

ESCUELA SUPERIOR POLITECNICA DEL LITORAL



Escuela de Diseño y Comunicación Visual

TÓPICO DE GRADUACIÓN

Previo a la obtención del título de
Analista de Soporte de Microcomputadoras

T e m a :

Manual de Administración y Seguridades
de Redes

E m p r e s a :

Instituto Nacional Galápagos

A u t o r e s :

Wladimir Serguey Valverde Rodríguez
Joseph Isaac Castro Guanga
Andy Karen García Loor
David Jonathan Caicedo Carrera

DIRECTOR :

Lsi. José Luis Ramírez

Año 2007



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

TÓPICO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ANALISTA DE SOPORTE DE MICROCOMPUTADORES

TEMA:

MANUAL DE ADMINISTRACION Y SEGURIDADES
DE REDES

EMPRESA:

INSTITUTO NACIONAL GALÁPAGOS

AUTORES:

WLADIMIR SERGUEY VALVERDE RODRIGUEZ

JOSEPH ISAAC CASTRO GUANGA

ANDY KAREN GARCÍA LOOR

DAVID JONATHAN CAICEDO CARRERA

DIRECTOR:

LSI. JOSÉ LUÍS RAMÍREZ

AÑO:

2007



DECLARACIÓN EXPRESA

La responsabilidad de los hechos, ideas y doctrinas expuestas en este tópico de graduación nos corresponden exclusivamente. Y el patrimonio intelectual de la misma a EDCOM (*Escuela de diseño y comunicación visual*) de la Escuela Superior Politécnica del Litoral.

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



DEDICATORIA

Queremos dedicar este manual primeramente a Dios a quien le debemos todo, también a nuestros padres por el sacrificio que han hecho por nosotros para poder culminar con éxito nuestros estudios, y a nuestras familias y amigos que nos ayudaron durante el tiempo que ha durado nuestra carrera.



AGRADECIMIENTOS

Agradecemos a todos los profesores los cuales han sido nuestra guía en este difícil camino al éxito, en nuestra formación profesional en especial al analista José Luís Ramírez por su ayuda incondicional en este tópico de graduación. A nuestros amigos entrañables de la universidad: Raúl Maldonado, Betto Quiroz y a todos aquellos que de alguna u otra manera nos han ayudado en este proyecto.



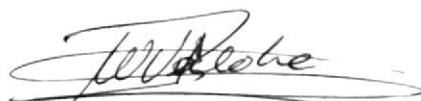
FIRMA DEL DIRECTOR DE TÓPICO



LSI. JOSÉ LUIS RAMÍREZ
DIRECTOR DE TÓPICO



FIRMA DE LOS AUTORES DE TÓPICO



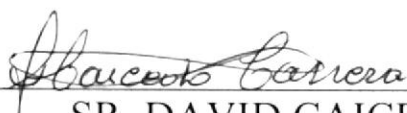
SR. WLADIMIR VALVERDE RODRÍGUEZ



SR. JOSEPH CASTRO GUANGA



SRA. ANDY GARCÍA LOOR



SR. DAVID CAICEDO CARRERA

INDICE DE CONTENIDO

CAPÍTULO 1 GENERALIDADES

1.1.	INTRODUCCIÓN	1
1.2.	OBJETIVO DE ESTE MANUAL	1
1.3.	A QUIEN VA DIRIGIDO ESTE MANUAL.....	1
1.4.	LO QUE SE DEBE CONOCER.....	1
1.5.	ORGANIZACIÓN DE ESTE MANUAL	2
1.6.	ACERCA DE ESTE MANUAL.....	2

CAPÍTULO 2 SITUACIÓN ACTUAL

2.1.	ANTECEDENTES DE LA EMPRESA	1
2.1.1.	MISIÓN	1
2.1.2.	VISIÓN	1
2.2.	INFRAESTRUCTURA LAN	2
2.2.1.	CARACTERÍSTICAS DE LAS ESTACIONES DE TRABAJO (GUAYAQUIL Y QUITO).....	2
2.2.1.1.	MATRIZ.	2
2.2.1.2.	SUCURSAL COORDINACIÓN GUAYAQUIL.....	3
2.2.1.3.	SUCURSAL COORDINACIÓN QUITO.	3
2.3.	CARACTERÍSTICAS DE LOS SERVIDORES (SAN CRISTOBAL).....	3
2.4.	MEDIOS DE COMUNICACIÓN	4
2.4.1.	ALÁMBRICOS	4
2.4.1.1.	MATRÍZ SAN CRISTOBAL.....	4
2.4.1.2.	SUCUSALES COORDINACIONES	4
2.4.2.	INALÁMBRICOS	4
2.5.	DISPOSITIVOS DE CONMUTACIÓN	4
2.5.1.	ENLACE PRINCIPAL	5
2.5.2.	DISPOSITIVOS DE ENRUTAMIENTO.....	5
2.5.3.	DESCRIPCIÓN DE EQUIPOS DE LA RED WAN	6
2.6.	RECEPCIÓN DE INTERNET EN EL EDIFICIO MATRÍZ.....	7
2.7.	PROBLEMAS ENCONTRADOS.....	8

CAPÍTULO 3 PROPUESTA

3.1.	PROBLEMAS ENCONTRADOS.....	1
3.2.	SOLUCIÓN PROPUESTA	2
3.3.	ESTUDIO DE FACTIBILIDAD	2
3.3.1.	FACTIBILIDAD TÉCNICA	2
3.3.2.	ENLACES.....	3

CAPÍTULO 4 IMPLEMENTACIÓN

4.1.	ANÁLISIS DE PISOS APLICATIVOS.....	1
4.1.1.	MATRIZ SAN CRISTÓBAL	1
4.1.2.	SUCURSAL COORDINACION QUITO	2
4.1.3.	SUCURSAL COORDINACIÓN GUAYAQUIL.....	3

4.2.	ENLACE DE DATOS	4
4.2.1.	MATRÍZ – QUITO.....	4
4.2.2.	MATRÍZ – GUAYAQUIL	5
4.2.3.	GUAYAQUIL-QUITO.....	6
4.3.	COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS MATRÍZ Y SUCURSALES	7

CAPÍTULO 5 ROUTERS Y SWITCHES

5.1.	INTRODUCCIÓN A LOS ROUTERS	1
5.2.	VENTAJAS DE LOS ROUTERS	1
5.3.	DESVENTAJAS DE LOS ROUTERS.....	1
5.4.	MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER.....	2
5.4.1.	CABLE DCE (DATA CIRCUIT EQUIPMENT).....	2
5.4.2.	CABLE DTE (DATA TERMINAL EQUIPMENT)	2
5.4.3.	CABLE UTP (CAT 5E)	3
5.4.4.	CONECTOR RJ45	3
5.4.5.	PUERTO SERIAL (CONECTOR COM).....	4
5.5.	PARTES INTERNAS DE UN ROUTER.....	4
5.6.	PARTES EXTERNAS DEL ROUTER	6
5.6.1.	INTERFACES	6
5.7.	REDUNDANCIA EN LOS ROUTERS	7
5.8.	REDUNDANCIA EN LA CONFIGURACIÓN DE ROUTERS	8
5.8.1.	HSRP.....	8
5.8.1.1.	CARACTERÍSTICAS	9
5.8.1.2.	IMPLEMENTACIÓN.....	9
5.8.1.3.	ELECCIÓN DEL ROUTER "ACTIVO"	9
5.8.1.4.	PASO DE ESTADO "STANDBY" A ESTADO "ACTIVO".....	9
5.8.1.5.	CONFIGURACIÓN	10
5.9.	ENRUTAMIENTO.....	10
5.9.1.	ENRUTAMIENTO ESTÁTICO	10
5.10.	ENRUTAMIENTO DINÁMICO	11
5.10.1.	PROTOCOLOS DE ENRUTAMIENTO	11
5.11.	TIPOS DE PROTOCOLOS.....	11
5.11.1.	EL PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP)	11
5.12.	FUNCIONAMIENTO RIP	12
5.12.1.	VENTAJAS Y DESVENTAJAS.....	13
5.12.2.	MENSAJES RIP	13
5.12.2.1.	PETICIÓN	13
5.12.2.2.	RESPUESTA	13
5.12.2.3.	FORMATO DE LOS MENSAJES RIP.....	13
5.13.	EL PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY (IGRP)	14
5.13.1.	EL PROTOCOLO EIGRP	14
5.13.2.	TABLA DE VECINOS.....	15
5.13.3.	TABLA DE TOPOLOGÍA	15
5.13.4.	TABLA DE ENCAMINAMIENTO.....	16
5.14.	EL PROTOCOLO CONOCIDO COMO "PRIMERO LA RUTA MÁS CORTA" (OSPF)	16
5.14.1.	ESTADOS DE OSPF	17

5.14.2.	ESTADO DESACTIVADO (DOWN STATE).....	17
5.14.3.	ESTADO DE INICIALIZACIÓN (INIT STATE)	18
5.14.4.	ESTADO DE DOS-VÍAS (TWO-WAY)	18
5.14.5.	ESTADO EXSTART.....	18
5.14.6.	ESTADO DE INTERCAMBIO (EXCHANGE)	18
5.14.7.	ESTADO CARGANDO (LOADING)	19
5.14.8.	ESTADO DE ADYACENCIA (ADJACENCY).....	19
5.15.	LISTAS DE CONTROL DE ACCESO (ACL'S)	19
5.15.1.	FUNCIONAMIENTO DE LAS ACL	20
5.15.2.	CREACIÓN DE LAS ACL	20
5.15.3.	FUNCIÓN DE LA MÁSCARA WILDCARD EN UNA ACL.....	21
5.15.4.	ROUTER (CONFIG) #ACCESS-LIST 1 PERMIT 0.0.0.0 255. 255. 255. 255	22
5.15.5.	TIPOS DE ACL	22
5.15.5.1.	ACL ESTÁNDAR	22
5.15.5.2.	ACL EXTENDIDA.....	22
5.15.6.	UBICACIÓN DE UNA ACL	23
5.15.7.	PORQUE CREAR UNA ACL.....	23
5.16.	CONEXIONES DE LOS ROUTERS	24
5.17.	ACCESO A LA APLICACIÓN HYPERTERMINAL.....	25
5.18.	CONFIGURACIÓN DE ROUTERS	29
5.18.1.	COMANDOS BÁSICOS DE ROUTER	33
5.18.2.	GUARDAR CAMBIOS DEL ROUTER.....	34
5.18.3.	CONFIGURAR NOMBRE DE ROUTERS	34
5.18.4.	CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER.....	35
5.18.5.	ASIGNACIÓN DE IP'S A LAS INTERFACES.....	36
5.18.6.	DECLARAR EL PROTOCOLO DE ENRUTAMIENTO (RIP)	36
5.18.7.	PROTOCOLO DE ENRUTAMIENTO (OSPF)	37
5.19.	REDISTRIBUCIÓN DE RUTAS	37
5.19.1.	CASO DE ESTUDIO DEL INSTITUTO NACIONAL GALÁPAGOS.....	39
5.20.	CONFIGURACIÓN DETALLADAS DE ROUTERS	40
5.21.	CONFIGURACIÓN DE ROUTER MATRÍZ SAN CRISTÓBAL.....	40
5.21.1.	GUARDAR CONFIGURACIÓN.....	43
5.22.	CONFIGURACIÓN DE ROUTER GUAYAQUIL	48
5.22.1.	GUARDAR CONFIGURACIÓN.....	49
5.23.	CONFIGURACIÓN DE ROUTER QUITO.....	52
5.23.1.	GUARDAR CONFIGURACIÓN.....	54
5.24.	INTRODUCCIÓN A LOS SWITCHES	57
5.24.1.	ENCAPSULAMIENTO	57
5.24.2.	SEGMENTACIÓN	58
5.24.3.	COLISIÓN	59
5.25.	CONFIGURACIÓN DE SWITCHES	60
5.25.1.	MODOS DE INTERFAZ USUARIO.....	61
5.26.	CONFIGURACIÓN DE CONTRASEÑAS	61
5.27.	ASPECTOS BÁSICOS DE LAS VLAN.....	62
5.28.	CONFIGURACIÓN DE VLAN POR DEFECTO	63
5.28.1.	CREACIÓN DE VLAN'S.....	63
5.28.2.	BORRADO DE VLAN'S	64
5.28.3.	ASIGNACIÓN DE VLAN'S A LOS PUERTOS	65
5.28.4.	ENRUTAMIENTO ENTRE VLAN.....	65

5.28.5.	INTERFACES FÍSICAS Y LÓGICAS	66
5.28.6.	ASIGNAR SWITCH DE TIPO SERVER.....	67
5.28.7.	CONFIGURACIÓN DE UN ENRUTAMIENTO ENTRE DISTINTAS VLAN	68
5.29.	PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE SWITCH (INSTITUTO NACIONAL GALÁPAGOS).....	70
5.29.1.	ACCESO A LA APLICACIÓN HYPERTERMINAL.....	70
5.29.2.	CONFIGURACIÓN DEL SWITCH MATRÍZ PRINCIPAL	73
5.29.3.	CONFIGURACIÓN DEL SWITCH GUAYAQUIL	83
5.29.4.	CONFIGURACIÓN DEL SWITCH QUITO	88
5.30.	TABLAS DE LOS SEGMENTOS DE LAS REDES DEL INSTITUTO NACIONAL GALAPAGOS	92
5.30.1.	MATRÍZ SAN CRISTÓBAL	92
5.30.2.	GUAYAQUIL.....	93
5.30.3.	QUITO	93

CAPÍTULO 6 SEGURIDADES

6.1.	INTRODUCCIÓN	1
6.1.1.	DEFINICIONES	1
6.1.2.	SEGURIDAD GLOBAL	2
6.1.3.	IMPLEMENTACIÓN.....	2
6.2.	POLÍTICAS GENERALES DE SEGURIDAD.....	3
6.2.1.	¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI)? ...	3
6.3.	ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA ...	3
6.3.1.	ALGUNOS PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD.....	4
6.3.2.	PROPOSICIÓN DE UNA FORMA DE REALIZAR EL ANÁLISIS PARA LLEVAR A CABO UN SISTEMA DE SEGURIDAD INFORMÁTICA.....	4
6.3.3.	¿POR QUÉ LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA GENERALMENTE NO CONSIGUEN IMPLANTARSE?	5
6.4.	NIVELES DE TRABAJO.....	6
6.4.1.	CONFIDENCIALIDAD	6
6.4.2.	INTEGRIDAD.....	6
6.4.3.	AUTENTICIDAD.....	6
6.4.4.	NO REPUDIO.....	7
6.4.5.	DISPONIBILIDAD DE LOS RECURSOS Y DE LA INFORMACIÓN	7
6.4.6.	CONSISTENCIA.....	7
6.4.7.	CONTROL DE ACCESO A LOS RECURSOS	7
6.4.8.	AUDITORÍA	7
6.4.9.	ALGORITMO.....	7
6.5.	ACERCA DE LOS PROCEDIMIENTOS.....	9
6.5.1.	PROCEDIMIENTO DE ALTA DE CUENTA DE USUARIO	9
6.5.2.	PROCEDIMIENTO DE BAJA DE CUENTA DE USUARIO	10
6.5.3.	PROCEDIMIENTO PARA DETERMINAR LAS BUENAS PASSWORDS	10
6.5.4.	PROCEDIMIENTOS DE VERIFICACIÓN DE ACCESOS.....	11
6.5.5.	PROCEDIMIENTO PARA EL CHEQUEO DEL TRÁFICO DE LA RED..	11
6.5.6.	PROCEDIMIENTO PARA EL MONITOREO DE LOS VOLUMENES DE CORREO	11

6.5.7.	PROCEDIMIENTOS PARA EL MONITOREO DE CONEXIONES ACTIVAS	11
6.5.8.	PROCEDIMIENTO DE MODIFICACIÓN DE ARCHIVOS	12
6.5.9.	PROCEDIMIENTOS PARA EL RESGUARDO DE COPIAS DE SEGURIDAD.....	12
6.5.10.	PROCEDIMIENTOS PARA LA VERIFICACIÓN DE LAS MÁQUINAS DE LOS USUARIOS.....	12
6.5.11.	PROCEDIMIENTOS PARA EL MONITOREO DE LOS PUERTOS EN LA RED	12
6.5.12.	PROCEDIMIENTOS DE CÓMO DAR A PUBLICIDAD LAS NUEVAS NORMAS DE SEGURIDAD	12
6.5.13.	PROCEDIMIENTOS PARA LA DETERMINACIÓN DE IDENTIFICACIÓN DE USUARIO Y GRUPO DE PERTENENCIA POR DEFECTO ..	13
6.5.14.	PROCEDIMIENTOS PARA RECUPERAR INFORMACIÓN	13
6.5.15.	CHECK-LISTS	13
6.6.	TIPOS DE ATAQUES Y VULNERABILIDADES	14
6.6.1.	NEGACIÓN DE SERVICIO (<i>DENIAL OF SERVICE</i>)	14
6.6.2.	¿QUÉ ES “DENIAL OF SERVICE”? DESCRIPCIÓN DE ATAQUES.....	14
6.6.3.	MODOS DE ATAQUE	15
6.6.4.	CONSUMO DE RECURSOS ESCASOS, LIMITADOS, O NO RENOVABLES	15
6.6.4.1.	CONECTIVIDAD	15
6.6.4.2.	APROVECHAMIENTO DE LOS RECURSOS DEL OTRO	15
6.6.4.3.	CONSUMO DE ANCHO DE BANDA	16
6.6.4.4.	CONSUMO DE OTROS RECURSOS	16
6.6.5.	DESTRUCCIÓN O ALTERACIÓN DE LA INFORMACIÓN DE CONFIGURACIÓN	17
6.6.6.	DESTRUCCIÓN O ALTERACIÓN FÍSICA DE LOS COMPONENTES DE LA RED	17
6.6.7.	PREVENCIÓN Y RESPUESTA.....	17
6.7.	CRACKING DE PASSWORDS	18
6.7.1.1.	DESCUBRIR UNA PASSWORD.....	18
6.7.2.	E-MAIL BOMBING Y SPAMMING	19
6.7.2.1.	DESCRIPCIÓN	19
6.7.2.2.	DETALLES TÉCNICOS.....	19
6.7.2.3.	¿CÓMO PROCEDER?	20
6.8.	PROBLEMAS DE SEGURIDAD EN EL FTP	21
6.8.1.	EL COMANDO PORT.....	21
6.8.2.	EL PROTOCOLO FTP.....	21
6.8.3.	EL ATAQUE “FTP BOUNCE”	21
6.8.3.1.	“SCANNING” DE PORTS.....	21
6.8.3.2.	“BYPASS” DE DISPOSITIVOS BÁSICOS DE FILTRADO DE PAQUETES.....	22
6.8.3.3.	BYPASS DE DISPOSITIVOS DE FILTRADO DINÁMICOS	22
6.9.	SOLUCIONES.....	22
6.9.1.	SOFTWARE DEL FTP SERVER.....	22
6.9.2.	CONFIGURACIÓN DEL FTP SERVER	23
6.9.3.	CONFIGURACIÓN DE RED.....	23

6.10.	TELNET.....	24
6.11.	SEGURIDAD EN NETBIOS	24
6.11.1.1.	PEQUEÑA RED LAN SIN ACCESO A INTERNET Y SIN INTRA O EXTRANET.....	24
6.11.1.2.	REDES LAN CON INTERNET, INTRANET O EXTRANET.....	25
6.11.1.3.	REDES WAN	25
6.11.1.4.	¿QUÉ HACER?	25
6.12.	DESCRIPCIÓN DE ALGUNAS HERRAMIENTAS DE CONTROL Y SEGUIMIENTO DE ACCESOS	25
6.12.1.	HERRAMIENTAS PARA WINDOWS NT	26
6.12.1.1.	MONITOR DE EVENTOS	26
6.12.1.2.	MONITOR DE RED.....	26
6.12.1.3.	MONITOR DE PERFORMANCE	26
6.12.1.4.	ERRORES DE PERMISOS DE ACCESOS	26
6.12.1.5.	ERRORES DE LOGON	26
6.13.	PAQUETES PARA WINDOWS.....	26
6.13.1.	WINDOWS NT RESOURCE KIT.....	26
6.13.1.1.	C2CONFIG.....	27
6.13.1.2.	DUMPEL	27
6.13.1.3.	PASSPROP	27
6.13.1.4.	INTERNET SCANNER	27
6.13.1.5.	SCANNT.....	27
6.13.1.6.	NETXRAY.....	27
6.13.1.7.	SUCK SERVER.....	27
6.13.1.8.	RED BUTTON	28
6.14.	SÍNTESIS.....	28

CAPÍTULO 7 NORMATIVAS DE CABLEADO

7.1	NORMATIVAS DE CABLEADO ESTRUCTURADO.....	1
7.1.1	NORMATIVA 1	1
7.1.2	NORMATIVA 2.....	1
7.1.3	NORMATIVA 3.....	2
7.1.4	NORMATIVA 4.....	2
7.1.5	NORMATIVA 5.....	3
7.1.6	NORMATIVA 6.....	3
7.1.7	NORMATIVA 7.....	4
7.1.8	NORMATIVA 8.....	4
7.1.9	NORMATIVA 9.....	5
7.1.10	NORMATIVA 10.....	5
7.1.11	NORMATIVA 11.....	6
7.1.12	NORMATIVA 12.....	6
7.1.13	NORMATIVA 13.....	7
7.1.14	NORMATIVA 14.....	7
7.1.15	NORMATIVA 15.....	8
7.1.16	NORMATIVA 16.....	8
7.1.17	NORMATIVA 17.....	9
7.1.18	NORMATIVA 18.....	9
7.1.19	NORMATIVA 19.....	10

7.1.20	NORMATIVA 20.....	10
7.1.21	NORMATIVA 21.....	11
7.1.22	NORMATIVA 22.....	11
7.1.23	NORMATIVA 23.....	12
7.1.24	NORMATIVA 24.....	12
7.1.25	NORMATIVA 25.....	13
7.1.26	NORMATIVA 26.....	13
7.1.27	NORMATIVA 27.....	14
7.1.28	NORMATIVA 28.....	14
7.1.29	NORMATIVA 29.....	15
7.1.30	NORMATIVA 30.....	15
7.1.31	NORMATIVA 31.....	16
7.1.32	NORMATIVA 32.....	16
7.1.33	NORMATIVA 33.....	17
7.1.34	NORMATIVA 34.....	17
7.1.35	NORMATIVA 35.....	18
7.1.36	NORMATIVA 36.....	18
7.1.37	NORMATIVA 37.....	19
7.1.38	NORMATIVA 38.....	19
7.1.39	NORMATIVA 39.....	20
7.1.40	NORMATIVA 40.....	20
7.1.41	NORMATIVA 41.....	21
7.1.42	NORMATIVA 42.....	21
7.1.43	NORMATIVA 43.....	22
7.1.44	NORMATIVA 44.....	22
7.1.45	NORMATIVA 45.....	23
7.1.46	NORMATIVA 46.....	23
7.1.47	NORMATIVA 47.....	24
7.1.48	NORMATIVA 48.....	24
7.1.49	NORMATIVA 49.....	25
7.1.50	NORMATIVA 50.....	25
7.1.51	NORMATIVA 51.....	26
7.1.52	NORMATIVA 52.....	26
7.1.53	NORMATIVA 53.....	27
7.1.54	NORMATIVA 54.....	27
7.1.55	NORMATIVA 55.....	28
7.1.56	NORMATIVA 56.....	28
7.1.57	RECOMENDACIÓN 1.....	29
7.1.58	RECOMENDACIÓN 2.....	29
7.1.59	RECOMENDACIÓN 3.....	30
7.1.60	RECOMENDACIÓN 4.....	30
7.1.61	RECOMENDACIÓN 5.....	31
7.1.62	RECOMENDACIÓN 6.....	31
7.1.63	RECOMENDACIÓN 7.....	32
7.1.64	RECOMENDACIÓN 8.....	32
7.1.65	RECOMENDACIÓN 9.....	33
7.1.66	RECOMENDACIÓN 10.....	33
7.1.67	RECOMENDACIÓN 11.....	34

INDICE DE TABLAS

CAPÍTULO 1

Tabla 1.1 Generalidades	2
-------------------------------	---

CAPÍTULO 2

Tabla 2-1 Distribución de Pcs en Matriz	2
Tabla 2-2 Distribución de Pcs en Coordinación Guayaquil	3
Tabla 2-3 Distribución de Pcs en coordinación Guayaquil	3
Tabla 2-4 Características Servidor Base de datos	3
Tabla 2-5 Características Servidor Base de datos	3
Tabla 2-6 Dispositivos de Conmutación	4
Tabla 2-7 Dispositivos de Enrutamiento	5
Tabla 2-8 Dispositivos de Enrutamiento	6
Tabla 2-9 Problemas Encontrados	8

CAPÍTULO 3

Tabla 3.1 Problemas Encontrados	1
Tabla 3.2 Solución Propuesta	2
Tabla 3.3 Factibilidad Técnica	3
Tabla 3.4 Enlaces	3

CAPÍTULO 5

Tabla 5-1: Clases De Acl's	21
Tabla 5-2 Comandos Básicos De Router	34
Tabla 5-3 Matriz	92
Tabla 5-4 Matriz Direcciones	92
Tabla 5-5 Matriz Direcciones Lan	93
Tabla 5-6 Guayaquil	93
Tabla 5-7 Guayaquil Direcciones	93
Tabla 5-8 Guayaquil Direcciones Lan	93
Tabla 5-9 Quito	93
Tabla 5-10 Quito Direcciones	94
Tabla 5-11 Quito Direcciones Lan	94

CAPÍTULO 7

Tabla 7-1 Longitud y Tipos de Fibra Óptica	12
Tabla 7-2 Cables con identificador	28
Tabla 7-3 Uso de Hilos de fibra Óptica	33

INDICE DE FIGURAS

CAPÍTULO 2

Figura 2-1 Enlace Principal.....	5
Figura 2-2 Recepción de Internet.....	6
Figura 2-3 Recepción de Internet.....	7

CAPÍTULO 4

Figura 4-1 Implementación Coordinación San Cristóbal	1
Figura 4-2 Implementación coordinación Quito	2
Figura 4-3 Implementación Coordinación Guayaquil	3
Figura 4-5 Enlace Matriz –Guayaquil.....	5
Figura 4-6 Enlace Guayaquil-Quito	6
Figura 4-7 Gráfico Comunicación Wan Ingala.....	7

CAPÍTULO 5

Figura 5-1 Cable DCE	2
Figura 5-2 Cable DTE	2
Figura 5-3 Cable UTP	3
Figura 5-4 Conector RJ45	3
Figura 5-5 Puerto Serial	4
Figura 5-6 Interfaces Del Router	6
Figura 5-7 Interfaces Del Router	8
Figura 5-8 Esquema De Comunicación.....	11
Figura 5-9 RIP	12
Figura 5-10: IGRP.....	14
Figura 5-12: ACL'S	20
Figura 5-14 Conexiones De Los Routers	24
Figura 5-15 Conexiones De Los Routers	24
Figura 5-16 Entorno de Windows.....	25
Figura 5-17 Menú inicio	25
Figura 5-18 Selección de programa (hiperterminal)	26
Figura 5-19 Nueva conexión	26
Figura 5-20 Conectar a.....	27
Figura 5-21 Conexión cancelada al router.....	27
Figura 5-22 Propiedades de com 1	28
Figura 5-23 Configuración Router.....	28
Figura 5-24 Configuración Router.....	29
Figura 5-25 Configuración global.....	29
Figura 5-26 Configuración Ethernet	30
Figura 5-27 Configuración RAM del router.....	30
Figura 5-28 Configuración show running-config	31
Figura 5-29 Configuración comando show ip route	31
Figura 5-30 Configuración comando show interfaces	32
Figura 5-31 Configuración comando ip address.....	32
Figura 5-32 Caso De Estudio INGALA	39

Figura 5-33 Switch.....	57
Figura 5-34 Interfaz De Usuario	61
Figura 5-35 Configuración de contraseñas	62
Figura 5-36 Aspectos De Vlans	62
Figura 5-37 Vlan Por Defecto	63
Figura 5-38 Asignación De Nombre A VLAN	64
Figura 5-39 Borrado De VLAN	65
Figura 5-41 Enrutamiento Entre Vlan.....	66
Figura 5-42 Enrutamiento Entre Vlan 2.....	66
Figura 5-43 Interfaces Físicas Y lógicas.....	67
Figura 5-44 Determinación De Switch	68
Figura 5-45 Enrutamiento Entre Vlans	68
Figura 5-46 Modo Configuración Global	69
Figura 5-47 Entorno de Windows.....	70
Figura 5-48 Menú inicio	70
Figura 5-49 Selección de programa (hiperterminal).....	71
Figura 5-50 Nueva conexión.....	71
Figura 5-51 Conectar a.....	72
Figura 5-52 Propiedades de com 1	72
Figura 5-53 Conexión al switch 1	73

CAPÍTULO 6

Figura 6-1 Interrupción	8
Figura 6-2 Intercepción	9
Figura 6-3 Modificación.....	9
Figura 6-4 Tiempos De Búsquedas.....	19
Figura 6-5 Cuadro de síntesis 1	28
Figura 6-6 Cuadro de síntesis 2	28

CAPÍTULO 7

Figura 7-1 Normativa 1	1
Figura 7-2 Normativa 2	1
Figura 7-3 Normativa 3	2
Figura 7-4 Normativa 4	2
Figura 7-5 Normativa 5	3
Figura 7-6 Normativa 6	3
Figura 7-7 Normativa 7	4
Figura 7-8 Normativa 8	4
Figura 7-9 Normativa 9	5
Figura 7-10 Normativa 10	5
Figura 7-11 Normativa 11	6
Figura 7-12 Normativa 12	6
Figura 7-13 Normativa 13	7
Figura 7-14 Normativa 14	7
Figura 7-15 Normativa 15	8
Figura 7-16 Normativa 16	8
Figura 7-17 Normativa 17	9

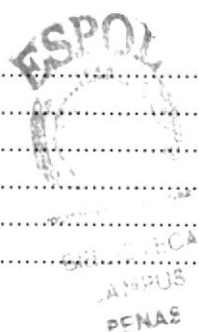


Figura 7-18 Normativa 18	9
Figura 7-19 Normativa 19	10
Figura 7-20 Normativa 20	10
Figura 7-21 Normativa 21	11
Figura 7-22 Normativa 22	11
Figura 7-23 Normativa 23	12
Figura 7-24 Normativa 24	12
Figura 7-25 Normativa 25	13
Figura 7-26 Normativa 26	13
Figura 7-27 Normativa 27	14
Figura 7-28 Normativa 28	14
Figura 7-29 Normativa 29	15
Figura 7-30 Normativa 30	15
Figura 7-31 Normativa 31	16
Figura 7-32 Normativa 32	16
Figura 7-33 Normativa 33	17
Figura 7-34 Normativa 34	17
Figura 7-35 Normativa 35	18
Figura 7-36 Normativa 36	18
Figura 7-37 Normativa 37	19
Figura 7-38 Normativa 38	19
Figura 7-39 Normativa 39	20
Figura 7-40 Normativa 40	20
Figura 7-41 Normativa 41	21
Figura 7-42 Normativa 42	21
Figura 7-43 Normativa 43	22
Figura 7-44 Normativa 44	22
Figura 7-45 Normativa 45	23
Figura 7-46 Normativa 46	23
Figura 7-47 Normativa 47	24
Figura 7-48 Normativa 48	24
Figura 7-49 Normativa 49	25
Figura 7-50 Normativa 50	25
Figura 7-51 Normativa 51	26
Figura 7-52 Normativa 52	26
Figura 7-53 Normativa 53	27
Figura 7-54 Normativa 54	27
Figura 7-55 Normativa 55	28
Figura 7-56 Normativa 56	28
Figura 7-57 Recomendación 1	29
Figura 7-58 Recomendación 2	29
Figura 7-59 Recomendación 3	30
Figura 7-60 Recomendación 4	30
Figura 7-61 Recomendación 5	31
Figura 7-62 Recomendación 6	31
Figura 7-63 Recomendación 7	32
Figura 7-64 Recomendación 8	32
Figura 7-65 Recomendación 9	33
Figura 7-66 Recomendación 10	33





CAPÍTULO 1

GENERALIDADES

1.1. INTRODUCCIÓN

Este manual fue elaborado con la finalidad de servir como guía de consulta para el usuario a nivel de redes. Ya que contiene información clara y concisa de cómo manejar una red Lan y Wan.

El cual permitirá configurar un router desde los comandos más básicos hasta la comunicación de los mismos con diferentes protocolos, todo esto lo podrán realizar un técnico de redes, un administrador de redes hasta un jefe de networking.

1.2. OBJETIVO DE ESTE MANUAL

El objetivo de este manual es guiar a todos aquellos usuarios interesados en el área de redes como al personal encargado en la administración de las mismas, en aspecto tanto de seguridades como configuración de equipos con la finalidad de despejar cualquier tipo de inquietud relacionado a este tema lo cual se basa en dos puntos básicos.

- Como configurar routers y switches.
- Establecer un servidor.

1.3. A QUIEN VA DIRIGIDO ESTE MANUAL

Va orientado a los usuarios finales con conocimientos en redes involucrados en la etapa de implementación de la red tanto a nivel LAN como WAN.

Administrador de redes.- Es la persona encargada de asistir a las redes y llevar la correcta organización de la red.

1.4. LO QUE SE DEBE CONOCER

Las personas que operan las redes, tanto a nivel LAN o WAN tienen que tener los siguientes conocimientos mínimos.

- a. Conocimientos básicos en diseño de redes
- b. Conocimientos básicos en ruteadores y switches
- c. Conocimientos en sistemas operativos tanto en cliente como en servidor

1.5. ORGANIZACIÓN DE ESTE MANUAL

Este manual está organizado en siete partes principales:

Generalidades	
Capítulo 1	Generalidades Explica brevemente el contenido de este manual.
Capítulo 2	Situación Actual Se especifica el estado de la empresa en el aspecto de redes, los dispositivos que cuenta en la actualidad así como el resultado de los mismos con sus problemas.
Capítulo 3	Solución Propuesta Aquí se le ha dado dos soluciones enfocados en los problemas que se ha encontrado detallando los requerimientos en factibilidades técnicas, operativas y económicas.
Capítulo 4	Análisis de piso e implementación WAN A través de gráficos se demuestra como serán los enlaces WAN entre las sucursales y matriz con los dispositivos.
Capítulo 5	Configuraciones de routers y switch En este Capítulo se habla de los aspectos básicos con los cuales cuenta un router y switch como también la manera de configurar los equipos mencionados anteriormente.
Capítulo 6	Seguridades Este capítulo trata sobre las implicaciones a considerar en las seguridades de la red la cual abarca los aspectos físicos y lógicos
Capítulo 7	Normativas En este Capítulo se habla de las normas aplicables a la implementación de un cableado estructurado

Tabla 1.1 Generalidades

1.6. ACERCA DE ESTE MANUAL

Este manual contiene diversas ilustraciones e instrucciones que debe seguir un administrador de redes para poder configurar equipos de enrutamiento y conmutación así como un servidor con sus respectivos servicios.



CAPÍTULO 2

SITUACIÓN ACTUAL

2.1. ANTECEDENTES DE LA EMPRESA

El **Instituto Nacional Galápagos, INGALA**, se crea mediante decreto de la Cámara Nacional de Representante el 7 de febrero de 1980, publicado en el Registro Oficial No. 131 del 21 de febrero de 1980 en la presidencia del Dr. Jaime Roldós Aguilera.

El 18 de marzo de 1998, con la aprobación de la Ley Orgánica de Régimen Especial para la Conservación y el Desarrollo Sustentable de la provincia de Galápagos y la Reforma Constitucional en este mismo año (Art. 239), se establece una reorientación al rol institucional del INGALA, siendo mandatario y obligatorio la gestión de la Planificación regional, el seguimiento y control de la inversión en Galápagos, y la implementación de las políticas de crecimiento poblacional, entre otras funciones. Uno de los aspectos que no fueron considerados en la formulación de la ley, es el hecho de habersele asignado funciones de trascendental importancia (**Planificación Regional y Control de Residencia**), sin los recursos financieros ni económicos, para el cumplimiento de las que determinan esta elevada responsabilidad.

La promulgación de la Ley Orgánica de Régimen Especial para la Conservación y el Desarrollo Sustentable para la provincia de Galápagos, produce una reorientación del rol institucional, generando el progreso de reestructuración.

Con patrimonio propio, autonomía administrativa y financiera, con sede en PUERTO BAQUERIZO MORENO, cantón SAN CRISTOBAL, Provincia de Galápagos; adscrita a la Presidencia de la Republica con jurisdicción en Galápagos, y Coordinaciones en QUITO Y GUAYAQUIL en el Ecuador continental.

2.1.1. MISIÓN

Organismo de la Presidencia de la Republica, rector de la Planificación Regional que establece políticas, coordina y gestiona acciones con los diferentes actores sociales, económicos, culturales y ambientales a nivel local, nacional e internacional, para el Desarrollo Humano Sostenible y la Conservación de los Sistemas Ecológicos de Galápagos.

2.1.2. VISIÓN

El INGALA será la institución modelo de Planificación y Gestión Ambiental, de reconocido prestigio, con solvencia Técnica, calida y credibilidad en sus productos y servicios, para asegurar el Desarrollo Humano y Sostenible y la Conservación de los Sistemas Ecológicos de la provincia de Galápagos.

“El Objetivo Central del Manejo de las Islas Galápagos es lograr la conservación de los ecosistemas y desarrollo sustentable de su población.

Para alcanzarlo es necesario la acción comprometida de todos quienes habitan o nos relacionamos con ellas”.

2.2. INFRAESTRUCTURA LAN

La Institución posee un cableado no estructurado que no cumple con las normas para las redes LAN.

2.2.1. CARACTERISTICAS DE LAS ESTACIONES DE TRABAJO (GUAYAQUIL Y QUITO)

- PC de escritorio HP Compaq Pentium 4 - 2,8 Ghz
Memoria Ram de 256 Mb.
Disco duro de 40 Gigas
CD-Write incorporado
Mouse y teclado HP
Monitor HP 5500 15"
UPS TRIPP-LITE de 305 watts
- PC de escritorio Compaq Pentium 4 – 2,8 Ghz
Memoria Ram de 256 Mb.
Disco duro de 80 Gigas
CD-write incorporado Samgsung
Mouse y teclado
Monitor Compaq de 15"
UPS UNITEK de 350 watts
- Computadora portátil Toshiba de 1,3 Ghz
Memoria Ram de 128 Mb.
Disco duro de 10 Gigas
Mouse extratech



2.2.1.1. MATRIZ.

El Ingala San Cristóbal cuenta con 20 equipos incluyendo los servidores repartidos de la siguiente manera:

CANTIDAD PC	UBICACIÓN
2	Gerencia
2	Dirección Jurídica
3	Dirección Administrativa
3	Dirección Financiera
1	R.R.H.H.
2	Control De Residencia
1	Servicio De Investigaciones
2	Archivo Central
1	Contabilidad
2	Comunicación Social
1	Planificación

Tabla 2-1 Distribución de Pcs en Matriz

2.2.1.2. SUCURSAL COORDINACIÓN GUAYAQUIL

Posee 2 máquinas distribuidas de la siguiente forma:

CANTIDAD PC	UBICACIÓN
1	Contabilidad
1	Administración

Tabla 2-2 Distribución de Pcs en Coordinación Guayaquil

2.2.1.3. SUCURSAL COORDINACIÓN QUITO.

Posee 1 máquina distribuida de la siguiente forma:

CANTIDAD PC	UBICACIÓN
1	Administración

Tabla 2-3 Distribución de Pcs en coordinación Guayaquil

2.3. CARACTERÍSTICAS DE LOS SERVIDORES (SAN CRISTOBAL)

El edificio matriz posee 2 servidores los cuales brindan los servicios de Base de datos de los residentes.

