ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACION VISUAL

TOPICO DE GRADUACION

PREVIO A LA OBTENCION DEL TITULO DE:

ANALISTA DE SOPORTE DE MICROCOMPUTADORES

TEMA:

ESTRUCTURA DE REDES COMPUHELP

MANUAL DE USUARIO Y CONFIGURACIONES

AUTORES:

Robert Miguel Ruiz González

Paola Katiuska Vaca Panchana

DIRECTOR:

ANL. Fabián Barboza

AÑO:

2007

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

TEMA:

ESTRUCTURA DE REDES COMPUHELP

MANUAL DE USUARIO Y CONFIGURACIONES

AUTORES:

ROBERT MIGUEL RUIZ GONZÁLEZ
PAOLA KATIUSKA VACA PANCHANA

DIRECTOR:

ANL. FABIÁN BARBOZA

AÑO

2007

AGRADECIMIENTO

Agradezco primeramente a Dios por darme salud y fuerza para salir adelante, también quiero expresar mi agradecimiento a las personas que colaboraron con el presente manual.

A Víctor Hugo Cedeño, por colaborar con las atenciones prestadas para el análisis de la empresa Compuhelp.

A el Analista Fabián Barboza director del tópico de redes, por la excelente capacitación que nos impartió durante sus clases.

Finalmente, agradezco a mis compañeros y amigos por la motivación brindada.

Robert Miguel Ruiz González

AGRADECIMIENTO

Agradezco a Dios y a mi familia que siempre estuvieron a mi lado en los momentos importantes de mi vida, nada seria posible sin ellos.

Paola Katiuska Vaca Panchana

DEDICATORIA

A mi Madre Licenciada Grecia González por su esfuerzo y apoyo incondicional que ha hecho de mí una persona responsable.

Robert Miguel Ruiz González

DEDICATORIA

A mi madre que ha sido la luz que me guia siempre dentro de los pasos de nuestro señor Jesucristo.

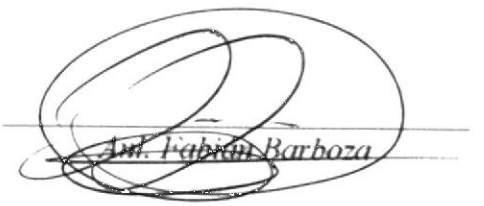
Paola Katiuska Vaca Panchana

DECLARACIÓN EXPRESA

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

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

FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN



FIRMA DE LOS AUTORES DEL TÓPICO DE GRADUACIÓN

Robert Miguel Ruiz González

Paola ~~Katinska~~ Laca Panchana

RESUMEN

Las redes son hoy en día los pilares fundaméntales del mundo empresarial, debido a que está sujeta a cambios constantes. Al desarrollar la Tesis de Grado procuramos transmitir la naturaleza constantemente cambiante de las redes, de tal forma que los usuarios perciban rápidamente su importancia y relevancia. Dentro del contenido de este manual se incluye la solución a problemas de redes a nivel WAN, también normativas y recomendaciones de cableado estructurado, configuración de routers y switches para la comunicación WAN, y finalmente como configurar los servidores necesarios para manejar seguridades dentro de la empresa, bajo la plataforma más rígida que existe, como lo es Linux.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

GENERALIDADES

1. GENERALIDADES

1.1 INTRODUCCIÓN

El presente manual de usuario y configuraciones, es producto del análisis e investigaciones realizadas a la estructura de red de la empresa Compuhelp, con el fin de optimizar sus recursos en lo referente a su infraestructura LAN y comunicación WAN.

1.2 A QUIÉN VA DIRIGIDO ÉSTE MANUAL

Éste manual está dirigido a las personas responsables del manejo de red de la Empresa Compuhelp, con el fin de facilitarles la búsqueda de soluciones rápidas y oportunas en el momento que se presente un imprevisto dentro de la red, con el único objetivo de evitar problemas a futuro. Por lo que se ha detallado sugerencias prácticas que guían a los usuarios de manera oportuna para solucionar cualquier inconveniente.

Se ha utilizado un lenguaje flexible, con el fin de que el personal administrativo y técnico pueda entender fácilmente lo explicado en el manual.

1.3 ¿POR QUÉ ÉSTE MANUAL?

El presente manual contiene un análisis detallado de las configuraciones de los dispositivos de enrutamiento, para poder conocer de manera oportuna, como se encuentran comunicados el edificio Matriz de la empresa Compuhelp con todas sus sucursales y a su vez poder monitorear el rendimiento su comunicación.

1.4 ORGANIZACIÓN DEL CONTENIDO DE ÉSTE MANUAL

El presente manual de usuario contiene una serie de capítulos, los cuales brindan conocimiento de la estructura de red de la empresa Compuhelp, y a su vez soluciones claras para que ayuden a mejorar y organizar el estado de su red, con el fin de monitorear su rendimiento; durante la lectura de este manual podrá notar que cada uno de los capítulos tiene un propósito.

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

Capítulo 1 **Generalidades.**
Especificaciones del contenido del manual y recomendaciones para poder interpretarlo.

Capítulo 2 **Situación actual.**
La Situación actual de la empresa Compuhelp comprende el estado actual en que se encuentra la empresa.

Capítulo 3 **Solución propuesta.**
Determina 2 alternativas que demanda el caso de estudio que se aplico a la empresa Compuhelp.

Capítulo 4 **Implementación WAN.**
Demuestra la implementación a nivel de la comunicación WAN.

Capítulo 5 **Cableado Estructurado: Normativas y recomendaciones ilustradas.**
Especifica como se debe implementar el cableado, cumpliendo las normas y estándares.

Capítulo 6 **Configuración de dispositivos.**
Le da a conocer todas las configuraciones de los dispositivos indicados en la implementación WAN.

Capítulo 7 **Configuración de LINUX.**
Determina las configuraciones aplicadas en el Sistema Operativo Linux Fedora Core 3.

CAPÍTULO 2

SITUACIÓN ACTUAL

2. SITUACIÓN ACTUAL

2.1 ANTECEDENTES

La convergencia de las tecnologías de la información y las telecomunicaciones es el polo de desarrollo con mayor crecimiento en la economía de la era de la globalización. El cambio hacia nuevas infraestructuras, más dinámicas y flexibles, disponibles las 24 horas del día, los 365 días del año, desde cualquier ubicación y en tiempos razonables, se ha convertido en la pauta que marca el ritmo, que define la melodía, para dejar de ser el sueño futurista de unos cuantos especialistas.

Por otro lado la eficiencia de una empresa, su capacidad de generar riqueza o de capear el temporal, se mide por el grado de cohesión interna entre los recursos que utiliza y las metas que persigue. Dicho de otra forma, en la actualidad no se trata de "inventar la bicicleta", desviando la atención y los recursos de la empresa hacia lo que no constituye su objetivo principal, sino de encontrar al socio estratégico que le ayude en la implementación de soluciones optimas.

Lo interesante de este proceso es que se da con igual dinámica "en la vertical como en la horizontal", es decir que su aplicación no es propiedad exclusiva de grandes corporaciones o instituciones, sino que debe ser el día a día de cualquier empresa, por pequeña que sea, si quiere perdurar en un futuro próximo inmediato.

Compuhelp le ofrece el concurso de experimentados ingenieros, tecnólogos y técnicos instaladores certificados y especializados en la implementación de soluciones y en el análisis, diagnóstico y afinación del motor de su empresa, es decir, las tecnologías de la información y las telecomunicaciones. Consulte con nosotros, permítanos convertirnos en sus socios tecnológicos.

COMPUHELP
ESPECIALISTAS EN SOLUCIONES

Figura 2-1: Logotipo de la empresa Compuhelp

2.2 MISIÓN

Ser la mejor experiencia de servicios tecnológicos para sus clientes, en base al profesionalismo y compromiso con su responsabilidad.

2.3 VISIÓN

La filosofía de la empresa se basa en el trabajo eficaz y eficiente para conseguir su propósito:

"Brindar soporte y consultoría tecnológica, de alta calidad y destacado profesionalismo, en tiempos oportunos y a precios competitivos"

- Obtener la satisfacción total de los clientes.
- Ofrecer servicios de óptima calidad.
- Orientarse permanentemente hacia la excelencia corporativa.

Perspectiva

- Realizar productos y servicios demostrando calidad, confianza y honestidad.
- Establecer relación directa con diseñadores de tecnologías y fabricantes.
- Contribuir al desarrollo empresarial nacional.

2.4 UBICACIÓN DE LA MATRIZ Y SUCURSALES

MAPA GEOGRÁFICO DEL ECUADOR

Figura 2-2: Ubicación de Matriz y Sucursales

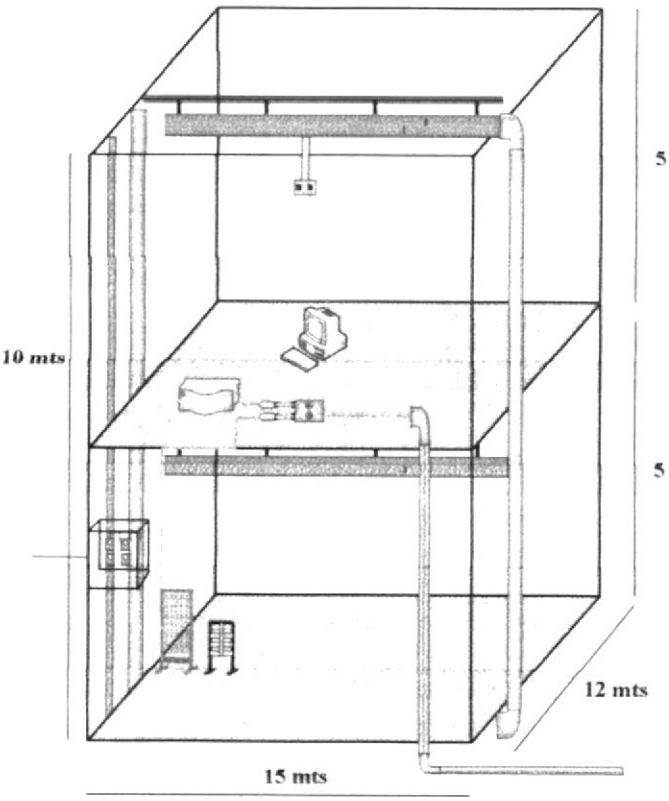
2.5 INFRAESTRUCTURA LAN

2.5.1 GUAYAQUIL

El edificio Matriz de la empresa "Compuhelp" cuenta con 2 pisos, sus dimensiones son de 10 m de alto, 15 m de ancho y 12 m de fondo, cada piso del edificio posee una altura de 5 m. Se maneja una velocidad de 100 MBPS en el backbone vertical, incluyendo los servidores de correo, web y firewalls.

Conexión a tierra:
El edificio cuenta con una conexión a tierra, lo que brinda mayor seguridad a los equipos en caso de una descarga o algún tipo de anomalía eléctrica imprevista, la misma que se encuentra ubicada del lado izquierdo del edificio (sector de los medidores).

GRÁFICO DEL EDIFICO COMPUHELP MATRIZ GUAYAQUIL



Leyenda:

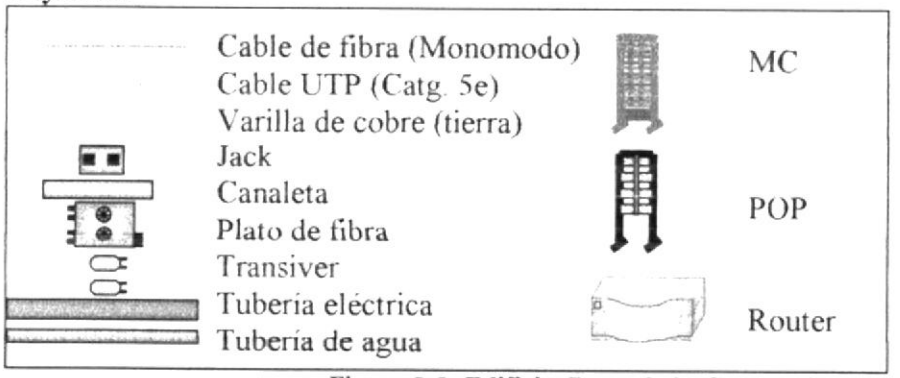


Figura 2-3: Edificio Compuhelp Guayaquil

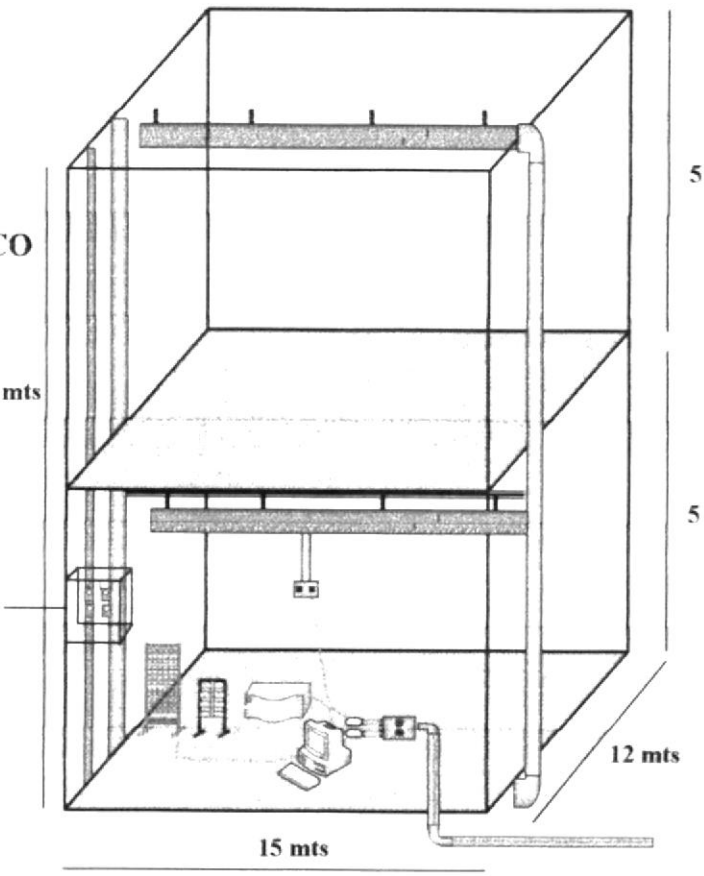
2.5.2 QUITO

El edificio Sucursal de la empresa "Compuhelp" cuenta con 2 pisos, sus dimensiones son de 10 m de alto, 15 m de ancho y 12 m de fondo, cada piso posee una altura de 5 m. Se maneja una velocidad de 100 MBPS en el backbone vertical.

Conexión a tierra:

El edificio cuenta con una conexión a tierra, lo que brinda mayor seguridad a los equipos en caso de una descarga o algún tipo de anomalía eléctrica imprevista, la misma que se encuentra ubicada del lado izquierdo del edificio (sector de los medidores).

GRÁFICO DEL EDIFICO COMPUHELP SUCURSAL QUITO



Leyenda:

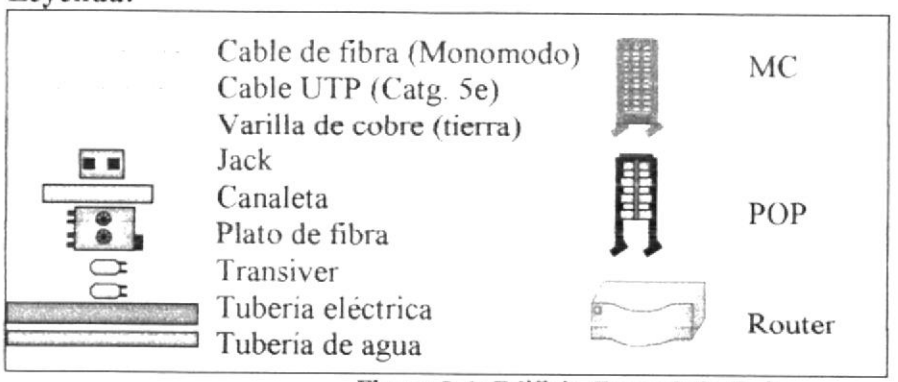


Figura 2-4: Edificio Compuhelp Quito

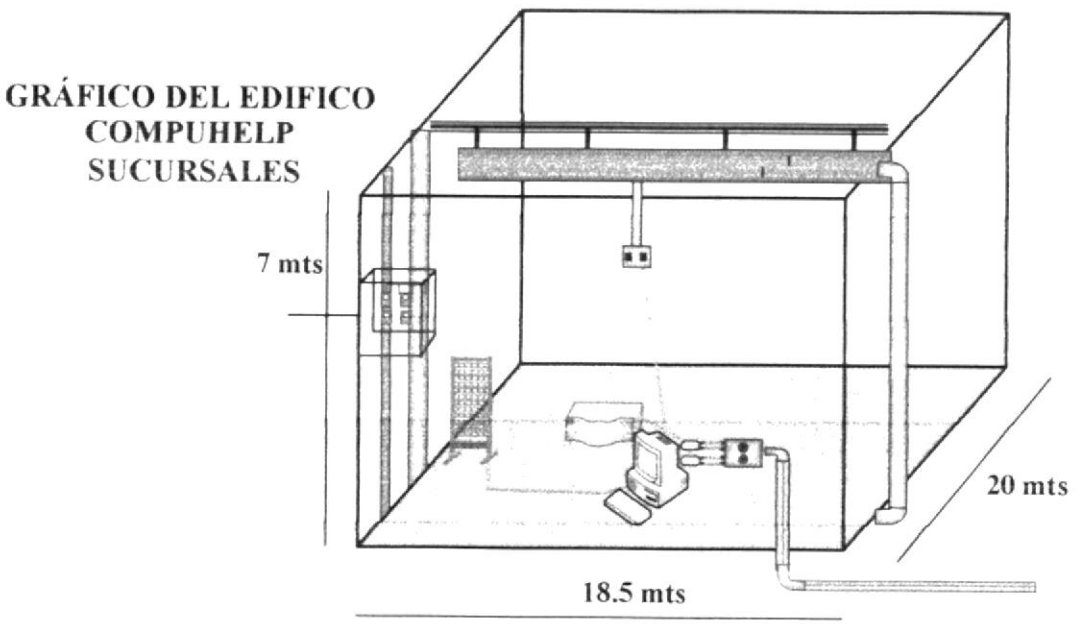
2.5.3 SUCURSALES

Los edificios de las Sucursales de la empresa "Compuhelp" cuentan con 1 piso, sus dimensiones son de 7 m de alto, 18.5 m de ancho y 20 m de fondo. Se maneja una velocidad de 100 MBPS en el backbone vertical. Todas las sucursales excepto Quito poseen la misma infraestructura debido a los estándares de la compañía.

Entre las Sucursales que mantiene los estándares de infraestructura tenemos: Cuenca, Manta, Salinas, Santo Domingo y Loja.

Conexión a tierra:

El edificio cuenta con una conexión a tierra, lo que brinda mayor seguridad a los equipos en caso de una descarga o algún tipo de anomalía eléctrica imprevista, la misma que se encuentra ubicada del lado izquierdo del edificio (sector de los medidores).



Leyenda:

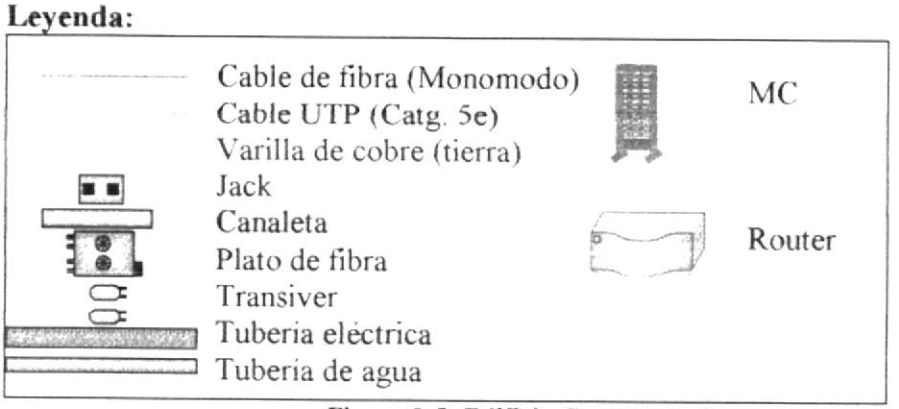


Figura 2-5: Edificio Compuhelp Sucursales

2.5.4 CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO

La empresa se ha destacado por mantener una estandarización en lo que se refiere a la implementación de equipos tanto en su matriz como en todas las sucursales. Dentro de toda la empresa se encuentran equipos de la reconocida marca como es Hewlett Packard.

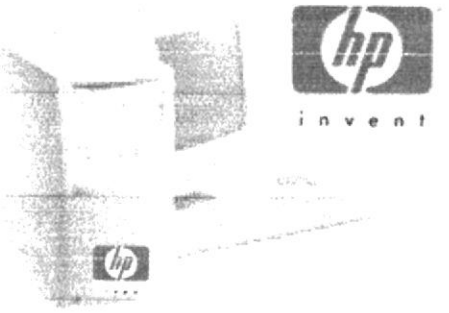


Figura 2-6: Estación de trabajo

2.5.4.1 MATRIZ (GUAYAQUIL)

En el Edificio Matriz Guayaquil encontramos 17 Computadoras.

2.5.4.2 SUCURSAL (QUITO)

En el Edificio Matriz Guayaquil encontramos 15 Computadoras.

2.5.4.3 SUCURSALES

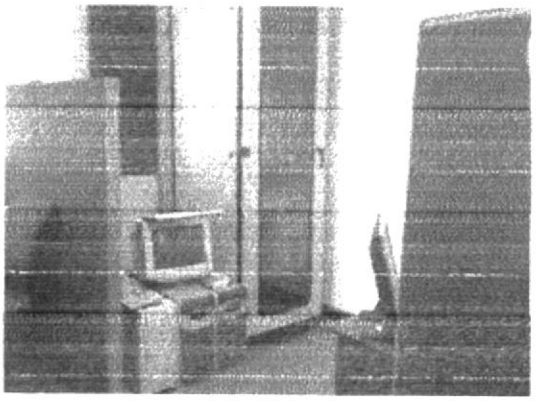
En el Edificio Matriz Guayaquil encontramos 13 Computadoras.

Características Generales que poseen todas las estaciones de trabajo en Matriz y Sucursales

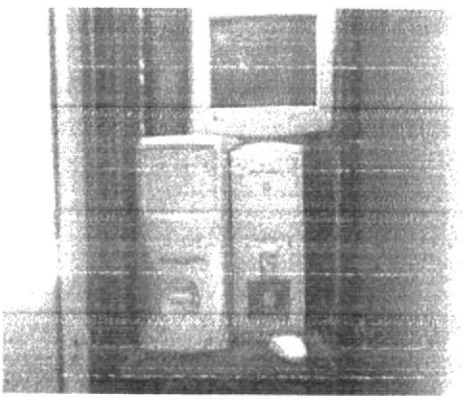
Procesador Intel Pentium IV de 3.0 GHz
Disco Duro de 80 GB 7200 rpm
Memoria RAM de 512 MB
Ethernet D-Link 10/100 Mbps

2.5.5 CARACTERÍSTICAS DE LOS SERVIDORES

Debemos mencionar que existe una estandarización referente a los servidores, ya que poseen las mismas caracteristicas a nivel de toda la empresa.



SERVER ISA
(FIREWALL)



SERVER DNS
(EXCHANGE 2003)

Figura 2-7: Servidores

2.5.5.1 MATRIZ (GUAYAQUIL)

1 Servidor de CORREO
1 servidor DNS
1 Servidor DHCP
1 Servidor WEB
1 Servidor ISA (Firewall)
1 Servidor de Base de Datos

2.5.5.2 SUCURSAL (QUITO)

1 Servidor CORREO
1 servidor DNS
1 Servidor WEB
1 Servidor DHCP
1 Servidor ISA (Firewall)
1 Servidor de Base de Datos

2.5.5.3 SUCURSALES

1 Servidor DHCP
1 Servidor ISA (Firewall)
1 Servidor de Base de Datos

Características Generales que poseen todos los servidores en Matriz y Sucursales

- Procesador Intel Pentium Xeon de 2.8 Ghz
- Memoria de 1 Ghz
- 2 Ethernet D-Link (DFE-530TX) 10/100/1000 Mbps.
- Arreglo de 4 discos Scosi (HD 89.9GB c/u)

2.5.6 GRÁFICO DEL MC

2.5.6.1 MATRIZ GUAYAQUIL

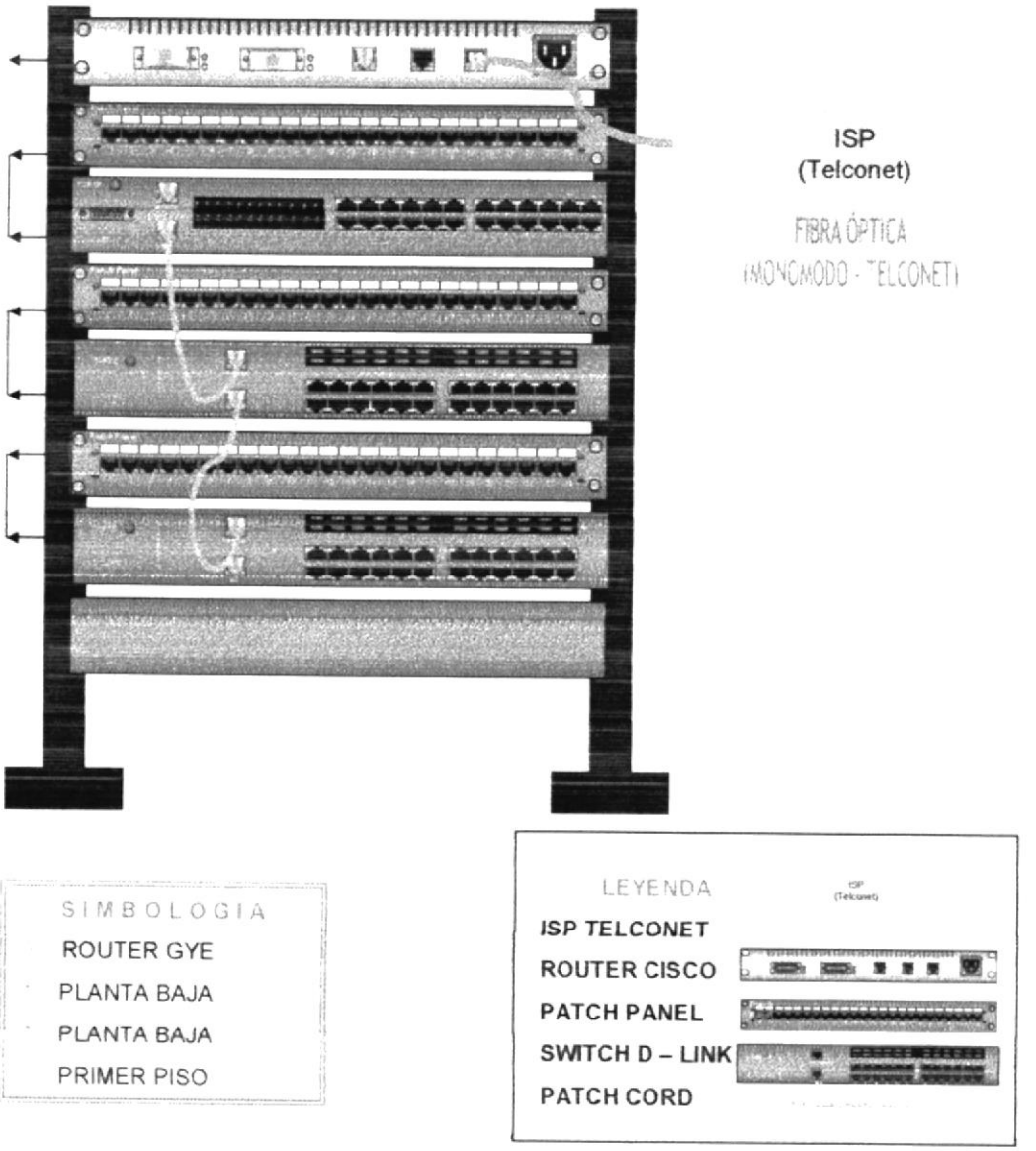
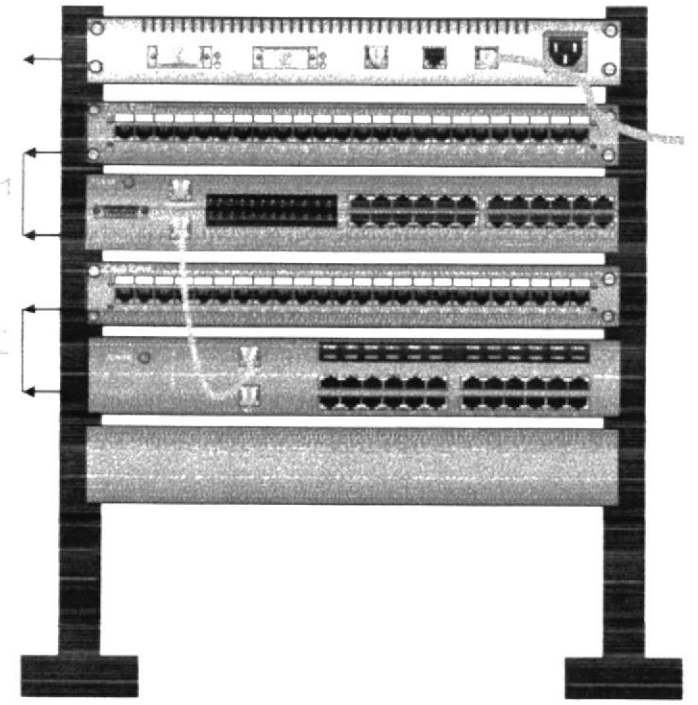


Figura 2-8: MC Matriz Guayaquil

2.5.6.2 SUCURSAL QUITO



ISP
(Telconet)

FIBRA ÓPTICA
(MONOMODO - TELCONET)

SIMBOLOGÍA
ROUTER UIO
PLANTA BAJA
PRIMER PISO

LEYENDA
ISP TELCONET
ROUTER CISCO
PATCH PANEL
SWITCH D – LINK
PATCH CORD

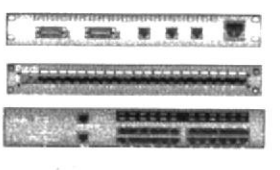
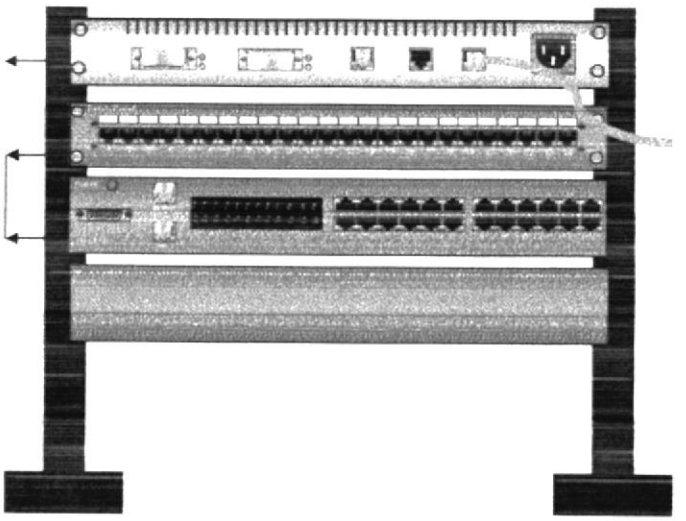


Figura 2-9: MC Sucursal Quito

2.5.6.3 SUCURSALES



ISP
(Telconet)

FIBRA ÓPTICA
(MONOMODO - TELCONET)

SIMBOLOGIA

ROUTER SUCURSALES
CUENCA, LOJA, MANTA,
STO. DOMINGO, SALINAS.
PLANTA BAJA

LEYENDA

ISP TELCONET
ROUTER CISCO
PATCH PANEL
SWITCH D – LINK
PATCH CORD

NOTA:

Mencionamos que así como todas las sucursales poseen una misma estructura, de la misma forma, poseen los Patch Panel, debido a que mantienen una estandarización dentro del negocio (Proyección hacia un futuro).

Figura 2-10: MC Sucursales

2.5.7 DISTRIBUCIÓN DEL CABLEADO

2.5.7.1 MATRIZ - GUAYAQUIL

La infraestructura del edificio Matriz Guayaquil cuenta con lo siguiente:

Por el backbone horizontal de la planta baja pasan 24 cables UTP Categoría 5e y por el primer piso pasan 15 cables UTP Categoría 5e que se distribuyen en las distintas áreas mediante canaletas.

Cableado Horizontal y Vertical

- Cable UTP categoria 5e sin blindar

2.5.7.2 SUCURSALES

La infraestructura de los edificios de las sucursales a nivel nacional de la empresa Compuhelp se rige bajo una estandarización es por eso que cuenta con lo siguiente:

Cableado Horizontal y Vertical

- Cable UTP categoría 5e sin blindar

2.5.8 ANÁLISIS DE PISO LÓGICO

2.5.8.1 MATRIZ (GUAYAQUIL)

2.5.8.1.1 PLANTA BAJA

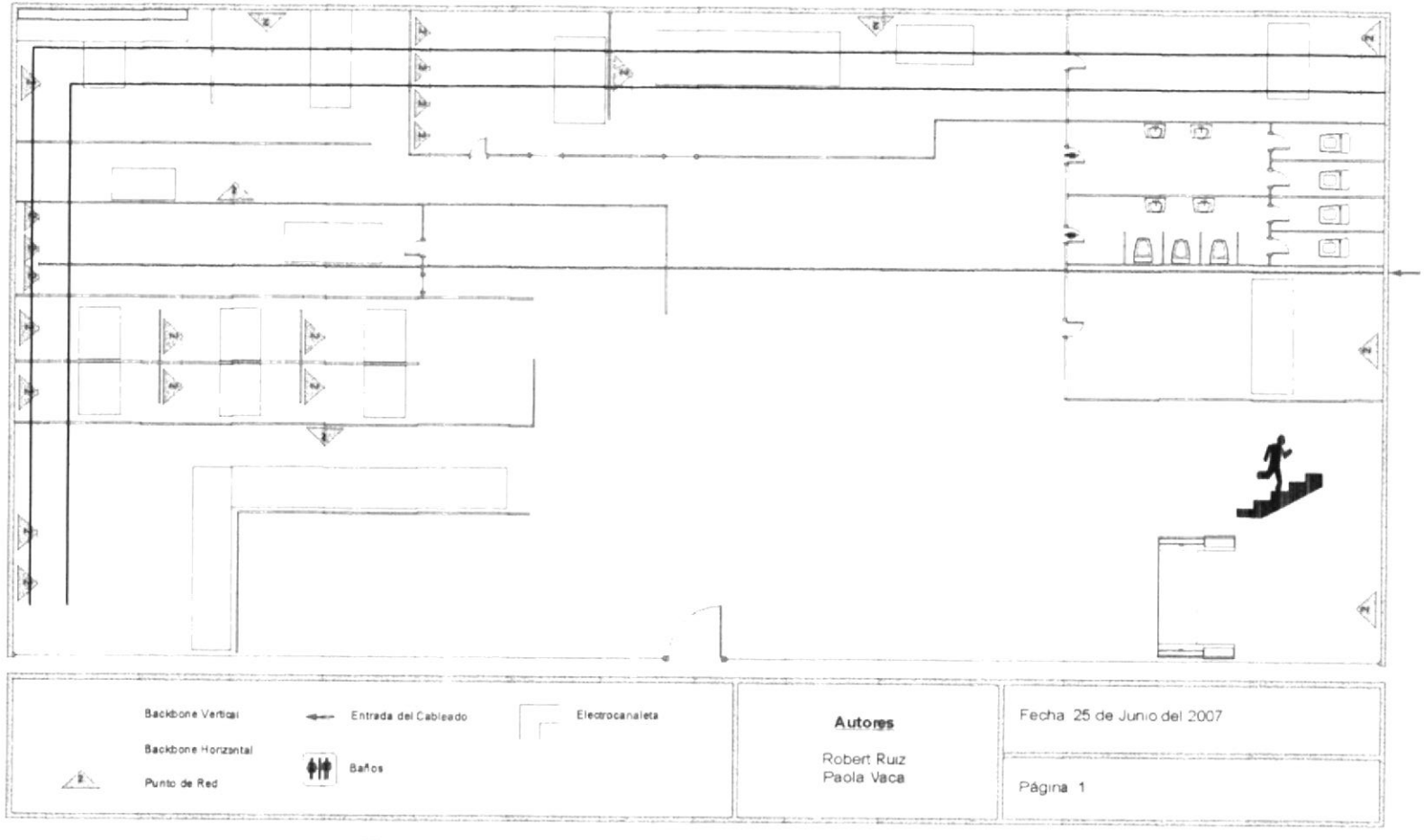


Figura 2-11: Análisis de Piso Lógico – Edificio Matriz (Planta Baja)

2.5.8.1.2 PRIMER PISO

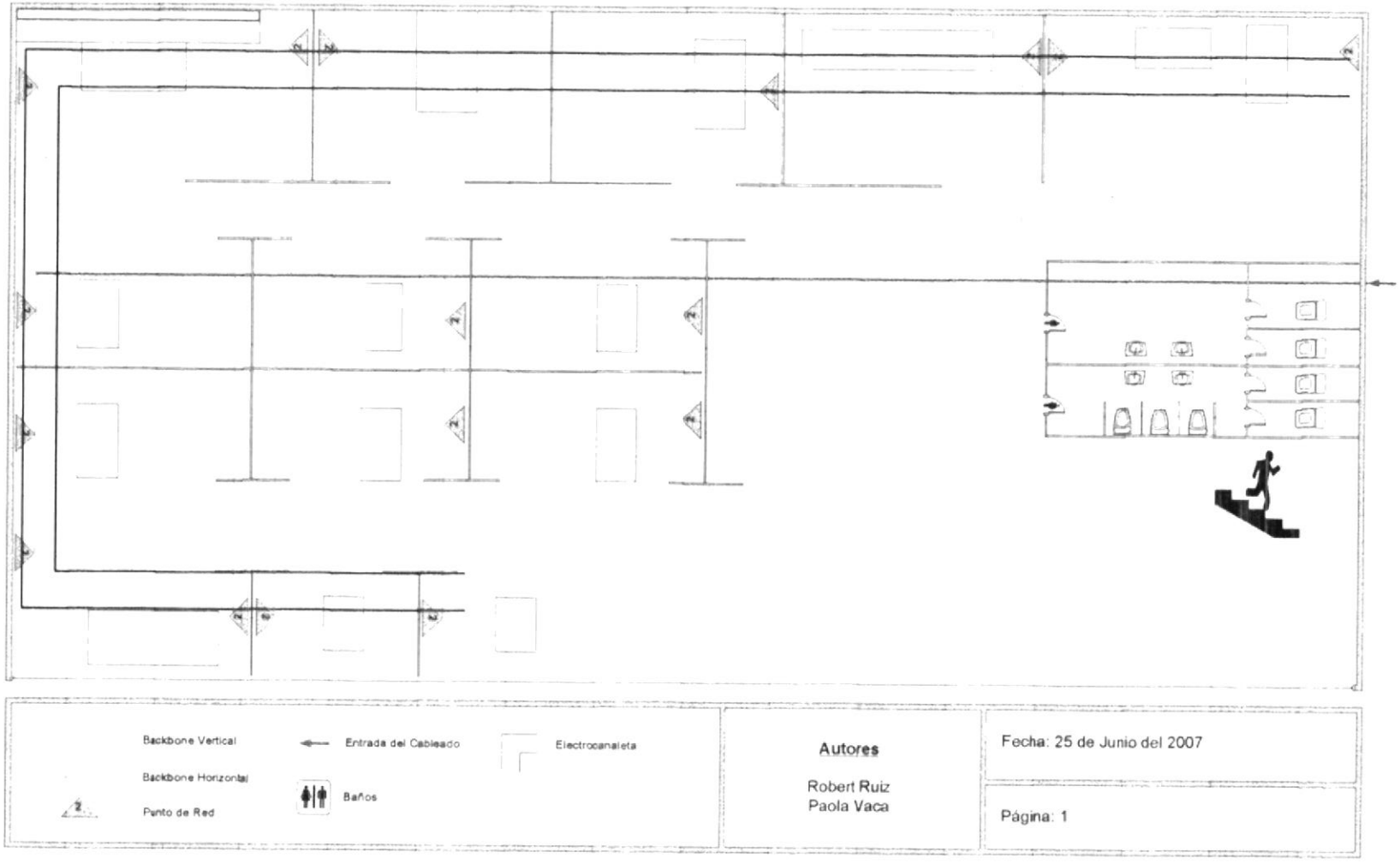


Figura 2-12: Análisis de Piso Lógico – Edificio Matriz (Primer Piso)

2.5.8.2 SUCURSAL (QUITO)
2.5.8.2.1 PLANTA BAJA

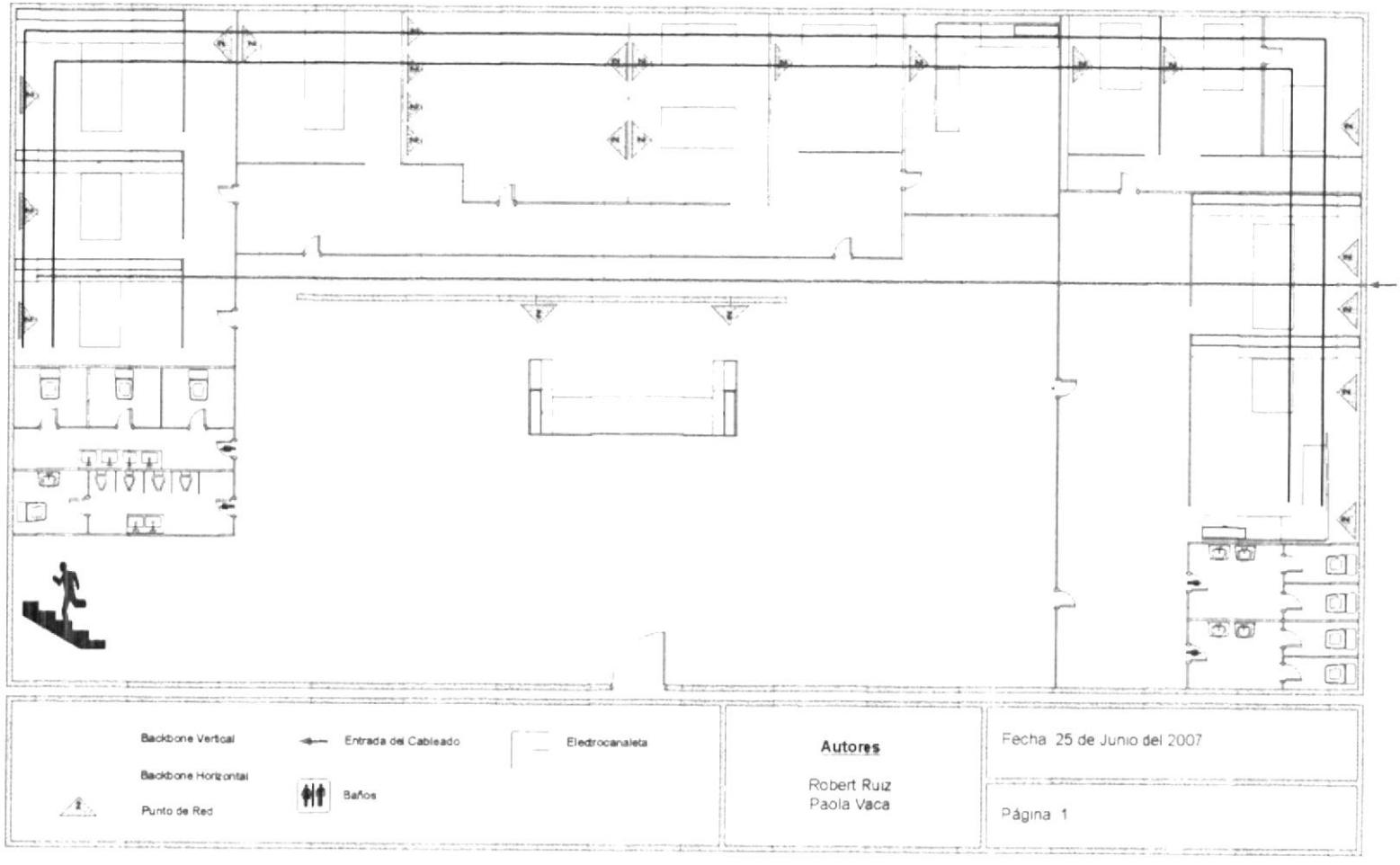


Figura 2-13: Análisis de Piso Lógico – Sucursal Quito (Planta Baja)

2.5.8.2.2 PRIMER PISO

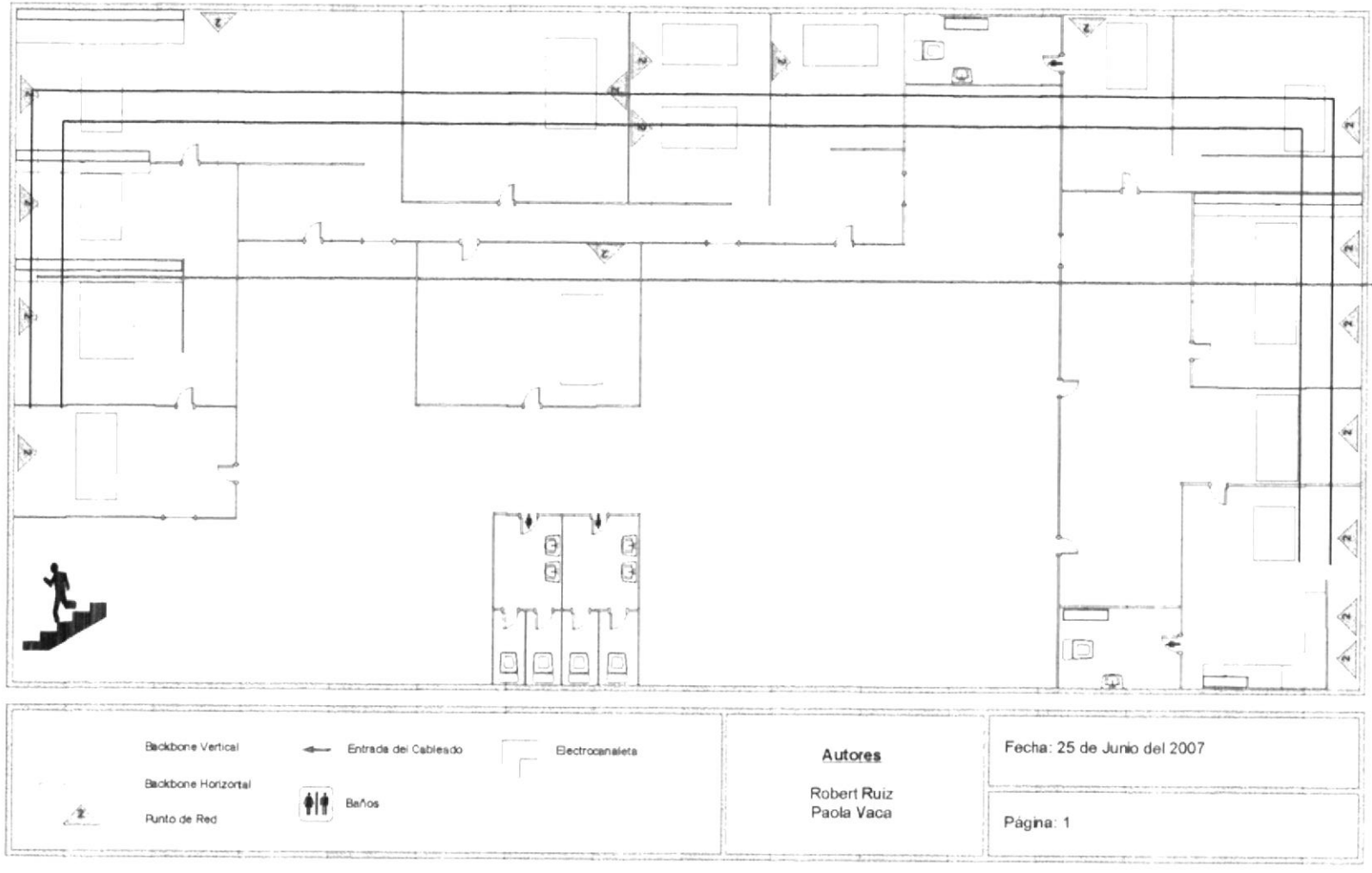


Figura 2-14: Análisis de Piso Lógico – Sucursal Quito (Primer Piso)

2.5.8.3 SUCURSALES
2.5.8.3.1 PLANTA BAJA

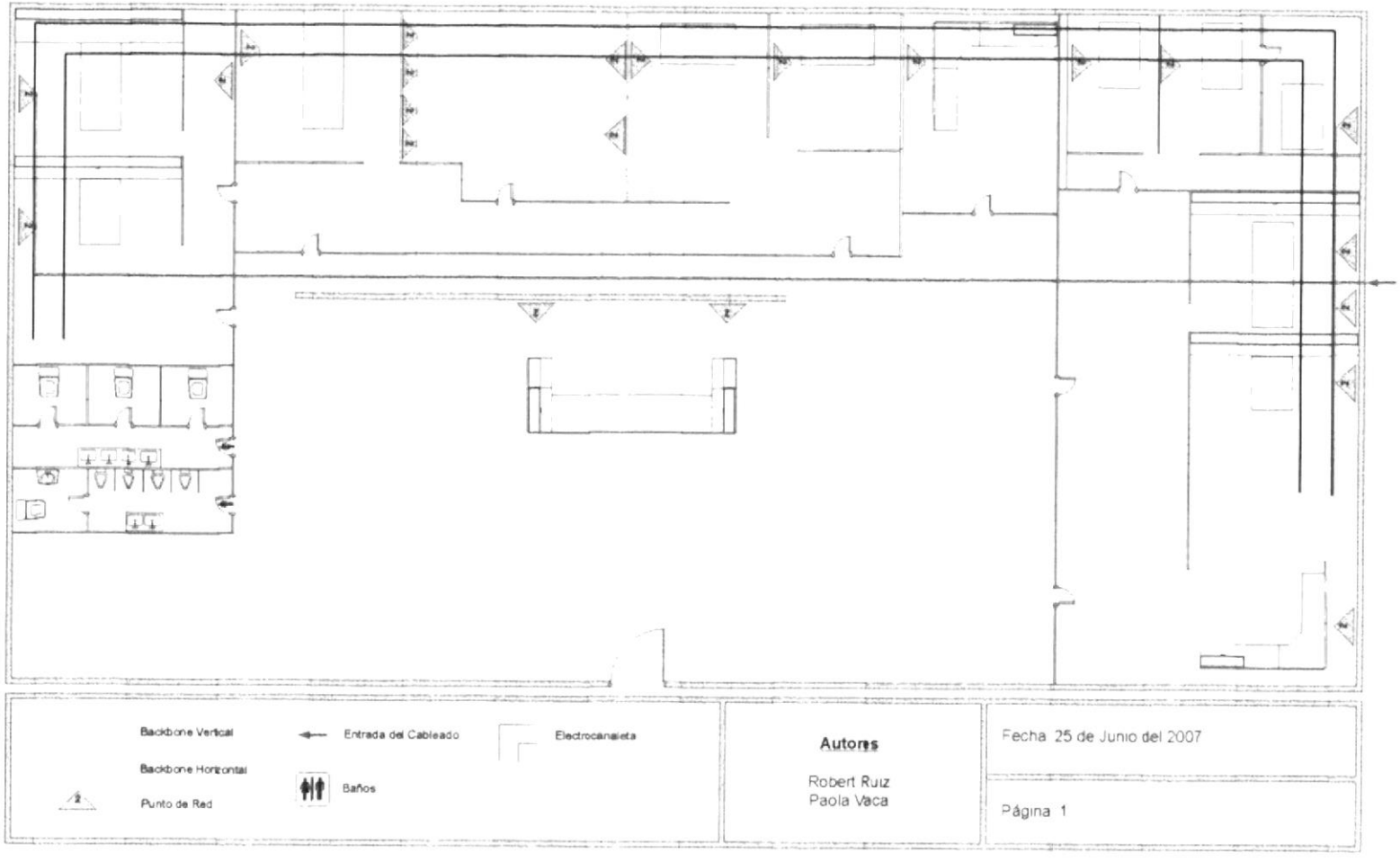


Figura 2-15: Análisis de Piso Lógico – Sucursales (Planta Baja)

2.5.9 ANÁLISIS DE PISO APLICATIVO

2.5.9.1 MATRIZ (GUAYAQUIL)

2.5.9.1.1 PLANTA BAJA

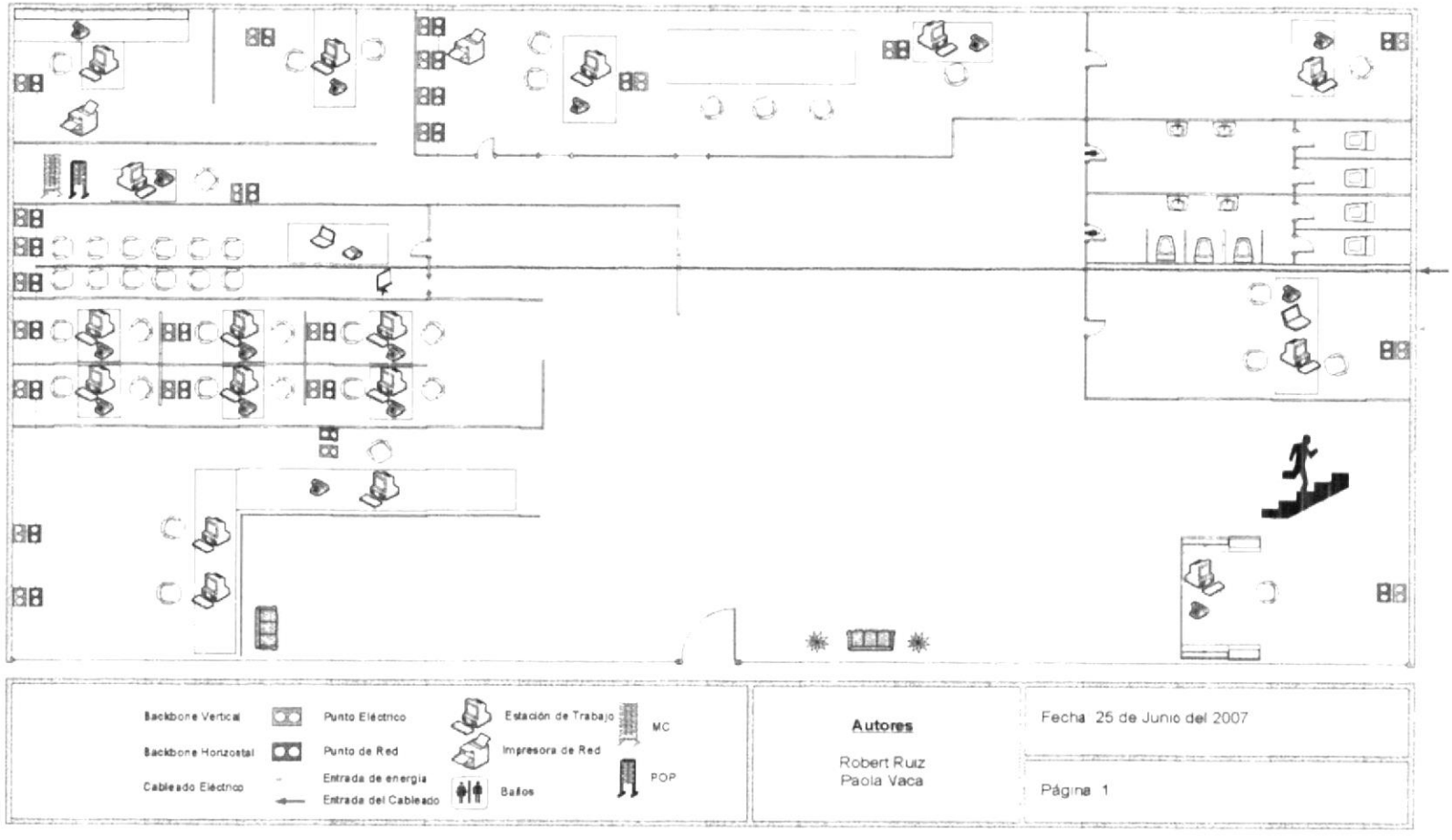


Figura 2-16: Análisis de Piso Aplicativo – Edificio Matriz (Planta Baja)

2.5.9.1.2 PRIMER PISO

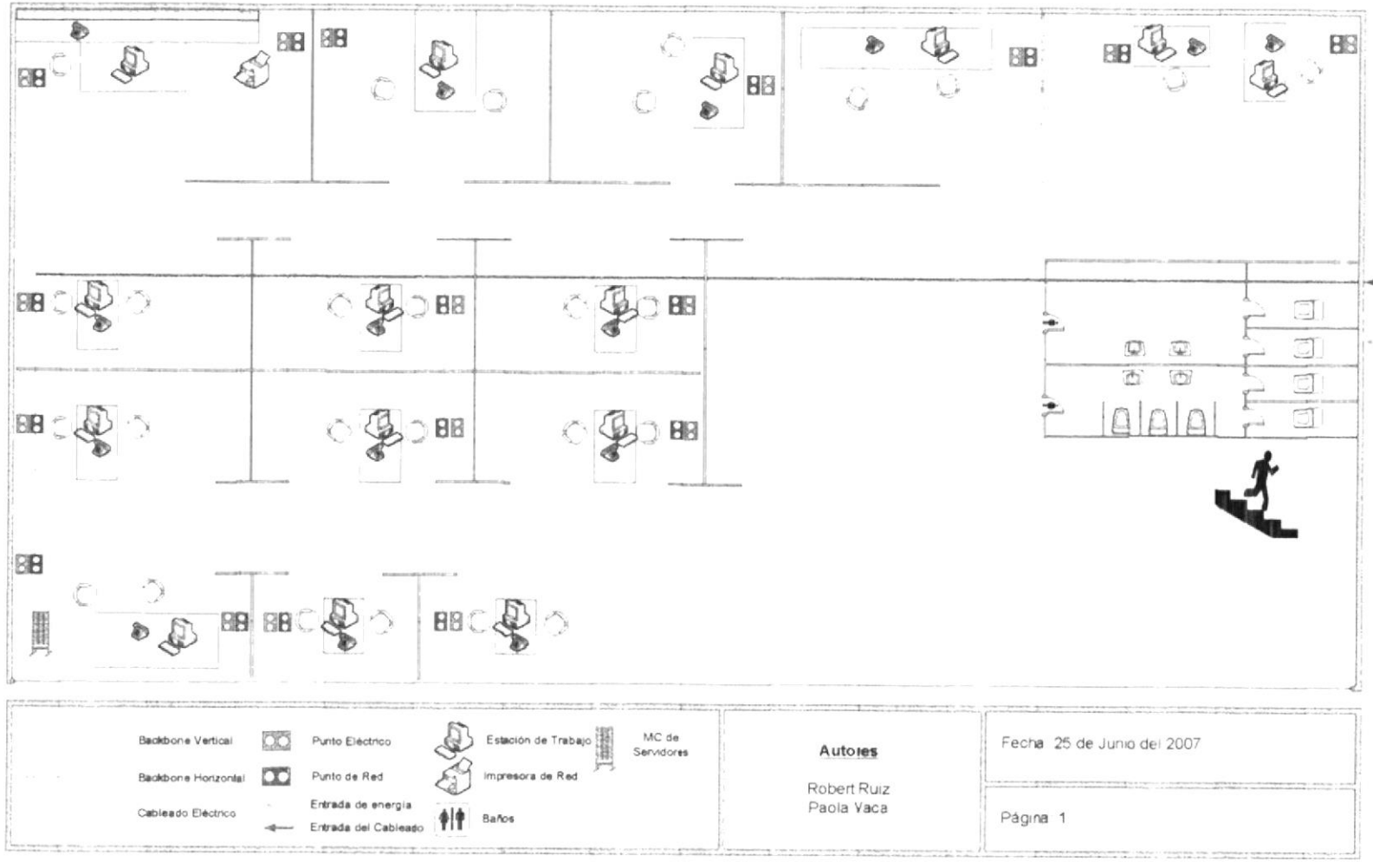


Figura 2-17: Análisis de Piso Aplicativo – Edificio Matriz (Primer Piso)

2.5.9.2 SUCURSAL (QUITO)
2.5.9.2.1 PLANTA BAJA

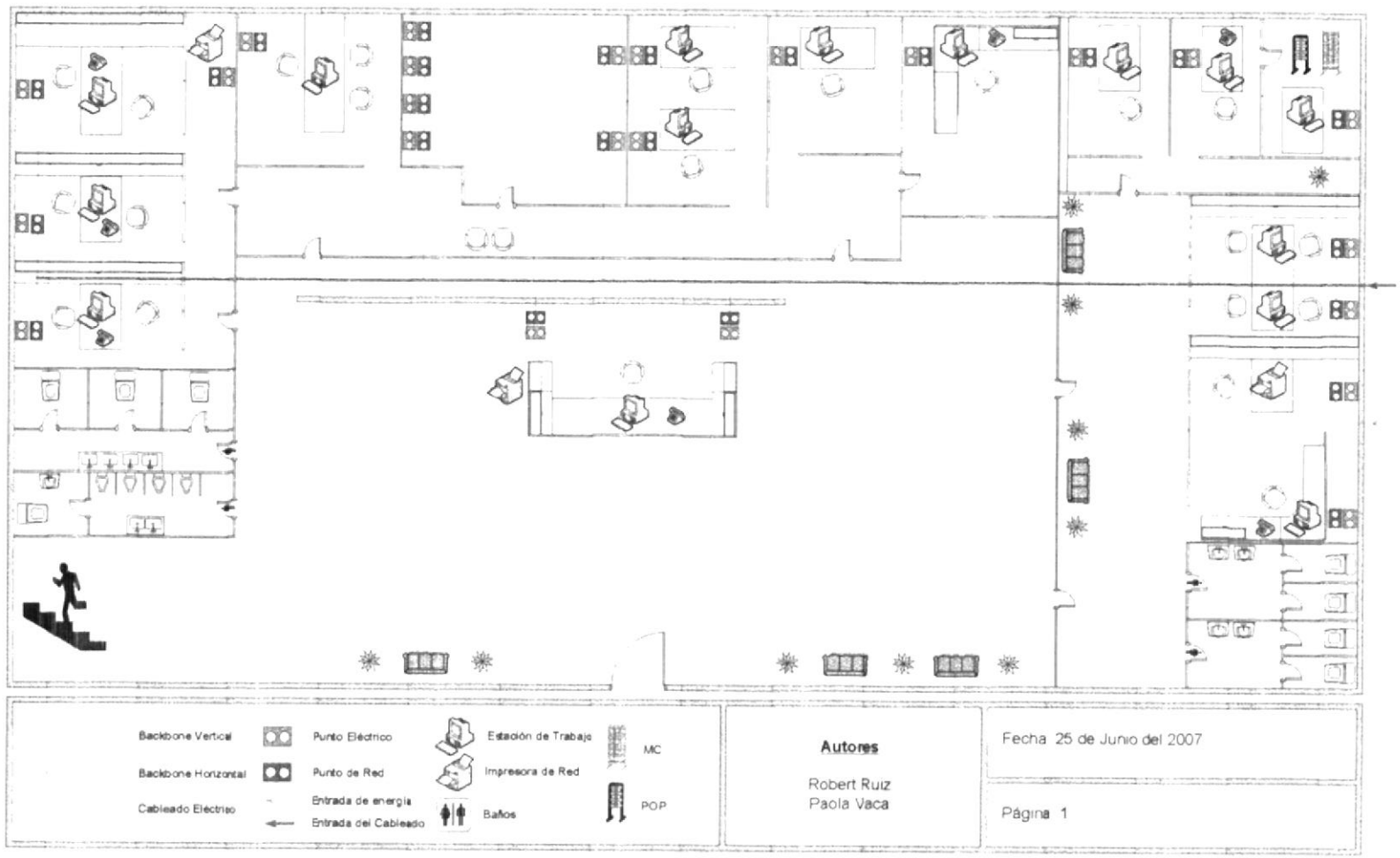


Figura 2-18: Análisis de Piso Aplicativo – Sucursal Quito (Planta Baja)

2.5.9.2.2 PRIMER PISO

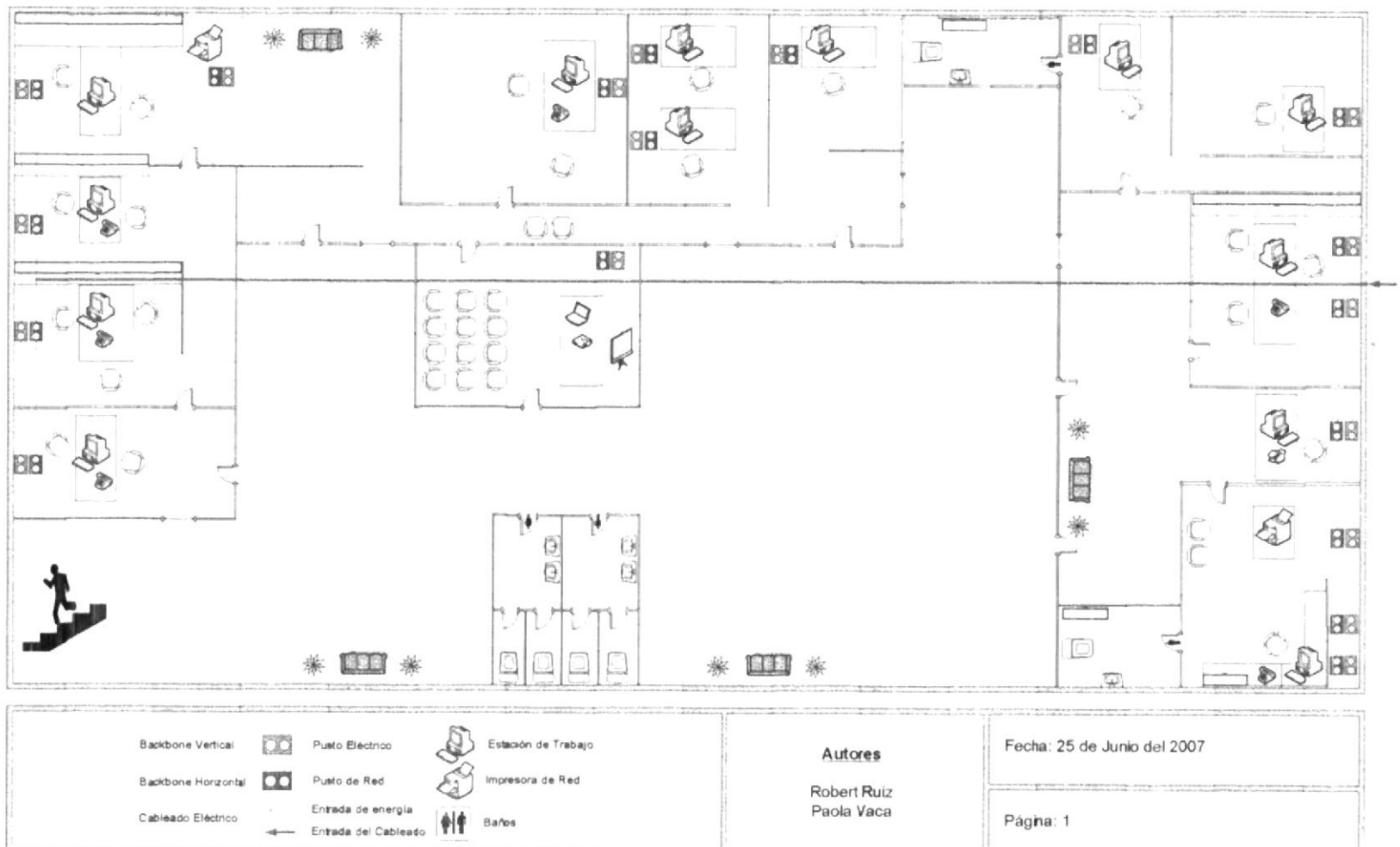


Figura 2-19: Análisis de Piso Aplicativo – Sucursal Quito (Primer Piso)

2.5.9.3 SUCURSALES
2.5.9.3.1 PLANTA BAJA

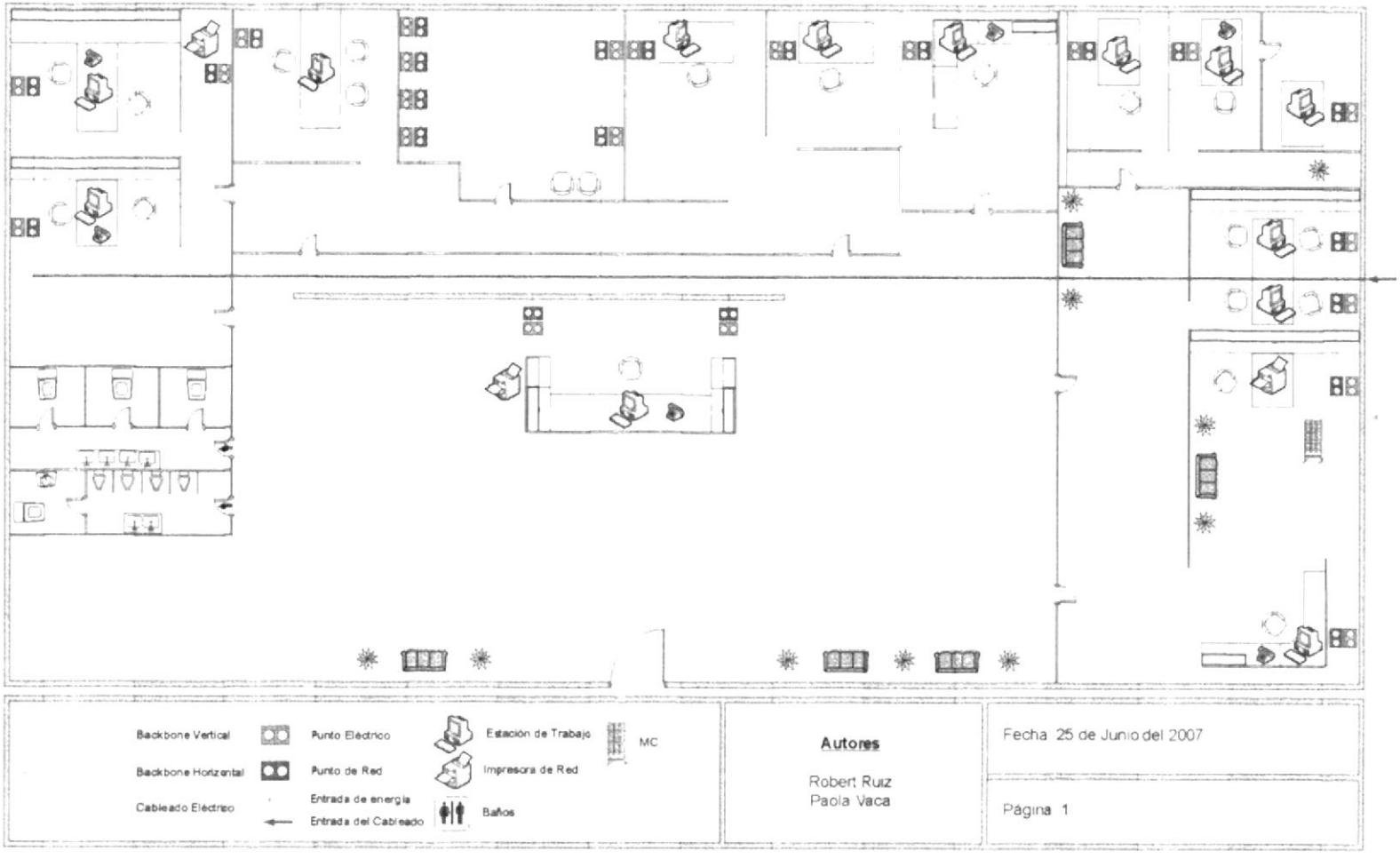
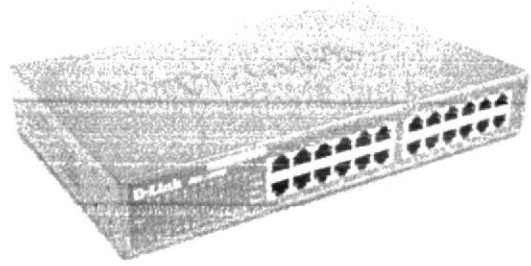


Figura 2-20: Análisis de Piso Aplicativo – Sucursales (Planta Baja)

2.6 DISPOSITIVOS DE CONMUTACIÓN



Switch D-Link DES 1024D
Fast Ethernet Switch
10/100 Mbps

Figura 2-21: Dispositivos de Conmutación

2.6.1 MATRIZ

En la planta baja de la Matriz, se encuentran 3 Switches de 24 puertos marca D – Link. Velocidad de 10/100 Mbps, los cuales se encuentran ubicados en el MC de donde sale la distribución del cableado para las diferentes áreas de la empresa.

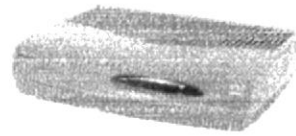
2.6.2 SUCURSALES

En cada Sucursal, encontramos 2 Switches de 24 puertos marca D – Link, con una velocidad de 10/100 Mbps.

Nota:
Debido a la estandarización de la empresa se mantienen las mismas características de los dispositivos de comunicación.

2.7 INFRAESTRUCTURA WAN

2.7.1 DISPOSITIVOS DE ENRUTAMIENTO



CISCO 1750

Figura 2-22: Dispositivos de Enrutamiento

2.7.1.1 MATRIZ (GUAYAQUIL)

Se encuentra 1 Router marca CISCO, este router pertenece a la compañía telconet (Proveedores del servicio de Internet), este router es administrado únicamente por los proveedores.

2.7.1.2 SUCURSALES

Todas las sucursales poseen 1 Router marca CISCO, estos routers pertenecen a la compañía telconet (Proveedores del servicio de Internet).

Características Generales de los Routers (Matriz y Sucursales):

- 2 Wics de Ranuras de las tarjetas de interfaz Wan.
- Ranura para modulo de red
- Ranura del modulo de integración avanzado
- Rendimiento entre 15 y 25 Kbps.

2.7.2 COMUNICACIÓN MATRIZ SUCURSALES

2.7.2.1 GRÁFICO DE MEDIOS WAN

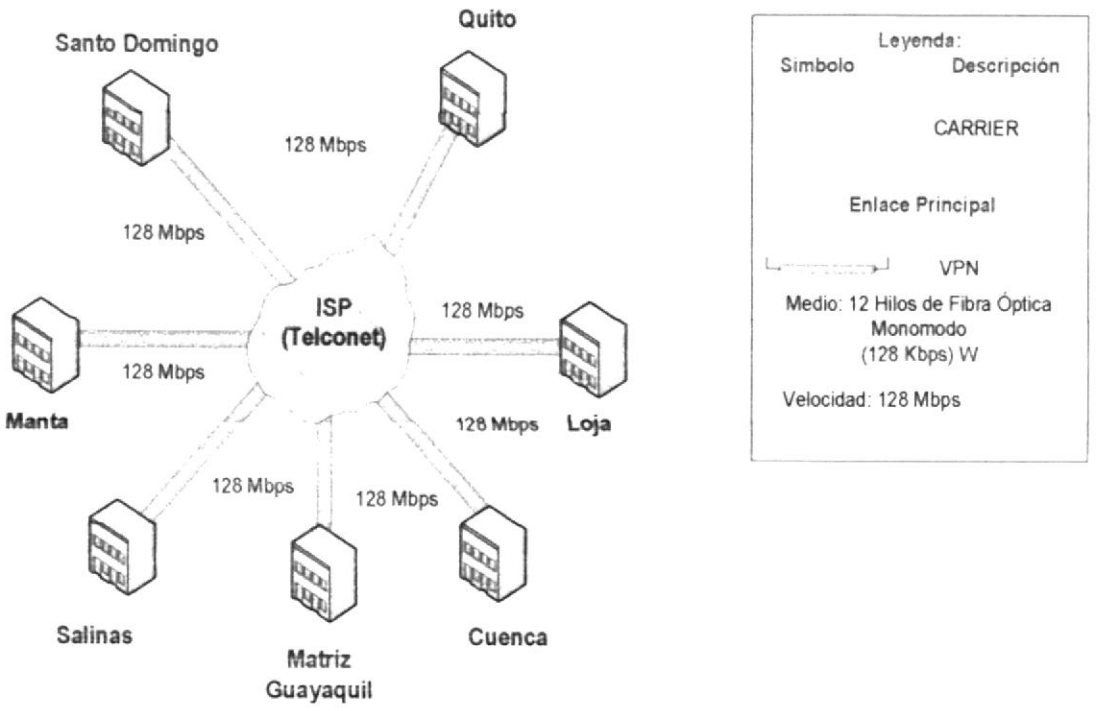


Figura 2-23: Gráfico de Medios Wan

2.7.2.2 GRÁFICO DE COMUNICACIÓN DE DISPOSITIVOS WAN

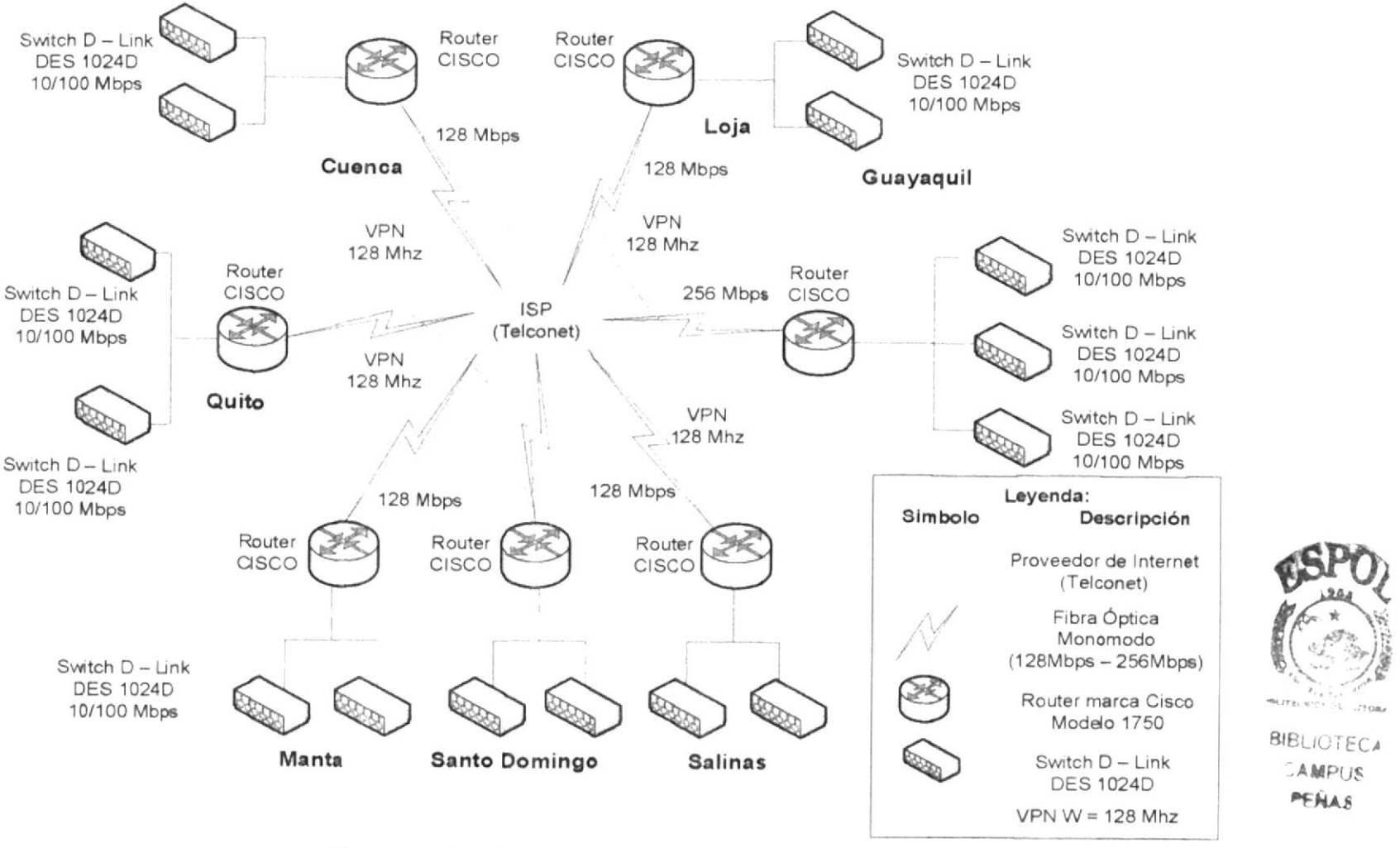


Figura 2-24: Gráfico de comunicación de dispositivos Wan

2.8 SEGURIDADES

2.8.1 FIREWALL

La empresa Compuhelp cuenta con un servidor ISA en la Matriz y en cada una de las sucursales, en este servidor se encuentran las configuraciones Proxy (Firewall). Este se encarga del reconocimiento de varios protocolos para lograr una filtración de alta calidad.

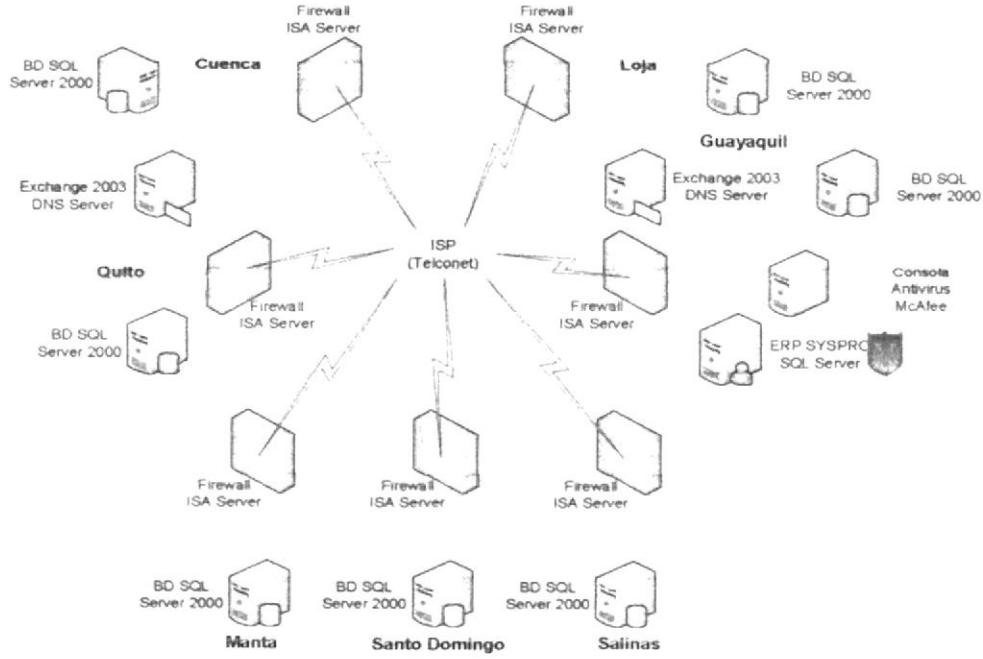


Figura 2-25: Gráfico de Seguridades (Firewall)

2.8.2 ANTIVIRUS

Cuentan con un excelente software denominado McAfee, es esencial ya que garantiza que el contenido que entra y sale de la empresa obedezca las políticas de seguridad y normas de privacidad.

Las amenazas usan más de un protocolo para infiltrarse en las redes. Reconocerlos es fundamental para garantizar que todos los protocolos estén protegidos y seguros.

- La revisión de SMTP protege el tráfico de e-mails.
- La revisión de HTTP protege el tráfico de la web. También protege a los usuarios que poseen cuentas personales en Internet.
- La revisión de POP3 protege el tráfico de e-mails por Internet cuando los usuarios utilizan las PC de la empresa para leer e-mails de sus cuentas personales.

Figura 2-26: Antivirus

2.9 ACCESO A INTERNET

SERVICIOS DE INTERNET DEDICADO POR FIBRA ÓPTICA

Este servicio le proporciona una conexión permanente a Internet y le permite configurar las opciones de acuerdo a las necesidades específicas de la empresa.

Los servicios de Internet Dedicado de Telconet, brindan una de las redes más avanzadas en el Ecuador, basadas en tecnología de alta velocidad, cuenta con todos los servicios de un Centro de Operaciones de Red (NOC), interconexión al NAP Local en Ecuador y al NAP Internacional en Miami, redundancia de plataforma y redundancia de interconexión internacional entre muchos otros servicios, que aseguran una respuesta óptima con altos estándares internacionales tanto tecnológicos como de servicio al cliente. La conexión es mediante fibra óptica monomodo con una velocidad de 256 Mbps para Guayaquil, de 128 Mbps para las sucursales y con un ancho de banda de 128 Kbps.

Gráfico de Acceso a Internet

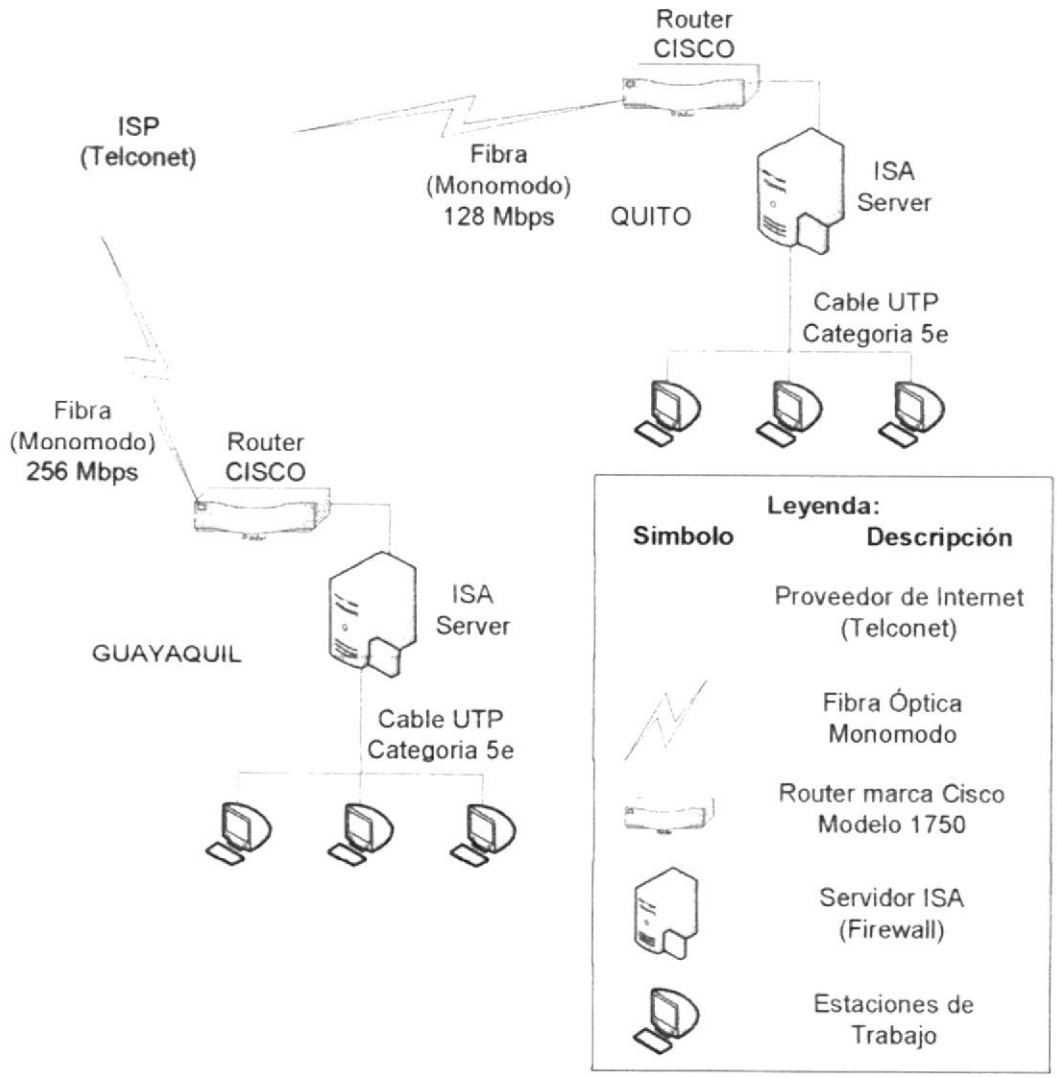


Figura 2-27: Acceso a Internet

2.10 PROBLEMAS ENCONTRADOS

Luego del análisis realizado a la empresa Compuhelp, se llego a la conclusión de que existen los siguientes problemas:

- No existe una comunicación directa entre Matriz y Sucursales (Comunicación VPN)
- No poseen enlaces de respaldo a nivel de la WAN.
- No cuentan con dispositivos propios de ruteo.
- Sobrecarga de los puntos eléctricos. (Matriz - Guayaquil)

CAPÍTULO 3

SOLUCIÓN PROPUESTA

3. SOLUCIÓN PROPUESTA

3.1 PROBLEMAS ENCONTRADOS

Problema	Causa	Efecto
No existe una comunicación directa entre Matriz y Sucursales (Enlaces VPN).	No se visualizo a futuro las necesidades de la empresa.	Complejidad de acceso al momento de comunicarse la Matriz con las Sucursales.
No poseen enlaces de respaldo a nivel de la WAN.	No se ha invertido en infraestructura WAN. (Medios de Comunicación Backup)	Perdida de paquetes de datos cuando colapsan los enlaces WAN.
No cuentan con dispositivos propios de ruteo.	No se ha invertido en infraestructura WAN. (Dispositivos de Comunicación)	Costos muy elevados. Seguridad de información depende de terceros.
Sobrecarga de los puntos eléctricos. (Matriz - Guayaquil)	No se visualizo a futuro el crecimiento de la empresa	Daños Eléctricos a las estaciones de trabajo.

Tabla 3-1: *Problemas encontrados* en Compuhelp

3.2 SOLUCIÓN PROPUESTA

Problema	Solución	Alcance
No existe una comunicación directa entre Matriz y Sucursales (Enlaces VPN).	*Implementación* de fibra óptica en los enlaces principales y microondas en los enlaces secundarios.	Mejores Tiempos de Respuestas. Respaldo en la transmisión de datos.
No poseen enlaces de respaldo a nivel de la WAN.	Adquisición de Medios WAN. (Fibra Óptica Monomodo - VPN)	Prevención de pérdida de datos cuando ocurra un imprevisto dentro de la comunicación WAN.
No cuentan con dispositivos propios de ruteo.	Adquisición de Dispositivos WAN (Ruteadores)	Mejora el rendimiento de los enlaces WAN.
Sobrecarga de los puntos eléctricos. (Matriz - Guayaquil)	Balance de cargas de voltaje en los brekes y restauración del tendido eléctrico.	Evitar daños eléctricos a las estaciones de trabajo.

Tabla 3-2: Solución Propuesta

3.3 ESTUDIO DE LA FACTIBILIDAD

3.3.1 ALTERNATIVA "A"

De acuerdo al estudio de nuestro análisis realizado a la empresa Compuhelp, se sugiere que con la adquisición de fibra óptica para los enlaces principales y de antenas microondas para los enlaces secundarios, con lo cual mejoraremos la seguridad de la información en la red WAN.

3.3.1.1 FACTIBILIDAD TÉCNICA

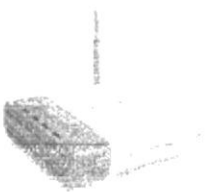
Cantidad	Descripción	Imagen	Ubicación
12	Antenas microondas Unidireccional 120° Frecuencia 2.4 Ghz, ganancia 2.4 Dbi		Matriz Guayaquil Sucursal Quito Sucursal Cuenca Sucursal Loja Sucursal Salinas Sucursal Manta Sucursal Santo Domingo
3	Fibra Óptica monomodo, 12 hilos, 10/125 micras		Matriz Guayaquil Sucursal Quito Sucursal Cuenca
7	Ruteadores 2 Puertos Eth0 10/100 Mbps 3 Slot para tarjetas Wic de interface Wan		Matriz Guayaquil Sucursal Quito Sucursal Cuenca Sucursal Loja Sucursal Salinas Sucursal Manta Sucursal Santo Domingo
7	Access Point Punto de acceso inalámbrico Banda de frecuencia: 2.4 GHz Alcance máximo en interior: 200 m		Matriz Guayaquil Sucursal Quito Sucursal Cuenca Sucursal Loja Sucursal Salinas Sucursal Manta Sucursal Santo Domingo

Tabla 3-3: Factibilidad Técnica "A"

3.3.1.2 FACTIBILIDAD ECONÓMICA

Cantidad	Descripción	Costo Unitario (Dólares)	Costo Total (Dólares)
12	Antenas microondas Unidireccional 120° Frecuencia 2.4 Ghz, ganancia 2.4 Dbi	$ 225	$ 2700
3	Fibra Óptica monomodo, 12 hilos, 10/125 micras Incluye: Instalación de todos los enlaces que se requieren	$ 1200	$ 7200
7	Ruteadores 2 Puertos Eth0 10/100 Mbps 3 Slot para tarjetas Wic de interface Wan	$ 800	$ 5600
7	Access Point Banda de frecuencia: 2.4 GHz	$ 75	$ 525
Total			$ 16025

Tabla 3-4: Factibilidad Económica "A"

3.3.1.3 FACTIBILIDAD OPERATIVA

Fase	Duración / Semanas
Fase de Análisis de la red Lan y Wan 1 Ingeniero en Telecomunicaciones 1 Técnico en Redes	2
Fase de Diseño de la red Wan 1 Ingeniero en Telecomunicaciones	1
Fase de Implementación de la red Wan 1 Ingeniero en Telecomunicaciones 4 Técnicos en Redes	4
Fase de Prueba de la red Wan 1 Ingeniero en Telecomunicaciones 4 Técnicos en Redes	4
Fase de Documentación de la red Wan 1 Ingeniero en Telecomunicaciones 1 Técnico en Redes	1

Tabla 3-5: Factibilidad Operativa "A"

3.3.1.4 COSTOS OPERATIVOS

Fase	Duración Semanas	Costo Semanas (Dólares)	Costo Total (Dólares)	Costo Fase (Dólares)
Fase de Diseño de la red Wan 1 Ingeniero en Telecomunicaciones	1	$ 200	$ 200	$ 200
Fase de Implementación de la red Wan 1 Ingeniero en Telecomunicaciones 4 Técnicos en Redes	4	$ 200 $ 70	$ 800 $ 1120	$ 1920
Fase de Prueba de la re Wan 1 Ingeniero en Telecomunicaciones 4 Técnicos en Redes	4	$ 200 $ 70	$ 800 $ 1120	$ 1920
Fase de Documentación de la red Wan 1 Ingeniero en Telecomunicaciones 1 Técnico en Redes	1	$ 200 $ 70	$ 200 $ 140	$ 340
Costo Total Operativo				$ 4380

Tabla 3-6: Costos Operativos "A"

3.3.1.5 COSTO TOTAL DE LA ALTERNATIVA "A"

Dentro de esta alternativa incluimos los imprevistos.

Descripción	Costo Total (Dólares)
Factibilidad Económica	$ 16025
Servicios Profesionales	$ 4380
Total	**$ 20405**
Iva 12%	**$ 2448.6**
Costo total de la Propuesta	**$ 22853.6**

Tabla 3-7: Costo total de la alternativa "A"

3.3.1.6 VENTAJAS

- Transmisión de información por medios seguros.
- Mayores tiempos de respuestas en la transmisión de datos.
- Comunicación directa entre la Matriz con las Sucursales.
- Al tener los enlaces WAN por microondas se establece una conexión segura y con sus respectivos respaldos mediante VPN.
- Mejor infraestructura WAN para un futuro crecimiento de la empresa.

3.3.1.7 BENEFICIOS

- Mejor atención a clientes.
- Modernización de la empresa, con nuevas tecnologías.

3.3.1.8 GARANTÍA

La compañía FAST SOLUTIONS S.A. ofrece una garantía técnica de 6 meses, que incluye:

Figura 3-1: Logo de Fast Solutions

1. Soporte y seguimiento a las redes WAN.
2. Falla de comunicación.
3. Enlaces WAN muy lentos.

Valores que no cubre la garantía:

1. En caso de perdida de los enlaces por mala administración de la red WAN por parte de los técnicos de su empresa.
2. Al presentarse un problema dentro de la WAN y tratar de solucionarlo por sus propios medios, debiendo comunicarse inmediatamente con FAST SOLUTIONS S.A.

Nota:
Si se presenta uno de estos casos y de no respetar las cláusulas de la garantía, tendrá que cancelar los valores, por la revisión y solución del problema presentado.

3.3.1.9 FORMA DE PAGO DE LA ALTERNATIVA "A"

A continuación detallaremos la forma de pago mediante el cual se cancelarán los valores por el estudio realizado a su prestigiosa empresa.

- Después de la aceptación de la propuesta se receptara, el 60% del valor total de la propuesta, que corresponde a un monto de $ 13712.16 en la fecha del 11 de Julio del 2007.

- Al comenzar la fase de prueba se receptara el valor pendiente a cancelar, que es el 40% del valor total de la propuesta, que corresponde a un monto de $ 9141.44 en la fecha del 17 de Agosto del 2007.

