

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



TÓPICO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ANÁLISIS DE SOPORTE DE MICROCOMPUTADORES

TEMA:

**ADMINISTRACIÓN Y SEGURIDADES DE
REDES “DEVIESCORD S.A.”**

MANUAL DE USUARIO

AUTORES:

**PASCUAL MUJICA GONZÁLEZ
ALFREDO BORBOR ROSALES**

DIRECTOR:

ING. ROCKY BARZOLA GILCES

**AÑO
2010**

ESCUELA SUPERIOR POLITECNICA DEL LITORAL



**TÓPICO DE GRADUACIÓN
PREVIO A LA OBTENCIÓN DE TITULO DE
ANÁLISIS DE SOPORTE DE
MICROCOMPUTADORES**

**TEMA:
ADMINISTRACIÓN Y SEGURIDADES DE
REDES “DEVIESCORD S.A”**

MANUAL DE USUARIO

**AUTORES:
PASCUAL MUJICA GONZÁLEZ
ALFREDO BORBOR ROSALES**

**DIRECTOR:
ING. ROCKY BARBOZA GILCES**

**AÑO
2010**



AGRADECIMIENTO

Mis más sinceros agradecimientos a mi familia, que me apoyaron para la culminación de este objetivo. Un agradecimiento especial a mis padres Sr Andrés Mujica y Sra. Nancy González por ser las personas que me han brindado siempre su apoyo, ya que gracias a su esfuerzo, trabajo y consejos soy la persona que soy en la vida.

Gracias a Dios por darme esta Familia.

Sr.Pascual Mujica González.



BIBLIOTECA
CAMPUS
PEÑAS

AGRADECIMIENTO

Mis más sinceros agradecimientos a todos y cada uno de los miembros de mi familia que de una u otra forma me han prestado su ayuda, motivación, y han sabido comprenderme en los momentos difíciles por los que pasa cualquier persona. Así mismo a mis compañeros que han sabido ganarse mi respeto y admiración y que pasaron a ser además mis amigos fuera de la institución educativa.

Gracias a Dios por haberme bendecido con una gran familia y amigos con los cuales podre contar siempre.

Sr. Alfredo Borbor Rosales



BIBLIOTECA
CAMPUS
PEÑAS

DEDICATORIA

Todo el esfuerzo expresado en este proyecto se los dedico a mis padres, compañeros y profesores, ya que gracias a la influencia de cada uno de ellos, se logro culminar este objetivo

Sr. Pascual Mujica González



BIBLIOTECA
CAMPUS
PEÑAS

DEDICATORIA

El esfuerzo expresado en este proyecto va dedicado a mis padres Sr. Alfredo Borbor Pozo y Sra. Martha Rosales Enriquez, por estar en los buenos y malos momentos que ha sabido atravesar mi carrera.

Sr. Alfredo Borbor Rosales



BIBLIOTECA
CAMPUS
PEÑAS

DECLARACIÓN EXPRESA

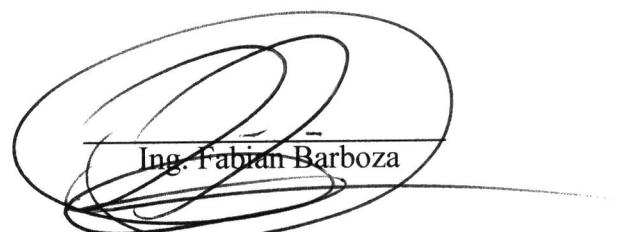
La responsabilidad por los hechos, ideas y doctrinas expuestas en este Proyecto de Graduación nos corresponden exclusivamente; y el patrimonio intelectual del mismo al ***EDCOM (Escuela de Diseño y Comunicación Visual)*** de la Escuela Superior Politécnica del Litoral.

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



BIBLIOTECA
CAMPUS
PEÑAS

FIRMA DE LOS MIEMBROS DEL TRIBUNAL DE GRADO

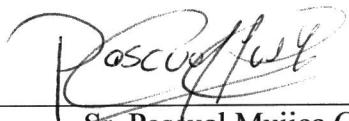


Ing. Fabian Barboza

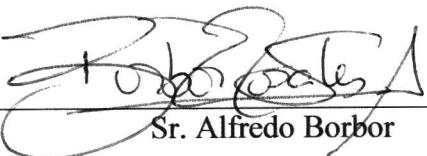


Delegado

FIRMA DE LOS AUTORES DEL TÓPICO



Sr. Pascual Mujica González



Sr. Alfredo Borbor

TABLA DE CONTENIDO

CAPÍTULO 1

1	GENERALIDADES.....	1
1.1	INTRODUCCION	1
1.2	OBJETIVO DEL MANUAL	1
1.3	A QUIEN VA DIRIGUIDO ESTE MANUAL	1
1.4	QUE SE DEBE CONOCER	1
1.5	ORGANIZACIÓN DEL CONTENIDO DE ESTE MANUAL.....	1

CAPÍTULO 2

2	SITUACION ACTUAL.....	2
2.1	ANTECEDENTES	2
2.1.1	MISIÓN	2
2.1.2	VISIÓN.....	2
2.2	AREAS ADMINISTRATIVAS.....	3
2.3	INFRAESTRUCTURA LAN	4
2.4	CARACTERISTICAS DE LOS SERVIDORES	7
2.5	CARACTERISTICAS DE LAS ESTACIONES DE TRABAJO.....	8
2.6	MEDIOS DE COMUNICACIÓN	9
2.6.1	ALAMBRICOS	9
2.6.2	INALÁMBRICOS.....	9
2.7	DISPOSITIVOS DE COMUNICACIÓN	10
2.7.1	CONMUTACIÓN.....	10
2.7.2	ENRUTAMIENTO.....	11
2.8	INFRAESTRUCTURA WAN	12
2.9	COMUNICACIÓN WAN MATRIZ-SUCURSAL.....	12
2.9.1	A NIVEL DE DISPOSITIVOS DE COMUNICACIÓN	12
2.10	RECEPCIÓN DE SERVICIO DE INTERNET.....	13
2.11	GRAFICO RECEPCIÓN DE SERVICIO DE INTERNET	13
2.12	SEGURIDADES.....	14
2.13	FIREWALL.....	14
2.14	UBICACIÓN FÍSICA DEL FIREWALL	15
2.15	PROBLEMAS ENCONTRADOS.....	16



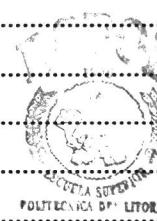
CAPÍTULO 3

3.1	SOLUCIÓN PROPUESTA	BIBLIOTECA.....	17
3.2	PROBLEMAS ENCONTRADO	CAMPUS.....	17
3.3	SOLUCION PROPUESTA	PEÑAS.....	18
3.4	ANÁLISIS DE FACTIBILIDAD ALTERNATIVA "A"	19	
3.4.1	FACTIBILIDAD ECONÓMICA.....	20	

3.4.2	FACTIBILIDAD OPERATIVA	21
3.4.3	COSTOS OPERATIVOS	22
3.4.4	COSTOS TOTAL DEL PRESUPUESTO ALTERNATIVA "A"	23
3.4.5	VENTAJAS	23
3.4.6	BENEFICIOS	23
3.4.7	CONDICIONES COMERCIALES	24
3.4.7.1.1	FORMA DE PAGO	24
3.4.7.1.2	GARANTÍA DE LA ALTERNATIVA "A"	24
3.4.8	DIAGRAMA GANTT ALTERNATIVA "A"	25
3.5	ALTERNATIVA # "B"	26
3.5.1	FACTIBILIDAD ECONÓMICA	27
3.5.2	FACTIBILIDAD OPERATIVA	28
3.5.3	COSTOS OPERATIVOS	29
3.5.4	COSTO TOTAL DEL PRESUPUESTO ALTERNATIVA "B"	30
3.5.5	VENTAJAS	30
3.5.6	BENEFICIOS	30
3.5.7	CONDICIONES COMERCIALES	31
3.5.7.1.1	FORMA DE PAGO	31
3.5.7.1.2	GARANTÍA DE LA ALTERNATIVA "B"	31
3.5.8	DIAGRAMA GANTT ALTERNATIVA "B"	32

CAPÍTULO 4

4	GRÁFICO DE RED LAN Y WAN DE DEVIES CORP	33
4.1	INTRODUCCION A LOS ROUTERS	33
4.2	MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER	33
4.2.1	CABLE DCE (Data Circuit Equipment)	33
4.2.2	CABLE DTE (Data Terminal Equipment)	33
4.2.3	CABLE UTP (Cat 5E)	34
4.2.4	CONECTOR RJ45	34
4.2.5	PUERTO SERIAL (CONECTOR COM)	35
4.2.6	PARTES INTERNAS DE UN ROUTER	36
4.2.7	PARTES EXTERNAS DEL ROUTER	37
4.2.8	CONEXIONES INTERNAS DEL ROUTER	37
4.3	INTERFAZ DTE-DCE	38
4.4	MODOS DEL ROUTER	38
4.5	ENRUTAMIENTO	39
4.5.1	PROTOCOLOS ENRUTADOS	39
4.5.2	PROTOCOLOS DE ENRUTAMIENTO	39
4.5.2.1	ENRUTAMIENTO ESTATICO	39
4.6	ENRUTAMIENTO DINAMICO	40



4.6.1.1	TIPOS DE DIRECCIONAMIENTO	40
4.6.1.2	DIRECCIONAMIENTO CON CLASE	40
4.7	PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO(RIP).....	40
4.7.1	CARACTERÍSTICAS PRINCIPALES DE RIP.....	41
4.7.2	FUNCIONAMIENTO RIP.....	41
4.7.3	VENTAJAS	41
4.7.4	INCONVENIENTES.....	42
4.7.5	LIMITACIONES RIP	42
4.7.6	MENSAJES RIP.....	42
4.8	PROTOCOLO "PRIMERO LA RUTA MÁS CORTA" (OSPF).....	43
4.8.1	FUNCIÓN DE OSPF	43
4.8.1.1	CARACTERÍSTICAS DE OSPF	43
4.8.1.1.1	RESPUESTA RÁPIDA Y SIN BUCLES ANTE CAMBIOS.....	43
4.8.1.1.2	SEGURIDAD ANTE LOS CAMBIOS.	44
4.8.1.1.3	SOPORTE DE MÚLTIPLES MÉTRICAS.....	44
4.8.1.1.4	BALANCEADO DE CARGA EN MÚLTIPLES CAMINOS.	44
4.8.1.1.5	ESCALABILIDAD EN EL CRECIMIENTO DE RUTAS EXTERNAS.	44
4.8.1.2	TRÁFICO DE ENRUTAMIENTO.....	45
4.8.1.3	TIPOS DE AREA QUE DISTINGUE OSPF	45
4.8.1.3.1	ÁREA BACKBONE	45
4.8.1.3.2	ÁREA STUB.....	45
4.8.2	INTERFACES EN OSPF.....	46
4.8.3	ESTADO DE LAS INTERFACES	46
4.8.4	ESTADO DESACTIVADO (DOWN)	46
4.8.5	ESTADO DE INICIALIZACIÓN (INIT).....	46
4.8.6	ESTADO BIDIRECCIONAL (TWO-WAY)	47
4.8.7	ESTADO DE INTERCAMBIO (EXCHANGE)	47
4.8.8	ESTADO CARGANDO (LOADING)	47
4.8.9	PARA QUÉ SE UTILIZA LA REDISTRIBUCIÓN DE RUTAS.....	48
4.8.10	LAS MÉTRICAS	48
4.8.11	REDISTRIBUCIÓN EN RIP.....	49
4.8.12	REDISTRIBUCIÓN EN OSPF.....	49
4.9	DEFINICIÓN Y FUNCIÓN DEL SWITCH.....	49
4.9.1	LED SISTEMAS – SWITCHES	50
4.9.2	LAN VIRTUALES (VLAN).....	50
4.9.3	TIPOS DE VLAN	50
4.9.3.1	VLANS BASADAS EN PUERTOS (MEMBERSHIP BY PORT GROUP)	50
4.9.3.2	VLAN BASADAS EN MAC (MEMBERSHIP BY MAC ADDRESS)	51
4.9.3.3	VLANS DE CAPA 3 (LAYER 3-BASED VLANS).....	51
4.9.3.4	VLANS BASADAS EN REGLAS (POLICY BASED VLANS).	52



4.10	LISTAS DE CONTROL DE ACCESO	52
4.10.1	FUNCIONAMIENTO DE LAS ACL.....	53
4.10.1.1	MÁSCARA DE WILDCARD.....	53
4.10.1.2	PALABRAS CLAVES ESPECIALES UTILIZADAS EN LAS ACL.....	53
4.10.2	TIPO DE ACL: ESTÁNDAR	54
4.10.3	TIPO DE ACL: EXTENDIDA	54
4.10.4	LISTA DE ACCESO ENTRANTE.....	54
4.10.5	LISTA DE ACCESO SALIENTE.....	54
4.11	TELNET	54
4.12	PING (ICMP).....	54
4.13	FTP	55
4.14	SSH	55
4.15	FIREWALL.....	56
4.16	CREACIÓN DE LAS ACL.....	56
4.17	CONFIGURACION DE ROUTERS	57
4.18	COMANDOS BASICOS DE ROUTER	61
4.19	CONFIGURACION DE LOS ROUTERS	65
4.19.1	ASIGNACION DE NOMBRE A ROUTERS.....	65
4.19.2	CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER	66
4.19.3	CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER MILAGRO	66
4.19.4	CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER DURAN	67
4.19.5	CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER SANTA ELENA.....	67
4.19.6	CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER GUAYAS.....	67
4.19.7	CONFIGURACION DE INTERFACES SERIALES	68
4.19.8	CONFIGURACION DE PROTOCOLOS DE ENRUTAMEINTO	71
4.19.8.1	PROTOCOLO OSPF	71
4.19.9	PROTOCOLO RIP VERSION 2	72
4.19.10	SHOW RUNING-CONFIG	81
4.19.11	CONFIGURACION DE SWITCH.....	83
4.19.11.1	ASIGNACION DE NOMBRE AL SWITCH MILAGRO.....	83
4.19.12	ASIGNACION DE NOMBRE AL SWITCH DURAN	84
4.19.12.1	ASIGNACION DE NOMBRE AL SWITCH GUAYAS.....	84
4.19.12.2	ASIGNACION DE NOMBRE AL SWITCH SANTA ELENA	84
4.19.13	CONFIGURACION DE INTERFACES ETHERNET MILAGRO.....	85
4.19.14	CONFIGURACION DE INTERFACES ETHERNET DURAN	85
4.19.15	CONFIGURACION DE INTERFACES ETHERNET DURAN	86
4.19.16	CONFIGURACION DE INTERFACES ETHERNET SANTA ELENA	86
4.19.17	CONFIGURACION DE SUB-INTERFACES MILAGRO.....	86
4.19.18	CONFIGURACION DE SUB-INTERFACES DURAN	89
4.19.19	CONFIGURACION DE SUB-INTERFACES GUAYAS.....	90

4.19.20	CONFIGURACION DE SUB-INTERFACES SANTA ELENA	91
4.19.21	CONFIGURACION DE VLAN MILAGRO	92
4.19.22	CONFIGURACION DE VLAN DURAN	93
4.19.23	CONFIGURACION DE VLAN GUAYAS	93
4.19.24	CONFIGURACION DE VLAN SANTA ELENA.....	94
4.19.25	ASIGNACION DE PUERTOS A VLANS.....	95
4.19.26	ASIGNACION DE PUERTOS A VLANS MILAGRO	95
4.19.27	ASIGNACION DE PUERTOS A VLANS DURAN	96
4.19.28	ASIGNACION DE PUERTOS A VLANS GUAYAS.....	96
4.19.29	ASIGNACION DE PUERTOS A VLANS SANTA ELENA.....	97
4.19.30	CONFIGURACION ACCESS LIST	101

CAPÍTULO 5

5	GLOSARIO DE TÉRMINOS TÉCNICOS	102
---	-------------------------------------	-----



BIBLIOTECA
CAMPUS
PEÑAS

INDICES DE FIGURAS

CAPÍTULO 2

Figura 2-1 Devies Corp. Milagro	2
Figura 2-2 Red LAN Matriz Milagro.....	4
Figura 2-3 Red LAN Sucursal Quevedo	5
Figura 2-4 Red LAN Sucursal Santo Domingo.....	6
Figura 2-5 Comunicación WAN Matriz-Sucursal (Dispositivos)	12
Figura 2-6 Recepción de Internet	13
Figura 2-7 Ubicación Física del Firewall	15

CAPÍTULO 4

Figura 4-1 Cable DCE.....	33
Figura 4-2 Cable DTE	33
Figura 4-3 Conector RJ45	34
Figura 4-4 Cable UTP Cat 5E	34
Figura 4-5 Puerto serial	35
Figura 4-6 Partes internas de un router.....	37
Figura 4-7 Partes Externas de un router	37
Figura 4-8 Diagrama Funcionamiento de un ACL.....	53
Figura 4-9 SSH.....	55
Figura 4-10 Firewall en las ACL.....	56
Figura 4-11 Configuración Router	57
Figura 4-12 Configuracion Global	57
Figura 4-13 Configuracion ethernet	58
Figura 4-14 Configuración ram del router.....	58
Figura 4-15 Configuración show running-config.....	59
Figura 4-16 Configuración show ip route	59
Figura 4-17 Configuración show interfaces	60
Figura 4-18 Configuración ip addres.....	60

INDICES DE TABLAS

CAPÍTULO 2

Tabla 2-1 Características De Los Servidores	7
Tabla 2-2 Características estaciones de trabajo Milagro	8
Tabla 2-3 Características estaciones de trabajo Quevedo	8
Tabla 2-4 Características estaciones de trabajo Santo Domingo.....	8
Tabla 2-5 Características de los dispositivos de conmutación	10
Tabla 2-6 Característica de los dispositivos de Enrutamiento.....	11

CAPÍTULO 3

Tabla 3-1 Problemas, Causas, Efectos	17
Tabla 3-2 Problema, Solución, Alcance	18
Tabla 3-3 Factibilidad Económica Alternativa “A”	20
Tabla 3-4 Factibilidad Operativa Alternativa “A”	21
Tabla 3-5 Costos Operativos Alternativa “A”	22
Tabla 3-6 Costo Total del Presupuesto Alternativa “A”	23
Tabla 3-7 Factibilidad Económica Alternativa “B”	27
Tabla 3-8 Factibilidad Operativa Alternativa “B”.....	28
Tabla 3-9 Costos Operativos Alternativa “B”	29
Tabla 3-10 Costos Total del Presupuesto alternativa “B”	30

CAPÍTULO 4

Tabla 4-1 Comandos Basicos del Router	61
Tabla 4-2 Comandos Modos Exec Privilegiados	62
Tabla 4-3 Comandos Modos De Configuracion Global.....	63
Tabla 4-4 Submodo de configuración de Interfaz	64
Tabla 4-5 Submodo de Configuracion De Linea.....	64
Tabla 4-6 Submodo de Configuracion del Protocolo	64
Tabla 4-7 Interpretación de una ruta RIP	77



BIBLIOTECA
CAMPUS
PEÑAS



CAPÍTULO 1

GENERALIDADES

1 GENERALIDADES

1.1 INTRODUCCION

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

1.2 OBJETIVO DEL MANUAL

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

Luego de leer este manual el usuario estará en la capacidad de realizar diversas configuraciones de dispositivos de comunicación.

1.3 A QUIEN VA DIRIGUIDO ESTE MANUAL

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

1.4 QUE SE DEBE CONOCER

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

- ✓ Conceptos básicos de redes de informática y sistemas operativos
- ✓ Conocimientos básicos de navegadores de internet y tecnologías basadas e internet

1.5 ORGANIZACIÓN DEL CONTENIDO DE ESTE MANUAL

Este manual se encuentra dividido en 5 capítulos distribuidos en orden numéricos, los cuales se detallan a continuación

Capítulo 1 - Generalidades

Capítulo 2 - Situación Actual

Capítulo 3 – Solución Propuesta

Capítulo 4 – Configuración de Dispositivos de Comunicación y Enrutamiento



BIBLIOTECA
CAMPUS
PEÑAS



BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 2

SITUACION ACTUAL

2 SITUACION ACTUAL

2.1 ANTECEDENTES



Figura 2-1 Devies Corp. Milagro

Devies Supermercado Mayorista es el primer supermercado creado en el Ecuador con multiples formatos de venta (mayorista, distribuidor y autoservicio) con el fin de atender a comerciantes de las zonas centro y sur del país.

Nuestro compromiso y filosofia, además de brindar productos de excelente calidad y a buenos precios, se enfoca en desarrollar con nuestros clientes y proveedores relaciones comerciales de largo plazo que nos permitan a todos consolidarnos en el mercado y hacer negocios rentables.

2.1.1 MISIÓN

Comercializar productos y servicios excediendo las expectativas de nuestros clientes y proveedores, logrando negocios de beneficio mutuo, contando con personal calificado y motivado y comprometiéndonos con el desarrollo comunitario.

2.1.2 VISIÓN

Ser el proveedor preferido del comercio ecuatoriano.



BIBLIOTECA
CAMPUS
PEÑAS

2.2 AREAS ADMINISTRATIVAS

La Matriz de Devies Corp. Se encuentra ubicado en la ciudad de Milagro, consta de dos sucursales ubicadas en las localidades de Quevedo y Santo Domingo la primera creada en el año 2007 y la segunda inaugurada en el año del 2008.

Buscando el mejoramiento continuo en todos los procesos con el fin de optimizar los recursos y verlos reflejados en las utilidades como en las de los clientes y proveedores.

Consta de los siguientes departamentos:

Secretaría: se encarga de todo lo relacionado con la atención al cliente, a saber: emisión de tarjetas, tramitación de solicitudes de ingreso.

Compras: encargada de la adquisición de todos los insumos y suministros para la matriz y sucursales.

Control ventas: revisa la facturación de los diferentes puntos de venta, el cuadre de las respectivas cajas, etc.

Contabilidad: preparación de los estados financieros de la institución a través de procesos contables de las operaciones diarias realizadas por cada uno de los departamentos del Club.

Caja General: se ocupa de la revisión de la facturación de los diferentes puntos de venta, elaboración de cheques, pagos a proveedores, pagos a empleados, etc.

Sistemas Y Computación: En esta área se encuentra los servidores principales, así como también el mantenimiento y desarrollo de los sistemas integrados.

Es el área responsable de todos los equipos de cómputo y de la instalación de puntos de redes

Área Recursos Humanos: Recursos humanos: se encarga de controlar la asistencia del personal, selección y contratación de empleados, otorgamiento de préstamos al personal, proceso de roles de pago, políticas de capacitación de los empleados en cuanto al uso de uniforme, horarios de trabajo y normas a seguir.