MARCA/MODELO	IBM
PROCESADOR	INTEL 2.0 Ghz
SISTEMA OPERATIVO	WINDOWS 2000 SERVER
FUNCIÓN	BASES DE DATOS
DISCOS DUROS	2 DE 30 GB
MEMORIA	256MB DDR1
TARJETA DE RED	ETHERNET 10/100 Mbps
UBICACIÓN	ARCHIVO CENTRAL

Tabla 2-4 Características Servidor Base de datos

MARCA/MODELO	IBM / MPN 33P2931
PROCESADOR	INTEL 2.0 Ghz
SISTEMA OPERATIVO	WINDOWS 2000 SERVER
FUNCIÓN	BASES DE DATOS
DISCOS DUROS	2 DE 40 GB SCI
MEMORIA	256MB DDR1
TARJETA DE RED	ETHERNET 10/100 Mbps
UBICACIÓN	ARCHIVO CENTRAL

Tabla 2-5 Características Servidor Base de datos

2.4. MEDIOS DE COMUNICACIÓN

2.4.1. ALÁMBRICOS

2.4.1.1. MATRÍZ SAN CRISTOBAL

El medio utilizado para la comunicación entre las maquinas en el Edificio Matriz de la INGALA es cable UTP categoría 5, con velocidad de transmisión de 10 Mbps.

2.4.1.2. SUCUSALES COORDINACIONES

El medio que se utiliza en las Coordinaciones de Quito y Guayaquil para la comunicación entre las maquinas es cable UTP categoría 5, con velocidad de transmisión de 10 Mbps.

2.4.2. INALÁMBRICOS

Enlace satelital trabajando en banda KU con un ancho de banda de 64 Kbps.
Este enlace se utiliza para la actualización de las bases de datos entre la matriz ubicada en San Cristóbal con el continente (Quito).

Cabe destacar que para este tipo de comunicación se utiliza como carrier a la compañía Global Crossing.

2.5. DISPOSITIVOS DE CONMUTACIÓN

A continuación se detallan los dispositivos de conmutación utilizados en el edificio Matriz y sus Coordinaciones:

CANTIDAD	DISPOSITIVO	MARCA	MODELO	CARACTERÍSTICAS	UBICACIÓN
4	Hub	3Com	Office connect	Dual Speed de 8 Puertos	Edificio Matriz San Cristóbal
1	Hub	3Com	Office connect	Dual Speed de 8 Puertos	Coordinación Guayaquil

Tabla 2-6 Dispositivos de Conmutación

2.5.1. ENLACE PRINCIPAL

El enlace principal es a través de satélite el cual es proporcionado por la compañía Impsat localizada en Quito.
El enlace de Quito a guayaquil se hace mediante Dial Up a través de Andinatel.

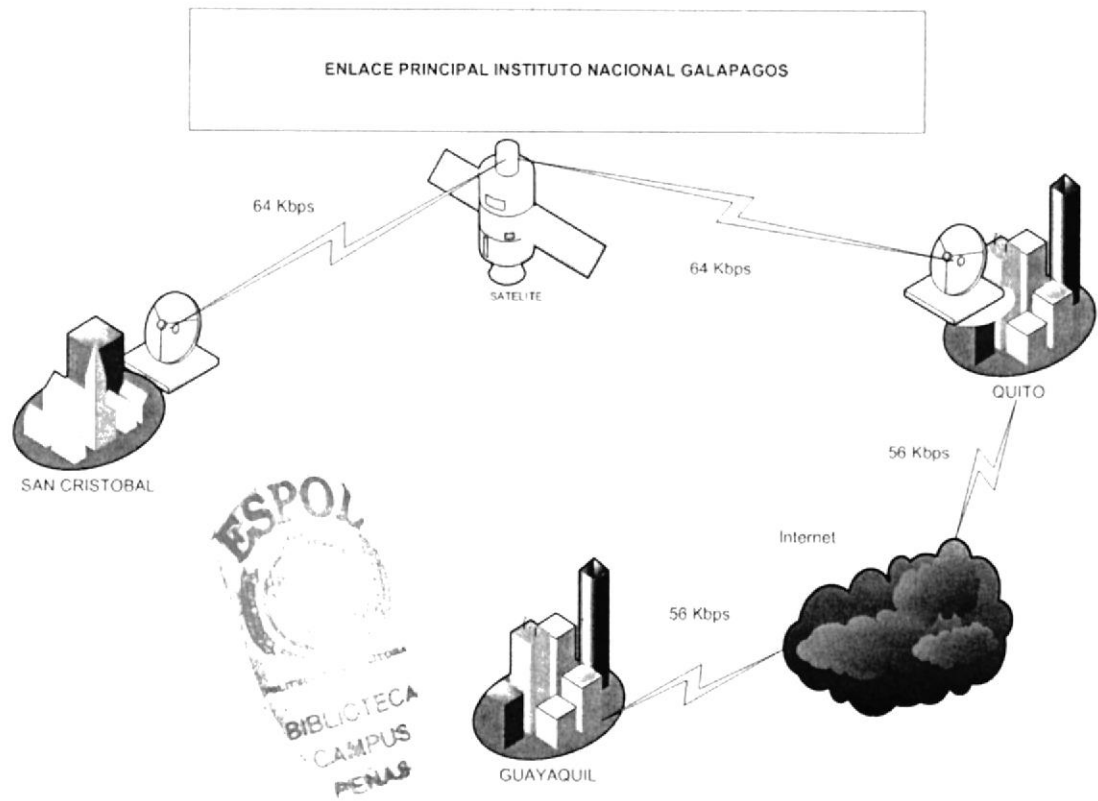


Figura 2-1 Enlace Principal

2.5.2. DISPOSITIVOS DE ENRUTAMIENTO

CANTIDAD	DISPOSITIVO	MARCA	MODELO	CARACTERI STICAS	UBICACIÓN
1	Router	Cisco	2600	Protocolos de interconexión fast ethernet, serial.	EDIFICIO MATRIZ SAN CRIDTOBAL
1	Router	Cisco	2600	Protocolos de interconexión fast ethernet, serial.	EDIFICIO QUITO

Tabla 2-7 Dispositivos de Enrutamiento

2.5.3. DESCRIPCIÓN DE EQUIPOS DE LA RED WAN

EQUIPOS	CARACTERISTICAS	UBICACIÓN
1 Antena	1383 Ku-Band Antenna 3.8 mt marca Prodelin With 40 watt SSPA + Scopus Encoder	Edificio Matriz San Cristóbal/Quito
1 Transceiver	10 vatios Codan C-band marca EFData	Edificio Matriz San Cristóbal/Quito
1 Feed	Port Circular Feed marca EFData	Edificio Matriz San Cristóbal/Quito
1 LNA	Frequency range of 10.95 to 11.7 GHz marca EFData	Edificio Matriz San Cristóbal/Quito
1 Módem Satelital	SDM-300 High rate to 100meg, ASI I/F available marca EFData	Edificio Matriz San Cristóbal/Quito

Tabla 2-8 Dispositivos de Enrutamiento

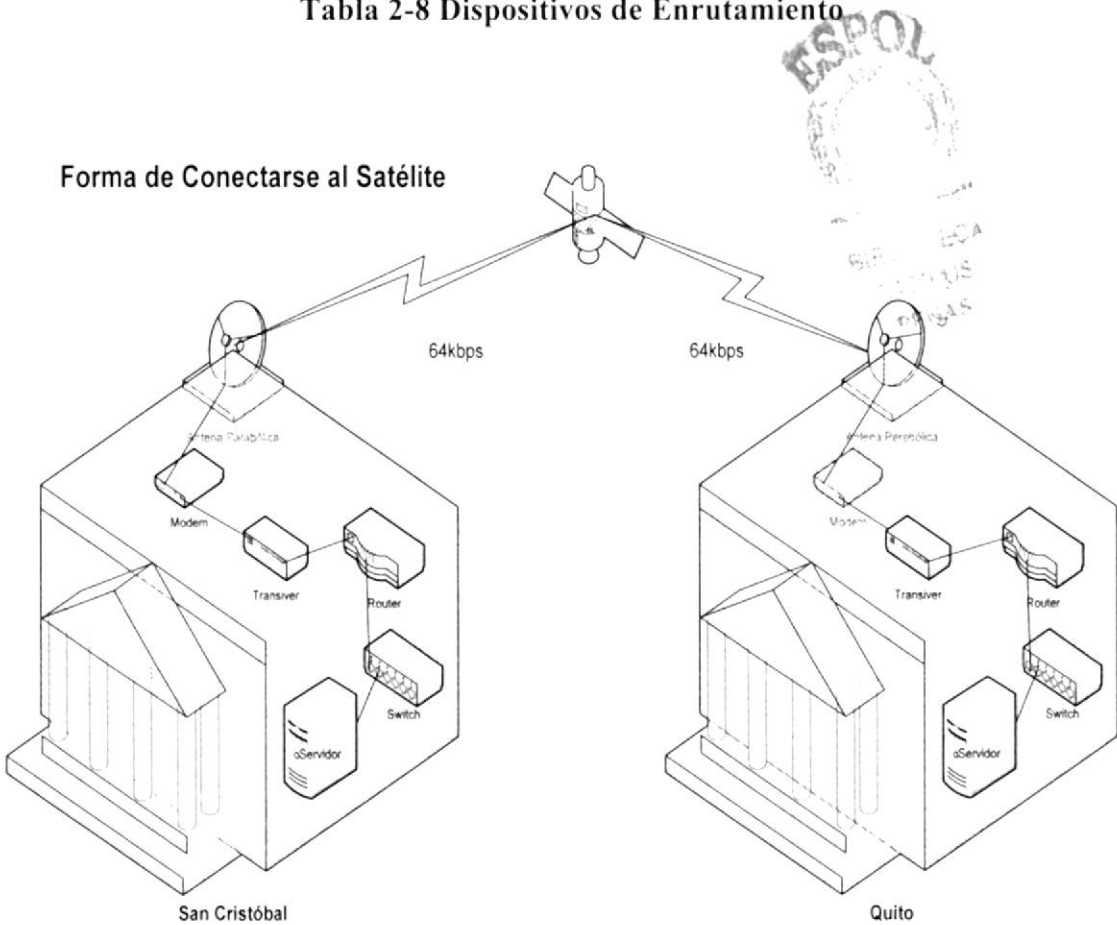


Figura 2-2 Recepción de Internet

2.6. RECEPCIÓN DE INTERNET EN EL EDIFICIO MATRÍZ

La conexión de Internet llega a través de un enlace dial up (PACIFICTEL)

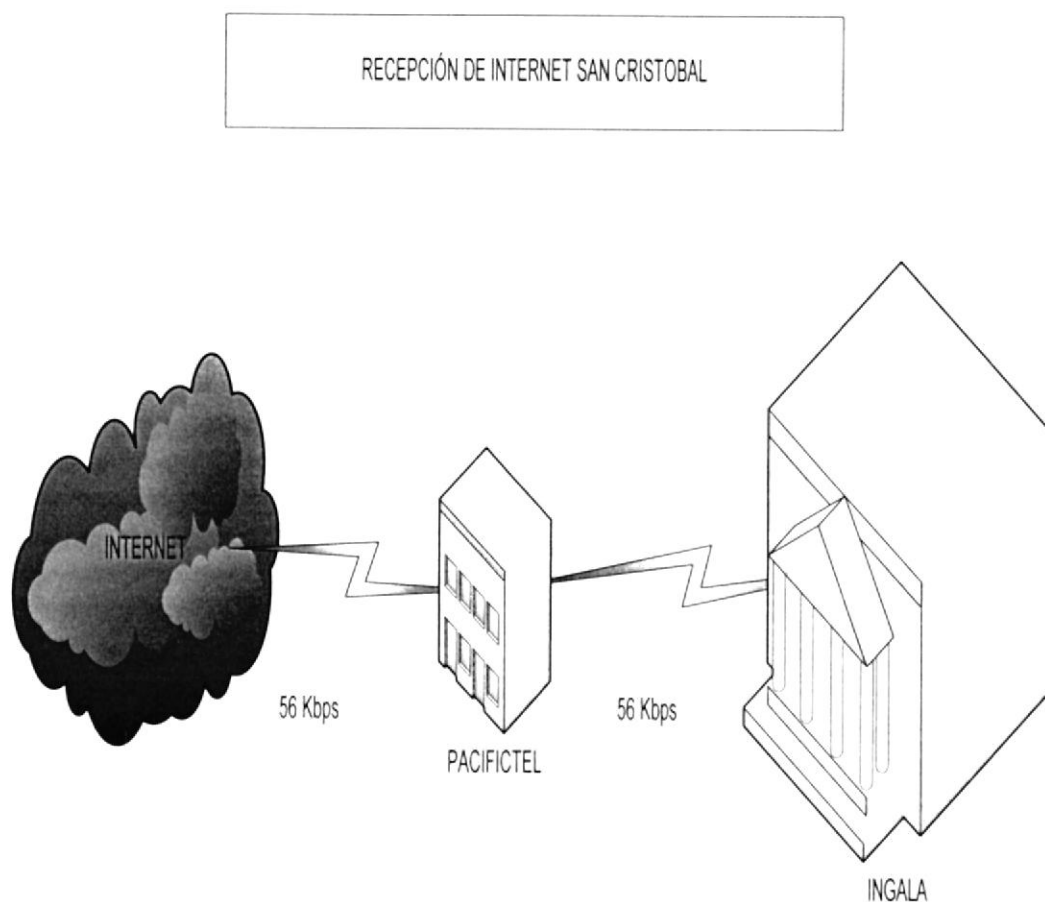


Figura 2-3 Recepción de Internet



2.7. **PROBLEMAS ENCONTRADOS**

• Inexistencia de cableado estructurado en ninguna parte de la institución.
• Lentitud en comunicaciones entre matriz y continente.
• Equipos de conmutación obsoletos.
• Existencia de broadcast y tráfico en la red Lan.
• Servidores desactualizados a nivel de hardware en Matriz.
• Conexiones a Internet ineficaces e ineficientes.
• Comunicación real de datos inexistente entre Matriz- Guayaquil y Guayaquil –Quito

Tabla 2-9 Problemas Encontrados





CAPÍTULO 3

PROPUESTA

3.1. PROBLEMAS ENCONTRADOS

PROBLEMA	CAUSA	EFEECTO
Inexistencia de cableado estructurado en ninguna parte de la institución.	Personal no capacitado en el área de sistemas estructurados.	Deficiente escalabilidad de la red Lan. Dificultad para mejoras futuras. Pobre administración en la red actual.
Lentitud en la comunicación entre la matriz y sus sucursales.	Poco ancho de banda para las comunicaciones Wan.	Perdida de tiempo en el envío de datos entre las sucursales y matriz.
Equipos de conmutación obsoletos.	Todas las maquinas comparten demasiados recursos que impactan negativamente en el rendimiento.	Lentitud en la actualización de las bases de datos y accesos a los recursos de los demás usuarios.
Existencia de broadcast y exceso en tráfico en la Lan.	No existe segmentación en la red Lan.	Frecuente congestionamiento en la red Lan. Aumento de los dominios de colisión. Disminución en el rendimiento de la red.
Servidores de bajo rendimiento a nivel de hardware en Matriz.	Escasa memoria en los servidores	Lentitud en los procesos que se llevan a cabo en línea, deficiencia en la autenticación y autorización de las maquinas cliente.
Conexión a Internet ineficaz e ineficientes. Hay momentos en que no se pueden conectar o se conectan de forma lenta. A veces o pueden abrir el correo de Quito.	Conexión dial up solo utilizada cuando se la requiere	No hay comunicación en línea entre las sucursales. Falta de seguridad en la transmisión de datos.
Comunicación real de datos inexistente entre Matriz- Guayaquil y Guayaquil -Quito	Solo hay comunicación de datos entre Matriz y Quito.	Lentitud los tramites de residentes y colonos en Guayaquil y Quito

Tabla 3.1 Problemas Encontrados



3.2. SOLUCIÓN PROPUESTA

PROBLEMA	SOLUCIÓN	ALCANCE
Inexistencia de cableado estructurado en ninguna parte de la institución.	Implementación de un sistema de cableado estructurado	Optima administración de la red Lan y ordenado crecimiento de la misma
Lentitud en la comunicación entre la matriz y coordinaciones	Contratación de enlace de 128 Kbps para conexión satelital.	Mejora de la velocidad de transmisión de datos entre matriz y coordinaciones.
Equipos de conmutación obsoletos.	Reemplazo de los hubs por switches	Mejorar la velocidad de transmisión en la red Lan
Existencia de broadcast y tráfico en la Lan.	Implementación de vlans y segmentación en la red	Evitar broadcast en nuestra red y una mejor administración.
Servidores de bajo rendimiento a nivel de hardware en Matriz.	Compra e instalación de 1Gb de memoria adicional. Actualización de la Bios del mainboard	Procesos más rápidos en los servidores.
Conexión a Internet ineficaz e ineficientes. Hay momentos en que no se pueden conectar o se conectan de forma lenta. A veces o pueden abrir el correo de Quito.	Contratación de enlace de 128 Kbps para conexión satelital.	Comunicación rápida y en línea entre las coordinaciones..

Tabla 3.2 Solución Propuesta

3.3. ESTUDIO DE FACTIBILIDAD

Como principal objetivo de nuestra propuesta, es manejar una velocidad integral dentro de la empresa, haciendo uso de equipos que están acordes a la tecnología actual, además de llevar una rápida y segura comunicación Wan, con sus respectivas adquisiciones de equipos.

3.3.1. FACTIBILIDAD TÉCNICA

CANTIDAD	DESCRIPCIÓN	CARACTERÍSTICAS	UBICACIÓN
1	Switch	2810-24 Gigabit 10/100/1000 Gigabit Switch 24-port 10/100/1000BASE-T (RJ-45) Gigabit Ethernet	Matriz
1	Switch	HP ProCurve 2810-24Gigabit 10/100/1000 Gigabit Switch 12-port 10/100/1000BASE-T (RJ-45) Gigabit Ethernet	Guayaquil
1	Router	Protocolos de interconexión fast ethernet, serial.	Guayaquil
1	Firewall	Cisco ASA Appliance 4 interfaz giga ethernet 1 interfaz fase ethernet	Matriz
1	S:O	Smart cisco para Frewall ASA 5520	Matriz
2	Tarjetas de memoria	Compaq Fast Memory DDR 1 1Gb	Matriz
305 mt	Cable UTP	Cat 6 Bobina	Matriz
50	Conectores	RJ 45	Matriz

44	Patch Cord	Cat 6	Matriz
50 mt	Canaletas	32 x 12 de 2 metros cada una	Matriz
22	Caja de terminación	Para Empotrar a la pared	Matriz
22	Wall plate	De 2 servicios	Matriz
1	rack	Piso abierto de 44 UR de 1.95 mtr	Matriz
1	Patch panel	24 puertos Cat 6	Matriz
1	Regleta multitoma	8 conectores	Matriz
1	Bandeja de rack	Standard	Matriz

Tabla 3.3 Factibilidad Técnica

3.3.2. ENLACES

El enlace para las telecomunicaciones entre las diferentes localidades (matriz y sucursales). El cual brindará un servicio de un ancho de banda de 128 Kbps en sustitución del enlace satelital de 64 Kbps.

CANTIDAD	DESCRIPCIÓN	CARACTERÍSTICAS	UBICACIÓN
1	Enlace	Enlace de datos de 128 Kbps	Matriz-Quito
1	Enlace	Enlace de datos de 128 Kbps	Guayaquil- Matriz