3.3.1.10 DIAGRAMA DE GANTT DE LA ALTERNATIVA "A"

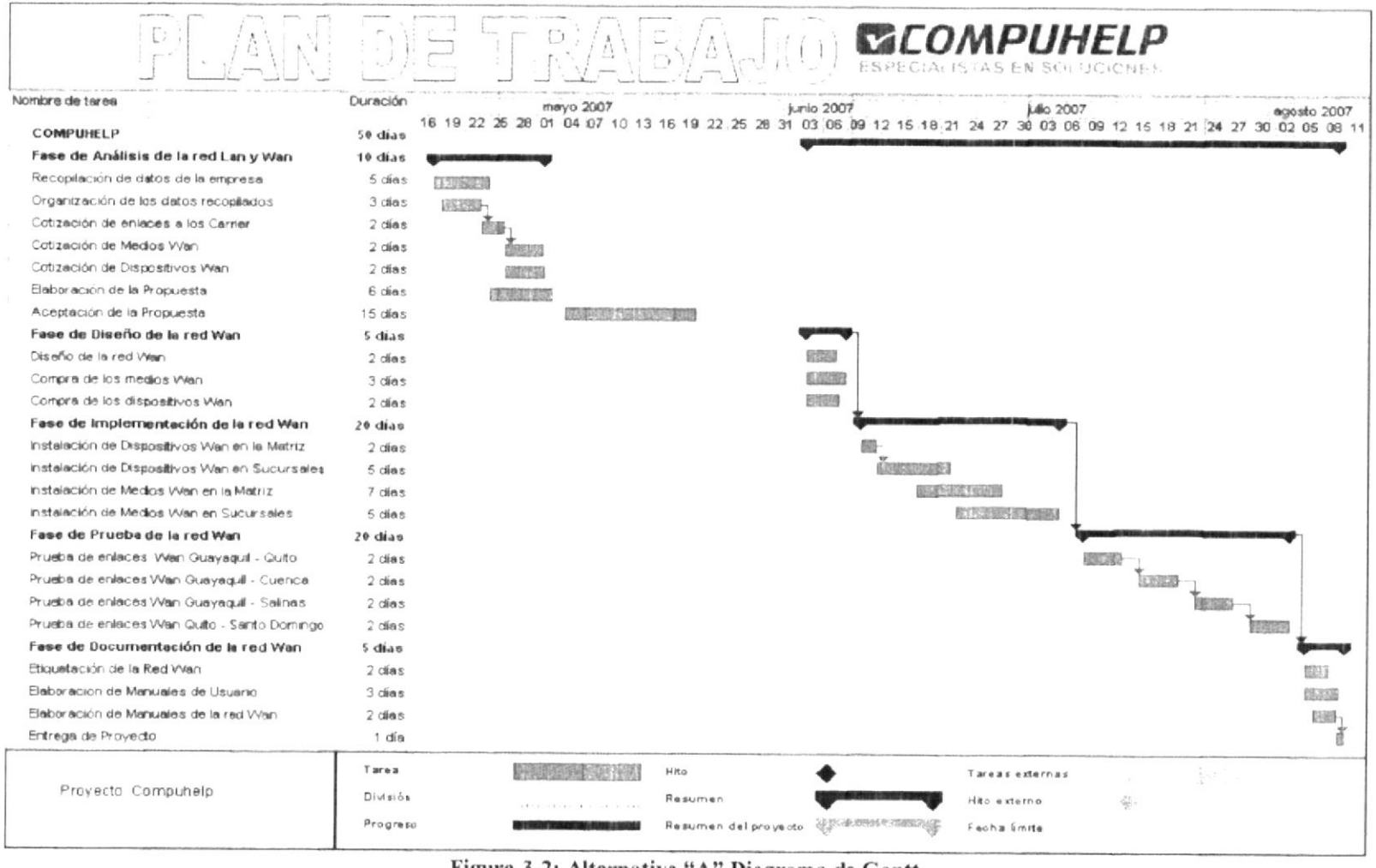


Figura 3-2: Alternativa "A" Diagrama de Gantt

3.3.2 ALTERNATIVA "B"

De acuerdo a los problemas encontrados hemos planteado otra alternativa como solución. En esta alternativa se sugiere la adquisición de Routers de marca debido a que su empresa no cuenta con sus propios equipos de ruteo para la transmisión de datos, ya que estos equipos son proporcionados por la empresa proveedora de Internet.

3.3.2.1 FACTIBILIDAD TÉCNICA

Cantidad	Descripción	Imagen	Ubicación
7	Router ➢ 2 Puertos Fast Ethernet 10/100 Mbps. ➢ 1 Slot de Modulo de Red. ➢ 3 Slot para tarjetas Wic de interfaz Wan. ➢ 2 Slot para modulo de integridad avanzada. ➢ Fuente redundante.		Matriz Guayaquil Sucursal Quito Sucursal Cuenca Sucursal Loja Sucursal Salinas Sucursal Manta Sucursal Santo Domingo

Tabla 3-8: Factibilidad Técnica "B"

3.3.2.2 FACTIBILIDAD ECONÓMICA

Cantidad	Descripción	Costo Unitario (Dólares)	Costo Total (Dólares)
7	Router ➢ 2 Puertos Fast Ethernet 10/100 Mbps. ➢ 1 Slot de Modulo de Red. ➢ 3 Slot para tarjetas Wic de interfaz Wan. ➢ 2 Slot para modulo de integridad avanzada. ➢ Fuente redundante.	$ 800.00	$ 5600.00
Total			$ 5600.00

Tabla 3-9: Factibilidad Económica "B"

3.3.2.3 FACTIBILIDAD OPERATIVA

Fase	Duración / Semanas
Fase de Análisis de la red Wan 1 Ingeniero en Telecomunicaciones	1
Fase de Diseño de la red Wan 1 Ingeniero en Telecomunicaciones	1
Fase de Implementación de la red Wan 2 Ingeniero en Telecomunicaciones 2 Técnico en Redes	3
Fase de Prueba de la red Wan 2 Ingeniero en Telecomunicaciones 2 Técnico en Redes	2
Fase de Documentación de la red Wan 1 Ingeniero en Telecomunicaciones	1

Tabla 3-10: Factibilidad Operativa "B"

3.3.2.4 COSTOS OPERATIVOS

Fase	Duración Semanas	Costo Semanas (Dólares)	Costo Total (Dólares)	Costo Fase (Dólares)
Fase de Diseño de la red Wan 1 Ingeniero en Telecomunicaciones	1	$ 200	$ 200	$ 200
Fase de Implementación de la red Wan 2 Ingeniero en Telecomunicaciones 2 Técnico en Redes	3	$ 200 $ 70	$ 1200 $ 420	$ 1620
Fase de Prueba de la red Wan 2 Ingeniero en Telecomunicaciones 2 Técnico en Redes	2	$ 200 $ 70	$ 800 $ 280	$ 1080
Fase de Documentación de la red Wan 1 Ingeniero en Telecomunicaciones	1	$ 200	$ 200	$ 200
Costo Total Operativo				$ 3100

Tabla 3-11: Costos Operativos "B"

3.3.2.5 COSTO TOTAL DE LA ALTERNATIVA "B"

Dentro de esta alternativa incluimos los imprevistos.

Descripción	Costo Total (Dólares)
Factibilidad Económica	$ 5600
Servicios Profesionales	$ 3100
Total	**$ 8700**
Iva 12%	**$ 1044**
Costo total de la Propuesta	**$ 9744**

Tabla 3-12: Costo total de la alternativa "B"

3.3.2.6 VENTAJAS

- Debido a la adquisición tecnológica en dispositivos se puede ampliar la cobertura de la red wan.
- Mayores tiempos de respuestas en la transmisión de datos.
- Incremento en la velocidad y tiempo de respuesta en el tráfico de la red Lan.
- Fortalecer los servicios que brindan a sus clientes debido a la adquisición tecnológica en dispositivos de ruteo y conmutación.

3.3.2.7 BENEFICIOS

- Clientes satisfechos debido a soluciones rápidas a sus problemas.

3.3.2.8 GARANTÍA

La compañía FAST SOLUTIONS S.A. ofrece una garantía técnica de 6 meses, con respaldo de los proveedores de los dispositivos de enrutamiento.

1. Soporte y seguimiento a las redes WAN.
2. Enlaces WAN muy lentos.

Valores que no cubre la garantía:

1. Al presentarse un problema dentro de la WAN y tratar de solucionarlo por sus propios medios, debiendo comunicarse inmediatamente con FAST SOLUTIONS S.A. Ya que puede causar un daño a los ruteadores.

Nota:
Si se presenta uno de estos casos y de no respetar las cláusulas de la garantía, tendrá que cancelar los valores, por la revisión y solución del problema presentado.

3.3.2.9 FORMA DE PAGO DE LA ALTERNATIVA "B"

A continuación detallaremos la forma de pago mediante el cual se cancelarán los valores por el estudio realizado a su prestigiosa empresa.

- Después de la aceptación de la propuesta se receptara, el 75% del valor total de la propuesta, que corresponde a un monto de $ 17304 en la fecha del 19 de Junio del 2007.

- Al finalizar la fase de prueba se receptara el valor pendiente a cancelar, que es el 25% del valor total de la propuesta, que corresponde a un monto de $ 5768 en la fecha del 8 de Agosto del 2007.

3.3.2.10 DIAGRAMA DE GANTT DE LA ALTERNATIVA "B"

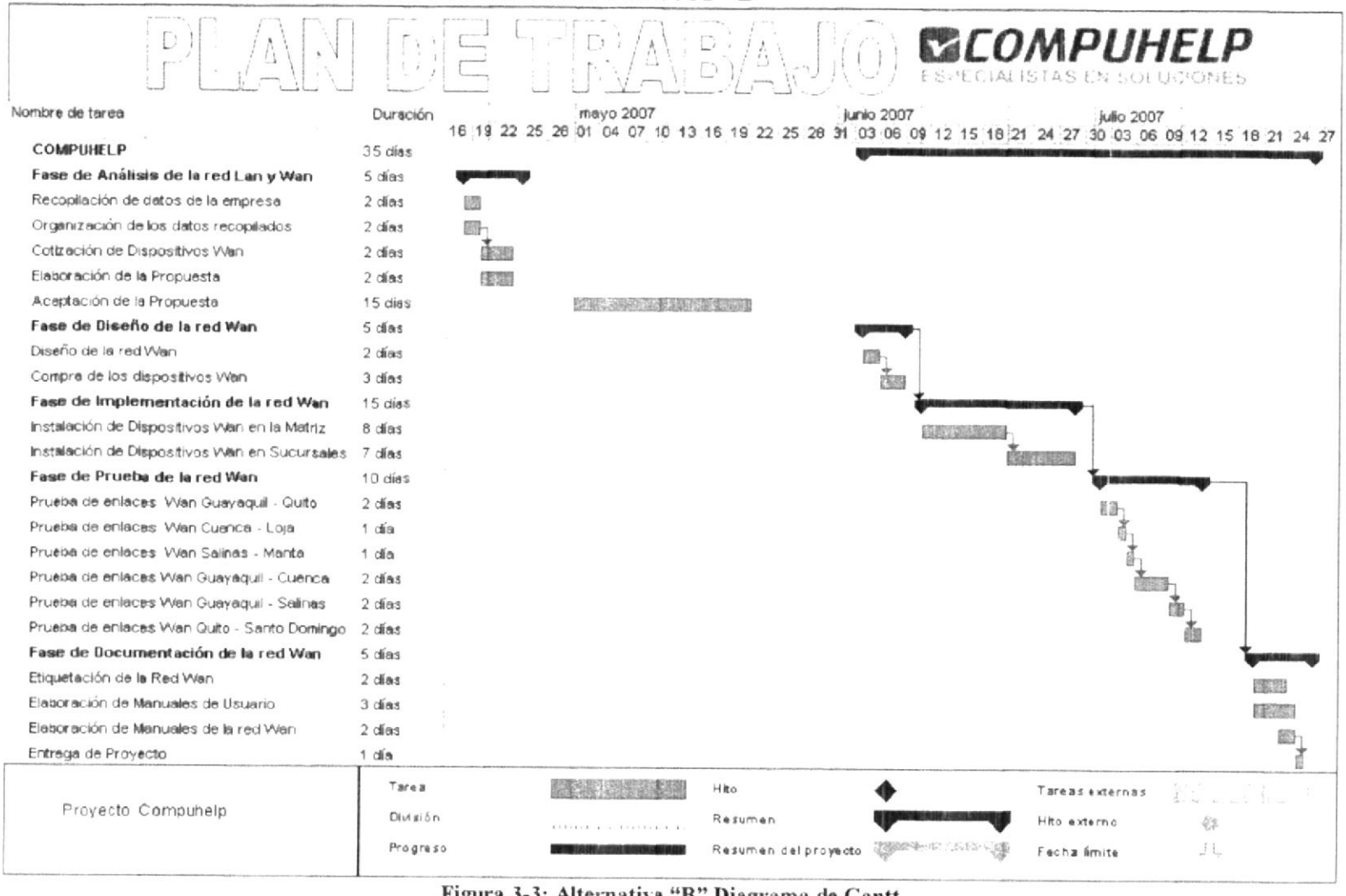


Figura 3-3: Alternativa "B" Diagrama de Gantt

CAPÍTULO 4

IMPLEMENTACIÓN WAN

4. IMPLEMENTACIÓN WAN

4.1 GRÁFICO DE MEDIOS DE COMUNICACIÓN

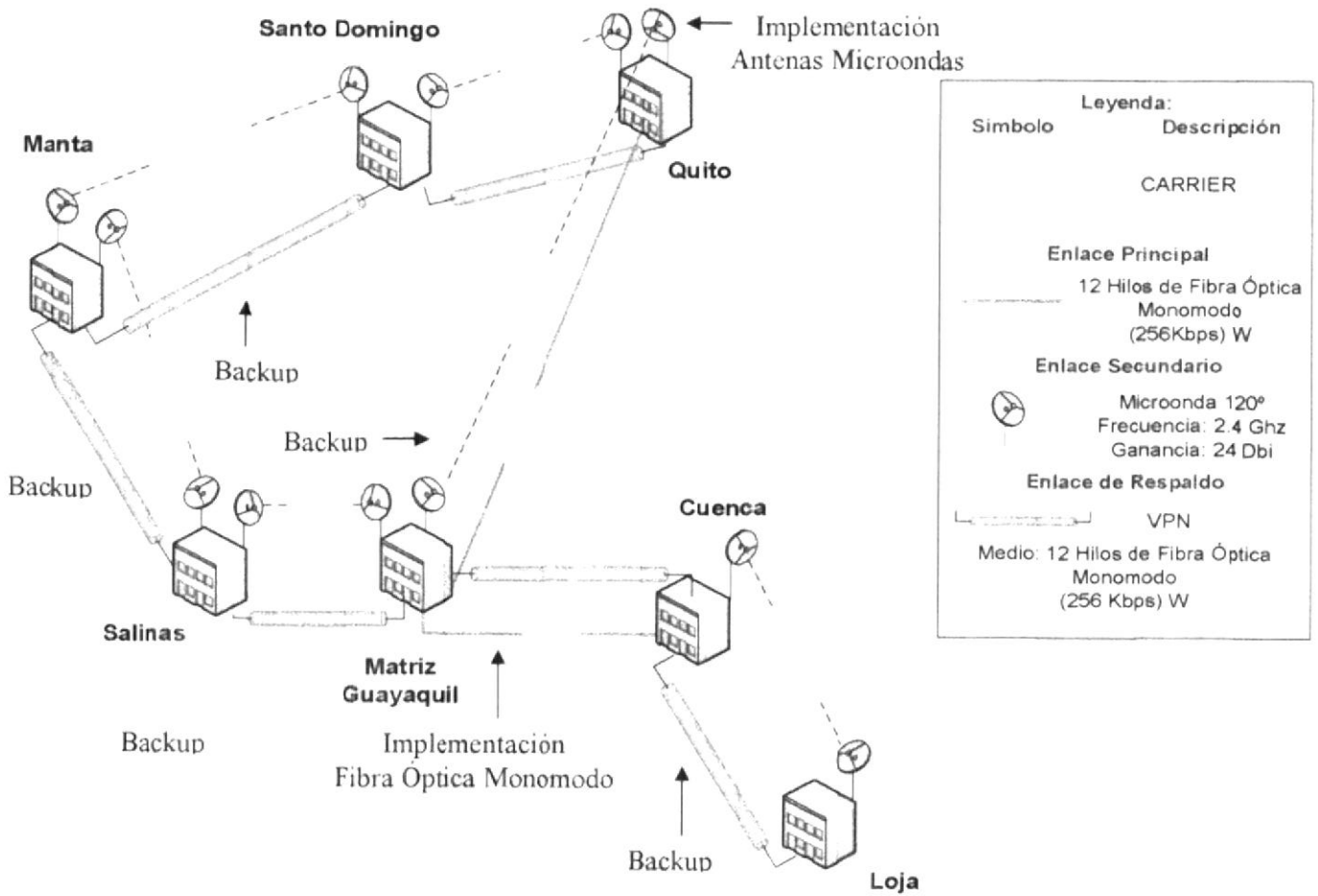


Figura 4-1: Implementación de Medios de comunicación Wan

4.2 GRÁFICO DE DISPOSITIVOS DE COMUNICACIÓN

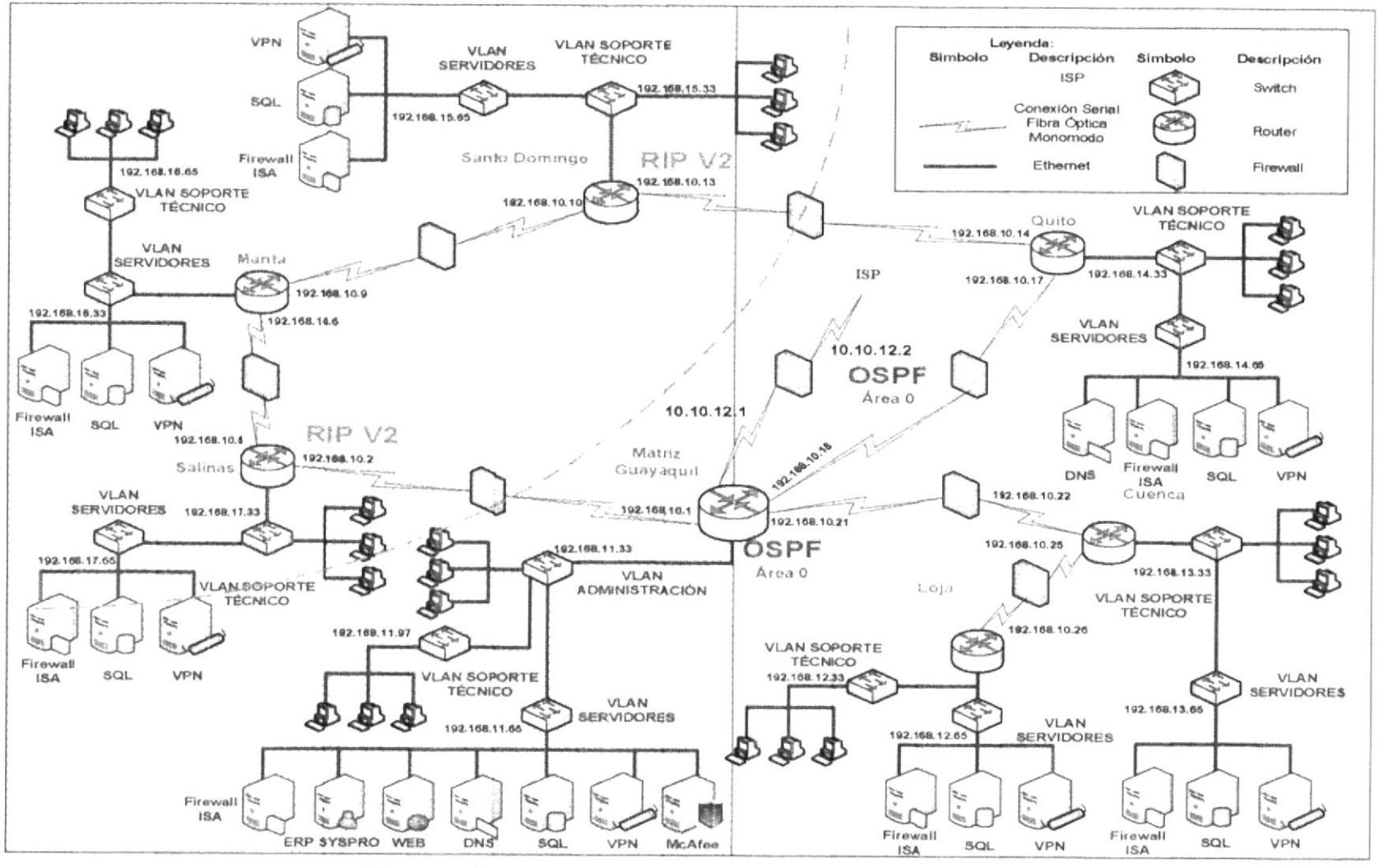


Figura 4-2: Implementación de dispositivos de Comunicación Wan

CAPÍTULO 5

NORMATIVAS DE CABLEADO ESTRUCTURADO

5. NORMATIVAS DE CABLEADO ESTRUCTURADO

△ → Recomendación

▲ → Obligatoriedad

5.1 NORMATIVAS

▲ **Normativa 1:**

Consideraciones de interferencia electromagnética.

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

Requisitos tales como:

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

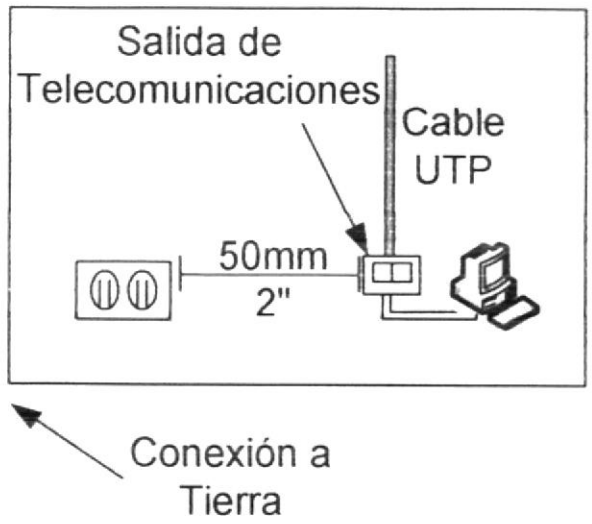


Figura 5-1: Normativa 1

Normativa 2:

Aplicado a topología.

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

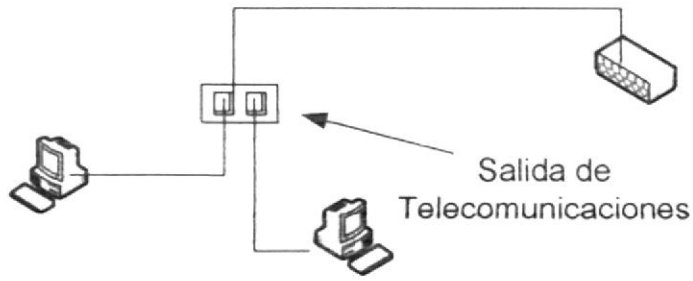


Figura 5-2: Normativa 2

Normativa 3:

Se aplicará conexión cruzada para conexiones de cable horizontal y el backbone vertical.

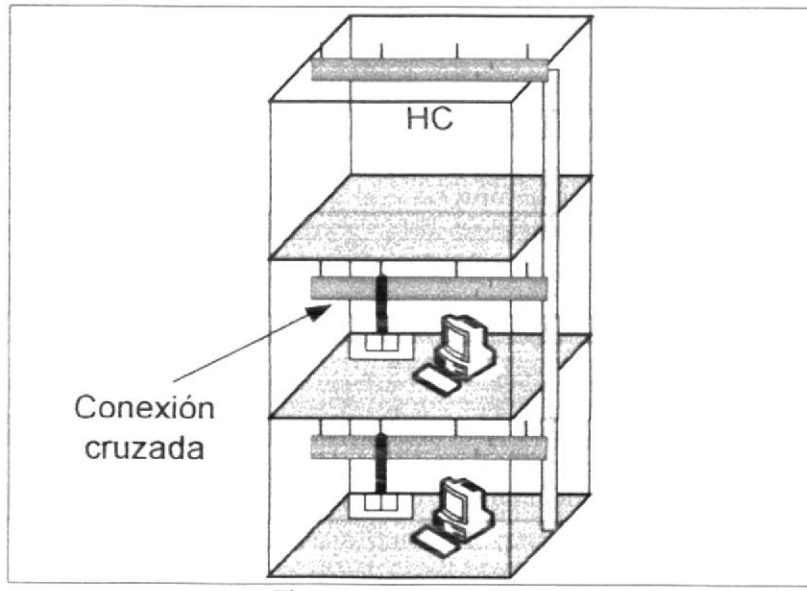


Figura 5-3: Normativa 3

Normativa 4:

Cada área de trabajo será atendida por un HC localizado en el mismo piso o en un piso adyacente.

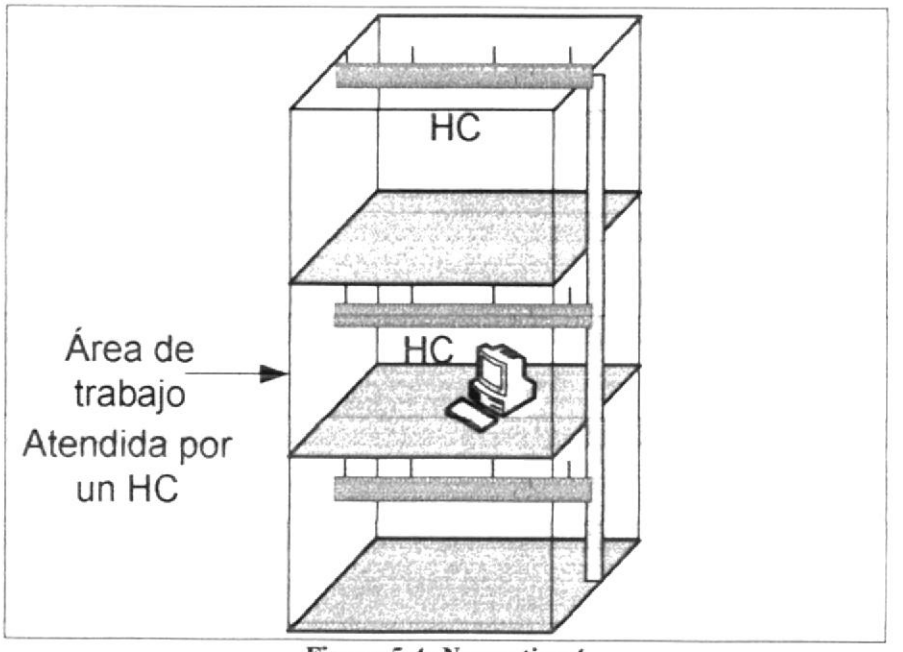


Figura 5-4: Normativa 4

Normativa 5:

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

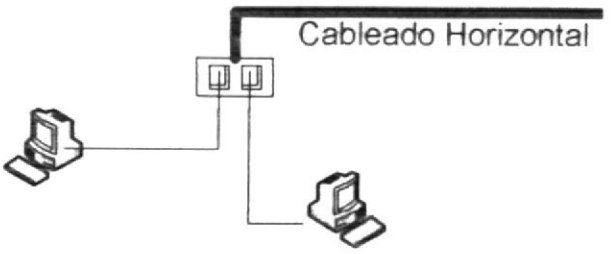


Figura 5-5: Normativa 5

Normativa 6:

La longitud del cableado entre las salidas de telecomunicación y el HC, no excederá los 90 m, independientemente del tipo de medio.

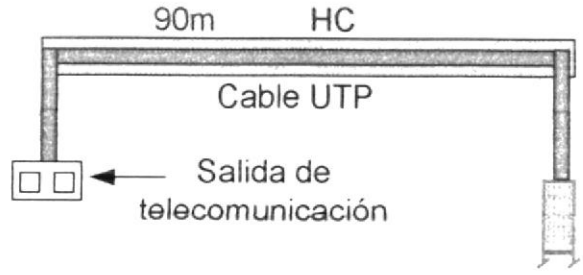


Figura 5-6: Normativa 6

Normativa 7:

La longitud individual o combinada del Patch Cord del par trenzado balanceado 24 AWG (Calibre Americano de alambre) o fibra óptica utilizado en el HC, no excederá los 5 m.

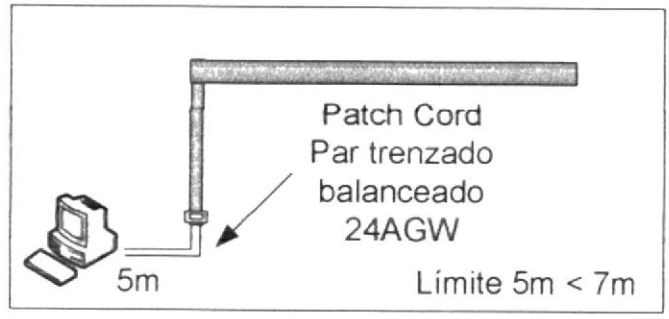


Figura 5-7: Normativa 7

Normativa 8:

La longitud del canal del cableado Horizontal incluyendo los Patch Cord de equipos en ambos extremos no excederá los 100 m independientemente del medio.

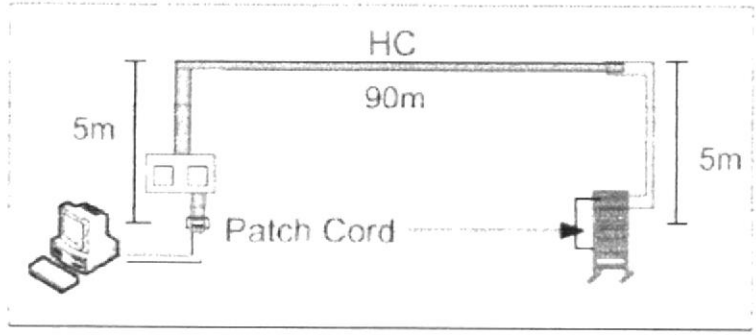


Figura 5-8: Normativa 8

Normativa 9:

La longitud de los cordones de tipo del área de trabajo de par trenzado balanceado no excederá los 20 m cuando se une un punto de consolidación.

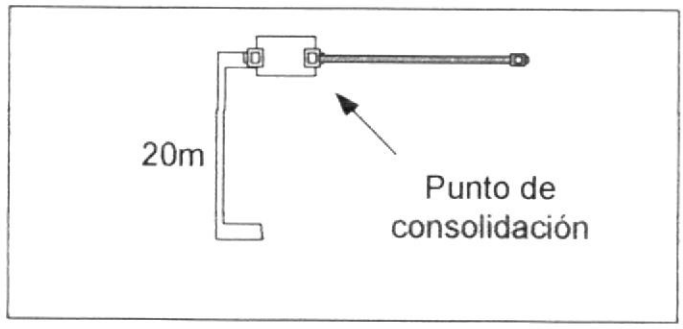


Figura 5-9: Normativa 9

Normativa 10:
No se permitirá más de un punto de consolidación dentro del mismo tendido del cableado horizontal.

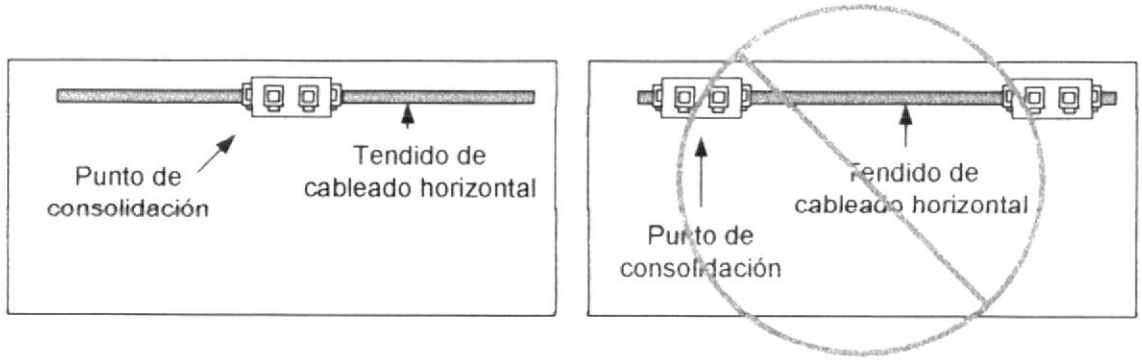


Figura 5-10: Normativa 10

Normativa 11:
No se permitirá conexión cruzada o equipo activo en el punto de consolidación.

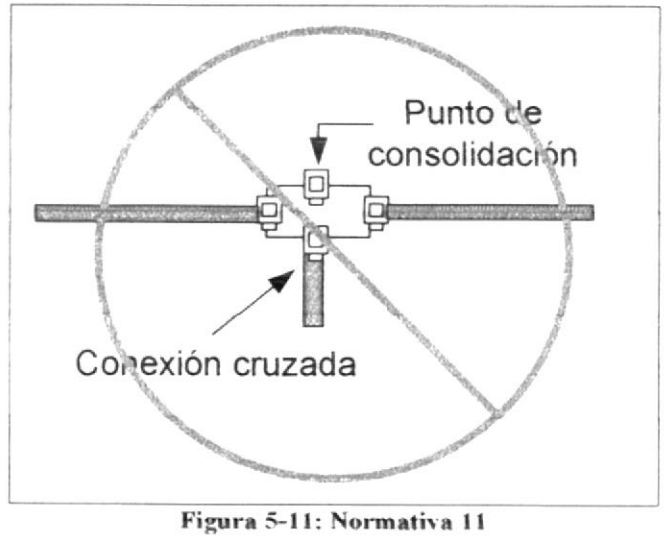


Figura 5-11: Normativa 11

Punto de Consolidación:
Es un Hardware de conexión que proporciona una interconexión entre el cableado de oficina abierta y el cableado horizontal.

Normativa 12:

Cada cable horizontal que salga del punto de consolidación tendrá sus cuatro pares terminados en un toma modular de ocho posiciones en el área de trabajo.

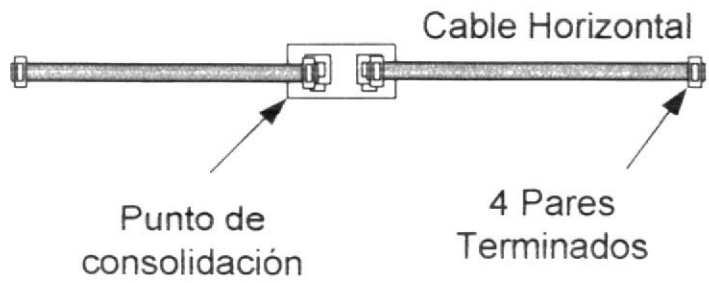


Figura 5-12: Normativa 12

Normativa 13:

La distancia máxima entre el HC y la salida de telecomunicaciones será de 90 m.

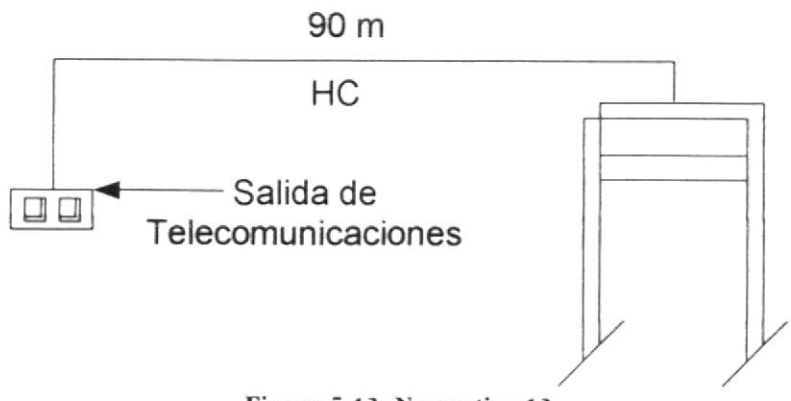


Figura 5-13: Normativa 13

Normativa 14:

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

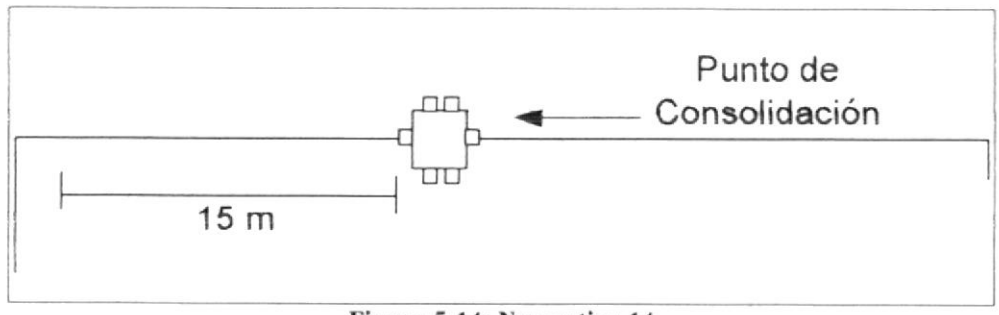


Figura 5-14: Normativa 14

Normativa 15:

La distancia mínima entre el punto de consolidación y la salida de telecomunicaciones será de 5 m.

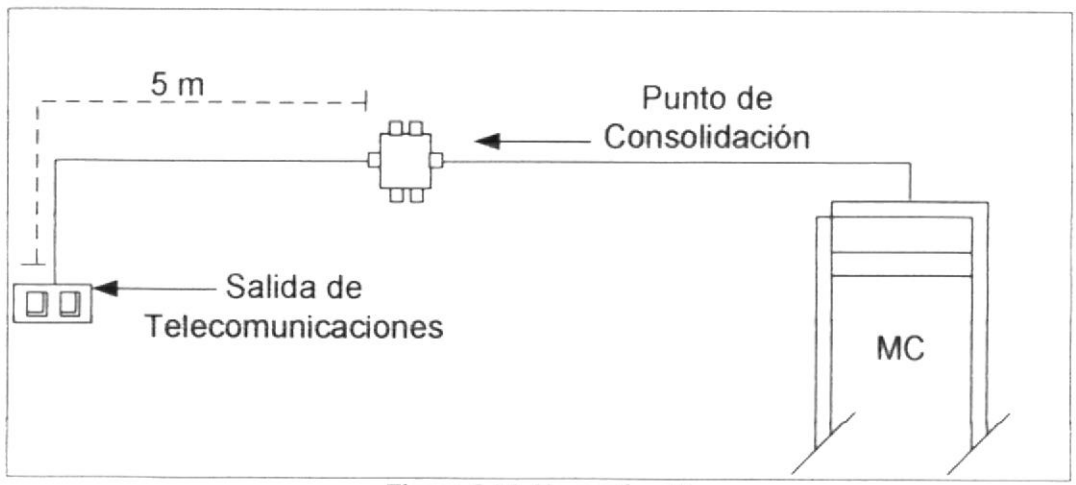


Figura 5-15: Normativa 15

Normativa 16:

La distancia de canal del cableado horizontal incluyendo los 2 cables de equipos en ambos extremos no excederá los 100 m, independientemente del medio.

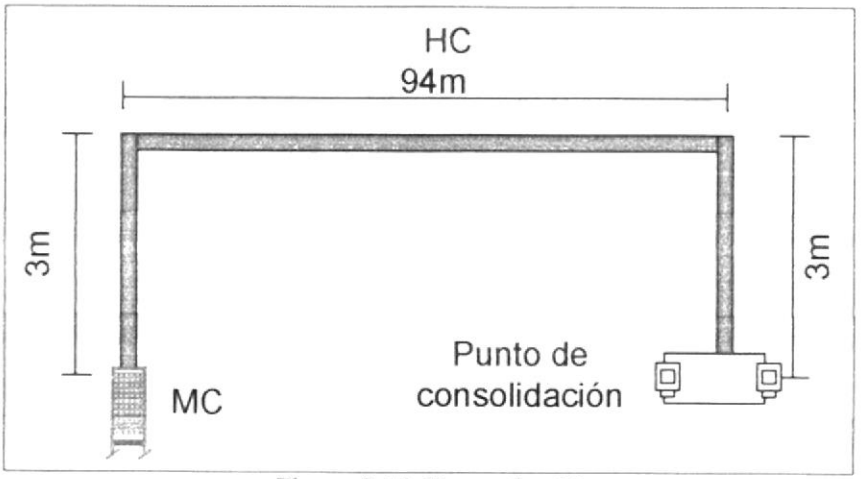


Figura 5-16: Normativa 16

Normativa 17:

Todos los pares de cable estarán totalmente terminados en ambos extremos.

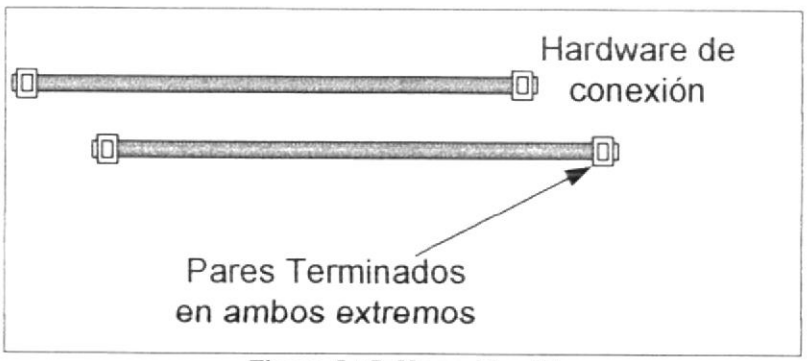


Figura 5-17: Normativa 17

Normativa 18:

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

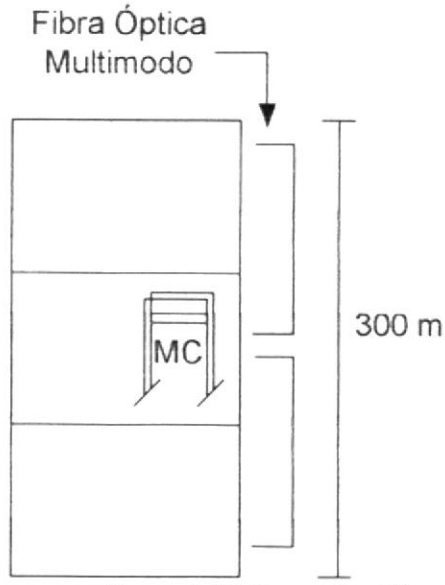


Figura 5-18: Normativa 18

Normativa 19:

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

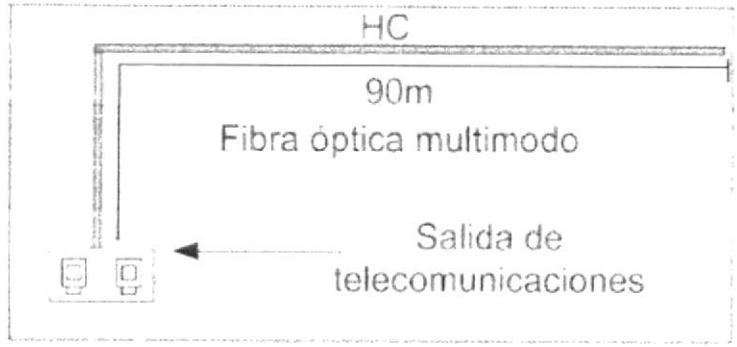


Figura 5-19: Normativa 19

Normativa 20:

Las canalizaciones horizontales del cableado se diseñaran e instalaran para cumplir los reglamentos eléctricos y de comunicación, locales y nacionales y normas aplicables.

Figura 5-20: Normativa 20

Normativa 21:

Las canalizaciones serán apropiadas para el ambiente en el cual se instalarán y no se obstacularizarán por ductos de calefacción, ventilación y aire acondicionado, distribución de energia eléctrica o estructuras de edificios.

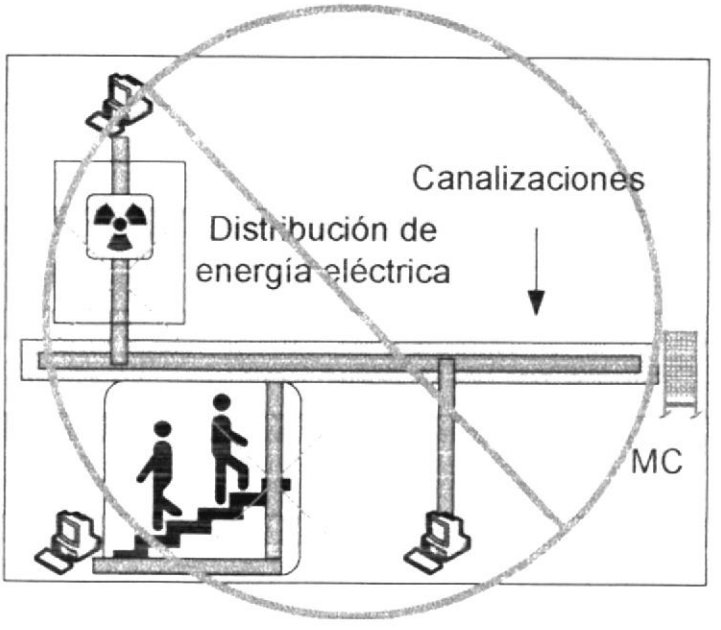


Figura 5-21: Normativa 21

Normativa 22:

Las canalizaciones horizontales se instalarán o seleccionarán de manera que el radio mínimo de curvatura de los cables horizontales se mantenga dentro de las especificaciones del fabricante durante y después de la instalación.

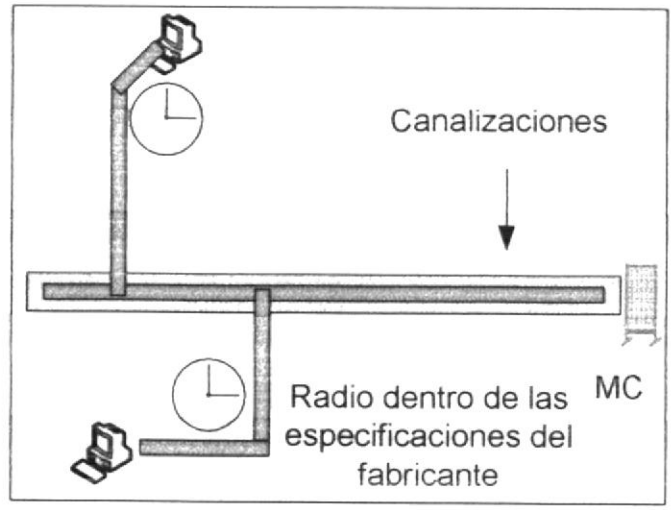


Figura 5-22: Normativa 22

Normativa 23:

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

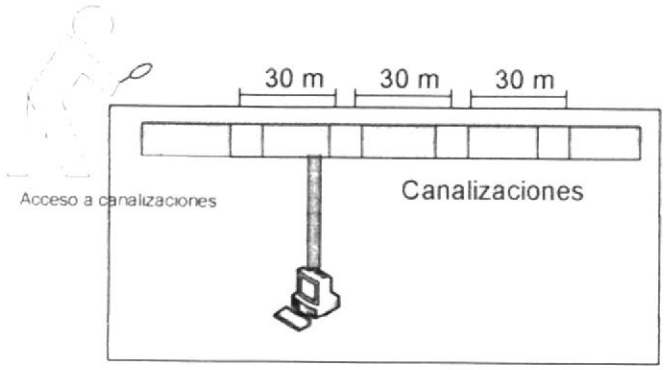


Figura 5-23: Normativa 23

Normativa 24:

El Backbone usara la topología tipo estrella jerárquica con respecto al MC.

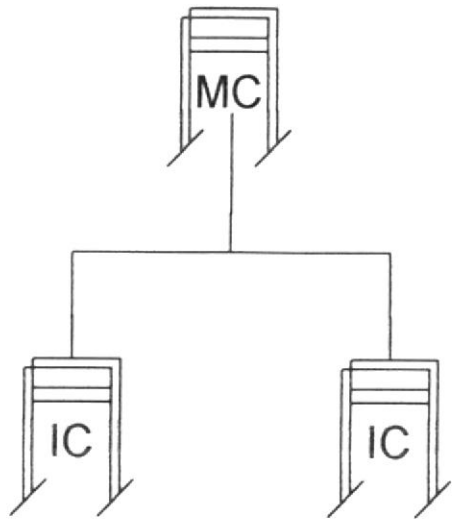


Figura 5-24: Normativa 24

Normativa 25:

Para cada tendido de Backbone de edificio que sea mayor de 90 m de longitud debe proveerse cable de fibra óptica.

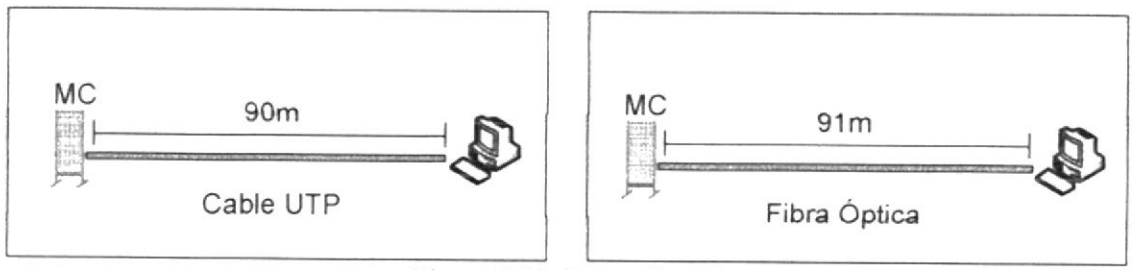


Figura 5-25: Normativa 25

Normativa 26:

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

- 3000 m para fibra óptica monomodo.
- 2000 m para fibra óptica multimodo.
- 2000 m para par trenzado balanceado para aplicaciones PBX.

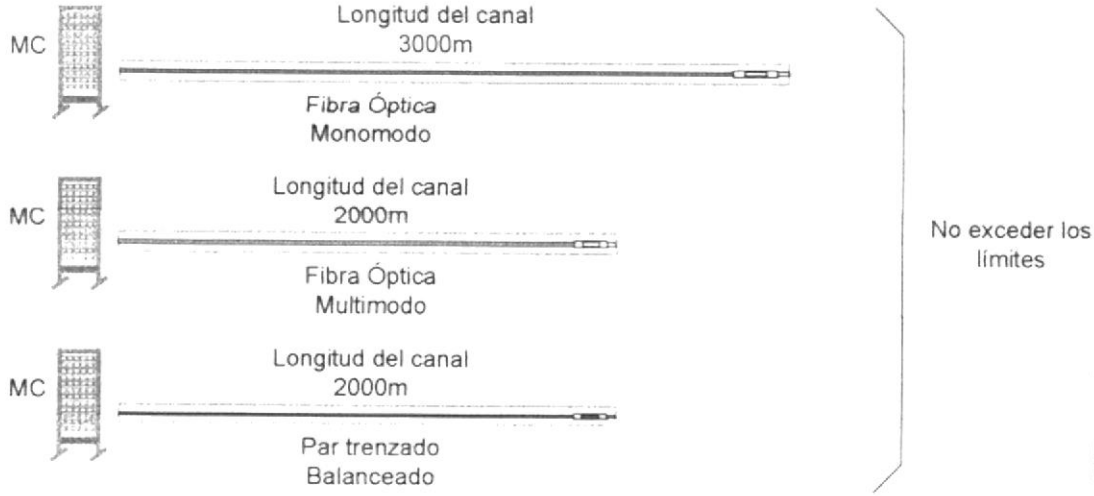


Figura 5-26: Normativa 26

Normativa 27:

Las canalizaciones de edificio proveerán acceso a todos los cuartos de telecomunicaciones, cuartos de equipos vía cometidas localizadas en el mismo edificio.

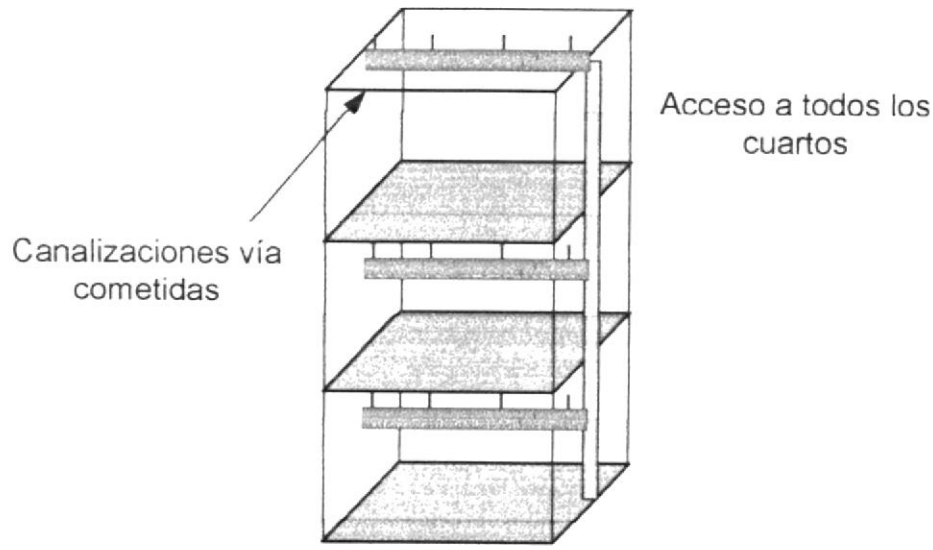


Figura 5-27: Normativa 27

Normativa 28:

Las canalizaciones no se ubicarán en ductos de ascensores.

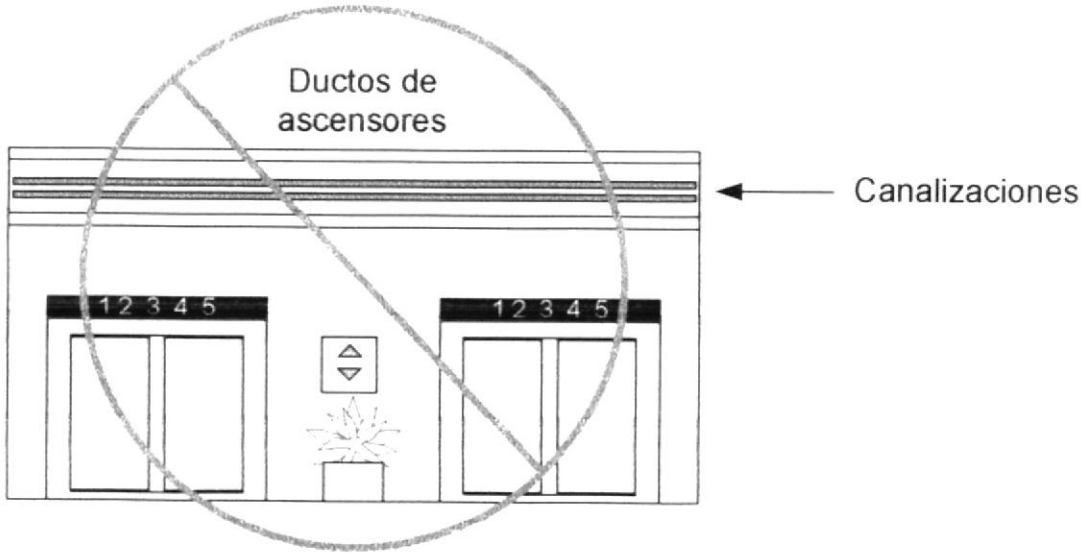


Figura 5-28: Normativa 28

Normativa 29:

El cable que corra entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará expuesto en el área de trabajo u otros espacios con acceso público.

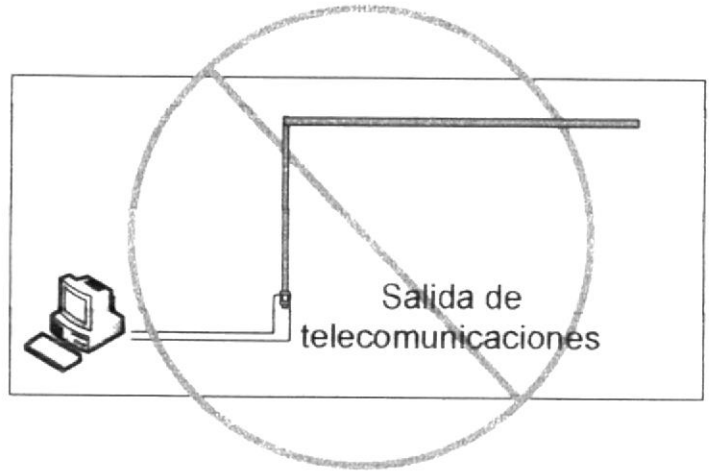


Figura 5-29: Normativa 29

Normativa 30:

El cuarto de telecomunicaciones se diseñara y equipara para tener equipos de telecomunicaciones, terminaciones de cables y asociados.

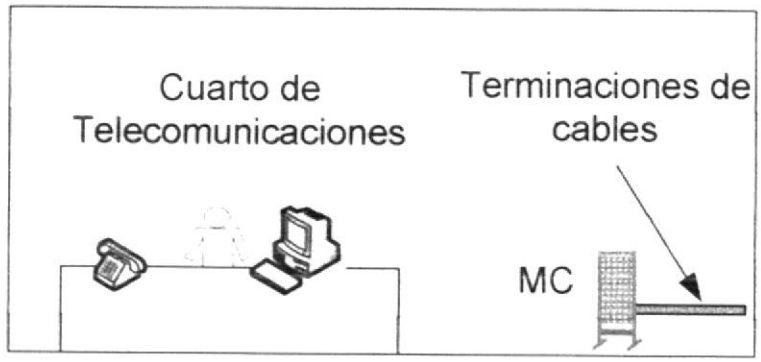


Figura 5-30: Normativa 30

Normativa 31:

El cuarto de telecomunicaciones estará dedicado a las telecomunicaciones. El acceso a los cuartos de telecomunicaciones se restringirá al personal de servicio autorizado y no será compartido por servicios del edificio que puedan interferir con los servicios de telecomunicación o se utilicen para servicio de mantenimiento del edificio.

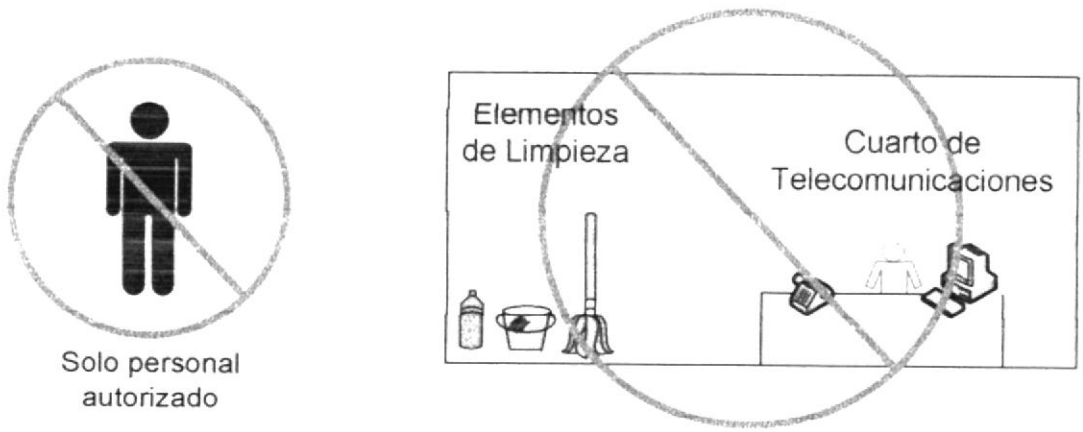


Figura 5-31: Normativa 31

Normativa 32:

Las instalaciones de puesta y unida a tierra cumplirán con los reglamentos y normas aplicables.

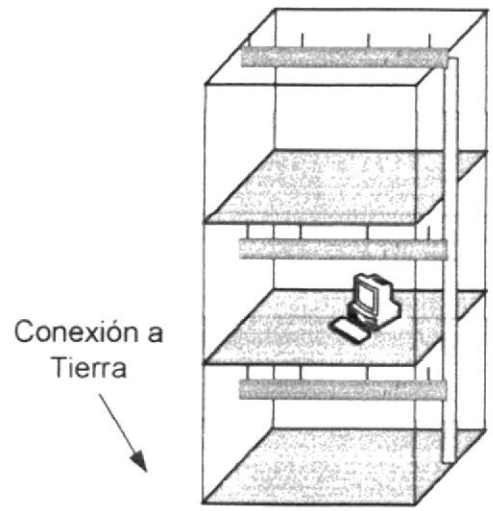


Figura 5-32: Normativa 32

Normativa 33:

Las cajas o gabinetes usados como espacios alternativos cumplirán los requisitos de separación, tendrán la puerta con vista y cerradura, se montara en una ubicación fija.

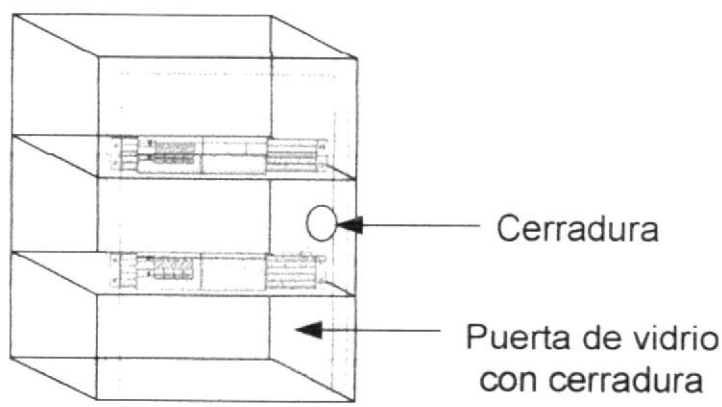


Figura 5-33: Normativa 33

Normativa 34:

El cuarto de equipos no será compartido por servicios de edificio que puedan interferir con los sistemas de telecomunicaciones o se utilicen para servicios de mantenimiento de edificio.

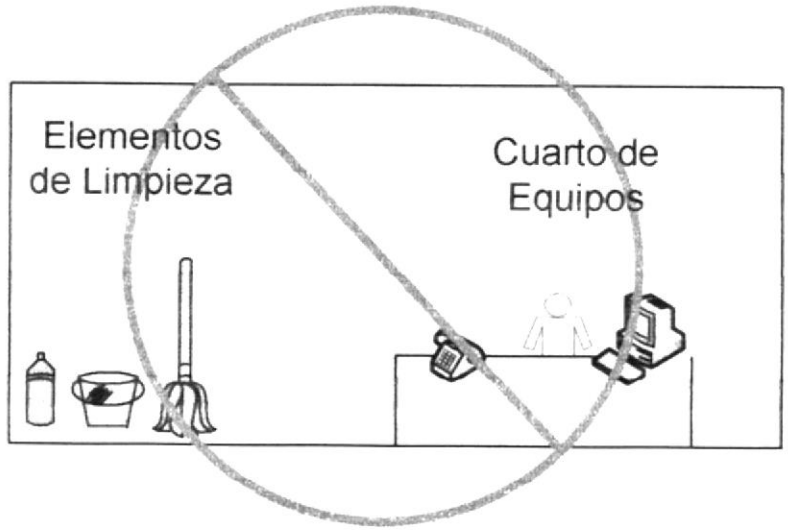


Figura 5-34: Normativa 34

Normativa 35:

El cableado se instalará para facilitar el rotulado, la documentación y para permitir el código de color, en forma consistente de acuerdo a los requisitos.

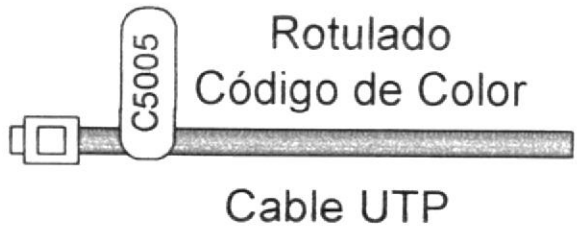


Figura 5-35: Normativa 35

Normativa 36:

La instalación de gabinetes y rack deberá proporcionar las separaciones estructuradas en los reglamentos y normas aplicadas.

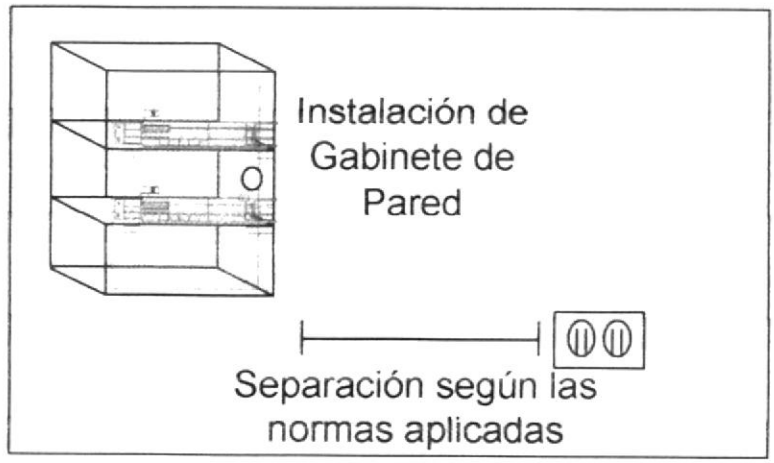


Figura 5-36: Normativa 36

Normativa 37:

Los cables de telecomunicaciones se soportarán con dispositivos diseñados para este fin en forma independiente de cualquier otra estructura.

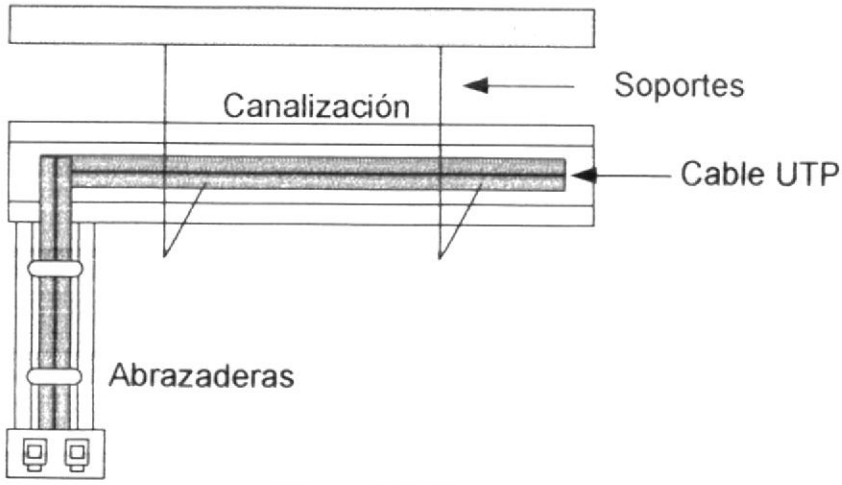


Figura 5-37: Normativa 37

Normativa 38:

Los cables enrutados verticalmente, como el caso de los cables del backbone u horizontal enrutados en el piso, se soportarán con abrazaderas u otros mecanismos. Se requiere un mínimo de dos soportes por piso.

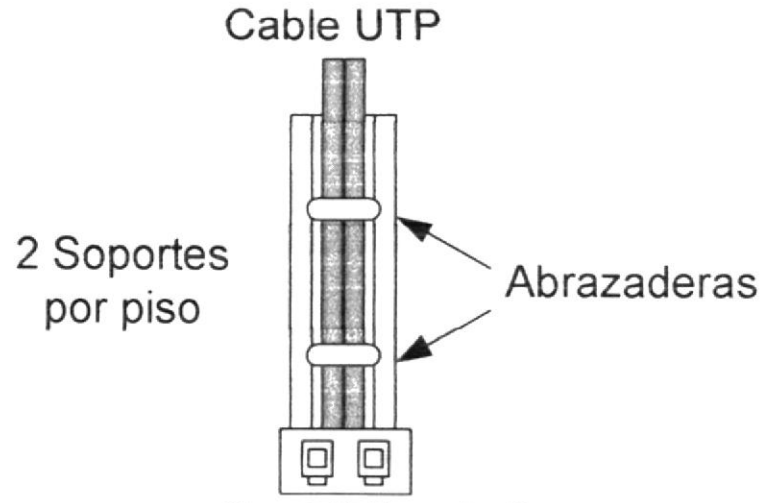


Figura 5-38: Normativa 38

Normativa 39:

El número de cables horizontales (Par trenzado balanceado o cable de fibra óptica) colocados en un soporte o canalización se limitara a una cantidad que no altere la forma geométrica de los cables.

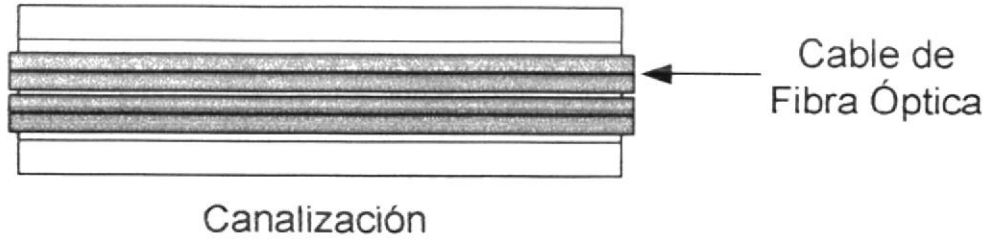


Figura 5-39: Normativa 39

Normativa 40:

Las canalizaciones tipo bandeja o canal no excederán la capacidad máxima de 50% de llenado y un máximo interior de 6 pulgadas.

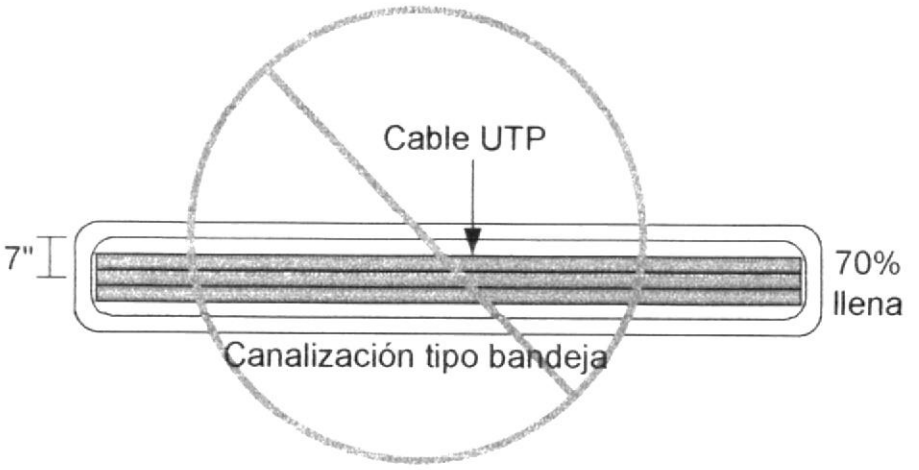


Figura 5-40: Normativa 40

Normativa 41:

Para canalizaciones en espacios de techo falso, los sistemas de soporte de cable se diseñarán e instalarán con un mínimo de 3 pulgadas por encima de la rejilla del techo soportado.

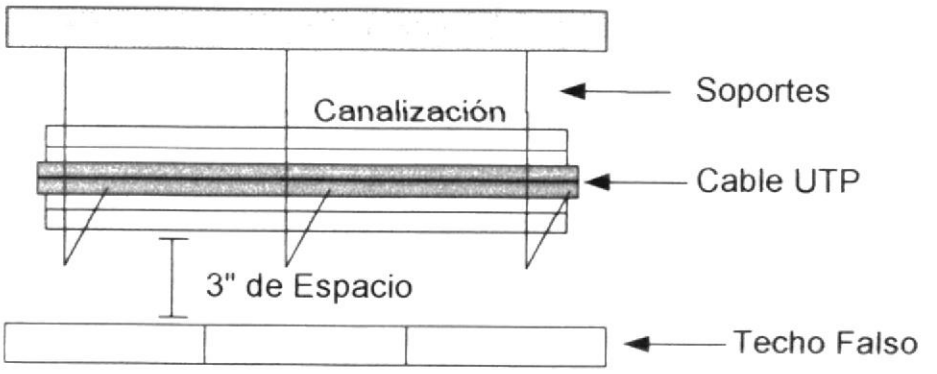


Figura 5-41: Normativa 41

Normativa 42:

Los cables se instalarán en canalizaciones y espacios que brinden protección adecuada contra la intemperie y demás riesgos de entorno.

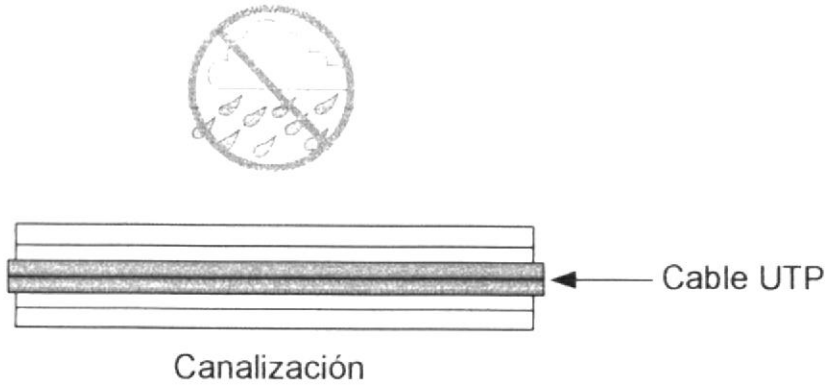


Figura 5-42: Normativa 42

Normativa 43:

No se permitirá el engrapado de ningún tipo de cable reconocido.

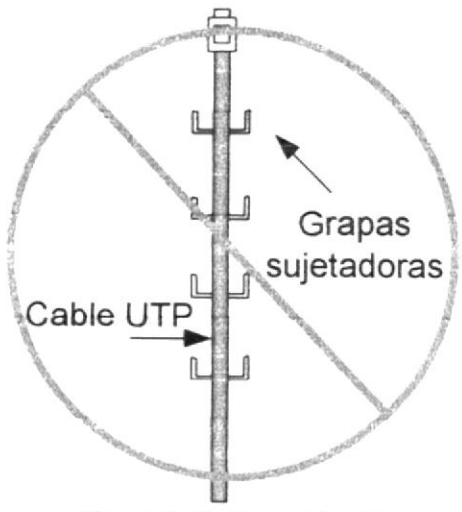


Figura 5-43: Normativa 43

Normativa 44:

El radio mínimo de curvatura en condiciones de no tensión (cuando el cable es solo colocado, no alado) será de:

Cuatro veces el diámetro externo del cable para UTP.
1 Pulgada para SCTP o SFTP del diámetro menor igual a 6 milímetros.
2 Pulgadas para SCTP o SFTP del diámetro mayor a 6 milímetros (0.25 pulgadas)

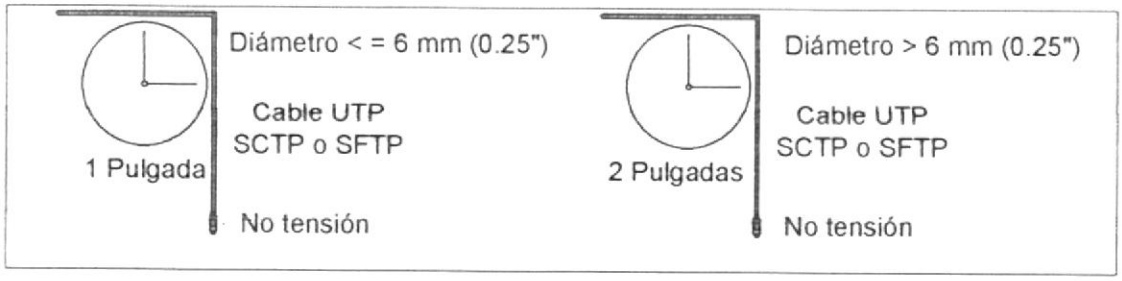


Figura 5-44: Normativa 44

Normativa 45:

El radio mínimo de curvatura para cable horizontal de 2 y 4 hilos de fibra será de 25 milímetros (1 pulgada) bajo condiciones de no tensión y de 50 milímetros bajo condiciones de tensión, en donde la tensión máxima de halado permitida es de 222 Newton (50 libras fuerza)

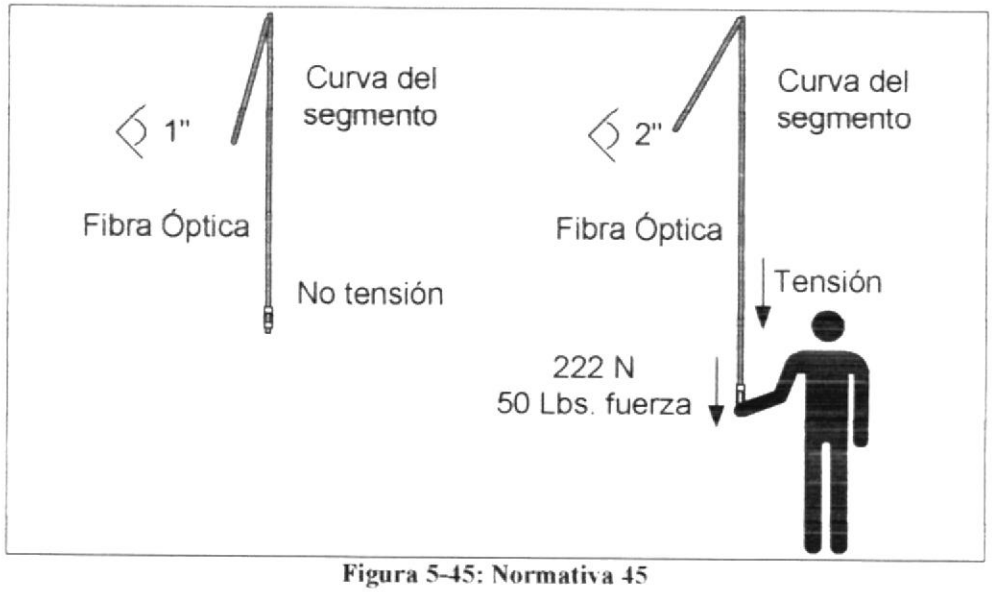


Figura 5-45: Normativa 45

Normativa 46:

El radio de curvatura para cable de backbone de fibra óptica de interiores no será menor a 10 veces el diámetro exterior del cable bajo condiciones de no tensión y no menor a 15 veces bajo condiciones de tensión.

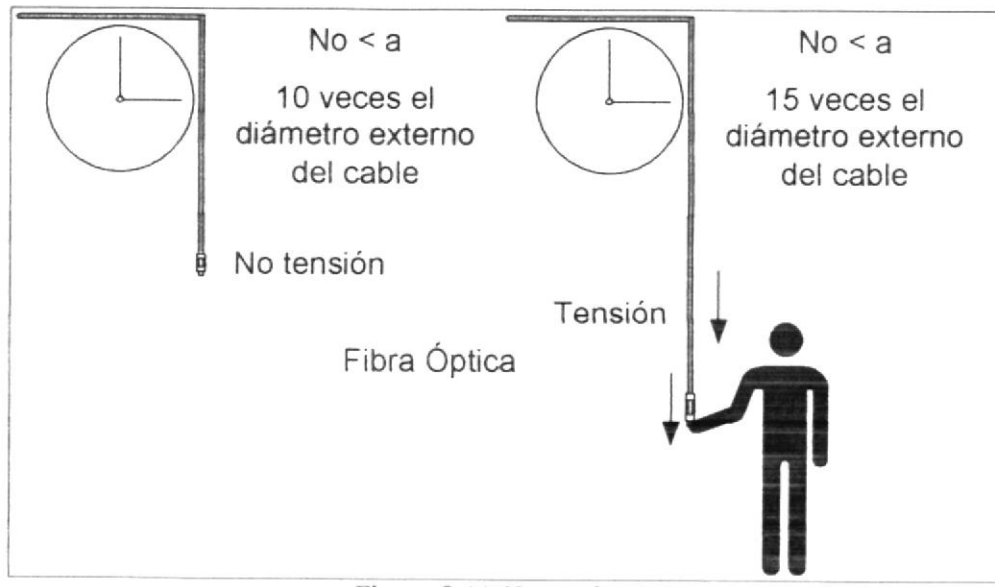


Figura 5-46: Normativa 46

Normativa 47:

El radio de curvatura para cable backbone de fibra óptica externo no será menor a 10 veces el diámetro exterior del cable bajo condiciones de no tensión y no menor a 20 veces bajo condiciones de tensión, en donde la tensión de halado permitida usualmente es menor a 2670 newton (600 libras fuerza)

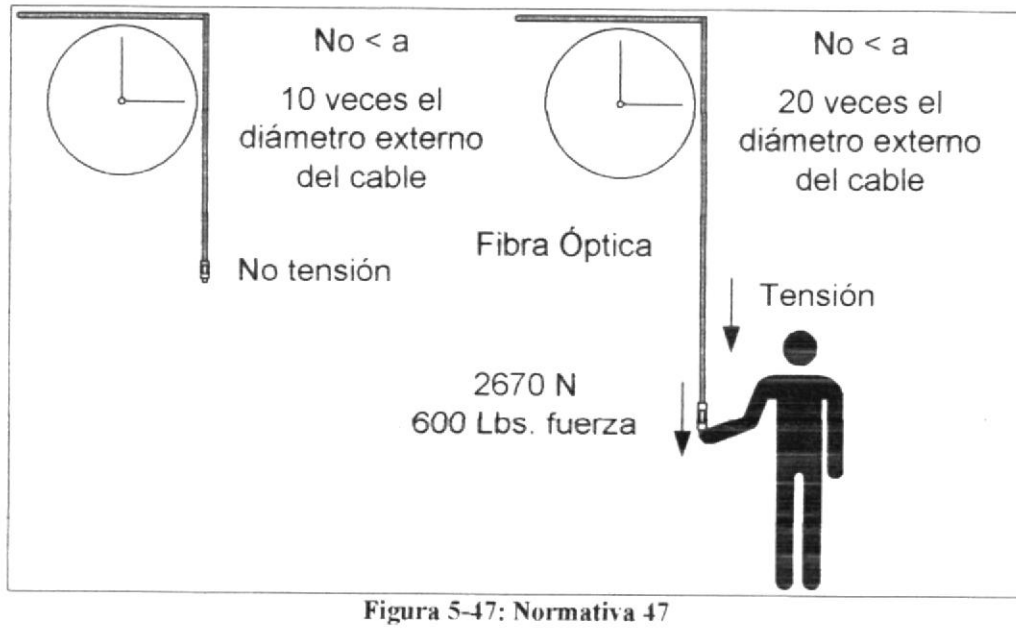


Figura 5-47: Normativa 47

Normativa 48:

El hardware de conexión se instalará de manera que se brinde un control de cable instalado y bien organizado.

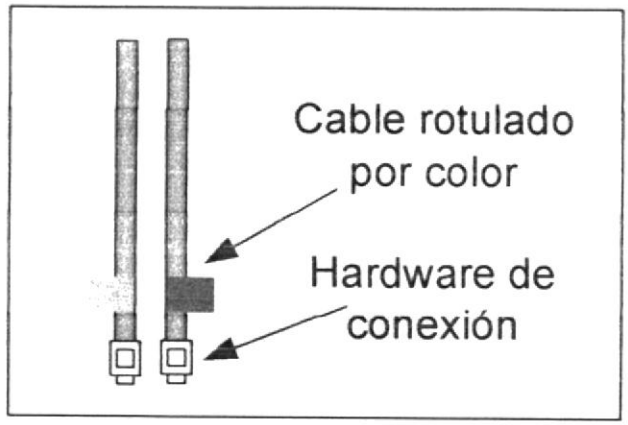


Figura 5-48: Normativa 48

Normativa 49:

Con el fin de reducir el descentrenzado de los pares de cable, el instalador debe pelar solo aquella cantidad de forro que se requiere para terminar en el hardware de conexión para par trenzado balanceado.

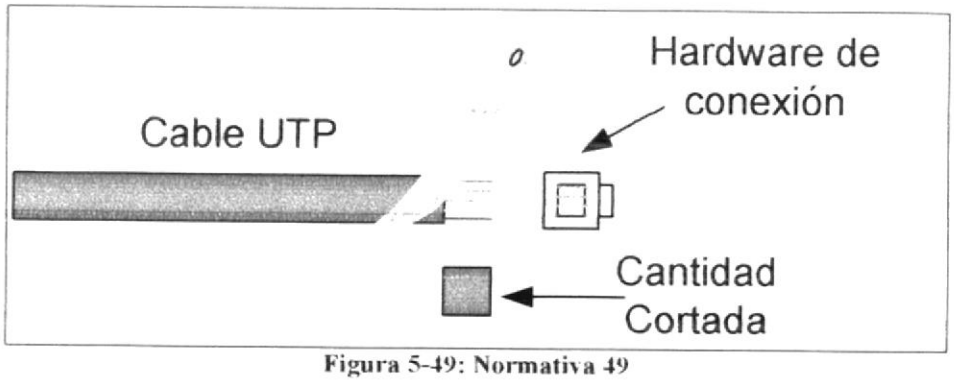


Figura 5-49: Normativa 49

Normativa 50:

La cantidad máxima de descentrenzado de cada par resultante de la terminación en el hardware de conexión será de 13 milimetros para cables de categoría 5e o mayor y de 75 milímetros para cables de categoria 3.

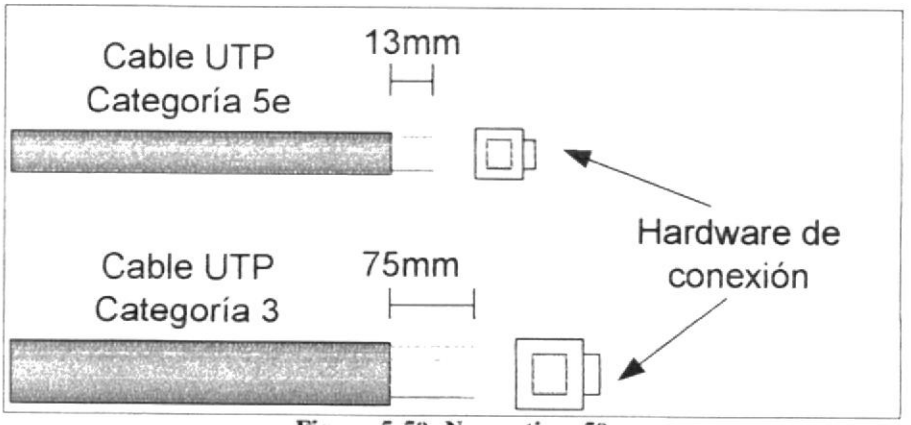


Figura 5-50: Normativa 50

Normativa 51:

No se deberá terminar cables de diferentes categorías de desempeño en el mismo hardware de conexión.

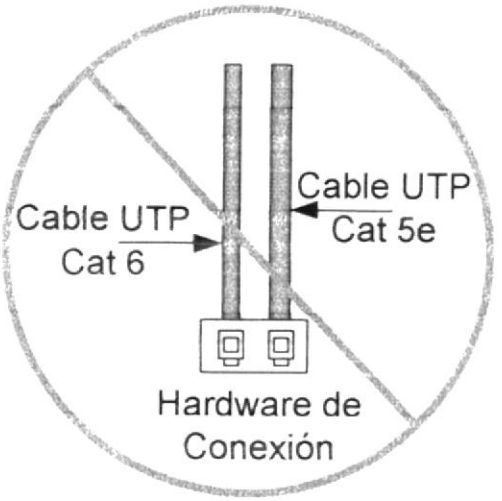


Figura 5-51: Normativa 51

Normativa 52:

Los identificadores que se utilizan para acceder a grupos de registros del mismo tipo deben ser únicos.

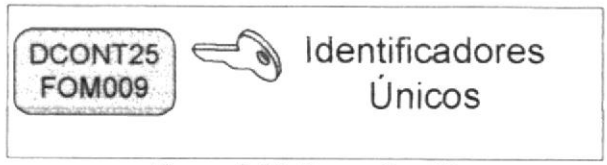


Figura 5-52: Normativa 52

Normativa 53:

El rotulado debe realizarse, ya sea pegando o colocando firmemente una etiqueta independiente al elemento que se va a administrar o marcando el elemento directamente.

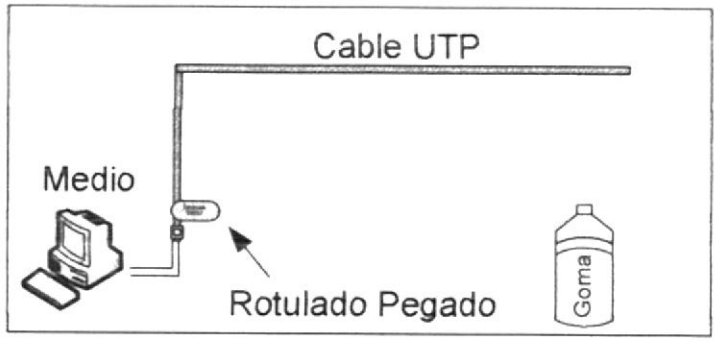


Figura 5-53: Normativa 53

Normativa 54:

El rotulado debe ser elegible y permanecer firmemente unido al elemento durante todo el tiempo de garantía.

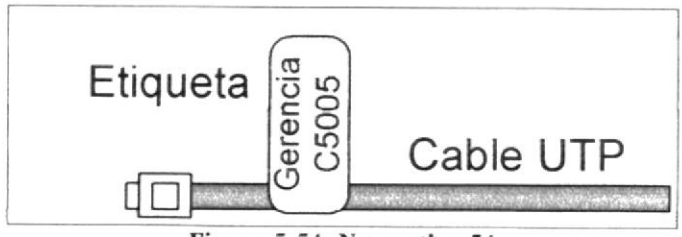


Figura 5-54: Normativa 54

Normativa 55:

A cada cable se le asignará un identificador único que sirva como referencia en sus registros respectivos.

Ej.:

DESCRIPCIÓN	IDENTIFICADOR
Cable N° 9 de fibra óptica multimodo	FOM009
Cable N° 5 de UTP categoría 5e	C5005

Figura 5-55: Normativa 55

Normativa 56:

Los cables de los subsistemas horizontales y backbone deberán rotularse en cada extremo. El cable o su etiqueta se marcarán con su identificador y será colocado dentro de los 3 cm. Del extremo del cable, esta marca deberá permanecer en el cable después de terminar la instalación.

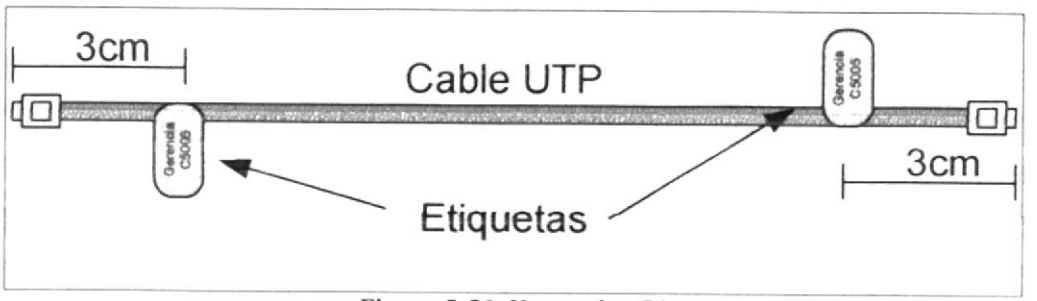


Figura 5-56: Normativa 56

5.2 RECOMENDACIONES

Recomendación 1:
Se puede ampliar interconexiones para conexiones del cableado horizontal y equipos con puertos individuales.

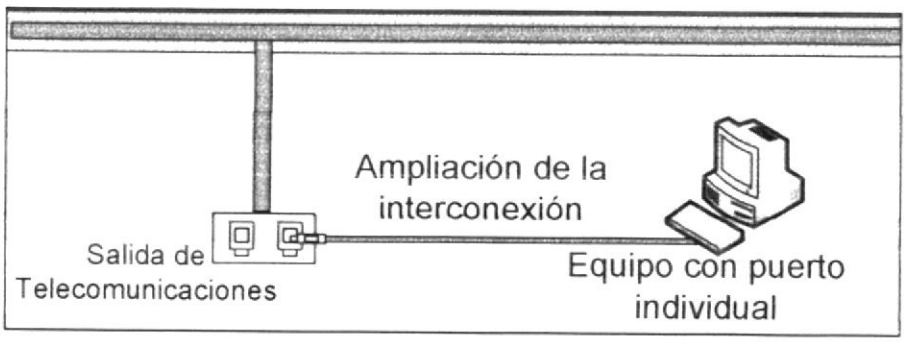


Figura 5-57: Recomendación 1

Recomendación 2:
Con el fin de proveer una infraestructura de capas para crear un ambiente de oficina se recomienda un mínimo de un cuarto de telecomunicaciones por cada piso.

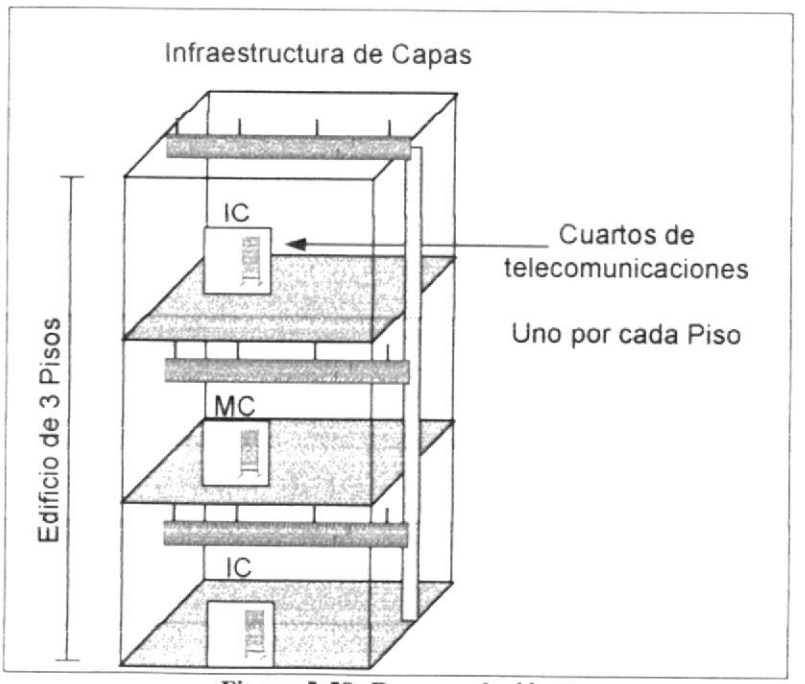


Figura 5-58: Recomendación 2

Recomendación 3:

El área que puede atenderse efectivamente por los cuartos de telecomunicación abarca un radio máximo de 60 m.

Figura 5-59: Recomendación 3

Recomendación 4:

Se recomienda un mínimo de 15 m entre el HC y la salida de telecomunicación.

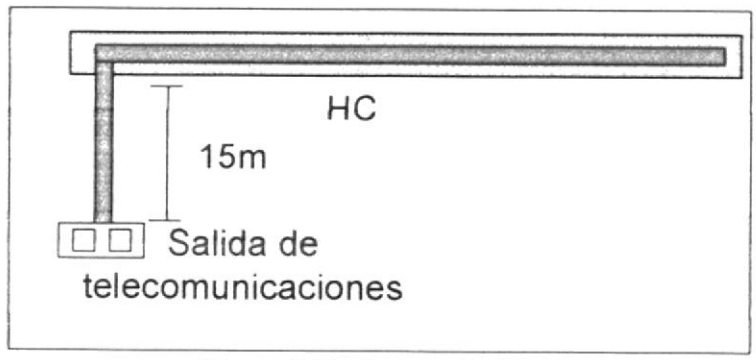


Figura 5-60: Recomendación 4

Recomendación 5:

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

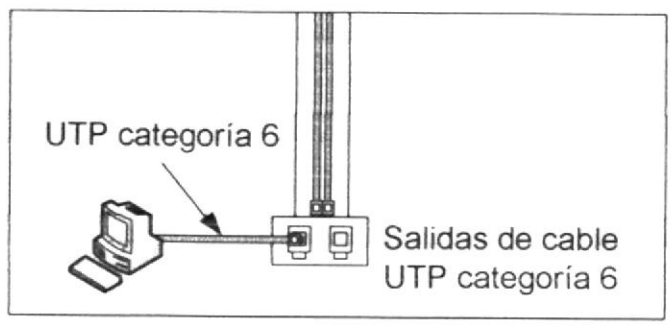


Figura 5-61: Recomendación 5

Recomendación 6:

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

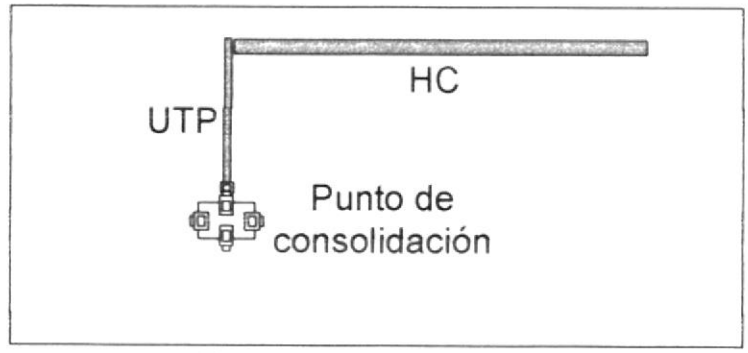


Figura 5-62: Recomendación 6

Recomendación 7:

El cableado del Backbone del edificio debe diseñarse con la capacidad de reserva suficiente para atender salidas adicionales de telecomunicación desde el MC.

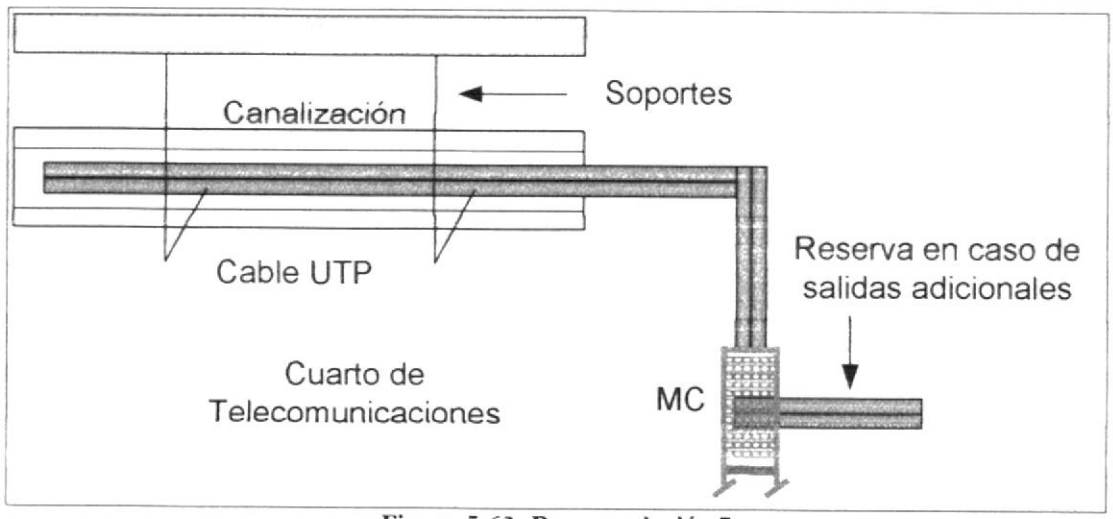


Figura 5-63: Recomendación 7

Recomendación 8:

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

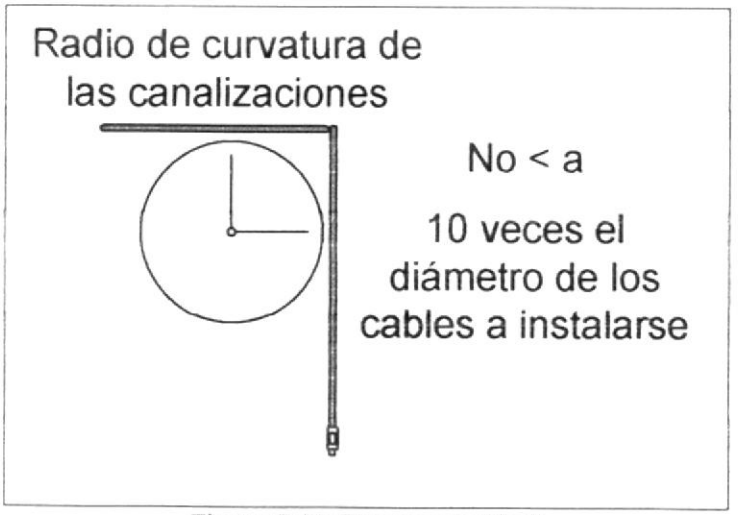


Figura 5-64: Recomendación 8

Recomendación 9:

Ningún segmento de canal obtendrá más de 2 curvas de 90° entre puntos de acceso.

