145 Pantalla de configuración de la cache_men.

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

cache_dir ufs /var/spool/squid 100 16 256 , descomentar

El parámetro **cache_access_log,** sirve para monitorear la actividad de los hosts que tenga a cargo el Proxy.

cache_access_log /var/log/squid/access_log, descomentar

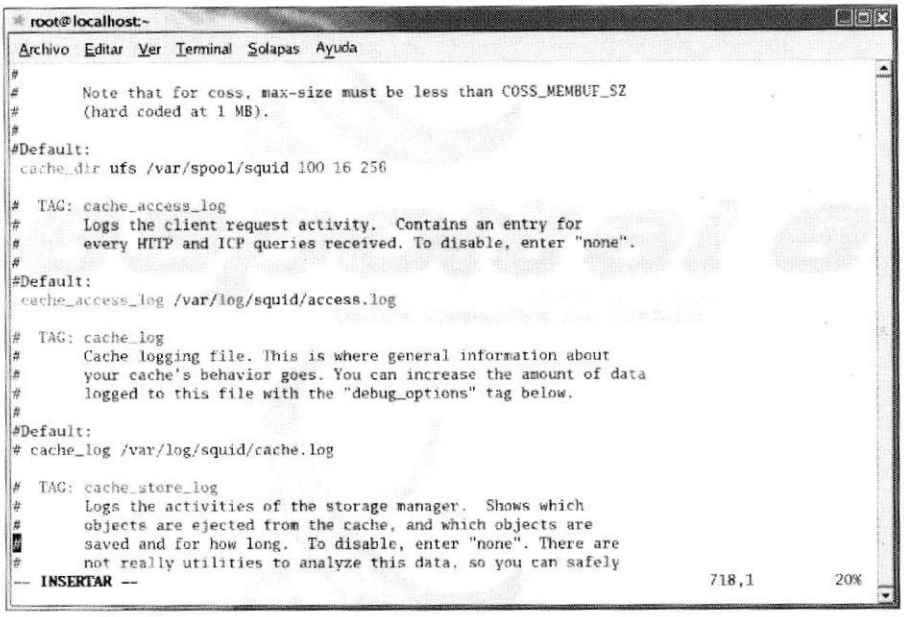


Figura 6.146 Pantalla de configuración de cache_dir y cahe_access_log.

pid-filename, Descomentar

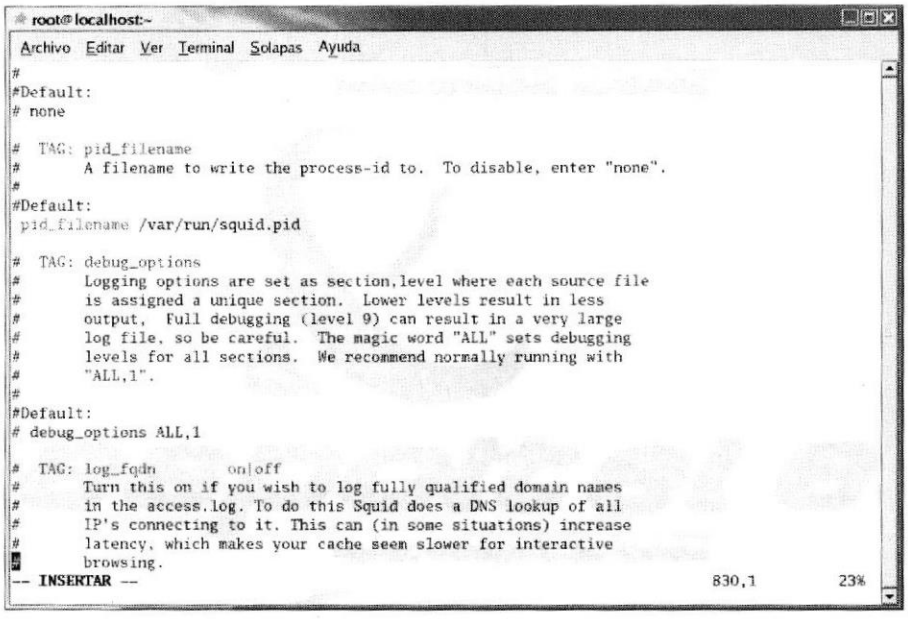


Figura 6.147 Pantalla de configuración del pid_filename.

4. Configurar las listas de control de acceso

acl red src 192.168.10.1 /255.255.255.0

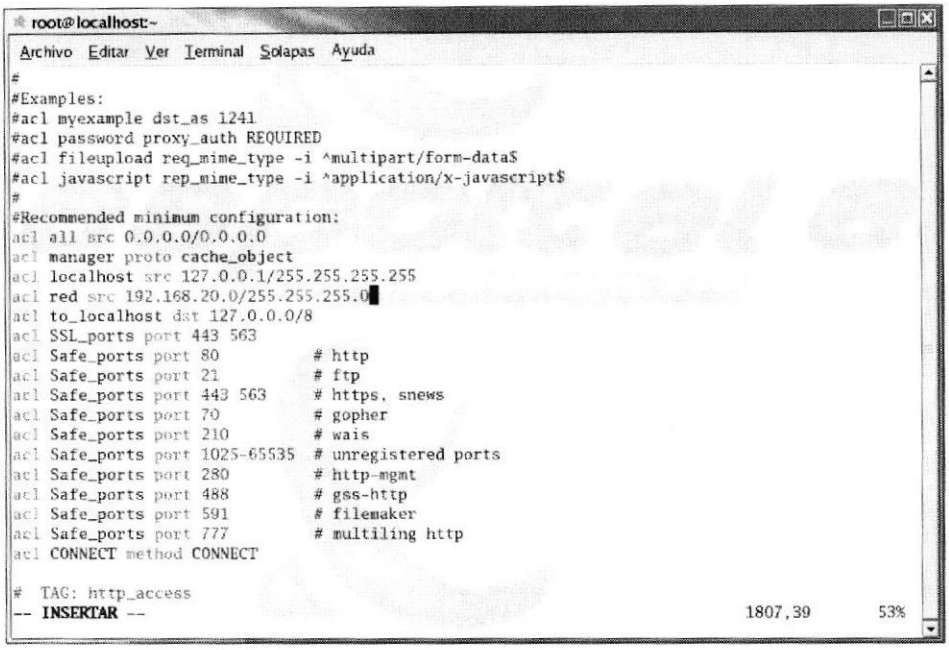


Figura 6.148 Pantalla de configuración sección de acl-

5. Incluir las listas de control de acceso en las reglas de control de acceso

   http_access allow red web

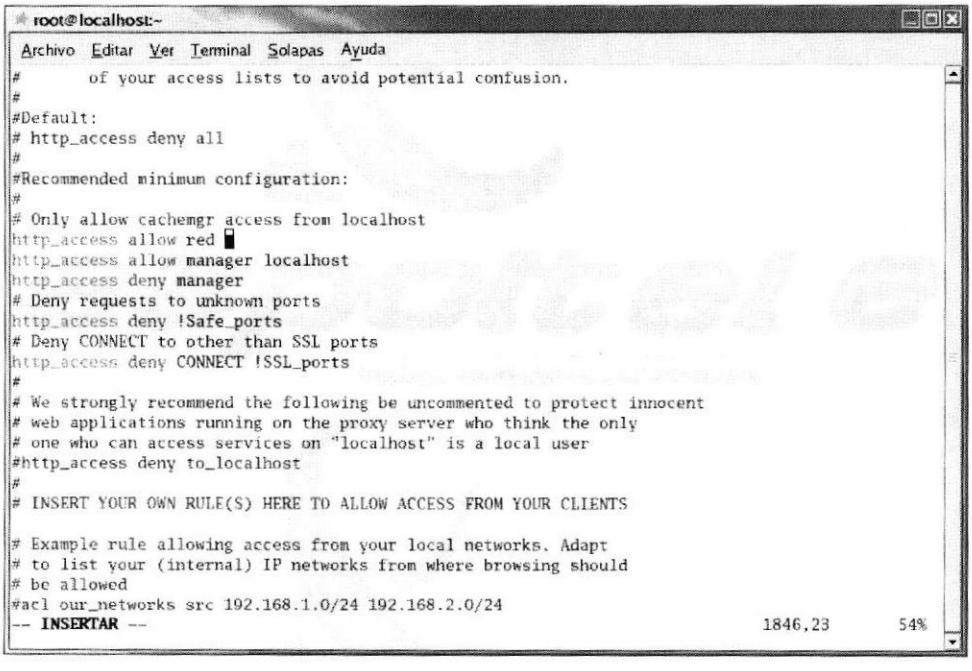


Figura 6.149 Pantalla de configuración del archivo squid.conf sección http_access.

6. Reiniciar el servicio

   [root@localhost /]# service squid restart

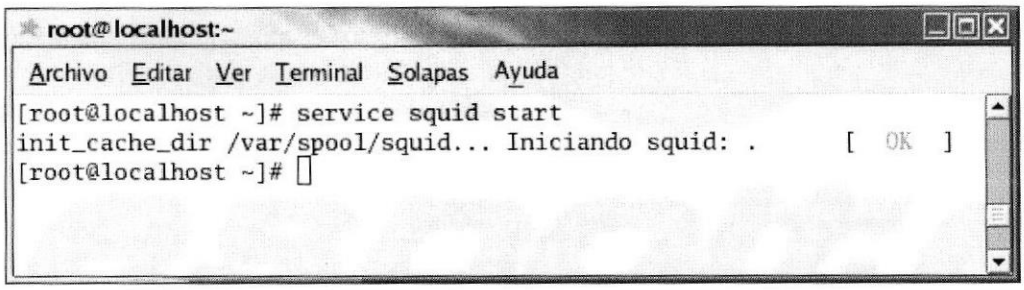


Figura 6.150 Pantalla de reiniciar el servicio de squid.

6.7.6.6 CONFIGURACION EN EL CLIENTE WINDOWS EN PROXY.

1. Ingrese al explorador de Windows, elija Menú Herramientas, y luego Opciones de Internet.

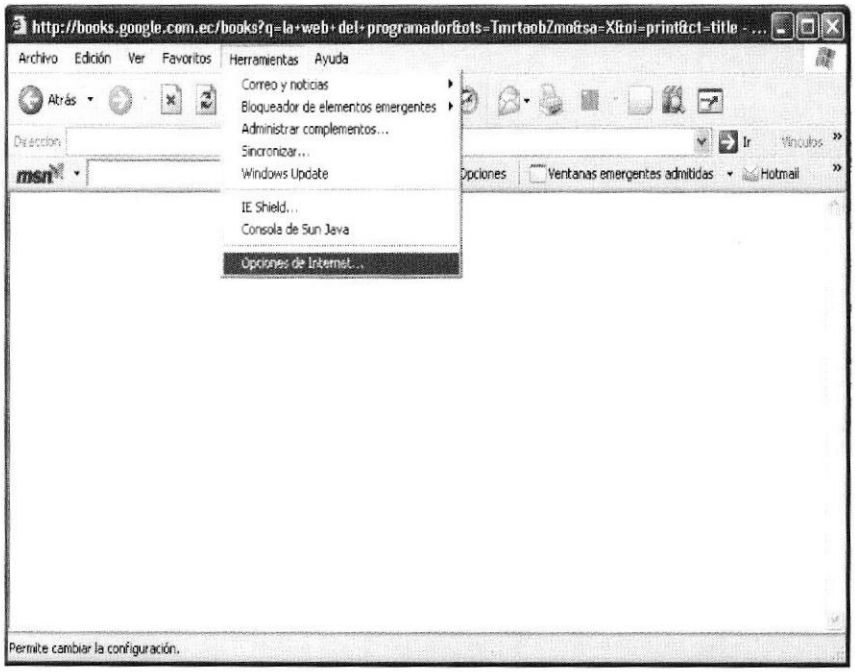


Figura 6.151 Pantalla del internet Explorer.

2. Dentro de Opciones de Internet escoja Conexiones, y Configuración de la red LAN.

Figura 6.152 Pantalla de Opciones de Internet.

3. En esta pantalla se debe colocar la dirección del servidor y el puerto de comunicación en este caso para proxy es el 8080.

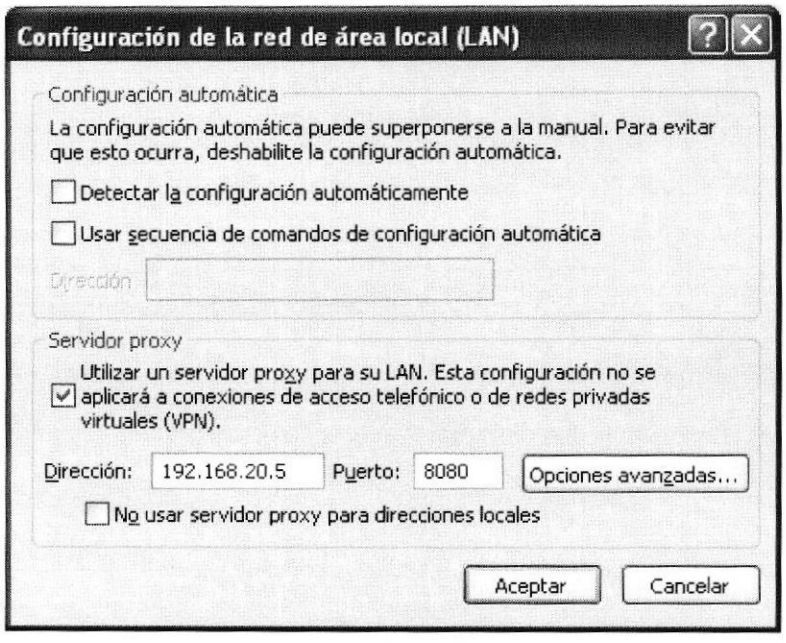


Figura 6.153 Pantalla de configuración de la red de área ocal.

4. Proceda a cargar la página www.espoltel.net, la misma que debe de estar configurada previamente en DNS y WEB SERVER.

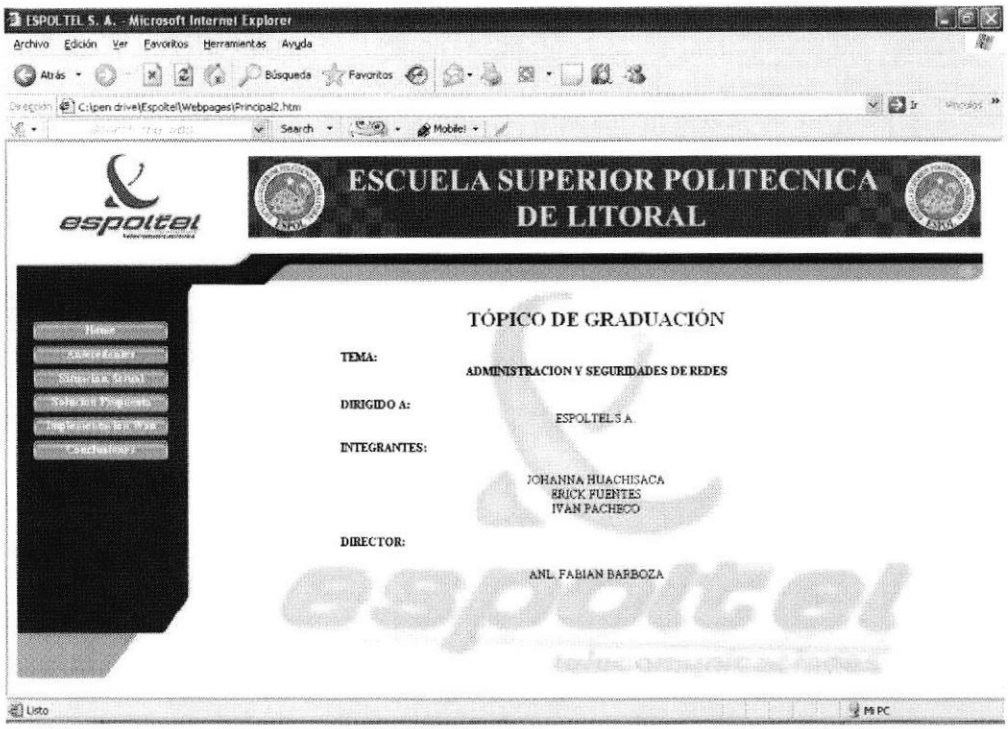


Figura 6.154 Pantalla de Internet Explorer cargada la página de espoltel.net.

6.7.6.7 DENEGAR ACCESOS POR HORA.

1. Incluir las listas de control de acceso (acl)
   acl (nombre de la lista) time (día) (hora inicio)-(hora fin)
   Ej.: acl matutino time A 12:00-12:10

   acl (nombre de la regla) src (ip de la red o la maquina a restringir)/
   Ej.: acl cliente src 192.168.12.2/255.255.255.248

Los días están determinados por las letras

- Lunes M
- Martes T
- Miércoles W
- Jueves H
- Viernes F
- Sábado A
- Domingo S

Pueden combinarse los días, aunque la hora inicio y hora fin debe ser asignados en formato 24:00.

2. Incluir las reglas de control de acceso
   http_acces deny cliente matutino 1

3. Reiniciar el servicio
   [root@localhost /]# service squid start

6.7.6.8 CONFIGURACIÓN EN EL CLIENTE WINDOWS PARA DENEGAR ACCESO POR HORA EN PROXY.

1. Abrir Internet Explorer, elegir Menú / Herramientas / Opciones de Internet.

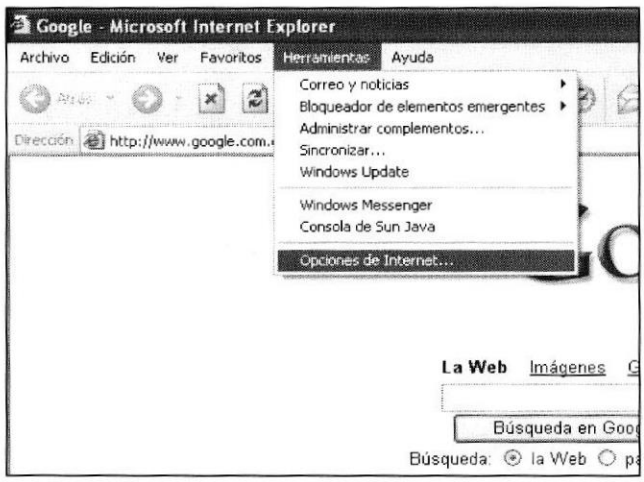


Figura 6.155 Pantalla de Internet Explorer.

2. De la pantalla que aparece elegir Conexiones / Configuración de Lan / Servidor Proxy.

Figura 6.156 Pantalla de opciones de internet.

3. **Dirección** 192.168.20.5 (IP del servidor) **Puerto** 8080.

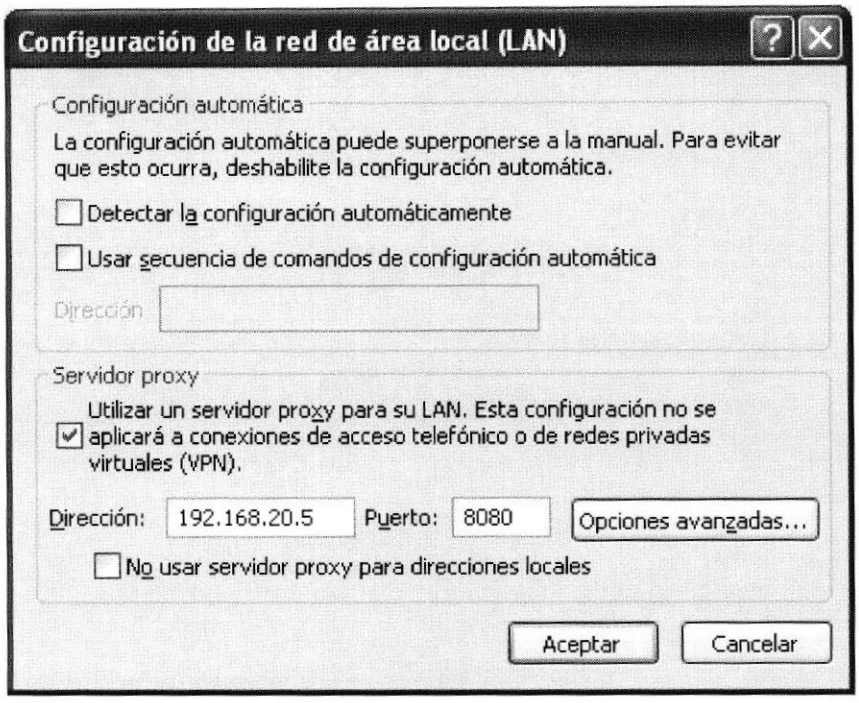


Figura 6.157 Pantalla de configuración de la red de área local.

4. Ingresar al sitio web mediante el navegador. Recordar que debió haber asignado la dirección DNS en la máquina Windows.

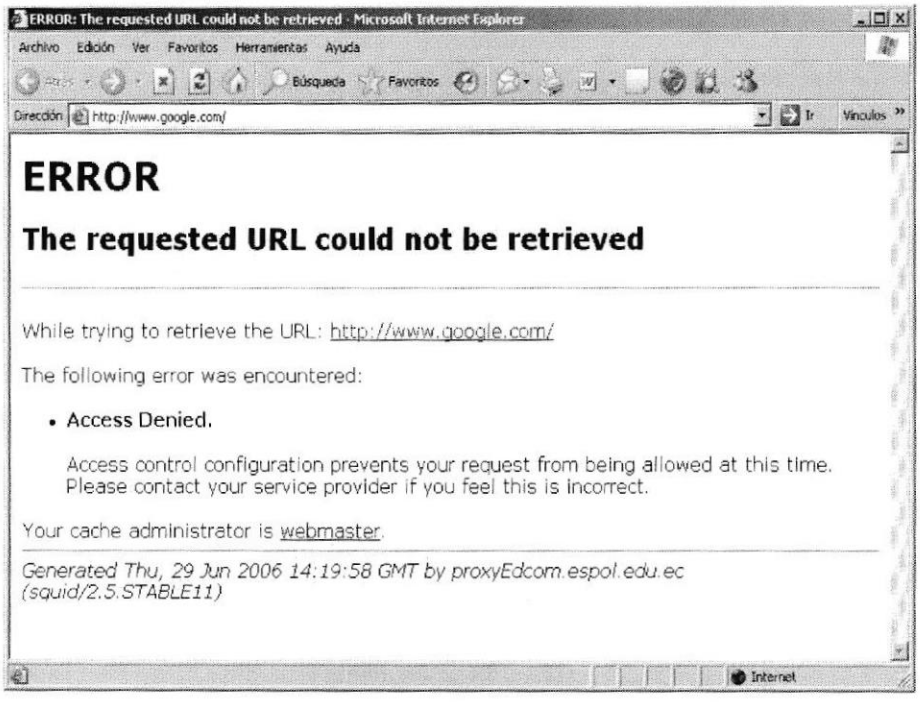


Figura 6.158 Pantalla de internet Explorer con error al cargar la página.

6.7.6.9 ACCESO CON AUTENTICACIÓN (PASSWORD)

1. Ingresar al directorio de squid y crear archivo claves

[root@localhost /]# cd /etc/squid
[root@localhost /]# touch /etc/squid/claves

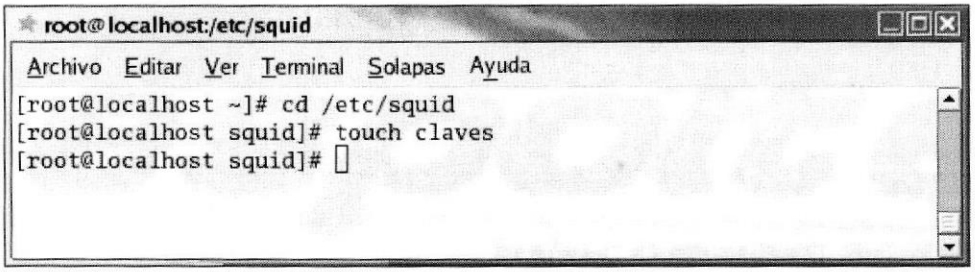


Figura 6.159 Pantalla de creación de archivo claves.

2. Asignar permisos al archivo claves .

[root@localhost /]# chmod +600 claves

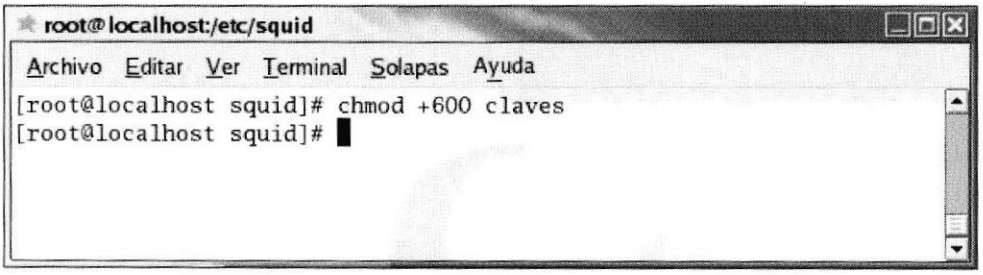


Figura 6.160 Pantalla de asignación de permisos al archivo claves.

3. Cambiar de propietario al archivo.

[root@localhost /]# chown squid:squid claves

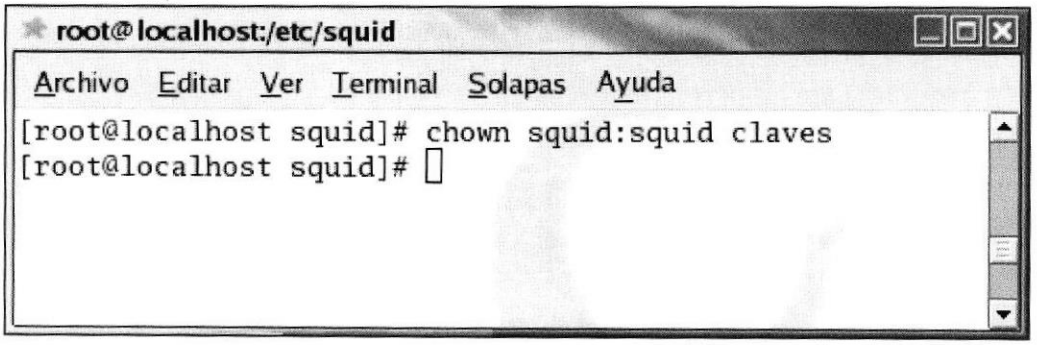


Figura 6.161 Pantalla de cambiar de propietario al archivo claves.

4. Asignar contraseña al usuario user1 de linux.

[root@localhost /]# htpasswd –b claves user1 user1

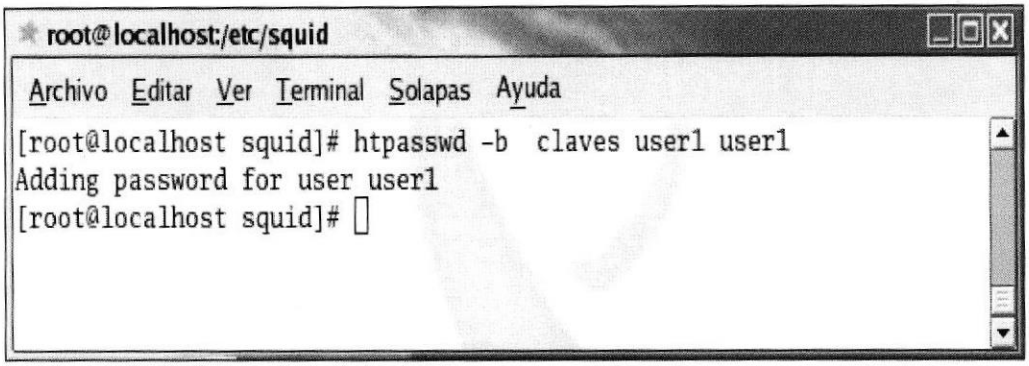


Figura 6.162 Pantalla de asignar contraseña a un usuario linux.