Tabla 3.4 Enlaces



CAPÍTULO 4

IMPLEMENTACIÓN WAN

4.1. ANÁLISIS DE PISOS APLICATIVOS

4.1.1. MATRIZ SAN CRISTÓBAL

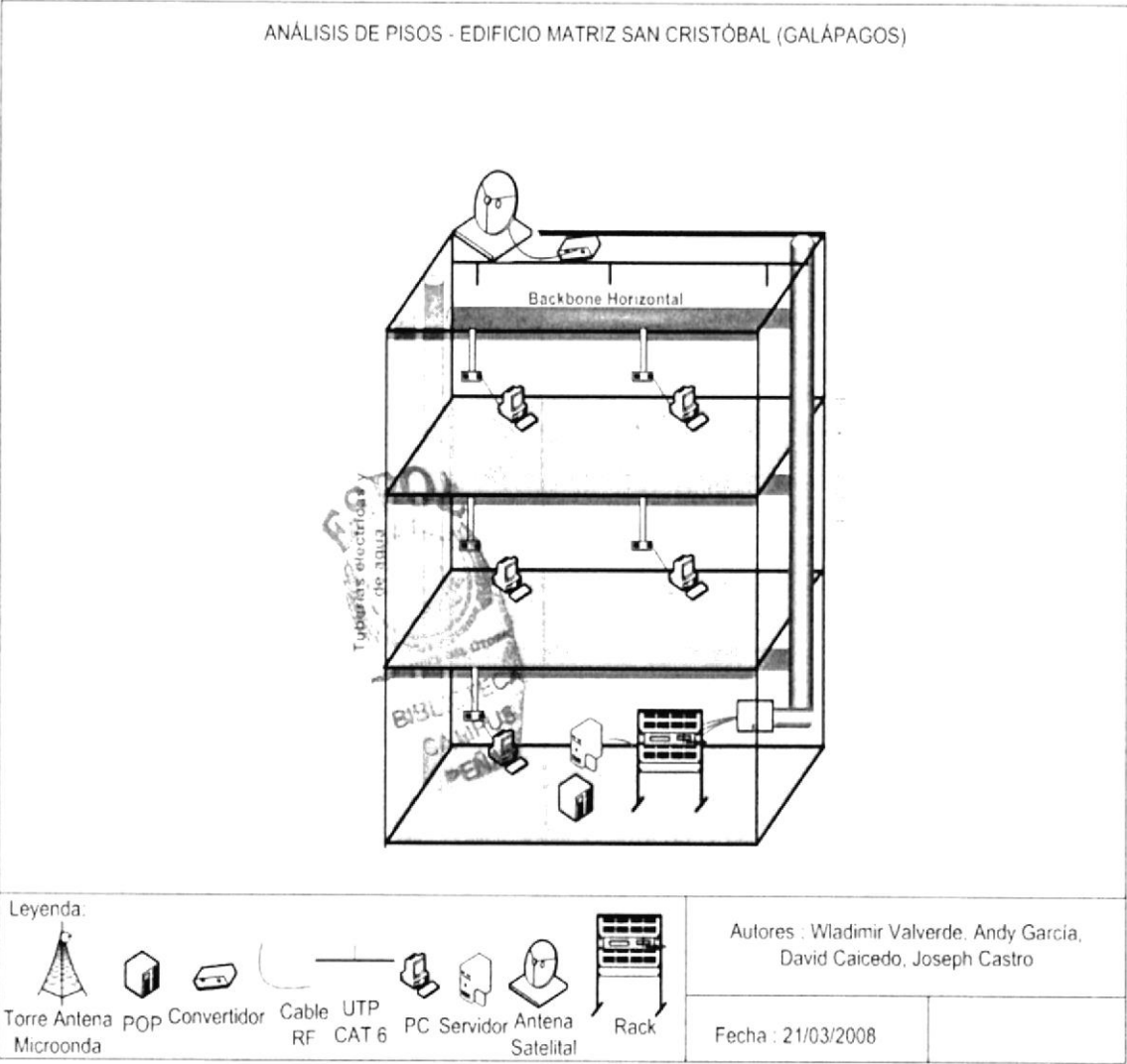


Figura 4-1 Implementación Coordinación San Cristóbal

4.1.2. SUCURSAL COORDINACIÓN QUITO

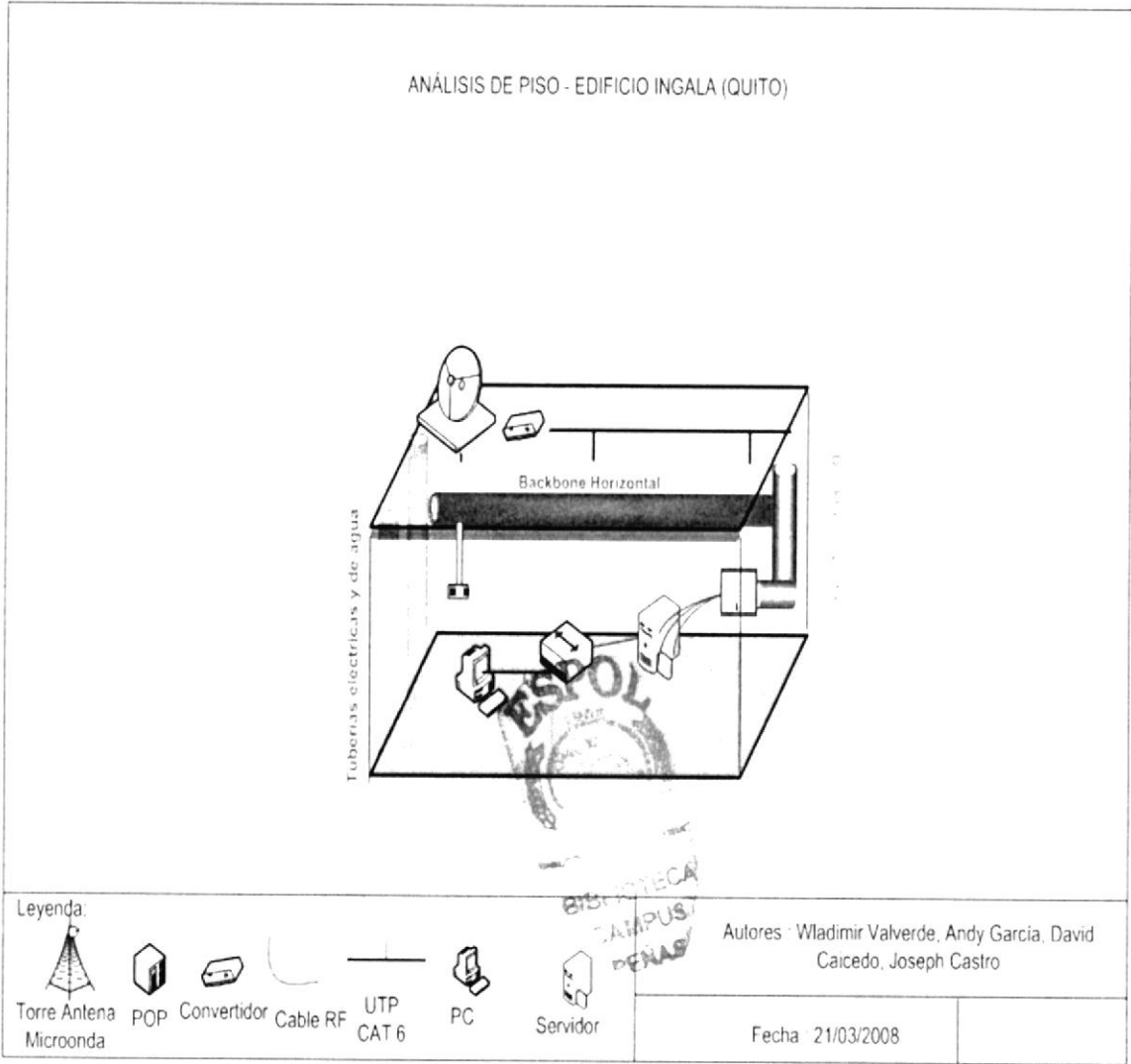


Figura 4-2 Implementación coordinación Quito

4.1.3. SUCURSAL COORDINACIÓN GUAYAQUIL

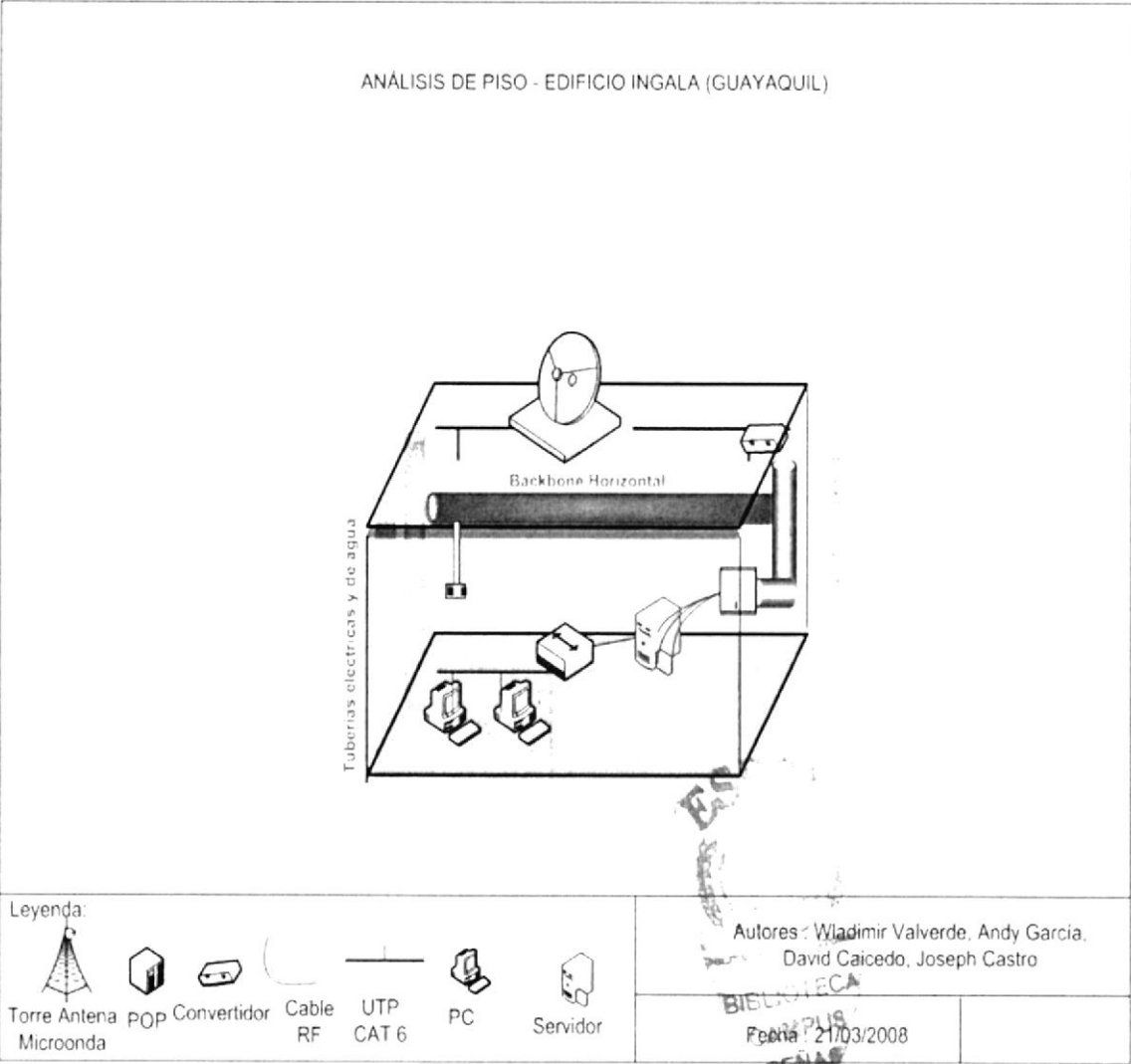


Figura 4-3 Implementación Coordinación Guayaquil

4.2. ENLACE DE DATOS

4.2.1. MATRÍZ – QUITO

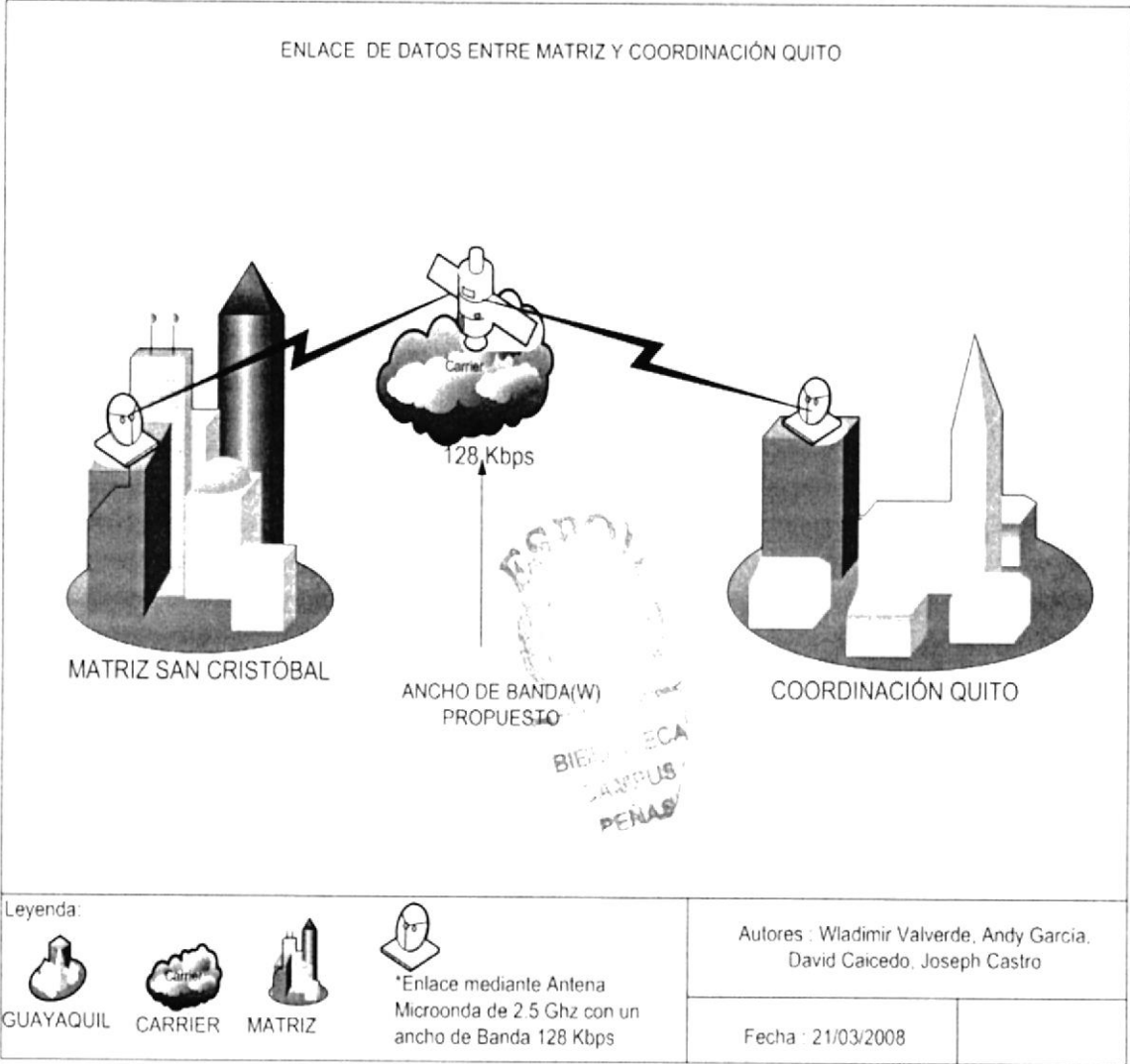


Figura 4-4 Enlace Datos Matriz-Quito

4.2.2. MATRÍZ – GUAYAQUIL

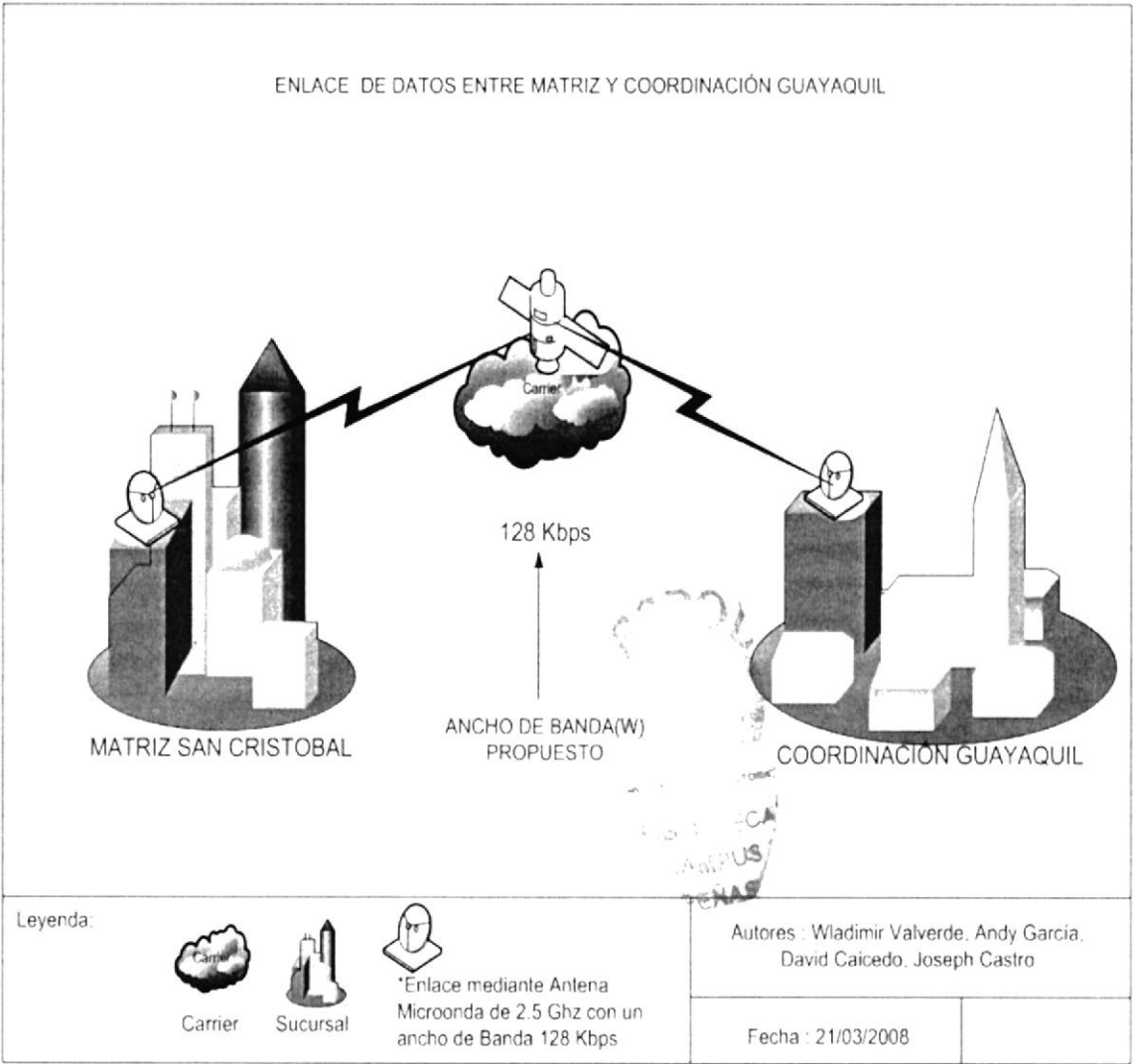


Figura 4-5 Enlace Matriz –Guayaquil

4.2.3. GUAYAQUIL-QUITO

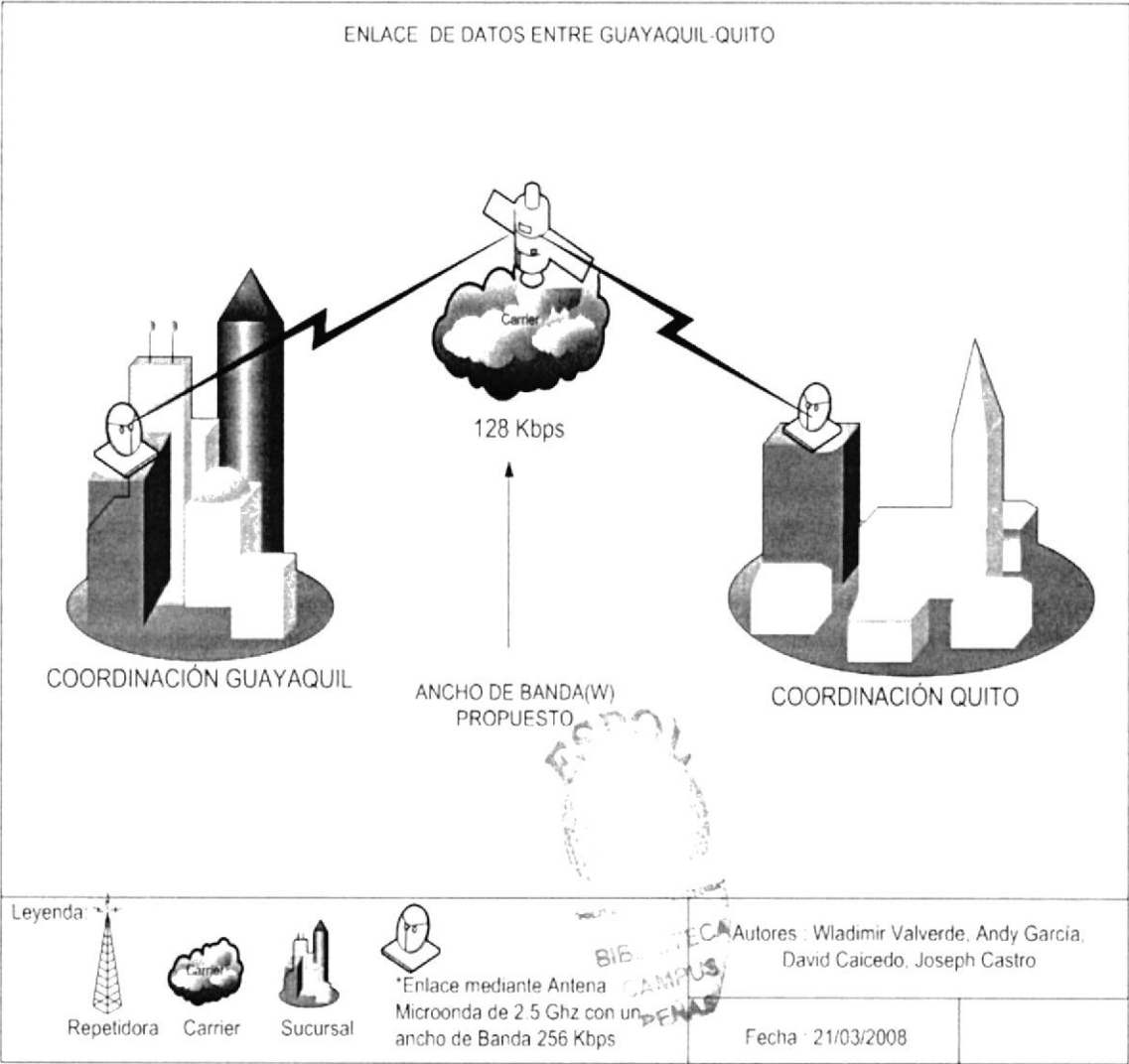


Figura 4-6 Enlace Guayaquil-Quito

4.3. COMUNICACIÓN WAN A NIVEL DE DISPOSITIVOS MATRÍZ Y SUCURSALES

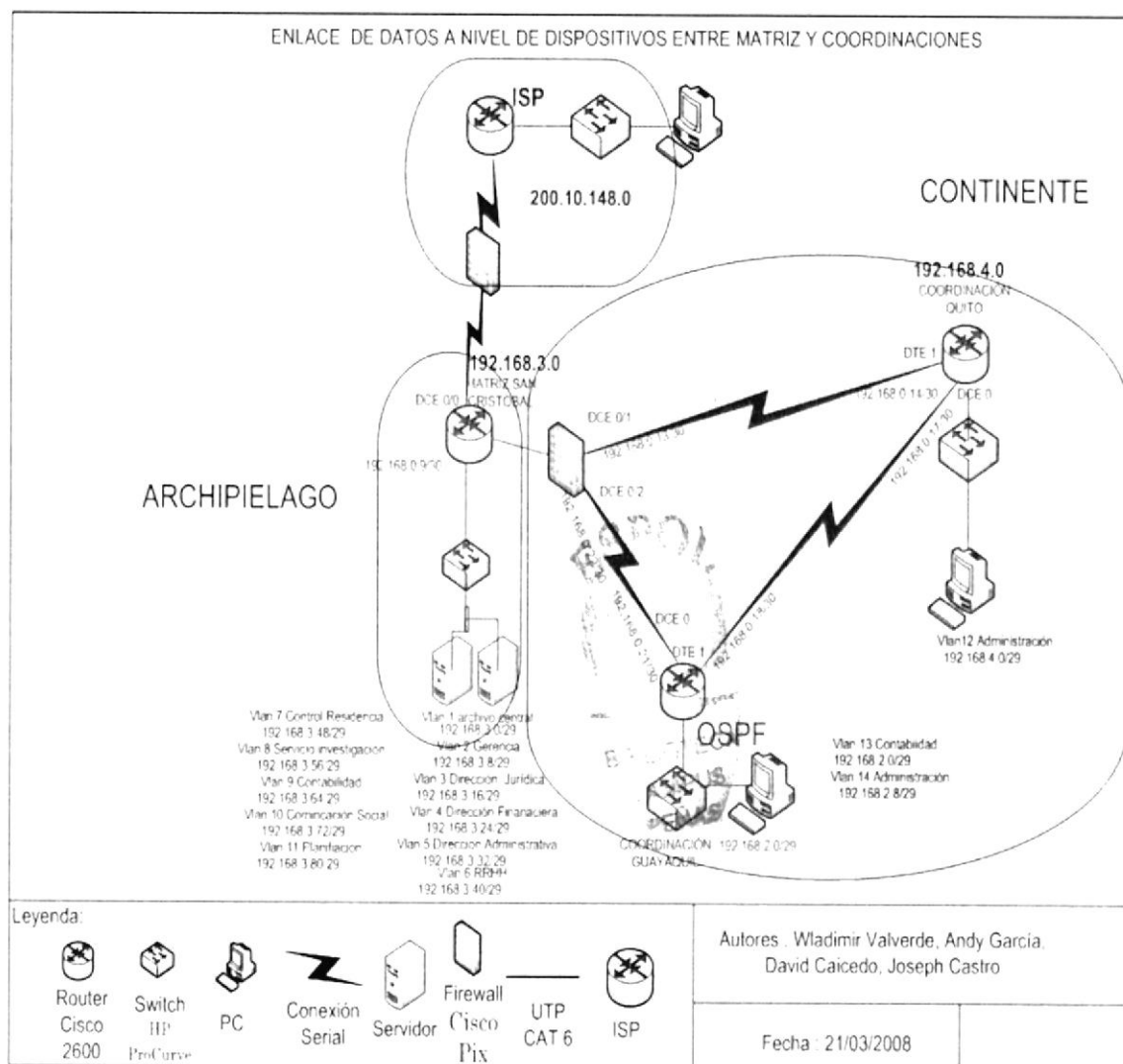


Figura 4-7 Gráfico Comunicación Wan Ingala



CAPÍTULO 5

CONFIGURACIÓN ROUTERS Y SWITCHES

5.1. INTRODUCCIÓN A LOS ROUTERS

Un router es un tipo especial de computador. Cuenta con los mismos componentes básicos que un PC estándar de escritorio. Cuenta con un CPU, memoria, bus de sistema y distintas interfaces de entrada/salida. Sin embargo, los routers están diseñados para cumplir algunas funciones muy específicas que, en general, no realizan los computadores de escritorio. Por ejemplo, los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

Al igual que los computadores, que necesitan sistemas operativos para ejecutar aplicaciones de software, los routers necesitan el software denominado Sistema operativo de internetworking (IOS) para ejecutar los archivos de configuración. Estos archivos de configuración contienen las instrucciones y los parámetros que controlan el flujo del tráfico entrante y saliente de los routers. Específicamente, a través de los protocolos de enrutamiento, los routers toman decisiones sobre cuál es la mejor ruta para los paquetes. El archivo de configuración especifica toda la información necesaria para una correcta configuración y usos de los protocolos enrutados y de enrutamiento seleccionados, o habilitados, en el router.

5.2. VENTAJAS DE LOS ROUTERS

Seguridad. Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.

Flexibilidad. Las redes interconectadas con router no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con bridge.

Soporte de Protocolos. Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.

5.3. DESVENTAJAS DE LOS ROUTERS

- Lentitud de proceso de paquetes respecto a los bridges.
- Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
- Precio superior a los bridges.
- Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para una gran interconexión de redes con múltiples tipos de RALs, MANs, WANs y diferentes protocolos. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas.

5.4. MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER

5.4.1. 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 marcara el clock rate.

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

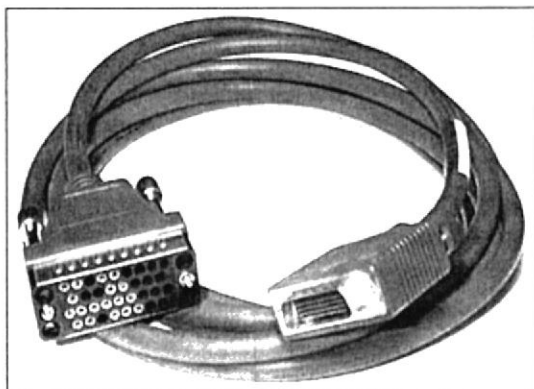


Figura 5-1 Cable DCE

5.4.2. 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 distinguible por tener el conector smartnet más grande.



Figura 5-2 Cable DTE



5.4.3. 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.

Para la conexión entre el Gabinete y la roseta de conexión el largo máximo aceptado es de 100 metros.

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.

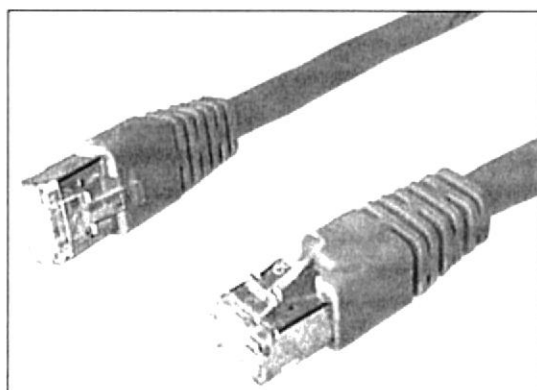


Figura 5-3 Cable UTP

5.4.4. CONECTOR RJ45

El conector RJ-45, es similar al telefónico, pero algo más grande y con capacidad para ocho contactos o hilos. El conector RJ-45, debe existir en cada extremo del cable de par trenzado. Para conectar el cable a la tarjeta, colocar el conector de forma que la patilla de plástico quede en línea con la ranura de la hembra y empuje el conector hasta escuchar un clic (el conector es similar al enchufe de plástico que se utiliza para conectar un cordón telefónico con un enchufe telefónico de pared).

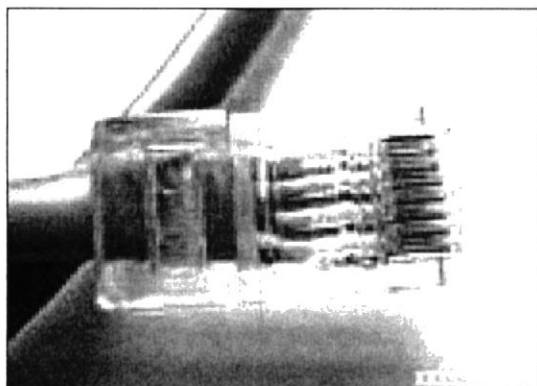


Figura 5-4 Conector RJ45



5.4.5. PUERTO SERIAL (CONECTOR COM)

El puerto serie usa conectores tipo D-9. Estos puertos hacen transferencia de datos en serie; o sea comunican la información de un bit en una línea.

Estos puertos son compatibles con dispositivos como módems externos y los mouse.

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).

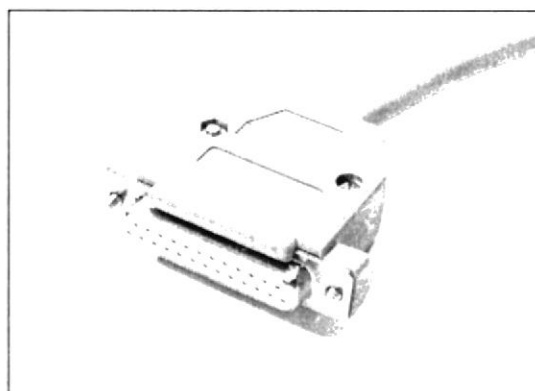


Figura 5-5 Puerto Serial

5.5. PARTES INTERNAS DE UN ROUTER

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

- **CPU:** La unidad central de procesamiento. (CPU) ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varias CPU.
- **RAM:** La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Por lo general, la RAM se divide de forma lógica en memoria del procesador principal y memoria compartida de entrada/salida (I/O). Las interfaces de almacenamiento temporal de los paquetes comparten la memoria de I/O compartida. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más Módulos de memoria en línea doble (DIMM).

Tiene las siguientes características y funciones:

- Almacena las tablas de enrutamiento.
 - Guarda el caché ARP.
 - Guarda el caché de conmutación rápida.
 - Crea el buffer de los paquetes (RAM compartida).
 - Mantiene las colas de espera de los paquetes.
 - Brinda una memoria temporal para el archivo de configuración del router mientras está encendido.
 - Pierde el contenido cuando se apaga o reinicia el router.
- **NVRAM:** La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

La NVRAM tiene las siguientes características y funciones:

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

La memoria flash tiene las siguientes características y funciones:

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

- **ROM:** La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM en los tomas.
 - La memoria de sólo lectura (ROM) tiene las siguientes características y funciones:
 - Guarda las instrucciones para el diagnóstico de la prueba al inicio (POST).
 - Guarda el programa bootstrap y el software básico del sistema operativo.
 - Requiere del reemplazo de chips que se pueden conectar en el motherboard para las actualizaciones del software.
- **BUSES:** La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces.

5.6. PARTES EXTERNAS DEL ROUTER

5.6.1. INTERFACES

Una interfaz en términos generales se puede definir como un medio de acople entre dos dispositivos.

En los routers son las interfaces las que permiten conectar a las redes. Un router básicamente tiene tres tipos de interfaces o conexiones: LAN's, WAN's y puertos de consola/Aux.

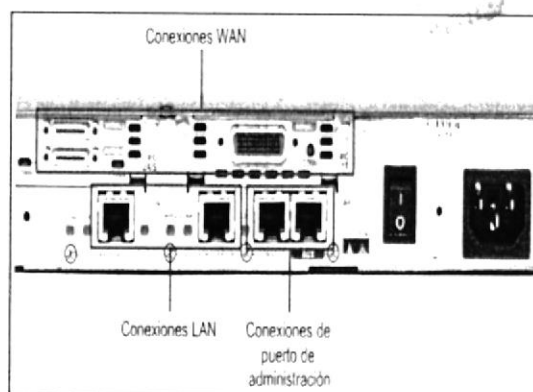


Figura 5-6 Interfaces Del Router

- **Conexiones LAN's.-** Por lo general son tecnología Ethernet.
- **Conexiones WAN's.-** Pueden ser seriales por lo general vienen dos por cada Router.

- **Conexiones RDSI.-** Los puertos de consola/Aux. son puertos para la administración o configuración de la máquina.

5.7. REDUNDANCIA EN LOS ROUTERS

De nada sirve tener servidores con componentes duplicados y redundantes y un suministro eléctrico constante y equilibrado si algunos de los componentes de la red fallan y no se accede al servidor.

Los componentes más normales en una red son:

- **Routers (enrutador):** Es un dispositivo que interconecta segmentos de red o redes enteras
- **Switch (Conmutador):** Es un dispositivo que interconecta dos o más segmentos de red
- **Tarjeta de red o NIC:** Es un dispositivo electrónico que permite a una DTE (Data Terminal Equipment), ordenador o impresora, acceder a una red y compartir recursos
- **Cables de red:** Para interconectar los diferentes componentes, existen muchos y variados tipos, siendo los más comunes el cable de par trenzado y el de fibra óptica
- **Lineas de conexión:** a la red de área amplia, WAN (por ejemplo Internet)

Cualquiera de estos componentes puede fallar, dejando al sistema incomunicado. Pero existen técnicas para evitar que esto ocurra, lo que se suele hacer es configurar la red, para que al menos existan 2 caminos diferentes entre dos componentes A y B.

En el gráfico siguiente hay un esquema, en el que se puede ver como configurar una red con redundancia doble desde el servidor hasta Internet.

De esta manera se puede estropear un router, un switch y una tarjeta de red a la vez sin que se pierda conectividad.

El mismo esquema se podría ampliar para tener redundancia triple o cuádruple de los componentes.

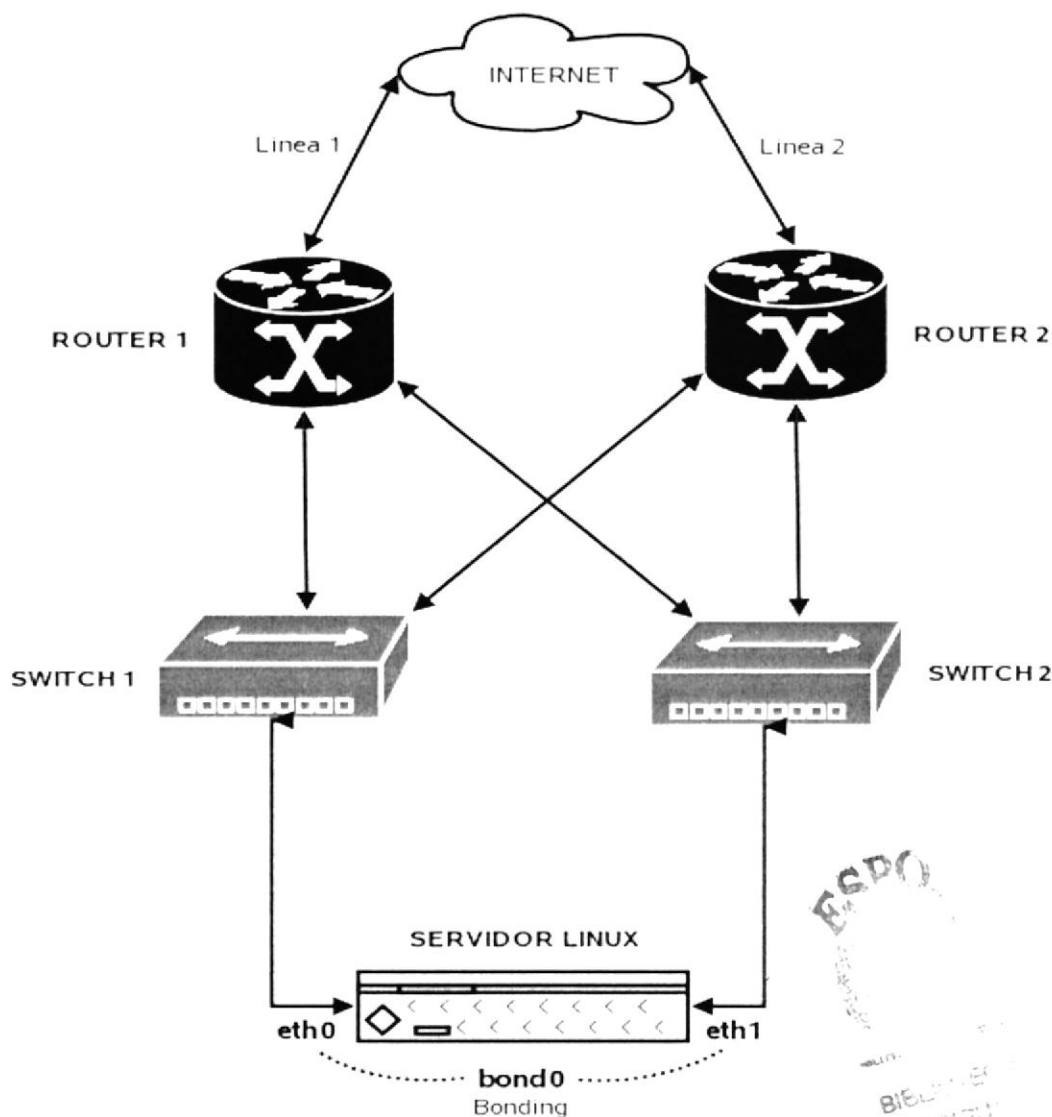


Figura 5-7 Interfaces Del Router

5.8. REDUNDANCIA EN LA CONFIGURACIÓN DE ROUTERS

5.8.1. HSRP

El Hot Standby Router Protocol es un protocolo de enrutamiento de "hot standby", propiedad de Cisco que proporciona una disponibilidad de red de alto desempeño y cambios de topología de red transparentes, evitando en la medida de lo posible la existencia de puntos de fallo únicos en la red. HSRP ofrece tanto rutas de acceso redundantes como equipos redundantes en lugares clave de la red para evitar que cualquier dispositivo cause que los recursos vitales de la red dejen de poder utilizarse.

5.8.1.1. CARACTERÍSTICAS

HSRP está concebido como protocolo para manejar redundancia de capa 3 en el gateway de la LAN. Por lo tanto administra redundancia entre interfaces que están en una misma red o subred.

El funcionamiento del protocolo HSRP es el siguiente, crea un grupo de router de "hot standby" con un router guía o maestro para atender todos los paquetes que se envían a la dirección de espera en caliente. El router guía se controla a través de otros routers del grupo, y si alguno falla, uno de estos routers de reserva hereda la posición de guía así como la dirección del grupo de "hot standby".

5.8.1.2. IMPLEMENTACIÓN

Imagine que dispone de una red que cuenta con dos routers redundantes, RouterA y RouterB. Dichos routers pueden estar en dos posibles estados diferentes: primario (RouterA) y standby (Router B).

Para administrar la redundancia, ambos routers (el router primario y el standby) intercambian paquetes HSRP hello que le permiten a cada uno conocer el estado del otro. Estos paquetes hello utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985.

Si el router primario o activo no envía paquetes hello al router standby por un determinado periodo de tiempo, el router standby asume que el primario está fuera de servicio por algún motivo y hereda la posición de router primario o activo. De este modo, el router que estaba standby asume la responsabilidad de la IP virtual y comienza a responder a la dirección MAC virtual a la que apunta la IP virtual.

HSRP se encuentra disponible desde Cisco IOS 10.0, pero se han incorporado nuevas funcionalidades en las versiones 11 y 12.

5.8.1.3. ELECCIÓN DEL ROUTER "ACTIVO"

Para determinar cual es el router activo se configura una prioridad. La prioridad por defecto es 100 y el router de mayor prioridad es el que se establecerá como activo. Hay que tener presente que HSRP no se limita a 2 routers, sino que se pueden generar grupos de router que trabajen en conjunto de modo que se dispondría de múltiples dispositivos en situación standby.

5.8.1.4. PASO DE ESTADO "STANDBY" A ESTADO "ACTIVO"

El router en espera (standby) toma el lugar del router activo, una vez que el temporizador holdtime expira (un equivalente a tres paquetes hello que no vienen desde el router activo, timer hello por defecto definido a 3 y holdtime por defecto definido a 10). Los tiempos de convergencia dependerán de la configuración de los temporizadores para el grupo y del tiempo de convergencia del protocolo de enrutamiento empleado.

Por otra parte, si el estado del router activo pasa a down, el router decrementa su prioridad. Así, el router Standby lee ese decremento en forma de un valor presente en el campo de prioridad del paquete hello, y se convertirá en el router activo si ese valor decrementado es inferior a su propia prioridad. Este proceso decremental puede ser configurado de antemano estableciendo un valor por defecto del decremento (normalmente, de 10 en 10).

5.8.1.5. CONFIGURACIÓN

Para el RouterA, que va a establecer como maestro o primario:

```
Configuración de la dirección IP de la interfaz Ethernet.  
Configuración de la dirección IP virtual.  
Configuración de la prioridad HSRP con un valor igual a 100.
```

Para el RouterB:

```
Configuración de la dirección IP de la interfaz Ethernet.  
Configuración de la dirección IP virtual.  
Configuración de la prioridad HSRP con un valor menor a 100.
```

En los terminales conectados a los routers se configura la dirección IP virtual como default gateway, no la dirección real de la interfaz de los dispositivos. De este modo, si uno de los dispositivos queda fuera de servicio el otro toma su lugar automáticamente y de modo transparente para los nodos.

El tiempo requerido para este cambio es menor a los 10 segundos.

5.9. ENRUTAMIENTO

5.9.1. ENRUTAMIENTO ESTÁTICO

Las operaciones con rutas estáticas pueden dividirse en tres partes:

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

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

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

Para verificar la distancia administrativa de una ruta en particular use el comando show ip route address, donde la dirección ip de dicha ruta se inserta en la opción address. Si se desea una distancia administrativa diferente a la distancia por defecto, se introduce un valor entre 0 y 255 después de la interfaz de salida.

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta.

A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida.

Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

5.10. ENRUTAMIENTO DINÁMICO

5.10.1. PROTOCOLOS DE ENRUTAMIENTO

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

Ejemplos de protocolos de enrutamiento:

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

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

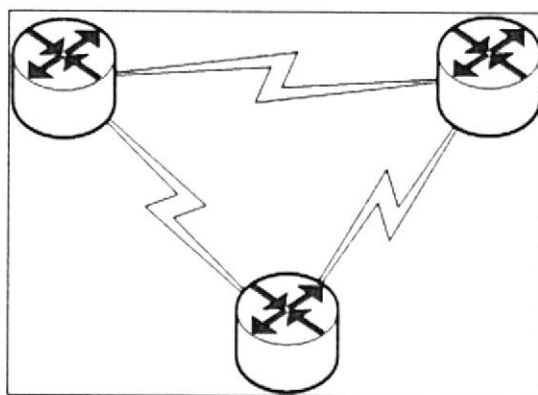


Figura 5-8 Esquema De Comunicación

5.11. TIPOS DE PROTOCOLOS

5.11.1. EL PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP)

Es un protocolo de enrutamiento por vector-distancia, en uso en miles de redes en todo el mundo. El hecho que RIP se base en estándares abiertos y que sea de fácil implementación hace que resulte atractivo para algunos administradores de redes, aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados.

RIP ha evolucionado a lo largo de los años desde el Protocolo de enrutamiento con definición de clases, RIP Versión 1 (RIP v1), hasta el Protocolo de enrutamiento sin clase, RIP Versión 2 (RIP v2).

Las mejoras en RIP v2 incluyen:

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

Sus características principales son las siguientes:

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

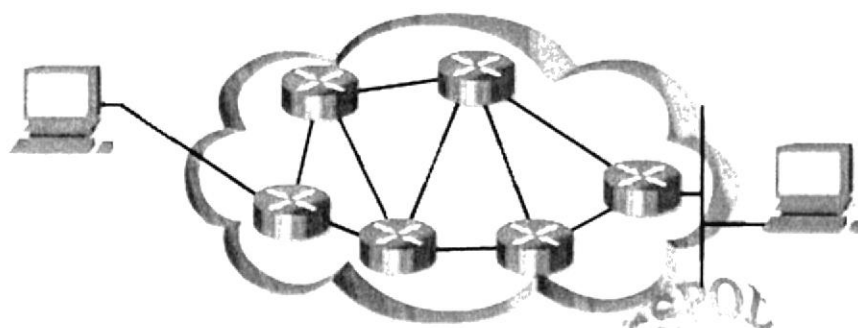


Figura 5-9 RIP

5.12. FUNCIONAMIENTO RIP

RIP utiliza UDP para enviar sus mensajes y el puerto bien conocido 520. RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.

RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado)

RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).

La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino.

Teniendo en cuenta el límite de 15 saltos mencionado anteriormente. Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada.

Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.

Las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.

5.12.1. VENTAJAS Y DESVENTAJAS

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

Por otra parte, tiene la desventaja que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos (por cuántos routers o equipos similares pasa la información); no toma en cuenta otros criterios importantes, especialmente el ancho de banda.

Esto puede causar ineficiencias, ya que puede preferir una ruta de bajo ancho de banda.

5.12.2. MENSAJES RIP

Los mensajes RIP pueden ser de dos tipos.

5.12.2.1. PETICIÓN

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

5.12.2.2. 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.
- Mensajes enviados como respuesta a mensajes de petición.
- Mensajes enviados cuando cambia algún coste. Sólo se envían las rutas que han cambiado.

5.12.2.3. FORMATO DE LOS MENSAJES RIP

Los mensajes tienen una cabecera que incluye el tipo de mensaje y la versión del protocolo RIP, y un máximo de 25 entradas RIP de 20 bytes.



Las entradas en RIPv1 contienen la dirección IP de la red de destino y la métrica.

Las entradas en RIPv2 contienen la dirección IP de la red de destino, su máscara, el siguiente enrutador y la métrica. La autenticación utiliza la primera entrada RIP.

5.13. EL PROTOCOLO DE ENRUTAMIENTO INTERIOR DE GATEWAY (IGRP)

IGRP es un protocolo de enrutamiento basado en la tecnología vector-distancia. Utiliza una métrica compuesta para determinar la mejor ruta basándose en el ancho de banda, el retardo, la confiabilidad y la carga del enlace. El concepto es que cada router no necesita saber todas las relaciones de ruta/enlace para la red entera.

Cada router publica destinos con una distancia correspondiente. Cada router que recibe la información, ajusta la distancia y la propaga a los routers vecinos. La información de la distancia en IGRP se manifiesta de acuerdo a la métrica. Esto permite configurar adecuadamente el equipo para alcanzar las trayectorias más óptimas.

Entre las características de diseño claves del IGRP se destacan las siguientes:

Es un protocolo de enrutamiento por vector-distancia.

Se considera el ancho de banda, la carga, el retardo y la confiabilidad para crear una métrica compuesta.

Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

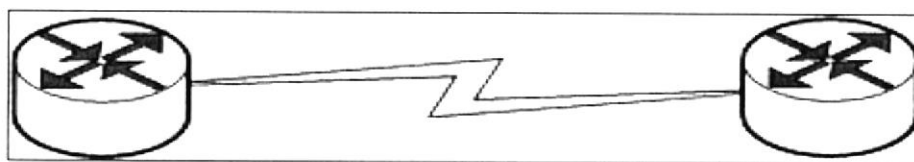


Figura 5-10: IGRP

5.13.1. EL PROTOCOLO EIGRP

Es un protocolo de encaminamiento híbrido, propietario de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP.

Sin embargo, EIGRP es más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP.

Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP.

Las características claves del EIGRP son las siguientes:

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

Los routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos.

Las rutas reciben un estado y se pueden rotular para proporcionar información adicional de utilidad.

EIGRP mantiene las siguientes tres tablas:

5.13.2. TABLA DE VECINOS

Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes.

Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP.

5.13.3. TABLA DE TOPOLOGÍA

La tabla de topología se compone de todas las tablas de encaminamiento EIGRP recibidas de los vecinos.

EIGRP toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino.

EIGRP rastrea esta información para que los routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente.

La información que el router recibe de los vecinos se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor.

Esta información también se introduce a la tabla de topología. Los routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red (como IP, IPv6 o IPX). La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

5.13.4. TABLA DE ENCAMINAMIENTO

La tabla de encaminamiento EIGRP contiene las mejores rutas hacia un destino. Esta información se recupera de la tabla de topología.

Los routers EIGRP mantienen una tabla de encaminamiento por cada protocolo de red.

5.14. EL PROTOCOLO CONOCIDO COMO "PRIMERO LA RUTA MÁS CORTA" (OSPF)

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

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

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

OSPF ofrece soluciones a los siguientes problemas:

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

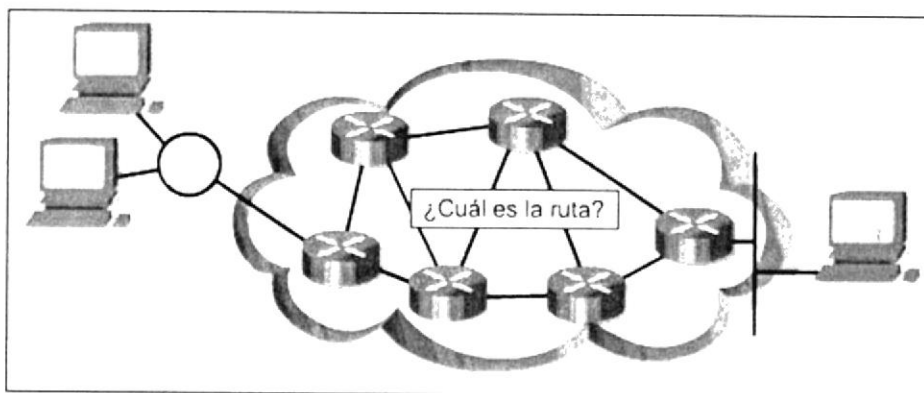


Figura 6.11 OSPF

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

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

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

TIPOS DE ÁREA

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

ÁREA BACKBONE

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

ÁREA STUB

Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento.

Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento. T-so-stubby

ÁREA NOT-SO-STUBBY

También conocidas como NSSA se trata es un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

5.14.1. ESTADOS DE OSPF

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

5.14.2. ESTADO DESACTIVADO (DOWN STATE)

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

5.14.3. ESTADO DE INICIALIZACIÓN (INIT STATE)

Los encaminadores OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los encaminadores vecinos. Cuando una interfaz recibe su primer paquete Hello, el encaminador entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa.

Los dos tipos de relaciones son Dos-Vías y Adyacencia. Un encaminador debe recibir un Hello desde un vecino antes de establecer algún tipo de relación.

5.14.4. ESTADO DE DOS-VÍAS (TWO-WAY)

Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de dos-vías, o comunicación bidireccional, con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen.

Un enrutador ingresa al estado de Dos-Vías cuando se ve a sí mismo en un paquete Hello proveniente de un vecino.

El estado de Dos-Vías es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos.

Para aprender los estados de enlace de otros encaminadores y eventualmente construir una tabla de encaminamiento, cada encaminador OSPF debe formar a lo menos una adyacencia.

Una adyacencia es una relación avanzada entre encaminadores OSPF que involucra una serie de estados progresivos que se basa no tan solo en paquetes Hello, si no que otros 4 paquetes OSPF.

Aquellos encaminadores intentando volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.

5.14.5. ESTADO EXSTART

Técnicamente, cuando un encaminador y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs.

Los dos encaminadores vecinos emplean paquetes Hello para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos.

Aquel encaminador con el mayor router ID "gana" y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.

5.14.6. 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.

5.14.7. 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).

5.14.8. ESTADO DE ADYACENCIA (ADJACENCY)

Cuando el estado de carga ha sido completado, los enrutadores se vuelven completamente adyacentes. Cada enrutador mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

5.15. LISTAS DE CONTROL DE ACCESO (ACL'S)

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

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

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

Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX).

Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router.

El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

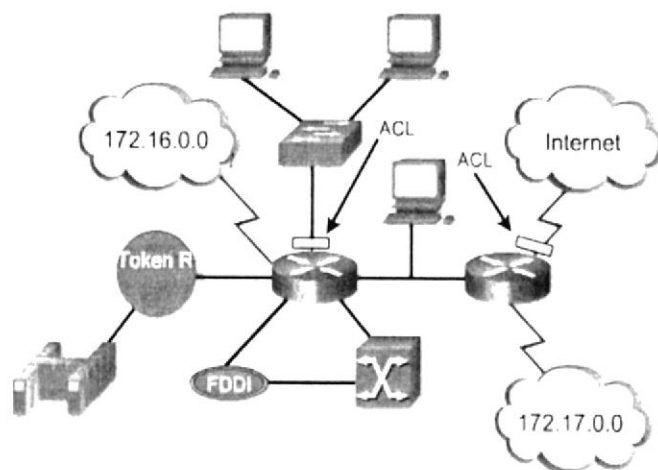


Figura 5-12: ACL'S

5.15.1. FUNCIONAMIENTO DE LAS ACL

El orden en el que se ubican las sentencias de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo.

Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL.

Una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo.

Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican.

Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice deny any (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea deny any no sea visible como última línea de una ACL, está ahí y no permitirá que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada.

Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el deny any al final de las ACL para reforzar la presencia dinámica de la prohibición implícita deny.

5.15.2. CREACIÓN DE LAS ACL

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

Protocolo	Intervalo
IP	1-99, 1300-1999
IP extendido	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX extendido	900-999
Protocolo de publicación de servicio IPX	1000-1099

Tabla 5-1: Clases De Acl's

Después de ingresar al modo de comando apropiado y que se decide el número de tipo de lista, el usuario ingresa sentencias de lista de acceso utilizando el comando access-list, seguida de los parámetros necesarios. Este es el primero de un proceso de dos pasos. El segundo paso consiste en asignar la lista a la interfaz apropiada. En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, usando el comando ip access-group en el modo de configuración de interfaz. Al asignar una ACL a una interfaz, se debe especificar la ubicación entrante o saliente. Después de crear una ACL numerada, se la debe asignar a una interfaz.

5.15.3. FUNCIÓN DE LA MÁSCARA WILDCARD EN UNA ACL

Una máscara wildcard es una cantidad de 32-bits que se divide en cuatro octetos. Una máscara wildcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar como tratar los bits de la dirección IP correspondiente.

Las máscaras wildcard no guardan relación funcional con las máscaras de subred. Se utilizan con distintos propósitos y siguen distintas reglas.

Las máscaras de subred y las máscaras de wildcard representan dos cosas distintas al compararse con una dirección IP. Las máscaras de subred usan unos y ceros binarios para identificar las porciones de red, de subred y de host de una dirección IP.

Las máscaras de wildcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones any y host. Para explicarlo de forma sencilla, la opción any reemplaza la dirección IP con 0.0.0.0 y

la máscara wildcard por 255.255.255.255. Esta opción concuerda con cualquier dirección con la que se la compare.

La máscara 0.0.0.0 reemplaza la opción host. Esta máscara necesita todos los bits de la dirección ACL y la concordancia de dirección del paquete. Esta opción sólo concuerda con una dirección.

5.15.4. ROUTER (CONFIG) #ACCESS-LIST 1 PERMIT 0.0.0.0 255. 255. 255. 255

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

Se la puede escribir como:

Router (config) #access-list 1 permit any

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

Router (config) #access-list 1 permit 192.168.15.15 0.0.0.0

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

Se la puede escribir como:

Router (config) #access-list 1 permit host 192.168.15.15

El ejemplo del párrafo anterior se lo puede resumir con la palabra reservada host, la cual es equivalente a una sola IP (192.168.15.15).

5.15.5. TIPOS DE ACL

5.15.5.1. ACL ESTÁNDAR

En la versión 12.0.1 del IOS de Cisco, se usaron por primera vez números adicionales (1300 al 1999) para las ACL's estándar pudiendo así proveer un máximo posible de 798 ACL's estándar adicionales, a las cuales se les conoce como ACL's IP expandidas. (También entre 1300 y 1999 en IOS recientes)

En la primera sentencia ACL, cabe notar que no hay máscara wildcard. En este caso donde no se ve ninguna lista, se utiliza la máscara por defecto, que es la 0.0.0.0. Esto significa que toda la dirección debe concordar o que esta línea en la ACL no aplica y el router debe buscar una concordancia en la línea siguiente de la ACL.

La sintaxis completa del comando ACL estándar es:

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

El uso de remark facilita el entendimiento de la lista de acceso. Cada remark está limitado a 100 caracteres.

5.15.5.2. ACL EXTENDIDA

Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos y números de puerto. Esto ofrece mayor flexibilidad para establecer que verifica la ACL. Una vez descartados los paquetes, algunos protocolos devuelven un paquete al emisor, indicando que el destino era inalcanzable.

Es posible configurar múltiples sentencias en una sola ACL. Puede haber tanta cantidad de sentencias de condición como sean necesarias, siendo la única limitación la memoria disponible en el router. La sintaxis de una sentencia ACL extendida puede ser muy extensa y a menudo, se vuelve engorrosa en la ventana terminal. Las wildcards también tienen la opción de utilizar las palabras clave host o any en el comando.

