ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Escuela de Diseño y Comunicación Visual

TÓPICO DE GRADUACIÓN

Previo a la obtención del Título de
Analista de Soporte de Microcomputadores

Tema:

Administración y Seguridades de Redes
Armada del Ecuador

Manual de Usuario

Autores:

Gerardo Omar Ortega Echeverría
Angel Daniel Saldarreaga Arrieta

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

ADMINISTRACIÓN Y SEGURIDADES DE REDES ARMADA DEL ECUADOR

MANUAL DE USUARIO

AUTORES
GERARDO OMAR ORTEGA ECHEVERRÍA
ÁNGEL DANIEL SALDARREAGA ARRIETA

DIRECTOR
ANL. FABIÁN BARBOZA

AÑO
2007

AGRADECIMIENTO

Agradezco a Jehová Dios por mantenerme con vida y poder servirle, de igual manera quedo muy agradecido a quienes me han apoyado en todo sentido para lograr que se cumplan mis metas seglares, entre quienes constan mis padres y a los docentes quienes nos dirigieron e implantaron sus conocimientos.

Gerardo Ortega

Ante todo quiero agradecer al Señor Dios Todopoderoso, por darme la oportunidad de vivir, a la persona que me trajo al mundo mi adorada madre, a toda mi familia, por darme el apoyo necesario para poder cumplir esta meta, a los docentes que supieron guiarme y dotarme de conocimientos, al director de nuestro tópico porque de una u otra manera tenía razón en hacer que nos esforcemos cada vez más, por último y no por menos a la pequeña personita por la cual mis sueños no desmayan, mi amada hija Fiorella, te amo mucho.

Ángel Saldarreaga

DEDICATORIA

Dedicado de una manera especial para todos nuestros familiares, amigos y demás personas que de una u otra manera nos ayudaron a culminar nuestra carrera.

DECLARACIÓN EXPRESA

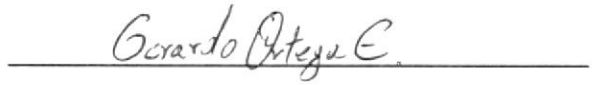
La responsabilidad por los hechos, ideas y doctrinas expuestas en este Tópico de Graduación nos corresponden exclusivamente. Y el patrimonio intelectual de la misma a EDCOM (***Escuela de Diseño y Comunicación Visual***) de la Escuela Superior Politécnica del Litoral.

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

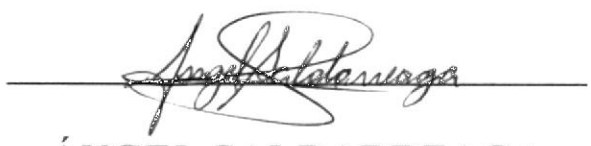
FIRMA DEL DIRECTOR DEL TÓPICO

ANL. FABIAN BARBOZA

FIRMA DE LOS AUTORES DEL TÓPICO



GERARDO ORTEGA



ÁNGEL SALDARREAGA

ÍNDICE GENERAL

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 6

CAPÍTULO 7

ANEXO A

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 5

CAPÍTULO 6

ÍNDICE DE FIGURAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 6

CAPÍTULO 7

CAPÍTULO 1

GENERALIDADES

1 GENERALIDADES

1.1 INTRODUCCIÓN

Este manual es una guía de consulta para usuarios, estudiantes que se desempeñen en el área de redes o deseen aplicar configuraciones o servicios para una red Informática.

1.2 OBJETIVO DEL MANUAL

El objetivo de este manual es brindar una guía de consulta rápida y la comprensión del contenido del mismo de una manera sencilla.

Luego de leer este manual el usuario estará en la capacidad de realizar diversas configuraciones en el sistema operativo Linux, administrar y configurar dispositivos de comunicación.

1.3 ¿A QUIÉN VA DIRIGIDO ESTE MANUAL?

Este manual va dirigido para usuarios, estudiantes que se desempeñen en el área de redes que requieran solidificar sus conocimientos y poder realizar configuraciones de diferentes servicios necesarios para la administración y el buen desempeño de una red Informática.

1.4 QUE SE DEBE CONOCER

Los conocimientos previos que deben tener los usuarios para que comprendan y utilicen este manual son:

- Conceptos básicos de redes de Informática y Sistemas Operativos.
- Conocimientos básicos de navegadores de Internet y tecnologías basadas en Internet.

1.5 ORGANIZACIÓN DEL CONTENIDO DE ESTE MANUAL

Este manual se encuentra dividido en 7 capítulos distribuidos en orden numérico, los cuales se detallan a continuación:

Capítulo 1 : Generalidades
Capítulo 2 : Situación Actual
Capítulo 3 : Solución Propuesta
Capítulo 4 : Implementación
Capítulo 5 : Normativas de Cableado Estructurado
Capítulo 6 : Linux Fedora Core 3
Capítulo 7 : Configuración de Dispositivos de Comunicación

CAPÍTULO 2

SITUACIÓN ACTUAL

2 SITUACIÓN ACTUAL

2.1 ANTECEDENTES

La Armada del Ecuador nació en 1936 como una rama auxiliar del Ejército, encargada de servicios internos como el cuidado de faros, lucha contra el contrabando, transporte de tropas o abastecimientos a las regiones apartadas, visitas al Archipiélago de Galápagos y acciones de emergencia en momentos de crisis nacional o internacional.

En esos tiempos, la Armada como fuerza de defensa apenas tenía valor, por la falta de conciencia nacional sobre la importancia del mar y protección de sus recursos. La frontera marítima quedó prácticamente abandonada y la fuerza naval fue considerada, como innecesaria o como un lujo.

En los últimos años, esto cambio y el Gobierno Nacional se ha preocupado por brindar los debidos recursos a esta rama del Ejército Nacional.

La Marina Ecuatoriana se ha revelado en estos sesenta años, como una entidad creadora. En casi todos los campos de la actividad marítima, ha tenido que crear y diseñar las estructuras, leyes y reglamentos para presentarlos a la nación y luchar por su aprobación y aplicación.

2.2 MISIÓN

Organizar, entrenar, equipar y mantener el poder naval, así como participar en los procesos que garanticen la seguridad de la nación y propendan a su desarrollo, con la finalidad de contribuir a la consecución y mantenimiento de los objetivos nacionales, de acuerdo a la planificación prevista para tiempo de paz, conflicto y de guerra.

2.3 VISIÓN

Una armada con poder naval disuasivo lista para enfrentar las amenazas; comprometida con el desarrollo y proyección de los intereses marítimos; conformada por hombres de elevada capacidad profesional y moral.

2.4 INFRAESTRUCTURA LAN

El edificio DIGMAT se encuentra ubicado en la ciudad de Guayaquil, en la Av. 25 de Julio dentro de la Base Naval Sur, el cual está conformado por cinco pisos en los cuales se encuentran los siguientes repartos:

Planta Baja : Recepción y alojamiento de oficiales y tripulantes.
Primer Piso : DIGMAT (Dirección General de Material).
Segundo Piso : CETEIG (Centro de Tecnología Informática).
Tercer Piso : DIECAR (Dirección General de Armamento).
Cuarto Piso : DIRABA (Dirección de Abastecimiento).
Quinto Piso : DIGPER (Dirección General de Personal).

El cableado de red es estructurado y de tipo UTP categoría 5e, el cual se encuentra certificado, las conexiones de red de cada piso se encuentran empotradas y el MC se encuentra ubicado en el segundo piso (CETEIG) el cual cuenta con gabinetes acondicionados para los diferentes dispositivos de comunicación. A este lugar solo puede ingresar personal autorizado.

El reparto CETEIG es el encargado de la administración de la red, cuenta con divisiones de programación y análisis de proyectos.

2.4.1 ESTACIONES DE TRABAJO

El edificio DIGMAT cuenta en total con 90 estaciones de trabajo las cuales manejan programas utilitarios y los módulos de los sistemas administrativos y de control de maquinaria que poseen los diferentes repartos.

Repartos	Cantidad de PC's
DIGMAT	24
CETEIG	12
DIECAR	20
DIRABA	24
DIGPER	10

Tabla 2-1: Estaciones de trabajo

Las estaciones de trabajo de todos los repartos poseen las mismas características las cuales se detalla a continuación:

Características de los PC's	
Marca	HP
Sistema operativo	Windows XP
Procesador	Pentium 4 de 2 Ghz
Memoria	256 Mb de RAM
Disco duro	40 Gb.
Tarjeta de red	1 tarjeta10/100 Mbps

Tabla 2-2: Características de PC's

2.4.2 SERVIDORES

2.4.2.1 REPARTO CETEIG

Los servidores Canopus y DIGPER poseen las mismas características que se detallan a continuación.

Figura 2-1: Servidor Dell

Características	
Descripción	Canopus Server, Web Server DIGPER
Marca	Dell
Modelo	Optiplex GX270
Sistema operativo	Linux Red Hat
Procesador	Pentium IV de 3 Ghz
Memoria	512 Mb de RAM
Disco duro	2 discos: uno de 60 Gb y uno de 80 Gb.
Tarjeta de red	1 de 10/100 Mbps
Servicio que brinda Canopus Servicio que brinda DIGPER	Sistema administrativo a nivel interno. Página Web del personal que labora en las F.F.A.A.

Tabla 2-3: Características de Servidor Canopus, DIGPER

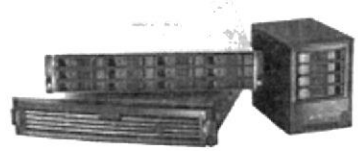


Figura 2-2: Servidor Intel

Características	
Descripción	Citrix Server
Marca	Intel
Sistema operativo	Windows 2000 Server
Procesador	Pentium IV de 3,2 Ghz
Memoria	1 Gb de RAM
Disco duro	2 discos de 17 Gb
Tarjeta de red	2 de 10/100 Mbps
Servicio que brinda	Sistema de control de la maquinaria de buques

Tabla 2-4: Características de Servidor Citrix

Figura 2-3: Servidor Dell

Características	
Descripción	Proxy Server
Marca	Dell
Modelo	Optiplex GX270
Sistema operativo	Red Hat Advanced Server 2.1
Procesador	Pentium III de 1 Ghz
Memoria	1 Gb de RAM
Disco duro	2 discos DE 17 Gb
Tarjeta de red	2 de 10/100 Mbps
Servicio que brinda	Compartir la conexión de Internet

Tabla 2-5: Características de Servidor Proxy

Figura 2-4: Servidor IBM

Características	
Descripción	Desarrollo Canopus
Marca	IBM
Modelo	Netfinity
Sistema operativo	Windows 2000 Server
Procesador	Pentium IV de 1.8 Ghz
Memoria	256 Mb de RAM
Disco duro	120 Gb
Tarjeta de red	2 de 10/100 Mbps
Servicio que brinda	Actualización del sistema del servidor Canopus

Tabla 2-6: Características de Servidor Canopus

Los servidores Backup Canopus y SISMAC poseen las mismas características que se detallan a continuación.

Figura 2-5: Servidor IBM

Características	
Descripción	Backup Canopus, SISMAC Server
Marca	IBM
Modelo	Netfinity 5500
Sistema operativo	Red Hat Linux
Procesador	Pentium II 500 Mhz
Memoria	256 Mb de RAM
Disco duro	40 Gb
Tarjeta de red	1 de 10/100 Mbps
Servicio que brinda Backup Canopus Servicio que brinda SISMAC	Respaldo del servidor canopus principal Habilita el sistema del servidor Citrix en otra plataforma (Oracle)

Tabla 2-7: Características de Servidor Backup Canopus, SISMAC

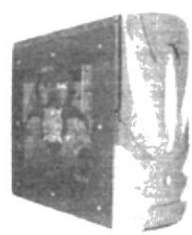


Figura 2-6: PC Clon

Características	
Descripción	Proxy Server Backup
Marca	PC Clon
Sistema operativo	Red Hat Linux
Procesador	Pentium III de 750 Mhz
Memoria	192 Mb de RAM
Disco duro	2 discos de 8 Gb
Tarjeta de red	2 de 10/100 Mbps
Servicio que brinda	Respaldo del servidor Proxy principal

Tabla 2-8: Características de Servidor Backup Proxy

2.4.3 ANÁLISIS DE PISO LÓGICOS DEL EDIFICIO DIGMAT

2.4.3.1 PRIMER PISO – REPARTO DIGMAT

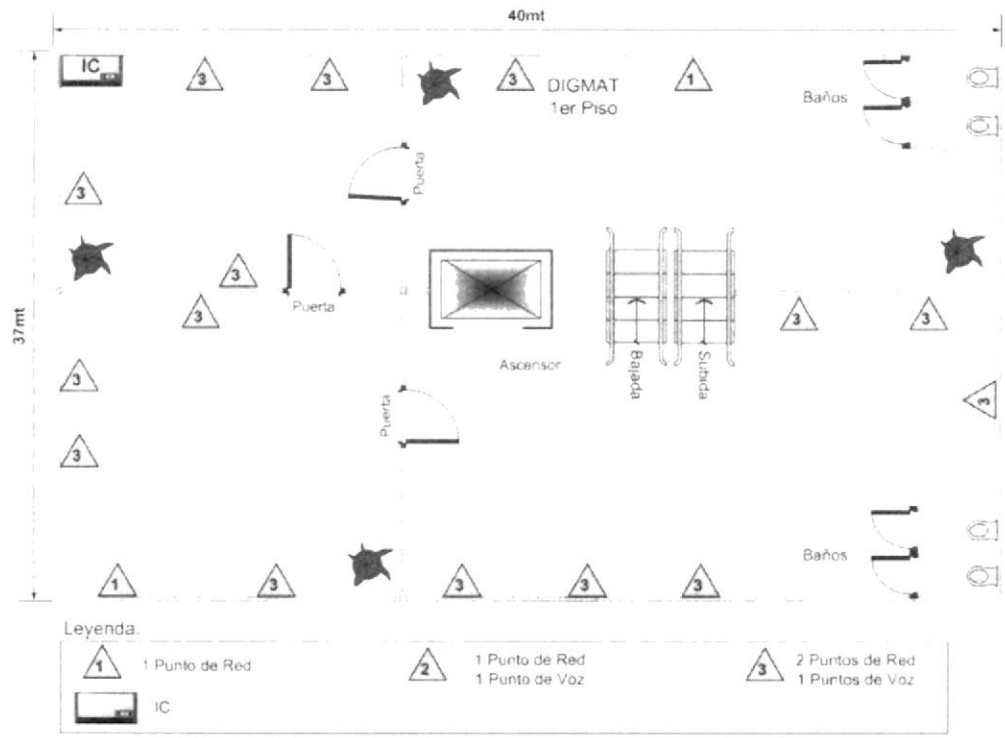


Figura 2-7: Análisis de piso lógico del reparto DIGMAT

2.4.3.2 SEGUNDO PISO – REPARTO CETEIG

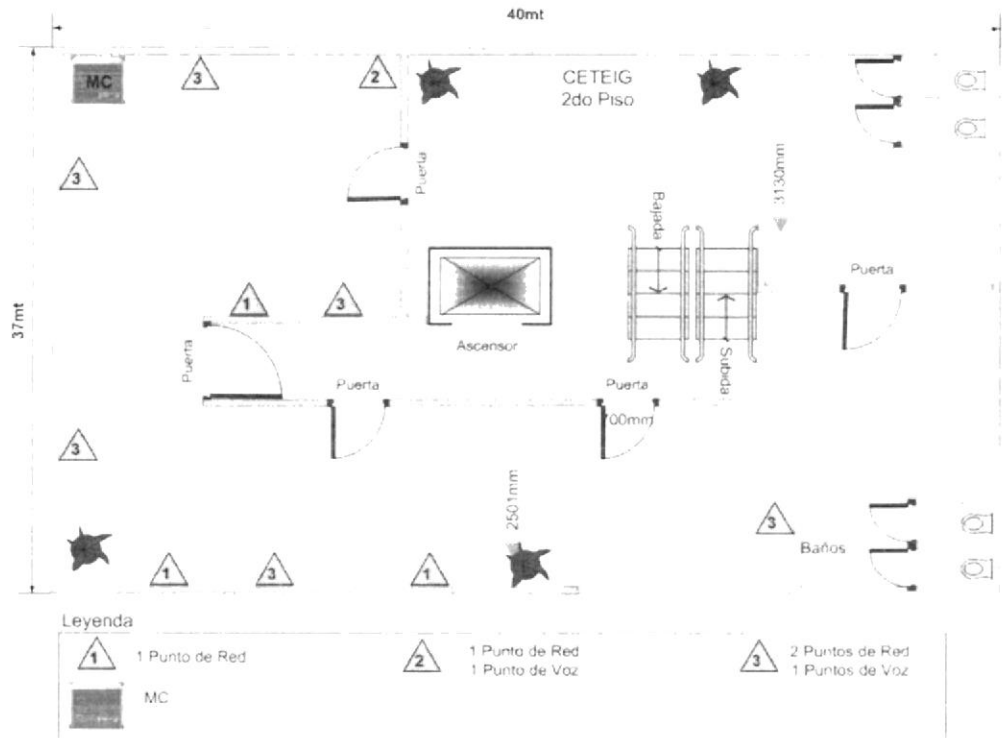


Figura 2-8: Análisis de piso lógico del reparto CETEIG

2.4.3.3 TERCER PISO – REPARTO DIECAR

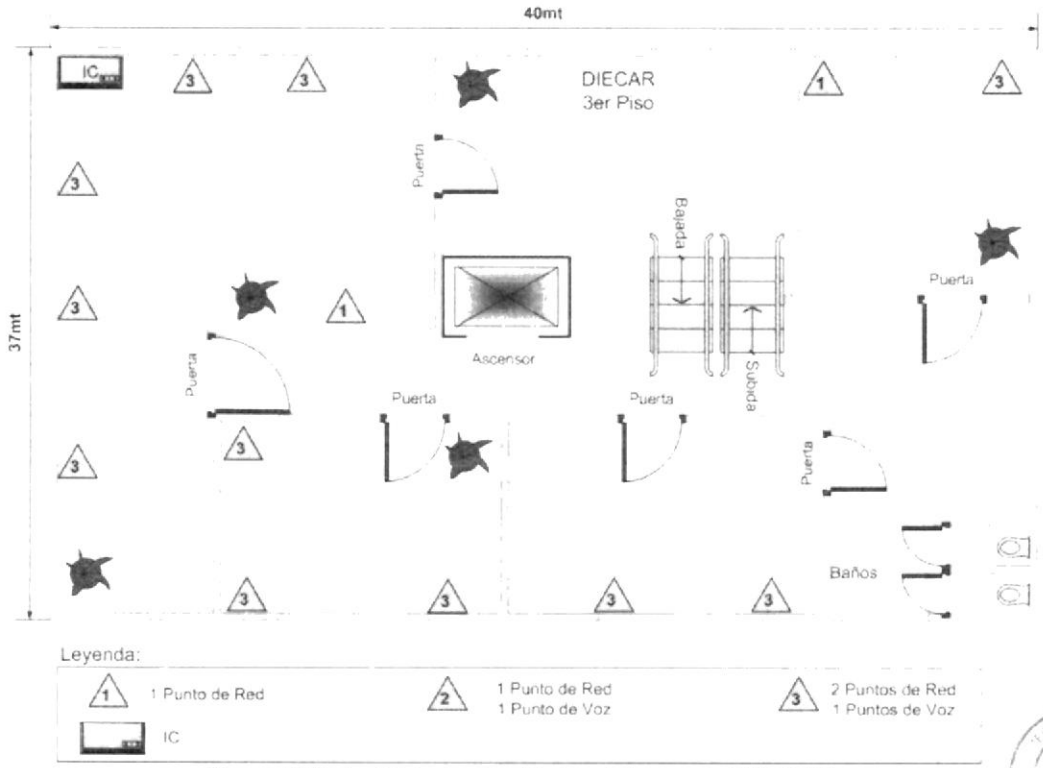


Figura 2-9: Análisis de piso lógico del reparto DIECAR

2.4.3.4 CUARTO PISO – REPARTO DIRABA

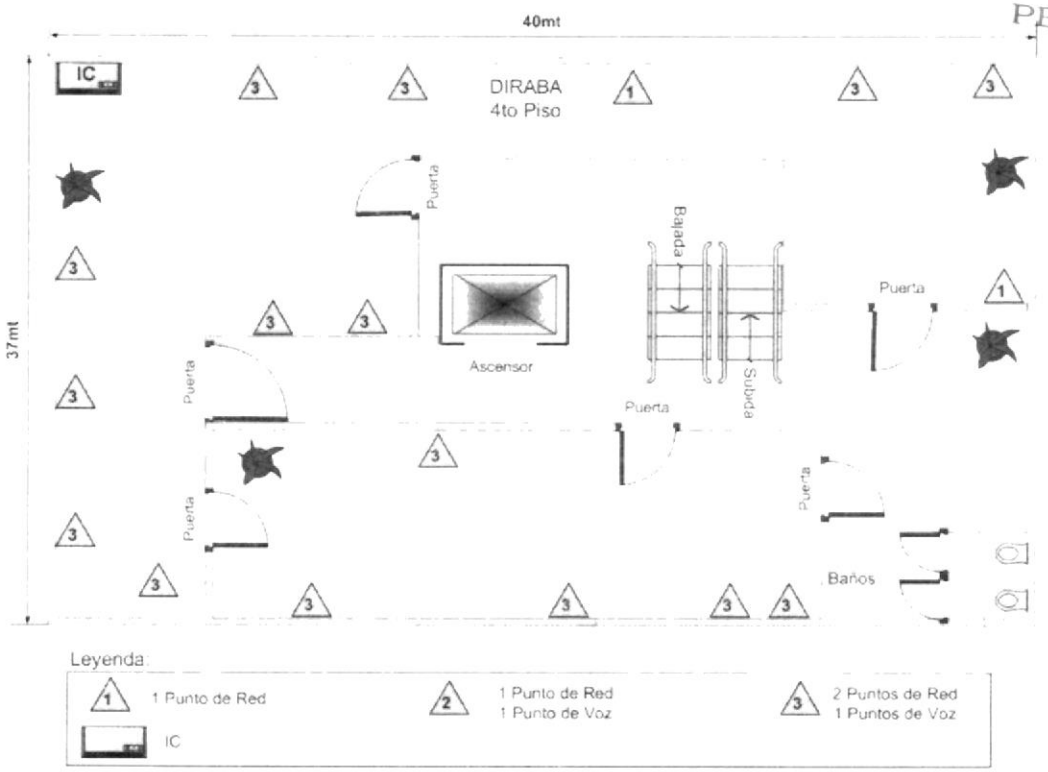


Figura 2-10: Análisis de piso lógico del reparto DIRABA

2.4.3.5 QUINTO PISO – REPARTO DIGPER

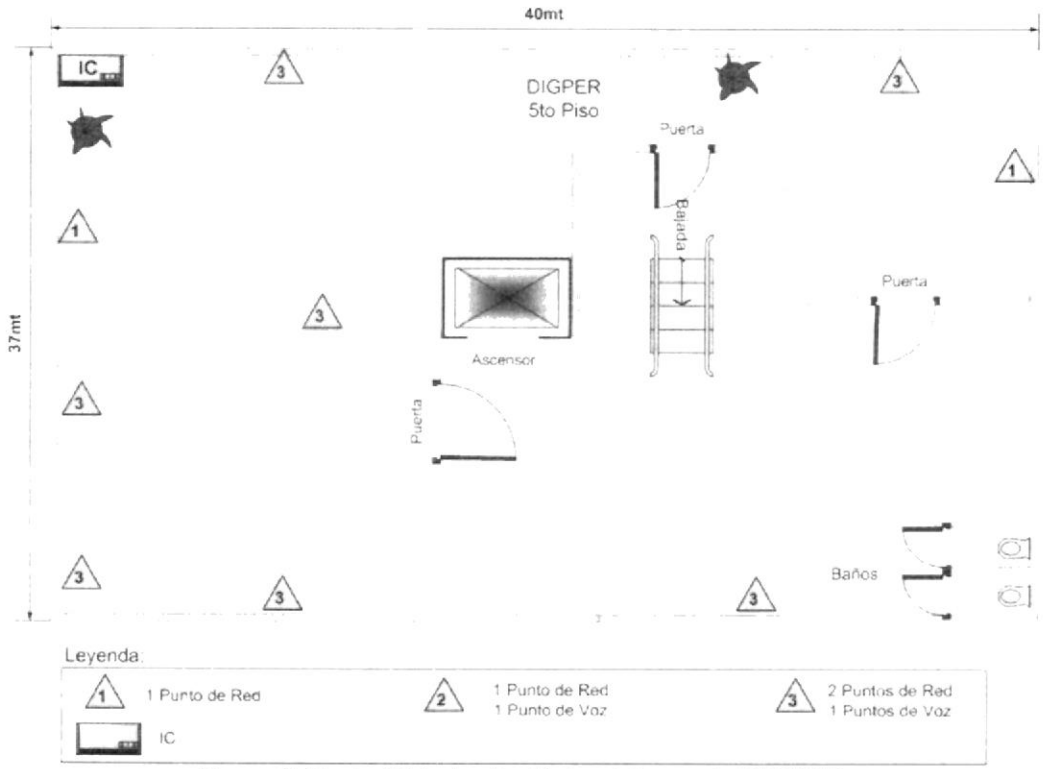


Figura 2-11: Análisis de piso lógico del reparto DIGPER

2.4.4 ANÁLISIS DE PISO APLICATIVOS DEL EDIFICIO DIGMAT

2.4.4.1 PRIMER PISO – REPARTO DIGMAT

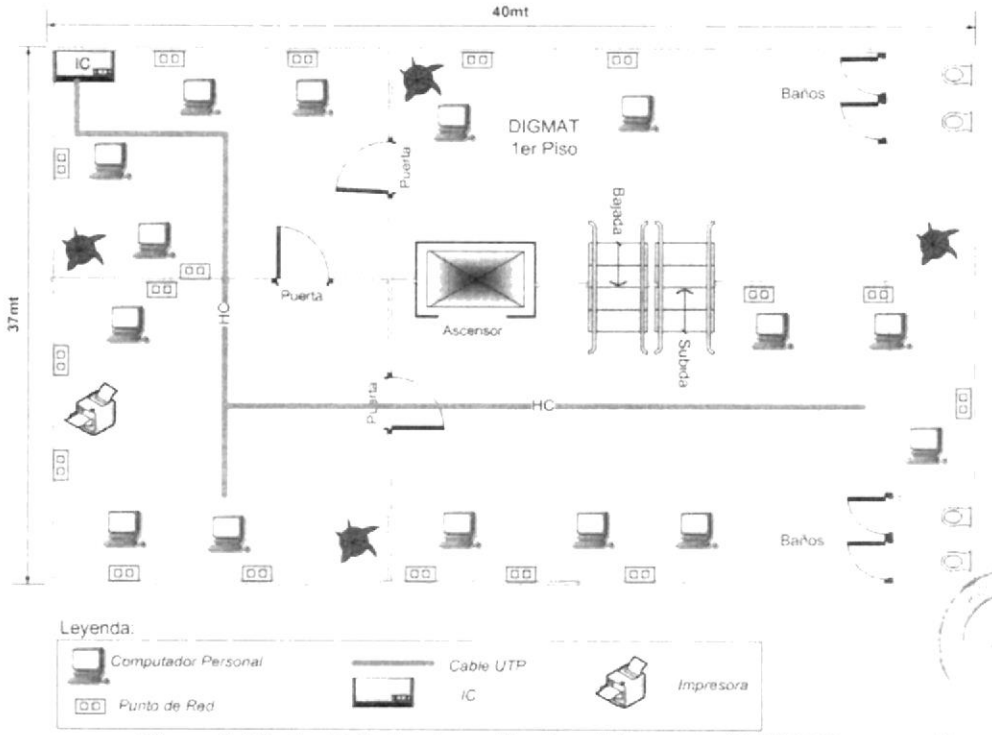


Figura 2-12: Análisis de piso aplicativo del reparto DIGMAT

2.4.4.2 SEGUNDO PISO – REPARTO CETEIG

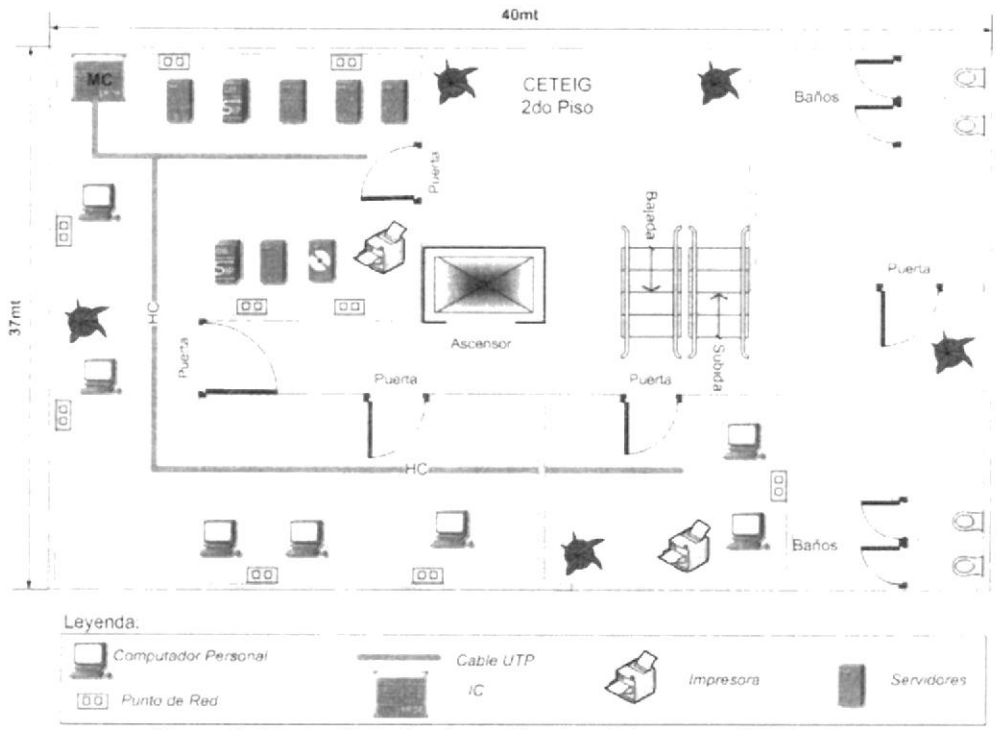


Figura 2-13: Análisis de piso aplicativo del reparto DIECAR

2.4.4.3 TERCER PISO – REPARTO DIECAR

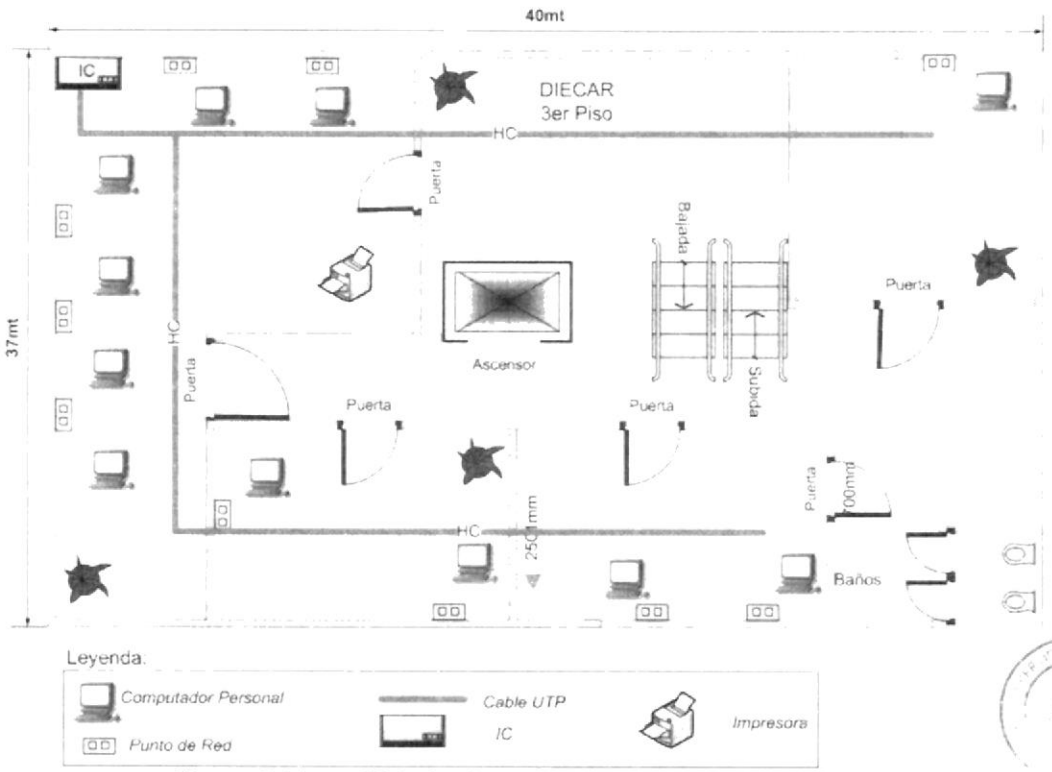


Figura 2-14: Análisis de piso aplicativo del reparto DIECAR

2.4.4.4 CUARTO PISO – REPARTO DIRABA

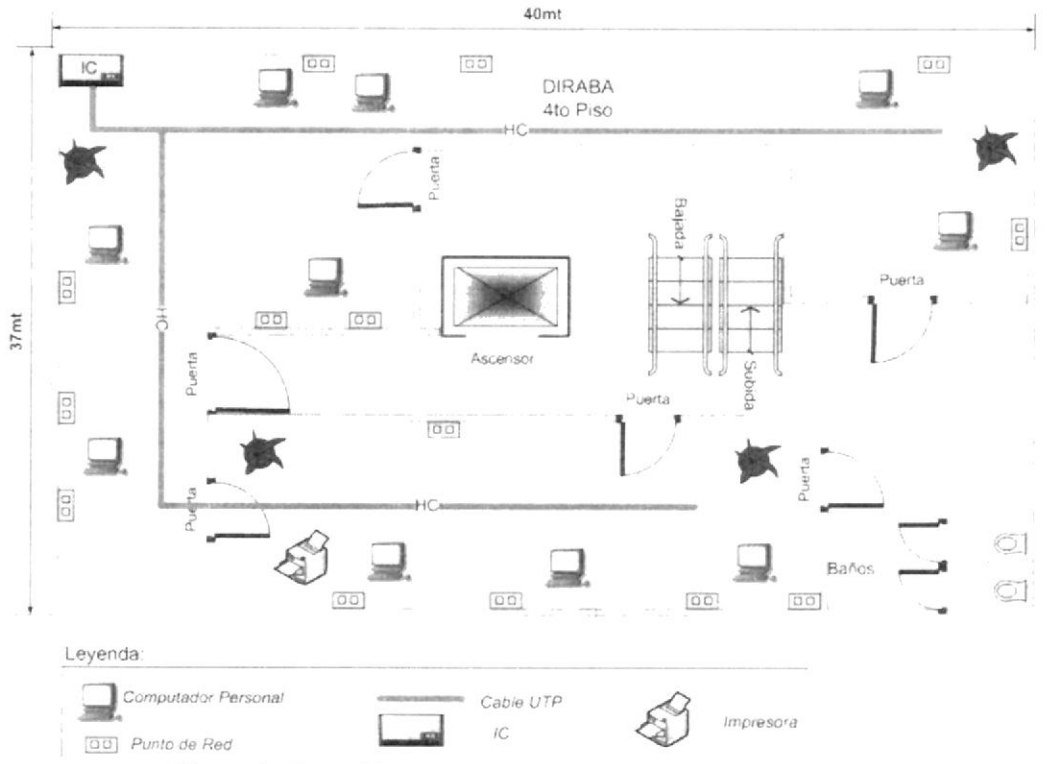


Figura 2-15: Análisis de piso aplicativo del reparto DIRABA

2.4.4.5 QUINTO PISO – REPARTO DIGPER

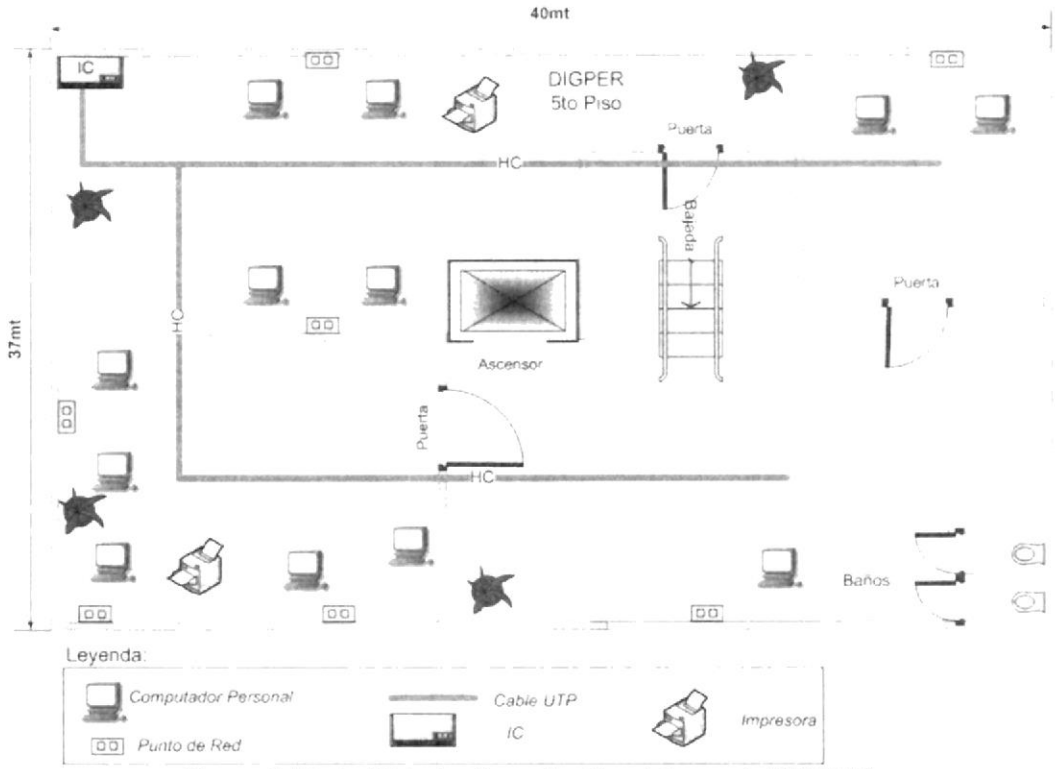


Figura 2-16: Análisis de piso aplicativo del reparto DIGPER

2.4.5 DISPOSITIVOS DE CONMUTACIÓN

2.4.5.1 REPARTO CETEIG

Descripción: CISCO CATALYST 3524
Cantidad: 1
Características:

- 8 Mb Memoria RAM
- 4 Mb Memoria Flash
- Velocidad de transferencia de datos:100 Mbps
- 24 puertos Ethernet 10Base-T, Ethernet 100Base-TX
- Protocolo de gestión remota: SNMP, RMON
- Monitorización en red, capacidad dúplex, enlace ascendente, activable, apilable
- 2 Ranuras de expansión libres

Interfaces:

- 1 gestión - RS-232 - RJ-45 hembra

Figura 2-17: Cisco Catalyst 3524

2.4.5.2 REPARTOS: CETEIG, DIECAR, ESUNA, QUITO, BASNOR

Descripción: CISCO CATALYST 2924
Cantidad: 1 por cada reparto
Características:

- 4 Mb Memoria RAM
- 4 Mb Memoria Flash
- Velocidad de transferencia de datos:100 Mbps
- 24 puertos Ethernet 10Base-T, Ethernet 100Base-TX
- Protocolo de gestión remota: SNMP, RMON
- Monitorización en red, capacidad dúplex, activable.

Interfaces:

- 1 gestión - RS-232 - RJ-45 hembra

Figura 2-18: Cisco Catalyst 2924

2.4.5.3 REPARTOS: DIRABA, DIGMAT, DIGPER

Descripción: CISCO CATALYST 2950
Cantidad: 1 por cada reparto
Características:

- 16 Mb Memoria RAM
- 8 Mb Memoria Flash
- Velocidad de transferencia de datos:100 Mbps
- 12 puertos Ethernet 10Base-T, Ethernet 100Base-TX
- Protocolo de gestión remota: SNMP, RMON
- Auto-sensor por dispositivo, negociación automática, activable

Interfaces:

- 1 gestión - RS-232 - RJ-45 hembra

Figura 2-19: Cisco Catalyst 2950

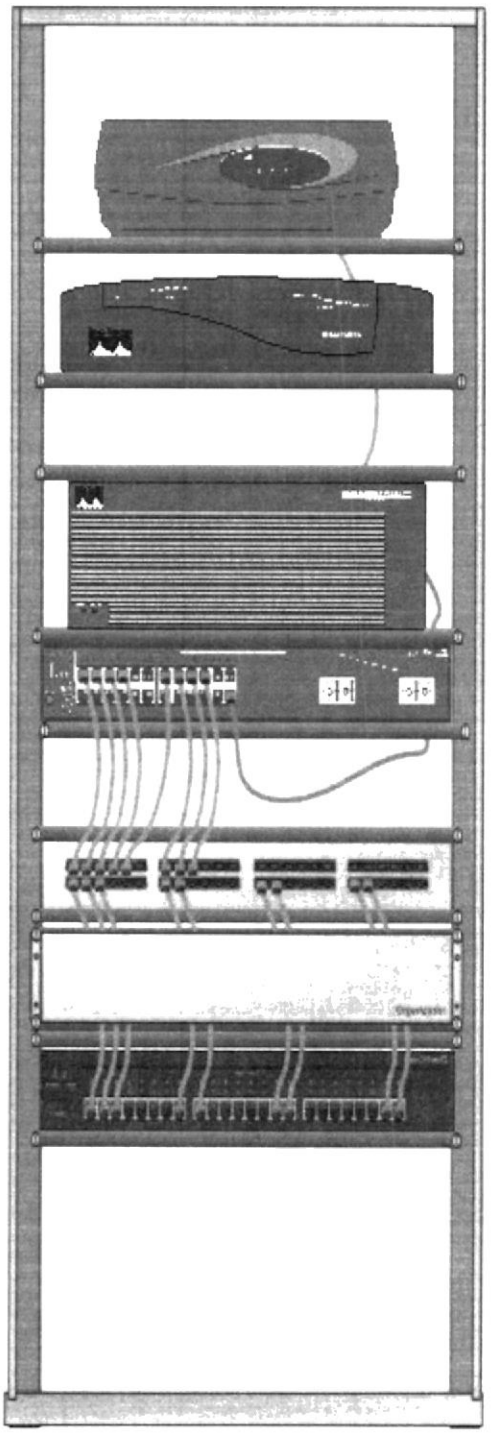
2.4.5.4 REPARTOS: DIRABA, DIGMAT

Descripción: 3COM BASELINE
Cantidad: 1 por cada reparto
Características:

- Velocidad de transferencia de datos:100 Mbps
- 16 puertos Ethernet 10Base-T, Ethernet 100Base-TX
- Control de flujo, capacidad dúplex, conmutador MDI/MDI-X, negociación automática

Figura 2-20: 3COM Baseline

2.4.6 MC DEL EDIFICIO DIGMAT



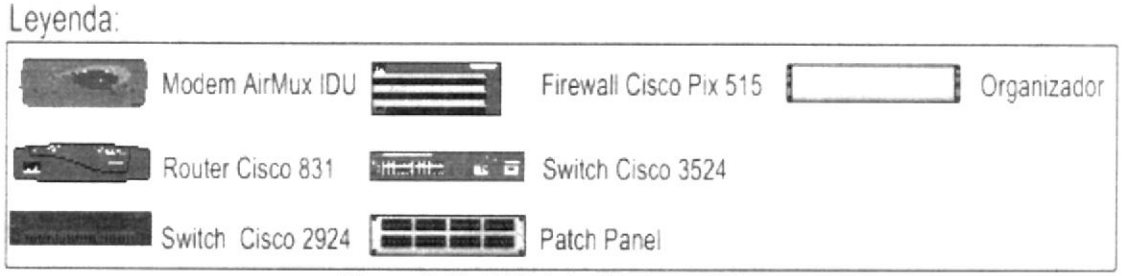


Figura 2-21: MC del edificio DIGMAT

2.4.7 DISTRIBUCIÓN DE BACKBONE VERTICAL EN EDIFICIO DIGMAT

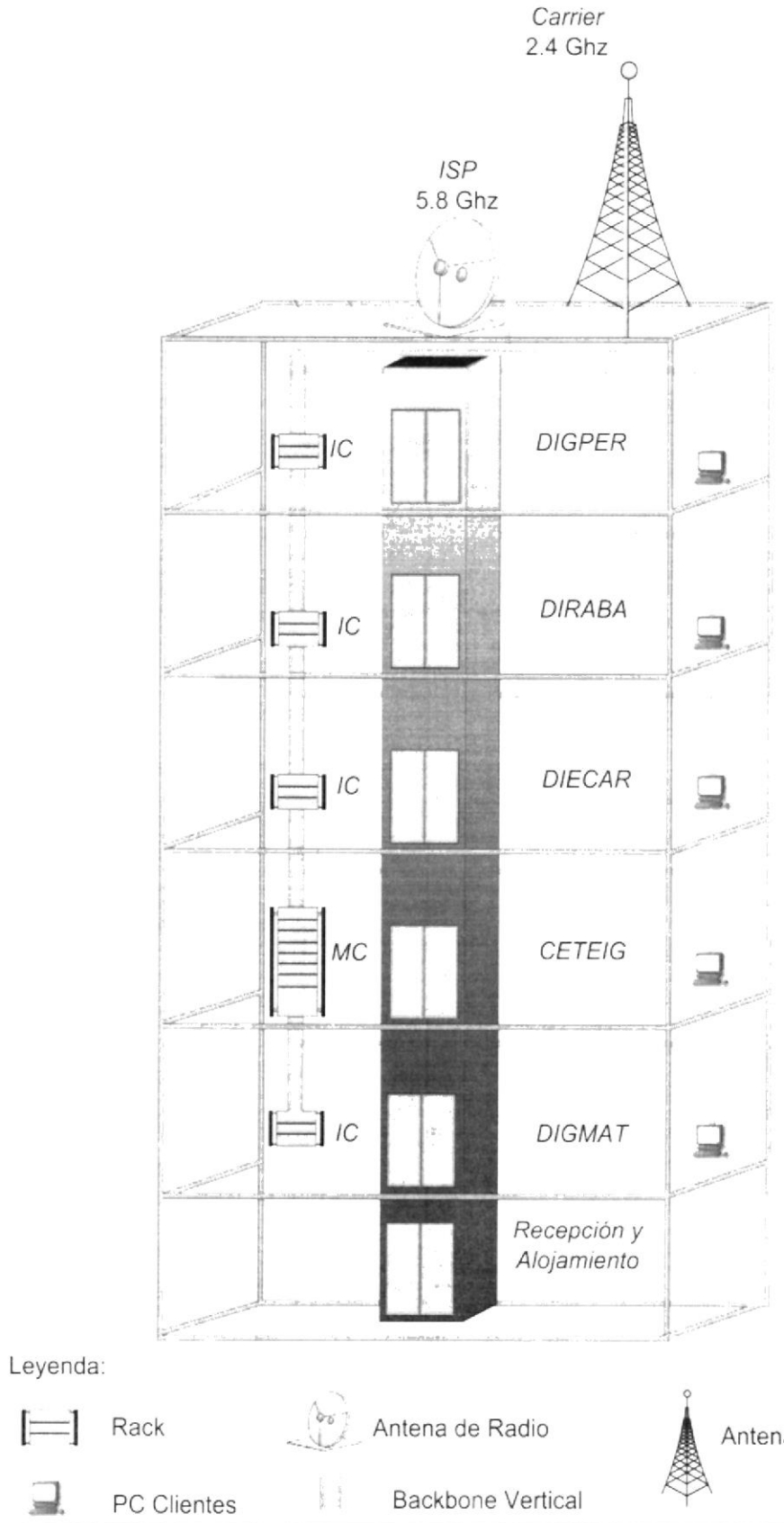


Figura 2-22: Backbone vertical en el edificio DIGMAT

2.4.8 MEDIOS DE COMUNICACIÓN

2.4.8.1 ALÁMBRICOS

2.4.8.1.1 CABLE UTP CATEGORÍA 5E

UTP (del inglés: Unshielded Twisted Pair, par trenzado no apantallado) Son unos conductores de información, generalmente en una red LAN. Se puede emplear distintos tipos de trenzados, dependiendo de la manera en que se la quiera realizar. Se encuentra normalizado de acuerdo a la norma TIA/EIA-568-B.
Es un cable de cobre, y por tanto conductor de electricidad, que se utiliza para telecomunicaciones y que consta de uno o más pares, ninguno de los cuales está blindado (apantallado). Cada par -Pair- es un conjunto de dos conductores aislados con un recubrimiento plástico; este par se trenza -Twisted- para que la señales transportadas por ambos conductores (de la misma magnitud y sentido contrario) no generen interferencias ni resulten sensibles a emisiones. La U de UTP significa 'sin blindaje' ó 'no apantallado' (Unshielded en su original inglés). Esto quiere decir que este cable no incorpora ninguna malla metálica que rodee ninguno de sus elementos (pares) ni el cable mismo.
El cable es más económico, flexible, delgado y fácil de instalar. Además no necesita mantenimiento, ya que ninguno de sus componentes precisa ser puesto a tierra.
Se utiliza en telefonía y redes de ordenadores, por ejemplo en LAN Ethernet (10BASE T) y Fast Ethernet (100 BASE TX); actualmente ha empezado a usarse también en redes Gigabit Ethernet.

Velocidad: 100 Mbps
Ancho de Banda: 100 Mhz

Para Redes Locales los colores estandarizados son:
- Naranja/Blanco - Naranja
- Verde/Blanco - Verde
- Blanco/Azul - Azul
- Blanco/Café – Café

Figura 2-23: Cable UTP Categoría 5e

Emplea conectores especiales, denominados RJ (Registered Jack), siendo los más comúnmente utilizados los RJ-11, (de 4 patillas) y RJ-45 (de 8 patillas).

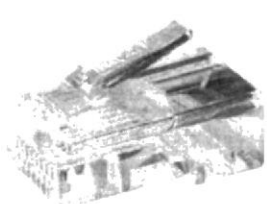


Figura 2-24: Conector RJ-45

2.4.8.2 INALÁMBRICOS

2.4.8.2.1 ANTENAS DE RADIO

HYPERGAIN HG5827G 5.8 GHZ

Figura 2-25: Hypergain HG5827G

Características	
Frecuencia	5725-5850 Mhz
Ganancia	27 DBI
Ancho de Onda Horizontal	6 grados
Ancho de Onda Vertical	9 grados
Impedancia	50 Ohm
Máx. ingreso de energía	100 Watts
Peso	2.4 Kg
Dimensiones	60 cm x 40 cm

Tabla 2-9: Características de Hypergain HG5827G

HYPERGAIN HG2415U 2.4 GHZ

Figura 2-26: Hypergain HG2415U

Características	
Frecuencia	2400-2500 Mhz
Ganancia	15 DBI
Ancho de Onda Horizontal	360 grados
Ancho de Onda Vertical	8 grados
Impedancia	50 Ohm
Máx. ingreso de energía	100 Watts
Peso	1.5 Kg
Dimensiones	1.03 mm x 38.6 mm

Tabla 2-10: Características de Hypergain HG2415U

2.5 INFRAESTRUCTURA WAN

La Armada del Ecuador tiene diferentes repartos, algunos tienen sus propios edificios, el edifico DIGMAT se encuentra conectado con los edificios del reparto ESSUNA y BASNOR, a su vez este último hace de puente para poder conectarse con el edificio del reparto de QUITO.
El proveedor de estos enlaces de datos es Telconet el mismo que funciona de carrier y tienen un ancho de banda de 256 Kbps respectivamente.
Su medio de comunicación es inalámbrico y utilizan antenas de radio (Frec. 2.4 Ghz) para poder conectarse entre los edificios.

2.5.1 ENLACE WAN A NIVEL DE MEDIOS DE COMUNICACIÓN

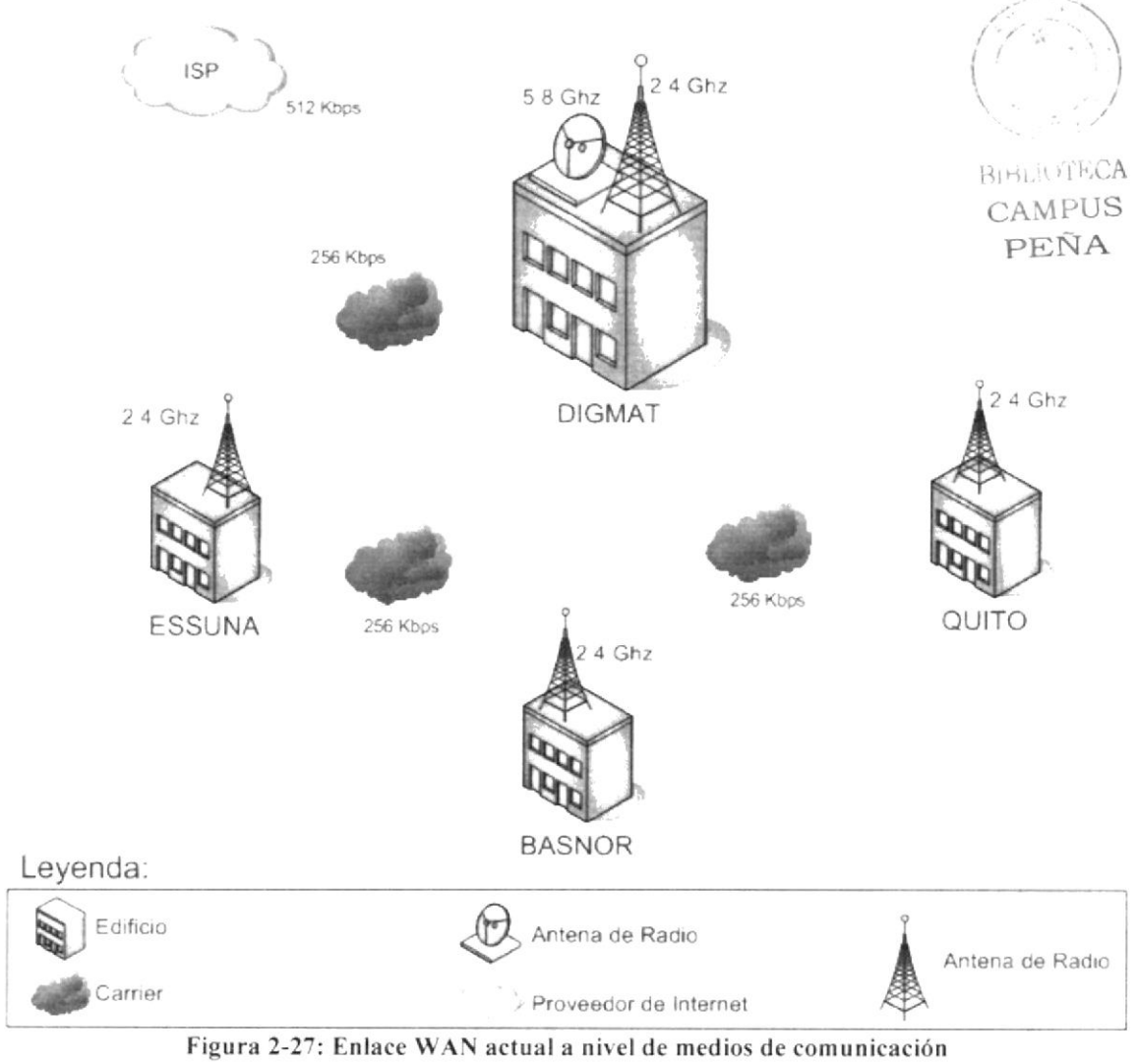


Figura 2-27: Enlace WAN actual a nivel de medios de comunicación

2.5.2 ENLACE WAN A NIVEL DE DISPOSITIVOS DE COMUNICACIÓN

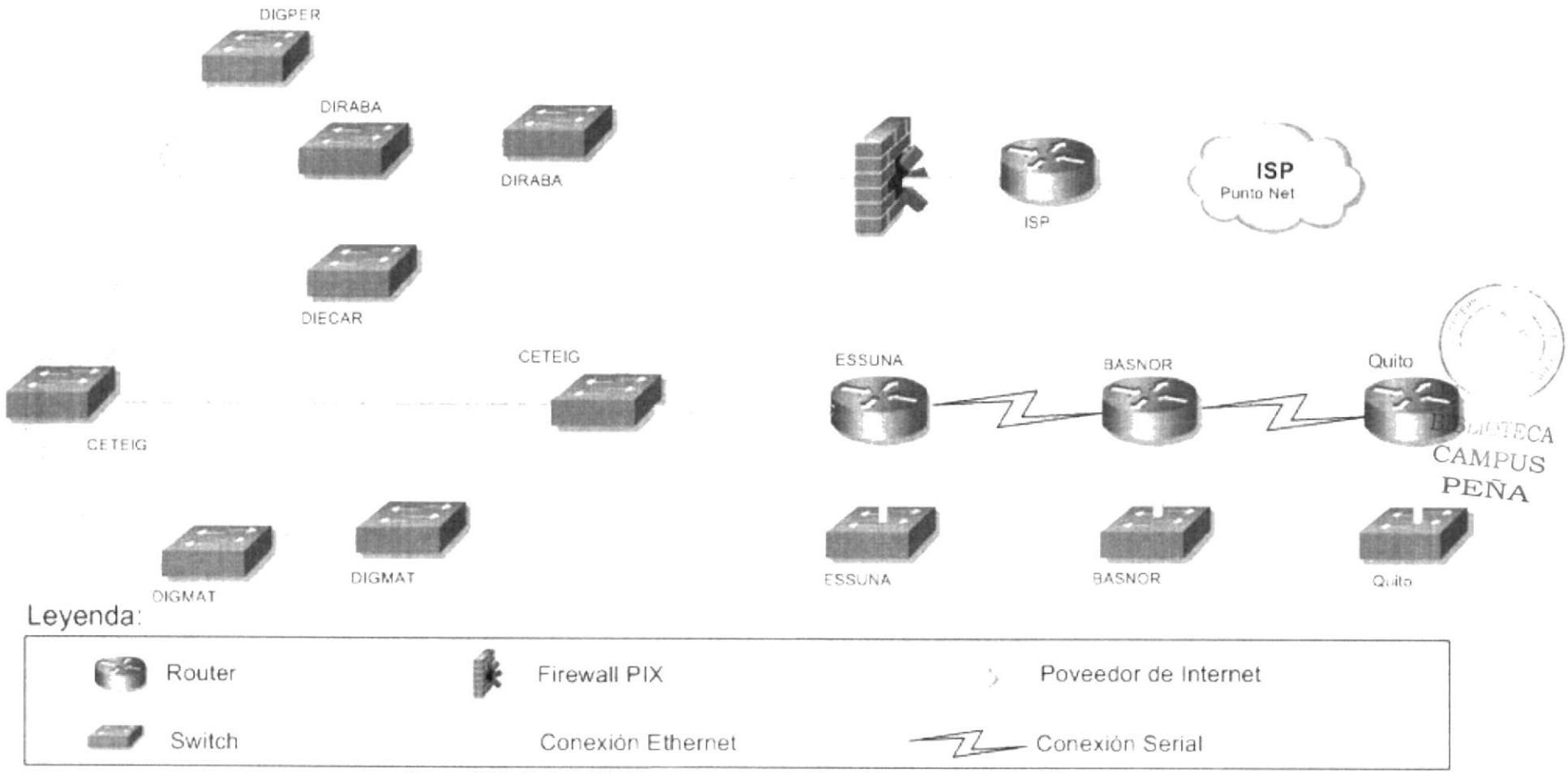


Figura 2-28: Enlace WAN actual a nivel de dispositivos de comunicación

2.5.3 DISPOSITIVOS DE ENRUTAMIENTO

2.5.3.1 MATRIZ DIGMAT

Descripción: CISCO 831
Utilización: Conexión con ISP.
Cantidad: 1
Características:

- Procesador Motorola
- 64 Mb Memoria RAM
- 16 Mb Memoria Flash
- Velocidad de transferencia de datos:100 Mbps
- Protocolo de direccionamiento: IGRP, RIP-1, RIP-2
- Protocolo de gestión remota: SNMP, Telnet
- Protección Firewall, soporte de DHCP, soporte de NAT, VPN, soporte para PAT, soporte para Syslog.

Interfaces:

- 2 Ethernet 10Base-T/100Base-TX - RJ-45
- 1 gestión - consola - RJ-45

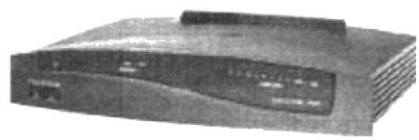


Figura 2-29: Cisco 831

2.5.3.2 SUCURSALES: BASNOR, ESSUNA, QUITO

Descripción: CISCO 2621
Utilización: Conexión entre repartos
Cantidad: 1 por cada reparto
Características:

- Procesador Motorola MPC860 50 Mhz
- 64 Mb Memoria RAM
- 32 Mb Memoria Flash
- Velocidad de transferencia de datos: 100 Mbps
- Protocolo de direccionamiento: OSPF, BGP, RIP-1, RIP-2
- Protocolo de gestión remota: RMON
- VPN, soporte de NAT, Firewall, enrutamiento entre VLAN, soporte DHCP.
- 4 Ranuras de expansión libres

Interfaces:

- 2 red - Ethernet 10Base-T/100Base-TX - RJ-45
- 2 seriales RS-232 (DB-15)
- 1 gestión - consola - RJ-45
- 1 red - auxiliar - RJ-45

Figura 2-30: Cisco 2621

2.6 SEGURIDAD

Ubicación: Reparto CETEIG
Descripción: CISCO PIX 515E
Cantidad: 1
Características:

- Procesador Intel Celeron 433 Mhz x86-to-RISC
- 64 Mb Memoria RAM
- 16 Mb Memoria Flash
- Velocidad de transferencia de datos:100 Mbps
- Protocolo de direccionamiento: OSPF
- Protocolo de gestión remota: SNMP
- Túneles VPN: 200
- Sesiones concurrentes : 130000
- Protección firewall, criptografía 56 bits, criptografía 168 bits, soporte de DHCP, soporte de NAT, VPN, soporte para PAT, soporte VLAN, filtrado de contenido, activable, soporte IPv6, cifrado de 256 bits, prevención de ataque Dos, Quality of Service (QoS)

Interfaces:

- 2 red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 gestión - consola - RJ-45
- 1 redistribución - RS-232 - D-Sub de 15 espigas (DB-15)

Figura 2-31: Cisco PIX 515E

2.7 CONEXIÓN A INTERNET

La conexión a Internet se lo realiza a través de radio con una frecuencia de 5.8 Ghz con un ancho de banda de 512 Kbps, su proveedor es Punto Net.

2.7.1 INTERNET A NIVEL DE MEDIOS

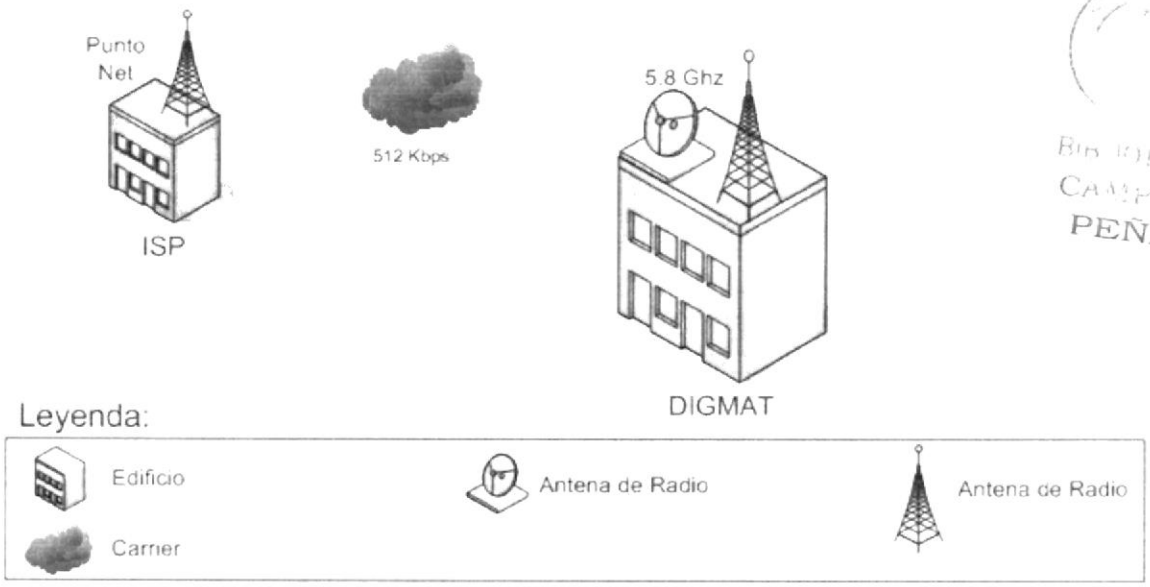


Figura 2-32: Internet a nivel de medios de comunicación

2.7.2 INTERNET A NIVEL DE DISPOSITIVOS

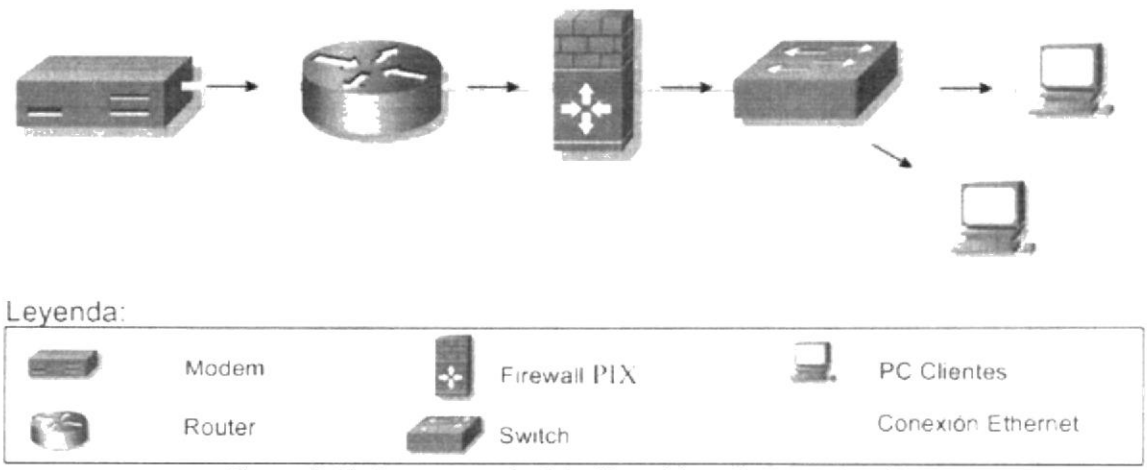


Figura 2-33: Internet a nivel de dispositivos de comunicación

2.8 PROBLEMAS ENCONTRADOS

- Congestionamiento de la red LAN
- Ancho de banda de Internet insuficiente
- No existe enlace WAN entre Matriz DIGMAT y Sucursal Quito
- Personal técnico poco capacitado en el área de redes (CETEIG).

CAPÍTULO 3

SOLUCIÓN PROPUESTA

3 SOLUCIÓN PROPUESTA

3.1 PROBLEMAS ENCONTRADOS

Problema	Causa	Efecto
Congestionamiento de la Red LAN	Existencia de Broadcast	Tiempos de respuesta altos en los usuarios finales. lentitud en la red.
Ancho de Banda de Internet Insuficiente	Numerosa cantidad de usuarios navegando	Lentitud en la navegación
No existe enlace WAN entre Matriz DIGMAT y Sucursal Quito	Falta de planificación al implementar enlaces WAN.	Pérdida de comunicación entre Matriz y sucursal.
Personal técnico poco capacitado en el área de redes (CETEIG).	Falta de asignación de recursos económicos para la capacitación del personal de CETEIG.	Gastos adicionales en contratar técnicos capacitados.

Tabla 3-1: Problema, causa, efecto

3.2 SOLUCIÓN PROPUESTA

Problema	Solución	Alcance
Congestionamiento de la Red LAN.	Creación de Redes Virtuales (VLAN's).	Reducción de dominios de broadcast.
Ancho de Banda de Internet Insuficiente.	Segmentar y aumentar el ancho de banda.	Mayor perfomance en navegación de Internet.
No existe enlace WAN entre Matriz DIGMAT y Sucursal Quito.	Creación de enlace WAN entre Matriz DIGMAT y sucursal Quito.	Comunicación permanente y efectiva entre todas las sucursales.
Personal técnico poco capacitado en el área de redes (CETEIG).	Capacitación técnica en redes del personal de CETEIG.	Resolución de problemas técnicos de redes a tiempo.

Tabla 3-2: Problema, solución, alcance

3.3 ESTUDIO DE FACTIBILIDAD

3.3.1 ALTERNATIVA A

- El objetivo de esta alternativa es colocar un dispositivo de enrutamiento central mediante el cual se puedan establecer conexiones entre las diferentes sucursales y a su vez poder comunicar las VLAN's de los diferentes repartos.

3.3.1.1 FACTIBILIDAD TÉCNICA

Cant.	Descripción	Ubicación
1	Router	Reparto ESSUNA

Tabla 3-3: Factibilidad técnica A

Características:

- 64 Mb Memoria RAM
- 32 Mb Memoria Flash
- Protocolo de direccionamiento: OSPF, HSRP, RIP-2
- Protocolo de gestión remota: SNMP, RMON, Telnet
- VPN, soporte de NAT, Firewall, enrutamiento entre VLAN, DHCP
- 1 Ranuras de expansión libre (memoria)

Interfaces:

- 1 red - Ethernet 10Base-T/100Base-TX - RJ-45
- 2 seriales RS-232 (DB-15)
- 1 gestión - consola - RJ-45
- 1 red - auxiliar - RJ-45

3.3.1.2 FACTIBILIDAD OPERATIVA

Cant.	Actividad	Semanas
	Fase de Análisis de red LAN y WAN	
1	Ingeniero de Telecomunicaciones	1
1	Analista de Soporte	1
	Fase de Diseño de red WAN	
1	Ingeniero de Telecomunicaciones	1
	Fase de Implementación de red WAN	
1	Ingeniero de Telecomunicaciones	1
1	Técnico en Redes	1
	Fase de Prueba de red WAN	
1	Ingeniero de Telecomunicaciones	1
1	Técnico en Redes	1
	Fase de Documentación de red WAN	
1	Ingeniero de Telecomunicaciones	1
1	Analista de Soporte	1

Tabla 3-4: Factibilidad operativa A

3.3.1.3 FACTIBILIDAD ECONÓMICA

3.3.1.3.1 COSTOS DE HARDWARE

Cant.	Descripción	Valor Unitario	Total
1	Router	1.300,00	1.300,00
Total			**$ 1.300,00**

Tabla 3-5: Costos de hardware A

3.3.1.3.2 COSTOS OPERATIVOS

Cant.	Actividad	Semanas	Costo Semanal	Total
	Fase de Diseño de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
	Fase de Implementación de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
1	Técnico en Redes	1	70,00	70,00
	Fase de Prueba de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
1	Técnico en Redes	1	70,00	70,00
	Fase de Documentación de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
1	Analista de Soporte	1	80,00	80,00
Total				**$ 700,00**

Tabla 3-6: Costos operativos A

3.3.1.3.3 COSTOS DE ENLACES

Cant.	Descripción	Valor	Total
1	Instalación de enlace de Internet	450,00	450,00
1	Instalación de enlace de Datos	450,00	450,00
Total Instalación			**$ 900,00**
	Descripción	**Valor Mensual**	**Total**
1	Internet a 1 Mbps por Fibra óptica mono.	1.200,00	1.200,00
1	Datos a 256 Kbps por Fibra óptica mono.	400,00	400,00
Total Mensual			**$ 1.600,00**

Tabla 3-7: Costos de enlaces A

3.3.1.4 COSTO TOTAL DE LA ALTERNATIVA A

Factibilidad	Total
Costos de Hardware	1.300,00
Costos Operativos	700,00
Costos de Enlaces	900,00
Total	**$ 2.900,00**

Tabla 3-8: Costo total de alternativa A

3.3.1.5 FORMA DE PAGO

- 60% Al aceptar la Propuesta
- 20% Al iniciar la Fase de Implementación
- 20% Al culminar el Proyecto

3.3.1.6 VENTAJAS

- Descongestionamiento de la red.
- Rendimiento óptimo de red.
- Alta velocidad en el acceso a Internet.
- Administración centralizada y monitoreo del enlace WAN
- Rápida detección de posibles errores en la comunicación entre los dispositivos intercomunicados.

3.3.1.7 BENEFICIOS

- Conexión permanente entre Matriz y sucursales.
- Eliminación de gastos en contratación de personal ajeno a CETEIG.
- Ahorro de tiempo y mejora de productividad en los repartos.

3.3.1.8 GARANTÍA

Se otorgará un período de garantía una vez culminado el proyecto, el cual será de 3 meses, tiempo en el cual nos comprometemos a brindar el soporte respectivo sin ningún costo adicional. Pasado este período se procederá a realizar el cobro de los respectivos honorarios.

La garantía del equipo es de 1 año, a partir de la compra del mismo, esta garantía es cubierta por el proveedor del equipo.

3.3.1.9 DIAGRAMA DE GANTT A

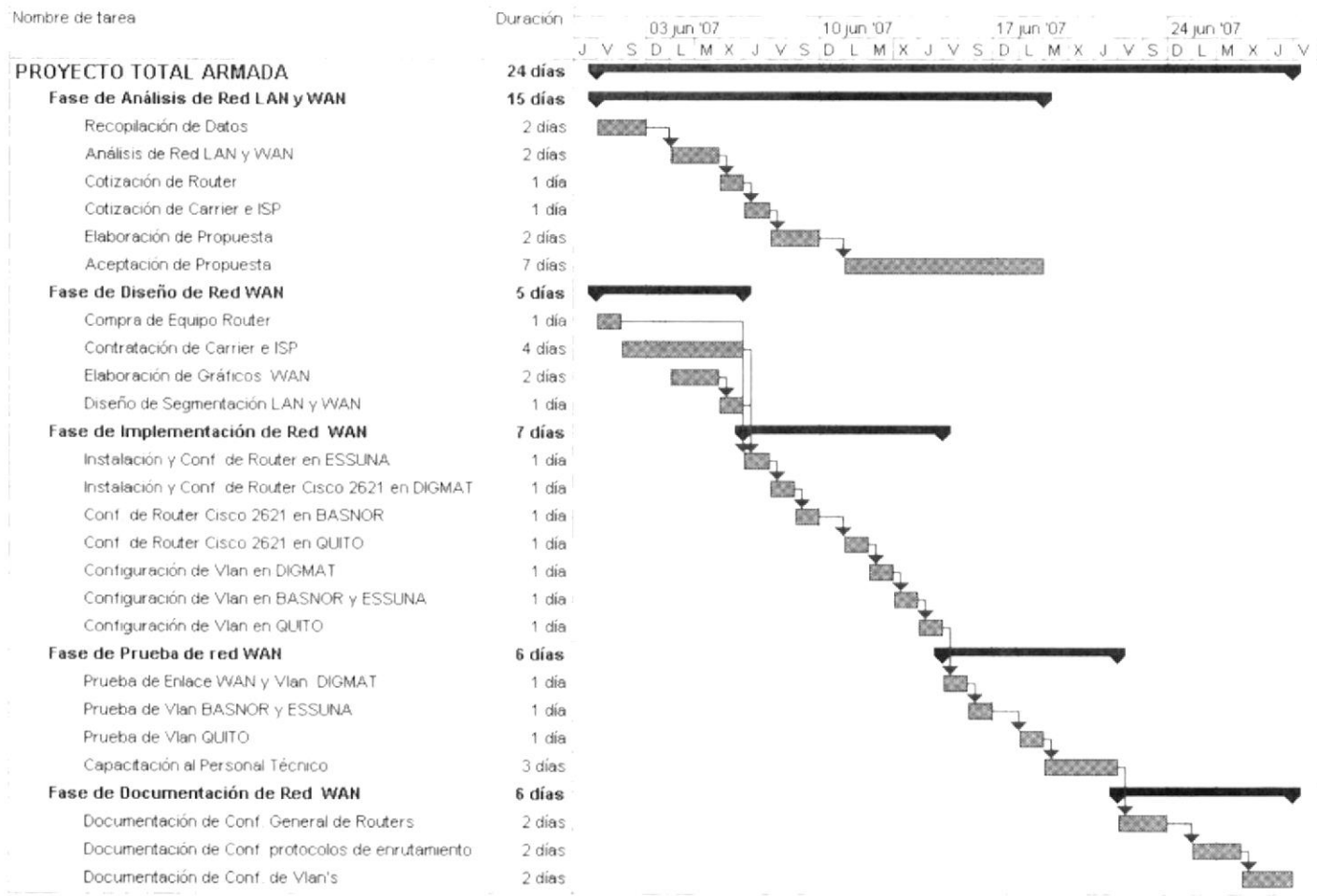


Figura 3-1: Diagrama de Gantt A

3.3.2 ALTERNATIVA B

- El objetivo de esta alternativa es igual al de la anterior, pero con un costo de inversión inferior, debido a que se invertirá en un equipo de menor costo, y los enlaces serán a través de otros medios de transmisión.

3.3.2.1 FACTIBILIDAD TÉCNICA

Cant.	Descripción	Ubicación
1	Router	Reparto ESSUNA

Tabla 3-9: Factibilidad técnica B

Características:

- 64 Mb Memoria RAM
- 8 Mb Memoria Flash
- Protocolo de direccionamiento: OSPF, BGP-4,RIP-1, RIP-2
- Protocolo de gestión remota: SNMP, Telnet
- Protección firewall, soporte de NAT, VPN, soporte VLAN

Interfaces:

- 1 red - Ethernet 10Base-T/100Base-TX - RJ-45
- 2 seriales RS-232 (DB-50)
- 1 gestión - consola - RJ-45
- 1 red - auxiliar - RJ-45

3.3.2.2 FACTIBILIDAD OPERATIVA

Cant.	Actividad	Semanas
	Fase de Análisis de red LAN y WAN	
1	Ingeniero de Telecomunicaciones	1
1	Analista de Soporte	1
	Fase de Diseño de red WAN	
1	Ingeniero de Telecomunicaciones	1
	Fase de Implementación de red WAN	
1	Ingeniero de Telecomunicaciones	1
1	Técnico en Redes	1
	Fase de Prueba de red WAN	
1	Ingeniero de Telecomunicaciones	1
1	Técnico en Redes	1
	Fase de Documentación de red WAN	
1	Ingeniero de Telecomunicaciones	1
1	Analista de Soporte	1

Tabla 3-10: Factibilidad operativa B

3.3.2.3 FACTIBILIDAD ECONÓMICA

3.3.2.3.1 COSTOS DE HARDWARE

Cant.	Descripción	Valor Unitario	Total
1	Router	800,00	800,00
Total			**$ 800,00**

Tabla 3-11: Costos de hardware B

3.3.2.3.2 COSTOS OPERATIVOS

Cant.	Actividad	Semanas	Costo Semana	Total
	Fase de Diseño de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
	Fase de Implementación de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
1	Técnico en Redes	1	70,00	70,00
	Fase de Prueba de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
1	Técnico en Redes	1	70,00	70,00
	Fase de Documentación de red WAN			
1	Ingeniero de Telecomunicaciones	1	120,00	120,00
1	Analista de Soporte	1	80,00	80,00
Total				**$ 700,00**

Tabla 3-12: Costos operativos B

3.3.2.3.3 COSTOS DE ENLACES

Cant.	Descripción	Valor	Total
1	Instalación de enlace de Datos	300,00	300,00
Total Instalación			**$ 300,00**
Cant.	**Descripción**	**Valor mensual**	**Total**
1	Internet a 1 Mbps por Radio.	1.000,00	1.000,00
1	Datos a 256 Kbps por Radio.	400,00	400,00
Total Mensual			**$ 1.400,00**

Tabla 3-13: Costos de enlaces B

3.3.2.4 COSTO TOTAL DE LA ALTERNATIVA B

Factibilidad	Total
Costos de Hardware	800,00
Costos Operativos	700,00
Costos de Enlaces	300,00
Total	**$ 1.800,00**

Tabla 3-14: Costo total de alternativa B

3.3.2.5 FORMA DE PAGO

- 60% Al aceptar la Propuesta
- 20% Al iniciar la fase de Implementación
- 20% Al culminar la fase de Documentación

3.3.2.6 VENTAJAS

- Descongestionamientos en la red
- Rendimiento de red óptimo.
- Velocidad en el acceso a Internet.
- Administración centralizada y monitoreo del enlace WAN
- Rápida detección de posibles errores en la comunicación entre los dispositivos intercomunicados.