5. Configurar el archivo squid.conf, para descomentar la línea donde se especifica el parámetro de autenticación de contraseñas.

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

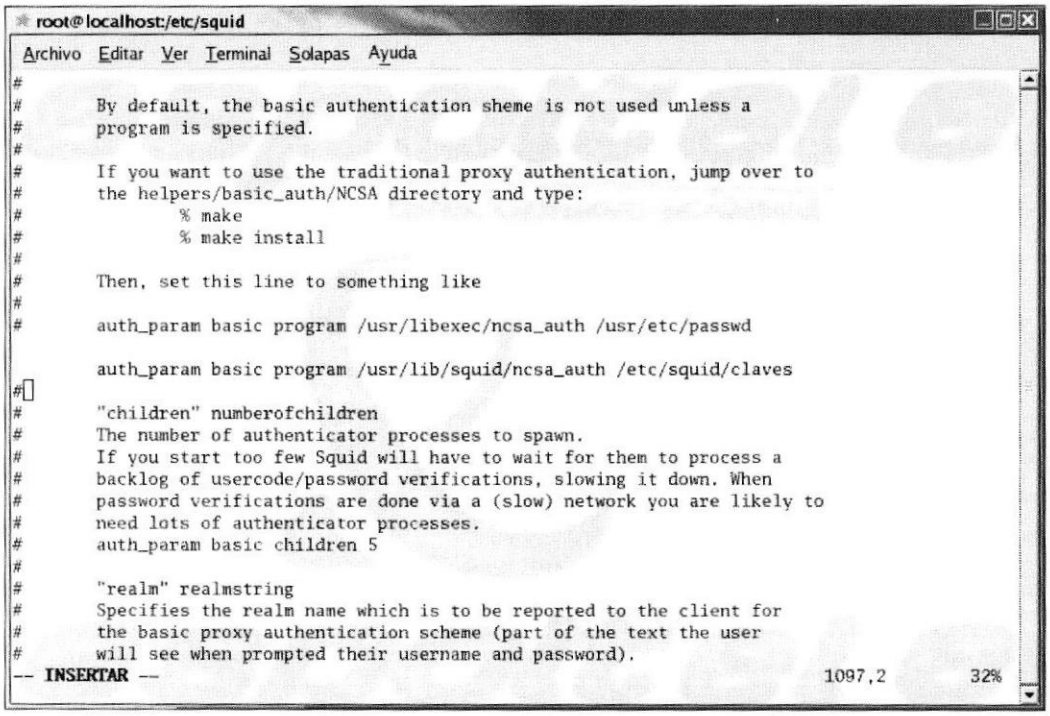


Figura 6.163 Pantalla del archivo squid.conf, sección autenticación de claves.

6. Incluir la lista de control de acceso.
acl password proxy_auth REQUIRED

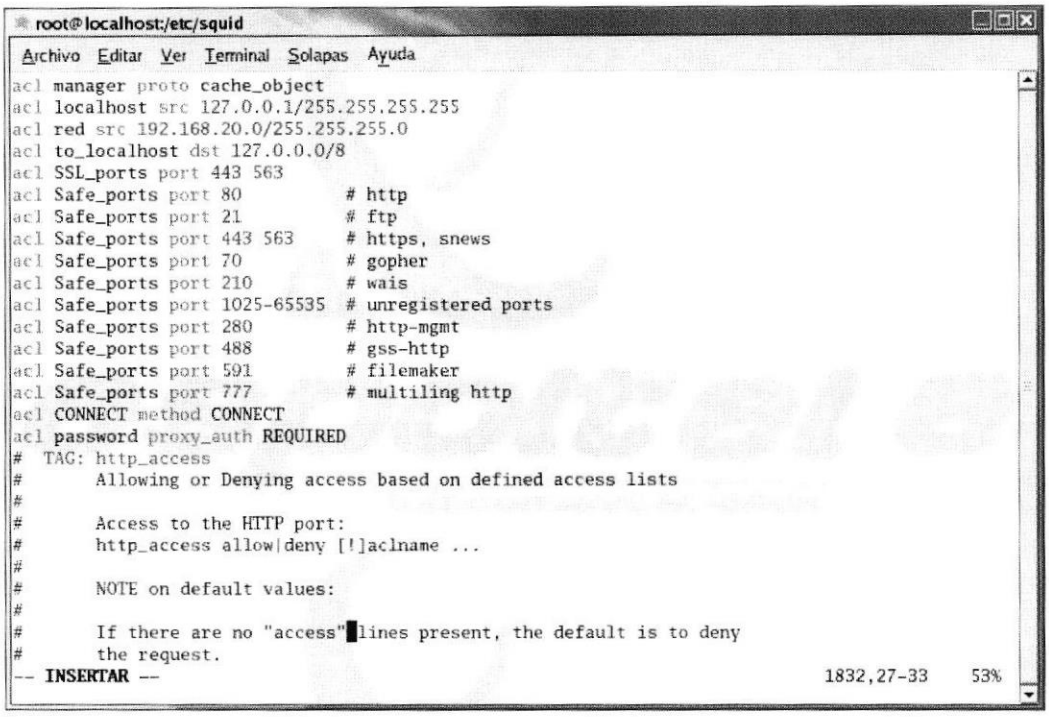


Figura 6.164 Pantalla de archivo squid.conf, sección acl.

7. Incluir la regla de control de acceso.
   http_access allow cliente password

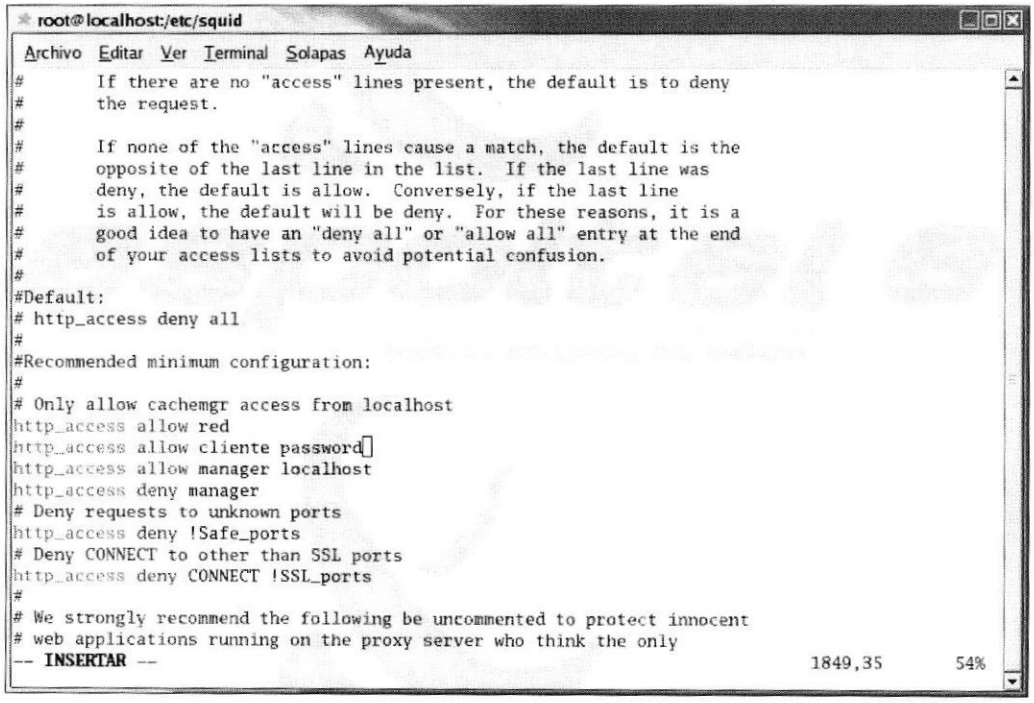


Figura 6.165 Pantalla de archivo squid.conf, sección http_access

8. Reiniciar el servicio.

   [root@localhost /]# service squid restart

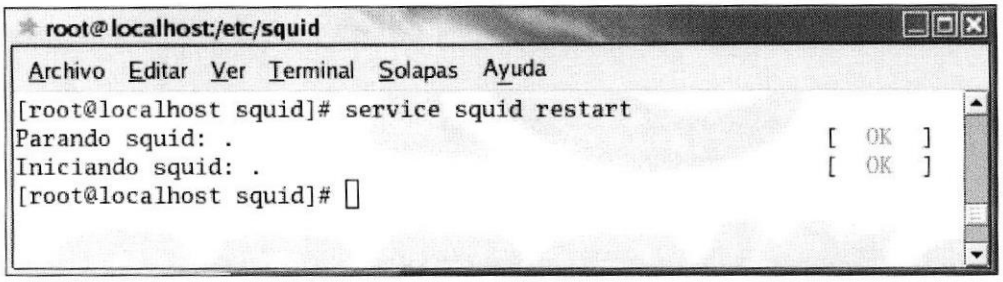


Figura 6.166 Pantalla para reiniciar el servicio de squid.

6.7.6.10 CONFIGURACIÓN EN EL CLIENTE WINDOWS PARA AUTENTICACIÓN DE PASSWORD.

1. Abrir Internet Explorer, elegir Menú / Herramientas / Opciones de Internet.

Figura 6.167 Pantalla de Internet Explorer.

2. De la pantalla que aparece elegir Conexiones / Configuración de Lan / Servidor Proxy.

Figura 6.168 Pantalla de opciones de internet.

3. **Dirección** 192.168.20.5 (IP del servidor) **Puerto** 8080.

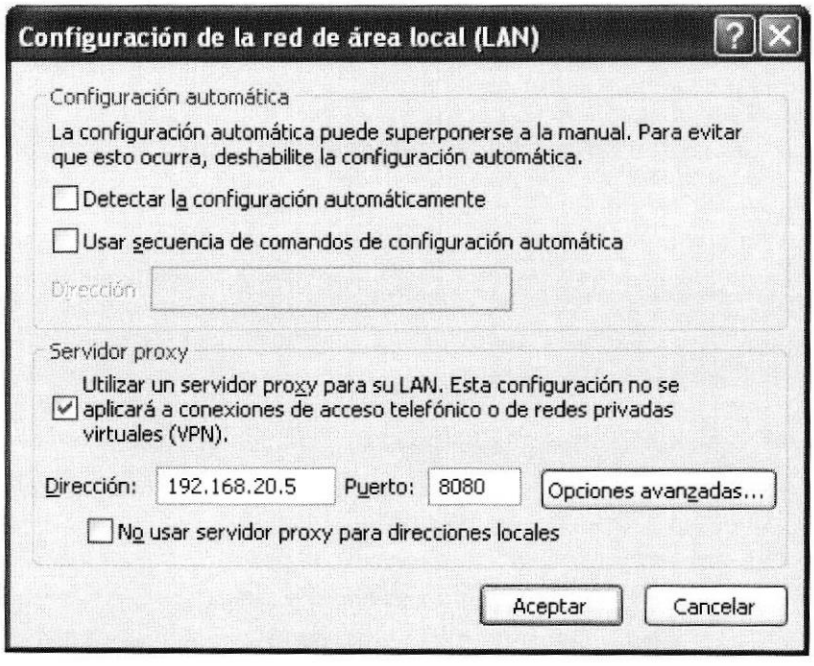


Figura 6.169 Pantalla de configuración de la red de área local.

4. Ingresar al sitio web mediante el navegador. Recordar que se debió haber asignado la dirección DNS en la máquina Windows.

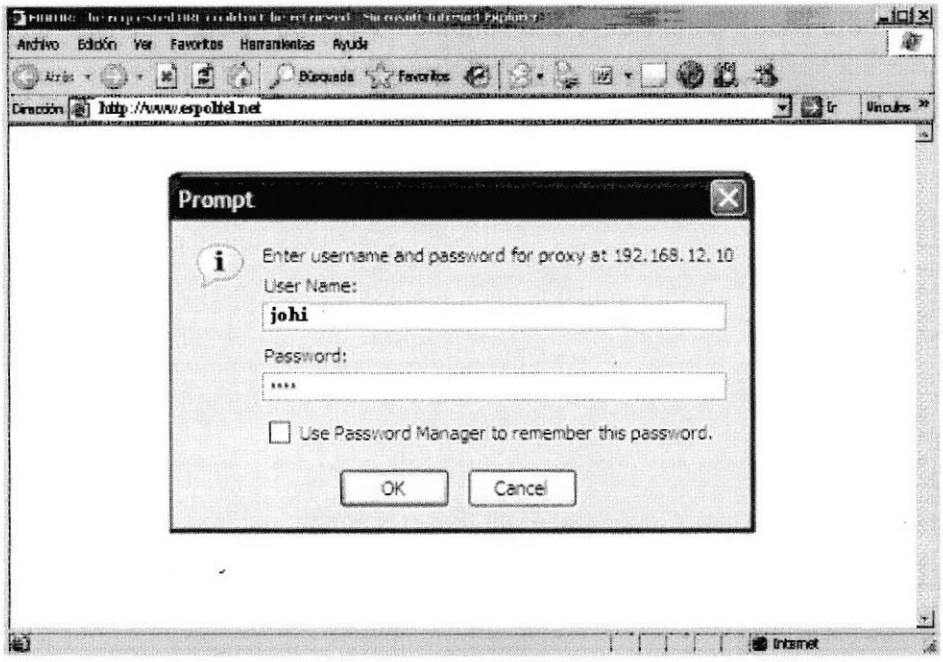


Figura 6.170 Pantalla de autenticación de usuario y contraseña en Proxy.

5. Si es correcta la clave y no hay ninguna regla por cumplir, comenzará a cargar la página.

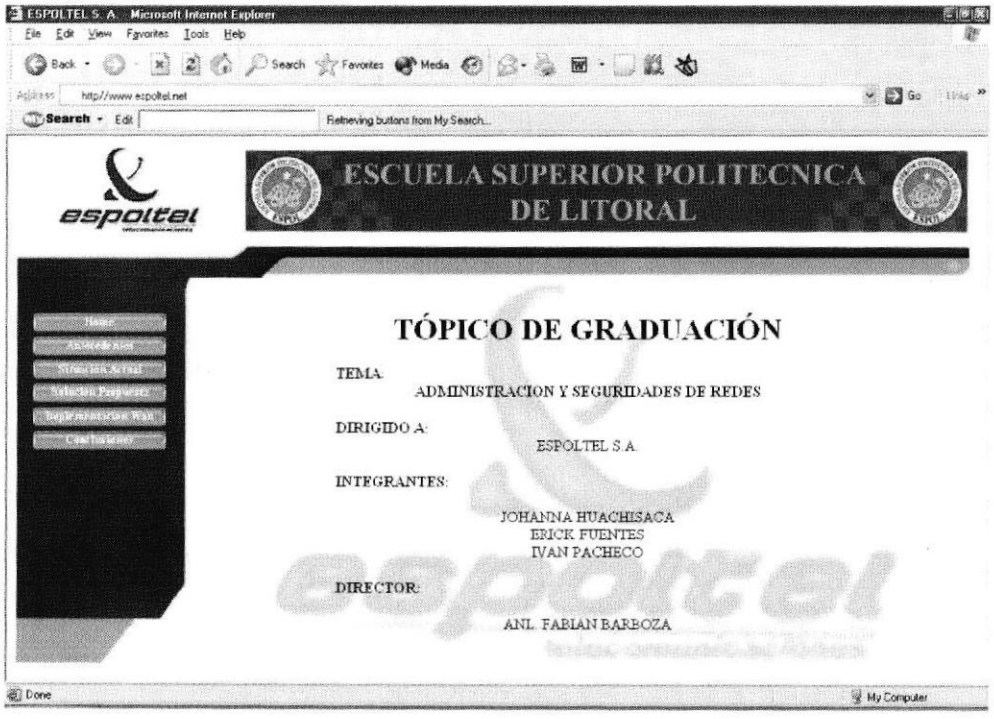


Figura 6.171 Pantalla de internet Explorer cargada la página de espoltel.net.

6. Caso contrario seguirá solicitando la clave.

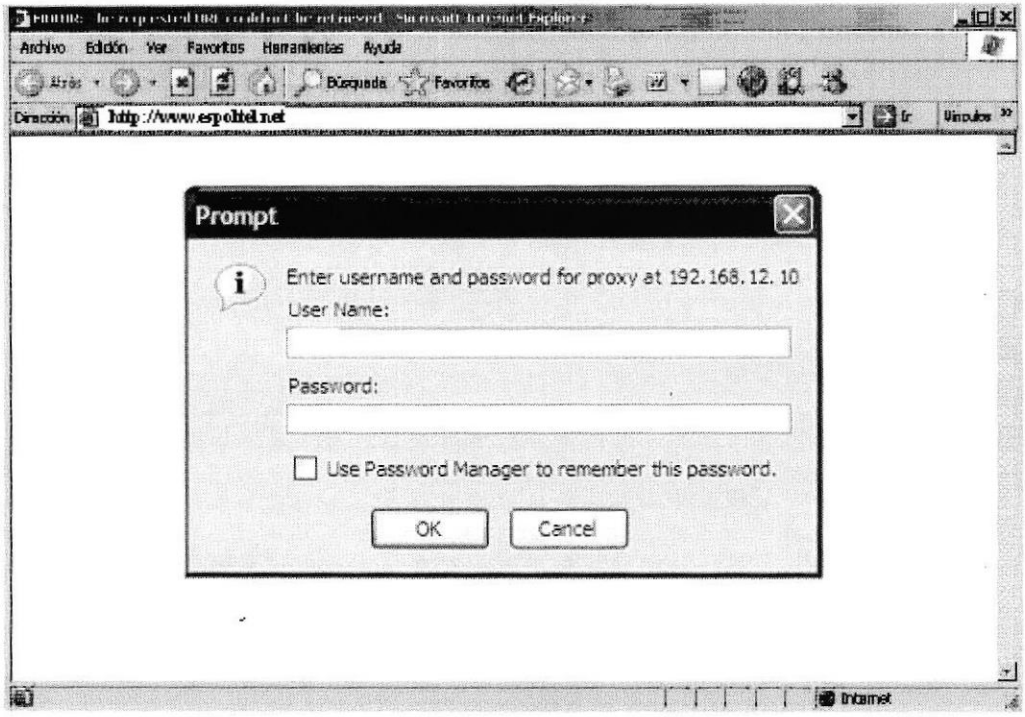


Figura 6.172 Pantalla de solicitud de usuario y contraseña.

6.7.6.11 DENEGAR PÁGINAS PROHIBIDAS

1. Editar y configurar el archivo squid.conf

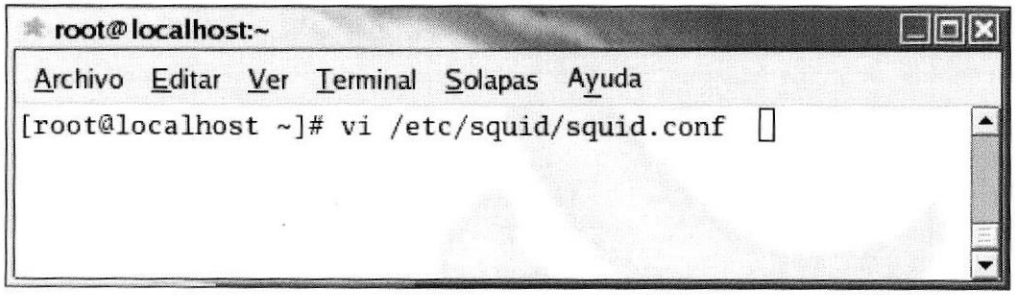


Figura 6.173 Pantalla de ingreso al archivo squid .conf

2. Incluir lista de control de acceso
   acl prohibidos src "/sitios/denegados"

3. Incluir regla de control de acceso
   http_access deny red prohibidos

4. Crear un archivo donde se alojarán los nombres de los sitios prohibidos en el directorio etc y editarlo.

```
[root@localhost /]# touch /etc/porno
[root@localhost /]# vi /etc/porno
```

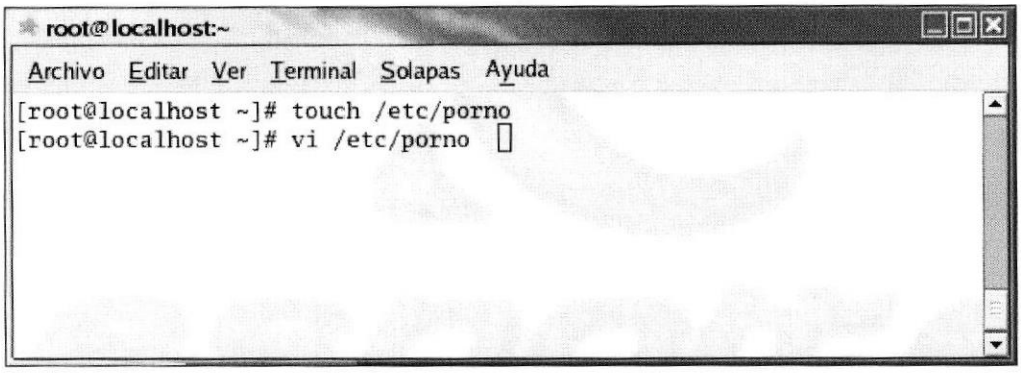


Figura 6.174 Pantalla de creación y edición del archivo porno.

5. Una vez editado el archivo registrar las direcciones de las páginas prohibidas

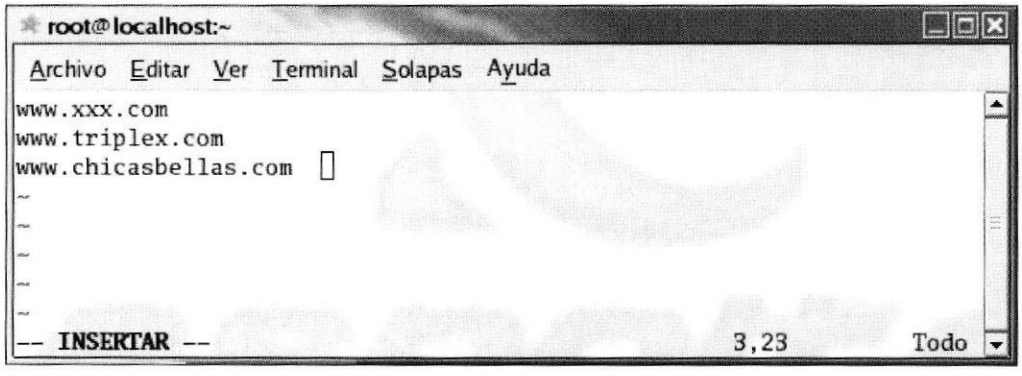


Figura 6.175 Pantalla de registro de las páginas prohibidas.

Salir con el comando :wq para guardar los cambios del archivo.

6. Reiniciar el servicio

[root@localhost /]# service squid restart

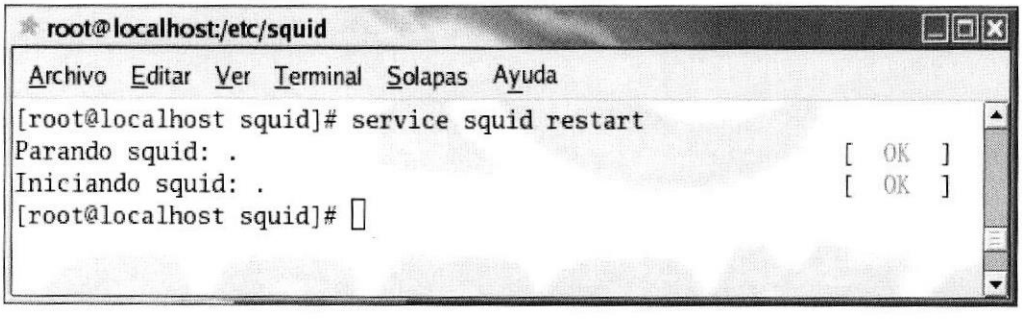


Figura 6.176 Pantalla de reiniciar el servicio del squid.

6.7.6.12 CONFIGURACIÓN EN EL CLIENTE WINDOWS PARA NO INGRESAR A PÁGINAS PROHIBIDAS.

1. Abrir Internet Explorer, elegir Menú / Herramientas / Opciones de Internet.

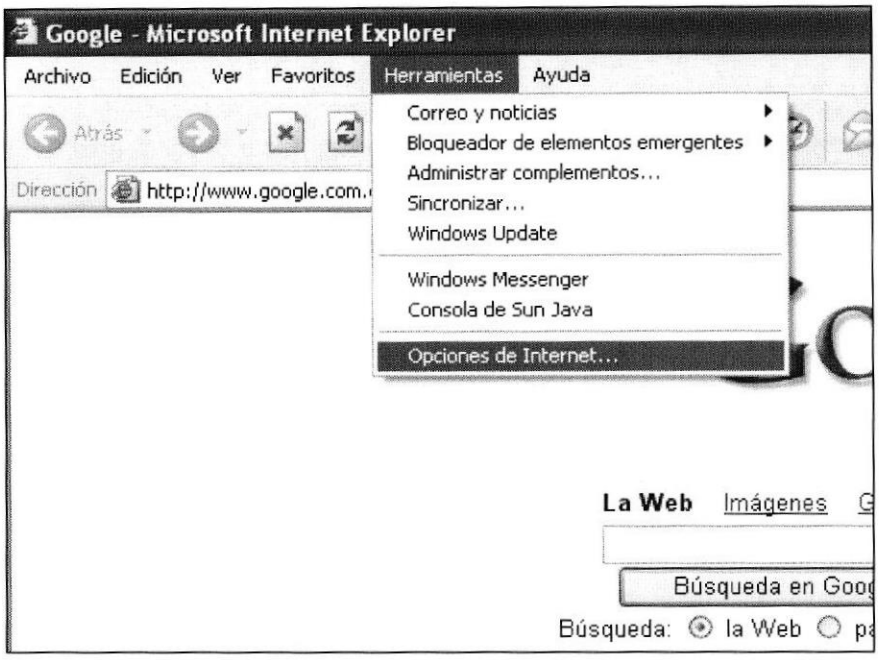


Figura 6.177 Pantalla de Internet Explorer.

2. De la pantalla que aparece elegir Conexiones / Configuración de Lan / Servidor Proxy.

Figura 6.178 Pantalla de opciones de internet.

3. **Dirección** 192.168.20.5 (IP del servidor) **Puerto** 8080.

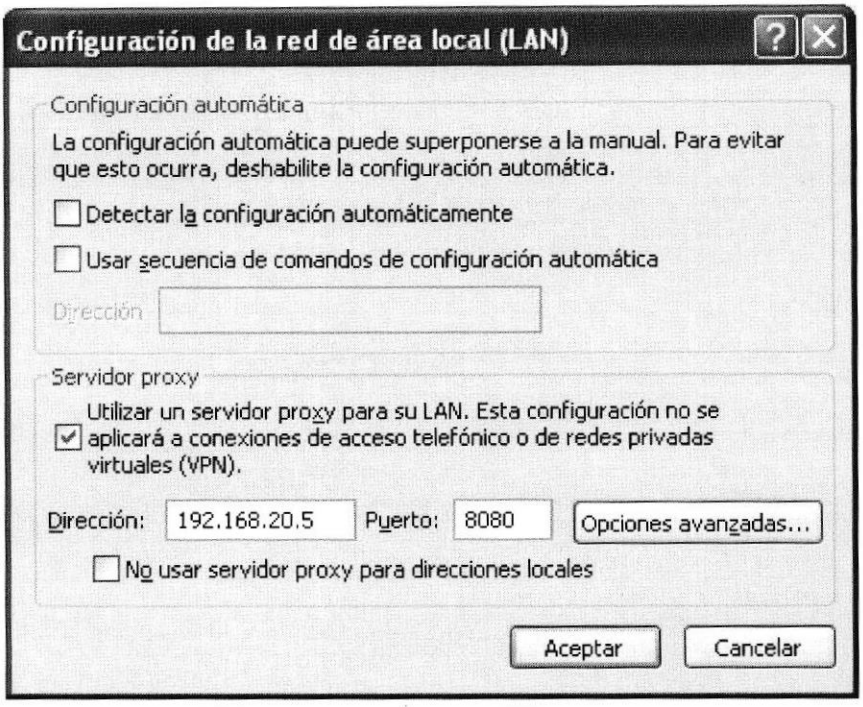


Figura 6.179 Pantalla de configuración de la red de área local.