Al final de la sentencia de la ACL extendida, se obtiene más precisión con un campo que especifica el Protocolo para el control de la transmisión (TCP) o el número de puerto del Protocolo de datagrama del usuario (UDP).

Las operaciones lógicas pueden especificarse como igual (eq), desigual (neq), mayor a (gt) y menor a (lt) aquellas que efectuarán las ACL extendidas en protocolos específicos. Las ACL extendidas utilizan el número de lista de acceso entre 100 y 199.

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

5.15.6. UBICACIÓN DE UNA ACL

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican las direcciones destino, de modo que se deben colocar lo más cerca posible del destino.

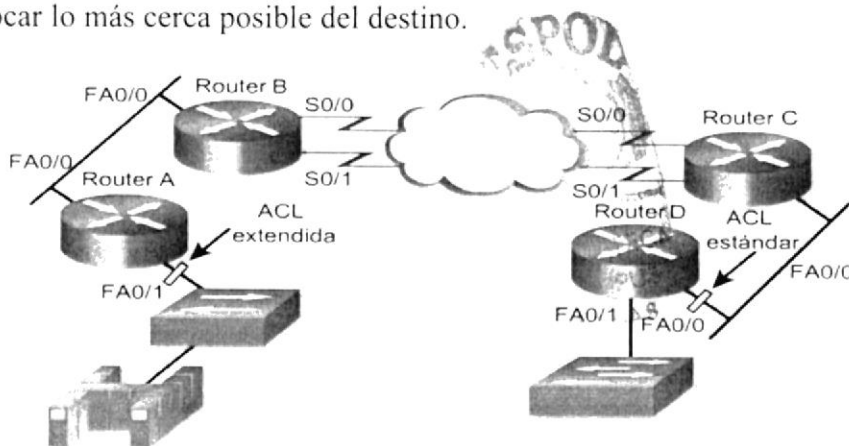


Figura 5.13: Ubicación De Una Acl

5.15.7. PORQUE CREAR UNA ACL

- Limitar el tráfico de red y mejorar el rendimiento de la red.
- Reducir la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Brindar control de flujo de tráfico.

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

5.16. CONEXIONES DE LOS ROUTERS

Para comenzar a trabajar en los routers debe tener conectados los routers y todos sus dispositivos en los cuales va a trabajar.



Figura 5-14 Conexiones De Los Routers

Luego conecta el cable en el puerto de la consola en la parte posterior del router, para comenzar la configuración.

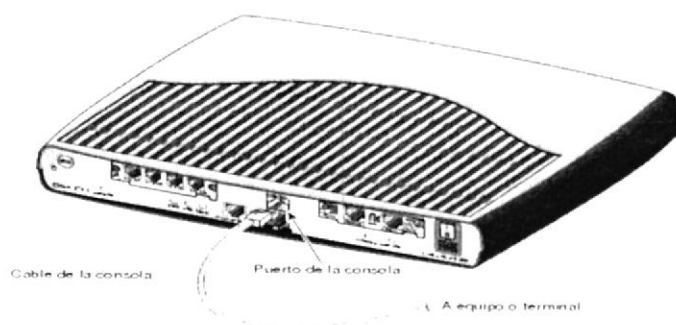


Figura 5-15 Conexiones De Los Routers

5.17. ACCESO A LA APLICACIÓN HYPERTERMINAL

1. En la barra de tareas de Windows seleccionar con el Mouse la opción Inicio

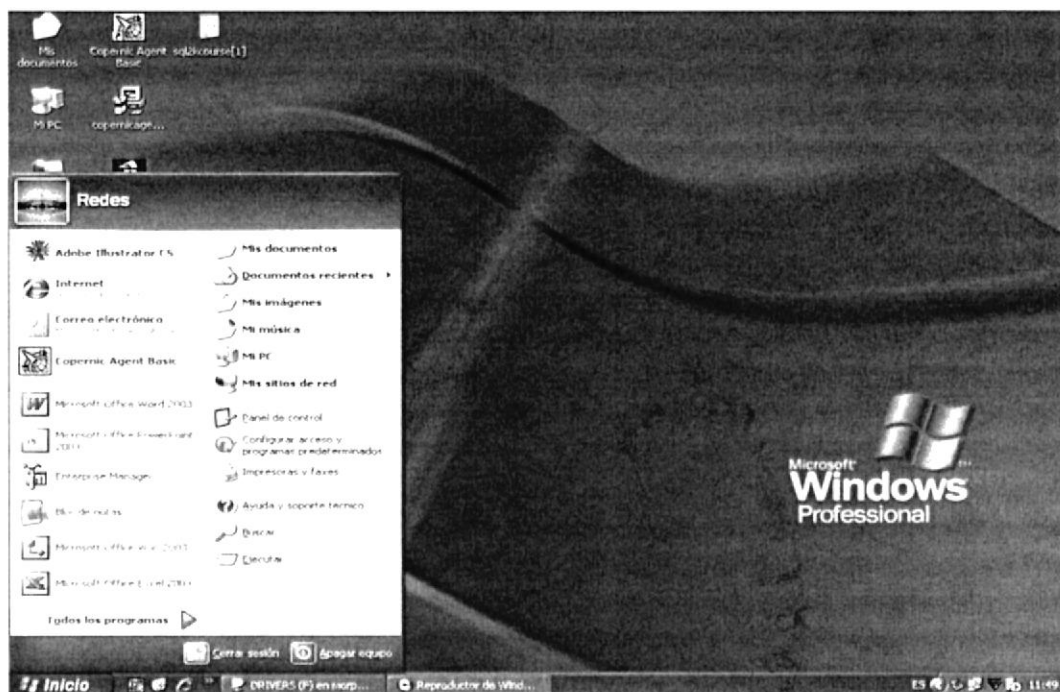


Figura 5-16 Entorno de Windows

2. Se abrirá un menú donde seleccione la opción todos los programas.

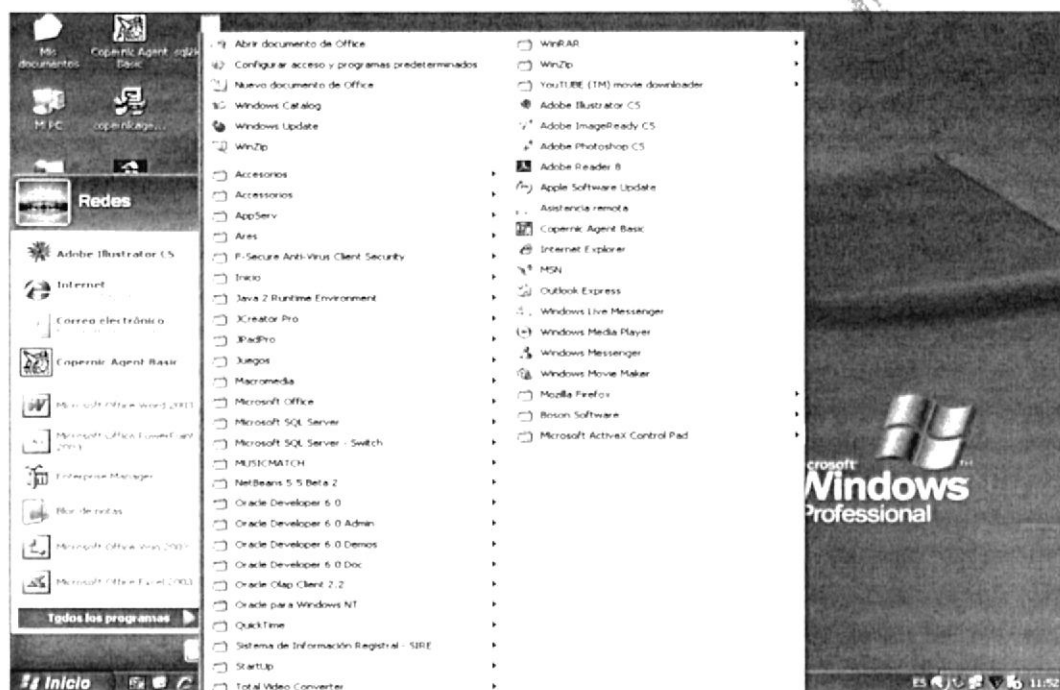


Figura 5-17 Menú inicio

3. Aquí encontrará un acceso directo llamado HyperTerminal, al cual le dará clic y mostrará la siguiente pantalla

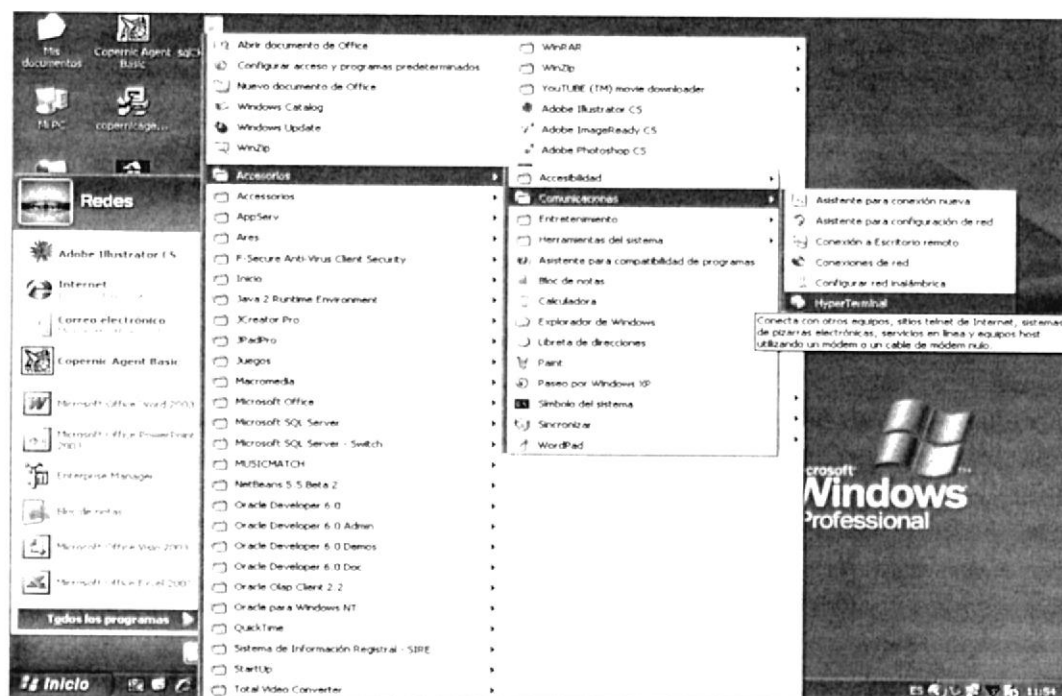


Figura 5-18 Selección de programa (hiperterminal)

4. En el cuadro de texto denominado Nombre se colocará un identificador a la conexión en este caso será Instituto Nacional Galápagos y dará Aceptar, si da clic en el botón Cancelar no existirá ninguna conexión

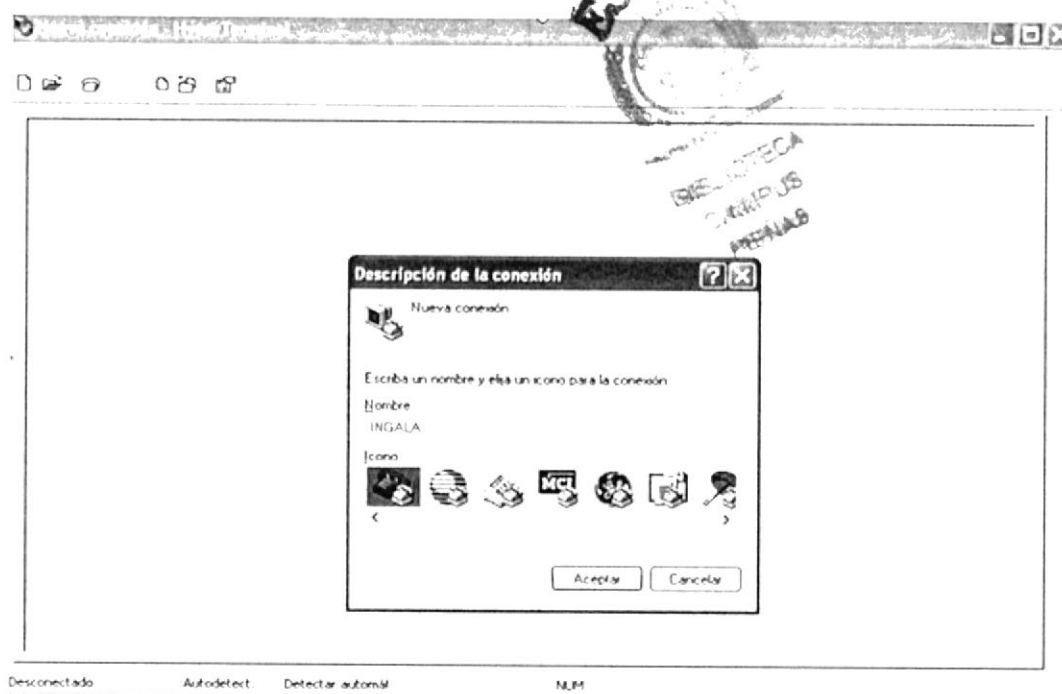


Figura 5-19 Nueva conexión

5. En la siguiente pantalla se pedirá ingresar algunos detalles de conexión como País o región, Código de área, número de teléfono y conectar usando. Las tres primeras no son obligatorias son opcionales mientras que la última opción deberá escoger el puerto del computador al cual se va conectar el router en este caso va ser el puerto COM 1 y da clic en el botón Aceptar

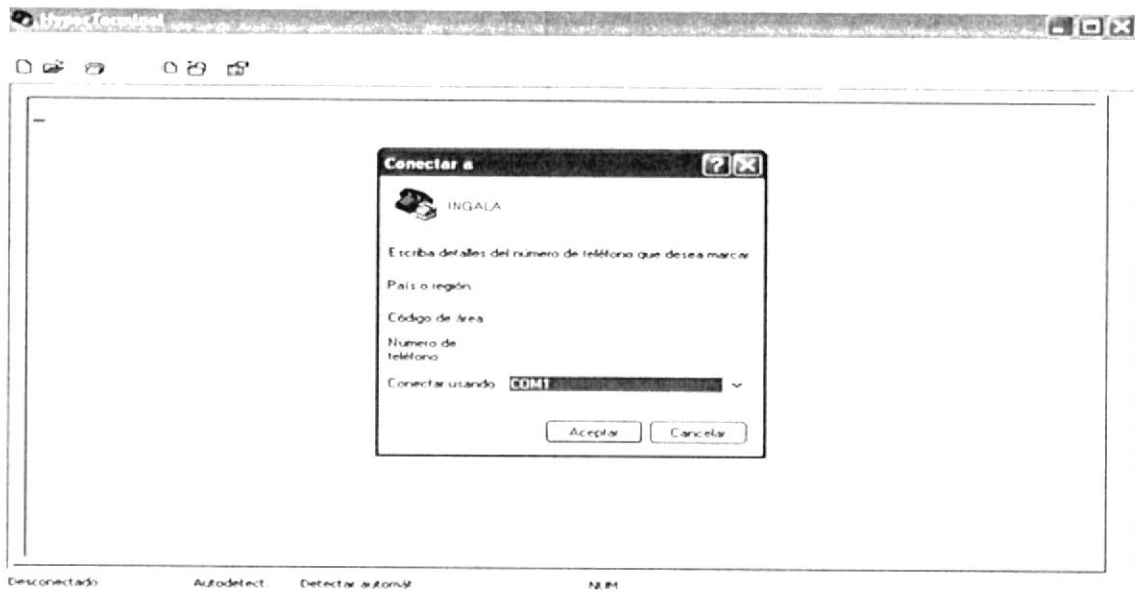


Figura 5-20 Conectar a....

Sugerencia:



Si da clic en el botón Cancelar no habrá terminado de realizar la conexión por consiguiente no se habrá conectado tendiendo un pantalla en blanco

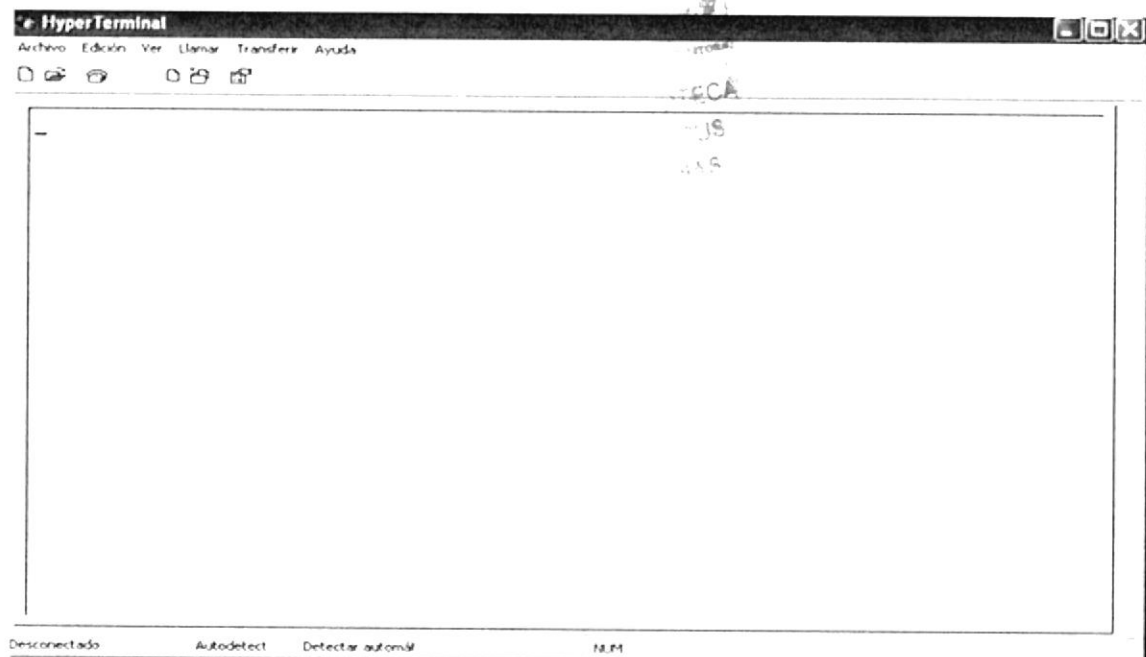


Figura 5-21 Conexión cancelada al router

Sugerencia:

Se los puede establecer al dar clic en el botón **Restaurar predeterminados**

6. En la siguiente pantalla encontrará algunos parámetros de conexión de los cuales deberá establecer y dar clic en el botón Aceptar.
 - a) 9600 bps. (velocidad de transmisión del cable serial de conexión)
 - b) 8 bits de Datos (configuración del procesamiento de datos al pasar al Hyperterminal en bits por segundo)
 - c) Ninguno (paridad) (utilizado para comprobar errores en el grupo de bits de datos transferidos entre uno o varios equipos)
 - d) 1 (bit de parada) (medida de transporte por la que pasan datos al Hyperterminal)
 - e) Ninguno control del flujo (se refiere a la información que viaja)

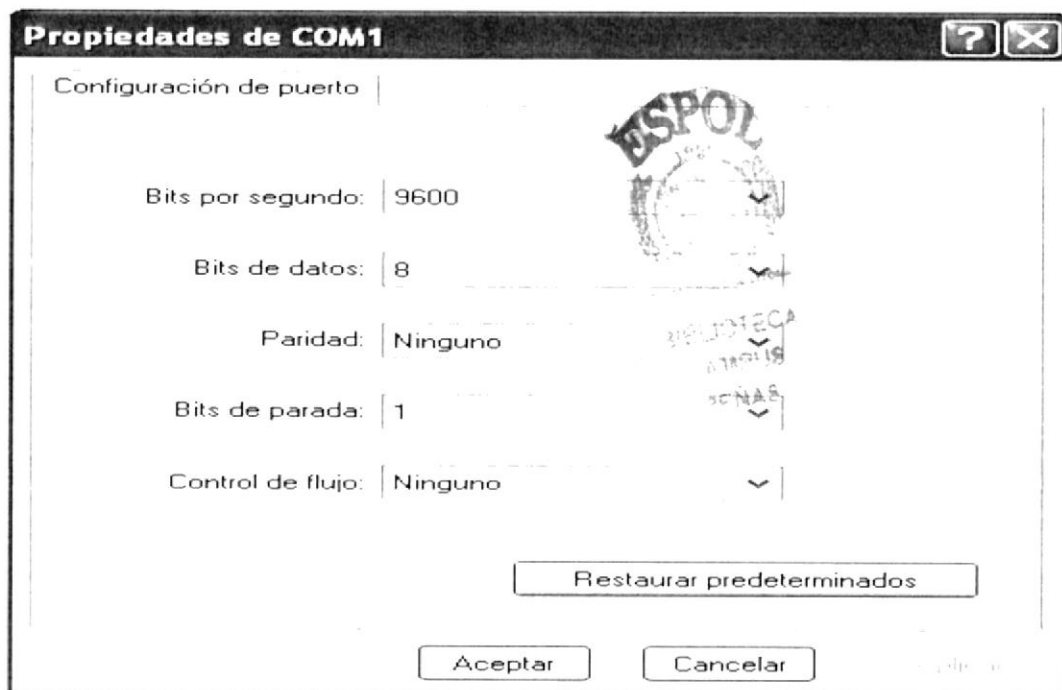


Figura 5-22 Propiedades de com 1

7. Una vez colocado los parámetros dará clic en el botón Aceptar y podrá empezar con la configuración del router a través de la consola Hyperterminal.

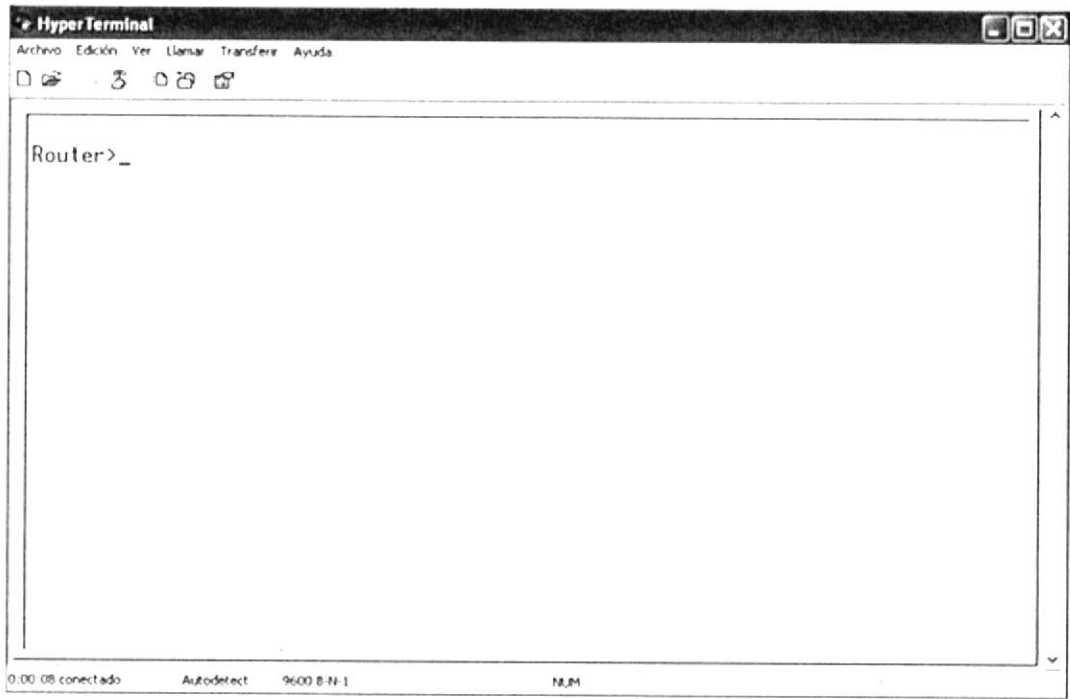


Figura 5-23 Configuración Router

5.18. CONFIGURACIÓN DE ROUTERS

A continuación se va a mostrar el uso de los comandos mas frecuentes usados en los routers:

El comando **enable** permite cambiar de modo de usuario normal a privilegiado (esto se lo puede ver reflejado en el cambio del Prometén donde se verá el cambio del signo mayor > al signo #).

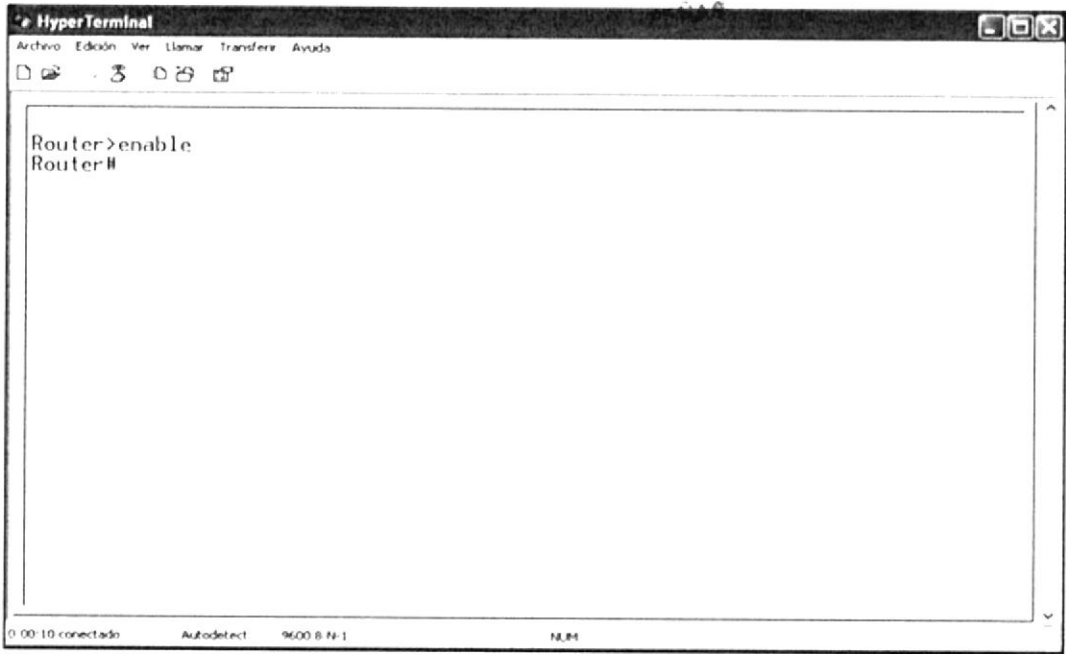
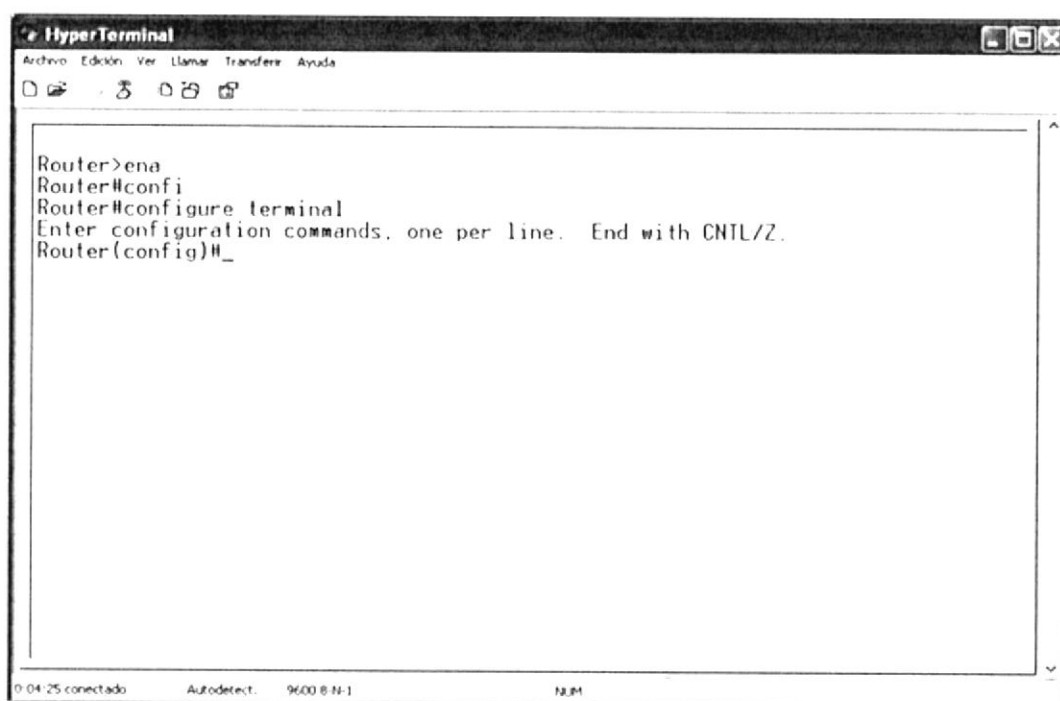


Figura 5-24 Configuración Router

El comando `configure Terminal` permite ingresar al modo configuración global



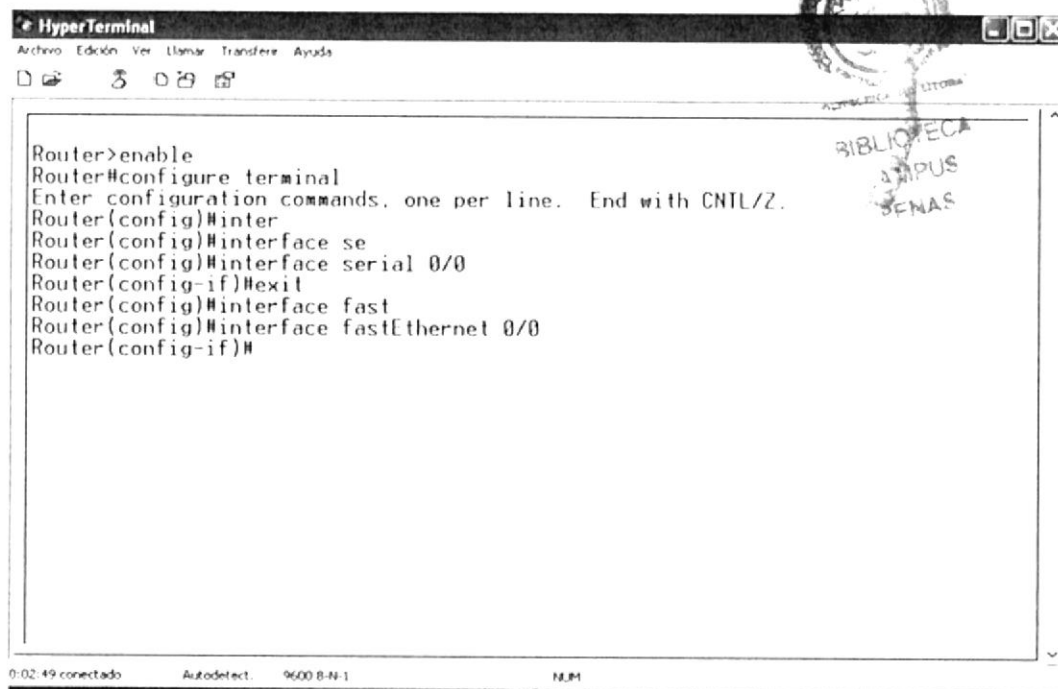
A screenshot of a HyperTerminal window titled "HyperTerminal". The menu bar includes "Archivo", "Edición", "Ver", "Llamar", "Transferir", and "Ayuda". Below the menu is a toolbar with icons for file operations. The main text area shows the following commands and prompts:

```
Router>ena
Router#confi
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#_
```

The status bar at the bottom indicates "0:04:25 conectado", "Autodetect.", "9600 8-N-1", and "NUM".

Figura 5-25 Configuración global

El comando **interface** permite ingresar a la configuración de la interfaz dependiendo del tipo por ejemplo Serial, Ethernet y dependiendo del número de interfaz



A screenshot of a HyperTerminal window titled "HyperTerminal". The menu bar includes "Archivo", "Edición", "Ver", "Llamar", "Transferir", and "Ayuda". Below the menu is a toolbar with icons for file operations. The main text area shows the following commands and prompts:

```
Router>enable
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)#exit
Router(config)#interface fast
Router(config)#interface fastEthernet 0/0
Router(config-if)#
```

The status bar at the bottom indicates "0:02:49 conectado", "Autodetect.", "9600 8-N-1", and "NUM".

Figura 5-26 Configuración Ethernet

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

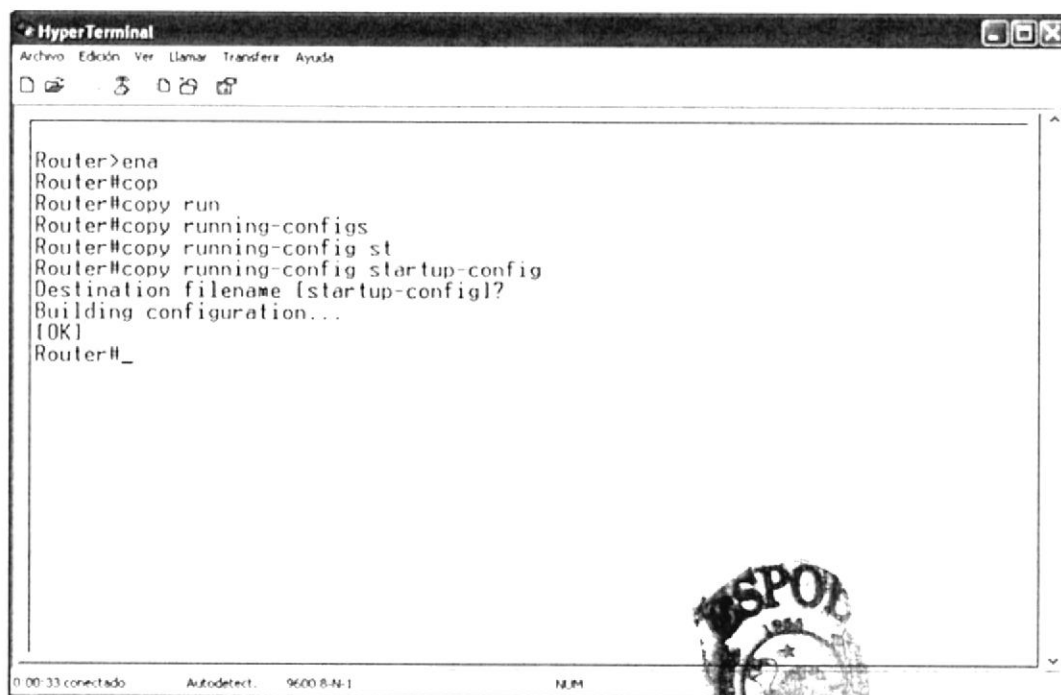


Figura 5-27 Configuración RAM del router

El comando **show running-config** permite ver las direcciones IP que se encuentran o no levantada la interfaz, también se puede reconocer del DCE o DTE dependiendo si tiene o no un **Clock Rate**

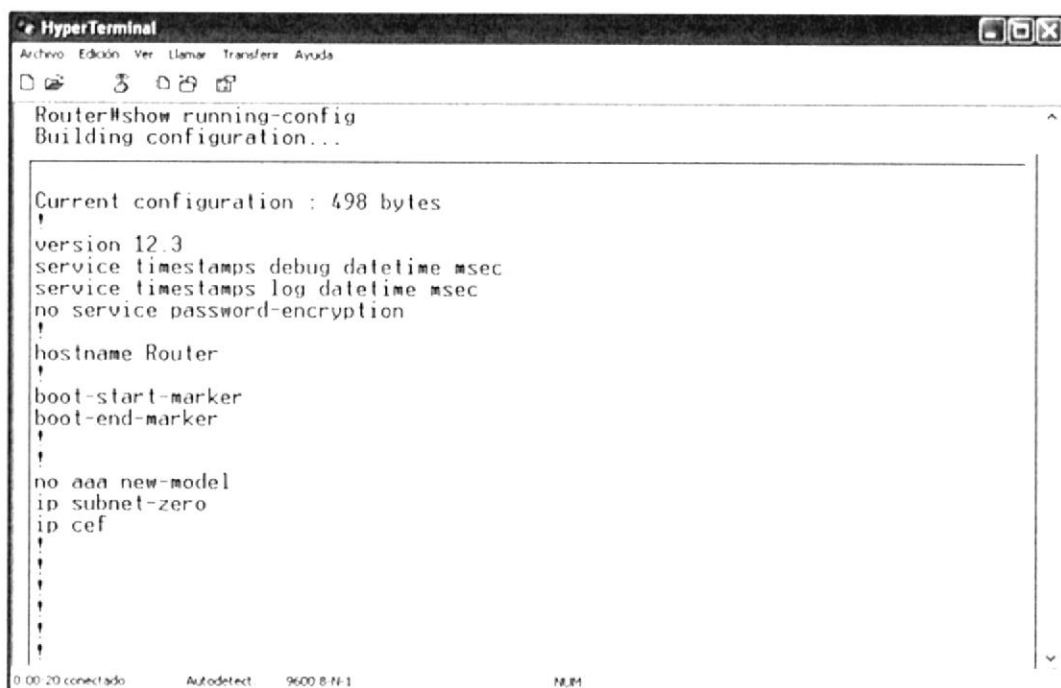
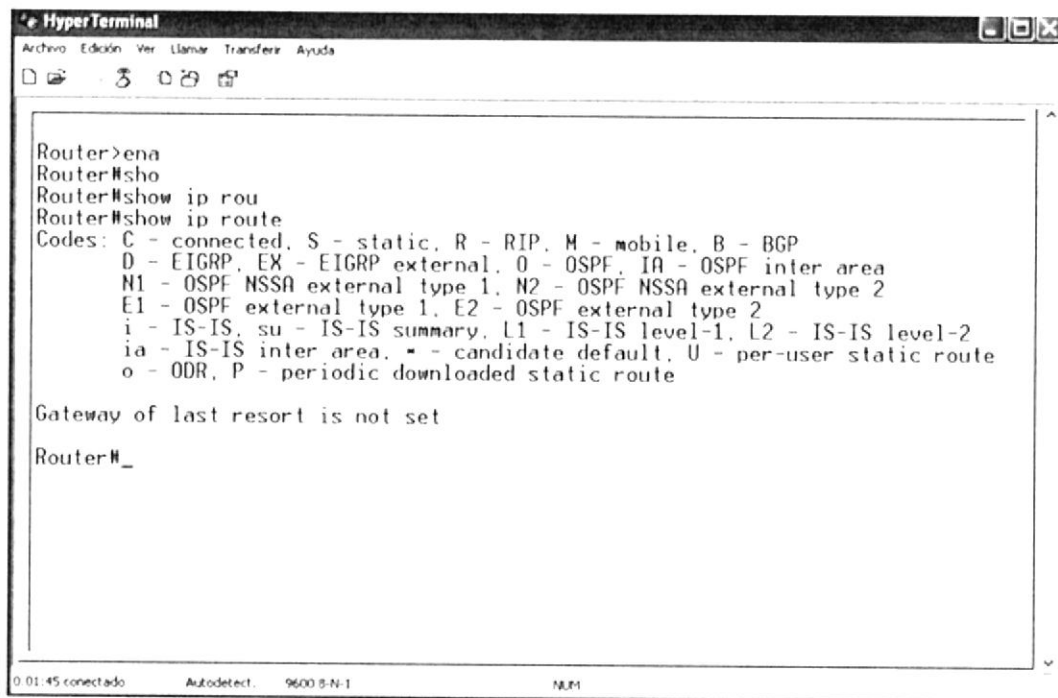


Figura 5-28 Configuración show running-config

El comando show ip route muestra la entrada de las tablas de enrutamiento



```

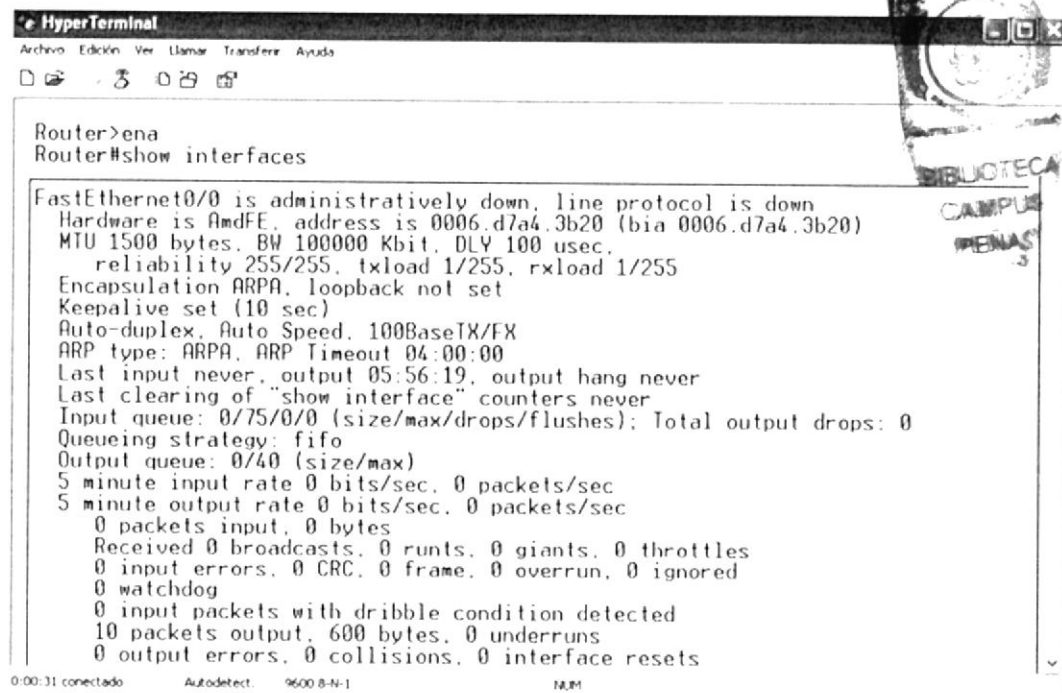
Router>ena
Router#sho
Router#show ip rou
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, 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

Router#_
  
```

Figura 5-29 Configuración comando show ip route

El comando show interfaces muestra el estado de las interfaces



```

Router>ena
Router#show interfaces

FastEthernet0/0 is administratively down, line protocol is down
  Hardware is AmdFE, address is 0006.d7a4.3b20 (bia 0006.d7a4.3b20)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 05:56:19, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    10 packets output, 600 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
  
```

Figura 5-30 Configuración comando show interfaces

El comando **ip address** sirve para asignar la dirección IP (que consta de dirección y de máscara de red) a una interfaz, el comando **no shutdown** sirve para levantar dicha

interfaz cambiará de estado a **Up** pero a su vez si su estado vuelve a cambiar a **Dow** es debido a que la interfaz conectada a la interfaz que levantó no a sido levantada.