3.3.2.7 BENEFICIOS

- 38% de ahorro con respecto a la alternativa anterior
- Eliminación de gastos en contratación de personal ajeno a CETEIG.
- Conexión permanente entre Matriz y sucursales.
- Ahorro de tiempo y mejora de productividad en los repartos.

3.3.2.8 GARANTÍA

Se otorgará un período de garantía una vez culminado el proyecto, el cual será de 3 meses, tiempo en el cual nos comprometemos a brindar el soporte respectivo sin ningún costo adicional. Pasado este período se procederá a realizar el cobro de los respectivos honorarios.

La garantía del equipo es de 1 año, a partir de la compra del mismo, esta garantía es cubierta por el proveedor del equipo.

3.3.2.9 DIAGRAMA DE GANTT B

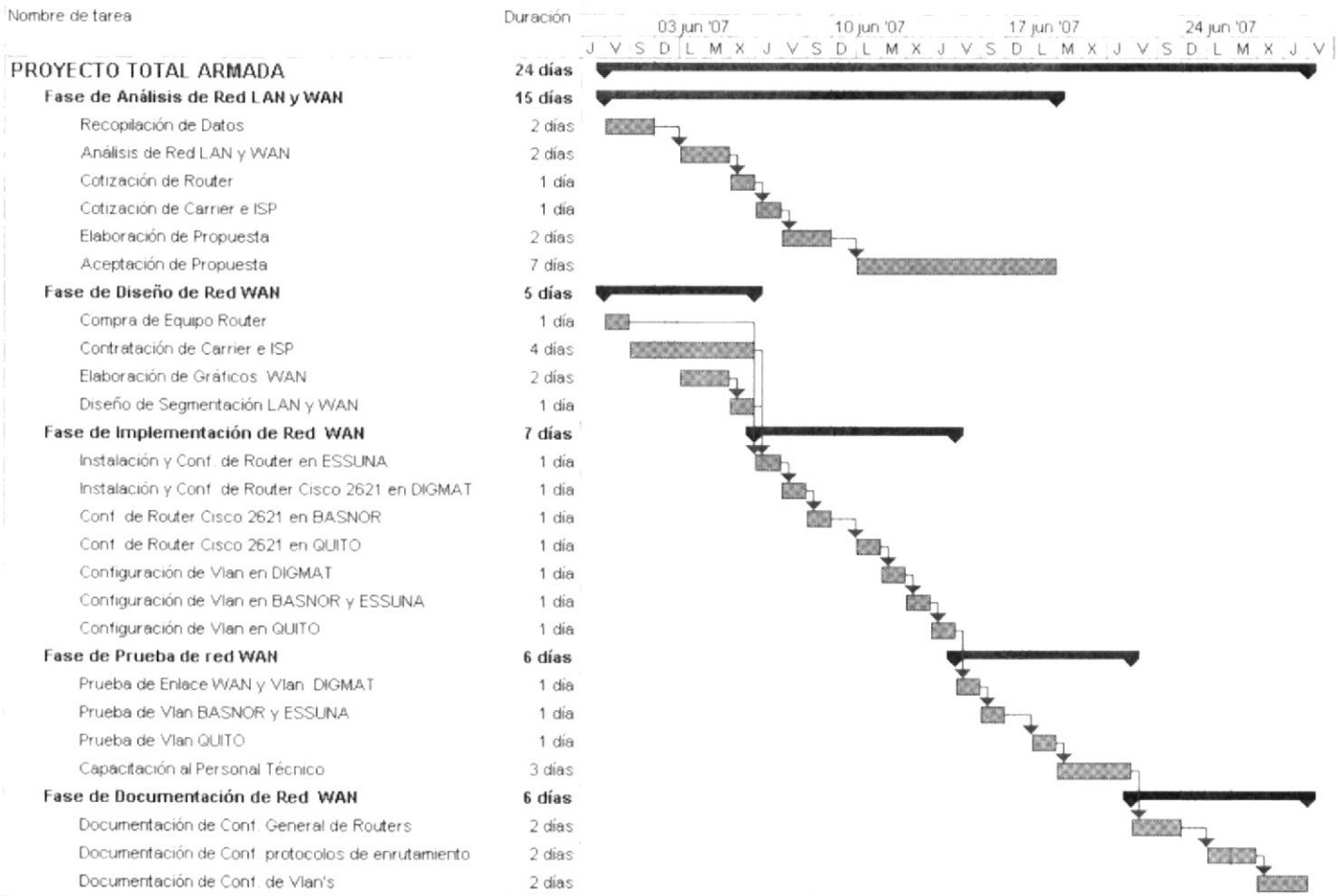


Figura 3-2: Diagrama de Gantt B

CAPÍTULO 4

IMPLEMENTACIÓN

4 IMPLEMENTACIÓN

4.1 ENLACE WAN A NIVEL DE MEDIOS

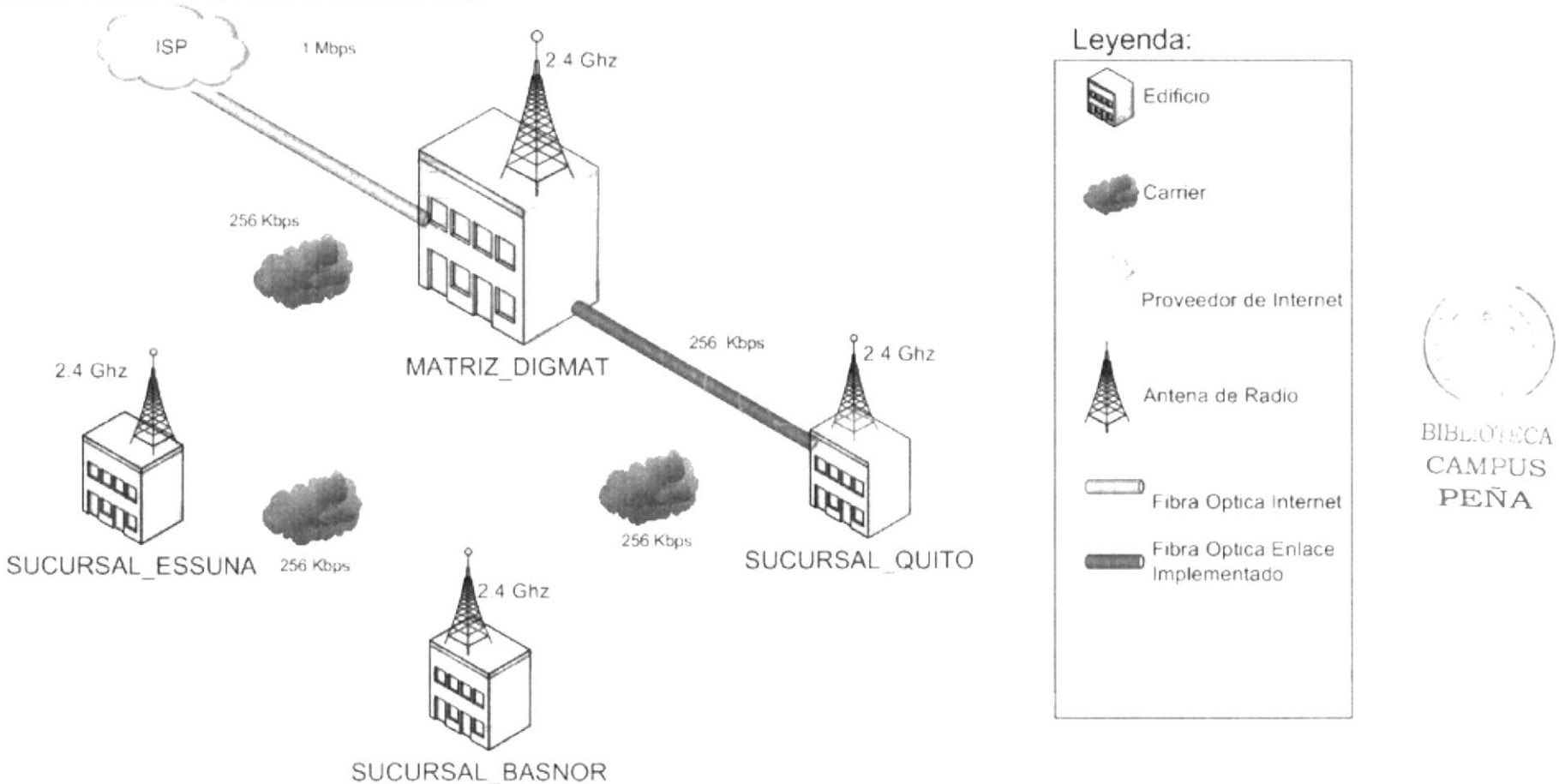


Figura 4-1: Enlace WAN implementado a nivel de medios de comunicación

4.2 ENLACE WAN A NIVEL DE DISPOSITIVOS

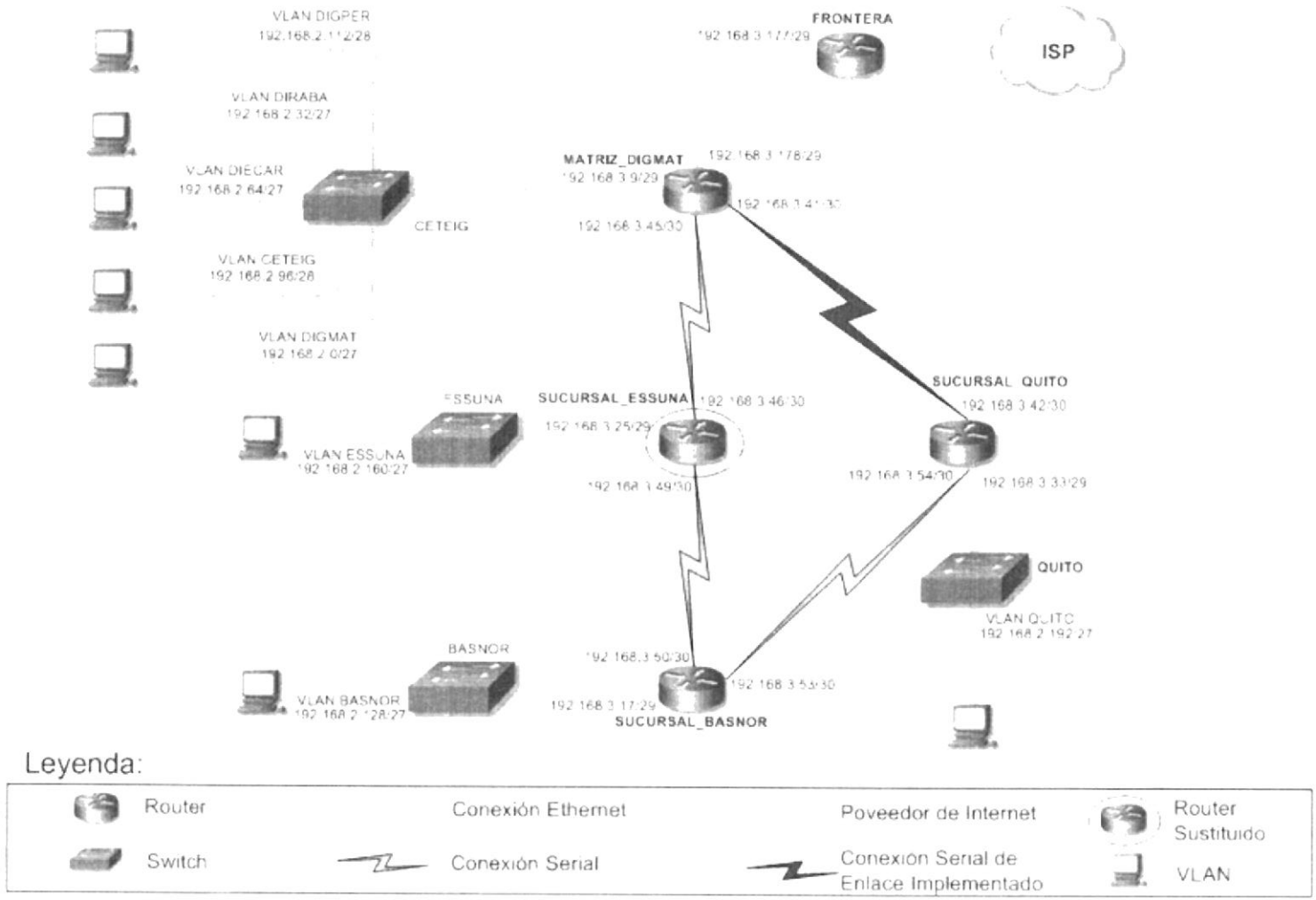


Figura 4-2: Enlace WAN implementado a nivel de dispositivos de comunicación

CAPÍTULO 5

NORMATIVAS DE CABLEADO ESTRUCTURADO

5 NORMATIVAS DE CABLEADO ESTRUCTURADO

5.1 NORMATIVAS OBLIGATORIAS

1 ▲

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

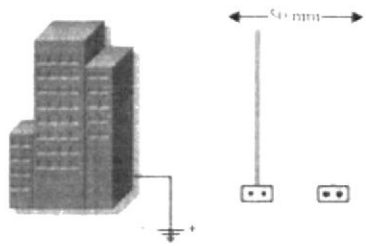


Figura 5-1: Normativa obligatoria 1

2 ▲

El cableado horizontal deberá estar configurado como topología estrella, con cada salida de telecomunicaciones conectadas con un HC.

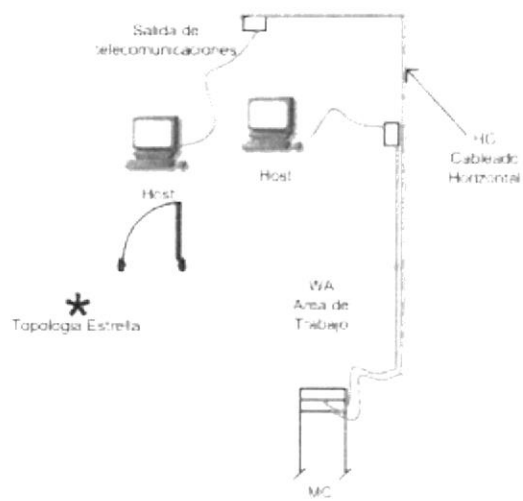


Figura 5-2: Normativa obligatoria 2

3 ▲

Se emplearán conexiones cruzadas para conexiones entre cableado horizontal y backbone y para conexiones entre cableado horizontal y equipos con salidas de puerto múltiple.

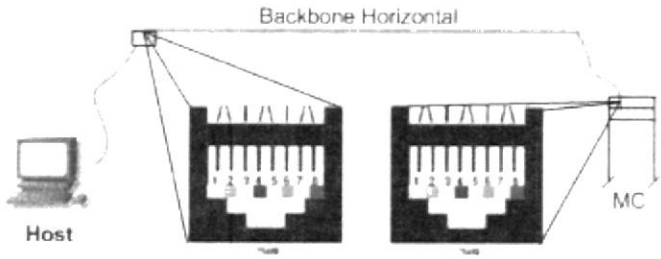


Figura 5-3: Normativa obligatoria 3

4 ▲

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

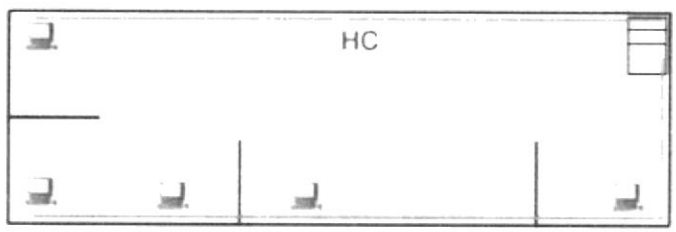


Figura 5-4: Normativa obligatoria 4

5 ▲

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

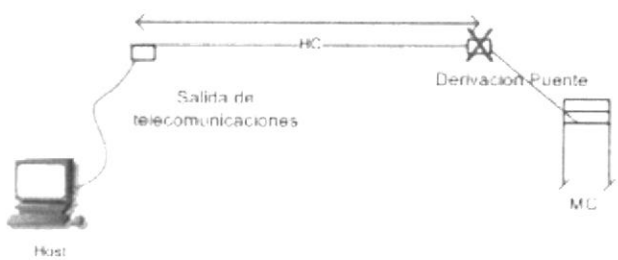


Figura 5-5: Normativa obligatoria 5

6 ▲

La longitud del cable entre la salida de telecomunicaciones y el HC no excederá los 90 metros independientemente del tipo del medio.

Figura 5-6: Normativa obligatoria 6

7 ▲

La longitud individual o combinada de patchcord de par trenzado balanceado 24 AWG (calibre americano de alambre) o fibra óptica utilizado en el HC no excederá los 5 metros.

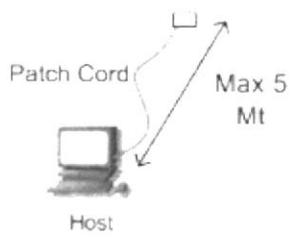


Figura 5-7: Normativa obligatoria 7

8 ▲

La longitud del canal del cableado horizontal incluyendo los patchcords de equipos en ambos extremos no excederá los 100 metros independientemente del medio.

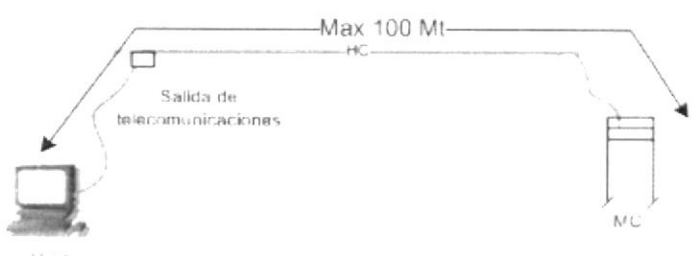


Figura 5-8: Normativa obligatoria 8

9 ▲

La longitud de los cordones del cable del área de trabajo de par trenzado balanceado no excederá los 20 metros cuando se use un punto de consolidación.

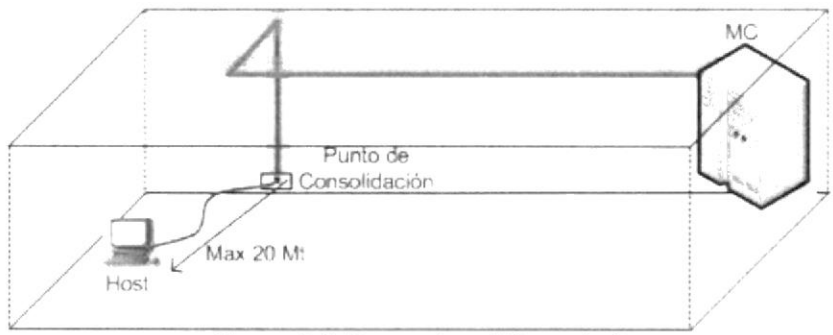


Figura 5-9: Normativa obligatoria 9

10 ▲

No se permitirá más de un punto de consideración dentro del mismo tendido de cable horizontal.

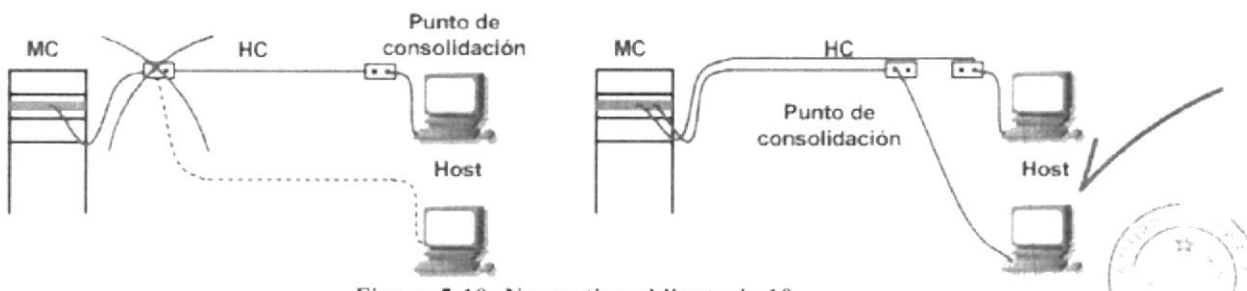


Figura 5-10: Normativa obligatoria 10

11 ▲

No se permitirán conexiones cruzadas o equipo activo en el punto de consolidación.
Punto de consolidación: Es un hardware de conexión que proporciona una interconexión entre cableado de oficina abierto y el cableado horizontal.

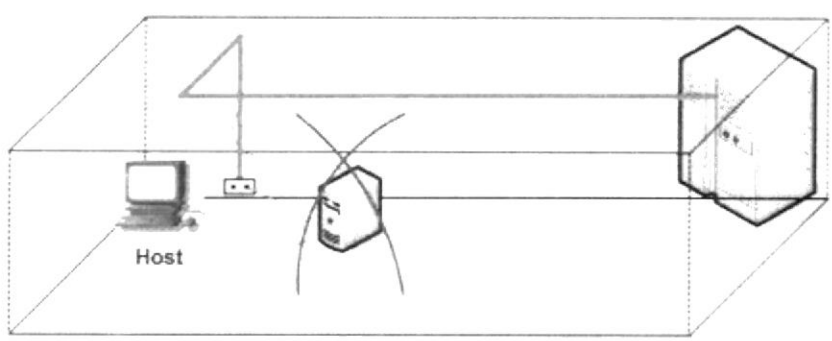


Figura 5-11: Normativa obligatoria 11

12 ▲

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

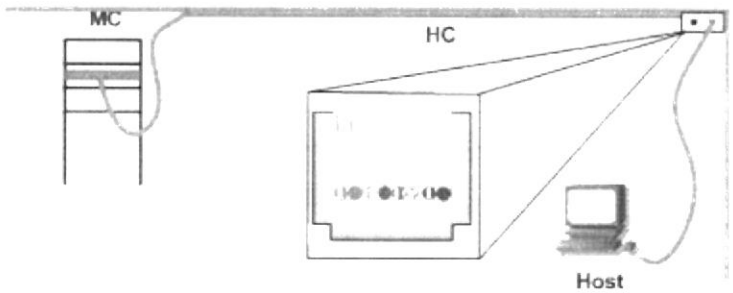


Figura 5-12: Normativa obligatoria 12

13 ▲

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

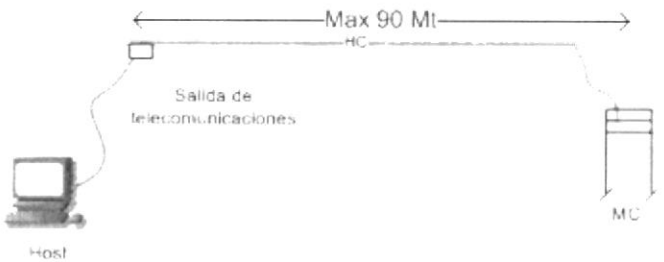


Figura 5-13: Normativa obligatoria 13

14 ▲

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

Figura 5-14: Normativa obligatoria 14

15 ▲

La distancia mínima entre el punto consolidación y la salida de telecomunicaciones será de 15 metros.

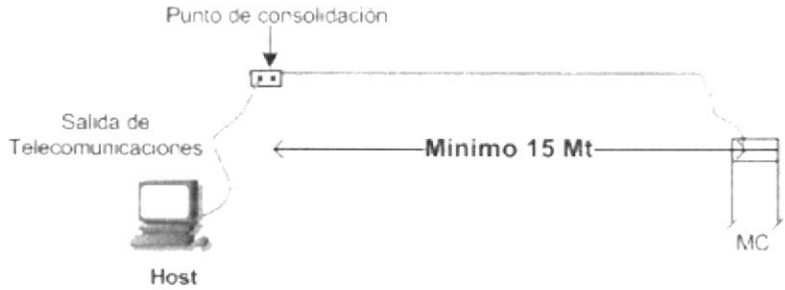


Figura 5-15: Normativa obligatoria 15

16 ▲

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

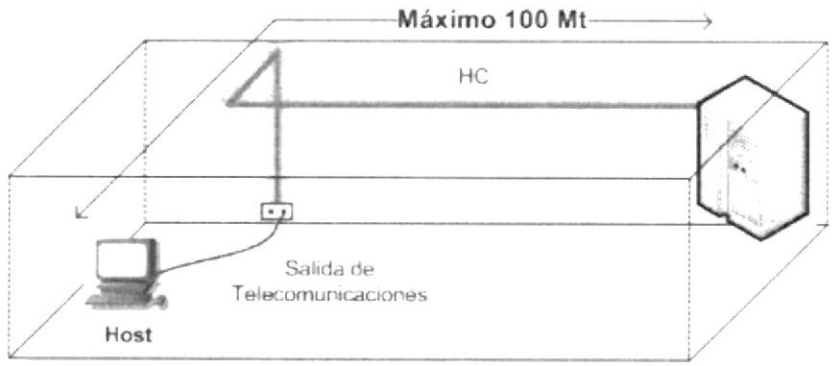


Figura 5-16: Normativa obligatoria 16

17 ▲

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

Figura 5-17: Normativa obligatoria 17

18 ▲

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

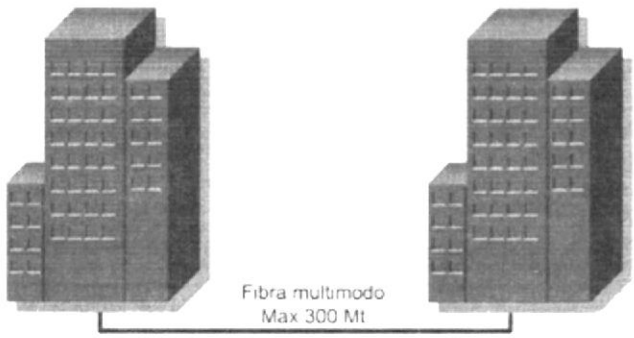


Figura 5-18: Normativa obligatoria 18

19 ▲

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

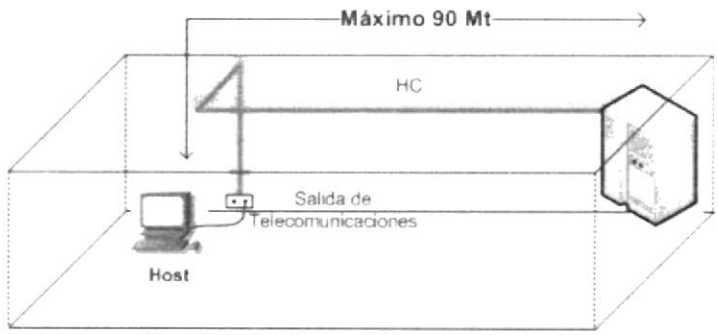


Figura 5-19: Normativa obligatoria 19

20 ▲

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

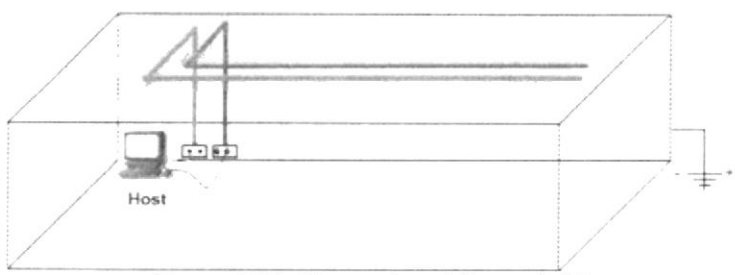


Figura 5-20: Normativa obligatoria 20

21 ▲

Las canalizaciones horizontales serán apropiadas para el ambiente en el cual se instalarán y no se obstaculizarán por ductos de calefacción, ventilación y aire acondicionado, distribución de energía eléctrica o estructuras del edificio.

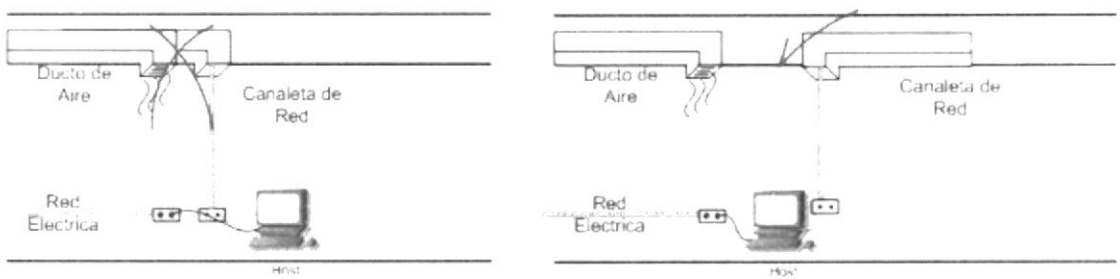


Figura 5-21: Normativa obligatoria 21

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.

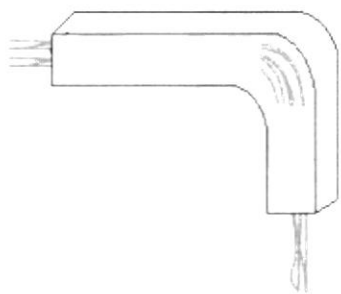


Figura 5-22: Normativa obligatoria 22

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 máximo de 30 metros.

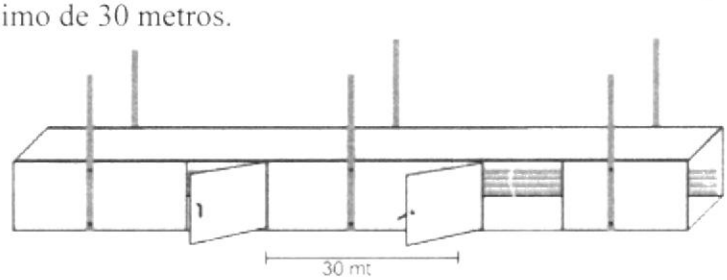


Figura 5-23: Normativa obligatoria 23

24 ▲

El backbone usará la topología tipo estrella jerárquica con respecto al MC.

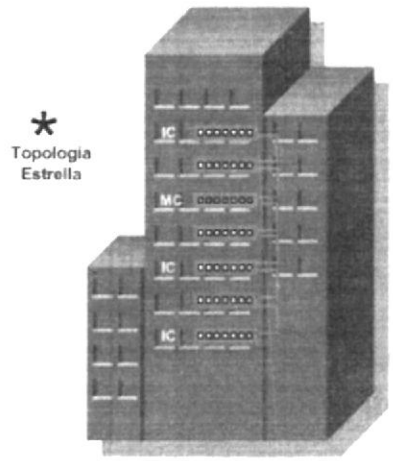


Figura 5-24: Normativa obligatoria 24

25 ▲

Para cada tendido de backbone de edificio que sea mayor de 100 metros de longitud debe proveerse cable de fibra óptica

Figura 5-25: Normativa obligatoria 25

26 ▲

La longitud total del canal de cable entre el MC y cualquier HC no excederá los siguientes límites:
3.000 metros para fibra óptica monomodo.
2.000 metros para fibra óptica multimodo.
2.000 metros para par trenzado para aplicación PBX.

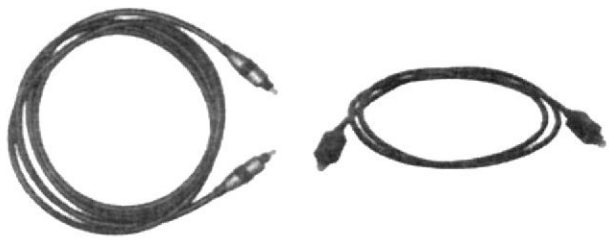


Figura 5-26: Normativa obligatoria 26

27 ▲

Las canalizaciones de edificio proveerán acceso a todos los cuartos de telecomunicación, cuartos de equipos y acometidas localizadas en el mismo edificio.

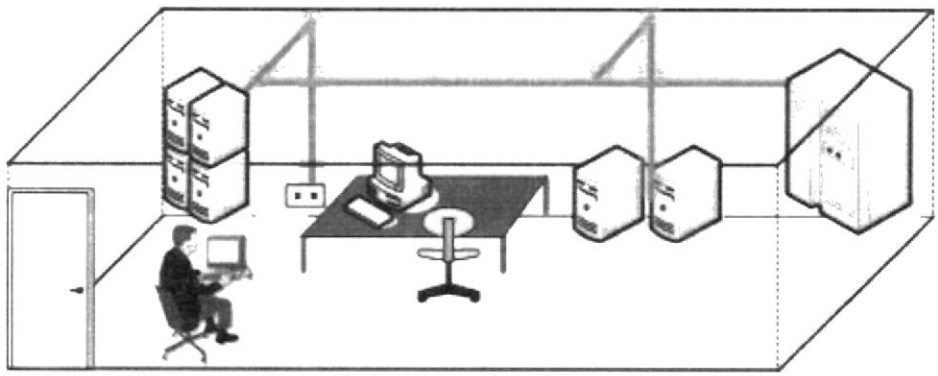


Figura 5-27: Normativa obligatoria 27

28 ▲

Las canalizaciones no se ubicarán en ductos de ascensores.

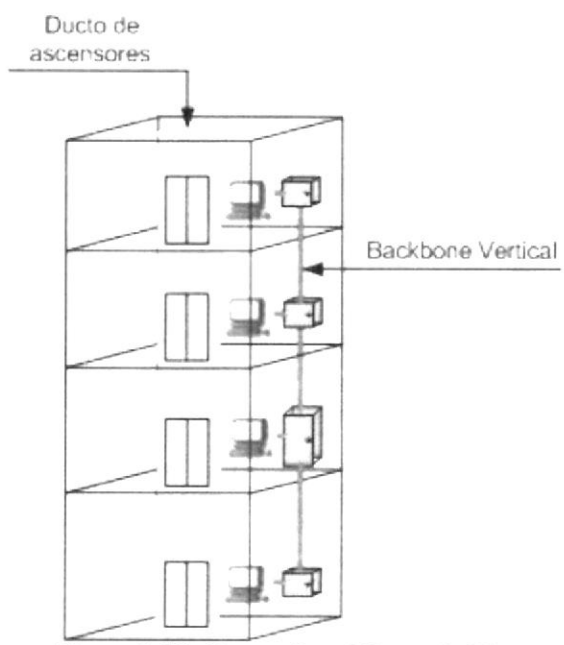


Figura 5-28: Normativa obligatoria 28

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.

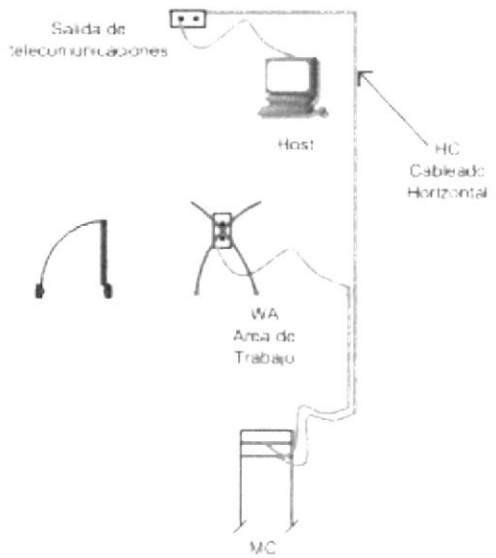


Figura 5-29: Normativa obligatoria 29

30 ▲

El cuarto de telecomunicaciones se diseñará y equipará para contener equipos de telecomunicaciones, terminaciones de cables y asociados.

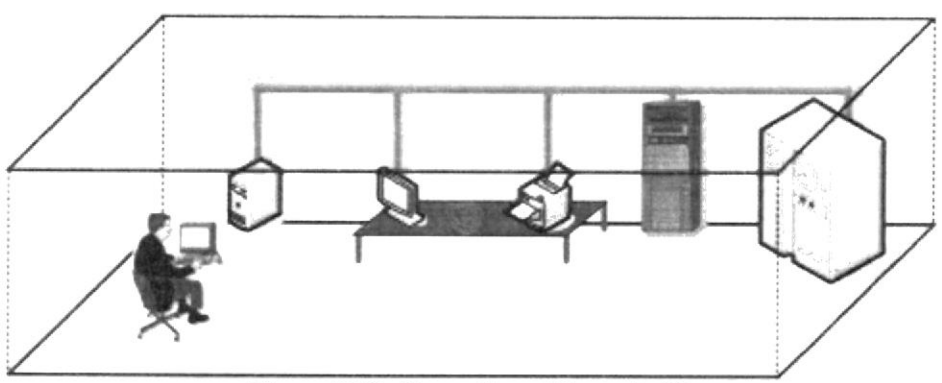


Figura 5-30: Normativa obligatoria 30

31 ▲

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

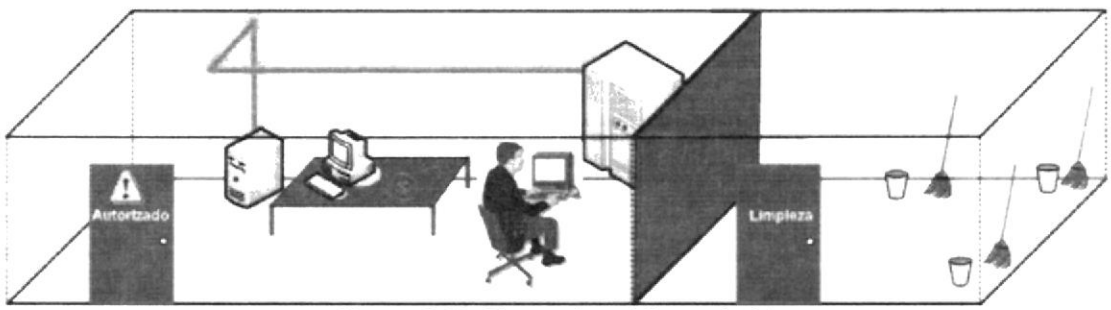


Figura 5-31: Normativa obligatoria 31

32 ▲

Las instalaciones de cable puesto a tierra cumplirán con los reglamentos y normas aplicables.

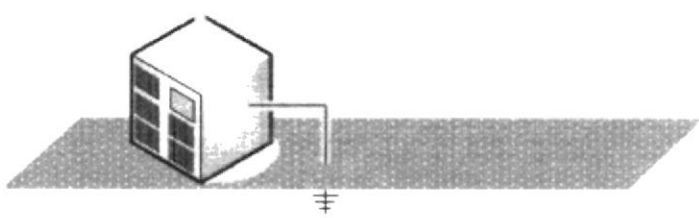


Figura 5-32: Normativa obligatoria 32

33 ▲

Las capas o gabinetes usados como espacios alternativos cumplirán los requisitos de separación, tendrán una puerta provista con cerradura y se montarán en una ubicación fija.

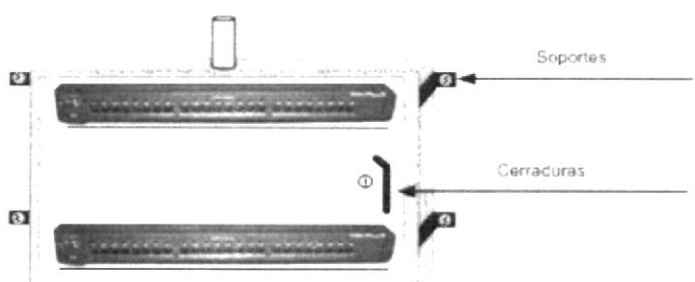


Figura 5-33: Normativa obligatoria 33

34 ▲

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

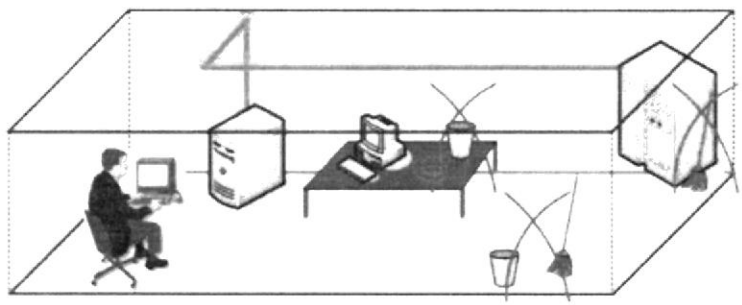


Figura 5-34: Normativa obligatoria 34

35 ▲

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

Figura 5-35: Normativa obligatoria 35

36 ▲

La instalación de gabinetes y racks deberán proporcionar las separaciones de instalada establecida en los reglamentos y normas a aplicar.

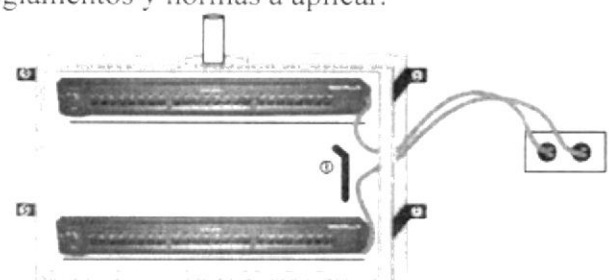


Figura 5-36: Normativa obligatoria 36

37 ▲

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

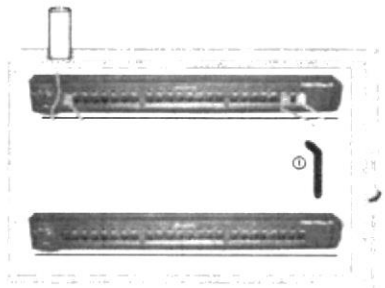


Figura 5-37: Normativa obligatoria 37

38 ▲

Los cables enrutados verticalmente, como en el caso de los cables de backbone u horizontales enrutados entre piso, se soportarán con abrazaderas u otros mecanismos. Se requiere un mínimo de 2 soportes por piso.

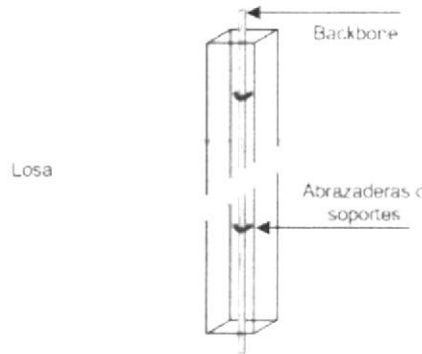


Figura 5-38: Normativa obligatoria 38

39 ▲

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

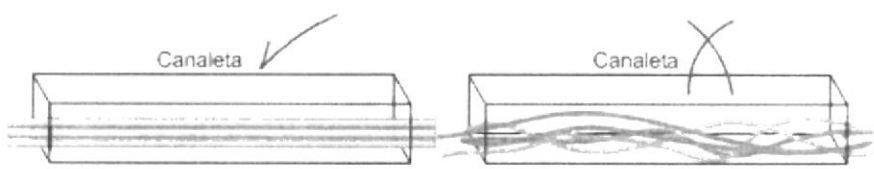


Figura 5-39: Normativa obligatoria 39

40 ▲

Las canalizaciones tipo bandeja o canal no excederán una capacidad máxima de 50% de llenado y una altura máxima interior de 6 pulgadas.

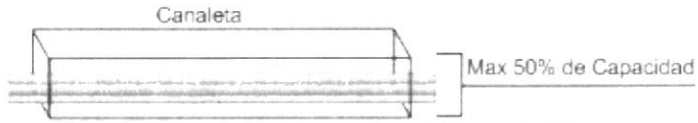


Figura 5-40: Normativa obligatoria 40

41 ▲

Para canalizaciones en espacio de techos falsos, los sistemas de soporte de cables se diseñarán e instalarán con un mínimo de 3 pulgadas por encima de la rejilla del techo soportado.

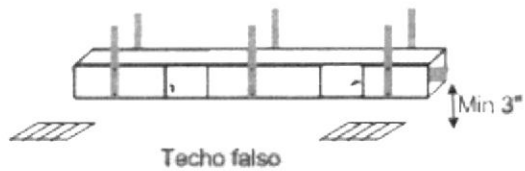


Figura 5-41: Normativa obligatoria 41

42 ▲

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

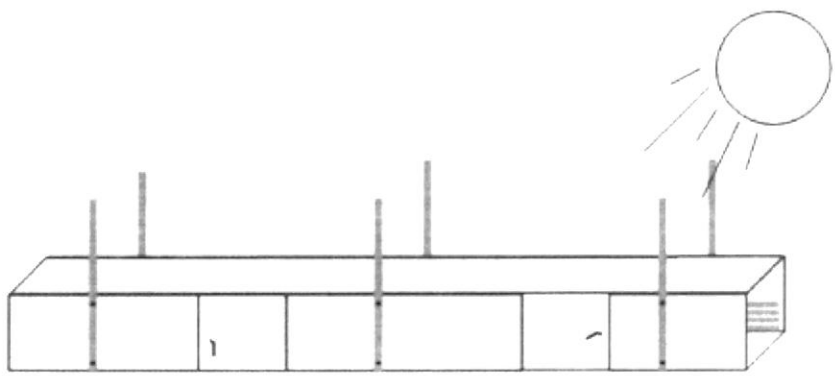


Figura 5-42: Normativa obligatoria 42

43 ▲

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

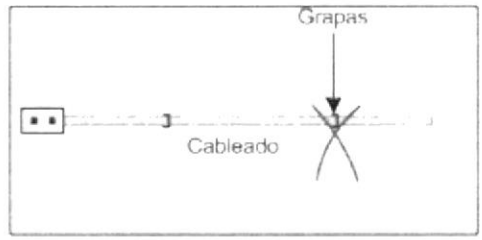


Figura 5-43: Normativa obligatoria 43

44 ▲

El radio mínimo de curvatura en condiciones de no tensión, cuando el cable es sólo colocado no halado será de:
4 veces el diámetro externo del cable para UTP.
1 pulgada para SCTP o SFTP de diámetro menor o igual a 6 milímetros.
2 pulgadas para SCTP o SFTP de diámetro mayor a 6 milímetros (0,25 pulgadas).

Figura 5-44: Normativa obligatoria 44

45 ▲

El radio mínimo de curvatura para cable horizontal de 2 y 4 fibras 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 será de 225N "Newton" (50 libras fuerza).

Figura 5-45: Normativa obligatoria 45

46 ▲

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

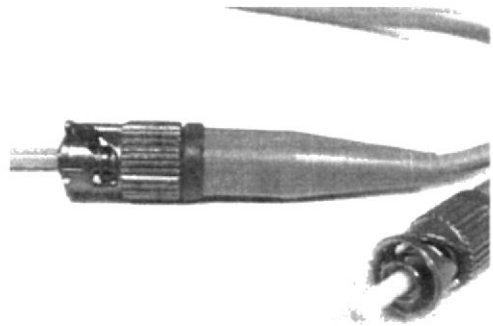


Figura 5-46: Normativa obligatoria 46

47 ▲

El radio de curvatura para cable backbone de fibra óptica externa no será menor a 10 veces el diámetro externo del cable bajo condiciones de no tensión, y no menor a 20 veces bajo condiciones de tensión, en donde la tensión de halada permitida usualmente es menor a 2.670N (600 libras fuerza).

Figura 5-47: Normativa obligatoria 47

48 ▲

El cable que corre entre el cuarto de telecomunicaciones y salida de telecomunicaciones, no estará expuesto en el área de trabajo ni en otros espacios con acceso público.

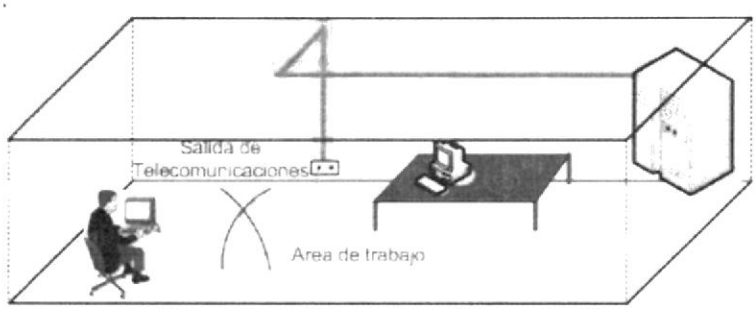


Figura 5-48: Normativa obligatoria 48

49 ▲

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

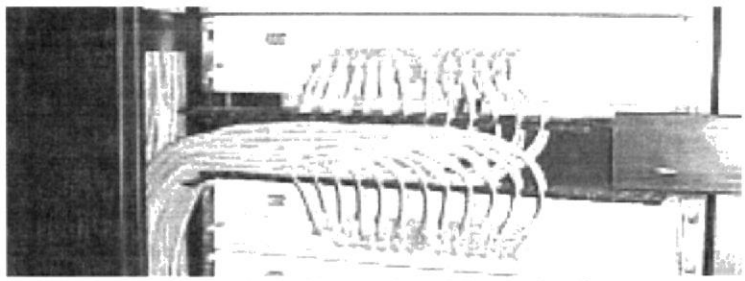


Figura 5-49: Normativa obligatoria 49

50 ▲

Con el fin de reducir el desentrenzado de los pares de cables, el instalador debe pelar sólo aquella cantidad de forro que se requiera para terminar en el hardware de conexión para par trenzado balanceado.

Figura 5-50: Normativa obligatoria 50

51 ▲

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

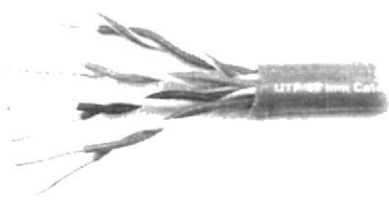


Figura 5-51: Normativa obligatoria 51

52 ▲

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

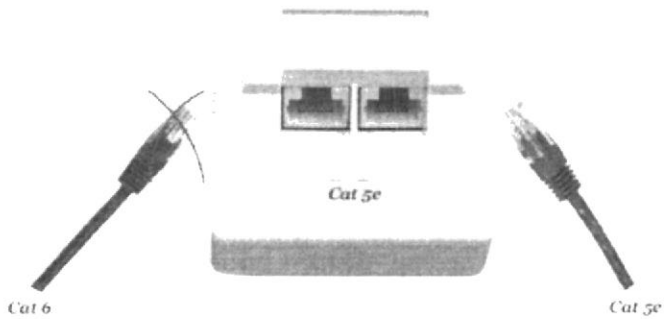


Figura 5-52: Normativa obligatoria 52

53 ▲

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

Figura 5-53: Normativa obligatoria 53

54 ▲

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.

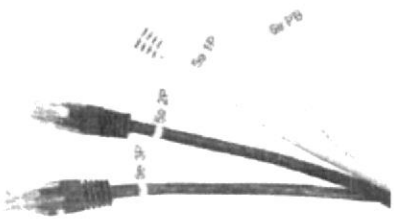


Figura 5-54: Normativa obligatoria 54

55 ▲

El rotulado deberá ser legible y permanecer firmemente unido al elemento durante todo el período de garantía.

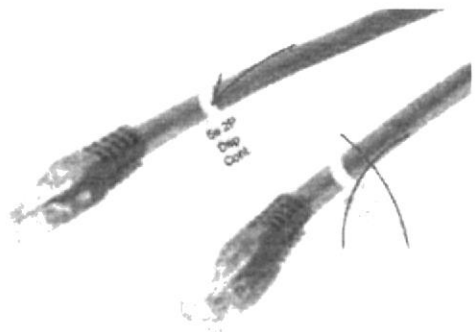


Figura 5-55: Normativa obligatoria 55

56 ▲

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

Descripción	Identificador
Cable N° 9 de fibra óptica multimodo	FOM009
Cable N° 5 de UTP categoría 5e	C5005

Tabla 5-1: Identificación de cables

Figura 5-56: Normativa obligatoria 56

57 ▲

Los cables de los subsistemas horizontales y backbone deberán rotularse en cada extremo. El cable con su etiqueta se marcará con su identificador y colocado dentro de los 30 centímetros del extremo del cable, esta marca deberá permanecer en el cable después de terminar la instalación.

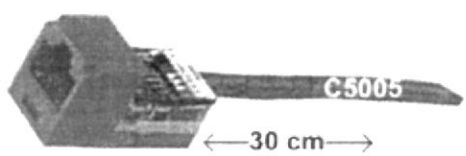


Figura 5-57: Normativa obligatoria 57

5.2 NORMATIVAS DE RECOMENDACIÓN

1 △

Se pueden emplear interconexiones para conexiones entre cableado horizontal y equipos con puertos individuales

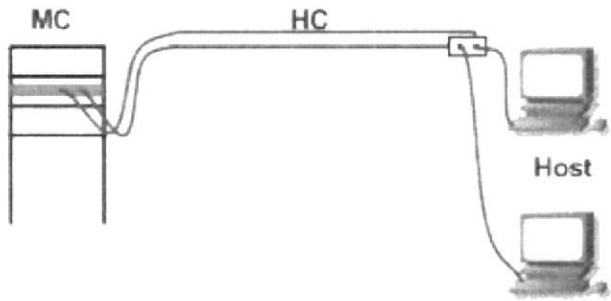


Figura 5-58: Normativa recomendada 1

2 △

Con el fin de proveer una infraestructura capaz de acomodar un ambiente de oficina dinámicos se recomienda enfáticamente un mínimo de un cuarto de telecomunicaciones por cada piso.

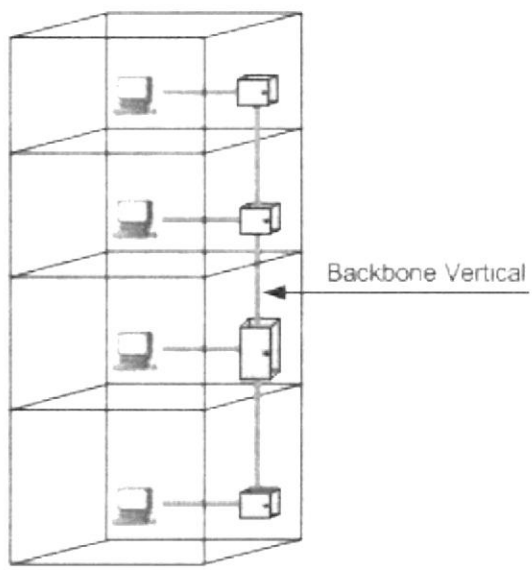


Figura 5-59: Normativa recomendada 2

3 △

El área que puede atenderse efectivamente por un cuarto de telecomunicaciones abarca un radio máximo de 60 metros.

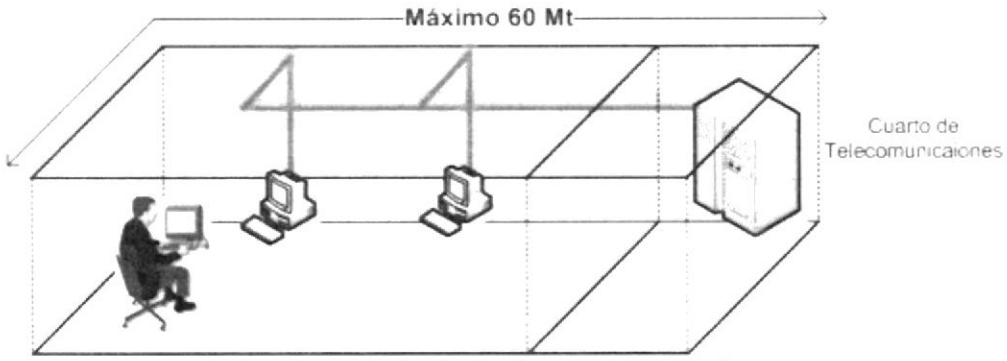


Figura 5-60: Normativa recomendada 3

4 △

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

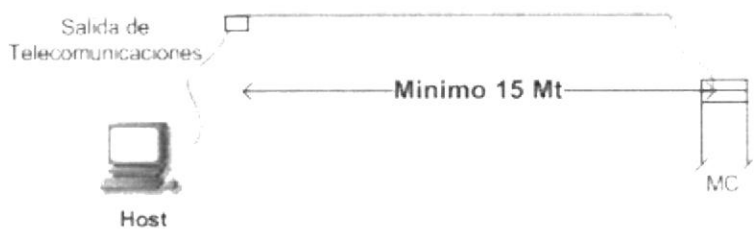


Figura 5-61: Normativa recomendada 4

5 △

Se recomienda un mínimo de 2 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.

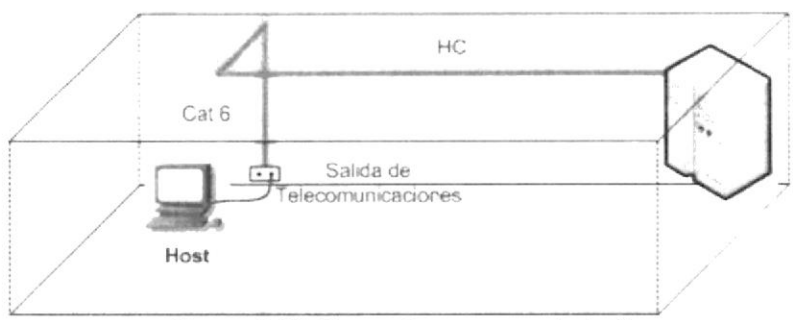


Figura 5-62: Normativa recomendada 5

6 △

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

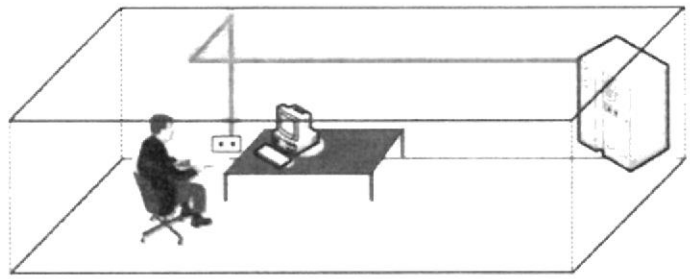


Figura 5-63: Normativa recomendada 6

7 △

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

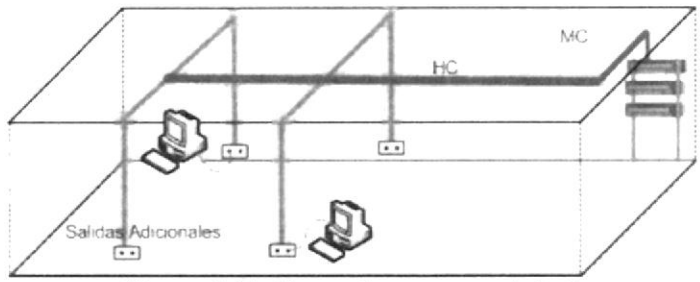


Figura 5-64: Normativa recomendada 7

8 △

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

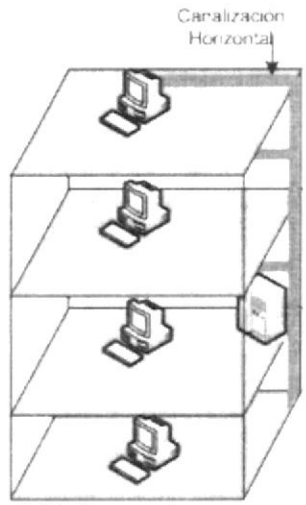


Figura 5-65: Normativa recomendada 8

9 △

Ningún segmento de canal contendrá más de 2 curvas de 90 grados entre puntos de acceso.

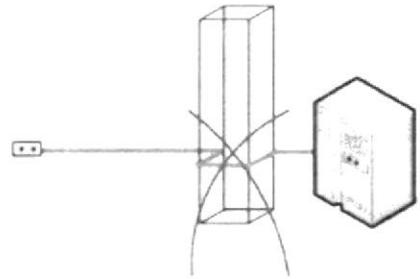


Figura 5-66: Normativa recomendada 9

10 △

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

Aplicación	Nº de hilos de fibra
Voz	2
Video	2
Lan	2
Crecimiento	6
Total	**12**

Tabla 5-2: Asignación de hilos de fibra óptica

11 △

Para cables de backbone se recomienda un mínimo de 3 metros de reserva de cable en cada extremo.

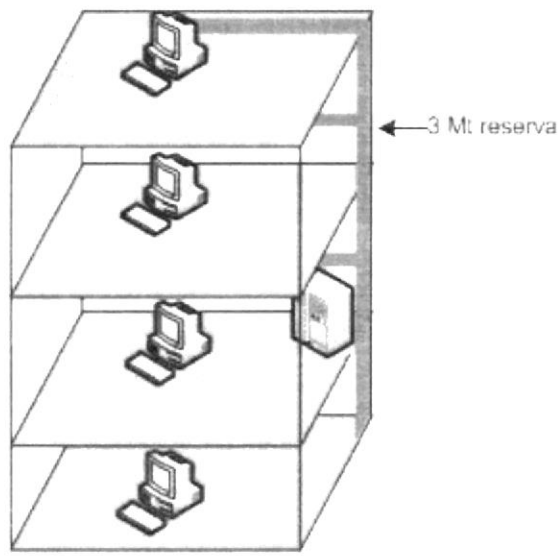


Figura 5-67: Normativa recomendada 11

12 △

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

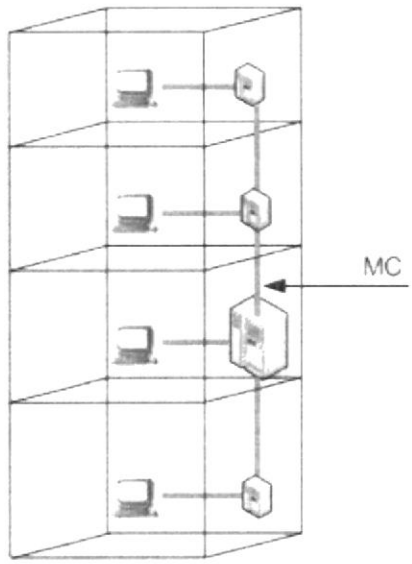


Figura 5-68: Normativa recomendada 12

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.

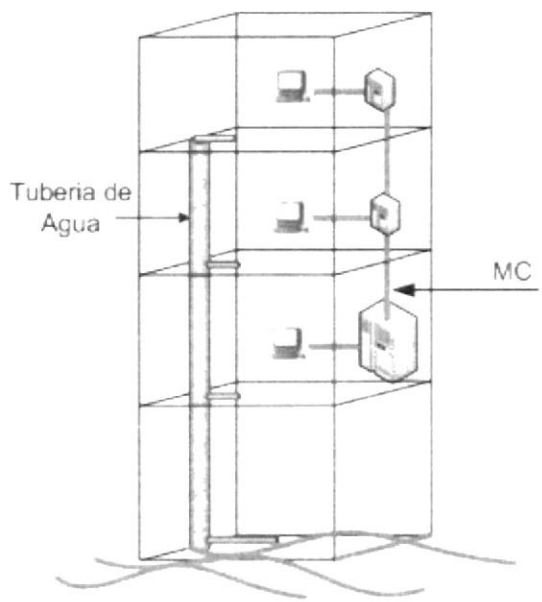


Figura 5-69: Normativa recomendada 13

CAPÍTULO 6

LINUX FEDORA CORE 3

6 LINUX FEDORA CORE 3

6.1 INTRODUCCIÓN

Linux a simple vista es 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 y Pentium II, así como los clones AMD y Cyrix. También soporta máquinas basadas en SPARC, DEC Alpha, PowerPC/PowerMac, y Mac/Amiga Motorola 680x0.

6.2 HISTORIA

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.
El 5 de octubre de 1991, Linus anunció la primera versión "Oficial" de Linux, -versión 0.02. 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.

6.3 CARACTERÍSTICAS PRINCIPALES

- Multitarea, utiliza la llamada multitarea preventiva, la cual asegura que todos los programas que se están utilizando en un momento dado serán ejecutados, siendo el sistema operativo el encargado de ceder tiempo de microprocesador a cada programa.
- Multiusuario, muchos usuarios usando la misma maquina al mismo tiempo.
- Multiplataforma, Linux funciona actualmente en las siguientes plataformas:
  - ✓ Acorn: Archimedes, A5000 y las series RiscPC: (ARM, StrongARM, Intel XScale etc.)
  - ✓ Archimedes, A5000 y las series RiscPC: (ARM, StrongARM, Intel XScale etc.)
  - ✓ AMD64: Procesadores de AMD con tecnología de 64-bits (conocidos inicialmente como x86-64)
  - ✓ IA-64: PC's con tecnología de 64-bits Intel Itanium
  - ✓ Series: IBM zSeries (z800, z890, z900, z990, z9) y virtualizado bajo el sistema operativo z/VM.
  - ✓ Intel: 80386 y superiores: IBM PC's y compatibles: 80386, 80486, la serie Pentium completa; AMD Athlon, Duron, Thunderbird; las series

Cyrix. El soporte para microprocesadores Intel 8086, 8088, 80186, 80188 e 80286 está siendo desarrollado (véase el proyecto ELKS)

- Multiprocesador: Soporte para sistemas con mas de un procesador esta disponible para Intel y SPARC.
- Protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.
- Carga de ejecutables por demanda: Linux sólo lee del disco aquellas partes de un programa que están siendo usadas actualmente.
- Memoria virtual usando paginación (sin intercambio de procesos completos) a disco: A una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio.
- Librerías compartidas de carga dinámica (DLL's) y librerías estáticas.
- Compatible con POSIX, System V y BSD a nivel fuente.
- Emulación de iBCS2, casi completamente compatible con SCO, SVR3 y SVR4 a nivel binario.
- Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente.
- Emulación de 387 en el núcleo, de tal forma que los programas no tengan que hacer su propia emulación matemática. Cualquier máquina que ejecute Linux parecerá dotada de coprocesador matemático.
- Soporte para muchos teclados nacionales o adaptados y es bastante fácil añadir nuevos dinámicamente.
- Consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video). Se crean dinámicamente y puedes tener hasta 64.
- Soporte para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, y tiene un avanzado sistema de archivos propio con una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.
- Acceso transparente a particiones MS-DOS (o a particiones OS/2 FAT) mediante un sistema de archivos especial: no es necesario ningún comando especial para usar la partición MS-DOS, esta parece un sistema de archivos normal de Unix (excepto por algunas restricciones en los nombres de archivo, permisos, y esas cosas). Las particiones comprimidas de MS-DOS 6 no son accesibles en este momento, y no se espera que lo sean en el futuro. El soporte para VFAT (WNT, Windows 95) ha sido añadido al núcleo de desarrollo y estará en la próxima versión estable.
- Un sistema de archivos especial llamado UMSDOS que permite que Linux sea instalado en un sistema de archivos DOS.
- Sistema de archivos de CD-ROM que lee todos los formatos estándar de CD-ROM.
- TCP/IP, incluyendo ftp, telnet, NFS, etc.
- Software cliente y servidor Netware.
- Lan Manager / Windows Native (SMB), software cliente y servidor.

6.4 EL KERNEL

Es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema. Como hay muchos programas y el acceso al hardware es limitado, el núcleo también se encarga de decidir qué programa podrá hacer uso de un dispositivo de hardware y durante cuanto tiempo, lo que se conoce como multiplexado. Acceder al hardware directamente puede ser realmente complejo, por lo que los núcleos suelen implementar una serie de abstracciones del hardware. Esto permite esconder la complejidad, y proporciona una interfaz limpia y uniforme al hardware subyacente, lo que facilita su uso para el programador.
Hay cuatro tipos de Núcleo o Kernel:

- Los núcleos monolíticos facilitan abstracciones del hardware subyacente realmente potentes y variadas.
- Los micronúcleos (en inglés microkernel) proporcionan un pequeño conjunto de abstracciones simples del hardware, y usan las aplicaciones llamadas servidores para ofrecer mayor funcionalidad.
- Los híbridos (micronúcleos modificados) son muy parecidos a los micronúcleos puros, excepto porque incluyen código adicional en el espacio de núcleo para que se ejecute más rápidamente.
- Los exonúcleos no facilitan ninguna abstracción, pero permiten el uso de bibliotecas que proporcionan mayor funcionalidad gracias al acceso directo o casi directo al hardware.

6.5 VENTAJAS DE LINUX FEDORA

Las ventajas e inconvenientes que podemos encontrar en Linux frente a otros sistemas operativos dependerán considerablemente de la distribución que usemos, ya que cada distribución suele incorporar utilidades propias que afectan tanto a la instalación como al posterior funcionamiento y uso del sistema. Debido a esto sólo mencionaremos aquellas que, por lo general, son las más frecuentes y se encuentran en la mayoría de distribuciones.

- Precio: Debido a que su licencia es GNU, podemos descargarlo gratuitamente desde Internet o comprarlo a un precio muy asequible por la mayoría de usuarios.
- Requerimientos: Actualmente los sistemas operativos necesitan mucha máquina y recursos del sistema para ejecutarse con fluidez, Linux, al poder funcionar exclusivamente en modo texto sin la necesidad de cargar un entorno gráfico puede ejecutarse en cualquier máquina a partir de un i386.
- Estabilidad: Al tener su núcleo basado en Unix, hereda esa estabilidad que siempre ha caracterizado a los sistemas Unix.
- Seguridad: A nivel de servidor podemos encontrar que la seguridad de Linux frente a otros servidores del mercado es mucho mayor.
- Compatibilidad: Reconoce la mayoría de otros sistemas operativos en una red.
- Multitarea real: Es posible ejecutar varias aplicaciones y procesos simultáneamente.

- Velocidad: Debido a la multitarea real que incorpora, y que no es necesario cargar su entorno gráfico para ejecutar servicios o aplicaciones, hacen que su velocidad sea muy superior a los actuales sistemas operativos.
- Código Fuente: El paquete incluye el código fuente, por lo que es posible modificarlo y adaptarlo a nuestras necesidades libremente.
- Entorno de Programación: Es ideal para la programación, ya que se puede programar para otros sistemas operativos.
- Crecimiento: Su sistema de crecimiento, gracias a la licencia GNU, el código abierto, y la gran comunidad de miles de programadores, es de los más rápidos que existen en la actualidad.

6.6 DESVENTAJAS DE LINUX FEDORA

- Soporte: Algunos Linux no cuentan con empresas que lo respalden, por lo que no existe un soporte sólido como el de otros sistemas operativos.
- Simplicidad: No es tan fácil de usar como otros sistemas operativos, aunque actualmente algunas distribuciones están mejorando su facilidad de uso, gracias al entorno de ventanas, sus escritorios y las aplicaciones diseñadas específicamente para él, cada día resulta más sencillo su integración y uso.
- Software: No todas las aplicaciones Windows se pueden ejecutar bajo Linux, y a veces es difícil encontrar una aplicación determinada, y lo más importante, es que no todas las aplicaciones están en castellano.
- Hardware: Actualmente Linux soporta un máximo de 16 procesadores simultáneamente, contra los 64 procesadores de otros sistemas operativos.

6.7 ESTRUCTURA DEL SISTEMA DE ARCHIVOS

El sistema de archivo de Linux sigue todas las convenciones de Unix, lo cual significa que tiene una estructura determinada, compatible y homogénea con el resto de los sistemas Unix. Todo el sistema de archivos de Unix tiene un origen único la raíz o root representada por /. Bajo este directorio se encuentran todos los ficheros a los que puede acceder el sistema operativo. Estos ficheros se organizan en distintos directorios cuya misión y nombre son estándar para todos los sistema Unix.

- /Raíz del sistema de archivos.
- /dev Contiene ficheros del sistema representando los dispositivos que estén físicamente instalados en el ordenador.
- /etc Este directorio esta reservado para los ficheros de configuración del sistema. En este directorio no debe aparecer ningún fichero binario (programas). Bajo este deben aparecer otros dos subdirectorios:
- /etc/X11 Ficheros de configuración de X Window
- /etc/skel Ficheros de configuración básica que son copiados al directorio del usuario cuando se crea uno nuevo.
- /lib Contiene las librerías necesarias para que se ejecuten los programas que residen en /bin (no las librerías de los programas de los usuarios).
- /proc Contiene ficheros especiales que o bien reciben o envían información al kernel del sistema (Se recomienda no modificar el contenido de este directorio y sus ficheros).

- /sbin Contiene programas que son únicamente accesibles al superusuario o root.
- /usr Este es uno de los directorios más importantes del sistema puesto que contiene los programas de uso común para todos los usuarios. Su estructura suele ser similar a la siguiente:
- /usr/X11R6 Contiene los programas para ejecutar X Window.
- /usr/bin Programas de uso general, lo que incluye el compilador de C/C++.
- /usr/doc Documentación general del sistema.
- /usr/etc Ficheros de configuración generales. /usr/include Ficheros de cabecera de C/C++ (.h).
- /usr/info Ficheros de información de GNU. /usr/lib Librerías generales de los programas.
- /usr/man Manuales accesibles con el comando man
- /usr/sbin Programas de administración del sistema. /usr/src Código fuente de programas.
- /usr. Como por ejemplo las carpetas de los programas que se instalen en el sistema.
- /var. Este directorio contiene información temporal de los programas (lo cual no implica que se pueda borrar su contenido.

6.7.1 TIPOS DE ARCHIVOS

La base del sistema de archivos de Linux, es obviamente el archivo, que no es otra cosa que la estructura empleada por el sistema operativo para almacenar información en un dispositivo físico como un disco duro, un disquete, un CD-ROM o un DVD. Como es natural un archivo puede contener cualquier tipo de información, desde una imagen en formato PNG o JPEG a un texto o una página WEB en formato HTML, el sistema de archivos es la estructura que permite que Linux maneje los archivos que contiene.
Todos los archivos de Linux tienen un nombre, el cual debe cumplir unas ciertas reglas:

- Un nombre de archivo puede tener entre 1 y 255 caracteres.
- Se puede utilizar cualquier carácter excepto la barra inclinada / y no es recomendable emplear los caracteres con significado especial en Linux, que son los siguientes: = ^ ~ ' " ` * ; - ? [ ] ( ) ! & ~ < >. Para emplear ficheros con estos caracteres o espacios hay que introducir el nombre del fichero entre comillas.
- Se pueden utilizar números exclusivamente si así se desea. Las letras mayúsculas y minúsculas se consideran diferentes, y por lo tanto no es lo mismo carta.txt que Carta.txt ó carta.Txt

Linux sólo distingue tres tipos de archivos:

- Archivos o ficheros ordinarios, son los .txt, .htm (o .html), .png y .jpg (o .jpeg).
- Directorios (o carpetas), es un archivo especial que agrupa otros ficheros de una forma estructurada.
- Archivos especiales, son la base sobre la que se asienta Linux, puesto que representan los dispositivos conectados a un ordenador, como puede ser una impresora. De esta forma introducir información en ese archivo equivale a enviar información a la impresora. Para el usuario estos dispositivos tienen el mismo aspecto y uso que los archivos ordinarios.

6.7.2 ENLACES

Los enlaces son un tipo de archivo común cuyo objetivo es crear un nuevo nombre para un archivo determinado. Una vez creado el enlace simbólico éste permite acceder al fichero que enlaza de igual modo que si se hubiera copiado el contenido del mismo a otro fichero, con la ventaja de que este realmente no se ha copiado. Los enlaces simbólicos son especialmente útiles cuando se quiere que un grupo de personas trabajen sobre un mismo fichero, puesto que permiten compartir el fichero pero centralizan las modificaciones.
Como ejemplo se puede suponer la existencia de un fichero llamado balance.1999.txt, al que se crea un enlace simbólico balance.txt. Cualquier acceso a balance.txt es traducido por el sistema de forma que se accede al contenido de balance.1999.txt.

6.8 REQUERIMIENTOS DE HARDWARE MÍNIMOS

- Procesador Pentium II
- Memoria 64 Mb
- Espacio físico en disco duro 3Gb
- Unidad de CD-ROM
- Tarjeta de Red 10 Mbps
- Tarjeta de Video VGA

6.9 REQUERIMIENTOS DE HARDWARE ÓPTIMOS

- Procesador Pentium IV
- Memoria 512 Mb
- Espacio físico en disco duro 10 Gb
- Unidad de CD-ROM
- Tarjeta de Red 10/100 Mbps
- Tarjeta de Video SVGA

6.10 INSTALACIÓN DE LINUX-FEDORA

Fedora Core 3, incluye software necesario para instalar un sistema completo de servicios de red más comunes. Se puede seleccionar la opción de servidor durante la instalación o también escoger paquetes de programas individuales o instalarlos luego.

6.10.1 CONSIDERACIONES PREVIAS A LA INSTALACIÓN

Para instalar Linux Fedora se necesita de 5 discos de de instalación, si se desea todos los paquetes del sistema.
Si se instala Linux como servidor lo más común es que se necesite los 3 primeros CD's de instalación

6.10.2 CANCELAR INSTALACIÓN

Para cancelar el proceso de instalación en cualquier momento, antes de la pantalla de instalación de los paquetes, presione **Ctrl.-Alt-Del**.
Linux Fedora no realizará cambios antes de que comience a instalar los paquetes.

6.10.3 INICIANDO INSTALACIÓN

Para iniciar la instalación de Fedora Core3, inicie el computador desde el disco 1. También se puede instalar desde memorias USB, Discos duros o servidores Web, este manual especifica la instalación desde Discos.

6.10.4 CONFIGURANDO EL BIOS

El BIOS (Sistema básico de entrada y salida) debe soportar el inicio desde diferentes dispositivos. Si el computador cumple con los requisitos indicados anteriormente, no tendrá ningún inconveniente.
Para acceder al setup del BIOS realice lo siguiente:

- Encienda el computador
- Al arrancar el equipo presione constantemente la tecla **supr.**, de esta manera ingrese al setup. El presionar la tecla **supr.** puede variar dependiendo del fabricante de la mainboard pero entre las otras teclas que están son la **F2** o **F10.**
- Estando en el setup muévase con las teclas direccionales al menú donde dice Boot y seleccione la unidad de CD-ROM como primer dispositivo de arranque. En otros mainboards la opción es **Advanced Bios Features**. Para ir moviendo las opciones utilice las teclas de + o **-.**

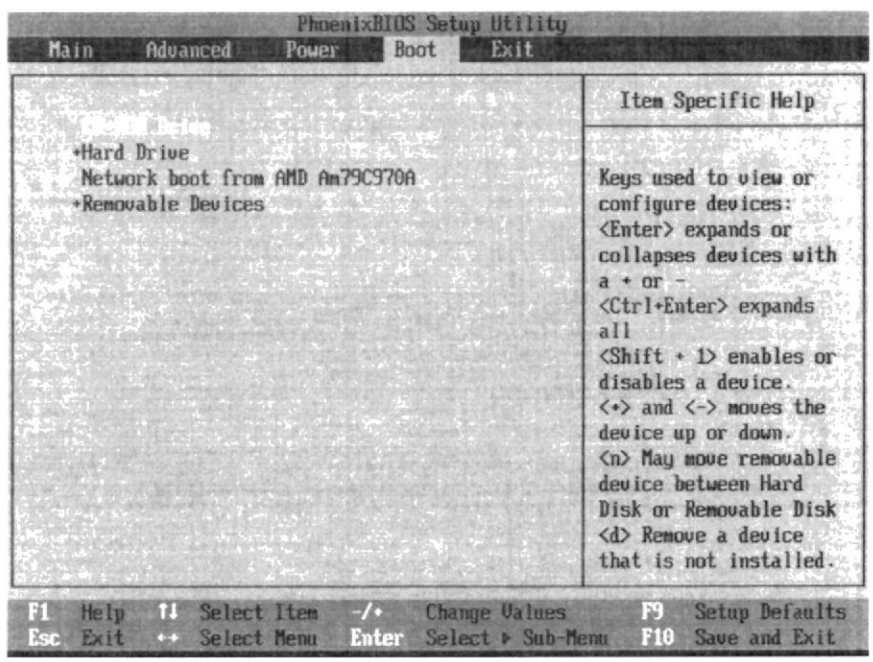


Figura 6-1: Configuración de Buteo

- Salga con la tecla **esc** del menú y presione la tecla F10 para grabar los cambios y salir.