4. Ingrese al sitio web mediante el navegador. Recordar que se debió haber asignado la dirección DNS en la máquina Windows.

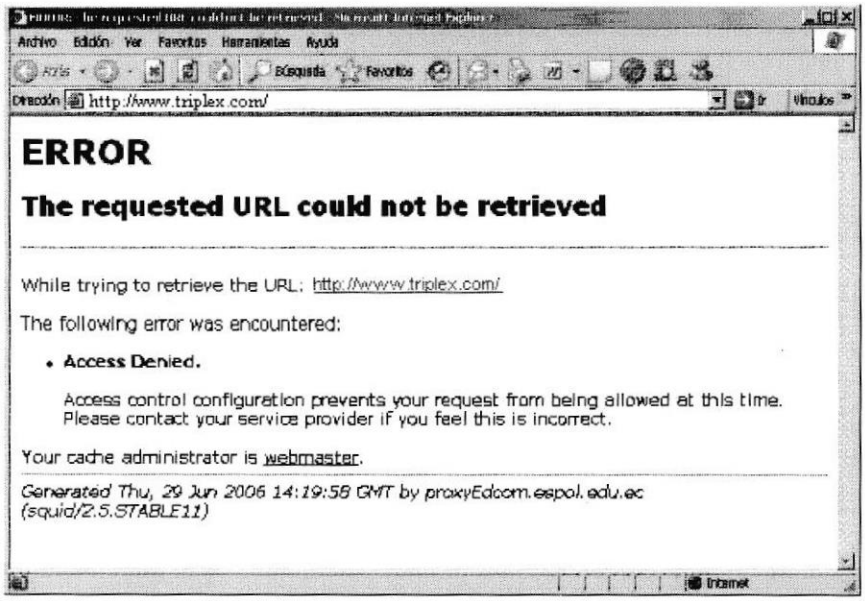


Figura 6.180 Pantalla de Internet con error al cargar páginas pornográficas.

En caso de reiniciar el servidor los servicios no se inician, por lo tanto deberá activarlos con el comando Setup.

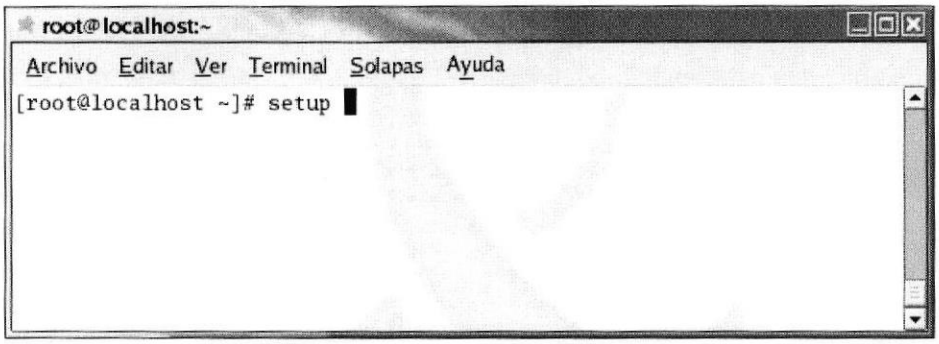


Figura 6.181 Pantalla de ingreso al setup.

A continuación aparecerá una pantalla, la misma que contiene el menú "Elija una Herramienta", donde deberá escoger la opción Servicios del Sistema y luego Ejecutar una Herramienta.

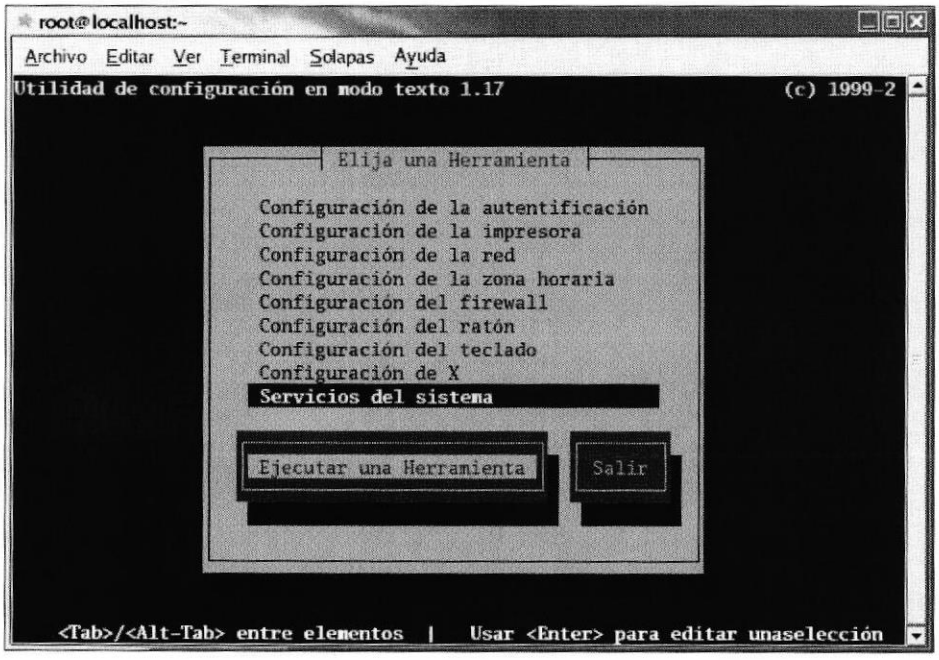


Figura 6.182 Pantalla de ingreso a Servicios del sistema.

Aparece la ventana de Servicios donde debe habilitar squid y elegir Ok.

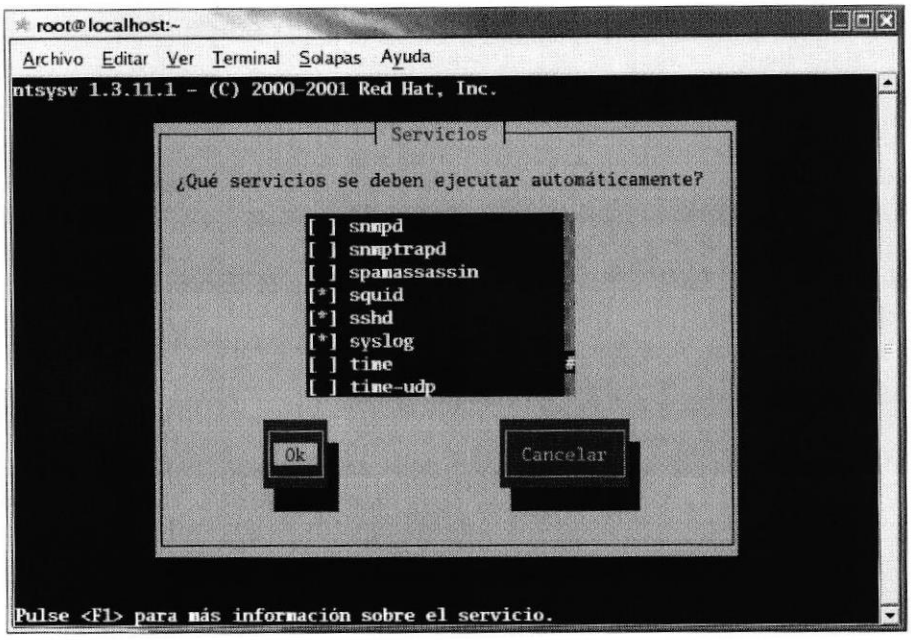


Figura 6.183 Pantalla de configuración del paquete squid.

6.7.7 CONFIGURACIÓN DEL SERVIDOR DE CORREO.

Sendmail es el agente de transporte de correo más común de Internet en los sistemas Linux.

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

Mail Server es un programa chico, diseñado para manejar los servicios POP3 y SMTP para pequeñas empresas o para uso individual.

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

SMTP, Simple Mail 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.

6.7.7.1 FUNCIONAMIENTO.

La utilización de sendmail como demonio en el sistema permite enviar y recibir correo SMTP. Para ello, sendmail se queda como proceso residente escuchando el puerto 25, admitiendo y realizando conexiones SMTP cuando sea necesario (es decir actúa como un agente de transporte de correo (MTA)).Cuando reciba una petición de conexión, creara un proceso hijo que se encargara de ello, mientras el proceso padre seguirá escuchando el puerto 25.

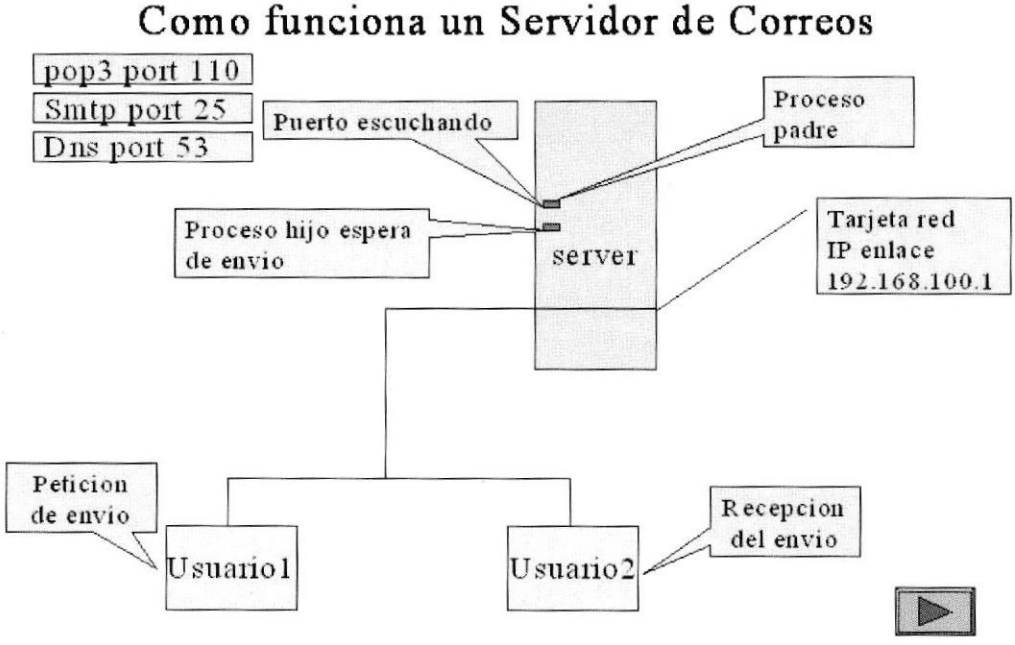


Figura 6.184 Esquema de Servidor de correo.

6.7.7.2 CARACTERÍSTICAS.

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

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

- Recogida de mails provenientes de un Mail Transport Agent (MTA).
- Elección de la estrategia de reparto de los mails.

- Si el mail es local en el sistema, enviara el mail al programa de reparto local de mails.
- Si el mail no es local, sendmail utilizara el DNS del sistema para determinar el host al que debe ser enviado el mail.

6.7.7.3 REQUERIMIENTOS.

- Un servidor con al menos 32 MB RAM y alguna distribución de Linux instalada.
- Deben de estar bien configurado los parámetros de red y un servidor de nombres -DNS-.
- Tener instalados los paquetes sendmail, sendmail-cf, m4, xinet que vienen incluidos en el CD de instalación o servidor FTP de actualizaciones para la versión de la distribución que usted utilice.

6.7.7.4 CONFIGURACIÓN DEL SERVIDOR DE CORREO.

1. Comprobar si esta instalado el servicio sendmail y dovecot si no instalarlo.

[root@localhost /]# rpm –qa sendmail
[root@localhost /]# rpm –qa dovecot

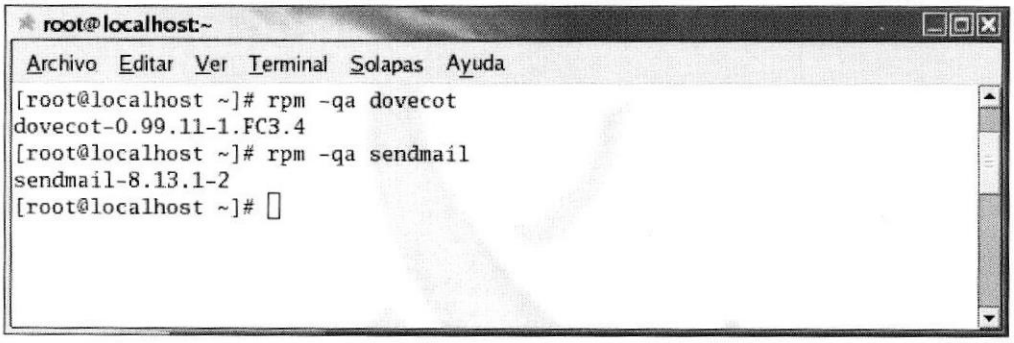


Figura 6.185 Pantalla de verificación de los paquetes del web Server..

3. Editar y configurar el archivo del servicio Dovecot

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

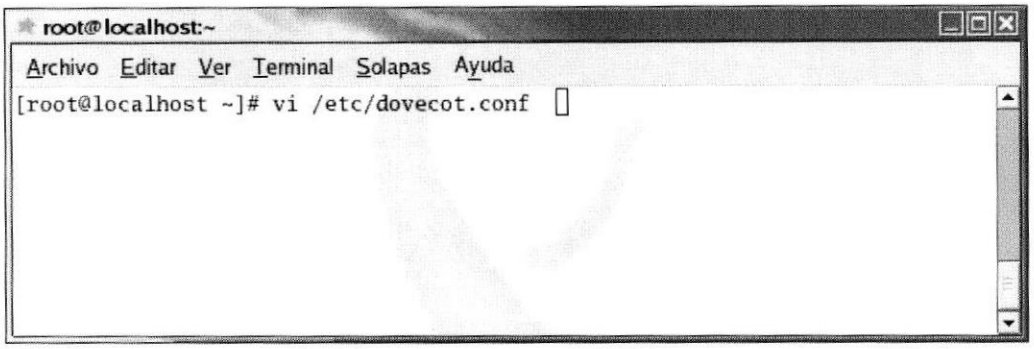


Figura 6.186 Pantalla para ingresar al archivo dovecot.conf.

Descomentar la línea, agregar los parámetros ;ya que este es el puerto por donde escucha dovecot. Salir con :wq para guardar los cambios.
protocols = imap imaps pop3

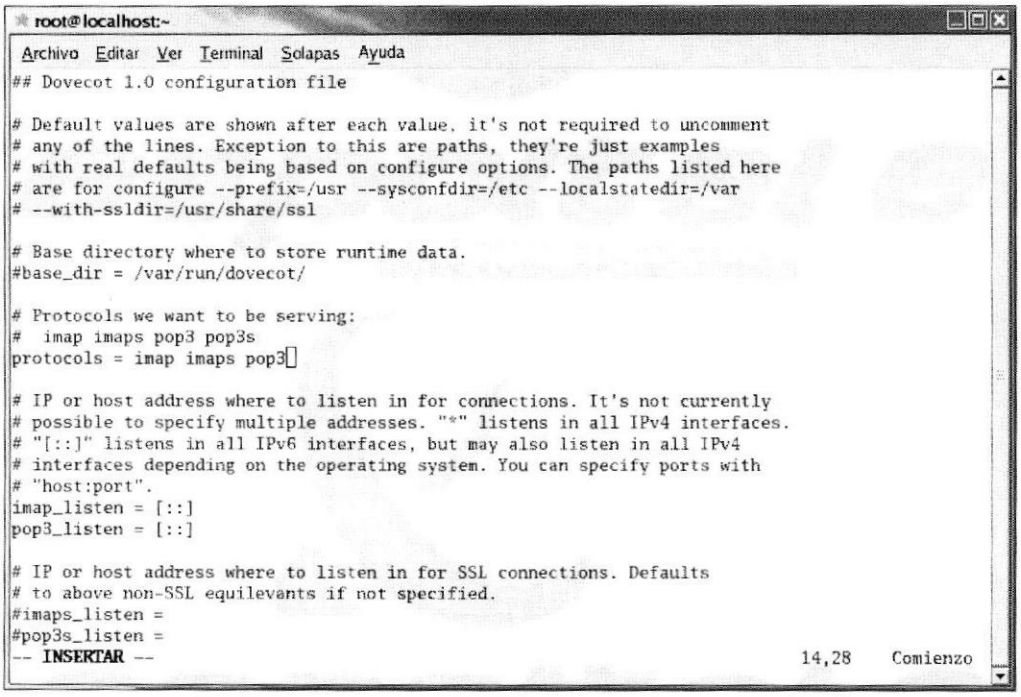


Figura 6.187 Pantalla de edición del dovecot.conf sección protocols.

4. Editar y configurar el archivo del servicio Sendmail

[root@localhost /etc/mail/]# vi /etc/mail/sendmail.cf

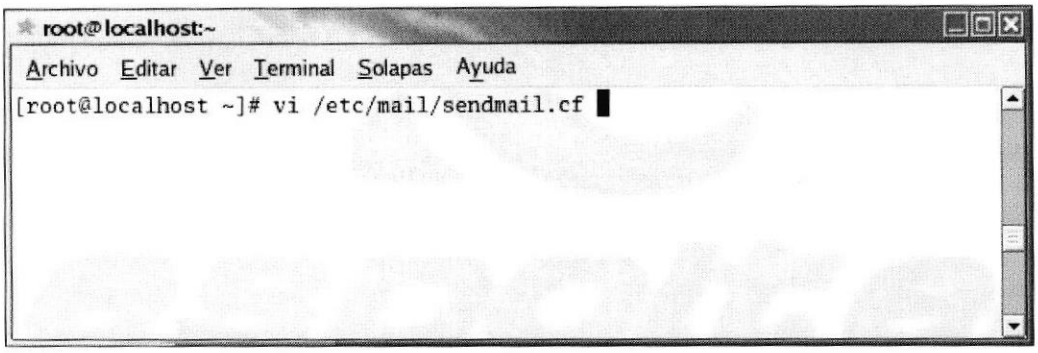


Figura 6.188 Pantalla para el ingreso al archivo sendamil.cf.

Agregar los parámetros y salir con: wq para guardar los cambios.

5. En Cwlocalhost, especificar el nombre del dominio con el que está trabajando.

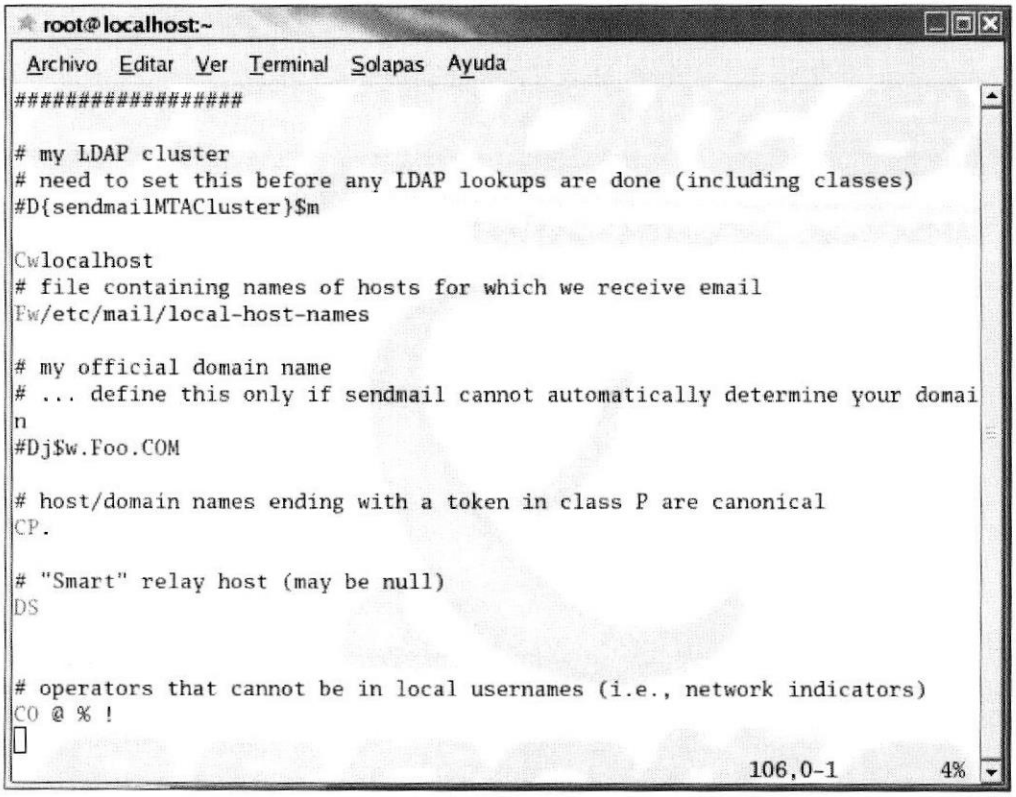


Figura 6.189 Pantalla para visualizar el Cw.

Cambiar el nombre del localhost por el nuevo del dominio, en este caso espoltel.

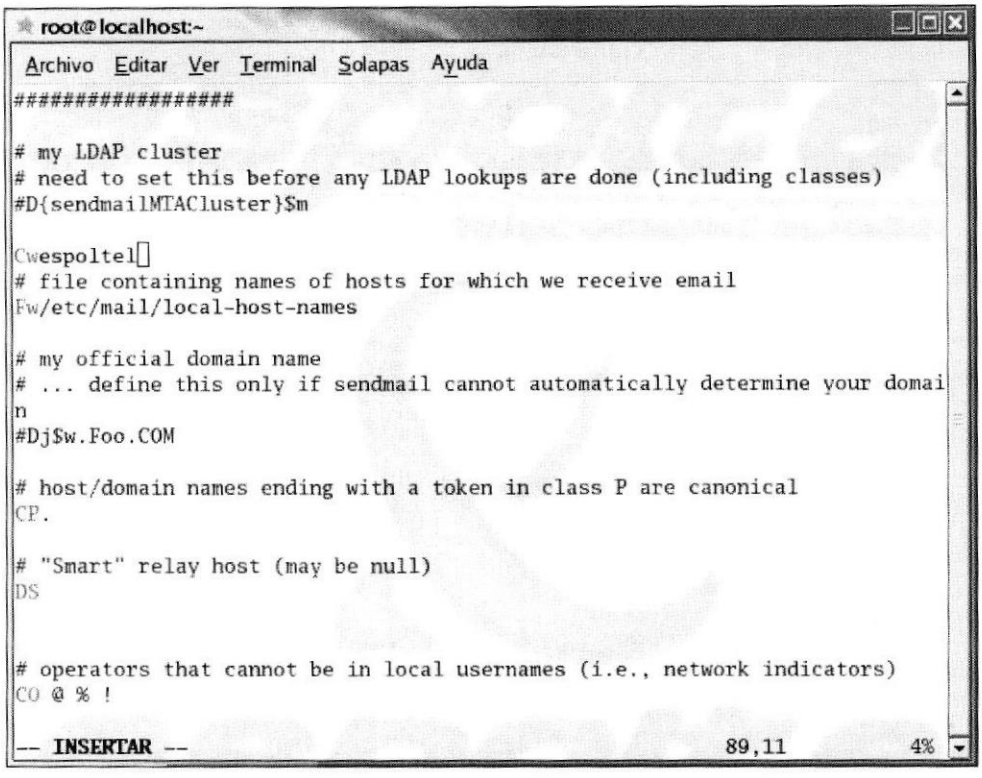


Figura 6.190 Pantalla donde cambia el localhost por espoltel en Cw.

6. Descomentar los cambios en los parámetros Demon Port Option y Client Port Options

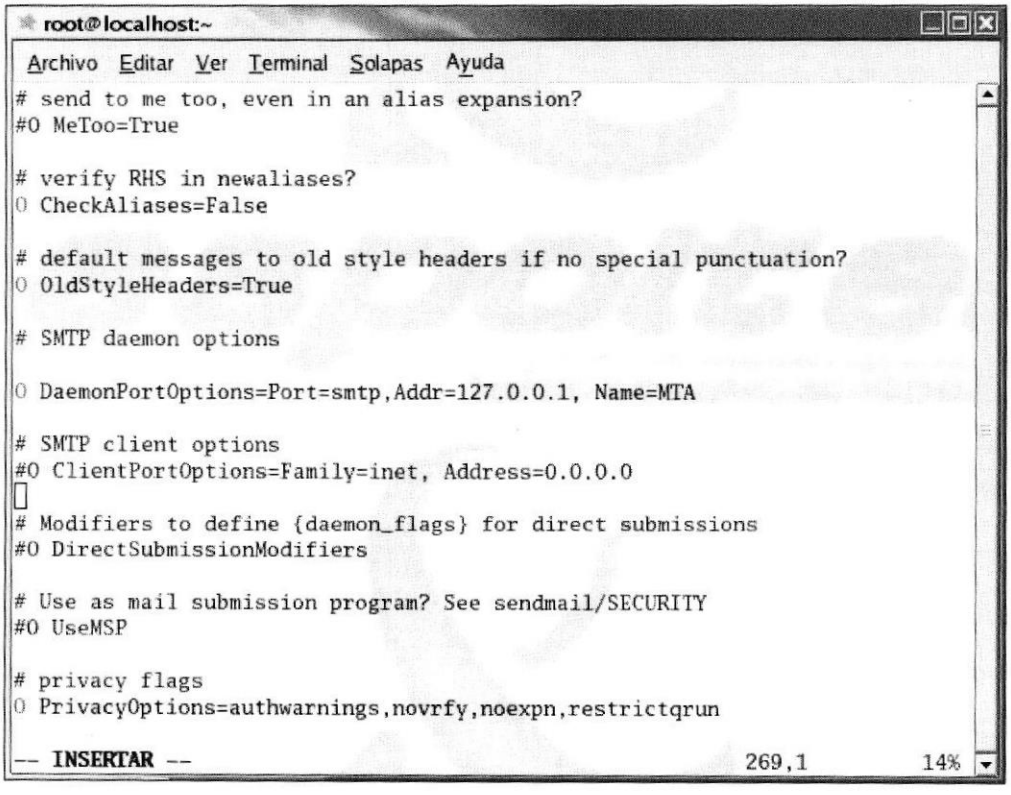


Figura 6.191 Pantalla de configuración del smtp daemon options y client options.

- # SMTP daemon options
  O DaemonPortOptions=Port=smtp,Addr=0.0.0.0, Name=MTA

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

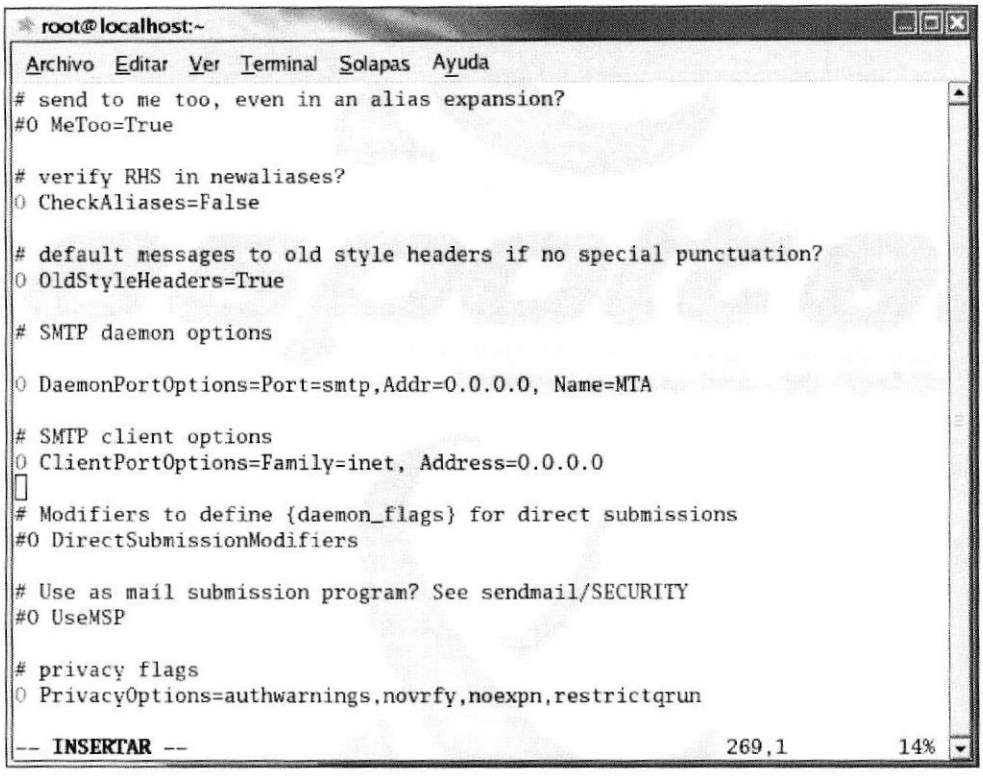


Figura 6.192 Pantalla de configuración del archivo sendmail.cf sección dominio y cliente.

