

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

T e m a :

Administración y Seguridad en Redes

Manual de Usuario

Autores:

Karina Elizabeth Miranda Arévalo

Silvia Elizabeth Ramos Santana

Wilson Humberto Yáñez Barcia

DIRECTOR:

Anl. Fabian 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 SEGURIDAD EN REDES

MANUAL DE USUARIO

AUTORES
KARINA ELIZABETH MIRANDA AREVALO
SILVIA ELIZABETH RAMOS SANTANA
WILSON HUMBERTO YANEZ BARCIA

DIRECTOR
ANL. FABIAN BARBOZA

AÑO
2007

AGRADECIMIENTO

Queremos agradecer a nuestro Padre Celestial por habernos permitido culminar este proyecto realizado con mucho empeño.

A nuestros Padres también queremos agradecer por habernos apoyado incondicionalmente a lo largo de nuestra carrera universitaria y ayudarnos a obtener nuestro título.

A nuestros Profesores por habernos enseñado con paciencia y esfuerzo, ya que gracias a la enseñanza de ellos hemos podido culminar este proyecto.



DEDICATORIA

Este trabajo fue hecho con mucho esfuerzo y empeño, por eso se lo dedicamos en primer lugar al creador de nuestras vidas Dios, ya que sin Él no hubiera sido posible realizarlo.

En segundo lugar a nuestros Padres quienes nos apoyaron desde el inicio de nuestros estudios y quienes estuvieron ahí para darnos aliento y fuerza para continuar y no rendirnos, y por último a los verdaderos amigos que realmente nos ayudaron con sus palabras y quienes demostraron ser nuestros verdaderos amigos en las buenas y las malas, y quienes nos ayudaron a sonreír cuando realmente queríamos llorar.



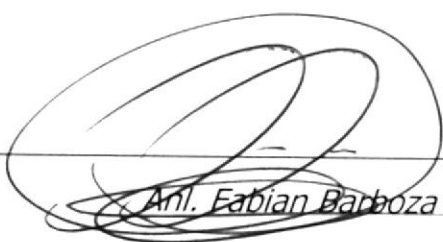
DECLARACIÓN EXPRESA

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

(Reglamentos de Exámenes Y Títulos Profesionales de la ESPOL).



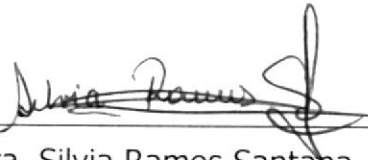
FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN



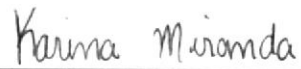
Aní. Fabian Barboza

RECIBIDO
EN
LA
SECRETARÍA
DE
EDUCACIÓN
Y
CULTURA
DEL
GOBIERNO
NACIONAL
DE
COLOMBIA
EL
10
DE
NOVIEMBRE
DE
2010

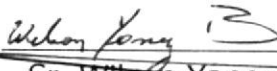
FIRMA DE AUTORES

A handwritten signature in black ink, appearing to read 'Silvia Ramos', written over a horizontal line.

Srta. Silvia Ramos Santana

A handwritten signature in black ink, appearing to read 'Karina Miranda', written over a horizontal line.

Srta. Karina Miranda Arévalo

A handwritten signature in black ink, appearing to read 'Wilson Yanez', written over a horizontal line. The signature is enclosed within an oval-shaped stamp.

Sr. Wilson Yanez Barcia

ÍNDICE GENERAL

CAPÍTULO 1

1. GENERALIDADES	1
1.1 INTRODUCCIÓN	1
1.2 OBJETIVO DE ESTE MANUAL.....	1
1.3 A QUIEN VA DIRIGIDO	1

CAPÍTULO 2

2. SITUACIÓN ACTUAL	1
2.1 ANTECEDENTES DE LA EMPRESA	1
2.2 MISIÓN DE LA EMPRESA.....	1
2.3 VISIÓN DE LA EMPRESA	1
2.4 INFRAESTRUCTURA LAN DE LA EMPRESA.....	2
2.5 MATRIZ DE GUAYAQUIL.....	2
2.6 AGENCIA PORTETE.....	2
2.7 AGENCIA URDESA	3
2.8 ESTRUCTURA DE LOS EDIFICIOS	4
2.8.1. MATRIZ (TERCER PISO)	4
2.8.2. PORTETE (PLANTA BAJA)	5
2.8.3. EDIFICIO URDESA.....	6
2.9 ANÁLISIS DE PISO LÓGICO.....	7
2.9.1. MATRIZ (GUAYAQUIL).....	7
2.9.2. AGENCIA (PORTETE).....	8
2.9.3. AGENCIA (URDESA).....	9
2.10 ANÁLISIS PISO APLICATIVO.....	10
2.10.1. MATRIZ (GUAYAQUIL).....	10
2.10.2. AGENCIA (PORTETE).....	11
2.10.3. AGENCIA (URDESA)	12
2.11 CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO	13
2.11.1. MATRIZ – GUAYAQUIL.....	13
2.11.2. AGENCIA PORTETE	14
2.11.3. AGENCIA URDESA.....	14
2.12 CARACTERÍSTICAS DE LOS SERVIDORES.....	15
2.12.1. MATRIZ - GUAYAQUIL	15
2.12.2. AGENCIA PORTETE	17
2.12.3. AGENCIA URDESA	17
2.13 DISPOSITIVOS DE CONMUTACIÓN	18
2.13.1. MATRIZ – GUAYAQUIL.....	18
2.13.2. AGENCIA PORTETE	19
2.13.3. AGENCIA - URDESA.....	20
2.14 GRÁFICO DEL MC	21
2.14.1. MATRIZ GUAYAQUIL	21

2.14.2.	AGENCIA PORTETE	22
2.14.3.	ANGENCIA URDESA.....	23
2.15	INFRAESTRUCTURA GENERAL DE LA RED LAN	24
2.15.1.	MATRIZ	24
2.15.2.	AGENCIAS (PORTETE – URDESA).....	24
2.16	INFRAESTRUCTURA WAN DE LA EMPRESA SERVIPAGOS	25
2.17	INFRAESTRUCTURA GENERAL DE LA COMUNICACIÓN WAN	25
2.18	TOPOLOGÍA ANILLO	26
2.18.1.	ANILLO NORTE (GRÁFICO DE COMUNICACIÓN)	26
2.18.2.	ANILLO SUR (GRÁFICO DE COMUNICACIÓN).....	27
2.19	INFRAESTRUCTURA WAN A NIVEL DE DISPOSITIVOS	28
2.19.1.	TOPOLOGÍA ANILLO NORTE	29
2.19.2.	TOPOLOGÍA ANILLO SUR.....	30
2.20	DISPOSITIVOS DE ENRUTAMIENTO	31
2.20.1.	MATRIZ – GUAYAQUIL.....	31
2.20.2.	AGENCIA PORTETE	32
2.20.3.	SUCURSAL - URDESA.....	32
2.21	INFRAESTRUCTURA DE SEGURIDAD DE REDES WAN	33
2.22	INFRAESTRUCTURA RECEPCIÓN DE INTERNET.....	34
2.23	PROBLEMAS ENCONTRADOS EN LA SITUACIÓN ACTUAL	35

CAPÍTULO 3

3.	SOLUCIÓN PROPUESTA	1
3.1	PROBLEMAS ENCONTRADOS	1
3.2	SOLUCIÓN	2
3.3	ESTUDIO DE LA ALTERNATIVA "A"	3
3.3.1.	FACTIBILIDAD TÉCNICA	3
3.4	FACTIBILIDAD ECONÓMICA	5
3.4.1.	COSTOS EQUIPOS.....	5
3.4.2.	COSTO DE ALQUILER DE LOS DISPOSITIVOS CON EL ISP.....	5
3.4.3.	COSTO DEL ENLACE	6
3.4.4.	COSTO DE AUMENTO ANCHO DE BANDA	6
3.4.5.	COSTO OPERATIVO.....	7
3.5	FACTIBILIDAD OPERATIVA	8
3.5.1.	DETALLE DE LA FASE DE ANÁLISIS LAN Y WAN	8
3.6	COSTO TOTAL DE LA PROPUESTA "A"	9
3.7	VENTAJAS & BENEFICIO	10
3.7.1.	VENTAJAS.....	10
3.7.2.	BENEFICIO	10
3.8	FORMA DE PAGO	11
3.9	GARANTÍA.....	11
3.10	GANT-A.....	12
3.11	ESTUDIO DE LA ALTERNATIVA "B"	13
3.11.1.	FACTIBILIDAD TÉCNICA.....	13
3.12	FACTIBILIDAD ECÓNOMICA	15
3.12.1.	COSTO DE EQUIPOS	15

3.12.2. COSTO DEL ENLACE CON EL ISP.....	15
3.12.3. COSTO DE AUMENTO ANCHO DE BANDA.....	16
3.12.4. COSTO OPERATIVO.....	17
3.13 FACTIBILIDAD OPERATIVA	18
3.13.1. DETALLE DE LA FASE DE ANÁLISIS LAN Y WAN	18
3.14 COSTO TOTAL DE LA PROPUESTA "B"	19
3.15 VENTAJAS & BENEFICIO	20
3.15.1. VENTAJAS.....	20
3.15.2. BENEFICIO	20
3.16 FORMA DE PAGO.....	21
3.17 GARANTÍA.....	21
3.18 GANT-B.....	22

CAPÍTULO 4

4. IMPLEMENTACIÓN WAN	1
4.1 NIVEL WAN	1
4.2 ENLACE DE CONEXIÓN	3
4.3 IMPLEMENTACIÓN DEL MC	5
4.3.1. MC (MATRIZ)	5
4.3.2. MC (PORTETE)	6
4.4 ANCHO DE BANDA (MATRIZ-URDESA)	7
4.5 IMPLEMENTACIÓN DE VLAN.....	8

CAPÍTULO 5

5. NORMATIVAS.....	1
5.1 REGLAS DEL CABLEADO ESTRUCTURADO.....	1
5.2 OBLIGATORIO	1
5.3 RECOMENDACIONES	29

CAPÍTULO 6

6. LINUX.....	1
6.1 INTRODUCCIÓN DE LINUX.....	1
6.2 COMPONENTES DE LINUX.....	2
6.3 REQUERIMIENTO DE HARDWARE.....	4
6.4 INTRODUCCIÓN A FEDORA CORE3.....	5
6.5 ENTRADA AL BIOS.....	6
6.6 INSTALACIÓN DE LINUX	8
6.7 CONFIGURACIÓN DE POST-INSTALACIÓN LINUX.....	25
6.8 INICIO DE SESIÓN AMBIENTE GRÁFICO	29
6.9 INICIO DE SESIÓN MODO TEXTO.....	30
6.10 COMANDOS DE LINUX	32
6.11 INFORMACIÓN DEL SISTEMA Y USUARIOS	39
6.12 DIRECTORIOS	40

6.13	ORGANIZACIÓN DE LOS DIRECTORIOS	42
6.14	LISTADO DIRECTORIOS COMANDOS BÁSICOS.....	44
6.15	ARCHIVOS ESPECIALES	44
6.16	SISTEMAS DE ARCHIVOS	45
6.17	CONFIGURACIÓN STANDAR PARA CUALQUIER SERVICIO.....	46
6.17.1.	CONFIGURACIÓN DE LA TRAJETA DE RED MODO TEXTO	46
6.17.2.	CONFIGURACIÓN DE LA TARJETA DE RED MODO GRÁFICO	48
6.18	SERVIDOR SAMBA	50
6.19	SERVICIOS DE SAMBA	50
6.20	DEMONIOS DE SAMBA.....	51
6.20.1.	QUÉ HACE SAMBA DESDE CLIENTE	51
6.20.2.	SAMBA. VISIÓN DESDE SERVIDOR.....	52
6.20.3.	OBJETIVO	53
6.20.4.	ESQUEMA SAMBA.....	53
6.21	CONFIGURACIÓN DEL SERVIDOR SAMBA EN LINUX	54
6.22	CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	64
6.23	SERVIDOR DNS	66
6.23.1.	BÚSQUEDAS CON DNS	68
6.23.2.	TIPOS DE SERVIDORES DE NOMBRES.....	69
6.23.3.	LA BASE DE DATOS DNS.....	70
6.23.4.	OBJETIVO DEL DNS.....	71
6.23.5.	APLICACIONES DE DNS	72
6.23.6.	BENEFICIOS.....	72
6.24	CONFIGURACIÓN DEL SERVICIO DNS EN LINUX	73
6.25	CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	81
6.26	SERVIDOR WEB SERVER.....	84
6.26.1.	BENEFICIOS AL INSTALAR UN SERVIDOR WEB EN LINUX:	85
6.26.2.	HTTP REQUEST	86
6.27	CONFIGURACIÓN DE SERVIDOR WEB EN LINUX	87
6.28	ACCESO DEL CLIENTE EN WINDOWS	93
6.29	SERVIDOR PROXY	95
6.30	CONFIGURACIÓN DE SERVIDOR PROXY EN LINUX.....	97
6.30.1.	AUTENTICAR	103
6.30.2.	LISTAS Y REGLAS DE CONTROL DE ACCESO.....	106
6.30.3.	PARA BLOQUEAR UNA PÁGINA.....	107
6.31	CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	111
6.31.1.	COMPROBACIÓN DE SU SALIDA POR PROXY	111
6.31.2.	COMPROBACIÓN DE AUTENTIFICACION.....	113
6.31.3.	COMPROBACIÓN DE PÁGINAS DENEGADAS.....	114
6.31.4.	COMPROBACIÓN DE DENEGACIÓN POR TIEMPO	115
6.32	SERVIDOR SENDMAIL.....	116
6.32.1.	ENVIAR MENSAJES (SERVIDOR DE CORREO SMTP)	117
6.32.2.	(SERVIDOR DE CORREO POP).....	117
6.32.3.	OBJETIVO DE SERVIDOR POP.....	117
6.32.4.	OBJETIVO DE SERVIDOR DE CORREO	118
6.33	CONFIGURACIÓN DEL SERVIDOR SENDMAIL EN LINUX.....	119
6.34	CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	125
6.35	SERVIDOR FIREWALLS	131



6.35.1. INTRODUCCIÓN A IPTABLES.	132
6.35.2. REGLAS DE IPTABLES.....	132
6.35.3. COMANDOS PARA AÑADIR Y MANIPULAR CADENAS.....	133
6.36 COMANDOS STANDAR PARA CONFIGURACIÓN DE FIREWALL.....	134
6.36.1. BLOQUEAR TELNET	135
6.36.2. BLOQUEAR SMPT	136
6.36.3. BLOQUEAR FTP	137
6.36.4. BLOQUEAR HTTP	138
6.36.5. BLOQUEAR DNS	139
6.36.6. BLOQUEAR POP3.....	140
6.36.7. ACEPTACIÓN DE REGLAS.....	143
6.36.8. CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	152
6.37 SERVIDOR DHCP (Dynamic Host Configuration Protocol).....	155
6.37.1. QUE REALIZA DHCP :	155
6.37.2. COMPONENTTES PRINCIPALES DE DHCP	155
6.37.3. COMO FUNCIONA DHCP	156
6.37.4. VENTAJAS DE DHCP	157
6.37.5. DESVENTAJAS DE DHCP	157
6.37.6. CONFIGURACIÓN DEL SERVIDOR DHCP	158
6.37.7. CONFIGURACIÓN EN EL CLIENTE WINDOWS.....	161

CAPÍTULO 7

7. CONFIGURACIÓN DE ROUTERS Y SWITCH.....	1
7.1 INTRODUCCIÓN	1
7.2 INTERFAZ DTE-DCE.....	2
7.3 COMPONENTES INTERNOS DEL ROUTER.....	3
7.3.1. RAM	4
7.3.2. NVRAM	4
7.3.3. FLASH	4
7.3.4. ROM.....	4
7.3.5. CONSOLA	5
7.3.6. INTERFAZ	5
7.4 CONEXIONES EXTERNAS DEL ROUTER	6
7.4.1. CONEXIÓN LAN	6
7.4.2. CONEXIÓN WAN	6
7.4.3. CONEXIONES DE PUERTOS ADMINISTRATIVOS.....	6
7.5 VENTAS Y DESVENTAJAS DE UN ROUTERS	7
7.6 FUNCIONES DE UN ROUTER	7
7.7 BENEFICIOS DE UN ROUTER.....	7
7.8 TECNOLOGÍA DE RUTEADOR	8
7.9 HYPERTERMINAL.....	9
7.10 CONFIGURACIÓN DEL HYPERTERMINAL	10
7.11 MODOS DE UN ROUTER.....	14
7.12 COMADOS SHOWS	15
7.12.1. SHOW VERSIÓN.....	15
7.12.2. SHOW INTERFACES.....	16



7.12.3.	SHOW PROTOCOLS	17
7.12.4.	SHOW CLOCK	17
7.12.5.	SHOW HISTORY	17
7.12.6.	SHOW IP ROUTE	18
7.12.7.	SHOW VLANS	18
7.12.8.	SHOW ACCESS-LISTIS	19
7.12.9.	SHOW TERMINAL	19
7.12.10.	SHOW RUNNING-CONFIG	20
7.12.11.	SHOW FLASH	21
7.13	PROTOCOLOS DE ENRUTAMIENTOS	22
7.13.1.	INTRODUCCIÓN	22
7.14	ENRUTAMIENTO DINÁMICO VS. ESTÁTICO	23
7.15	PROTOCOLOS RIP	24
7.15.1.	INTRODUCCIÓN HISTÓRICA	24
7.15.2.	INTRODUCCIÓN TÉCNICA	24
7.15.3.	VERSIONES RIP	25
7.15.4.	CARACTERÍSTICAS RIP	26
7.15.5.	MÁSCARA DE RED DE RIP	26
7.15.6.	VERSIÓN 1 DE RIP	26
7.15.7.	VERSIÓN 2 DE RIP	26
7.15.8.	VENTAJAS Y DESVENTAJAS DE RIP	27
7.15.8.1.	VENTAJAS	27
7.15.8.2.	DESVENTAJAS	27
7.15.9.	FUNCIONAMIENTO RIP	27
7.16	PROTOCOLOS OSPF	28
7.16.1.	INTRODUCCIÓN HISTÓRICA	28
7.16.2.	INTRODUCCIÓN TÉCNICA	29
7.16.3.	CARACTERÍSTICAS OSPF	30
7.16.4.	CONEXIONES QUE SOPORTA OSPF	30
7.16.5.	VENTAJAS Y DESVENTAJAS DE OSPF	31
7.16.5.1.	VENTAJAS	31
7.16.5.2.	DESVENTAJAS	31
7.16.6.	FUNCIONAMIENTO DE OSPF	32
7.16.7.	DESCUBRIMIENTO VECINO OSPF	32
7.16.8.	DETERMINANDO EL DR	33
7.16.9.	RESPONSABILIDADES DEL DR:	33
7.16.10.	FORMANDO ADYACENCIAS	34
7.16.11.	SINCRONIZACIÓN DE LAS BASES DE DATOS	35
7.16.12.	CALCULANDO LA TABLA DE ENCAMINAMIENTO	37
7.16.13.	ANUNCIANDO LOS ESTADOS DE LOS ENLACES	37
7.16.14.	CONCLUSIONES DEL PROTOCOLÓ OSPF	38
7.17	LISTA DE ACCESO	39
7.17.1.	INTRODUCCIÓN	39
7.17.2.	EJECUCIÓN DE LAS ACLS	40
7.17.3.	CREACIÓN DE LAS ACLS	41
7.17.3.1.	ACLS ESTÁNDAR	41
7.17.3.2.	ACLS EXTENDIDAS	42
7.17.4.	¿POR QUÉ USAR ACLS?	43



7.18 SWITCHES	44
7.18.1. INTRODUCCIÓN	44
7.18.2. TECNOLOGÍA DE SWITCH.....	44
7.18.3. QUE ES UNA SEGMENTACIÓN	45
7.18.4. TIPOS DE SWICHT	45
7.18.4.1. TIPOS DE CAPAS DE SWITCH.....	46
7.18.4.1.1. SWITCH CAPA 2	46
7.18.4.1.2. SWITCH CAPA 3	48
7.18.4.1.3. SWITCH CAPA 4	49
7.18.4.2. CONSIDERACIONES ACERCA DE SWITCH	49
7.19 VLANS.....	50
7.19.1. INTRODUCCIÓN	50
7.19.2. SEGMENTACIÓN TRADICIONAL.....	51
7.19.2.1. SEGMENTACIÓN CON VLANS	51
7.19.3. ENCAPSULAMIENTO	52
7.19.4. CARACTERÍSTICAS DE LAS VLANS	52
7.19.4.1. ASIGNACIÓN A VLANS	52
7.19.4.1.1. ESTÁTICA:	52
7.19.4.1.2. DINÁMICA:	52
7.19.5. TIPOS DE VLANS.....	53
7.19.5.1. VLAN ENTRE SWITCHES: FILTRADO.....	53
7.19.5.2. VLAN ENTRE SWITCHES: ETIQUETADO	54
7.19.5.3. SEGURIDAD DE VLANS	55
7.19.5.4. VENTAJAS DE LAS VLANS.....	55
7.20 IMPLEMENTACIÓN WAN	56
7.21 GRÁFICO LÓGICO DE LA COMUNICACIÓN WAN	57
7.22 CONFIGURACIÓN DE LOS ROUTER Y SWICHT	58
7.22.1. ASIGNACIÓN DE NOMBRE AL ROUTER.....	58
7.22.2. CONFIGURACIÓN DE LAS INTERFACES (s0/0 - s0/1).....	61
7.22.2.1. ROUTER_1	66
7.22.2.2. ROUTER_2	67
7.22.2.3. VERIFICAR SI LAS DIRECCIONES FUERON LEVANTADAS CON ÉXITO	68
7.22.2.4. CONFIGURAR LAS FASTETHERNET	71
7.22.2.5. ROUTER URDESA	72
7.22.2.6. VERIFICAR SI LAS DIRECCIONES FASTETHERNET FUERON LEVANTADAS CON ÉXITO	73
7.22.2.7. CONFIGURAR TELNET.....	75
7.22.3. VERIFICACIÓN TELNET	81
7.22.3.1. ROUTER_CONEXIÓN_PORTETE.....	81
7.22.4. CONFIGURACIÓN DE LOS PROTOCOLOS ENRUTAMIENTO.....	82
7.22.4.1. ROUTER PORTETE	83
7.22.4.1.1. PROTOCOLO RIP	83
7.22.4.2. ROUTER MATRIZ	84
7.22.4.2.1. ROUTER_CONEXIÓN_PORTETE.....	84
7.22.4.2.1.1. PROTOCOLO RIP	84
7.22.4.2.1.2. PROTOCOLO OSPF	85
7.22.4.2.2. ROUTER_CONEXIÓN_URDESA	86

7.22.4.2.2.1. PROTOCOLO OSPF	86
7.22.4.2.2.2. PROTOCOLO RIP	86
7.22.4.2.2.3. ROUTER_CORE	87
7.22.4.2.2.4. PROTOCOLO OSPF	87
7.22.4.3. ROUTER URDESA	88
7.22.4.3.1. ROUTER_1	88
7.22.4.3.1.1. PROTOCOLO RIP	88
7.22.4.3.2. ROUTER_2	89
7.22.4.3.2.1. PROTOCOLO RIP	89
7.22.5. SHOW IP ROUTER	90
7.22.5.1. ROUTER PORTETE	90
7.22.5.2. ROUTER MATRIZ	91
7.22.5.2.1. ROUTER_CONEXIÓN_PORTETE	91
7.22.5.2.2. ROUTER_CORE	92
7.22.5.2.3. ROUTER_CONEXIÓN_URDESA	93
7.22.5.3. ROUTER URDESA	94
7.22.5.3.1. ROUTER_1	94
7.22.5.3.2. ROUTER_2	95
7.22.6. PRUEBAS COMUNICACIÓN ENTRE SUCURSALES Y MATRIZ	96
7.22.6.1. ROUTER PORTETE	96
7.22.6.1.1. ROUTER MATRIZ	97
7.22.6.1.1.1. ROUTER_CONEXIÓN_PORTETE	97
7.22.6.1.1.2. ROUTER_CORE	98
7.22.6.1.1.3. ROUTER_CONEXIÓN_URDESA	100
7.22.6.2. ROUTER URDESA	101
7.22.6.2.1. ROUTER_1	101
7.22.6.2.2. ROUTER_2	102
7.22.6.3. CONFIGURACIÓN DE LAS VLANS	104
7.22.6.3.1. CONFIGURACIÓN VLANS PORTETE	104
7.22.6.3.2. PRUEBAS DE COMUNICACIÓN ENTRE VLANS PORTETE	112
7.22.6.3.3. CONFIGURACIÓN VLANS URDESA	114
7.22.6.3.4. PRUEBAS DE COMUNICACIÓN ENTRE VLANS URDESA	121
7.22.6.3.5. CONFIGURACIÓN VLANS MATRIZ	123
7.22.6.3.6. SWITCH 1 MASTER	123
7.22.6.3.7. SWITCH 2 ESCLAVO	124
7.22.6.3.8. CONFIGURACIÓN SWITCH 1 MASTER	125
7.22.6.3.8.1. PRUEBAS DE COMUNICACIÓN VLANS DEL SWITCH MASTER	133
7.22.6.3.8.2. CONFIGURACIÓN SWITCH 2 ESCLAVO	136
7.22.6.3.8.3. PRUEBAS DE COMUNICACIÓN ENTRE VLANS DEL SWITCH ESCLAVO	143
7.22.6.3.9. PRUEBAS DE COMUNICACIÓN ENTRE SWITCH MASTER- ESCLAVO	145
7.22.6.3.10. PRUEBAS DE COMUNICACIÓN ENTRE SWITCH ESCLAVO- MASTER	148

ANEXO

A. GLOSARIO DE PALABRAS TÉCNICAS..... 152

ÍNDICE DE IMÁGENES



CAPÍTULO 2

Figura 2-1: edificio Matriz	4
Figura 2-2: Edificio Portete	5
Figura 2-3: edificio Urdesa	6
Figura 2-4: piso Lógico Matriz	7
Figura 2-5: piso Lógico Portete	8
Figura 2-6: piso Lógico Urdesa	9
Figura 2-7: piso aplicativo Matriz	10
Figura 2-8: piso aplicativo Portete	11
Figura 2-9: piso aplicativo Urdesa	12
Figura 2-10: Mc-Matriz	21
Figura 2-11: Mc-Portete	22
Figura 2-12: Mc-Urdesa	23
Figura 2-13: Gráfico Comunicación Wan	25
Figura 2-14: Gráfico Anillo Norte	26
Figura 2-15: Gráfico Anillo Sur	27
Figura 2-16: Gráfico Nivel Dispositivos	28
Figura 2-17: Anillo Norte Nivel Dispositivos	29
Figura 2-18: Anillo Sur Nivel Dispositivos	30
Figura 2-19: Infraestructura Nivel Wan	33
Figura 2-20: Infraestructura recepción Internet	34

CAPÍTULO 3

Figura 3-1: Gant A	12
Figura 3-2: Gant B	22

CAPÍTULO 5

Figura 5-1: Normativa 1	1
Figura 5-2: Normativa 1	1
Figura 5-3: Normativa 2	2
Figura 5-4: Normativa 3	2
Figura 5-5: Normativa 4	3
Figura 5-6: Normativa 5	3
Figura 5-7: Normativa 6	4
Figura 5-8: Normativa 7	4
Figura 5-9: Normativa 8	5
Figura 5-10: Normativa 9	5
Figura 5-11: Normativa 10	6

Figura 5-12: Normativa 11	6
Figura 5-13: Normativa 12	7
Figura 5-14: Normativa 13	7
Figura 5-15: Normativa 14	8
Figura 5-16: Normativa 15	8
Figura 5-17: Normativa 16	9
Figura 5-18: Normativa 17	9
Figura 5-19: Normativa 18	10
Figura 5-20 Normativa 19	10
Figura 5-21: Normativ 20	11
Figura 5-22: Normativa 21	11
Figura 5-23: Normativa 22	12
Figura 5-24: Normativa 23	12
Figura 5-25: Normativa 24	13
Figura 5-26: Normativa 25	14
Figura 5-27: Normativa 26	14
Figura 5-28: Normativa 27	15
Figura 5-29: Normativa 28	15
Figura 5-30: Normativa 29	16
Figura 5-31: Normativa 30	16
Figura 5-32: Normativa 31	17
Figura:5-33: Normativa 32	17
Figura 5-34: Normativa 33	18
Figura 5-35: Normativa 34	18
Figura 5-36 : Normativa 35	19
Figura 5-37: Normativa 36	19
Figura 5-38: Normativa 37	20
Figura 5-39: Normativa 38	20
Figura 5-40: Normativa 39	21
Figura 5-41: Normativa 40	21
Figura 5-42: Normativa 41	22
Figura 5-43: Normativa 42	22
Figura 5-44: Normativa 43	23
Figura 5-45: Normativa 44	23
Figura 5-46: Normativa 45	24
Figura 5-47: Normativa 46	24
Figura 5-48: Normativa 47	24
Figura 5-49: Normativa 48	25
Figura 5-50: Normativa 49	25
Figura 5-51: Normativa 50	26
Figura 5-52: Normativa 51	26
Figura 5-53: Normativa 52	26
Figura 5-54: Normativa 53	27
Figura 5-55: Normativa 54	27
Figura 5-56: Normativa 55	28
Figura 5-57: Normativa 56	28
Figura 5-58: Recomendación 1	29
Figura 5-59: Recomendación 2	29

Figura 5-60: Recomendación 3	30
Figura 5-61: Recomendación 4	30
Figura 5-62: Recomendación 5	31
Figura 5-63: Recomendación 6	31
Figura 5-64: Recomendación 7	32
Figura 5-65: Recomendación 8	32
Figura 5-66: Recomendación 9	33
Figura 5-67: Recomendación 10	33
Figura 5-68: Recomendación 11	34
Figura 5-69: Recomendación 12	34
Figura 5-70: Recomendación 13	35
Figura 5-71: Recomendación 14	35

CAPÍTULO 6

Figura 6-1: Pinguino.....	1
Figura 6-2: GNU/LINUX	2
Figura 6-3: Pantalla del Bios.....	7
Figura 6-4: Ingreso del Cd de Arranque.....	8
Figura 6-5: opción de sKip	8
Figura 6-6: Bienvenido a Fedora Core	9
Figura 6-7: Configuración de teclado	9
Figura 6-8: Selección del Lenguaje.....	10
Figura 6-9: Tipo de Instalación	10
Figura 6-10: Configuración de particionamiento del disco	11
Figura 6-11: Configuración del disco.....	12
Figura 6-12: Partición de swap	12
Figura 6-13: Partición de Boot.....	13
Figura 6-14: Configuración de Directorio raíz	13
Figura 6-15: Creación de todas las particiones.....	14
Figura 6-16: Configuración de gestor de arranque.....	14
Figura 6-17: Configuración de la red.....	15
Figura 6-18: Configuración del cortafuego.....	15
Figura 6-19: Advertencia de Cortafuego.....	16
Figura 6-20: Soporte adicional de idioma	16
Figura 6-21: Selección de horario.....	17
Figura 6-22: Configuración de contraseña	17
Figura 6-23: Selección de paquetes de escritorio	18
Figura 6-24: Selección de grupos de paquetes	18
Figura 6-25: Selección de paquetes de Servidores	19
Figura 6-26: Selección de paquetes de desarrollo	19
Figura 6-27: Selección de paquetes de sistemas	20
Figura 6-28: Listo para la instalación	21
Figura 6-29: Medio de instalación requerido.....	21
Figura 6-30: Instalación de paquetes 1	22
Figura 6-31: Instalación de los paquetes 2	22
Figura 6-32: Ingreso del segundo cd de fedora.....	23
Figura 6-33: ingreso del último cd para la instalación.....	23

Figura 6-34: reinicio del sistema	24
Figura 6-35: ingreso al entorno de linux	25
Figura 6-36: Bienvenido al entorno de fedora	25
Figura 6-37: Acuerdo de licencia	26
Figura 6-38: configuración de fecha y hora	26
Figura 6-39: configuración de la pantalla	27
Figura 6-40: usuario del sistema.....	27
Figura 6-41: configuración de tarjeta de sonido	28
Figura 6-42: finalización de la configuración.....	28
Figura 6-43: ingreso del root a fedora corel3	29
Figura 6-44: ingreso de contraseña	29
Figura 6-45: Ingreso del login	30
Figura 6-46: Ingreso root.....	30
Figura 6-47: Ingreso la contraseña del root	31
Figura 6-48: Ingreso a modo texto	31
Figura 6-49: configuración de la tarjeta de red.....	46
Figura 6-50: levantamiento de la tarjeta de red	47
Figura 6-51: ingreso al setup	48
Figura 6-52: configuración de la red	48
Figura 6-53: confirmación de configuración.....	48
Figura 6-54: configuración tcp/ip.....	49
Figura 6-55: levantamiento de tarjeta red	49
Figura 6-56: entorno samba	53
Figura 6-57: verificación de paquete.....	54
Figura 6-58: Editor de Samba	54
Figura 6-59: global settings.....	55
Figura 6-60: cambios en global settings.....	55
Figura 6-61: encriptación de claves.....	56
Figura 6-62: descomentamos el encriptación	56
Figura 6-63: share definitions sin cambios.....	57
Figura 6-64: cambios realizados en share definitions.....	57
Figura 6-65: Creación de la carpeta de respaldo	58
Figura 6-66: cambio de propietario	59
Figura 6-67: creación de usuarios	60
Figura 6-68: creación de archivo práctica	60
Figura 6-69: permisos a la carpeta.....	61
Figura 6-70: levantamiento del servicio samba	62
Figura 6-71: ingreso al setup	62
Figura 6-72: ingreso al servicio de sistema.....	63
Figura 6-73: elección de paquete smb.....	63
Figura 6-74: ejecutar en el cliente.....	64
Figura 6-75: ingreso de usuario creado en servidor samba	64
Figura 6-76: ingreso a la carpeta.....	65
Figura 6-77: Archivo creado en Linux.....	65
Figura 6-78: Ingreso al archivo respaldo.....	65
Figura 6-79: raíz del árbol.....	66
Figura 6-80: Gráfico del DNS.....	71
Figura 6-81: verificación de paquete bind.....	73

Figura 6-82: editar configuración de zona	73
Figura 6-83: cambios en zona	74
Figura 6-84: ingreso al var/named	75
Figura 6-85: copia de configuración a localhost	75
Figura 6-86: visualización de la zona servipagos	75
Figura 6-87: editar zona servipagos	76
Figura 6-88: sin cambios en configuración de zona	76
Figura 6-89: cambios en zona servipagos	77
Figura 6-90: copia de zona servipagos	77
Figura 6-91: editar resolv	78
Figura 6-92: cambios en resolv	78
Figura 6-93: levantamiento del server named	79
Figura 6-94: prueba del ping	79
Figura 6-95: ping a www.servipagos.com	79
Figura 6-96: ingreso del setup	79
Figura 6-97: ingreso del servicio de sistema	80
Figura 6-98: elección de servicio named	80
Figura 6-99: ingreso de las propiedades de la red	81
Figura 6-100: ingreso de las propiedades de area local	81
Figura 6-101: priopiedades tcp/ip	82
Figura 6-102: configuración de ip de dns	82
Figura 6-103: Ingreso a Ejecutar	83
Figura 6-104: Prueba de conectividad al dominio	83
Figura 6-105: esquema web server	86
Figura 6-106: verificación de paquete httpd	87
Figura 6-107: ingreso a la configuración httpd	87
Figura 6-108: editar configuración de hhttpd	88
Figura 6-109: línea de index	88
Figura 6-110: name virtual	88
Figura 6-111: cambios en virtual host	89
Figura 6-112: para levantar más de un dominio	89
Figura 6-113: creación de carpeta sitio	90
Figura 6-114: permisos a index	90
Figura 6-115: reinicio de servicio httpd	90
Figura 6-116: ingreso al setup	91
Figura 6-117: ingreso al servicio de sistema	91
Figura 6-118: selección de servicio httpd	92
Figura 6-119 ingreso a opciones de conexión	93
Figura 6-120: ingreso a LAN settings	93
Figura 6-121: detección automática	94
Figura 6-122: navegación de página	94
Figura 6-123: esquema de servidor Proxy	96
Figura 6-124: verificación de paquete squid	97
Figura 6-125: editar paquete de squid	97
Figura 6-126: línea del puerto 8080	97
Figura 6-127: Línea de cache_mem	98
Figura 6-128: configuración de cache_dir	98
Figura 6-129: configuración cache_access_log	99

Figura 6-130: localhost.....	99
Figura 6-131: acceso al puerto 8080.....	99
Figura 6-132: servicio restaurado	100
Figura 6-133: creación de acl.....	100
Figura 6-134: acl de nombre puerto	101
Figura 6-135: restauramos squid.....	101
Figura 6-136: ingreso al setup	102
Figura 6-137: ingreso al servicio de sistema.....	102
Figura 6-138: elección de servicio squid.....	102
Figura 6-139: creación de archivos claves	103
Figura 6-140: permisos de archivo claves	103
Figura 6-141: cambio de propietario.....	104
Figura 6-142: ingreso de clave para autenticar.....	104
Figura 6-143: acl de autenticar	105
Figura 6-144: ruta auth_param.....	105
Figura 6-145: cambios en ruta auth_param	105
Figura 6-146: acl activada.....	106
Figura 6-147: acceso para autenticación.....	106
Figura 6-148: acl de páginas prohibidas.....	107
Figura 6-149: ingreso al archivo para denegar páginas.....	107
Figura 6-150: ingreso de páginas a denegar acceso	107
Figura 6-151: editar squid.....	108
Figura 6-152: acl de páginas prohibidas.....	108
Figura 6-153: accesos denegados para páginas	108
Figura 6-154: servicio squid restaurado	109
Figura 6-155: acl de tiempo.....	109
Figura 6-156: acceso por tiempo	109
Figura 6-157: restaurar esquid.....	110
Figura 6-158: opciones de internet	111
Figura 6-159: ingreso lan settings	111
Figura 6-160: detección de puerto proxy	112
Figura 6-161: ingreso de usuario con permisos	113
Figura 6-162: página cargada	113
Figura 6-163: acceso denegado	114
Figura 6-164: acceso negado por tiempo.....	115
Figura 6-165: verificación de paquete sendmail.....	119
Figura 6-166: verificación de paquete dovecot	119
Figura 6-167: ingreso a DOVECOT	119
Figura 6-168: protocolo agragado	120
Figura 6-169: editamos sendmail.....	120
Figura 6-170: cambios en loopback.....	120
Figura 6-171: Ingreso de dominio	121
Figura 6-172: configuración de network.....	121
Figura 6-173: ingreso de dominio.....	121
Figura 6-174: ingreso a vi hosts	122
Figura 6-175: direccionamiento de dominio.....	122
Figura 6-176: reinicio de sednmail	122
Figura 6-177: ingreso del setup	123

Figura 6-178: ingreso al servicio de sistema.....	123
Figura 6-179: elección de paquete sendmail	123
Figura 6-180: lectura de mail	124
Figura 6-181: ingreso al outlook Express	125
Figura 6-182: ingreso a cuentas	125
Figura 6-183: agregar cuenta.....	126
Figura 6-184: nombre de cuenta	126
Figura 6-185: nombre de usuario con dominio	127
Figura 6-186: ingreso de protocolo y ip del servidor.....	127
Figura 6-187: ingreso de cuenta y clave nueva	128
Figura 6-188: finalización de cuenta	128
Figura 6-189: vista de conexión con el servidor.....	129
Figura 6-190: vista de llegada de correo	129
Figura 6-191: ingreso al mail que llego desde Linux	130
Figura 6-192: esquema de firewall	131
Figura 6-193: ingreso al setup	141
Figura 6-194: configuración de firewall	141
Figura 6-195: configuración de cortafuego	141
Figura 6-196: regla creada.....	142
Figura 6-197: visualización de regla creada.....	143
Figura 6-198: editamos el firewall	144
Figura 6-199: creación de regla	144
Figura 6-200: permisos a firewall	144
Figura 6-201: vi rc.local.....	145
Figura 6-202: configuración de rc.local.....	145
Figura 6-203: ingreso a xinetd	145
Figura 6-204: habilitamos telnet.....	146
Figura 6-205: configuración de telnet.....	146
Figura 6-206: servicio restaurado	147
Figura 6-207: conexión vía telnet	147
Figura 6-208: ingreso al servidor por telnet.....	148
Figura 6-209: bloqueo de telnet	149
Figura 6-210: prueba de ping.....	149
Figura 6-211: bloqueo de ping.....	150
Figura 6-212: ejecutar con ip del servidor	152
Figura 6-213: ingreso al servidor de linux en windows.....	152
Figura 6-214: vista de reglas creadas en Linux.....	153
Figura 6-215: Bloqueo de Telnet en Windows.....	153
Figura 6-216: ping desde dirección permitida	154
Figura 6-217: bloqueo de ping.....	154
Figura 6-218: Esquema de DHCP	155
Figura 6-219: verificación de paquete dhcp.....	158
Figura 6-220: creación de archivo dhcp	158
Figura 6-221: editamos el dhcp	159
Figura 6-222: configuración de dhcp	160
Figura 6-223: restaurar dhcp.....	160
Figura 6-224: propiedades a conexión.....	161
Figura 6-225: propiedades de área local	161

Figura 6-226: propiedades de tcp/ip	162
Figura 6-227: detección automática	162
Figura 6-228: ingreso de consola	163
Figura 6-229: verificación dhcp	163

CAPÍTULO 7

Figura 7-1: Conexiones varios segmentos de red	1
Figura 7-2: DCE - DTE	2
Figura 7-3: Componentes del router	3
Figura 7-4: Conexiones Externas del Router	6
Figura 7-5: Conexiones Hyperterminal	9
Figura 7-6: Cable rollover	9
Figura 7-7: Inicio Hyperterminal	10
Figura 7-8: Nombre a la Conexión	11
Figura 7-9: Puerto de conexión	11
Figura 7-10: Configuración de los bits	12
Figura 7-11: Pantalla de inicio del HYPERTERMINAL	13
Figura 7-12: Gráfico de los modos	14
Figura 7-13: show Versión	15
Figura 7-14: Show interfaces	16
Figura 7-15: Show Protocols	17
Figura 7-16: Show Clock	17
Figura 7-17: Show History	17
Figura 7-18: Show ip Router	18
Figura 7-19: show vlan	18
Figura 7-20: show access listis	19
Figura 7-21: Show terminal	19
Figura 7-22: Show running-config	20
Figura 7-23: Show Flash	21
Figura 7-24: Gráfico enrutamiento	22
Figura 7-25: Cabecera OSPF Figura 7-26: Paquetes Hello de OSPF	32
Figura 7-27: Paquete DD de OSPF	34
Figura 7-28: (tipo 1) RLA ("Router Links Advertisement") de OSPF	35
Figura 7-29:(Tipo 2) NLA ("Network Links Advertisement") de OSPF	35
Figura 7-30:(Tipo 3 y 4) SLA ("Summary Links Advertisement") de OSPF	36
Figura 7-31:(Tipo 5) ELA ("External Links Advertisement") de OSPF	36
Figura 7-32: Gráfico flujo grama de una aceptación de ACL	39
Figura 7-33: Función de ACL	40
Figura 7-34: Gráfico dispositivos Switch	44
Figura 7-35: Dominios de broadcasts	46
Figura 7-36: Gráfico comunicación entre Vlans	50
Figura 7-37: Gráfico segmentación tradicional	51
Figura 7-38: Gráfico segmentación con vlans	51
Figura 7-39: Gráfico vlan entre switches: filtrado	53
Figura 7-40: Gráfico vlan entre switches: etiquetado	54
Figura 7-41: Implementación protocolos Enrutamiento	56
Figura 7-42: Implementación protocolos Enrutamiento Lógico	57

Figura 7-43: Configuración de la tarjeta de red Dpto Cajas.....	109
Figura 7-44: Configuración de la tarjeta de red Dpto gerencia	109
Figura 7-45: Configuración de la tarjeta de red Dpto Sistema	110
Figura 7-46: Configuración de la tarjeta de red Dpto jefe Caja.....	110
Figura 7-47: Configuración de la tarjeta de red Dpto Contabilidad.....	111
Figura 7-48: prueba de comunicación entre vlan 1.1	112
Figura 7-49: prueba de comunicación entre vlan 1.2	112
Figura 7-50: prueba de comunicación entre vlan 1.3	113
Figura 7-51: prueba de comunicación entre vlan 1.4.....	113
Figura 7-52: Configuración de la tarjeta de red Dpto Caja 2	119
Figura 7-53: Configuración de la tarjeta de red Dpto Cómputo	119
Figura 7-54: Configuración de la tarjeta de red Dpto Jefe Caja 2.....	120
Figura 7-55: Configuración de la tarjeta de red Dpto Gerencia 2.....	120
Figura 7-56: prueba de comunicación entre vlan 2.1	121
Figura 7-57: prueba de comunicación entre vlan 2.2	121
Figura 7-58: prueba de comunicación entre vlan 2.3	122
Figura 7-59: prueba de comunicación entre vlan 2.4	122
Figura 7-60: Configuración de la tarjeta de red Dpto RRHH.....	130
Figura 7-61: Configuración de la tarjeta de red Dpto S. Administrativo	130
Figura 7-62: Configuración de la tarjeta de red Dpto Calidad	131
Figura 7-63: Configuración de la tarjeta de red Dpto Operación	131
Figura 7-64: Configuración de la tarjeta de red Dpto Comercialización	132
Figura 7-65: prueba de comunicación entre vlan 3.1	133
Figura 7-66: prueba de comunicación entre vlan 3.2	133
Figura 7-67: prueba de comunicación entre vlan 3.3	134
Figura 7-68: prueba de comunicación entre vlan 3.4	134
Figura 7-69: prueba de comunicación entre vlan 3.5	135
Figura 7-70: Configuración de la tarjeta de red Dpto Auditoría.....	141
Figura 7-71: Configuración de la tarjeta de red Dpto Desarrollo	141
Figura 7-72: Configuración de la tarjeta de red Dpto Gerencia.....	142
Figura 7-73: Configuración de la tarjeta de red Dpto Recepción	142
Figura 7-74: prueba de comunicación entre vlan 4.1	143
Figura 7-75: prueba de comunicación entre vlan 4.2	143
Figura 7-76: prueba de comunicación entre vlan 4.3	144
Figura 7-77: prueba de comunicación entre vlan 4.4	144
Figura 7-78: prueba de comunicación entre vlan 5.1	145
Figura 7-79: prueba de comunicación entre vlan 5.1	146
Figura 7-80: prueba de comunicación entre vlan 5.2	147
Figura 7-81: prueba de comunicación entre vlan 5.3	148
Figura 7-82: prueba de comunicación entre vlan 5.4	149
Figura 7-83: prueba de comunicación entre vlan 5.5	150



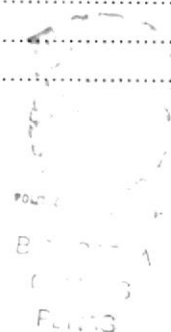
INDICE DE TABLAS

CAPÍTULO 2

Tabla 2-1: Características De Las Estaciones De Trabajo Matriz.....	13
Tabla 2-2: Características De Las Estaciones De Trabajo Portete.....	14
Tabla 2-3: Características De Las Estaciones De Trabajo Urdesa.....	14
Tabla 2-4: Características De Servidores Matriz.....	15
Tabla 2-5: Características De Las Estaciones De Trabajo Matriz.....	16
Tabla 2-6: Características De Servidores De Portete.....	17
Tabla 2-7: Características De Servidores Urdesa.....	17
Tabla 2-8: Dispositivos Conmutación Switch Matriz.....	18
Tabla 2-9: Dispositivos Conmutación moden Matriz.....	18
Tabla 2-10: Dispositivos Conmutación Hub Portete.....	19
Tabla 2-11: Dispositivos Conmutación Moden Portete.....	19
Tabla 2-12: Dispositivos Conmutación Switch Urdesa.....	20
Tabla 2-13: Dispositivos Conmutación Moden Urdesa.....	20
Tabla 2-14: Infraestructura lan Matriz.....	24
Tabla 2-15: Infratesrucura Lan Sucursales.....	24
Tabla 2-16: Tabla enrutamiento Matriz.....	31
Tabla 2-17: Tabla Enrutamiento Portete.....	32
Tabla 2-18: Tabla enrutamiento Urdesa.....	32

CAPÍTULO 3

Tabla 3-1: Problemas.....	1
Tabla 3-2: Solución.....	2
Tabla 3-3: Factibilidad Técnica "A" Equipos Propios.....	3
Tabla 3-4: Factibilidad Técnica de Alquiler "A" Dispostivos Alquiler.....	4
Tabla 3-5: Factibilidad Economica "A"Costos Equipos.....	5
Tabla 3-6: Factibilidad Economica "A"Costos Alquiler Dispositivos.....	5
Tabla 3-7: Factibilidad Economica "A" Costo de Enlace.....	6
Tabla 3-8: Factibilidad Economica "A" Costo Aumento Ancho de Banda.....	6
Tabla 3-9: Factibilidad Economica "A" Costo Operativo.....	7
Tabla 3-10: Factibilidad Operativa "A".....	8
Tabla 3-11: Costo Total Factibilidad "A".....	9
Tabla 3-12: Factibilidad Técnica "B".....	13
Tabla 3-13: Factibilidad técnica "B".....	14
Tabla 3-14: Factibilidad Economica "B" Costo de Equipos.....	15
Tabla 3-15: Factibilidad Economica "B" Costo Enlace con el ISP.....	15
Tabla 3-16: Factibilidad Economica "B" Costo Aumento Ancho de banda.....	16
Tabla 3-17: Factibilidad Operativa "B" Costo Operativos.....	17
Tabla 3-18: Factibilidad Operativa "B".....	18
Tabla 3-19: Costo Total Factibilidad "B".....	19



CAPÍTULO 4

Tabla 4-1: Implementación Antena microonda "Portete"	1
Tabla 4-2: Implementación Antena Miroonda "Matriz"	2
Tabla 4-3: Enlace de Conexión.....	3
Tabla 4-4: Enlace Portete-Matriz.....	4
Tabla 4-5: Implementación MC Matriz	5
Tabla 4-6 Implementación MC Portete	6
Tabla 4-7: Implementación Ancho de Banda.....	7
Tabla 4-8: Implementación Vlan Matriz.....	8
Tabla 4-9: Implementación Vlan Urdesa	8
Tabla 4-10: Implementación Vlan Portete.....	9

CAPÍTULO 5

Tabla 5-1: Identificador de Cable 1	28
Tabla 5-2: Identificador de cable 2	28
Tabla 5-3: Recomendación Fibra Optica.....	33

CAPÍTULO 6

Tabla 6-1: Requerimiento de hardware	4
Tabla 6-2: Directorios	43
Tabla 6-3: Lista contenido de directorio	44
Tabla 6-4: Lista Archivos especiales.....	44
Tabla 6-5: Raíz del árbol	67

CAPÍTULO 7

Tabla 7-1: Ventajas y desventajas del Router	7
Tabla 7-2: Modos de un Router	14
Tabla 7-3: Comandos UP-Down	17
Tabla 7-4: Versiones de RIP	25
Tabla 7-5: Tipos de Swicht	45
Tabla7-6 significado 1 de C - R	90
Tabla 7-7: significado 2 de C – R O.....	91
Tabla 7-8: significado 3 de C – R OE2	92
Tabla 7-9: significado 4 de C – R-O	93
Tabla 7-10: significado 5 de C - R.....	94
Tabla 7-11: significado 6 de C - R	95





CAPÍTULO 1

GENERALIDADES

1. GENERALIDADES

1.1 INTRODUCCIÓN

En la actualidad, las empresas de toda índole se ven en la necesidad de mantener una comunicación interactiva entre las diferentes entidades que la conforman.

Además de comunicarse con otras empresas que se encuentran en sociedad; hay que observar que no deben sacrificar por ello la integridad, la operatividad y los costos para lograrlo.

Por tal motivo la seguridad de las redes es de suma importancia, es por eso que se habla de dispositivos en software y hardware que las protegen.

Es así que el concepto de comunicación se hace vital, y mas aun la seguridad que se le agregue al hecho de tener la información correcta, en el lugar y manos adecuadas.

1.2 OBJETIVO DE ESTE MANUAL

El objetivo general del Manual es, identificar los riesgos del estado actual y de las seguridades tecnológicas de redes que posee la empresa, proveer de una solución en tecnología de redes que ayude al desarrollo normal de la operación del mismo de forma ágil y eficiente basándose en la seguridad, confidencialidad, integridad y disponibilidad a fin de evitar futuros ataques.

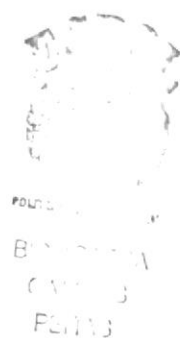
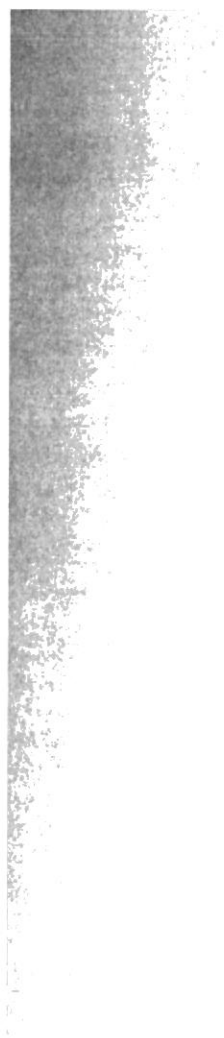
Mejorar su servicio actual, ganar prestigio para que la empresa sea aceptada y brinde confianza dentro del mercado de las cooperativas de pago, y que como consecuencia pueda ampliar su cartera de clientes.

Minimizar el impacto de posibles ataques a la red de forma que la normal funcionalidad de la empresa no se vea afectada.

1.3 A QUIEN VA DIRIGIDO

Este manual va dirigido al personal del departamento de sistemas que deseen ver como se realizaron las implementaciones tanto como en el servidor y en las configuraciones a nivel de dispositivos.





CAPÍTULO 2

SITUACIÓN ACTUAL

2. SITUACIÓN ACTUAL

2.1 ANTECEDENTES DE LA EMPRESA

Gracias a la iniciativa de Ejecutivos de PRODUBANCO y el entonces BANCO POPULAR un 27 de Abril de 1998, se conformó la empresa, SERVIPAGOS.

A finales de abril de 1998, arrancó con la agencia Colón y Santo Domingo en Quito, Escobedo y Alborada en Guayaquil, desde esa fecha, con la colaboración de todos, han crecido, logrando un posicionamiento en el mercado como una empresa diferente, que ofrece muchos valores agregados a los clientes como los horarios de atención, nuestra rapidez y actitud en el servicio.

Han logrado crecer en medio de la crisis de los años 1999 y 2000, con mucho esfuerzo, esto lo ha fortalecido, y ha unido como grupo de trabajo, lo duro del camino que ha preparado para enfrentar un futuro que lo ven con mucho optimismo.

La empresa SERVIPAGOS cuenta con 48 sucursales a nivel nacional Y una matriz en Guayaquil situado en las calles: Pasaje Los Ángeles E3-19 y avenida Eloy Alfaro.

2.2 MISIÓN DE LA EMPRESA

Proveer soluciones de cobros y pagos, de gran cobertura, a través de agencias, teléfono, Internet y demás canales de distribución, agrupando clientes para disminuir sus costos; brindando a los consumidores un servicio rápido y accesible, calidad de vida en el trabajo a los colaboradores y rentabilidad a los accionistas; en un marco de colaboración con la sociedad.

2.3 VISIÓN DE LA EMPRESA

Ser el mejor y más grande canal de distribución de servicios y soluciones de cobros y pagos del Ecuador con proyección internacional



2.4 INFRAESTRUCTURA LAN DE LA EMPRESA

La empresa SERVIPAGOS cuenta con 48 sucursales, por lo tanto el caso estudio está reflejado en tres edificios importantes de la ciudad de Guayaquil y a su vez cuenta con varios problemas, por eso se ha tomado en consideración los siguientes edificios como: matriz y sucursales.

2.5 MATRIZ DE GUAYAQUIL

El edificio matriz cuenta con una sola planta en el tercer piso de un edificio situado en las calles: Pasaje Los Ángeles E3-19 y avenida Eloy Alfaro, en la matriz cuenta con 10 departamentos, continuación se detallará los departamentos que existen en la matriz:

- Recursos Humanos
- Servicio al Cliente
- Calidad
- Servicios Administrativos
- Operaciones
- Comercialización
- Auditoría
- Producción & Desarrollo (Sistema)
- Gerencia
- Recepción

2.6 AGENCIA PORTETE

La Agencia Portete de Guayaquil, es una sucursal que se encuentra en un solo piso en la planta baja y los demás piso están conformados por departamentos familiares la agencia Portete está conformada por los siguientes departamentos:

- Caja
- Gerencia
- Sistema
- Jefe de caja
- Contabilidad

2.7 AGENCIA URDESA

La Agencia Urdesa de Guayaquil, también está considerada como una de las sucursales principales de la empresa SERVIPAGOS, es una agencia que conforma en una villa solamente y sus departamentos que conforman en dicha agencia son los siguientes:

- Caja
- Jefe de Caja
- Gerencia
- Computo
- Bodega



2.8 ESTRUCTURA DE LOS EDIFICIOS

Una vez detallados los departamentos que conforman en cada edificio, matriz y agencias, se procede a detallar como es la infraestructura de los edificios ya mencionados.

2.8.1. MATRIZ (TERCER PISO)

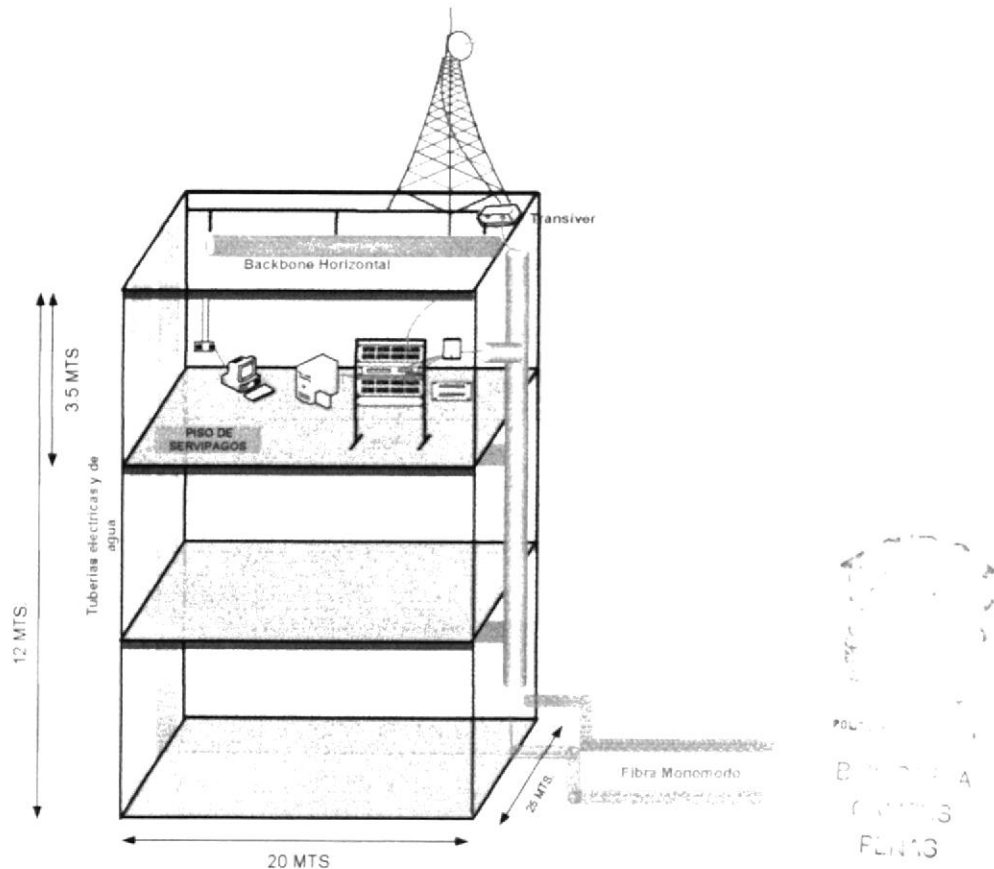


Figura 2-1: edificio Matriz

LEYENDAS		
		Tubería de agua
		Tubería eléctrico
		Backbone Vertical
		Backbone Horizontal
		TRANSIVER
		modem
		Antena
		COBRE
		Fibra Monomodo
		Plato de Fibra
		Rack
		Punto de red

2.8.2. PORTETE (PLANTA BAJA)

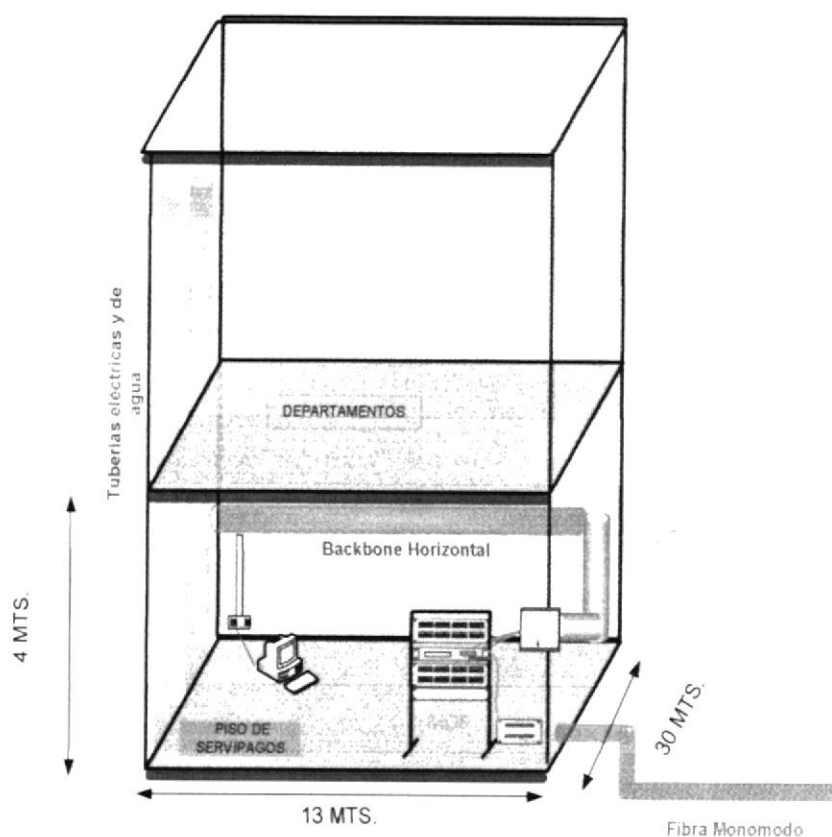


Figura 2-2: Edificio Portete

LEYENDAS		
		Tubería de agua
		Tubería eléctrico
		Backbone Vertical
		Backbone Horizontal
		Fibra Monomodo
2 U		Plato de Fibra
2 U		Rack
2 U		Punto de red



2.8.3. EDIFICIO URDESA

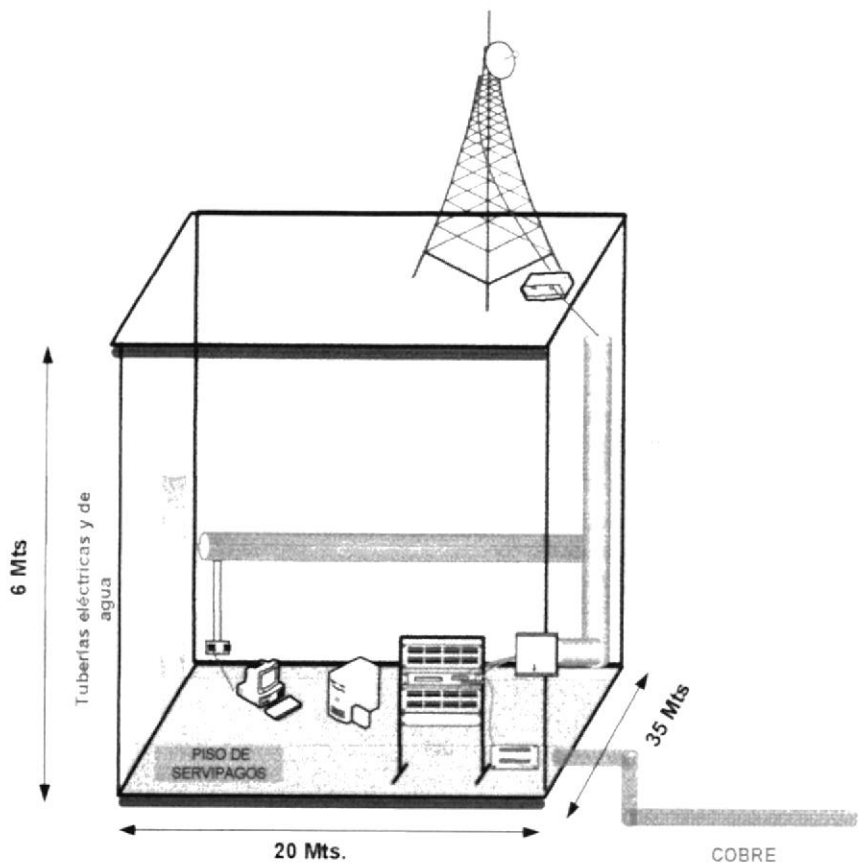


Figura 2-3: edificio Urdesa

Leyenda		
Subtítulo de leyenda		
Símbolo	Total	Descripción
	1	PC
	2	Panel de conexiones
	1	Ethernet
	1	Puerta
	2	Bandeja de cables/espaciador
	1	Torre de transmisión
	1	Servidor
	1	Servidor proxy



2.9 ANÁLISIS DE PISO LÓGICO

2.9.1. MATRIZ (GUAYAQUIL)

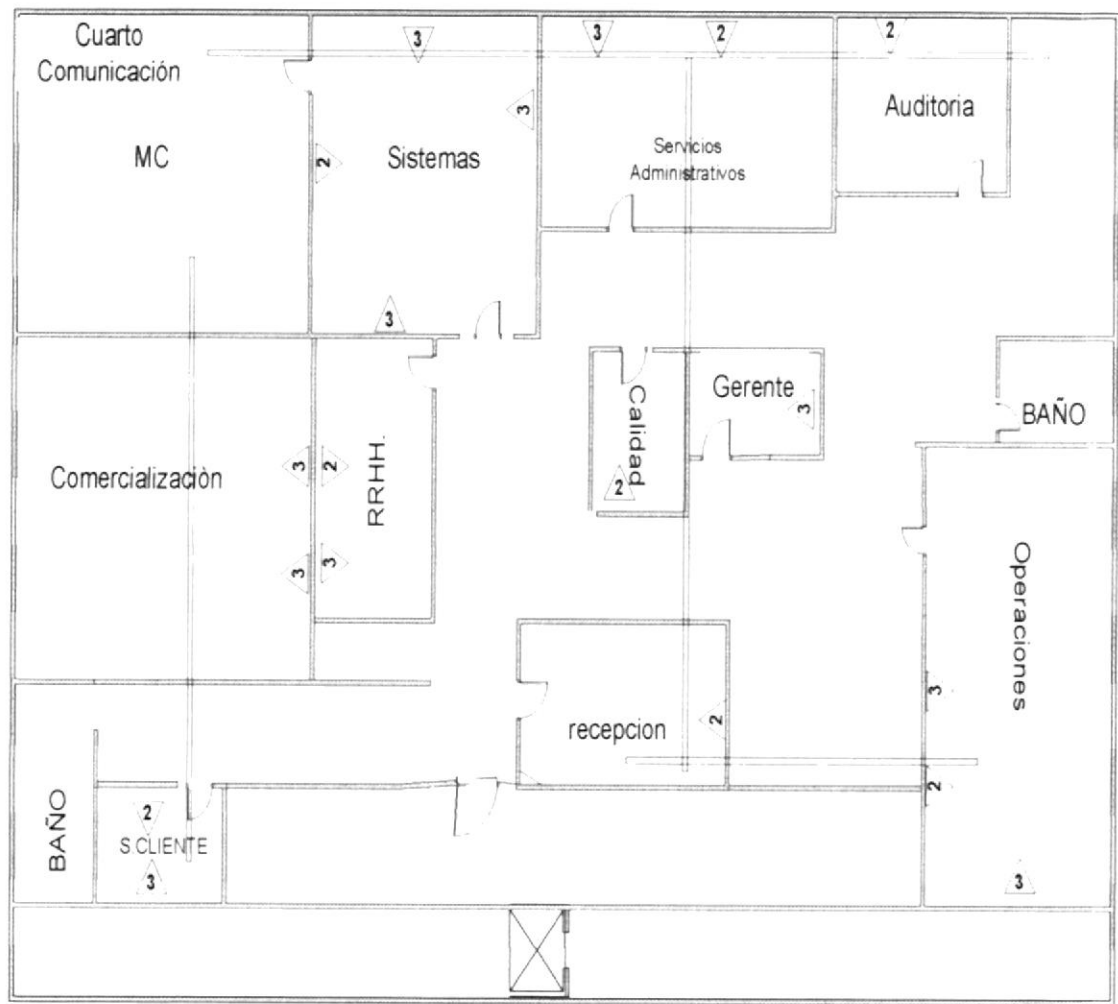


Figura 2-4: piso Lógico Matriz

Edificio Matriz		
Subtítulo de leyenda		
Símbolo	Total	Descripción
	11	2 Puntos de Datos y 1 de Voz
	1	Ascensor
	8	1 Punto de datos y 1 punto de voz



2.9.2. AGENCIA (PORTETE)

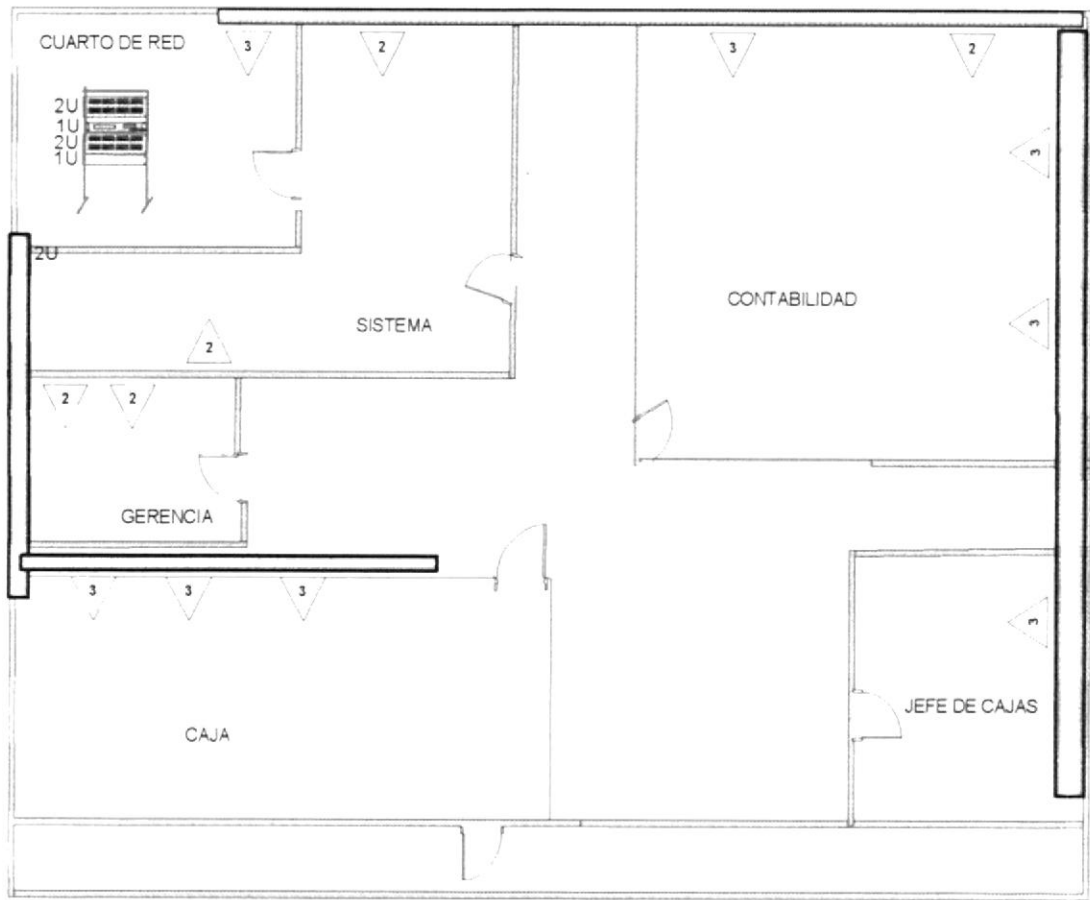


Figura 2-5: piso Lógico Portete

Edificio Portete		
Subtítulo de leyenda		
Símbolo	Total	Descripción
	6	2 Puntos de Datos y 1 de Voz
	5	1 Punto de datos y 1 punto de voz



2.9.3. AGENCIA (URDESA)

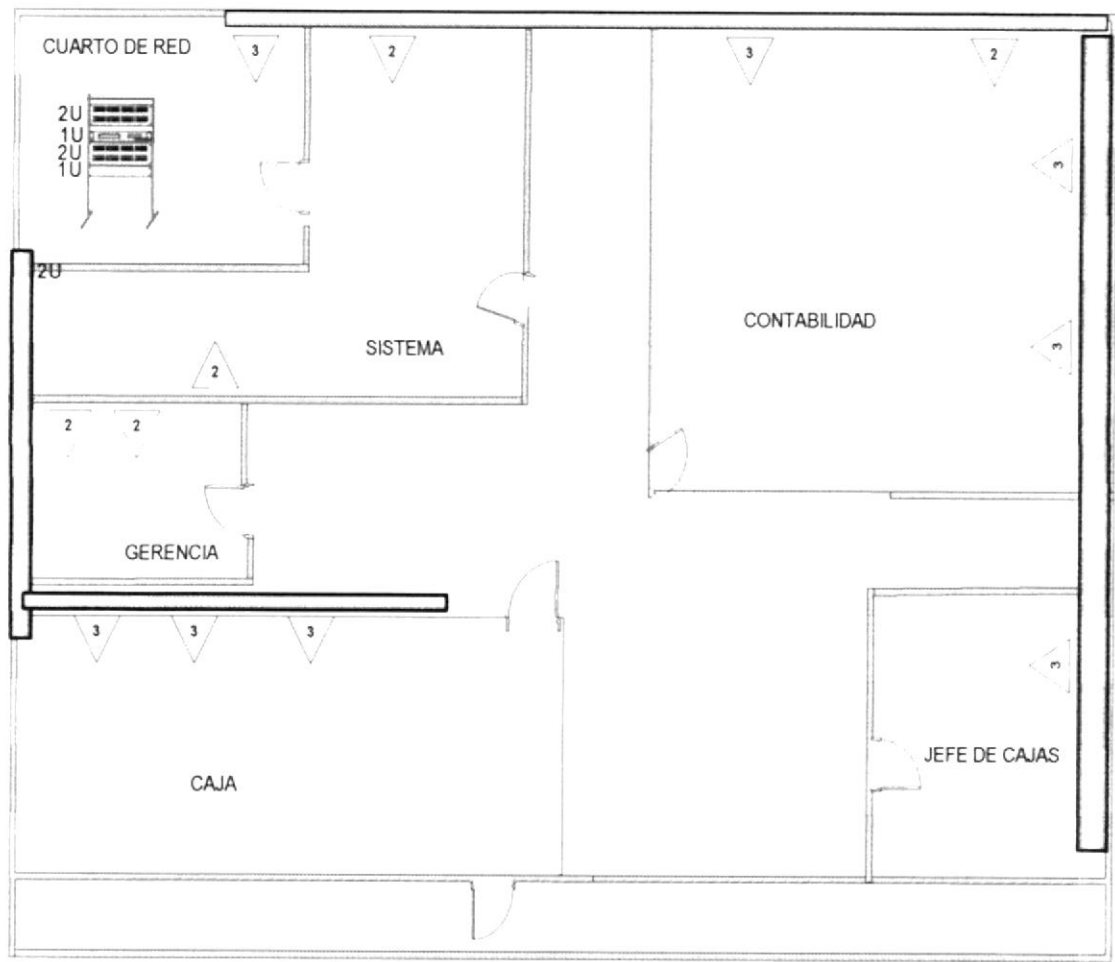


Figura 2-6: piso Lógico Urdesa

Edificio Portete		
Subtítulo de leyenda		
Símbolo	Total	Descripción
3	3	2 Puntos de Datos y 1 de Voz
2	8	1 Punto de datos y 1 punto de voz



2.10 ANÁLISIS PISO APLICATIVO

2.10.1. MATRIZ (GUAYAQUIL)

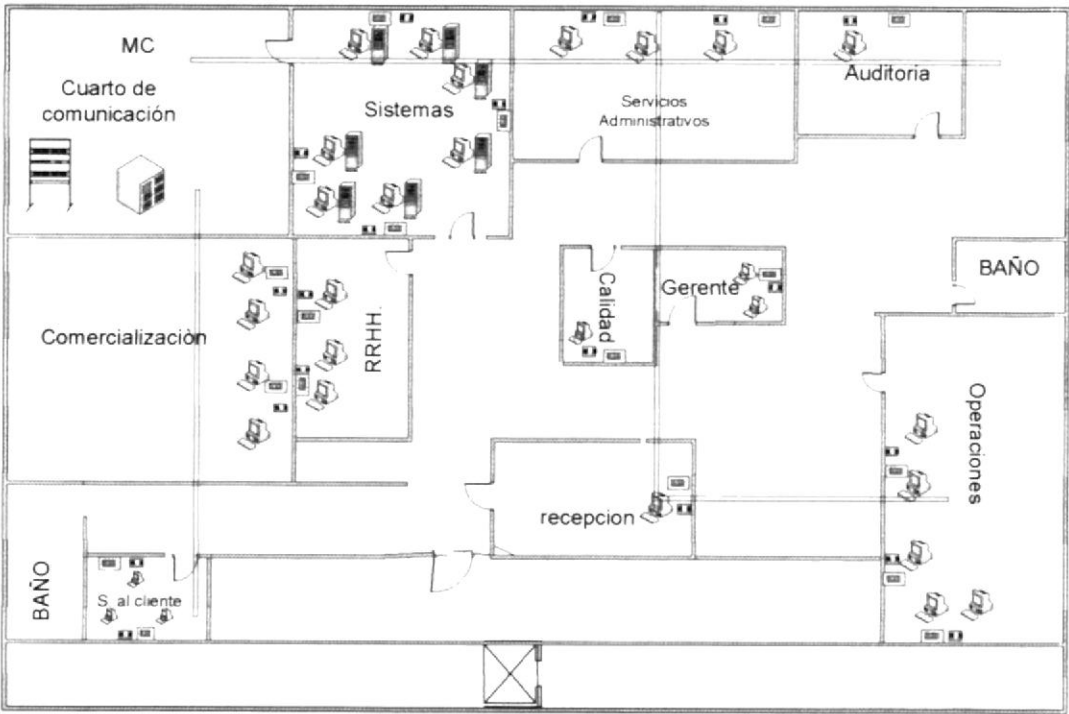


Figura 2-7: piso aplicativo Matriz

MATRIZ		
DISPOSITIVOS DE LA MATRIZ		
Símbolo	Total	Descripción
	28	PC.18
	2	Panel de conexiones
	1	Central de conmutación
	1	Bandeja de cables/espaciador
	1	RACK
	28	Face plate
		canaleta
	7	Servidores
		Puntos Electricos

POC
B
C
F

2.10.2. AGENCIA (PORTETE)

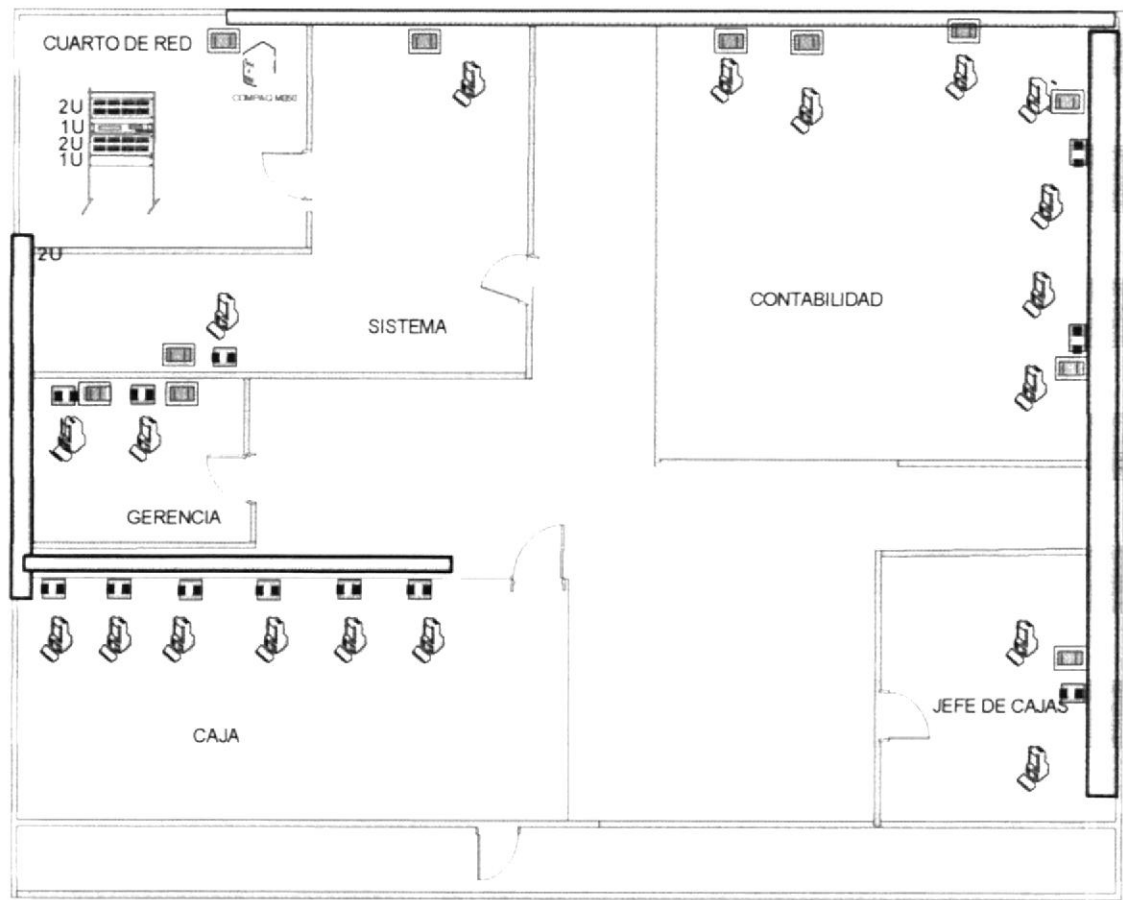


Figura 2-8: piso aplicativo Portete

Leyenda		
Subtítulo de leyenda		
Símbolo	Total	Descripción
	12	PC
	2	Panel de conexiones
	1	Bandeja de cables/ espaciador
	1	Servidor
	12	Face Plate
	3	Canaletas
	15	Punto Electrico

POU
B
C
FLV13

2.10.3. AGENCIA (URDESA)

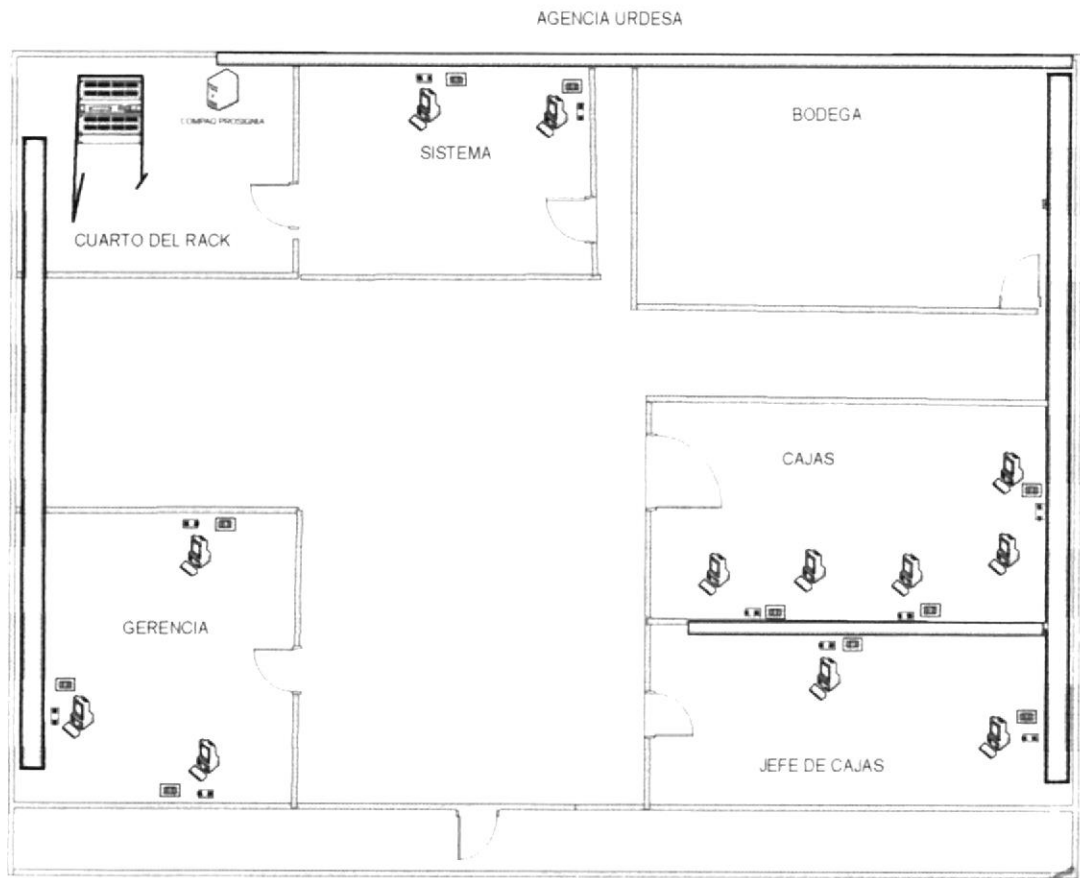


Figura 2-9: piso aplicativo Urdesa

Leyenda		
Subtítulo de leyenda		
Símbolo	Total	Descripción
	12	PC
	2	Panel de conexiones
	1	Bandeja de cables/espaciador
	1	Servidor
	12	Jack
	3	Canaletas
	11	Punto Eléctrico

2.11 CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO

2.11.1. MATRIZ – GUAYAQUIL

DPTO.	CANTIDAD	CARACTERÍSTICAS
- Recursos Humanos - Servicios Administrativos - Operaciones	3 3 5	computadora Pentium 4 marca Compaq Procesador 2.6 Mhz disco duro 40 GB Memoria ram 512 DDR T.Red 100/100 Mbps S.O Windows XP
- Servicio al Cliente - Calidad	3 3	computadora Pentium 4 marca Compaq Procesador 2.6 Mhz disco duro 40GB memoria ram 256 (DDR) T.Red 100/100 bps S.O Windows XP
- Comercialización - Auditoría - Gerencia - Recepción	4 3 2 3	computadora Pentium 4 marca Compaq Procesador 2.6 Mhz Memoria 256 (DDR) disco duro 80 GB T.Red 100/100 Mbps S.O Windows XP

Tabla 2-1: Características De Las Estaciones De Trabajo Matriz

2.11.2. AGENCIA PORTETE

DPTO	CANTIDAD	CARACTERÍSTICAS
- Caja - Gerencia - Sistema - Jefe de Caja - Contabilidad	6 2 2 2 7	Computadora Pentium 4 marca Compaq modelo LK428 Procesador 2.6 Mhz disco duro 40GB memoria ram 256 (DDR) T.Red 100/100 Mbps

Tabla 2-2: Características De Las Estaciones De Trabajo Portete

2.11.3. AGENCIA URDESA

DPTO	CANTIDAD	CARACTERÍSTICAS
- Caja - Gerencia - Jefe de caja - Sistema	5 3 2 2	computadora Pentium 4 marca Compaq modelo KS230 Procesador 2.6 Mhz disco duro 40GB memoria ram 256 (DDR) T.Red 100/100 Mbps ranura PCI

Tabla 2-3: Características De Las Estaciones De Trabajo Urdesa

2.12 CARACTERÍSTICAS DE LOS SERVIDORES

2.12.1. MATRIZ - GUAYAQUIL

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Producción &desarrollo (Sistema)	1	Servidor Proxy	marca Compaq disco duro 80 GB Procesador 3.0 Mhz memoria ram 1 GB (DDR) 2 T.Red 100/1000 Mbps Procesador Doble Núcleo S.O. linux red Hat
Producción &desarrollo (Sistema)	1	Servidor Proxy Backup	marca Compaq Procesador 3.2 Mhz Doble Núcleo disco duro 80 GB memoria ram 2 GB (DDR) T.Red 100/1000 Mbps S.O. linux red Hat Fuentes Redundantes
Producción &desarrollo (Sistema)	1	Servidor Webserver Dns	marca Compaq Procesador 3.0 Mhz Doble Núcleo disco duro 120 GB memoria ram 2 GB (DDR) T.Red 100/1000 Mbps S.O. linux red Hat Fuentes Redundantes

Tabla 2-4: Características De Servidores Matriz

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Producción & desarrollo (Sistema)	1	Servidor Bdc (Nt)	marca Compaq modelo (Prosignia) Procesador 533 Mhz disco duro 40 Gb memoria ram 128 Mb (DDR) T.Red 100/1000 Mbps S.O. Windows NT
Producción & desarrollo (Sistema)	1	Servidor Db	marca Compaq modelo (Prosignia) Procesador 533 Mhz disco duro 40 memoria ram 128 Mb (DDR) T.Red 100/1000 Mbps S.O. Windows NT
Producción & desarrollo (Sistema)	1	Servidor De Correo	marca Compaq modelo (DL-220 MT) Procesador 2.8Mhz de doble núcleo bus de 800 disco duro 60 Gb memoria ram 512 Mb (DDR) T.Red 100/1000 Mbps S.O. Red Hat
Producción & desarrollo (Sistema)	1	Servidor Firewall	CLON
Producción & desarrollo (Sistema)	1	(Backup) Servidor Firewall	Intel P4, 512 Mb disco duro 60 Gb S.O. Linux red Hat T.Red 100/1000 Mbps

Tabla 2-5: Características De Las Estaciones De Trabajo Matriz

2.12.2. AGENCIA PORTETE

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Sistema	1	Servidor Correo Electrónico	marca Compaq modelo (DL-220 MT) Procesador 3.0 Mhz disco duro 80 Gb memoria ram 512 Mb (DDR) T.Red 100/1000 Mbps S.O. Red Hat

Tabla 2-6: Características De Servidores De Portete**2.12.3. AGENCIA URDESA**

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Computo	1	Servidor Correo Electrónico	marca Compaq modelo (Prosignia) Procesador 2.8Mhz de doble núcleo bus de 800 disco duro 40 Gb memoria ram 256 Mb (DDR) T.Red 100/1000 Mbps S.O. Red Hat

Tabla 2-7: Características De Servidores Urdesa

POLICIA
 B. MOREA
 C. S. S.
 ELIAS

2.13 DISPOSITIVOS DE CONMUTACIÓN

2.13.1. MATRIZ – GUAYAQUIL

SWITCH

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Producción &desarrollo (Sistema)	2	Switch	3Com Baseline Switch modelo2024 Administrables Stackeables Puertos truncados Fuentes Redundantes Velocidad de 100MBPS 24 puertos Capa 2

Tabla 2-8: Dispositivos Conmutación Switch Matriz

MÓDEM

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Producción &desarrollo (Sistema)	2	Módem	Protocolo Soportado v.92 v.90 56Kbps Cable Telefónico Interfaz PCI Chipset: Motorola
Cómputo	2	Módem Externo	Marca: OVISLINK Fax/Módem 14.400 / 56.600 externo (V.90 Y 56KFLEX)..Carcasa Negra

Tabla 2-9: Dispositivos Conmutación moden Matriz



2.13.2. AGENCIA PORTETE

HUB

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Cómputo	1	Hub	24 Puertos Velocidad de 10 Mbps No Administrables

Tabla 2-10: Dispositivos Conmutación Hub Portete

MÓDEM

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Cómputo	2	Módem	Protocolo Soportado v.92 v.90 56Kbps Cable Telefónico Interfaz PCI Chipset: Motorola
Cómputo	2	Módem Externo	Marca: OVISLINK Fax/Módem 14.400 / 56.600 externo (V.90 Y 56KFLEX)..Carcasa Negra

Tabla 2-11: Dispositivos Conmutación Modem Portete

ROUTER
BIOLOGIA
CANTAS
FENIS

2.13.3. AGENCIA - URDESA

SWITCH

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Cómputo	1	SWITCH	3Com Baseline Switch modelo 2024 Administrables Stackeables Puertos truncados Fuentes Redundantes Velocidad de 100mbps 24 puertos Capa 2

Tabla 2-12: Dispositivos Conmutación Switch Urdesa

MÓDEM

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Cómputo	1	Módem	Protocolo Soportado v.92 v.90 56Kbps Cable Telefónico Interfaz PCI Chipset: Motorola
Cómputo	1	Módem Externo	Marca: OVISLINK Fax/Módem 14.400 / 56.600 externo (V.90 Y 56KFLEX)..Carcasa Negra

Tabla 2-13: Dispositivos Conmutación Modem Urdesa

2.14 GRÁFICO DEL MC

2.14.1. MATRIZ GUAYAQUIL

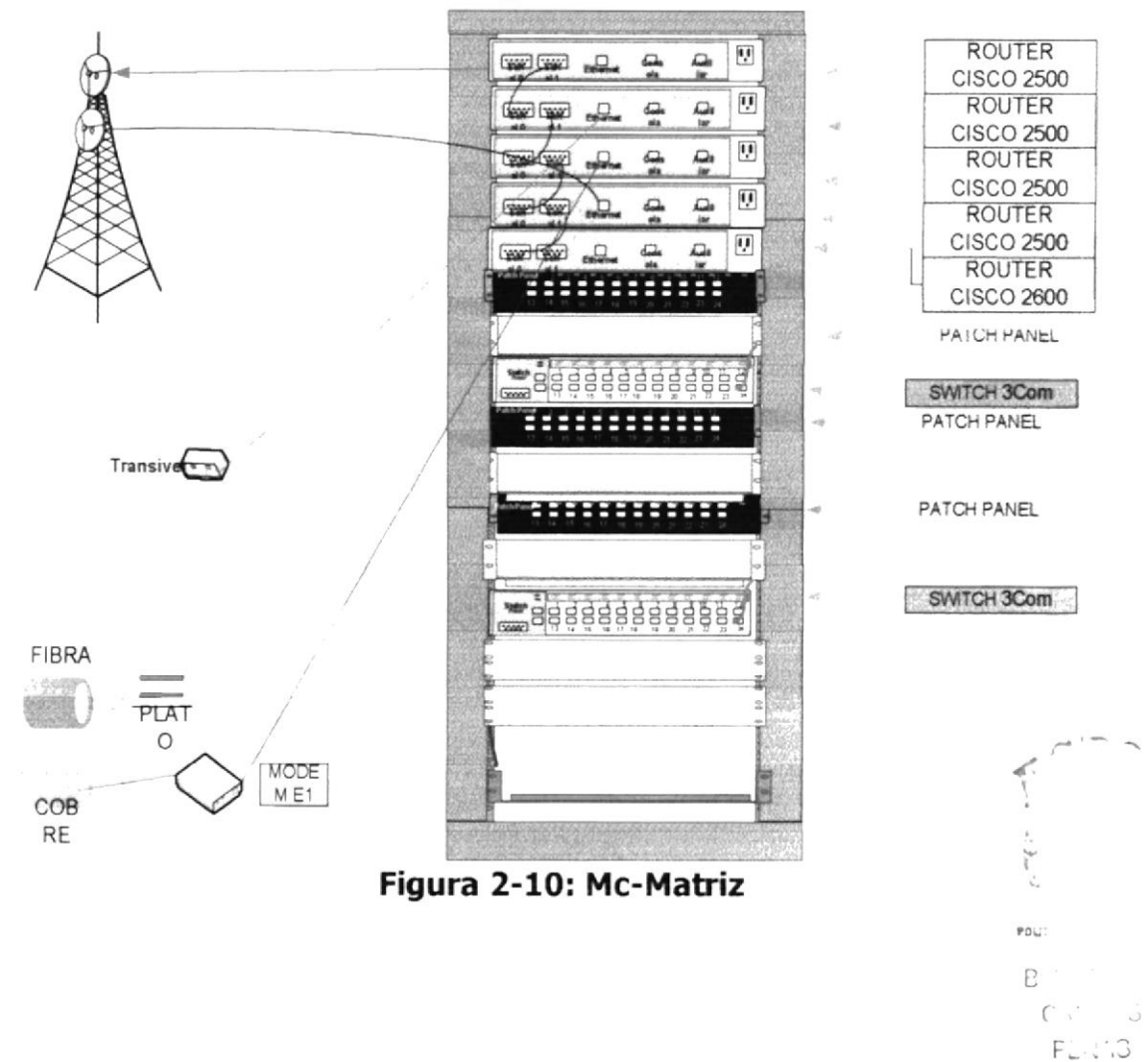
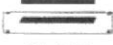
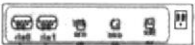


Figura 2-10: Mc-Matriz

LEYENDAS

 FIBRA	 PLATO	 ISP	 Routers	 switch
 COBRE	 MODEM E1	 Transiver	 Patch Panel	

2.14.2. AGENCIA PORTETE

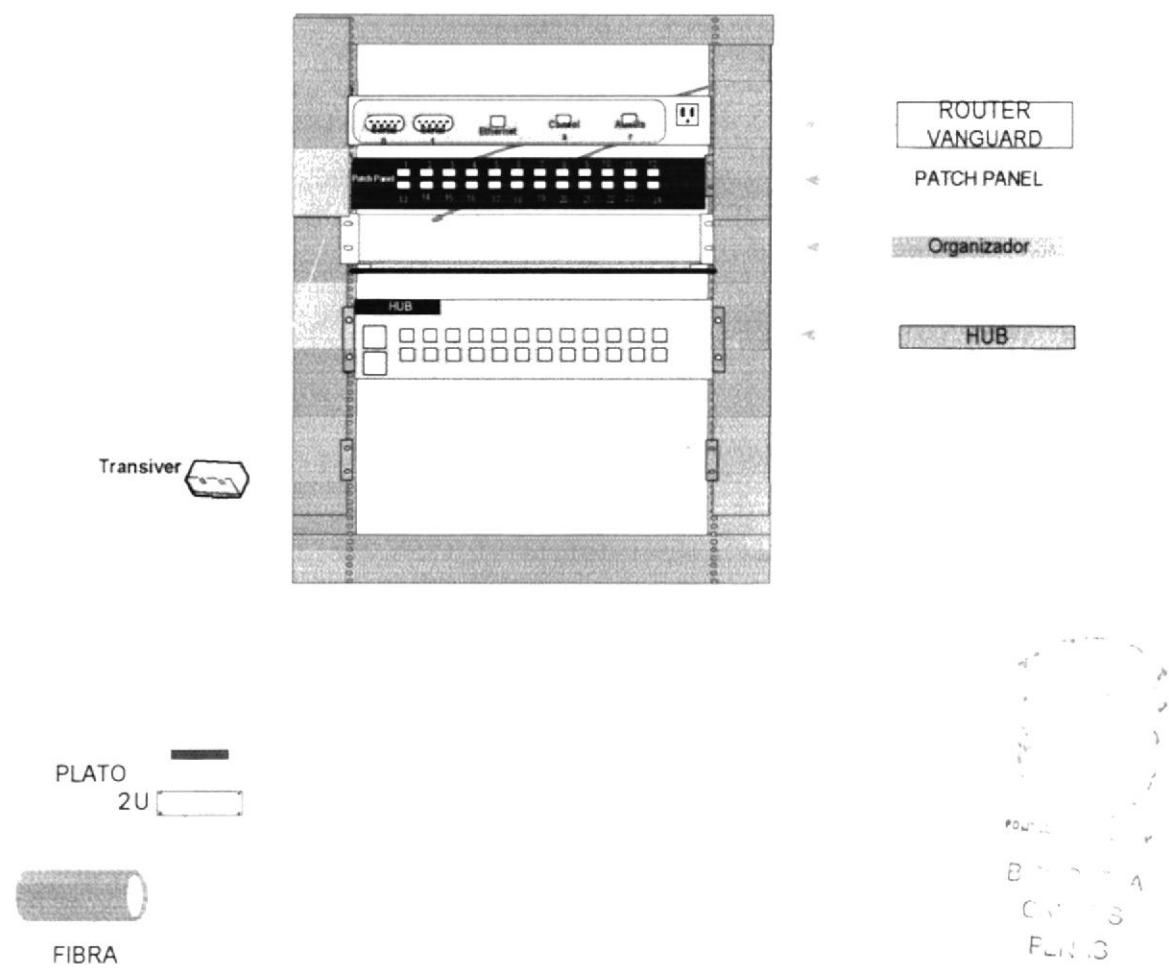
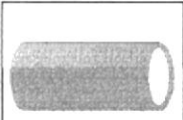
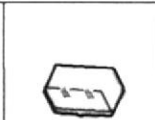
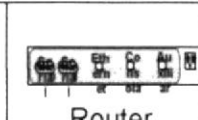
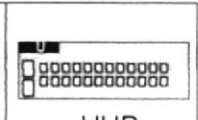


Figura 2-11: Mc-Portete

LEYENDAS

					
FIBRA	PLATO	Transiver	Router	Patch Panel	HUB

2.14.3. AGENCIA URDESA

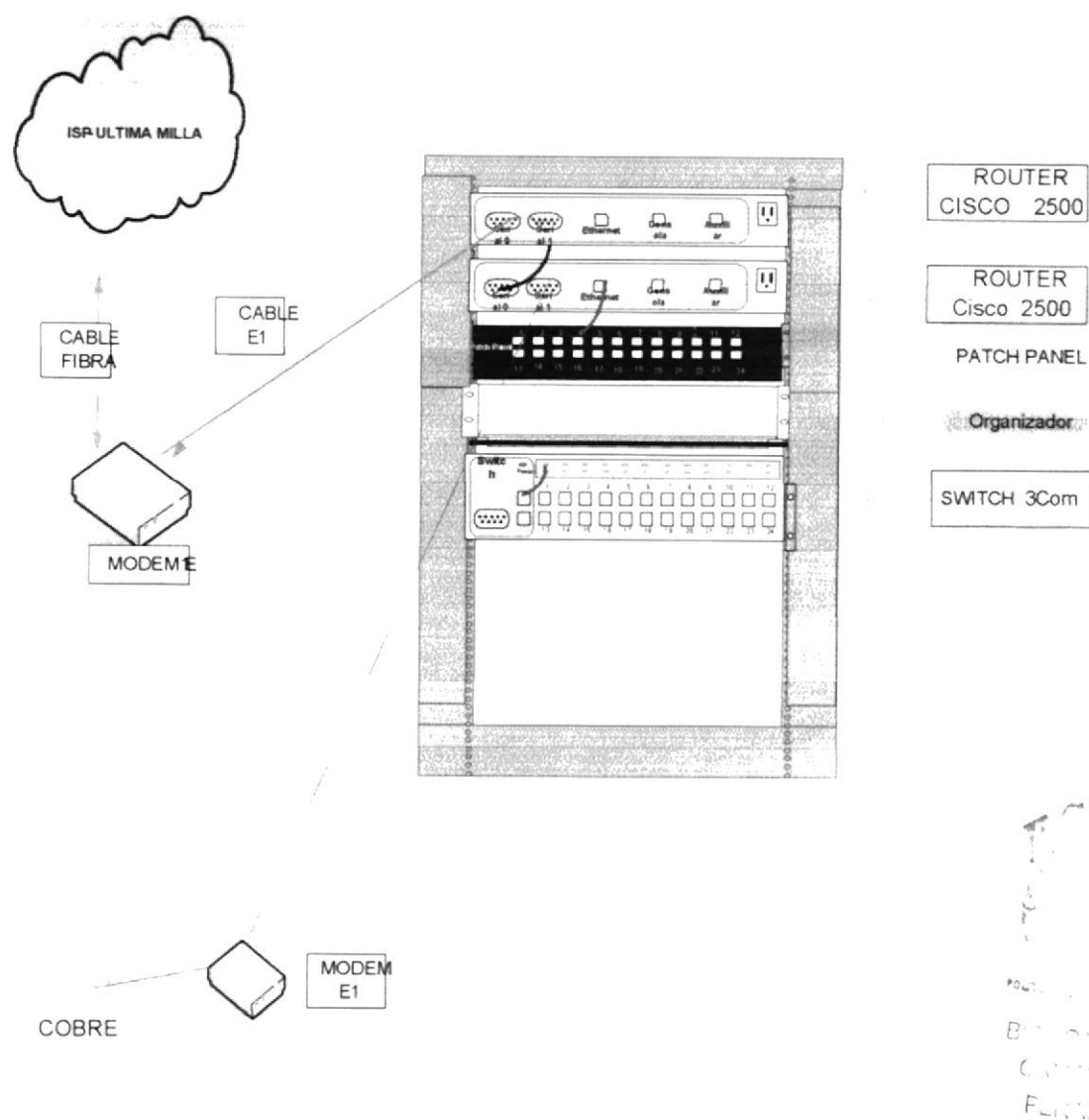
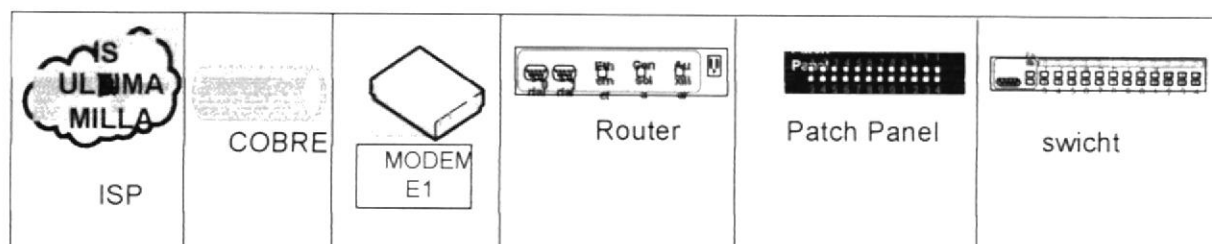


Figura 2-12: Mc-Urdesa

LEYENDAS



2.15 INFRAESTRUCTURA GENERAL DE LA RED LAN

2.15.1. MATRIZ

Continuación se detalla las características que posee la infraestructura de la red interna de la empresa SERVIPAGOS.

Tipo red	Lan
Topología de red	estrella
Cableado UTP	Categoría 5e
Tarjeta red	Velocidad 10/100 Mbps
Switch	Marca: 3Com Modelo: 2024 24 Puertos Administrables Tecnología Puertos truncados. Fuentes redundante. stackeable velocidad 100Mbps 24 puertos Capa 3

Tabla 2-14: Infraestructura lan Matriz

2.15.2. AGENCIAS (PORTETE – URDESA)

Tipo red	Lan
Topología de red	Estrella(esta topología esta asignada en todos las sucursales)
Cableado UTP	Categoría 5e
Tarjeta red	Velocidad 100/100Mbps
Switch	Marca: 3Com Modelo: 2024 No Hay Tecnología 24 puertos Velocidad 10 Mbps

Tabla 2-15: Infratesrucura Lan Sucursales



2.16 INFRAESTRUCTURA WAN DE LA EMPRESA SERVIPAGOS

Una vez analizado el estudio a nivel LAN; se comenzará hacer el segundo análisis de estudio, que se trata el análisis WAN de la empresa SERVIPAGOS. La comunicación WAN de dicha empresa se destaca por la comunicación anillo que más adelante se lo va a explicar.

2.17 INFRAESTRUCTURA GENERAL DE LA COMUNICACIÓN WAN

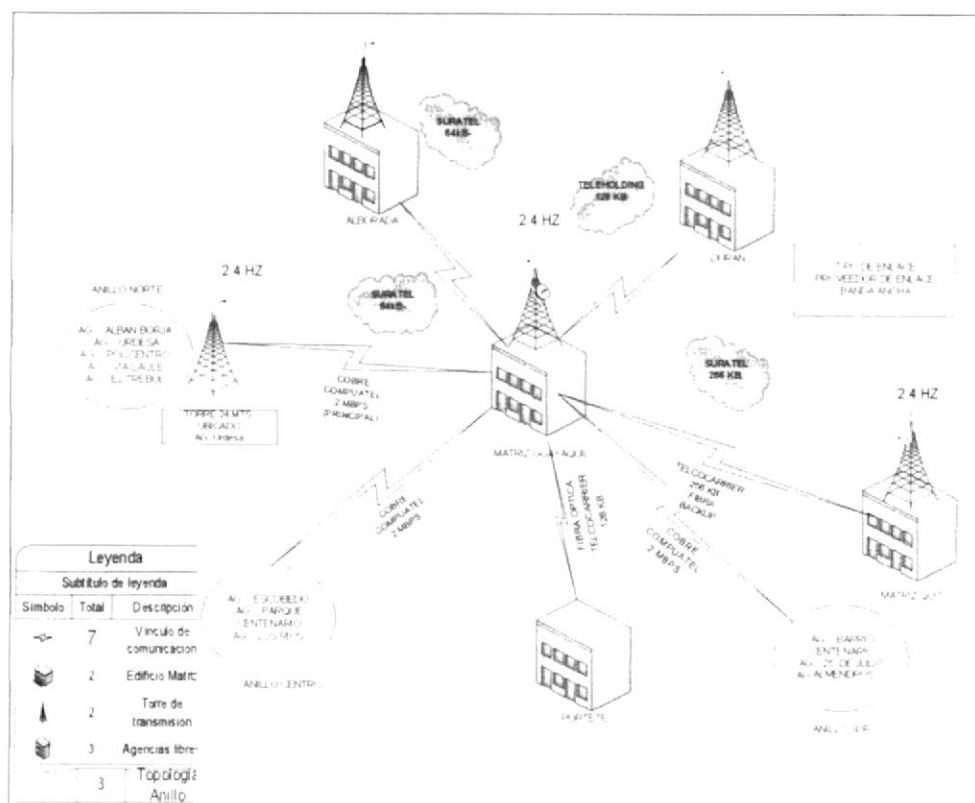


Figura 2-13: Gráfico Comunicación Wan

DESCRIPCIÓN DE LA COMUNICACIÓN WAN

Este gráfico demuestra en una forma general como está conectado todos los edificios tanto Matriz como sucursales, las sucursales se conectan entre sí dando forma de una topología anillo, es decir, las sucursales se conectan con una sucursal principal; que es la que se encarga de trasladar los paquetes de datos a la matriz, eso se denomina "anillo Norte"; "anillo sur", o el nombre según le corresponda.

2.18.2. ANILLO SUR (GRÁFICO DE COMUNICACIÓN)

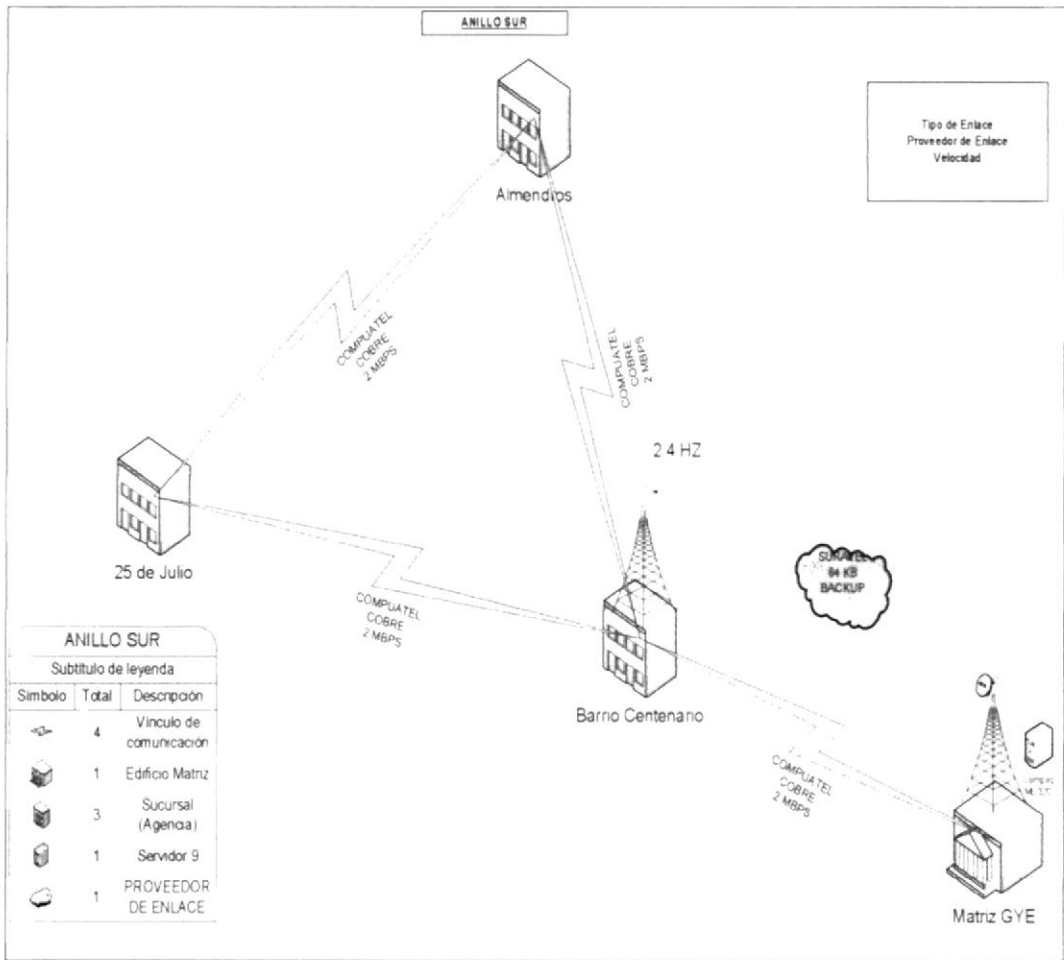


Figura 2-15: Gráfico Anillo Sur

DESCRIPCIÓN DEL ANILLO SUR

Las agencias 25 de Julio y Almendros están enlazadas con la agencia Barrio Centenario que conforman un anillo entre estas sucursales, mediante el tipo de enlace cobre ya que su proveedor de enlace es Compuatel y su velocidad es de 2 Mbps.

La agencia Barrio Centenario se conecta directo con la Matriz mediante cobre y su proveedor de enlace es Compuatel, y su velocidad es de 2 Mbps, También Consta de un proveedor de enlace Backup vía Microonda con su proveedor de enlace Suratel y su velocidad es de 64Kb.

2.19 INFRAESTRUCTURA WAN A NIVEL DE DISPOSITIVOS

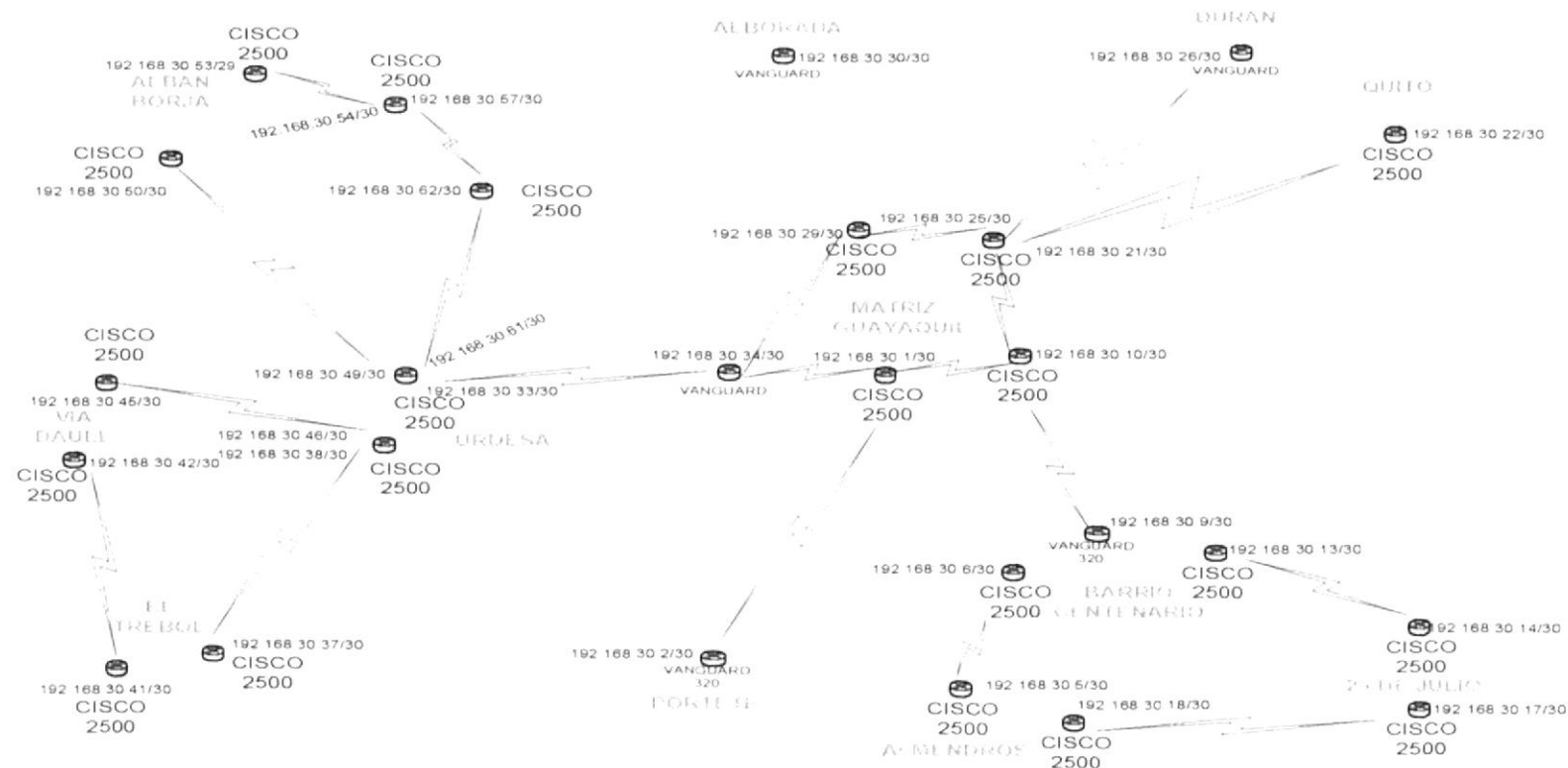


Figura 2-16: Gráfico Nivel Dispositivos

Solo las agencias Escobedo; Barrio Centenario, Durán, Portete, Alborada, y una en la Matriz usan ruteadores Vanguard 320. Todas las sucursales que forman las topologías anillos; La ciudad de Quito y 4 en la matriz utilizan un router cisco 2500.

2.19.1. TOPOLOGÍA ANILLO NORTE

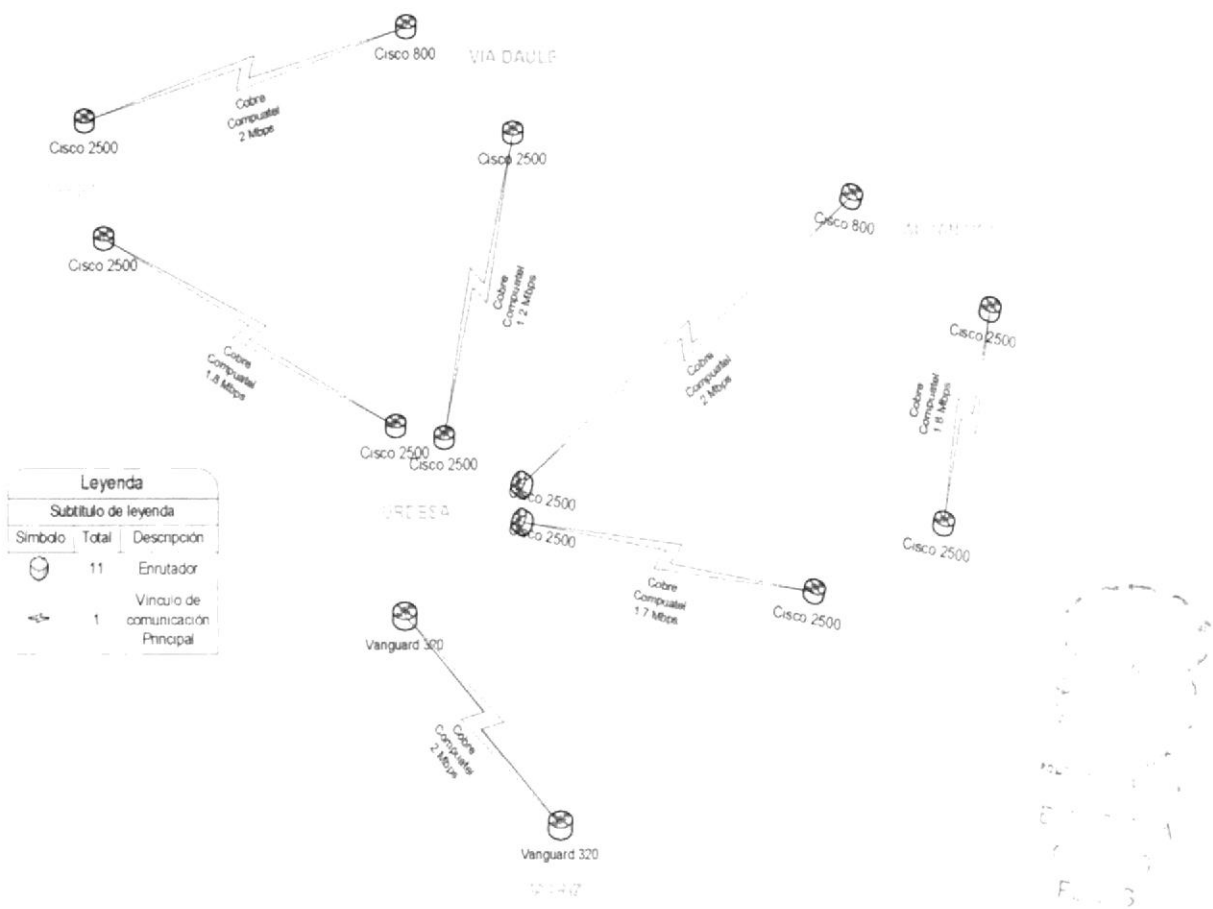


Figura 2-17: Anillo Norte Nivel Dispositivos

DESCRIPCIÓN DE LA TOPOLOGÍA ANILLO NORTE

La topología Anillo norte se trata de diversas sucursales que se conectan con una sucursal principal que es la encargada de trasladar los paquetes a la matriz.

En este gráfico no muestra que existen 2 anillos y forman uno solo:

El primer anillo lo conforman la Agencia el Trébol y Daule y se conectan con Urdesa.

El segundo anillo lo forman Alban Borja, Policentro, y se conectan con la sucursal Urdesa.

Por lo tanto, la sucursal Urdesa es la encargada de trasladar los paquetes a la matriz.

Los que conforman el anillo norte cuentan con un router Cisco 2500 cada sucursal.

2.19.2. TOPOLOGÍA ANILLO SUR

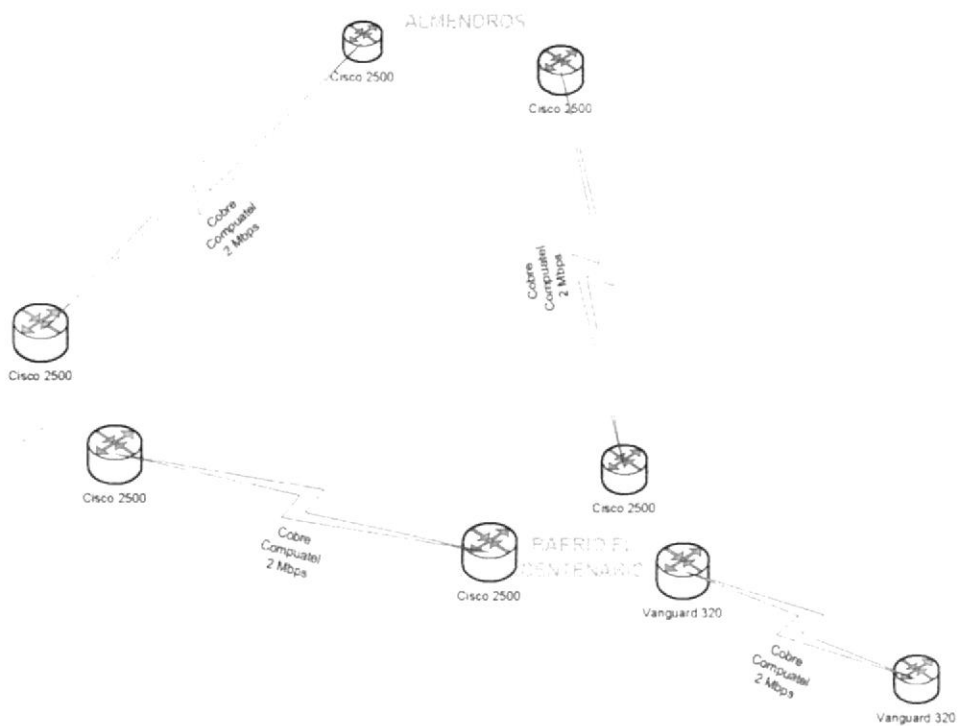


Figura 2-18: Anillo Sur Nivel Dispositivos

DESCRIPCIÓN DE LA TOPOLOGÍA ANILLO SUR

El anillo sur está conformado por diversas sucursales que están cerca de su sector, donde las diversas sucursales se conectan con la sucursal principal, que es la encargada de trasladar los paquetes de datos a la Matriz. En el gráfico se demuestra que:

La sucursal 25 de Julio y Almendros con una distancia de 3 Km. se conectan con la sucursal principal que es la del Barrio Centenario. El Barrio Centenario se encargará de hacer el traslado de los paquetes a la matriz.

Los que conforma el anillo sur cuenta con un router Cisco 2500 cada sucursal.



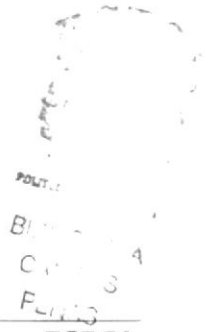
2.20 DISPOSITIVOS DE ENRUTAMIENTO

2.20.1. MATRIZ – GUAYAQUIL

ROUTER

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Producción &desarrollo (Sistema)	4	Router Cisco 2500	Una plataforma fija conexiones WAN, con opciones múltiples Cuatro puertos manejados Mbps de 10/100 interruptor Hasta 20 túneles de VPN puerto de consola por conectar término de la consola EIA/TIA-232 puerto auxiliar por conectar un término o módem Capacidad para vlans
Producción &desarrollo (Sistema)	1	Router Cisco 2600	Opción redundante de la fuente de alimentación Velocidad 12.000-15.000pps) Arquitectura: alto rendimiento
Producción &desarrollo (Sistema)	4	Router Vanguard 320	Cable con Terminal V.35 Incorpora los protocolos de la herencia

Tabla 2-16: Tabla enrutamiento Matriz



2.20.2. AGENCIA PORTETE

ROUTER

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Computo	1	Router Vanguard 320	Cable con Terminal V.35 Incorpora los protocolos de la herencia

Tabla 2-17: Tabla Enrutamiento Portete

2.20.3. SUCURSAL - URDESA

ROUTER

DPTO	CANTIDAD	TIPO	CARACTERÍSTICAS
Computo	2	Router Cisco 2500	Una plataforma fija conexiones WAN, con opciones múltiples Cuatro puertos manejados Mbps de 10/100 interruptor Hasta 20 túneles de VPN puerto de consola por conectar término de la consola EIA/TIA-232 puerto auxiliar por conectar un término o módem Capacidad para vlans

Tabla 2-18: Tabla enrutamiento Urdesa



2.21 INFRAESTRUCTURA DE SEGURIDAD DE REDES WAN

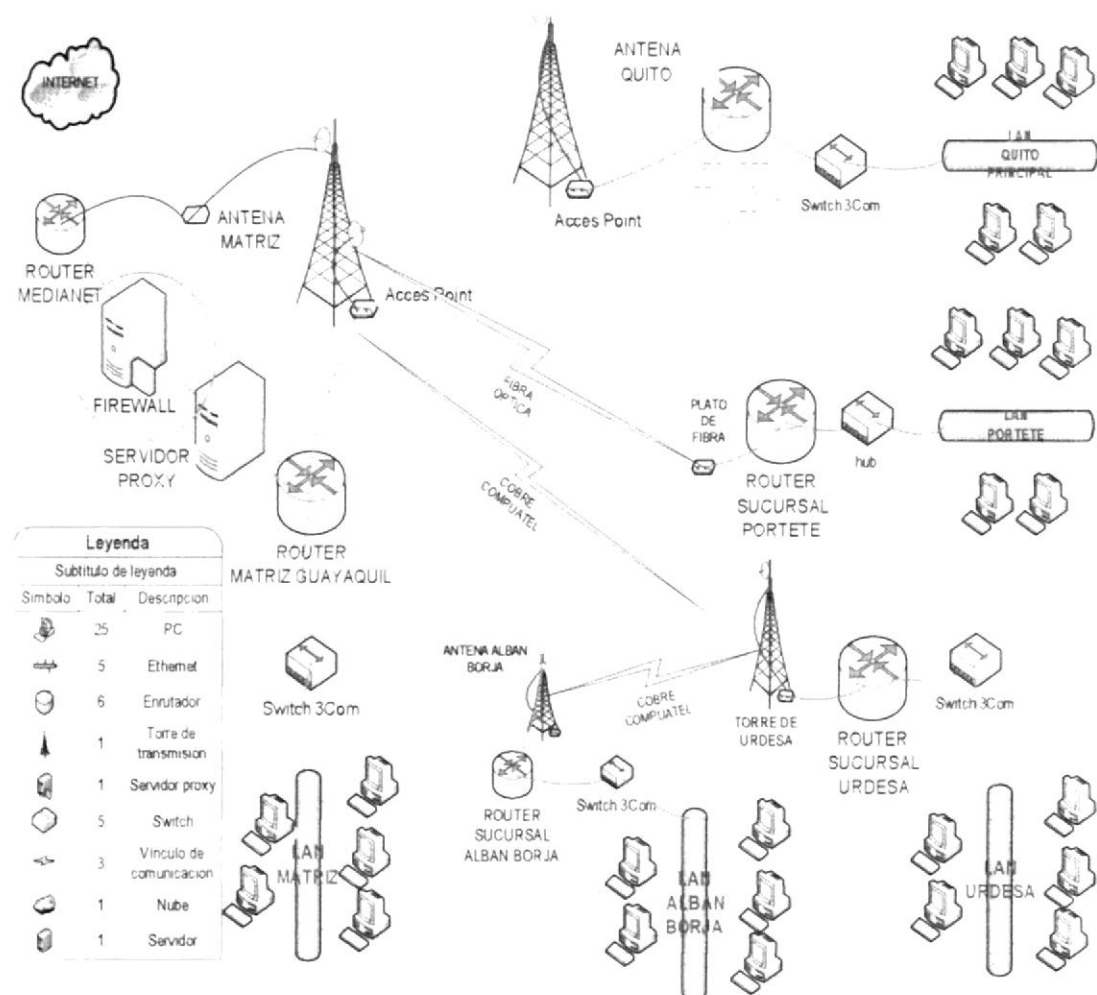


Figura 2-19: Infraestructura Nivel Wan

DESCRIPCIÓN DE LA INFRAESTRUCTURA DE LA SEGURIDAD WAN

Los Firewalls están aplicados a nivel de Software en un servidor Linux Hat, donde todas las sucursales si quieren salir a Internet deben pasar por los Firewalls que se encuentran en la matriz



2.22 INFRAESTRUCTURA RECEPCIÓN DE INTERNET

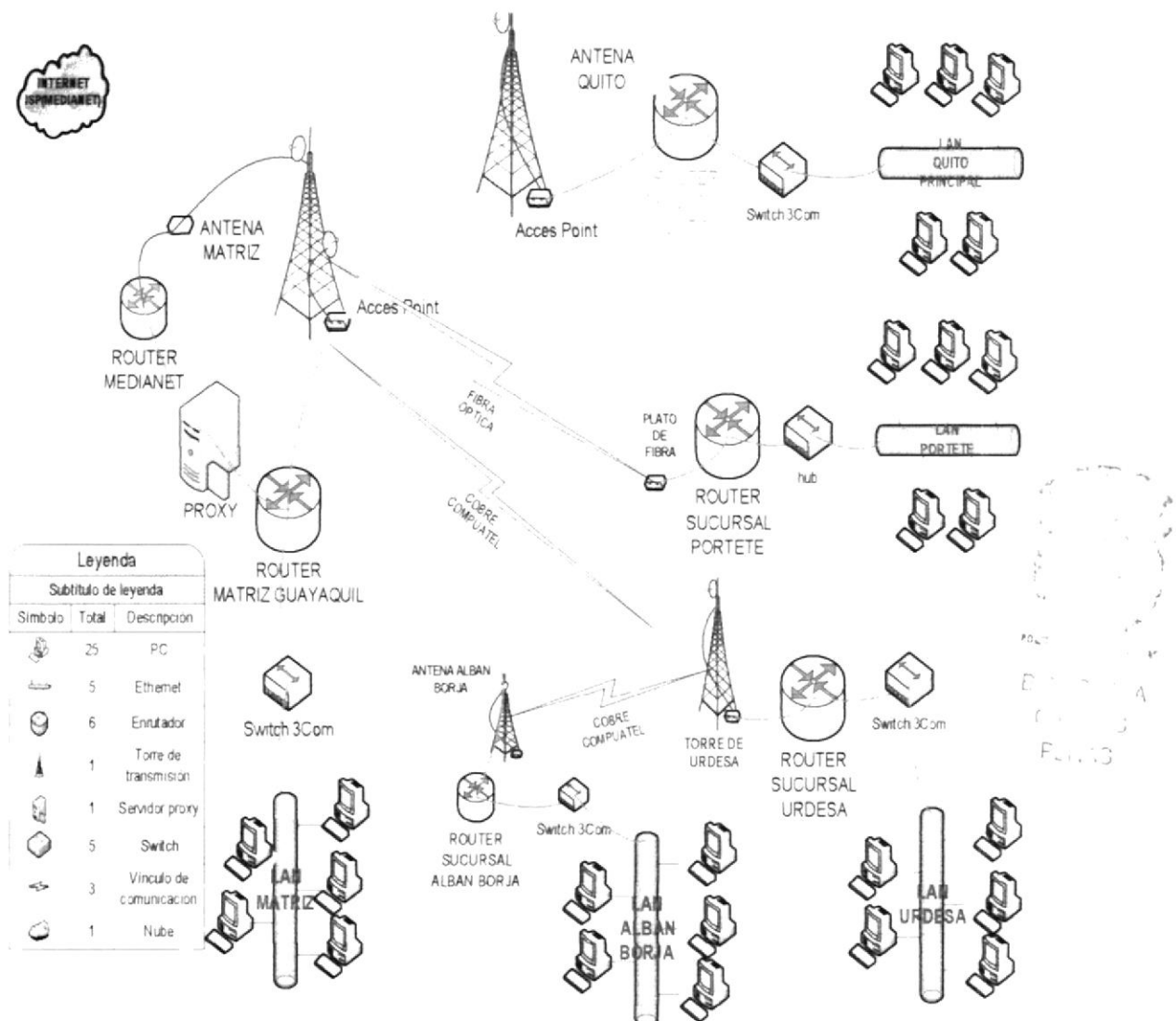


Figura 2-20: Infraestructura recepción Internet

La infraestructura del Internet está compuesta por un ISP (MEDIANET) que da servicio de Internet a la empresa SERVIPAGOS, quién recibe el Internet es la matriz y a su vez es la encargada de repartir Internet a sus sucursales.

2.23 PROBLEMAS ENCONTRADOS EN LA SITUACIÓN ACTUAL

- Colisión en la red Lan de la sucursal Portete
- Lentitud en el sistema mediante los procesos en los servidores de Base de Datos.
- Lentitud en la comunicación WAN entre la Sucursal Urdesa y la Matriz. Por motivo que el ancho de banda es bajo.
- No existe un respaldo de comunicación WAN entre matriz y Agencia Portete
- Congestión en la red Lan de toda la empresa.





CAPÍTULO 3

SOLUCIÓN PROPUESTA

3. SOLUCIÓN PROPUESTA

3.1 PROBLEMAS ENCONTRADOS

PROBLEMAS	CAUSAS	EFEECTO
Colisión en la red Lan de la sucursal Portete	Uso de dispositivos inadecuados (HUBS)	Congestionamiento en la red Lan
Lentitud en el sistema mediante los procesos en los servidores de Base de Datos.	La capacidad de los disco duros están sobrepasado a su limite	Demora en recibir informes de la base de datos
Lentitud en la comunicación WAN entre la Sucursal Urdesa y la Matriz	No cuenta con suficiente ancho de banda.	Tiempos de respuesta altos
No existe un respaldo de comunicación WAN entre matriz y Agencia Portete	La empresa no tomaron consideración de un respaldo secundario.	En caso que falle la comunicación principal no habrá comunicación entre sucursal y matriz
Congestión en la red Lan de toda la empresa	Existencia de broadcast en la red Lan. La red Lan no está segmentada	Lentitud en la red tiempo de respuesta altos en los usuarios.