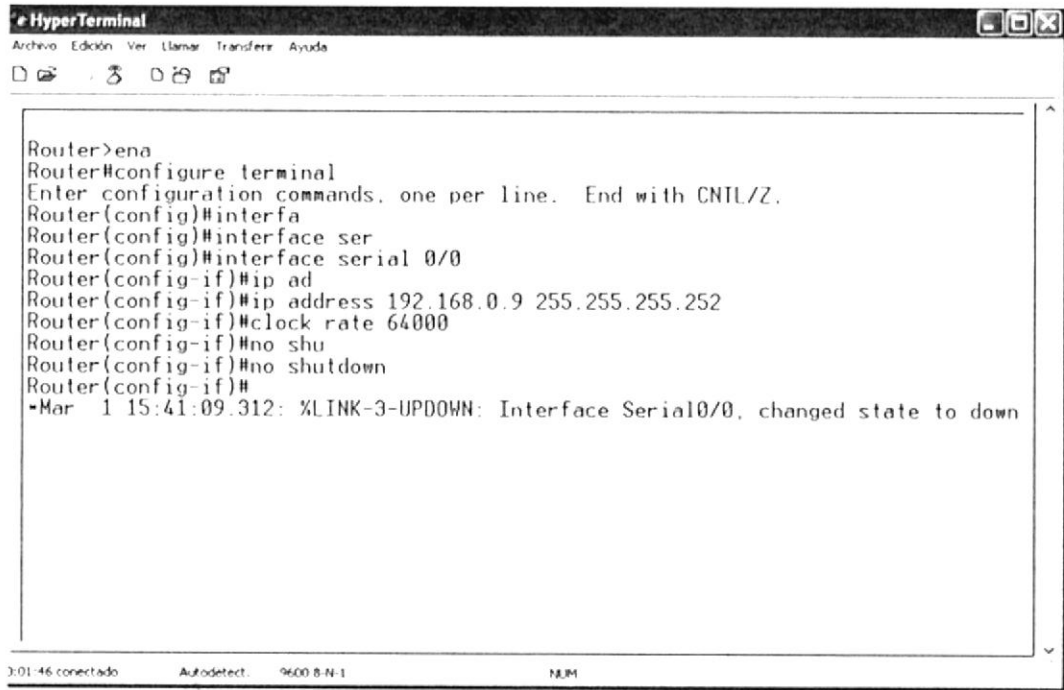


Figura 5-31 Configuración comando ip address

5.18.1. COMANDOS BÁSICOS DE ROUTER

COMANDO	DESCRIPCION
show history	Muestra un historial de los comandos ingresados.
show flash	Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados
show interfaces	Muestra las estadísticas completas de todas las interfaces del router.
show controllers	Ver los enlaces DCE/DTE que usa el router.
show users	Muestra los usuarios conectados al router.
show ip route	Verifica la tabla de enrutamiento.
show version	Despliega la información acerca del router de la imagen de IOS que esté corriendo en la RAM
show ARP	Muestra la tabla ARP del router
show protocols	Muestra el estado global de las interfaces.
show startup-configuration	Muestra el archivo de configuración almacenado en la NVRAM.

show running-configuration	Muestra el contenido del archivo de configuración activo.
configure terminal	Ingreso al modo de configuración global
interface serial	Ingreso al modo de configuración de interfaz serial.
interface fastethernet	Ingreso al modo de configuración de interfaz fastethernet.
ip address	Especifique la dirección de la interfaz y la máscara de subred.
no ip address	Dar de baja a la dirección ip asignada.
clock rate	Fija la velocidad de sincronización.
enable secret	Habilitar la clave en forma encriptada. No se muestra en el show run
enable password	Habilita la clave en forma cifrada.
shutdown	Dar de baja a la interfaz
exit	Salir en forma progresiva.
Ctrl.Z	Salir del modo privilegiado de forma rápida.
wr	Guardar los cambios en la NVRAM de forma rápida.
erase running startup -config	Borrar la configuración activa.
no shutdown	Levanta la interfaz.
line console 0	Comando para ingresar al modo de configuración del puerto consola.
login	Habilita la opción de introducir un usuario.
password [xxx]	Configura el password de acceso.
line vty 0 4	Comando para ingresar al modo de configuración de las terminales virtuales (sesiones telnet).
bandwidth	Configura el parámetro ancho de banda (en Kb) que utilizan los protocolos de enrutamiento en el cálculo de la métrica. No tiene relación real con el.

Tabla 5-2 Comandos Básicos De Router

5.18.2. GUARDAR CAMBIOS DEL ROUTER

Los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en a RAM del router llamado **running – config**.

Para poder ver su contenido se debe ejecutar el comando **show running-config**.

Si se tuviese que reiniciar el router por A o B motivos lo que estaba guardado en el **running-config** se perdería, para evitar eso se hace una copia del **running-config** al **startup-config**. Ello se puede hacer desde el modo Privilegiado con el siguiente comando:

```
Router#copy running-config startup-config
```

Copia de la Configuración actual al archivo de arranque

```
Destination filename [startup-config]?
```

Archivo de destino

```
Building configuration ...
```

Guardando configuración

```
[OK]
```

5.18.3. CONFIGURAR NOMBRES DE LOS ROUTERS

Una de las configuraciones mas básicas es asignar un nombre al router lo cual ayuda a una mejor administración de a red al identificar de manera única los routers dentro de nuestra red.

Esta configuración se la realiza en el modo de configuración Global con el comando **hostname** de la siguiente manera

```
Router>
```

```
Router> enable
```

Acceso al modo privilegiado.

```
Router# configure terminal
```

Entra al modo de configuración global.

```
Router (config) #hostname Matriz
```

Asigna el nombre del Router

```
Matriz (config) #exit
```

Sale de la configuración global.

```
Matriz#
```

5.18.4. CONFIGURACIÓN DE CONTRASEÑAS EN EL ROUTER

Se puede restringir el acceso al router estableciendo contraseñas tanto para la consola como para la terminal.

El **line console 0** debe utilizarse para establecer una contraseña de conexión en el terminal de consola.

El modo de configuración **line vty 0 4** sirve para establecer una contraseña de conexión en sesiones TELNET entrantes.

```
Router# configure terminal
```

Entra al modo de configuración global.

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

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router#conf ter

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

Router (config) #line console 0

consola

Router (config-line) #password cisco

contraseña

Router (config-line) #login

login para la contraseña

Router#conf ter

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

Router (config) #line vty 0 4

terminal virtual

Router (config-line) #password cisco

contraseña

Router (config-line) #login

login para la contraseña

Router (config-line) #enable password cisco

habilitar contraseña

Sugerencia:



Cada password debe tener un mínimo de cuatro caracteres y máximo de ocho caracteres



5.18.5. ASIGNACIÓN DE IP'S A LAS INTERFACES

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 **máscara de subred**.

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

Router# configure terminal

Entra al modo de configuración global.

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

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router (config) #interface serial 0/0

Se ingresa a la interfaz a configurar

Router (config-if) #ip address 192.168.0.9 255.255.255.252

Se asigna la dirección IP y la máscara de subred que es 252 ya que es la dirección de un router

Router (config-if) #clock rate 64000

Velocidad de sincronización con los demás router

Router (config-if) #no shutdown

Comando para levantar la interfaz

%LINK-3-UPDOWN: Interface Serial0/0, changed state to up

Indica la interfaz que se ha levantado

Router (config-if) #

5.18.6. DECLARAR EL PROTOCOLO DE ENRUTAMIENTO (RIP)

Router# configure terminal

Entra al modo de configuración global.

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

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router (config) # router rip

Protocolo a configurar

Router (config-router) #version 2

Version del Protocolo

Router (config-router) #network 192.168.0.8

Red que aprende

5.18.7. PROTOCOLO DE ENRUTAMIENTO (OSPF)

Router# configure terminal

Entra al modo de configuración global.

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

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router (config) # router ospf 1

Protocolo a configurar

Router (config-router) #network 192.168.0.12 0.0.0.3 area 0

Red que aprende con la respectiva wildcard y el área en que se encuentran

Router (config-router) #

5.19. REDISTRIBUCIÓN DE RUTAS

En los esquemas Wan es muy probable tener áreas con protocolos diferentes, en estos casos se aplica lo que se conoce como redistribución de rutas de un protocolo como por ejemplo RIP versión 2 hacia un protocolo diferente como OSPF.

Para poder realizar este proceso se debe ejecutar el comando **redistribuye protocolo** donde protocolo es el protocolo que va a inyectar dentro del que está configurando

Router# configure terminal

Entra al modo de configuración global.

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

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router (config) # router ospf 1

Protocolo a configurar

Router (config-router) #network 192.168.0.12 0.0.0.3 area 0

Red que aprende con la respectiva wilcard y el área en que se encuentran

Router (config-router) #network 192.168.0.20 0.0.0.3 area 0

Red que aprende con la respectiva wilcard y el área en que se encuentran

Router (config-router) #redistribute rip

Redistribución de protocolos

Router (config-router) #exit

Sale de modo configuración global

Router#

Router# configure terminal

Entra al modo de configuración global.

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

Con este comando se comprueba que se ha ingresado al modo de configuración global y que se presiona CTRL+Z para salir.

Router (config) # router rip

Protocolo a configurar

Router (config-router) #version 2

Version del Protocolo

Router (config-router) #network 192.168.0.8

Red que aprende

Router (config-router) #redistribute ospf 1

Redistribución de protocolos

Router (config-router) #exit

Sale de modo configuración global



5.19.1. CASO DE ESTUDIO DEL INSTITUTO NACIONAL GALÁPAGOS

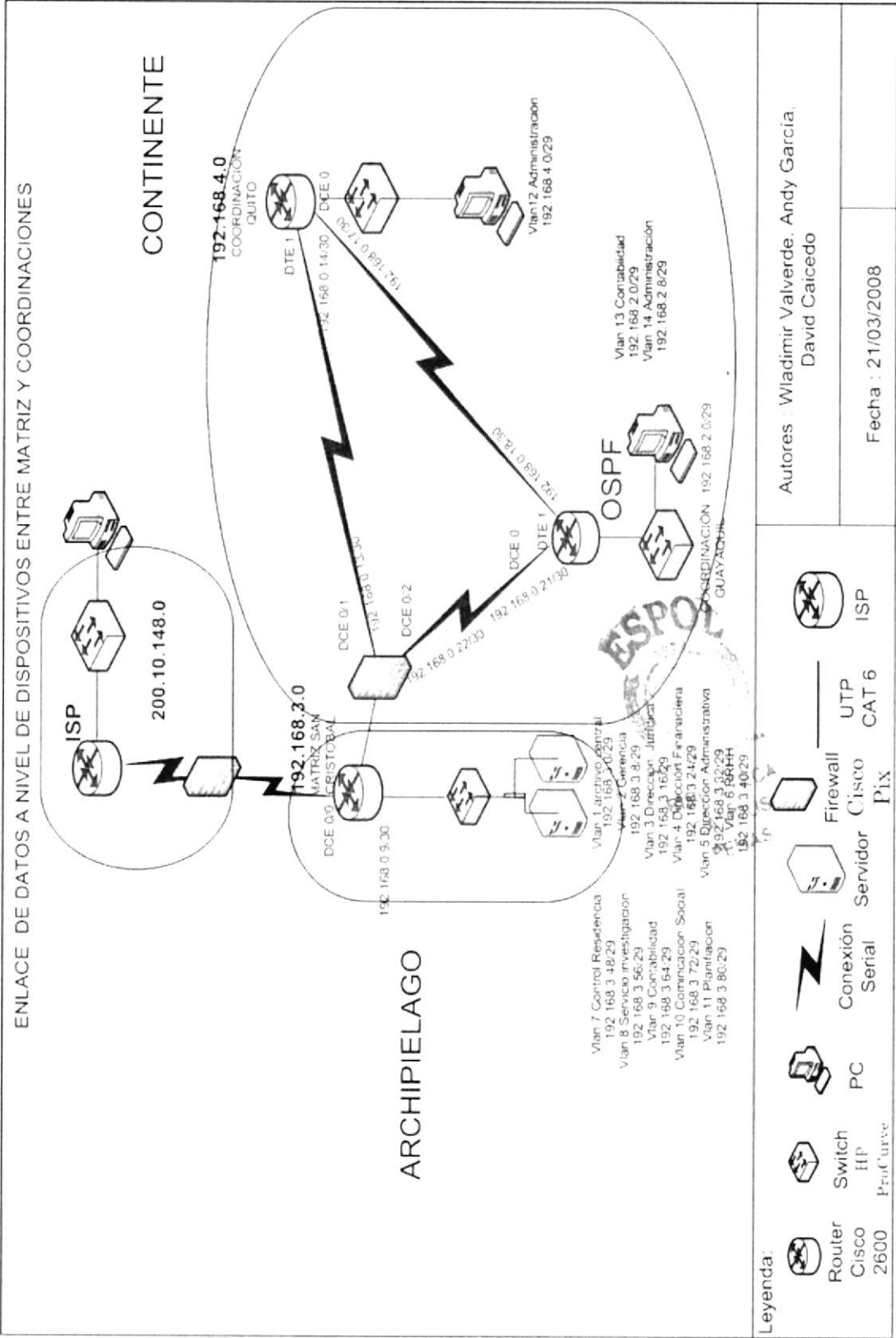


Figura 5-32 Caso De Estudio INGALA

5.20. CONFIGURACIÓN DETALLADAS DE ROUTERS

A continuación se va a pasar a configurar de manera detallada el grafico WAN de los routers Matriz San Cristóbal donde se trabajara con un segmento de red que va a ser 192.168.0.0

Se posse 3 routers en donde 1 router Matriz San Cristóbal es el principal y a su vez se tiene los Router frontera de 2 sucursales se establecerá 1 protocolos de enrutamiento OSPF que será el área dividida por la linea roja

5.21. CONFIGURACIÓN DE ROUTER MATRÍZ SAN CRISTÓBAL

Para un mejor entendimiento, se ha colocado debajo de algunos comandos una breve descripción de los mismos, se reconocerá por que su formato es de color azul.

Acceso al modo de Configuración principal.

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router (config) # exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router (config) #hostname Matriz

Sirve para asignarle un nombre al router (Matriz)

Matriz (config) #

Creación de Contraseñas

Matriz#enable

Ingresar al modo EXEC privilegiado

Matriz#configure terminal

Ingresar al modo de configuración global

Matriz (config) #

Matriz (config) #line console 0

Ingresar a configurar la consola

Matriz (config-line) #password cisco

Asignar una contraseña a la consola

Matriz (config-line) #login

Petición de contraseña

Matriz (config-line) #exit

Salir de la configuración de la consola

Matriz (config) #line vty 0 4



Ingresar a configurar la Terminal virtual

Matríz (config-line) #password cisco

Asignar una contraseña a la Terminal virtual

Matríz (config-line) #login

Petición de contraseña

Matríz (config-line) #exit

Salir de la configuración de la Terminal virtual**Configuración de las Interfaces.**

Matríz (config) #interface FastEthernet 1/0

Ingresar a la interfaz que se va a configurar

Matríz (config-if) #ip address 192.168.0.16 255.255.255.248

Asignar una dirección ip con su respectiva máscara

Matríz (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Matríz (config-if) #exit

Salir de la configuración de la interfaz

Matríz (config) #interface serial 0/0

Ingresar a la interfaz que se va a configurar

Matríz (config-if) #ip address 192.168.0.9 255.255.255.252

Asignar una dirección ip con su respectiva máscara

Matríz (config-if) #clock rate 64000

Asignar el valor para el sincronizador del reloj

Matríz (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Matríz (config-if) #exit

Salir de la configuración de la interfaz

Matríz (config) #interface serial 0/1

Ingresar a la interfaz que se va a configurar

Matríz (config-if) #ip address 192.168.0.13 255.255.255.252

Asignar una dirección ip con su respectiva máscara

Matríz (config-if) #clock rate 64000

Asignar el valor para el sincronizador del reloj

Matríz (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Matríz (config-if) #exit

Salir de la configuración de la interfaz

Matríz (config) #interface serial 0/2

Ingresar a la interfaz que se va a configurar

Matríz (config-if) #ip address 192.168.0.22 255.255.255.252

Asignar una dirección ip con su respectiva máscara

Matríz (config-if) #clock rate 64000

Asignar el valor para el sincronizador del reloj

Matríz (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Matríz (config-if) #exit

Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento RIPv2 y de distribución de Rutas por OSPF

Matríz#configure terminal

Ingresar al modo de configuración global

Matríz (config) #router rip

Habilitar el protocolo de enrutamiento a configurar

Matríz (config-router) #version 2

Asignar la versión del protocolo ya asignado

Matríz (config-router) #network 192.168.0.8

Asignar la dirección de la red

Matríz (config-router) #default-metric 10

Asignar 1 métrica para que se enruten los paquetes desde ospf.

Matríz (config-router) # redistribute ospf 1

Distribuir rip hacia las redes ospf

Matríz (config-router) #exit

Salir de la configuración del protocolo de enrutamiento

Matríz (config) #

Para deshabilitar el Protocolo de enrutamiento RIP se utilizar el comando “no router rip”.

Matríz#configure terminal

Ingresar al modo de configuración global

Matríz (config) #no router rip

Desactiva el protocolo de enrutamiento rip

Matríz (config) #

Configuración de Protocolo de Enrutamiento OSPF y de distribución de Rutas por RIPv2

Matríz#configure terminal

Ingresar al modo de configuración global

Matríz (config) #router ospf 1

Habilitar el protocolo de enrutamiento a configurar

Matríz (config-router) #network 192.168.0.12 0.0.0.3 area 0

Matríz (config-router) #network 192.168.0.16 0.0.0.3 area 0

Matríz (config-router) #network 192.168.0.20 0.0.0.3 area 0

Matríz (config-router) #network 192.168.2.0 0.0.0.7 área 0

Matríz (config-router) #network 192.168.2.8.0.0.7 área 0

Matríz (config-router) #network 192.168.3.0 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.8 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.16 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.24 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.32 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.40 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.48 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.56 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.64 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.72 0.0.0.7 área 0

Matríz (config-router) #network 192.168.3.0.80.0.0.7 área 0

Asignar la dirección de la red, wildcard y área respectiva

Matríz (config-router) # redistribute rip subnets

Distribuye protocolo ospf hacia las subredes de rip

Matríz (config-router) #exit

Salir de la configuración del protocolo de enrutamiento

Matríz (config) #

Para deshabilitar el Protocolo de enrutamiento OSPF se utilizar el comando “no router ospf 1”.

Matríz#configure terminal

Ingresar al modo de configuración global

Matríz (config) #no router ospf 1

Desactiva el protocolo de enrutamiento rip

Matríz (config) #

5.21.1. GUARDAR CONFIGURACIÓN

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

Matríz#copy running-config startup-config

Guardar una copia de la configuración a la NVRAM

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

Configuración de Listas de Acceso

Bloquear toda la subred 192.168.3.0/29, excepto el servidor con la siguiente ip 192.168.3.3

Matríz #configure terminal

Ingresar al modo de configuración global

Matríz (config) # access-list 1 permit host 192.168.3.3

Asignar permiso a un host específico

Matríz (config) # access-list 1 deny 192.168.3.0 0.0.0.7

Negar el acceso a la red a las demás ip's

Matríz (config) # access-list 1 permit any

Colocar una línea implícita para ésta acl

Matríz (config) # exit

Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

Matríz# configure terminal

Ingresar al modo de configuración global

Matríz (config) # interface fast-Ethernet 1/0

Ingresar a la interfaz que se va a asignar la acl

Matríz (config) # ip access-group 1 in

Levantar la acl de manera entrante

ACL extendida

Matríz# configure terminal

Ingresar al modo de configuración global

Matríz (config) # access-list 101 permit ip host 192.168.3.10 host 192.168.3.3

Asignar permiso a un host específico

Matríz_Guayaquil (config) #access-list101deny ip192.168.3.00.0.0.0.31host
192.168.3.3

Negar el acceso a la red a las demás ip's

Matríz (config) # access-list 101 permit ip any any

Colocar una línea implícita para ésta acl

Matríz (config) # exit

Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

Matríz#configure terminal

Ingresar al modo de configuración global

Matríz (config) # interface fast-Ethernet 1/0

Ingresar a la interfaz que se va a asignar la acl

Matríz (config) # ip access-group 101 in

Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.0.3.

Matríz# configure terminal

Ingresar al modo de configuración global

Matríz (config) # access-list 120 permit tcp host 192.168.3.10 host 192.168.3.3 any eq
telnet

Ingresar a la interfaz que se va a asignar la acl

Matríz (config) #access-list 120 deny any any

Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

Matríz# configure terminal

Ingresar al modo de configuración global

Matríz (config) # interface fast-Ethernet 1/0

Ingresar a la interfaz que se va a asignar la acl

Matríz (config) # ip access-group 101 in

Levantar la acl de manera entrante

SHOW RUN

Matríz#show running-config

**Muestra el contenido del archivo de configuración activo o la configuración
para una interfaz específica o información de un map class.**

Version 12.1

Versión del Sistema Operativo del Router

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

Servicio de encriptación de contraseña no esta activo

!hostname Matriz
enable password cisco
!
ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!!
interface Serial0/0
Tipo de Interfaz
ip address 192.168.0.9 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast
clock rate 64000

Indica la velocidad del puerto en bits por segundo Lo encuentra en la DCE.

bandwidth 1544
!

interface Serial0/1

Tipo de Interfaz

ip address 192.168.0.13 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast
clock rate 64000

Indica la velocidad del puerto en bits por segundo Lo encuentra en la DCE.

bandwidth 1544
!

interface Serial0/2

Tipo de Interfaz

ip address 192.168.0.22 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast
clock rate 64000

Indica la velocidad del puerto en bits por segundo Lo encuentra en la DCE.

bandwidth 1544
!

interface Serial0/3

Tipo de la interfaz

no ip address

Esto significa que no tiene ninguna ip asignada

no ip directed-broadcast
bandwidth 1544
shutdown

Esto describe el estado de la interfaz, Up(Levantada) o Down (Caída)

interface FastEthernet1/0

Tipo de la interfaz

ip address 192.168.0.25 255.255.255.248

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast

bandwidth 100000

router rip

Protocolo de Enrutamiento

version 2

Versión del protocolo de Enrutamiento

redistribute OSPF 1

Distribuye protocolo rip hacia las redes ospf

network 192.168.0.0

Redes configuradas con el protocolo de Enrutamiento Rip

default-metric 10

Métrica para el enrutamiento de paquetes de ospf a rip

!

router ospf 1

Protocolo de Enrutamiento

redistribute RIP

Distribuye protocolo ospf hacia las subredes rip

network 192.168.0.12 0.0.0.3 area 0

network 192.168.0.16 0.0.0.3 area 0

network 192.168.0.20 0.0.0.3 area 0

network 192.168.2.0 0.0.0.7 área 0

network 192.168.2.8.0.0.0.7 área 0

network 192.168.3.0 0.0.0.7 área 0

network 192.168.3.8 0.0.0.7 área 0

network 192.168.3.16 0.0.0.7 área 0

network 192.168.3.24 0.0.0.7 área 0

network 192.168.3.32 0.0.0.7 área 0

network 192.168.3.40 0.0.0.7 área 0

network 192.168.3.48 0.0.0.7 área 0

network 192.168.3.56 0.0.0.7 área 0

network 192.168.3.64 0.0.0.7 área 0

network 192.168.3.72 0.0.0.7 área 0

network 192.168.3.0.80.0.0.7 área 0

**Redes configuradas con el protocolo de Enrutamiento Ospf**

ip classless

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

banner motd ^C

Indica el mensaje de Bienvenida del Router

Bienvenido al Router Matriz

^C

no ip http server

line con 0

login

transport input none

password cisco

Contraseña para línea de comandos

```
line aux 0
line vty 0 4
login
password cisco
```

Contraseña para Telnet

```
no scheduler allocate
end
```

SHOW IP ROUTE

Matriz#show ip route

C.-Conectado.

S.- Estático.

I.- Protocolo IGRP.

R. - Protocolo Rip.

B. - Protocolo BGP.

D. - Protocolo EIGRP.

EX. – Protocolo EIGRP externo.

O.- Protocolo OSPF.

IA.- El número de las rutas recibidas de otras áreas del OSPF.

E1.- Rutas recibidas de otras áreas del OSPF tipo externo 1.

E2.- Rutas recibidas de otras áreas del OSPF tipo externo 2.

i.- Son las rutas recibidas de los anuncios del protocolo del IS-IS.

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

Descripción de Protocolos usados

Gateway of last resort is not set

Conectada Directamente	Red con la que esta conectada			Interfaz
C	192.168.0.24/29 is directly connected,			FastEthernet1/0
Protocolo Rip	Red aprendida por Rip	Distancia administrativa y ancho de banda	Ip asignada a la interfaz	interfaz
R	192.168.0.32/29	[120/11] via	192.168.0.10, 00:06:40,	Serial0/0
Protocolo ospf	Red aprendida por ospf	Distancia administrativa y ancho de banda	Ip asignada a la interfaz	Interfaz
O	192.168.0.16/30	[110/64] via	192.168.0.17, 01:32:14,	FastEthernet1/0
	192.168.0.0/0 is variably subnetted, 8 subnets			
C	192.168.0.24/29 is directly connected, FastEthernet1/0			
C	192.168.0.8/30 is directly connected, Serial0/0			
R	192.168.0.32/29 [120/1] via 192.168.0.10, 00:06:40, Serial0/0			

C 192.168.0.12/30 is directly connected, Serial0/1
C 192.168.0.20/30 is directly connected, Serial0/2
O 192.168.0.16/30 [110/64] via 192.168.0.17, 01:32:14, FastEthernet1/0
O 192.168.0.48/29 [110/64] via 192.168.0.49, 01:32:59, FastEthernet1/0
O 192.168.0.40/29 [110/64] via 192.168.0.41, 01:28:04, FastEthernet1/0

5.22. CONFIGURACIÓN DE ROUTER GUAYAQUIL

Para un mejor entendimiento, se ha colocado debajo de algunos comandos una breve descripción de los mismos, se reconocerá por que su formato es de color azul.

Acceso al modo de Configuración principal.

Router>enable
 Ingresar al modo EXEC privilegiado
Router#configure terminal
 Ingresar al modo de configuración global
Router (config) # exit
 Salir un nivel
Router#

Configuración de los nombres de los Routers

Router>enable
 Ingresar al modo EXEC privilegiado
Router#configure terminal
 Ingresar al modo de configuración global
Router (config) #hostname Guayaquil
 Sirve para asignarle un nombre al router (Guayaquil)
Guayaquil (config) #

Creación de Contraseñas

Guayaquil #enable
 Ingresar al modo EXEC privilegiado
Guayaquil #configure terminal
 Ingresar al modo de configuración global
Guayaquil (config) #
Guayaquil (config) #line console 0
 Ingresar a configurar la consola
Guayaquil (config-line) #password cisco
 Asignar una contraseña a la consola
Guayaquil (config-line) #login
 Petición de contraseña
Guayaquil (config-line) #exit
 Salir de la configuración de la consola

Guayaquil (config) #line vty 0 4
 Ingresar a configurar la Terminal virtual
Guayaquil (config-line) #password cisco

Asignar una contraseña a la Terminal virtual

Guayaquil (config-line) #login

Petición de contraseña

Guayaquil (config-line) #exit

Salir de la configuración de la Terminal virtual**Configuración de las Interfaces.**

Guayaquil (config) #interface FastEthernet 0/0

Ingresar a la interfaz que se va a configurar

Guayaquil (config-if) #ip address 192.168.0.32 255.255.255.248

Asignar una dirección ip con su respectiva máscara

Guayaquil (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Guayaquil (config-if) #exit

Salir de la configuración de la interfaz

Guayaquil (config) #interface serial 1

Ingresar a la interfaz que se va a configurar

Guayaquil (config-if) #ip address 192.168.0.10 255.255.255.252

Asignar una dirección ip con su respectiva máscara

Guayaquil (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Guayaquil (config-if) #exit

Salir de la configuración de la interfaz**Configuración de Protocolo de Enrutamiento RIPv2**

Guayaquil #configure terminal

Ingresar al modo de configuración global

Guayaquil (config) #router rip

Habilitar el protocolo de enrutamiento a configurar

Guayaquil (config-router) #version 2

Asignar la versión del protocolo ya asignado

Guayaquil (config-router) #network 192.168.0.8

Guayaquil (config-router) #network 192.168.1.0

Asignar la dirección de la red

Guayaquil (config-router) #default-metric 10

Asignar 1 métrica para que se enruten los paquetes desde ospf.

Guayaquil (config-router) #exit

Salir de la configuración del protocolo de enrutamiento

Guayaquil (config) #

Para deshabilitar el Protocolo de enrutamiento RIP se utilizar el comando “no router rip”.

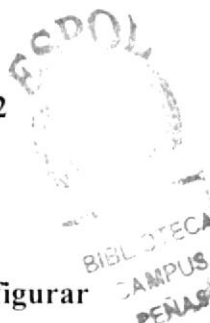
Guayaquil #configure terminal

Ingresar al modo de configuración global

Guayaquil (config) #no router rip

Desactiva el protocolo de enrutamiento rip

Guayaquil (config) #



5.22.1. GUARDAR CONFIGURACIÓN

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

Guayaquil #copy running-config startup-config

Guardar una copia de la configuración a la NVRAM

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

SHOW RUN

Guayaquil #show running-config

Muestra el contenido del archivo de configuración activo o la configuración para Una interfaz específica o información de un map class.

Version 12.1

Versión del Sistema Operativo del Router

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

Servicio de encriptación de contraseña no esta activo

!
hostname Guayaquil
enable password cisco
!
ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!
interface Serial0
Tipo de Interfaz
no ip address
Esto significa que no tiene ninguna ip asignada
no ip directed-broadcast
bandwidth 1544
shutdown

Esto describe el estado de la interfaz, Up(Levantada) o Down (Caída)

!
interface Serial1
Tipo de Interfaz
ip address 192.168.0.10 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast
bandwidth 1544



!
interface FastEthernet0/0

Tipo de la interfaz

ip address 192.168.0.33 255.255.255.248

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast
bandwidth 100000

!
interface Bri0
no ip address
no ip directed-broadcast
shutdown

!
!
router rip

Protocolo de Enrutamiento

version 2

Versión del protocolo de Enrutamiento

network 192.168.0.0

Redes configuradas con el protocolo de Enrutamiento Rip

ip classless

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

no ip http server

!
banner motd ^C

Indica el mensaje de Bienvenida del Router

Bienvenido al Router HcdGuayaquil Babahoyo

^C

line con 0
transport input none
password cisco

Contraseña para línea de comandos

line aux 0
line vty 0 4
login
password cisco

Contraseña para Telnet

!
no scheduler allocate
end

SHOW IP ROUTE

Guayaquil #show ip route

C.-Conectado.

S.- Estático.

I.- Protocolo IGRP.

R. - Protocolo Rip.



- B. - Protocolo BGP.
- D. - Protocolo EIGRP.
- EX. – Protocolo EIGRP externo.
- O.- Protocolo OSPF.
- IA.- El número de las rutas recibidas de otras áreas del OSPF.
- E1.- Rutas recibidas de otras áreas del OSPF tipo externo 1.
- E2.- Rutas recibidas de otras áreas del OSPF tipo externo 2.
- i.- Son las rutas recibidas de los anuncios del protocolo del IS-IS.

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

Descripción de Protocolos usados

Gateway of last resort is not set

Conectada directamente		Red con la que esta conectada		Interfaz
C		192.168.0.8/30 is directly connected,		Serial1
Protocolo Rip	Red aprendida por Rip	Distancia administrativa y ancho de banda	Ip asignada a la interfaz	interfaz
R	192.168.0.12/30	[120/1] via 192.168.0.10, 00:09:25,		Serial1
192.168.0.0/0 is variably subnetted, 5 subnets				
C	192.168.0.8/30 is directly connected,	Serial1		
C	192.168.0.32/29 is directly connected,	FastEthernet0/0		
R	192.168.0.12/30 [120/1] via 192.168.0.9, 00:09:25,	Serial1		
R	192.168.0.20/30 [120/1] via 192.168.0.9, 00:01:44,	Serial1		
R	192.168.0.24/29 [120/1] via 192.168.0.9, 00:05:16,	Serial1		

5.23. CONFIGURACIÓN DE ROUTER QUITO

Para un mejor entendimiento, se ha colocado debajo de algunos comandos una breve descripción de los mismos, se reconocerá por que su formato es de color azul.

Acceso al modo de Configuración principal.

Router>enable

Ingresa al modo EXEC privilegiado

Router#configure terminal

Ingresa al modo de configuración global

Router (config) # exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router (config) #hostname Quito

Sirve para asignarle un nombre al router (Quito)

Quito (config) #

Creación de Contraseñas

Quito #enable

Ingresar al modo EXEC privilegiado

Quito #configure terminal

Ingresar al modo de configuración global

Quito (config) #

Quito (config) #line console 0

Ingresar a configurar la consola

Quito (config-line) #password cisco

Asignar una contraseña a la consola

Quito (config-line) #login

Peticion de contraseña

Quito (config-line) #exit

Salir de la configuración de la consola

Quito (config) #line vty 0 4

Ingresar a configurar la Terminal virtual

Quito (config-line) #password cisco

Asignar una contraseña a la Terminal virtual

Quito (config-line) #login

Peticion de contraseña

Quito (config-line) #exit

Salir de la configuración de la Terminal virtual



Configuración de las Interfaces.

Quito (config) #interface FastEthernet 0/0

Ingresar a la interfaz que se va a configurar

Quito (config-if) #ip address 192.168.0.49 255.255.255.248

Asignar una dirección ip con su respectiva máscara

Quito (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Quito (config-if) #exit

Salir de la configuración de la interfaz

Quito (config) #interface serial 1

Ingresar a la interfaz que se va a configurar

Quito (config-if) #ip address 192.168.0.14 255.255.255.252

Asignar una dirección ip con su respectiva máscara

Quito (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Quito (config-if) #exit

Salir de la configuración de la interfaz

Quito (config) #interface serial 0

Ingresar a la interfaz que se va a configurar

Quito (config-if) #ip address 192.168.0.17 255.255.255.252

Asignar una dirección ip con su respectiva máscara

Quito (config-if) #clock rate 64000

Asignar el valor para el sincronizador del reloj

Quito (config-if) #no shutdown

Habilitar la interfaz para que pueda funcionar

Quito (config-if) #exit

Configuración de Protocolo de Enrutamiento OSPF

Quito #configure terminal

Ingresar al modo de configuración global

Quito (config) #router ospf 1

Habilitar el protocolo de enrutamiento a configurar

Quito (config-router) #network 192.168.0.12 0.0.0.3 area 0

Quito (config-router) #network 192.168.0.16 0.0.0.3 area 0

Quito (config-router) #network 192.168.4.0 0.0.0.7 area 0

Asignar la dirección de la red, wildcard y área respectiva

Quito (config-router) #exit

Salir de la configuración del protocolo de enrutamiento

Quito (config) #

Para deshabilitar el Protocolo de enrutamiento OSPF se utilizar el comando “no router ospf 1”.

Quito #configure terminal

Ingresar al modo de configuración global

Quito (config) #no router ospf 1

Desactiva el protocolo de enrutamiento rip

Quito (config) #

**5.23.1. GUARDAR CONFIGURACIÓN**

Al igual que un PC convencional los routers se pueden ver afectados por problemas en el fluido eléctrico, cuando sucede esto todos los cambios que se hayan efectuado en el router (y que no se hayan guardado) se perderán. Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

Quito #copy running-config startup-config

Guardar una copia de la configuración a la NVRAM

Lo que se le indica al router con esta instrucción es que el contenido del archivo running-config se copie en el startup-config.

El archivo running-config se encuentra en memoria RAM y el startup-config se almacena en memoria NVRAM, así si se pierde el fluido eléctrico la configuración que se tenía se recuperará de la memoria NVRAM (startup-config).

SHOW RUN

Quito #show running-config

Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

Building configuration...

!Version 12.1

Versión del Sistema Operativo del Router

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

Servicio de encriptación de contraseña no esta activo

!

hostname Quito

enable password cisco

!

ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

interface Serial0

Tipo de Interfaz

ip address 192.168.0.17 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast

clock rate 64000

Indica la velocidad del puerto en bits por segundo Lo encuentra en la DCE

bandwidth 1544

!

interface Serial1

Tipo de Interfaz

ip address 192.168.0.14 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast

bandwidth 1544

!

!

interface FastEthernet0/0

Tipo de Interfaz

ip address 192.168.0.49 255.255.255.248

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast

bandwidth 100000

!

interface Bri0

no ip address

no ip directed-broadcast

shutdown

!

router ospf 1



Protocolo de Enrutamiento

```

network 192.168.0.12 0.0.0.3 area 0
network 192.168.0.16 0.0.0.3 area 0
network 192.168.0.48 0.0.0.7 area 0
network 192.168.4.0 0.0.0.7 area 0
network 192.168.4.8 0.0.0.7 area 0
network 192.168.4.16 0.0.0.15 area 0
network 192.168.4.32 0.0.0.15 area 0

```

Redes configuradas con el protocolo de Enrutamiento Ospf

!

ip classless

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

no ip http server

!

!