7. Comprobar los puertos abiertos
   Netstat –an | more, o netstat –plan | more
   Deben estar escuchando los puertos 25 (SMTP) y el 110 (POP3)

8. Ingresar y editar el archivo hosts. Que se encuentra en el directorio etc.

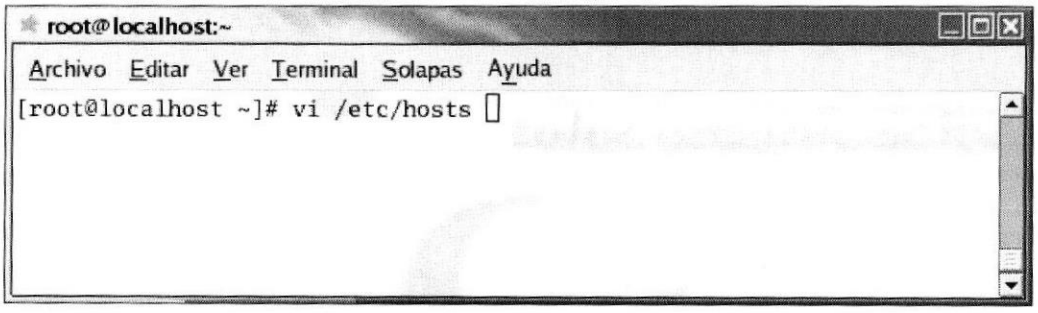


Figura 6.193 Pantalla para ingresar al archivo hosts.

9. A continuación aparecerá una ventana similar a la siguiente donde se debe colocar tanto en la dirección de la looback como en la ip del servidor de correo el nombre que se asignó antes en Cw.

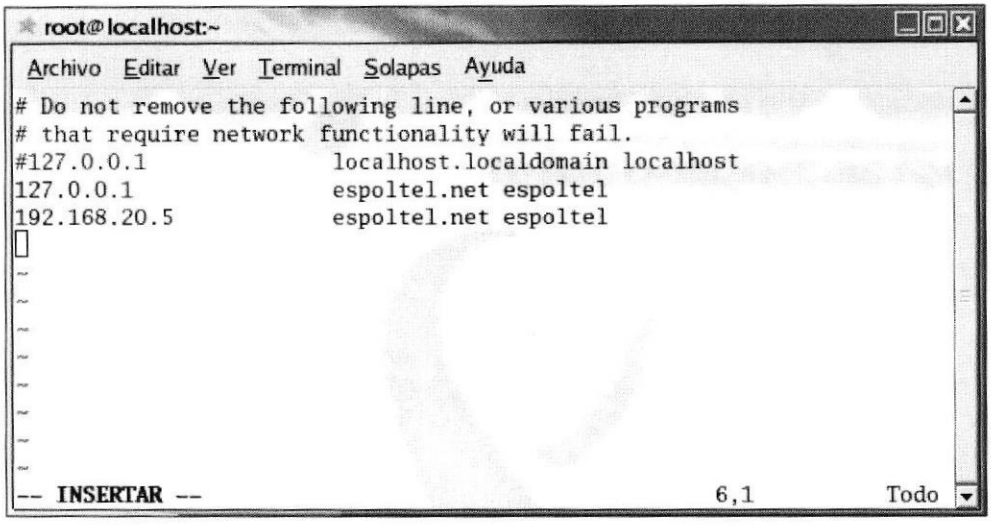


Figura 6.194 Pantalla de configuración del archivo host.

10. Ingresar y editar el archivo network que se encuentra en el directorio sysconfig.

[root@localhost /]# vi /etc/sysconfig/network

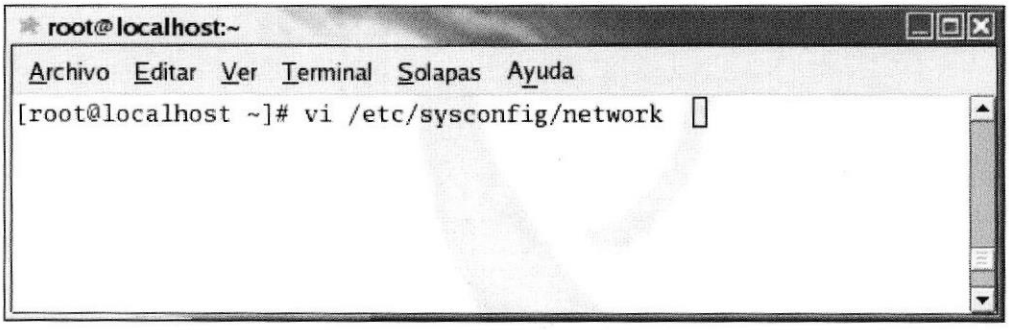


Figura 6.195 Pantalla de ingreso al archivo network

11. En el archivo editado se mostrará el parámetro HOSTNAME el mismo que deberá asignársele el nombre de espoltel.net por ser el nombre del dominio.

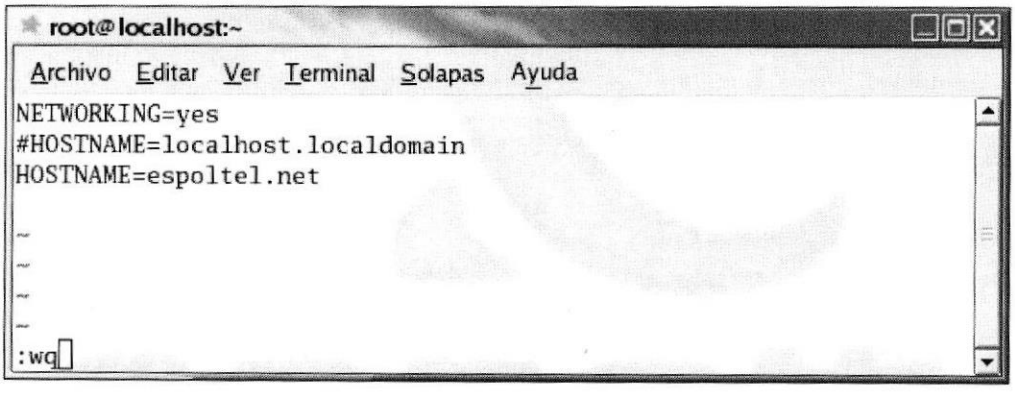


Figura 6.196 Pantalla de configuración del archivo network.

12. Reinicie los servicios del sendmail, dovecot y network.

[root@localhost /]# service network restart

[root@localhost /]# service dovecot restart

[root@localhost /]# service sendmail restart

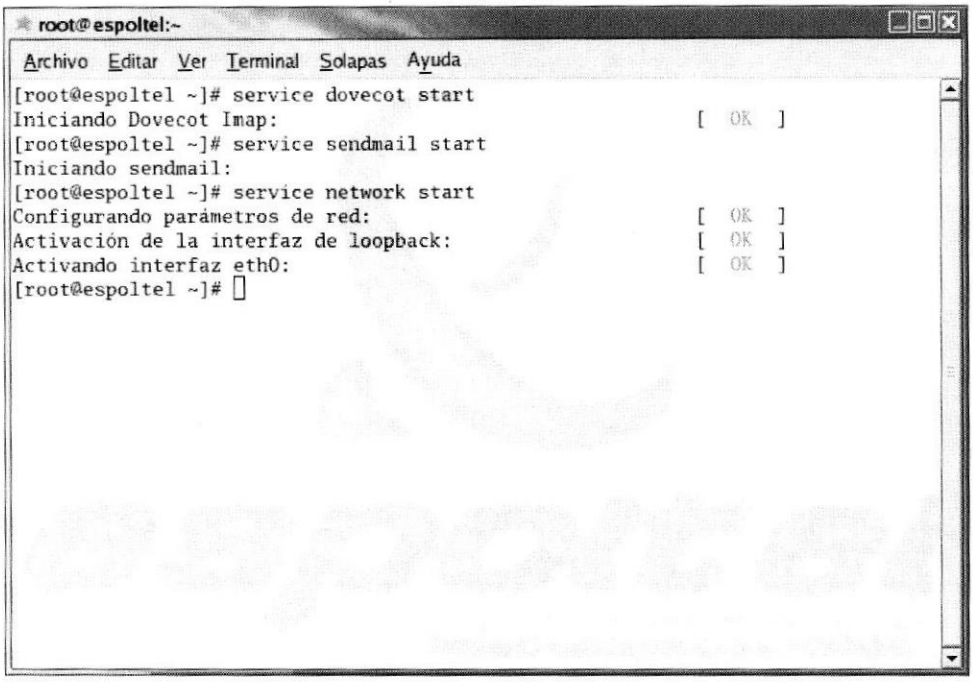


Figura 6.197 Pantalla de inicialización de los servicios del web Server.

A continuación se deberá reiniciar la pc con el fin de que se carguen las configuraciones realizadas.

6.7.7.5 CONFIGURACIÓN EN EL ENTORNO LINUX PARA COMUNICARSE CON WINDOWS.

- Para verificar se envía un mail al root

  [root@localhost /]# mail root@espoltel.net

  Subject: nombre_usuario a enviar el mail.
  Finalizar el mensaje con punto

  .

  Cc:/nombre_usuario2

- Para verificar un mail desde el usuario administrador

  [root@localhost /]# su -
  [root@localhost /]# mail

- Para verificar correos de otros usuarios

  [root@localhost /]# mail –u nombre_usuario

- Para cambiar de usuario

[root@localhost /]# su – nombre_usuario
[root@localhost /]# su – regresa al root pidiendo clave.

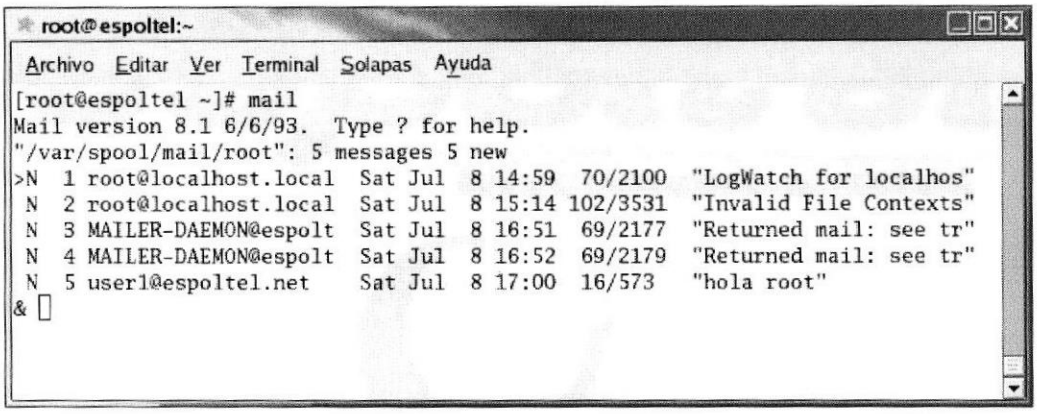


Figura 6.198 Pantalla que muestra la verificación de los correos recibidos al root.

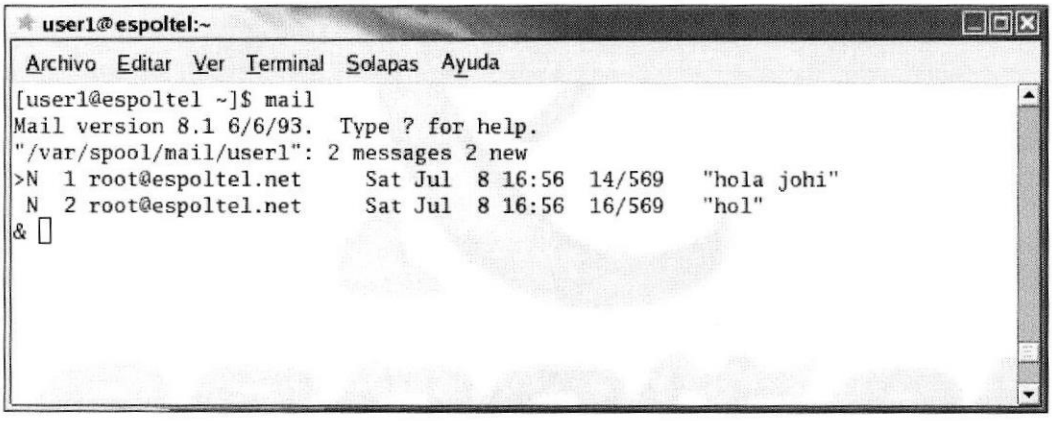


Figura 6.199 Pantalla que muestra la verificación de los correos recibidos al user1.

En caso de reiniciar el servidor los servicios no se inician, por lo tanto deberá activarlos con el comando Setup.

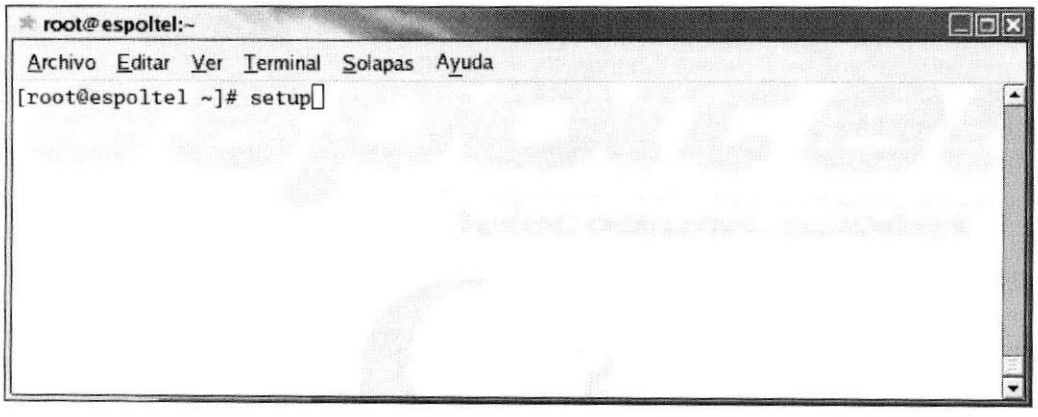


Figura 6.200 Pantalla de ingreso al setup.

A continuación aparecerá una pantalla, la misma que contiene el menú "Elija una Herramienta", donde debe escoger la opción Servicios del Sistema y luego Ejecutar una Herramienta.

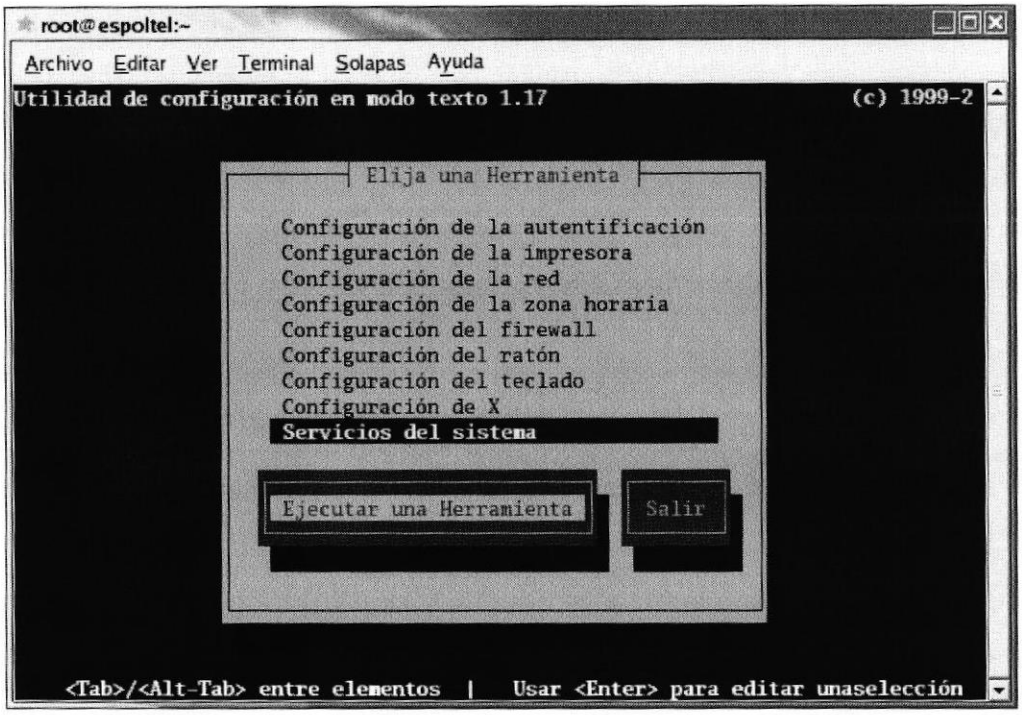


Figura 6.201 Pantalla de ingreso a los servicios del sistema.

Aparece la ventana de Servicios donde deberá habilitar Sendmail y Dovecot y elija Ok.

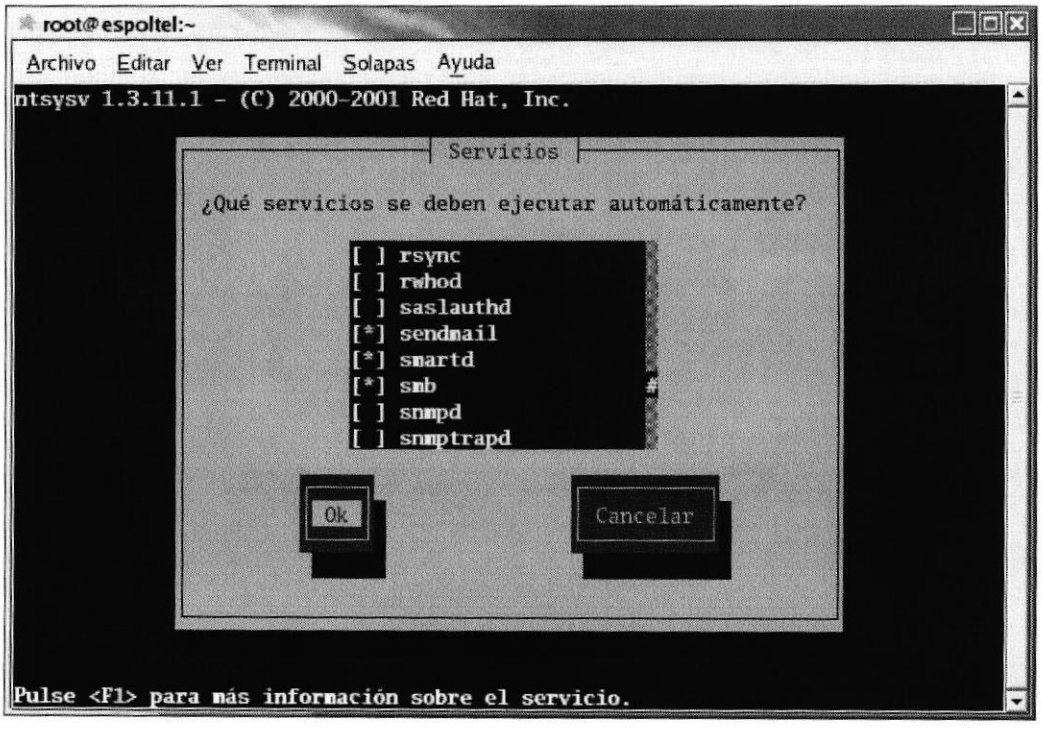


Figura 6.202 Pantalla de configuración del paquete sendmail.

A continuación se muestra la pantalla donde el paquete de dovecot se encuentra habilitado.

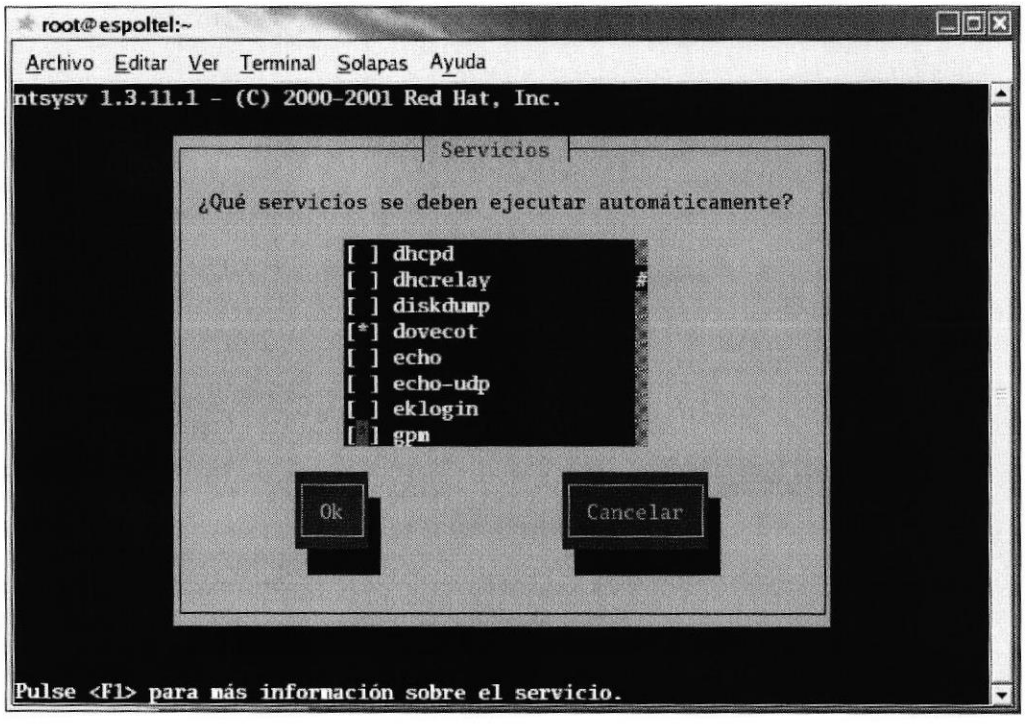


Figura 6.203 Pantalla de configuración del paquete dovecot.

6.7.7.7.1 CONFIGURANDO EL CLIENTE WINDOWS EN SERVIDOR DE CORREO

1. Se procede a configurar el Outlook Express, dando un clic en el botón inicio y eligiendo la opción de correo electrónico.

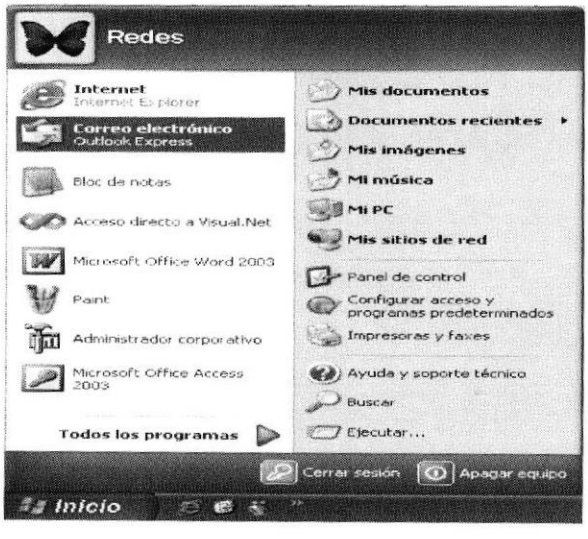


Figura 6.204 Pantalla de ingreso al Outlook Express.

2. Se abrirá la pantalla principal del Outlook Express en la cual se va a empezar la configuración, dando clic en herramientas y seleccionando cuentas de correos como se detalla a continuación.

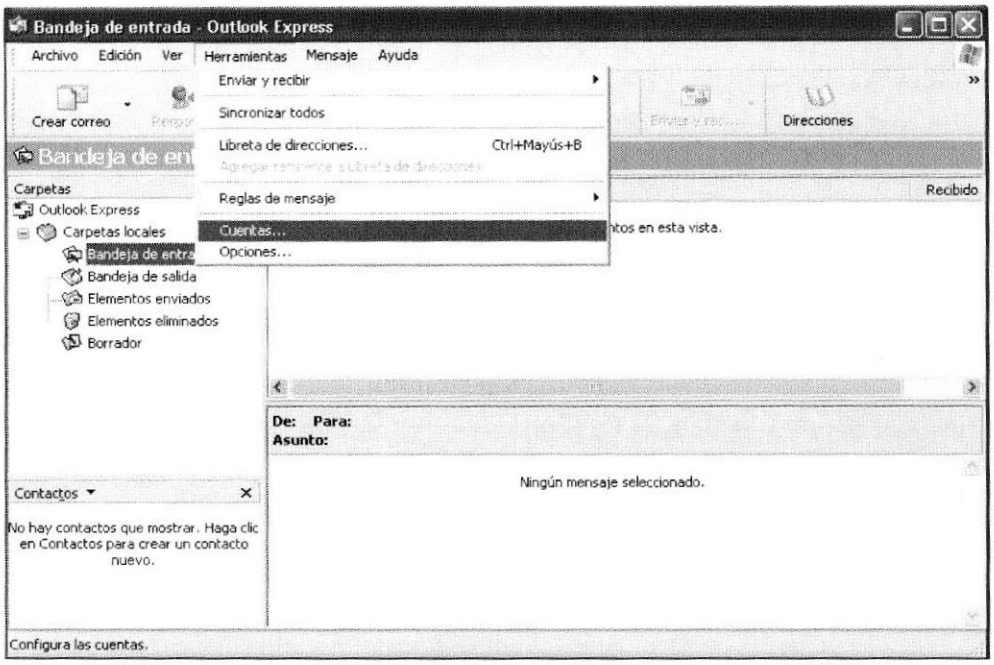


Figura 6.205 Pantalla de la Bandeja de entrada del Outlook Express.

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

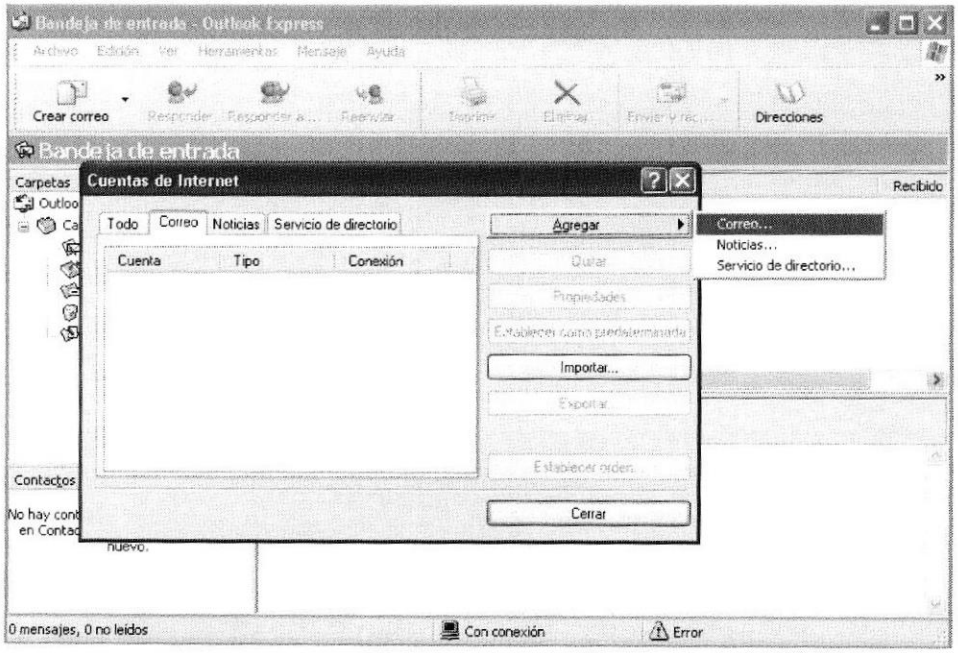


Figura 6.206 Pantalla de creación de cuentas.