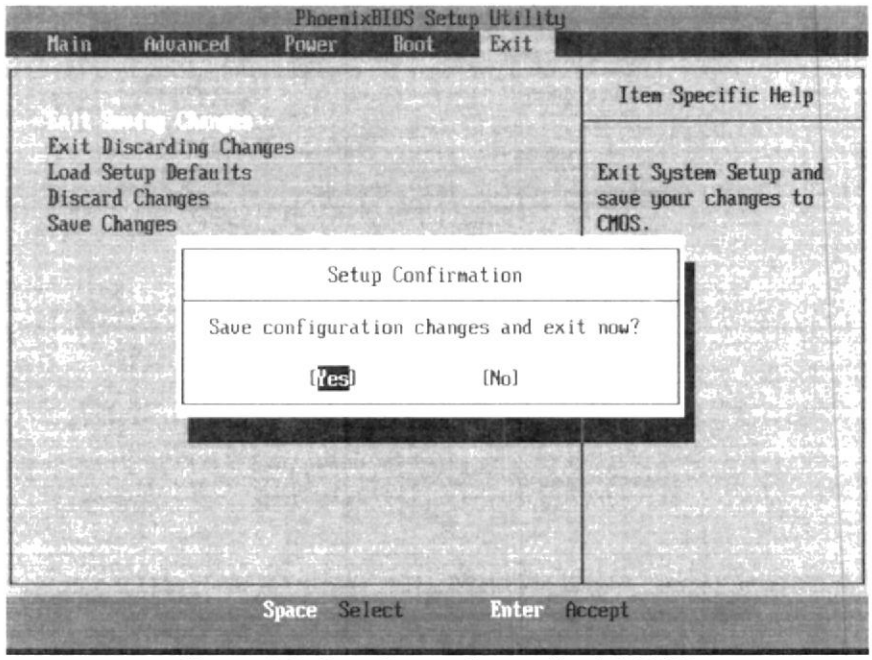


Figura 6-2: Guardar configuración del BIOS

- Ingrese el CD 1 en la unidad de CD-ROM,
- Acepte los cambios y presione la tecla ENTER en **Yes**

6.10.5 ARRANQUE DE INSTALACIÓN

Se presenta una pantalla de bienvenida a modo texto, a continuación presione la tecla **ENTER** para iniciar la instalación.

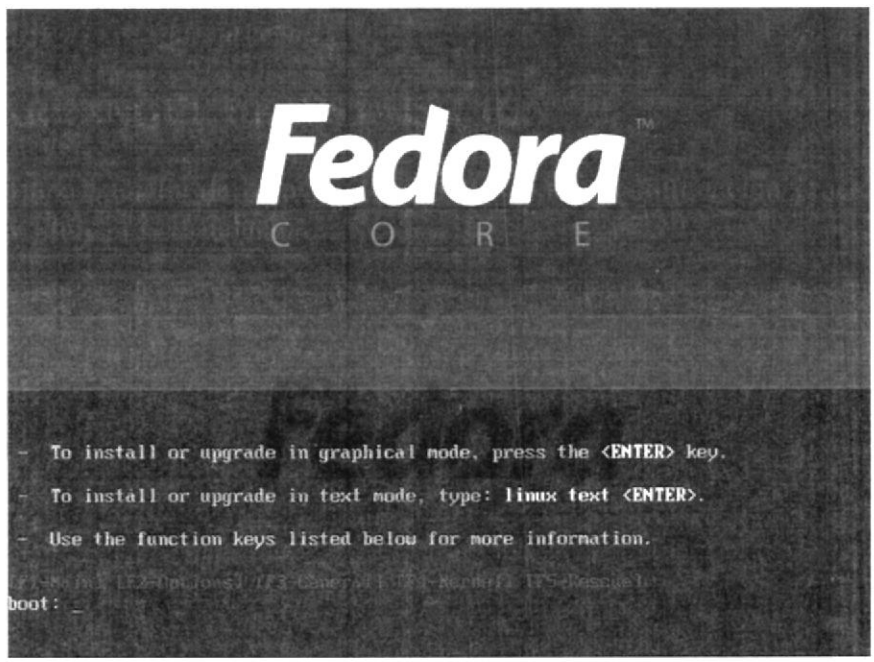


Figura 6-3: Buteo de Linux Fedora

Luego aparece en pantalla el menú para verificar la integridad del disco a partir del cual se realizará la instalación, seleccione «OK» (opcional) y pulse la tecla **ENTER**, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione «**Skip**» y pulse la tecla **ENTER.**

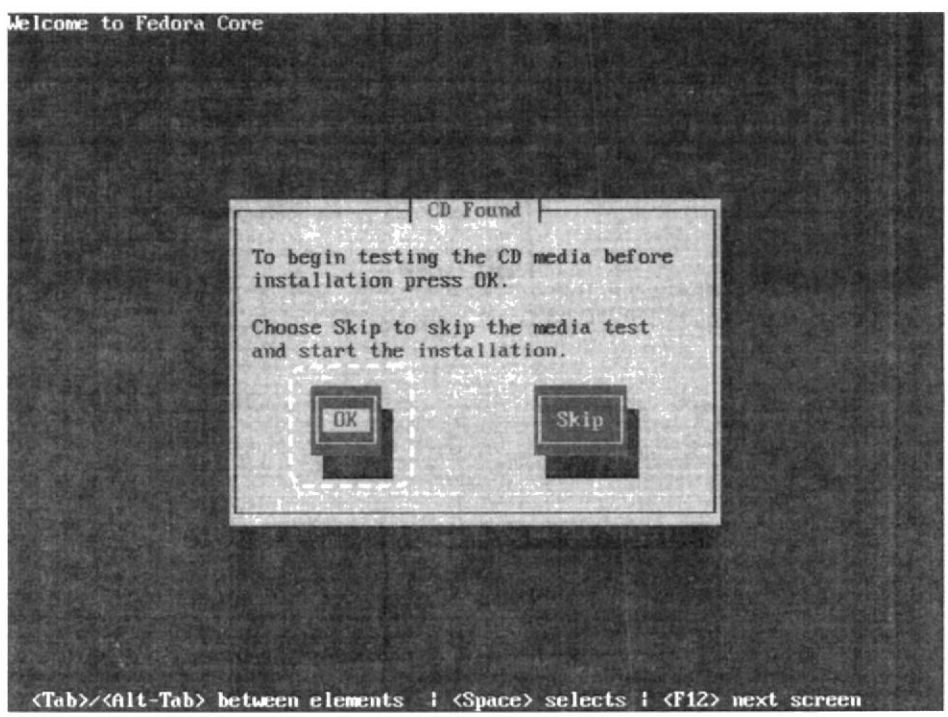


Figura 6-4: Test del CD

Haga clic sobre el botón «**Next**» en cuanto aparezca la pantalla de bienvenida de **Fedora Core**, que aparecerá en modo gráfico.

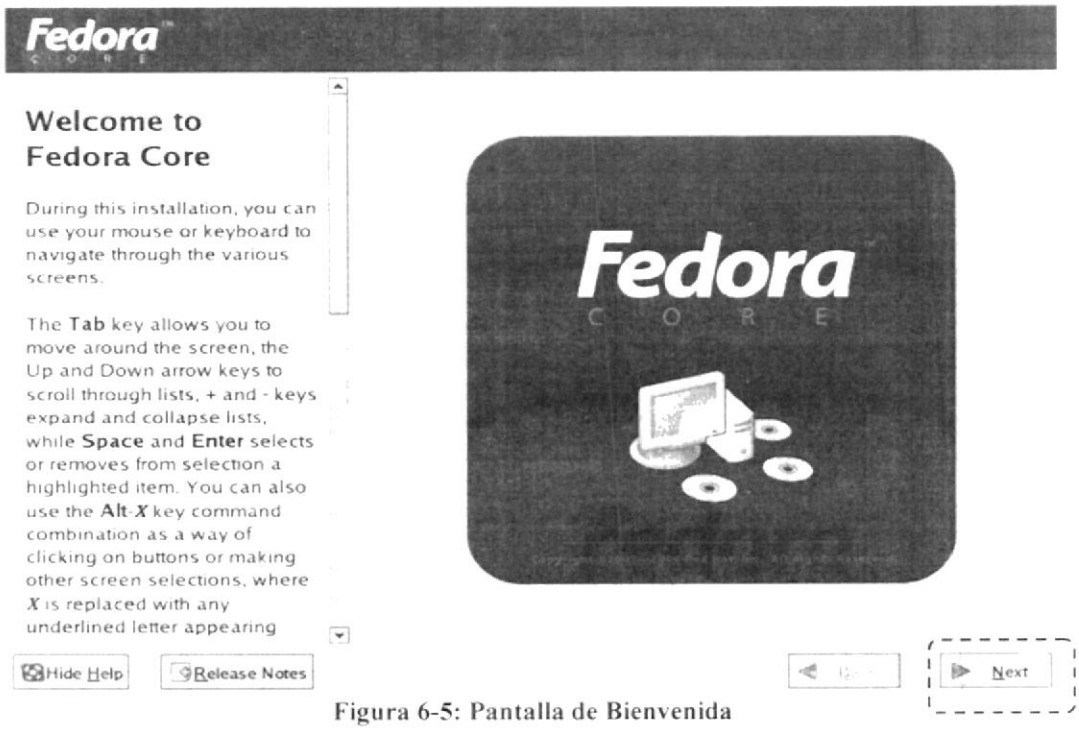


Figura 6-5: Pantalla de Bienvenida

En esta pantalla se observará un menú que presenta la selección de idiomas, para esta instalación utilice la opción «**Spanish**» como idioma que será utilizado. Luego de clic en **NEXT.**

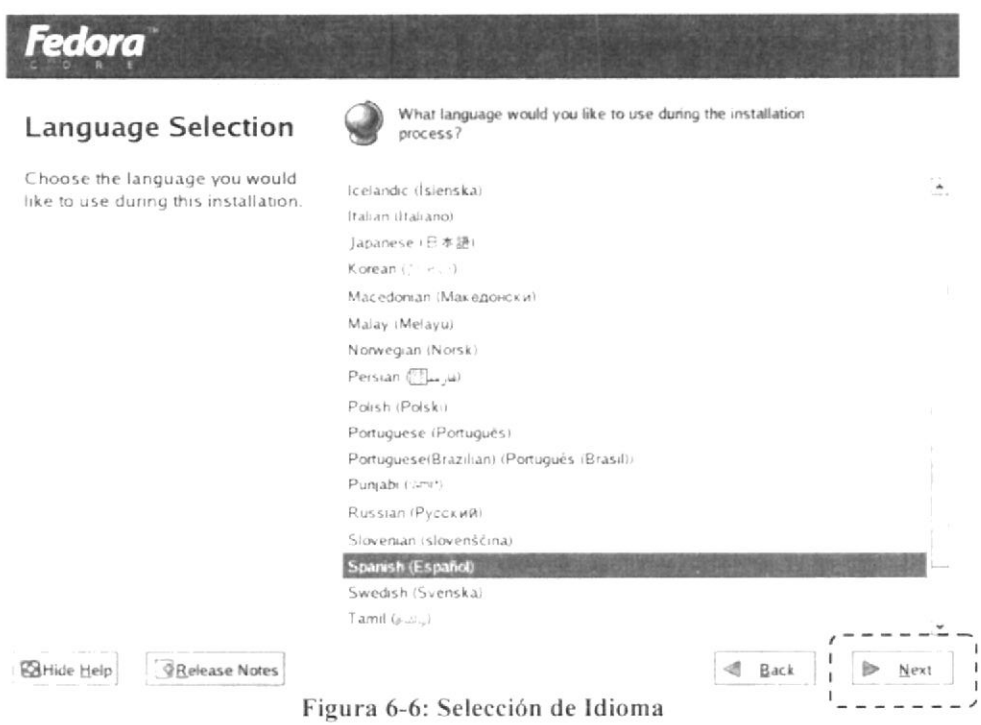


Figura 6-6: Selección de Idioma

En esta pantalla se observará la selección del mapa de teclado que corresponda al dispositivo utilizado. El mapa **«Spanish»** corresponde a la disposición del teclado Español España. Al terminar, haga clic sobre el botón **«Siguiente».**

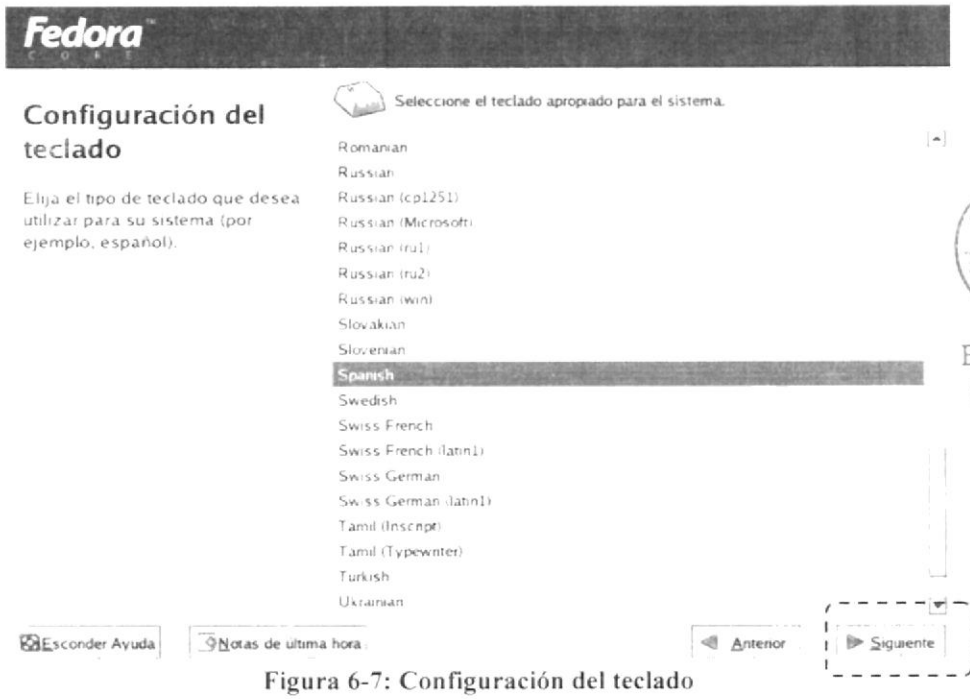


Figura 6-7: Configuración del teclado

En este menú usted procederá a seleccionar el tipo de instalación que va a realizar Elija el tipo de instalación «**Personalizada**» para realizar esta con un mayor control de las opciones disponibles. Al terminar, haga clic sobre el botón «**Siguiente**».

Figura 6-8: Tipo de instalación

En esta pantalla se procede a configurar el particionamiento del disco duro, dependiendo del tipo de instalación. Este menú presenta dos opciones: *Particionamiento Automático y Particionamiento Manual con Disk Fruid.*

Se sugiere al usuario utilizar la opción Disk Druid ya que permite configurar las particiones en un entorno interactivo, como son el sistema de archivo, puntos de montaje, tamaño de las particiones. Al terminar, haga clic sobre el botón «Siguiente» para ingresar a la herramienta para particiones del disco duro.

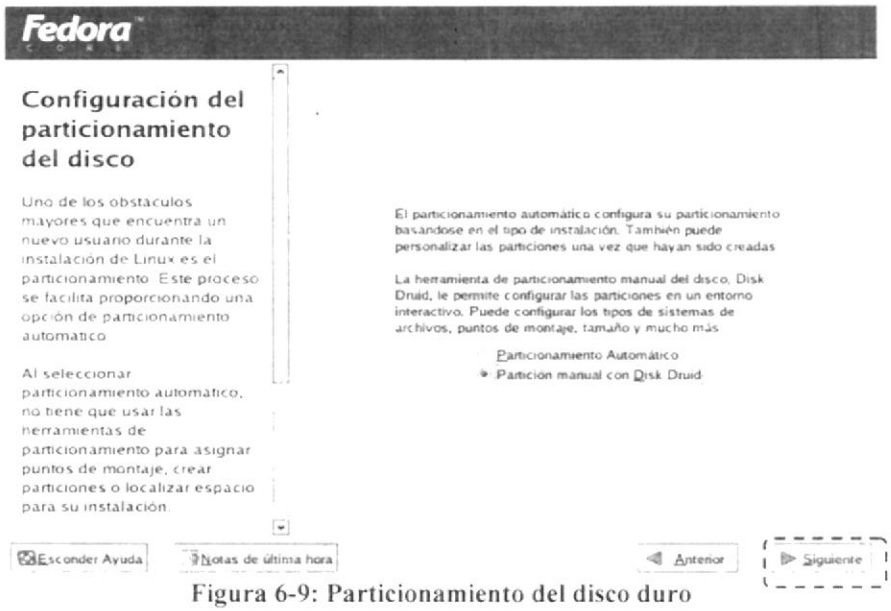


Figura 6-9: Particionamiento del disco duro

La herramienta de particiones mostrará el espacio disponible. Haga clic en el botón nuevo.

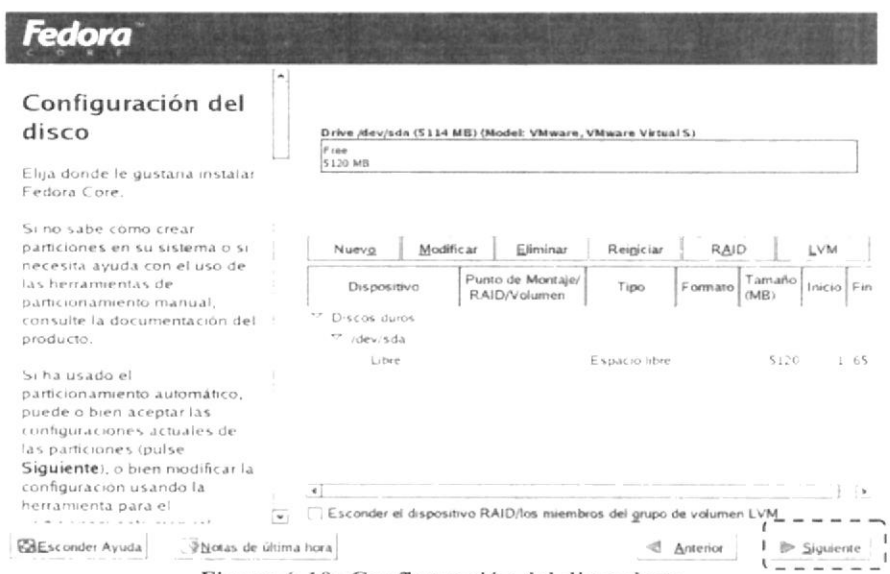


Figura 6-10: Configuración del disco duro

Campos de la partición

- Dispositivo: Este campo muestra el nombre del dispositivo de la partición.
- Punto de montaje: Un punto de montaje es el lugar en la jerarquía de directorios a partir del cual un volumen existe; el volumen se "monta" en este lugar.
- Tipo: Este campo muestra el tipo de partición (por ejemplo, ext2, ext3, o vfat).
- Formato: Este campo muestra si la partición que se está creando se formateará.
- Tamaño: Este campo muestra el tamaño de la partición (en MB).
- Comienzo: Este campo muestra el cilindro en su disco duro donde la partición comienza.
- Final: Este campo muestra el cilindro en su disco duro donde la partición termina.

Cree la partición /boot y asigne 100MB de tamaño. El /boot es donde se almacena el arranque del sistema de Linux.

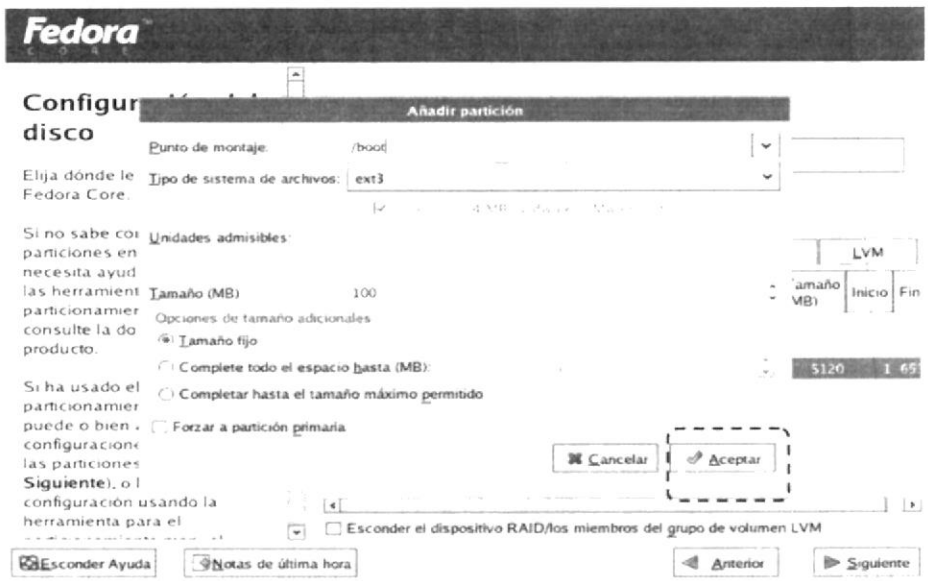


Figura 6-11: Configuración de la partición Boot

La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de **«Tipo de sistema de archivos»** la opción **«swap».**
Esta partición es la que servirá de memoria virtual en Linux por lo cual el tamaño que le dará en MB será el doble de tamaño que tenga instalado en memoria RAM en el computador. En este caso se tiene 256MB de memoria RAM física por lo tanto asigne un tamaño de 512MB.

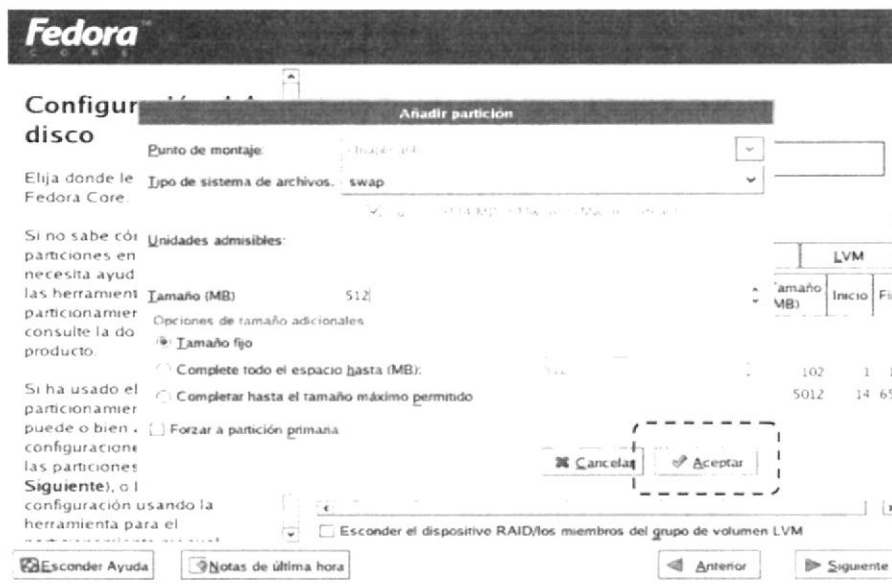


Figura 6-12: Configuración del particionamiento Swap

Cree la partición / la cual será el tamaño de almacenamiento, esto va a ser dependiendo de la cantidad de paquetes que se van a instalar.
Dependiendo de las necesidades y la cantidad de paquetes que se vaya a instalar determine el tamaño, para una instalación mínima se sugiere dar un tamaño de 4000MB

que es equivalente a 4GB por lo tanto necesita un disco duro no más pequeño que ese tamaño.

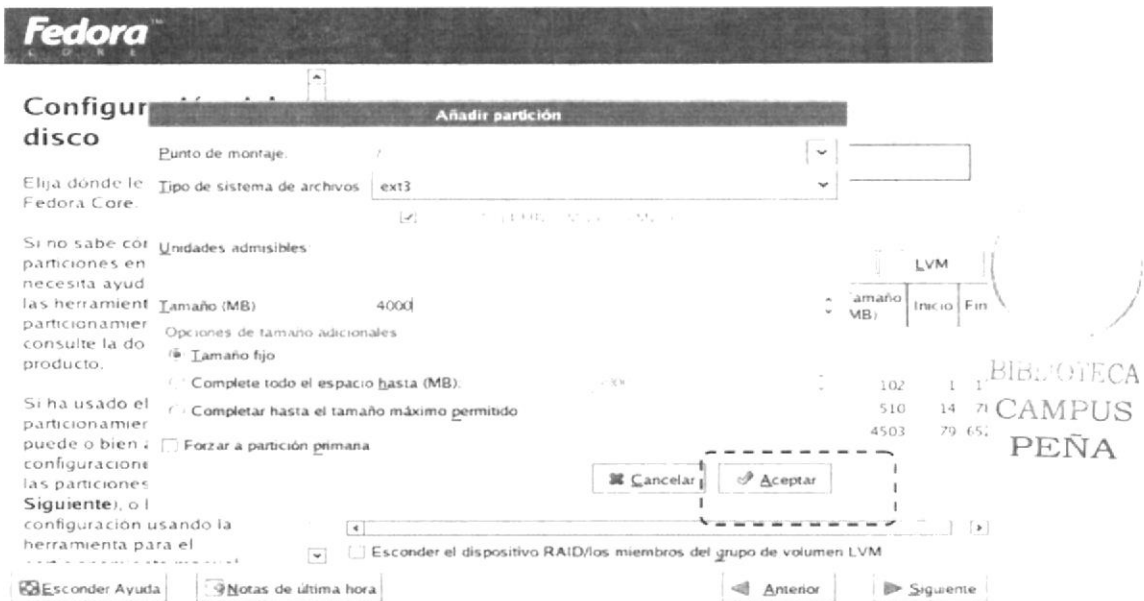


Figura 6-13: Configuración de la partición Raíz

El gestor de arranque es el primer software que se ejecuta cuando se arranca el computador. Es responsable de la carga y de la transferencia del control al software del sistema operativo del kernel. El kernel, por otro lado, inicializa el resto del sistema operativo.

El programa de instalación le ofrece dos gestores de arranque, GRUB y LILO.

GRUB (Grand Unified Bootloader), que se instala por defecto, es un gestor de arranque muy potente ya que puede cargar una gran variedad de sistemas operativos libres así como sistemas operativos de propietarios.

Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de corrida 1, o cualquiera otro, haga clic en la casilla «Usar la contraseña del gestor de arranque».

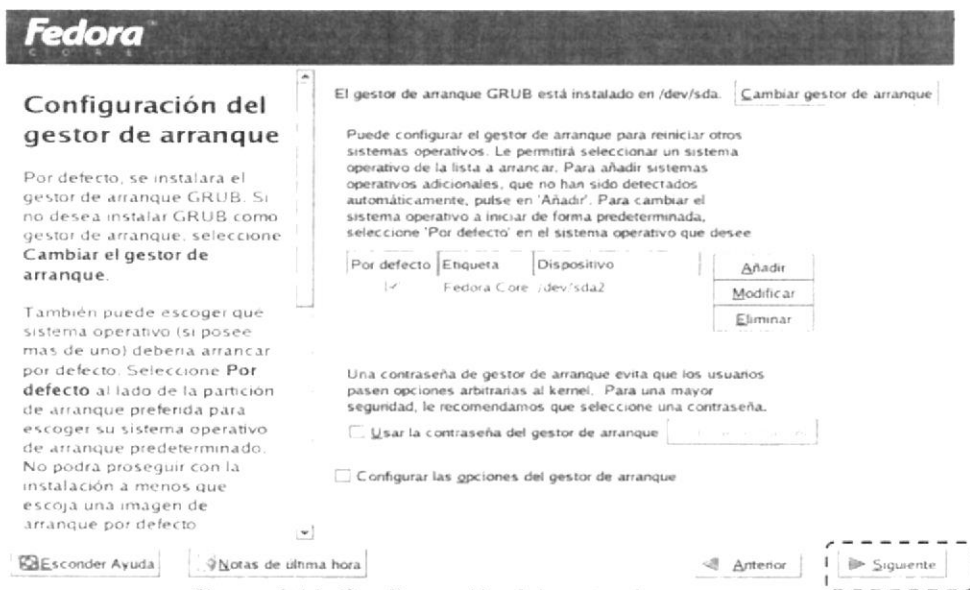


Figura 6-14: Configuración del gestor de arranque

En la ventana emergente para modificar la interfaz eth0, desactive la casilla **Configurar usando DHCP** para poder configurar y especificar la dirección IP y máscara de subred que utilizará en adelante el sistema y de clic en **«Siguiente».**

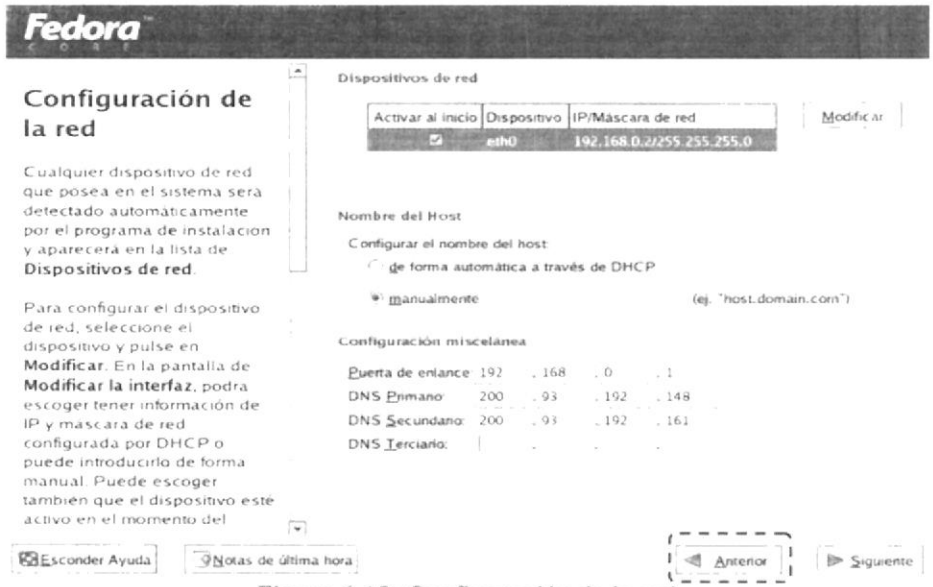


Figura 6-15: Configuración de la red

Configuración de Cortafuegos

La configuración "ningún cortafuegos" proporciona un acceso completo al sistema y no realiza ningún tipo de verificación de seguridad. La comprobación de seguridad es la desactivación del acceso a determinados servicios. Tan sólo se recomienda esta opción si está usando una red certificada y segura (no Internet).

No configure cortafuegos en este momento. La herramienta utilizada para tal fin, system-config-securitylevel, crea un cortafuego simple y con muchas limitaciones. Se recomienda considerar otras alternativas como Firestarter o Shorewall. Al terminar, haga clic sobre el botón «**Siguiente**».

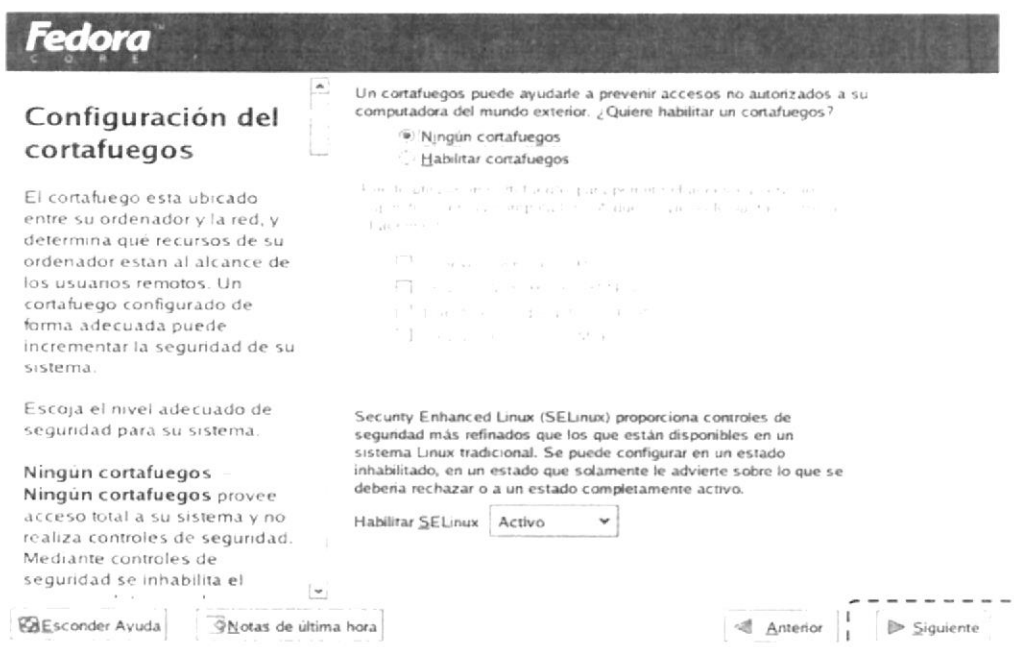


Figura 6-16: Configuración del cortafuego

Seleccione el idioma predeterminado a utilizar en el sistema. Al terminar, haga clic sobre el botón «**Siguiente**».

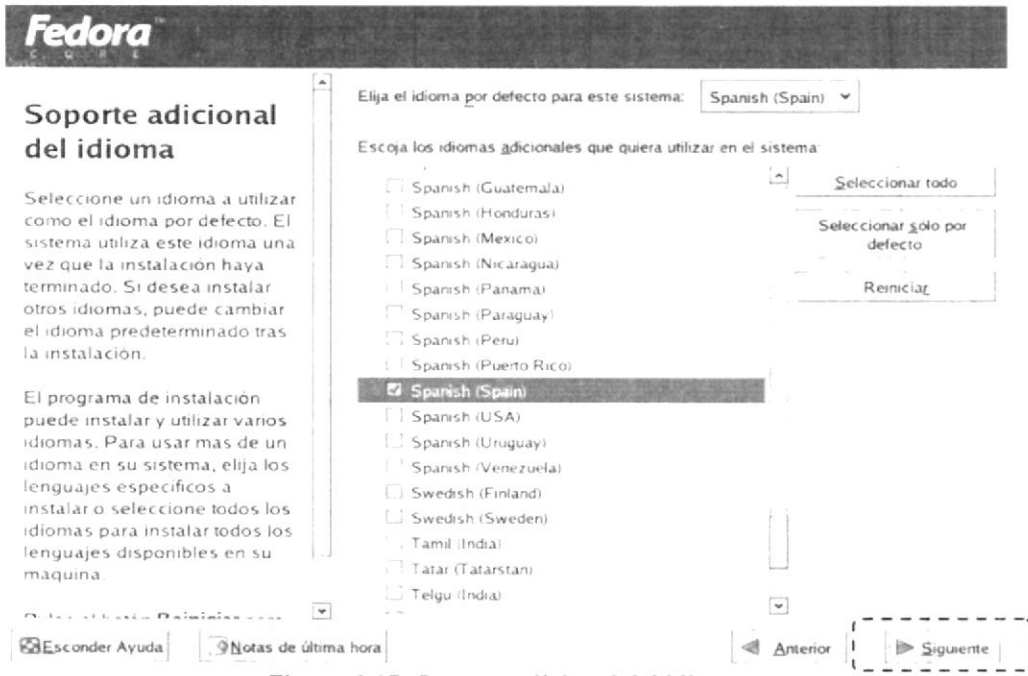


Figura 6-17: Soporte adicional del idioma

Seleccione la casilla **«El sistema horario usará UTC»**, que significa que el reloj del sistema utilizará **UTC** (**T**iempo **U**niversal **C**oordinado), que es el sucesor de **GMT** (b>**G**reenwich **M**ean **T**ime, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Haga clic con el ratón sobre la región que corresponda en el mapa mundial o seleccione en el siguiente campo la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

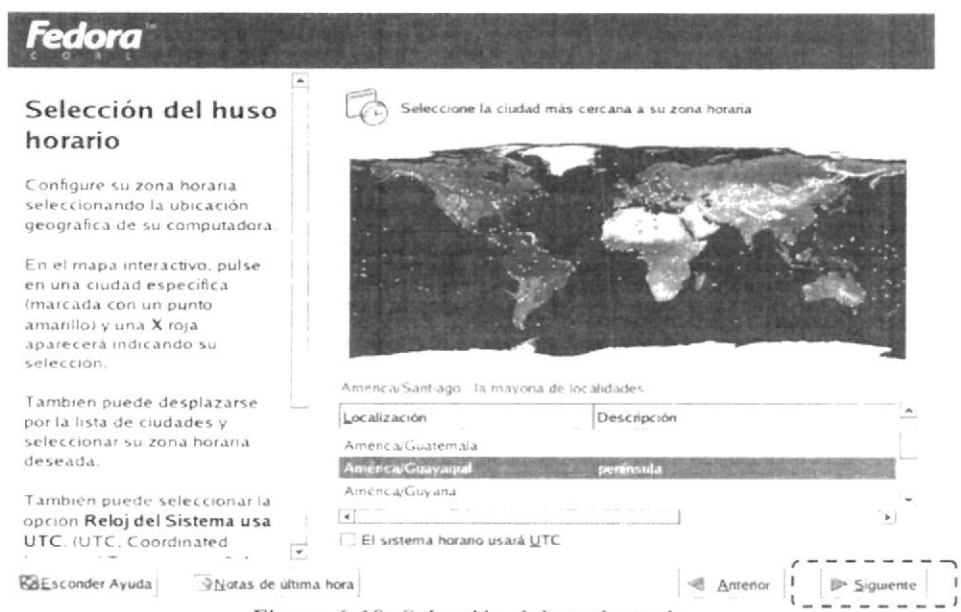


Figura 6-18: Selección del uso horario

En la Pantalla de configuración de contraseña del root, se le asigna una clave de acceso al usuario root. Debe escribirla dos veces a fin de verificar que está coincide. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así como cualquier combinación que tenga relación con datos personales, esta contraseña es útil para la administración del sistema.

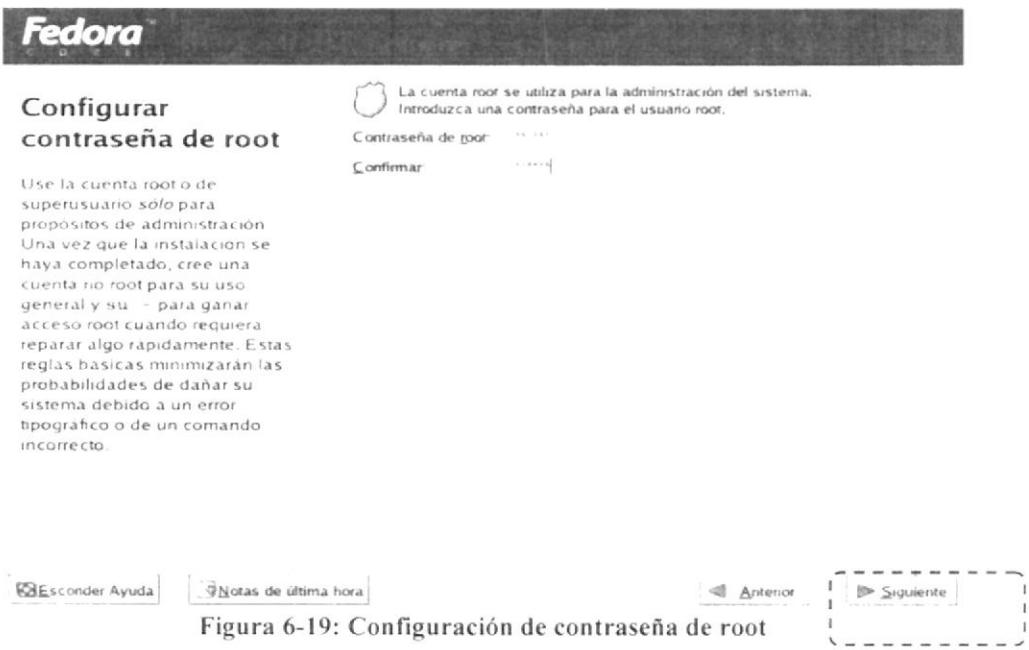


Figura 6-19: Configuración de contraseña de root

Al terminar, haga clic sobre el botón «**Siguiente**», y espere a que el sistema haga la lectura de información de los grupos de paquetes.

En la siguiente pantalla podrá seleccionar los grupos de paquetes que desea instalar en el sistema. Añada o elimine a su conveniencia dependiendo de las configuraciones que vaya a realizar en el servidor. Una vez hecho lo anterior, haga clic sobre el botón «**Siguiente**» a fin de iniciar el proceso.

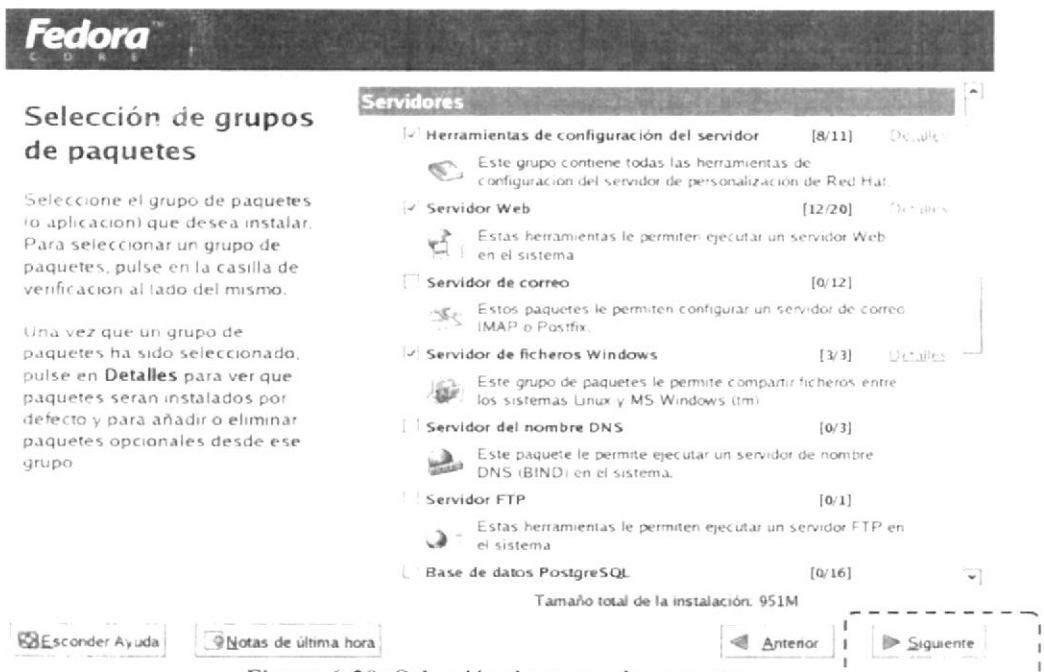


Figura 6-20: Selección de grupo de paquetes

Después de haber seleccionado todos los paquetes nos pedirá la confirmación para empezar a copias los mismos.

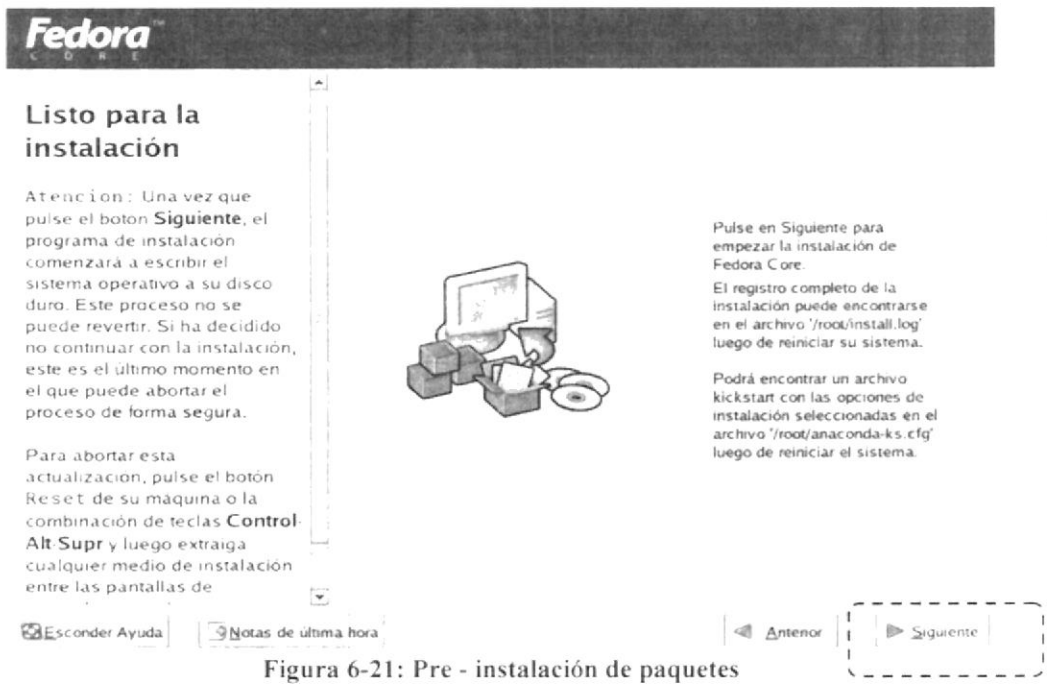


Figura 6-21: Pre - instalación de paquetes

Esta pantalla se muestra la instalación de los paquetes en progreso, este se inicia de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo. Espere a que se terminen los preparativos del proceso de instalación, el tiempo dependerá del número de paquetes a instalar.

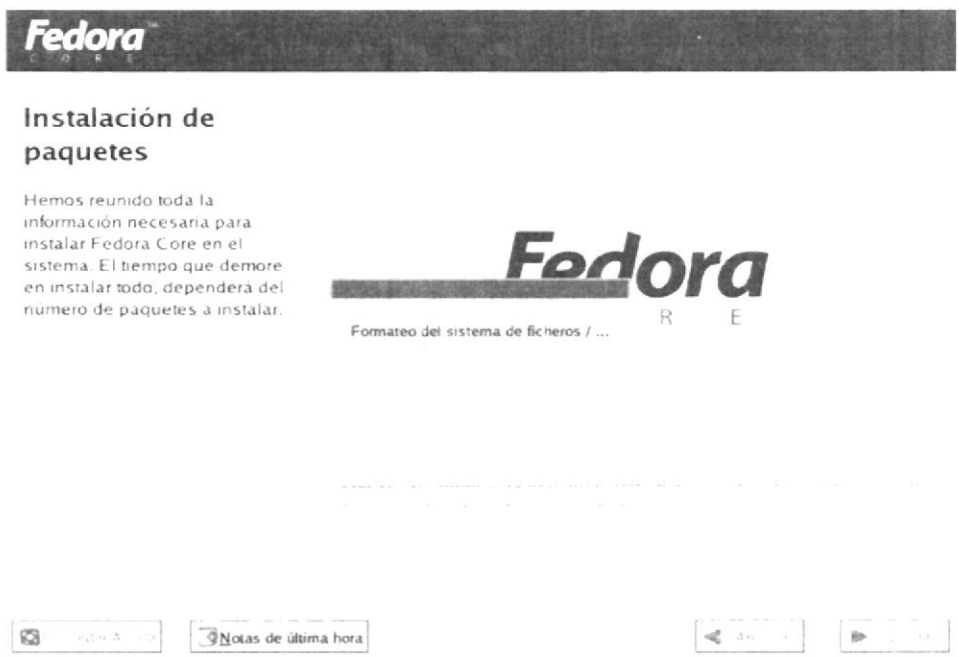


Figura 6-22: Instalación de paquetes

Una vez concluida la instalación de los paquetes, haga clic sobre el botón «**Reiniciar**».

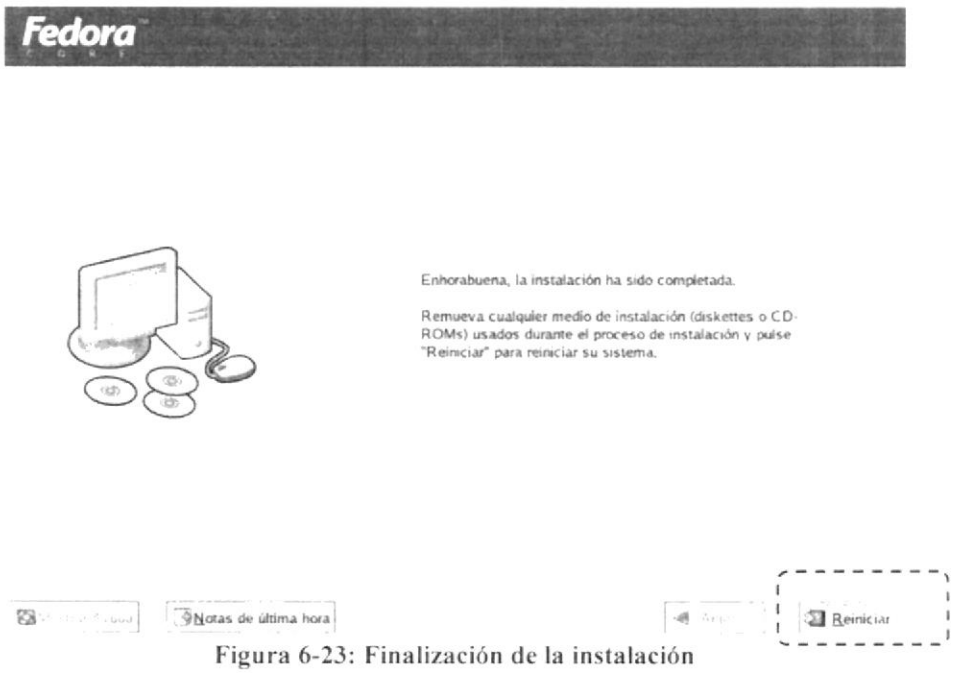


Figura 6-23: Finalización de la instalación

6.11 CONFIGURACIÓN POST – INSTALACIÓN

El Agente de configuración se carga la primera vez que usted inicia el nuevo sistema de *Fedora Core*..

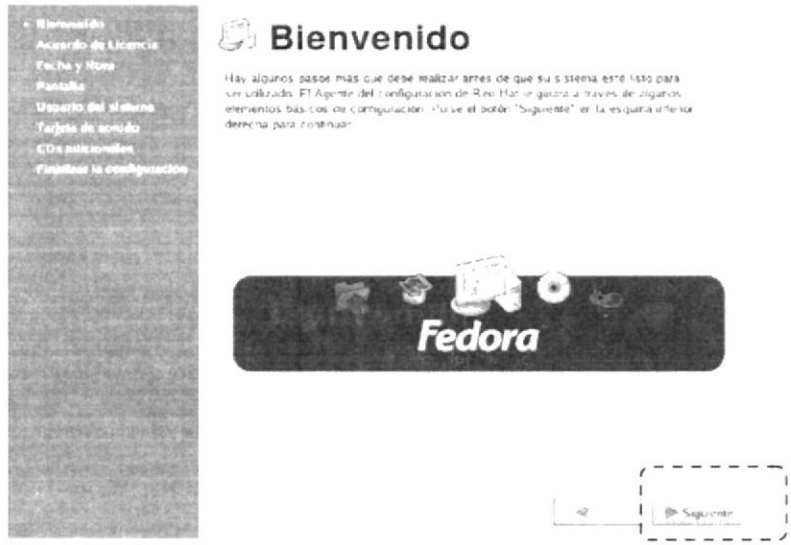


Figura 6-24: Pantalla de Bienvenido

Seleccione **«Siguiente»** para comenzar el agente de configuración

6.11.1 ACUERDO DE LICENCIA

Esta pantalla exhibe los términos de licencia que contiene *Fedora Core*. Cada paquete de software en *Fedora Core* esta cubierto por su propia licencia que ha sido aprobada por la *OSI Open Source Initiative* (Iniciativa de Código Abierto).

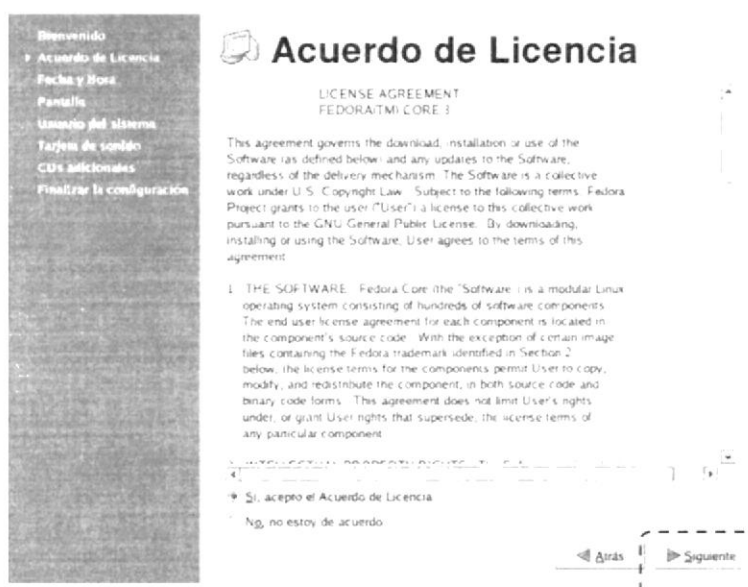


Figura 6-25: Acuerdo de Licencia

Seleccione Sí, acepto y luego de clic en **«Siguiente»** para continuar el agente de configuración

6.11.2 CONFIGURACIÓN DE LA FECHA Y HORA.

Proceda a configurar Fecha y Hora con la que funcionará el sistema.

Figura 6-26: Fecha y Hora

Seleccione **«Siguiente»** para continuar el agente de configuración

6.11.3 CONFIGURACIÓN DEL MONITOR.

En esta pantalla el agente configurará el monitor automáticamente, puede cambiar la resolución del tamaño a su comodidad y la profundidad de colores. Seleccione «**Siguiente**» para continuar.

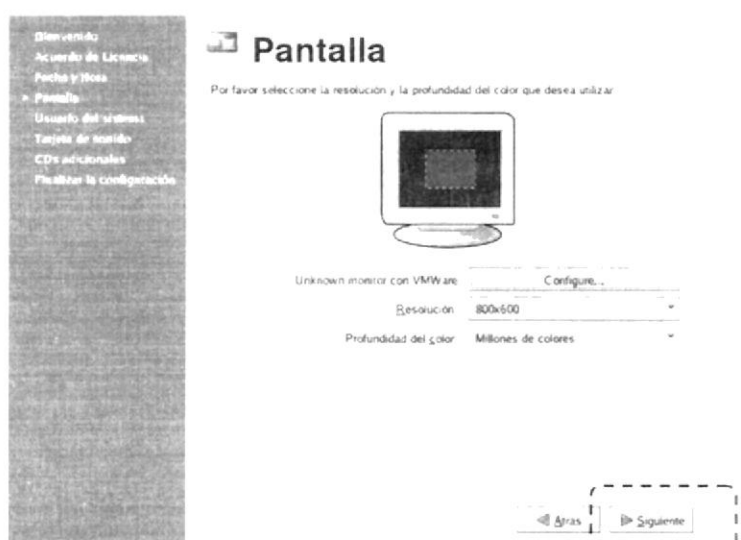


Figura 6-27: Resolución del monitor

6.11.4 USUARIOS DEL SISTEMA.

Cree una cuenta de usuario para usted con esta pantalla. Siempre use esta cuenta para iniciar sesión en su sistema Fedora Core, En el caso de administrar varios servicios puede usar la cuenta de *root* y saltar este paso si lo desea, podrá crear usuarios del sistema que no tendrán privilegios administrativos como el super-usuario root.

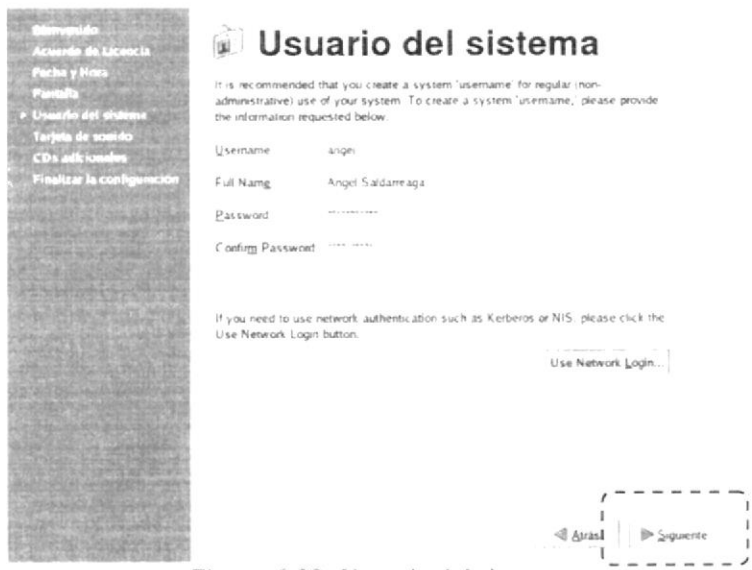


Figura 6-28: Usuario del sistema

Seleccione **«Siguiente»** para continuar el agente de configuración

6.11.5 TARJETA DE SONIDO.

El agente de configuración detectará la tarjeta de sonido si dispone y mostrará el modelo, realice una prueba de sonido.

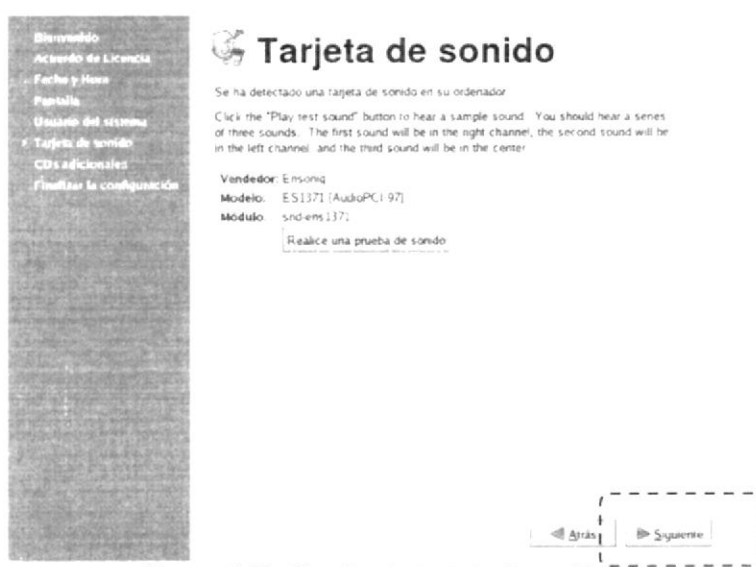


Figura 6-29: Prueba de tarjeta de sonido

Seleccione **«Siguiente»** para continuar el agente de configuración

6.11.6 CDS ADICIONALES.

En esta pantalla podrá instalar aplicaciones adicionales insertando el CD de aplicaciones y dando clic en Instalar.

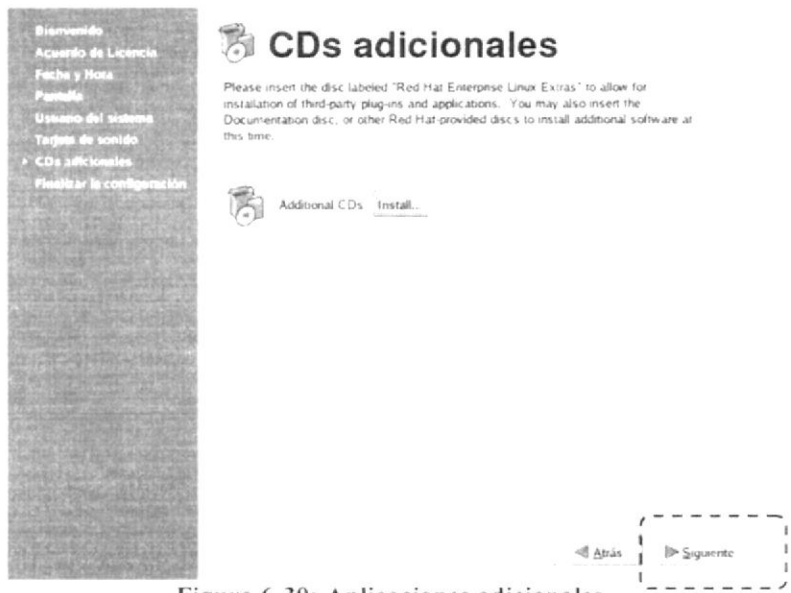


Figura 6-30: Aplicaciones adicionales

Seleccione **«Siguiente»** para continuar el agente de configuración

Finalmente está terminada la configuración y el usuario puede empezar a trabajar en el entorno de Fedora Core 3.

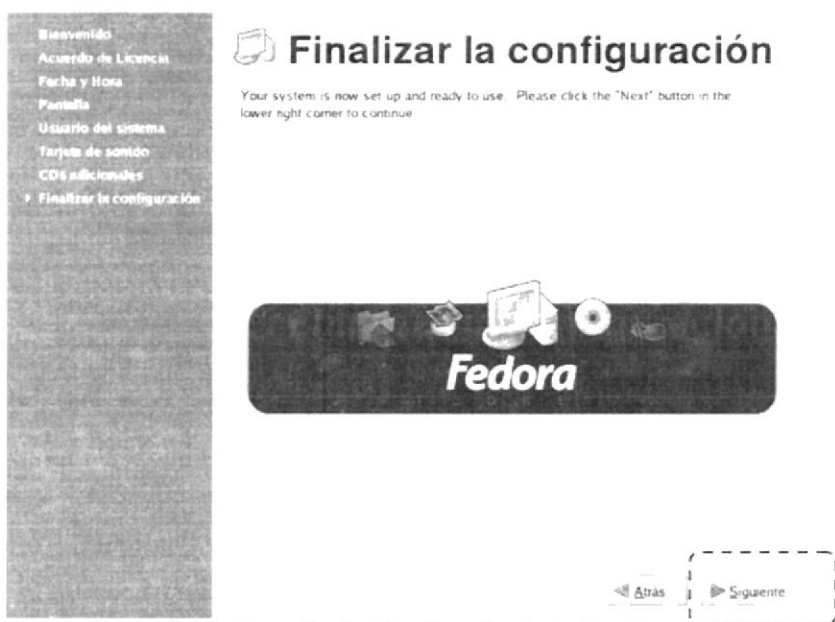


Figura 6-31: Pantalla de Finalización de la Configuración

6.11.7 CARGANDO SERVICIOS

Esta pantalla aparece en el momento que se están cargando los servicios.

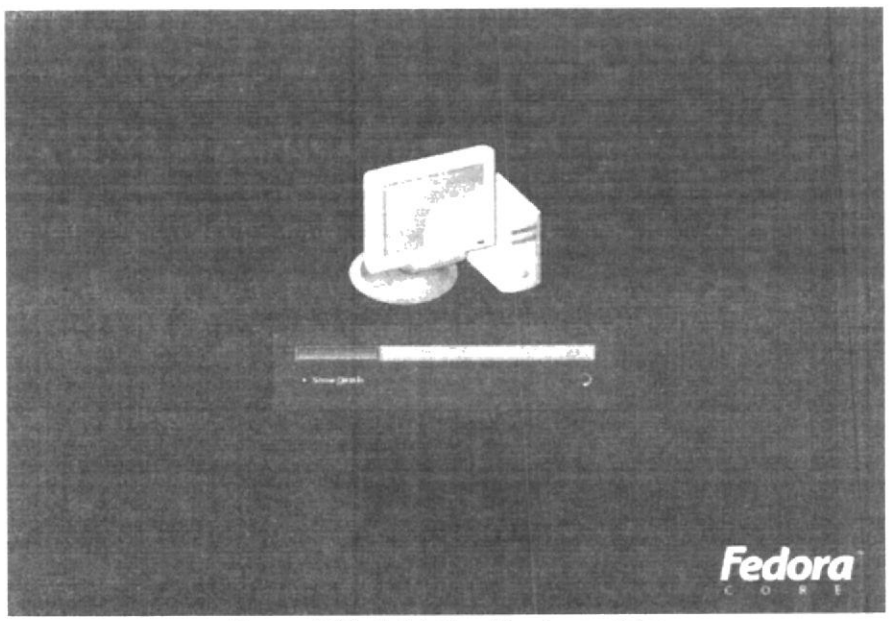


Figura 6-32: Inicialización de servicios

6.12 INICIO DE SESIÓN EN LINUX FEDORA

Para iniciar sesión en una instalación de Linux normalmente existen dos opciones las cuales son:

- Modo texto
- Modo gráfico

6.12.1 MODO TEXTO.

La combinación de las teclas **Ctrl** - ***Alt*** - ***F1*** permite ingresar a un inicio de sesión en **Modo texto** aunque con la misma combinación terminada en F2, F3, F4, F5 y F6 también permiten iniciar sesión en modo texto cada una de estas combinaciones son terminales diferentes, de modo que puedo estar levantando configurando algún servicio en una Terminal y enviando un correo en otra.

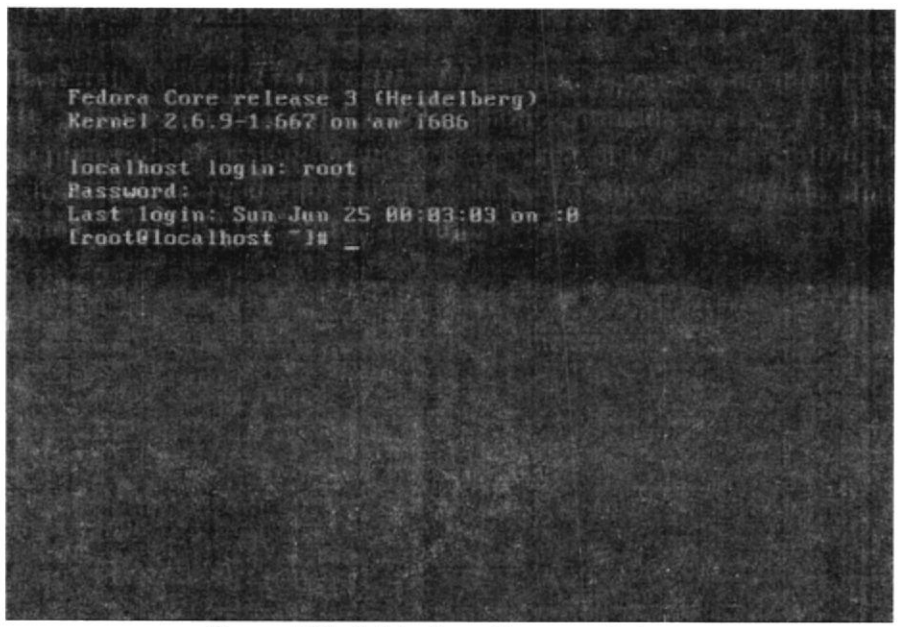


Figura 6-33: Inicio de sesión en modo texto

6.12.2 MODO GRÁFICO.

La combinación de las teclas ***Ctrl*** - ***Alt*** - ***F7*** permite ingresar a un inicio de sesión en **Modo gráfico**, aunque desde el modo gráfico se puede abrir Terminales en forma de ventanas, cuando usted ha realizado una instalación de Linux agregando el modo gráfico este se cargará por defecto.

Esta pantalla muestra la sesión de Linux en modo gráfico en la cual el usuario ingresará el ***username*** del administrador en esta caso utilizamos ***root*** (viene por default desde la instalación de Linux), en caso de que el usuario tenga otro username con su respectivo ***password*** también podrá ingresar al sistema operativo pero no con los mismos privilegios del administrador.

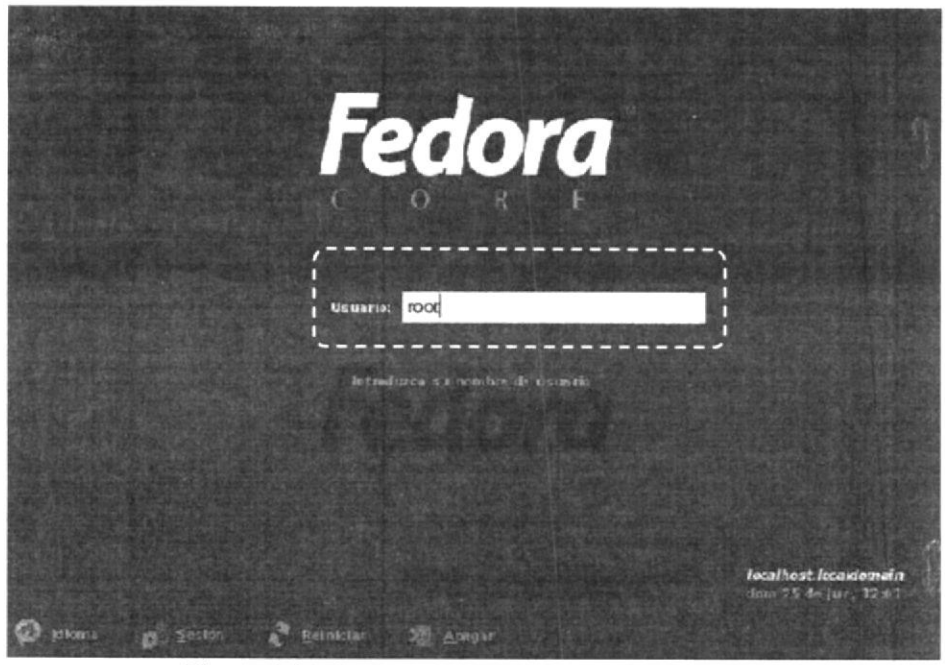


Figura 6-34: Ingreso de username en modo gráfico

La primera vez que se accede al sistema la contraseña empleada será la proporcionada por el administrador del sistema.

Por motivos de seguridad la contraseña debe cumplir ciertas condiciones tales como: Contener al menos seis caracteres, contener al menos un carácter numérico o especial y dos alfabéticos, ser diferente del nombre de login.

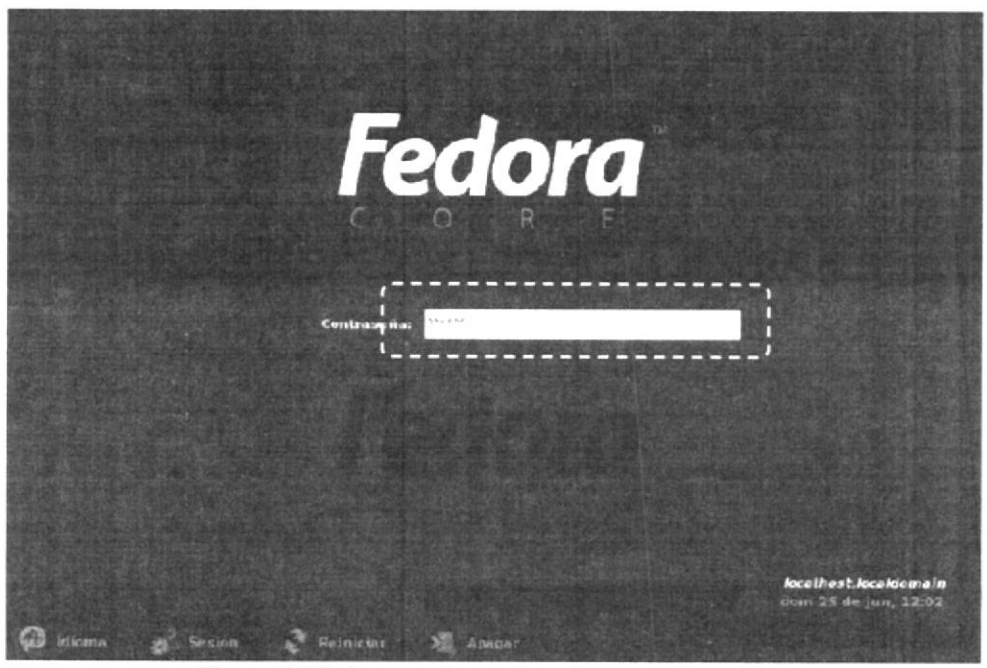


Figura 6-35: Ingreso de contraseña en modo gráfico

6.13 ENTORNO DE LINUX

Una vez que acceda podrás ver el entorno de Linux (escritorio).

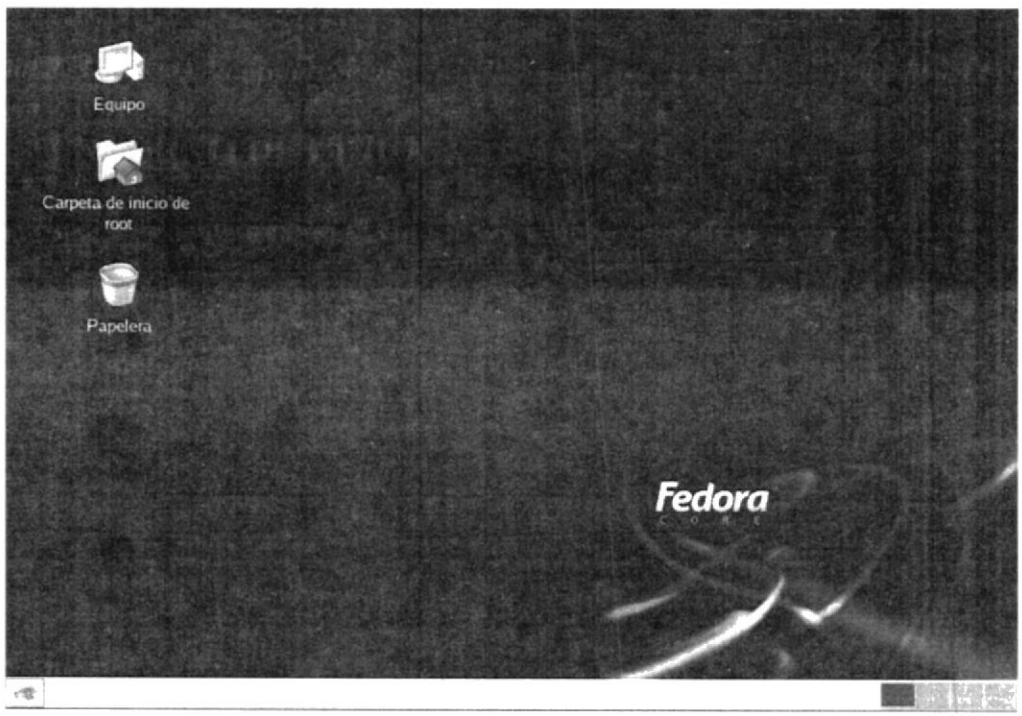


Figura 6-36: Entorno de Linux Fedora

6.14 AGREGAR O QUITAR PAQUETES

Si necesita agregar o quitar algún paquete de instalación realice lo siguiente: De clic en aplicaciones elija configuración del sistema y de clic en Añadir/Eliminar aplicaciones.

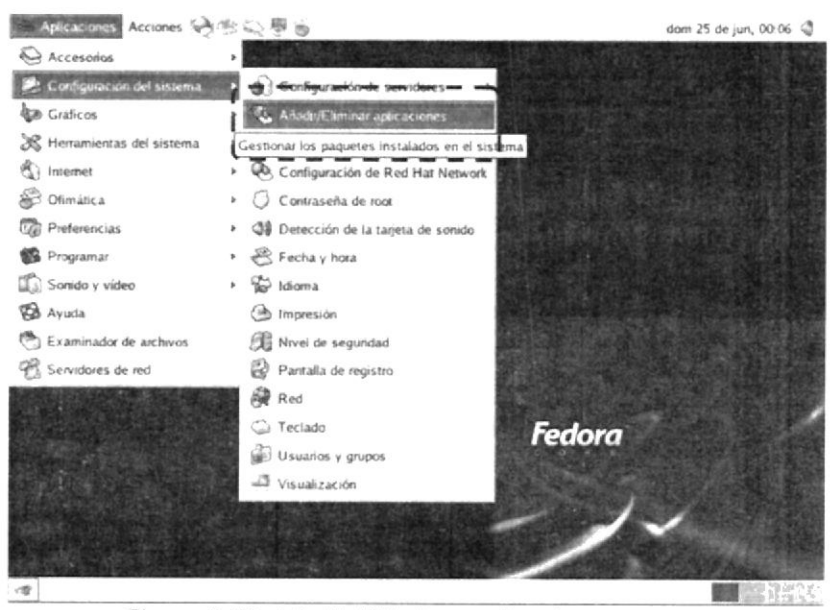


Figura 6-37: Añadir/Eliminar aplicaciones

6.15 COMANDOS BÁSICOS

- ✓ **cp**
  Copia archivos a un destino especificado
  Ejemplo: **[root@armada /]** #cp *estearchivo.txt* /home/*estedirectorio*

- ✓ **mv**
  Mueve archivos a un destino especificado
  Ejemplo: **[root@armada /]** #mv *estearchivo.txt* /home/*estedirectorio*

- ✓ **date**
  Muestra la fecha
  Ejemplo: **[root@armada /]** #date

- ✓ **delete**
  Borra un archivo
  Ejemplo: **[root@armada /]** #delete *archivo.txt*

- ✓ **mkdir**
  Crea un directorio
  Ejemplo: **[root@armada /]** #mkdir *Datos*

- ✓ **rmdir**
  Borra un directorio
  Ejemplo: **[root@armada /]** #rmdir *Datos*

- ✓ **cd**
  Permite cambiarse de directorio
  Ejemplo: **[root@armada /]** #cd */etc*
  Si agrega un espacio y dos puntos seguidos permiten salir del directorio actual.
  Ejemplo: **[root@armada /]** #cd ..

- ✓ **ls**
  Lista los archivos de un directorio
  ls –a Lista todos los archivos incluso los ocultos.
  ls –l Lista todos los atributos de los archivos listados .
  Ejemplo: **[root@armada /]** #ls –a /etc

- ✓ **logout**
  Salir de la sesión actual
  Ejemplo: **[root@armada /]** #logout

- ✓ **shutdown**
  Da de baja al sistema
  shutdown –h now apaga el sistema
  shutdown –r now reinicia el sistema
  Ejemplo: **[root@armada /]** #shutdown –r now

- ✓ **clear**
  Limpia la pantalla de la Terminal
  Ejemplo: **[root@armada /]** #clear

- ✓ **exit**
  Cierra la Terminal (shell)
  Ejemplo: **[root@armada /]** #exit

- ✓ **more**
  Muestra el contenido de los archivos indicados por pantalla
  Ejemplo: **[root@armada /]** #more */etc/smb.conf*

- ✓ **cat**
  Concatena archivos o muestra el contenido completo sin pausa
  Ejemplo: **[root@armada /]** #cat */etc/squid/squid.conf*

- ✓ **echo**
  Muestra caracteres en pantalla
  Ejemplo: **[root@armada /]** #echo *este mensaje*

- ✓ **grep**
  Busca texto dentro de un archivo
  Ejemplo: **[root@armada /]** #grep *esta palabra o frase archivo.txt*

- ✓ **man**
  Muestra ayuda sobre un comando
  Ejemplo: **[root@armada /]** #man *cd*

- ✓ **pwd**
  Muestra la localización de un archivo en el sistema
  Ejemplo: **[root@armada /]** #pwd

- ✓ **free**
  Muestra la memoria y su uso actual
  Ejemplo: **[root@armada /]** #free

- ✓ **chmod**
  Modifica los permisos de un archivo o directorio, se basa en estos valores:
  r: lectura 4
  w: escritura 2
  x : ejecución 1
  +/- : + agrega permisos, - quita permisos
  Ejemplo: **[root@armada /]** #chmod *+777 archivo.txt*

- ✓ **service**
  Para chequear los estados de cualquiera de los servicios del sistema
  Sintaxis: service <nombre del servicio> estado
  status : Muestra el estado actual del servicio
  stop : Detiene el servicio
  start : Arranca un servicio
  restart : Reinicia un servicio
  reload : Recarga un servicio sin detenerlo
  Ejemplo: **[root@armada /]** # service dhcp start

- ✓ **ping**
  Comprueba el estado de la conexión con uno o varios equipos remotos, para determinar si un sistema IP específico es accesible en una red.
  Ejemplo: **[root@armada /]** #ping 192.168.0.11

- ✓ **Ctrl + c**
  Combinación de teclas que detiene un proceso en ejecución

- ✓ **useradd**
  Crea usuarios al sistema
  Ejemplo: **[root@armada /]** #useradd angel

- ✓ **passwd**
  Este comando agrega contraseñas a usuarios del sistema
  Ejemplo: **[root@armada /]** #passwd angel

- ✓ **touch**
  Crea archivo sin contenido.
  Ejemplo: **[root@armada /]** #touch *dato.txt*

- ✓ **updatedb**
  Actualiza la base de datos del sistema
  Ejemplo: **[root@armada /]** #updatedb

- ✓ **slocate**
  Busca un archivo en el sistema, se recomienda previamente actualizar la base de datos.
  Ejemplo: **[root@armada /]** #slocate *smb.conf*

- ✓ **rpm**
  Chequea el estado de los paquetes rpm, necesarios para instalar algún paquete del sistema.
  rpm – q Verifica si se tiene instalado algún paquete
  rpm – i Instala un paquete determinado
  rpm – i Desinstala un paquete determinado
  Ejemplo: **[root@armada /]** #rpm –q squid

- ✓ **tar**
  tar –cvf Empaquetar archivos
  tar –xvf Desempaqueta archivos
  c: Crea un nuevo archivo tar.
  v: Modo verbose, quiere decir que mostrará por pantalla las operaciones que va realizando archivo por archivo, si no se pone esta opción ejecutará la acción pero en pantalla no veremos el proceso.
  x: Extrae los archivos (Descomprime los ficheros que se encuentran dentro del archivo tar).
  f: Cuando se usa con la opción -c, usa el nombre del archivo especificado para la creación del archivo tar; cuando se usa con la opción -x, retira del archivo el archivo específico.
  Ejemplo: **[root@armada /]** #tar –cvf *paquete.tar /etc*

- ✓ **gzip**
  Comprime un archivo
  Ejemplo: **[root@armada /]** # gzip *comprimido.gz*

- ✓ **chown**
  Cambia propietario de archivo
  Ejemplo: **[root@armada /]** #chown *angel /etc/texto.txt*

- ✓ **chgrp**
  Cambia grupo de archivo
  Ejemplo: **[root@armada /]** #chgrp ventas */etc/texto.txt*

- ✓ **ln**
  Crea un enlace físico para un determinado archivo
  Enlace físico: Es crear otro archivo idéntico con un nombre diferente.
  Ejemplo: **[root@armada /]** #ln original copia
  ln –s Crea un enlace simbólico para un determinado archivo
  Enlace simbólico: Es crear otro archivo idéntico con un nombre diferente, pero si se realizan cambios en uno de los dos se reflejan en ambos dichos cambios.
  Ejemplo: **[root@armada /]** #ln –s original copia

- ✓ **who**
  Para saber todos los usuarios que están conectados a nuestro sistema.
  Ejemplo: **[root@armada /]** #who
  who am I:Para saber con que usuario se está conectado al sistema.
  Ejemplo: **[root@armada /]** #who am I

6.16 EDITOR VI

Vi es uno de los editores de texto más poderos y añejos que hay en el mundo de la informática. Resulta sumamente útil conocer la funcionalidad básica de Vi a fin de facilitar la edición de ficheros de texto simple, principalmente ficheros de configuración.
Por lo general, Vi se instala de modo predefinido en la mayoría de las distribuciones de GNU/Linux a través del paquete vim-minimal.