Tabla 3-1: Problemas

3.2 SOLUCIÓN

PROBLEMAS	SOLUCIÓN	ALCANCE
Colisión en la red Lan de la sucursal Portete	Remplazar los dispositivos de Red por dispositivos adecuados a sus requerimientos (usos de switches Administrable capa 2)	Disminuir las colisiones y mejorar los tiempos de respuesta en la Red
Lentitud en el sistema mediante los procesos en los servidores de Base de Datos.	Adquirir un nuevo servidor que ofrezca mejor rendimiento. Y mayor capacidad de almacenamiento	El equipo nuevo brindará soporte y puede generar procesos rápidamente.
Lentitud en la comunicación WAN entre la Sucursal Urdesa y la Matriz	Adquirir mas ancho de banda al proveedor	Mejorar las comunicaciones en línea, y garantizar la comunicación en línea
No existe un respaldo de comunicación WAN entre matriz y Agencia Portete	Implementar el uso de un enlace secundario que garantice comunicación estable entre sucursal y matriz	La empresa contará un respaldo secundario en caso de perdida de enlace principal
Congestión en la red Lan de toda la empresa	Creación de subredes, (implementación de VLANS)	- Las VLANS mejoran la seguridad de la red Lan y ayudan a controlar los broadcasts - Control, tráfico de red

Tabla 3-2: Solución

3.3 ESTUDIO DE LA ALTERNATIVA "A"

Esta alternativa está orientada a mejorar los tiempos de respuestas en la red, brindar mayor ancho de banda; medios de respaldos para mantener una comunicación segura.

3.3.1. FACTIBILIDAD TÉCNICA

En esta factibilidad se detalla los dispositivos y equipos que se van adquirir para la empresa.

CANT	DESCRIPCIÓN	UBICACIÓN	EDIFICIO	GRÁFICO
1	• Marca Power ConnectTM • Modelo 5324 • Switch Gigabit flexible, con alta seguridad y fácil administración • Capa 2 • Capacidad 100 MBPS • Soporta 24 grupos de VLANs	Dpto. Computo	•Portete	
1	• Servidor IBM • Modelo: System x 206m • Procesador: Intel Pentium Dual Core 3.00GHz. • Memoria de 2 GB. • Disco duro: 120GB Hasta 4 discos, capacidad de almacenamiento • Tarjeta red 100/1000 Mbps • Incluido con el sistema Operativo Windows 2003 Server (Licencia por un año)	Dpto. Sistemas	• Matriz	

Tabla 3-3: Factibilidad Técnica "A" Equipos Propios

NOTA

En la factibilidad A se ha llegado a un acuerdo con el ISP **TELCOCARRIER**; quienes serán la empresa que alquilará los dispositivos, para la comunicación entre Matriz y Agencia Portete.
A Continuación se detalla los dispositivos que se alquilarán.

CANT	DESCRIPCIÓN	UBICACIÓN	EDIFICIO	GRÁFICO
2	ANTENA T/GRILLA - MARCA : hypelink 24 DBI ganancia - Frecuencia 2.4 Ghz	Terraza de los edificio	- Matriz - Portete	
2	PIGTAIL Tipo N ancho a SMA	Terraza de los edificio	- Matriz - Portete	
2	MODEN - LINKSYS ADSL2 MODEM WITH USB & ETHERNET ADSL2MUE - Para transportar enlaces digitales E1 PR1	Dpto. Sistemas	- Matriz - Portete	
2	ACCESPOINT - Marca BRIDGE 5.8 GHZ - TT2800.11a 54 MBPS 8 Grados	Terraza de los edificio	- Matriz - Portete	

Tabla 3-4: Factibilidad Técnica de Alquiler “A” Dispostivos Alquiler

3.4 FACTIBILIDAD ECONÓMICA

3.4.1. COSTOS EQUIPOS

En este cuadro se muestra los valores de cuanto van a costar los materiales que se adquirirán.

Costos de equipos			
Cant.	descripción	costo unitario	costo total
1	Switch PowerConnectTM 5324	\$ 700	\$ 700
1	Servidor IBM Sistema x.	\$1859	\$1859
Total implemento			\$2,559

Tabla 3-5: Factibilidad Economica "A"Costos Equipos

3.4.2. COSTO DE ALQUILER DE LOS DISPOSITIVOS CON EL ISP

En la factibilidad A se ha llegado a un acuerdo con el proveedor ISP telocarrier, que consiste en alquilar los dispositivos tales como: antena, accespoint, Módem, que facilitará una factibilidad más económica, con la finalidad de estos dispositivos hacer una conexión de Tecnología **WIRELESS EXTENDED WAN.**

Continuación se detalla el precio de alquiler de los dispositivos.

Costos de equipos			
Cant.	descripción	costo unitario	Costo total
1	Switch Administrable	\$ 700	\$ 700
1	Servidor de Base de Datos.	\$1859	\$1859
Total implemento			\$2,559

Tabla 3-6: Factibilidad Economica "A"Costos Alquiler Dispositivos

3.4.3. COSTO DEL ENLACE

Costo del Enlace			
Tipo de Enlace	distancia	costo mensual	costo total
Microondas	4 Km.	\$150	\$450
Total			\$450

Tabla 3-7: Factibilidad Economica "A" Costo de Enlace

3.4.4. COSTO DE AUMENTO ANCHO DE BANDA

DETALLE	Ancho de banda kbps	Costo mensual
Alquiler de ancho de banda	512	\$ 600

Tabla 3-8: Factibilidad Economica "A" Costo Aumento Ancho de Banda

3.4.5. COSTO OPERATIVO

FASES	PERSONAL	SEMANAS	COSTOS POR PERSONAL SEMANAL	COSTO	COSTO FASE
Fase de diseño de la red Wan	1 Ing. en telecomunicación	2 días	\$ 33.33 por día	\$ 66.66	
COSTO FASE					\$ 66.66
Fase de implementación Wan	1 Adm. red	7 días	\$ 25 por día	\$ 300	
	1 Ing. en Telecomunicación	3 días	\$33,33 por día	\$ 99.99	
	2 Asistentes redes	7 días	\$ 20 por día	\$ 280	
COSTO FASE					\$ 554,99
Fase de prueba Wan	1 Adm. red	1 semana 4 días	\$25 por día	\$ 250	
	1 Ing. en Telecomunicación	2 días	\$33,33 por día	\$ 66,66	
	2 Asistentes de redes	1 semana 4 días	\$20 por día	\$ 400	
COSTO FASE					\$ 716,66
Fase de documentación Wan	1 Adm. red	5 días	\$ 25	\$ 125	
	1 Ing. en Telecomunicación	3 días	\$ 33,33	\$ 99,99	
COSTO FASE					\$ 224,99
TOTAL DEL COSTO OPERATIVO					\$ 1,563.03

Tabla 3-9: Factibilidad Economica "A" Costo Operativo

3.5 FACTIBILIDAD OPERATIVA

FASES	SEMANA	TOTAL SEMANA
FASE DE ANÁLISIS DE LA RED LAN Y WAN		
1 Ing. en Telecomunicación	2 semanas	
1 Adm. de Red	2 semanas	
semana por fase		
2 semanas		
FASE DE DISEÑO DE LA RED WAN		
1 Ing. en Telecomunicación	2 días	
semanas por fase		
2 días		
FASE DE IMPLEMENTACIÓN WAN		
1 Adm. Red	1 semana 1 día	
1 Ing. en Telecomunicación	3 días	
2 Asistentes de redes	1 semana 1 día	
semanas por fase		
1 semana 1 día		
FASE DE LA PRUEBA DE LA RED WAN		
1 Adm. red	1 semana 4 días	
2 Asistentes de redes	1 semana 4 días	
1 Ing. en Telecomunicación	2 días	
semanas por fase		
1 semana 4 días		
FASE DE DOCUMENTACIÓN WAN		
1 Adm. redes	5 días	
1 Ing. en Telecomunicación	3 días	
semanas por fase		
8 días		
TOTAL DE SEMANAS		6 Semanas 3 días

Tabla 3-10: Factibilidad Operativa "A"

3.5.1. DETALLE DE LA FASE DE ANÁLISIS LAN Y WAN

En la fase de análisis se detalla el estudio realizado de la empresa SERVIPAGOS con el objetivo de verificar los problemas actuales que tienen la empresa tanto a nivel LAN como WAN, para darle solución a los problemas encontrados. Las personas que intervienen en esta fase que durará 2 semanas serán un Ingeniero en Telecomunicación y un Administrador de Red.

3.6 COSTO TOTAL DE LA PROPUESTA "A"

El costo de de la factibilidad "A" está orientada a sus gastos y beneficio que se le dará a la empresa **SERVIPAGOS**.

COSTO TOTAL FACTIBILIDAD ECONÓMICA	
Costo de Equipos	\$2,559.00
Costo de alquiler de Dispositivos	\$570.00
Costo del enlace	\$450.00
Costo de aumento del ancho de banda	\$ 600.00
Costo Operativo	\$ 1,563.03
SUB TOTAL DE LA PROPUESTA A	\$5,742.03
Costo total de la factibilidad Económica	\$6,603.33

Tabla 3-11: Costo Total Factibilidad "A"



3.7 VENTAJAS & BENEFICIO

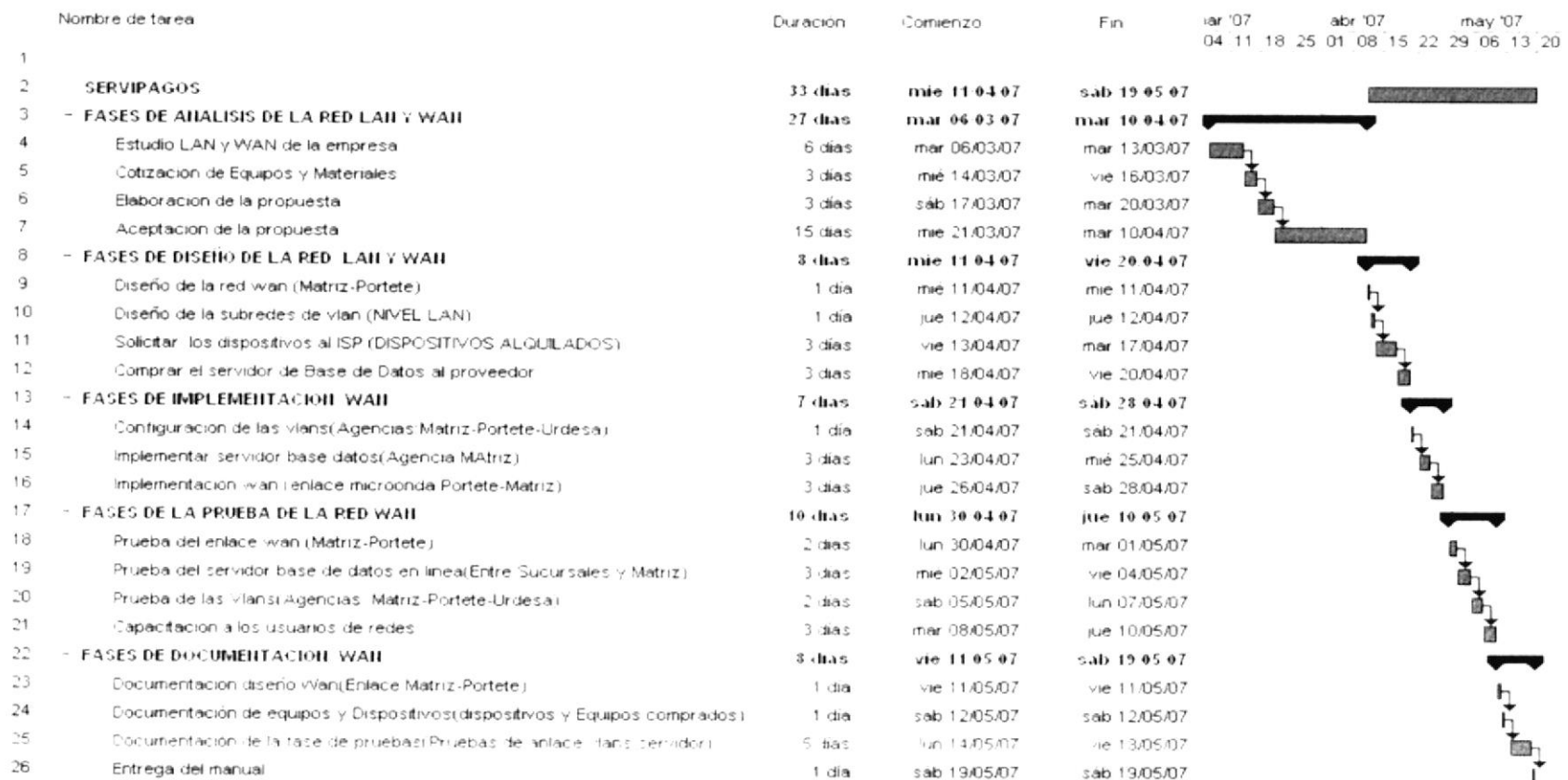
3.7.1. VENTAJAS

- Garantizamos nuestros servicios en los dispositivos adquiridos por 3 meses.
- Los envíos de paquetes de datos sucursal y matriz serán más rápidos.
- Gracias a este proyecto Todas las sucursales no tendrán pérdidas de Enlaces.

3.7.2. BENEFICIO

- La empresa tendrá una imagen más eficaz y eficiente.
- Los clientes de Servipagos contarán con un servicio rápido y mejorado sin demora alguna.

3.10 GANT-A



3.8 FORMA DE PAGO

A continuación se detallará la forma de pago de la alternativa "A"

Esta propuesta esta sujeta a los estudios realizados de la empresa de existir un cambio se le comunicará con anticipación, de aceptar esta propuesta se deberá enviar.

60% de la aceptación de la propuesta (al inicio de la primera fase)

40% del costo total al finalizar el contrato

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

3.9 GARANTÍA

La garantía que se ofrece será basado en soporte técnico que se brinda, una vez terminado el proyecto que se realizará a la Empresa, el tiempo de duración de 3 meses sin costo alguno, durante los 3 meses si se llega a efectuar un problema ustedes podrán contar con nuestros servicios directamente, siempre y cuando este dentro de la garantía.

Pasado de los 3 meses se pierde la garantía, si ustedes desean podrán renovar un contrato de 3 meses o más, para que ustedes cuenten con nuestros servicios de calidad.

El valor por renovar el contrato tendrá un costo adicional.

Las garantías de equipos y dispositivos los brindarán los proveedores con los cuales se trabajará (**TELCOCARRIER**).



3.11 ESTUDIO DE LA ALTERNATIVA "B"

La Factibilidad B utilizará para mejorar los tiempos de respuestas anivel Lan y Wan equipos con alta tecnología que pertenecerán a la empresa Servipagos

3.11.1. FACTIBILIDAD TÉCNICA

En esta factibilidad no se alquilan dispositivos, en este caso se van a comprar los equipos que van a ser propiedad de la empresa. .

CANT	DESCRIPCIÓN	UBICACIÓN	EDIFICIO	GRÁFICO
2	Módem externo ADSL con interfaz Ethernet 10/100BASE-TX.	Dpto. Sistemas	Matriz Portete	
1	- Modelo: NonStop s76 2 procesadores 300 MHz - Memoria 1 GB estándar máx. 3GBmemoria - Disco duro 120GB,capacida d de colocar 3 disco mas - Tarjeta red 100/1000Mbps - Incluido el sistema Operativo Windows 2003 Server (Licencia por un año) - Garantía: 2años	Dpto. Sistemas	Matriz	

Tabla 3-12: Factibilidad Técnica "B"



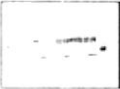
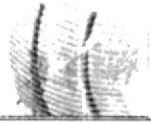
CANT	DESCRIPCIÓN	UBICACIÓN	EDIFICIO	GRÁFICO
1	Switch administrable • 24 puertos RJ45 • Velocidad 10-100MBPS • Soporta 24 grupos de VLANs. • Capa 2	Dpto. Sistemas	• Portete	
2	ANTENAS MICROONDAS GRILLA • Antenas GRILLA. • son antenas de aberturas pequeñas, rectangulares • trabaja frecuencia 2.4GHz • 24 DBI ganancia • Gira 8 grados	Terraza de los edificio mencionado	• Matriz • Portete	
2	ACCESPOINT • 5.8 GHZ • TT2800.11a • 54 MBPS	Terraza de los edificio mencionado	• Matriz • Portete	
2	PIGTAIL • Tipo N ancho a SMA 50 Cm	Terraza de los edificio mencionado	• Matriz • Portete	

Tabla 3-13: Factibilidad técnica "B"

3.12 FACTIBILIDAD ECÓNOMICA

3.12.1. COSTO DE EQUIPOS

En este cuadro se muestran los valores de cuanto van a costar los materiales que se va adquirir que van hacer propio de la empresa.

Costos de Equipos			
Cant.	descripción	costo unitario	costo total
2	antena microonda grilla	\$74.50	\$149.00
2	Accespoint	\$ 544.00	\$ 1088.00
2	Pigtail de tipo N ancho	\$8.50	\$ 17.00
2	Módem externo	\$53.60	\$ 107.20
1	Switch administrable	\$ 476	\$ 476
1	Servidor de Base de Datos	\$1700	\$1700
Total			\$3,537.20

Tabla 3-14: Factibilidad Economica "B" Costo de Equipos

3.12.2. COSTO DEL ENLACE CON EL ISP

Costó del Enlace			
Tipo de Enlace	distancia	costo mensual	costo total
Microondas	4 Km.	210	210
Total			210

Tabla 3-15: Factibilidad Economica "B" Costo Enlace con el ISP

3.12.3. COSTO DE AUMENTO ANCHO DE BANDA

DETALLE	Ancho de banda kbps	Costo mensual
Alquiler de ancho de banda	256	\$ 160

Tabla 3-16: Factibilidad Economica "B" Costo Aumento Ancho de banda



3.12.4. COSTO OPERATIVO

FASES	PERSONAL	SEMANAS	COSTOS POR PERSONAL SEMANAL	COSTO	COSTO FASE
Fase de diseño de la red Lan & Wan	1 Ing. en Telecomunicación	2 días	\$ 33,33 por día	\$ 66.66	
COSTO FASE					\$66.66
Fase de implementación De la red Wan	1 Adm. red	1 semana 1 día	\$ 150.00 \$25 por día	\$175.00	
	2 Asistente de redes	1 semana 1 día	\$120.00 \$20 por día	\$ 280.00	
	1 Ing. en Telecomunicación	3 días	\$ 33.33 por día	\$99.99	
COSTO FASE					\$ 554.99
Fase de prueba De la red Wan	1 Adm. red	1 semana 4 días	\$ 150.00 (\$25 por días)	\$ 250.00	
	1 Ing. en Telecomunicación	3 días	\$ 33.33 por día	\$ 99.99	
	2 Asistentes de redes	1 semana 1 día	\$ 100.00 (\$20 por día)	\$ 120.00	
COSTO FASE					\$ 549.99
Fase de documentación De la red Wan	1 Adm. red	10 días	\$ 25	\$ 250.00	
	1 Ing. en Telecomunicación	2 días	\$ 33,33	\$66.66	
COSTO FASE					\$ 316.66
TOTAL DEL COSTO OPERATIVO					\$1,303.03

Tabla 3-17: Factibilidad Operativa "B" Costo Operativos

3.13 FACTIBILIDAD OPERATIVA

FASES	SEMANA	TOTAL SEMANA
FASES DE ANALISIS DE LA RED LAN Y WAN		
1 Ing. en Telecomunicación	2 semanas	
1 Adm. Redes	2 semanas	
semana por fases		2 semanas
FASES DE DISEÑO DE LA RED WAN		
1 ing. en telecomunicación	2 días	
semana por fases		2 días
FASES DE IMPLEMENTACION WAN		
1 Adm. redes	1semanas 1 día	
1 ing. en telecomunicación	3 días	
2 Asistente redes	1semanas 1 día	
semana por fases		1semana 1 día
FASES DE LA PRUEBA DE LA RED WAN		
1 Adm. redes	10 días	
2 Asistente redes	10 días	
1 ing. en telecomunicación	3 días	
semana por fases		10 días
FASES DE DOCUMENTACION WAN		
1 Adm. redes	10 días	
1 ing. en telecomunicación	2 días	
semana por fases		10 días
TOTAL DE SEMANAS		6 SEMANAS 4 días

Tabla 3-18: Factibilidad Operativa "B"

3.13.1. DETALLE DE LA FASE DE ANÁLISIS LAN Y WAN

En la fase de análisis se detalla el estudio realizado de la empresa SERVIPAGOS con el objetivo de verificar los problemas actuales que tienen la empresa tanto a nivel LAN como WAN, para darle solución a los problemas encontrados. Las personas que intervienen en esta fase que durará 2 semanas serán un Ingeniero en Telecomunicación y un Administrador de red.

3.14 COSTO TOTAL DE LA PROPUESTA "B"

El costo de la factibilidad "B" está orientado a sus gastos y sus beneficios que se le dará a la empresa **SERVIPAGOS**.

TOTAL PROPUESTA "B"	
Costos de Equipos	\$3,537.20
Costo del enlace con el ISP	\$210.00
Costo de aumento ancho de banda	\$ 160.00
Costo operativo	\$1,303.03
SUB TOTAL DE LA PROPUESTA B	\$5,210.23
COSTO TOTAL DE LA PROPUESTA B \$5,991.76	

Tabla 3-19: Costo Total Factibilidad "B"



3.15 VENTAJAS & BENEFICIO

3.15.1. VENTAJAS

- Los envíos de paquetes de datos sucursal y matriz serán más rápidos.
- Gracias a este proyecto todas las sucursales no tendrán pérdida de enlace.

3.15.2. BENEFICIO

- La empresa contará con servidor mejorado.
- Los clientes de Servipagos contarán con un servicio más rápido sin demora alguna.



3.16 FORMA DE PAGO

A continuación se detallará la forma de pago de la alternativa "B"

Esta propuesta está sujeta a los estudios realizados de la empresa de existir un cambio se le comunicará con anticipación, de aceptar la propuesta se deberá enviar.

60% de la aceptación de la propuesta (al inicio de la primera fase)

40% del costo total al finalizar el contrato

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

3.17 GARANTÍA

La garantía que se ofrece será basada en soporte técnico que se brinda, es decir, una vez terminado el proyecto que se realizará a la Empresa, el tiempo de duración será por 3 meses sin costo alguno, durante los 3 meses si se llega a efectuar un problema ustedes podrán contar con nuestros técnicos servicios, siempre y cuando están dentro de la garantía.

Pasado de los 3 meses se pierde la garantía, si ustedes desean podrán renovar un contrato de 3 meses o más, para que ustedes cuenten con nuestros servicios.

El valor por renovar el contrato tendrá un costo adicional.

Las garantías de equipos y dispositivos los brindarán las empresas a las que ustedes decidan comprar.



3.18 GANT-B

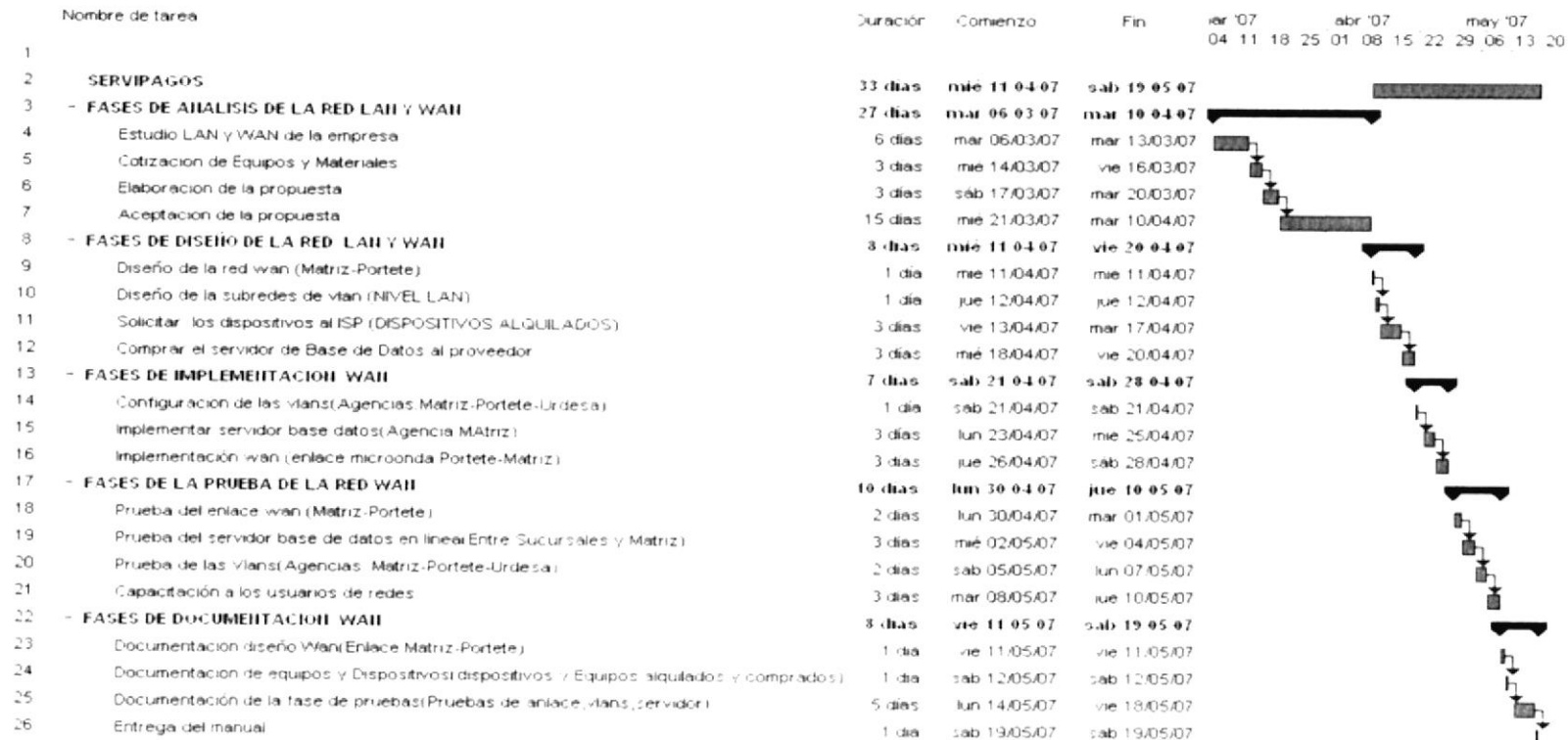


Figura 3-2: Gant B

Proyecto: ALT_B Fecha: lun 21/05/07	Tarea		Relic		Tarea externa:	
	Origen		Relic		Relic externo	
	Progreso		Relic		Fecha final	



CAPÍTULO 4

IMPLEMENTACIÓN

WAN



4. IMPLEMENTACIÓN WAN

4.1 NIVEL WAN

La implementación está dirigida a nivel Wan, donde en el sistema actual se encuentra que existe pérdida de comunicación, por motivo que no tiene un respaldo ENTRE LOS EDIFICIOS MATRIZ Y PORTETE, por lo tanto se aplicará una solución para dicho problema de tal manera se utilizará respaldo microonda.

TÍTULO	Leyenda	Autores:
Gráfico del edificio Portete	Antena microonda Backbone Vertical	K. Miranda S. Ramos W. Yanez
IMPLEMENTACIÓN ANTENA MICROONDA 2.4 GHZ PORTETE BLOQUE A CANTOS FLUJO Tuberías eléctricas y de agua DEPARTAMENTOS Backbone Horizontal PISO DE SERVIDORES 2U 1U 2U 1U MD5 13 MTS 30 MTS Backbone Vertical Fibra Monomodo EXISTENTE NOTA: en este gráfico se detalla donde se ubicará la antena que será la comunicación de respaldo que se encuentra en la parte superior del edificio.		

Tabla 4-1: Implementación Antena microonda "Portete"

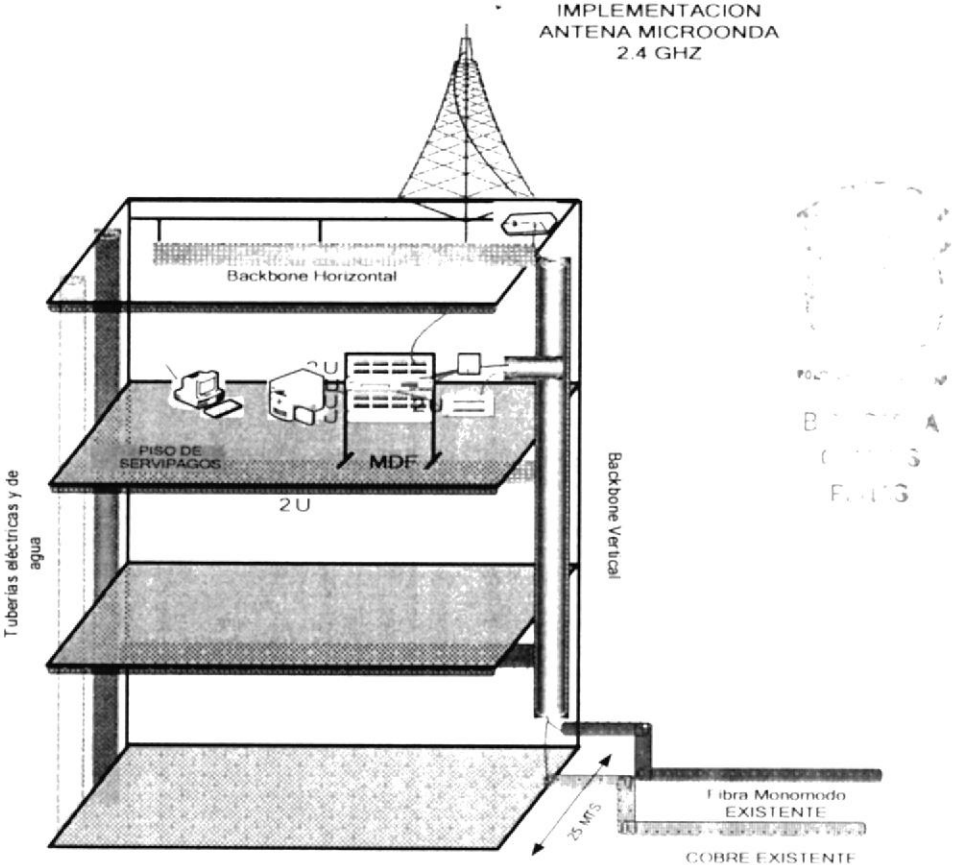
TÍTULO Gráfico del Edificio Matriz	Leyenda  Antena Principal de comunicacion  Backbone Vertical	Autores: K. Miranda S. Ramos W. Yanez
 IMPLEMENTACION ANTENA MICROONDA 2.4 GHZ Backbone Horizontal PISO DE SERVIDORES MDF 2 U Backbone Vertical Tuberías eléctricas y de agua 25 Mts Fibra Monomodo EXISTENTE COBRE EXISTENTE NOTA: en este gráfico se detalla donde se ubicará la antena de respaldo Matriz-Portete, que se encuentra en las torres de antena de la matriz		

Tabla 4-2: Implemantación Antena Miroonda "Matriz"

4.2 ENLACE DE CONEXIÓN

La conexión será de enlace serial, que trabajará en una frecuencia de 2.4 GHZ. Con un ancho de banda 128 Kbps, que se conectará entre el edificio Matriz y Portete. Para que sea conexión serial; se va a contar con un módem que también está dentro de la implementación

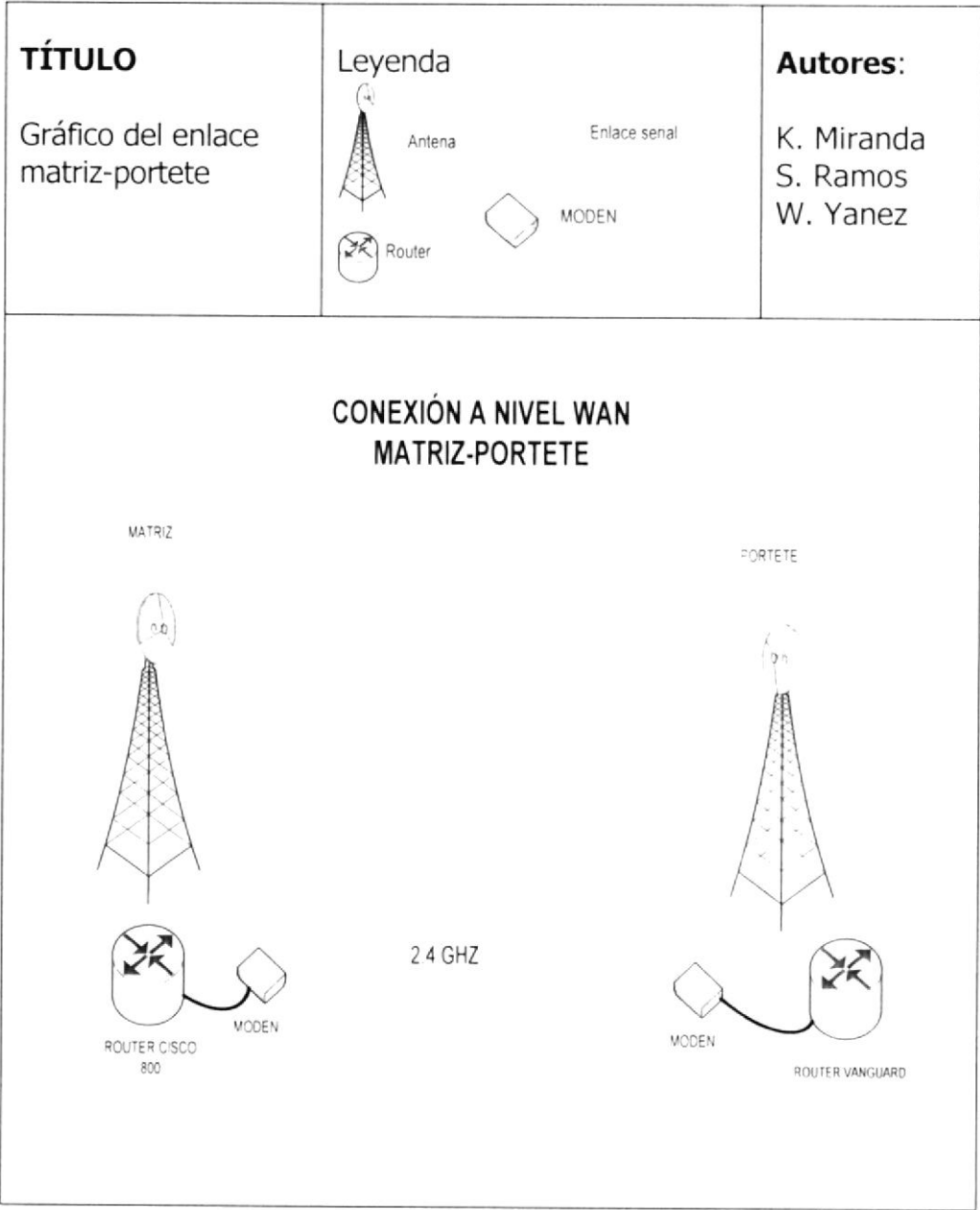


Tabla 4-3: Enlace de Conexión

En este gráfico se demuestra que, la conexión principal es por medio de fibra óptica que tiene una velocidad 256 KBPS, mientras que el backup es por enlace microonda

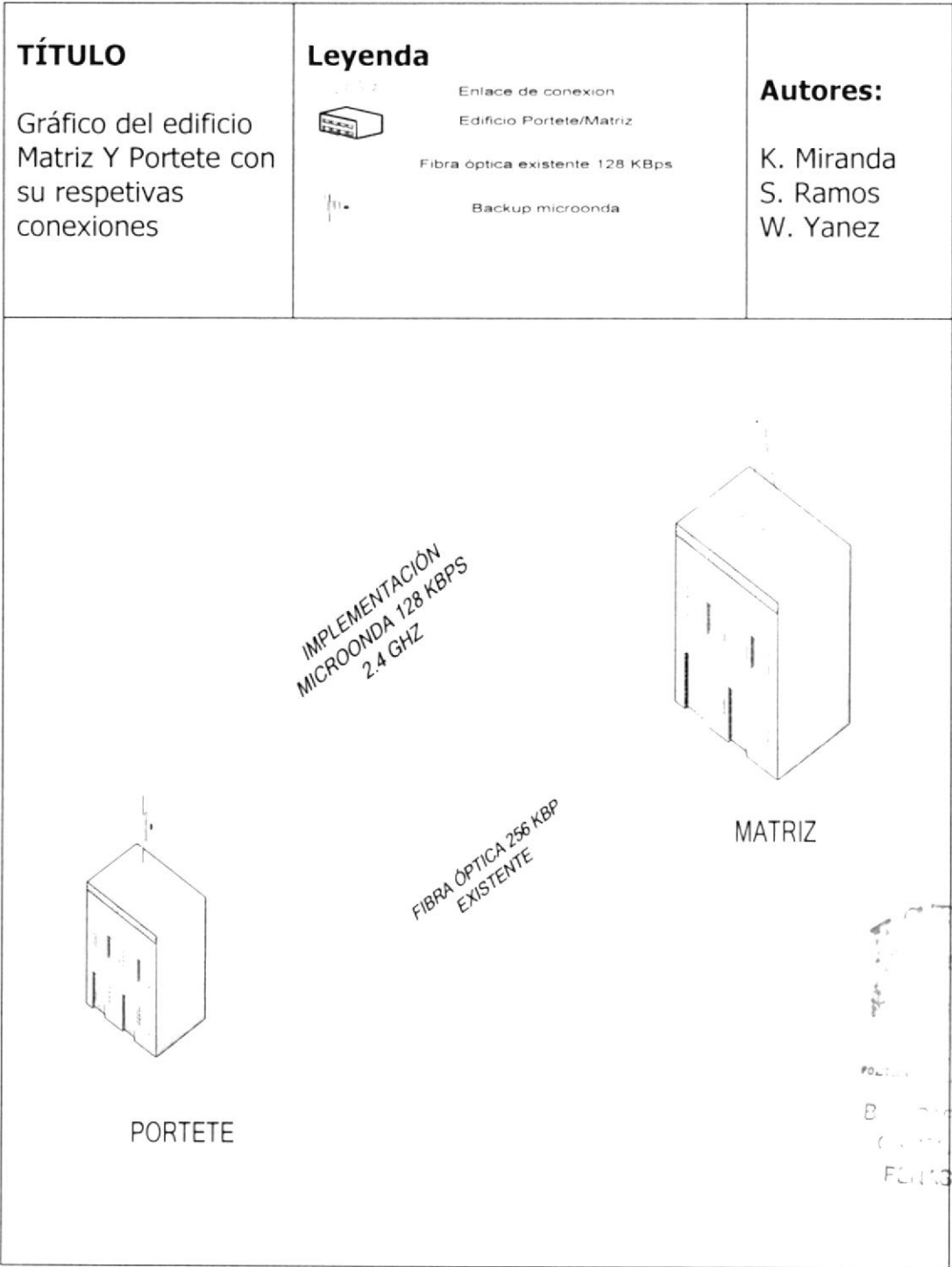


Tabla 4-4: Enlace Portete-Matriz

4.3 IMPLEMENTACIÓN DEL MC

4.3.1. MC (MATRIZ)

En este gráfico se demuestra como va a quedar el MC del edificio Matriz después de la implementación.

También se indica que la antena de respaldo (Matriz-Portete) pasa mediante el módem que se adquirió y se conecta con el ruteador respectivo de la Empresa.

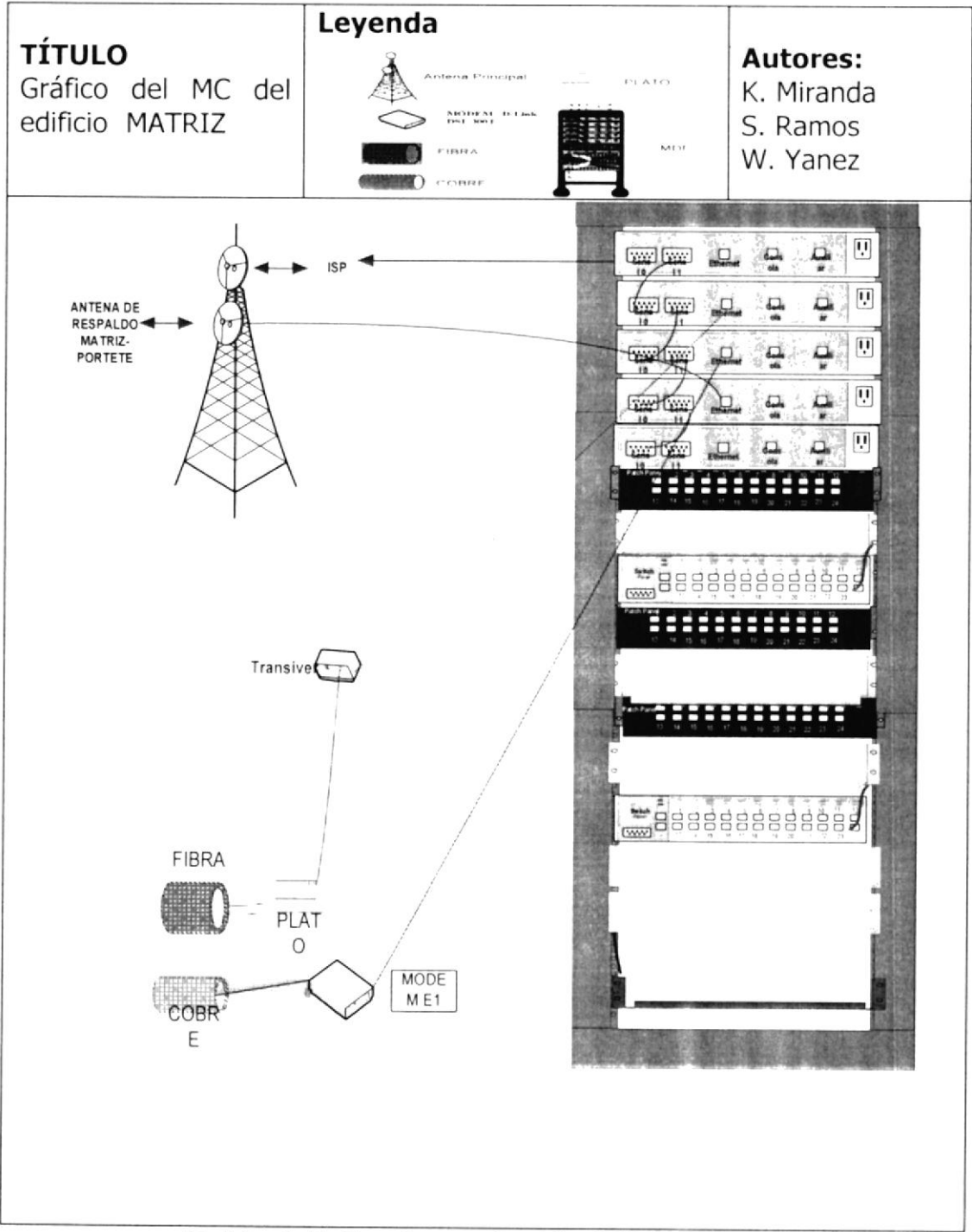


Tabla 4-5: Implemantación MC Matriz

4.3.2. MC (PORTETE)

En la sucursal portete posee como dispositivo un HUB actual, de tal manera este dispositivo ya no es usado, por eso se ha recomendado que compre nuevos dispositivos como: SWITCH "Administrable Capa 2" en el siguiente gráfico se demuestra como estará ubicado el dispositivo

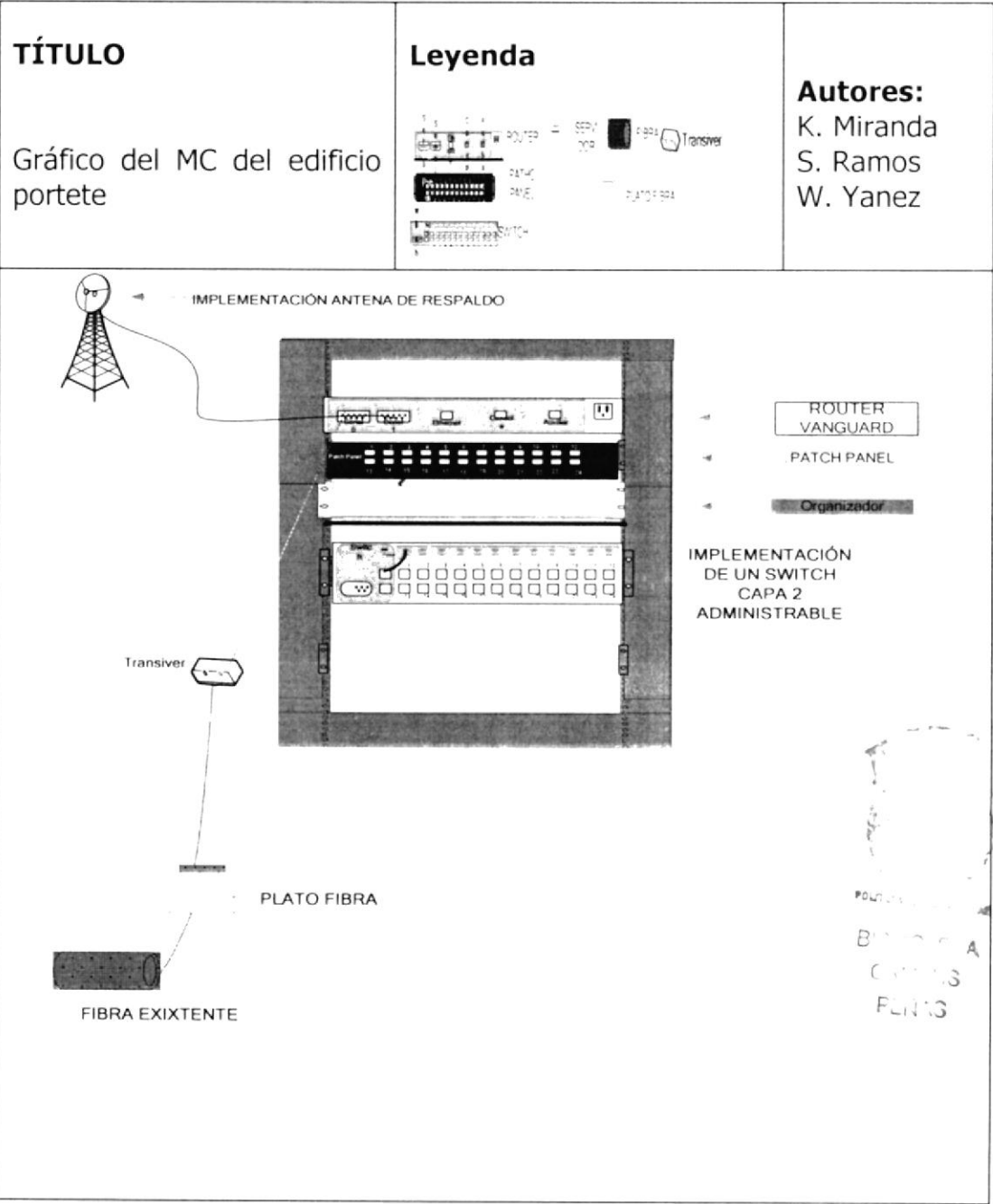


Tabla 4-6 Implementación MC Portete

4.4 ANCHO DE BANDA (MATRIZ-URDESA)

En Urdesa existe falla de comunicación en línea por motivo que tiene un ancho de banda de 128kbps, y genera pérdida de paquetes por lo tanto se necesitará adquirir aumentar el ancho de banda para que no fallé la comunicación.

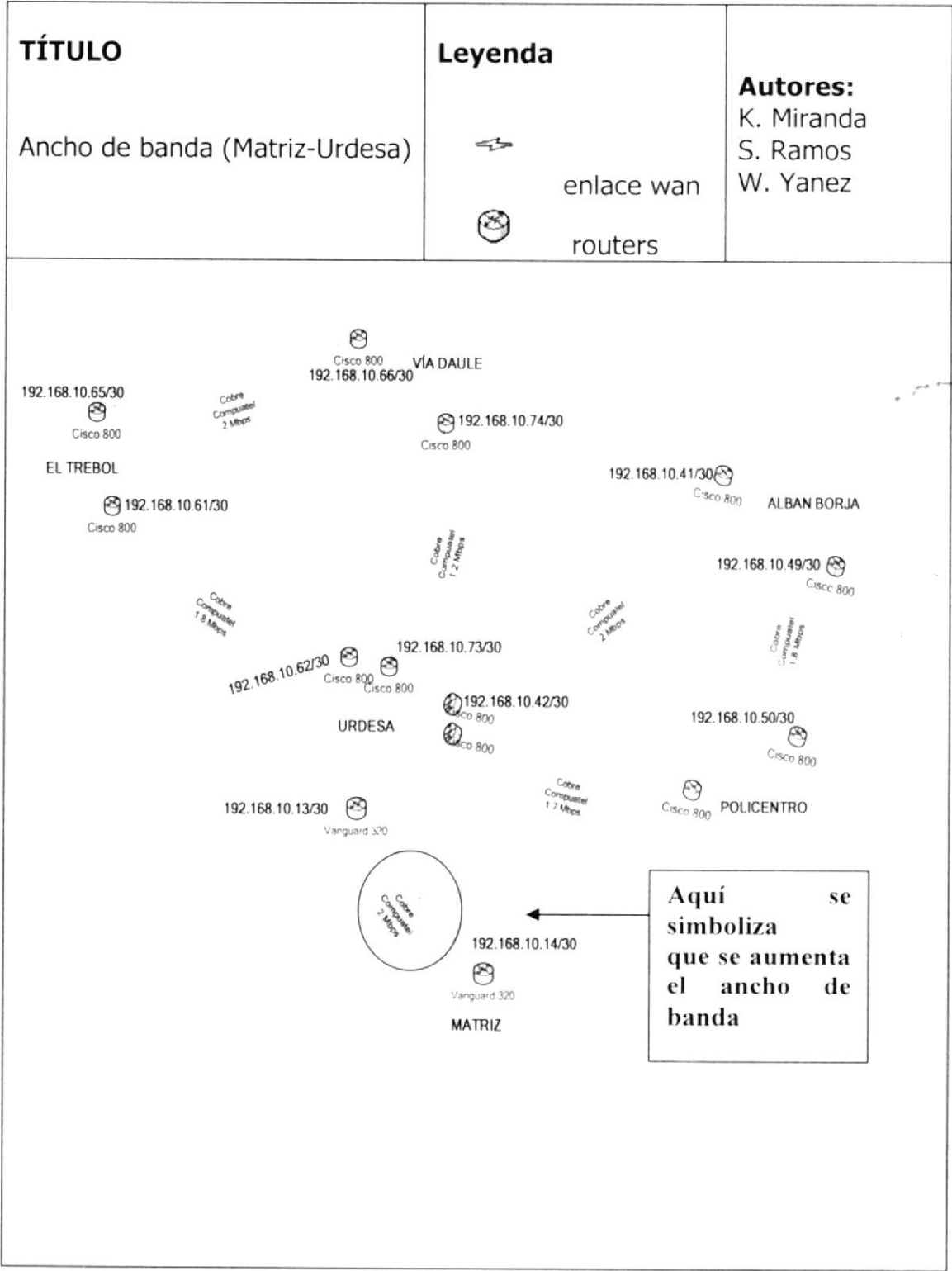


Tabla 4-7: Implementación Ancho de Banda

4.5 IMPLEMENTACIÓN DE VLAN

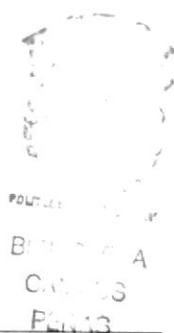
La Empresa Servipagos no cuenta con una red segmentada, para la seguridad se ha implementará subredes para todos los departamentos que tienen la empresa continuación se detalla como va a estar segmentada la **red LAN**

Agencia	VLAN	# PC	Red origen	Sub-interfaz	IP-disponibles
Matriz	sistema	7	192.168.30.177/28	30.178	179-190
	servicio al cliente	3	192.168.30.193/29	30.194	195-198
	Auditoría	4	192.168.30.200/29	30.201	202-206
	Comercialización	3	192.168.30.208/29	30.209	210-214
	r.r.h.h	3	192.168.30.216/29	30.217	218-222
	servicio al cliente	3	192.168.31.0/29	31.1	2-6
	calidad	3	192.168.31.8/29	31.9	10-14
	recepción	3	192.168.31.16/29	31.17	18-22
	gerente	2	192.168.31.24/29	31.25	26-30
	operación	5	192.168.31.32/29	31.33	34-38

Tabla 4-8: Implementación Vlan Matriz

Agencia	VLAN	# PC	Red origen	Sub-interfaz	IP-disponibles
Urdesa	Caja	5	192.168.30.144/29	30.145	146-150
	Gerencia	3	192.168.30.152/29	30.153	154-158
	Sistema	2	192.168.30.169/29	30.170	171-174
	Jefe caja	2	192.168.30.160/29	30.161	162-166

Tabla 4-9: Implementación Vlan Urdesa



Agencia	VLAN	# PC	Red origen	Sub- interfaz	IP- disponibles
Portete	Caja	5	192.168.30.96/29	30.97	98-102
	Gerencia	3	192.168.30.104/29	30.105	106-110
	Sistema	2	192.168.30.112/29	30.113	114-118
	Jefe caja	2	192.168.30.120/29	30.121	122-126
	Contabili- -dad	7	192.168.30.128/29	30.129	130-142

Tabla 4-10: Implementación Vlan Portete



CAPÍTULO 5 NORMATIVAS



5. NORMATIVAS

5.1 REGLAS DEL CABLEADO ESTRUCTURADO

▲ Obligatorio △ Recomendación

5.2 OBLIGATORIO

▲ Normativa 1

Consideraciones de interferencia electromagnética

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

1.- Todo sistema deberán estar puesto y unidos a tierra

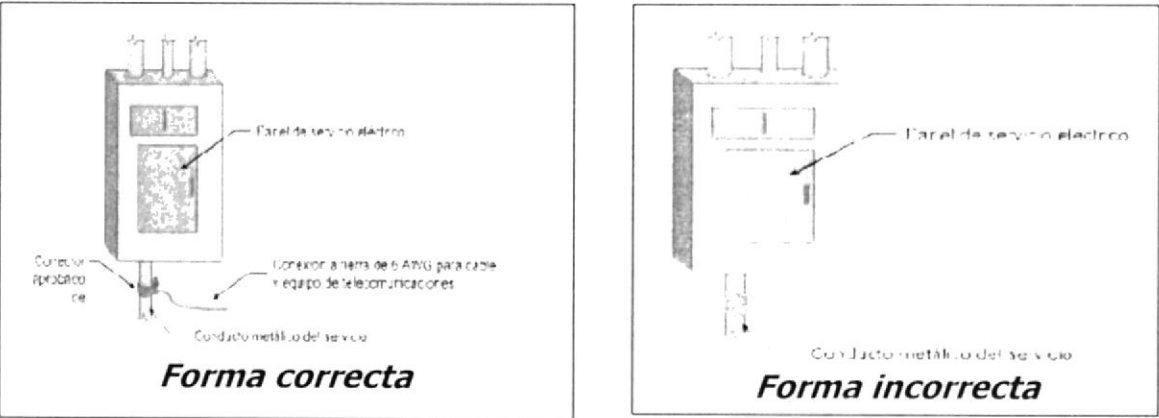


Figura 5-1: Normativa 1

2.- Deberán mantenerse una separación mínima de 50 mm (2 pulgadas) entre el cableado de telecomunicación de par trenzado sin blindaje (UTP) y los circuitos derivados menores a 3 KBA

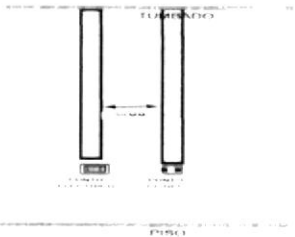


Figura 5-2: Normativa 1

▲ Normativa 2

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

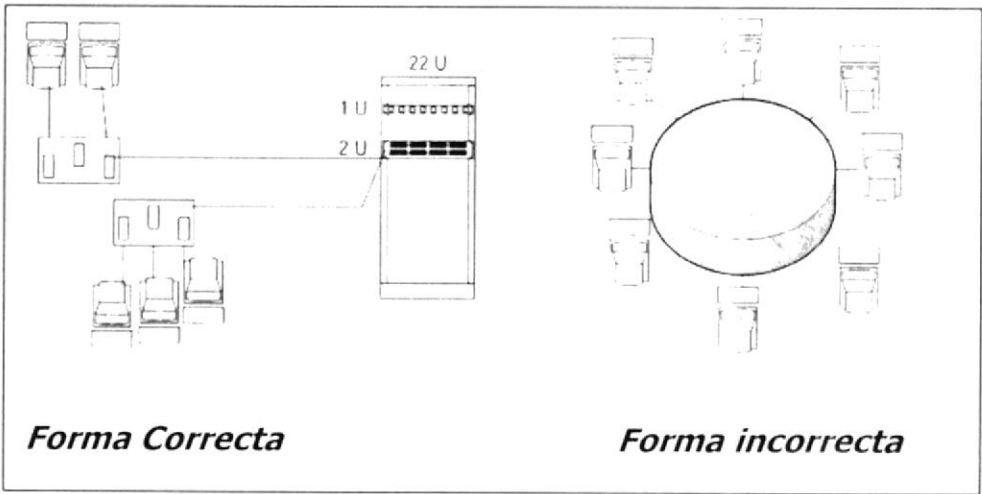


Figura 5-3: Normativa 2

▲ Normativa 3

Se aplicara conexión cruzadas para conexiones de cable horizontal y backbone

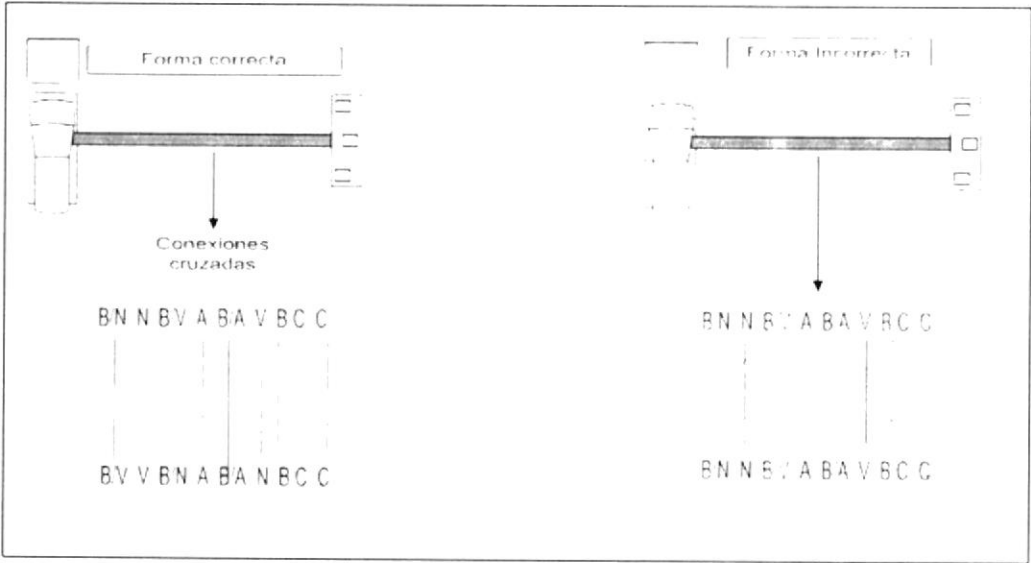


Figura 5-4: Normativa 3

▲ Normativa 4

Cada área de trabajo estará extendida por un H.C localizado en el mismo piso o en un piso adyacente

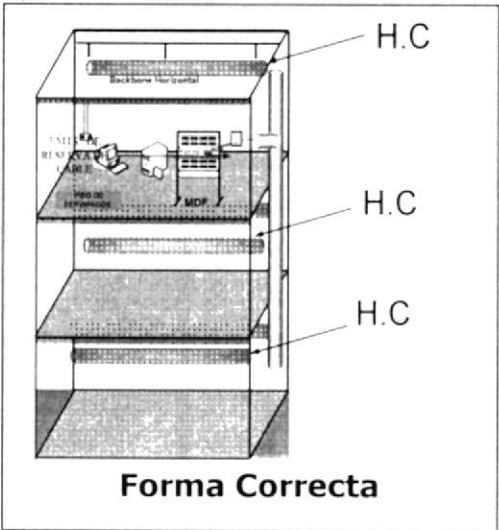


Figura 5-5: Normativa 4

▲ Normativa 5

No se permite el uso de derivaciones puenteadas en el H.C

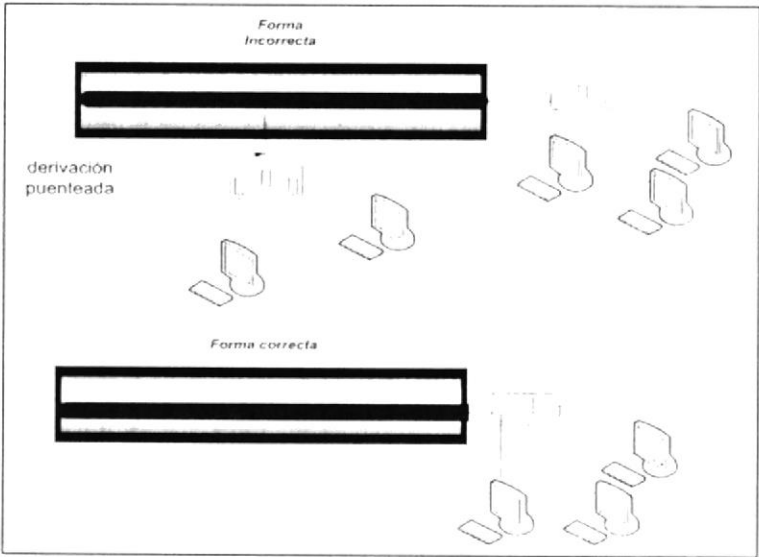
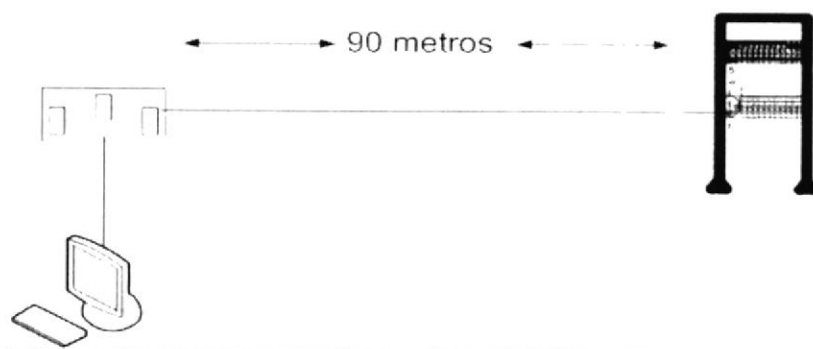


Figura 5-6: Normativa 5

**Normativa 6**

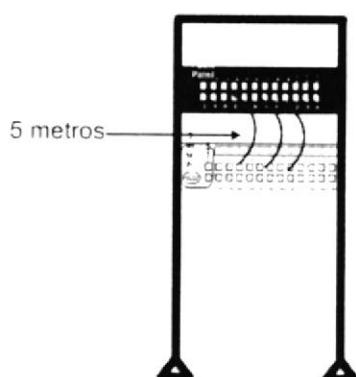
La longitud del cable entre la salida de telecomunicación y el H.C no excederá los 90mt. Independiente del tipo del medio



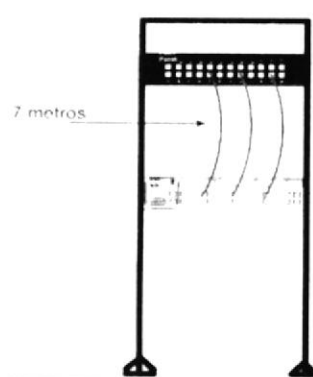
Forma Correcta
Figura 5-7: Normativa 6

**Normativa 7**

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



Forma Correcta



Forma Incorrecta.

Figura 5-8: Normativa 7

▲ Normativa 8

No se permitirá más de un punto de consolidación dentro del mismo tendido del cableado horizontal

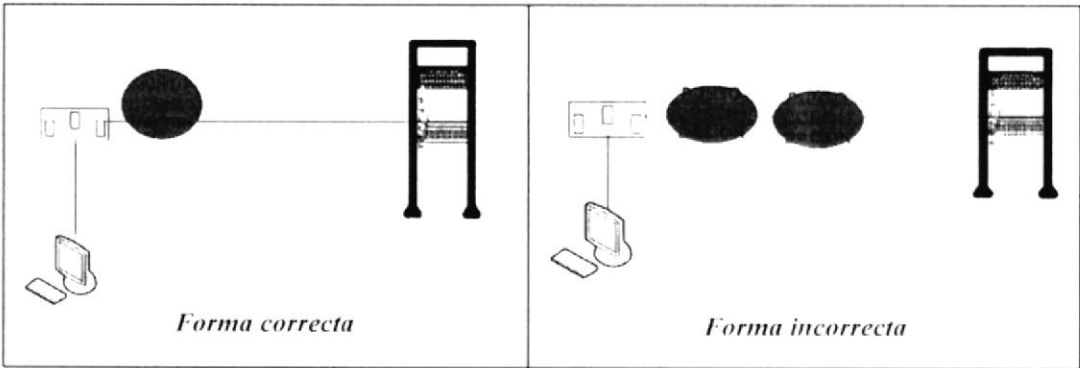


Figura 5-9: Normativa 8

▲ Normativa 9

No se permitirá conexiones cruzados o equipo activo en el punto de consolidación

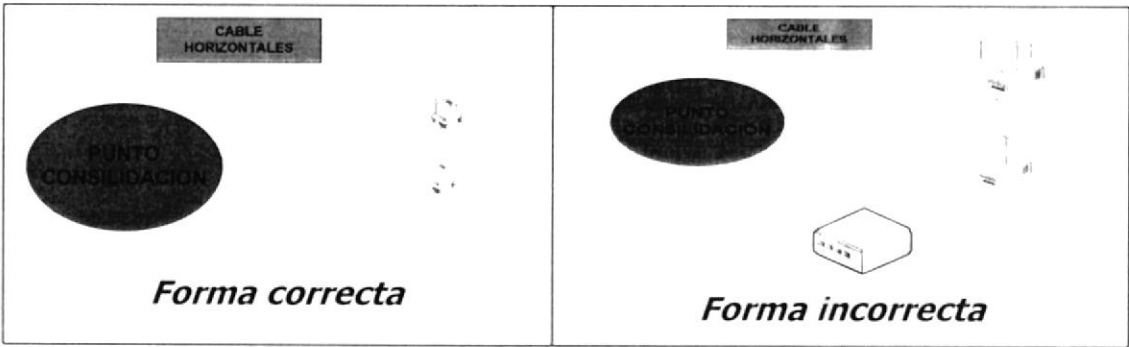


Figura 5-10: Normativa 9

Nota:

Punto de consolidación: es un hardware de conexión que proporciona interconexión entre cableado de oficina abierto y cableado horizontal

▲ Normativa 10

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

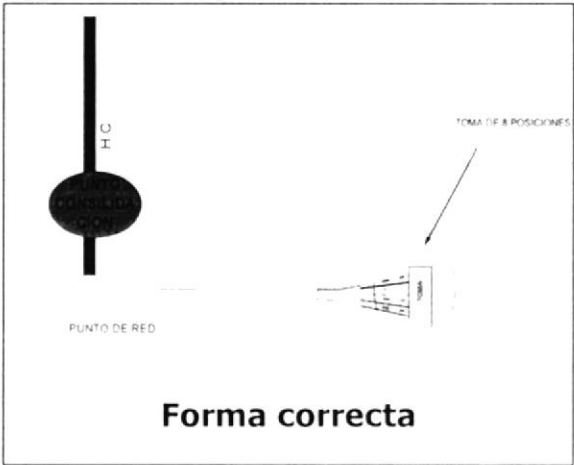


Figura 5-11: Normativa 10

▲ Normativa 11

La distancia máx. Entre el H.C y la salida de telecomunicación será de 90mt.



Figura 5-12: Normativa 11

▲ Normativa 12

La distancia min. Entre el H.C y el punto de consolidación será de 15mt.

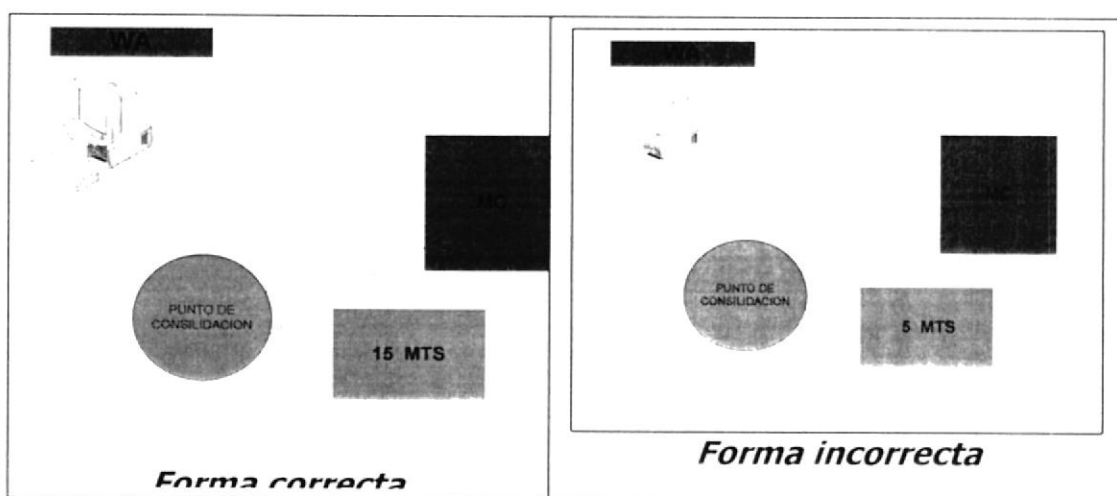


Figura 5-13: Normativa 12

▲ Normativa 13

La distancia min. Entre el punto consolidación y la salida de telecomunicación será de 15mt.

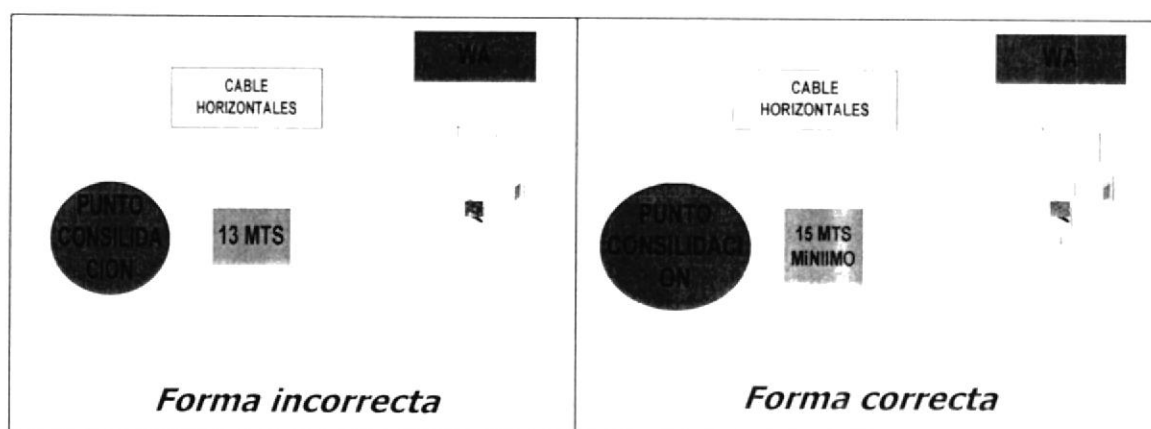


Figura 5-14: Normativa 13

▲ **Normativa 14**

La distancia del canal del cableado horizontal incluyendo patchcord y salida de telecomunicación NO excederá a 100mts.



▲ **Normativa 15**

Todos los pares del cable estarán totalmente terminados en ambos extremos

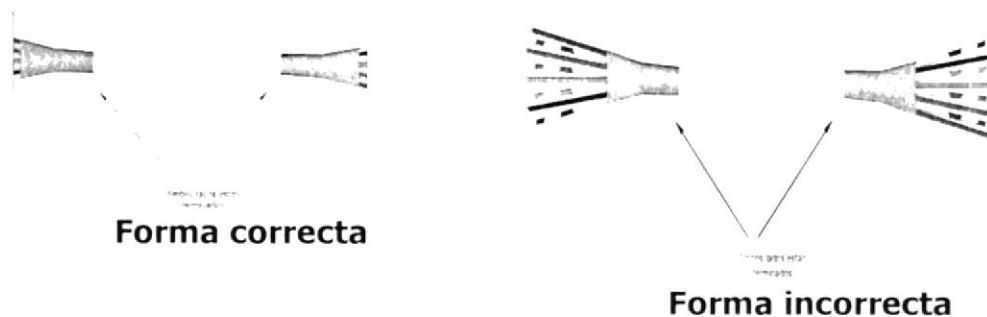


Figura 5-16: Normativa 15

▲ Normativa 16

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

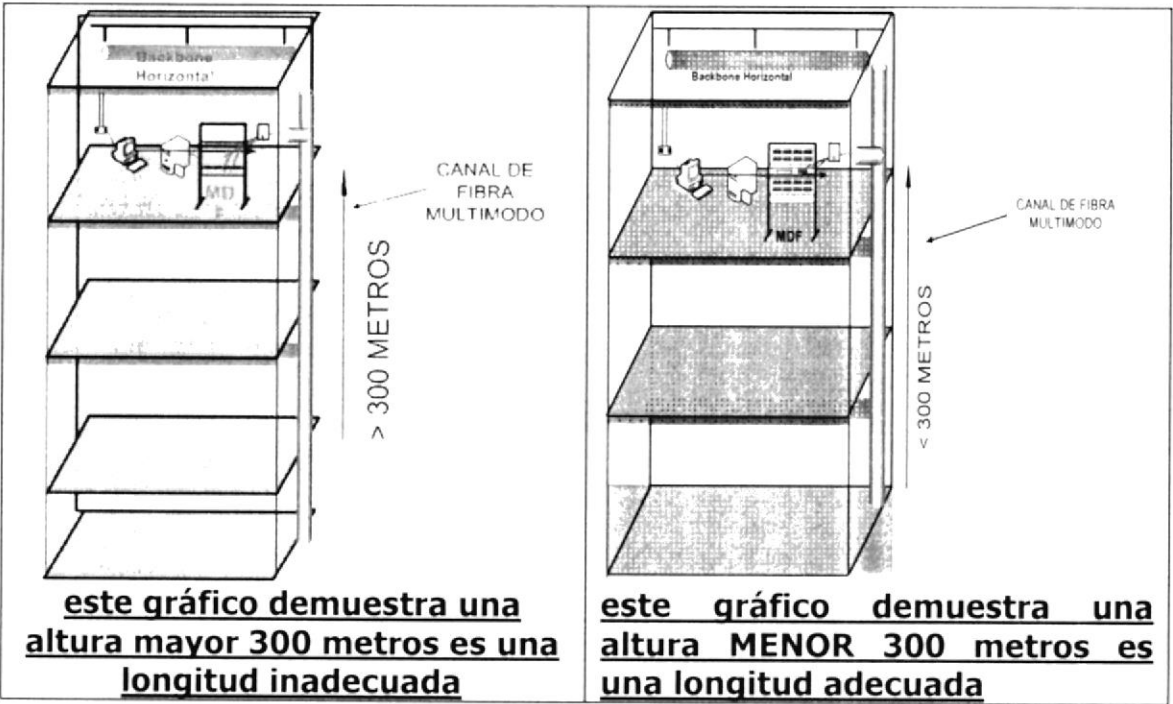


Figura 5-17: Normativa 16

▲ Normativa 17

La longitud del cableado de fibra óptica multimodo entre HC y la salida de telecomunicación no excede los 90mt.

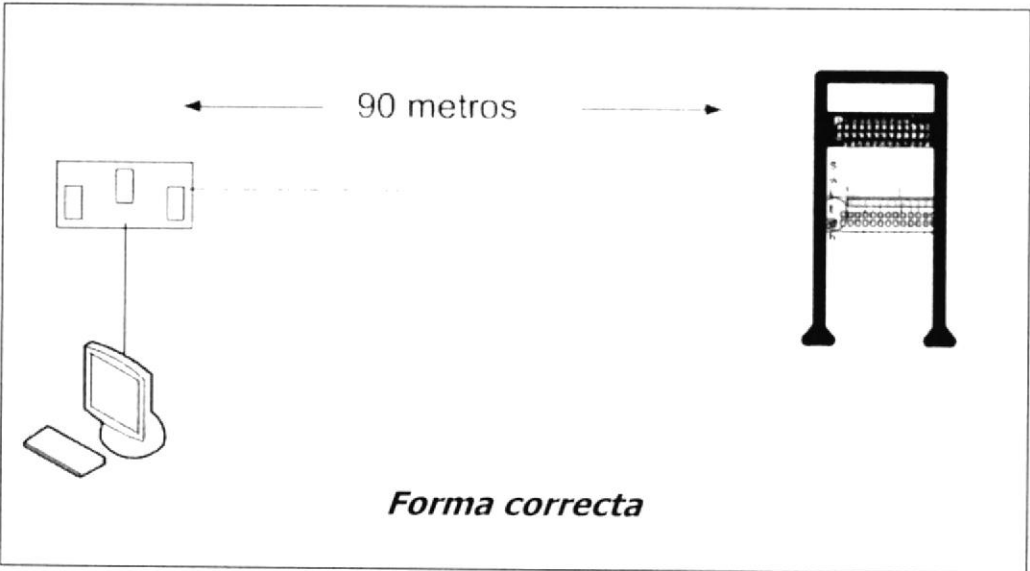
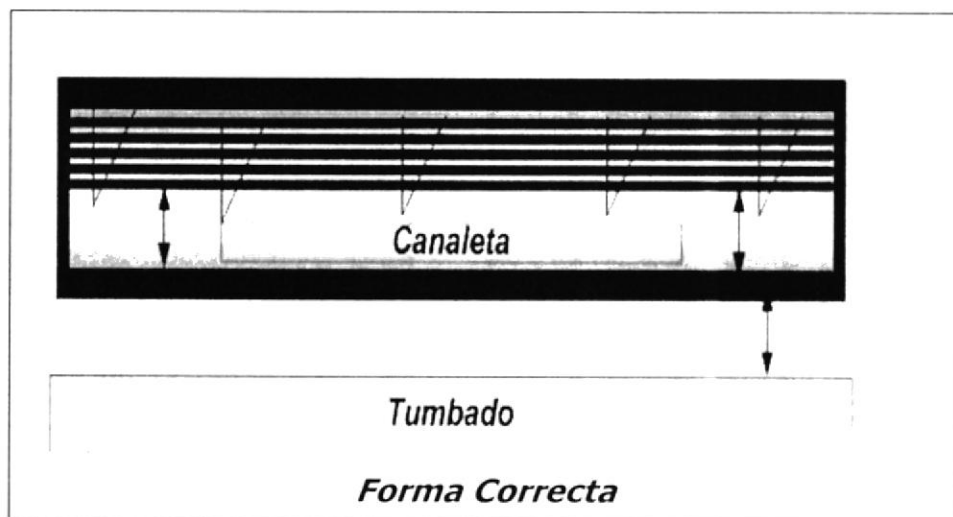


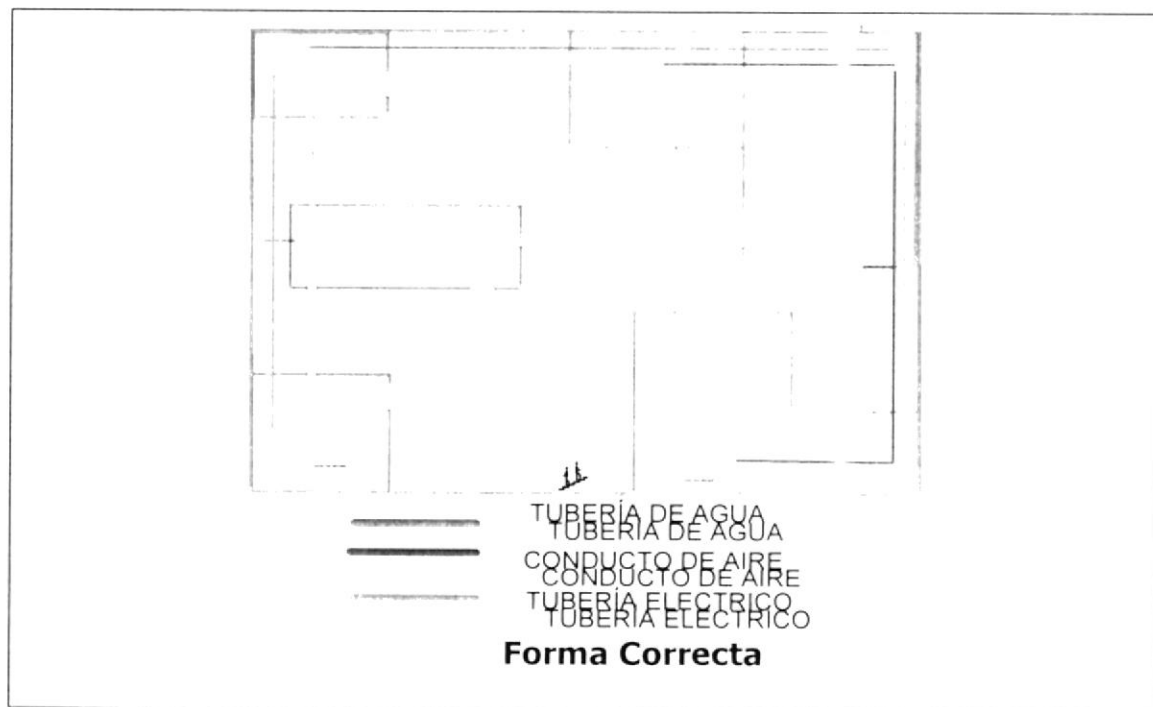
Figura 5-18: Normativa 17

▲ Normativa 18

Las canalizaciones horizontales se diseñaran e instalara para cumplir los reglamentos eléctricos y de construcciones locales y nacionales y normas aplicables

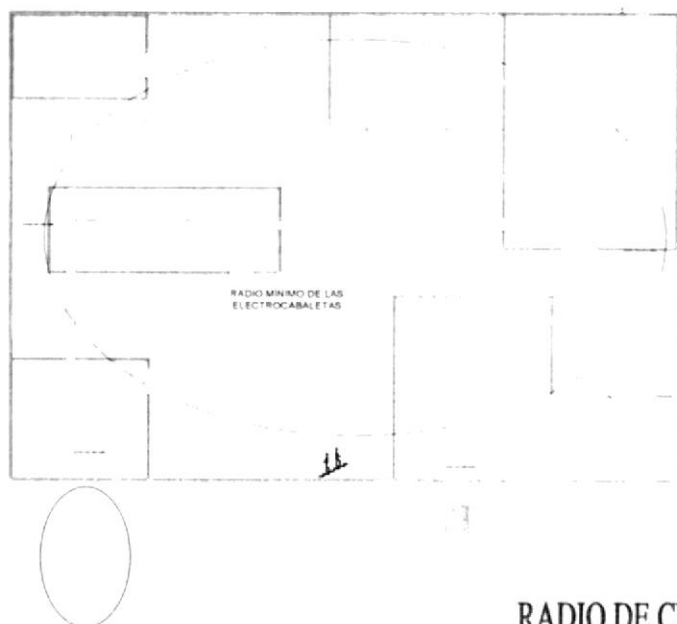
**Figura 5-19: Normativa 18****▲ Normativa 19**

Las canalizaciones horizontales serán apropiados para el ambiente en el cual se instalara y no se obstaculizara por conductos de aires, ventilación y airé acondicionado distribución eléctrico o estructura del edificio

**Figura 5-20 Normativa 19**

▲ **Normativa 20**

Las canalización horizontal deberán mantener un radio min. De curvatura de cables horizontal según la especificación del fabricante



RADIO DE CURVATURA
Figura 5-21: Normativ 20

▲ **Normativa 21**

Todas las canalización instaladas serán accesible con el fin de ejecutar adiciones, cambios, retiros de cables .las canalización cerradas tendrán puntos de acceso de una distancia 30mts.



Forma Correcta
Figura 5-22: Normativa 21

▲ **Normativa 22**

El backbone vertical deberá usar topología estrella jerárquica desde el MC hasta IC

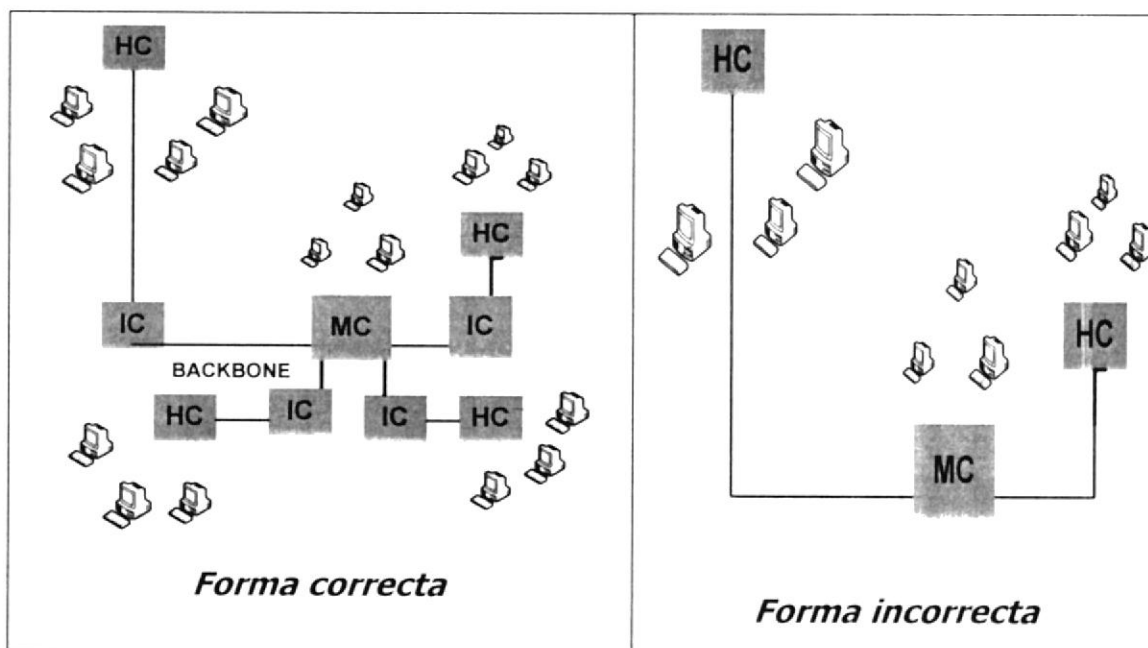


Figura 5-23: Normativa 22

▲ **Normativa 23**

Para cada tendido del backbone del edificio que sea mayor de 90mts. De longitud deberá proveer de cable de fibra óptica

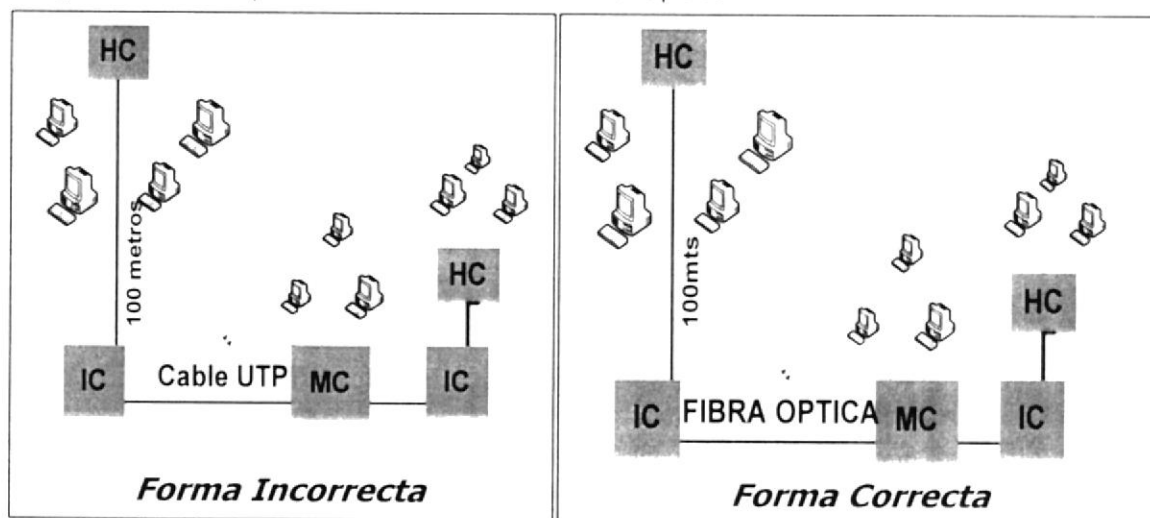


Figura 5-24: Normativa 23

**Normativa 24**

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

3000mts. Para Fibra Óptica monomodo

2000mts. Para Fibra Óptica multimodo

2000mts. Para par trenzado con aplicación PBX

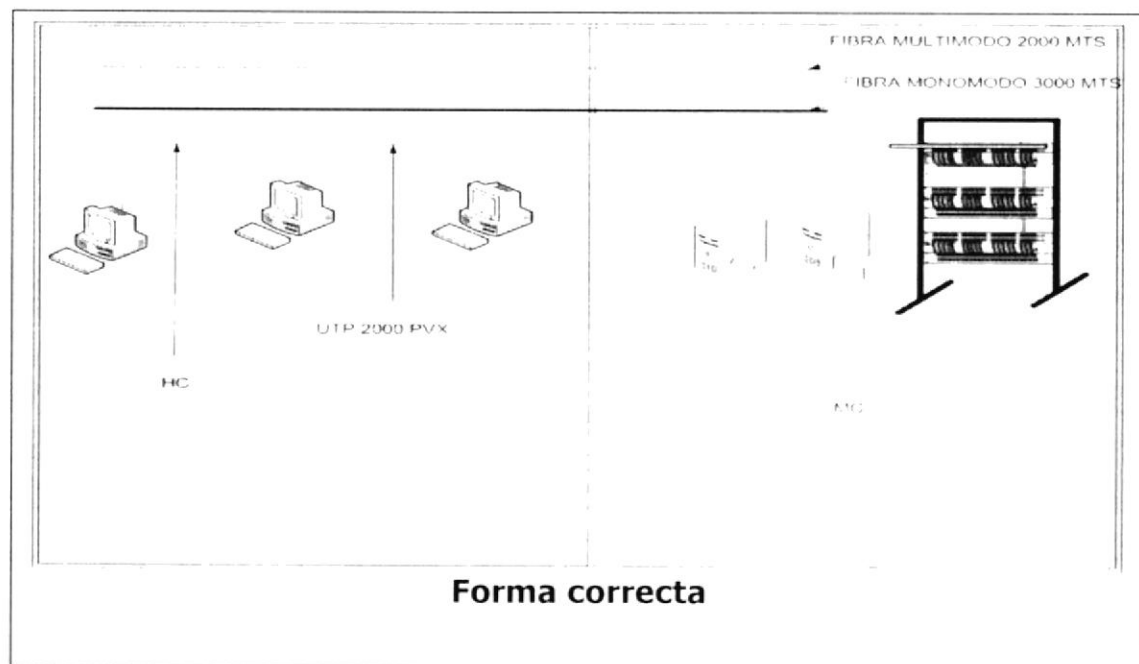


Figura 5-25: Normativa 24

Nota 1

Si el backbone de par trenzado balanceado sobrepasa los 100mts. Su uso se restringe solo para soportar aplicaciones de voz

▲ Normativa 25

Las canalizaciones del edificio proveerán acceso a todos los cuartos de comunicación, cuartos de equipos y/o acometidos localizadas en el mismo edificio

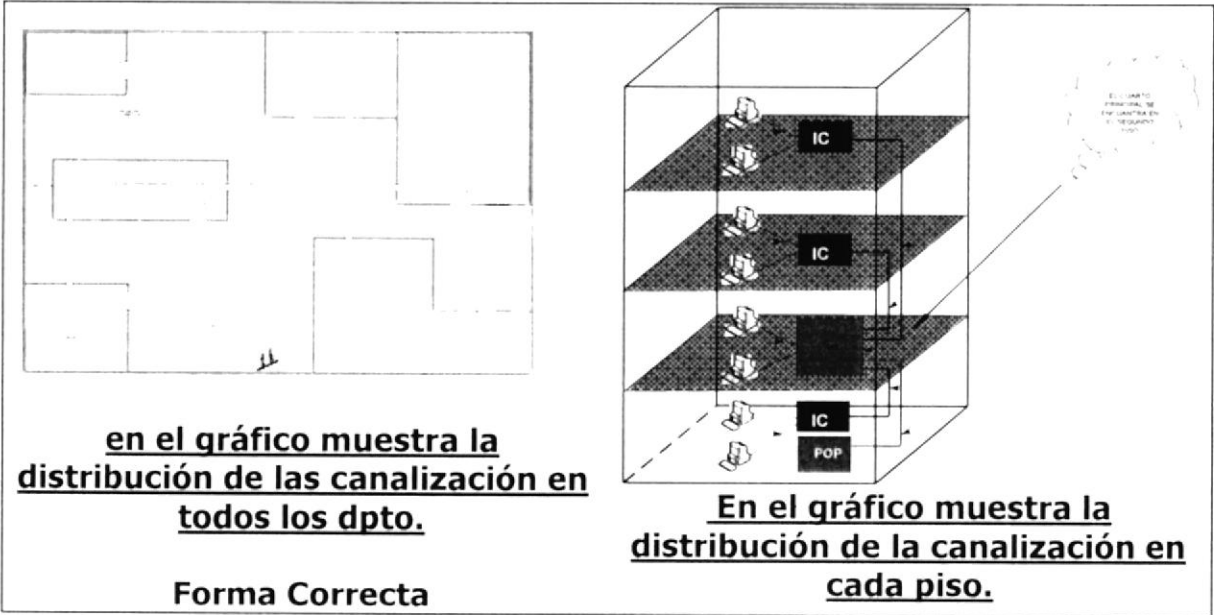


Figura 5-26: Normativa 25

▲ Normativa 26

La canalización no se ubicara en ductos de ascensores

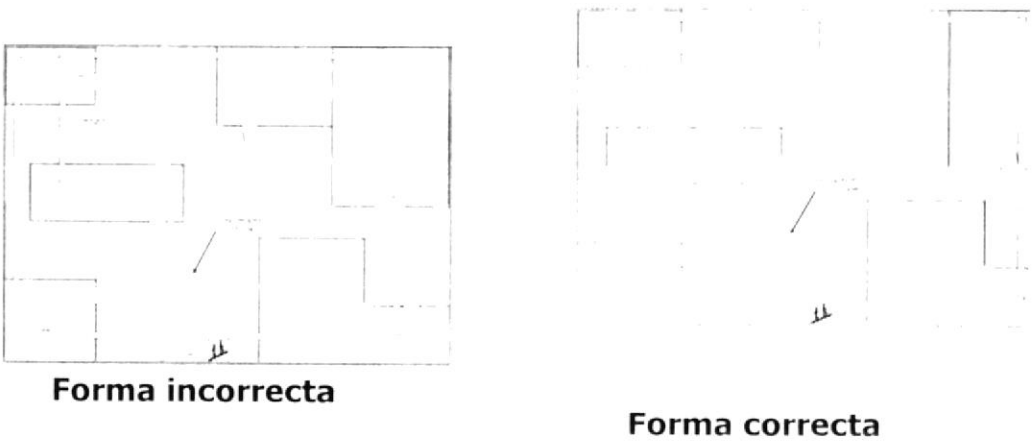


Figura 5-27: Normativa 26

▲ Normativa 27

El cable que corre entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará puesto el área de trabajo u otros espacios con público



Figura 5-28: Normativa 27

▲ Normativa 28

El cuarto de telecomunicaciones se diseñara y equipara el cuarto para contener equipos de telecomunicación terminaciones de cables y asociados.

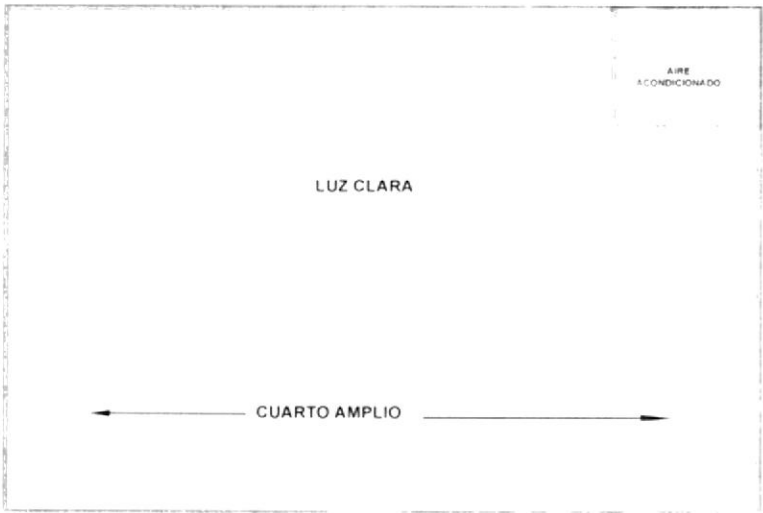


Figura 5-29: Normativa 28

▲ **Normativa 29**

El acceso a los cuartos de telecomunicación se restringirá al personal de servicio autorizado y no será compartido por servicios del edificio que puedan interferir con los sistemas de telecomunicación



Figura 5-30: Normativa 29

▲ **Normativa 30**

Las instalación separación de hilos a tierra, cumplirán las normas y reglas aplicables.

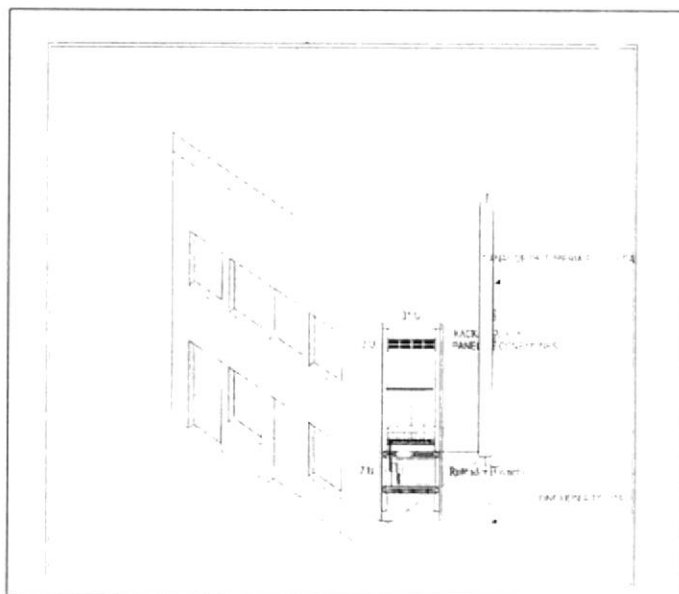


Figura 5-31: Normativa 30

▲ Normativa 31

Los gabinetes usados como espacio alternativos cumplirán los requisitos de telecomunicación que tendrán una puerta con cerradura y se montara en una ubicación fija



Figura 5-32: Normativa 31

▲ Normativa 32

El cuarto de equipo no será compartido con servicio del edificio que pueda interferir la telecomunicación o se utiliza mantenimiento del edificio

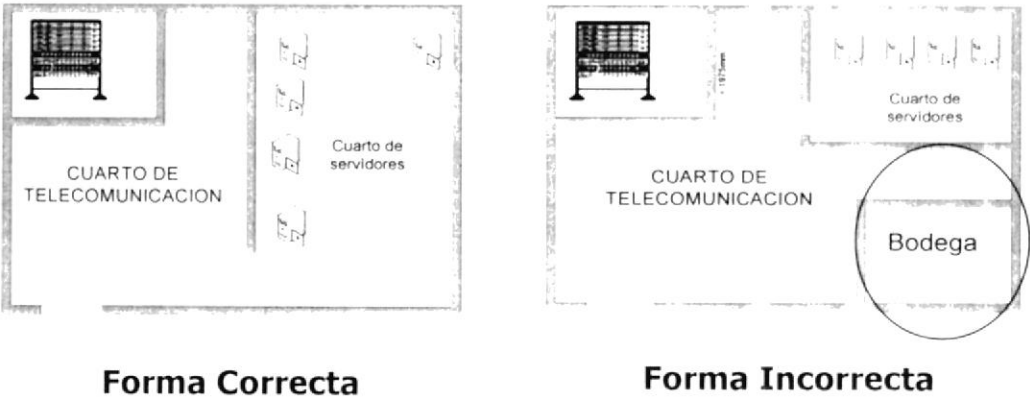


Figura:5-33: Normativa 32

▲ **Normativa 33**

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

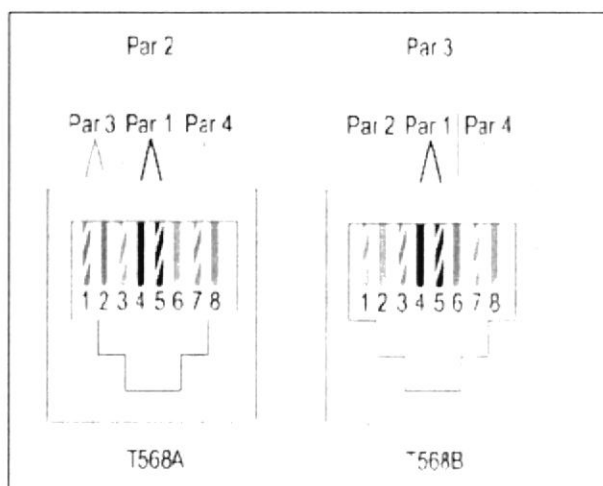


Figura 5-34: Normativa 33

▲ **Normativa 34**

La instalación del gabinete en el rack deberá proporcionar la separación instalada en las normas y reglas necesaria

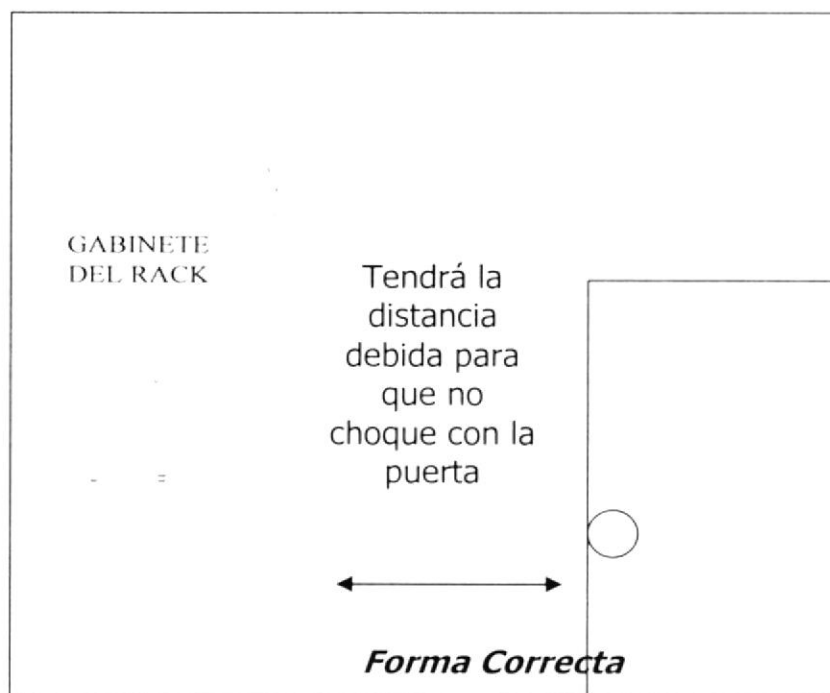


Figura 5-35: Normativa 34

▲ **Normativa 35**

Los cables de telecomunicación soportaran dispositivos diseñados para este equipo y en forma independiente a cualquier otra estructura.

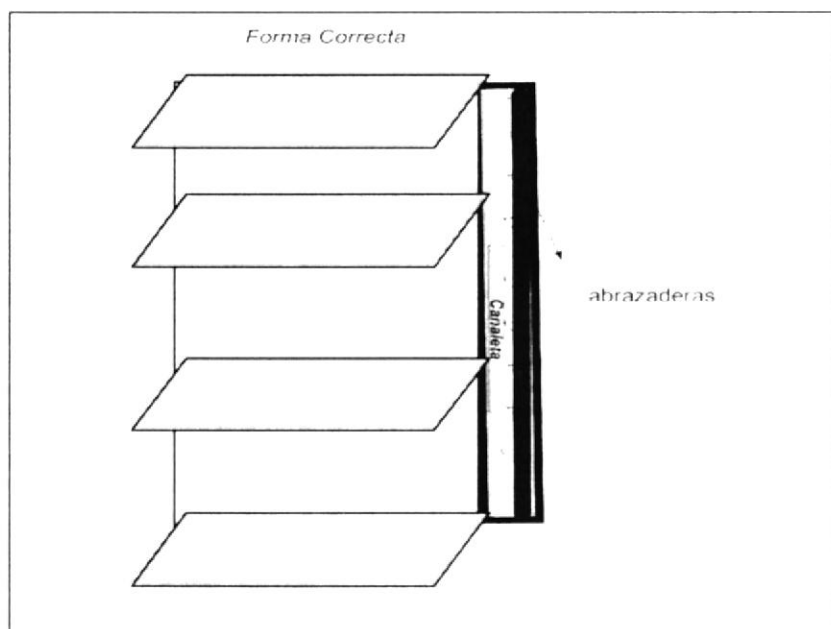


Figura 5-36 : Normativa 35

▲ **Normativa 36**

Los cables enrutados verticalmente, como en el caso del cable backbone horizontal enrutados entre piso, se soportaran con abrazadera u otro mecanismo requiera un min. De 2 soportes por piso.



Figura 5-37: Normativa 36

▲ **Normativa 37**

Los números de cables horizontales (par trenzado balanceado cable fibra óptica) colocado en un soporte de canalización, se limitará a una cantidad que no altere de forma genética el cable.

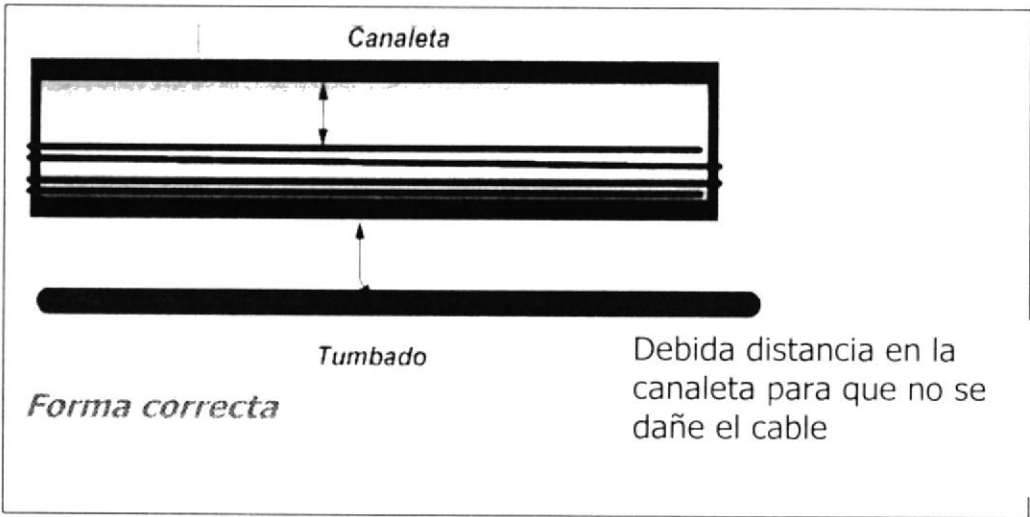


Figura 5-38: Normativa 37

▲ **Normativa 38**

La canalización de tipo bandeja o canal no excederá una capacidad máx. 50% de llenado y una altura máxima de interior de 6 pulgadas

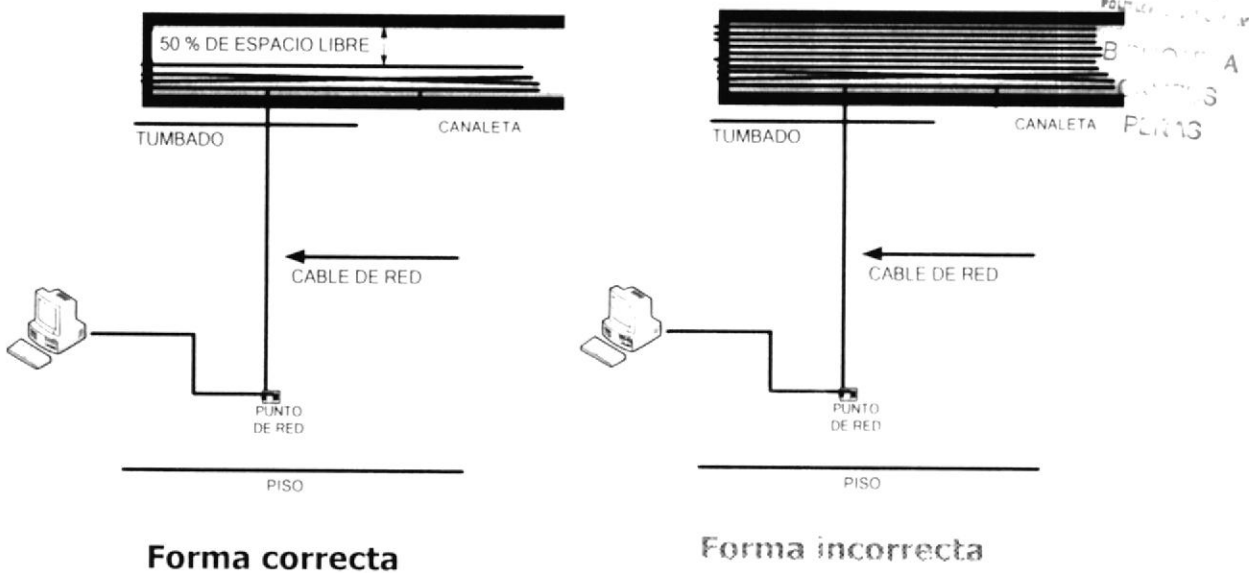


Figura 5-39: Normativa 38

▲ **Normativa 39**

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

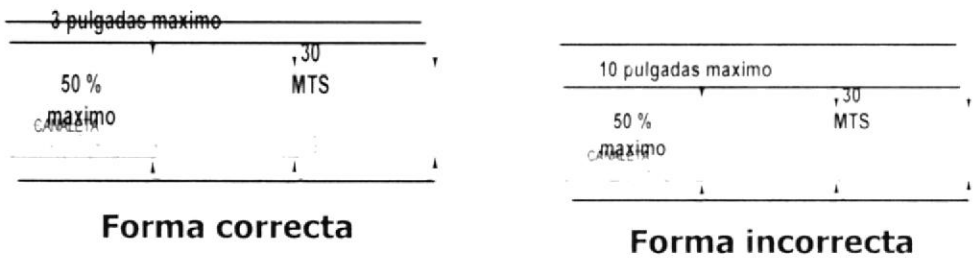


Figura 5-40: Normativa 39

▲ **Normativa 40**

Las tensiones máximas del jalado del cable con radio mínimo de curvatura no sobrepasan las especificaciones del fabricante.

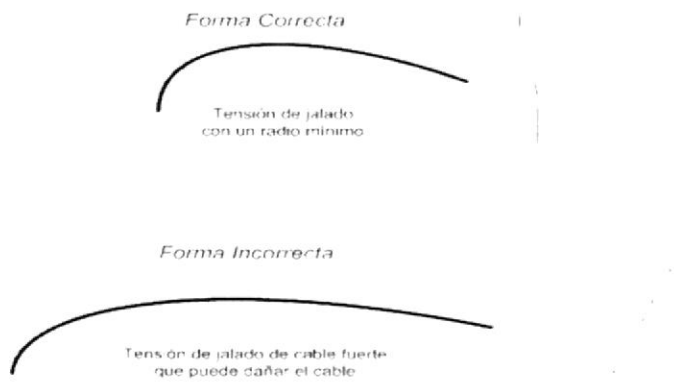


Figura 5-41: Normativa 40

**Normativa 41**

No se permitirá el engrapado de ningún tipo de cable reconocido



Figura 5-42: Normativa 41

**Normativa 42**

Los cables se instalarán en canalizaciones y espacios que rinde protección adecuada contra la intemperie y demás riesgo del entorno

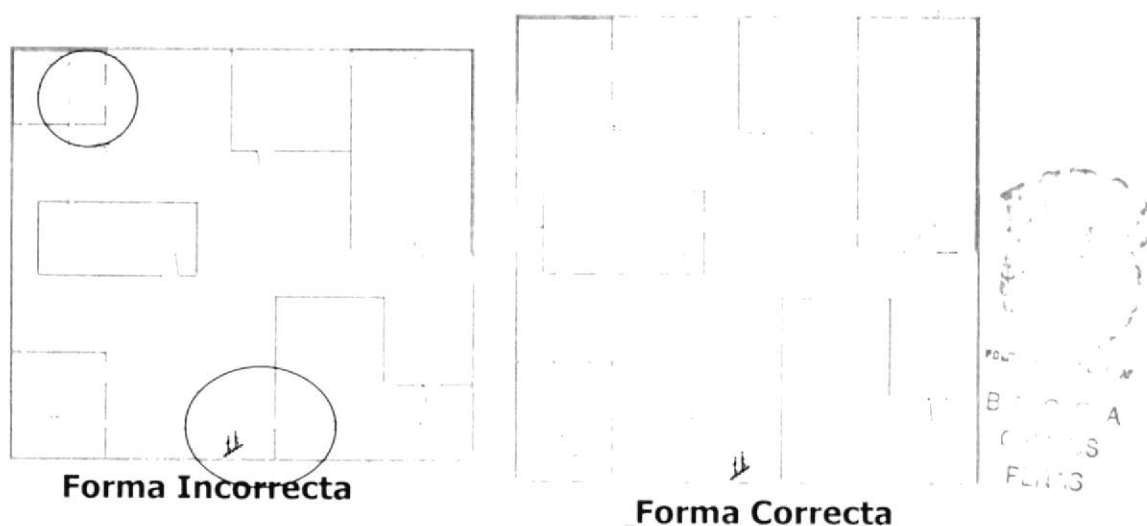


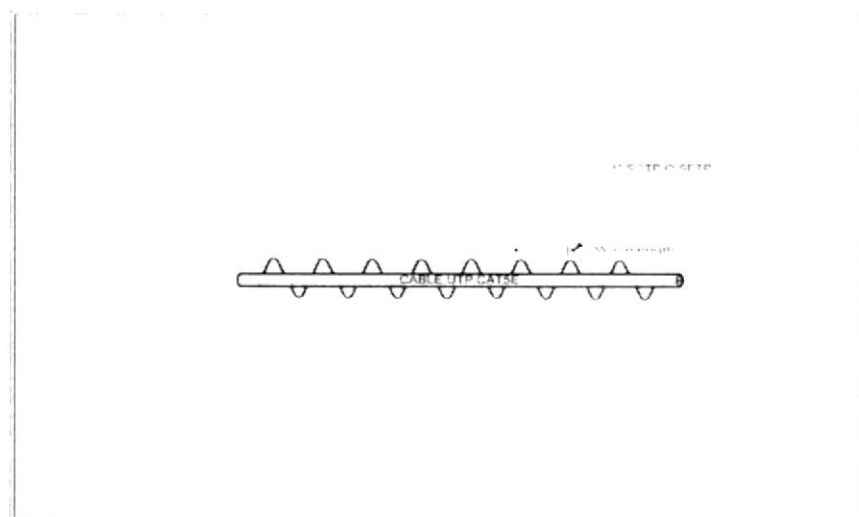
Figura 5-43: Normativa 42

**Normativa 43**

El radio min. De curvatura, en condiciones de no tensión (cuando el cable es solo colocado no alojado) será de:

1" para SCPP o SFTP de diámetro < igual 6 milímetro

2" para SCPP o SFTP de diámetro >6 milímetro (0.25")

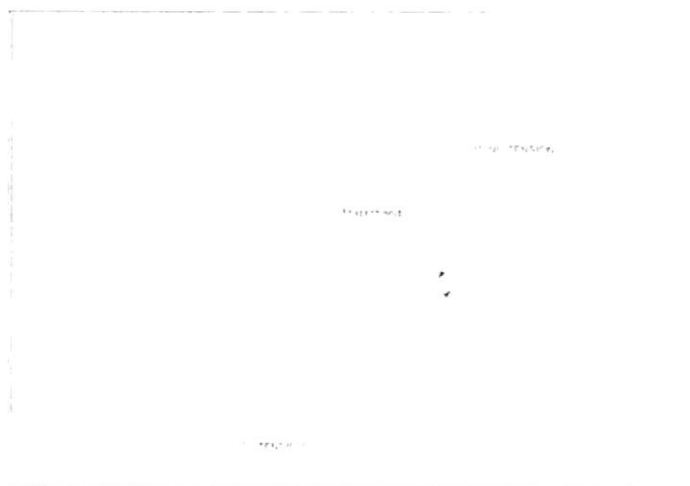


Forma correcta

Figura 5-44: Normativa 43

**Normativa 44**

El radio min. de curvatura para cable horizontal de 2 y 4 fibras será de 1" bajo condición de no tensión y de 2" bajo condiciones de tensión; la tensión máx. de jalado permitida será de 222N ("Niutom" (libras fuerzas))



Forma correcta

Figura 5-45: Normativa 44

▲ **Normativa 45**

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

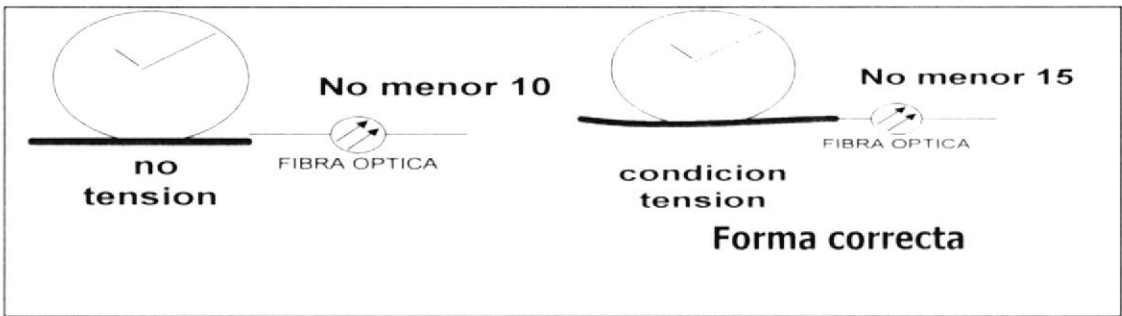


Figura 5-46: Normativa 45

▲ **Normativa 46**

El radio de curvatura para cable backbone de fibra externo no será < 10 a veces el diámetro externo del cable bajo condiciones a no tensión, y no < a 20 veces el diámetro de cable extremo bajo condición de tensión, en donde la tensión del cable extendida será < 2670 N (600` libras de fuerza).

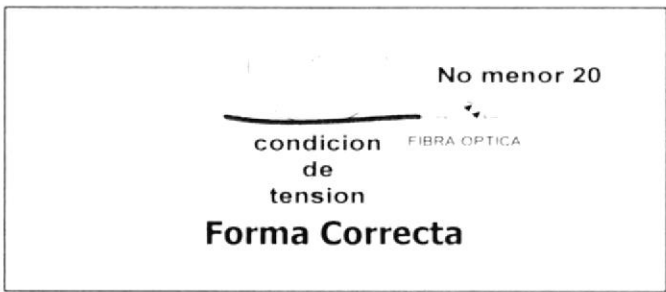


Figura 5-47: Normativa 46

▲ **Normativa 47**

El cable que corra entre el cuarto de telecomunicación y salida de telecomunicación, no estará expuesto en el área de trabajo u otro espacio acceso al publico

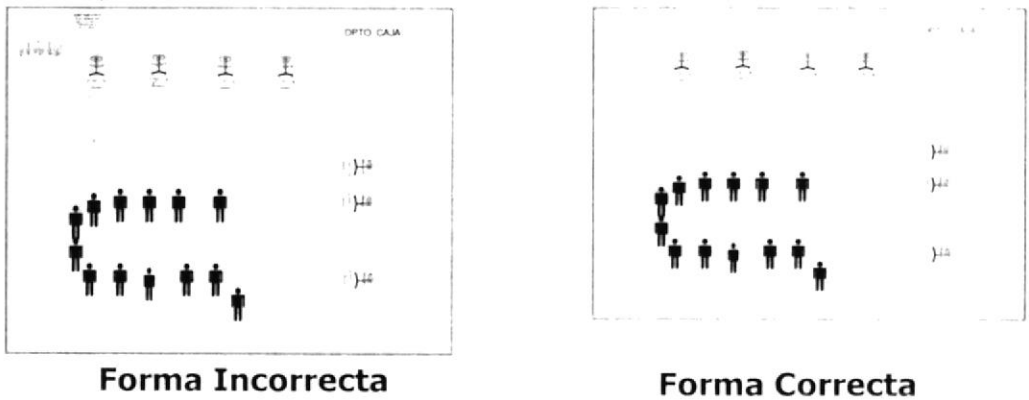


Figura 5-48: Normativa 47

▲ Normativa 48

El hardware de conexión se instalará de una manera que evite un control de cables ordenados y bien organizados

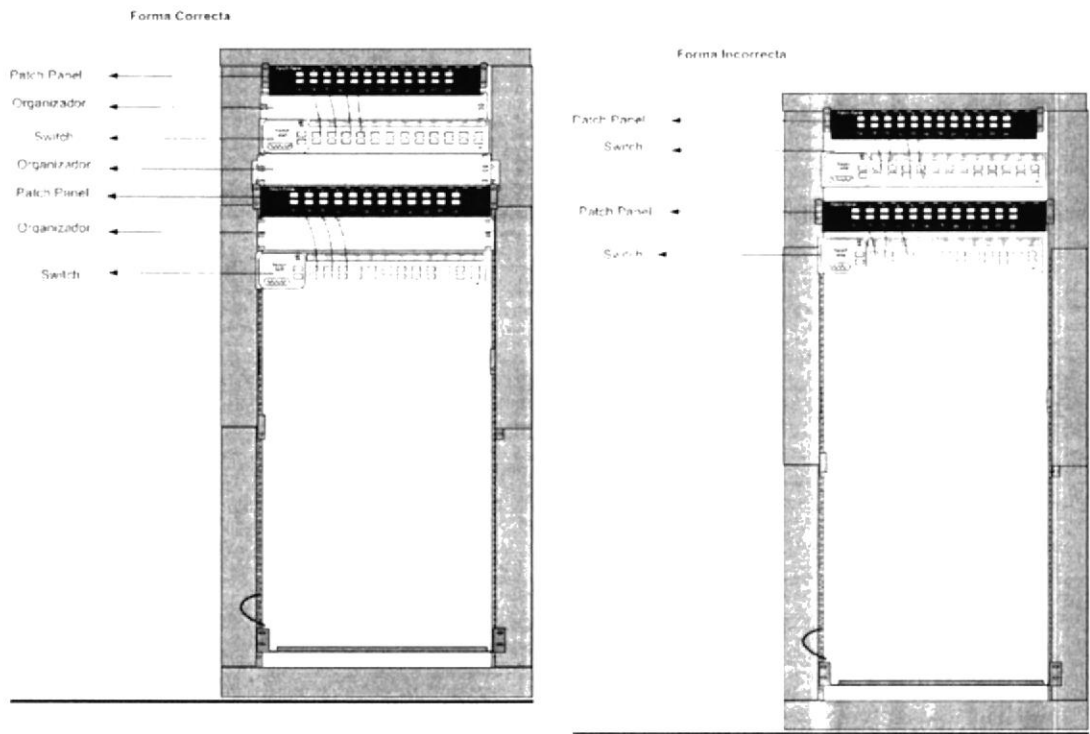


Figura 5-49: Normativa 48

▲ Normativa 49

Con el fin de reducir el desentrenado de par trenzado instalador debe de pelar cantidad de forros que se requiera para determinar el hardware de comunicación

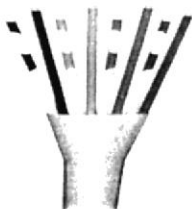


Figura 5-50: Normativa 49

▲ Normativa 50

La cantidad máx. del desentrenado de cada par trenzado, resultante de comunicación del hardware de conexión, será de 13 milímetro, para cable de categoría 5e o > y de 75 milímetro para cables de cat 3

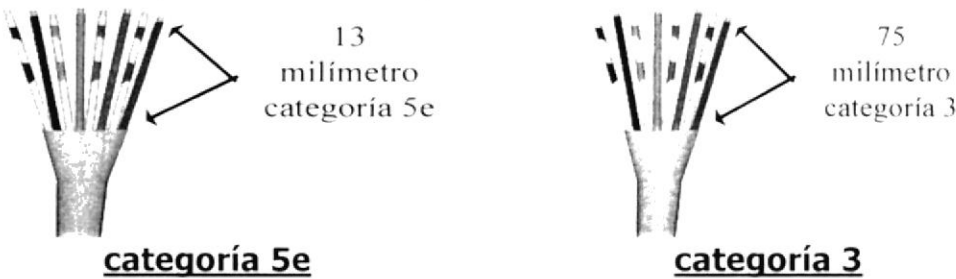
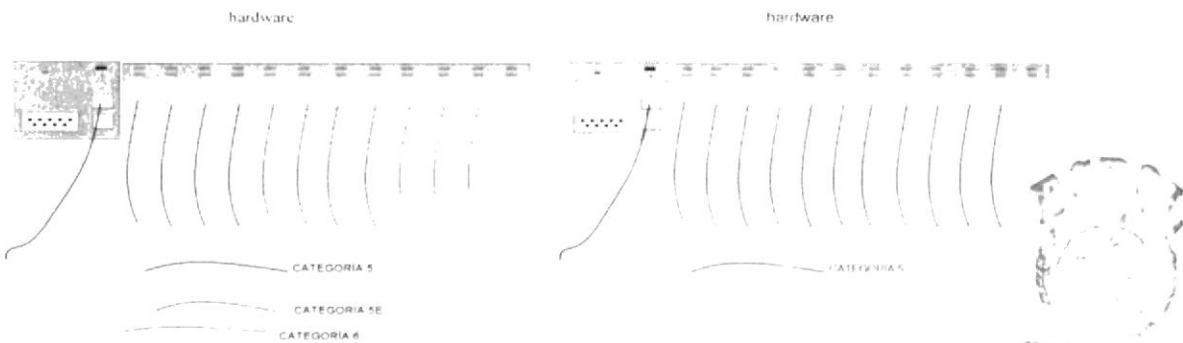


Figura 5-51: Normativa 50

▲ Normativa 51

No se deberá terminar cables de diferente categoría de desempeño en el mismo hardware de telecomunicación



Forma incorrecta

Forma correcta

Figura 5-52: Normativa 51

▲ Normativa 52

Los identificadores que se utiliza para acceder a grupos de registro del mismo equipo deben ser únicos

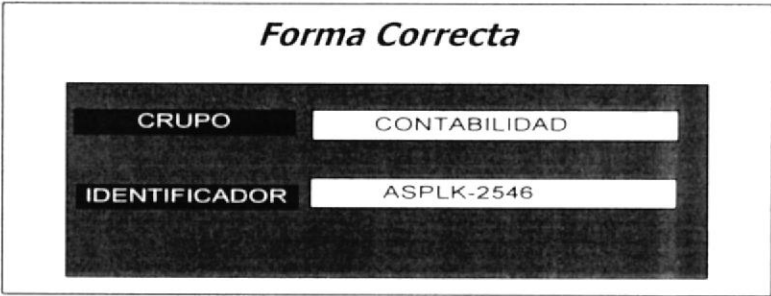


Figura 5-53: Normativa 52

▲ Normativa 53

El rotulado se deberá realizar ya sea pegando o colocando firmemente una etiqueta independiente al elemento que se va a registrar o marcando el elemento directamente.

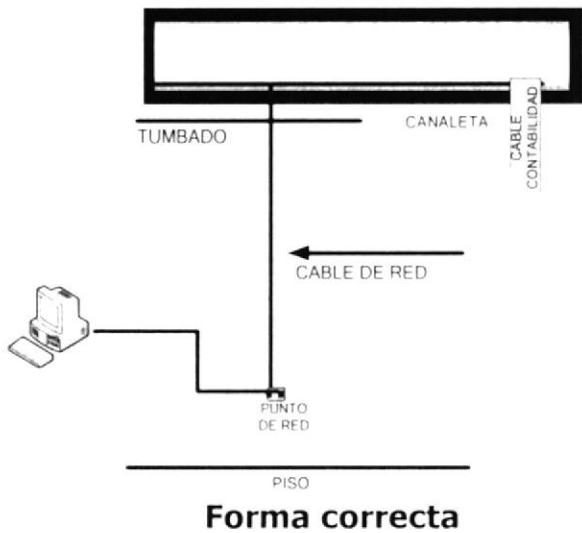


Figura 5-54: Normativa 53

▲ Normativa 54

El rotulado deberá ser legible y permanecer firmemente unido al elemento durante el periodo de garantía (5 años de garantía según el fabricante)

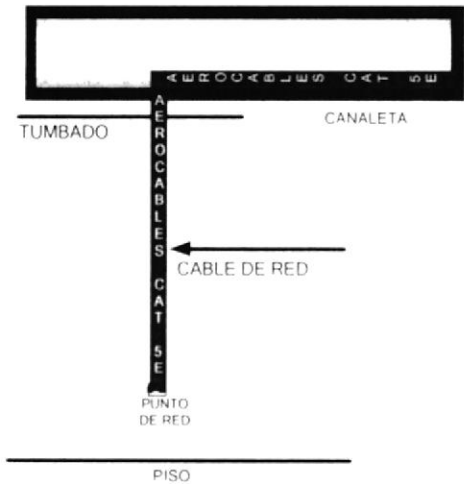


Figura 5-55: Normativa 54

▲ **Normativa 55**

A cada cable se asignara un identificador único que sirva referencia a su respetivo ejemplo

Descripción	Identificador
Cable numero 9 de fibra óptica monomodo	FOM009
Cable numero 5 UTP cat 5E	C5005

Tabla 5-1: Identificador de Cable 1
hardware

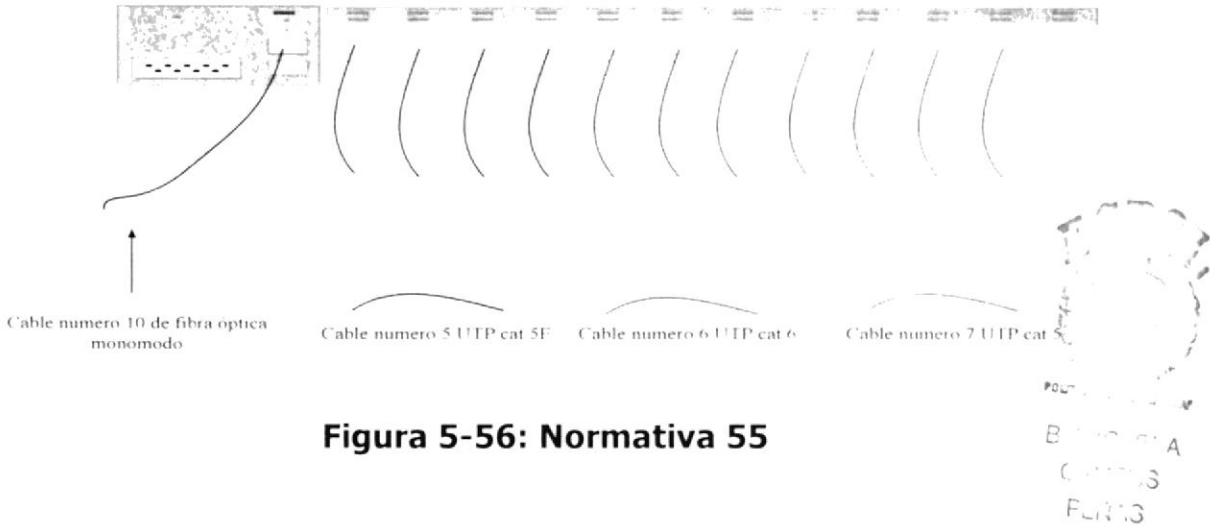


Figura 5-56: Normativa 55

Descripción	Identificador
Cable numero 10 de fibra óptica monomodo	FOM009
Cable numero 5 UTP cat 5E	C5005E
Cable numero 6 UTP cat 6	C6006
Cable numero 7 UTP cat 5	C7005

Tabla 5-2: Identificador de cable 2

▲ **Normativa 56**

Los cables de subsistema horizontal y backbone deberán rotularse en cada extremo, la etiqueta puede ser colocada a 30cm del cable, esta marca deberá permanecer en el cable después de terminar la instalación

Forma Correcta

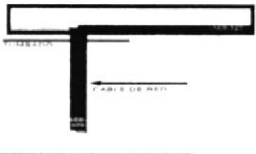


Figura 5-57: Normativa 56

5.3 RECOMENDACIONES



Recomendación 1

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

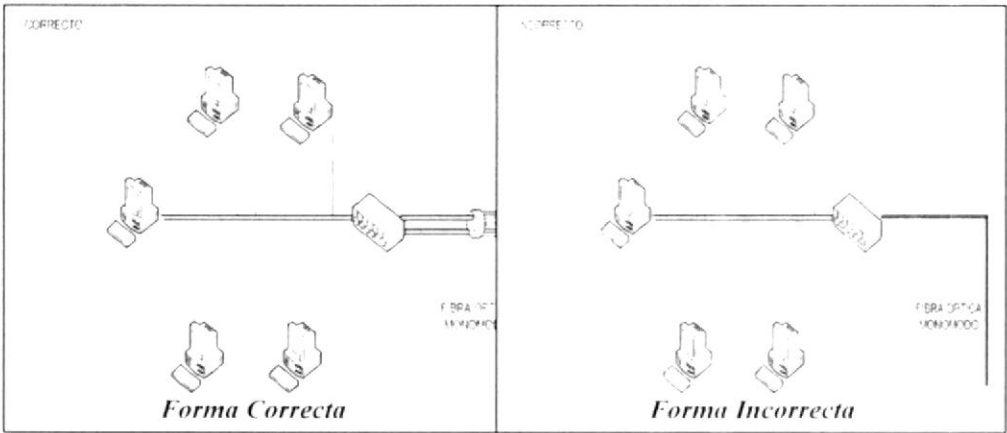


Figura 5-58: Recomendación 1



Recomendación 2

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

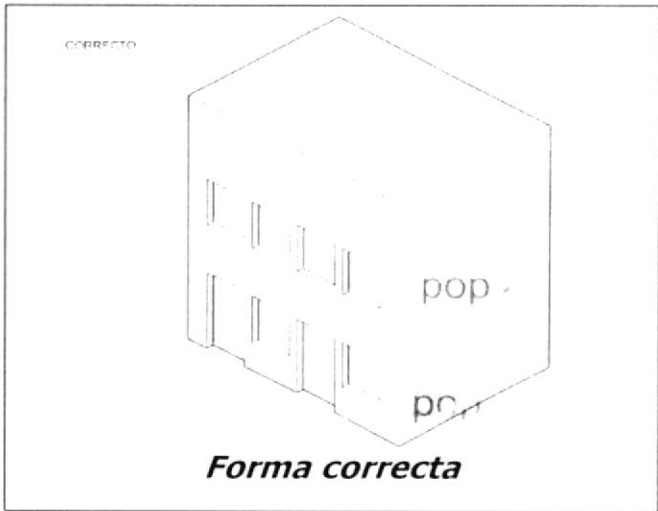


Figura 5-59: Recomendación 2



Recomendación 3

El área que puede atenderse efectivamente por un cuarto de telecomunicación abarca un radio máximo de 60mt.