4. Ingresar al Outlook Express y colocar un nombre para mostrar, clic en siguiente.

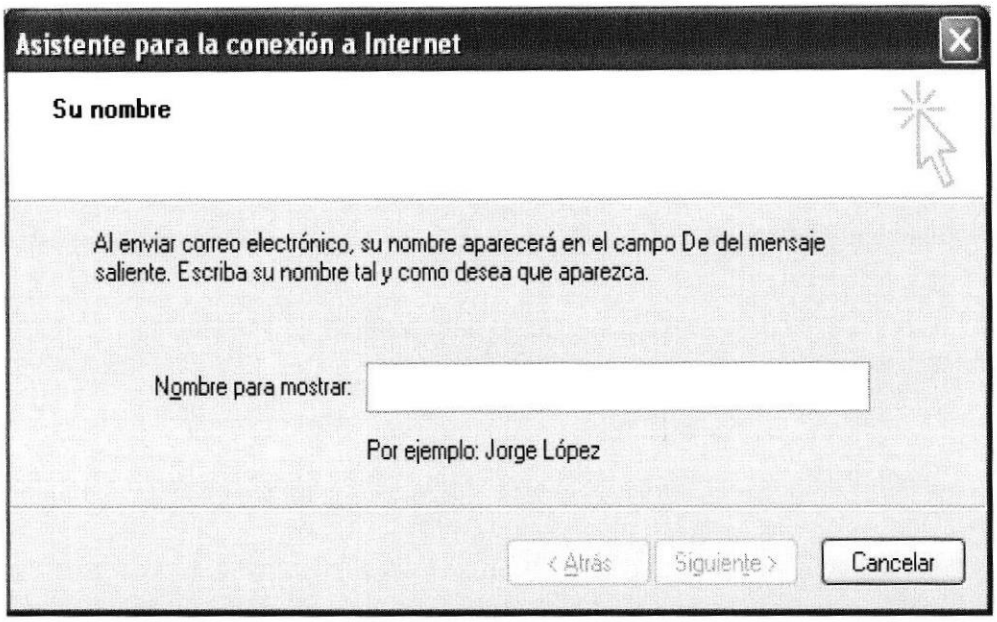


Figura 6.207 Pantalla de asistente para la conexión a internet solicitando nombre.

5. Colocar la dirección de correo asociado al usuario que se creó en Linux, clic en siguiente.

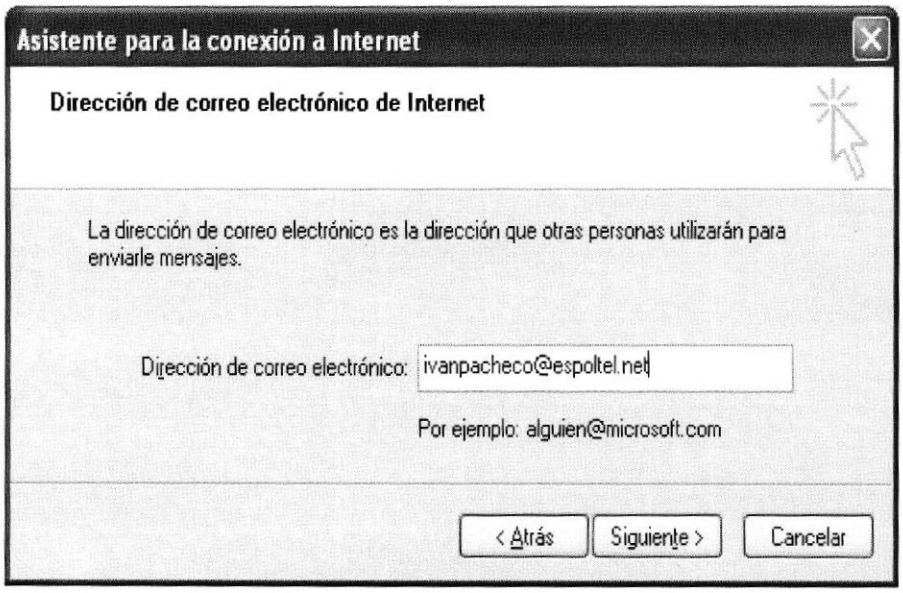


Figura 6.208 Pantalla del asistente para la conexión a internet solicitando dirección de correo.

6. Especificar el servidor de correo entrante (POP3) y el servidor de correo saliente (SMTP), en este caso los dos son la misma dirección del servidor Linux, clic en siguiente

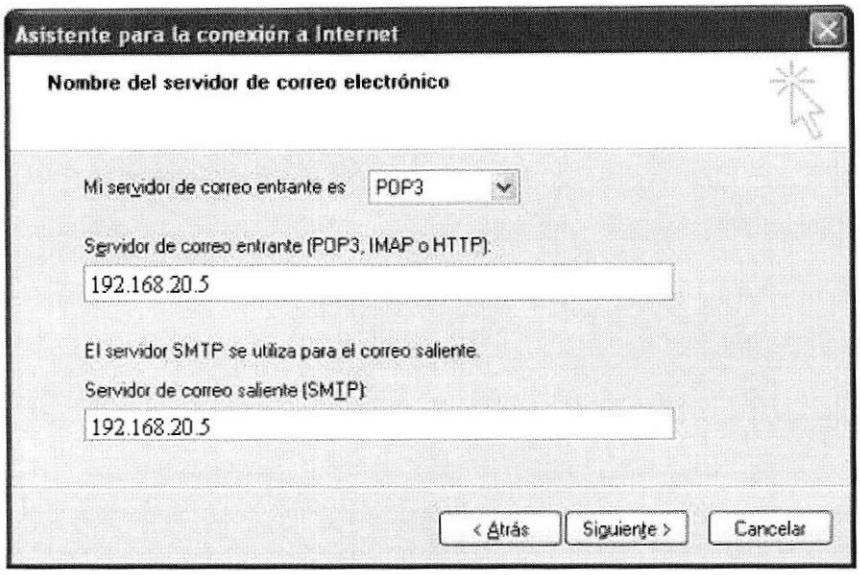


Figura 6.209 Pantalla del asistente para la conexión a internet solicitando servidor de correo.

7. Ingresar el nombre de usuario y contraseña proporcionado por el servidor Linux, clic en siguiente

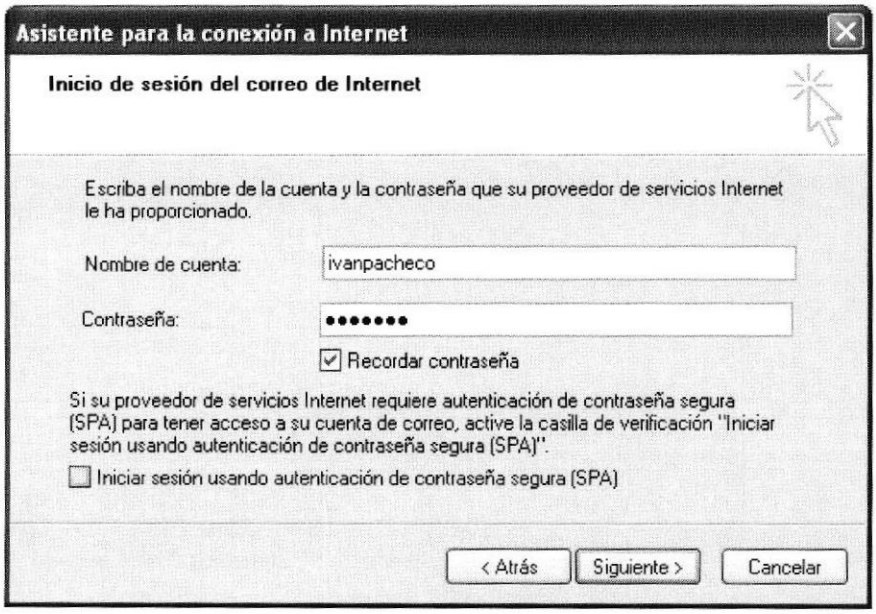


Figura 6.210 Pantalla del asistente para la conexión a internet solicitando nombre y clave.

8. Clic en finalizar para verificar que la información escrita anteriormente esta correcta.

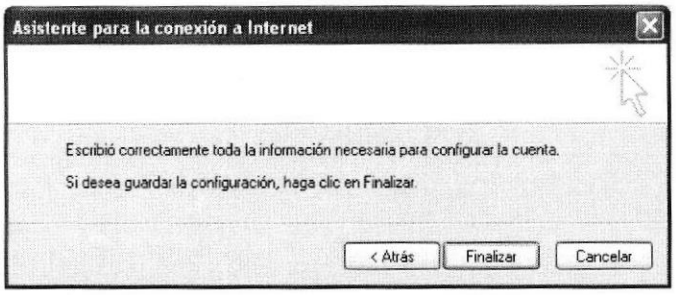


Figura 6.211 Pantalla para finalizar la creación de la cuenta.

9. 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 192.168.20.5 .

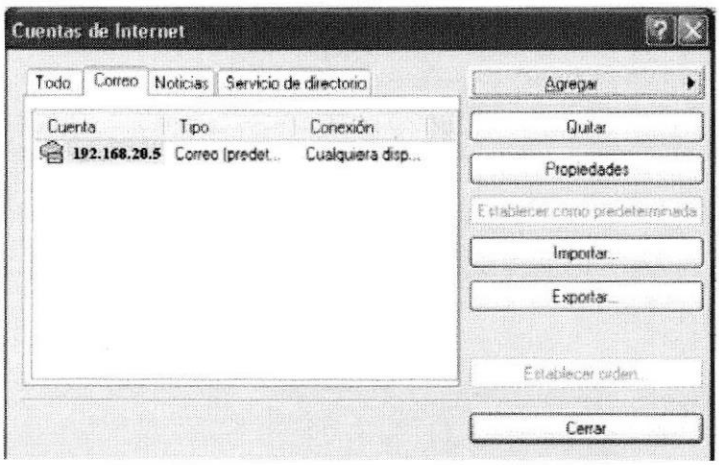


Figura 6.212 Pantalla de cuentas de internet.

Ahora podrá enviar y recibir mensajes de correos de los usuarios creados en el servidor Linux.

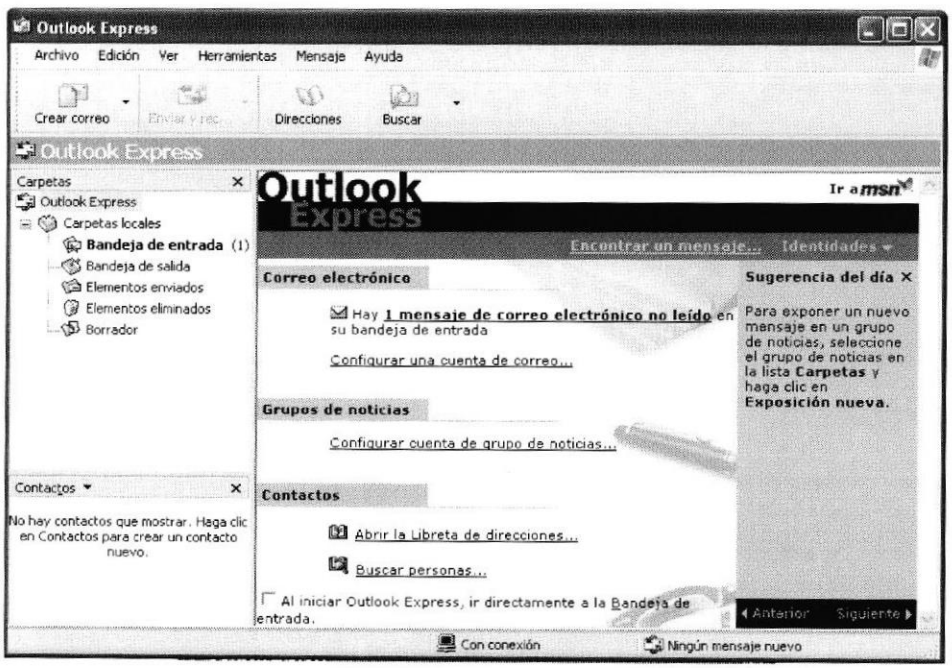


Figura 6.213 Pantalla de entrada y salida del correo.

Para realizar la prueba de envío y recepción de mensajes de correo en el Outlook Express ingrese a la opción enviar y recibir mensajes en la barra de herramientas y donde saldrá una pantalla que muestra la búsqueda de los mensajes que son enviados y recibidos.

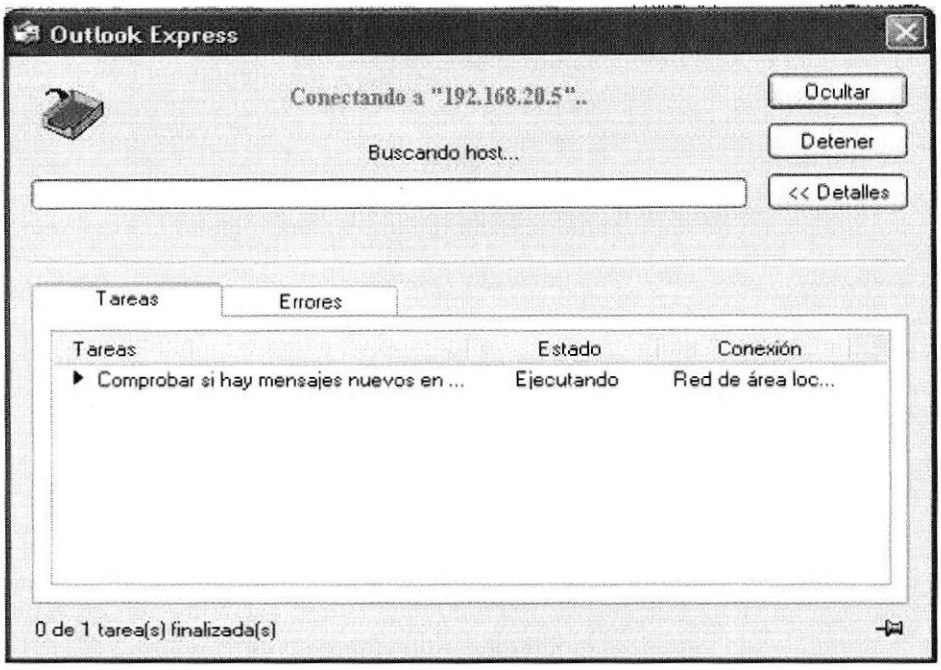


Figura 6.214 Pantalla de Conectado al servidor Linux.

Luego verificar en la bandeja de Outlook si se ha recibido correos de alguna otra cuenta.

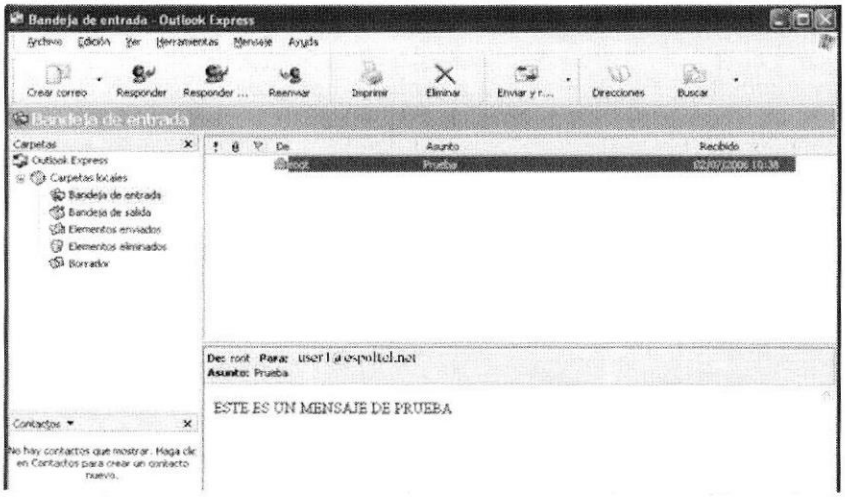


Figura 6.215 Revisando bandeja de entrada.

Verificar cuenta de correo, enviando un correo a alguna cuenta existente.

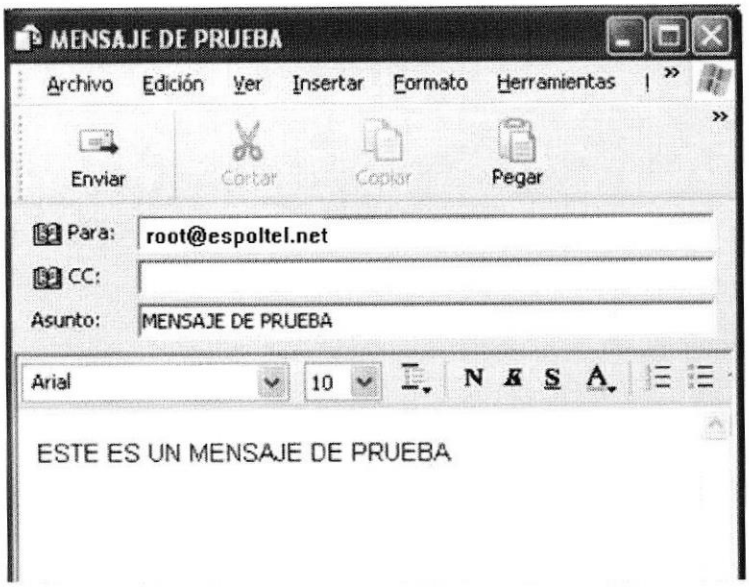


Figura 6.216 Enviando correo a otra cuenta.

Si el correo se ha enviado exitosamente deberá aparecer en la opción "**Elementos Enviados**" de Microsoft Outlook

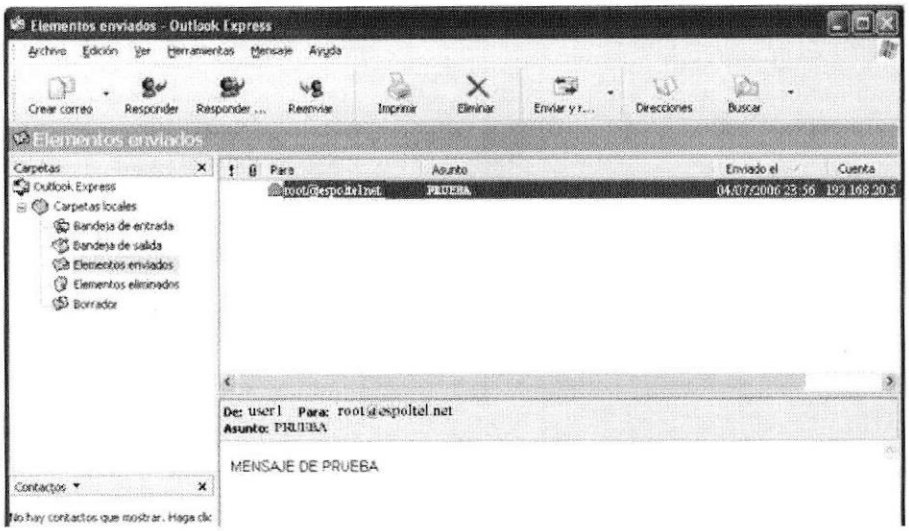


Figura 6.217 Verificar elementos enviados

6.7.8 CONFIGURACIÓN DE SEGURIDADES (FIREWALL)

Conocido también como muro de fuego, éste impedirá el acceso no autorizado a sus servicios e información, y/o controlar el acceso de los usuarios de su red a Internet.

Es la interfaz entre el ordenador y la red. Determina que recursos de su equipo están accesibles para los usuarios remotos de la red. Un Firewall bien configurado puede aumentar significativamente la seguridad de su sistema.

Existen 3 tipos de reglas:

INPUT = ENTRADA AL SERVIDOR
OUTPUT = SERVIDOR HACIA FUERA
FORDWARD = REDIRECCIONAR

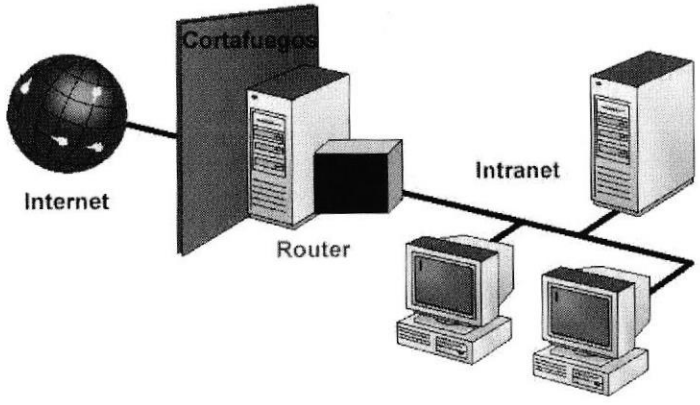


Figura 6.187 Esquema del Firewall

6.7.8.1 CARACTERÍSTICAS

- Disposición de elementos que controlan los accesos a ciertas partes de una red.
- Se accede por un único punto muy controlado.
- Previene de ataques por otras zonas.
- Restringe las salidas a Internet por un único punto muy controlado.
- Semejante a un foso y un puente en un castillo medieval

6.7.8.2 DESHABILITAR EL FIREWALL

1. Para deshabilitar el firewall debe digitar el comando setup.

[root@localhost /]#**setup**

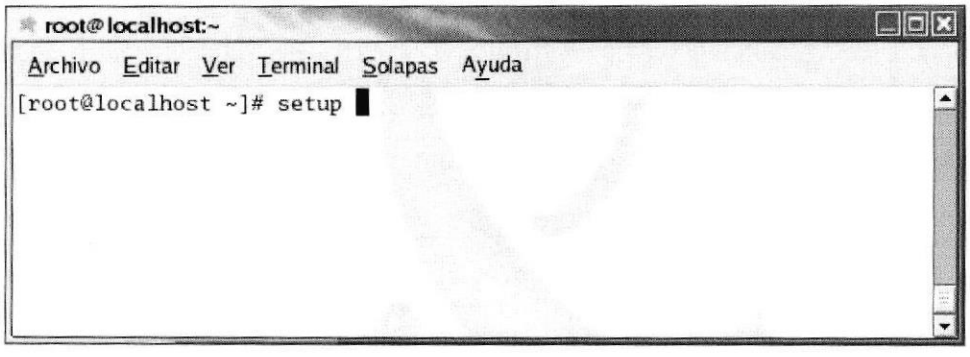


Figura 6.218 Pantalla para ingresar al setup.

2. De la ventana que aparece elegir la opción Configuración del firewall y dar clic en el botón Ejecutar una Herramienta.

Figura 6.219 Pantalla para elegir Herramienta de Configuración del Firewall.

3. Buscar en el listado que muestra la ventana la opción firewall, ([*] firewall), a continuación se visualizará una pantalla para proceder a deshabilitar. Una vez realizado el cambio dar clic en Aceptar.

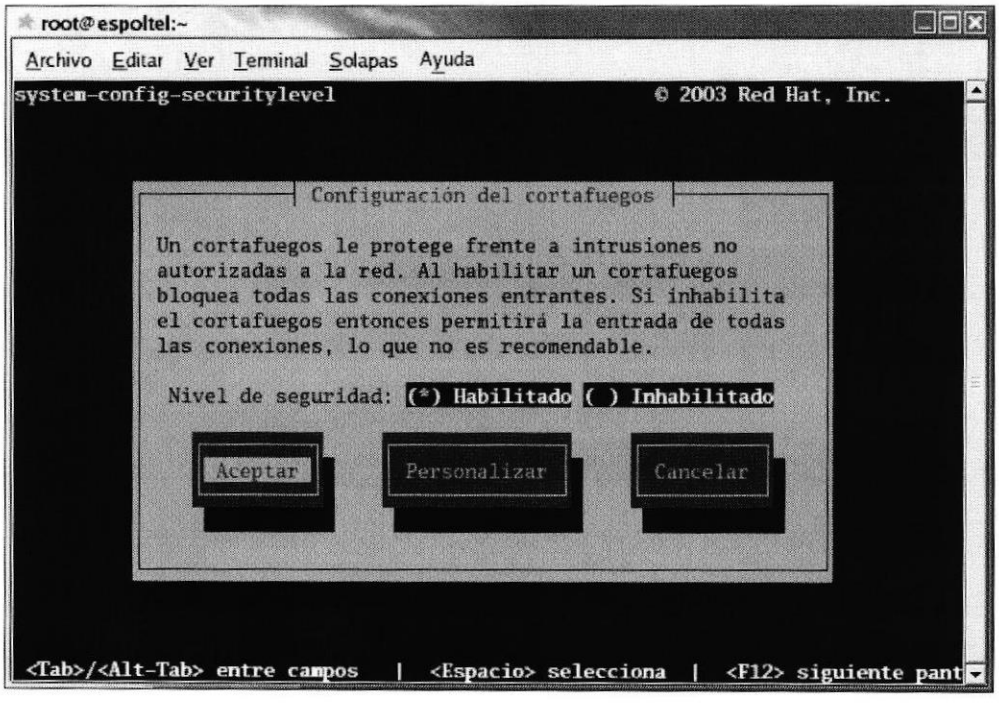


Figura 6.220 Pantalla para elegir la configuración del Firewall.

4. Al volver al menú principal dé clic en **Salir**

6.7.8.3 CONFIGURACIÓN DE FIREWALL.

1. Bloquear PING

iptables -A INPUT -s 192.168.20.0/24 -d 192.168.20.5/24 -p icmp -j DROP
iptables -A INPUT -s 192.168.20.0/24 -d 192.168.20.5/24 -p icmp -j REJECT

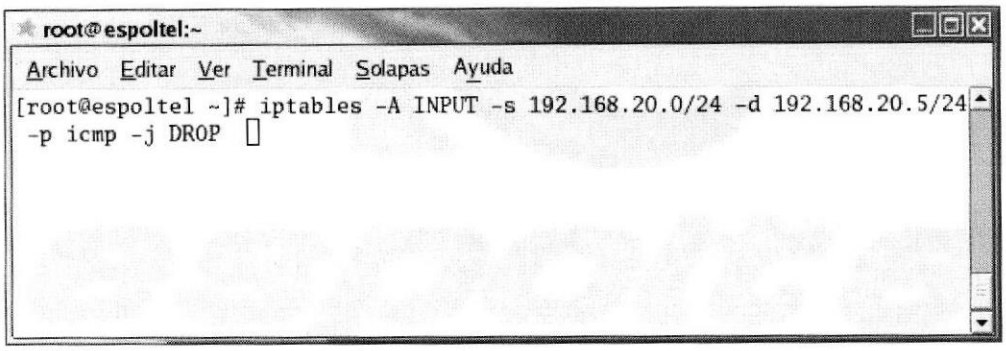


Figura 6.221 Pantalla configuración de un firewall lógico para bloquear ping.