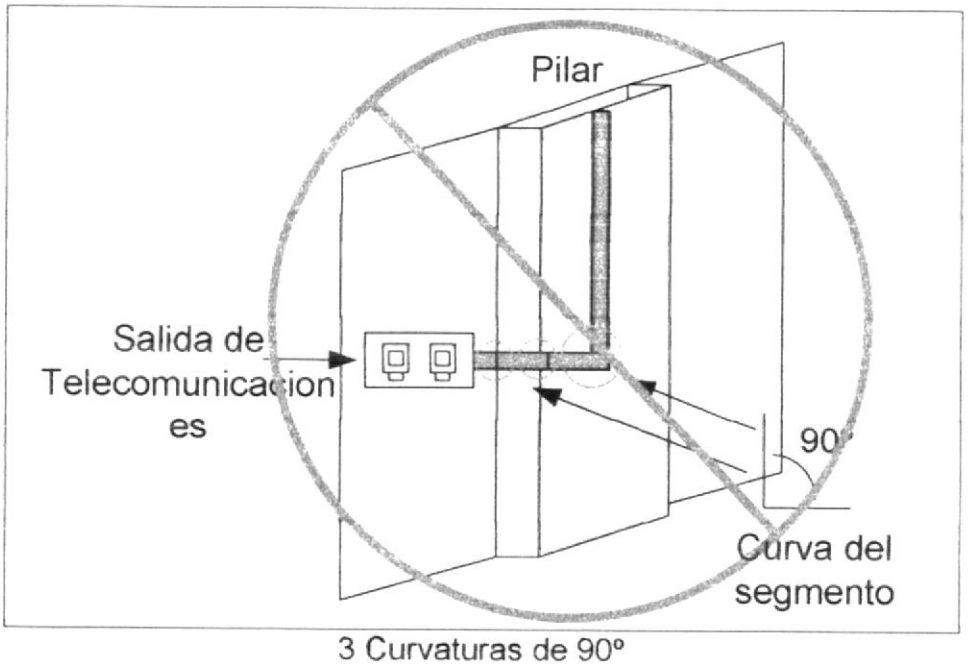


Figura 5-65: Recomendación 9

Recomendación 10:

Se recomienda que se provea, como mínimo 2 hilos de fibra óptica para cada aplicación conocida a atender por el sistema de backbone de edificios durante su periodo de planificación. Debe proveerse un factor de crecimiento del 100%.

Aplicación	Nº de hilos de Fibra
Voz	2
Video	2
LAN	2
Crecimiento	6
	12

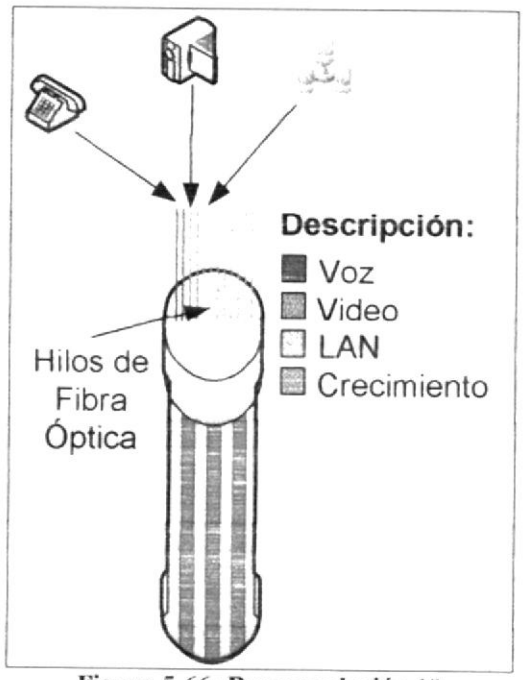


Figura 5-66: Recomendación 10

Recomendación 11:

Para cable de Backbone se recomienda un mínimo de 3 m de reserva de cable en cada extremo.

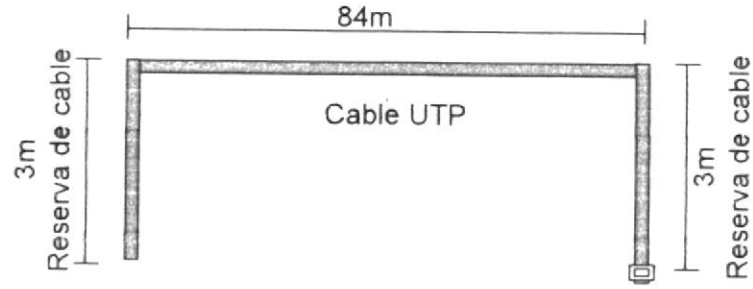


Figura 5-67: Recomendación 11

Recomendación 12:

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

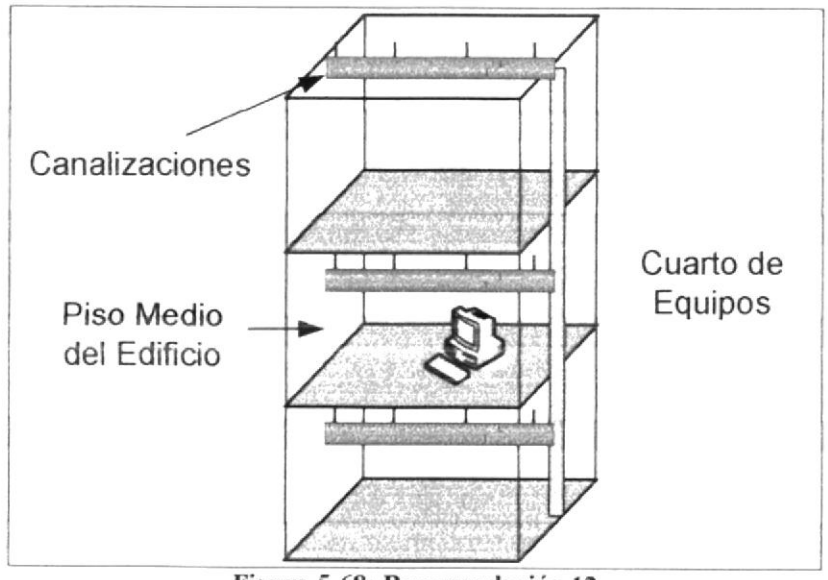


Figura 5-68: Recomendación 12

Recomendación 13:

Se recomienda que el cuarto de equipos se ubique por encima del nivel de inundación y este protegido contra infiltraciones de tuberías de agua y drenaje.

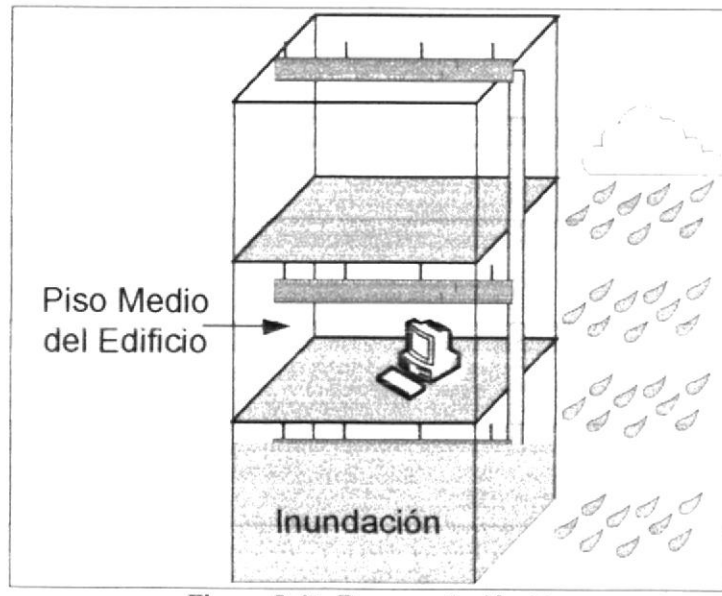


Figura 5-69: Recomendación 13

CAPÍTULO 6

CONFIGURACIÓN DE ROUTERS Y SWITCHES

6. CONFIGURACIÓN DE DISPOSITIVOS

6.1 INTRODUCCIÓN A LOS ROUTERS

Un router es un tipo especial de computador, ya que cuenta con los mismos componentes básicos que posee una computadora. Posee un CPU, memoria, bus de sistema y distintas interfaces de entrada/salida.

Los routers están diseñados para cumplir algunas funciones específicas que no realizan las computadoras. Entre algunas funciones que realiza el router mencionamos, que los routers conectan y permiten la comunicación entre dos redes y determinan cual es la mejor ruta para la transmisión de datos a través de las redes conectadas.

Todo router al igual que las computadoras, necesitan de un sistema operativo para ejecutar sus aplicaciones de software, los routers necesitan un 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.

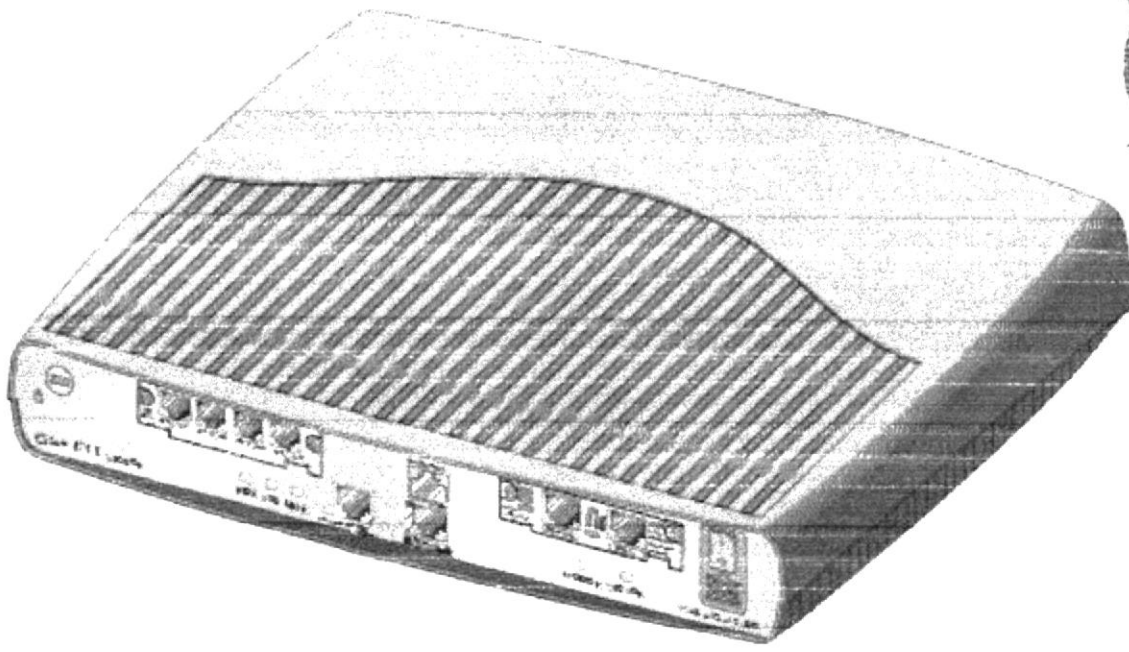


Figura 6-1: Router

6.1.1 FUNCIONES DE LOS ROUTERS

La función principal de un router es enrutar paquetes.

Podemos mencionar que un router es un dispositivo LAN **(Local Área Network):** Redes de Área Local Y WAN **(Wide Área Network):** Redes de Amplia Cobertura. El router proporciona conexiones con y entre los diversos estándares de enlace de datos y físico WAN.

6.1.2 ESTÁNDARES

- EIA/TIA - 232, V35, X.21, G.703, RDSI, T1, T3, E1 y E3, Xdsl, SONET.

6.1.3 PROTOCOLOS

Los routers mediante protocolos permite el control de los enlaces de datos de alto nivel (HDLC)

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

6.1.4 COMPONENTES INTERNOS DEL ROUTER

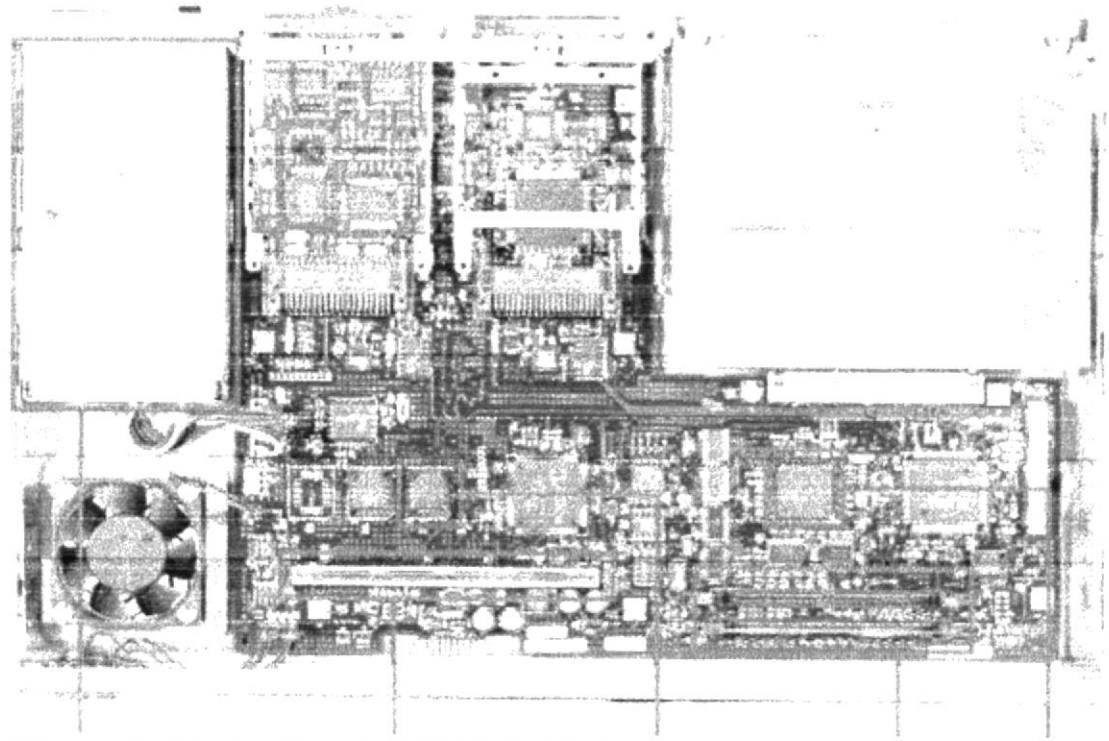


Figura 6-2: Componentes internos del Router

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

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

RAM: La memoria de acceso aleatorio (RAM) se usa para almacenar 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).

Tiene las siguientes características y funciones:

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

NVRAM: La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

La NVRAM tiene las siguientes características y funciones:

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

Memoria flash: La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los Módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.

La memoria flash tiene las siguientes características y funciones:

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

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

- La memoria de sólo lectura (ROM) tiene las siguientes características y funciones:
- Guarda las instrucciones para el diagnóstico de la prueba al inicio (POST).
- Guarda el programa bootstrap y el software básico del sistema operativo.
- Requiere del reemplazo de chips que se pueden conectar en el motherboard para las actualizaciones del software.

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

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

Las interfaces tienen las siguientes características y funciones:

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

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

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

6.1.5 SECUENCIA DE ARRANQUE

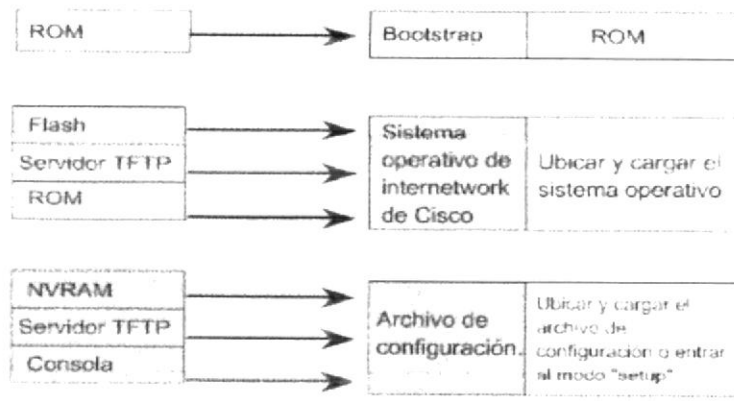


Figura 6-3: Secuencia de arranque

6.1.6 CONEXIONES EXTERNAS DEL ROUTER

La función de los puertos de administración es diferente a la de las otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red por donde se transmiten los paquetes. El puerto de administración proporciona una conexión basada en texto para la configuración y diagnóstico de fallas del router. Los puertos auxiliares y de consola constituyen las interfaces de administración comunes. Estos son puertos seriales asincronos EIA-232. Están conectados a un puerto de comunicaciones de un computador. El computador debe ejecutar un programa de emulación de Terminal para iniciar la sesión basada en texto con el router. A lo largo de esta sesión, el administrador de la red puede administrar el dispositivo.

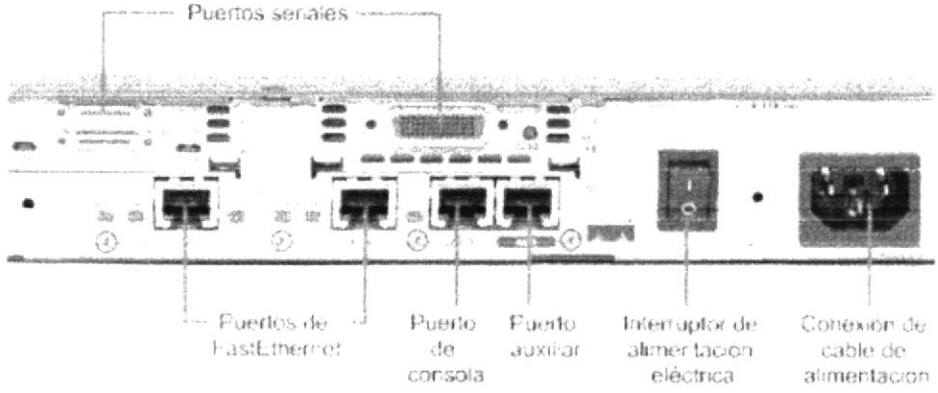


Figura 6-4: Conexiones Externas del Router

6.1.7 TECNOLOGÍAS WAN

Entre las tecnologías que soporta un router podemos mencionar:

- X.25
- ATM
- SMDS
- RDSI
- xDSL

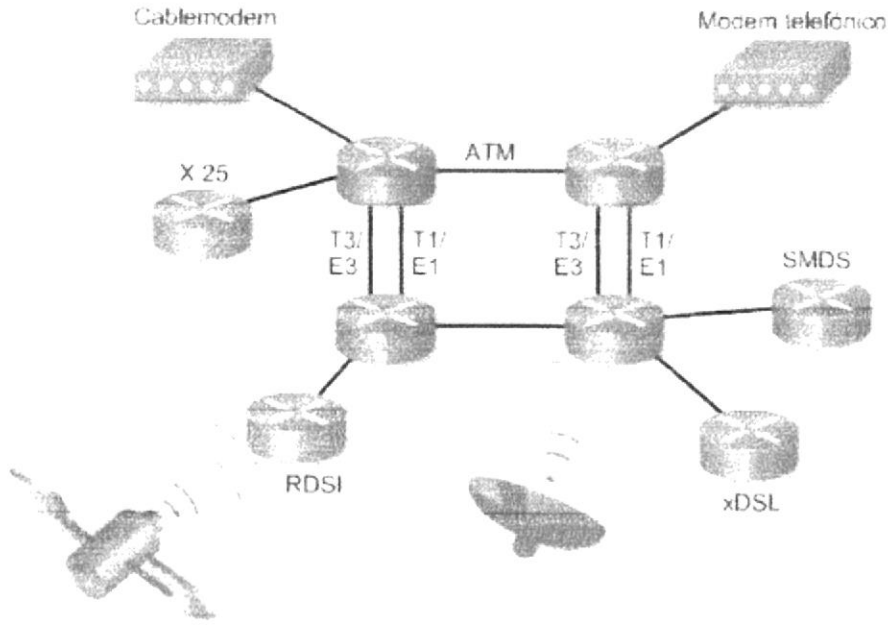


Figura 6-5: Tecnologías que posee un Router

6.1.8 CONEXIONES DEL PUERTO DE ADMINISTRACIÓN

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

Una vez que la configuración inicial se ha introducido en el router a través del puerto de consola o auxiliar, entonces, se puede conectar el router a la red para realizar un diagnóstico de fallas o monitoreo. Además, el router puede configurarse desde un lugar remoto haciendo telnet a una línea de Terminal virtual o marcando el número de un módem conectado al puerto de consola o auxiliar del router.

El puerto de consola es un puerto de administración que se utiliza para proveer acceso al router fuera de banda. Se usa para la configuración inicial de router, el monitoreo y los procedimientos de recuperación de desastres. Para realizar la conexión al puerto de consola, se usa un cable transpuesto o de consola y un adaptador RJ-45 a DB-9 para conectarse al PC.

Para conectar una Terminal al puerto de consola del router, conecte la Terminal mediante un cable transpuesto **RJ-45** a **RJ-45** y un adaptador **RJ-45** a **DB-9** o **RJ-45** a **DB-25**.

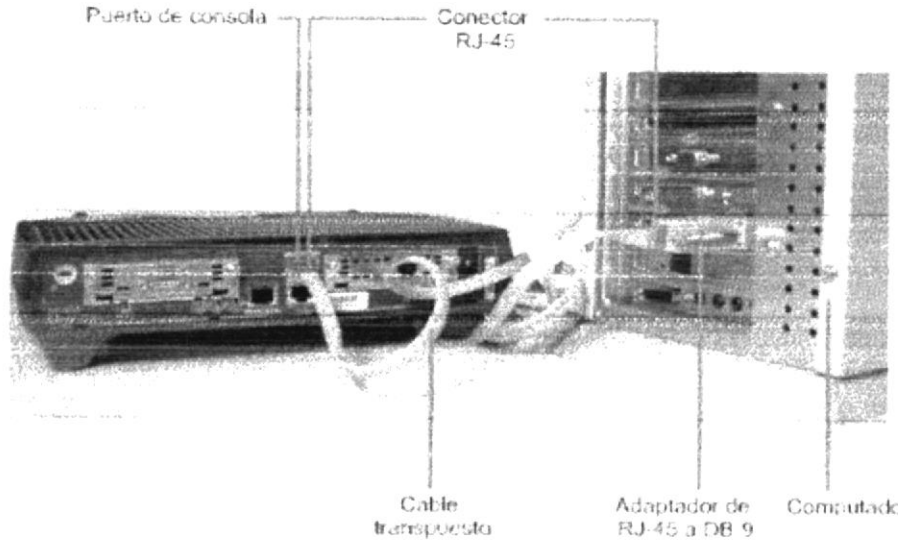


Figura 6-6: Conexiones del puerto de Administración

6.2 INTRODUCCIÓN A LOS SWITCHES

Un switch es un dispositivo de red de Capa 2 que actúa como punto de concentración para la conexión de estaciones de trabajo, servidores, routers, hubs y otros switches.

Los switches pertenecen a la tecnología estándar actual de las LAN Ethernet que utilizan una topología en estrella. Un switch ofrece varios circuitos virtuales punto a punto dedicados entre los dispositivos de red conectados, de manera que es poco probable que se produzcan colisiones.

Debido a la función dominante de los switches en las redes modernas, la capacidad para comprender y configurar switches es esencial para la asistencia técnica de la red.

Los nuevos switches tienen una configuración preestablecida con valores de fábrica. Esta configuración rara vez cumple con las necesidades de los administradores de red. Los switches se pueden configurar y administrar desde una interfaz de línea de comando (CLI). Los dispositivos de red también se pueden configurar y administrar a través de una interfaz y un navegador basados en Web. La configuración básica del switch, las actualizaciones de IOS y la recuperación de contraseñas son capacidades esenciales del administrador de red.

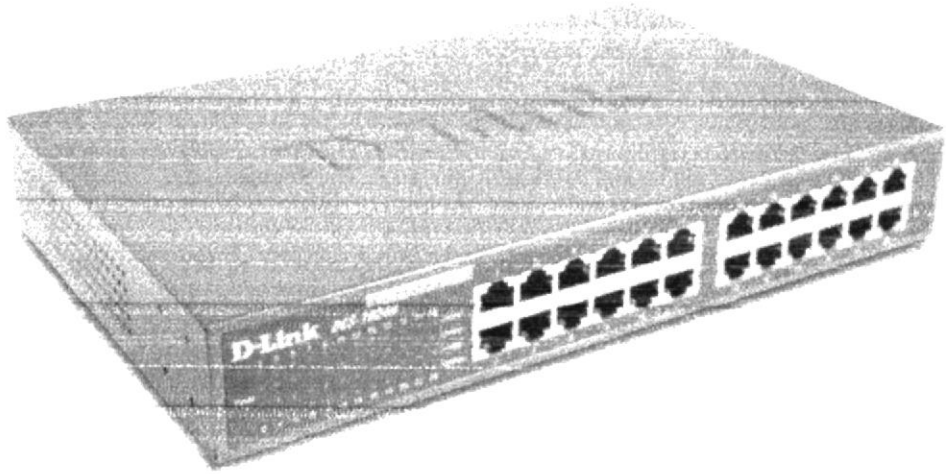


Figura 6-7: Switch

6.2.1 INTERCONEXIÓN DE CONMUTADORES Y PUENTES.

Los puentes (bridges) y conmutadores (switches) pueden ser conectados unos a los otros, pero existe una regla que dice que sólo puede existir un único camino entre dos puntos de la red. En caso de que no se siga esta regla, se forma un bucle en la red, que produce la transmisión infinita de datagramas de una red a otra.

Sin embargo, esos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

6.2.2 FUNCIONAMIENTO DE LOS CONMUTADORES

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo vaya desde el puerto origen al puerto de destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

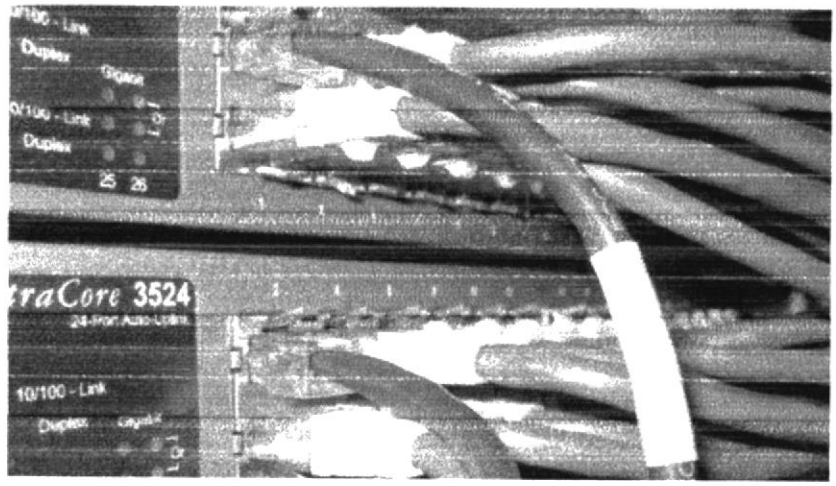


Figura 6-8: Funcionamiento de los conmutadores

6.2.3 BUCLES DE RED E INUNDACIONES DE TRÁFICO

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Como se ha comentado se emplea el protocolo spanning tree para evitar este tipo de fallos.

6.2.4 SPANNING TREE

Spanning Tree Protocol (STP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE_802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de lazos. STP es transparente a las estaciones de usuario.

Los bucles infinitos ocurren cuando hay rutas alternativas hacia una misma máquina o segmento de red de destino. Estas rutas alternativas son necesarias para proporcionar redundancia, ofreciendo una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando hay lazos en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast y multicast, al no existir ningún campo TTL (Time To Live, Tiempo de Vida) en la Capa 2, tal y como ocurre en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos casos la red queda inutilizada. Un router, por el contrario, si podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de lazos. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la LAN.

Existen varias variantes del Spaning Tree Protocol, debido principalmente al tiempo que tarda el algoritmo utilizado en converger. Una de estas variantes es el Rapid Spanning Tree Protocol

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo de tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

6.3 INTRODUCCIÓN A LAS VLAN

Una VLAN (acrónimo de Virtual LAN, red de área local virtual') es una red de computadoras lógicamente independiente. Varias VLANs pueden coexistir en un único switch físico.

Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente una computadora a otra ubicación: puede permanecer en la misma VLAN sin necesidad de ninguna reconfiguración de hardware.

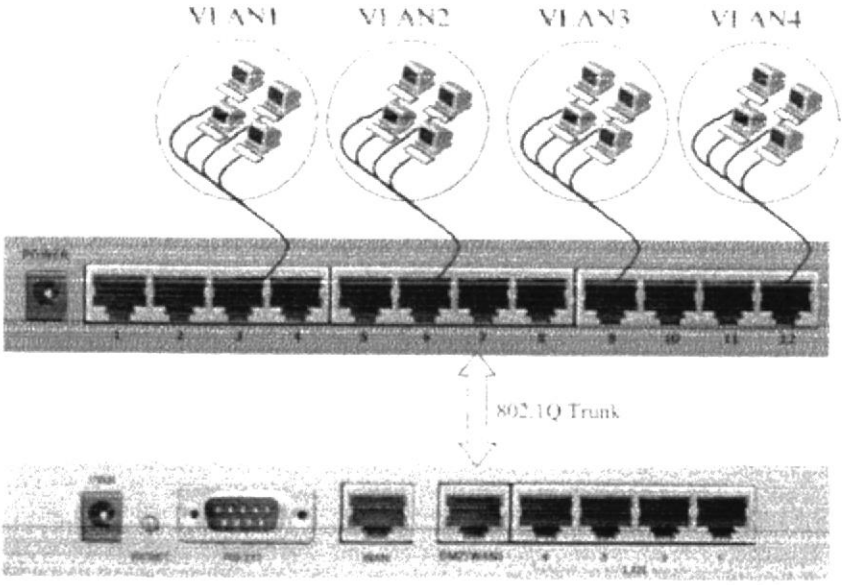


Figura 6-9: Vlan

6.3.1 PROTOCOLOS Y DISEÑO

El protocolo de etiquetado **IEEE 802.1Q** domina el mundo de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del **IEEE 802.1Q,** y el VLT (Virtual LAN Trunk) de 3Com. Algunos usuarios prefieren actualmente 802.1Q a ISL.

Los primeros diseñadores de redes solían configurar VLANs con el objeto de reducir el tamaño del dominio de colisión en un único segmento Ethernet grande, mejorando así el rendimiento. Cuando los switches Ethernet hicieron desaparecer este problema (porque no tienen dominio de colisión), el interés se desplazó a reducir el tamaño del dominio de difusión en la subcapa MAC. Las VLANs también pueden servir para restringir el acceso a recursos de red con independencia de la topología física de ésta, si bien la robustez de este método es discutible al ser el salto de VLAN (VLAN hopping) un método común de evitar tales medidas de seguridad.

Las VLANs funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).

En el contexto de las VLANs, el término trunk ('tronco') designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports ('puertos etiquetados') de dispositivos con soporte de VLANs, por lo que a menudo son enlaces switch a switch o switch a router más que enlaces a nodos. (Para mayor confusión, el término trunk también se usa para lo que Cisco denomina «canales»; véase agregación de enlaces). Un router (switch de nivel 3) funciona como backbone para el tráfico de red transmitido entre diferentes VLANs.

En los dispositivos Cisco, VTP (VLAN Trunking Protocol) permite definir dominios de VLAN, lo que facilita las tareas administrativas. VTP también permite «podar», lo que significa dirigir tráfico VLAN específico sólo a los switches que tienen puertos en la VLAN destino.

6.3.2 IEEE 802.1Q

El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes con puentes para compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

6.3.3 ASPECTOS BÁSICOS DE LAS VLAN

Una VLAN es una agrupación lógica de dispositivos o usuarios que se pueden agrupar por función, departamento o aplicación, sin importar su ubicación física.

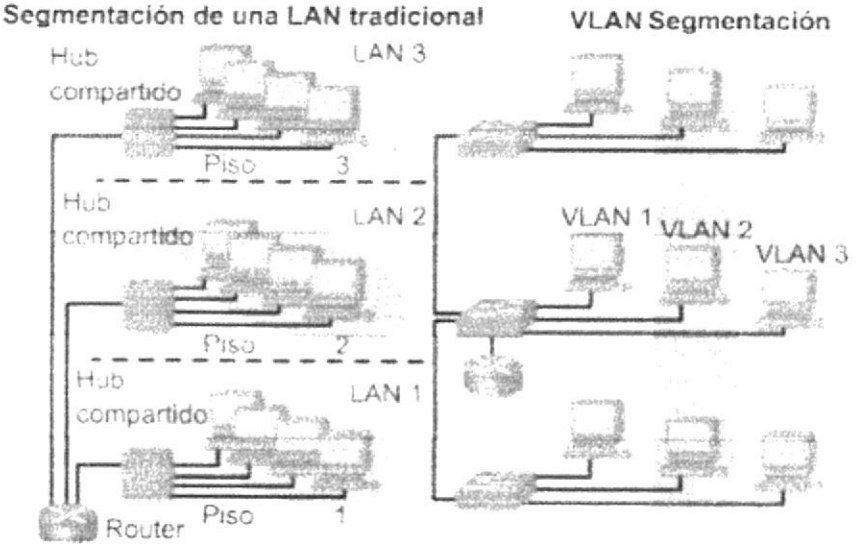


Figura 6-10: Comparación de una LAN tradicional y una VLAN

Las VLAN se configuran en el switch a través del software. Debido a la cantidad de implementaciones de VLAN que compiten entre sí es posible que deba requerirse el uso de un software propietario por parte del fabricante del switch. La agrupación de puertos y usuarios en comunidades de interés, conocidos como organizaciones VLAN, puede obtenerse mediante el uso de un solo switch o una conexión más potente entre los switches ya conectados dentro de la empresa. Al agrupar puertos y usuarios en varios switches, las VLAN pueden abarcar infraestructuras contenidas en un solo edificio o en edificios interconectados. Las VLAN ayudan a utilizar con efectividad el ancho de banda dado que comparten el mismo dominio de broadcast o la misma red de Capa 3. Las VLAN optimizan la acumulación y uso del ancho de banda. Las VLAN se disputan el mismo ancho de banda aunque los requisitos del ancho de banda pueden variar considerablemente según el grupo de trabajo o el departamento.

A continuación, presentamos algunos de los temas de configuración de las VLAN:

- Un switch crea un dominio de broadcast
- Las VLAN ayudan a administrar los dominios de broadcast
- Las VLAN se pueden definir en grupos de puerto, usuarios o protocolos
- Los switches LAN y el software de administración de red suministran un mecanismo para crear las VLAN

Las VLAN ayudan a controlar el tamaño de los dominios de broadcast y a ubicar el tráfico. Las VLAN se asocian con redes individuales. Por lo tanto, los dispositivos de red en las distintas VLAN no se pueden comunicar directamente entre sí sin la intervención de un dispositivo de enrutamiento de Capa 3.

6.3.4 ENRUTAMIENTO ENTRE VLAN

Cuando el host en un dominio de broadcast desea comunicarse con un host en otro dominio de broadcast, debe utilizarse un router.

El puerto 1 en un switch forma parte de la VLAN 1 y el puerto 2 forma parte de la VLAN 200.

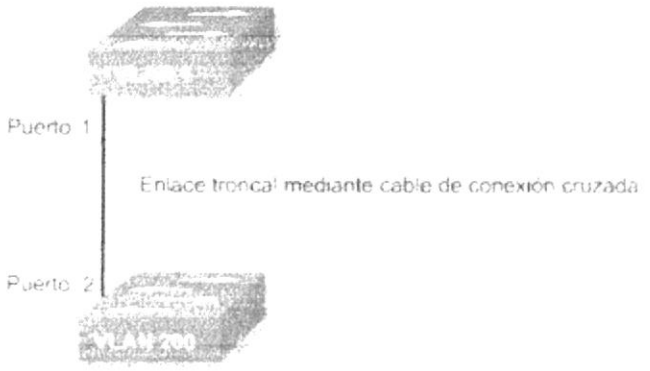


Figura 6-11: Enlace Troncal

Si todos los puertos de switch formaran parte de la VLAN 1, es posible que los hosts conectados a estos puertos puedan comunicar entre sí. Sin embargo, en este caso, los puertos forman parte de distintas VLAN, la VLAN 1 y la VLAN 200. Se debe utilizar un router si los hosts de las distintas VLAN necesitan comunicarse entre sí.

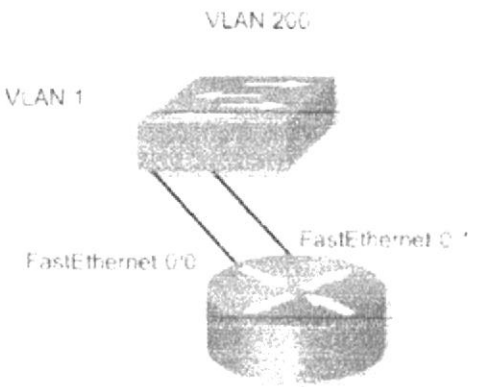


Figura 6-12: Enlace Switch - Router

Dado que los routers evitan la propagación de broadcast y utilizan algoritmos de envío más inteligentes que los switches, los routers ofrecen un uso más eficiente del ancho de banda. Esto da como resultado simultáneamente una selección de ruta flexible y óptima.

Si una VLAN abarca varios dispositivos, se utiliza un enlace troncal para interconectar los dispositivos. El enlace troncal transporta el tráfico para varias VLAN

Recuerde que cuando un host en una VLAN desea comunicarse con un host de otra VLAN, se debe utilizar un router.

6.3.5 INTERFACES FÍSICAS Y LÓGICAS

En una situación tradicional, una red con cuatro VLAN requeriría cuatro conexiones físicas entre el switch y el router externo.

A medida que las tecnologías como por ejemplo el Enlace inter-switch (ISL) se vuelven más comunes, los diseñadores de red empiezan a utilizar enlaces troncales para conectar los routers a los switches. A pesar de que se puede utilizar cualquier tecnología de enlace troncal como por ejemplo ISL, 802.1Q, 802.10 o la emulación LAN (LANE), los enfoques basados en Ethernet como por ejemplo ISL y 802.1Q son más comunes.

A medida que aumenta la cantidad de VLAN en una red, el enfoque físico de tener una interfaz de router por VLAN se vuelve rápidamente no escalable. Las redes con muchas VLAN deben utilizar el enlace troncal de VLAN para asignar varias VLAN a una interfaz de router única.

El router puede admitir varias interfaces lógicas en enlaces físicos individuales. Por ejemplo, la interfaz de FastEthernet 0/0 puede admitir tres interfaces virtuales numeradas como FastEthernet 0/0.1, 0/0.2 y 0/0.3.

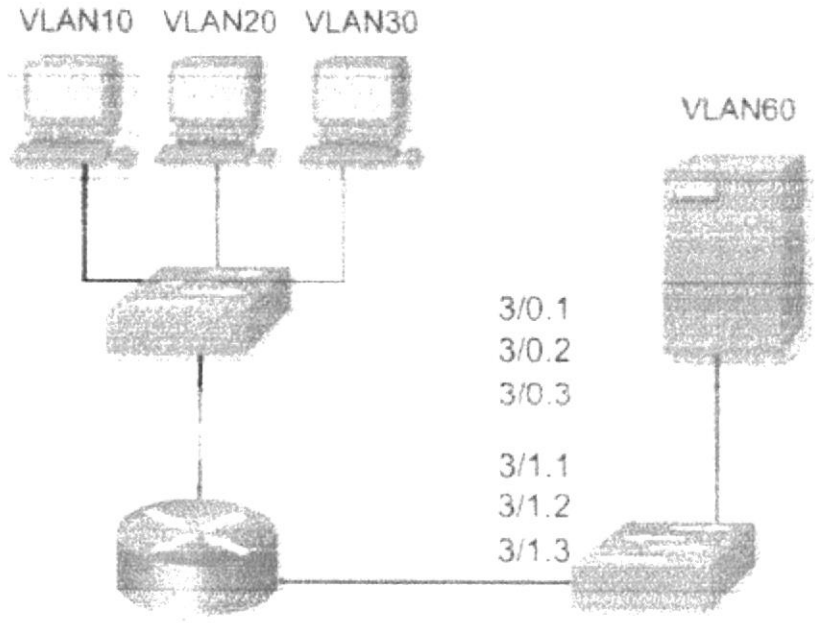


Figura 6-13: Interfaces físicas y lógicas

La ventaja principal del uso del enlace troncal es una reducción en la cantidad de puertos de router y switch que se utiliza. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de router conectado a un enlace troncal puede ampliarse hasta un número mucho más alto de VLAN que el diseño de "un enlace por VLAN".

6.4 ENRUTAMIENTO

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino.

Cuando los routers usan enrutamiento dinámico, esta información se obtiene de otros routers. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios.

6.4.1 ENRUTAMIENTO DINÁMICO

El objetivo de un protocolo de enrutamiento es crear y mantener una tabla de enrutamiento.

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.

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

Los sistemas autónomos (AS) permiten la división de la red global en subredes de menor tamaño, más manejables.

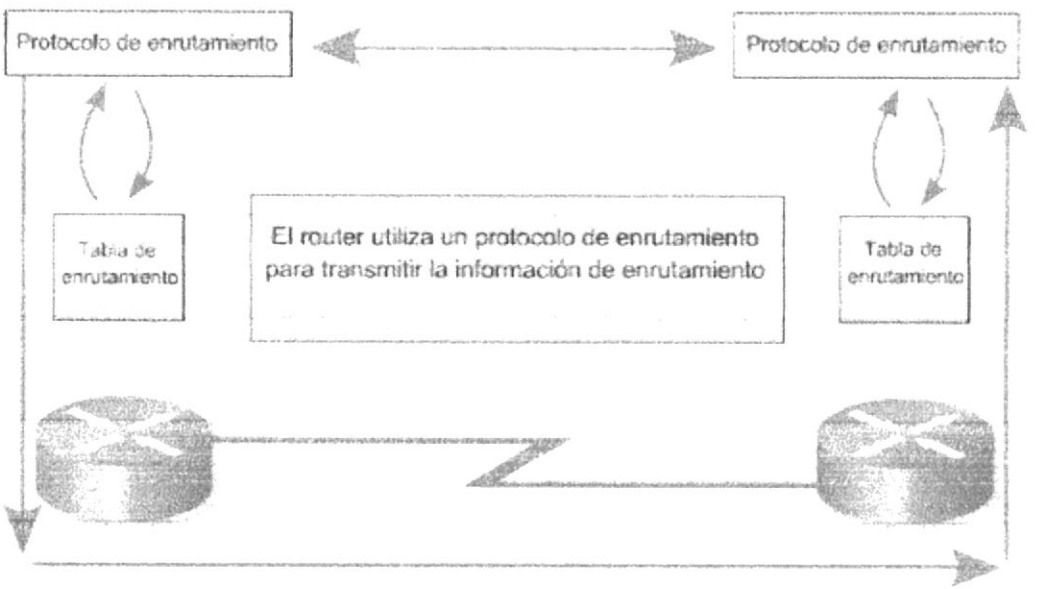


Figura 6-14: Enrutamiento dinámico

6.4.2 ENRUTAMIENTO ESTÁTICO

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:

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

Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando **ip route**.

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

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta. A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

6.4.3 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, los routers están configurados con una ruta por defecto 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. En realidad, una ruta por defecto es una ruta estática especial que utiliza este formato:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 s0
```

La máscara 0.0.0.0, cuando se ejecuta el AND lógico hacia la dirección de IP de destino del paquete, siempre obtiene la red 0.0.0.0. Si el paquete no coincide con una ruta más específica en la tabla de enrutamiento, será enviado hacia la red 0.0.0.0.

6.5 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 permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios.

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.

6.5.1 TIPOS DE PROTOCOLOS DE ENRUTAMIENTO

El Protocolo de información de enrutamiento (RIP). Sus características principales son las siguientes:

- 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.

El Protocolo de enrutamiento interior de gateway (IGRP) es un protocolo patentado desarrollado por Cisco. Entre las características de diseño claves del IGRP se destacan las siguientes:

- 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.

El EIGRP es un protocolo mejorado de enrutamiento por vector-distancia, patentado por Cisco. Las características claves del EIGRP son las siguientes:

- Es un protocolo mejorado de enrutamiento por vector-distancia.
- 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.

6.5.2 CLASES DE PROTOCOLOS DE ENRUTAMIENTO

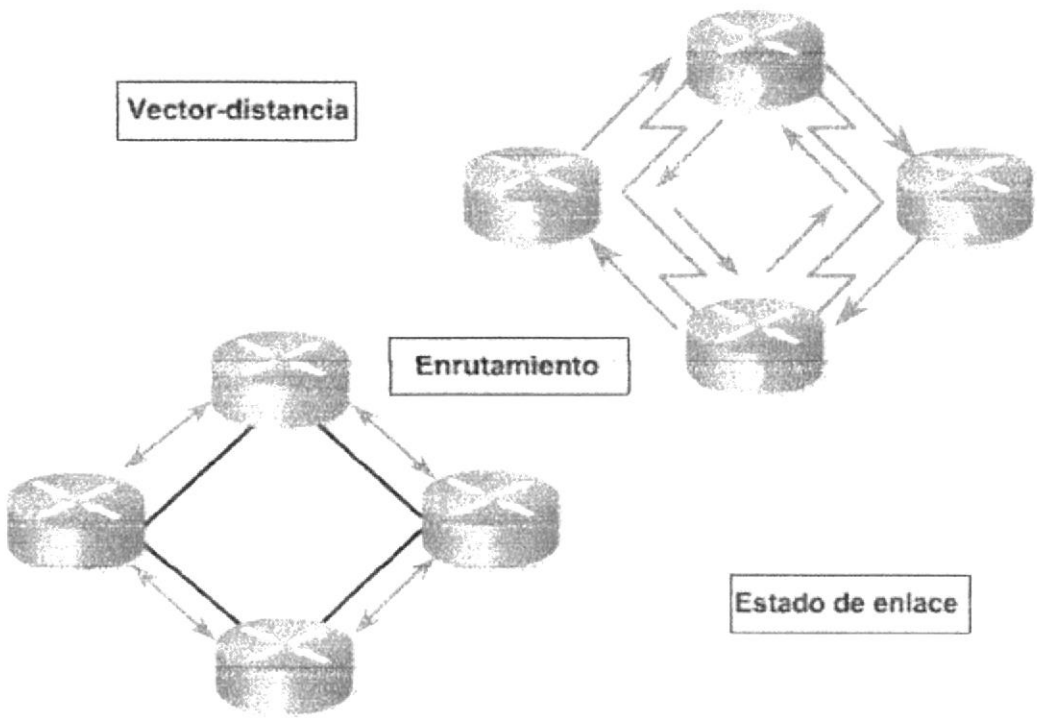


Figura 6-15: Protocolos de enrutamiento

6.5.3 PROTOCOLO DE ENRUTAMIENTO RIP

El Protocolo RIP es un protocolo de enrutamiento por vector-distancia, usado en miles de redes en todo el mundo. Debido a que el protocolo RIP se basa en estándares abiertos, es fácil de implementar y hace que resulte interesante para algunos administradores de redes, aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados.

RIP ha evolucionado a lo largo de los años 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 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.

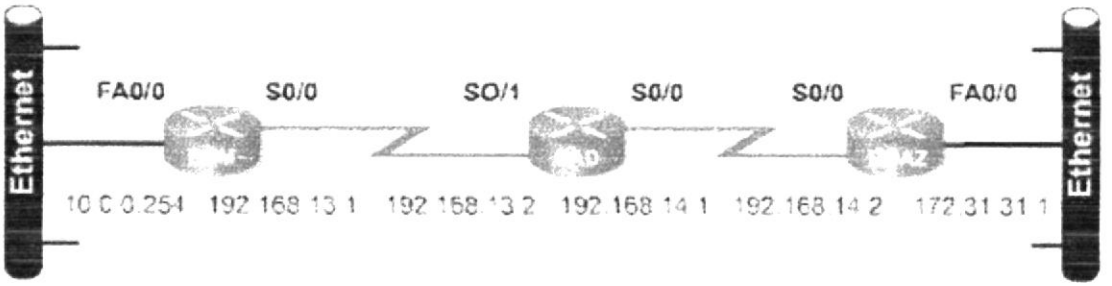


Figura 6-16: Protocolo de enrutamiento RIP

6.5.3.1 CARACTERÍSTICAS DE 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.
- Protocolo tipo broadcast
- Máximo numero de rutas 6, por defecto son 4

6.5.3.2 COMO CONFIGURAR RIP

Router(config)#router rip → Selecciona al RIP como protocolo de enrutamiento.
Router(config-router)#network 10.0.0.0 → Especifica una red conectada directamente.
Router(config-router)#network 192.168.12.0 → Especifica una segunda red conectada directamente.
Router(config)#show ip protocols → Verifica que un protocolo de enrutamiento este bien configurado y que se encuentra recibiendo actualizaciones.
Router(config)#show ip route → Verifica que las rutas recibidas por los routers RIP vecinos estén instaladas en la tabla de enrutamiento.

6.5.3.3 PROTOCOLO DE ENRUTAMIENTO RIP V2

Rip V2 posee mayor capacidad para transportar información relativa al enrutamiento de paquetes. Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de las tablas.

- RIP v2 es una versión mejorada de RIP v1
- Es un protocolo de vector-distancia que usa el número de saltos como métrica.
- Utiliza temporizadores de espera para evitar los bucles de enrutamiento – la opción por defecto es 180 segundos.
- Utiliza horizonte dividido para evitar los bucles de enrutamiento.
- Utiliza 16 saltos como métrica para representar una distancia infinita
- RIP v2 ofrece el enrutamiento por prefijo, que le permite enviar información de máscara de subred con la actualización de la ruta.

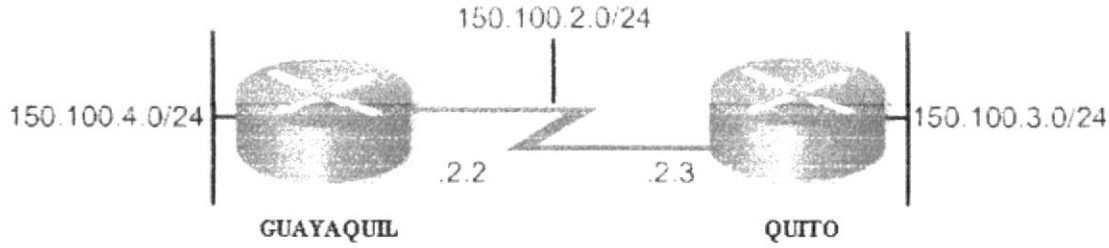


Figura 6-17: Protocolo de enrutamiento RIP versión 2

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.

6.5.3.4 COMO CONFIGURAR RIP V2

Router(config)#router rip → selecciona al RIP como protocolo de enrutamiento.
Router(config)#version 2 → define la version del RIP
Router(config-router)#network 192.168.0.0 → especifica una red conectada directamente.
Router(config-router)#network 192.168.1.0 → especifica una segunda red conectada directamente.
Router(config)#show ip protocols → Verifica que un protocolo de enrutamiento este bien configurado y que se encuentra recibiendo actualizaciones.
Router(config)#show ip route → Verifica que las rutas recibidas por los routers RIP vecinos estén instaladas en la tabla de enrutamiento.
Router(config)#show ip interface brief → Se puede usar para visualizar un resumen de la información y del estado de la interfaz.

6.5.4 PROTOCOLOS DE ENRUTAMIENTO DE ESTADO DE ENLACE

Los algoritmos de estado de enlace también se conocen como SPF ("primero la ruta más corta"). 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 vector-distancia provee información indeterminada sobre las redes lejanas y no tiene información acerca de los routers distantes. El algoritmo de enrutamiento de estado del enlace mantiene información completa sobre routers lejanos y su interconexión.

El algoritmo SPF determina la conectividad de la red. El router construye esta topología lógica en forma de árbol, con él mismo como raíz, y cuyas ramas son todas las rutas posibles hacia cada subred de la red. Luego ordena dichas rutas, y coloca las rutas más cortas primero (SPF). El router que primero conoce de un cambio en la topología envía la información al resto de los routers, para que puedan usarla para hacer sus actualizaciones y publicaciones.

El protocolo público conocido como "Primero la ruta más corta" (OSPF) es un protocolo de enrutamiento de estado de enlace no patentado. Las características clave del OSPF son las siguientes:

- Es un protocolo de enrutamiento de estado de 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.

El Protocolo de gateway de frontera (BGP) es un protocolo de enrutamiento exterior. Las características claves del BGP son las siguientes:

- Es un protocolo de enrutamiento exterior por vector-distancia.
- Se usa entre ISPs o entre los ISPs y sus clientes.
- Se usa para enrutar el tráfico de Internet entre sistemas autónomos.

6.5.5 PROTOCOLO DE ENRUTAMIENTO OSPF

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). El término "libre" en "Primero la ruta libre más corta" significa que está abierto al público y no es propiedad de ninguna empresa.
OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes. Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento.

OSPF es apropiado para Internetworks grandes y escalables y la mejor ruta se determina a base de la velocidad del enlace. OSPF selecciona la ruta mediante el costo, una métrica basada en el ancho de banda. Los routers que implementan los protocolos de vector-distancia necesitan menos memoria y menos potencia de procesamiento que los que implementan el protocolo OSPF.

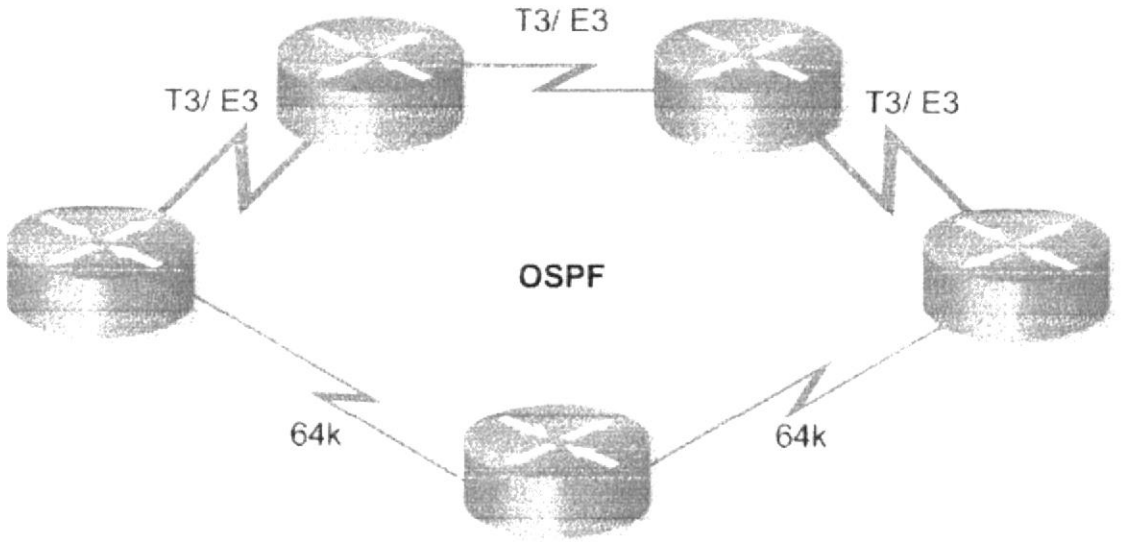


Figura 6-18: Protocolo de enrutamiento OSPF

6.5.5.1 CARACTERÍSTICAS DE OSPF

- Mantienen una compleja base de datos de información de topología.
- Mantiene información completa sobre routers lejanos y su interconexión.
- OSPF se basa en las normas de código abierto, lo que significa que muchos fabricantes lo pueden desarrollar y mejorar.
- Reúnen la información de ruta de todos los demás routers de la red o dentro de un área definida de la red.
- Envían actualizaciones desencadenadas sólo cuando se haya producido un cambio de red.
- Usan un mecanismo hello para determinar la posibilidad de comunicarse con los vecinos
- Admite VLSM

OSPF ofrece soluciones a los siguientes problemas:

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

6.5.5.2 TIPOS DE REDES OSPF

Las interfaces OSPF reconocen tres tipos de redes:

- Multiacceso de broadcast como por ejemplo Ethernet.
- Redes punto a punto.
- Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay.

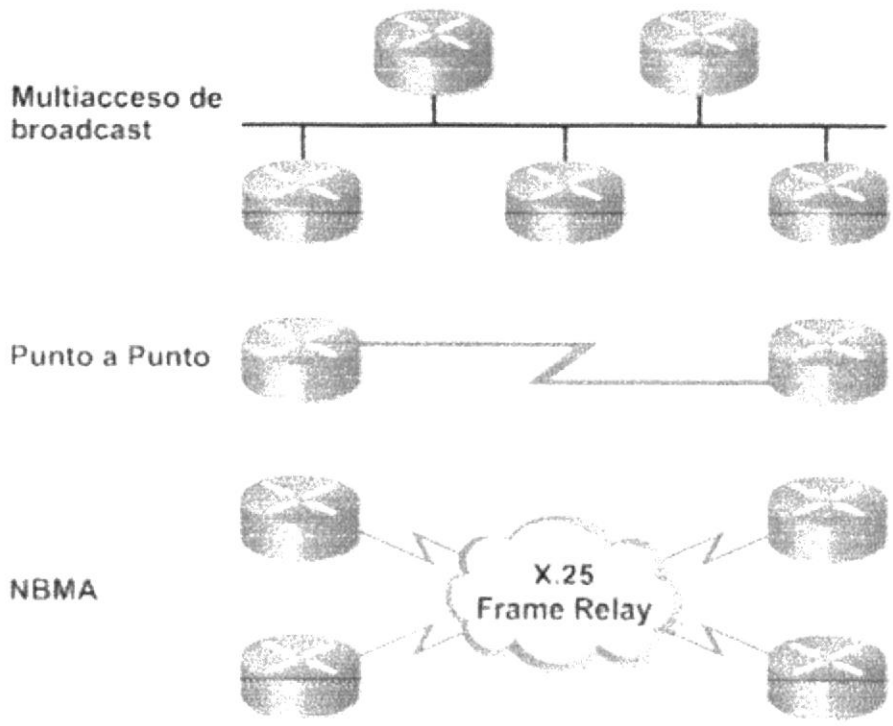


Figura 6-19: Tipos de red OSPF

6.5.6 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.

Para habilitar el enrutamiento OSPF, utilice la sintaxis de comando de configuración global:

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.

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. Índica 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.

6.5.6.1 DIRECCIÓN DE LOOPBACK OSPF

Cuando se inicia el proceso OSPF, Cisco IOS utiliza la dirección IP activa local más alta como su ID de router OSPF. Si no existe ninguna interfaz activa, el proceso OSPF no se iniciará. Si la interfaz activa se desactiva, el proceso OSPF se queda sin ID de router y por lo tanto deja de funcionar hasta que la interfaz vuelve a activarse.

Para asegurar la estabilidad de OSPF, deberá haber una interfaz activa para el proceso OSPF en todo momento. Es posible configurar una interfaz de loopback, que es una interfaz lógica, para este propósito. Al configurarse una interfaz loopback, OSPF usa esta dirección como ID del router, sin importar el valor. En un router que tiene más de una interfaz loopback, OSPF toma la dirección IP de loopback más alta como su ID de router.

Para crear y asignar una dirección IP a una interfaz de loopback use los siguientes comandos:

Router(config)#**interface loopback** number
Router(config-if)#**ip address 192.168.12.1 255.255.255.255**

Se considera buena práctica usar interfaces loopback para todos los routers que ejecutan OSPF. Esta interfaz de loopback se debe configurar con una dirección que use una máscara de subred de 32 bits de 255.255.255.255. Una máscara de subred de 32 bits se denomina una máscara de host porque la máscara de subred especifica la red de un host. Cuando se solicita que OSPF publique una red loopback, OSPF siempre presenta la dirección loopback como una ruta de host con una máscara de 32 bits.

6.5.6.2 VERIFICACIÓN DE CONFIGURACIÓN OSPF

Para verificar la configuración de OSPF existe una serie de comandos show. Se explica la manera en que los comandos show se pueden utilizar para realizar el diagnóstico de fallas de OSPF.

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

Show ip route. - Esto muestra las rutas que el router conoce y describe como se conocieron. 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 comando 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.

6.6 CONFIGURACIONES EN EL ROUTER

6.6.1 MODOS DE INTERFAZ DE USUARIO

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

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

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

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

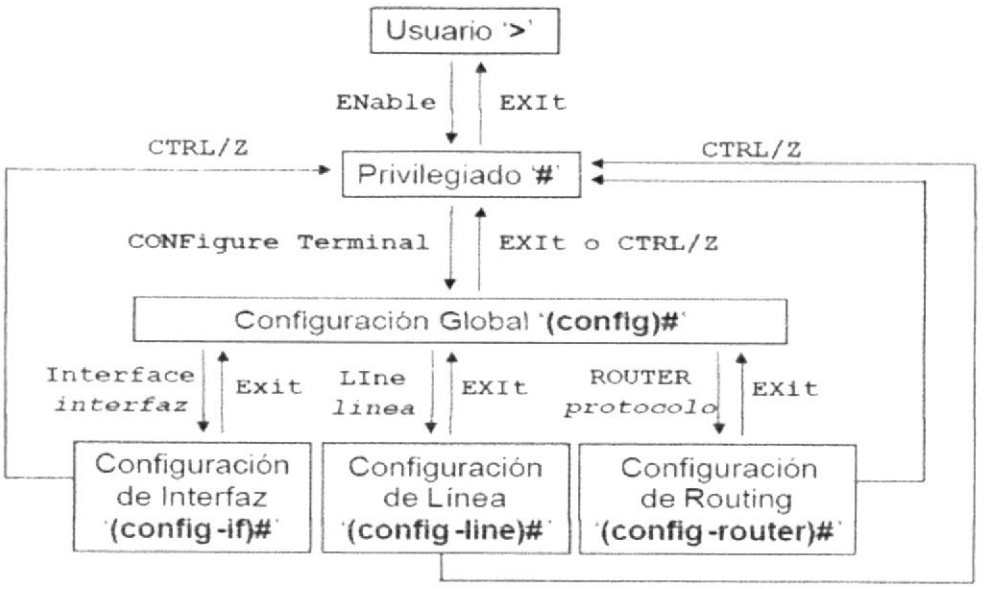


Figura 6-20: Tipos de usuarios

Sólo se puede ingresar al modo de configuración global desde el modo EXEC privilegiado. Los siguientes son modos específicos a los que también se puede ingresar desde el modo de configuración global:

- Interfaces
- Sub-interfaces
- Línea
- Router
- Mapas de enrutamiento

Para regresar al modo EXEC usuario desde el modo EXEC privilegiado, se pueden ejecutar los comandos disable o exit. Para regresar al modo EXEC privilegiado desde el modo de configuración global, ejecute exit o Control-Z. Control-Z también se puede usar para regresar directamente al modo EXEC privilegiado desde cualquier modo de configuración global secundario.

El modo de configuración global, a menudo abreviado como 'global config', es el modo de configuración principal. Estos son algunos de los modos de operación a los que se puede ingresar desde el modo de configuración global:

- Modo de interfaz
- Modo de línea
- Modo router
- Modo de subinterfaz
- Modo de controlador

Al ingresar a estos modos específicos, la petición de entrada del router cambia para señalar el modo de configuración en uso. Todo cambio de configuración que se realice, tendrá efecto únicamente en las interfaces o procesos relativos a ese modo particular.

Al escribir 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.

6.6.2 CONFIGURACIÓN DEL NOMBRE DE ROUTER

Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante el comando hostname seguido del nombre que le queramos asignar al router.
Al presionar 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 configurar.

6.6.3 CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER

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

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

Se debe fijar contraseñas en una o más de las líneas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante Telnet.

Normalmente, los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY. 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. Los siguientes comandos se utilizan para establecer contraseñas en las líneas de VTY:

Los comandos **enable password y enable secret** 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. Se recomienda habilitar siempre enable secret, ya que a diferencia de enable password, la contraseña estará siempre cifrada. Estos son los comandos que se utilizan para configurar las contraseñas:

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**. El siguiente comando se utiliza para cifrar las contraseñas al mostrar los datos de configuración:

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.

6.6.4 USO DE LOS COMANDOS SHOW

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

- **show interfaces:** Muestra las estadísticas completas de todas las interfaces del router. Para ver las estadisticas de una interfaz especifica, ejecute el comando show interfaces seguido de la interfaz especifica y el número de puerto. Por ejemplo:
- **show controllers serial:** Muestra información especifica 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 especifica o información de un map class.

6.6.5 CONFIGURACIÓN DE UNA INTERFAZ SERIAL

Es posible configurar una interfaz serial desde la consola o a través de una línea de Terminal virtual. Siga estos pasos para configurar una interfaz serial:

1. Ingrese al modo de configuración global
2. Ingrese al modo de configuración de interfaz
3. Especifique la dirección de la interfaz y la máscara de subred
4. Si el cable de conexión es DCE, fije la velocidad de sincronización. Omita este paso si el cable es DTE.
5. 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. Configura la dirección de IP mediante los siguientes comandos:

Las interfaces seriales necesitan una señal de sincronización que controle la comunicación. En la mayoría de los entornos, un dispositivo DCE, por ejemplo un CSU, proporciona dicha señal. Por defecto, los routers Cisco son dispositivos DTE, pero se pueden configurar como dispositivos DCE.

Tal vez, las interfaces de router que más se usan en los servicios WAN son las interfaces seriales.

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.

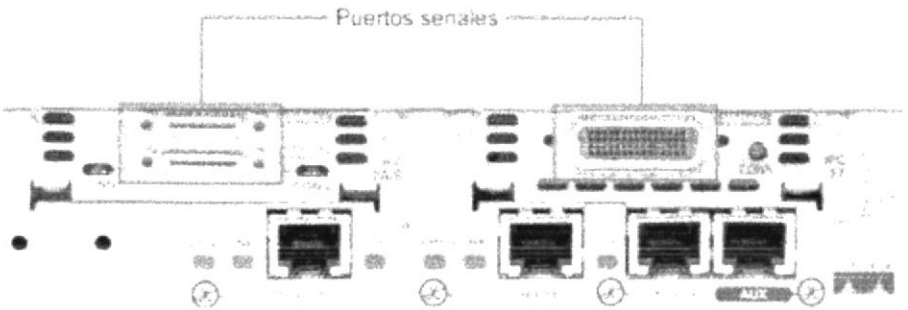


Figura 6-21: Tipos de Puertos Seriales

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.

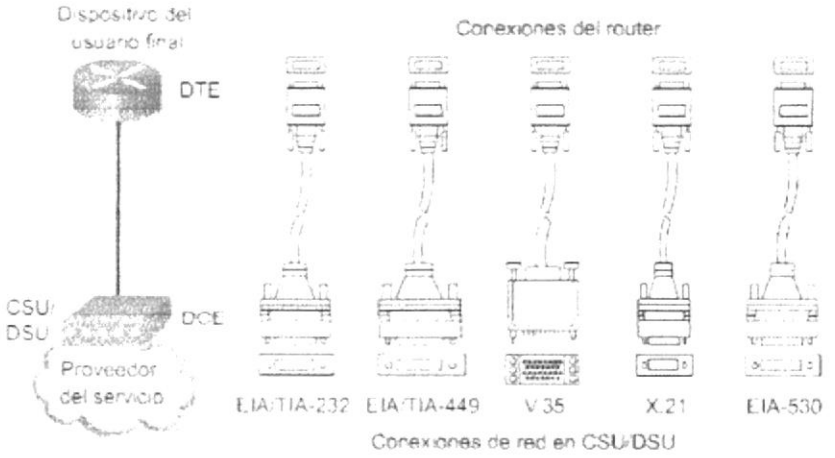


Figura 6-22: Conexiones DTE / DCE

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.

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

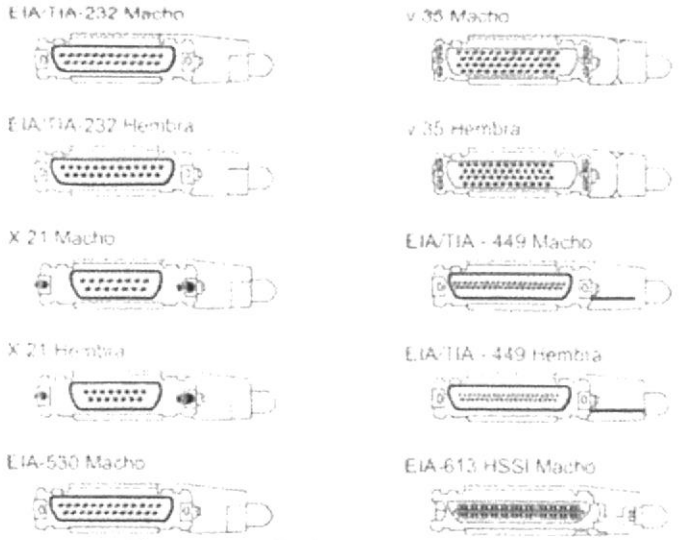


Figura 6-23: Seriales que posee un Router

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.

Se utilizará una velocidad de sincronización de 64000. Los comandos para fijar la velocidad de sincronización y activar una interfaz serial son los siguientes:

6.6.6 CONFIGURACIÓN DE UNA INTERFAZ ETHERNET

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

Para configurar una interfaz Ethernet, siga estos pasos:

1. Ingrese al modo de configuración global
2. Ingrese al modo de configuración de interfaz
3. Especifique la dirección de la interfaz y la máscara de subred
4. 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.

6.6.7 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 especifico. La descripción de la interfaz puede ayudar a un usuario de red a recordar información específica de la interfaz, como por ejemplo, a cuál red atiende dicha interfaz. La descripción es sólo un comentario escrito acerca de la interfaz.

6.6.8 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.

El procedimiento para configurar la tabla de host es:

1. Ingrese al modo de configuración global en el router.
2. Ejecute el comando **ip host** seguido del nombre del router y todas las direcciones de IP asociadas con las interfaces en cada router.
3. Repita el proceso, hasta que todos los routers de la red hayan sido configurados.
4. Guarde la configuración en la NVRAM.

6.6.9 LISTAS DE CONTROL DE ACCESO (ACL'S)

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

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACL'S). Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior.

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

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

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

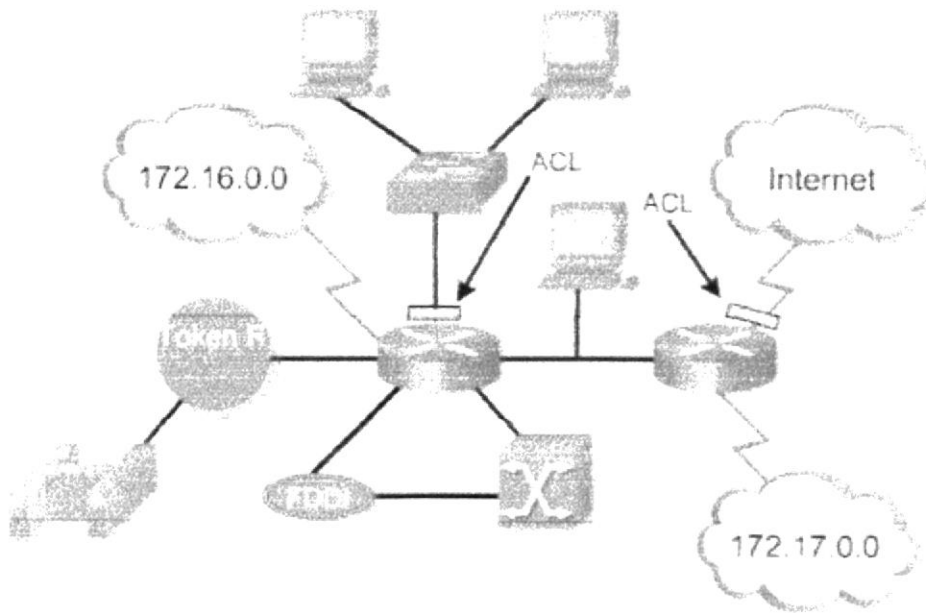


Figura 6-24: Gráfico de ubicación de ACL'S

6.6.9.1 FUNCIONAMIENTO DE LAS ACL

El orden en el que se ubican las sentencias de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL.

Una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo. Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice **deny any** (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea deny any no sea visible como última línea de una ACL, está ahí y no permitirá que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada. Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el deny any al final de las ACL para reforzar la presencia dinámica de la prohibición implícita deny.

6.6.9.2 CREACIÓN DE LAS ACL

Las ACL se crean en el modo de *configuración global*. Existen varias clases diferentes de ACL`s: estándar, extendidas, IPX, AppleTalk, entre otras. Cuando configura las ACL en el router, cada ACL debe identificarse de forma única, asignándole un número. Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista.

Después de ingresar al modo de comando apropiado y que se decide el número de tipo de lista, el usuario ingresa sentencias de lista de acceso utilizando el comando **access-list,** seguida de los parámetros necesarios. Este es el primero de un proceso de dos pasos. El segundo paso consiste en asignar la lista a la interfaz apropiada.

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

6.6.10 FUNCIÓN DE LA MÁSCARA WILDCARD

Una máscara wildcard es una cantidad de 32-bits que se divide en cuatro octetos. Una máscara wildcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar como tratar los bits de la dirección IP correspondiente. Las máscaras wildcard no guardan relación funcional con las máscaras de subred. Se utilizan con distintos propósitos y siguen distintas reglas. Las máscaras de subred y las máscaras de wildcard representan dos cosas distintas al compararse con una dirección IP. Las máscaras de subred usan unos y ceros binarios para identificar las porciones de red, de subred y de host de una dirección IP. Las máscaras de wildcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.

Durante el proceso de máscara wildcard, la dirección IP en la sentencia de la lista de acceso tiene la máscara wildcard aplicada a ella. Esto crea el valor de concordancia, que se utiliza para comparar y verificar si esta sentencia ACL debe procesar un paquete o enviarlo a la próxima sentencia para que se lo verifique. La segunda parte del proceso de ACL consiste en que toda dirección IP que una sentencia ACL en particular verifica, tiene la máscara wildcard de esa sentencia aplicada a ella. El resultado de la dirección IP y de la máscara debe ser igual al valor de concordancia de la ACL

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones **any y host**. Para explicarlo de forma sencilla, la opción **any** reemplaza la dirección IP con **0.0.0.0** y la máscara wildcard por **255.255.255.255**. Esta opción concuerda con cualquier dirección con la que se la compare. La máscara 0.0.0.0 reemplaza la opción host. Esta máscara necesita todos los bits de la dirección ACL y la concordancia de dirección del paquete. Esta opción sólo concuerda con una dirección.

Router(config)#access-list 1 **permit** 0.0.0.0 255. 255. 255. 255

Agregar un número identificador a la acl, colocar la palabra reservada permit, la cual aceptará la condición a establecer y posteriormente el rango de direcciones a aceptar, en éste caso se acepta todas las direcciones Ip's con todas sus máscaras.

Router(config)#access-list 1 **permit any**

El ejemplo del párrafo anterior se lo puede resumir con la palabra reservada **any**, la cual es equivalente a 0.0.0.0 255.255.255.255

Router(config)#access-list 1 permit 192.168.12.15 0.0.0.0

Agregar un número identificador a la acl, colocar la palabra reservada permit, la cual aceptará la condición a establecer y posteriormente la dirección ip con su wildcard correspondiente, la misma que permitirá el acceso sólo a la ip específica.

Router(config)#access-list 1 permit host 192.168.1215

6.6.11 GRÁFICO DE DISPOSITIVOS DE COMUNICACIÓN WAN (RIP - OSPF)

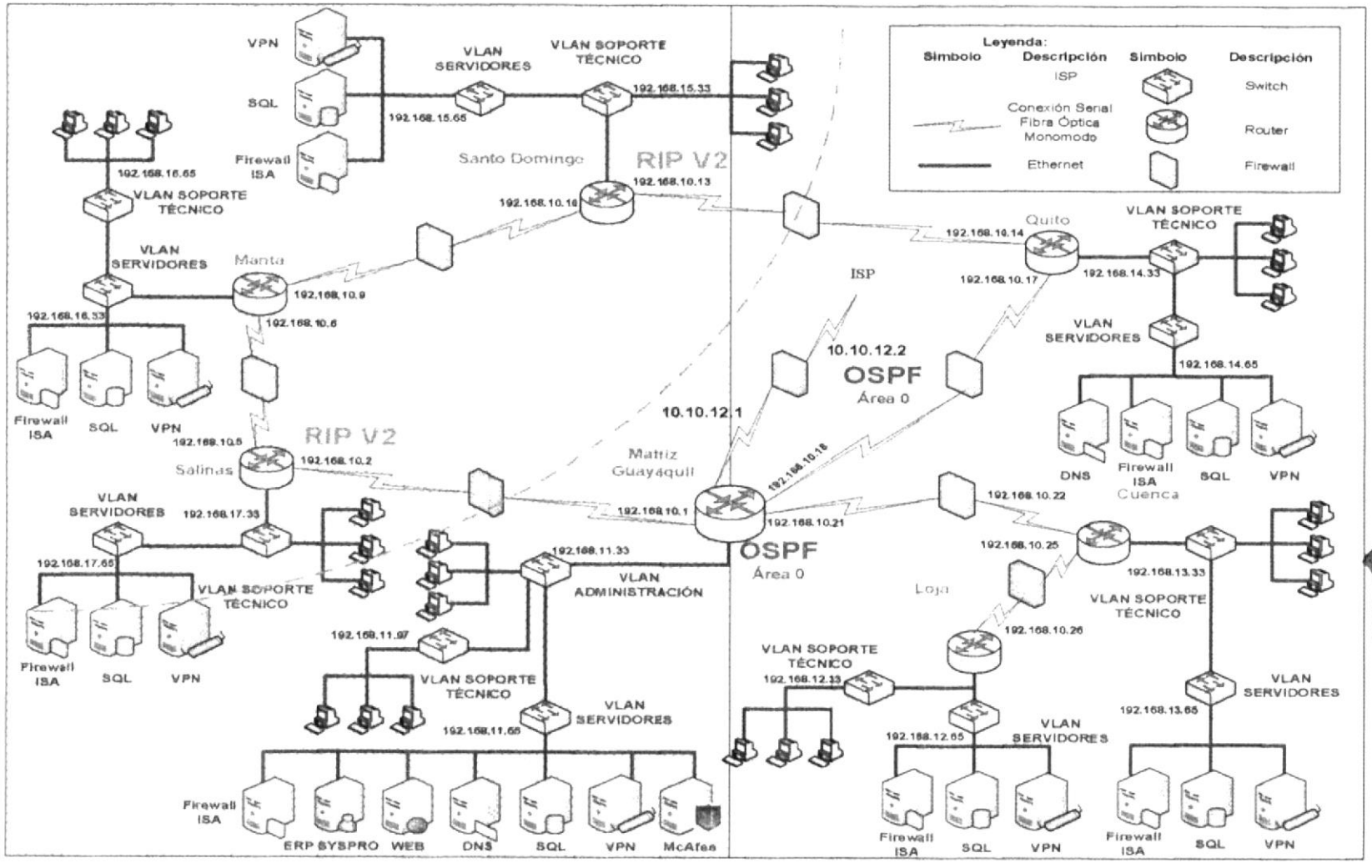


Figura 6-25: Dispositivos de Comunicación Wan

6.6.12 PROCEDIMIENTO PARA LA CONFIGURACIÓN DE LOS ROUTERS

Ahora se procederá a configurar paso a paso los diferentes Routers de la empresa Compuhelp.

6.6.12.1 CONEXIÓN DE UNA TERMINAL CON LA CONSOLA DEL ROUTER

Antes de empezar, se debe tener claro que la conexión se realizará a través de la Aplicación HyperTerminal de Windows.

HyperTerminal es un programa que se puede utilizar para conectarse con otros equipos, sitios Telnet, sistemas de boletines electrónicos (BBS, Bulletin Board Systems), servicios en línea y equipos host, mediante un módem, un cable de módem nulo o una conexión (Winsock) TCP/IP.

Pasos a seguir:

1. Con un cable transpuesto **RJ-45** a **RJ-45** y un adaptador **RJ-45** a **DB-9** o **RJ-45** a **DB-25** conectar de una Terminal (PC – Personal Computer) al puerto de consola del Router.
2. Abra la aplicación HyperTerminal siguiendo los siguientes pasos.

➢ En el Escritorio de Windows de clic con el botón izquierdo en el menú "Inicio"

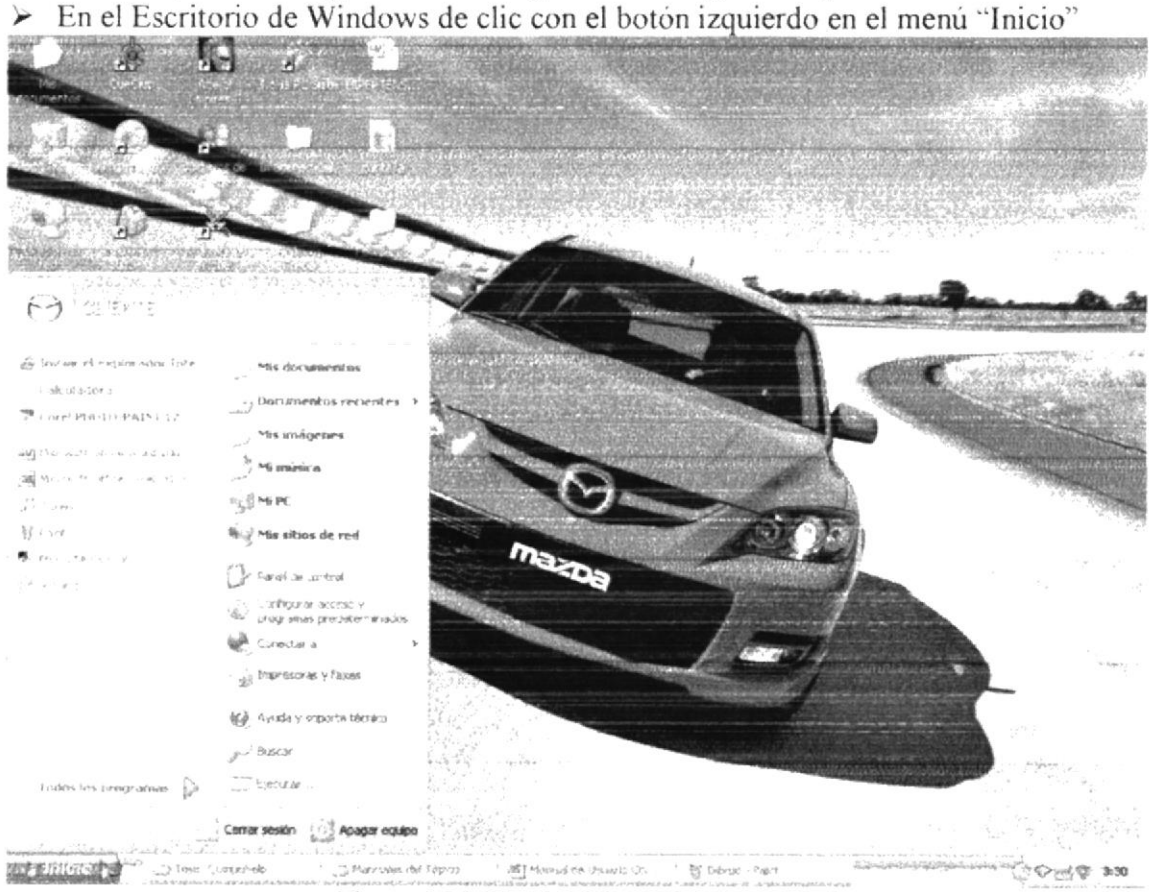


Figura 6-26: Menú Inicio en Windows XP

- En el menú desplegable busque la opción "Todos los Programas" o "Programas" según la versión y de clic con el botón izquierdo la cual desplegará otro pequeño submenú.

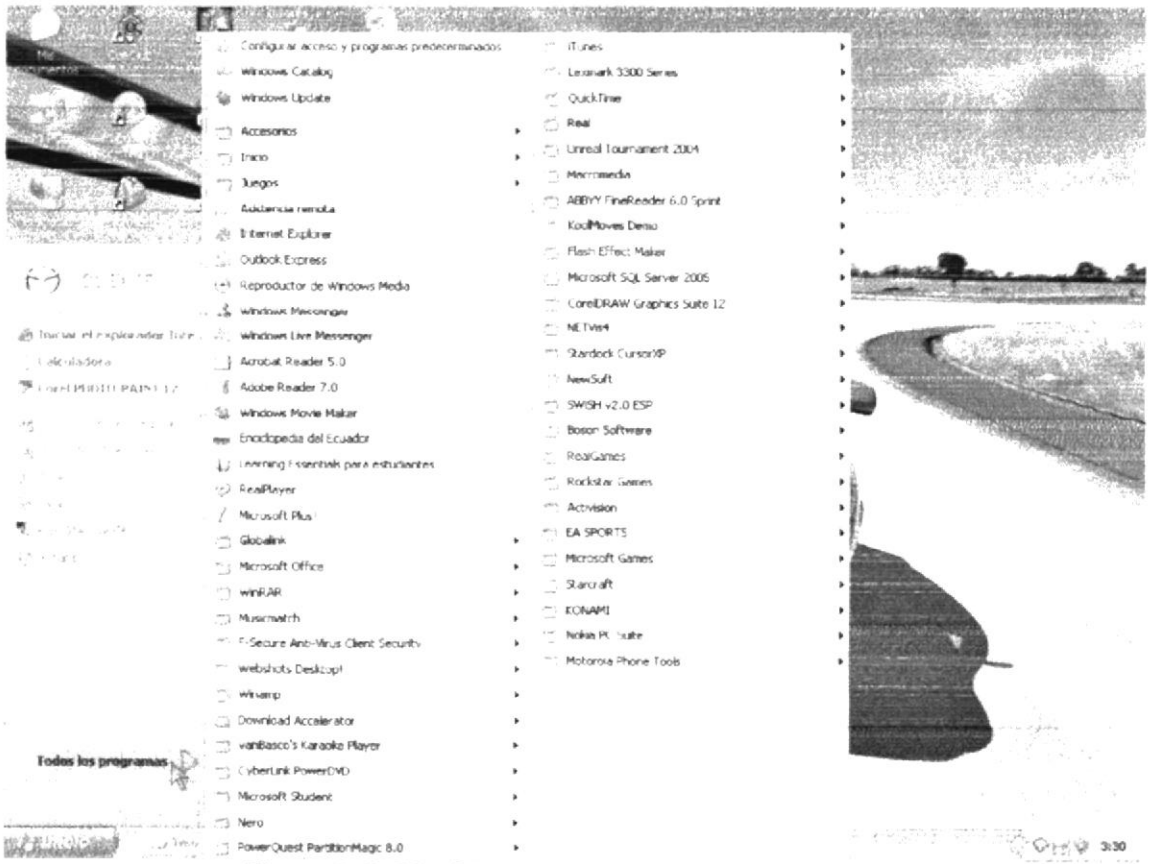


Figura 6-27: Menú Todos los Programas en Windows XP

- En este submenú busque la opción "Accesorios" y de clic izquierdo, la cual hará acceder a un nuevo nivel de submenú.

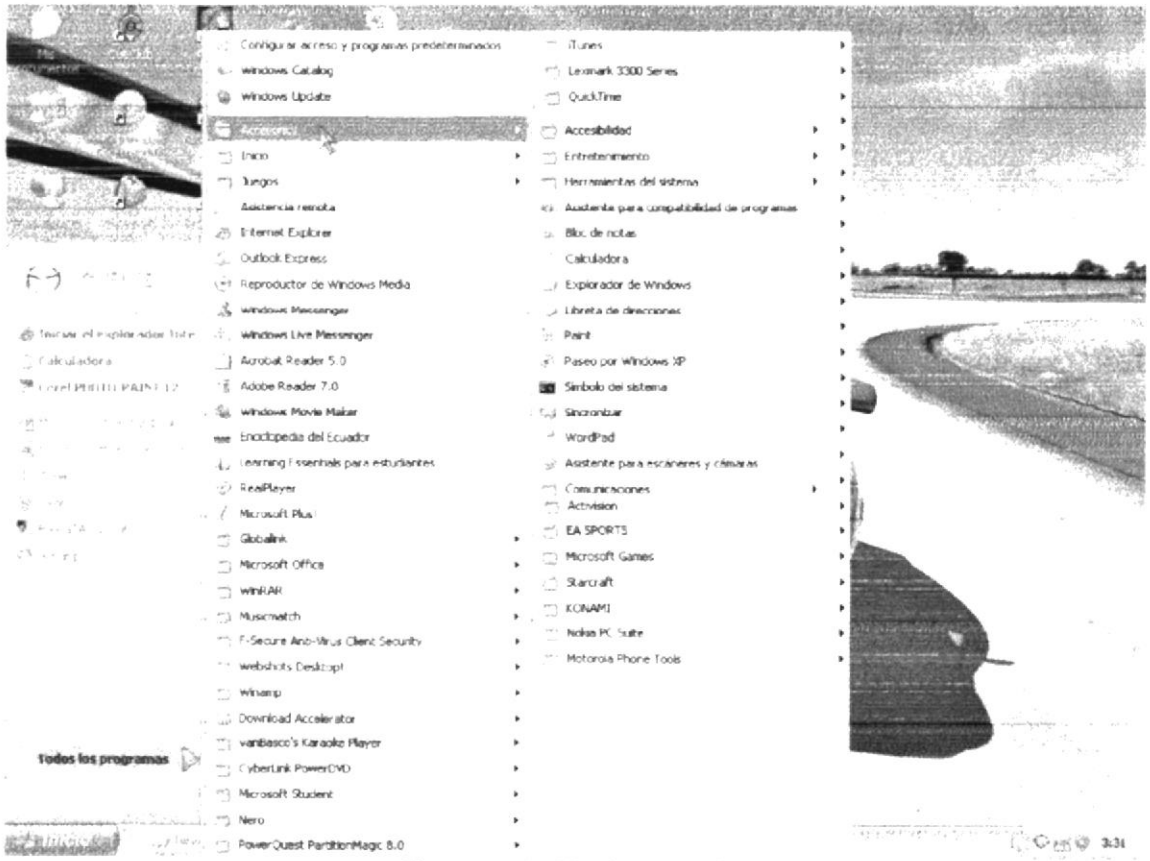


Figura 6-28: Menú Accesorios

- En este submenú aparecerán algunas de las herramientas que proporciona Windows, y la que interesa es la de Comunicaciones, de clic izquierdo.

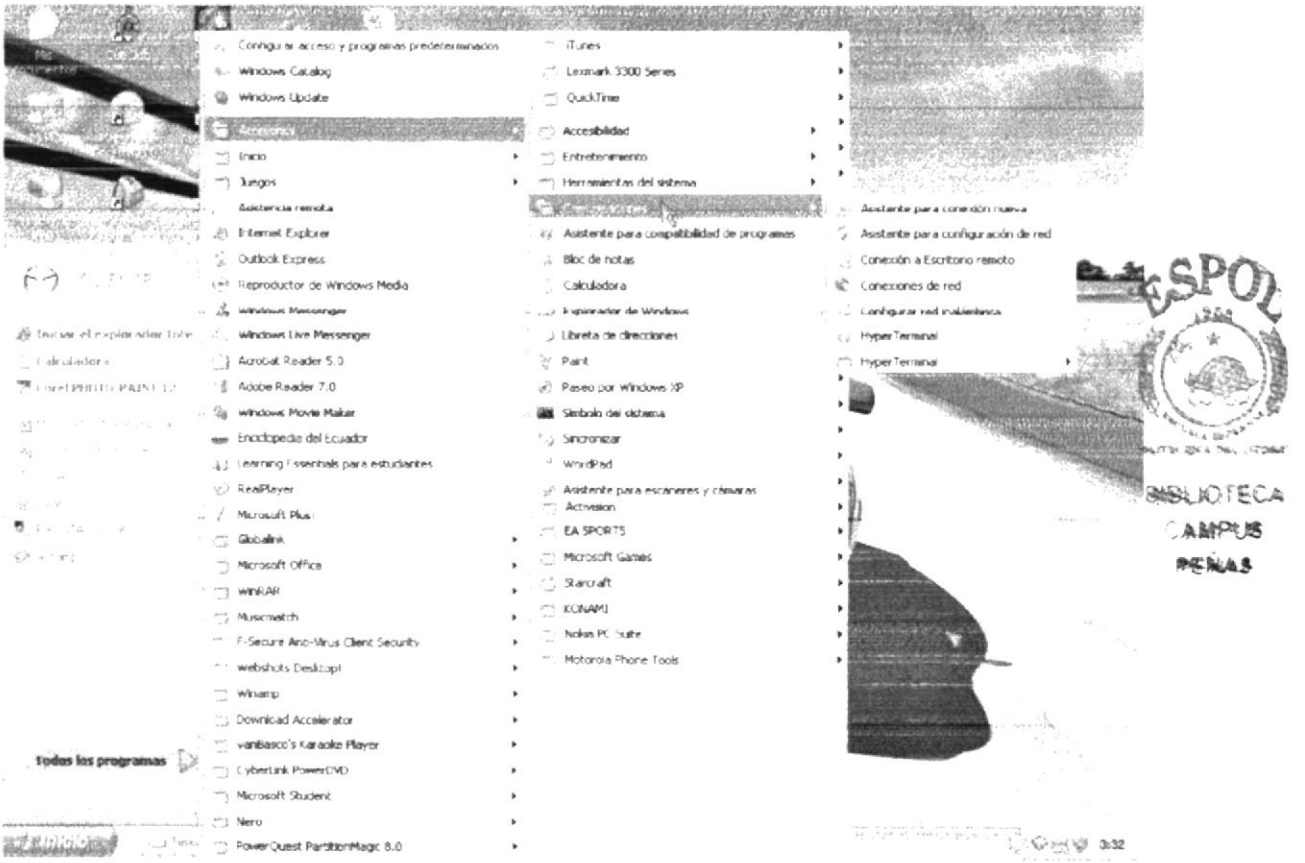


Figura 6-29: Menú Comunicaciones

- Busque la aplicación de HyperTerminal en el submenú que se desplegó y de clic izquierdo.

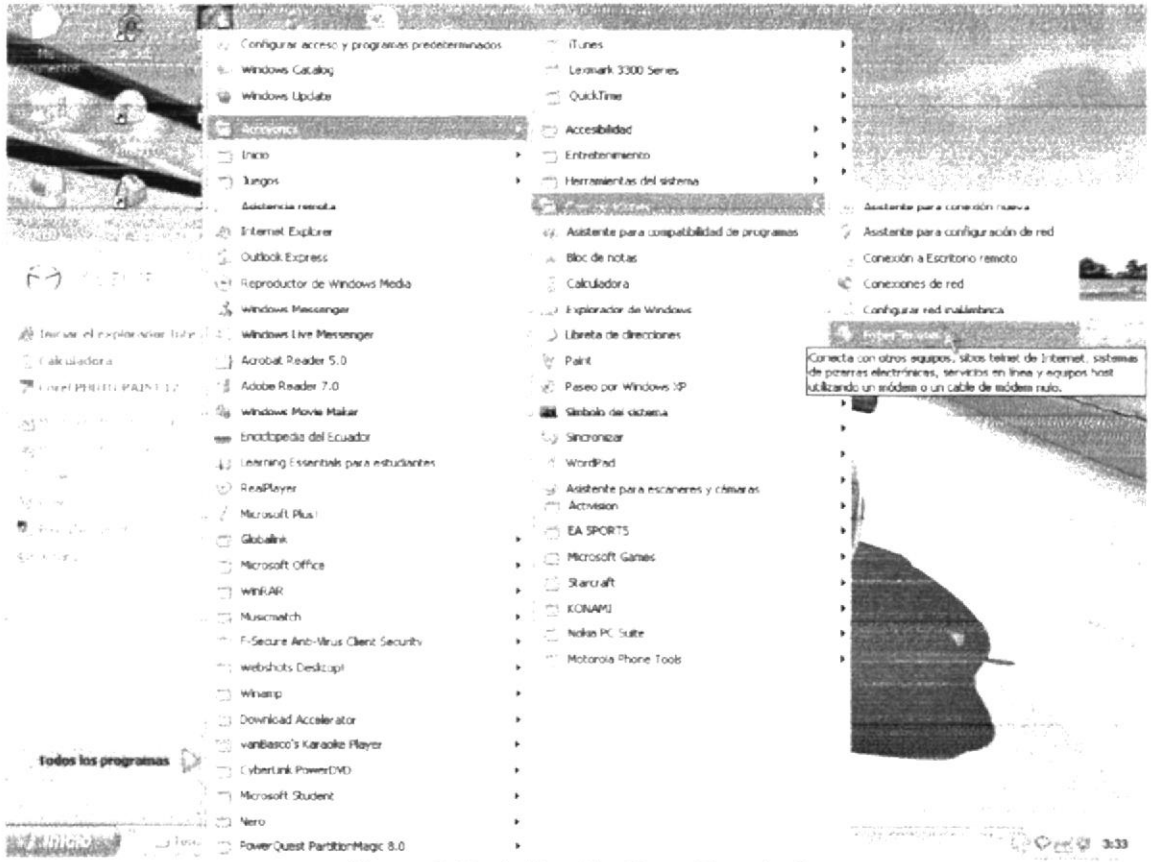


Figura 6-30: Aplicación HyperTerminal

3. Una vez que se ha encontrado de clic izquierdo en el menú de HyperTerminal, si es la primera vez que se accede a esta aplicación, aparecerá una ventana de Advertencia, donde se recomienda establecer la Aplicación HyperTerminal como programa predeterminado de Telnet.

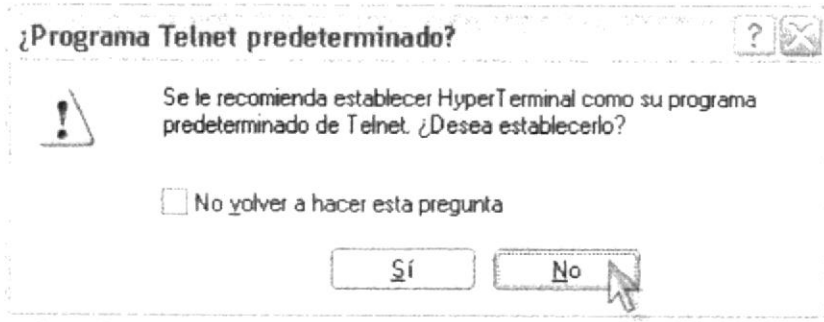


Figura 6-31: Recomendación de programa para Telnet Aplicación HyperTerminal

- La primera opción es si se desea volver a ver esta pregunta la próxima vez que se acceda al HyperTerminal. Esta opción no afectará en lo más mínimo a la conexión realizada.
- Ahora presenta dos opciones de respuesta referente a la recomendación que hace Windows, si se acepta "Sí" automáticamente aparecerá una ventana, la cual le solicita cierta información para una conexión mediante un MODEM; pero como este no es el caso simplemente "cancelamos", y automáticamente aparecerá la ventana de "Descripción de conexión" de la HyperTerminal.

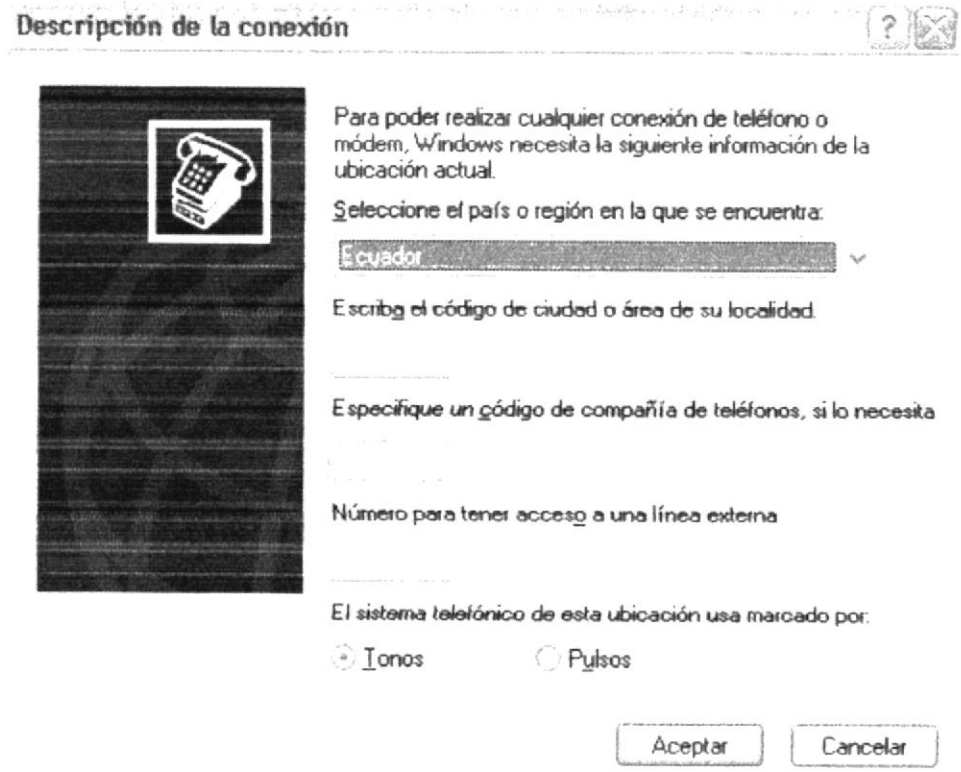


Figura 6-32: *Menú Información de Ubicación*

- Si en un caso en la ventana que Windows recomienda establecer a la aplicación HyperTerminal como predeterminada para Telnet, se la cancela, automáticamente aparecería la ventana de "Descripción de la conexión" de la HyperTerminal.

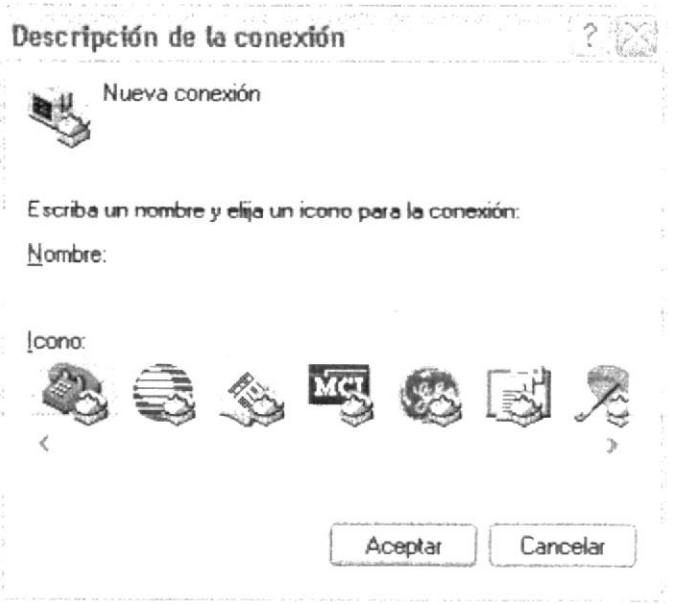


Figura 6-33: Pantalla de Descripción de la conexión de la HyperTerminal

4. En la ventana de **"Descripción de la conexión"** de la HyperTerminal le pide un nombre y un icono para la conexión.
- El nombre puede ser cualquiera, en este caso se llamará COMPUHELP.
- Cada icono es un tipo de conexión diferente, para este caso debe utilizar el primero el que viene marcado por default.
- Si se llena los datos que pide la ventana de "Descripción de conexión" y de clic en aceptar, automáticamente aparecerá la venta de "Conectar a"

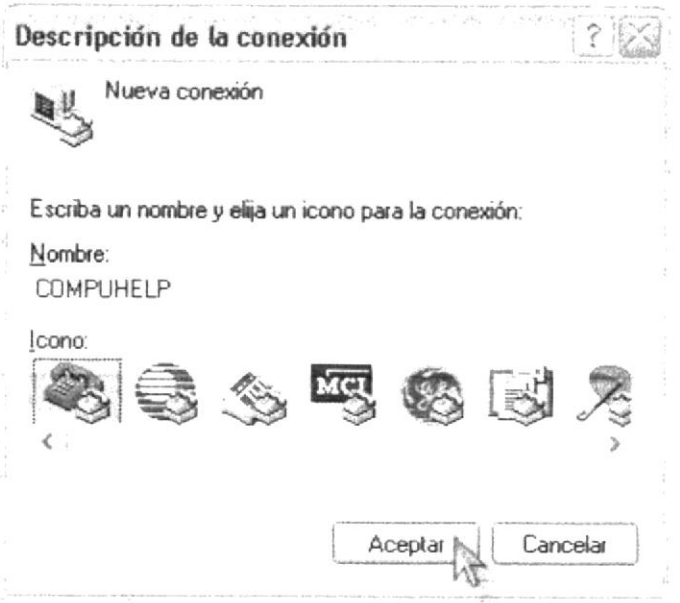


Figura 6-34: Pantalla Descripción de la conexión

5. En la ventana de **"Conectar a"** aparte de la opción **"Conectar usando"** las demás vendrán deshabilitadas, y en la opción habilitada escoger por medio de que puerto del computador y conectarse al router, por lo general es el puerto COM1, y viene por default. Desplegando la caja de texto se podrá ver los diferentes puertos disponibles del PC.

Figura 6-35: Seleccionar conexión

Figura 6-36: Pantalla Conectar a

- Si cancela la ventana de **"Conectar a"**, automáticamente se cerrará y quedará activa la ventana de **"Nueva Conexión – HyperTerminal"**, y se procederá a cerrarlo según lo explicado antes.
- Si acepta, aparecerá una ventana de **"Propiedades del COM1"**, estas son la propiedades del puerto que se escoge para conectarse con el Router.

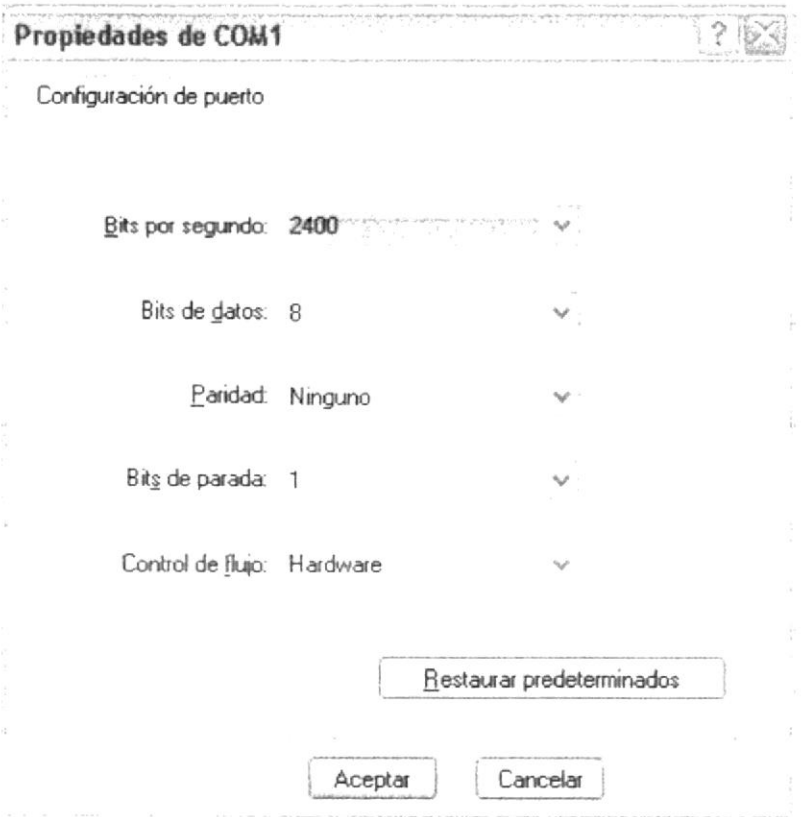


Figura 6-37: Pantalla Propiedades de COM1

6. En la ventana de **"Propiedades de COM1"**, debe configurar según las especificaciones dadas a continuación.

- 9600 bps
- 8 bits de datos
- Ninguno (paridad)
- 1 (Bit de parada)
- Ninguno (Control de flujo)

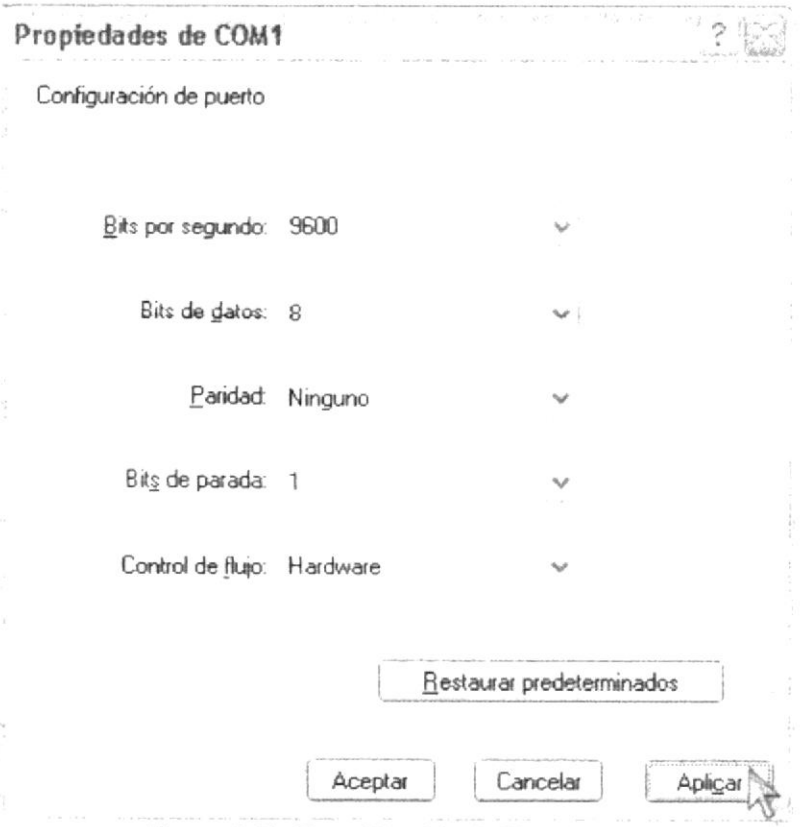


Figura 6-38: Especificación de Bits de datos

a. La pantalla de **"Propiedades de COM1"** proporciona 3 diferentes opciones: Restaurar Predeterminados, Aceptar, Cancelar y Aplicar. Cada una tiene una función diferente. Si se da clic izquierdo en el botón **Restaurar Predeterminados,** las propiedades del COM1 regresarán a las que estaban cuando recién se abrió la ventana.
b. La segunda opción es **"Aplicar"**, esta opción establecerá las opciones que se están configurando, pero aún no los hará surtir efecto.
c. La otra opción es la ventana de **"Propiedades de COM1"** es la de **"Aceptar"**, esta opción surtirá efecto las opciones configuradas, inclusive se podrá obviar el paso de primero **"Aplicar"** y luego **"Aceptar"**. Una vez dado clic en **"Aceptar"** conectarse inmediatamente al **Router.**
d. La tercera y ultima opción es la de **"Cancelar"**, si le da clic aquí automáticamente la ventana se cerrará y se activará la ventana de **"Nueva Conexión - HyperTerminal"**, luego se la cierra según lo requerido y ya aprendido.

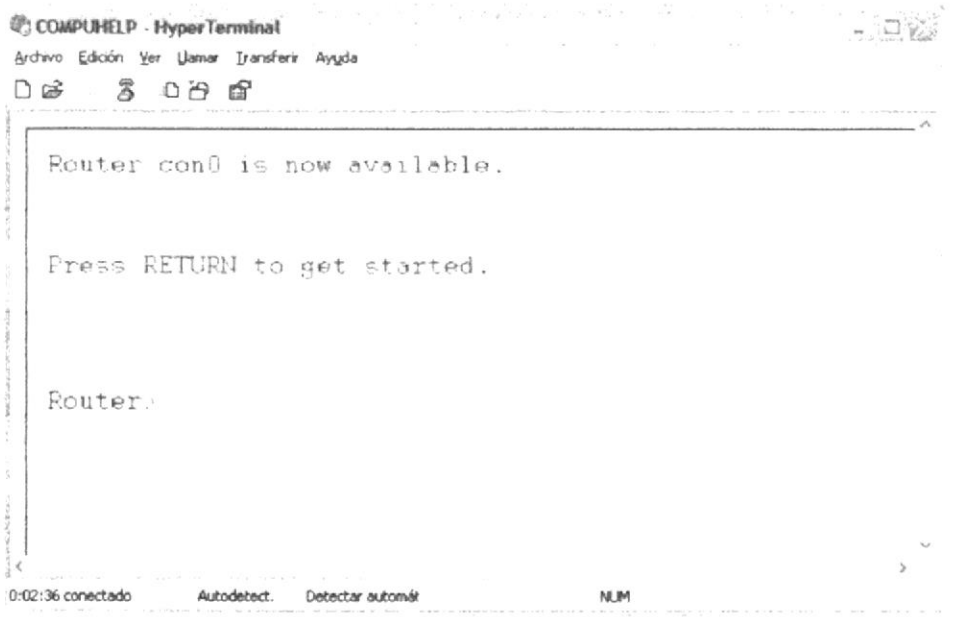


Figura 6-39: Pantalla Inicio de Interfaz con el Router

6.6.13 COMANDOS BÁSICOS PARA VER EL ESTADO DE UN ROUTER

Comandos	Descripción
show run	Presenta la configuración actual realizada.
show interface	Muestra el estado de las Interfaces Seriales y Ethernet.
show clock	Presenta la hora fijada en el Router.
show hosts	Presenta los nombres del host y sus direcciones.
show users	Presenta los usuarios conectados al router.
show history	Presenta el historial de los comandos ingresados.
show protocols	Presenta el estado global de las interfaces del router.
show ip route	Verifica la ruta estática en la tabla de enrutamiento.
show ip protocols	Verifica que un protocolo de enrutamiento esté bien configurado y que esté recibiendo actualizaciones.
show ip route	Verifica que las rutas recibidas por los routers vecinos se encuentren en la tabla de enrutamiento.
show Vlan	Verifica la configuración de la Vlan.

Tabla 6-1: Comando para ver el estado de un router

6.7 CONFIGURACIÓN DE ROUTERS COMPUHELP

6.7.1 MATRIZ – GUAYAQUIL

6.7.1.1 ASIGNACIÓN DE NOMBRE AL ROUTER PARA IDENTIFICARLO.

Router>enable

Ingresa al modo EXEC privilegiado