2.3 INFRAESTRUCTURA LAN

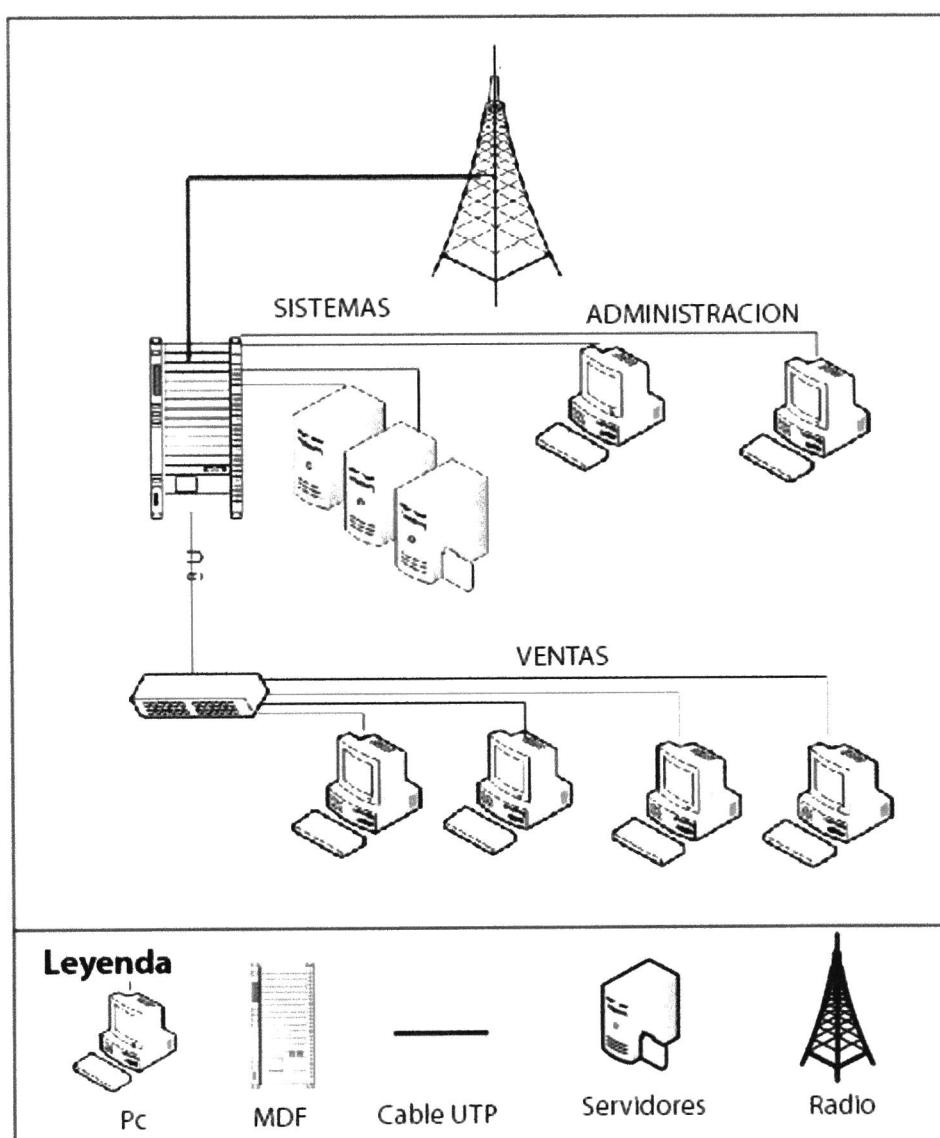
Devies Corp en su infraestructura LAN esta divido de las siguientes maneras:

- ✓ Ventas
- ✓ Administración
- ✓ Sistemas

Cada Unos de ellos separados por edificios diferentes, las cuales poseen red LAN categoría 5e con estándar EIA/TIA-568B

La topología de red que maneja en cada unos de sus sucursales es en estrella

DEVIES CORP MATRIZ MILAGRO



BIBLIOTECA
CAMPUS
PEÑAS

Figura 2-2 Red LAN Matriz Milagro

DEVIES CORP SUCURSAL QUEVEDO

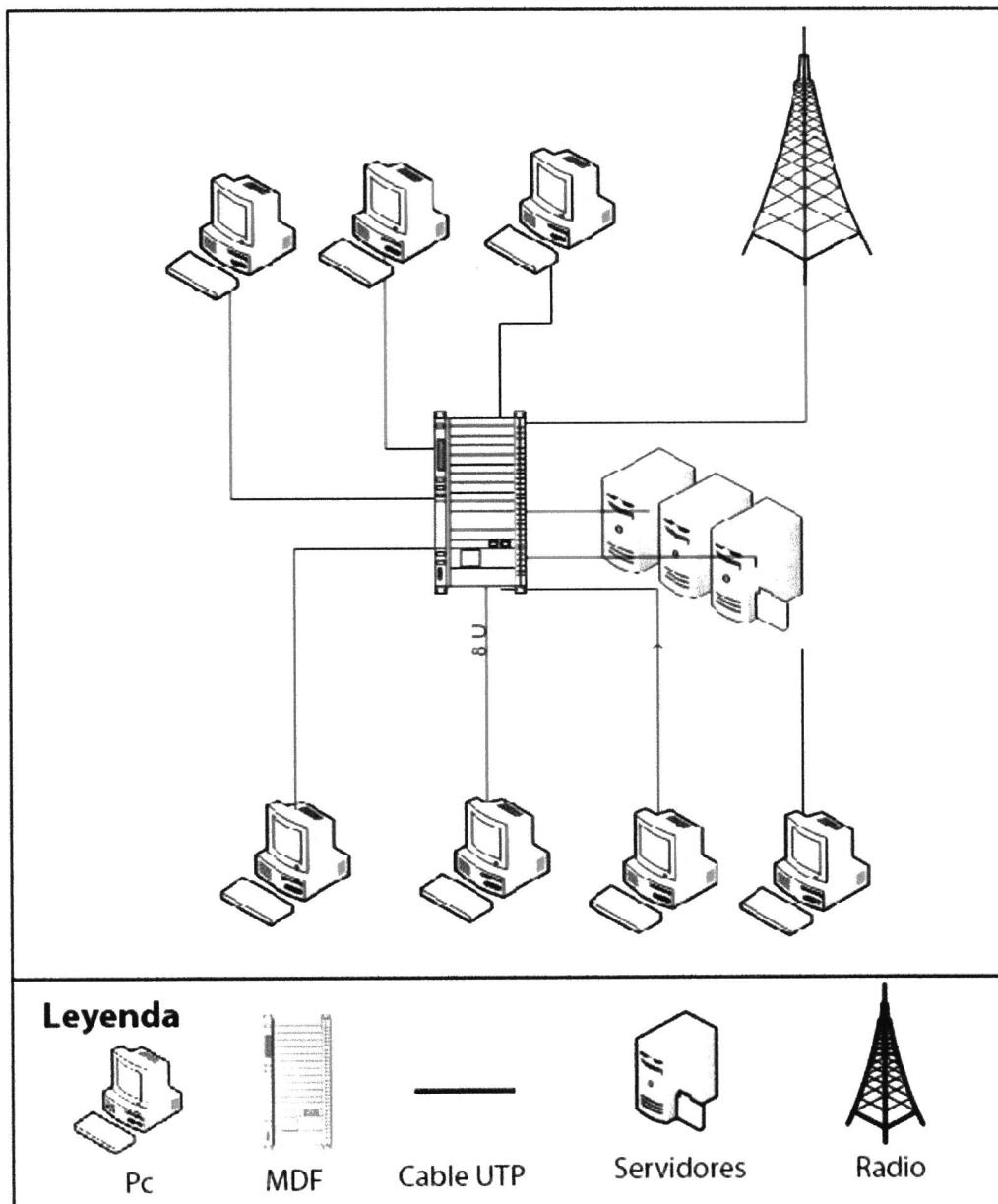


Figura 2-3 Red LAN Sucursal Quevedo

DEVIES CORP SUCURSAL SANTO DOMINGO

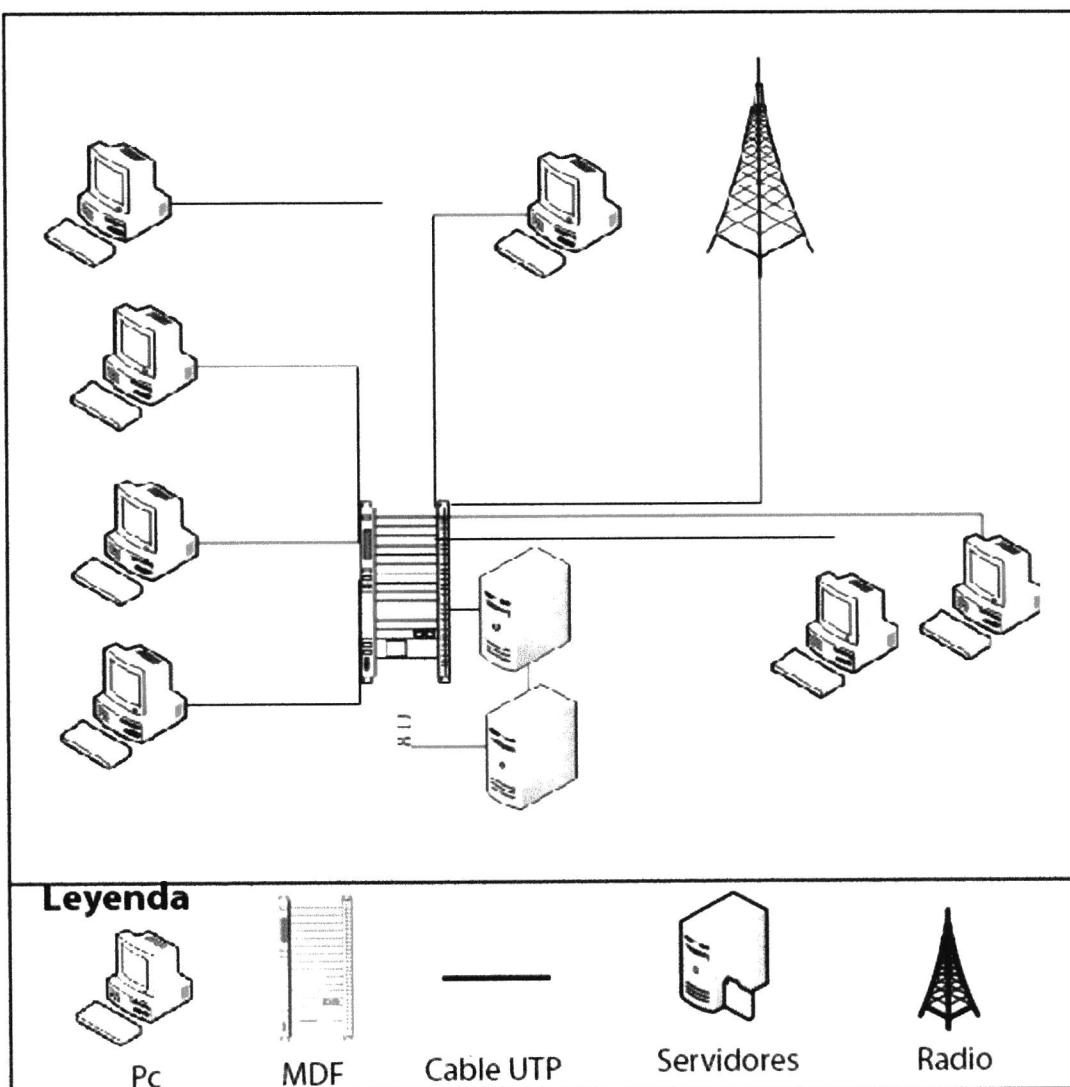


Figura 2-4 Red LAN Sucursal Santo Domingo



BIBLIOTECA
CAMPUS
PEÑAS

2.4 CARACTERISTICAS DE LOS SERVIDORES

Posee 10 servidores que cumplen las siguientes funciones:

CANTIDAD	ROL O SERVICIO	SISTEMA OPERATIVO	PROCESADOR	MEMORIA RAM	DISCO DURO	NIC	
1	Servidor de Base de Datos (Principal)	Windows 2003 Server	Intel Dual Core 2.8 GHz	2 Gb	160 Gb	10/100 /1000 Mbps	
1	Replica de Base de Datos (DataWarehouse)		Intel Xeon Proliant 2.8 GHz				
1	Servidor Exchange (Correo)		Intel Core 2 Duo 2.0 GHz				
1	File and Print Server		1 Gb	250 Gb			
1	Active Directory - DNS - DHCP						
1	Terminal Server		Intel 2.8 GHz	2 Gb	300 Gb		
1	Actualización de Antivirus (WSUS)						
1	ISA Server - Firewall		Intel Dual Core 2.0 GHz	2 Gb	300 Gb		
1	Controlador de Dominio						
1	Servidor de Antivirus Fore Front Client						

Tabla 2-1 Características De Los Servidores

2.5 CARACTERISTICAS DE LAS ESTACIONES DE TRABAJO

Devies Corp. Consta de una Matriz ubicada en la ciudad de Milagro con 100 estaciones de trabajos, ubicado en los diferentes departamentos con las siguientes características:

CANTIDAD	PROCESADOR	MEMORIA RAM	DISCO DURO	NIC	SISTEMA OPERATIVO
32	INTEL INTEL ATOM 1.66 GHZ	2GB	160 GB	10/100 Mbps	Windows Vista Home Edition
28	INTEL 1,8 GHZ	1GB	320GB		Windows XP Professional
13	Intel Dual Core 1,6 GHz		120 GB		
27	Intel PIII 1,8 GHz	512MB	80 GB		

Tabla 2-2 Características estaciones de trabajo Milagro

La sucursal de la ciudad de Quevedo, la segunda en número de computadores consta de las siguientes estaciones de trabajo que cumplen las siguientes características:

CANTIDAD	PROCESADOR	MEMORIA RAM	DISCO DURO	NIC	SISTEMA OPERATIVO
15	INTEL ATOM 1.66 GHZ	1GB	320 GB	10/100 Mbps	Windows XP Professional
22	Intel Dual Core 1,6 GHz	2GB			
3	Intel P IV 1,8 GHz	512MB			

Tabla 2-3 Características estaciones de trabajo Quevedo

Finalmente la sucursal del Cantón Santo Domingo con 30 estaciones de trabajo

CANTIDAD	PROCESADOR	MEMORIA RAM	DISCO DURO	NIC	SISTEMA OPERATIVO
12	INTEL INTEL ATOM 1.66 GHZ	3GB	320 GB	10/100 Mbps	Windows Vista Ultimate
13	Intel Core 2 Duo 1,6 GHz	2GB			Windows 7

Tabla 2-4 Características estaciones de trabajo Santo Domingo

2.6 MEDIOS DE COMUNICACIÓN

2.6.1 ALAMBRICOS

Actualmente Devies Corp utiliza como medio principal de comunicación cable UTP categoría 5e con velocidad de transmisión de 100 Mbps con un ancho de banda de 150 Mhz.

2.6.2 INALÁMBRICOS

No existe enlaces inalámbricos a nivel LAN en ninguna de sus sucursales

2.7 DISPOSITIVOS DE COMUNICACIÓN

2.7.1 CONMUTACIÓN

A continuación detallamos los dispositivos de comunicación que utiliza Devies Corp.

LUGAR	DISPOSITIVO	MARCA	MODELO	CARACTERISTICAS
MATRIZ MILAGRO	1 Modem	Advantek	Analógico Fask V.23 y Bell - 202	Velocidad 56 Kbps Transmisión Full dúplex con línea dedicada para teleproceso
				
	2 Switch	3 COM	Baseline Plus Modelo 2226	Administrable 48 puertos 10/100 Mbps 2 puertos Gigabit de uso dual (Cobre o Fibra) Comutador 10/100 Mbps de nivel 2 Transmisión Half dúplex de 1 GHz Control de acceso a la re IEEE 802.1X
QUEVEDO	2 SWITCH	D-LINK	1024D	No Administrable 24 puertos 10/100 Mbps Soporte full-dúplex y half - dúplex para cada puerto Control de flujo contra la perdida de datos Leds de diagnósticos en el panel frontal
SANTO DOMINGO				

Tabla 2-5 Características de los dispositivos de conmutación

2.7.2 ENRUTAMIENTO

Este router es el encargado del encaminamiento de los paquetes, recepción de internet, es administrado por el carrier Telconet.

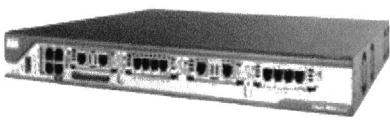
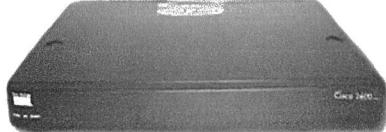
LUGAR	DISPOSITIVO	MARCA	MODELO	CARATERISTICAS
DEVIES CORP	2 ROUTER 	CISCO	2801	Cisco IOS, cifrado de hardware, soporte de MPLS Protocolos de interconexión de datos Ethernet - Fast Ethernet Protocolo de transporte IPSec Protocolo de gestión remota SNMP3
	1 ROUTER 			2 Puertos Ethernet 10/100/100 Mbps 2 Ranuras para tarjetas de interfaz WAN 1 Ranura para el modulo de red Memoria de sistemas DRAM de 24 a 64 MB Memoria de sistemas DRAM de 24 a 64 MB Memoria flash de 4 a 16 Mb

Tabla 2-6 Característica de los dispositivos de Enrutamiento

2.8 INFRAESTRUCTURA WAN

En lo que se refiere a la infraestructura WAN, mantiene conexiones desde las sucursales de Quevedo y Santo Domingo hacia la matriz Milagro, este enlace se lo realiza mediante su carrier administrado por Telconet.

En la matriz cuenta con un router marca Cisco que es el encargado de llevar las comunicaciones entre las redes WAN, así mismo de la administración de Telconet.

Consta de un ancho de banda de 800Ghz y una velocidad de transmisión de 256 Kbps

2.9 COMUNICACIÓN WAN MATRIZ-SUCURSAL

2.9.1 A NIVEL DE DISPOSITIVOS DE COMUNICACIÓN

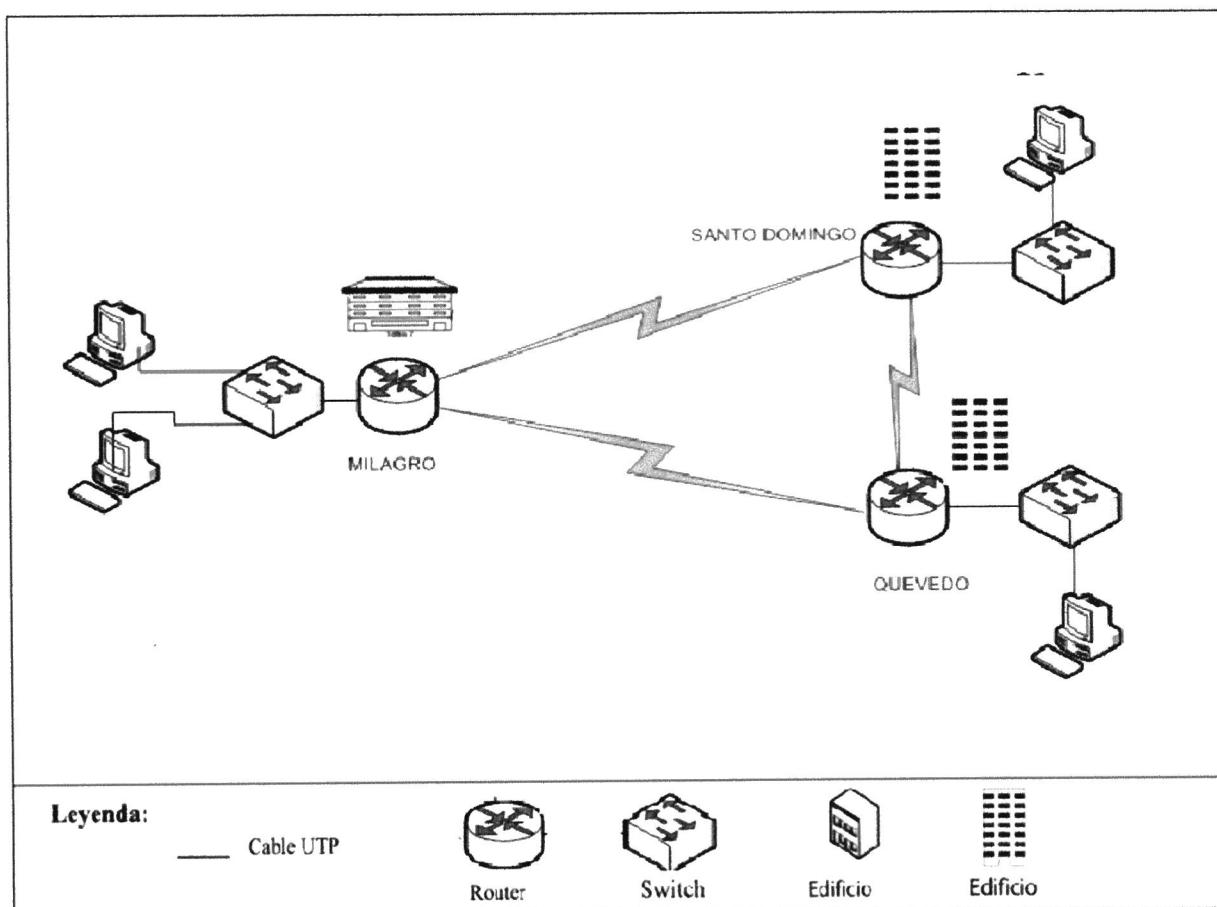


Figura 2-5 Comunicación WAN Matriz-Sucursal (Dispositivos)

2.10 RECEPCIÓN DE SERVICIO DE INTERNET

El proveedor del servicio de internet es telconet, que es el encargado a la vez de la comunicación entre las distintas sucursales y la matriz en Milagro, este es repartido para sus diferentes usuarios, con un ancho de banda de 512 Kbps

2.11 GRAFICO RECEPCIÓN DE SERVICIO DE INTERNET

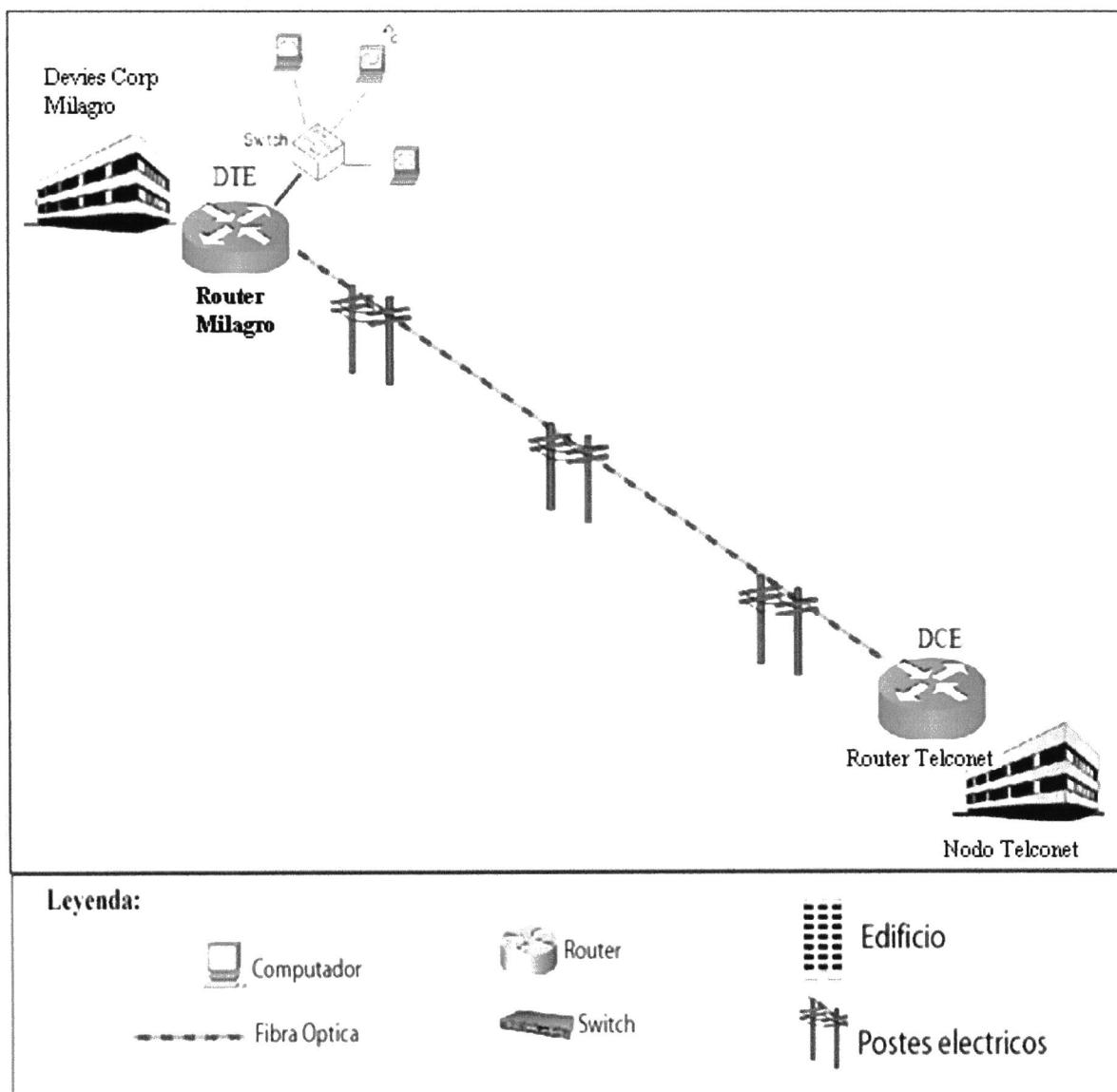


Figura 2-6 Recepción de Internet

2.12 SEGURIDADES

Para garantizar que los recursos informáticos estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos mencionaremos algunos métodos de seguridad establecidos.

Posee un sistema de cámaras que vigilan dentro como fuera de las instalaciones, existen cámaras con tecnología IP, pero no está trabajado adecuadamente

2.13 FIREWALL

El firewall se encuentra en el ISA Server que permite o bloquea las transmisiones de una red a la otra, además realiza las siguientes funciones:

- ✓ Filtrado de paquetes
- ✓ (Servidores Proxy) Permitir y denegar internet para diversos usuarios
- ✓ Denegación de descargas de video, música

En el ISA Server se encuentra instalado el Antivirus Kaspersky que protege los datos de servidores que operan con Microsoft Windows contra todo tipo de programas maliciosos. El producto fue diseñado específicamente para servidores corporativos con altas cargas de trabajo.