6.16.1 MODOS DE VI

Vi tiene tres modos de utilización, pero detallaremos los dos más comunes:

- **Modo normal:** En este modo Vi interpretará todo lo que escribamos para realizar acciones determinadas. Es el modo predeterminado cuando arranca el editor.

- **Modo inserción:** Este modo se utiliza para modificar el contenido de un archivo, es decir, escribir texto, eliminarlo o desplazarnos por él. Es el modo que más se utiliza. Para volver al modo normal desde este modo, presionaremos siempre la tecla ESC.

6.16.2 SINTAXIS DE VI

Vi [**opciones**] [**fichero**]

- Opciones: aquí pondremos las opciones admitidas por Vi
- Fichero: si el archivo tecleado existe, se mostrará, sino crearemos un archivo en blanco con el nombre especificado. Puede especificar más de un fichero separados por espacios en blanco.

Para editar un archivo de configuración haga lo siguiente:
vi squid.conf

- Modo normal: Estando en modo normal presionamos

yy Copia la línea actual
yn° Copiamos N líneas desde la posición actual y hacia abajo
p Pegamos lo copiado debajo de la línea actual
P Pegamos lo copiado encima de la línea actual
U Deshace todo los cambios que se han producido en la línea actual
u Deshace el último cambio
Crtl+R Rehace un cambio
:red Rechace un cambio
:/cadena Buscamos la cadena de caracteres desde la posición actual y hasta el final del fichero. Utilizamos la tecla "n" para ir adelante y "N" para ir atrás.
:nohl Al hacer la búsqueda de la cadena se resaltan los resultados para eliminar el resaltado tecleamos esta combinación de teclas.
:q Sale si no hubo cambios en el fichero
:q! Sale descartando todos los cambios en el fichero
:w Graba los cambios sin salir del fichero
:wq Graba los cambios y sale del fichero
:x Graba los cambios y sale del fichero
:saveas Guarda el fichero con otro nombre
:set ic Realizamos búsquedas ignorando las mayúsculas/minúsculas
:setnumber Numera las líneas
:syntax on Activa el coloreado de sintaxis en archivos de código fuente

- Modo de inserción: Para ingresar a modo inserción presionamos

i Insertar texto antes del carácter sobre el que esta el cursor
I Inserta texto al comienzo de la línea en la que está el cursor
Insert Inserta texto
a Inserta texto después del carácter sobre el que esta el cursor
A Inserta texto al final de la línea que esta el cursor
o Abre una nueva línea e inicia insertar texto en la nueva línea.
dd Elimina la línea actual donde se encuentre el cursor.

6.17 INGRESAR A UNA TERMINAL

Hay dos opciones de acceder a una Terminal:

- De clic en aplicaciones, herramientas del sistema y elija abrir una Terminal.
- Clic derecho en el escritorio, elija abrir una Terminal, cualquiera de las dos opciones lo llevará a la siguiente pantalla en la cual puede realizar las configuraciones tanto de la tarjeta de red como de los servidores.

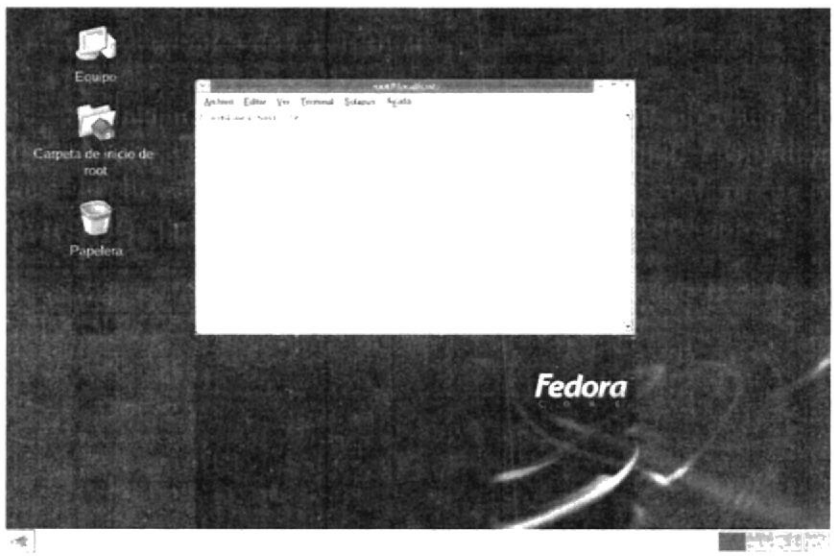


Figura 6-38: Terminal de Linux

6.18 CONFIGURAR LA TARJETA DE RED

En caso de que no este configurada la tarjeta de red, tendrá dos opciones a seguir:

6.18.1 AMBIENTE TEXTO

Abra una Terminal y ejecute el comando ***ifconfig***.

ifconfig	:	Comando para configurar la tarjeta de red.
eth0	:	Nombre del adaptador de red
192.168.0.11	:	Dirección IP asignada a la tarjeta de red de la máquina.
netmask.	:	La máscara de red por defecto. Ej. 255.255.255.0
up/down	:	Para levantar el adaptador de red (up), o bajarlo (down)

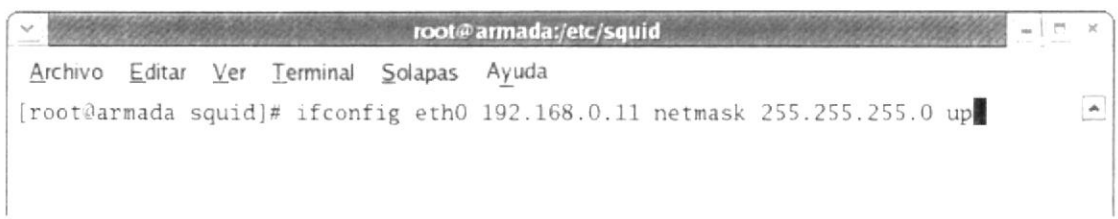


Figura 6-39: Configuración de la tarjeta de red en ambiente texto

6.18.2 AMBIENTE GRÁFICO

- Utilice el comando ***netconfig*** y aparece la interfaz gráfica.
  Le preguntará si desea configurar la red y presione la tecla enter en Sí

Dirección IP : 192.168.0.11
Máscara de red: 255.255.255.0

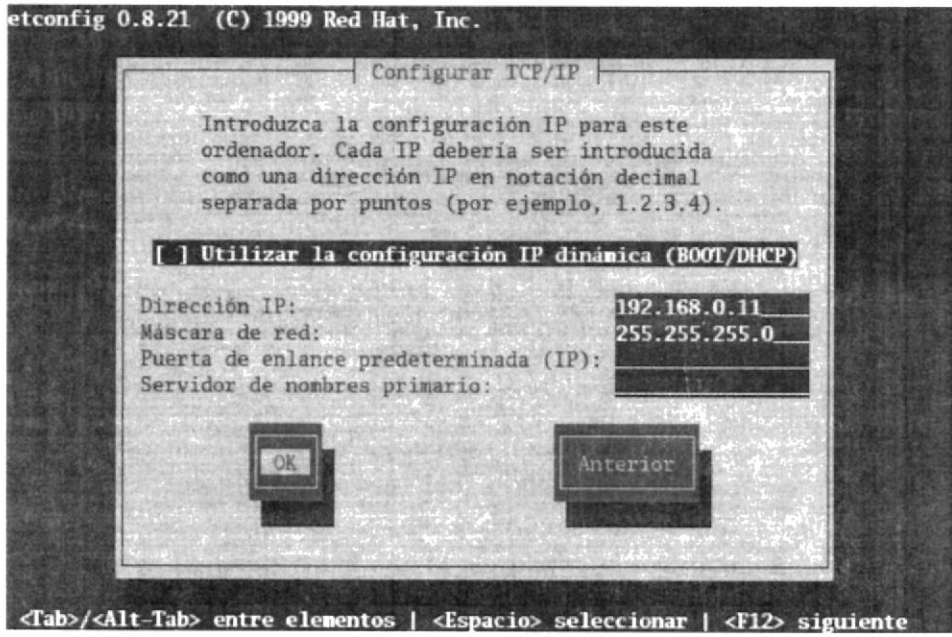


Figura 6-40: Configuración de la tarjeta de red en ambiente gráfico

Una vez asignada la IP con su máscara proceda a reiniciar los servicios de la tarjeta de red para que tome los cambios realizados.

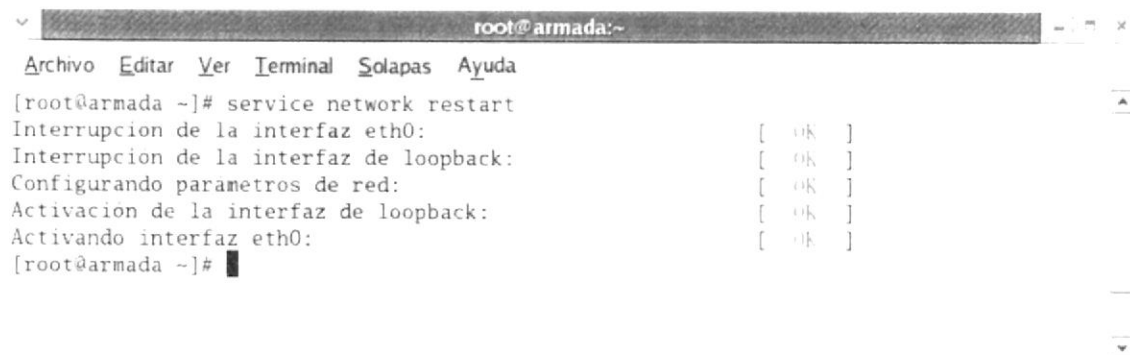


Figura 6-41: Reiniciando los servicios de la tarjeta de red

6.19 SERVIDOR SAMBA

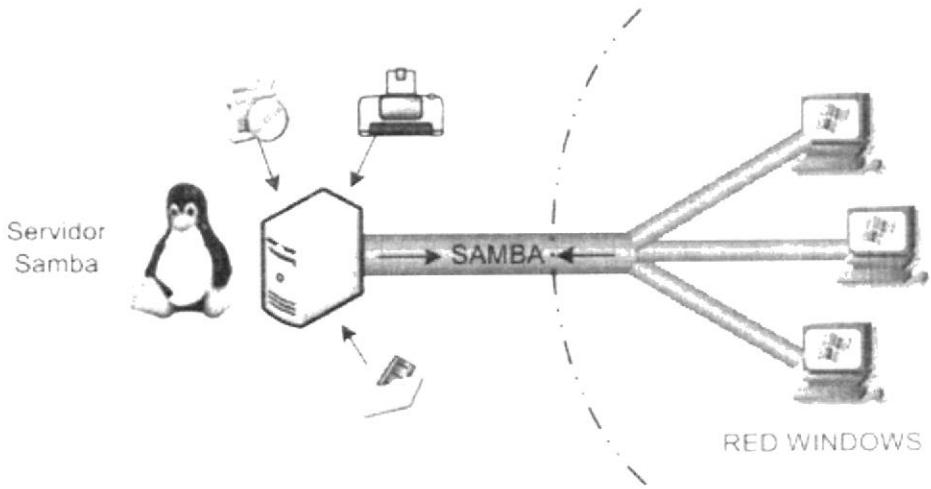


Figura 6-42: Esquema de Samba

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con Linux o Mac OS X se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

SMB es un protocolo de comunicación de alto nivel que puede implementarse sobre diversos protocolos como TCP/IP, NetBEUI y IPX/SPX, junto con la ubicación de dichos protocolos en los niveles OSI y en la pila TCP/IP. Entre todas esas alternativas, tanto en el caso de Samba como de Windows 2000/XP, SMB se implementa habitualmente encima de NetBIOS sobre TCP/IP (esta alternativa se ha convertido en el estándar para compartir recursos entre sistemas Windows y Linux).

Históricamente, este protocolo fue desarrollado inicialmente por IBM como el IBM PC Network SMB Protocol o Core Protocol a principios de los años 80. Desde entonces, diversos fabricantes (especialmente Microsoft) han ido ampliando su funcionalidad progresivamente, creando diferentes variantes (versiones) de SMB. Desafortunadamente, en ocasiones el cambio de versión ha conllevado el rebautizar el propio protocolo. En este sentido, SMB ha recibido, entre otros, los siguientes nombres: Core Protocol, DOS Lan Manager, LAN Manager, NTLM (NT Lan Manager), y en los últimos años, CIFS (Common Internet File System). Todos ellos, por tanto, hacen referencia a SMB, aunque se diferencien en algunos detalles de su funcionalidad y/o implementación.

Si nos fijamos en su interfaz, SMB es un protocolo de tipo cliente/servidor, donde el ordenador "servidor" ofrece recursos (archivos, impresoras, etc.) que pueden ser utilizados remotamente por los ordenadores "cliente" a través de la red. Asimismo, es un protocolo de los denominados petición/respuesta, indicando que las comunicaciones se inician siempre desde el cliente como una petición de servicio al servidor (dicha petición se denomina precisamente SMB), que la procesa y retorna una respuesta a dicho cliente. (En realidad, existe un caso en que el servidor envía un mensaje al cliente sin haber recibido una petición de éste, pero la discusión del protocolo a ese nivel queda

fuera del ámbito de este texto). La respuesta del servidor puede ser positiva (con el resultado de procesar la petición del cliente) o negativa (mensaje de error), en función del tipo de petición, la disponibilidad del recurso, el nivel de acceso (permisos) del cliente, etc.

Características

Samba es una implementación de una docena de servicios y una docena de protocolos, entre los que están: NetBIOS sobre TCP/IP (NetBT), SMB (también conocido como CIFS), DCE/RPC o más concretamente, MSRPC, el servidor WINS también conocido como el servidor de nombres NetBIOS (NBNS), la suite de protocolos del dominio NT, con su Logon de entrada a dominio, la base de datos del gestor de cuentas seguras (SAM), el servicio Local Security Authority (LSA) o autoridad de seguridad local, el servicio de impresoras de NT y recientemente el Logon de entrada de Active Directory, que incluye una versión modificada de Kerberos y una versión modificada de LDAP. Todos estos servicios y protocolos son frecuentemente referidos de un modo incorrecto como NetBIOS o SMB.

Samba configura directorios Unix/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de Linux pueden montar en sus sistemas de archivos estás unidades de red como si fueran dispositivos locales, o utilizar la orden smbclient para conectarse a ellas muy al estilo del cliente de la línea de órdenes ftp. Cada directorio puede tener diferentes permisos de acceso sobrepuestos a las protecciones del sistema de archivos que se esté usando en Linux. Por ejemplo, las carpetas home pueden tener permisos de lectura y escritura para cada usuario, permitiendo que cada uno acceda a sus propios archivos; sin embargo, deberemos cambiar los permisos de los archivos localmente para dejar al resto ver nuestros archivos, ya que con dar permisos de escritura en el recurso no será suficiente.

Los ficheros relacionados con la idea del servidor Samba se agrupan en el directorio ***/etc/samba***. El fichero de configuración principal es: ***smb.conf***, este fichero consta de varias secciones que se identifican a través de una cadena encerrada entre corchetes.

6.19.1 REQUERIMIENTOS DE CONFIGURACIÓN SAMBA

- Tener instalado el sistema Linux Fedora Core 3
- Tener una IP estática en el Server Linux
- Tener configurada la tarjeta de red, tanto en el Server Linux como en el cliente.
- Tener instalado el paquete de Samba (smb)
- Deshabilitar los firewalls en el Server Linux y clientes.

Es necesario deshabilitar los firewalls para no tener ningún tipo de restricciones al momento de levantar los servicios, ya que estos usan puertos y protocolos que podrían ser bloqueados por el o los cortafuegos. De esta manera no tendremos ningún tipo de conflicto al realizar nuestra configuración.

6.19.2 CONFIGURACIÓN SAMBA

Verificar si está instalado el paquete *smb*, digitando el siguiente comando: **[root@armada /] # rpm –q smb**

Proceda a editar el archivo de configuración de samba de la siguiente manera: **[root@armada /] vi /etc/samba/smb.conf.**

Una vez que el fichero esta abierto modifique las siguientes líneas:

Workgroup: Indica el grupo de trabajo en el cual se va a compartir información y equipos; en este caso nuestro workgroup es: [**CETEIG**].

Netbios name: Es el nombre de la máquina, en este caso es: [**Server**].

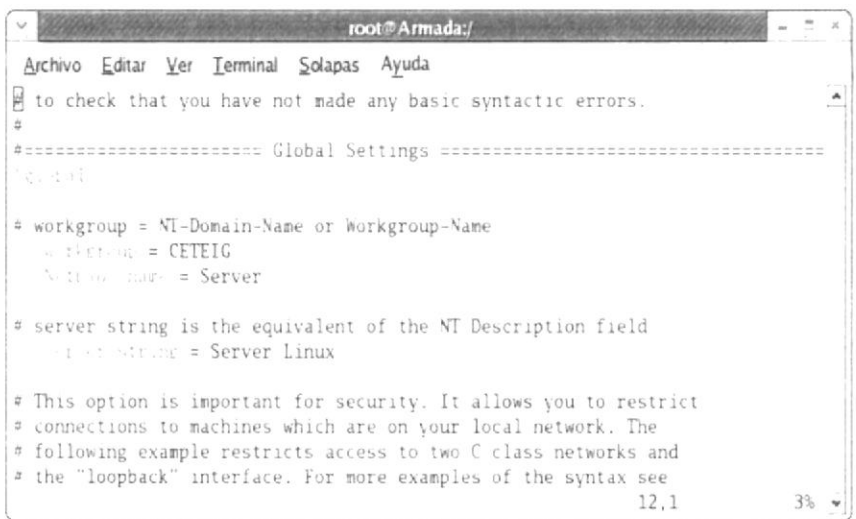


Figura 6-43: Configuración de Global Settings

A continuación diríjase a la sección del ***Share Definitions*** y modifique las siguientes líneas:

path = /Respaldo [ruta del directorio]

valid user = Usuario1 [usuarios que tendrán acceso]

writable = yes [permiso de escritura]

browseable = yes [permiso de navegación]

public = yes [acceso para usuario guest o invitado]

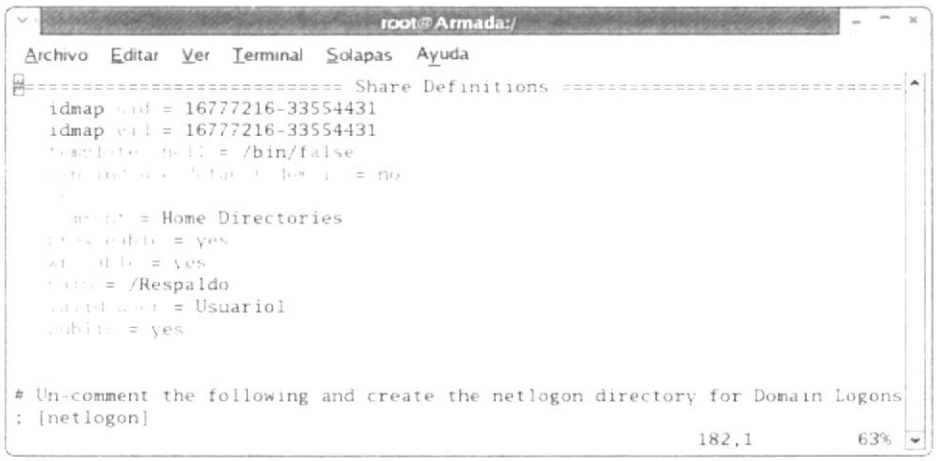


Figura 6-44: Configuración de Share Definitions

Para guardar cambio realizados presione la tecla ***esc*** y digite ***:wq*** seguidamente presione la tecla enter...
Las configuraciones hechas en esta sección se aplican a la totalidad de los recursos compartidos, independientemente de la configuración especifica.

El siguiente paso es crear un directorio (***Respaldo***) con el comando: ***mkdir***.

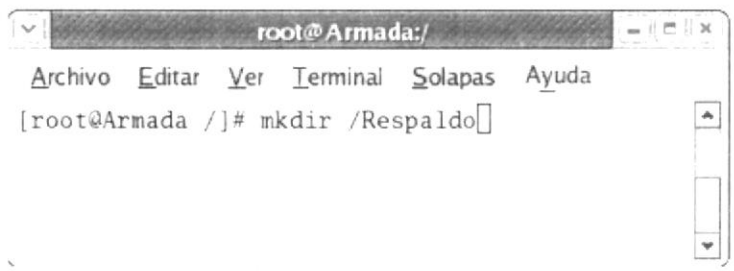


Figura 6-45: Creación de directorio a compartir

Cree un archivo dentro del directorio anterior (Ejemplo.txt), esto lo hará con el comando ***touch***.

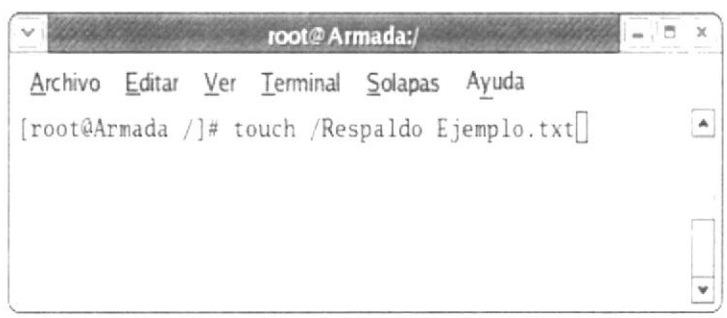


Figura 6-46: Creación de fichero a compartir

Asigne los permisos al directorio y al archivo con el comando ***chmod*** que autoriza permisos

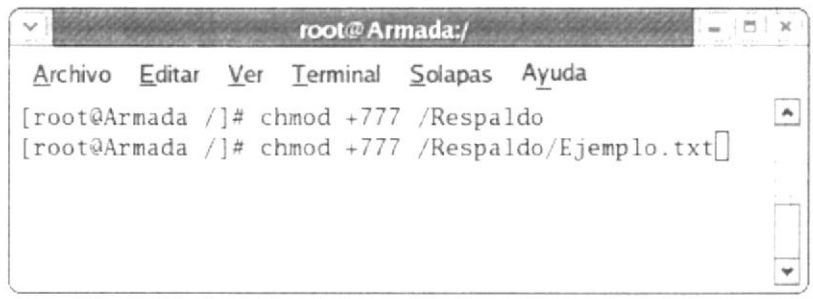


Figura 6-47: Aplicación de permisos a directorio y fichero

En esta sección creará los usuarios que anteriormente registró en *valid user* que esta dentro del *share definition* y luego asigne la respectiva contraseña con los comandos *adduser* para agregar al usuario y *passwd* para asignar la contraseña.

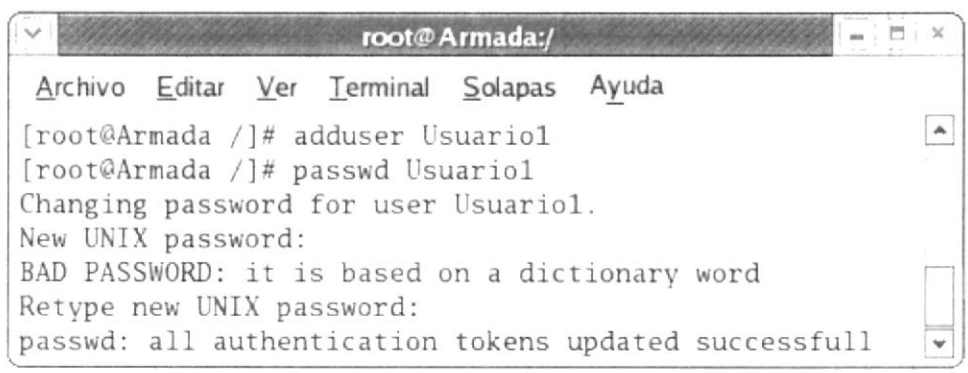


Figura 6-48: Agregando usuario al sistema

Para trabajar en el servicio de Samba asigne contraseñas a los usuarios, de esta forma podremos acceder a los recursos de Linux desde el cliente Windows.
Utilice el comando smbpasswd para agregar la contraseña seguido del nombre del usuario, a continuación pedirá que ingrese la contraseña y que la confirme

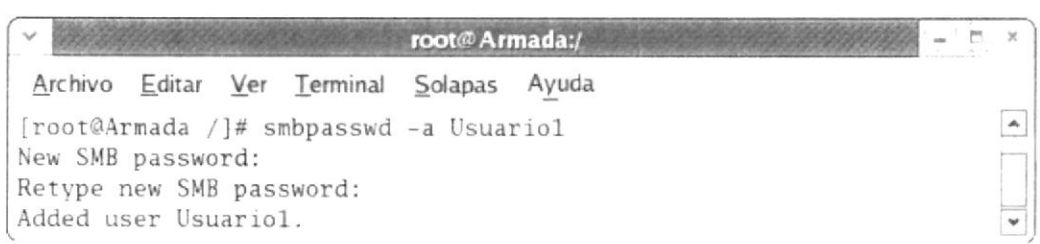


Figura 6-49: Asignando contraseña al usuario de Samba

Proceda a levantar los servicios de samba con el comando service smb start.

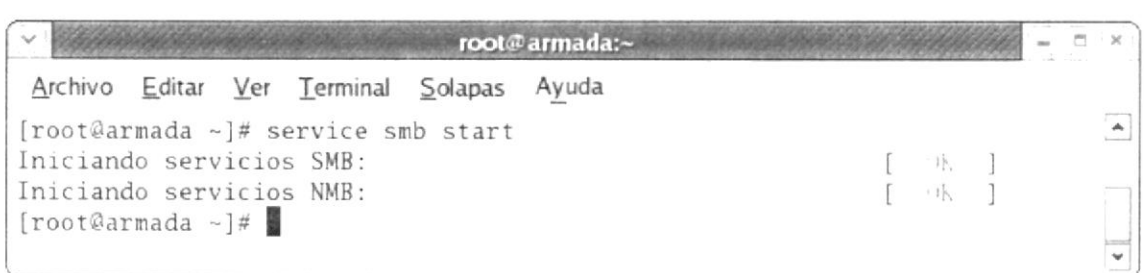


Figura 6-50: Levantando servicios de Samba

6.19.3 CARGAR SERVICIOS SAMBA AL INICIAR EL SISTEMA

Digite **setup** en la Terminal y habilite el servicio **smb** para que se ejecute automáticamente al iniciar Fedora.
Proceda a entrar en servicios del sistema, marcándolo y luego con la tecla tab ubíquese en ejecutar una herramienta y presione la tecla enter.

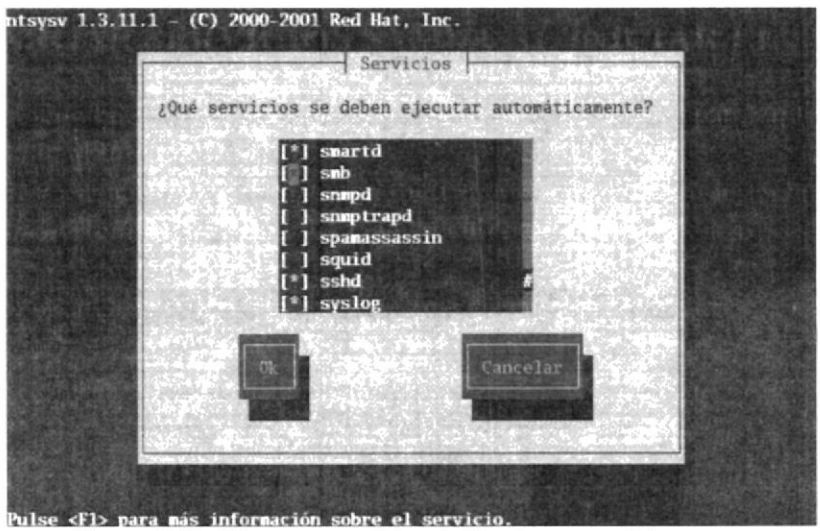


Figura 6-51: Ejecutar servicios de Samba automáticamente

6.19.4 POSIBLES ERRORES AL RESTAURAR LOS SERVICIOS DE SAMBA

Si se presentan errores proceda a realizar los siguientes pasos:

- Verificar si esta levantada la tarjeta de red, de no estarlo volver a configurarla con los pasos antes mencionados.
- Verificar si los firewall están deshabilitados, ya que es un requerimiento para que samba funcione
- Verificar en los servicios del sistema si están instalados los paquetes smb, network y xinetd
- Verificar si están asignados los permisos a los usuarios para poder acceder a mis recursos Linux desde Windows.

6.19.5 CONFIGURACIÓN EN CLIENTE WINDOWS

De clic sobre el menú Inicio, ente al Panel de Control, de doble clic en Conexiones de Red y se presenta la siguiente pantalla.

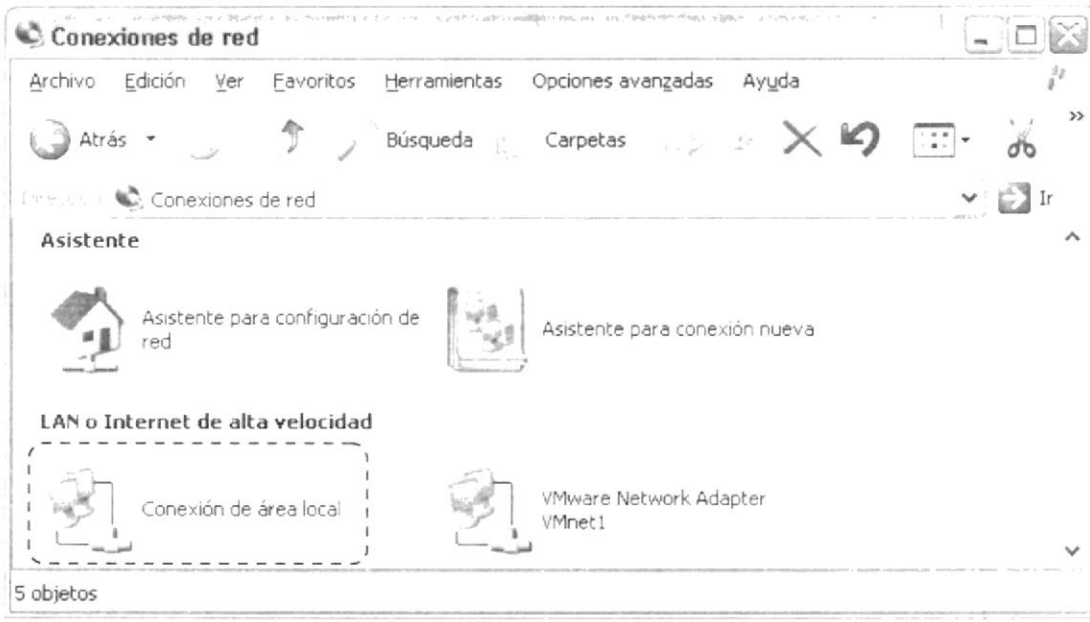


Figura 6-52: Conexiones de red

De doble clic en Conexión de área local y entre a Propiedades

Figura 6-53: Estado de conexión de área local

Ubíquese en Protocolo Internet (TCP/IP) y de clic en Propiedades

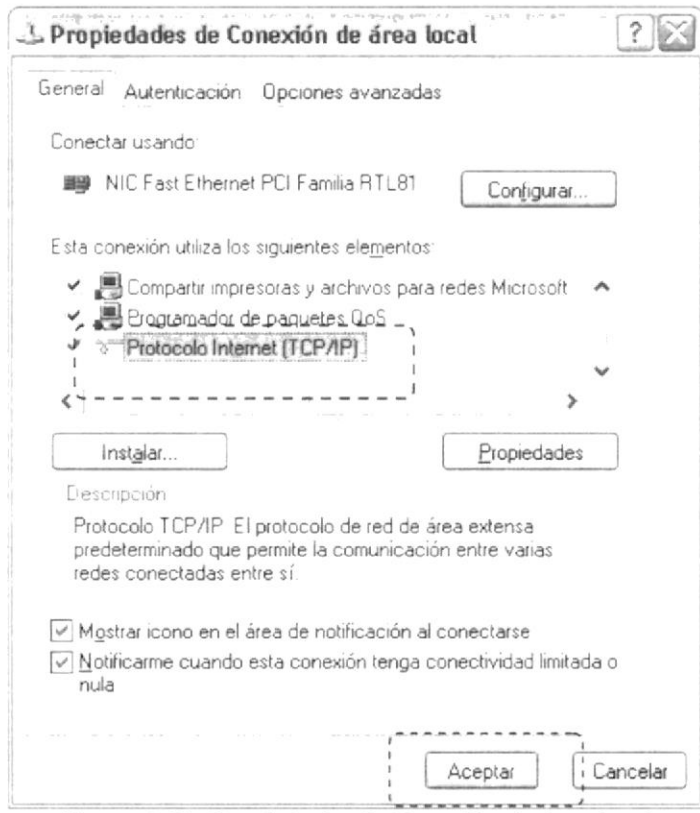


Figura 6-54: Propiedades de Conexión de área local

Habilite **Dirección IP** y **Máscara de subred.**

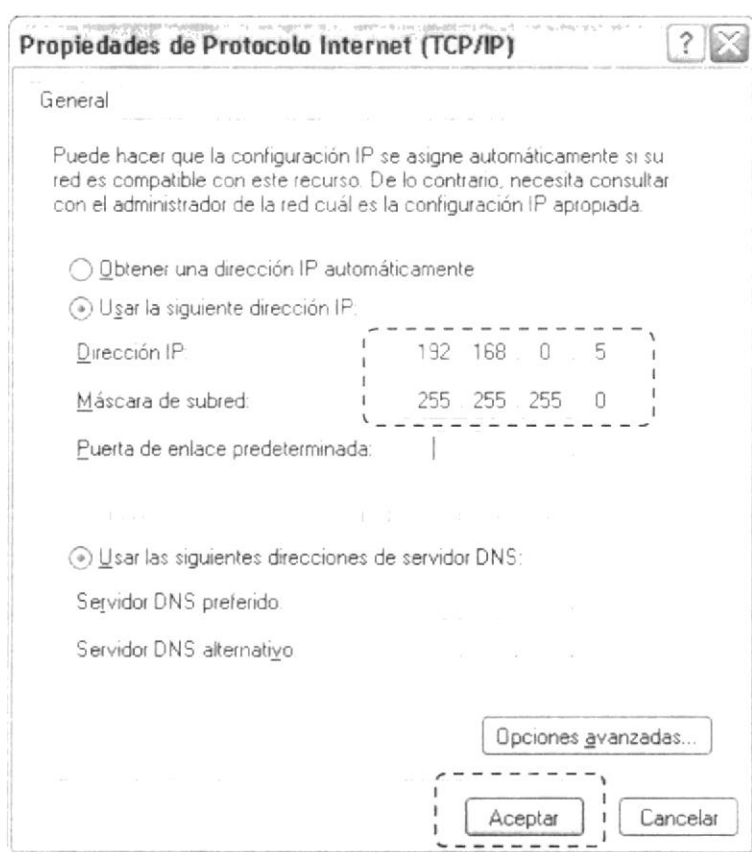


Figura 6-55: Asignando IP en cliente Windows

Luego de clic derecho sobre el icono **Mi PC** y entre en propiedades con clic izquierdo

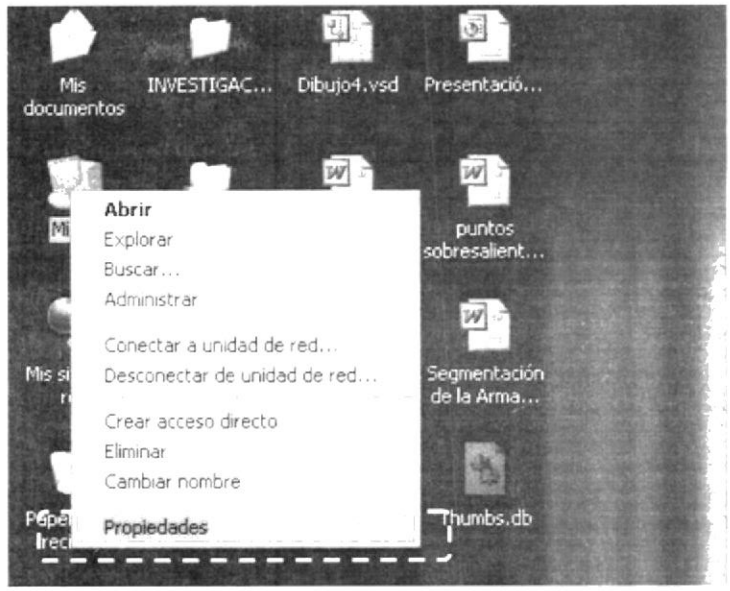


Figura 6-56: Propiedades de Mi PC

Ubíquese en la pestaña **Nombre de Equipo** y de clic en cambiar

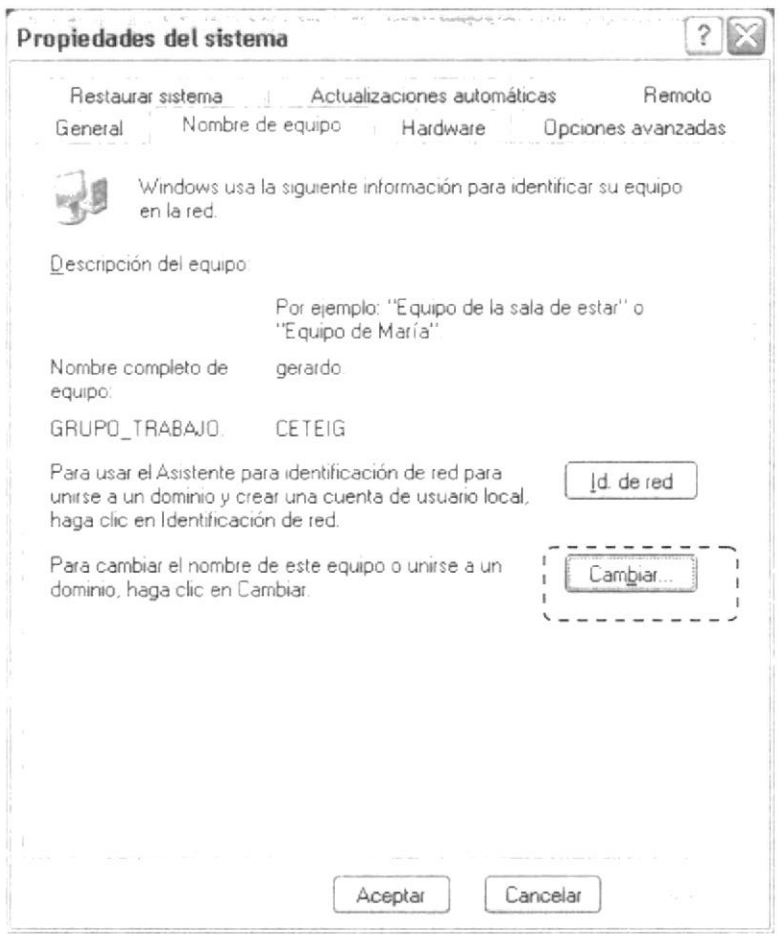


Figura 6-57: Propiedades del Sistema

En el gráfico que se muestra a continuación digite el nombre de grupo en este caso *CETEIG*.

Figura 6-58: Configuración de grupo de trabajo

Acceda a la máquina Linux por medio de la dirección IP, vaya a inicio, se abre el cuadro de diálogo *ejecutar* y ponga la dirección de el servidor en este caso 192.168.0.11.

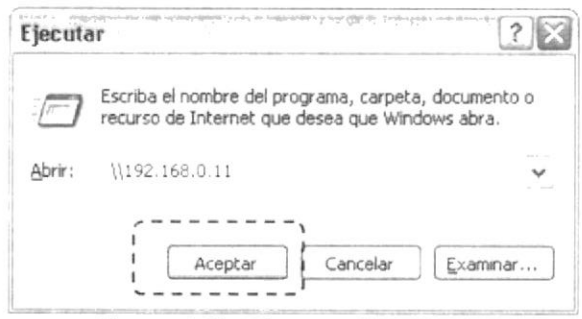


Figura 6-59: Ejecutar dirección IP

Ingrese el usuario al que le dio los permisos en la configuración de samba con su respectivo *password*.

Figura 6-60: Ingresando Usuario y Contraseña

Luego verifique que tenga acceso a los recursos compartidos en nuestro servidor Samba.

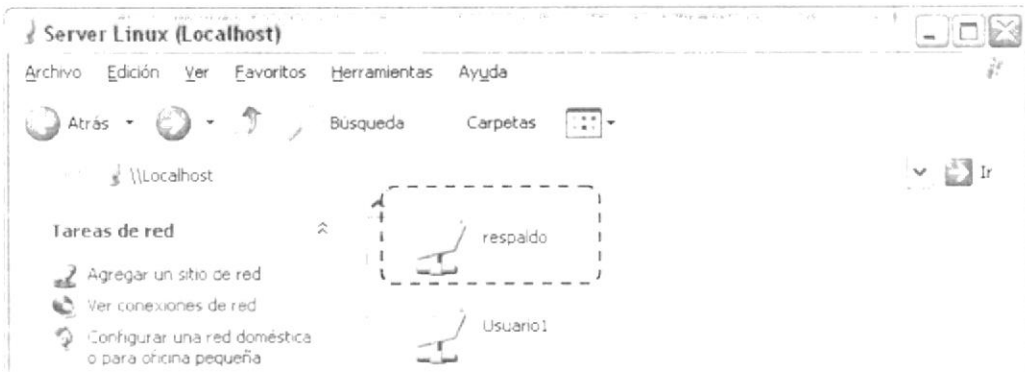


Figura 6-61: Directorio compartido por Samba

Ingrese a la carpeta que dio los permisos en el servidor y encontrará los archivos compartidos.

Figura 6-62: Archivos compartidos por samba

Una vez que pueda abrir sus archivos ha configurado su servidor de samba correctamente.

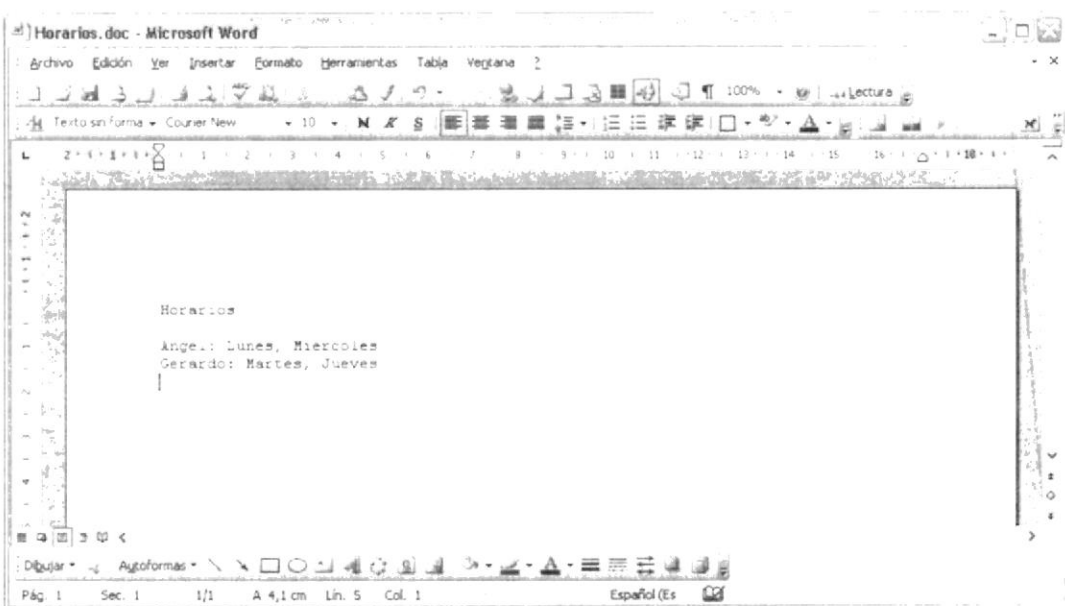


Figura 6-63: Ejecución de archivo compartido por samba

6.20 SERVIDOR DNS

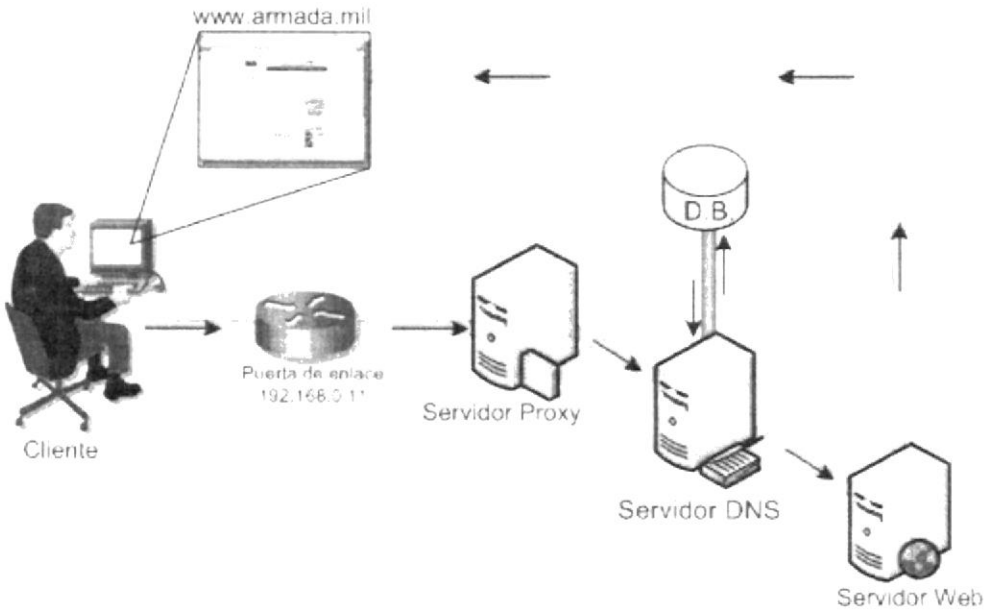


Figura 6-64: Esquema de DNS

DNS (acrónimo de Domain Name System) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombre de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El DNS nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección IP.
Los Servidores DNS utilizan TCP y UDP en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud UDP desde un Cliente DNS seguida por una sola respuesta UDP del servidor. TCP interviene cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como transferencia de zonas.

Componentes de un DNS.
Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

Clientes DNS.
Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

Servidores DNS.
Son servicios que contestan las consultas realizadas por los Clientes DNS. Hay dos tipos de servidores de nombres:

- ✓ Servidor Maestro: También denominado Primario. Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.

- ✓ Servidor Esclavo: También denominado Secundario. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado transferencia de zona.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para las zonas de DNS. De acuerdo al RFC 2182, el DNS requiere que al menos tres servidores existan para todos los dominios delegados (o zonas).
Una de las principales razones para tener al menos tres servidores para cada zona es permitir que la información de la zona misma esté disponible siempre y forma confiable hacia los Clientes DNS a través de Internet cuando un servidor DNS de dicha zona falle, no esté disponible y/o esté inalcanzable.
Contar con múltiples servidores también facilita la propagación de la zona y mejoran la eficiencia del sistema en general al brindar opciones a los Clientes DNS si acaso encontraran dificultades para realizar una consulta en un Servidor DNS. En otras palabras: tener múltiples servidores para una zona permite contar con redundancia y respaldo del servicio.
Con múltiples servidores, por lo general uno actúa como Servidor Maestro o Primario y los demás como Servidores Esclavos o Secundarios. Correctamente configurados y una vez creados los datos para una zona, no será necesario copiarlos a cada Servidor Esclavo o Secundario, pues éste se encargará de transferir los datos de manera automática cuando sea necesario.

Los Servidores DNS responden dos tipos de consultas:

- ✓ Consultas Iterativas (no recursivas): El cliente hace una consulta al Servidor DNS y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al Servidor DNS que tiene la Zona de Autoridad capaz de resolver la consulta.

- ✓ Consultas Recursivas: El Servidor DNS asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el Cliente DNS. El Servidor DNS desarrolla entonces Consultas Iterativas separadas hacia otros Servidores DNS (en lugar de hacerlo el Cliente DNS) para obtener la respuesta solicitada.

Zonas de Autoridad.
Permiten al Servidor Maestro o Primario cargar la información de una zona. Cada Zona de Autoridad abarca al menos un dominio y posiblemente sus sub-dominios, si estos últimos no son delegados a otras zonas de autoridad.
La información de cada Zona de Autoridad es almacenada de forma local en un fichero en el Servidor DNS.

Las zonas que se pueden resolver son:

Zonas de Reenvío.
Devuelven direcciones IP para las búsquedas hechas para nombres FQDN (Fully Qualified Domain Name).
En el caso de dominios públicos, la responsabilidad de que exista una Zona de Autoridad para cada Zona de Reenvío corresponde a la autoridad misma del dominio, es

decir, y por lo general, quien esté registrado como autoridad del dominio tras consultar una base de datos WHOIS. Quienes compran dominios a través de un NIC (por ejemplo: www.nic.mx) son quienes se hacen cargo de las Zonas de Reenvío, ya sea a través de su propio Servidor DNS o bien a través de los Servidores DNS de su ISP.
Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un NIC como requisito para tener derecho legal a utilizarlo y poder propagarlo a través de Internet.

Zonas de Resolución Inversa.
Devuelven nombres FQDN (Fully Qualified Domain Name) para las búsquedas hechas para direcciones IP.
En el caso de segmentos de red públicos, la responsabilidad de que exista de que exista una Zona de Autoridad para cada Zona de Resolución Inversa corresponde a la autoridad misma del segmento, es decir, y por lo general, quien esté registrado como autoridad del segmento tras consultar una base de datos WHOIS.
Los grandes ISP, y en algunos casos algunas empresas, son quienes se hacen cargo de las Zonas de Resolución Inversa.

6.20.1 REQUERIMIENTOS DE CONFIGURACIÓN DNS

- Tener instalado el sistema Linux Fedora Core 3
- Tener una IP estática en el Server Linux
- Tener configurada la tarjeta de red, tanto en el Server Linux como en el cliente.
- Tener instalado el paquete named
- Deshabilitado los firewall (cortafuegos)

Es necesario deshabilitar los firewalls para no tener ningún tipo de restricciones al momento de levantar los servicios, ya que estos usan puertos y protocolos que podrían ser bloqueados por el o los cortafuegos. De esta manera no tendremos ningún tipo de conflicto al realizar nuestra configuración.

6.20.2 CONFIGURACIÓN DNS

Verificar si está instalado el paquete *bind*, digitando el siguiente comando: **[root@armada /] # rpm –q bind**

Proceda a editar el archivo de configuración llamado named de la siguiente manera: **[root@armada /] vi /etc/ named.conf**

En este archivo encontrará todos los dominios ya existentes, edítelo presionando la *i*, y escriba las siguientes líneas:

zone "armada.mil" IN {
type master;
file "armada.mil";
allow-update {none;};
};

Para salir y guardar presione la tecla **esc** y digite **:wq** seguidamente presione la tecla enter.

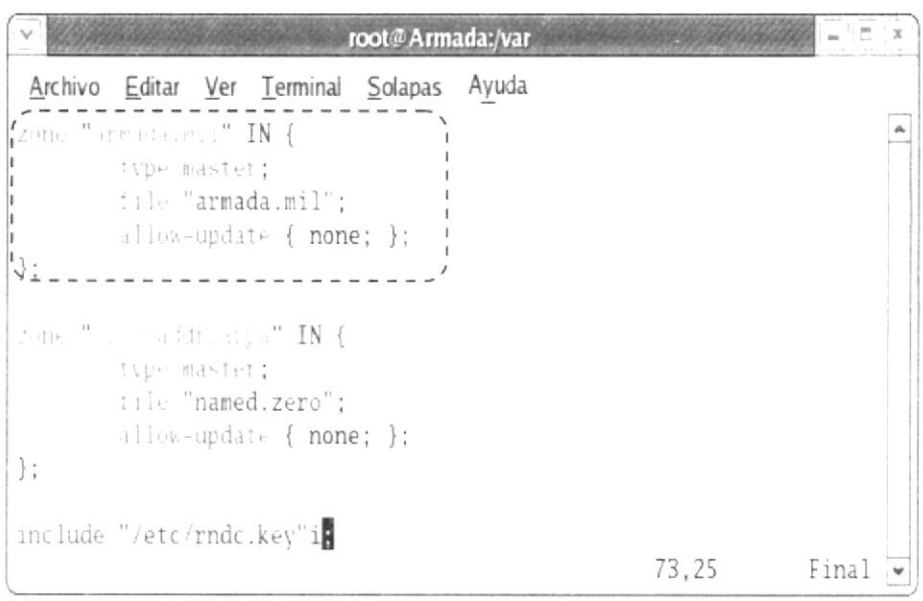


Figura 6-65: Creación de Zona

Zone indicará el nombre completo de la Zona creada.

El campo **type**, indica si se tratará de un servidor principal (*master*) o secundario (*slave*) de la zona.

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

Luego digite la siguiente ruta que permitirá ingresar al archivo named donde creará el dominio.

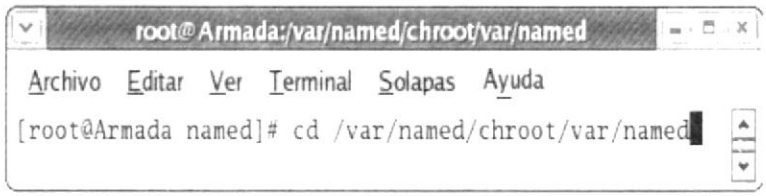


Figura 6-66: Ruta para ingresar al archivo named.conf

Dentro del directorio ***[root@Armada named]#*** proceda a copiar el archivo localhost.zone a uno recién creado (armada.com) digitando el siguiente comando ***cp localhost.zone armada.com.***

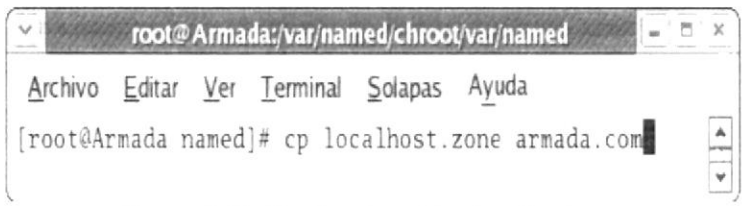


Figura 6-67: Copiar el archivo localhost.zone

Ahora modifique el archivo que copió en este caso armada.com, digitando la siguiente ruta. ***[root@Armada named]# vi armada.mil***

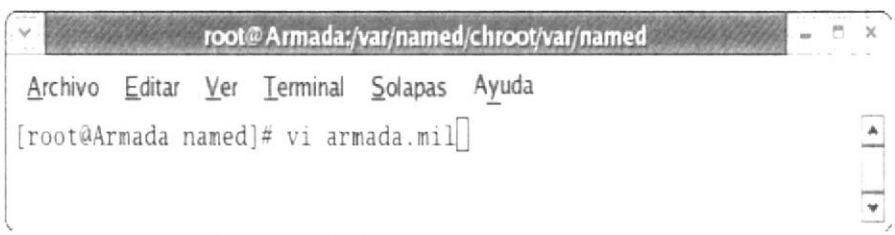


Figura 6-68: Editar el archivo armada.mil

A continuación edite el archivo que copió para su caso armada.mil

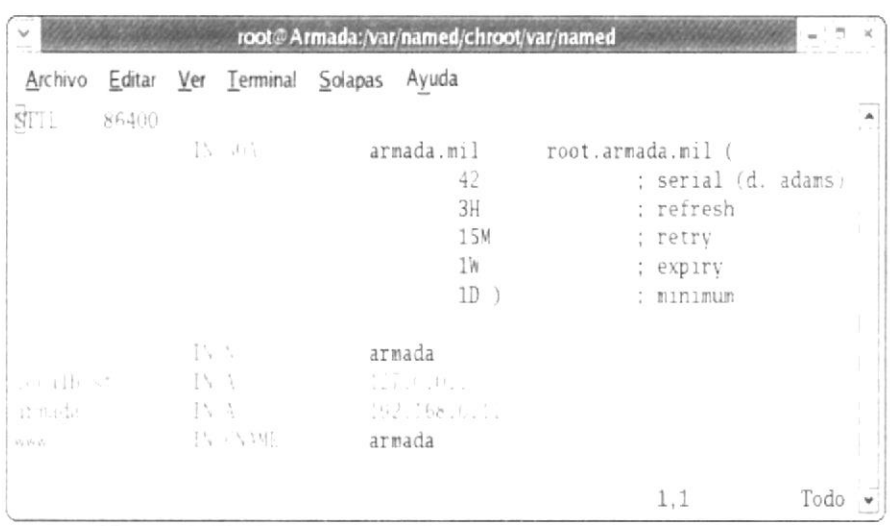


Figura 6-69: Editando y estableciendo el dominio armada.mil

En este archivo encontrará los siguientes registros:

Tipo de Registro.	Descripción.
A (Address)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv4 de 32 bits.
AAAA	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv6 de 128 bits.
CNAME (Canonical Name)	Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los sub-dominios y registros DNS del dominio original.
MX (Mail Exchanger)	Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.
PTR (Pointer)	Registro de apuntador que resuelve direcciones IPv4 hacia el nombre anfitriones. Es decir, hace lo contrario al registro A. Se utiliza en zonas de Resolución Inversa.
NS (Name Server)	Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio.
SOA (Start of Authority)	Registro de inicio de autoridad que especifica el Servidor DNS Maestro (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.
TXT (Text)	Registro de texto que permite al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras DNSBL (DNS-based Blackhole List) para la filtración de Spam. Otro ejemplo de uso son las VPN, donde suele requerirse un registro TXT para definir una llave que será utilizada por los clientes.

Tabla 6-1: Tipos de registro del fichero armada.mil

Personalice su dominio e inicie los servicios del named con el comando que se detalla a continuación: service named start

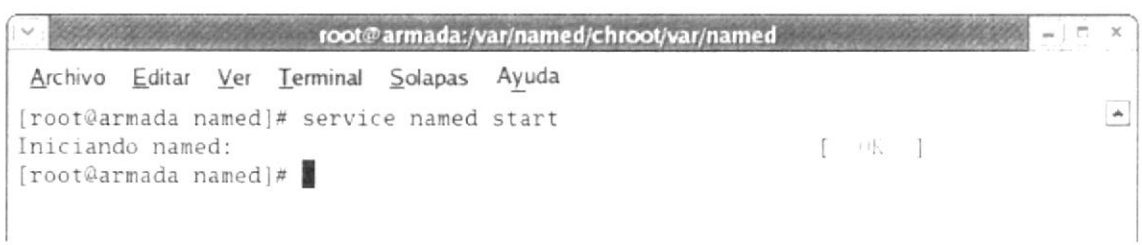


Figura 6-70: Iniciando el servicio de DNS

Lo siguiente probará que esta resolviendo los nombres por IP, haga ping al *DNS* creado.
[root@Armada /] ping www.armada.mil

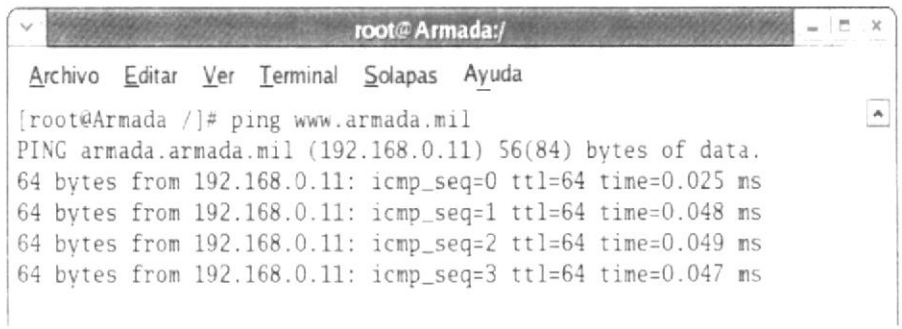


Figura 6-71: Verificando el dominio creado

En caso de que el ping no funcione digite la siguiente ruta: ***[root@Armada /] vi /etc/resolv.conf.*** Ahí encontrará el *NameServer*, y deberá confirmar que la IP sea la misma que la de la tarjeta de red (192.168.0.11).

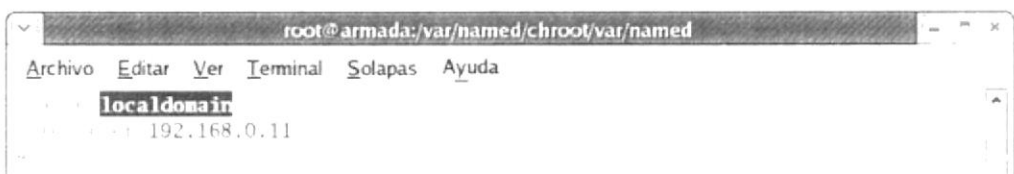


Figura 6-72: Verificación del archivo resolv.conf

6.20.3 CARGAR SERVICIOS DNS AL INICIAR EL SISTEMA

Digite **setup** en la Terminal y habilite el servicio **named** para que se ejecute automáticamente al iniciar Fedora.
Proceda a entrar en servicios del sistema, marcándolo y luego con la tecla tab ubíquese en ejecutar una herramienta y presione la tecla enter.

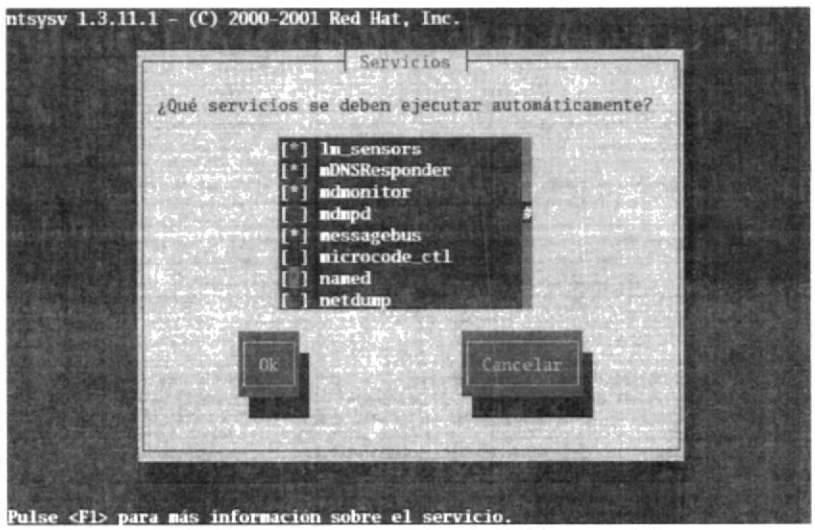


Figura 6-73: Ejecutar los servicios de DNS automáticamente

6.20.4 CONFIGURACIÓN EN CLIENTE WINDOWS

De clic sobre el menú Inicio, entre al Panel de Control, de doble clic en Conexiones de Red y presentará la siguiente pantalla.

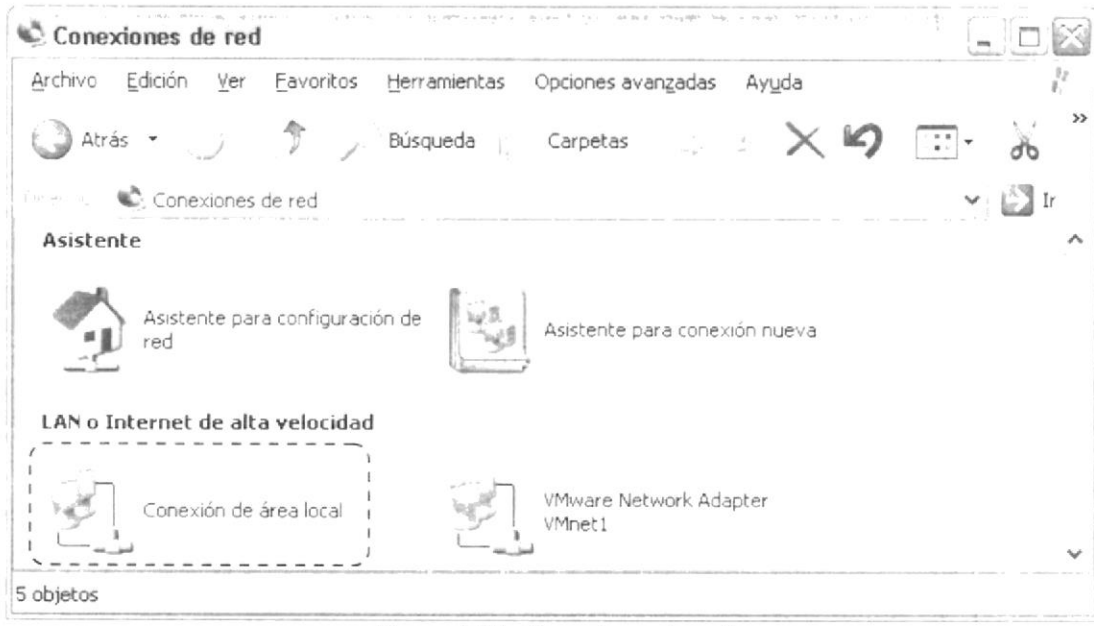


Figura 6-74: Conexiones de red

De doble clic en Conexión de área local y entre a Propiedades

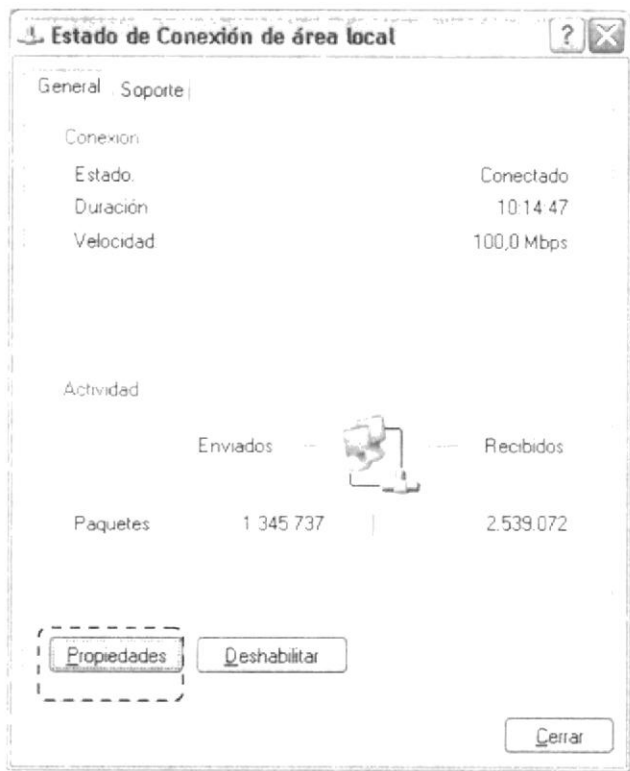


Figura 6-75: Estado de conexión de área local

Ubíquese en Protocolo Internet (TCP/IP) y de clic en Propiedades.

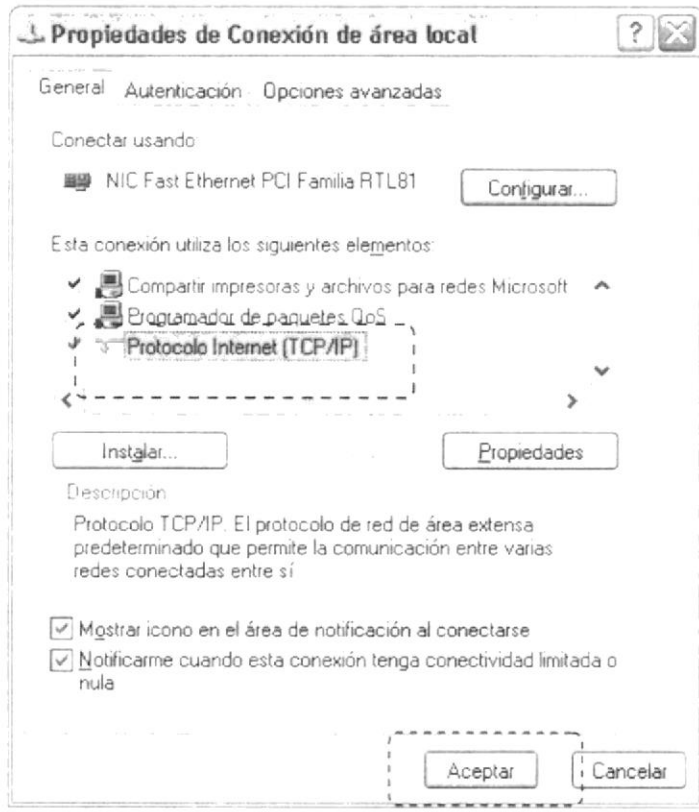


Figura 6-76: Propiedades de Conexión de área local

Habilite **Usar las siguientes direcciones de servidor DNS** y coloque la dirección de IP del Servidor y Acepte.

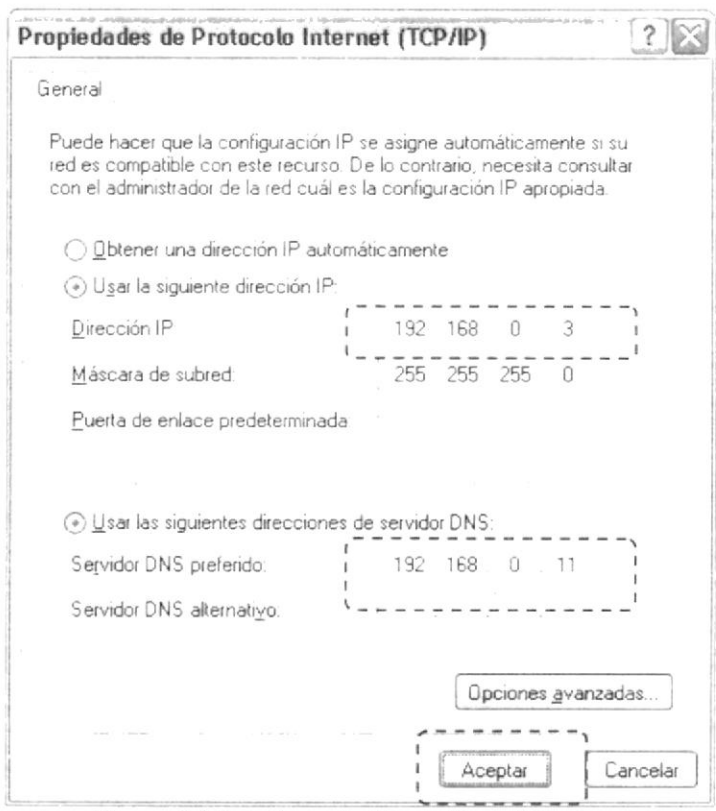


Figura 6-77: Asignando IP en cliente Windows

Una vez que haya procedido a configurar el protocolo **(TCP/IP)** de clic en Inicio y luego clic en Ejecutar.

Figura 6-78: Ingresar a la aplicación Ejecutar

Escriba el comando **ping www.armada.mil** y como resultado muestra la dirección IP del servidor DNS, lo que significa que se encuentra conectado.

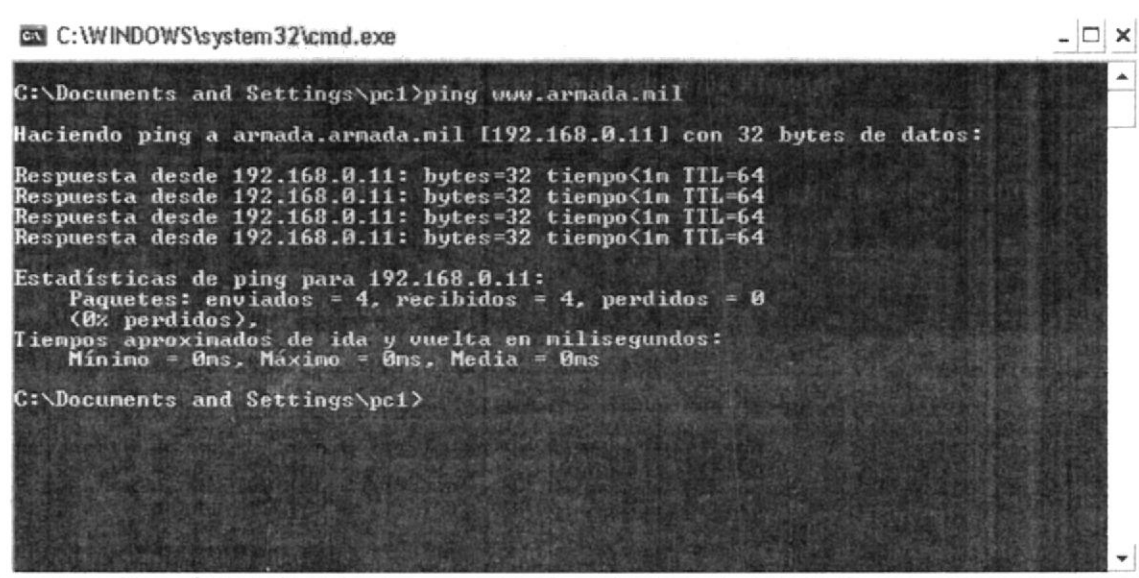


Figura 6-79: Verificando el dominio desde Windows

6.21 SERVIDOR WEB

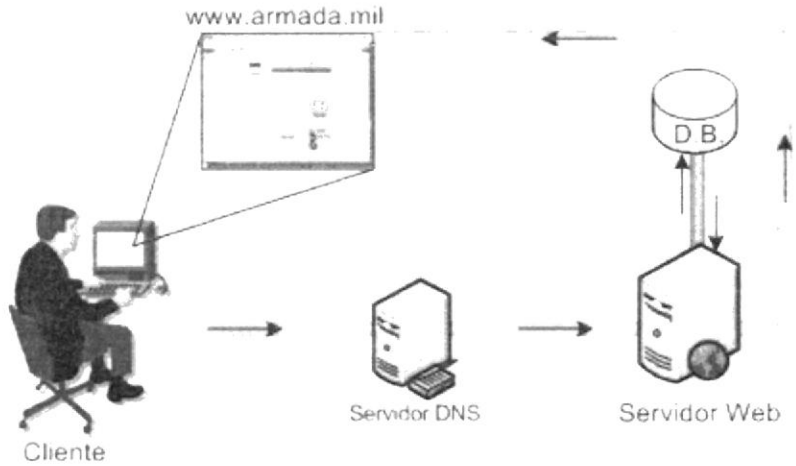


Figura 6-80: Esquema de Servidor Web

Un servidor Web se encarga de mantenerse a la espera de peticiones HTTP llevada a cabo por un cliente HTTP que solemos conocer como navegador. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. A modo de ejemplo, al teclear www.ejemplo.org en nuestro navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo muestra en pantalla. Como vemos con este ejemplo, el cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Acerca del protocolo HTTP.

HTTP (Hypertext Transfer Protocol, o Protocolo de Transferencia de Hipertext), es el método utilizado para transferir o transportar información en la Red Mundial (WWW, World Wide Web). Su propósito original fue el proveer una forma de publicar y recuperar documentos HTML.

El desarrollo del protocolo fue coordinado por World Wide Web Consortium y la IETF (Internet Engineering Task Force, o Fuerza de Trabajo en Ingeniería de Internet), culminando con la publicación de varios RFC (Request For Comments), de entre los que destaca el RFC 2616, mismo que define la versión 1.1 del protocolo, que es el utilizado hoy en día.

HTTP es un protocolo de solicitud y respuesta a través de TCP, entre agentes de usuarios (Navegadores, motores de índice y otras herramientas) y servidores, regularmente utilizando el puerto 80. Entre la comunicación entre éstos puede intervenir como servidores Intermediarios (Proxies), puertas de enlace y túneles.

Sobre el servicio Web clásico podemos disponer de aplicaciones Web. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- ✓ Aplicaciones en el lado del cliente: el cliente Web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java o Javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un

navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Normalmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje javascript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins

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

Acerca de Apache.
El servidor HTTP Apache es un software (libre) servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 [1] y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que originalmente Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. Era, en inglés, a patchy server (un servidor "parcheado").
El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.
Apache presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.
Apache tiene amplia aceptación en la red: en el 2005, Apache es el servidor HTTP más usado, siendo el servidor HTTP del 70% de los sitios Web en el mundo y creciendo aún su cuota de mercado (estadísticas históricas y de uso diario proporcionadas por Netcraft).La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas puede en la mayoría de los casos ser abusada solamente por los usuarios locales y no puede ser accionada remotamente. Sin embargo, algunas de las ediciones antedichas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache. Por lo tanto, aconsejamos fuertemente a todos los usuarios de PHP, sin importar la versión a aumentar a los 5.2.1 o 4.4.5 lanzamientos cuanto antes. Para los usuarios que aumentan a PHP 5.2 de PHP 5.0 y de PHP 5.1, una guía de la mejora está disponible aquí, detallando los cambios entre esos lanzamientos y PHP 5.2.1.

6.21.1 REQUERIMIENTOS DE CONFIGURACIÓN WEB SERVER

- Tener instalado el sistema Linux Fedora Core 3
- Tener una IP estática en el Server Linux
- Tener configurada la tarjeta de red, tanto en el Server Linux como en el cliente.
- Tener instalado el paquete httpd
- Tener instalado, configurado y activo el servidor DNS
- Deshabilitado los firewall (cortafuegos)

Es necesario deshabilitar los firewalls para no tener ningún tipo de restricciones al momento de levantar los servicios, ya que estos usan puertos y protocolos que podrían ser bloqueados por el o los cortafuegos. De esta manera no tendremos ningún tipo de conflicto al realizar nuestra configuración.