```
Press Enter to Start


Router>
Router>ena

Router#
```

Router#configure terminal

Ingresa al modo de configuración global

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#
```

Router(config)#hostname Matriz_Guayaquil

Sirve para asignarle un nombre al router (Matriz_Guayaquil)

```
Router(config)#hostname Matriz_Guayaquil

Matriz_Guayaquil(config)#
```

Matriz_Guayaquil(config)#

6.7.1.2 LEVANTANDO LAS INTERFACES SERIALES

Matriz_Guayaquil(config)#interface serial 0/0

Permite ingresar a la interfaz que se va a configurar

```
Matriz_Guayaquil(config)#interface serial 0/0
Matriz_Guayaquil(config-if)#
```

Matriz_Guayaquil(config-if)#ip address 192.168.10.1 255.255.255.252

Agregar IP – IP asignada – Máscara de Red

Se asigna una dirección ip con su respectiva máscara de red

```
Matriz_Guayaquil(config-if)#ip address 192.168.10.1 255.255.255.252
Matriz_Guayaquil(config-if)#
```

Matriz_Guayaquil(config-if)#clock rate 56000 → Sincronización

Asignación de Reloj

Ingresa el valor para el sincronizador del reloj, solo se debe aplicar cuando el router esta definido como DCE.

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

Matriz_Guayaquil(config-if)#no shutdown → Comando que levanta las interfaces

Levanta la interfaz para que pueda funcionar

```
Matriz_Guayaquil(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up
Matriz_Guayaquil(config-if)#
```

Cambia el estado y muestra que la Interface esta levantada

Matriz_Guayaquil(config-if)# exit

Sale de la configuración de la interfaz serial 0/0

```
Matriz_Guayaquil(config-if)#exit
Matriz_Guayaquil(config)#
```

Matriz_Guayaquil(config)#interface serial 0/1

Permite ingresar a la interfaz que se va a configurar

```
Matriz_Guayaquil(config)#interface serial 0/1
Matriz_Guayaquil(config-if)#
```

Matriz_Guayaquil(config-if)#ip address 192.168.10.18 255.255.255.252

Agregar IP – IP asignada – Máscara de Red

Asigna una dirección ip con su respectiva máscara de red

```
Matriz_Guayaquil(config-if)#ip address 192.168.10.18 255.255.255.252
Matriz_Guayaquil(config-if)#
```

Matriz_Guayaquil(config-if)#no shutdown → Comando que levanta las interfaces

Levanta la interfaz para que pueda funcionar

```
Matriz_Guayaquil(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/1, changed state to up
Matriz_Guayaquil(config-if)#
```

Cambia el estado y muestra que la Interface esta levantada

Matriz_Guayaquil(config-if)# exit

Sale de la configuración de la interfaz serial 0/1

```
Matriz_Guayaquil(config-if)#exit
Matriz_Guayaquil(config)#
```

Matriz_Guayaquil(config)#interface serial 0/2

Permite ingresar a la interfaz que se va a configurar

```
Matriz_Guayaquil(config)#interface serial 0/2
Matriz_Guayaquil(config-if)#
```

Matriz_Guayaquil(config-if)#ip address 192.168.10.21 255.255.255.252

Agregar IP – IP asignada – Máscara de Red

Asigna una dirección ip con su respectiva máscara de red

```
Matriz_Guayaquil(config-if)#ip address 192.168.10.21 255.255.255.252
Matriz_Guayaquil(config-if)#
```

Matriz_Guayaquil(config-if)#no shutdown

Levanta la interfaz para que pueda funcionar

```
Matriz_Guayaquil(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/2, changed state to up
Matriz_Guayaquil(config-if)#
```

Cambia el estado y muestra que la Interface esta levantada

Matriz_Guayaquil(config-if)# exit

Sale de la configuración de la interfaz serial 0/2

```
Matriz_Guayaquil(config-if)#exit
Matriz_Guayaquil(config)#
```

6.7.1.3 LEVANTANDO LAS INTERFACES ETHERNET

Matriz_Guayaquil(config)#interface fastethernet 0/0

Ingresa a la interfaz que se va a configurar

Matriz_Guayaquil(config-if)#ip address 192.168.11.33 255.255.255.248

Asigna una dirección ip con su respectiva máscara de red

Matriz_Guayaquil(config-if)#no shutdown

Levanta la interfaz para que pueda funcionar

```
Matriz_Guayaquil(config)#interface fastethernet 0/0
Matriz_Guayaquil(config-if)#ip address 192.168.11.33 255.255.255.248
Matriz_Guayaquil(config-if)#no shutdown
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Matriz_Guayaquil(config-if)#
```

Matriz_Guayaquil(config-if)#exit

Sale de la configuración de la interfaz ethernet

6.7.1.4 ASIGNAR SEGURIDAD EN MODO CONSOLA

Matriz_Guayaquil(config-if)#exit

Sale de la configuración de la interfaz ethernet

Matriz_Guayaquil(config)#line console 0 → Configuración de consola

Ingresa a configurar la consola

Matriz_Guayaquil(config-line)#password cisco→ Contraseña asignada

Asigna una contraseña a la consola

Matriz_Guayaquil(config-line)#login → Para que le pida la contraseña

Petición de contraseña

Matriz_Guayaquil(config-line)#exit

Sale de la configuración de la consola

Matriz_Guayaquil(config)#enable password cisco → Encriptar contraseña

Habilita el password asignado

Matriz_Guayaquil(config)#

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

6.7.1.5 ASIGNAR SEGURIDAD EN MODO PRIVILEGIADO

Matriz_Guayaquil(config)#line vty 0 4 → Control de acceso remoto Telnet

Ingresa a configurar la Terminal virtual

Matriz_Guayaquil(config-line)#password cisco → Contraseña asignada

Asigna una contraseña a la Terminal virtual

Matriz_Guayaquil(config-line)#login → Para que le pida la contraseña

Petición de contraseña

Matriz_Guayaquil(config-line)#exit

Sale de la configuración de la Terminal virtual

Matriz_Guayaquil(config)#enable secret cisco → Encriptar contraseña

Habilita el password asignado

Matriz_Guayaquil(config)#

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

6.7.1.6 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO RIP VERSIÓN 2

Matriz_Guayaquil(config)#

Matriz_Guayaquil(config)#router rip → Protocolo de enrutamiento

Este comando le permite habilitar el protocolo de enrutamiento rip.

```
Matriz_Guayaquil(config)#router rip
Matriz_Guayaquil(config-router)#
```

Matriz_Guayaquil(config-router)#version 2 → Se especifica la versión de rip

Le especifica la versión del protocolo de enrutamiento rip.

```
Matriz_Guayaquil(config-router)#version 2
Matriz_Guayaquil(config-router)#
```

Matriz_Guayaquil(config-router)#network 192.168.10.0 → Segmento de red
Matriz_Guayaquil(config-router)#network 192.168.11.0 → Segmento de red
Matriz_Guayaquil(config-router)#network 192.168.12.0 → Segmento de red
Matriz_Guayaquil(config-router)#network 192.168.13.0 → Segmento de red
Matriz_Guayaquil(config-router)#network 192.168.14.0 → Segmento de red
Matriz_Guayaquil(config-router)#network 192.168.15.0 → Segmento de red
Matriz_Guayaquil(config-router)#network 192.168.16.0 → Segmento de red
Matriz_Guayaquil(config-router)#network 192.168.17.0 → Segmento de red

Mediante el comando network se especifica, las redes que se van a enrutar mediante este protocolo. (Redes conectadas)

```
Matriz_Guayaquil(config-router)#network 192.168.10.0
Matriz_Guayaquil(config-router)#network 192.168.11.0
Matriz_Guayaquil(config-router)#network 192.168.12.0
Matriz_Guayaquil(config-router)#network 192.168.13.0
Matriz_Guayaquil(config-router)#network 192.168.14.0
Matriz_Guayaquil(config-router)#network 192.168.15.0
Matriz_Guayaquil(config-router)#network 192.168.16.0
Matriz_Guayaquil(config-router)#network 192.168.17.0

Matriz_Guayaquil(config-router)#
```

Matriz_Guayaquil(config-router)#exit

Sale de la configuración del router

6.7.1.7 CONFIGURACIÓN PROTOCOLO DE ENRUTAMIENTO OSPF

Matriz_Guayaquil(config)#

Modo de configuración global

Matriz_Guayaquil(config)#router ospf 1 → Protocolo de enrutamiento

Este comando habilita el protocolo de enrutamiento ospf.

```
Matriz_Guayaquil(config-router)#exit
Matriz_Guayaquil(config)#router ospf 1

Matriz_Guayaquil(config-router)#
```

Matriz_Guayaquil(config- router)# network 192.168.10.0 0.0.0.3 area 0 → Ruta

Matriz_Guayaquil(config- router)# network 192.168.10.17 0.0.0.3 area 0

Matriz_Guayaquil(config- router)# network 192.168.10.21 0.0.0.3 area 0

Especifica la ruta por donde van a llegar los paquetes.

```
Matriz_Guayaquil(config-router)#network 192.168.10.0 0.0.0.3 area 0
Matriz_Guayaquil(config-router)#network 192.168.10.17 0.0.0.3 area 0
Matriz_Guayaquil(config-router)#network 192.168.10.21 0.0.0.3 area 0

Matriz_Guayaquil(config-router)#
```

Matriz_Guayaquil(config- router)# redistribute rip → Redistribuye para rip

Este comando permite redistribuir paquetes rip, por toda la red.

```
Matriz_Guayaquil(config-router)#redistribute rip

Matriz_Guayaquil(config-router)#
```

Matriz_Guayaquil(config- router)# → **Usar las teclas (Ctrl. + Z)**

Regresa al modo privilegiado.

```
Matriz_Guayaquil(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Matriz_Guayaquil#
```

Matriz_Guayaquil# wr

Este comando permite guardar las configuraciones que haya realizado.

```
Matriz_Guayaquil#wr
Building configuration...
[OK]

Matriz_Guayaquil#
```

6.7.1.8 ENRUTAMIENTO DE VLAN 10

Matriz(config-subif)# interface fastethernet 0.1

Esta línea le indica como declarar las sub-interfaces del router.

Matriz(config-subif)# ip address 192.168.11.121 255.255.255.248

Esta línea le permite asignar una dirección Ip a la sub-interfaces del router con la máscara de subred.

Matriz(config-subif)# encapsulation dot1q 10

En esta línea mostramos el encapsulamiento de la vlan.

Matriz(config- subif)# no shutdown

En esta línea nos permite levantar la sub-interfaces del router.


```
Matriz_Guayaquil(config)#interface fastethernet 0.1
Matriz_Guayaquil(config-subif)#ip address 192.168.11.121 255.255.255.248
Matriz_Guayaquil(config-subif)#encapsulation dot1q 10
Matriz_Guayaquil(config-subif)#no shutdown
Matriz_Guayaquil(config-subif)#
```

6.7.1.9 ENRUTAMIENTO DE VLAN 20

Matriz(config-subif)# interface fastethernet 0.2

Esta línea le indica como declarar las sub-interfaces del router.

Matriz(config-subif)# ip address 192.168.11.129 255.255.255.248

Esta línea nos permite asignar una dirección Ip a la sub-interfaces del router con la máscara de subred.

Matriz(config-subif)# encapsulation dot1q 20

En esta línea mostramos el encapsulamiento de la vlan.

Matriz(config- subif)# no shutdown

En esta línea nos permite levantar la sub-interfaces del router.

```
Matriz_Guayaquil(config)#interface fastethernet 0.2
Matriz_Guayaquil(config-subif)#ip address 192.168.11.129 255.255.255.248
Matriz_Guayaquil(config-subif)#no shutdown
Matriz_Guayaquil(config-subif)#
```

6.7.1.10 ENRUTAMIENTO DE VLAN 30

Matriz(config-subif)# interface fastethernet 0.3

Esta línea le indica como declarar las sub-interfaces del router.

Matriz(config-subif)# ip address 192.168.11.138 255.255.255.248

Esta línea nos permite asignar una dirección Ip a la sub-interfaces del router con la máscara de subred.

Matriz(config-subif)# encapsulation dot1q 30

En esta línea mostramos el encapsulamiento de la vlan.

Matriz(config- subif)# no shutdown

En esta línea nos permite levantar la sub-interfaces del router.

```
Matriz_Guayaquil(config)#interface fastethernet 0.3
Matriz_Guayaquil(config-subif)#ip address 192.168.11.138 255.255.255.248
Matriz_Guayaquil(config-subif)#no shutdown
Matriz_Guayaquil(config-subif)#
```

6.7.1.11 SHOW RUN ROUTER - MATRIZ

```
Matriz#show run
Building configuration...

!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Matriz
!
!
!
ip subnet-zero
!
!
!
!
interface Serial0/0
 ip address 192.168.10.1 255.255.255.252
 no ip directed-broadcast
 clock rate 56000
 bandwidth 1544
!
interface Serial0/1
 ip address 192.168.10.18 255.255.255.252
 no ip directed-broadcast
 bandwidth 1544
!
interface Serial0/2
 ip address 192.168.10.21 255.255.255.252
 no ip directed-broadcast
 bandwidth 1544
!
interface Serial0/3
 ip address 192.168.10.30 255.255.255.252
 no ip directed-broadcast
 bandwidth 1544
!
interface Ethernet1/0
 no ip address
 no ip directed-broadcast
 bandwidth 10000
 shutdown
!
!
router rip
```

Mascara de red

Ip asignada para el serial 0/0

Ip asignada para el serial 0/1

Ip asignada para el serial 0/2

Ip asignada para el serial 0/3

```
 version 2
 redistribute OSPF 1
 network 192.168.10.0
 network 192.168.11.0
 network 192.168.12.0
 network 192.168.13.0
 network 192.168.14.0
 network 192.168.15.0
 network 192.168.16.0
 network 192.168.17.0
!
router ospf 1
 redistribute RIP
 network 192.168.10.0 0.0.0.3 area 0
 network 192.168.10.16 0.0.0.3 area 0
 network 192.168.10.20 0.0.0.3 area 0
!
ip classless
no ip http server
!
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

Matriz#
```

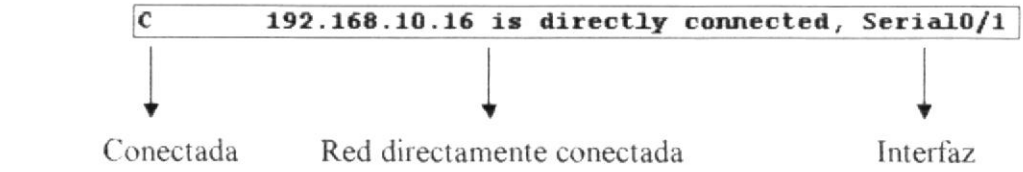
Redistribución OSPF 1
En el Protocolo Rip versión 2

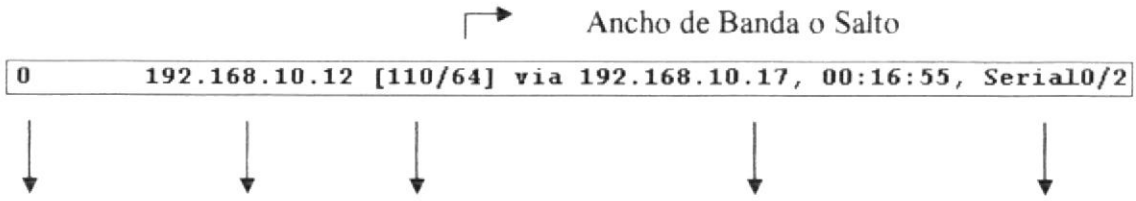
6.7.1.12 SHOW IP ROUTER - MATRIZ

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

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 7 subnets
C       192.168.10.0 is directly connected, Serial0/0
C       192.168.10.16 is directly connected, Serial0/1
C       192.168.10.20 is directly connected, Serial0/2
R       192.168.10.4 [120/1] via 192.168.10.2, 00:04:15, Serial0/0
R       192.168.10.8 [120/2] via 192.168.10.2, 00:04:22, Serial0/0
O       192.168.10.12 [110/64] via 192.168.10.17, 00:16:55, Serial0/2
O       192.168.10.24 [110/64] via 192.168.10.25, 00:14:15, Serial0/2

Matriz#
```

Significado de Códigos del Router:

- C → Conectado.
- S → Estático.
- I → Protocolo IGRP.
- R → Protocolo RIP.
- M → Móvil
- B → Protocolo BGP.
- D → Protocolo EIGRP.
- EX → Protocolo EIGRP externo.
- O → Protocolo OSPF.
- IA → El número de las rutas recibidas de otras áreas del OSPF.
- E1 → Rutas recibidas de otras áreas del OSPF tipo externo 1.
- E2 → Rutas recibidas de otras áreas del OSPF tipo externo 2.
- I → Son las rutas recibidas de los anuncios del protocolo del IS-IS.
- U → Usuario estático en el router.





6.7.1.13 SHOW INTERFACES - MATRIZ

```
Matriz#show interfaces
Serial0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.10.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

Serial0/1 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.10.18/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/2 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.10.21/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
```

```
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/3 is down, line protocol is down
  Hardware is HD64570
  Internet address is 192.168.10.30/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet1/0 is administratively down, line protocol is down
  Hardware is Lance, address is 000C.3782.8690 (bia 000C.3782.8690)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never

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

Matriz#
```

6.7.1.14 CREACIÓN DE VLAN'S - MATRIZ

Switch#vlan database

En esta línea mostramos como crear una vlan.

switch(vlan)# vlan10 name administración

switch(vlan)# vlan20 name soporte

switch(vlan)# vlan30 name servidores

En esta línea mostramos como crear una vlan con su respectivo nombre.

```
Switch#vlan database
Switch(vlan)#vlan 10 name administracion
VLAN 10 added:
    Name:administracion
Switch(vlan)#vlan 20 name soporte
VLAN 20 added:
    Name:soporte
Switch(vlan)#vlan 30 name servidores
VLAN 30 added:
    Name:servidores
Switch(vlan)#
```

← Creación de vlan

Asignación de nombre

switch # configure terminal

Nos ubicamos en el modo global del Switch.

switch (config)# interface fastethernet 0/1

En esta línea ingresamos al interfaz del switch.

switch (config)#switchport mode trunk

En esta línea Definimos un puerto en modo truncado

switch (config)#switchport access vlan 10

En esta línea asignamos a la vlan una o más interfaces.

switch (config)# interface fastethernet 0/2

En esta linea ingresamos al interfaz del switch.

switch (config)#switchport access vlan 10

En esta linea asignamos a la vlan una o más interfaces.

switch (config)# interface fastethernet 0/3

En esta linea ingresamos al interfaz del switch.

switch (config)#switchport access vlan 20

En esta linea asignamos a la vlan una o más interfaces.

```
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fasethernet 0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fasethernet 0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
```

6.7.1.15 SHOW VLAN

VLAN.- Es el número de la vlan.

Name.- Es el nombre asignado a la vlan.

Status.- Es el estado en que se encuentra la vlan.

Ports.- Son los puertos asignados a las vlans.

```
Switch(config-if)#exit
Switch(config)#exit
Switch#show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Switch#
```

6.7.1.16 SHOW INTERFACES

```
Switch#show interfaces

Vlan 1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 000C.5705.2213 (bia 000C.5705.2213)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000C.5705.2214 (bia 000C.5705.2214)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo

  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/2 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000C.5401.8140 (bia 000C.5401.8140)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/3 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000C.9718.6536 (bia 000C.9718.6536)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/4 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.8611.6236 (bia 000C.8611.6236)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set

  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/5 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.3496.9250 (bia 000C.3496.9250)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
```

```
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/6 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.5567.2318 (bia 000C.5567.2318)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/7 is down, line protocol is down

  Hardware is Fast Ethernet, address is 000C.2649.6848 (bia 000C.2649.6848)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/8 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.2864.6415 (bia 000C.2864.6415)
```

```
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/9 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.4650.5212 (bia 000C.4650.5212)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/10 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.5908.5115 (bia 000C.5908.5115)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
```

```
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.5299.6266 (bia 000C.5299.6266)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/12 is down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.5000.3333 (bia 000C.5000.3333)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out

Switch#
```

6.7.1.17 HACIENDO PING

```
Matriz#ping 192.168.10.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.26

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.26, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.25

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.25, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#
```

```
Matriz#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#
Matriz#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Matriz#ping 192.168.10.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Manta#ping 192.168.10.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Manta#ping 192.168.10.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

6.7.2 SUCURSAL – SALINAS

6.7.2.1 ASIGNACIÓN DE NOMBRE AL ROUTER PARA IDENTIFICARLO

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname Sucursal_Salinas

Sirve para asignarle un nombre al router (Sucursal_Salinas)

Sucursal_Salinas(config)#

6.7.2.2 LEVANTANDO LAS INTERFACES SERIAL

Sucursal_Salinas(config)#interface serial 1

Ingresar a la interfaz que se va a configurar

Sucursal_Salinas(config-if)#ip address 192.168.10.2 255.255.255.252

Asignar una dirección ip con su respectiva máscara de red

Sucursal_Salinas(config-if)#no shutdown

Levantar la interfaz para que pueda funcionar

Sucursal_Salinas(config-if)# exit

Salir de la configuración de la interfaz serial 1

Sucursal_Salinas(config)#interface serial 0

Ingresar a la interfaz que se va a configurar

Sucursal_Salinas(config-if)#ip address 192.168.10.5 255.255.255.252

Asignar una dirección ip con su respectiva máscara de red

Sucursal_Salinas(config-if)#clock rate 56000

Asignar el valor para el sincronizador del reloj

Sucursal_Salinas(config-if)#no shutdown

Levantar la interfaz para que pueda funcionar

Sucursal_Salinas(config-if)#

6.7.2.3 LEVANTANDO LAS INTERFACES ETHERNET

Sucursal_Salinas(config-if)#exit

Salir de la configuración de la interfaz serial 0

Sucursal_Salinas(config)#interface ethernet 0

Ingresar a la interfaz que se va a configurar

Sucursal_Salinas(config-if)#ip address 192.168.17.2 255.255.255.248

Asignar una dirección ip con su respectiva máscara de red

Sucursal_Salinas(config-if)#no shutdown

Levantar la interfaz para que pueda funcionar

Sucursal_Salinas(config-if)#

6.7.2.4 ASIGNAR SEGURIDAD EN MODO CONSOLA

Sucursal_Salinas(config-if)#exit

Salir de la configuración de la interfaz ethernet

Sucursal_Salinas(config)#line console 0

Ingresar a configurar la consola

Sucursal_Salinas(config-line)#password cisco → Contraseña asignada

Asignar una contraseña a la consola

Sucursal_Salinas(config-line)#login → Para que pida la contraseña

Petición de contraseña

Sucursal_Salinas(config-line)#exit

Salir de la configuración de la consola

Sucursal_Salinas(config)#enable passwd cisco

Habilitar el password asignado

Sucursal_Salinas(config)#

6.7.2.5 ASIGNAR SEGURIDAD EN MODO PRIVILEGIADO

Sucursal_Salinas(config)#line vty 0 4 → **Control de acceso remoto Telnet**

Ingresar a configurar la Terminal virtual

Sucursal_Salinas(config-line)#password cisco → **Contraseña asignada**

Asignar una contraseña a la Terminal virtual

Sucursal_Salinas(config-line)#login → **Para que pida la contraseña**

Petición de contraseña

Sucursal_Salinas(config-line)#exit

Salir de la configuración de la Terminal virtual

Sucursal_Salinas(config)#enable secret cisco → **Encriptar contraseña**

Habilitar el password asignado

Sucursal_Salinas(config)#

6.7.2.6 CONFIGURACIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO

RIP V2

Sucursal_Salinas(config)#

Sucursal_Salinas(config)#router rip → **Protocolo de enrutamiento**

Sucursal_Salinas(config-router)#version 2 → **Versión de rip**

Sucursal_Salinas(config-router)#network 192.168.10.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#network 192.168.11.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#network 192.168.12.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#network 192.168.13.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#network 192.168.14.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#network 192.168.15.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#network 192.168.16.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#network 192.168.17.0 → **Redes conectadas**

Sucursal_Salinas(config-router)#exit

6.7.2.7 ENRUTAMIENTO DE VLAN 40

Sucursal_Salinas(config-subif)# interface fastethernet 0.1

Esta línea le indica como declarar las sub-interfaces del router.

Sucursal_Salinas(config-subif)# ip address 192.168.17.121 255.255.255.248

Esta línea nos permite asignar una dirección Ip a la sub-interfaces del router con la máscara de subred.

Sucursal_Salinas(config-subif)# encapsulation dot1q 40

En esta línea mostramos el encapsulamiento de la vlan.

Sucursal_Salinas(config- subif)# no shutdown

En esta línea nos permite levantar la sub-interfaces del router.

6.7.2.8 ENRUTAMIENTO DE VLAN 50

Sucursal_Salinas(config-subif)# interface fastethernet 0.2

Esta línea le indica como declarar las sub-interfaces del router.

Sucursal_Salinas(config-subif)# ip address 192.168.17.129 255.255.255.248

Esta línea nos permite asignar una dirección Ip a la sub-interfaces del router con la máscara de subred.

Sucursal_Salinas(config-subif)# encapsulation dot1q 50

En esta línea mostramos el encapsulamiento de la vlan.

Sucursal_Salinas(config- subif)# no shutdown

En esta línea nos permite levantar la sub-interfaces del router.

6.7.2.9 CREACIÓN DE VLAN'S - SALINAS

Switch#vlan database

En esta linea mostramos como crear una vlan.

switch(vlan)# vlan 40 name soporte

switch(vlan)# vlan 50 name servidores

En esta linea mostramos como crear una vlan con su respectivo nombre.

```
Switch#vlan database
Switch(vlan)#vlan 40 name soporte
VLAN 40 added:
    Name:soporte
Switch(vlan)#vlan 50 name servidores
VLAN 50 added:
    Name:servidores
Switch(vlan)#
```

← Creación de vlan

Asignación de nombre

switch # configure terminal

Nos ubicamos en el modo global del Switch.

switch (config)# interface fastethernet 0/1

En esta linea ingresamos al interfaz del switch.

switch (config)#switchport mode trunk

En esta línea Definimos un puerto en modo truncado

switch (config)#switchport access vlan 40

En esta linea asignamos a la vlan una o más interfaces.

switch (config)# interface fastethernet 0/2

En esta línea ingresamos al interfaz del switch.

switch (config)#switchport access vlan 40

En esta línea asignamos a la vlan una o más interfaces.

switch (config)# interface fastethernet 0/3

En esta línea ingresamos al interfaz del switch.

switch (config)#switchport access vlan 50

En esta línea asignamos a la vlan una o más interfaces.

```
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 40
Switch(config-if)#interface fasethernet 0/2
Switch(config-if)#switchport access vlan 40
Switch(config-if)#interface fasethernet 0/3
Switch(config-if)#switchport access vlan 50
Switch(config-if)#
```

6.7.2.10 SHOW VLAN

VLAN.- Es el número de la vlan.

Name.- Es el nombre asignado a la vlan.

Status.- Es el estado en que se encuentra la vlan.

Ports.- Son los puertos asignados a las vlans.

```
Switch(config-if)#exit
Switch(config)#exit
Switch#show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Switch#
```

6.7.2.11 HACIENDO PING

```
Salinas#ping 192.168.10.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Salinas#ping 192.168.10.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.14, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5), round-trip min/avg/max = 1/2/4 ms
Salinas#ping 192.168.10.15

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.15, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5), round-trip min/avg/max = 1/2/4 ms
Salinas#ping 192.168.10.16

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.16, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5), round-trip min/avg/max = 1/2/4 ms
Salinas#ping 192.168.10.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Salinas#ping 192.168.10.
```

6.7.3 SUCURSAL – QUITO

6.7.3.1 ASIGNACIÓN DE NOMBRE AL ROUTER PARA IDENTIFICARLO

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname Sucursal_Quito

Sirve para asignarle un nombre al router (Sucursal_Quito)

Sucursal_Quito(config)#

6.7.3.2 LEVANTANDO LAS INTERFACES SERIAL

Sucursal_Quito(config)#interface serial 0

Ingresar a la interfaz que se va a configurar

Sucursal_Quito(config-if)#ip address 192.168.10.1 255.255.255.252

Asignar una dirección ip con su respectiva máscara de red

Sucursal_Quito(config-if)#no shutdown

Levantar la interfaz para que pueda funcionar

Sucursal_Quito(config-if)#clock rate 56000

Asignar el valor para el sincronizador del reloj

Sucursal_Quito(config-if)# exit

Salir de la configuración de la interfaz serial 0

Sucursal_Quito(config)#interface serial 1

Ingresar a la interfaz que se va a configurar

Sucursal_Quito(config-if)#ip address 192.168.10.18 255.255.255.252

Asignar una dirección ip con su respectiva máscara de red

Sucursal_Quito(config-if)#no shutdown

Levantar la interfaz para que pueda funcionar

Sucursal_Quito (config-if)# exit

Salir de la configuración de la interfaz serial 1

Sucursal_Quito(config)#interface serial 2

Ingresar a la interfaz que se va a configurar

Sucursal_Quito(config-if)#ip address 192.168.10.21 255.255.255.252

Asignar una dirección ip con su respectiva máscara de red

Sucursal_Quito(config-if)#no shutdown

Levantar la interfaz para que pueda funcionar

Sucursal_Quito(config-if)#

6.7.3.3 LEVANTANDO LAS INTERFACES ETHERNET

Sucursal_Quito(config-if)#exit

Salir de la configuración de la interfaz serial 2

Sucursal_Quito(config)#interface ethernet 0

Ingresar a la interfaz que se va a configurar

Sucursal_Quito(config-if)#ip address 192.168.10.9 255.255.255.248

Asignar una dirección ip con su respectiva máscara de red

Sucursal_Quito(config-if)#no shutdown

Levantar la interfaz para que pueda funcionar

Sucursal_Quito(config-if)#

6.7.3.4 ASIGNAR SEGURIDAD EN MODO CONSOLA

Sucursal_Quito(config-if)#exit

Salir de la configuración de la interfaz ethernet

Sucursal_Quito(config)#line console 0

Ingresar a configurar la consola

Sucursal_Quito(config-line)#password cisco

Asignar una contraseña a la consola

Sucursal_Quito(config-line)#login

Petición de contraseña

Sucursal_Quito(config-line)#exit

Salir de la configuración de la consola

Sucursal_Quito(config)#enable password cisco

Habilitar el password asignado

Sucursal_Quito(config)#

6.7.3.5 ASIGNAR SEGURIDAD EN MODO PRIVILEGIADO

Sucursal_Quito(config)#line vty 0 4

Ingresar a configurar la Terminal virtual

Sucursal_Quito(config-line)#password cisco

Asignar una contraseña a la Terminal virtual

Sucursal_Quito(config-line)#login

Petición de contraseña

Sucursal_Quito(config-line)#exit

Salir de la configuración de la Terminal virtual

Sucursal_Quito(config)#enable secret cisco

Habilitar el password asignado

Sucursal_Quito(config)#

6.7.3.6 CONFIGURACIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO

RIP V2

Sucursal_Quito(config)#

Sucursal_Quito(config)#router rip → Protocolo de enrutamiento

Sucursal_Quito(config-router)#version 2 → Versión de rip

Sucursal_Quito(config-router)#network 192.168.10.0 → Red Conectada

Sucursal_Quito(config-router)#network 192.168.11.0 → Red Conectada

Sucursal_Quito(config-router)#network 192.168.12.0 → Red Conectada

Sucursal_Quito(config-router)#network 192.168.13.0 → Red Conectada

Sucursal_Quito(config-router)#network 192.168.14.0 → Red Conectada

Sucursal_Quito(config-router)#network 192.168.15.0 → Red Conectada

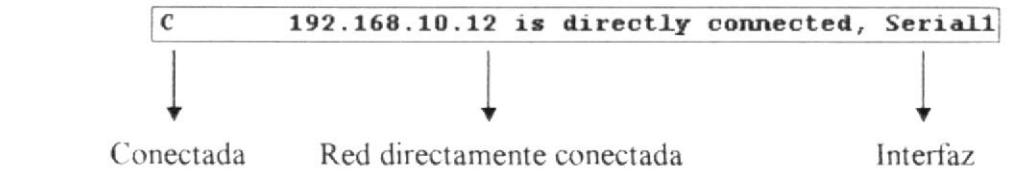
Sucursal_Quito(config-router)#network 192.168.16.0 → Red Conectada

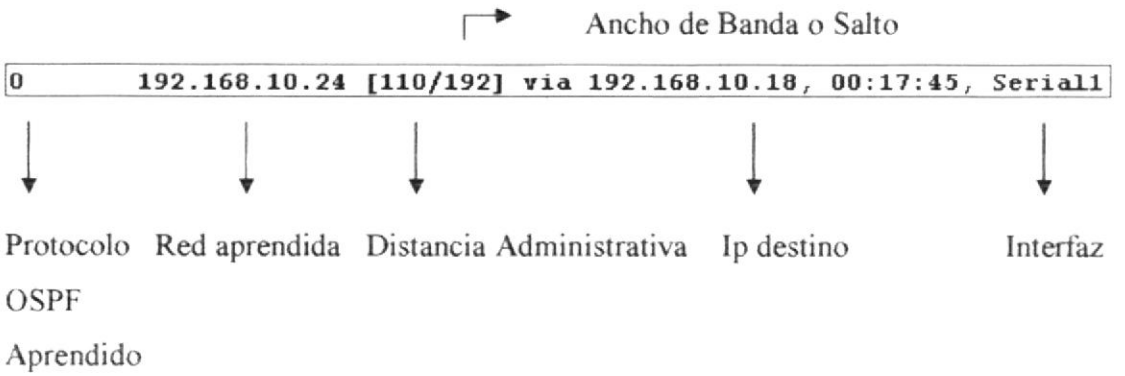
Sucursal_Quito(config-router)#network 192.168.17.0 → Red Conectada

Sucursal_Quito(config-router)#exit

6.7.3.7 SHOW IP ROUTE

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

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 5 subnets
C       192.168.10.12 is directly connected, Serial1
C       192.168.10.16 is directly connected, Serial0
O       192.168.10.0 [110/64] via 192.168.10.18, 00:18:25, Serial1
O       192.168.10.20 [110/64] via 192.168.10.18, 00:18:25, Serial1
O       192.168.10.24 [110/192] via 192.168.10.18, 00:17:45, Serial1

Quito#
```





6.7.3.8 ENRUTAMIENTO DE VLAN 60

Sucursal_Salinas(config-subif)# interface fastethernet 0.1

Esta línea le indica como declarar las sub-interfaces del router.

Sucursal_Salinas(config-subif)# ip address 192.168.14.121 255.255.255.248

Esta línea le permite asignar una dirección Ip a la sub-interfaces del router con la máscara de subred.

Sucursal_Salinas(config-subif)# encapsulation dot1q 60

Esta línea le permite el encapsulamiento de la vlan.

Sucursal_Salinas(config- subif)# no shutdown

Esta línea le permite levantar la sub-interfaces del router.

6.7.3.9 ENRUTAMIENTO DE VLAN 70

Sucursal_Salinas(config-subif)# interface fastethernet 0.2

Esta línea le indica como declarar las sub-interfaces del router.

Sucursal_Salinas(config-subif)# ip address 192.168.14.129 255.255.255.248

Esta línea le permite asignar una dirección Ip a la sub-interfaces del router con la máscara de subred.

Sucursal_Salinas(config-subif)# encapsulation dot1q 70

Esta línea le permite el encapsulamiento de la vlan.

Sucursal_Salinas(config- subif)# no shutdown

En esta línea le permite levantar la sub-interfaces del router.

6.7.3.10 CREACIÓN DE VLAN'S - QUITO

Switch#vlan database

Comando que le permite crear vlan's.

switch(vlan)# vlan 60 name soporte

switch(vlan)# vlan 70 name servidores

Esta línea le muestra como asignarle un nombre a la vlan.

```
Switch#vlan database                    ← Creación de vlan
Switch(vlan)#vlan 60 name soporte       ←┐
VLAN 60 added:                           Asignación de nombre
    Name:soporte
Switch(vlan)#vlan 70 name servidores
VLAN 70 added:
    Name:servidores
Switch(vlan)#
```


switch # configure terminal

Ubíquese en el modo global del Switch.

switch (config)# interface fastethernet 0/1

En esta línea se ingresa al interfaz del switch.

switch (config)#switchport mode trunk

En esta línea se define un puerto en modo truncado

switch (config)#switchport access vlan 50

En esta línea se le asigna a la vlan una o más interfaces.

switch (config)# interface fastethernet 0/2

En esta línea ingrese al interfaz del switch.

switch (config)#switchport access vlan 50

En esta línea asígnele a la vlan una o más interfaces.

switch (config)# interface fastethernet 0/3

En esta linea ingrese al interfaz del switch.

switch (config)#switchport access vlan 60

En esta linea asignele a la vlan una o más interfaces.

```
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 60
Switch(config-if)#interface fasethernet 0/2
Switch(config-if)#switchport access vlan 60
Switch(config-if)#interface fasethernet 0/3
Switch(config-if)#switchport access vlan 70
Switch(config-if)#
```

6.7.3.11 SHOW VLAN

VLAN.- Es el número de la vlan.

Name.- Es el nombre asignado a la vlan.

Status.- Es el estado en que se encuentra la vlan.

Ports.- Son los puertos asignados a las vlans.

```
Switch(config-if)#exit
Switch(config)#exit
Switch#show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
60   enet  100060     1500  -      -      -        -    -        0      0
70   enet  100070     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Switch#
```

6.7.3.12 HACIENDO PING