2.14 UBICACIÓN FÍSICA DEL FIREWALL

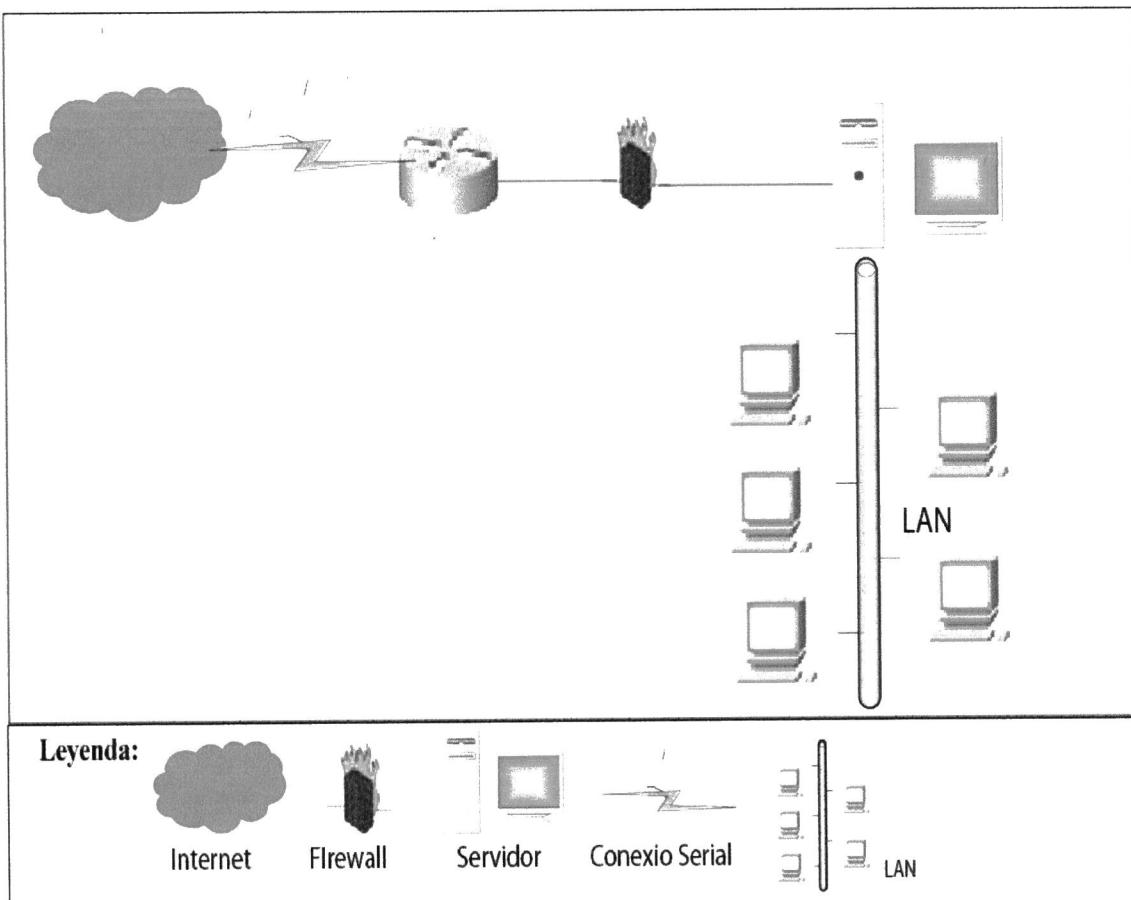


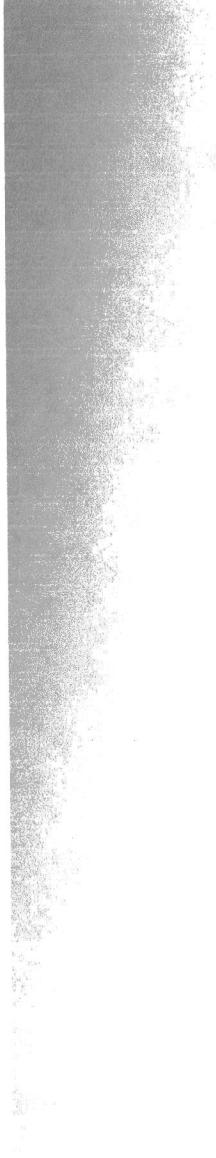
Figura 2-7 Ubicación Física del Firewall



BIBLIOTECA
CAMPUS
PEÑAS

2.15 PROBLEMAS ENCONTRADOS

- Insuficiente ancho de banda entre sucursal y Matriz
- No existe respaldo entre la matriz y sucursal
- Congestionamiento de la red interna
- En la sucursal Quevedo no todos los usuarios están conectados en red Lan



BIBLIOTECA
CAMPUS
PEÑAS

CAPÍTULO 3

SOLUCION PROPUESTA



3.1 SOLUCIÓN PROPUESTA**3.2 PROBLEMAS ENCONTRADO**

PROBLEMA	CAUSA	EFFECTO
❖ Insuficiente ancho de banda entre sucursal y Matriz	❖ Falta de presupuesto	❖ Demoras en las consultas desde la sucursal hacia la base de datos de la matriz
❖ No existe respaldo entre la matriz y sucursal	❖ La empresa no se a preocupado en los problemas a causar	❖ Pérdida total de la comunicación entre matriz y sucursal
❖ Congestionamiento de la red interna	❖ Red no segmentada ❖ Existencia de broadcast en la red	❖ Lentitud en la red Lan ❖ Tiempos de respuestas altos
❖ En la sucursal Quevedo no todos los usuarios están conectados en red Lan	❖ Descuido por parte del administrador de red	❖ No existe comunicación interna entre los usuarios de la red Lan

Tabla 3-1 Problemas, Causas, Efectos

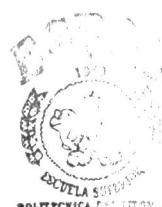


BIBLIOTECA
CAMPUS
PEÑAS

3.3 SOLUCION PROPUESTA

PROBLEMA	SOLUCION	ALCANCE
❖ Insuficiente ancho de banda entre sucursal y matriz	❖ Aumentar el ancho de banda acorde al numero de usuarios	❖ Con mayor ancho de banda a nivel WAN, se podrá agilitar los procesos y aplicaciones
❖ No existe respaldo de comunicación WAN	❖ Implementar un enlace de Bakcup que nos permitirá tener un plan de contingencia	❖ Contar con un respaldo seguro, al caer el enlace principal
❖ Congestionamiento de la red interna	❖ Creación de Vlan departamentales por sucursales	❖ Control y disminución de broadcast ❖ Mejoramiento de tiempos de respuestas en la transmisión de datos en la red interna
❖ En la sucursal Quevedo no todos los usuarios están conectado en red Lan	❖ Adquirir dispositivos nuevos de conmutación	❖ Comunicación interna entre los usuarios de la red ❖ Facilidad de compartir recurso tales como archivos, impresoras...etc

Tabla 3-2 Problema, Solución, Alcance



BIBLIOTECA
CAMPUS
PEÑAS

3.4 ANÁLISIS DE FACTIBILIDAD ALTERNATIVA “A”

Esta alternativa permitirá un mejor rendimiento en la infraestructura a nivel WAN invirtiendo en medios y dispositivos de comunicaciones lo cual permitirá una excelente transmisión de los datos y por lo tanto beneficiara el crecimiento de la empresa para esto se debe:

- ✓ Adquirir switch administrables con fuentes redundantes para un mejor control de la red LAN
- ✓ Contratar un nuevo Proveedor de Internet (Ecuanet) nos servirá como enlace Backup

Se trabajara con dispositivos de comunicación de marca D-Link, cabe mencionar que todos los dispositivos de la empresa son de este tipo de marca, motivo por el cual usaremos para así tener una misma línea de producto



BIBLIOTECA
CAMPUS
PEÑAS

3.4.1 FACTIBILIDAD ECONÓMICA.

CANTIDAD	CARACTERÍSTICAS	PRECIO UNITARIO	TOTAL
5	Switch D Link DES-3828P Tecnología Administrable Puertos: 24 puertas RJ-45 10/100/1000Mbps Máximo grupos VLAN: VLAN 4K (4K Static VLANs, 255 Dynamic VLANs) Multiples IP por VLAN: 2 Fuente de alimentación redundante MAC Address Learning: Actualización Automática Método de acceso: CSMA/CD	\$400.00	\$2,000.00
3	Servicio de Enlace Wan(Telconet) 1 Mbps (1año)	\$300,00	\$10,800,00
3	Servicio de Enlace Wan Bakcup (Ecunet) 1 Mbps (1año)	\$250,00	\$9,000,00
TOTAL			\$21.800.00

Tabla 3-3 Factibilidad Económica Alternativa “A”

3.4.2 FACTIBILIDAD OPERATIVA

CANTIDAD	ACTIVIDAD	SEMANA
1	Fase de Análisis de la red LAN y MAN Ingeniero en Telecomunicaciones	1
1	Técnico en Redes	
1	Fase de Diseño de la red LAN y MAN Ingeniero En Telecomunicaciones	1
1	Fase de Implementación de la red LAN y MAN Ingeniero En Telecomunicaciones	2
3	Técnico en Redes	
1	Fase de Prueba de la red LAN y MAN Ingeniero En Telecomunicaciones	1
1	Técnico en Redes	
1	Fase De Documentación de la Red LAN y MAN Ingeniero En Telecomunicaciones	1
1	Técnico en Redes	

Tabla 3-4 Factibilidad Operativa Alternativa “A”



BIBLIOTECA
CAMPUS
PEÑAS

3.4.3 COSTOS OPERATIVOS

CANTIDAD	ACTIVIDAD	SEMANA	COSTOS	TOTAL
1	Fase de Análisis de la red LAN y MAN Ingeniero en Telecomunicaciones	1	\$200 \$180	\$200 \$180
1	Técnico en Redes			
1	Fase de Diseño de la red LAN y MAN Ingeniero En Telecomunicaciones	1	\$ 200	\$ 200
1	Fase de Implementación de la red LAN y MAN Ingeniero En Telecomunicaciones	2	\$ 220	\$ 440
3	Técnico en Redes		\$ 180	\$ 1080
1	Fase de Prueba de la red LAN y MAN Ingeniero En Telecomunicaciones	1	\$ 200	\$ 200
1	Técnico en Redes		\$ 150	\$ 150
1	Fase De Documentación de la red LAN y MAN Ingeniero En Telecomunicaciones	1	\$ 200	\$ 200
1	Técnico en Redes		\$ 180	\$ 180
Total				\$ 2,830.00

Tabla 3-5 Costos Operativos Alternativa "A"

3.4.4 COSTOS TOTAL DEL PRESUPUESTO ALTERNATIVA “A”

DESCRIPCIÓN	COSTO
Factibilidad Economica	\$13.700.00
Costos Operativos	\$ 2,830.00
Sub Total	\$16,530.00
I.V.A	\$1,983.60
Total	\$18,513.60

Tabla 3-6 Costo Total del Presupuesto Alternativa “A”

3.4.5 VENTAJAS

- ❖ La empresa contará con un plan de contingencia en posibles fallas en enlaces Wan
- ❖ Dispositivos de comunicación que ofrecen confiabilidad en la transmisión de datos
- ❖ Mejora en tiempo de respuesta entre comunicaciones de usuarios finales
- ❖ Mayor eficiencia, productividad y seguridad en la red Lan
- ❖ Mejora en el tráfico de la red

3.4.6 BENEFICIOS

- ❖ Información actualizada en la matriz (Milagro) y todas las sucursales
- ❖ Respaldo en los enlaces de sucursales
- ❖ Seguridad en las comunicaciones
- ❖ Comunicación rápida y segura entre matriz y sucursales



BIBLIOTECA
CAMPUS
PEÑAS

3.4.7 CONDICIONES COMERCIALES

3.4.7.1.1 FORMA DE PAGO

A continuación se detalla la forma de pago establecido

60 % A la firma del proyecto

40% Una vez finalizado el proyecto

3.4.7.1.2 GARANTÍA DE LA ALTERNATIVA “A”

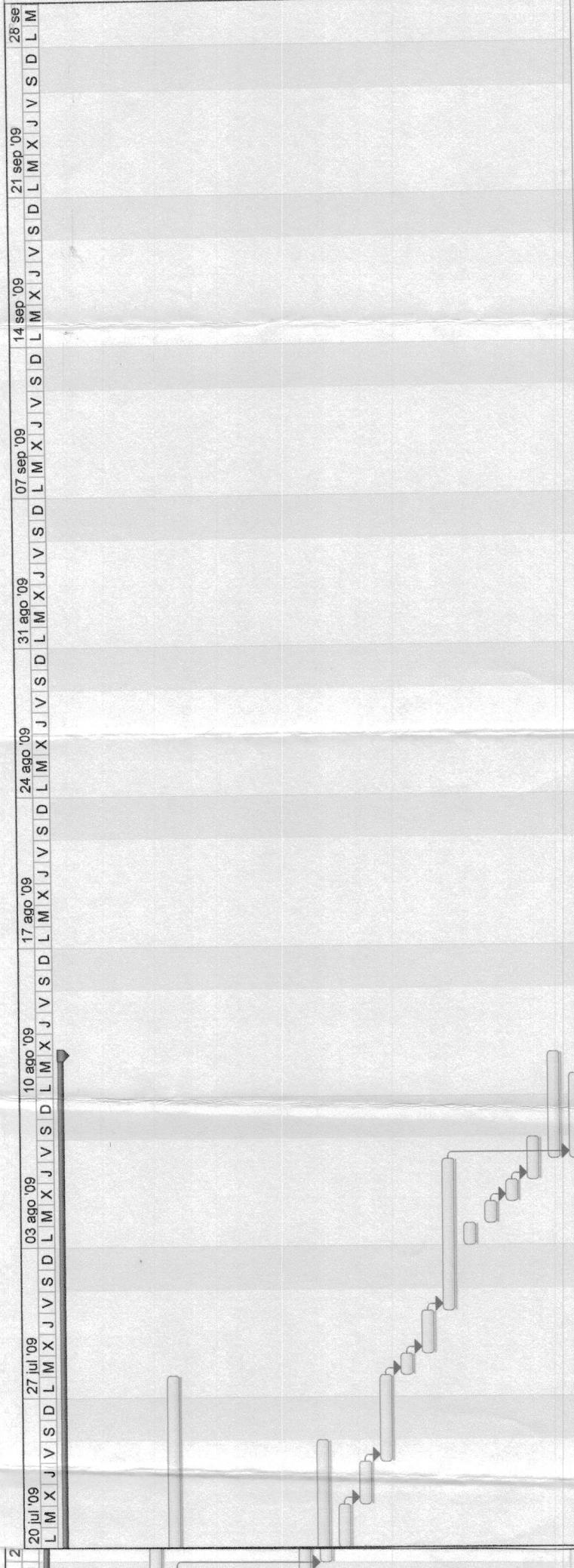
- ✓ Soporte técnico por 6 meses en las configuraciones de los dispositivos de comunicación
- ✓ Garantía por 3 año por los dispositivos de conmutación por parte de la empresa vendedora



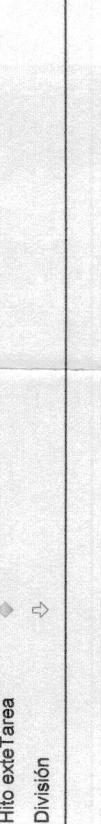
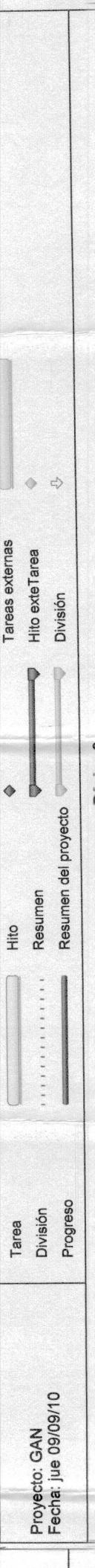
BIBLIOTECA
CAMPUS
PEÑAS,

3.4.8 DIAGRAMA GANTT ALTERNATIVA “A”

Cabe mencionar que en las dos alternativas se toma el mismo tiempo de trabajo, motivo por el cual se usara el mismo diagrama de gan



Id	Nombre de tarea	Tarea	División	Progreso	Hito	Resumen	Tareas externas	Hito exte Tarea
1	FASE DE ANALISIS LAN Y MAN							
2	Recopilación De Información							
3	Cotización de Dispositivos y Materiales de Comunicación							
4	Elaboración de la Propuesta							
5	Aceptación de la Propuesta							
6	FASE DE DISEÑO LAN Y MAN							
7	Compra de Dispositivos y equipos de commutacion y enrutamiento.							
8	Elaboración del diseño de Red WAN.(Milagro)							
9	Elaboración del diseño de Red WAN.(Santo Domingo)							
10	Elaboración del diseño de Red WAN.(Quievedo)							
11	Elaboración del diseño de enlace WAN backup.							
12	FASE DE IMPLEMENTACION							
13	Conexión de enlaces de fibra a la red WAN (Milagro)							
14	Conexión de enlaces de fibra a la red WAN (Santo Domingo)							
15	Conexión de enlaces de fibra a la red WAN (Santo Quievedo)							
16	Configuración de Vlans Matriz Milagro							
17	Configuración de Vlans Sucursales							
18	FASE DE PRUEBA LAN Y MAN							
19	Prueba de Dispositivos de Commutacion en La Matriz Milagro							
20	Prueba de Dispositivos de Commutacion en las Sucursales							
21	Prueba de Enlaces WAN en la Matriz y Sucursales							
22	Capacitación a los Usuarios							
23	FASE DE DOCUMENTACION							
24	Elaboración de Manuales de Red Lan y Man para el Usuario							
25								



3.5 ALTERNATIVA # "B"

Con esta alternativa mejoraremos de igual manera la infraestructura a nivel WAN invirtiendo en medios de dispositivos de comunicación tales como:

- ✓ Adquirir switch administrables con fuentes redundantes para un mejor control de la red LAN
- ✓ Contratar un nuevo Proveedor de Internet (PuntoNet) nos servirá como enlace Backup

Con esta alternativa se trabajara con dispositivos de conmutación de marca 3Com

3.5.1 FACTIBILIDAD ECONÓMICA.

CANTIDAD	CARACTERÍSTICAS	PRECIO UNITARIO	TOTAL
5	Switch 3COM 2928 HPWR Tecnología Administrable Puertos 24 10/100/1000 Mbps puertos PoE y 4 puertos SFP de 1000 Mbps Nivel 3: 32 rutas estáticas Protocolo de gestión remota: SNMP, RMON, SNMP	\$350,00	\$ 1,750. 00
3	Servicio de Enlace Wan Bakcup (Punto Net) 1 Mbps (1año)	\$250,00	\$ 9000,00
TOTAL			\$10,750.00

Tabla 3-7 Factibilidad Económica Alternativa “B”

3.5.2 FACTIBILIDAD OPERATIVA

CANTIDAD	ACTIVIDAD	SEMANA
1	Fase de Análisis de la red LAN y MAN Ingeniero en Telecomunicaciones	1
1	Fase de Diseño de la red LAN y MAN Ingeniero En Telecomunicaciones	1
1	Fase de Implementación de la red LAN y MAN Ingeniero En Telecomunicaciones	2
3	Técnico en Redes	
1	Fase de Prueba de la red LAN y MAN Ingeniero En Telecomunicaciones	1
1	Técnico en Redes	
1	Fase De Documentación de la red LAN y MAN Ingeniero En Telecomunicaciones	1
1	Técnico en Redes	

Tabla 3-8 Factibilidad Operativa Alternativa “B”

3.5.3 COSTOS OPERATIVOS

CANTIDAD	ACTIVIDAD	SEMANA	COSTOS	TOTAL
1	Fase de Análisis de la red LAN y MAN Ingeniero en Telecomunicaciones	1	\$200	\$200
1	Fase de Diseño de la red LAN y MAN Ingeniero En Telecomunicaciones	1	\$ 200	\$ 200
1	Fase de Implementación de la red LAN y MAN Ingeniero En Telecomunicaciones	2	\$ 220	\$ 440
3	Técnico en Redes		\$ 180	\$ 1080
1	Fase de Prueba de la red LAN y MAN Ingeniero En Telecomunicaciones	1	\$ 200	\$ 400
1	Fase De Documentación de la red LAN y MAN Ingeniero En Telecomunicaciones	1	\$ 200	\$ 200
1	Técnico en Redes		\$ 150	\$ 150
Total				\$2.670.00

Tabla 3-9 Costos Operativos Alternativa "B"

3.5.4 COSTO TOTAL DEL PRESUPUESTO ALTERNATIVA “B”

DESCRIPCIÓN	COSTO
Factibilidad Económica	\$10,750.00
Costos Operativos	\$2.670.00
Sub Total	\$13,420.00
I.V.A	\$1,610.40
Total	\$15,030.40

Tabla 3-10 Costos Total del Presupuesto alternativa “B”

3.5.5 VENTAJAS

- ❖ La empresa contará con un plan de contingencia en posibles fallas en enlaces Wan
- ❖ Dispositivos de comunicación que ofrecen confiabilidad en la transmisión de datos
- ❖ Mejora en tiempo de respuesta entre comunicaciones de usuarios finales
- ❖ Mayor eficiencia, productividad y seguridad en la red Lan
- ❖ Mejora en el tráfico de la red

3.5.6 BENEFICIOS

- ❖ Información actualizada en la matriz (Milagro) y todas las sucursales
- ❖ Respaldo en los enlaces de sucursales
- ❖ Seguridad en las comunicaciones
- ❖ Comunicación rápida y segura entre matriz y sucursales

3.5.7 CONDICIONES COMERCIALES

3.5.7.1.1 FORMA DE PAGO

A continuación se detalla la forma de pago establecido

60 % A la firma del proyecto

40% Una vez finalizado el proyecto

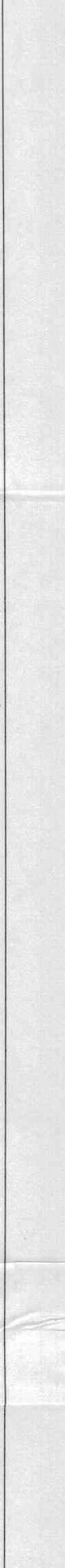
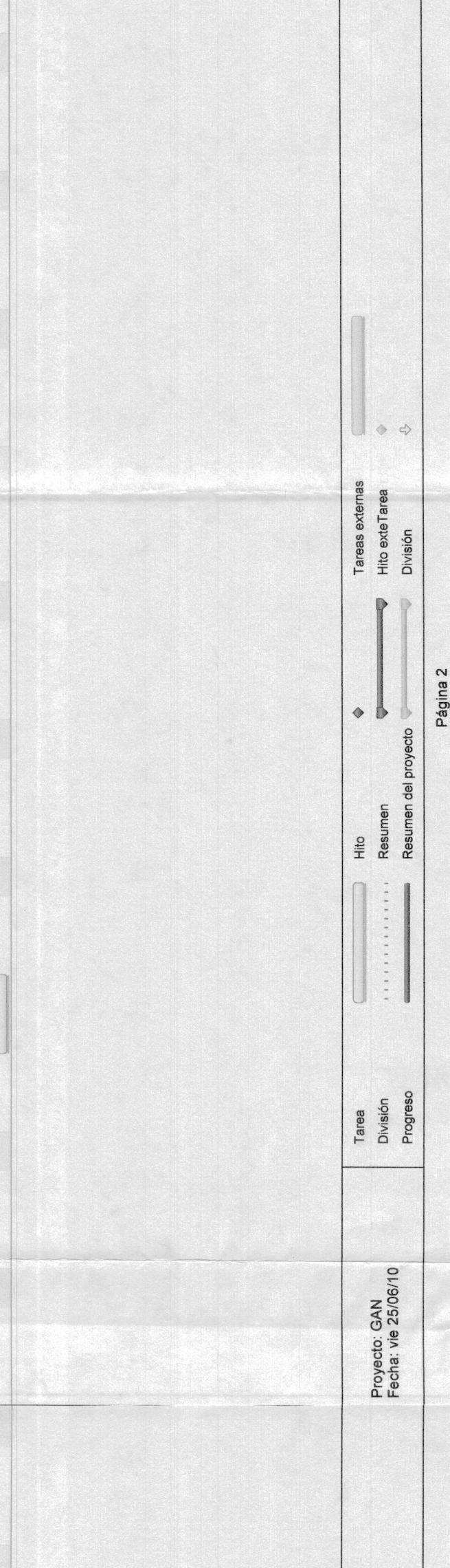
3.5.7.1.2 GARANTÍA DE LA ALTERNATIVA “B”

- ✓ Soporte técnico por 6 meses en las configuraciones de los dispositivos de comunicación
- ✓ Garantía por 3 año por los dispositivos de conmutación por parte de la empresa vendedora



BIBLIOTECA
CAMPUS
PEÑAS

3.5.8 DIAGRAMA GANTT ALTERNATIVA “B”

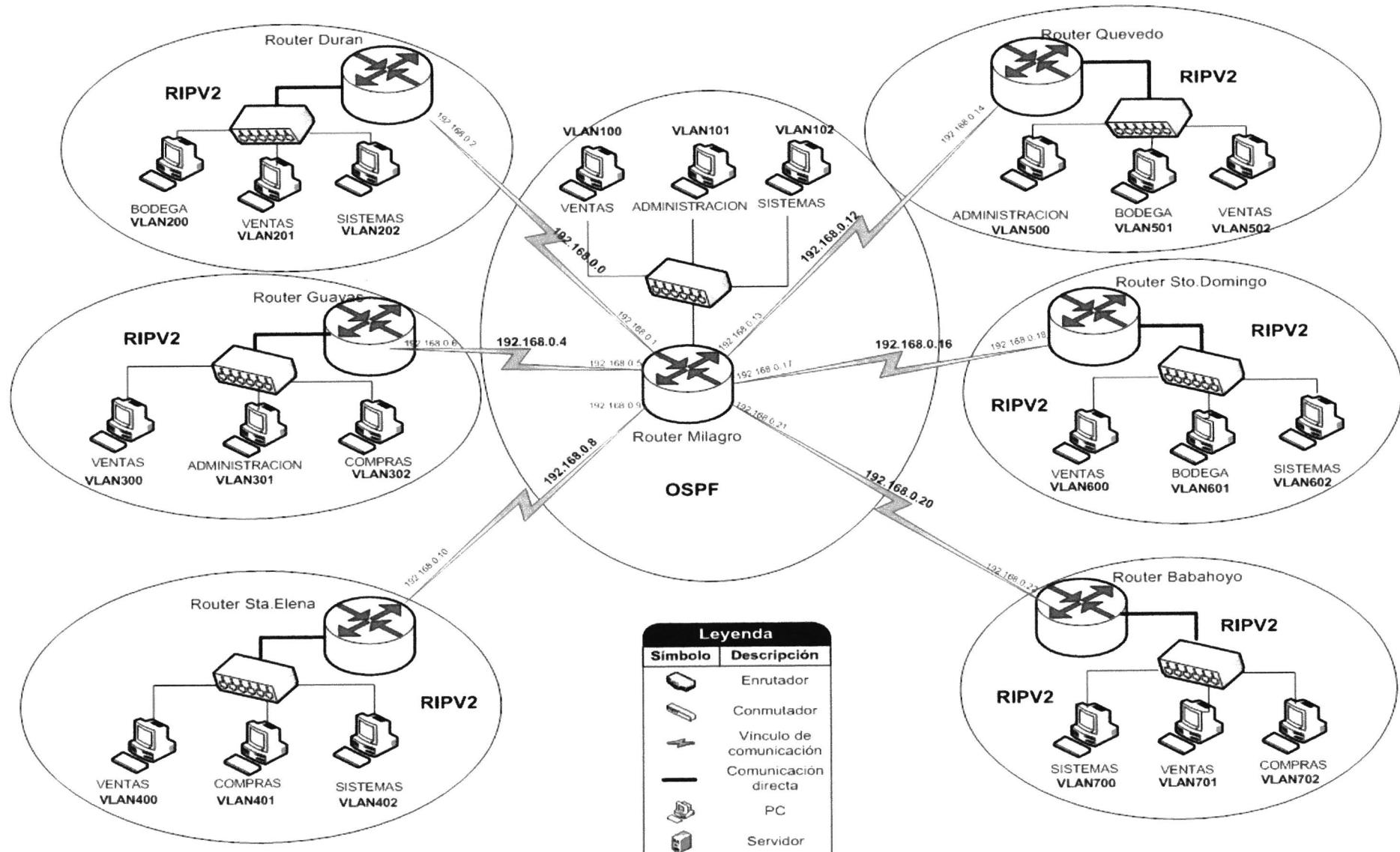




CAPÍTULO 4

CONFIGURACION DE DISPOSITIVOS DE CONMUTACION Y ENRUTAMIENTO

4 GRÁFICO DE RED LAN Y WAN DE DEVIES CORP



4.1 INTRODUCCION A LOS ROUTERS

El enrutador (calco del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. Un router es básicamente un ordenador muy rápido. Tiene un procesador, memoria, software y conexiones de entrada y salida. Estas entradas y salidas serán donde se conecten los equipos de red, los cuales queremos que comuniquen con otros equipos.