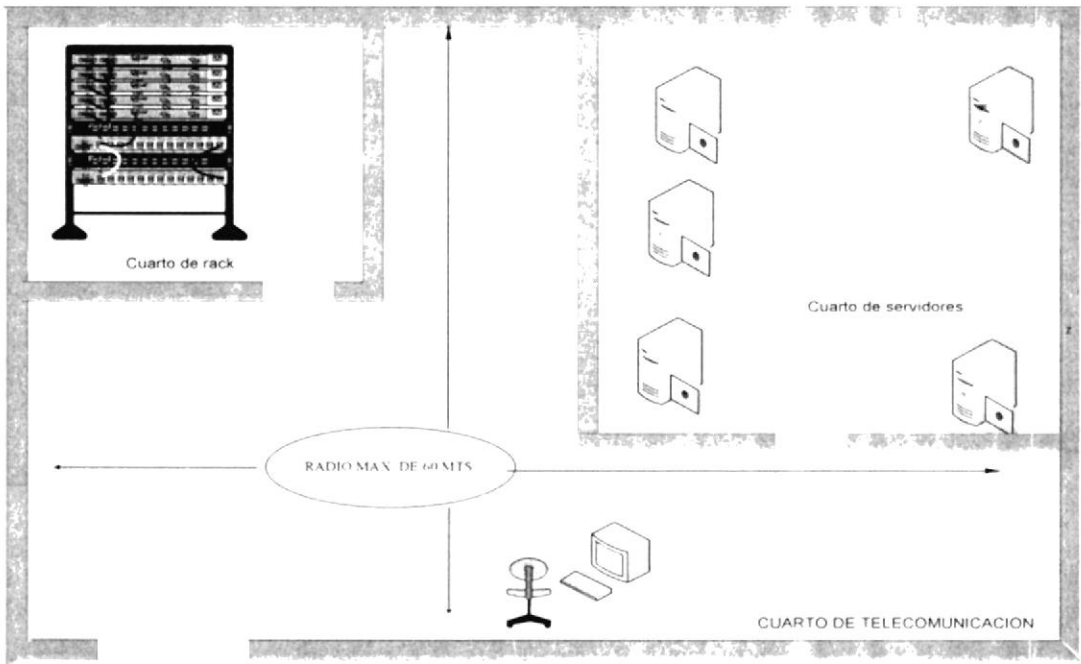


Figura 5-60: Recomendación 3



Recomendación 4

Se recomienda un min. De 15mt. Entre el H.C. y la salida de telecomunicación

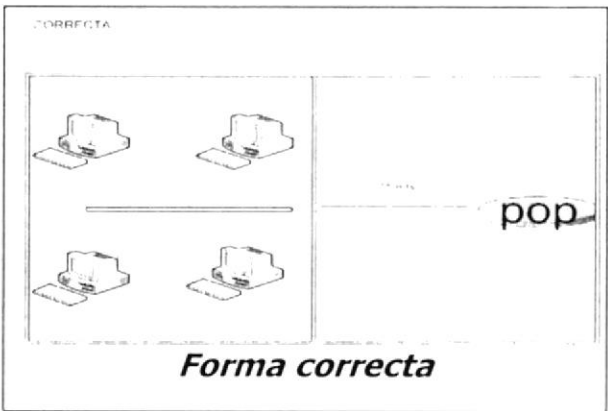
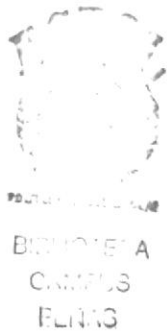


Figura 5-61: Recomendación 4



**Recomendación 5**

Se recomienda un min. De 2 salida de cat. 6 por cada área de trabajo individual con el fin de soportar, numerosas aplicaciones diseñados para operar sobre el cableado de par trenzado

CABLE HORIZONTAL

5 U

FORMA
CORRECTA

2 SALIDAS DE CAT 6

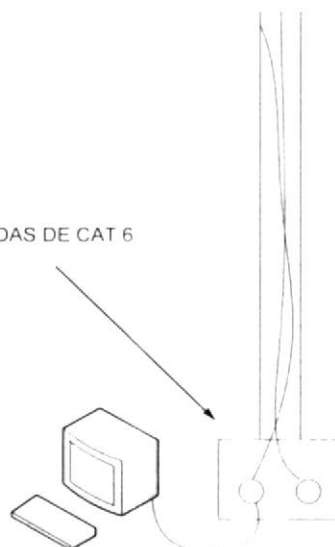


Figura 5-62: Recomendación 5

**Recomendación 6**

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

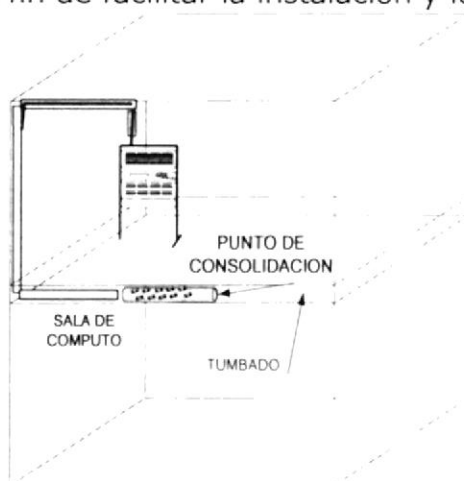
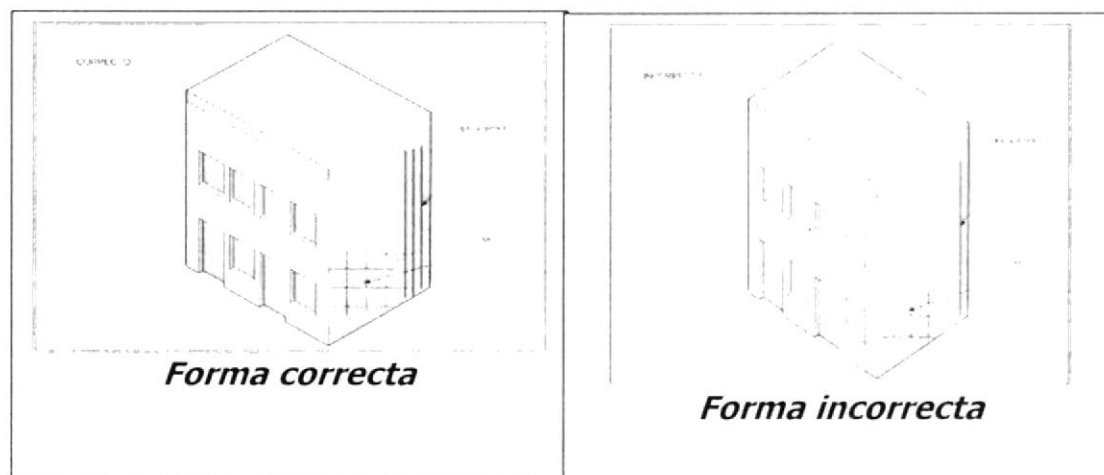


Figura 5-63: Recomendación 6

**Recomendación 7**

El cableado de backbone de edificio debe diseñarse con la capacidad de reservas suficientes para tener salidas adicionales de telecomunicación desde el MC

**Figura 5-64: Recomendación 7****Recomendación 8**

El radio de cobertura interior mín. De la canalización horizontal no debe ser inferior a 10 veces del mayor diámetro de los cables a instalarse

**Figura 5-65: Recomendación 8**

BIBLIOTECA
CAMPUS
PEÑAS



Recomendación 9

Ningún Segmento De Canalización contendrá más de 2 curvas de 90 o entre puntos de acceso

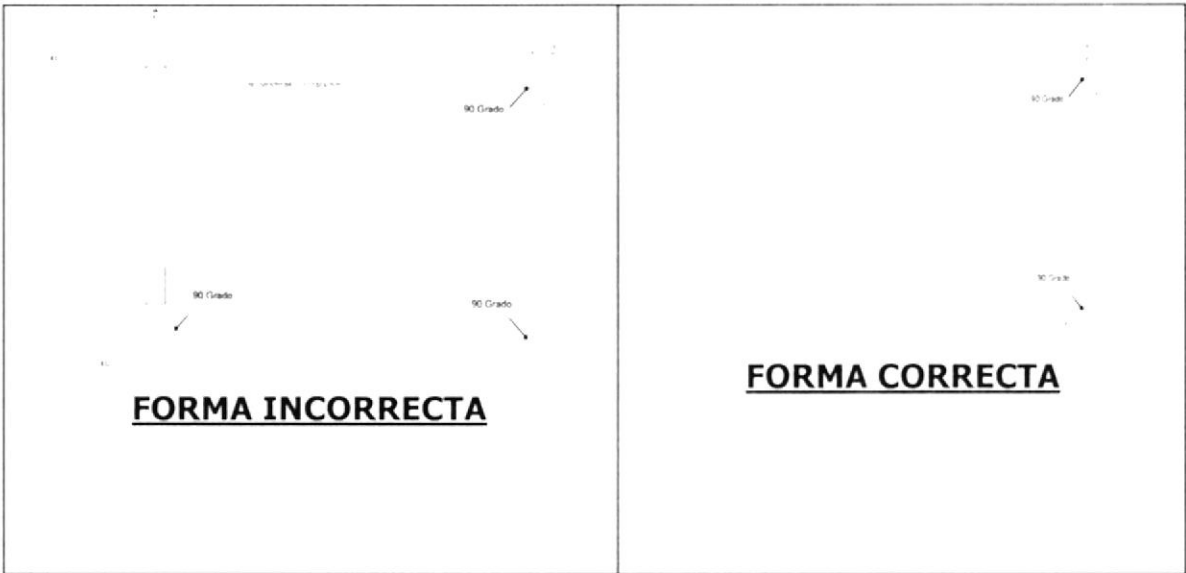


Figura 5-66: Recomendación 9



Recomendación 10

Se recomienda que se proveer como min. 2 hilos de fibra óptica por cada aplicación conocida durante su periodo de planificación debe proveerse de una aplicación de 100%

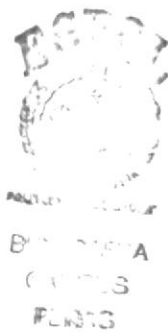
Voz	2	2 hilos para voz de datos
Video	2	Mínimo fibra de 12 hilos
Lan	2	Desde un mismo cable utp de 8 hilos sacar 2 conectores
Crecimiento	6	Cable utp <90mts; >90 fibra óptica
TOTAL	12	

Tabla 5-3: Recomendación Fibra Optica



FORMA CORRECTA

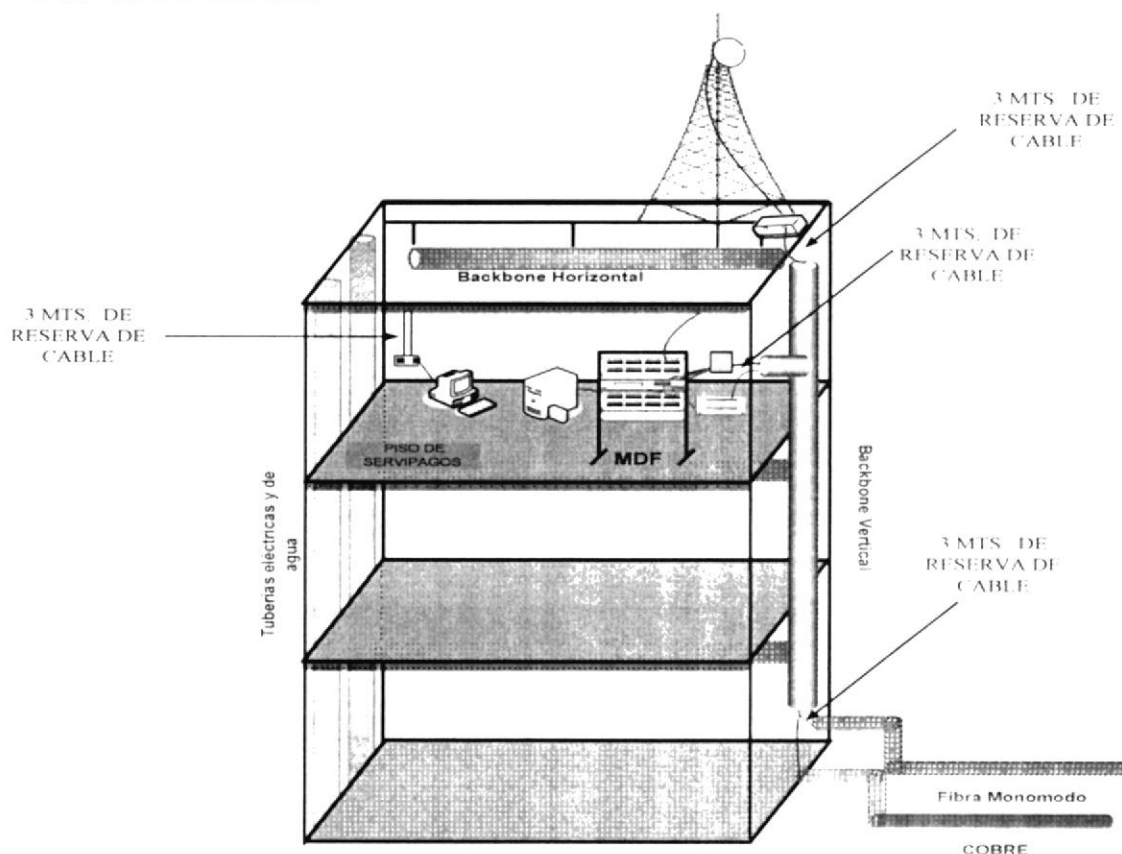
Figura 5-67: Recomendación 10





Recomendación 11

Para cables backbone se recomienda un mínimo de 3mts. De reserva de cable en cada lado o extremo



FORMA CORRECTA

Figura 5-68: Recomendación 11



Recomendación 12

Los acabados en el cuarto de telecomunicación debe ser de color claro para mejorar la iluminación del mismo



FORMA CORRECTA

Figura 5-69: Recomendación 12



Recomendación 13

Cuando sea factible, en un edificio de varios pisos, se recomienda que el cuarto de quipo se localice en el piso de medio y una ubicación que facilite el acceso a canalización de los cuartos de telecomunicación de otro piso

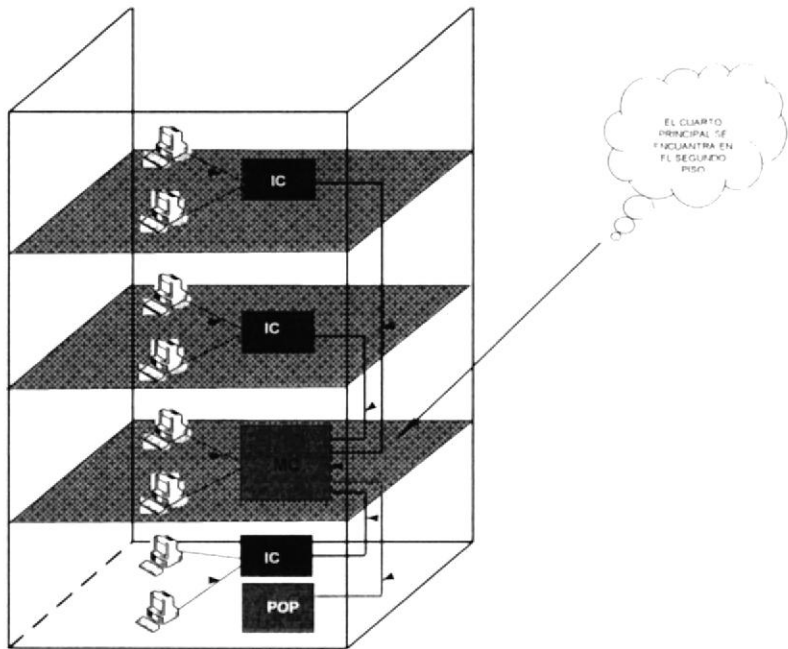


Figura 5-70: Recomendación 13



Recomendación 14

Se recomienda que el cuarto de equipos se ubique por encima del Nivel De Inundación y este protegido con filtraciones de tuberías

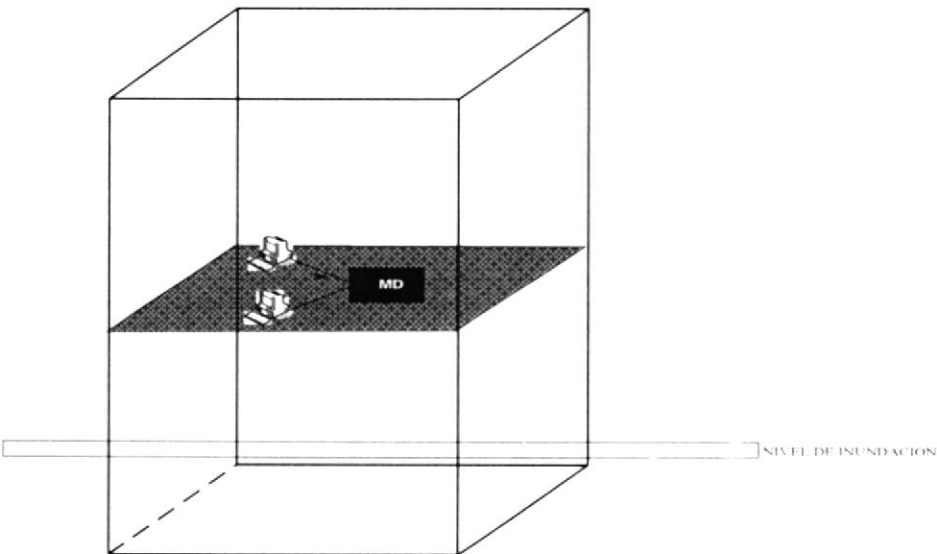


Figura 5-71: Recomendación 14



CAPÍTULO 6

LINUX

6. LINUX

6.1 INTRODUCCIÓN DE LINUX

Linux es el núcleo de sistema operativo libre más popular y constituye la base del sistema operativo Linux (también llamado GNU/Linux), que ha comenzado a competir con sistemas operativos no libres como Unix y Windows.

El núcleo Linux, escrito casi completamente en C con algunas extensiones GNU C, fue desarrollado por el hacker finlandés Linus Torvalds en un intento por obtener un sistema operativo libre similar a Unix que funcionará con microprocesadores Intel 80386. El proyecto nació en 1991 con un famoso mensaje en el grupo comp.os.minix de Usenet, que contenía lo siguiente:

Muy pronto, los hackers de Minix aportaron ideas y código al núcleo Linux, y hasta hoy ha recibido contribuciones de miles de programadores. Originalmente Linux era solamente el nombre del núcleo.

La mascota de Linux es un pingüino llamado Tux, creado por Larry Ewing.



Figura 6-1: Pinguino

Linux da una alternativa real a otros sistemas propietarios en muchos casos. Es un producto maduro que permite desplegar plataformas empresariales y entornos de trabajo de escritorio. Tiene software disponible para las tareas principales en un negocio, sea el proceso de textos u hojas de cálculo, sea la navegación por Internet, el diseño web, cubriendo así todas las necesidades. Se puede afirmar que hay paquetes de software para cubrir casi cualquier requisito.

Proyectos como Linex o Factura linux han dotado a Linux de herramientas para llevar a cabo las tareas empresariales, organizaciones como AENOR están certificando la compatibilidad con el hardware que Ud. adquiere, y finalmente, fabricantes como Red Hat o Suse ofertan soporte comercial a sus distribuciones.

Pero además, Linux es libre, y por tanto Ud. cuenta con múltiples elecciones... no solo el soporte de Red Hat o Suse, sino un soporte más directo de mano de Capa Tres Soluciones Tecnológicas o incluso mantener Ud. mismo su instalación. Linux le da el poder de escoger aquello que desee, le da la posibilidad de decidir. Y además por un coste de despliegue y compra varios órdenes de magnitud por debajo de Microsoft.

Olvide los problemas ya conocidos del mundo Windows (virus, incompatibilidades, el precio del producto y sus licencias, etc) Deje de pagar por los programas y sus actualizaciones, sumese al mundo del software libre

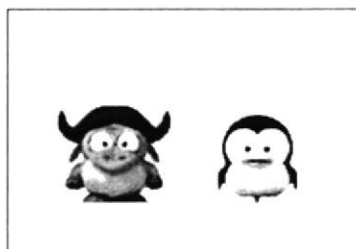


Figura 6-2: GNU/LINUX



6.2 COMPONENTES DE LINUX

Linux se puede dividir generalmente en cuatro componentes principales: el núcleo (kernel), el shell, el sistema de archivos y las utilidades.

El núcleo: es el programa modular que ejecuta programas y gestiona dispositivos de hardware tales como los discos y las impresoras.

El shell: proporciona una interfaz para el usuario. Recibe órdenes del usuario y las envía al núcleo para ser ejecutadas.

El sistema de archivos: organiza la forma en que se almacenan los archivos en dispositivos de almacenamiento tales como los discos. Los archivos están organizados en directorios. Cada directorio puede contener un número cualquiera de subdirectorios, cada uno de los cuales puede a su vez, contener otros archivos.

El núcleo, el shell y el sistema de archivos forman en conjunto la estructura básica del sistema operativo. Con estos tres elementos puede ejecutar programas, gestionar archivos e interactuar con el sistema. Además, Linux cuenta con unos programas de software llamados utilidades que han pasado a ser considerados como características estándar del sistema.

Las utilidades: son programas especializados, tales como editores, compiladores y programas de comunicaciones, que realizan operaciones de computación estándar. Incluso uno mismo puede crear sus propias utilidades.

Linux es Multitarea:

La multitarea no consiste en hacer que el procesador realice más de un trabajo al mismo tiempo (un solo procesador no tiene esa capacidad), lo único que realiza es presentar las tareas de forma intercalada para que se ejecuten varias simultáneamente. Por lo tanto, en Linux es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.

Linux es Multiusuario:

Para que pueda desarrollar esta labor (de compartir los recursos de un ordenador) es necesario un sistema operativo que permita a varios usuarios acceder al mismo tiempo a través de terminales, y que distribuya los recursos disponibles entre todos. Así mismo, el sistema debería proporcionar la posibilidad de que más de un usuario pudiera trabajar con la misma versión de un mismo programa al mismo tiempo, y actualizar inmediatamente cualquier cambio que se produjese en la base de datos, quedando reflejado para todos.

Pues bien, este sistema operativo no lo tiene que inventar puesto que ya está inventado. Pero no todo es tan bonito como se pinta ya que el hecho de que se conecten a tu ordenador más usuarios significa que es más difícil mantener tu seguridad.

Linux es multiplataforma

Es decir que puede correr en muchas CPU distintas (Intel, AMD, motorola, sun, sparc, etc.)

Linux es Seguro:

Linux se autoprotege; NO existen virus para Linux.

En la estructura de Linux aparecen cuatro elementos situados en bloques diferentes, cada uno de los cuales tiene encomendado una función:

Hardware.

Núcleo o Kernel.

Shell.

Usuario.

6.3 REQUERIMIENTO DE HARDWARE

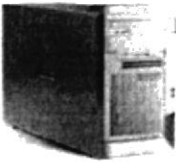
EQUIPO(SERVIDOR LINUX)	MÍNIMO	ÓPTIMO
	Procesador: Intel® Pentium® 2	Procesador: Intel® Pentium® 3
	Memoria RAM: 256MB	Memoria RAM: de 512 mb
	Disco duro: 3GB	Disco duro: 10
	Tarjeta de red: Ethernet 10 mbps	Tarjeta de red: Ethernet 10/100 mbps

Tabla 6-1: Requerimiento de hardware

Nota:

Se recomienda utilizar un equipo que cumpla con estas características o similares a ellas para poder tener un uso óptimo con todos los servicios utilizados, como ejemplo el Servidor de Correo ya que si su uso es para una cantidad mayor de usuarios como en el caso de una empresa grande se necesita un equipo de mayor capacidad

Recomendación

Procesador: Intel® Pentium® D Dual Core EM64T 3.00GHz
2 x 2MB cache L2 Bus Frontal de 800MHz
Memoria RAM: de 1GB

Disco duro: 160 GB SAS Hot-Swap
Tarjeta de red: Ethernet 10/100/1000 gigabit / on planar / Full duplex
Fuente de poder: 400 Watts



6.4 INTRODUCCIÓN A FEDORA CORE3



Fedora Project es el sistema libre de Red Hat, que aunque no da un soporte directo al mismo desde su lanzamiento, si se ha convertido en su patrocinador principal, aunque el código que lo forma está abierto y cualquiera puede incluir y/o ayudar a mejorarlo.

Mejorar Linux no se trata de programar únicamente; si sabes Inglés y Español ya puedes ayudar a traducir información, manuales,... e incluso probar las nuevas aplicaciones es muy útil para comprobar su estabilidad.

Permite disfrutar de un sistema potente y eficaz aunque Red Hat no le dé soporte directamente. Además es muy fácil de instalar, contiene herramientas de escritorio muy útiles, montones de programas muy variados, se ha convertido en un serio candidato que se debe probar.

En cualquier caso, Fedora Core 3 (la última versión de Fedora a 02/04/05) es un sistema muy estable, fácil de instalar y sencillo de configurar..

NOTA: El acceso al BIOS varía dependiendo del Hardware que utilice, sin embargo, las opciones más comunes son las teclas ESC, F2 o DEL.



6.5 ENTRADA AL BIOS

Nada más encender el ordenador, la primera pantalla que aparece es generada por la propia BIOS. En la mayoría de los equipos clónicos, esta pantalla informa de las características de chipset y versión de la BIOS instalada. Debajo de los códigos superiores, identificará el tipo de microprocesador y bajo este se comenzará a chequear la memoria del sistema. En este momento es cuando se debe pulsar una determinada tecla que se permitirá acceder a los menús de configuración.

Lo normal es que también aparezca un mensaje que avise de qué tecla es la que permitirá entrar al menú mencionado.

Generalmente, siempre que se encuentre ante una BIOS de la empresa AMI o AWARD, la tecla para el acceso es DEL o SUPR. En otro tipo de BIOS, como las PHOENIX, se tendrá que presionar la tecla F2.

En las pantallas de configuración se modifica todo tipo de parámetros que afectarán directamente al funcionamiento del hardware, haciendo que éste trabaje de una manera más o menos optimizada. Lo complicado de todo este asunto es que cada empresa que fabrica BIOS suele tener opciones diferentes de configuración, acorde con el tipo de placa base en la que se va a instalar. Aquí se intentará explicar con detalle todos los parámetros más comunes que se puede encontrar en cualquier tipo de BIOS, aunque seguro que no se podrá explicar todos. Aún así no hay que preocuparse, ya que muchos de estos parámetros no serán cruciales para la configuración del sistema.

Las BIOS más extendidas son las AWARD, por lo tanto se elige esta marca para pasar a explicar las pantallas de configuración.

Para facilidad se ha trabajado en un programa llamado `wmware` pulsando sobre el simbolo de "play" " Star this virtual machine" mientras arranca, se pulsa sobre "F2" para entrar en la bios virtual de esta máquina, el motivo es simple, se quiere escoger que "Botee" desde el DVD como si del bios real se tratara.

Con las teclas de flecha, arriba/abajo, se lo pone en color blanco la unidad de DVD/cd-rom, y una vez en blanco, con las teclas "+" y "-" se la sube al primer lugar como esta imagen, así arrancara la máquina virtual desde el DVD. Una vez hecho, sobre "exit" como una bios normal y se sale guardando cambios.



Figura 6-3: Pantalla del Bios

Tras guardar cambios, se reinicia la máquina virtual, y se empieza a botear desde el dvd o cdroom

Ahora arranca de nuevo la máquina virtual, para que se ingrese los cd's que se van a necesitar para instalar linux.



6.6 INSTALACIÓN DE LINUX

Arranque de CD/DVD de Fedora en la pc: se ingresa los CDS o DVD para la instalación de Fedora Core 3 en la unidad lectora de CD-ROM/DVD" de la computadora, se presiona **F10**, para comenzar la instalación de manera que se pueda iniciar la instalación automáticamente.

Pulse cualquier tecla para iniciar desde CD...

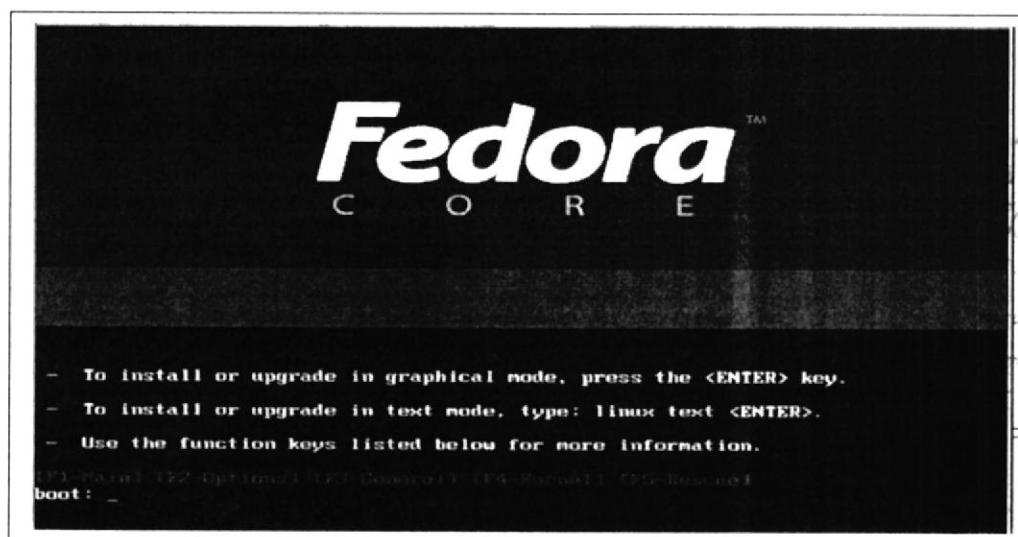


Figura 6-4: Ingreso del Cd de Arranque

En esta pantalla pregunta si se desea hacer un skandisk al disco o si se quiere omitir ese paso. Se escoge la opción **1** skip y va directo a la instalación

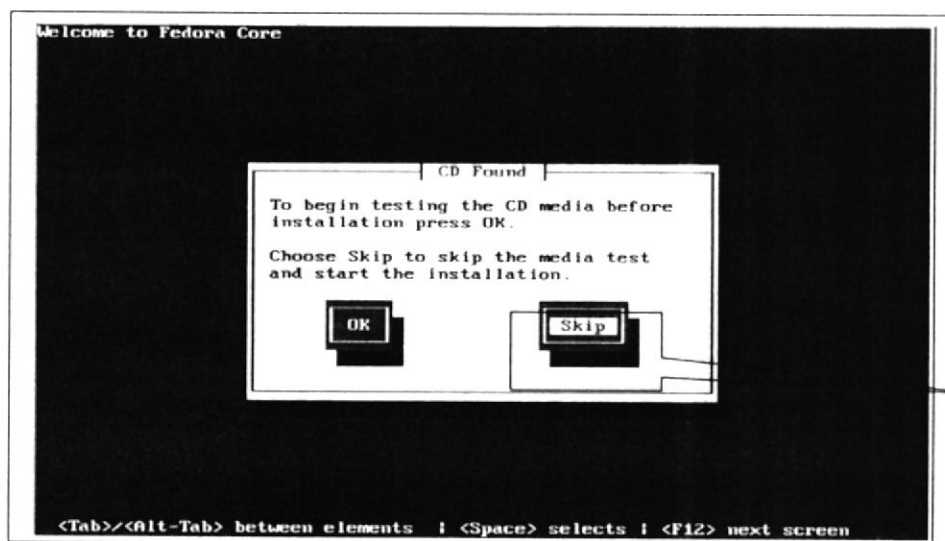


Figura 6-5: opción de skip

Welcome to Fedora Core: Da la Bienvenida para comenzar a elegir los cambios del sistema sea del idioma, mouse, teclado etc. Elegir **1 siguiente**

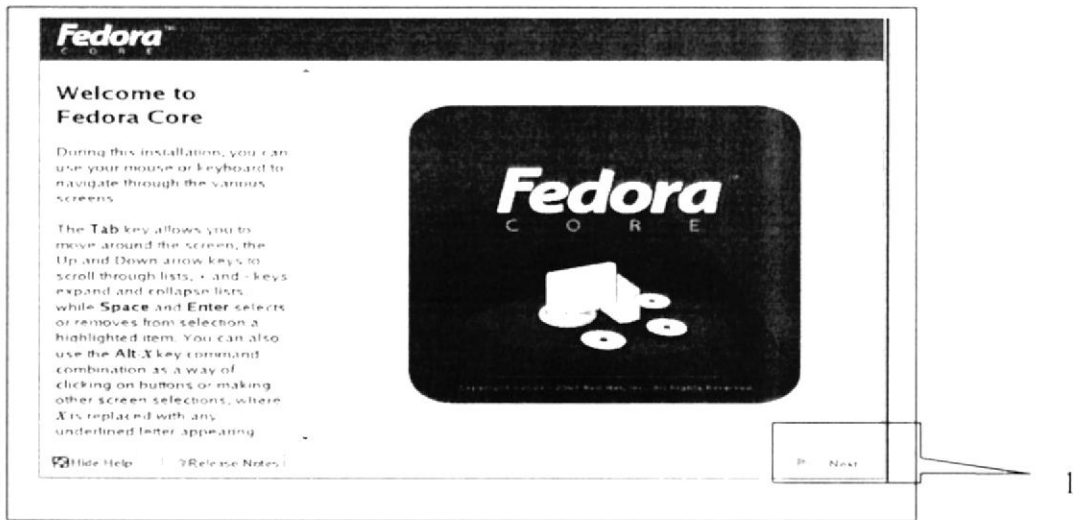


Figura 6-6: Bienvenido a Fedora Core

Configuración del Teclado: Se selecciona el tipo de teclado para que los caracteres de las teclas coincidan y no muestren otros caracteres, en este caso se selecciona **1 Spanish** y se presiona **2 siguiente**

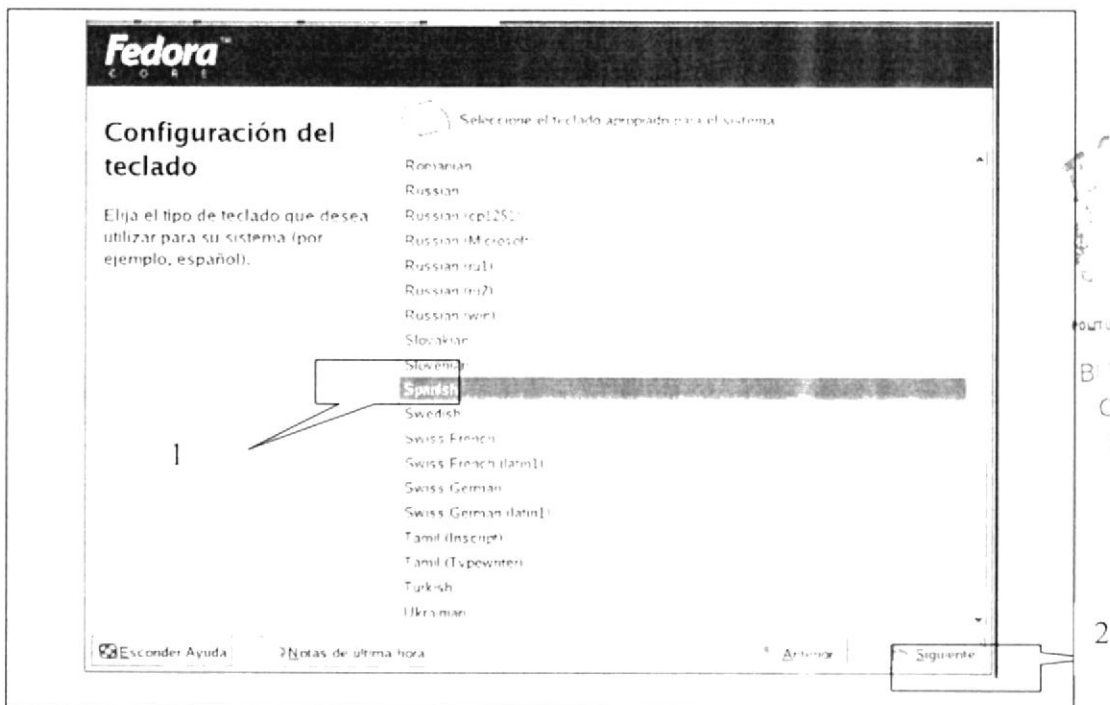


Figura 6-7: Configuración de teclado

Selección de Idioma: Se selecciona **1 Spanish(Español)** y se presiona **2 NEXT** para continuar

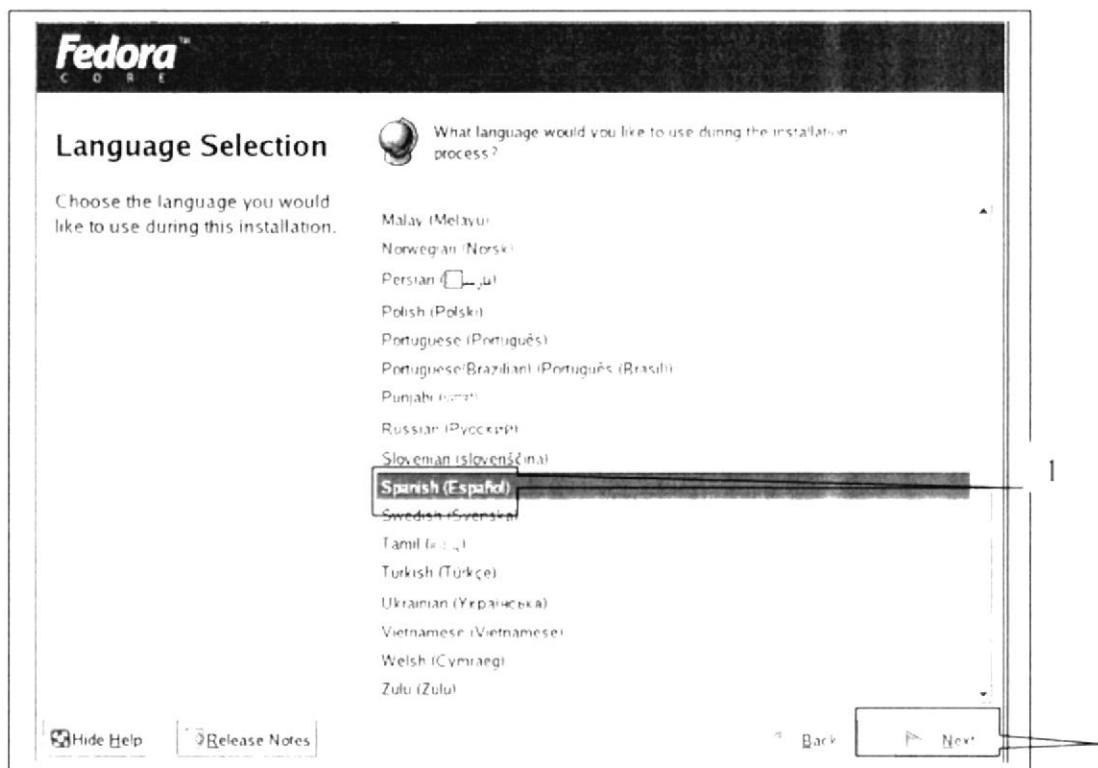


Figura 6-8: Selección del Lenguaje

Tipo de Instalación: Se selecciona **1. Personalizada** para poder tener control en la elección de paquetes de Software, proceso de instalación y preferencias de particionamiento. Se escoge **2. siguiente**.

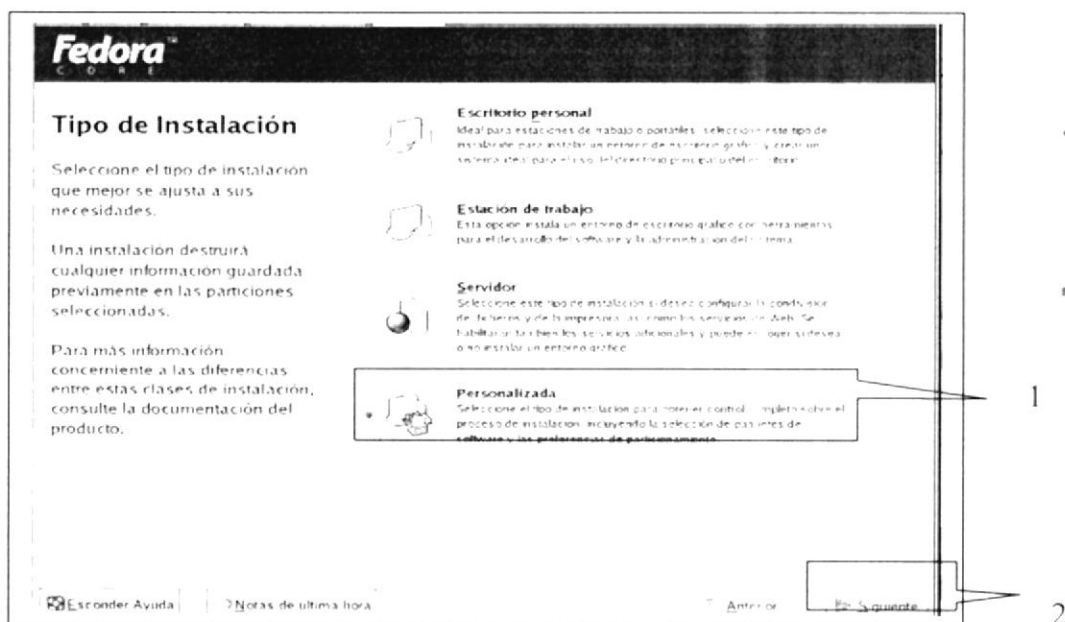


Figura 6-9: Tipo de Instalación

Escritorio Personal.- Instala un entorno de escritorio gráfico y crear un sistema ideal para el uso del directorio principal o del escritorio.

Estación de Trabajo.- Instala un entorno de escritorio gráfico como el desarrollo del software y la administración de Sistemas.

Servidor.- Configura la condivisione de ficheros e impresoras, así como los servicios web, se habilitan servicios adicionales.

Personalizada.- Se obtiene el control completo sobre el proceso de instalación, incluyendo la selección de paquete de software, y las preferencias de particionamiento

Configuración del Particionamiento del Disco: Se selecciona **1.Partición manual con Disk Druid** para poder asignar puntos de montaje, partición para swap, el boot y raíz que son importante en la instalación. Se selecciona **2.siguiente.**

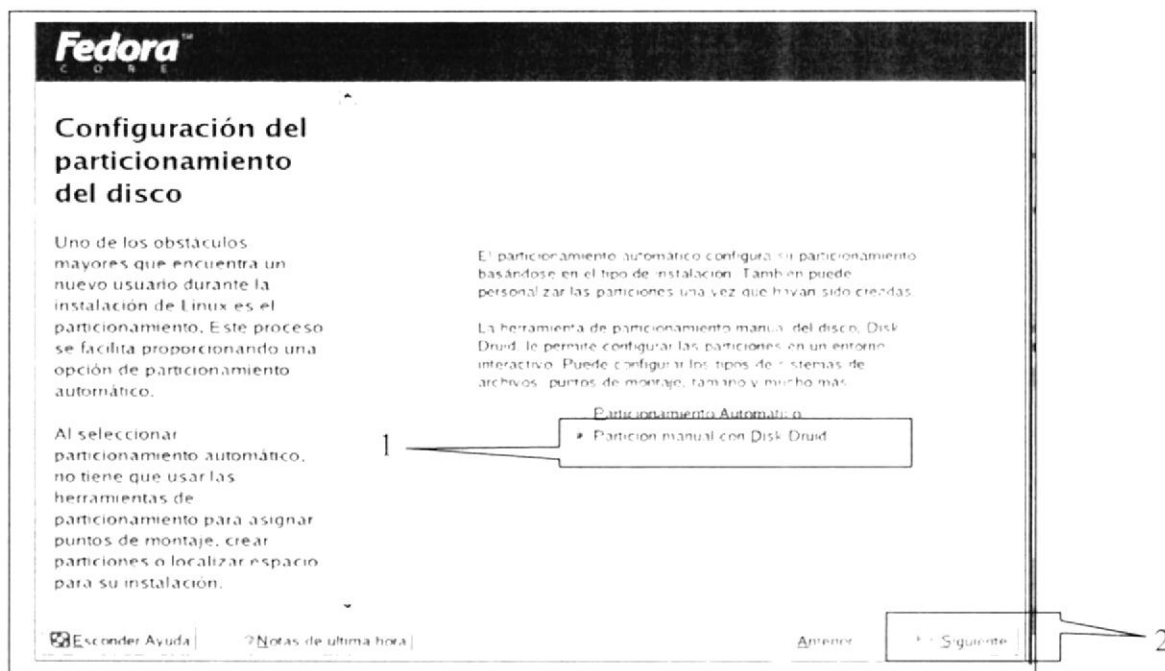


Figura 6-10: Configuración de particionamiento del disco

Configuración del Disco: Paso 1 Se ubica el puntero en **Libre** y se presiona **Nuevo** para crear los particionamientos necesarios en el Sistema **Paso 2** siguiente

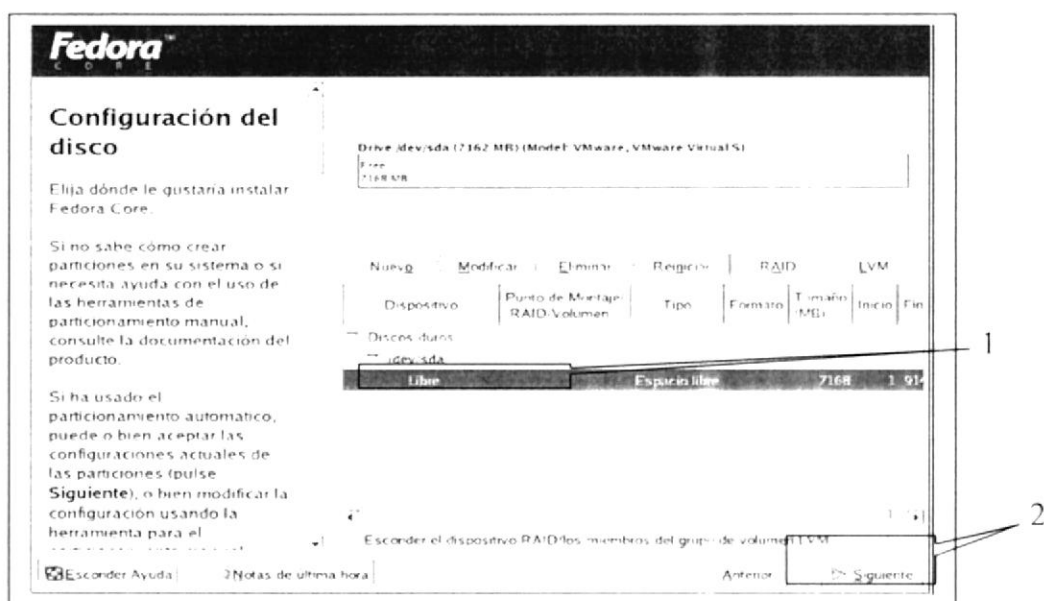


Figura 6-11: Configuración del disco

Se añade **swap** esta partición es obligatoria, **1 swap** es la memoria virtual de Linux y su tamaño (MB) es el doble de memoria que se tiene en nuestra PC. Se escoge **2 ACEPTAR**

Recomendaciones: Se recomienda duplicar la memoria ram solo hasta 512MB.

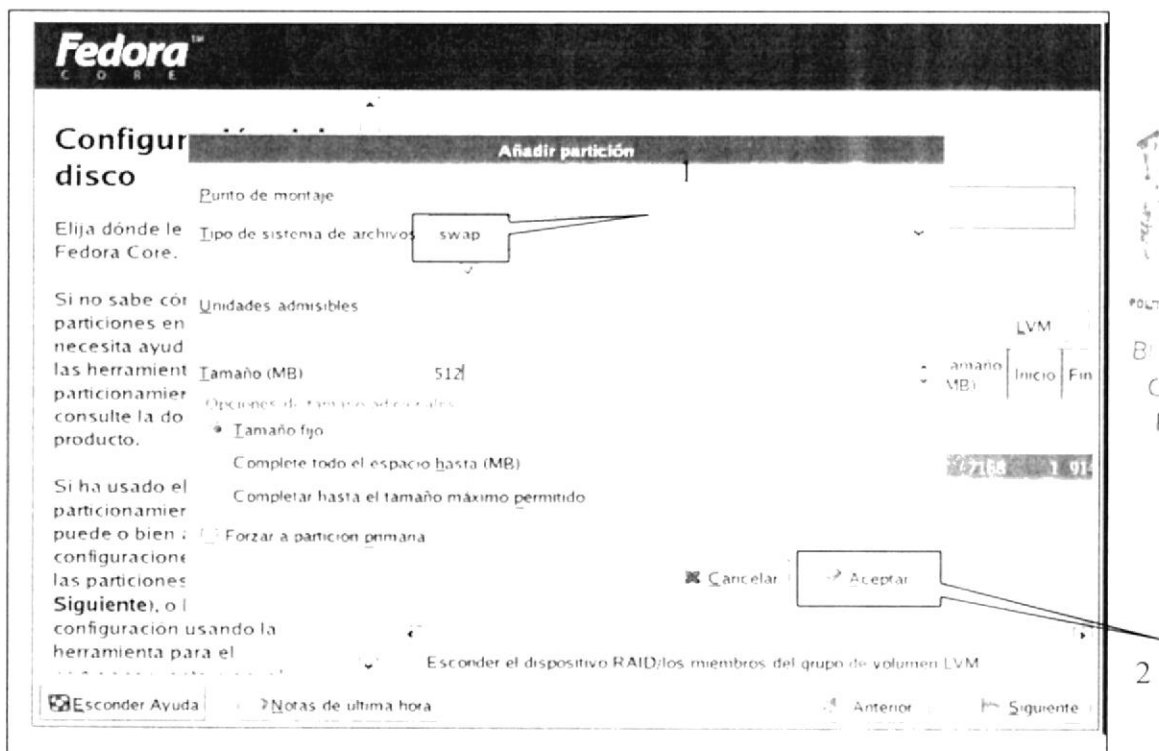


Figura 6-12: Partición de swap

Paso 1: El directorio **/boot**: Para buear 2 sistemas Operativos aquí se guarda el **Kernel**. **Paso 2** se elige **ACEPTAR**

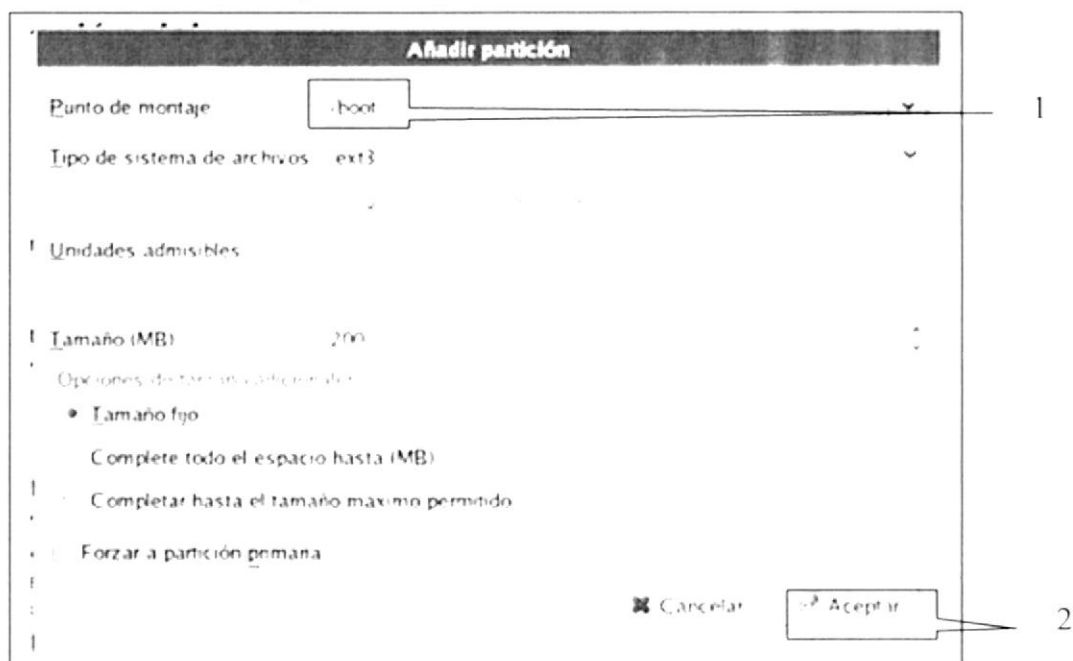


Figura 6-13: Partición de Boot

Paso 1: **/=El DIRECTORIO RAIZ** es obligatorio, aquí se guarda toda la estructura del directorio de Linux. **Paso 2** se elige **ACEPTAR**

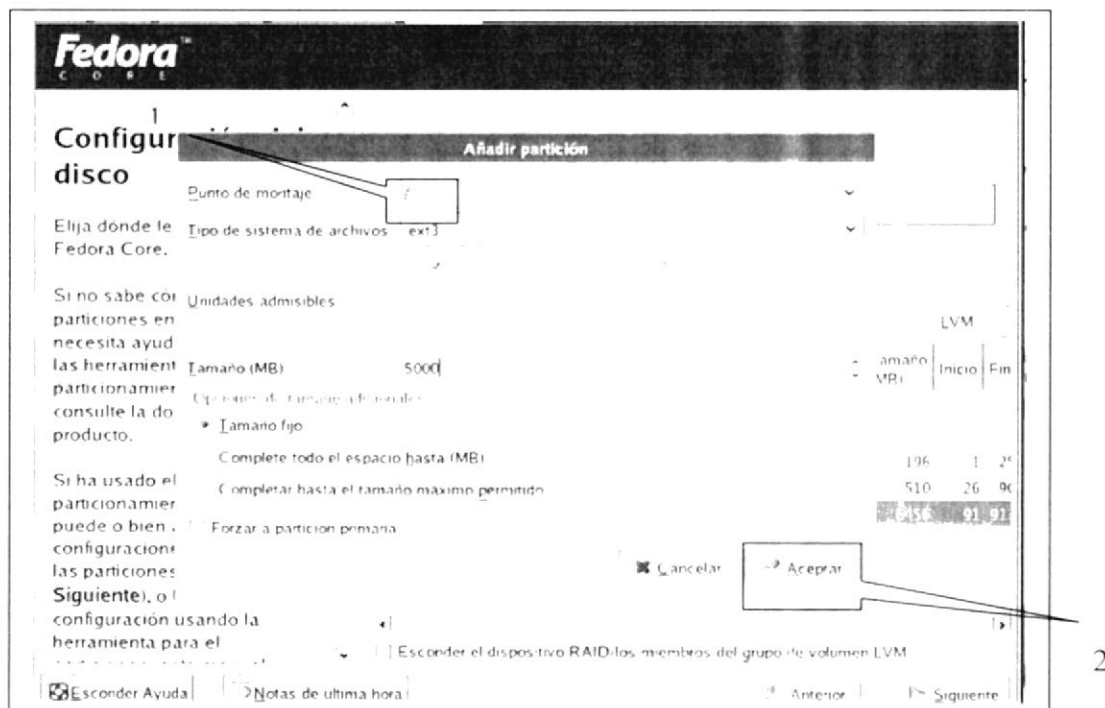


Figura 6-14: Configuración de Directorio raíz

Así quedará particionado el sistema operativo. Se elige. **Paso 1 Siguiente**

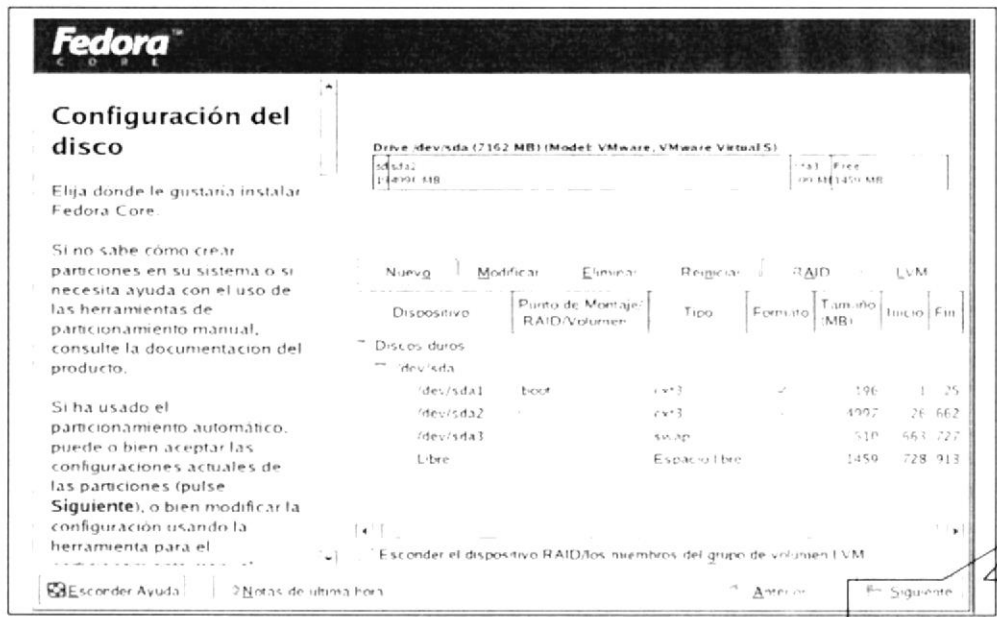


Figura 6-15: Creación de todas las particiones

Gestor de Arranque: Aquí se elige con que Sistema Operativo arranca primero en el momento de encender la PC por defecto esta señalado **FEDORA CORE** pero se puede cambiar por **WINDOWS** en modificar en este caso se arranca con **FEDORA CORE**. **Paso 1 se selecciona Siguiente.**

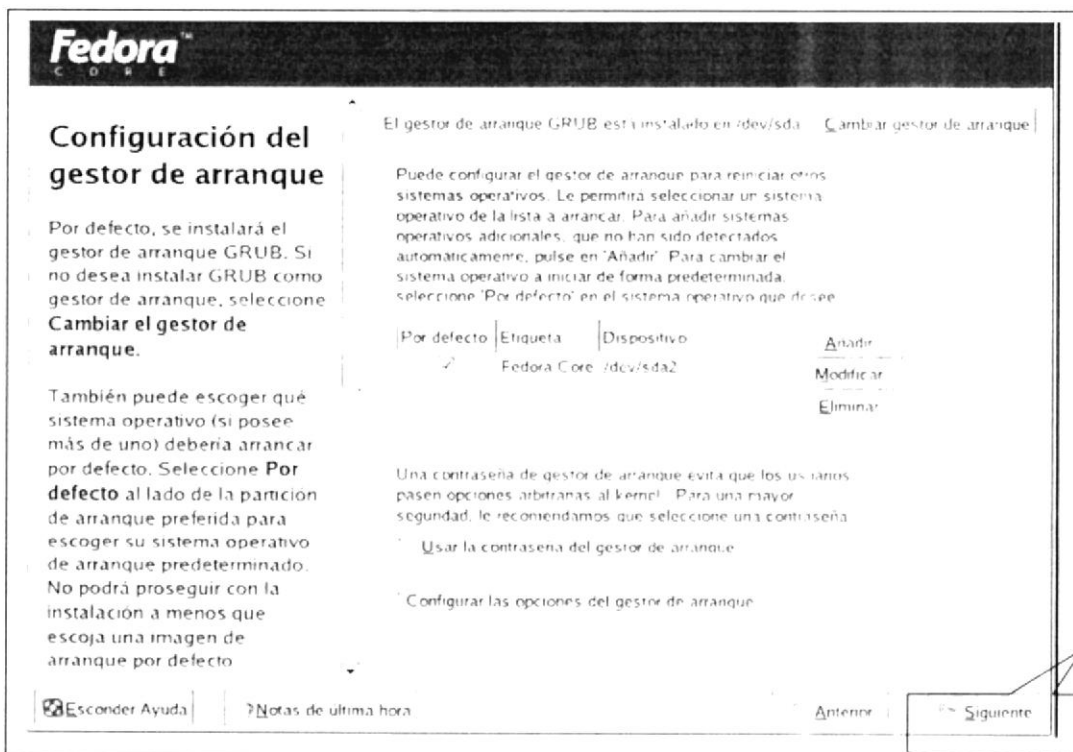


Figura 6-16: Configuración de gestor de arranque

Configuración de la red: Aquí se configura la tarjeta de red **eth0** aparece solo una tarjeta de red, porque solo existe una tarjeta de red. Da también la opción de elegir su configuración de forma manual o automática, se selecciona de **forma automática a través de DHCP**. **Paso 1 se elige Siguiente.**

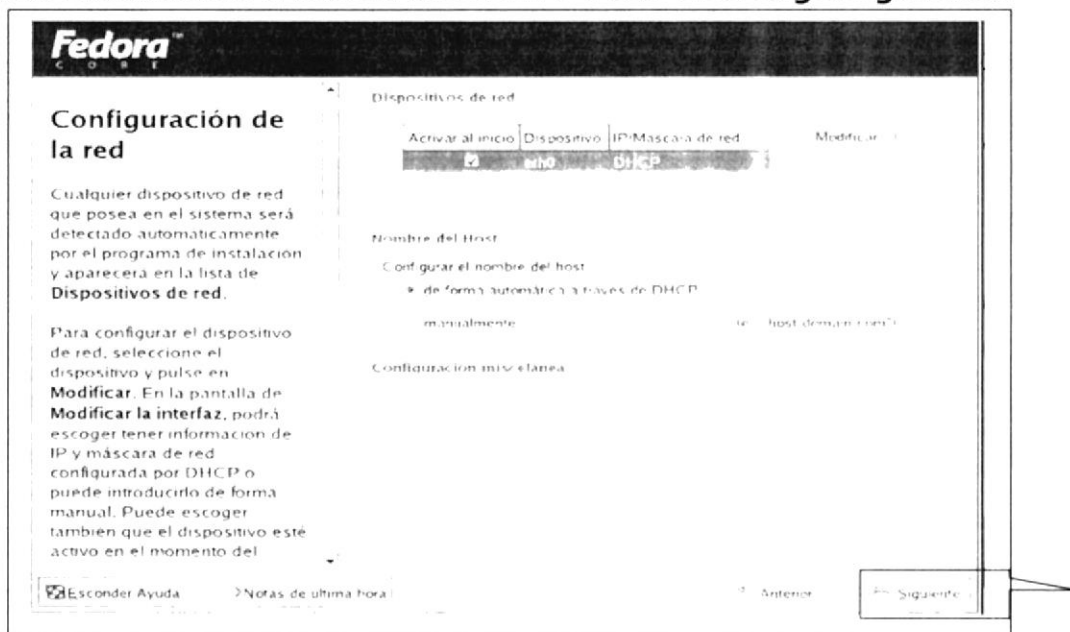


Figura 6-17: Configuración de la red

Configuración de Cortafuegos/Firewall: Aquí se habilitan los firewalls, no se lo habilita en este momento por eso se elige **Paso 1** Ningún cortafuego esto significa que el firewall de Linux no esta habilitado **Paso 2 siguiente**

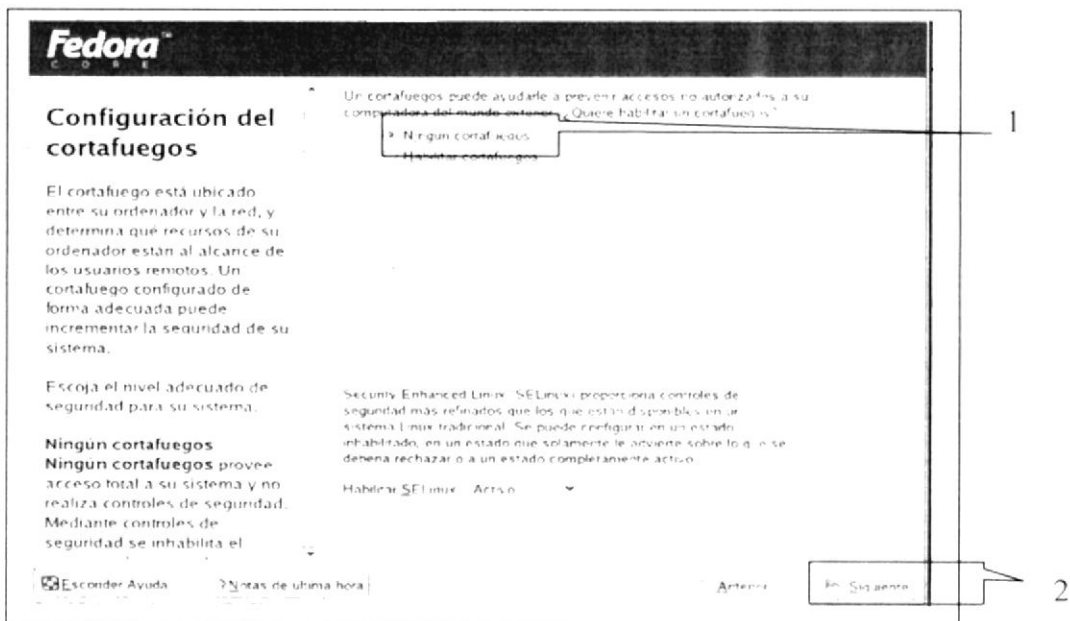


Figura 6-18: Configuración del cortafuego

Aparecerá esta pantalla de **Advertencia se selecciona Paso 1 PROCEDER**

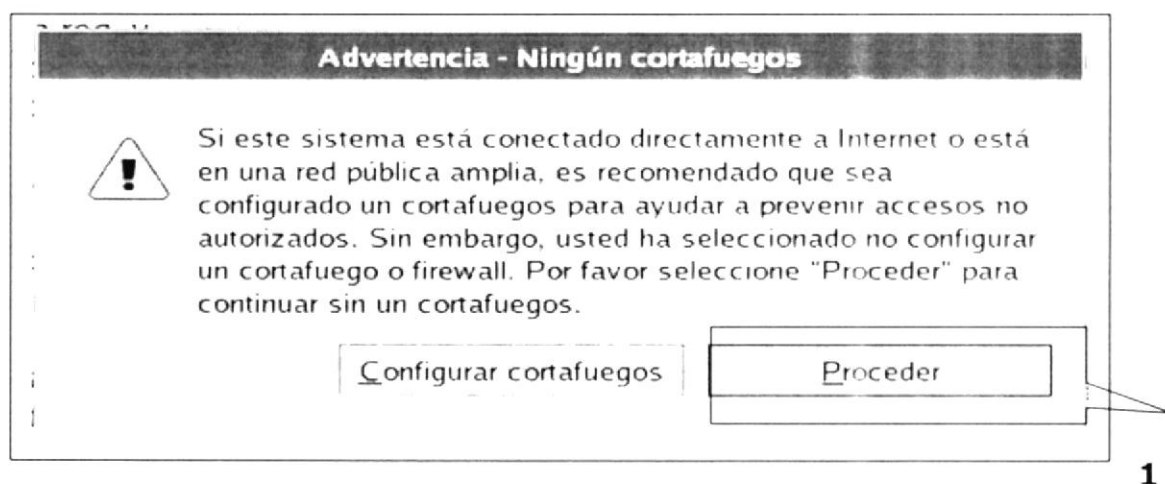


Figura 6-19: Advertencia de Cortafuego

Soporte adicional del Idioma: se selecciona **Paso 1 Spanish (ecuador)** porque es el idioma a utilizar en este sistema da más opciones de idiomas. Se escoge **Paso 2 siguiente**

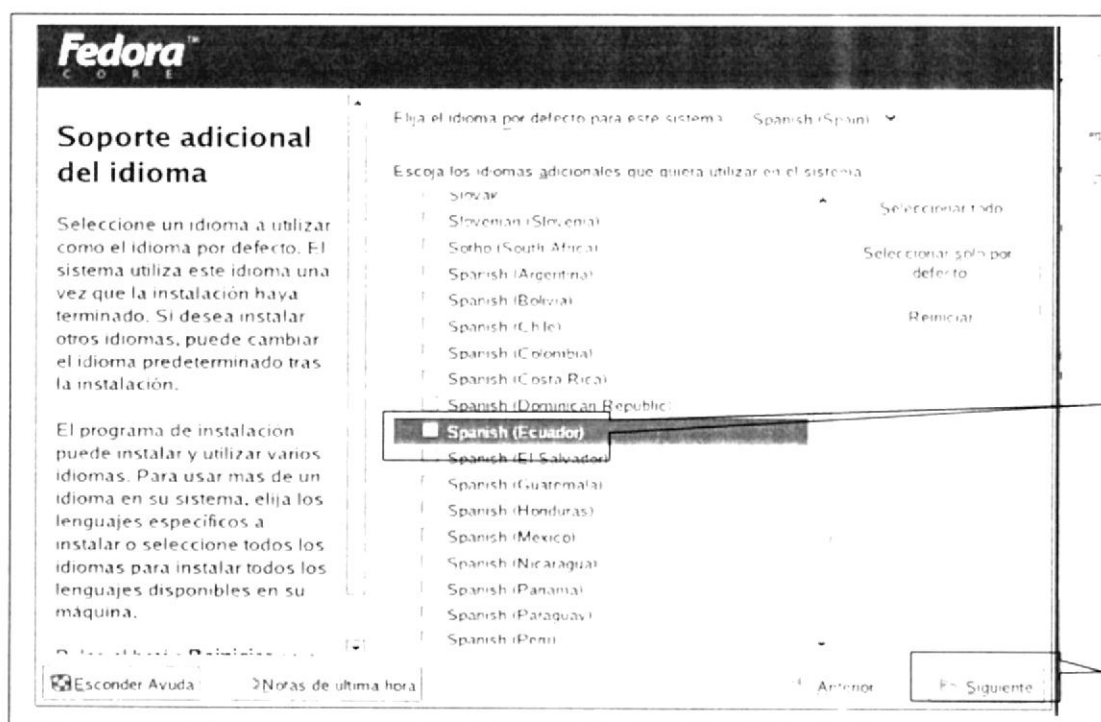


Figura 6-20: Soporte adicional de idioma

Selección de Horario: En el mapa se busca la ciudad mas cercana de donde se encontra en esta caso **Paso 1** se ubica en **AMERICA /GUAYAQUIL**. Se escoge **Paso 2** siguiente

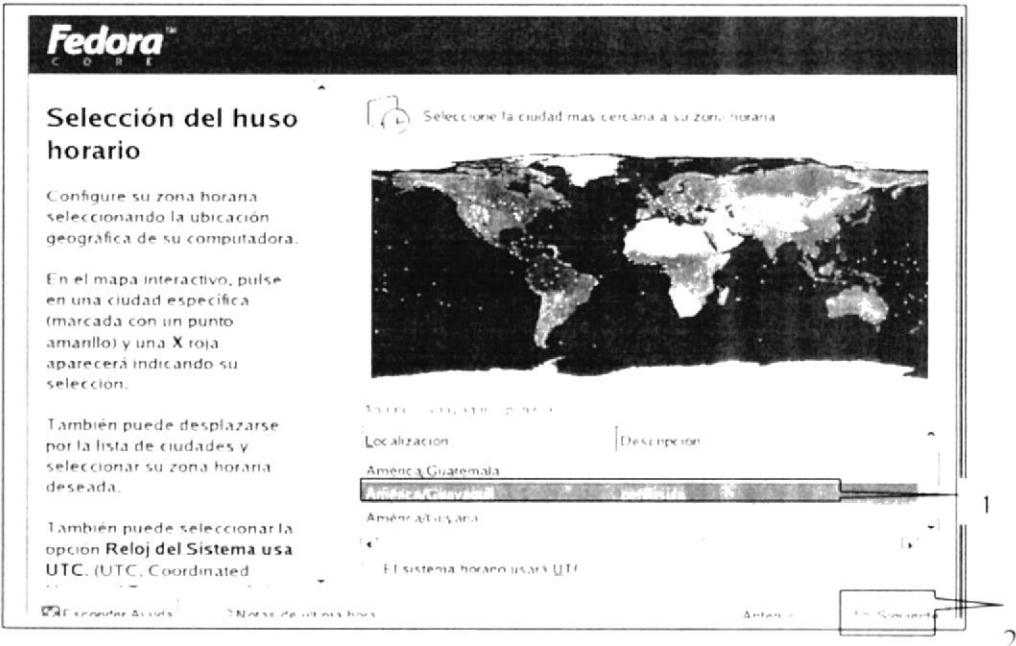


Figura 6-21: Selección de horario

Paso 1 Configuración de contraseña para el root: Esta cuenta es la cuenta del administrador con fines administrar todo lo referente al sistema. Se escoge **Paso 2 siguiente**

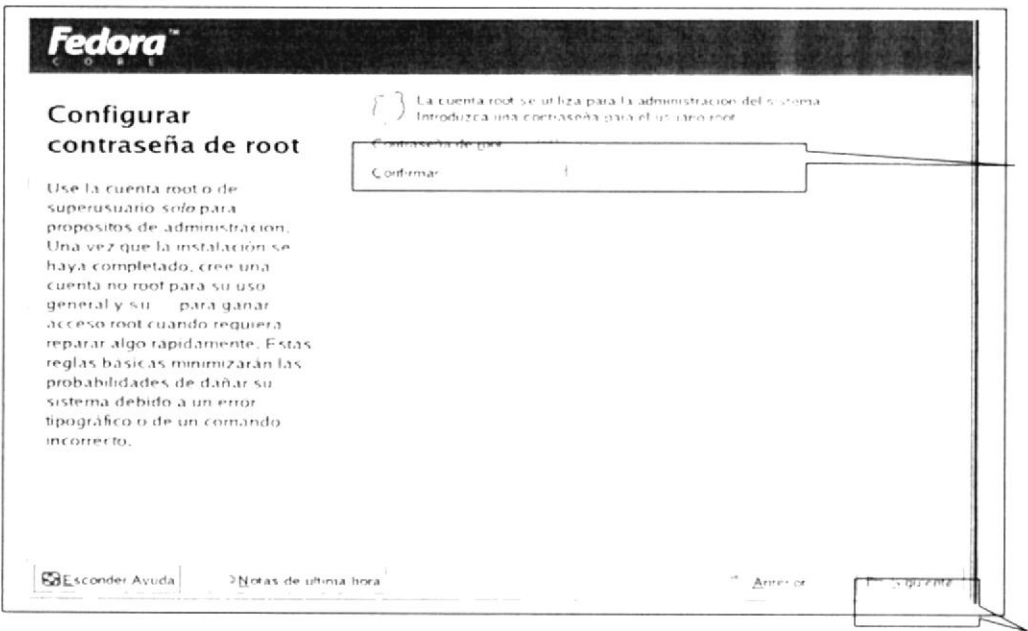


Figura 6-22: Configuración de contraseña

Selección de paquetes: Aquí se elegirá todos los paquetes que se necesitará para la instalación

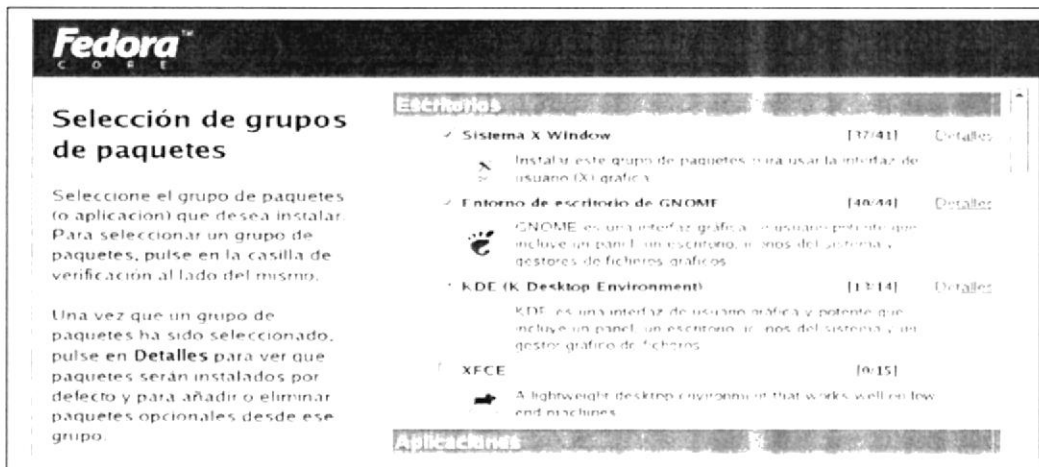
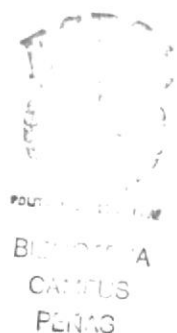


Figura 6-23: Selección de paquetes de escritorio



Figura 6-24: Selección de grupos de paquetes



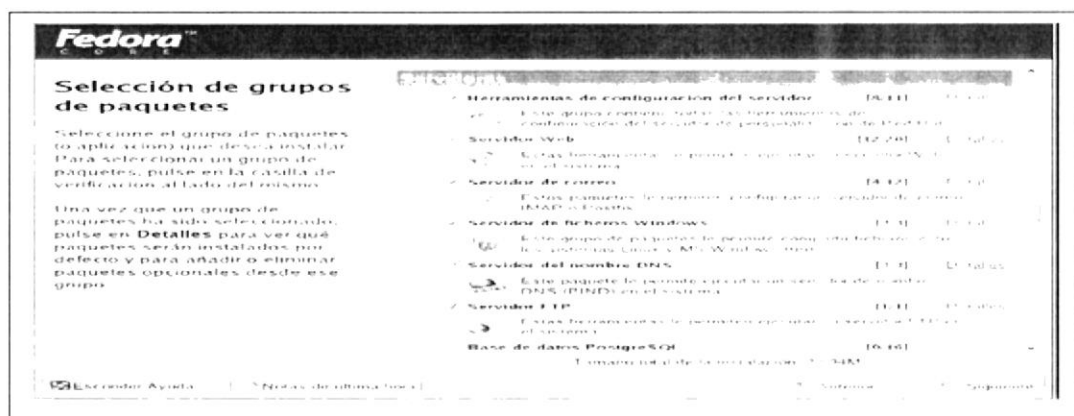


Figura 6-25: Selección de paquetes de Servidores

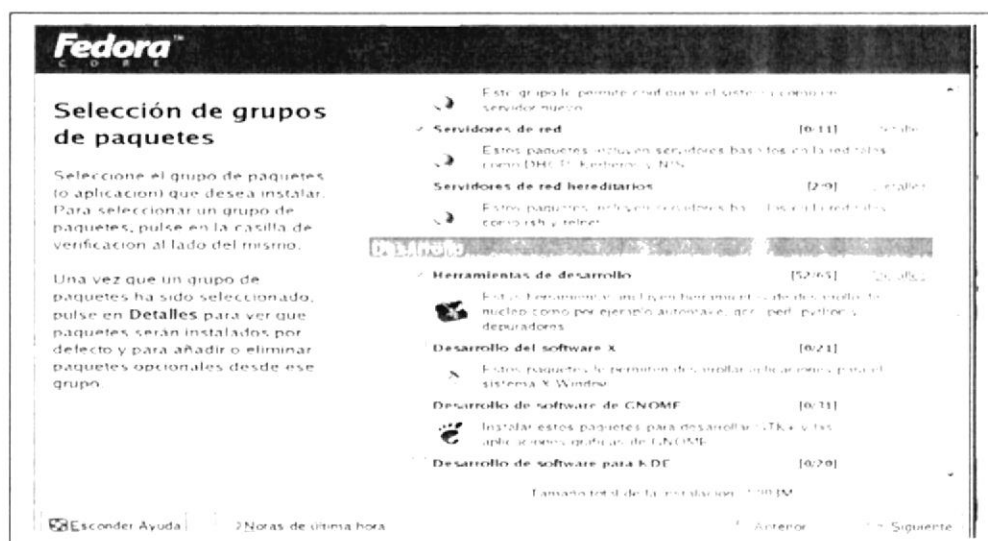


Figura 6-26: Selección de paquetes de desarrollo

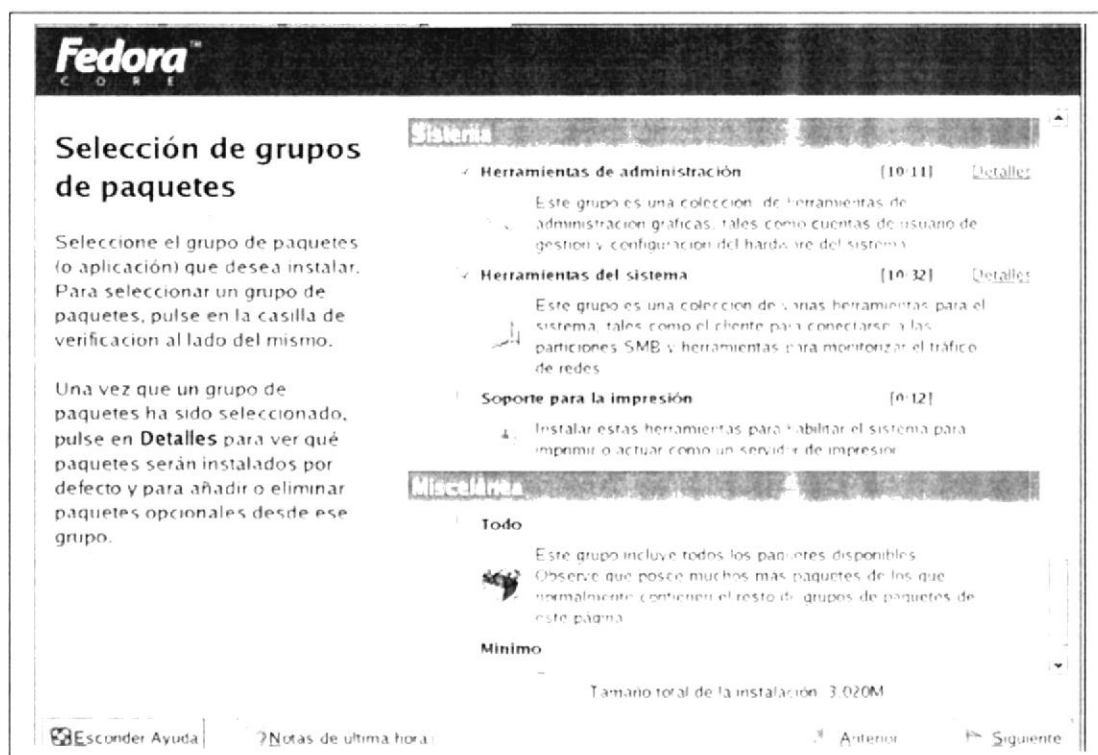


Figura 6-27: Selección de paquetes de sistemas



Luego de haber seleccionado todo los paquetes necesarios se elige **Siguiente**.

Instalación de paquetes: Fedora comenzará llevando a cabo todas las operaciones necesarias para la configuración del disco duro, tal y como se lo se indica anteriormente en el apartado de particionamiento. Presionar **Paso 1 SIGUIENTE**.

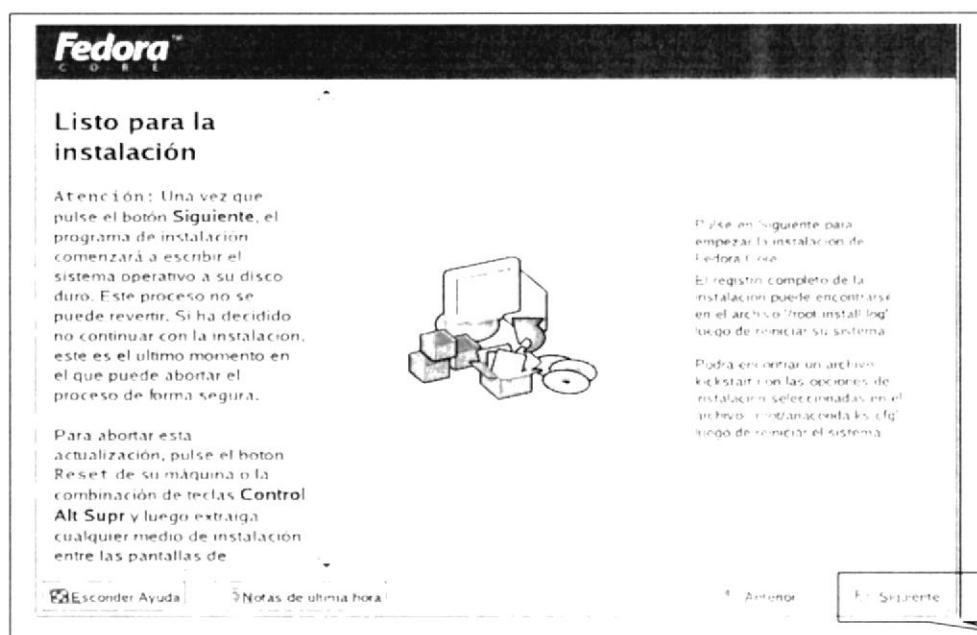


Figura 6-28: Listo para la instalación

Para la instalación se necesita 3 CDs de Fedora Core 3.

Paso 1 Presionar **CONTINUAR**

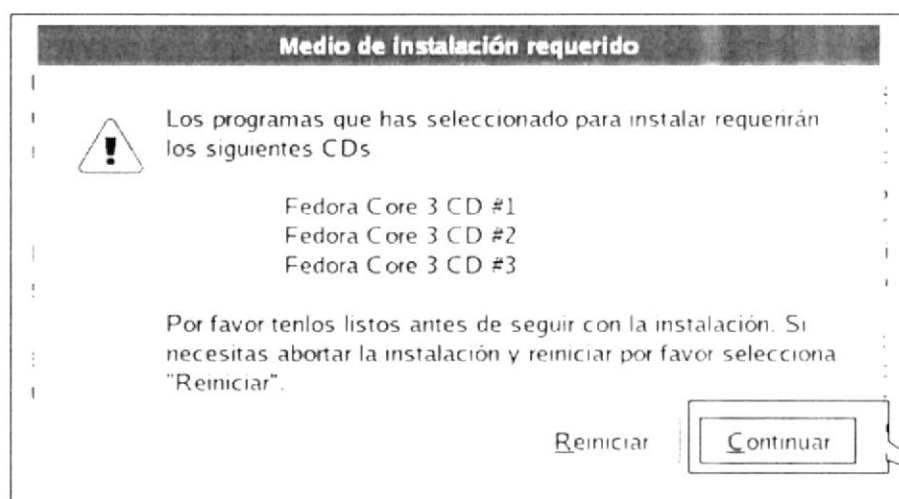


Figura 6-29: Medio de instalación requerido

Instalación: Fedora Core 3 está copiando los programas o paquetes al disco duro. No extraer el CD o DVD hasta que se indique:

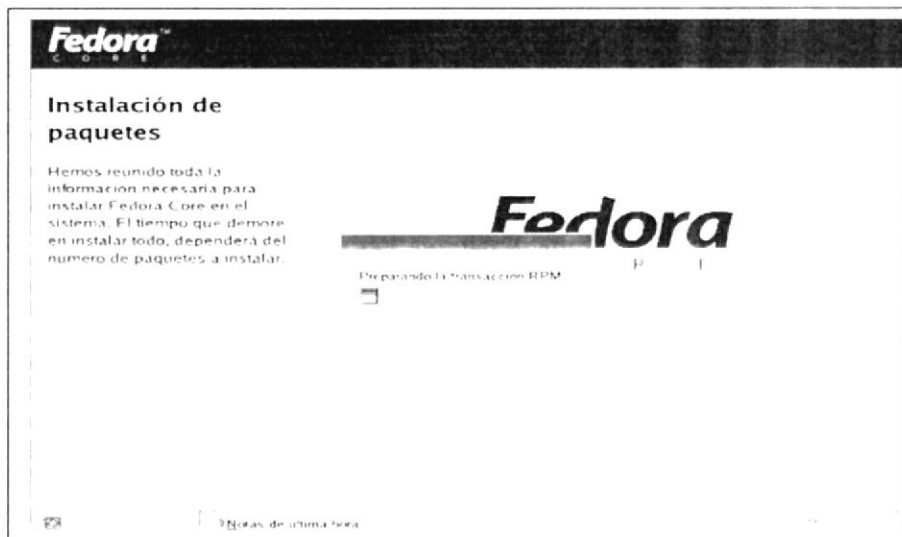


Figura 6-30: Instalación de paquetes 1

El tiempo de Instalación lleva de 30 minutos a 90 dependiendo de los paquetes que se eligieron al momento de la instalación.

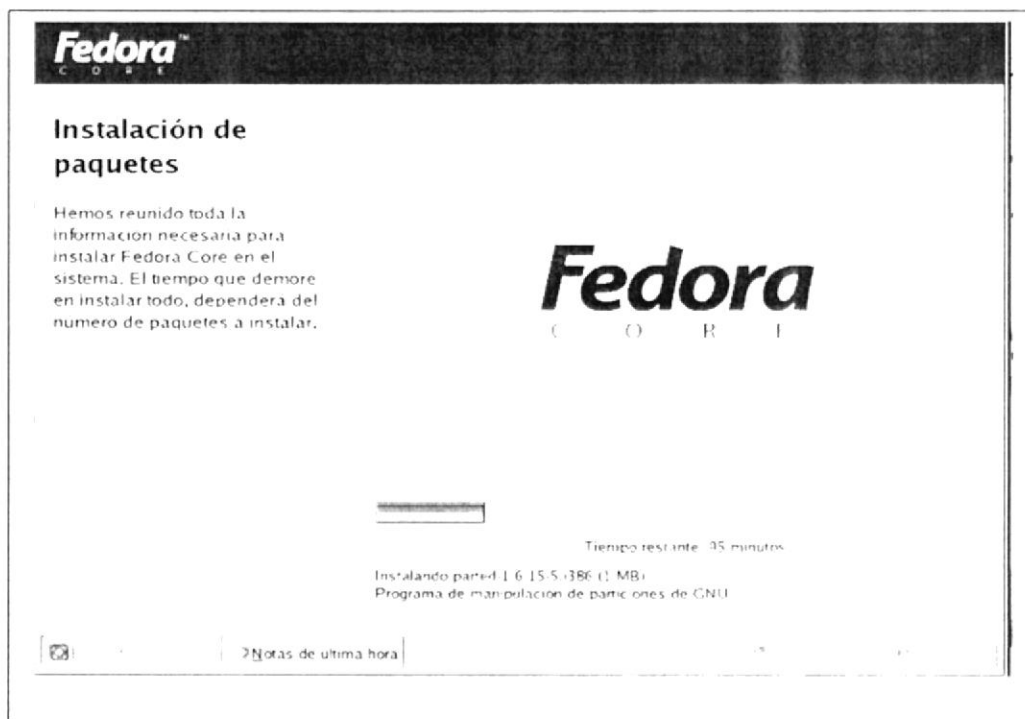


Figura 6-31: Instalación de los paquetes 2

Pide Ingresar el CDs 2 para continuar con la instalación. Se ingresa el CD correspondiente en la unidad lectora de la PC Paso 1 ACEPTAR

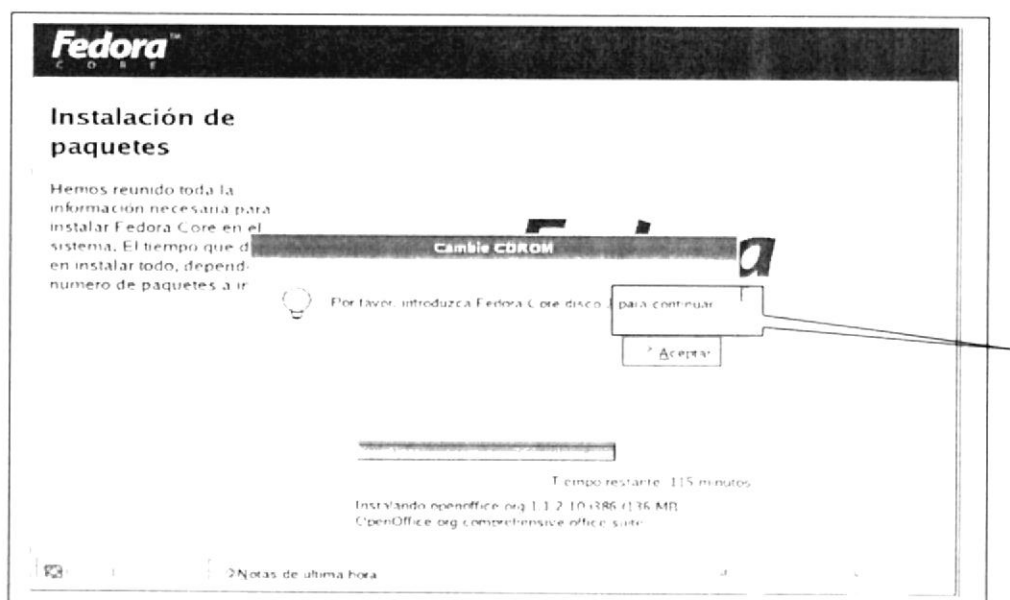


Figura 6-32: Ingreso del segundo cd de fedora

Se ingresa el último CDs de la instalación de FEDORA CORE 3 Paso 1 ACEPTAR

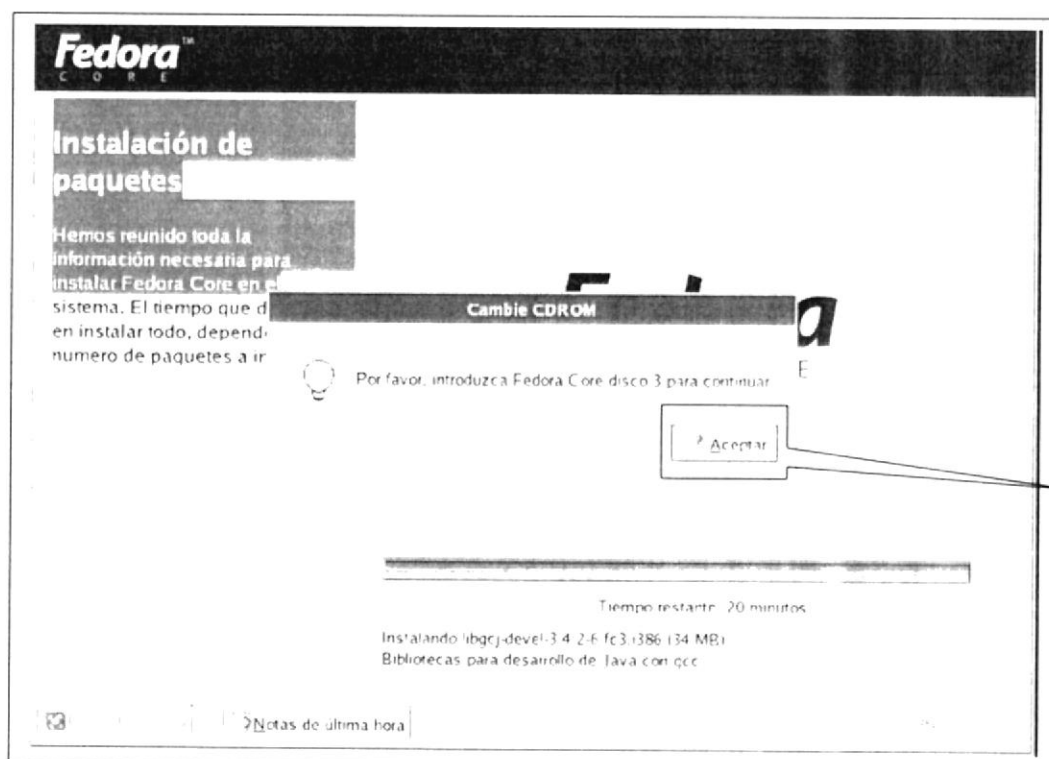


Figura 6-33: ingreso del último cd para la instalación

Paso 1 Reiniciar el Sistema para que se guarde los cambios

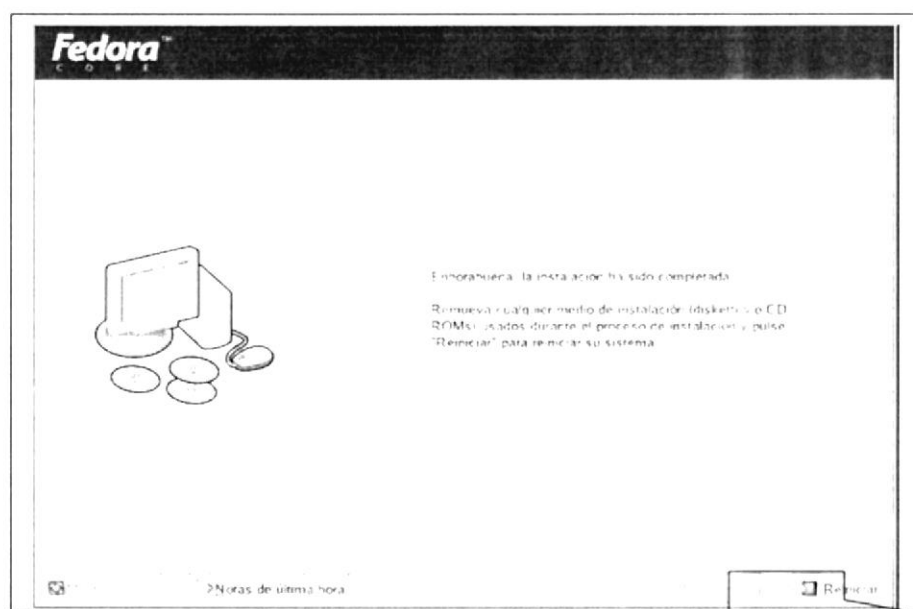


Figura 6-34: reinicio del sistema



6.7 CONFIGURACIÓN DE POST-INSTALACIÓN LINUX

En esta pantalla se comienza ingresando al entorno de Linux.

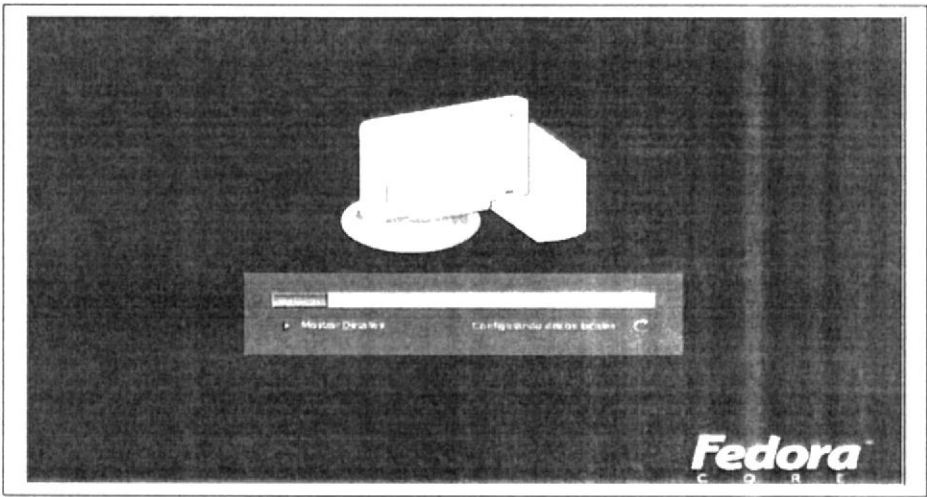


Figura 6-35: ingreso al entorno de linux

Da la Bienvenida a **FEDORA CORE Paso 1** se escoge **SIGUIENTE**

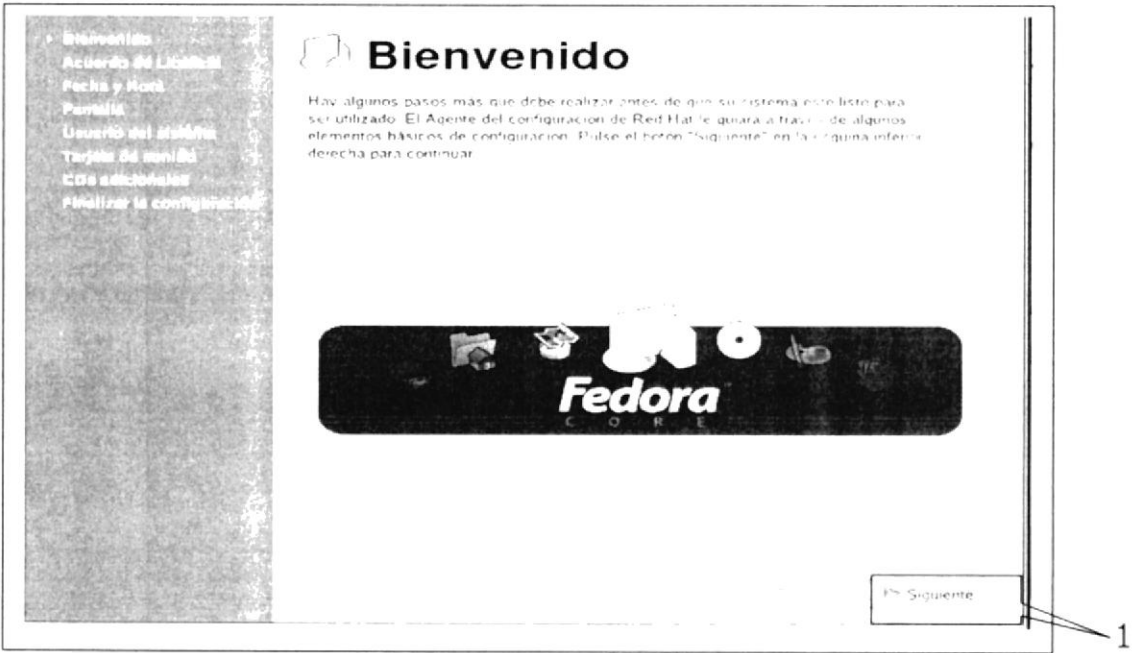


Figura 6-36: Bienvenido al entorno de fedora

Muestra el acuerdo de la Licencia, se acepta. **Paso 1** Si, acepto el acuerdo de licencia **Paso 2** se escoge **Siguiente**

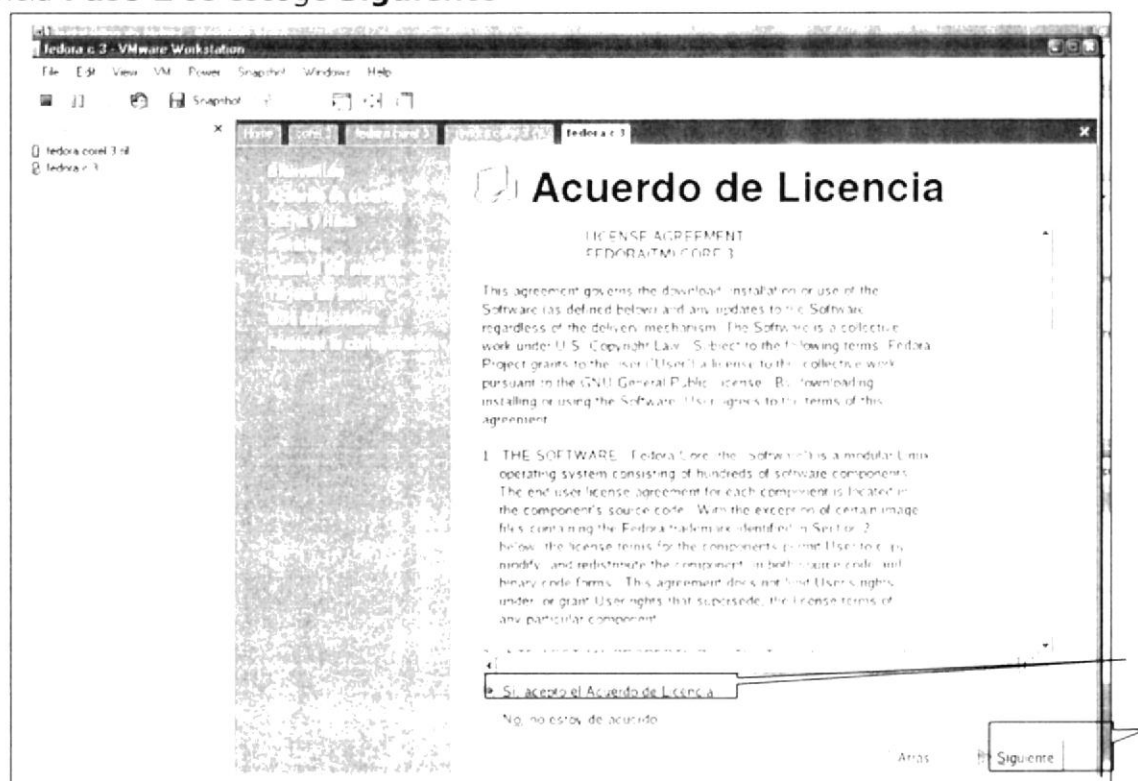


Figura 6-37: Acuerdo de licencia

Paso 1 Configuración de FECHA Y HORA: Se selecciona la fecha y hora.
Paso 2 Se escoge **Siguiente**

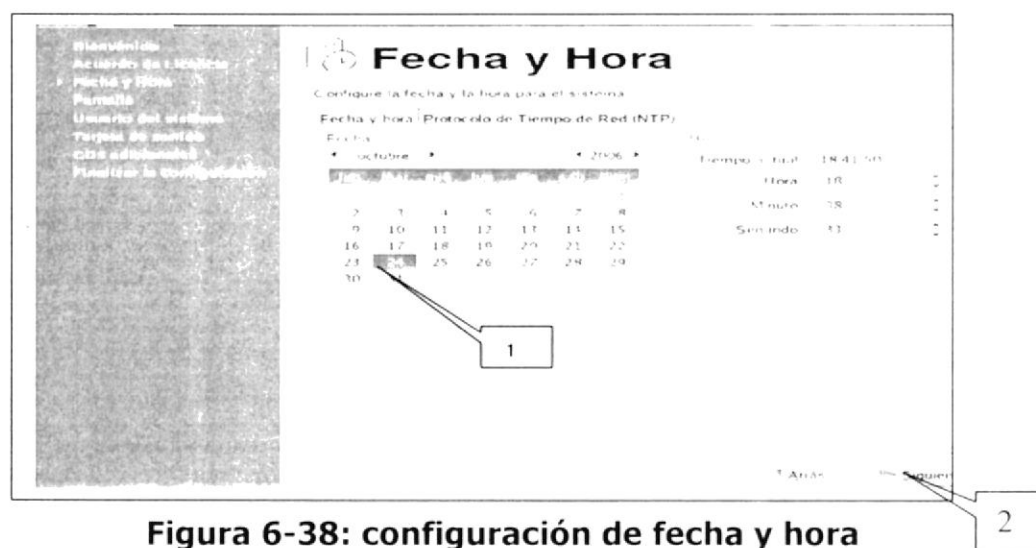


Figura 6-38: configuración de fecha y hora

Configuración de Pantalla: Muestra la configuración de la pantalla donde se podrá cambiar la resolución de la misma. **Paso 1** se escoge **Siguiente**

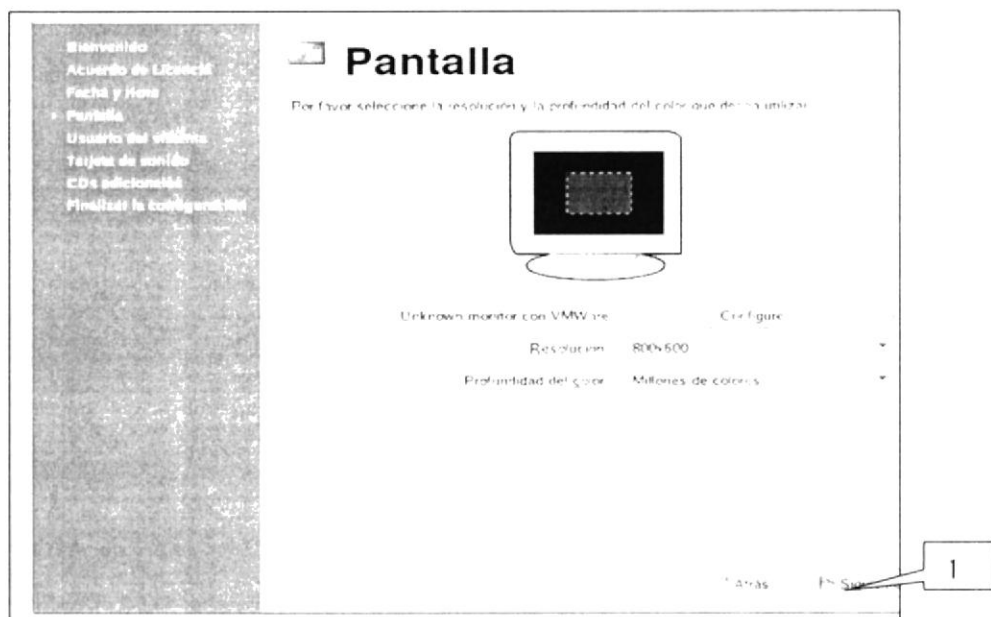


Figura 6-39: configuración de la pantalla

Paso 1 se asigna al Usuario del sistema en este caso el administrador será **SERVIPAGOS** con su respectiva contraseña. **Paso 2** se elige **Siguiente**

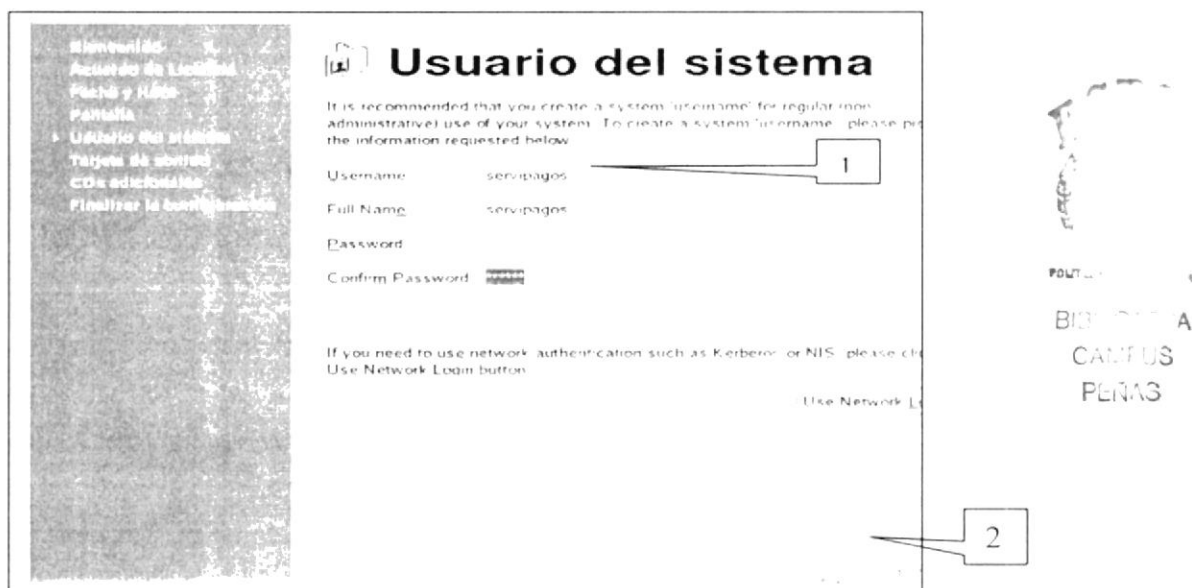


Figura 6-40: usuario del sistema

Configuración de Tarjeta de Sonido: Da opción a realizar una prueba de sonido. **Paso 1** se elige **SIGUIENTE**

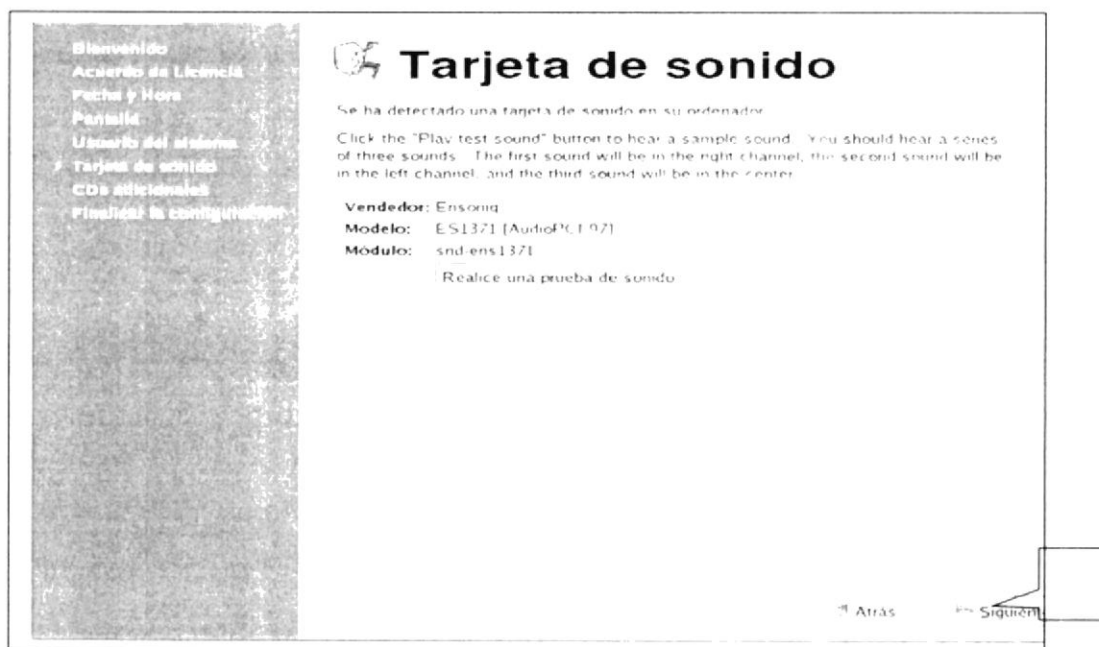


Figura 6-41: configuración de tarjeta de sonido

Finaliza la Configuración. **Paso 1** Elegir **SIGUIENTE**



Figura 6-42: finalización de la configuración

6.8 INICIO DE SESIÓN AMBIENTE GRÁFICO

Paso 1 se ingresa a Fedora como administrador **ROOT** se presiona ENTER

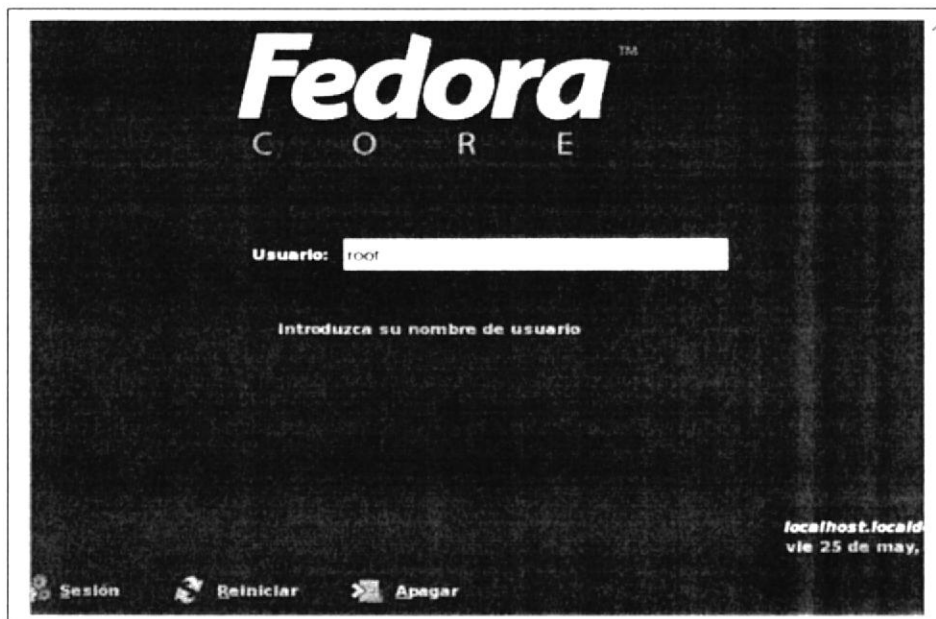


Figura 6-43: ingreso del root a fedora corel3

Paso 2 se ingresa la contraseña de administrador root

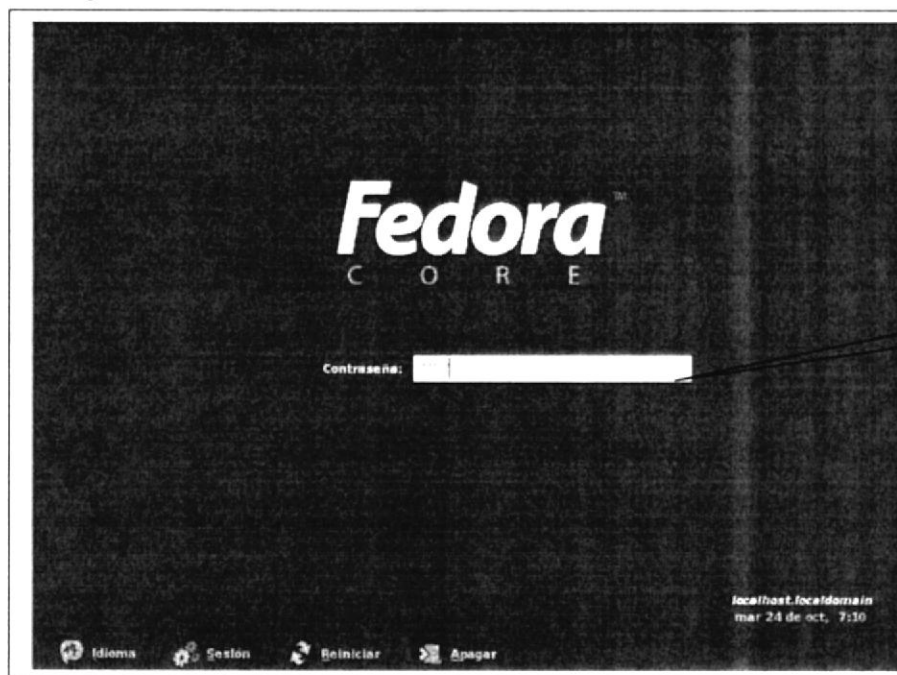


Figura 6-44: ingreso de contraseña

6.9 INICIO DE SESIÓN MODO TEXTO

Si no creó una cuenta de usuario durante la instalación, deberá ingresar como root. Dependiendo de su elección durante la instalación verá una pantalla de texto (consola) o una pantalla gráfica (Pantalla de acceso gráfica) en la cual deberá ingresar su nombre de cuenta y la contraseña asociada a esa cuenta.

Para ingresar al modo texto de Linux se presiona la combinación de teclas **crtl-alt+F1,F2...F6** para regresar a sesión de modo gráfico se presiona **crtl-alt+F7**.

En la primera pantalla pide el ingreso de un usuario

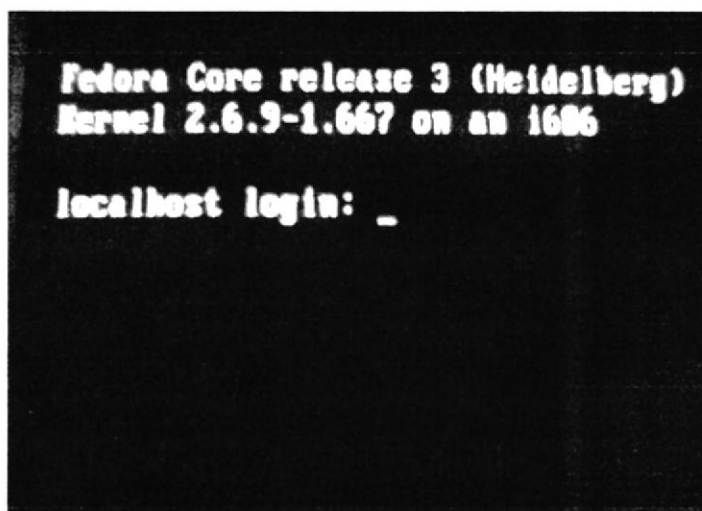


Figura 6-45: Ingreso del login

Se ingresa con el usuario administrador en Linux, que es el root.

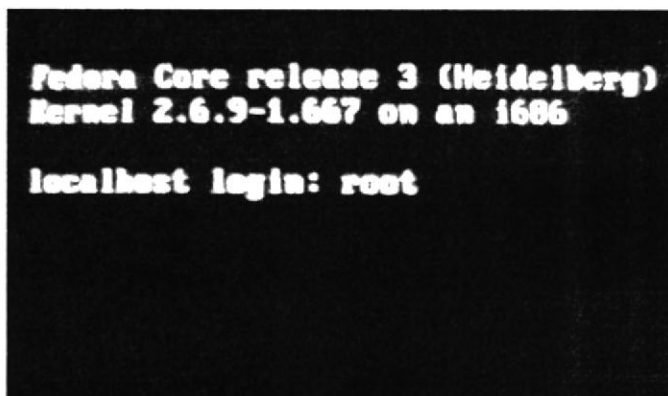


Figura 6-46: Ingreso root

Después de ingresar el usuario administrador root se debe ingresar la contraseña de root que se ha configurado en la instalación de linux.

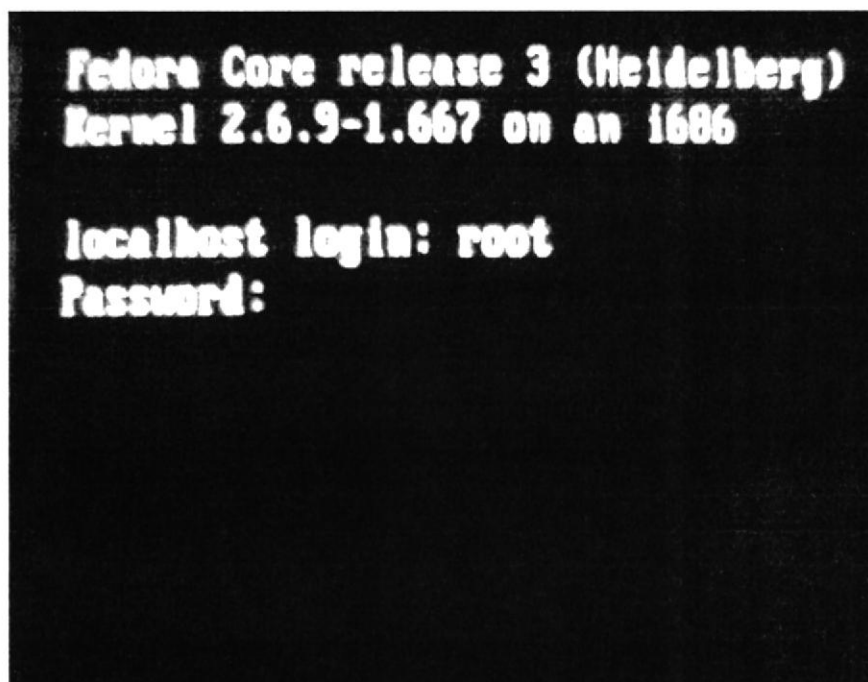


Figura 6-47: Ingreso la contraseña del root

Después de que ha ingresado la contraseña Linux se permitirá trabajar en modo texto.

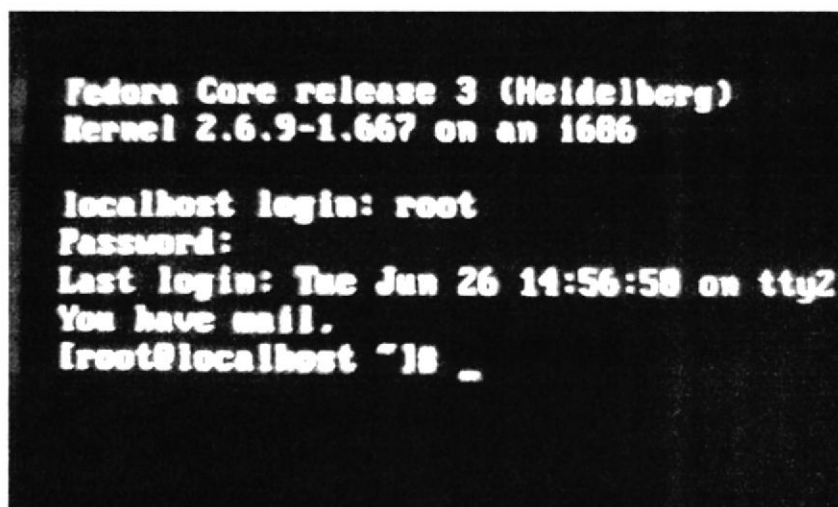


Figura 6-48: Ingreso a modo texto

6.10 COMANDOS DE LINUX

Aquí se explica comandos básicos de Linux que sirvan para las siguientes configuraciones que luego se utilizarán.

Nota: “[]” indica que son opcionales. “...” que puede ir más de una. Las opciones suelen comenzar con “-” o “--”. Si en la explicación del comando se acaba con “...” es porque hay muchas más opciones o información que es mejor consultar en la página del manual.

cd [directorio]

Descripción Cambia de directorio. Sin argumentos lleva al directorio del usuario (HOME). Si el directorio es “..” sube un nivel.

Propósito: ingresar a directorio

Sintaxis: root@localhost ~]# cd carpeta

Touch

Descripción Crea archivos en cualquier directorio

Propósito: Crear archivos

Sintaxis: root@localhost ~]# touch file

pwd

Descripción muestra el directorio actual de trabajo.

Propósito: mostrar directorio actual

Sintaxis: root@localhost ~]# pwd

La opción “-R” hace un listado recursivo en la jerarquía de directorios.

“/”

La ayuda, sirve para buscar una cadena, “q” para salir...

Redirecciones: > < |

Todos los comandos de GNU-Linux/Unix tienen asociado una “entrada estándar” (normalmente el teclado), una “salida estándar”, (normalmente la consola o pantalla) y una “salida estándar de error” (habitualmente la misma pantalla).

Es posible redireccionar esas entradas y salidas hacia un fichero o directamente a otro comando.



"comando ... > fichero": redirecciona la salida del comando hacia el fichero.

"comando ... < fichero": redirecciona la entrada y lee desde el fichero.

"|": La redirección "|" (tubería o "pipe) permite "entubar" las salidas a entradas de otros procesos evitando el uso de ficheros temporales y ejecución no sincronizada de comandos.

La concatenación de comandos es muy potente y típica de la filosofía de Unix y Linux. Por ejemplo:

mv [opciones...] fuente... destino

Descripción Cambia el nombre de un fichero por otro o mueve una serie de ficheros y directorios a un directorio destino.

Propósito: cambiar de destino los ficheros

Sintaxis: root@localhost ~]# mv carpeta cd/etc/carpeta

mkdir [opciones...] directorio

Descripción Crea el directorio con el nombre indicado.

Propósito: crear directorio

Sintaxis: root@localhost ~]# mkdir sitio

rmdir [opciones...] directorio...

Descripción Borra uno o varios directorios si están vacíos

Propósito: borrar directorios

Sintaxis: root@localhost ~]# rmdir sitio

rm [opciones...] ficheros

Descripción Borra ficheros.

Propósito: borrar

Sintaxis: root@localhost ~]# rm -f carpeta

Opciones

-f para forzar el borrado sin preguntar al usuario

-r pregunta antes de borrar

*****borra recursivamente todos los subdirectorios.

Utilidad que sirve para modificar ficheros de texto plano:

- pulse "i" para editar el fichero.
- pulse "ESCAPE", a continuación ":wq" e **INTRO** para guardar los cambios y cerrar el fichero.

passwd nombreusuario

Descripción Cambia la contraseña al usuario especificado

Propósito: cambia el password

Sintaxis: root@localhost ~]# passwd silvia

ifconfig

Descripción Muestra la IP del pc y la configuración de red

Propósito: muestra la ip actual del pc

Sintaxis: root@localhost ~]# ifconfig

ping host

Descripción Realiza ping entre pcs

Propósito: ver conectividad

Sintaxis: root@localhost ~]# ping 192.168.20.5

chown

Descripción Cambia el propietario del archivo nombre archivo a nombre usuario

Propósito: Cambiar de propietario

Sintaxis: root@localhost ~]# chown root:Silvia /carpeta

ifdown eth0

Descripción Para el servicio de red 'eth0'

ifup eth0

Descripción Arranca el servicio de red 'eth0' ifup eth0

ifconfig eth0 up

Propósito: levanta la red



Sintaxis: root@localhost ~]# ifconfig 192.168.20.3 up

ifconfig ath0 down

Propósito: Para caer la red

Sintaxis: root@localhost ~]# ifconfig 192.168.20.3 down

chmod

Descripción: Este comando, lo que hace , es poner un documento a su antojo de quien se desee que lo use, lo vea y ejecute. (Tiene que ser root para usar este comando)

Propósito: Cambia los permisos de archivos o carpetas especificadas.

Los permisos afectan a:

u : usuario (dueño)
g : grupo
o : otros
a : todos

Las opciones son:

+ : agrega permiso
- : quita permiso
= : asigna permiso

Los permisos son:

r : lectura
w : escritura
x : ejecución

Permisos de archivos en formato binario y octal.**Binario Octal Permisos**

000 0 ---
001 1 --x
010 2 -w-
011 3 -wx
100 4 r--
101 5 r-x
110 6 rw-
111 7 rwx



Sintaxis: `chmod [permisos] archivos ...`

cp

Descripción El comando `cp` copia archivos de carpeta a carpeta.

Propósito: copia archivos

Sintaxis: `root@localhost ~ ]# cp [opcion] archivo_fuente archivo_destino`
`cd [opcion] archivo1 archivo2 ... directorio_destino (2)`

Opciones:

- f:** Borrar los archivos de destino ya existentes
- p:** Preservar los permisos, el usuario y el grupo del archivo a copiar
- v:** Da información en pantalla sobre los archivos que se van copiando.

Ejemplo: `cp /root/Silvia/archivo.txt /root/Silvia.txt`

chgrp

Descripción: Con éste comando el root o administrador del sistema, como quieran llamarlo, puede cambiar el grupo al que pertenece cada usuario.

Propósito: cambiar el grupo al que pertenece uno o varios archivos

Sintaxis: `root@localhost ~ ]# chgrp [grupo] [archivo]`

Ejemplo: `chgrp otros quade.txt` (cambia quade.txt al grupo "otros")

deluser

Descripción: Con éste comando se podrá borrar usuarios al sistema. (Tiene que ser root)

Propósito: borrar usuarios

Ejemplo:

`root@localhost ~ ]# deluser Silvia`

netstat

Descripción: Con el comando netstat, se podrá pedir información acerca de los puertos de la máquina.

Propósito: Muestra las estadísticas del protocolo y conexiones TCP/IP actuales.

Opciones:

-a: Muestra todas las conexiones abiertas y puertos de escucha.

-e: Muestra estadística Ethernet. (Se puede combinar con -s)

-n: Muestra números de puertos y direcciones en formato numérico.

-s: Muestra conexiones del protocolo especificado por proto; que puede ser TCP o UDP e IP.

-r: Muestra el contenido de la tabla de rutas.

-S: Muestra estadísticas por protocolo. En forma predeterminada se muestra para TCP, UDP e IP.

-p se puede especificar el predeterminado)

Ejemplo: root@localhost ~]# netstat

file [opciones...] [ficheros...]

Descripción: Muestra información más detallados del tipo de contenido los ficheros.

Propósito: mostrar contenido de archivo

Ejemplo:

root@localhost ~]# File prueba



6.11 INFORMACIÓN DEL SISTEMA Y USUARIOS

date [opciones] [formato]

Descripción: Muestra (o cambia) la fecha y hora del sistema.

Propósito: muestra fecha del sistema

Ejemplo:

root@localhost ~]# Date

su [opciones] [usuario]

Descripción: Permite establecer una nueva sesión con otro usuario. Si no se especifica usuario lo hará con el "root".

Propósito: establece una nueva sesión

Ejemplo:

root@localhost ~]# su -silvia

mount [...]

Descripción: Sin argumentos muestra los sistemas de ficheros montados, su dispositivo correspondiente en /dev y en que directorio se han montado

Propósito: montar dispositivos

Ejemplo:

root@localhost ~]# mount /dev/hdb /media/cdroom/

passwd [opciones...] [usuario]

Descripción Permite cambiar la clave de acceso de un usuario. Si es el root, puede especificar el usuario del que desea cambiar la contraseña.

Propósito: cambia la clave

Ejemplo:

root@localhost ~]# Passwd silvia

6.12 DIRECTORIOS

slocate [opciones...] patrón

Busca nombres de ficheros que cumplan con el patrón en una base de datos que normalmente se actualiza cada día.

mail

Descripción: Con éste comando lo que se hace es mandar un mail a alguien

Propósito: manda y recibe mails

Sintaxis: mail [usuario1 usuario2...]

Ejemplo:

root@localhost ~]# mail Silvia@servipagos.com

zip

Descripción: Con éste comando se comprime archivos

Propósito: comprimir

Sintaxis: prueba.zip

Ejemplo:

root@localhost ~]# prueba.zip

gzip

Descripción: Con éste comando se descomprime archivos comprimidos

Propósito: descomprimir

Sintaxis: gzip prueba.txt

Ejemplo:

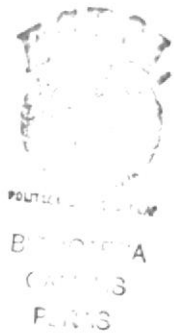
root@localhost ~]# gzip prueba.txt

etc

Descripción: Con éste comando se ve los archivos de configuración de sistema

Propósito: ver archivos de configuración

Sintaxis: etc



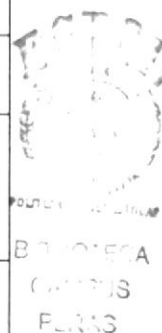
Ejemplo:

root@localhost ~]# cd /etc

6.13 ORGANIZACIÓN DE LOS DIRECTORIOS

Linux organiza la información en archivos, los cuales están contenidos en directorios. Un directorio puede contener subdirectorios, teniendo así una estructura jerárquica, como en cualquier otro sistema operativo.

Directorio	Descripción
/	Raíz (<i>root</i>), forma la base del sistema de archivos.
/boot	Archivos del kernel (compilados).
/bin	Archivos ejecutables esenciales para todos los usuarios.
/dev	Archivos de dispositivos.
/etc	Archivos de configuración.
/etc/rc.d	Archivos de inicialización (Red Hat).
/home	Generalmente, directorios de los usuarios.
/home/ftp	Contenido del servidor FTP.
/home/httpd	Contenido del servidor WWW.
lib	Librerías esenciales y módulos del kernel.
/mnt	Directorios donde ``montar" diversos dispositivos temporalmente.
/mnt/cdrom	Directorio donde se ``monta" el CD-ROM.
/mnt/floppy	Directorio donde se ``monta" el disquete.
/proc	Información sobre partes del sistema.
/root	Directorio del usuario principal del sistema.
/sbin	Archivos ejecutables para tareas de administración.
/tmp	Temporal.



/usr	Programas, documentación, fuentes,...compartidos por todo el sistema
/var	Archivos variables del sistema, bitácoras, temporales,...

Tabla 6-2: Directorios

6.14 LISTADO DIRECTORIOS COMANDOS BÁSICOS

COMANDOS	DESCRIPCION
ls	lista directorios y ficheros.
ls -i	lista directorios y ficheros con sus i-números.
ls -a	lista directorios y ficheros en orden alfabético
ls -s	lista directorios y ficheros con su tamaño en bloque (1 bloque= 512 bytes)
ls -r	lista directorios y ficheros en orden inverso.
ls -u	lista directorios y ficheros según último acceso
ls -l	lista todos los directorios y ficheros en formato largo

Tabla 6-3: Lista contenido de directorio

6.15 ARCHIVOS ESPECIALES

COMANDOS	DESCRIPCION
/etc/passwd	Contiene todos los logins y passwords
/etc/motd:	Mensaje del día
/etc/profile:	Se ejecuta al introducir al entrar en el sistema

Tabla 6-4: Lista Archivos especiales



6.16 SISTEMAS DE ARCHIVOS

El ext2 tiene un tamaño de i-nodo fijo entre 1 y 4K, independientemente del tamaño de la partición. El tamaño del i-nodo se selecciona al crear el sistema de archivos y es seleccionable por el usuario. El ext2 tiene una unidad similar al cluster, llamada bloque, y que es, por lo general de 1K, especificable por el usuario e independiente del tamaño de la partición, lo cual asegura un buen aprovechamiento del espacio libre con archivos pequeños.

El ext2 no usa una FAT, sino una tabla de i-nodos distribuidos en un número determinable de grupos a través de la superficie, lo cual permite balancear la distribución de los bloques de archivos en la superficie a través de dichos grupos para asegurar la mínima fragmentación.

El ext2 tiene un límite máximo de 4GB de archivo, pero no limita el tamaño máximo de la partición a 4GB, como es el caso de la FAT.

El ext2 tiene soporte para detección de un sistema de archivos desmontado incorrectamente cuando el sistema se apaga de forma errónea, y capacidad para autorecuperarlo en caso de fallo accidental.

El ext2 mantiene información de la última vez que se montó y se accedió al volumen (sistema de archivos), así como del número de veces que se ha montado dicho volumen desde la última comprobación automática, así como la fecha en la que se comprobó su integridad por última vez.

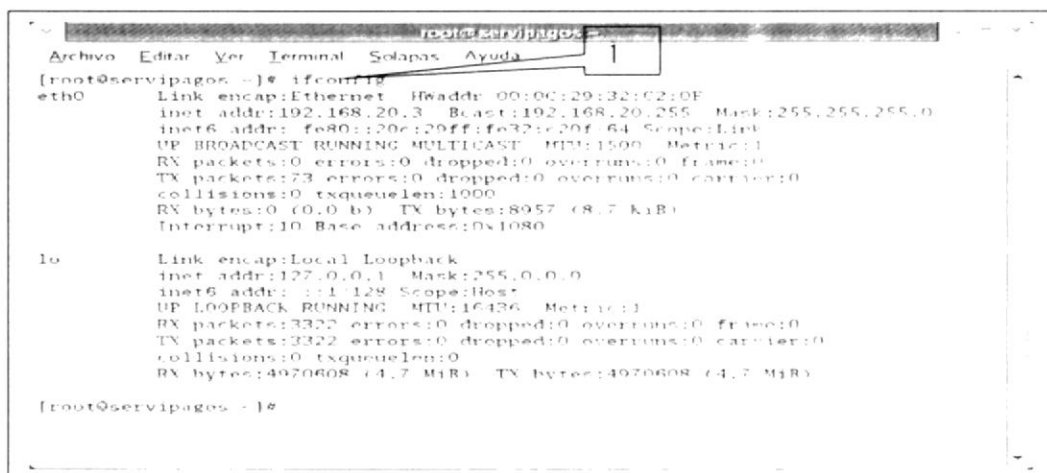


6.17 CONFIGURACIÓN STANDAR PARA CUALQUIER SERVICIO

6.17.1. CONFIGURACIÓN DE LA TRAJETA DE RED MODO TEXTO

Es necesario configurar la tarjeta de red para las configuraciones que se van a utilizar.