```
Santo_Domingo#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Santo_Domingo#ping 192.168.10.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Santo_Domingo#ping 192.168.10.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Santo_Domingo#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Santo_Domingo#ping 192.168.10.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Santo_Domingo#
```

CAPÍTULO 7

CONFIGURACIÓN DE LINUX

7. CONFIGURACIÓN DE LINUX

7.1 INTRODUCCIÓN A LINUX

Linux es, a simple vista, un Sistema Operativo. Es una implementación de libre distribución UNIX para computadoras personales (PC), servidores, y estaciones de trabajo. Fue desarrollado para el i386 y ahora soporta los procesadores i486, Pentium, Pentium Pro, Pentium II, entre otros, así como los clones AMD y Cyrix. También soporta máquinas basadas en SPARC, DEC Alpha, PowerPC / PowerMac.

Como sistema operativo, Linux es muy eficiente y tiene un excelente diseño. Es multitarea, multiusuario, multiplataforma y multiprocesador; en las plataformas Intel corre en modo protegido; protege la memoria para que un programa no pueda hacer caer al resto del sistema, carga sólo las partes de un programa que se usan, comparte la memoria entre programas aumentando la velocidad y disminuyendo el uso de memoria, usa un sistema de memoria virtual por páginas, utiliza toda la memoria libre para cache.

Linux permite usar bibliotecas enlazadas tanto estáticas como dinámicamente, se distribuye con código fuente, usa hasta 64 consolas virtuales, tiene un sistema de archivos avanzado pero puede usar los de los otros sistemas, y soporta redes tanto en TCP/IP como en otros protocolos.

Figura 7-1: Logo identificador de Linux

7.1.1 HISTORIA DE LINUX

LINUX hace su aparición a principios de la década de los noventa, era el año 1991 y por aquel entonces un estudiante de informática de la Universidad de Helsinki, llamado Linus Torvalds empezó, como una afición y sin poderse imaginar a lo que llegaría este proyecto, a programar las primeras líneas de código de este sistema operativo llamado LINUX.

Este comienzo estuvo inspirado en MINIX, un pequeño sistema Unix desarrollado por Andy Tanenbaum. Las primeras discusiones sobre Linux fueron en el grupo de noticias comp.os.minix, en estas discusiones se hablaba sobre todo del desarrollo de un pequeño sistema Unix para usuarios de Minix que querían más.

Linus nunca anuncio la versión 0.01 de Linux (agosto 1991), esta versión no era ni siquiera ejecutable, solamente incluía los principios del núcleo del sistema, estaba escrita en lenguaje ensamblador y asumía que uno tenía acceso a un sistema Minix para su compilación.

El 5 de octubre de 1991, Linus anuncio la primera versión "Oficial" de Linux, - versión 0.02. Con esta versión Linus pudo ejecutar Bash (GNU Bourne Again Shell) y gcc (El compilador GNU de C) pero no mucho más funcionaba. En este estado de desarrollo ni se pensaba en los términos soporte, documentación, distribución.

Después de la versión 0.03, Linus salto en la numeración hasta la 0.10, más y mas programadores a lo largo y ancho de Internet empezaron a trabajar en el proyecto y después de sucesivas revisiones, Linus incremento el número de versión hasta la 0.95 (Marzo 1992). Más de un año después (diciembre 1993) el núcleo del sistema estaba en la versión 0.99 y la versión 1.0 no llego hasta el 14 de marzo de 1994.

Desde entonces no se ha parado de desarrollar, la versión actual del núcleo es la 2.2 y sigue avanzando día a día con la meta de perfeccionar y mejorar el sistema.

7.1.2 LINUS BENEDICT TORVALDS

Linus Benedict Torvalds nació en Helsinki, Finlandia, el año 1969. Empezó a "trabajar" con ordenadores a los 10 años, cuando su abuelo le compró un Comodore el año 1980. Este buen señor era un matemático y estadista. Trabajaba en la Universidad y fue quién "enganchó" al mundo de los computadores a Linus Torvalds.

Con el paso del tiempo, Linus pasó a tener un Sinclair QL, un gran ordenador de Clive Sinclair (creador del conocido Spectrum), que tenía algún pequeño error de diseño. Linus se sintió especialmente atraído por esta máquina, después de crear aplicaciones para ésta computadora y de haber retocado su hardware con la finalidad de adaptarlo a sus necesidades. El problema que tenía dicha máquina era que los recursos eran insuficientes para poder llevar a la práctica los planes de Linus. Además, no era un equipo compatible. Así pues, el mes de enero de 1991 compró su primer PC, un 386.

En 1988 cuando Linus entró a la Universidad, en este mismo año fue cuando un sistema operativo didáctico, basado en Unix y creado por Andy Tanenbaum, empezó a cobrar importancia. Dicho sistema operativo era el famoso Minix.

Linus entró a formar parte de la comunidad de usuarios de Minix. Tanenbaum cometió un error en su sistema operativo. Era demasiado limitado, tanto técnicamente como políticamente, es decir, en ningún momento tuvo en cuenta la posibilidad de incluir Minix al proyecto GNU (creado el año 1983 por Richard Stallman). En realidad, la creación de Andy Tanenbaum estaba pensada para ser distribuida comercialmente. Su principal error fue ceder todos los derechos a Prentice Hall, que empezó a cobrar 150 dólares por licencia.

Así pues, Linus tomó la decisión de cambiar esta política debido a que el sistema Minix era ideal para los estudiantes de sistemas operativos, y su precio era considerablemente alto. Llegamos de nuevo al año 1991, cuando Linus se acabó de comprar su primer 386. En aquellos momentos, la intención de Linus era clara; crear un nuevo Kernel de UNIX basado en el Kernel de Minix y modificarlo periódicamente de manera que fuera capaz de ejecutar aplicaciones GNU.

7.2 REQUERIMIENTOS PARA LA INSTALACIÓN DE LINUX

Para un buen desempeño del sistema Operativo Linux Fedora Core 3 se recomienda:

7.2.1 REQUERIMIENTO MÍNIMO

- Procesador Intel Pentium II de 300 Mhz
- 64 MB de RAM
- 3 GB de Espacio en Disco
- Unidad de CD – ROM
- Tarjeta de Red 10/100 Mbps
- 3 Discos de Instalación (Fedora Core 3)

7.2.2 REQUERIMIENTO ÓPTIMO

- Procesador Intel Pentium IV de 3.00 Ghz
- 512 MB de RAM
- 5 GB de Espacio en Disco
- Unidad de CD – ROM
- Tarjeta de Red 10/100 Mbps
- 3 Discos de Instalación (Fedora Core 3)

7.3 DESCRIPCIÓN DEL BIOS

El BIOS (Basic Input Output System – Sistema Básico de Entrada Salida) es un programa que se encuentra grabado en un chip de la placa base, concretamente en una memoria de tipo ROM (Read - Only Memory). Este programa es el que se encarga de comprobar el hardware instalado en el sistema, ejecutar un test inicial de arranque, inicializar circuitos, manipular periféricos y dispositivos a bajo nivel y cargar el sistema de arranque que permite iniciar el sistema operativo. En resumen, es lo que permite que el ordenador arranque correctamente en primera instancia.

Inicialmente era muy complicado modificar la información del BIOS en el ROM, pero hoy en día la mayoría de los BIOS están almacenados en una memoria flash capaz de ser rescrita, esto es lo que permite que se pueda actualizar. El BIOS se apoya en otra memoria, llamada CMOS porque se construye con esa tecnología, en ella carga y almacena los valores que necesita y que son susceptibles de ser modificados (cantidad de memoria instalada, numero de discos duros, fecha y hora, etc). A pesar de que apaguemos el ordenador, los valores de la memoria de BIOS se mantienen intactos, ¿cómo es posible?, pues gracias a una pila que la alimenta. Puesto que el consumo es muy bajo y se recarga al encender el ordenador, la pila puede durar varios años.

Cuando hay problemas con la pila, los valores de dicha memoria tienden a perderse, y es cuando pueden surgir problemas en el arranque del tipo: pérdida de fecha y hora, necesidad de reconfigurar dispositivos en cada arranque, y otros. En caso de problemas sustituir la pila es trivial, basta con comprar una de iguales características, retirar la vieja y colocar la nueva en su lugar.

En condiciones normales no es necesario acceder al BIOS ya que al instalar un dispositivo, siempre que hayamos tenido la precaución de asegurarnos que es compatible o aceptable por nuestra placa base, éste es reconocido inmediatamente y configurado por BIOS para el arranque. No obstante, hay ocasiones en las que se hace necesario acceder a su configuración, en este manual veremos cómo hacerlo y algunos ejemplos.

7.3.1 ACCESO Y MANIPULACIÓN DEL BIOS

Para acceder al programa de configuración del BIOS, generalmente llamado CMOS, Setup, tendremos que hacerlo pulsando un botón durante el inicio del arranque del ordenador. Generalmente suele ser la tecla "Supr" aunque esto varía según los tipos de placa y en portátiles. Otras teclas empleadas son: "F1", "Esc", o incluso una combinación, para saberlo con exactitud bastará con una consulta al manual de su placa base o bien prestando atención a la primera pantalla del arranque, ya que suele figurar en la parte inferior un mensaje similar a este: Press DEL to enter SETUP.

Figura 7-2: Pantalla principal de arranque

7.3.2 ASPECTO DEL BIOS

El aspecto general del BIOS dependerá de qué tipo en concreto tenga en su placa, las más comunes son: Award, Phoenix (se han unido) y AMI. Bastante similares pero no iguales. El programa del BIOS suele estar en un perfecto inglés y además aparecen términos que no son realmente sencillos.

Aunque tengan nombres diferentes, existen algunos apartados comunes a todos los tipos de BIOS. Una clasificación puede ser:

1. Configuración básica de parámetros - Standard CMOS Setup.
2. Opciones de BIOS - BIOS Features, Advanced Setup.
3. Configuración avanzada y chipset - Chipset features.
4. Password, periféricos, discos duros, etc.
5. Otras utilidades.

Bajo el **1er punto** se puede encontrar la configuración de la fecha y hora, los discos duros conectados (IDE) y la memoria detectada, entre otras cosas.

En el **punto 2** existen muchos parámetros modificables, suelen aparecer: caché, secuencia de arranque (Boot sequence), intercambio de disqueteras, etc.

En el **punto 3** podemos encontrar parámetros relativos a las características del chipset, memoria RAM, buses y controladores.

Bajo el **punto 4** hemos reunido una serie de opciones que suelen estar distribuidas, gracias a ellas podemos insertar una contraseña de acceso al programa del BIOS, modificar parámetros relativos a los periféricos integrados, control de la administración de energía, control de la frecuencia y el voltaje, etc. Y finalmente en el **punto 5** reunimos las opciones que nos permiten guardar los cambios efectuados, descartarlos, cargar valores por defecto, etc.

7.3.3 CONFIGURACIÓN DEL BIOS PARA LA INSTALACIÓN DE LINUX

En la parte inferior de la interfaz del programa se puede ver el inventario de teclas necesarias para que pueda navegar entre las opciones y modificarlas, es importante que lo lea y que lo tenga en cuenta.

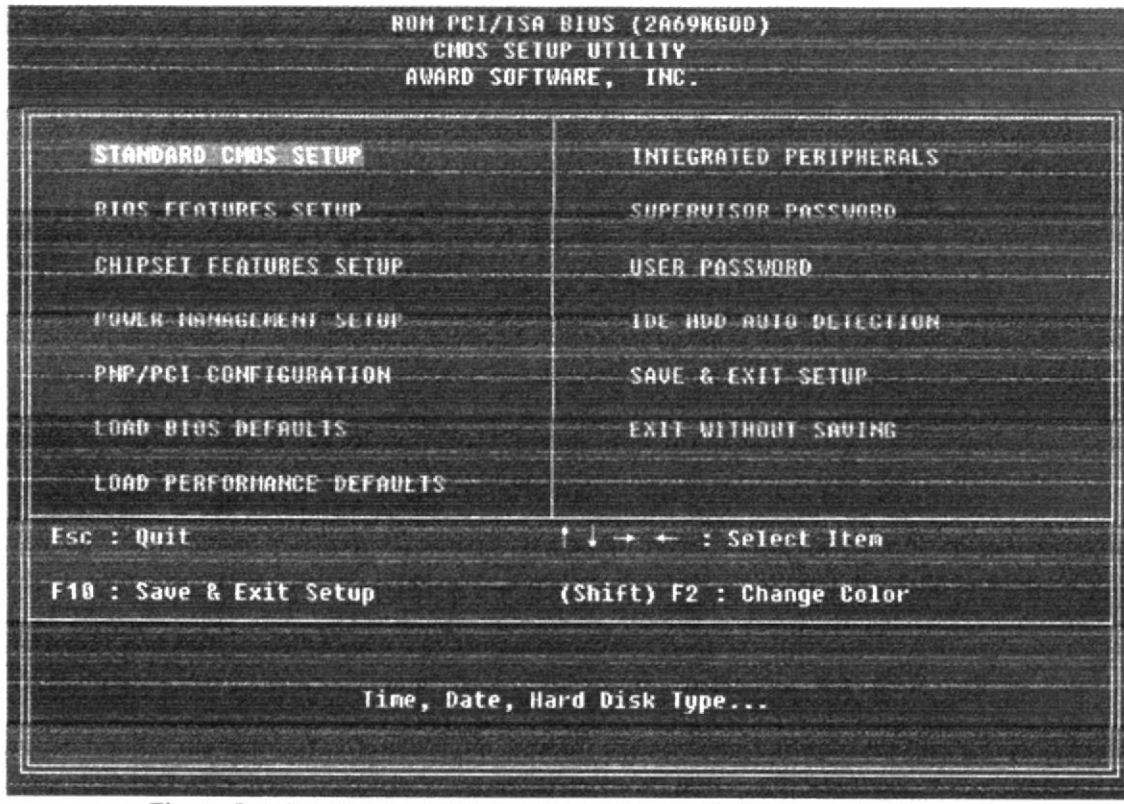


Figura 7-3: Imagen de la interfaz más común de BIOS (Award y Phoenix)

Con las teclas direccionales debe desplazarse hasta el ítem BIOS FEATURES SETUP (Arreglos que ofrece el Bios) y presione enter.

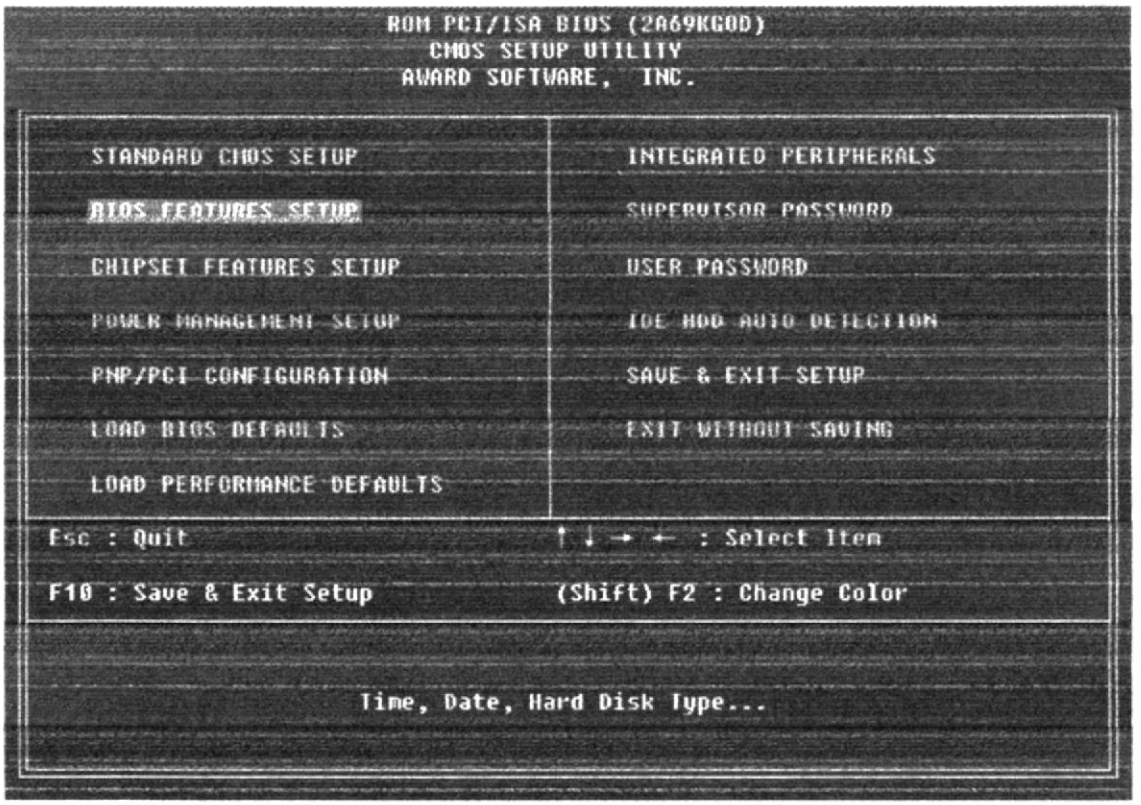


Figura 7-4: Seleccionando las opciones del Bios

En la siguiente pantalla seleccione Boot Sequence (Secuencia de arranque) y con la tecla (**AvPág**) elija CDROM, para que el PC arranque desde el CDROM (dé quitar la protección antivirus, (Disabled) y cuando termine con la instalación de Linux puede activarla (Enabled)).

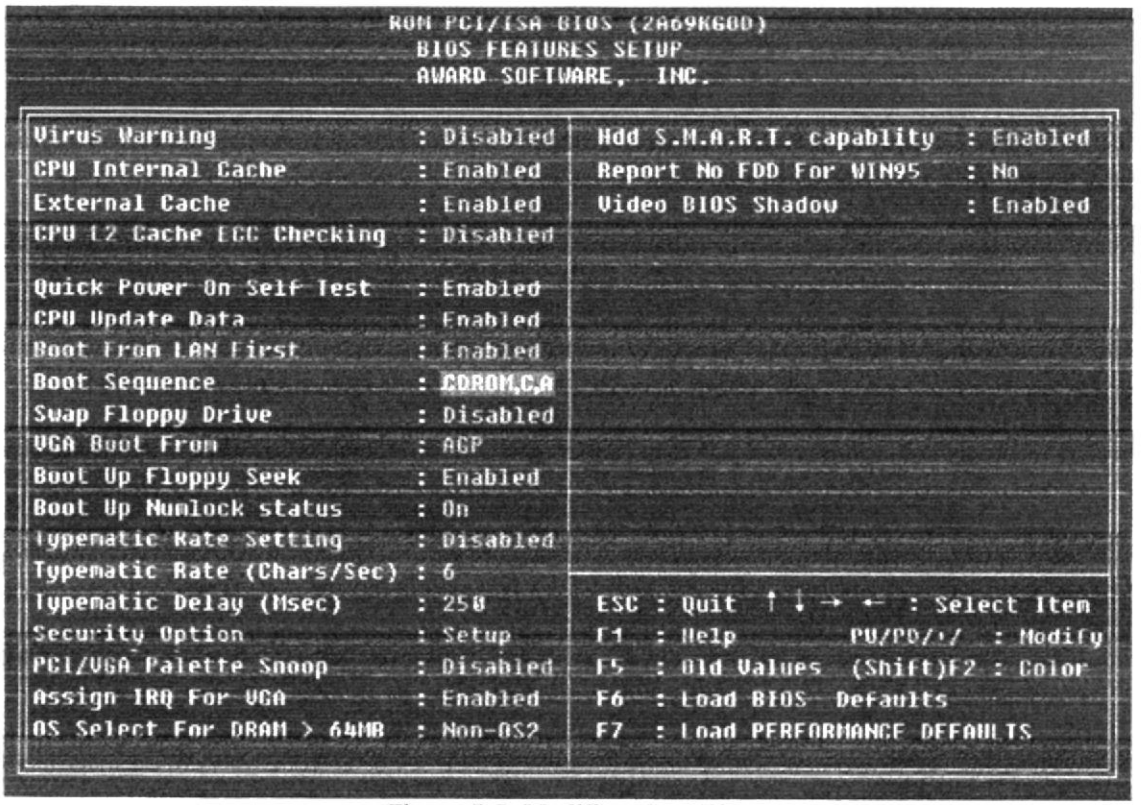


Figura 7-5: Modificando el Bios

Presione la tecla ESC para salir y regresar al menú principal del Setup, donde debe seleccionar el item SAVE & EXIT SETUP (Guardar y salir) y presione enter.

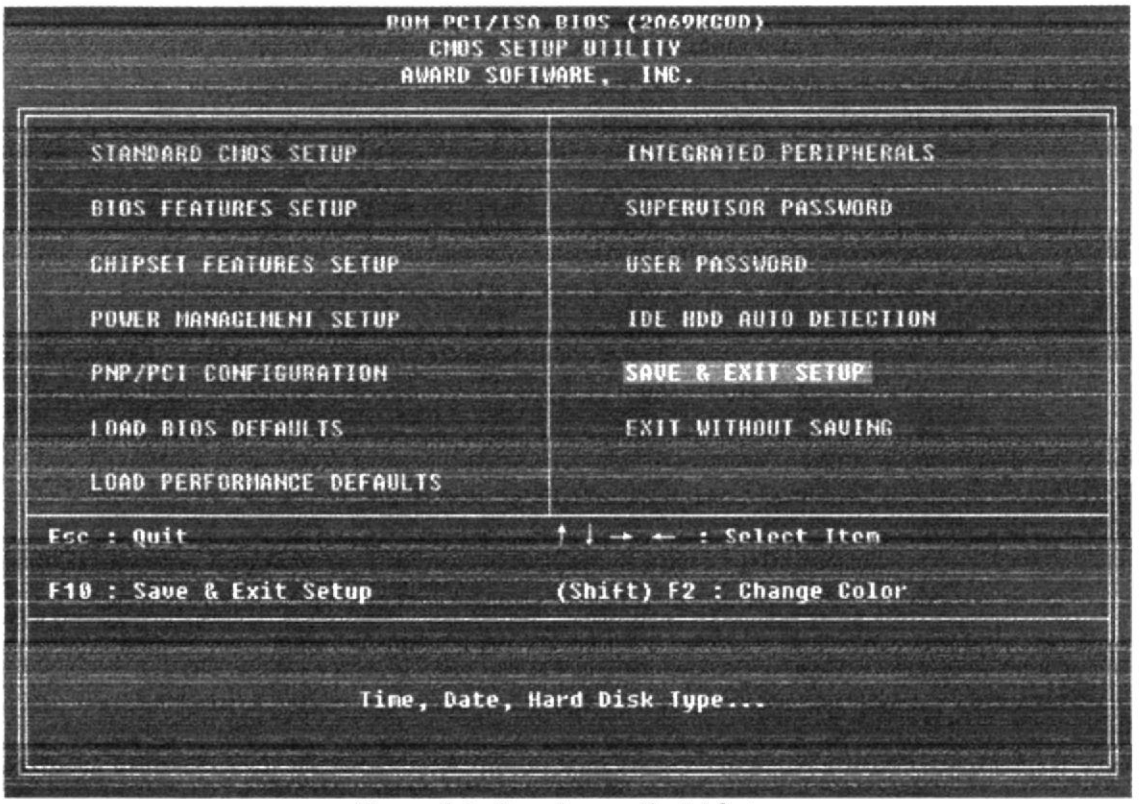


Figura 7-6: Guardar y salir del Setup

Luego le aparece una pequeña pantalla donde le pregunta si desea guardar los cambios realizados en el Bios, presione la tecla (**Y**) para grabar y presione enter.

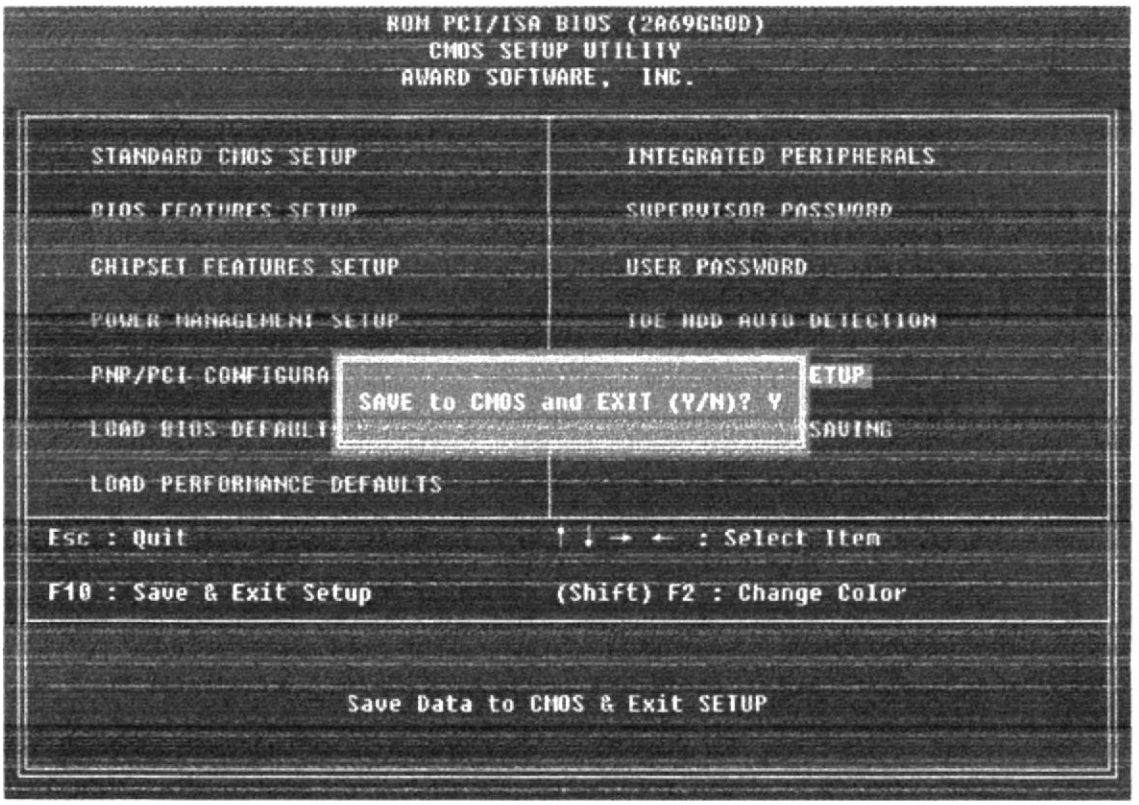


Figura 7-7: Guardando los cambios en el Bios

7.4 INSTALACIÓN DE LINUX FEDORA CORE 3

Inserte el Disco N° 1 de Linux Fedora Core 3 en la unidad de CD - ROM luego debe reiniciar el equipo para que automáticamente detecte el disco y proceda con la instalación.

Después le aparecerá la pantalla del asistente, donde le indica si desea instalar Linux Fedora Core 3 en modo gráfico o en modo texto.

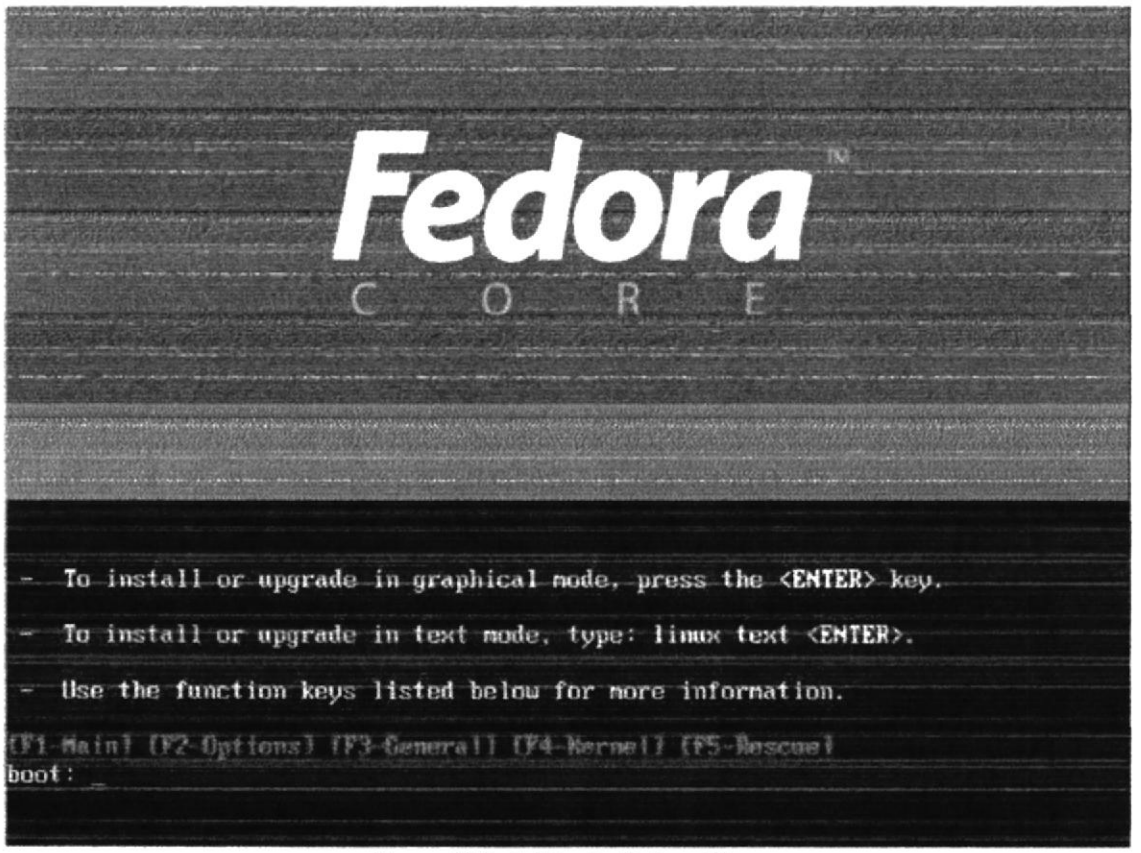


Figura 7-8: Asistente Fedora Core

Después aparece una pantalla de comprobación para verificar el correcto funcionamiento de los CD´s de instalación. Luego presione Skip, con la tecla enter para que salte esta opción.

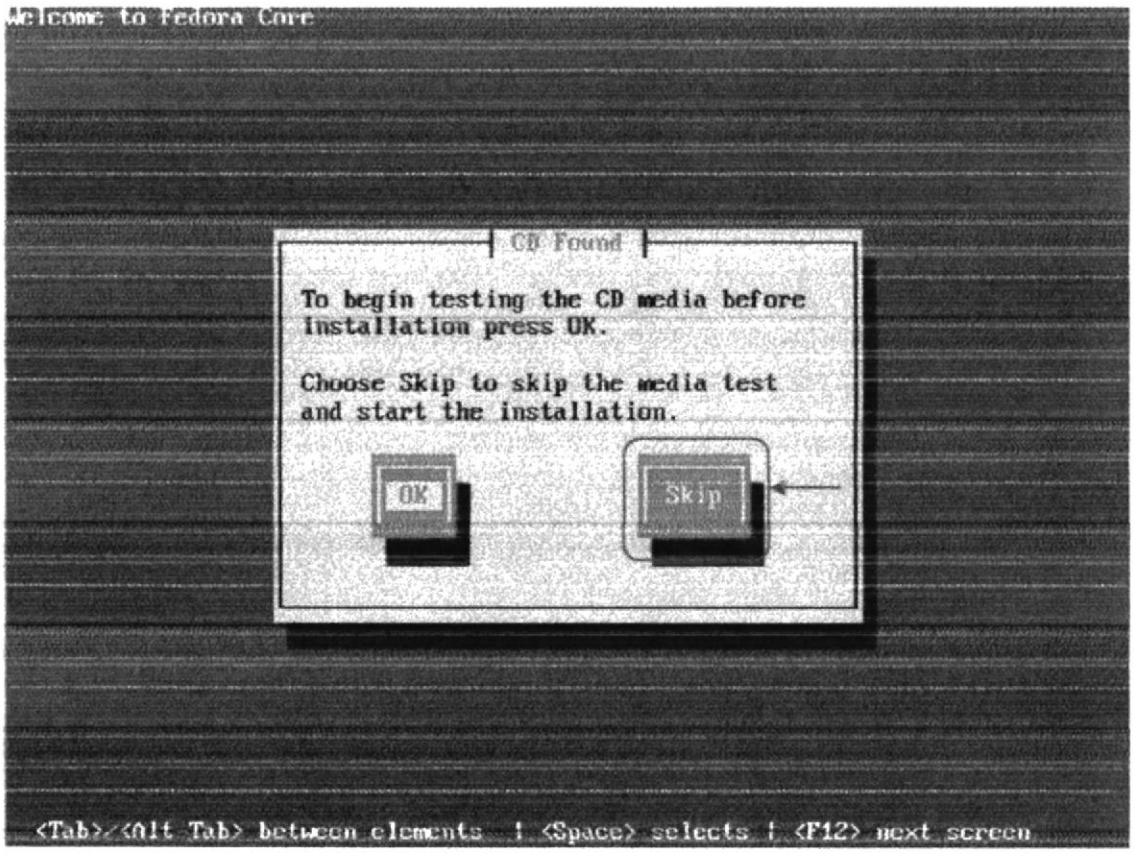


Figura 7-9: Asistente Fedora Core

Luego le aparece la pantalla de bienvenida, donde le indica los pasos a seguir para su correcta instalación, entre ellos menciona que puede usar el Mouse o el teclado para navegar entre las diferentes pantallas durante la instalación.

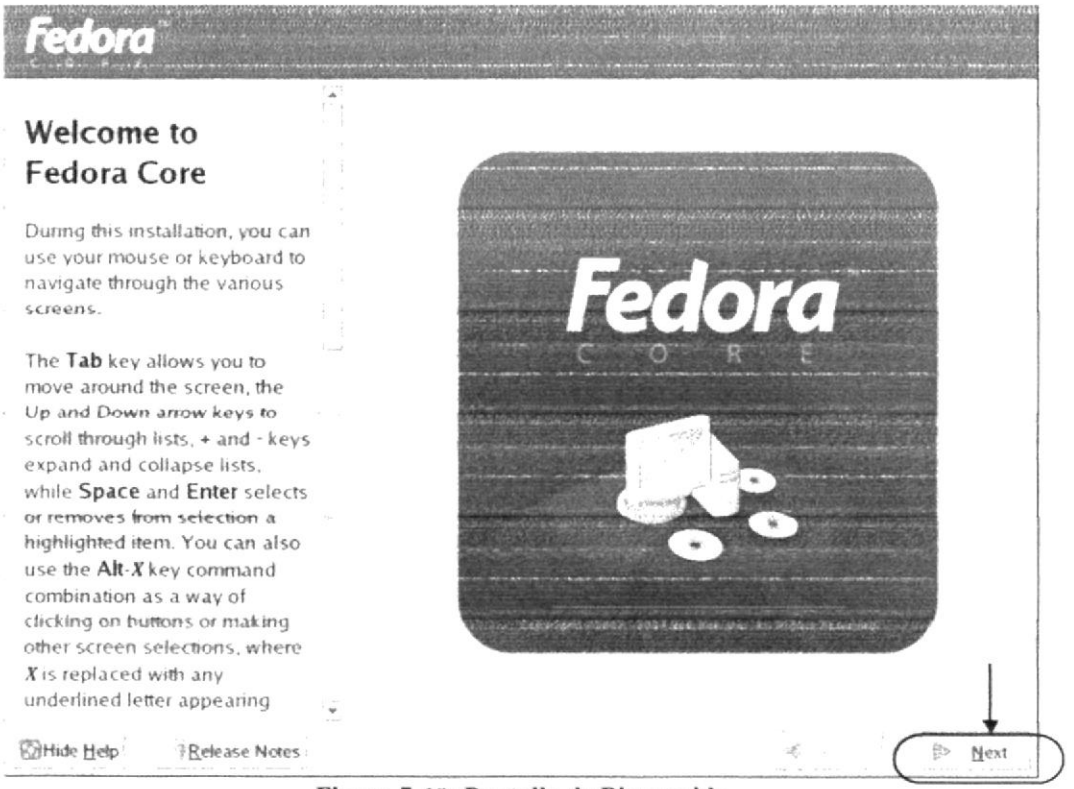


Figura 7-10: Pantalla de Bienvenida

En la siguiente pantalla debe elegir el idioma para continuar con la instalación, seleccione Spanish (Español) y presione next.

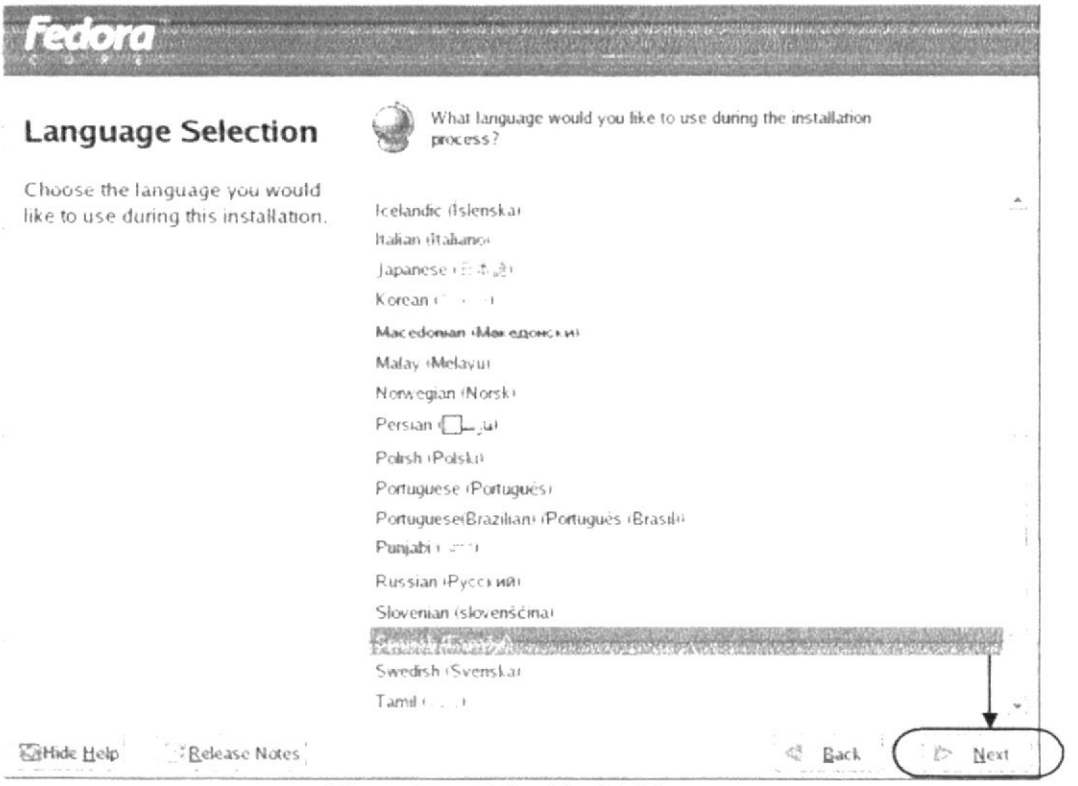


Figura 7-11: Selección del Idioma

Luego le pide que seleccione la configuración del teclado que va a utilizar, en este caso Spanish (Español) y presione next.

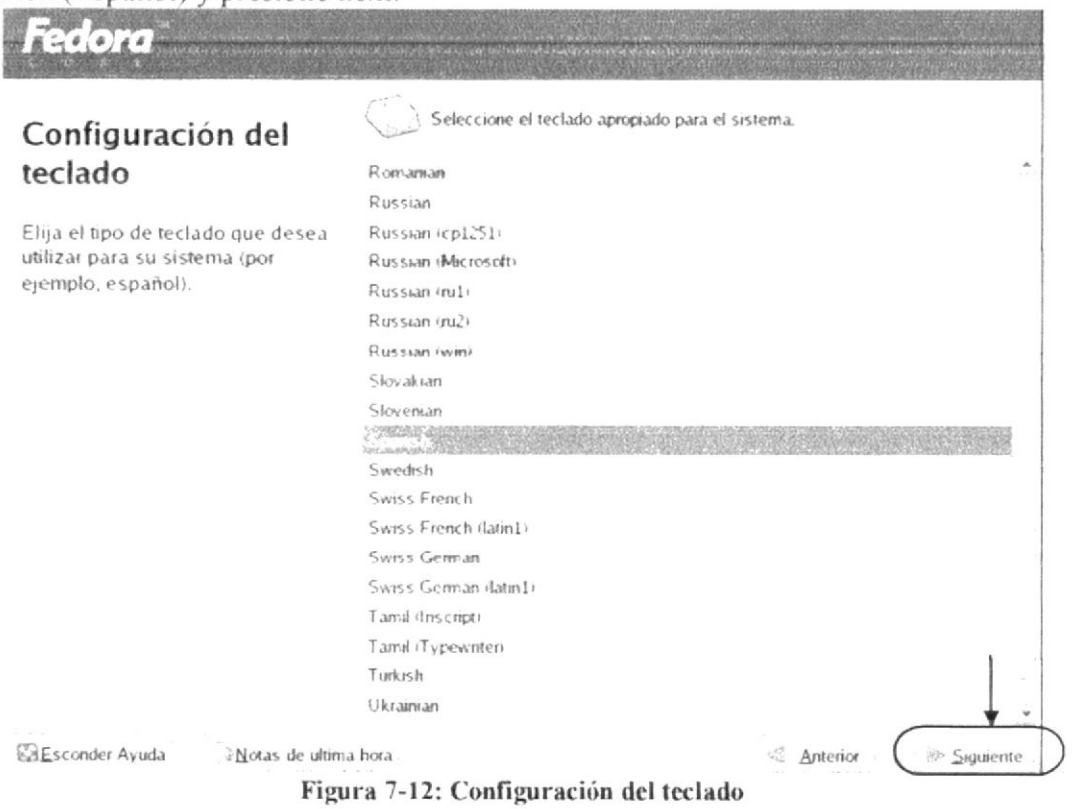


Figura 7-12: Configuración del teclado

Luego seleccione el tipo de instalación que necesita, en este caso personalizada.

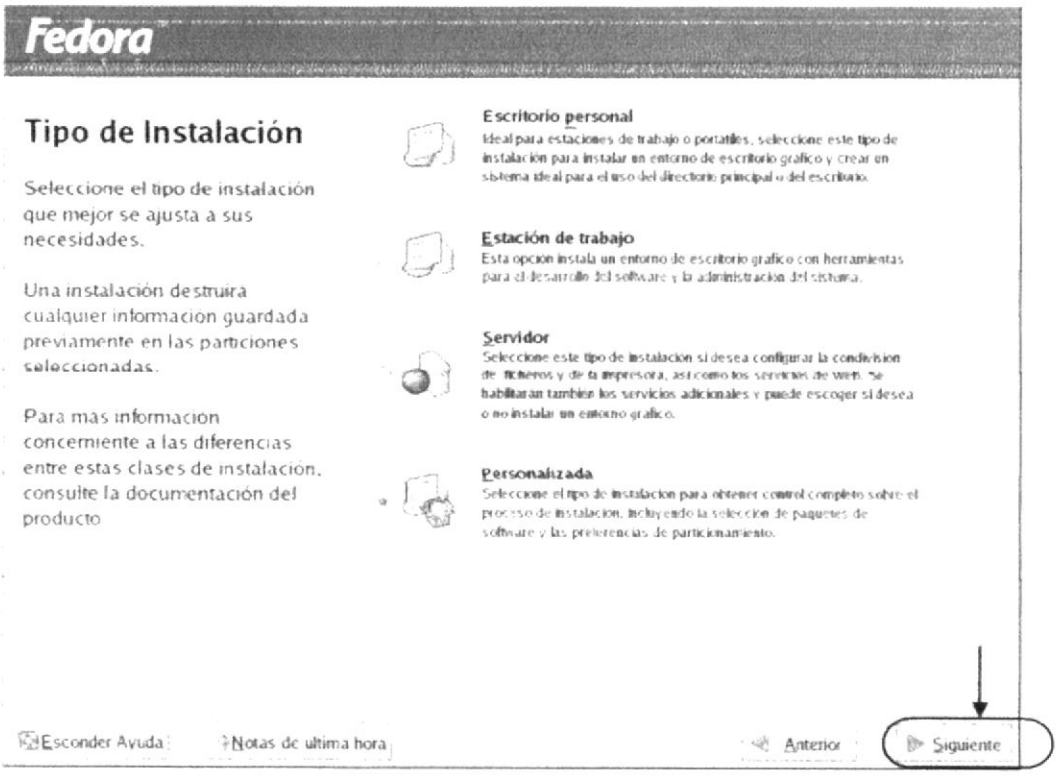


Figura 7-13: Tipo de Instalación Personalizada

Tipos de Instalación:

- Si elige esta opción le permite darle un uso personal a Linux como una estación de escritorio.

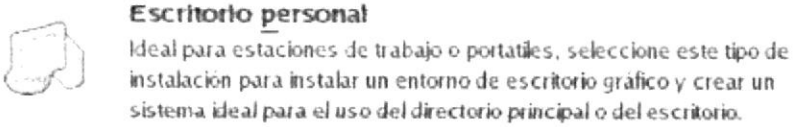


Figura 7-14: Escritorio Personal

- Si elige esta opción, es para usuarios que van a trabajar en Linux, para desarrollar programas.

Figura 7-15: Estación de trabajo

- Si elige esta opción, le permite utilizar Linux como servidor, ya que el asistente instalará todos los paquetes relacionados con los servidores.

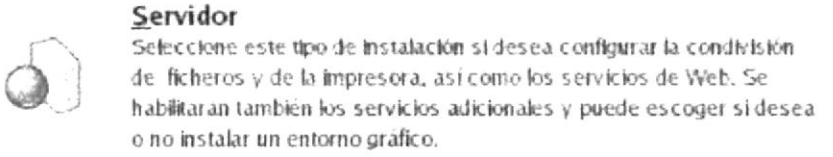


Figura 7-16: Servidor

- Si elige esta opción, le permite realizar una configuración completamente personalizada en donde podrá instalar paquetes adicionales.

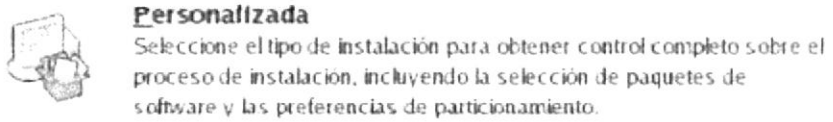


Figura 7-17: Personalizada

Luego el asistente le pregunta si desea darle una partición al disco de forma automática o de forma manual, seleccione Partición manual.

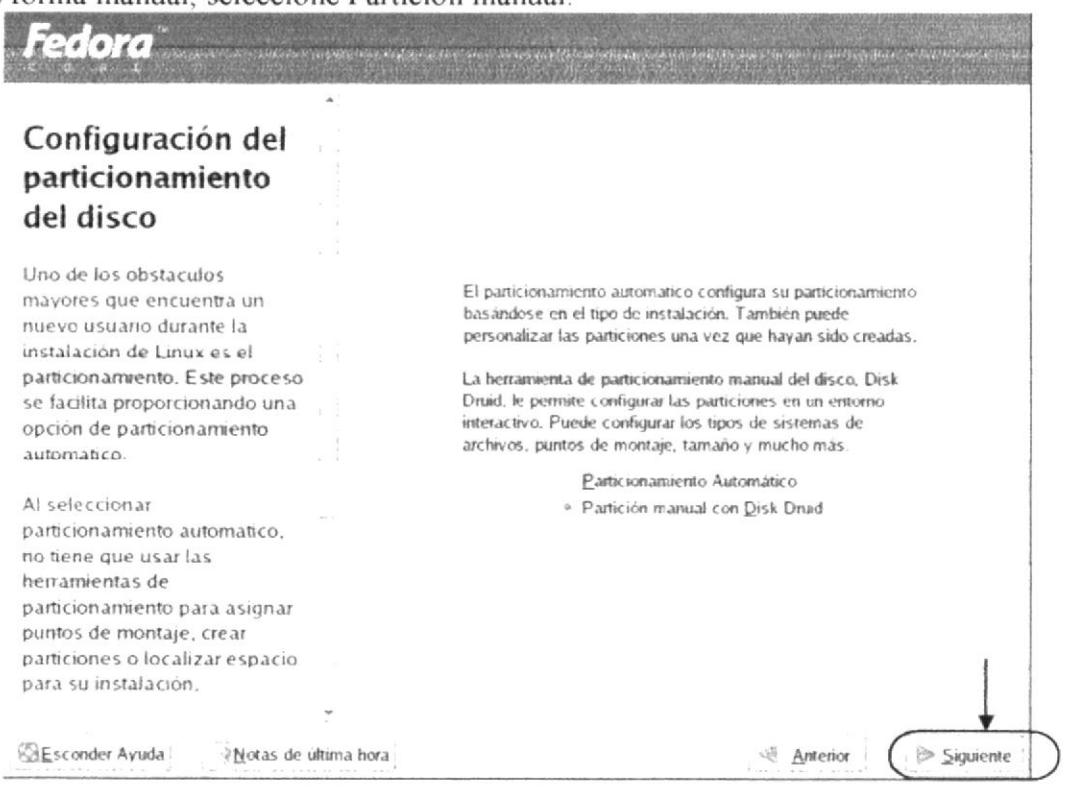


Figura 7-18: Partición del Disco

Partición automática:
La partición automática, configura la partición basándose en el tipo de instalación.

Partición manual:
La partición manual del disco, le permite configurar en un entorno interactivo, los tipos de sistemas de archivo, punto de montaje, tamaño, entre otros.

En esta pantalla el asistente le muestra el espacio disponible que posee su disco duro, para que pueda configurarlo e instalar Linux Fedora Core 3.

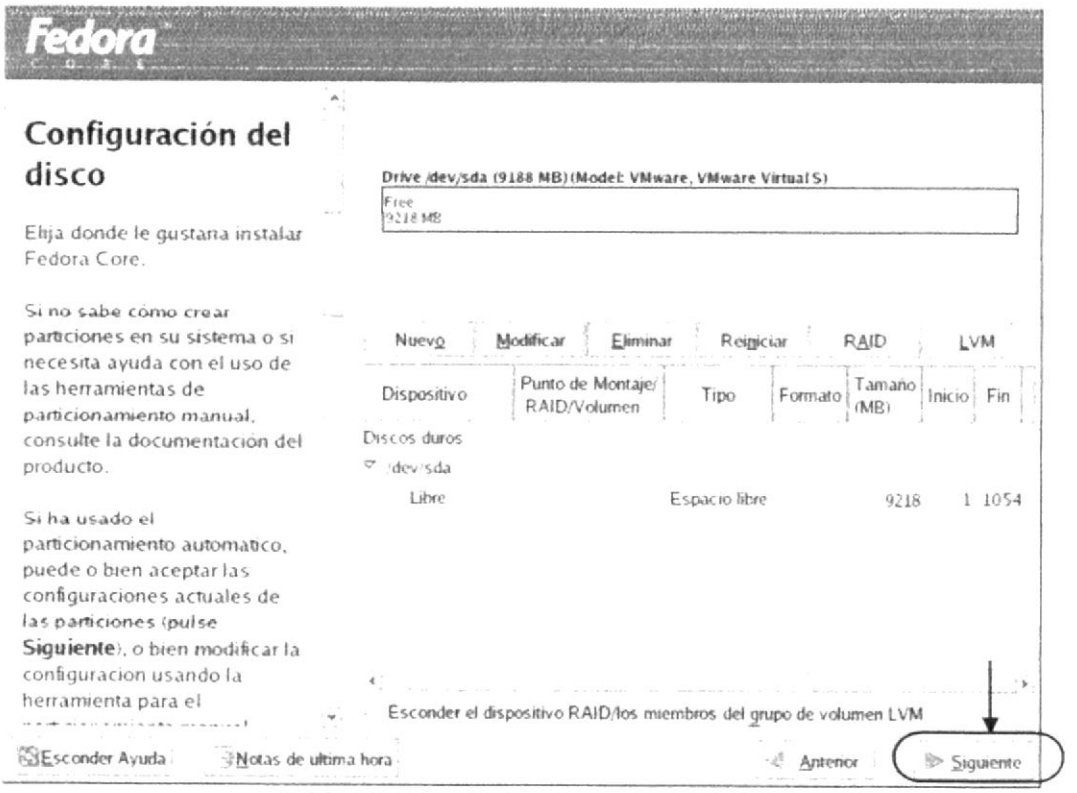


Figura 7-19: Configuración del Disco

Luego proceda a crear las particiones que necesitará, comenzando por la **/boot**, que le servirá de ayuda cuando instale otro Sistema Operativo, posee un tamaño mínimo de 100 MB.

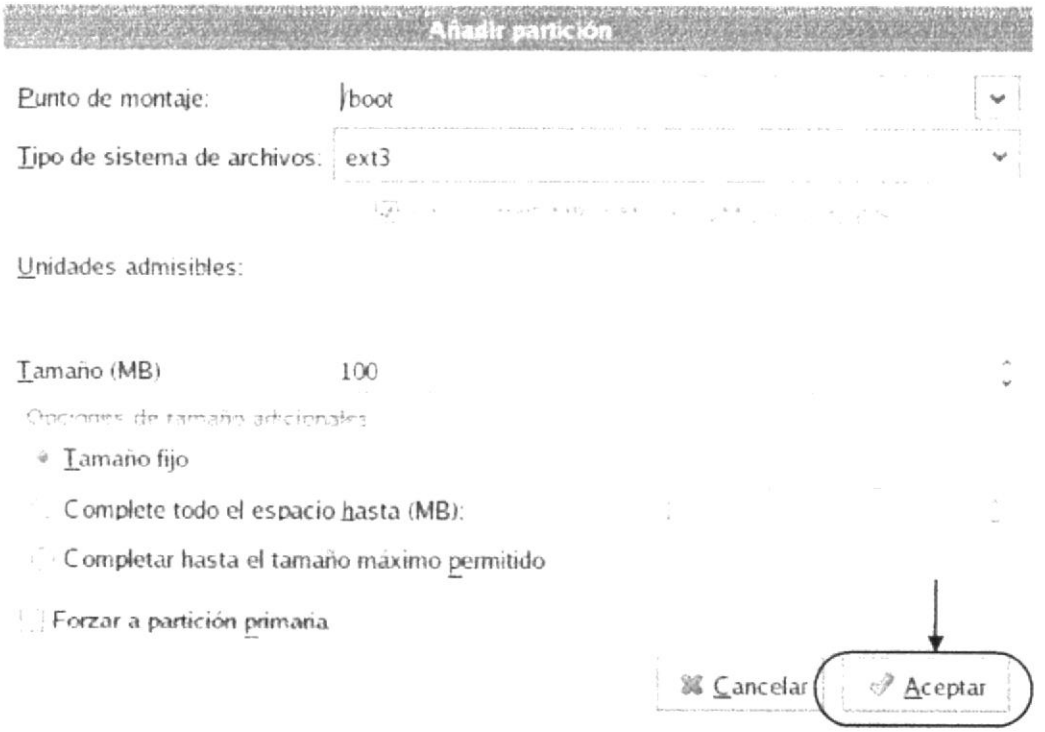


Figura 7-20: Partición /boot

La siguiente partición que va a crear es la swap, este es un espacio reservado en el disco duro para poder usarse como una extensión de memoria virtual del sistema. Esta partición equivale al doble de lo que posee la memoria RAM en la computadora.

Memoria RAM	→	**Swap**
64 MB	→	128 MB
128 MB	→	256 MB
256 MB	→	512 MB Valor máximo para el sistema Swap

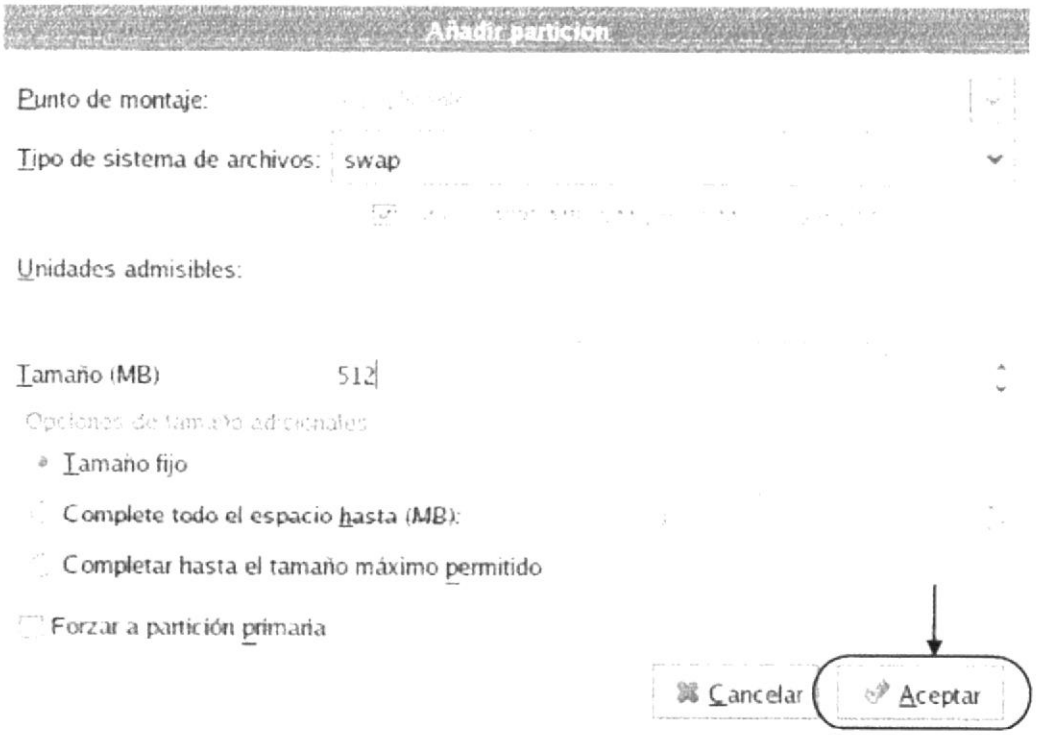


Figura 7-21: Partición swap

La ultima partición que va a crear es la Raíz la cual esta representada por (/) y es la partición principal donde se guardará su sistema de archivos, la misma que debe tener un tamaño mínimo de 3000 MB.

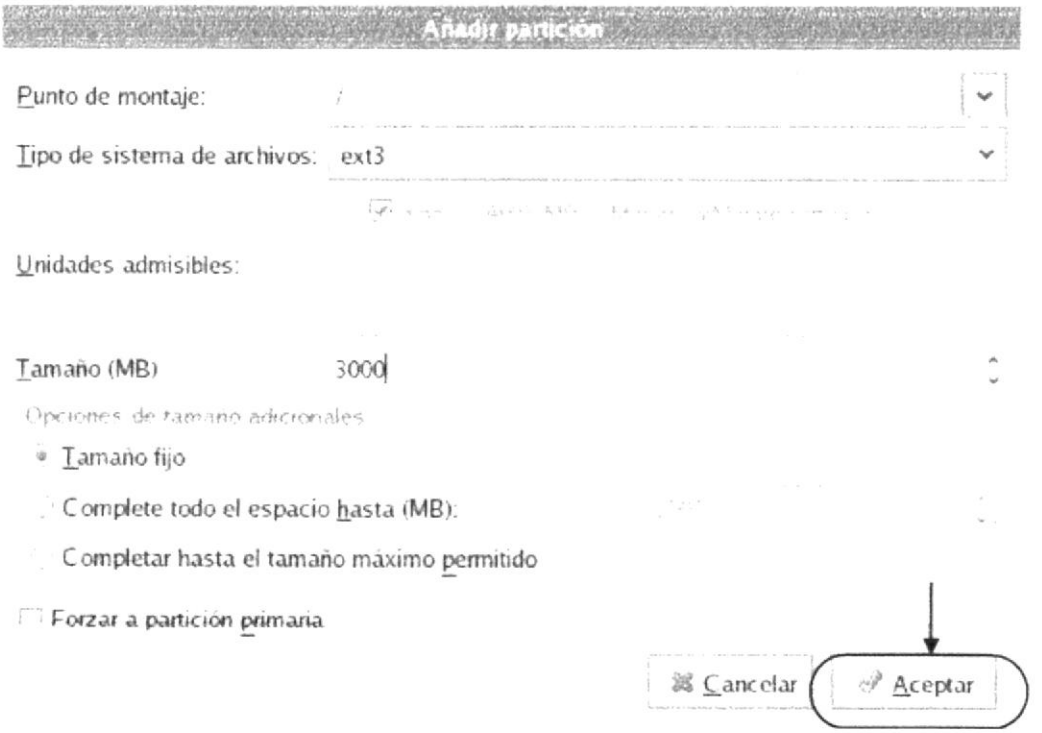


Figura 7-22: Partición de Raíz (/)

Luego de crear sus particiones el asistente le mostrará los valores que ingresó y el espacio libre que posee en el disco duro.

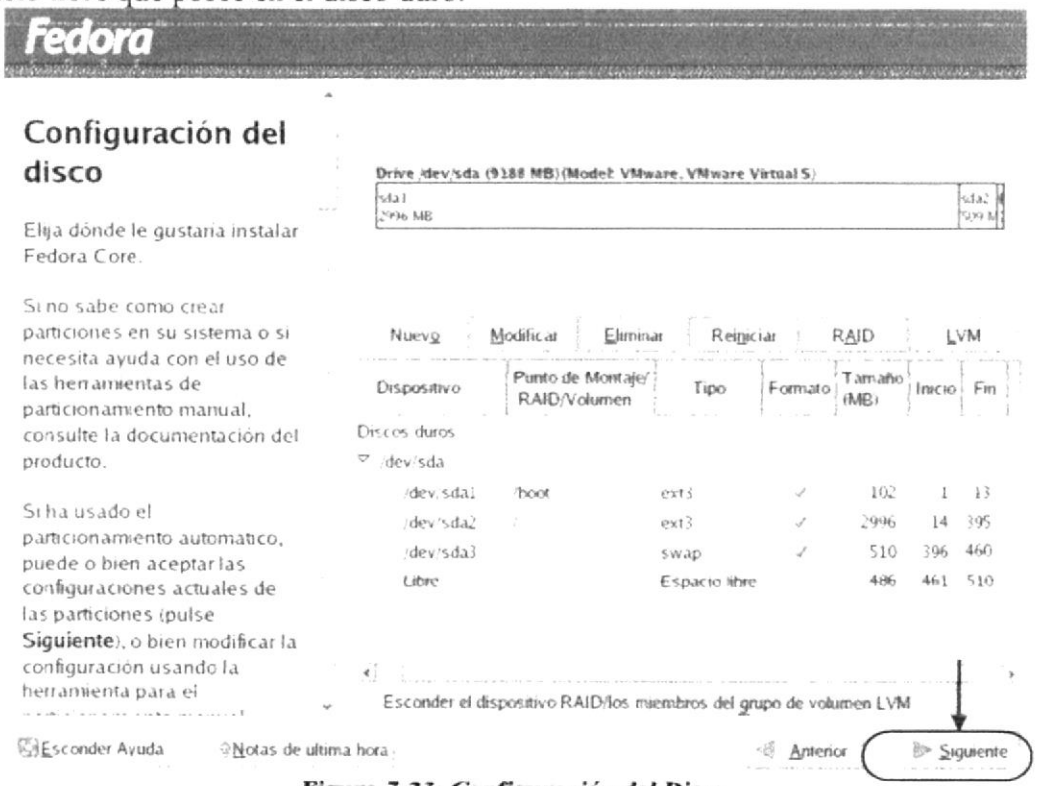


Figura 7-23: Configuración del Disco

En la siguiente pantalla el asistente le indica el gestor de arranque, el cual le permite elegir con que sistema operativo desea que se inicie el equipo en caso de que exista otro.

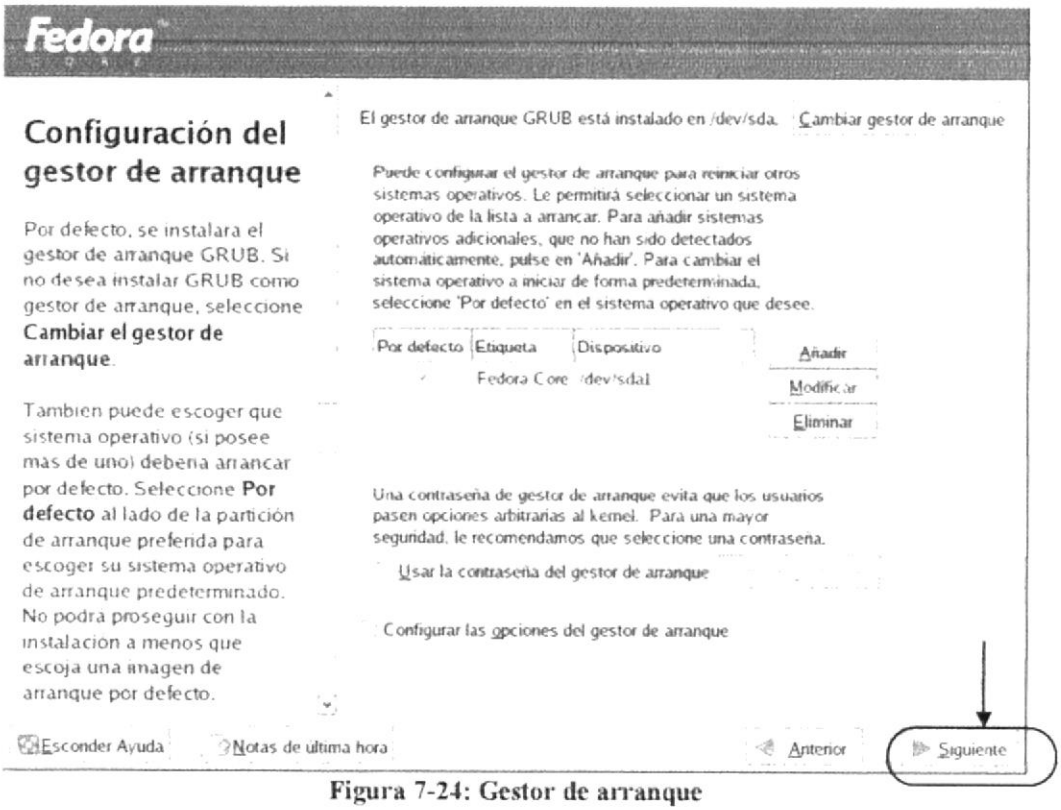


Figura 7-24: Gestor de arranque

En la siguiente pantalla el asistente le indica si desea configurar la tarjeta de red, omita este paso y le de clic en siguiente (puede configurar la tarjeta de red más adelante en modo comando).

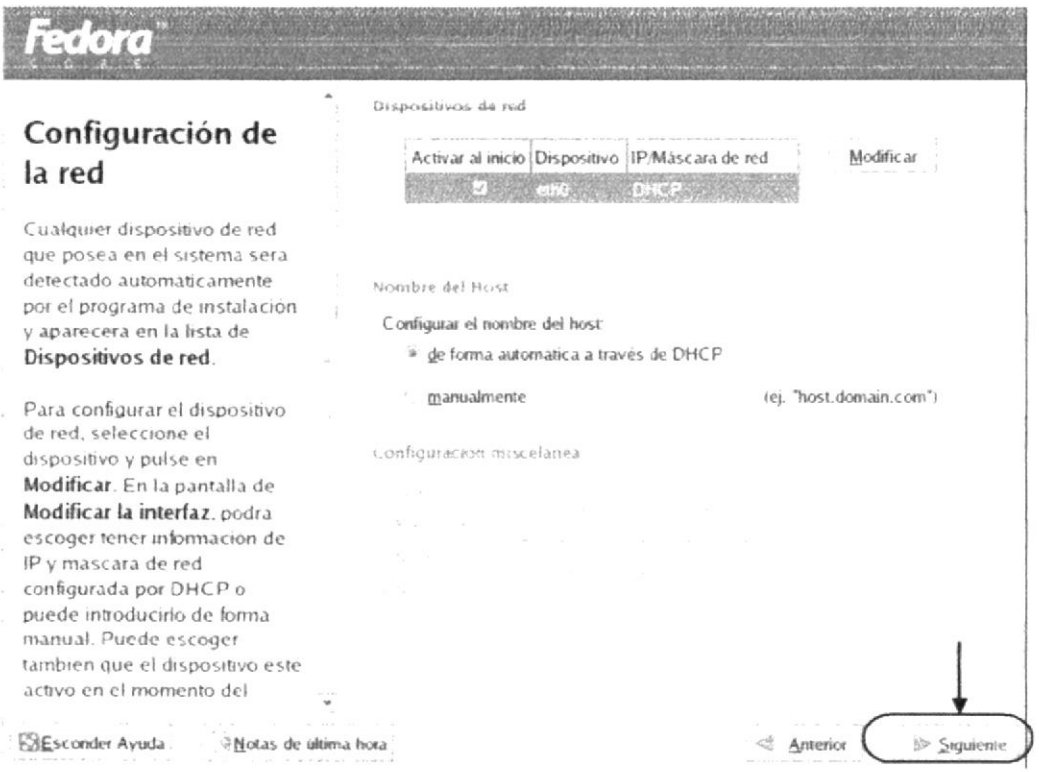


Figura 7-25: Configurando la red

Luego el asistente le da la opción de configurar los Firewalls, omita esta opción y seleccione ningún cortafuego (puede configurar los firewalls más adelante en modo comando).

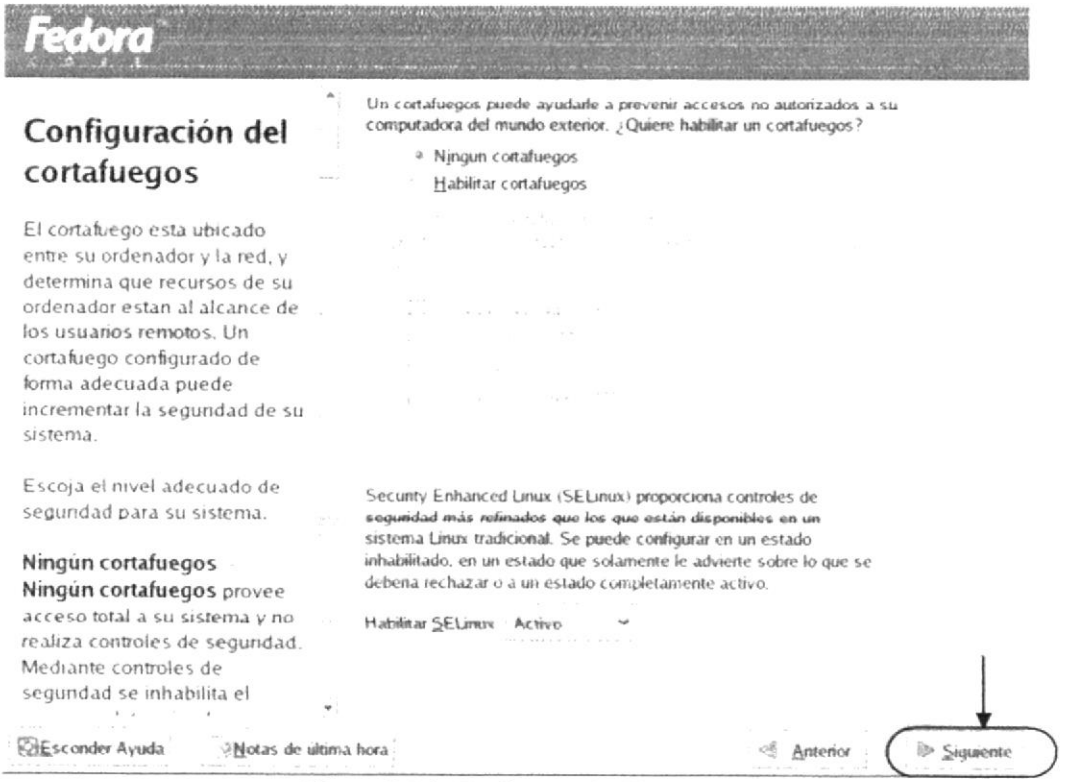


Figura 7-26: Configurando Firewalls

Luego el asistente le muestra una advertencia para omitir o no la configuración de los cortafuegos, seleccione proceder.

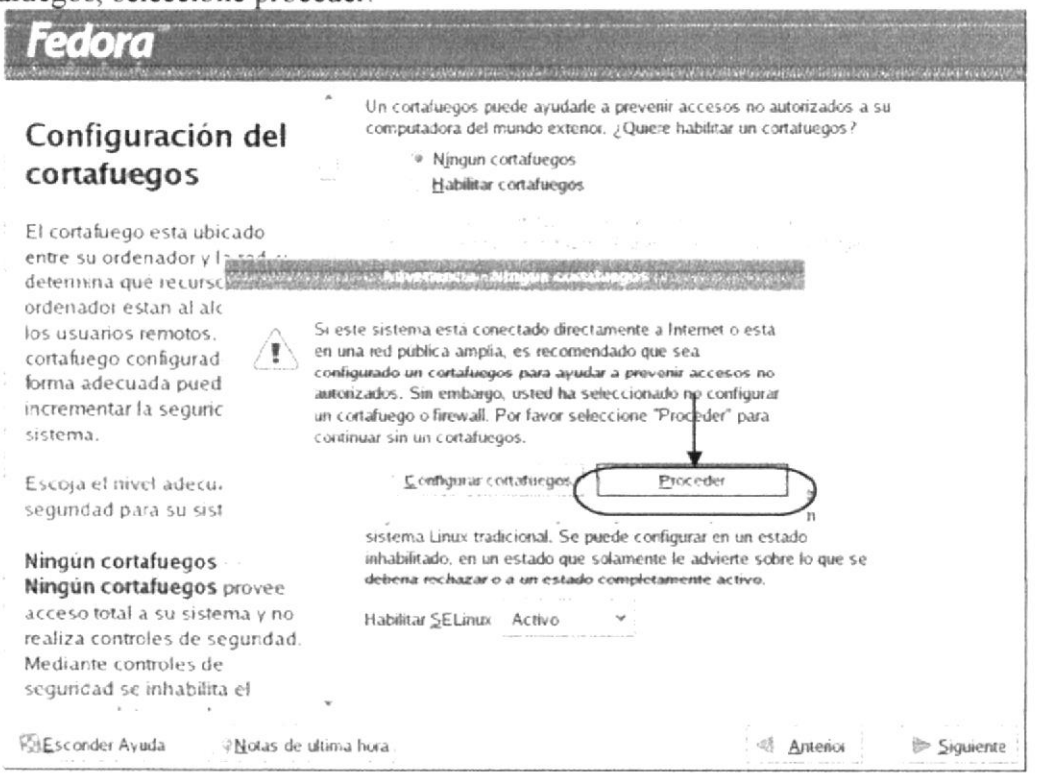


Figura 7-27: Advertencia – deshabilitar Firewalls

Luego el asistente le pide seleccionar el idioma por defecto para cambiar el idioma predeterminado después de la instalación.

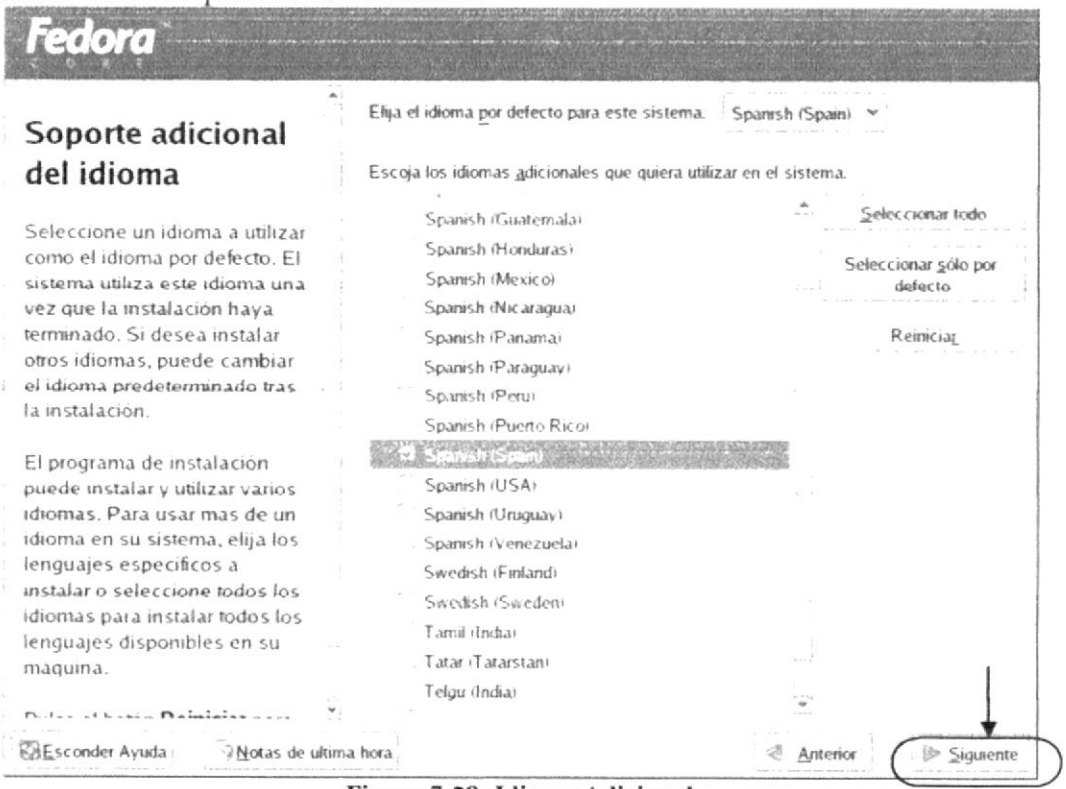


Figura 7-28: Idioma Adicional

En la siguiente pantalla configure la zona horaria. (América/Guayaquil)

Figura 7-29: Zona Horaria

Luego el asistente le pide que ingrese una contraseña para el administrador (Root) y asigne como contraseña tópico.

Figura 7-30: Contraseña del administrador

En la siguiente pantalla seleccione los paquetes que va a instalar para la configuración necesaria.

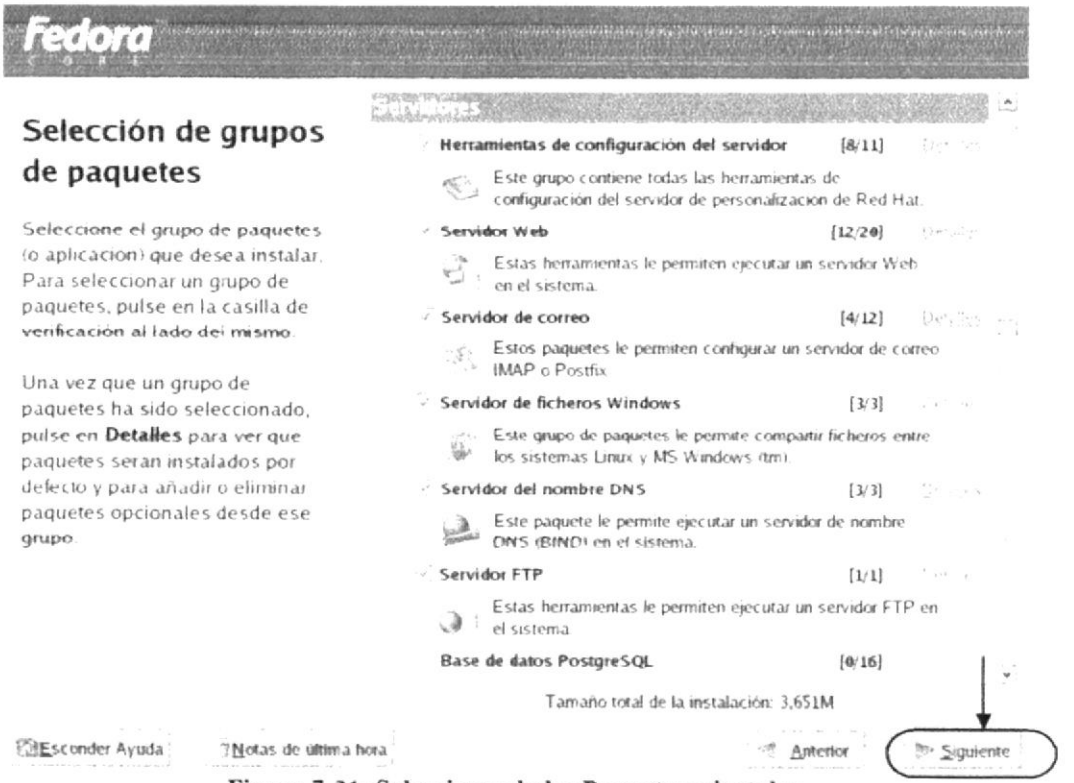


Figura 7-31: Seleccionando los Paquetes a instalar

Luego el asistente le indica que todo está listo para la instalación.

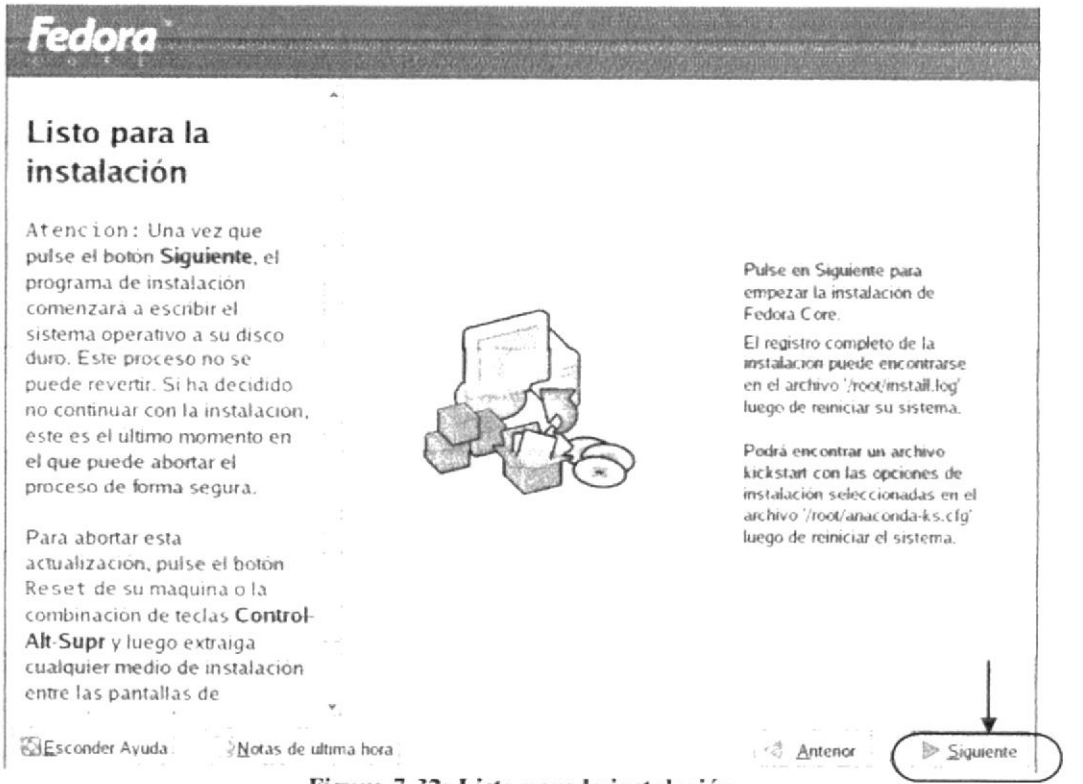


Figura 7-32: Listo para la instalación

Luego el asistente le indica que disco va a utilizar de acuerdo a los paquetes que selecciono.

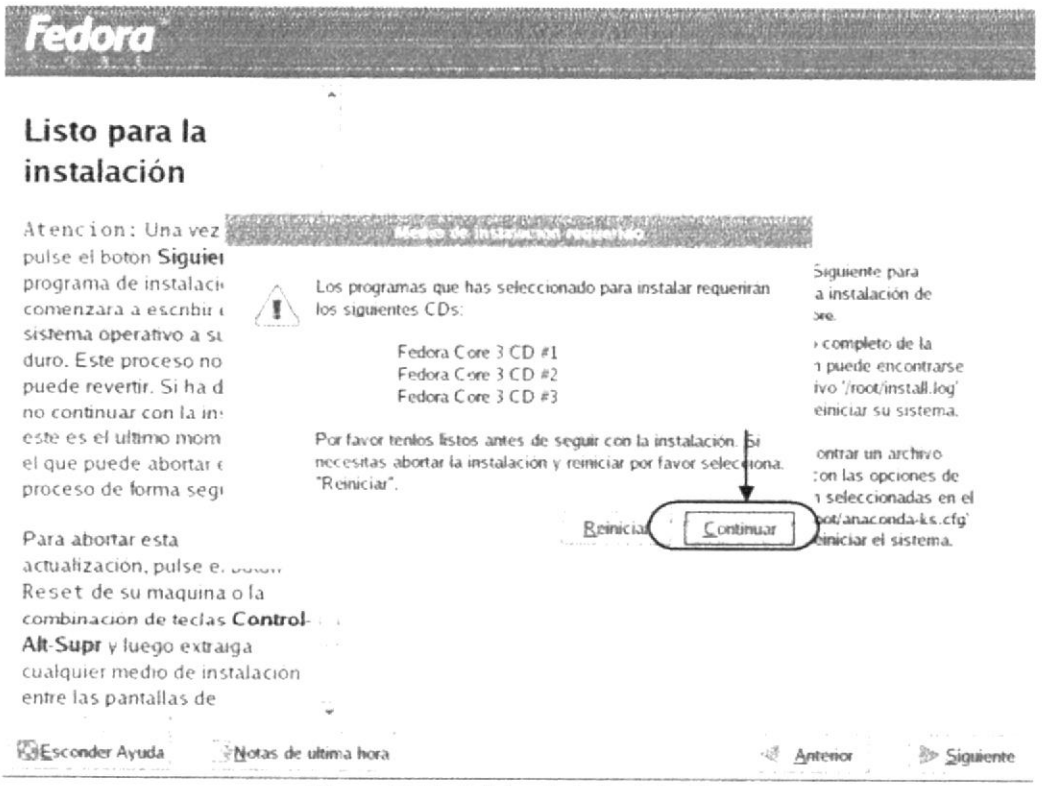


Figura 7-33: Iniciando la instalación

En esta pantalla el asistente le muestra el proceso de formateo del sistema de ficheros, en este caso la particiones que creó.

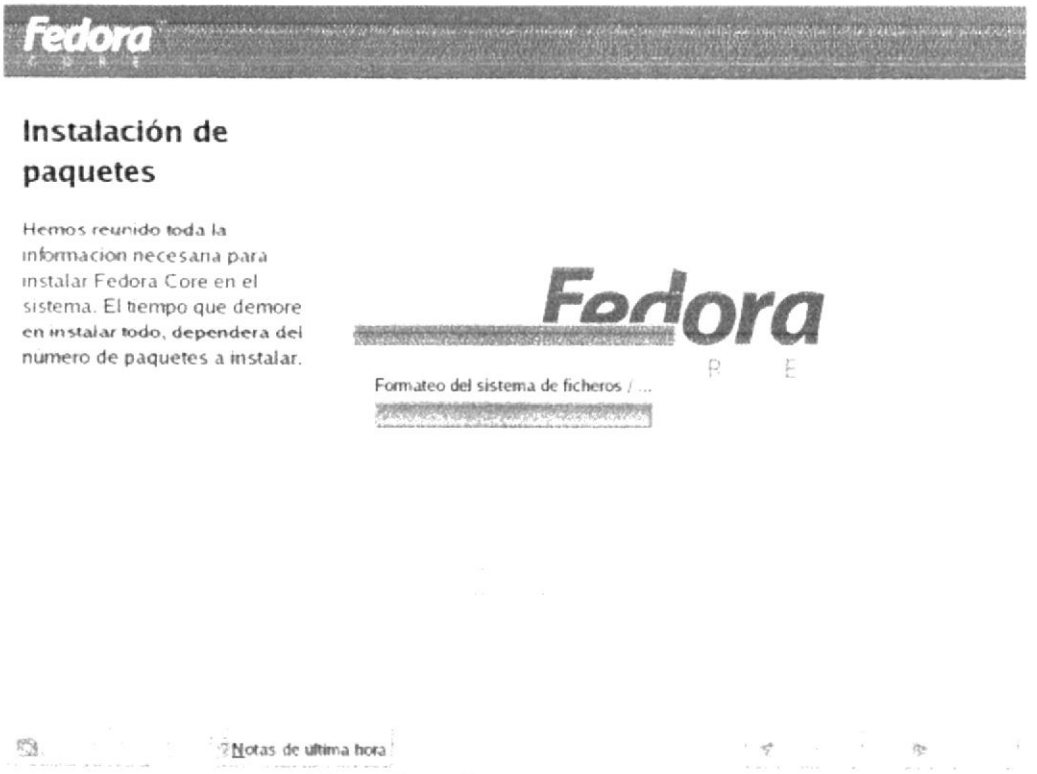


Figura 7-34: Formateando Ficheros

El asistente le muestra que ya se ha iniciado la instalación del sistema operativo Linux Fedora Core 3.

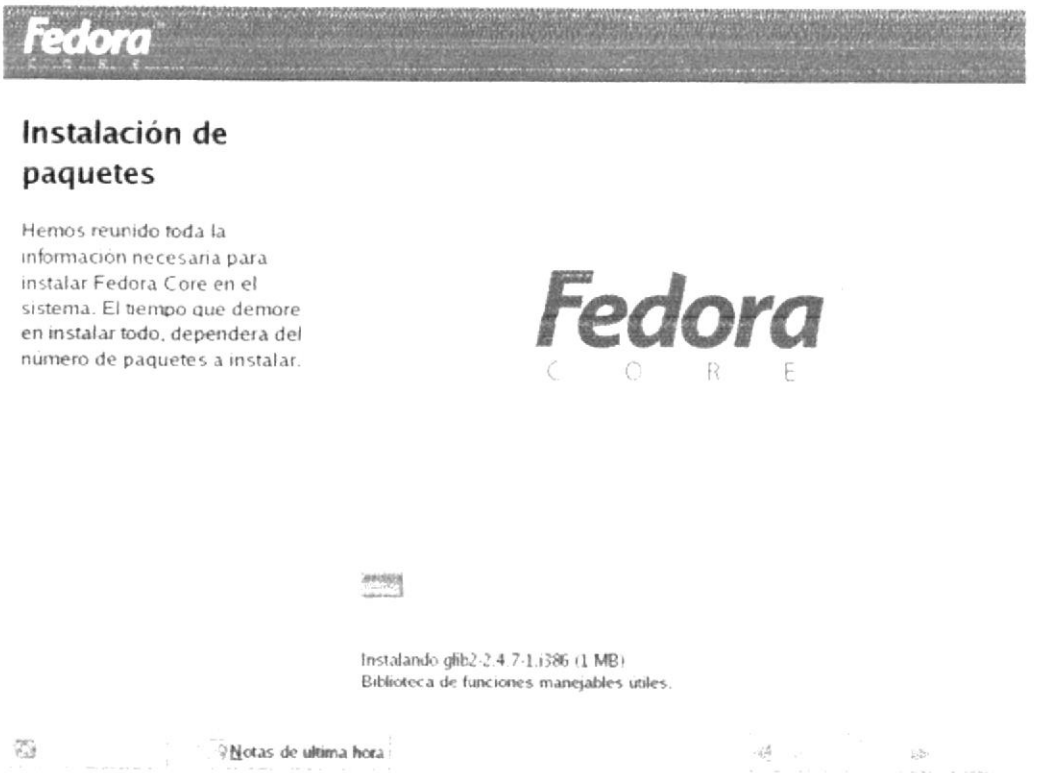


Figura 7-35: Instalando Paquetes

Continúa la secuencia de instalación del sistema operativo Linux Fedora Core 3.

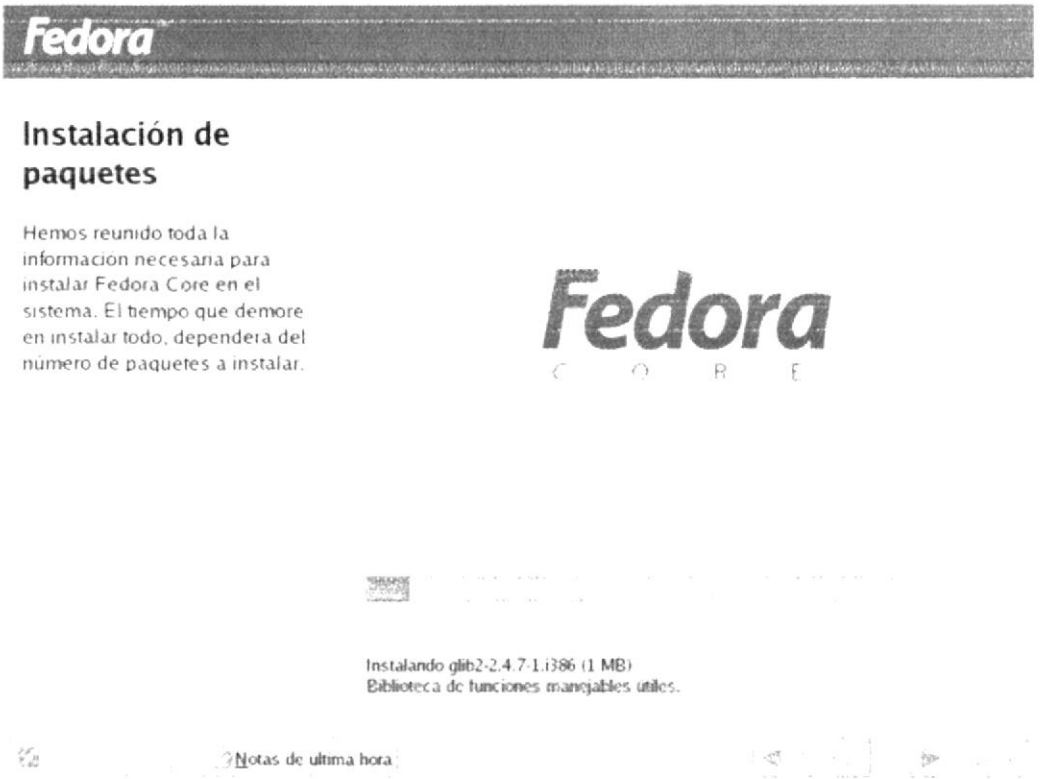


Figura 7-36: Secuencia de Instalación

El asistente le muestra una pantalla para que inserte el segundo disco de instalación necesario para continuar.

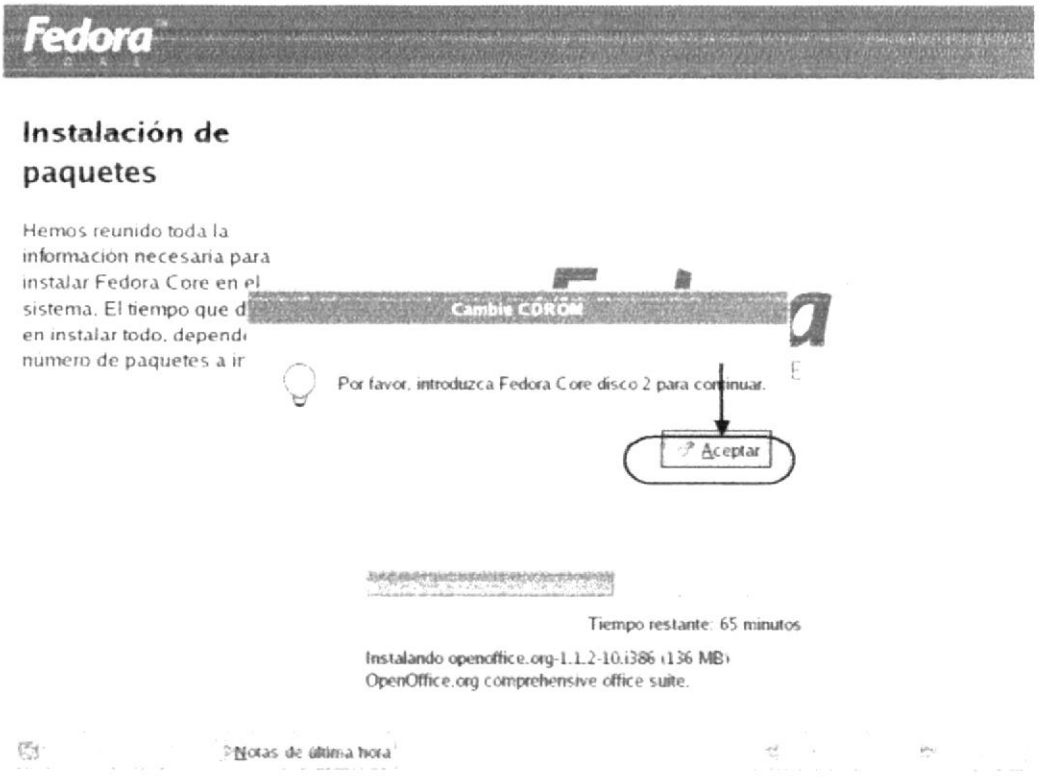


Figura 7-37: Insertando el Segundo Disco de Instalación

Continúa la secuencia de instalación, de las aplicaciones del sistema operativo.

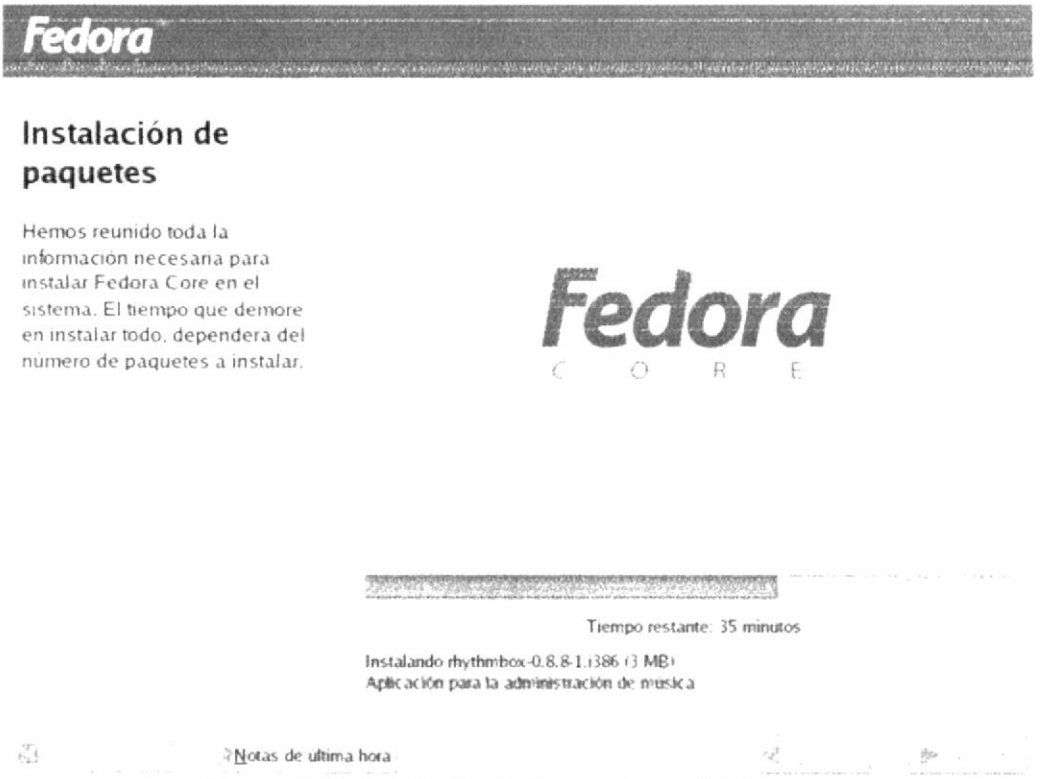


Figura 7-38: Instalación de Herramientas del Sistema

El asistente le indica que inserte el tercer disco de instalación, necesario para continuar.

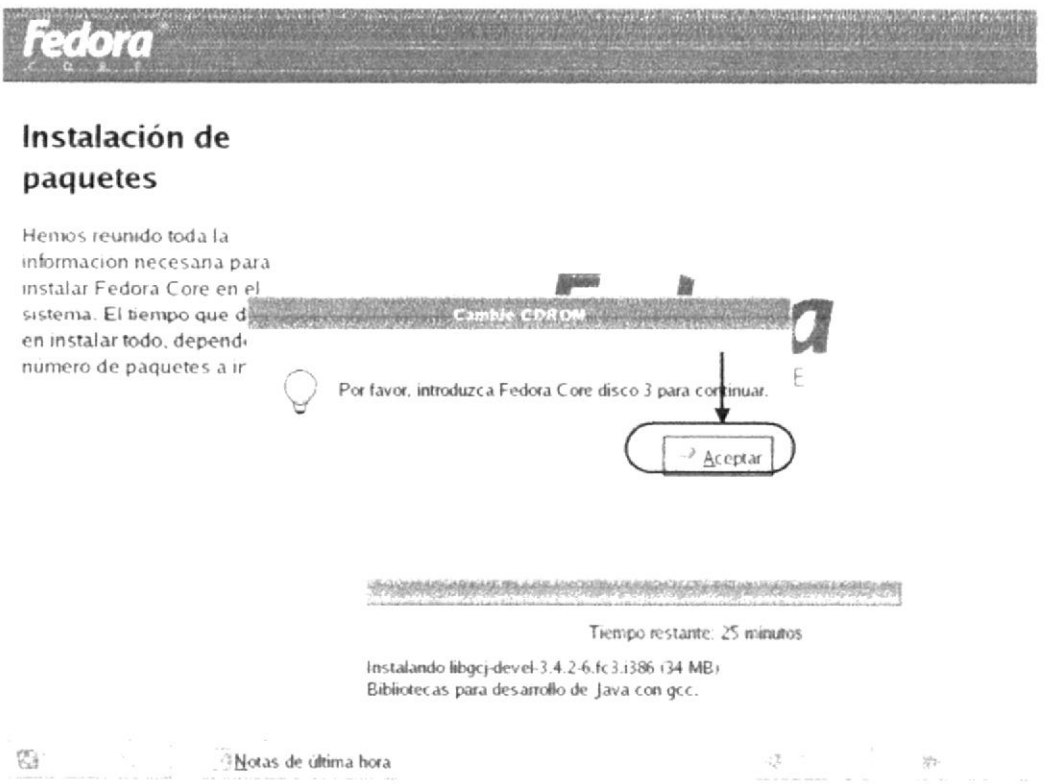


Figura 7-39: Insertando el Tercer Disco de Instalación

Luego de la instalación el asistente le pide retirar el disco y reiniciar el equipo.

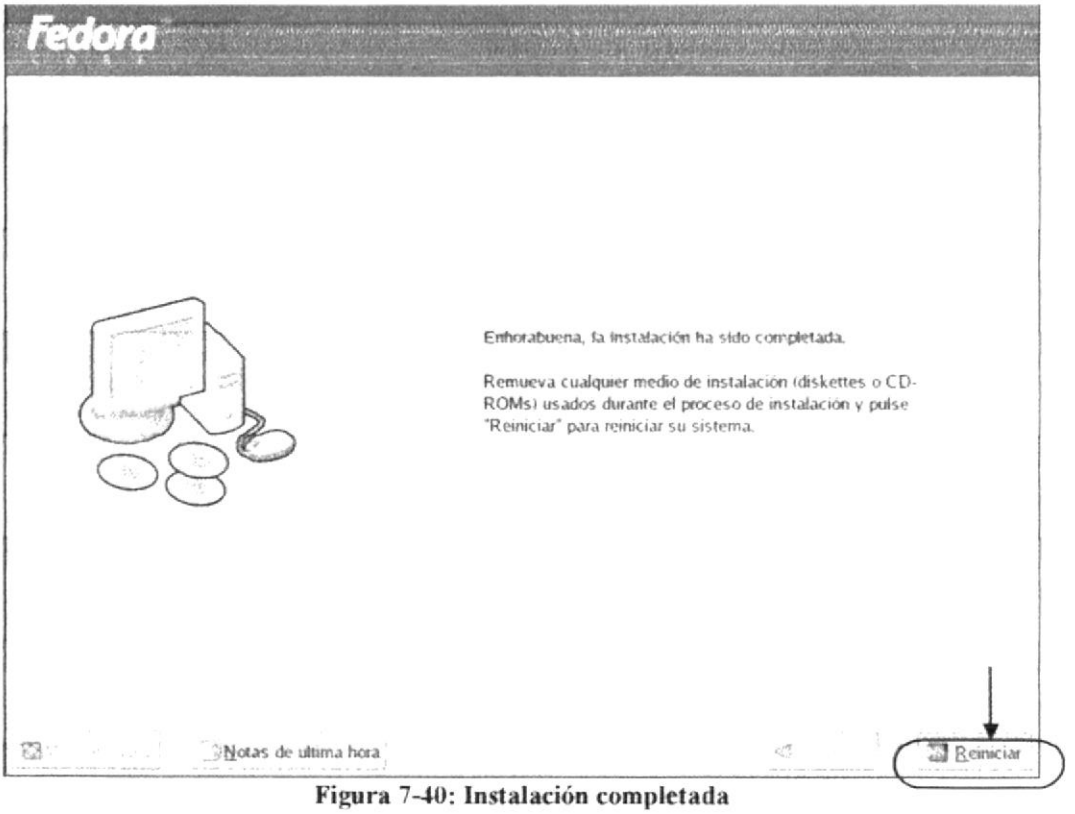


Figura 7-40: Instalación completada

7.5 CONFIGURACIÓN POST INSTALACIÓN DE LINUX

Una vez que la computadora, se haya reiniciado le mostrará una pantalla de bienvenida a Linux Fedora Core 3, de clic en siguiente para continuar.

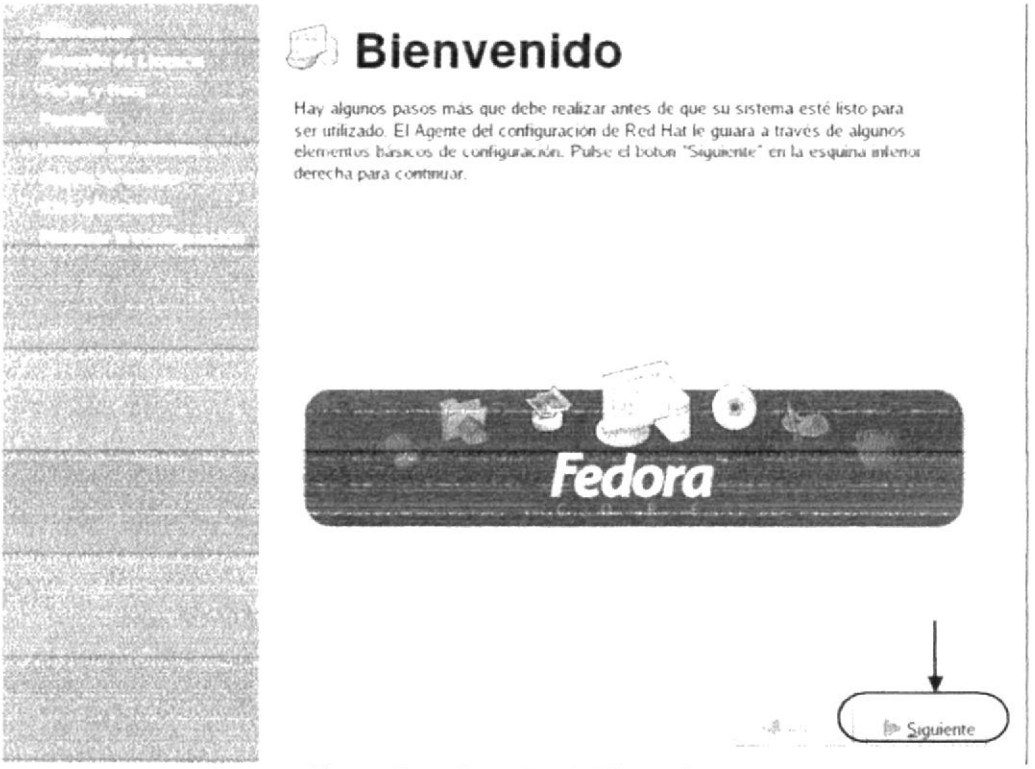


Figura 7-41: Pantalla de Bienvenida

En la siguiente pantalla le muestra el Acuerdo de Licencia, acepte las condiciones y luego de clic en Siguiente para continuar.

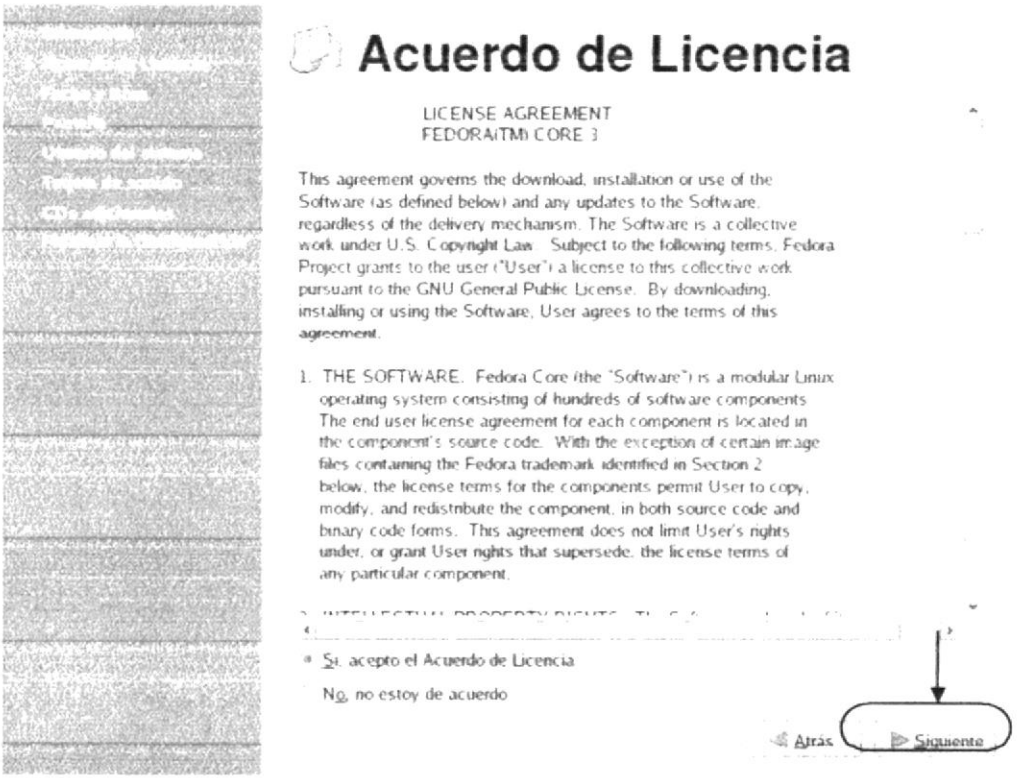


Figura 7-42: Acuerdo de Licencia

El asistente le da la opción de configurar la hora y fecha actual. De clic en Siguiente.

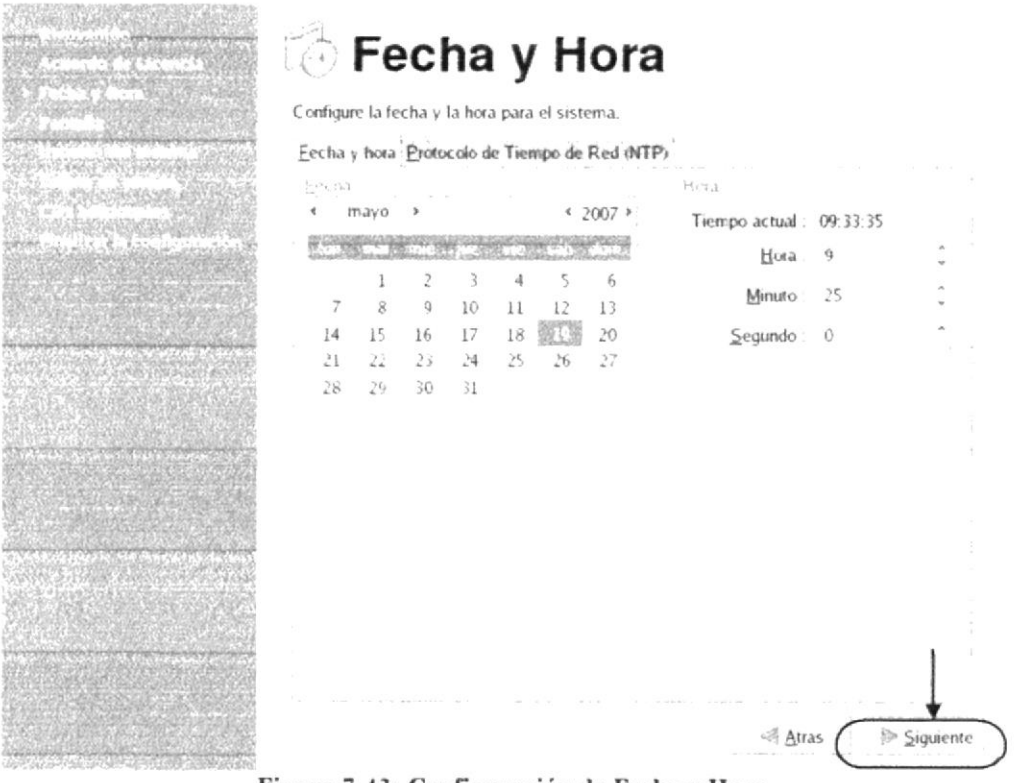


Figura 7-43: Configuración de Fecha y Hora

En esta pantalla el asistente le permitirá configurar la resolución de la pantalla.

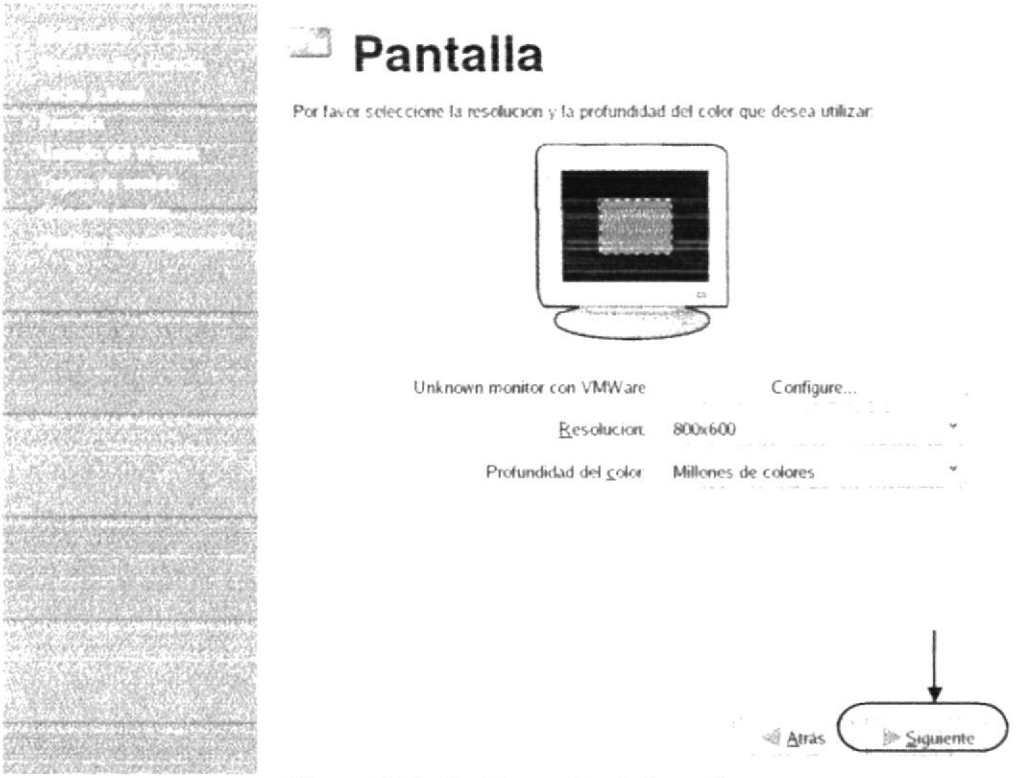


Figura 7-44: Configuración de Pantalla

Luego el asistente le muestra la pantalla de Usuario del Sistema, donde tiene opción a crear otro usuario aparte del Root, de clic en Siguiente para omitir el ingreso de otro usuario.

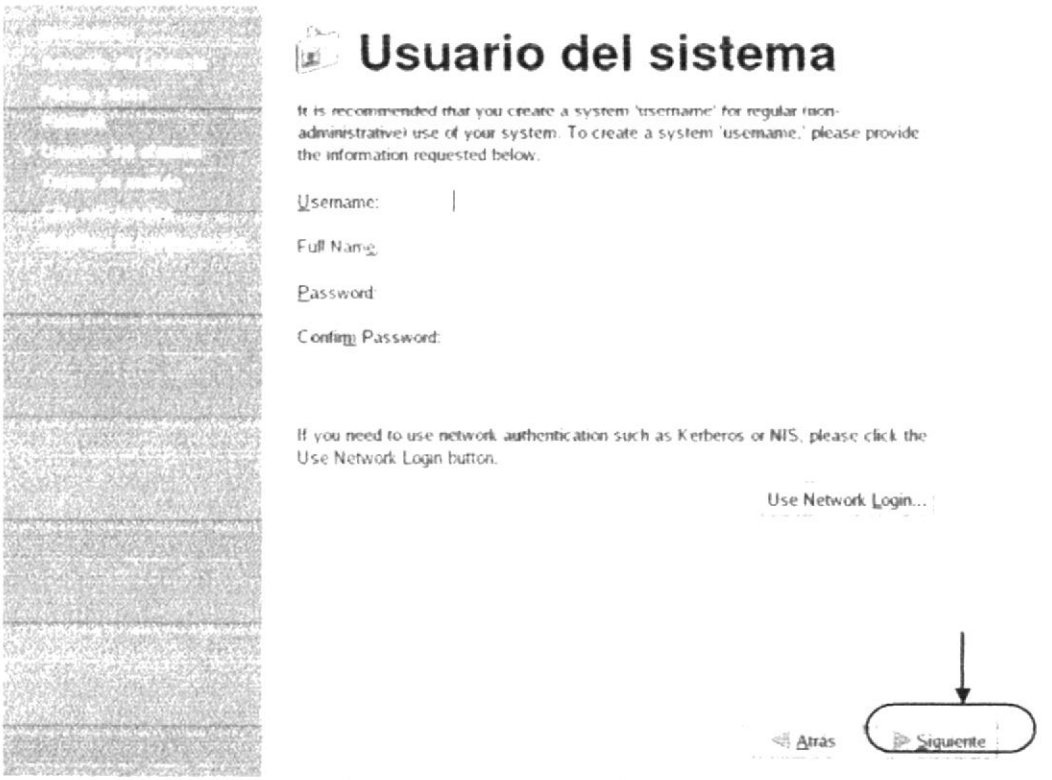


Figura 7-45: Usuario del Sistema

Luego el asistente le mostrará un mensaje de advertencia, que le indica que es muy recomendado que una cuenta del usuario personal sea creada. Si se continúa sin una cuenta, sólo puede anotar en la cuenta de la raíz que sólo es reservado para el uso administrativo. De clic en continuar

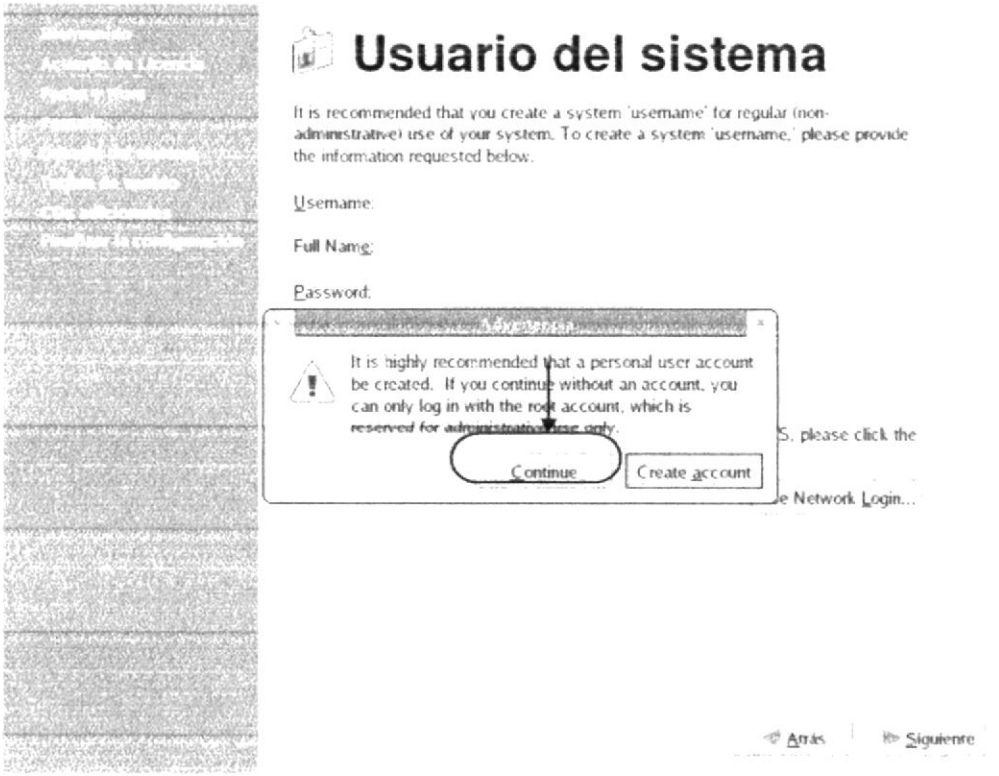


Figura 7-46: Advertencia al no crear un usuario

En esta pantalla el asistente le dará la opción de configurar la tarjeta de sonido, para continuar con la instalación de clic izquierdo en Siguiente.

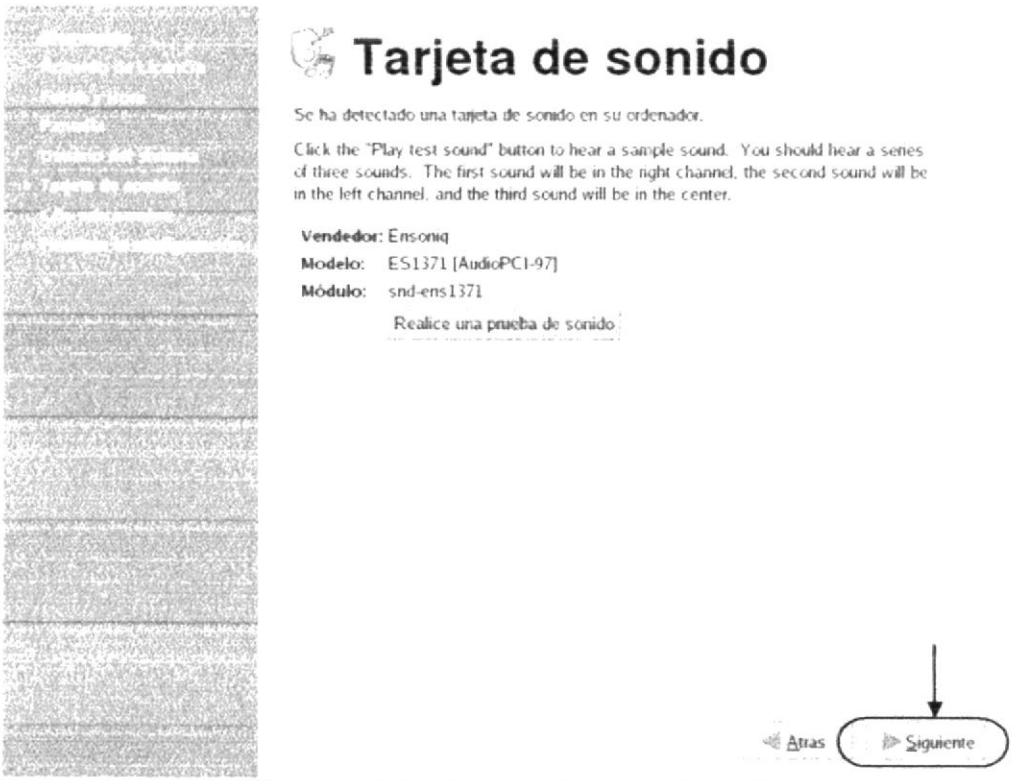


Figura 7-47: Configurando la tarjeta de sonido

En esta pantalla el asistente le preguntará si desea insertar un disco con software extra referente a la instalación de Linux Fedora Core 3, para continuar con la instalación de clic izquierdo en siguiente.

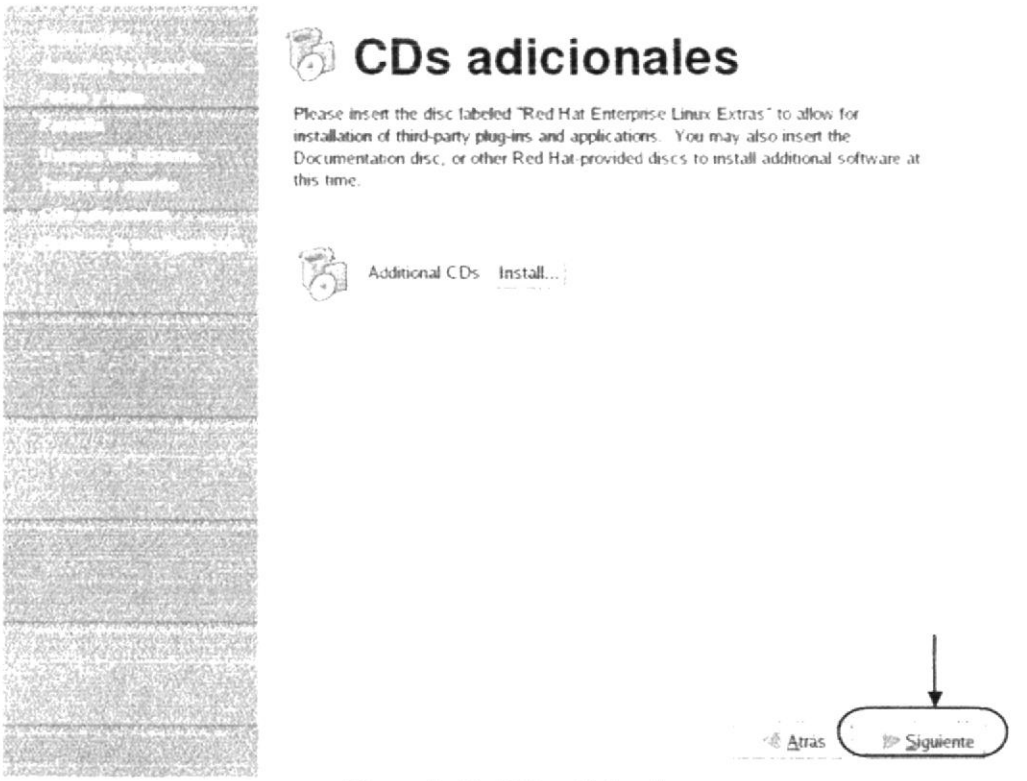


Figura 7-48: CD's adicionales

En esta pantalla el asistente le muestra la finalización de la post - configuración del sistema, para finalizar la instalación de Linux Fedora Core 3, de clic en siguiente.

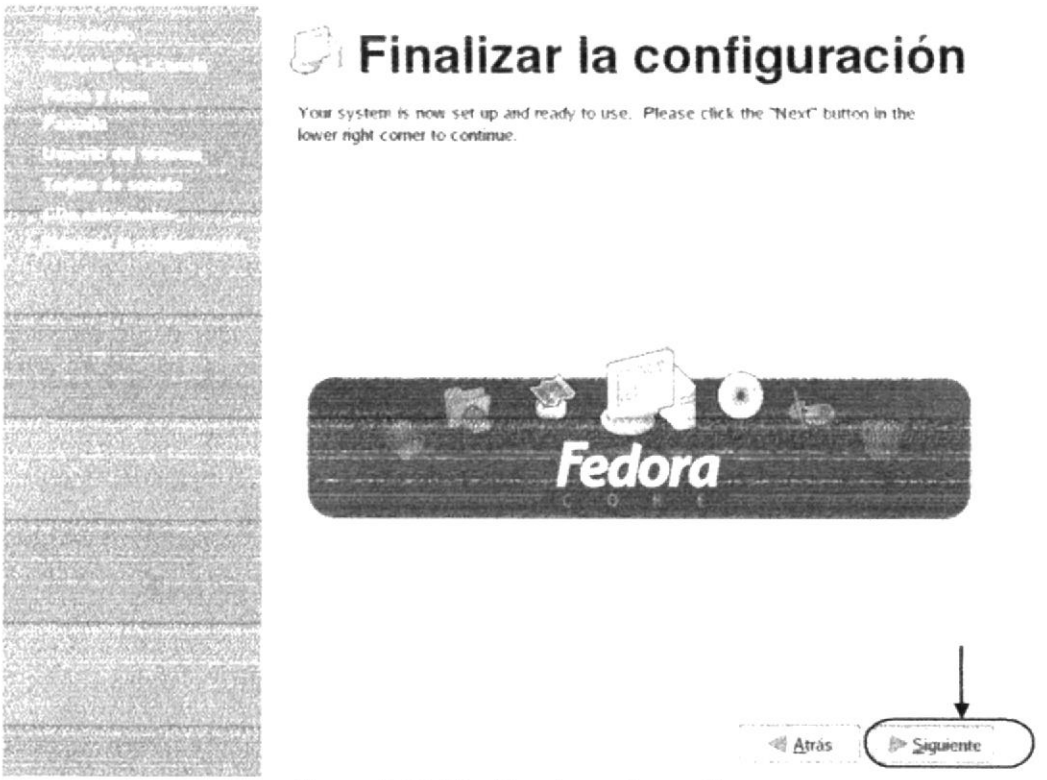


Figura 7-49: Finalizar la configuración

7.6 INICIALIZACIÓN DE LINUX FEDORA

7.6.1 MODO GRÁFICO

Luego de arrancar el sistema ingrese el nombre del usuario, en este caso ingrese como el administrador (root).

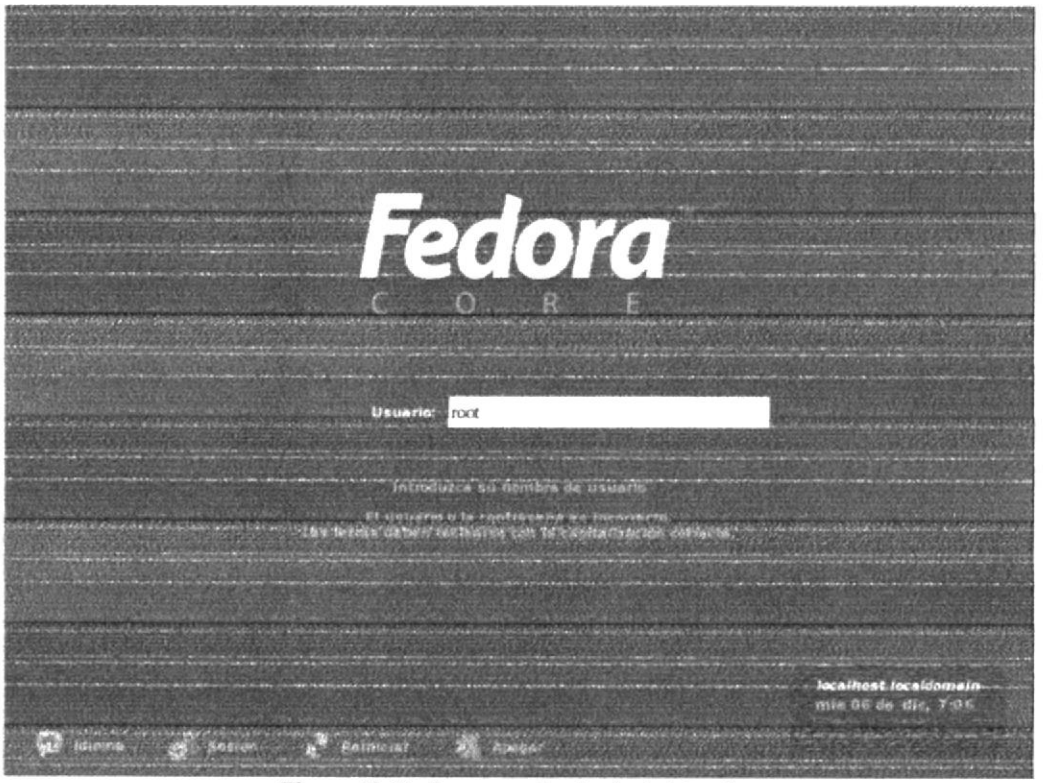


Figura 7-50: Ingresando el administrador

Luego Linux Fedora Core 3 le pide que ingrese la contraseña que le asigno durante la instalación (Tópico).

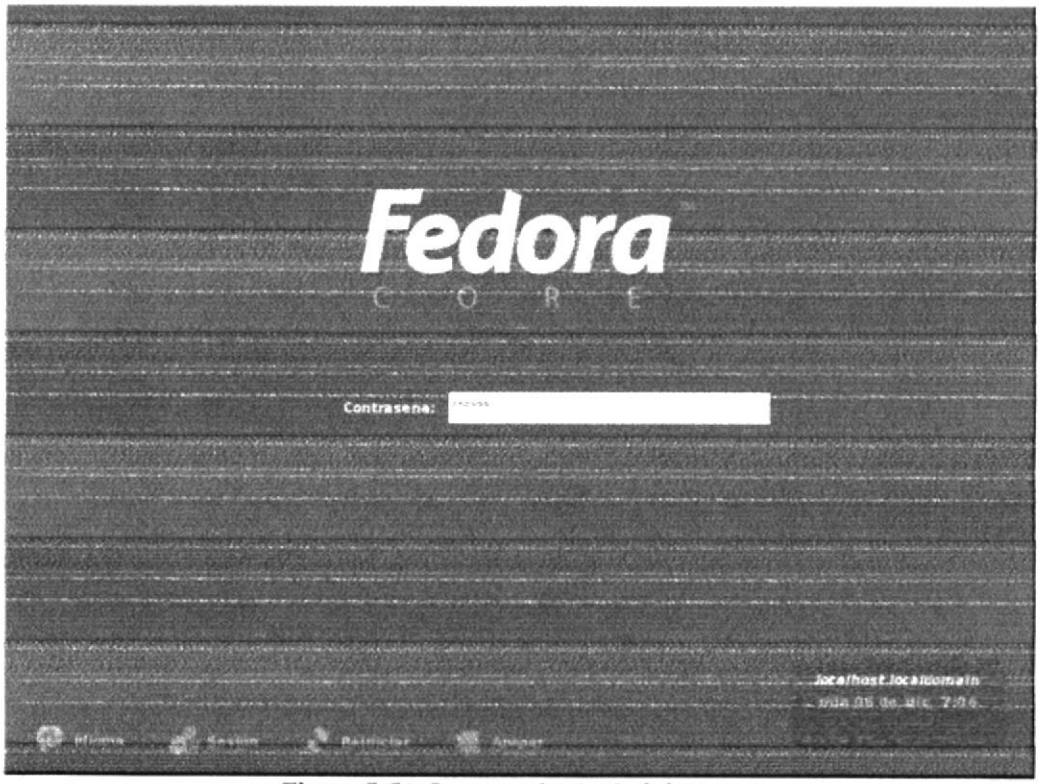


Figura 7-51: Ingresando el administrador

Luego de iniciar sesión mediante el administrador Linux le presenta su modo gráfico.

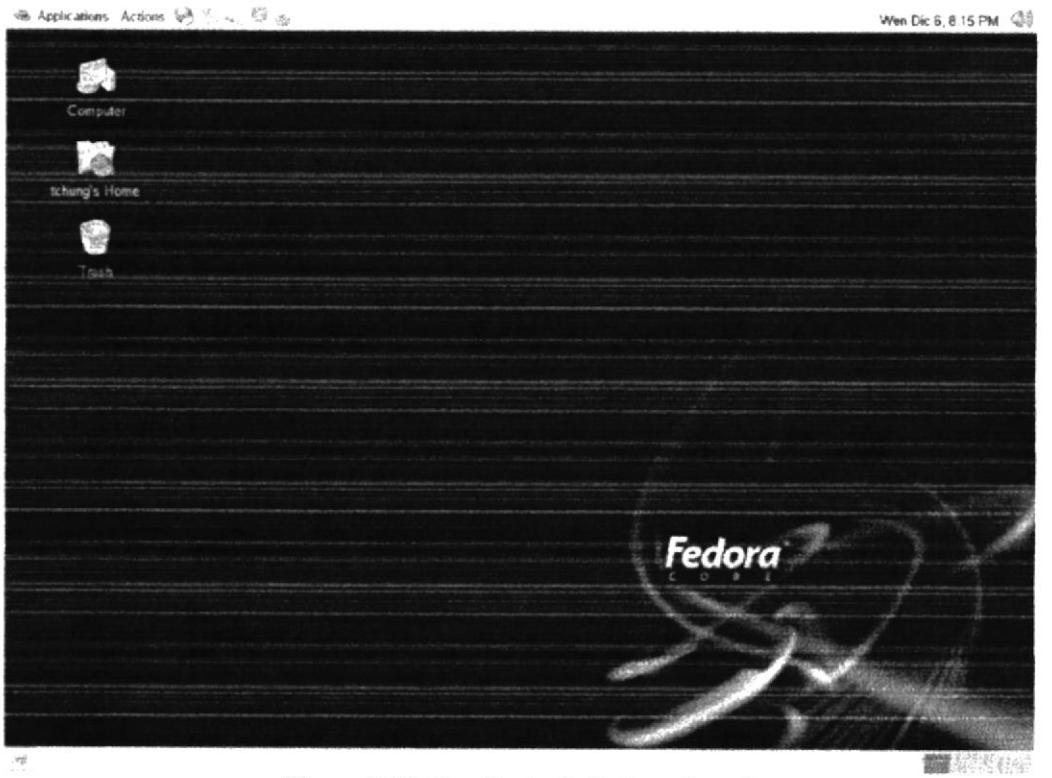


Figura 7-52: Escritorio de Fedora Core 3

Para abrir una Terminal de clic en Aplicaciones, herramientas de sistema y seleccione Terminal.

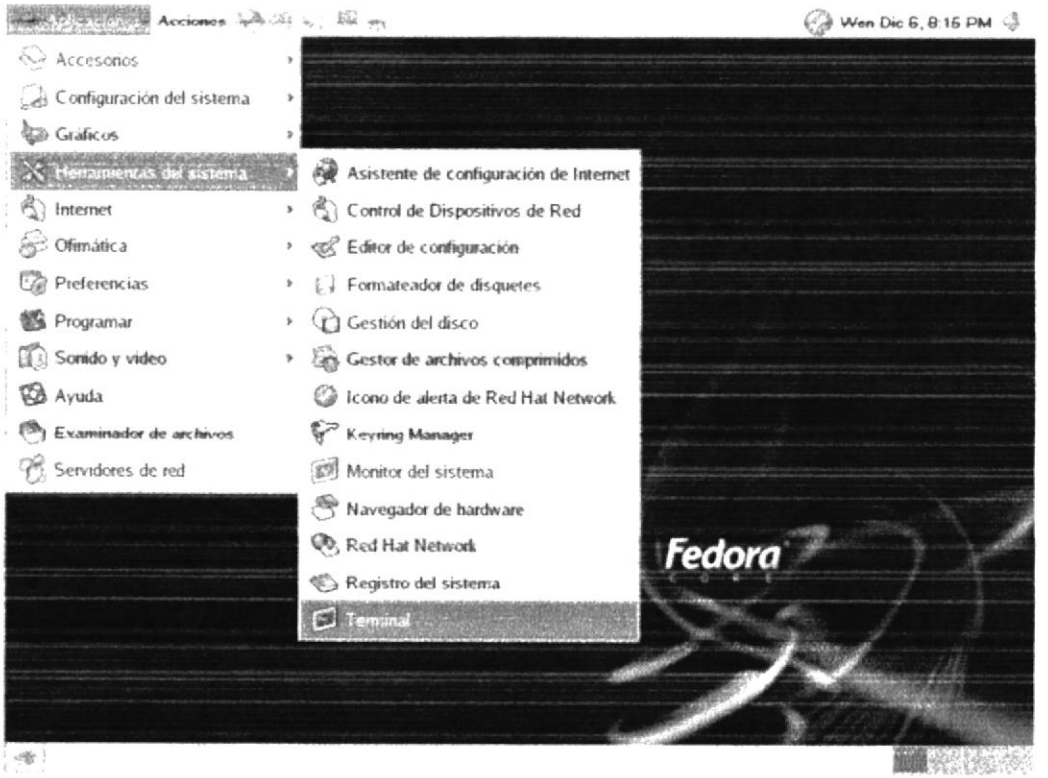


Figura 7-53: Abriendo el Terminal

7.6.2 MODO TEXTO

Para poder inicializar el sistema Operativo en modo texto, debe digitar la combinación de teclas Ctrl. + Alt. + F1 o en secuencia, hasta la tecla F6, ya que el Sistema operativo Linux Fedora Core 3, posee 6 consolas en modo texto.

Después de haber digitado la combinación de teclas para ingresar al Sistema Operativo en modo texto aparecerá una pantalla, en la cual le pedirá el usuario del localhost.

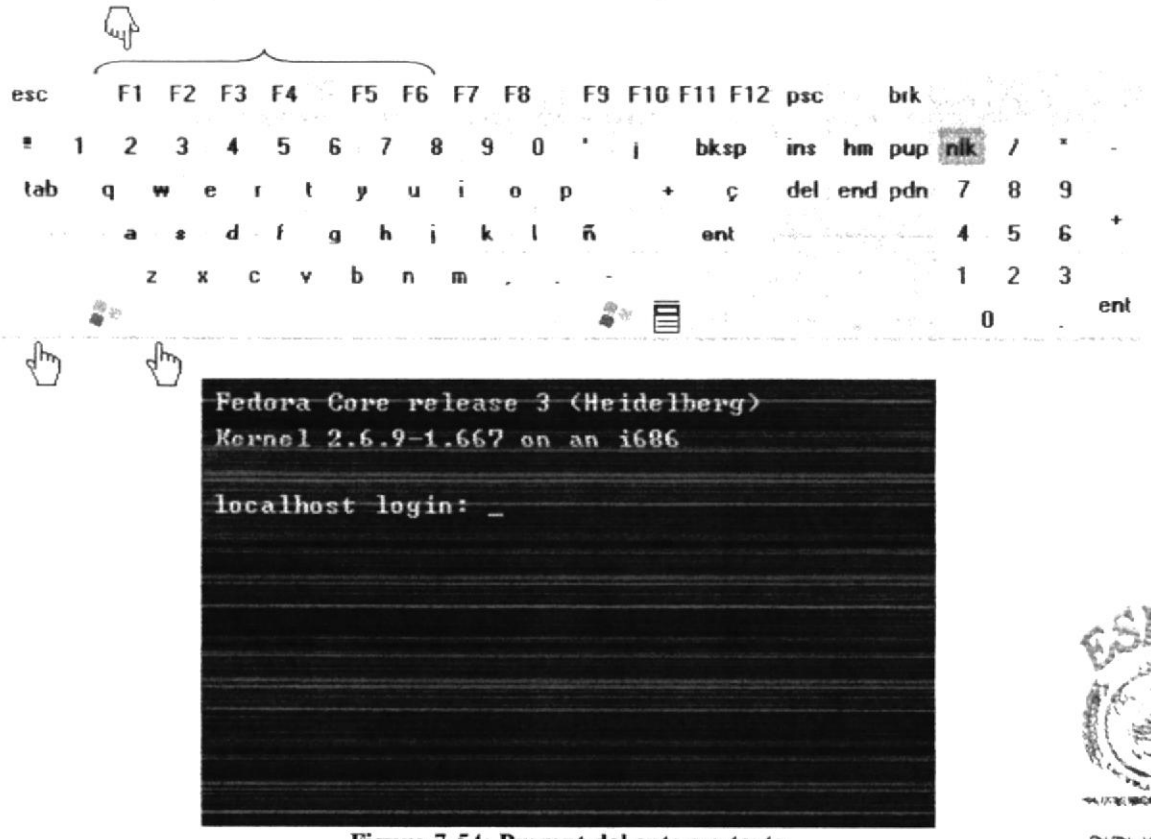


Figura 7-54: Prompt del entorno texto

Después ingrese el usuario root el cual es el usuario privilegiado.

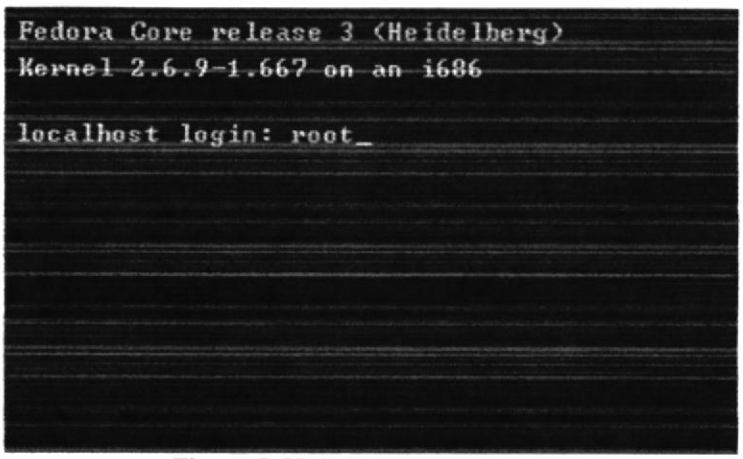


Figura 7-55: Ingresando el usuario

Luego le pide que ingrese la contraseña que le asigno al momento de la instalación.

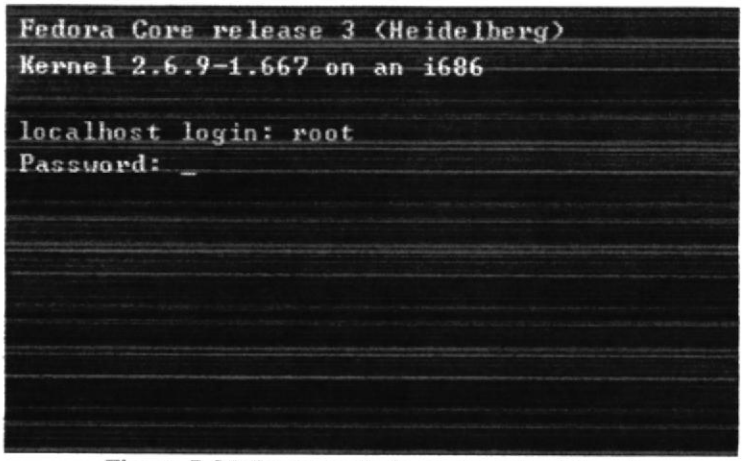


Figura 7-56: Ingresando la contraseña del root

Después de haber ingresado el password le aparecerá una pantalla, en la cual se puede visualizar que ya ingresó al Sistema Operativo Linux Fedora Core 3 en modo Texto.

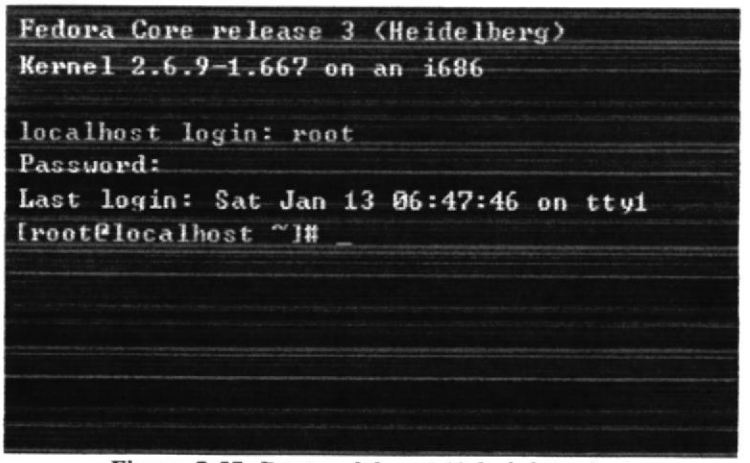


Figura 7-57: Dentro del root (Administrador)

7.7 COMANDOS BÁSICOS DE LINUX FEDORA CORE 3

Comando	Sintaxis	Descripción
adduser	**adduser** usuario	Permite crear un usuario
cat	**cat** etc	Es un comando simple, que muestra el contenido de un fichero mostrándolo por pantalla y sin ningún tipo de pausa. Un caso especial se produce cuando se ejecuta el comando cat sin parámetros. Entonces el comando se queda esperando a que se introduzcan caracteres por pantalla, mostrándolos linea a linea hasta que pulsa Ctrl-D.
cd	**cd** /etc	Ingresar a un directorio
chmod	**chmod** +777 documentos **chmod** +777 archivo.txt **chmod** → Comando + → Asignación 777 → Lectura, escritura y ejecución **archivo.txt** → Nombre del archivo	Este comando permite la asignación de permisos de lectura, escritura y ejecución a directorios y archivos
chown	**chown** user1: root archivo.txt	Comando para cambiar usuario, propietario o grupo de propietario
clear	**Clear**	Permite borrar pantalla
cp	**cp [-frivu]** archivo.txt /root/	Permite copiar ficheros y directorios
cp –f	**cp [–f]**	Sobrescribe el fichero destino
cp –i	**cp [–i]**	Pregunta al usuario si desea sobrescribir o no el archivo
cp –r	**cp [–r]**	Copia recursivamente directorios y subdirectorios
cp –u	**cp [–u]**	Solo sobrescribe si el fichero destino es más antiguo que el origen