4.2 MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER

4.2.1 CABLE DCE (Data Circuit Equipment)

Es el cable que se conectará al equipo que realiza la función de DCE. Para simular la conexión serie con otro router, se utilizan dos cables uno DCE-DTE. Siendo el DCE el que marcará el clock rate.

Es un conector hembra distingible por tener el conector smartnet más pequeño.



Figura 4-1 Cable DCE

4.2.2 CABLE DTE (Data Terminal Equipment)

Es el cable que se conectará al equipo que realiza la función de DTE. Generalmente será el cable que unirá un router a un modem CSU/DSU.

Es un conector macho distingible por tener el conector smartnet más grande.

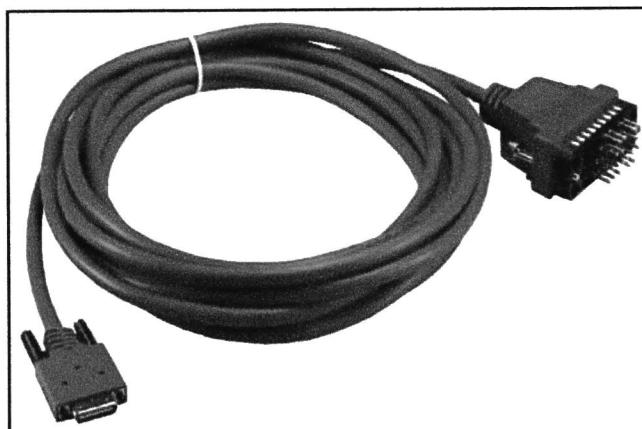


Figura 4-2 Cable DTE

4.2.3 CABLE UTP (Cat 5E)

Es el cable más usado y provee una infraestructura a través de la cual la mayoría de los productos pueden ser conectados. El diseño de un Sistema de cableado UTP tiene una configuración de estrella, están conectados a un Patch Panel Central y los HUB's o Switch son utilizados para conectar a un servicio.

El cable consiste en 4 pares torcidos y existen 5 categorías siendo las tres más importantes (3, 4 y 5) utilizadas en transmisión de datos. El cable Categoría 5 soporta transmisión de datos hasta 100 Megabytes por segundo



Figura 4-3 Cable UTP Cat 5E

4.2.4 CONECTOR RJ45

El RJ45 es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado, (el conector es similar al enchufe de plástico que se utiliza para conectar un cordón telefónico con un enchufe telefónico de pared)

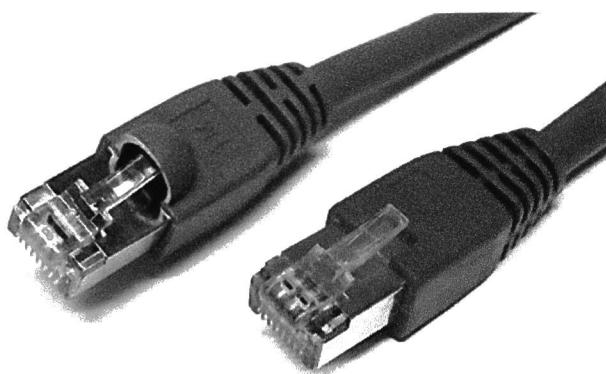


Figura 4-4 Conector RJ45



BIBLIOTECA
CAMPUS
PENAS

4.2.5 PUERTO SERIAL (CONECTOR COM)

Los puertos serie, también llamados puertos de comunicación (COM), son bidireccionales. La comunicación bidireccional permite a cada dispositivo recibir datos, así como también transmitirlos. Los dispositivos seriales usan distintos pines para recibir y transmitir datos. Usando el mismo pin, limitaría la comunicación a half-duplex, esto quiere decir que la información solamente podría viajar en una dirección a la vez.

Usando distintos pines, permite que la comunicación sea full-duplex, en la cual la información puede viajar en ambas direcciones al mismo tiempo.

La mayoría de los software utilizan el término COM (derivado de comunicaciones) seguido de un número para designar un puerto serie (por ejemplo, COM1 ó COM2).

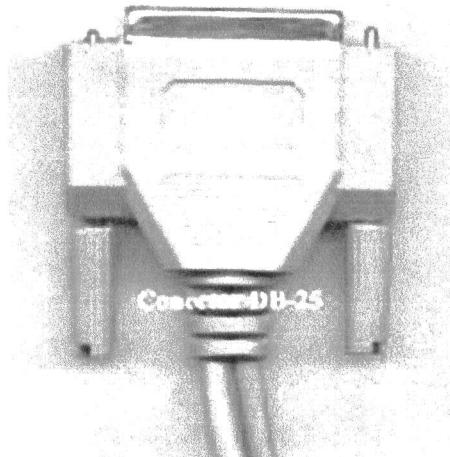


Figura 4-5 Puerto serial



BIBLIOTECA
CAMPUS
PEÑAS

4.2.6 PARTES INTERNAS DE UN ROUTER

Entre los principales componentes de un enrutador son:

- ✓ RAM/DRAM: Almacena las tablas de enrutamiento, el caché ARP, el caché de commutación rápida, el búfering de paquetes (RAM compartida) y las colas de espera de paquetes. La RAM también proporciona memoria temporal y/o de trabajo para el archivo de configuración de un router mientras el router está encendido. El contenido de la RAM se pierde si se produce un corte de energía eléctrica o si se reinicia el equipo
- ✓ NVRAM: La RAM no volátil almacena la copia de respaldo del archivo de configuración/archivo de configuración de inicio del router. El contenido de la NVRAM se conserva durante un corte de energía o si se reinicia el equipo.
- ✓ Flash: ROM borrible y reprogramable que retiene la imagen y el microcódigo del sistema operativo. La memoria Flash activa las actualizaciones del software sin eliminar ni reemplazar los chips del procesador. El contenido de la Flash se conserva durante los cortes de energía o reinicio. La memoria Flash puede almacenar múltiples versiones del software IOS
- ✓ ROM: Contiene diagnósticos de encendido, un programa bootstrap y software del sistema operativo. Las actualizaciones del software en la ROM requieren la eliminación y el reemplazo de chips enchufables en la CPU



BIBLIOTECA
CAMPUS
PEÑAS

La principal responsabilidad de un router es dirigir los paquetes destinados a redes locales y remotas al:

Determinar la mejor ruta para enviar paquetes hacia su destino; el router usa su tabla de enrutamiento para determinar la mejor ruta para reenviar el paquete. Cuando el router recibe un paquete, examina su dirección IP de destino y busca la mejor coincidencia con una dirección de red en la tabla de enrutamiento del router. La tabla de enrutamiento también incluye la interfaz que se utilizará para enviar el paquete. Cuando se encuentra una coincidencia, el router encapsula el paquete IP en la trama de enlace de datos de la interfaz de salida. Luego, el paquete se envía hacia su destino.

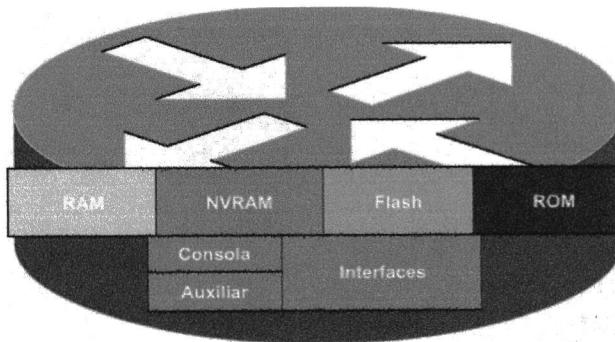


Figura 4-6 Partes internas de un router

4.2.7 PARTES EXTERNAS DEL ROUTER

Un router básicamente tiene tres tipos de interfaces o conexiones: de consola/Aux.

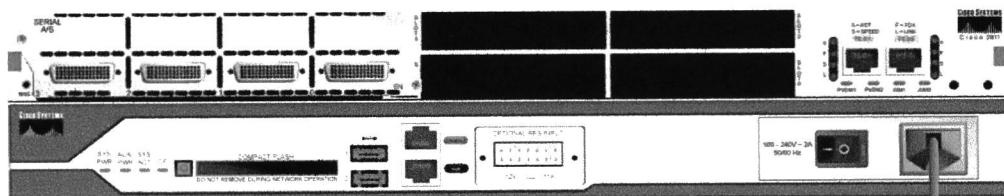


Figura 4-7 Partes Externas de un router

4.2.8 CONEXIONES INTERNAS DEL ROUTER

La función de los puertos de administración es diferente a la de las otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red por donde se transmiten los paquetes. El puerto de administración proporciona una conexión basada en texto para la configuración y diagnóstico de fallas del router. Los puertos auxiliares y de consola constituyen las interfaces de administración comunes. Estos son paquetes seriales asíncronos EIA – 232. Están conectados a un puerto de comunicaciones de un computador.

El computador debe ejecutarse un programa de comunicación de terminal para iniciar la sesión basada en el texto con el router.

4.3 INTERFAZ DTE-DCE

En una comunicación hay cuatro unidades básicas involucradas, un DTE y un DCE en un extremo y un DTE y un DCE en el otro. Un DTE genera los datos y los pasa a su DCE que los convierte a un formato apropiado y los introduce en la red. Cuando llega la señal al receptor, se efectúa el proceso inverso. Para entendernos un DTE podría ser un ordenador y un DCE un modem

Equipo Terminal de datos (DTE)

Incluye cualquier unidad que funcione como origen o destino para datos digitales binarios

Equipo Terminal del circuito de datos (DCE)

En cualquier dispositivo que transmite o recibe datos en forma de señal analógica o digital a través de una red.

4.4 MODOS DEL ROUTER

Modo usuario: Permite consultar toda la información relacionada al router sin poder modificarla. El shell es el siguiente:

Router >

Usuario privilegiado: Permite visualizar el estado del router e importar o exportar imágenes de IOS. El shell es el siguiente:

Router #

Modo de configuración global: Permite utilizar los comandos de configuración generales del router. El shell es el siguiente:

Router (config) #

Modo de configuración de interfaces: Permite utilizar comandos de configuración de interfaces (Direcciones IP, máscaras, etc.). El shell es el siguiente:

Router (config-if) #

Modo de configuración de línea: Permite configurar una línea (ejemplo: acceso al router por Telnet). El shell es el siguiente:

Router (config-line) #

Modo espacial: RXBoot Modo de mantenimiento que puede servir, especialmente, para reiniciar las contraseñas del router. El shell es el siguiente:

4.5 ENRUTAMIENTO

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino.

4.5.1 PROTOCOLOS ENRUTADOS

Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

4.5.2 PROTOCOLOS DE ENRUTAMIENTO

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

Protocolos de enrutamiento:

- ✓ Protocolo de información de enrutamiento (RIP).
- ✓ Protocolo de enrutamiento de gateway interior (IGRP).
- ✓ Protocolo de enrutamiento de gateway interior mejorado (EIGRP).
- ✓ Protocolo “Primero la ruta más corta” (OSPF).

4.5.2.1 ENRUTAMIENTO ESTATICO

Las rutas estaticas deben ser configuradas manualmente por el administrador en el router. La distancia administrativa es un parámetro por lo general opcional que da una medida del nivel de confiabilidad que posee la ruta. La distancia administrativa que posee una ruta estatica es de 1 por defecto.



BIBLIOTECA
CAMPUS
PEÑAS

4.6 ENRUTAMIENTO DINAMICO

Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers, el objetivo de este es crear y mantener una tabla de enrutamiento.

Aprenden todas las rutas disponibles, además de incluir las mejores rutas en las tablas de enrutamiento y descartar rutas que ya no son válidas.

4.6.1.1 TIPOS DE DIRECCIONAMIENTO

Para el diseño de arquitectura de cualquier red, es también muy importante conocer y utilizar los siguientes conceptos, con el fin de optimizar y simplificar el direccionamiento y el tamaño de las tablas de enrutamiento. Gracias a la utilización de estas técnicas, los datos reales a principios de 2000 mostraban que el tamaño de la tabla de enrutamiento era aproximadamente de 76000 rutas.

4.6.1.2 DIRECCIONAMIENTO CON CLASE

Es también conocido como Direccionamiento IP básico. Siguiendo este modelo de direccionamiento, a una dirección IP únicamente se le puede asignar su máscara predeterminada o máscara natural. Esto supone muy poca flexibilidad, y no es recomendable salvo para redes locales muy pequeñas.

4.7 PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO(RIP)

Es uno de los protocolos de enrutamiento mas antiguos utilizado por dispositivos basados en IP. Es un protocolo vector distancia que utiliza la cuenta de saltos de router como métrica. La cuenta de saltos máxima de RIP es de 15. Cualquier ruta que exeda de los 15 saltos se etiqueta como inalcanzable al establecerse la cuenta de saltos en 16. En RIP la información de enrutamiento de propaga de un router a los otros vecinos por medio de una difusión de IP usando el protocolo UDP y el puerto 520.

El protocolo RIP versión 1 es un protocolo de enrutamiento con clase que no admite la publicación de la información de la mascara de red. El protocolo RIP versión 2 es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5.

4.7.1 CARACTERÍSTICAS PRINCIPALES DE RIP

- ✓ Es un protocolo de enrutamiento basado en vector-distancia.
- ✓ Utiliza el número de saltos como métrica para la selección de rutas
- ✓ El número máximo de saltos permitidos en RIP es de 15
- ✓ Difunde actualizaciones de enrutamiento por medio de la tabla de enrutamiento completa cada 30 segundos, por omisión.
- ✓ Puede realizar equilibrado de carga en un máximo de seis rutas de igual coste
- ✓ RIP 1, requiere que se use una sola máscara de red para cada número de red de clase principal que es anunciado. La máscara es una máscara de subred de longitud fija, además no contempla actualizaciones desencadenadas.
- ✓ RIP 2, permite máscaras de subred de longitud variable (VLSM) en la interconexión

4.7.2 FUNCIONAMIENTO RIP

RIP V1 utiliza el puerto UDP 520 para enviar sus mensajes por difusión Broadcast. RIP V2 utiliza propagación multicast 224.0.0.9.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancia. La distancia o métrica está determinada por el número de saltos del router hasta alcanzar la red de destino.

RIP no es capaz de detectar bucles, 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 inalcanzable.

La métrica de un destino se calcula como el número de saltos comunicado por un vecino más la distancia en alcanzar a ese vecino. La tabla de rutas hacia ese destino se actualiza sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la de la ruta almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.

4.7.3 VENTAJAS

- ✓ En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar.
- ✓ Es un protocolo abierto, soportado por muchos fabricantes.



BIBLIOTECA
CAMPUS
PENAS

4.7.4 INCONVENIENTES

- ✓ 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, como por ejemplo ancho de banda de los enlaces.
- ✓ Por ejemplo, si tenemos una metrica de 2 saltos hasta el destino con un enlace de 64 kbps y una metrica de 3 saltos, pero con un enlace de 2 Mbps, lamentablemente RIP tomara el enlace de menor número de saltos aunque sea el más lento. Protocolo usado pero con limitaciones.

4.7.5 LIMITACIONES RIP

- ✓ No envía actualización de máscara de subred en sus actualizaciones.
- ✓ Envía las actualizaciones en Broadcast a 255.255.255.255.
- ✓ No admite la autenticación.
- ✓ No puede admitir enrutamiento entre dominios de VLSM o sin clase (CIDR).

4.7.6 MENSAJES RIP

Los mensajes RIP pueden ser de dos tipos.

Petición: Enviados por algún enrutador recientemente iniciado que solicita información de los enrutadores vecinos.

Respuesta: mensajes con la actualización de las tablas de enrutamiento.

Existen tres tipos:

Mensajes ordinarios: Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos. Se envía la tabla de routeo completa.

Mensajes enviados como respuesta a mensajes de petición.

Mensajes enviados cuando cambia algún coste. Se envía toda la tabla de routeo.



BIBLIOTECA
CAMPUS
PEÑAS

4.8 PROTOCOLO "PRIMERO LA RUTA MÁS CORTA" (OSPF)

Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autenticar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o sin clases CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas.

4.8.1 FUNCIÓN DE OSPF

El fundamento principal en el cual se basa un protocolo de estado de enlace es en la existencia de un mapa de la red el cual es poseído por todos los nodos y que regularmente es actualizado.

Para llevar a cabo este propósito la red debe de ser capaz de entre otros objetivos de:

- ✓ Almacenar en cada nodo el mapa de la red.
- ✓ Ante cualquier cambio en la estructura de la red actuar rápidamente, con seguridad si crear bucles y teniendo en cuenta posibles particiones o uniones de la red.

4.8.1.1 CARACTERÍSTICAS DE OSPF

Las principales características son:

4.8.1.1.1 RESPUESTA RÁPIDA Y SIN BUCLES ANTE CAMBIOS.

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

4.8.1.1.2 SEGURIDAD ANTE LOS CAMBIOS.

Para que el algoritmo de routing funcione adecuadamente debe existir una copia idéntica de la topología de la red en cada nodo de esta.

Existen diversos fallos que pueden ocurrir en la red como fallos de los protocolos de sincronización o inundación, errores de memoria, introducción de información errónea.

El protocolo OSPF especifica que todos los intercambios entre routers deben ser autenticados. El OSPF permite una variedad de esquemas de autenticación y también permite seleccionar un esquema para un área diferente al esquema de otra área. La idea detrás de la autenticación es garantizar que sólo los routers confiables difundan información de routing.

4.8.1.1.3 SOPORTE DE MÚLTIPLES MÉTRICAS.

La tecnología actual hace que sea posible soportar varias métricas en paralelo.

Evaluando el camino entre dos nodos en base a diferentes métricas es tener distintos mejores caminos según la métrica utilizada en cada caso, pero surge la duda de cual es el mejor. Esta elección se realizará en base a los requisitos que existan en la comunicación.

Diferentes métricas utilizadas pueden ser:

- ✓ Mayor rendimiento
- ✓ Menor retardo
- ✓ Menor coste
- ✓ Mayor fiabilidad

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

4.8.1.1.4 BALANCEADO DE CARGA EN MÚLTIPLES CAMINOS.

OSPF permite el balanceado de carga entre los nodos que exista más de un camino. Para realizar este balanceo aplica:

Una versión de SPF con una modificación que impide la creación de bucles parciales.

Un algoritmo que permite calcular la cantidad de tráfico que debe ser enviado por cada camino.

4.8.1.1.5 ESCALABILIDAD EN EL CRECIMIENTO DE RUTAS EXTERNAS.

OSPF soluciona este problema permitiendo tener en la base de datos del mapa local los denominados "gateway link state records". Estos registros nos permiten almacenar el valor de las métricas calculadas y hacen más fácil el cálculo de la ruta óptima para el exterior. Por cada entrada externa existirá una nueva entrada de tipo "gateway link state records" en la base de datos, es decir, la base de datos crecerá linealmente con el número de entradas externas tal como ocurre con los protocolos de vector distancia.

4.8.1.2 TRÁFICO DE ENRUTAMIENTO

OSPF mantiene actualizada la capacidad de enrutamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. Esta difusión se realiza a través de varios tipos de paquetes:

- ✓ Paquetes Hello (tipo 1). Cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.
- ✓ Paquetes de descripción de base de datos estado-enlace (DataBase Description, DBD) (tipo 2). Se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.

Paquetes de estado-enlace o Link State Advertisements (LSA). Los cambios en el estado de los enlaces de un router son notificados a la red mediante el envío de mensajes LSA. Dependiendo del estatus del router y el tipo de información transmitido,

4.8.1.3 TIPOS DE AREA QUE DISTINGUE OSPF

4.8.1.3.1 ÁREA BACKBONE

OSPF establece una jerarquía en la red y la parte en “areas”, existiendo una área especial denominada “backbone area”.

En un “área” se aplica el protocolo OSPF de manera independiente como si de una red aislada se tratase, es decir, los routers del area solo contiene en su mapa local la topología del área, así que el coste en calculo es proporcional al tamaño del área y no de la totalidad de la red.

Cada área incluye un conjunto de subredes IP. La comunicación entre routers de un área se resuelve directamente a través del mapa local de área que cada router posee.

4.8.1.3.2 ÁREA STUB

El problema del incremento de rutas externas que debían ser summarizadas en multitud de áreas pequeñas ha quedado resuelto con la introducción del concepto de “stub area” un área donde todas las rutas externas son summarizadas por una ruta por defecto.

Una stub area funciona exactamente igual que una area normal de OSPF con unas cuantas restricciones, acerca de prohibir la entrada de rutas externas en las bases de datos de los routers.

También no se podrá conectar un “border route” con una “stub area”. Esto es lógico si nosotros consideramos que los “border routers” conectan los sistemas autónomos con Internet y normalmente deberían estar sujetos a la “backbone area” .

Los nodos de una red basada en OSPF se conectan a ella a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace (link) define la configuración que asume la interfase correspondiente. OSPF soporta las siguientes tipos de enlace, y provee para cada uno de ellos una configuración de interfaz:

- ✓ Punto a punto (point-to-point, abreviadamente ptcp).
- ✓ Punto a multipunto (point-to-multipoint, abreviadamente ptmp).
- ✓ Broadcast.
- ✓ Enlace virtual (virtual link).
- ✓ Enlace de múltiple acceso no-broadcast (Non-broadcast Multiple Access, NBMA).