2. Bloquear TELNET

iptables -A INPUT -s 192.168.20.0/24 -d 192.168.20.5/24 –p tcp --dport 23 - j DROP

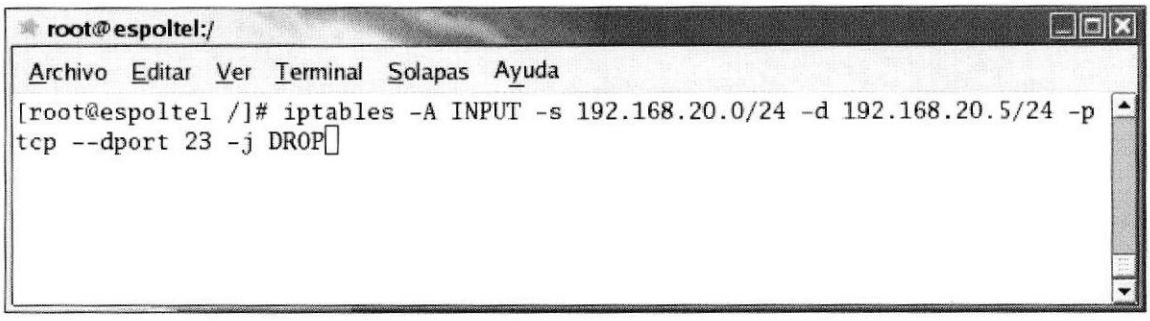


Figura 6.222 Pantalla configuración de un firewall lógico para bloquear telnet.

3. Bloquear FTP

iptables –A INPUT –s 192.168.20.0/24 –d 192.168.20.5/24 –p tcp --dport 21 –j DROP

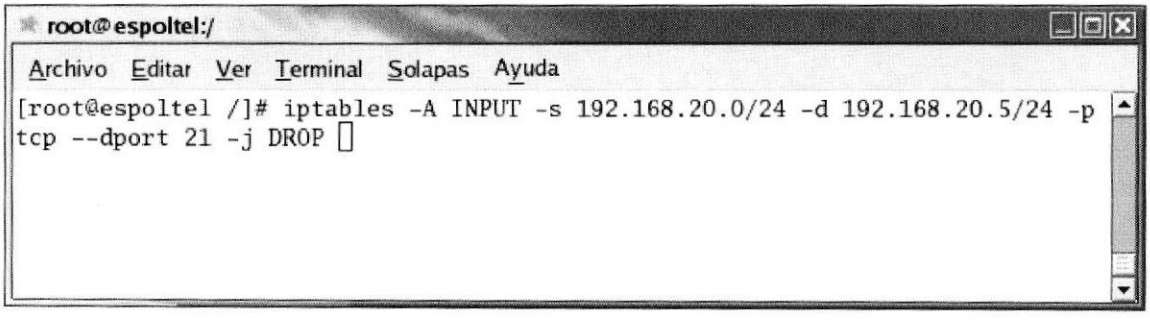


Figura 6.223 Pantalla configuración de un firewall lógico par bloquear ftp.

4. Verificar las iptables creadas.

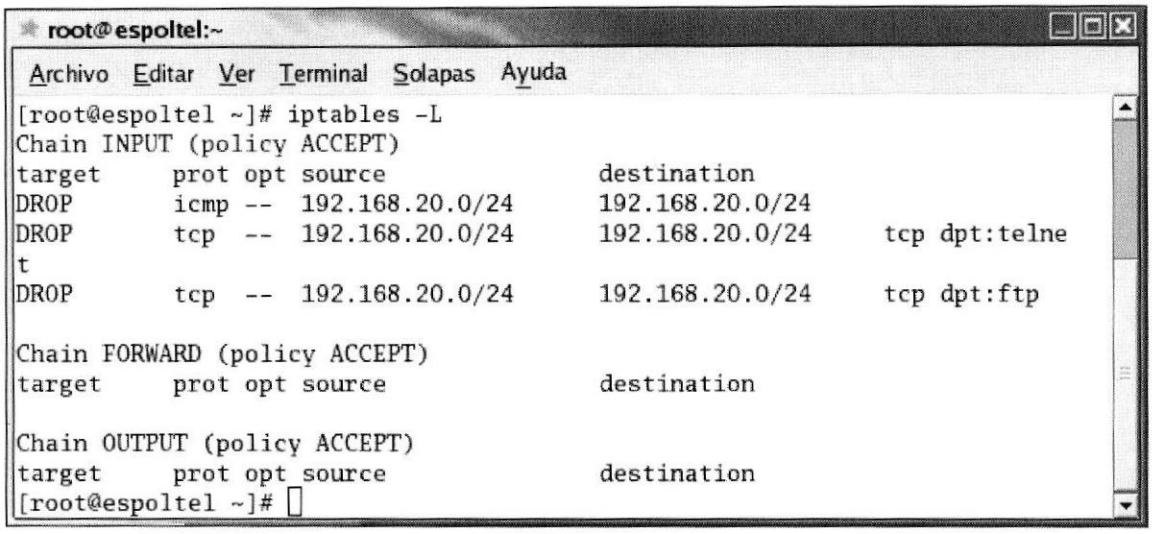


Figura 6.224 Verificación de iptables

VERIFICACIÓN DE PING.

Si la iptables creada esta bien configurada saldrá la siguiente pantalla.

Figura 6.225 Respuesta afirmativa de ping.

Si la respuesta es negativa, la pantalla a salir sera:

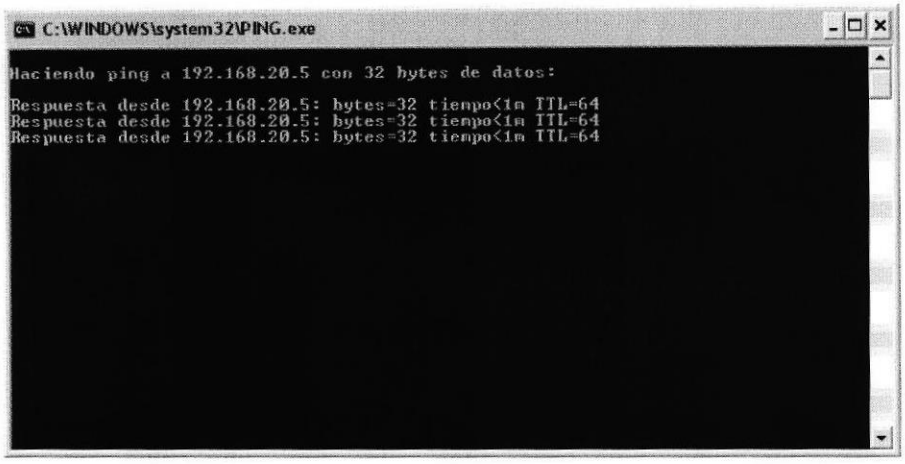


Figura 6.226 Respuesta negativa de ping.

VERIFICACIÓN DE TELNET.

Si la iptable de bloqueo de telnet está bien configurada la pantalla a mostrarse será:

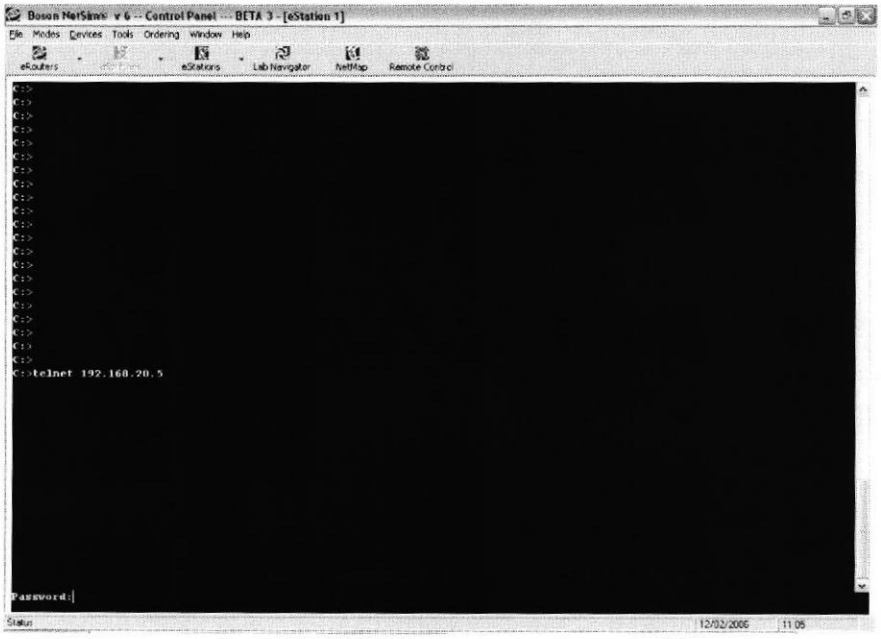


Figura 6.227 Haciendo telnet.

Aparecerá luego un mensaje indicando que n se ha podido realizar la conexión.

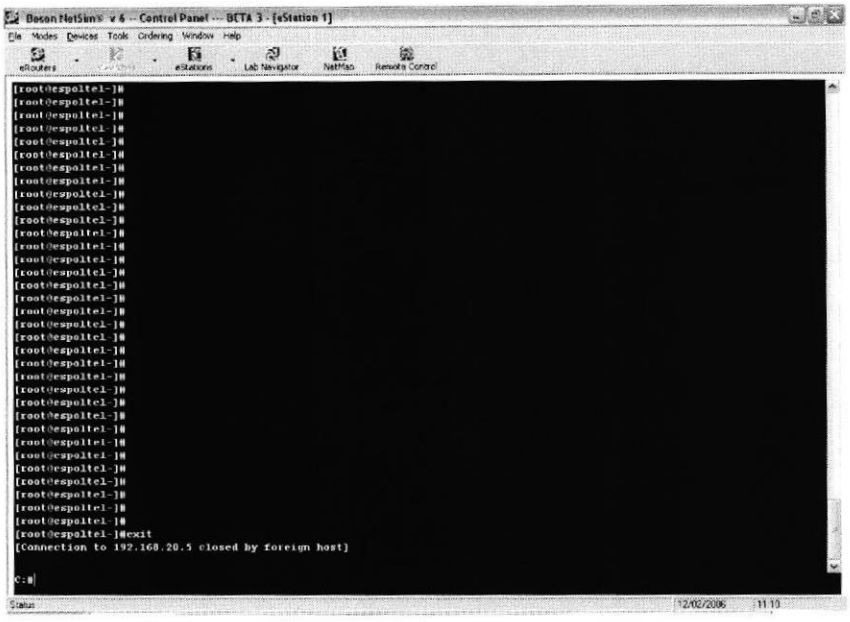


Figura 6.228 Mensaje de no conexión.

6.7.9 CONFIGURACIÓN DEL SERVIDOR DHCP.

El Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un protocolo desarrollado para asignar direcciones IP a los clientes que lo soliciten, es un estándar de TCP/IP diseñado para reducir la complejidad de la administración de configuraciones de direcciones mediante la utilización de un equipo central para administrar centralmente direcciones IP así como otros detalles de configuración de la red. Windows 2000 Server proporciona el servicio DHCP, que habilita al equipo servidor para funcionar como servidor DHCP y que permite configurar equipos clientes habilitados para DHCP en la red como se describe en el estándar actual de diseño de DHCP.

Protocolo empleado para que los host (clientes) puedan obtener configuración dinámica a través de un servidor.

Asigna direcciones IP a las computadoras de los usuarios cuando estas arrancan.

6.7.9.1 FUNCIONAMIENTO.

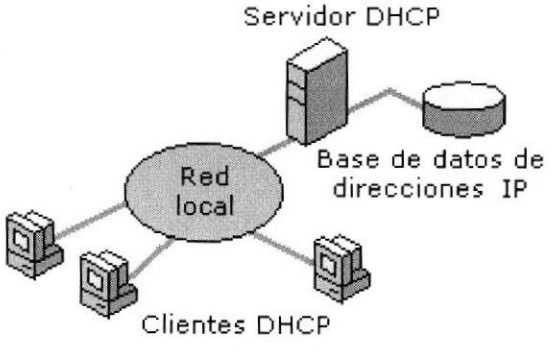


Figura 6.229 Esquema de funcionamiento de un Servidor DHCP.

6.7.9.2 CARATERÍSTICAS.

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

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

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

6.7.9.3 REQUERIMIENTOS.

- Tener un servidor linux y un computador con Windows.
- DHCP
- UDHCPD

6.7.9.4 CONFIGURACIÓN DE DHCP.

1. Verificar si el paquete del dhcp está instalado.

root@localhost /]# rpm -q dhcp

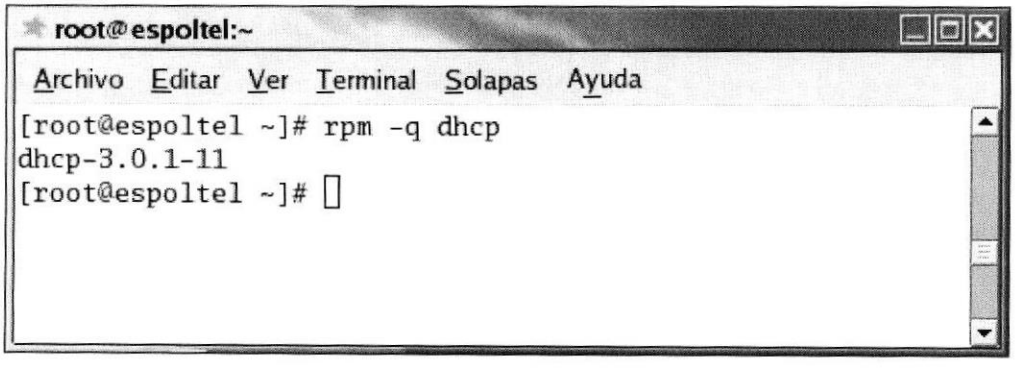


Figura 6.230 Pantalla para verificar el paquete de dhcp.

2. Crear el archivo dhcp.conf de la siguiente manera

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

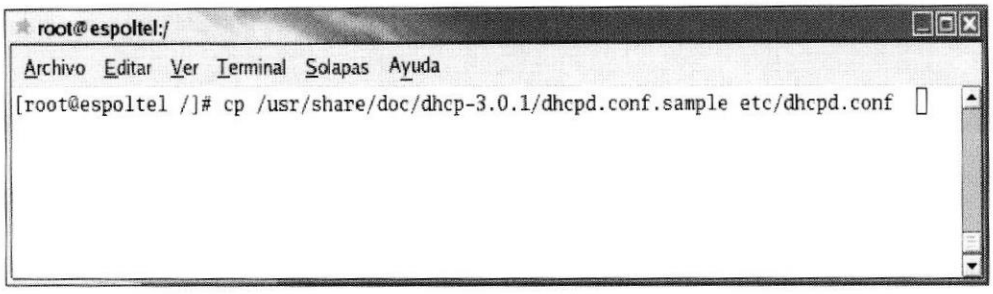


Figura 6.231 Pantalla donde se muestra la copia de archivo dhcp.conf.sample al dhcpd.conf.

3. Editar el archivo dhcpd.conf. con el comando **vi.**

root@localhost /]# vi /etc/dhcpd.conf

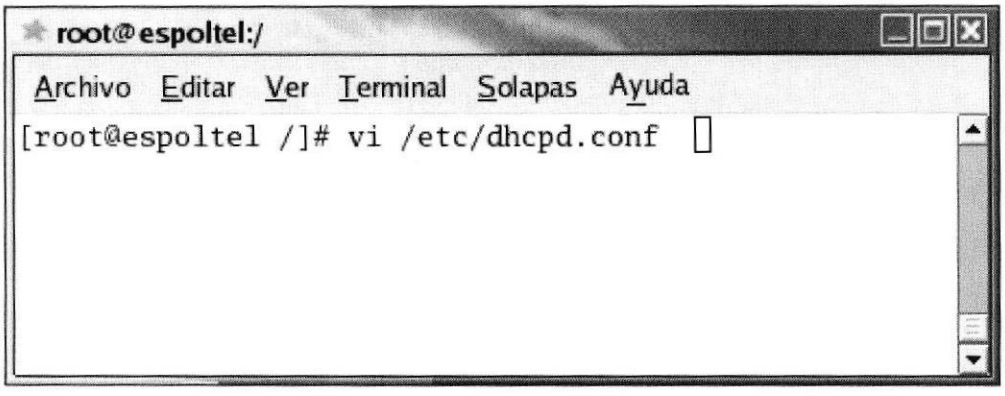


Figura 6.232 Pantalla de edición del archivo dhcpd.conf.

4. Configurar el archivo dhcpd.conf

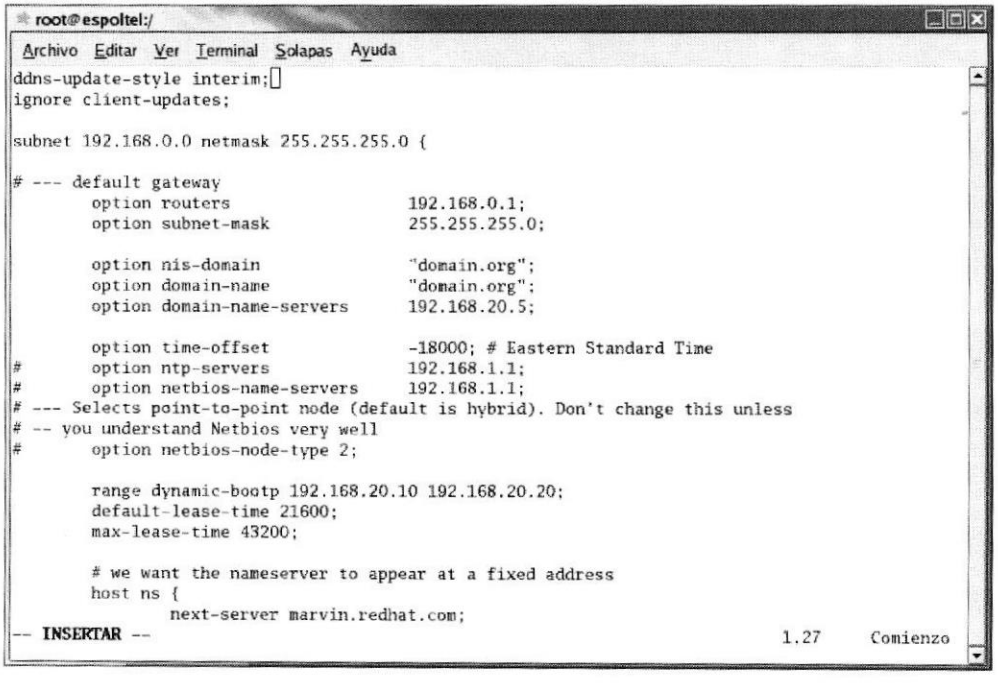


Figura 6.233 Pantalla de configuración del archivo dhcpd.conf

- En la línea subnet se asigna el segmento de red con su respectiva máscara.
- Subset 192.168.0.0 netmask 255.255.255.0
- Opcional colocar la línea del gateway
- Option routers 192.168.20.5
- Option subset-mask 255.255.255.0
- Digitar la dirección del DNS
- Option domain-name-servers 192.168.20.5
- Definir el rango de IP desde - hasta
- Range dynamic-bootp 192.168.21.10 192.168.21.20
- Salir con :wq para guardar los cambios.

5. Se debe crear un archivo en la siguiente ruta que es donde se guardaran todas las direcciones ip asignadas por dhcp.

root@localhost /]# touch /var/lib/dhcp/dhcpd.leases

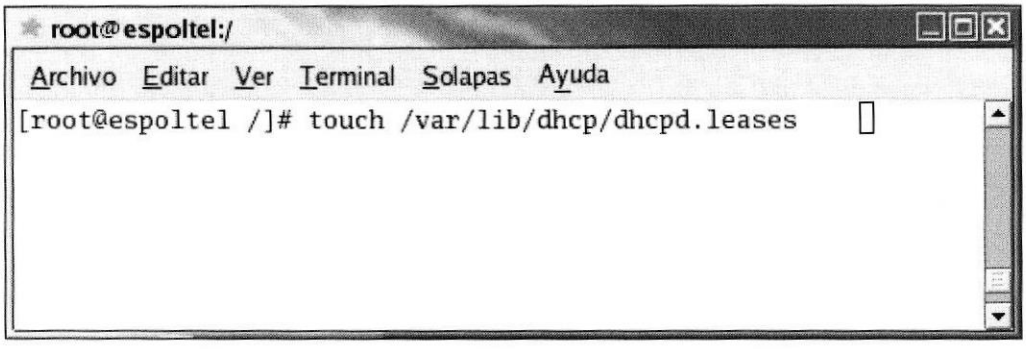


Figura 6.234 Pantalla de creación del archivo dhcpd.leases.

6. Para añadir dhcp al arranque del sistema, ejecute:

[root@localhost /]# chkconfig dhcpd on

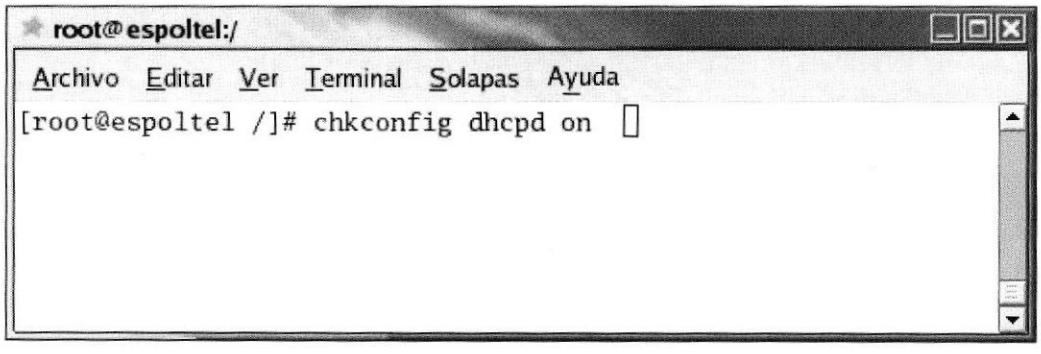


Figura 6.235 Pantalla de arranque del sistema.

7. Verificar el estado del proceso de dhcpd cada vez que se realice un cambio.

[root@localhost /]# pgrep dhcpd

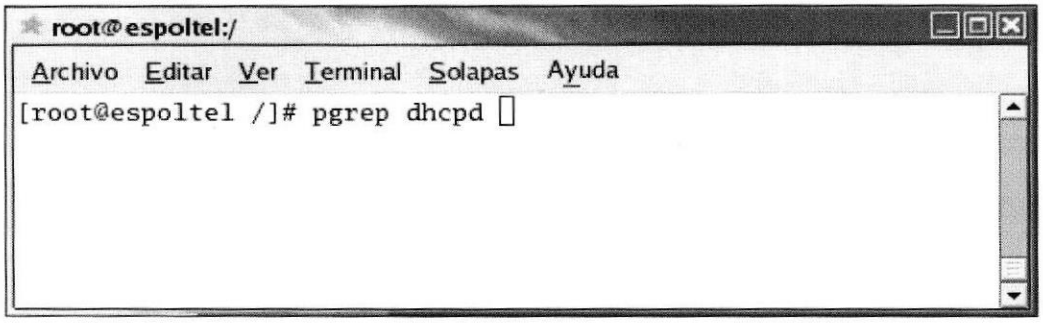


Figura 6.236 Pantalla de verificación del proceso de dhcpd.

8. Iniciar el servicio del dhcpd

[root@localhost /]# service dhcpd restart

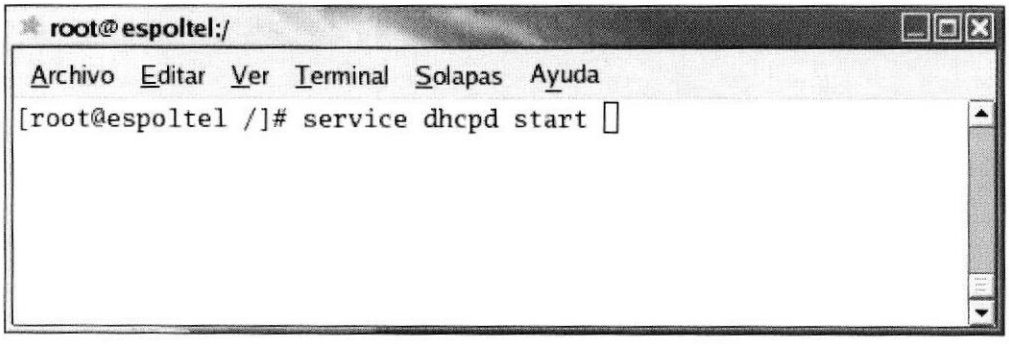


Figura 6.237 Pantalla de inicialización del dhcpd.

6.7.9.5 CONFIGURANDO EL CLIENTE WINDOWS EN DHCPD.

Se debe ingresar a mis sitios de red, este icono se encuentra en el escritorio de Windows.

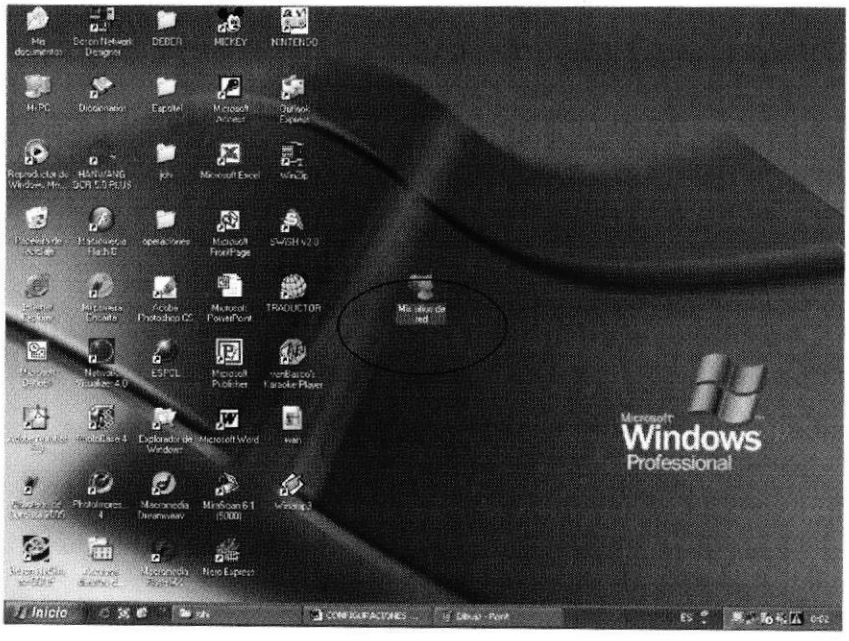


Figura 6.238 Pantalla del entorno de Windows.

Si el icono, no apareciera, debe ir al explorador de Windows; donde escoja mis sitios de red y proceder a dar clic derecho opción propiedades.

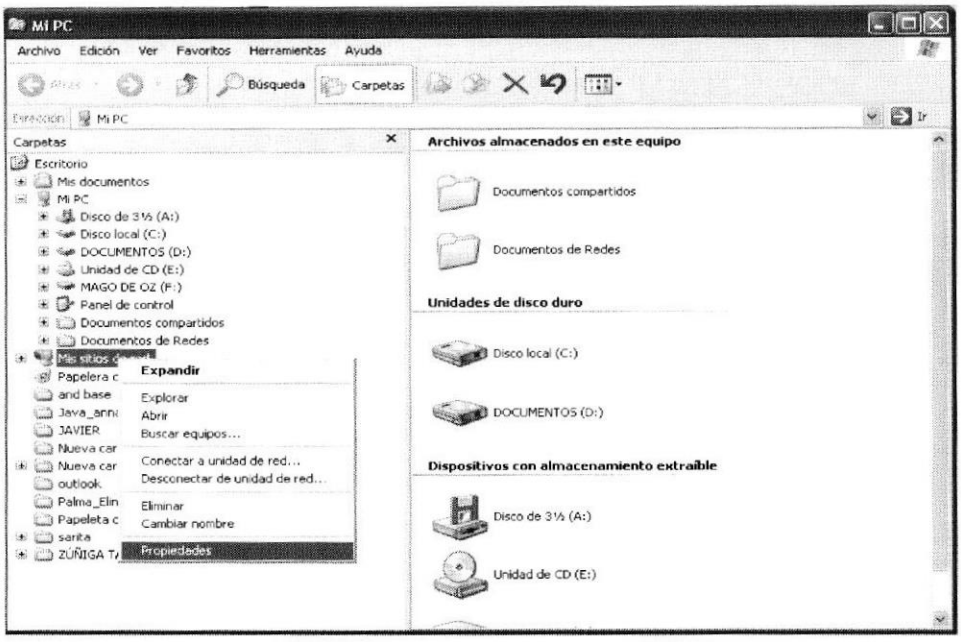


Figura 6.239 Pantalla del explorador de Windows.