Paso 1 se verifica si está configurada la tarjeta de red con el comando `ifconfig`, este comando muestra la dirección IP que tiene EL servidor.



```
root@servipagos ~
Archivo Editar Ver Terminal Solapas Ayuda
[root@servipagos ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:32:C2:0F
          inet addr:192.168.20.3  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:c20f 64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:8057 (8.7 KiB)
          Interrupt:10 Base address:0x1080

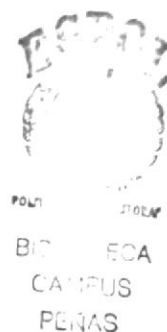
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1:128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3322 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3322 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4970608 (4.7 MiB)  TX bytes:4970608 (4.7 MiB)

[root@servipagos ~]#
```

Figura 6-49: configuración de la tarjeta de red

Eth0.- significa que es la tarjeta de red, se visualiza la dirección ip que en este caso es 192.168.20.3

Lo.- significa la dirección de loopback que es 127.0.0.1



Paso 2 Si no esta configurada la tarjeta de red se configura con las siguientes líneas.

Ifconfig eth0 192.168.20.3 up

Ifconfig Muestra la IP del pc y la configuración de red

Eth0: Tarjeta de red **192.168.20.3** dirección de la tarjeta de red **up** levantar servicio



Figura 6-50: levantamiento de la tarjeta de red

6.17.2. CONFIGURACIÓN DE LA TARJETA DE RED MODO GRÁFICO

Paso 1 Otra forma de configurar la tarjeta de red es de manera de la interfaz grafica, con el comando **"setup"**.

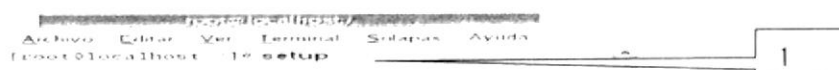


Figura 6-51: ingreso al setup

Paso 2 saldrá la siguiente pantalla, se ubica en la opción de **"Configuración de la red"** **Paso 3** se presiona el botón de **"Ejecutar una Herramienta"**

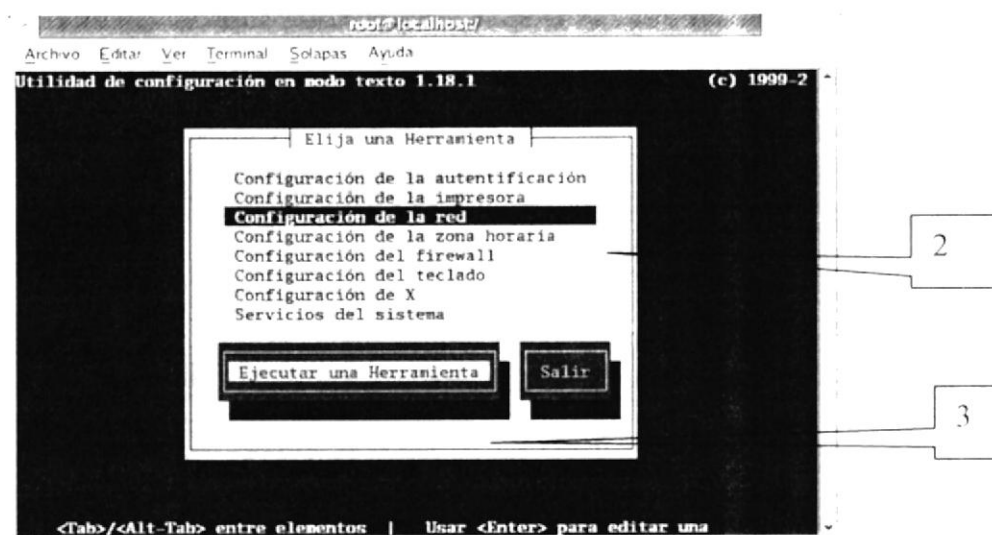


Figura 6-52: configuración de la red

Paso 4 La siguiente pantalla, se pregunta si se desea configurar la tarjeta de red. En este caso se selecciona **"Si"**, el cual permite continuar, caso contrario se sale de la configuración.

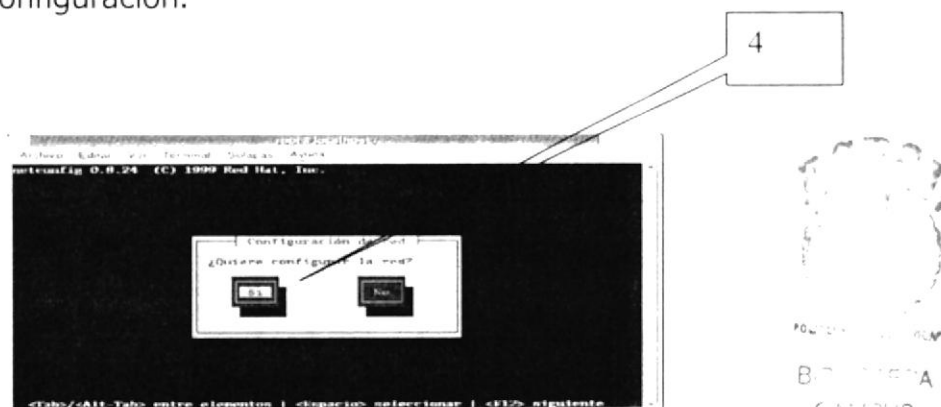


Figura 6-53: confirmación de configuración

Paso 5 se ingresa la dirección IP y máscara de red, las opciones de puerta de enlace y servidor de nombres primario aparecen automáticamente pero si uno desea la puede modificar.

Paso 6 se presiona "OK" para finalizar la configuración.

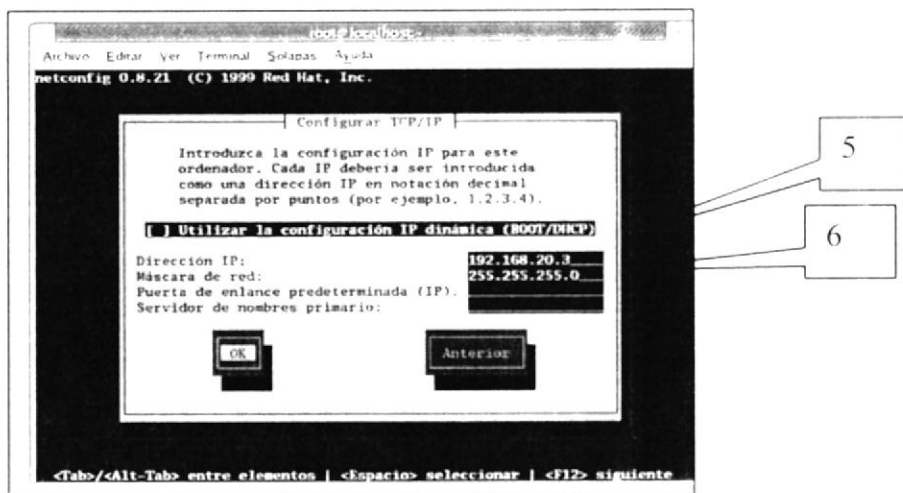


Figura 6-54: configuración tcp/ip

Paso 7 Se debe reiniciar el servicio luego de haber configurado la tarjeta de red de la siguiente manera:



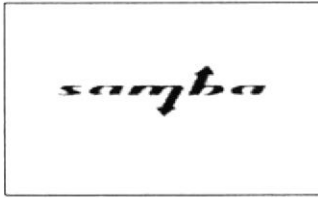
Figura 6-55: levantamiento de tarjeta red

SERVICE NETWORK START

service nombre_servicio start Inicia el servicio especificado
"nombre_servicio"

OK.- Significa que la configuración realizada ha sido exitosa

6.18 SERVIDOR SAMBA



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

Samba es la idea de Andrew Tridgell. El proyecto nació en 1991 cuando Andrew creó un programa servidor de ficheros para su red local, que soportaba un raro protocolo DEC de Digital Pathworks. Hoy, la suite Samba implica a un par de demonios que proporcionan recursos compartidos a clientes SMB sobre la red (las particiones son denominadas a veces también como servicios).

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

6.19 SERVICIOS DE SAMBA

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



6.20 DEMONIOS DE SAMBA

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

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

Samba se encuentra actualmente mantenido y es ampliado por un grupo de voluntarios bajo la supervisión activa de Andrew Tridgell. Al igual que el sistema operativo Linux, Samba es considerado por sus autores Open Source software (OSS), y es distribuido bajo la the GNU General Public License (GPL). Como información adicional, se puede afirmar que es algo verdaderamente testimonial el que entidades tanto comerciales como no comerciales estén dispuestas a gastar dinero para dar soporte a un proyecto Open Source.

Microsoft también ha contribuido materialmente poniendo a disposición su definición de SMB y del Internet-savvy Common Internet File System (CIFS), como Public Request for Comments (RFC), y otros documentos estandar. El protocolo CIFS es el nuevo nombre de las futuras versiones del protocolo SMB que serán usadas en los productos Windows. De hecho, se puede encontrar el protocolo escrito como "SMB/CIFS".

6.20.1. QUÉ HACE SAMBA DESDE CLIENTE

Como se explicó antes, Samba puede ayudar a las máquinas Windows y Unix a coexistir en la misma red. Sin embargo, existen algunas razones específicas por las cuales podrías desear instalar un servidor Samba en nuestra red:

- No querer pagar licencias para un servidor Windows NT o 2000/2003 Server (en adelante servidor NT) para obtener las funcionalidades que este proporciona.
- Querer proporcionar un área común para datos o directorios de usuarios en orden a realizar una transición desde un servidor NT hacia un Unix, o viceversa.
- Querer compartir impresoras a entre clientes Windows y Unix.
- Facilitar acceso a ficheros NT desde un servidor Unix.

6.20.2. SAMBA. VISIÓN DESDE SERVIDOR.

Como se menciona antes, Samba actualmente contiene varios programas que sirven para diferentes pero determinados propósitos. Se va a introducir una breve explicación de cada uno de ellos. La mayoría de los programas que vienen con la distribución de Samba se centran en sus dos demonios. Echer un vistazo a las responsabilidades de cada demonio:

smbd

El demonio `smbd` es responsable de manejar los recursos compartidos entre la máquina servidora Samba y sus clientes. Proporciona servicios de archivos, impresión y visualización a los clientes SMB a través de una o más redes. `smbd` controla todas las notificaciones entre el servidor Samba y los clientes de red. Además, es responsable de la autenticación de usuarios, bloqueo de recursos y la compartición de datos a través del protocolo SMB.

nmbd

El demonio `nmbd` es un sencillo servidor de nombres que imita la funcionalidad de los servidores WINS y de resolución de nombres NetBIOS. Este demonio está a la escucha de peticiones para el servidor de nombres y proporciona la información apropiada cuando se le llama. También proporciona listas de visualización del Entorno de Red y participa en las elecciones de los visualizadores.

La distribución de Samba también está acompañada por un pequeño grupo de herramientas tipo línea de comandos Unix:

smbclient

Un cliente tipo FTP Unix que puede ser usado para conectar a recursos compartidos por Samba.

smbtar

Un programa para realizar copias de seguridad de datos sitos en los recursos compartidos, similar al comando Unix `"tar"`.

nmblookup

Un programa que proporciona búsquedas de nombres NetBIOS sobre TCP/IP.

smbpasswd

Un programa que permite a un administrador cambiar las passwords encriptadas usadas por Samba.

smbstatus

Un programa para reportar las conexiones de red actuales hacia los recursos compartidos por el servidor Samba.

testparm

Un simple programa para validar el fichero de configuración de Samba.

testprns

Un programa que testea si varias impresoras son reconocidas por el demonio smbd.

6.20.3. OBJETIVO

Compartir uno o varios sistemas de archivos

Compartir uno o varios sistemas de archivos distribuidos

Compartir impresoras instaladas en el servidor entre los clientes Windows de la red

Autenticar a los clientes que ingresan en un dominio Windows

6.20.4. ESQUEMA SAMBA

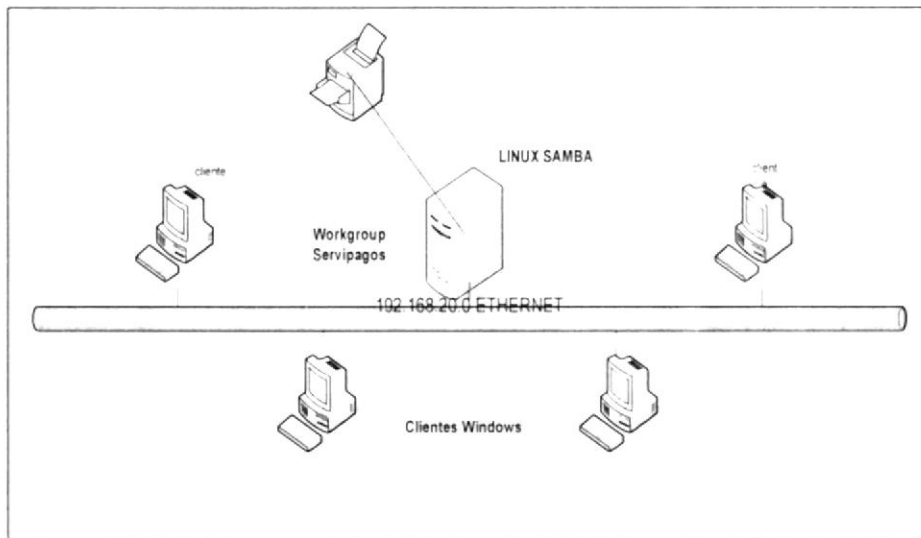


Figura 6-56: entorno samba

6.21 CONFIGURACIÓN DEL SERVIDOR SAMBA EN LINUX

A continuación realizar los siguientes pasos para la configuración de Samba.

Paso 1 Verificar si el paquete de samba está instalado de la siguiente manera:
Rpm -qa samba.-

rpm:Verifica paquetes instalados -q nombre_paquete:Samba

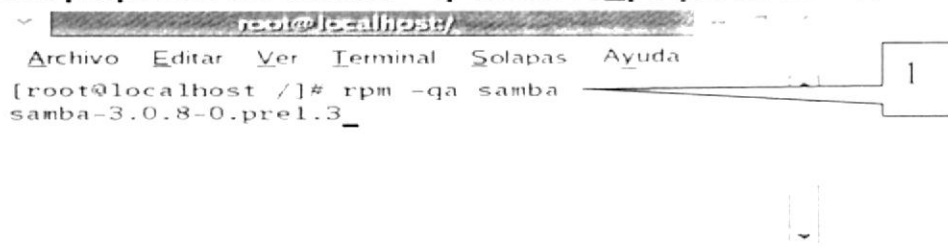


Figura 6-57: verificación de paquete

Paso 2 se editael archivo smb.conf, que se encuentra en la siguiente ruta:

Cd /etc/ En el directorio raíz se guardan todos los servicios instalados en el equipo, accediendo a este directorio.

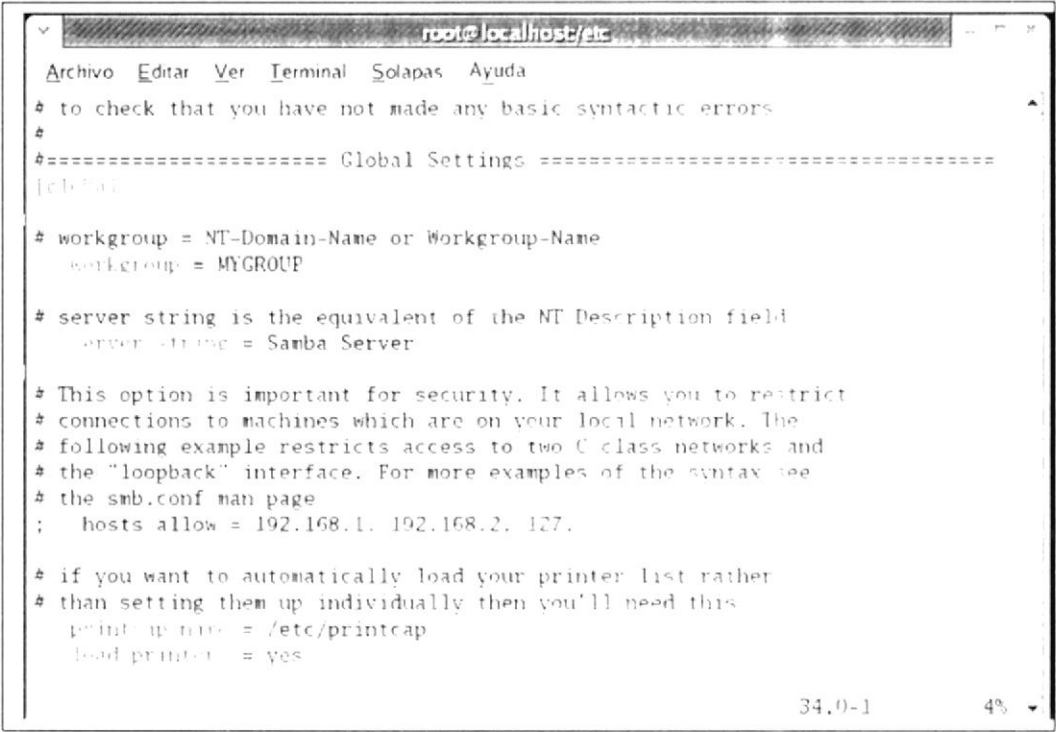
Ingresar a la configuración de samba a editar con el siguiente comando

Vi samba/smb.conf : Ingresar a editar la configuración del servicio samba



Figura 6-58: Editor de Samba

Los cambios se realizan en la sección **Global Settings**, como se lo detalla en esta pantalla. Así esta por primera vez en el sistema



```
root@localhost:/etc
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# to check that you have not made any basic syntactic errors
#
#===== Global Settings =====
[global]

# workgroup = NT-Domain-Name or Workgroup-Name
#                workgroup = MYGROUP

# server string is the equivalent of the NT Description field
#                server string = Samba Server

# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
#                hosts allow = 192.168.1. 192.168.2. 127.

# if you want to automatically load your printer list rather
# than setting them up individually then you'll need this
#                printcap name = /etc/printcap
#                load printers = yes

34,0-1  4%
```

Figura 6-59: global settings

Realizar los siguientes cambios en GLOBAL SETTINGS

GLOBAL SETTINGS Define los parámetros de Samba a nivel global del servidor así como los parámetros que se establecerán por defectos en el resto de las secciones.

Paso 1 En **WORKGROUP**, se escribe el grupo de trabajo del que el servidor Samba hace parte.



```
root@localhost:/etc
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# to check that you have not made any basic syntactic errors
#
#===== Global Settings =====
[global]

# workgroup = NT-Domain-Name or Workgroup-Name
#                workgroup = MYGROUP

# server string is the equivalent of the NT Description field
#                server string = Samba Server

# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
#                hosts allow = 192.168.1. 192.168.2. 127.

# if you want to automatically load your printer list rather
# than setting them up individually then you'll need this
#                printcap name = /etc/printcap
#                load printers = yes

INSERTAR  11,1
```

Figura 6-60: cambios en global settings

Paso 2 El campo **NETBIOS NAME**, permite definir el nombre de la máquina, no como un nombre de DNS, sino como un nombre de resolución de nombres propio del protocolo NetBIOS. Es importante entender que son dos cosas totalmente diferentes.

Paso 3 El campo **SERVER STRING** define el nombre con el cual se lo va a encontrar en windows

Paso 4 El campo **HOSTS ALLOW** lista de los ordenadores que se permite acceder

Paso 5 Buscar las siguientes líneas (ver cuadro rojo)

`encrypt passwords=yes`

`Smb passwd file= /etc/samba/smbpasswd`

Se encuentran deshabilitadas

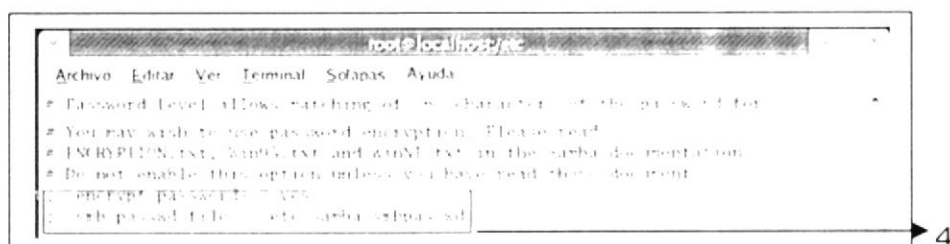


Figura 6-61: encriptación de claves

Habilitar el encriptamiento de las claves (ver cuadro rojo) figura 55

encrypt passwords=yes se habilita el encriptamiento de las claves

Smb passwd file= /etc/samba/smbpasswd Aquí es donde se guardarán las claves de samba

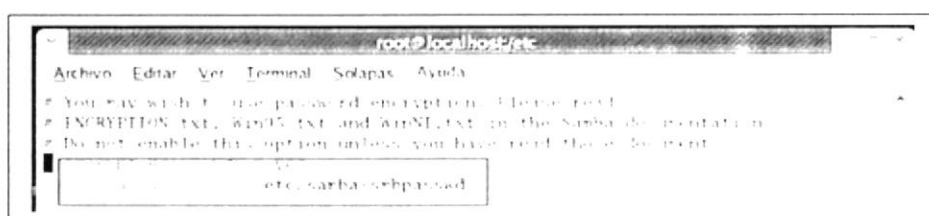
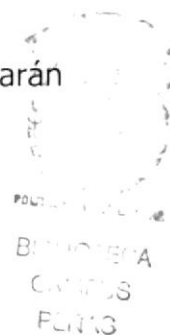


Figura 6-62: descomentamos el encriptación



Paso 6 se ubica en la sección de **Share Definitions** para hacer los siguientes cambios:

HOMES Define automáticamente un recurso de red por cada usuario conocido por samba. Este recurso esta por defecto asociado al directorio de conexión de cada usuario en el ordenador en el que Samba está instalado.
Así es la apariencia por primera vez antes de realizar las configuraciones necesarias



Figura 6-63: share definitions sin cambios

Realizar los siguientes cambios

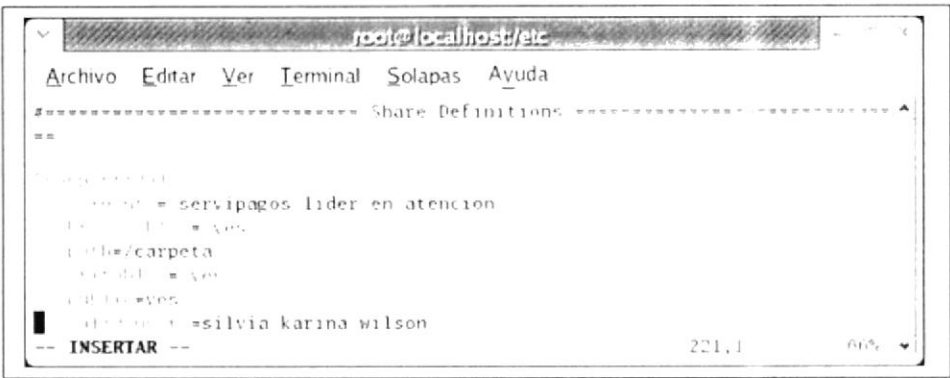


Figura 6-64: cambios realizados en share definitions

Comment Descripción del servicio

browseable El servicio aparece en la lista de recursos

path: Directorio asociado al servicio

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

Public para que sea pública, en caso de poner **NO** es para limitar el acceso a ciertos usuarios.

Añadir **valid users** lista de usuarios que pueden acceder a ese recurso.

En su ausencia, el recurso es accesible por todos los usuarios del servidor Samba. Si esta línea esta presente el acceso esta reservado únicamente a los usuarios mencionados.

Paso 7 Grabar los cambios con presionando **SHIFT:wq**

":wq" e **INTRO** para guardar los cambios y cerrar el fichero.

Paso 8 Crear la carpeta con el **comando mkdir** en la ruta que se especifica y editar de la siguiente manera ej:

medir respaldo.txt.- carpeta creada con extencion txt en la ruta de etc

mkdir nombredirectorio : Crea un directorio
mkdir respaldo.txt

Paso 9 ingresar a la carpeta para escribir un mensaje con **vi carpeta.txt** escribir y guardar

Vi carpeta.txt Editar el archivo creado

Paso 10 Grabar los cambios con presionando **SHIFT:wq**

":wq" e **INTRO** para guardar los cambios y cerrar el fichero.

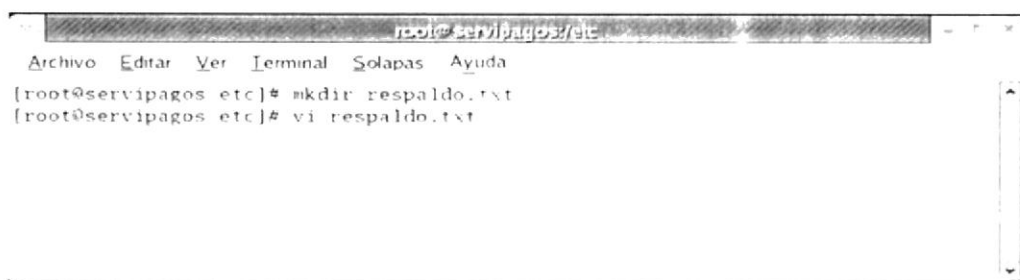


Figura 6-65: Creación de la carpeta de respaldo

ls Lista los ficheros de un directorio concreto

Paso 11 Escribir el comando **ls** y ver que está creada el archivo carpeta, como propietario tiene al root cambiar el propietario para poder acceder con otros usuarios.

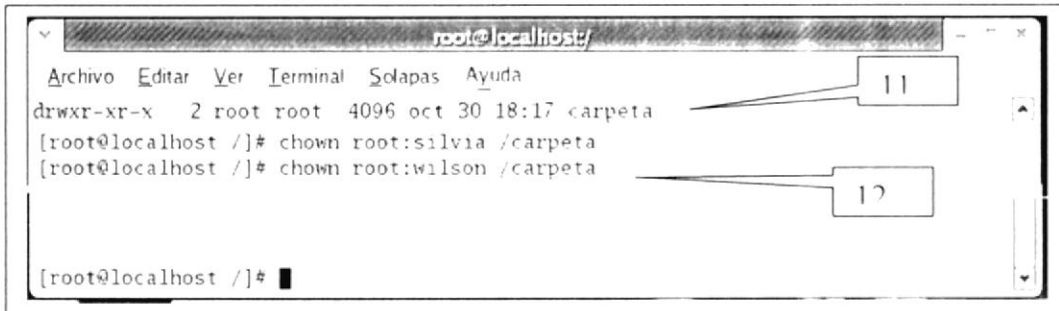


Figura 6-66: cambio de propietario

Paso 12 Realizar cambio de propietario con el siguiente comando ej: `chown root:slvia /carpeta`

Explicación:

CHOWN ROOT:SILVIA /CARPETA

Cambia el propietario del archivo nombre archivo a nombre usuario

Paso 13 Crear los usuarios validos para el Servidor Samba

adduser <nombre_usuario>

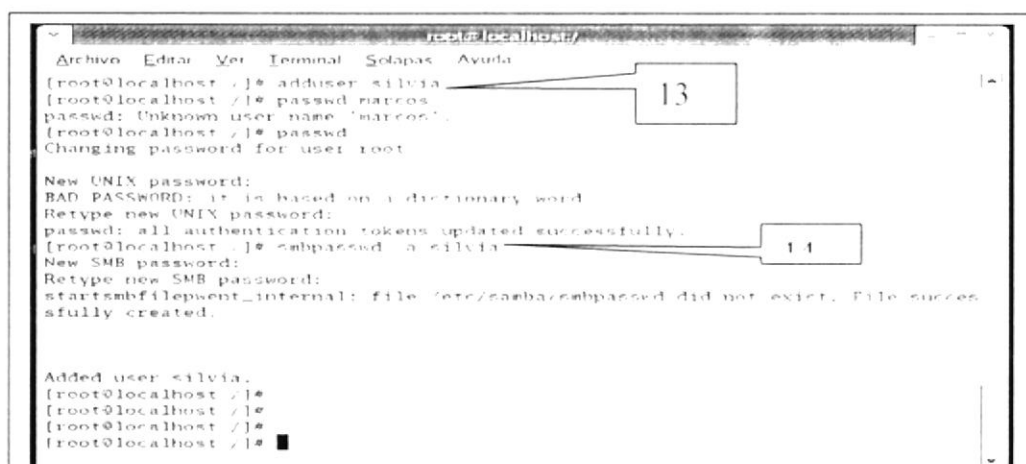
Al crear un usuario le pedirá una contraseña por cada usuario que se valla a crear

Passwd Cambia la clave de acceso para el usuario actual. Root puede cambiar la clave de cualquier usuario `passwd usuario`

Adduser silvia

passwd <contraseña>

passwd *****

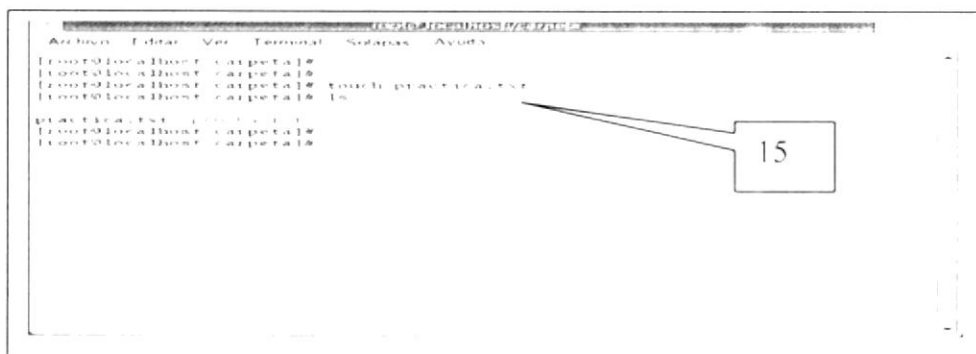
Paso 14 Convertir el usuario de samba a un usuario de windows**Figura 6-67: creación de usuarios****smbpasswd**

Un programa que permite a un administrador cambiar las passwords encriptadas usadas por Samba.

Paso 15 Ingresar carpeta para crear el archivo prueba.txt de la siguiente manera

Ej: Touch practica.txt

Touch: Crear archivos **nombre archivo** practica.txt

**Figura 6-68: creación de archivo práctica**

Paso 16 Se da los permisos necesarios a carpeta con el comando **chmod +777 /respaldo.txt**

chmod permisos fichero/directorio: Cambia los permisos de ficheros/directorios

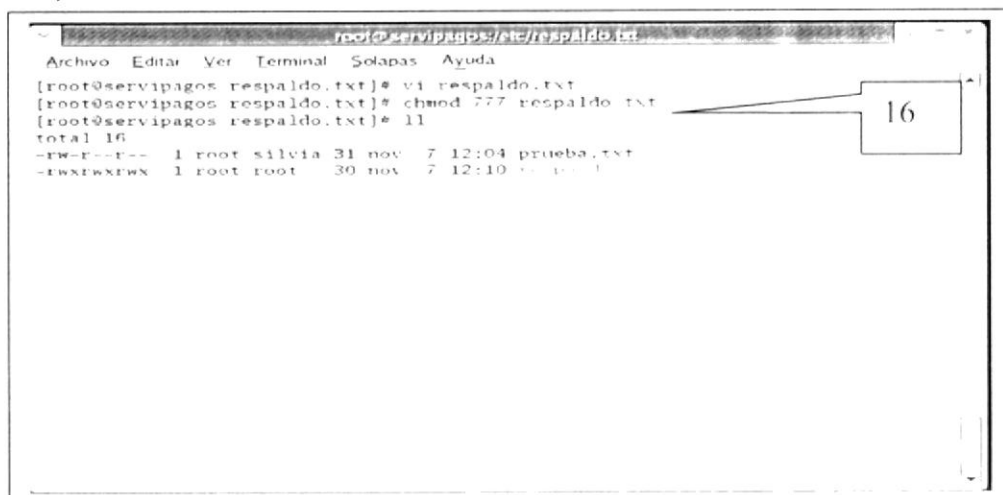


Figura 6-69: permisos a la carpeta

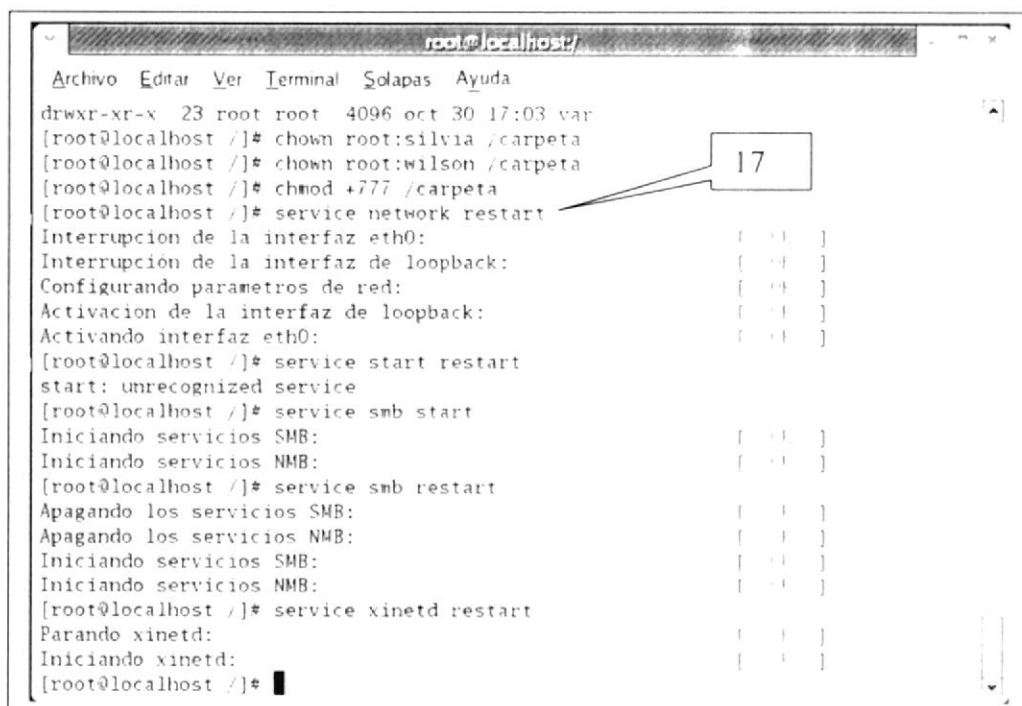
RW-USUARIO **R-** -GRUPO USUARIO **R-** -OTRO USUARIO **1** ENLACE FISICO

777=R-READ PESO = 4 **W-WRITE PESO = 2** **X-EJECUCION PESO =1**

Paso 17 Reiniciar los Servicios para levantar **SAMBA** con los comando **service smb Start**, **service Smb restart**, **service xinetd restart**, levantar tarjeta **service network restart**

service nombre_servicio start Inicia el servicio especificado "nombre_servicio"

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

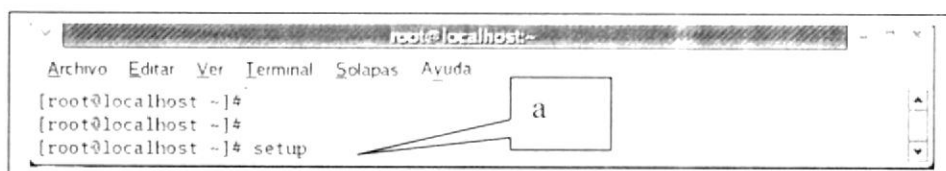


```
root@localhost/~
Archivo Editar Ver Terminal Solapas Ayuda
drwxr-xr-x 23 root root 4096 oct 30 17:03 var
[root@localhost /]# chown root:silvia /carpeta
[root@localhost /]# chown root:wilson /carpeta
[root@localhost /]# chmod +777 /carpeta
[root@localhost /]# service network restart
Interrupcion de la interfaz eth0: [  OK  ]
Interrupción de la interfaz de loopback: [  OK  ]
Configurando parametros de red: [  OK  ]
Activacion de la interfaz de loopback: [  OK  ]
Activando interfaz eth0: [  OK  ]
[root@localhost /]# service start restart
start: unrecognized service
[root@localhost /]# service smb start
Iniciando servicios SMB: [  OK  ]
Iniciando servicios NMB: [  OK  ]
[root@localhost /]# service smb restart
Apagando los servicios SMB: [  OK  ]
Apagando los servicios NMB: [  OK  ]
Iniciando servicios SMB: [  OK  ]
Iniciando servicios NMB: [  OK  ]
[root@localhost /]# service xinetd restart
Parando xinetd: [  OK  ]
Iniciando xinetd: [  OK  ]
[root@localhost /]#
```

Figura 6-70: levantamiento del servicio samba

Nota: Para que arranque los servicios de Servidor al inicializar el computador realizar los siguientes pasos

Paso a) Si se tiene problemas en levantar Samba ingresar al **setup**



```
root@localhost/~
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# setup
```

Figura 6-71: ingreso al setup

Paso b) Elegir **Servicio del Sistema** presionar **enter**



Figura 6-72: ingreso al servicio de sistema

- c) Ingresar a esta pantalla, con las teclas direccionales buscar **SMB**.
d) elegir y presionar la barra espaciadora dar **OK**.

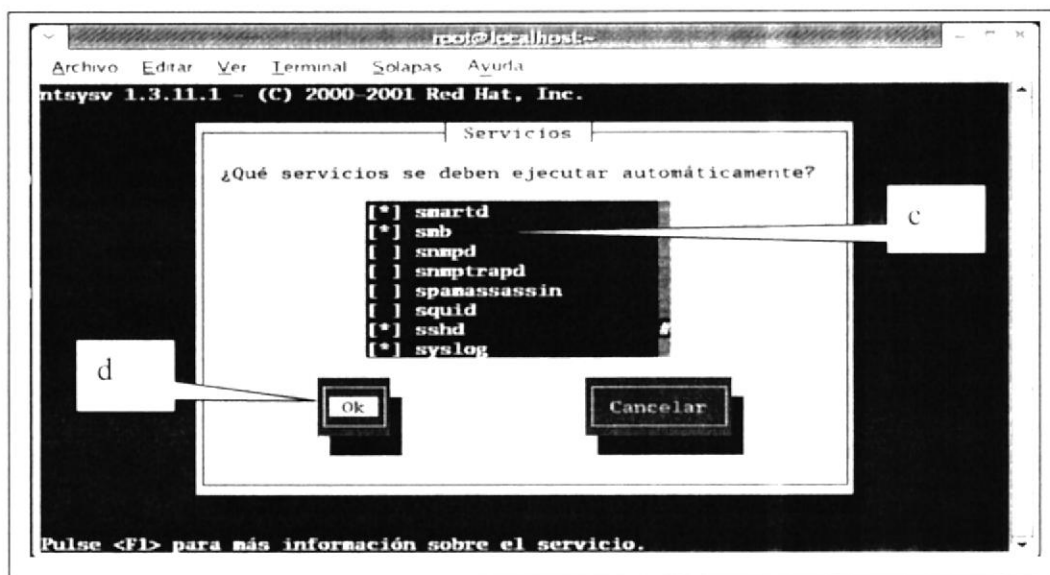


Figura 6-73: elección de paquete smb

6.22 CONFIGURACIÓN EN EL CLIENTE WINDOWS

Paso 18 Ingresar a Ejecutar ingresando con la dirección ip del servidor

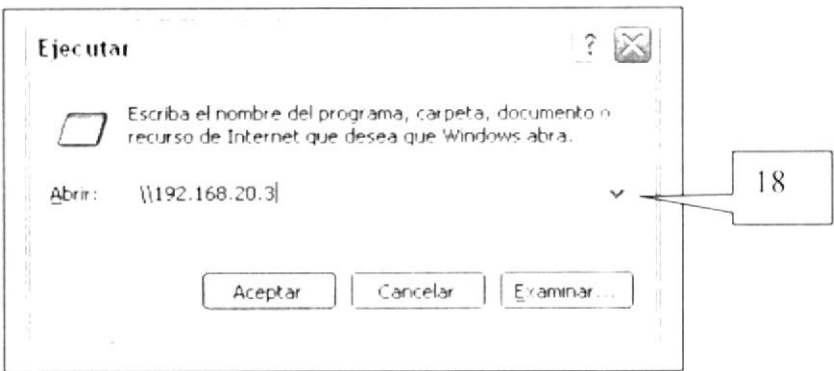


Figura 6-74: ejecutar en el cliente

Paso 19 Ingresar con el usuario que se crea en Linux el cual se le da permiso para visualizarse en Windows

Usuario Silvia
Contraseña *****



Figura 6-75: ingreso de usuario creado en servidor samba

Paso 20 Ingresar directo a la red que se tiene y visualizar **compartida** es la carpeta que se crea en Linux para compartir con Windows

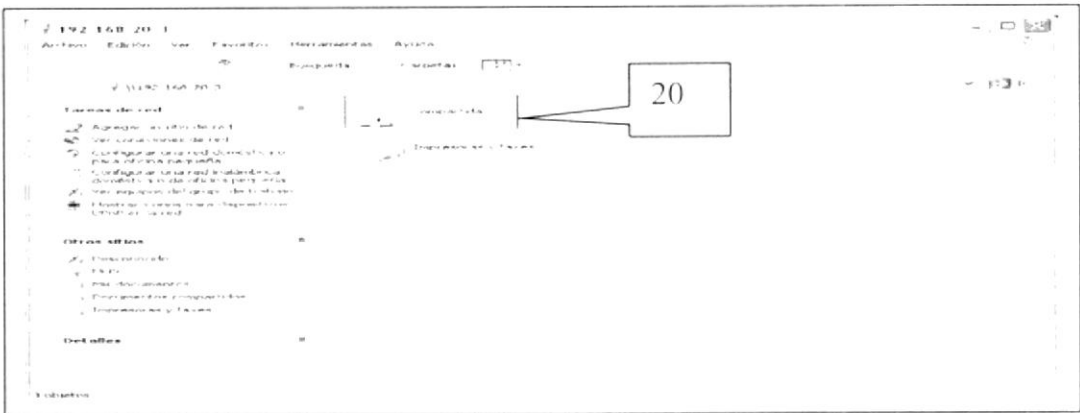


Figura 6-76: ingreso a la carpeta

Paso 21 Ingresar a la carpeta **COMPARTIDA** que se creo en Linux y se podrá visualizarse el archivo respaldo

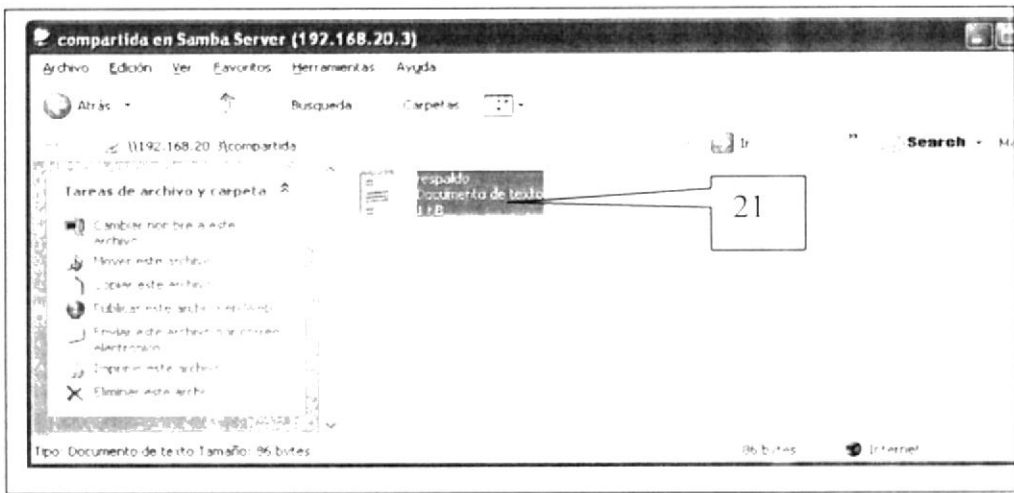


Figura 6-77: Archivo creado en Linux

Paso 22 Ingreso de Archivo **RESPALDO** creado en Linux

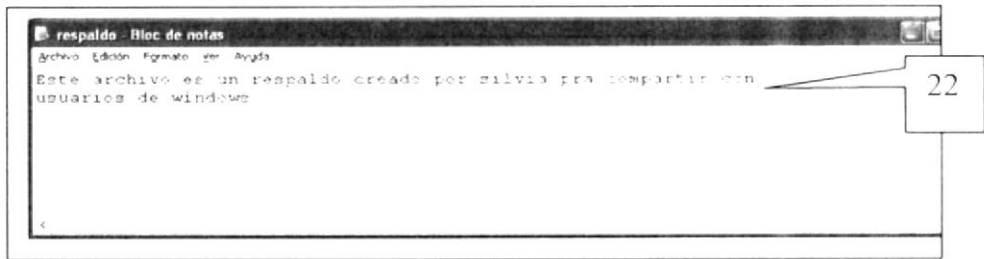


Figura 6-78: Ingreso al archivo respaldo

6.23 SERVIDOR DNS

El DNS organiza los nombres de máquina (hostname) en una jerarquía de dominios. Un *dominio* es una colección de nodos relacionados de alguna forma—porque estén en la misma red, tal como los nodos de una universidad—. Por ejemplo, las universidades americanas se agrupan en el dominio edu. Cada universidad tiene allí un *subdominio*, tal como la universidad Groucho Marx, que posee el subdominio groucho.edu. A su vez, se puede encontrar nuevos subdominios dentro, como el Departamento de Matemáticas (maths). Finalmente, un nodo de ese departamento llamado erdos tendrá un nombre completo (conocido como totalmente cualificado) tal como erdos.maths.groucho.edu. Este nombre totalmente cualificado también se conoce por las siglas FQDN. En Figura 70 se ve una parte del espacio de nombres. La raíz del árbol, que se identifica con un punto sencillo, es lo que se denomina *dominio raíz* y es el origen de todos los dominios. Para indicar que un nombre es FQDN, a veces se termina su escritura en un punto. Este punto significa que el último componente del nombre es el dominio raíz.

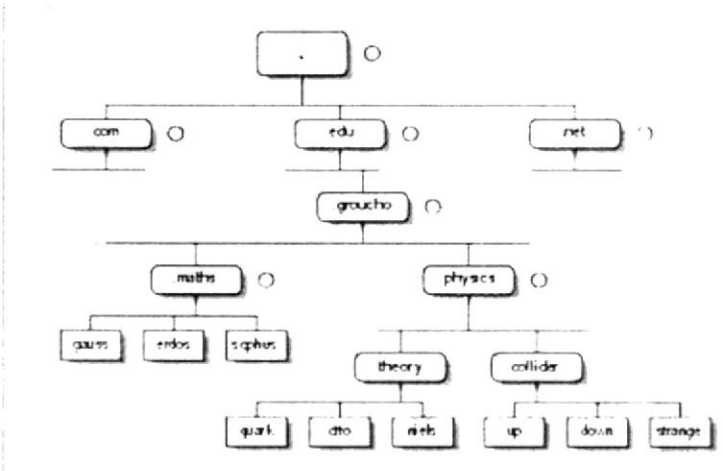


Figura 6-79: raíz del árbol



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

Dominio	Descripción
Edu	Instituciones universitarias, casi todas norteamericanas.
com	Organizaciones comerciales.
org	Organizaciones no comerciales. Las redes privadas UUCP suelen estar en este dominio.
net	Pasarelas y otras redes administrativas.
mil	El ejército norteamericano.
gov	El gobierno norteamericano.
uucp	Dominio para redes UUCP.

Tabla 6-5: Raíz del árbol

6.23.1. BÚSQUEDAS CON DNS

Se verá ahora la parte más ingeniosa del DNS. La idea es que si se desee buscar la dirección IP del sistema erdos, DNS pensará, "Preguntar a la gente que lo maneja, y lo dirá."

De hecho, el DNS es como una gigantesca base de datos distribuida. Está realizada a través de los llamados servidores de nombres, que proporcionan la información de uno o varios dominios. Para cada zona, debe haber dos o más servidores de nombres capaces de responder por ella. Para obtener la dirección IP de erdos, todo lo que se necesita es contactar con el servidor de nombres de la zona groucho.edu y obtendrá los datos solicitados.

¿Cómo se llega al servidor de nombres de la Universidad Groucho Marx? En el caso de que el ordenador no esté equipado con un oráculo de resolución de direcciones, el DNS lo hace también. Cuando la aplicación quiera buscar la información de erdos, contactará con un servidor de nombres local, quien lleva a cabo una secuencia de peticiones. En primer lugar pregunta al servidor de nombres raíz, preguntando por erdos.maths.groucho.edu. El servidor raíz reconoce que el nombre no pertenece a ninguna de sus zonas de autoridad pero sí sabe qué hacer con la zona edu. Esto es, devuelve a el servidor más información sobre los servidores de nombres que pueden servir la zona edu. Ahora el servidor preguntará por este nombre a uno de esos servidores. Ellos enviarán a uno que tenga información autorizada del dominio groucho.edu. Ahora el servidor interrogará a éste y finalmente obtendrá la dirección de erdos.

Aparentemente la búsqueda de una dirección IP supone mucho tráfico, sin embargo es minúsculo si se lo compara con la consulta de un gigantesco fichero HOSTS.TXT. Aun así hay técnicas para mejorar el rendimiento.

Para acelerar futuras peticiones de nombres, el servidor almacena la información obtenida en la búsqueda anterior en su caché local. Así, la próxima vez que se busque algún nodo de groucho.edu, ya no habrá que ir a los servidores raíz o los de la zona edu.

Por supuesto, el servidor de nombres no almacenará para siempre la información en la caché; la limpiará cada cierto tiempo. El tiempo de vida se llama TTL (del inglés time to live). En cada zona DNS el administrador asigna un valor de TTL.



6.23.2. TIPOS DE SERVIDORES DE NOMBRES

Los servidores de nombres que mantienen oficialmente la información de una zona se conocen como autorizados de la zona, y a veces se conocen como servidores principales o maestros. Cualquier petición de nodos de esa zona irá a parar a uno de estos servidores principales.

Los servidores principales deben estar bien sincronizados. Es decir, uno de ellos será llamado primario, que carga su información de un fichero, y hacer a los demás secundarios, que obtienen su información pidiéndosela periódicamente al primario.

El objetivo de tener varios servidores principales es distribuir la carga y dar cierta tolerancia a fallos. Cuando uno de los servidores principales falla, todas las peticiones acabarán en los demás. Por supuesto, este esquema no protege de fallos del servidor que produzcan errores en todas las peticiones DNS, como podrían ser errores del software.

También se puede instalar un servidor de nombres que no es maestro de ninguna zona.[3] Esto es útil, para dar servicio de nombres a una red local aprovechando sus características de ahorro de ancho de banda gracias a su caché. Estos servidores se conocen como de sólo-caché.

6.23.3. LA BASE DE DATOS DNS

Se ha visto que el DNS no sólo sabe de direcciones IP de máquinas, pero también almacena otras informaciones.

Cada unidad de información del DNS se llama Registro de Recurso (RR). Cada registro tiene un tipo asociado que describe el dato que contiene, y una clase que especifica el tipo de red al que se aplica. Esto último se adapta a diferentes esquemas de dirección, como direcciones IP (la clase IN), direcciones Hesiod (utilizadas por el sistema Kerberos del MIT) y algunas más. El RR típico es el registro A, que asocia un nombre completamente cualificado con una dirección IP.

Un nodo puede ser conocido por más de un nombre. Por ejemplo, se puede tener un servidor que proporciona tanto servicio FTP como WWW, y tendrá dos nombres: ftp.máquinass.org y www.máquinass.org. Sin embargo, uno de estos nombres debe ser identificado como oficial o canónico. La diferencia es que el canónico es el único registro A que debe existir apuntando a esa dirección IP, mientras que el resto de los nombres deben ser alias (registros CNAME), que apuntan al nombre canónico.

No se van a revisar todos los tipos de RR aquí, pero se verá algún ejemplo más amplio. En Ejemplo 6-4 se ve una parte de la base de datos DNS que está cargada en los servidores de nombres para la zona physics.groucho.edu.

DNS es el Domain Name System (Sistema de Nombres de Dominio), las reglas de nomenclatura de las máquinas y el software que mapea los nombres a números IP. Una conversión es simplemente una asociación entre dos cosas, en este caso un nombre de máquina, como ftp.linux.org y el número IP de la máquina, 192.168.20.3

Comenzar con un servidor caching only server Servidor que se limita a guardar en una caché las IPs de los nombres de máquina más solicitados, obteniéndolas de servidores externos. , y se continuará con la configuración de un servidor DNS primario para un dominio.

DNS es una base de datos cuyo ámbito es la Red. Mantenga su DNS limpia y consistente y conseguirá un buen servicio de ella. Aprenda a usarla, administrarla, depurarla y será otro buen administrador, salvando a la red de caer sobre sus rodillas sobrecargada por falta de mantenimiento.

Para que su máquina pueda ser encontrada por otros ordenadores en Internet, es necesaria que sea referenciada por su dirección IP.

6.23.4. OBJETIVO DEL DNS

Configurar búsquedas de clientes por nombre y resolver problemas con el servidor de almacenamiento de nombres dedicado.

Demostrar entendimiento del registro de dominio y proceso de traducción del DNS.

Traducir (resolver) los nombres de una máquina (y dominio) a direcciones IP utilizadas en Internet es el trabajo de máquinas que ofrecen el servicio de nombres de dominio (DNS).

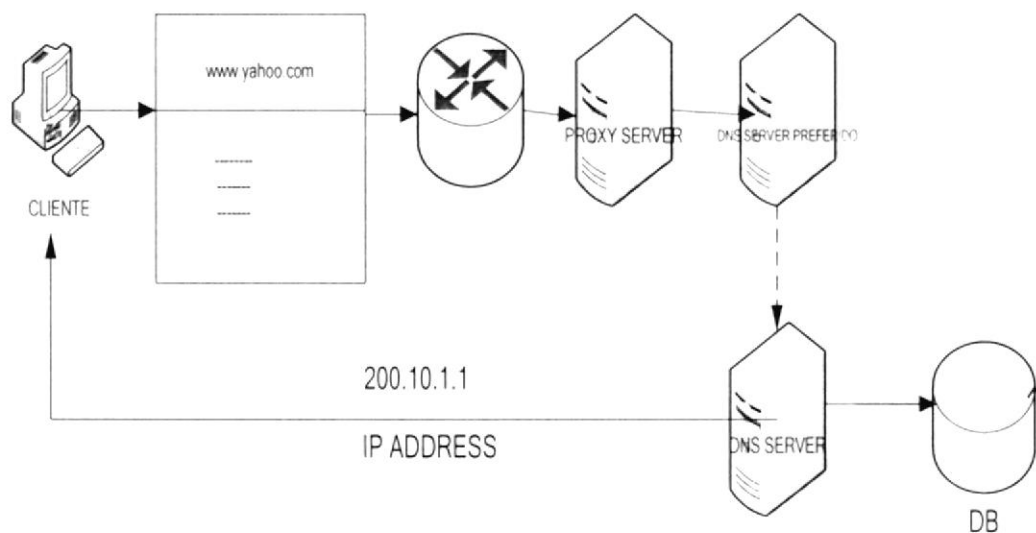


Figura 6-80: Gráfico del DNS

6.23.5. APLICACIONES DE DNS

Muchas implementaciones de DNS proporcionan tres utilidades bastante comunes para consultar a servidores de nombres:

Host: Obtiene una dirección IP asociada con un nombre de host o un nombre de host asociado con una dirección IP.

Nslookup: Permite localizar información acerca de los nodos de red, examinar los contenidos de la base de datos de un servidor de nombres y establecer la accesibilidad a servidores de nombres.

DIG ("Domain Internet Groper"): Permite probar los servidores de nombres, reunir grandes volúmenes de información de nombres de dominio y ejecutar simples consultas de nombres de dominio.

6.23.6. BENEFICIOS

Conveniencia: Nombres conocidos por el usuario son más fácil de recordar que sus respectivas direcciones IP.

Consistencia: Las direcciones IP pueden cambiar pero los nombres permanecen constantes.

Simplicidad: Usuarios necesitan aprender solo un nombre para encontrar recursos ya sea en Internet o en una Intranet.



6.24 CONFIGURACIÓN DEL SERVICIO DNS EN LINUX

A continuación realizar los siguientes pasos para la configuración de DNS .

Paso 1 Verificar si el paquete named esta instalado de la siguiente manera:

rpm:Verifica paquetes instalados -q nombre_paquete: bind

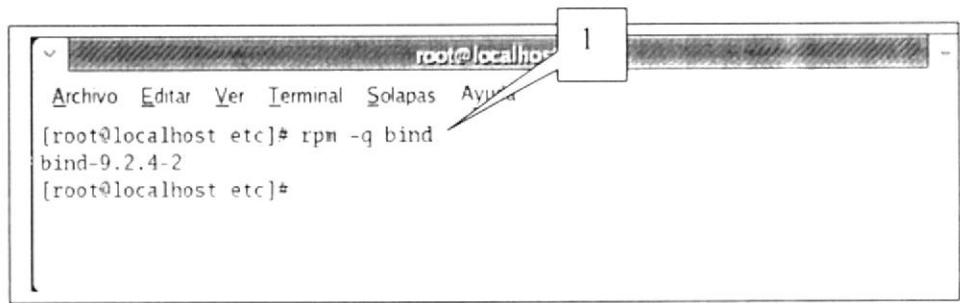


Figura 6-81: verificación de paquete bind

Paso 2 Ingresar a editarlo como se muestra en la pantalla

Vi named.conf : editar el servicio de dns

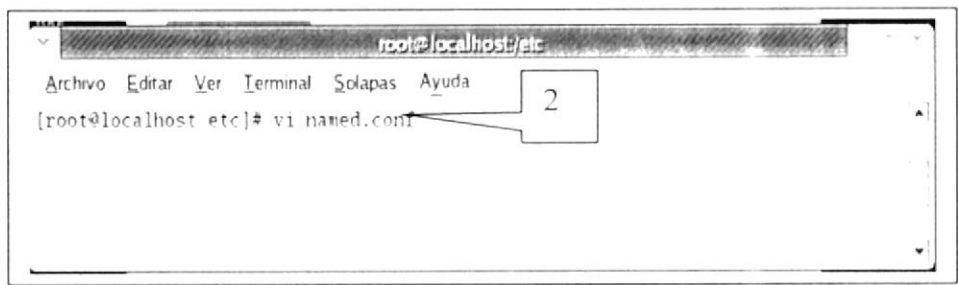


Figura 6-82: editar configuración de zona

Paso 3 Ingresar a las configuraciones de zona por primera vez luce así copiar la zona de local host presionando **"y"** y el numero de líneas a copiar este caso son **5** y se pega con **v**

Escribir la zona nueva en este caso será la de **servipagos**

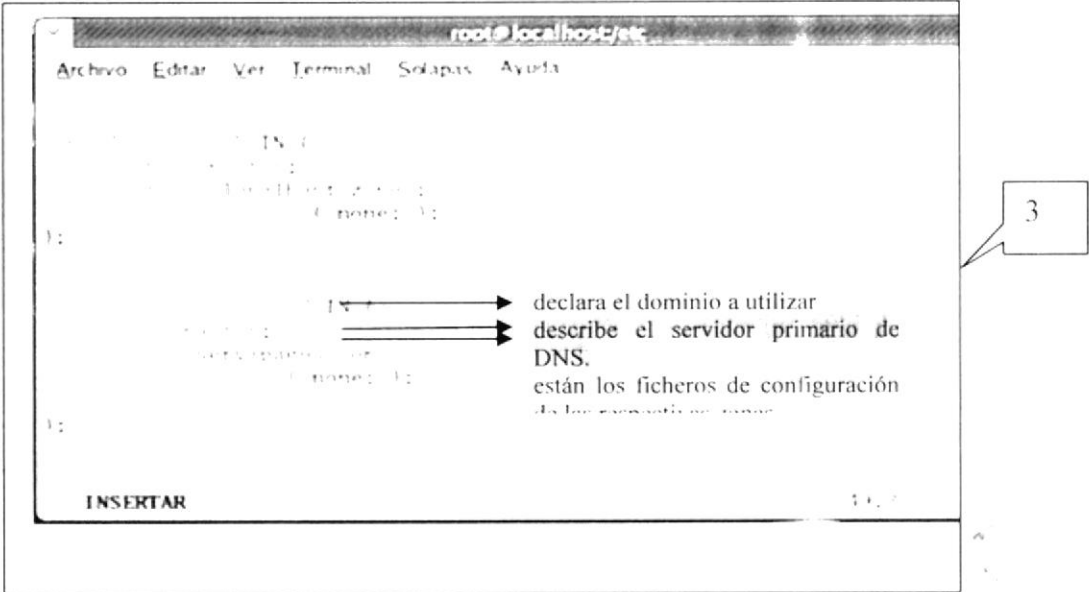


Figura 6-83: cambios en zona

Explicación de los campos de la zona de servipagos

- Zone** .- declara el dominio a utilizar
- Type Master** .- quiere decir que eso describe el servidor primario de DNS.
- File** .- están los ficheros de configuración de las respectivas zonas

Paso 4 Grabar los cambios con presionando **SHIFT:wq**

":wq" e **INTRO** para guardar los cambios y cerrar el fichero.

Después de configurar el named.conf, se procede a ejecutar los siguientes comandos:

Paso 5 `Cd /var/named/chroot/var/named/` es donde se guarda el dominio que se ha creado.

cd [ruta exacta o relativa].

var/ : Directorio que contiene archivos de administración y datos históricos del sistema

named : directorio del paquete bind

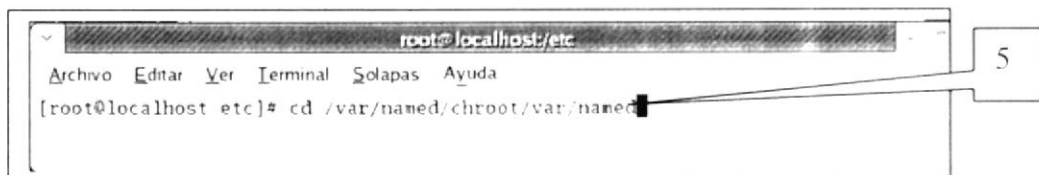


Figura 6-84: ingreso al var/named

Paso 6 Copiar la zona creada de servipagos en la de localhost.zone de la siguiente manera

cp [ruta del archivo a copiar] [directorio en donde se desea copiar]

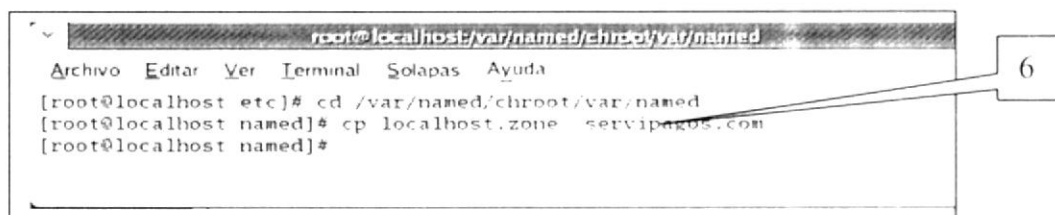


Figura 6-85: copia de configuración a localhost

Paso 7 Escribir el comando **ls** para visualizar la zonas que están creadas, aparecerá servipagos

ls Lista los ficheros y directorios de la ubicación actual

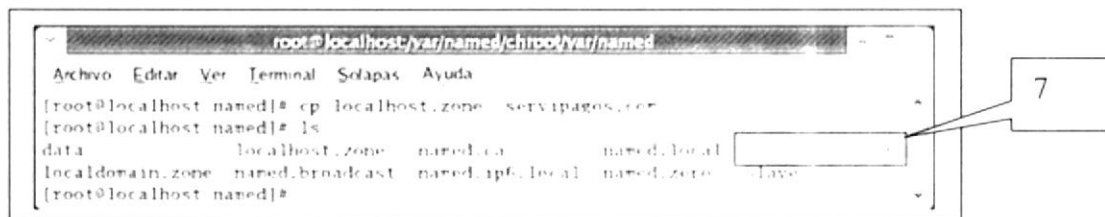


Figura 6-86: visualización de la zona servipagos

Paso 8 Editar el archivo (**vi SERVIPAGOS.COM**) para modificarlo y configurar el dominio, siguiendo el siguiente forma:

Vi Utilidad que sirve para modificar ficheros de texto plano:

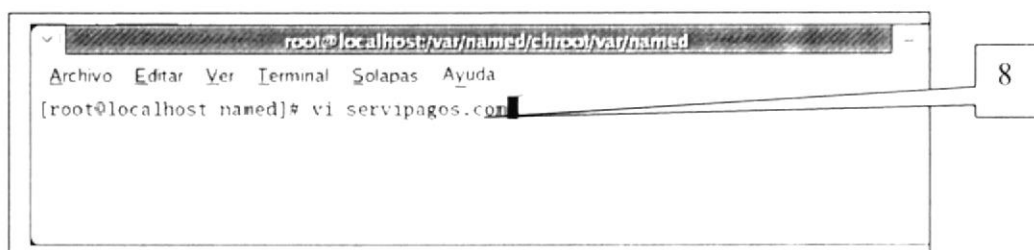


Figura 6-87: editar zona servipagos

El archivo que se presenta sin editar es el siguiente, se lo explicará de la siguiente forma:

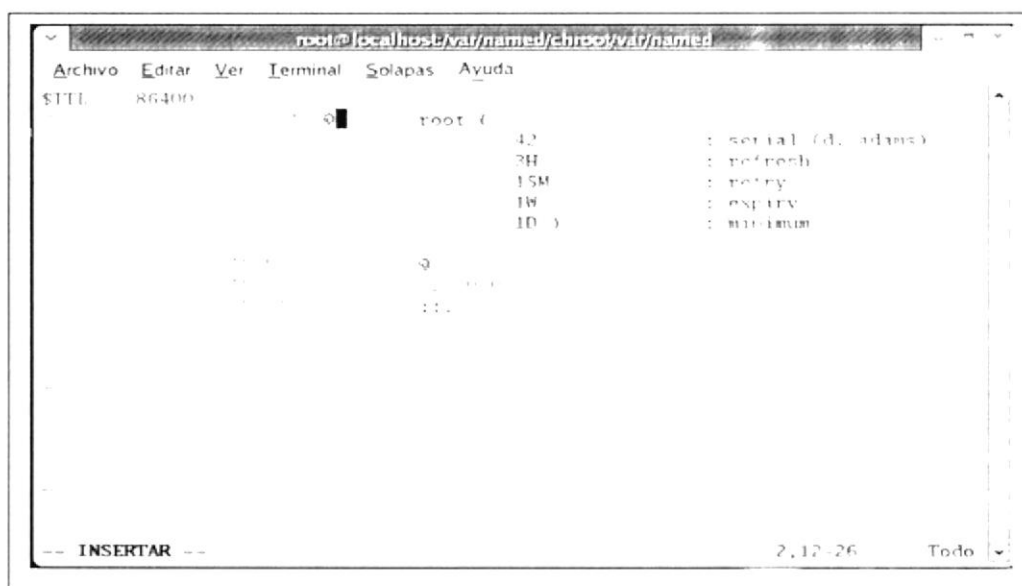


Figura 6-88: sin cambios en configuración de zona

- a) SOA.-** Marca el principio de la zona de autoridad (dominio, dirección del responsable de zona, numero de serie.....)
- b) NS.-** Apunta a una posición específica del servidor de nombres
- c) A.-** Especifica la dirección real IP

- d) **CNAME.-** El nombre canónico para un alias
- e) **@.-** Al principio de línea de los archivos de zona indica que no se necesita nombre.



Figura 6-89: cambios en zona servipagos

Editar el archivo con el dominio que se valla a crear, en este caso va hacer de servipagos.com y los demás detalles, tal como se presenta en la siguiente pantalla:

Paso 9 Copiar la zona creada en la ruta donde se guarda los dominios

cp archivo1 servipagos.com.zone archivo2 /var/named/chroot
Realiza una copia de un fichero

var/: Directorio que contiene archivos de administración y datos históricos del sistema

named : directorio del paquete bind

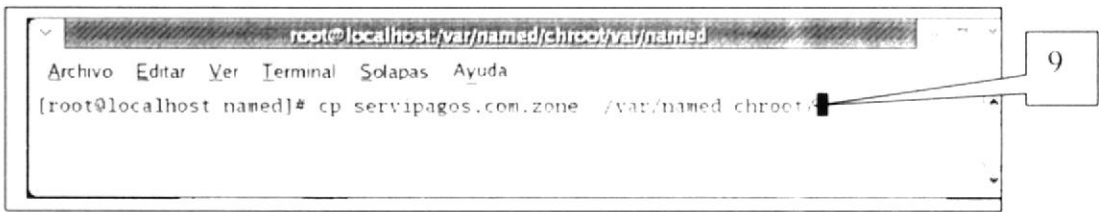


Figura 6-90: copia de zona servipagos

Paso 10 Editar el fichero resolv.conf. Su ruta exacta debe de estar en /etc/resolv.conf

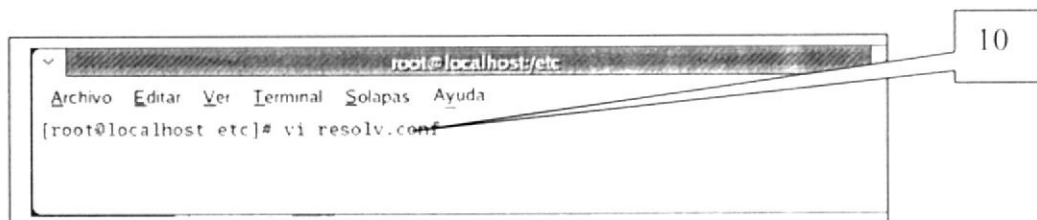


Figura 6-91: editar resolv

Paso 10.1 Esto es lo que debe aparecer en el fichero para poder navegar correctamente.

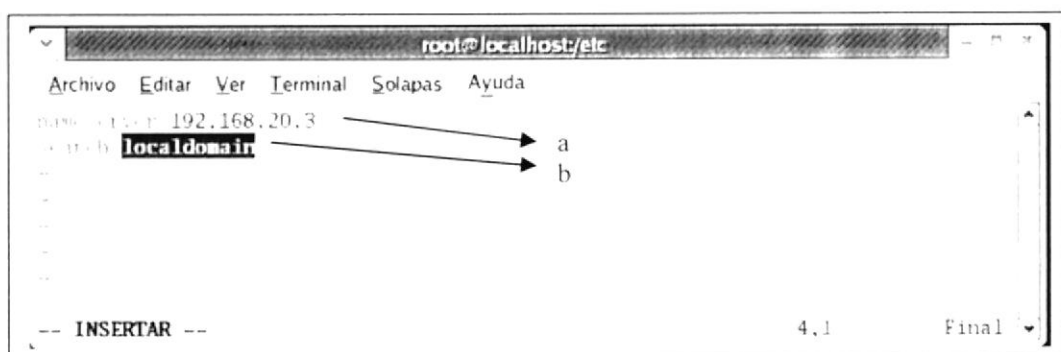


Figura 6-92: cambios en resolv

a) La línea `nameserver` especifica la dirección de su servidor de nombres, en este caso su propia máquina, ya que es ahí donde named se estará ejecutando. Si quiere una lista de varios servidores ponga una línea nameserver para cada uno.

b) La línea `search` especifica en qué dominios se buscaría para cualquier nombre de máquina a la que quiera conectar.

Paso 11 se ha configurado el DNS, restaurar los servicios, de la siguiente manera:

Service named Start , Service named restart, service named satus

service nombre_servicio start Inicia el servicio especificado
"nombre_servicio"

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

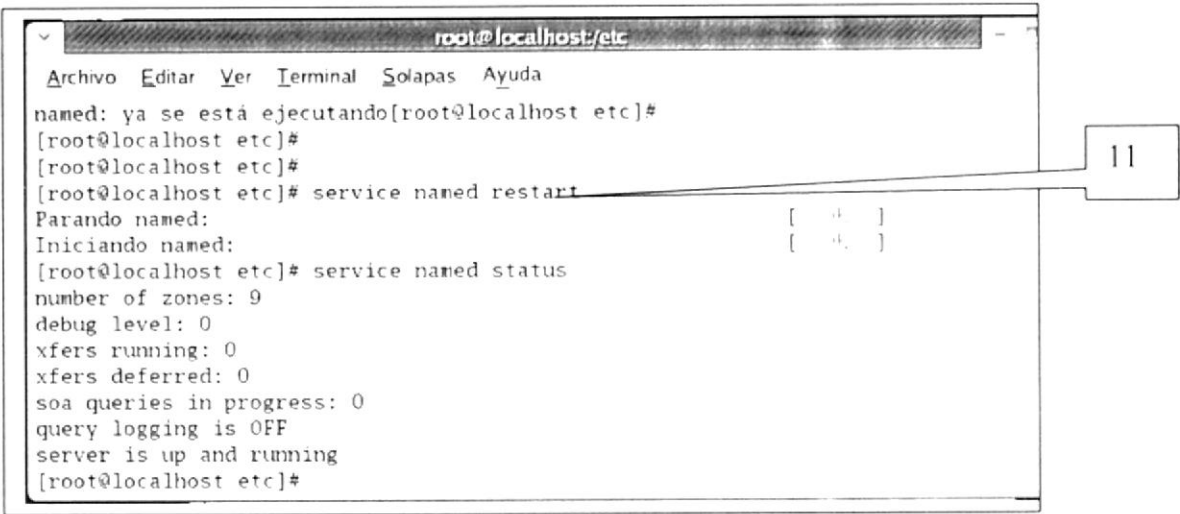


Figura 6-93: levantamiento del server named

Paso 12 Comprobar haciendo ping a el dominio www.servipagos.com

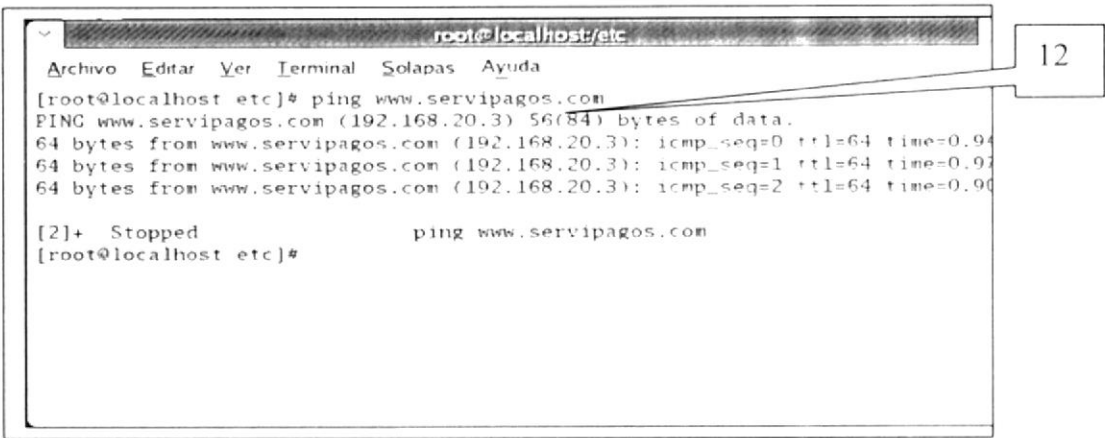


Figura 6-95: ping a www.servipagos.com

Nota: Para que arranque los servicios de Servidor al inicializar el computador realizar los siguientes pasos

a) Si no se tiene respuestas ingresar al setup

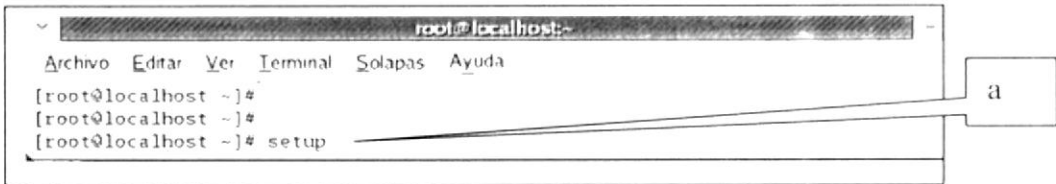


Figura 6-96: ingreso del setup

b) Elegir la opción de **SERVICIOS DE SISTEMA**

Figura 6-97: ingreso del servicio de sistema

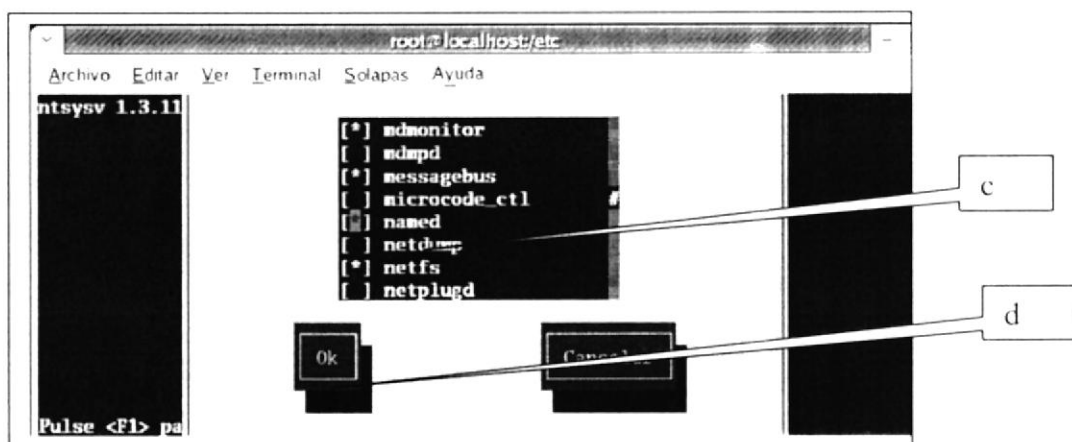
c) Ingresar a esta pantalla, Y con las teclas direccionales buscar **NAMED**d) elegir Y presionando la barra espaciadora dar **OK**

Figura 6-98: elección de servicio named

6.25 CONFIGURACIÓN EN EL CLIENTE WINDOWS

En el lado del cliente realizar las siguientes configuraciones:

Paso 13 Ingresar en Mis Sitios de Red, dar un clic derecho

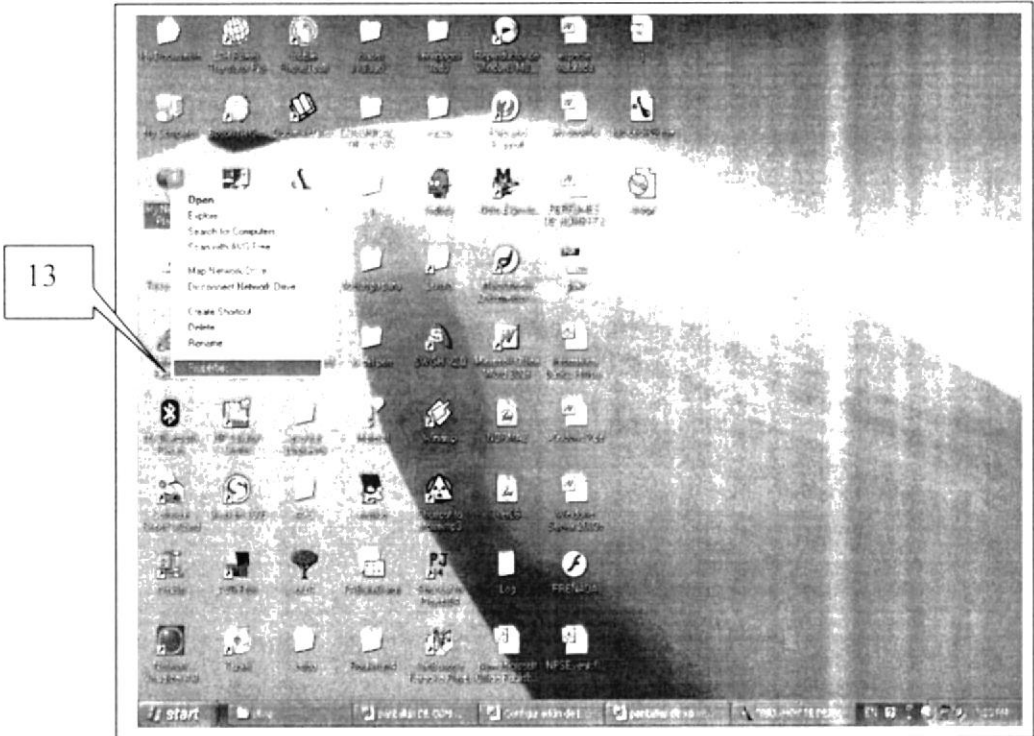


Figura 6-99: ingreso de las propiedades de la red

Paso 14 Ingresar a la red de área local dar clic derecho

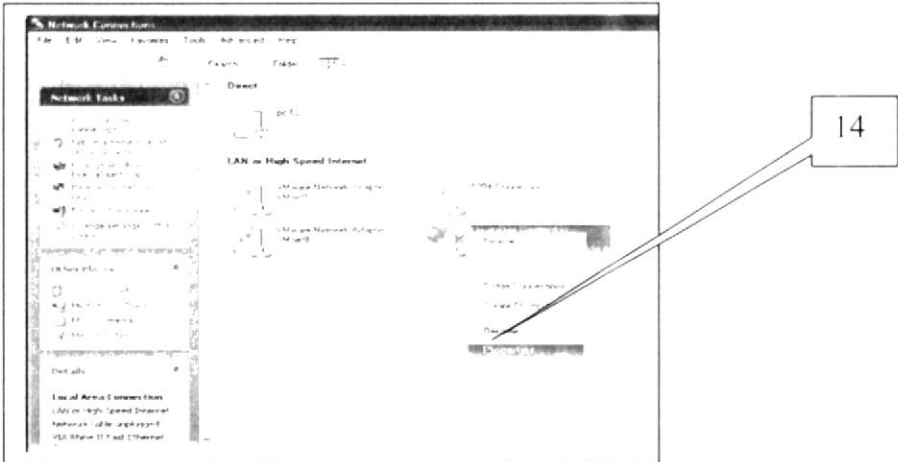


Figura 6-100: ingreso de las propiedades de area local

Paso 15 Ingresar en las **Propiedades** de INTERNET PROTOCOL TCP/IP

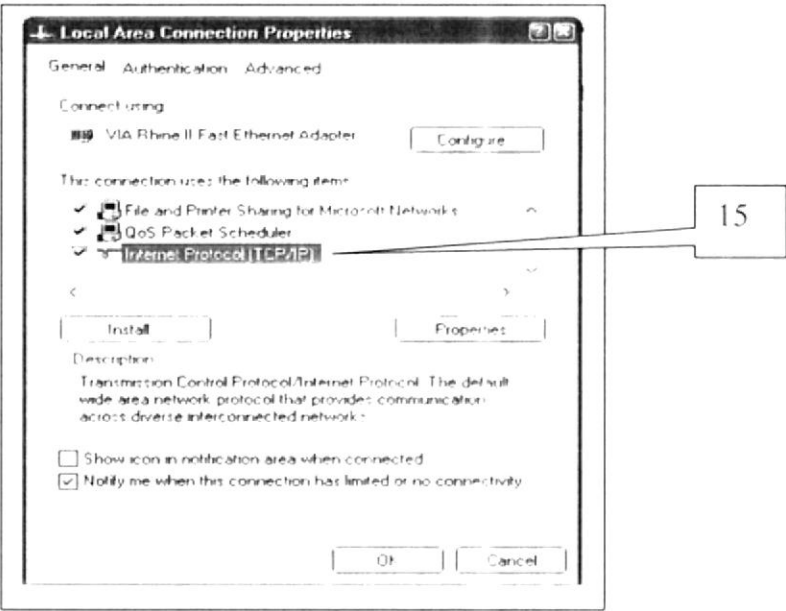


Figura 6-101: priopiedades tcp/ip

Paso 16 En el **PREFERIDO** DNS SERVER poner la dirección ip del servidor de Linux, **192.168.20.3** OK

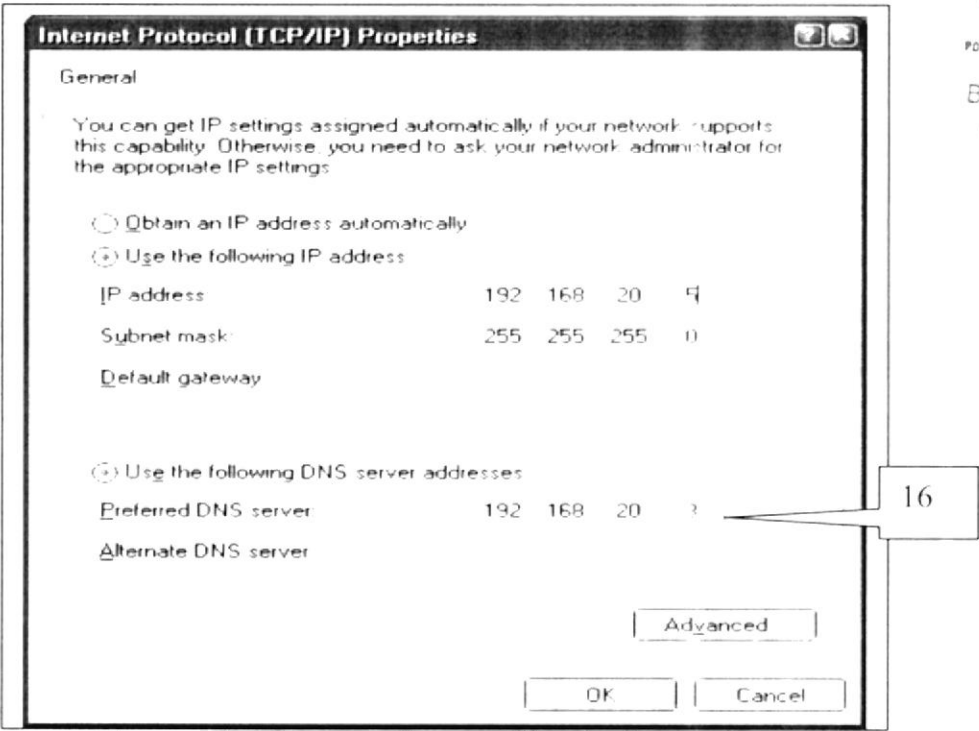


Figura 6-102: configuración de ip de dns

Paso 17 Ingresar a Inicio y escoger RUN(ejecutar)

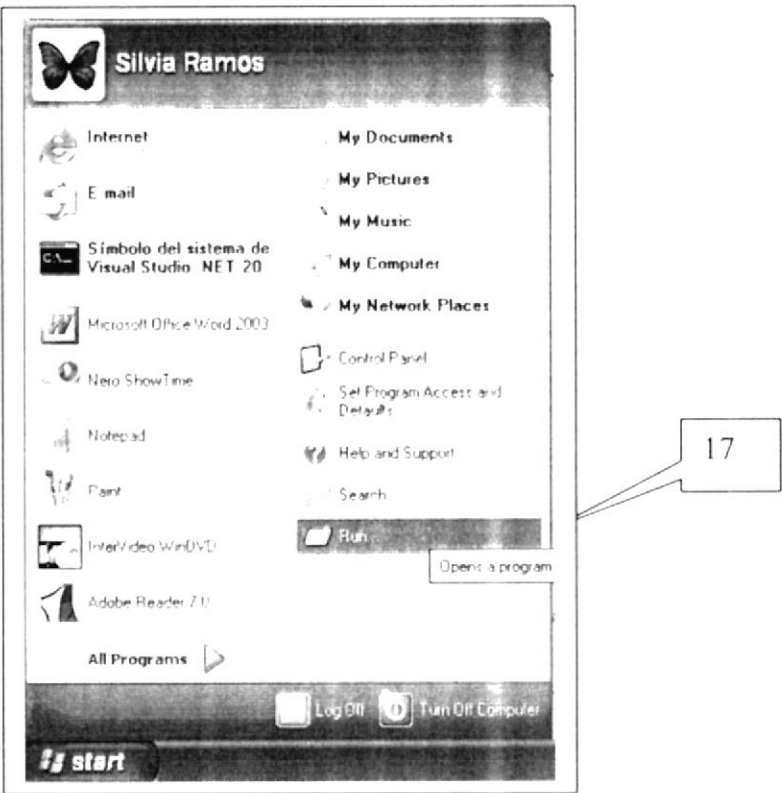


Figura 6-103: Ingreso a Ejecutar

Paso 18 Verificar si hay conectividad con el dominio en este caso es www.servipagos.com

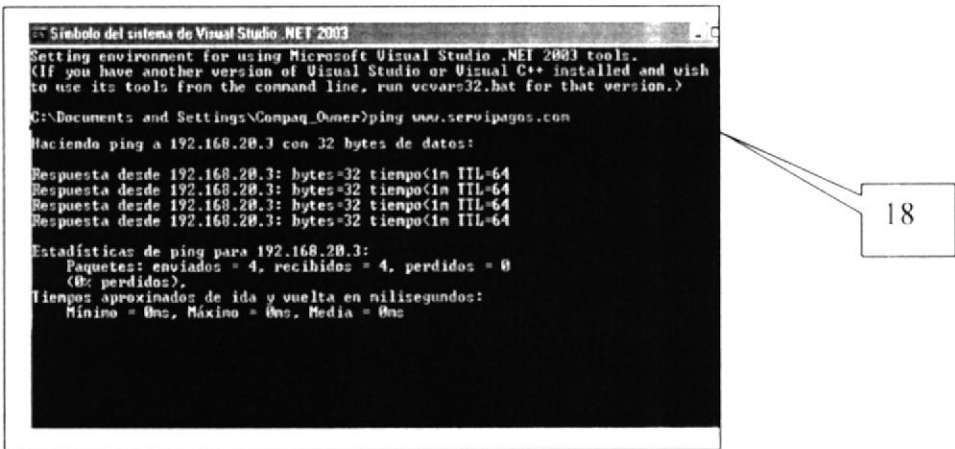


Figura 6-104: Prueba de conectividad al dominio

6.26 SERVIDOR WEB SERVER

Básicamente, un servidor Web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).

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

Un servidor es una computadora que entrega a otras computadoras (los clientes), una información que ellos requieren bajo un lenguaje común, denominado protocolo. Por lo tanto al ver una página Web es porque el servidor les entrega una página HTML vía protocolo HTTP (HyperText Transport Protocol) o protocolo para la transmisión de hipertexto, a través de una conexión TCP/IP por el puerto 80.

Por lo tanto en el **Servidor Web** es donde se almacena la información estática accedida y/o las aplicaciones que la generan.

Beneficios al instalar un servidor Web en Linux? :

Apache puede soportar de una forma más fácil y eficiente una amplia variedad de sistemas operativos.

El servidor puede personalizarse mejor para las necesidades de cada sitio web.

Un servidor es una computadora que entrega a otras computadoras (los clientes), una información que ellos requieren bajo un lenguaje común, denominado protocolo. Por lo tanto al ver una página Web es porque el servidor les entrega una página HTML vía protocolo HTTP (HyperText Transport Protocol) o protocolo para la transmisión de hipertexto, a través de una conexión TCP/IP por el puerto 80.

Por lo tanto en el Servidor Web es donde se almacena la información estática accedida y/o las aplicaciones que la generan.



6.26.1. BENEFICIOS AL INSTALAR UN SERVIDOR WEB EN LINUX:

- Apache puede soportar de una forma más fácil y eficiente una amplia variedad de sistemas operativos.
- El servidor puede personalizarse mejor para las necesidades de cada sitio web. El servidor HTTPD puede ser usado en la oficina para proveer acceso transparente a la información residente en diferentes servidores, en varias localizaciones y directorios. La información pueden ser simples documentos en Word, Hojas de cálculo de Lotus o complejas bases de datos.

La aplicación de esta tecnología esta siendo típicamente usada como sigue:

- Publicación de documentos corporativos: Estos documentos pueden incluir noticias, informes anuales, mapas, instalaciones de la compañía, listas de precios, información sobre productos, y cualquier documento que sea de valor en una entidad corporativa.
- Acceso a directorios de búsqueda: Acceso rápido a agendas telefónicas corporativas y similares. Esta información puede ser replicada en el sitio Web o, vía scripts CGI, el servidor Web puede servir como interfaz a la base de datos preexistente o nuevas aplicaciones. Esto quiere decir que usando los mismos mecanismos de acceso estándar, la información puede hacerse más accesible de una forma simple. Esto significa que puede ser usada para crear una interface con RDBMS como ORACLE y SYBASE para generar información en tiempo real.

6.26.2. HTTP REQUEST

El protocolo HTTP es un protocolo de pedido/respuesta. Un cliente envía una solicitud a un servidor. En dicha solicitud incluye un método, URI y versión de http.

Luego incluye una serie de encabezados y modificadores. Opcionalmente, puede incluir un cuerpo adicional con contenidos.

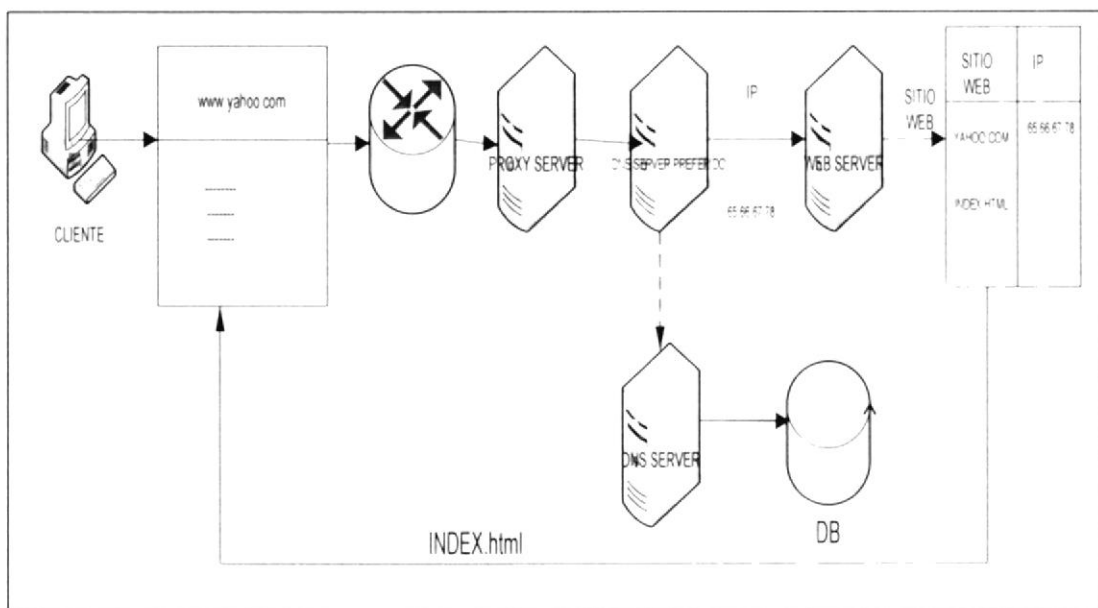


Figura 6-105: esquema web server

6.27 CONFIGURACIÓN DE SERVIDOR WEB EN LINUX

Paso 1 Para realizar la configuración de Web Server (Servidor Web) se necesita tener levantado DNS y contar con el paquete **httpd**, lo que se verificará de la siguiente manera:

rpm:Verifica paquetes instalados -q nombre_paquete:httpd

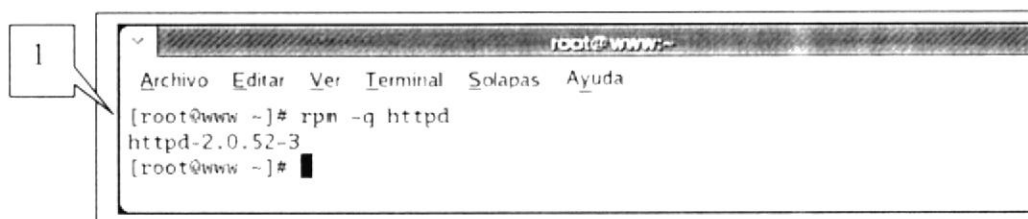


Figura 6-106: verificación de paquete httpd

Paso 2 Ingresar de la siguiente manera, ingresar a **cd /etc/httpd**.

Cd /etc/httpd : En el directorio se guardan todos los servicios instalados en el equipo

Paso 3 ingresar al archivo de configuración de httpd con el siguiente comando

Cd : Cambia del directorio actual al directorio especificado **cd conf**

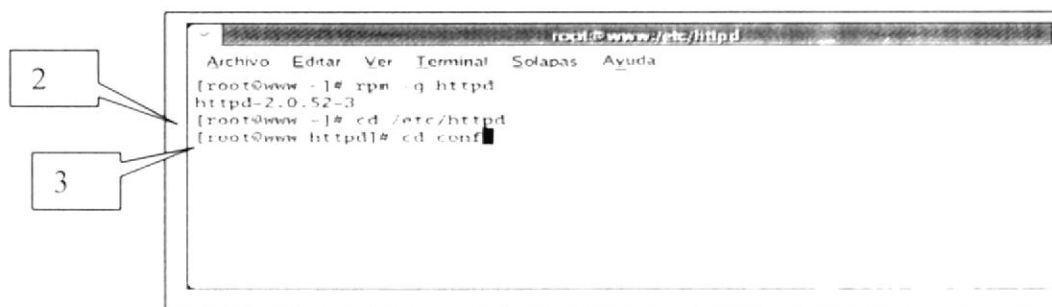


Figura 6-107: ingreso a la configuración httpd

Paso 4 Editar la configuración de la siguiente forma :httpd.conf

Vi httpd.conf: Edita un archivo de configuración de httpd.

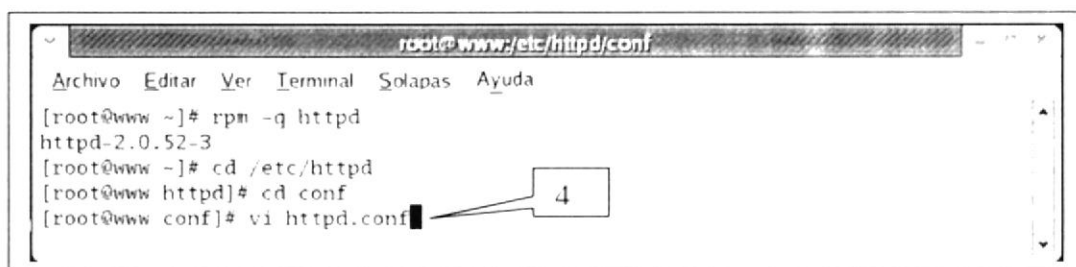


Figura 6-108: editar configuración de httpd

Paso 5 Buscar la línea **DirectoryIndex** se guarda el index de la página, agregar index.html que es donde se va a levantar la página de Servipagos

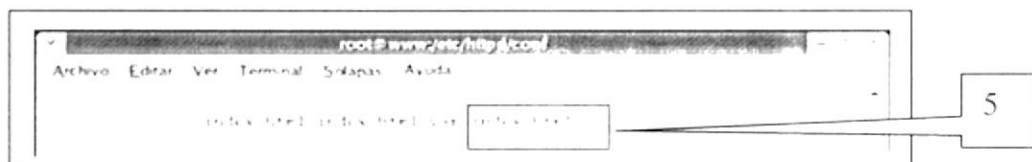


Figura 6-109: línea de index

Paso 6 En la línea del **<virtual host *:80>** hacer los siguientes cambios:

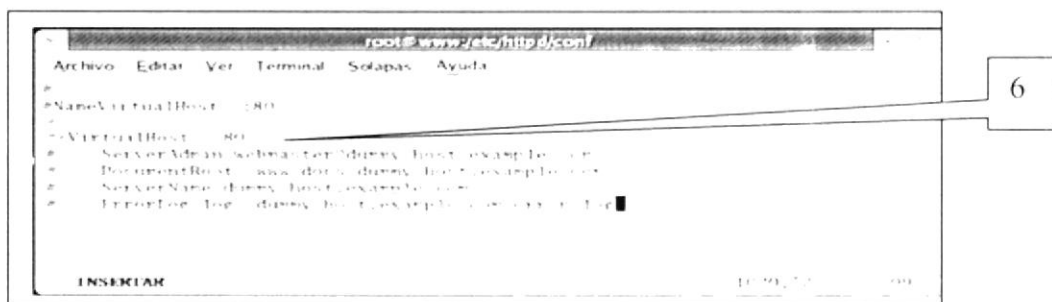


Figura 6-110: name virtual

- a) **<VirtualHost *:80>**.-Ubicarse Virtual host
- b) **ServerAdmin** Llega el error a esta página
- c) **DocumentRoot**.- en esta ruta se va a crear la carpeta en la cual va a estar alojada la página.
- d) **ServerName**.- aquí se especificará la dirección de la página (DNS)

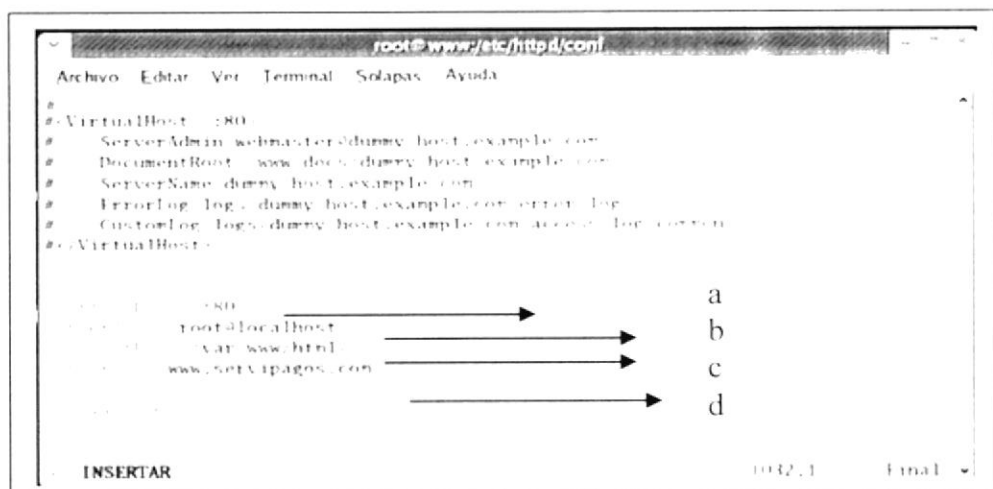


Figura 6-111: cambios en virtual host

Paso 7 El NameVirtualHost *:80 para levantar mas de un dominio

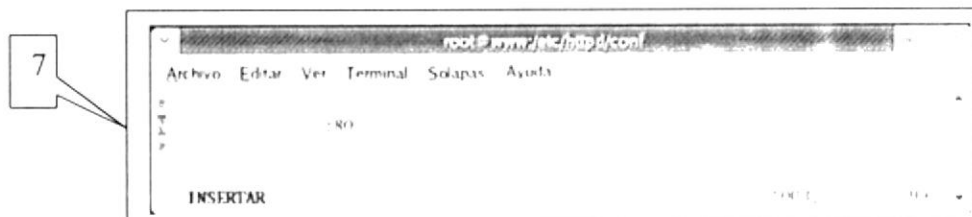


Figura 6-112: para levantar más de un dominio

Paso 8 Salir y guardar los cambios con **shift:wq**

"**wq**" e **INTRO** para guardar los cambios y cerrar el fichero.

Paso 9 Ingresar a la ruta `cd /var/www/html` donde se va alojar el sitio

cd Cambia de directorio

var/www/html : Directorio que contiene archivos de administración y datos históricos del sistema de html

Paso 10 Crear la carpeta donde se almacenará la página en este caso la carpeta se llama **SITIO**

Mkdir : Crea un directorio. Mkdir **SITIO**

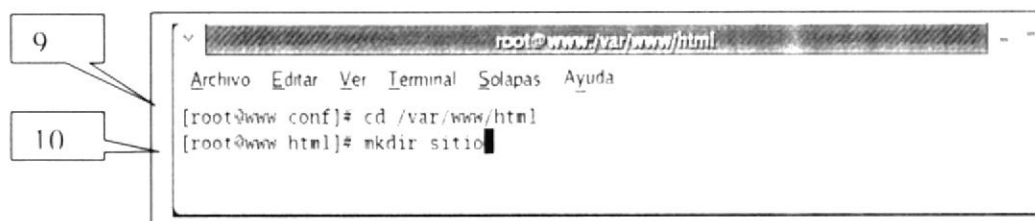


Figura 6-113: creación de carpeta sitio

Paso 11 Luego de Haber creado la carpeta ingresar al **INDEX** con el siguiente comando **VI INDEX.HTML**

vi index.html : Editar un archivo llamado index.html

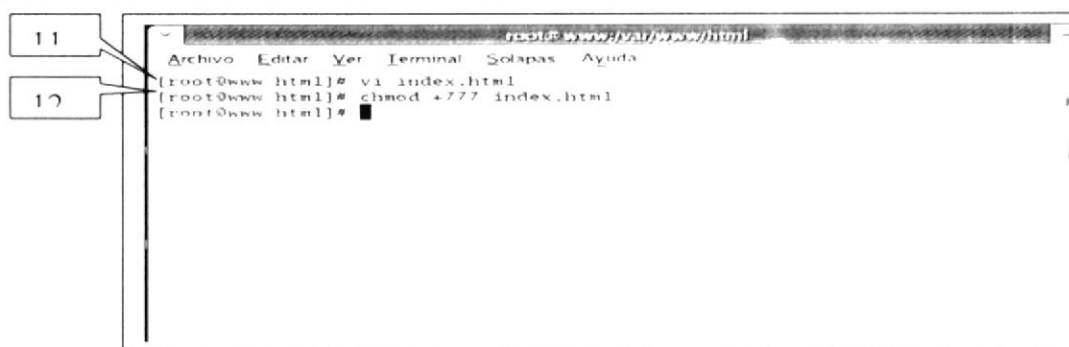


Figura 6-114: permisos a index

Paso 12 Dar permisos a la página con el comando **chmod +777**

Chmod: Cambia los atributos.

RW-USUARIO R- -GRUPO USUARIO R- -OTRO USUARIO 1 ENLACE FISICO

777=R-READ PESO = 4 W-WRITE PESO = 2 X-EJECUCION PESO =1

Paso 13 Reiniciar los servicios de la siguiente manera:

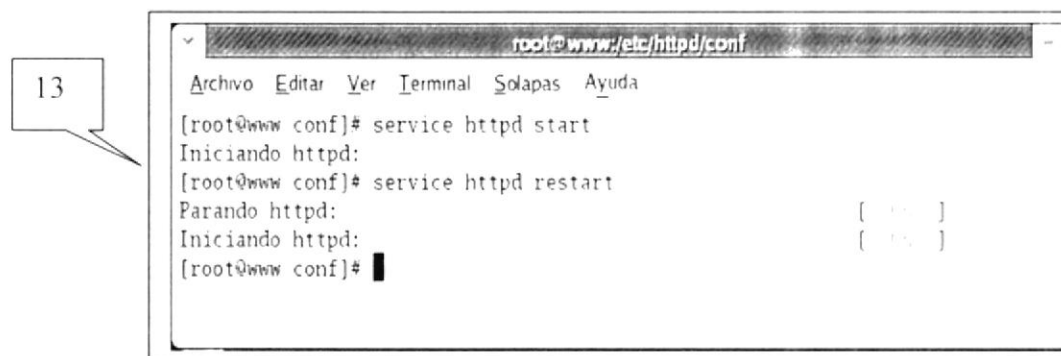


Figura 6-115: reinicio de servicio httpd

service nombre_servicio start Inicia el servicio especificado "nombre_servicio"

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

Nota: Para que arranque los servicios de Servidor al inicializar el computador realizar los siguientes pasos

a) Si ase tiene problemas ingresar al setup

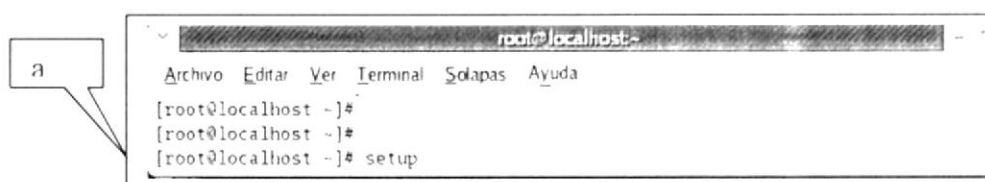


Figura 6-116: ingreso al setup

b) Ingresar a Servicios del Sistema

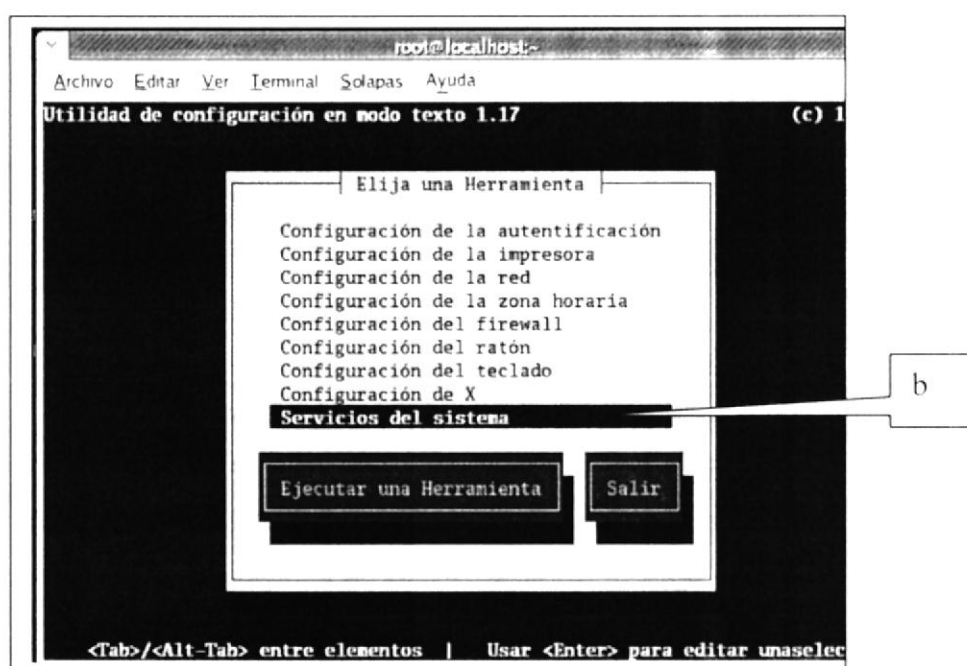


Figura 6-117: ingreso al servicio de sistema

- c) Ingresar a esta pantalla, y con las teclas direccionales buscar **HTTPD**
d) elegir y presionar la barra espaciadora dar **OK**

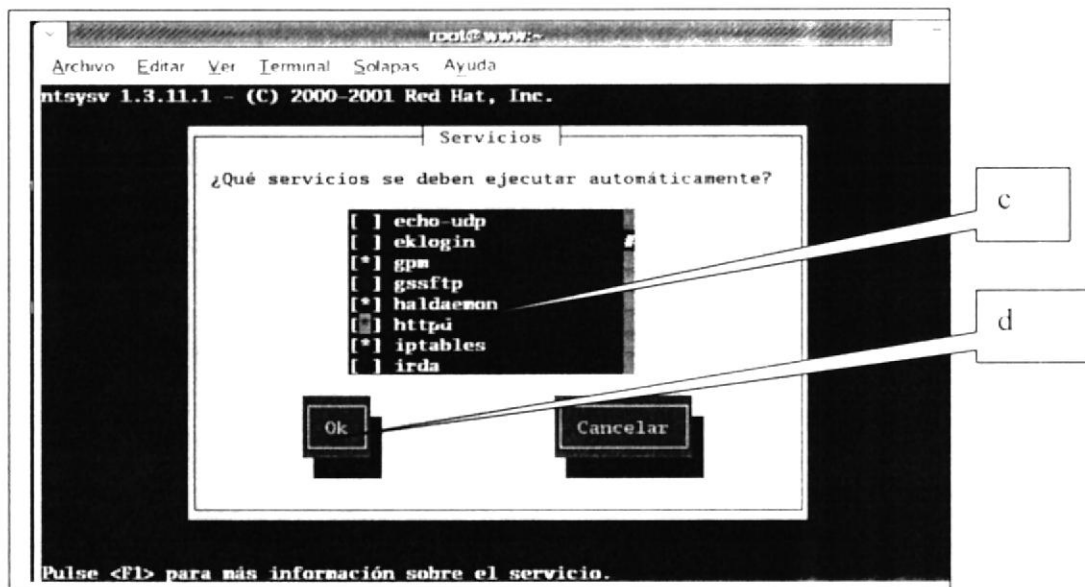


Figura 6-118: selección de servicio httpd



6.28 ACCESO DEL CLIENTE EN WINDOWS

En el lado del cliente realizar las siguientes configuraciones:

Paso 14 Ingresar al Explorador de Windows, Herramientas, opciones de Internet como se ve en la siguiente pantalla:



Figura 6-119 ingreso a opciones de conexión

Paso 15 Ingresar a conexiones elegir **LAN SETTINGS**

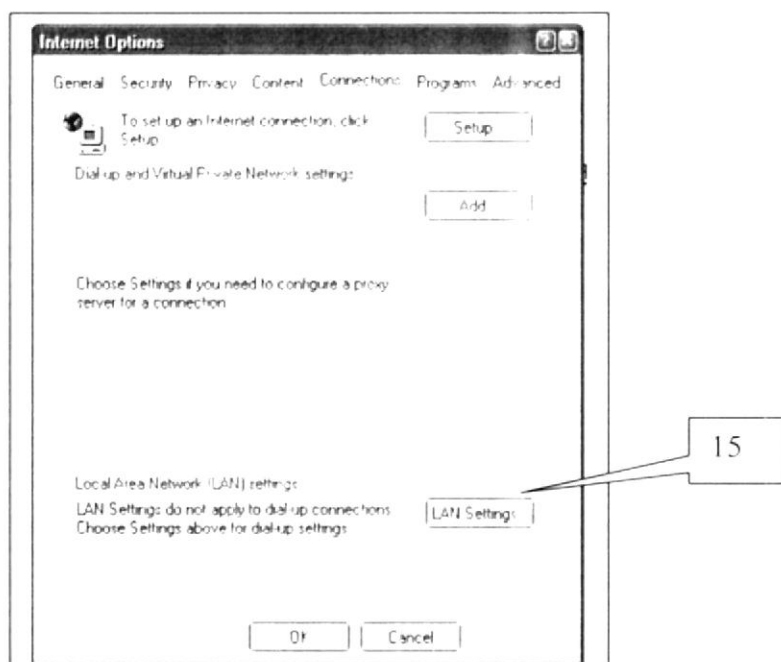


Figura 6-120: ingreso a LAN settings

Paso 16 Aquí seleccionar Configuración LAN elegir Automatically detect settings (detección automática) para Web Server

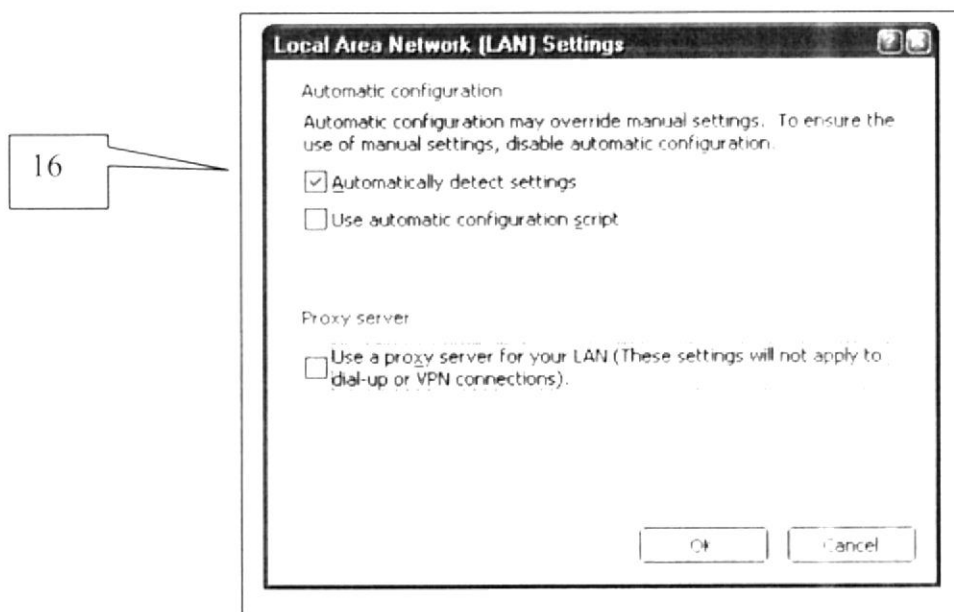


Figura 6-121: detección automática

Paso 17 Acceder al sitio Web mediante el navegador.

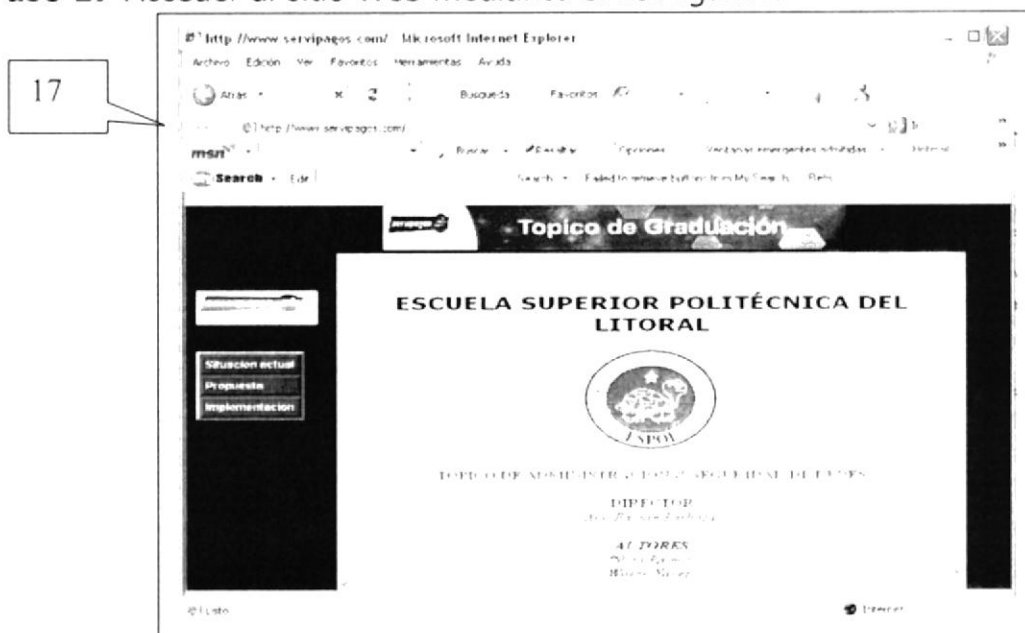


Figura 6-122: navegación de página

6.29 SERVIDOR PROXY

Un proxy no es más que un programa de software con la utilidad de "dar servicio", esto es, permitir algún tipo de acceso a una máquina (en la que está corriendo el programa) desde otras; sólo que en este caso, el ordenador que ejecuta el servicio no es el destino final en la comunicación, sino sólo una pasarela que facilita el tráfico hacia otros lugares de una red.

Así dicho puede parecer un poco lioso, resultarán útiles unos ejemplos: En un ordenador conectado a Internet se puede ejecutar un servidor web, lo que permitirá que otros ordenadores (clientes) se puedan conectar al el y leer mediante un determinado protocolo parte de la información contenida en el disco duro. En este caso el servidor, el ordenador, es el destino final de la comunicación establecida desde esos ordenadores remotos. En cambio, si se instala un servidor proxy en la máquina los ordenadores que accedan a él, fundamentalmente no "querrán" leer el disco duro, sino tener acceso a otros ordenadores a través de el, por lo que el equipo estará simplemente actuando como una pasarela.

Todo servidor corriendo (estando abierto) en un equipo, genera un archivo de texto en el que se van registrando las peticiones de los ordenadores que acceden a él y el tipo de solicitud que le están haciendo. Básicamente, se registran: el momento de la comunicación (día y hora), la IP del ordenador que está accediendo al servidor, el protocolo empleado, los puertos utilizados (en el servidor y el cliente), y la solicitud que se hace, sea el acceso a ficheros en disco duro, o la petición de enlace a otra IP externa, etc. Es posible registrar más datos, pero estos son los más elementales. Estos archivos de texto, que reciben el nombre de log, son almacenados en el disco duro del ordenador servidor; además, es importante su almacenamiento por razones relacionadas con la seguridad.

Una situación típica en la que es posible que sea necesario instalar un servidor proxy, es cuando se dispone de una red de varios ordenadores y sólo uno de ellos tiene posibilidad de salida a Internet. Dejando de lado el hecho de que hay sistemas mejores para hacerlo, puede que, por las circunstancias que sea, sólo haya una opción viable para hacer que los demás equipos puedan salir también a Internet: la de instalar un servidor proxy en el equipo que originalmente tiene el módem.

En este caso, en nuestra red, el equipo que tendría salida directa a Internet sería el que tiene instalado el proxy, mientras que los demás accederán a ese ordenador solicitándole que les dé acceso a Internet. El único ordenador que tendrá una IP pública en la Internet será el que está corriendo el proxy, los demás no serán "visibles" para Internet, porque será como si sólo hubiera un ordenador navegando.

En este ejemplo, el servidor proxy tendría una utilidad meramente privada; accesible sólo desde los equipos que están en su red, y nada más.

Los servidores proxy existen en redes abiertas en Internet desde hace mucho tiempo. Una de las posibilidades de "acción" de este tipo de dispositivos es la de almacenar en su disco duro (u otro dispositivo de almacenamiento) las páginas web que los ordenadores clientes van solicitándole, aunque sean páginas que están en cualquier sitio de Internet. El servidor proxy, a medida que otro ordenador solicita que le muestre una página situada fuera de su red, la almacena para el caso de que otro ordenador vuelva a solicitarle la misma página; entonces si eso sucede, el proxy, en lugar de ir a buscar la página fuera de su red, la leerá en su disco duro para servirla al ordenador que la solicitó, con lo que se gana tiempo. Es lo que se conoce como proxy-caché.

El "cacheado" de archivos no es tan exótico como puede parecer, también los ordenadores hacen un caché guardando las páginas que se han visitado, de manera que si se regresa a una página que ya ha visto con anterioridad durante la misma sesión, la página se cargará más rápido, puesto que el navegador va a leer a el disco duro, donde ya está almacenada. Dependiendo de cómo se haya configurado el navegador, esas páginas almacenadas en el equipo, podrán estar disponibles para tras sesiones o no. La diferencia reside en si se activa que se vacíe el caché de disco cada vez que se cierra el navegador (en cuyo caso no estarán disponibles de una sesión a otra) o no lo activa (y entonces sí estarán disponibles entre sesiones). En Microsoft Internet Explorer, esa opción se encuentra en: Herramientas --> Opciones de Internet --> Opciones avanzadas --> Vaciar la carpeta Archivos temporales de Internet cuando se cierre el explorador.

Otra utilidad de un proxy público es la de hacer la navegación más anónima, puesto que como ya se mencionaba antes, al navegar a través de un proxy, todos los lugares visitados "creerán" que nuestra IP es la del proxy, y no la que en realidad se tiene. Aunque el anonimato no hay forma de entenderlo en términos absolutos pues, como se dijo antes, el proxy estará guardando un log en el que se registran las solicitudes asociadas a nuestra IP.

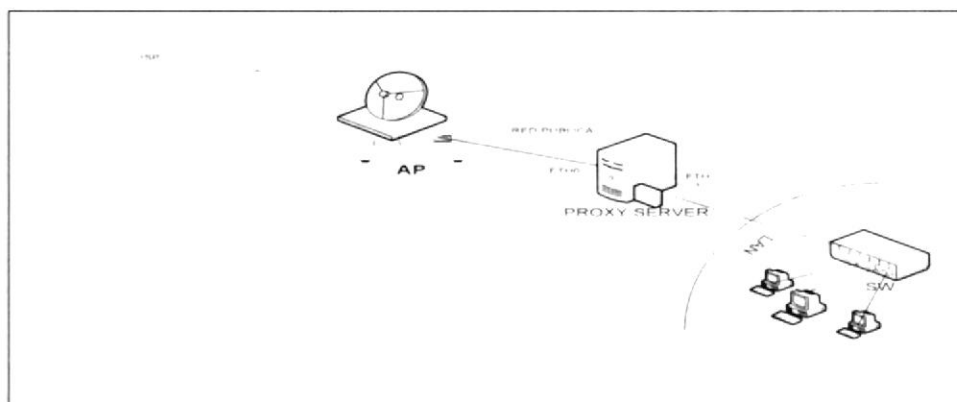


Figura 6-123: esquema de servidor Proxy

6.30 CONFIGURACIÓN DE SERVIDOR PROXY EN LINUX

Paso 1 Verificar que está instalado es el **squid**

rpm: Verifica paquetes instalados -q **nombre_paquete:** Squid

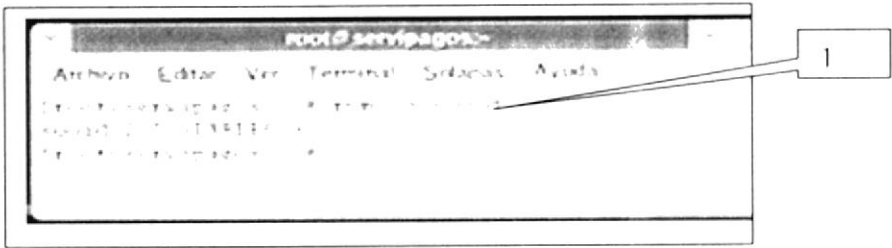


Figura 6-124: verificación de paquete squid

Paso 2 Editar el archivo **squid** en la ruta de cd /etc: En el directorio se guardan todos los servicios instalados en el equipo.

Vi squid.conf: Edita un archivo de configuración del paquete squid.

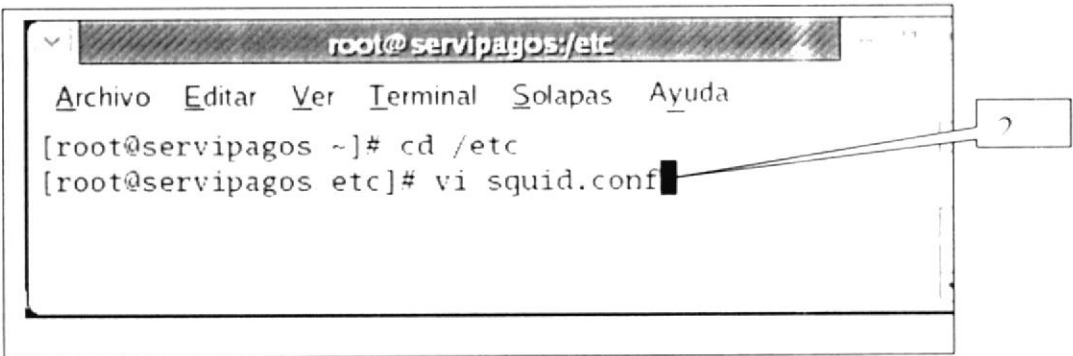


Figura 6-125: editar paquete de squid

Paso 3 En esta sección se debe habilitar ciertas líneas, como es el caso del puerto 8080, el cual permite **escuchar**

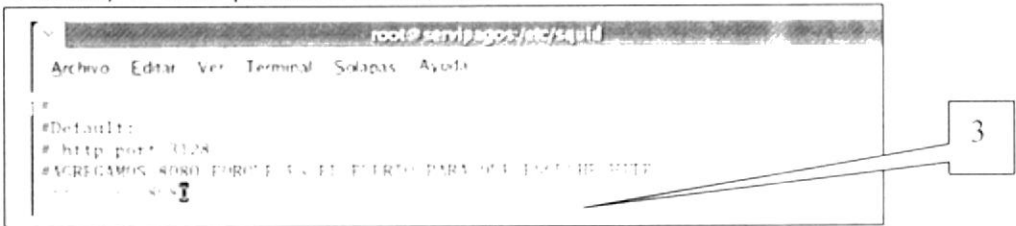


Figura 6-126: línea del puerto 8080

Paso 4 Bajar con las teclas direccionales para editar en la sección de **caché_mem** en la cual se habilita y cambia a 16 MB.

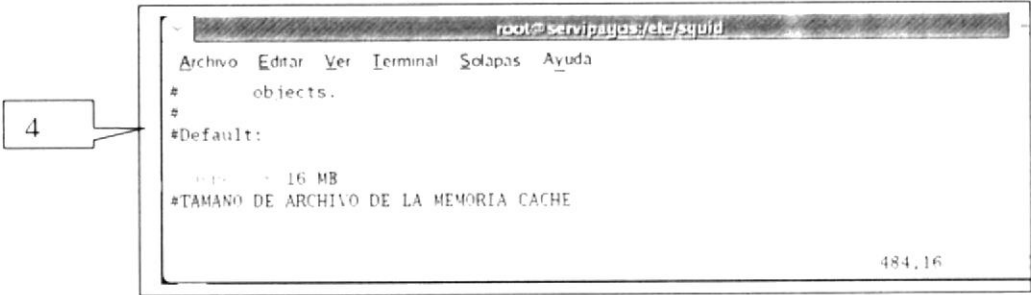


Figura 6-127: Línea de **cache_mem**

Paso 5 Buscar la siguiente línea la cual sirve para monitorear la actividad de los hosts que tenga a cargo el proxy)

- **Cache_dir** `ufs /var/spool/squid`

Cache_dir :Busca una aplicación en la lista de directorios

Spool: Colas de trabajos para realizar más tarde

Squid :paquete squid para Proxy

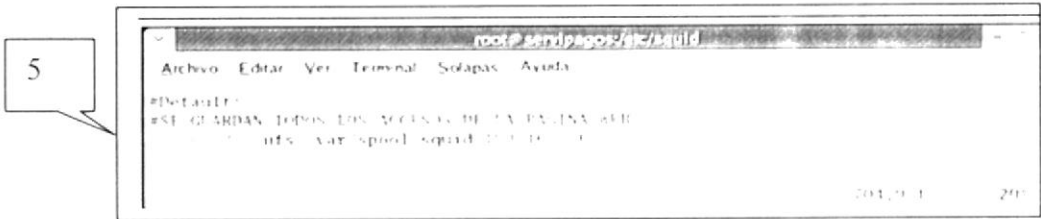


Figura 6-128: configuración de **cache_dir**

Paso 6 Buscar la siguiente línea `Cache_access_log /var/log/squid/access_log`

Cache_access :Accesa a una aplicación en la lista de aplicaciones



- **Cache_access_log /var/log/squid/access_log**

/var/log/ Para saber los posibles errores que ocurren al intentar iniciar el entorno gráfico lo mejor es ir a los logs

Squid :paquete squid para Proxy

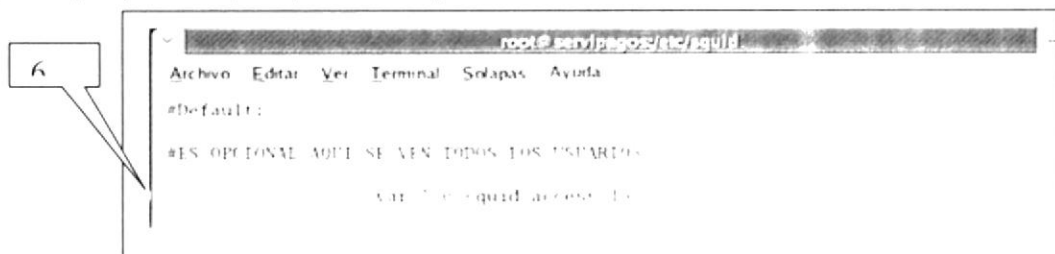


Figura 6-129: configuración cache_access_log

Paso 7 Buscar visible de la siguiente manera **/visible** se copia, pega y modifica agregando **visible hostname localhost**

visible_hostname localhost
máquina

hostname Visualiza el nombre de la

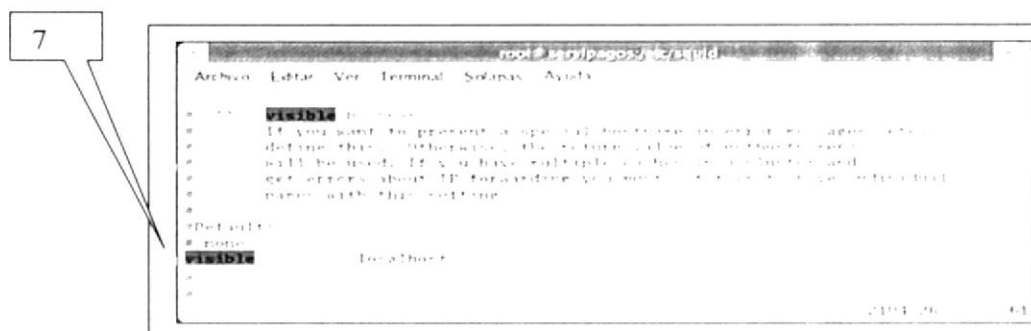


Figura 6-130: localhost

Paso 8 Aquí se permite la red que se ha especificado en la ACL pueda tener acceso a navegar:

http_access allow red puerto: Contenido del servidor WWW.