6.21.2 CONFIGURACIÓN WEB SERVER

Verifique si está instalado el paquete *httpd*, de la siguiente manera:
[root@armada /] # rpm –q httpd

Proceda a editar el archivo de configuración llamado httpd de la siguiente manera:
[root@armada /] # vi /etc/httpd/conf/httpd.conf

En el editor proceda a modificar las siguientes líneas:
Descomente para que pueda escuchar el servidor por el puerto 80

Figura 6-81: Configuración de puerto a escuchar

DocumentRoot: Esta línea es la ubicación donde estará el directorio que almacena la página Web

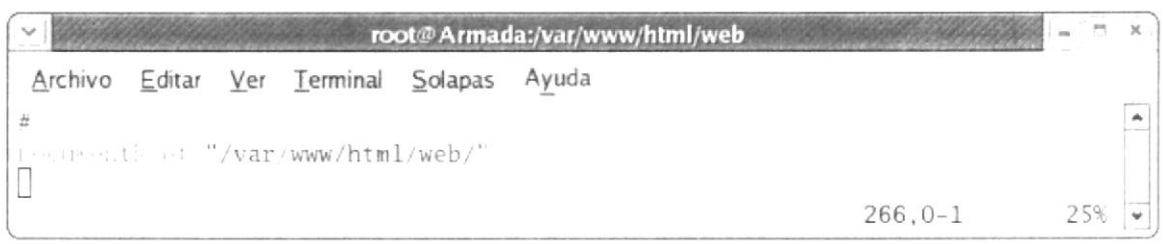


Figura 6-82: Configuración de Directorio Web

DirectoryIndex: Aquí describa el nombre del archivo con su respectiva extensión

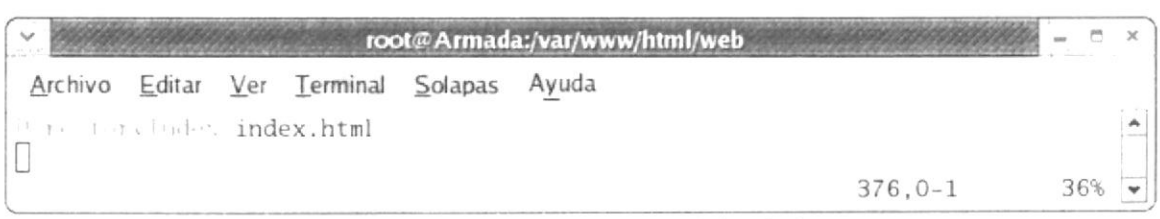


Figura 6-83: Configuración de página Index

Ubíquese en la parte final del archivo y encontrará esta sección que procederá a copiarla más abajo y descomentará las opciones mostradas en la imagen.

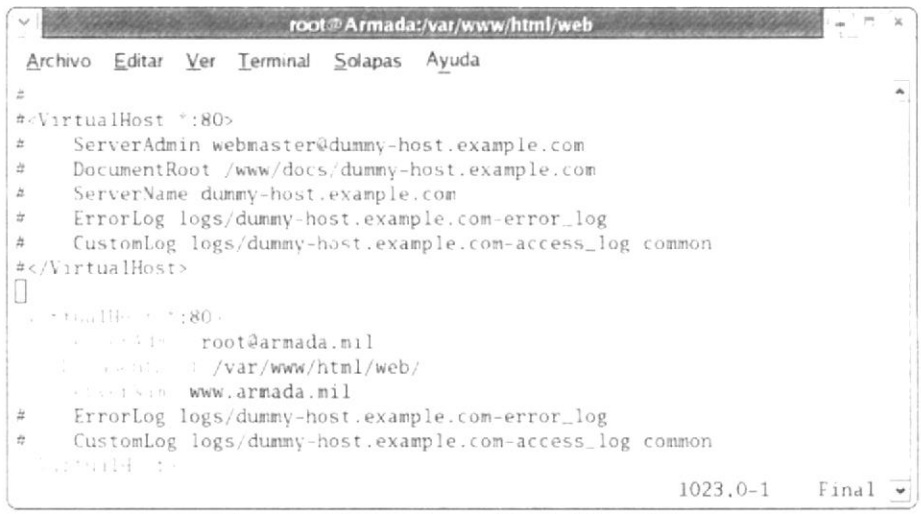


Figura 6-84: Configuración de Virtual Host

Donde especificará:
ServerAdmin : Especifica que cuenta administra el servidor
DocumentRoot: Se detalla la ruta donde se guardarán las páginas
ServerName : El nombre del servidor de DNS

Ubíquese en la ruta donde especificó que se encontrará el documento y proceda a crear la carpeta que contendrá el archivo:

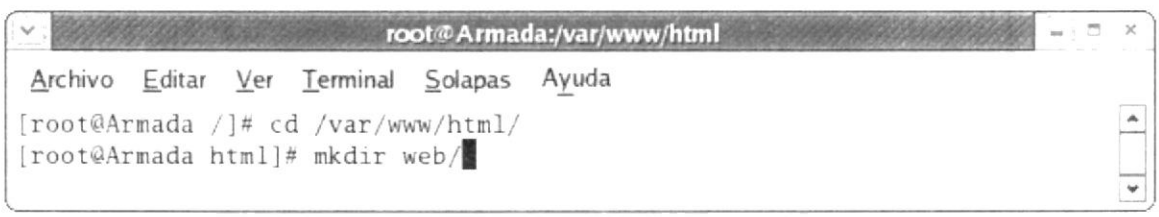


Figura 6-85: Creación de directorio Web

Ingrese a la carpeta creada y cree un nuevo archivo que servirá de prueba denominado de igual forma como antes lo detalló:

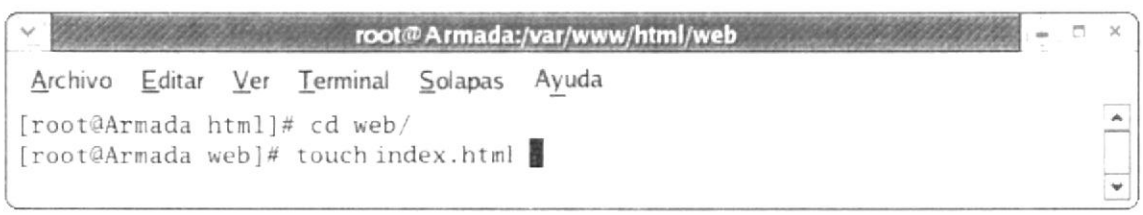


Figura 6-86: Creación de página Index

Para editarlo ponemos: **vi index.html**

Por cuestiones de ejemplo digite la siguiente leyenda. PAGINA WEB DE PRUEBA
Para salir y grabar presione la tecla **ESC** y digite **:wq** seguidamente presione la tecla enter.

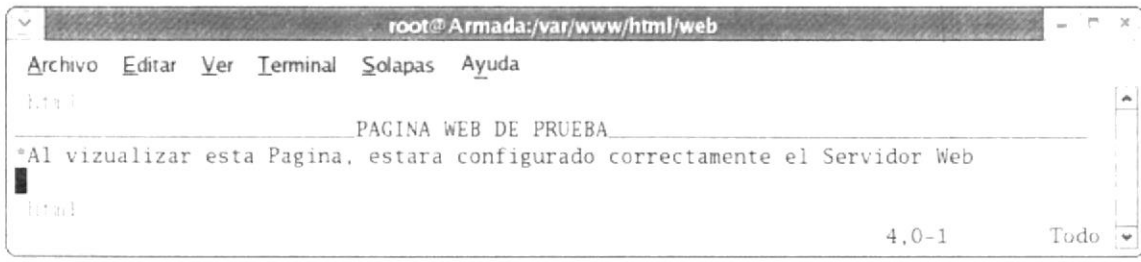


Figura 6-87: Editando página Index

Creado el archivo html proceda a iniciar el servicio del servidor http.

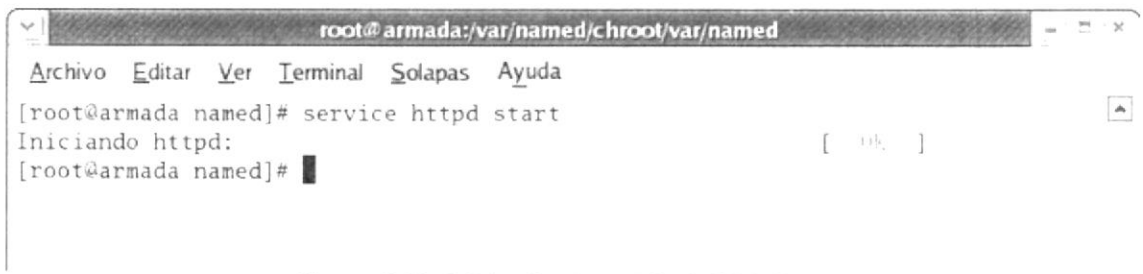


Figura 6-88: Iniciando el servicio de Web Server

Reiniciados los servicios, diríjase al navegador preferido en LINUX y en la barra de direcciones digite la página: www.armada.mil.

En este caso se pondrá una página ya desarrollada. Para probarla en el navegador, abra el Mozilla Firefox y vaya a Edit – Preferencies – General – Conexión Settings
Y habilite la opción **Direct connection to the Internet**

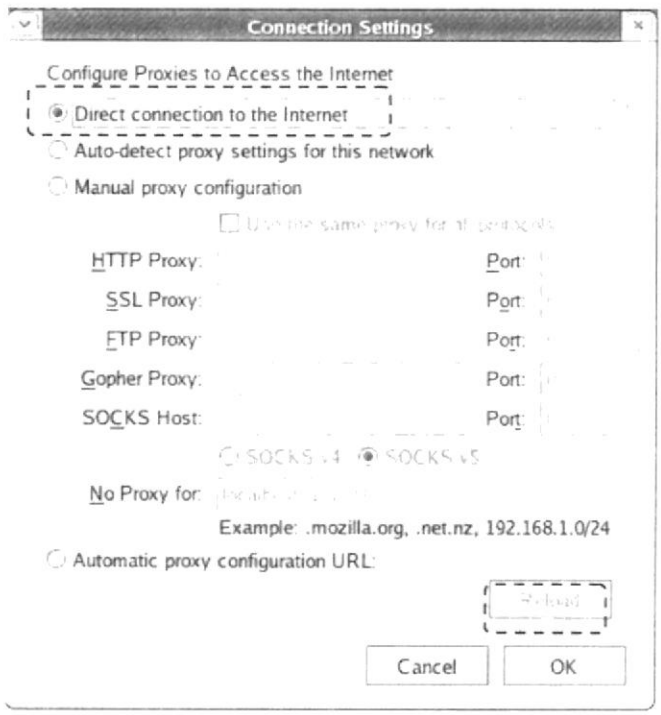


Figura 6-89: Configuración de conexión en Firefox

Digite www.armada.mil y aparecerá el sitio Web

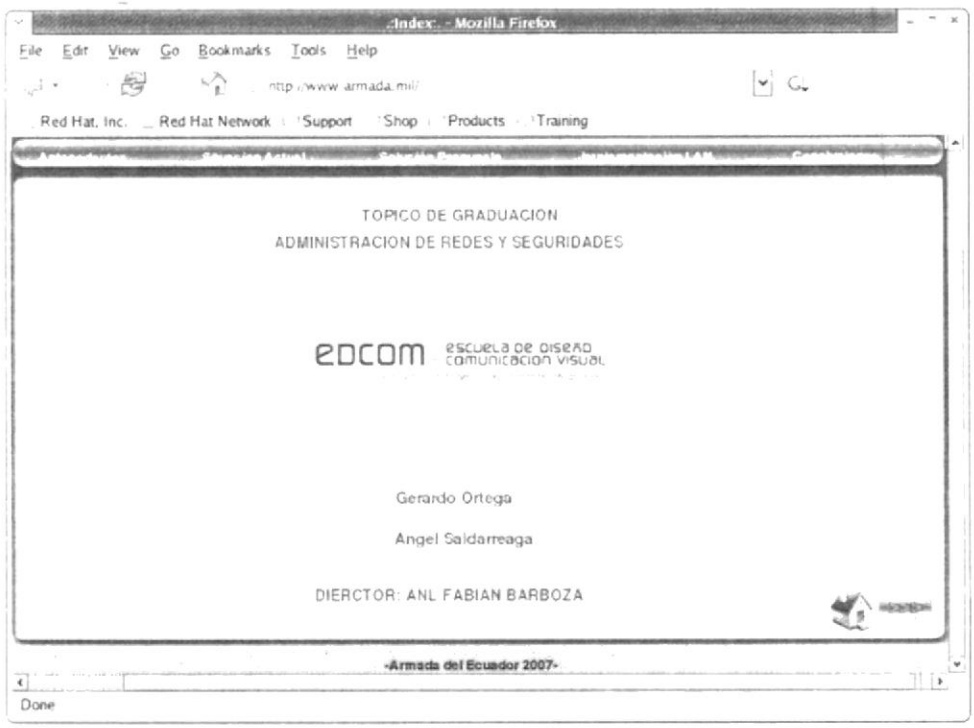


Figura 6-90: Presentación de Página Web en Firefox

6.21.3 CARGAR SERVICIOS WEB SERVER AL INICIAR EL SISTEMA

Digite **setup** en la Terminal y habilite el servicio **httpd** para que se ejecute automáticamente al iniciar Fedora.
Proceda a entrar en servicios del sistema. marcándolo y luego con la tecla tab ubíquese en ejecutar una herramienta y presione la tecla enter.

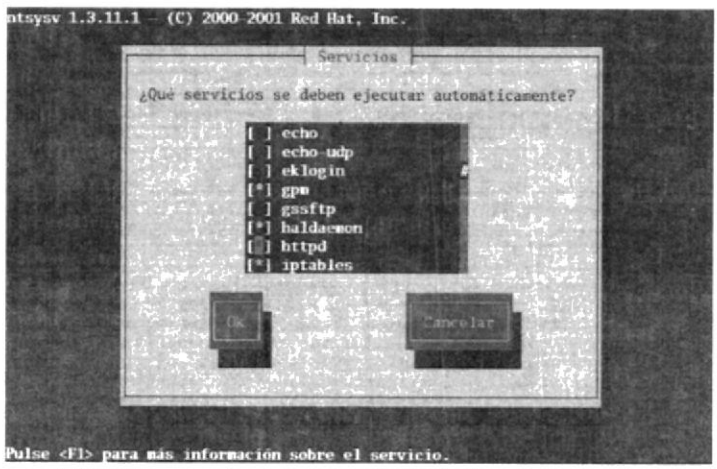


Figura 6-91: Ejecutar los servicios de Web Server automáticamente

6.21.4 CONFIGURACIÓN EN CLIENTE WINDOWS

De clic sobre el menú Inicio, entre al Panel de Control, de doble clic en Conexiones de Red y presentará la siguiente pantalla.

Figura 6-92: Conexiones de red

De doble clic en Conexión de área local y entre a Propiedades

Figura 6-93: Estado de conexión de área local

Ubíquese en Protocolo Internet (TCP/IP) y de clic en Propiedades

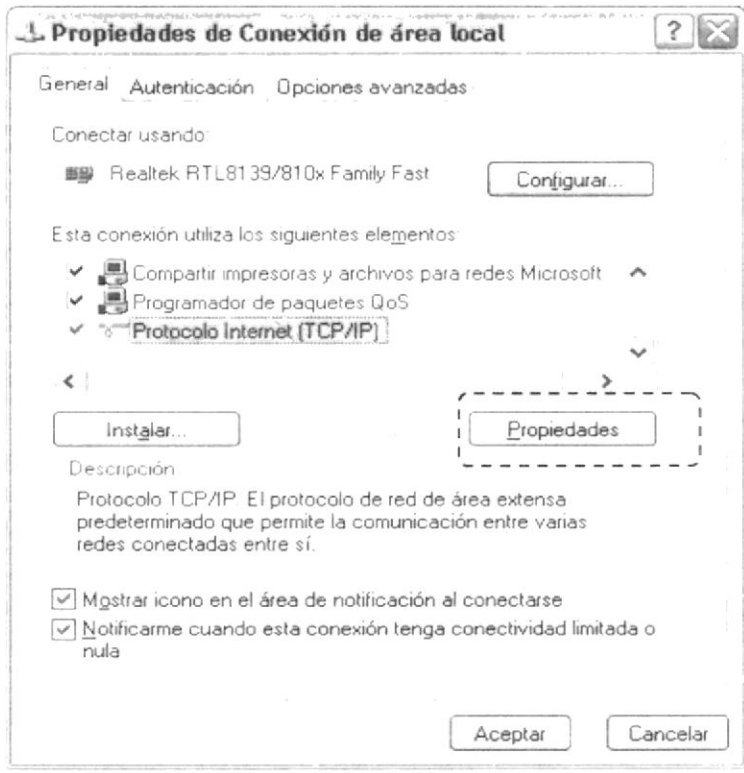


Figura 6-94: Propiedades de Conexión de área local

Habilite usar las siguientes direcciones del servidor DNS y coloque la dirección de IP del Servidor en Puerta de enlace y Acepte.

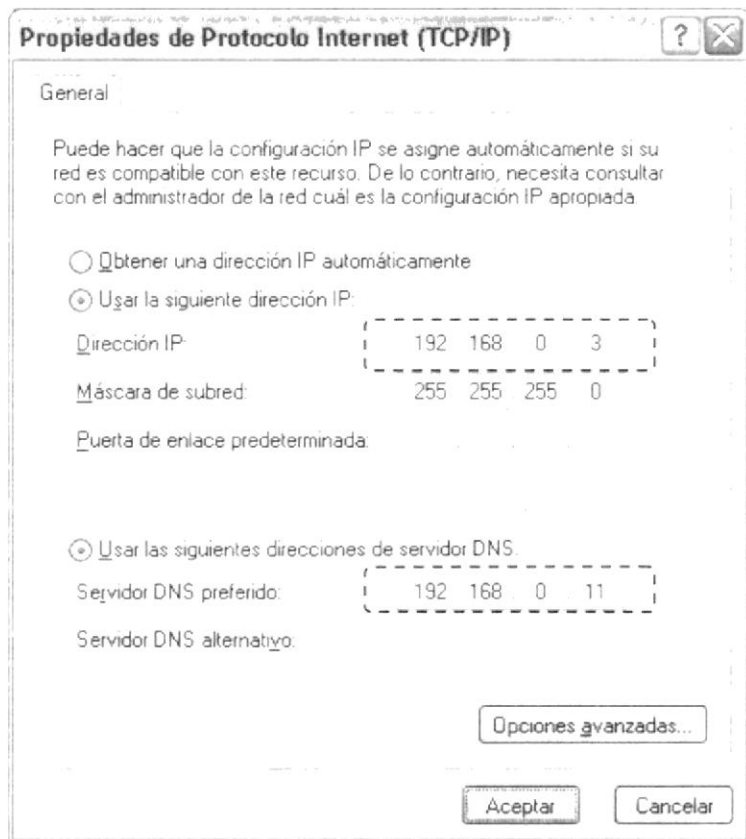


Figura 6-95: Asignando IP en cliente Windows

Una vez realizadas estas configuraciones en las propiedades del Protocolo Internet, abra el navegador, vaya al menú Herramientas – Opciones de Internet – Conexiones – Configuración de área local y marque la opción Detectar la configuración automáticamente.
Esto lo hará para que la conexión el Web Server sea directa.

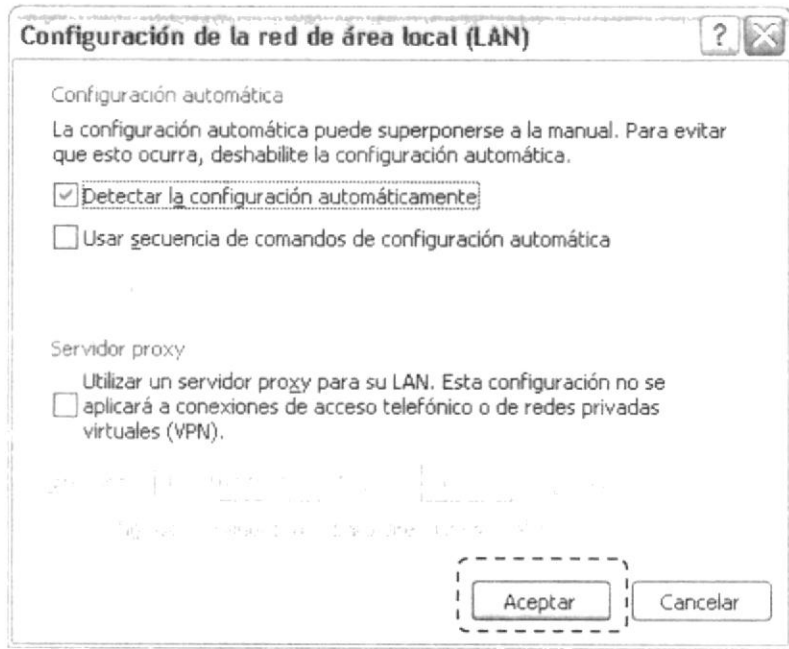


Figura 6-96: Configuración de conexión en Internet Explorer

Acepte y digite en la barra de direcciones la página Web creada: www.armada.mil seguidamente presione la tecla enter.

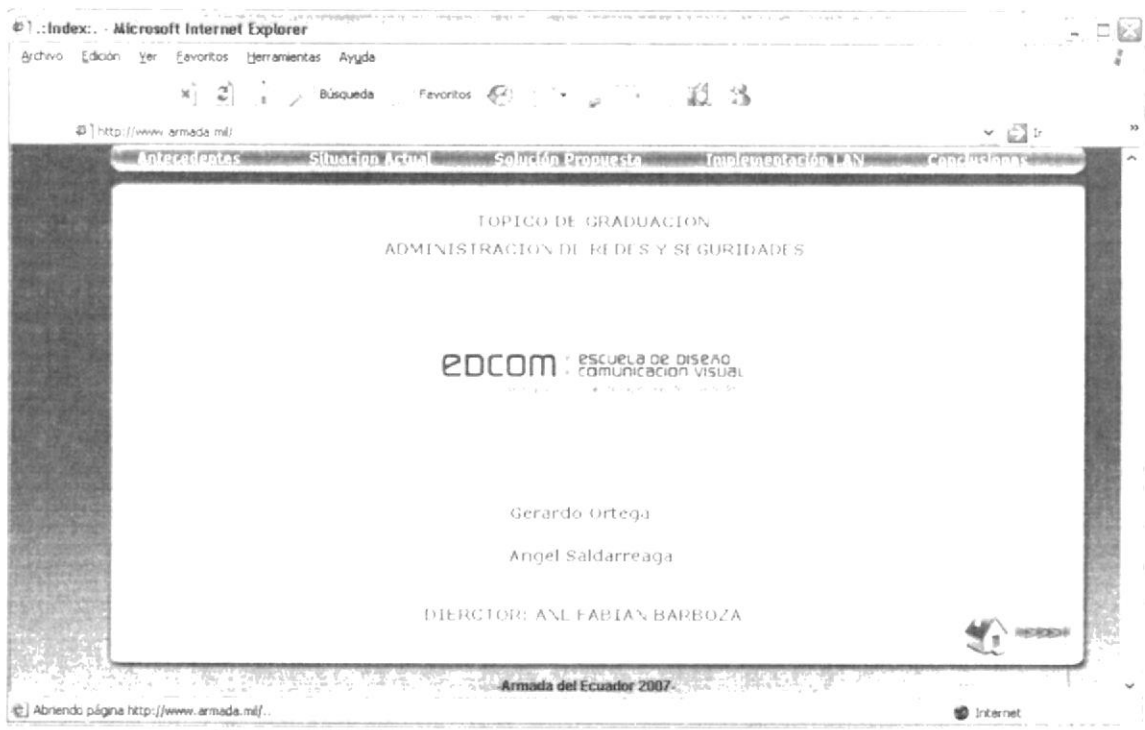


Figura 6-97: Presentación de Página Web en Internet Explorer

6.22 SERVIDOR PROXY

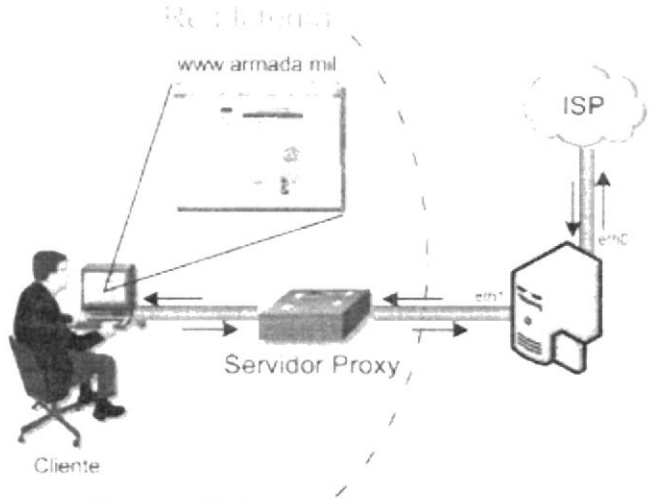


Figura 6-98: Diagrama de Servidor Proxy

Un 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 por ejemplo: una página Web en una caché que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de Proxy se agrupan diversas técnicas.

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

Durante el proceso de brindar el servicio ocurre lo siguiente:

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

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

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

Cuando se recibe una petición para un recurso de Red especificado en un URL (Uniform Resource Locator) el Servidor Intermediario busca el resultado del URL dentro del caché. Si éste es encontrado, el Servidor Intermediario responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el Servidor Intermediario lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de respuestas a solicitudes (hits) (ejemplos: LRU, LFUDA y GDSF).
Los Servidores Intermediarios para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

Características de Proxy en Linux:

- ✓ Proxy y Caché de HTTP, FTP, y otras URLs
- ✓ Proxy para SSL
- ✓ Jerarquías de Caché
- ✓ ICP, HTCP, CARP, Caché Digests
- ✓ Caché transparente
- ✓ Control de acceso
- ✓ Aceleración de servidores HTTP
- ✓ SNMP
- ✓ Caché de resolución DNS

Acerca de Squid.
Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo sustento lógico libre, está disponible el código fuente para quien así lo requiera.
Entre otras cosas, Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL,

caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.
Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes. Al iniciar Squid da origen a un número configurable (5, de modo predefinido a través del parámetro dns_children) de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores DNS.

Ventajas de Proxy
Este suele tener lo que denominamos una caché, con una copia de las páginas Web que se van visitando. Entonces, si varias personas que acceden a Internet a través del mismo Proxy acceden al primer sitio Web, el Proxy la primera vez accede físicamente al servidor destino, solicita la página y la guarda en la caché, además de enviarla al usuario que la ha solicitado. En sucesivos accesos a la misma información por distintos usuarios, el Proxy sólo comprueba si la página solicitada se encuentra en la caché y no ha sido modificada desde la última solicitud. En ese caso, en lugar de solicitar de nuevo la página al servidor, envía al usuario la copia que tiene en la caché. Esto mejora el rendimiento o velocidad de la conexión a Internet de los equipos que están detrás del Proxy.

Desventajas de Proxy
Tenemos la posibilidad de recibir contenidos que no están actualizados, tener que gestionar muchas conexiones y resultar un cuello de botella, o el abuso por personas que deseen navegar anónimamente. También el Proxy puede ser un limitador, por no dejar acceder a través suyo a ciertos protocolos o puertos.

6.22.1 REQUERIMIENTOS DE CONFIGURACIÓN PROXY

- Tener instalado el sistema Linux Fedora Core 3
- Tener una IP estática en el Server Linux
- Tener configurada la tarjeta de red, tanto en el Server Linux como en el cliente.
- Tener instalado el paquete de squid
- Deshabilitado los firewall (cortafuegos)

Es necesario deshabilitar los firewalls para no tener ningún tipo de restricciones al momento de levantar los servicios, ya que estos usan puertos y protocolos que podrían ser bloqueados por el o los cortafuegos. De esta manera no tendremos ningún tipo de conflicto al realizar nuestra configuración.

Tómese en consideración que, de ser posible, se debe utilizar siempre las versiones estables más recientes de todo el software que vaya a instalar, a fin de contar con los parches de seguridad necesarios. Ninguna versión de Squid anterior a la 2.5.STABLE1 se considera como apropiada debido a fallas de seguridad de gran importancia, y ningún administrador competente utilizaría una versión inferior a la 2.5.STABLE1.

6.22.2 CONFIGURACIÓN PROXY

Verifique si está instalado el paquete *squid*, de la siguiente manera:
[root@armada /] # rpm –q squid

Proceda a editar el archivo de configuración llamado squid de la siguiente manera:
[root@armada /] # vi /etc/squid/squid.conf

Parámetro http_port
Squid por defecto utilizará el puerto 3128 para atender peticiones, pero se puede especificar que lo haga en otro puerto o bien que lo haga en varios puertos a la vez.
En el caso de un Proxy Transparente, regularmente se utilizará el puerto 80 y se valdrá del redireccionamiento de peticiones de modo tal que no habrá necesidad alguna de modificar la configuración de los navegadores Web para utilizar el servidor Proxy, bastará con utilizar como puerta de enlace al servidor. Es importante recordar que los servidores Web, como Apache, también utilizan dicho puerto, por lo que será necesario reconfigurar el servidor Web para utilizar otro puerto disponible, o bien desinstalar o deshabilitar el servidor Web.
Regularmente algunos programas utilizados comúnmente por los usuarios suelen traer por defecto el puerto 8080 -servicio de cacheo www-.
Descomente esta línea y coloque el puerto 8080.

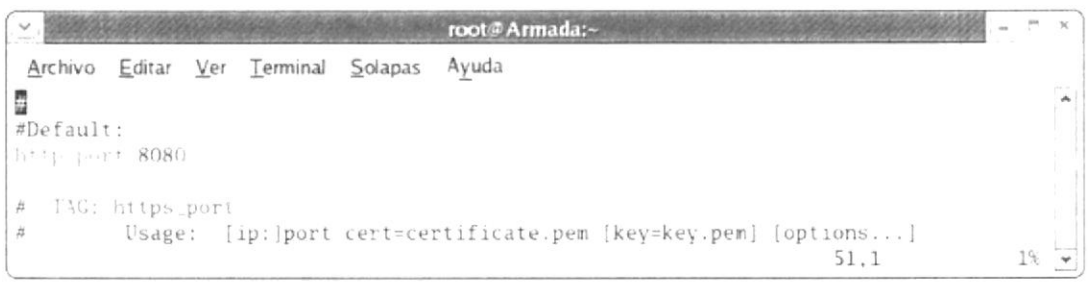


Figura 6-99: Configurando http_port

Parámetro cache_mem
El parámetro cache_men establece la cantidad ideal de memoria para lo siguiente:

- ✓ Objetos en tránsito.
- ✓ Objetos Hot.
- ✓ Objetos negativamente almacenados en el caché.

Los datos de estos objetos se almacenan en bloques de 4 Kb. El parámetro cache_mem especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Coloque 16MB

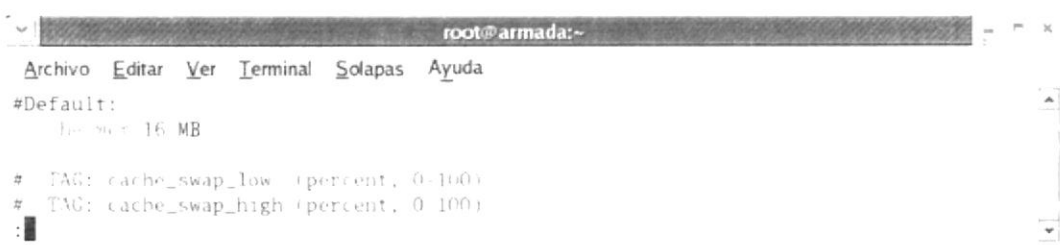


Figura 6-100: Configurando cache_mem

Parámetro cache_dir

Este parámetro se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid. Para entender esto un poco mejor, responda a esta pregunta: ¿Cuanto desea almacenar de Internet en el disco duro? Por defecto Squid utilizará un caché de 100 MB, de modo tal que encontrará la siguiente línea:

cache_dir ufs /var/spool/squid 100 16 256

Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande el caché, más objetos de almacenarán en éste y por lo tanto se utilizará menos el ancho de banda.

Los números 16 y 256 significan que el directorio del caché contendrá 16 subdirectorios con 256 niveles cada uno. No modifique esto números, no hay necesidad de hacerlo.

Es muy importante considerar que si se especifica un determinado tamaño de caché y este excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente. Sea cauteloso con el tamaño de caché especificado.

Descomente esta línea y deje el valor por defecto

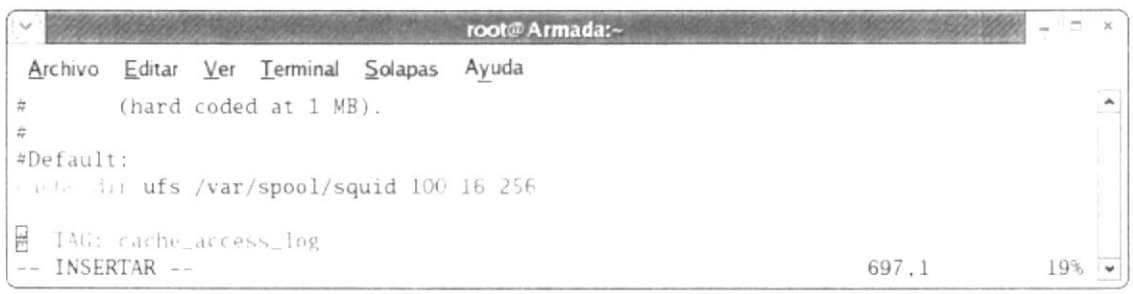


Figura 6-101: Configurando cache_dir

Parámetro cache_access_log

Este parámetro sirve para monitorear la actividad de los hosts que tiene a cargo el servidor Proxy. Proceda a descomentar esta línea

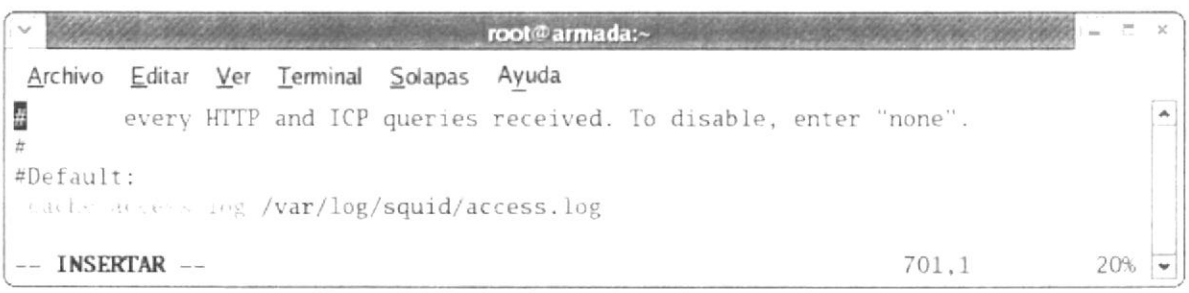


Figura 6-102: Configurando cache_access_log

Listas de Control de Acceso

Es necesario establecer Listas de Control de Acceso que definan una red o bien ciertas máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.

Regularmente una lista de control de acceso se establece siguiendo la siguiente sintaxis:
acl [**nombre de la lista**] src [**lo que compone a la lista**]

Aumente las siguientes líneas:
acl CETEIG src 192.168.0.11/255.255.255.0
acl puerto myport 8080
En la cual esta definiendo a CETEIG en un rango de 254 IP disponibles
En la segunda acl declare el puerto 8080

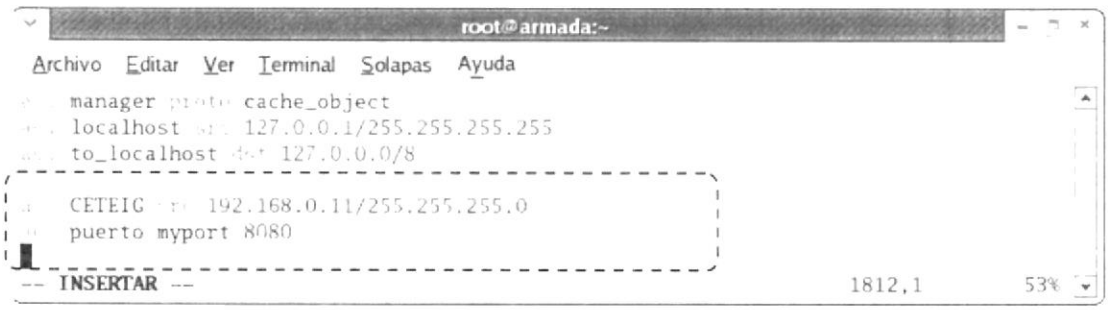


Figura 6-103: Estableciendo ACL's

Luego aplique las reglas para permitir o denegar el acceso a Squid. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

La sintaxis básica es la siguiente:
http_access [**allow**] [**lista de control de acceso**]
Aumente la siguiente línea:
http_access allow CETEIG puerto
La cual significa que esta dando acceso a todo el rango de IP's de CETEIG a través del puerto 8080.

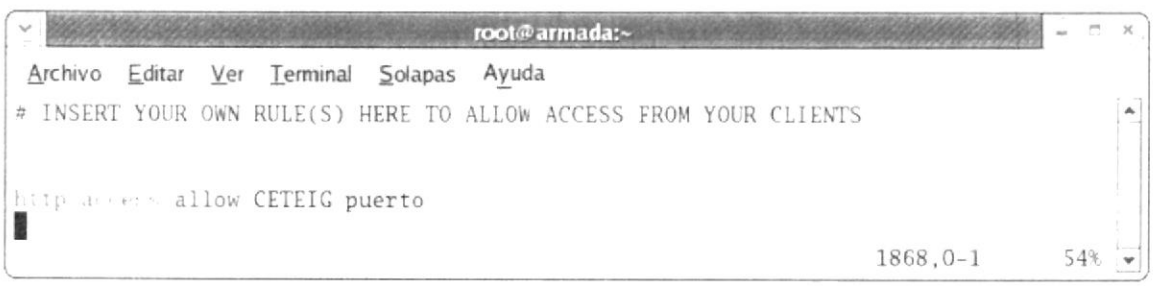


Figura 6-104: Definiendo regla para ACL

Proceda a iniciar el squid con el siguiente comando: service squid start

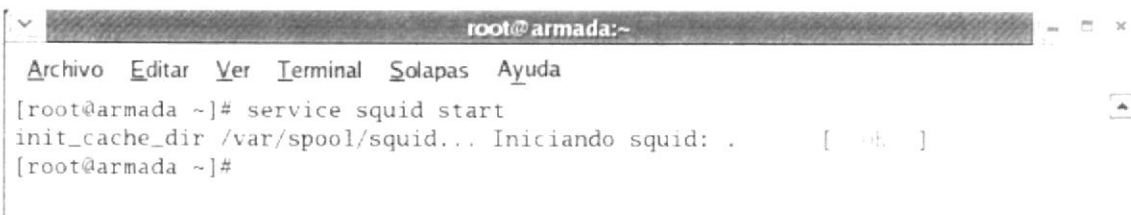


Figura 6-105: Iniciando el servicio de Proxy

6.22.3 CARGAR SERVICIOS PROXY AL INICIAR EL SISTEMA

Digite **setup** en la Terminal y habilite el servicio **squid** para que se ejecute automáticamente al iniciar Fedora.
Proceda a entrar en servicios del sistema, marcándolo y luego con la tecla tab ubíquese en ejecutar una herramienta y presione la tecla enter.

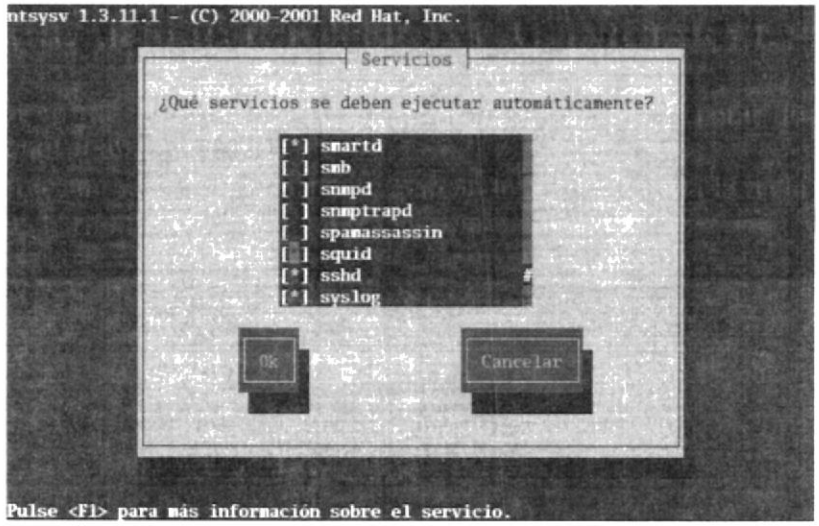


Figura 6-106: Ejecutar el servicio de Proxy automáticamente

6.22.4 CONFIGURACIÓN EN CLIENTE WINDOWS

De clic sobre el menú Inicio, entre al Panel de Control, de doble clic en Conexiones de Red y presentará la siguiente pantalla.

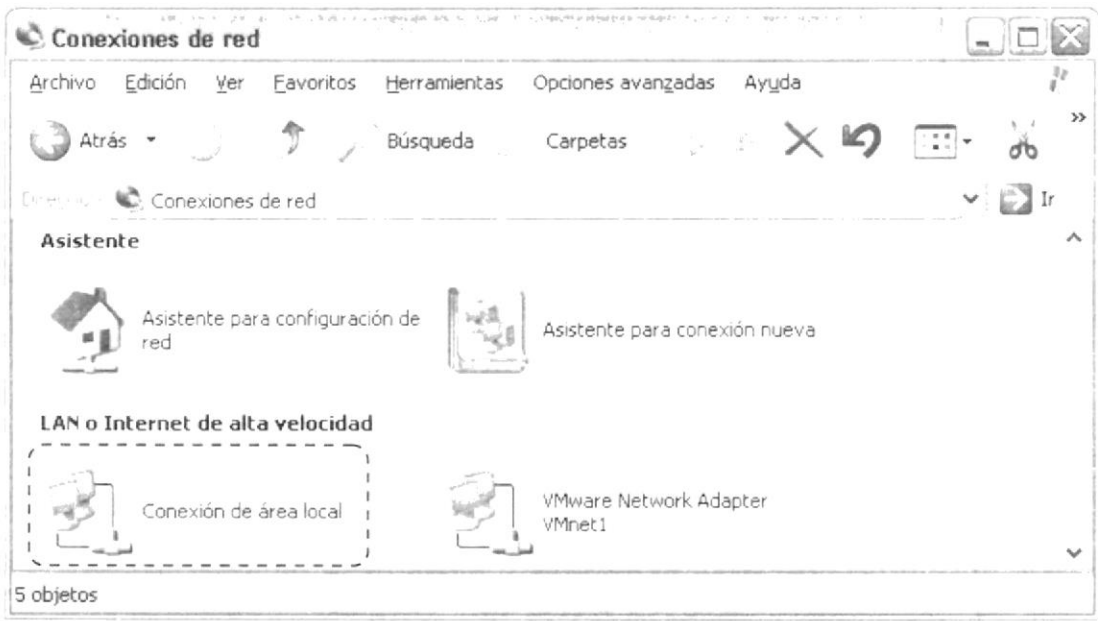


Figura 6-107: Conexiones de red

De doble clic en Conexión de área local y entre a Propiedades

Figura 6-108: Estado de Conexión de área local

Ubíquese en Protocolo Internet (TCP/IP) y de clic en Propiedades

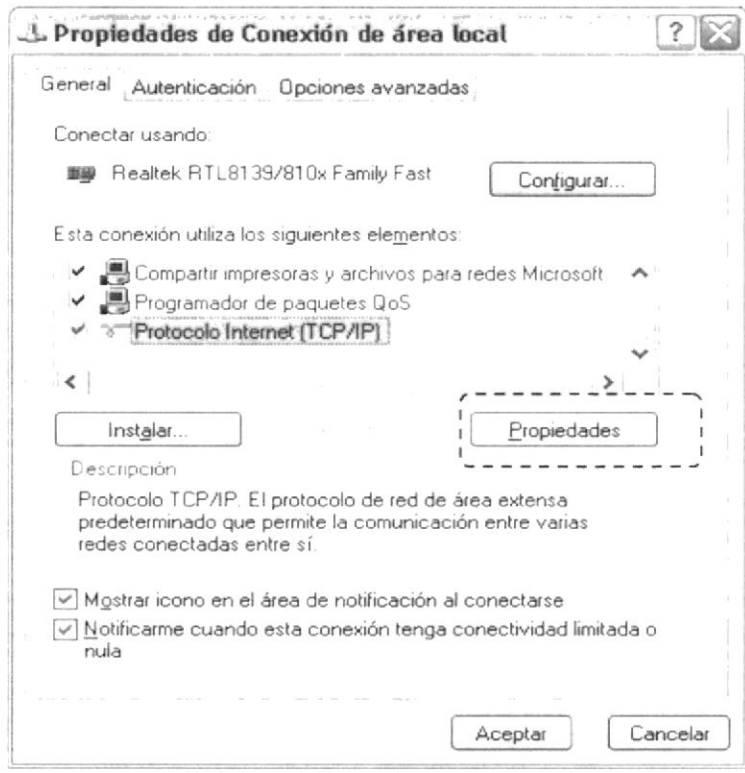


Figura 6-109: Propiedades de Conexión de área local

Habilite usar las siguientes direcciones del servidor DNS y coloque la dirección de IP del Servidor en Puerta de enlace y acepte

Figura 6-110: Asignando IP en cliente Windows

Una vez realizadas estas configuraciones en las propiedades del Protocolo Internet, abra el navegador vaya al menú Herramientas – Opciones de Internet – Conexiones – Configuración de área local y marque la opción: Utilizar un servidor Proxy para su LAN.
Esto hará para que la conexión con el Web Server sea a través del Proxy.

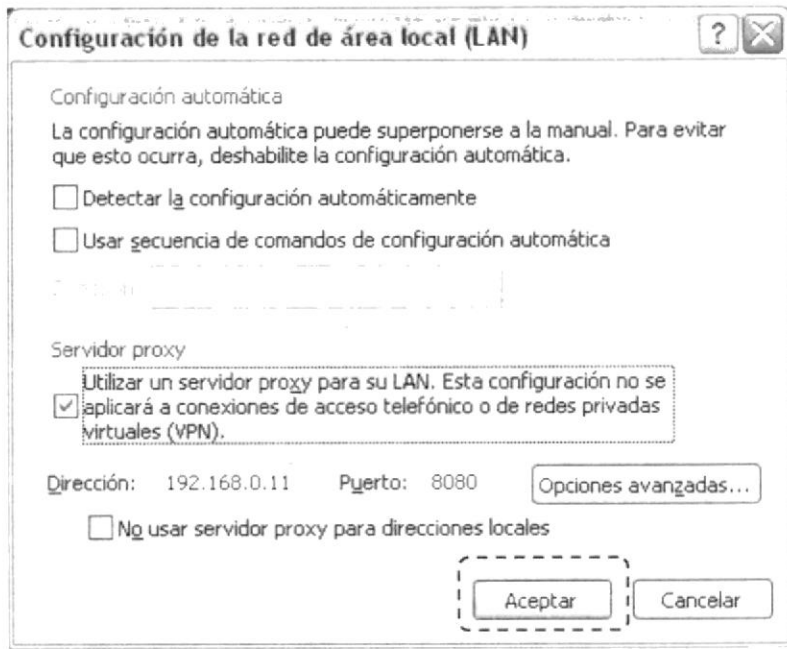


Figura 6-111: Configuración de conexión a través de Proxy en Internet Explorer

Acepte y digite en la barra de direcciones la página Web creada: www.armada.mil seguidamente presione la tecla enter.

Figura 6-112: Presentación de Página Web en Internet Explorer

6.22.5 RESTRICCIÓN DE ACCESO POR HORARIOS

La sintaxis para crear Listas de control de acceso que definan horarios es la siguiente:
acl **[nombre del horario]** time **[días de la semana]** **[hh:mm-hh:mm]**
Los días de la semana se definen con letras, las cuales corresponden a la primera letra del nombre en inglés, de modo que se utilizarán del siguiente modo:

- ✓ S Domingo
- ✓ M Lunes
- ✓ T Martes
- ✓ W Miércoles
- ✓ H Jueves
- ✓ F Viernes
- ✓ A Sábado

El horario se define en formato de 24 horas
Para aplicar la restricción proceda a crear la acl para lo cual escriba lo siguiente:
acl horario time H 14:01-15:30

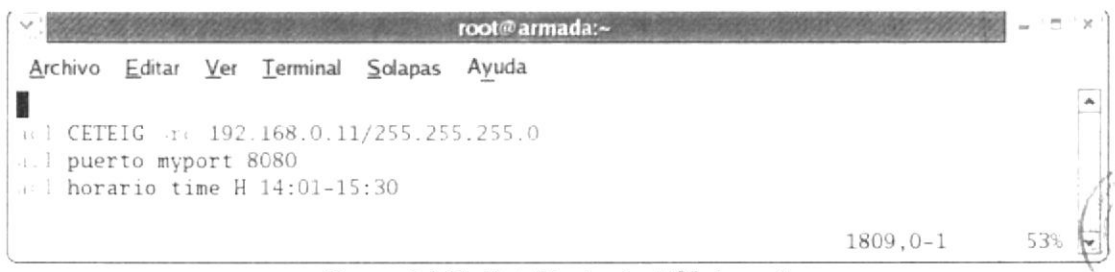


Figura 6-113: Estableciendo ACL horario

Después de haber creado las acl proceda a ingresar a la regla de control.
http_access deny CETEIG puerto horario
En la cual esta restringiendo la navegación a todo el rango de IP's de CETEIG los días jueves de 2:01 p.m a 3:30 p.m.

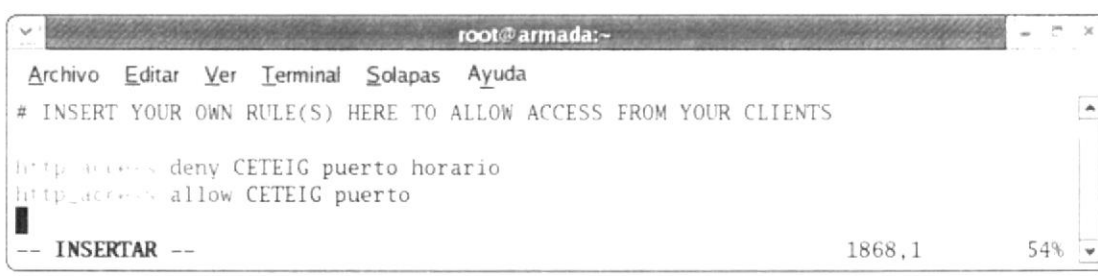


Figura 6-114: Definiendo regla para ACL

Finalmente, solo bastará recargar Squid para que tomen efecto los cambios y pueda hacer pruebas. Aplique el comando service squid reload.

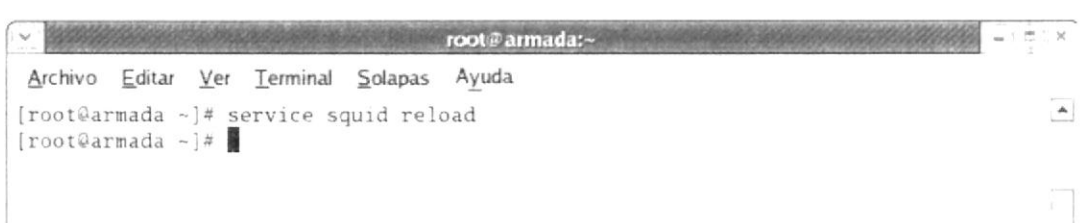


Figura 6-115: Recargando el servicio de Proxy

6.22.6 CONFIGURACIÓN EN CLIENTE WINDOWS

Abra el navegador vamos al menú Herramientas – Opciones de Internet –Conexiones – Configuración de área local y marque la opción: Utilizar un servidor Proxy para su LAN.

Figura 6-116: Configuración de conexión a través de Proxy en Internet Explorer

Acepte y digite en la barra de direcciones www.hi5.com. La prueba se realizó a las 2:30 p.m. de un día jueves por lo tanto bloquea el acceso.

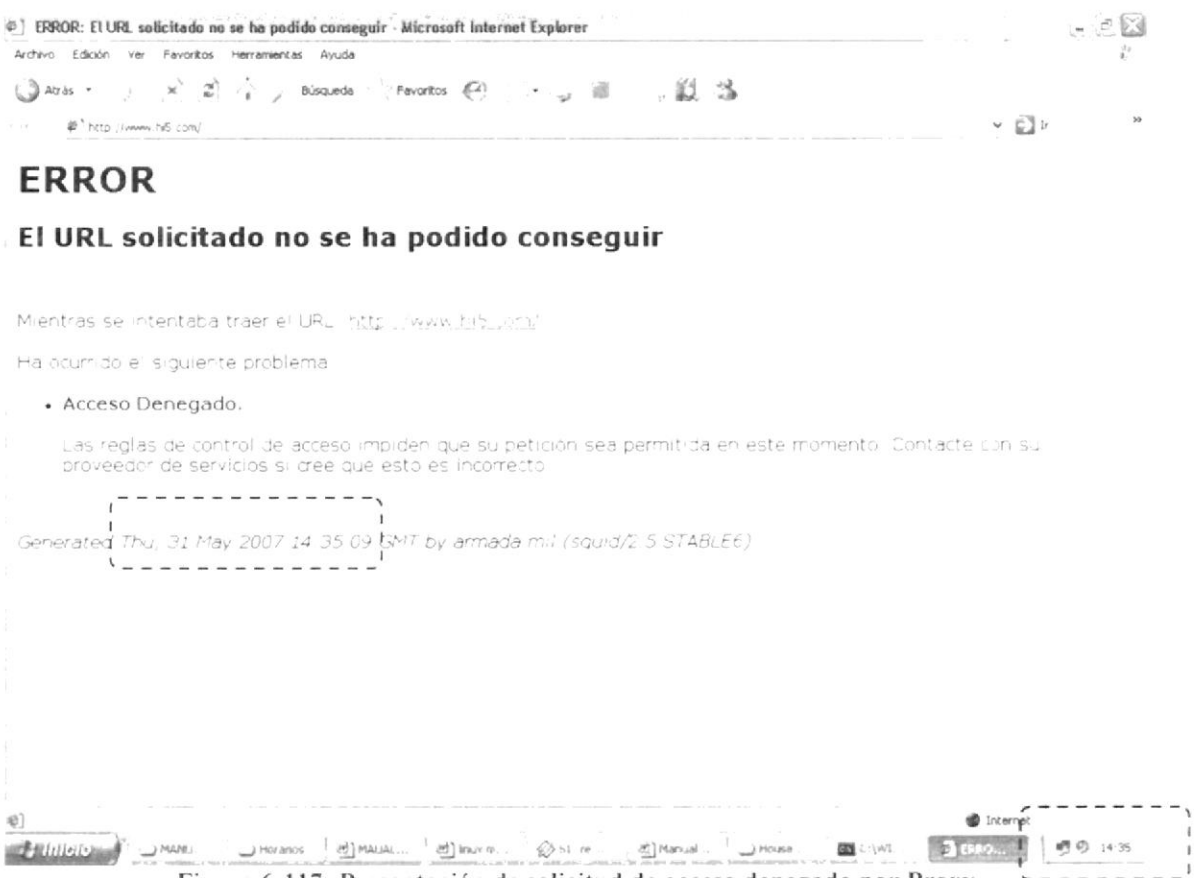


Figura 6-117: Presentación de solicitud de acceso denegado por Proxy

6.22.7 RESTRICCIÓN DE ACCESO A SITIOS WEB

Primeramente genere un archivo que contendrá una lista la cual contendrá las direcciones Web. **vi /etc/squid/sitios_p**

Figura 6-118: Editando el archivo de páginas a bloquear

Defina la acl de la siguiente manera:
acl sitios_prohibidos src "/etc/squid/sitios_p"
En la cual el origen será la ruta donde creo el archivo con la lista de direcciones Web.

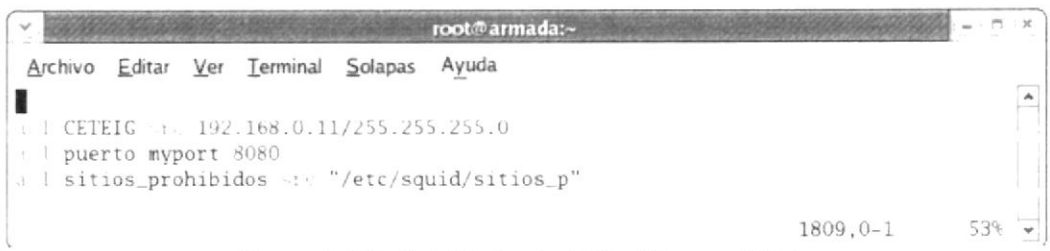


Figura 6-119: Estableciendo ACL sitios_prohibidos

Ahora aplique la regla de control:
http_access deny CETEIG puerto sitios_prohibidos
La cual nos indica que bloqueará el acceso a todo el rango de IP's de CETEIG que quieran navegar a través del puerto 8080 y que sean sitios prohibidos.

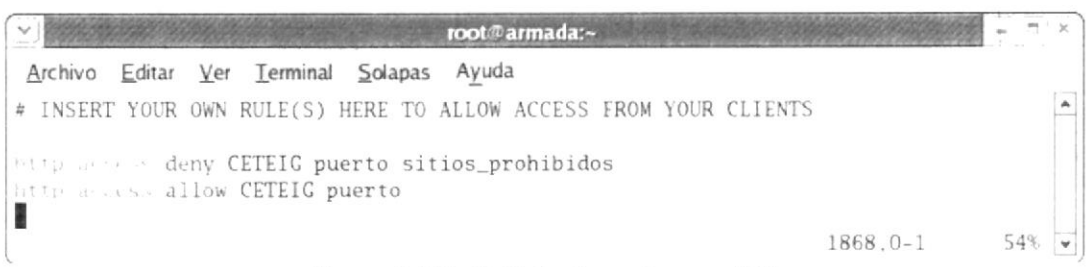


Figura 6-120: Definiendo regla para ACL

Finalmente, Aplique el comando service squid reload, para recargar los servicios

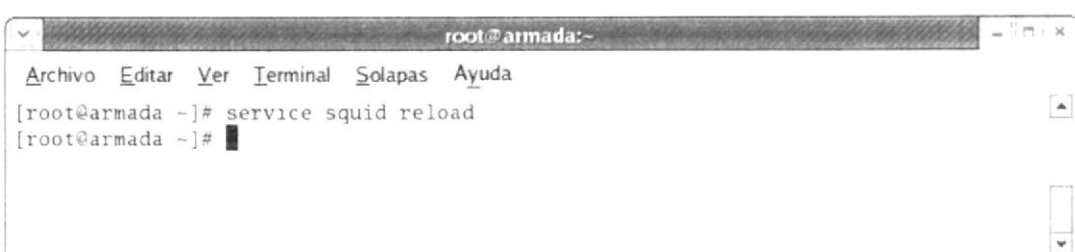


Figura 6-121: Recargando el servicio de Proxy

6.22.8 CONFIGURACIÓN EN CLIENTE WINDOWS

Abra el navegador vaya al menú Herramientas – Opciones de Internet – Conexiones – Configuración de área local y marque la opción: Utilizar un servidor Proxy para su LAN.

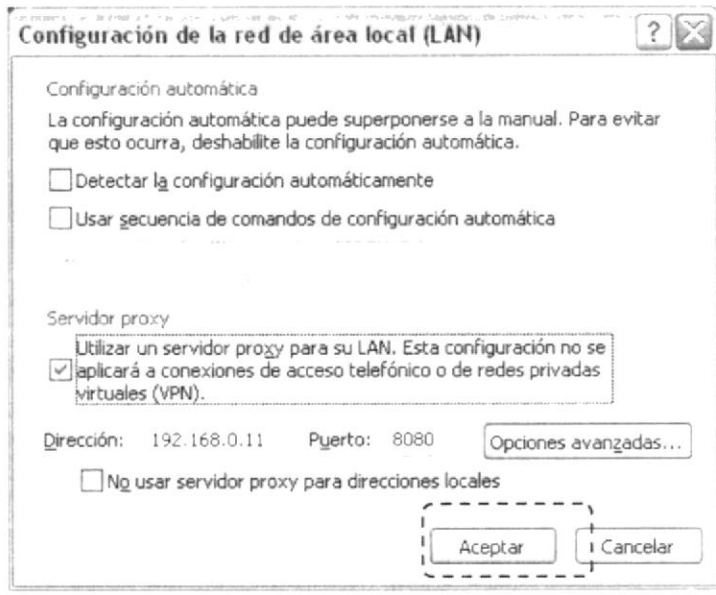


Figura 6-122: Configuración de conexión a través de Proxy en Internet Explorer

Acepte y digite en la barra de direcciones www.hi5.com. Por lo tanto bloquea el acceso, porque no es una página admitida

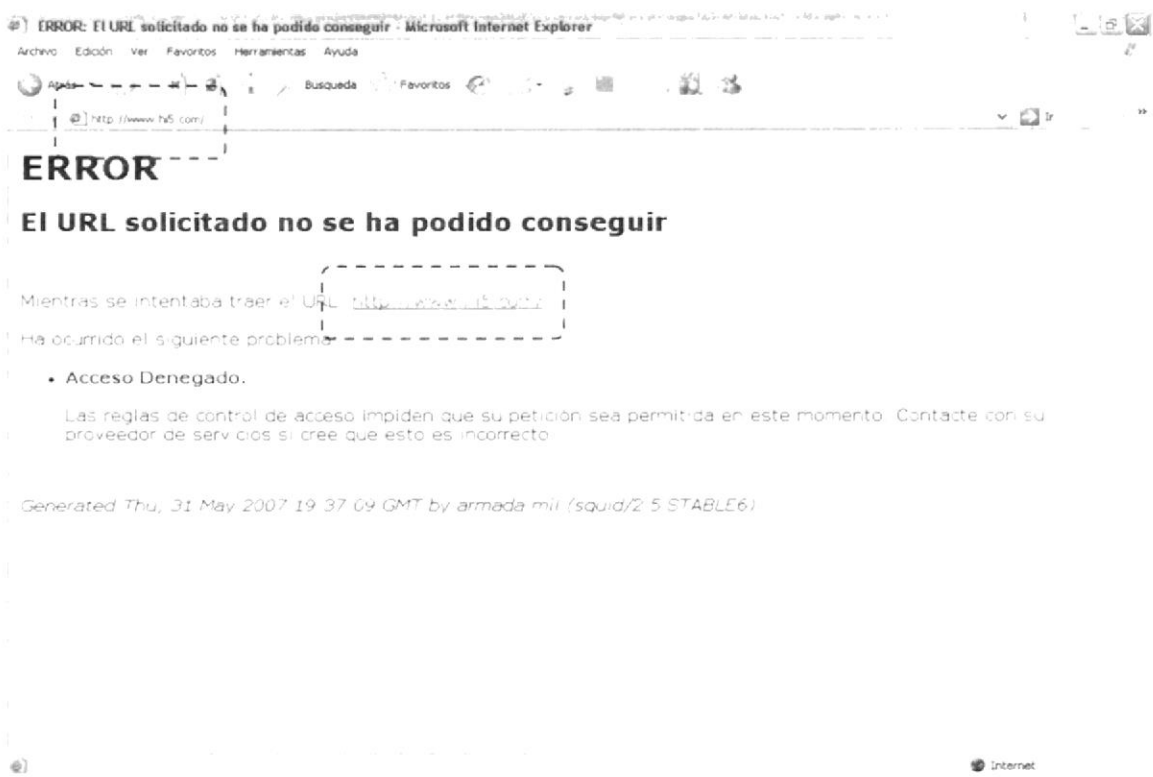


Figura 6-123: Presentación de solicitud de acceso denegado por Proxy

6.22.9 RESTRICCIÓN DE ACCESO POR AUTENTIFICACIÓN

Se requerirá la creación previa de un fichero que contendrá los nombres de usuarios y sus correspondientes claves de acceso (cifradas).
Proceda a crear el fichero: **touch /etc/squid/autorizados**

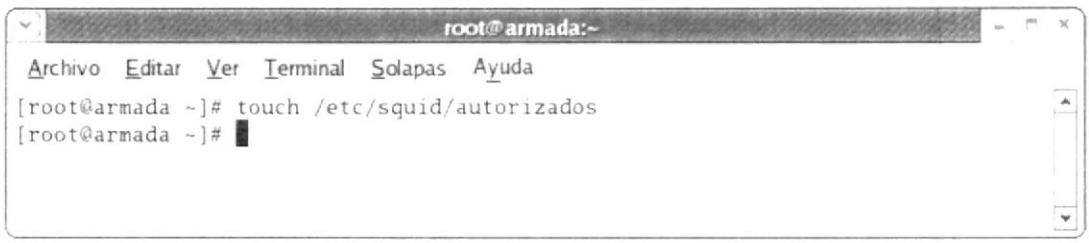


Figura 6-124: Ceración del archivo autorizados

Ahora cambie el propietario del fichero creado, para que pertenezca al grupo de squid aplique el siguiente comando:
chown squid:squid /etc/squid/autorizados

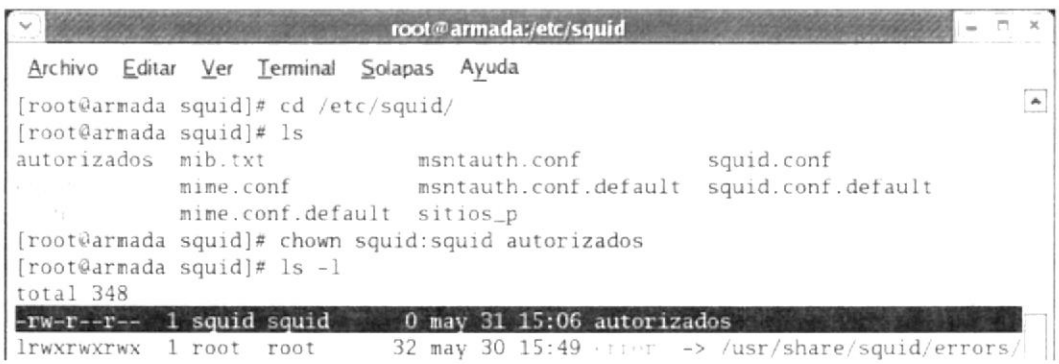


Figura 6-125: Cambiando propietario del archivo prohibidos

Edite el archivo de configuración de squid
vi /etc/squid/squid.conf

Descomente la línea para indicar que el programa de autenticación se utilizará. Localice la sección que corresponde a la etiqueta *auth_param basic program*.

Proceda a añadir el siguiente parámetro:
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/autorizados

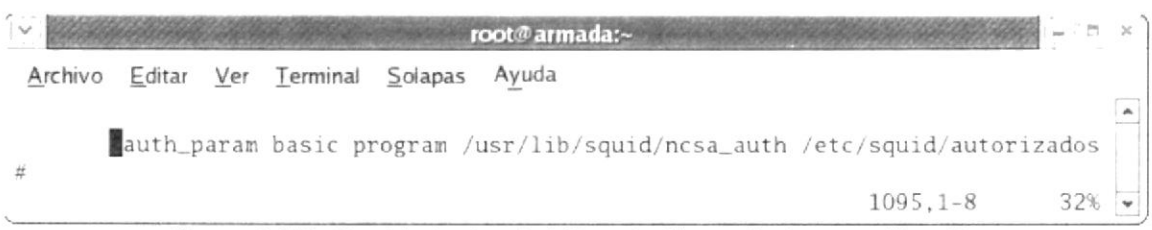


Figura 6-126: Estableciendo y habilitando directorio de autentificación

Descomente una acl llamada password con el parámetro *proxy_auth* que significa que el Proxy pedirá para la navegación autentificación

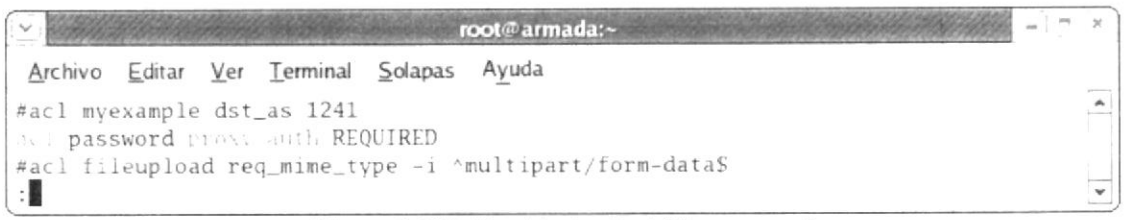


Figura 6-127: Estableciendo ACL password

Ahora aplique la regla de control:

http_access allow CETEIG puerto password

La cual nos indica que se dará el acceso a todo el rango de IP's de CETEIG que quieran navegar a través del puerto 8080 que tenga un nombre de usuario y contraseña.

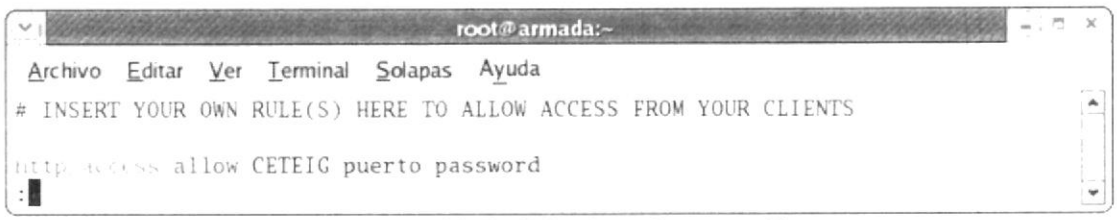


Figura 6-128: Definiendo regla para ACL

Agregue un usuario al sistema

useradd gerardo

passwd gerardo

Una vez creado el usuario agréguelo al fichero seguido de su username y password, con el siguiente comando:

htpasswd –b autorizados gerardo gerardo

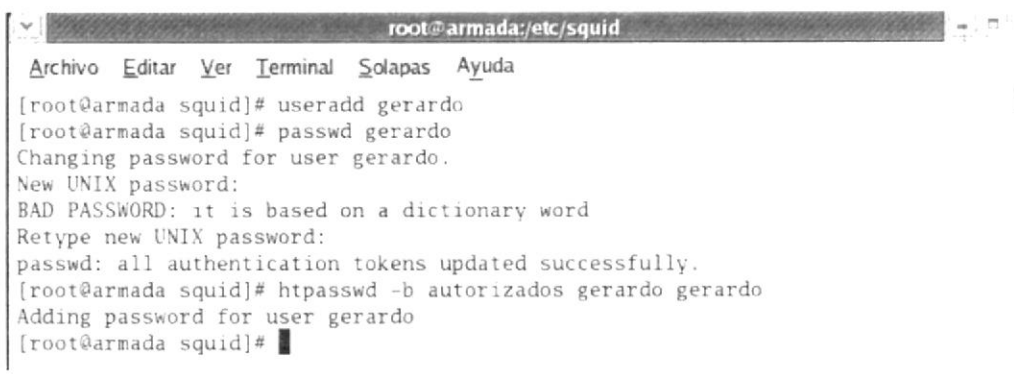


Figura 6-129: Agregando usuario de Proxy

De esta maneta da de alta al usuario del sistema para que pueda utilizar la autentificación en el Proxy.

Finalmente, Aplique el comando service squid reload, para recargar los servicios

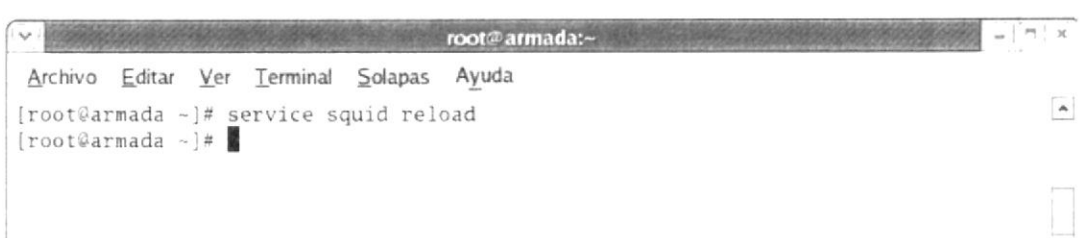


Figura 6-130: Recargando el servicio de Proxy

6.22.10 CONFIGURACIÓN EN CLIENTE WINDOWS

Abra Internet Explorer y coloque en la barra de direcciones www.armada.mil. Digite el usuario y contraseña y de clic en aceptar.

Figura 6-131: Configuración de conexión a través de Proxy en Internet Explorer

Una vez autentificados se podrá navegar normalmente.

Figura 6-132: Presentación de Página Web en Internet Explorer

6.23 SERVIDOR DE CORREO

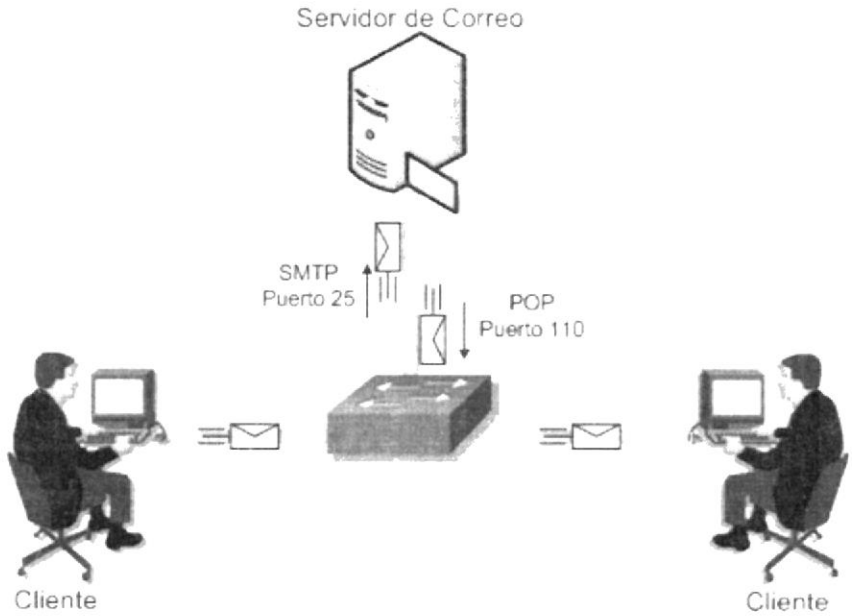


Figura 6-133: Diagrama de Servidor de Correo

Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) 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.

SMTP (Simple Mail Transfer Protocol).
Es un protocolo estándar de Internet del Nivel de Aplicación utilizado para la transmisión de correo electrónico a través de una conexión TCP/IP. Este es de hecho el único protocolo utilizado para la transmisión de correo electrónico a través de Internet. Es un protocolo basado sobre texto y relativamente simple donde se especifican uno más destinatarios en un mensaje que es transferido. A lo largo de los años han sido muchas las personas que han editado o contribuido a las especificaciones de SMTP, entre las cuales están Jon Postel, Eric Allman, Dave Crocker, Ned Freed, Randall Gellens, John Klensin y Keith Moore.
Para determinar el servidor SMTP para un dominio dado, se utilizan los registros MX (Mail Exchanger) en la Zona de Autoridad correspondiente al ese mismo dominio contestado por un Servidor DNS. Después de establecerse una conexión entre el remitente (el cliente) y el destinatario (el servidor), se inicia una sesión SMTP, ejemplificada a continuación.

POP3 (Post Office Protocol version 3).
Es un protocolo estándar de Internet del Nivel de Aplicación que recupera el correo electrónico desde un servidor remoto a través de una conexión TCP/IP desde un cliente local. El diseño de POP3 y sus predecesores es permitir a los usuarios recuperar el correo electrónico al estar conectados hacia una red y manipular los mensajes recuperados sin necesidad de permanecer conectados. A pesar de que muchos clientes de correo electrónico incluyen soporte para dejar el correo en el servidor, todos los clientes de POP3 recuperan todos los mensajes y los almacenan como mensajes nuevos en la computadora o anfitrión utilizado por el usuario, eliminan los mensajes en el servidor y terminan la conexión.

IMAP (Internet Message Access Protocol).
Es un protocolo estándar de Internet del Nivel de Aplicación utilizado para acceder hacia el correo electrónico en un servidor remoto a través de una conexión TCP/IP desde un cliente local.
La versión más reciente de IMAP es la 4, revisión 1, y está definida en el RFC 3501. IMAP trabaja sobre TCP en el puerto 143.
Fue diseñado por Mark Crispin en 1986 como una alternativa más moderna que cubriera las deficiencias de POP3.

Acerca de Sendmail.
Es el más popular agente de transporte de correo (MTA o Mail Transport Agent), responsable quizá de poco más del 70% del correo electrónico del mundo. Aunque por largo tiempo se le ha criticado por muchos incidentes de de seguridad, lo cierto es que éstos siempre han sido resueltos en pocas horas.

Acerca de Dovecot.
Dovecot es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo. Dovecot puede utilizar tanto el formato mbox como maildir y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.

Ventajas de un Servidor de Correo en Linux:

- ✓ No dependerá de los servicios gratuitos (Hotmail, Yahoo!, etc).
- ✓ Puede enviar correos masivos a grupos y garantizar que los mensajes son recibidos en las cuentas de los destinatarios.
- ✓ Puede crear todas las cuentas de redireccionamiento que necesite.
- ✓ Puede crear todos los grupos de correo que necesite.
- ✓ El correo puede ser consultado a través de Internet o descargado a su PC.
- ✓ No necesita adquirir ningún software.
- ✓ Es muy fácil de manejar para el usuario o el administrador.

6.23.1 REQUERIMIENTOS DE CONFIGURACIÓN MAIL SERVER

- Tener instalado el sistema Linux Fedora Core 3
- Tener una IP estática en el Server Linux
- Tener configurada la tarjeta de red, tanto en el Server Linux como en el cliente.
- Tener instalado los paquetes de sendmail y dovecot
- Deshabilitado los firewall (cortafuegos)

Es necesario deshabilitar los firewalls para no tener ningún tipo de restricciones al momento de levantar los servicios, ya que estos usan puertos y protocolos que podrían ser bloqueados por el o los cortafuegos. De esta manera no tendremos ningún tipo de conflicto al realizar nuestra configuración.

6.23.2 CONFIGURACIÓN MAIL SERVER

Verifique si están instalados los paquetes de *sendamil* y *dovecot*, de la siguiente manera:
[root@armada /] # rpm –q sendmail
[root@armada /] # rpm –q dovecot

Edite el archivo de configuración de sendmail:
[root@armada /] # vi /etc/mail/sendmail.cf

Modifique esta linea
Cwarmada.mil
Especifique el nombre de nuestro dominio

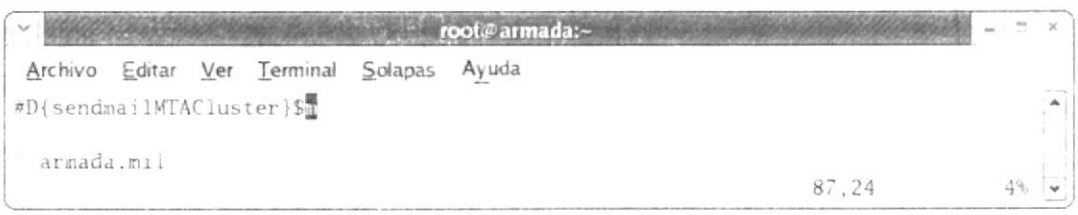


Figura 6-134: Estableciendo el dominio armada.mil

Descomente el parámetro de la etiqueta SMTP daemon options
Y cambie la dirección 127.0.0.1 por 0.0.0.0, que significa que el puerto oirá para cualquier red.

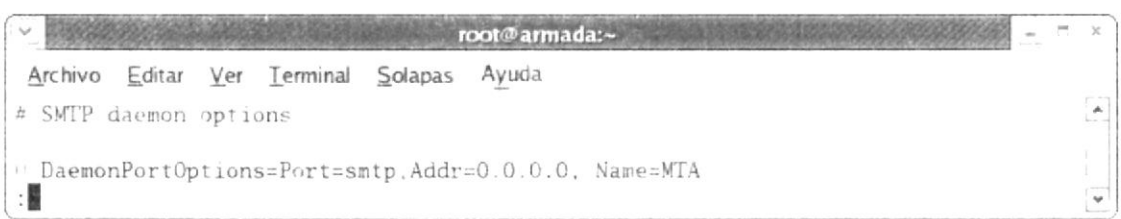


Figura 6-135: Configurando daemon options para protocolo SMTP

Descomente el parámetro de la etiqueta SMTP client options.