Tanto en la primera opción, como en la segunda se mostrarán ventanas de conexiones de red, dé clic derecho al icono de conexiones de área local y elija propiedades.

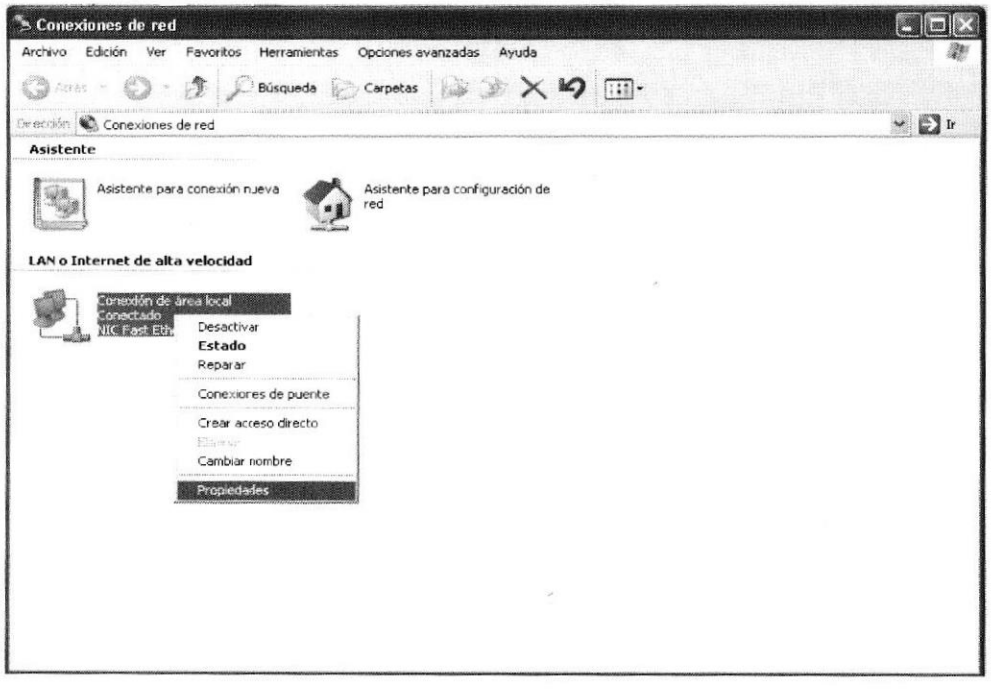


Figura 6.240 Pantalla de conexiones de red.

De la ventana que se muestra en propiedades de conexiones de área local, proceda dar doble clic sobre Protocolo Internet (TCP/IP).

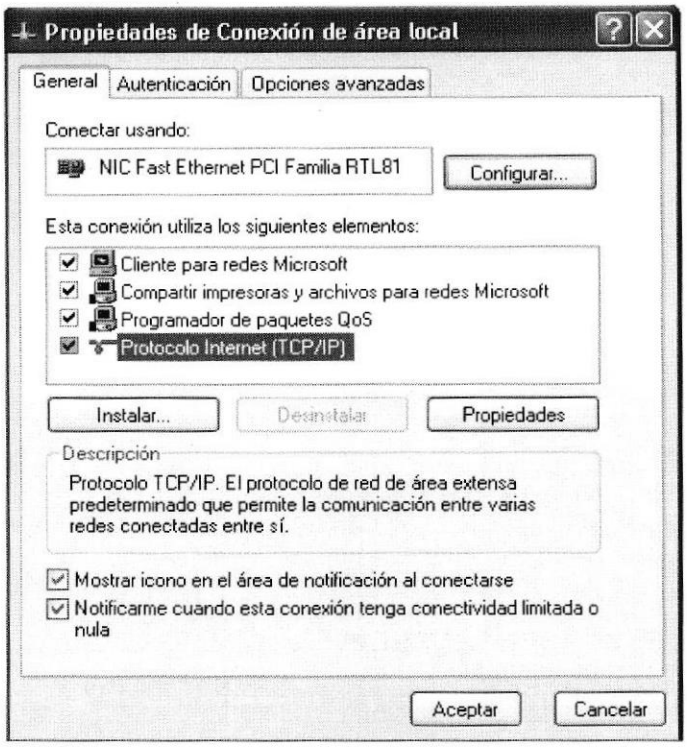


Figura 6.241 Pantalla de propiedades de conexión de área local.

Una vez realizado el proceso, configure la tarjeta de red de manera automática. y presione Ok.

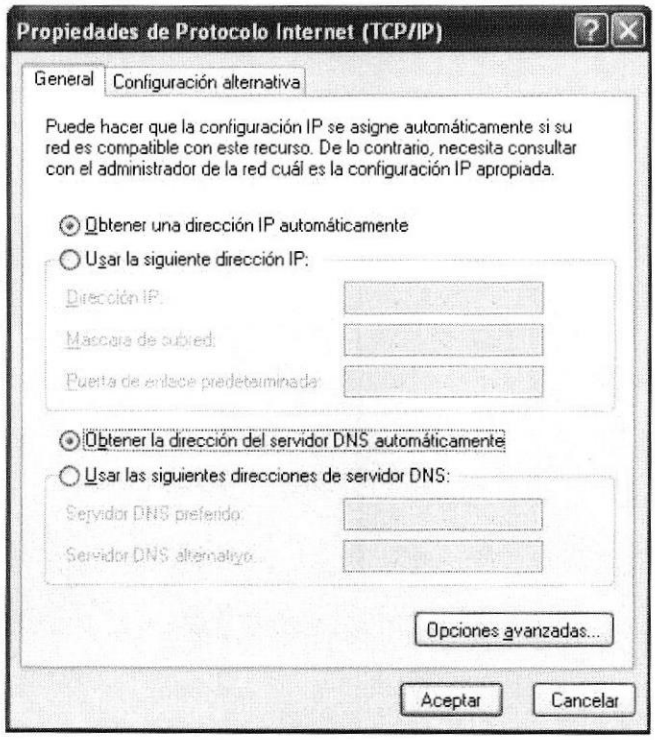


Figura 6.242 Pantalla de Propiedades (TCP/IP).

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

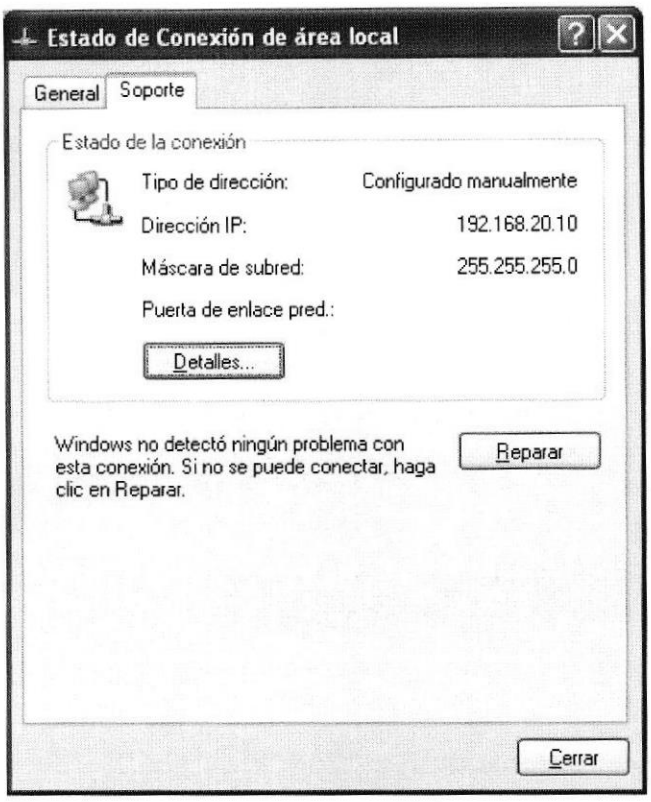


Figura 6.243 Pantalla de verificación de ip dinámica.

En caso de reiniciar el servidor los servicios no se inician, por lo tanto deberá activarlos con el comando Setup.

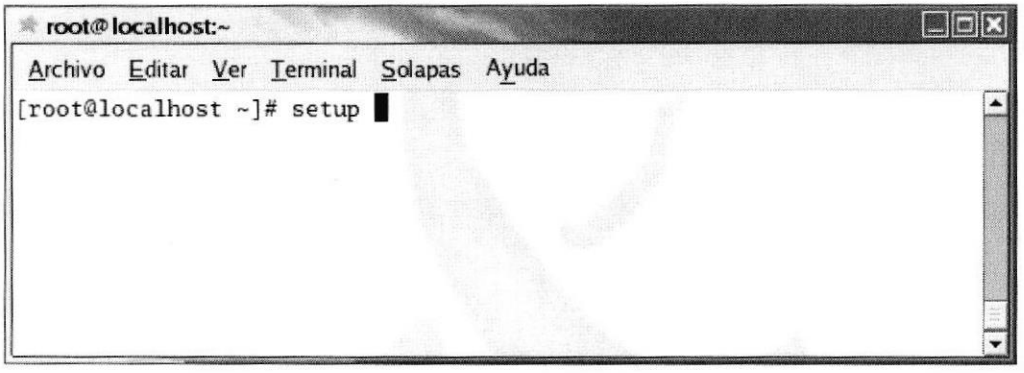


Figura 6.244 Pantalla de ingreso al setup.

A continuación aparecerá una pantalla, la misma que contiene el menú "Elija una Herramienta", donde deberá escoger la opción Servicios del Sistema y luego Ejecutar una Herramienta.

Figura 6.245 Pantalla de ingreso a Servicios del sistema.

Aparece la ventana de Servicios donde debe habilitar squid y elegir Ok.

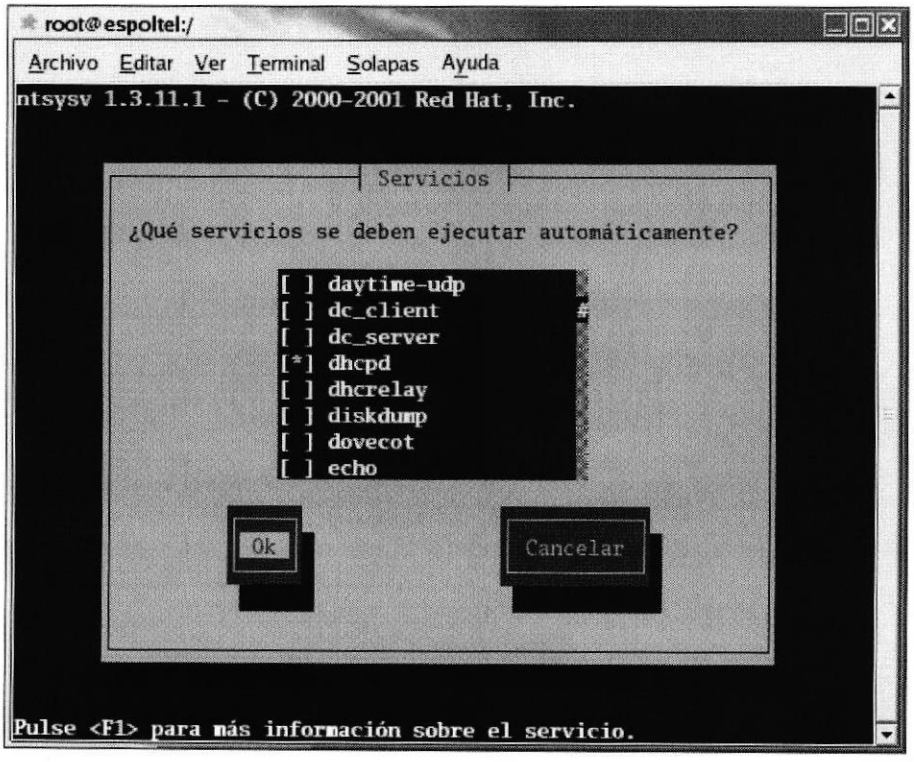


Figura 6.246 Pantalla de configuración del paquete squid.

6.7.10 CONFIGURACIÓN MRTG

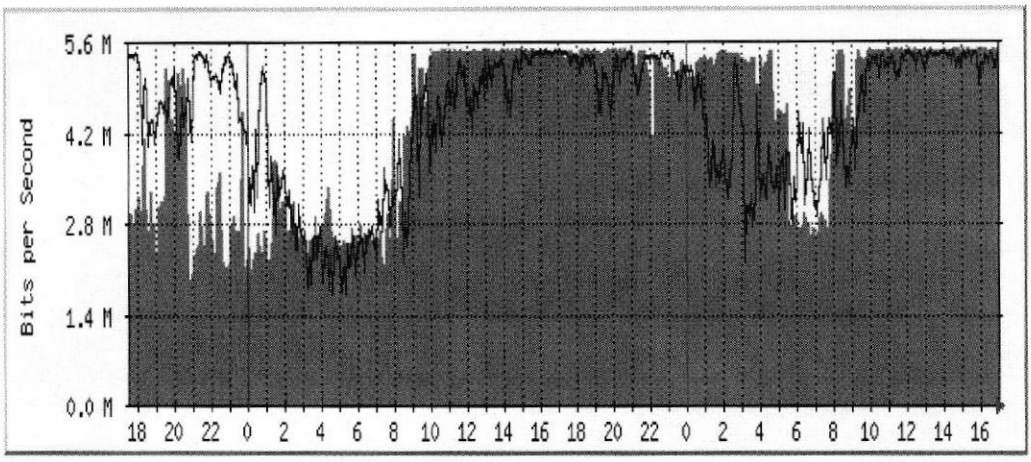


Figura 6.247 Pantalla de funcionamiento del MRTG.

Router Traffic Grapher (MRTG) es la más importante de las aplicaciones de monitorización de tráfico que se encuentra para servidores Linux.

En el caso más general, MRTG usa SNMP (Simple Network Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (routers o servidores). Los gráficos generados con MRTG, además de una vista diaria detallada, representan también el tráfico de los últimos siete días, las cuatro últimas semanas y los últimos doce meses. Esto es posible porque MRTG mantiene un archivo de todos los datos que ha obtenido del dispositivo de red. Este archivo es consolidado automáticamente, así que no crece con el tiempo, pero contiene todos los datos relevantes del tráfico de los últimos dos años. Todo esto se realiza de una manera eficiente.

6.7.10.1 REQUERIMIENTOS DE SOFTWARE:

- Debe tener instalado librerías de Perl y C.
- Para su optima compilación debe tener instalado librerías como:
  - gd
  - libpng
  - Zlib
- Compilar las librerías requeridas
- Configurar SNMP
- Compilar el MRTG
- Configurar MRTG

6.7.10.2 CONFIGURACIÓN DE DHCP.

1. Tener instalados
   SNMPD
   Net-snmp-utils
   Librerías de Perl
   Librerías C

2. Tener configurados
   Servidor dns
   Servidor http

3. Configurar snmp
   Path /etc/snmp/snmpd.conf
   #Reglas de control de acceso al agente, establece quien
   #puede conectarse, permisos de lectura, escritura,
   #que ramas puedes ver, etc.

```
com2sec              local          localhost      secreto
com2sec              mynetwork      192.168.20.5   secreto

group  MyRWGroup v1      local
group  MyRWGroup v2c     local
group  MyRWGroup usm     local
group  MyROGroup  v1     mynetwork
group  MyROGroup  v2c    mynetwork
group  MyROGroup  usm    mynetwork

#Ramas MIB que se permiten ver
view   all      included      .1      80

#Establece permisos de lectura y escritura
access MyROGroup ""      any     noauth exact   all   none  none
access MyRWGroup ""      any     noauth exact   all   all   none

#Información del Contacto del Sistema
syslocation BankHacker
syscontact BankHacker

service snmpd start

#Comprobación
snmpwalk -Os -c secreto -v 1 localhost system
```

4. Descomprimo y compilo zlib, libpng, gd y mrtg

   Crear el directorio para la compilación:

```
mkdir -p /usr/local/src
cd /usr/local/src
```

   ZLIB

```
gunzip -c zlib-*.tar.gz | tar xf -
rm zlib-*.tar.gz
mv zlib-* zlib
cd zlib
./configure
make
cd ..
```

LIBPNG

```
gunzip -c libpng-*.tar.gz |tar xf -
rm libpng-*.tar.gz
mv libpng-* libpng
cd libpng
make -f scripts/makefile.std CC=gcc ZLIBLIB=../zlib \
ZLIBINC=../zlib
rm *.so.* *.so
cd ..
```

GD

```
gunzip -c gd-*.tar.gz | tar xf -
rm gd-*.tar.gz
mv gd-* gd
cd gd
env CPPFLAGS="-I../zlib -I../libpng" LDFLAGS="-L../zlib \
-L../libpng" ./configure --disable-shared --without-freetype \
--without-jpeg
```

(el slash (\) significa que se deja un espacio y continúa la línea que viene)

```
make

cp .libs/* .
(ingresar lo anterior 2 veces (cp .libs/* .))
```

(Ingresar lo siguiente para versiones del gd anteriores al 2.0)

```
perl -i~ -p -e s/gd_jpeg.o//g Makefile
make INCLUDEDIRS="-I. -I../zlib -I../libpng" \
LIBDIRS="-L../zlib -L. -L../libpng" \
LIBS="-lgd -lpng -lz -lm" \
CFLAGS="-O -DHAVE_LIBPNG"
cd ..
```

MRTG

```
cd /usr/local/src
gunzip -c mrtg-2.13.2.tar.gz | tar xvf -
cd mrtg-2.13.2
./configure     --prefix=/usr/local/mrtg-2          \
                --with-gd=/usr/local/src/gd         \
                --with-zlib=/usr/local/src/zlib     \
```

--with-png=/usr/local/src/libpng

make

make install

5. Crear directorios de configuración y archivos de configuración
   mkdir /var/www/html/espol/mrtg
   (espol es la carpeta donde esta alojada la página web)
   touch /etc/mrtg.cfg

6. Configurar directorios de trabajo, opciones, salida y especificar la comunidad con su respectiva ip
   /usr/local/mrtg-2/bin/cfgmaker \
   --global 'WorkDir: /var/www/html/espol/mrtg' \
   --global 'Options[_]: bits,growright' \
   --output /etc/mrtg.cfg \
   secreto@192.168.20.5

   (espol es la carpeta donde esta alojada la página web)
   (secreto@192.168.20.5 hace referencia a lo que se creó en el snmpd.conf)

7. Cargar la configuración
   env LANG=C /usr/local/mrtg-2/bin/mrtg /etc/mrtg.cfg
   (ingresar lo anterior 3 veces)

8. Editar el CRONTAB para actualizar cada 5 minutos
   crontab -e
   Programación del CRON para refresh cada 5 minutos
   00,05,10,15,20,25,30,35,40,45,50,55 * * * * /usr/local/mrtg-2/bin/mrtg /etc/mrtg.cfg

9. Se prueba cargando la página
   http://www.espoltel.net/mrtg/

GLOSARIO

GLOSARIO DE TÉRMINOS

A

Ancho de Banda: La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también se usa para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

ARP: Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Comparar con RARP.

Asignación de direcciones: Técnica que permite que distintos protocolos interoperen traduciendo direcciones desde un formato a otro. Por ejemplo, al enrutar IP a través de una red Frame Relay, las direcciones IP se deben mapear a las direcciones Frame Relay de modo que los paquetes IP se puedan transmitir por la red. Ver también resolución de direcciones.

B

Banda Ancha: Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica. Comparar con banda ancha.

Broadcast: Envío de información en cualquier formato a mas de un lugar de destino

Banda Base: Característica de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha. Ver la diferencia con banda ancha. Término utilizado en la WWW

Bps: (Bits per Second). Medida que representa la rapidez con que los bits de datos se transmiten a través de un medio de comunicaciones. Por ejemplo: un módem de 28.8 Kbps es capaz de transferir 28.800 bits por segundo.

Bit: (Binary Digit ó Dígito Binario). Es un dígito en base 2,es decir, 0 ó 1.Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

Byte: Unidad de medida de la cantidad de información en formato digital. Usualmente un byte consiste de 8 bits. Un bit es un cero (0) o un uno (1). Esa secuencia de números

(byte) pueden simbolizar una letra o un espacio (un carácter). Un kilobyte (Kb) son 1024 bytes y un Megabyte (Mb) son 1024 Kilobytes.

Bloqueo: En un sistema de conmutación, una condición en al que no hay ninguna ruta disponible para completar un circuito. El término también se usa para describir una situación en la que no se puede iniciar una actividad hasta que la otra no se haya completado.

C

Cable blindado: cable que posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

Cable coaxial: cable compuesto por un conductor cilíndrico exterior hueco que rodea un conductor de alambre interno único. En la actualidad se usan dos tipos de cable coaxial en la LAN: cable de 50 ohmios, que se usa para la señalización digital, y cable de 75 ohmios que se usa para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro, sin embargo no es susceptible a la interferencia electromagnética y es capaz de brindar velocidades de datos más altas.

Cable neutro: Cable de circuito que se conecta a la conexión a tierra en la central de energía y en el transformador.

Cableado backbone: Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN.

Cableado de Categoría 1: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 1 se usa para comunicaciones telefónicas y no es adecuado para transmitir datos. Comparar con cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5..

Cableado de Categoría 2 : Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5.

Cableado de Categoría 3: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 3 se usa en las redes 10BASE-T y puede transmitir datos a velocidades de hasta 10 Mbps. Comparar con cableado de

Categoría 1, cableado de Categoría 2, cableado de Categoría 4 y cableado de Categoría 5..

Cableado de Categoría 4: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 4 se usa en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 5..

Cableado de Categoría 5: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 4..

Caché: Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso más rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los accesos a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

CD: Detección de portadora. Señal que indica si una interfaz está activa. También, una señal generada por un módem que indica que se ha conectado una llamada.

Canaleta decorativa Tipo de canal montado en la pared que tiene una cubierta removible que se usa para admitir el cableado horizontal. La canaleta decorativa es lo suficientemente grande como para contener dos cables.

Canaleta: Un tipo de canal adosado a la pared que tiene una cubierta removible para dar apoyo al cableado horizontal. La canaleta es lo suficientemente grande como para contener varios cables.

Capa física: La Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Capa de control de enlace de datos: La Capa 2 del modelo de arquitectura SNA. Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

Capa de red: La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

Capa de transporte: La Capa 4 del modelo de referencia OSI. Esta capa es responsable de la comunicación confiable de red entre nodos finales. La capa de transporte

suministra mecanismos para establecer, mantener y terminar los circuitos virtuales, detección y recuperación de errores de transporte y control del flujo de información.

Capa de sesión: La Capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de capa de presentación.

Capa de servicios de presentación: La Capa 6 del modelo de arquitectura SNA. Esta capa suministra administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Corresponde aproximadamente a la capa de presentación del modelo OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control física, capa de servicios de transacción y capa de control de transmisión.

Capa de aplicación: La Capa 7 del modelo de referencia OSI. Esta capa suministra servicios a los procesos de aplicación (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de terminal) que están fuera del modelo OSI. La capa de aplicación identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos que se requieren para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos. Corresponde aproximadamente a la capa de servicios de transacción del modelo SNA. Ver también capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

Carrier: Compañía que proporciona servicios de telecomunicaciones a través de medios de comunicación de datos (Fibra óptica, microondas, radio, conexión telefónica o enlace satelital). Los cuales pueden ser propios o alquilados, estos proveedores suelen suministrar sus servicios basándose en redes de compañías telefónicas.

Cliente: Nodo que solicita servicios a un servidor.

Colisión: En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

Cola: Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

Conector RJ: Conector macho registrado. Conectores estándar que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ

Costo: Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia

un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.

Consola: DTE a través del cual se introducen los comandos en un host.

Correo electrónico: Aplicación de red utilizada ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.

CSMA/CD: Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón).

Cliente: Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

Computador: Es un dispositivo electrónico compuesto básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

Contraseña ó Password: Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los Sistemas y recursos de la computadora.

CPU: (Central Processing Unit ó Unidad central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

Cuadro de Diálogo: Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

Cuadro de Texto: Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de diálogo, el cuadro de texto puede estar en blanco o contener texto.

Cursor: Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo caracter a visualizar cuando se pulse una tecla.

CSU: Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con el loop telefónico digital local. A menudo se denomina, de forma conjunta con DSU, como CSU/DSU.

D

Db: Decibelios

Dominio: En Internet, una parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía

DCE: equipo de comunicación de datos. Equipo de comunicación de datos (expansión EIA) o equipo de terminación de circuito de datos (expansión ITU-T). El dispositivo y las conexiones de una red de comunicaciones que abarca el extremo de la red de la interfaz usuario a red. El DCE proporciona una conexión física con la red, envía tráfico y suministra una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE. Comparar con DTE.

Descifrado: La aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando por lo tanto los datos a su estado original, no cifrado.

Dato: Son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

DTE: Equipo de terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario-red que actúa como origen de datos, destino de datos o ambas. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y por lo general usa señales de temporización generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadores, traductores de protocolo y multiplexores.

Directorio: En D.O.S., una lista de nombres de archivo que contiene toda la información de los archivos almacenados. A partir de Windows 95 este término se reemplazó por CARPETA.

Dirección: Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico" (email address); "IP" (dirección Internet); y "dirección hardware".

Dirección del Protocolo de Internet (dirección IP): Dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red con Protocolo de control de transmisión/Protocolo Internet (TCP/IP). Número único que consta de 4 partes separadas por puntos. Una dirección IP se suele representar en una notación decimal con puntos que indica cada octeto (ocho bits o un

byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 172.16.255.255.

Cada computadora conectada a Internet tiene un único número de IP. Si la máquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem).

Disco Rígido: Unidad de almacenamiento permanente de información. Éste es el que guarda la información cuando apagamos la computadora. Aquí se guardan la mayoría de los programas y el sistema operativo. Su capacidad de almacenamiento se mide en Megabytes (Mb) o Gigabytes (Gb), en donde 1024 Mb = 1Gb.

Disquete: Dispositivo que puede insertarse y extraerse en una unidad de disco.

DNS: (Domain Name System ó Sistema de Nombres de Dominio). El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de éstos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes son: .COM (comercial - empresas), .EDU (educación, centros docentes), .ORG (organización sin ánimo de lucro), . NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejército USA). La mayoría de los países tienen un dominio propio. Por ejemplo, AR (Argentina) .PY (Paraguay), .US (Estados Unidos de América), .ES (España), ..AU (Australia), etc.

Dominio: (Domain Name). Nombre único que identifica a un sitio de Internet. Los nombres de dominio tienen 2 o más secciones, separadas por puntos. La sección de la izquierda es la más específica, y la de la derecha, la más general. Una computadora particular puede tener más de un nombre de dominio, pero un nombre de dominio se refiere únicamente a una PC.

Download ó descargar: En Internet es el proceso de transferir información desde un servidor de información a la propia PC.

Documentación: Manual escrito que detalla el manejo de un sistema o pieza de hardware.

Doble Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón) dos veces, sin desplazarlo. Esta acción sirve para ejecutar una determinada aplicación, como por ejemplo: inicializarla.

DSU: Unidad de servicio de datos. Dispositivo que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión como, por ejemplo, T1 y E1. La DSU también es responsable de funciones tales como

DVD: (Digital Versatile Disc ó Disco Versátil Digital). Disco que sirve para almacenar más datos de contenido digital, como música o video, que un CD. Un DVD guarda un mínimo de 4.7 Gigabytes (el tamaño de una película de cine).