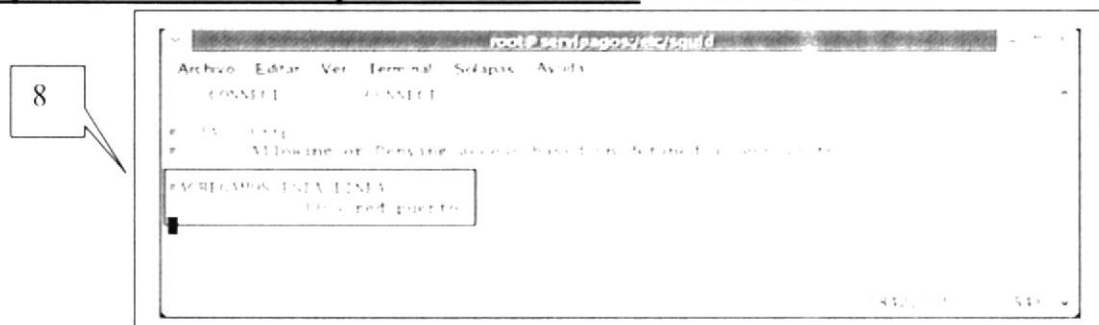


Figura 6-131: acceso al puerto 8080

Paso 9 Restaurar el servicio squid con el comando

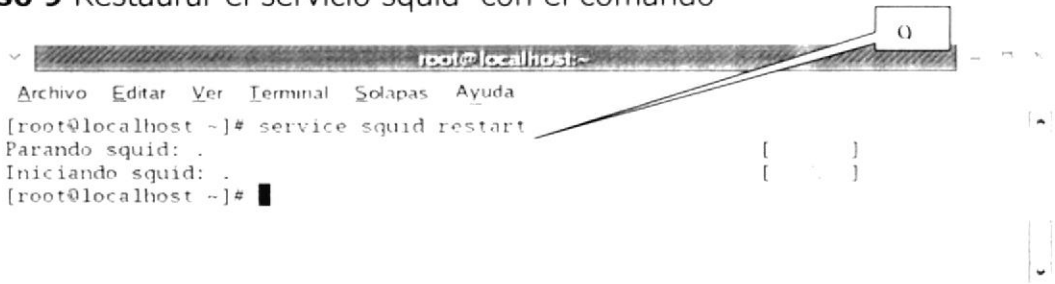


Figura 6-132: servicio restaurado

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

Paso 10 Se regresa a configurar en el squid los ACL ver el cuadro rojo

acl **red** src **192.168.20.0/255.255.255.0**

acl : regla **nombre** red src **lugar de origen** 192.168.20.0.
(ip del servidor y máscara)

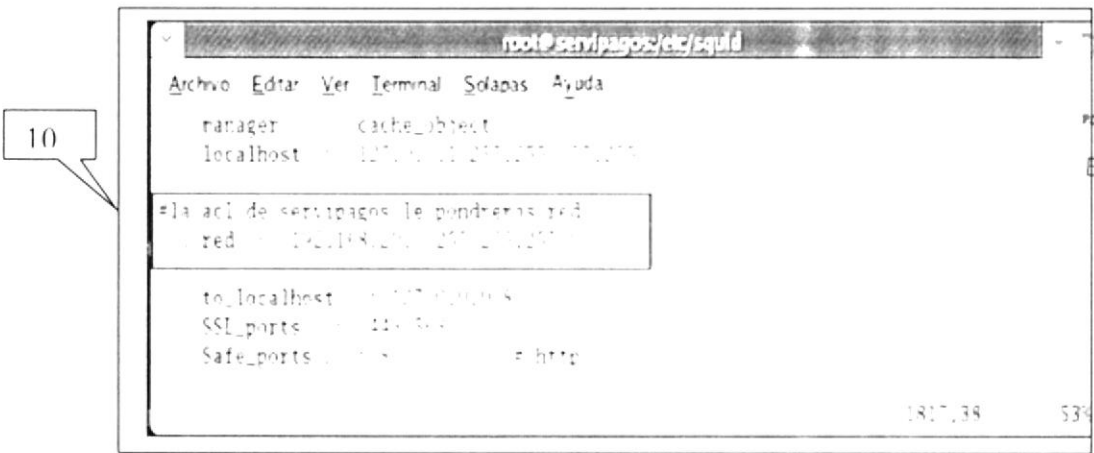


Figura 6-133: creación de acl

Paso 11 Agregar al ACL para el Puerto para Proxy es **8080**

Acl:regla nombre puerto tipo myport puerto 8080

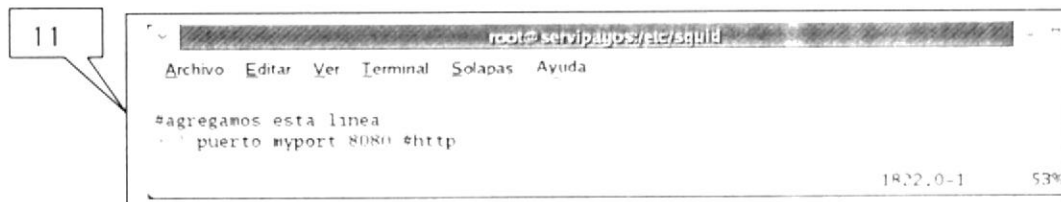


Figura 6-134: acl de nombre puerto

Paso 12 Iniciar el servicio squid con el comando

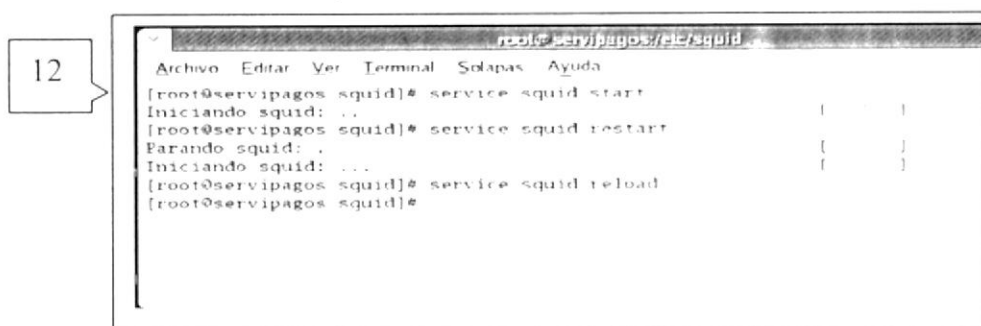


Figura 6-135: restauramos squid

service nombre_servicio start Inicia el servicio especificado
"nombre_servicio"

service nombre_servicio restart Reinicia el servicio especificado
"nombre_servicio"

Nota: Para que arranque los servicios de Servidor al inicializar el computador realizar los siguientes pasos

a) Si se tiene problemas ingresar al setup



Figura 6-136: ingreso al setup

b) Ingresar a Servicios del Sistema



Figura 6-137: ingreso al servicio de sistema

c) Ingresar a esta pantalla, y con las teclas direccionales buscar **SQUID**

d) elegir y presionar la barra espaciadora dar **OK**

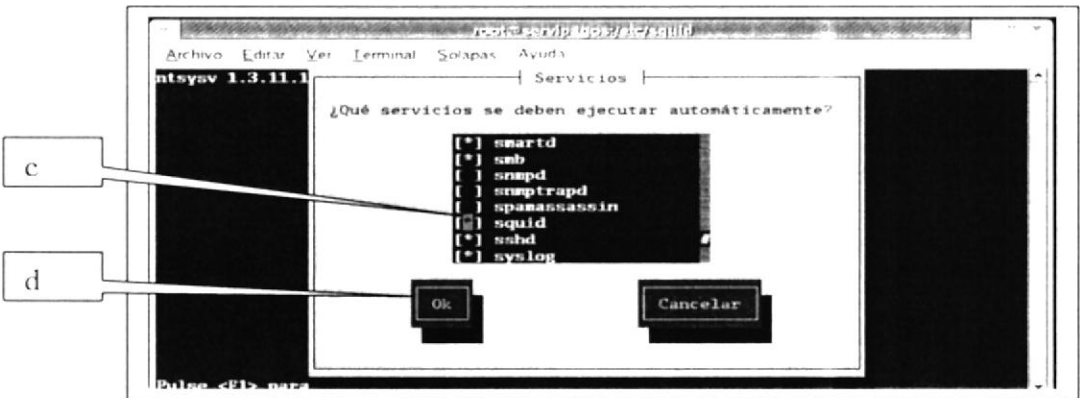


Figura 6-138: elección de servicio squid

6.30.1. AUTENTICAR

Se procede a crear un fichero /ETC/SQUID/CLAVES:

ACCESO CON AUTENTICACIÓN (PASSWORD): Crear el archivo claves en la siguiente ruta.

Paso 13 touch /etc/squid/claves : Crear un archivo en la ruta /etc/squid/claves

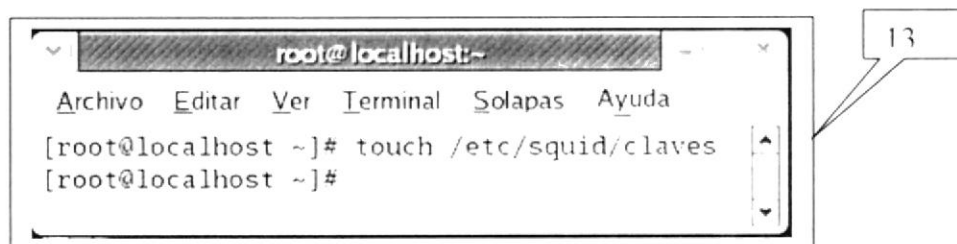


Figura 6-139: creación de archivos claves

Se da permisos al archivo. Se cambia de propietario al archivo.

Paso 14 chmod 600 /etc/squid/claves

Chmod : Asigna al fichero nombreadarchivo permisos de lectura, escritura y ejecución para el propietario, grupo e invitado

Salvo que vaya a utilizarse un guión a través del servidor web para administrar las claves de acceso, como medida de seguridad, este fichero debe hacerse leíble y escribible solo para el usuario squid:



Figura 6-140: permisos de archivo claves

Paso 15 `chown squid:squid /etc/squid/claves`

Chown :Cambia el propietario del archivo nombrearchivo a nombreusuario

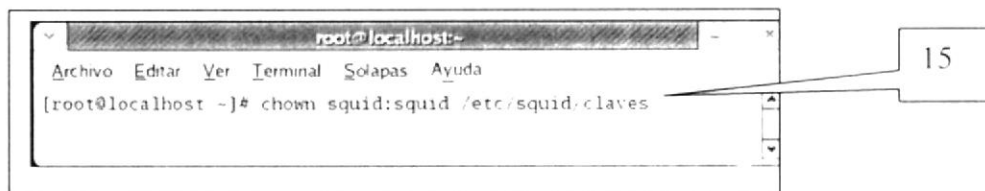


Figura 6-141: cambio de propietario

Paso 16 A continuación se debe dar de alta las cuentas que sean necesarias, utilizar el comando `htpasswd -mismo` que viene incluido en el paquete `httpd-2.0.x-.` Ejemplo:

Asignar contraseña

htpasswd /etc/squid/claves (usuario existente)

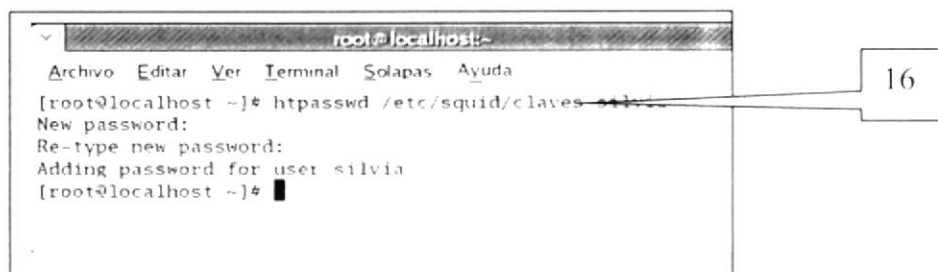


Figura 6-142: ingreso de clave para autenticar

Lo anterior solicitará teclear una nueva clave de acceso para el usuario *Silvia* y confirmar tecleando ésta de nuevo. Repita con el resto de las cuentas que requiera dar de alta.

Todas las cuentas que se den de alta de este modo son independientes a las ya existentes en el sistema. Al dar de alta una cuenta o cambiar una clave de acceso lo estará haciendo **EXCLUSIVAMENTE** para el acceso al servidor Proxy. Las cuentas son independientes a las que se tengan existentes en el sistema como serían *shell*, correo y Samba.

Paso 17 Crear la ACL con el nombre de password **proxy_auth silvia**

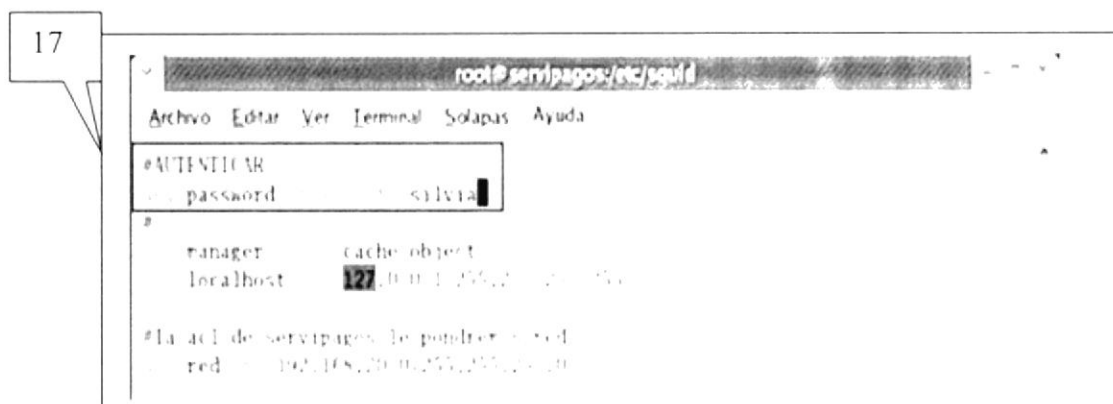


Figura 6-143: acl de autenticar

Paso 18 Se debe editar el fichero `/etc/squid.conf` y se especificará el programa de autenticación que se utilizará. Localice la sección que corresponde a la etiqueta `auth_param basic program`. Por defecto no está especificado programa alguno.

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

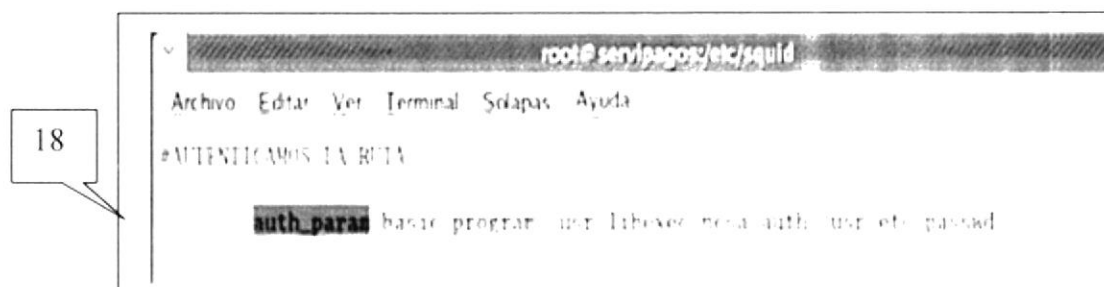


Figura 6-144: ruta auth_param

Después de encontrar la línea `auth_param` se habilita de la siguiente manera:

Paso 19 `auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves`

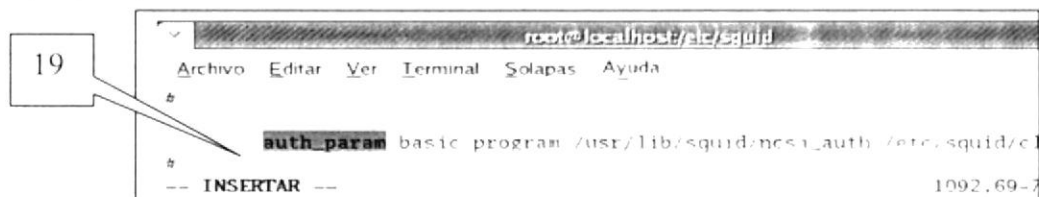


Figura 6-145: cambios en ruta auth_param

/usr/lib/squid/ncsa_auth usr/ : Directorio que contiene programas y archivos para la configuración de los usuarios corresponde a la localización de el programa para autenticar .

/etc/squid/claves al fichero que contiene las cuentas y sus claves de acceso.

6.30.2. LISTAS Y REGLAS DE CONTROL DE ACCESO.

El siguiente paso corresponde a la definición de una Lista de Control de Acceso. Se especifica una denominada passwd la cual se configurará para utilizar obligatoriamente la autenticación para poder acceder a Squid. Debe localizarse la sección de Listas de Control de Acceso y añadir la siguiente línea:

Paso 20 Incluir lista de control de acceso.

acl password proxy_auth REQUIRED

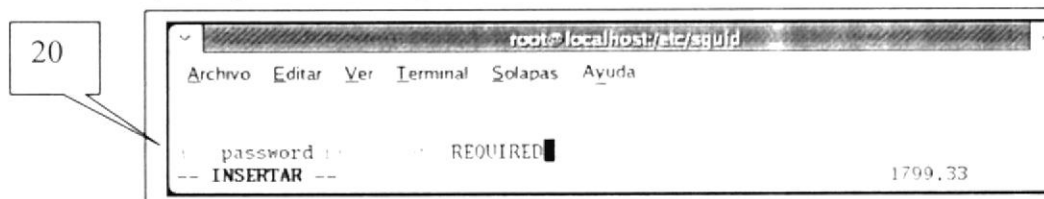


Figura 6-146: acl activada

Habiendo hecho lo anterior, se debe tener en la sección de Listas de Control de Acceso algo como lo siguiente:

Paso 21 Incluir regla de control de acceso

http_access allow cliente password



Figura 6-147: acceso para autenticación

Se añade passwd, la definición de la Lista de Control de Acceso que requiere utilizar clave de acceso, a la regla actual, de modo que quede como se muestra a continuación:

Paso 22 Salir con :wq para guardar los cambios.

":wq" e **INTRO** para guardar los cambios y cerrar el fichero.

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y se pueda hacer pruebas

Paso 23 Reiniciar el servicio.

service squid restart

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

6.30.3. PARA BLOQUEAR UNA PÁGINA

Paso 24 Crear la acl pornografía dstdomain .sexy.com para que todo lo que venga de ese dominio no lo acepte (ver recuadro rojo)

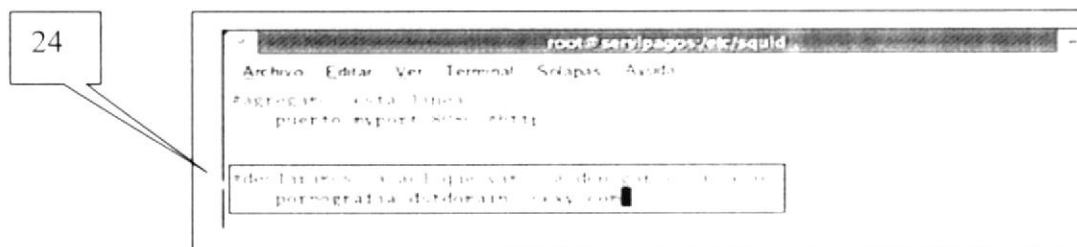


Figura 6-148: acl de páginas prohibidas

Se debe definir una *Lista de Control de Acceso* que a su vez defina al fichero */etc/squid*. Esta lista se denominará como "pornografía". De modo tal, la línea correspondiente quedaría del siguiente modo:

Service squid reload

Paso 25 Crear la página para hacer la prueba

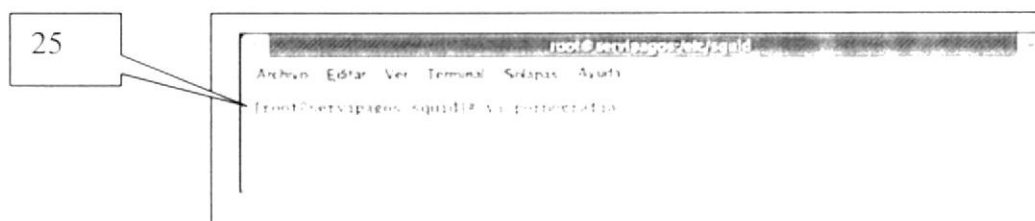


Figura 6-149: ingreso al archivo para denegar páginas

Paso 26 Ingresar a editar el archivo creado

Lo primero será generar una lista la cual contendrá direcciones Web y palabras usualmente utilizadas en nombres de ciertos dominios. Ejemplos:

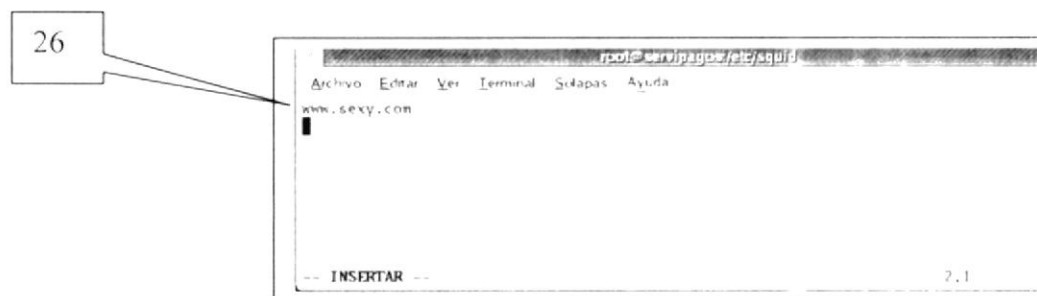


Figura 6-150: ingreso de páginas a denegar acceso

Paso 27 se declara la ACL que se va a bloquear al ingresar al **vi.squid.conf**

Vi squid.conf : Edita un archivo en el directorio squid.

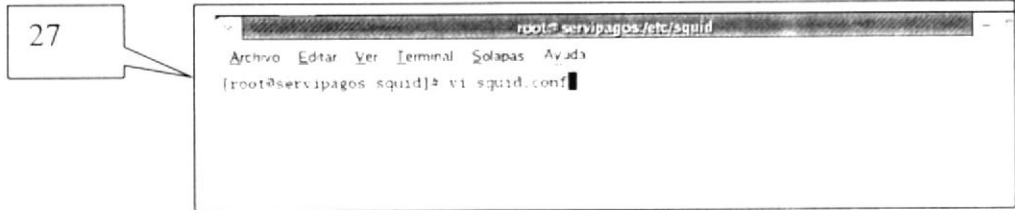


Figura 6-151: editar squid

Paso 28 Declarar la ACL llamada **pornografía**

Acl : regla
origen de ruta

nombre arch_porno

src

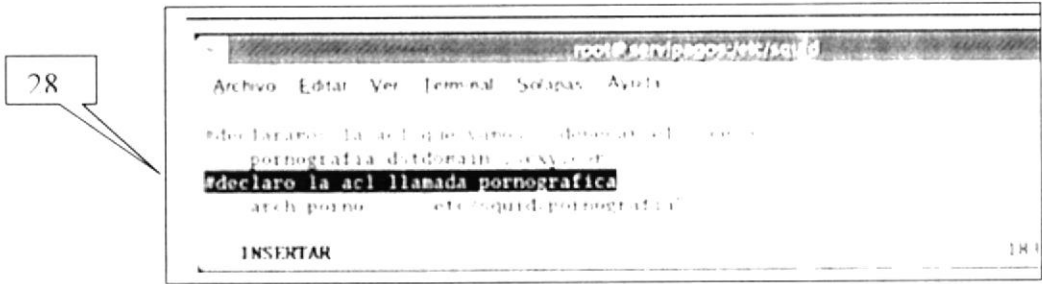


Figura 6-152: acl de páginas prohibidas

Paso 29 Buscar los **HTTP_ACCESS**

A continuación se especifica, modifica una Regla de Control de Acceso existente al agregar deny red_prohibida que se denegará el acceso a la Lista de Control de Acceso denominada sitiosdenegados: (ver recuadro rojo).

Crear un **http_access deny red_prohibida puerto llamado porno**



Figura 6-153: accesos denegados para páginas

Paso 30 Guardar y actualizar con el comando `service squid reload`

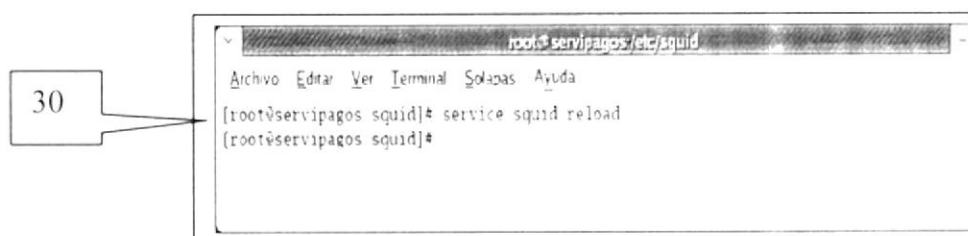


Figura 6-154: servicio squid restaurado

Service squid reload: Muestra el estado del servicio especificado

Paso 31 Deganar el tiempo, crear la acl time1 time MTMHF (ver recuadro rojo)

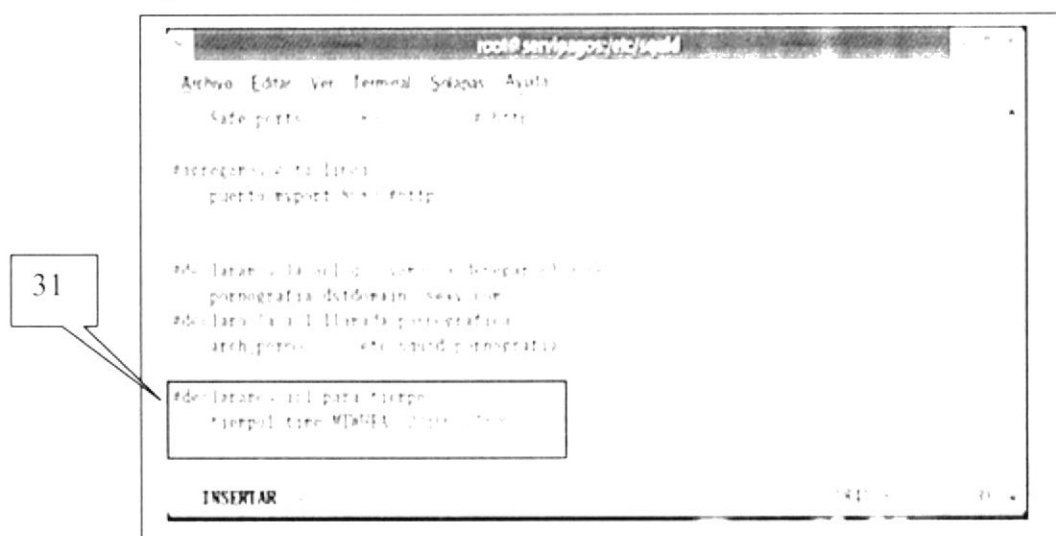


Figura 6-155: acl de tiempo

Paso 32 Para que los usuarios no naveguen en esa red crear un `http_access` deny con usuario de nombre `red_servipagos` (**ver recuadro rojo**)

Se ha denegado la navegación al usuario **LUCAS** por el **tiempo1** que se ha configurado antes

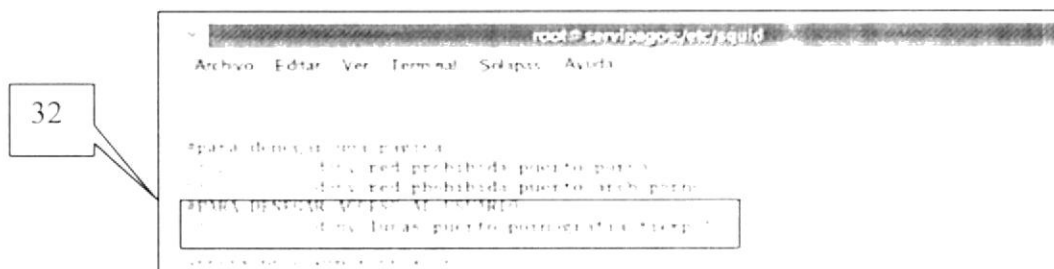
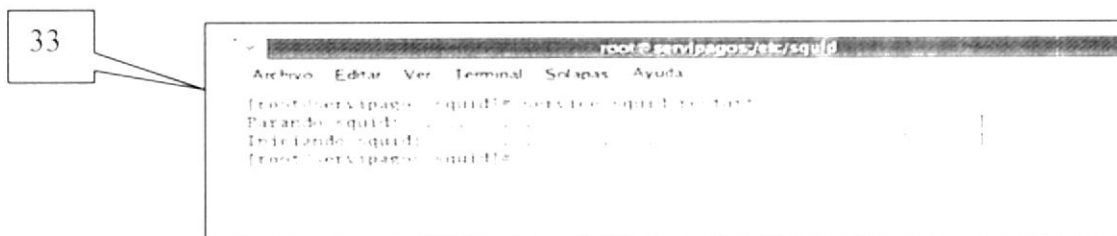


Figura 6-156: acceso por tiempo

Paso 33 Restaurar los Servicios**Figura 6-157: restaurar squid**

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"



6.31 CONFIGURACIÓN EN EL CLIENTE WINDOWS

6.31.1. COMPROBACIÓN DE SU SALIDA POR PROXY

En el lado del cliente se realizan las siguientes configuraciones:

Paso 34 Ingresar al Explorador de Windows, Herramientas, opciones de Internet como se observa en la siguiente pantalla:

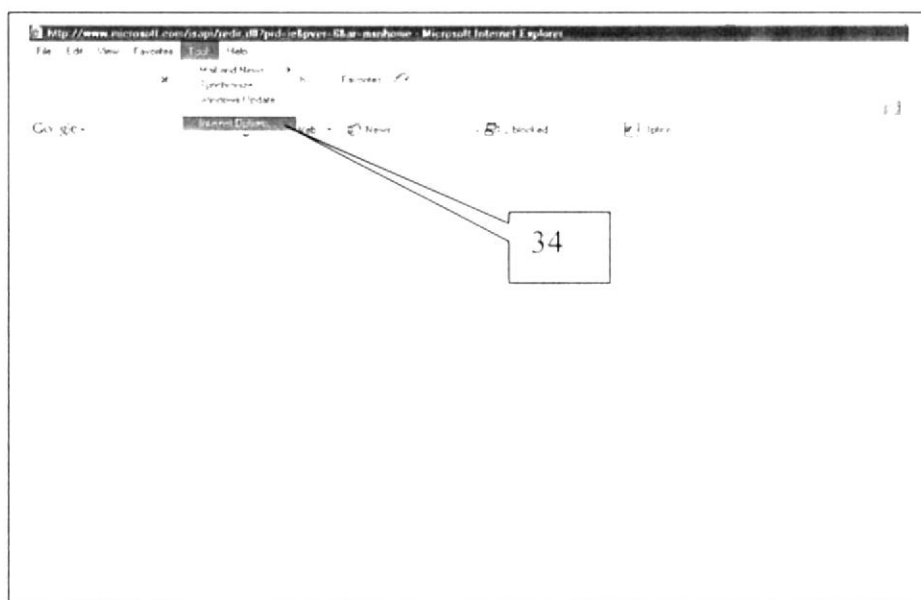


Figura 6-158: opciones de internet

Paso 35 Ingresar a conexiones, se elige LAN SETTINGS

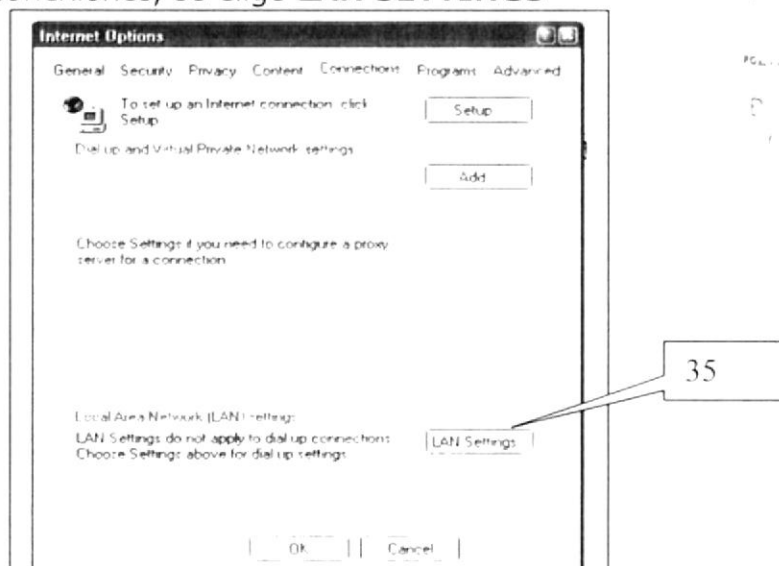


Figura 6-159: ingreso lan settings

Paso 36 En este cuadro de diálogo, configurar el panel que dice "Servidor Proxy" en el cual se pondrá la dirección IP que se haya puesto en el Servidor Linux, y su puerto correspondiente en este caso será el puerto 8080. Presionar el botón **"Aceptar"**

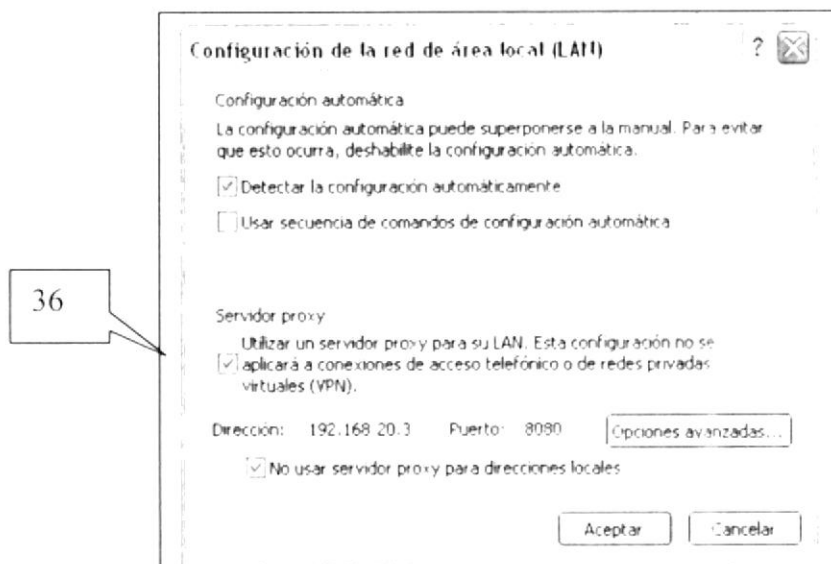
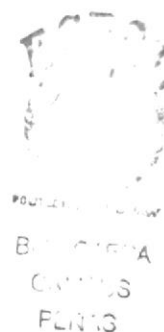


Figura 6-160: detección de puerto proxy



6.31.2. COMPROBACIÓN DE AUTENTIFICACION

Paso 37 Ingresar al navegador de Windows automáticamente sale la pantalla para ingresar el usuario que se ha autorizado para la navegación.

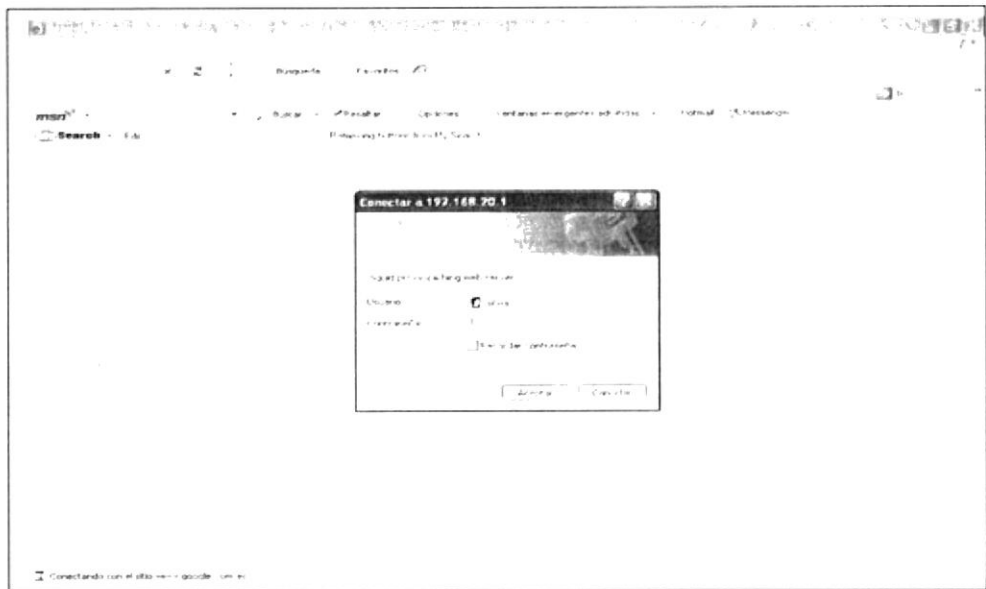


Figura 6-161: ingreso de usuario con permisos

Paso 38 A continuación usted puede cargar su página deseada en este caso será www.servipagos.com, que es la que se configuró para el DNS y WEB SERVER.

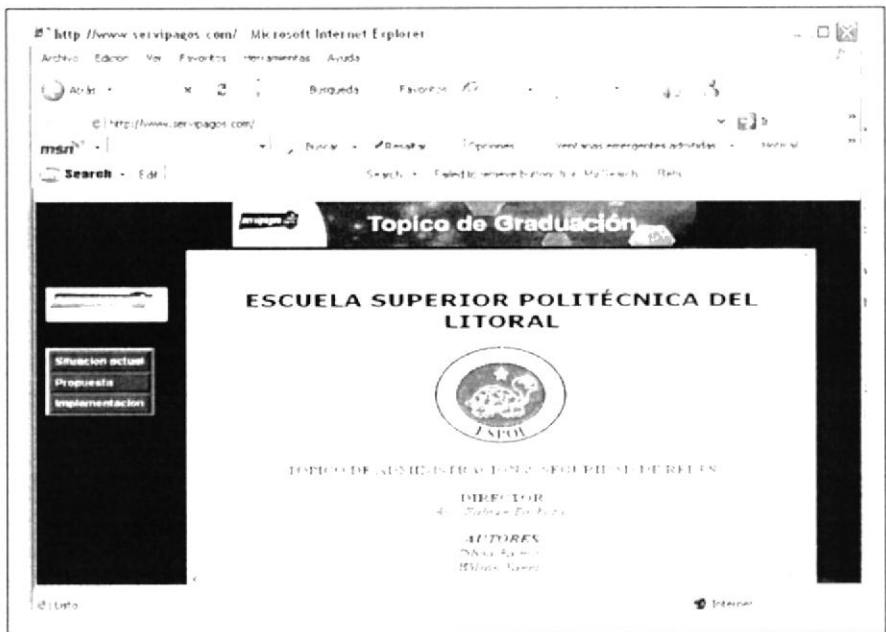


Figura 6-162: página cargada

6.31.3. COMPROBACIÓN DE PÁGINAS DENEGADAS

Paso 39 Ingresar la página que se ha denegado en este caso es www.sexo.com para comprobar que los pasos de la configuración para denegar páginas ha sido exitoso.

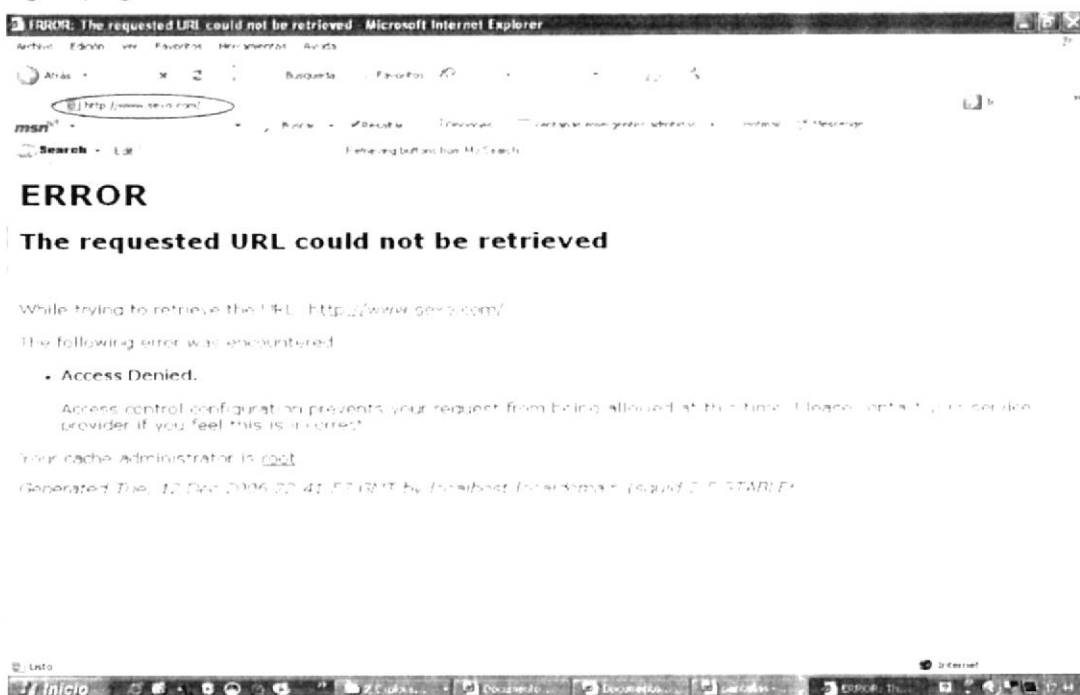
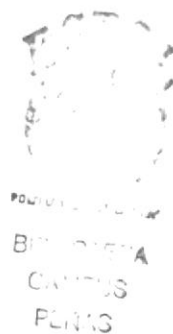


Figura 6-163: acceso denegado



6.31.4. COMPROBACIÓN DE DENEGACIÓN POR TIEMPO

Paso 40 Ingresar al explorador de Windows, escribir en la dirección de url : cualquier página en este ejemplo se escogió www.yahoo.com , y se puede ver en la pantalla que sale acceso denegado porque no se encuentra en un horario permitido de navegación

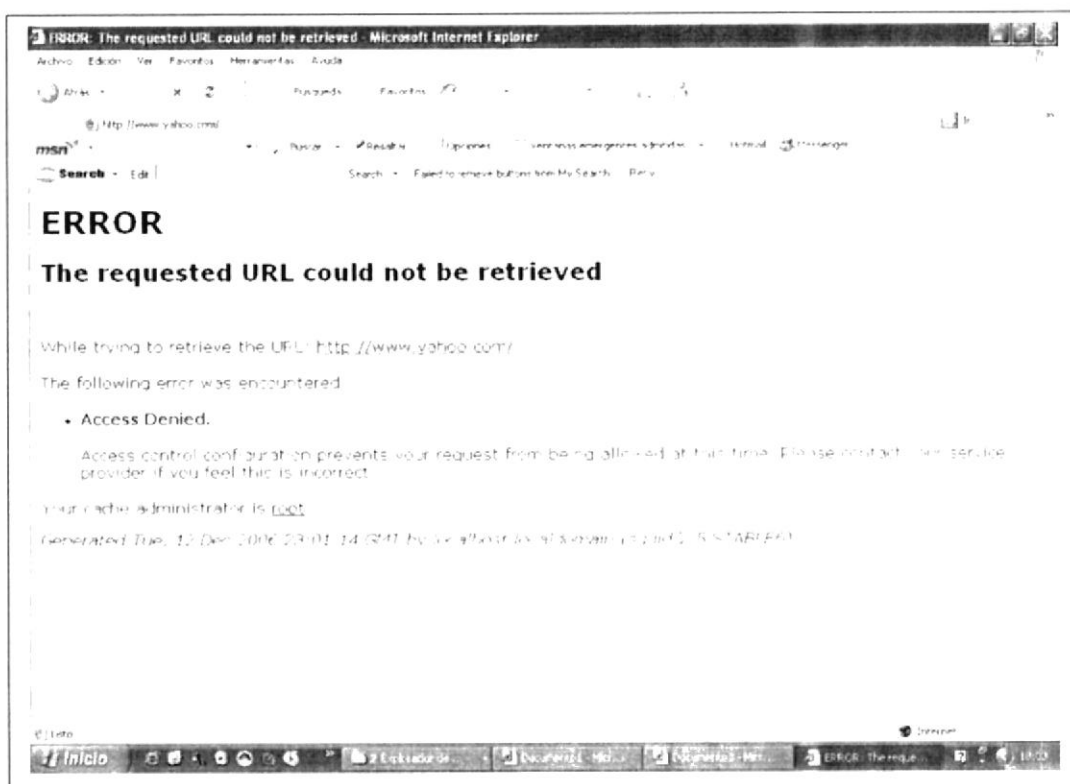
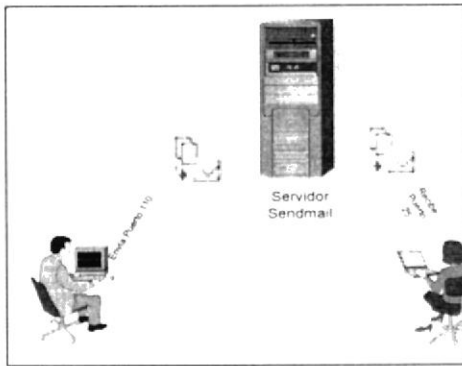


Figura 6-164: acceso negado por tiempo

6.32 SERVIDOR SENDMAIL



El Correo Electrónico es un sistema que permite a los usuarios enviar y recibir mensajes a través de la Internet. SMTP es un protocolo que asegura este sistema para enviar y recibir Información de una manera fluida.

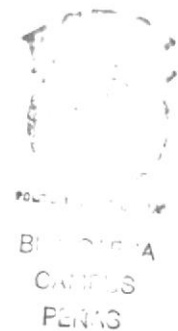
En muchos aspectos, el correo electrónico o e-mail (electronic mail) es similar al correo postal. Al igual que este se utiliza para enviar cartas u otra Información a gente conocida.

SMTP

Por otro lado, el protocolo SMTP, en su versión original, no dispone de mecanismos de autenticación del usuario que envía un mensaje. Esto permite el uso fraudulento de servidores SMTP por parte de personas ajenas a la organización, así como el envío de mensajes con remite falso.

Para paliar estas "deficiencias", se han generalizado mecanismos de control de acceso a los servidores SMTP basados en la confianza respecto a clientes locales o en la desconfianza respecto a determinadas organizaciones "fichadas" como origen de correo basura. Si bien es cierto que estas medidas han conseguido limitar el uso fraudulento de los servidores SMTP de las organizaciones por parte de terceros, no han conseguido evitar el envío de mensajes falsificados desde el interior de la organización y han dificultado la utilización del servicio a personas de la organización con necesidad de desplazarse.

Servidor de correo. El elemento fundamental del correo Internet es el Servidor de correo (mail server), un ordenador dedicado a almacenar los mensajes que usted envía y recibe, y que funciona como buzón donde se depositan todos los mensajes de entrada y salida. Por supuesto, el servidor de correo cumple un papel trascendental tanto en el envío como en la recepción de correo.



6.32.1. ENVIAR MENSAJES (SERVIDOR DE CORREO SMTP)

Cuando usted abre su programa de correo y envía un mensaje, lo que realidad hace el programa de correo es enviar el mensaje desde su ordenador servidor de correo y luego se desconecta. A partir de ese momento, es el servidor correo quién se encarga de enviar el mensaje al destinatario buscando la ruta más adecuada, comprobando que existe un destinatario con esa dirección y reintentándolo las veces que haga falta (cuando el servidor de correo del destinatario está desconectado temporalmente). El protocolo utilizado para enviar correo desde servidor de correo a otro, incluso desde su ordenador al servidor de correo,

Se denomina SMTP (Simple mail Transfer Protocol). Y, por extensión, el servidor de correo que envía sus mensajes hasta los destinatarios finales se llama SMTP .

6.32.2. (SERVIDOR DE CORREO POP)

Cuando a usted le envían un mensaje, dicho mensaje se está enviando servidor de correo, el cual tiene un buzón especial para usted donde se depositan todos los mensajes que le lleguen. En cualquier momento, usted puede conectarse con el servidor de correo y recoger los mensajes que han llegado a su buzón particular. Protocolo utilizado para conectarse a un servidor de correo y recoger en el buzón mensajes pendientes de leer se llama POP (Post Office Protocol) y actualmente utiliza la versión 3 (POP3), y el servidor de correo que recibe y guarda los mensajes que le envían los usuarios se llama servidor POP (servidor POP3).

6.32.3. OBJETIVO DE SERVIDOR POP

Cuenta en servidor de correo. Como se estará imaginando, tiene que haber algún método fiable y seguro para asegurar la privacidad de los mensajes que se envían y reciben servidor de correo. En caso contrario, cualquier usuario que estuviera en Internet podría conectarse con el servidor de correo de su proveedor y leer sus mensajes. Para ello, todos servidores de correo, ya sean SMTP, POP o SMTP/POP, sólo permiten el acceso a usuarios que tienen abierta una cuenta en ellos. Una cuenta es simplemente un nombre usuario y una contraseña que comprueban su identidad y le abren el acceso a los mensajes su buzón exclusivo. Por tanto, cuando un programa de correo se conecta con un servidor correo para enviar o recibir un mensaje, lo primero que debe hacer es introducir el nombre usuario y la contraseña para conectarse al servidor y, luego, enviar o recibir el mensaje.

6.32.4. OBJETIVO DE SERVIDOR DE CORREO

Independencia de los usuarios de sistema y las cuentas de correo electrónico.

Un dominio principal donde se crean cuentas de correo.

Múltiples dominios virtuales con redirecciones a las cuentas del dominio principal.

Transporte seguro del tráfico mediante.

Acceso a los buzones por IMAP y por webmail.

Listas de correo.

6.33 CONFIGURACIÓN DEL SERVIDOR SENDMAIL EN LINUX

Paso 1 Verificar si está instalado el servicio sendmail y dovecot, utilizando los siguientes comandos:

rpm:Verifica paquetes instalados -q nombre_paquete: sendmail

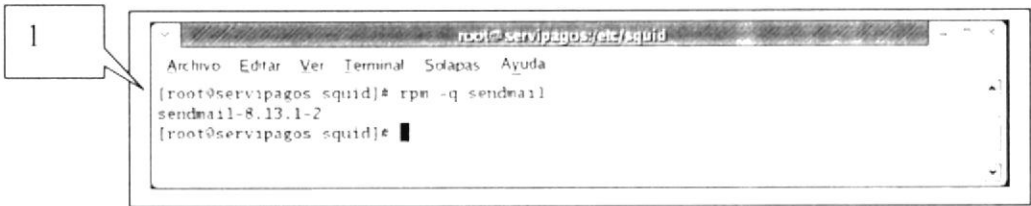


Figura 6-165: verificación de paquete sendmail

Paso 2 Verificar la herramienta dovecot

rpm:Verifica paquetes instalados -q nombre_paquete:dovecot

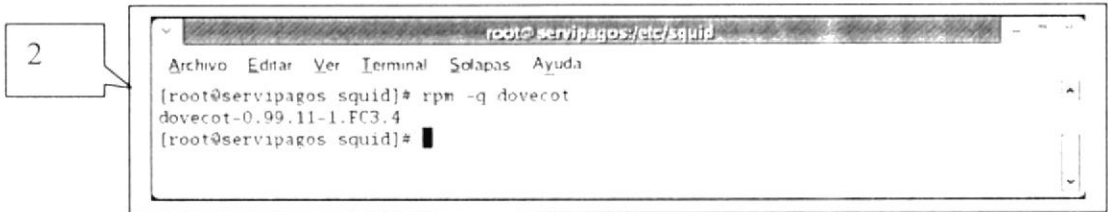


Figura 6-166: verificación de paquete dovecot

Paso 3 Editar el archivo de dovecot.conf



Figura 6-167: ingreso a DOVECOT

El paquete imap es reemplazado por dovecot, el cual funciona como otros servicios. Se debe modificar el fichero /etc/dovecot.conf y habilitar los servicios de imap y/o pop3 del siguiente modo (de modo predefinido están habilitados imap e imaps):

Paso 4 Habilitar protocolos y Agregar pop3 que es por donde escucha el puerto 110 (ver recuadro rojo)

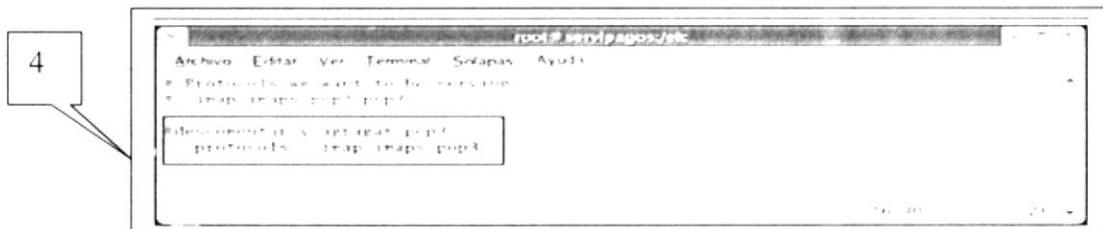


Figura 6-168: protocolo agragado

Paso 5 Ingresar a mail para editar sendmail.cf

Vi sendmail.cf :

Este parámetro permite establecer el mensaje de bienvenida al establecer la conexión al servidor. Es posible ocultar el nombre y al versión de sendmail, esto con el objeto de agregar seguridad por secreto. Funciona simplemente haciendo que quién se conecta hacia el servidor no pueda saber que software con ellos dificultar que el servicio sea vulnerable.

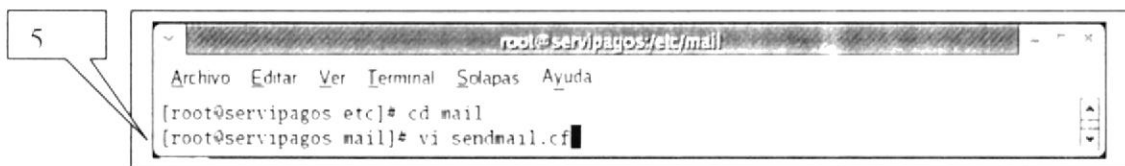


Figura 6-169: editamos sendmail

Paso 6 De modo predefinido **Sendmail** escucha peticiones a través de la interfaz de retorno del sistema a través de **IPv4** (127.0.0.1) y no a través de otros dispositivos de red. Solo se necesita eliminar la restricción de la interfaz de retorno para poder recibir correo desde Internet o la LAN. Localice la siguiente línea: Por primera vez se busca de la siguiente manera /127 se encuentra la dirección de lookback se la cambia por 0.0.0.0 y se la habilita como muestra esta pantalla, ver recuadro rojo

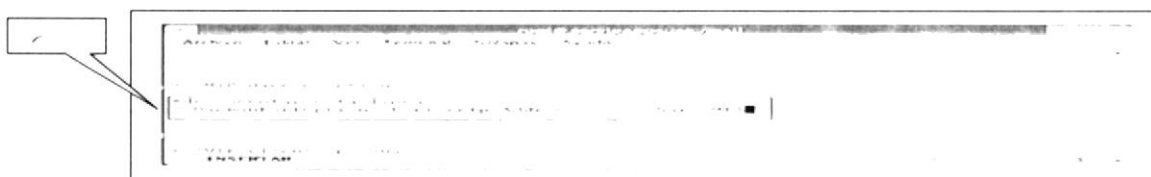


Figura 6-170: cambios en loopback

Paso 7 Añadir al final del fichero /etc/mail/sendmail.cf un parámetro que defina que dominio.com se va a utilizar, se trata de un dominio local. Note que no debe haber espacios entre Cw y dominio.com, y que Cw se escribe con una C mayúscula y una w minúscula. (ver recuadro rojo)

Ej: Cwservipagos.com

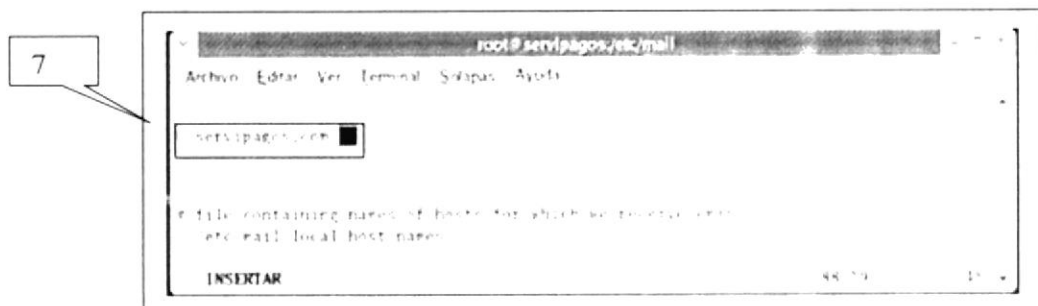


Figura 6-171: Ingreso de dominio

Paso 8 Ingresar a cd/etc/sysconfig/ para editar con el fin que el sistema de configuración lea el siguiente dominio SERVIPAGOS.COM

Cd /etc/sysconfig : En el directorio de sistema de configuración se guardan todos los servicios instalados en el equipo

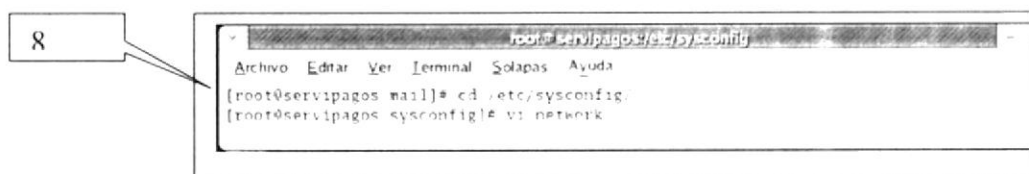


Figura 6-172: configuración de network

Paso 9 Se modifica y se agrega lo siguiente como dominio local Ej:

HOSTNAME=SERVIPAGOS.COM

HOSTNAME Visualiza el nombre de la máquina Se ingresa el dominio local a utilizar en el servidor de Send mail



Figura 6-173: ingreso de dominio

Paso 10 Ingresar a editar el hosts

Vi hosts: Se edita la ruta de origen en la lista de host.

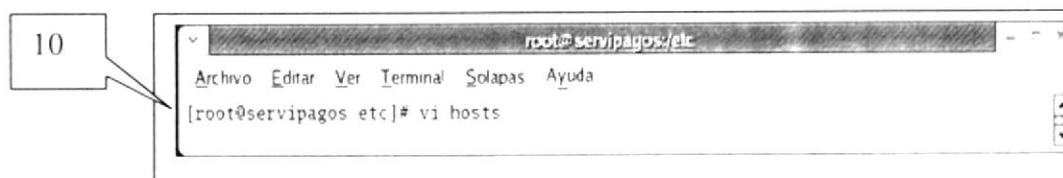


Figura 6-174: ingreso a vi hosts

Paso 11 Cambiar localhost.localdomain localhost por www.servipagos.com servipagos.com

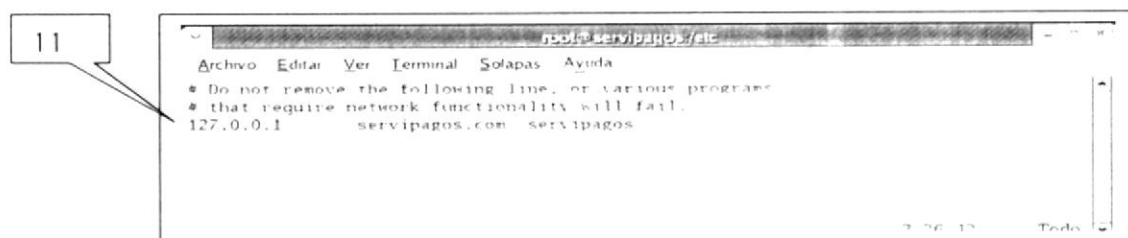


Figura 6-175: direccionamiento de dominio

Paso 12 Reiniciar los servicios de sendmail de la siguiente manera



Figura 6-176: reinicio de sednmail

service nombre_servicio start Inicia el servicio especificado "nombre_servicio"

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

Nota: Para que arranque los servicios de Servidor al inicializar el computador realizar los siguientes pasos

a) Si se tiene problemas entrar en el setup

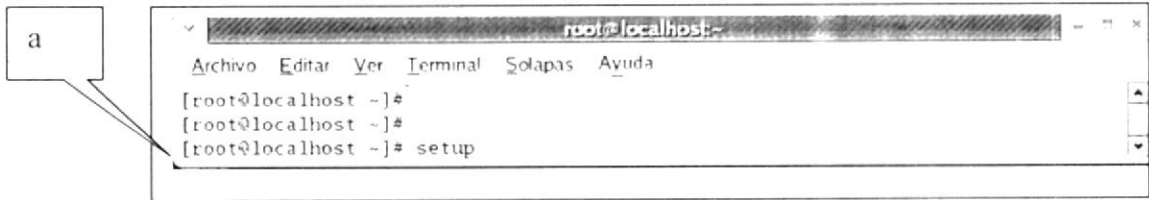


Figura 6-177: ingreso del setup

b) Ingresar a Servicios del Sistema



Figura 6-178: ingreso al servicio de sistema

c) Ingresar a esta pantalla, y con las teclas direccionales buscar **SQUID**

d) elegir y presionar la barra espaciadora, dar **OK**

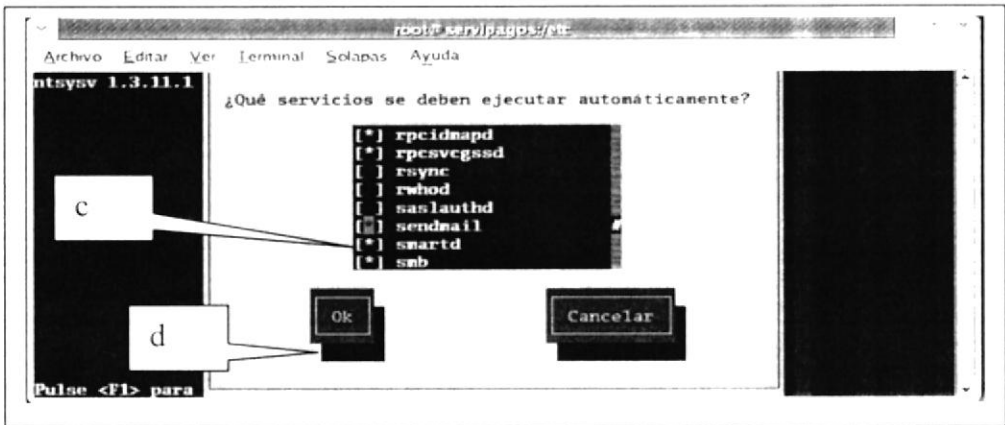


Figura 6-179: elección de paquete sendmail

Paso 13 Para verificar los mail si se envía un mail al root

```
[ ]# mail silvia@servipagos.com
```

Subject: tercera prueba

Cc:/root

Se finaliza el mensaje con punto

- Para verificar un mail desde el usuario administrador (root)

```
[ ]# su -
```

```
[ ]# mail
```

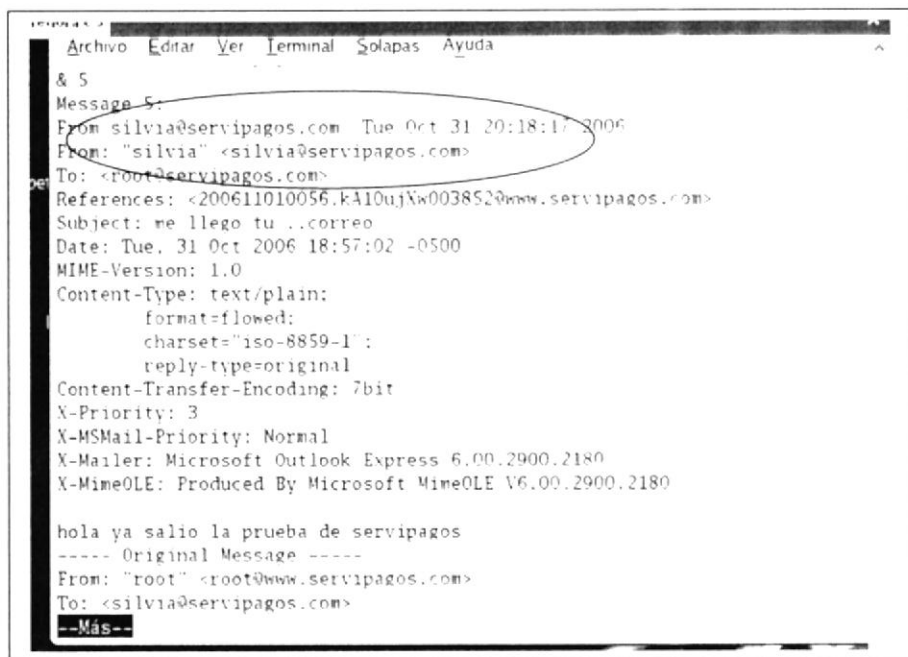


Figura 6-180: lectura de mail

6.34 CONFIGURACIÓN EN EL CLIENTE WINDOWS

Paso 14 Ingresar a configurar el Outlook Express, dar clic en el botón inicio y elegir la opción de correo electrónico.

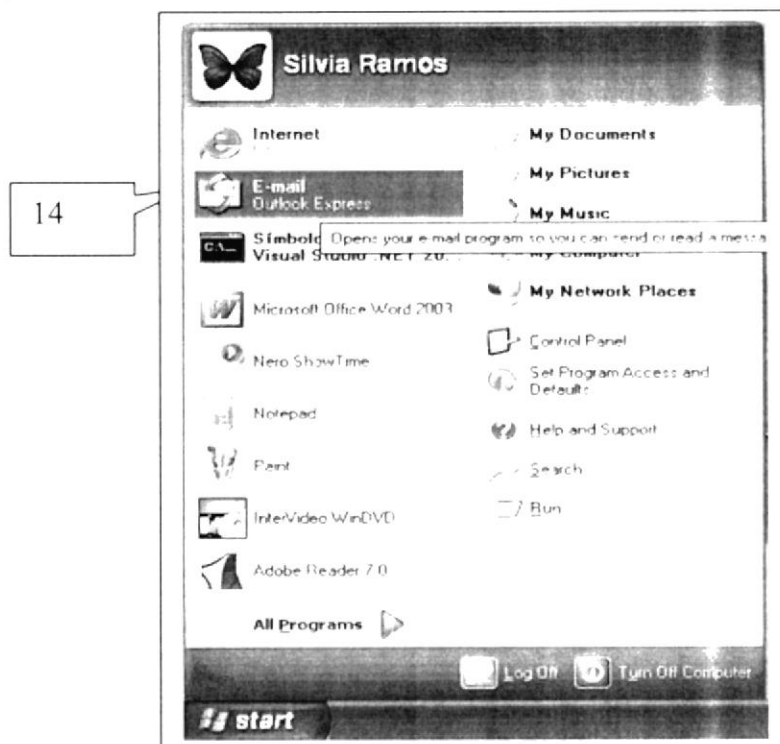


Figura 6-181: ingreso al outlook Express

Paso 15 Se abrirá la pantalla principal del Outlook Express en la cual se va a empezar a realizar la configuración, dar clic en herramientas y seleccionar cuentas de correos como se lo detalla a continuación.

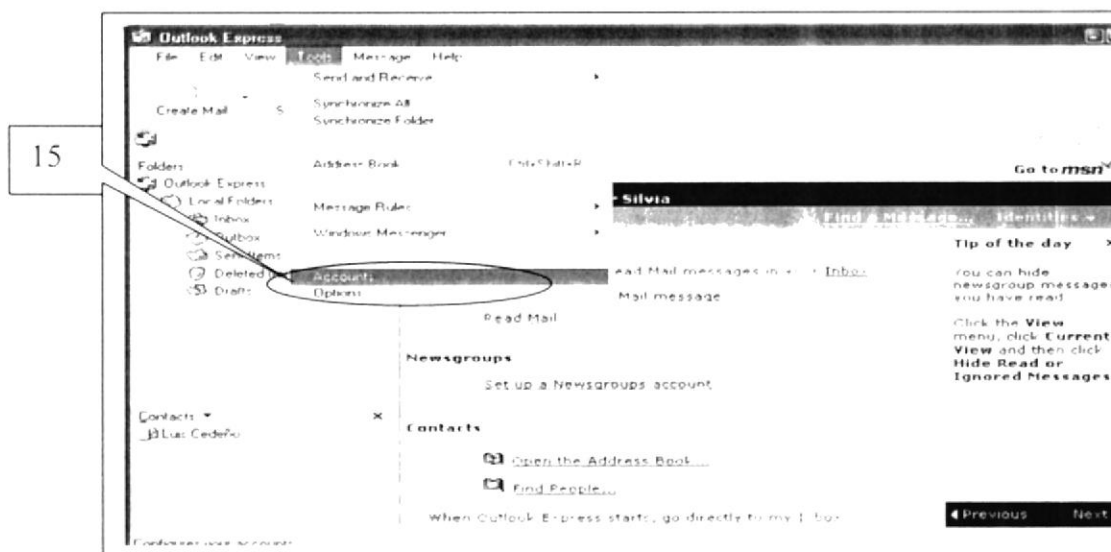


Figura 6-182: ingreso a cuentas

Paso 16 Aparecerá la siguiente pantalla a manera de un asistente para poder configurar la nueva cuenta de correo electrónico, en la cual se da clic en agregar y se elige la opción correo.

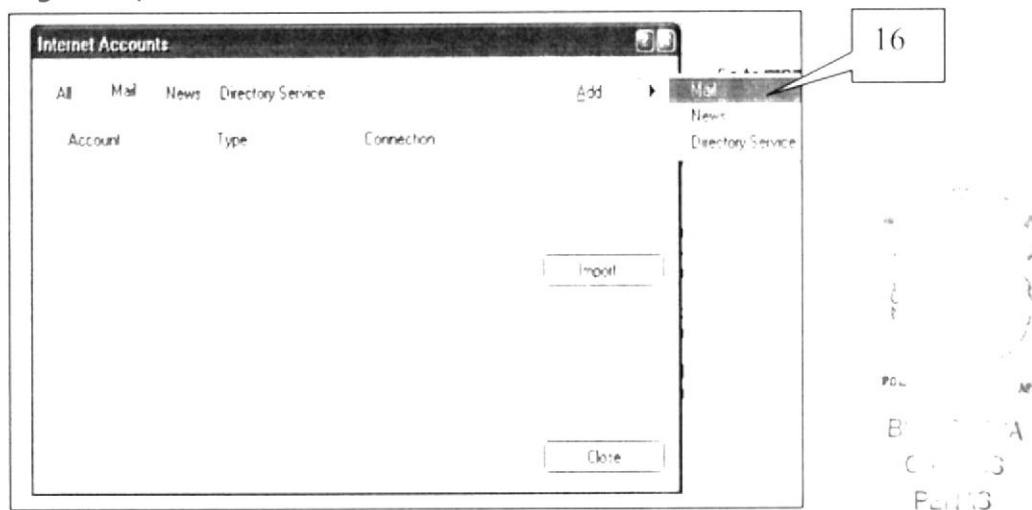


Figura 6-183: agregar cuenta

Paso 17 Ingresar al Outlook Express y colocar un nombre para mostrar, clic en **Siguiente**.

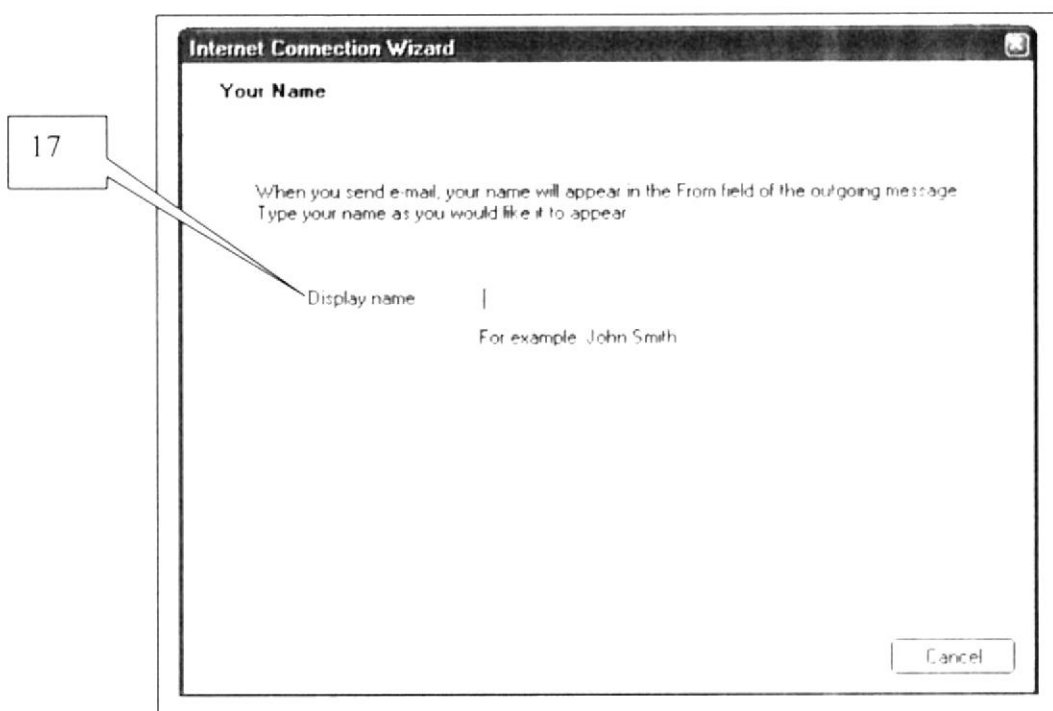


Figura 6-184: nombre de cuenta

Paso 18 Colocar la dirección de correo asociado al usuario que se ha creado en Linux, clic en **Siguiente**.

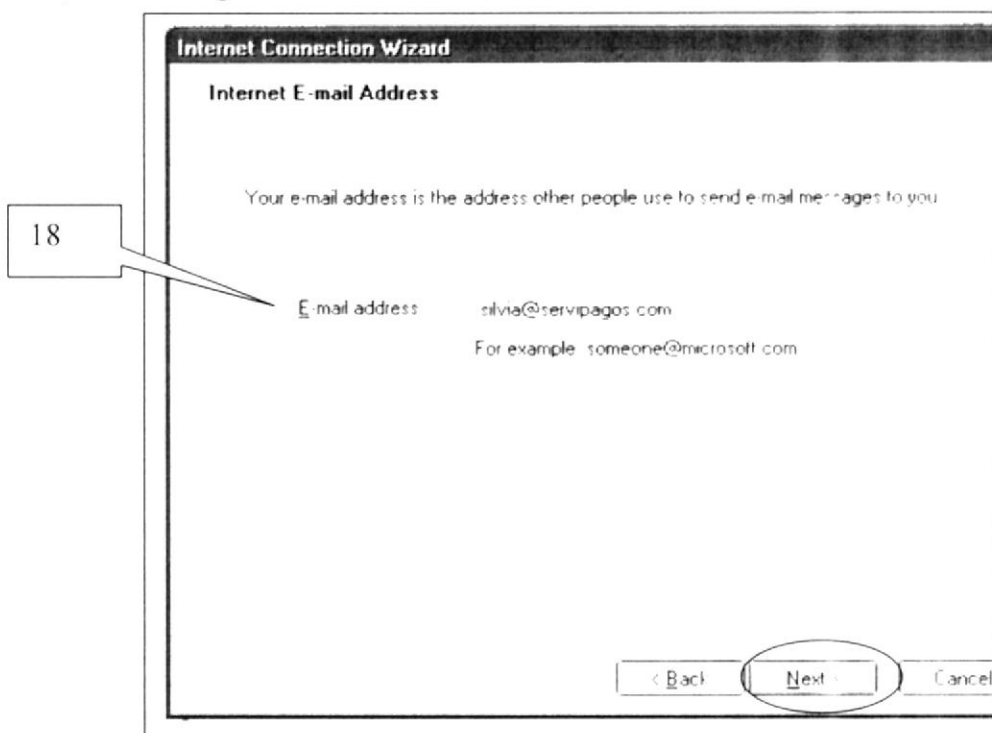


Figura 6-185: nombre de usuario con dominio

Paso 19 Especificar el servidor de correo entrante (POP3)

Paso 20 el servidor de correo saliente (SMTP), se refiere a la misma dirección del servidor Linux, clic en **Siguiente**

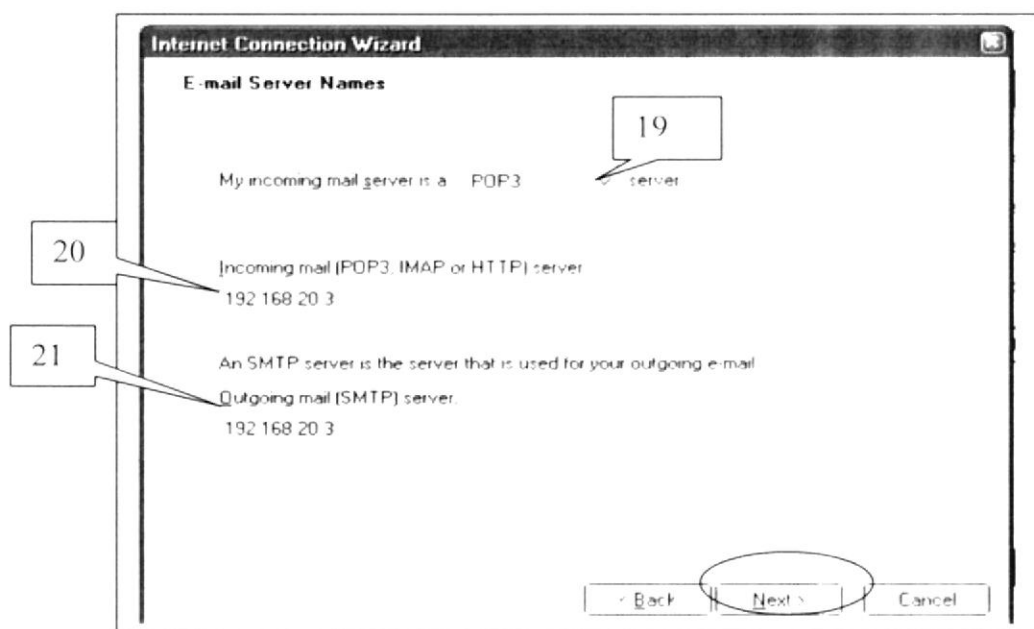


Figura 6-186: ingreso de protocolo y ip del servidor

Paso 22 Ingresar el nombre de usuario y contraseña proporcionado por el servidor Linux, clic en **Siguiente**.

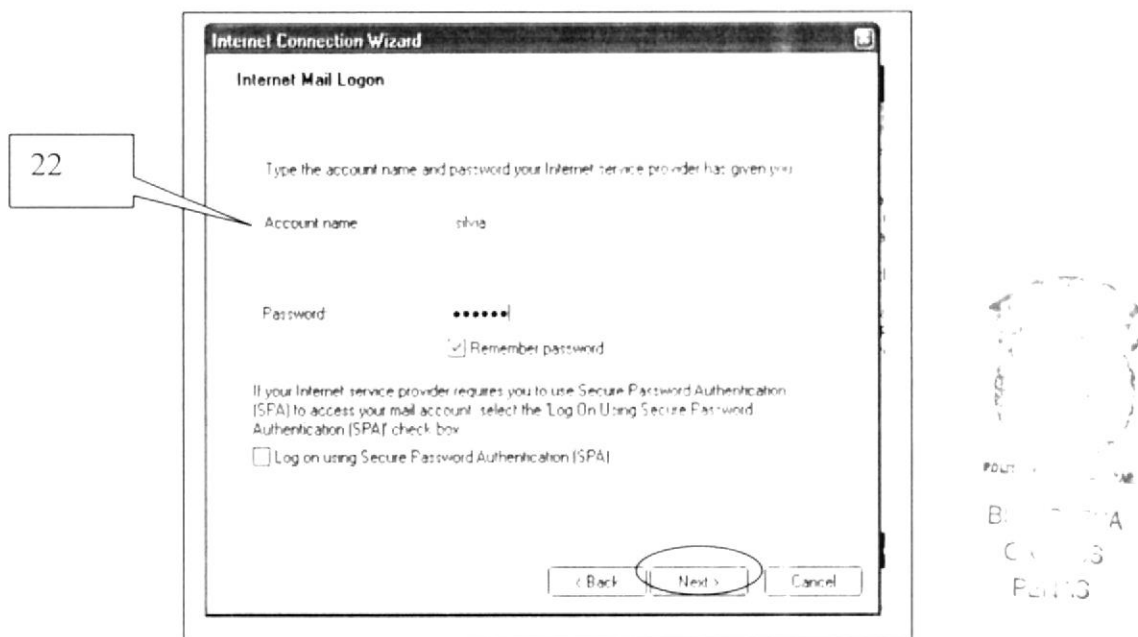


Figura 6-187: ingreso de cuenta y clave nueva

Paso 23 Hacer Click en finalizar para verificar que la información escrita anteriormente esta correcta.

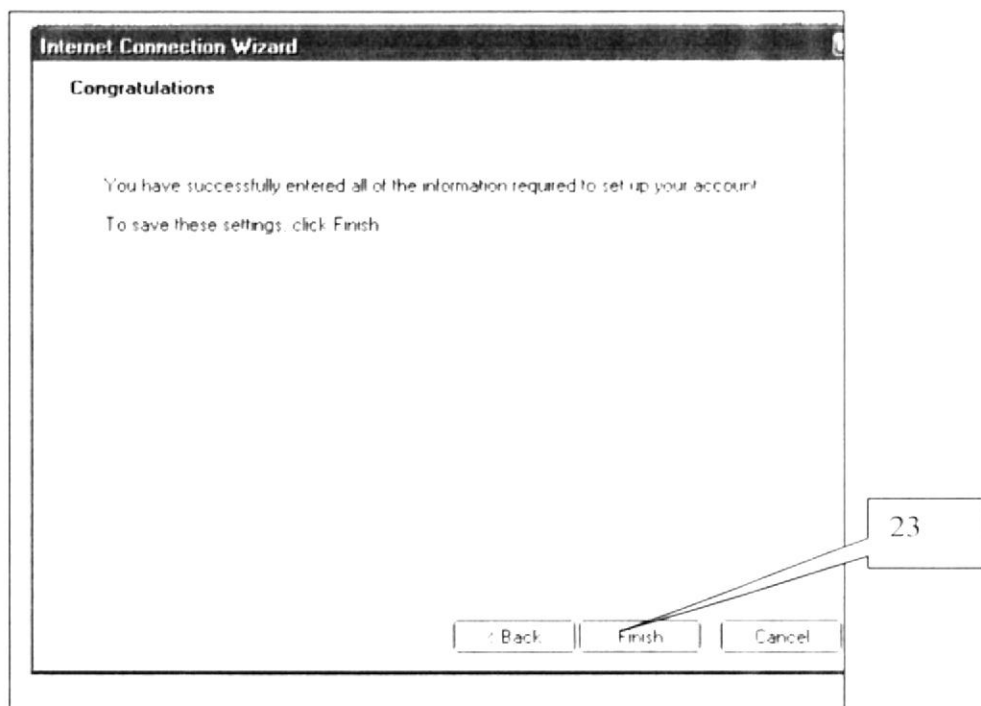


Figura 6-188: finalización de cuenta

Paso 24 Visualizar una pantalla con las cuentas de correo que existen, a la vez la cuenta que está como predeterminada en este caso **192.168.20.3**

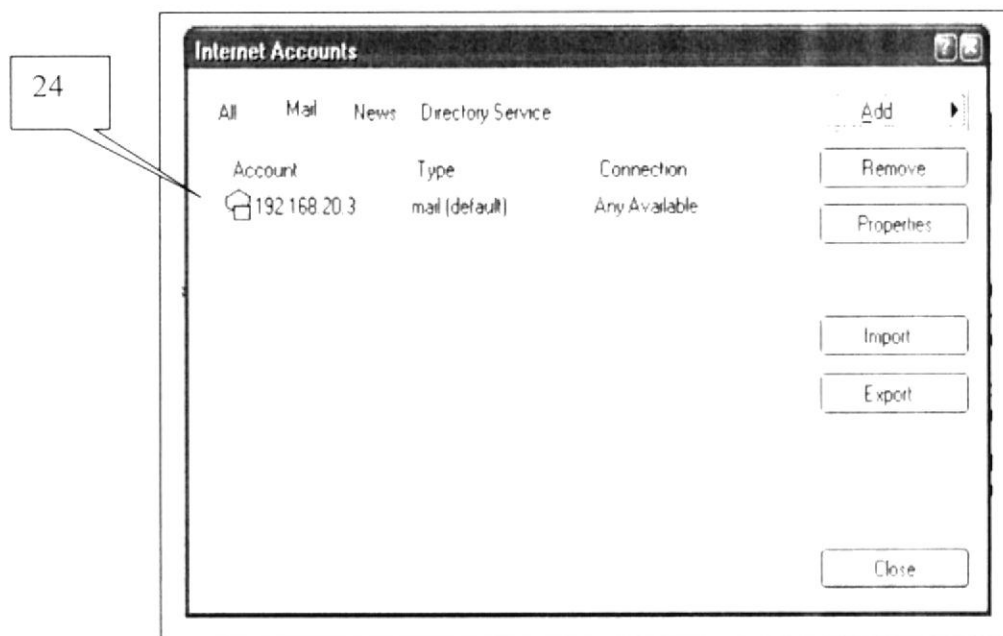


Figura 6-189: vista de conexión con el servidor

Paso 25 Ahora se podrá enviar y recibir mensajes de correos de los usuarios creados en el servidor Linux. (Ver los cuadros rojos)

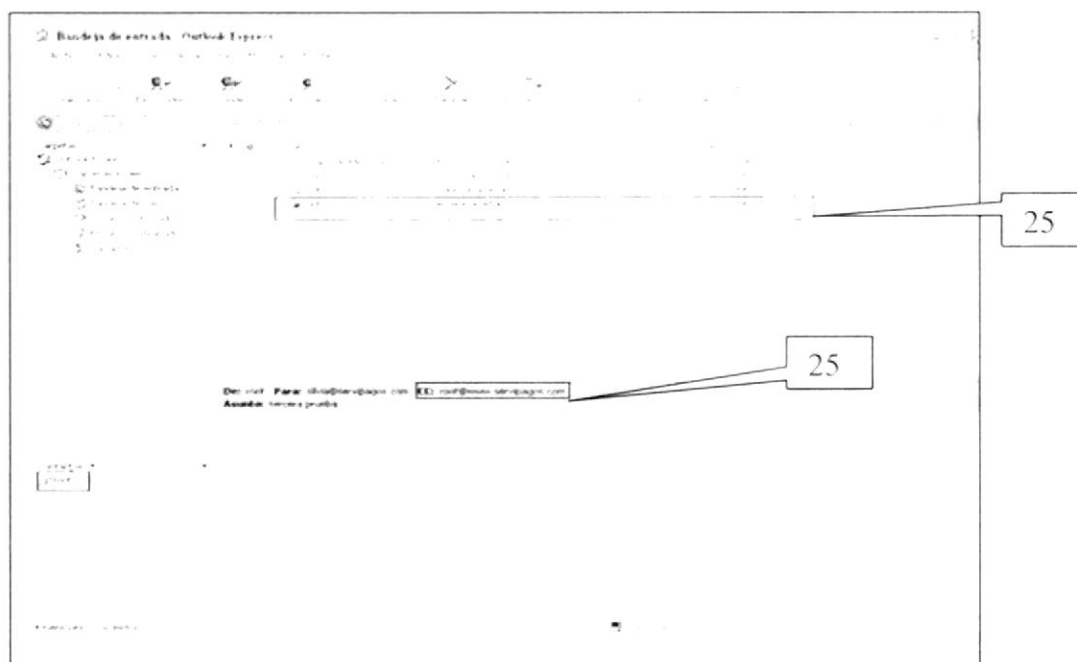


Figura 6-190: vista de llegada de correo

Paso 26 Dar doble clic en root para leer lo que se ha enviado, Aparece la siguiente pantalla donde se muestra que root tiene el dominio que se crea en el servidor linux

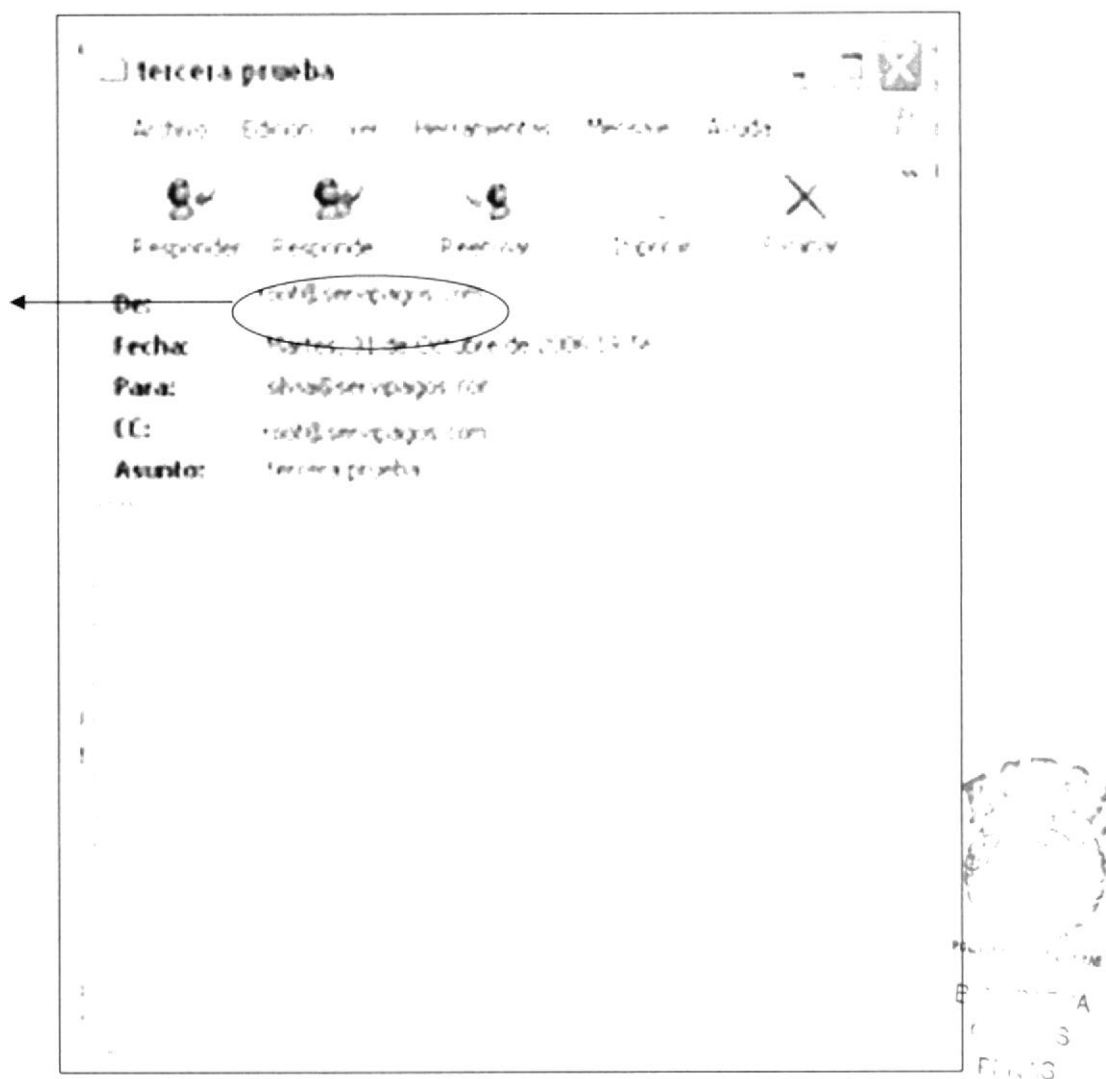


Figura 6-191: ingreso al mail que llego desde Linux

6.35 SERVIDOR FIREWALLS



La traducción más acertada de este término inglés al idioma español es la palabra cortafuegos. Se ve cual es la definición en el DRAE1.

<<Cortafuego o cortafuegos. (De cortar y fuego). m. Agr. Vereda ancha que se deja en los sembrados y montes para que no se propaguen los incendios. || 2. Arq. Pared toda de fábrica, sin madera alguna, y de un grueso competente, que se eleva desde la parte inferior del edificio hasta más arriba del caballete, con el fin de que, si hay fuego en un lado, no se pueda este comunicar al otro.

Estas dos definiciones ya introducen una idea muy aproximada al significado de la palabra firewall en términos informáticos, en ellas, aparecen términos como lado, lo que implica la existencia de dos o más partes y comunicar lo que pone de manifiesto que las partes están conectadas.

Bien, pues casi sin analogías, eso es un firewall en términos de sistemas computacionales.

Un cortafuegos, es un sistema informático, simple o compuesto que actúa como punto de conexión segura entre otros dos o más sistemas informáticos.

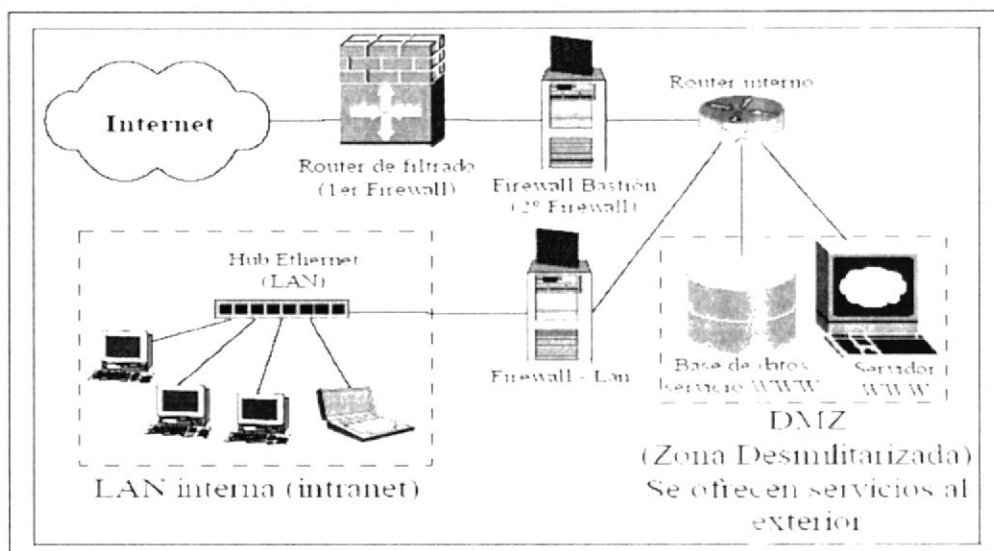


Figura 6-192: esquema de firewall

6.35.1. INTRODUCCIÓN A IPTABLES.

Lo Iptables es como se conoce al módulo Netfilter, la herramienta estándar actual de cortafuegos bajo el sistema operativo l10 estándar Linux de cortafuegos.

En realidad, es suficiente con kernels compatibles con NETFILTER. Es decir, recompilando un kernel de la serie 2.3.15. Como antes, no puedo afirmar que en futuras versiones no se sustituya IPTables por una nueva herramienta. Es decir, que si en el momento de leer esto, transcurre el año 2010, dudo que el documento le aporte nada útil.

Como siempre, el término actual en este mundo informático, no puede alejarse más de unos pocos meses a partir de la fecha de elaboración del documento.

6.35.2. REGLAS DE IPTABLES

Bajo iptables, cada paquete filtrado se procesa únicamente usando las reglas de una cadena, en lugar de hacerse con múltiples. Es decir, un paquete FORWARD que llega al sistema usando ipchains tendrá que pasar por las cadenas INPUT, FORWARD, y OUTPUT para llegar a su destino. Con iptables, el paquete tan solo se envía a la cadena INPUT si su destino es el sistema local y tan solo los envía a la cadena OUTPUT si el sistema local es quién genera los paquetes. Por esta razón, deberá estar seguro de situar la regla destinada a interceptar un paquete en particular en la cadena adecuada que será la que vea el paquete. La principal ventaja es que tendrá un control más refinado sobre la disposición de cada paquete. Si está intentando bloquear el acceso a un sitio web en particular, ahora es posible bloquear los intentos de acceso desde clientes que están en máquinas que utilicen el servidor como pasarela (gateway). Una regla OUTPUT que deniegue el acceso no prevendrá más el acceso a las máquinas que utilicen el servidor como pasarela.

El objetivo DENY ha sido cambiado por DROP. En ipchains, los paquetes que cumplían una regla en una cadena podían ser redirigidos a un objetivo DENY, que dejaba caer el paquete en silencio. Este objetivo deberá cambiarse a DROP con iptables para obtener el mismo resultado.

El comando iptables es un poco más reticente sobre el lugar que ocupan las diferentes opciones. Por ejemplo, ahora se debe especificar el puerto origen y destino después del protocolo (ICMP, TCP, o UDP) que se vaya a utilizar en una regla de una cadena.

- Cuando se especifica las interfaces de red que se va a usar en una regla, se debe utilizar sólo interfaces de entrada (opción -i) con cadenas INPUT o FORWARD y las de salida (opción -o) con cadenas FORWARD o OUTPUT. Esto es necesario debido al hecho de que las cadenas OUTPUT no se utilizan más con las interfaces de entrada, y las cadenas INPUT no son vistas por los paquetes que se mueven hacia las interfaces de salida

6.35.3. COMANDOS PARA AÑADIR Y MANIPULAR CADENAS

COMANDOS BÁSICOS

Iptables -F: Borrado de reglas

Iptables -L: Listado de reglas que se están aplicando

Iptables -A: Agregar regla

Iptables -D: Borrar una regla

TIPOS DE REGLAS

Input : Entrada al servidor

Output: Servidor hacia fuera

Fordward: Redireccionar

ACCIONES

Accepts : Acepta la regla

Drop : Borra la regla

6.36 COMANDOS STANDAR PARA CONFIGURACIÓN DE FIREWALL

Comandos Estándar para configuración de Firewalls

A=Add D>Delete S=Origen P=Protocolo J=Acción Aplicar

Bloquear PING

```
Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p icmp -j DROP
```

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

Extensiones ICMP:

icmp-type: Puede especificarse el tipo de mensaje ICMP tanto por su número como por los siguientes identificadores: echo-request, echoreply, source-quench, time-exceeded, destination-unreachable, network-unreachable, host-unreachable, protocol-unreachable, y port-unreachable.

-DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).



6.36.1. BLOQUEAR TELNET

Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p tcp --dport 23 -j DROP

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

23 Puerto de Telnet

-DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).

6.36.2. BLOQUEAR SMPT

Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p tcp --dport 25 -j DROP.

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

25 Puerto de SMPT

-DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).

6.36.3. BLOQUEAR FTP

Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p tcp --dport 21 -j DROP.

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

21 Puerto de FTP

-DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).

6.36.4. BLOQUEAR HTTP

```
Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p tcp --dport 80 -j DROP
```

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

80 Puerto de **FTP**

-DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).



6.36.5. BLOQUEAR DNS

Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p tcp --dport 53 -j DROP.

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

53 Puerto de DNS

-DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).

6.36.6. BLOQUEAR POP3

```
Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p tcp --dport 110 -j DROP
```

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

110 Puerto de POP3

-DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).



Nota: Para que arranque los servicios de Servidor al inicializar el computador realizar los siguientes pasos

a) Si se tiene problemas entrar en el setup

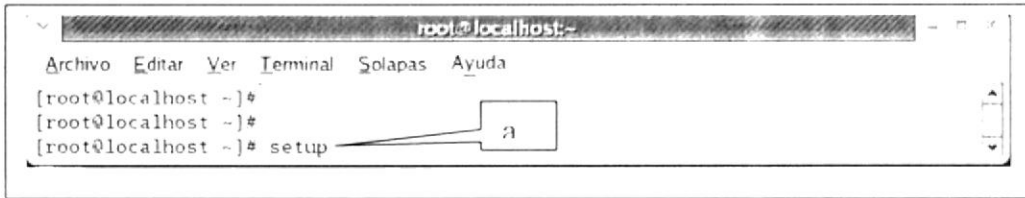


Figura 6-193: ingreso al setup

b) Se Ubica en **Configuración del Firewall** presionar la tecla enter para ingresar



Figura 6-194: configuración de firewall

c) Se ubica en **Habilitar** con la **tecla TAB** presionar **barra espaciadora** en habilitados y se ubicar en **Aceptar**, presionar esa opción.

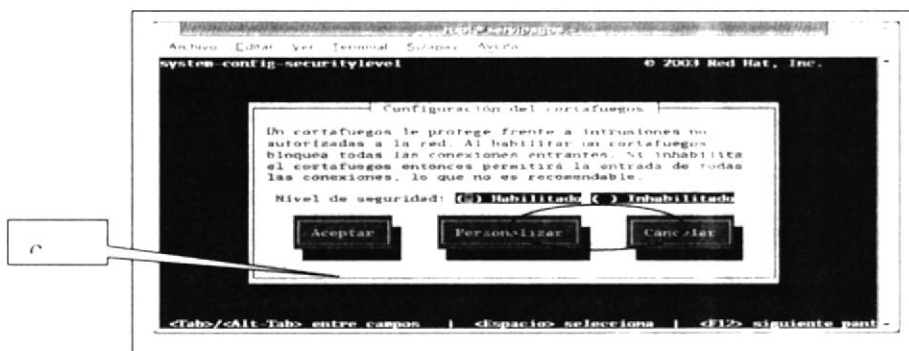


Figura 6-195: configuración de cortafuego

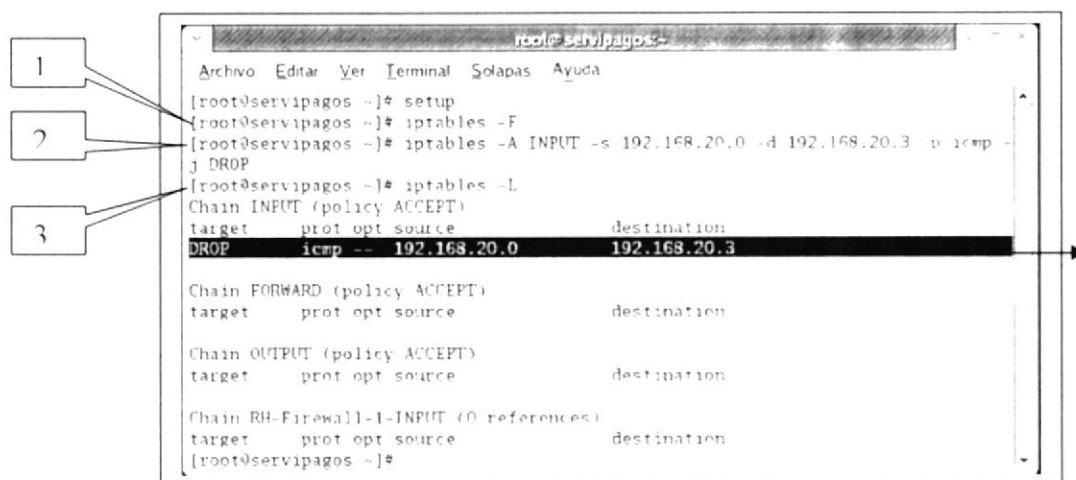
d) Salir de las herramientas.

Paso 1 Borrar los firewalls con el siguiente comando
iptables -F

Bloquear el ping

Paso 2 Iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p icmp -j DROP

Paso 3 Revisar con el comando **iptables -L**



```
root@servipagos:~  
Archivo Editar Ver Terminal Solapas Ayuda  
[root@servipagos ~]# setup  
[root@servipagos ~]# iptables -F  
[root@servipagos ~]# iptables -A INPUT -s 192.168.20.0 -d 192.168.20.3 -p icmp -j DROP  
[root@servipagos ~]# iptables -L  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
DROP icmp -- 192.168.20.0 192.168.20.3  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
Chain RH-Firewall-1-INPUT (0 references)  
target prot opt source destination  
[root@servipagos ~]#
```

Figura 6-196: regla creada



6.36.7. ACEPTACIÓN DE REGLAS

Paso 1

```
Iptables -A INPUT -s 192.168.20.5/32 -d 192.168.20.3 -p icmp -j ACCEPT
```

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.5)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla. (192.168.20.3)

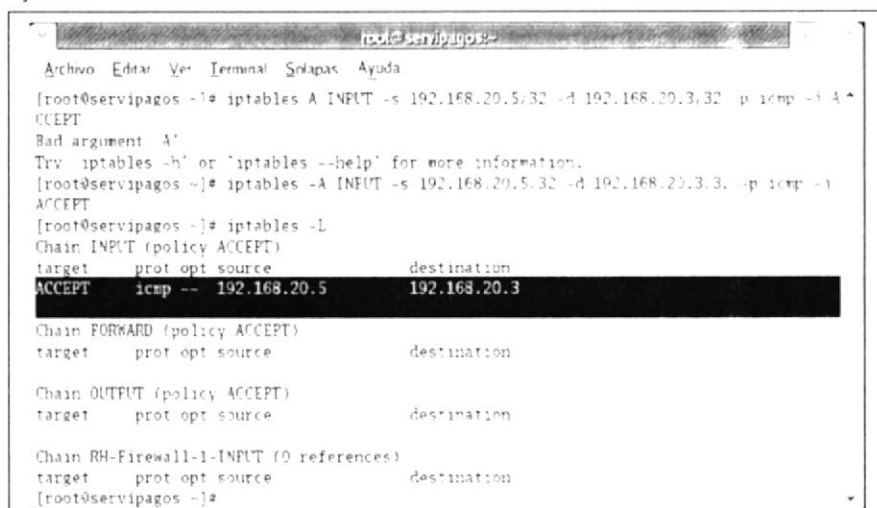
-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

23 Puerto de Telnet

-ACCEPT: Acepta una regla de una chain (se puede indicar el orden o su condición).



```

root@servipagos:~# iptables -A INPUT -s 192.168.20.5/32 -d 192.168.20.3 -p icmp -j ACCEPT
Bad argument 'A'
Try 'iptables -h' or 'iptables --help' for more information.
root@servipagos:~# iptables -A INPUT -s 192.168.20.5/32 -d 192.168.20.3 -p icmp -j ACCEPT
root@servipagos:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT icmp -- 192.168.20.5 192.168.20.3
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain RH-Firewall-1-INPUT (0 references)
target prot opt source destination
root@servipagos:~#
  
```

Figura 6-197: visualización de regla creada

Paso 2 Editar el Firewall

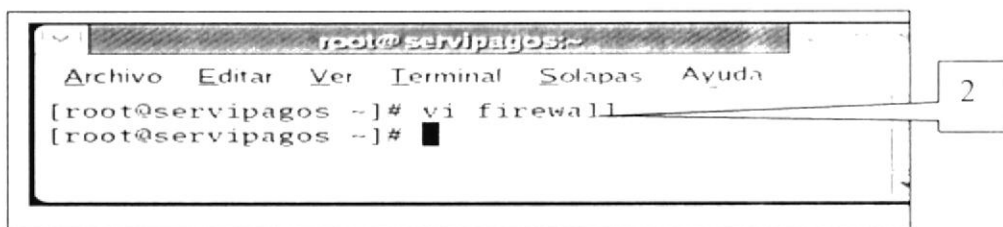


Figura 6-198: editamos el firewall

Paso 3 Escribir la regla anterior y guardar en FIREWALL

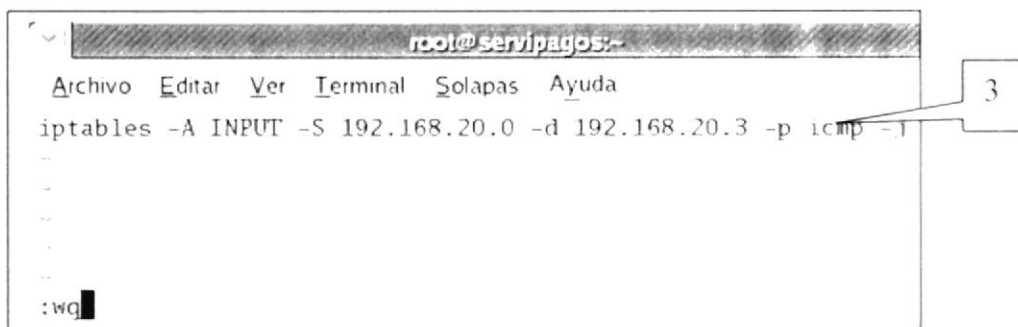


Figura 6-199: creación de regla

Paso 4 Dar los permisos con **chmod 777** firewall y se lo visualiza con **ls f***

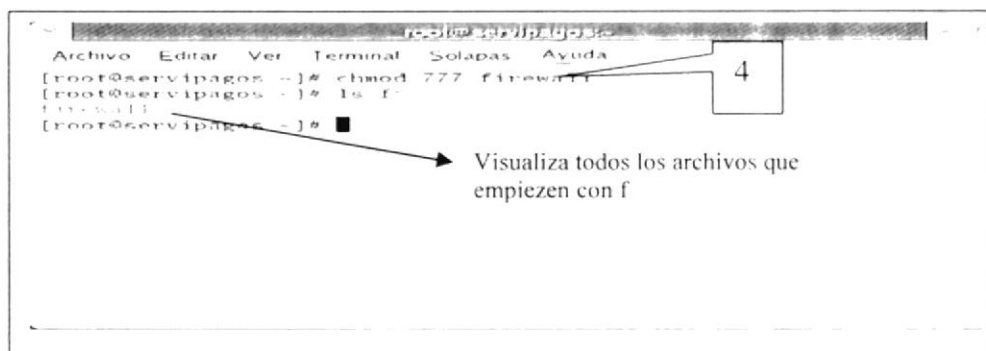


Figura 6-200: permisos a firewall

BIOMEDICA
CIVILIS
FELIX

Paso 5 Ingresar a editar vi rc.local

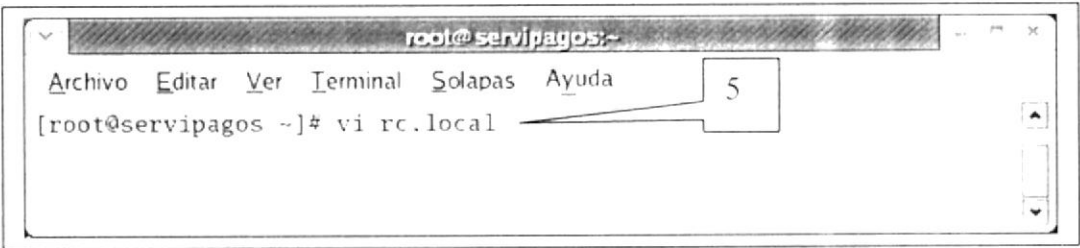


Figura 6-201: vi rc.local

Paso 6 Escribir la siguiente ruta y guardar ver ejemplo /etc/firewall

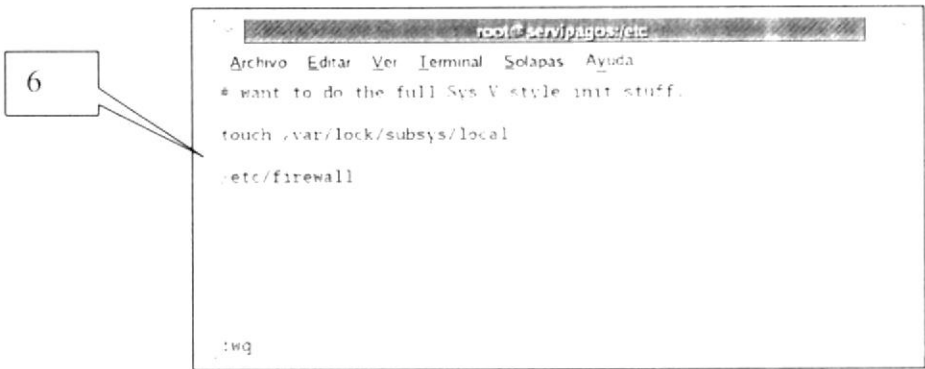


Figura 6-202: configuración de rc.local

Paso 7 Habilitar TELNET, Ingresar a etc el comando cd xinetd.d

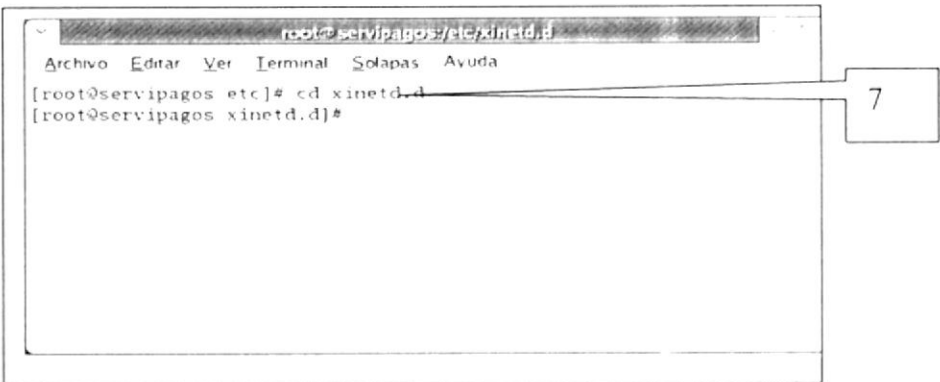


Figura 6-203: ingreso a xinetd

Paso 8 Ingresar habilitar telnet con el comando **vi kbr5-telnet**

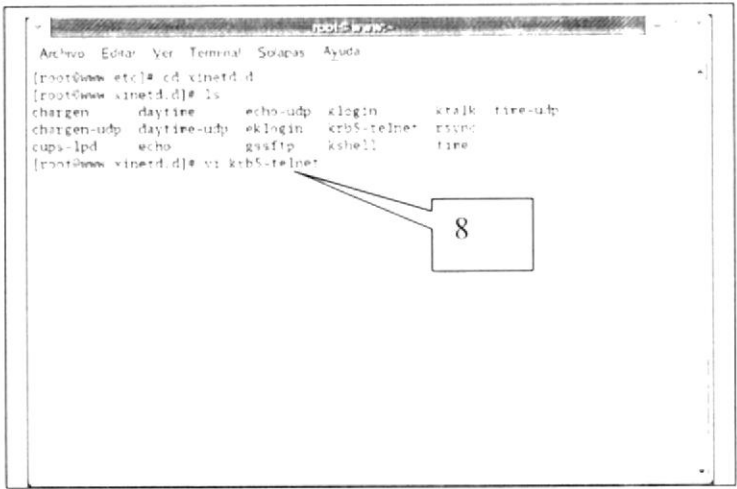


Figura 6-204: habilitamos telnet

Paso 9 Luego de presionar intro, ingresar al editor de telnet, donde se cambia en **disable** que diga **no**

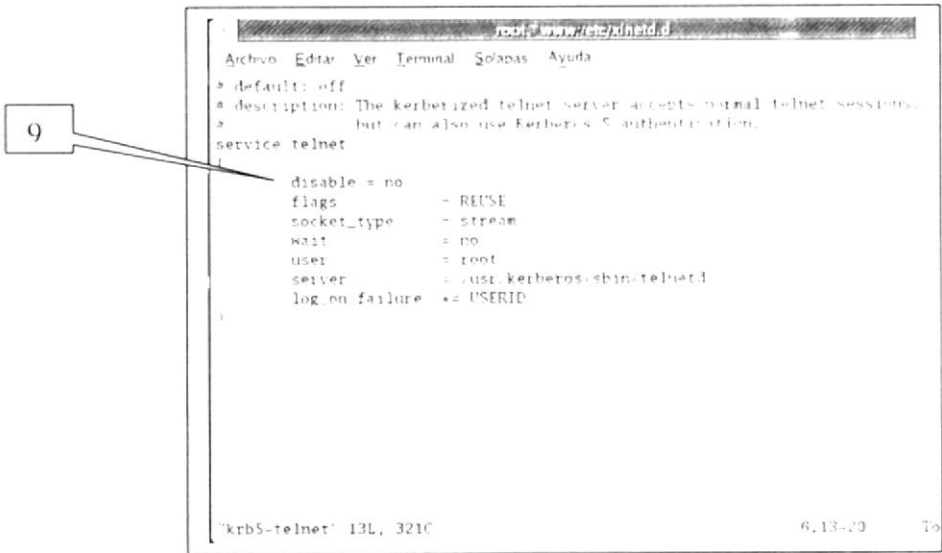
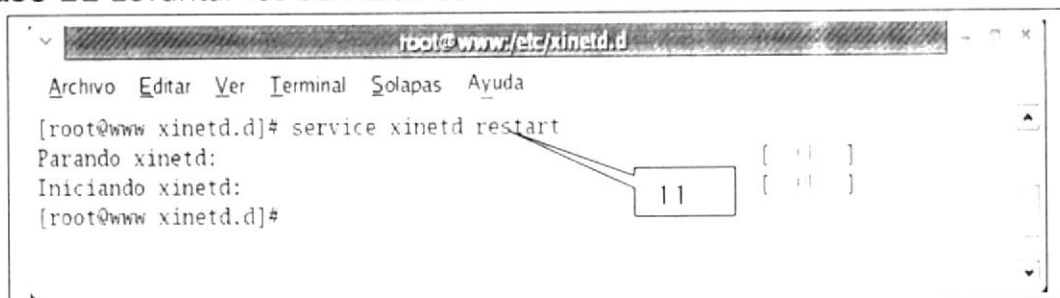


Figura 6-205: configuración de telnet

Paso 10 Grabar los cambios con **shift :wq**



Paso 11 Levantar los servicios con **service xinetd restart**

```
root@www/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
[root@www xinetd.d]# service xinetd restart
Parando xinetd:
Iniciando xinetd:
[root@www xinetd.d]#
```

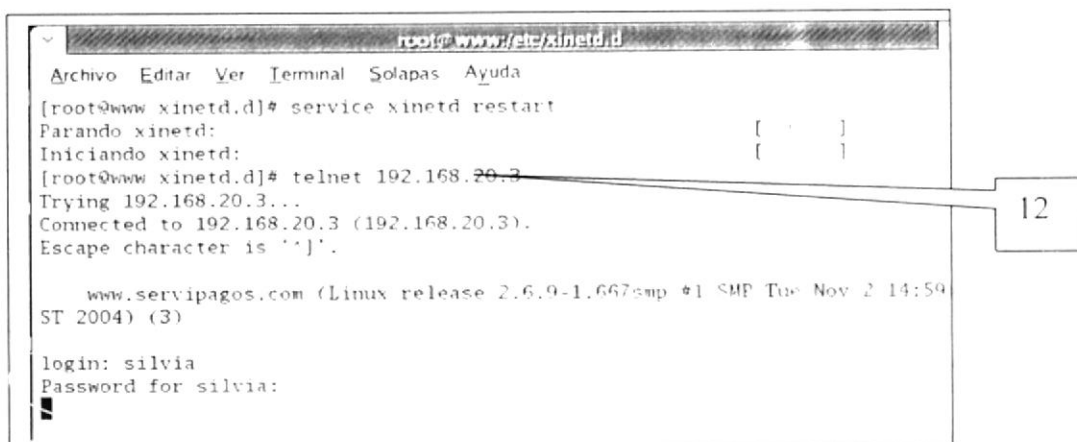
Figura 6-206: servicio restaurado

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

Paso 12 Realizar la siguiente prueba tratando de hacer telnet al servidor Linux Ej:

telnet 192.168.20.3 (la ip address del servidor)

Nota: Crear un usuario utilizando la **clave de root**, **no** se recomienda ingresar con **root**.



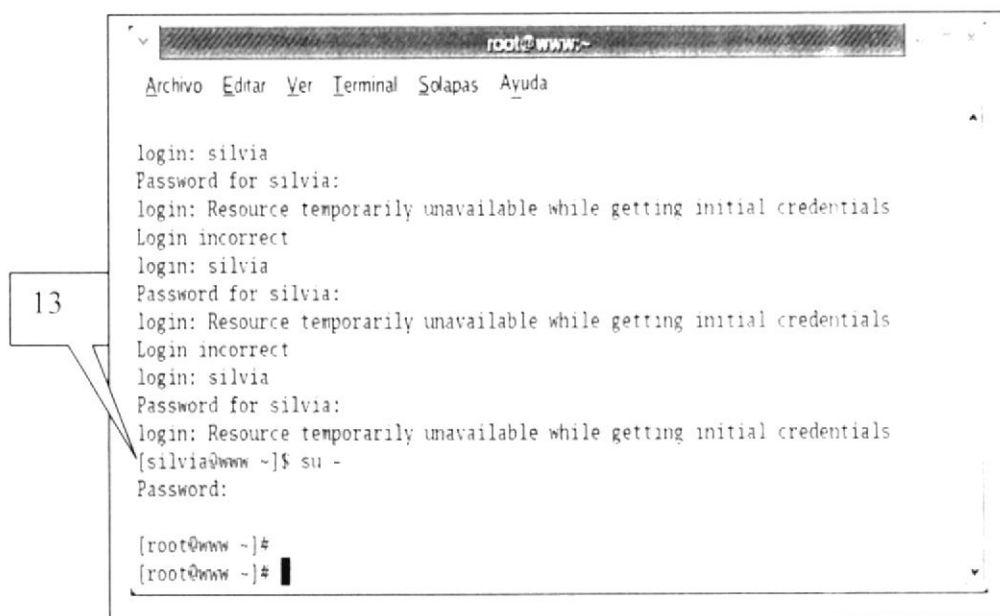
```
root@www/etc/xinetd.d
Archivo Editar Ver Terminal Solapas Ayuda
[root@www xinetd.d]# service xinetd restart
Parando xinetd:
Iniciando xinetd:
[root@www xinetd.d]# telnet 192.168.20.3
Trying 192.168.20.3...
Connected to 192.168.20.3 (192.168.20.3).
Escape character is '''.

www.servipagos.com (Linux release 2.6.9-1.667smp #1 SMP Tue Nov 2 14:59
ST 2004) (3)

login: silvia
Password for silvia:
```

Figura 6-207: conexión vía telnet

Paso 13 Para que no pida ingreso de un user y poder tener las utilidades de root ingresar de la siguiente manera, Ingresar el comando **su -**, y presionar la tecla **intro**, ingresar directo solo pide el **passwd** ingresar contraseña del root



```

root@www:~
Archivo Editar Ver Terminal Solapas Ayuda

login: silvia
Password for silvia:
login: Resource temporarily unavailable while getting initial credentials
Login incorrect
login: silvia
Password for silvia:
login: Resource temporarily unavailable while getting initial credentials
Login incorrect
login: silvia
Password for silvia:
login: Resource temporarily unavailable while getting initial credentials
[silvia@www ~]$ su -
Password:

[root@www ~]#
[root@www ~]#
  
```

Figura 6-208: ingreso al servidor por telnet

Paso 14 Para Bloquear telnet utilizar la siguiente regla

Iptables -A INPUT -s 192.168.20.5 -d 192.168.20.3 -p tcp -dport 23 -j DROP

Explicación de la Regla

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.5)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:

TCP, especifica el puerto que debe utilizar el origen del datagrama para concordar con esta regla.

--dport: Igual que la opción anterior pero para el puerto destino.

23 Puerto de Telnet

–DROP: Elimina una regla de una chain (se puede indicar el orden o su condición).

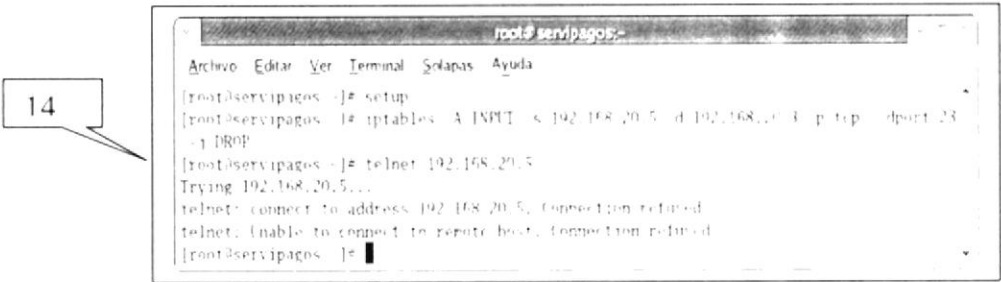


Figura 6-209: bloqueo de telnet

Paso 15 Verificación de conectividad por medio del ping desde el servidor Linux 192.168.20.3 hacia estación de trabajo Windows 192.168.20.5

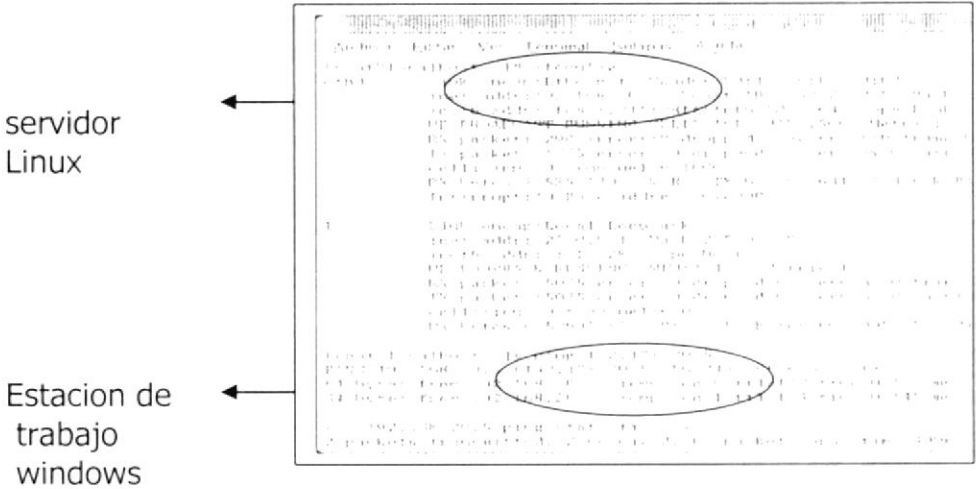


Figura 6-210: prueba de ping

Paso 16 Luego de verificación del ping crear una regla para bloquear a otra dirección ip de Windows que no sea la dirección 192.168.20.5

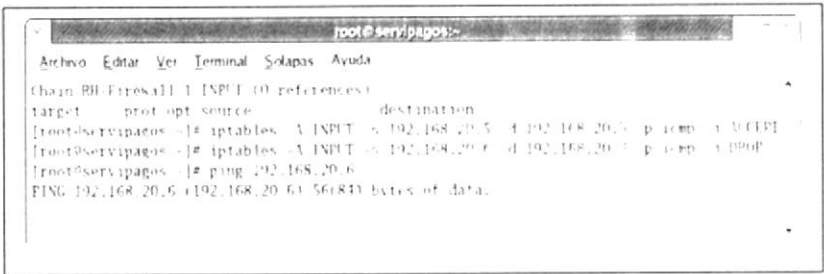


Figura 6-211: bloqueo de ping

- a) Iptables -A INPUT -s 192.168.20.5 -d 192.168.20.3 -p icmp -j ACCEPT
- b) Iptables -A INPUT -s 192.168.20.6 -d 192.168.20.3 -p icmp -j DROP

Explicación de la Regla

La regla a acepta a la dirección 192.168.20.5 , mientras que la regla b deniega a la dirección 192.168.20.6

iptables -A: Inserta al final de una cadena una nueva regla.

-s: Indica un dominio o IP (rango de IPs) de origen sobre el que se evalúa la condición de la regla. (192.168.20.0)

-d: Indica un dominio o IP (rango de IPs) de destino el que se evalúa la condición de la regla.(192.168.20.3)

-p: Especifica el protocolo del datagrama que concordará con esta regla. Los nombres válidos de protocolos son tcp, udp, icmp, o un número, si se conoce el número del protocolo de IP. Cada protocolo lleva asociados sus propios modificadores a través de las extensiones correspondientes:



Extensiones ICMP:

icmp-type: Puede especificarse el tipo de mensaje ICMP tanto por su número como por los siguientes identificadores: echo-request, echoreply, source-quench, time-exceeded, destination-unreachable, network-unreachable, host-unreachable, protocol-unreachable, y port-unreachable.

–**DROP**: Elimina una regla de una chain (se puede indicar el orden o su condición).

–**ACCEPT**: Acepta una regla de una chain (se puede indicar el orden o su condición).

6.36.8. CONFIGURACIÓN EN EL CLIENTE WINDOWS

Paso 14 Ir a inicio y buscar ejecutar escribir telnet y la ip del servidor en este caso 192.168.20.3

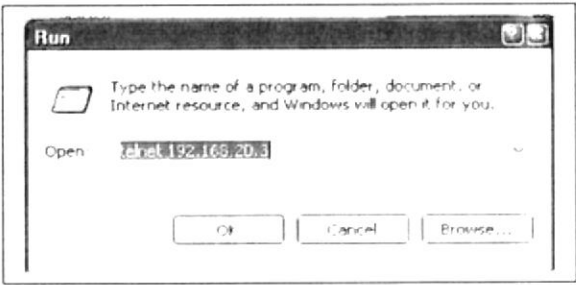


Figura 6-212: ejecutar con ip del servidor

Paso 15 Ingresar de modo consola pide el login que es un usuario que se crea en Linux en este ejemplo se ingresa con silvia

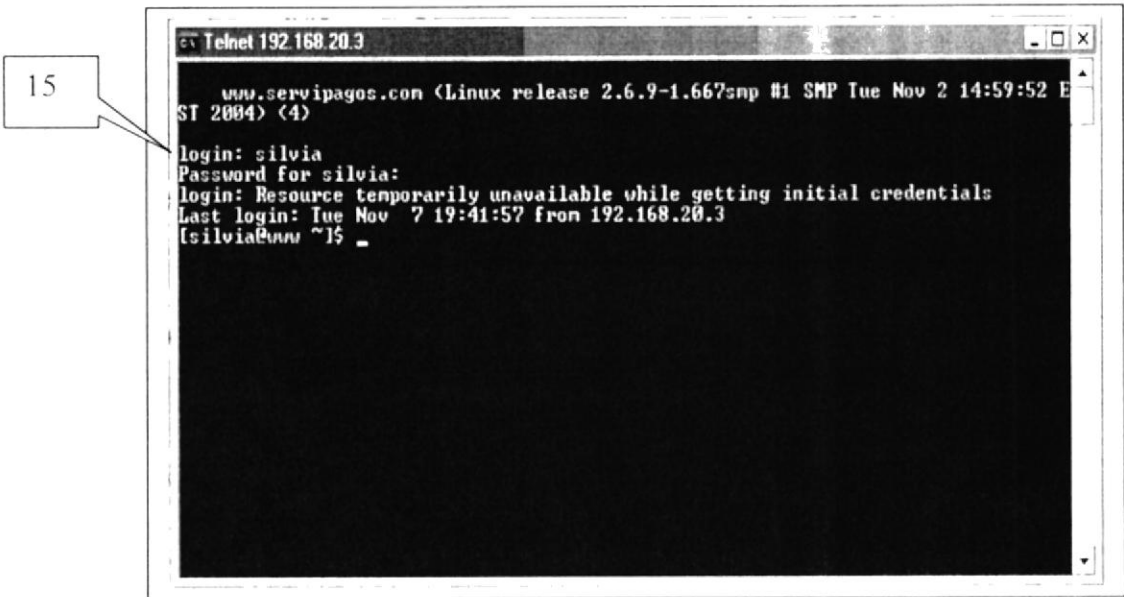


Figura 6-213: ingreso al servidor de linux en windows

Paso 16 Escribir el comando su- para ingresar como administrador.

Paso 17 Una vez ingresado como administrador se puede hacer uso de sus recursos un ejemplo es escribir **iptables -L** muestra todos las reglas que se han aplicado en firewall



Figura 6-214: vista de reglas creadas en Linux

Paso 18 Luego de comprobar que si hay conectividad remota, se procederá a bloquear telnet para la ip 192.168.20.5

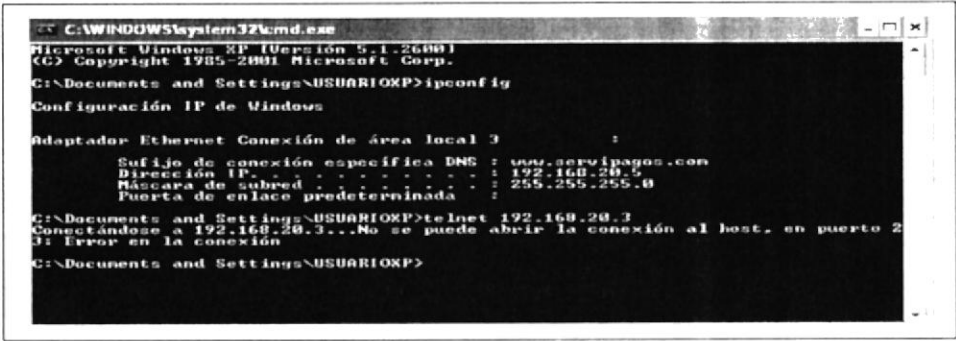


Figura 6-215: Bloqueo de Telnet en Windows

Paso 19 Comprobar conectividad entre el servidor y estación de trabajo de Windows con la dirección ip permitida en este caso es 192.168.20.5

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\USUARIOXP>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local 3 :
    Sufijo de conexión específica DNS : www.servipagos.com
    Dirección IP. . . . . : 192.168.20.5
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada :

C:\Documents and Settings\USUARIOXP>ping 192.168.20.3

Haciendo ping a 192.168.20.3 con 32 bytes de datos:
Respuesta desde 192.168.20.3: bytes=32 tiempo<in TTL=64
Respuesta desde 192.168.20.3: bytes=32 tiempo<in TTL=64
Respuesta desde 192.168.20.3: bytes=32 tiempo<in TTL=64
Respuesta desde 192.168.20.3: bytes=32 tiempo<in TTL=64

Estadísticas de ping para 192.168.20.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\USUARIOXP>
```

Figura 6-216: ping desde dirección permitida

Paso 20 Comprobación de bloqueo de una dirección no permitida (192.168.20.6) hacia el servidor de Linux

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\USUARIOXP>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local 3 :
    Sufijo de conexión específica DNS : www.servipagos.com
    Dirección IP. . . . . : 192.168.20.6
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada :

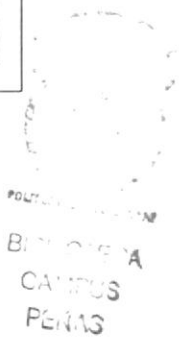
C:\Documents and Settings\USUARIOXP>ping 192.168.20.3

Haciendo ping a 192.168.20.3 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.20.3:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Documents and Settings\USUARIOXP>
```

Figura 6-217: bloqueo de ping



6.37 SERVIDOR DHCP (Dynamic Host Configuration Protocol)

6.37.1. QUE REALIZA DHCP :

- a) entregar IPs a clientes de red
- b) compatibilizar con BOOTP para booteo de máquinas Diskless

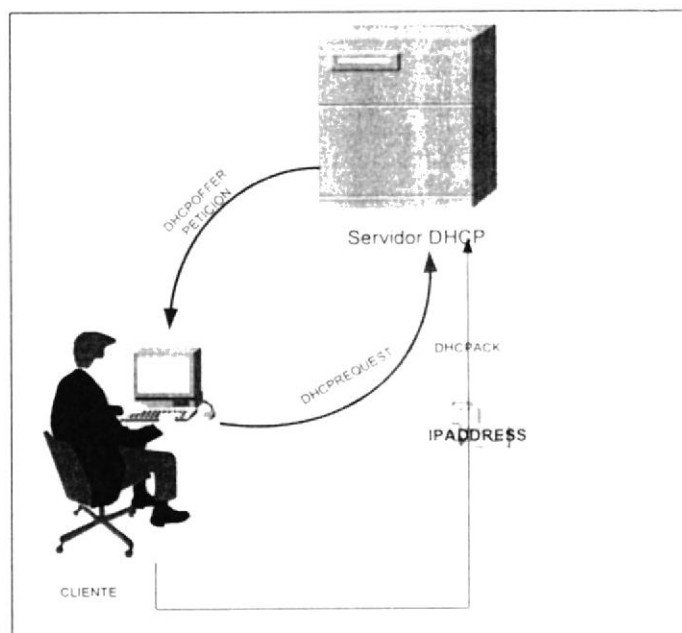


Figura 6-218: Esquema de DHCP

6.37.2. COMPONENTES PRINCIPALES DE DHCP

- 1) llamado "protocolo" que sirve para entrega de configuraciones específicas "per-host" desde un servidor DHCP
- 2) llamado "mecanismo" que sirve para la localización de direcciones de red a hosts.

Por sobre todo, DHCP es un modelo de cliente-servidor.

En toda LAN usando TCP-IP, todas las máquinas deben tener un número IP. Esto se puede lograr de tres maneras:

- a) configurando cada cliente por separado, evitando choques de IP (configuración "per- host")
- b) asignando un IP por cliente, de manera dinámica o estática (DHCP) . Cada cliente por separado en a) tendrá un número IP asignado por el administrador de red. En b) cada número IP estará asignado dentro de un "pozo" de números IP dispuestos por el servidor DHCP.

6.37.3. COMO FUNCIONA DHCP

Explicación detallada de que es lo que ocurre:

Etapas de descubrimiento:

Cuando un host no posee un número IP determinado (o sea, necesita un IP de un servidor DHCP), manda un mensaje llamado.

DHCPDISCOVER. Este mensaje es enviado dentro de la capa física de la red. Este mensaje incluye además algunos parámetros adicionales, como IPs sugeridos o tiempo de duración del número IP anterior que tuvo (si lo hubiera).

Etapas de Ofrecimiento:

El mensaje llega a un servidor DHCP (los clientes que no posean el servicio DHCP ignoran este mensaje). El servidor responde de la misma manera física, pero con un mensaje llamado DHCPOFFER. Este mensaje es enviado a toda la red (broadcast a 255.255.255.255) o únicamente al cliente. El cliente sabe como responder, ya que uno de los parámetros del mensaje

DHCPDISCOVER es la MACAddress (Dirección física de la tarjeta de red).

Etapas de Ofrecimiento:

El cliente recibe UNA O MÁS peticiones DHCPOFFER de uno o más servidores. El cliente entonces elige (por tiempo de respuesta, por IP, etc... es bastante oscuro el proceso de elección). Al elegir, el cliente envía un mensaje DHCPREQUEST al servidor que ha elegido para su IP (server identifier), junto con otras opciones. Si el cliente no recibe mensajes DHCPOFFER, expira la petición y reenvía un nuevo mensaje DHCPDISCOVER.

Etapas de Encuentro:

El servidor recibe el broadcast con el mensaje DHCPREQUEST del cliente. El servidor responde con un mensaje DHCPACK que contiene los parámetros para el cliente (el numero IP). Aquí viene la etapa de "leasing" de IP. Si el servidor no puede satisfacer el mensaje DHCPREQUEST, el servidor igualmente debe responder con un DHCPACK. El servidor marca los números IPs no disponibles.

Etapas de Préstamo:

El cliente recibe el mensaje DHCPACK y revisa si la configuración esta OK. Si el cliente detecta un error, arroja un mensaje DHCPDECLINE y reinicia el proceso. Si en vez de recibir un DHCPACK, el cliente recibe un mensaje DHCPNAK, el cliente reinicia el proceso. Cuando esto ocurre (DHCPDECLINE y DHCPNAK), el cliente expira la petición y la reinicia.

Etapas de Devolución:

El cliente envía un mensaje DHCPRELEASE al servidor cuando libera su IP.

Si el proceso falla a las 10 veces, NO HAY IP. Simple. (En cliente Windows el número IP que entrega es siempre 169.254... Si aparece eso, fallo DHCP en algún lado) Esto es el proceso simple y básico. Hay distintos tipos de interacciones entre C/S, sobre todo cuando un cliente YA dispone de un número IP (antiguo léase). En este caso, la negociación solo ocurre con un DHCPREQUEST, DHCPACK/DHCPNAK y DHCPRELEASE

6.37.4. VENTAJAS DE DHCP

Las ventajas del uso de DHCP son:

- a) solo se configura un servidor para entregar números IP para clientes de red
- b) se entregan todos los parámetros básicos de TCP-IP
- c) facilidad de configuración (sabia frase "prende y funciona")

6.37.5. DESVENTAJAS DE DHCP

a) 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.

b) los mensajes tienden a fallar sobre todo si las tarjetas de red hacen la negociación de velocidad (más conocido como Network Speed Auto-Sense, que falla con una rapidez increíble) ya que la red se llena de "basura física".

- En la línea subnet se asigna el segmento de red con su respectiva máscara.