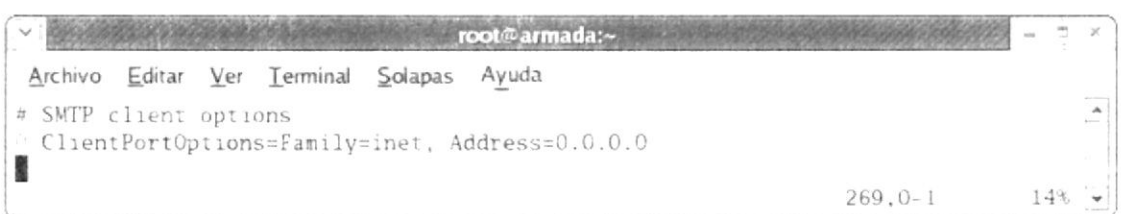


Figura 6-136: Configurando daemon options para protocolo SMTP

Edite el archivo de configuración de dovecot:
[root@armada /] # vi /etc/dovecot.conf

En el parámetro protocols añada el pop3.
Más abajo descomente las líneas imap_listen, pop3_listen
imap_listen = [::]
pop3_listen = [::]
Significa que ambos puertos están escuchando para cualquier red

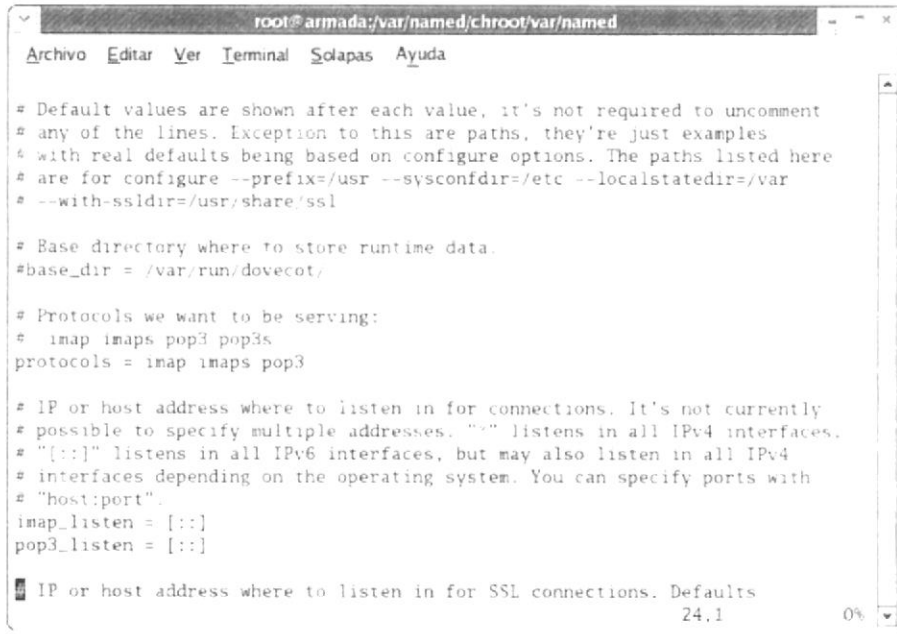


Figura 6-137: Añadiendo el protocolo pop3

Guarde los cambios y salga
Edite el fichero hosts:
[root@armada /] # vi /etc/hosts

Donde se confirmará que la dirección del servidor tenga su correspondiente dominio si no existiera agréguelo.

192.168.0.11 armada.mil armada

IP del servidor dominio alias del computador

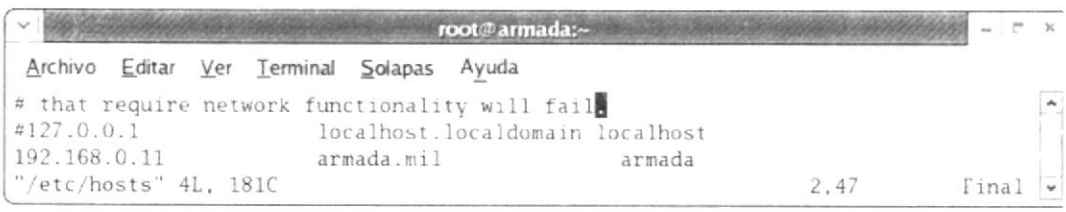


Figura 6-138: Verificando el archivo hosts

Edite el fichero network:
[root@armada /] # vi /etc/sysconfig/network
Confirme que el hostname sea el mismo nombre del dominio, de no estar iguales cámbielo.

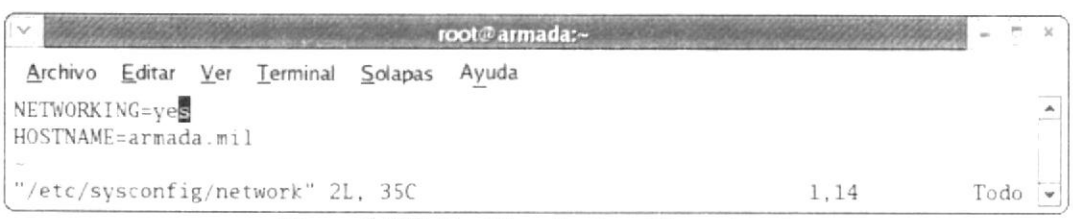


Figura 6-139: Verificando el archivo network

Al realizar los cambios proceda a reiniciar el servicio de red

[root@armada /] # service network restart

En caso de presentar algún error reinicie el equipo, continúe y edite el fichero krb5-telnet

[root@armada /] # vi /etc/xinet.d/krb5-telnet

En el parámetro disable cambie el yes por no, para poder realizar un telnet desde el cliente Windows.

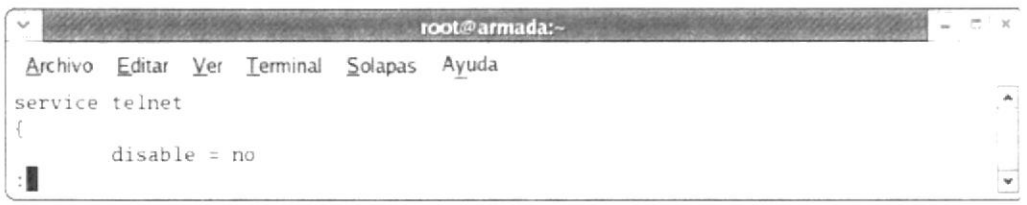


Figura 6-140: Habilitando Telnet

Guarde los cambios y salga. Proceda a iniciar los servicios dovecot y sendmail

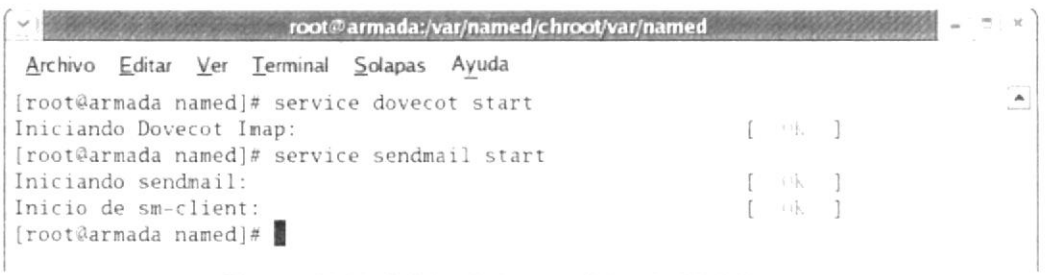


Figura 6-141: Iniciando los servicios de Mail Server

Ahora ejecute el siguiente comando

[root@armada /] # netstat –an|more

El cual permite observar todos los puertos que están escuchando, deberá confirmar que los puertos 25 y 110 se encuentren en dicho estado.

0.0.0.0:25 LISTEN

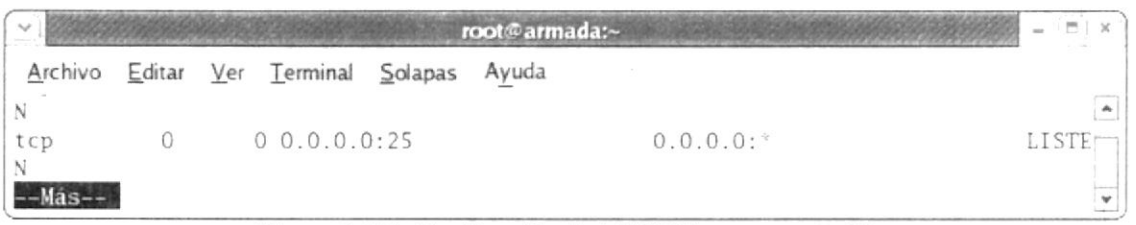


Figura 6-142: Verificación de LISTEN para puerto 25

0 :::110 LISTEN

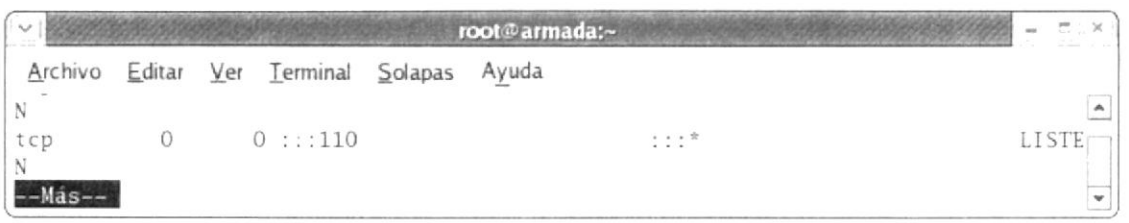


Figura 6-143: Verificación de LISTEN para puerto 110

Indica que ambos puertos están escuchando para cualquier red, continúe y agregue un usuario al sistema
useradd ceteig
passwd ceteig
Al agregar este usuario al sistema automáticamente es un usuario de correo.
Ahora proceda a enviar un correo a este usuario desde root, con el siguiente comando:
mail destinatario@domino tecla enter – contenido del mail – un punto + enter para finalizar el contenido – otro punto para enviar una copia y tecla enter.

mail ceteig@armada.mil
Subject: Prueba de Correo
Este correo es enviado desde el Servidor Linux
.
CC: .

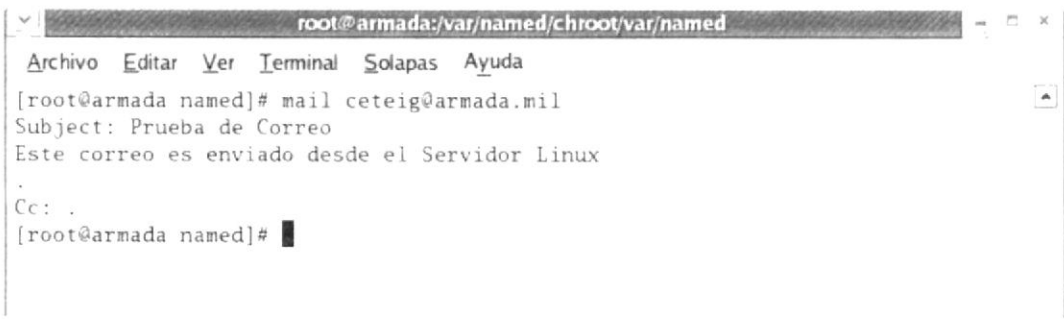


Figura 6-144: Envío de correo desde Server Linux

6.23.3 CARGAR SERVICIOS MAIL SERVER AL INICIAR EL SISTEMA

Digite **setup** en la Terminal y habilite los servicios **sendmail** y **dovecot** para que se ejecuten automáticamente al iniciar Fedora.
Proceda a entrar en servicios del sistema, marcándolo y luego con la tecla tab ubíquese en ejecutar una herramienta y presione la tecla enter. Con las flechas direccionales nos movemos y una vez seleccionado el servicio con la tecla tab nos ubicamos en OK y aceptamos los cambios presionando la tecla enter.

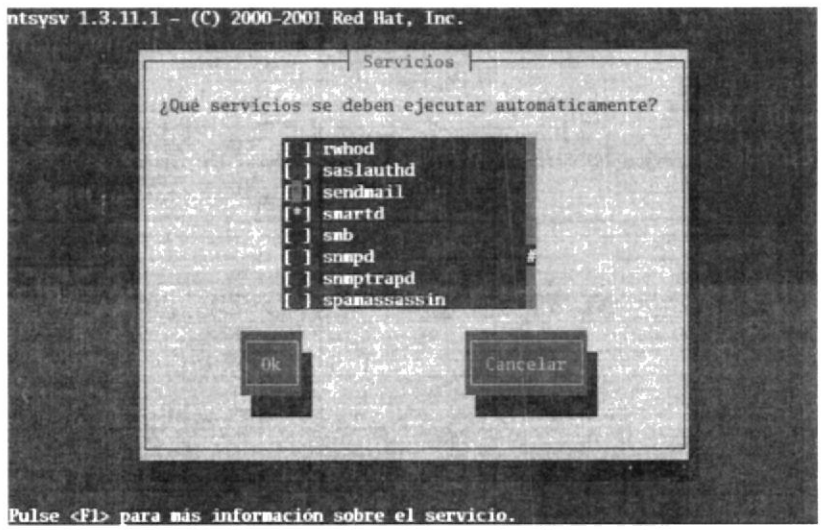


Figura 6-145: Ejecutar el servicio sendmail automáticamente

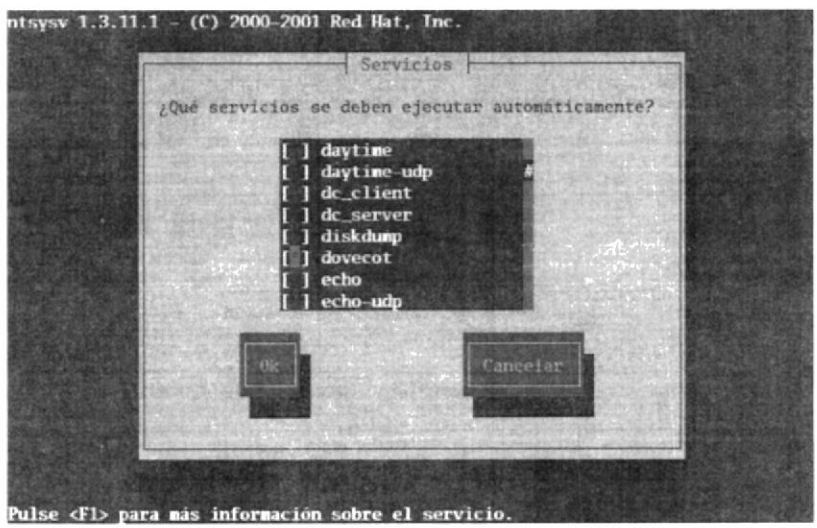


Figura 6-146: Ejecutar el servicio dovecot automáticamente

6.23.4 CONFIGURACIÓN EN CLIENTE WINDOWS

Estando en Windows de clic en inicio – ejecutar y escriba cmd, para entrar a la consola de comandos del cliente.

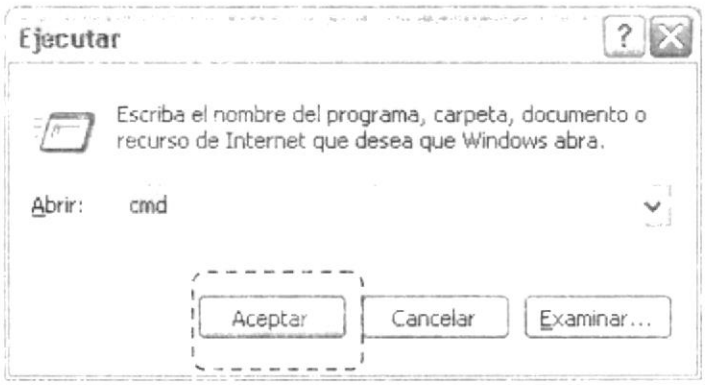


Figura 6-147: Ejecutar consola DOS

Realice el telnet al servidor Linux para el puerto 110
telnet 192.168.0.11 110

Figura 6-148: Telnet a dovecot

Si el puerto está escuchando responderá. OK dovecot ready.

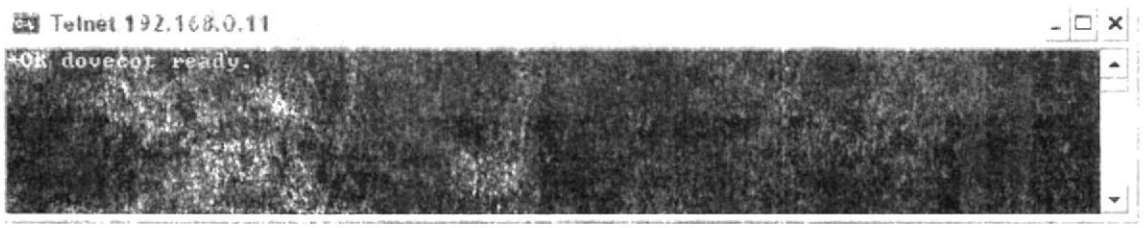


Figura 6-149: Respuesta de dovecot

Ahora proceda a configurar una cuenta de correo en el programa predeterminado para leer correos en el cliente, los cuales pueden ser Outlook Express o Microsoft Office Outlook. En este caso será el último mencionado.

Figura 6-150: Ingresando a Microsoft Office Outlook

Vaya al menú herramientas – cuentas de correo electrónico y ponga la opción crear nueva cuenta de correo electrónico. El tipo de servidor POP3, de clic en siguiente

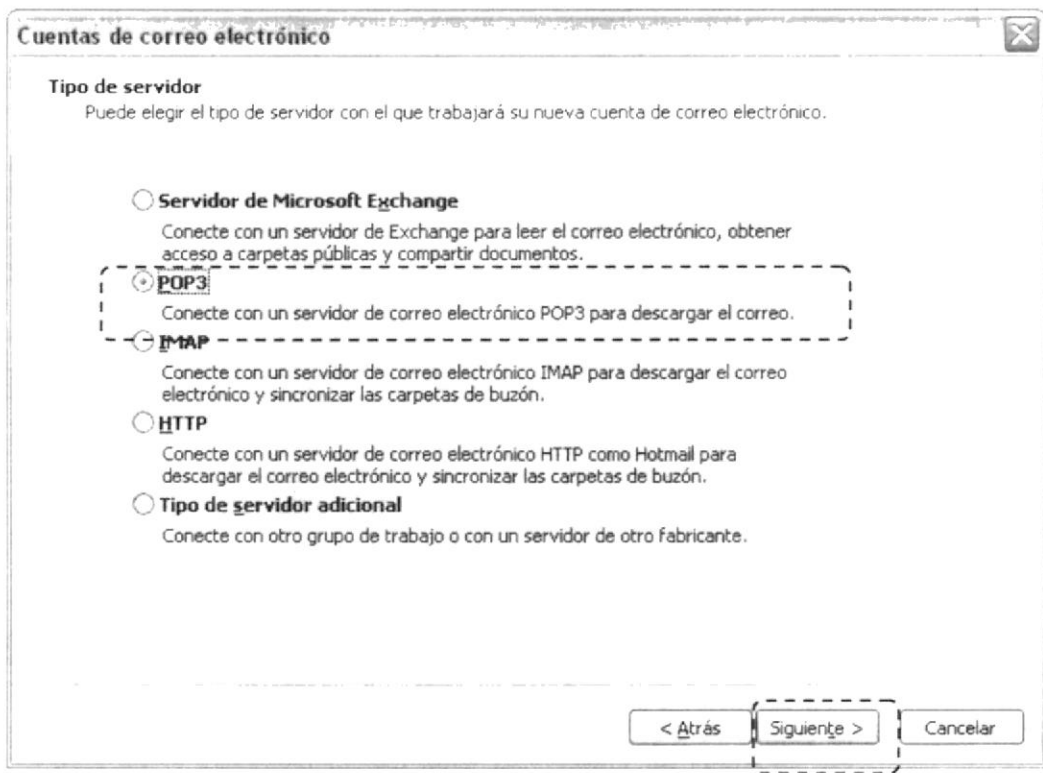


Figura 6-151: Configurando el tipo de servidor

Proceda a llenar los datos de nuestro correo
En dirección de correo entrante y saliente ubicamos la IP de nuestro servidor Linux

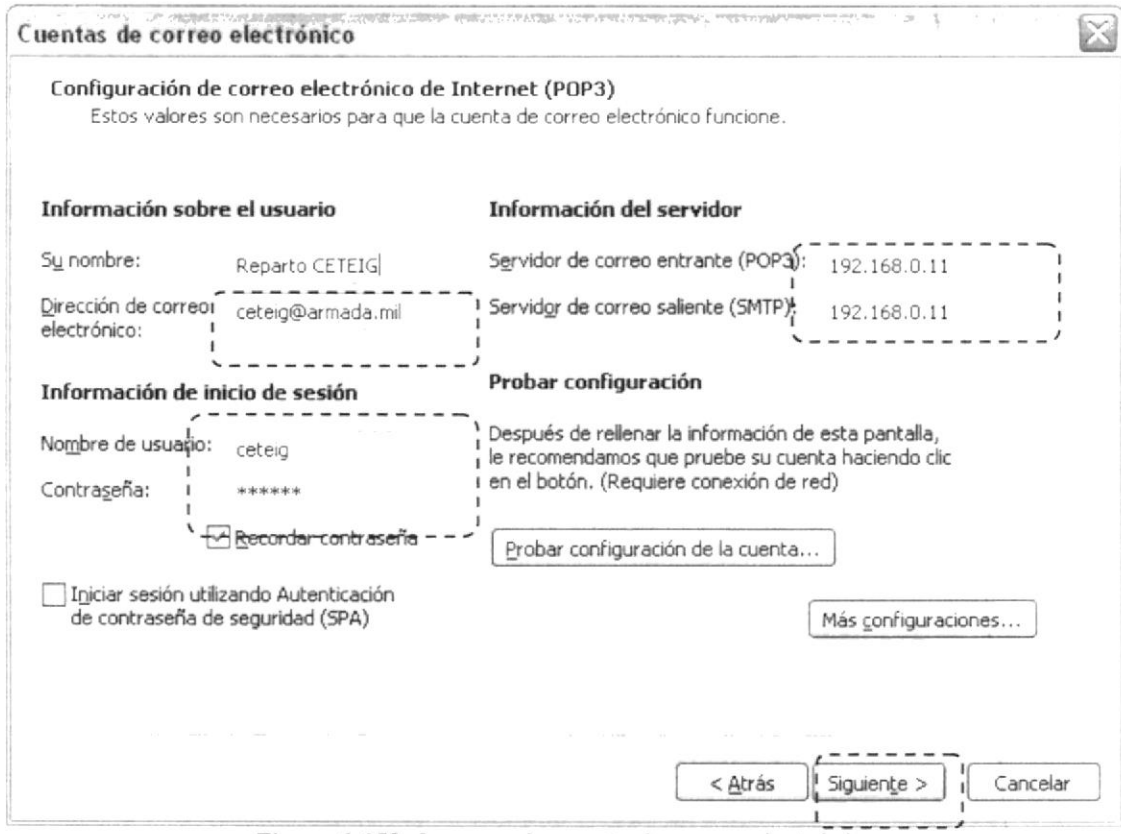


Figura 6-152: Ingresando cuenta de correo electrónico

De clic en siguiente y finalice el asistente.
Estando en la ventana principal de clic en enviar y recibir.

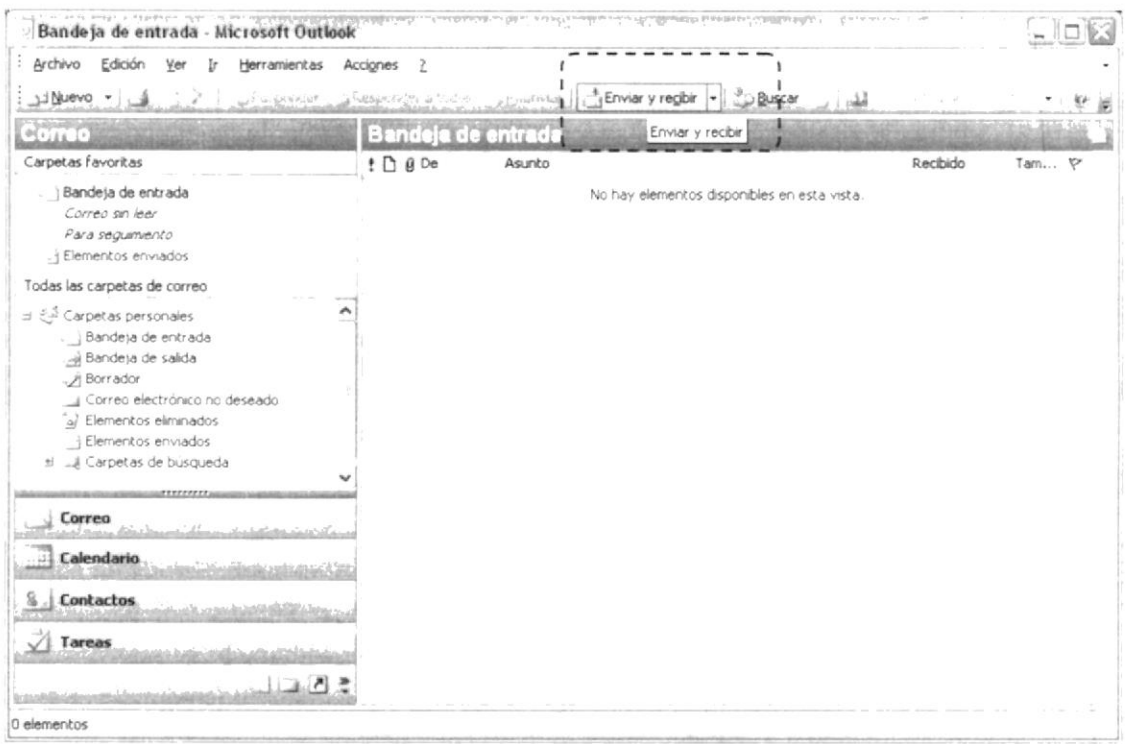


Figura 6-153: Ejecutando recibir correo en Microsoft Outlook

Al terminar el proceso de enviar y recibir aparece una ventana de status, al finalizar en la bandeja de entrada el mail enviado desde el servidor Linux.

De clic en el mail para leerlo. Luego en el menú superior de clic en responder

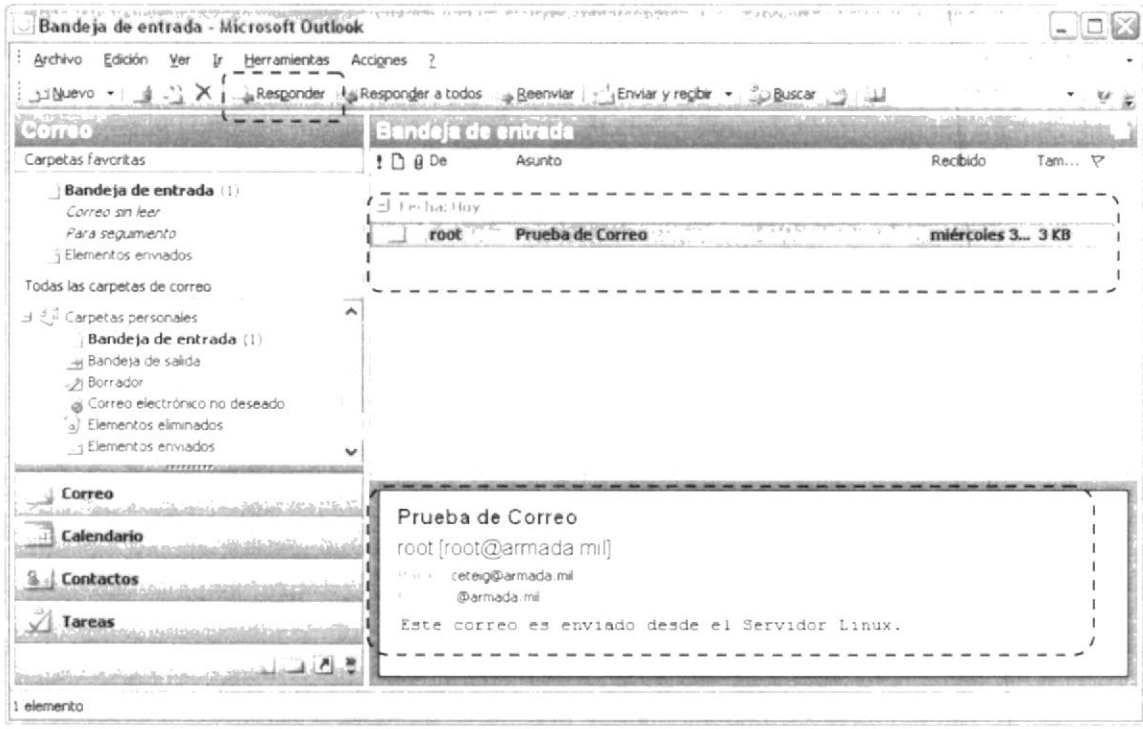


Figura 6-154: Bandeja de Entrada de Microsoft Outlook

Responda el mail al correo de root, en el contenido del mensaje coloque: Mensaje de Respuesta al Servidor Linux desde cliente Windows.

Figura 6-155: Redactando y enviando correo de respuesta a root

6.23.5 RECEPCIÓN DE CORREO EN SERVIDOR LINUX

Ingrese al sistema con el usuario de root, aparecerá un mensaje que ha recibido un nuevo correo.

Figura 6-156: Nuevo correo en root

Digite el comando mail para leer el nuevo correo, digite el número 1 para indicar que el número de correo es el que desea leer de la lista.

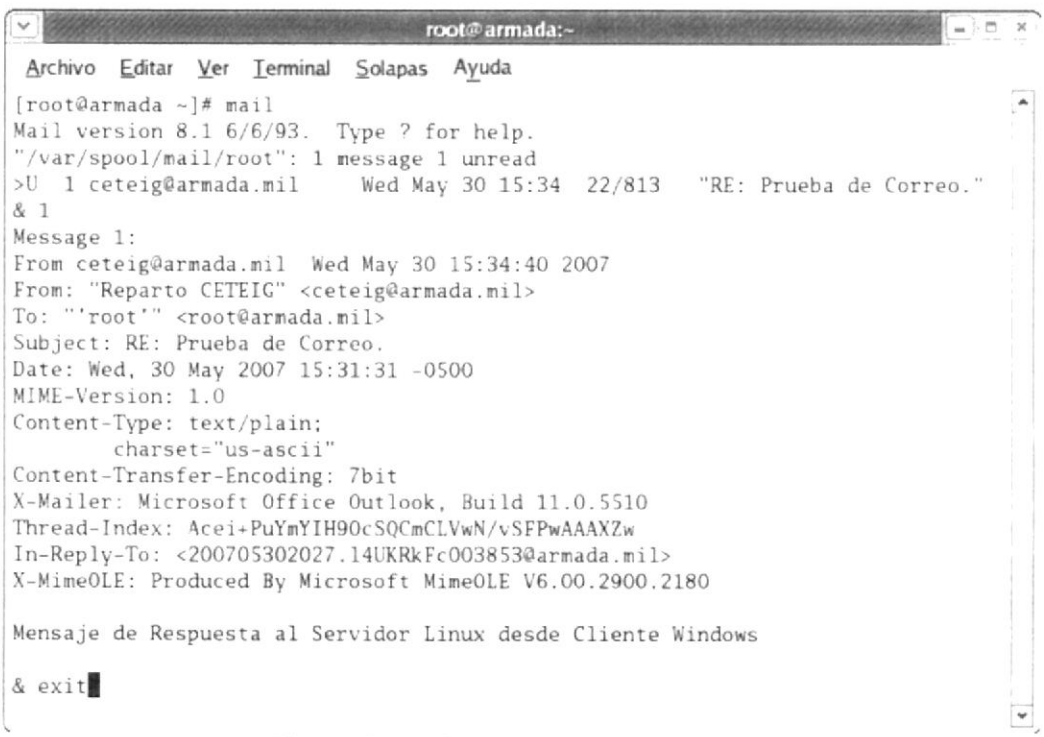


Figura 6-157: Contenido del correo en root

Recibido este mensaje queda probado el servidor de correo para salir digite exit.

6.24 SERVIDOR DHCP

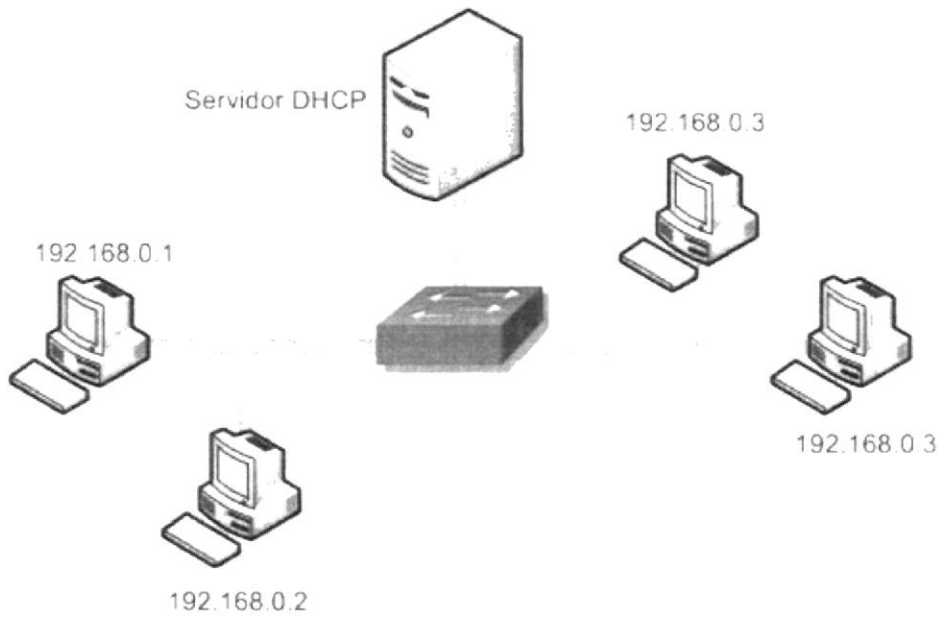


Figura 6-158: Diagrama de Servidor DHCP

DHCP (acrónimo de Dynamic Host Configuration Protocol que se traduce Protocolo de configuración dinámica de servidores) es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP; máscara de sub-red, puerta de enlace, etc.) a partir de un servidor DHCP. Su propósito principal es hacer más fáciles de administrar las redes grandes. DHCP existe desde 1993 como protocolo

Sin la ayuda de un servidor DHCP, tendrían que configurarse de forma manual cada dirección IP de cada anfitrión que pertenezca a una Red de Área Local. Si un anfitrión se traslada hacia otra ubicación donde existe otra Red de Área Local, se tendrá que configurar otra dirección IP diferente para poder unirse a esta nueva Red de Área Local.

Un servidor DHCP entonces supervisa y distribuye las direcciones IP de una Red de Área Local asignando una dirección IP a cada anfitrión que se una a la Red de Área Local. Cuando, por mencionar un ejemplo, una computadora portátil se configura para utilizar DHCP, a ésta le será asignada una dirección IP y otros parámetros de red necesarios para unirse a cada Red de Área Local donde se localice.

Existen tres métodos de asignación en el protocolo DHCP:

- ✓ **Asignación manual:** La asignación utiliza una tabla con direcciones MAC (acrónimo de Media Access Control Address, que se traduce como dirección de Control de Acceso al Medio). Sólo los anfitriones con una dirección MAC definida en dicha tabla recibirá el IP asignada en la misma tabla. Esto se hace a través de los parámetros hardware ethernet y fixed-address.

- ✓ **Asignación automática:** Una dirección de IP disponible dentro de un rango determinado se asigna permanentemente al anfitrión que la requiera.

- ✓ **Asignación dinámica:** Se determina arbitrariamente un rango de direcciones IP y cada anfitrión conectado a la red está configurada para solicitar su dirección IP al servidor cuando se inicia el dispositivo de red, utilizando un intervalo de tiempo controlable (parámetros default-lease-time y max-lease-time) de modo que las direcciones IP no son permanentes y se reutilizan de forma dinámica.

Procesos del servicio DHCP

- ✓ Ámbito servidor DHCP: es el proceso de agrupamiento administrativo de equipos o clientes de una subred que utilizan el servicio DHCP.

- ✓ Rango servidor DHCP: El proceso de rango está definido por un grupo de direcciones IP en una subred determinada, como por ejemplo de 192.168.0.1 a 192.168.0.254, que el servidor DHCP puede conceder a los clientes.

- ✓ Concesión o alquiler de direcciones: el proceso de concesión es un período de tiempo que los servidores DHCP especifican, durante el cual un equipo cliente puede utilizar una dirección IP asignada.

Ventajas del uso de DHCP

- ✓ Configuración segura y confiable: DHCP evita los errores de configuración que se producen por la necesidad de escribir los valores manualmente en cada equipo. Así mismo, DHCP ayuda a evitar los conflictos de direcciones que se producen al configurar un equipo nuevo en la red con una dirección IP ya asignada.

- ✓ Reduce la administración de la configuración: La utilización de servidores DHCP puede reducir significativamente el tiempo necesario para configurar y modificar la configuración de los equipos de la red. Los servidores se pueden configurar para que suministren un conjunto completo de valores de configuración adicionales al asignar concesiones de direcciones. Estos valores se asignan mediante opciones DHCP.

Desventajas del uso de DHCP

- ✓ Al entregar números IP dentro de la red, habiendo un DNS, no hay un puente intermedio entre DNS y DHCP directo. Es decir, hay que agregar las máquinas "a mano" en el DNS.

- ✓ La seguridad, no nos permite saber que direcciones han sido signadas a nuestros posibles servidores

- ✓ Mayor difusión de paquetes en la red, aunque hoy en día con la velocidad de las redes no parece demasiado problemático.

6.24.1 REQUERIMIENTOS DE CONFIGURACIÓN DHCP

- Tener instalado el sistema Linux Fedora Core 3
- Tener una IP estática en el Server Linux
- Tener configurada la tarjeta de red, tanto en el Server Linux como en el cliente.
- Tener instalado el paquete dhcp
- Deshabilitado los firewall (cortafuegos)

Es necesario deshabilitar los firewalls para no tener ningún tipo de restricciones al momento de levantar los servicios, ya que estos usan puertos y protocolos que podrían ser bloqueados por el o los cortafuegos. De esta manera no tendremos ningún tipo de conflicto al realizar nuestra configuración.

6.24.2 CONFIGURACIÓN DHCP

Verifique si está instalado el paquete *dhcp* de la siguiente manera:
[root@armada /] # rpm –q dhcp

Copie el fichero de ejemplo de dhcp:
cp /usr/share/doc/dhcp-3.01/dhcpd.conf.sample /etc/dhcpd.conf

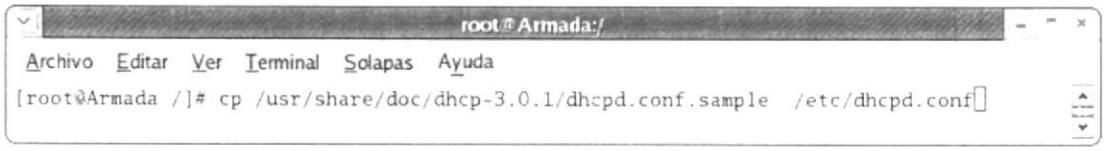


Figura 6-159: Copiando archivo dhcp.conf.sample

Edite el archivo dhcpd.conf y modifique los siguientes parámetros
[root@armada /] # vi /etc/dhcpd.conf

option routers coloque la IP de la puerta de entrada

option subset-mask la máscara de subred de la puerta de enlace
En este caso es la IP de la máquina 192.168.0.11 máscara 255.255.255.0

option domain-name coloque el nombre del dominio.

option domain-name-servers coloque 192.168.0.11 IP del servidor de DNS (hay que tener un servidor DNS previamente instalado y configurado)

range dynamic-bootp 192.168.0.12 192.168.0.254 defina el rango de direcciones IP que estarán disponibles en este caso serán desde la .12 hasta la .254

Figura 6-160: Editando archivo de configuración de DHCP

Salga y guarde los cambios

Proceda a crear un archivo en la siguiente ruta, en este archivo se almacenarán las direcciones IP de las máquinas que tenga en el servidor DHCP
[root@armada /] touch /var/lib/dhcp/dhcpd.leases

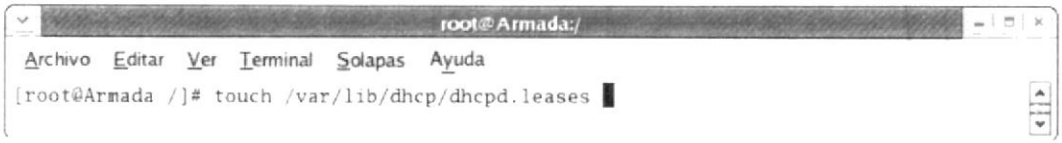


Figura 6-161: Creando archivo dhcpd.leases

Inicie el servicio del dhcpd:
service dhcpd start

Figura 6-162: Iniciando servicio de DHCP

6.24.3 CARGAR SERVICIOS DHCP AL INICIAR EL SISTEMA

Digite **setup** en la Terminal y habilite el servicio **dhcp** para que se ejecute automáticamente al iniciar Fedora.
Proceda a entrar en servicios del sistema, marcándolo y luego con la tecla tab ubíquese en ejecutar una herramienta y presione la tecla enter. Con las flechas direccionales muévase y una vez seleccionado el servicio con la tecla tab ubíquese en OK y acepte los cambios presionando la tecla enter.

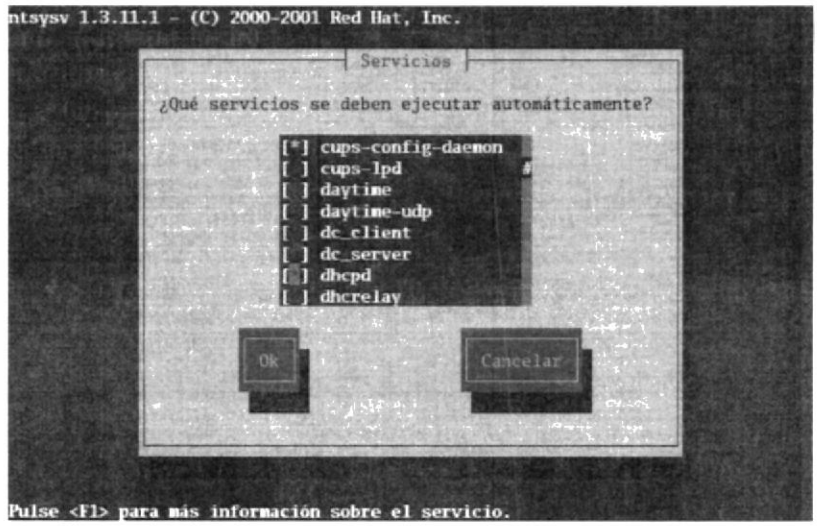


Figura 6-163: Ejecutar el servicio de DHCP automáticamente

6.24.4 CONFIGURACIÓN EN CLIENTE WINDOWS

De clic sobre el menú Inicio, entre al Panel de Control, de doble clic en Conexiones de Red y presentará la siguiente pantalla.

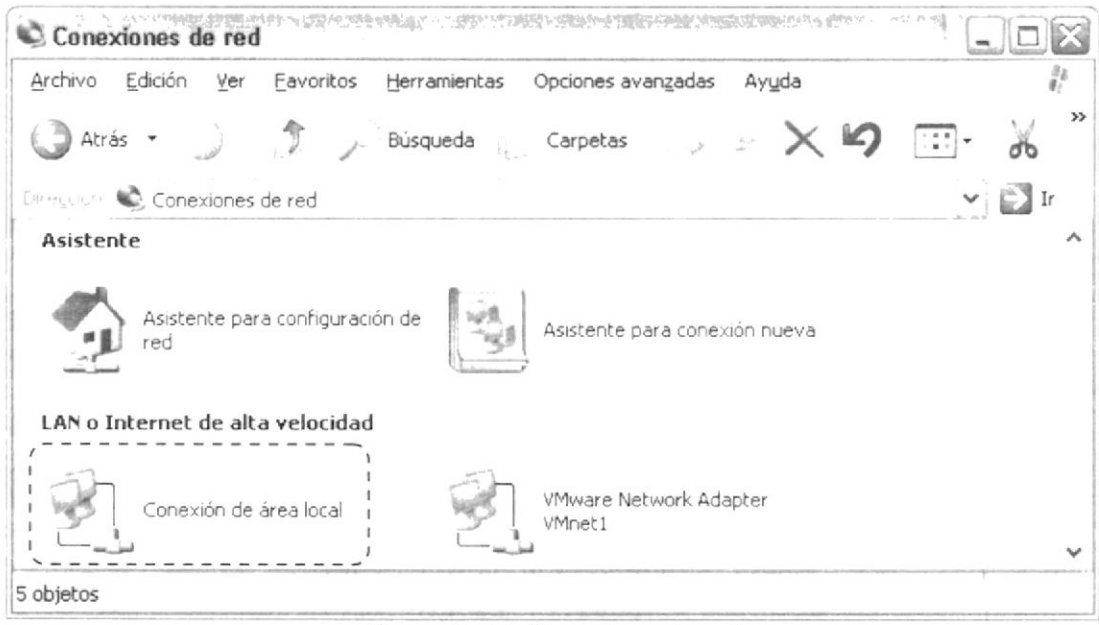


Figura 6-164: Conexiones de red

De doble clic en Conexión de área local y entre a Propiedades

Figura 6-165: Estado de conexión de área local

Ubíquese en Protocolo Internet (TCP/IP) y de clic en Propiedades

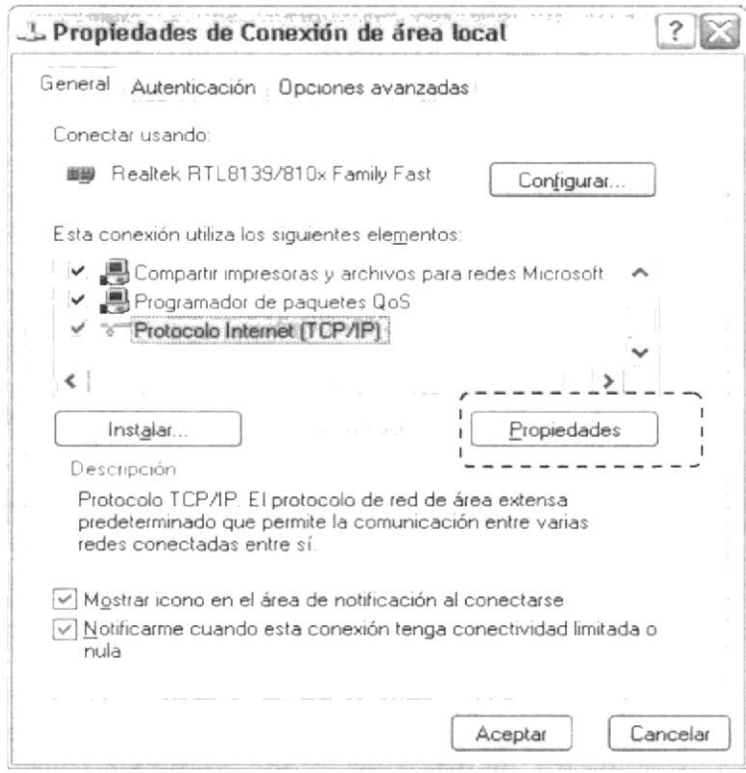


Figura 6-166: Propiedades de Conexión de área local

Habilite: Obtener una dirección IP automáticamente. Obtener la dirección del servidor DNS automáticamente.

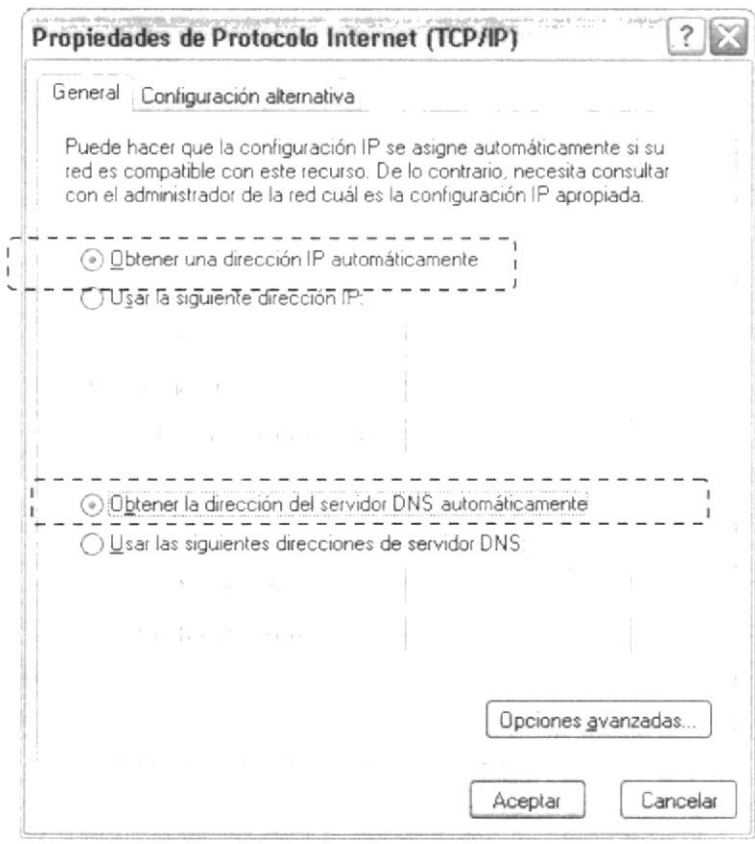


Figura 6-167: Estableciendo IP automática en cliente Windows

De clic en inicio – ejecutar, escriba cmd, para entrar a la consola de comandos.

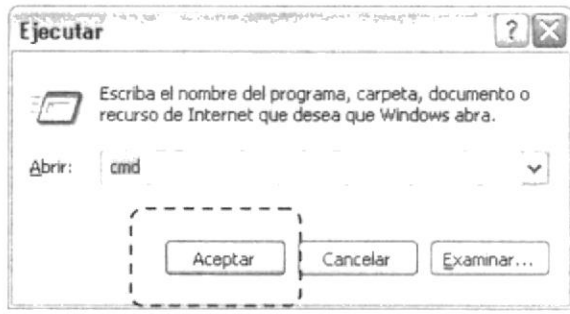


Figura 6-168: Ejecutar consola D.O.S.

Aplique el comando **ipconfig /renew** para que tome la dirección que asignará el servidor DHCP. Digite **ipconfig** para observar la nueva dirección IP.

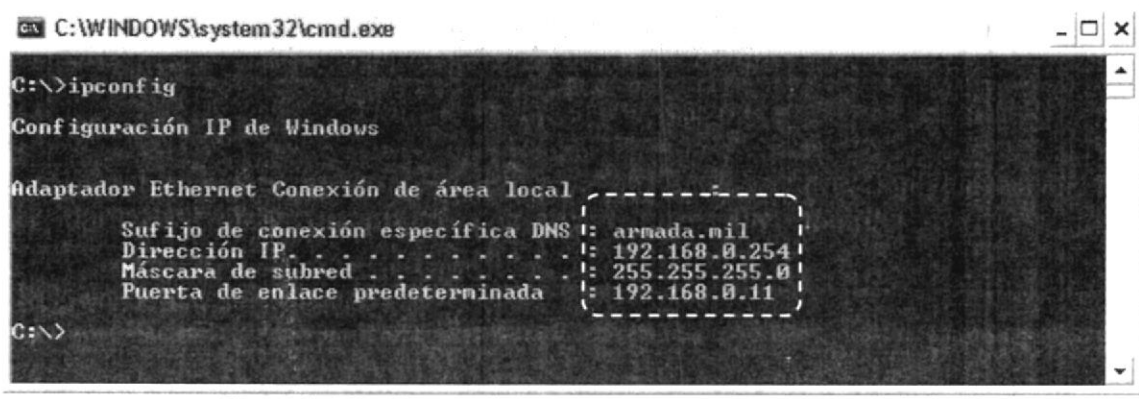


Figura 6-169: Obteniendo IP automática en consola de D.O.S.

En modo gráfico de doble clic sobre conexiones de red y ubíquese en la pestaña de soporte.

6.25 FIREWALL

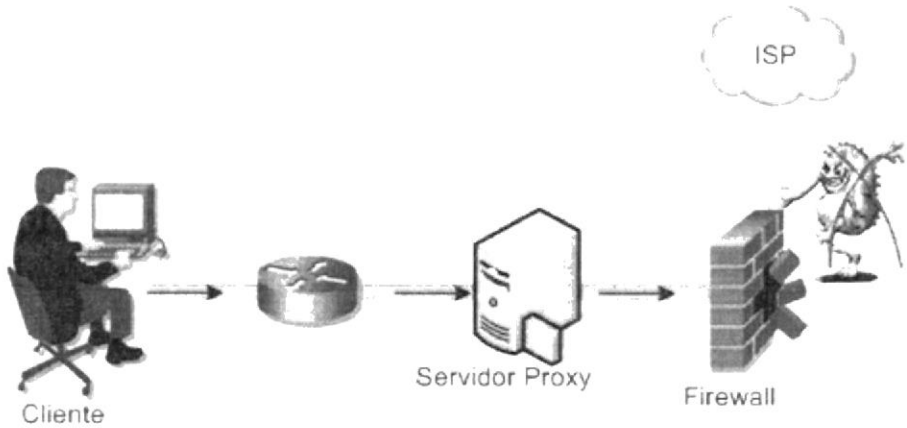


Figura 6-171: Diagrama de Firewall

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el módem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes.
Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.
De este modo un firewall puede permitir desde una red local hacia Internet servicios de Web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la Web, (si es que poseemos un servidor Web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde

Tipos de cortafuegos

Cortafuegos de capa de red o de filtrado de paquetes

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

Cortafuegos de capa de aplicación

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

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

Limitaciones de un cortafuegos

- ✓ Un cortafuegos no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

- ✓ El cortafuegos no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El cortafuegos no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.

- ✓ El cortafuegos no puede proteger contra los ataques de Ingeniería social

- ✓ El cortafuegos no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real esta en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

- ✓ El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet. Instalar un firewall es en buena medida una buena solución para protegerse de ataques a una red interna o de usuarios no deseados. Actualmente, el Kernel de Linux (Por ejemplo LinuxPPP 6.2, Red Hat™ 6.2) soporta filtrado de paquetes, que pueden se utilizados para implementar un sencillo firewall.

Las cadenas de un firewall no son mas que reglas que se utilizan para que el paquete cumpla con alguna de ellas y en un cierto orden. Esto quiere decir que el paquete debe de cumplir con alguna regla. La regla determina que es lo que va a suceder con el paquete que ha sido recibido. Si el paquete no coincide la próxima regla determinara que hacer con el. Si llega al final de esta regla se utilizara la política que se encuentra por omisión.

Existen tres tipos de reglas por omisión que se utilizan:

- **INPUT:** Aceptación de paquetes de entrada. Todos los paquetes que vienen de una de las interfaces de la red local son revisadas por la regla de entrada. Si el paquete no coincide con alguna de las reglas de entrada este los rechaza.

- **OUTPUT:** Esta regla define los permisos para enviar paquetes IP. Todos los paquetes se encuentran listos para ser enviados a una de las interfaces de la red local y son revisados por la regla de salida. Si el paquete no coincide con alguna de las reglas el paquete es rechazado.

- **FORWARD:** Esta regla define los permisos para el envío del paquete a otro sitio. Todos los paquetes se envían a un equipo remoto. Nuevamente, si el paquete no coincide con alguna de las reglas este paquete es rechazado.

Las reglas en un Firewall se crean de igual forma como se a mencionado con anterioridad, tenemos una condición que debe de cumplirse para que el paquete de entrada o salida tenga los permisos para poder llegar a su destino. Los valores que debemos de utilizar para crear una regla se muestran a continuación:

- **ACCEPT:** Este valor quiere decir que permite pasar a los paquetes que pasan a través del Firewall. Todos aquellos paquetes que cumplan con la regla de entrada podrán tener acceso de entrada o salida.
- **DROP:** Este valor quiere decir que los paquetes no podrán ser aceptados. Aquellos paquetes que coincidan con la regla (DROP) no podrán llegar a su destino serán eliminados.

- **REJECT:** Es casi igual al valor DROP pero es mas fina la forma de negar el acceso de los paquetes. Por ejemplo los mensajes ICMP se envían de regreso al originador de este paquete, indicándole que este ha sido rechazado.

- **MASQ:** Este valor es únicamente utilizado para el envío y cadenas definidas por el usuario y puede ser utilizado únicamente si el kernel es compilado con el soporte de enmascaramiento. Con eso, los paquetes serán enmascarados como si se tratara del equipo maestro (tu maquina que tiene instalado el Firewall, para que entiendas). Desafortunadamente, los paquetes que regresen del equipo remoto al que se enviaron los paquetes enmascarados, deben de pasar por el equipo maestro y este debe desenmascarar el paquete para que pueda ser recibido por su originador.

- **REDIRECT:** Este valor indica que únicamente los paquetes serán redireccionados de la entrada las cadenas definidas por el usuario y pueden ser únicamente utilizados cuando el kernel es compilado con el soporte de "Transparent Proxy". Con esto, los paquetes puedes ser redireccionados al soquet local de la maquina maestro siempre y cuando estos sean enviados desde un host remoto.

- **RETURN:** Este valor es definido por las colas, esto quiere decir que el procesamiento de paquetes continuara en la próxima regla de la siguiente cadena.

  Las condiciones de las declaraciones se vuelven más complejas a medida que se tienen diversos tipos de paquetes que filtrar. Los paquetes IP se agrupan por tipo de paquete, los cuales tienes características semejantes entre ellos, así con esto, podemos determinar más fácilmente que paquetes coinciden con alguna regla o no. Las reglas contienen un conjunto de valores para cada uno de los parámetros.

- **PROTOCOL:** El protocolo de paquetes es revisado. El protocolo especificado puede ser uno de los siguientes: TCP, UDP, ICMP o todos ellos, de igual forma pueden ser valores numéricos que representan a cada uno de estos protocolos y

los hace diferentes uno de otro. Los nombres y valores de estos protocolos se almacenan en el archivo /etc/protocols

- **SOURCE:** De donde provienen los paquetes. La información fuente contiene la dirección IP que muestra la procedencia o un rango de direcciones al igual que la mascara de esas redes, estas también pueden incluir la especificación del puerto o ICMP. Este puede proporcionar el nombre del servicio que se solicita el número del puerto, el valor número de ICMP o el nombre del servicio ICMP que se solicita.

- **DESTINATION:** Es el mismo valor como en el parámetro *SOURCE* pero esta vez se especifica a donde el paquete va a ser enviado.

- **INTERFACE:** Los mismos valores como en el *PARAMETRO SOURCE* pero esta vez indica por que interfaces el paquete debe de ser enviado.

- **FRAGMENT:** Esto significa que la regla únicamente observara fragmentos de un paquete completo.

- **SYN BIT SET:** Únicamente coinciden paquetes del tipo TCP y si se encuentra habilitado y el SYN BIT a ACK y FIN se encuentran limpios. Estos pueden ser paquetes utilizados para la inicialización de conexión de una petición TCP; Por ejemplo, el bloqueo de paquetes de entrada hacia una interfase que realiza conexiones del tipo TCP. Esta opción es útil cuando el tipo de protocolo es TCP.

En el firewall, tenemos los siguientes comandos:
iptables – L el cual nos lista las reglas que se están ejecutando en el firewall
iptables – F el cual da de baja a todas las reglas del firewall
iptables – A el cual nos permite añadir una regla
iptables – D el cual nos permite borrar una regla

Para lo cual tenemos los puertos más conocidos:

- ✓ ftp = 21
- ✓ sch = 22
- ✓ telnet = 23
- ✓ smtp = 25
- ✓ dns = 53
- ✓ http = 80
- ✓ pop3 = 110
- ✓ ping = icmp

6.25.1 REQUERIMIENTOS DE CONFIGURACIÓN FIREWALL

- Tener instalado el sistema Linux Fedora Core 3
- Tener una IP estática en el Server Linux
- Tener configurada la tarjeta de red, tanto en el Server Linux como en el cliente.
- Tener instalado el paquete iptables

6.25.2 VERIFICACIÓN EN EL CLIENTE WINDOWS

De clic en inicio – ejecutar y escriba cmd, para entrar a la consola de comandos del cliente. Como no tiene configurado aún el Firewall tendrá estos privilegios.

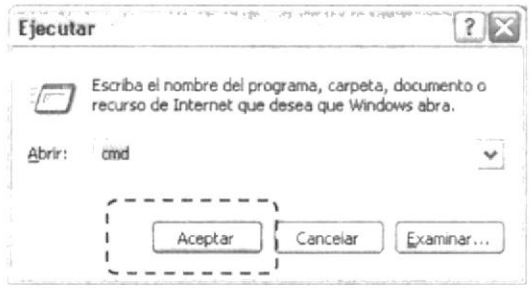


Figura 6-172: Ejecutar consola D.O.S.

Realice un ping al servidor Linux y obtendrá respuesta.Digite: ping 192.168.0.11

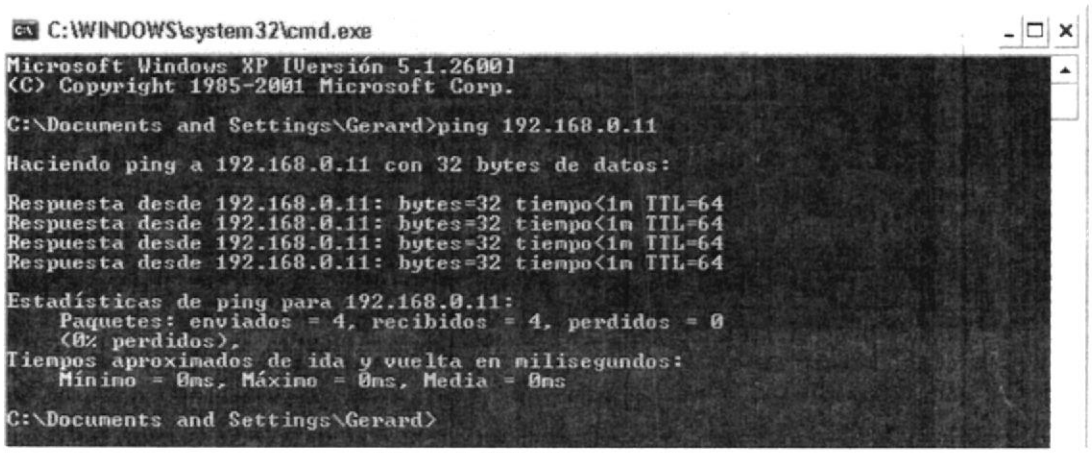


Figura 6-173: Ping permitido

Realice un telnet al servidor Linux. Digite: telnet 192.168.0.11

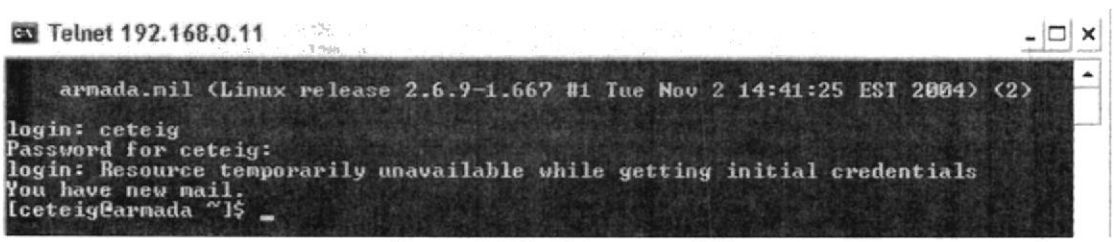


Figura 6-174: Telnet permitido

Finalmente realice un Ftp al servidor Linux. Digite: ftp 192.168.0.11

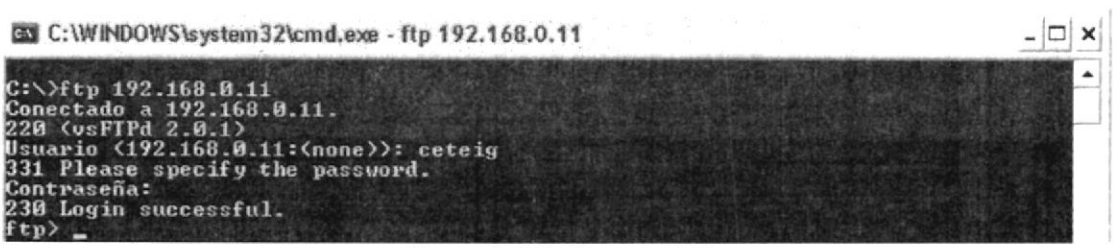


Figura 6-175: Ftp permitido

6.25.3 CONFIGURACIÓN FIREWALL

Verifique si está instalado el paquete de iptables de la siguiente manera:
[root@armada /] # rpm –q iptables

Empiece por dar de baja a todas las reglas del firewall y aplique el siguiente comando:
iptables –F
Y liste para comprobar que en realidad se dieron de baja a las reglas
iptables –L

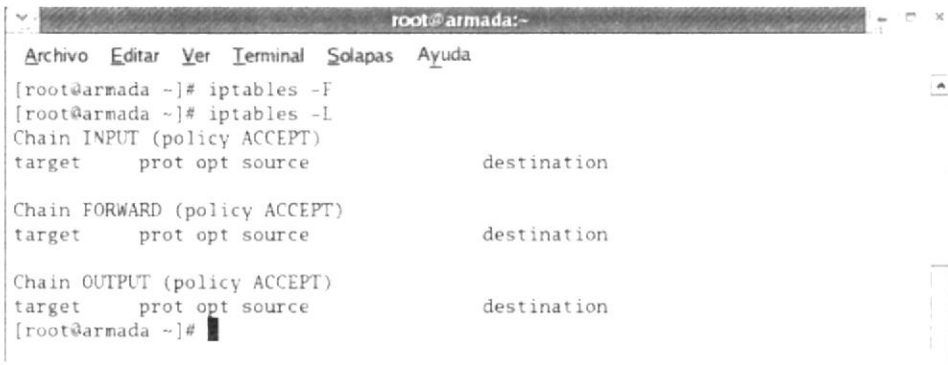


Figura 6-176: Bajar reglas de Firewall

Ahora proceda a añadir las reglas, las cuales serán:

- ✓ Bloquear ping
- ✓ Bloquear telnet
- ✓ Permitir ftp

Agregue las reglas digitando lo siguiente:

iptables –A INPUT –s 192.168.0.0/24 **–d** 192.168.0.11/32 **–p icmp –j DROP**

añadir red origen red destino protocolo acción

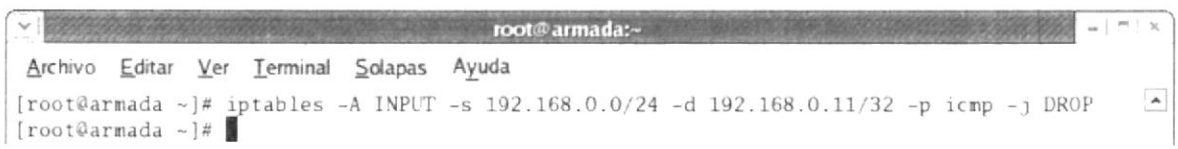


Figura 6-177: Aplicando regla para bloquear ping

iptables –A INPUT –s 192.168.0.0/24 **–d** 192.168.0.11/32 **–p tcp --dport 23 –j DROP**

añadir red origen red destino protocolo puerto acción

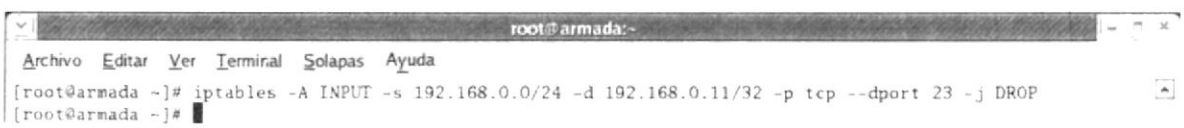


Figura 6-178: Regla para bloquear telnet

iptables –A INPUT –s 192.168.0.0/24 **–d** 192.168.0.11/32 **–p tcp --dport 21 –j ACCEPT**

añadir red origen red destino protocolo puerto acción

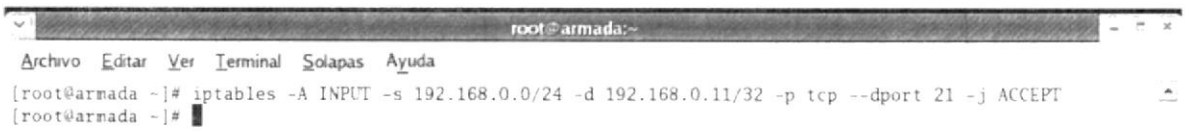


Figura 6-179: Regla para permitir Ftp

6.25.4 CARGAR SERVICIOS FIREWALL AL INICIAR EL SISTEMA

Digite **setup** en la Terminal y habilite el servicio **iptables** para que se ejecute automáticamente al iniciar Fedora.
Proceda a entrar en servicios del sistema, marcándolo y luego con la tecla tab ubíquese en ejecutar una herramienta y presione la tecla enter. Con las flechas direccionales muévase y una vez seleccionado el servicio con la tecla tab ubíquese en OK y acepte los cambios presionando enter.

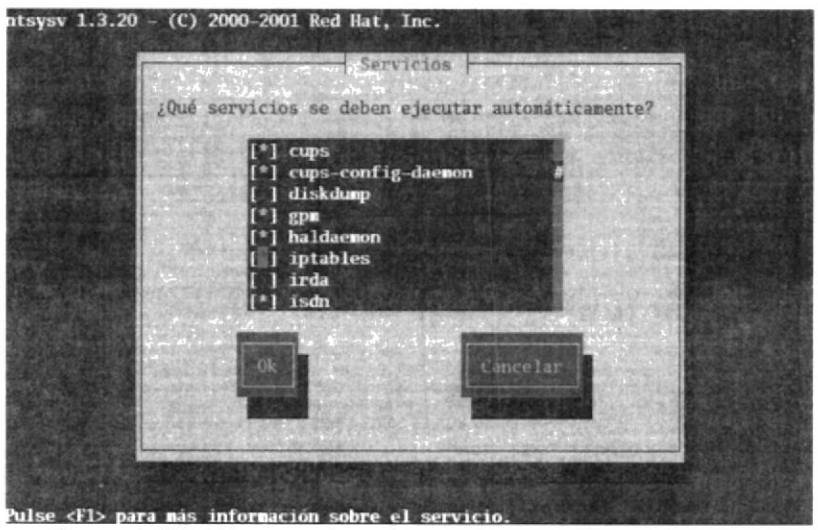


Figura 6-180: Ejecutar el servicio de Firewall automáticamente

6.25.5 RESTRICCIONES EN EL CLIENTE WINDOWS

De clic en inicio – ejecutar y escriba cmd, para entrar a la consola de comandos del cliente. El Firewall ya está configurado y observará las restricciones y privilegios.

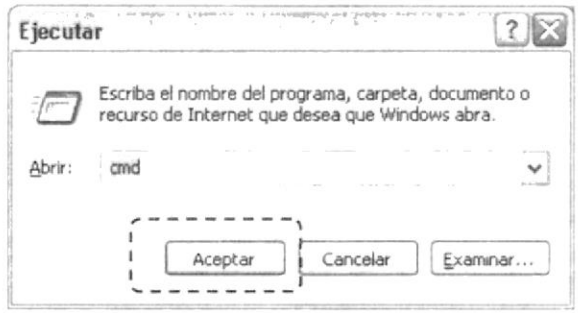


Figura 6-181: Ejecutar consola D.O.S.

Realice un ping al servidor Linux (192.168.0.11), el firewall lo bloqueará.

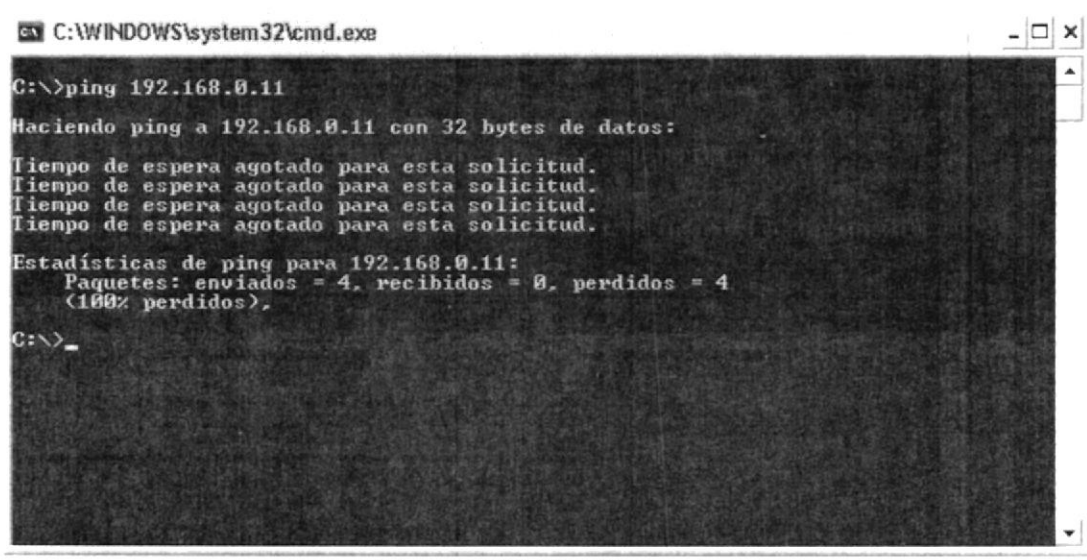


Figura 6-182: Ping bloqueado

Luego realice un telnet al servidor Linux, el firewall lo bloqueará.

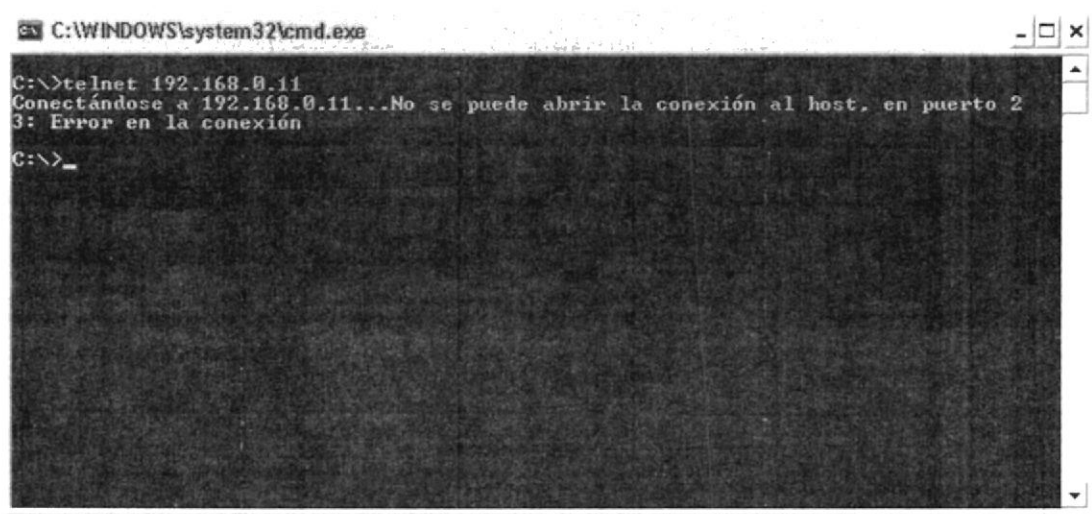


Figura 6-183: Telnet bloqueado

Finalmente realice un Ftp al servidor Linux, el firewall lo permitirá

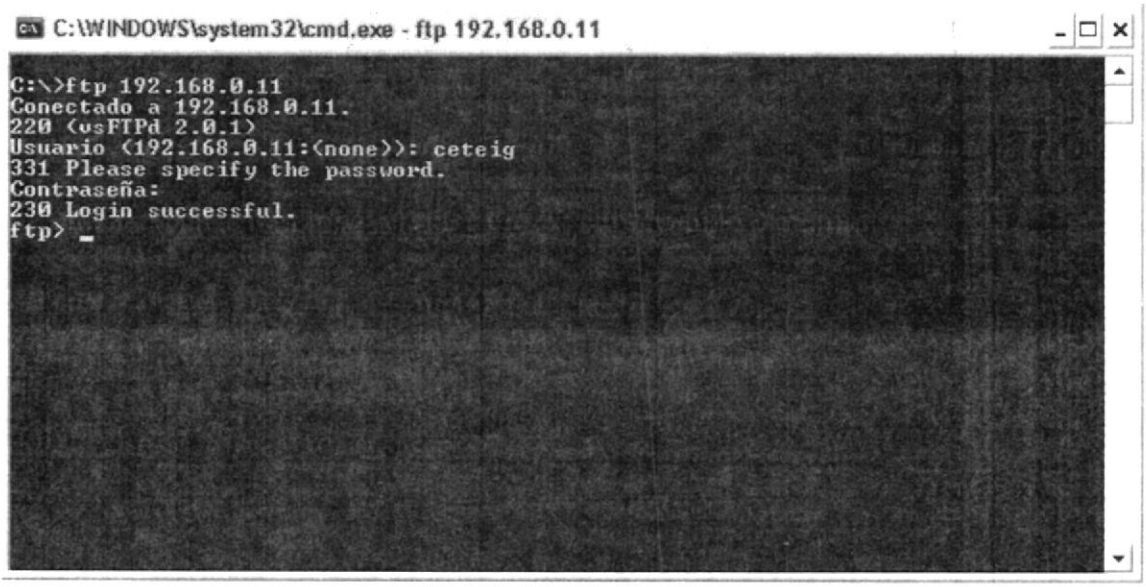


Figura 6-184: Ftp permitido

CAPÍTULO 7

CONFIGURACIÓN DE DISPOSITIVOS

7 CONFIGURACIÓN DE DISPOSITIVOS

7.1 ROUTER

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio. Cuenta con una CPU, memoria, bus de sistema y distintas interfaces de entrada/salida.
Los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.
Los routers necesitan el software denominado IOS (Sistema Operativo de Internetworking) 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.

7.1.1 FUNCIONES DEL ROUTER

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

7.1.2 TECNOLOGÍAS

Las tecnologías que soportan los routers son las siguientes:

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

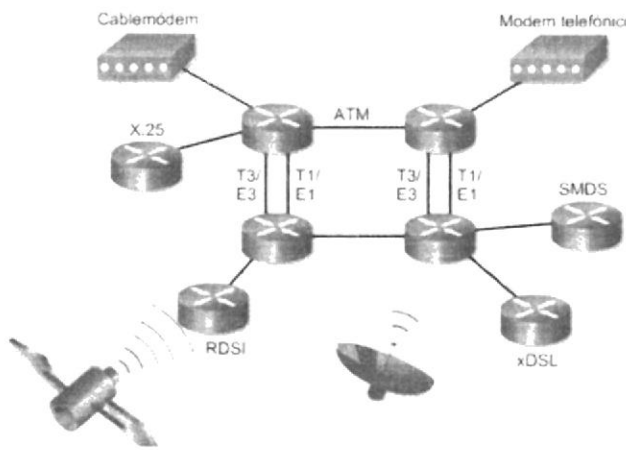


Figura 7-1: Tecnologías soportadas por routers

7.1.3 COMPONENTES INTERNOS DEL ROUTER

Los principales componentes internos del router son:

- ✓ La memoria de acceso aleatorio (RAM).
- ✓ La memoria de acceso aleatorio no volátil (NVRAM).
- ✓ La memoria flash.
- ✓ La memoria de sólo lectura (ROM) y las interfaces.