4.8.2 INTERFACES EN OSPF

Los nodos de una red basada en OSPF se conectan a ella a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace (link) define la configuración que asume la interfase correspondiente. OSPF soporta las siguientes tipos de enlace, y provee para cada uno de ellos una configuración de interfaz:

- ✓ Punto a punto (point-to-point, abreviadamente ptcp).
- ✓ Punto a multipunto (point-to-multipoint, abreviadamente ptmp).
- ✓ Broadcast.
- ✓ Enlace virtual (virtual link).
- ✓ Enlace de múltiple acceso no-broadcast (Non-broadcast Multiple Access, NBMA).

4.8.3 ESTADO DE LAS INTERFACES

- ✓ Down (sin actividad).
- ✓ Waiting (estado de espera).
- ✓ Loopback.
- ✓ Point-to-point (interface punto a punto)
- ✓ DR, abreviatura de Designated Router (interface de enrutador designado).
- ✓ Backup, por Backup Designated Router (interface de enrutador designado auxiliar, BDR).
- ✓ DROther (interface en una red broadcast o NBMA sin estatus DR ni BDR).

4.8.4 ESTADO DESACTIVADO (DOWN)

En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización)

4.8.5 ESTADO DE INICIALIZACIÓN (INIT)

Los routers (enrutadores) OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los Routers vecinos. Cuando una interfaz recibe su primer paquete Hello, el router entra al estado de Inicialización.

Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa.

Los dos tipos de relaciones son Bidireccional y Adyacencia. Un router debe recibir un paquete Hello (Hola) desde un vecino antes de establecer algún tipo de relación.

4.8.6 ESTADO BIDIRECCIONAL (TWO-WAY)

(encaminador = enrutador)

Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de comunicación bidireccional (dos-vías) con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un enrutador ingresa al estado Bidireccional cuando se ve a sí mismo en un paquete Hello proveniente de un vecino.

4.8.7 ESTADO DE INTERCAMBIO (EXCHANGE)

En el estado de intercambio, los encaminadores vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los encaminadores se describen sus bases de datos de estado de enlace entre ellos. Los encaminadores comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace.

Si alguno de los encaminadores recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.

4.8.8 ESTADO CARGANDO (LOADING)

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

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

Sin embargo, cuando un dispositivo aprende información de enrutamiento a partir de diferentes fuentes (p.e. rutas estáticas o a través de diferentes protocolos) Cisco IOS permite que la información aprendida por una fuente sea publicada hacia otros dispositivos utilizando un protocolo diferente. Por ejemplo, que una ruta aprendida a través de RIP sea publicada hacia otros dispositivos utilizando OSPF. Esto es lo que se denomina **“Redistribución”** de rutas. Utilizar un protocolo de enrutamiento para publicar rutas que son aprendidas a través de otro medio (otro protocolo, rutas estáticas o directamente conectadas).

El mecanismo de redistribución es propietario de Cisco IOS. Este mecanismo establece algunas reglas:

- ✓ La ruta a redistribuir debe estar presente en la tabla de enrutamiento.
- ✓ No se redistribuyen rutas que están presentes en tablas topológicas de los protocolos pero no en la tabla de enrutamiento.
- ✓ La ruta redistribuida será recibida por el dispositivo vecino con la métrica raíz del protocolo en el que se redistribuye.

4.8.9 PARA QUÉ SE UTILIZA LA REDISTRIBUCIÓN DE RUTAS

Para que dos dispositivos (routers o switches capa 3) intercambien información de enrutamiento es preciso, en principio, que ambos dispositivos utilicen el mismo protocolo, sea RIP, EIGRP, OSPF, BGP, etc. Diferentes protocolos de enrutamiento, o protocolos configurados de diferente forma (p.e. diferente sistema autónomo en EIGRP) no intercambian información.

Sin embargo, cuando un dispositivo aprende información de enrutamiento a partir de diferentes fuentes (p.e. rutas estáticas o a través de diferentes protocolos) Cisco IOS permite que la información aprendida por una fuente sea publicada hacia otros dispositivos utilizando un protocolo diferente. Por ejemplo, que una ruta aprendida a través de RIP sea publicada hacia otros dispositivos utilizando OSPF. Esto es lo que se denomina "Redistribución" de rutas. Utilizar un protocolo de enrutamiento para publicar rutas que son aprendidas a través de otro medio (otro protocolo, rutas estáticas o directamente conectadas). El mecanismo de redistribución es propietario de Cisco IOS. Este mecanismo establece algunas reglas:

- ✓ La ruta a redistribuir debe estar presente en la tabla de enrutamiento.
- ✓ No se redistribuyen rutas que están presentes en tablas topológicas de los protocolos pero no en la tabla de enrutamiento.
- ✓ La ruta redistribuida será recibida por el dispositivo vecino con la métrica raíz del protocolo en el que se redistribuye.

4.8.10 LAS MÉTRICAS

Cada protocolo de enrutamiento utiliza una métrica diferente. Esto hace que al redistribuir rutas se pierda la métrica original del protocolo y sea redefinida en los términos del nuevo protocolo. Por ejemplo, si se redistribuye una ruta OSPF con una métrica de 1642 en RIP, RIP le asignará una métrica en cantidad de saltos (entre 1 y 15).

La métrica con la que un protocolo recibe las rutas aprendidas por otro, se denomina **métrica raíz**.

Cada protocolo utiliza una métrica raíz por defecto:

- ✓ RIP - métrica raíz por defecto: infinito.
- ✓ EIGRP - métrica raíz por defecto: infinito.
- ✓ OSPF - métrica raíz por defecto: 20.

Esta métrica raíz por defecto también puede ser modificada utilizando el comando **default metric**.

4.8.11 REDISTRIBUCIÓN EN RIP

Como en EIGRP, al redistribuir en RIP el protocolo utiliza una métrica por defecto de infinito, con lo que es necesario especificar una métrica diferente para que el router vecino incorpore la información de enrutamiento en su tabla.

4.8.12 REDISTRIBUCIÓN EN OSPF

La métrica por defecto que utiliza OSPF es de 20, por lo que no exige que especifiquemos una métrica para que la ruta sea aprendida por los dispositivos adyacentes. Sin embargo, cuando hay múltiples subredes de una misma red y se desea publicar rutas para cada subred, es preciso indicarlo pues de lo contrario OSPF sumarizará todas las subredes al límite de la clase y publicará una sola ruta.

4.9 DEFINICIÓN Y FUNCIÓN DEL SWITCH

El switch (palabra que significa “comutador”) es un dispositivo que permite la interconexión de redes sólo cuando esta conexión es necesaria. Para entender mejor que es lo que realiza, pensemos que la red está dividida en segmentos por lo que, cuando alguien envía un mensaje desde un segmento hacia otro segmento determinado, el switch se encargará de hacer que ese mensaje llegue única y exclusivamente al segmento requerido.

El switch opera en la capa 2 del modelo OSI, que es el nivel de enlace de datos, y tienen la particularidad de aprender y almacenar las direcciones (los caminos) de dicho nivel, por lo que siempre irán desde el puerto de origen directamente al de llegada, para evitar los bucles (habilitar mas de un camino para llegar a un mismo destino). Asimismo, tiene la capacidad de poder realizar las conexiones con velocidades diferentes en sus ramas, variando entre 10 Mbps y 100 Mbps.

De esta manera los Switches reciben tramas en una interfaz, seleccionan el puerto correcto por el cual enviar las tramas, y entonces envían la trama de acuerdo a la selección de ruta. Los switches elaboran y mantienen las tablas de envío, además también elaboran y mantienen una topología sin bucles en toda la LAN. Los switches LAN o de la Capa 2 envían tramas en base a la información de la dirección MAC. La diferencia entre la conmutación de Capa 2 y Capa 3 es el tipo de información que se encuentra dentro de la trama.

La latencia de switch es el período transcurrido desde el momento que una trama entra a un switch hasta que la trama sale del switch. La latencia se mide en fracciones de segundo.

4.9.1 LED SISTEMAS – SWITCHES

Una vez que se conecta el cable de energía eléctrica, el switch inicia una serie de pruebas denominadas Autocomprobación de Encendido (POST).

POST se ejecuta automáticamente para verificar que el switch funcione correctamente.

El LED del sistema indica el éxito o falla de la POST. Si el LED del sistema está apagado pero el switch está enchufado, entonces POST está funcionando.

Si el LED del sistema está verde, entonces la POST fue exitosa.

Pero si el LED del sistema está ámbar, entonces la POST falló. La falla de la POST se considera como un error fatal. No se puede esperar que el switch funcione de forma confiable si la POST falla.

4.9.2 LAN VIRTUALES (VLAN)

Las LANs virtuales (VLANs) son agrupaciones, definidas por software, de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes. Este concepto, fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un complejo conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de conmutación LAN se están introduciendo en este nuevo mundo a través de caminos diferentes, complicando aún más su divulgación entre los usuarios.

Además, la red virtual simplifica el problema de administrar los movimientos, adiciones y cambios del usuario dentro de la empresa. Asimismo, se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica al coste de unas pocas pulsaciones del administrador de la red.

4.9.3 TIPOS DE VLAN

Por la razón de que hay varias formas en que se puede definir una VLAN, se dividen éstas en cuatro tipos principales: basadas en puertos, basadas en MAC, VLANs de capa 3 y basada en reglas (policy based).

4.9.3.1 VLANS BASADAS EN PUERTOS (MEMBERSHIP BY PORT GROUP)

Según este esquema, la VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o también, en algunos casos, sobre varios conmutadores. La asignación de los equipos a la VLAN se hace en base a los puertos a los que están conectados físicamente.

Muchas de las primeras implementaciones de las VLANs definían la pertenencia a la red virtual por grupos de puertos (por ejemplo, los puertos 1,2,3,7 y 8 sobre un conmutador forman la VLAN A, mientras que los puertos 4,5 y 6 forman la VLAN B). Además, en la mayoría, las VLANs podían ser construidas sobre un único conmutador.

La segunda generación de implementaciones de VLANs basadas en puertos contempla la aparición de múltiples conmutadores (por ejemplo, los puertos 1 y 2 del conmutador 1 y los puertos 4,5,6 y 7 del conmutador 2 forman la VLAN A; mientras que los puertos 3,4,5,6,7 y 8 del conmutador 1 combinados con los puertos 1,2,3 y 8 del conmutador 2 configuran la VLAN B). Este esquema es el descrito por la figura 3.

La agrupación por puertos es todavía el método más común de definir la pertenencia a una VLAN, y su configuración es bastante directa. El definir una red virtual completamente basada en puertos no permite a múltiples VLANs el incluir el mismo segmento físico (o conmutador).

De todos modos, la principal limitación de definir VLANs por puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro.

4.9.3.2 VLAN BASADAS EN MAC (MEMBERSHIP BY MAC ADDRESS)

Constituye la segunda etapa de la estrategia de aproximación a la VLAN, y trata de superar las limitaciones de las VLANs basadas en puertos. Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC. Este tipo de implementación tiene varias ventajas y desventajas.

Desde que las direcciones MAC (media access control -control de acceso al medio-) se encuentran implementadas directamente sobre la tarjeta de interfaz de la red (NIC - network interface card-), las VLANs basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLANs basadas en MAC pueden ser vistas como una VLAN orientada al usuario.

Entre los inconvenientes de las VLANs basadas en MAC está el requerimiento de que todos los usuarios deben inicialmente estar configurados para poder estar en al menos una VLAN. Después de esa configuración manual inicial, el movimiento automático de usuarios es posible, dependiendo de la solución específica que el distribuidor haya dado. Sin embargo, la desventaja de tener que configurar inicialmente la red llega a ser clara en redes grandes, donde miles de usuarios deben ser asignados explícitamente a una VLAN particular. Algunos distribuidores han optado por realizar esta configuración inicial usando herramientas que crean VLANs basadas en el actual estado de la red, esto es, una VLAN basada en MAC es creada para cada subred.

4.9.3.3 VLANS DE CAPA 3 (LAYER 3-BASED VLANS).

Las VLANs de capa 3 toman en cuenta el tipo de protocolo (si varios protocolos son soportados por la máquina) o direcciones de la capa de red, para determinar la pertenencia a una VLAN. Aunque estas VLANs están basadas en información de la

capa 3, esto no constituye una función de encamiento y no debería ser confundido con el enrutamiento en la capa de red.

Habiendo hecho la distinción entre VLANs basadas en información de la capa 3 y el concepto de encaminamiento o routing, hay que apuntar que algunos distribuidores están incorporando varios conceptos de la capa 3 en sus conmutadores, habilitando funciones normalmente asociadas al enrutamiento.

Hay varias ventajas en definir VLANs de capa 3. En primer lugar, permite el particionado por tipo de protocolo, lo que puede parecer atractivo para los administradores que están dedicados a una estrategia de VLAN basada en servicios o aplicaciones. En segundo lugar, los usuarios pueden físicamente mover sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de la estación (este es un beneficio principalmente para los usuarios de TCP/IP). Y en tercer lugar,

definir una VLAN de capa 3 puede eliminar la necesidad de marcar las tramas para comunicar miembros de la red mediante conmutadores, reduciendo los gastos de transporte.

Una de las desventajas de definir la VLAN de capa 3 (al contrario de lo que ocurría en las dos anteriores) es su modo de trabajo. El inspeccionar direcciones de la capa 3 en paquetes consume más tiempo que buscar una dirección MAC en tramas. Por esta razón, los conmutadores que usan información de la capa 3 para la definición de VLANs son generalmente más lentos que los que usan información de la capa 2. Esta diferencia no ocurre en todas las distintas implementaciones de cada distribuidor.

Las VLANs basadas en capa 3 son particularmente efectivas en el trato con TCP/IP, pero mucho menos efectivas con protocolos como IPX, DECnet o AppleTalk, que no implican configuración manual. Además tienen la dificultad al tratar con protocolos no enrutables como NetBIOS (estaciones finales que soportan protocolos no enrutables no pueden ser diferenciadas y, por tanto, no pueden ser definidas como parte de una VLAN).

4.9.3.4 VLANS BASADAS EN REGLAS (POLICY BASED VLANS).

Este esquema es el más potente y flexible, ya que permite crear VLANs adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. Estas reglas pueden ser, por ejemplo, de acceso, con objeto de alcanzar unos ciertos niveles de seguridad en la red. Una vez que el conjunto de reglas que constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red.

4.10 LISTAS DE CONTROL DE ACCESO

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

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

Las ACLs son conjuntos de reglas con un identificador común y que las reglas aplican una acción a los paquetes que cumplan una condición que, en el caso de las ACL estándar, es que tengan la dirección origen coincidente con la dirección de referencia.



BIBLIOTECA
CAMPUS
PEÑAS

4.10.1 FUNCIONAMIENTO DE LAS ACL

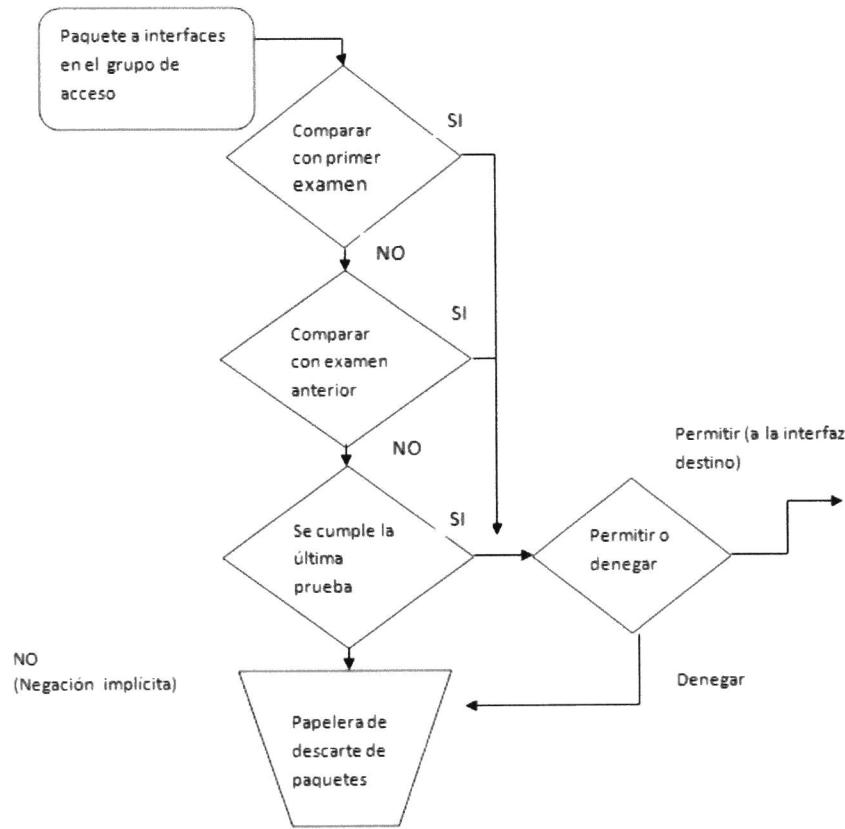


Figura 4-8 Diagrama Funcionamiento de un ACL

4.10.1.1 MÁSCARA DE WILDCARD

Una máscara wildcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar cómo tratar los bits de la dirección IP correspondientes.

Las máscaras wildcard no guardan relación funcional con las máscaras de subred. Se utilizan con distintos propósitos y siguen distintas reglas. Las máscaras de subred y las máscaras de wildcard representan dos cosas distintas al compararse con una dirección IP. La máscara wildcard le indica al Router qué bits de la dirección usar en las comparaciones.

4.10.1.2 PALABRAS CLAVES ESPECIALES UTILIZADAS EN LAS ACL

- ✓ Any: Reemplaza la dirección IP con 0.0.0.0 y la máscara wildcard por 255.255.255.255.
- ✓ Esta opción concuerda con cualquier dirección con la que se la compare.
- ✓ Host: Reemplaza la máscara 0.0.0.0. Esta máscara necesita todos los bits de la dirección ACL
- ✓ y la concordancia de dirección del paquete. Esta opción sólo concuerda con una dirección.

4.10.2 TIPO DE ACL: ESTÁNDAR

La idea de las **ACLs estándar** es filtrar tráfico con base en las **direcciones origen** de los paquetes que entran o salen de una interfaz, aquella en la que se instala la ACL. Lo anterior implica un nivel básico de filtrado: direcciones IP origen de todos los paquetes interceptados

4.10.3 TIPO DE ACL: EXTENDIDA

Las ACL extendidas permiten especificar hacia dónde se dirige el tráfico y con ésta característica, puede bloquear o permitir un tráfico mucho más específico: sólo tráfico que proviene del host pero se dirige a una red en particular o a otro host en particular o sólo el tráfico de una red que se dirige a otra red en particular, las acl extendidas no sólo permiten especificar las direcciones origen y destino sino discriminar por protocolos e incluso por parámetros particulares de cada protocolo

4.10.4 LISTA DE ACCESO ENTRANTE

Los paquetes entrantes son procesados antes de ser enrutados a una interfaz de salida, si el paquete pasa las pruebas de filtrado, será procesado para su enrutamiento (evita la sobrecarga asociada a las búsquedas en las tablas de enrutamiento si el paquete ha de ser descartado por las pruebas de filtrado).

4.10.5 LISTA DE ACCESO SALIENTE

Los paquetes entrantes son enrutados a la interfaz de salida y después son procesados por medio de la lista de acceso de salida antes de su transmisión. Las listas de acceso expresan el conjunto de reglas que proporcionan un control añadido para los paquetes que entran en interfaces de entrada, paquetes que se transmiten por el router, y paquetes que salen de las interfaces de salida del router. Las listas de acceso no actúan sobre paquetes originados en el propio router, como las actualizaciones de enrutamiento a las sesiones Telnet salientes.

4.11 TELNET

Es un protocolo de comunicación que permite al usuario una computadora con conexión a internet establecer una sesión como terminal remoto de otro sistema de la red. Si el usuario no dispone de una cuenta en el ordenador o compilador remoto, puede conectarse como usuario anónimo o también por (www).

4.12 PING (ICMP)

Es una petición al emisor para verificar o comprobar el estado del enlace trabajar con un paquete de comunicaciones llamado echo.

4.13 FTP

Es un protocolo de transferencia de archivos que se utiliza en internet y otras redes para transferir archivos entre servidores o entre un usuario o un servidor.

Puerto 21 A nivel general, FTP tiene algunos aspectos reseñables:

- FTP tiene dos conexiones distintas: una para los comandos (control) y otra para la transmisión de ficheros (datos). La manera estándar de hacer un túnel SSH en una conexión FTP se centra únicamente en la protección de la conexión de control, es decir, del login/password de la sesión y de los comandos utilizados. Los ficheros se intercambiarán sin utilizar el túnel SSH.
- Es necesario usar el modo pasivo ("passive mode") para la conexión de datos o de lo contrario el servidor FTP tratará de conectar con la máquina remota que se encuentre al otro lado del túnel SSH (típicamente la propia máquina servidora) y no con la máquina cliente que realiza la petición.

Debido a estos problemas de seguridad, y gracias a las nuevas prestaciones de la versión 2 de SSH, el SSH tunneling en conexiones FTP está siendo reemplazado por conexiones "sftp", que proporcionan protección tanto de datos como de comandos, sin necesidad de modificar el servidor FTP existente.

4.14 SSH

SSH es un protocolo seguro y un conjunto de herramientas para reemplazar otras más comunes (inseguras). Fue diseñado desde el principio para ofrecer un máximo de seguridad y permitir el acceso remoto a servidores de forma segura. SSH se puede utilizar para asegurar cualquier tráfico basado en red, configurándolo como un pipe (p. ej., vinculándolo a cierto puerto en ambos extremos).

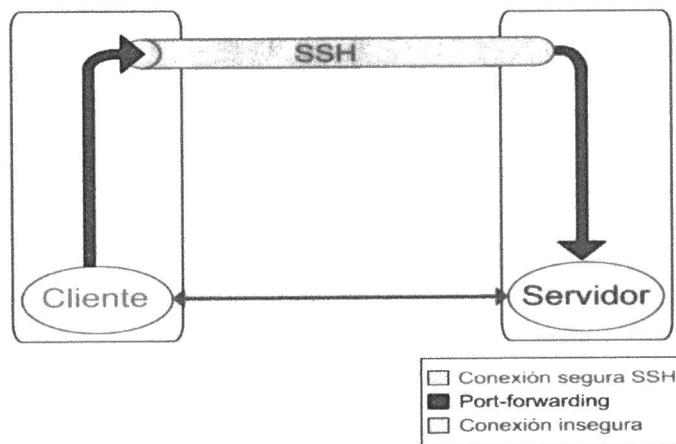


Figura 4-9 SSH

4.15 FIREWALL

Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos.

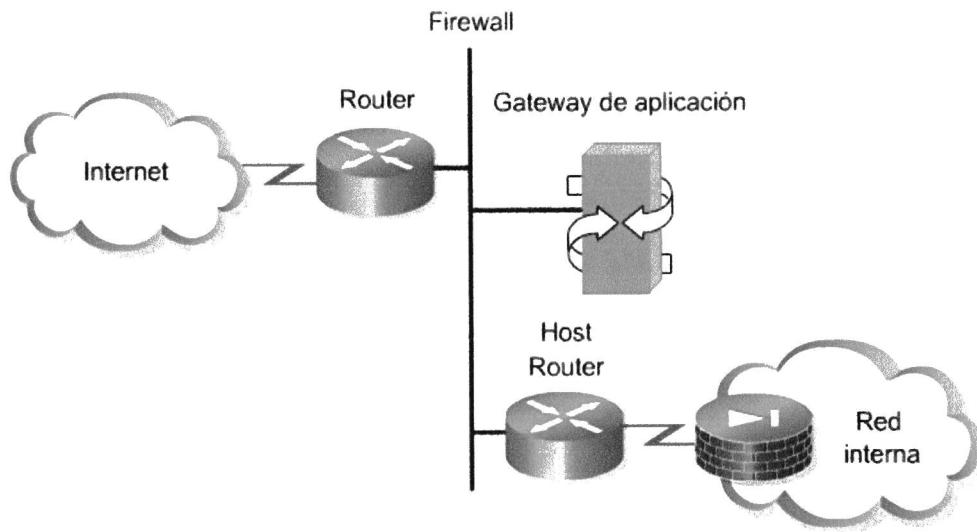


Figura 4-10 Firewall en las ACL

Se deben utilizar ACL en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet.

Se necesita configurar las ACL en routers fronterizos, que son aquellos situados en las fronteras de la red, para brindar mayor seguridad.