Subnet 192.168.11.0 netmask 255.255.255.0

Subnet <network> netmask <mask>; indica la subred y la máscara para los clientes

- Opcional colocar la línea del gateway

Option routers 192.168.11.8

option routers; indica los routers de la red

6.37.6. CONFIGURACIÓN DEL SERVIDOR DHCP

Paso 1 Para realizar esta configuración se necesita contar con el paquete **dhcpd**, verificando su instalación de la siguiente manera:

rpm: Verifica paquetes instalados -q **nombre_paquete:dhcp**

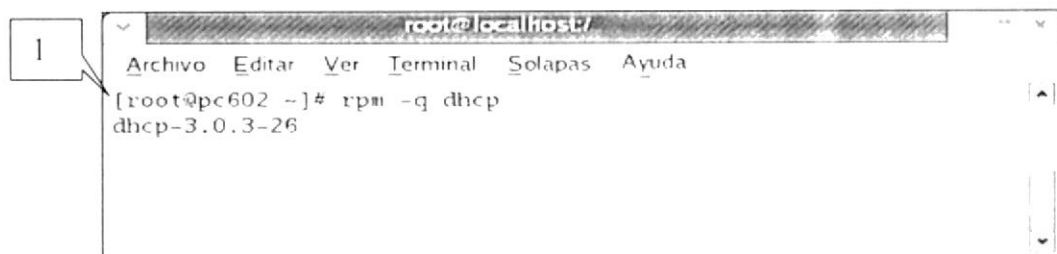


Figura 6-219: verificación de paquete dhcp

Paso 2 A continuación crear el archivo **dhcpd.conf** con las mismas características del dhcp, lo cual será realizado de la siguiente manera:

cp /usr/share/doc/dhcp-3.0.1/dhcpd.conf.sample /etc/dhcpd.conf

cp [ruta del archivo a copiar] [directorio en donde se desea copiar]

/usr/share/doc Documentación independientes de la arquitectura.

dhcp -3.0.1 :versión de paquete dhcp

/dhcpd.conf.sample: archivo de configuración para paquete dhcpd

/etc Archivos de configuración.

Dhcpd.conf : Configuración de paquete

Figura 6-220: creación de archivo dhcp

Paso 3 Configurar el archivo `dhcpd.conf` el cual ha sido creado en la ruta `/etc/dhcpd.conf`:

vi /etc/dhcpd.conf

vi Utilidad que sirve para modificar ficheros de texto plano:

/etc Archivos de configuración.

Dhcpd.conf : Configuración de paquete

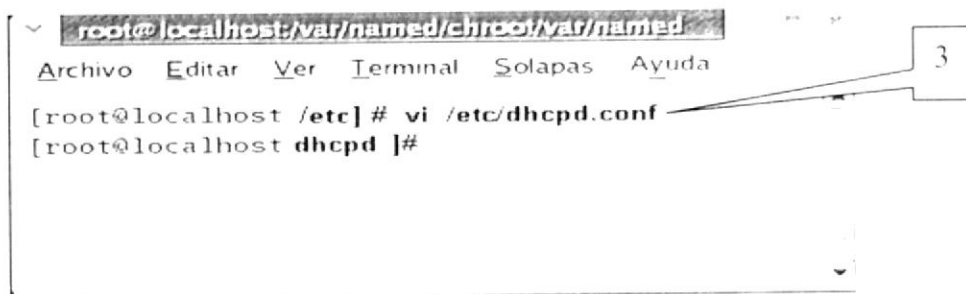


Figura 6-221: editamos el dhcp

Paso 4 Editar el archivo de la siguiente manera: (ver recuadros rojos)

Explicación de los campos que se encuentra en la pantalla

Option subset-mask 255.255.255.0

option subnet-mask <mask>; indica la máscara de red

- Digitar la dirección del DNS

Option domain-name-servers 200.10.148.5

option "<dominio>"; indica el dominio por defecto

option domain-name-servers ; indica los servidores DNS

Paso 5 –Definir el rango de direcciones ip a utilizar Ej:

Range dynamic-bootp 192.168.20.2 192.168.20.50
indica el rango de IPs a entregar

```

root@localhost:
Archivo Editar Ver Terminal Solapas Ayuda
ddns-update-style interim;
ignore client-updates;
subnet 192.168.20.0 netmask 255.255.255.0 {
    *
    default gateway
        option routers                192.168.0.1;
        option subnet-mask           255.255.255.0;

    option nis-domain                 "domain.org";
    option domain-name                "domain.org";
    option domain-name-servers       192.168.1.1;

    option time-offset                -18000; # Eastern Standard Time
    *
    option ntp-servers                192.168.1.1;
    *
    option netbios-name-servers       192.168.1.1;
    *
    Selects point to point mode (default is hybrid). Don't change this unless
    you understand Netbios very well
    *
    option netbios-node-type 2;

    range dynamic-bootp 192.168.20.2 192.168.20.50;
    default-lease-time 21600;
    max-lease-time 43200;

    # we want the nameserver to appear at a fixed address
    host ns {
        next-server marvin.redhat.com;
        hardware ethernet 12:34:56:78:AB:CD;
    }
}
"/etc/dhcpd.conf" 31L, 852C
1.1 Comienzo

```

Figura 6-222: configuración de dhcp

Paso 6 Guardar los cambios realizados con las teclas **Esc** y **:wq**.

":wq" e **INTRO** para guardar los cambios y cerrar el fichero.

Paso 7 Restaurar el servicio del dhcpd: **service dhcpd restart**

service nombre_servicio restart Reinicia el servicio especificado "nombre_servicio"

```

root@localhost:
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost named]# service dhcpd restart
Parando dhcpd: [ 66% ]
Iniciando dhcpd: [ 66% ]

```

Figura 6-223: restaurar dhcp

6.37.7. CONFIGURACIÓN EN EL CLIENTE WINDOWS

En el lado del cliente realizar las siguientes configuraciones:

Paso 8 Ingresar en Mis Sitios de Red, dar un clic derecho

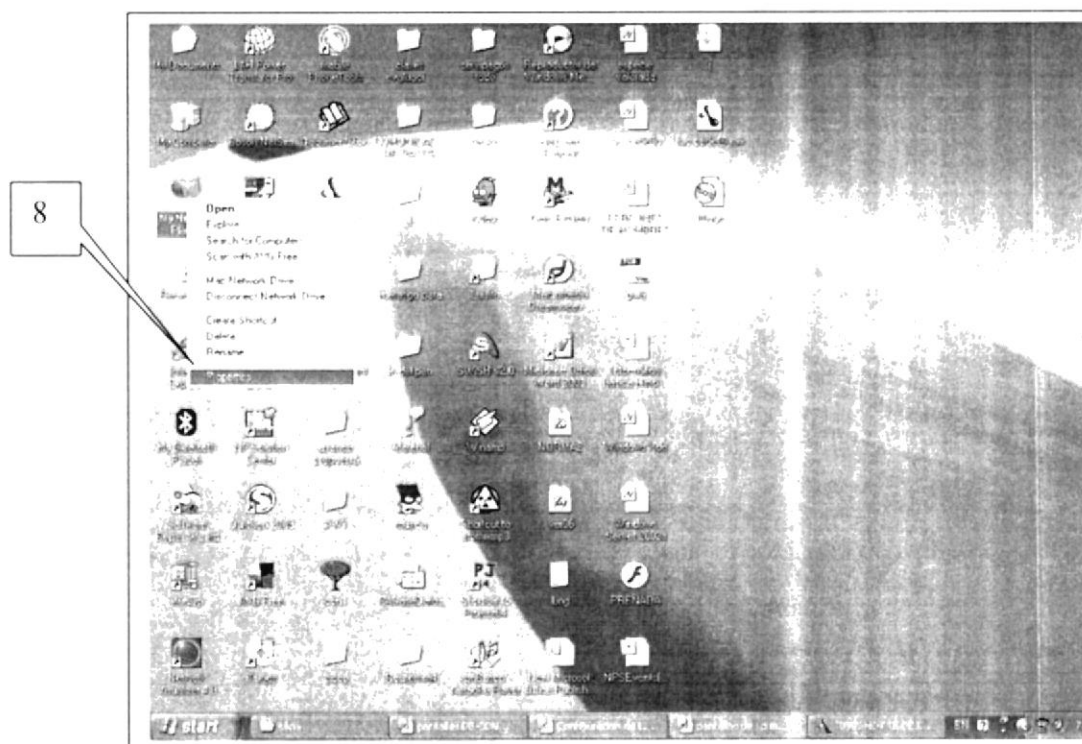


Figura 6-224: propiedades a conexión

Paso 9 Ingresar a la red de área local dar clic derecho

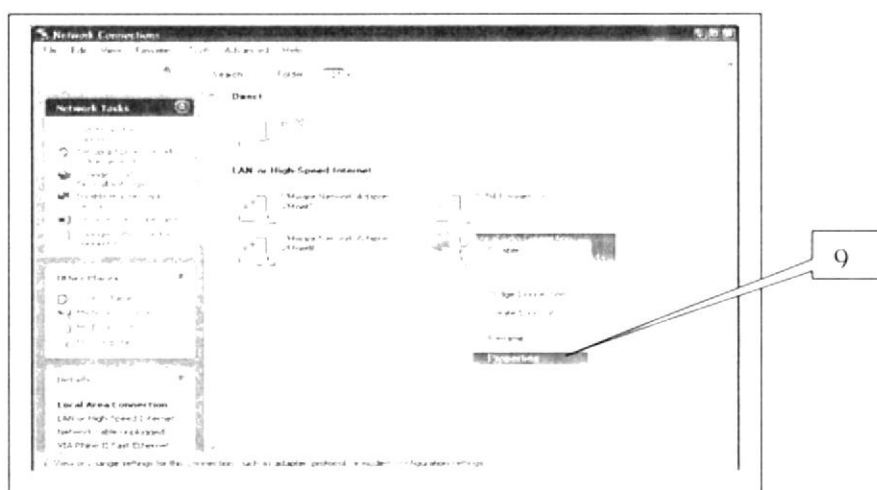
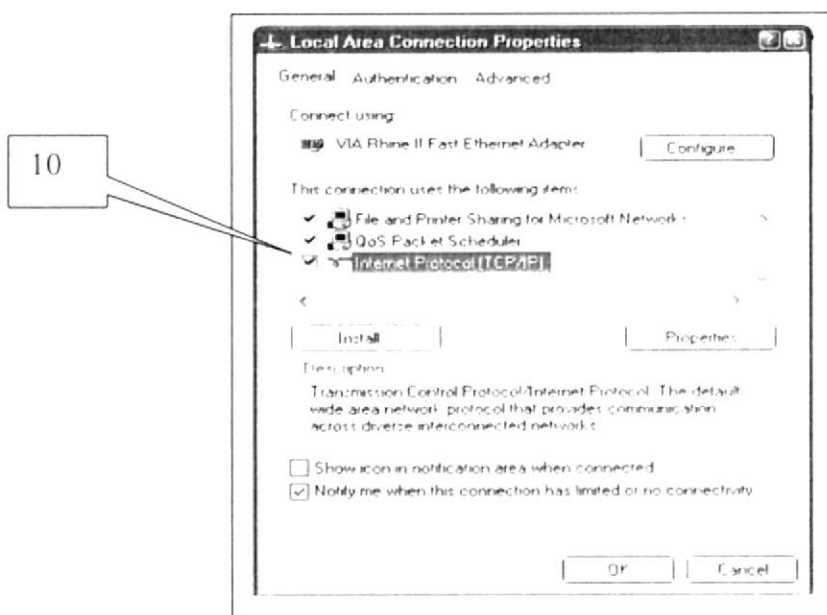
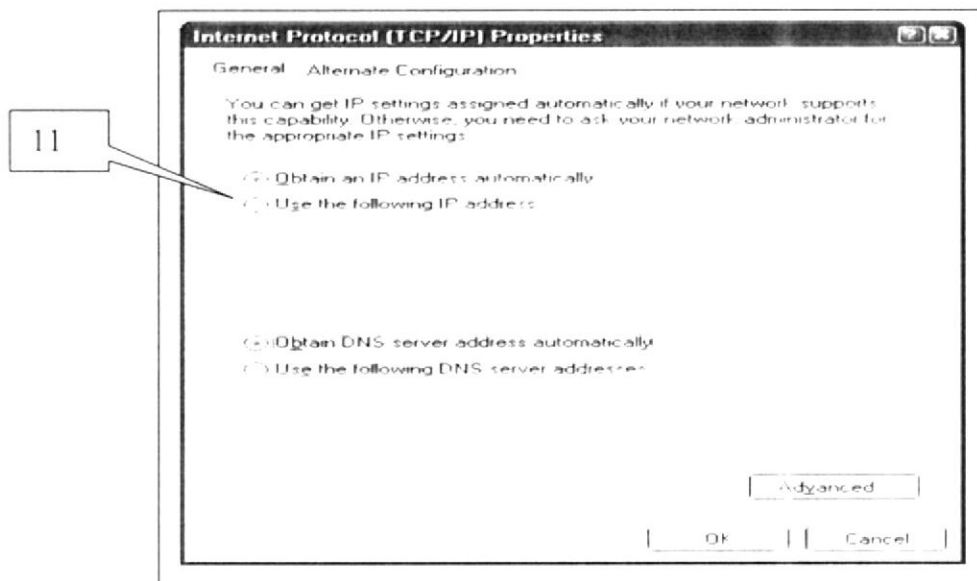


Figura 6-225: propiedades de área local

Paso 10 Ingresar en las **Propiedades** de INTERNET PROTOCOL TCP/IP**Figura 6-226: propiedades de tcp/ip**

Paso 11 Configurar la tarjeta de red de manera dinámica, en este caso se pondrá la opción obtener una dirección IP automáticamente y obtener la dirección del servidor DNS automáticamente como se lo detalla a continuación

**Figura 6-227: detección automática**

Paso 12 Ingresar a inicio (Start) elegir ejecutar (run) ingresar con cmd para ingresar al modo consola

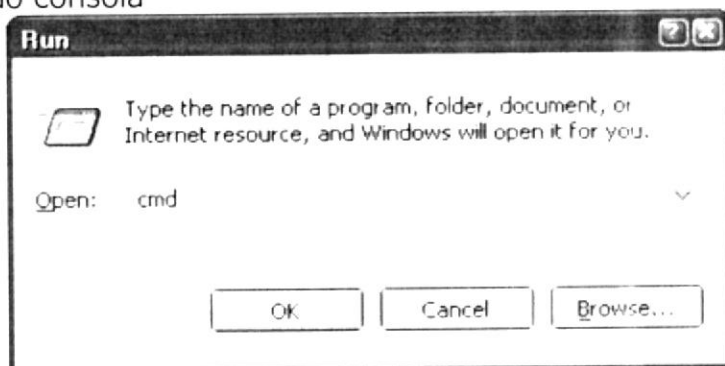


Figura 6-228: ingreso de consola

Paso 13 Realizar la verificación del servicio dhcp con el comando ipconfig que muestra la ip que tiene la máquina, **a)** realizar la prueba del ping para verificar que esa dirección ip dada por el servidor dhcp tiene conectividad con el servidor de Linux.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\USUARIOXP>ping 192.168.20.3
Haciendo ping a 192.168.20.3 con 32 bytes de datos:
Respuesta desde 192.168.20.3: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.3: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.3: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.20.3: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 192.168.20.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\Documents and Settings\USUARIOXP>ipconfig
Configuración IP de Windows

Adaptador Ethernet Conexión de área local 3 :
    Sufijo de conexión específica DNS : domain.org
    Dirección IP. . . . . : 192.168.20.20
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada : 192.168.0.1
C:\Documents and Settings\USUARIOXP>
```

Figura 6-229: verificación dhcp

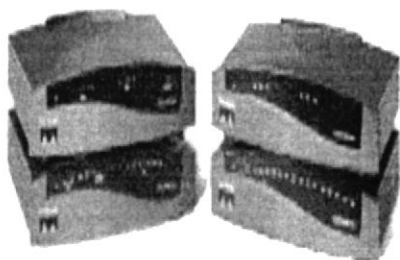


CAPÍTULO 7

CONFIGURACIÓN DE ROUTERS Y SWITCHES

7. CONFIGURACIÓN DE ROUTERS Y SWITCH

7.1 INTRODUCCIÓN



Un router trabaja mediante protocolos enrutamientos específicamente para nivel wan, a su vez es un dispositivo de hardware para interconexión de redes de las computadoras que opera en la **capa tres** (nivel de red) del modelo OSI.

El router se interconecta con diferentes segmentos de red, o algunas veces hasta redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones basadas en diversos parámetros con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice

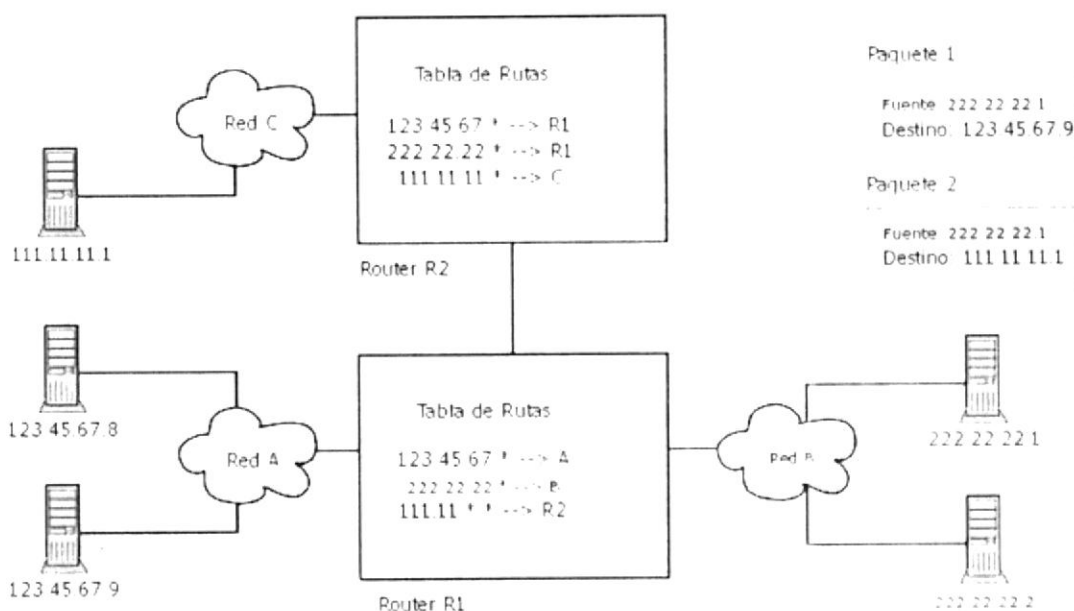


Figura 7-1: Conexiones varios segmentos de red

7.2 INTERFAZ DTE-DCE

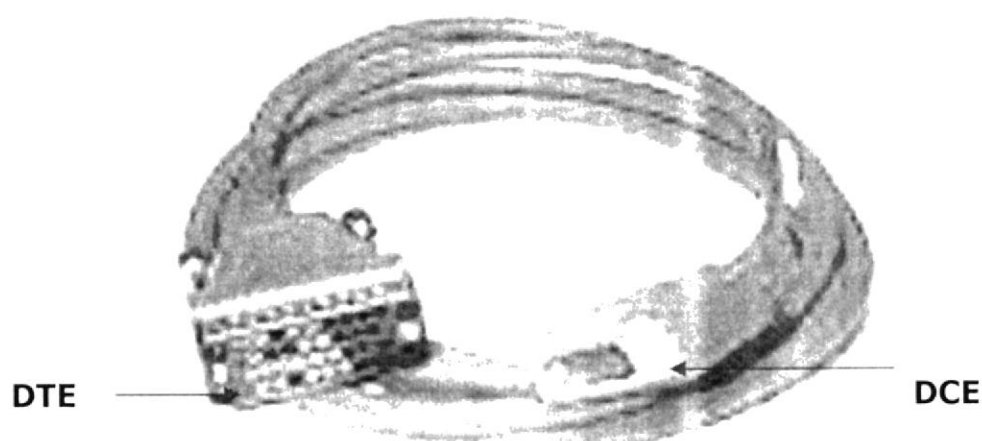


Figura 7-2: DCE - DTE

Para analizar las características del nivel físico del modelo OSI es indispensable considerar las características del canal de salida de datos del puerto de salida del equipo emisor de datos conocido normalmente como Equipo Terminal de Datos (DTE) y las del canal de entrada de datos del puerto de entrada de datos del equipo receptor de datos denominado normalmente Equipo de Terminación del Circuito de Datos (DCE). Este equipo puede incluso constituir el equipo de comunicación de datos o una parte de él.



7.3 COMPONENTES INTERNOS DEL ROUTER

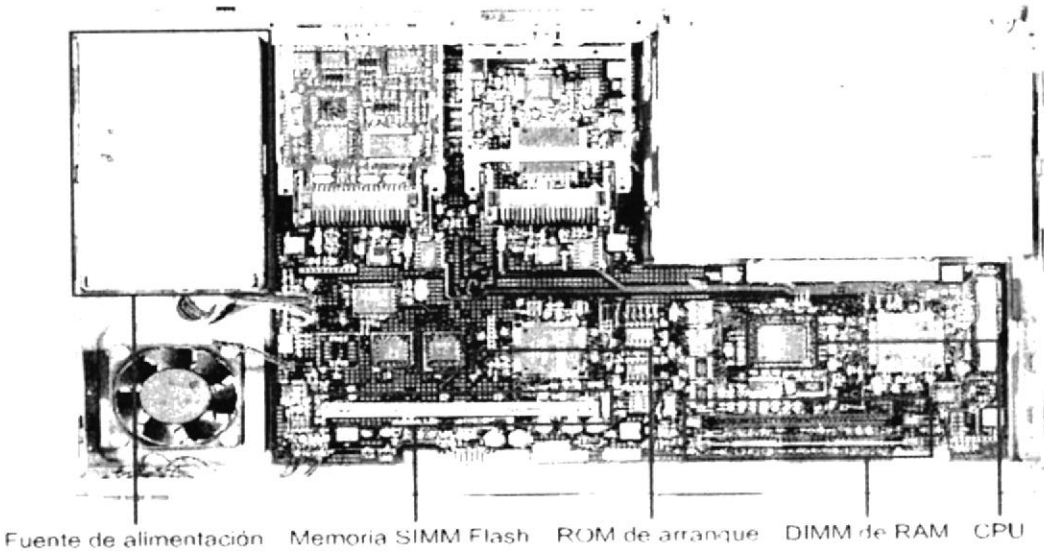


Figura 7-3: Componentes del router

El router internamente esta compuesto por partes que son:

- ↓ RAM
- ↓ NVRAM
- ↓ FLASH
- ↓ ROM
- ↓ CONSOLA
- ↓ INTERFAZ



Memoria	Propósito
ROM	Guarda el ROM monitor, y la boot ROM
Memoria Flash	Guarda la Imagen del Sistema (Cisco IOS)
NVRAM	Guarda el archivo de configuración (startup-config)
RAM	Guarda la configuración en operación (running-config), tablas de ruteo, caches, queues, packets, etc.

7.3.1. RAM

La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más Módulos de memoria en línea doble (DIMM).

7.3.2. NVRAM

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

7.3.3. FLASH

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

7.3.4. ROM

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

7.3.5. CONSOLA

El puerto de consola proporciona es el acceso físico para la configuración inicial.

7.3.6. INTERFAZ

Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring. Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser configuraciones fijas o modulares. Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de configuraciones fijas o modulares. Los puertos de Consola/AUX son puertos seriales que se utilizan principalmente para la configuración inicial del router. Estos puertos no son puertos de networking. Se usan para realizar sesiones terminales desde los puertos de comunicación del computador o a través de un módem.



7.4 CONEXIONES EXTERNAS DEL ROUTER

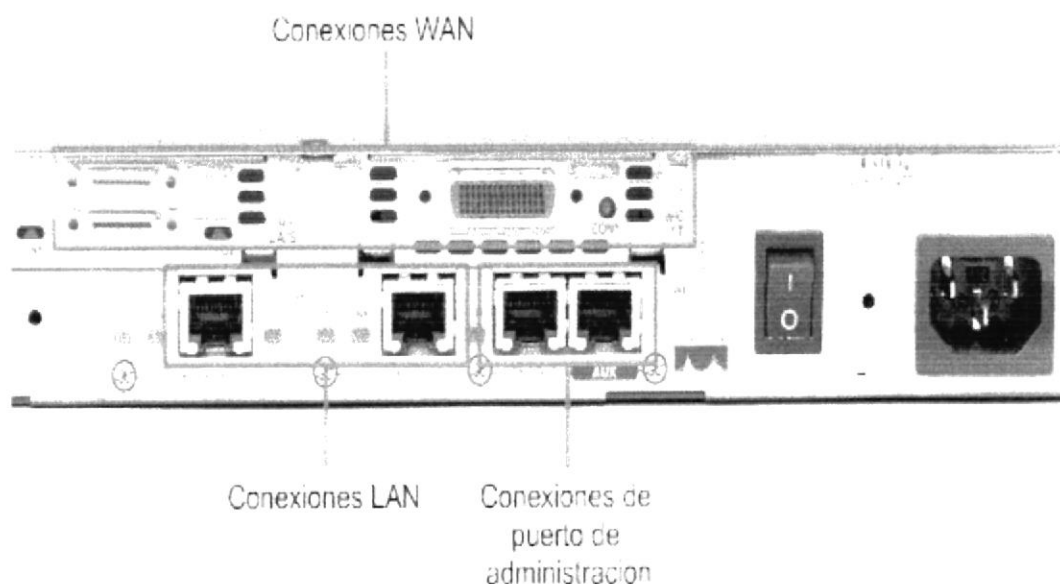


Figura 7-4: Conexiones Externas del Router

El router externamente esta compuesto por:

- + CONEXIÓN WAN
- + CONEXIÓN LAN
- + CONEXIONES DE PUERTOS ADMINISTRATIVOS

7.4.1. CONEXIÓN LAN

Esta conexión permite conectarse a una red cercana, es decir, a una red **LAN** mediante conexión ethernet.

7.4.2. CONEXIÓN WAN

Esta conexión permite estar comunicado a grandes distancia como proveedor de Internet (ISP); sucursales lejanos, es decir, mediante conexiones seriales

7.4.3. CONEXIONES DE PUERTOS ADMINISTRATIVOS

Esta conexión permite controlar todos los movimientos que se efectúa en un ruteador e incluso en esta conexión se lo utiliza para configurar los dispositivos mediante el conector de la consola.

7.5 VENTAS Y DESVENTAJAS DE UN ROUTERS

VENTAJA	DESVENTAJAS
❖ Segmentación eficiente de tráfico y broadcats . ❖ Manejo de protocolos de nivel 3. ❖ Interconexión de redes heterogéneas ❖ Dependiendo del protocolo de ruteo pueden manejar múltiples caminos para un mismo destino y balancear cargas de enlaces. ❖ Proveen escalabilidad para redes muy grandes.	❖ Complejos de operar. ❖ Utilizan protocolos complejos de implementar para los fabricantes de equipos. ❖ Lentos ❖ Caros

Tabla 7-1: Ventajas y desventajas del Router

7.6 FUNCIONES DE UN ROUTER

Las funciones primarias de un ruteador son:

- ❖ Segmentar la red dentro de dominios individuales de broadcast.
- ❖ Suministrar un envío inteligente de paquetes. Y Soportar rutas redundantes en la red.
- ❖ Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los broadcast no pasarán a través del ruteador.

7.7 BENEFICIOS DE UN ROUTER

Otros importantes beneficios del ruteador son:

- ❖ Proporcionar seguridad a través de filtros de paquetes, en ambiente LAN y WAN.
- ❖ Consolidar el legado de las redes de mainframe IBM, con redes basadas en PCs a través del uso de Data Link Switching (DLSw).
- ❖ Permitir diseñar redes jerárquicas, que delegan autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- ❖ Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, FastEthernet, Token Ring, FDDI y ATM.



7.8 TECNOLOGÍA DE RUTEADOR

Un ruteador es un dispositivo general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN.

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes. El ruteador realiza dos funciones básicas:

1. El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta área el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.
2. La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesamiento de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.



7.9 HYPERTERMINAL

La conexión **HYPERTERMINAL** se trata de la conexión del router al computador.

Mediante sus conexiones:

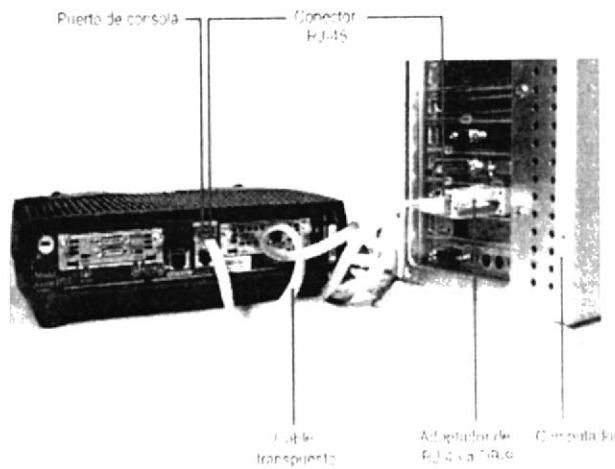


Figura 7-5: Conexiones Hyperterminal

Conexión RJ-45 del punto de router desde la consola

Conexión DB-9 del punto de la computadora desde com 1 o com 2 depende del modelo; en este caso se utiliza com 1



Figura 7-6: Cable rollover

7.10 CONFIGURACIÓN DEL HYPERTERMINAL

Paso uno

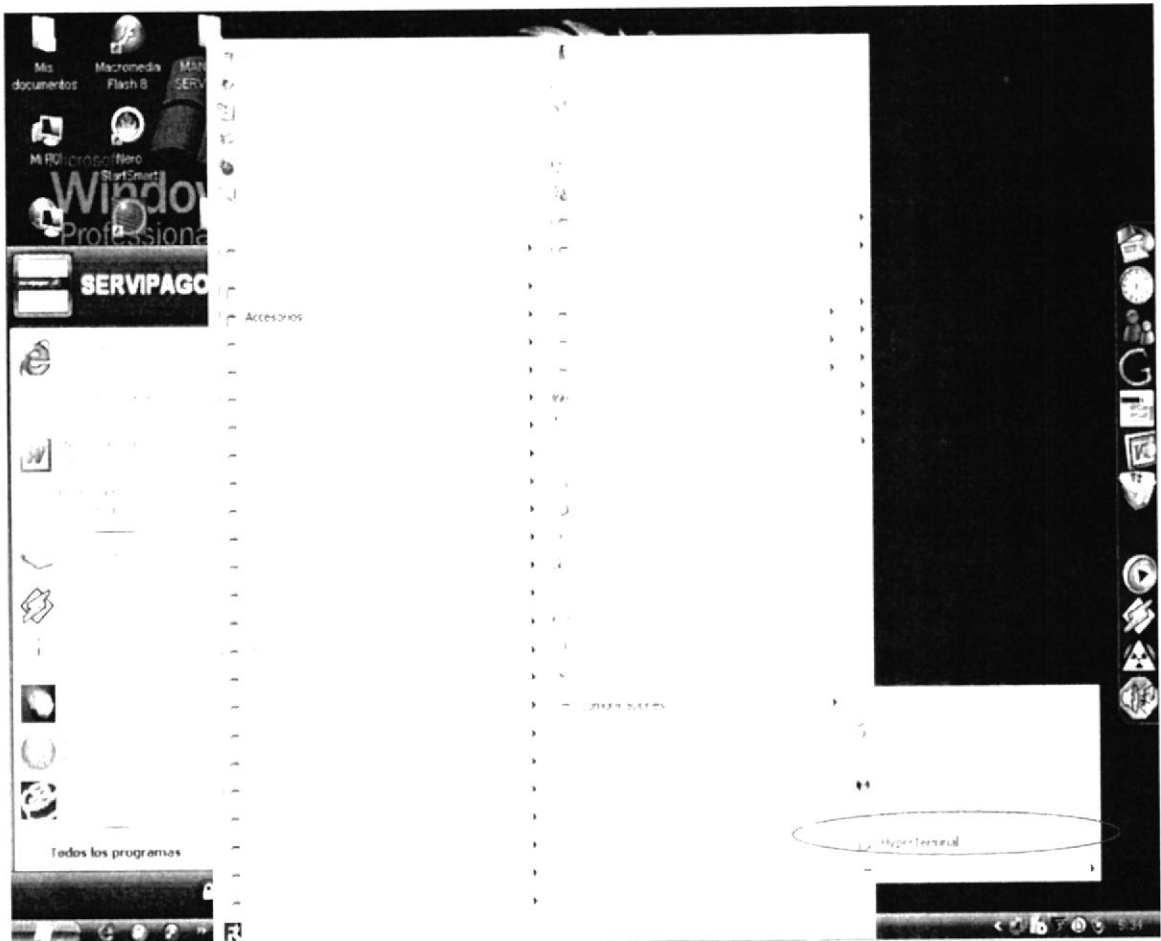


Figura 7-7: Inicio Hyperterminal

Abrir el Hyperterminal de la siguiente manera:

- ↓ Hacer clic en inicio
- ↓ Escoger la opción accesorios
- ↓ Luego hacer click en comunicación
- ↓ Por último dar click en Hyperterminal



Paso 2

Al abrir el hyperterminal, se darán las opciones de crear una nueva conexión, se le pone un nombre que identifique la BBS, por ejemplo 'SERVIPAGOS' y se elige el icono que se guste.



Figura 7-8: Nombre a la Conexión

Paso 3

En esta pantalla se elige el puerto para conectar el router con el cable rollover, cabe indicar que puede conectarse mediante el com1, com2, com3 dependiendo el tipo de conexión que tenga la PC.

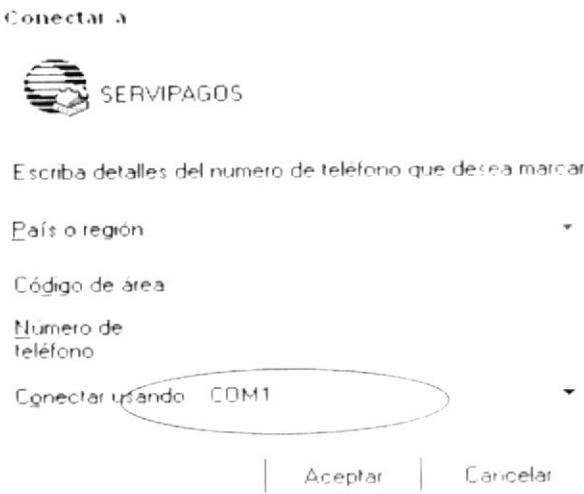


Figura 7-9: Puerto de conexión

Paso 4

A continuación se debe configurar los bits.

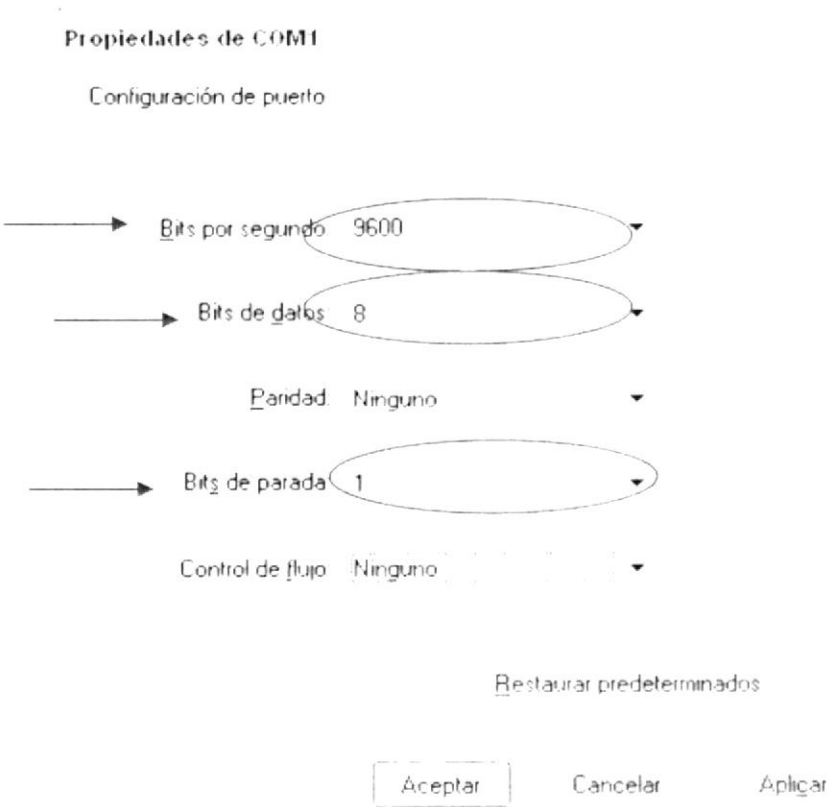


Figura 7-10: Configuración de los bits

NOTA: Los bits son parámetros por defecto del puerto de consola



Paso 5

Una vez configurado el HYPERTERMINAL aparecerá una ventana donde allí se puede configurar y monitorial los router; en el siguiente gráfico se dará una idea de cómo sería la pantalla de inicio del HYPERTERMINAL.

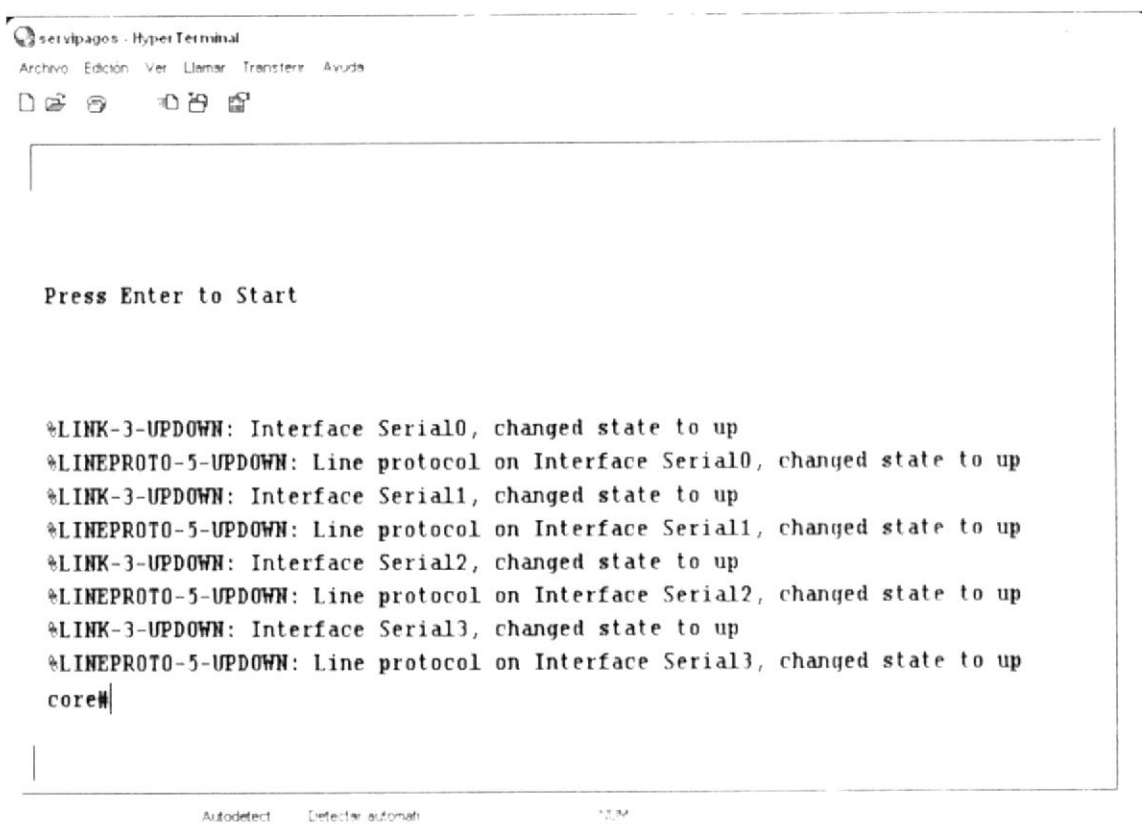


Figura 7-11: Pantalla de inicio del HYPERTERMINAL

7.11 MODOS DE UN ROUTER

Al momento de ingresar a la consola de un router existen 3 tipos modos:

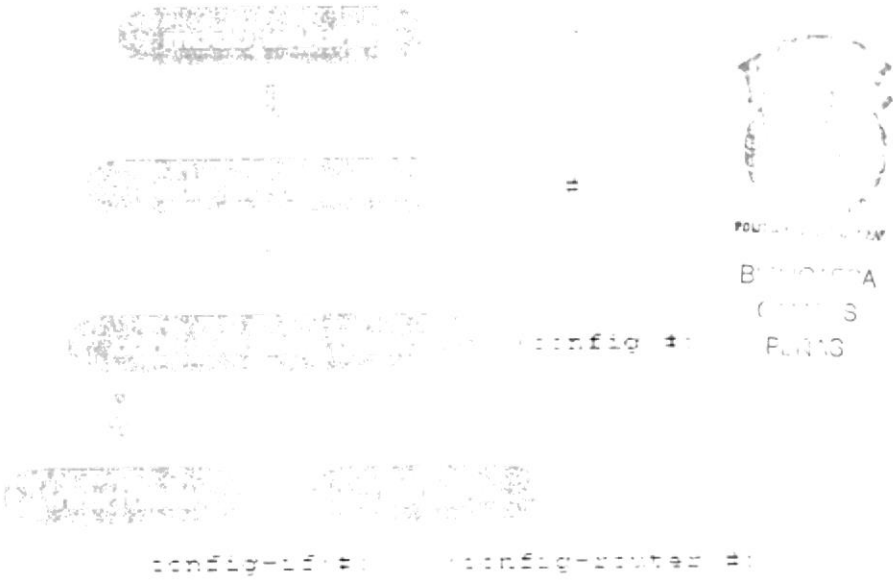


Figura 7-12: Gráfico de los modos

MODO	DETALLE
Modo usuario	El que solo puede visualizar pero no modificar nada
Modo privilegiado	El que puede modificar editar configurar un ruteador.
Modo Global	Se trata al ingresar a la configuración principal del router

Tabla 7-2: Modos de un Router

7.12 COMADOS SHOWS

Los comandos **SHOWS** permiten visualizar los contenidos del router para saber si hay falla de algo.

Continuación se detalla los tipos de **SHOWS** que existen:

7.12.1. SHOW VERSIÓN

Muestra la versión del IOS, versión del bootstrap; tiempo arriba; tiempo enrutador; cantidad de memoria instalada.

```
matriz_core#show version

Boson Operating Simulation Software
BOSS (tm) C2600 Software (C2600-Enterprise), Version 12.1, RELEASE SOFTWARE
Copyright (c) 1998-2003 by Boson Software, Inc.

BOSS ROM: System Bootstrap, Version 12.2, RELEASE SOFTWARE
matriz_core Uptime is 0 days, 0 hours, 0 minutes
System restarted by power-on
System image file is ""flash:c2600-enterprise.12.1.boss"", booted via flash
Boson 2600 (BOSS) processor (revision 5.0)
1 Fast Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
3 ISDN Basic Rate interface(s)
32K bytes of simulated non-volatile configuration memory.
8192K bytes of simulated System flash (Read/Write)

Configuration register is 0X2102
```

Figura 7-13: show Versión

7.12.2. SHOW INTERFACES

Muestra un reporte de las interfaces disponibles en el equipo

```
matriz_core#show interfaces
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.30.6/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Serial1 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.30.9/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
```

Figura 7-14: Show interfaces



7.12.3. SHOW PROTOCOLS

Muestra si las interfaces están arriba

```
matriz_core#show protocols
Global values:
  Internet Protocol routing is enabled
Serial0 is up, line protocol is up
  Internet address is 192.168.30.6/30
Serial1 is up, line protocol is up
  Internet address is 192.168.30.9/30
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.30.33/29
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
```

Figura 7-15: Show Protocols

COMADOS	DETALLE
UP	La interfaz están levantada
DOWN	La interfaz no están levantadas

Tabla 7-3: Comandos UP-Down

7.12.4. SHOW CLOCK

Muestra la hora en la consola del router

```
matriz_core#show clock
*00:17:11 UTC March 1 1993
```

Figura 7-16: Show Clock

7.12.5. SHOW HISTORY

Muestra el historial del los últimos cambios efectuado en la consola del rutedor

```
matriz_core#show history
show version
show memory
show interfaces
show protocols
show clock
show history
```

Figura 7-17: Show History

7.12.6. SHOW IP ROUTE

Muestra la tabla de ruteo

```
Mtr_conex Port#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
```

```
192.168.30.0/0 is variably subnetted, 9 subnets
C      192.168.30.4/30 is directly connected, Serial1
C      192.168.30.0/30 is directly connected, Serial0
R      192.168.30.64/29 [120/1] via 192.168.30.1, 00:01:19, Serial0
R      192.168.30.72/29 [120/1] via 192.168.30.1, 00:01:41, Serial0
R      192.168.30.80/29 [120/1] via 192.168.30.1, 00:03:39, Serial0
R      192.168.30.88/29 [120/1] via 192.168.30.1, 00:05:39, Serial0
R      192.168.30.96/29 [120/1] via 192.168.30.1, 00:07:13, Serial0
R      192.168.30.16/29 [120/1] via 192.168.30.1, 00:03:20, Serial0
O      192.168.30.8/30 [110/64] via 192.168.30.9, 00:12:46, Serial1
```

Figura 7-18: Show ip Router

7.12.7. SHOW VLANS

Muestra la tabla de las vlans

```
Switch#show vlan
```

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

Figura 7-19: show vlan

7.12.8. SHOW ACCESS-LISTIS

Permite ver los acces-list que fueron creados en el router asignado en este gráfico se demuestra que se ha denegado telnet y ping.

```
enlace_1#show access-lists
Extended IP access list 101
    deny  icmp 192.168.10.40 0.0.0.3 host 192.168.10.42 (0 matches)
    deny  tcp 192.168.10.40 0.0.0.3 host 192.168.10.42 eq telnet (0 matches)
```

Figura 7-20: show access listis

7.12.9. SHOW TERMINAL

Permite ver el tiempo que se ha conectado con el hyperterminal con su equipo.

```
Mtr_conex Urd#show terminal
Line 0, Location: "", Type: ""
Length: 24lines, Width: 80 columns
Status: PSI Enabled, Ready, Active, Automore On
Capabilities: none
Modem state: Ready
Group codes: 0
Special Chars: Escape Hold Stop Start Disconnect Activation
                ^x none - - none
Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch
           00:10:00 never none not set
           Idle Session Disconnect Warning
           never
           Login-sequence User Response
           00:00:30
           Autoselect Intial Wait
           not set

Modem type is unknown
Session limit is not set
Time since activation: 00:01:32
Editing is enabled
History size is enabled, history size is 10
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are none
Allowed output transports are lat pad v120 mop telnet rlogin nasi
Preferred transport is lat
No output characters are padded
No special data dispatching characters
```



Figura 7-21: Show terminal

7.12.10. SHOW RUNNING-CONFIG

Permite ver la configuración actual del router

```
Mtr_conex_Port#show running-config
BUILDING CONFIGURATION...

!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Mtr_conex_Port
enable password cisco
!
!
!
ip subnet-zero
!
!
!
!
interface Serial0
 ip address 192.168.30.2 255.255.255.252
 no ip directed-broadcast
 clock rate 64000
 bandwidth 1544
!
interface Serial1
 ip address 192.168.30.5 255.255.255.252
 no ip directed-broadcast
 bandwidth 1544
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 bandwidth 100000
 shutdown
!
interface Bri0
 no ip address
 no ip directed-broadcast
 shutdown
!
!
ip classless
no ip http server
!
!
!
line con 0
 login
 transport input none
 password cisco
line aux 0
line vty 0 4
 login
 password cisco
!
no scheduler allocate
end
```

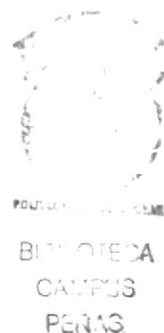


Figura 7-22: Show running-config

7.12.11. SHOW FLASH

Permite ver la memoria flash del router

```
Mtr_conex_Urd#show flash
System flash directory:
File Length Name/status
  1  5880916 c2600-js-mz.121-9.T.bin
[5880980 bytes used, 2507628 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)
```

Figura 7-23: Show Flash



7.13 PROTOCOLOS DE ENRUTAMIENTOS

7.13.1. INTRODUCCIÓN

Un aspecto fundamental en las redes de conmutación de paquetes es el encaminamiento y los algoritmos que para él se emplean. A lo largo de las clases teóricas, se han diferenciado dos técnicas para los mismos (por vector distancia y por estado del enlace) y se han analizado dos de los posibles algoritmos de camino más corto. En este manual, se observará cómo funcionan dos de los protocolos de enrutamiento que se utilizan en IP (**R.I.P. y O.S.P.F.**).

- ✦ El primero de ellos será un protocolo de **vector distancia**
- ✦ El segundo lo será de **estado del enlace**. Que no permitirá observar cómo se crean las tablas de rutas de los routers de la red, ni cuál es la información intercambiada entre los mismos, pero sí se podrá comprobar como es posible encaminar los paquetes en función de distintos criterios.

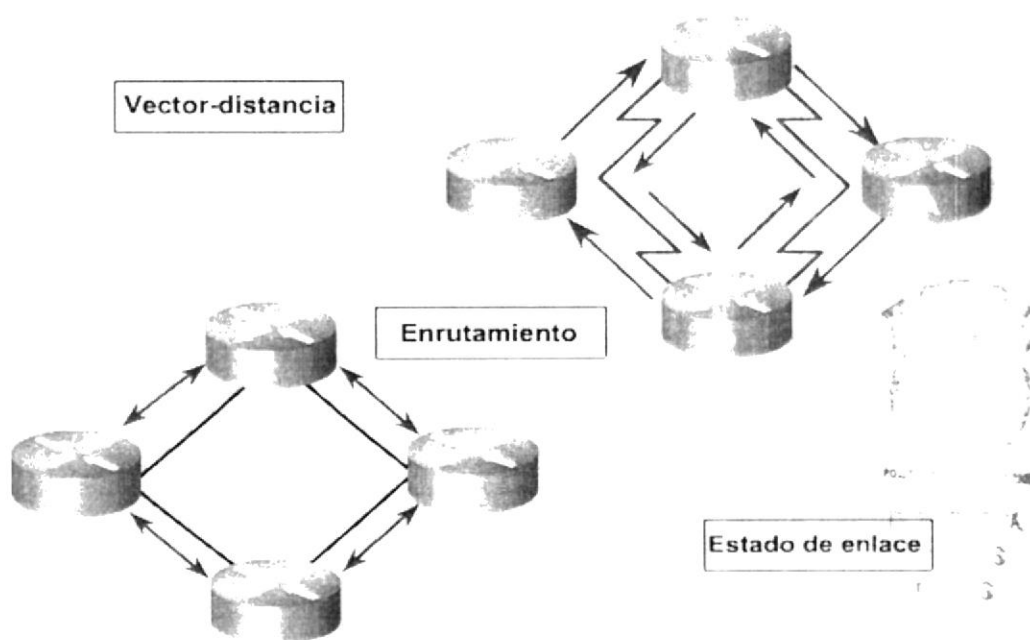


Figura 7-24: Gráfico enrutamiento

7.14 ENRUTAMIENTO DINÁMICO VS. ESTÁTICO

Básicamente existen dos maneras de enrutar a otros hosts fuera del nodo local y son utilizando enrutamiento estático o enrutamiento dinámico.

Cada método tiene ventajas e inconvenientes, pero cuando una red crece finalmente el enrutamiento dinámico es la única manera factible de gestionar la red.

Por este motivo se plantea la necesidad de utilizar protocolos de enrutamiento dinámico en vez de usar rutas estáticas en *todos* los nodos.

Existen programas para llevar el enrutamiento dinámico en la mayoría de los sistemas operativos, por lo que no debe ser complicado instalarlos en un nodo. Para sistemas UNIX existe un programa, zebra, que puede gestionar los protocolos de enrutamiento estáticos mencionados en este documento. Además zebra es software gratuito con licencia GPL.

Hay que destacar que el uso de estos protocolos será transparente al usuario final y será exclusivamente un tema para los gestores de nodos en caso que el nodo conecte a otros. Desde el punto de vista del cliente el enrutamiento será resuelto mediante la configuración DHCP automática cuando el cliente conecta al nodo.

Como no es obligatorio que un nodo conecta a otros, el uso de estos protocolos y el enrutamiento dinámico no es obligatorio. En algunos casos una ruta estática puede ser suficiente para realizar la conexión.

7.15 PROTOCOLOS RIP

7.15.1. INTRODUCCIÓN HISTÓRICA



Uno de los protocolos de routing más antiguos es el Routing Information Protocol o más comúnmente llamado RIP. Utiliza algoritmos de vector distancia para calcular sus rutas. Este tipo de algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

Los protocolos vector distancia fueron descritos académicamente por: R.E. Bellman, L.R. Ford Jr y D.R. Fulkerson .

La primera organización que implementó un protocolo de vector distancia fue la compañía Xerox en su protocolo GIP (Gateway Information Protocol), este protocolo estaba incluido dentro de la arquitectura XNS (Xerox Network Systems). GIP se utilizaba para intercambiar información de routing entre redes o sistemas autónomos no adyacentes. Pero claro, Xerox había implementado su propio protocolo propietario.

Poco después la Universidad de California en Berkeley creo una variante llamada "routed", esta variante del GIP introdujo novedades como modificación del campo de direccionamiento, que se consiguió más flexible , también se añadió un temporizador que limitaba a 30 segundos el tiempo máximo de actualización, es decir, el tiempo máximo permitido sin saber la información de los vecinos, y por supuesto se integró dentro de UNIX, con lo cual pasó a ser abierto.

7.15.2. INTRODUCCIÓN TÉCNICA

RIP es un protocolo de routing de vector distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies. RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto. RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace.

7.15.3. VERSIONES RIP

También existe un RIP para IPX; casualmente lleva el mismo acrónimo, pero no está directamente relacionado con el RIP para redes IP, ad-hoc.

RIPv1	✓ No soporta subredes ni CIDR. ✓ Tampoco incluye ningún mecanismo de autenticación de los mensajes. ✓ No se usa actualmente. ✓ Su especificación está recogida en el RFC 1058.
RIPv2	✓ Soporta subredes, CIDR y VLSM. ✓ Soporta autenticación utilizando uno de los siguientes mecanismos: ○ no autenticación ○ autenticación mediante contraseña ○ autenticación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). ○ Su especificación está recogida en el RFC 1723-2453.
RIPng	✓ RIP para IPv6. Su especificación está recogida en el RFC 2080

Tabla 7-4: Versiones de RIP

7.15.4. CARACTERÍSTICAS RIP

- ✓ RIP utiliza UDP para enviar sus mensajes y el puerto bien conocido 520.
- ✓ RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.
- ✓ RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado)
- ✓ RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).

7.15.5. MÁSCARA DE RED DE RIP

La característica de máscara de red de *rip* está soportada para ambas versiones, la 1 y la 2.

7.15.6. VERSIÓN 1 DE RIP

Originalmente no contenía información de la máscara. En la versión 1 de RIP, las clases eran utilizadas originalmente para determinar el tamaño de la máscara. Las redes de Clase A utilizaban 8 bits para la máscara, las redes de Clase B utilizaban 16 bits para la máscara, mientras que las redes de Clase C utilizaban 24 bits para la máscara. Actualmente, el método más utilizado para el tamaño de la máscara de un paquete consiste en asignar al paquete la máscara en base al interfaz que recibió el paquete.

7.15.7. VERSIÓN 2 DE RIP

Soporta la máscara de subred de tamaño variable (variable length subnet mask VLSM). Extendiendo la submáscara de red, la máscara puede ser dividida y puede reusarse. Cada subred puede usarse para propósitos diferentes como grandes o medianas LANs y enlaces WAN. El demonio *ripd* de Quagga no soporta las máscaras no secuenciales, las cuales están incluidas en la especificación de RIP versión 2.

En caso de existir información similar con el mismo prefijo y métrica, la información antigua será eliminada. Rip actualmente no soporta rutas multipath con el mismo coste.



7.15.8. VENTAJAS Y DESVENTAJAS DE RIP

7.15.8.1. VENTAJAS

En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar. Además, es un protocolo abierto, soportado por muchos fabricantes.

7.15.8.2. DESVENTAJAS

Por otra parte, tiene la desventaja que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos (por cuántos routers o equipos similares pasa la información); no toma en cuenta otros criterios importantes, especialmente el ancho de banda. Esto puede causar ineficiencias, ya que puede preferir una ruta de bajo ancho de banda.

7.15.9. FUNCIONAMIENTO RIP

- ✓ RIP utiliza UDP para enviar sus mensajes y el puerto bien conocido 520.
- ✓ RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.
- ✓ RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado)
- ✓ RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).
- ✓ La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino. Teniendo en cuenta el límite de 15 saltos mencionado anteriormente. Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.
- ✓ Las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.



7.16 PROTOCOLOS OSPF

7.16.1. INTRODUCCIÓN HISTÓRICA



encaminamiento estándar.

En 1988, el grupo: Fuerza de Trabajo de Ingenieros de Internet (IETF) empezó a desarrollar un nuevo protocolo de enrutamiento que reemplazaría al protocolo RIP. Se desarrolló entonces el protocolo de pasarela interior Primero el camino abierto más corto (OSPF - Open Shortest Path First). OSPF es un protocolo de encaminamiento para redes IP que se basa en las especificaciones de RFC descritas al final del documento. En la década de los 90 OSPF fue recomendado como un protocolo de

El protocolo OSPF propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de bases de datos con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de encaminamiento más cortas. En este proceso se calculan tanto las métricas de estado del enlace como de distancia, en el caso de RIP se calcula sólo la distancia y no el tráfico del enlace, por esta causa OSPF es un protocolo de encaminamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de encaminamiento distribuida y de rápida propagación, entre las características más resaltantes de OSPF están:

- ✓ Rápida detección de cambios en la topología y restablecimiento muy rápido de rutas sin bucles.
- ✓ Poca sobrecarga, usa actualizaciones que informan de los cambios de rutas.
- ✓ División de tráfico por varias rutas equivalentes.
- ✓ Encaminamiento según el tipo de servicio.
- ✓ Uso de multienvío en las redes de área local.
- ✓ Máscaras de subred y superred.
- ✓ Autenticación.

En abril de 1990, la NASA cambió al protocolo OSPF y el tráfico de enrutamiento se redujo drásticamente. Tras un cambio e interrupción de la red, las informaciones de encaminamiento global se restablecían rápidamente (a los pocos segundos comparados con los minutos de otros protocolos mas antiguos). La versión " de OSPF se publicó a mediados de 1991 y en marzo de 1994 apareció una versión " revisada.



7.16.2. INTRODUCCIÓN TÉCNICA

OSPF (Open shortest path first, El camino más corto primero)

Es un protocolo de routing link-state no propietario, esto quiere decir principalmente dos cosas: Primero que es de libre uso y suele estar soportados por la mayoría de los equipos destinados a ofrecer servicios a la red y Segundo el ser un link-state quiere decir que a diferencia de RIP o IGRP que son Distance-vector, no mandan continuamente la tabla de rutas a sus vecinos sino que solo lo hacen cuando hay cambios en la topología de red, de esta forma se evita el consume de ancho de banda innecesario. En un cambio de topología OSPF envía el cambio inmediatamente de forma que la convergencia de la red es mas rápida que en los distance-vector donde depende de timers asignados, de forma que en un link-state el tiempo de convergencia puede ser de 4 o 5 segundos según la red en RIP puede ser de 180 segundos.

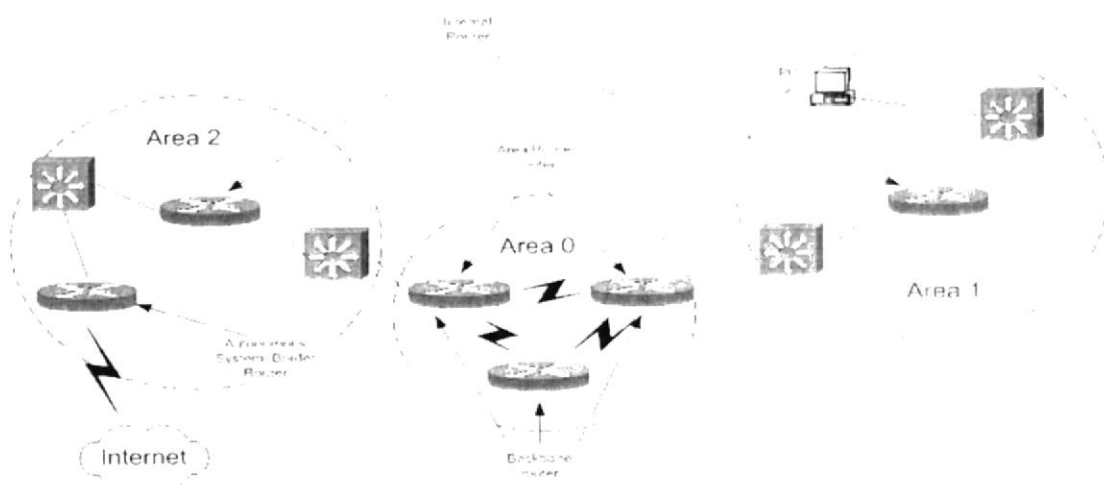


Figure 233. Gráfico protocolo OSPF

Los routers que forman parte de la red con OSPF se les denomina según su situación y su función dentro de la red de la siguiente forma:

Internal router: Un router con todas las redes directamente conectadas a la misma área. Estos solo mantienen una copia del algoritmo de routing.

Área Border Router: ABRs es un router que une un área al área 0 comparte la información entre las dos áreas y gestiona que redes se tiene que compartir entre ellas.

Backbone Routers: Son los routers que pertenecen al área 0 y responsable de la propagación de las redes entre distintas áreas.

Autonomous System Boundary Routers: Son routers conectados a otros AS o Internet. También suele ser el router que intercambia entre protocolos de routing IGP y EGP.

7.16.3. CARACTERÍSTICAS OSPF

- OSPF es un protocolo de encaminamiento interior, pero está diseñado para operar con un protocolo exterior adecuado, tal como BGP (Border Gateway Protocol).
- OSPF es complejo en comparación con RIP.
- Mucha de su complejidad tiene un sólo propósito: asegurar que las bases de datos topológicas son las mismas para todos los routers dentro de un área.
- Si los routers tuvieran bases de datos independientes, podrían tomar decisiones mutuamente conflictivas.
- OSPF se comunica por medio de IP (su número de protocolo es el 89).
- Es un protocolo de estado de enlace, primero el camino más corto.
- La especificación de OSPF hace uso de máquinas de estado para definir el comportamiento de los routers que siguen en el protocolo.
- Hay una máquina por componente y el estado de uno es independiente del resto.
- OSPF soporta rutas específicas de hosts, redes y subredes.
- El protocolo OSPF reconoce tres tipos de conexiones y redes:

7.16.4. CONEXIONES QUE SOPORTA OSPF

- Conexiones punto a punto entre dos ruteadores
- Redes multiacceso por difusión (la mayoría de las Lan)
- Redes multiacceso sin difusión (la mayoría en redes Wan)

Las redes multiacceso son todas aquellas que interconectan múltiples equipos donde cada uno es capaz de comunicarse con todos los otros equipos; la mayoría de las redes LAN y WAN tienen esta prioridad



7.16.5. VENTAJAS Y DESVENTAJAS DE OSPF

7.16.5.1. VENTAJAS

- Las rutas calculadas mediante OSPF nunca presentan bucles.
- OSPF puede escalar a interconexiones de redes mayores o mucho mayores.
- La reconfiguración correspondiente a los cambios de topología de la red es más rápida.
- Utilizan métricas de costos para seleccionar rutas a través de la red
- Utiliza actualizaciones generales por eventos e inundaciones LSA: (intercambia cambios en la red)
- Cada router tiene una topología de su propia red
- Cada router tiene una base de datos topológicos

7.16.5.2. DESVENTAJAS

- Este protocolo necesita un router que tenga más memoria y potencia de procesamiento
- Para reducir las bases de las políticas es necesario dividir la red en áreas (se necesita un Administrador capacitado)
- Al inicio del proceso se debe inundar la red con mensajes LSA, puede degradar la red

7.16.6. **FUNCIONAMIENTO DE OSPF**

- 1. Descubrir vecinos OSPF
- 2. Elegir el DR
- 3. Formar adyacencias
- 4. Sincronizar bases de datos
- 5. Calcular la tabla de encaminamiento
- 6. Anunciar los estados de enlaces



A continuación se describen cada uno de los seis pasos de funcionamiento del OSPF.

7.16.7. **DESCUBRIMIENTO VECINO OSPF**

Cuando los “routers” OSPF se activan, inician y mantienen relaciones con sus vecinos usando el protocolo Hello.

El protocolo además asegura que la comunicación entre vecinos sea bidireccional.

Los paquetes Hello se envían periódicamente al exterior por todas las interfaces de los “routers”.

La comunicación bidireccional se indica si el propio “router” aparece en el paquete Hello

Del vecino.

0	8	16	31
Version #	Type	Packet Length	
Router ID			
Area ID			
Checksum		Autype	
Authentication			

Figura 7-25: Cabecera OSPF

0	16	24	31
O S P F Packet Header (24 bytes)			
Network Mask			
Dead Interval		Hello Int	Priority
Designated Router			
Backup Designated Router			
Neighbor			

Repeated for each neighbor

Figura 7-26: Paquetes Hello de OSPF

7.16.8. DETERMINANDO EL DR

Se usa el protocolo Hello. El "router" examina la lista de sus vecinos, desecha cualquiera que no tenga comunicación bidireccional o que tenga un RP de ver, y graba el DR, el BDR y la RP que ha declarado cada uno de ellos. El "router" se añade él mismo a la lista, usando el valor RP configurado para la interfaz cero (desconocido) para el DR y el BDR, en el caso de que este proceso esté en proceso de activaciones determina el BDR y el DR.

La intención del mecanismo es la siguiente:

- ❖ Que cuando un "router" se active, no debería usurpar la posición del BDR actual aunque tenga un RP superior.
- ❖ Que la promoción de un BDR a DR debería ser ordenada y requerir que el BDR acepte sus responsabilidades.
- ❖ El algoritmo no siempre da lugar a que el "router" de mayor prioridad sea el DR, ni tampoco que el segundo de mayor prioridad sea el DR.

7.16.9. RESPONSABILIDADES DEL DR:

El DR genera para la red los anuncios de los estados de los enlaces, que inundan el área y describen esta red a todos los "routers" de todas las redes del área.

El DR se hace adyacente a otros "routers" de la red.

El BDR se hace adyacente a todos los demás "routers" de la red. Esto asegura que cuando ocupe el puesto del DR lo pueda hacer rápidamente.

7.16.10. FORMANDO ADYACENCIAS

La siguiente decisión es si se debería formar una adyacencia con uno de sus vecinos: En redes multiacceso, todos los "routers" se hacen adyacentes al DR y la BDR.

En enlaces punto a punto (virtuales), cada "router" forma siempre una adyacencia con el "router" del otro extremo.

Si se toma la decisión de no formar una adyacencia, el estado de la comunicación con el vecino permanece en el estado "2-way".

Las adyacencias son estables usando paquetes DD ("Database Description").

Se emplea un procedimiento de sondeo-respuesta para describir la base de datos.

El "router" con mayor ID se convertirá en maestro, el otro en esclavo. Los paquetes DD enviados por el maestro (sondeos) serán reconocidos por los DDs del esclavo (respuestas). El paquete contiene números de secuencia para asegurar la correspondencia entre sondeos y respuestas. Este proceso se denomina DEP ("Database Exchange Process").

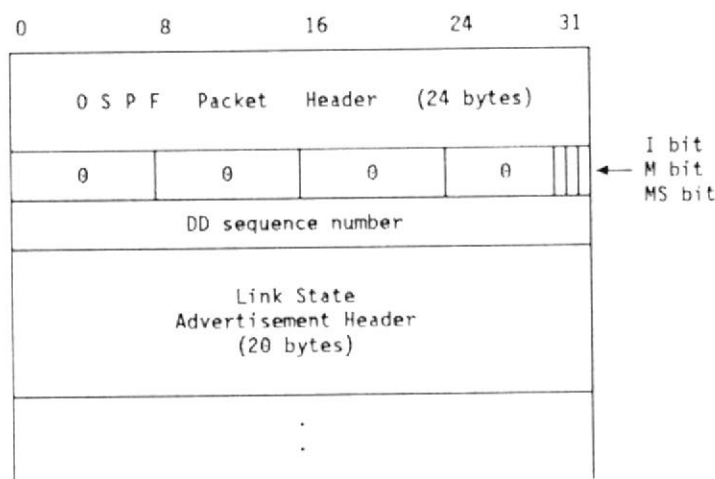


Figura 7-27: Paquete DD de OSPF

7.16.11. SINCRONIZACIÓN DE LAS BASES DE DATOS

Después de terminar el DEP ("Database Exchange Process"), cada "router" tiene una lista de aquellos anuncios para los que el vecino tiene más instancias actualizadas, que se solicitan por medio de paquetes LSR ("Link State Request"). La respuesta a un LSR es un LSU ("Link State Update") que contiene algunos o todos los anuncios solicitados.

Si no se repite respuesta, se repite la solicitud.

NOTA: Los anuncios vienen en los siguientes cinco formatos

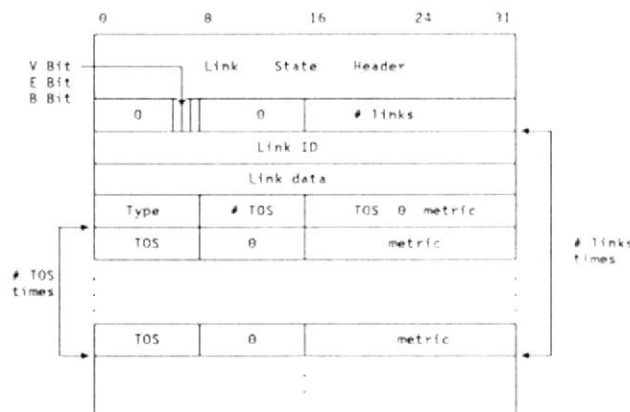


Figura 7-28: (tipo 1) RLA ("Router Links Advertisement") de OSPF

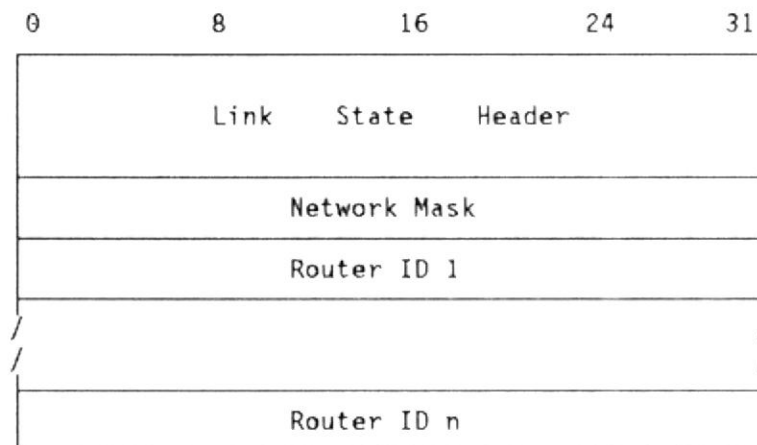


Figura 7-29:(Tipo 2) NLA ("Network Links Advertisement") de OSPF

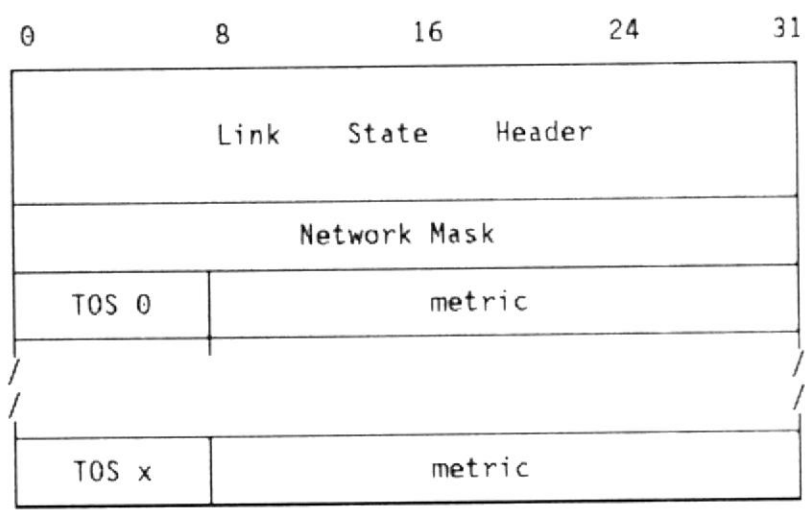


Figura 7-30:(Tipo 3 y 4) SLA ("Summary Links Advertisement") de OSPF

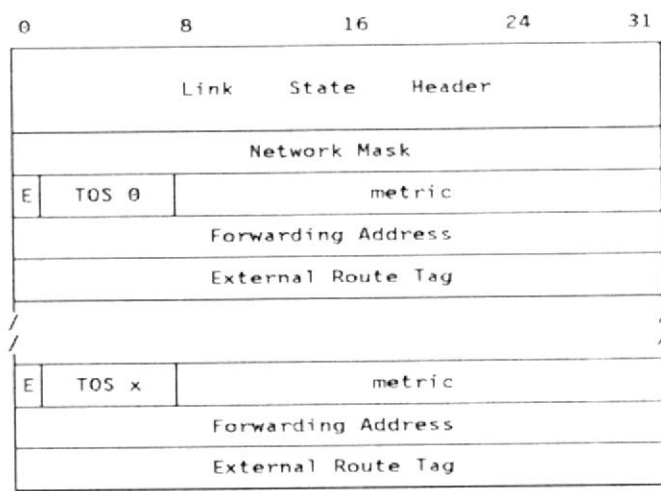


Figura 7-31:(Tipo 5) ELA ("External Links Advertisement") de OSPF

Cuando se han respondido los paquetes LSR, las bases de datos se sincronizan y los routers" se describen como totalmente adyacentes. La adyacencia se añade a los anuncio de los dos "routers" correspondientes.

7.16.12. CALCULANDO LA TABLA DE ENCAMINAMIENTO

Usando como entrada las bases de datos de estados de enlaces de las áreas con las que está conectado, el "router" ejecuta el algoritmo SPF para construir su tabla de encaminamiento. El cálculo consiste en los siguientes pasos:

- ❖ Las rutas intra-área se calculan construyendo el árbol mínimo para cada área conectada usando el mismo "router" como raíz del árbol. El "router" calcula además si el área puede actuar como área de tránsito para enlaces virtuales.
- ❖ Las rutas inter-área se calculan examinando los SLA. Para los ABR (que forman parte de la troncal) sólo se utilizan los anuncios correspondientes a la troncal.
- ❖ Si el "router" está conectado a una o más áreas de tránsito, el "router" sustituye las rutas que haya calculado por rutas que pasen por áreas de tránsito si estas son mejores.
- ❖ Las rutas externas se calculan examinando los anuncios externos del AS. Las localizaciones de los ASBR ya se conocen debido a que se determinan como cualquier otra ruta intra-área o inter-área.

7.16.13. ANUNCIANDO LOS ESTADOS DE LOS ENLACES

Un "router" anuncia periódicamente el estado de su enlace, por lo que la ausencia de un anuncio reciente indica a los vecinos del "router" que no está activo. Todos los "routers" que hayan establecido comunicación bidireccional con un vecino ejecutan un contador de inactividad para detectar ese suceso.

La comunicación se debe establecer desde cero, incluyendo la resincronización de las bases de datos.

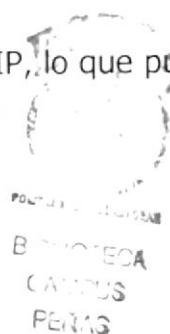
Un "router" también relanza sus anuncios cuando su estado cambia.

Un router puede lanzar diversos anuncios para cada área. Estos se propagan a través del área por el procedimiento de inundación. Cada "router" emite un RLA. Si el "router" es además el DR para una o más de las redes del área, originará NLAs para estas. Los ABR generan una SLA para cada destino inter-área conocido. Los ASBR originan un ASL para cada destino externo conocido. Los destinos se anuncian uno cada vez de tal forma que el cambio de una sola ruta puede inundar la red sin tener que enviar el resto de las rutas. Durante el proceso de inundación, un solo LSU puede llevar muchos anuncios.

7.16.14. CONCLUSIONES DEL PROTOCOLÓ OSPF

OSPF es un protocolo de encaminamiento complejo. Los beneficios de esta complejidad (sobre RIP) son los siguientes:

- ✓ Debido a las bases de datos de estados de enlaces sincronizados, los "router" OSPF convergerán mucho más rápido que los "routers" RIP tras cambios de topología. Este efecto se hace más pronunciado al aumentar el tamaño del AS.
- ✓ Incluye encaminamiento TOS ("Type of Service") diseñado para calcular rutas separadas para cada tipo de servicio. Para cada destino, pueden existir múltiples rutas, cada una para uno o más TOSs
- ✓ Utiliza métricas ponderadas para distintas velocidades el enlace. Por ejemplo, un enlace T1 a 544 Mbps podría tener una métrica de 1 y un SLP a 9600 bps una de 10.
- ✓ Proporciona balanceamiento de la carga ya que una pasarela OSPF puede emplear varios caminos de igual coste mínimo. A cada ruta se le asocia una máscara de subred, permitiendo subnetting de longitud variable y supernetting. Todos los intercambios entre "routers" se pueden autenticar mediante el uso de passwords.
- ✓ OSPF soporta rutas específicas de hosts, redes y subredes.
- ✓ OSPF permite que las redes y los hosts contiguos se agrupen juntos en áreas dentro de un AS, simplificando la topología y reduciendo la cantidad de información de encaminamiento que se debe intercambiar. La topología de un área es desconocida para el resto de las áreas.
- ✓ Minimiza los broadcast permitiendo una topología de grafo más compleja en la que las redes multiacceso tienen un DR que es responsable de describir esa red a las demás redes del área. Permitiendo el intercambio de información de encaminamiento externa, es decir, información de encaminamiento obtenida de otro AS.
- ✓ Permite configurar el encaminamiento dentro del AS según una topología virtual más que sólo las conexiones físicas. Las áreas se pueden unir usando enlaces virtuales que crucen otras áreas sin requerir encaminamiento complicado.
- ✓ Permite el uso de enlaces punto a punto sin direcciones IP, lo que puede ahorrar recursos escasos en el espacio de direcciones IP.



7.17 LISTA DE ACCESO

7.17.1. INTRODUCCIÓN

Es una Listas de sentencias que se aplican a una interfaz del router indicando de qué tipos de paquetes se deben aceptar y qué tipos de paquetes se deben denegar.

La aceptación y rechazo se pueden basar en dirección origen, dirección destino, protocolo de capa superior y número de puerto pero también se pueden crear para todos los protocolos enrutados de red (IP,IPX) (1 ACL por cada protocolo enrutado).

Se pueden configurar en el router para controlar el acceso a una red o subred filtrado de tráfico entrante y saliente de interfaces.

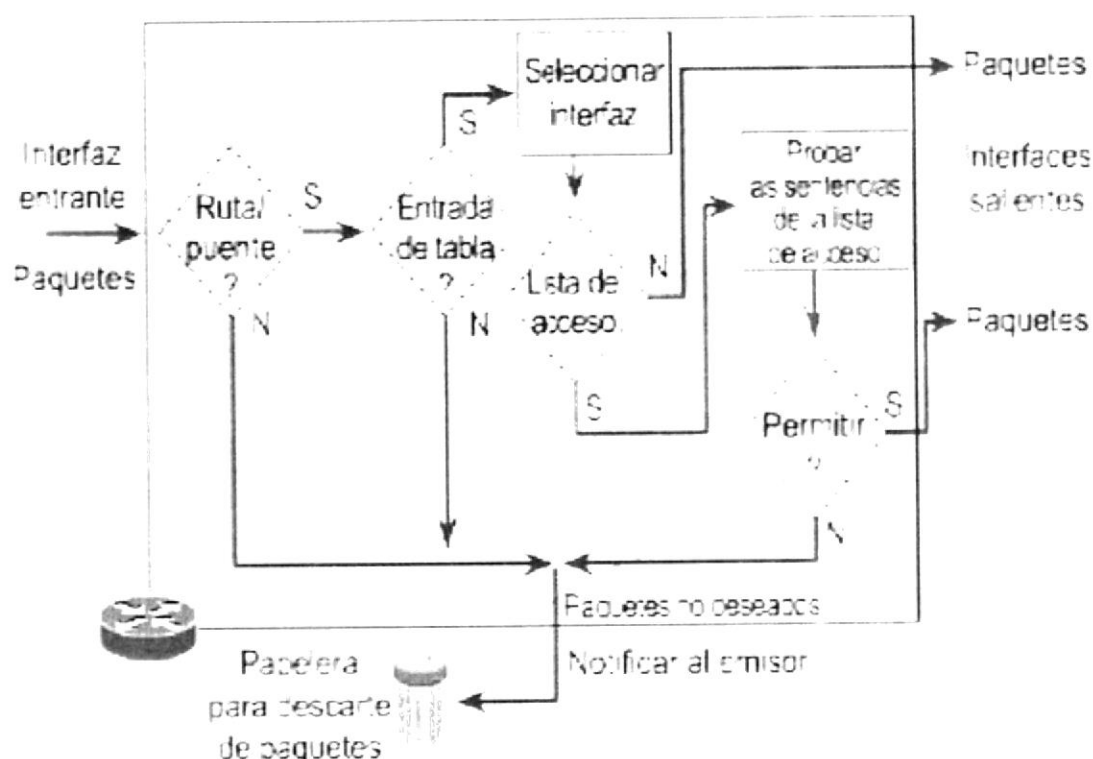


Figura 7-32: Gráfico flujo grama de una aceptación de ACL

7.17.2. EJECUCIÓN DE LAS ACLS

El orden de las sentencias de la ACL es importante

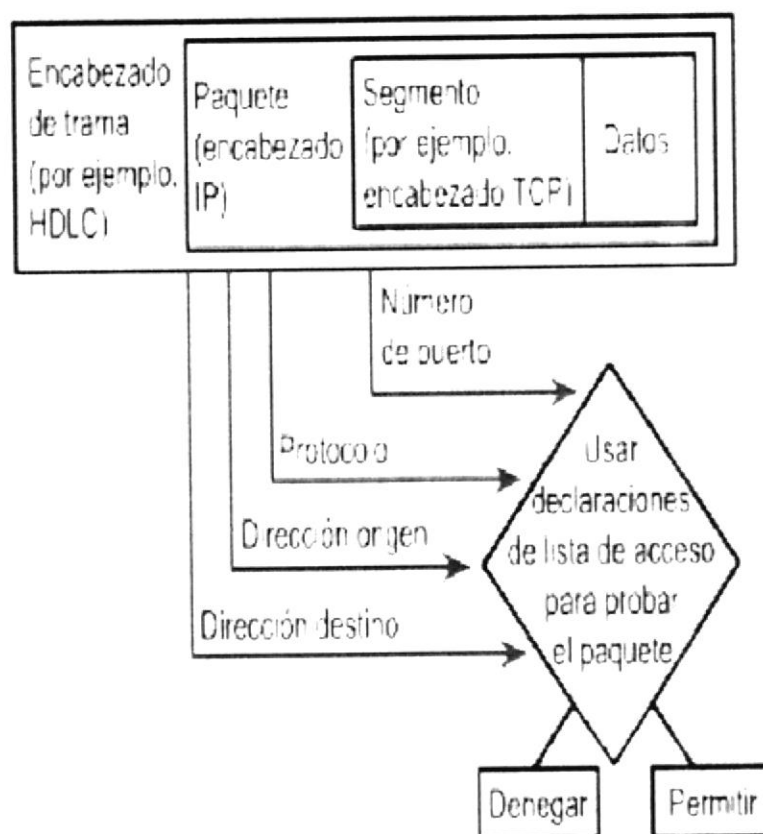


Figura 7-33: Función de ACL

- ✓ Cuando el router está decidiendo si desea enviar o bloquear un paquete, el IOS prueba el paquete, verificando si cumple o no cada sentencia de condición, en el orden en que se crearon las sentencias
- ✓ Una vez que se verifica que existe una coincidencia, no se siguen verificando otras sentencias de condición
- ✓ Para añadir sentencias en una ACL hay que eliminar la ACL completa y volver a crearla con las nuevas sentencias de condiciones

7.17.3. CREACIÓN DE LAS ACLS

Desde el modo de configuración global: **(config)#** ; existen 2 tipos de ACL:

- ❖ ACL estándar del 1 al 99
- ❖ ACL extendida del 100 al 199

Es importante seleccionar y ordenar lógicamente las ACL de forma cuidadosa que se deben seleccionar los protocolos IP que se deben verificar; si todos los demás protocolos no se verifican

7.17.3.1. ACLS ESTÁNDAR

Una ACL estándar puede servir para bloquear todo el tráfico de una red o de un host específico, permite también todo el tráfico de una red específica o denegar paquetes por protocolos

Ejemplo (permite acceso a todos los hosts de las 3 redes especificadas):

Router(config)# access-list 1 permit 192.5.34.0 0.0.0.255

Router(config)# access-list 1 permit 128.88.0.0 0.0.255.255

Router(config)# access-list 1 permit 36.0.0.0 0.255.255.255

- ↓ (Nota: cualquier otro acceso está implícitamente denegado) **(access-list 1 deny any)**

7.17.3.2. ACLS EXTENDIDAS

Ofrecen una mayor cantidad de opciones de control que las ACLs estándares, son más versátiles, verifican direcciones origen y destino de los paquetes, protocolos, números de puertos y otros parámetros específicos.

Las ACLs extendidas usan un número dentro del intervalo del 100 al 199, al final de la sentencia de la ACL extendida, se puede especificar y opcionalmente el número de puerto de protocolo TCP o UDP para el que se aplica la sentencia:

- ✓ **20 y 21: datos y programa FTP**
- ✓ **23: Telnet**
- ✓ **25: SMTP**
- ✓ **53: DNS**
- ✓ **69: TFTP**



Ejemplo 1 (denegar FTP entre dos redes y permitir todo lo demás):

```
Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255  
172.16.3.0 0.0.0.255 eq 21
```

```
Router(config)# access-list 101 permit ip 172.16.4.0 0.0.0.255  
0.0.0.0 255.255.255.255
```

```
Router(config)# access-list 101 deny ip 0.0.0.0 255.255.255.255  
0.0.0.0 255.255.255.255 (implícito)
```

- Ejemplo 2 (denegar Telnet a hosts de una red y permitir todo lo demás):

```
Router(config)# access-list 102 deny tcp 172.16.4.0 0.0.0.255  
any eq 23
```

```
Router(config)# access-list 102 permit ip any any
```

```
Router(config)# access-list 102 deny ip 0.0.0.0 255.255.255.255  
0.0.0.0 255.255.255.255 (implícito)
```

7.17.4. ¿POR QUÉ USAR ACLS?

- ✓ Limita el tráfico de red, mejorando su rendimiento
- ✓ Proporciona control de flujo del tráfico que debe pasar por el router
- ✓ Proporciona un nivel básico de seguridad de acceso a la red en función de distintos parámetros
- ✓ El administrador puede decidir qué tipo de tráfico se envía o bloquea en los interfaces del router
- ✓ Pertenecen a la categoría de cortafuegos de filtrado de paquetes (capa 3 y 4)

7.18 SWITCHES

7.18.1. INTRODUCCIÓN

Un switch denominado en el idioma castellano se la llama también "**conmutador**"; 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 Interconnection). Un conmutador o switch se 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.

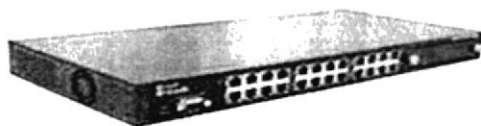


Figura 7-34: Gráfico dispositivos Switch

7.18.2. TECNOLOGÍA DE SWITCH

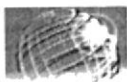
Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

7.18.3. QUE ES UNA SEGMENTACIÓN

La segmentación se trata de dividir un segmento de red en varias direcciones osea direcciones ip con la finalidad que estas ip sean utilizadas en varias máquinas que se encuentra conectadas en la red, esta dirección ip no se puede repetirse en la red ya que produce problemas de dirección de ip en la red.



NOTA: Las direcciones ip son direcciones que se la denomina direcciones lógicas

7.18.4. TIPOS DE SWICHT

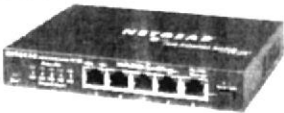
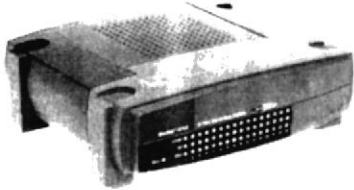
SWICHT	IMAGEN
✓ Switchs Netgear de 4 puertos	
✓ Linksys de 8 puertos	
✓ Cisco de 8 puertos	
✓ Linksys de 8 puertos	
✓ Linksys de 24 puertos.	
✓ Cisco de 48 puertos.	

Tabla 7-5: Tipos de Swicht

7.18.4.1.1. TIPOS DE CAPAS DE SWITCH

El SWITCH tiene a tomar distintas conexiones a medida que se plantean nuevos esquemas para mejorar el rendimiento de las redes de área local. Además los Switch pueden ser administrables y esclavos por lo tanto cada switch pueden ser diferentes tipos de capas conocidas que son:

- Switch capa 2.
- Switch capa 3.
- Switch capa 4.

7.18.4.1.1.1. SWITCH CAPA 2

Este es el tipo de switch de red de área local (LAN) más básico, el cual opera en la capa 2 del modelo OSI. Su antecesor es el bridge, por ello, muchas veces al switch se le refiere como un bridge multipuerto, pero con un costo más bajo, con mayor rendimiento y mayor densidad por puerto.

El switch capa 2 hace sus decisiones de envío de datos en base a la dirección MAC destino contenida en cada frame. Estos, al igual que los bridges, segmentan la red en dominios de colisión, proporcionando un mayor ancho de banda por cada estación.

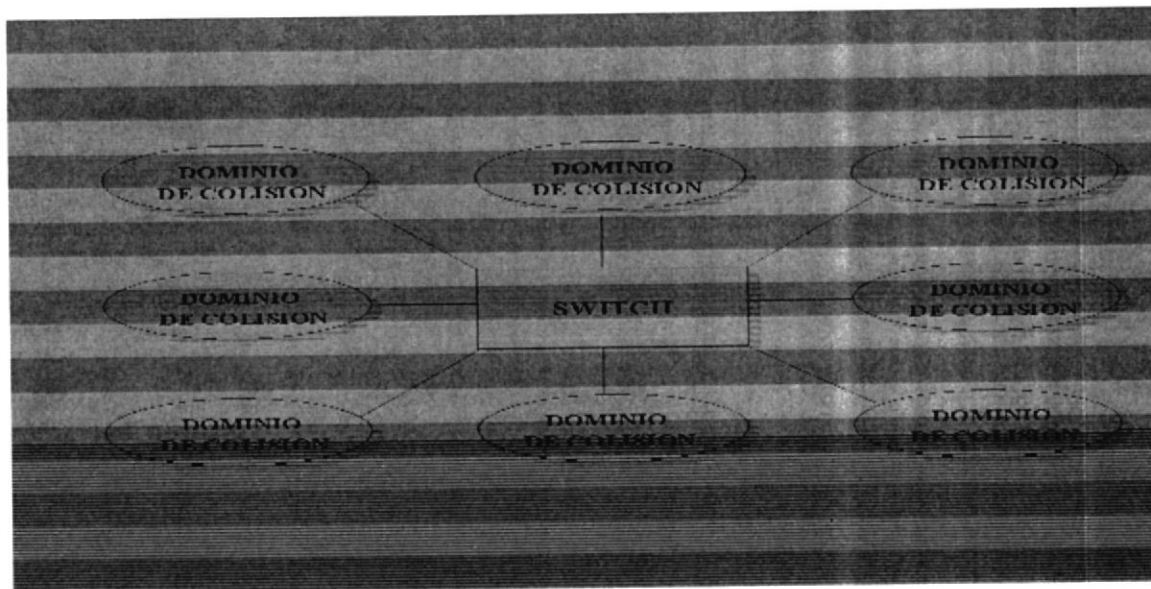
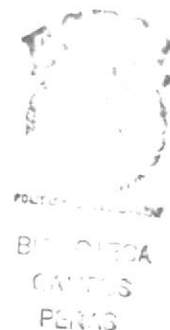


Figura 7-35: Dominios de broadcasts



La configuración de los switches capa 2 y el soporte de múltiples protocolos es totalmente transparente a las estaciones terminales. Como igual es el soporte de las redes virtuales (VLAN's), las cuales son una forma de segmentación que permite crear dominios de broadcasts formando así grupos de trabajo independientes de la ubicación física.

El uso de procesadores especializados (**ASIC: Application Specific Integrated Circuit**) incrementaron la velocidad de conmutación de los switches, en comparación con los bridges, porque pueden enviar los datos a todos los puertos de forma casi simultánea.

Estos switches siguen, principalmente, dos esquemas para envío de tráfico, los cuales son:

- **Cut-trough:** comienzan el proceso de envío antes de que el frame sea completamente recibido. En estos switches la latencia es baja porque sólo basta con leer la dirección MAC destino para comenzar a transferir el frame. La desventaja de este esquema, es que los frames corruptos (corruptos, enanos, con errores, etc.) son también enviados.
- **Store-and-forward:** lee y valida el paquete completo antes de iniciar el proceso de envío. Esto permite que el switch descarte paquetes corruptos y se puedan definir filtros de tráfico. La desventaja de este esquema es que la latencia se incrementa con el tamaño del paquete.

Algunos switches implementan otros esquemas (Fragment free) o esquemas híbridos en base a rendimiento y porcentaje de errores, pasando en un momento de modo Cut-trough al modo Store-and-forward y, viceversa.



7.18.4.1.1.2. SWITCH CAPA 3

Este tipo de switches integran routing y switching para producir altas velocidades (medidas en millones de paquetes por segundo). Esta es una tecnología nueva (Lippis, 1997) a los cuales los vendedores se refieren muchas veces como: Netflow, tag switching (Packet, 1998), Fast IP (3Com, 1997).

Este nuevo tipo de dispositivos es el resultado de un proceso de evolución natural de las redes de área local, ya que, combinan las funciones de los switches capa 2 con las capacidades de los routers (3Com, 1997).

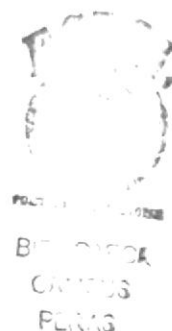
Existen dos tipos de switches de capa 3:

- **Packet-by-packet (PPL3).**
- **Cut-trough (CTL3).**

En ambos tipos de switches, se examinan todos los paquetes y se envían a sus destinos. La diferencia real entre ellos es el rendimiento. PPL3 enruta todos los paquetes, en tanto que los switches CTL3 efectúan la entrega de paquetes de una forma un poco distinta, estos switches investigan el destino del primer paquete en una serie. Una vez que lo conoce, se establece una conexión y el flujo es conmutado en capa 2 (con el consiguiente, rendimiento del switching de capa 2) (Lippis, Jun1997).

Funciones:

- Procesamiento de rutas: esto incluye construcción y mantenimiento de la tabla de enrutamiento usando RIP y OSPF.
- Envío de paquetes: una vez que el camino es determinado, los paquetes son enviados a su dirección destino. El TTL (Time-To-Live) es decrementado, las direcciones MAC son resueltas y el checksum IP es calculado.
- Servicios especiales: traslación de paquetes, priorización, autenticación, filtros



7.18.4.1.1.3. SWITCH CAPA 4

La información en los encabezados de los paquetes comúnmente incluyen direccionamiento de capa 2 y 3, tal como: tipo de protocolo de capa 3, TTL y checksum. Hay también información relevante a las capas superiores, como lo es el tipo de protocolo de capa 4 (UDP, TCP, entre otros.) y el número de puerto (valor numérico que identifica la sesión abierta en el host a la cual pertenece el paquete).

En el caso de los switches capa 3, éstos son switches capa 2 que utilizan la información del encabezado de capa 3. Lo mismo ocurre con los switches capa 4, son switches capa 3 que procesan el encabezado de la capa. También son conocidos como switches sin capa (Layerless switches).

La información del encabezado de capa 4 permite clasificar de acuerdo a secuencias de paquetes manejados por aplicación (denominados "flujos"). Ahora bien, dependiendo del diseño del switch, éste puede dar servicios o garantizar ancho de banda por "flujos". Algunos de los diseños de capa 4 son (Torrent, 1998)

7.18.4.2. CONSIDERACIONES ACERCA DE SWITCH

Los diseñadores y administradores de redes necesitan saber como y cuando usar las tecnologías de las que se ha hablado hasta ahora:

- ✓ Colocar los switches capa 3 en puntos de concentración de la red o como backbone colapsado para eliminar "cuellos de botella".
- ✓ Evitar enrutar en los switches capa 2 ubicados en los extremos o fronteras de la red.
- ✓ Escoger switches capa 3 que tengan buffers con capacidad desde 50 hasta 100 paquetes por puerto y enviar millones de paquetes por segundo en la capa 3.
- ✓ Evitar retardos excesivos, limitando los dominios de colisión entre 10 y 20 usuarios.
- ✓ Cuando se escogen switches capa 2 con soporte de VLAN se debe tomar en cuenta que la comunicación inter-vlan se hace usando un router y que, éste puede convertirse en un "cuello de botella" si la red es muy grande.

7.19 VLANS

7.19.1. INTRODUCCIÓN

La definición de VLANs se lleva a cabo en un único switch (servidor), La información sobre las VLANs se transmite mediante el backbone hacia los demás switches (clientes) usando el protocolo VTP (VLAN Trunk Protocol), si un switch se puede configurar para ignorar los mensajes VTP (modo transparente) , La configuración del switch sólo puede hacerse dentro de la VLAN de gestión (Management VLAN), por defecto, VLAN 1.

A su vez las vlan también se la utiliza para reducir los broadcast en la red y dividir la red por cada departamento.

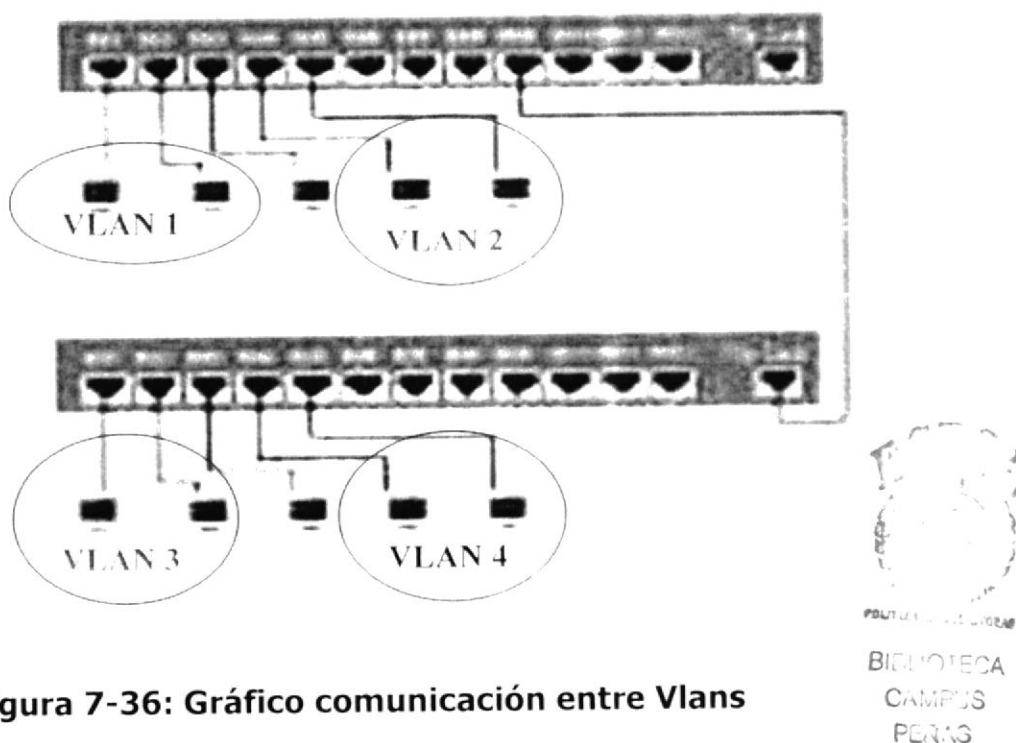
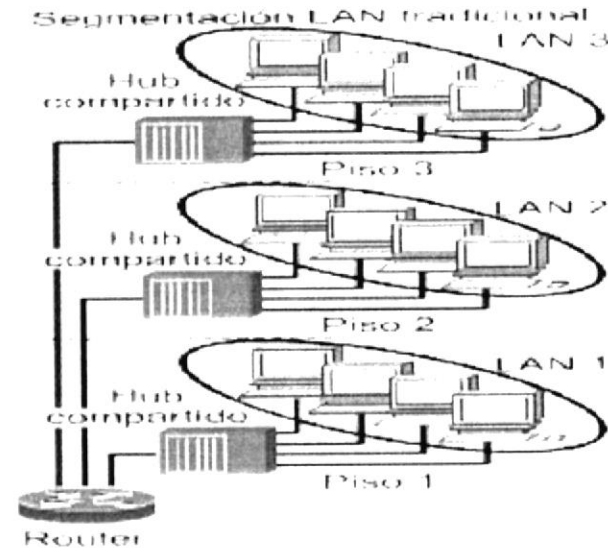


Figura 7-36: Gráfico comunicación entre Vlan

7.19.2. SEGMENTACIÓN TRADICIONAL

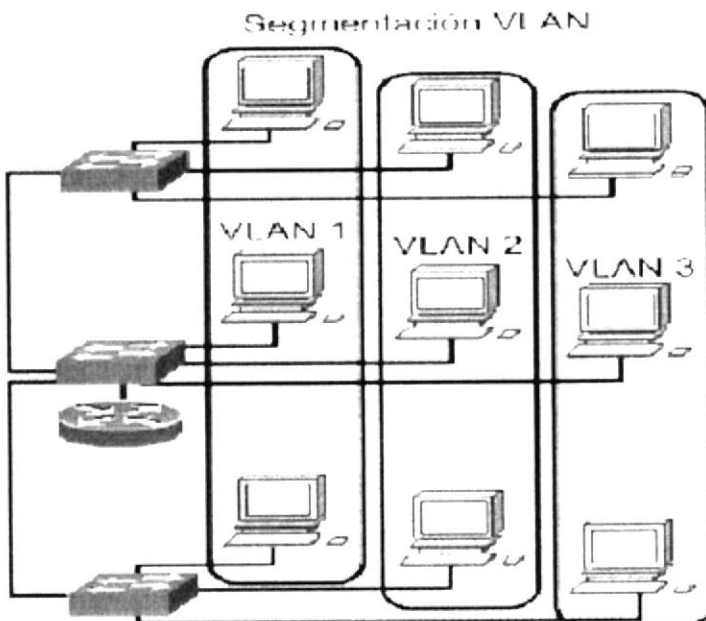
Cada usuario se conecta al hub/switch más próximo físicamente



- ✓ La pertenencia de un usuario a una red u otra está limitada por el cableado físico
- ✓ Si un segmento emplea hubs para la interconexión, todos los usuarios pertenecen al mismo dominio de colisión (no así si se usan switches)
- ✓ Los dominios de broadcast están delimitados por el router

Figura 7-37: Gráfico segmentación tradicional

7.19.2.1. SEGMENTACIÓN CON VLANs



- ✓ Cada usuario se conecta al switch VLAN más próximo físicamente.
- ✓ Se definen varias VLANs en los switches.
- ✓ Los usuarios se agrupan en las VLANs, según criterio del administrador.
- ✓ La pertenencia de un usuario a una VLAN no depende del cableado físico.
- ✓ Cada VLAN es un dominio de broadcast.
- ✓ El router permite la comunicación entre VLANs.

Figura 7-38: Gráfico segmentación con vlans

7.19.3. ENCAPSULAMIENTO

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una subred se deben colocar en paquetes que se puedan administrar mediante las vlans y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión). preparan que los datos lleguen a su destino.

7.19.4. CARACTERÍSTICAS DE LAS VLANS

- Crean una topología virtual independiente de la física
- Permiten agrupar a los usuarios en grupos de trabajo flexibles
- Funcionan en los niveles 2 y 3 de OSI
- La comunicación entre VLANs requiere enrutamiento de capa 3 (routers)
- Permiten controlar el tamaño de los dominios de broadcast
- Necesitan administración
- Pueden ayudar a aumentar la seguridad de la red



7.19.4.1. ASIGNACIÓN A VLANS

La asignación de usuarios a las VLANs definidas puede ser:

7.19.4.1.1. ESTÁTICA:

Cada puerto del switch es asignado a una VLAN. Por tanto, el usuario conectado a ese puerto pertenecerá a la VLAN.

- ✓ El administrador debe realizar la configuración VLAN manualmente
- ✓ Fácil de administrar
- ✓ Implementación más eficiente

7.19.4.1.2. DINÁMICA:

La pertenencia se determina en función de la dirección física (capa 2), dirección lógica (capa 3), tipo de protocolo, etc.

- ✓ Necesita de un servidor de configuración VLAN (que hay que mantener)
- ✓ Al conectar un usuario a un puerto, el switch consulta el servidor de configuración para determinar a qué VLAN pertenece
- ✓ No necesita administración al realizar desplazamientos de usuarios
- ✓ Seguridad: notificación cuando usuarios no autorizados acceden a la red

7.19.5. TIPOS DE VLANS

7.19.5.1. VLAN ENTRE SWITCHES: FILTRADO

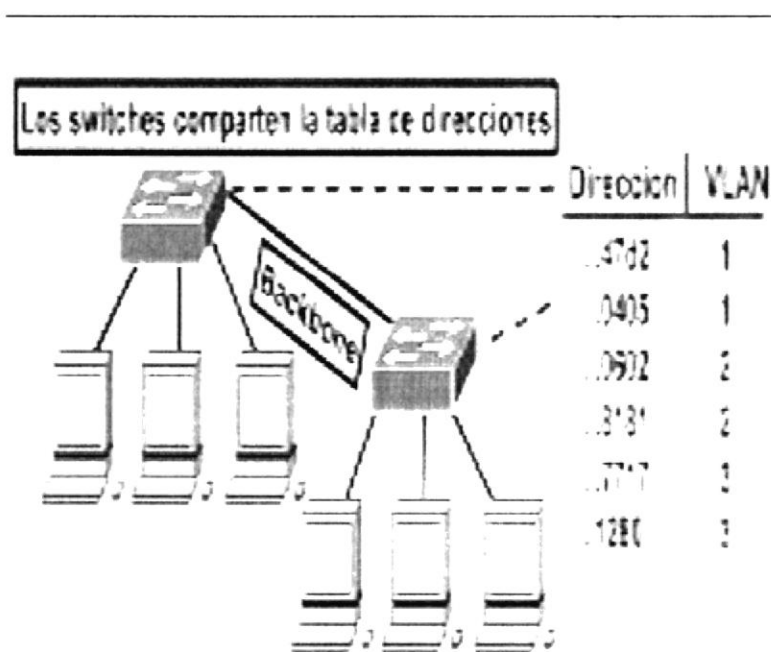


Figura 7-39: Gráfico vlan entre switches: filtrado

- ✓ Cada switch desarrolla una tabla de filtrado, que asocia cada dirección física con la VLAN a la que pertenece
- ✓ Los switches comparten las tablas a través del backbone
- ✓ Cuando una trama llega a un switch, éste puede determinar a qué VLAN pertenece empleando la tabla
- ✓ Esta técnica permite filtrar en función de cualquier parámetro de la trama (dirección física, lógica, ...)
- ✓ No es escalable; no se emplea actualmente

7.19.5.2. VLAN ENTRE SWITCHES: ETIQUETADO

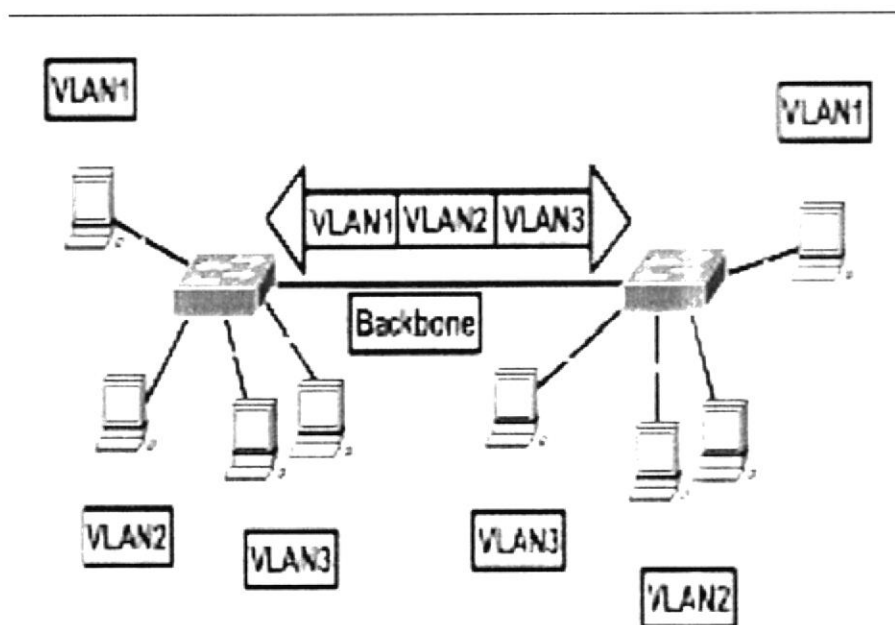


Figura 7-40: Gráfico vlan entre switches: etiquetado

- ✓ Cada VLAN tiene asociado un identificador
- ✓ Las tramas procedentes de los usuarios se etiquetan con el identificador correspondiente a la VLAN a la que pertenecen
- ✓ El etiquetado se lleva a cabo en el switch (capa 2 OSI)
- ✓ Las tramas etiquetadas atraviesan el backbone
- ✓ Cuando una trama etiquetada va a abandonar el backbone, el switch elimina el identificador
- ✓ Estándar IEEE 802.1Q



7.19.5.3. SEGURIDAD DE VLANS

- ✓ Un usuario sólo puede ver el tráfico broadcast de su VLAN.
- ✓ Un usuario no puede conectarse a la red sin la aprobación del administrador.
- ✓ Configuración de los switches: sólo desde la VLAN de gestión.
- ✓ Los routers pueden incorporar listas de control de acceso para filtrar el tráfico entre VLANs.

7.19.5.4. VENTAJAS DE LAS VLANS

- ✓ Permite reducir los broadcast.
- ✓ Brinda una mayor seguridad en la red LAN.
- ✓ Reduce congestionamiento en la red.
- ✓ Brinda estabilidad al usuario en el manejo de la red.
- ✓ Si un departamento genera un broadcast no le afectaría al resto de los departamentos.

7.20 IMPLEMENTACIÓN WAN

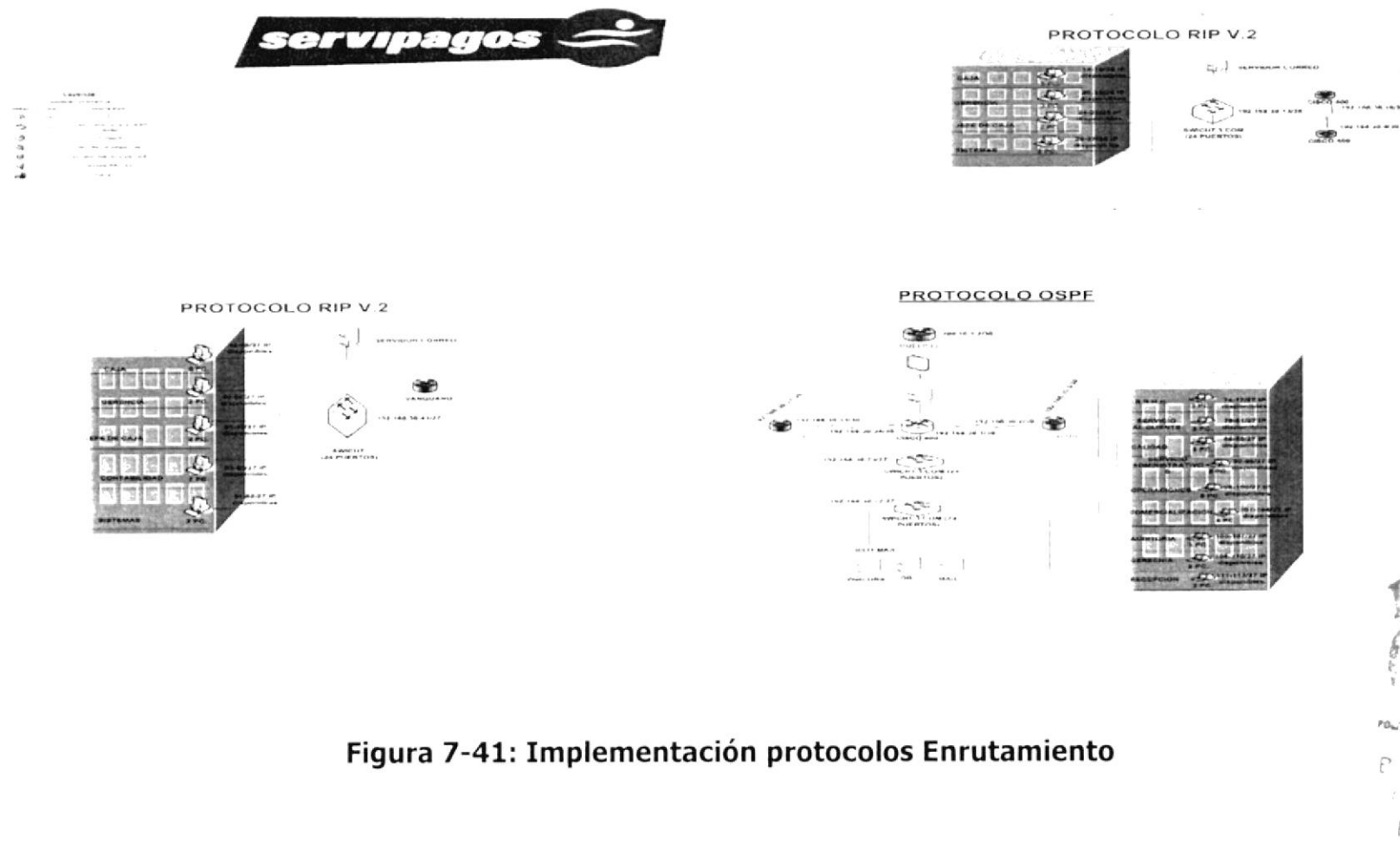


Figura 7-41: Implementación protocolos Enrutamiento

7.21 GRÁFICO LÓGICO DE LA COMUNICACIÓN WAN

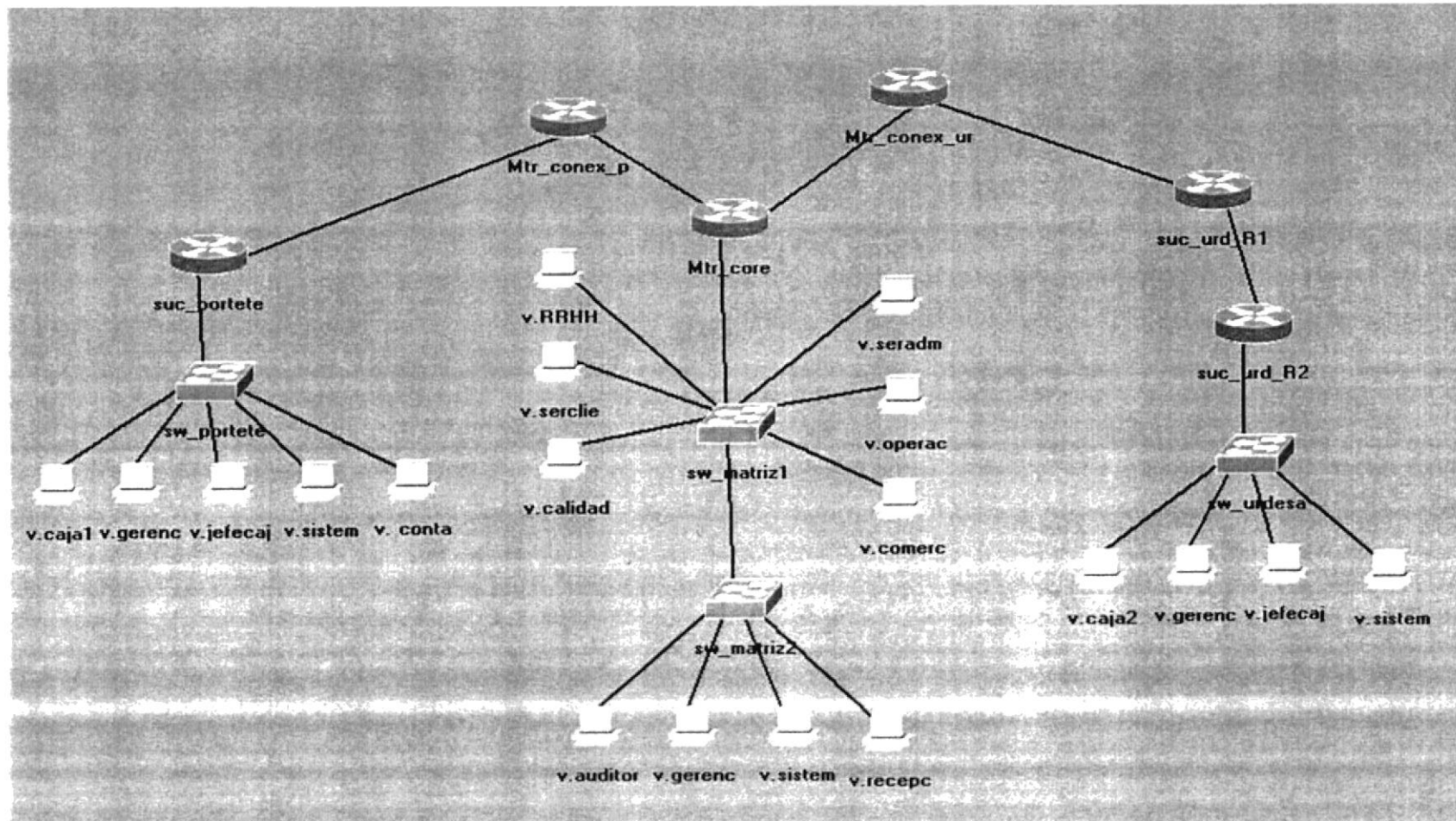


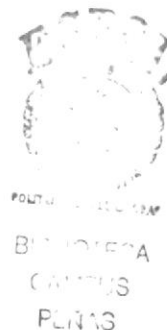
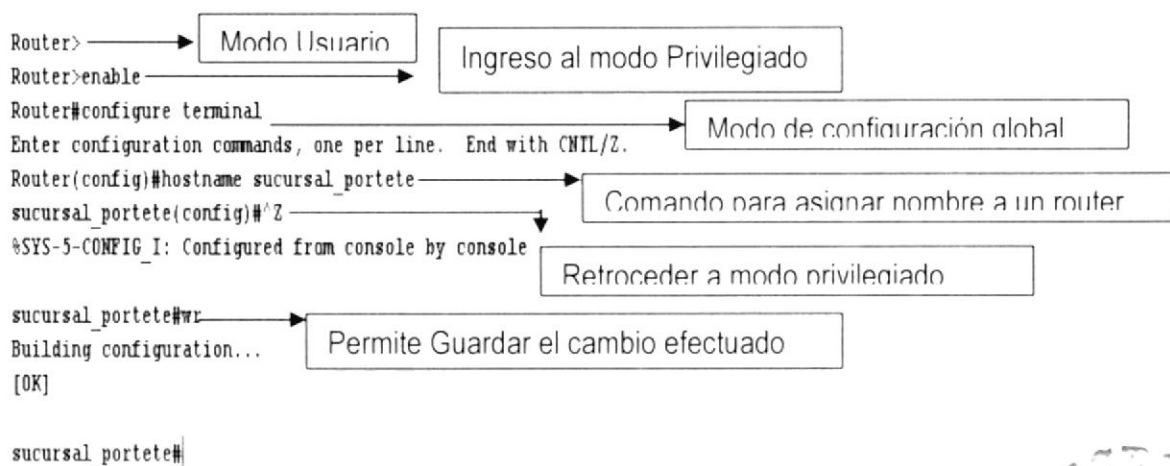
Figura 7-42: Implementación protocolos Enrutamiento Lógico

7.22 CONFIGURACIÓN DE LOS ROUTER Y SWICHT

7.22.1. ASIGNACIÓN DE NOMBRE AL ROUTER

ROUTER PORTETE

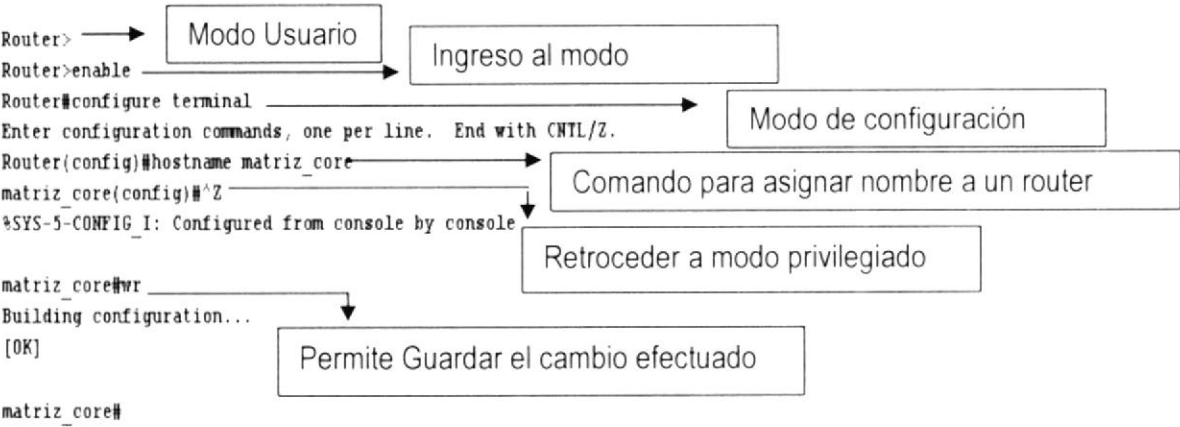
Press Enter to Start



ROUTER MATRIZ

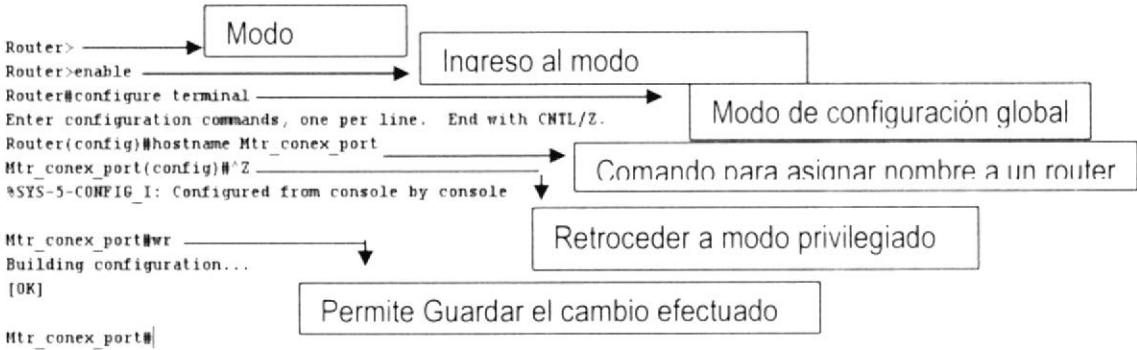
Router_Core

Press Enter to Start



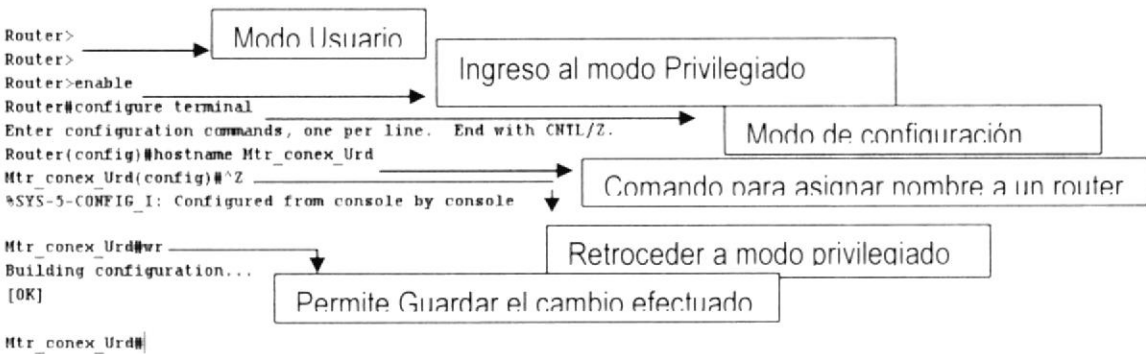
Router_conexión_Portete

Press Enter to Start



Router_conexión_Urdesa

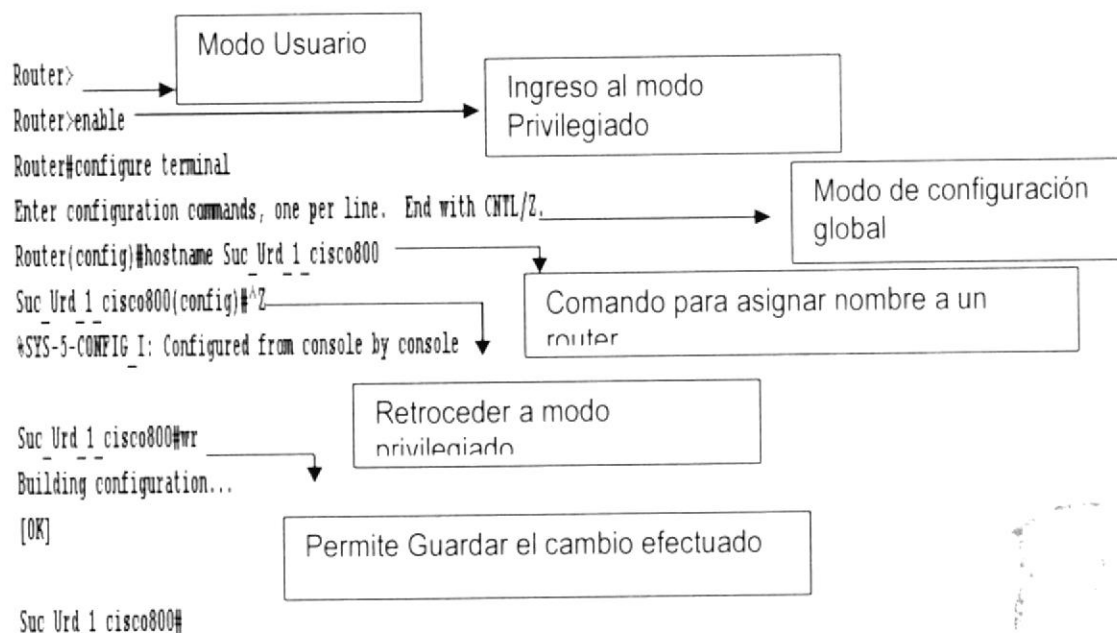
Press Enter to Start



ROUTER URDESA

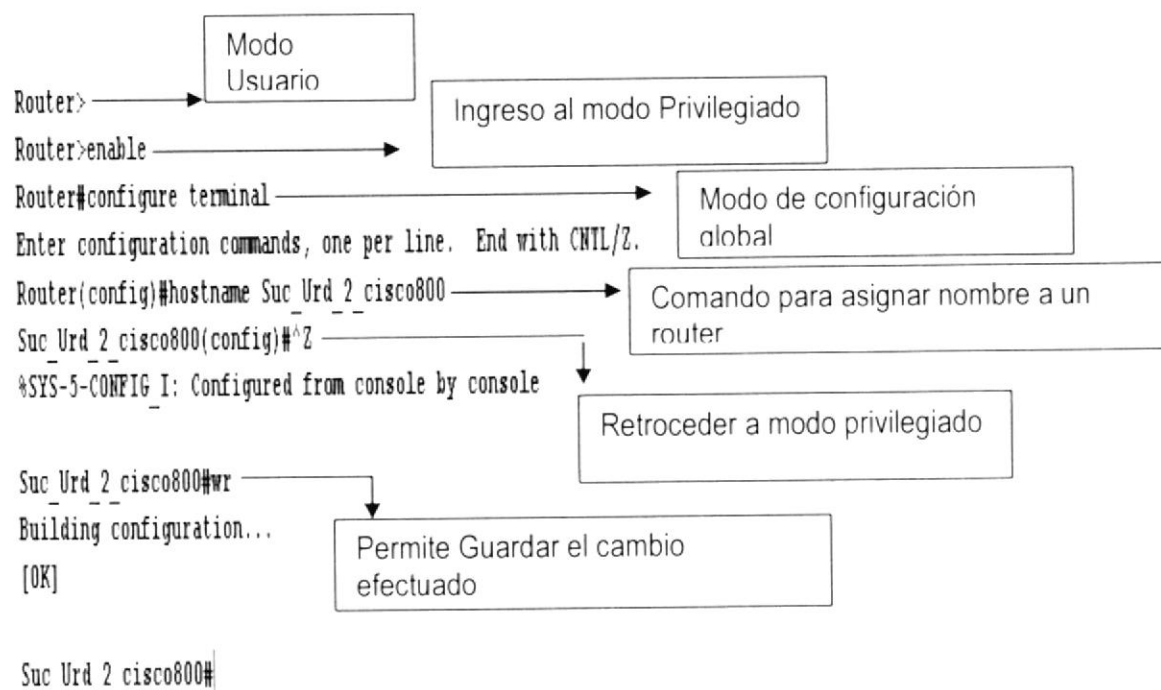
Router_1

Press Enter to Start



Router_2

Press Enter to Start



7.22.2. CONFIGURACIÓN DE LAS INTERFACES (s0/0 - s0/1)



NOTA: Antes de configurar las interfaces en cualquier router lo primero que se debe dar cuenta con que nombre están asignados las seriales con el comando **SHOW PROTOCOLS**, y a su vez permiten ver si las seriales están bajas o no.