cp –v	**cp [–v]**	Muestra por pantalla las operaciones que realiza el comando
date	**date**	Con el comando date se puede obtener la fecha actual. Si se le pasa una hora como parámetro, modificará la hora del sistema (sólo un usuario especial conocido como superusuario o root tiene permiso para cambiar la hora del sistema).

down	ifconfig eth0 192.168.12.1 **down** **ifconfig** → Configura la tarjeta de red. **eth0** → Nombre en Linux de la tarjeta de red **192.168.12.1** → Ip asignada **down** → Comando	Dar de baja a la tarjeta de red
fdformat	**fdformat** /dev/fd0	Formatear
find - name	**find – name** listado.txt	Nos permite buscar ficheros
find - size	**find – size 60k**	Permite buscar archivos que ocupan 60 Kilobytes a partir del directorio actual
gzip	**gzip** archivo.txt	Comprimir archivo
gunzip	**gunzip** archivo.txt	Permite descomprimir archivos compatibles con zip
home	**home**	Permite ver los directorios del usuario creados
ifconfig	**ifconfig**	Nos permite verificar la configuración de la tarjeta de red
less	**less** etc	Comando que permite visualizar el contenido de un fichero, haciendo pausas en su visualización.
ls	**ls**	Muestra el contenido de un directorio
ls –a	**ls –a**	Muestra todos los archivo, incluyendo los ocultos
ls –al	**ls –al**	Muestra los atributos de los archivos y directorios
ls –t	**ls –t**	Permite ordenar los archivos por fecha de modificación
mail	**mail**	Permite enviar y recibir correos electrónicos
man	**man**	Muestra la página del manual del comando o recurso
mkdir	**mkdir** documentos	Nos permite crear un directorio
more	**more** archivo.txt	Permite mostrar el contenido de los ficheros indicados por pantallas, puede usarse en combinación con otros comandos
mount	**mount** /dev/hd0/media/cdrom	Permite montar o tener acceso a las unidades de cdrom, diskettes y disco duros
mv	**mv** documentos/ etc	Permite mover o renombrar directorios
passwd	**passwd** usuario	Nos permite asignar contraseña a usuarios
ping	**ping** 192.168.12.1	Permite comprobar si existe acceso remoto a un host

pwd	**pwd**	Permite ver el directorio actual en el que se encuentra
reboot	**reboot**	Reiniciar
reload	service smb **reload**	Permite recargar un servicio sin detener su ejecución
restart	service smb **restart**	Permite reiniciar un servicio deteniendo su ejecución e inicializándolo otra vez
rm	**rm** archivo.txt **rm** → Comando **archivo.txt** → Nombre del directorio	Permite eliminar archivos
rmdir	**rmdir** documentos	Borra directorios que no tengan contenido
rmdir [- ri]	**rmdir [- ri]** documentos	Permite borrar directorios, una condición para que el comando funcione correctamente es que los directorios a eliminar estén vacios. Si no lo están, habrá que borrar los ficheros que contiene antes de borrar el directorio. Para borrar todos los directorios (vacios) se utiliza la opción –r con la opción –i entramos en el modo interactivo, el que se nos pregunta antes de eliminar cada directorio.
rm [- friv]	**rm [- friv]** archivo.txt	Comando que permite eliminar archivos. Hay que tener cuidado, aquí no existe una papelera de reciclaje. Lo que se borra se pierde, y no se puede recuperar de ninguna forma.
rm [- f]	**rm [- f]** archivo.txt	Fuerza la ejecución del comando, sin ningún tipo de pregunta
rm [- i]	**rm [- i]** archivo.txt	Pregunta si se desea eliminar el archivo
rm [- r]	**rm [- r]** archivo.txt	Actúa recursivamente el directorios y subdirectorios
rm [- v]	**rm [- v]** archivo.txt	Muestra la operación realizada
rpm –e	**rpm –e** samba	Sirve para desinstalar un paquete
rpm –i	**rpm –i** samba	Permite Instalar un paquete
rpm –q	**rpm –q** samba	Sirve para verificar si se encuentra instalados los paquetes
service	**service** smb start	Sirve para ver los estados de cualquiera de los servicios, en conjunto con otros comandos
start	service squid **start**	Permite iniciar un servicio
status	service network **status**	Muestra el estado actual de un servicio

startx	**startx**	Levantar modo gráfico
slocate	**slocate** /etc/listado.txt	Sirve para buscar archivos o directorios
stop	service xinetd **stop**	Permite detener un servicio
tar	**tar** cvf archivo.tar /etc	Permite empaquetar ficheros y crea un nuevo fichero de archivos
	tar xvf archivo.tar	Permite extraer los ficheros en el directorio actual
	tar czvf archivo.tar.gz /etc	Permite empaquetar y comprimir
telnet	**telnet** 192.168.12.1	Nos permite conectar de forma remota a cualquier computador especificando su dirección IP
touch	**touch** archivo.txt	Permite crear archivos con su respectiva extensión
umount	**umount** /media/cdrom	Desmontar disquete
up	ifconfig eth0 192.168.12.1 **up**	Asignar una dirección IP
updatedb	updatedb	Permite actualizar la base de dato de los archivos
userdel	**userdel** usuario_1	Sirve para borrar los usuarios creados
vi	**vi** archivo.txt	Nos permite editar el contenido de un archivo
	wq	Nos permite salir de un fichero y guarda los cambios realizados
	x	Nos permite salir de un archivo y guarda los cambios realizados
	yy 4	Nos permite copiar un número de específico de lineas, especificado con anterioridad.
	q!	Nos permite salir de un fichero sin guardar los cambios realizados
	p	Permite pegar las lineas copiadas
	i	Inserta, e indica al fichero que se comenzará a escribir en el
	dd	Borra Línea
	w	Permite solo guardar
	n	Permite movilizarse entre las palabras buscadas

Tabla 7-1: Comando Básicos en Linux

7.8 CONFIGURACIONES BÁSICAS EN LINUX FEDORA CORE 3

En esta pantalla se muestra el modo comando, donde puede realizar las diferentes configuraciones que necesite.

Figura 7-58: Modo Comando Fedora Core 3

Recomendación: Para realizar las diferentes configuraciones en Fedora Core 3, debe tener deshabilitado el Firewall y configurar la tarjeta de red.

7.8.1 DESHABILITAR EL FIREWALL

Para deshabilitar el firewall debe digitar el siguiente comando (setup).

Figura 7-59: Ingresando al Setup

Luego aparece la pantalla de herramientas del sistema donde debe seleccionar la opción de configuración de firewall y de clic en Ejecutar una herramienta o presione enter.

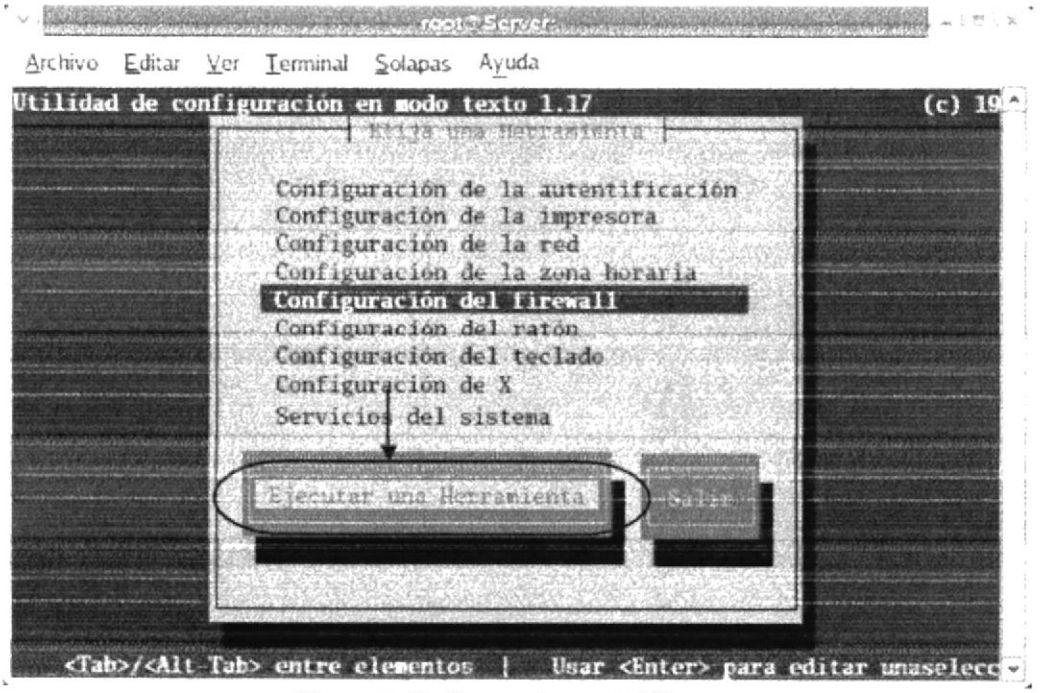


Figura 7-60: Herramientas del Sistema

Después aparece la pantalla de configuración de cortafuegos, aquí debe verificar si el nivel de seguridad se encuentra habilitado, para inhabilitarlo presione la barra espaciadora y presione enter o de clic en aceptar.

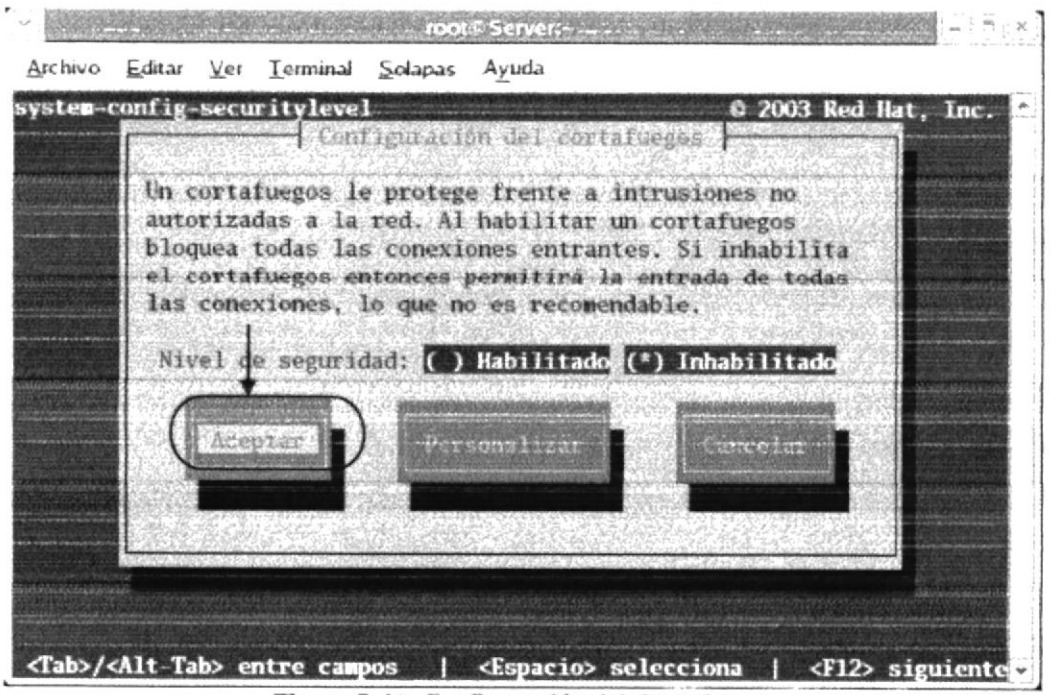


Figura 7-61: Configuración del Cortafuegos

Luego regrese al menú de herramientas y de clic en salir.

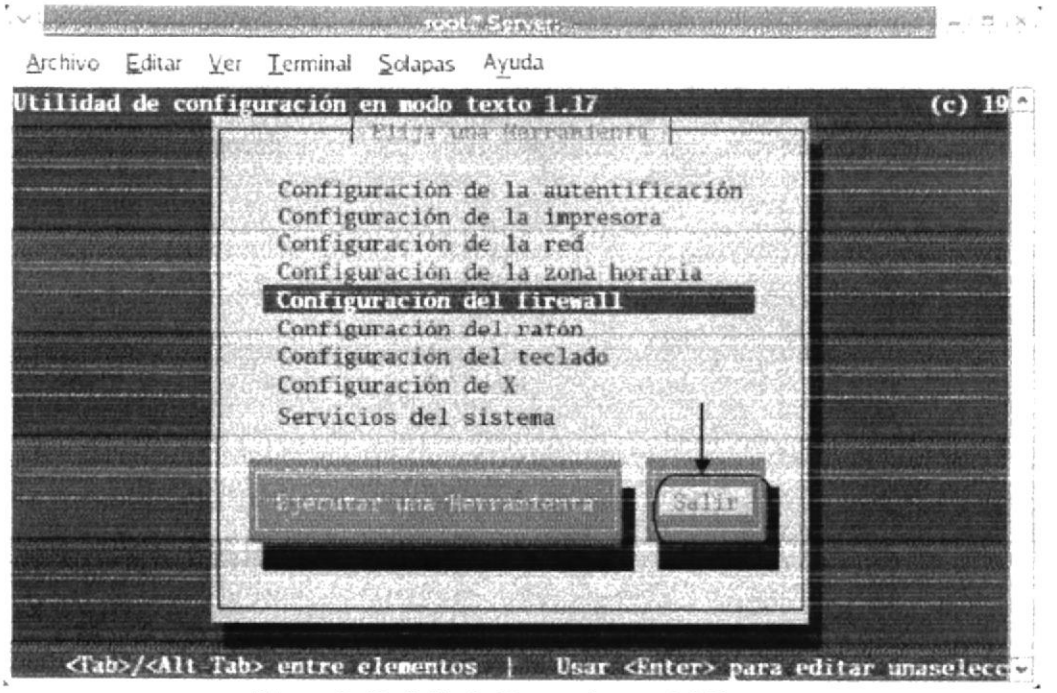


Figura 7-62: Salir de Herramientas del Sistema

7.8.2 CONFIGURACIÓN DE LA TARJETA DE RED

7.8.2.1 AMBIENTE GRÁFICO

Ingrese el comando netconfig, para configurar la tarjeta de red.

Figura 7-63: Usando el comando netconfig

Luego le muestra una pantalla donde le pregunta si desea configurar la red, seleccione la opción si.

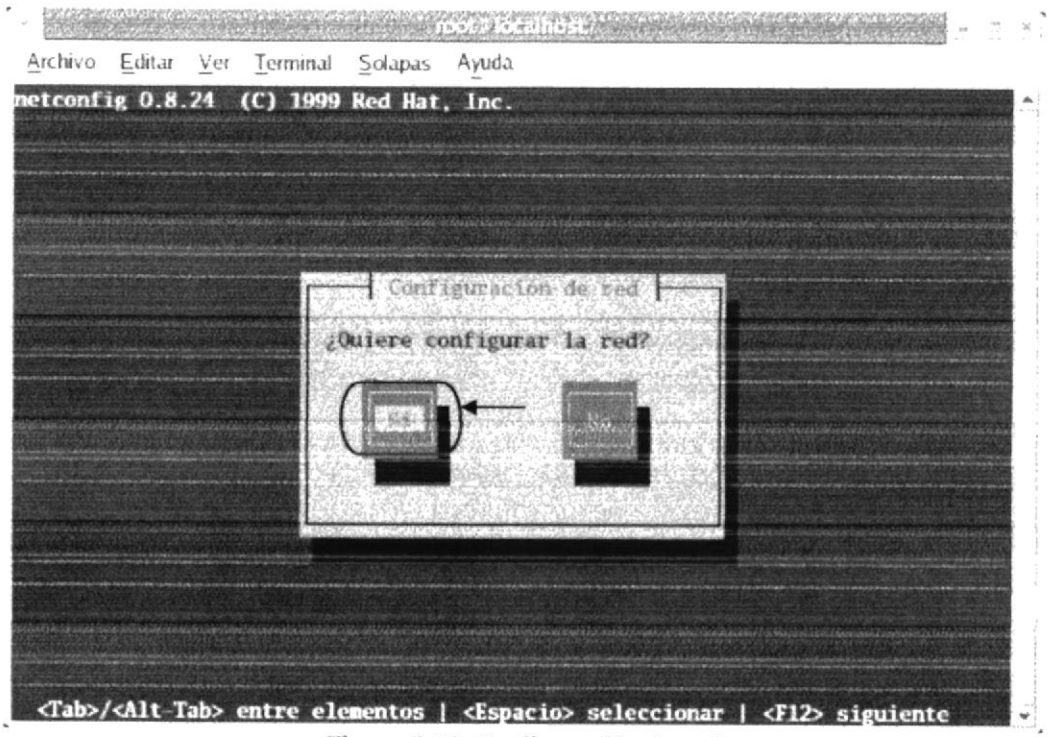


Figura 7-64: Configuración de red

Luego debe asignar una dirección Ip para la tarjeta de red, con su respectiva máscara de red, presione la tecla tabular y le debe aparecer automáticamente la puerta de enlace e ingrese la Ip del servidor DNS y presione Ok.

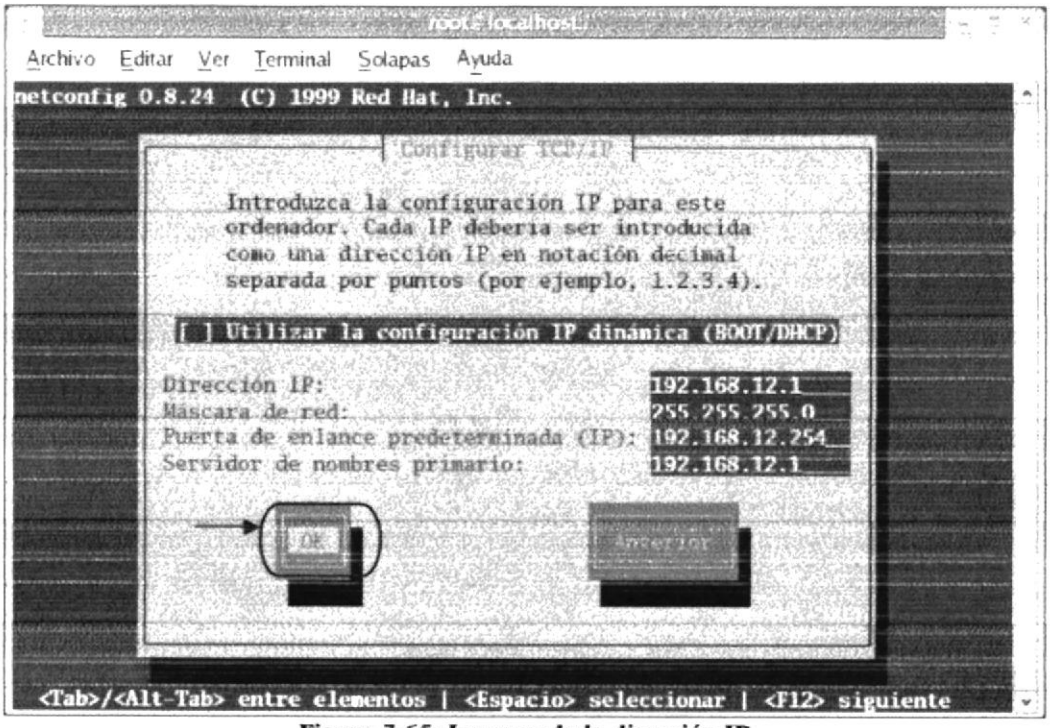


Figura 7-65: Ingresando la dirección IP

Luego que ingrese la dirección Ip con su respectiva máscara de red, verifique el estado de la tarjeta de red con el comando ifconfig.

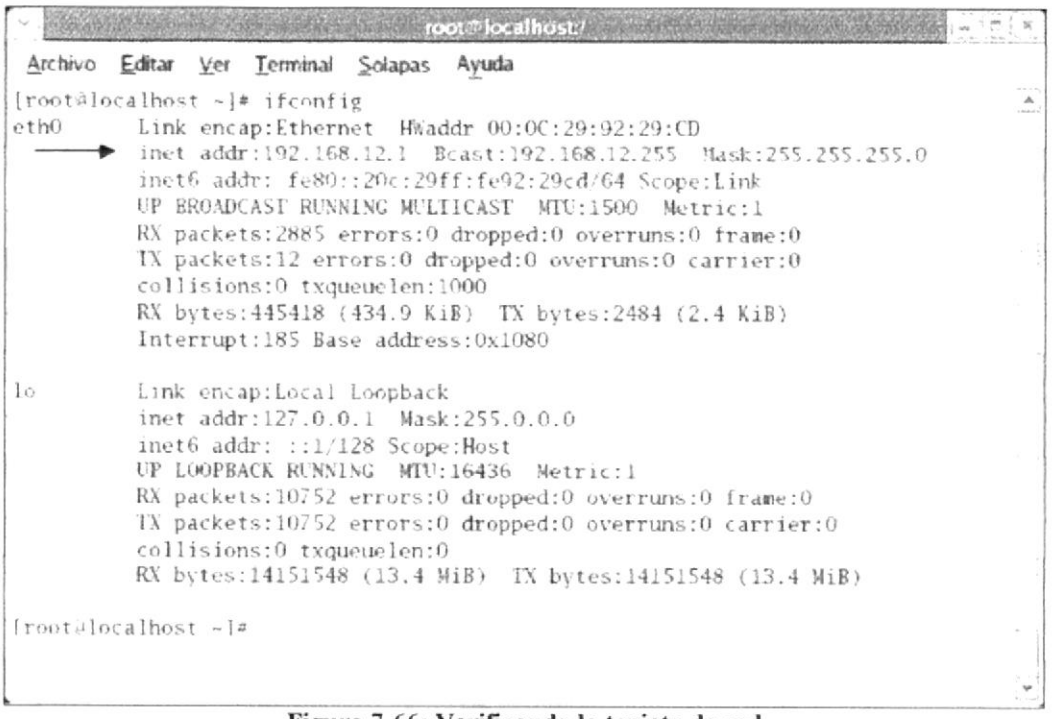


Figura 7-66: Verificando la tarjeta de red

7.8.2.2 AMBIENTE TEXTO

Para la asignación de una dirección IP a la tarjeta de red, ingrese el comando ifconfig.

Ej.: ifconfig eth0 192.168.12.1 up

ifconfig: Este comando sirve para asignarle una dirección IP a la tarjeta de red.
eth0: Es la representación de la tarjeta de red en Linux.
192.168.12.1: Dirección IP que se le asignará.
up: Permite levantar el servicio.

Figura 7-67: Usando el comando ifconfig

Para que la configuración tenga efecto debe ingresar el comando: service network restart

Figura 7-68: Reiniciando los servicios de la tarjeta de red

Luego de levantar la tarjeta de red asignándole una dirección IP, verifique su estado con el comando ifconfig.

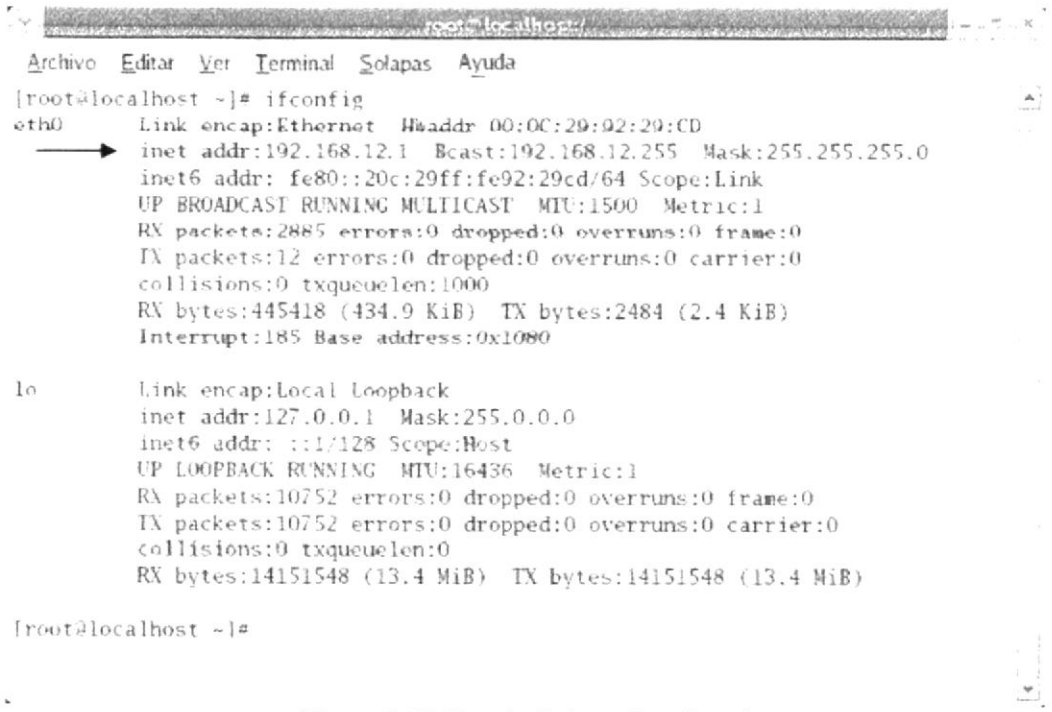


Figura 7-69: Estado de la tarjeta de red

7.9 SERVIDOR SAMBA

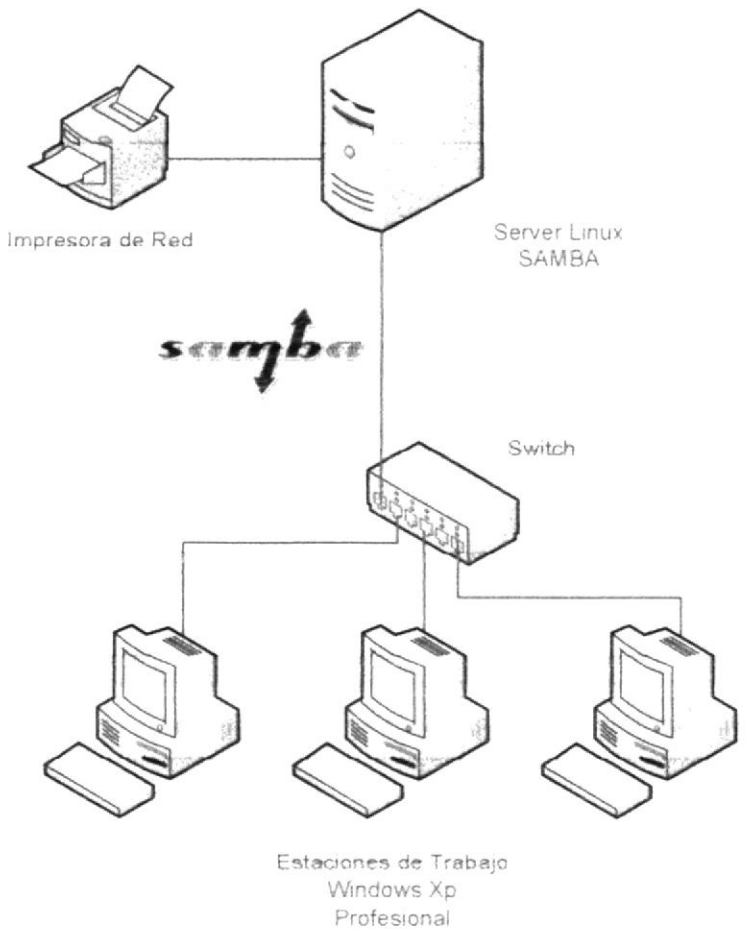


Figura 7-70: Samba Server

Samba es una suite de aplicaciones Unix que habla el protocolo SMB (Server Message Block). Muchos sistemas operativos, incluidos Windows y OS/2, usan SMB para operaciones de red cliente - servidor. Mediante el soporte de este protocolo, Samba permite a los servidores Unix entrar en acción, comunicando con el mismo protocolo de red que los productos de Microsoft Windows. De este modo, una máquina Unix con Samba puede enmascararse como servidor en su red Microsoft y ofrecer los siguientes servicios:

- Compartir uno o más sistemas de archivos.
- Compartir impresoras, instaladas tanto en el servidor como en los clientes.
- Ayudar a los clientes, con visualizador de Clientes de Red.
- Autentificar clientes contra un dominio Windows.
- Proporcionar o asistir con un servidor de resolución de nombres WINS.

Samba es la idea de Andrew Tridgell, quien actualmente lidera el equipo de desarrollo de Samba development desde su casa de Canberra, Australia. El proyecto nació en 1991 cuando Andrew creó un programa servidor de ficheros para su red local, que soportaba un raro protocolo DEC de Digital Pathworks. Aunque él no lo supo en ese momento, aquel protocolo más tarde se convertiría en SMB. Unos cuantos años después, él lo expandió como su servidor SMB particular y comenzó a distribuirlo como producto por Internet bajo el nombre de servidor SMB. Sin embargo, Andrew no pudo mantener ese nombre, ya que pertenecía como nombre de producto de otra compañía, así que intentó lo siguiente para buscarle un nuevo nombre desde Unix: grep -i 's.*m.*b' /usr/dict/words y la respuesta fue: salmonberry samba sawtimber scramble.

De ésta manera nació el nombre de Samba. Hoy, la suite Samba implica a un par de demonios que proporcionan recursos compartidos a clientes SMB sobre la red (las comparticiones son denominadas a veces también como servicios). Estos demonios son:

smbd
Un demonio que permite compartición de archivos e impresoras sobre una red SMB y proporciona autentificación y autorización de acceso para clientes SMB.

nmbd
Un demonio que busca a través del Windows Internet Name Service (WINS), y ayuda mediante un visualizador.

Samba se encuentra actualmente mantenido y es ampliado por un grupo de voluntarios bajo la supervisión activa de Andrew Tridgell. Al igual que el sistema operativo Linux, Samba es considerado por sus autores Open Source software (OSS), y es distribuido bajo la the GNU General Public License (GPL). Desde su concepción, el desarrollo de Samba ha sido patrocinado en parte por la Australian National University, donde Andrew Tridgell hizo su doctorado. En adición, algunas partes del desarrollo han sido patrocinadas por distribuidores independientes como Whistle and SGI. Es algo verdaderamente testimonial el que entidades tanto comerciales como no comerciales estén dispuestas a gastar dinero para dar soporte a un esfuerzo Open Source.

En el momento de la impresión de este libro, Andrew ha completado su trabajo de doctorado y ha pasado a formar parte de una compañía desarrolladora de Linux de San Francisco.

Microsoft también ha contribuido materialmente poniendo a disposición su definición de SMB y del Internet - savvy Common Internet File System (CIFS), como Public Request for Comments (RFC), y otros documentos estándar. El protocolo CIFS es el nuevo nombre de las futuras versiones del protocolo SMB que serán usadas en los productos Windows, los dos términos pueden ser usados aleatoriamente en éste libro, de hecho, se vera el protocolo escrito como "SMB/CIFS".

7.9.1 DEFINICIÓN

SMB (acrónimo de Server Message Block). La interconectividad entre un equipo con Linux instalado y el resto de los equipos en red en una oficina con alguna versión de Windows es importante, ya que esto permitirá compartir archivos e impresoras. Esta interconectividad se consigue exitosamente a través de SAMBA.

7.9.2 REQUERIMIENTOS PARA CONFIGURACIÓN DE UN SAMBA SERVER

- Debe tener instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Debe tener asignada una dirección IP estática.
- Debe tener inhabilitado el firewall de Linux.
- Haber instalado el paquete samba el cual se verifica con el comando rpm –qa samba.

7.9.2.1 ACTIVACIÓN AUTOMÁTICA DE LOS SERVICIOS SMB

1. Ingrese el comando setup, seleccione servicios del sistema y presione enter.

Figura 7-71: Servicios del Sistema

2. Active con la barra espaciadora los servicios smb y presione ok para guardar los cambios. Esta opción le permite que se activen los servicios smb, cada vez que se inicialice el sistema.

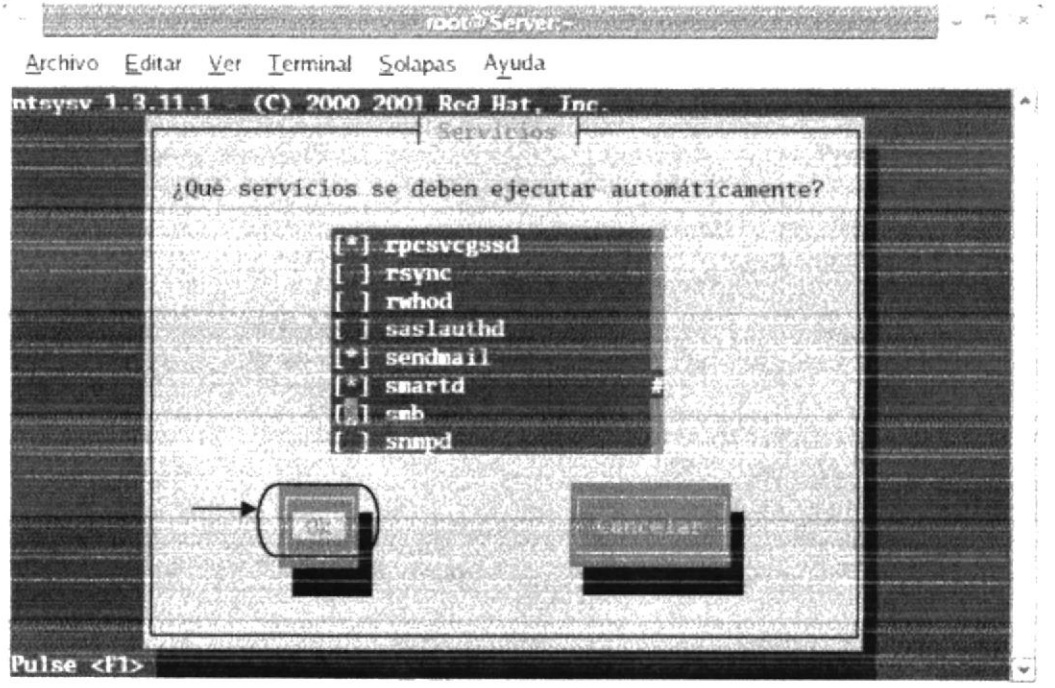


Figura 7-72: Servicio smb

7.9.3 CONFIGURACIÓN SAMBA

1. Verifique con el siguiente comando si se encuentra instalado el paquete Samba.
   rpm –qa samba

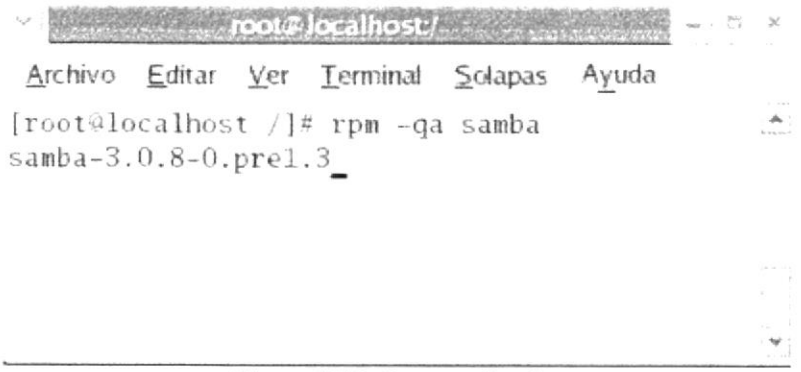


Figura 7-73: Paquete Samba

2. Edite el fichero de samba que se encuentra en el directorio /etc/samba con el nombre de smb.conf

Figura 7-74: Editando el Fichero de Samba

3. Dentro del archivo smb configure en el Global Settings (Escenas Globales) lo siguiente:

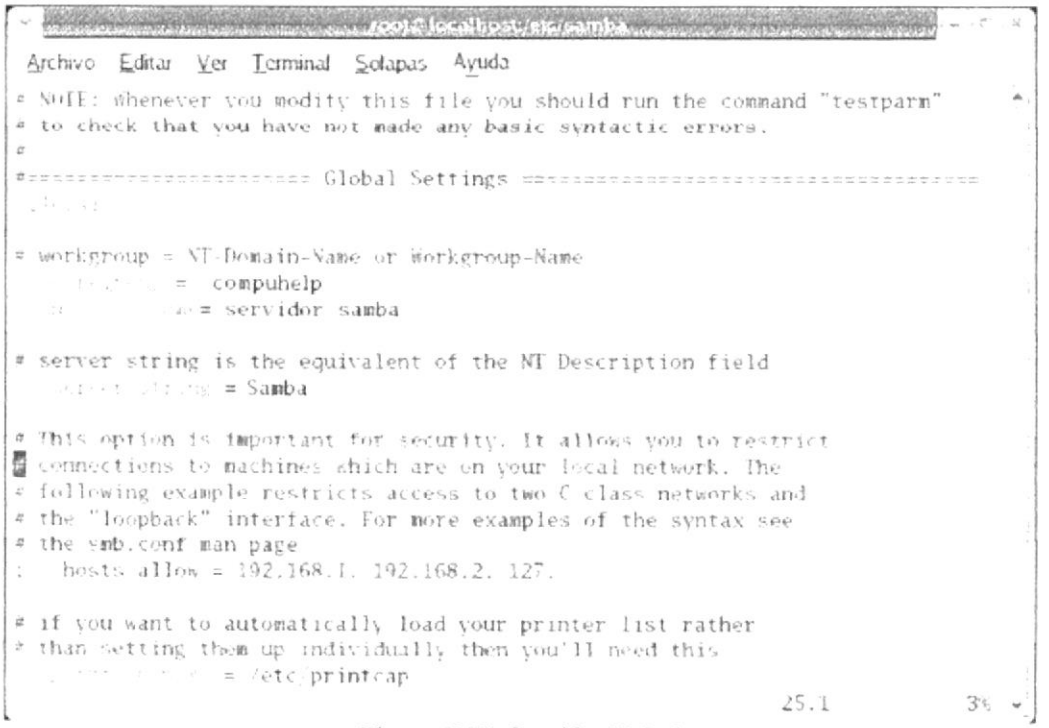


Figura 7-75: Sección Global

Global Settings

Las escenas globales contienen 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. Aquí también puede encontrar los modos de funcionamiento de Samba.

- **Workgroup,** permite asignarle el nombre del grupo de trabajo del servidor Samba.

  workgroup = compuhelp (Grupo de trabajo)

- **Netbios name,** esta línea la debe agregar, esto le permite definir el nombre de su servidor.

  netbios name = servidor samba (Descripción del servidor)

- **Server String,** permite agregarle un comentario para que reconozca su servidor entre las estaciones de trabajo Windows.

  server string = Samba (Comentario del Servidor)

- **Hosts allow,** permite el control de acceso a los recursos de ciertas máquinas.

  host allow = [registrar las ip de las pc]

4. Busque la sección Share definitions, edite las líneas como se indica en el gráfico y guarde los cambios con el comando (:wq).

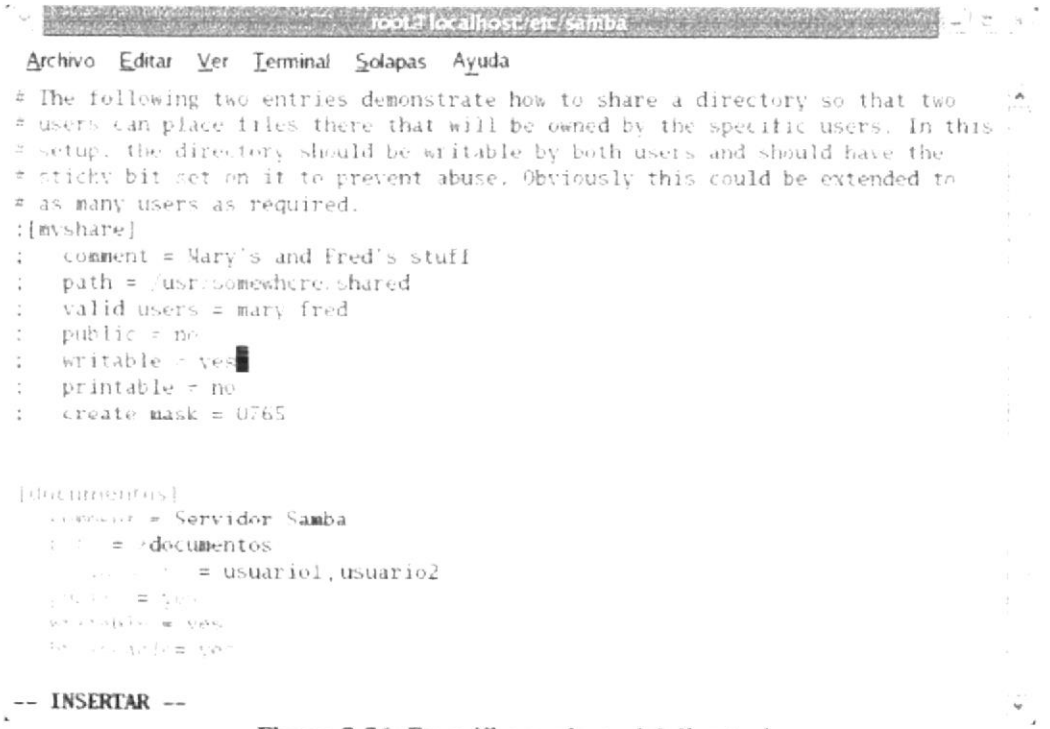


Figura 7-76: Especificar valores del directorio

La sección **Share definitions** contiene la lista de particiones de disco efectuadas por la máquina. Se aconseja primero crear la partición compartida y después precisar para cada partición sus propiedades particulares.

- **comment**, permite que agregue un comentario a su servidor samba.

  comment = Servidor Samba

- **Path**, permite definir el directorio que va a compartir.

  Path = / documentos

- **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, se podrá añadir la línea:

  valid users = usuario1, usuario2

- **public**, indica si desea poner su servidor como público.

  public = yes

- **Writable**, indica que este recurso debe ser anunciado por nmbd, y por tanto debe tener permiso de escritura para todos los usuarios.

  writable = yes

- **Browseable**, indica que este recurso debe ser anunciado por nmbd, y por tanto ser visible para todos los usuarios.

  browseable = yes

5. Cree el directorio con el nombre que le asignó en la configuración del archivo smb, con el comando (mkdir)

Figura 7-77: Crear Directorio

6. Con el comando touch creamos un archivo de tipo texto para realizar una prueba de acceso desde una estación de trabajo conectada previamente al servidor samba.

- **[root@localhost /]# cd** → Ingrese a un directorio.

Cd /documento

- **[root@localhost /]# touch** → Cree un archivo

Touch archivo.txt (crear un archivo de tipo texto)

- **[root@localhost /]# ls** → Verifique los archivos que se encuentran dentro del directorio.

Ls (Enlista el contenido de un directorio)

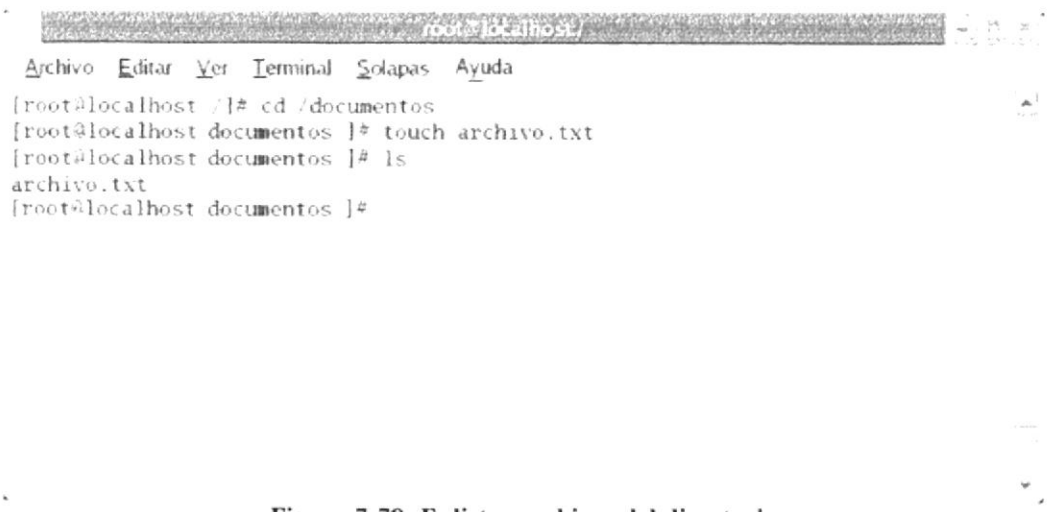


Figura 7-78: Enlistar archivos del directorio

7. Asígnele los permisos de lectura y escritura, tanto al directorio como al archivo de tipo texto.

Los permisos en chmod, utilizan los dígitos del 0-7. La representación es la suma de los permisos y el número resultante va a ser de 4 dígitos.

r = 4
w = 2
x= 1

Ejemplo: Representar rwx - - r-x - - r -- (rwxr-xr--)

400	Lectura por parte del dueño
200	Escritura por parte del dueño
100	Ejecución por parte del dueño
040	Lectura por parte del grupo
010	Ejecución por parte del grupo
004	Lectura por otros
754	RESULTADO

Octal	Propietario	Grupo	Otros	Completo
Número	Columna 1	Columna 2	Columna 3	Código
777	rwx	rwx	rwx	rwxrwxrwx
755	rwx	r-x	r-x	rwxr-xr-x
700	rwx	---	---	rwx------
666	rw-	rw-	rw-	rw-rw-rw-

Tabla 7-2: Permisos de Lectura, escritura y ejecución

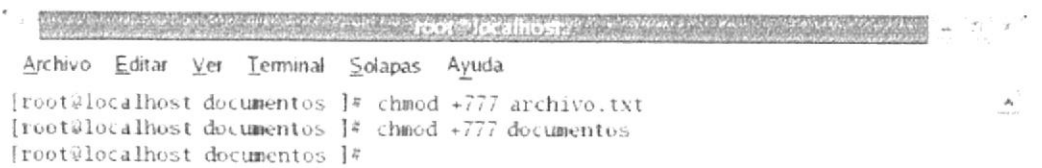


Figura 7-79: Asignación de Permisos

7.9.3.1 CREACIÓN DE USUARIO PARA SAMBA

8. Después cree el usuario con el nombre que le asignó en la configuración del archivo smb, para que desde una estación de trabajo Windows se pueda acceder al directorio creado. Luego de crear el usuario asígnele una contraseña.

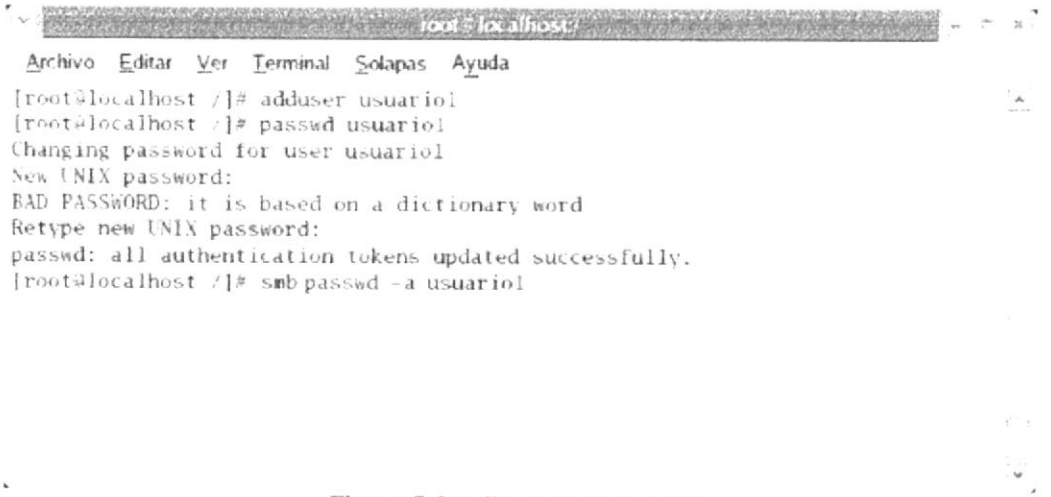


Figura 7-80: Creando un Usuario

- Cree los usuarios que anteriormente se registraron en valid user.

  adduser usuario1

- Asigne una contraseña para el usuario creado.

  passwd usuario1

- Asignele una contraseña para los usuarios para que puedan hacer uso del servicio de samba.

  smb passwd –a usuario1

9. Inicie los servicios de samba.

- Service smb start

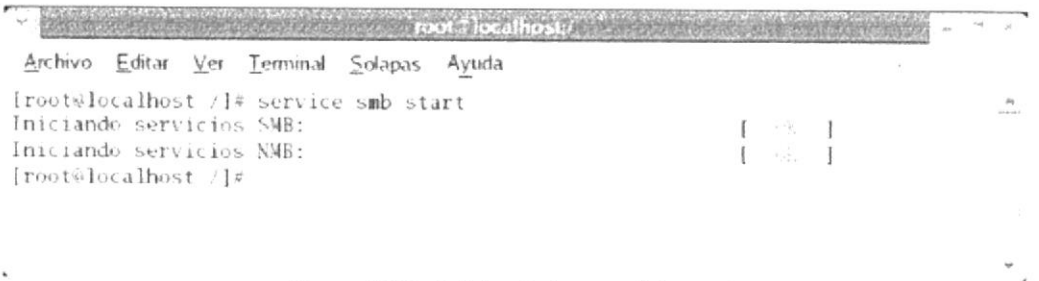


Figura 7-81: Iniciando los servicios smb

7.9.4 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. De clic derecho en mis sitios de red y de clic en propiedades.

Figura 7-82: Propiedades de Windows

2. De clic derecho en conexión de área local y de clic en propiedades.

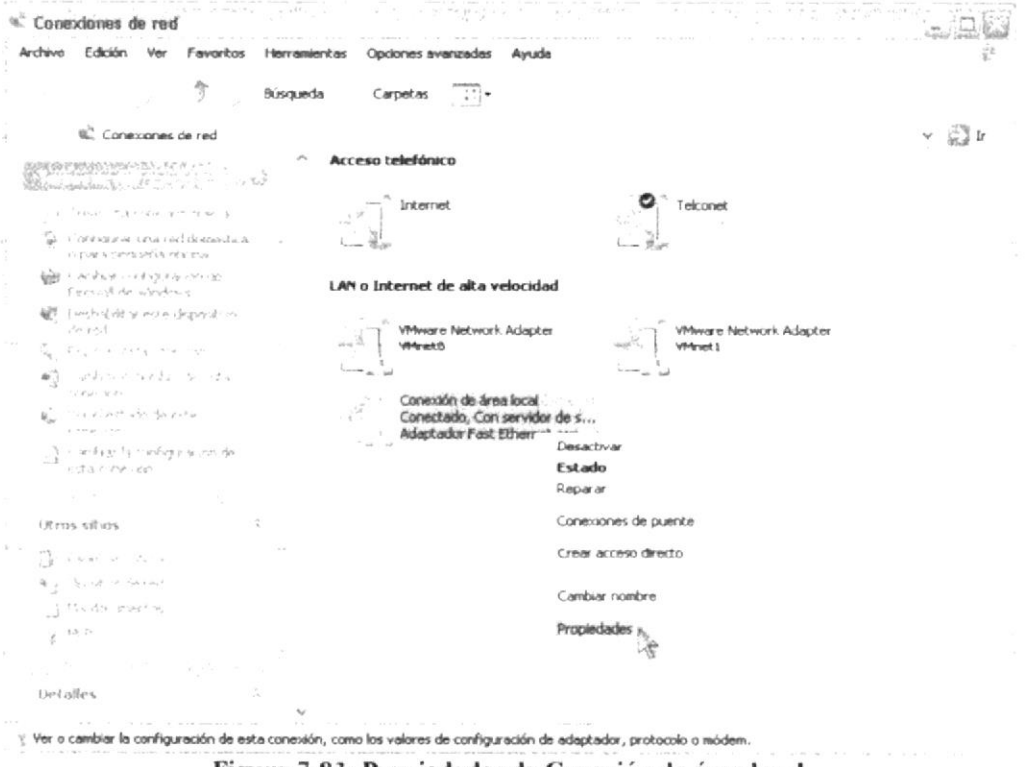


Figura 7-83: Propiedades de Conexión de área local

3. Seleccione el ítem Protocolo Internet TCP/IP y de clic en propiedades.

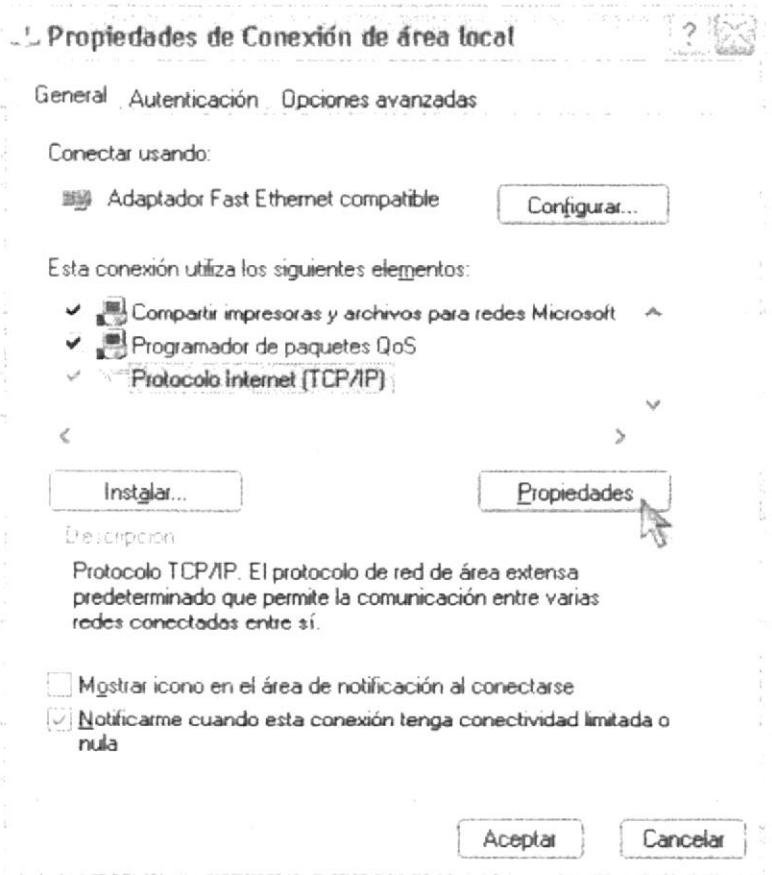


Figura 7-84: Protocolo TCP/IP

4. Luego asígnele una dirección Ip a su máquina y de clic en aceptar.

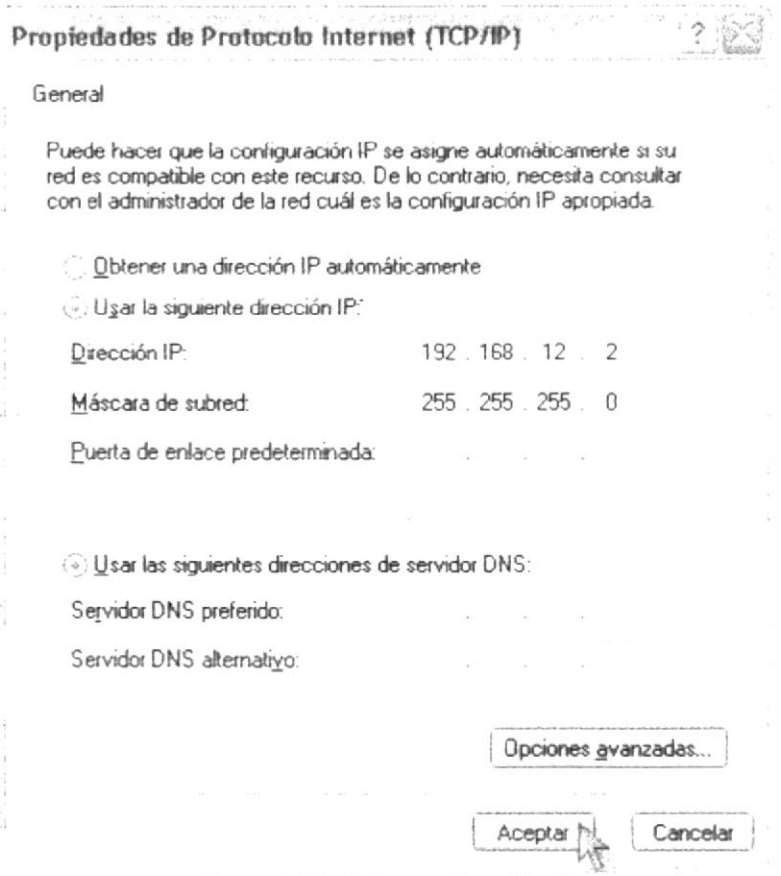


Figura 7-85: Asignar dirección IP

5. Luego de asignarle una dirección Ip a su máquina, proceda a buscar su servidor samba. De clic derecho en Mis sitios de red y seleccione buscar equipos.

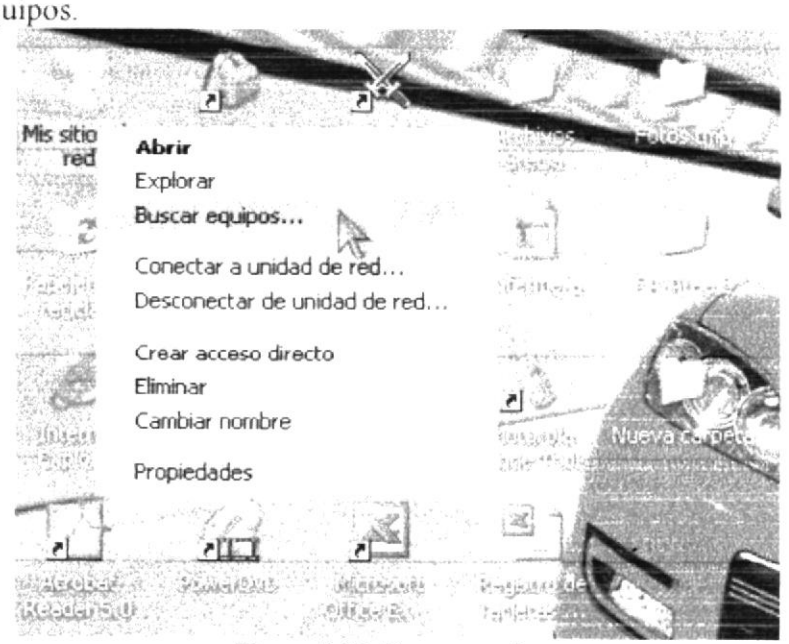


Figura 7-86: Buscar equipos

6. Ingrese el nombre que le asigno a su servidor en el fichero de samba y de clic en búsqueda.

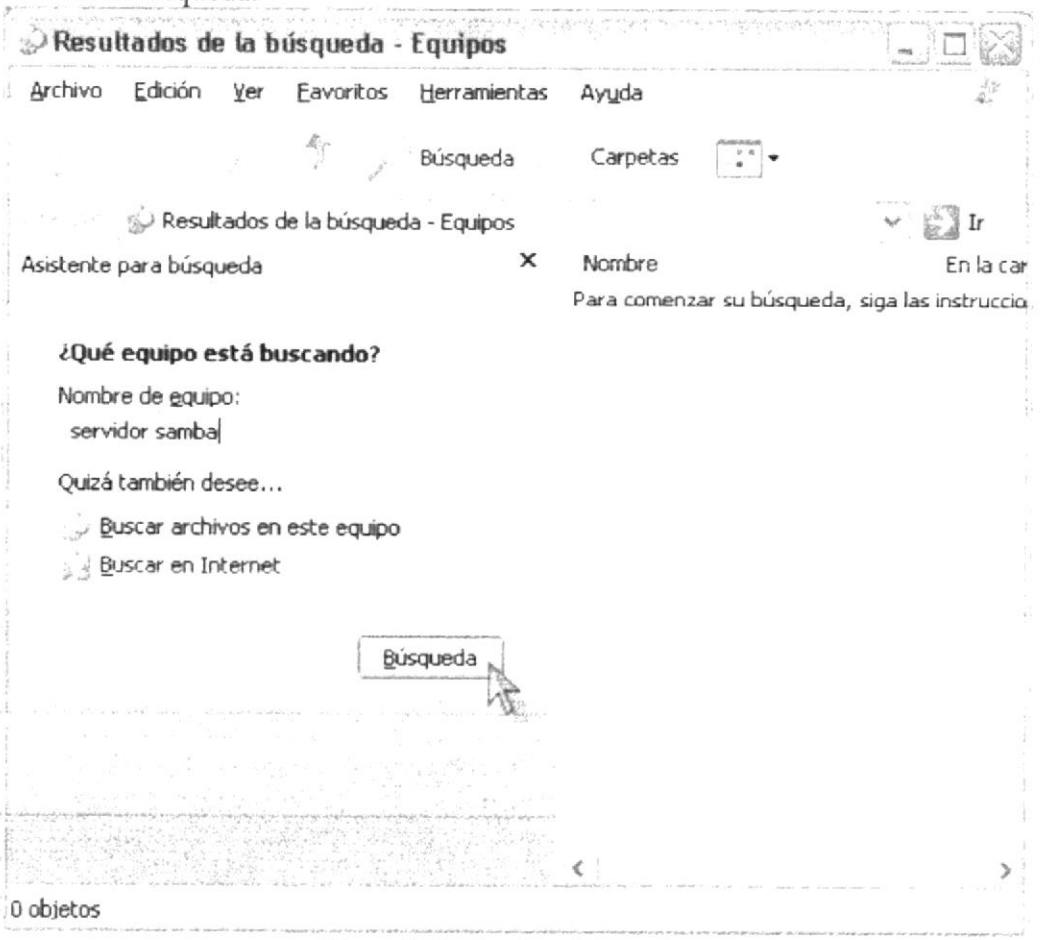


Figura 7-87: Nombre del Servidor

7. Luego de localizar el servidor samba, de clic sobre el icono del servidor.

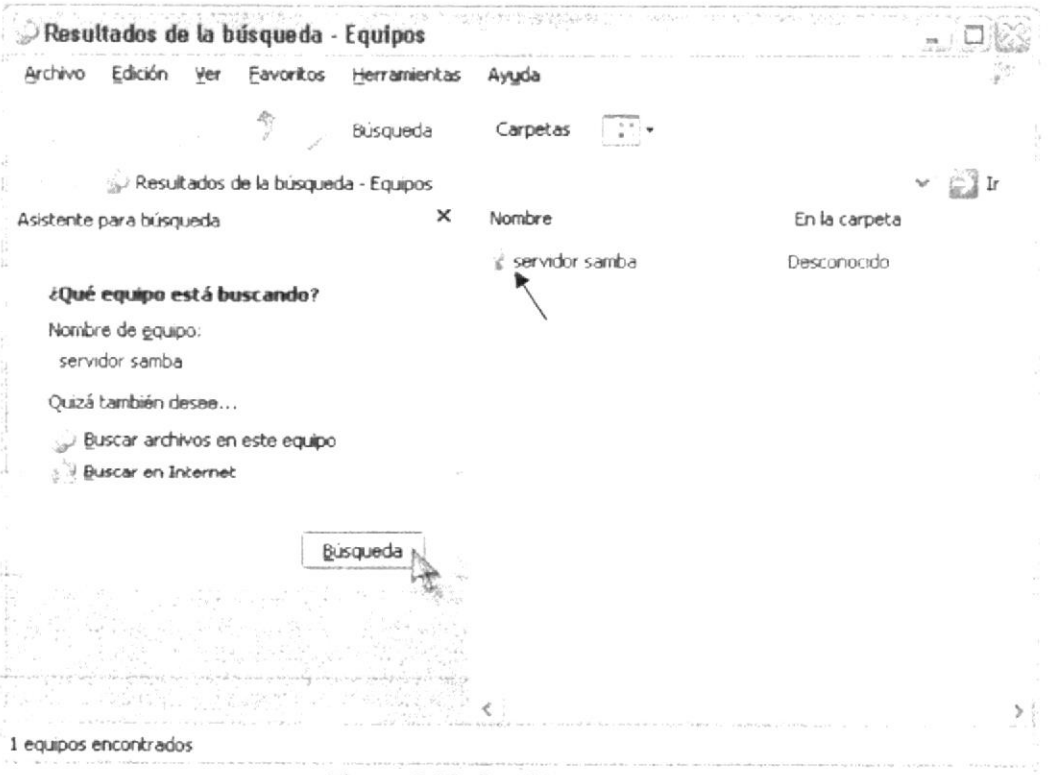


Figura 7-88: Servidor encontrado

8. Al momento de ingresar al servidor, automáticamente este le va a pedir el usuario y la contraseña que creo en el fichero de samba.

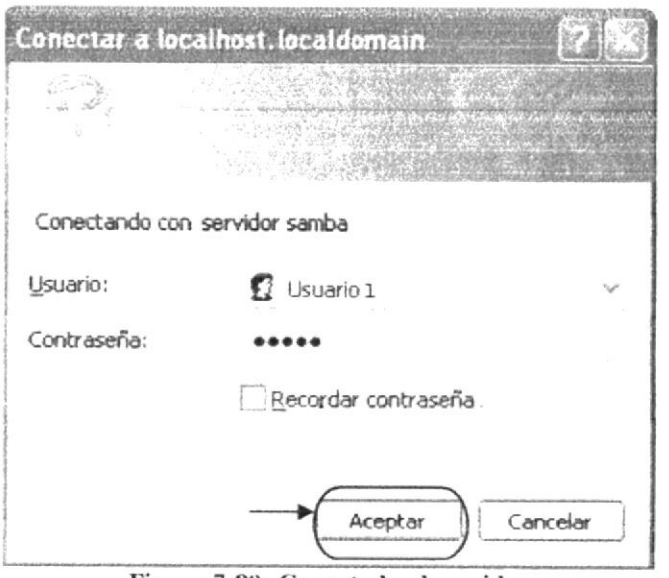


Figura 7-89: Conectado al servidor

9. Una vez ingresado el usuario con su respectiva contraseña, el servidor le mostrara todos los recursos compartidos. Ingrese al directorio documentos.

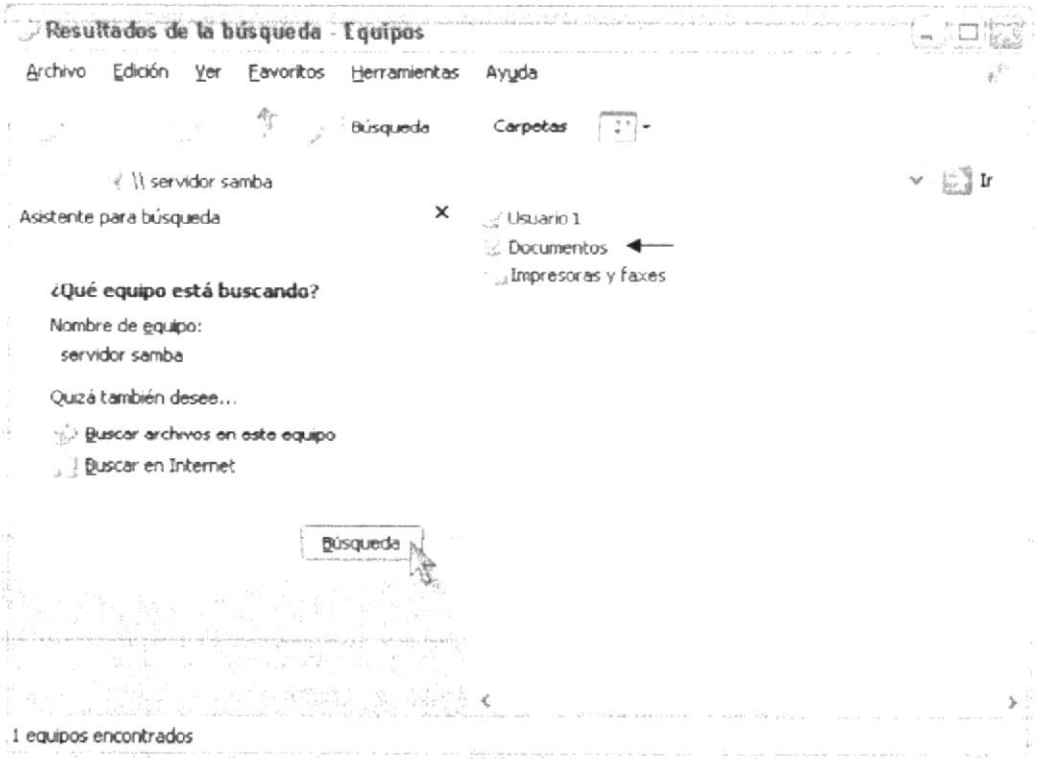


Figura 7-90: Ingresando al directorio

10. Una vez que ingrese al directorio abra el archivo, para realizar una prueba de comprobación.

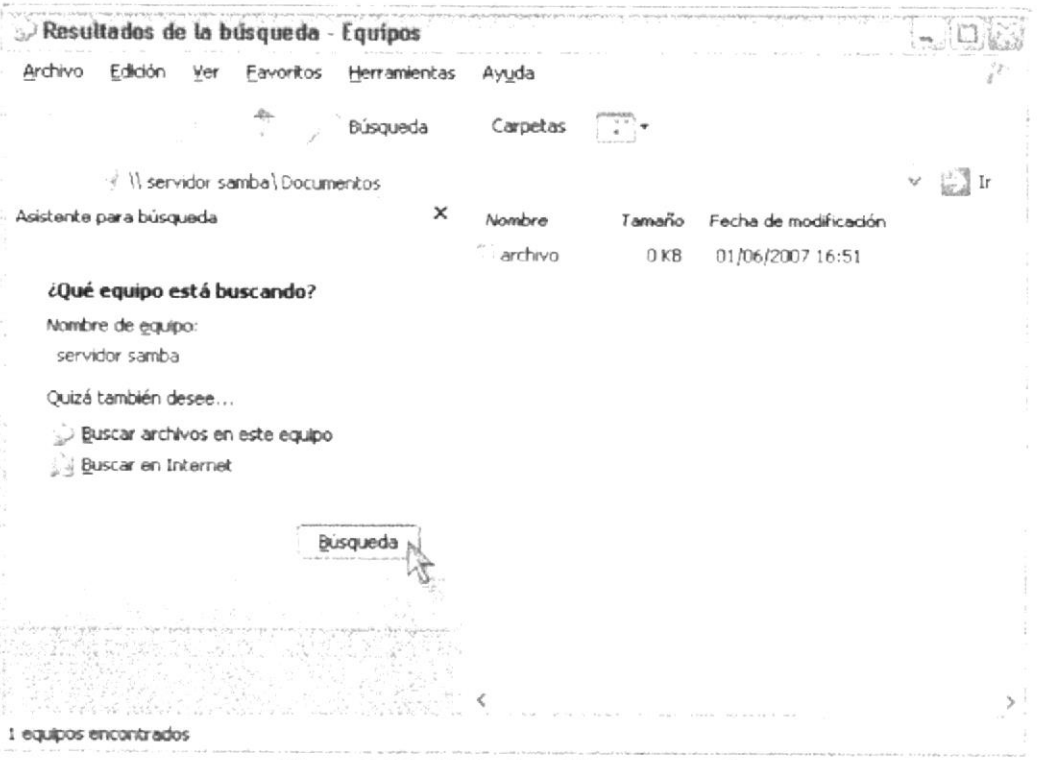


Figura 7-91: Abrir el archivo encontrado

11. Escriba cualquier información y guarde los cambios para luego verificarlos en el servidor y comprobar los permisos de lectura y escritura.

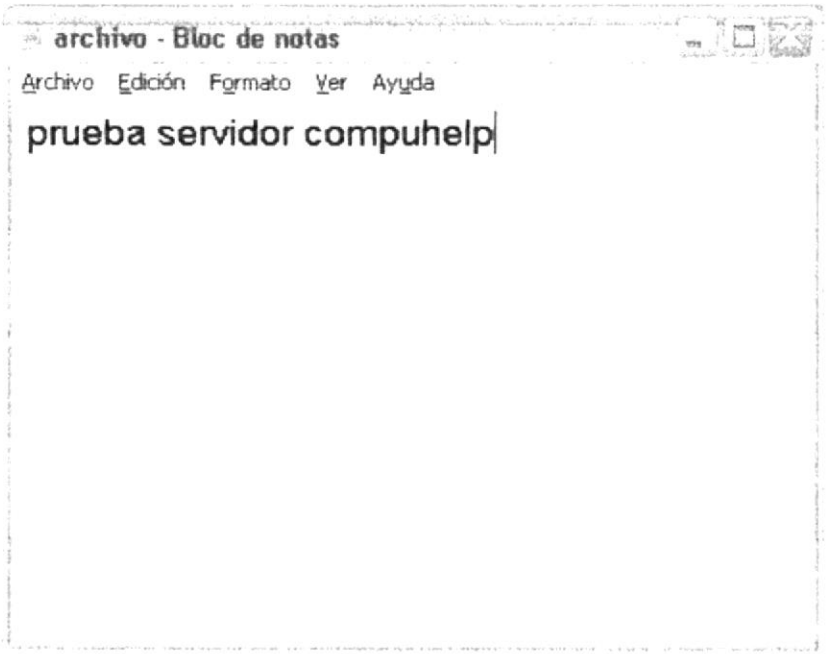


Figura 7-92: Editando el archivo

12. Ingrese al servidor y busque el *directorio* Documentos y con el editor de texto VI abra el archivo.

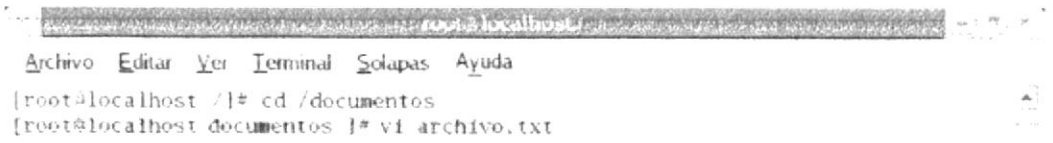


Figura 7-93: Abriendo el archivo para comprobar la configuración

13. Observe la comprobación de permisos de lectura, como de escritura.

Figura 7-94: Prueba exitosa de la configuración Samba

7.10 SERVIDOR DNS (DOMAIN NAME SERVER)

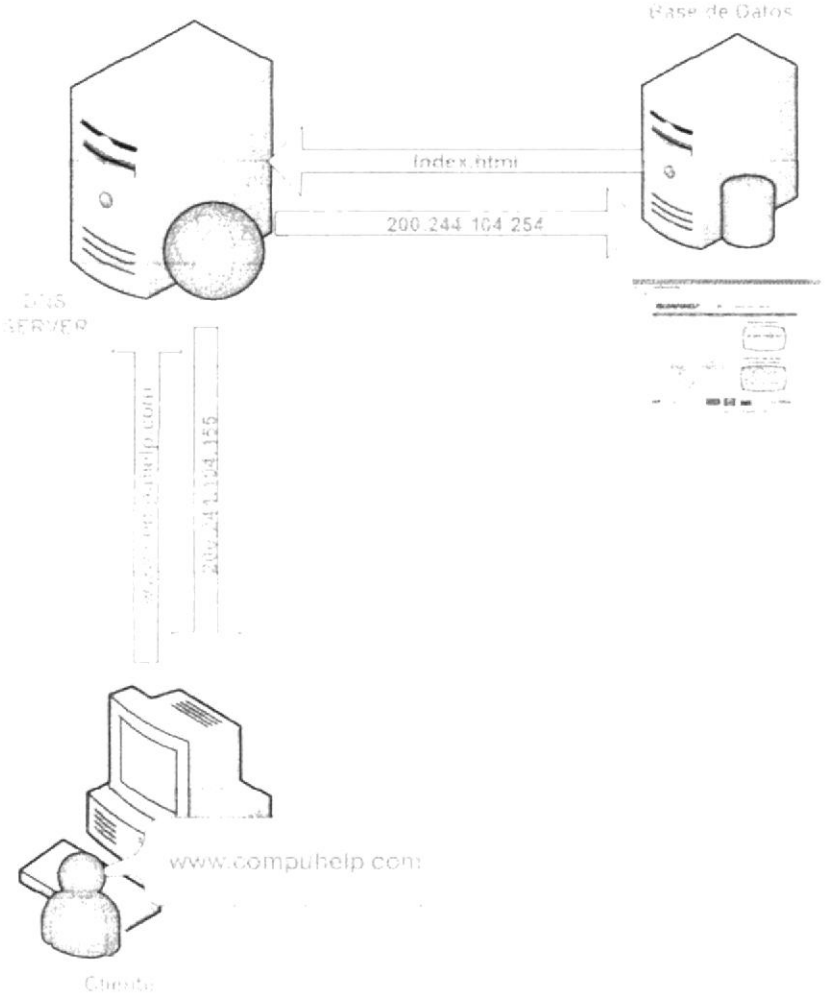


Figura 7-95: DNS Server

El servidor DNS es un conjunto de bases de datos en las que figura la relación entre las direcciones, nombre de dominio y las direcciones numéricas. Mediante el DNS los usuarios acceden a los sites de Internet sin necesidad de conocer largas listas de números. Un servidor DNS *sirve para transformar la IP* de un servidor web en un dominio.

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. 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, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos (técnicamente, este archivo aún existe - la mayoría de los sistemas operativos actuales todavía pueden ser configurados para revisar su archivo hosts).

El DNS organiza los nombres de máquina (hostname) en una jerarquía de dominios. Un dominio es una colección de nodos relacionados de alguna forma porque estén en la misma red, tal como los nodos de una universidad. Por ejemplo, las universidades americanas se agrupan en el dominio edu. Cada universidad tiene allí un subdominio, tal como la universidad Groucho Marx, que posee el subdominio groucho.edu. A su vez, podemos encontrar nuevos subdominios dentro, como el Departamento de Matemáticas (maths). Finalmente, un nodo de ese departamento llamado erdos tendrá un nombre completo (conocido como totalmente cualificado) tal como erdos.maths.groucho.edu. Este nombre totalmente cualificado también se conoce por las siglas FQDN.

7.10.1 FUNCIÓN DEL SERVICIO DNS

Cuando un programa cliente (por ejemplo, el navegador) hace una petición de una dirección de Internet, el servidor DNS del proveedor de acceso, procesa la consulta, intentando buscar el dominio en su tabla de 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 el dominio es el responsable de asociar el nombre de dominio con el servidor DNS correspondiente, de manera que siempre queda asegurada su "visibilidad".

7.10.2 BENEFICIOS AL INSTALAR UN SERVIDOR DNS

- **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.

7.10.3 ZONAS

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

Existen dos tipos de zonas, las primarias y las secundarias.

7.10.3.1 ZONAS PRIMARIAS

Las zonas primarias son aquellas que contienen permisos tanto de lectura como de escritura para el archivo que pertenece a la zona, cualquier cambio en la zona es registrado en este archivo.

7.10.3.2 ZONAS SECUNDARIAS

Las zonas secundarias son aquellas que contienen permisos de sólo lectura sobre el archivo de la zona. Cualquier cambio en la zona será registrado en el archivo de la zona primaria y luego replicado a la zona secundaria.

La raíz del árbol, que se identifica con un punto sencillo, es lo que se denomina dominio raíz y es el origen de todos los dominios. Para indicar que un nombre es FQDN, a veces se termina su escritura en un punto. Este punto significa que el último componente del nombre es el dominio raíz.

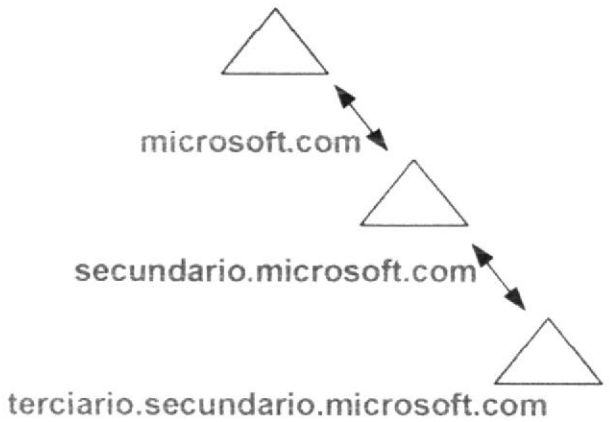


Figura 7-96: Jerarquía de nombres de dominio

Dependiendo de su localización en la jerarquía, un dominio puede ser de primer nivel (top-level), segundo nivel o tercer nivel. Se pueden añadir todos los niveles que queramos, pero no son habituales. Los que siguen son los dominios de primer nivel que veremos con frecuencia:

Dominio	Descripción
edu	Instituciones universitarias, casi todas norteamericanas.
com	Organizaciones comerciales.
org	Organizaciones no comerciales.
net	Pasarelas y otras redes administrativas.
mil	El ejército
gov	El gobierno
uucp	Dominio para redes UUCP.

Tabla 7-3: Descripción de dominio

7.10.4 DEFINICIÓN

DNS (Domain Name System), es un sistema para asignar nombres a equipos y servicios de red que se ordenan en forma jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes de protocolos TCP/IP, como Internet, para localizar equipos y servicios con nombres de una manera sencilla.

Cuando el cliente ingresa un nombre DNS en un explorador, los servicios DNS interpretan el nombre para asociar la búsqueda con las direcciones.

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.

7.10.5 REQUERIMIENTOS PARA CONFIGURACIÓN DE UN DNS SERVER

- Debe tener instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Debe tener asignada una dirección IP estática.
- Debe tener deshabilitado el firewall.
- Debe haber instalado el paquete bind, se verifica con el comando rpm –q bind.

7.10.6 CONFIGURACIÓN DNS

1. Verifique con el siguiente comando si se encuentra instalado el paquete DNS.
   rpm –q bind

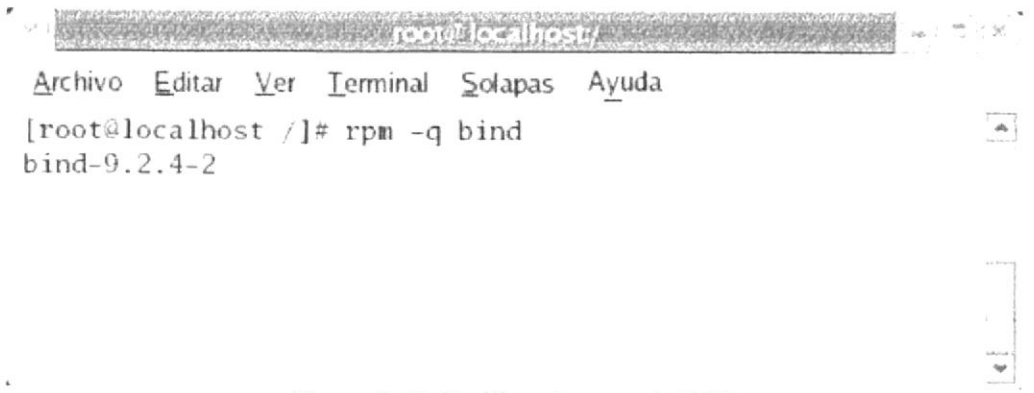


Figura 7-97: Verificando paquete DNS

2. Edite con el vi el archivo named.conf
   vi /etc/ named.conf

Figura 7-98: Ingresando a configurar el DNS

7.10.6.1 CONFIGURANDO EL NAMED

3. En esta pantalla cree una zona para su dominio.

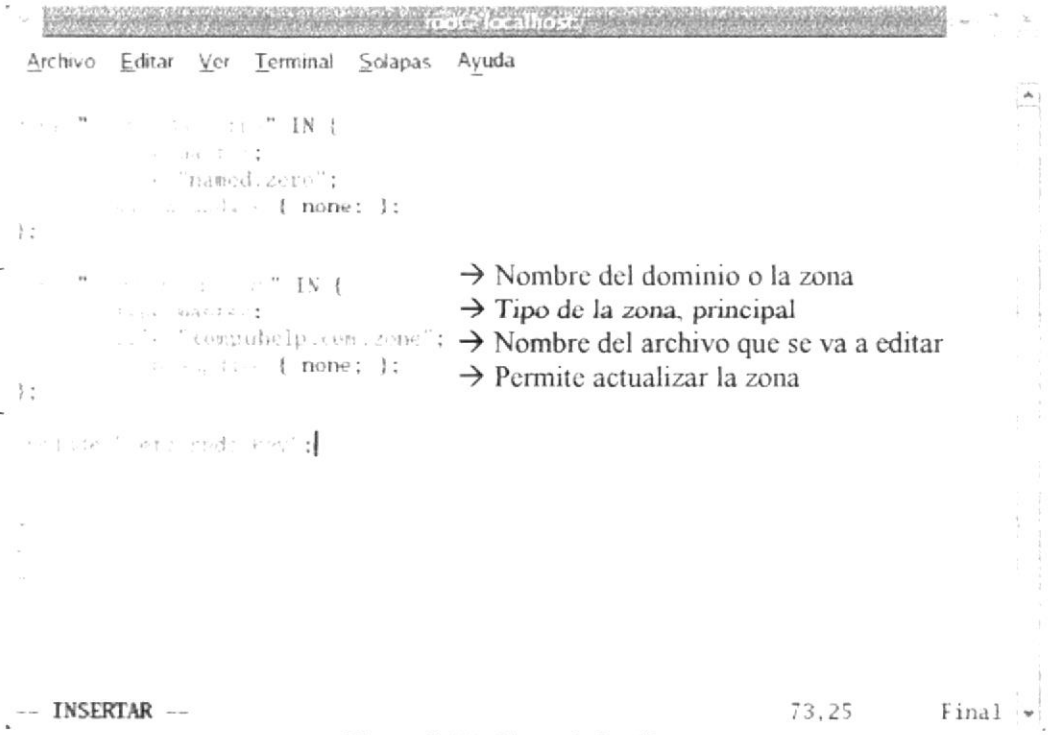


Figura 7-99: Creando las Zonas

Paso A:

- Copie las siguientes lineas:

```
en zone "localhost" IN {
        type master;
        file "nombre.zone";
        allow-update {nome};
        };
```

Paso B:

- Realice los siguientes cambios:

```
en zone "compuhelp.com"{
        type master;
        notify no;
        file "compuhelp.com.zone";
        allow-update{nome};
        };
```

- Salga con el comando (**:wq**) para guardar los cambios.

4. Para que ingrese al named, debe escribir la siguiente ruta.
cd /var/named/chroot/var/named/

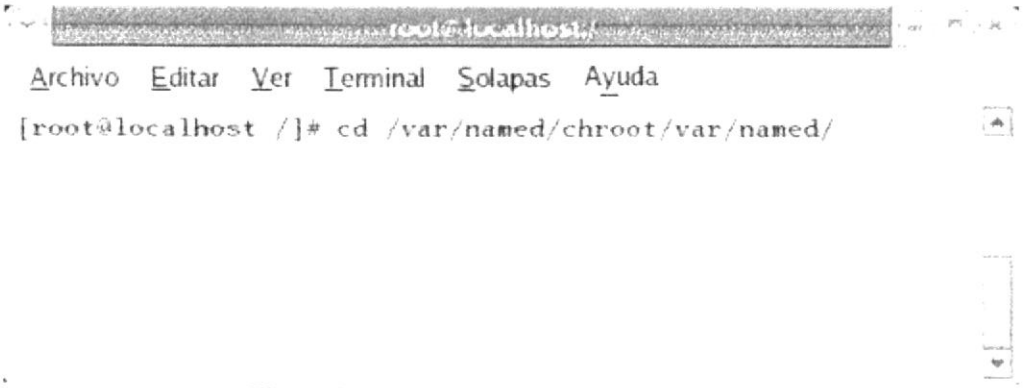


Figura 7-100: Ingresando al directorio named

5. Realice una copia del contenido del archivo localhost.zone al de compuhelp.com.zone

Figura 7-101: Copiando las zonas

6. Edite el archivo copiado mediante el comando
vi compuhelp.com.zone

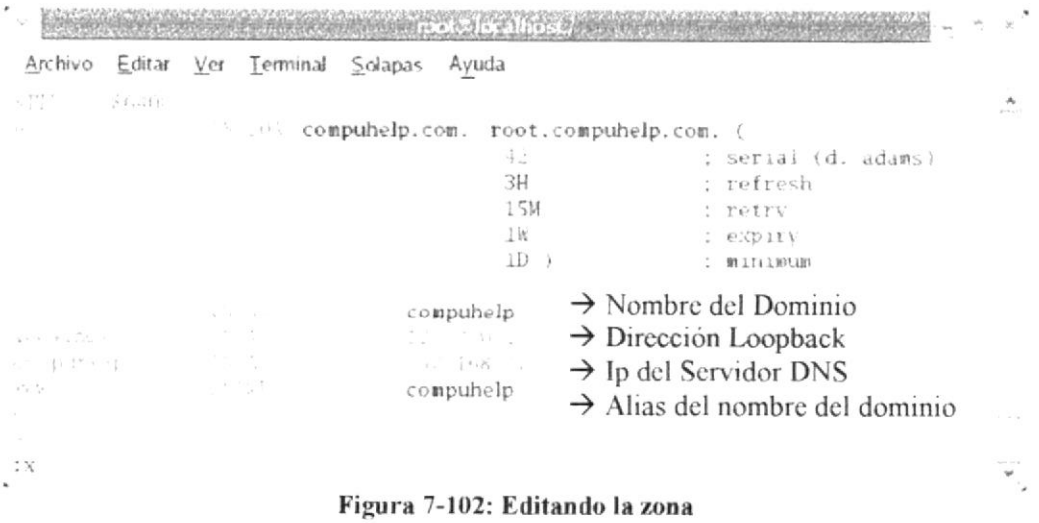


Figura 7-102: Editando la zona

Para mejor compresión de este fichero:
NS: Es el Name Server, es el servidor de nombre de dominio.
SOA: Es una abreviatura de Stara of Authority.
@: Es una notación especial que simboliza el origen.
CNAME: Registra el nombre y hace que un nombre sea un alias.
REFRESH: Tiempo de actualización de la pagina.
RETRY: Tiempo de reintento de consulta.
EXIPIRE: Tiempo de expiración de la pagina.
MINIMUN: Tiempo total de vida.

7. Inicie los servicios named
   Service named start

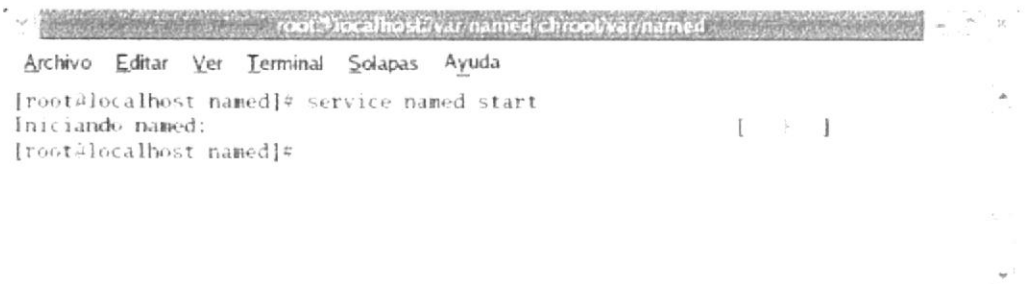


Figura 7-103: Iniciando los servicios named

8. Luego edite el archivo resolv.conf que se encuentra en el directorio etc.

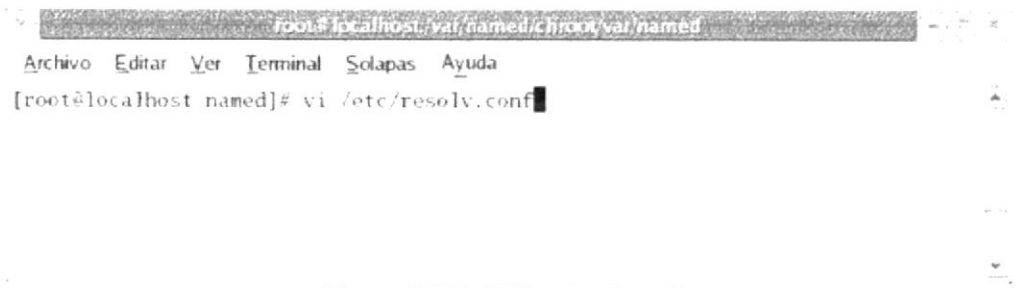


Figura 7-104: Editando el resolv

9. Luego en el archivo resolv agregue la línea nameserver con la dirección Ip del servidor.

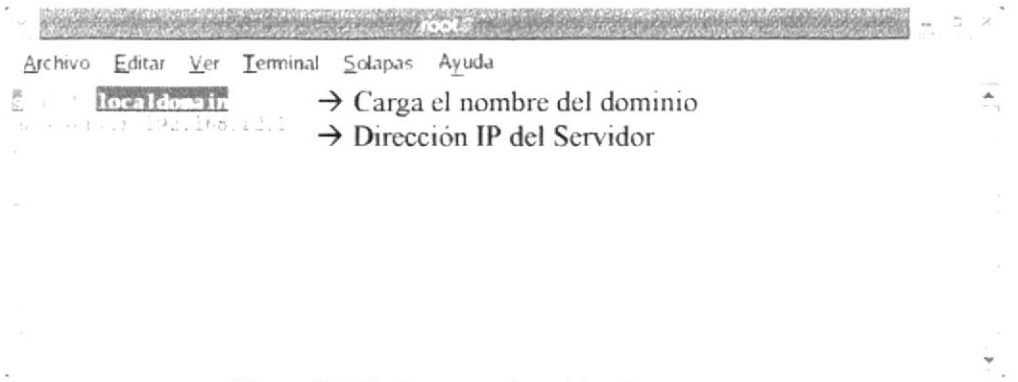


Figura 7-105: Agregar dirección al name server

10. Puede comprobar que la configuración DNS funciona haciendo ping a la dirección del dominio www.compuhelp.com en lugar de la dirección Ip del servidor 192.168.12.1

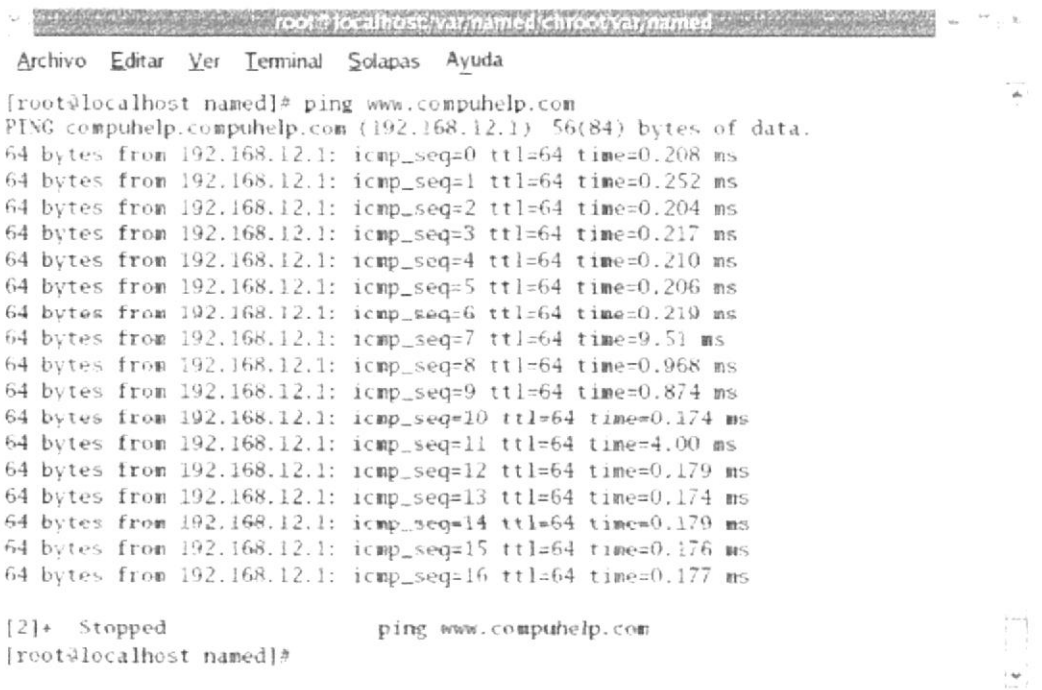


Figura 7-106: Comprobación exitosa del DNS

7.10.7 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. De clic derecho en mis sitios de red y de clic en propiedades.

Figura 7-107: Propiedades de Windows

2. De clic derecho en conexión de área local y de clic en propiedades.

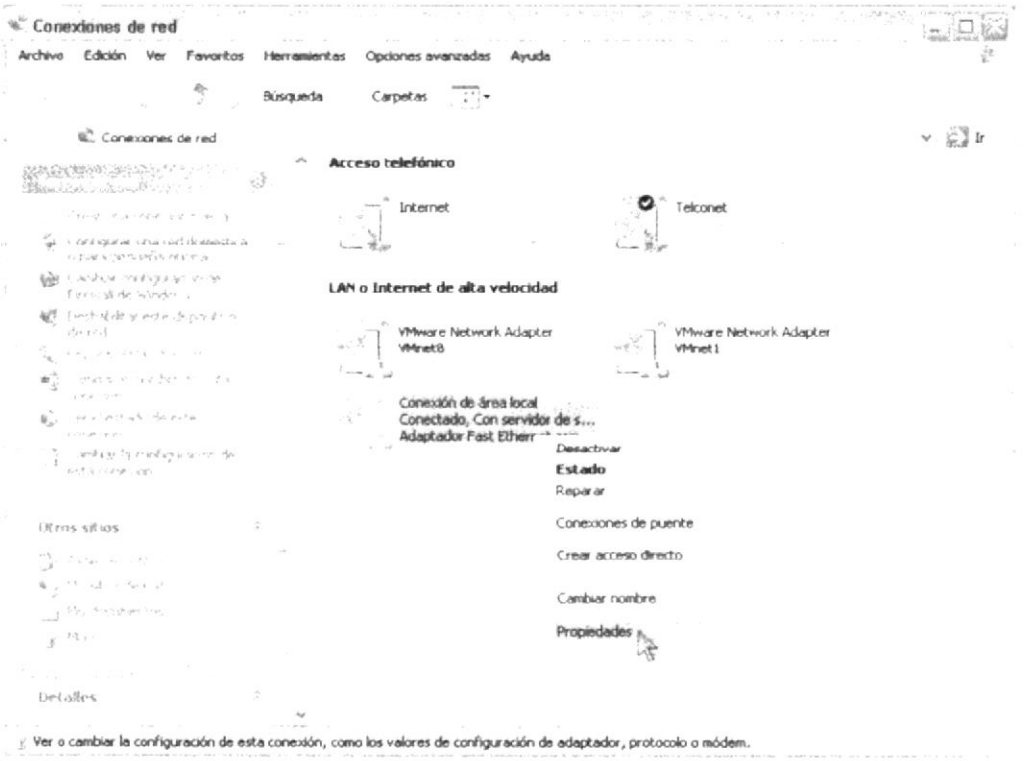


Figura 7-108: Propiedades de Conexión de área local

3. Seleccione el item Protocolo Internet TCP/IP y de clic en propiedades.

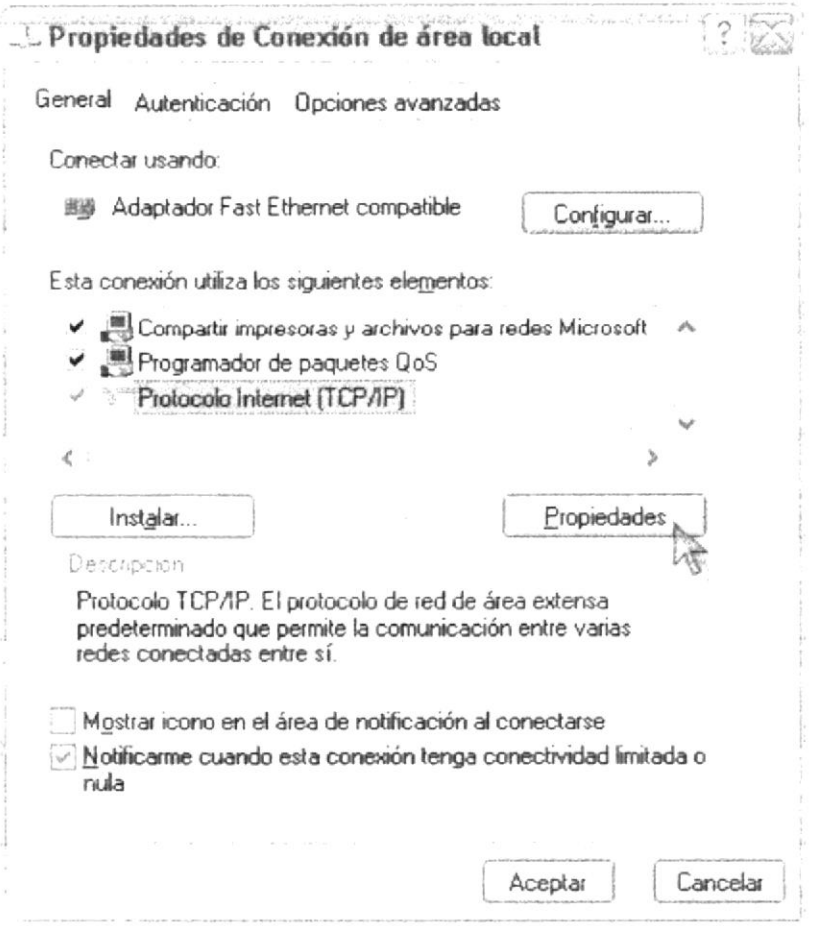


Figura 7-109: Protocolo TCP/IP

4. Ingrese la dirección ip del servidor DNS y de clic en aceptar.

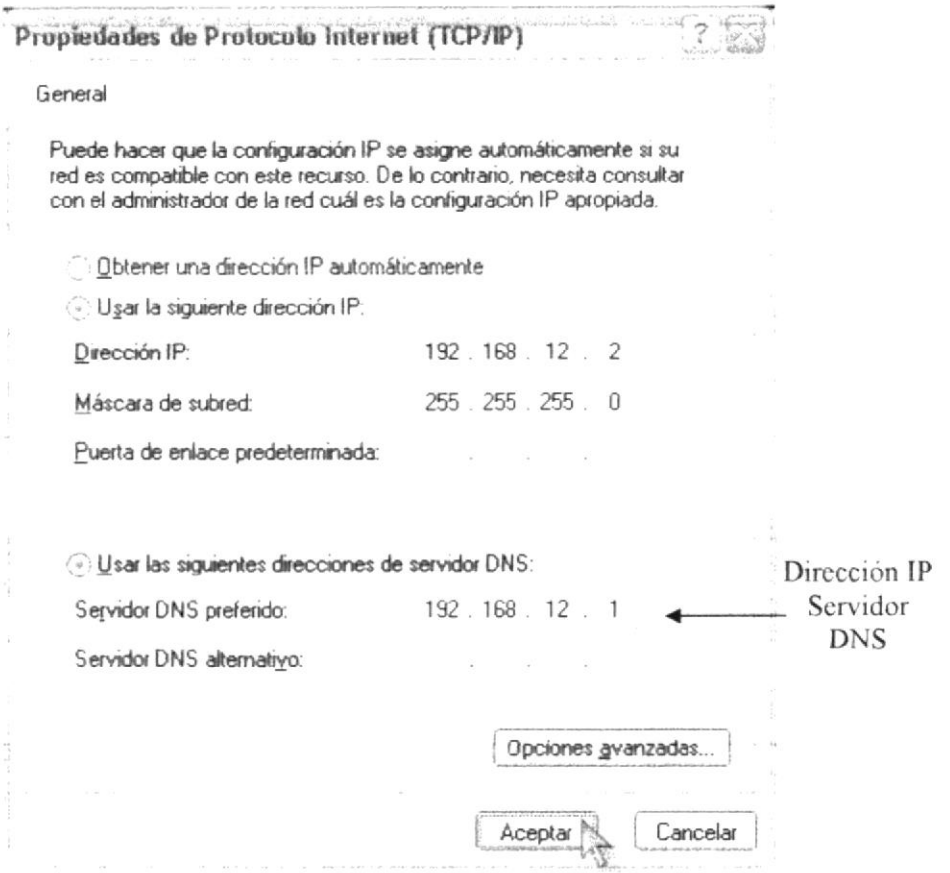


Figura 7-110: Asignar dirección del Servidor DNS

5. De clic izquierdo en inicio, y seleccione ejecutar.

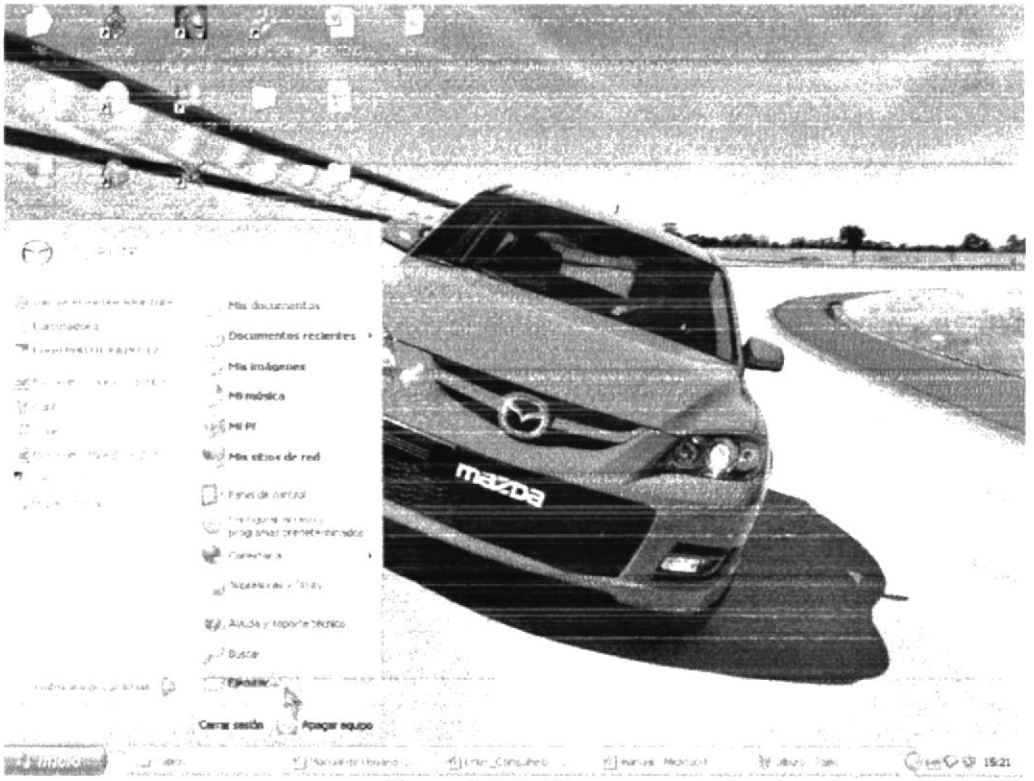


Figura 7-111: Ejecutar

6. Luego le aparece una pequeña ventana, donde debe ingresar el comando cmd, para ingresar al DOS de Windows.

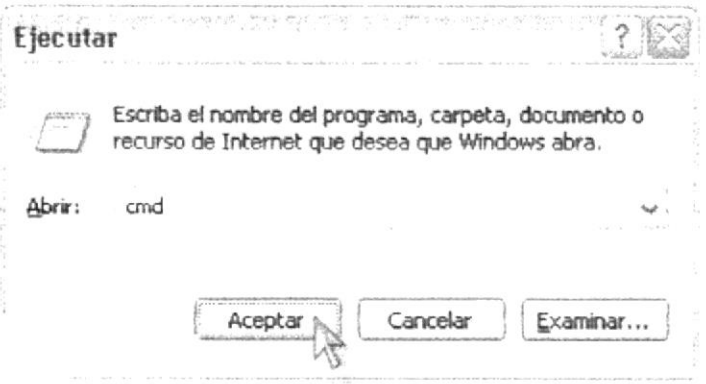


Figura 7-112: Comando cmd

7. Luego le aparecerá la pantalla del DOS donde debe realizar su prueba.

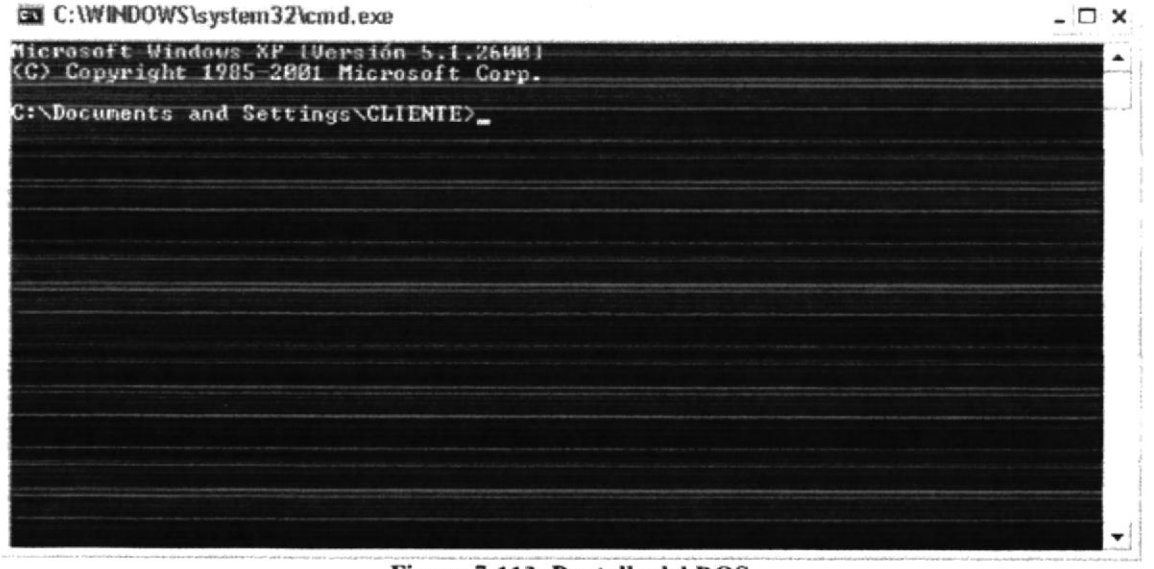


Figura 7-113: Pantalla del DOS

8. Ingrese el comando ping, seguido de su dominio, en este caso www.compuhelp.com

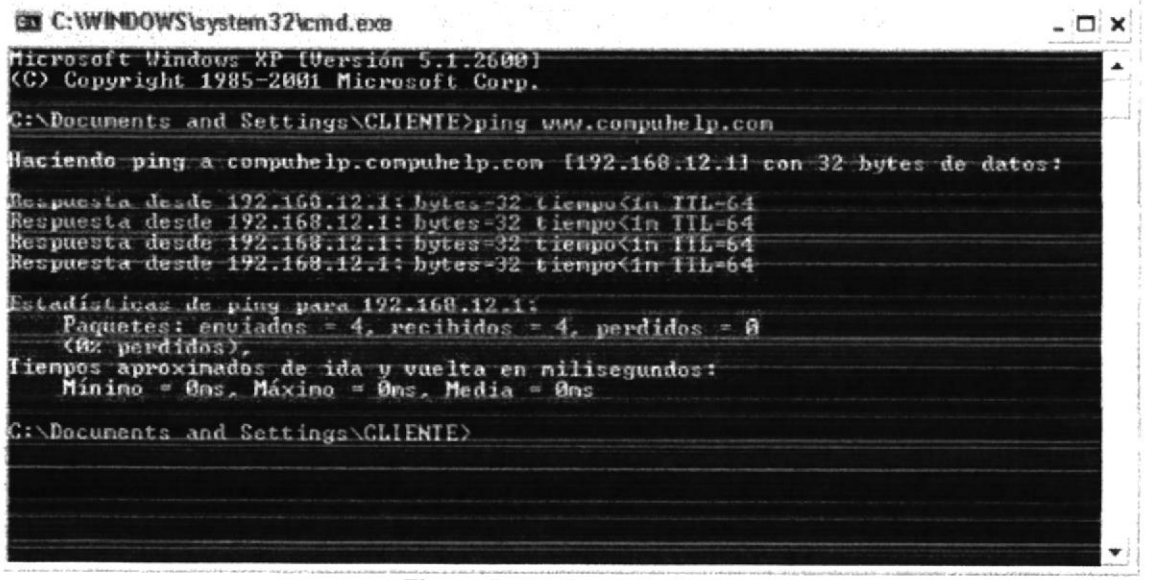


Figura 7-114: Prueba exitosa

7.11 WEB SERVER (SERVIDOR WEB)

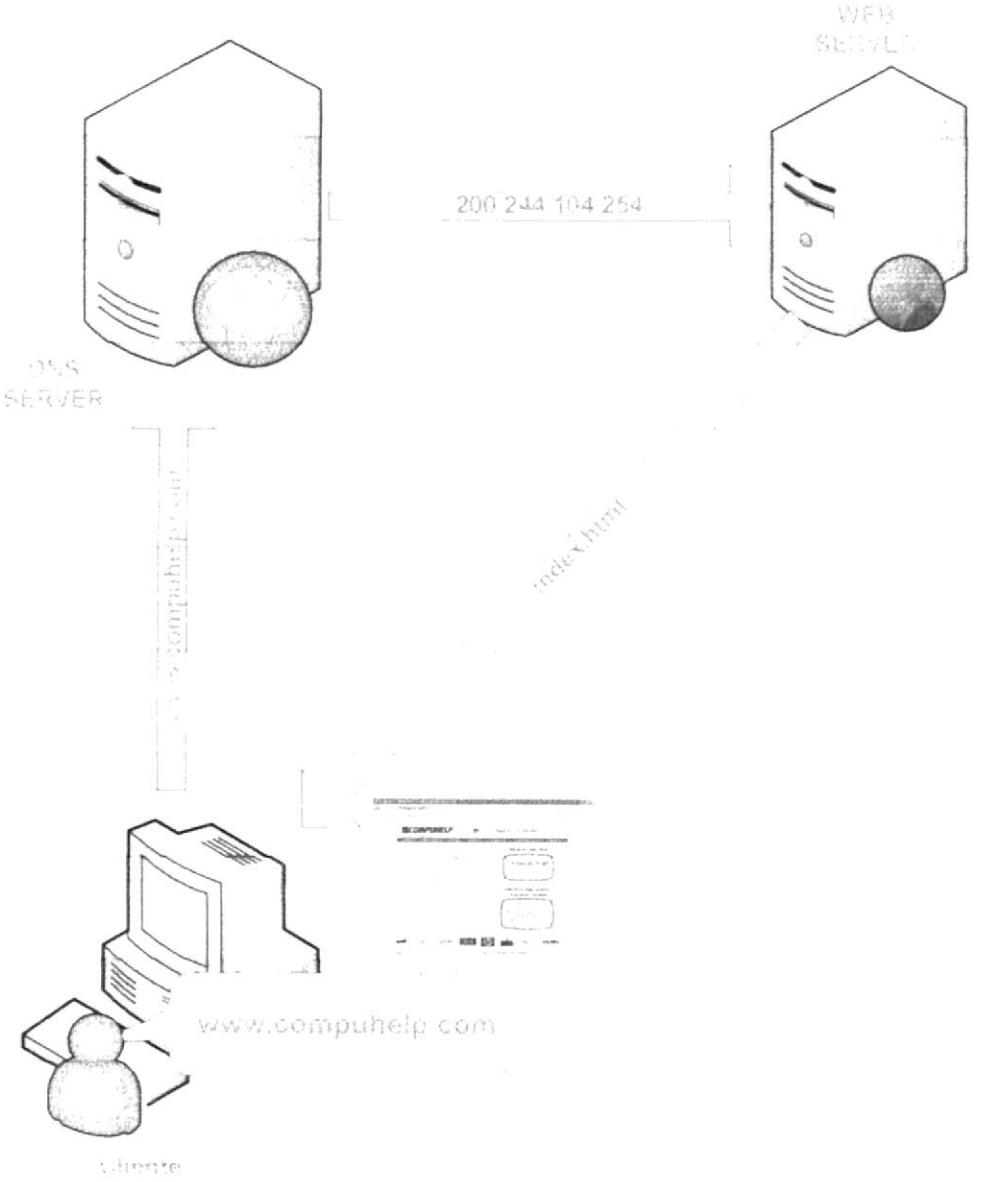


Figura 7-115: Como funciona el Web Server

El servidor web es la aplicación que se encarga de almacenar páginas Web junto con sus archivos asociados y bases de datos para posteriormente entregarlas a los buscadores Web por medio del http.

Apache está diseñado para ser un servidor web potente y flexible que pueda funcionar en la más amplia variedad de plataformas y entornos. Las diferentes plataformas y los diferentes entornos, hacen que a menudo sean necesarias diferentes características o funcionalidades, o que una misma característica o funcionalidad sea implementada de diferente manera para obtener una mayor eficiencia. Apache se ha adaptado siempre a una gran variedad de entornos a través de su diseño modular.

Los Servidores Web son aquéllos que permiten a los clientes compartir datos, documentos y multimedia en formato Web. Aunque es parte de la tecnología Cliente-Servidor, el servidor Web aporta algunas ventajas adicionales, como acceso más simple a la información tan solo con un clic.

Una dirección de Internet (a veces llamada dirección URL o Localizador de recursos universal) suele estar compuesta por cuatro partes:

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

Versatilidad

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

Confiabilidad

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

Seguridad

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

Economía

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

7.11.1 DEFINICIÓN

Un servidor Web es una aplicación que satisface las solicitudes HTTP, FTP, SMTP, HTTPD realizadas por los navegadores. Para ello, el ordenador que la soporta debe estar conectado a la Internet o a la Intranet y por lo tanto, debe tener asignada una dirección IP.

7.11.2 REQUERIMIENTOS PARA CONFIGURACIÓN DE UN WEB SERVER

- Debe tener instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Debe haberle asignado un IP estática al servidor.
- Debe tener deshabilitado el firewall.
- Debe haber instalado el paquete httpd el cual se verifica con el comando rpm –q httpd.
- Debe tener levantado los servicios DNS.
- Debe tener habilitado un dominio.

7.11.3 CONFIGURACIÓN WEB SERVER

1. Verifique que se encuentre instalado el paquete web server
   rpm –q httpd

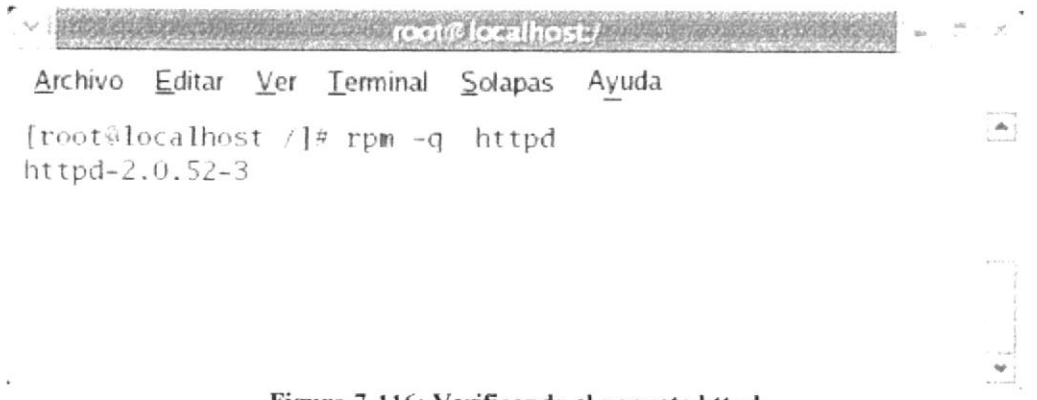


Figura 7-116: Verificando el paquete httpd

2. Configure el archivo httpd.conf que se encuentra en la siguiente ruta
   vi /etc/httpd/conf/httpd.conf

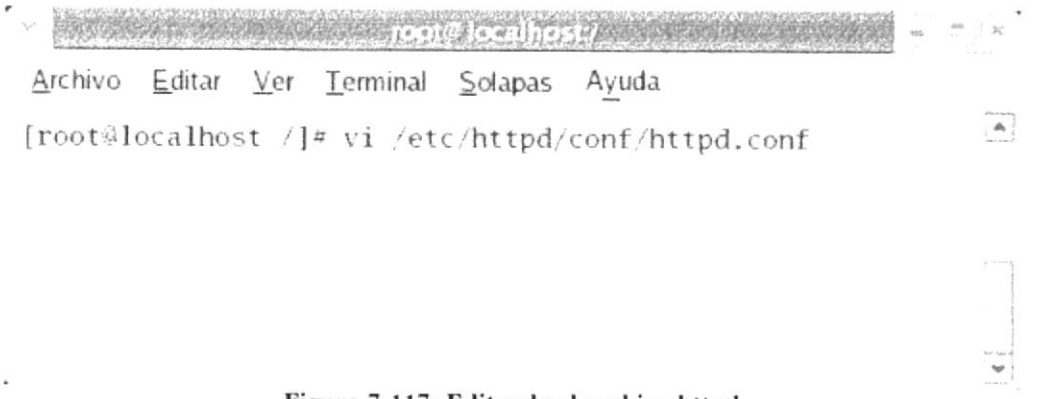


Figura 7-117: Editando el archivo httpd

3. Edite el archivo descomentando la línea de NameVirtualHost *:80, en donde le permite levantar varias zonas.

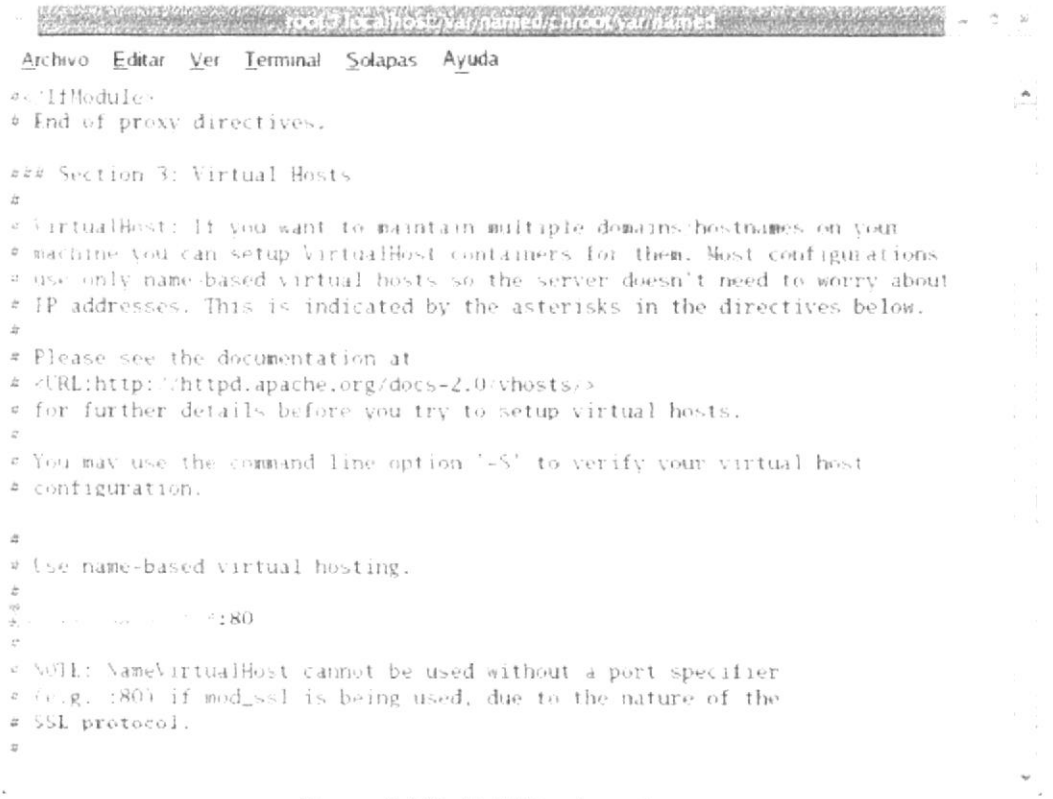


Figura 7-118: Habilitando varias zonas

4. Copie todo el párrafo desde virtual host *:80, hasta virtual host y realice los siguientes cambios:

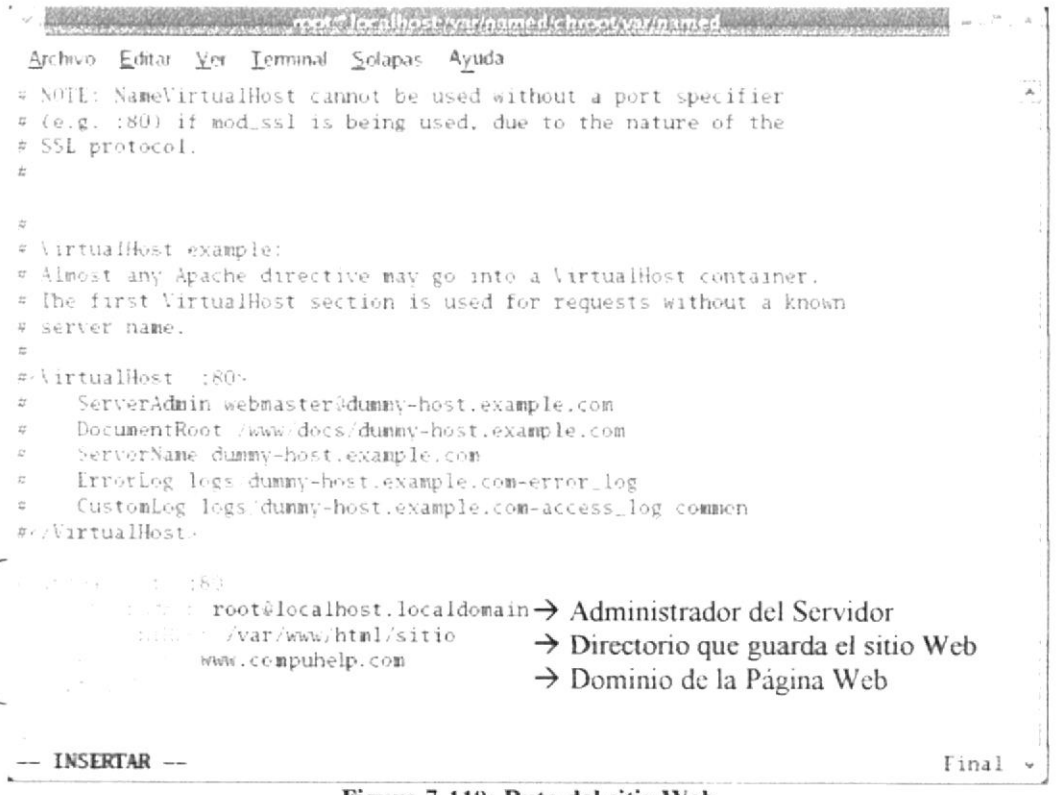


Figura 7-119: Ruta del sitio Web

5. Luego ingrese a la ruta especificada en el document root.
cd /var/www/html/

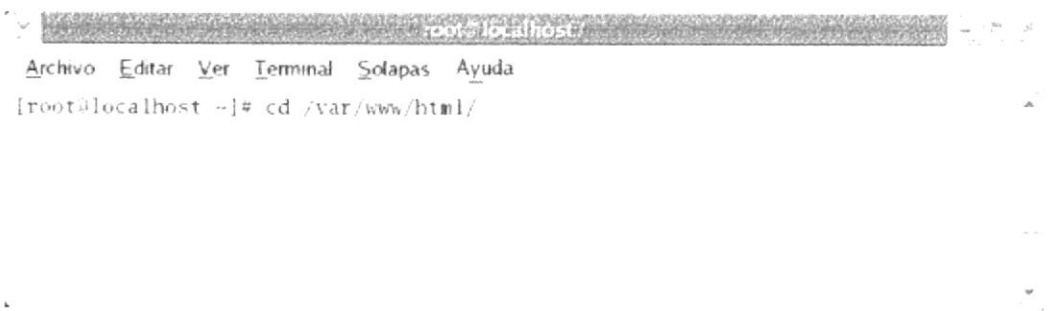


Figura 7-120: Ingresando al directorio html

6. Cree la carpeta donde será ubicada su página Web.
mkdir sitio

Figura 7-121: Creando el directorio de nuestra página

7. Ingrese a la carpeta con el comando cd
cd sitio

Figura 7-122: Ingresando al directorio de nuestra página

8. Cree un archivo con extensión html para verificar el funcionamiento de su configuración.
Touch index.html

Figura 7-123: Creando un archivo de prueba

9. Edite el archivo con el comando VI.

Figura 7-124: Editando el archivo de prueba HTML

10. Dentro del archivo html, agregue un mensaje de prueba para poder visualizarlo en el navegador.

Figura 7-125: Creando un mensaje de prueba HTML

11. Inicie los servicios httpd
service httpd start

Figura 7-126: Iniciando los servicios httpd

7.11.4 CONFIGURACIÓN EN EL CLIENTE WINDOWS

En Windows acceda mediante el navegador a su sitio web. Antes de que ingrese al navegador debe tener asignada la dirección DNS en su máquina Windows.

1. De clic derecho en mis sitios de red, luego de clic en propiedades.

Figura 7-127: Propiedades de red

2. De clic derecho en conexión de área local y de clic en propiedades.

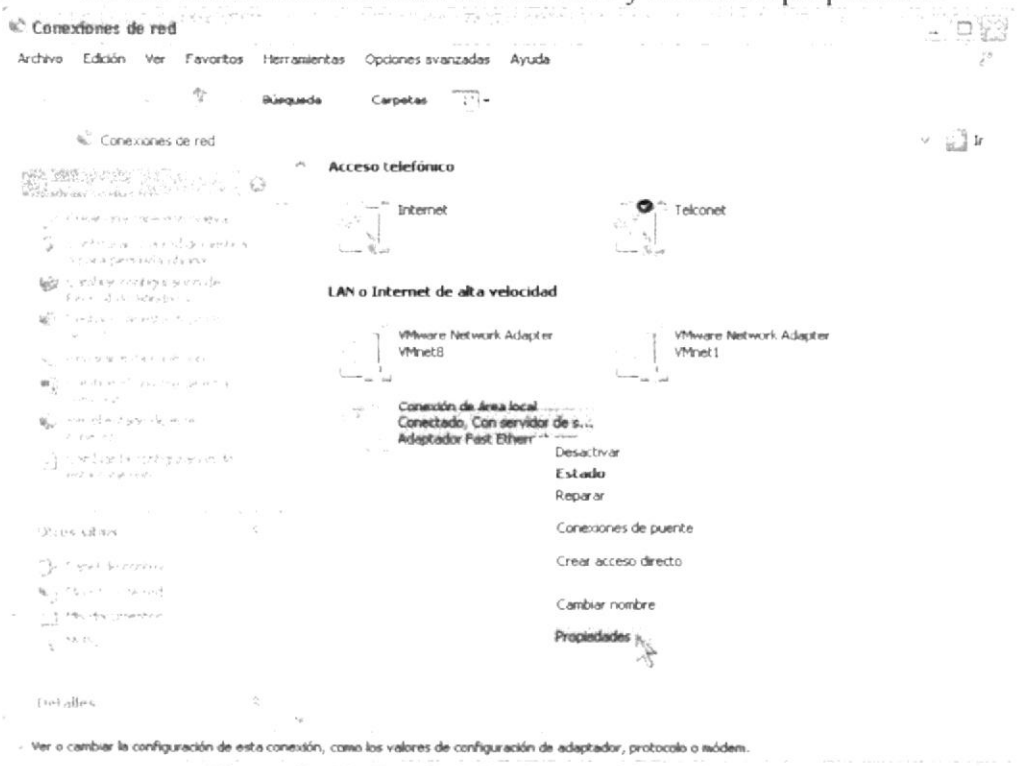


Figura 7-128: Propiedades de conexión de área local

3. Seleccione Protocolo Internet TCP/IP y de clic en propiedades.

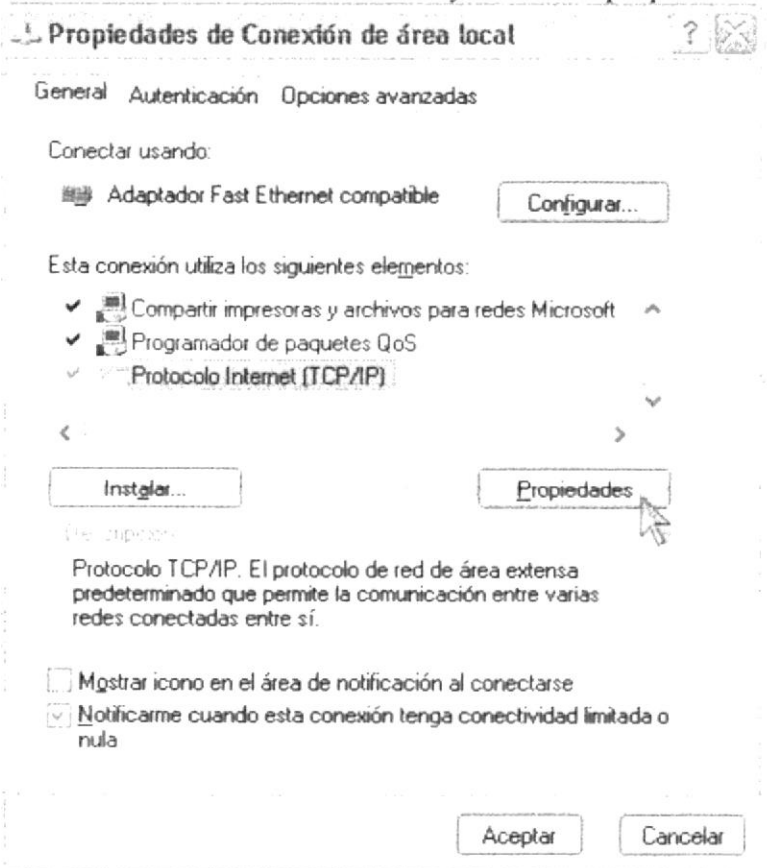


Figura 7-129: Propiedades TCP/IP

4. Ingrese la dirección del servidor DNS preferido y luego de clic en aceptar.

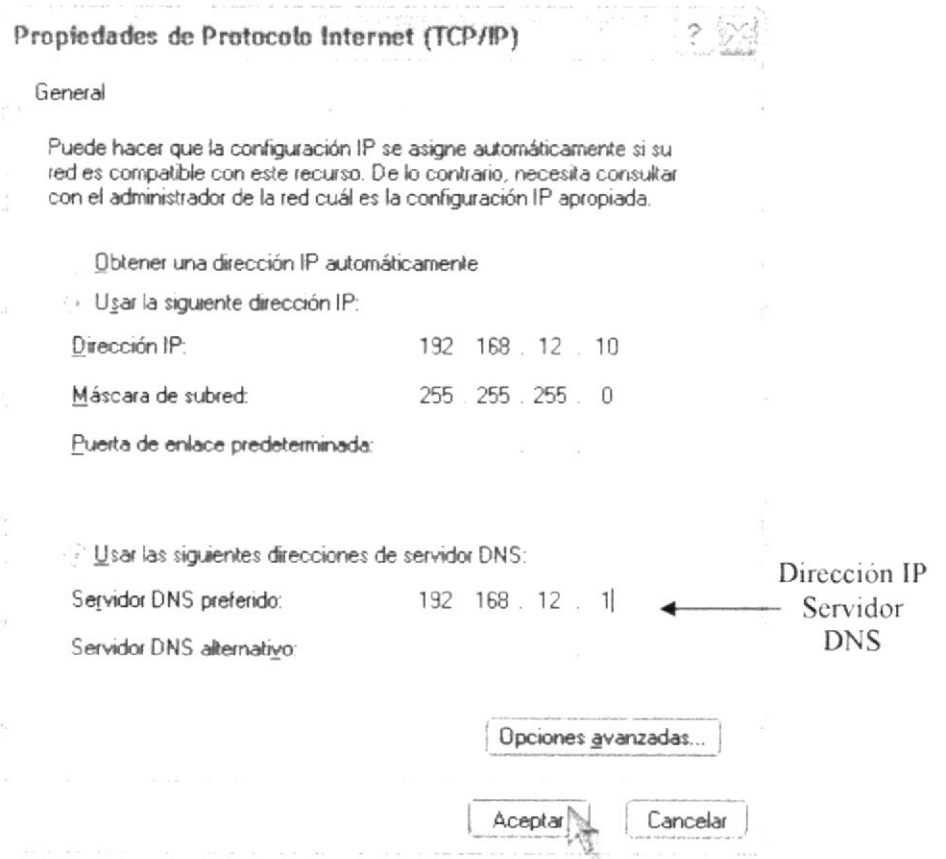


Figura 7-130: Verificando la IP del Servidor DNS

5. Abra el Internet Explorer y escriba el nombre de su dominio www.compuhelp.com

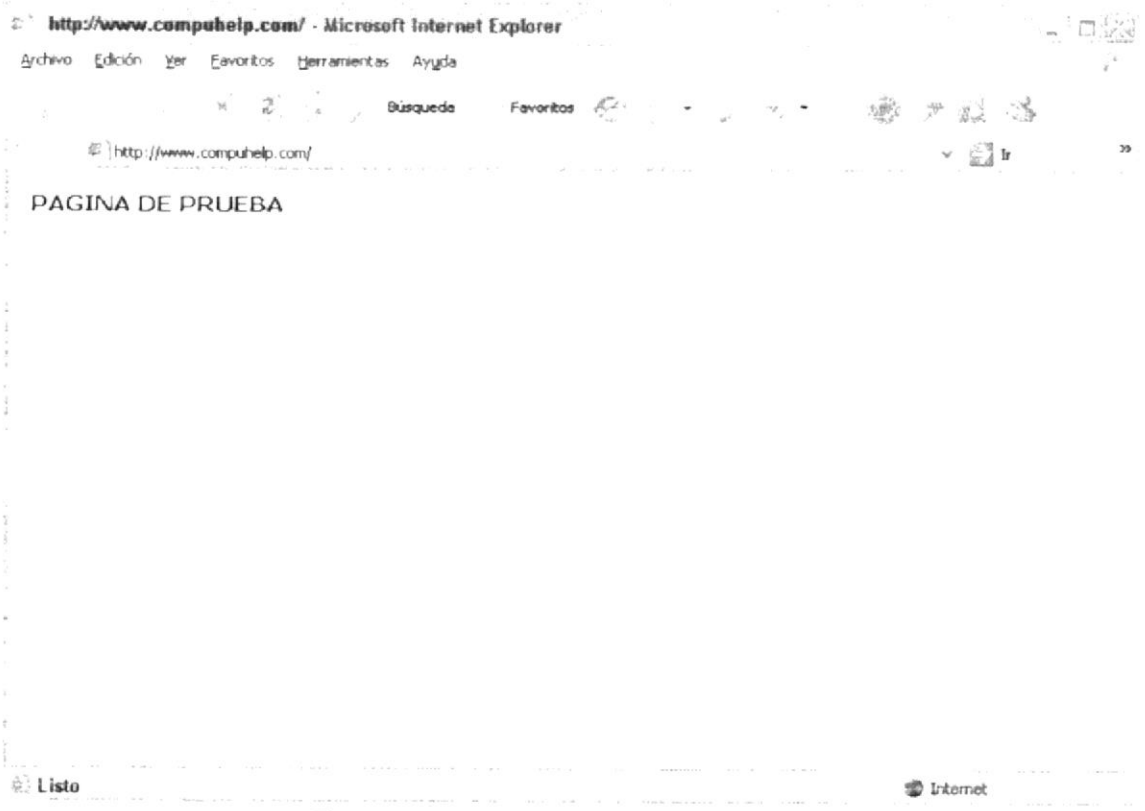


Figura 7-131: Prueba exitosa del Web Server

7.12 MAIL SERVER (SERVIDOR DE CORREO)

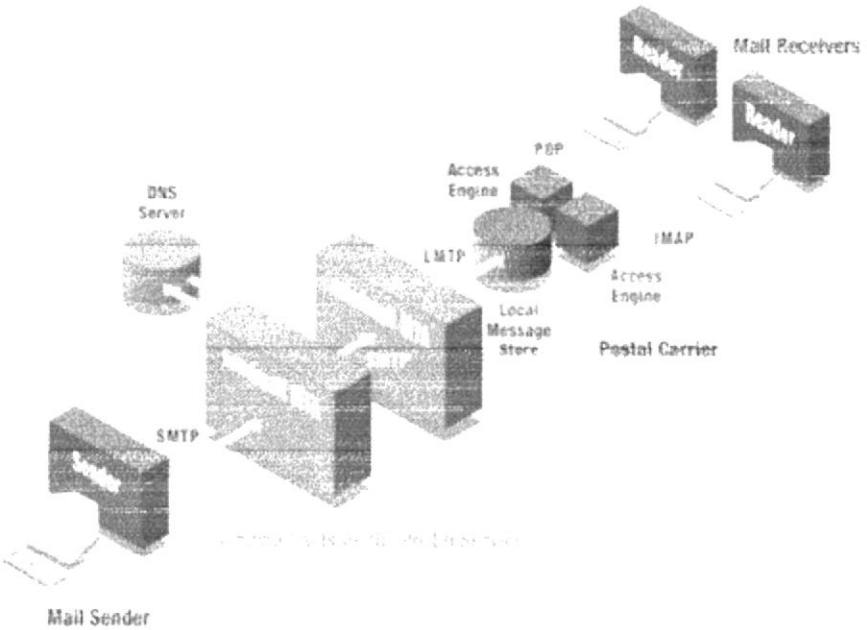


Figura 7-132: Como funciona el Servidor de correo

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

Cuando alguien envía un correo electrónico a usuario@compuhelp.com, se establece la comunicación con el puerto TCP 25 del "Host" vía SMTP, si el puerto esta disponible y el "Servidor de Mail" puede recibir correo electrónico para usuario@compuhelp.com entonces el "Servidor de Mail" lo guarda en disco duro para que posteriormente sea leído por el usuario.

Al igual que los servidores de páginas, existen varios servidores de Mail (también llamados MTA "Mail Transfer Agent") uno de los más comunes y también Open Source es llamado: Sendmail, sin embargo, su configuración no es nada fácil, el archivo principal de configuración sendmail.cf es considerado uno de los archivos más complejos con los que trabaja un administrador de Unix. Además de Sendmail existen alternativas como smail y qmail que también son Open-Source.

7.12.1 DEFINICIÓN

Mail Server es un servidor de correo que trabaja con los servicios dovecot y sendmail, con los protocolos POP3 y SMTP que utilizan los puertos 110 y 25 respectivamente, que soporta un número ilimitado casillas de mail, y listas de correo.

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

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

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

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

Un servidor de correo consta en realidad de dos servidores: un servidor SMTP que es el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que es el que permite 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.

Versatilidad

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

Confiabilidad

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

Seguridad

IMAP/POP con SSL, SMTP autentificado, claves encriptadas con CRAM-MD5, DIGEST-MD5, Kerberos, NT-Login o POP-before-SMTP. Lo que quiera en materia de seguridad y control de relay puede ser realizado, siempre con el máximo rendimiento.

Rapidez

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

Economía

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

7.12.2 REQUERIMIENTOS PARA LA CONFIGURACIÓN DE UN MAIL SERVER

- Debe tener instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Debe haberle asignado una IP estática al servidor.
- Debe tener deshabilitado el firewall.
- Debe haber instalado el paquete sendmail el cual se verifica con el comando rpm –q sendmail.
- Debe haber instalado el paquete dovecot el cual se verifica con el comando rpm –q dovecot.

7.12.3 CONFIGURACIÓN MAIL SERVER

1. Verifique si está instalado el paquete sendmail.
   rpm –q sendmail

Figura 7-133: Verificando el paquete sendmail

2. Edite el Hosts para que le dé un nombre a su servidor.

Figura 7-134: Editando el hosts

3. Al ingresar al hosts, le muestra la dirección de loopback.

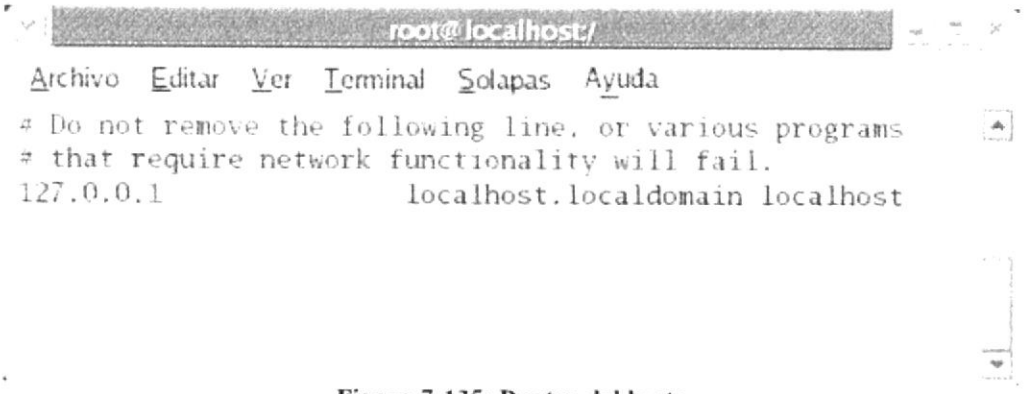


Figura 7-135: Dentro del hosts

4. Comente la dirección de loopback y escriba debajo de la línea.

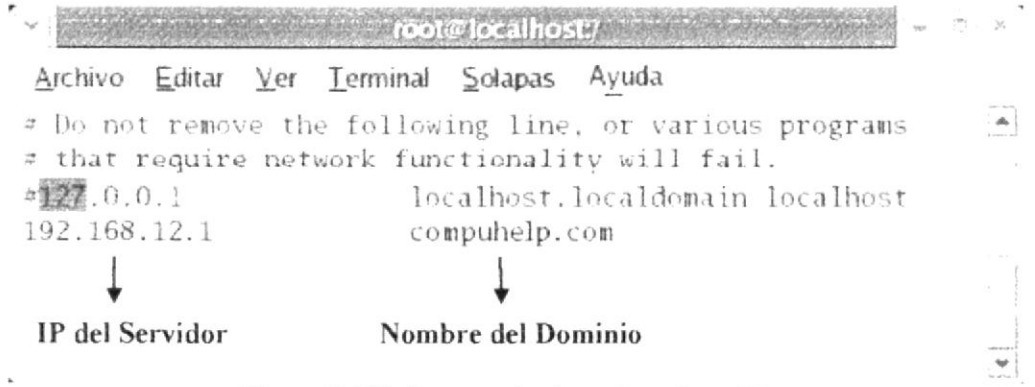


Figura 7-136: Ingresando el nombre al servidor

5. Configure el archivo del servicio Sendmail
   vi /etc/mail/sendmail.cf

Figura 7-137: Editando el sendmail

6. En Cwlocalhost cambie por Cwcompuhelp.com, nombre del dominio.

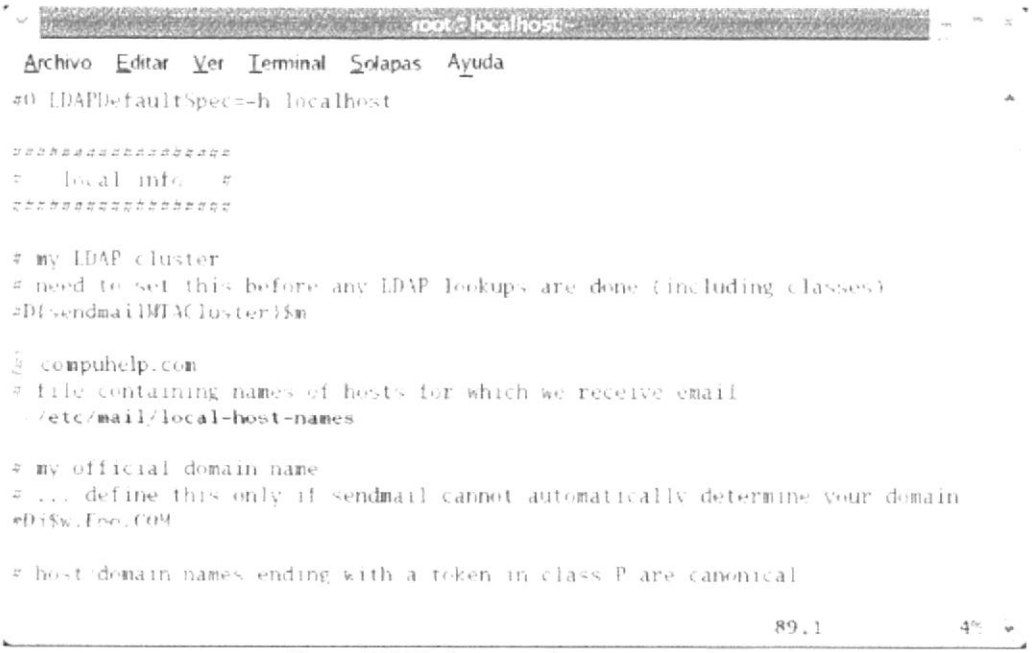


Figura 7-138: Agregando los parámetros

7. Cambie la dirección loopback por 0.0.0.0,

➢ # SMTP daemon options
O DaemonPortOptions=Port=smtp,Addr=0.0.0.0, Name=MTA

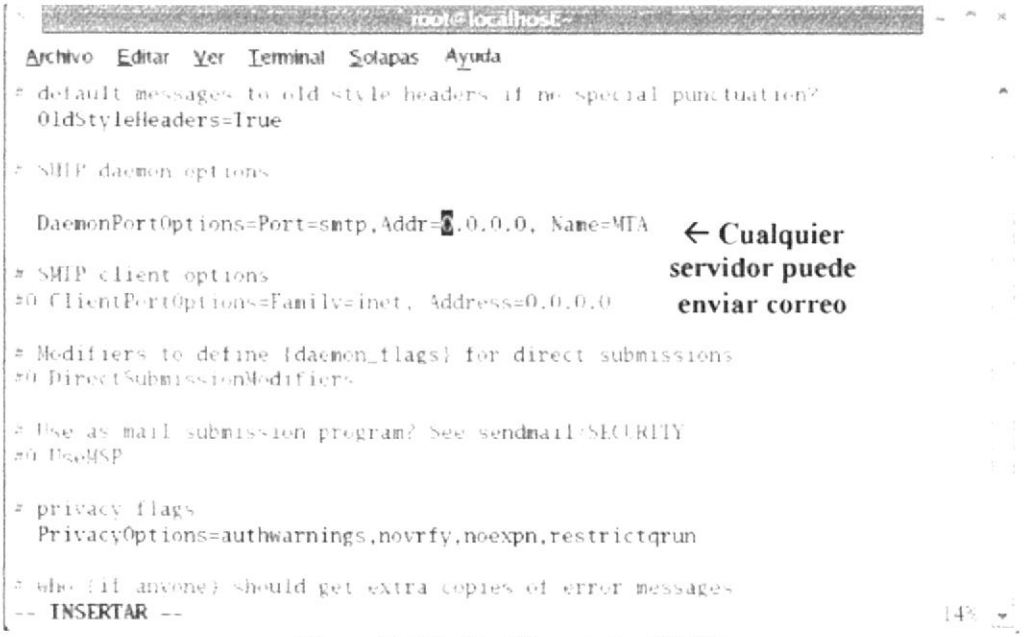


Figura 7-139: Modificando los SMTP

8. Habilite la linea de las opciones del cliente.
➢ # SMTP client options
O ClientPortOptions=Family=inet, Addr=0.0.0.0

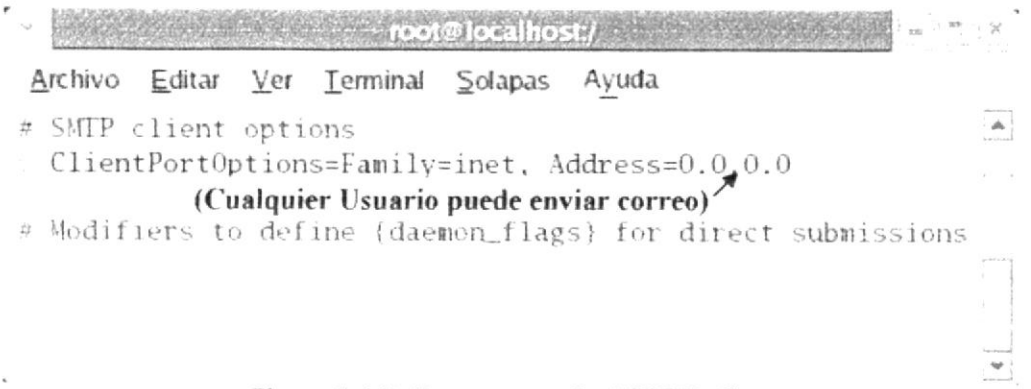


Figura 7-140: Descomentando el SMTP client

9. Luego edite el archivo del servicio Dovecot
   vi /etc/dovecot.conf

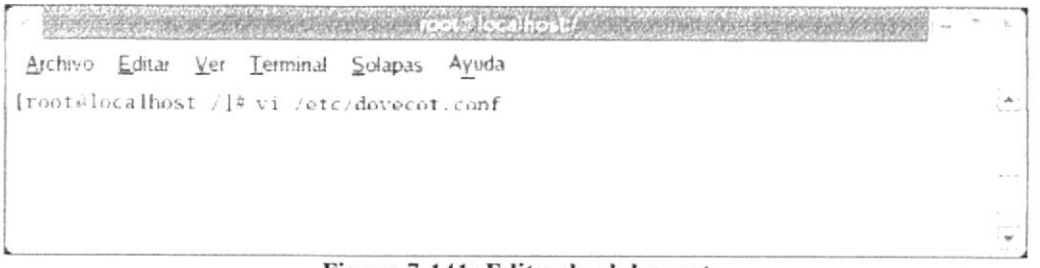


Figura 7-141: Editando el dovecot

10. Luego ingrese los parámetros y salga del editor.
    protocols = imap imaps pop3

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

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

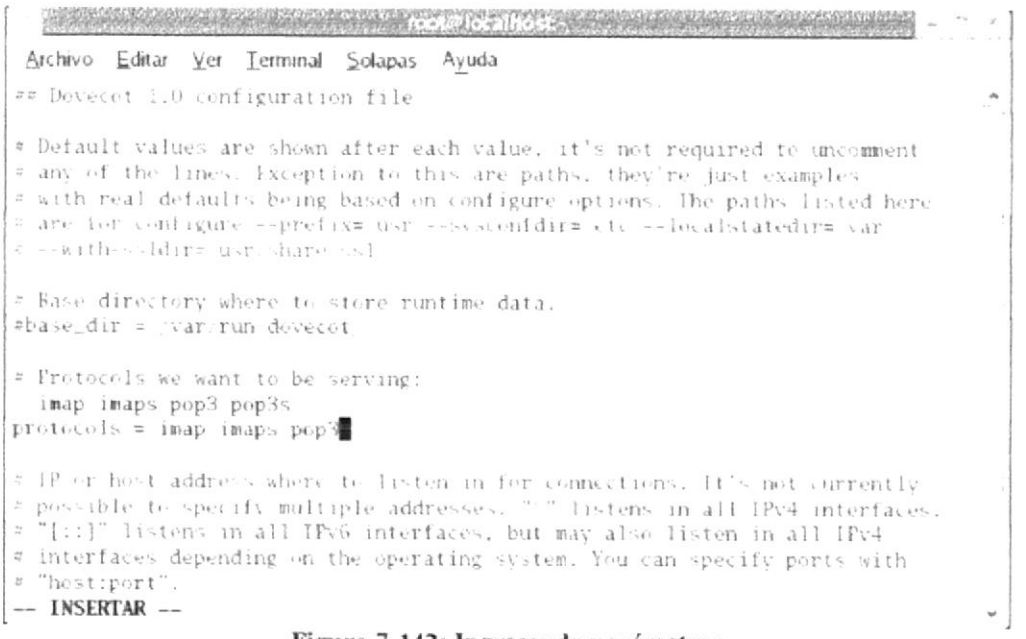


Figura 7-142: Ingresando parámetros

11. Luego inicie los servicios sendmail.

Figura 7-143: Iniciando los servicios sendmail

12. Luego inicie los servicios dovecot.

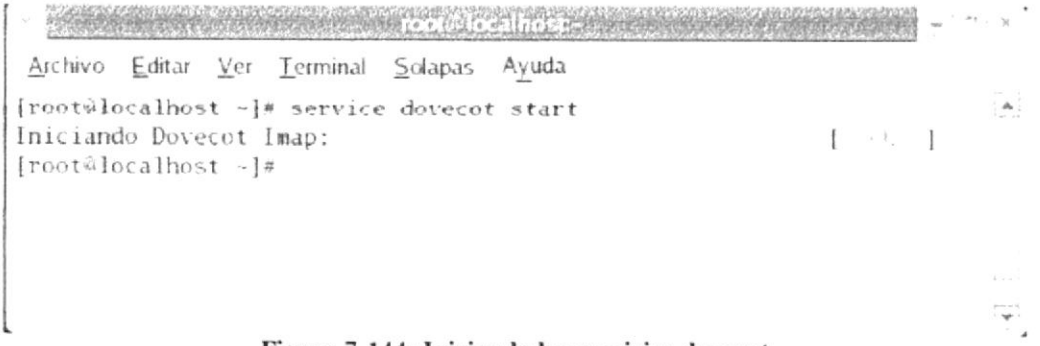


Figura 7-144: Iniciando los servicios dovecot

13. Puede verificar los puertos habilitados utilizando los siguientes comandos:
netstat –an | more, o netstat –plan | more
Deben estar habilitados los puertos 110 (POP3) y 25 (SMTP)

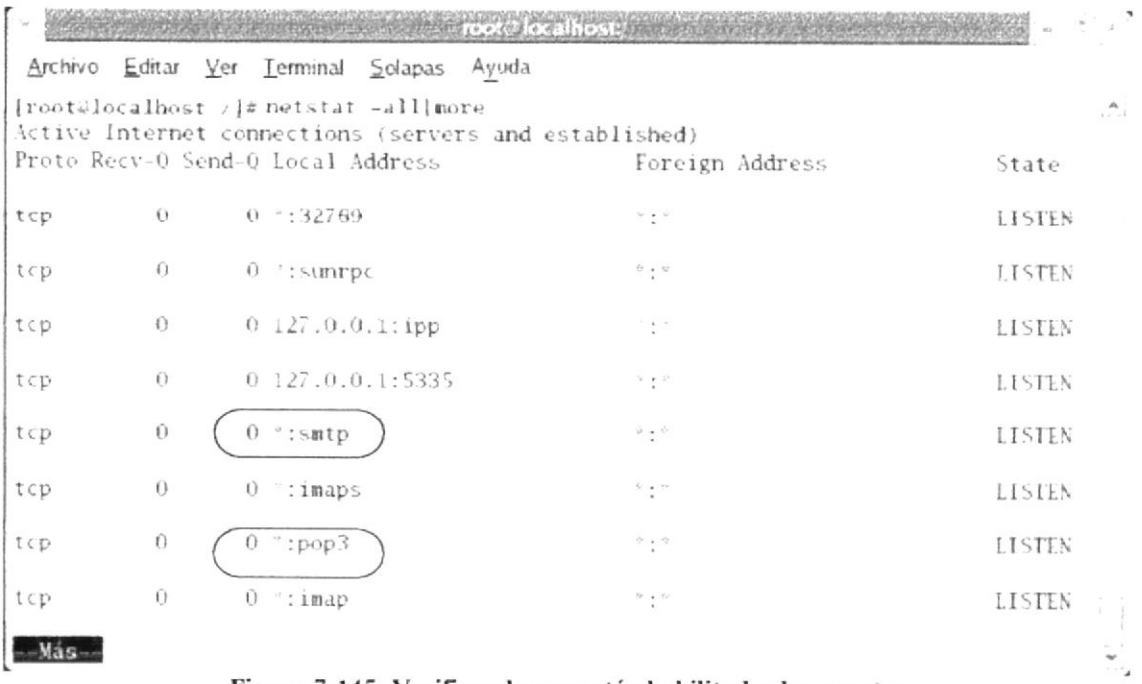


Figura 7-145: Verificando que estén habilitados los puertos

Sugerencia:

- Puede verificar si envia un mail al root
  [ ]# mail root@compuhelp.com
  Subject: nombre_usuario
  El mensaje tiene que finalizar con un punto
  .
  cc:/nombre_usuario2

- Puede revisar si existe un mail
  [ ]# mail

- Puede cambiar de usuario
  [ ]# su – nombre_usuario
  [ ]# su – regresa al root pidiendo clave.

7.12.4 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. Para que proceda a configurar el Outlook Express, de clic en inicio y elija la opción de correo electrónico (Outlook Express) dentro del menú inicio de Windows XP

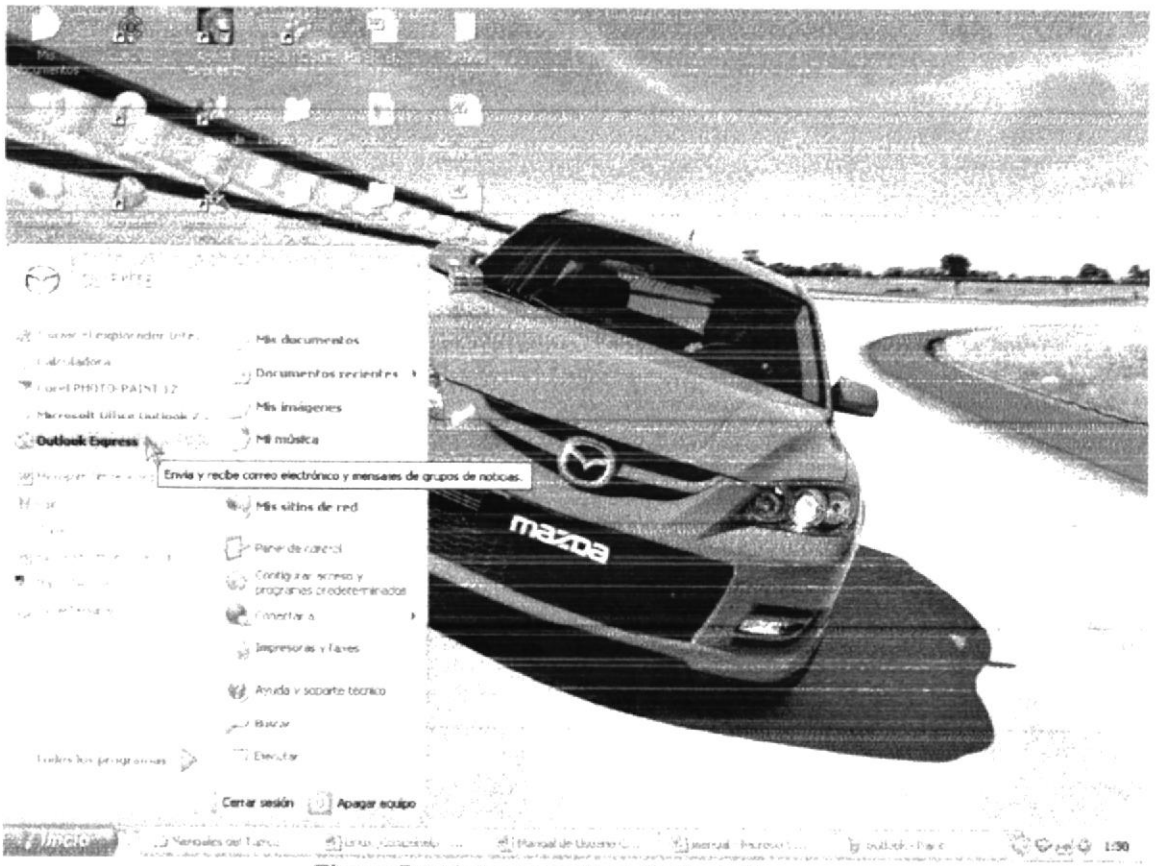


Figura 7-146: Ingresando al Outlook Express

2. Después le aparecerá la pantalla de bienvenida, que sale por defecto.

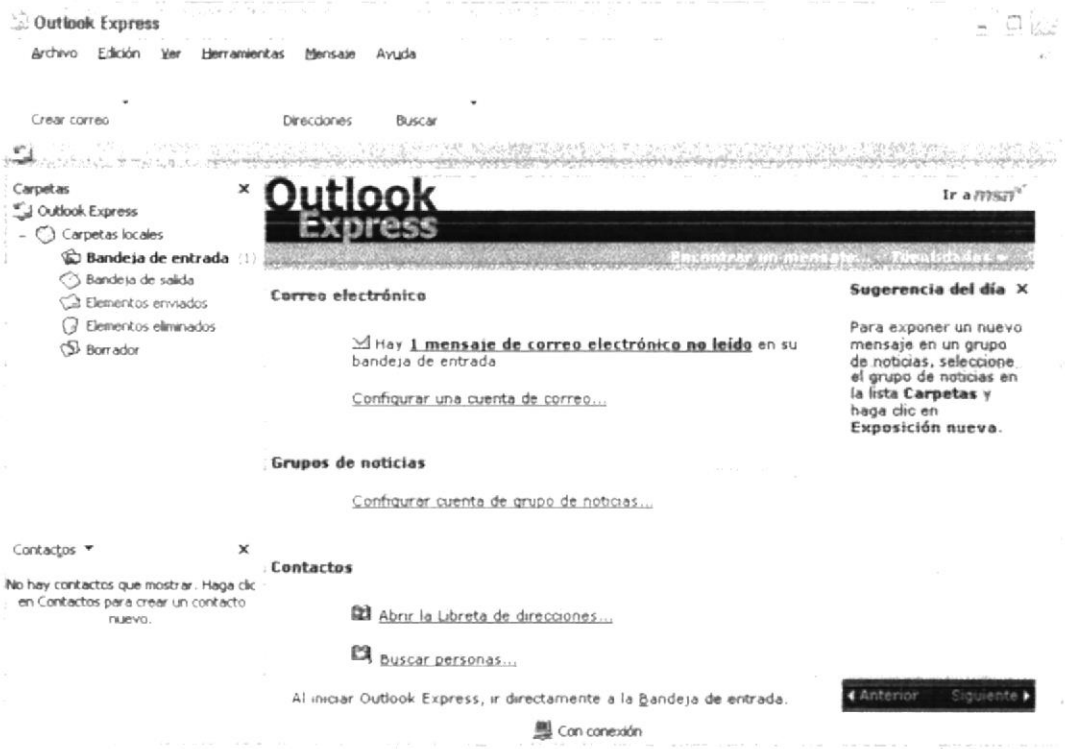


Figura 7-147: Pantalla de Bienvenida al Outlook Express

3. Luego de clic en herramientas y posteriormente seleccione cuentas de correos como se lo detalla a continuación.

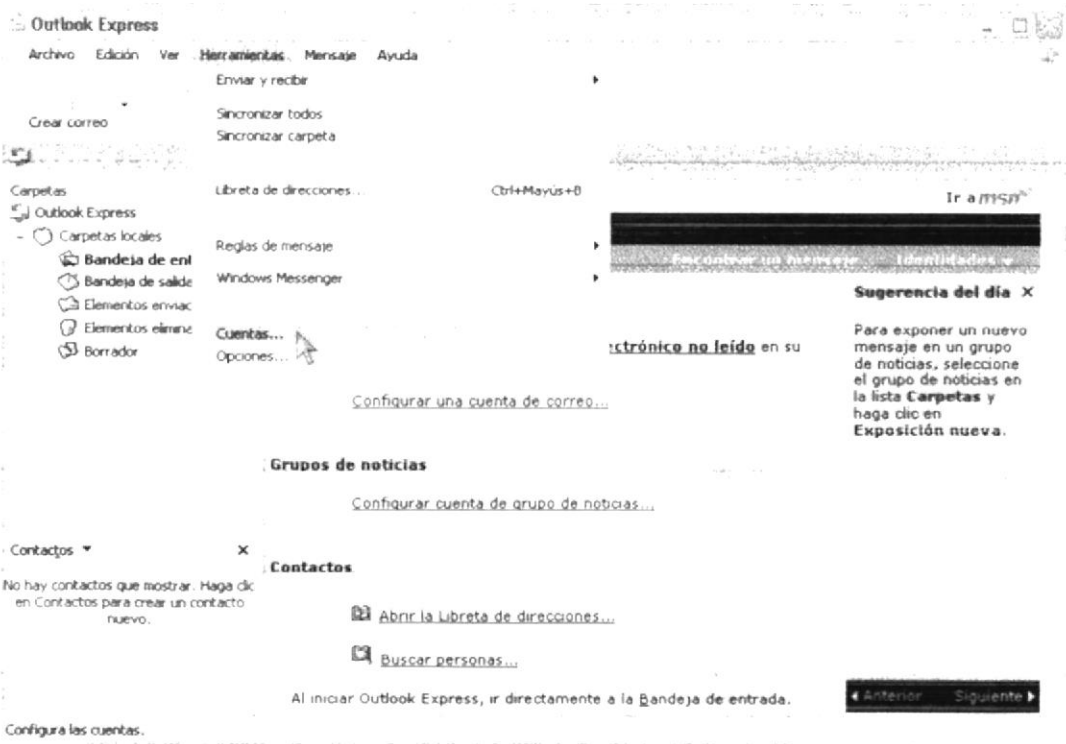


Figura 7-148: Configurar una cuenta de correo electrónico

4. Aparecerá la siguiente pantalla a manera de un asistente para poder configurar la nueva cuenta de correo electrónico, de clic en agregar y posteriormente elija la opción correo.

Figura 7-149: Agregar correo electrónico

5. Después que ingrese en Agregar correo el asistente le indicará que nombre desea que aparezca en su cuenta de correo, luego se irá a la siguiente pantalla, de clic en siguiente.

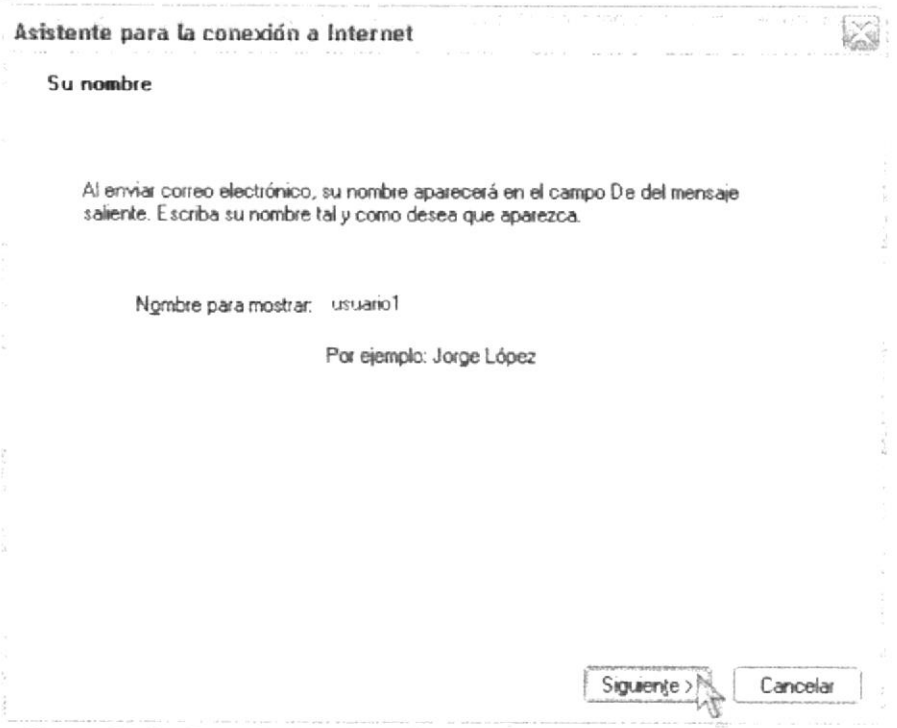


Figura 7-150: Pantalla de asignación de nombre a la cuenta de correo

6. Se colocará su dirección de correo asociado al usuario que creó en Linux, de clic en siguiente.

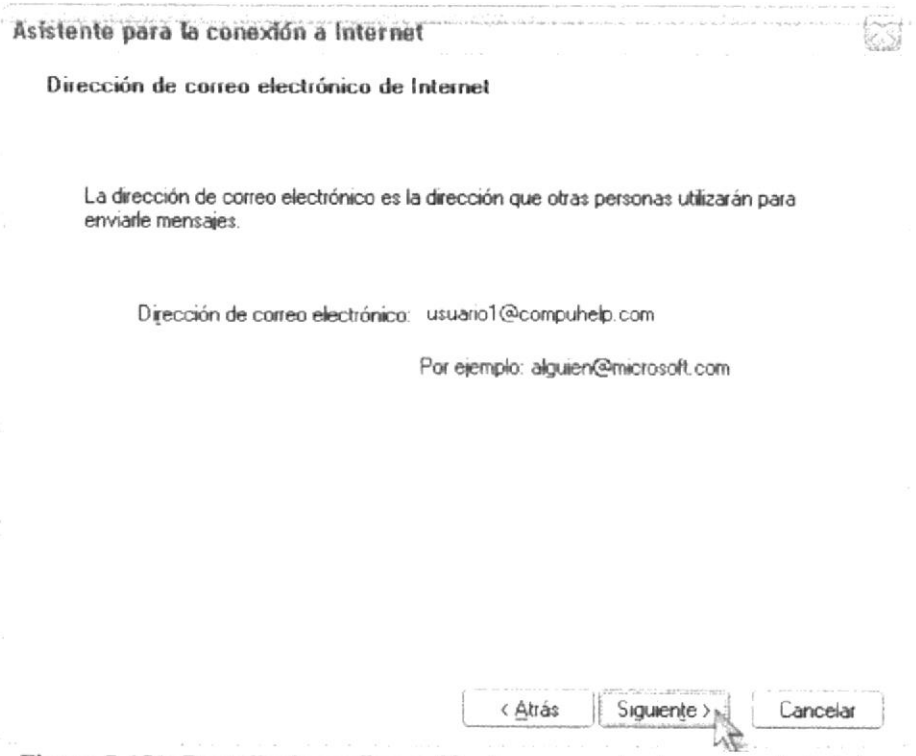


Figura 7-151: Pantalla de configuración de una cuenta de correo electrónico

7. Se especifica 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, luego de clic en siguiente

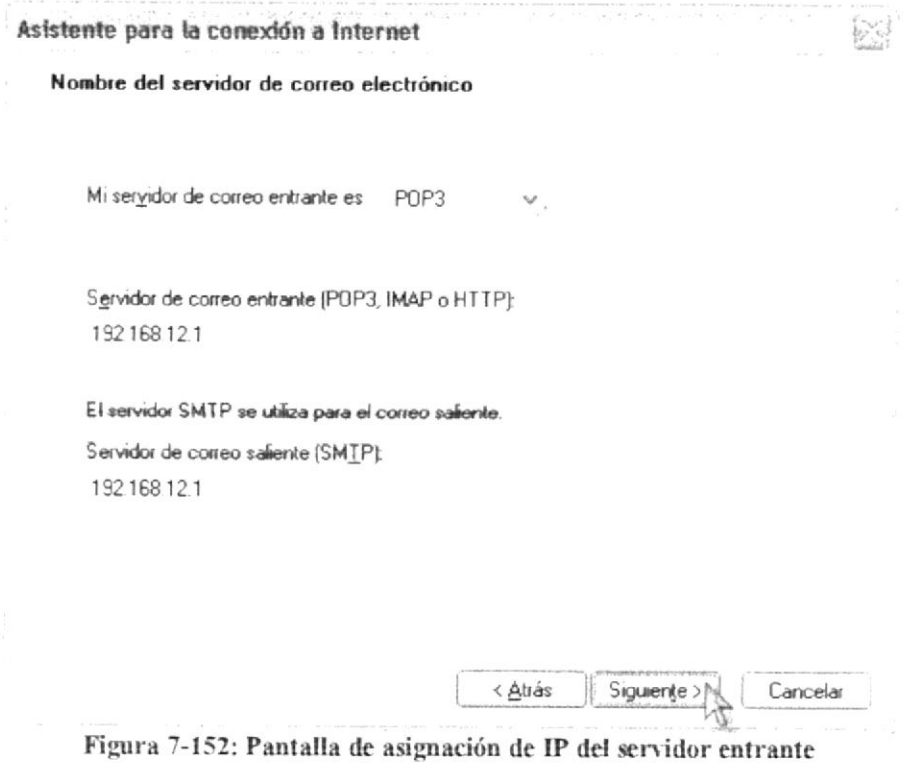


Figura 7-152: Pantalla de asignación de IP del servidor entrante

8. Ingrese el nombre de usuario y contraseña proporcionado por el servidor Linux, de clic en siguiente.

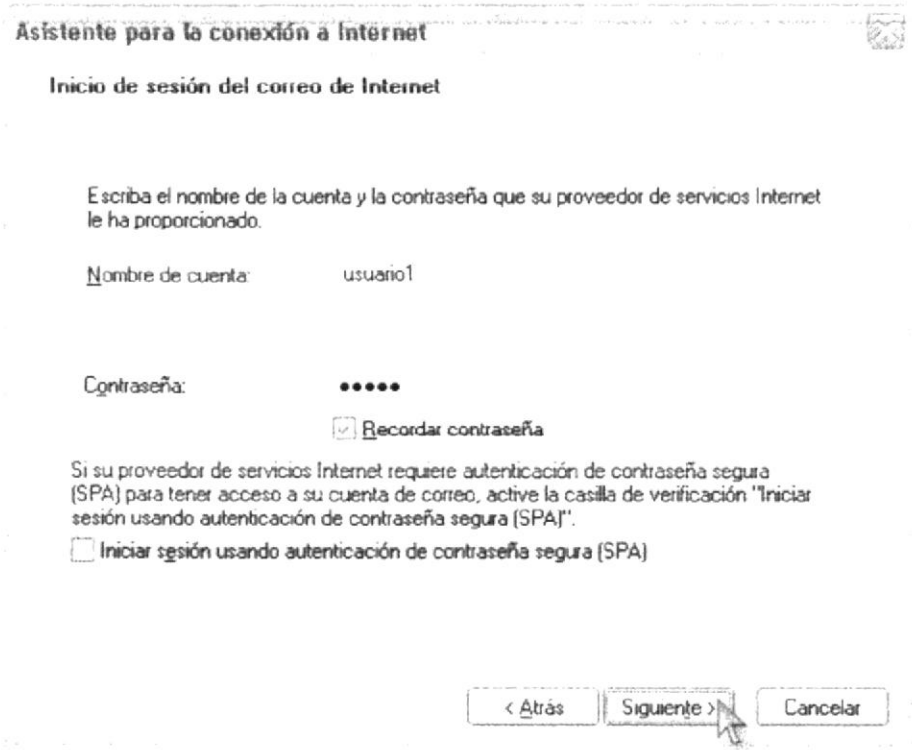


Figura 7-153: Pantalla de asignación de contraseña

9. De clic en finalizar para confirmar que la información escrita anteriormente es correcta.

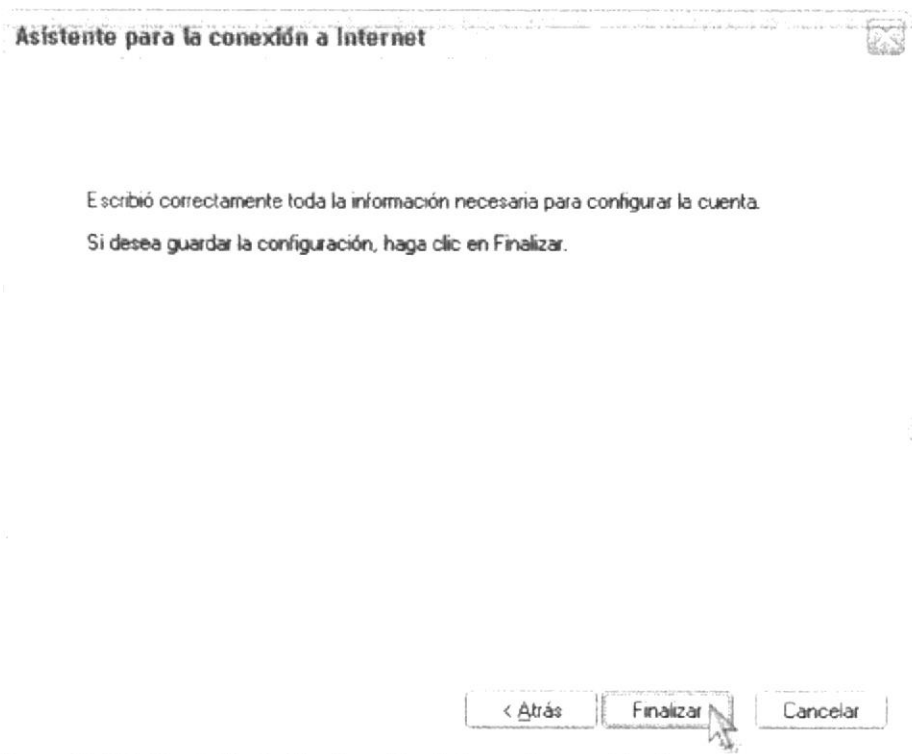


Figura 7-154: Pantalla de finalización de la configuración de una cuenta de correo

10. Terminada la configuración debe visualizar una pantalla con las cuentas de correo que existen, a la vez la cuenta que esta como predeterminada en este caso 192.168.12.1

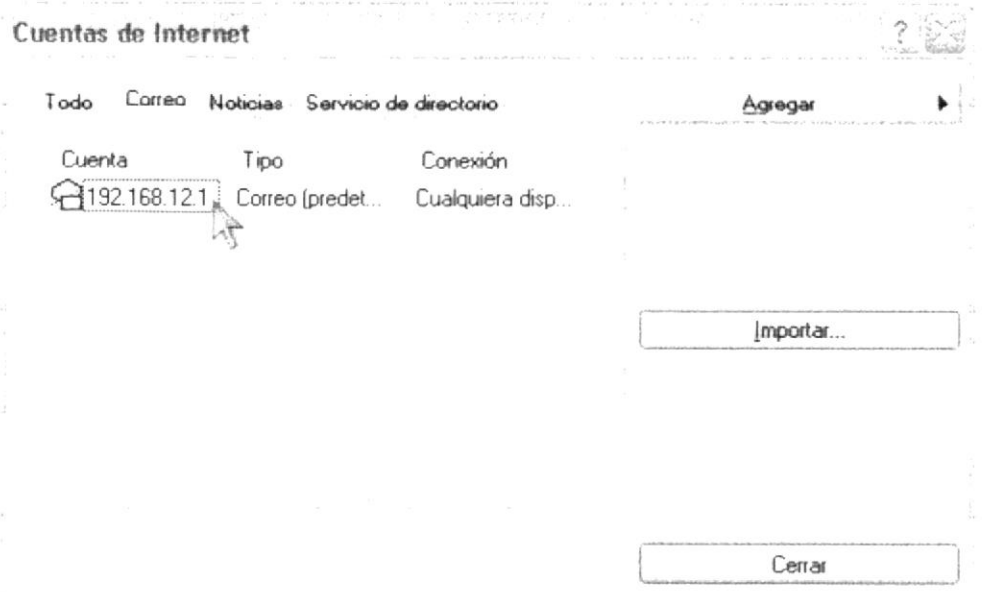


Figura 7-155: Listado de cuentas de correo electrónico configuradas

11. Para crear un mensaje de correo nuevo, de clic en archivo, seleccione nuevo y luego de clic en mensaje de correo.

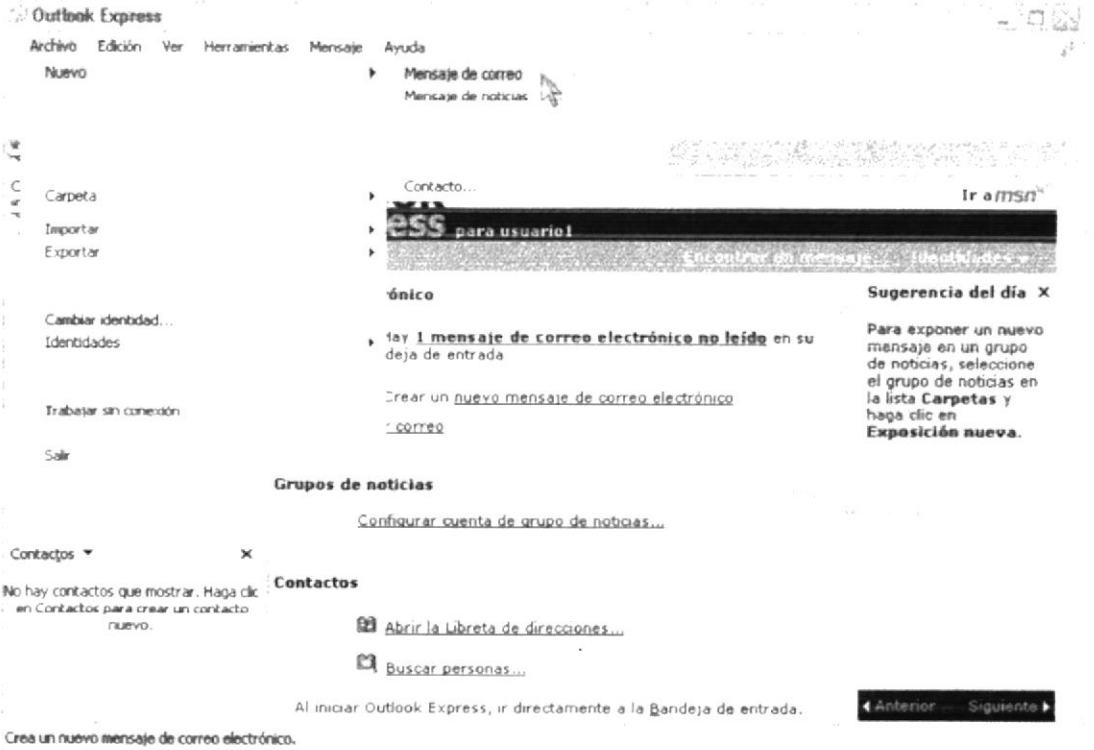


Figura 7-156: Crear un mensaje nuevo de correo

12. Pantalla que le permite enviar correos, ingrese el correo del administrador Linux y de clic izquierdo en enviar.

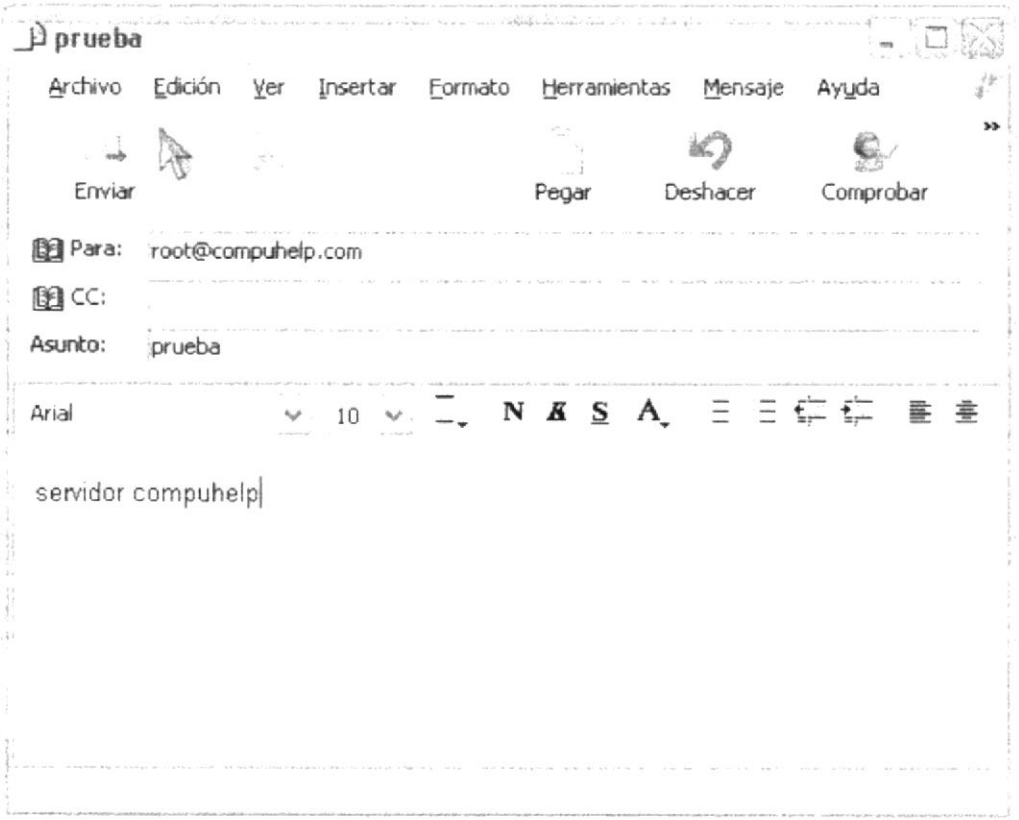


Figura 7-157: Prueba de correo

13. Pantalla de la bandeja de salida del correo que le muestra el mensaje enviado al servidor Linux.

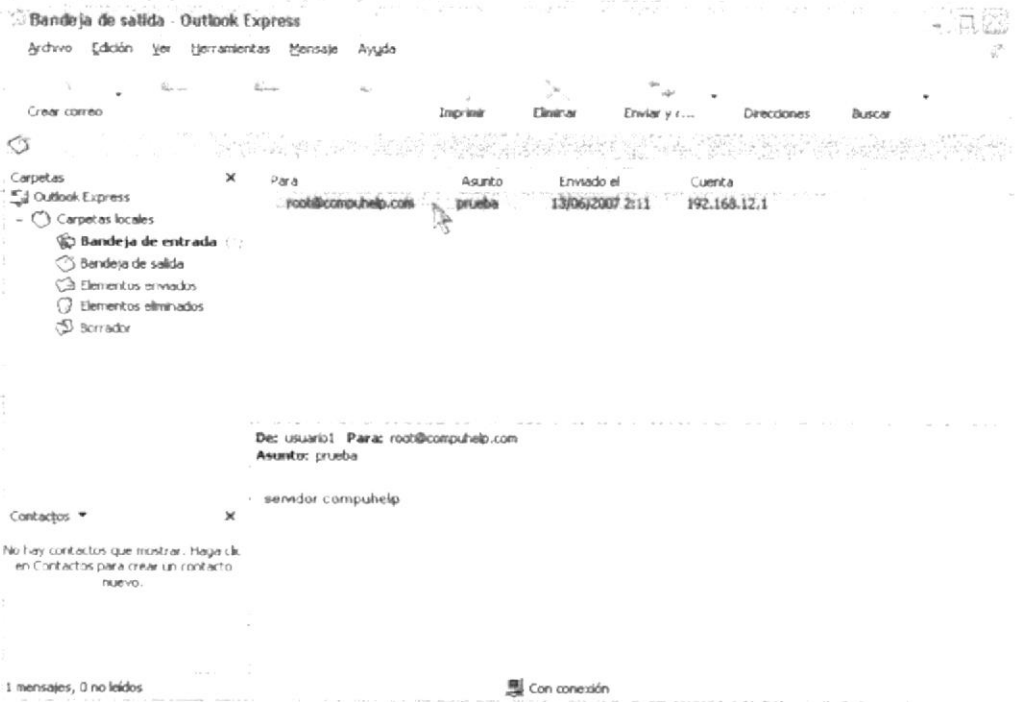


Figura 7-158: Bandeja de salida

14. Para realizar la prueba de envío y recepción de mensajes de correo, ingrese en el servidor el comando mail.

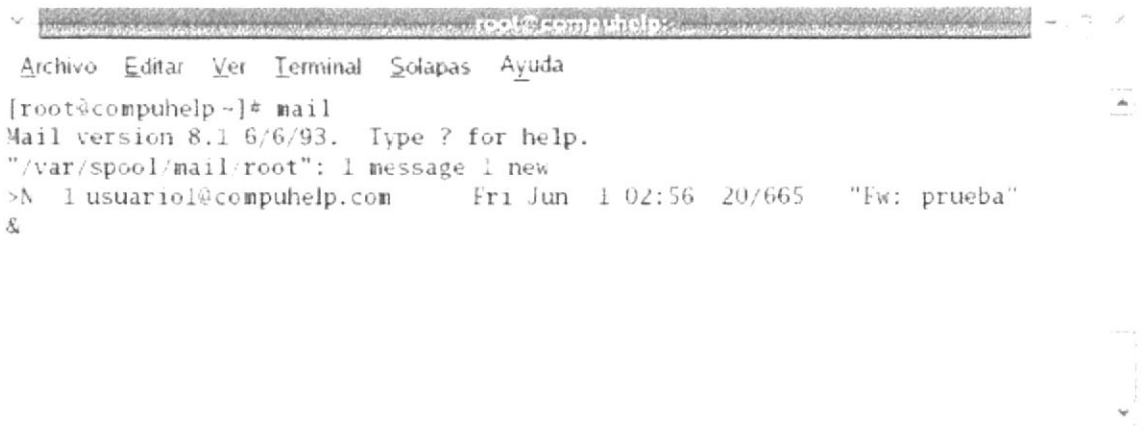


Figura 7-159: Comando mail

7.13 PROXY

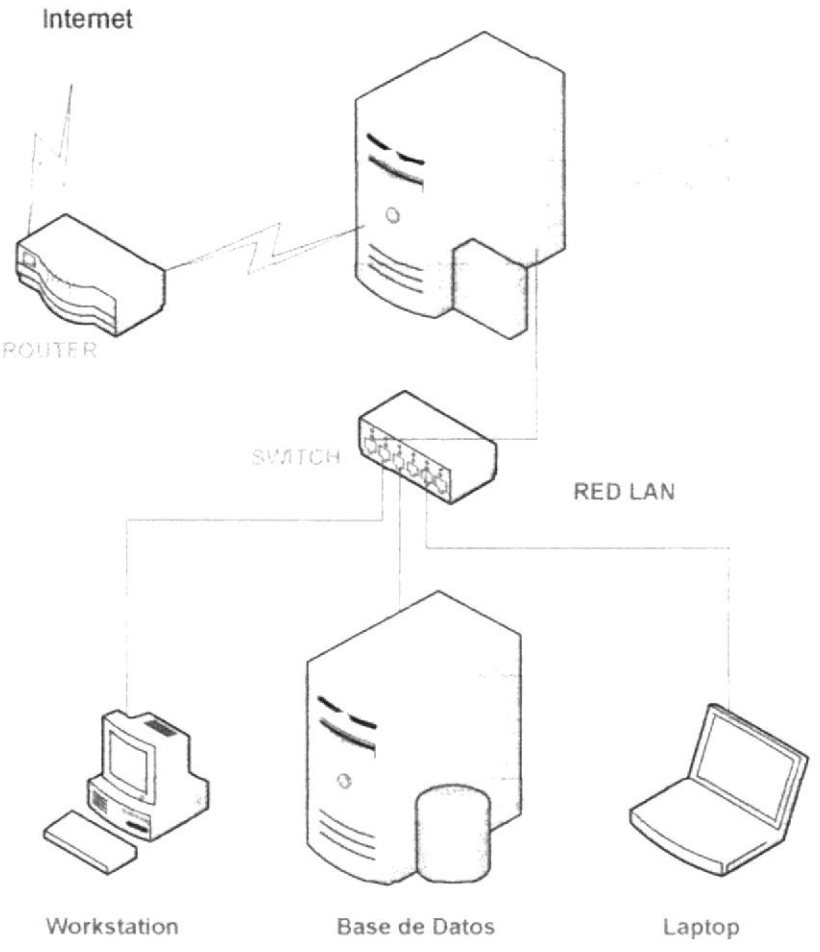


Figura 7-160: Como funciona Proxy

El servidor proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (Ej.: una página web) en una cache que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

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

Un Servidor Intermediario (Proxy) se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:
Cliente se conecta hacia un Servidor Intermediario (Proxy).
Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto.

Funciona como servidor de seguridad y como filtro de contenidos

Es un mecanismo de seguridad implementado por el ISP o los administradores de la red en un entorno de Intranet para desactivar el acceso o filtrar las solicitudes de contenido para ciertas sedes Web consideradas ofensivas o dañinas para la red y los usuarios.

Mejora el rendimiento

Guarda en la memoria caché las páginas Web a las que acceden los sistemas de la red durante un cierto tiempo. Cuando un sistema solicita la misma página web, el servidor proxy utiliza la información guardada en la memoria caché en lugar de recuperarla del proveedor de contenidos. De esta forma, se accede con más rapidez a las páginas Web.

Navegue a mayor velocidad

Acelere la navegación en su empresa e institución almacenando las páginas más visitadas.

Baje costos

Ahorre ancho de banda. Aproximadamente el 30% de los sitios visitados son siempre los mismos, por lo que guardándolos localmente en un Proxy Server se ahorra en el costo del enlace.

Aplique políticas de seguridad

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

Obtenga mayor información

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

Administre eficientemente la navegación

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

7.13.1 VENTAJAS

- Ahorro de Tráfico: Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.

- Velocidad en Tiempo de respuesta: El servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.

- Demanda a Usuarios: Puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.

- Filtrado de contenidos: El servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.

- Modificación de contenidos: Basándose en la misma función del filtrado, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

7.13.2 REQUERIMIENTOS PARA LA CONFIGURACIÓN DE UN PROXY SERVER

- Debe tener instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Debe haberle asignado una IP estática al servidor.

- Debe tener deshabilitado el firewall.

- Debe haber instalado el paquete squid el cual se verifica con el comando rpm –q squid.

7.13.3 CONFIGURACIÓN PROXY

1. Verifique si se encuentra instalado el servicio squid
   rpm -q squid

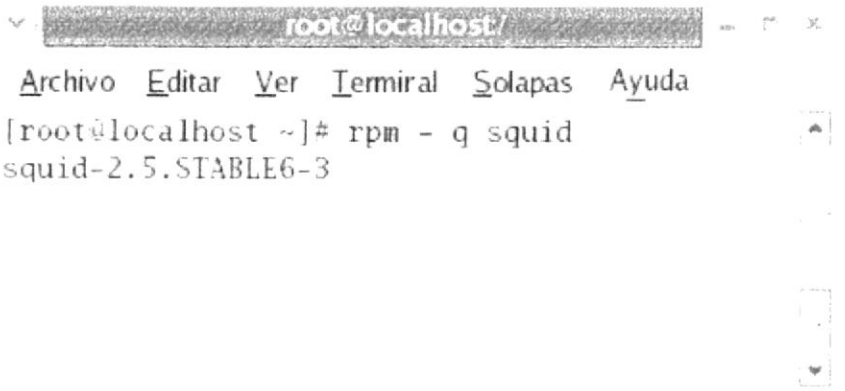


Figura 7-161: Verificación del paquete squid

2. Edite con el comando vi el archivo squid
   vi /etc/squid/squid.conf

Figura 7-162: Entrando a la configuración del squid

3. Busque la línea http_port y agregue una línea pero con el puerto 8080 por donde tendrá salida el Proxy.

   http_port 8080

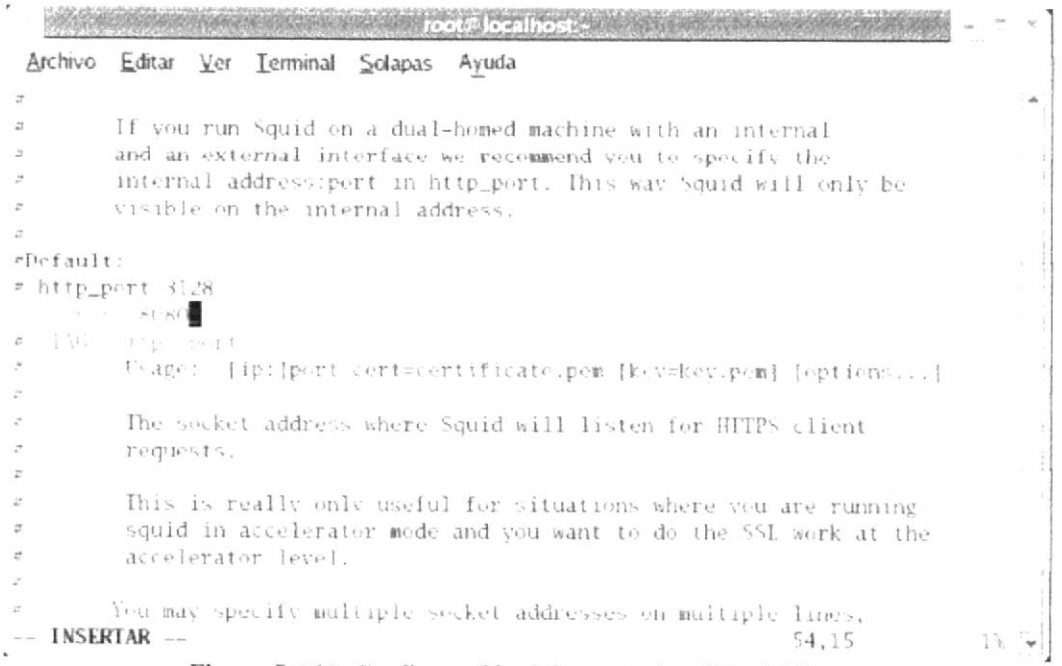


Figura 7-163: Configuración del puerto de salida del Proxy

4. Busque la línea cache_mem y agregue otra línea similar, pero con 16 MB.

   cache_mem 16 MB

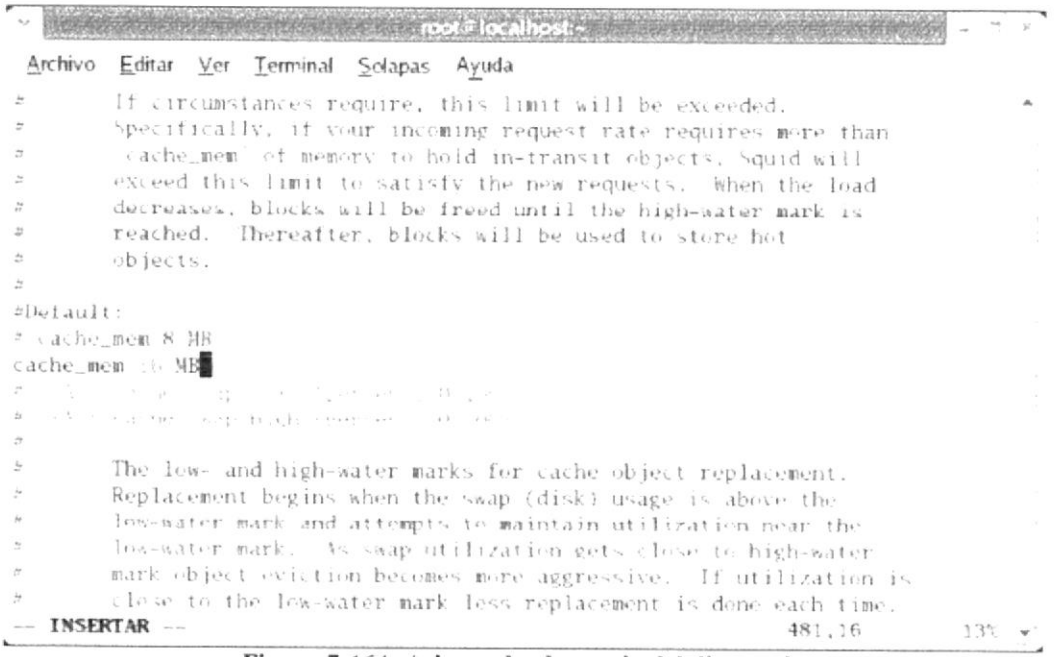


Figura 7-164: Asignando el espacio del directorio

5. Busque la línea cache_dir y luego habilítela, esta línea permite asignarle un directorio al proxy.

   cache_dir ufs /var/spool/squid 100 16 256

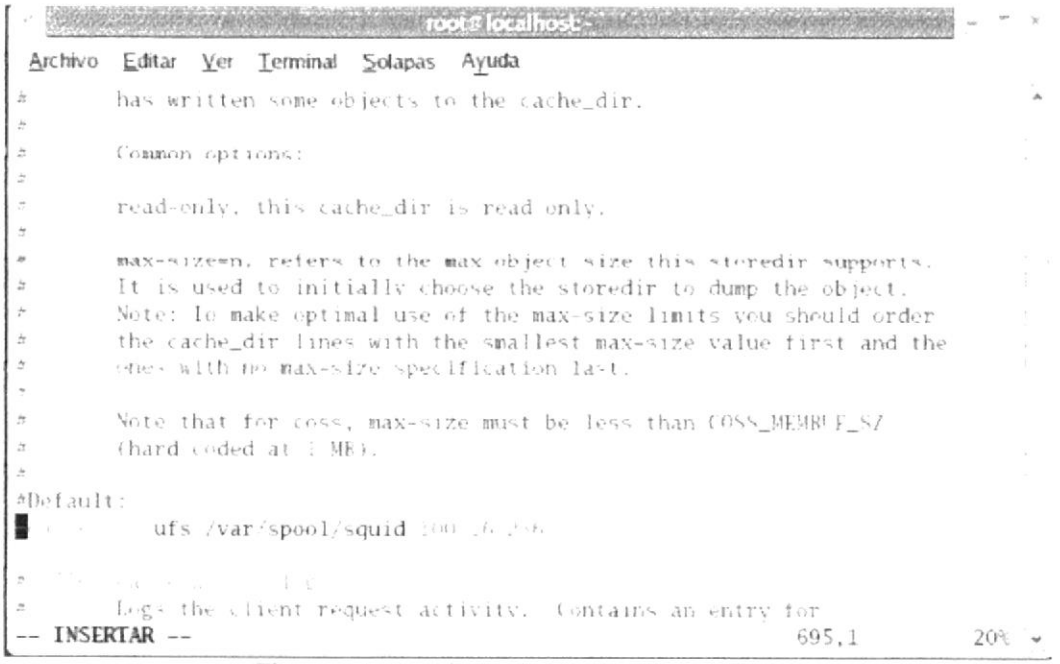


Figura 7-165: Asignando un directorio al Proxy

6. Busque las líneas de acl, para que agregue las líneas con el puerto por donde va a salir el Proxy y el segmento al que pertenece.

   acl puerto myport 8080 → Puerto que va a usar el servidor.
   acl mired src 192.168.12.1 /255.255.255.0 → Control de acceso a Internet

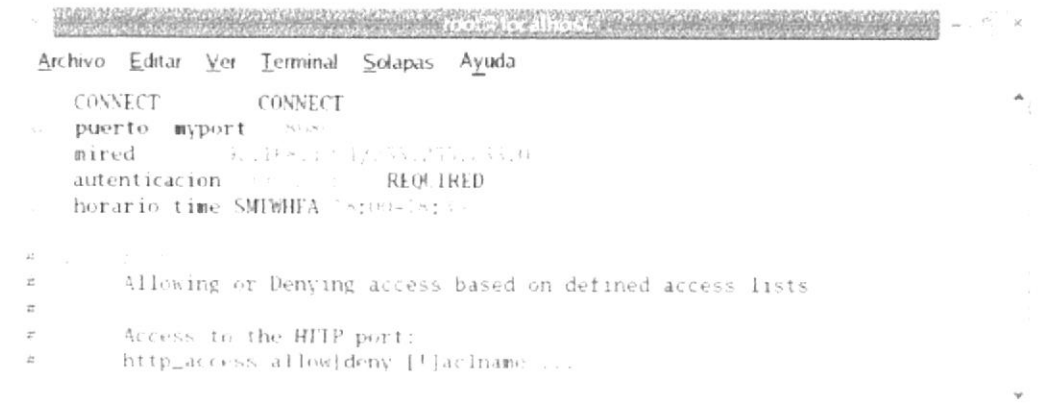


Figura 7-166: Creación de las ACL (Listas de Acceso)

7. Incluya las listas en las reglas de control de acceso, debe tener en cuenta el orden en que ubica sus reglas.

   http_acces allow puerto mired → Orden de lectura de las acl

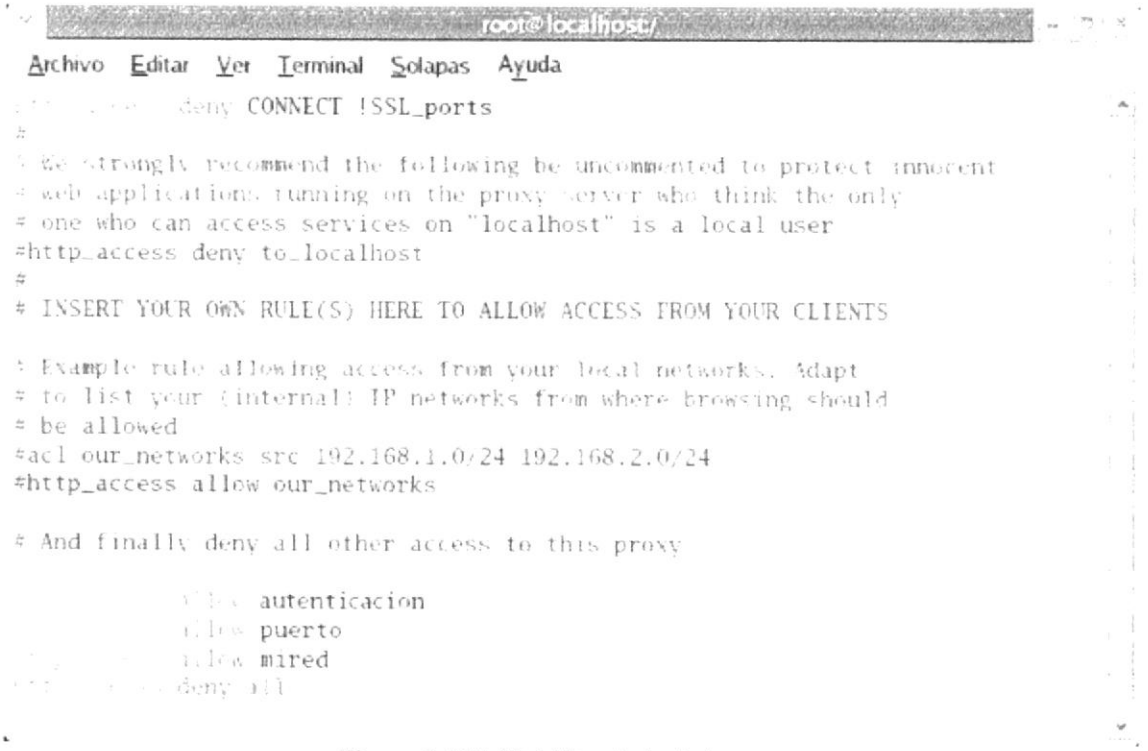


Figura 7-167: Habilitando la Acl

8. Inicie los servicios de squid
   service squid restart

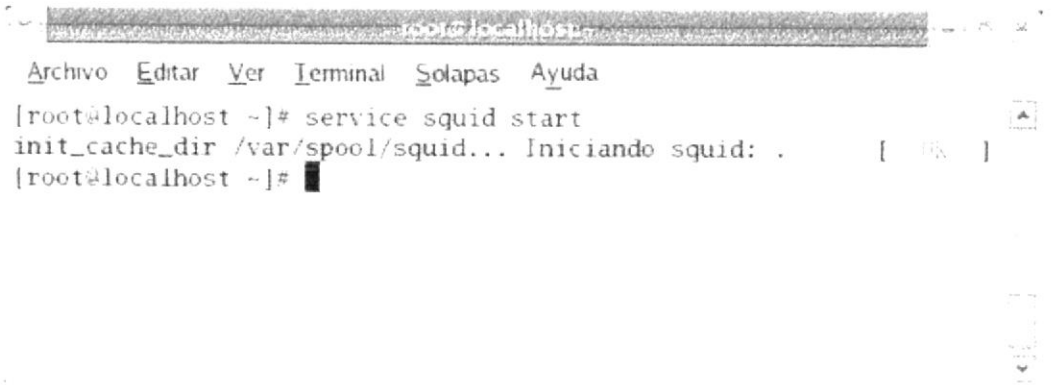


Figura 7-168: Iniciando los servicios del squid

7.13.4 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. Abra Internet Explorer, elija Menú / Herramientas / Opciones de Internet

Figura 7-169: Ingresando a las opciones del Internet

2. Seleccione dando un clic en conexiones.

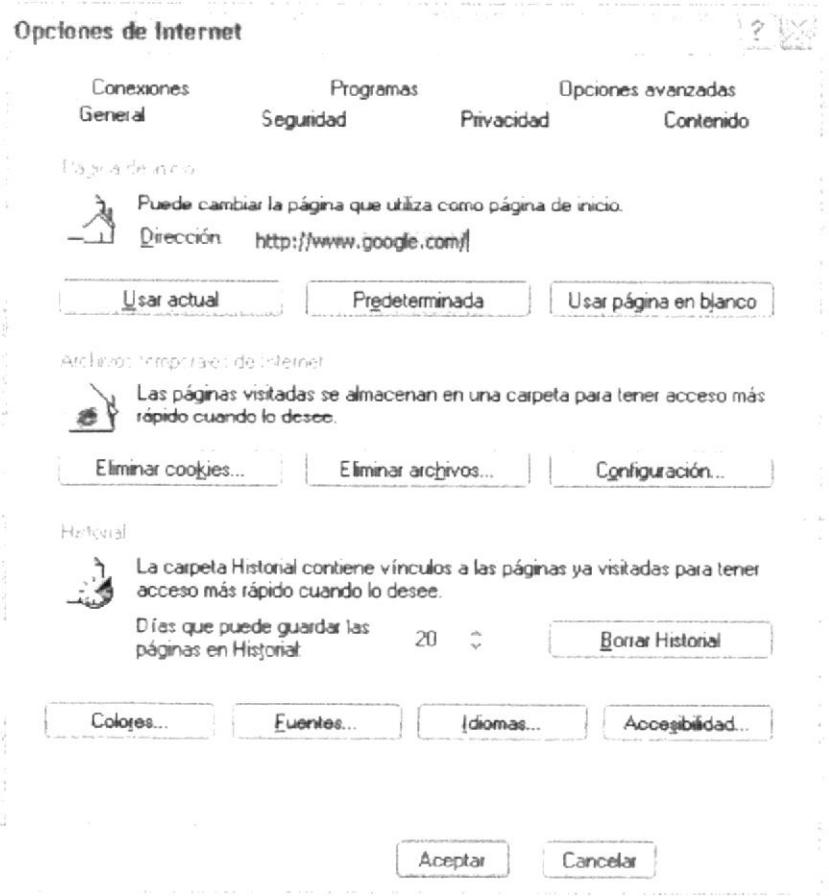


Figura 7-170: Seleccionando la opción de conexiones

3. De clic izquierdo en el botón de configuración de LAN.

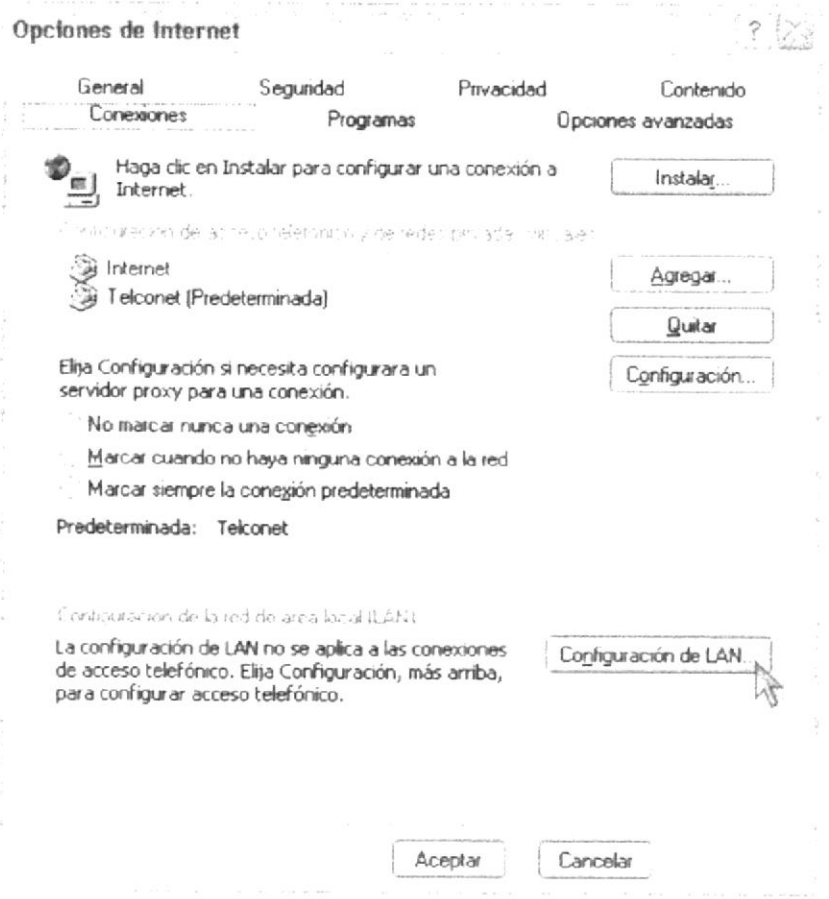


Figura 7-171: Ingresando a la Configuración LAN

4. Ingrese la dirección 192.168.12.1 (IP del servidor) Puerto 8080

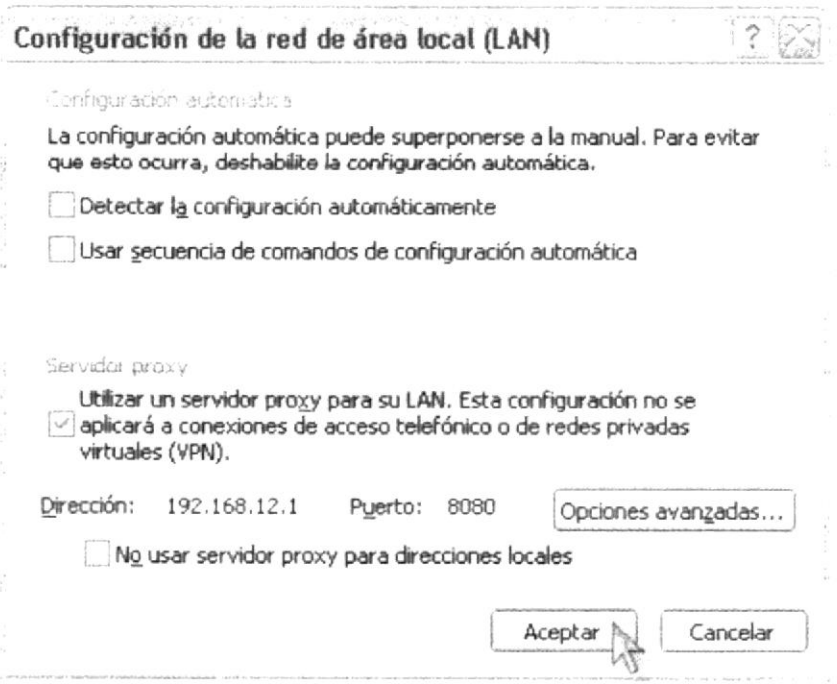


Figura 7-172: Ingresando la Ip del Servidor y el puerto de salida

5. Para comprobar cargue en el explorador su dominio.

Figura 7-173: Prueba exitosa de la configuración Proxy

7.13.4.1 DENEGAR ACCESOS A INTERNET POR HORA

1. Incluya las listas de control de acceso (acl)
   acl (nombre de la lista) time (dia) (hora inicio)-(hora fin)
   Ejm: acl horario time SMTWHFA 18:00-18:30
   acl (nombre de la regla) src (ip de la red o la máquina a restringir)
   Ejm: acl mired src 192.168.12.2/255.255.255.0

   Los días están determinados por las letras

Lunes	M	Viernes	F
Martes	T	Sábado	A
Miércoles	W	Domingo	S
Jueves	H		

Sugerencia:
Puede combinar los días para los accesos. La hora inicio y hora fin debe ser asignados en formato 24:00

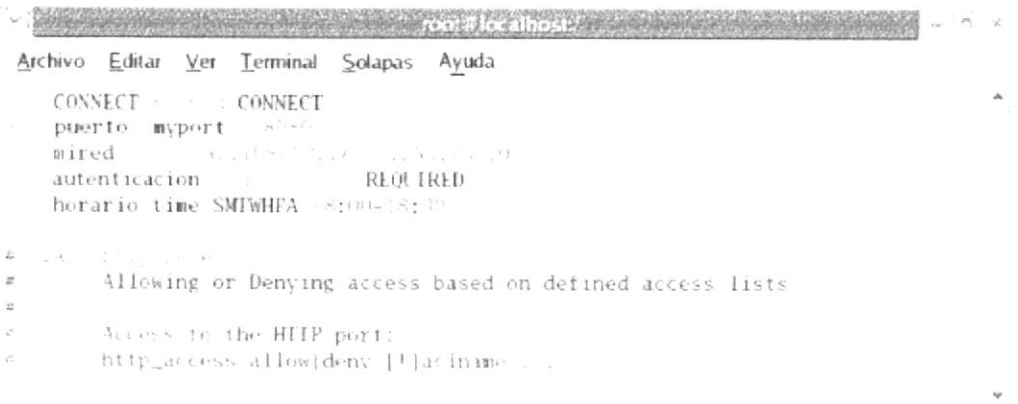


Figura 7-174: Creando las listas de acceso

2. Incluya las listas en las reglas de control de acceso
   http_acces deny! horario

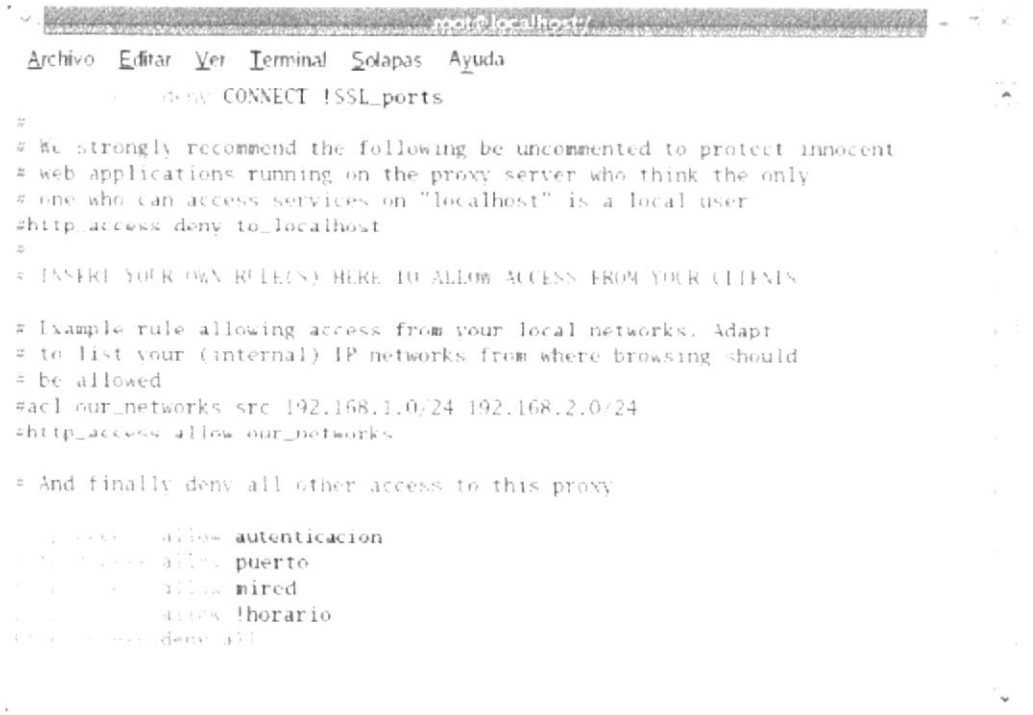


Figura 7-175: Reglas de control de acceso por horario

3. Reinicie los servicios de squid
   service squid restart

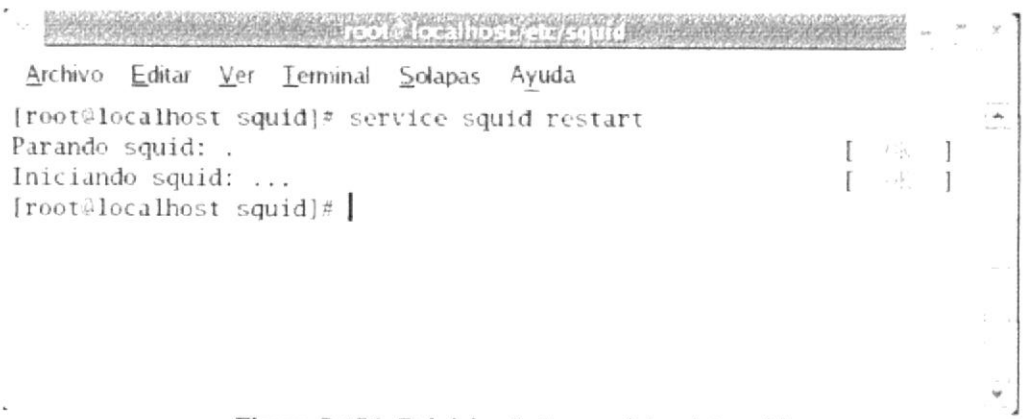


Figura 7-176: Reiniciando los servicios del squid

7.13.4.2 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. Para verificar la configuración en el cliente Windows, de clic en el icono de Internet Explorer.

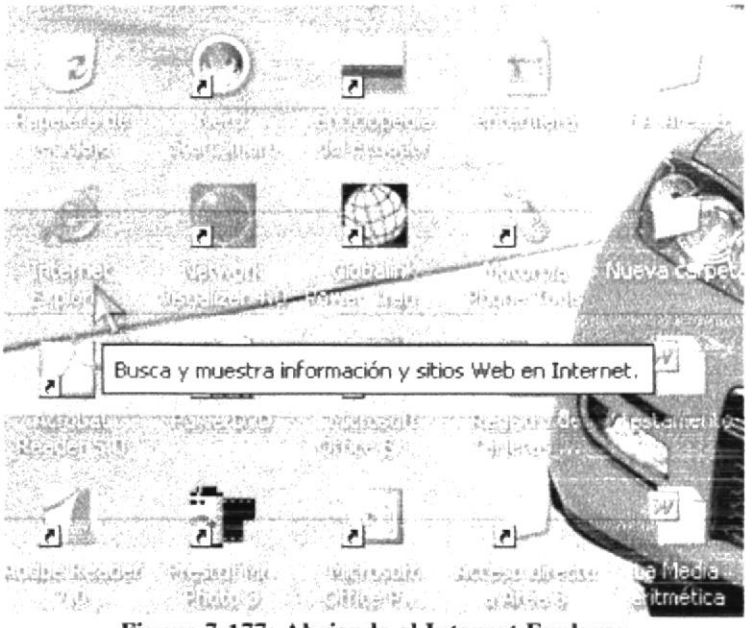


Figura 7-177: Abriendo el Internet Explorer

2. Luego le aparecerá una pantalla con un mensaje de error, por restricción del administrador.

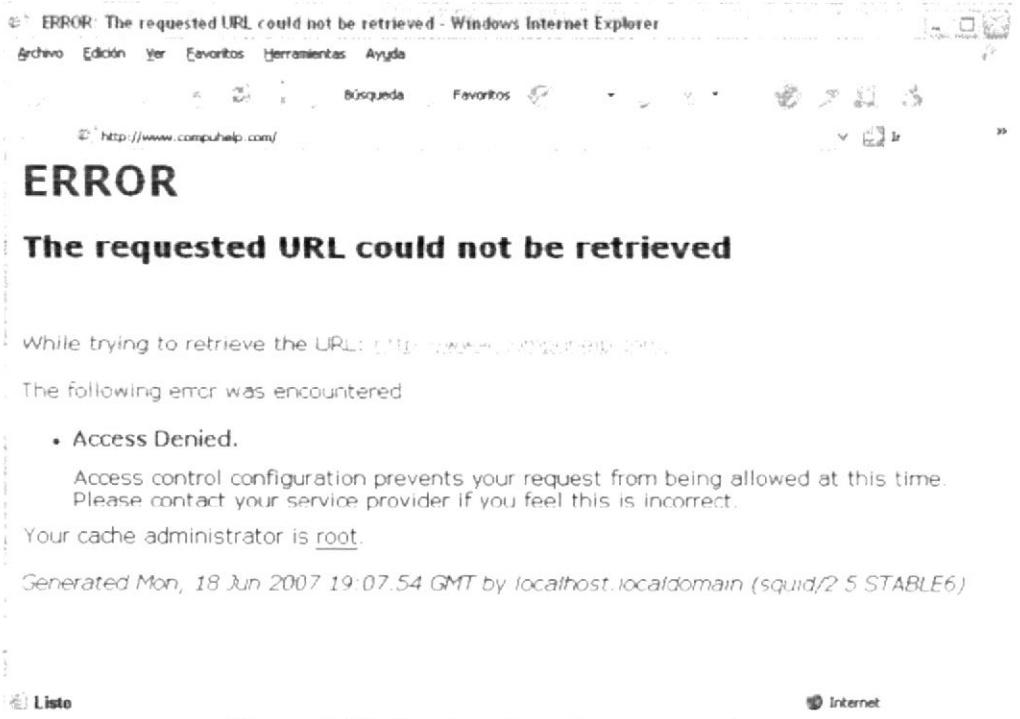


Figura 7-178: Prueba exitosa del proxy por hora

7.13.4.3 REGLAS DE ACCESO PARA AUTENTICACIÓN

1. Cree un archivo para las claves
   touch claves

2. Levante los permisos para el archivo
   chmod 600 claves

3. Cambie de propietario al archivo
   chown squid:squid /etc/squid/claves

4. Asigne las contraseñas
   htpasswd /etc/squid/claves usuario1

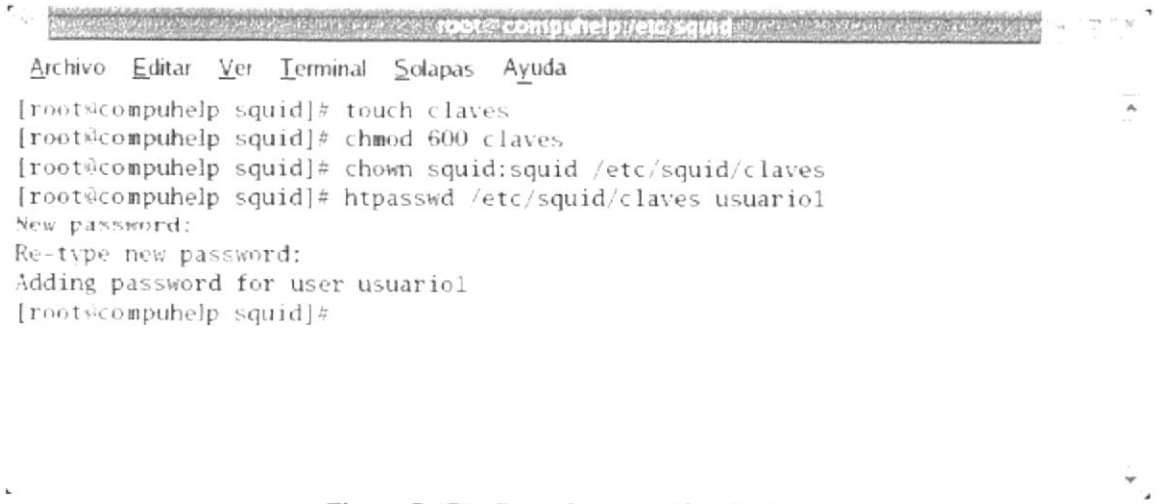


Figura 7-179: Creando un archivo de claves

5. Edite el archivo squid

   Sugerencias:
   Especificamos la ruta del programa básico de parámetros de autentificación y ruta de contraseñas.
   auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves

(Programa de autentificación) – (Ruta del Programa) – (Cuentas y claves de acceso)

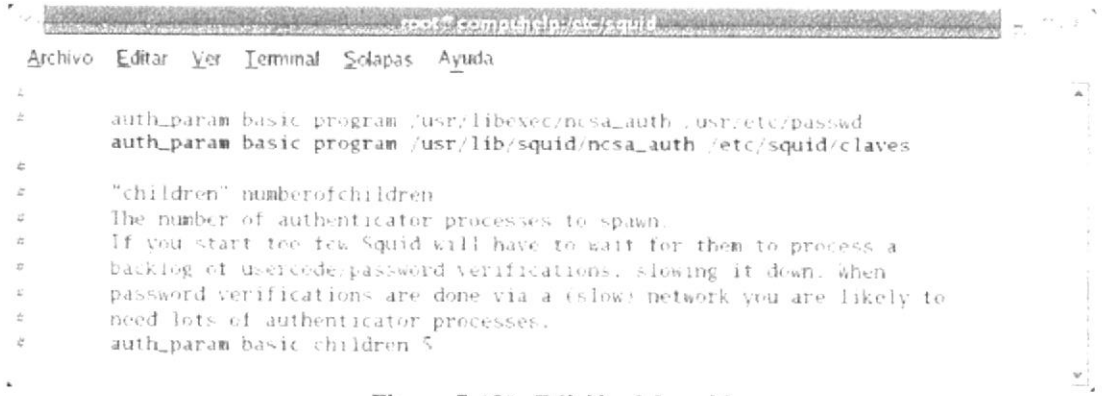


Figura 7-180: Edición del squid

6. Incluya la lista de control de acceso
   acl autenticación proxy_auth REQUIRED