4.16 CREACIÓN DE LAS ACL

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

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

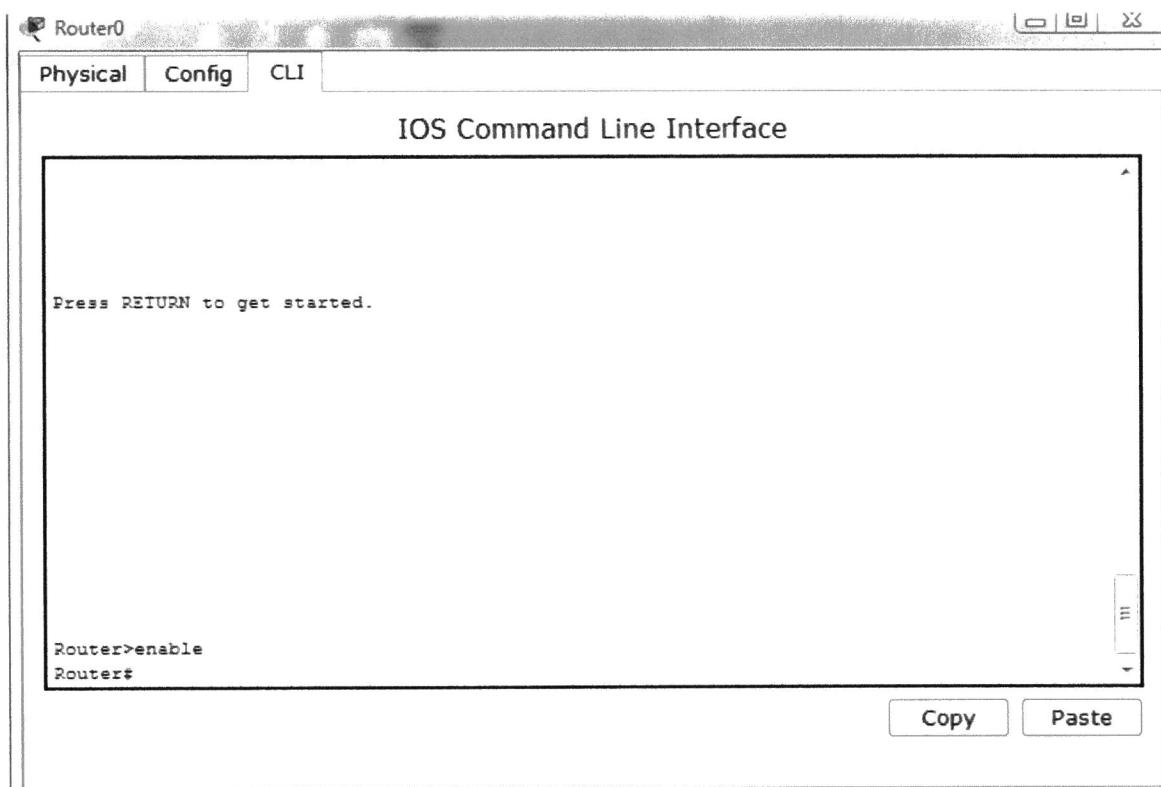


BIBLIOTECA
CAMPUS
PEÑAS

4.17 CONFIGURACION DE ROUTERS

Estos son los comandos mas usados en la configuración de los routers:

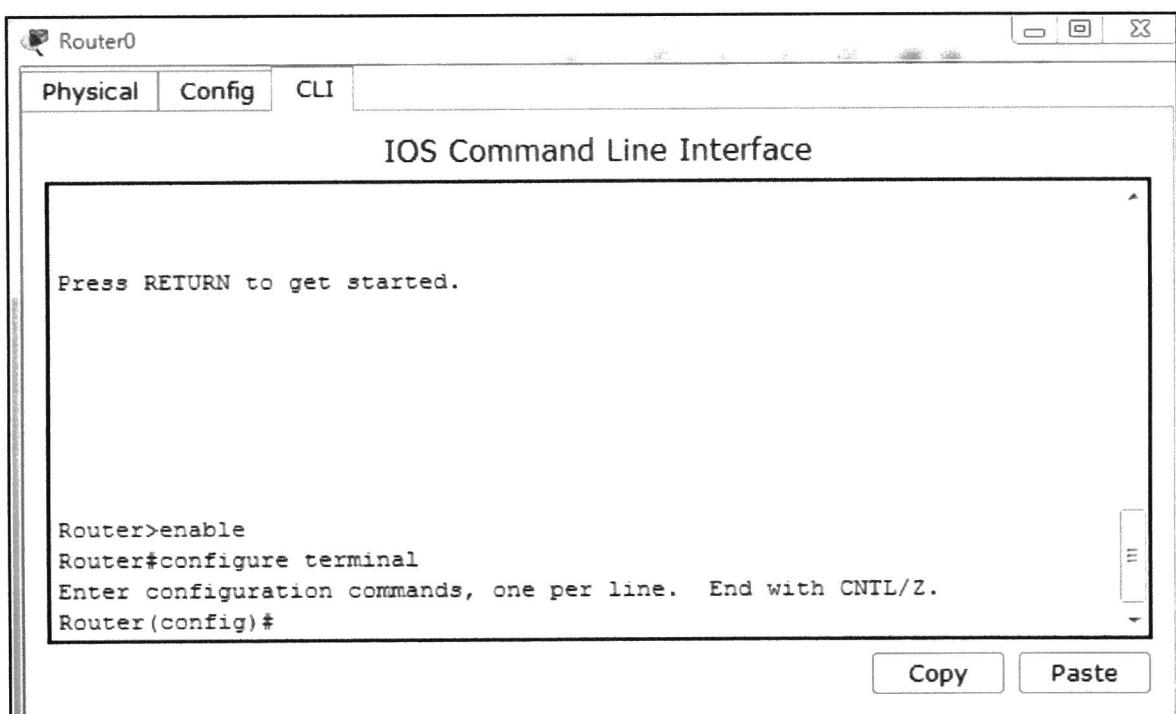
El comando **enable** permite estar en modo de usuario privilegado.



The screenshot shows a window titled "Router0" with three tabs at the top: "Physical", "Config", and "CLI". The "CLI" tab is selected. The main area is labeled "IOS Command Line Interface" and contains the text "Press RETURN to get started.". At the bottom of the screen, the command history shows "Router>enable" and "Router#". Below the terminal window are two buttons: "Copy" and "Paste".

Figura 4-11 Configuración Router

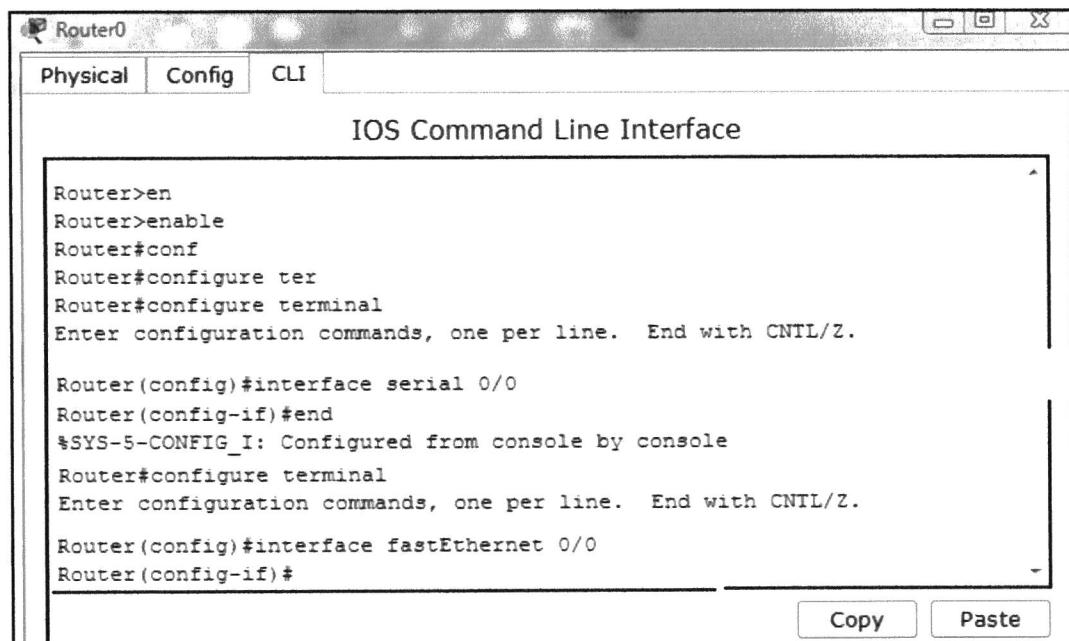
El comando **Configure Terminal** permite pasar al modo configuración global.



The screenshot shows a window titled "Router0" with three tabs at the top: "Physical", "Config", and "CLI". The "CLI" tab is selected. The main area is labeled "IOS Command Line Interface" and contains the text "Press RETURN to get started.". At the bottom of the screen, the command history shows "Router>enable", "Router#configure terminal", and "Enter configuration commands, one per line. End with CNTL/Z.". Below the terminal window are two buttons: "Copy" and "Paste".

Figura 4-12 Configuracion Global

El comando **interface** permite pasar a la configuración de la interfaz dependiendo del tipo: Serial, Ethernet y el número de interfaz.



The screenshot shows the Router0 CLI interface. The title bar says "Router0". The tabs at the top are "Physical", "Config" (which is selected), and "CLI". The main window title is "IOS Command Line Interface". The command history and output area contains the following text:

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

Router(config)#interface serial 0/0
Router(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

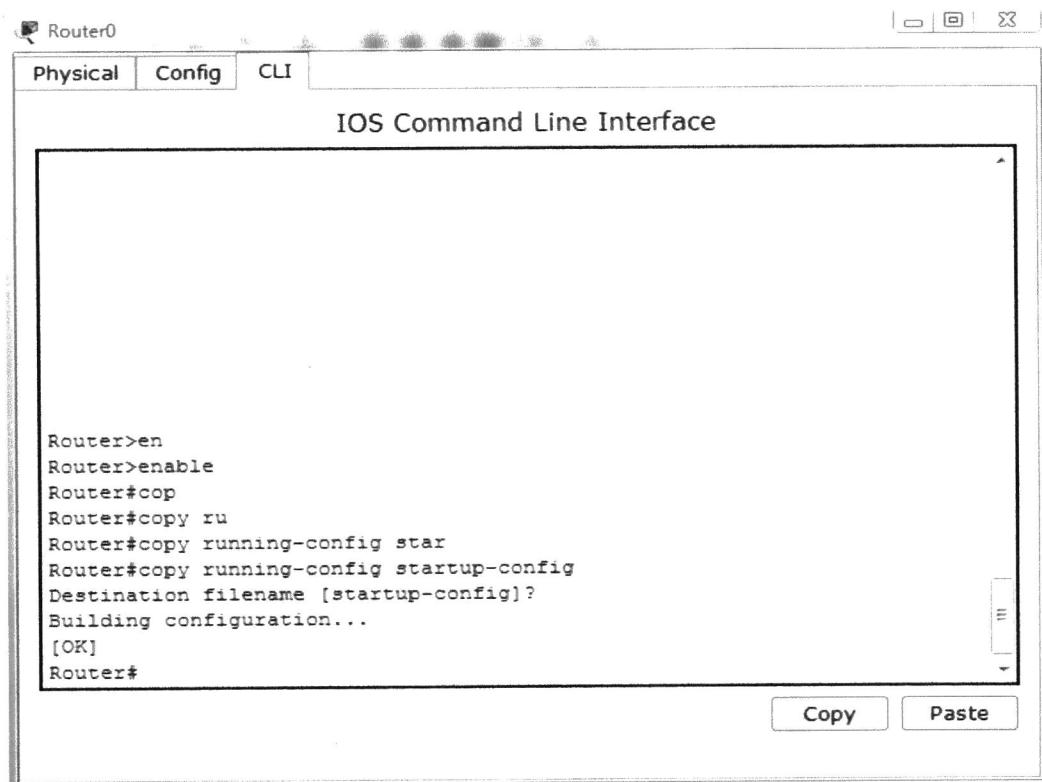
Router(config)#interface fastEthernet 0/0
Router(config-if)#

```

At the bottom right of the main window are "Copy" and "Paste" buttons.

Figura 4-13 Configuracion ethernet

El comando **copy running-config startup-config** copia la configuración almacenada en la NVRAM a la RAM del router



The screenshot shows the Router0 CLI interface. The title bar says "Router0". The tabs at the top are "Physical", "Config" (which is selected), and "CLI". The main window title is "IOS Command Line Interface". The command history and output area contains the following text:

```
Router>en
Router>enable
Router#cop
Router#copy ru
Router#copy running-config star
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#

```

At the bottom right of the main window are "Copy" and "Paste" buttons.

Figura 4-14 Configuración ram del router

El comando **show running-config** permite ver las configuraciones que están actualmente corriendo en el router.

The screenshot shows the Router0 CLI interface with the 'CLI' tab selected. The window title is 'Router0'. The main area displays the output of the 'show running-config' command:

```
Router#show ru
Router#show running-config
Building configuration...

Current configuration : 330 bytes
!
version 12.2
no service password-encryption
!
hostname Router
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
```

At the bottom right of the output window are 'Copy' and 'Paste' buttons.

Figura 4-15 Configuración show running-config

El comando **show ip route** muestra las tablas de enrutamiento

The screenshot shows the Router0 CLI interface with the 'CLI' tab selected. The window title is 'Router0'. The main area displays the output of the 'show ip route' command:

```
--More--
Router>sh
Router>show ip
Router>show ip ro
Router>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
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      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, ia - IS-IS inte
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

Router>
Router>
Router>
```

At the bottom right of the output window are 'Copy' and 'Paste' buttons.

Figura 4-16 Configuración show ip route

El comando **show interfaces** muestra las interfaces

The screenshot shows the Router0 CLI interface. The title bar says "Router0". Below it are three tabs: "Physical", "Config" (which is selected), and "CLI". The main window title is "IOS Command Line Interface". The command entered was "Router#show interfaces". The output details the configuration and status of the FastEthernet0/0 interface, which is administratively down and disabled. It provides information about hardware type (Lance), address, MTU, BW, DLY, encapsulation (ARPA), ARP type, and various counters for input and output traffic.

```
Router#sh
Router#show in
Router#show interfaces
FastEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is Lance, address is 000d.bd8b.938a (bia 000d.bd8b.938a)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    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, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
```

Copy Paste

Figura 4-17 Configuración show interfaces

El comando **ip address** sirve para asignar la dirección IP a una interfaz, el comando **no shutdown** sirve para levantar, dicha interfaz cambiara de estado Up.

The screenshot shows the Router0 CLI interface. The title bar says "Router0". Below it are three tabs: "Physical", "Config" (which is selected), and "CLI". The main window title is "IOS Command Line Interface". The command entered was "Router#conf t", followed by "Router(config)#interface serial 0/0", "Router(config-if)#ip address 192.168.0.1 255.255.255.252", and "Router(config-if)#no shutdown". The output shows the configuration mode prompt "Router(config-if)" and several log messages indicating state changes for the Serial0/0 interface, such as "LINK-5-CHANGED" and "LINEPROTO-5-UPDOWN".

```
Router#conf
Router#configure terminal
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inter
Router(config)#interface se
Router(config)#interface serial 0/0
Router(config-if)#ip ad
Router(config-if)#ip address 192.168.0.1 255.255.255.252
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to down
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
Router(config-if)#

```

Copy Paste

Figura 4-18 Configuración ip address

4.18 COMANDOS BASICOS DE ROUTER

MODO EXE USUARIO

Comando	Descripción
enable	Ingresar al modo EXE privilegiado
logout	Sale del modo EXEC
ping { dirección_ip/nombre}	Envia una petición de eco para diagnosticar la conectividad básica de red
show cdp	Muestra el intervalo entre publicaciones CDP, tiempo de validez y versión de la publicación
show clock	Muestra la hora y fecha del router
show history	Muestra el historial de comandos ingresados
show host	Muestra una lista en cache de nombre host y direcciones
show ip interfaces	Muestra un breve resumen de la información y del estado de una dirección IP
show ip rip database	Muestra el contenido de la base de datos privada de RIP
show ip route [direcciones/protocolo]	Muestra el contenido de la tabla de enrutamiento IP. El parámetro de dirección permite acotar la información que se desea visualizar, exclusivamente a la dirección ingresada. El parámetro protocolo permite por ejemplo:rip ,igrp,static y connected
show sessions	Muestra las conexiones Telnet establecidas en el router
show versión	Muestra información sobre el Cisco IOS y la plataforma
Show ARP	Muestra la tabla arp del router
Show flash	Muestra información acerca de la memoria flash
telnet [dirección ip/nombre]	Permite conectarse remotamente a un host
traceroute	Muestra la ruta tomada por los paquetes hacia un destino

Tabla 4-1 Comandos Basicos del Router

MODO EXEC PRIVILEGIADO

Comando	Descripción
configure memory	Carga información de configuración de la NVRAM
configure terminal	Configura la terminal manualmente desde la terminal de consola
copy flash ftp	Copia la imagen del sistema desde la memoria flash a un servidor ftp
copy running-config startup-config	Guarda la configuracion active en la NVRAM
copy running-config tftp	Almacena la configuración activa de un servidor TFTP
copy tftp running-config	Carga la información recibida de vecinos CDP
disable	Sale del modo EXEC privilegiado hacia el modo EXEC usuario
erase flash	Borra el contenido de la memoria flash
erase starup-config	Borra el contenido de la NVRAM
no debug all	Descativa todas las depuraciones actividades en el dispositivo
reload	Reinicia el router
setup	Entra a la facilidad de dialogo de configuración inicial
show access-list [Nro ACL/nombre_acl]	Muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o numero de ACL como opción a este comando
show arp	Muestra la asignación de direcciones IP a MAC a interfaz del router
show cdp traffic	Muestra los contadores CDP, incluyendo el numero de paquetes enviados y recibidos, y los errores de checksum
show controllers serial [numero]	Muestra infomación importante como que tipo de cable se encuentra conectado
show memory	Muestra estadísticas acerca de las memorias del router, incluyendo estadísticas de memoria disponibles
show processes	Muestra información acerca de los procesos activos
show protocols	Muestra los protocolos de capa 3 configurados
show running-config	Muestra la configuración actual en la RAM

Tabla 4-2 Comandos Modos Exec Privilegiados



BIBLIOTECA
CAMPUS
PEÑAS

MODO DE CONFIGURACION GLOBAL

Comando	Descripción
acces-list Nro_ACL {permit/deny}Origen	Crea o agrega una sentencia de condición a la ACL que permite o denegara los paquetes que llegan desde un origen. Este ultimo parámetro puede ser una dirección IP mas una mascara wildcard, la palabra host mas una dirección IP o el wildcard any
access-list Nro_ACL {permit/deny}proto_origen Destino [operador Nro_puerto]	Crea o agrega una sentencia de condición a la ACL que permitirá o denegara los paquetes de lleguen desde un Origen y vayan hacia un Destino.Promo identifica el protocolo a verificar
boot system rom	Especifica que el router cargue el IOS desdela ROM
boot system tftp nombre_imagen_IOS dir_IP_serverTftp	Especifica que el router cargue el IOS desde un servidor TFTP Ej:boot system tftp c2500-IOS 24.232.150.1
clock set hh:mm:ss mes dia	Modifica la fecha y hora del router Ej clock set 12:30:00 July 12 2004
enable password contraseña	Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio Ej. Enable password class
Enable secret contraseña	Especifica una capa de seguridad adicional mediante de comando enable password Ej. Enable secret class
hostname nombre	Modifica el nombre del router Ej hostmane Lab_A
interface tipo numero	Configura un tipo de interfaz y entra al modo de configuración de interfaz. Ej. Interface Ethernet 0
ip Access-list {standard/extended} nombre	Permite crear una ACL nombrada. Se debe indicar el tipo. Este comando ingresa al router al submundo de configuración que puede reconocerse por el prompt
ip classless	Permite que el router tome en cuéntalos limites con definiciones de clases de las redes en su tabla de enrutamiento y simplemente trasnmita hacia la ruta por defecto
ip domain-look up	Habilita la conversión de nombre a dirección en el router
ip host nombre_host dir_ipl...	Crea una entrada de nombre a direccion estatica en el archive de configuración del router
ip route dirección red mascara dir..ip_salto	Establece rutas estaticas
line tipo numero	Identifica una línea especifica para la configuración e inicia el modo de reunión de comando de configuración

Tabla 4-3 Comandos Modos De Configuracion Global

SUBMODO DE CONFIGURACION DE INTERFAZ

Comando	Descripción
clock rate velocidad	Configura la velocidad de reloj para las conexiones de hardware en interfaces eriales como: modulos de interfaz de red y procesadores de interfaz a una velocidad de bits aceptable Ej. Clock rate 5600
description descripción	Agrega una descripción a la interfaz
ip Access-group NroACL [in/out]	Asigna la ACL indicada a la interfaz ya sea para que verifique los paquetes entrantes (in) o los salientes (out)
ip address dirección_ip_mascara_red	Asigna una dirección y una máscara de subnetmask e inicia el procesamiento ip en una interfaz Ej. 192.168.0.1 255.255.255.0
no shutdown	Reinicia una interfaz desactivada
shutdown	Inhabilita una interfaz

Tabla 4-4 Submodo de configuración de Interfaz

SUBMODO DE CONFIGURACION DE LINEA

Comando	Descripción
access-class Nro_Acl in	En las líneas VTY, asigna una lista de control de acceso a las conexiones establecidas vía telnet
login	Habilita la verificación de la contraseña en el momento de la conexión
password contraseña	Asigna la contraseña a ser solicitada en el momento de la conexión

Tabla 4-5 Submodo de Configuración De Línea

SUBMODO DE CONFIGURACION DEL PROTOCOLO DE ENRUTAMIENTO

Comando	Descripción
network dirección_de_red	Asigna una dirección de red a la cual el router se encuentra directamente conectado, lo que hará que se envíe y reciba publicaciones de enrutamiento a través de esa interfaz, además que sea publicado a los routers vecinos
Redistribute static	Si se asigna una ruta estática a una interfaz que no está definida en el proceso RIP, mediante el comando network, no será publicado la ruta a menos que se digite este comando

Tabla 4-6 Submodo de Configuración del Protocolo



BIBLIOTECA
CAMPUS
PEÑAS

4.19 CONFIGURACION DE LOS ROUTERS

4.19.1 ASIGNACION DE NOMBRE A ROUTERS

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

Router>enable ←—————

En el modo usuario normal, digite el comando enable para ingresar en el modo privilegiado

Router#configure terminal ←————— Ingrese al modo de configuración global

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

Este mensaje aparecerá indicando que debe ingresar comando de configuración

Router(config)#hostname MILAGRO

Con el comando hostname asignamos el nombre del dispositivo

Router>enable

Router#configure terminal

Router(config)#hostname DURAN

Router>enable

Router#configure terminal

Router(config)#hostname STA_ELENA

Router#configure terminal

Router(config)#hos

Router(config)#hostname GUAYAS

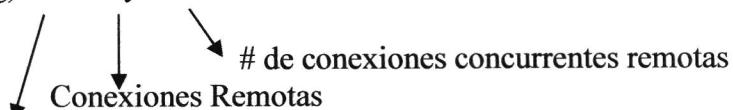
4.19.2 CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER**4.19.3 CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER
MILAGRO**

Se puede restringir el acceso a personas no autorizadas estableciendo contraseñas tanto para la consola como para la terminal.

El **line console 0** se utiliza para establecer contraseña de conexión en el terminal de consola.

El modo de configuración **line vty 0 4** establece contraseña de conexión en sesiones de TELNET.

MILAGRO(config)# line vty 0 4



Tipo

MILAGRO(config-line)#password cisco

Con el comando **password** asignamos la contraseña

MILAGRO(config-line)#login

Con el comando **login active** el inicio con la contraseña

MILAGRO (config-line)#exit

Salga con el comando **exit** para poder configurar el acceso por consola

MILAGRO (config)#line console 0

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

MILAGRO (config-line)#password cisco

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

MILAGRO (config-line)#login

Active el inicio con la contraseña



BIBLIOTECA
CAMPUS
PEÑAS

4.19.4 CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER DURAN

```
DURAN(config)#line vty 0 4  
DURAN (config-line)#password cisco  
DURAN (config-line)#login  
DURAN (config-line)#exit  
DURAN (config)#line console 0  
DURAN (config-line)#password cisco  
DURAN (config-line)#login
```

4.19.5 CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER SANTA ELENA

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

4.19.6 CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER GUAYAS

```
GUAYAS(config)#line vty 0 4  
GUAYAS (config-line)#password cisco  
GUAYAS (config-line)#login  
GUAYAS (config-line)#exit  
GUAYAS (config)#line console 0  
GUAYAS (config-line)#password cisco  
GUAYAS (config-line)#login
```

4.19.7 CONFIGURACION DE INTERFACES SERIALES

La Asignación de las IP'S es uno de los pasos primordiales junto con la asignación de los protocolos para establecer comunicación.

La forma de asignar las IP es la misma tanto en routers como en switches, se aplica el comando **interface serial/interface ethernet /interface fastethernet(A)**, en donde A es el número de la interfaz, entra a la interface y con el comando **ip address (dir) (mask)** asigna la dirección donde dir es la dirección IP y mask es la mascara de subred.

Despues de asignar la IP se asigna un **Clock rate** dependiendo si es DCE o DTE, para luego ejecutar el comando **no shutdown** para que la interfaz se levante.

Serial 0/0

MILAGRO>

MILAGRO#configure terminal ← Ingrese al modo de configuración global

Con el comando *configure terminal* ingresamos al modo de usuario privilegiado para poder entrar al modo de configuración general

MILAGRO(config)#interface serial 0/0