```
sucursal_portete#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 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
```

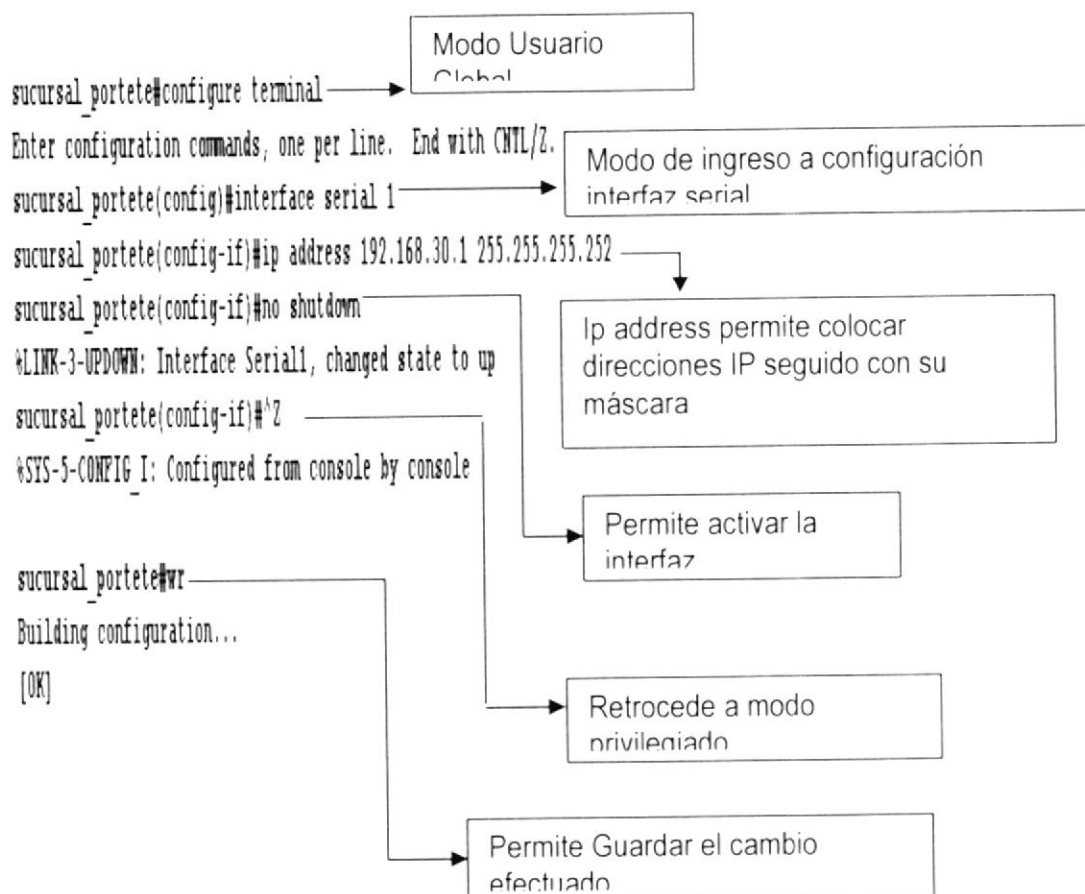
Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado

Es la interfaz serial administrable y la línea protocolo que está (bajo)

Es la fastethernet administrable y la línea protocolo que está (bajo)

ROUTER PORTETE

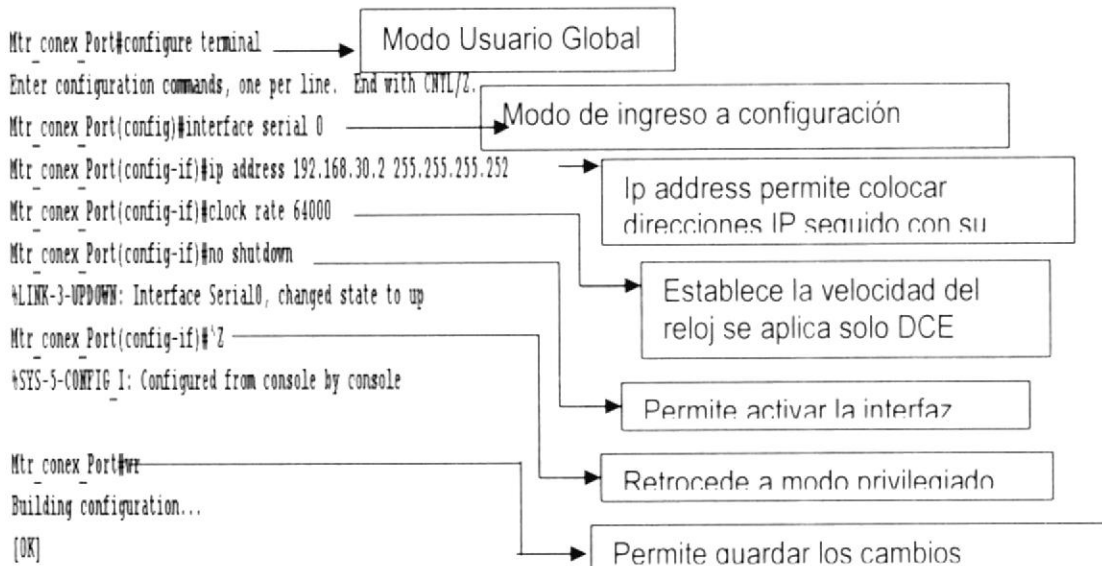
❖ Configuración de la serial 1 del router portete

BIBLIOTECA
CAMPUS
PERAS

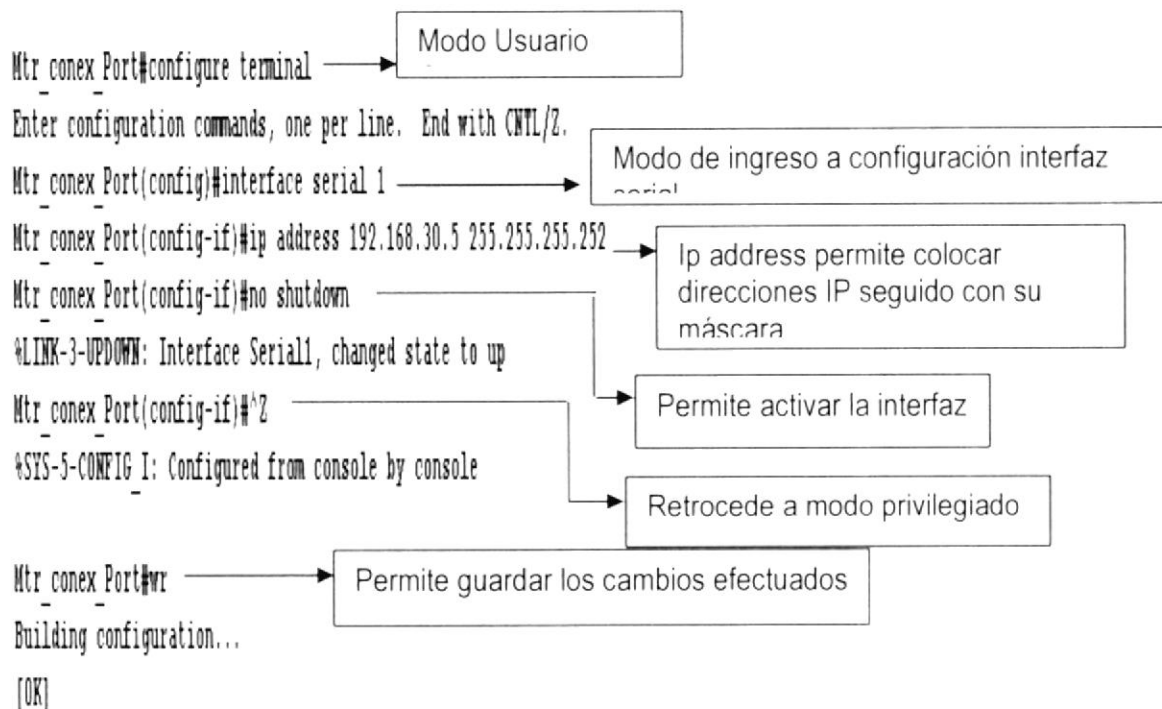
ROUTER MATRIZ

Router_ conexión _Portete

❖ Configuración de la serial 0 del router conexión_portete

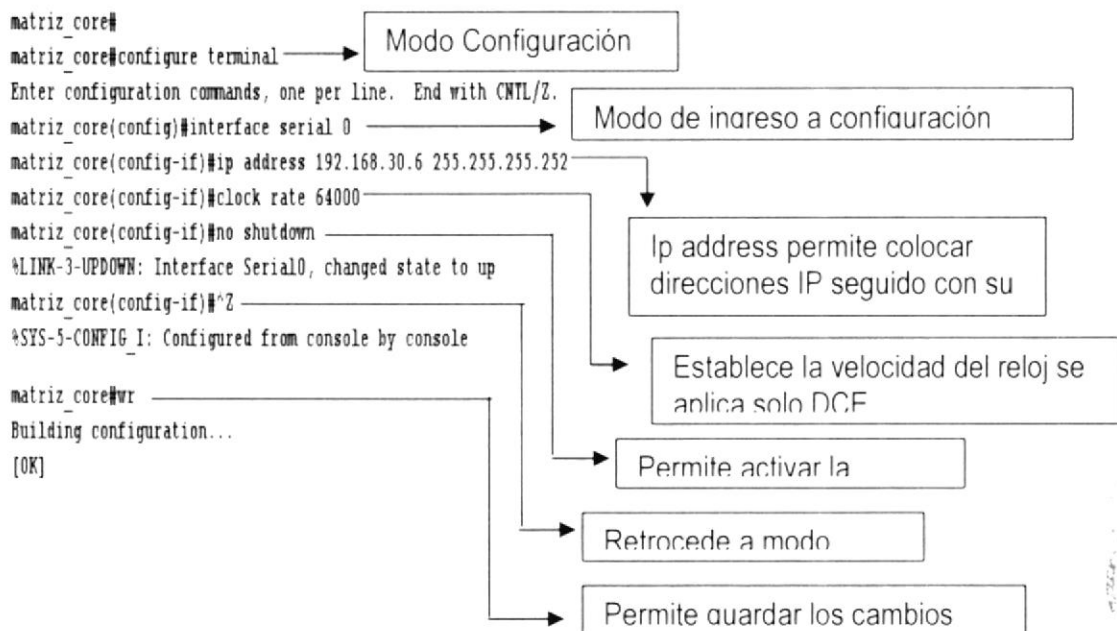


❖ Configuración de la serial1 1 del router conexión_portete

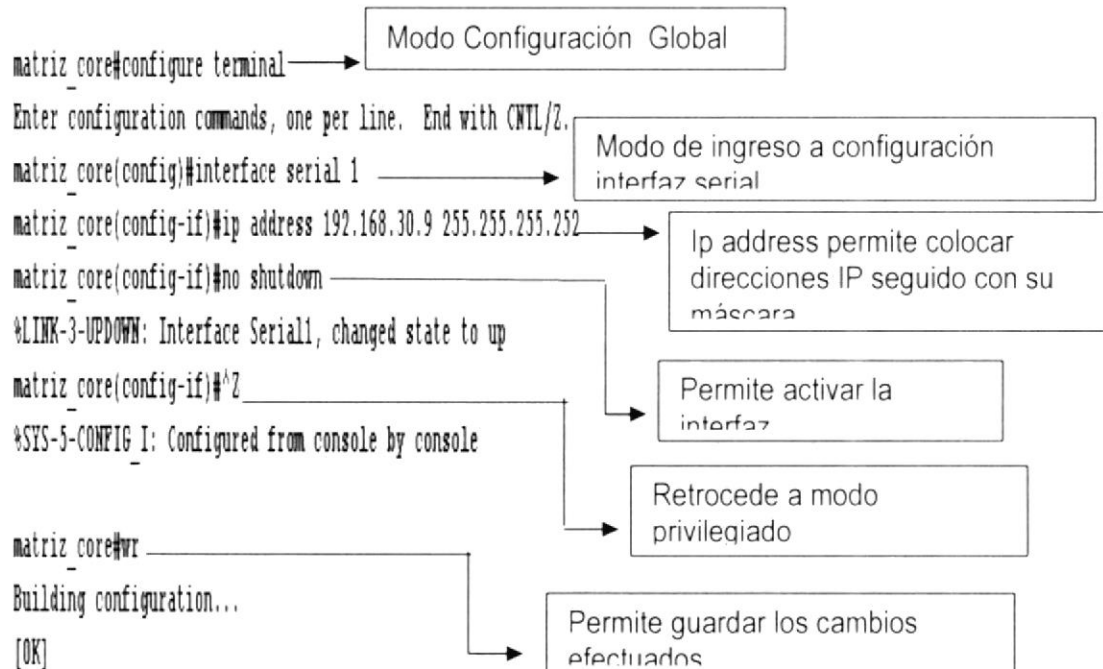


Router_matriz_core

Configuración de la serial 0 del router matriz_core

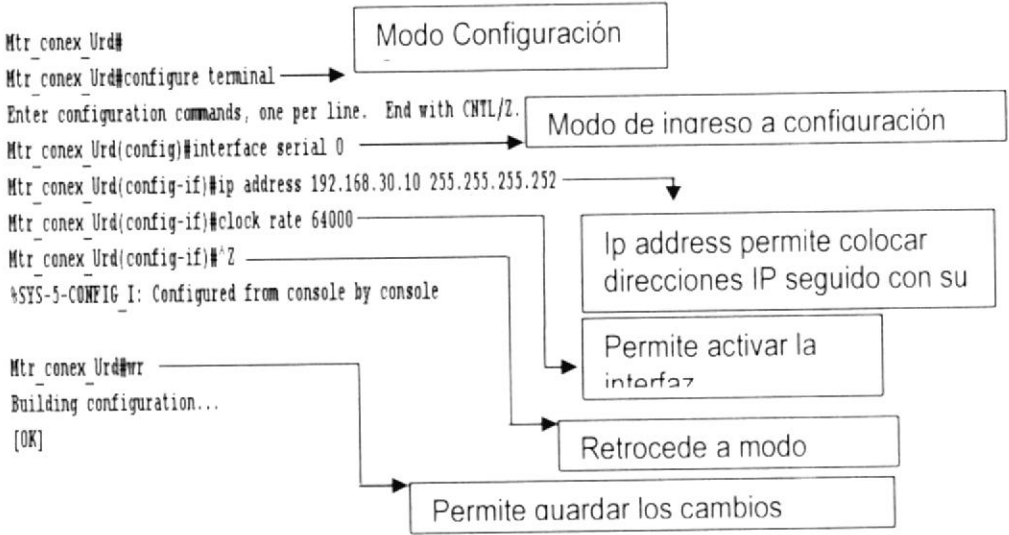


❖ Configuración de la serial 1 del router matriz_core

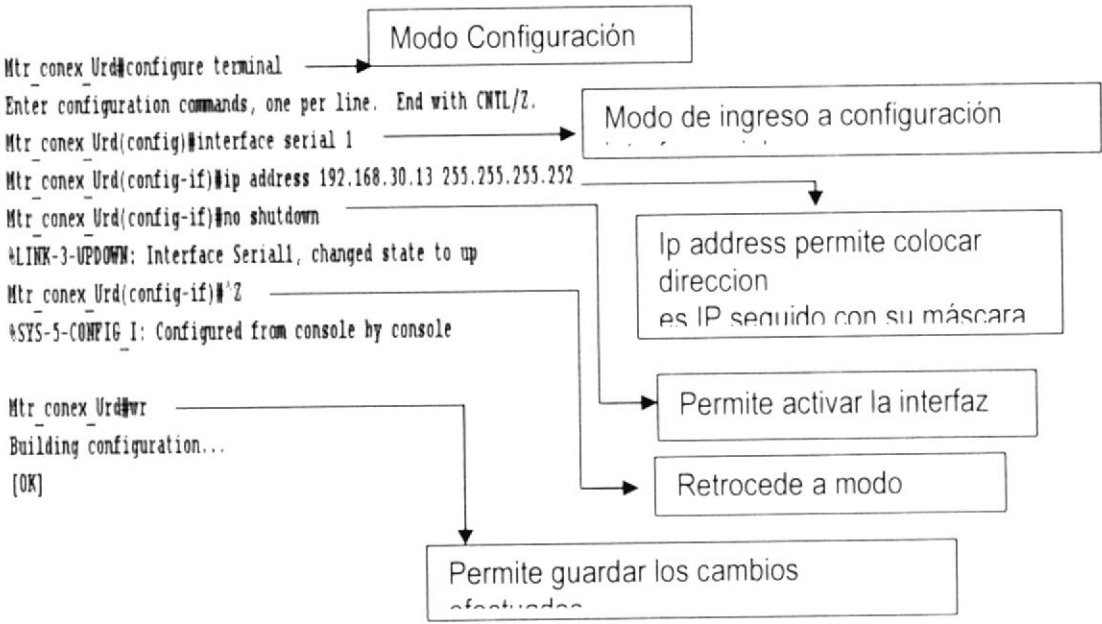


Router_ conexión _Urdesa

❖ Configuración de la serial 0 del router conexión _Urdesa



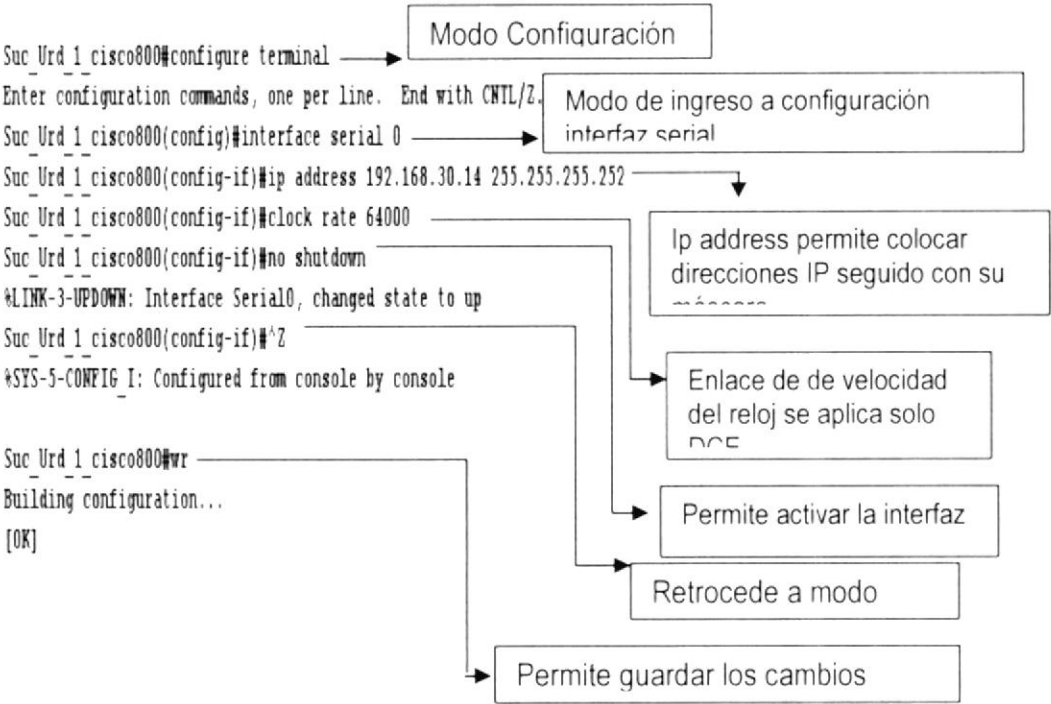
❖ Configuración de la serial 1 del router conexión _Urdesa



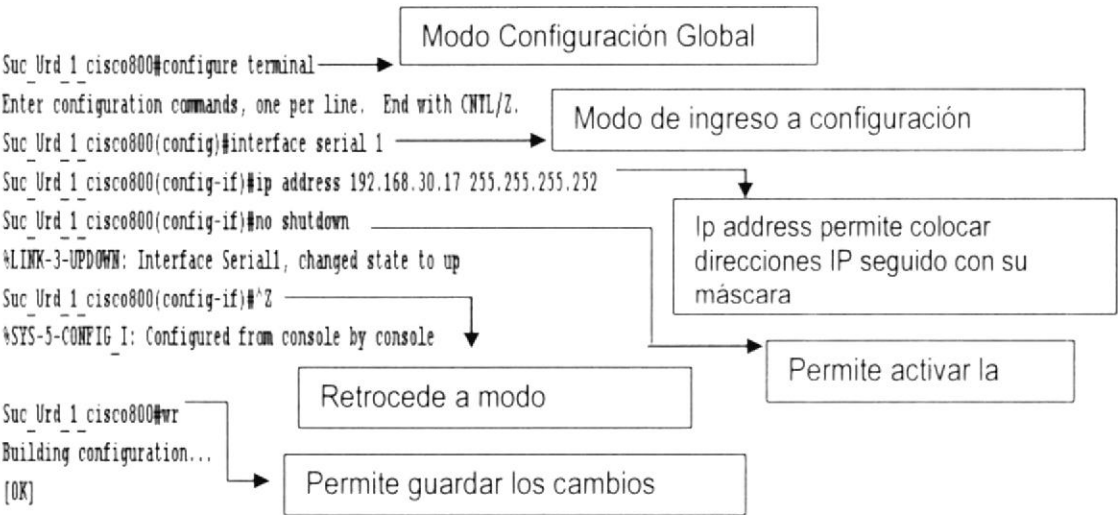
ROUTER URDESA

7.22.2.1. ROUTER_1

❖ Configuración de la serial 0 del router Urdesa

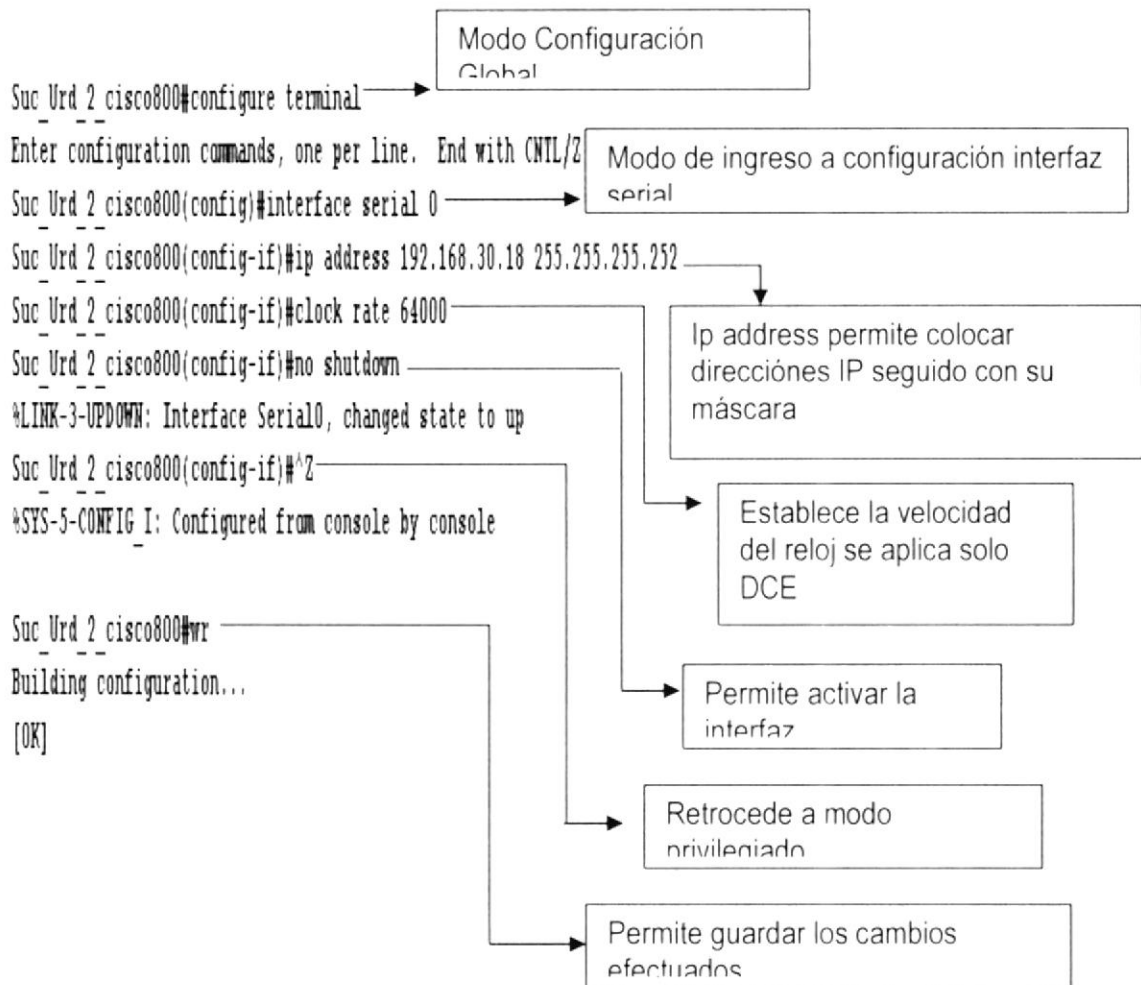


❖ Configuración de la serial 1 del router Urdesa



7.22.2.2. ROUTER_2

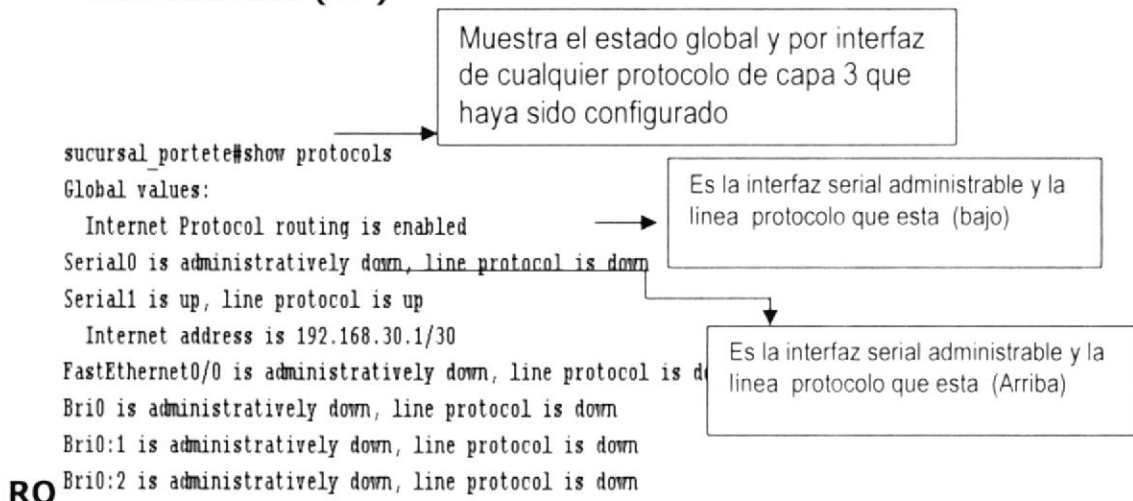
❖ Configuración de la serial 0 del router Urdesa



7.22.2.3. VERIFICAR SI LAS DIRECCIONES FUERON LEVANTADAS CON ÉXITO

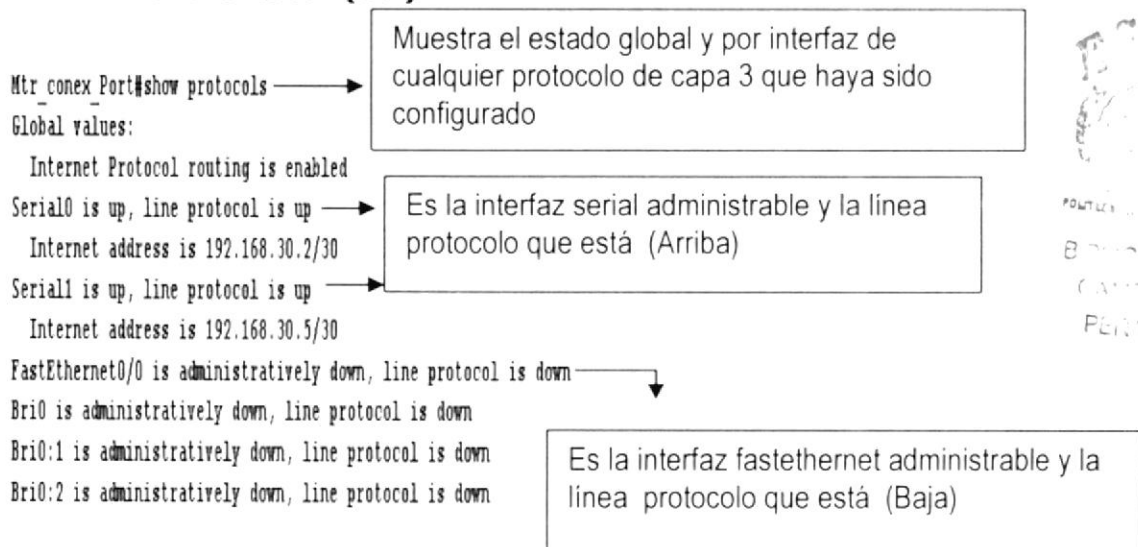
ROUTER PORTETE

- ✓ La dirección **192.168.30.1** que se conecta con el router Mtr_conex_port está levantada (UP)



Router_conexión_Portete

- ✓ La dirección **192.168.30.2** que se conecta con el router sucursal_portete está levantada (UP)
- ✓ La dirección **192.168.30.5** que se conecta con el router matriz_core está levantada (UP)



Router_mariz_core

- ✓ La dirección **192.168.30.6** que se conecta con el router conexión_portete está levantada **(UP)**
- ✓ La dirección **192.168.30.9** que se conecta con el router conexión_urdesa está levantada **(UP)**

matriz_core#show protocols

Global values:

Internet Protocol routing is enabled

Serial0 is up, line protocol is up

Internet address is 192.168.30.6/30

Serial1 is up, line protocol is up

Internet address is 192.168.30.9/30

FastEthernet0/0 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 el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado

Es la interfaz serial administrable y la línea protocolo que está (Arriba)

Es la interfaz fastethernet administrable y la línea protocolo que

Router_conexión_Urdesa

- ✓ La dirección **192.168.30.10** que se conecta con el router matriz_core está levantada **(UP)**
- ✓ La dirección **192.168.30.13** que se conecta con el router 1 de Urdesa está levantada **(UP)**

Mtr_conex_Urd#show protocols

Global values:

Internet Protocol routing is enabled

Serial0 is up, line protocol is up

Internet address is 192.168.30.10/30

Serial1 is up, line protocol is up

Internet address is 192.168.30.13/30

FastEthernet0/0 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 el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado

Es la interfaz serial administrable y la línea protocolo que está (Arriba)

Es la interfaz fastethernet administrable y la línea protocolo que está (Baja)

ROUTER URDESA

Router_1

- ✓ La dirección **192.168.30.14** que se conecta con el router conexión_Urdesa está levantada (**UP**)
- ✓ La dirección **192.168.30.17** que se conecta con el router 2 de Urdesa está levantada (**UP**)

Suc_Urd_1_cisco800#show protocols
Global values:

Internet Protocol routing is enabled
Serial0 is up, line protocol is up
Internet address is 192.168.30.14/30
Serial1 is up, line protocol is up
Internet address is 192.168.30.17/30

FastEthernet0/0 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 el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado

Es la interfaz serial administrable y la línea protocolo que está (Arriba)

Es la interfaz fastethernet administrable y la línea protocolo

Router_2

- ✓ La dirección **192.168.30.18** que se conecta con el router 1 de Urdesa está levantada (**UP**)

Suc_Urd_2_cisco800#show protocols
Global values:

Internet Protocol routing is enabled
Serial0 is up, line protocol is up
Internet address is 192.168.30.18/30

Serial1 is administratively down, line protocol is down
FastEthernet0/0 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 el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido

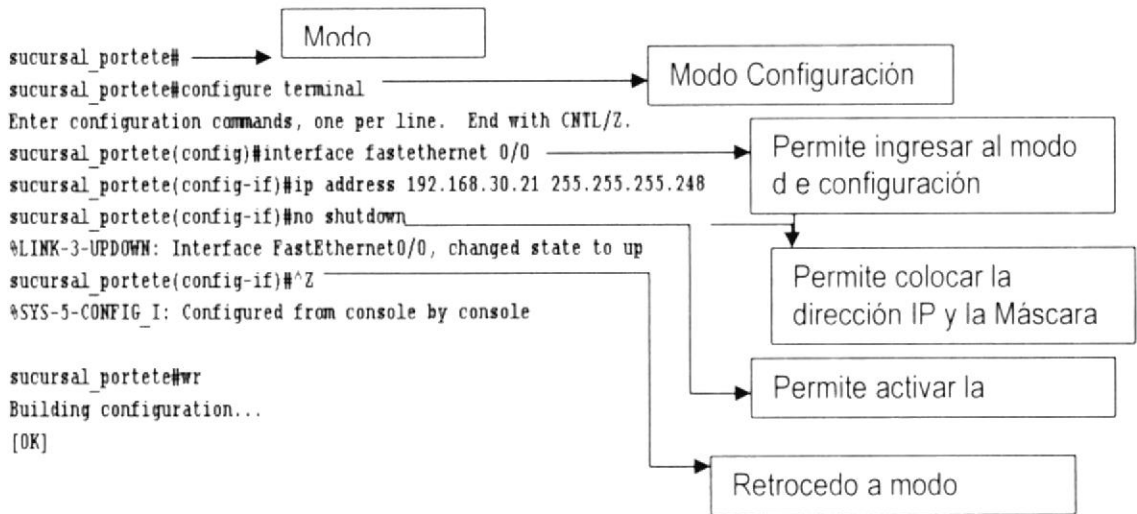
Es la interfaz serial administrable y la línea protocolo que está (Arriba)

Es la interfaz fastethernet administrable y la línea protocolo



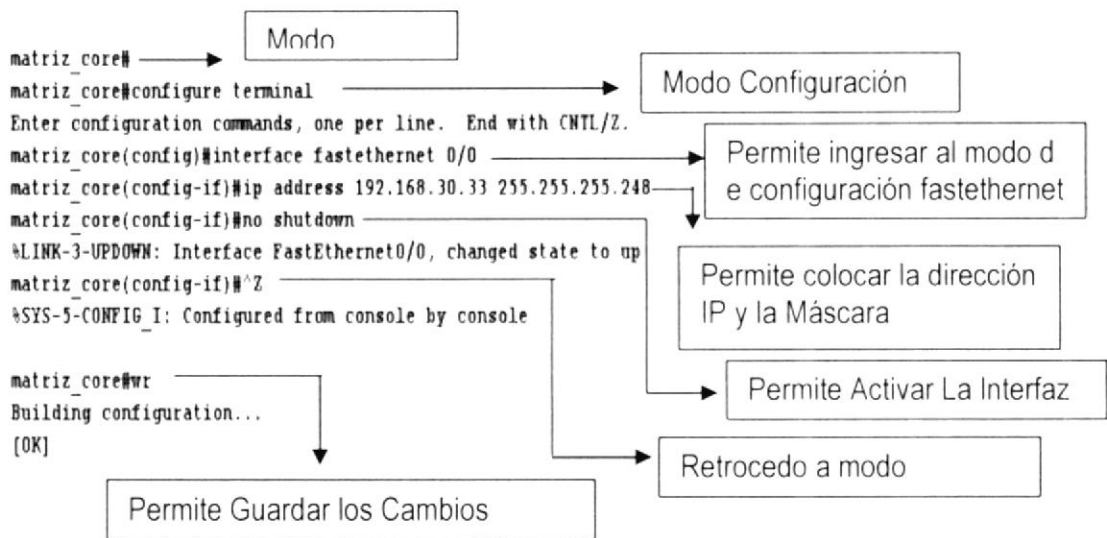
7.22.2.4. CONFIGURAR LAS FASTETHERNET

ROUTER PORTETE



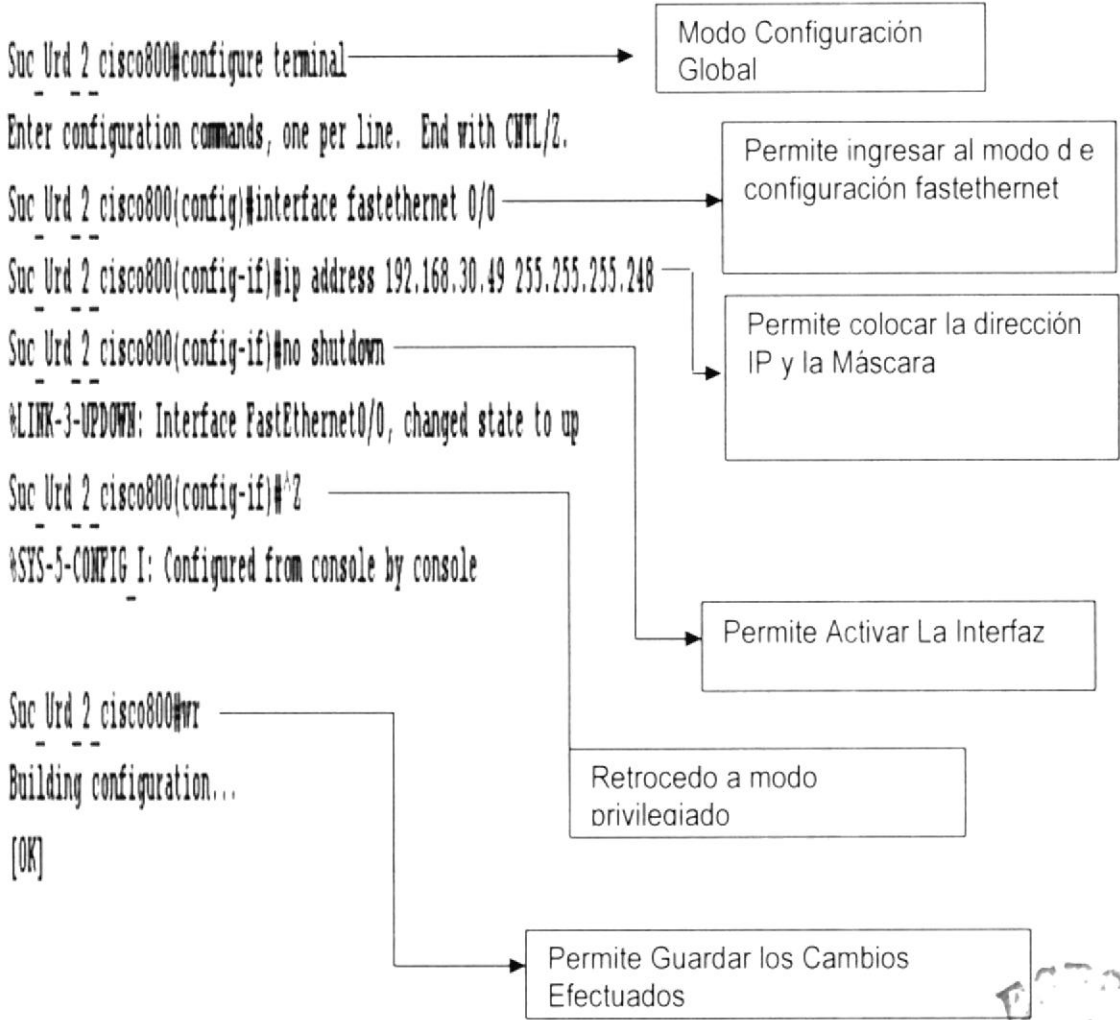
ROUTER MATRIZ

Router_matriz_core



7.22.2.5. ROUTER URDESA

Router_2



7.22.2.6. VERIFICAR SI LAS DIRECCIONES FASTETHERNET FUERON LEVANTADAS CON ÉXITO

ROUTER PORTETE

- ✓ La dirección **192.168.30.21** que pertenece a la fastethernet de portete está levantada (**UP**)

```
sucursal_portete#show protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled
```

```
Serial0 is administratively down, line protocol is down
```

```
Serial1 is up, line protocol is up
```

```
Internet address is 192.168.30.1/30
```

```
FastEthernet0/0 is up, line protocol is up
```

```
Internet address is 192.168.30.21/29
```

Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido

Es la interfaz serial administrable y la línea protocolo que está

Es la interfaz serial administrable y la línea protocolo que está

Es la interfaz fastethernet administrable y la línea protocolo

ROUTER MATRIZ

Router_matriz_core

- ✓ La dirección **192.168.30.33** que pertenece a la fastethernet de matriz_core está levantada (**UP**)

```
matriz_core#show protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled
```

```
Serial0 is up, line protocol is up
```

```
Internet address is 192.168.30.6/30
```

```
Serial1 is up, line protocol is up
```

```
Internet address is 192.168.30.9/30
```

```
FastEthernet0/0 is up, line protocol is up
```

```
Internet address is 192.168.30.33/29
```

Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido

Es la interfaz serial administrable y la línea protocolo que está

Es la interfaz fastethernet administrable y la línea protocolo que está (Arriba)

ROUTER URDESA**Router_2**

- ✓ La dirección **192.168.30.49** que pertenece a la fastethernet del router 2 de Urdesa está levantada (**UP**)

Suc_Urd_2_cisco800#show protocols

Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido

Global values:

Internet Protocol routing is enabled

Serial0 is up, line protocol is up

Es la interfaz serial administrable y la línea protocolo que está (Arriba)

Internet address is 192.168.30.18/30

Serial1 is administratively down, line protocol is down

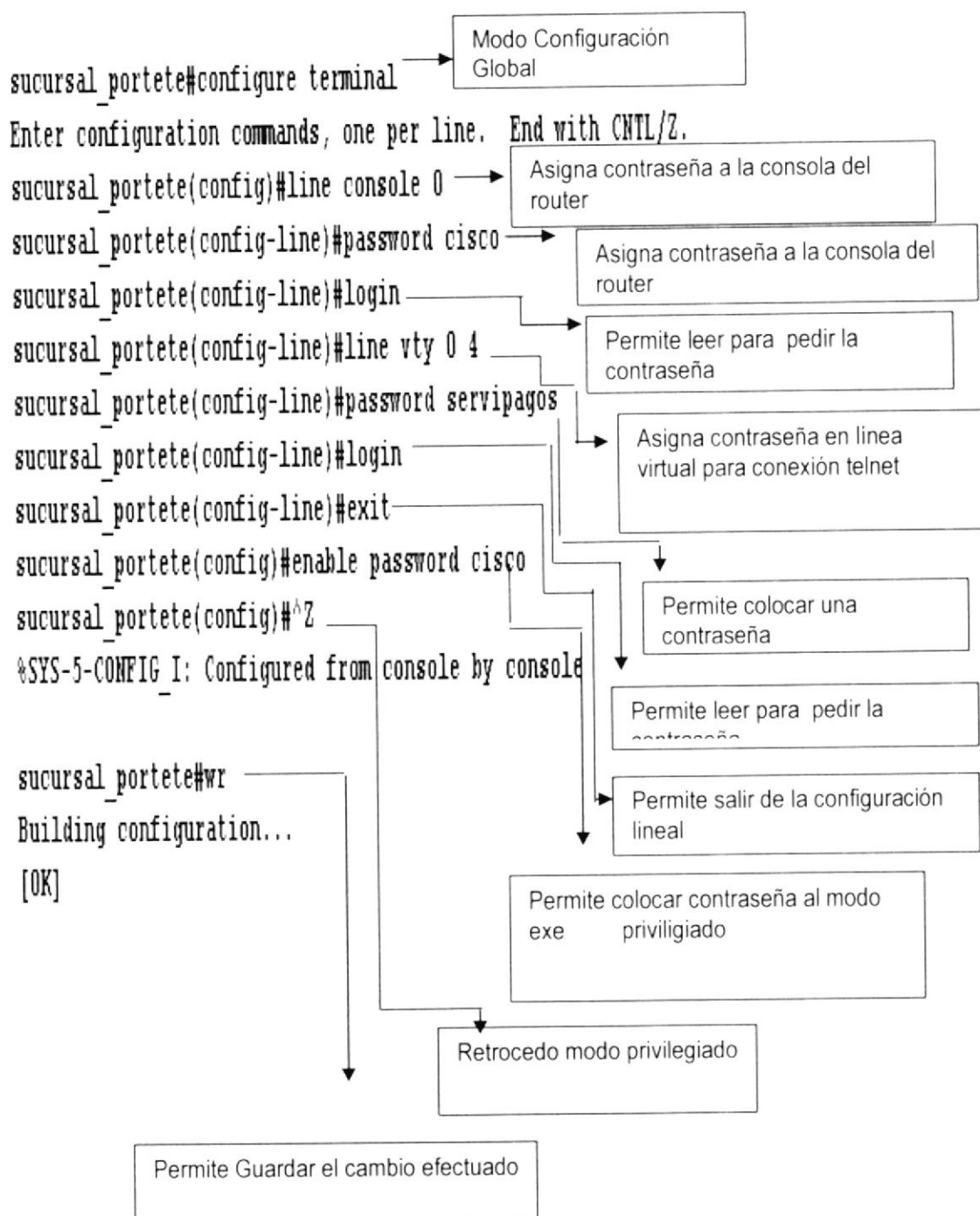
FastEthernet0/0 is up, line protocol is up

Es la interfaz fastethernet administrable y la línea protocolo

Internet address is 192.168.30.49/29

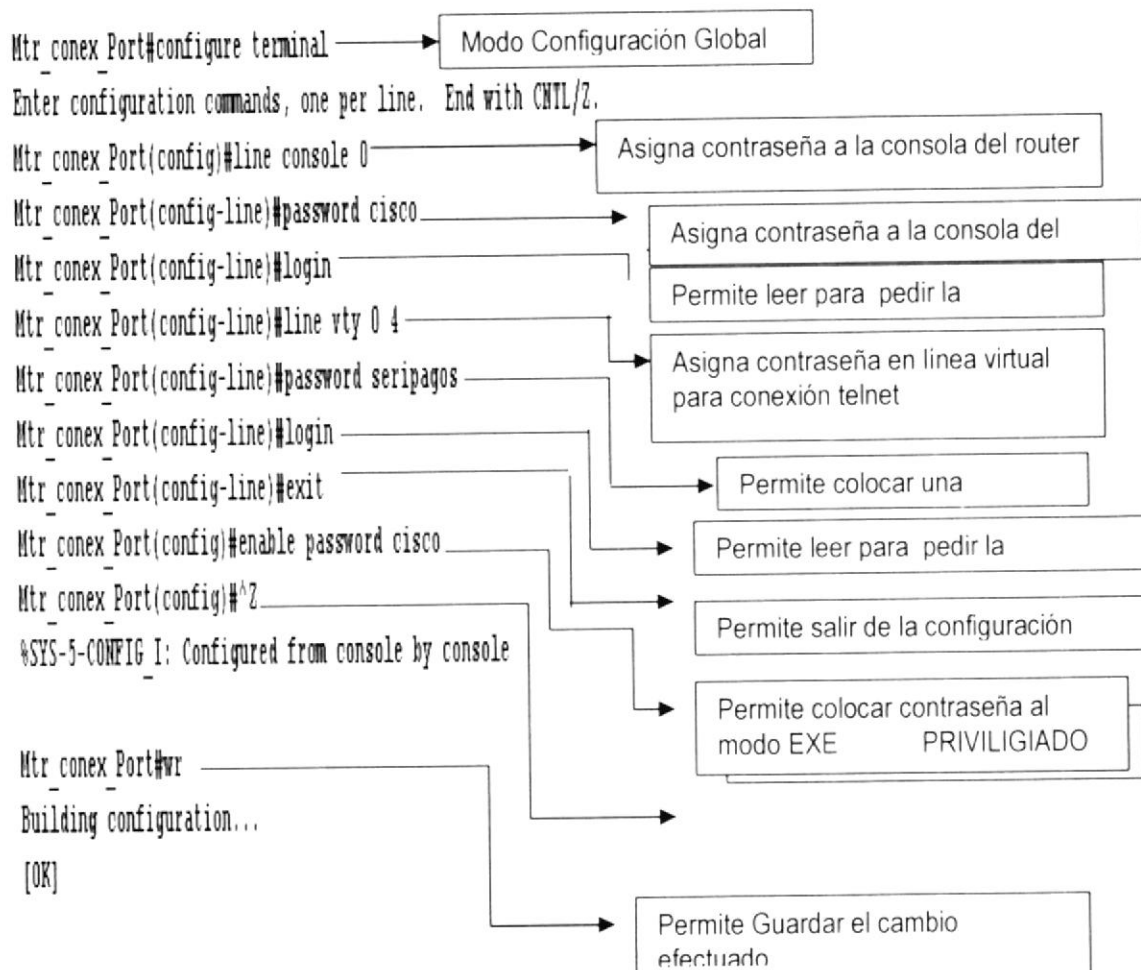
7.22.2.7. CONFIGURAR TELNET

ROUTER PORTETE

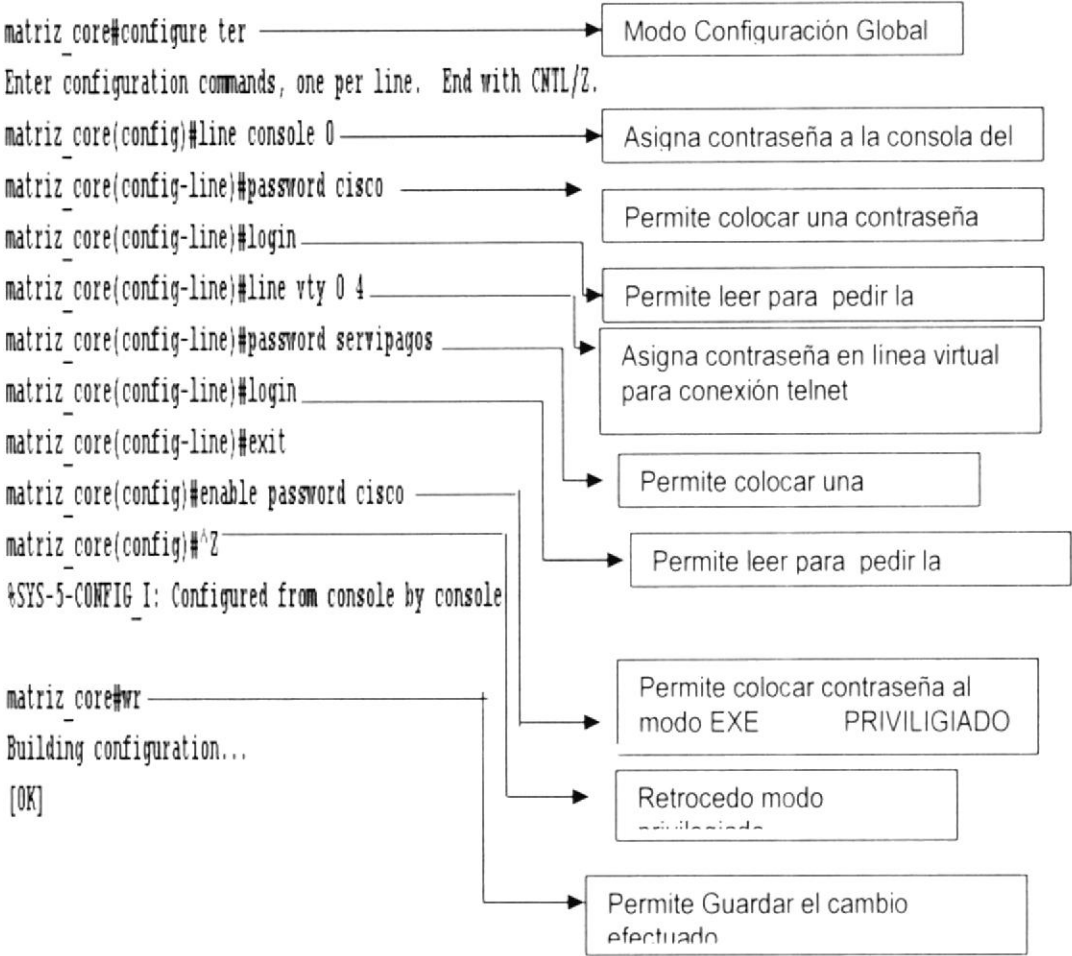


ROUTER MATRIZ

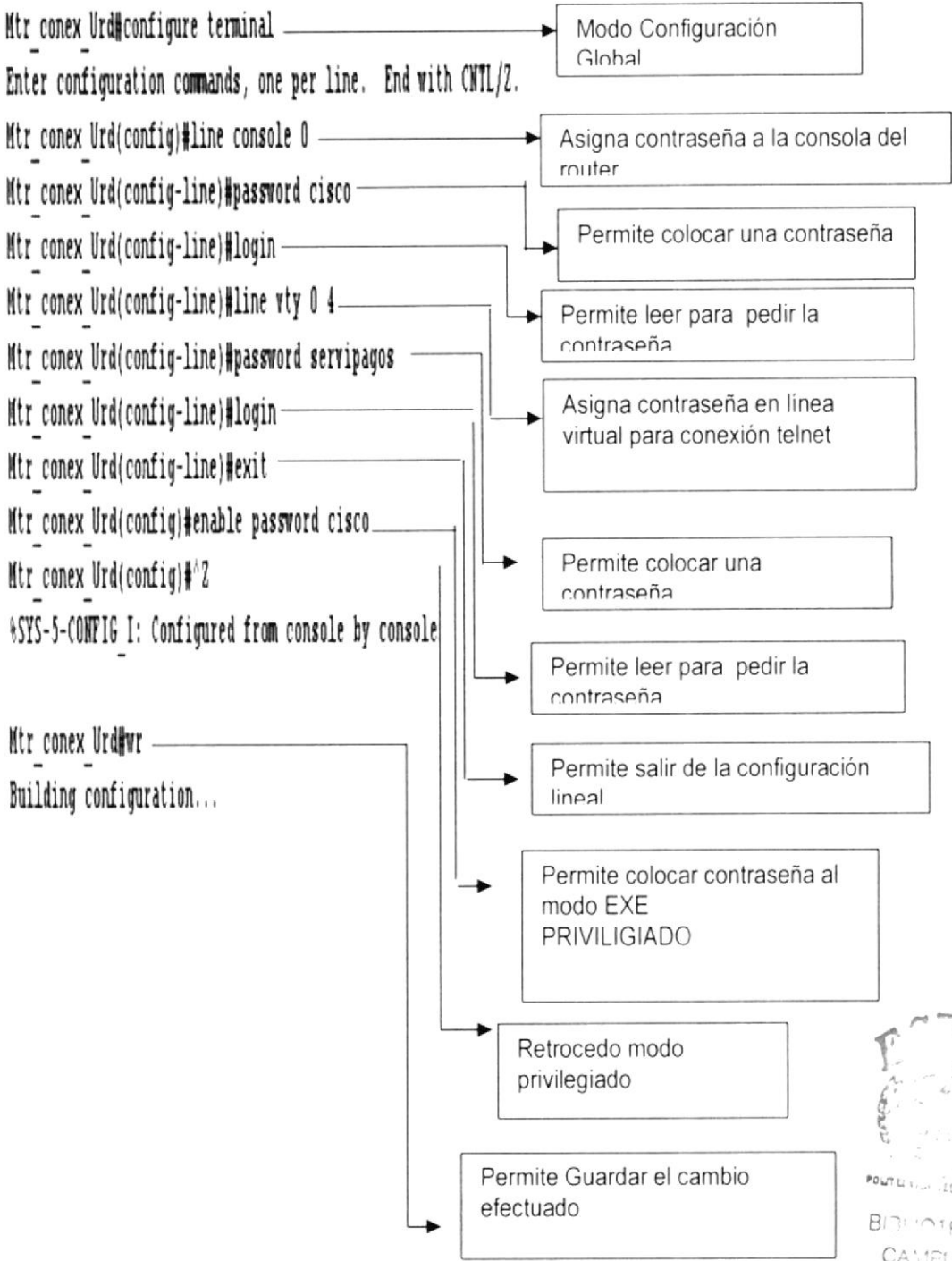
Router_conexión_Portete



Router_Core

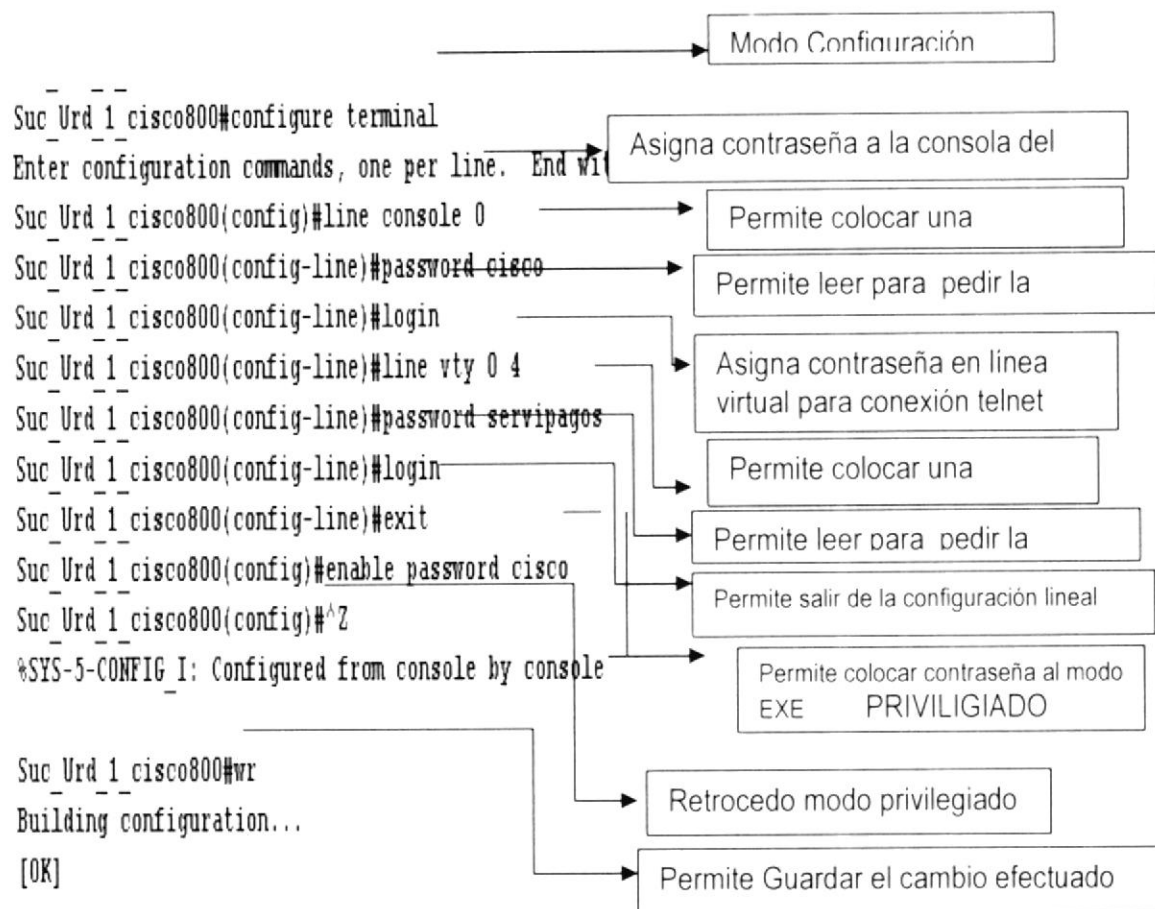


Router_ conexión_Urdesa

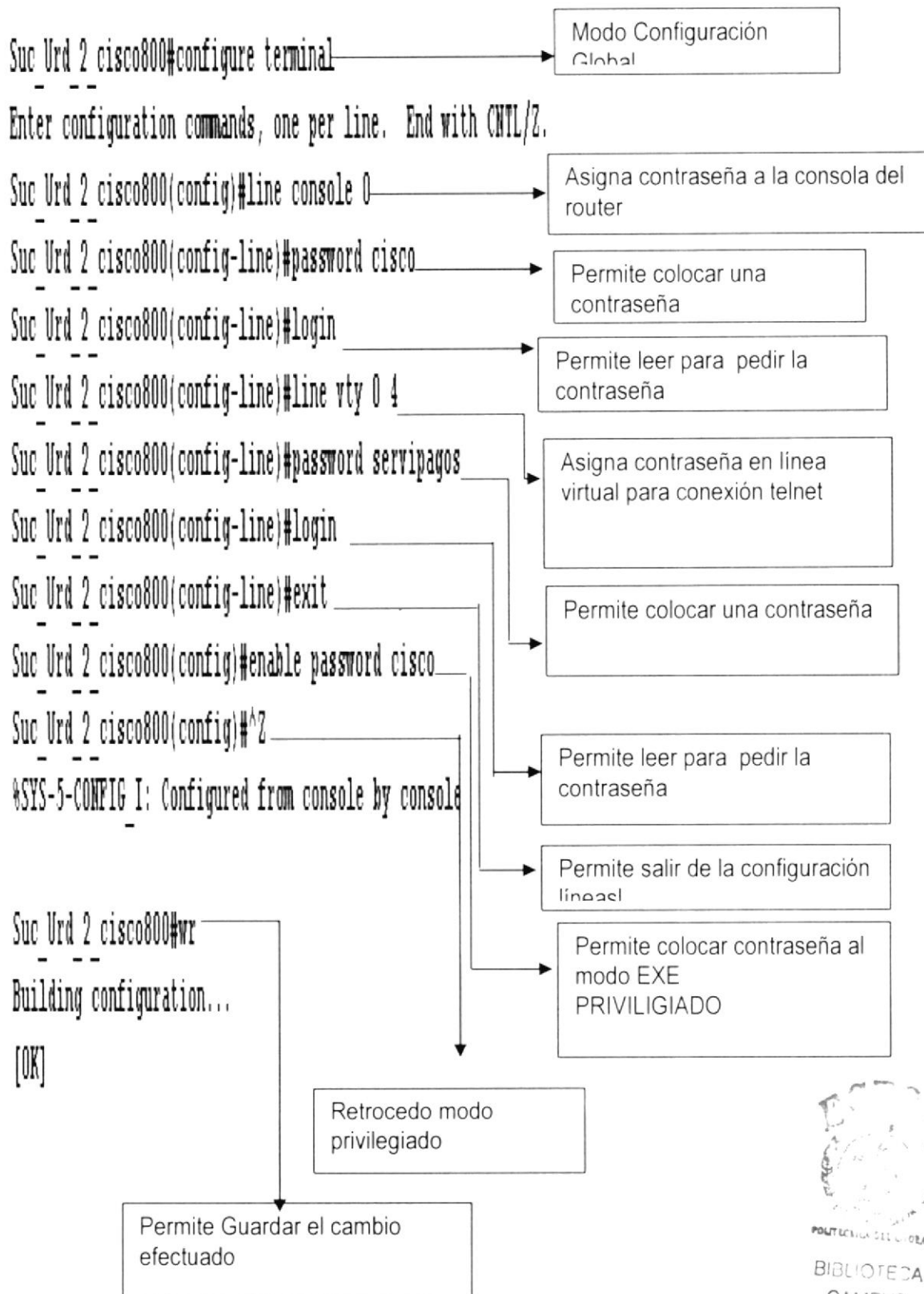


ROUTER URDESA

Router_1



Router_2



7.22.3. VERIFICACIÓN TELNET

- ✓ Estando en el router matriz **conexión_portete** se hace telnet al router **matriz_core**: en la siguiente imagen se demuestra lo efectuado.

ROUTER MATRIZ

7.22.3.1. ROUTER_ CONEXIÓN _PORTETE

```
Mtr_conex_Port#telnet 192.168.30.6 ← 1

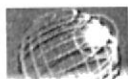
matriz_core>enable ← 2
Enter password:
matriz_core#show protocols ← 3
Global values:
  Internet Protocol routing is enabled
  Serial0 is up, line protocol is up
    Internet address is 192.168.30.6/30
  Serial1 is up, line protocol is up
    Internet address is 192.168.30.9/30
  FastEthernet0/0 is up, line protocol is up
    Internet address is 192.168.30.33/29
  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

matriz_core#exit ← 4
[Connection to 192.168.30.6 closed by foreign host]

Mtr_conex_Port#|
```

1. Hacer **TELNET** desde el router conexión portete hacia el router core de la matriz.
2. Una vez hecho **TELNET** pedirá la contraseña para poder acceder al otro ruteador
3. Ya hecho telnet y puesto la contraseña se está dentro del otro ruteador estando físicamente en otro para verificar si en realidad se está en el otro ruteador colocar el comando **show protocols** para ver las direcciones del dispositivo.
4. Cuando se quiera salir del **TELNET** únicamente hay que escribir **EXIT** y automáticamente se regresa al router donde se hizo telnet

7.22.4. CONFIGURACIÓN DE LOS PROTOCOLOS ENRUTAMIENTO



NOTA: los protocolos enrutamiento están ligado a nivel **WAN** manejan varios tipos de protocolos que son:

- ❖ Rip V.1
- ❖ Rip V.2
- ❖ Ospf
- ❖ Igrp
- ❖ Eigrp

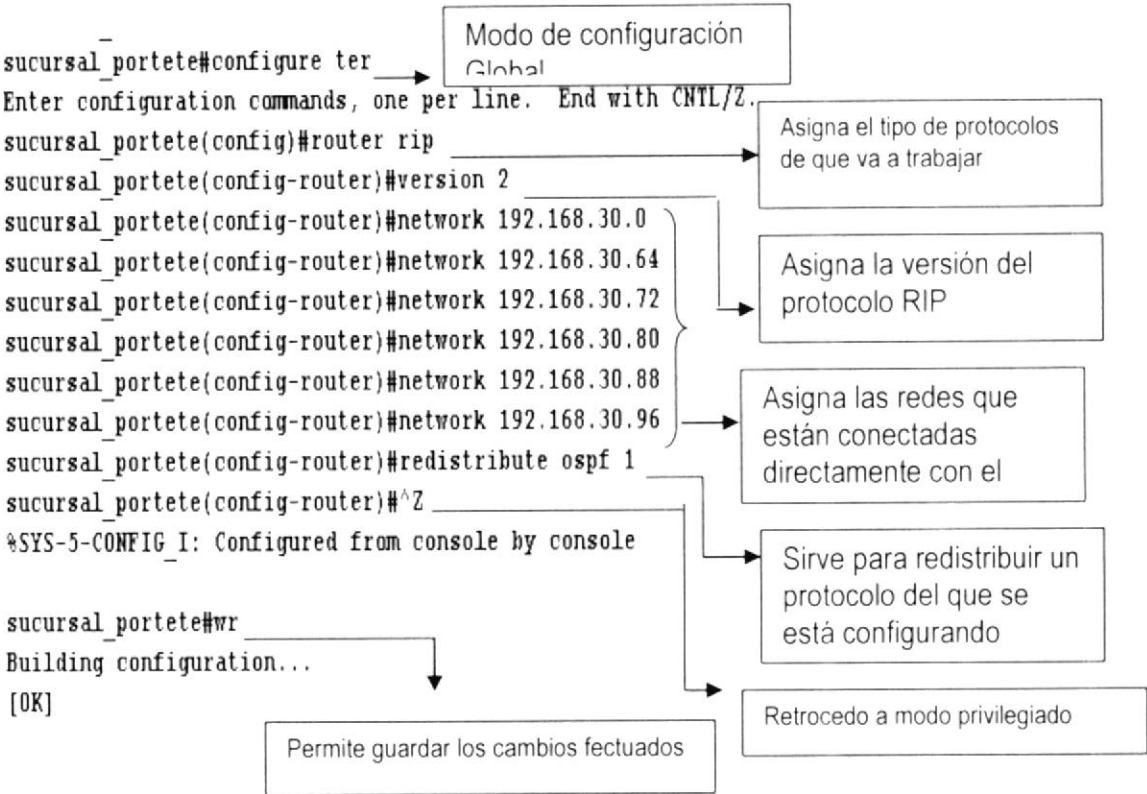


7.22.4.1. ROUTER PORTETE



NOTA: El router de Portete es protocolo **Rip V.2**

7.22.4.1.1. PROTOCOLO RIP



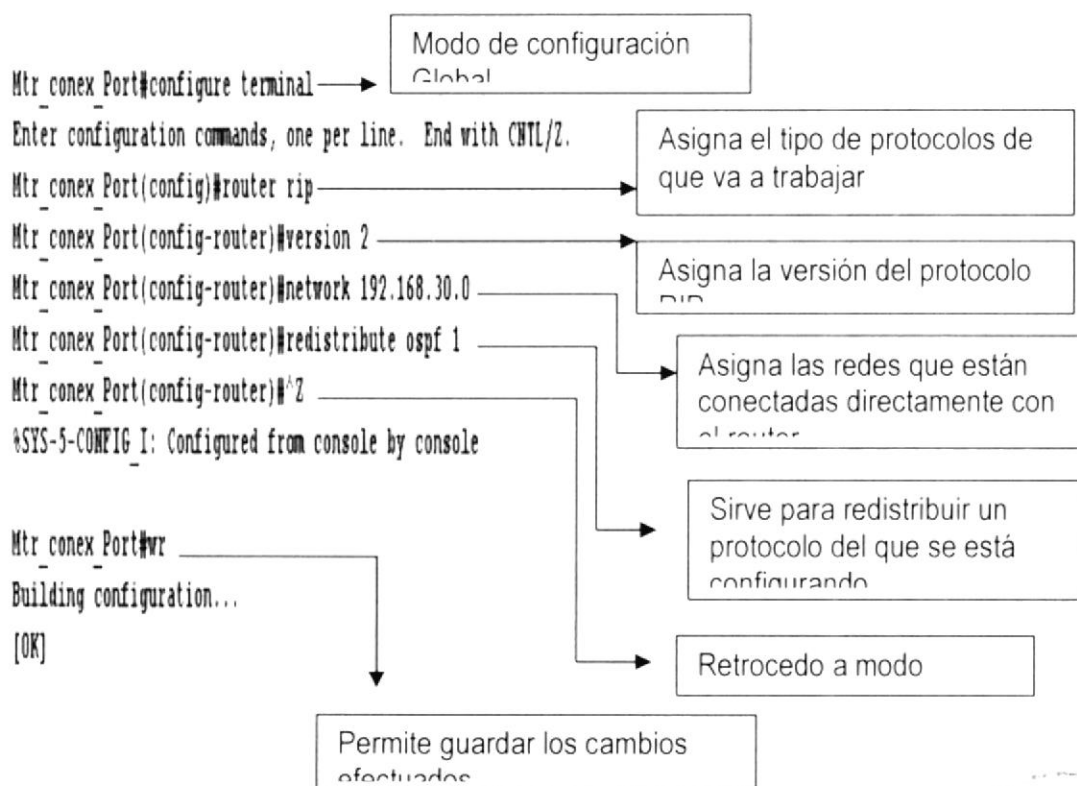
7.22.4.2. ROUTER MATRIZ



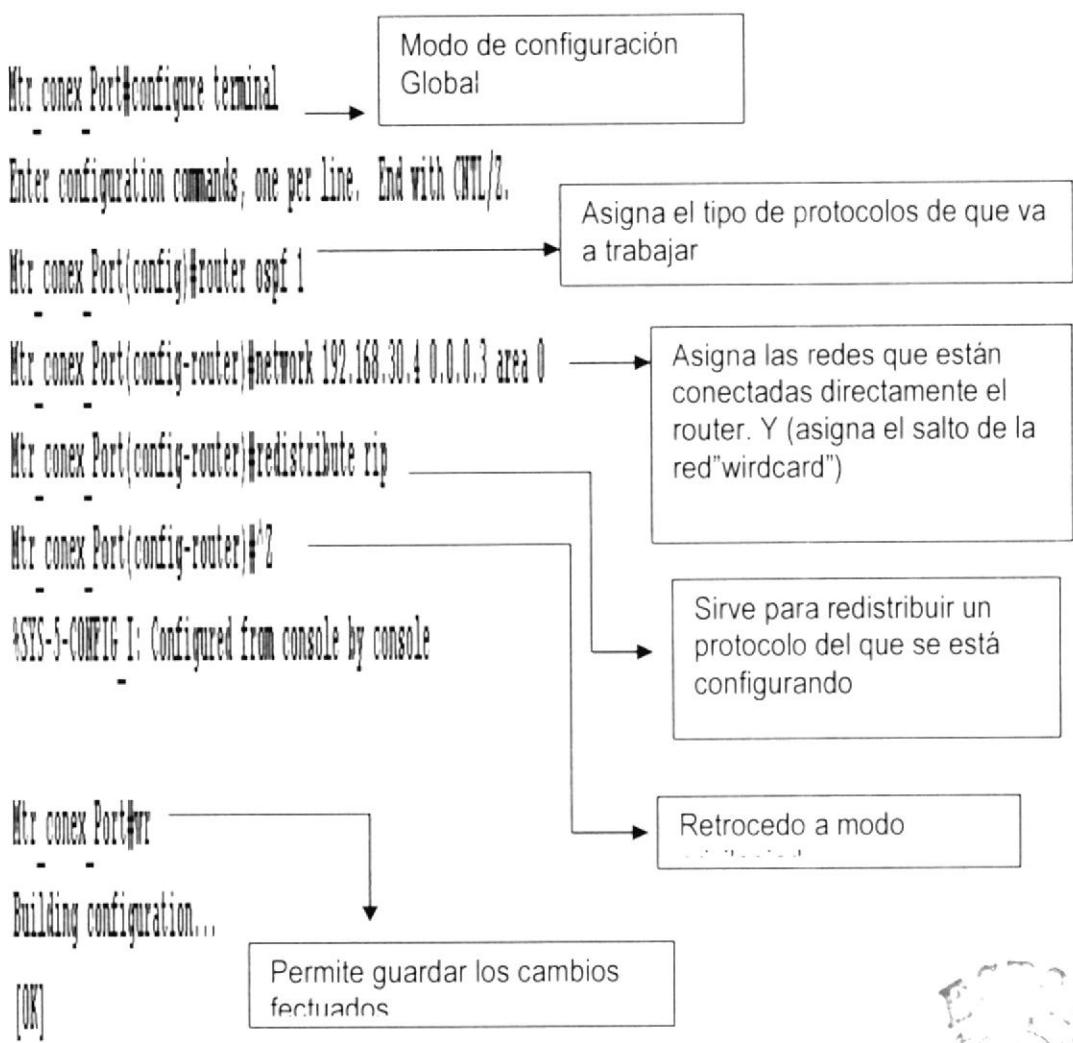
NOTA: Los routers conexión con sucursales con routers de fronteras por lo tanto en este router se aplican los dos protocolos **RIP** y **OSPF** para que puedan pasar los datos de un protocolo a otro sin problemas.

7.22.4.2.1. ROUTER_CONEXIÓN_PORTETE

7.22.4.2.1.1. PROTOCOLO RIP



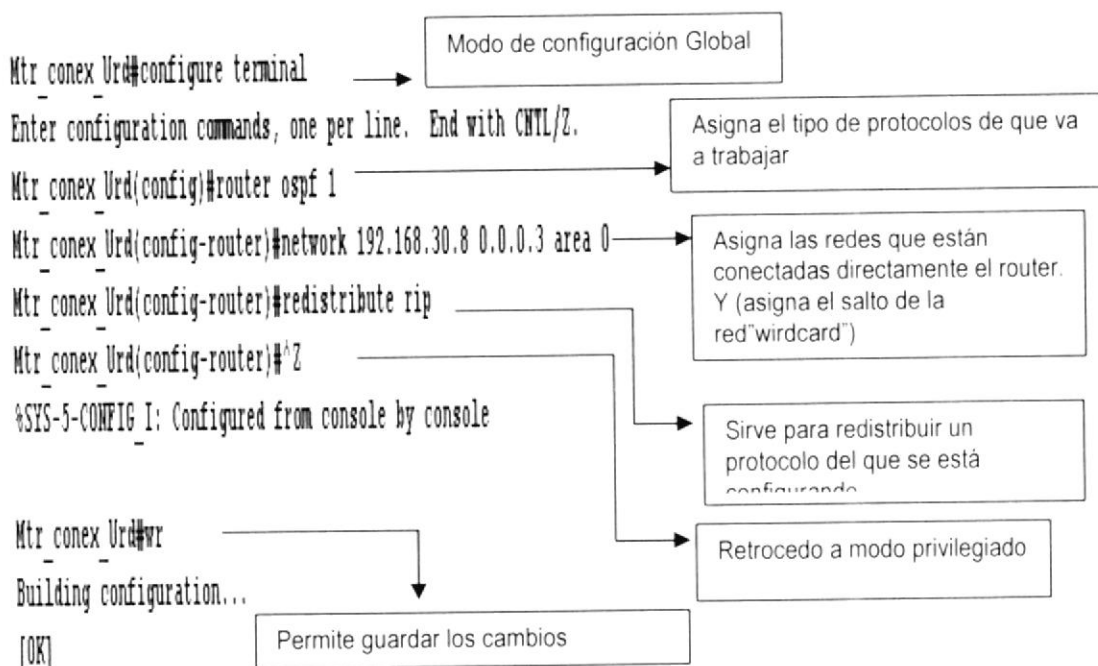
7.22.4.2.1.2. PROTOCOLO OSPF



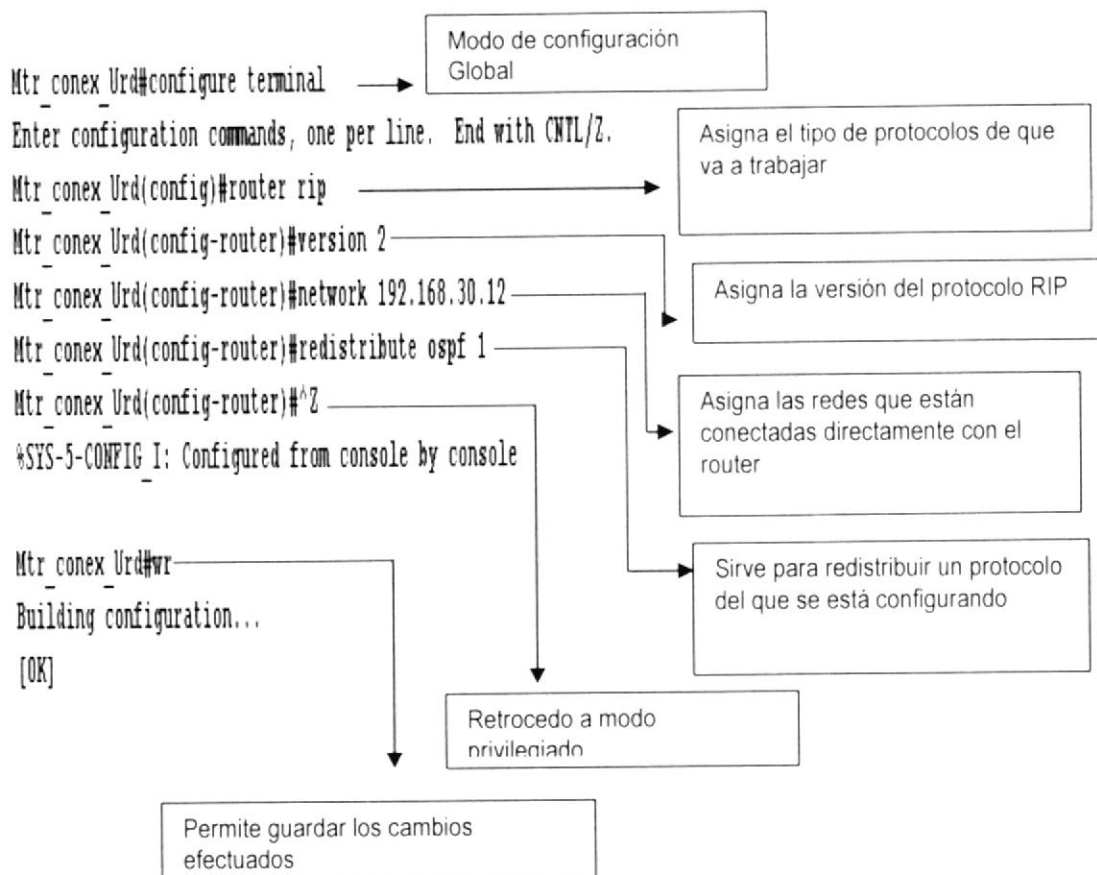
BIBLIOTECA
CAMPUS
PEÑAS

7.22.4.2.2. ROUTER_CONEXIÓN_URDESA

7.22.4.2.2.1. PROTOCOLO OSPF



7.22.4.2.2.2. PROTOCOLO RIP



7.22.4.2.2.3. ROUTER_CORE



NOTA: El router **CORE** es el router principal donde permite pasar los datos de un extremo a otro, el core vendría hacer un puente de comunicaciones donde pasan los datos de un extremo a otro; en este router está configurado el protocolo **OSPF** que se comunica con los routers de fronteras.

7.22.4.2.2.4. PROTOCOLO OSPF

```
matriz_core#configure terminal
Enter configuration commands, one per line. End with CWT/?.

matriz_core(config)#router ospf 1

matriz_core(config-router)#network 192.168.30.4 0.0.0.3 area 0
matriz_core(config-router)#network 192.168.30.8 0.0.0.3 area 0
matriz_core(config-router)#^Z
^SYS-5-COUP1G I: Configured from console by console

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

Modo de configuración Global

Asigna el tipo de protocolos de que va a trabajar

Asigna las redes que están conectadas directamente el router. Y (asigna el salto de la red "wildcard")

Retrocedo a modo privilegiado

Permite guardar los cambios efectuados

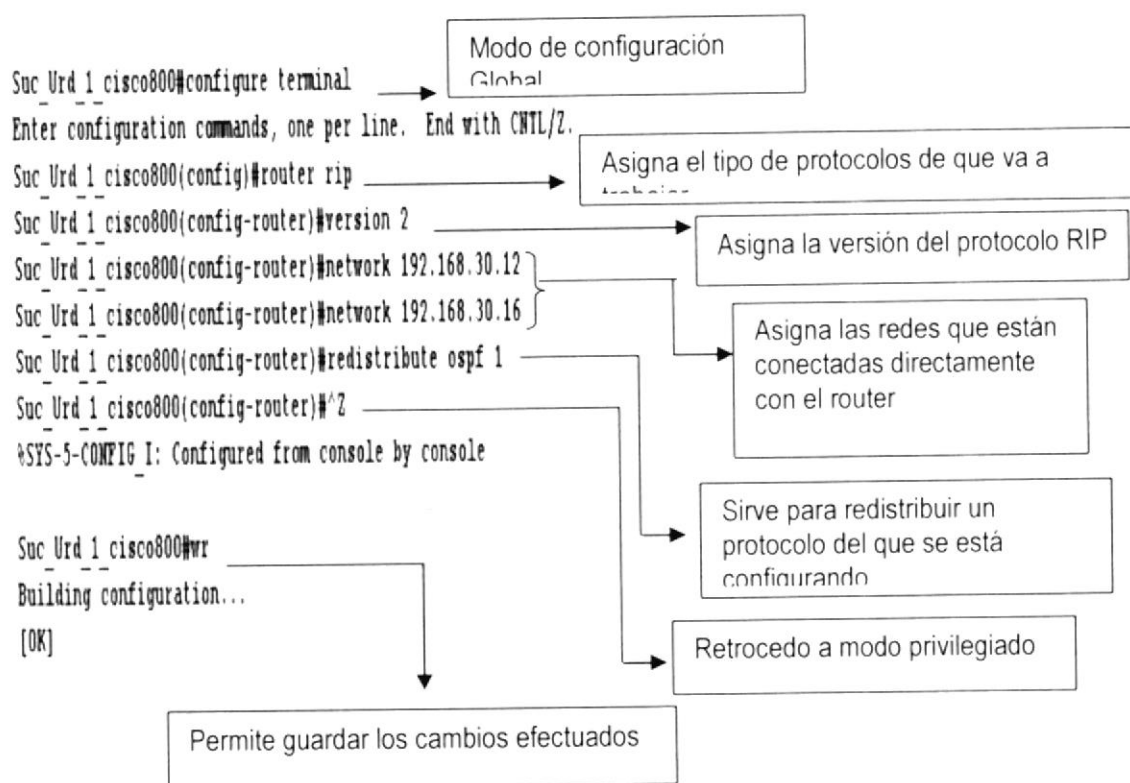
7.22.4.3. ROUTER URDESA



NOTA: Los routers de Urdesa van hacer protocolo **Rip V.2**

7.22.4.3.1. ROUTER_1

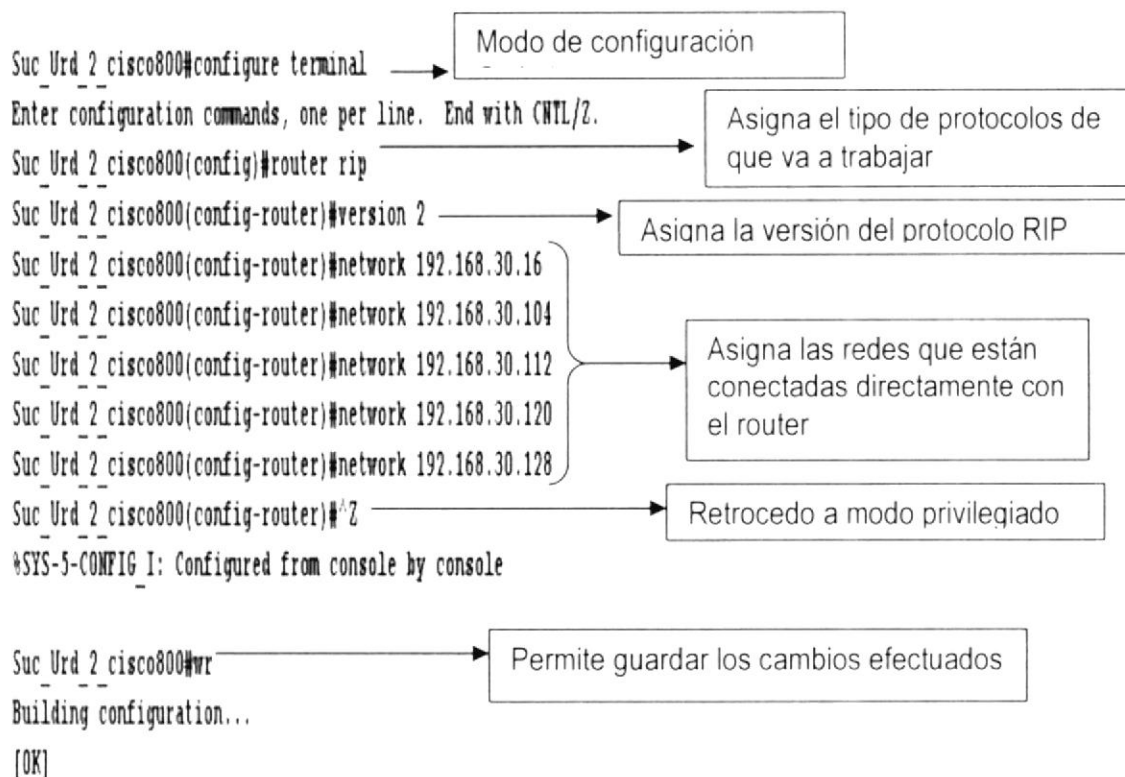
7.22.4.3.1.1. PROTOCOLO RIP



BIBLIOTECA
CAMPUS
PEÑAS

7.22.4.3.2. ROUTER_2

7.22.4.3.2.1. PROTOCOLO RIP



7.22.5. SHOW IP ROUTER



NOTA: SHOW IP ROUTER Permite ver la tabla de ruteo donde se indicará los protocolos levantados pueden ser: **C** (conectadas); **O** (ospf); **R** (rip) **y** entre otros.

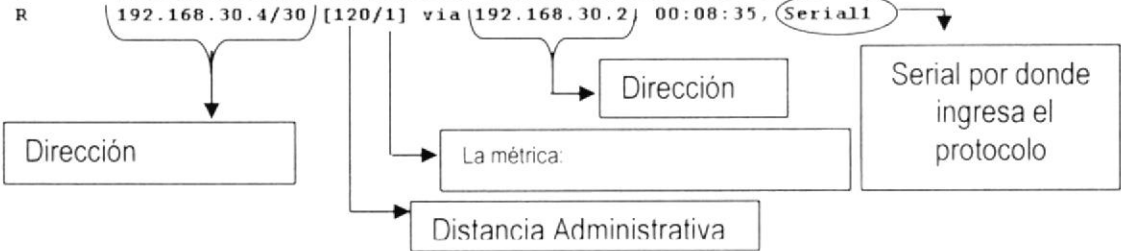
7.22.5.1. ROUTER PORTETE

- ✓ El router Portete aprendió la red **192.168.30.4** como rip, ya que esa red le pertenece al serial 1 del router conexión_portete.

```
sucursal_portete#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
```

```
192.168.30.0/0 is variably subnetted, 8 subnets
C    192.168.30.0/30 is directly connected, Serial1
C    192.168.30.64/29 is directly connected, 192.168.30.65
C    192.168.30.72/29 is directly connected, 192.168.30.73
C    192.168.30.80/29 is directly connected, 192.168.30.81
C    192.168.30.88/29 is directly connected, 192.168.30.89
C    192.168.30.96/29 is directly connected, 192.168.30.97
C    192.168.30.16/29 is directly connected, FastEthernet0/0
R    192.168.30.4/30 [120/1] via 192.168.30.2, 00:08:35, Serial1
```



NOTA: LA MÉTRICA se trata como alcanza una red en particular Distancia Administrativa es la confiabilidad de una ruta

SÍMBOLO	DETALLE
C	Directamente conectado con el router
R	Protocolo de enrutamiento RIP

Tabla7-6 significado 1 de C - R



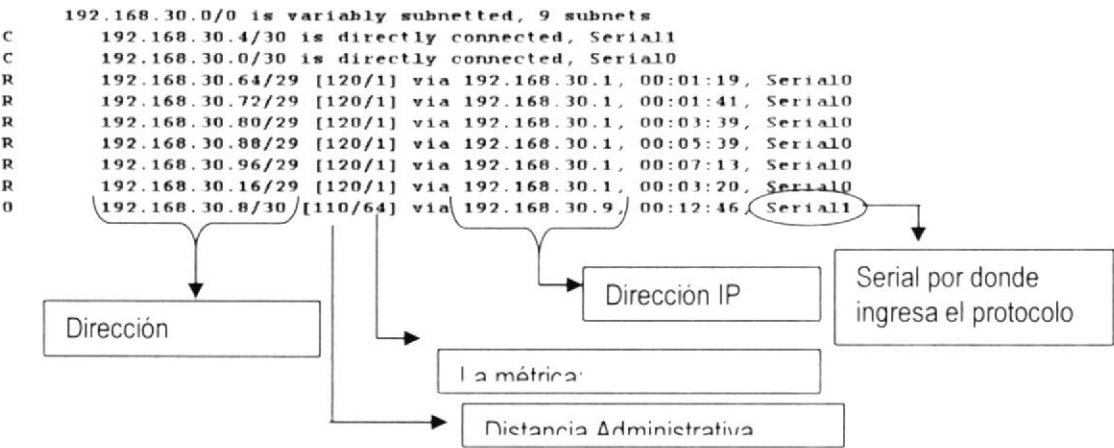
7.22.5.2. ROUTER MATRIZ

7.22.5.2.1. ROUTER_ CONEXIÓN _PORTETE

- ✓ El router conexión portete aprendió como rip las siguientes redes:
- 192.168.30.64
 - 192.168.30.72
 - 192.168.30.80
 - 192.168.30.88
 - 192.168.30.96
 - 192.168.30.16
- Ya que estas redes le pertenecen a las Vlans de las sucursal portete:
- ✓ El router conexión portete aprendió la red **192.168.30.8** como ospf, ya que esa red le pertenece al serial 1 del router Core de la misma matriz

```
Mtr_conex_Port#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
```



NOTA: LA MÉTRICA se trata como alcanza una red en particular
Distancia Administrativa es la confiabilidad de una ruta

SÍMBOLO	DETALLE
C	Directamente conectado con el router
R	Protocolo de enrutamiento RIP
O	Protocolo de enrutamiento OSPF

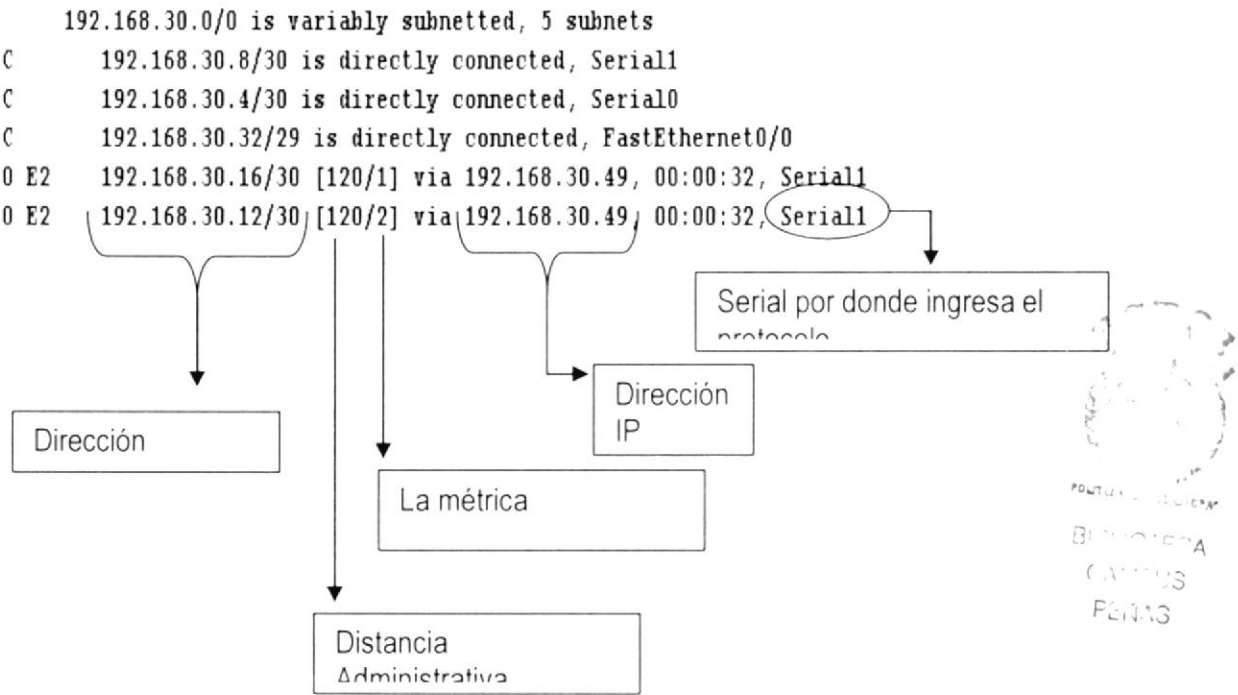
Tabla 7-7: significado 2 de C – R O

7.22.5.2.2. ROUTER_CORE

- ✓ El router core aprendió la red **192.168.30.16 y 192.168.30.12** como ospf, ya que la red **30.16** le pertenece al serial 1 del router 2 de la sucursal urdesa. Y a la red **30.12** le pertenece al serial 1 de router conexión urdesa de la misma matriz.

```
matriz_core#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
```



NOTA: LA MÉTRICA se trata como alcanza una red en particular Distancia Administrativa es la confiabilidad de una ruta

SÍMBOLO	DETALLE
C	Directamente conectado con el router
R	Protocolo de enrutamiento RIP
OE2	Protocolo de enrutamiento OSPF extendida

Tabla 7-8: significado 3 de C – R OE2

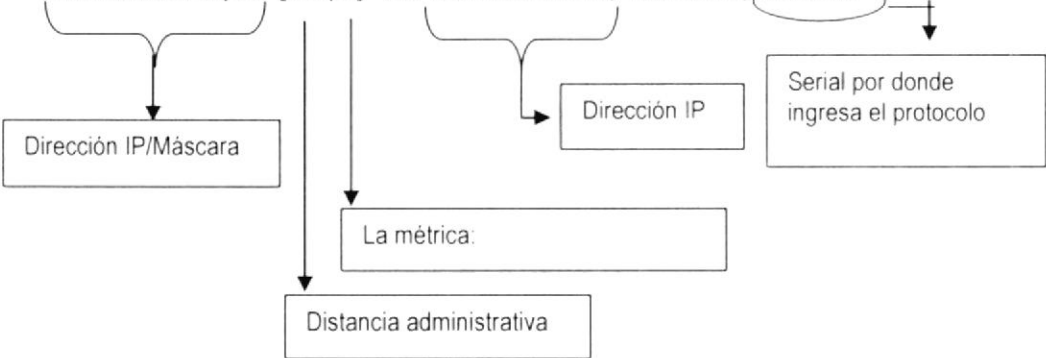
7.22.5.2.3. ROUTER_ CONEXIÓN_ URDESA

- ✓ El router conexión urdesa aprendió la red **192.168.30.16** y **192.168.30.48** como rip, ya que la red **30.16** le pertenece a la serial 1 del router 2 de urdesa y a la red **30.48** le pertenece a la fastethernet del router 2 de la sucursal urdesa .
- ✓ El router conexión urdesa aprendió la red **192.168.30.4** como ospf, ya que esa red le pertenece a la serial 1 del router conexión portete.

```
Mtr_conex_Urd#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

```
192.168.30.0/0 is variably subnetted, 5 subnets
C    192.168.30.8/30 is directly connected, Serial0
C    192.168.30.12/30 is directly connected, Serial1
O    192.168.30.4/30 [110/128] via 192.168.30.9, 00:11:23, Serial1
R    192.168.30.16/30 [120/1] via 192.168.30.14, 00:03:33, Serial1
R    192.168.30.48/29 [120/2] via 192.168.30.14, 00:09:22, Serial1
```



NOTA: LA MÉTRICA se trata como alcanza una red en particular Distancia Administrativa es la confiabilidad de una ruta

SÍMBOLO	DETALLE
C	Directamente conectado con el router
R	Protocolo de enrutamiento RIP
O	Protocolo de enrutamiento OSPF

Tabla 7-9: significado 4 de C – R-O

7.22.5.3. ROUTER URDESA

7.22.5.3.1. ROUTER_1

- ✓ El router uno de la sucursal urdesa aprendió la red **192.168.30.8** y **192.168.30.48** como rip, ya que a la red **30.8** le pertenece a la serial 0 del router core y a la red **30.48** le pertenece a la fastethernet del router dos de la misma sucursal

```
Suc_Urd_1_cisco800#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

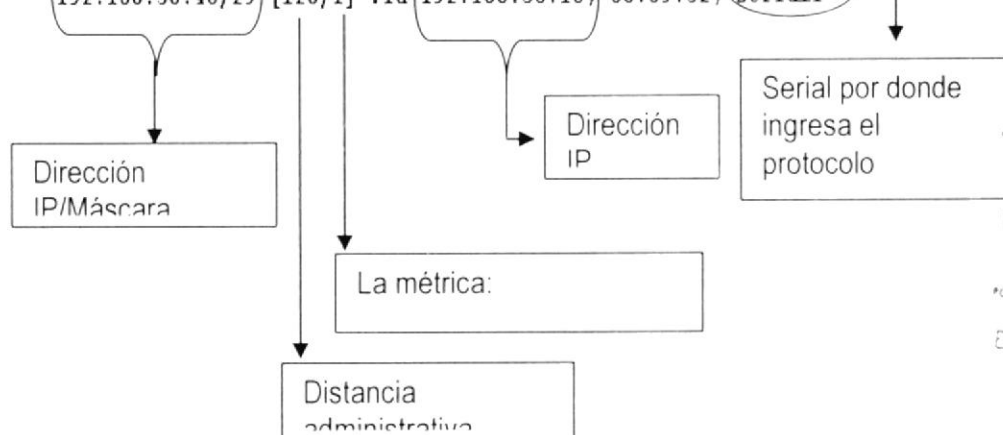
192.168.30.0/0 is variably subnetted, 4 subnets

C 192.168.30.12/30 is directly connected, Serial0

C 192.168.30.16/30 is directly connected, Serial1

R 192.168.30.8/30 [120/1] via 192.168.30.13, 00:09:17, Serial0

R 192.168.30.48/29 [120/1] via 192.168.30.18, 00:09:32, Serial1



NOTA: LA MÉTRICA se trata como alcanza una red en particular
Distancia Administrativa es la confiabilidad de una ruta

SÍMBOLO	DETALLE
C	Directamente conectado con el router
R	Protocolo de enrutamiento RIP

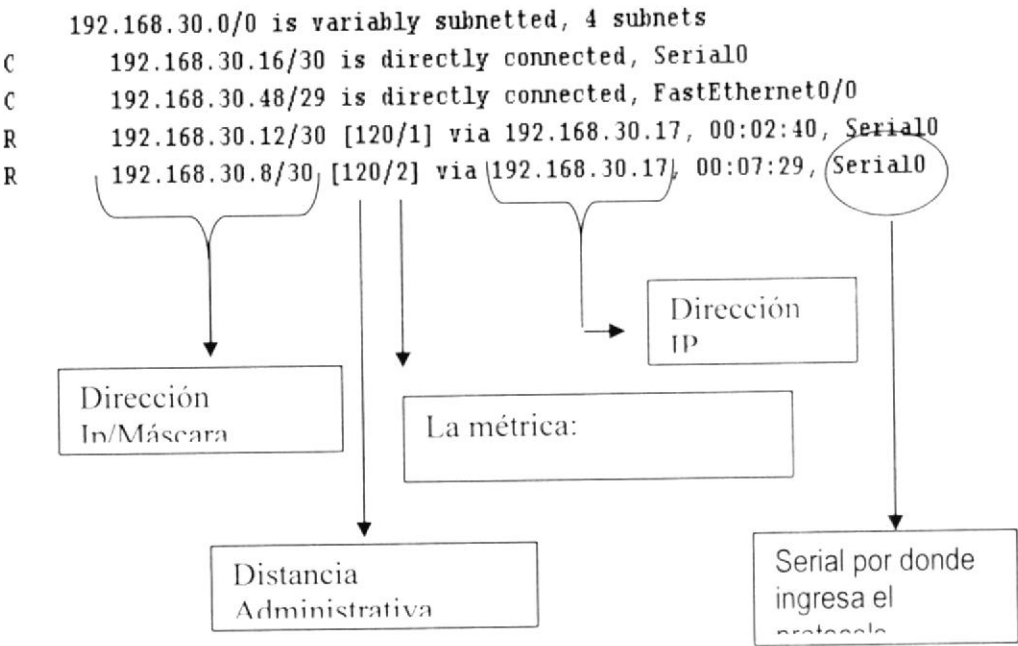
Tabla 7-10: significado 5 de C - R

7.22.5.3.2. ROUTER_2

- ✓ El router dos de la sucursal urdesa aprendió la red **192.168.30.12** y **192.168.30.8** como rip, ya que la red **30.12** le pertenece a la serial 0 del router uno de la misma sucursal. Y a la red **30.8** le pertenece a la serial 0 del router core.

```
Suc_Urd_2_cisco800#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



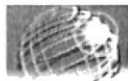
NOTA: LA MÉTRICA se trata como alcanza una red en particular
Distancia Administrativa es la confiabilidad de una ruta

SÍMBOLO	DETALLE
C	Directamente conectado con el router
R	Protocolo de enrutamiento RIP

Tabla 7-11: significado 6 de C - R



7.22.6. PRUEBAS COMUNICACIÓN ENTRE SUCURSALES Y MATRIZ



NOTA: Una vez realizado las configuraciones de los protocolos de enrutamientos comenzarán las pruebas de ping, con la finalidad de saber si los dispositivos se comunican el uno con el otro.

7.22.6.1. ROUTER PORTETE

- ✓ El router portete hace ping a su propio fastethernet para ver si tiene conexión entre ellos mismo.

```
sucursal_portete#ping 192.168.30.21
```

Prueba conectividad a una dirección IP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.21, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Respuesta ping

- ✓ El router portete hace ping a la IP que sale de la serial 1 de su propio router

```
sucursal_portete#ping 192.168.30.1
```

Prueba conectividad a una dirección IP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Respuesta

- ✓ El router portete hace ping a la IP del router conexión portete que llega mediante la serial 0.

```
sucursal_portete#ping 192.168.30.2
```

Prueba conectividad a una dirección IP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Respuesta



7.22.6.1.1. ROUTER MATRIZ

7.22.6.1.1.1. ROUTER_CONEXIÓN_PORTETE

- ✓ El router conexión portete hace ping a su propia serial 0 y serial 1 para ver si tiene conexión entre el mismo

Serial 0

```
Mtr_conex_Port#ping 192.168.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Prueba conectividad a una dirección IP

Respuesta

Serial 1

```
Mtr_conex_Port#ping 192.168.30.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Prueba conectividad a una dirección IP

Respuesta ning

- ✓ El router conexión portete hace ping a la IP del router sucursal portete que llega hacia la serial 1

```
Mtr_conex_Port#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Prueba conectividad a una dirección IP

Respuesta ning



El router conexión portete hace ping a la IP del router core de su propia matriz que llega hacia la serial 0

```
Mtr_conex_Port#ping 192.168.30.6
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.6, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta nina

7.22.6.1.1.2. ROUTER_CORE

- ✓ El router core hace ping a su propia serial 0 y serial 1 para ver si tiene conexión entre el mismo

Serial 0

```
matriz_core#ping 192.168.30.6
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.6, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta

Serial 1

```
matriz_core#ping 192.168.30.9
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.9, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta



El router core de la matriz hace ping a la IP del router conexión portete que llega hacia la serial 1

```
matriz_core#ping 192.168.30.5
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.30.5, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta

- ✓ El router core de la matriz hace ping a la IP del router conexión urdesa que llega hacia la serial 0

```
matriz_core#ping 192.168.30.10
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.30.10, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta



7.22.6.1.1.3. ROUTER_CONEXIÓN_URDESA

- ✓ El router conexión urdesa hace ping a su propia serial 0 y serial 1 para ver si tiene conexión entre el mismo

Serial 0

Mtr_conex_Urd#ping 192.168.30.10

Prueba conectividad a una dirección IP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.10, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Respuesta

Serial 1

Mtr_conex_Urd#ping 192.168.30.13

Prueba conectividad a una dirección IP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.13, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Respuesta ping

- ✓ El router conexión urdesa de la matriz hace ping a la IP del router core de la misma matriz que llega hacia la serial 1

Mtr_conex_Urd#ping 192.168.30.9

Prueba conectividad a una dirección IP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.9, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Respuesta

- ✓ El router conexión urdesa de la matriz hace ping a la IP del router uno de la sucursal urdesa que llega hacia la serial 0

Mtr_conex_Urd#ping 192.168.30.14

Prueba conectividad a una dirección IP

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.14, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Respuesta ping

7.22.6.2. ROUTER URDESA

7.22.6.2.1. ROUTER_1

- ✓ El router uno de la sucursal urdesa hace ping a su propia serial 0 y serial 1 para ver si tiene conexión entre el mismo

Serial 0

```
Suc_Urd_1_cisco800#ping 192.168.30.14
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.14, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta

Serial 1

```
Suc_Urd_1_cisco800#ping 192.168.30.17
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.17, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta

- ✓ El router uno de la sucursal urdesa hace ping a la IP del router conexión urdesa que llega hacia la serial 1

```
Suc_Urd_1_cisco800#ping 192.168.30.13
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.13, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta



- ✓ El router uno de la sucursal urdesa hace ping a la IP del router dos de la misma sucursal urdesa que llega hacia la serial 0

```
Suc_Urd_1_cisco800#ping 192.168.30.18
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.30.18, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta

7.22.6.2.2. ROUTER_2

- ✓ El router dos de la sucursal urdesa hace ping a su propia serial 0 y fastethernet para ver si tiene conexión entre el mismo

Serial 0

```
Suc_Urd_2_cisco800#ping 192.168.30.18
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.30.18, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta

Fastethernet

```
Suc_Urd_2_cisco800#ping 192.168.30.49
```

Prueba conectividad a una dirección IP

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.30.49, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Respuesta



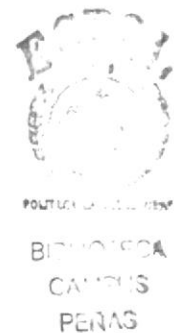
- ✓ El router dos de la sucursal urdesa hace ping a la IP del router uno de la misma sucursal urdesa que llega hacia la serial 0

```
Suc_Urd_2_cisco800#ping 192.168.30.17
```

→ Prueba conectividad a una dirección IP

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.17, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

→ Respuesta



7.22.6.3. CONFIGURACIÓN DE LAS VLANS



NOTA: para comenzar a configurar las vlans primeramente se tiene que subnetear bien ya que aquí se tiene que sacar las subinterfaces, por lo tanto cada subinterfaz vendría hacer una vlan diferente.

7.22.6.3.1. CONFIGURACIÓN VLANS PORTETE

SWITCH PORTETE

Primer Paso

- ✓ Primer paso es cuantas vlan se van a utilizar y se lo configurar en un switch que soporte vlan, el siguiente código muestra como se configura la creación de una o varias vlans

```
Switch#vlan database
Switch(vlan)#vlan 10 name caja
Switch(vlan)#vlan 20 name gerencia
Switch(vlan)#vlan 30 name sistema
Switch(vlan)#vlan 40 name jefe_caja
Switch(vlan)#vlan 50 name contabilidad
APPLY completed.
Exiting....
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Se aplica esta línea para dar inicio a una o varias creaciones de vlans

Esta línea indica la creación de vlan en un orden numérico secuencial; seguido con el nombre de vlan

Comando que permite copiar a la NVRAM para guardar un respaldo en la ram

POC...
BIO... ECA
CAM... US
PER... 3

Segundo Paso

- ✓ Verificar si las vlans fueron creadas con éxito, hacer con un show vlan

Switch#show vlan

VLAN	Nombre	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10	caja	active	
20	gerencia	active	
30	sistema	active	
40	jefe_caja	active	
50	contabilidad	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Nombre de la vlan

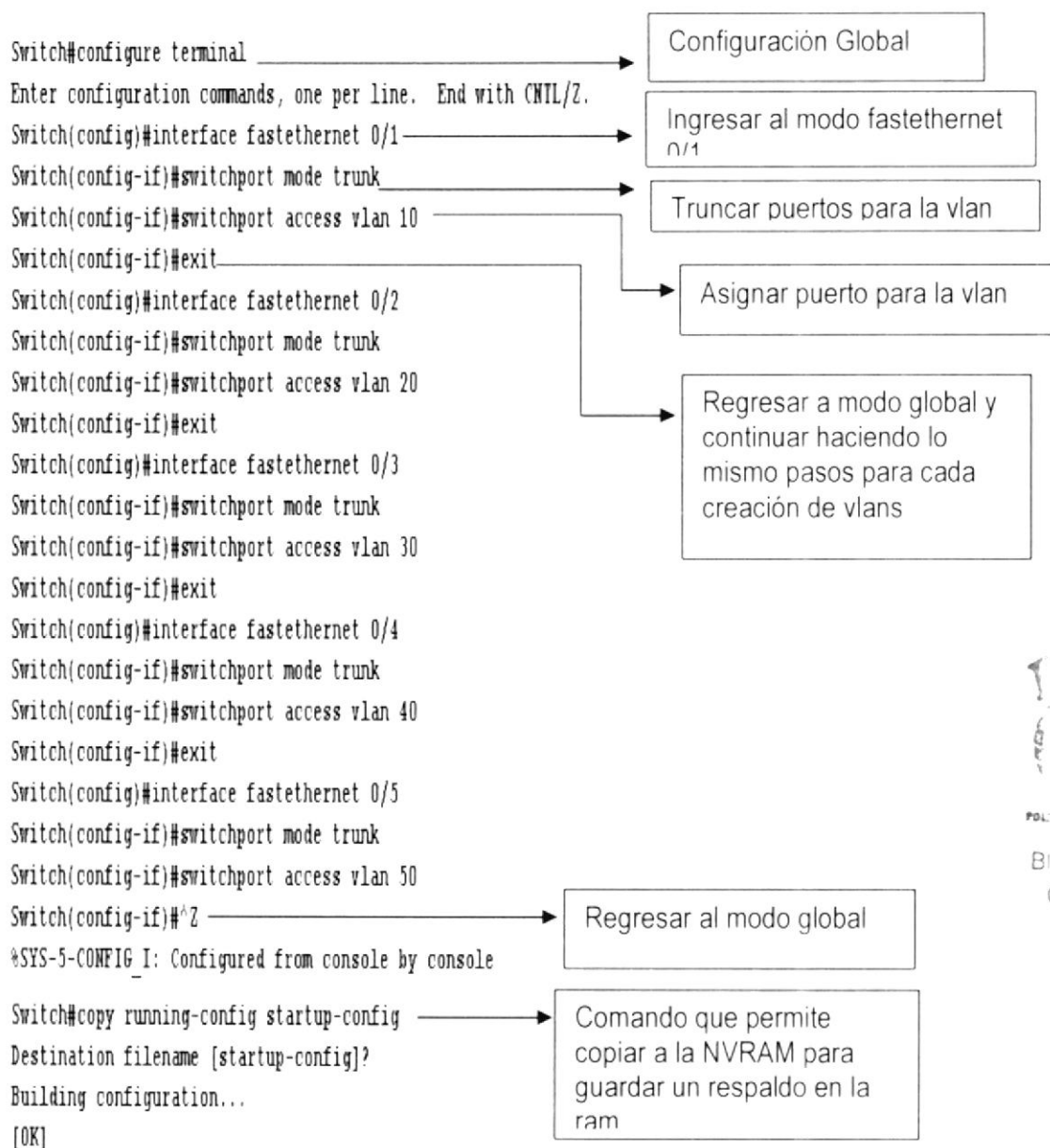
Vlan por defecto utilizado para administrar

Puertos que pertenecen a la vlan



Tercer Paso

- ✓ Una vez realizadas las vlan; asignar los puertos fastethernet en las vlans según sean asignados por el administrador



Cuarto Paso

- ✓ Verificar si los puertos fueron asignados en sus respectivas vlans

Nombre de la vlan

Switch#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
10	caja	active	Fa0/1
20	gerencia	active	Fa0/2
30	sistema	active	Fa0/3
40	jefe_caja	active	Fa0/4
50	contabilidad	active	Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

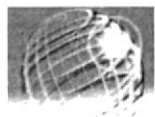
Vlan por defecto utilizado para administrar

Puertos asignados en cada vlans



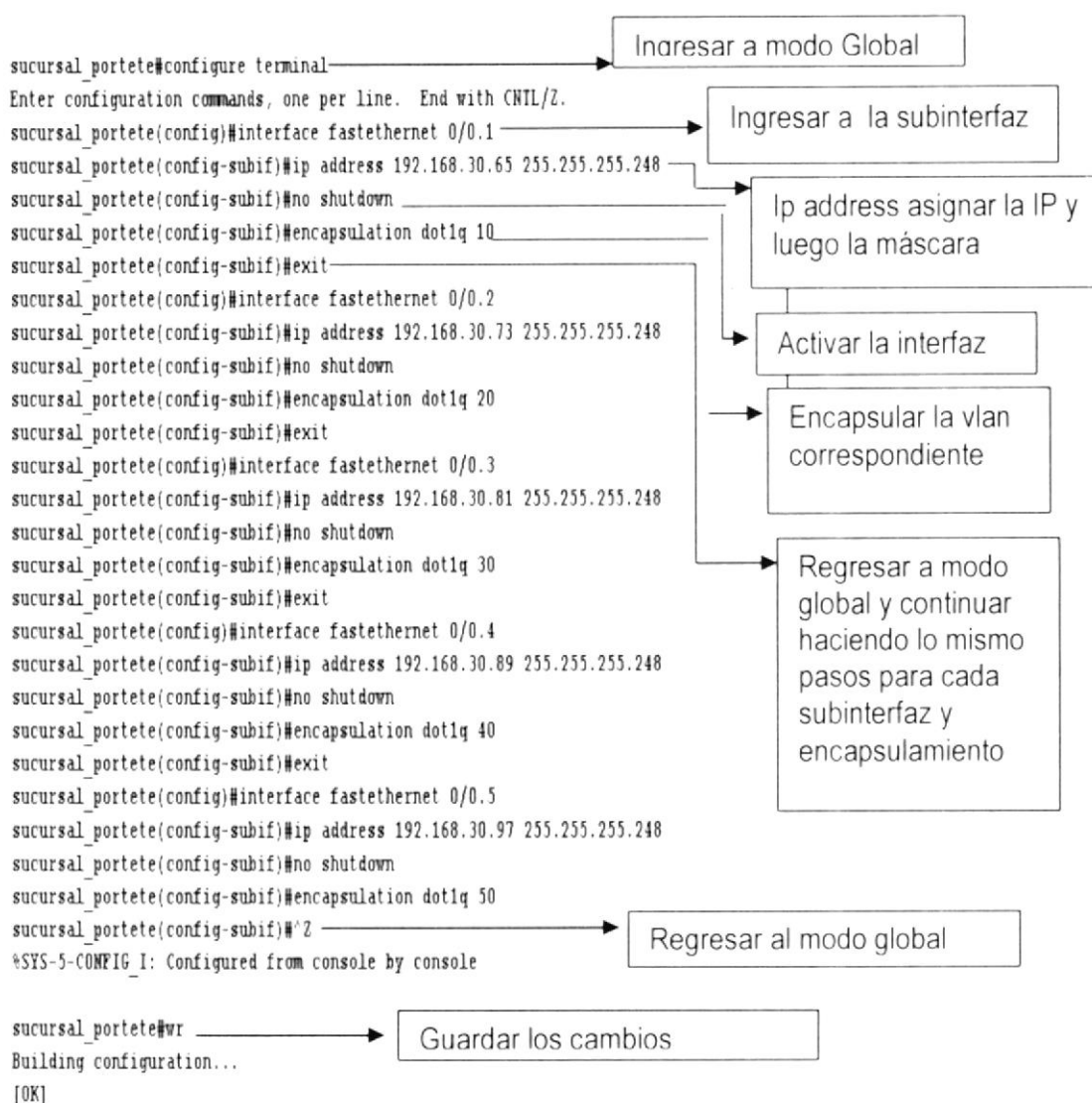
ROUTER PORTETE

NOTA: Una vez realizadas las vlans en el switch se procede a configurar las subinterfaces en el router donde se especifica en el router cuales serán las subinterfaces y en que vlan serán asignadas. En el puerto que viajan las vlan hacia al router es **802.1Q**



Primer Paso

- ✓ En el router se tendrá que configurar las subinterfaces con sus respectivas vlans; con la finalidad para que se puedan comunicarse una vlan con otra.



HOST

Una vez configurados los switches y el routers se procede a configurar las máquinas de cada usuario donde se asigna la IP y el gateway por donde pasará la comunicación

Host dpto. Cajas

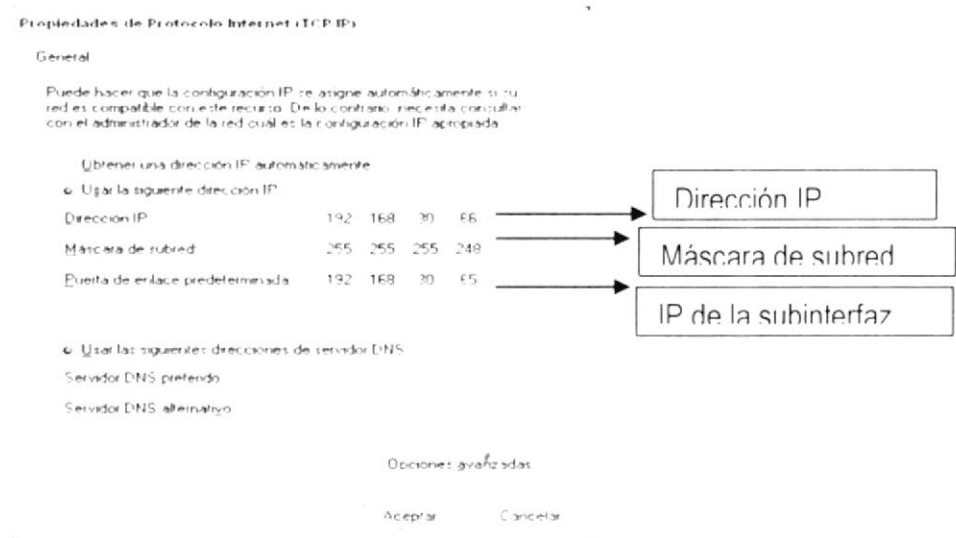


Figura 7-43: Configuración de la tarjeta de red Dpto Cajas

Host dpto. Gerencia

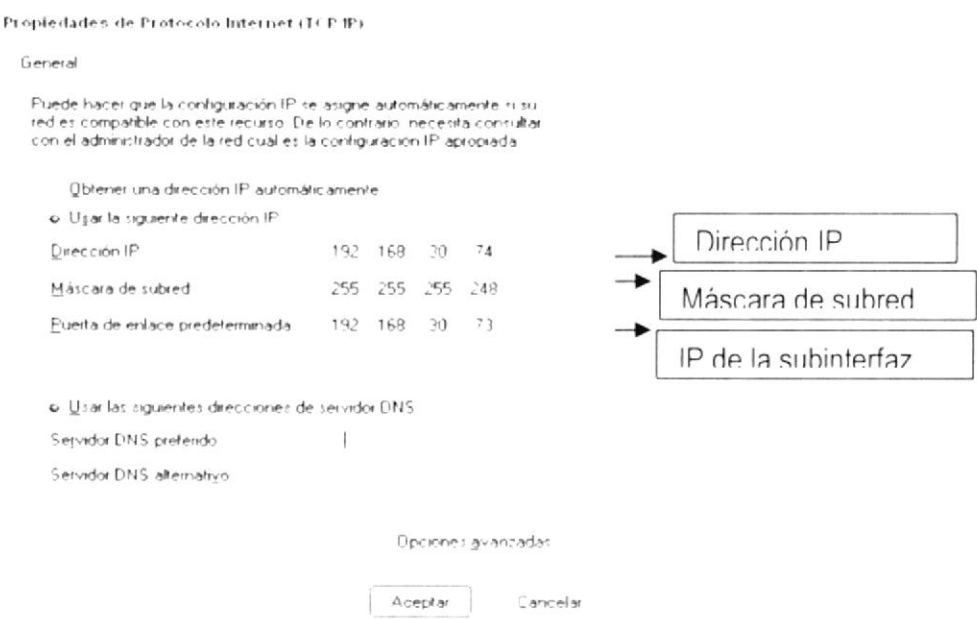


Figura 7-44: Configuración de la tarjeta de red Dpto gerencia

Host dpto. Sistema

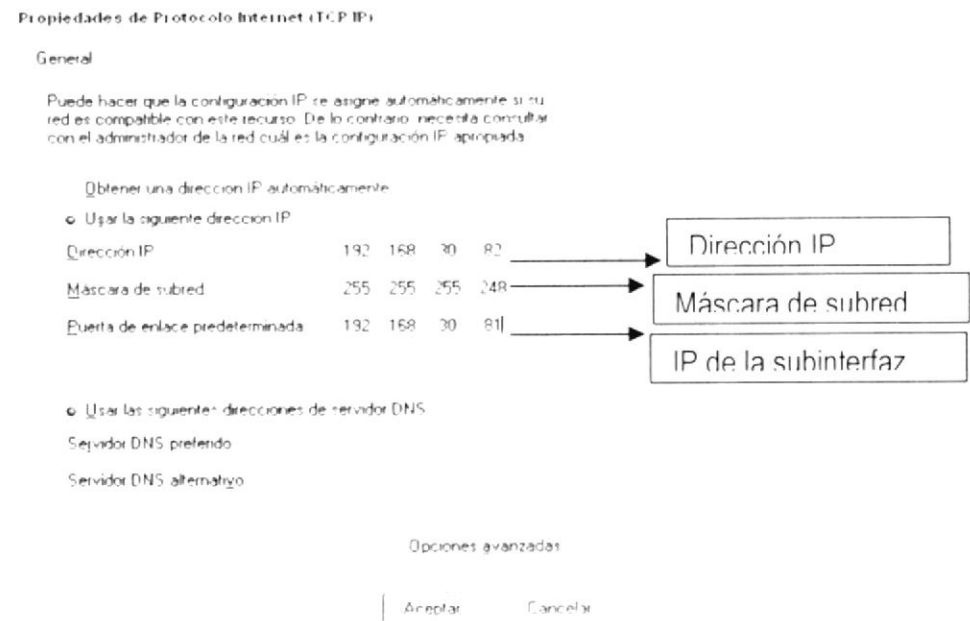


Figura 7-45: Configuración de la tarjeta de red Dpto Sistema

Host dpto. Jefe de cajas

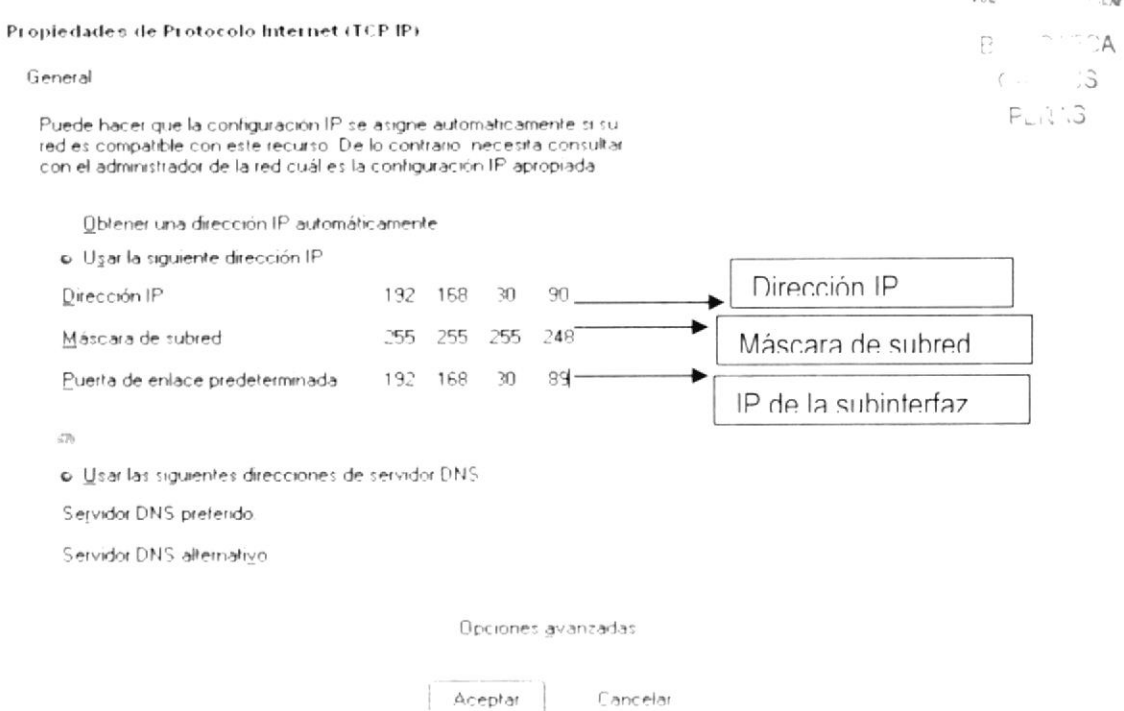


Figura 7-46: Configuración de la tarjeta de red Dpto jefe Caja

Host dpto. Contabilidad

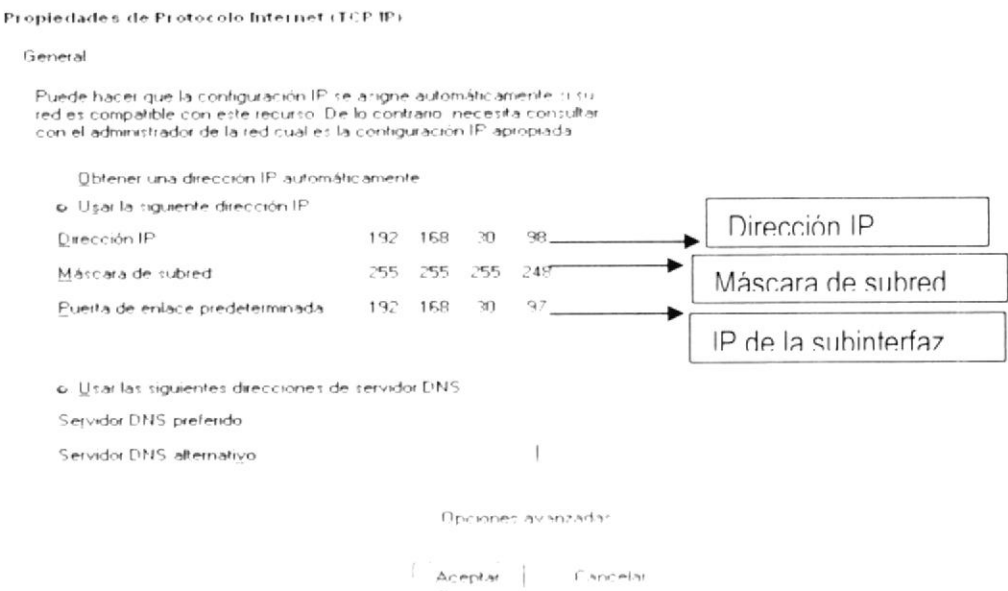


Figura 7-47: Configuración de la tarjeta de red Dpto Contabilidad

7.22.6.3.2. PRUEBAS DE COMUNICACIÓN ENTRE VLANS
PORTETE



NOTA: Una vez asignadas las ip y el gateway de cada máquina se comienzan con las pruebas de las vlans para ver si se comunica las computadoras de la una con la otra.

- ❖ La vlan Cajas hace ping a la vlan Gerencia

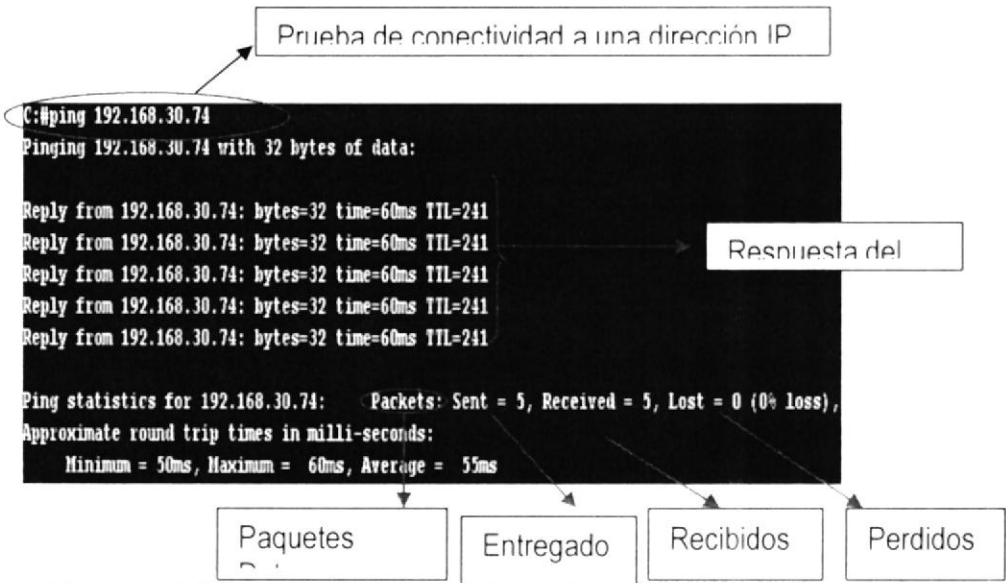


Figura 7-48: prueba de comunicación entre vlan 1.1

- ❖ La vlan Gerencia hace ping a la vlan sistema

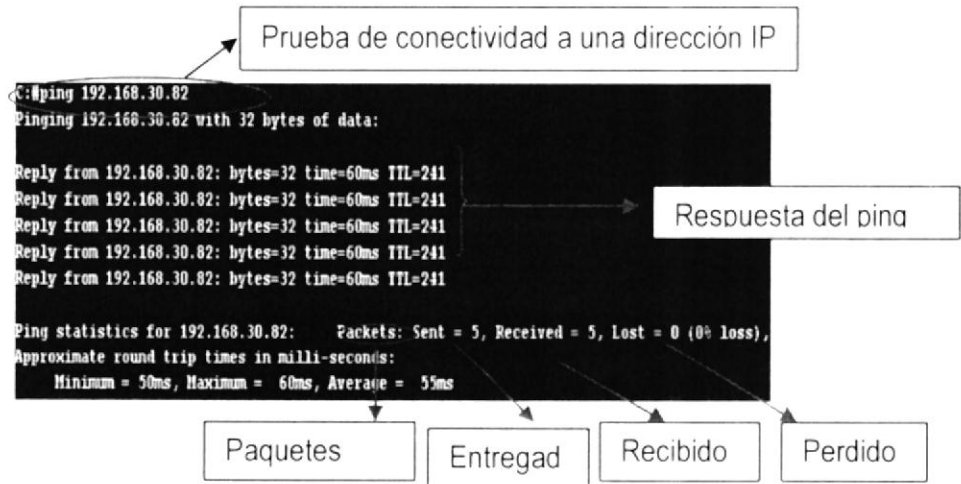


Figura 7-49: prueba de comunicación entre vlan 1.2

- ❖ La vlan sistema hace ping a la vlan Jefe de cajas

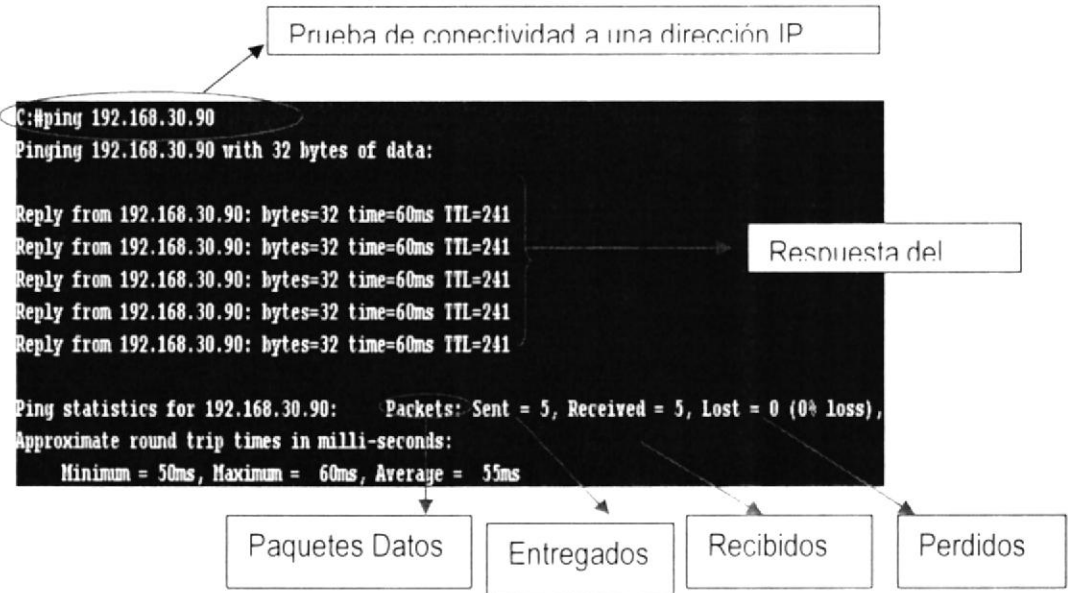


Figura 7-50: prueba de comunicación entre vlan 1.3

- ❖ La vlan Jefe de cajas hace ping a la vlan contabilidad

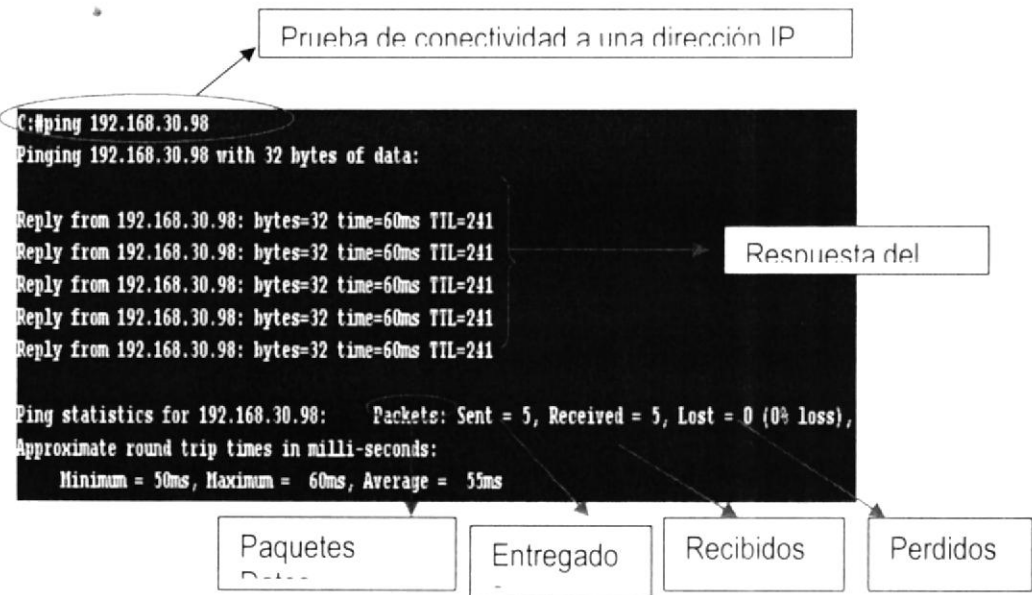


Figura 7-51: prueba de comunicación entre vlan 1.4

7.22.6.3.3. CONFIGURACIÓN VLANS URDESA

SWITCH URDESA

Primer Paso

- ✓ Primer paso es cuantas vlan se van a utilizar y se lo configura en un switch que soporte vlan, el siguiente código muestra como se configura la creación de una o varias vlans

```
Switch#vlan database
Switch(vlan)#vlan 10 name caja
VLAN 10 added:
    Name:caja
Switch(vlan)#vlan 20 name computo
VLAN 20 added:
    Name:computo
Switch(vlan)#vlan 30 name jefe_caja
VLAN 30 added:
    Name:jefe_caja
Switch(vlan)#vlan 40 name gerencia
VLAN 40 added:
    Name:gerencia
Switch(vlan)#vlan 50 name bodega
VLAN 50 added:
    Name:bodega
APPLY completed.
Exiting...
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Se aplica esta línea para dar inicio a una o varias creaciones de vlans

Esta línea indica la creación de vlan en un orden numérico secuencial; seguido con el nombre de vlan

Comando que permite copiar a la NVRAM para guardar un respaldo en la ram



Segundo Paso

- ✓ Verificar si las vlans fueron creadas con éxito, se hace un show vlan

Nomhre de la vlan

Switch#show vlan

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

Vlan por defecto utilizado para administrar

Puertos que pertenecen a la vlan

Tercer Paso

- ✓ Una vez realizadas las vlan; asignar los puertos fastethernet en las vlans según sean asignados por el administrador

```
Switch#configure terminal
Enter configuration commands, one per line. End with Ctrl-Z
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 40
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 50
Switch(config-if)#^Z

%SYS-5-CONFIG I: Configured from console by console
```

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración Global

Ingresar al modo fastethernet

Truncar puertos para la vlan

Asignar puerto para la vlan

Regresar a modo global y continuar haciendo lo mismo pasos para cada creación de vlans

[Regresar al modo global](#)

Comando que permite copiar a la NVRAM para guardar un respaldo en la ram



Cuarto Paso

- ✓ Verificar si los puertos fueron asignados en sus respectivas vlans

Nombre de la vlan

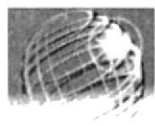
Switch#show vlan

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

Vlan por defecto utilizado para administrar

Puertos asignados en cada vlans

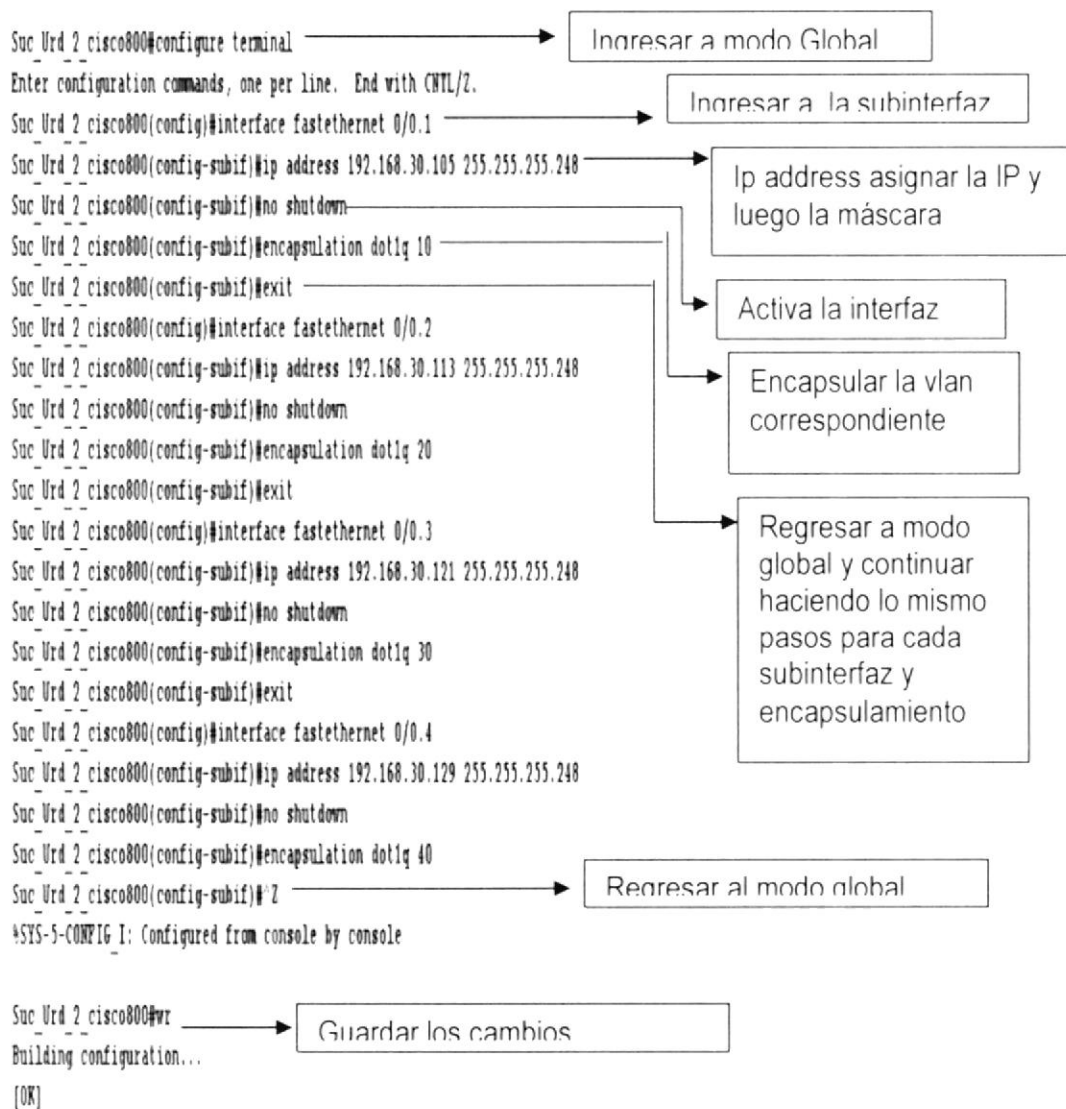
ROUTER URDESA



NOTA:Una vez realizados las vlans en el switch se procede a configurar las subinterfaces en el router donde se especifica en el router cuales serán las subinterfaces y en que vlan serán asignadas. En el puerto que viajan las vlan hacia al router es **802.1Q**

Primer Paso

- ✓ En el router se tendrá que configurar las subinterfaces con sus respectivas vlans; con la finalidad para que se puedan comunicarse una vlan con otra.