```
root@localhost:/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
    CONNECT -     CONNECT
    puerto  myport    9000
    mired     192.168.10.0/255.255.255.0
    autenticacion  proxy_auth  REQUIRED
    horario time SMTWHFA 08:00-18:30

#  TAG: http_port
#       Allowing or Denying access based on defined access lists
#
#       Access to the HTTP port:
#       http_access allow|deny [!]aclname ...
```

Figura 7-181: Listas de acceso

7. Incluya las reglas de control de acceso
   http_access allow autenticación

```
root@localhost:/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
#       http_access deny CONNECT !SSL_ports
#
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks.  Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks

# And finally deny all other access to this proxy

http_access allow autenticacion
http_access allow puerto
http_access allow mired
http_access deny all
```

Figura 7-182: Reglas de control de acceso

8. Luego reinicie los servicios del squid
   service squid restart

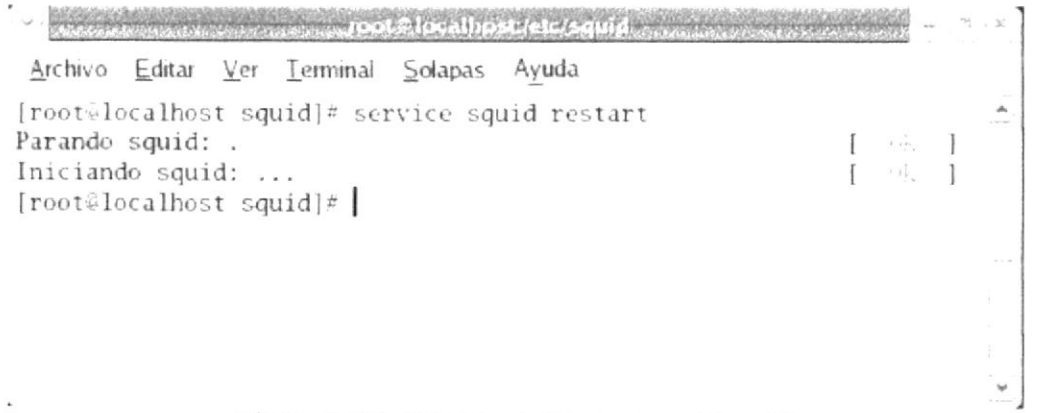


Figura 7-183: Reiniciando los servicios del squid

7.13.4.4 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. Para verificar la configuración en el cliente Windows, de clic en el icono de Internet Explorer.

Figura 7-184: Abriendo el Internet Explorer

2. Luego le aparecerá una pequeña ventana, indicándole que ingrese el usuario y el password creado en el proxy.

Figura 7-185: Ingresando el usuario para autentificación

7.13.4.5 DENEGAR ACCESO A LAS PÁGINAS PROHIBIDAS

1. Edite con el vi el archivo squid

2. Incluya la lista de control de acceso
   acl pagina url_regex "/etc/squid/pagina"

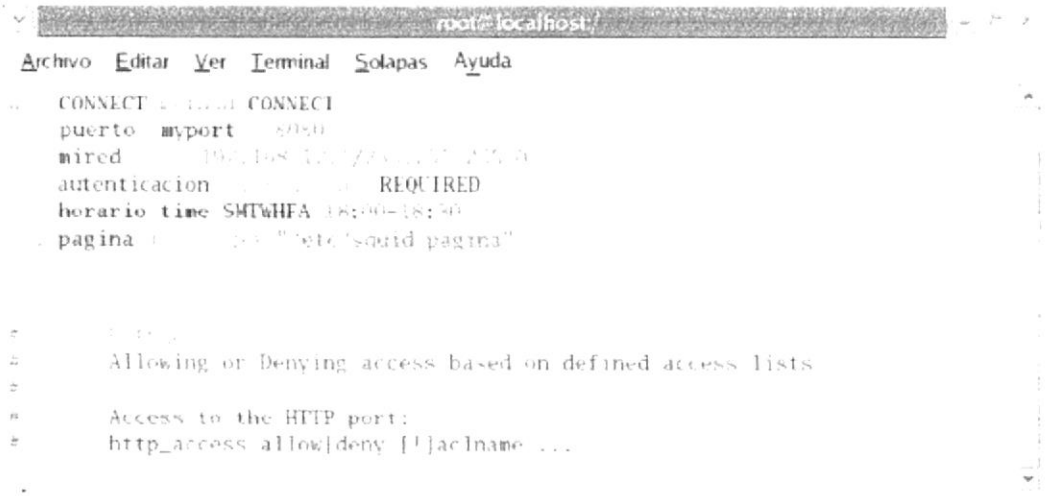


Figura 7-186: Control de acceso de páginas prohibidas

3. Incluya las reglas de control de acceso
   http_access deny !página

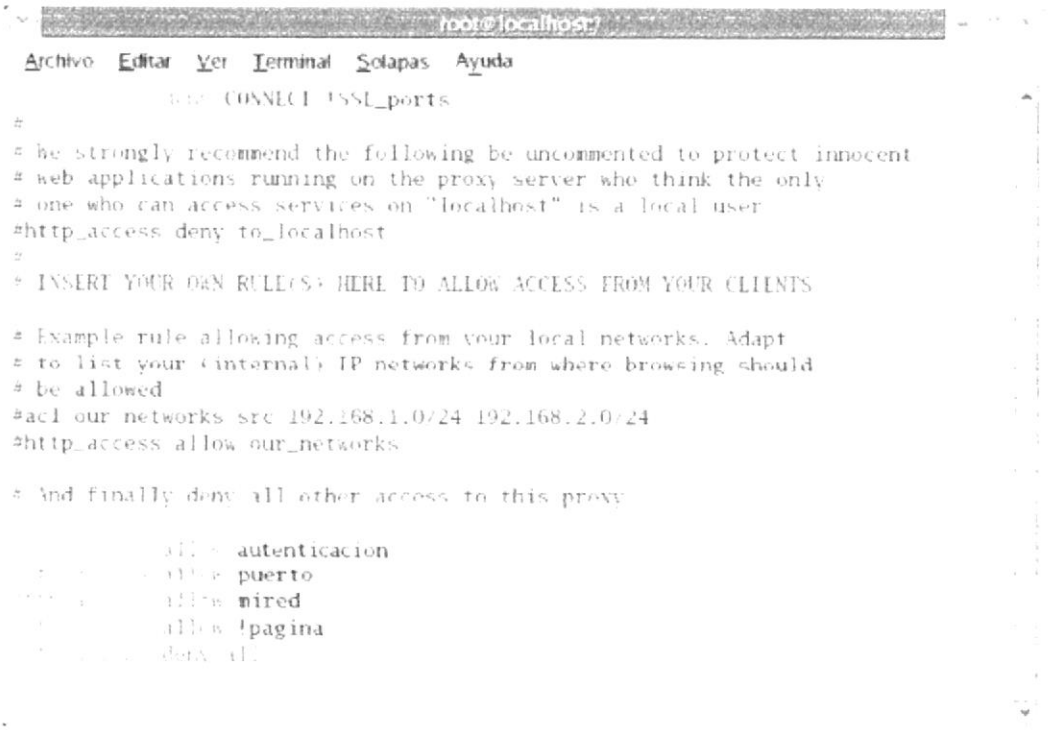


Figura 7-187: Reglas de control de páginas prohibidas

4. Cree el archivo que contiene los nombres de sitios prohibidos
   touch denegados

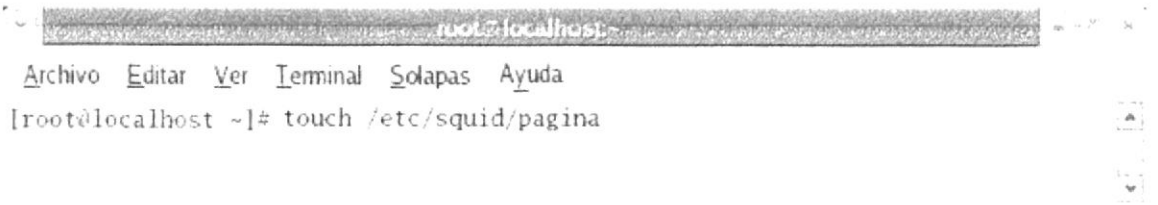


Figura 7-188: Creando un archivo para los sitios

5. Edite el archivo de páginas prohibidas
   vi /sitios/denegados

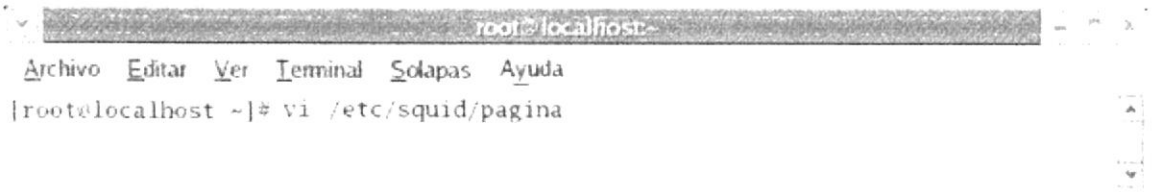


Figura 7-189: Editando el archivo de sitios

6. Luego ingrese las dirección de las páginas webs prohibidas.

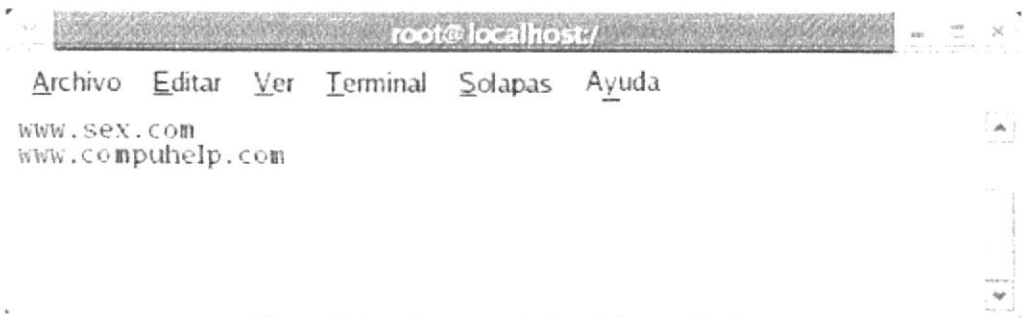


Figura 7-190: Ingresando los sitios prohibidos

7. Reinicie los servicios del squid con la siguiente linea de comandos:
   service squid restart

Figura 7-191: Reiniciando los servicios del squid

7.13.4.6 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. Para verificar la configuración en el cliente Windows, de clic en el icono de Internet Explorer.

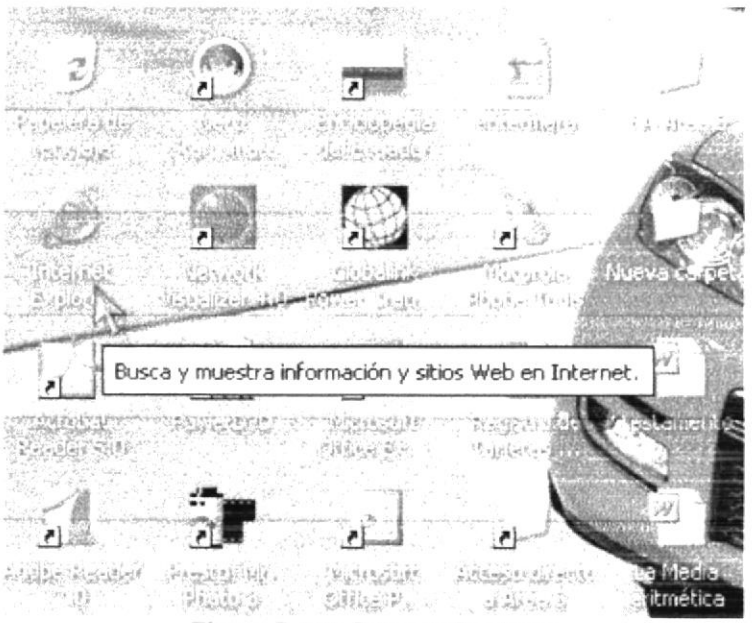


Figura 7-192: Internet Explorer

2. Luego le aparecerá una pantalla con un mensaje de error, por restricción del administrador.

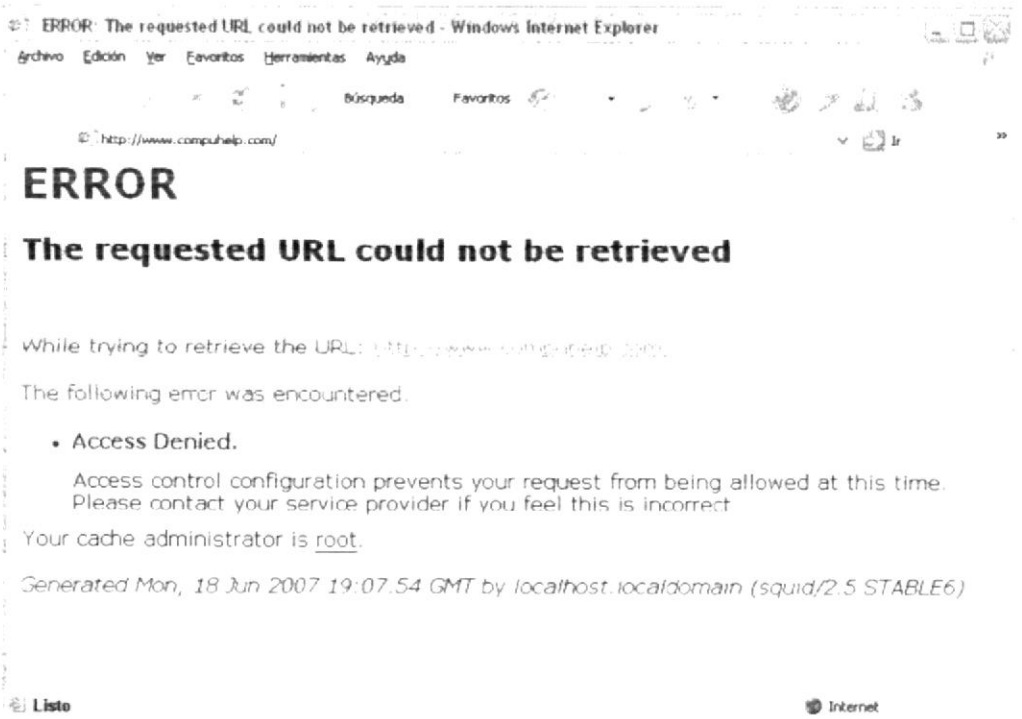


Figura 7-193: Prueba exitosa de páginas prohibidas

7.14 FIREWALL

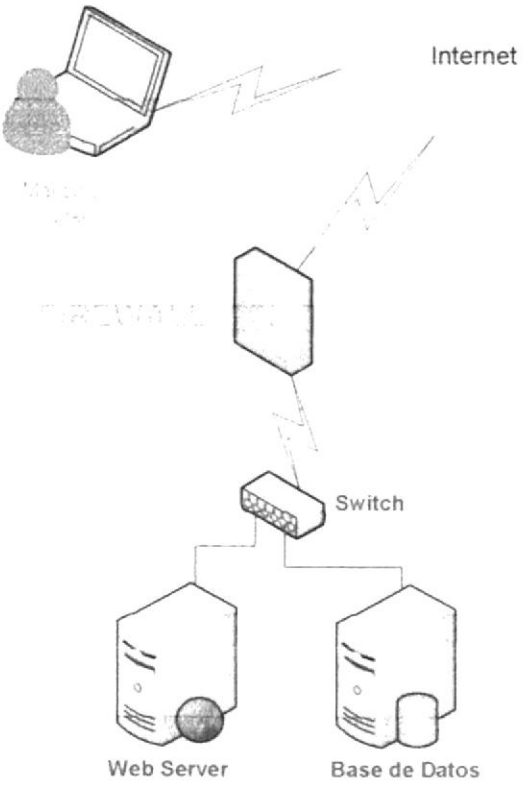


Figura 7-194: Como funciona un firewall

Un firewall es un dispositivo que filtra el tráfico entre redes, puede ser un dispositivo físico o un software sobre un sistema operativo.

Es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta.

Dependiendo de los servicios configurados en el servidor (web, correo, archivo, etc.), y tras un exhaustivo análisis de la utilización, rendimiento del servidor y de la red interna se configura un firewall en el mismo servidor para tal fin.

7.14.1 DEFINICIÓN

Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Existen 3 tipos de reglas:

INPUT = Entrada al servidor
OUTPUT = Servidor hacia fuera
FORDWARD = Redireccionar

7.14.2 CARACTERÍSTICAS DE UN FIREWALL LINUX

Filtrado a nivel de Núcleo

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

Requerimientos de Hardware

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

Flexibilidad

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

Economía

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

7.14.3 VENTAJAS DE UN CORTAFUEGOS

- **Protege de intrusiones.-** El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

- **Protección de información privada.-** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

- **Optimización de acceso.-** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

7.14.4 REQUERIMIENTOS PARA LA CONFIGURACIÓN DE UN FIREWALL

- Debe tener instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Debe haberle asignado una dirección IP estática al servidor.

- Debe tener habilitado el firewall.

7.14.5 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. Ingrese al DOS y verifique si los usuarios tienen habilitada la opción de hacer ping; de clic en inicio, y seleccione ejecutar.

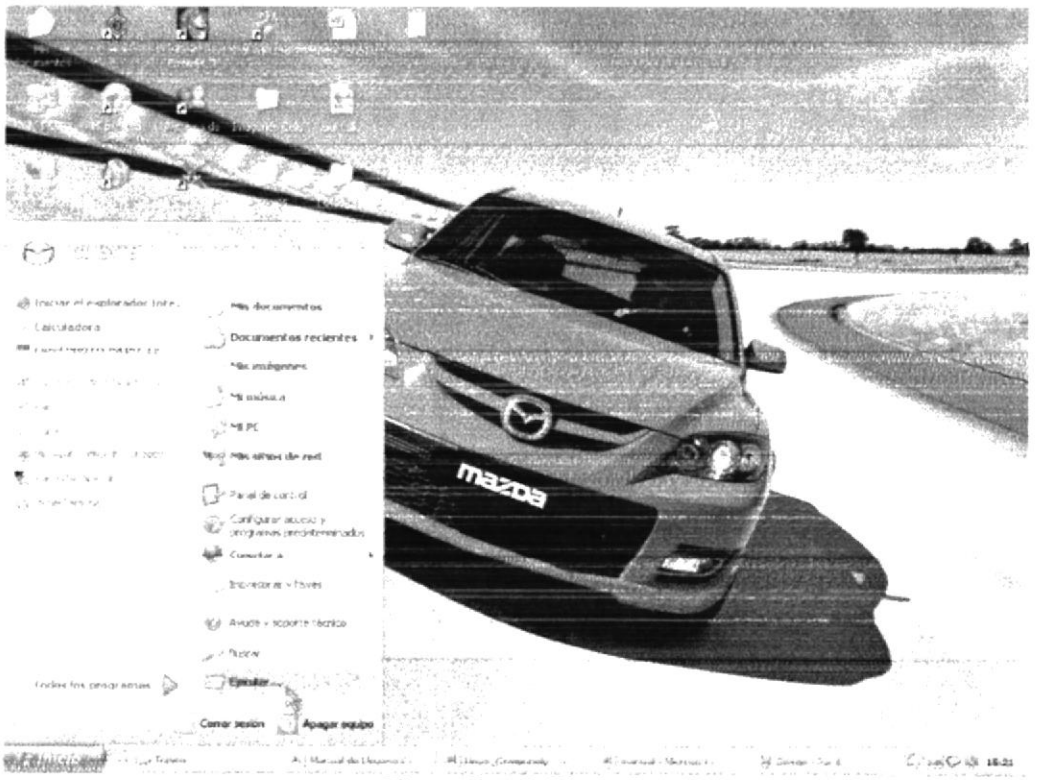


Figura 7-195: Ejecutar

2. Luego le aparece una pequeña ventana, donde debe ingresar el comando cmd, para ingresar al DOS de Windows.

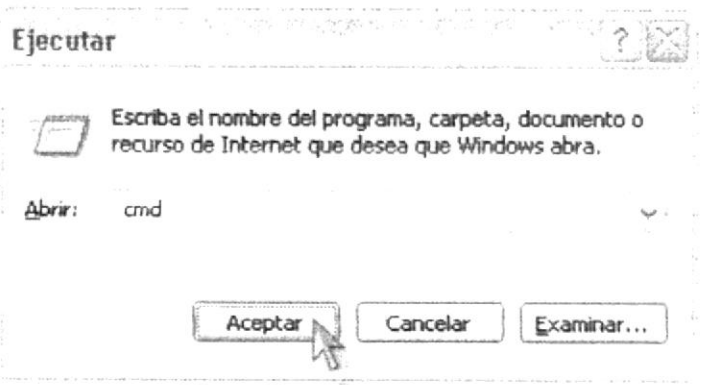


Figura 7-196: Comando cmd

3. Luego le aparecerá la pantalla del DOS donde debe realizar ping al servidor.

Figura 7-197: Pantalla haciendo ping

4. Bloquear Ping

Esta línea de comando sirve para denegar ping, para que los usuarios que tienen el mismo segmento de red no puedan acceder a un Servidor determinado.

iptables -A INPUT -s 192.168.12.0/24 -d 192.168.12.1/24 -p icmp -j DROP
iptables -A INPUT -s 192.168.12.0/24 -d 192.168.12.1/24 -p icmp -j REJECT

iptables → Palabra reservada
-A INPUT → Agregar
-s → Red Origen
192.168.12.0/24 → Red origen
-d → Red Destino
192.168.12.1/24 → IP Servidor
-p → Protocolo
icmp →
-j → Acción a aplicar
DROP → Denegar

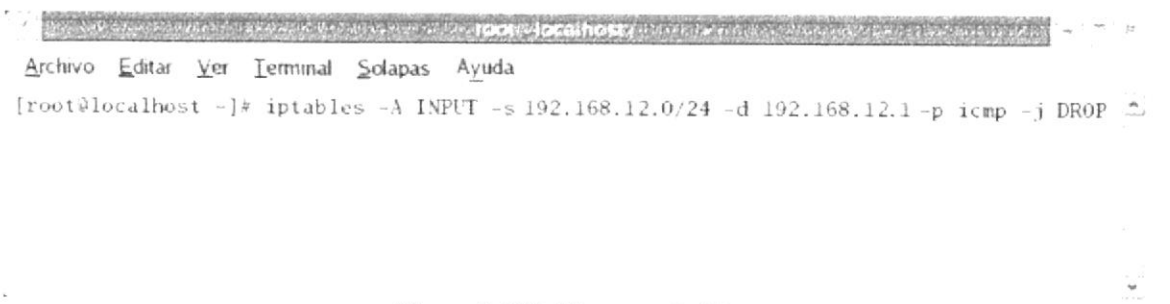


Figura 7-198: Bloqueando Ping

5. Verifique en el servidor que se esta denegando el ping para cualquier usuario del mismo segmento de red. Verifique con el comando iptables – L

```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  192.168.12.0/24      192.168.12.1

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Figura 7-199: Verificar el estado de Ping

6. Desde el cliente compruebe, haciendo ping al servidor y le tiene que dar como resultado, host de destino inaccesible.

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

C:\Documents and Settings\CLIENTE>ping 192.168.12.1

Haciendo ping a 192.168.12.1 con 32 bytes de datos:

Host de destino inaccesible.
Host de destino inaccesible.
Host de destino inaccesible.
Host de destino inaccesible.

Estadísticas de ping para 192.168.12.1:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Documents and Settings\CLIENTE>_
```

Figura 7-200: Ping bloqueado

7. Bloquee Telnet con la siguiente linea:

iptables -A INPUT -s 192.168.12.0/24 -d 192.168.12.1/24 –p tcp --dport 23 - j DROP

```
root@localhost:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# iptables -A INPUT -s 192.168.12.0/24 -d 192.168.12.1 -p tcp --dport 23 -j DROP
```

Figura 7-201: Bloqueando Telnet

8. Para verificar si se denegó el telnet debe hacerlo con el comando iptables –L

```
root@localhost:/
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.12.0/24     192.168.12.1        tcp dpt:telnet
DROP       tcp  --  192.168.12.0/24     192.168.12.1        tcp dpt:telnet

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Figura 7-202: Verificando el estado de Telnet

9. Para comprobar haga una prueba desde el cliente, haciendo telnet al servidor. Observe que se encuentra denegado el telnet.

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

C:\Documents and Settings\CLIENTE>telnet 192.168.12.1
Conectándose a 192.168.12.1...No se puede abrir la conexión al host, en puerto 2
3: Error en la conexión

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

Figura 7-203: Comprobación de bloqueo de Telnet

10. Bloquee FTP

iptables –A INPUT –s 192.168.12.0/24 –d 192.168.12.1/24 –p tcp --dport 21 –j DROP

7.15 DHCP

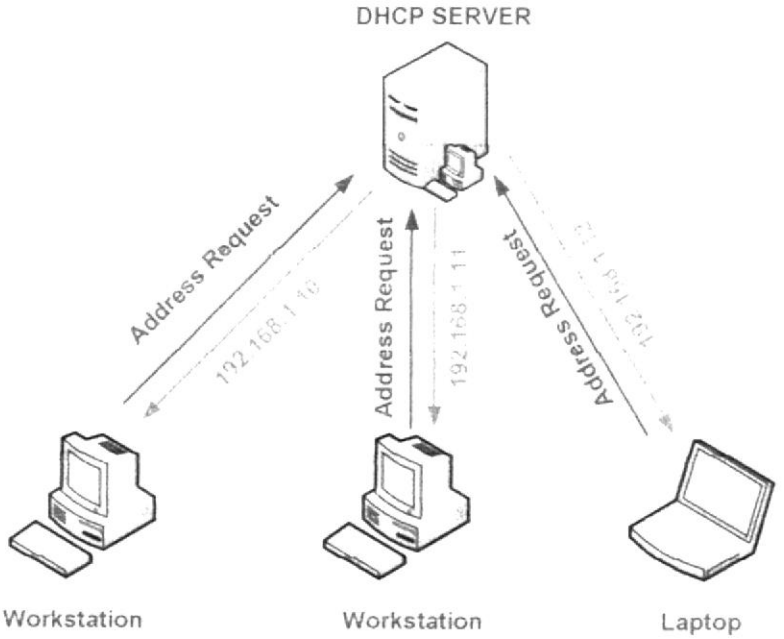


Figura 7-204: Como funciona DHCP

La configuración de DHCP se basa en un fichero de texto, la lectura del fichero de configuración sólo se realiza durante el inicio, nunca cuando ya está en ejecución, por tanto cualquier modificación requiere detener el servicio DHCP y volverlo a iniciar. En este fichero se especifican las características de comportamiento como son el rango de direcciones asignadas, el tiempo de asignación de direcciones, el nombre del dominio, los gateways, etc. DHCP almacena en memoria la lista de direcciones de cada computadora en la red a quien está sirviendo. Cuando se arranca un cliente DHCP le solicita una dirección al servidor, éste busca una dirección disponible y se la asigna. En otros casos, el servidor DHCP también puede asignar direcciones fijas a determinados equipos de la red.

7.15.1 DEFINICIÓN

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

7.15.2 MÉTODOS DE ASIGNACIÓN DE DIRECCIONES IP

- Asignación manual o estática: Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente y evitar el acceso a usuarios no identificados.

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

- Asignación dinámica: Este método permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. Facilita la instalación de nuevas máquinas clientes a la red.

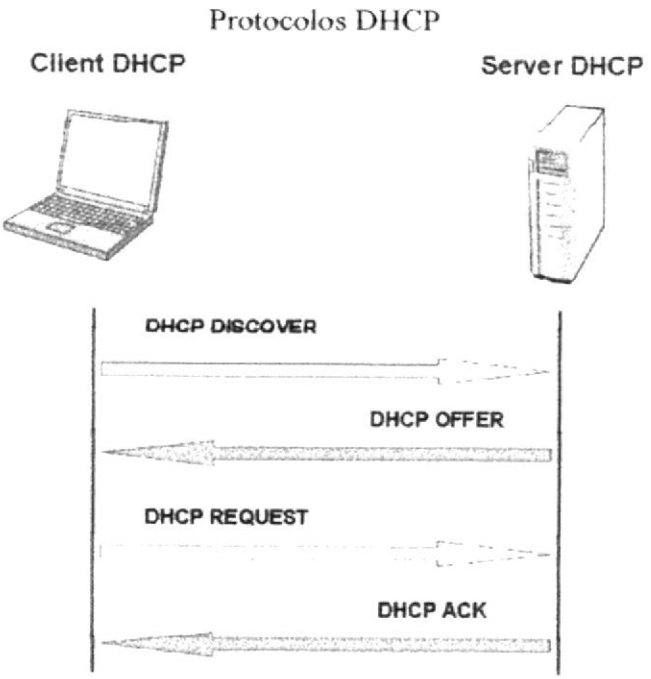


Figura 7-205: Protocolos DHCP

DHCP Discover

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

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

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

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

7.15.3 BENEFICIOS AL INSTALAR UN SERVIDOR DHCP

- Puede administrar de manera centralizada toda la información de configuración de IP. De esta forma se elimina la necesidad de configurar manualmente los clientes individualmente cuando se implanta por primera vez TCP/IP o cuando se necesitan cambios en la infraestructura de IP.

- Asegura que los clientes de DHCP, obtengan parámetros de configuración de IP precisos y en tiempo, sin intervención del usuario. Como la configuración es automática se elimina gran parte de los problemas.

- El administrador aumenta su flexibilidad para el cambio de la información de configuración de IP, lo que permite que el administrador cambie la configuración de IP de manera sencilla cuando se necesitan los cambios.

7.15.4 REQUERIMIENTOS PARA LA CONFIGURACIÓN DE UN DHCP SERVER

- Debe tener instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.

- Deber haberle asignado una dirección IP estática al servidor.

- Debe haber instalado el paquete DHCP el cual se verifica con el comando rpm –q dhcpd.

- Debe tener deshabilitado el firewall.

7.15.5 CONFIGURACIÓN DHCP

1. Verifique si se encuentra instalado el paquete DHCP.
   rpm -q dhcp

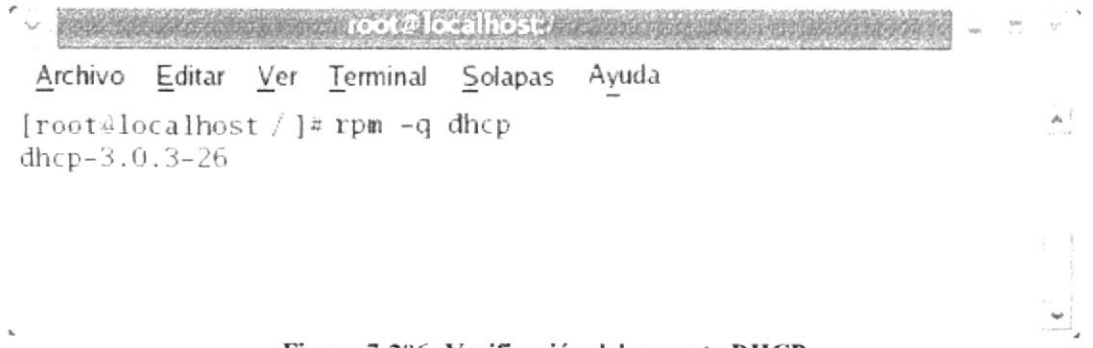


Figura 7-206: Verificación del paquete DHCP

2. Cree el archivo dhcp.conf de la siguiente manera
   cp /usr/share/doc/dhcp-3.01/dhcpd.conf.sample etc/dhcpd.conf

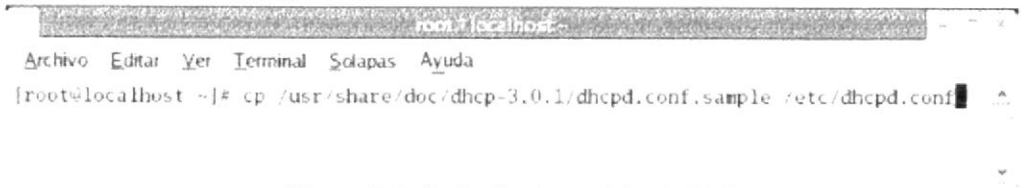


Figura 7-207: Copiando archivo DHCP

3. Configure el archivo dhcpd.conf
   vi /etc/dhcpd.conf

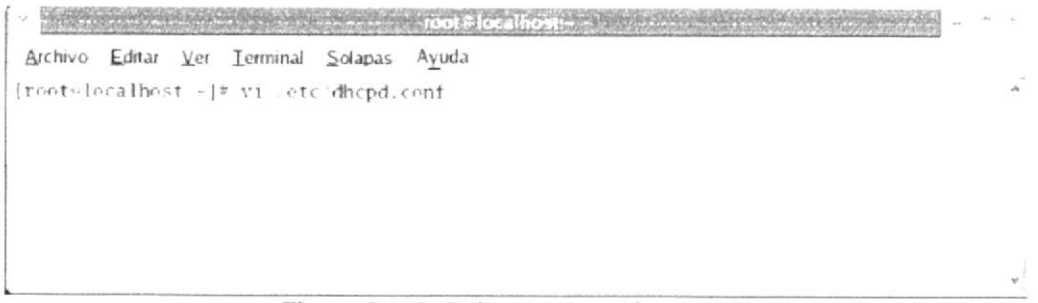


Figura 7-208: Editando el archivo DHCP

4. Luego edite el archivo

a. En la línea subnet asigne el segmento de red con su respectiva máscara.
   Subset 192.168.12.0 netmask 255.255.255.0

- Opcional que coloque la línea del gateway
  Option routers 192.168.12.1
  Option subset-mask 255.255.255.0
- Digite la dirección del DNS
  Option domain-name-servers 192.168.12.1
- Defina el rango de Ip's desde - hasta
  Range dynamic-bootp 192.168.12.10 192.168.12.50
- Salga y guarde los cambios.

option routers 192.168.12.1: Es donde define los gateway de la red.
option subset-mask 255.255.255.0: Es donde define la máscara general de la red.
option nis-domain "compuhelp.com": Es donde define el nombre del dominio DNS.
option domain-name "compuhelp.com": Es donde define el nombre del dominio DNS que se añade a los nombres de host.
option domain-name-servers 192.168.12.1: Es donde define la dirección del Servidor DNS en la red.
range dynamic-bootp 192.168.12.10 192.168.12.50: Es donde designará el rango de direcciones Ip's disponibles.

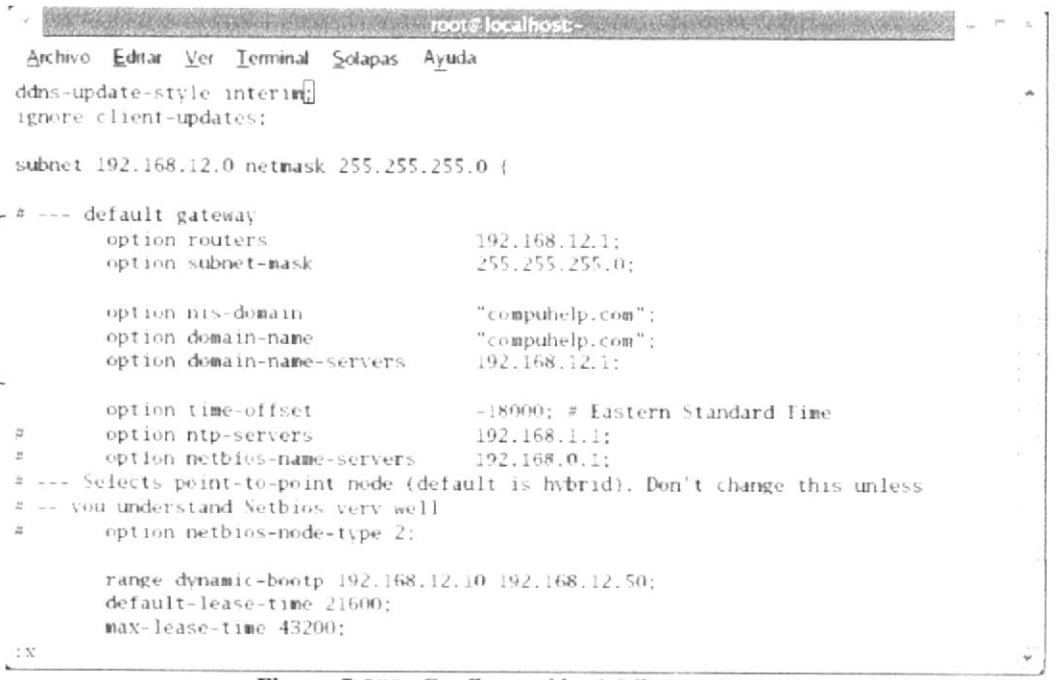


Figura 7-209: Configuración del fichero DHCP

5. Debe crear un archivo en la siguiente ruta que es donde se guardarán todas las direcciones Ip's asignadas por el servidor DHCP.
   touch /var/lib/dhcp/dhcpd.leases

Figura 7-210: Creación de archivo para guardar direcciones asignadas

6. Inicie los servicios del dhcpd con la siguiente linea de comandos:
   Service dhcpd start

Figura 7-211: Iniciando los servicios DHCP

7.15.6 CONFIGURACIÓN EN EL CLIENTE WINDOWS

1. De clic derecho en mis sitios de red y luego de clic en propiedades.

Figura 7-212: Propiedades de red

2. De clic derecho en conexión de área local y luego de clic en propiedades.

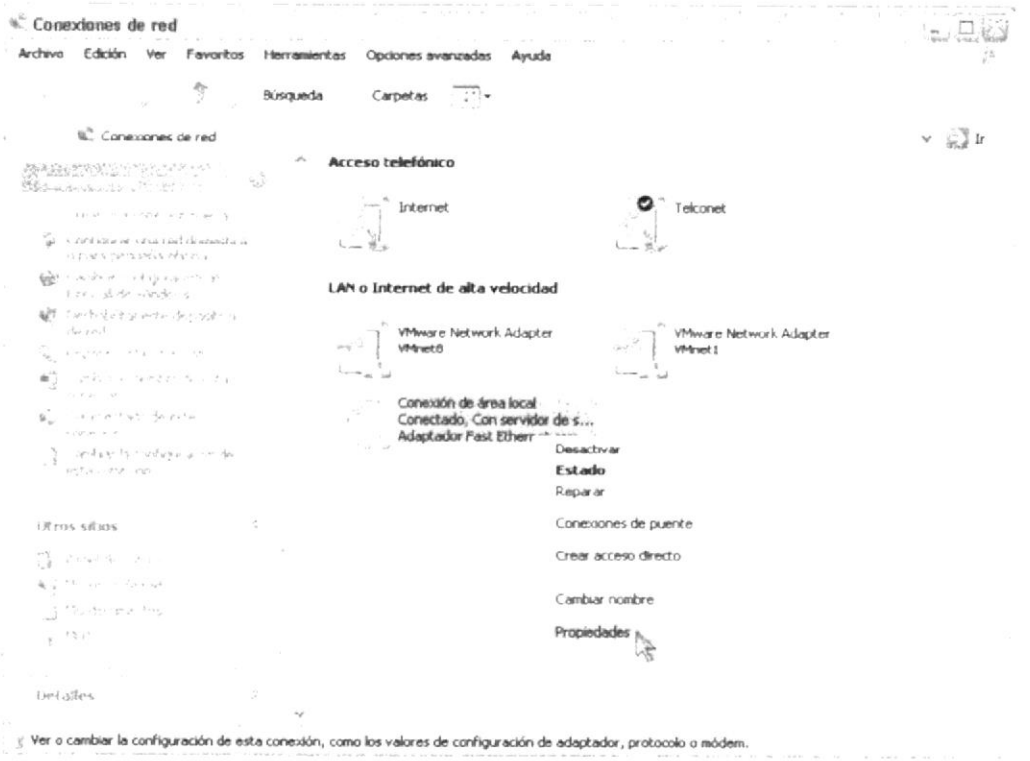


Figura 7-213: Conexión de área local

3. Seleccione Protocolo Internet TCP/IP y de clic en propiedades.

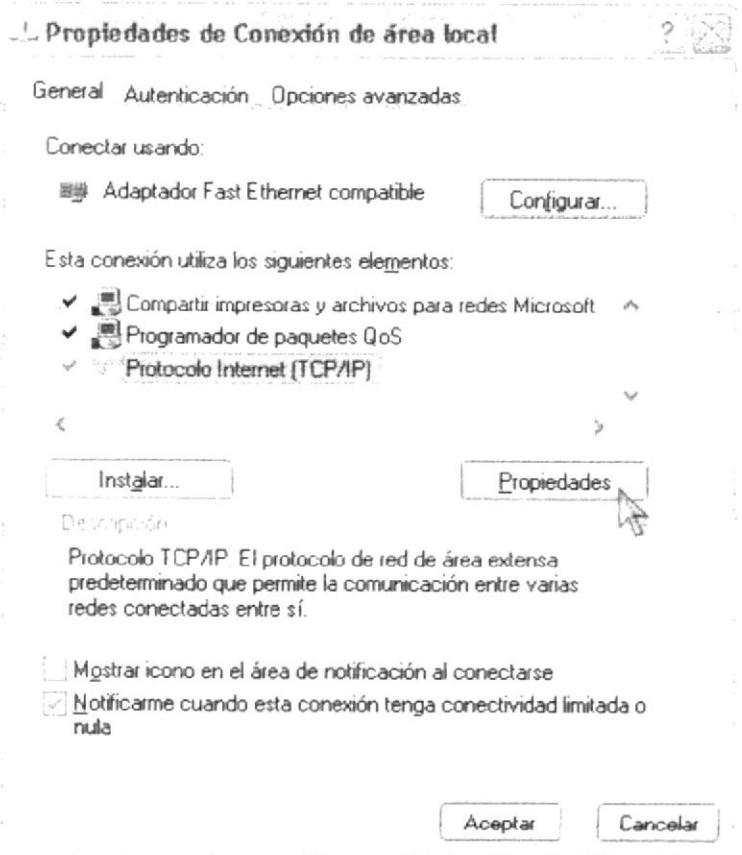


Figura 7-214: Protocolo TCP/IP

4. Seleccione obtener Ip automáticamente y de clic en aceptar.

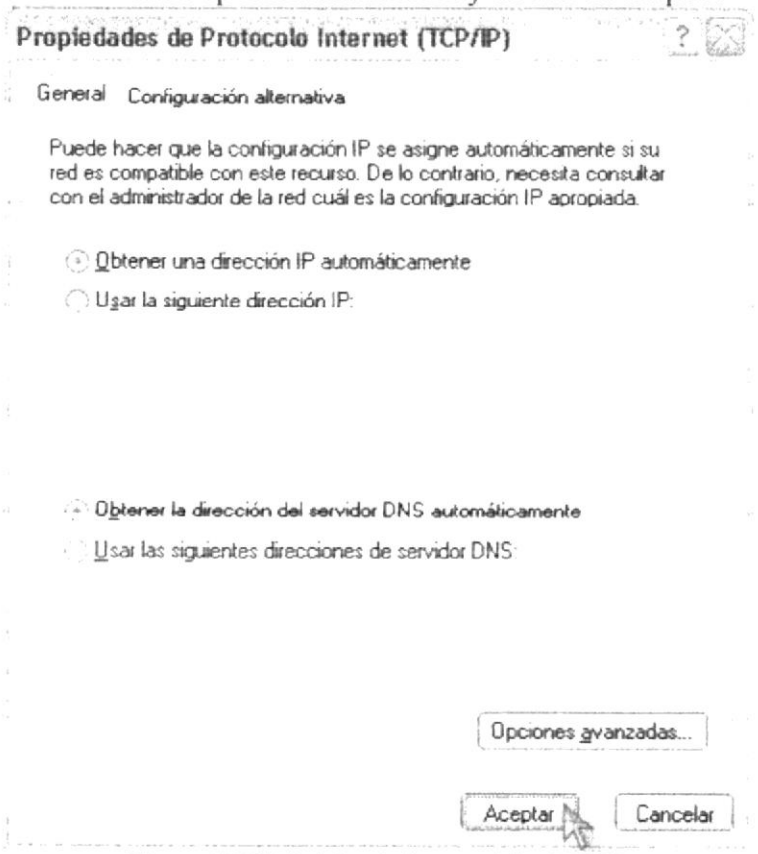


Figura 7-215: Iniciando los servicios DHCP

5. Verifique el estado dando un clic derecho en propiedades de conexión y seleccione estado.

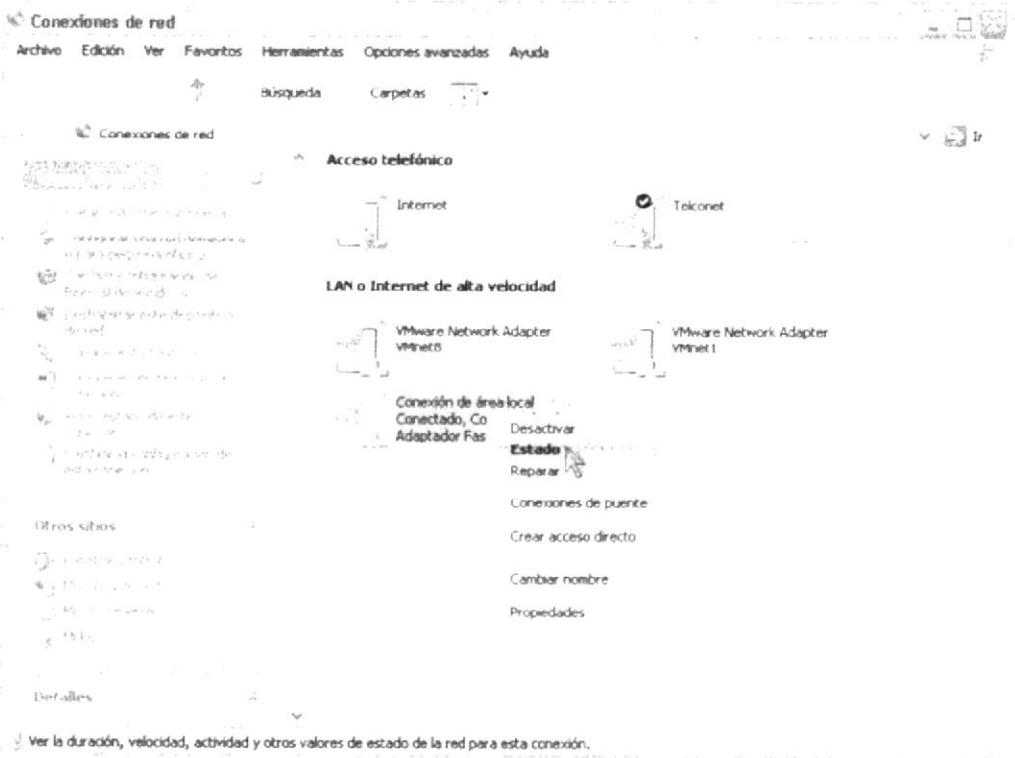


Figura 7-216: Estado de la conexión de red

6. En la pantalla que aparece, ubíquese sobre la pestaña soporte y de clic izquierdo.

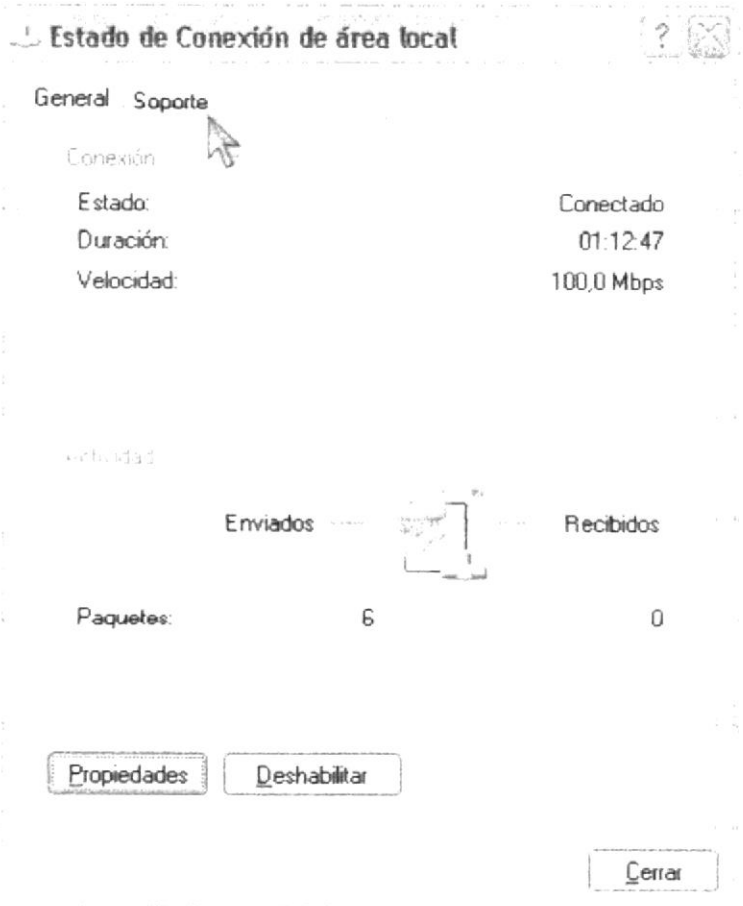


Figura 7-217: Soporte de la conexión de área local

7. En esta pantalla se puede verificar la dirección IP asignada por DHCP con su respectiva máscara de subred y puerta de enlace predeterminada. Luego de verificar la dirección IP, de clic izquierdo en Cerrar.

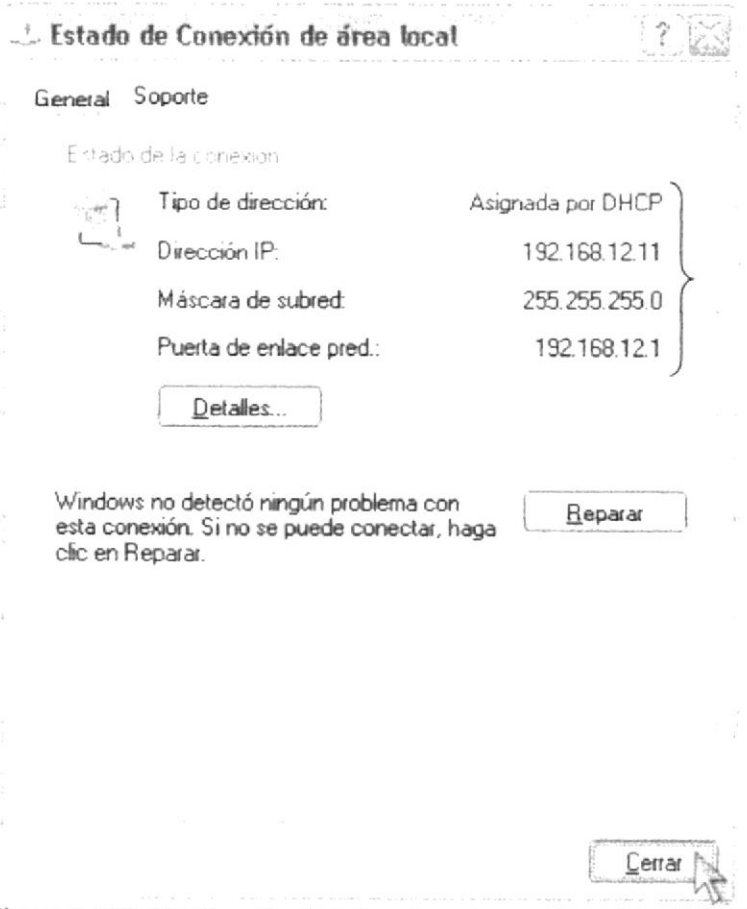


Figura 7-218: Verificación de la Ip asignada por el servidor DHCP

ANEXO

GLOSARIO DE TÉRMINOS TÉCNICOS

Para solucionar cualquier duda, referente a palabras técnicas que no son muy comunes, se ha organizado en orden alfabético las palabras y siglas con sus respectivos significado.

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 operen 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 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 por segundo). 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) puede 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 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.

Cableado backbone: Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN. Ver cableado vertical.

Cableado de Categoría 5e: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5e se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 4. Ver también EIA/TIA-568By UTP.

Caché: Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso más rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los accesos a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

Canaleta: 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 de control de enlace de datos: La Capa 2 del modelo de arquitectura. Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

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.

Cliente: Nodo que solicita servicios a un servidor.

Colisión: En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

Cola: Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

Conector RJ: Conector macho registrado. Conectores estándar que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ

Costo: Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.

Consola: DTE a través del cual se introducen los comandos en un host.

Correo electrónico: Aplicación de red utilizada ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.

CSMA/CD: Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón).

Cliente: Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

Computador: Es un dispositivo electrónico compuesto básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

Contraseña ó Password: Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los Sistemas y recursos de la computadora.

CPU: (Central Processing Unit ó Unidad central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

Cuadro de Diálogo: Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

Cuadro de Texto: Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de diálogo, el cuadro de texto puede estar en blanco o contener texto.

Cursor: Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo carácter a visualizar cuando se pulse una tecla.

CSU: Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con el loop telefónico digital local. A menudo se denomina, de forma conjunta con DSU, como CSU/DSU.

D

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 via 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 = 1 Gb.

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.

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.

E

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.

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.

Firewall: Router o servidor de acceso, designado como un búfer entre cualquier red pública conectada y una red privada.

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.

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.

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.

I

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.

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.

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.

K

Kbps: (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobits esta formado por mil bits.

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.

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.

Máscara de red: Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

Máscara wildcard: Cantidad de 32 bits que se usan de forma conjunta con una dirección IP para determinar cuáles son los bits de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

MDF: Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

Megabyte (MB): 1.048.576 bytes; 1.024 Kilobytes.

Megahertz (MHZ): 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.

Métrica: Método por el cual un algoritmo de enrutamiento determina que una ruta es mejor que otra. Esta información se guarda en las tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de comunicación, retardo, número de saltos, carga, MTU, costo de la ruta y confiabilidad.

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.
NET: Titulo 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

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.

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

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

Panel de conexión: Conjunto de ubicaciones de pines 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.

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.

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.

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.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

RIP: Protocolo de información de enrutamiento. IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet.

RMON: Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitoreo remoto de los dispositivos conectados a la red.

ROM: Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.

Ruta estática: Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

Ruta por defecto: Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

S

Segmento: La sección de una red limitada por puentes, routers o switches. Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

SMTP: Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico.

Sondeo: Método de acceso en el que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

Switch: Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

Switch LAN: Switch de alta velocidad que envía paquetes entre segmentos de enlaces 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.

Transiver: 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.

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.

Workgroups Director: Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroups 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.

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.

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.