```

↓      ↓      ↓
Comando Interfaz Número del Puerto

```

Con el comando *interface serial 0/0* ingresamos a la interfaz a configurar.

MILAGRO (config-if)#ip address 192.168.0.1 255.255.255.252

```

↓      ↓      ↓
Comando Dirección serial de salida Mascara de subred

```

Se asigna la dirección IP y su respectiva mascara de subred con el comando *ip address*

MILAGRO (config-if)#clock rate 56000

```

↓      →
Comando que permite asignar Velocidad de sincronización del
sincronización de reloj en reloj
interfaz DCE

```

MILAGRO (config-if)#no shutdown

Levante la interfaz con el comando *no shutdown*, si desea bajar la interfaz anteponga el *no* al comando *shutdown*

%LINK-5-CHANGED: Interface Serial0/0, changed state to down
Este mensaje aparecerá indicando que esta levantada la interface
Salga con *exit*



BIBLIOTECA
CAMPUS
PEÑAS

Serial 0/1

```
MILAGRO(config)#interface serial 0/1  
MILAGRO(config-if)#ip address 192.168.0.5 255.255.255.252  
MILAGRO(config-if)#clock rate 56000  
MILAGRO(config-if)#no shutdown
```

MILAGRO(config-if)#exit

%LINK-5-CHANGED: Interface Serial0/1, changed state to down
Este mensaje aparecerá indicando que esta levantada la interface
Salga con exit

Serial 0/2

```
MILAGRO(config)#interface serial 0/2  
MILAGRO(config-if)#ip address 192.168.0.9 255.255.255.252  
MILAGRO(config-if)#clock rate 56000  
MILAGRO(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial0/2, changed state to down
MILAGRO(config-if)#ex
MILAGRO(config-if)#exit

Serial 0/3

```
MILAGRO(config)#interface serial 0/3  
MILAGRO(config-if)#ip address 200.200.200.1 255.255.255.252  
MILAGRO(config-if)#clock rate 56000  
MILAGRO(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial0/3, changed state to down
MILAGRO(config-if)#exit

Serial 1/0

```
MILAGRO(config)#interface serial 1/0  
MILAGRO(config-if)#ip address 192.168.0.13 255.255.255.252  
MILAGRO(config-if)#clock rate 56000  
MILAGRO(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial1/0, changed state to down
MILAGRO(config-if)#exit

Serial 1/1

```
MILAGRO(config)#interface serial 1/1  
MILAGRO(config-if)#ip address 192.168.0.17 255.255.255.252  
MILAGRO(config-if)#clock rate 56000  
MILAGRO(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial1/1, changed state to down
MILAGRO(config-if)#exit

Serial 1/2

```
MILAGRO(config)#interface serial 1/2
MILAGRO(config-if)#ip address 192.168.0.21 255.255.255.252
MILAGRO(config-if)#clock rate 56000
MILAGRO(config-if)#no shutdown
```

DURAN>

Serial 0/1

```
DURAN(config)#interface serial 0/1
DURAN(config-if)#ip address 192.168.0.2 255.255.255.252
DURAN(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
Router(config-if)#ex
Router(config-if)#exit

GUAYAS>

```
GUAYAS(config)#interface serial 0/1
GUAYAS(config-if)#ip address 192.168.0.6 255.255.255.252
GUAYAS(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial0/1, changed state to up
GUAYAS(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
GUAYAS(config-if)#exit



BIBLIOTECA
CAMPUS
PEÑAS

4.19.9 PROTOCOLO RIP VERSION 2

MILAGRO>

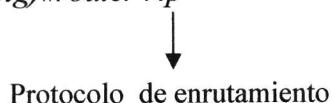
MILAGRO>enable ← Ingrese al modo privilegiado

En el modo usuario normal, digite el comando enable para ingresar en el modo privilegiado

MILAGRO#configure terminal ← Ingrese al modo de configuración global

Con el comando `configure terminal` ingresamos al modo de configuración general

MILAGRO(config)#router rip



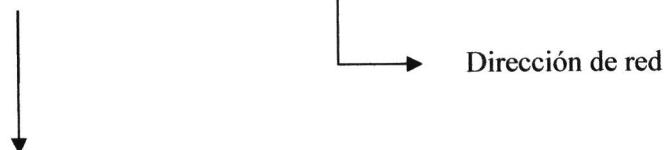
Para configurar el Protocolo RIP en un router, debemos utilizar el comando `router rip`. Para deshabilitar el protocolo RIP debemos anteponer el prefijo `no` al comando.

MILAGRO(config-router)#version 2

Versión del protocolo rip

Para especificar la versión de rip que desea

comando de configuración de enruteamiento versión. Para volver a los valores por defecto usaremos el prefijo no al comando



Network: Identifica las redes directamente conectadas, identificadas por medio de su correspondiente mascara de wildcard

MII-AGB0(config-router)#redistribute ospf1 metric 1

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

Finalmente, grabe los cambios en la NVARM con el comando wr

MILAGRO #wr

Building configuration...

[OK]

MILAGRO #

Redistribuya los paquetes rip por la red ospf

MILAGRO (config-router)#redistribute rip

Redistribute rip: Para que todos los router contenidos dentro del mismo sistema autónomo tengan conocimiento de la existencia de esa ruta es necesario redistribuirla dentro del protocolo

MILAGRO (config-router)#^Z

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



Finalmente, grabe los cambios en la NVARM con el comando wr

MILAGRO #wr

Building configuration...

[OK]

MILAGRO #

Algunos comandos para la verificación y control OSPF son:

Show ip route: Muestra la tabla de enrutamiento**Show ip protocols:** Muestra los parámetros del protocolo**Show ip ospf neighbors:** Muestra la información de los vecinos OSPF**Debut ip ospf events:** Muestra adyacencias, DR, inundaciones etc.**Debug ip ospf packet:** Muestra la información de los paquetes**Debug ip ospf hello:** Muestra las actualizaciones hello

DURAN#ENable
DURAN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DURAN(config)#ROUTer rip
DURAN(config-router)#version 2
DURAN(config-router)#network 192.168.0.0
DURAN(config-router)#network 192.168.1.0
DURAN(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console
DURAN#wr
Building configuration...
[OK]

DURAN#

DURAN #copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
DURAN#
Este mensaje aparecerá cuando se haya grabado todas las configuraciones realizadas correctamente

GUAYAS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
GUAYAS(config)#ROUTer rip
GUAYAS (config-router)#version 2
GUAYAS (config-router)#network 192.168.0.4
GUAYAS (config-router)#network 192.168.2.0
GUAYAS (config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console
GUAYAS #wr
Building configuration...
[OK]



BIBLIOTECA
CAMPUS
PEÑAS

GUAYAS #copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

STA_ELENA #

STA_ELENA#ENable

STA_ELENA#configure terminal

STA_ELENA (config)#ROUTer rip

STA_ELENA (config-router)#version 2

STA_ELENA (config-router)#network 192.168.0.8

STA_ELENA (config-router)#network 192.168.3.0

STA_ELENA (config-router)#^Z

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

STA_ELENA #wr

Building configuration...

[OK]

STA_ELENA#

STA_ELENA #copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

STA_ELENA #



BIBLIOTECA
CAMPUS
PEÑAS

COMANDO SHOW IP ROUTE MILAGRO

Ver contenido Tabla Enrutamiento, rutas que el router conoce

Router>

Router>enable

← Ingrese al modo privilegiado

Digite el comando show ip route

MILAGRO#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
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 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, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

192.168.0.0/30 is subnetted, 6 subnets

C 192.168.0.0 is directly connected, Serial0/0
 C 192.168.0.4 is directly connected, Serial0/1
 C 192.168.0.8 is directly connected, Serial0/2
 C 192.168.0.12 is directly connected, Serial1/0
 C 192.168.0.16 is directly connected, Serial1/1
 C 192.168.0.20 is directly connected, Serial1/2

192.168.1.0/24 is variably subnetted, 5 subnets, 3 masks

R 192.168.1.0/24 [120/1] via 192.168.0.2, 00:00:19, Serial0/0
 O E2 192.168.1.0/28 [110/64] via 192.168.0.2, 00:00:04, Serial0/0

↓
 Camino por el cual la dirección de red se ha aprendido

↓
 Ancho de banda

↓
 Distancia Administrativa

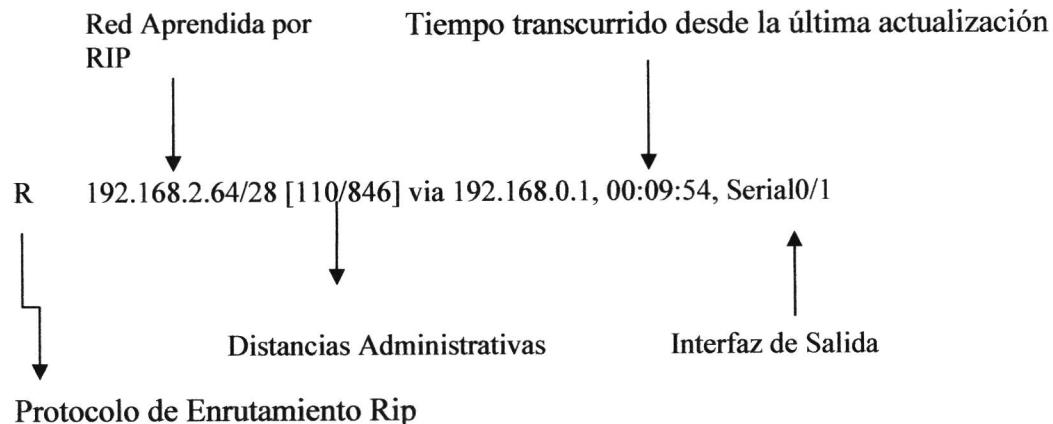
↓
 Longitud de la Mascara

↓
 Dirección de red aprendida por Ospf

↓
 Extendida de 2

↓
 Protocolo de Enrutamiento OSPF

O E2 192.168.5.0/24 [110/64] via 192.168.0.2, 00:00:04, Serial0/0
O E2 192.168.6.0/24 [110/64] via 192.168.0.2, 00:00:04, Serial0/0
 192.168.7.0/28 is subnetted, 4 subnets
C 192.168.7.0 is directly connected, FastEthernet0/0
C 192.168.7.16 is directly connected, FastEthernet0/0.1
C 192.168.7.32 is directly connected, FastEthernet0/0.2
C 192.168.7.48 is directly connected, FastEthernet0/0.3
O E2 200.200.2.0/24 [110/64] via 192.168.0.2, 00:00:04, Serial0/0
 200.200.200.0/30 is subnetted, 1 subnets
C 200.200.200.0 is directly connected, Serial0/3
O 192.168.2.64/28 [110/846] via 192.168.0.1, 00:09:54, Serial0/1



RESULTADO	DESCRIPCION
R	Identifica el origen de la ruta como RIP
192.168.2.64	Identifica la dirección de la red remota
/24	Mascara de subred que se usa para esta red
[110/846]	Distancia Administrativa y la métrica
via 192.168.0.1	Especifica la dirección de router del siguiente salto (R2) que envía tráfico hacia la red remota
00:09:54	Especifica la cantidad de tiempo desde que se actualizó la ruta
Serial0/1	Especifica la interfaz local por la cual se puede llegar a la red remota

Tabla 4-7 Interpretación de una ruta RIP



BIBLIOTECA
CAMPUS
PEÑAS

COMANDO SHOW IP ROUTE DURAN

DURAN#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

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

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, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.0.0/30 is subnetted, 6 subnets

C 192.168.0.0 is directly connected, Serial0/1

O 192.168.0.4 [110/128] via 192.168.0.1, 00:01:36, Serial0/1

O 192.168.0.8 [110/128] via 192.168.0.1, 00:01:36, Serial0/1

O 192.168.0.12 [110/128] via 192.168.0.1, 00:01:36, Serial0/1

O 192.168.0.16 [110/128] via 192.168.0.1, 00:01:36, Serial0/1

R 192.168.0.20 [120/1] via 192.168.0.1, 00:00:07, Serial0/1

192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks

C 192.168.1.0/28 is directly connected, FastEthernet0/0

C 192.168.1.16/30 is directly connected, FastEthernet0/0.1

C 192.168.1.32/30 is directly connected, FastEthernet0/0.2

C 192.168.1.48/30 is directly connected, FastEthernet0/0.3

R 192.168.2.0/24 [120/2] via 192.168.0.1, 00:00:07, Serial0/1

R 192.168.3.0/24 [120/2] via 192.168.0.1, 00:00:07, Serial0/1

R 192.168.4.0/24 [120/2] via 192.168.0.1, 00:00:07, Serial0/1

R 192.168.5.0/24 [120/2] via 192.168.0.1, 00:00:07, Serial0/1

192.168.7.0/28 is subnetted, 3 subnets

O 192.168.7.16 [110/65] via 192.168.0.1, 00:01:36, Serial0/1

O 192.168.7.32 [110/65] via 192.168.0.1, 00:01:36, Serial0/1

O 192.168.7.48 [110/65] via 192.168.0.1, 00:01:36, Serial0/1

R 200.200.2.0/24 [120/2] via 192.168.0.1, 00:00:07, Serial0/1

200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks

R 200.200.200.0/24 [120/1] via 192.168.0.1, 00:00:07, Serial0/1

O 200.200.200.0/30 [110/128] via 192.168.0.1, 00:01:36, Serial0/1

DURAN#

COMANDO SHOW IP ROUTE GUAYAS

GUAYAS#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

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

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, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.0.0/30 is subnetted, 6 subnets

O 192.168.0.0 [110/128] via 192.168.0.5, 00:36:55, Serial0/1

C 192.168.0.4 is directly connected, Serial0/1

O 192.168.0.8 [110/128] via 192.168.0.5, 00:36:55, Serial0/1

O 192.168.0.12 [110/128] via 192.168.0.5, 00:36:55, Serial0/1

O 192.168.0.16 [110/128] via 192.168.0.5, 00:36:55, Serial0/1

R 192.168.0.20 [120/1] via 192.168.0.5, 00:00:12, Serial0/1

R 192.168.1.0/24 [120/2] via 192.168.0.5, 00:00:12, Serial0/1

192.168.2.0/28 is subnetted, 4 subnets

C 192.168.2.0 is directly connected, FastEthernet0/0

C 192.168.2.16 is directly connected, FastEthernet0/0.1

C 192.168.2.32 is directly connected, FastEthernet0/0.2

C 192.168.2.48 is directly connected, FastEthernet0/0.3

R 192.168.3.0/24 [120/2] via 192.168.0.5, 00:00:12, Serial0/1

R 192.168.4.0/24 [120/2] via 192.168.0.5, 00:00:12, Serial0/1

R 192.168.5.0/24 [120/2] via 192.168.0.5, 00:00:12, Serial0/1

192.168.7.0/28 is subnetted, 3 subnets

O 192.168.7.16 [110/65] via 192.168.0.5, 00:36:55, Serial0/1

O 192.168.7.32 [110/65] via 192.168.0.5, 00:36:55, Serial0/1

O 192.168.7.48 [110/65] via 192.168.0.5, 00:36:55, Serial0/1

R 200.200.2.0/24 [120/2] via 192.168.0.5, 00:00:12, Serial0/1

200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks

R 200.200.200.0/24 [120/1] via 192.168.0.5, 00:00:12, Serial0/1

O 200.200.200.0/30 [110/128] via 192.168.0.5, 00:36:55, Serial0/1

GUAYAS#



BIBLIOTECA
CAMPUS
PEÑAS

COMANDO SHOW IP ROUTE SANTA ELENA

STA_ELENA#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

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

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, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.0.0/30 is subnetted, 6 subnets

O 192.168.0.0 [110/128] via 192.168.0.9, 01:10:40, Serial0/1

O 192.168.0.4 [110/128] via 192.168.0.9, 01:10:40, Serial0/1

C 192.168.0.8 is directly connected, Serial0/1

O 192.168.0.12 [110/128] via 192.168.0.9, 01:10:40, Serial0/1

O 192.168.0.16 [110/128] via 192.168.0.9, 01:10:40, Serial0/1

R 192.168.0.20 [120/1] via 192.168.0.9, 00:00:23, Serial0/1

R 192.168.1.0/24 [120/2] via 192.168.0.9, 00:00:23, Serial0/1

R 192.168.2.0/24 [120/2] via 192.168.0.9, 00:00:23, Serial0/1

192.168.3.0/28 is subnetted, 4 subnets

C 192.168.3.0 is directly connected, FastEthernet0/0

C 192.168.3.16 is directly connected, FastEthernet0/0.1

STA_ELENA#

4.19.10 SHOW RUNING-CONFIG

Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica

Router>**Router>enable**

← Ingrese al modo privilegiado

↓ Digite el comando show running-config

MILAGRO(config)# show running-config

Building configuration...

Current configuration : 865 bytes

! _____ Indica la versión del IOS

version 12.2

no service password-encryption

!

hostname MILAGRO

← Muestra el nombre del dispositivo

!

!

ip ssh version 1

!

!

interface FastEthernet0/0

← Muestra la configuración de la interfaz Ethernet

ip address 192.168.0.97 255.255.255.224

duplex auto

← Comunicacion Simultanea

speed auto

!

interface FastEthernet0/0.1

← Muestra la configuración de la sub-interfaz fas Ethernet 0/0.1

encapsulation dot1Q 100

← Encapsulamiento asignando a la vlan 100 por el puerto dot1q

ip address 192.168.0.129 255.255.255.22

↓ Muestra la dirección IP y la máscara de sub red asignada a la VLAN

!

!

interface Serial0/0

← Muestra la dirección IP y la máscara de la seria 0/0

ip address 192.168.0.5 255.255.255.252

clock rate 56000

!

interface Serial0/1

← Muestra la configuración de la interfaz Serial 0/1

ip address 192.168.0.2 255.255.255.252
!
router ospf 1 Muestra que está habilitado el protocolo de enrutamiento OSPF
log-adjacency-changes
redistribute rip subnets Redistribuya los paquetes rip por la red ospf
Indica las redes que se están asignando
network 192.168.0.0 0.0.0.3 area 0
!
router rip

version 2 ← Muestra la versión del protocolo RIP
redistribute ospf 1 metric 1 Redistribucion de los paquetes ospf
Indica las redes que se están asignando
network 192.168.0.0
!
ip classless ← Muestra el acceso a las redes no remotas con
mascaras de sub-red diferentes
!
!
no ip http server ← Indica que no existe servidor http
!
line con 0 ← Indica la configuración del Puerto auxiliar

```
line vty 0 4 ← Configuración remota por telnet
  login
!
!
end ← Muestra la configuración de la interfaz Serial 0/0
```

4.19.11 CONFIGURACION DE SWITCH

4.19.11.1 ASIGNACION DE NOMBRE AL SWITCH MILAGRO

Switch>

Switch>enable ← Ingrese al modo privilegiado

↓ Ingrese al modo de configuración Global
Switch#configure terminal

↓ Asignamos el nombre con el comando hostname
Switch(config)#hostname SW_MILAGRO

↓ Salimos con CRTL+Z
SW_MILAGRO(config)#^Z

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

↓ Guardamos los cambios con el comando copy running-config startup-config
SW_MILAGRO# copy running-config startup-config

Building configuration...

[OK]

SW_MILAGRO#



BIBLIOTECA
CAMPUS
PEÑAS

4.19.12 ASIGNACION DE NOMBRE AL SWITCH DURAN

Switch#configure terminal

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

Switch(config)#ho

Switch(config)#hostname SW_DURAN

SW_DURAN(config)#

4.19.12.1 ASIGNACION DE NOMBRE AL SWITCH GUAYAS

Switch#configure terminal

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

Switch(config)#ho

Switch(config)#hostname SW_GUAYAS

SW_GUAYAS(config)#

4.19.12.2 ASIGNACION DE NOMBRE AL SWITCH SANTA ELENA

Switch#configure terminal

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

Switch(config)#ho

Switch(config)#hostname SW_SANTAELENA

SW_SANTAELENA(config)#

4.19.13 CONFIGURACION DE INTERFACES ETHERNET

MILAGRO

MILAGRO>

MILAGRO>enable ←————

Ingrese al modo privilegiado

En el modo usuario normal, aigue el comando enavie para ingresar en el modo privilegiado

MILAGRO #configure terminal ←———— Ingrese al modo de configuración global

Digite el comando configure terminal para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general

MILAGRO (config)#interface fastEthernet 0/0 → Numero del puerto

↓ Entrar al modo de configuración de interfaz ethernet

Digite el comando interface fastethernet 0/0 para poder ingresar al modo de configuración de la interface fastethernet

MILAGRO (config-if)#ip address 192.168.7.1 255.255.255.240

↓ Asigna una dirección IP y máscara de subred para las rutas.

↓ Dirección ip de la puerta de enlace

↓ Máscara de Subred

Asigne la dirección ip con sus respectivas máscaras de subred con el comando ip address

MILAGRO(config-if)#no shutdown

Levante la interfaz puesta con el comando no shutdown, si quiere bajar la interfaz anteponga el no al comando shutdown

4.19.14 CONFIGURACION DE INTERFACES ETHERNET

DURAN

DURAN>

DURAN#configure terminal

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

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.240

Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

4.19.15 CONFIGURACION DE INTERFACES ETHERNET DURAN

GUAYAS>

```
GUAYAS#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#interface fastEthernet 0/0  
Router(config-if)#ip address 192.168.2.1 255.255.255.240  
Router(config-if)#no shutdown  
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed  
state to up  
Router(config-if)#exit
```

4.19.16 CONFIGURACION DE INTERFACES ETHERNET SANTA ELENA

SANTA ELENA>

```
STA_ELENA #configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
STA_ELENA (config)#interface fastEthernet 0/0  
STA_ELENA (config-if)#ip address 192.168.3.1 255.255.255.240  
STA_ELENA (config-if)#no shutdown  
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed  
state to up
```

4.19.17 CONFIGURACION DE SUB-INTERFACES MILAGRO

Para configurar una sub-interfaz debemos ingresar al modo de usuario privilegiado

FastEthernet 0/0.1

MILAGRO >

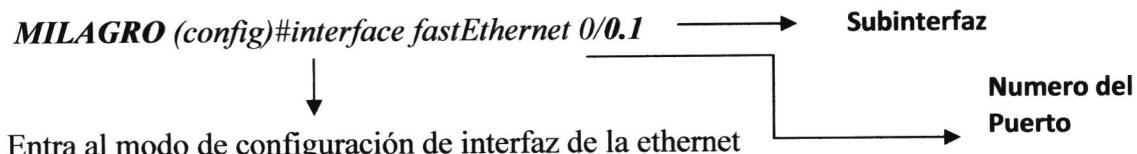
MILAGRO >enable———— Ingrese al modo privilegiado

En el modo usuario normal, digite el comando enable para ingresar en el modo privilegiado

MILAGRO#configure terminal

Ingrese al modo de configuración global

Digite el comando configure terminal para ingresar al modo de usuario privilegiado para poder entrar al modo de configuración general



Digite el comando `interface fastethernet 0/0.1` para ingresar en el modo de configuración de la sub-interfaz

MILAGRO (config-subif)#encapsulation dot1Q 101 → **Numero de la Vlan**

↓
Encapsulamiento de la VLAN

↓
Protocolo de cuminicacion utilizado por las vlans

Para definir el tipo de encapsulamiento digite el comando `encapsulation dot1Q 100` y el y el numero de la VLAN que en este caso en 100

MILAGRO(config-subif)#ip address 192.168.7.17 255.255.255.240

↓
Direccion ip de la Puerta de Enlace

↓
Mascara de red

Asignamos la dirección IP seguida de su máscara de sub-red a las sub-interfaz con el comando `ip address`

MILAGRO(config-subif)#no shutdown

Levante la interfaz puesta con el comando `no shutdown`, si quiere bajar la interfaz anteponga el `no` al comando `shutdown`

FastEthernet 0/0.2

MILAGRO >

MILAGRO >enable ←

Ingrese al modo privilegiado

En el modo usuario normal, sigue el comando `enable` para ingresar en el modo privilegiado

MILAGRO #configure terminal ← Ingrese al modo de configuración global

Ingresamos al modo de usuario global



BIBLIOTECA
CAMPUS
PEÑAS

MILAGRO (config)#interface fastEthernet 0/0.2

↓ ↓ ↓
Comando Interfaz Número de la interfaz

Con el comando *interface fastethernet 0/0.2* ingresamos al modo de configuración de la sub-interfaz

MILAGRO(config-subif)#encapsulation dot1Q 201 → Numero de la Vlan

↓ ↓
Encapsulamiento de la VLAN Protocolo de cuminicacion devlans

Para definir el tipo de encapsulamiento digite el comando *encapsulation dot1Q 400* y el numero de la VLAN que en este caso es 200

MILAGRO (config-subif)#ip address 192.168.7.33 255.255.255.240

↓ ↓
Direccion ip de la Puerta de Enlace Mascara de red

Asignamos la dirección IP seguida de su máscara de sub-red a las sub-interfaz con el comando *ip address*

MILAGRO(config-subif)#no shutdown

Levante la interfaz puesta con el comando *no shutdown*, si quiere bajar la interfaz anteponga el *no* al comando *shutdown*

FastEthernet 0/0.3

MILAGRO >

MILAGRO >enable ← Ingrese al modo privilegiado

En el modo usuario normal, digite el comando *enable* para ingresar en el modo privilegiado

MILAGRO #configure terminal ← Ingrese al modo de configuración global

MILAGRO (config)#interface fastEthernet 0/0.3

Con el comando *interface fastethernet 0/0.3* ingresamos al modo de configuración de la sub-interfaz

MILAGRO (config-subif)#encapsulation dot1Q 301

MILAGRO (config-subif)#ip address 192.168.7.49 255.255.255.240

Asignamos la dirección IP seguida de su máscara de sub-red a las sub-interfaz con el comando *ip address*

MILAGRO (config-subif)#no shutdown

Levante la interfaz puesta con el comando *no shutdown*, si quiere bajar la interfaz anteponga el *no* al comando *shutdown*

4.19.18 CONFIGURACION DE SUB-INTERFACES DURAN

DURAN >

0/0.1