HOST



Una vez configurados los switch y el router se procede a configurar las máquinas de cada usuario donde se asigna la IP y el gateway por donde pasará la comunicación

Host dpto. Caja

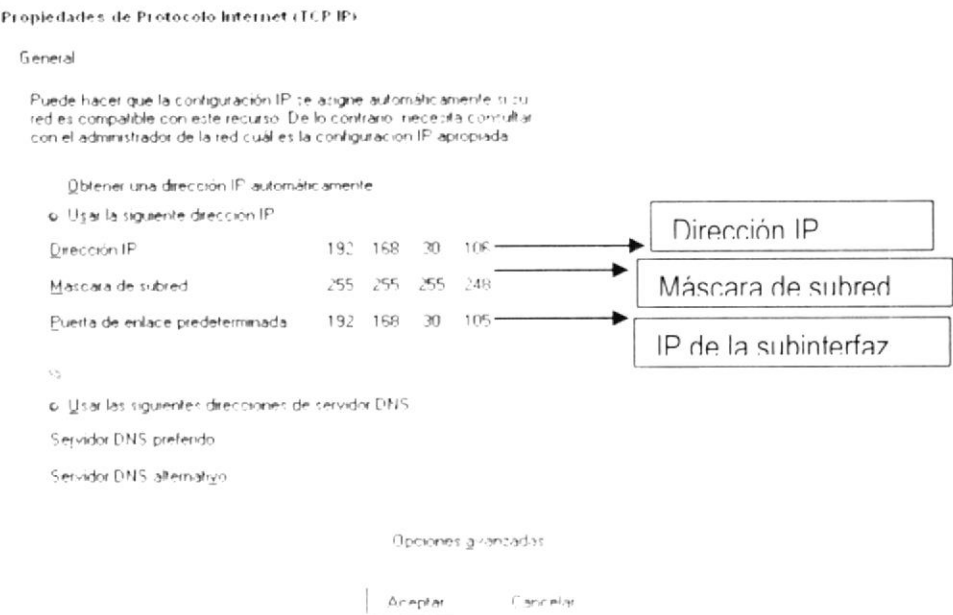


Figura 7-52: Configuración de la tarjeta de red Dpto Caja 2

Host dpto. Cómputo

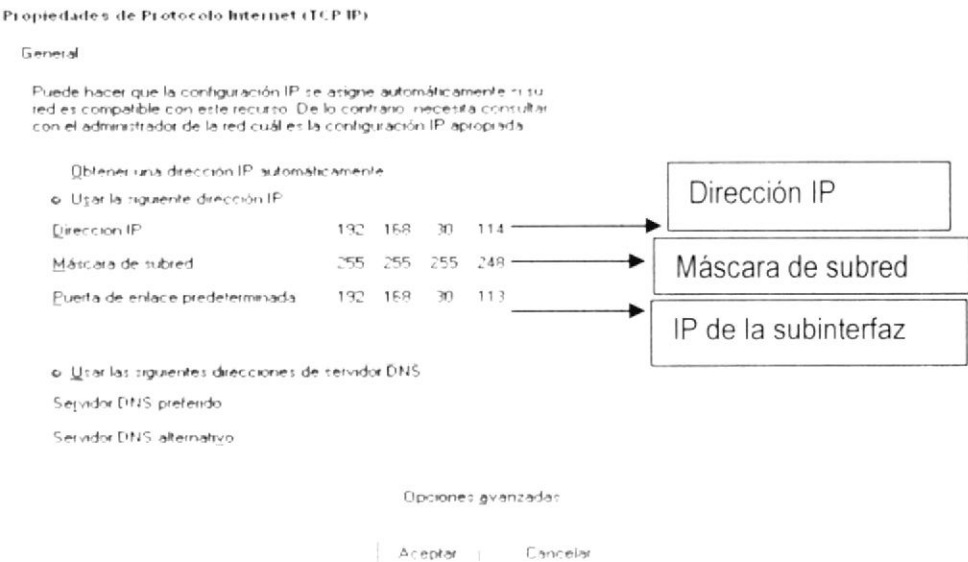


Figura 7-53: Configuración de la tarjeta de red Dpto Cómputo

Host dpto. Jefe Cajas

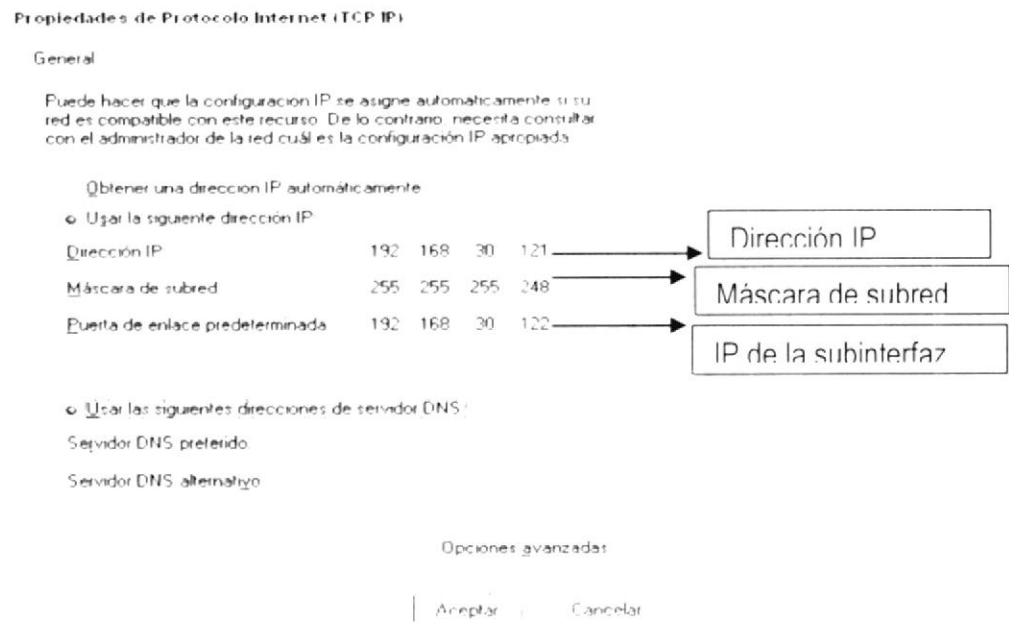


Figura 7-54: Configuración de la tarjeta de red Dpto Jefe Caja 2

Host dpto. Gerencia

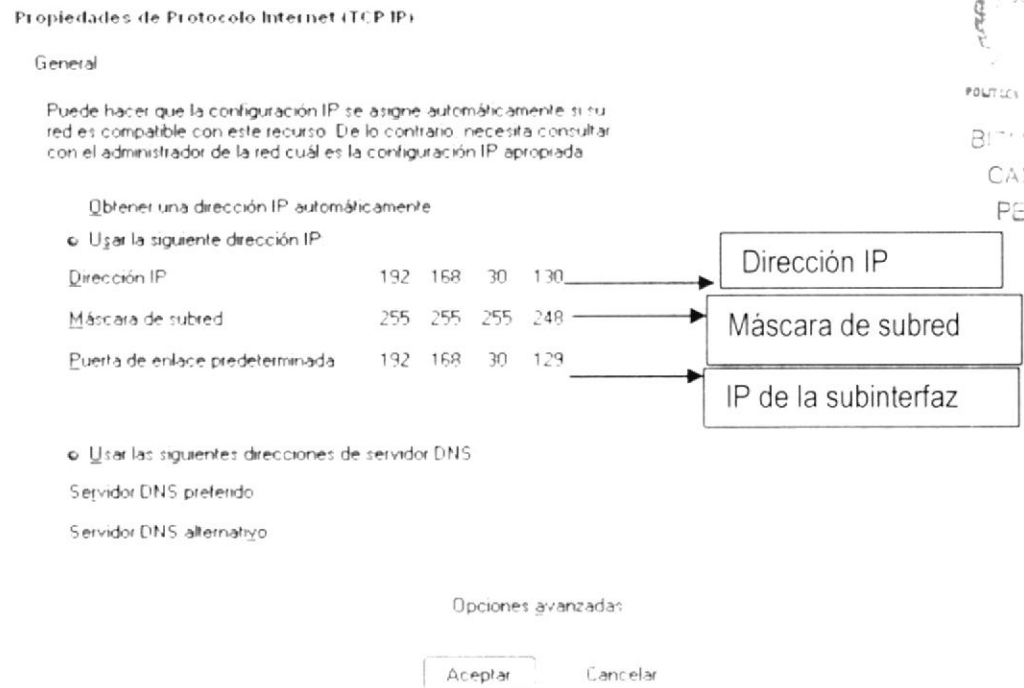
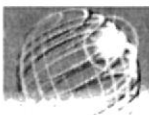


Figura 7-55: Configuración de la tarjeta de red Dpto Gerencia 2

7.22.6.3.4. PRUEBAS DE COMUNICACIÓN ENTRE VLANS URDESA



NOTA: Una vez asignadas las ip y el gateway de cada máquina comienzan las pruebas de las vlans para ver si se comunica las computadoras de la una con la otra.

- ❖ La vlan caja hace ping a la vlan Computo

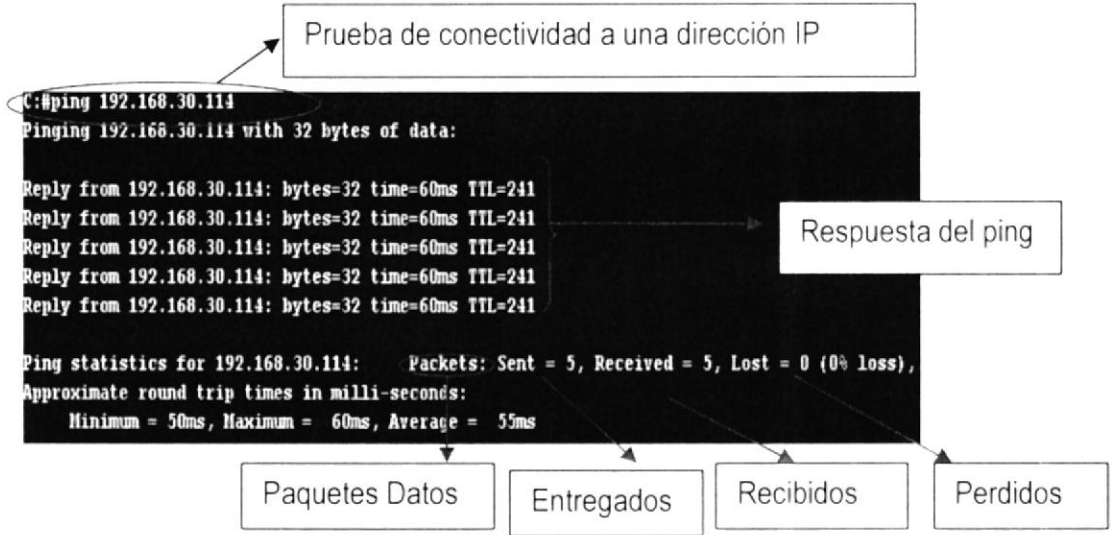


Figura 7-56: prueba de comunicación entre vlan 2.1

- ❖ La vlan Computo hace ping a la vlan Jefe cajas

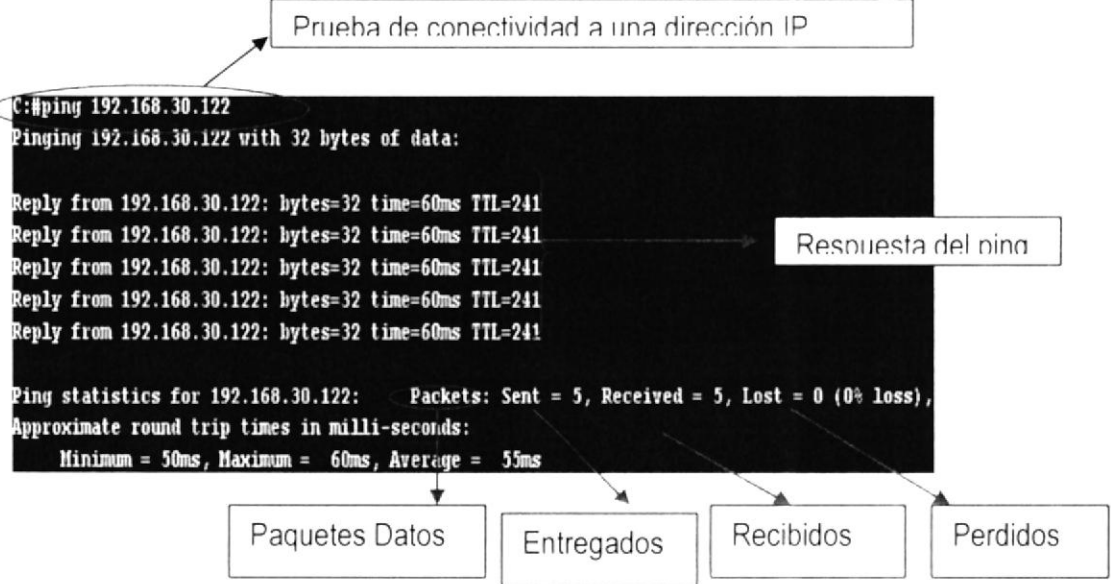


Figura 7-57: prueba de comunicación entre vlan 2.2

La vlan Jefe cajas hace ping a la vlan Gerencia

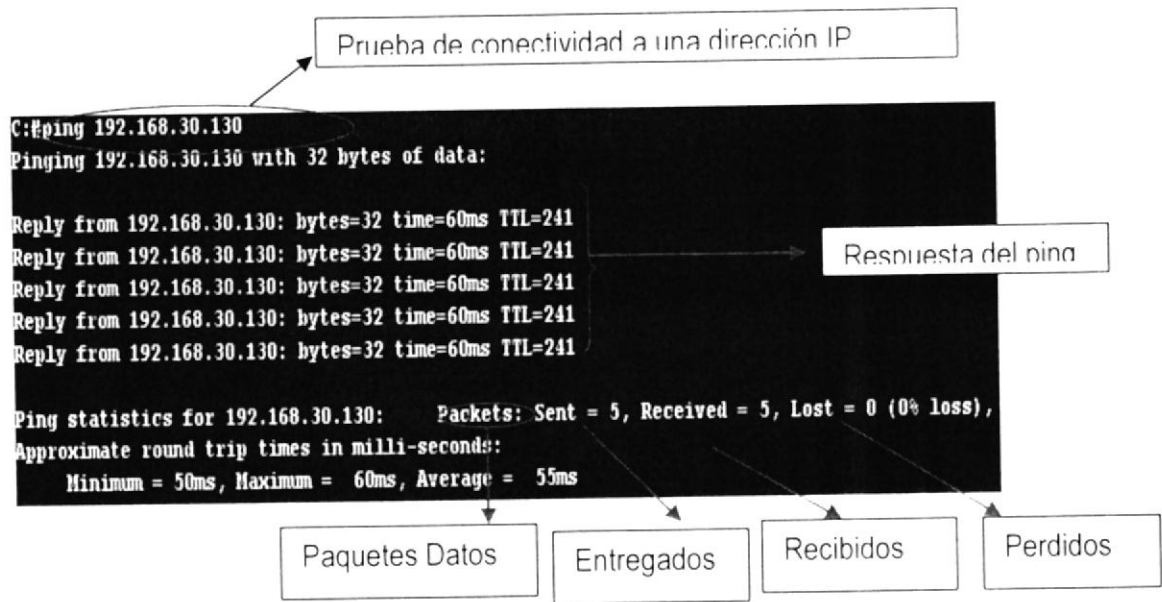


Figura 7-58: prueba de comunicación entre vlan 2.3

❖ La vlan Gerencia hace ping a la vlan Caja

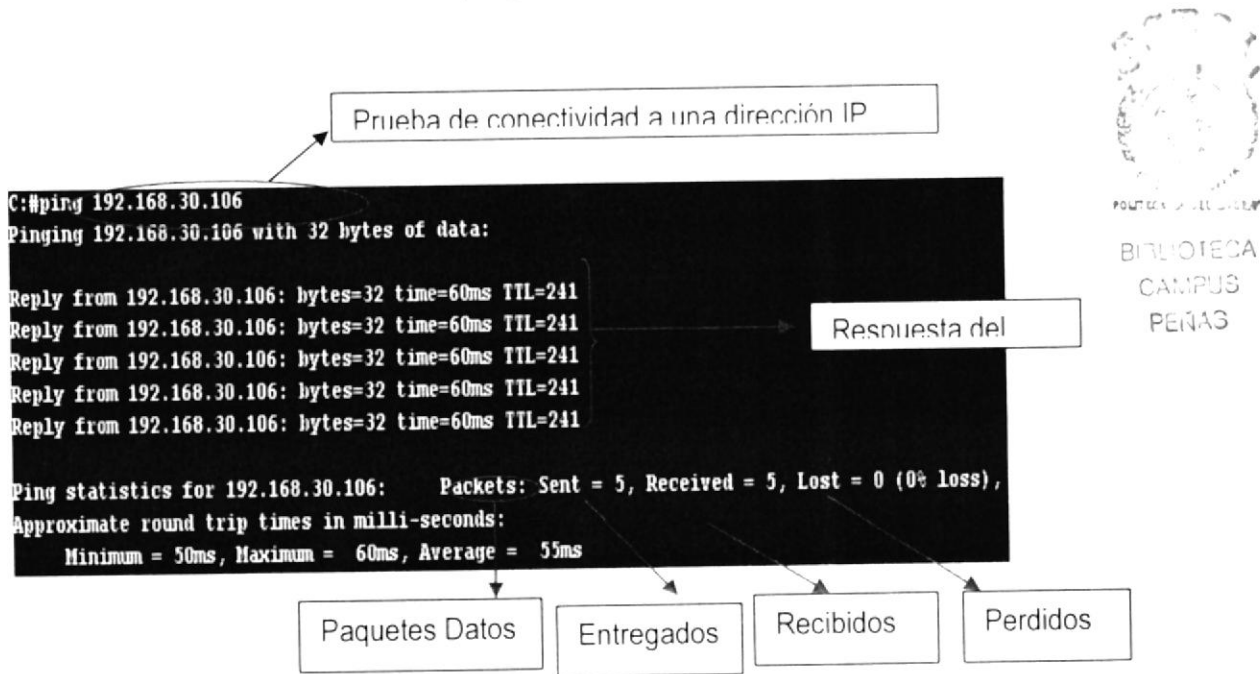


Figura 7-59: prueba de comunicación entre vlan 2.4

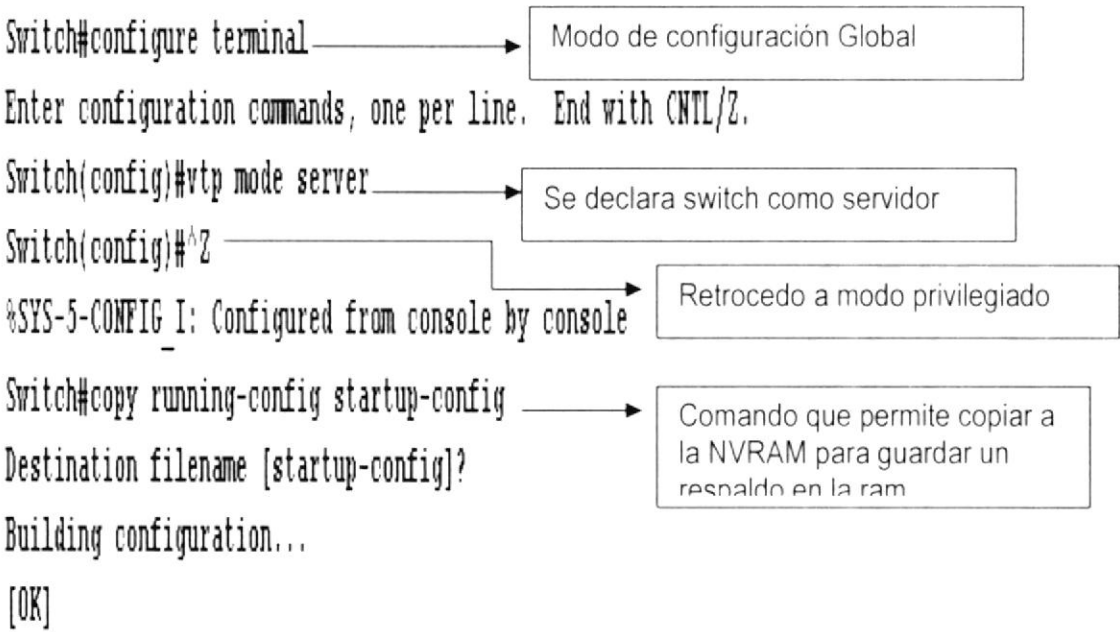
7.22.6.3.5. CONFIGURACIÓN VLANS MATRIZ



NOTA: en la matriz existen 2 switch uno es master y el otro es esclavo por lo tanto se debe configurar esa parte del switch primeramente para que se puedan comunicarse el uno con el otro dispositivo

7.22.6.3.6. SWITCH 1 MASTER

- ✓ En el Switch master se debe declarar como Switch master por lo tanto a continuación se detalla como es la configuración



7.22.6.3.7. SWITCH 2 ESCLAVO

- ✓ En el Switch Esclavo se debe declarar como cliente por lo tanto a continuación se detalla como es la configuración

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp mode client
Switch(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

→ Modo de configuración Global

→ Se declara switch como cliente

→ Retrocedo a modo privilegiado

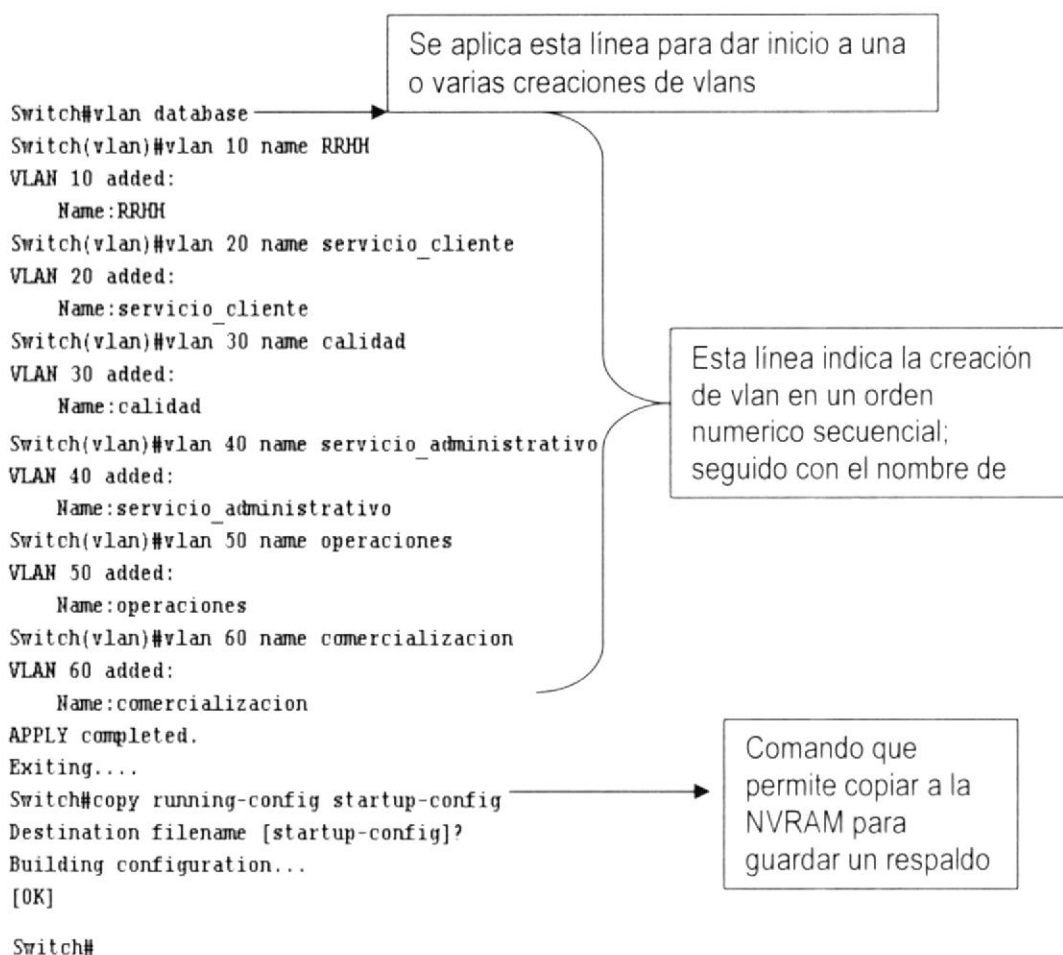
→ Comando que permite copiar a la NVRAM para guardar un respaldo en la ram



7.22.6.3.8. CONFIGURACIÓN SWITCH 1 MASTER

Primer Paso

- ✓ Primer paso es cuantas vlan se van a utilizar y se lo configurar en un switch que soporte vlan, el siguiente código muestra como se configura la creación de una o varias vlans



Segundo Paso

- ✓ Verificar si las vlans fueron creadas con éxito haciendo un show vlan

Switch#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10	RRHH	active	
20	servicio_cliente	active	
30	calidad	active	
40	servicio_administrativo	active	
50	operaciones	active	
60	comercializacion	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

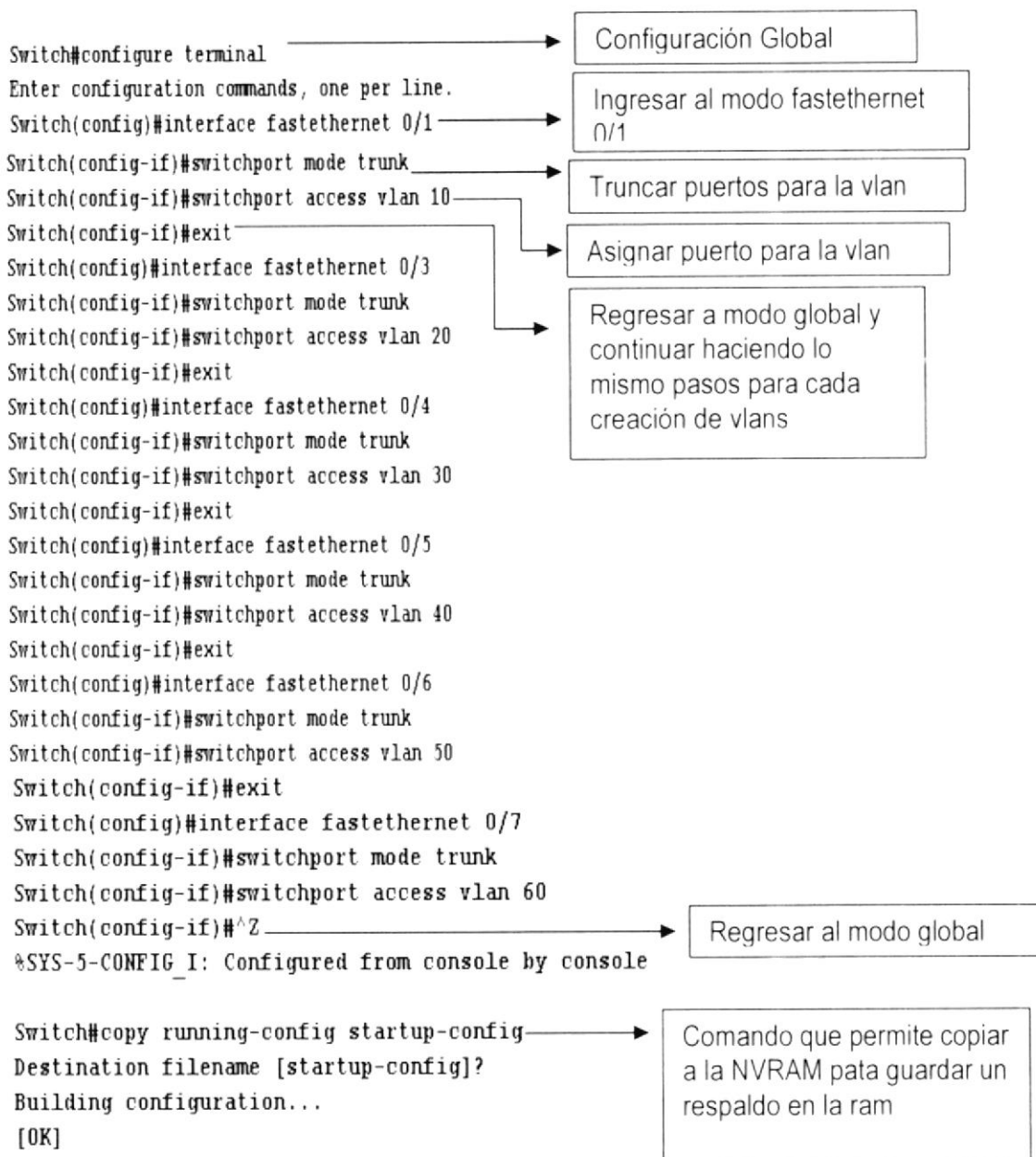
Nombre de la vlan

Vlan por defecto utilizado para administrar

Puertos que pertenecen a la vlan

Tercer Paso

- ✓ Una vez realizadas las vlan; asignar los puertos fastethernet en las vlans según sean asignados por el administrador



Cuarto Paso.

- ✓ Verificar si los puertos fueron asignados en sus respectivas vlans

Nombre de la vlan

Switch#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
10	RRHH	active	Fa0/1
20	servicio_cliente	active	Fa0/3
30	calidad	active	Fa0/4
40	servicio_administrativo	active	Fa0/5
50	operaciones	active	Fa0/6
60	comercializacion	active	Fa0/7
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	

Vlan por defecto utilizado para administrar

Puertos asignados en cada vlans



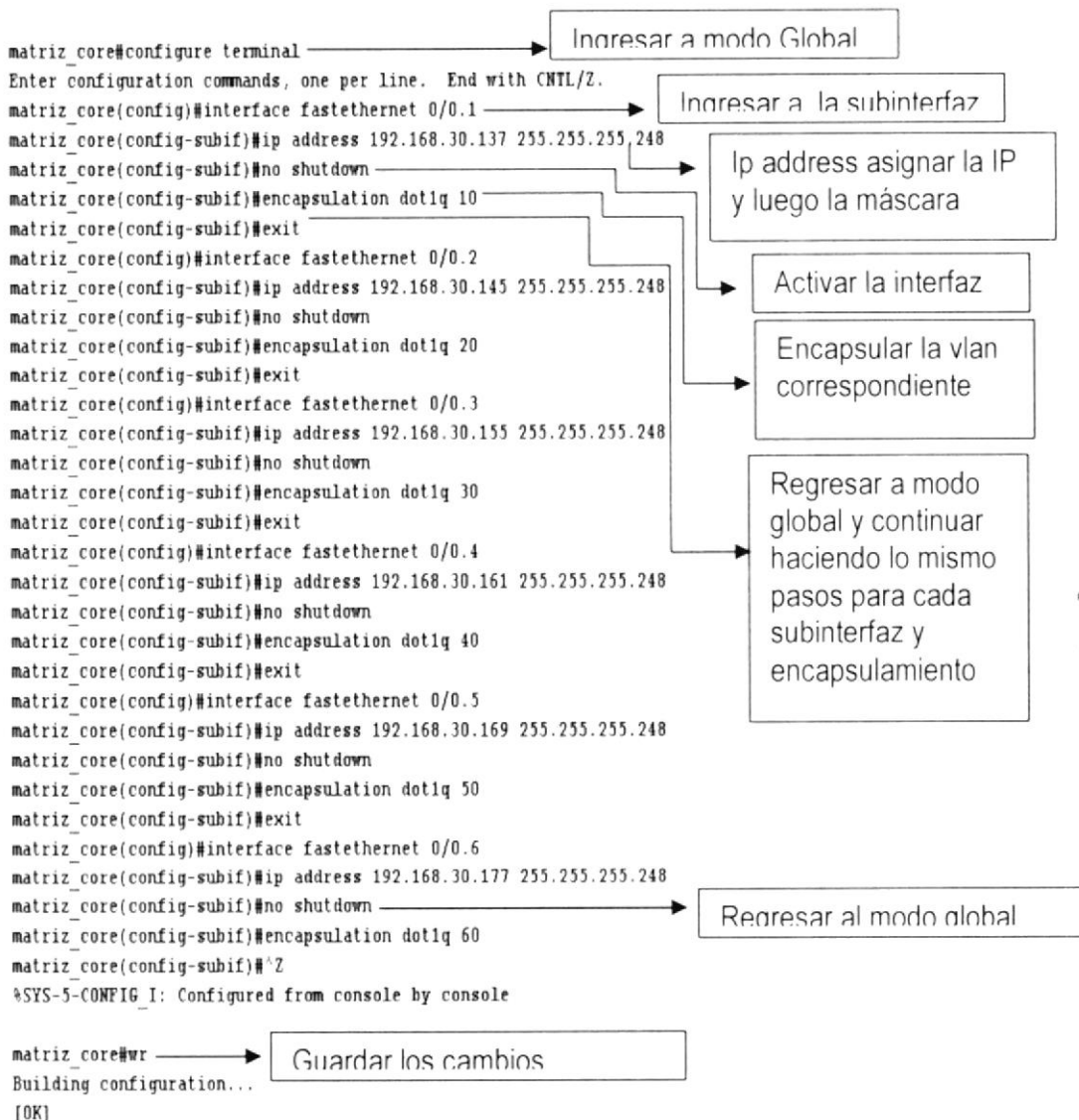
ROUTER MATRIZ



NOTA: Una vez realizados los vlans en el switch se procede a configurar las subinterfaces en el router donde se especifica en el router cuales serán las subinterfaces y en que vlan serán asignadas. En el puerto que viajan las vlan hacia al router es **802.1Q**

Primer Paso

- ✓ En el router se tendrá que configurar las subinterfaces con sus respectivas vlans; con la finalidad para que se puedan comunicarse una vlan con otra.



HOST

Una vez configurados los switch y el router se procede a configurar las máquinas de cada usuario donde se asigna la IP y el gateway por donde pasará la comunicación

Host dpto. Recurso Humanos

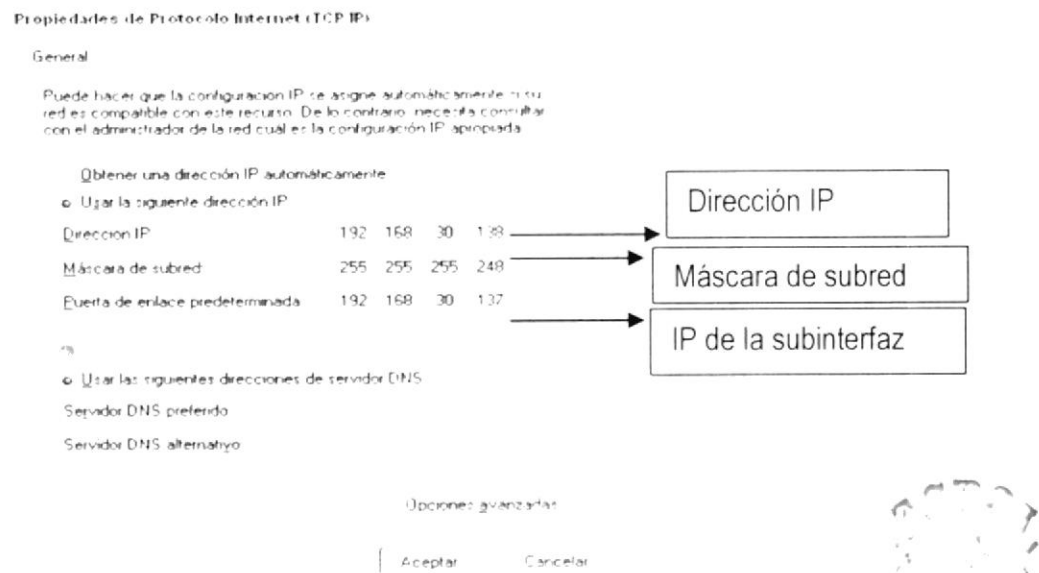


Figura 7-60: Configuración de la tarjeta de red Dpto RRHH

Host dpto. Servicio Administrativo

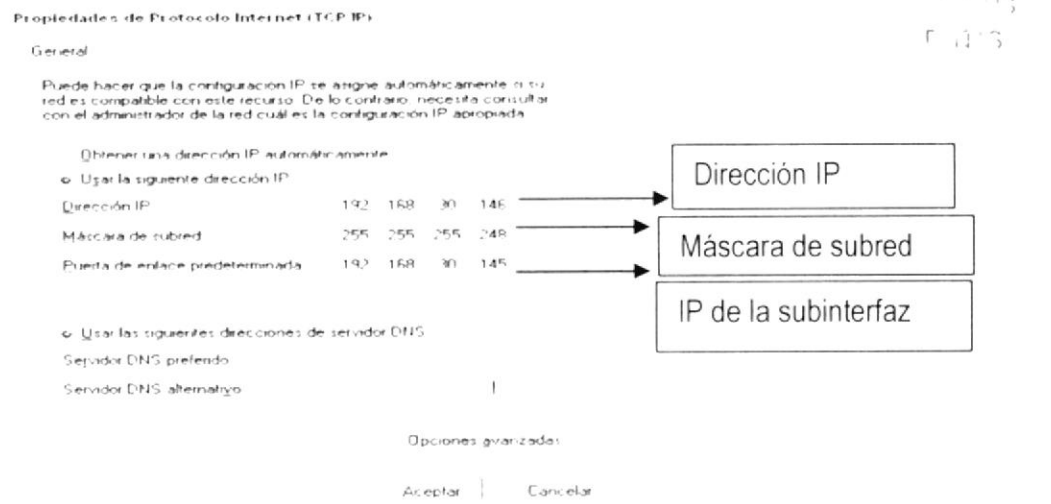


Figura 7-61: Configuración de la tarjeta de red Dpto S. Administrativo

Host dpto. Calidad

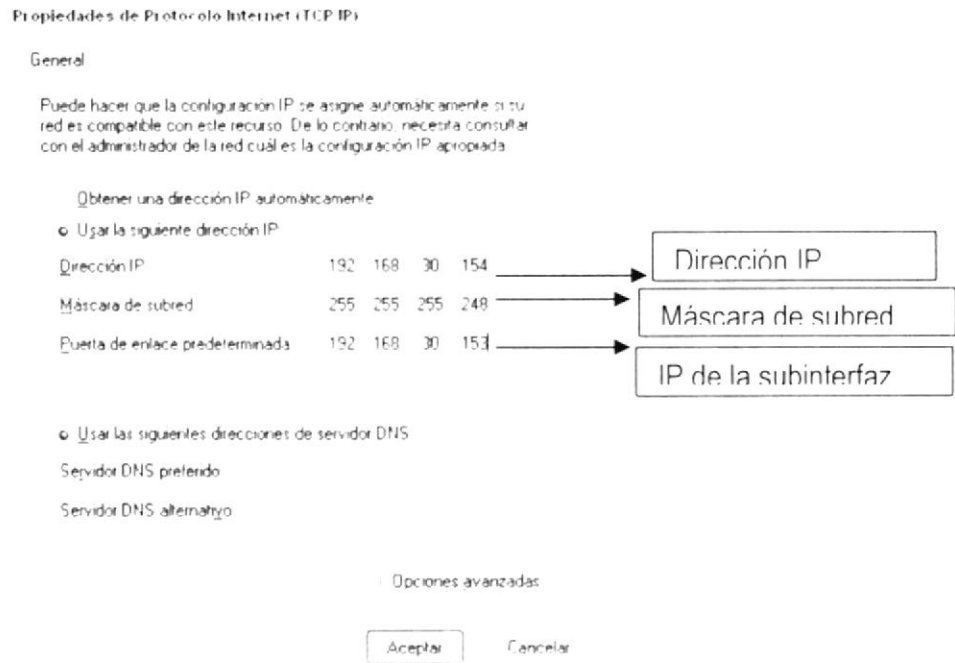


Figura 7-62: Configuración de la tarjeta de red Dpto Calidad

Host dpto. Operación

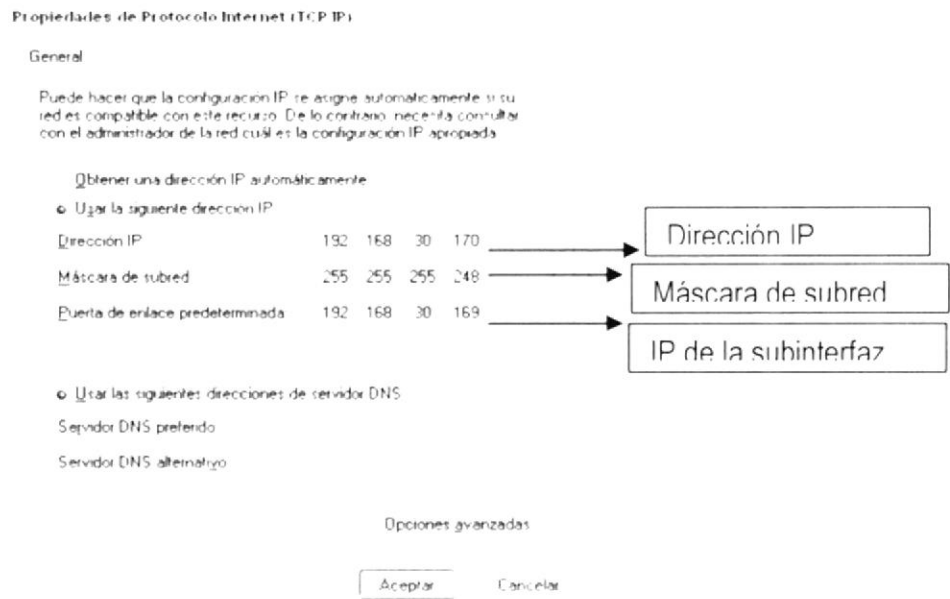


Figura 7-63: Configuración de la tarjeta de red Dpto Operación

Host dpto. Comercialización

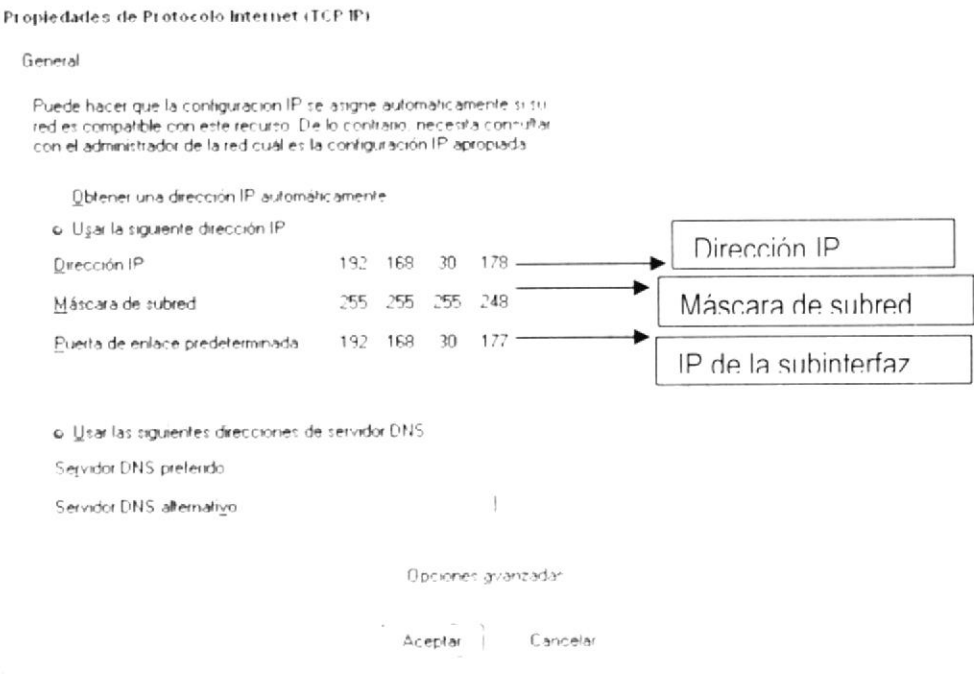


Figura 7-64:Configuración de la tarjeta de red Dpto Comercialización



7.22.6.3.8.1. PRUEBAS DE COMUNICACIÓN VLANS DEL SWITCH MASTER



NOTA: Una vez asignadas las ip y el gateway de cada máquina comienzan las pruebas de las vlans para ver si se comunica las computadoras de la una con la otra estando las vlan en el mismo switch

- ❖ La vlan Recursos Humanos hace ping a la vlan Servicio Cliente

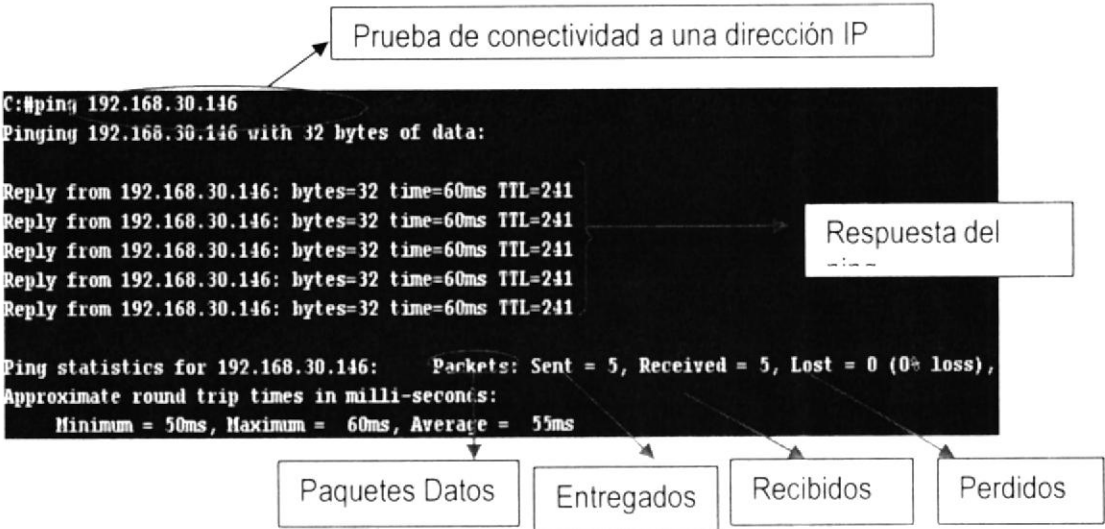


Figura 7-65: prueba de comunicación entre vlan 3.1

- ❖ La vlan Servicio Cliente hace ping a la vlan Calidad

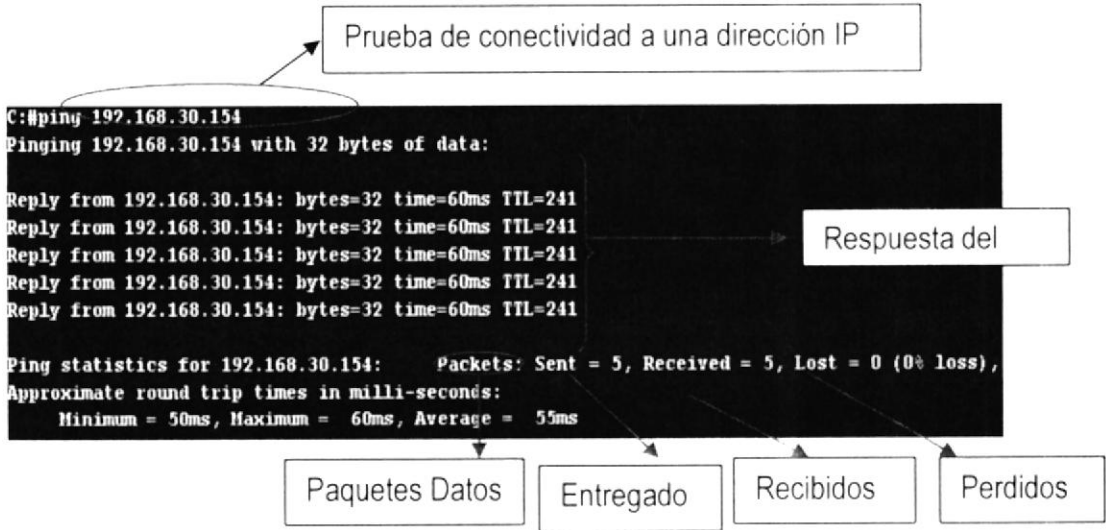


Figura 7-66: prueba de comunicación entre vlan 3.2

- ❖ La vlan Calidad hace ping a la vlan Servicio Administrativo

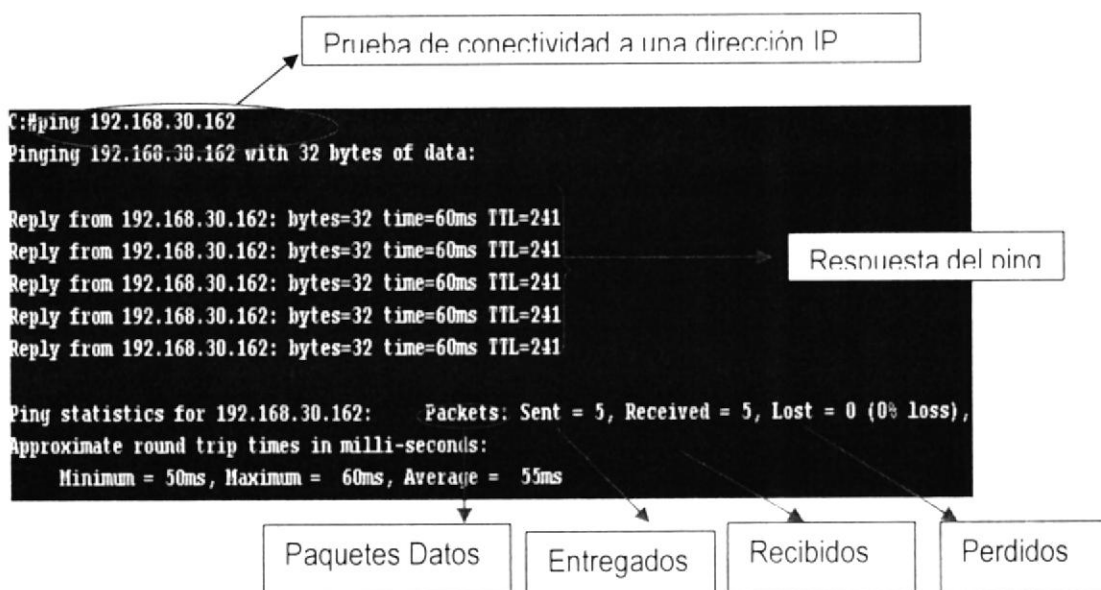


Figura 7-67: prueba de comunicación entre vlan3.3

- ❖ La vlan Servicio Administrativo hace ping a la vlan Operación

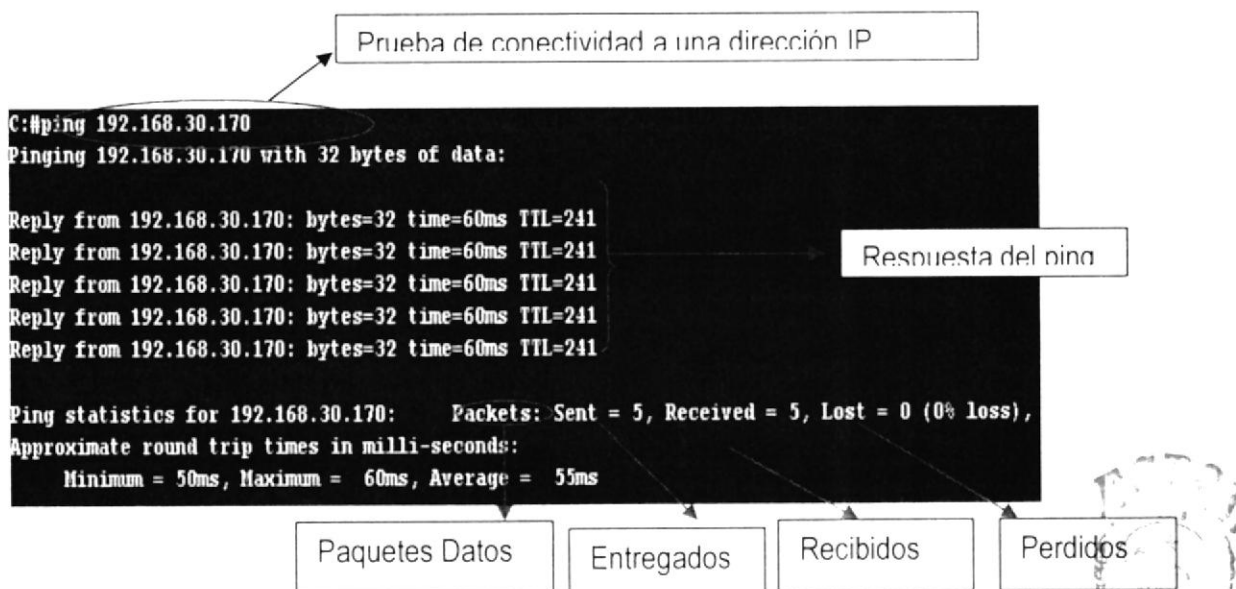


Figura 7-68: prueba de comunicación entre vlan 3.4

- ❖ La vlan Operación hace ping al fastethernet del router

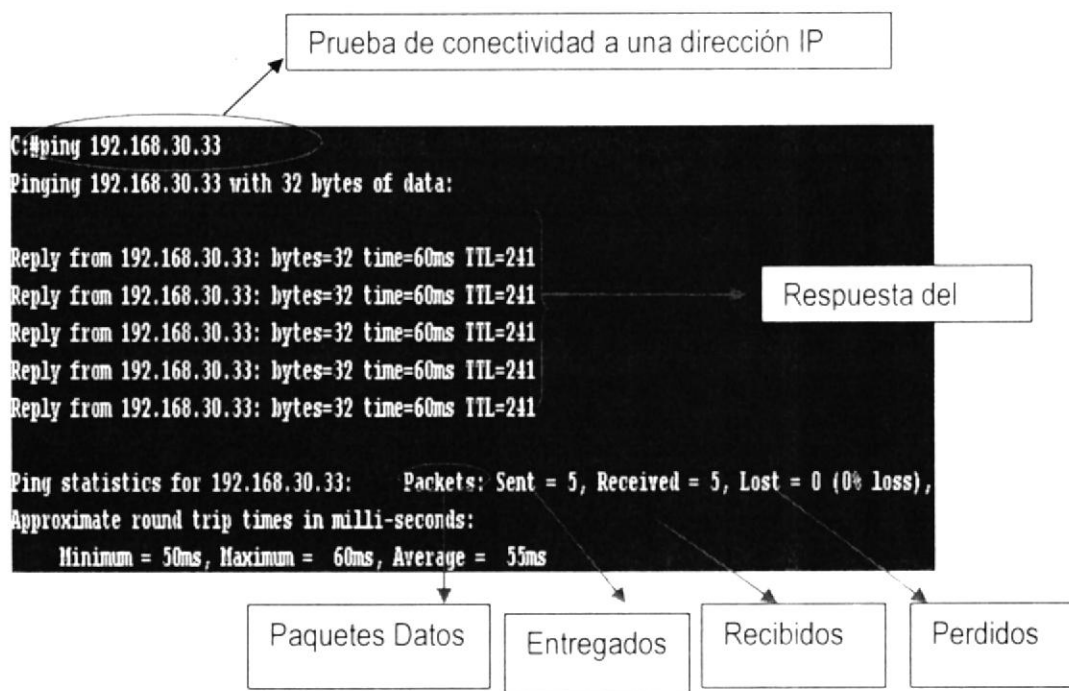
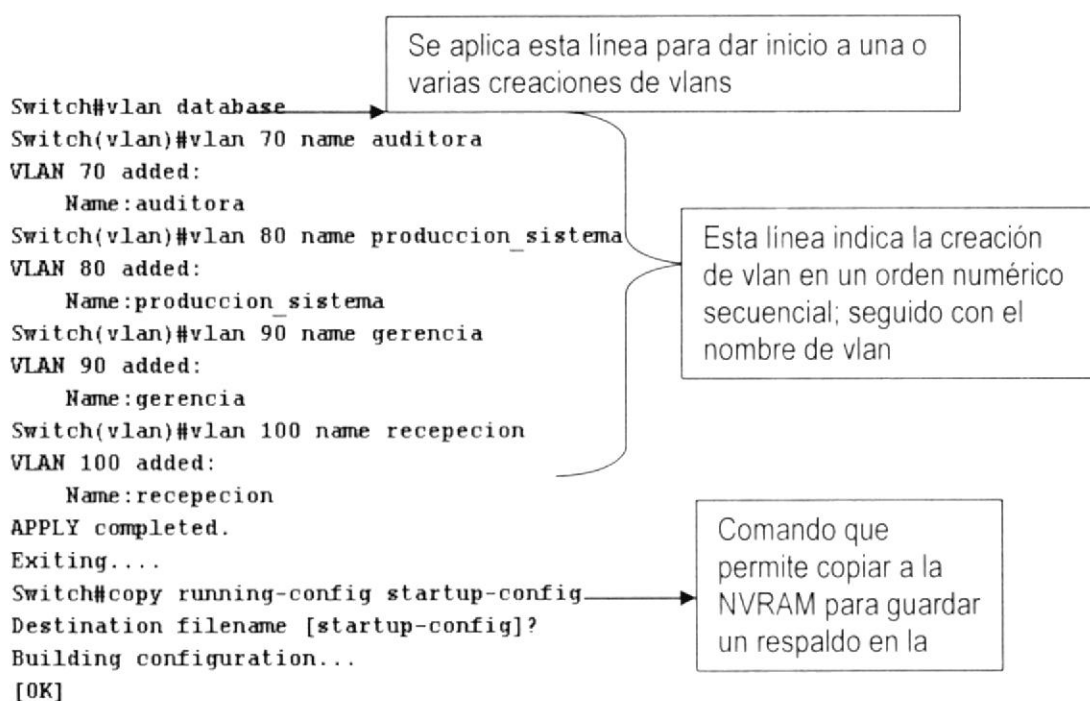


Figura 7-69: prueba de comunicación entre vlan 3.5

7.22.6.3.8.2. CONFIGURACIÓN SWITCH 2 ESCLAVO

Primer Paso

- ✓ Primer paso es cuantas vlan se van a utilizar y se lo configurar en un switch que soporte vlan, el siguiente código muestra como se configura la creación de una o varias vlans



Segundo Paso

- ✓ Verificar si las vlans fueron creadas con éxito haciendo un show vlan

Nombre de la vlan

Switch#show vlan

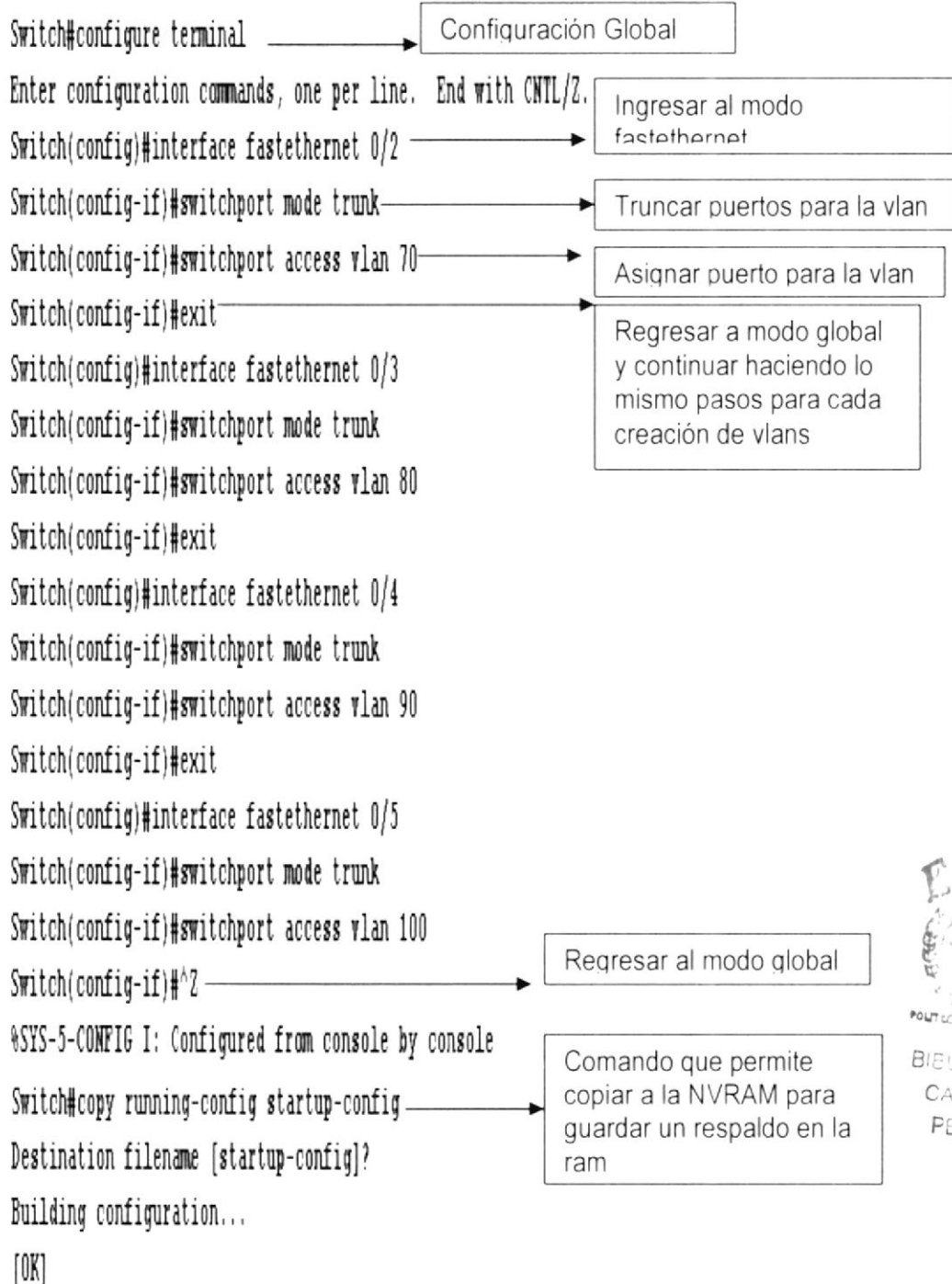
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
70	auditora	active	
80	produccion_sistema	active	
90	gerencia	active	
100	recepcion	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Vlan por defecto utilizado para administrar

Puertos que pertenecen a la vlan

Tercer Paso

- ✓ Una vez realizadas las vlan; asignar los puertos fastethernet en las vlans según sean asignados por el administrador



Cuarto Paso.

- ✓ Verificar si los puertos fueron asignados en sus respectivas vlans

Nombre de la vlan

Switch#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
70	auditora	active	Fa0/2
80	produccion_sistema	active	Fa0/3
90	gerencia	active	Fa0/4
100	recepcion	active	Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Vlan por defecto utilizado para administrar

Puertos asignados en cada vlans

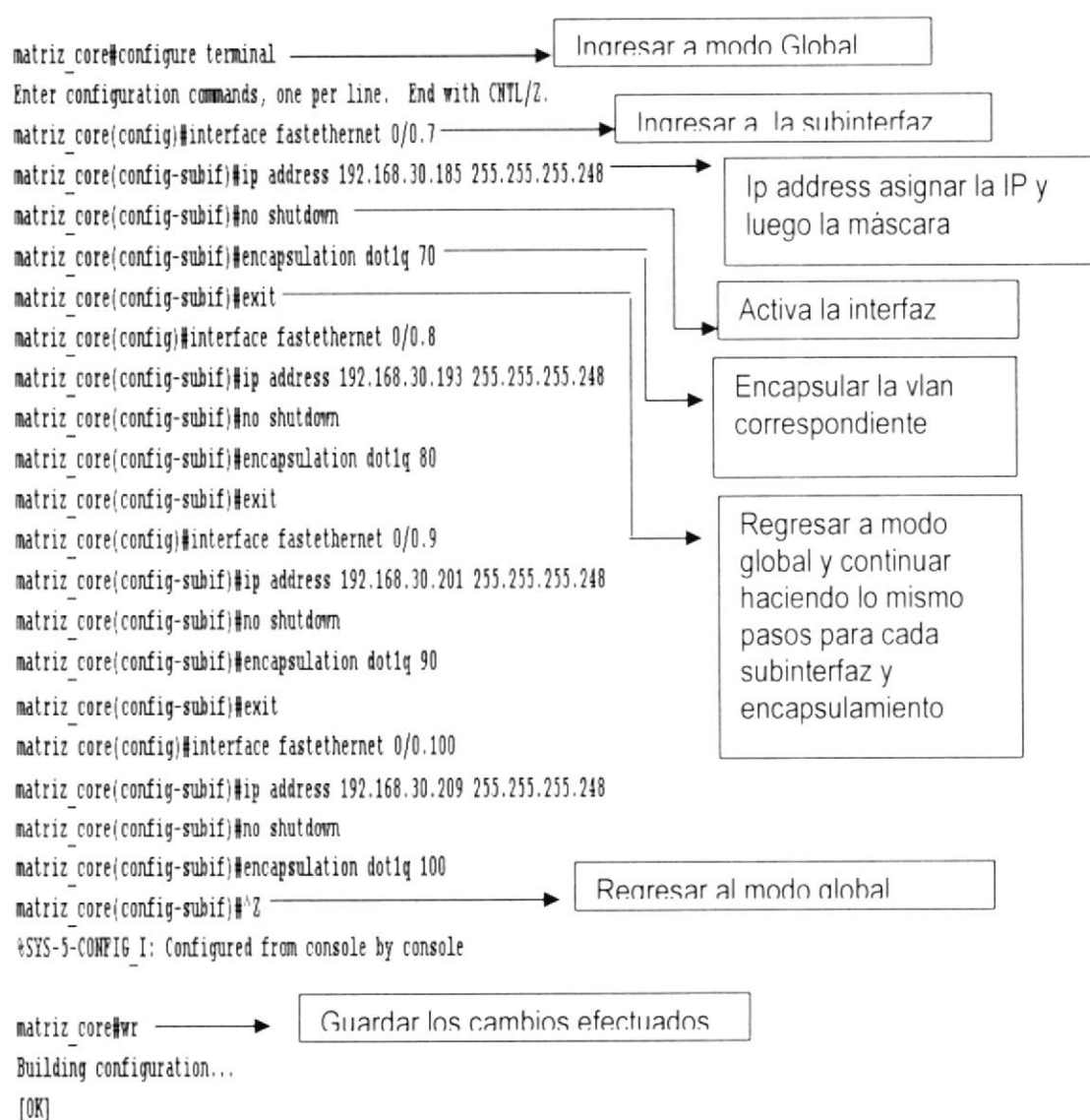
ROUTER MATRIZ



NOTA: Una vez realizadas las vlans en el switch se procede a configurar las subinterfaces en el router donde se especifica en el router cuales serán las subinterfaces y en que vlan serán asignadas. En el puerto que viajan las vlan hacia al router es **802.1Q**

Primer Paso

- ✓ En el router se tendrá que configurar las subinterfaces con sus respectivas vlans; con la finalidad para que se puedan comunicarse una vlan con otra.



HOST



Una vez configurados los switch y el router se procede a configurar las máquinas de cada usuario donde se asigna la IP y el gateway por donde pasará la comunicación

Host Dpto. Auditoría

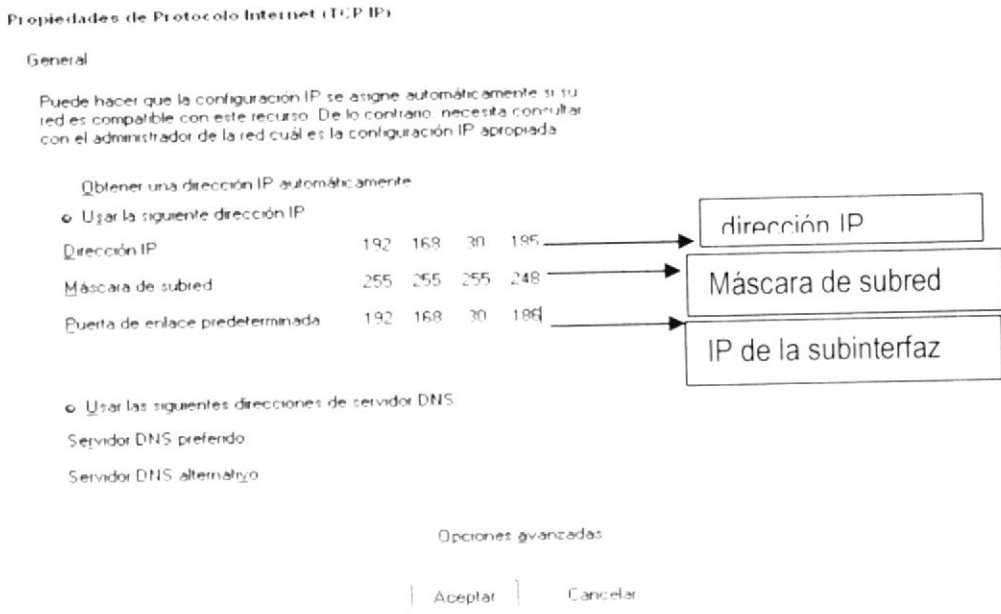


Figura 7-70: Configuración de la tarjeta de red Dpto Auditoría

Host Dpto. Producción & Desarrollo (Sistema)

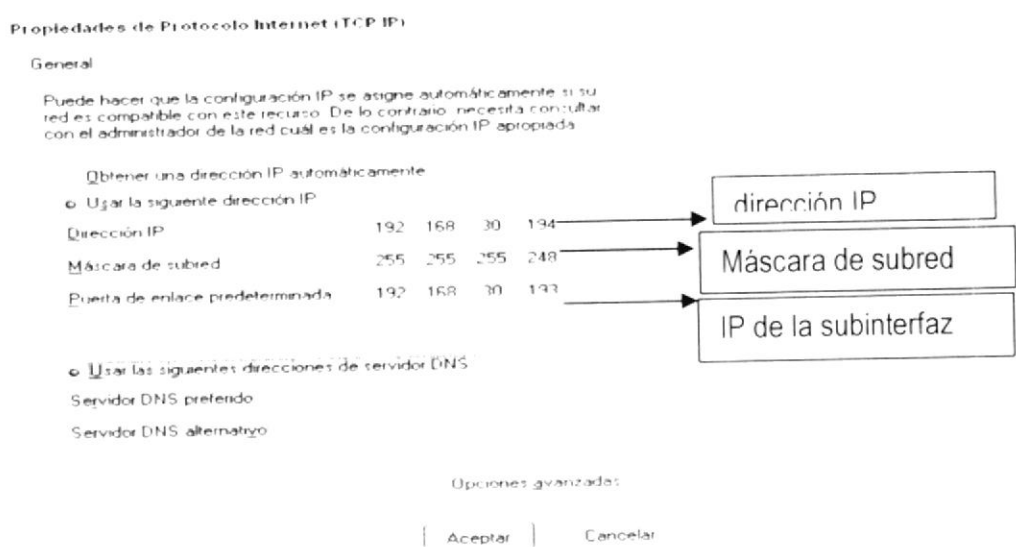


Figura 7-71: Configuración de la tarjeta de red Dpto Desarrollo

Host Dpto. Gerencia

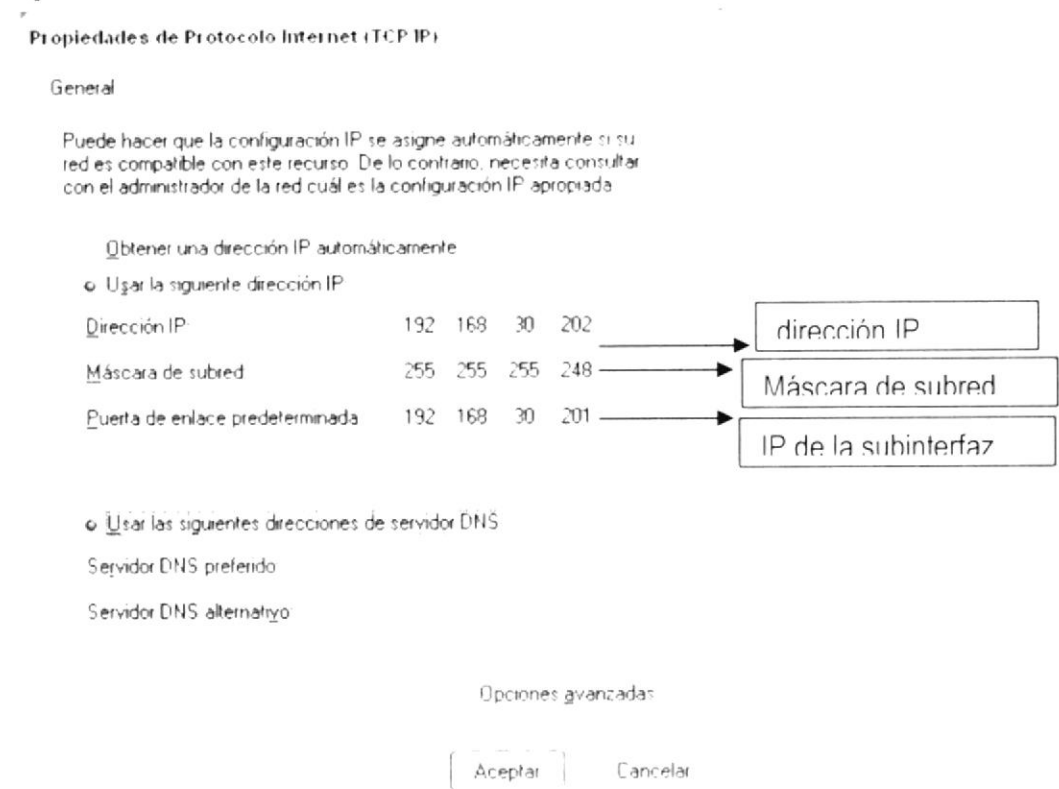


Figura 7-72: Configuración de la tarjeta de red Dpto Gerencia

Host Dpto. Recepción

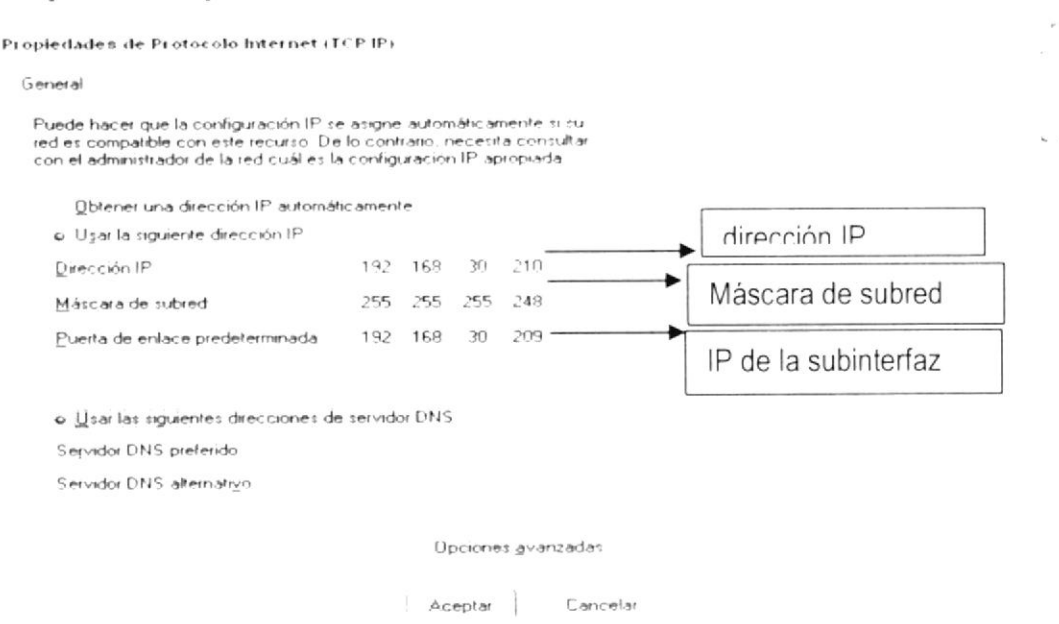


Figura 7-73: Configuración de la tarjeta de red Dpto Recepción

7.22.6.3.8.3. PRUEBAS DE COMUNICACIÓN ENTRE VLANS DEL SWITCH ESCLAVO



NOTA: Una vez asignadas las ip y el gateway de cada máquina comienzan las pruebas de las vlans para ver si se comunica las computadoras de la una con la otra estando las vlan en el mismo shwicht

❖ La vlan Auditoría hace ping a la vlan producción_sistema

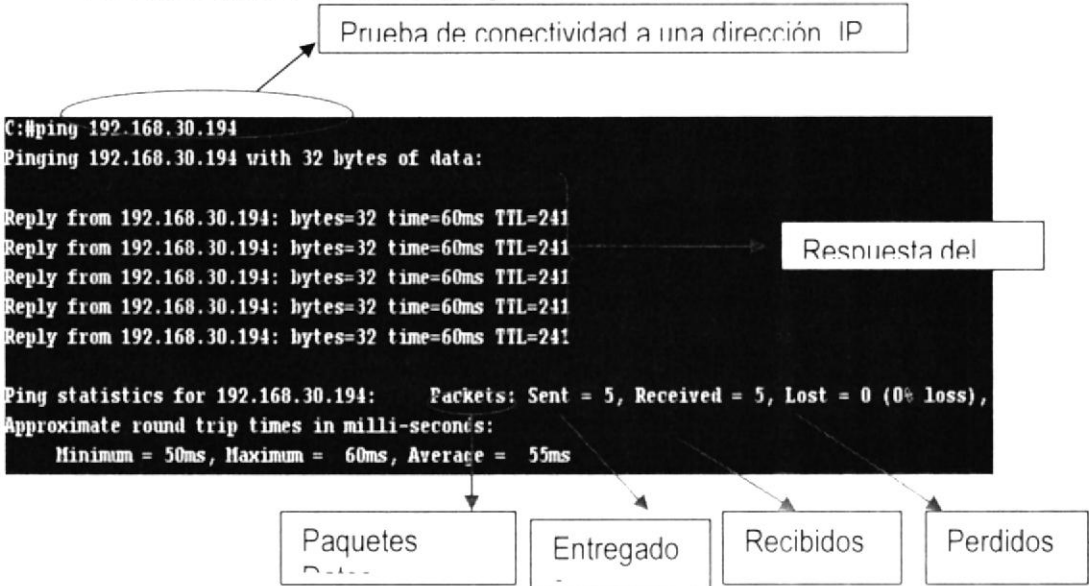


Figura 7-74: prueba de comunicación entre vlan 4.1

❖ La vlan producción_sistema hace ping a la vlan Gerencia

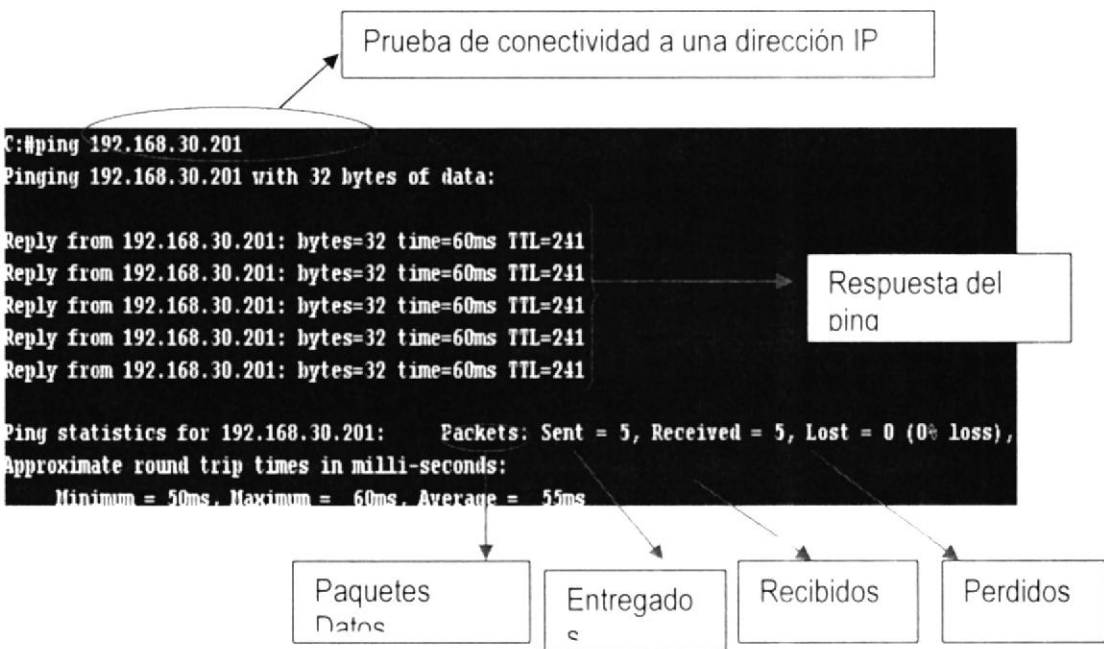


Figura 7-75: prueba de comunicación entre vlan 4.2

- ❖ La vlan Gerencia hace ping a la vlan Recepción

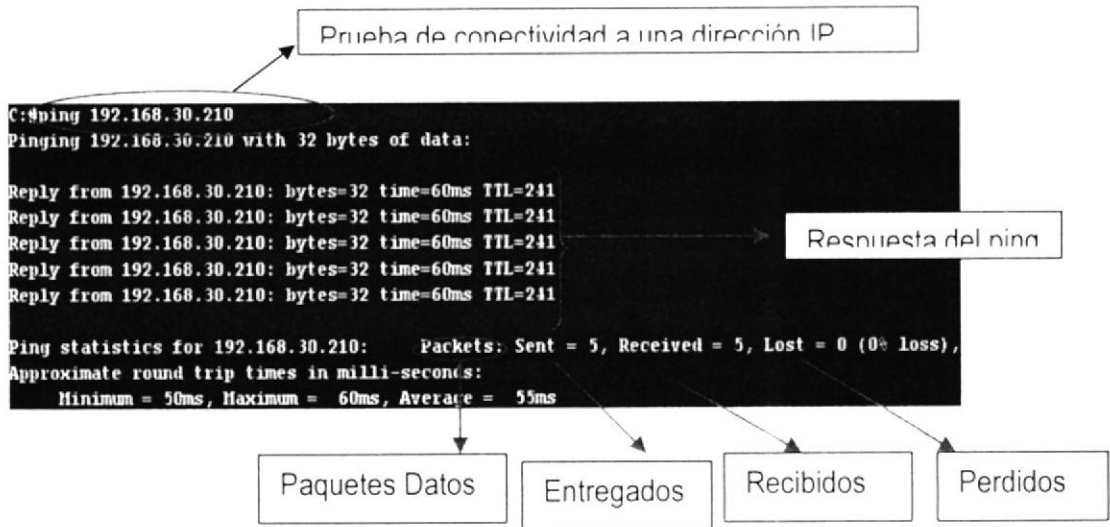


Figura 7-76: prueba de comunicación entre vlan 4.3

- ❖ La vlan recepción que se encuentra en el router esclavo hace ping a la fastethernet de Switch master

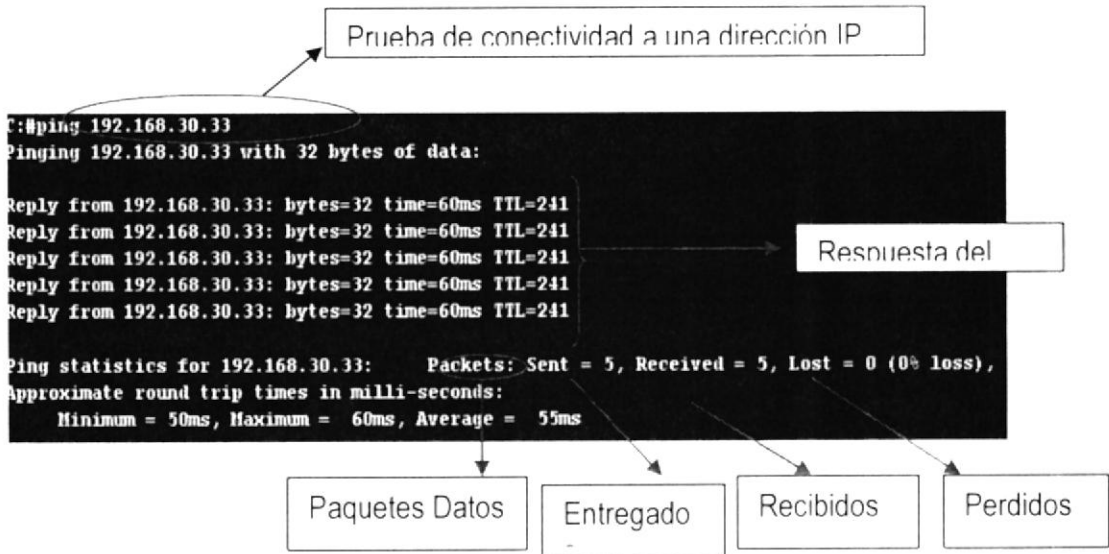


Figura 7-77: prueba de comunicación entre vlan 4.4

7.22.6.3.9. PRUEBAS DE COMUNICACIÓN ENTRE SWITCH MASTER-ESCLAVO

- ❖ La vlan RRHH (192.168.30.138) que se encuentra en el Switch master hace ping a la vlan producción (192.168.30.193) que se encuentra en el Switch esclavo

```
C:\#ip
HELP
Manipulates ip address for Workstation.

IPCONFIG [/ip] [/dg]
/ip      Adds the ip address and subnet mask to the workstation
/dg      Adds the default gateway to the workstation

Examples:
C> ipconfig /ip 157.1.1.12 255.0.0.0
C> ipconfig /dg 157.1.1.1

Boson BOSS 5.0 IP Configuration
Ethernet adapter Local Area Connection:
    IP Address. . . . . : 192.168.30.138
    Subnet Mask . . . . . : 255.255.255.248
    Default Gateway . . . . . : 192.168.30.137

You can also use winipcfg to configure the IP Address

C:\#ping 192.168.30.193
Pinging 192.168.30.193 with 32 bytes of data:

Reply from 192.168.30.193: bytes=32 time=60ms TTL=241
Reply from 192.168.30.193: bytes=32 time=60ms TTL=241
Reply from 192.168.30.193: bytes=32 time=60ms TTL=241
Reply from 192.168.30.193: bytes=32 time=60ms TTL=241
Reply from 192.168.30.193: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.30.193:    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 60ms, Average = 55ms
```

Respuesta del

Paquetes Datos

Entregado

Recibidos

Perdidos

Figura 7-78: prueba de comunicación entre vlan 5.1

- ❖ La vlan servicio_cliente (192.168.30.146) que se encuentra en el Switch master hace ping a la vlan Gerencia (192.168.30.202) que se encuentra en el Switch esclavo

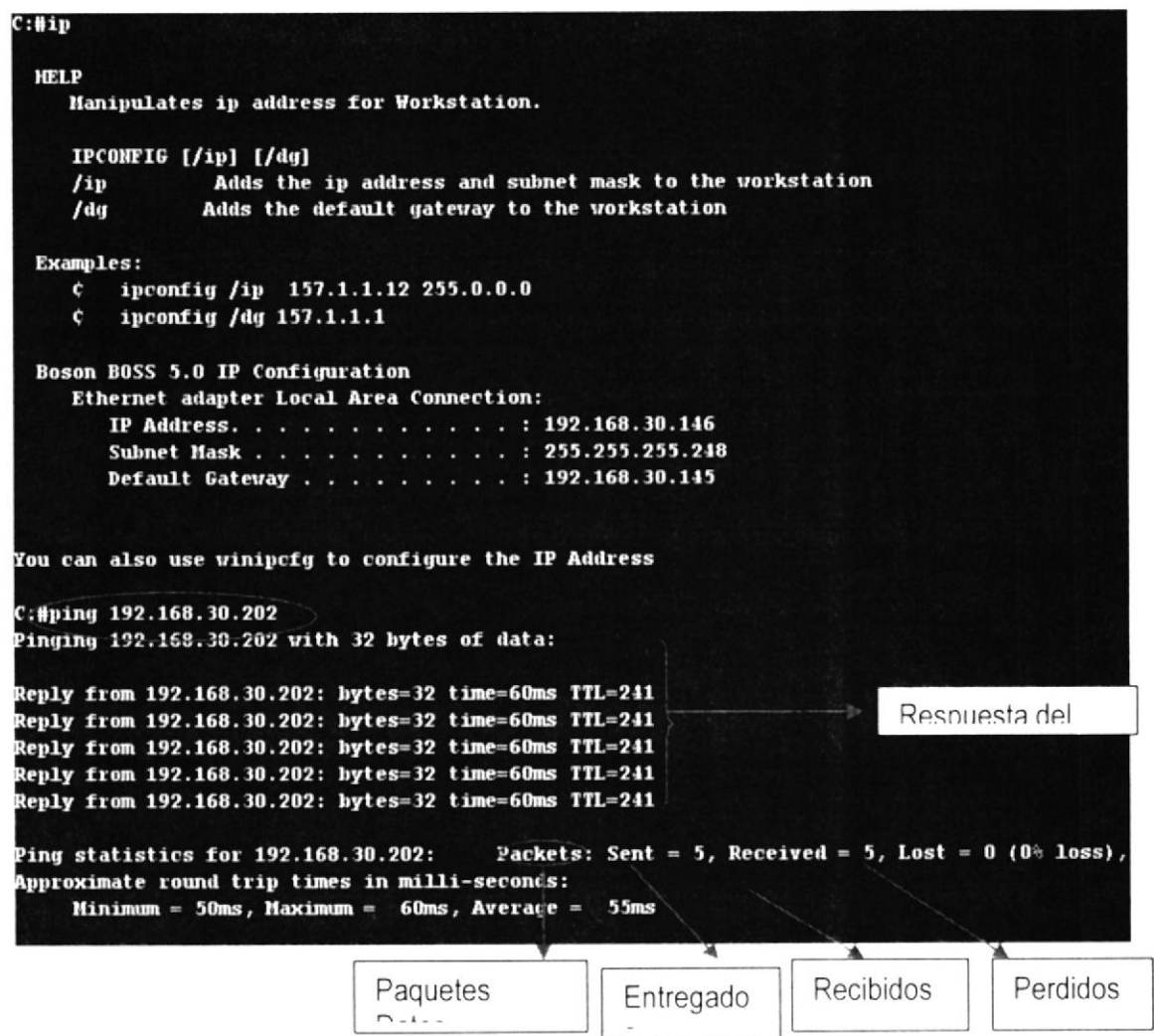


Figura 7-79: prueba de comunicación entre vlan 5.1



- ❖ La vlan servicio_Administrativo (192.168.30.162) que se encuentra en el Switch master hace ping a la vlan Recepción (192.168.30.210) que se encuentra en el Switch esclavo

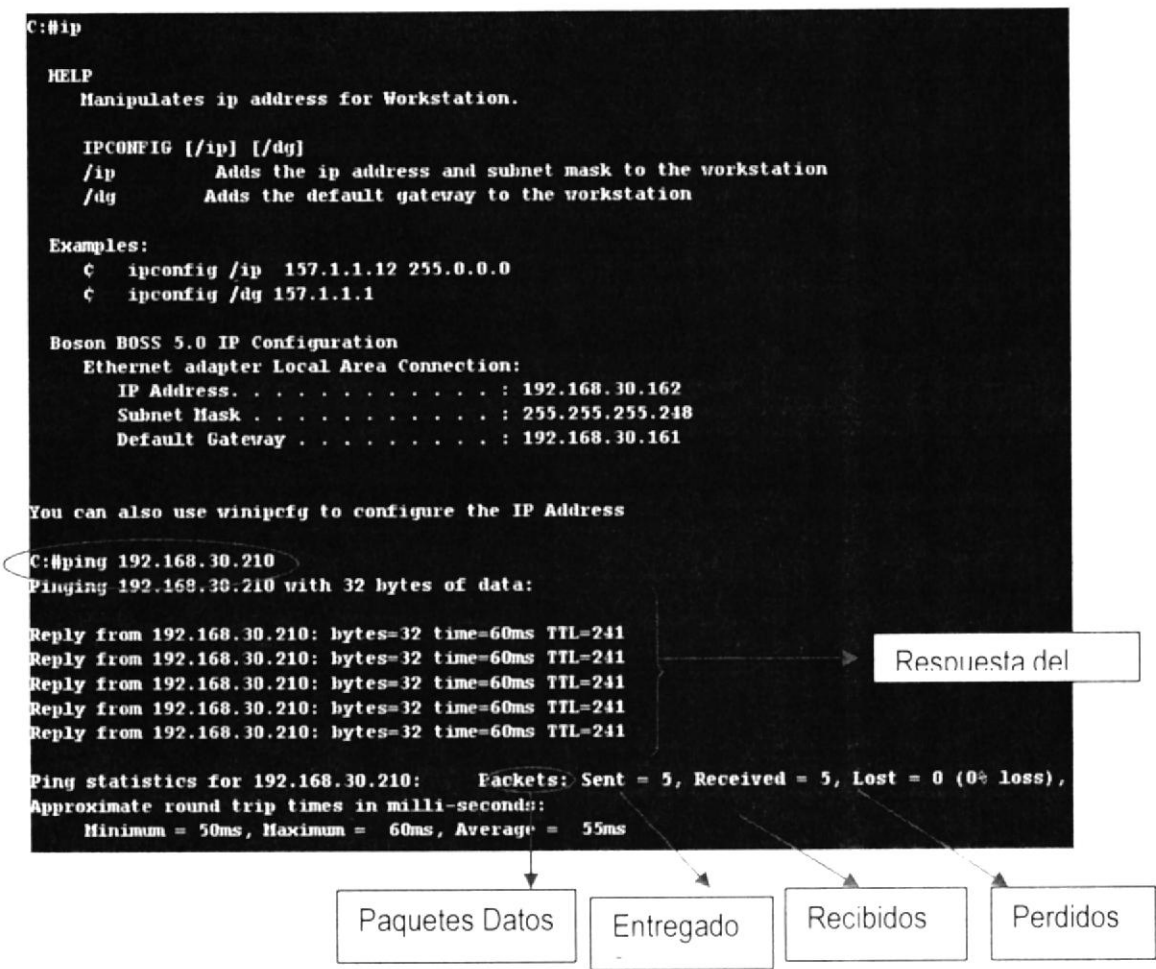


Figura 7-80: prueba de comunicación entre vlan 5.2



7.22.6.3.10. PRUEBAS DE COMUNICACIÓN ENTRE SWITCH ESCLAVO-MASTER

- ❖ La vlan Auditoría (192.168.30.186) que se encuentra en el Switch esclavo hace ping a la vlan calidad (192.168.30.154) que se encuentra en el Switch master

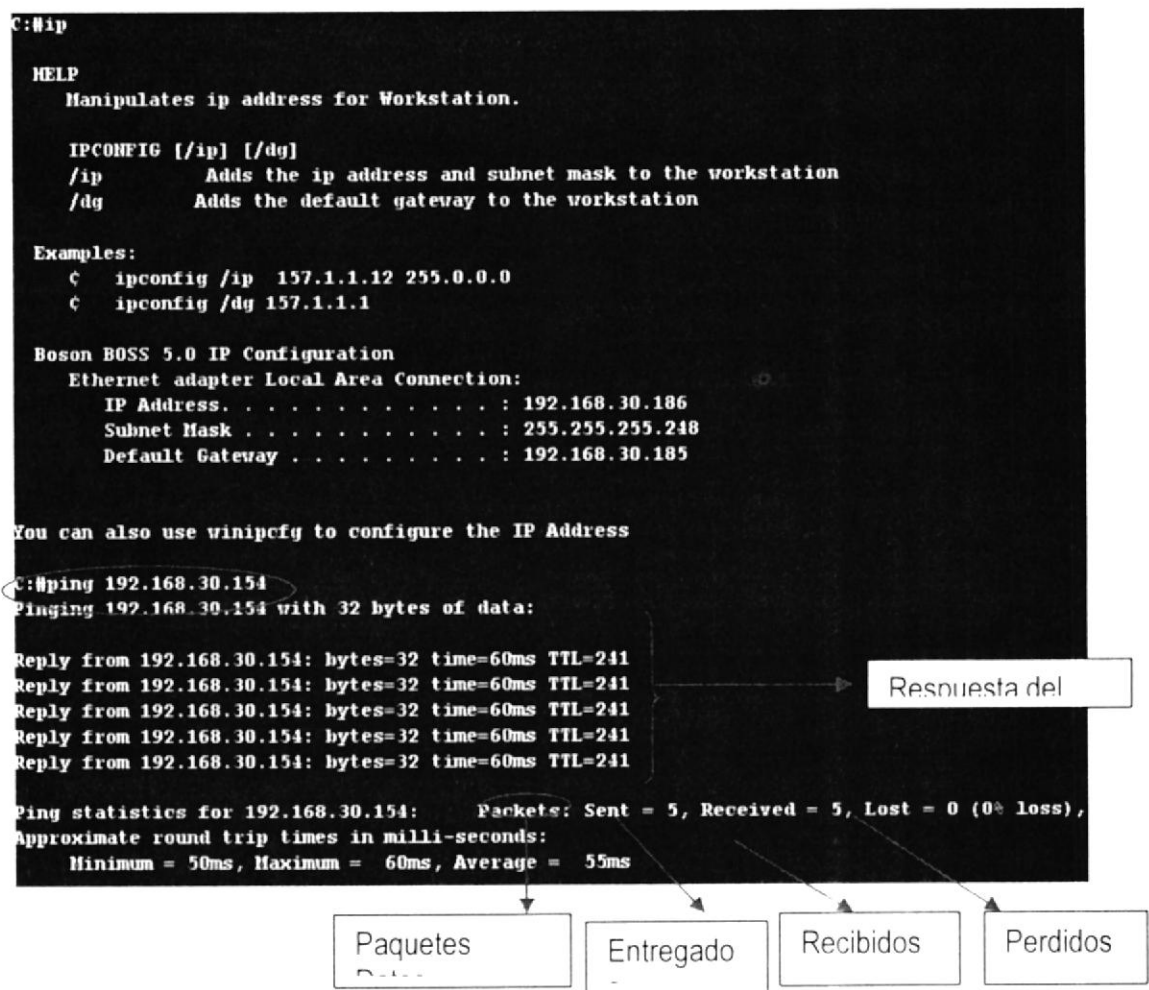


Figura 7-81: prueba de comunicación entre vlan 5.3



- ❖ La vlan producción_sistema (192.168.30.194) que se encuentra en el Switch esclavo hace ping a la vlan operación (192.168.30.170) que se encuentra en el Switch master

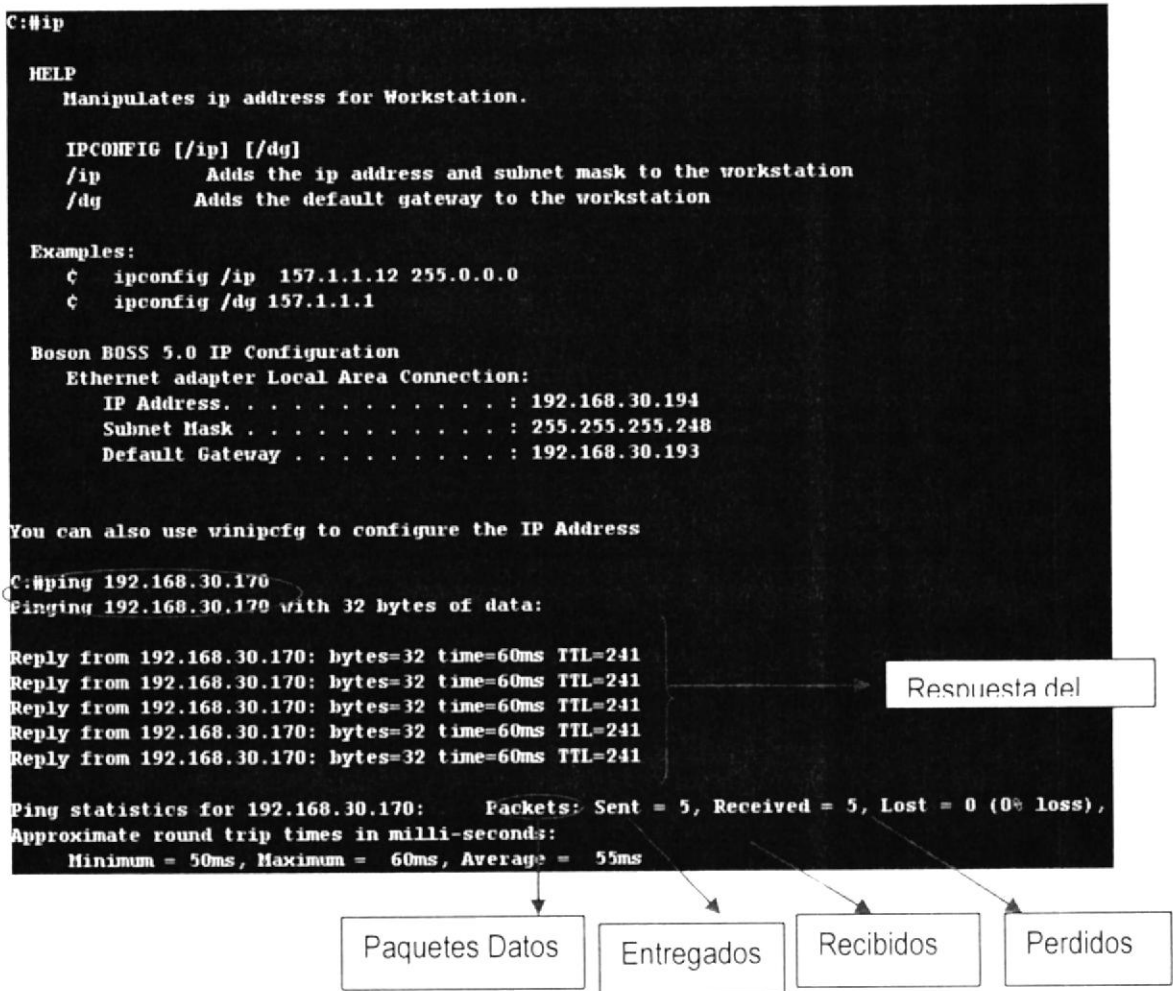


Figura 7-82: prueba de comunicación entre vlan 5.4



- ❖ La vlan recepción (192.168.30.202) que se encuentra en el Switch esclavo hace ping a la vlan RRHH (192.168.30.138) que se encuentra en el Switch master

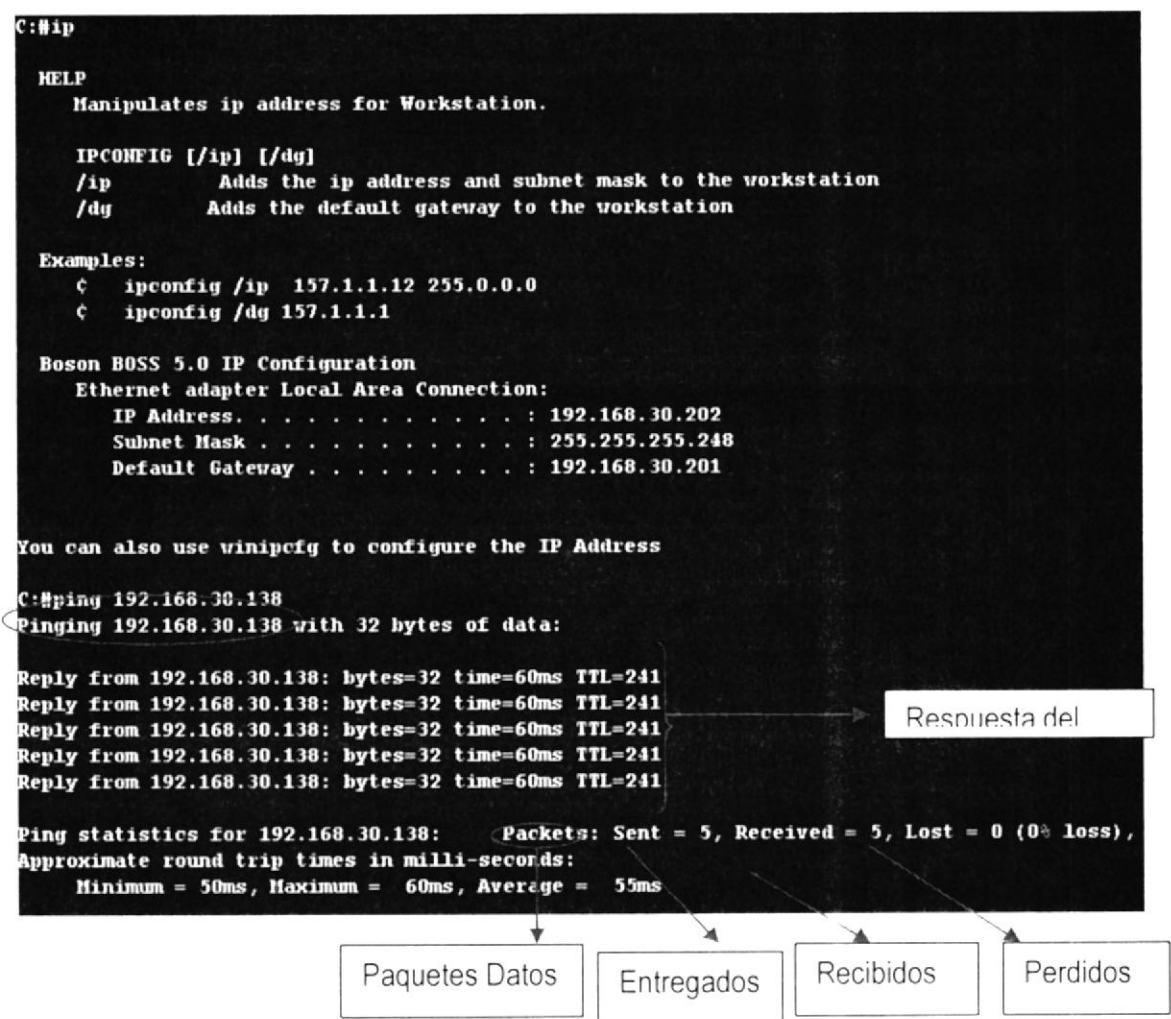


Figura 7-83: prueba de comunicación entre vlan 5.5





ANEXO

GLOSARIO DE TERMINOS

A. GLOSARIO DE PALABRAS TÉCNICAS

A

Ancho de Banda: La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también se usa para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

Arp: Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Comparar con RARP.

Asignación de direcciones: Técnica que permite que distintos protocolos interoperen traduciendo direcciones desde un formato a otro. Por ejemplo, al enrutar IP a través de una red Frame Relay, las direcciones IP se deben mapear a las direcciones Frame Relay de modo que los paquetes IP se puedan transmitir por la red. Ver también resolución de direcciones.



B

Banda Ancha: Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica. Comparar con banda ancha.

Broadcast: Envío de información en cualquier formato a más de un lugar de destino

Banda Base: Característica de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha. Ver la diferencia con banda ancha. Término utilizado en la WWW.

Bps: (Bits per Second). Medida que representa la rapidez con que los bits de datos se transmiten a través de un medio de comunicaciones. Por ejemplo: un módem de 28.8 Kbps es capaz de transferir 28.800 bits por segundo.

Bit: (Binary Digit ó Dígito Binario). Es un dígito en base 2, es decir, 0 ó 1. Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

Byte: Unidad de medida de la cantidad de información en formato digital. Usualmente un byte consiste de 8 bits. Un bit es un cero (0) o un uno (1). Esa secuencia de números (byte) pueden simbolizar una letra o un espacio (un carácter). Un kilobyte (Kb) son 1024 bytes y un Megabyte (Mb) son 1024 Kilobytes.

Bloqueo: En un sistema de conmutación, una condición en el que no hay ninguna ruta disponible para completar un circuito. El término también se usa para describir una situación en la que no se puede iniciar una actividad hasta que la otra no se haya completado.

C

Cable blindado: Cable que posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

Cable coaxial: Cable compuesto por un conductor cilíndrico exterior hueco que rodea un conductor de alambre interno-único. En la actualidad se usan dos tipos de cable coaxial en la LAN: cable de 50 ohmios, que se usa para la señalización digital, y cable de 75 ohmios que se usa para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro, sin embargo no es susceptible a la interferencia electromagnética y es capaz de brindar velocidades de datos más altas.

Cable neutro: Cable de circuito que se conecta a la conexión a tierra en la central de energía y en el transformador.

Cableado backbone: Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN. Ver cableado vertical.

Cableado de Categoría 1: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 1 se usa para comunicaciones telefónicas y no es adecuado para transmitir datos. Comparar con cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 2: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568By UTP.

Cableado de Categoría 3: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 3 se usa en las redes 10BASE-T y puede transmitir datos a velocidades de hasta 10 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 4: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 4 se usa en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 5: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 4. Ver también EIA/TIA-568By UTP.

Caché: Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso más rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los accesos a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

Canaleta decorativa: Tipo de canal montado en la pared que tiene una cubierta removible que se usa para admitir el cableado horizontal. La canaleta decorativa es lo suficientemente grande como para contener dos cables.

Canaleta: Un tipo de canal adosado a la pared que tiene una cubierta removible para dar apoyo al cableado horizontal. La canaleta es lo suficientemente grande como para contener varios cables.

Capa física: La Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Capa de control de enlace de datos: La Capa 2 del modelo de arquitectura SNA. Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

Capa de red: La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

Capa de transporte: La Capa 4 del modelo de referencia OSI. Esta capa es responsable de la comunicación confiable de red entre nodos finales. La capa de transporte suministra mecanismos para establecer, mantener y terminar los circuitos virtuales, detección y recuperación de errores de transporte y control del flujo de información

Capa de sesión: La Capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de capa de presentación.

Capa de servicios de presentación: La Capa 6 del modelo de arquitectura SNA. Esta capa suministra administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Corresponde aproximadamente a la capa de presentación del modelo OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control física, capa de servicios de transacción y capa de control de transmisión.

Capa de aplicación: La Capa 7 del modelo de referencia OSI. Esta capa suministra servicios a los procesos de aplicación (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de terminal) que están fuera del modelo OSI. La capa de aplicación identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos que se requieren para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos. Corresponde aproximadamente a la capa de servicios de transacción del modelo SNA. Ver también capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

Cliente: Nodo que solicita servicios a un servidor.

Colisión: En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

Cola: Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

Conector RJ: Conector macho registrado. Conectores estándar que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ

Costo: Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.

Consola: DTE a través del cual se introducen los comandos en un host.

Correo electrónico: Aplicación de red utilizada ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.

CSMA/CD: Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón).

Cliente: Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

Computador: Es un dispositivo electrónico compuesto básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

Contraseña ó Password: Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los Sistemas y recursos de la computadora.

CPU; (Central Processing Unit ó Unidad central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

Cuadro de Diálogo: Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

Cuadro de Texto: Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de diálogo, el cuadro de texto puede estar en blanco o contener texto.

Cursor: Símbolo en pantalla que indica la posición activa, generalmente titilante.

Muestra la posición en que aparecerá el próximo carácter a visualizar cuando se pulse la tecla.

CSU: Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con el loop telefónico digital local. A menudo se denomina, de forma conjunta con DSU, como CSU/DSU.

D

Db: Decibelios

Dominio: En Internet, una parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía

DCE: Equipo de comunicación de datos. Equipo de comunicación de datos (expansión EIA) o equipo de terminación de circuito de datos (expansión ITU-T). El dispositivo y las conexiones de una red de comunicaciones que abarca el extremo de la red de la interfaz usuario a red. El DCE proporciona una conexión física con la red, envía tráfico y suministra una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE. Comparar con DTE.

Descifrado: La aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando por lo tanto los datos a su estado original, no cifrado.

Dato: Son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

DTE: Equipo de terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario-red que actúa como origen de datos, destino de datos o ambas. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y por lo general usa señales de temporización

generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadores, traductores de protocolo y multiplexores.

Directorio: En D.O.S., una lista de nombres de archivo que contiene toda la información de los archivos almacenados. A partir de Windows 95 este término se reemplazó por CARPETA.

Dirección: Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico* (emáíl address); "IP" y (direccion de Internet) y "dirección hardware".

Dirección del Protocolo de Internet (dirección IP): Dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red con Protocolo de control de transmisión/Protocolo Internet (TCP/IP). Número único que consta de 4 partes separadas por puntos. Una dirección IP se suele representar en una notación decimal con puntos que indica cada octeto (ocho bits o un byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 172.16.255.255.

Cada computadora conectada a Internet tiene un único número de IP. Si la máquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem).

Disco Rígido: Unidad de almacenamiento permanente de información. Éste es el que guarda la información cuando apagamos la computadora. Aquí se guardan la mayoría de los programas y el sistema operativo. Su capacidad de almacenamiento se mide en Megabytes (Mb) o Gigabytes (Gb), en donde 1024 Mb = 1Gb.

Disquete: Dispositivo que puede insertarse y extraerse en una unidad de disco.

DNS: (Domain Name System ó Sistema de Nombres de Dominio). El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de éstos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes son: .COM (comercial - empresas), .EDU (educación, centros docentes), .ORG (organización sin ánimo de lucro), .NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejército USA). La mayoría de los países tienen un dominio propio. Por ejemplo, AR (Argentina) .PY (Paraguay), .US (Estados Unidos de América), .ES (España), .AU (Australia), etc.

Dominio: (Domain Name). Nombre único que identifica a un sitio de Internet. Los nombres de dominio tienen 2 o más secciones, separadas por puntos. La sección de la izquierda es la más específica, y la de la derecha, la más general.

Una computadora particular puede tener más de un nombre de dominio, pero un nombre de dominio se refiere únicamente a una PC.

Download ó descargar: En Internet es el proceso de transferir información desde un servidor de información a la propia PC.

Documentación: Manual escrito que detalla el manejo de un sistema o pieza de hardware.

Doble Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón) dos veces, sin desplazarlo. Esta acción sirve para ejecutar una determinada aplicación, como por ejemplo: inicializarla.

DSU: Unidad de servicio de datos. Dispositivo que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión como, por ejemplo, TI y El.

DVD: (Digital Versatile Disc ó Disco Versátil Digital). Disco que sirve para almacenar más datos de contenido digital, como música o video, que un CD. Un DVD guarda un mínimo de 4.7 Gigabytes (el tamaño de una película de cine).

E

EI: Estándar Europeo equivalente al americano TI. Los circuitos EI y TI. Los dos usan canales de 64 Kbps, pero el TI tiene 24 mientras que el EI tiene 32 canales.

EIA/TIA-568: Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

Encapsulamiento: El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

Emulación de terminal: Aplicación de red en la que un computador ejecuta software que la hace aparecer ante un host remoto como una terminal conectada directamente.

Enrutamiento: Proceso para encontrar una ruta hacia un host destino. El enrutamiento en redes de gran tamaño es muy complejo dada la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ethernet: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3. Ver también 10BASE2, 10BASE5, 10BASE-F, 10BASE-T, 10Broad36 e IEEE 802.3.

Elemento de Pantalla: Partes que constituyen una ventana o cuadro de diálogo como por ejemplo: la barra de título, los botones de "Maximizar" y "Minimizar", los bordes de las ventanas y las barras de desplazamiento.

Escritorio: Fondo de la pantalla sobre la cual aparecen ventanas, iconos y cuadros de diálogo.

Estación de trabajo: Computador de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. Llamadas así para distinguirlas de los que se conocen como servidores.

Expandir: Mostrar los niveles de directorio ocultos del árbol de directorios. Con el administrador de archivos es posible expandir un solo nivel de directorio, una rama del árbol de directorio o todas las ramas a la vez.

Explorador: Llamado también explorador Web. Interfaz cliente que permite al usuario ver documentos HTML en el World Wide Web, en otra red o en su propio equipo; seguir los hipervínculos y transferir archivos. Un ejemplo es Microsoft Internet Explorer.

Extensión: Está compuesto por un punto y un sufijo de hasta tres caracteres situados al final de un nombre de archivo. La extensión suele indicar el tipo de archivo o directorio.

F

Fibra monomodo: Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único. Ver también fibra multimodo.

Fibra multimodo: Fibra óptica que permite la propagación de múltiples frecuencias de luz.

Firewall: Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red

privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Fluctuación de fase: Distorsión analógica de la línea de comunicación provocada por la variación de una señal de sus posiciones de temporización de referencia. La fluctuación de fase puede provocar la pérdida de datos, especialmente a altas velocidades.

Flujo de datos: Todos los datos que se transmiten a través de la línea de comunicaciones en una sola operación de lectura o escritura. ,

Frecuencia: Cantidad de ciclos, medidos en hercios, de una señal de corriente alterna por unidad de tiempo.

FTP: Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP, que se usa para transferir archivos entre nodos de la red. El FTP se define en la RFC 959.

Full dúplex: Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora. -

G

Gateway: En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función, y gateway se refiere a un dispositivo con fines especiales que ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra.

Sateway fronterizo: Router que se comunica con routers de otros sistemas autónomos.

Giga: Prefijo que indica un múltiplo de 1.000 millones, o sea 10⁹. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 1.073.741.824.

Grupo de trabajo: Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

H

Hardware: Son todos los componentes físicos que componen una PC.

Hercio: Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

Hexadecimal: Base 16. Representación numérica que usa los dígitos 0 a 9, con su significado habitual, y las letras A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, luego $16A_2 = 256$, etc. ;-.-;

Host: Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

HTML: (HyperText Markup Language). Lenguaje utilizado para crear los documentos de hipertexto que se emplean en la WWW. Los documentos HTML son simples archivos de texto que contienen instrucciones (llamadas tags) entendibles por el Navegador (Browser).

HTTP: (HyperText Transport Protocol). Protocolo utilizado para transferir archivos de hipertexto a través de Internet. Requiere de un programa "cliente" de HTTP en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la WWW.

Hub: Dispositivo de hardware o software que contiene módulos de red y equipo de internetwork múltiples, independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen, las señales que se envían a través de ellos).



I

IEEE: Instituto de ingenieros eléctricos y electrónicos. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN del IEEE son los estándares de LAN predominantes en el mundo actual

IEEE 802.1: Especificación del IEEE que describe un algoritmo que evita los loops de capa dos mediante la creación de un spanning tree. El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo de Digital y el algoritmo IEEE 802.1 no son exactamente los mismos, ni tampoco son compatibles.

IEEE 802.12: Estándar LAN del IEEE que especifica la capa física y la subcapa MAC de la capa de enlace de datos. El IEEE 802.12 usa el esquema de acceso a los medios de prioridad de demanda a 100 Mbps a través de una diversidad de medios físicos. Ver también IOOVB-Any LAN.

IEEE 802.2: Protocolo LAN del IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 administra errores, entramado, control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se usa en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3: Protocolo LAN del IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 usa acceso CSMA/CD a diversas velocidades sobre diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican las implementaciones de Fast Ethernet. Las variantes físicas de la especificación IEEE 802.3 original incluyen 10BASE2, 10BASE5, 10BASE-F, 10BASE-T y 10Broad36. Las variantes físicas de Fast Ethernet incluyen 100BASE-T, 100BASE-T4y 100BASE-X.

Icono: Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc.

IDF: Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

Impresora: Dispositivo de salida, cuya funcionalidad es transcribir/pasar un documento (imagen y/o texto) desde el ordenador (procesador de textos, bloc

de notas, visor de imágenes, etc.) a un medio físico, generalmente papel, mediante el uso de cinta, cartuchos de tinta o también con tecnología láser.

Impresora de Inyección a tinta: Crean imágenes directamente sobre el papel al rociar tinta a través de una pequeñas boquillas, su calidad de impresión es bastante alta.

Impresora Predeterminada: Impresora que se utiliza si se elige el comando Imprimir, no habiendo especificado antes la impresora que se desea utilizar. Sólo puede haber una impresora predeterminada, que debe ser la que se utilice con mayor frecuencia.

Información: Es lo que se obtiene del procesamiento de datos, es el resultado final.

Informática cliente-servidor: Término que se usa para describir los sistemas de red informáticos distribuidos (de procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: cliente (front end) y servidor (back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos actuales.

Internetwork: Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red.

IP: Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad. Documentado en la RFC 791.

IP access-group: Comando que enlaza una lista de acceso existente con una interfaz de salida.

IP host: Comando que se usa para crear una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.

IP multicast: Técnica de enrutamiento que permite que el tráfico IP se propague desde un origen hacia un número de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, se envía un paquete a un grupo de multicast que se identifica mediante una sola dirección de grupo de destino IP.

IPX: Intercambio de paquetes de internetworking. Protocolo de capa de red (Capa 3) de NetWare que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

Interfaz: Una conexión e interacción entre hardware, software y usuario, es decir, como la plataforma o medio de comunicación entre usuario o programa.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

Intranet: Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno.

ISO: Organización Internacional de Normalización. Organización internacional que es responsable por una amplia gama de estándares, incluyendo aquellos relevantes para el networking. ISO desarrolló el modelo de referencia OSI, un modelo de referencia de networking sumamente popular.

J

Jumper: Término que se usa para los cables de interconexión que se encuentran en el armario de cableado.

K

Kbps: (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit esta formado por mil bits.

Kilobyte: Es el equivalente a 1024 bytes.



L

LAN: Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido. Comparar con MAN y WAN.

Latencia: Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir también sucede en el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

LED: Diodo emisor de luz. Dispositivo semiconductor que emite luz producida por la conversión de energía eléctrica. Las lámparas de estado en los dispositivos de hardware generalmente son LED.

Línea de acceso telefónico: Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

Línea de comunicación: Enlace físico (como, por ejemplo, un cable o circuito de teléfono) que conecta uno o más dispositivos con uno o más dispositivos.

Línea de mira: Característica de determinados sistemas de transmisión como, por ejemplo, los sistemas láser, de microondas e infrarrojos, en los que no puede existir ninguna obstrucción en la ruta directa entre el transmisor y el receptor.

Línea dedicada: Línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir. Ver también línea arrendada.

Lista de acceso: Lista que mantienen los routers Cisco para controlar el acceso hacia o desde el router para diversos servicios (por ejemplo, para evitar que los paquetes que tienen una determinada dirección IP salgan de una interfaz específica del router).

LSA: Publicación de estado de enlace. Paquete de broadcast que usan los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de la ruta. Los routers receptores usan las LSA para mantener sus tablas de enrutamiento

Login: Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del password, el login no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

M

MAC: Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

MICIP: Protocolo de capa de red que encapsula paquetes IP en DDS o transmisión a través de AppleTalk.

Malla: Topología de red en la que los dispositivos se organizan de una manera administrable, segmentada, con varias interconexiones, a menudo redundantes, ubicadas estratégicamente entre nodos de la red. Ver también malla completa y malla parcial.

Malla completa: Término que describe a una red en la que los dispositivos están organizados en una topología de malla, en la que cada nodo de la red tiene un circuito físico o un circuito virtual que lo conecta a todos los otros nodos de la red. Una malla completa brinda una gran cantidad de redundancia pero, dado que su implementación puede resultar excesivamente cara, generalmente se la reserva para los backbones de la red. Ver también malla y malla parcial.

MAN: Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

MAP: Protocolo de automatización de fabricación. Arquitectura de red creada por General Motors para satisfacer las necesidades específicas las instalaciones fabriles. El MAP especifica una LAN de transmisión de tokens similar a IEEE 802.4. Ver también IEEE 802.4.

Mapa de cableado: Característica suministrada por la mayoría de los analizadores de cable. Se usa para probar las instalaciones de cableado de par trenzado, y muestra cuáles hilos están conectados a cuáles pines, en conectores macho y hembra.

Mapa de topología: Herramienta para administrar un switch ATM LightStream 2020 que examina una red y muestra el estado de sus nodos y enlaces troncales. El mapa de topología es una aplicación basada en HP OpenView que se ejecuta en un NMS.

Máscara de red: Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

Máscara wildcard: Cantidad de 32 bits que se usan de forma conjunta con una dirección IP para determinar cuáles son los bits de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

MDF: Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

Megabyte (MB): 1.048.576 bytes; 1.024 Kilobytes.

Megahertz: Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

Memoria RAM: Memoria de acceso aleatorio cuyo contenido permanecerá presente mientras el computador permanezca encendido.

Memoria ROM: Memoria de sólo lectura. Chip de memoria que sólo almacena permanentemente instrucciones y datos de los fabricantes.

Microonda: este enlace esta constituido por dos transceptores de radio provistos de antenas parabólicas que se apuntan directamente entre si. La radio puede transportar transmisiones punto a punto de muchos anchos de banda. Su alcance varia según el tamaño de la antena, el clima en la zona y la magnitud de la potencia emitida contemplando todos estos conjuntos la señal puede llegar hasta 80 Km.

Módem: (Modulator, Demodulator). Dispositivo que se conecta a la computadora y a la red telefónica y que permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

Mouse: Permite convertir el movimiento de la mano en desplazamiento de un cursor sobre la pantalla.

Multicast: la multidifusión (multicast) permite que grupos de usuarios seleccionados reciban la misma transmisión de datos en una red los cuales están identificados por una única dirección de grupo de destino IP.



N

Navegador de Web: Aplicación de cliente de hipertexto basada en GUI como, por ejemplo, Mosaic, que se usa para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a través de la WWW e Internet. Ver también hipertexto, Internet, Mosaic y WWW.

NBP: Protocolo de enlace de denominación. Protocolo AppleTalk de nivel de transporte que convierte un nombre dado en forma de una cadena de caracteres en una dirección de internetwork.

NET: Título de entidad de red. Direcciones de red, definidas por la arquitectura de red ISO.

NetBIOS: Sistema básico de entrada/salida de red. API que usan las aplicaciones de una LAN IBM para solicitar servicios de procesos de red de nivel inferior. Estos servicios pueden incluir establecimiento y terminación de sesión y transferencia de información

NetWare: NOS distribuido de uso generalizado desarrollado por Novell. Suministra acceso remoto transparente a archivos, y muchos otros servicios de red distribuida.

Networking: Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NIC: Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

NOS: Sistema operativo de red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos. Los ejemplos de NOS incluyen LAN Manager, NetWare, NFS y VINES.

Número de host: Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

Número de red: Parte de una dirección IP que especifica la red a la que pertenece el host.

Número de saltos: Métrica de enrutamiento que se usa para medir la distancia entre un origen y un destino. El RIP usa el número de saltos como su única métrica.

NVRAM: RAM no volátil. RAM que retiene su contenido cuando una unidad se apaga. En los productos Cisco, la NVRAM se usa para guardar la información de configuración.

Nodo: En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma.

Nombre de usuario: La secuencia de caracteres que lo identifica. Al conectarse a una computadora, generalmente necesita proporcionar su nombre y contraseña de usuario. Esta información se usa para verificar que la persona está autorizada para usar el Sistema.



O

Operador de red: Persona que monitorea y controla una red de forma continua, ejecutando tareas como

Oscilación: Señal secundaria superpuesta a la onda de 60 Hz. Tiene una magnitud que varía entre el 15% y el 100% del voltaje normal de la línea de alimentación. Ver sobrevoltaje, pico y baja de voltaje.

OSI: Interconexión de sistemas abiertos. Programa internacional de normalización creado por la ISO y la UIT-T para desarrollar estándares de interconexión que faciliten la interoperabilidad de equipos de múltiples proveedores.

OSINET: Asociación internacional diseñada para promover OSI en las arquitecturas de los proveedores.

OSPF: Versión abierta del algoritmo "Primero la ruta libre más corta". Algoritmo de enrutamiento IGP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad Internet. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga. El OSPF deriva de una versión inicial del protocolo ISIS.

P

PAD: Ensamblador/desensamblador de paquetes. Dispositivo que se usa para conectar dispositivos simples (como terminales de modo de carácter) a una red, los cuales no admiten toda la funcionalidad de un protocolo específico. Los PAD almacenan los datos en el búfer de los PAD y ensamblan y desensamblan los paquetes que se envían a dichos dispositivos finales.

Panel de conexión: Conjunto de ubicaciones de pin y puertos que se puede montar en un bastidor o una consola de pared en el armario de cableado. Los paneles de conexión actúan como conmutadores que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

Paquete de choque: Paquete que se envía al transmisor para informarle que hay congestión y que debe reducir su velocidad de envío.

Par trenzado: Medio de transmisión de relativa baja velocidad compuesto por dos cables aislados dispuestos en un patrón en espiral regular. Los cables pueden ser blindados o no blindados. El uso del par trenzado es común en aplicaciones de telefonía y es cada vez más común en las redes de datos. Ver también STP y UTP.

Paradiafonía: Energía de interferencia transferida de un circuito a otro.

PBX: Central telefónica privada. Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas y públicas.

PCI: Información de control de protocolo. Información de control que se agrega a los datos del usuario para formar un paquete OSI.

Pila de protocolo: Conjunto de protocolos de comunicación relacionados que operan de forma conjunta y, como un grupo, cumplen con la comunicación en

alguna o en las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo y, a menudo, un solo protocolo de la pila se dirige a una cantidad de capas a la vez. El TCP/IP es un protocolo de pila típico.

Ping: Abreviatura para Packet Internet Groper o Packet Inter-network Groper, una utilidad que se usa para determinar si una dirección IP en particular está disponible. Funciona enviando un paquete a la dirección especificada y esperando una respuesta. El PING se usa principalmente para diagnosticar las fallas de las conexiones de Internet.

Plan de distribución: Diagrama simple que indica dónde están ubicados los tendidos de cable y la cantidad de habitaciones hacia las que se dirigen.

POP: Punto de presencia. Punto de presencia es el punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y el servicio de distribución principal del edificio.

Portadora: Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos. Ver también modulación.

POST: Autocomprobación de encendido. Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando ese dispositivo se enciende.

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

Puerto: Interfaz de un dispositivo de internetworking (como, por ejemplo, un router) En terminología ip, un proceso de capa superior que recibe información de las capas Inferiores. Un conector hembra de un panel de conexión el cual acepta el mismo tamaño de conector que el de un rj45. Los cables de conexión se usan en estos puertos para realizar interconexiones entre los computadores conectados al panel. Es esta interconexión conexión la que permite la operación de la lan.

Página Web: Documento de World Wide Web. Una página Web suele consistir en un archivo HTML, con sus archivos asociados de gráficos y secuencias de comandos, en un directorio determinado de un equipo concreto (y, por tanto, identificable mediante una dirección URL).

Periféricos: Cualquier dispositivo de hardware conectado a una computadora.

Pixel: (PICTure cELL). Es la parte más pequeña de una pantalla de video, constituido por uno o más puntos que se consideran como una unidad. Es por tanto, el bloque de construcción de imágenes.

Protocolo: Método por el que los equipos se comunican en Internet. El protocolo más común en el World Wide Web es HTTP. Otros protocolos de Internet incluyen FTP, Gopher y telnet. El protocolo forma parte de la dirección URL completa de un recurso.

Proveedor: Institución o empresa que provee acceso a uno o varios servicios de Internet.

R

RAM: Memoria de acceso directo aleatorio. Memoria volátil que puede ser leída y escrita por un microprocesador.

Red: Conjunto de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red de conexión única: Red que tiene una sola conexión con un router

Redireccionar: Parte de los protocolos ICMP y ES-IS que permiten que un router le indique a un host que puede ser más efectivo usar otro router.

Redistribución: Permitir que la información de enrutamiento detectada a través de un protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento. A veces denominada redistribución de ruta.

Redundancia: En internetworking, la duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan ejecutar el trabajo de aquellos que han fallado. Ver también sistema redundante.

Rendimiento: Velocidad de la información que llega a, y posiblemente atraviesa, un punto particular de un sistema de red.

Repetidor: Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red.

Retardo: El tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. También, el tiempo que se requiere para mover un paquete desde el origen hacia el destino a través de una ruta específica.

RF: Radiofrecuencia. Término genérico que se usa para referirse a frecuencias que corresponden a transmisiones radioeléctricas. Las redes de televisión por cable y de banda ancha usan tecnología RF.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red.

Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

RIP: Protocolo de información de enrutamiento. IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet.

RMON: Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitoreo remoto de los dispositivos conectados a la red.

ROM: Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.

Ruta estática: Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

Ruta por defecto: Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

S

Segmento: La sección de una red limitada por puentes, routers o switches. Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

SMTP: Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico

Sondeo: Método de acceso en el que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

Switch: Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI:



Switch LAN: Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches LAN envían tráfico basándose en las direcciones MAC. Esta variedad de switch LAN a veces se denomina switch de trama. Los switches LAN a menudo se clasifican de acuerdo con el método que usan para enviar tráfico: conmutación de paquetes por método de corte y conmutación de paquetes por almacenamiento y envío. Los switches multicapas son un subconjunto inteligente de los switches LAN.

Servidor: Computadora o programa que brinda un servicio específico al "cliente", que se ejecuta en otras computadoras. El término puede referirse tanto a un equipo de una red que envía archivos o ejecuta aplicaciones para otros equipos de la red; el software que se ejecuta en el equipo servidor y que efectúa la tarea de servir archivos y ejecutar aplicaciones; o bien, en la programación orientada a objetos, un fragmento de código que intercambia información con otro fragmento de código cuando se pide.

SO: (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software: Todos los componentes no físicos de una PC (Programas).



T

TI: Servicio de portadora de WAN digital. TI transmite datos con formato DS-1 a 1.544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o B8ZS. Comparar con El. Ver también AMI, B8ZS y DS-1.

Tabla de enrutamiento: Tabla que se guarda en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas hacia destinos de red en particular y, en algunos casos, las métricas asociadas con esas rutas.

TFTP: Protocolo de Transferencia de Archivos Trivial. Versión simplificada del FTP que permite que los archivos se transfieran desde un computador a otra a través de una red.

Terminal: Dispositivo simple en el que los datos se pueden introducir o recuperar desde una red. Generalmente, las terminales tienen un monitor y un teclado pero no tienen ningún procesador ni unidad de disco local.

Topología: Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

Topología de anillo: Topología de red que consta de un conjunto de repetidores conectados entre sí mediante enlaces de transmisiones unidireccionales para formar un solo bucle cerrado. Cada estación de la red se conecta a la red en el repetidor. Aunque lógicamente están organizadas en anillo, las topologías de anillo a menudo están organizadas en una estrella de bucle cerrado.

Topología de bus: Arquitectura LAN lineal en la que las transmisiones de las estaciones de red se propagan a lo largo del medio y son recibidas por todas las otras estaciones.

Topología en árbol: Topología LAN similar a la topología bus, salvo que las redes en árbol pueden tener ramificaciones con múltiples nodos. Las transmisiones desde una estación atraviesan la longitud del medio y son recibidas por todas las otras estaciones.

Topología en estrella: Topología LAN en la que los puntos de terminación de una red se conectan a un switch central común mediante enlaces punto a punto. Una topología de anillo que está organizada como estrella implementa una estrella de loop cerrado unidireccional en lugar de enlaces punto a punto.

Topología en estrella jerárquica: Topología en estrella extendida en la que un hub central se conecta a través de cableado vertical con otros hubs que dependen del mismo.

Transceiver: Unidad de conexión al medio. Dispositivo que se usa en las redes Ethernet e IEEE 802.3 que suministra la interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que se puede incorporar a una estación o puede ser un dispositivo individual, ejecuta funciones de capa física, incluyendo la conversión de datos digitales desde la interfaz Ethernet, detección de colisiones e inyección de bits en la red.

Tunneling: Arquitectura que está diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.

Tarjeta de Interfaz de Red: (NIC). Dispositivo a través del cual computadoras de una red transmiten y reciben datos.

TCP/IP: (Transmisor Control Protocol/Internet Protocol). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

Telnet: Protocolo que permite al usuario de Internet conectarse y escribir comandos en un equipo remoto vinculado a Internet como si el usuario estuviera utilizando un terminal de texto conectado directamente al equipo. Forma parte del conjunto de protocolos TCP/IP.

Tiempo Real: Método para procesar la información en cuanto se recibe.

U

Unicast: En redes conmutadas ethernet, transferencia de archivos/paquetes entre dos entidades. Una difusión única puede iniciarla un servidor a una estación de trabajo, una estación a un servidor, una estación a una impresora o cualquier otra unidad única hacia otra entidad

UPS: (Uninterruptible Power Supply ó Suministro de Energía Ininterrumpida). Es un estabilizador electrónico que está preparado para suplir al computador cuando se presenten caídas de energía o cambios de voltaje.

URL: (Universal Resource Locator ó Localizador de Recursos Universal). Identifica de manera única la ubicación de un equipo, directorio o archivo en Internet. La dirección URL también indica el protocolo de Internet apropiado, como HTTP o FTP. Por ejemplo: <http://www.microsoft.com>.

USB: Tecnología que facilita la conexión de periféricos a la computadora. Esta reconoce automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo, ya que se conecta a la parte trasera de la PC a un enchufe especial (puerto USB). La tarjeta madre debe tener esta tecnología en su CHIPSET para poder conectar dispositivos de este tipo.

UTP: Cable de para trenzado no apantallado, lo que significa que no tiene envoltura alrededor del grupo de conductores. Estos cables se usan principalmente en redes de voz y datos

Usuario: Cualquier individuo que interactúa con el computador a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con el computador a nivel profesional.

V

Vector: Segmento de datos de un mensaje SNA. Un vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

Virtualización: Proceso que se usa para implementar una red basada en segmentos de red virtuales. Los dispositivos se conectan a segmentos virtuales independientemente de su ubicación física y de su conexión física con la red.

VLAN: LAN virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.

VLSM: Máscara de subred de longitud variable. Capacidad de especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

VTP: Protocolo de terminal virtual. Aplicación ISO para establecer una conexión de terminal virtual a través de una red.

Virus: Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan, se propagan a través de cualquier medio de almacenamiento, o a través de la LAN, o de la misma Internet.

W

WAN: Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

WorkGroup Director: Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroup Director se ejecuta en estaciones de trabajo UNIX, ya sea como una aplicación independiente o integrada con otra plataforma de administración de red basada en SNMP, brindando un sistema de gestión poderoso y transparente para los productos de grupo de trabajo de Cisco.

WWW: World Wide Web. Gran red de servidores de Internet la cual suministra servicios de hipertexto y otros a terminales que ejecutan aplicaciones de clientes como, por ejemplo, un navegador de Web. Ver también navegador de Web.

X

X Windows: Protocolo que interconecta estaciones de trabajo de interfaz gráfica de usuario con programas servidores de aplicaciones que utiliza TCP/IP.

Z

Zona de autoridad: Asociada con DNS, la zona de autoridad es una sección del árbol del nombre de