!

banner motd ^C

Indica el mensaje de Bienvenida del Router

Bienvenidos al Router Quito

^C

line con 0

login

transport input none

password cisco

Contraseña para línea de comandos

line aux 0

line vty 0 4

login

password cisco

Contraseña para Telnet

no scheduler allocate

end

SHOW IP ROUTE

Quito #show ip route

C.-Conectado.

S.- Estático.

I.- Protocolo IGRP.

R. - Protocolo Rip.

B. - Protocolo BGP.

D. - Protocolo EIGRP.

EX. – Protocolo EIGRP externo.

O.- Protocolo OSPF.

IA.- El número de las rutas recibidas de otras áreas del OSPF.

E1.- Rutas recibidas de otras áreas del OSPF tipo externo 1.

E2.- Rutas recibidas de otras áreas del OSPF tipo externo 2.

i.- Son las rutas recibidas de los anuncios del protocolo del IS-IS.



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

Descripción de Protocolos usados

Gateway of last resort is not set

Conectada directamente		Red con la que esta conectada		Interfaz
C		192.168.0.16/30 is directly connected,		Serial0
Protocolo ospf	Red aprendida por ospf	Distancia administrativa ancho de banda	Ip asignada a la interfaz	Interfaz
O	192.168.0.20/30	[110/64] via	192.168.0.18, 03:08:35,	FastEthernet0/0
192.168.0.0/0 is variably subnetted, 6 subnets				
C	192.168.0.16/30 is directly connected, Serial0			
C	192.168.0.12/30 is directly connected, Serial1			
C	192.168.0.48/29 is directly connected, FastEthernet0/0			
O	192.168.0.20/30	[110/64] via	192.168.0.18, 03:08:35,	FastEthernet0/0
O	192.168.0.40/29	[110/64] via	192.168.0.41, 03:08:35,	FastEthernet0/0
O	192.168.0.24/29	[110/64] via	192.168.0.25, 03:08:35,	FastEthernet0/0

5.24. INTRODUCCIÓN A LOS SWITCHES

Un switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection).

Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Un conmutador en el centro de una red en estrella.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

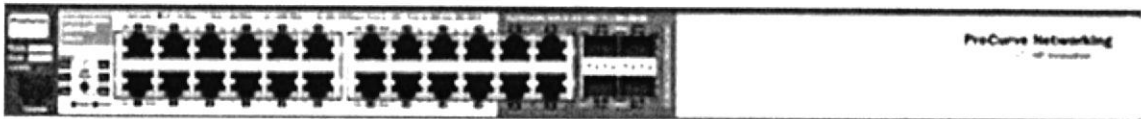


Figura 5-33 Switch

5.24.1. ENCAPSULAMIENTO

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

La capa de transporte divide los datos en unidades de un tamaño que se pueda administrar, denominadas segmentos. También asigna números de secuencia a los segmentos para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego la capa de red encapsula el segmento creando un paquete.

En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física.

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino. Pero si se deben enviar los datos a otro host a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia. Esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos (el paquete).

Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet. La excepción principal a esto es un dispositivo denominado gateway. Este es un dispositivo que ha sido diseñado para convertir los datos desde un formato, creado por las capas de aplicación, presentación y sesión, en otro formato. De modo que el gateway utiliza las siete capas del modelo OSI para hacer esto.

Flujo de paquetes a través de los dispositivos de Capa 2: Es importante recordar que los paquetes se ubican dentro de tramas, de modo que para comprender la forma en que viajan los paquetes en los dispositivos de la Capa 2, es necesario trabajar con la forma en que se encapsulan los paquetes, que es la trama. Cualquier cosa que le suceda a la trama también le sucede al paquete. Las NIC, los puentes y los switches involucran el uso de la información de la dirección de enlace de datos (MAC) para dirigir las tramas. Las NIC son el lugar donde reside la dirección MAC exclusiva.

La dirección MAC se utiliza para crear la trama.

Los puentes examinan la dirección MAC de las tramas entrantes. Si la trama es local (con una dirección MAC en el mismo segmento de red que el puerto de entrada del puente), entonces la trama no se envía a través del puente. Si la trama no es local (con una dirección MAC que no está en el puerto de entrada del puente), entonces se envía al segmento de red siguiente.

El puente toma una trama, la remueve, examina la dirección MAC y luego envía o no la trama, según lo que requiera la situación.

El switch es como un hub con puertos individuales que actúan como puentes. El switch toma una trama de datos, la lee, examina las direcciones MAC de la Capa 2 y envía las tramas (las conmuta) a los puertos adecuados.

5.24.2. SEGMENTACIÓN

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

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

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

Aunque los puentes y los switches comparten los atributos más importantes, todavía existen varias diferencias entre ellos. Los switches son significativamente más veloces porque realizan la conmutación por hardware, mientras que los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda.

Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch. Estos pueden soportar densidades de puerto más altas que los puentes. Algunos switches soportan la conmutación por el método cut-through, que reduce la latencia y las demoras de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward). Por último, los switches reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

5.24.3. COLISIÓN

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

Se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes como, por ejemplo, los repetidores, puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo. Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos.

El área dentro de la red donde los paquetes se originan y colisionan, se denomina dominio de colisión, e incluye todos los entornos de medios compartidos. Por ejemplo, un alambre puede estar conectado con otro a través de cables de conexión, transceptores, paneles de conexión, repetidores e incluso hubs. Todas estas interconexiones de la Capa 1 forman parte del dominio de colisión.

Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

Al igual que lo que ocurre con dos automóviles, que no pueden ocupar el mismo espacio, o la misma carretera, al mismo tiempo, tampoco es posible que dos señales ocupen el mismo medio simultáneamente. En general, se cree que las colisiones son malas ya que degradan el desempeño de la red. Sin embargo, una cantidad determinada de colisiones es una función natural de un entorno de medios compartidos (es decir, un dominio de colisión) ya que una gran cantidad de computadores intentan comunicarse entre sí simultáneamente, usando el mismo cable.

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

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

Un puente puede eliminar el tráfico innecesario en una red con mucha actividad dividiendo la red en segmentos y filtrando el tráfico basándose en la dirección de la estación.

El tráfico entre dispositivos en el mismo segmento no atraviesa el puente, y afecta otros segmentos. Esto funciona bien, siempre y cuando el tráfico entre segmentos no sea demasiado. En caso contrario, el puente se puede transformar en un cuello de botella, y de hecho puede reducir la velocidad de la comunicación

5.25. CONFIGURACIÓN DE SWITCHES

Se procederá ahora con la configuración de los Switches.

5.25.1. MODOS DE INTERFAZ USUARIO

Es posible que un switch ya esté pre-configurado y sólo deban introducirse contraseñas para los modos EXEC usuario o EXEC privilegiado. Se entra al modo de configuración de un switch desde el modo EXEC privilegiado.

En la CLI, el indicador del modo EXEC privilegiado por defecto es Switch#. En el modo EXEC usuario el indicador es Switch>.

La seguridad, la documentación y la administración son importantes para cada dispositivo de red.

Al switch se le debe otorgar un nombre de host y se deben establecer contraseñas en las líneas de consola y vty.

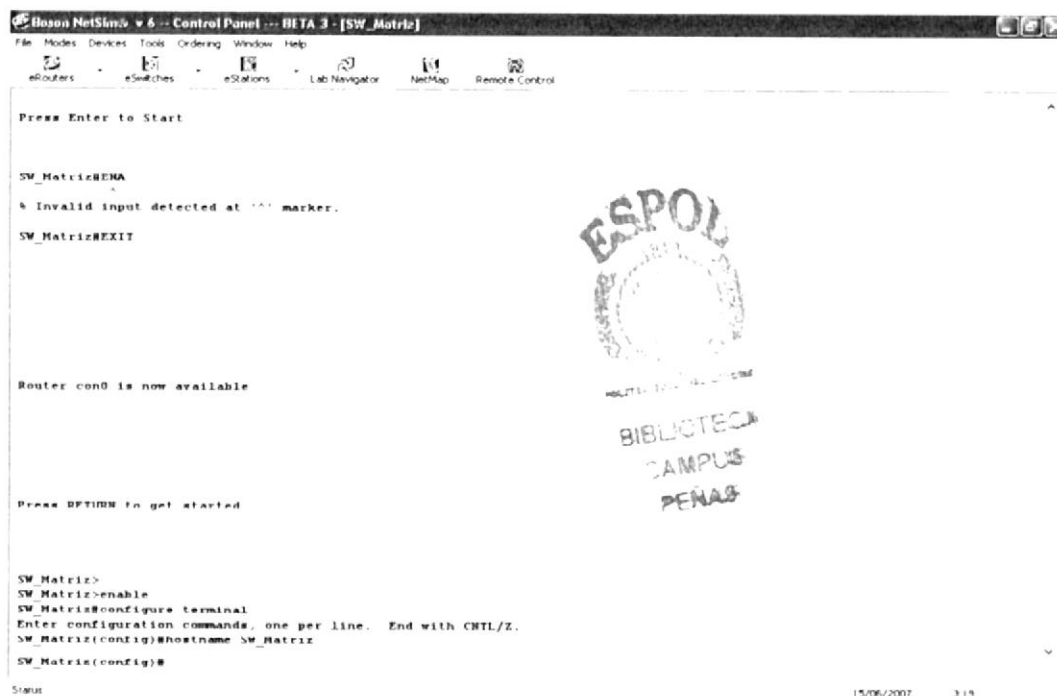


Figura 5-34 Interfaz De Usuario

5.26. CONFIGURACIÓN DE CONTRASEÑAS

Con fines de seguridad y administración, se deben establecer contraseñas en las líneas de consola y vty. También se debe establecer una contraseña enable y una contraseña enable secret.


```

Boson NetSim v6 - Control Panel - BETA 3 - [SW_Matriz]
File Modes Devices Tools Ordering Window Help
eRouters eSwitches eStations Lab Navigator NetMap Remote Control

Router con0 is now available

Press RETURN to get started.

SW_Matriz>
SW_Matriz>enable
SW_Matriz#configure terminal
Enter configuration commands, one per line. End with CRTL/Z.
SW_Matriz(config)#hostname SW_Matriz
SW_Matriz(config)#exit
SW_Matriz#
SW_Matriz#con
SW_Matriz#configure terminal
Enter configuration commands, one per line. End with CRTL/Z.
SW_Matriz(config)#line console 0
SW_Matriz(config-line)#password cisco
SW_Matriz(config-line)#login
SW_Matriz(config-line)#exit
SW_Matriz(config)#line vty 0 15
SW_Matriz(config-line)#password cisco
SW_Matriz(config-line)#login
SW_Matriz(config-line)#exit
SW_Matriz(config)#enable password cisco
SW_Matriz(config)#enable secret cisco
SW_Matriz(config)#

```

Figura 5-35 Configuración de contraseñas

En ciertas circunstancias es posible que se produzca acceso físico al switch, pero no pueda accederse al modo EXEC usuario o privilegiado debido a que las contraseñas no se conocen o se han olvidado.

5.27. ASPECTOS BÁSICOS DE LAS VLAN

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

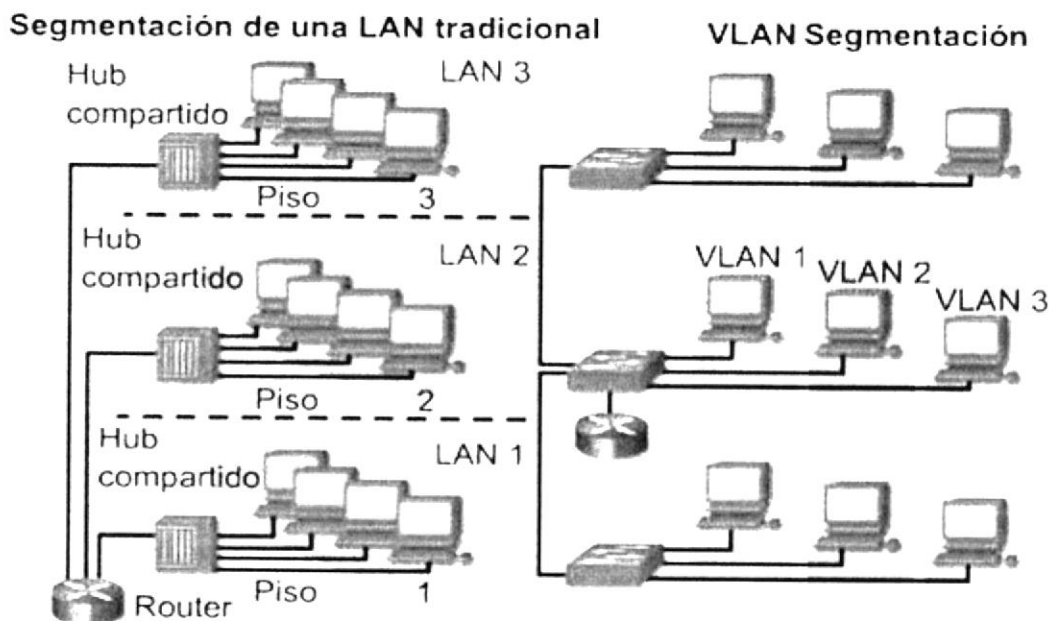


Figura 5-36 Aspectos De Vlans

Las VLAN se configuran en el switch a través del software.

Debido a la cantidad de implementaciones de VLAN que compiten entre sí es posible que deba requerirse el uso de un software propietario por parte del fabricante del switch.

La agrupación de puertos y usuarios en comunidades de interés, conocidos como organizaciones VLAN, puede obtenerse mediante el uso de un solo switch o una conexión más potente entre los switches ya conectados dentro de la empresa.

Al agrupar puertos y usuarios en varios switches, las VLAN pueden abarcar infraestructuras contenidas en un solo edificio o en edificios interconectados.

Las VLAN ayudan a utilizar con efectividad el ancho de banda dado que comparten el mismo dominio de broadcast o la misma red de Capa 3.

Las VLAN optimizan la acumulación y uso del ancho de banda. Las VLAN se disputan el mismo ancho de banda aunque los requisitos del ancho de banda pueden variar considerablemente según el grupo de trabajo o el departamento.

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

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

Las VLAN ayudan a controlar el tamaño de los dominios de broadcast y a ubicar el tráfico. Las VLAN se asocian con redes individuales.

Por lo tanto, los dispositivos de red en las distintas VLAN no se pueden comunicar directamente entre sí sin la intervención de un dispositivo de enrutamiento de Capa 3.

5.28. CONFIGURACIÓN DE VLAN POR DEFECTO

Para permitir que Telnet y otras aplicaciones TCP/IP puedan acceder al switch, se deberán establecer direcciones IP y un gateway por defecto. Por defecto, la VLAN 1 es la VLAN de administración. En una red basada en switch, todos los dispositivos de red deberían estar en la VLAN de administración. Esto permite que una sola estación de trabajo de administración acceda, configure y administre todos los dispositivos de red.



```

Boson NetSim v6 -- Control Panel -- BETA 3 - [SW_Matriz_Principal]
File Modes Devices Tools Ordering Window Help
eRouters eSwitches eStations Lab Navigator NetMap Remote Control

Press RETURN to get started.

Password:
Password:
Enter password:
SW_Matriz_Principal>ena
Enter password:
SW_Matriz_Principal#configure terminal
Enter configuration commands, one per line. End with CHTL/Z.
SW_Matriz_Principal(config)#interface vlan 1
SW_Matriz_Principal(config-if)#ip address 192.168.0.26 255.255.255.248
SW_Matriz_Principal(config-if)#ip ?
address          Set the IP address of an interface
SW_Matriz_Principal(config-if)#?
ip               Interface Internet Protocol config commands
switchport      Set switching mode characteristics
exit            Exit from interface configuration mode
description     Interface specific description
shutdown        Shutdown the selected interface
help            Description of the interactive help system
duplex          Configure duplex operation.
speed           Configure speed operation.
SW_Matriz_Principal(config-if)#ip default-gateway 192.168.0.27
SW_Matriz_Principal(config)#exit
SW_Matriz_Principal#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

SW_Matriz_Principal#

```

Figura 5-37 Vlan Por Defecto

5.28.1. CREACIÓN DE VLAN'S

Las VLAN se configuran en el switch a través del software.

- Ingrese al modo de configuración de Vlan con el comando *Vlan database*.
- Asigne un número y un nombre con el comando **Vlan number name nombre**.



```

Boson NetSim v6 -- Control Panel -- BETA 3 - [SW_Matriz_Principal]
File Modes Devices Tools Ordering Window Help
eRouters eSwitches eStations Lab Navigator NetMap Remote Control

Press RETURN to get started.

Password:
Password:
Enter password:
SW_Matriz_Principal>ena
Enter password:
SW_Matriz_Principal#vlan database
SW_Matriz_Principal(vlan)#vlan 5 name Sistemas
SW_Matriz_Principal(vlan)#vlan 6 name Contabilidad
SW_Matriz_Principal(vlan)#vlan 7 name RRHH
SW_Matriz_Principal(vlan)#vlan 8 name Gerencia

SW_Matriz_Principal(vlan)#vlan 9 name Logistica_Bodega
SW_Matriz_Principal(vlan)#exit
APPLY completed.
Exiting....
SW_Matriz_Principal#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

SW_Matriz_Principal#

```

Figura 5-38 Asignación De Nombre A VLAN

5.28.2. BORRADO DE VLAN'S

Los siguientes pasos permitirán que una nueva configuración se sobrescriba completamente a la configuración actual:

- Para eliminar la información de VLAN actual, borre el archivo de la base de datos VLAN, denominado `vlan.dat`, del directorio flash
- Borre el archivo de configuración de respaldo con el nombre `startup-config`
- Reinicie el switch con el comando `reload`

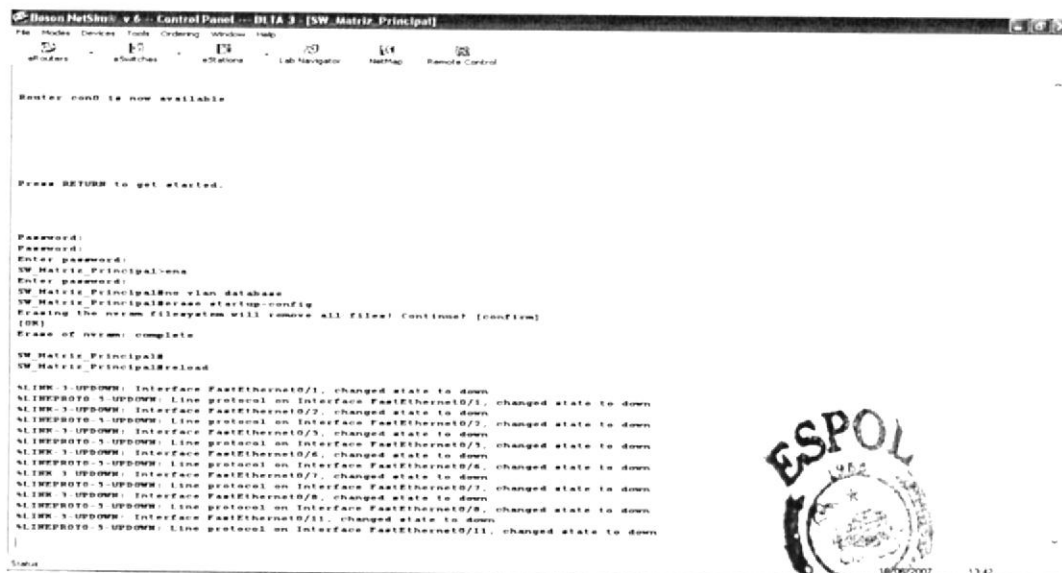


Figura 5-39 Borrado De VLAN

5.28.3. ASIGNACIÓN DE VLAN'S A LOS PUERTOS

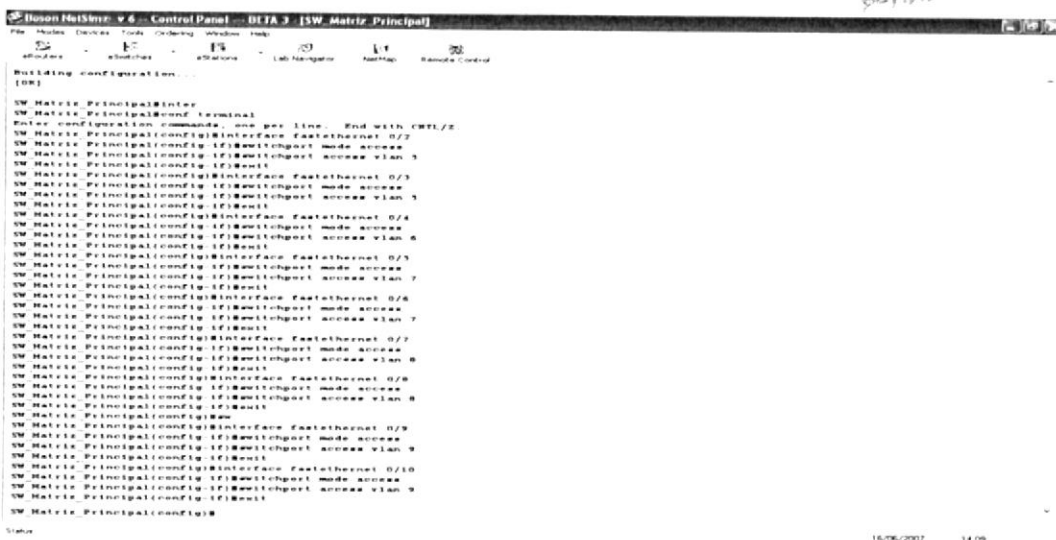


Figura 5-40 Asignación De Vlan's A Los Puertos

5.28.4. ENRUTAMIENTO ENTRE VLAN

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

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

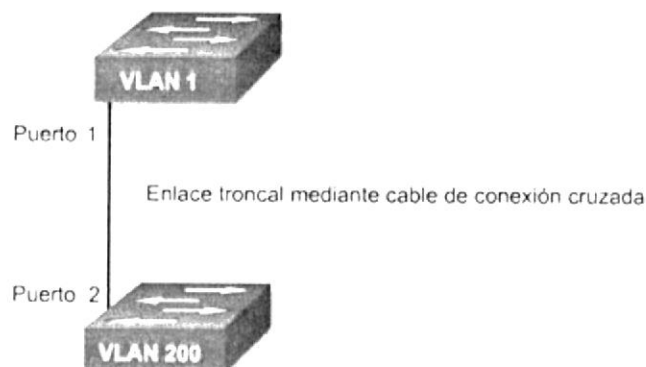


Figura 5-41 Enrutamiento Entre Vlan

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

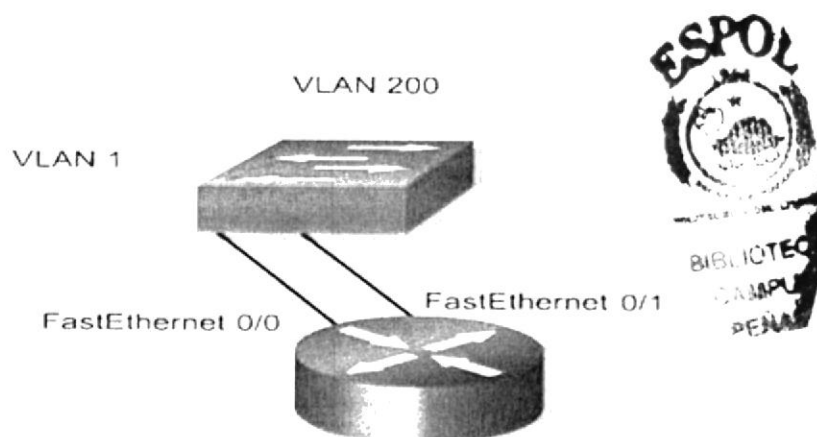


Figura 5-42 Enrutamiento Entre Vlan 2

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

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

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

5.28.5. INTERFACES FÍSICAS Y LÓGICAS

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

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

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

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

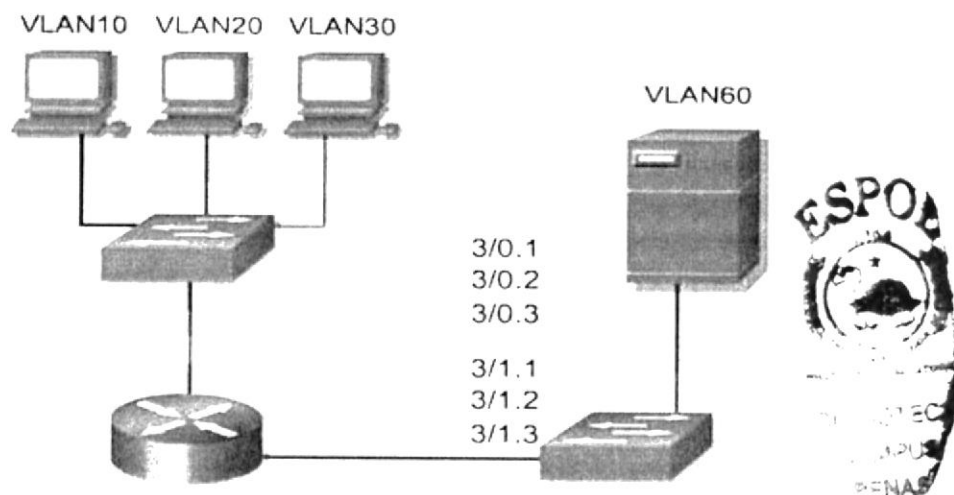


Figura 5-43 Interfaces Físicas Y lógicas

La ventaja principal del uso del enlace troncal es una reducción en la cantidad de puertos de router y switch que se utiliza.

Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de router conectado a un enlace troncal puede ampliarse hasta un número mucho más alto de VLAN que el diseño de "un enlace por VLAN".

5.28.6. ASIGNAR SWITCH DE TIPO SERVER

El rol de VTP es mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común. VTP es un protocolo de mensajería que usa tramas de enlace troncal de Capa 2 para agregar, borrar y cambiar el nombre de las

VLAN en un solo dominio. VTP también admite cambios centralizados que se comunican a todos los demás switches de la red.

Para determinar un switch de tipo Server debe estar en el MODO PRIVILEGED EXEC e ingresar al modo de configuración de vlan's con el comando "**Vlan database**", una vez adentro digitar la línea de comando " vtp < Server o client>" después digita el comando "vtp domain <nombre del dominio>" y por ultimo Salir de la configuración con el comando "exit".

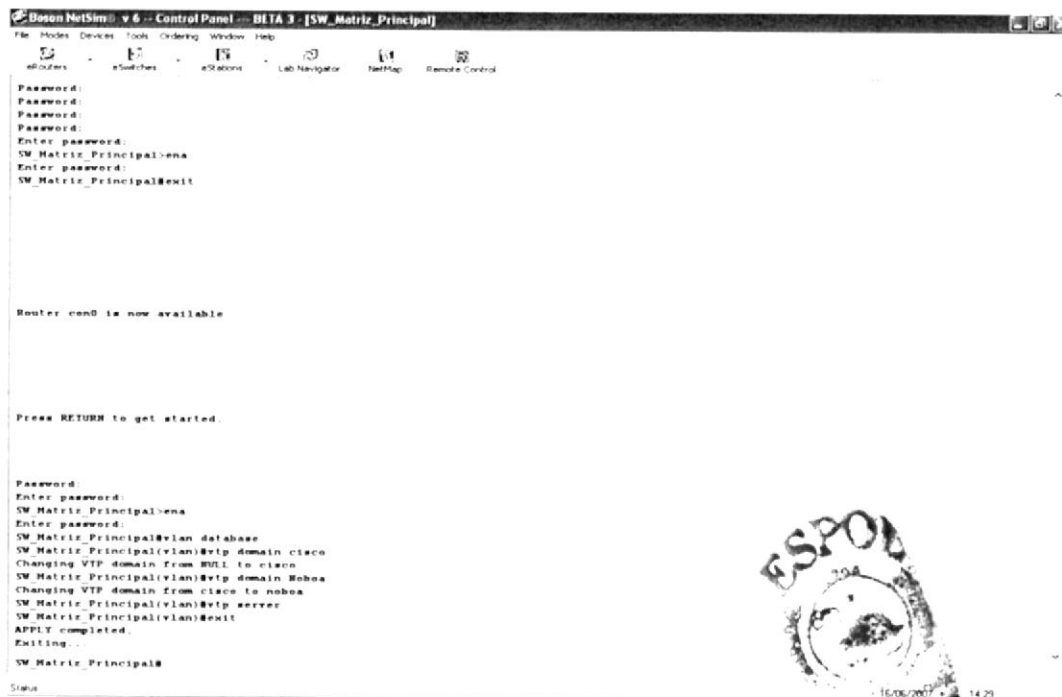


Figura 5-44 Determinación De Switch

5.28.7. CONFIGURACIÓN DE UN ENRUTAMIENTO ENTRE DISTINTAS VLAN

Para que el enrutamiento entre VLAN funcione correctamente, todos los routers y switches involucrados deben admitir el mismo encapsulamiento.

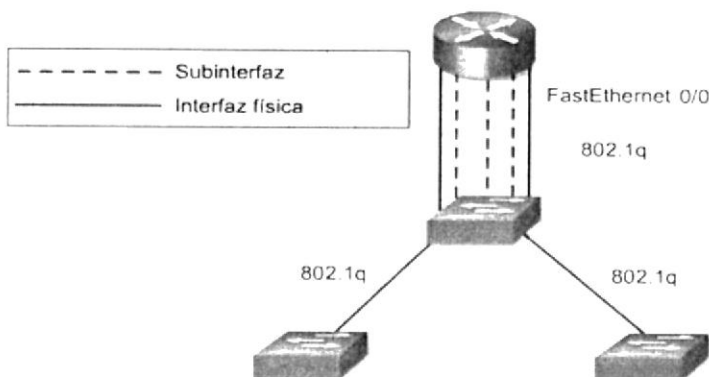


Figura 5-45 Enrutamiento Entre Vlans

En un router, una interfaz se puede dividir lógicamente en varias subinterfases virtuales. Las subinterfases ofrecen una solución flexible para el enrutamiento de varias corrientes de datos a través de una interfaz física única.

Para definir las subinterfaces en una interfaz física, realice las siguientes tareas:

- Identifique la interfaz.
- Defina el encapsulamiento de la VLAN.
- Asigne una dirección IP a la interfaz.

Para identificar la interfaz utilice el comando `interface` en el modo de configuración global.

Router (config) #interface fastethernet port-number. Subinterface-number

Port-number identifica la interfaz física y subinterface-number identifica la interfaz virtual (Vlan). El router debe poder comunicarse con el switch utilizando un protocolo de enlace troncal estandarizado.

Esto significa que ambos dispositivos conectados entre sí deben comprenderse. Para definir el encapsulamiento de la VLAN, introduzca el comando encapsulation en el modo de configuración de interfaz.Router (config-if) #encapsulation dot1q Vlan -number

Vlan-number identifica la VLAN para la cual la subinterfaz transportará el tráfico.

Se agrega un ID de VLAN a la trama sólo cuando la trama está destinada a una red no local. Cada paquete de VLAN transporta el ID de VLAN dentro del encabezado del paquete. Para asignar una dirección IP a la interfaz, introduzca el siguiente comando en el modo de configuración de interfaz.

Router (config-if) #ip address ip-address subnet-mask

IP-address y subnet-mask son las direcciones y la máscara de red de 32 bits de la interfaz específica.



Figura 5-46 Modo Configuración Global

5.29. PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE SWITCH (INSTITUTO NACIONAL GALÁPAGOS)

Ahora pasare a configurar paso a paso los diferentes Switch de la red Instituto Nacional Galápagos

5.29.1. ACCESO A LA APLICACIÓN HYPERTERMINAL

En la barra de tareas de Windows seleccionar con el Mouse la opción Inicio

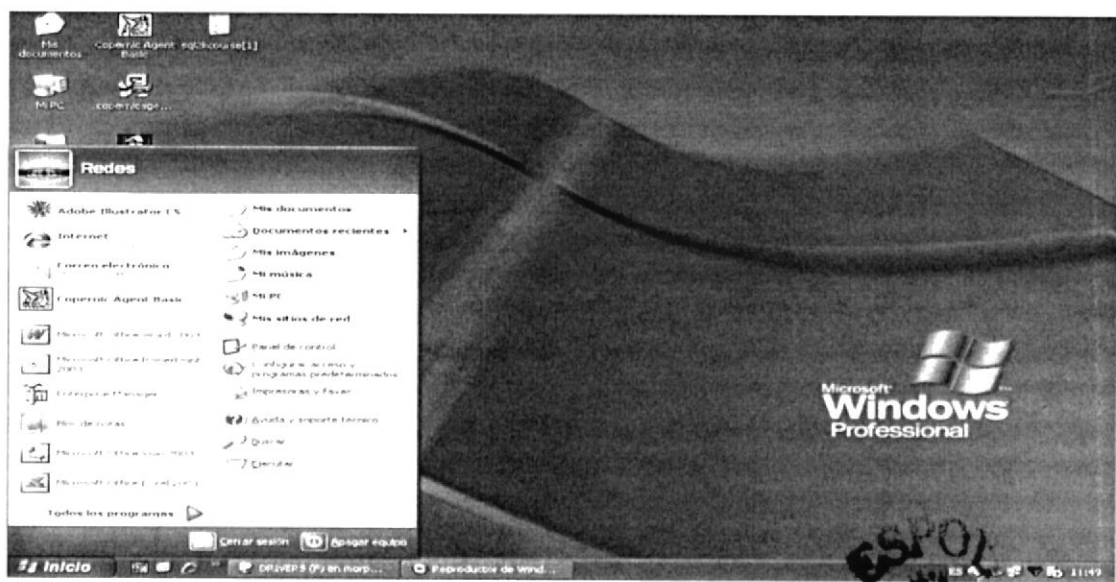


Figura 5-47 Entorno de Windows

Se abrirá un menú donde seleccione la opción todos los programas



Figura 5-48 Menú inicio

8. Aquí encontrará un acceso directo llamado HyperTerminal, al cual le dará clic y mostrará la siguiente pantalla.

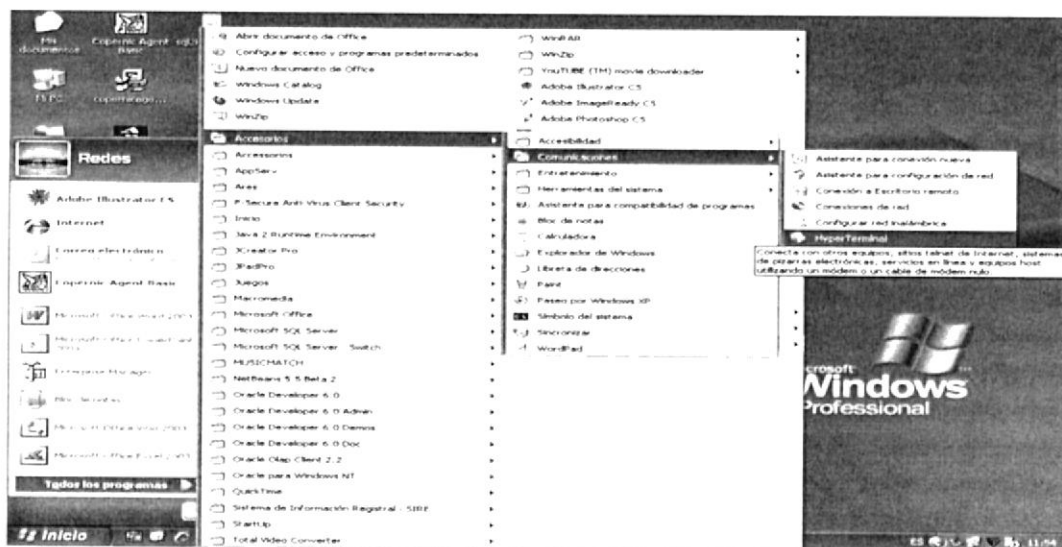


Figura 5-49 Selección de programa (hiperterminal)

En el cuadro de texto denominado Nombre se colocará un identificador a la conexión en este caso será Instituto Nacional Galápagos y dará Aceptar, si da clic en el botón Cancelar no existirá ninguna conexión

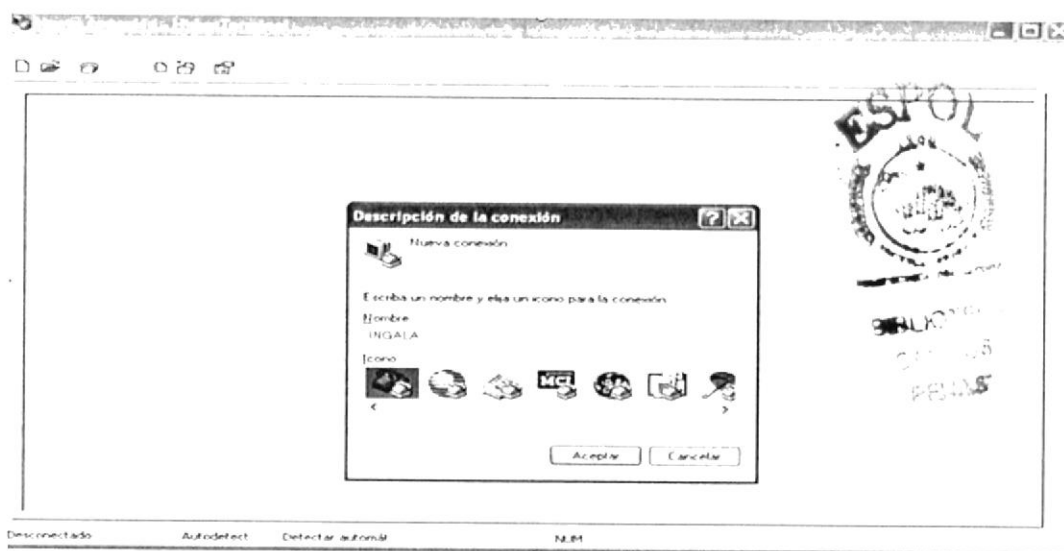


Figura 5-50 Nueva conexión

En la siguiente pantalla se pedirá ingresar algunos detalles de conexión como País o región, Código de área, Número de teléfono y conectar usando. Las tres primeras no son obligatorias son opcionales mientras que la ultima opción deberá escoger el puerto del computador al cual se va conectar el router en este caso va ser el puerto COM 1 y da clic en el botón Aceptar

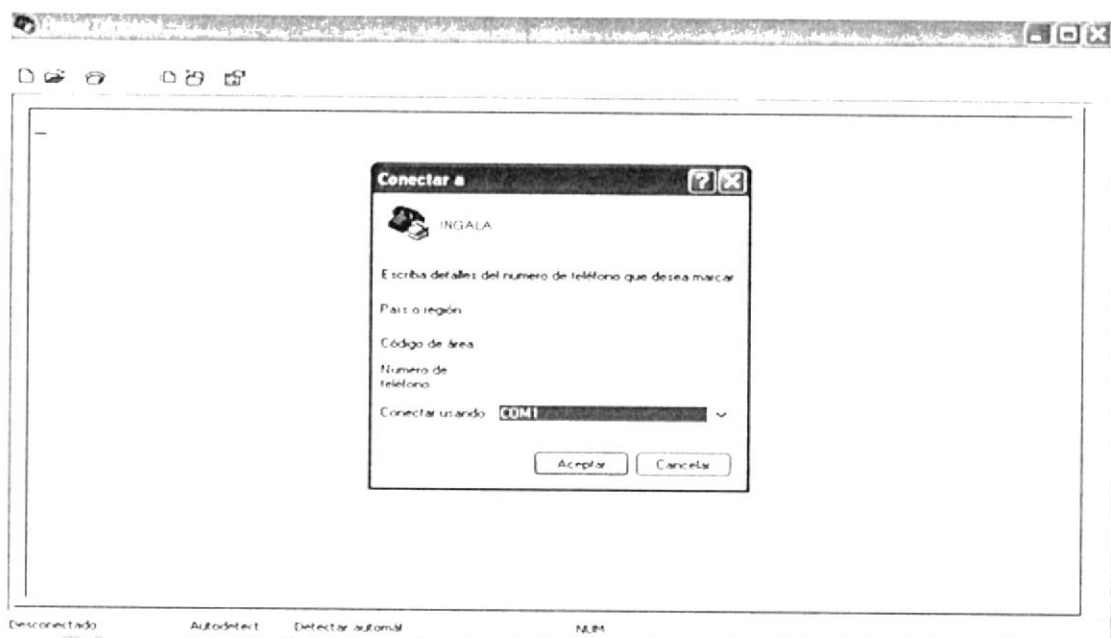


Figura 5-51 Conectar a....