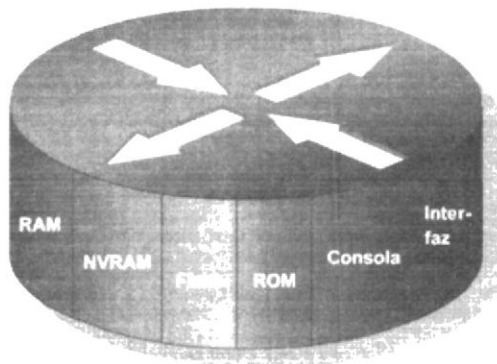


Figura 7-2: Componentes internos de un router

7.1.3.1 MEMORIA RAM

- ✓ 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.

7.1.3.2 MEMORIA NVRAM

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

7.1.3.3 MEMORIA FLASH

- ✓ 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)

7.1.3.4 MEMORIA ROM

- ✓ 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.

7.1.4 COMPONENTES EXTERNOS DEL ROUTER

Enter los componentes externos tenemos:

- ✓ Puertos.
- ✓ Interruptor de encendido.
- ✓ Entrada de Corriente.
- ✓ Leds.

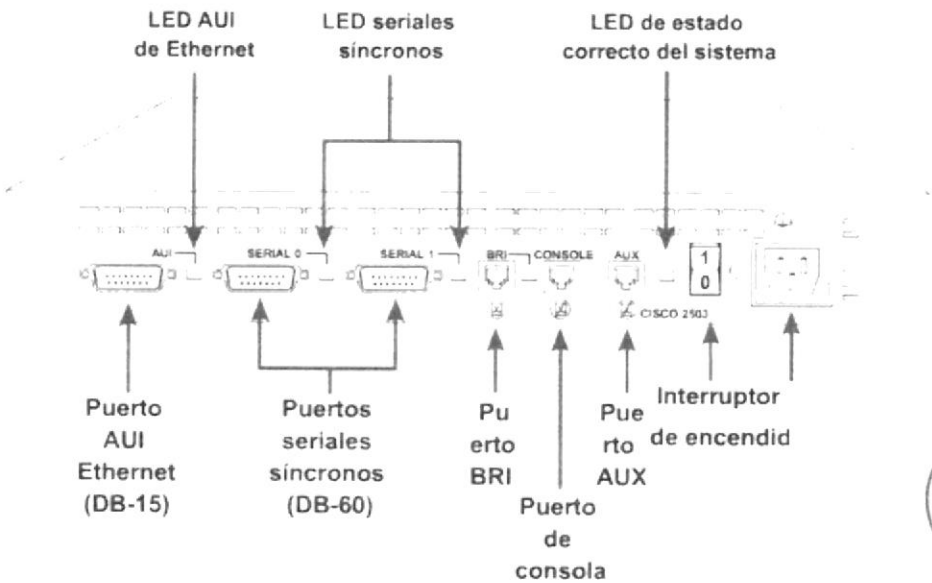


Figura 7-3: Componentes externos de un router

7.1.4.1 INTERFACES

Son puertos de conexiones que se encuentran en la parte externa posterior del mismo. Existen 3 clases de interfaces:

- ✓ Conexión LAN (Red de área local).
- ✓ Conexión WAN (Red de área amplia).
- ✓ Consola AUX.

7.1.5 CONEXIÓN DEL DISPOSITIVO

7.1.5.1 REQUERIMIENTOS.

- ✓ Computador con Tarjeta de Red 10/100 Mbps, Puerto Com disponible.
- ✓ Cable de Consola.
- ✓ Router.

7.1.5.2 CONEXIÓN FÍSICA

Para poder conectarse al Router y proceder a configurarlo deberá usar un cable Rollover RJ45.

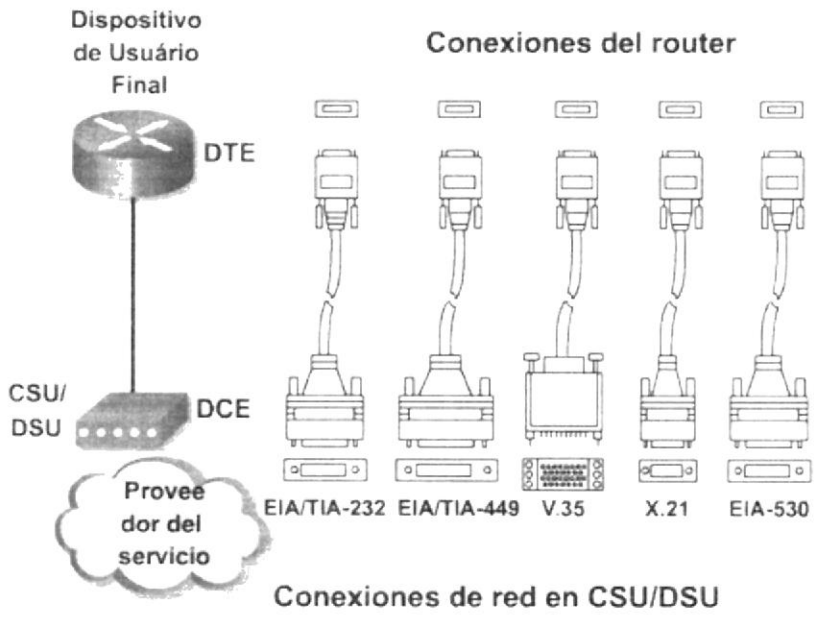


Figura 7-4: Tipos de conexiones físicas en un router

7.1.6 CONFIGURACIÓN EN HYPER TERMINAL

Para poder configurar el dispositivo tendrá que abrir el software Hyper Terminal que viene incluido en el Sistema Operativo Windows.

- Ingrese al Hyper Terminal eligiendo: Inicio, Todos los Programas, Accesorios, Comunicaciones, Hyper Terminal.

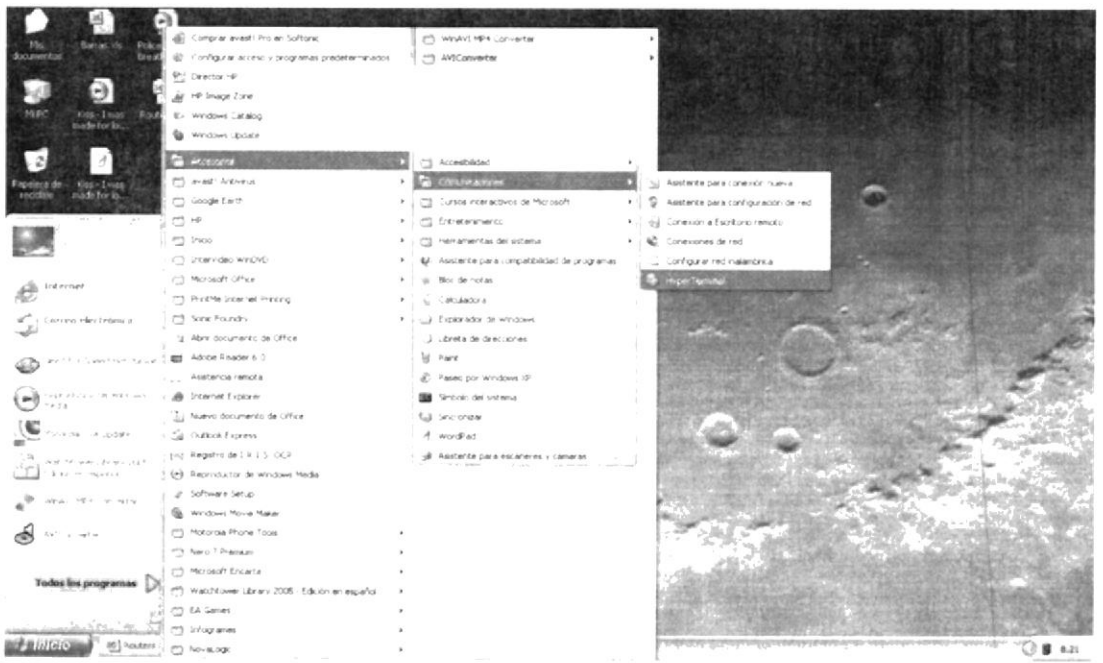


Figura 7-5: Ingresando a Hyper Terminal

- Si abre por primera vez el Hyper Terminal aparecerá una pantalla mostrando si desea que este software sea el predeterminado, elija su preferencia.

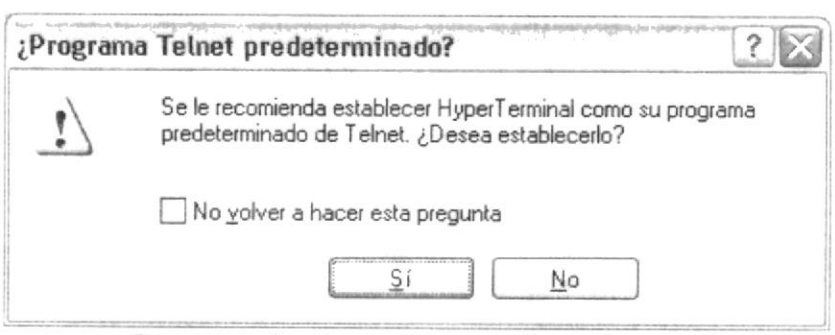


Figura 7-6: Cuadro de diálogo de Hyper Terminal

- Descripción de la conexión: Le pedirá que escriba un nombre y un icono para la conexión que establecerá, de clic en el botón aceptar.

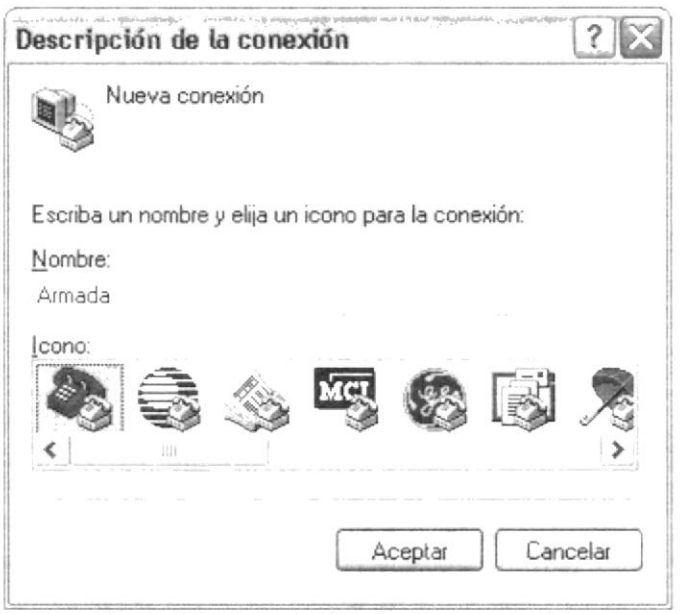


Figura 7-7: Descripción de nueva conexión

- Conectar a: Elija el puerto que vaya a usar para la conexión del dispositivo.

Figura 7-8: Asignando puerto de conexión

- Configuración del Puerto: Asigne los parámetros para el puerto de Consola.

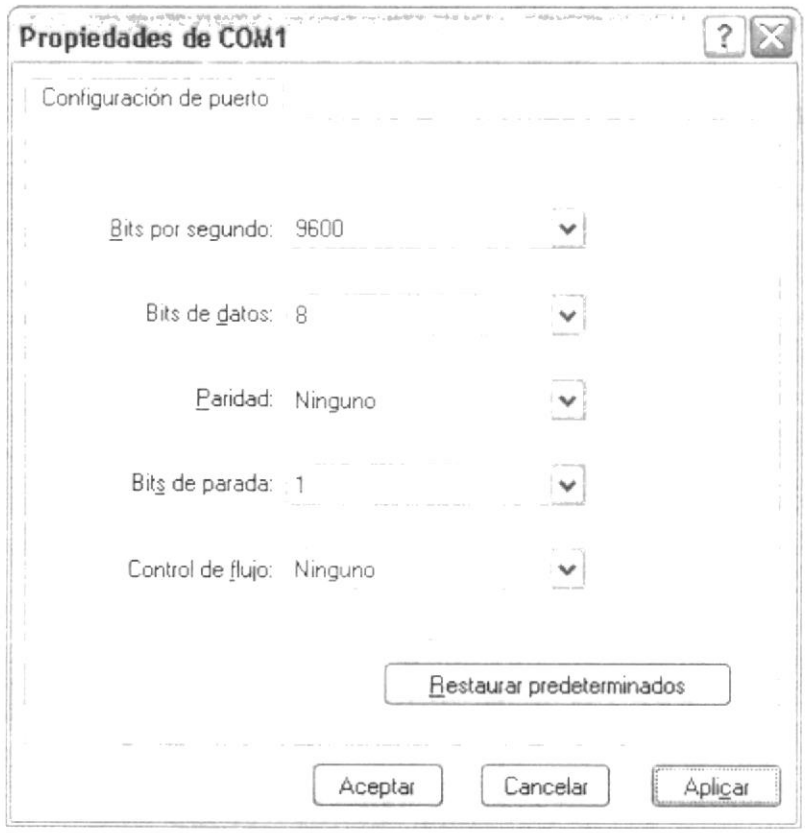


Figura 7-9: Configuración de puerto de conexión

- ✓ Bits por Segundo: Son los números de Bits transmitidos por segundo, este nos indica la velocidad de transmisión de los datos.

- ✓ Bits de Datos: Son los bits que conforman una palabra, configurará el procesamiento de datos al pasar por el Hyper Terminal.

- ✓ Paridad: Es un bit adicional, utilizado para comprobar si hay errores en los grupos de bits de datos transferidos, dentro de un equipo o entre equipos en conexiones asíncronas. En las conexiones de módem se suele utilizar 1 bit de paridad para comprobar la exactitud con la que se transmite cada carácter.

- ✓ Bits de parada: Se agrupan en tramas en los paquetes de datos de las comunicaciones asíncronas. Indican al módem de recepción que se ha enviado un byte. Los protocolos asíncronos actuales no requieren de más de un bit de parada.

- Pantalla de configuración: Una vez configurado el puerto, aparecerá esta pantalla, en la cual proceda a configurar el router ingresando los comandos respectivos.

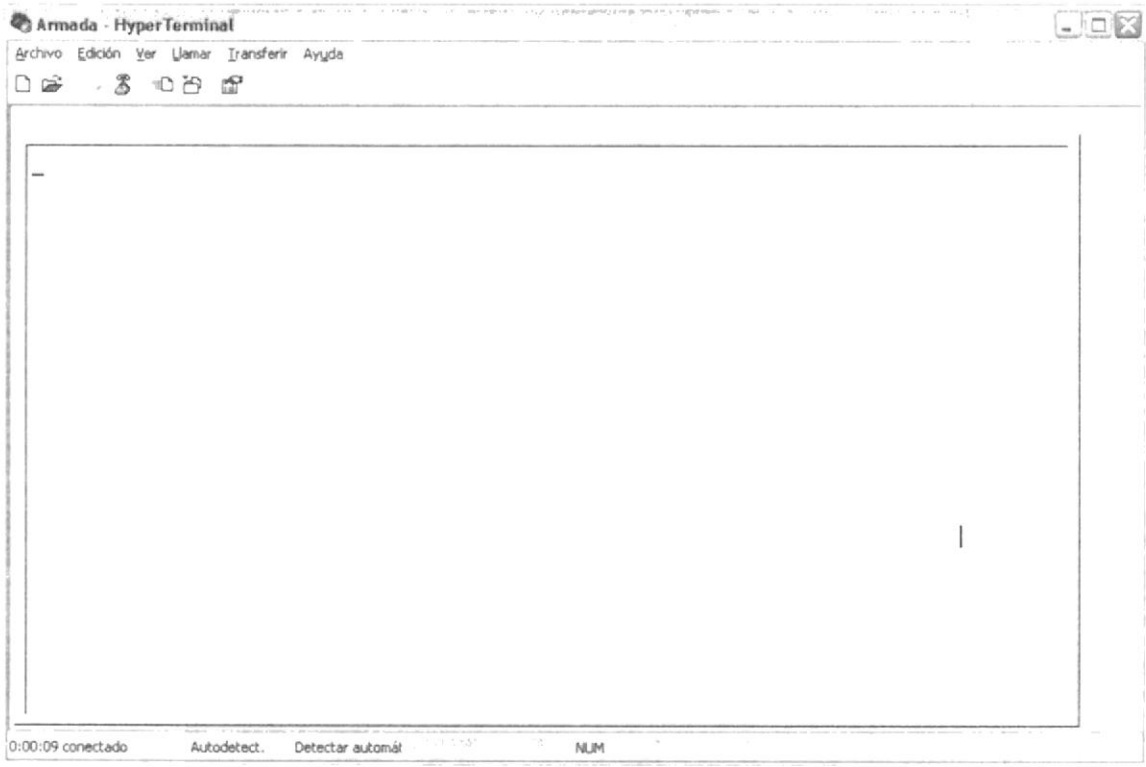


Figura 7-10: Pantalla de configuración en Hyper Terminal

✓ Si da clic en cerrar en la ventana aparecerá el siguiente cuadro de diálogo.

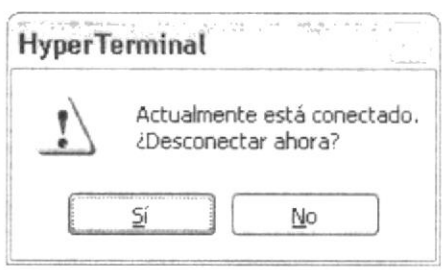


Figura 7-11: Desconectar conexión

- Si da clic en Sí pedirá guardar el nombre de la conexión.
- Al dar clic en NO o CANCELAR regresará a la pantalla principal de configuraciones.

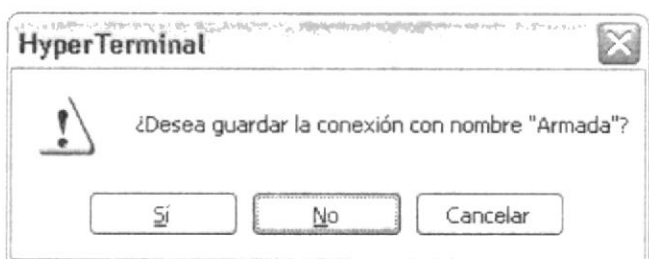


Figura 7-12: Guardar conexión

7.1.7 MODOS DE OPERACIÓN EN LOS ROUTERS

La interfaz de línea de comandos es una estructura jerárquica, la misma que requiere el ingreso a distintos modos para realizar tareas particulares.

Estos modos de operación son los siguientes:

- Modo EXEC usuario.
- Modo EXEC privilegiado.
- Modo de configuración global.
- Modo de configuración específica.

7.1.7.1 MODO EXEC USUARIO

Solo permite una cantidad determinada de comandos básicos. Es un modo de visualización solamente, este nivel no permite ningún comando que pueda cambiar la configuración del router. Para reconocer que se esta en este modo observe el prompt de la siguiente manera:

Router>

7.1.7.2 MODO EXEC PRIVILEGIADO

Este modo da acceso a varios comandos del router. Se puede configurar una contraseña, la cual será solicitada al usuario antes de dar acceso a este modo.
Para ingresar a este modo debe estar en el modo EXEC usuario y digitar el comando **enable** o abreviado **ena** seguido de la tecla enter.
Para reconocer que se esta en este modo observe el prompt de la siguiente manera:

Router#

Para obtener ayuda y saber de los diferentes comandos estando en este modo digite un signo de interrogación "**?**" seguido de la tecla enter y mostrará información de ayuda de los diferentes comandos.

7.1.7.3 MODO DE CONFIGURACIÓN GLOBAL

En este modo puede ingresar a realizar configuraciones específicas del router.
Solo se puede ingresar a este modo estando previamente en el modo EXEC privilegiado.

En este modo se podrá realizar las configuraciones más avanzadas del router, es necesario tener conocimientos para operar en este modo.

Los modos específicos a los que se tiene acceso son los siguientes:

- Interfaces.
- Subinterfaces.
- Controlador.
- Línea.
- Línea de Mapa.
- Clase de Mapa.
- Router.
- Mapas de Enrutamiento.

Para ingresar a este modo debe estar en el modo EXEC privilegiado y digitar el comando **configure terminal** o abreviado **conf ter** seguido de un enter.
Para reconocer que esta en este modo observe el prompt de la siguiente manera:

Router(config)#

Para regresar a el modo privilegiado digite **exit** o la combinación de teclas **Ctrl.-Z**.

7.1.8 COMANDOS SHOW

Varios son los comandos con esta sentencia, son de gran utilidad y nos ayudan para examinar el contenido de los archivos del router y para diagnosticar posibles fallas. Se utilizan estos comandos en modo privilegiado, como en modo usuario.
A continuación explicamos los más útiles:

- show history: Presenta un historial de los comandos ingresados.
- show users: Presenta todos los usuarios conectados al router.
- show clock: Presenta la hora fijada en le router.
- show hosts: Presenta la lista nombres de hosts con sus direcciones.
- show flash: Presenta información acerca de la memoria flash.
- show version: Presenta información de la imagen del IOS que se esta ejecutando en el router. Además puede ver cuanto tiempo de encendido tiene el dispositivo.
- show controllers serial 0: muestra información del hardware, en este caso de nuestra interface serial 0, además nos indica si la serial es DCE o DTE.
- show interfaces: Presenta toda la información estadística de todas las interfaces del router. Aquí puede observar las direcciones IP que hemos asignado a nuestras interfaces. Digitando el comando seguido de la interface a consultar.
- show protocols: Presenta el estado de los protocolos y nos indica si están levantados o caídos.
- show running-configuration: Presenta el contenido del archivo de configuración activo o la configuración de una interfaz específica.
- show ip route: Presenta los protocolos de enrutamiento junto a sus respectivas interfaces, formando la tabla de ruteo.

7.1.9 ASIGNACIÓN DE NOMBRE AL ROUTER

Se recomienda identificar a cada dispositivo con su respectivo nombre para la posterior identificación., se lo hace ingresando a la configuración global y digitando el comando *hostname* seguido del nombre en este caso MATRIZ.

Router>

Ingrese al modo privilegiado.

Router>*enable*

Ingrese al modo de configuración global.

Router#*configure terminal*

Asigne nombre con el comando hostname seguido del mismo.

Router (config)#*hostname MATRIZ*

comando nombre del router

Salga con Ctrl.- Z.

MATRIZ (config)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#*wr*
Building configuration...
[OK]

MATRIZ#

7.1.10 ASIGNACIÓN DE CONTRASEÑA AL ROUTER

La contraseña restringirá el acceso a los dispositivos, dando el acceso al debido administrador, para asignar la contraseña debe habilitar el acceso remoto y por línea de consola.

Línea de comando

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>*enable*

Ingrese al modo de configuración global.

MATRIZ#*configure terminal*

Habilite el acceso por consola con el comando line console 0.

MATRIZ (config)#*line console 0*

Ingrese el comando password seguido de la contraseña.

MATRIZ (config-line)#*password cisco*

comando contraseña del router

Active el inicio con la contraseña.

MATRIZ (config-line)#*login*

Salga con Ctrl.- Z.

MATRIZ (config)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#*wr*
Building configuration...
[OK]

MATRIZ#

Línea de acceso remoto

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>*enable*

Ingrese al modo de configuración global.

MATRIZ#*configure terminal*

Habilite el acceso remoto con el comando line vty 0 4.

MATRIZ (config)#*line vty 0 4*

Ingrese el comando password seguido de la contraseña.

MATRIZ (config-line)#*password espol*

comando contraseña del router

Active el inicio con la contraseña.

MATRIZ (config-line)#*login*

Salga con Ctrl.- Z.

MATRIZ (config)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#*wr*
Building configuration...
[OK]

MATRIZ#

7.1.11 CONFIGURACIÓN DE INTERFACES DEL ROUTER

Para proceder a configurar las diferentes interfaces del router debe de tener determinadas las IP correspondientes con sus respectivas máscaras de subred, para cada tipo de interfaz sea esta serial o ethernet.

Interfaces Seriales

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>enable

Ingrese al modo de configuración global.

MATRIZ#configure terminal

Ingrese el comando interface seguido de la interfaz.

MATRIZ (config)# interface serial 0

comando interfaz número de la interfaz

Asigne la IP a la interfaz con el comando ip address.

MATRIZ (config-if)#ip address 192.168.3.2 255.255.255.252

comando dirección IP máscara de subred

Levante la interfaz con el comando no shutdown.

MATRIZ (config-if)#no shutdown

Salga con Ctrl.- Z.

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

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#wr
Building configuration...
[OK]

MATRIZ#

Interfaces Ethernet

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>*enable*

Ingrese al modo de configuración global.

MATRIZ#*configure terminal*

Ingrese el comando interface seguido de la interfaz.

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

comando interfaz número de la interfaz

Asigne la IP a la interfaz con el comando ip address.

MATRIZ (config-if)#*ip address 192.168.3.9 255.255.255.248*

comando dirección IP máscara de subred

Levante la interfaz con el comando no shutdown.

MATRIZ (config-if)#*no shutdown*

Salga con Ctrl.- Z.

MATRIZ (config)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#*wr*
Building configuration...
[OK]

MATRIZ#

Se puede tener interfaces ethernet o fastethernet en nuestro router, para lo cual solo cambie la sentencia del comando dependiendo del tipo de interfaz que vaya a configurar.

Subinterfaces Ethernet

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>*enable*

Ingrese al modo de configuración global.

MATRIZ#*configure terminal*

Ingrese el comando interface seguido de la interfaz.

MATRIZ (config)# *interface fastethernet 1/0.1*

comando interfaz número de la subinterfaz

Agregue un comentario con el comando description.

MATRIZ (config-subif)#*description VLAN VENTAS*

comando comentario

Habilite el protocolo dot1q para comunicar la VLAN.

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

comando protocolo número de VLAN

Asigne la IP a la subinterfaz con el comando ip address.

MATRIZ (config-subif)#*ip address 192.168.2.113 255.255.255.240*

comando dirección IP máscara de subred

Salga con Ctrl.- Z.

MATRIZ (config-subif)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#*wr*
Building configuration...
[OK]

MATRIZ#

7.1.12 PROTOCOLO DE ENRUTAMIENTO RIP VERSION 2

RIP son las siglas de Routing Information Protocol (Protocolo de información de encaminamiento). Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers, aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

Breve Historia
El origen del RIP fue el protocolo de Xerox, el GWINFO. Una versión posterior, fue conocida como routed, distribuida con Berkeley Standard Distribution (BSD) Unix en 1982. RIP evolucionó como un protocolo de enrutamiento de Internet, y otros protocolos propietarios utilizan versiones modificadas de RIP. El protocolo Apple Talk Routing Table Maintenance Protocol (RTMP) y el Banyan VINES Routing Table Protocol (RTP), por ejemplo, están los dos basados en una versión del protocolo de enrutamiento RIP. La última mejora hecha al RIP es la especificación RIP 2, que permite incluir más información en los paquetes RIP y provee un mecanismo de autenticación muy simple.

Descripción
El Protocolo de Información de Enrutamiento (RIP) es un protocolo de vector-distancia que utiliza un contador de saltos como métrica. RIP es muy usado para enrutar tráfico en redes globales como un protocolo de gateway interior (IGP), lo que significa que realiza el enrutamiento en sistemas autónomos. Los protocolos de gateway exterior, como el BGP (Border Gateway Protocol), realizan el enrutamiento entre dos sistemas autónomos.

Actualización de Enrutamiento
El protocolo RIP envía mensajes de actualización de enrutamiento cuando detecta que la topología de la red ha cambiado. Cuando un router recibe un mensaje de actualización que incluye cambios no registrados, este actualiza su propia tabla para asentar la nueva ruta. El valor de la métrica para el mensaje es aumentado por el router en uno, y el origen es indicado como el próximo salto. Los enrutamientos con RIP utilizan solamente la mejor ruta (la que tenga la métrica mas baja) hacia un destino. Luego de que un router actualiza sus tablas, inmediatamente comienza a transmitir la información de actualización de enrutamiento a los routers vecinos. Estas actualizaciones son enviadas independientemente de las actualizaciones programadas que RIP envía.

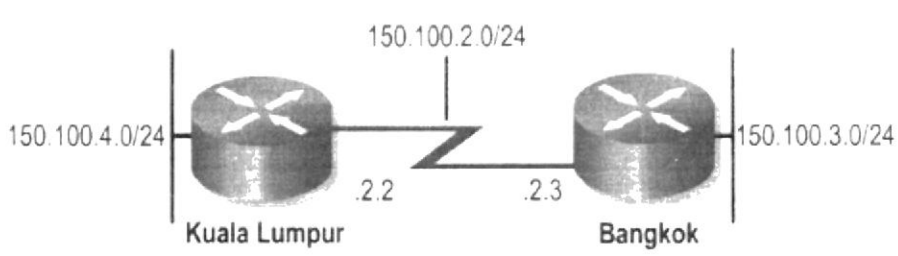


Figura 7-13: Diagrama enrutamiento RIP

RIP Timers
RIP utiliza una gran cantidad de relojes para regular su perfomance. Entre ellos se incluyen los routing-update timer, route timeout y route-flush timer. Los routing-update timer establecen el intervalo entre las actualizaciones de tablas de enrutamiento periódicas. Por lo general, este valor esta seteado en 30 segundos, con un rango muy pequeño de segundos agregados a cada tiempo para prevenir colisiones. Cada entrada en las tablas de enrutamiento tienen un route timeout timer asociado con ellas. Cuando el route timeout timer expira, la ruta es señalada como invalida, pero no es borrada de la tabla hasta que expira el route-flush timer.

Métrica de Enrutamiento de RIP
RIP utiliza una métrica simple para determinar las distancias entre un origen y un destino. Esta métrica se mide en "saltos", cada salto esta determinados por cada router que atraviesa la información. Con cada salto desde el origen hacia el destino es aumentado en uno un contador. Cuando un router recibe una actualización de enrutamiento que contiene una nueva ruta o algún cambio con respecto a sus propias tablas, el router modifica sus tablas, y luego agrega un valor a la métrica, esto indica que las tablas han sido actualizadas, la dirección IP del origen será utilizada para el próximo salto.

Estabilidad de RIP
Para ajustarse rápidamente a los cambios en la red, RIP especifica un número de parámetros de estabilidad que son comunes a muchos protocolos de enrutamiento. Rip, por ejemplo, implementa el llamado Horizonte Dividido y el mecanismo de Temporizadores de espera para prevenir que se propague información de enrutamiento incorrecta. Además, el protocolo RIP previene los loops de enrutamiento utilizando el método de Cuenta al infinito.

Prevención de loops
El protocolo Rip previene loops continuos implementando un límite de saltos desde el origen al destino final. El número máximo de saltos permitido por el protocolo RIP es de 15 saltos. Si un router recibe una actualización que contiene una nueva entrada o algún cambio no registrado, y el aumento del valor del campo de salto llega a 16 o lo supera, el destino de la red se considera inalcanzable.

Formato de los paquetes RIP Versión 2
A continuación describimos los campos de un paquete RIPv2:

Figura 7-14: Campos de un paquete Ripv2

- ✓ Command: Indica si el paquete es una solicitud o una respuesta. La solicitud le pide al router que envíe parte o toda su tabla de enrutamiento. La respuesta puede ser también una actualización de tablas de enrutamiento regular (puede no haber sido pedida explícitamente) o puede también ser la respuesta a una solicitud previa. Las repuestas contienen entonces entradas de tablas de enrutamiento.

- ✓ Versión: Especifica que versión del protocolo RIP estamos utilizando.
- ✓ Unused: Valor establecido en cero.
- ✓ Address-Family Identifier (AFI): Especifica la dirección de familia utilizada. RIP esta diseñado para portar información de diferentes protocolos. Cada entrada tiene una dirección de identificación que indica cual es el tipo de direcciones especificadas. El valor del campo de AFI para IP es 2. Si la AFI para la primera entrada es 0xFFFF, significa que el resto de la entrada contiene información de autenticación. Actualmente, la información de autenticación es nada más simple que un password.
- ✓ Route Tag: Provee un método para distinguir entre rutas internas (reconocidas por RIP) y rutas externas (reconocidas por otros protocolos).
- ✓ IP Address: Especifica la dirección IP para la entrada.
- ✓ Subnet Mask: Contiene la máscara de subred para la entrada. Si este campo esta en cero, quiere decir que no se ha especificado ninguna máscara de subred para la entrada.
- ✓ Next Hop: Indica la dirección IP del próximo salto al cual el paquete debe ser enviado.
- ✓ Metric: Indica cuantos saltos o redes han sido traspasadas desde el destino. Este valor debe estar entre 1 y 15, si este valor es 16, se toma como ruta no valida o inalcanzable (unreachable).

Limitaciones

RIP no está diseñado para resolver cualquier posible problema de encaminamiento. El RFC 1720 (STD 1) describe estas limitaciones técnicas de RIP como "graves" y el IETF está evaluando candidatos para reemplazarlo. Entre los posibles candidatos están OSPF("Open Shortest Path First Protocol" Versión 2) y el IS-IS de OSI IS-IS (ver IS-IS("Intermediate System to Intermediate System" de OSI)). Sin embargo, RIP está muy extendido y es probable que permanezca sin sustituir durante algún tiempo. Tiene las siguientes limitaciones:

- ✓ El coste máximo permitido en RIP es 16, que significa que la red es inalcanzable. De esta forma, RIP es inadecuado para redes grandes(es decir, aquellas en las que la cuenta de saltos puede aproximarse perfectamente a 16).
- ✓ RIP carece de servicios para garantizar que las actualizaciones proceden de "routers" autorizados. Es un protocolo inseguro.
- ✓ RIP sólo usa métricas fijas para comparar rutas alternativas. No es apropiado para situaciones en las que las rutas necesitan elegirse basándose en parámetros de tiempo real tales como el retardo, la fiabilidad o la carga.
- ✓ El protocolo depende de la cuenta hasta infinito para resolver algunas situaciones inusuales. Como se describió antes (Vector-Distance), la resolución de un bucle requeriría mucho tiempo(si la frecuencia de actualizaciones fuese limitada) o mucho ancho de banda(si las actualizaciones se enviasen por cada cambio producido). A medida que crece el tamaño del dominio, la inestabilidad del algoritmo vector-distancia de cara al cambio de topología se hace patente. RIP especifica mecanismos para minimizar los problemas con la cuenta hasta infinito(descritos más abajo) que permiten usarlo con dominios mayores, pero eventualmente su operatividad será nula.

7.1.13 PROTOCOLO DE ENRUTAMIENTO OSPF

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

Breve historia
El protocolo OSPF Primero la ruta libre más corta (Open Shortest Path First) fue creado a finales de los 80. Se diseño para cubrir las necesidades de las grandes redes IP que otros protocolos como RIP no podían soportar, incluyendo VLSM, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de ruta de multidifusión.

Descripción
OSPF funciona dividiendo una Intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza a un área backbone mediante un router fronterizo. Todos los paquetes enviados desde una dirección de una estación de trabajo de un área a otra de un área diferente atraviesan el área backbone, independientemente de la existencia de una conexión directa entre las dos áreas.

Aunque es posible el funcionamiento de una red OSPF únicamente con el área backbone, OSPF escala bien cuando la red se subdivide en un número de áreas más pequeñas.

OSPF es probablemente el tipo de protocolo IGP más utilizado en redes grandes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural a RIP, es VLSM o sin clases desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que también soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas. Una red OSPF se puede descomponer en redes más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red y donde hay otras áreas conectadas a ella. Las rutas entre diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.
Los encaminadores en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. Los encaminadores eligen a un encaminador designado' (DR) y un encaminador designado secundario (BDR) que actúan como hubs para reducir el tráfico entre los diferentes encaminadores. OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusiones usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa IP directamente, mediante el IP protocolo 89.

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

- ✓ Estado Desactivado (Down State): En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado.

- ✓ Estado de Inicialización (Init State): Los encaminadores OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los encaminadores vecinos. Cuando una interfaz recibe su primer paquete Hello, el encaminador entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa. Los dos tipos de relaciones son Dos-Vías y Adyacencia. Un encaminador debe recibir un Hello desde un vecino antes de establecer algún tipo de relación.

- ✓ Estado de Dos-Vías (Two-Way): Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de dos-vías, o comunicación bidireccional, con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un enrutador ingresa al estado de Dos-Vías cuando se ve a sí mismo en un paquete Hello proveniente de un vecino. El estado de Dos-Vías es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos. Para aprender los estados de enlace de otros encaminadores y eventualmente construir una tabla de encaminamiento, cada encaminador OSPF debe formar a lo menos una adyacencia. Una adyacencia es una relación avanzada entre encaminadores OSPF que involucra una serie de estados progresivos que se basa no tan solo en paquetes Hello, si no que otros 4 paquetes OSPF. Aquellos encaminadores intentando volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado.

- ✓ Estado ExStart: Técnicamente, cuando un encaminador y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs. Los dos encaminadores vecinos emplean paquetes Hello para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos.
  Aquel encaminador con el mayor router ID "gana" y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.

- ✓ Estado de Intercambio (Exchange): En el estado de intercambio, los encaminadores vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los encaminadores se describen sus bases de datos de estado de enlace entre ellos. Los encaminadores comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace. Si alguno de los encaminadores recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.

- ✓ Estado Cargando (Loading): Después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un enrutador recibe un LSR este responde empleando un paquete de actualización de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace (LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

- ✓ Estado de Adyacencia (Adjacency): Cuando el estado de carga ha sido completada, los enrutadores se vuelven completamente adyacentes. Cada enrutador mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

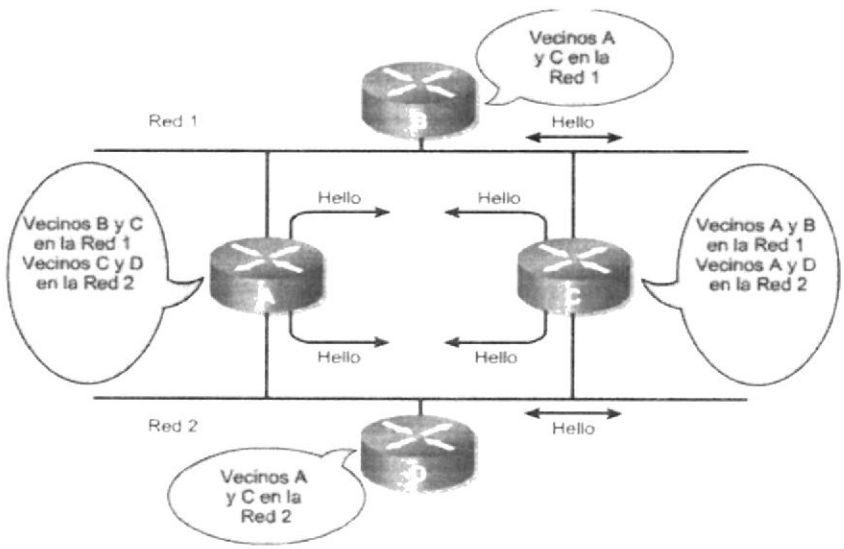


Figura 7-15: Diagrama enrutamiento OSPF

Tipos de área

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

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

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

- ✓ Area not-so-stubby: También conocidas como NSSA se trata es un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

Características de OSPF

Las principales características son:

- Respuesta rápida y sin bucles ante cambios.

La algoritmia SPF sobre la que se basa OSPF permite con la tecnología actual que existe en los nodos un tiempo de respuesta en cuanto tiempo de computación para el cálculo del mapa local de la red mucho más rápido que dicho calculo en el protocolo RIP. Además como todos los nodos de la red calculan el mapa de manera idéntica y poseen el mismo mapa se genera sin bucles ni nodos que se encuentren contando en infinito; principal problema sufrido por los protocolos basados en la algoritmia de vector distancia como RIP.

- Seguridad ante los cambios.

Para que el algoritmo de routing funcione adecuadamente debe existir una copia idéntica de la topología de la red en cada nodo de esta.
Existen diversos fallos que pueden ocurrir en la red como fallos de los protocolos de sincronización o inundación, errores de memoria, introducción de información errónea.
El protocolo OSPF especifica que todos los intercambios entre routers deben ser autentificados. El OSPF permite una variedad de esquemas de autentificación y también permite seleccionar un esquema para un área diferente al esquena de otra área. La idea detrás de la autentificación es garantizar que sólo los routers confiables difundan información de routing.

- Soporte de múltiples métricas.

La tecnología actual hace que sea posible soportar varias métricas en paralelo.
Evaluando el camino entre dos nodos en base a diferentes métricas es tener distintos mejores caminos según la métrica utilizada en cada caso, pero surge la duda de cual es el mejor. Esta elección se realizara en base a los requisitos que existan en la comunicación.
Diferentes métricas utilizadas pueden ser:
Mayor rendimiento
Menor retardo
Menor coste
Mayor fiabilidad

La posibilidad de utilizar varias métricas para el calculo de una ruta, implica que OSPF provea de un mecanismo para que una vez elegida una métrica en un paquete para realizar su routing esta sea la misma siempre para ese paquete, esta característica dota a OSPF de un routing de servicio de tipo en base a la métrica.

- Balanceado de carga en múltiples caminos.

OSPF permite el balanceado de carga entre los nodos que exista más de un camino. Para realizar este balanceo aplica:
Una versión de SPF con una modificación que impide la creación de bucles parciales.
Un algoritmo que permite calcular la cantidad de trafico que debe ser enviado por cada camino.

- Escalabilidad en el crecimiento de rutas externas.

El continuo crecimiento de Internet es debido a que cada vez son más los sistemas autónomos que se conectan entre si a través de routers externos. Además de tener en cuenta la posibilidad de acceder al exterior del sistema autónomo a través de un determinado router externo u otro se debe tener en cuenta que se tiene varios proveedores de servicios y es más versátil elegir en cada momento el router exterior y servicio requerido que establecer una ruta y servicio por defecto cuando se trata de routing externo como se tenia hasta ahora.
OSPF soluciona este problema permitiendo tener en la base de datos del mapa local los denominados "gateway link state records".Estos registros nos permiten almacenar el valor de las métricas calculadas y hacen más fácil el calculo de la ruta óptima para el exterior. Por cada entrada externa existirá una nueva entrada de tipo "gateway link state records" en la base de datos, es decir, la base de datos crecerá linealmente con el número de entradas externas tal como ocurre con los protocolos de vector distancia, pero el coste del calculo de las rutas crecerá en función de N*log*N para OSPF y no en función de N^2 como ocurre en los protocolos de vector distancia.

Integrando OSPF a la tecnología actual.

Una de las grandes ventajas de OSPF es que este ha sido diseñado para adaptarse al máximo a los protocolos TCP/IP.

- Redes Locales

La existencia de redes locales formadas por host que se conectaban a un router para acceder al exterior era un hecho patente cuando se creo OSPF y siguiendo la procedimiento explicado anteriormente cada nodo hubiese tenido que especificar su enlace con el router.

OSPF introduce un nuevo enlace el "link to a stub network" que es una variante del "router link" que basándose en el concepto de subred del modelo IP permite asignar a la red local un número de subred y especificar solamente un enlace entre el router y la subred.

El enlace hacia un vecino es identificado por la dirección IP de su vecino y el enlace hacia la red local es identificado por su red o número de subred.

- Redes Broadcast

OSPF da soporte a los servicios broadcast para ello implementa un mecanismo que simula el funcionamiento broadcast que se basa en la elección de un router como maestro a través del cual se pasaran todas las comunicaciones entre dos routers, es decir se establece el "designated router" y se crea un "virtual node".

Para realizar el mapa local cada router tendrá dos enlaces:
Un enlace de él hacia su propia red broadcast cuyo enlace conocerá el propio router.
Un enlace de él hacia el "virtual node", que será identificado por el router designado o"designated router"
La presencia del "designated router" es la de simplificar el procedimiento broadcast, ya que cuando un router quiere enviar un mensaje envía un mensaje al "designated router" usando la dirección multicast "all-designated router" (224.0.0.6).Si es un nuevo

mensaje el "designated router" lo reenvia a la red usando la dirección multicast "all-OSPF-routers" (224.0.0.5).
Si el "designated router" tiene problemas de funcionamiento todo este procedimiento fallará, por ello cuando se elige al "designated router" OSPF también elige al mismo tiempo al"backup designated router" con el cual también mantienen enlaces virtuales todos los routers, que en caso de fallo asumirá el rol de router designado y otro router será elegido como backup.
El router de backup permanece siempre en escucha de todos los mensajes cuya dirección multicast es "all-designated-router" a la espera del fallo del "designated router", que es detectado por el protocolo HELLO del OSPF.

- Redes No Broadcast.

En la documentación de OSPF este tipo de redes son aquellas que ofrecen conectividad entre todos sus miembros pero no permiten un servicio broadcast o multicast como pueden ser redes "frame-relay o"ATM".
OSPF trata este tipo de redes con un mecanismo parecido al explicado en redes broadcast, eligiendo al "designated router" y al "backup router", pero estableciendo los circuitos virtuales entre routers solo bajo demanda.
En estas redes los mensajes son enviados punto a punto, del "designated router" a cada uno de los routers. De igual modo cuando un router envía un mensaje al "designated router" lo envía también al "backup designated".

- Routing Jerárquico:

El routing jerárquico surge de la necesidad de resolver el problema debido al aumento del tamaño de las redes que implica un mayor coste en calculo de rutas, tiempo de transmisión de datos, memoria.
OSPF establece una jerarquía en la red y la parte en "areas", existiendo una área especial denominada "backbone area".
En un "área" se aplica el protocolo OSPF de manera independiente como si de una red aislada se tratase, es decir, los routers del area solo contiene en su mapa local la topología del área, así que el coste en calculo es proporcional al tamaño del área y no de la totalidad de la red.
Cada área incluye un conjunto de subredes IP. La comunicación entre routers de un área se resuelve directamente a través del mapa local de área que cada router posee.
Estas áreas se conectan entre si a través del "backbone area", mediante routers que pertenecen normalmente a una "area" y al "backbone area".Estos routers se denominan "area-border routers" y como mínimo existe uno entre una área y el backbone.
Los "area-border routers" mantienen varios mapas locales de estado de enlaces, uno por cada área a las cuales pertenecen. Estos emiten unos registros de estados de enlaces para anunciar que conjunto de subredes IP son accesibles a través de ellos. Cuando un router de un área quiere intercambiar tráfico con un router de otra área, estos deben realizarlo a través de los "area-border routers".Estas se denominan "inward routes".
Existe otro tipo de router el que realiza el intercambio de tráfico con routers de otros sistemas autónomos. La información almacenada en cada router externo es idéntica para cada una de ellos
La sumarización de registros representa los enlaces entre un "area-border router" y una red en el "backbone area" o en otra área. La métrica utilizada es la longitud del camino entre el "area-border router" y la red. Este mecanismo va a permitir que diferentes

"area-border router" establezcan para un destino diferentes caminos, según el resultado de su métrica pero con la salvedad de que no producirán bucles, debido a que la estricta jerarquía de OSPF solo permite que se conecten áreas a través del backbone.
OSPF provee en su jerarquía de routing la posibilidad de que un área se divida en dos a causa de algún fallo en los enlaces o en los routers pero siempre se quedan los fragmentos conectados directamente al "backbone area" a través de dos condiciones:
Los "area-border router" solo se guarda los enlaces de las redes y subredes que son alcanzables por ese router en un momento determinado.
El "backbone area" se guarde información de las redes que componen cada área aunque no de su topología.
El mecanismo OSPF para solucionar el caso de una partición del "area backbone" está un poco sujeto a por donde se realiza está partición ya que este podrá ser cubierto siempre y cuando existan "area-border router" que sean capaces de establecer caminos virtuales por dentro de sus areas para establecer nuevos caminos de intercambio de información.
Estos describirán enlaces virtuales que deben ser almacenados en la base de registros del "area backbone".
La métrica del enlace virtual será calculada teniendo en cuenta el coste de los enlaces reales por los que pasa el enlace virtual en el área local donde se realiza el enlace virtual.
A partir de este enlace virtual deben ser sincronizados y actualizados todos los routers del "area backbone".

- Stub Areas:

El problema del incremento de rutas externas que debían ser sumarizadas en multitud de áreas pequeñas ha quedado resuelto con la introducción del concepto de "stub area" un área donde todas las rutas externas son sumarizadas por una ruta por defecto.
Una stub area funciona exactamente igual que una area normal de OSPF con unas cuantas restricciones, acerca de prohibir la entrada de rutas externas en las bases de datos de los routers.
Una stub area puede estar conectada por mas de un "area-border router"al backbone, pero no se podrá elegir para salir del área el router, ni configurar un enlace virtual sobre una stub area.
También no se podrá conectar un "border route" con una "stub area". Esto es lógico si nosotros consideramos que los "border routers" conectan los sistemas autónomos con Internet y normalmente deberían estar sujetos a la "backbone area".

7.1.14 CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO

OSPF

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>*enable*

Ingrese al modo de configuración global.

MATRIZ#*configure terminal*

Habilite el protocolo ospf con el comando router.

MATRIZ (config)# *router* ospf 1

comando protocolo de enrutamiento

Declare las redes directamente conectadas al router

MATRIZ (config-router)#*network 192.168.3.40 0.0.0.3 area 0*

comando dirección de red willcard número de área

Redistribuya los paquetes rip por la red ospf

MATRIZ (config-router)#*redistribute rip*

Salga con Ctrl.- Z.

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

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#*wr*
Building configuration...
[OK]

MATRIZ#

RIP VERSION 2

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>*enable*

Ingrese al modo de configuración global.

MATRIZ#*configure terminal*

Habilite el protocolo rip con el comando router.

MATRIZ (config)# *router* rip

comando protocolo de enrutamiento

Declare la versión del protocolo rip.

MATRIZ (config-router)#*version 2*

Declare las redes directamente conectadas al router.

MATRIZ (config-router)#*network 192.168.2.176*

comando dirección de red

Redistribuya los paquetes ospf por la red rip.

MATRIZ (config-router)#*redistribute rip*

Salga con Ctrl.- Z.

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

Finalmente, grabe los cambios en la NVRAM con el comando wr.

MATRIZ#*wr*
Building configuration...
[OK]

MATRIZ#

7.1.15 SHOW IP ROUTE

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>enable

Digite el comando show ip route

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

192.168.3.0/0 is variably subnetted, 3 subnets
C 192.168.3.40/30 is directly connected, Serial0
O 192.168.3.52/30 [110/64] via 192.168.3.42, 00:50:45, FastEthernet0/1
R 192.168.3.176/29 [120/1] via 192.168.3.178, 00:04:36, FastEthernet0/0

R 192.168.3.8/29 [120/1] via 192.168.3.178, 00:03:34, FastEthernet0/0

Código Red aprendida Distancia Salto IP de entrada Hora Interfaz

Código: Indica que la Subred esta:
C Conectada directamente.
R Aprendida por Rip.
O Aprendida por OSPF.
Red aprendida: Dirección de subred aprendida.
Distancia: Indica la distancia administrativa
Salto: Indica el número de saltos que se han realizado para llegar al router
IP de Entrada: Muestra la IP de la interfaz por la cual ingresan las redes aprendidas.
Hora: Indica la hora de la ultima actualización.
Interfaz: Muestra porque tipo de interfaz están ingresando las redes aprendidas.

7.1.16 SHOW PROTOCOLS

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>*enable*

Digite el comando show protocols

MATRIZ#*show protocols*

```
Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.3.41/30

Serial1 is up, line protocol is up
  Internet address is 192.168.3.45/30

FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.178/29

FastEthernet0/1 is administratively down, line protocol is down

Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down
```


Muestra que está levantada y configurada la interfaz y el protocolo.

Serial0 is up, line protocol is up

Muestra la IP asignada a la interfaz.

Internet address is 192.168.3.178/29

Muestra que no está configurada y deshabilitada la interfaz y el protocolo.

FastEthernet0/1 is administratively down, line protocol is down

Muestra que no está configurado y deshabilitado el bridge y el protocolo.

Bri0 is administratively down, line protocol is down

7.1.17 SHOW RUN

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>enable

Digite el comando show running-config

MATRIZ#*show running-config*

Building configuration...
Version 12.1

Indica la Versión del IOS

service timestamps debug uptime
service timestamps log uptime
no service password-encryption

Indica el modo de encriptación de contraseña.

hostname MATRIZ

Muestra el nombre del dispositivo.

ip subnet-zero
interface Serial0

Muestra la configuración de la interfaz Serial 0

ip address 192.168.3.41 255.255.255.252

Muestra la dirección ip y la máscara de subred de la interface

no ip directed-broadcast
clock rate 64000

Presenta la velocidad del puerto en bps.

bandwidth 1544

Valor del ancho de banda que posee el enlace.

interface Serial1

Muestra la configuración de la interfaz Serial 1

ip address 192.168.3.45 255.255.255.252

Muestra la dirección ip y la máscara de subred de la interface.

no ip directed-broadcast
bandwidth 1544

Valor del ancho de banda que posee el enlace.

interface FastEthernet0/0

Muestra la configuración de la interfaz fastethernet 0/0.

ip address 192.168.3.178 255.255.255.248
Muestra la dirección ip y la máscara de subred de la interface.

no ip directed-broadcast
bandwidth 100000
ip ospf priority 0
Valor del ancho de banda que posee el enlace.

interface FastEthernet0/1
Muestra la configuración de la interfaz fastethernet 0/1

ip address 192.168.3.9 255.255.255.248
Muestra la dirección ip y la máscara de subred de la interface.

no ip directed-broadcast
bandwidth 100000
Valor del ancho de banda que posee el enlace.

interface FastEthernet0/1.1
Muestra la configuración de la sub-interfaz fastethernet 0.1/1.

encapsulation dot1q 10
Encapsulamiento asignado a la vlan 10 por el puerto dot1q.

ip address 192.168.2.113 255.255.255.240
Muestra la dirección ip y la máscara de subred asignada a la vlan.

interface Bri0
no ip address
Muestra que el bridge no tiene ip y esta deshabilitado
no ip directed-broadcast
shutdown
!
router rip
Muestra que esta habilitado el protocolo de enrutamiento rip.

version 2
Muestra la versión del protocolo rip.

redistribute OSPF 1
Se ha configurado la redistribución de paquetes rip.

network 192.168.3.0
Indica las redes que están asignadas al protocolo.

router ospf 1
Muestra que esta habilitado el protocolo de enrutamiento ospf.

redistribute RIP

Se ha configurado la redistribución de paquetes ospf.

network 192.168.2.112 0.0.0.15 area 0
network 192.168.2.32 0.0.0.31 area 0
network 192.168.2.64 0.0.0.31 area 0
network 192.168.2.96 0.0.0.15 area 0

Indica las redes que están asignadas al protocolo

ip classless

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

no ip http server

Indica que no existe servidor http.

line con 0
transport input none
line aux 0

Indica la configuración del Puerto auxiliar.

line vty 0 4

Configuración remota por telnet.

!
no scheduler allocate
end

Finaliza la presentación de la configuración del router.

7.1.18 LISTAS DE CONTROL DE ACCESO (ACL)

La Lista de Control de Acceso o ACL (del inglés, Access Control List) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL's permiten controlar el flujo del tráfico en equipos de redes, tales como routers. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

- ✓ Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior.
- ✓ Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router.
- ✓ Permiten la administración del tráfico y aseguran el acceso hacia y desde una red.
- ✓ Las ACL pueden aplicarse en Protocolos Enrutados:
  Protocolo de Internet (IP)
  Intercambio de paquetes de Internetwork (IPX)
- ✓ Las ACL se definen según el protocolo, la dirección o el puerto.
- ✓ El orden en el que se ubican las sentencias de la ACL es muy importante

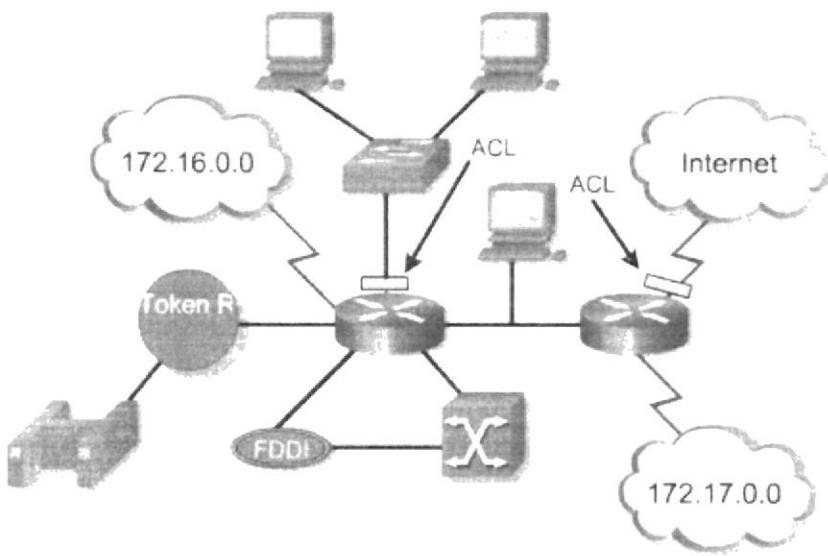


Figura 7-16: Diagrama de ACL's

7.1.18.1 TIPOS DE ACL

Se definen dos tipos ACL para aplicar en los routers las cuales son:

- ✓ ACL Estándar
- ✓ ACL Extendida

ACL Estándar

Se colocan cerca del destino del tráfico.
Las ACL's estándar solo usan las direcciones origen para hacer la comprobación.
El intervalo que se usa para este tipo de acl es de 1-99 y de 1300-1999
Sintaxis del comando
access-list (número) (deny | permit) (IP origen) (wildcard origen)
access-list 2 deny 192.168.12.2
access-list 2 deny 192.168.12.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 deny 192.0.0.0 0.255.255.255

ACL Extendida

Se coloca cerca del origen del tráfico, por eficiencia - es decir, para evitar tráfico innecesario en el resto de la red.
Las ACL's extendidas permiten usar tanto las direcciones origen como destino para hacer la comprobación.
El intervalo que se usa para este tipo de acl es de 100-199 y de 2000-2699

Sintaxis del comando
access-list (número) (deny | permit) (protocolo) (IP origen) (wildcard origen) (IP destino) (wildcard destino)

El "protocolo" puede ser (entre otros) IP (todo tráfico de tipo TCP/IP), TCP, UDP, ICMP.

access-list 114 permit tcp 192.168.12.0 0.0.0.255 any eq telnet

Ejemplo: Permitir tráfico HTTP y "ping" (ICMP) al servidor 172.16.0.1, para todos. Denegar todo lo demás.

access-list 102 permit icmp any host 172.16.0.1
access-list 102 permit tcp any host 172.16.0.1 eq www

7.1.18.2 PORQUÉ CREAR UNA ACL

- ✓ Limitar el tráfico de red y mejorar el rendimiento de la red.
- ✓ Reducir la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- ✓ Brindar control de flujo de tráfico.
- ✓ Restringir el envío de las actualizaciones de enrutamiento.
- ✓ Proporcionar un nivel básico de seguridad para el acceso a la red.
- ✓ Tipos de tráfico que se envían o bloquean en las interfaces del router. Permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- ✓ Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- ✓ Analizar ciertos hosts para permitir o denegar acceso a partes de una red.
- ✓ Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

7.1.18.3 FUNCIÓN DE LA WILCARD EN UNA ACL

- ✓ Las máscaras de wildcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas.
- ✓ La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.
- ✓ La opción any reemplaza la dirección IP con 0.0.0.0 y la máscara wildcard por 255.255.255.255. Esta opción concuerda con cualquier dirección con la que se la compare.

7.1.18.4 ENCABEZADO DE UNA ACL

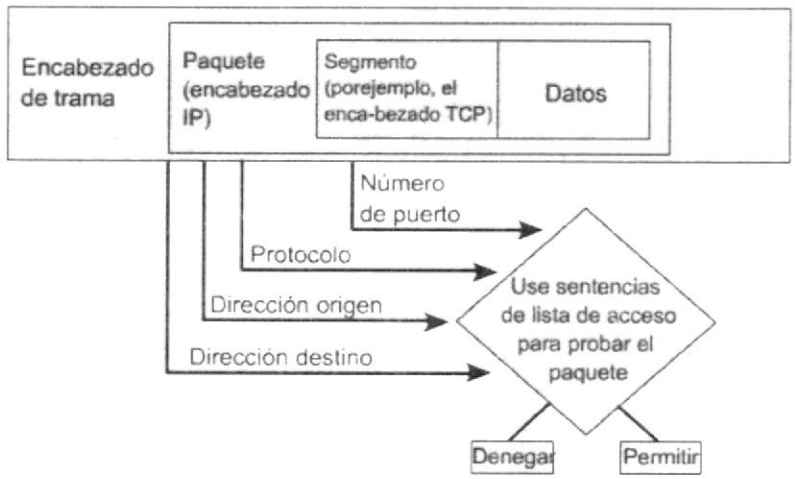


Figura 7-17: Diagrama de Encabezado de ACL's

Puntos de decisión de las ACL son:
Direcciones origen y destino
Protocolos y números de puerto de capa superior

Figura 7-18: Definiciones de ACL's

Se debe definir una ACL para cada protocolo habilitado en la interfaz.
Se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente.
Cada interfaz puede contar con varios protocolos y direcciones definidas.
Si el router tiene dos interfaces configuradas para IP, AppleTalk e IPX, se necesitan 12 ACLs separadas. Una ACL por cada protocolo, multiplicada por dos por dirección entrante y saliente, multiplicada por dos por el número de puertos.

7.1.18.5 REGLAS BÁSICAS DE UNA ACL

- ✓ Una lista de acceso por protocolo y por dirección.
- ✓ Aplicar listas de acceso estándar que se encuentran lo más cerca posible del destino.
- ✓ Aplicar listas de acceso extendidas que se encuentran lo más cerca posible del origen.
- ✓ Las sentencias se procesan de forma secuencial desde el principio de la lista hasta el final hasta que se encuentre una concordancia, si no se encuentra ninguna, se rechaza el paquete.
- ✓ Hay un deny any (denegar cualquiera) implícito al final de todas las listas de acceso. Esto no aparece en la lista de configuración.
- ✓ Las entradas de la lista de acceso deben realizar un filtro desde lo particular a lo general. Primero se deben denegar hosts específico y por último los grupos o filtros generales.
- ✓ Primero se examina la condición de concordancia. El permiso o rechazo se examina SÓLO si la concordancia es cierta.
- ✓ Utilice el editor de texto para crear comentarios que describan la lógica, luego complete las sentencias que realizan esa lógica.
- ✓ Siempre, las líneas nuevas se agregan al final de la lista de acceso. El comando no access-listx elimina toda la lista. No es posible agregar y quitar líneas de manera selectiva en las ACL numeradas.
- ✓ Se debe tener cuidado cuando se descarta una lista de acceso. Si la lista de acceso se aplica a una interfaz de producción y se la elimina, según sea la versión de IOS, puede haber una deny any (denegar cualquiera) por defecto aplicada a la interfaz, y se detiene todo el tráfico.
- ✓ Los filtros salientes no afectan al tráfico que se origina en el router local.

7.1.18.6 VERIFICACIÓN DE UNA ACL

show ip interface: muestra información de la interfaz IP e indica si se ha establecido alguna ACL.

show access-lists: muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número ACL como opción a este comando.

show running-config: también revela las listas de acceso en el router y la información de asignación de interfaz.

7.1.19 CREACIÓN Y CONFIGURACIÓN DE ACL EN ROUTER

MATRIZ>

Ingrese al modo privilegiado.

MATRIZ>enable

Ingrese al modo de configuración global.

MATRIZ#configure terminal

Declare la ACL con el comando access-list.

MATRIZ (config)# access-list 102 deny tcp any 192.168.3.0 eq telnet

102	deny	tcp	any	192.168.3.0	eq	telnet
Identificador	Acción	Protocolo	Cantidad	Segmento	Operación	Protocolo bloqueado

Identificador: Es el número que identifica a la acl
Acción: Operación la cual va a realizar la acl (deny|permit)
Protocolo: Protocolo al cual se va a regir el bloqueo
Cantidad: Conjunto de usuarios en este caso declarado a cualquiera
Segmento: IP origen del segmento que se esta autorizando o negando el acceso
Operación: Indica el protocolo que se va a ejecutar.

7.2 SWITCH

Un switch es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

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.

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.

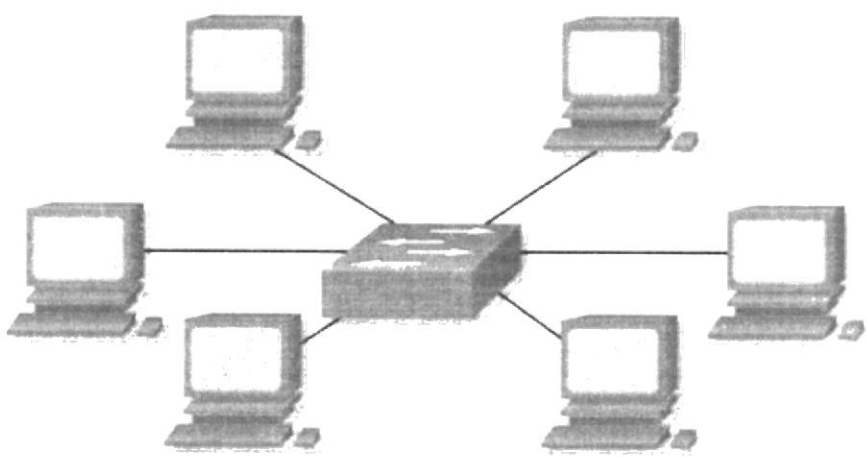


Figura 7-19: Computadores conectados a un Switch

7.2.1 ENCAPSULAMIENTO

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión. La capa de transporte divide los datos en unidades de un tamaño que se pueda administrar, denominadas segmentos. También asigna números de secuencia a los

segmentos para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego la capa de red encapsula el segmento creando un paquete.
Le agrega al paquete una dirección de red destino y origen, por lo general IP. En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física.

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino. Pero si se deben enviar los datos a otro host a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia. Esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos (el paquete).
Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet. La excepción principal a esto es un dispositivo denominado gateway. Este es un dispositivo que ha sido diseñado para convertir los datos desde un formato, creado por las capas de aplicación, presentación y sesión, en otro formato. De modo que el gateway utiliza las siete capas del modelo OSI para hacer esto.
Es importante recordar que los paquetes se ubican dentro de tramas, de modo que para comprender la forma en que viajan los paquetes en los dispositivos de la Capa 2, es necesario trabajar con la forma en que se encapsulan los paquetes, que es la trama. Cualquier cosa que le suceda a la trama también le sucede al paquete. Las NIC, los puentes y los switches involucran el uso de la información de la dirección de enlace de datos (MAC) para dirigir las tramas. Las NIC son el lugar donde reside la dirección MAC exclusiva. La dirección MAC se utiliza para crear la trama. Los puentes examinan la dirección MAC de las tramas entrantes. Si la trama es local (con una dirección MAC en el mismo segmento de red que el puerto de entrada del puente), entonces la trama no se envía a través del puente. Si la trama no es local (con una dirección MAC que no está en el puerto de entrada del puente), entonces se envía al segmento de red siguiente.
El puente toma una trama, la remueve, examina la dirección MAC y luego envía o no la trama, según lo que requiera la situación.
El switch es como un hub con puertos individuales que actúan como puentes. El switch toma una trama de datos, la lee, examina las direcciones MAC de la Capa 2 y envía las tramas (las conmuta) a los puertos adecuados.

7.2.2 SWITCH CAPA 3

Aunque los conmutadores o switches son los elementos que fundamentalmente se encargan de encaminar las tramas de nivel 2 entre los diferentes puertos, existen los denominados conmutadores de nivel 3, que permiten crear en un mismo dispositivo múltiples redes de nivel 3 (VLAN's) y encaminar los paquetes (de nivel 3) entre las redes, realizado por tanto las funciones de encaminamiento o routing.

7.2.3 SEGMENTACIÓN

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host. Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 de dirección MAC destino, los switches pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños. Si la LAN no se divide en segmentos, las LAN cuyo tamaño sea mayor que un grupo de trabajo pequeño se congestionarían rápidamente con tráfico y colisiones y virtualmente no ofrecerían ningún ancho de banda.

Al dividir redes de gran tamaño en unidades autónomas, los puentes y los switches ofrecen varias ventajas. Un puente, o switch, reduce el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo se envía un determinado porcentaje de tráfico. Los puentes y los switches amplían la longitud efectiva de una LAN, permitiendo la conexión de estaciones distantes que anteriormente no estaban permitidas.

Aunque los puentes y los switches comparten los atributos más importantes, todavía existen varias diferencias entre ellos. Los switches son significativamente más veloces porque realizan la conmutación por hardware, mientras que los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda. Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch. Estos pueden soportar densidades de puerto más altas que los puentes. Algunos switches soportan la conmutación por el método cut- through, que reduce la latencia y las demoras de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward). Por último, los switches reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

7.2.4 COLISIÓN

Uno de los problemas que se puede producir, cuando dos bits se propagan al mismo tiempo en la misma red, es una colisión. En una red pequeña y de baja velocidad es posible implementar un sistema que permita que sólo dos computadores envíen mensajes, cada uno por turnos. Esto significa que ambas pueden mandar mensajes, pero sólo podría haber un bit en el sistema. El problema es que en las grandes redes hay muchos computadores conectados, cada uno de los cuales desea comunicar miles de

millones de bits por segundo. Recordar que los "bits" en realidad son paquetes que contienen muchos bits.

Se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes como, por ejemplo, los repetidores, puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo. Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos. El área dentro de la red donde los paquetes se originan y colisionan, se denomina dominio de colisión, e incluye todos los entornos de medios compartidos. Por ejemplo, un alambre puede estar conectado con otro a través de cables de conexión, transceptores, paneles de conexión, repetidores e incluso hubs. Todas estas interconexiones de la Capa 1 forman parte del dominio de colisión. Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

Al igual que lo que ocurre con dos automóviles, que no pueden ocupar el mismo espacio, o la misma carretera, al mismo tiempo, tampoco es posible que dos señales ocupen el mismo medio simultáneamente.

En general, se cree que las colisiones son malas ya que degradan el desempeño de la red. Sin embargo, una cantidad determinada de colisiones es una función natural de un entorno de medios compartidos (es decir, un dominio de colisión) ya que una gran cantidad de computadores intentan comunicarse entre sí simultáneamente, usando el mismo cable.

Los repetidores regeneran y retemporizan los bits, pero no pueden filtrar el flujo de tráfico que pasa por ellos. Los datos (bits) que llegan a uno de los puertos del repetidor se envían a todos los demás puertos. El uso de repetidor extiende el dominio de colisión, por lo tanto, la red a ambos lados del repetidor es un dominio de colisión de mayor tamaño.

Se puede reducir el tamaño de los dominios de colisión utilizando dispositivos inteligentes de networking que pueden dividir los dominios. Los puentes, switches y routers son ejemplos de este tipo de dispositivo de networking. Este proceso se denomina segmentación.

Un puente puede eliminar el tráfico innecesario en una red con mucha actividad dividiendo la red en segmentos y filtrando el tráfico basándose en la dirección de la estación. El tráfico entre dispositivos en el mismo segmento no atraviesa el puente, y afecta otros segmentos. Esto funciona bien, siempre y cuando el tráfico entre segmentos no sea demasiado. En caso contrario, el puente se puede transformar en un cuello de botella, y de hecho puede reducir la velocidad de la comunicación. La mejor solución para este problema es la utilización de switches para la correcta segmentación de una LAN

7.2.5 ASIGNACIÓN DE NOMBRE AL SWITCH

Switch>

Ingrese al modo privilegiado.

Switch>*enable*

Ingrese al modo de configuración global.

Switch#*configure terminal*

Asigne nombre con el comando hostname seguido del mismo.

Switch (config)#*hostname SW_MATRIZ*

comando nombre del switch

Salga con Ctrl.- Z.

SW_MATRIZ (config)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios con el comando cop r st.

SW_MATRIZ#*cop r st*
Building configuration...
[OK]

SW_MATRIZ#

7.3 VLANS

Una VLAN (acrónimo de Virtual LAN, "red de área local virtual") es una red de computadoras lógicamente independiente. Varias VLAN's pueden coexistir en un único switch físico.
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 VLAN's mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLAN's surge cuando se traslada físicamente una computadora a otra ubicación: puede permanecer en la misma VLAN sin necesidad de ninguna reconfiguración hardware.
Una LAN virtual (VLAN) es muy similar a la red de área local común que estás ya al corriente de, no obstante los dispositivos no necesitan necesariamente ser conectados con el mismo segmento físicamente. Para entender este mejor puedes pensar simplemente en los dispositivos que se realizan como si él fuera conectado con el mismo alambre a pesar del hecho que puede ser conectada en las varias conexiones físicas a través del segmento del LAN. Esto está realmente fresco porque el LAN virtual puede realmente ser conectado en los varios puntos físicos sino reaccionar como si fuera conectado directamente. En fin, el VLAN es una red independiente compuesta de varias computadoras. Y, varias VLAN's puede coexistir con un interruptor físico.

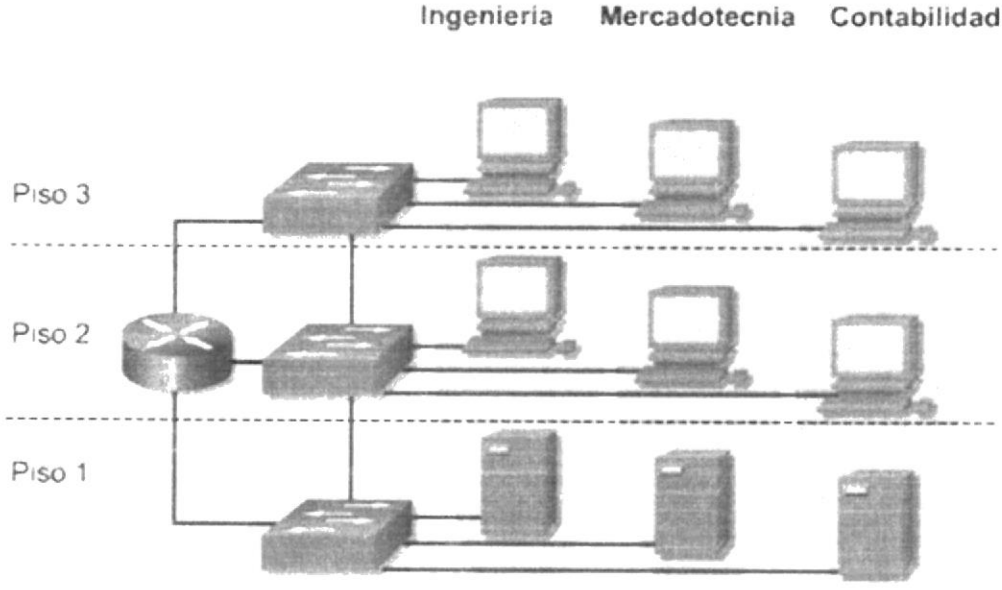


Figura 7-20: Diagrama de VLAN's

Protocolo 802.1Q

El protocolo de etiquetado IEEE 802.1Q domina el mundo de las VLAN's. 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 VLAN's 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 VLAN's 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 VLAN's funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLAN's 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 VLAN's, el término trunk ('tronco') designa una conexión de red que transporta múltiples VLAN's identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports ('puertos etiquetados') de dispositivos con soporte de VLAN's, 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 VLAN's.

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.

7.3.1 TIPOS DE VLAN

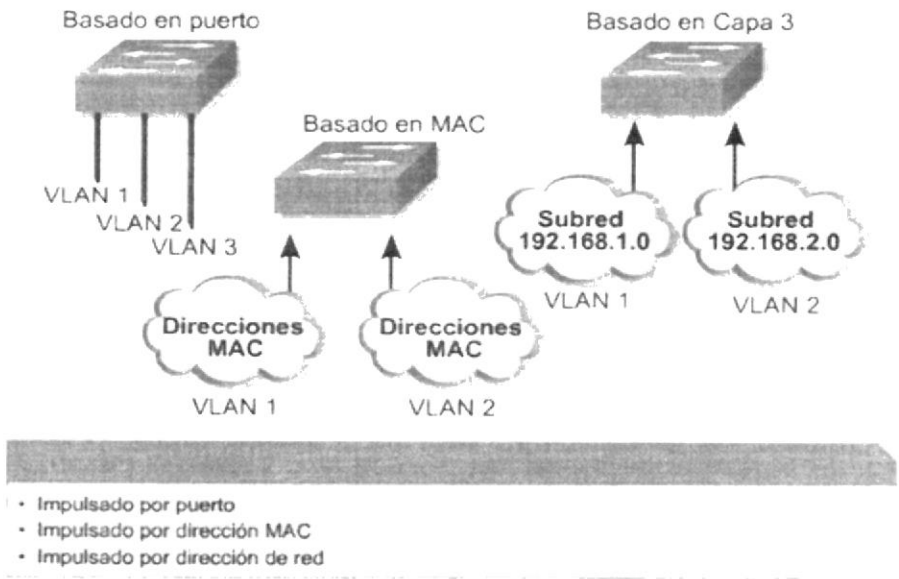


Figura 7-21: Diagrama Tipos de VLAN's

Basado en Puerto
Es el método de configuración más común
Los puertos se asignan individualmente, en grupo, en fila o en 2 o mas switches
Es de uso sencillo y se implementa a menudo donde el protocolo de control de Host Dinámico (DHCP) se usa para asignar las direcciones IP a los host de Red

Dirección MAC
Se implementa con escasa frecuencia hoy en día.
Es necesario introducir y configurar cada dirección de forma individual
La administración, diagnósticos de fallas y la gestión son complejas por ende son difíciles de manejar

Basado en protocolos
Se configuran de una manera similar a las direcciones MAC, pero usan una dirección lógica o IP
Ya no son comunes debido al uso del DHCP.

Ventajas
Hay una ventaja al VLAN con respecto al LAN y es flexibilidad considerable en el diseño total y la puesta en práctica. Puesto que el VLAN se pone en ejecución a través del software en vez del hardware el administrador no tiene ningún problema que localiza averías o aún que se amplía en el futuro. Una de las ventajas más grandes con el VLAN es cuando la computadora se debe mover a una diversa localización física. Cuando se mueve el VLAN no necesita hacer el hardware configurar de nuevo porque el VLAN sigue configurado. La mudanza de un LAN convencional que fija esta manera con resultados similares es virtualmente imposible. Otras ventajas se experimentan con el VLAN también incluyendo flexibilidad realzada, velocidad, seguridad, y menos costoso que el LAN convencional.

Desventajas
Hay desventajas de VLAN también. Éstos incluyen limitaciones de la difusión y del dispositivo así como los apremios portuarios. Aunque, un buen administrador puede compensar las limitaciones de la difusión meticuloso planeando la configuración y fijar de VLAN.
No verás generalmente VLAN's en la casa de una persona común porque no es necesario. Esto es porque son convenientes para las corporaciones grandes que tienen una gran cantidad de computadoras que estén comunicando constantemente datos dentro de la oficina y al exterior de mundo. El VLAN es considerablemente más ventajoso a los negocios grandes que las viejas redes del LAN y debido a esto valen la inversión más grande.

7.3.2 CREACIÓN Y CONFIGURACIÓN DE VLAN

SW_MATRIZ>

Ingrese al modo privilegiado.

SW_MATRIZ>*enable*

Ingrese a la base de datos de las VLAN`s.

SW_MATRIZ# *vlan database*

Cree la VLAN con el comando vlan.

SW_MATRIZ (vlan)# *vlan 10 name VENTAS*

identificador nombre de VLAN

Salga con Ctrl.- Z.

MATRIZ (vlan)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios con el comando cop r st.

SW_MATRIZ#*cop r st*
Building configuration...
[OK]

SW_MATRIZ#

7.3.3 ASIGNACIÓN DE VLAN A LAS INTERFACES DEL SWITCH

SW_MATRIZ>

Ingrese al modo privilegiado.

SW_MATRIZ>*enable*

Ingrese al modo de configuración global.

SW_MATRIZ#*configure terminal*

Ingrese el comando interface seguido de la interfaz.

SW_MATRIZ (config)# *interface fastethernet 0/1*

Habilite la interfaz para poder establecer un enlace troncal.

SW_MATRIZ (config-if)#*switchport mode trunk*

Habilite el protocolo dot1q para comunicar las VLAN's.

SW_MATRIZ (config-if)# *switchport trunk encapsulation dot1q*

Salga de esa interfaz con exit.

SW_MATRIZ (config-if)# *exit*

Ingrese al la interfaz 2 del switch.