E

E1: Estándar Europeo equivalente al americano T1. Los circuitos E1 y T1. Los dos usan canales de 64 Kbps, pero el T1 tiene 24 mientras que el E1 tiene 32 canales.

EIA/TIA-568: Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

Encapsulamiento: El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

Emulación de terminal: Aplicación de red en la que un computador ejecuta software que la hace aparecer ante un host remoto como una terminal conectada directamente.

Enrutamiento: Proceso para encontrar una ruta hacia un host destino. El enrutamiento en redes de gran tamaño es muy complejo dada la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ethernet: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3. Ver también 10BASE2, 10BASE5, 10BASE-F, 10BASE-T, 10Broad36 e IEEE 802.3.

Elemento de Pantalla: Partes que constituyen una ventana o cuadro de diálogo como por ejemplo: la barra de título, los botones de "Maximizar" y "Minimizar", los bordes de las ventanas y las barras de desplazamiento.

Escritorio: Fondo de la pantalla sobre la cual aparecen ventanas, iconos y cuadros de diálogo.

Estación de trabajo: Computador de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. Llamadas así para distinguirlas de los que se conocen como servidores.

Expandir: Mostrar los niveles de directorio ocultos del árbol de directorios. Con el administrador de archivos es posible expandir un solo nivel de directorio, una rama del árbol de directorio o todas las ramas a la vez.

Explorador: Llamado también explorador Web. Interfaz cliente que permite al usuario ver documentos HTML en el World Wide Web, en otra red o en su propio equipo; seguir los hipervínculos y transferir archivos. Un ejemplo es Microsoft Internet Explorer.

Extensión: Está compuesto por un punto y un sufijo de hasta tres caracteres situados al final de un nombre de archivo. La extensión suele indicar el tipo de archivo o directorio.

F

Fibra monomodo: Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único. Ver también fibra multimodo.

Fibra multimodo: Fibra óptica que permite la propagación de múltiples frecuencias de luz.

Firewall: Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Fluctuación de fase: Distorsión analógica de la línea de comunicación provocada por la variación de una señal de sus posiciones de temporización de referencia. La fluctuación de fase puede provocar la pérdida de datos, especialmente a altas velocidades.

Flujo de datos: Todos los datos que se transmiten a través de la línea de comunicaciones en una sola operación de lectura o escritura.

Frecuencia: Cantidad de ciclos, medidos en hercios, de una señal de corriente alterna por unidad de tiempo.

FTP: Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP, que se usa para transferir archivos entre nodos de la red. El FTP se define en la RFC 959.

Full duplex: Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora

G

Gateway: En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función, y gateway se refiere a un dispositivo con fines especiales que

ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra.
Gateway fronterizo: Router que se comunica con routers de otros sistemas autónomos.

Giga: Prefijo que indica un múltiplo de 1.000 millones, o sea 10^9. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 2^{30}, o sea 1.073.741.824.

Grupo de trabajo: Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

H

Hardware: Son todos los componentes físicos que componen una PC.

Hercio: Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

Hexadecimal: Base 16. Representación numérica que usa los dígitos 0 a 9, con su significado habitual, y las letras A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, luego 16^2=256, etc.

Host : Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

HTML: (HyperText Markup Language). Lenguaje utilizado para crear los documentos de hipertexto que se emplean en la WWW. Los documentos HTML son simples archivos de texto que contienen instrucciones (llamadas tags) entendibles por el Navegador (Browser).

HTTP: (HyperText Transport Protocol). Protocolo utilizado para transferir archivos de hipertexto a través de Internet. Requiere de un programa "cliente" de HTTP en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la WWW.

Hub: Dispositivo de hardware o software que contiene módulos de red y equipo de internetwork múltiples, independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen, las señales que se envían a través de ellos).

I

IEEE: Instituto de ingenieros eléctricos y electrónicos. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN del IEEE son los estándares de LAN predominantes en el mundo actual.

IEEE 802.1: Especificación del IEEE que describe un algoritmo que evita los loops de capa dos mediante la creación de un spanning tree. El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo de Digital y el algoritmo IEEE 802.1 no son exactamente los mismos, ni tampoco son compatibles.

IEEE 802.12: Estándar LAN del IEEE que especifica la capa física y la subcapa MAC de la capa de enlace de datos. El IEEE 802.12 usa el esquema de acceso a los medios de prioridad de demanda a 100 Mbps a través de una diversidad de medios físicos. Ver también 100VG-Any LAN.

IEEE 802.2: Protocolo LAN del IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 administra errores, entramado, control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se usa en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3: Protocolo LAN del IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 usa acceso CSMA/CD a diversas velocidades sobre diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican las implementaciones de Fast Ethernet. Las variantes físicas de la especificación IEEE 802.3 original incluyen 10BASE2, 10BASE5, 10BASE-F, 10BASE-T y 10Broad36. Las variantes físicas de Fast Ethernet incluyen 100BASE-T, 100BASE-T4 y 100BASE-X.

Icono: Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc.

IDF: Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

Impresora: Dispositivo de salida, cuya funcionalidad es transcribir/pasar un documento (imagen y/o texto) desde el ordenador (procesador de textos, bloc de notas, visor de imágenes, etc.) a un medio físico, generalmente papel, mediante el uso de cinta, cartuchos de tinta o también con tecnología láser.

Impresora de Inyección a tinta: Crean imágenes directamente sobre el papel al rociar tinta a través de una pequeñas boquillas, su calidad de impresión es bastante alta.

Impresora Predeterminada: Impresora que se utiliza si se elige el comando Imprimir, no habiendo especificado antes la impresora que se desea utilizar. Sólo puede haber una impresora predeterminada, que debe ser la que se utilice con mayor frecuencia.

Información: Es lo que se obtiene del procesamiento de datos, es el resultado final.

Informática cliente-servidor: Término que se usa para describir los sistemas de red informáticos distribuidos (de procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: cliente (front end) y servidor (back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos actuales.

Internetwork: Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red.

IP: Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad. Documentado en la RFC 791.

IP access-group: Comando que enlaza una lista de acceso existente con una interfaz de salida.

IP host: Comando que se usa para crear una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.

IP multicast: Técnica de enrutamiento que permite que el tráfico IP se propague desde un origen hacia un número de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, se envía un paquete a un grupo de multicast que se identifica mediante una sola dirección de grupo de destino IP.

IPX: Intercambio de paquetes de internetworking. Protocolo de capa de red (Capa 3) de NetWare que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

Interfaz: Una conexión e interacción entre hardware, software y usuario, es decir, como la plataforma o medio de comunicación entre usuario o programa.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

Intranet: Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno.

ISO: Organización Internacional de Normalización. Organización internacional que es responsable por una amplia gama de estándares, incluyendo aquellos relevantes para el networking. ISO desarrolló el modelo de referencia OSI, un modelo de referencia de networking sumamente popular.

ISP: Un proveedor de servicios de Internet compra acceso directo a Internet a traves de una compañía de Internet, y revende el servicio a sus abonados a través de la conexión telefónica a redes mediante un modem (o a grandes clientes mediante circuitos de T1 o E1de línea privada o retransmisión de trama) a demás de añadir servicios propios, como son el correo electrónico, las páginas Web etc.

J

Jumper: Término que se usa para los cables de interconexión que se encuentran en el armario de cableado.

K

Kbps: (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit esta formado por mil bits.

Kilobyte: Es el equivalente a 1024 bytes.

L

LAN: Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido. Comparar con MAN y WAN.

Latencia: Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir tambien sucede en el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

LED: Diodo emisor de luz. Dispositivo semiconductor que emite luz producida por la conversión de energía eléctrica. Las lámparas de estado en los dispositivos de hardware generalmente son LED.

Línea de acceso telefónico: Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

Línea de comunicación: Enlace físico (como, por ejemplo, un cable o circuito de teléfono) que conecta uno o más dispositivos con uno o más dispositivos.

Línea de mira: Característica de determinados sistemas de transmisión como, por ejemplo, los sistemas láser, de microondas e infrarrojos, en los que no puede existir ninguna obstrucción en la ruta directa entre el transmisor y el receptor.

Línea dedicada: Línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir. Ver también línea arrendada.

Lista de acceso: Lista que mantienen los routers Cisco para controlar el acceso hacia o desde el router para diversos servicios (por ejemplo, para evitar que los paquetes que tienen una determinada dirección IP salgan de una interfaz específica del router).

LSA: Publicación de estado de enlace. Paquete de broadcast que usan los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de la ruta. Los routers receptores usan las LSA para mantener sus tablas de enrutamiento

Login: Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del password, el login no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

M

MAC: Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

MICIP: Protocolo de capa de red que encapsula paquetes IP en DDS o transmisión a través de AppleTalk.

Malla: Topología de red en la que los dispositivos se organizan de una manera administrable, segmentada, con varias interconexiones, a menudo redundantes, ubicadas estratégicamente entre nodos de la red. Ver también malla completa y malla parcial.

Malla completa: Término que describe a una red en la que los dispositivos están organizados en una topología de malla, en la que cada nodo de la red tiene un circuito físico o un circuito virtual que lo conecta a todos los otros nodos de la red. Una malla completa brinda una gran cantidad de redundancia pero, dado que su implementación puede resultar excesivamente cara, generalmente se la reserva para los backbones de la red. Ver también malla y malla parcial.

MAN: Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

MAP: Protocolo de automatización de fabricación. Arquitectura de red creada por General Motors para satisfacer las necesidades específicas las instalaciones fabriles. El MAP especifica una LAN de transmisión de tokens similar a IEEE 802.4. Ver también IEEE 802.4.

Mapa de cableado: Característica suministrada por la mayoría de los analizadores de cable. Se usa para probar las instalaciones de cableado de par trenzado, y muestra cuáles hilos están conectados a cuáles pines, en conectores macho y hembra.

Mapa de topología: Herramienta para administrar un switch ATM LightStream 2020 que examina una red y muestra el estado de sus nodos y enlaces troncales. El mapa de topología es una aplicación basada en HP OpenView que se ejecuta en un NMS.

Máscara de red: Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

Máscara wildcard: Cantidad de 32 bits que se usan de forma conjunta con una dirección IP para determinar cuáles son los bits de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

MD5: Message Digest 5. Algoritmo que se usa para la autenticación de mensajes en SNMP v.2. El MD5 verifica la integridad de la comunicación, autentica el origen y controla la puntualidad. Ver también SNMP2.

MDF: Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

Megabyte (MB): 1.048.576 bytes; 1.024 Kilobytes.

Megahertz: Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

Memoria RAM: Memoria de acceso aleatorio cuyo contenido permanecerá presente mientras el computador permanezca encendido.

Memoria ROM: Memoria de sólo lectura. Chip de memoria que sólo almacena permanentemente instrucciones y datos de los fabricantes.

Microonda: este enlace esta constituido por dos transceptores de radio provistos de antenas parabólicas que se apuntan directamente entre si. La radio puede transportar transmisiones punto a punto de muchos anchos de banda. Su alcance varia según el tamaño de la antena, el clima en la zona y la magnitud de la potencia emitida contemplando todos estos conjuntos la señal puede llegar hasta 80 Km.

Módem: (Modulator,Demodulator). Dispositivo que se conecta a la computadora y a la línea telefónica y que permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

Mouse: Permite convertir el movimiento de la mano en desplazamiento de un cursor sobre la pantalla.

Multicast: la multidifusión (multicast) permite que grupos de usuarios seleccionados reciban la misma transmisión de datos en una red los cuales están identificados por una única dirección de grupo de destino IP.

N

Navegador de Web: Aplicación de cliente de hipertexto basada en GUI como, por ejemplo, Mosaic, que se usa para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a través de la WWW e Internet. Ver también hipertexto, Internet, Mosaic y WWW.

NBP: Protocolo de enlace de denominación. Protocolo AppleTalk de nivel de transporte que convierte un nombre dado en forma de una cadena de caracteres en una dirección de internetwork.

NET: Título de entidad de red. Direcciones de red, definidas por la arquitectura de red ISO.

NetBIOS: Sistema básico de entrada/salida de red. API que usan las aplicaciones de una LAN IBM para solicitar servicios de procesos de red de nivel inferior. Estos servicios pueden incluir establecimiento y terminación de sesión y transferencia de información

NetWare: NOS distribuido de uso generalizado desarrollado por Novell. Suministra acceso remoto transparente a archivos, y muchos otros servicios de red distribuida.

Networking: Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NIC: Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

NOS: Sistema operativo de red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos. Los ejemplos de NOS incluyen LAN Manager, NetWare, NFS y VINES.

Número de host: Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

Número de red: Parte de una dirección IP que especifica la red a la que pertenece el host.

Número de saltos: Métrica de enrutamiento que se usa para medir la distancia entre un origen y un destino. El RIP usa el número de saltos como su única métrica.

NVRAM: RAM no volátil. RAM que retiene su contenido cuando una unidad se apaga. En los productos Cisco, la NVRAM se usa para guardar la información de configuración.

Nodo: En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma.

Nombre de usuario: La secuencia de caracteres que lo identifica. Al conectarse a una computadora, generalmente necesita proporcionar su nombre y contraseña de usuario. Esta información se usa para verificar que la persona está autorizada para usar el Sistema.

O

Operador de red: Persona que monitorea y controla una red de forma continua, ejecutando tareas como

Oscilación: Señal secundaria superpuesta a la onda de 60 Hz. Tiene una magnitud que varía entre el 15% y el 100% del voltaje normal de la línea de alimentación. Ver sobrevoltaje, pico y baja de voltaje.

OSI: Interconexión de sistemas abiertos. Programa internacional de normalización creado por la ISO y la UIT-T para desarrollar estándares de interconexión que faciliten la interoperabilidad de equipos de múltiples proveedores.

OSINET: Asociación internacional diseñada para promover OSI en las arquitecturas de los proveedores.

OSPF: Versión abierta del algoritmo "Primero la ruta libre más corta". Algoritmo de enrutamiento IGP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad Internet. Las características de OSPF incluyen enrutamiento por menor

costo, enrutamiento de múltiples rutas y balanceo de carga. El OSPF deriva de una versión inicial del protocolo ISIS

P

PAD: Ensamblador/desensamblador de paquetes. Dispositivo que se usa para conectar dispositivos simples (como terminales de modo de carácter) a una red, los cuales no admiten toda la funcionalidad de un protocolo específico. Los PAD almacenan los datos en el búfer de los PAD y ensamblan y desensamblan los paquetes que se envían a dichos dispositivos finales.

Panel de conexión: Conjunto de ubicaciones de pin y puertos que se puede montar en un bastidor o una consola de pared en el armario de cableado. Los paneles de conexión actúan como conmutadores que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

Paquete de choque: Paquete que se envía al transmisor para informarle que hay congestión y que debe reducir su velocidad de envío.

Par trenzado: Medio de transmisión de relativa baja velocidad compuesto por dos cables aislados dispuestos en un patrón en espiral regular. Los cables pueden ser blindados o no blindados. El uso del par trenzado es común en aplicaciones de telefonía y es cada vez más común en las redes de datos. Ver también STP y UTP.

Paradiafonía: Energía de interferencia transferida de un circuito a otro.

PBX: Central telefónica privada. Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas y públicas.

PCI: Información de control de protocolo. Información de control que se agrega a los datos del usuario para formar un paquete OSI.

Pila de protocolo: Conjunto de protocolos de comunicación relacionados que operan de forma conjunta y, como un grupo, cumplen con la comunicación en alguna o en las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo y, a menudo, un solo protocolo de la pila se dirige a una cantidad de capas a la vez. El TCP/IP es un protocolo de pila típico.

Ping: Abreviatura para Packet Internet Groper o Packet Inter-network Groper, una utilidad que se usa para determinar si una dirección IP en particular está disponible. Funciona enviando un paquete a la dirección especificada y esperando una respuesta. El PING se usa principalmente para diagnosticar las fallas de las conexiones de Internet.

Plan de distribución: Diagrama simple que indica dónde están ubicados los tendidos de cable y la cantidad de habitaciones hacia las que se dirigen.

POP: Punto de presencia. Punto de presencia es el punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y el servicio de distribución principal del edificio.

Portadora: Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos. Ver también modulación.

POST: Autocomprobación de encendido. Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando ese dispositivo se enciende.

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

Puerto: Interfaz de un dispositivo de internetworking (como, por ejemplo, un router).
En terminología IP, un proceso de capa superior que recibe información de las capas inferiores.
Un conector hembra de un panel de conexión el cual acepta el mismo tamaño de conector que el de un RJ45. Los cables de conexión se usan en estos puertos para realizar interconexiones entre los computadores conectados al panel. Es esta interconexión conexión la que permite la operación de la LAN.

Página Web: Documento de World Wide Web. Una página Web suele consistir en un archivo HTML, con sus archivos asociados de gráficos y secuencias de comandos, en un directorio determinado de un equipo concreto (y, por tanto, identificable mediante una dirección URL).

Periféricos: Cualquier dispositivo de hardware conectado a una computadora.

Pixel: (PICture cELL). Es la parte más pequeña de una pantalla de video, constituido por uno o más puntos que se consideran como una unidad. Es por tanto, el bloque de construcción de imágenes.

Protocolo: Método por el que los equipos se comunican en Internet. El protocolo más común en el World Wide Web es HTTP. Otros protocolos de Internet incluyen FTP, Gopher y telnet. El protocolo forma parte de la dirección URL completa de un recurso.

Proveedor: Institución o empresa que provee acceso a uno o varios servicios de Internet.

R

RAM: Memoria de acceso directo aleatorio. Memoria volátil que puede ser leída y escrita por un microprocesador.

Red: Conjunto de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red de conexión única: Red que tiene una sola conexión con un router

Redireccionar: Parte de los protocolos ICMP y ES-IS que permiten que un router le indique a un host que puede ser más efectivo usar otro router.

Redistribución: Permitir que la información de enrutamiento detectada a través de un protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento. A veces denominada redistribución de ruta.

Redundancia: En internetworking, la duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan ejecutar el trabajo de aquellos que han fallado. Ver también sistema redundante.

Rendimiento: Velocidad de la información que llega a, y posiblemente atraviesa, un punto particular de un sistema de red.

Repetidor: Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red.

Retardo: El tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. También, el tiempo que se requiere para mover un paquete desde el origen hacia el destino a través de una ruta específica.

RF: Radiofrecuencia. Término genérico que se usa para referirse a frecuencias que corresponden a transmisiones radioeléctricas. Las redes de televisión por cable y de banda ancha usan tecnología RF.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

RIP: Protocolo de información de enrutamiento. IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet.

RMON: Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitoreo remoto de los dispositivos conectados a la red.

ROM: Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.

Ruta estática: Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

Ruta por defecto: Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

S

Segmento: La sección de una red limitada por puentes, routers o switches.
Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

SMTP: Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico.

Spread Spectrum: Un sistema de espectro ensanchado es aquel que ocupa mas ancho de banda del mínimo requerido para la transferencia de señales de datos. La radio de espectro ensanchado emite y recibe señales portadoras en un espectro amplio de frecuencias.

Sondeo: Método de acceso en el que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

Switch: Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI:

Switch LAN: Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches LAN envían tráfico basándose en las direcciones MAC. Esta variedad de switch LAN a veces de denomina switch de trama. Los switches LAN a menudo se clasifican de acuerdo con el método que usan para enviar tráfico: conmutación de paquetes por método de corte y conmutación de paquetes por almacenamiento y envío. Los switches multicapas son un subconjunto inteligente de los switches LAN.

Servidor: Computadora o programa que brinda un servicio específico al "cliente", que se ejecuta en otras computadoras. El término puede referirse tanto a un equipo de una red que envía archivos o ejecuta aplicaciones para otros equipos de la red; el software que se ejecuta en el equipo servidor y que efectúa la tarea de servir archivos y ejecutar aplicaciones; o bien, en la programación orientada a objetos, un fragmento de código que intercambia información con otro fragmento de código cuando se pide.

SO: (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software: Todos los componentes no físicos de una PC (Programas).

T

T1: Servicio de portadora de WAN digital. T1 transmite datos con formato DS-1 a 1.544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o B8ZS. Comparar con E1. Ver también AMI, B8ZS y DS-1.

Tabla de enrutamiento: Tabla que se guarda en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas hacia destinos de red en particular y, en algunos casos, las métricas asociadas con esas rutas.

TFTP: Protocolo de Transferencia de Archivos Trivial. Versión simplificada del FTP que permite que los archivos se transfieran desde un computador a otra a través de una red.

Terminal: Dispositivo simple en el que los datos se pueden introducir o recuperar desde una red. Generalmente, las terminales tienen un monitor y un teclado pero no tienen ningún procesador ni unidad de disco local.

Topología: Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

Topología de anillo: Topología de red que consta de un conjunto de repetidores conectados entre sí mediante enlaces de transmisiones unidireccionales para formar un solo bucle cerrado. Cada estación de la red se conecta a la red en el repetidor. Aunque lógicamente están organizadas en anillo, las topologías de anillo a menudo están organizadas en una estrella de bucle cerrado.

Topología de bus: Arquitectura LAN lineal en la que las transmisiones de las estaciones de red se propagan a lo largo del medio y son recibidas por todas las otras estaciones.

Topología en árbol: Topología LAN similar a la topología bus, salvo que las redes en árbol pueden tener ramificaciones con múltiples nodos. Las transmisiones desde una estación atraviesan la longitud del medio y son recibidas por todas las otras estaciones.

Topología en estrella: Topología LAN en la que los puntos de terminación de una red se conectan a un switch central común mediante enlaces punto a punto. Una topología de anillo que está organizada como estrella implementa una estrella de loop cerrado unidireccional en lugar de enlaces punto a punto.

Topología en estrella jerárquica: Topología en estrella extendida en la que un hub central se conecta a través de cableado vertical con otros hubs que dependen del mismo.

Transceiver: Unidad de conexión al medio. Dispositivo que se usa en las redes Ethernet e IEEE 802.3 que suministra la interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que se puede incorporar a una estación o puede ser un dispositivo individual, ejecuta funciones de capa física, incluyendo la conversión de datos digitales desde la interfaz Ethernet, detección de colisiones e inyección de bits en la red.

TIA: Asociación de la Industria de las Telecomunicaciones. Organización que desarrolla estándares relacionados con las tecnologías de telecomunicaciones.

Tunneling: Arquitectura que está diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.

Tarjeta de Interfaz de Red: (NIC). Dispositivo a través del cual computadoras de una red transmiten y reciben datos.

TCP/IP: (Transmisor Control Protocol/Internet Protocol). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

Telnet: Protocolo que permite al usuario de Internet conectarse y escribir comandos en un equipo remoto vinculado a Internet como si el usuario estuviera utilizando un terminal de texto conectado directamente al equipo. Forma parte del conjunto de protocolos TCP/IP.

Tiempo Real: Método para procesar la información en cuanto se recibe.

U

Unicast: En redes conmutadas ethernet, transferencia de archivos/paquetes entre dos entidades. Una difusión única puede iniciarla un servidor a una estación de trabajo, una estación a un servidor, una estación a una impresora o cualquier otra unidad única hacia otra entidad

UPS: (Uninterruptible Power Supply ó Suministro de Energía Ininterrumpida). Es un estabilizador electrónico que está preparado para suplir al computador cuando se presenten caídas de energía o cambios de voltaje.

URL: (Universal Resource Locator ó Localizador de Recursos Universal). Identifica de manera única la ubicación de un equipo, directorio o archivo en Internet. La dirección URL también indica el protocolo de Internet apropiado, como HTTP o FTP. Por ejemplo: http://www.microsoft.com.

USB: Tecnología que facilita la conexión de periféricos a la computadora. Esta reconoce automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo, ya que se conecta a la parte trasera de la PC a un enchufe especial (puerto USB). La tarjeta madre debe tener esta tecnología en su CHIPSET para poder conectar dispositivos de este tipo.

UTP: Cable de para trenzado no apantallado, lo que significa que no tiene envoltura alrededor del grupo de conductores. Estos cables se usan principalmente en redes de voz y datos

Usuario: Cualquier individuo que interactúa con el computador a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con el computador a nivel profesional.

V

Vector: Segmento de datos de un mensaje SNA. Un vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

Virtualización: Proceso que se usa para implementar una red basada en segmentos de red virtuales. Los dispositivos se conectan a segmentos virtuales independientemente de su ubicación física y de su conexión física con la red.

VLAN: LAN virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.

VLSM: Máscara de subred de longitud variable. Capacidad de especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

VTP: Protocolo de terminal virtual. Aplicación ISO para establecer una conexión de terminal virtual a través de una red.

Virus: Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan, se propagan a través de cualquier medio de almacenamiento, o a través de la LAN, o de la misma Internet.

W

WAN: Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

WorkGroup Director: Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroup Director se ejecuta en estaciones de trabajo UNIX, ya sea como una aplicación independiente o integrada con otra plataforma de administración de red basada en SNMP, brindando un sistema de gestión poderoso y transparente para los productos de grupo de trabajo de Cisco.

WWW: World Wide Web. Gran red de servidores de Internet la cual suministra servicios de hipertexto y otros a terminales que ejecutan aplicaciones de clientes como, por ejemplo, un navegador de Web. Ver también navegador de Web.

X

X Windows: Protocolo que interconecta estaciones de trabajo de interfaz gráfica de usuario con programas servidores de aplicaciones que utiliza TCP/IP

Z

Zona de autoridad: Asociada con DNS, la zona de autoridad es una sección del árbol del nombre de dominio para el que un servidor de nombre es la autoridad.

0-9

10 mbps: Millones de bits por segundo unidad de velocidad de transferencia de información.

10 base T: Especificación Ethernet de banda base de 10 Mbps que usa dos pares de cables de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y el otro para recibir datos. 10BASE-T, que forma parte de la especificación IEEE 802.3, tiene una limitación de distancia de aproximadamente 100 metros por segmento. Ver también Ethernet e IEEE 802.3.

10 base-F: Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BASE-FB, 10BASE-FL y 10BASE-FP para Ethernet sobre cableado de fibra óptica. Ver también 10BASE-FB, 10BASE-FL, 10BASE-FP y Ethernet.

100 base FX: Especificación Fast Ethernet de banda base de 100 Mbps que usa dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una temporización de señal adecuada, el enlace 100BASE-FX no puede exceder una longitud de 400 metros. Basado en el estándar IEEE 802.3. Ver también 100BASE-X, Fast Ethernet e IEEE 802.3.

10 base-F: Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BASE-FB, 10BASE-FL y 10BASE-FP para Ethernet sobre cableado de fibra óptica. Ver también 10BASE-FB, 10BASE-FL, 10BASE-FP y Ethernet.

10 base-FB: Especificación Ethernet de banda base de 10 Mbps que usa cableado de fibra óptica. 10BASE-FB forma parte de la especificación IEEE 10BASE-F. No se utiliza para conectar estaciones de usuario pero, en cambio, suministra un backbone de señalización síncrona que permite que segmentos y repetidores adicionales se conecten a la red. Los segmentos 10BASE-FB pueden tener hasta 2000 metros de largo. Ver también 10BASE-F y Ethernet.

10 base-FL: Especificación Ethernet de banda base de 10 Mbps que usa cableado de fibra óptica. 10BASE-FL forma parte de la especificación IEEE 10BASE-F y, aunque puede interoperar con FOIRL, está diseñado para reemplazar a la especificación FOIRL. Los segmentos 10BASE-FL pueden tener hasta 1000 metros de largo si se usan con FOIRL, y hasta 2000 metros si se usan exclusivamente con 10BASE-FL. Ver también 10BASE-F, Ethernet, y FOIRL.

10 base-FP: Especificación Ethernet de banda base de fibra pasiva de 10 Mbps que usa cableado de fibra óptica. La 10BASE-FP forma parte de la especificación IEEE 10BASE-F. Organiza una cantidad de computadores en una topología en estrella sin necesidad de usar repetidores. Los segmentos 10BASE-FP pueden tener hasta 500 metros de largo. Ver también 10BASE-F y Ethernet.