```
DURAN(config)#interface fastEthernet 0/0.1
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed
state to upDURAN(config-subif)#en
DURAN(config-subif)#encapsulation dot1Q 100
DURAN(config-subif)#ip address 192.168.1.17 255.255.255.240
DURAN(config-subif)#no shutdown
DURAN(config-subif)#exit
```

0/0.2

```
DURAN(config)#interface fastEthernet 0/0.2
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed
state to upDURAN(config-subif)#en
DURAN(config-subif)#encapsulation dot1Q 200
DURAN(config-subif)#ip address 192.168.1.50 255.255.255.224
DURAN(config-subif)#no shutdown
DURAN(config-subif)#exit
```

0/0.3

```
DURAN(config)#interface fastEthernet 0/0.3
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed
state to upDURAN(config-subif)#en
DURAN(config-subif)#encapsulation dot1Q 300
DURAN(config-subif)#ip address 192.168.1.82 255.255.255.224
DURAN(config-subif)#no shutdown
DURAN(config-subif)#exit
```



4.19.19 CONFIGURACION DE SUB-INTERFACES GUAYAS

GUAYAS >

0/0.1

```
GUAYAS(config)#interface fastEthernet 0/0.1
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed
state to upDURAN(config-subif)#en
GUAYAS(config-subif)#encapsulation dot1Q 100
GUAYAS (config-subif)#ip address 192.168.2.17 255.255.255.240
GUAYAS (config-subif)#no shutdown
GUAYAS (config-subif)#exit
```

0/0.2

```
GUAYAS (config)#interface fastEthernet 0/0.2
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed
state to upDURAN(config-subif)#en
GUAYAS (config-subif)#encapsulation dot1Q 200
GUAYAS (config-subif)#ip address 192.168.2.50 255.255.255.224
GUAYAS (config-subif)#no shutdown
GUAYAS(config-subif)#exit
```

0/0.3

```
GUAYAS (config)#interface fastEthernet 0/0.3
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed
state to up(config GUAYAS -subif)#en
GUAYAS (config-subif)#encapsulation dot1Q 300
GUAYAS (config-subif)#ip address 192.168.2.82 255.255.255.224
GUAYAS (config-subif)#no shutdown
GUAYAS (config-subif)#exit
```



BIBLIOTECA
CAMPUS
PEÑAS

4.19.20 CONFIGURACION DE SUB-INTERFACES SANTA ELENA

SANTA ELENA >

0/0.1

```
STA_ELENA(config)#interface fastEthernet 0/0.1
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed
state to upDURAN(config-subif)#en
STA_ELENA (config-subif)#encapsulation dot1Q 100
STA_ELENA (config-subif)#ip address 192.168.3.17 255.255.255.240
STA_ELENA (config-subif)#no shutdown
STA_ELENA (config-subif)#exit
```

0/0.2

```
STA_ELENA (config)#interface fastEthernet 0/0.2
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed
state to upDURAN(config-subif)#en
STA_ELENA (config-subif)#encapsulation dot1Q 200
STA_ELENA (config-subif)#ip address 192.168.3.50 255.255.255.224
STA_ELENA (config-subif)#no shutdown
STA_ELENA (config-subif)#exit
```

0/0.3

```
STA_ELENA (config)#interface fastEthernet 0/0.3
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed
state to up(config GUAYAS -subif)#en
STA_ELENA (config-subif)#encapsulation dot1Q 300
STA_ELENA (config-subif)#ip address 192.168.2.82 255.255.255.224
STA_ELENA (config-subif)#no shutdown
GUAYAS (config-subif)#exi
```



BIBLIOTECA
CAMPUS
PEÑAS

4.19.21 CONFIGURACION DE VLAN MILAGRO

Switch>enable ← Ingrese al modo privilegiado

↓ Ingrese a la base de datos VLANs
Switch#vlan database

Vlan Database: La informacion se guarda en una base de datos, archivo vlan.dat en la memoria NVRAM

↓ Crea la VLAN con el comando VLAN

Switch(vlan)#vlan 101 name SISTEMAS

↓ ↓
Número de vlan Nombre de VLAN

Switch(vlan)#vlan [numero de vlan] name [nombre de vlan]

↓ Muestra la agregación de la VLAN
VLAN 101 added:

Name: SISTEMAS

Switch(vlan)#vlan 201 mane ADMINISTRACION

VLAN 201 added:

Name: ADMIN

SW_MILAGRO(config)#^Z

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

↓ Guardamos los cambios con el comando cop r st
SW_MILAGRO#wr

Building configuration...

[OK]

SW_MILAGRO#

4.19.22 CONFIGURACION DE VLAN DURAN

SW_DURAN#vlan database

% Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode.

SW_DURAN(vlan)#vl

SW_DURAN(vlan)#vlan 101 name SISTEMAS

VLAN 101 added:

Name: SISTEMAS

SW_DURAN(vlan)#vlan 102 name VENTAS

VLAN 102 added:

Name: VENTAS

SW_DURAN(vlan)#vlan 103 name BODEGA

VLAN 103 added:

Name: BODEGA

SW_DURAN(vlan)#exi

APPLY completed.

Exiting....

4.19.23 CONFIGURACION DE VLAN GUAYAS

SW_GUAYAS#vlan database

% Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode.

SW_GUAYAS(vlan)#vl

SW_GUAYAS (vlan)#vlan 201 name SISTEMAS

VLAN 101 added:

Name: SISTEMAS

SW_GUAYAS (vlan)#vlan 202 name VENTAS

VLAN 102 added:

Name: VENTAS

SW_GUAYAS (vlan)#vlan 203 name ADMINISTRACION

VLAN 103 added:

Name: BODEGA

SW_GUAYAS (vlan)#exi

APPLY completed.

Exiting....



BIBLIOTECA
CAMPUS
PEÑAS

4.19.24 CONFIGURACION DE VLAN SANTA ELENA

SW_SANTAELENA#vlan database

*% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.*

SW_STAELENA(vlan)#vl

SW_STAELENA (vlan)#vlan 301 name SISTEMAS

VLAN 101 added:

Name: SISTEMAS

SW_STAELENA (vlan)#vlan 302 name VENTAS

VLAN 102 added:

Name: VENTAS

SW_STAELENA (vlan)#vlan 303 name ADMINISTRACION

VLAN 103 added:

Name: BODEGA

SW_STAELENA (vlan)#exi

APPLY completed.

Exiting....

- 4.19.25 ASIGNACION DE PUERTOS A VLANS**
4.19.26 ASIGNACION DE PUERTOS A VLANS MILAGRO

Milagro>

Milagro >enable ← Ingrese al modo privilegiado

↓ Ingrese al modo de configuración Global
Milagro #configure terminal

↓ Digue el comando interface seguido de la interfaz a configurar
Milagro (config)#interface fastEthernet 0/1

↓ Habilite la interfaz para poder establecer un enlace troncal
Milagro (config-if)#switchport mode trunk

Setemos el puerto truncado

Switchport mode trunk: Hace que el puerto envíe información a todas las vlans

La información de todas la vlans creadas viajara por el enlace troncal automáticamente, la vlan 1 que es la vlan por defecto lleva la información de estado de los puertos

↓ Salgamos de la interfaz con exit
Switch(config-if)#exit

Ingresamos a las interfaces fasethernet para dar acceso a las vlan

Switch(config)#interface fastEthernet 0/2



BIBLIOTECA
CAMPUS
PEÑAS

↓ Agregue y de acceso a la VLAN para interfaz
Switch(config-if)#switchport access vlan 101

↓ Comando ↓ Identificador de VLAN

De esta manera se asigno y se da dado acceso a la VLAN 101 por el puerto 2 del switch

4.19.27 ASIGNACION DE PUERTOS A VLANS DURAN

*SW_DURAN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW_DURAN(config)#interface fastEthernet 0/2
SW_DURAN(config-if)#switchport access vlan 101
SW_DURAN(config-if)#ex
SW_DURAN(config)#interface fastEthernet 0/3
SW_DURAN(config-if)#switchport access vlan 102
SW_DURAN(config-if)#ex
SW_DURAN(config)#interface fastEthernet 0/4
SW_DURAN(config-if)#switchport access vlan 103
SW_DURAN(config-if)#ex
SW_DURAN(config)#interface fastEthernet 0/1
SW_DURAN(config-if)#sw
SW_DURAN(config-if)#switchport mode trunk
SW_DURAN(config-if)#+*

4.19.28 ASIGNACION DE PUERTOS A VLANS GUAYAS

*SW_GUAYAS #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW_GUAYAS (config)#interface fastEthernet 0/2
SW_GUAYAS (config-if)#switchport access vlan 201
SW_GUAYAS (config-if)#ex
SW_GUAYAS (config)#interface fastEthernet 0/3
SW_GUAYAS (config-if)#switchport access vlan 202
SW_GUAYAS (config-if)#ex
SW_GUAYAS (config)#interface fastEthernet 0/4
SW_GUAYAS (config-if)#switchport access vlan 203
SW_GUAYAS (config-if)#ex
SW_GUAYAS (config)#interface fastEthernet 0/1
SW_GUAYAS (config-if)#sw
SW_GUAYAS (config-if)#switchport mode trunk
SW_GUAYAS (config-if)#+*

4.19.29 ASIGNACION DE PUERTOS A VLANS SANTA ELENA

SW_STAELENA #configure terminal

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

SW_STAELENA (config)#interface fastEthernet 0/2

SW_STAELENA (config-if)#switchport access vlan 201

SW_STAELENA (config-if)#ex

SW_STAELENA (config)#interface fastEthernet 0/3

SW_STAELENA (config-if)#switchport access vlan 202

SW_STAELENA (config-if)#ex

SW_STAELENA (config)#interface fastEthernet 0/4

SW_STAELENA (config-if)#switchport access vlan 203

SW_STAELENA (config-if)#ex

SW_STAELENA (config)#interface fastEthernet 0/1

SW_STAELENA (config-if)#sw

SW_STAELENA (config-if)#switchport mode trunk

SW_STAELENA (config-if)#{}

COMANDO SHOW VLAN EN EL SWITCH MILAGRO

Switch>

Switch>enable ← Ingrese al modo privilegiado

↓ Digitemos el comando show vlan
Switch#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 → Puertos
		↓
		Estado de la Vlan
Vlan por defecto utilizado por el administrador		Fa0/9, Fa0/10, Fa0/11, Fa0/12
100 SISTEMAS	active	Fa0/2
200 ADMIN	active	Fa0/3
300 CONTABILIDAD	active	Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	



BIBLIOTECA
CAMPUS
PEÑAS

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	0	0	
100 enet	100100	1500	-	-	-	-	0	0	

200	enet	100200	1500	-	-	-	-	0	0
300	enet	100300	1500	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	0	0

VLAN: Muestra el identificador de la VLAN

Ports: Puertos asignados a la VLAN

Type: Tipo de tecnologías de las interfaces

SAID Número de encabezado para identificar las VLANs

MTU: Máximo tamaño de paquetes trasmisidos, se encuentran expresados en bytes

COMANDO SHOW VLAN EN EL SWITCH DURAN

Switch#show vlan

<i>VLAN Name</i>	<i>Status</i>	<i>Ports</i>
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
101 BODEGA	active	Fa0/2
102 VENTAS	active	Fa0/3
103 SISTEMAS	active	Fa0/4
104 VLAN0104	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

<i>VLAN</i>	<i>Type</i>	<i>SAID</i>	<i>MTU</i>	<i>Parent</i>	<i>RingNo</i>	<i>BridgeNo</i>	<i>Stp</i>	<i>BrdgMode</i>	<i>Trans1</i>	<i>Trans2</i>
1 enet	100001	1500	-	-	-	-	0	0		
101 enet	100101	1500	-	-	-	-	0	0		
102 enet	100102	1500	-	-	-	-	0	0		
103 enet	100103	1500	-	-	-	-	0	0		
104 enet	100104	1500	-	-	-	-	0	0		
1002 enet	101002	1500	-	-	-	-	0	0		
1003 enet	101003	1500	-	-	-	-	0	0		

COMANDO SHOW VLAN EN EL SWITCH GUAYAS

Switch#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
201 VENTAS	active	Fa0/2
202 ADMINISTRACION	active	Fa0/3
203 COMPRAS	active	Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	0	0	0
201	enet	100201	1500	-	-	-	-	0	0	0
202	enet	100202	1500	-	-	-	-	0	0	0
203	enet	100203	1500	-	-	-	-	0	0	0
1002	enet	101002	1500	-	-	-	-	0	0	0
1003	enet	101003	1500	-	-	-	-	0	0	0
1004	enet	101004	1500	-	-	-	-	0	0	0
1005	enet	101005	1500	-	-	-	-	0	0	0

Switch#



COMANDO SHOW VLAN EN EL SWITCH SANTA ELENA

Switch#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
201 VLAN0201	active	
202 VLAN0202	active	
203 VLAN0203	active	
301 VENTAS	active	Fa0/2
302 COMPRAS	active	Fa0/3
303 SISTEMAS	active	Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	0	0	
201	enet	100201	1500	-	-	-	-	0	0	
202	enet	100202	1500	-	-	-	-	0	0	
203	enet	100203	1500	-	-	-	-	0	0	
301	enet	100301	1500	-	-	-	-	0	0	
302	enet	100302	1500	-	-	-	-	0	0	
303	enet	100303	1500	-	-	-	-	0	0	
1002	enet	101002	1500	-	-	-	-	0	0	
1003	enet	101003	1500	-	-	-	-	0	0	
1004	enet	101004	1500	-	-	-	-	0	0	
1005	enet	101005	1500	-	-	-	-	0	0	

4.19.30 CONFIGURACION ACCESS LIST

El proceso de creación de una ACL se lleva a cabo creando la lista y posteriormente asociándola a una interfaz entrante o saliente.

En este caso crearemos una ACL que deniega los equipos que estén conectados a las vlans a hacer ping a los routers Core y de importancia en la empresa para evitar posibles ataques

MILAGRO>

MILAGRO >enable ← Ingrese al modo privilegiado

MILAGRO #configure terminal

Con el comando *configure terminal* ingresamos al modo de configuración general

MILAGRO (config)#access-list 102 deny icmp any host 192.168.0.0

Ingresamos los comandos para poder crear una acl

Router(config)#access-list[1-99][permit|deny][dirección de origen][mascara comodín]

1-99:Identifica el rango y la lista.

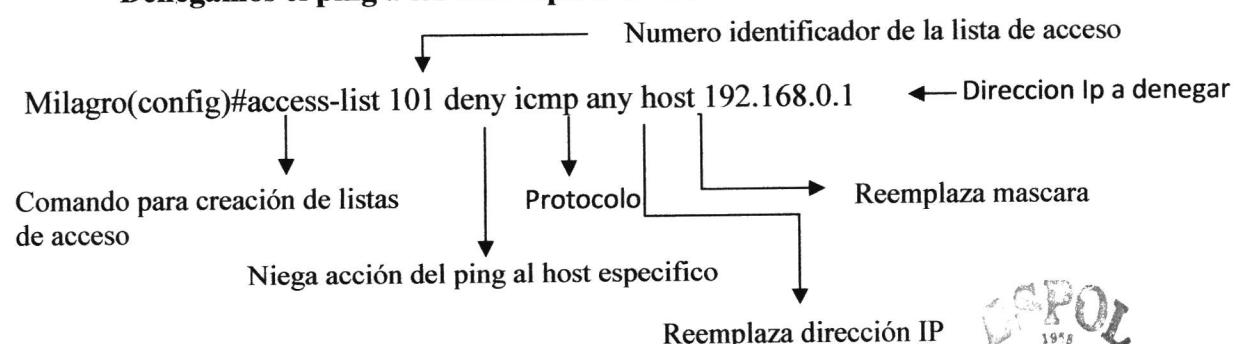
Permit|deny: Indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección especificada.

ICMP: Protocolo de mensajes de control de Internet) es un protocolo que permite administrar información relacionada con errores de los equipos en red

Dirección de origen: Identifica la dirección IP de origen.

Mascara comodín o wildcard: Identifica los bits del campo de la dirección que serán comprobados.

Denegamos el ping a los host especificados



```
Milagro(config)#access-list 101 deny icmp any host 192.168.0.1
Milagro(config)#access-list 101 deny icmp any host 192.168.0.5
Milagro(config)#access-list 101 deny icmp any host 192.168.0.9
Milagro(config)#access-list 101 deny icmp any host 192.168.0.13
Milagro(config)#access-list 101 deny icmp any host 192.168.0.17
Milagro(config)#access-list 101 deny icmp any host 192.168.0.21
Milagro(config)#access-list 101 deny icmp any host 200.200.200.0
Seteamos una linea en la que permita el ping a cualquier otro host
MILAGRO(config)#access-list 101 permit icmp any any
```

Router(config)#access-list[1-99][permit|deny][dirección de origen][mascara comodín]

1-99: Identifica el rango y la lista.

Permit-deny: Indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección especificada.

Dirección de origen: Identifica la dirección IP de origen.

Mascara comodín o wildcard: Identifica los bits del campo de la dirección que serán comprobados.

APLICANDO LAS ACLS A LA INTERFAZ

Ahora indicaremos el número de lista de acceso que será aplicada a esta interfaz

Para poder aplicar la lista de acceso debemos ubicarnos en la interfaz y subinterfaces, asignar el Access-group con su numero de acl correspondiente e indicarles si es que va de entrada o de salida de su interfaz, así tenemos:

```
MILAGRO(config)#interface fastEthernet 0/0
MILAGRO(config)#ip access-group 101 in
```

Número de lista de acceso: Indica el número de lista de acceso que será aplicada a esa interfaz.

In|out: Selecciona si la lista de acceso se aplicará como filtro de entrada o de salida

```
MILAGROconfig)#interface fastEthernet 0/0.1
MILAGRO(config)#ip access-group 101 in
MILAGR (config)#interface fastEthernet 0/0.2
MILAGR (config)#ip access-group 101 in
MILAGR (config)#interface fastEthernet 0/0.3
MILAGRO(config)#ip access-group 101 in
```



CAPÍTULO 5
GLOSARIO DE TÉRMINOS
TÉCNICOS



5 GLOSARIO DE TÉRMINOS TÉCNICOS

A

Access List.- |Permite establecer reglas para denegar y permitir paquetes entre routers

B

Broadcast .- Son mensajes que se envían a toda la red y como tal ocasionan congestionamiento en la misma.

BW.- Ancho de Banda de la interfaz en kilobits por segundo.

D

Database.- Ingresa en el modo base de datos de VLAN

Dimensiones.- una de las propiedades del espacio. El espacio, tal y como lo conocemos, es tridimensional. Para definir un volumen se necesitan tres medidas (dimensiones): longitud, anchura y altura.

F

Fibra Óptica.- fibra o varilla de vidrio u otro material transparente con un índice de refracción alto que se emplea para transmitir luz. Cuando la luz entra por uno de los extremos de la fibra, se transmite con muy pocas pérdidas incluso aunque la fibra esté curvada.

Firewall.- Mecanismo de seguridad utilizado para proteger una red interna de usuarios no deseados

Frecuencia.- término empleado en física para indicar el número de veces que se repite en un segundo cualquier fenómeno periódico.

Full duplex Back.- Transmite datos simultáneamente en ambas direcciones, emitiendo y recibiendo al mismo tiempo, se dice que operan en modo.

FTP.- Protocolo de transferencia de archivos que necesita internet para su funcionamiento

H

Half Duplex.- Sólo puede transmitir uno de ellos y el otro simplemente actúa de receptor, el modo de operación

Hardware is Lance.- Este campo describe el tipo de hardware que la interfaz está conectado.

Hostname nombre.- Modifica el nombre del router. Ej: hostname Lab_A

I

Interface fastethernet.- Entra al modo de configuración de interfaz de la ethernet

Interface serial.- Entra al modo de configuración de interfaz del serial

Interface tipo número.-Configura un tipo de interfaz y entra al modo de configuración de interfaz.

INTERNET.- Internet, interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente.

IOS.- Sistema operativo propio de los routers.

IP.- Protocolo usado en redes de comunicación.

Ip access-list.-Permite crear una ACL nombrada. Se debe indicar el tipo. Este comando ingresa al router al submodo de configuración que puede reconocerse por el prompt

Ip address.- Asigna una dirección IP y máscara de subred para las rutas.

Ip classless.-Permite que el router no tome en cuenta los límites con definición de clases de las redes en su tabla de enrutamiento y simplemente transmita hacia la ruta por defecto

Ip default-network dirección_red.-Establece una ruta por defecto. Ej: ip default-network 210.32.45.0

Ip route dirección_red máscara dir_ip_salto.-Establece rutas estáticas. Ej: ip route 210.42.3.0 255.255.255.0 211.1.2.1

ISP.-Proveedor De Servicio Internet.

L

LAN.- Local Area Network Las computadoras de una red de área local.

M

Mac.- Es una dirección Física asignada por el fabricante de la tarjeta de red .Se puede utilizar con fines administrativos para asignar políticas en la red.

Memoria Flash.- chip de memoria no volátil su contenido permanece aunque el aparato se desconecte de la corriente, que se puede reescribir. En cierto sentido se considera una variante de la EEPROM (Electrically Erasable Programmable Read-OnlyMemory, memoria de lectura solamente borrable y programable eléctricamente).

Memoria.- Los circuitos que permiten almacenar y recuperar la información. En un sentido más amplio, puede referirse también a sistemas externos de almacenamiento, como las unidades de disco o de cinta.

Metric.-Metrica que se utiliza en el OSPF.

NVRAM.- Parte interna de router, que almacena datos aun la conexión eléctrica haya fallado.



O

OSPF.- Es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos.

P

Ping.-Envía una petición de eco para diagnosticar la conectividad básica de red.

Procesador.- Unidad central de proceso, formado por uno o dos chips.

Proxy.- Un ordenador o computadora se dice que es de 64 bits si utiliza procesadores de 64-bit.

R

Redes.- Termino informatico utilizado para nombrar a conjunto de computadores interconectados entre si.

RIP.- Son las siglas de Routing Information Protocol. (Protocolo De Informacion De Enrutamiento)

Router protocolo de enrutamiento.-Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. Ej: router rip ó router igrp 120

Routers.- permite la comunicación entre diferentes segmentos de Red. El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados.

S

Servidor.- Computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos.

Software.- Programas de computadoras. Son las instrucciones responsables de que el hardware (la máquina) realice su tarea. Como concepto general, el software puede dividirse en varias categorías basadas en el tipo de trabajo realizado.

Switch .- El switch que usa es D-Link y pertenece a la capa 1 del modelo OSI cabe recalcar que no es administrable.

T

Telnet.- Nombre del Puerto servicio que permite acceder de manera remota a un dispositivo. Permite conectarse remotamente a un host

Topología.- Varias computadoras individuales conectadas entre sí forman una red de área local.

Transciver.-En términos informáticos convierte la luz a impulsos eléctricos.

Transmisión.- Transferencia de datos, en informática, transmisión de información de un lugar a otro, tanto dentro de un ordenador o computadora

Truning Port.- (PUERTO TRUNCADO) Permite Reducir el nivel de congestionamiento entre 2 Switch.

Trunk.- Especifica un puerto como punto extremo para un tronco VLAN
Undebug all .-Desactiva todas las depuraciones activadas en el dispositivo.

V

Velocidad.- Transferencia máxima se ajusta automáticamente en función de la cobertura y calidad de la transmisión.

Vlan.- Virtual local area network .Permite reducir los dominios de Broadcast.

W

Wildcard.-Máscara de longitud inversa.Es la máscara de subred que se utiliza con el protocolo de enrutamiento OSPF y aplicarlas en las ACL.

Wireless.-Red sin cable .Transmisión Only Direccional y Unidireccional.



BIBLIOTECA
CAMPUS
PENAS