SW_MATRIZ (config)# *interface fastethernet 0/2*

Agregue y de acceso la VLAN para esta interfaz.

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

comando identificador de vlan

De esta manera se ha asignado y dado acceso a la vlan 10 por el puerto 2 del switch.

Salga con Ctrl.- Z.

MATRIZ (config-if)# *^Z*
%SYS-5-CONFIG_I: Configured from console by console

Finalmente, grabe los cambios con el comando cop r st.

SW_MATRIZ#*cop r st*
Building configuration...
[OK]

7.3.4 SHOW VLAN

SW_MATRIZ>

Ingrese al modo privilegiado.

SW_MATRIZ>*enable*

Digite el comando show vlan.

SW_MATRIZ#show vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/12, Fa0/4, Fa0/5,
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                                                 Fa0/10, Fa0/11
10   VENTAS                            active    Fa0/2, Fa0/3

1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-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
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

VLAN: Muestra el identificador de la VLAN
Name: Indica el nombre de la Vlan
Status: Muestra cual es el estado de la VLAN
Ports: Puertos asignados a la vlan
Type: Tipo de tecnologías de las Interfaces
SAID: Número de encabezado para identificar las VLAN`s
MTU: Máximo tamaño de paquetes transmitidos, se encuentra en expresado en bytes.

7.4 DIAGRAMA DE DISPOSITIVOS WAN IMPLEMENTADO

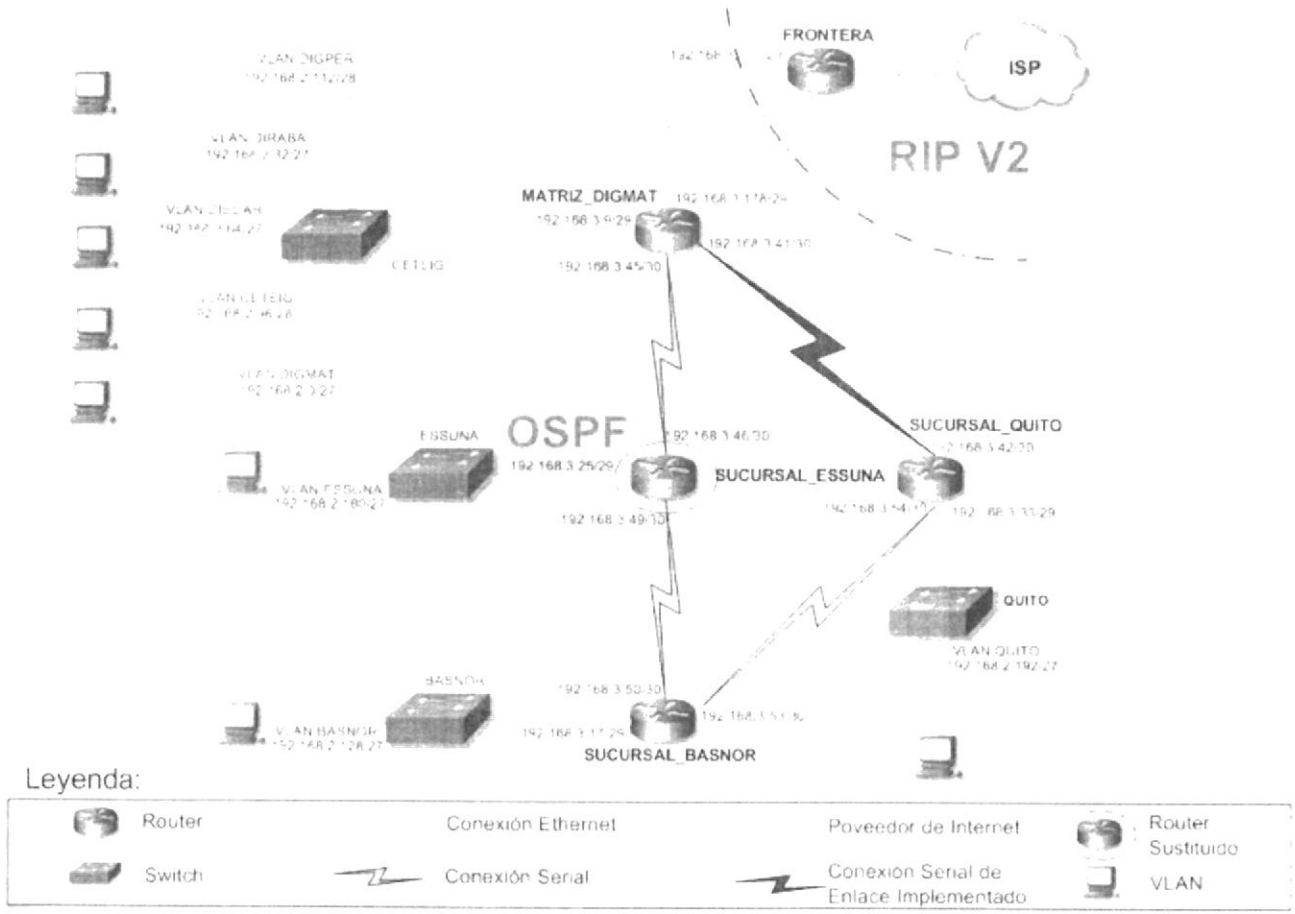


Figura 7-22: Diagrama de dispositivos WAN implementado

7.5 CONFIGURACIÓN DEL ROUTER FRONTERA

Ingrese al dispositivo, solicitará que presione un enter para proceder a digitar los comandos de configuración.

Press Enter to Start

7.5.1 ASIGNACIÓN DE NOMBRE

Router>*enable*
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado.

Router#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debe ingresar comandos de configuración.

Router(config)#hostname FRONTERA
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre.

7.5.2 ACCESO POR CONSOLA

FRONTERA(config)#line vty 0 4
Ingrese al modo de configuración del acceso por Terminal Virtual.

FRONTERA(config-line)#password cisco
Digite el comando password seguido del contraseña que quiera asignar.

FRONTERA(config-line)#login
Con el comando login active el inicio con la contraseña.

FRONTERA(config-line)#exit
Salga con el comando exit para poder configurar el acceso por consola.

FRONTERA(config)#line console 0
Habilite el acceso por consola con el comando line console 0.

FRONTERA(config-line)#password cisco
Ingrese el comando password seguido de la contraseña.

FRONTERA(config-line)#login
Active el inicio con la contraseña.

7.5.3 CONFIGURACIÓN DE INTERFACES ETHERNET

Fastethernet 0

FRONTERA(config)#interface fastethernet 0/0
Digite el comando interface fastethernet 0/0 para poder ingresar al modo de configuración de la interface.

FRONTERA(config-if)#description CONEXIÓN CON ROUTER MATRIZ_DIGMAT
Puede ingresar una descripción a la interfaz con el comando description.

FRONTERA(config-if)#ip address 192.168.3.177 255.255.255.248
Asigne la dirección IP con su respectiva máscara de subred con el comando ip address.

FRONTERA(config-if)#no shutdown
Levante la interfaz puesta con el comando no shutdown, si quiere bajar la interfaz anteponga no al comando shutdown.

%LINK-3-UPDOWN: Interface Fastethernet0/0, changed state to up
Este mensaje aparecerá indicando que está levantada la interfaz.

7.5.4 CONFIGURACIÓN DEL PROTOCOLO RIP VERSION 2

FRONTERA(config)#router rip
Habilite el protocolo de enrutamiento con el comando router rip.

FRONTERA(config-router)#version 2
Especifique la versión del protocolo digitando el comando versión 2.

FRONTERA(config-router)#network 192.168.2.176
Activado el protocolo de enrutamiento ingrese las redes directamente conectadas con el comando network seguido de la dirección de red.

7.5.5 GUARDAR CONFIGURACIÓN

Salga al modo usuario privilegiado.
FRONTERA#

FRONTERA#copy running-config startup-config
Con este comando proceda a grabar las configuraciones: copy running-config. startup-config.

Destination filename [startup-config]?
Building configuration...
[OK]
Este mensaje aparecerá cuando se haya grabado todas las configuraciones realizadas correctamente.

7.5.6 SHOW IP ROUTE FRONTERA

FRONTERA#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

192.168.3.0/0 is variably subnetted, 4 subnets
C 192.168.3.176/29 is directly connected, FastEthernet0/0
R 192.168.3.40/30 [120/1] via 192.168.3.178, 00:08:41, FastEthernet0/0
R 192.168.3.44/30 [120/1] via 192.168.3.178, 00:04:36, FastEthernet0/0
R 192.168.3.8/29 [120/1] via 192.168.3.178, 00:03:34, FastEthernet0/0

7.5.7 SHOW PROTOCOLS FRONTERA

FRONTERA#show protocols

Global values:
  Internet Protocol routing is enabled
Serial0 is administratively down, line protocol is down
Serial1 is administratively down, line protocol is down
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.177/29
FastEthernet0/1 is administratively down, line protocol is down
Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down

Serial0 / FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.3.178/29
Bri0 is administratively down, line protocol is down

7.5.8 SHOW RUN FRONTERA

```
Press Enter to Start
FRONTERA#show running-config
Building configuration...
Version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname FRONTERA
ip subnet-zero
interface Serial0
 no ip address
 no ip directed-broadcast
 bandwidth 1544
interface Serial1
 no ip address
 no ip directed-broadcast
 bandwidth 1544
interface FastEthernet0/0
ip address 192.168.3.177 255.255.255.248
 no ip directed-broadcast
 bandwidth 100000
interface FastEthernet0/1
no ip address
 no ip directed-broadcast
 bandwidth 100000
router rip
 version 2
 network 192.168.3.0
ip classless
no ip http server
line con 0
transport input none
line aux 0
line vty 0 4
no scheduler allocate
end
```

7.6 CONFIGURACIÓN DEL ROUTER MATRIZ_DIGMAT

Ingrese al dispositivo, solicitará que de un enter para proceder a digitar los comandos de configuración.

Press Enter to Start

7.6.1 ASIGNACIÓN DE NOMBRE

Router>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado

Router#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general.

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debe ingresar comandos de configuración.

Router(config)#hostname MATRIZ_DIGMAT
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre.

7.6.2 ACCESO POR CONSOLA

MATRIZ_DIGMAT(config)#line vty 0 4
Ingrese al modo de configuración del acceso por Terminal Virtual.

MATRIZ_DIGMAT(config-line)#password cisco
Digite el comando password seguido de la contraseña que quiera asignar.

MATRIZ_DIGMAT(config-line)#login
Con el comando Login active el inicio con la contraseña.

MATRIZ_DIGMAT(config-line)#exit
Salga con el comando exit para poder configurar el acceso por consola.

MATRIZ_DIGMAT(config)#line console 0
Habilite el acceso por consola con el comando line console 0.

MATRIZ_DIGMAT(config-line)#password cisco
Ingrese el comando password seguido de la contraseña.

MATRIZ_DIGMAT(config-line)#login
Active el inicio con la contraseña.

7.6.3 CONFIGURACIÓN DE INTERFACES ETHERNET

Fastethernet 0

MATRIZ_DIGMAT(config)#interface fastethernet 0/0
Digite el comando interface fastethernet 0/0 para poder ingresar al modo de configuración de la interface.

MATRIZ_DIGMAT(config-if)#description CONEXIÓN CON ROUTER FRONTERA
Puede ingresar una descripción a la interfaz con el comando description.

MATRIZ_DIGMAT(config-if)#ip address 192.168.3.178 255.255.255.248
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address.

MATRIZ_DIGMAT(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown.

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

Fastethernet 1

MATRIZ_DIGMAT(config)#interface fastethernet 0/1
Digite el comando interface fastethernet 0/0 para poder ingresar al modo de configuración de la interface.

MATRIZ_DIGMAT(config-if)#ip address 192.168.3.9 255.255.255.248
Asigne la dirección ip con su respectiva máscara de subred con el comando IP address.

MATRIZ_DIGMAT(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown.

%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.6.3.1 CONFIGURACIÓN DE SUB-INTERFACES

Para configurar una sub-interfaz debemos ingresar al modo de usuario privilegiado.

MATRIZ_DIGMAT(config)#interface fastethernet 1/0.1
Digite el comando *interface fastethernet 1/0.1* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.1.

MATRIZ_DIGMAT(config)#description VLAN DIGPER
Puede agregar un comentario a la interfaz con el comando description.

*MATRIZ_DIGMAT(config-subif)#*encapsulation dot1q 10
Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 10.

MATRIZ_DIGMAT(config-subif)#ip address 192.168.2.113 255.255.255.240
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando ip address.

MATRIZ_DIGMAT(config)#interface fastethernet 1/0.2
Digite el comando *interface fastethernet 1/0.2* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.2

MATRIZ_DIGMAT(config)#description VLAN DIRABA
Puede agregar un comentario a la interfaz con el comando description.

*MATRIZ_DIGMAT(config-subif)#*encapsulation dot1q 20
Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 20.

MATRIZ_DIGMAT(config-subif)#ip address 192.168.2.33 255.255.255.224
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando ip address.

MATRIZ_DIGMAT(config)#interface fastethernet 1/0.3
Digite el comando *interface fastethernet 1/0.3* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.3.

MATRIZ_DIGMAT(config)#description VLAN DIECAR
Puede agregar un comentario a la interfaz con el comando description.

*MATRIZ_DIGMAT(config-subif)#*encapsulation dot1q 30
Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 30.

MATRIZ_DIGMAT(config-subif)#ip address 192.168.2.65 255.255.255.224
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando *ip address.*

MATRIZ_DIGMAT(config)#interface fastethernet 1/0.4
Digite el comando *interface fastethernet 1/0.4* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.4.

MATRIZ_DIGMAT(config)#description VLAN CETEIG
Puede agregar un comentario a la interfaz con el comando description.

*MATRIZ_DIGMAT(config-subif)#*encapsulation dot1q 40

Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 40.

MATRIZ_DIGMAT(config-subif)#ip address 192.168.2.97 255.255.255.240
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando ip address.

MATRIZ_DIGMAT(config)#interface fastethernet 1/0.5
Digite el comando *interface fastethernet 1/0.5* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.5.

MATRIZ_DIGMAT(config)#description VLAN DIGMAT
Puede agregar un comentario a la interfaz con el comando description.

*MATRIZ_DIGMAT(config-subif)#*encapsulation dot1q 50
Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 50

MATRIZ_DIGMAT(config-subif)#ip address 192.168.2.1 255.255.255.224
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando ip address.

7.6.4 CONFIGURACIÓN DE INTERFACES SERIALES

Serial 0

MATRIZ_DIGMAT(config)#interface serial 0
Digite el comando interface serial 0 para poder ingresar al modo de configuración de la interface.

MATRIZ_DIGMAT(config-if)#ip address 192.168.3.41 255.255.255.252
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address.

MATRIZ_DIGMAT(config-if)#clock rate 64000
Asigne el clock rate con el valor de 64000.

MATRIZ_DIGMAT(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown.

%LINK-3-UPDOWN: Interface Serial0, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.
Salga con exit.

Serial 1

MATRIZ_DIGMAT(config)#interface serial 1
Digite el comando interface serial 1 para poder ingresar al modo de configuración de la interface.

MATRIZ_DIGMAT(config-if)#ip address 192.168.3.45 255.255.255.252
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address.

MATRIZ_DIGMAT(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown.

%LINK-3-UPDOWN: Interface Serial1, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.6.5 CONFIGURACIÓN DEL PROTOCOLO OSPF

MATRIZ_DIGMAT(config)#router ospf 1
Habilite el protocolo de enrutamiento con el comando router ospf 1.

MATRIZ_DIGMAT(config-router)#network 192.168.3.40 0.0.0.3 area 0
MATRIZ_DIGMAT(config-router)#network 192.168.3.44 0.0.0.3 area 0
MATRIZ_DIGMAT(config-router)#network 192.168.3.8 0.0.0.7 area 0

Activado el protocolo de enrutamiento ingrese las redes directamente conectadas con el comando *network* seguido de la Wildcard y el área en este caso 0.

MATRIZ_DIGMAT(config-router)#redistribute rip
Proceda a redistribuir los paquetes rip por nuestra red ospf con el comando redistribute rip.

7.6.6 CONFIGURACIÓN DEL PROTOCOLO RIP VERSION 2

MATRIZ_DIGMAT(config)#router rip
Habilite el protocolo de enrutamiento con el comando router rip.

MATRIZ_DIGMAT(config-router)#version 2
Especifique la versión del protocolo digitando el comando versión 2.

MATRIZ_DIGMAT(config-router)#network 192.168.2.176
Activado el protocolo de enrutamiento ingrese las redes directamente conectadas con el comando network seguido de la dirección de red.

MATRIZ_DIGMAT(config-router)#resdistribute ospf 1
Proceda a redistribuir los paquetes ospf por nuestra red rip con el comando redistribute ospf 1.

7.6.7 GUARDAR CONFIGURACIÓN

Salga al modo usuario Privilegiado.
MATRIZ_DIGMAT#

MATRIZ_DIGMAT#copy running-config startup-config
Con este comando proceda a grabar las configuraciones: copy running-config startup-config.

Destination filename [startup-config]?
Building configuration...
[OK]
Este mensaje aparecerá cuando se haya grabado todas las configuraciones realizadas correctamente.

7.6.8 SHOW IP ROUTE MATRIZ_DIGMAT

MATRIZ_DIGMAT#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

192.168.2.0/0 is variably subnetted, 5 subnets
C 192.168.2.112/28 is directly connected, 192.168.2.113
C 192.168.2.32/27 is directly connected, 192.168.2.33
C 192.168.2.64/27 is directly connected, 192.168.2.65
C 192.168.2.96/28 is directly connected, 192.168.2.97
C 192.168.2.0/27 is directly connected, 192.168.2.1

192.168.3.0/0 is variably subnetted, 8 subnets
C 192.168.3.40/30 is directly connected, Serial0
C 192.168.3.44/30 is directly connected, Serial1
C 192.168.3.8/29 is directly connected, FastEthernet0/1
O 192.168.3.32/29 [110/64] via 192.168.3.33, 00:50:45, FastEthernet0/1
O 192.168.3.52/30 [110/64] via 192.168.3.42, 00:50:45, FastEthernet0/1
O 192.168.3.48/30 [110/192] via 192.168.3.42, 00:50:45, FastEthernet0/1
O 192.168.3.24/29 [110/64] via 192.168.3.25, 00:50:45, FastEthernet0/1
R 192.168.3.176/29 [120/1] via 192.168.3.178, 00:04:36, FastEthernet0/0

7.6.9 SHOW PROTOCOLOS MATRIZ_DIGMAT

MATRIZ_DIGMAT#show protocols

Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.3.41/30

Serial1 is up, line protocol is up
  Internet address is 192.168.3.45/30

FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.178/29

FastEthernet0/1 is up, line protocol is up
  Internet address is 192.168.3.9/29

Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down

7.6.10 SHOW RUN MATRIZ_DIGMAT

Press Enter to Start

MATRIZ_DIGMAT#show running-config
Building configuration...
Version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname MATRIZ_DIGMAT
ip subnet-zero
interface Serial0
ip address 192.168.3.41 255.255.255.252
no ip directed-broadcast
clock rate 64000
bandwidth 1544
interface Serial1
ip address 192.168.3.45 255.255.255.252
no ip directed-broadcast
bandwidth 1544
interface FastEthernet0/0
ip address 192.168.3.178 255.255.255.248
no ip directed-broadcast
bandwidth 100000
ip ospf priority 0
interface FastEthernet0/1
ip address 192.168.3.9 255.255.255.248
no ip directed-broadcast
bandwidth 100000
interface FastEthernet0/1.1
encapsulation dot1q 10
ip address 192.168.2.113 255.255.255.240
interface FastEthernet0/1.2
encapsulation dot1q 20
ip address 192.168.2.33 255.255.255.224
interface FastEthernet0/1.3
encapsulation dot1q 30
ip address 192.168.2.65 255.255.255.224
interface FastEthernet0/1.4
encapsulation dot1q 40
ip address 192.168.2.97 255.255.255.240
interface FastEthernet0/1.5
encapsulation dot1q 50
ip address 192.168.2.1 255.255.255.224
interface Bri0
no ip address
no ip directed-broadcast
shutdown

```
!
router rip
version 2
redistribute OSPF 1
network 192.168.3.0
router ospf 1
redistribute RIP
network 192.168.3.8 0.0.0.7 area 0
network 192.168.3.44 0.0.0.3 area 0
network 192.168.3.40 0.0.0.3 area 0
network 192.168.2.112 0.0.0.15 area 0
network 192.168.2.32 0.0.0.31 area 0
network 192.168.2.64 0.0.0.31 area 0
network 192.168.2.96 0.0.0.15 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
```

7.7 CONFIGURACIÓN DEL SWITCH CETEIG

Ingrese al dispositivo, nos solicitará que demos un enter para proceder a digitar los comandos de configuración

Press Enter to Start

7.7.1 ASIGNACIÓN DE NOMBRE

Switch>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado

Switch#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debemos ingresar comandos de configuración

Switch(config)#hostname SW_CETEIG
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre.

7.7.2 CREACIÓN DE VLAN

SW_CETEIG#vlan database
Ingrese a la base de datos de las vlan.

SW_CETEIG(vlan)#vlan 10 name DIGPER
SW_CETEIG(vlan)#vlan 20 name DIRABA
SW_CETEIG(vlan)#vlan 30 name DIECAR
SW_CETEIG(vlan)#vlan 40 name CETEIG
SW_CETEIG(vlan)#vlan 50 name DIGMAT

Cree las VLAN's con su número identificador seguido del comando name con su nombre único.

7.7.3 ASIGNACIÓN DE VLAN A LAS INTERFACES

SW_CETEIG(config)#interface fastethernet 0/1
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport mode trunk
Configure esta interfaz en modo truncado.

SW_CETEIG(config-if)#switchport trunk encapsulation dot1q
Encapsule el puerto con el comando switchport trunk encapsulation dot1q.

SW_CETEIG(config)#interface fastethernet 0/2
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 10
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/3
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_CETEIG(config-if)#switchport access vlan 10
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/4
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_CETEIG(config-if)#switchport access vlan 20
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/5
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 20
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/6
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 30
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/7
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 30
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/8
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 40
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/9
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 40
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/10
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 50
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_CETEIG(config)#interface fastethernet 0/11
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_CETEIG(config-if)#switchport access vlan 50
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

7.7.4 SHOW VLAN SWITCH CETEIG

SW_CETEIG#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/12
10	DIGPER	active	Fa0/2, Fa0/3
20	DIRABA	active	Fa0/4, Fa0/5
30	DIECAR	active	Fa0/6, Fa0/7
40	CETEIG	active	Fa0/8, Fa0/9
50	DIGMAT	active	Fa0/10, Fa0/11
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
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

7.7.5 CREACIÓN DE ACL EN ROUTER MATRIZ_DIGMAT

MATRIZ_DIGMAT#configure terminal
Ingrese a la configuración global para proceder a configurar la acl en el dispositivo

MATRIZ_DIGMAT(config)# access-list 102 deny tcp any 192.168.3.0 eq telnet

Para proceder a configurar una acl bloqueo del telnet digite el comando *access-list* seguido del número que corresponda dependiendo si es estándar o extendida, la acción, el protocolo, cantidad, Segmento que quiera bloquear o permitir, y la operación con el protocolo.

Con está ACL se bloquea telnet al router matriz.

7.8 CONFIGURACIÓN DEL ROUTER SUCURSAL_QUITO

Ingrese al dispositivo, nos solicitará que demos un enter para proceder a digitar los comandos de configuración.

Press Enter to Start

7.8.1 ASIGNACIÓN DE NOMBRE

Router>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado

Router#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debemos ingresar los comandos de configuración

Router(config)#hostname SUCURSAL_QUITO
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre

7.8.2 ACCESO POR CONSOLA

SUCURSAL_QUITO(config)#line vty 0 4
Ingrese al modo de configuración del acceso por Terminal Virtual

SUCURSAL_QUITO(config-line)#password cisco
Digite el comando password seguido del contraseña que quiera asignar

SUCURSAL_QUITO(config-line)#login
Con el comando Login active el inicio con la contraseña

SUCURSAL_QUITO(config-line)#exit
Salga con el comando exit para poder configurar el acceso por consola

SUCURSAL_QUITO(config)#line console 0
Habilite el acceso por consola con el comando line console 0

SUCURSAL_QUITO(config-line)#password cisco
Ingrese el comando password seguido de la contraseña

SUCURSAL_QUITO(config-line)#login
Active el inicio con la contraseña

7.8.3 CONFIGURACIÓN DE INTERFACES ETHERNET

Fastethernet 0

SUCURSAL_QUITO(config)#interface fastethernet 0/0
Digite el comando *interface fastethernet 0/0* para poder ingresar al modo de configuración de la interface

SUCURSAL_QUITO(config-if)#description CONEXIÓN CON ROUTER DIGMAT
Puede ingresar una descripción a la interfaz con el comando *description*

SUCURSAL_QUITO(config-if)#ip address 192.168.3.33 255.255.255.248
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address

SUCURSAL_QUITO(config-if)#no shutdown
Levante la interface puesta con el comando *no shutdown*, si quiera bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.8.3.1 CONFIGURACIÓN DE SUB-INTERFACES

Para configurar una sub-interfaz debemos ingresar al modo de usuario privilegiado

SUCURSAL_QUITO(config)#interface fastethernet 1/0.1
Digite el comando *interface fastethernet 1/0.1* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.1

SUCURSAL_QUITO(config)#description VLAN QUITO
Puede agregar un comentario a la interfaz con el comando description

*SUCURSAL_QUITO(config-subif)#*encapsulation dot1q 80
Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 80

SUCURSAL_QUITO(config-subif)#ip address 192.168.2.193 255.255.255.224
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando *ip address*

7.8.4 CONFIGURACIÓN DE INTERFACES SERIALES

Serial 0

SUCURSAL_QUITO(config)#interface serial 0
Digite el comando interface serial 0 para poder ingresar al modo de configuración de la interface

SUCURSAL_QUITO(config-if)#ip address 192.168.3.42 255.255.255.25
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address

SUCURSAL_QUITO(config-if)#clock rate 64000
Asigne el clock rate con el valor de 64000

SUCURSAL_QUITO(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface Serial0, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

Serial 1

SUCURSAL_QUITO(config)#interface serial 1
Digite el comando interface serial 1 para poder ingresar al modo de configuración de la interface

SUCURSAL_QUITO(config-if)#ip address 2192.168.3.54 255.255.255.252
Asigne la dirección IP con su respectiva máscara de subred con el comando ip address

SUCURSAL_QUITO(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface Serial1, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.8.5 CONFIGURACIÓN DEL PROTOCOLO OSPF

SUCURSAL_QUITO(config)#router ospf 1
Habilite el protocolo de enrutamiento con el comando router rip

SUCURSAL_QUITO(config-router)#network 192.168.3.40 0.0.0.3 area 0
SUCURSAL_QUITO(config-router)#network 192.168.3.52 0.0.0.3 area 0
SUCURSAL_QUITO(config-router)#network 192.168.3.32 0.0.0.7 area 0
SUCURSAL_QUITO(config-router)#exit

Activado el protocolo de enrutamiento ingrese las redes directamente conectadas con el comando network seguido de la wilcard y el área en este caso 0

7.8.6 GUARDAR CONFIGURACIÓN

Salga al modo usuario Privilegiado
SUCURSAL_QUITO#

SUCURSAL_QUITO#copy running-config startup-config
Con este comando proceda a grabar las configuraciones: copy running-config startup-config

Destination filename [startup-config]?
Building configuration...
[OK]
Este mensaje aparecerá cuando se haya grabado todas las configuraciones realizadas correctamente

7.8.7 SHOW IP ROUTE SUCURSAL_QUITO

SUCURSAL_QUITO#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

192.168.3.0/0 is variably subnetted, 8 subnets
C 192.168.3.52/30 is directly connected, Serial0
C 192.168.3.40/30 is directly connected, Serial1
C 192.168.3.32/29 is directly connected, FastEthernet0/0
O 192.168.3.48/30 [110/64] via 192.168.3.53, 00:52:31, FastEthernet0/0
O 192.168.3.16/29 [110/64] via 192.168.3.17, 00:52:31, FastEthernet0/0
O 192.168.3.44/30 [110/128] via 192.168.3.41, 00:52:31, FastEthernet0/0
O 192.168.3.8/29 [110/64] via 192.168.3.9, 00:52:31, FastEthernet0/0
O 192.168.3.24/29 [110/192] via 192.168.3.53, 00:52:30, FastEthernet0/0

192.168.2.0/0 is variably subnetted, 5 subnets
C 192.168.2.192/27 is directly connected, 192.168.2.193
O 192.168.2.112/28 [110/64] via 192.168.2.113, 00:52:31, FastEthernet0/0
O 192.168.2.32/27 [110/64] via 192.168.2.33, 00:52:31, FastEthernet0/0
O 192.168.2.64/27 [110/64] via 192.168.2.65, 00:52:31, FastEthernet0/0
O 192.168.2.96/28 [110/64] via 192.168.2.97, 00:52:31, FastEthernet0/0

7.8.8 SHOW PROTOCOLS SUCURSAL_QUITO

SUCURSAL_QUITO#show protocols

Global values:
Internet Protocol routing is enabled
Serial0 is up, line protocol is up
Internet address is 192.168.3.54/30

Serial1 is up, line protocol is up
Internet address is 192.168.3.42/30

FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.3.33/29

FastEthernet0/1 is administratively down, line protocol is down
Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down

Serial0 / FastEthernet0/0 is up, line protocol is up

Internet address is 192.168.3.178/29

Bri0 is administratively down, line protocol is down

7.8.9 SHOW RUN SUCURSAL_QUITO

SUCURSAL_QUITO#show running-config

```
Building configuration...
Version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname SUCURSAL_QUITO
ip subnet-zero
interface Serial0
ip address 192.168.3.54 255.255.255.252
no ip directed-broadcast
clock rate 64000
bandwidth 1544
interface Serial1
ip address 192.168.3.42 255.255.255.252
no ip directed-broadcast
bandwidth 1544
interface FastEthernet0/0
ip address 192.168.3.33 255.255.255.248
no ip directed-broadcast
bandwidth 100000
ip ospf priority 0
!
interface FastEthernet0/0.1
encapsulation dot1q 80
ip address 192.168.2.193 255.255.255.224
!
interface FastEthernet0/1
no ip address
no ip directed-broadcast
bandwidth 100000
router ospf 1
network 192.168.3.32 0.0.0.7 area 0
network 192.168.3.40 0.0.0.3 area 0
network 192.168.3.52 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
```

7.9 CONFIGURACIÓN DEL SWITCH QUITO

Ingrese al dispositivo, nos solicitará que demos un enter para proceder a digitar los comandos de configuración

Press Enter to Start

7.9.1 ASIGNACIÓN DE NOMBRE

Switch>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado

Switch#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debemos ingresar comandos de configuración

Switch(config)#hostname SW_QUITO
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre

7.9.2 CREACIÓN DE VLAN

SW_QUITO#vlan database
Ingrese a la base de datos de las vlan.

SW_QUITO(vlan)#vlan 80 name QUITO

Cree las vlans con su número identificador seguido del comando name con su nombre único

7.9.3 ASIGNACIÓN DE VLAN A LAS INTERFACES

SW_QUITO(config)#interface fastethernet 0/1
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_QUITO(config-if)#switchport mode trunk
Configure esta interfaz en modo truncado

SW_QUITO(config-if)#switchport trunk encapsulation dot1q
Encapsule el Puerto con el comando *switchport trunk encapsulation dot1q*

SW_QUITO(config)#interface fastethernet 0/2

Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_QUITO(config-if)#switchport access vlan 80
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan

SW_QUITO(config)#interface fastethernet 0/3
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_QUITO(config-if)#switchport access vlan 80
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan

SW_QUITO(config)#interface fastethernet 0/4
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_QUITO(config-if)#switchport access vlan 80
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan

7.9.4 SHOW VLAN SWITCH QUITO

SW_QUITO#show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
80   enet  100080     1500  -      -      -        -    -        0      0
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
```

7.10 CONFIGURACIÓN DEL ROUTER SUCURSAL_BASNOR

Ingrese al dispositivo, nos solicitará que demos un enter para proceder a digitar los comandos de configuración

Press Enter to Start

7.10.1 ASIGNACIÓN DE NOMBRE

Router>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado

Router#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debemos ingresar comandos de configuración

Router(config)#hostname SUCURSAL_BASNOR
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre

7.10.2 ACCESO POR CONSOLA

SUCURSAL_BASNOR(config)#line vty 0 4
Ingrese al modo de configuración del acceso por Terminal Virtual

SUCURSAL_BASNOR(config-line)#password cisco
Digite el comando password seguido del contraseña que quiera asignar

SUCURSAL_BASNOR(config-line)#login
Con el comando Login active el inicio con la contraseña

SUCURSAL_BASNOR(config-line)#exit
Salga con el comando exit para poder configurar el acceso por consola

SUCURSAL_BASNOR(config)#line console 0
Habilite el acceso por consola con el comando line console 0

SUCURSAL_BASNOR(config-line)#password cisco
Ingrese el comando password seguido de la contraseña

SUCURSAL_BASNOR(config-line)#login
Active el inicio con la contraseña

7.10.3 CONFIGURACIÓN DE INTERFACES ETHERNET

Fastethernet 0

SUCURSAL_BASNOR(config)#interface fastethernet 0/0
Digite el comando interface fastethernet 0/0 para poder ingresar al modo de configuración de la interface

SUCURSAL_BASNOR(config-if)#ip address 192.168.3.17 255.255.255.248
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address

SUCURSAL_BASNOR(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.10.3.1 CONFIGURACIÓN DE SUB-INTERFACES

Para configurar una sub-interfaz debemos ingresar al modo de usuario privilegiado

SUCURSAL_BASNOR(config)#interface fastethernet 1/0.1
Digite el comando *interface fastethernet 1/0.1* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.1

SUCURSAL_BASNOR(config)#description VLAN BASNOR
Puede agregar un comentario a la interfaz con el comando description

SUCURSAL_BASNOR(config-subif)#encapsulation dot1q 70
Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 70

SUCURSAL_BASNOR(config-subif)# ip address 192.168.2.129 255.255.255.224
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando *ip address*

7.10.4 CONFIGURACIÓN DE INTERFACES SERIALES

Serial 0

SUCURSAL_BASNOR(config)#interface serial 0
Digite el comando interface serial 0 para poder ingresar al modo de configuración de la interface

SUCURSAL_BASNOR(config-if)#ip address 192.168.3.50 255.255.255.252
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address

SUCURSAL_BASNOR(config-if)#clock rate 64000
Asigne el clock rate con el valor de 64000

SUCURSAL_BASNOR(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface Serial0, changed state to up
Este mensaje aparecerá indicando que está levantada la interface.

Serial 1

SUCURSAL_BASNOR(config)#interface serial 1
Digite el comando interface serial 1 para poder ingresar al modo de configuración de la interface

SUCURSAL_BASNOR(config-if)#ip address 192.168.3.53 255.255.255.252
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address

SUCURSAL_BASNOR(config-if)#no shutdown
Levante la interface con el comando no shutdown, si quiere bajar la interface no al comando shutdown

%LINK-3-UPDOWN: Interface Serial1, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.10.5 CONFIGURACIÓN DEL PROTOCOLO OSPF

SUCURSAL_BASNOR(config)#router ospf 1
Habilite el protocolo de enrutamiento con el comando router rip

SUCURSAL_BASNOR(config-router)#network 192.168.3.52 0.0.0.3 area 0
SUCURSAL_BASNOR(config-router)#network 192.168.3.48 0.0.0.3 area 0
SUCURSAL_BASNOR(config-router)#network 192.168.3.16 0.0.0.7 area 0
Activado el protocolo de enrutamiento ingrese las redes directamente conectadas con el comando network seguido de la wilcard y el área en este caso 0

7.10.6 GUARDAR CONFIGURACIÓN

Salga al modo usuario Privilegiado
SUCURSAL_BASNOR#

SUCURSAL_BASNOR#copy running-config startup-config
Con este comando proceda a grabar las configuraciones: copy running-config startup-config

Destination filename [startup-config]?
Building configuration...
[OK]
Este mensaje aparecerá cuando se haya grabado todas las configuraciones realizadas correctamente

7.10.7 SHOW IP ROUTE SUCURSAL_BASNOR

SUCURSAL_BASNOR#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

192.168.2.0/0 is variably subnetted, 5 subnets
C 192.168.2.128/27 is directly connected, 192.168.2.129
O 192.168.2.112/28 [110/192] via 192.168.3.49, 00:51:07, FastEthernet0/0
O 192.168.2.32/27 [110/192] via 192.168.3.49, 00:00:58, FastEthernet0/0.1.1
O 192.168.2.64/27 [110/192] via 192.168.3.49, 00:00:58, FastEthernet0/0.1.1
O 192.168.2.96/28 [110/192] via 192.168.3.49, 00:00:58, FastEthernet0/0.1.1

192.168.3.0/0 is variably subnetted, 8 subnets
C 192.168.3.48/30 is directly connected, Serial0
C 192.168.3.52/30 is directly connected, Serial1
C 192.168.3.16/29 is directly connected, FastEthernet0/0
O 192.168.3.40/30 [110/64] via 192.168.3.42, 00:51:08, FastEthernet0/0
O 192.168.3.32/29 [110/64] via 192.168.3.33, 00:51:08, FastEthernet0/0
O 192.168.3.44/30 [110/64] via 192.168.3.49, 00:51:08, FastEthernet0/0
O 192.168.3.24/29 [110/64] via 192.168.3.25, 00:51:08, FastEthernet0/0
O 192.168.3.8/29 [110/192] via 192.168.3.54, 00:00:58, FastEthernet0/0.1.1

7.10.8 SHOW PROTOCOLS SUCURSAL_BASNOR

SUCURSAL_BASNOR#show protocols

Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.3.50/30

Serial1 is up, line protocol is up
  Internet address is 192.168.3.53/30

FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.17/29

FastEthernet0/1 is administratively down, line protocol is down
Bri0 is administratively down, line protocol is down
Bri0:1 is administratively down, line protocol is down
Bri0:2 is administratively down, line protocol is down

7.10.9 SHOW RUN SUCURSAL_BASNOR

SUCURSAL_BASNOR#show running-config
Building configuration...
Version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname SUCURSAL_BASNOR
ip subnet-zero
interface Serial0
ip address 192.168.3.50 255.255.255.252
no ip directed-broadcast
clock rate 64000
bandwidth 1544
interface Serial1
ip address 192.168.3.53 255.255.255.252
no ip directed-broadcast
bandwidth 1544
interface FastEthernet0/0
ip address 192.168.3.17 255.255.255.248
no ip directed-broadcast
bandwidth 100000
ip ospf priority 0
interface FastEthernet0/0.1
encapsulation dot1q 70
ip address 192.168.2.129 255.255.255.224
interface FastEthernet0/1
no ip address
no ip directed-broadcast
bandwidth 100000
interface Bri0
no ip address
no ip directed-broadcast
shutdown
router ospf 1
network 192.168.3.16 0.0.0.7 area 0
network 192.168.3.52 0.0.0.3 area 0
network 192.168.3.48 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

7.11 CONFIGURACIÓN DEL SWITCH BASNOR

Ingrese al dispositivo, nos solicitará que demos un enter para proceder a digitar los comandos de configuración.

Press Enter to Start

7.11.1 ASIGNACIÓN DE NOMBRE

Switch>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado.

Switch#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debemos ingresar comandos de configuración

Switch(config)#hostname SW_BASNOR
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre

7.11.2 CREACIÓN DE VLAN

SW_BASNOR#vlan database
Ingrese a la base de datos de las vlan.

SW_BASNOR(vlan)#vlan 10 name BASNOR

Cree las vlans con su número identificador seguido del comando name con su nombre único

7.11.3 ASIGNACIÓN DE VLAN A LAS INTERFACES

SW_BASNOR(config)#interface fastethernet 0/1
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_BASNOR(config-if)#switchport mode trunk
Configure esta interfaz en modo truncado

SW_BASNOR(config-if)#switchport trunk encapsulation dot1q
Encapsule el Puerto con el comando *switchport trunk encapsulation dot1q*

SW_BASNOR(config)#interface fastethernet 0/2
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_BASNOR(config-if)#switchport access vlan 70
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan

SW_BASNOR(config)#interface fastethernet 0/3
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_BASNOR(config-if)#switchport access vlan 70
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan

SW_BASNOR(config)#interface fastethernet 0/4
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_BASNOR(config-if)#switchport access vlan 70
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan

7.11.4 SHOW VLAN SWITCH BASNOR

SW_BASNOR#show vlan

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

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
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

7.12 CONFIGURACIÓN DEL ROUTER SUCURSAL_ESSUNA

Ingrese al dispositivo, nos solicitará que demos un enter para proceder a digitar los comandos de configuración

Press Enter to Start

7.12.1 ASIGNACIÓN DE NOMBRE

Router>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado

Router#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debemos ingresar comandos de configuración

Router(config)#hostname SUCURSAL_ ESSUNA
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre

7.12.2 ACCESO POR CONSOLA

SUCURSAL_ ESSUNA(config)#line vty 0 4
Ingrese al modo de configuración del acceso por Terminal Virtual

SUCURSAL_ ESSUNA(config-line)#password cisco
Digite el comando password seguido del contraseña que quiera asignar

SUCURSAL_ ESSUNA(config-line)#login
Con el comando Login active el inicio con la contraseña

SUCURSAL_ ESSUNA(config-line)#exit
Salga con el comando exit para poder configurar el acceso por consola

SUCURSAL_ ESSUNA(config)#line console 0
Habilite el acceso por consola con el comando line console 0

SUCURSAL_ ESSUNA(config-line)#password cisco
Ingrese el comando password seguido de la contraseña

SUCURSAL_ ESSUNA(config-line)#login
Active el inicio con la contraseña

7.12.3 CONFIGURACIÓN DE INTERFACES ETHERNET

Fastethernet 0

SUCURSAL_ ESSUNA(config)#interface fastethernet 0/0
Digite el comando interface fastethernet 0/0 para poder ingresar al modo de configuración de la interface

SUCURSAL_ ESSUNA(config-if)#ip address 192.168.3.25 255.255.255.248
Asigne la dirección ip con su respectiva máscara de subred con el comando IP address

SUCURSAL_ ESSUNA(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.12.3.1 CONFIGURACIÓN DE SUB-INTERFACES ETHERNET

Para configurar una sub-interfaz debemos ingresar al modo de usuario privilegiado

SUCURSAL_ ESSUNA(config)#interface fastethernet 1/0.1
Digite el comando *interface fastethernet 1/0.1* para ingresar en el modo de configuración de la sub-interfaz fastethernet 1/0.1

SUCURSAL_ ESSUNA(config)#description VLAN ESSUNA
Puede agregar un comentario a la interfaz con el comando description

SUCURSAL_ ESSUNA(config-subif)#encapsulation dot1q 60
Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1q* y el número de la Vlan que en este caso es 60

SUCURSAL_ ESSUNA(config-subif)#ip address 192.168.2.161 255.255.255.224
Por último asigne una dirección IP seguida de su máscara de sub-red a la sub-interfaz con el comando *ip address*

7.12.4 CONFIGURACIÓN DE INTERFACES SERIALES

Serial 0

SUCURSAL_ ESSUNA(config)#interface serial 0
Digite el comando interface serial 0 para poder ingresar al modo de configuración de la interface

SUCURSAL_ ESSUNA(config-if)#ip address 192.168.3.49 255.255.255.252
Asigne la dirección ip con su respectiva máscara de subred con el comando IP address

SUCURSAL_ ESSUNA(config-if)#clock rate 64000
Asigne el clock rate con el valor de 64000

SUCURSAL_ ESSUNA(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface Serial0, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

Serial 1

SUCURSAL_ ESSUNA(config)#interface serial 1
Digite el comando interface serial 1 para poder ingresar al modo de configuración de la interface

SUCURSAL_ ESSUNA(config-if)#ip address 192.168.3.46 255.255.255.252
Asigne la dirección ip con su respectiva máscara de subred con el comando ip address

SUCURSAL_ ESSUNA(config-if)#no shutdown
Levante la interface puesta con el comando no shutdown, si quiere bajar la interface anteponga no al comando shutdown

%LINK-3-UPDOWN: Interface Serial1, changed state to up
Este mensaje aparecerá indicando que están levantada la interface.

7.12.5 CONFIGURACIÓN DEL PROTOCOLO OSPF

SUCURSAL_ ESSUNA(config)#router ospf 1
Habilite el protocolo de enrutamiento con el comando router rip

SUCURSAL_ ESSUNA(config-router)#network 192.168.3.48 0.0.0.3 area 0
SUCURSAL_ ESSUNA(config-router)#network 192.168.3.44 0.0.0.3 area 0
SUCURSAL_ ESSUNA(config-router)#network 192.168.3.24 0.0.0.7 area 0
SUCURSAL_ ESSUNA(config-router)#exit

Activado el protocolo de enrutamiento ingrese las redes directamente conectadas con el comando network seguido de la Wildcard y el área en este caso 0

7.12.6 GUARDAR CONFIGURACIÓN

Salga al modo usuario Privilegiado
SUCURSAL_ ESSUNA#

SUCURSAL_ ESSUNA#copy running-config startup-config
Con este comando proceda a grabar las configuraciones: copy running-config startup-config

Destination filename [startup-config]?
Building configuration...
[OK]
Este mensaje aparecerá cuando se haya grabado todas las configuraciones realizadas correctamente.

7.12.7 SHOW IP ROUTE SUCURSAL_ESSUNA

SUCURSAL_ESSUNA#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

192.168.3.0/0 is variably subnetted, 8 subnets
C 192.168.3.44/30 is directly connected, Serial0
C 192.168.3.48/30 is directly connected, Serial1
C 192.168.3.24/29 is directly connected, FastEthernet0/0
O 192.168.3.52/30 [110/128] via 192.168.3.50, 00:51:38, FastEthernet0/0
O 192.168.3.16/29 [110/64] via 192.168.3.17, 00:51:38, FastEthernet0/0
O 192.168.3.40/30 [110/128] via 192.168.3.45, 00:51:38, FastEthernet0/0
O 192.168.3.8/29 [110/64] via 192.168.3.9, 00:51:38, FastEthernet0/0
O 192.168.3.32/29 [110/192] via 192.168.3.50, 00:17:57, FastEthernet0/0

192.168.2.0/0 is variably subnetted, 5 subnets
C 192.168.2.160/27 is directly connected, 192.168.2.161
O 192.168.2.112/28 [110/64] via 192.168.2.113, 00:51:38, FastEthernet0/0
O 192.168.2.32/27 [110/64] via 192.168.2.33, 00:51:38, FastEthernet0/0
O 192.168.2.64/27 [110/64] via 192.168.2.65, 00:51:38, FastEthernet0/0
O 192.168.2.96/28 [110/64] via 192.168.2.97, 00:51:38, FastEthernet0/0

7.12.8 SHOW PROTOCOLS SUCURSAL_ESSUNA

SUCURSAL_ESSUNA#show protocols

Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.3.46/30

Serial1 is up, line protocol is up
  Internet address is 192.168.3.49/30

FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.25/29

7.12.9 SHOW RUN SUCURSAL_ESSUNA

```
SUCURSAL_ESSUNA#show running-config
Building configuration...
Version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

hostname SUCURSAL_ESSUNA
ip subnet-zero
interface Serial0
ip address 192.168.3.46 255.255.255.252
no ip directed-broadcast
clock rate 64000
bandwidth 1544
interface Serial1
ip address 192.168.3.49 255.255.255.252
no ip directed-broadcast
bandwidth 1544
interface FastEthernet0/0
ip address 192.168.3.25 255.255.255.248
no ip directed-broadcast
bandwidth 100000
ip ospf priority 0
interface FastEthernet0/0.1
encapsulation dot1q 60
ip address 192.168.2.161 255.255.255.224
interface FastEthernet0/1
no ip address
no ip directed-broadcast
bandwidth 100000
router ospf 1
network 192.168.3.24 0.0.0.7 area 0
network 192.168.3.48 0.0.0.3 area 0
network 192.168.3.44 0.0.0.3 area 0

ip classless

no ip http server

line con 0
line aux 0

line vty 0 4

no scheduler allocate
end
```

7.13 CONFIGURACIÓN DEL SWITCH ESSUNA

Ingrese al dispositivo, nos solicitará que demos un enter para proceder a digitar los comandos de configuración

Press Enter to Start

7.13.1 ASIGNACIÓN DE NOMBRE

Switch>enable
En el modo usuario normal, digite el comando **enable** para ingresar en el modo privilegiado

Switch#configure terminal
Digite el comando **configure Terminal** para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

Enter configuration commands, one per line. End with CNTL/Z.
Este mensaje aparecerá indicando que debemos ingresar comandos de configuración

Switch(config)#hostname SW_ESSUNA
Digite el comando hostname seguido del nombre del dispositivo para determinar el nombre

7.13.2 CREACIÓN DE VLAN

SW_ESSUNA#vlan database
Ingrese a la base de datos de las vlan.

SW_ESSUNA(vlan)#vlan 10 name ESSUNA

Cree las vlans con su número identificador seguido del comando name con su nombre único

7.13.3 ASIGNACIÓN DE VLAN A LAS INTERFACES

SW_ESSUNA(config)#interface fastethernet 0/1
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_ESSUNA(config-if)#switchport mode trunk
Configure esta interfaz en modo truncado.

SW_ESSUNA(config-if)#switchport trunk encapsulation dot1q
Encapsule el Puerto con el comando *switchport trunk encapsulation dot1q.*

SW_ESSUNA(config)#interface fastethernet 0/2
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_ESSUNA(config-if)#switchport access vlan 10
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_ESSUNA(config)#interface fastethernet 0/3
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz.

SW_ESSUNA(config-if)#switchport access vlan 10
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

SW_ESSUNA(config)#interface fastethernet 0/4
Ingrese en la configuración de la interfaz con el comando *interface fastethernet* con el número de la interfaz

SW_ESSUNA(config-if)#switchport access vlan 10
Agregue esta interfaz a la vlan especificada con el comando switchport access vlan seguido del número de la vlan.

7.13.4 SHOW VLAN SWITCH ESSUNA

SW_ESSUNA#show vlan

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

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
60	enet	100060	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

ANEXO A

GLOSARIO DE TÉRMINOS TÉCNICOS

A

ACL (lista de control de acceso): Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router).

Actualización del enrutamiento: Mensaje que se envía desde el router para indicar si la red es accesible y la información de costo asociada. Normalmente, las actualizaciones del enrutamiento se envían a intervalos regulares y luego de que se produce un cambio en la topología de la red.

Administración de red: Uso de sistemas o acciones para mantener, caracterizar o realizar el diagnóstico de fallas de una red.

Administrador de red: Persona a cargo de la operación, mantenimiento y administración de una red.

Ancho de Banda: (Bandwidth en inglés). Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información. Se mide en millones de bits por segundo (Mbps). Una buena analogía es una autopista. Mientras más carriles tenga la calle, mayor cantidad de tráfico podrá transitar a mayores velocidades. El ancho de banda es un concepto muy parecido. Es la cantidad de información que puede transmitirse en una conexión durante una unidad de tiempo elegida.

ANSI: American National Standards Institute - Instituto Nacional de Normas de Estados Unidos.

Antena: Una antena es un dispositivo capaz de emitir o recibir ondas de radio.

Antivirus: Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente. Entre los más famosos están Norton (http://www.norton.com/) y McAfee (http://www.mcafee.com/) y Trend Micro Pccilin (http://www.antivirus.com/).

Apache: Apache es programa de servidor HTTP Web de código abierto (open source). Fue desarrollado en 1995 y actualmente es uno de los servidores Web más utilizados en la red. Usualmente corre en UNIX, Linux, BSD y Windows. Es un poderoso paquete de servidor Web con muchos módulos que se le pueden agregar y que se consiguen gratuitamente en el Internet. Uno de sus competidores es Microsoft IIS. http://www.apache.org/

Aplicación: Cualquier programa que corra en un sistema operativo y que haga una función específica para un usuario. Por ejemplo, procesadores de palabras, bases de datos, agendas electrónicas, etc.

B

Backbone: Mecanismo de conectividad primario en un sistema distribuido. Todos los sistemas que tengan conexión al backbone (columna vertebral) pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas.

Backup: Copia de Respaldo o Seguridad. Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

Balanceo de la carga: En el enrutamiento, la capacidad de un router para distribuir el tráfico a lo largo de todos sus puertos de red que están a la misma distancia desde la dirección destino. El balanceo de carga aumenta el uso de segmentos de red, aumentando así el ancho de banda efectivo de la red.

Banda ancha: Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etcétera).

Base de datos: Una base o banco de datos es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso. En una base de datos, la información se organiza en campos y registros. Un campo se refiere a un tipo o atributo de información, y un registro, a toda la información sobre un individuo. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo. Normalmente las bases de datos presentan la posibilidad de consultar datos, bien los de un registro o los de una serie de registros que cumplan una condición.

Baudios: El baudio es la medida que se utiliza para medir la velocidad de transmisión de los datos.

Binario: Sistema numérico compuesto por unos y ceros (1 = encendido; 0 = apagado).

Bit: Dígito Binario. Unidad mínima de almacenamiento de la información cuyo valor puede ser 0 ó 1 (falso o verdadero respectivamente).

Bps: Bits por Segundo. Velocidad a la que se transmiten los bits en un medio de comunicación

Broadcast: Paquete de datos enviado a todos los dispositivos de una red. Los broadcasts se identifican por una dirección broadcast.

Browser: Aplicación para visualizar todo tipo de información y navegar por el www con funcionalidades plenamente multimedia. Ejemplo: Internet Explorer, Firefox, etc.

Bug: Error en el hardware o en el software que, si bien no impide la ejecución de un programa, perjudica el rendimiento del mismo al no permitir la realización de determinadas tareas o al complicar su normal funcionamiento.

Byte: Conjunto de 8 bit, el cual suele representar un valor asignado a un carácter.

C

Cableado: Columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado

Caché: Copia que mantiene una computadora de las páginas web visitadas últimamente, de forma que si el usuario vuelve a solicitarlas, las mismas son leídas desde el disco duro sin necesidad de tener que conectarse de nuevo a la red; consiguiéndose así una mejora muy apreciable en la velocidad.

Carpeta: Espacio del disco duro de una computadora cuya estructura jerárquica en forma de árbol contiene la información almacenada en una computadora, habitualmente en archivos y es identificado mediante un nombre (ej. "Mis documentos").

Carriers: Operadores de telecomunicaciones propietarios de las redes troncales de Internet y responsables del transporte de los datos. Proporciona una conexión a Internet de alto nivel.

Clic: Cuando se oprime alguno de lo botones de un mouse el sonido es parecido a un "click". La palabra click escrita, se usa generalmente para indicarle al usuario que oprima el botón del mouse encima de un área de la pantalla.

Cliente: Aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red. Sistema o proceso el cual le solicita a otro sistema o proceso la prestación de un servicio.

Colisión: Una colisión sucede cuando dos sistemas están intentando usar el mismo medio de transmisión al mismo tiempo. Si múltiples estaciones envían datos al mismo tiempo se produce una colisión, en este caso cada estación esperara un tiempo aleatorio para comenzar de nuevo la transmisión.

Conexión Remota: Operación realizada en una computadora remota a través de una red de computadoras, como si se tratase de una conexión local.

Congestión: Situación que se produce cuando el tráfico existente sobrepasa la capacidad de una ruta de comunicación de datos.

Conmutación de Paquetes: Un portador separa los datos en paquetes. Cada paquete contiene la dirección de origen, la dirección de su destino, e información acerca de cómo volver a unirse con otros paquetes emparentados. Cada paquete de un mensaje recorre una ruta entre sistemas anfitriones (hosts), sin que esa ruta (path) esté previamente definida. Este proceso permite que paquetes de distintas localizaciones se entremezclen en las mismas líneas y que sean clasificados y dirigidos a distintas rutas.

Contraseña: Password. Código utilizado para accesar un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

D

Dato: Unidad mínima que compone cualquier información.

DCE: Acrónimo de Data Communications Equipment (Equipo para comunicaciones de datos). Se refiere a cualquier dispositivo que esté preparado para transmitir/recibir datos.

Denegación de Servicio: Incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red. Un ataque de denegación de servicio puede también destruir programas y archivos de un sistema informático. Aunque normalmente es realizado de forma intencionada y maliciosa, este tipo de ataques puede también ocurrir de forma accidental algunas veces. Si bien no suele producirse robo de información estos ataques pueden costar mucho tiempo y dinero a la persona u organización afectada.

Desencriptación/ Descifrado: Recuperación del contenido real de una información previamente cifrada.

DNS: Servidor de Nombres de Dominio. Servidor automatizado utilizado en el internet cuya tares es convertir nombres fáciles de entender (como www.armada.mil) a direcciones numéricas de IP.

Dominio: Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Comprenden una red de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios. Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre. Los más comunes son .com, .edu, .net, .org y .gov; la mayoría de los países tienen su propio dominio, y en la actualidad se están ofreciendo muchos dominios nuevos debido a la saturación de los dominios .com (utilizados muchas por empresas).

Download: Descarga. Proceso en el cual información es transferida desde un servidor a una computadora personal.

DTE: Acrónimo de Data Terminal Equipment (Equipo terminal de datos). Se refiere a cualquier dispositivo que esté preparado para recibir datos.

Dúplex: Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir/ transmitir cualquier tipo de información. Existen dos modalidades HALF-DUPLEX cuando puede recibir y transmitir alternativamente y FULL-DUPLEX cuando puede hacer ambas cosas simultáneamente.

E

EIA/ITIA-568: Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP.

E-mail: El e-mail, de las palabras inglesas electronic mail (correo electrónico), es uno de los medios de comunicación de más rápido crecimiento en la historia de la humanidad y más usados en Internet. Por medio del protocolo de comunicación TCP/IP, permite el intercambio de mensajes entre las personas conectadas a la red de manera similar al correo tradicional. Para ello es necesario disponer de una dirección de correo electrónico, compuesta por el nombre del usuario, la arroba "@" y el nombre del servidor de correo. Por ejemplo, sample@panamacom.com, donde 'sample' es el usuario y panamacom.com el nombre del host o servidor. El email esta conformado por los siguientes encabezados principales:

- ✓ De: (From) el nombre y dirección de email del que envía.
- ✓ Para: (To) el nombre y dirección de email del que recibe.
- ✓ Asunto: (Subject) es la breve descripción del contenido del email.
- ✓ CC: es la copia carbón (carbon copy) y define una o varias direcciones de email que van a recibir copia exacta enviada al destinatario(s) original. Todos pueden ver a quien se les envió los emails. Lo malo de esto es que muchas veces se forman cadenas de email extensas y caen en manos de algún spammer.
- ✓ CCO es la copia carbón oculta, en ingles BCC (blind carbon copy), lo mismo que CC. pero el/los destinatarios originales no podrán ver las direcciones de email que se hicieron copia.
- ✓ Adjunto, en inglés attachment. El email puede contener cualquier archivo en formato digital (texto, gráficos, hojas de cálculo, imágenes fijas o en movimiento, sonido, etc).

Encapsulamiento: El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

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.

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.

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, tiene ancho de banda de10 Mbps de forma que presenta una elevada velocidad de transmisión; y se ha convertido en un estándar de red corporativa.

E1: Estándar Europeo equivalente al americano Ti. Los circuitos El y Ti. Los dos usan canales de 64 Kbps, pero el Ti tiene 24 mientras que el El tiene 32 canales.

F

Fast Ethernet: Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT.

Fibra óptica: Fibra basada en el vidrio, que sustituye a los clásicos cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda electromagnética generada por un láser.

Firewall: Un cortafuegos o firewall en Inglés, es un equipo de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidos por las políticas de red, las cuales se fundamentan en las necesidades del usuario.

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.

G

Gateway: El significado técnico se refiere a un hardware o software que traduce dos protocolos distintos o no compatibles. Gateway o pasarela es un dispositivo, con frecuencia un ordenador, que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, un gateway de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

Gigabit: No debe ser confundido con Gigabyte. Un gigabit es igual a 10^9 (1.000.000.000) bits, que equivalen a 125 megabytes decimales.

Gigabyte: El gigabyte (GB) equivale a 1.024 millones de bytes, o 1024 Megabytes. Se usa comúnmente para describir el espacio disponible en un medio de almacenamiento.

GNU: El Proyecto GNU fue creado en 1984 con el fin de desarrollar un sistema operativo tipo Unix según la filosofía del "software libre".

Grupo de trabajo: Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

Gusano: Programa informático que se auto duplica y auto propaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (Marzo 1982). El primer gusano famoso de Internet apareció en Noviembre de 1988 y se propagó por sí solo a más de 6.000 sistemas a lo largo de Internet

H

Hardware: Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

HC: (interconexión horizontal): Armario de cableado donde el cableado horizontal se conecta a un panel de conmutación conectado mediante cableado backbone al MDF.

Hercio: Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

Host: Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas (ssh, FTP, www, email, etc.). Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

HTTP: En inglés Hypertext Transfer Protocol. Protocolo de Transferencia de Hipertexto. HTTP es un protocolo con la ligereza y velocidad necesaria para distribuir y manejar sistemas de información hipermedia. HTTP ha sido usado por los servidores World Wide Web desde su inicio en 1993.

Hub: El punto central de conexión para un grupo de nodos: útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

I

IEEE: (Instituto de Ingeniería Eléctrica y Electrónica): Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares de mayor importancia para las LAN de la actualidad.

ICMP: Internet Control Message Protocol. Protocolo de Control de Mensajes Internet. Es una extensión del IP (Internet Protocol) definida por RFC 792. Permite la generación de mensajes de error, paquetes de prueba e información relacionados a un IP. Un ejemplo es el comando "ping" que usa ICMP.

Icono: Símbolo gráfico que aparece en la pantalla de un ordenador con el fin de representar ya sea una determinada acción a realizar por el usuario (ejecutar un programa, leer una información, imprimir un texto, un documento, un dispositivo, un estado del sistema, etc).

IDF: (Servicio de distribución intermedia)Sala de comunicaciones secundaria para un edificio donde funciona una topología de networking en estrella. El IDF depende del MDF.

Impresora: Periférico que pasa la información de una computadora a un medio físico, que usualmente es el papel.

Intel: El fabricante líder de microprocesadores para PC. Los procesadores Intel fueron usados en las primeras computadoras que incorporaban el sistema operativo DOS de Microsoft. Su línea de procesadores Pentium incremento los niveles de desempeño de las computadoras a niveles superiores. Intel también fabrica tarjetas madre (motherboards), procesadores de red y un sin fin de circuitos procesadores que están pavimentando el futuro de la computación personal.

Interfaz: (Interface) Zona de contacto o conexión entre dos componentes de "hardware"; entre dos aplicaciones; o entre un usuario y una aplicación. Apariencia externa de una aplicación informática.

Interfaz Gráfica de Usuario: En inglés Graphic User Interface, corto como GUI. Componente de una aplicación informática que el usuario visualiza y a través de la cual opera con ella. Está formada por ventanas, botones, menús e iconos, entre otros elementos. Ejemplo, Windows y X window.

Internet: Una red mundial, de redes de computadoras. Es una interconexión de redes grandes y chicas alrededor del mundo. El Internet empezó en 1962 como una red para los militares llamada ARPANet, para que en sus comunicaciones no existan "puntos de falla". Con el tiempo fue creciendo hasta convertirse en lo que es hoy en día, una herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Sobre esta red se pueden utilizar múltiples servicios como por ejemplo emails, WWW, etc. que usen TCP/IP.

Internet Explorer: Conocido también como IE es el browser web de Microsoft, creado en 1995 para Windows y mucho después para Mac. En la actualidad navegadores como Firefox están ganando terreno.

Intranet: Red privada dentro de una compañía u organización que utiliza el navegador favorito de cada usuario, en su computadora, para ver menús con opciones desde cumpleaños del personal, calendario de citas, mensajería instantánea privada, repositorio de archivos y las normativas de la empresa entre otras. Es como si fuera un sitio web dentro de la empresa. Al usar los browser de internet como Internet Explorer, Firefox o Safari el intranet se convierte en multiplataforma. No importa la marca o sistema operativo de las computadoras dentro de la red, todos se pueden comunicar.

IP: (Internet Protocol), Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10

IT: Del ingles Information Technology (Tecnología de Información). Término muy general que se refiere al campo entero de la tecnología informática - que incluye hardware de computadoras y programación hasta administración de redes. La mayoría de las empresas medianas y grandes tienen departamentos de IT (TI en español).

ISP:(Internet Service Provider). Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

K

Kbps: Kilobits por segundo. Unidad de medida que comúnmente se usa para medir la velocidad de transmisión por una línea de telecomunicación, como la velocidad de un cable módem por ejemplo.

Kernel: El kernel (en ingles) es el centro esencial de un sistema operativo, el núcleo que proporciona servicios básicos para todas las partes del sistema operativo. El kernel contrasta con el "shell", la parte exterior del sistema operativo que interactúa con el usuario por medio de comandos. Kernel y shell son más usados en el mundo de Unix que en IBM o Microsoft Windows.

Kilobit: Su abreviatura es Kb. Aproximadamente mil bits (exactamente 1024). Se usa generalmente para referirse a velocidades de transmisión de datos.

Kilobyte: Unidad de medida equivalente a 1024 (dos elevado a la 10) bytes. Se usa frecuentemente para referirse a la capacidad de almacenamiento o tamaño de un archivo.

L

LAN: Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones. Por ejemplo, computadoras conectadas en una oficina, en un edificio o en varios. Se pueden optimizarse los protocolos de señal de la red hasta alcanzar velocidades de transmisión de 100 Mbps.

Latencia: Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir. Intervalo de tiempo que toma el procesamiento de una tarea.

Línea Conmutada: Dial Up. Conexión de red la cual se puede crear y desechar según se requiera que se establece usando un emulador de terminal y un módem y realiza una conexión de datos a través de una línea telefónica.

Línea Dedicada: Línea privada que se utiliza para conectar redes de área local de tamaño moderado a un proveedor de servicios de Internet y se caracteriza por ser una conexión permanente.

Log Files: Registro de todos los hits que un servidor ha recibido en un período de tiempo dado el cual puede ser utilizado por auditores externos para registrar el uso del sitio.

Login: Clave de acceso que se le asigna a un usuario con el propósito de que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de Internet junto con la dirección electrónica de la computadora que utiliza.

M

MAC: (Control de Acceso al Medio) Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

Máscara de subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Máscara wildcard: Cantidad de 32 bits que se utiliza junto con una dirección IP para determinar qué bits en una dirección IP deben ser ignorados cuando se compara dicha dirección con otra dirección IP. Una máscara wildcard se especifica al configurar una ACL.

Mbps: Megabits por Segundo. Unidad de medida de la capacidad de transmisión por una línea de telecomunicación donde cada megabit está formado por 1.048.576 bits.

Medio: Material utilizado para la transmisión de los datos. Puede ser cable de cobre, coaxial, fibra óptica o ondas electromagnéticas.

Megabyte: El Megabyte (MB) equivale a un millón de bytes, o mil kilobytes (exactamente 1,048,576 bytes).

MHz: Unidad de frecuencia que equivale a un millón de ciclos por segundo.

Microprocesador: Microchip. Circuito integrado en un soporte de silicón el cual está formado por transistores y otros elementos electrónicos miniaturizados. Es uno de los elementos esenciales de una computadora.

Modelo Cliente-Servidor: Sistema que se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor). De esta manera los clientes son los elementos que necesitan servicios del recurso y el servidor es la entidad que lo posee. El servidor los provee únicamente de la información sin hacerse cargo de otros procesos de forma que el tráfico en la red se ve aligerado y las comunicaciones entre las computadoras se realizan más rápido.

Módem: Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una ISDN, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información). Los módems pueden ser en internos (los que se colocan en una ranura de la computadora) y en externos (que se conectan a un puerto serial de la computadora).

MS-DOS: Sistema operativo DOS, de Microsoft. Su entorno es de texto, tipo consola, y no gráfico. Sigue siendo parte importante de los sistemas operativos gráficos de Windows.

Memoria flash: Almacenamiento no volátil que se puede borrar eléctricamente y reprogramar, de manera que las imágenes de software se pueden almacenar, iniciar y reescribir según sea necesario.

N

Nodo: Cada una de las computadoras individuales u otros dispositivos de la red.

NAT: (traducción de direcciones de red) Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a la Internet transformando esas direcciones en espacio de direccionamiento enrutable global. También denominado traductor de dirección de red.

NIC: (tarjeta de interfaz de red) Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

NVRAM: (RAM no volátil) Memoria RAM que conserva su contenido cuando se apaga una unidad.

Networking: Interconexión de estaciones de trabajo, dispositivos periféricos (por ejemplo, impresoras, unidades de disco duro, escáneres) y otros dispositivos. Término utilizado para referirse a las redes de telecomunicaciones en general.

O

OSPF: (Primero la ruta libre más corta) Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor costo, el enrutamiento de múltiples rutas, y el balanceo de carga.

OSI: Interconexión de Sistemas Abiertos (Open Systems Interconnect). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a trabes de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

Octeto: 8 bits. En networking, el término octeto se utiliza a menudo (en lugar de byte) porque algunas arquitecturas de máquina utilizan bytes que no son de 8 bits de largo.

Ordenador: En Hispanoamérica se le conoce comúnmente como computadora, pero en España les llaman ordenador.

Oracle: Oracle es básicamente una herramienta cliente/servidor para la gestión de Bases de Datos. Es manejador de base de datos relacional que hace uso de los recursos del sistema informático en todas las arquitecturas de hardware, para garantizar su aprovechamiento al máximo en ambientes cargados de información. Oracle corre en PC's, microcomputadoras, mainframes y computadoras con procesamiento paralelo masivo.

Off-line: No estar conectado a la red.

On-line: Estar conectado a una red

P

Panel de conmutación: Conjunto de ubicaciones de pins y puertos que se pueden montar en un bastidor o en una consola en el armario de cableado. Los paneles de conmutación actúan como tableros de conmutación 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 la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Ping: Packet Internet Groper. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa. Lo que se está haciendo en realidad es mandar paquetes a donde se le indique y nos dice cuanto tiempo demoró el paquete en ir y regresar, entre otras informaciones. Entre sus usos más comunes: resolver el nombre de host para saber su IP o simplemente verificar si una máquina está prendida. Un "ping" sin respuesta no necesariamente significa que la computadora no existe o esta apagada.

PPP (Protocolo Punto a Punto): Sucesor del SLIP, un protocolo que suministra conexiones router a router y host a red a través de circuitos síncronos y asíncronos.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina

Proxy: Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) los cuales impiden accesos no autorizados desde el exterior hacia la red privada.

Puente: Dispositivos que tienen usos definidos como interconectar segmentos de red a través de medios físicos diferentes (es usual ver puentes entre un cable coaxial y otro de fibra óptica). Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y física de modelo OSI).

Puerto: Número que aparece tras un nombre de dominio en una URL. Dicho número va precedido del signo (dos puntos). Canal de entrada/salida de una computadora.

Q

QoS: (calidad de servicio) Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

R

Rack: El Rack es un armario que ayuda a tener organizado todo el sistema informático de una empresa. Posee unos soportes para conectar los equipos con una separación estándar de 19". Debe estar provisto de ventiladores y extractores de aire, además de conexiones adecuadas de corriente. Hay modelos abiertos que sólo tienen los soportes con la separación de 19" y otros más costosos cerrados y con puerta panorámica para supervisar el funcionamiento de los equipos activos y el estado de las conexiones. También existen otros modelos que son para sujetar en la pared, estos no son de gran tamaño.

Raíz: (Root) Directorio inicial de un sistema de archivos mientras que en entornos LINUX/UNIX también se refiere al usuario principal.

RAM: Random Access Memory (memoria de acceso aleatorio). Memoria volátil (los datos e instrucciones se borran al apagarse la PC) que puede ser escrita y leída. La memoria del equipo permite almacenar datos de entrada, instrucciones de los programas que se están ejecutando en ese momento, los datos resultados del procesamiento y los datos que se preparan para la salida.

Red: (Network) Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Redundancia: Duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla.

Rendimiento: Velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

RJ45: Es uno de los dos tipos de conectores usados en las computadoras, emplea un cable y un conector muy similares a los del teléfono, donde cada PC tiene su propio cable.

.

ROM: Read Only Memory (memoria de sólo lectura). en la cual se almacena ciertos programas e información que necesita la computadora las cuales están grabadas permanentemente y no pueden ser cambiadas por el programador. Las instrucciones básicas para arrancar una computadora están grabadas aquí.

Router: Un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino. El router esta conectado por lo menos a dos redes, y determina hacia que lado enviar el paquete de data dependiendo en el entendimiento del router sobre las redes que esta conectado. Los routers crean o mantienen una "tabla" de rutas disponibles, y usa esta información para darle la mejor ruta a un paquete, en un determinado momento.

RPM: Package Manager (o RPM, originalmente llamado Red Hat Package Manager). Es una herramienta que facilita la administración de paquetes pensada básicamente para Linux. Es capaz de instalar, actualizar, desinstalar, verificar y solicitar programas.

S

Segmentación: Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de la red.

Segmento: Sección de una red que está rodeada de puentes, routers o switches 2. En una LAN que usa topología de bus, un circuito eléctrico continúo que a menudo está conectado a otros segmentos similares a través de repetidores. 3. En la especificación TCP, una unidad única de información de capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Servidor: Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes). También puede referirse a un software específico, como lo es el servidor WWW. Una computadora puede tener distintos software de servidor, proporcionando muchos servidores a clientes en la red.

Sesión: Conjunto relacionado de transacciones de comunicaciones orientadas a conexión entre dos o más dispositivos de red. 2. En SNA, una conexión lógica que permite que dos unidades de red direccionables se comuniquen.

Sesión Remota: Uso de los recursos de una computadora desde una terminal la cual no se encuentra cercana a dicha computadora.

Shell: Programa a través del cual un usuario se comunica con el sistema operativo. Existen varios tipos (sabores) de shells de UNIX, como son Bourne, Korn, C, shell.

SNMP: Acrónimo de Simple Network Management Protocol. Protocolo estándar para la administración de red en Internet. Prácticamente todos los sistemas operativos, routers, switches, módems cable o ADSL módem, firewalls, etc.

Software: Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

Spam: Envío masivo, indiscriminado y no solicitado de publicidad a través de email.

Squid: Servidor caché / proxy de alta capacidad y rendimiento de código fuente abierto, muy usado en servidores Linux.

Spyware: Son unos pequeños programas cuyo objetivo es mandar información, generalmente a empresas de mercadeo, del uso de internet, websites visitados, etc. del usuario, por medio del internet. Usualmente estas acciones son llevadas a cabo sin el conocimiento del usuario, y consumen ancho de banda, la computadora se pone lenta, etc.

Switch: Llamado también conmutador. Dispositivo utilizado para conectar varios equipos informáticos, en redes locales. Más seguro y fiable que el Hub.

T

Tabla de enrutamiento: Tabla almacenada en un router o en algún otro dispositivo de internetwork que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

Tarjeta Madre: Mother board en Inglés. Es una tarjeta de circuitos integrados que contiene varios microchips, como lo son normalmente: el microprocesador, circuitos electrónicos de soporte, ranuras para conectar parte o toda la RAM del sistema, la ROM y ranuras especiales (slots) que permiten conexión de tarjetas adaptadoras adicionales.

TCP/IP: El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet. Forma de comunicación básica que usa el Internet, la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

Telefonía IP: La señal analógica de la voz es convertida en señal digital que puede transitar por Internet. La calidad del sonido en las redes TCP/IP depende del ancho de banda del que se dispone.

Telnet: Servicio de Internet con el cual un usuario se puede conectar de forma remota a otra computadora, como si se hiciera desde un terminal local, usualmente por el puerto 23.

TIA (Asociación de la Industria de las Telecomunicaciones): Organización que desarrolla estándares relacionados con las tecnologías de telecomunicaciones. En conjunto, TIA y EIA han formalizado estándares, como EIA/TIA-232, para las características eléctricas de la transmisión de datos.

Topología de Red: Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Existen tres topologías principales de red anillo, bus y estrella.

Tunneling: Tecnología que permite que una red mande su data por medio de las conexiones de otra red. Funciona encapsulando un protocolo de red dentro de los paquetes de la segunda red. Es el acto de encapsular un protocolo de comunicación dentro de otro a través de dispositivos y Routers.

T-1: Una línea dedicada capaz de transferir datos a 1,544,000 bits – por-segundo. Teóricamente una T-1 a su máxima capacidad de transmisión transporta un megabyte en menos de 10 segundos. Sin embargo, esto no es lo suficiente rápido para pantallas completas con movimiento general, para las cuales se requiere al menos 10.00,000 bits-por-segundo. Una T-1 es el medio más rápido comúnmente usado para realizar conexiones a Internet.

T-3: Es una conexión a través de una línea conmutada capaz de transmitir datos a 44,736,000 bits por segundo. Esto es más que suficiente para desplegar video en pantalla completa con movimiento continuo.

U

UDP: (Protocolo de Datagrama de Usuario) Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

Unicast: Mensaje que se envía a un solo destino de red.

URL: (localizador de recursos uniforme) Esquema de direccionamiento estandarizado para acceder a documentos de hipertexto y otros servicios utilizando un explorador de Web.

Usuario: Persona que tiene una cuenta en una determinada computadora por medio de la cual puede acceder a los recursos y servicios que ofrece una red..

UTP (par trenzado no blindado): Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Hay cinco tipos de cableado UTP de uso común: cableado de Categoría 1, Categoría 2, Categoría 3, Categoría 4, Categoría 5 y Categoría 6.

V

Vínculo: Link. Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor Web a otro, cuando se navega por Internet.

Virtual: Término de frecuente utilización en el mundo de las tecnologías de la información y de las comunicaciones el cual designa dispositivos o funciones simulados.

Virus: Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas pueden actuar de diversas maneras.

VoIP: La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways, teléfonos IP y teléfonos estándares.

VPN: Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.

VLAN: (LAN virtual) Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

W

WAN: es un acrónimo de Wide Area Network Red de Área Extensa. Red de comunicaciones que cubre una gran área. Una red WAN puede abarcar una gran área geográfica y puede contener varias redes LAN.

Web site: Conjunto de páginas Web que usualmente comparten un mismo tema e intención.

WiFi: Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz. Ha ganado aceptación en mucho ambientes como una alternativa viable a los LANs cableados. Muchos hoteles, restaurantes, aeropuertos, etc. ofrecen acceso público a Internet por medio de WiFi. A estos lugares se les conoce como "hotspots". Se deben tomar las medidas mínimas de seguridad (firewall) en las computadoras con capacidad WiFi, y sobretodo en los routers inalámbricos para proteger el acceso a la red por personas ajenas a la misma. Sin los controles necesarios, cualquier persona cerca al radio de transmisión de su router inalámbrico puede conseguir conexión a Internet, navegar con su ancho de banda e incluso hackear su red privada.

Windows: Sistema operativo desarrollado por la empresa Microsoft cuyas diversas versiones (3.1, 95, 98, NT, 2000, XP, ME, etc) han dominado de forma abrumadora el mercado de las computadoras personales, aunque no se puede decir lo mismo del mercado de redes corporativas. Windows proporciona una interfaz estándar basada en menús desplegables, ventanas en pantalla y un dispositivo señalador como el ratón. Los programas deben estar especialmente diseñados para aprovechar estas características.

WLAN: Acrónimo en inglés para Wireless Local Area Network. Red inalámbrica de área local permite que un usuario móvil pueda conectarse a una red de área local (LAN) por medio de una conexión inalámbrica de radio. Hoy en día puede cubrir áreas desde 20 a 70 metros dentro de edificios y hasta 350 metros afuera. Este sistema de transmisión inalámbrica permite velocidades de hasta 3 a 4 Mbps.

World Wide Web: Comúnmente conocido como WWW. Es el sistema de información basado en hipertexto, cuya función es buscar y tener acceso a documentos a través de la red de forma que un usuario pueda accesar usando un navegador web. Creada a principios de los años 90 por Tim Berners-Lee, investigador en el CERN, Suiza. La información transmitida por el www puede ser de cualquier formato (texto, gráfico, audio y video).

X

X window: Entorno gráfico no exclusivo que se usa frecuentemente en Unix / Linux, de fuente abierta. Fue desarrollado en MIT y es independiente del hardware o del sistema operativo.