Sugerencia:

Si da clic en el botón Cancelar no habrá terminado de realizar la conexión por consiguiente no se habrá conectado tendiendo un pantalla en blanco.

En la siguiente pantalla encontrará algunos parámetros de conexión de los cuales deberá establecer y dar clic en el botón Aceptar.

- 9600 bps. (velocidad de transmisión del cable serial de conexión)
- 8 bits de Datos (configuración del procesamiento de datos al pasar al Hyperterminal en bits por segundo)
- Ninguno (paridad) (utilizado para comprobar errores en el grupo de bits de datos transferidos entre uno o varios equipos)
- 1 (bit de parada) (medida de transporte por la que pasan datos al Hyperterminal)
- Ninguno control del flujo (se refiere a la información que viaja)



Figura 5-52 Propiedades de com 1

Sugerencia:

Se los puede establecer al dar clic en el botón **Restaurar predeterminados**

Una vez colocado los parámetros dará clic en el botón Aceptar y podrá empezar con la configuración del Switch a través de la consola Hyperterminal.

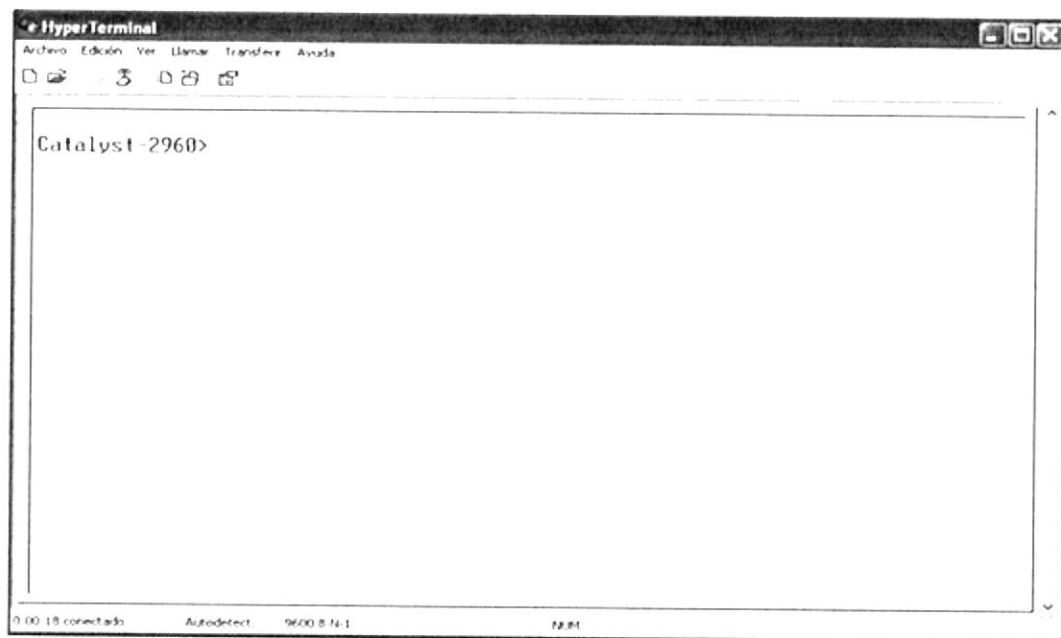


Figura 5-53 Conexión al switch 1

5.29.2. CONFIGURACIÓN DEL SWITCH MATRÍZ PRINCIPAL

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, se reconocerá por que su formato es de color azul.

Acceso al modo de Configuración principal.

Switch>enable

Ingresar al modo EXEC privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch (config) #exit

Salir un nivel

Configuración de los nombres del Switch Matriz

SW_Matriz_Principal>enable

Ingresar al modo EXEC privilegiado

SW_Matriz_Principal#configure terminal

Ingresar al modo de configuración global

SW_Matriz_Principal (config) #hostname SW_Matriz_Principal

Sirve para asignarle un nombre al Switch (SW_Matriz_Principal)

SW_Matriz_Principal (config) #

Configuración de Contraseñas

SW_Matriz_Principal#configure terminal

Ingresar al modo de configuración global

SW_Matriz_Principal (config) #line console 0

Ingresar a configurar la consola

SW_Matriz_Principal (config-line) #password <password>

Asignar una contraseña a la consola

SW_Matriz_Principal (config-line) #login

SW_Matriz_Principal (config-line) #exit

Salir de la configuración de la consola

SW_Matriz_Principal (config) #line vty 0 15

Ingresar a configurar la Terminal virtual

SW_Matriz_Principal (config-line) #password <password>

Asignar una contraseña a la Terminal virtual

SW_Matriz_Principal (config-line) #login

SW_Matriz_Principal (config-line) #exit

Salir de la configuración de la Terminal virtual

SW_Matriz_Principal (config) #enable password<password>

Agregar una contraseña para ingresar al swicht

SW_Matriz_Principal (config) #enable secret<password>

Agregar una contraseña encriptada para ingresar al swicht

Creación de VLAN's

SW_Matriz_Principal>enable

Ingresar al modo de configuración global

SW_Matriz_Principal#vlan database

Ingresar al modo de configuración de vlan's

SW_Matriz_Principal (Vlan) #Vlan 1 name Archivo Central

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 2 name Gerencia

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 3 name Dirección Jurídica

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 4 name Dirección Financiera

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 5 name Dirección Administrativa

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 6 name RRHH

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 7 name Control Residencia

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 8 name Servicio de Investigación

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 9 name Contabilidad

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Matriz_Principal (Vlan) #Vlan 10 name Comunicacion Social



Asignar un número referencial y un nombre a la Vlan que se va a crear
 SW_Matriz_Principal (Vlan) #Vlan 11 name Planificacion

Asignar un número referencial y un nombre a la Vlan que se va a crear
 SW_Matriz_Principal (Vlan) #exit

Salir del modo configuración de Vlan
 SW_Matriz_Principal#

Asignación de VLAN's a los puertos

SW_Matriz_Principal>enable

Ingresar al modo EXEC privilegiado

SW_Matriz_Principal#configure terminal

Ingresar al modo de configuración global

SW_Matriz_Principal (config) #

SW_Matriz_Principal (config) #interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access Vlan 1

Asignar el puerto a la Vlan 1

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/3

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 2

Asignar el puerto a la Vlan 2

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/4

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 3

Asignar el puerto a la Vlan 3

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/5

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 4

Asignar el puerto a la Vlan 4

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/6

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 5

Asignar el puerto a la Vlan 5

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/7



Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 6

Asignar el puerto a la Vlan 6

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/8

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 7

Asignar el puerto a la Vlan 7

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/9

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 8

Asignar el puerto a la Vlan 8

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/10

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 9

Asignar el puerto a la Vlan 9

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/11

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 10

Asignar el puerto a la Vlan 10

SW_Matriz_Principal (config-if) #exit

SW_Matriz_Principal (config) #interface fastethernet 0/12

Ingresar a la interfaz puerto que se va a configurar

SW_Matriz_Principal (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Matriz_Principal (config-if) #switchport access vlan 11

Asignar el puerto a la Vlan 11

SW_Matriz_Principal (config-if) #exit

Asignar SW_Matriz_Principal de Tipo Server

SW_Matriz_Principal>enable

Ingresar al modo EXEC privilegiado

SW_Matriz_Principal#vlan database

Ingresar al modo de configuración de Vlan

SW_Matriz_Principal (Vlan) #vtp domain ingala

Asignar un dominio vtp al SW_Matriz_Principal

SW_Matriz_Principal (Vlan) #vtp server

Configurar de modo server el SW_Matriz_Principal

SW_Matriz_Principal (Vlan) #exit

Salir al modo de configuración global

Configuración de un enrutamiento entre distintas VLAN (Router SW_Matriz_Principal)

Matriz>enable

Ingresar al modo EXEC privilegiado

Matriz#configure terminal

Ingresar al modo de configuración global

Matriz (config) #interface FastEthernet 1/0.1

Ingresar a la sub-interfaz que se va a configurar

Matriz (config-subif) #encapsulation dot1q 1

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 5

Matriz (config-subif) #ip address 192.168.3.1 255.255.255.224

Asignar una dirección ip con su respectiva máscara

Matriz (config-subif) #exit

Salir de la configuración de la sub-interfaz

Matriz (config) #interface FastEthernet 1/0.2

Ingresar a la sub-interfaz que se va a configurar

Matriz (config-subif) #encapsulation dot1q 2

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1

Matriz (config-subif) #ip address 192.168.3.2 255.255.255.224

Asignar una dirección ip con su respectiva máscara

Matriz (config-subif) #exit

Salir de la configuración de la sub-interfaz

Matriz (config) #interface FastEthernet 1/0.3

Ingresar a la sub-interfaz que se va a configurar

Matriz (config-subif) #encapsulation dot1q 3

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 2

Matriz (config-subif) #ip address 192.168.3.3 255.255.255.224

Asignar una dirección ip con su respectiva máscara

Matriz (config-subif) #exit

Salir de la configuración de la sub-interfaz

Matriz (config) #interface FastEthernet 1/0.4

Ingresar a la sub-interfaz que se va a configurar

Matriz (config-subif) #encapsulation dot1q 4

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 3

Matriz (config-subif) #ip address 192.168.3.4 255.255.255.240

Asignar una dirección ip con su respectiva máscara

Matriz (config-subif) #exit

Salir de la configuración de la sub-interfaz

Matriz (config) #interface FastEthernet 1/0.5

Ingresar a la sub-interfaz que se va a configurar

Matriz (config-subif) #encapsulation dot1q 5

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 4

Matriz (config-subif) #ip address 192.168.3.5 255.255.255.240

Asignar una dirección ip con su respectiva máscara



Matríz (config-subif) #exit
Salir de la configuración de la sub-interfaz

Matríz (config) #interface FastEthernet 1/0.6
Ingresar a la sub-interfaz que se va a configurar

Matríz (config-subif) #encapsulation dot1q 6
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 4

Matríz (config-subif) #ip address 192.168.3.6 255.255.255.240
Asignar una dirección ip con su respectiva máscara

Matríz (config-subif) #exit
Salir de la configuración de la sub-interfaz

Matríz (config) #interface FastEthernet 1/0.7
Ingresar a la sub-interfaz que se va a configurar

Matríz (config-subif) #encapsulation dot1q 7
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 4

Matríz (config-subif) #ip address 192.168.3.7 255.255.255.240
Asignar una dirección ip con su respectiva máscara

Matríz (config-subif) #exit
Salir de la configuración de la sub-interfaz

Matríz (config) #interface FastEthernet 1/0.8
Ingresar a la sub-interfaz que se va a configurar

Matríz (config-subif) #encapsulation dot1q 8
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 4

Matríz (config-subif) #ip address 192.168.3.8 255.255.255.240
Asignar una dirección ip con su respectiva máscara

Matríz (config-subif) #exit
Salir de la configuración de la sub-interfaz

Matríz (config) #interface FastEthernet 1/0.9
Ingresar a la sub-interfaz que se va a configurar

Matríz (config-subif) #encapsulation dot1q 9
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 4

Matríz (config-subif) #ip address 192.168.3.9 255.255.255.240
Asignar una dirección ip con su respectiva máscara

Matríz (config-subif) #exit
Salir de la configuración de la sub-interfaz

Matríz (config) #interface FastEthernet 1/0.10
Ingresar a la sub-interfaz que se va a configurar

Matríz (config-subif) #encapsulation dot1q 10
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 4

Matríz (config-subif) #ip address 192.168.3.10 255.255.255.240
Asignar una dirección ip con su respectiva máscara

Matríz (config-subif) #exit
Salir de la configuración de la sub-interfaz

Matríz (config) #interface FastEthernet 1/0.11
Ingresar a la sub-interfaz que se va a configurar

Matríz (config-subif) #encapsulation dot1q 11
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 4

Matríz (config-subif) #ip address 192.168.3.11 255.255.255.240
Asignar una dirección ip con su respectiva máscara

Matríz (config-subif) #exit
Salir de la configuración de la sub-interfaz

Matriz#copy runn-config startup-config

Guardar una copia de la configuración a la NVRAM

SHOW RUNNING-CONFIG

SW_Matriz_Principal#show running-config

Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

Version 12.1

Configuración actual del switch

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

El servicio de encriptación de contraseña no esta activo

!

hostname SW_Matriz_Principal

Nombre del switch

ip name-server 0.0.0.0

enable password cisco

!

!

ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!!

spanning-tree extend system-id

!!

interface FastEthernet0/1

Puertos físicos del switch, aquí se verifica a que Vlan pertenece

!

interface FastEthernet0/2

switchport mode access

switchport access vlan 1

Puerto asignado a la Vlan 5

bandwidth 100000

!

interface FastEthernet0/3

switchport mode access

switchport access vlan 2

Puerto asignado a la Vlan 5

bandwidth 100000

!

interface FastEthernet0/4

switchport mode access

switchport access vlan 3

Puerto asignado a la Vlan 6

bandwidth 100000

!

interface FastEthernet0/5

switchport mode access

switchport access vlan 4



Puerto asignado a la Vlan 7

bandwidth 100000

!

interface FastEthernet0/6

switchport mode access

switchport access vlan 5

Puerto asignado a la Vlan 7

bandwidth 100000

!

interface FastEthernet0/7

switchport mode access

switchport access vlan 6

Puerto asignado a la Vlan 8

bandwidth 100000

!

interface FastEthernet0/8

switchport mode access

switchport access vlan 7

Puerto asignado a la Vlan 8

bandwidth 100000

!

interface FastEthernet0/9

switchport mode access

switchport access vlan 8

Puerto asignado a la Vlan 9

bandwidth 100000

!

interface FastEthernet0/10

switchport mode access

switchport access vlan 9

Puerto asignado a la Vlan 9

bandwidth 100000

!

interface FastEthernet0/11

switchport mode access

switchport access vlan 10

Puerto asignado a la Vlan 10

bandwidth 100000

!

interface FastEthernet0/12

switchport mode access

switchport access vlan 11

Puerto asignado a la Vlan 11

bandwidth 100000

!

interface FastEthernet0/13

Puerto sin configurar

bandwidth 100000

!



```
interface FastEthernet0/14
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/15
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/16
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/17
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/18
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/19
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/20
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/21
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/22
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/23
    Puerto sin configurar
    bandwidth 100000
    !
interface FastEthernet0/24
    Puerto sin configurar
    bandwidth 100000
    !
vtp Server
vtp domain ingala
interface Vlan 1
    no ip address
    no ip route-cache
    shutdown
```



```
interface Vlan0001
no ip address
no ip route-cache
shutdown
```

```
vlan 1name 1
vlan 2name 2
```

```
vlan 3name 3
```

```
vlan 4name 4
```

```
vlan 5name 5
```

```
vlan 6name 6
```

```
vlan 7name 7
```

```
vlan 8name 8
```

```
vlan 9name 9
```

```
vlan 10name 10
```

```
vlan 11name 11
```

```
!
ip classless
no ip http server
!
```

```
line con 0
login
transport input none
password cisco
```

Contraseña para la línea de comandos

```
line aux 0
line vty 0 15
login
password cisco
```

Contraseña para telnet

```
!
no scheduler allocate
end
```

SHOW VLAN

VLAN.- Es el número de la vlan.

Name.- Es el nombre asignado a la vlan.

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



Ports.- Son los puertos asignados a la vlan.

SW_Matríz_Principal#show vlan

VLAN	Name	Status	Ports

1	default	active	Fa0/1 Número de puertos asignados a Vlan archivo_central
2	2	active	Fa0/2 Puertos asignados y activos a la Vlan gerencia
3	3	active	Fa0/3 Puertos asignados y activos a la Vlan dirección_jurídica
4	4	active	Fa0/4 Puertos asignados y activos a la Vlan dirección_financiera
5	5	active	Fa0/5 Puertos asignados y activos a la Vlan dirección_administrativa
6	6	active	Fa0/6 Puertos asignados y activos a la Vlan RRHH
7	7	active	Fa0/7 Puertos asignados y activos a la Vlan control_residencia
8	8	active	Fa0/8 Puertos asignados y activos a la Vlan servicio_investigación
9	9	active	Fa0/9 Puertos asignados y activos a la Vlan contabilidad
10	10	active	Fa0/10 Puertos asignados y activos a la Vlan comunicación_social
11	11	active	Fa0/11 Puertos asignados y activos a la Vlan planificación
1002	fdi-default	active	Vlan para red fdi active
1003	token-ring-default	active	Vlan para red token ring active
1004	fdinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	Ring	No	Bridge	No	Stp	Brdg	Mode	Trans1	Trans2

1	enet	100001	1500	-	-	-	-	-	0	0			
5	enet	100005	1500	-	-	-	-	-	0	0			
6	enet	100006	1500	-	-	-	-	-	0	0			
7	enet	100007	1500	-	-	-	-	-	0	0			
8	enet	100008	1500	-	-	-	-	-	0	0			
9	enet	100009	1500	-	-	-	-	-	0	0			
1002	fdi	101002	1500	-	-	-	-	-	0	0			
1003	tr	101003	1500	-	-	-	-	-	0	0			
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0			
1005	trnet	101005	1500	-	-	-	ibm	-	0	0			



5.29.3. CONFIGURACIÓN DEL SWITCH GUAYAQUIL

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, se reconocerá por que su formato es de color azul.

Acceso al modo de Configuración principal.

- Switch>enable
 - Ingresar al modo EXEC privilegiado
- Switch#configure terminal
 - Ingresar al modo de configuración global
- Switch(config) #exit
 - Salir un nivel

Configuración de los nombre del Swicht

SW_Guayaquil >enable

Ingresar al modo EXEC privilegiado

SW_Guayaquil #configure terminal

Ingresar al modo de configuración global

SW_Guayaquil (config) #hostname SW_Guayaquil

Sirve para asignarle un nombre al Swicht (SW_Guayaquil)

SW_Guayaquil (config) #

Configuración de Contraseñas

SW_Guayaquil #configure terminal

Ingresar al modo de configuración global

SW_Guayaquil (config) #line console 0

Ingresar a configurar la consola

SW_Guayaquil (config-line) #password <password>

Asignar una contraseña a la consola

SW_Guayaquil (config-line) #login

SW_Guayaquil (config-line) #exit

Salir de la configuración de la consola

SW_Guayaquil (config) #line vty 0 4

Ingresar a configurar la Terminal virtual

SW_Guayaquil (config-line) #password <password>

Asignar una contraseña a la Terminal virtual

SW_Guayaquil (config-line) #login

SW_Guayaquil (config-line) #exit

Salir de la configuración de la Terminal virtual

SW_Guayaquil (config) #enable password<password>

Agregar una contraseña para ingresar al router

SW_Guayaquil (config) #enable secret<password>

Agregar una contraseña encriptada para ingresar al router



Creación de VLAN's

SW_Guayaquil >enable

Ingresar al modo de configuración global

SW_Guayaquil #vlan database

Ingresar al modo de configuración de vlan's

SW_Guayaquil (Vlan) #Vlan 13 name contabilidad

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Guayaquil (Vlan) #Vlan 14 name administración

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Guayaquil (Vlan) #exit

Salir del modo configuración de Vlan

SW_Guayaquil #

Asignación de VLAN's a los puertos

SW_Guayaquil >enable

Ingresar al modo EXEC privilegiado

SW_Guayaquil #configure terminal

Ingresar al modo de configuración global

SW_Guayaquil (config) #

SW_Guayaquil (config) #interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

SW_Guayaquil (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Guayaquil (config-if) #switchport access Vlan 13

Asignar el puerto a la Vlan 13

SW_Guayaquil (config-if) #exit

SW_Guayaquil (config) #interface fastethernet 0/3

Ingresar a la interfaz puerto que se va a configurar

SW_Guayaquil (config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Guayaquil (config-if) #switchport access vlan 14

Asignar el puerto a la Vlan 14

SW_Guayaquil (config-if) #exit

Configuración de un enrutamiento entre distintas VLAN (Router SW_Guayaquil)

Guayaquil >enable

Ingresar al modo EXEC privilegiado

Guayaquil #configure terminal

Ingresar al modo de configuración global

Guayaquil (config) #interface FastEthernet 0/0.1

Ingresar a la sub-interfaz que se va a configurar

Guayaquil (config-subif) #encapsulation dot1q 1

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 10

Guayaquil (config-subif) #ip address 192.168.1.1 255.255.255.248

Asignar una dirección ip con su respectiva máscara

Guayaquil (config-subif) #exit

Salir de la configuración de la sub-interfaz

Guayaquil (config) #interface FastEthernet 0/0.2

Ingresar a la sub-interfaz que se va a configurar

Guayaquil (config-subif) #encapsulation dot1q 2

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 20

Guayaquil (config-subif) #ip address 192.168.2.9 255.255.255.248

Asignar una dirección ip con su respectiva máscara

Guayaquil (config-subif) #exit

Salir de la configuración de la sub-interfaz

Guayaquil (config) #interface FastEthernet 0/0.3

Ingresar a la sub-interfaz que se va a configurar

Guayaquil (config-subif) #encapsulation dot1q 3

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 30



Guayaquil (config-subif) #ip address 192.168.1.3 255.255.255.240

Asignar una dirección ip con su respectiva máscara

Guayaquil (config-subif) #exit

Salir de la configuración de la sub-interfaz

Guayaquil (config) #interface FastEthernet 0/0.4

Ingresar a la sub-interfaz que se va a configurar

Guayaquil (config-subif) #encapsulation dot1q 4

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 40

Guayaquil (config-subif) #ip address 192.168.1.4 255.255.255.248

Asignar una dirección ip con su respectiva máscara

Guayaquil (config-subif) #exit

Salir de la configuración de la sub-interfaz

Guayaquil #copy runn-config startup-config

Guardar una copia de la configuración a la NVRAM

SHOW RUNNING-CONFIG

SW_Guayaquil #show running-config

Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

Version 12.1

Configuración actual del switch

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

El servicio de encriptación de contraseña no esta activo

!

hostname SW_Guayaquil

Nombre del switch

ip name-server 0.0.0.0

enable password cisco

!

!!

ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!

!!

spanning-tree extend system-id

!

!

interface FastEthernet0/1

Puertos físicos del switch, aquí se verifica a que Vlan pertenece

!

interface FastEthernet0/2

switchport mode access

switchport access vlan 10

Puerto asignado a la Vlan 13

bandwidth 100000

!



```
interface FastEthernet0/3
switchport mode access
switchport access vlan 10
    Puerto asignado a la Vlan 14
bandwidth 100000
!
vlan 13 name 13

vlan 14 name 14
ip classless
no ip http server
!
!
line con 0
login
transport input none
password cisco

    Contraseña para la línea de comandos
line aux 0
line vty 0 15
login
password cisco

    Contraseña para telnet
!
no scheduler allocate
end
```

SHOW VLAN

- VLAN.-** Es el número de la vlan.
- Name.-** Es el nombre asignado a la vlan.
- Status.-** Es el estado en que se encuentra la vlan.
- Ports.-** Son los puertos asignados a la vlan.



SW_Guayaquil #show vlan

VLAN Name		Status	Ports
1	default	active	Fa0/1, Fa0/10, Fa0/11,Fa0/12 Número puertos asignados a Vlan administración
13	13	active	Fa0/2 Puertos asignados y activos a la Vlan contabilidad
14	14	active	Fa0/3 Puertos asignados y activos a la Vlan administración
1002	fdi-default	active	Vlan para red fddi active
1003	token-ring-default	active	Vlan para red token ring active
1004	fdinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	Ring	No Bridge	No Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0

5	enet	100005	1500	-	-	-	-	-	0	0
6	enet	100006	1500	-	-	-	-	-	0	0
7	enet	100007	1500	-	-	-	-	-	0	0
8	enet	100008	1500	-	-	-	-	-	0	0
9	enet	100009	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

5.29.4. CONFIGURACIÓN DEL SWITCH QUITO

Para un mejor entendimiento, se colocará debajo de algunos comandos una breve descripción de los mismos, se reconocerá por que su formato es de color azul.

Acceso al modo de Configuración principal.

Switch>enable

Ingresar al modo EXEC privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch(config) #exit

Salir un nivel

Configuración del nombre del Swicht Quito

SW_Quito>enable

Ingresar al modo EXEC privilegiado

SW_Quito#configure terminal

Ingresar al modo de configuración global

SW_Quito(config) #hostname SW_Quito

Sirve para asignarle un nombre al Swicht (SW_Quito)

SW_Quito (config) #



Configuración de Contraseñas

SW_Quito#configure terminal

Ingresar al modo de configuración global

SW_Quito(config) #line console 0

Ingresar a configurar la consola

SW_Quito(config-line) #password <password>

Asignar una contraseña a la consola

SW_Guayaquil (config-line) #login

SW_Guayaquil (config-line) #exit

Salir de la configuración de la consola

SW_Guayaquil (config) #line vty 0 4

Ingresar a configurar la Terminal virtual

SW_Guayaquil (config-line) #password <password>

Asignar una contraseña a la Terminal virtual

SW_Guayaquil (config-line) #login

SW_Quito(config-line) #exit

Salir de la configuración de la Terminal virtual

SW_Quito(config) #enable password<password>

Agregar una contraseña para ingresar al router

SW_Quito(config) #enable secret<password>

Agregar una contraseña encriptada para ingresar al router

Creación de VLAN's

SW_Quito>enable

Ingresar al modo de configuración global

SW_Quito#vlan database

Ingresar al modo de configuración de vlan's

SW_Quito(Vlan) #Vlan 12 name Administracion

Asignar un número referencial y un nombre a la Vlan que se va a crear

SW_Quito(Vlan) #exit

Salir del modo configuración de Vlan

SW_Quito#

Asignación de VLAN's a los puertos

SW_Quito>enable

Ingresar al modo EXEC privilegiado

SW_Quito#configure terminal

Ingresar al modo de configuración global

SW_Quito(config) #

SW_Quito(config) #interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

SW_Quito(config-if) #switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SW_Quito(config-if) #switchport access Vlan 12

Asignar el puerto a la Vlan 12

SW_Quito(config-if) #exit



Configuración de un enrutamiento entre distintas VLAN (Router SW_Quito)

Quito >enable

Ingresar al modo EXEC privilegiado

Quito #configure terminal

Ingresar al modo de configuración global

Quito (config) #interface FastEthernet 0/0.1

Ingresar a la sub-interfaz que se va a configurar

Quito (config-subif) #encapsulation dot1q 1

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 79

Quito (config-subif) #ip address 192.168.4.1 255.255.255.240

Asignar una dirección ip con su respectiva máscara

Quito (config-subif) #exit

Salir de la configuración de la sub-interfaz

Quito (config) #interface FastEthernet 0/0.2

Ingresar a la sub-interfaz que se va a configurar

Quito (config-subif) #encapsulation dot1q 2

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 80

Quito (config-subif) #ip address 192.168.4.2 255.255.255.240

Asignar una dirección ip con su respectiva máscara

Quito (config-subif) #exit

Salir de la configuración de la sub-interfaz

Quito (config) #interface FastEthernet 0/0.3

Ingresa a la sub-interfaz que se va a configurar

Quito (config-subif) #encapsulation dot1q 3

Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 81

Quito (config-subif) #ip address 192.168.4.3 255.255.255.240

Asignar una dirección ip con su respectiva máscara

Quito (config-subif) #exit

Salir de la configuración de la sub-interfaz

Quito #copy runn-config startup-config

Guardar una copia de la configuración a la NVRAM

SHOW RUNNING-CONFIG

SW_Quito#show running-config

Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

Version 12.1

Version del Sistema Operativo

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

El servicio de encriptación de contraseña no está activo

!

hostname SW_Quito

Nombre del switch

ip name-server 0.0.0.0

enable password cisco

!

!ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!

!spanning-tree extend system-id

!

!

interface FastEthernet0/1

Puertos físicos del switch, aquí se verifica a qué Vlan pertenece

!

interface FastEthernet0/2

switchport mode access

switchport access vlan 12

Puerto asignado a la Vlan 12

bandwidth 100000

!

vlan 12 name 12

ip classless



```
no ip http server
!
!
line con 0
login
transport input none
password cisco
```

Contraseña para la línea de comandos

```
line aux 0
line vty 0 15
login
password cisco
```

Contraseña para telnet

```
!
no scheduler allocate
end
```

SHOW VLAN

VLAN.- Es el número de la vlan.

Name.- Es el nombre asignado a la vlan.

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

Ports.- Son los puertos asignados a la vlan.

SW_Quito#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/10, Fa0/11, Fa0/12
12 12	active	Fa0/2
1002 fddi-default	active	Vlan para red fddi
1003 token-ring-default	active	Vlan para red token ring
1004 fddinet-default	active	
1005 trnet-default	active	



VLAN	Type	SAID	MTU	Parent	Ring	No Bridge	No Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	0	0	
5	enet	100005	1500	-	-	-	-	0	0	
6	enet	100006	1500	-	-	-	-	0	0	
7	enet	100007	1500	-	-	-	-	0	0	
8	enet	100008	1500	-	-	-	-	0	0	
9	enet	100009	1500	-	-	-	-	0	0	
1002	fddi	101002	1500	-	-	-	-	0	0	
1003	tr	101003	1500	-	-	-	-	0	0	
1004	fdnet	101004	1500	-	-	-	ieee	0	0	
1005	trnet	101005	1500	-	-	-	ibm	0	0	

5.30. TABLAS DE LOS SEGMENTOS DE LAS REDES DEL INSTITUTO NACIONAL GALAPAGOS

En las siguientes tablas se detallan los segmentos que se utilizaran en las distintas configuraciones de los dispositivos

5.30.1. MATRÍZ SAN CRISTÓBAL

Cantidad de direcciones de host requeridas	Dirección de red	Máscara de subred	Cantidad máxima de subredes posibles	En uso (Sí / No)	Nombre de la red
20	192.168.3.0	255.255.255.248	32	si	Matríz

Tabla 5-3 Matríz

Objetivo	DCE/DTE(si corresponde)	Velocidad de reloj	Nombre de la red	Dirección IP de la interfaz	Máscara de subred
UIO	DCE	64000	M_QUITO	192.168.0.12	255.255.255.252
MATRIZ	DTE		M_GYE	192.168.0.20	255.255.255.252
GYE	DCE	64000	GYE_UIO	192.168.0.16	255.255.255.252

Tabla 5-4 Matríz Direcciones

Ubicación: EDIFICIO PRINCIPAL 1ER PISO
Nombre del switch: SW_Matríz_Principal
Dirección IP del switch: 192.168.3.1



Descripción y objetivo	Velocidad	Duplex	Nombre de la red	Número de la red	Máscara de subred	VLAN	Tipo de puerto de switch	Encapsulamiento (en caso de ser necesario)
fastetherne t 0/1	100 MBS	FULL	Lan_matriz	192.168.3.1	224	0	ACCESS	dot1q 1
fastetherne t 0/2	100 MBS	FULL	Arch_central	192.168.3.2	224	1	ACCESS	dot1q 2
fastetherne t 0/3	100 MBS	FULL	gerencia	192.168.3.3	224	2	ACCESS	dot1q 3
fastetherne t 0/4	100 MBS	FULL	Dir_juridica	192.168.3.4	224	3	ACCESS	dot1q 4
fastetherne t 0/5	100 MBS	FULL	Dir_finan	192.168.3.5	224	4	ACCESS	dot1q 5
fastetherne t 0/6	100 MBS	FULL	Dir_admin	192.168.3.6	224	5	ACCESS	dot1q 6

fastetherne t 0/7	100 MBS	FULL	Rr_hh	192.168.3. 7	224	6	ACCESS	dot1q 7
fastetherne t 0/8	100 MBS	FULL	Cntr_resi	192.168.3. 8	224	7	ACCESS	dot1q 8
fastetherne t 0/9	100 MBS	FULL	Serv_inves t	192.168.3. 9	224	8	ACCESS	dot1q 9
fastetherne t 0/10	100 MBS	FULL	Contabilida d	192.168.3. 10	224	9	ACCESS	dot1q 10
fastetherne t 0/11	100 MBS	FULL	Com_socia	192.168.3. 11	224	10	ACCESS	dot1q 11
fastetherne t 0/12	100 MBS	FULL	Planificacio n	192.168.3. 12	224	11	ACCESS	dot1q 12

Tabla 5-5 Matriz Direcciones Lan

5.30.2. GUAYAQUIL

Cantidad de direcciones de host requeridas	Dirección de red	Máscara de subred	Cantidad máxima de subredes posibles	En uso (Sí / No)	Nombre de la red
6	192.168.1.0	255.255.255.248	32	 Sí	GYE

Tabla 5-6 Guayaquil

Objetivo	DCE/DTE(si corresponde)	Velocidad de reloj	Nombre de la red	Dirección IP de la interfaz	Máscara de subred
UIO	DCE	64000	M_QUITO	192.168.0.12	255.255.255.252
MATRIZ	DTE		M_GYE	192.168.0.20	255.255.255.252
GYE	DCE	64000	GYE_UIO	192.168.0.16	255.255.255.252

Tabla 5-7 Guayaquil Direcciones

Ubicación: EDIFICIO PRINCIPAL 1ER PISO
Nombre del switch: SW_Guayaquil
Dirección IP del switch: 192.168.1.1

Descripción y objetivo	Velocidad	Duplex	Nombre de la red	Número de la red	Máscara de subred	VLAN	Tipo de puerto de switch	Encapsulamiento (en caso de ser necesario)
fastethernet 0/1	100 MBS	FULL	Lan_Gye	192.168.1.1	248	0	ACCESS	dot1q 1
fastethernet 0/2	100 MBS	FULL	contabilidad	192.168.1.2	248	13	ACCESS	dot1q 2
fastethernet 0/3	100 MBS	FULL	admin	192.168.1.3	248	14	ACCESS	dot1q 3

Tabla 5-8 Guayaquil Direcciones Lan

5.30.3. QUITO

Cantidad de direcciones de host requeridas	Dirección de red	Máscara de subred	Cantidad máxima de subredes posibles	En uso (Sí / No)	Nombre de la red
6	192.168.1.0	255.255.255.248	32		UIO

Tabla 5-9 Quito

Objetivo	DCE/DTE(si corresponde)	Velocidad de reloj	Nombre de la red	Dirección IP de la interfaz	Máscara de subred
UIO	DCE	64000	M_QUITO	192.168.0.12	255.255.255.252
MATRIZ	DTE		M_GYE	192.168.0.20	255.255.255.252
GYE	DCE	64000	GYE_UIO	192.168.0.16	255.255.255.252

Tabla 5-10 Quito Direcciones

Ubicación: EDIFICIO PRINCIPAL 1ER PISO

Nombre del switch: SW_Quito

Dirección IP del switch: 192.168.4.1

Descripción y objetivo	Velocidad	Duplex	Nombre de la red	Número de la red	Máscara de subred	VLAN	Tipo de puerto de switch	Encapsulamiento (en caso de ser necesario)
fastethernet 0/1	100 MBS	FULL	Lan_Uio	192.168.4.1	248	0	ACCESS	dot1q 1
fastethernet 0/2	100 MBS	FULL	admin	192.168.4.2	248	15	ACCESS	dot1q 2

Tabla 5-11 Quito Direcciones Lan





CAPÍTULO 6 SEGURIDADES

6.1. INTRODUCCIÓN

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento.

Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

En este contexto, se ha elaborado este material. Con él se podrá facilitar las tareas de todos aquellos que se encuentran actualmente involucrados en las decisiones respecto de las redes de información y de sus modos de administración, al tiempo de alertar sobre la importancia crítica de la seguridad. Un adecuado tratamiento de esta problemática resulta absolutamente vital, debido a las amenazas cada vez mayores a las que la información se encuentra expuesta.

En el transcurso de las diversas secciones se desarrollarán básicamente, los siguientes temas:

El valor de los datos

Las políticas de seguridad informática

Los procedimientos para el resguardo de la información

Los principales ataques a las redes de información

Las passwords

Las herramientas de control y seguimiento de accesos



6.1.1. DEFINICIONES

Dado que se está tratando con conceptos que pueden tener múltiples interpretaciones, parece prudente acordar ciertos significados específicos. Por tanto, se ha recurrido a algunas definiciones, todas ellas extraídas del diccionario Espasa Calpe.

- . Seguridad: es “calidad de seguro”, y, seguro está definido como “libre de riesgo”.
- . Información: es “acción y efecto de informar”.
- . Informar: es “dar noticia de una cosa”.
- . Redes: es “el conjunto sistemático de caños o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin”.

Uniendo todas estas definiciones, se puede establecer qué se entiende por seguridad en redes.

Seguridad en Redes: es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin.

Si se trata de definir Seguridad en Redes con los elementos que se conocen, se puede llegar a una definición más acertada:

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

6.1.2. SEGURIDAD GLOBAL

¿Qué es una red global? El concepto de red global incluye todos los recursos informáticos de una organización, aún cuando estos no estén interconectados:

Redes de área local (LAN),
Redes de área metropolitana (MAN),
Redes nacionales y supranacionales (WAN),
Computadoras personales, minis y grandes sistemas.

De manera que, seguridad global es mantener bajo protección todos los componentes de una red global.

Al fin de cuentas, los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

Obtener de los usuarios la concientización de los conceptos, usos y costumbres referentes a la seguridad, requiere tiempo y esfuerzo. Que los usuarios se concienticen de la necesidad y, más que nada, de las ganancias que se obtienen implementando planes de seguridad, exige trabajar directamente con ellos, de tal manera que se apoderen de los beneficios de tener un buen plan de seguridad. (Por ejemplo: permite que se determine exactamente lo que debe hacer cada uno y cómo debe hacerlo, y, también las desviaciones que se pueden producir).

De esta forma, ante cualquier problema, es muy fácil determinar dónde se produjo o de dónde proviene. Para realizar esto, lo más usado, y que da muy buenos resultados es hacer “grupos de trabajo” en los cuales se informen los fines, objetivos y ganancias de establecer medidas de seguridad, de tal manera que los destinatarios finales se sientan informados y tomen para sí los conceptos. Este tipo de acciones favorece, la adhesión a estas medidas.

6.1.3. IMPLEMENTACIÓN

La implementación de medidas de seguridad, es un proceso técnico - administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Hay que tener muy en cuenta la complejidad que suma a la operatoria de la organización la implementación de estas medidas (ver párrafo “Impacto en la Organización”). Será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

También, como se ha mencionado anteriormente, es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

De todo lo expuesto anteriormente, resulta claro que proponer o identificar una política de seguridad requiere de un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.



6.2. POLÍTICAS GENERALES DE SEGURIDAD

6.2.1. ¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI)?

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes

Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que se desea proteger y el por qué de ello. Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

6.3. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

Como menciona el apartado anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

Objetivos de la política y descripción clara de los elementos involucrados en su definición.

Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

Definición de violaciones y de las consecuencias del no cumplimiento de la política.

Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales

que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes:

Crecimiento de la planta de personal,
Cambio en la infraestructura computacional, alta
Rotación de personal,
Desarrollo de nuevos servicios,
Cambio o diversificación de negocios
Otros.

6.3.1. ALGUNOS PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD

Si bien las características de la PSI que se ha mencionado hasta el momento, muestran una perspectiva de las implicaciones en la formulación de estas directrices, se revisara a continuación, algunos aspectos generales recomendados para la formulación de las mismas.

Considere efectuar un ejercicio de análisis de riesgos informáticos a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.

Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.

Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

Un último consejo: no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

6.3.2. PROPOSICIÓN DE UNA FORMA DE REALIZAR EL ANÁLISIS PARA LLEVAR A CABO UN SISTEMA DE SEGURIDAD INFORMÁTICA

Tal como puede visualizarse, en el gráfico están plasmados todos los elementos que intervienen para el estudio de una política de seguridad. Se comienza realizando una evaluación del factor humano interviniente teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad -, de los mecanismos con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), luego, el medio ambiente en que se desempeña el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las amenazas posibles. Una vez evaluado todo lo anterior, se origina un programa de seguridad, que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea. Luego, se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino.

6.3.3. ¿POR QUÉ LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA GENERALMENTE NO CONSIGUEN IMPLANTARSE?

Muchas veces, las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según algunos estudios resulta una labor ardua convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática. Muchos de los inconvenientes se inician por los tecnicismos informáticos y por la falta de una estrategia de mercadeo de los especialistas en seguridad que, llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad que, en muchos de los casos, lleva a comprometer su información sensible y por ende su imagen corporativa. Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe conocer las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir.

Una intrusión o una travesura pueden convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos. Luego, para que las PSI logren abrirse espacio en el interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su hacer diario, donde se identifiquen las necesidades y acciones que materializan las políticas. En este contexto, entender la organización, sus elementos culturales y comportamientos nos debe llevar a reconocer las pautas de seguridad necesarias y suficientes que aseguren confiabilidad en las

operaciones y funcionalidad de la compañía. A continuación, se mencionan algunas recomendaciones para concientizar sobre la seguridad informática:

Desarrolle ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de sus interlocutores.

Asocie el punto anterior a las estrategias de la organización y a la imagen que se tiene de la organización en el desarrollo de sus actividades.

Articule las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información.

Muestre una valoración costo-beneficio, ante una falla de seguridad.

Justifique la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización.

6.4. NIVELES DE TRABAJO

Confidencialidad

Integridad

Autenticidad

No Repudio

Disponibilidad de los recursos y de la información

Consistencia

Control de Acceso

Auditoria



6.4.1. CONFIDENCIALIDAD

Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

6.4.2. INTEGRIDAD

Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

· Causadas por errores de hardware y/o software.

· Causadas de forma intencional.

· Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

6.4.3. AUTENTICIDAD

En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

6.4.4. NO REPUDIO

Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede robar que, en efecto, el mensaje fue enviado y viceversa.

6.4.5. DISPONIBILIDAD DE LOS RECURSOS Y DE LA INFORMACIÓN

De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

6.4.6. CONSISTENCIA

Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

6.4.7. CONTROL DE ACCESO A LOS RECURSOS

Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

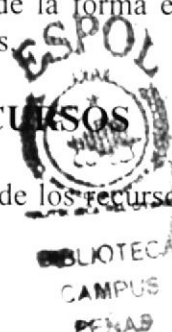
6.4.8. AUDITORÍA

Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre “espiar” y “monitorear” a los mismos. La ética es algo que todo buen administrador debe conocer y poseer.

Finalmente, todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios.

De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan sus derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales.



6.4.9. ALGORITMO

Cuando se piensa establecer una estrategia de seguridad, la pregunta que se realiza, en primera instancia, es: ¿en qué baso mi estrategia?. La respuesta a esta pregunta es bien simple. El algoritmo Productor/Consumidor. En este algoritmo, hay dos grandes entidades: una que es la encargada de producir la información; la otra entidad es el consumidor de esta información y otra, llamada precisamente “otros”. Entre el productor y el consumidor, se define una relación que tiene como objetivo una transferencia de “algo” entre ambos, sin otra cosa que intervenga en el proceso. Si esto se logra llevar a cabo y se mantiene a lo largo del tiempo, se estará en presencia de un sistema seguro.

En la realidad, existen entidades y/o eventos que provocan alteraciones a este modelo.

El estudio de la seguridad, en pocas palabras, se basa en la determinación, análisis y soluciones de las alteraciones a este modelo.

En una observación y planteo del modelo, determina que sólo existen cuatro tipos de alteraciones en la relación producción-consumidor (ver el gráfico del algoritmo) Antes de pasar a explicar estos casos, habrá que definir el concepto de “recurso”.

Recurso, está definido en el diccionario Espasa Calpe como “bienes, medios de subsistencia”. Esta es una definición muy general.

De todas maneras, resulta conveniente para esta tarea. Cabe mencionar como recurso a cualquier cosa, ya sean bienes específicos o que permitan la subsistencia de la organización como tal. Debido a ello, es que se puede diferenciar claramente tres tipos de recursos:

- . Físicos
- . Lógicos
- . Servicios.



Los recursos físicos son, por ejemplo, las impresoras, los servidores de archivos, los routers, etc.

Los recursos lógicos son, por ejemplo, las bases de datos de las cuales se extrae la información que permite trabajar en la organización.

Los servicios son, por ejemplo, el servicio de correo electrónico, de página WEB, etc. Todas las acciones correctivas que se lleven a cabo con el fin de respetar el modelo estarán orientadas a atacar uno de los cuatro casos. Explica y da ejemplos de cada uno de ellos.

El caso número uno es el de **Interrupción**. Este caso afecta la disponibilidad del recurso (tener en cuenta la definición de recurso: físico, lógico y servicio). Por ejemplo:

Por ejemplo:

Recurso afectado	Nombre	Causa	Efecto
Servicio	Correo electrónico	Alguien dio de baja el servidor (por algún método)	No poder enviar mail
Físico	Impresora	Falta de alimentación eléctrica.	No imprime

Figura 6-1 Interrupción

El segundo caso es el de **Intercepción**, en el cual se pone en riesgo la privacidad de los datos.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Datos sobre cuentas en el banco	Se ha puesto un dispositivo que permite monitorear los paquetes en la red y sacar información de ellos.	Conseguir datos privados sobre montos de cuentas corrientes
Servicio	Correo electrónico	Se ha implantado un programa que duplica los mensajes (mails) que salen de una sección y los envía a una dirección.	Leer información

Figura 6-2 Intercepción

El tercer caso, **Modificación** afecta directamente la integridad de los datos que le llegan al consumidor.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Base de datos de pagos en cuentas corrientes	Se ha implantado un programa que redondea en menos los pagos y carga éstos redondeos a una cuenta corriente	Incrementar el crédito de una cuenta corriente en base al redondeo realizado en los pagos
Servicio	Servidor de página WEB	Alguien logró ingresar como WEBMASTER y ha cambiado los contenidos de la página	Los datos mostrados en la página no son los reales

Figura 6-3 Modificación

6.5. ACERCA DE LOS PROCEDIMIENTOS

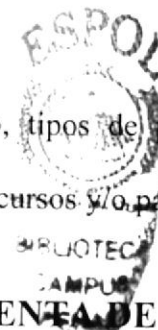
Si se piensa certificar ISO, es indispensable tener un manual de procedimientos escrito y llevarlo a cabo al pie de la letra. De esta manera, cabría pensar que un manual de procedimientos es un paso adelante para poder llegar a la certificación ISO.

6.5.1. PROCEDIMIENTO DE ALTA DE CUENTA DE USUARIO

Cuando un elemento de la organización requiere una cuenta de operación en el sistema, debe llenar un formulario que contenga, al menos los siguientes datos:

- . Nombre y Apellido
 - . Puesto de trabajo
 - . Jefe inmediato superior que avale el pedido
 - . Descripción de los trabajos que debe realizar en el sistema
 - . Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de “buen uso de los recursos” (para lo cual, se le debe dar una copia de tales normas).
 - . Explicaciones breves, pero claras de cómo elegir su password.
- Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:

- . Tipo de cuenta
 - . Fecha de caducidad
 - . Fecha de expiración
 - . Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y/o archivos)
- Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.



6.5.2. PROCEDIMIENTO DE BAJA DE CUENTA DE USUARIO

Este procedimiento es el que se lleva a cabo cuando se aleja un elemento de la organización o cuando alguien deja de trabajar por un determinado tiempo (licencia sin goce de sueldo, vacaciones, viajes prolongados, etc.). En base a la explicación anterior hay, entonces, dos tipos de alejamientos: permanente y parcial. Aquí, es necesario definir un circuito administrativo a seguir, y que como todos los componentes de la política de seguridad, debe estar fuertemente apoyado por la parte gerencial de la organización. Un ejemplo de este circuito, podría ser: ante el alejamiento de un elemento de la organización, la gerencia de personal (o la sección encargada de la administración de los RRHH), debe informar en un formulario de “Alejamiento de personal”, todos los datos del individuo que ha dejado la organización, así como de la posición que éste ocupaba y el tipo de alejamiento (permanente o no).

Una vez llegada la información al departamento encargado de la administración de sistemas, se utiliza para dar de baja o inhabilitar la cuenta del usuario. La definición de si se da de baja o se inhabilita es algo importante pues, si se da de baja, se deberían guardar y eliminar los archivos y directorios del usuario, mientras que si sólo se inhabilita, no pasa de esa acción. Si el alejamiento del individuo no era permanente, al volver a la organización, la sección que había informado anteriormente de la ausencia,

debe comunicar su regreso, por medio de un formulario dando cuenta de tal hecho para volver a habilitar la cuenta al individuo.

6.5.3. PROCEDIMIENTO PARA DETERMINAR LAS BUENAS PASSWORDS

Aunque no lo parezca, la verificación de palabras claves efectivas no es algo frecuente en casi ninguna organización. El procedimiento debe explicar las normas para elegir una password:

Se debe explicitar:

La cantidad de caracteres mínimo que debe tener,

No tiene que tener relación directa con las características del usuario.

Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.

Determinar, si es posible, el seguimiento de las palabras claves (llevar registros de las palabras claves anteriores elegidas por el usuario). Una vez que el usuario ha elegido su password, se le debe correr un “programa crackeador” para tener idea de cuán segura es, en base al tiempo que tarda en romper la palabra.

6.5.4. PROCEDIMIENTOS DE VERIFICACIÓN DE ACCESOS

Debe explicar la forma de realizar las auditorías de los archivos lógicos de ingresos a fin de detectar actividades anómalas. También debe detectar el tiempo entre la auditoría y cómo actuar en caso de detectar desviaciones.

Normalmente, este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos de “log” con diferentes fechas tomando en cuenta las reglas que se le han dado.

Ante la detección de un desvío, generan reportes informando al mismo. En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas y cómo se actúa cuando se generan alarmas.

6.5.5. PROCEDIMIENTO PARA EL CHEQUEO DEL TRÁFICO DE LA RED

Permite conocer el comportamiento del tráfico en la red, al detectar variaciones que pueden ser síntoma de mal uso de la misma. El procedimiento debe indicar el/los programas que se ejecuten, con qué intervalos, con qué reglas de trabajo, quién se encarga de procesar y/o monitorear los datos generados por ellos y cómo se actúa en consecuencia.

6.5.6. PROCEDIMIENTO PARA EL MONITOREO DE LOS VOLÚMENES DE CORREO

Este procedimiento permite conocer los volúmenes del tráfico de correo o la cantidad de “mails” en tránsito. Dicho procedimiento se encuentra realizado por programas que llevan las estadísticas, generando reportes con la información pedida.

El conocimiento de esta información permite conocer, entre otras cosas, el uso de los medios de comunicación, y si el servidor está siendo objeto de un “spam”.

Como en los casos anteriores, en el procedimiento debe estar explicitado quién es el encargado del mantenimiento y del análisis de los datos generados, y qué hacer cuando se detectan variaciones.

6.5.7. PROCEDIMIENTOS PARA EL MONITOREO DE CONEXIONES ACTIVAS

Este procedimiento se efectúa con el objeto de prevenir que algún usuario deje su terminal abierta y sea posible que alguien use su cuenta. El procedimiento es ejecutado por medio de programas que monitorean la actividad de las conexiones de usuarios.

Cuando detecta que una terminal tiene cierto tiempo inactiva, cierra la conexión y genera un log con el acontecimiento.

6.5.8. PROCEDIMIENTO DE MODIFICACIÓN DE ARCHIVOS

Este procedimiento sirve para detectar la modificación no autorizada y la integridad de los archivos y, en muchos casos, permite la traza de las modificaciones realizadas. Al igual que en los casos anteriores, debe estar bien determinada la responsabilidad de quién es el encargado del seguimiento y de actuar en caso de alarmas.

6.5.9. PROCEDIMIENTOS PARA EL RESGUARDO DE COPIAS DE SEGURIDAD

Este procedimiento debe indicar claramente dónde se deben guardar las copias de seguridad y los pasos a seguir en caso de problemas. Para lograr esto, deben estar identificados los roles de las personas que interactúan con el área, a fin de que cada uno sepa qué hacer ante la aparición de problemas.



6.5.10. PROCEDIMIENTOS PARA LA VERIFICACIÓN DE LAS MÁQUINAS DE LOS USUARIOS

Este procedimiento permitirá encontrar programas que no deberían estar en las máquinas de los usuarios y que, por su carácter, pueden traer problemas de licencias y fuente potencial de virus. El procedimiento debe explicitar los métodos que se van a utilizar para la verificación, las acciones ante los desvíos y quién/quienes lo llevarán a cabo.

6.5.11. PROCEDIMIENTOS PARA EL MONITOREO DE LOS PUERTOS EN LA RED

Este procedimiento permite saber qué puertos están habilitados en la red, y, en algunos casos, chequear la seguridad de los mismos.

El procedimiento deberá describir qué programas se deben ejecutar, con qué reglas, quién estará a cargo de llevarlo a cabo y qué hacer ante las desviaciones detectadas.

6.5.12. PROCEDIMIENTOS DE CÓMO DAR A PUBLICIDAD LAS NUEVAS NORMAS DE SEGURIDAD

Este tipo de procedimiento no siempre es tenido en cuenta. Sin embargo, en una organización es muy importante conocer las últimas modificaciones realizadas a los procedimientos, de tal manera que nadie pueda poner cómo excusa “que no conocía las modificaciones”.

En él, debe describirse la forma de realizar la publicidad de las modificaciones: puede ser mediante un mailing, por exposición en transparencias, por notificación expresa, etc.; quién estará a cargo de la tarea y las atribuciones que tiene.

Es fundamental tener en cuenta este último punto ya que un porcentaje de los problemas de seguridad, según está demostrado en estudios de mercado, proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios.

6.5.13. PROCEDIMIENTOS PARA LA DETERMINACIÓN DE IDENTIFICACIÓN DE USUARIO Y GRUPO DE PERTENENCIA POR DEFECTO

Este procedimiento determina la forma de establecer las identificaciones y los grupos a los que pertenecerán los usuarios por defecto en el momento de darlos de alta. En él deben explicarse, concisamente, los pasos a seguir para cambiar los derechos y las identificaciones de los usuarios dados de alta y la manera de documentar los mismos, así también como quién será responsable de la tarea.

6.5.14. PROCEDIMIENTOS PARA RECUPERAR INFORMACIÓN



Este procedimiento sirve para reconstruir todo el sistema o parte de él, a partir de las copias de seguridad. En él, deben explicarse todos los pasos a seguir para rearmar el sistema a partir de los back-up existentes, así como cada cuánto tiempo habría que llevarlos a cabo y quiénes son los responsables de dicha tarea.

6.5.15. CHECK-LISTS

Las check-lists, como su nombre lo indica, son listas con un conjunto de ítems referentes a lo que habría que chequear en el funcionamiento del sistema.

Algunos ejemplos de check-lists:

Asegurar el entorno. ¿Qué es necesario proteger? ¿Cuáles son los riesgos?

Determinar prioridades para la seguridad y el uso de los recursos.

Crear planes avanzados sobre qué hacer en una emergencia.

Trabajar para educar a los usuarios del sistema sobre las necesidades y las ventajas de la buena seguridad

Estar atentos a los incidentes inusuales y comportamientos extraños.

Asegurarse de que cada persona utilice su propia cuenta.

¿Están las copias de seguridad bien resguardadas?

No almacenar las copias de seguridad en el mismo sitio donde se las realiza

¿Los permisos básicos son de sólo lectura?

Sí se realizan copias de seguridad de directorios/archivos críticos, usar chequeo de comparación para detectar modificaciones no autorizadas.

Periódicamente rever todo los archivos de “booteo de los sistemas y los archivos de configuración para detectar modificaciones y/o cambios en ellos.

Tener sensores de humo y fuego en el cuarto de computadoras.

Tener medios de extinción de fuego adecuados en el cuarto de computadoras.

Entrenar a los usuarios sobre qué hacer cuando se disparan las alarmas.

Instalar y limpiar regularmente filtros de aire en el cuarto de computadoras.

Instalar UPS, filtros de línea, protectores gaseosos al menos en el cuarto de computadoras.

Tener planes de recuperación de desastres.

Considerar usar fibras ópticas como medio de transporte de información en la red.

Nunca usar teclas de función programables en una terminal para almacenar información de login o password.

Considerar realizar autolog de cuentas de usuario.

Concientizar a los usuarios de pulsar la tecla ESCAPE antes de ingresar su login y su password, a fin de prevenir los “Caballos de Troya”.

Considerar la generación automática de password.

Asegurarse de que cada cuenta tenga un password.

No crear cuentas por defecto o “guest” para alguien que está temporalmente en la organización.

No permitir que una sola cuenta esté compartida por un grupo de gente.

Deshabilitar las cuentas de personas que se encuentren fuera de la organización por largo tiempo.

Deshabilitar las cuentas “dormidas” por mucho tiempo.

Deshabilitar o resguardar físicamente las bocas de conexión de red no usadas.

Limitar el acceso físico a cables de red, routers, bocas, repetidores y terminadores.

Los usuarios deben tener diferentes passwords sobre diferentes segmentos de la red.

Monitorear regularmente la actividad sobre los gateways.

6.6. TIPOS DE ATAQUES Y VULNERABILIDADES

6.6.1. NEGACIÓN DE SERVICIO (*DENIAL OF SERVICE*)

En el presente apartado, se describirán los modos de ataques que podrían ocurrir más frecuentemente en las redes de información.

Debido a la pérdida de dinero y de tiempo que estos ataques pueden ocasionar, se presentarán también algunas formas de prevención y de respuesta a los mismos.

6.6.2. ¿QUÉ ES “DENIAL OF SERVICE”? DESCRIPCIÓN DE ATAQUES.

Denial of service es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos. Algunos ejemplos de este tipo de ataque son:

- . Tentativas de “floodear” (inundar) una red, evitando de esta manera el tráfico legítimo de datos en la misma.
- . Tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio.
- . Tentativas de evitar que una determinada persona tenga acceso a un servicio.
- . Tentativas de interrumpir un servicio específico a un sistema o a un usuario.

Cabría tener en cuenta que, el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Por ejemplo, un “hacker” puede utilizar un área del FTP anónimo como lugar para salvar archivos, consumiendo, de esta manera, espacio en el disco y generando tráfico en la red.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar inoperativa una computadora o una red.

De esta forma, toda una organización puede quedar fuera de Internet durante un tiempo determinado.

6.6.3. MODOS DE ATAQUE

Algunos ataques de negación de servicio se pueden ejecutar con recursos muy limitados contra un sitio grande y sofisticado. Este tipo de ataque se denomina “ataque asimétrico”. Por ejemplo, un atacante con una vieja PC y un módem puede poner fuera de combate a máquinas rápidas y sofisticadas. Últimamente, esto es común con ataques de los denominados “nukes” en los cuales caen instalaciones grandes, por ejemplo, de clusters Windows NT.

Hay tres tipos de ataques básicos de negación de servicios:

Consumo de recursos escasos, limitados, o no renovables
Destrucción o alteración de información de configuración
Destrucción o alteración física de los componentes de la red



6.6.4. CONSUMO DE RECURSOS ESCASOS, LIMITADOS, O NO RENOVABLES

Las computadoras y las redes necesitan para funcionar ciertos recursos: ancho de banda de la red, espacio de memoria y disco, tiempo de CPU, estructuras de datos, acceso otras computadoras y redes, entre otros.

6.6.4.1. CONECTIVIDAD

Los ataques de Negación de servicio se ejecutan, con frecuencia, contra la conectividad de la red. La meta del hacker es evitar que las computadoras se comuniquen en la red. Un ejemplo de este tipo de ataque es el “SYN flood” : En este tipo de ataque, el hacker comienza el proceso de establecer una conexión TCP a la máquina de la víctima, pero lo hace de manera tal que evita que la conexión se complete. En este tiempo, la máquina del atacado ha reservado uno entre un número limitado de las estructuras de datos requeridas para terminar la conexión inminente. El resultado es que las conexiones legítimas se rechazan mientras que la máquina del atacado se queda esperando para terminar esas falsas conexiones “medio abiertas”.

Debe tenerse en cuenta que este tipo de ataque no depende del ancho de banda que disponga el atacante. En este caso, el hacker está consumiendo las estructuras de datos del kernel, implicadas en establecer una conexión TCP. Un hacker con una simple conexión dial-up puede realizar este ataque contra una poderosa Workstation (este último es un buen ejemplo de un ataque asimétrico).

6.6.4.2. APROVECHAMIENTO DE LOS RECURSOS DEL OTRO

Un hacker también puede utilizar los recursos que usted dispone contra usted mismo, de maneras inesperadas. Por ejemplo, el caso de Negación de servicio UDP. En este ataque, el hacker utiliza los paquetes “falsificados” de UDP para conectar el servicio de generación de eco en una máquina con el servicio de chargen en otra máquina. El resultado es, que los dos servicios consumen todo el ancho de banda de red entre ellos. Así, la conectividad para todas las máquinas en la misma red desde cualquiera de las máquinas atacadas se ve afectada.

6.6.4.3. CONSUMO DE ANCHO DE BANDA

Un hacker puede, también, consumir todo el ancho de banda disponible en su red generando una gran cantidad de paquetes dirigidos a la misma. Típicamente, estos paquetes son de generación de eco de ICMP (ping), pero pueden ser cualquier otra cosa. Además, el hacker no necesita operar desde una sola máquina; él puede coordinar varias máquinas en diversas redes para alcanzar el mismo efecto.

6.6.4.4. CONSUMO DE OTROS RECURSOS

Además del ancho de banda de la red, los hackers pueden consumir otros recursos que su sistema necesite para funcionar. Por ejemplo, en muchos sistemas, un número limitado de las estructuras de datos en el kernel está disponible para almacenar información de procesos (identificadores, entradas en tablas de procesos, slots, etc.). Un hacker puede consumir estas estructuras de datos escribiendo un programa o un script que no haga nada pero que cree en varias ocasiones copias de sí mismo. Muchos sistemas operativos modernos, aunque no la totalidad de ellos, tienen recursos para protegerse contra este problema.

Además, aunque las tablas de procesos no se llenen, se consume CPU por la gran cantidad de procesos y conmutación entre los mismos. Un hacker puede también consumir su espacio en disco de otras maneras, por ejemplo:

- . Generar miles de mails (Spam, Bombing).
 - . Generar intencionalmente errores que deben ser logueados.
- En este tipo de ataque, se cita también la utilización indebida del syslog en unix. Es decir, utilizar el proceso syslog de la víctima para que registre eventos de otra máquina, llenando el espacio en disco con el archivo de syslog. Colocar archivos en su disco, utilizando ftp anónimo.

En general, se puede utilizar cualquier cosa que permita que los datos sean escritos en su disco para ejecutar un ataque de negación de servicio si no hay límites en la cantidad de datos que se pueden escribir (quotas).

No obstante, muchos sitios tienen esquemas de “lockout” de cuenta después de un cierto número de logins fallados. Un setup típico bloquea el login después de 3 o 5 tentativas falladas.

Un hacker puede utilizar este esquema para evitar que los usuarios legítimos entren. En algunos casos, incluso las cuentas privilegiadas, tales como root o administrador, pueden ser víctimas de este tipo de ataque.

Recuerde: siempre disponga de un método para acceder ante la emergencia de este tipo de ataques.

Un hacker puede hacer caer su sistema o ponerlo inestable, enviando datos inesperados. Un ejemplo de tal ataque es el “ping flood” o Pings de tamaño demasiado grande. Si su sistema está experimentando caídas frecuentes sin causa evidente, podría deberse a este tipo de ataque.

Hay otros componentes que pueden ser vulnerables a la negación de servicio y que deben vigilar se. Estos incluyen:

Impresoras

Unidades de cinta

Conexiones de red

Otros recursos limitados importantes para la operación de su sistema.

6.6.5. DESTRUCCIÓN O ALTERACIÓN DE LA INFORMACIÓN DE CONFIGURACIÓN

Una computadora incorrectamente configurada puede no funcionar bien o directamente no arrancar. Un hacker puede alterar o destruir la información de configuración de su sistema operativo, evitando de esta forma que usted use su computadora o red.

Vea algunos ejemplos:

Si un hacker puede cambiar la información de ruteo de sus routers, su red puede ser deshabilitada.

Si un hacker puede modificar la registry en una máquina Window NT, ciertas funciones pueden ser imposibles de utilizar, o directamente el sistema puede no volver a bootear.



6.6.6. DESTRUCCIÓN O ALTERACIÓN FÍSICA DE LOS COMPONENTES DE LA RED

Es muy importante la seguridad física de la red. Se debe resguardar contra el acceso no autorizado a las computadoras, los routers, los racks de cableado de red, los segmentos del backbone de la red, y cualquier otro componente crítico de la red.

6.6.7. PREVENCIÓN Y RESPUESTA

Tal como se ha expresado anteriormente, los ataques de Negación de servicio pueden dar lugar a pérdidas significativas de tiempo y dinero para muchas organizaciones, por lo que se recomiendan una serie de medidas:

Coloque access lists en los routers. Esto reducirá su exposición a ciertos ataques de negación de servicio

Instale patches a su sistema operativo contra flooding de TCP SYN. Esta acción permitirá reducir sustancialmente su exposición a estos ataques aunque no pueda eliminar el riesgo en forma definitiva.

Invalide cualquier servicio de red innecesario o no utilizado. Esto puede limitar la capacidad de un hacker de aprovecharse de esos servicios para ejecutar un ataque de negación de servicio. Por ejemplo: chargen, Echo, etc.

Si su sistema operativo lo permite, implemente sistemas de cuotas. Por ejemplo, si su sistema operativo soporta "disk Quotas" impleméntelo para todos los logins.

Si su sistema operativo soporta partición o volúmenes, separe lo crítico de lo que no lo es.

Observe el funcionamiento del sistema y establezca valores base para la actividad ordinaria. Utilice estos valores para calibrar niveles inusuales de la actividad del disco, del uso de la CPU, o del tráfico de red.

Incluya como parte de su rutina, el examen de su seguridad física. Considere, entre otras cosas, los servidores, routers, terminales desatendidas, ports de acceso de red y los gabinetes de cableado.

Utilice Tripwire o una herramienta similar para detectar cambios en la información de configuración u otros archivos.

Trate de utilizar configuraciones de red redundantes y fault-tolerant.



6.7. CRACKING DE PASSWORDS

En este apartado, se presentarán una serie de consideraciones referidas al "cracking de passwords".

El objetivo inicial consiste en entrar al server. Para ello, se procede como si se tratase de una máquina remota (telnet). Pero, debido a que se permite el acceso a múltiples usuarios, los sistemas nos solicitarán un nombre de identificación acompañado de una clave. Dicho nombre darse de alta en el sistema para que se pueda acceder. Cuando un usuario desea entrar en una máquina, el sistema solicitará:

Un login de acceso o nombre de usuario. Si el login es incorrecto, el sistema no lo notificará para impedirle conocer qué accesos se encuentran dados de alta.

Una password o palabra clave. Si la password coincide con la que tiene asignada el login que se emplea, el sistema permitirá el acceso.

6.7.1.1. DESCUBRIR UNA PASSWORD

Una vez encriptada una password, no se puede desencriptar. Sin embargo, esto no garantiza la seguridad de la password, puesto que no significa que la password no se pueda averiguar.

El mecanismo que se utiliza para descubrir (no desenscriptar) las passwords consiste en efectuar encriptaciones de palabras (posibles passwords) y comparar estas encriptaciones con el original.

Los programas buscadores de contraseñas son fácilmente diseñables. Si mediante un “bug” se obtiene el archivo /passwd, se puede iniciar un ataque de diccionario contra el mismo obteniéndose, de este modo, las passwords.

Otro tipo de ataque es el de “fuerza bruta”, que consiste simplemente en realizar todas las combinaciones posibles de caracteres hasta hallar la password. En el siguiente cuadro puede ver el tiempo de búsqueda de una password de acuerdo a la longitud y tipo de caracteres utilizados. Se supone una velocidad de búsqueda de 100.000 passwords por segundo.

En el siguiente cuadro puede ver el tiempo de búsqueda de una password de acuerdo a la longitud y tipo de caracteres utilizados. Se supone una velocidad de búsqueda de 100.000 passwords por segundo.

Long. En caracteres	26 letras (minúsculas)	36 letras y dígitos	52 (mayúsculas y minúsculas)	96 Todos los caracteres
6	50 minutos	6 horas	2.2 días	3 meses
7	22 horas	9 días	4 meses	23 años
8	24 días	10.5 meses	17 años	2287 años
9	21 meses	32.6	881 años	219.000 años
10	45 años	1159 años	45.838 años	21 millones de años

Figura 6-4 Tiempos De Búsquedas

6.7.2. E-MAIL BOMBING Y SPAMMING

En este apartado, se presentarán algunas de las dificultades que pueden surgir como consecuencia de la utilización de los servicios de mail. Se brindarán, por otro lado, algunas respuestas a dichos obstáculos.

6.7.2.1. DESCRIPCIÓN

El e-mail bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el mailbox del destinatario.

El spamming,, que es una variante del e-mail bombing, se refiere a enviar el email a centenares o millares de usuarios e, inclusive, a listas de interés.

El Spamming puede resultar aún más perjudicial si los destinatarios contestan el mail, haciendo que todos reciban la respuesta.

Puede, además, ocurrir inocentemente como resultado de enviar un mensaje a la lista y no darse cuenta de que la lista lo distribuye a millares de usuarios, o como resultado de mala configuración de un autorespondedor, por ejemplo el “vacation”. El e-mail bombing/spamming se puede combinar con el e-mail spoofing que altera la identidad de la cuenta que envía el mail -, logrando que sea más difícil determinar quién está enviando realmente el mail.

6.7.2.2. DETALLES TÉCNICOS

Cuando se proveen los servicios de e-mail los usuarios son, lógicamente, vulnerables al e-mail bombing y spamming.

En efecto, el e-mail spamming es casi imposible de prevenir. Un usuario con una dirección válida de mail puede realizar " Spam " a cualquier otra dirección de mail, newsgroup, o sistema de BBS.

Cuando gran cantidad de mails son dirigidos a un solo sitio, éste puede sufrir "denial of service" por pérdida de conectividad, caerse el sistema o producirse fallas en el servicio debido a:

Sobrecarga de conexiones de red;

Utilización de todos los recursos de sistema disponibles;

Llenado del disco como resultado de postings múltiples y de entradas en el "syslog".

6.7.2.3. ¿CÓMO PROCEDER?

Detección

Si un sistema aparece repentinamente lento (el e-mail es lento o no parece ser enviado o recibido), la razón puede ser que su mailer está intentando procesar una excesiva cantidad de mensajes. Esto puede comprobarse a través del "log" de sistema.

Reacción

Es importante:

Identificar la fuente del e-mail bomb/spam y configure su router para evitar el acceso de los paquetes entrantes de esa dirección. Puede colocar un "access list" en el port 25 (SMTP) del tipo "established" para esa dirección.

Observar los "headers" del e-mail para determinar su origen verdadero.

Ponerse en contacto con el sitio que usted identificó en su revisión con el propósito de alertarlos de la actividad del spammer.

Asegurarse de tener la versión mas actualizada del "daemon" de mail (por ejemplo sendmail) y aumente el grado de "debug" o "log" que posea el proceso, para detectar o alertar estas actividades. Tenga la precaución de vigilar el tamaño del archivo de log, que puede crecer considerablemente, si se esta bajo un e-mail-bombing.

Prevención

Desafortunadamente, hasta el momento, no hay manera de prevenir el bombardeo de e-mail o spamming y es imposible predecir el origen del ataque siguiente. Es trivial obtener acceso a listas de interés o acceder a información que contenga grandes volúmenes de direcciones de e-mail, las que proporcionan al atacante direcciones de destino para el spam.



Pueden desarrollarse herramientas internas, que pueden ayudar a reconocer y a responder al e-mail bombing/spamming reduciendo, de esta manera, el impacto de tal actividad. Tales herramientas deben aumentar las capacidades de log y alertar de mensajes que vienen de un mismo lugar en un corto período de tiempo.

Asimismo, deberían ser capaces de rechazar esos mensajes, o descartarlos. Si un sitio utiliza un número pequeño de servidores de e-mail, podría configurarse un "firewall" para asegurarse de que las conexiones de "smtp" fuera de su firewall puedan hacerse solamente a sus "hubs" de mail y a ninguno de los otros equipos.

Aunque esta operación no prevendrá un ataque, reduce al mínimo el número de las máquinas disponibles para un ataque basado en SMTP. De este modo, se puede controlar el tráfico entrante SMTP y filtrarlo de manera acorde.

Recuerde: no conteste y/o haga un forward de los Spams. De este modo evitará que el problema se propague.

6.8. PROBLEMAS DE SEGURIDAD EN EL FTP

6.8.1. EL COMANDO PORT

En los últimos años, se ha incrementado el debate en torno a los problemas relacionados con el comando PORT del protocolo del FTP. Estos problemas se basan en el uso erróneo de dicho comando.

6.8.2. EL PROTOCOLO FTP

Para entender estos ataques, es necesario tener una comprensión básica del protocolo FTP.

Un cliente abre una conexión al port de control de ftp (21) de un FTP SERVER. De este modo, para que el servidor sea capaz luego de enviar datos de nuevo a la máquina del cliente, una segunda conexión (de datos) debe abrirse entre el servidor y el cliente. Para hacer esta segunda conexión, el cliente envía un comando PORT al servidor.

Este comando incluye parámetros que indican al servidor cuál IP ADDRESS conectar y qué port abrir en aquella dirección.

El servidor luego abre aquella conexión, siendo la fuente de la conexión el port 20 del servidor y el destino el port identificado en los parámetros del comando PORT.

El comando PORT se utiliza generalmente sólo en el " modo activo " del ftp (por default). No se suele utilizar en modo pasivo (PASV). Debe notarse que los servidores de ftp generalmente implementan ambos modos en ejecución, y el cliente especifica qué método utilizar.

6.8.3. EL ATAQUE "FTP BOUNCE"

Conforme con el protocolo FTP, el comando PORT hace que la máquina que lo origina especifique una máquina de destino y un port arbitrarios para la conexión de datos.

Sin embargo, esto también significa que un hacker puede abrir una conexión un port del hacker eligiendo una máquina que puede no ser el cliente original.

Hacer esta conexión a una máquina arbitraria es hacer un ataque “ftp bounce”. Con fines ilustrativos, se presentan seguidamente varios ejemplos de cómo los hackers pueden utilizar el “ftp bounce”.

6.8.3.1. “SCANNING” DE PORTS

Un hacker que desea realizar una port scan contra un sitio puede hacerlo de un server FTP de un tercero, que actúa como un “puente” para el scan. El sitio de la víctima ve la exploración como procedente del server FTP más que de la fuente verdadera (el cliente FTP).

Bajo algunas circunstancias, esta técnica ofrece al hacker más ventajas que ocultar la fuente verdadera de la prueba.

Cuando el sitio previsto de la víctima está en la misma subnet que el server FTP server, o cuando no filtra tráfico del server FTP, el hacker puede utilizar la máquina del servidor como la fuente del port scan más que la máquina del cliente, desviando de esta manera los controles de acceso que de otra manera se aplicarían.

6.8.3.2. “BYPASS” DE DISPOSITIVOS BÁSICOS DE FILTRADO DE PAQUETES.

Un hacker puede realizar un “bypass” de un firewall en ciertas configuraciones de red. Por ejemplo, suponga que un sitio tiene su servidor de FTP anónimo detrás del firewall. Usando la técnica de port scan, un hacker determina que un web Server interno en ese sitio está disponible en el acceso 8080, un port normalmente bloqueado por un firewall. Conectándose al server FTP público del sitio, el hacker inicia una conexión entre el server FTP y un port arbitrario, en una máquina no pública del sitio (por ejemplo el web server interno en el port 8080). Como resultado, el hacker establece una conexión a una máquina que sería protegida de otra manera por el firewall.

6.8.3.3. BYPASS DE DISPOSITIVOS DE FILTRADO DINÁMICOS

Otro problema se refiere a los sitios que tienen firewalls que utilizan filtros dinámicos para protegerse. Los sitios están abiertos al ataque porque el firewall confía en la información que recibe.

En este ejemplo, el sitio de la víctima contiene todos sus sistemas detrás de un firewall que utiliza los filtros dinámicos. Una persona en el sitio de la víctima hojea las páginas de la Web y baja un Java applet construido por el hacker. Sin el conocimiento de esa persona, el Java applet abre una conexión de salida de ftp a la máquina del hacker. El applet entonces publica un comando PORT de ftp, ordenando a la máquina del servidor abrir una conexión a, por ejemplo, el port telnet que de otra manera se encontraba protegido detrás del firewall.

Como el firewall de filtros dinámicos examina los paquetes de salida para determinar si alguna acción se requiere de su parte, observa el comando PORT y permite una conexión entrante del server web remoto al port del telnet en la máquina de la víctima. Esta conexión normalmente no es permitida por el firewall; fue permitida en este caso porque el comando PORT fue realizado por el cliente.

6.9. SOLUCIONES

Los ataques de los ejemplos demuestran el componente base de la vulnerabilidad: los contenidos del comando PORT del ftp no son tan dignos de confianza mientras están bajo control de un potencial atacante.

El ejemplo del “ftp bounce” demuestra qué sucede cuando un servidor confía en la información. El ejemplo del filtro dinámico demuestra qué sucede cuando un firewall confía en la información.

6.9.1. SOFTWARE DEL FTP SERVER

La mejor solución al problema del “ftp bounce” desde la perspectiva de la seguridad es asegurarse de que el software del server FTP no puede establecer conexiones a máquinas arbitrarias.

Sin embargo, los sitios que confían en el comportamiento “RFC-compliant” pueden encontrar que el implementar esta solución afectará las aplicaciones que ellos utilizan. Por lo tanto, muchos vendedores ofrecen soluciones que permiten al sitio dar servicio de ftp adaptado a las necesidades del cliente.

Las implementaciones del vendedor caen en tres grupos:

1) conformidad estricta con funciones del RFC: el comando PORT se puede utilizar para conectar directamente con una máquina de una tercera persona, y ésta es la única funcionalidad permitida. Algunos vendedores que eligen mantener conformidad estricta, han tratado este problema modificando el resto de los servicios de red para rechazar las conexiones que se originaban en el port de datos del ftp (port:20).

2) supresión estricta del comando PORT: el comando PORT puede ser utilizado para conectar con el cliente de origen, y ésta es la única funcionalidad permitida.

3) comportamiento variable del comando PORT: el comando PORT se puede utilizar en las dos formas descritas, siendo una la forma por default. El cambiar entre ellas se logra generalmente con un parámetro en la línea de comando. Se debe tener cuidado de verificar cuál es el valor por default. Asimismo, se debe tener conciencia sobre la categoría en que se halla el software del server. La recomendación es utilizar la opción 2, o la opción 3 con la supresión habilitada.

6.9.2. CONFIGURACIÓN DEL FTP SERVER

Algunos de los ataques “ftp bounce” descriptos confían en unas o más máquinas del servidor (dependiendo del ataque) permitiendo el upload de archivos vía ftp (generalmente FTP anónimo).

Su sitio debe ofrecer recursos anónimos de upload solo si es absolutamente necesario. Incluso luego, usted debe configurar cuidadosamente el área entrante.

6.9.3. CONFIGURACIÓN DE RED

Hay algunas cosas a tener presente al configurar las “fronteras” de la red, esto es, los routers con access-lists y los firewalls.

Los sitios deben asegurarse de que se diseñe cuidadosamente la topología de red de modo que los límites eficaces del tráfico existan entre los sistemas que ofrecen niveles distintos del servicio. Por ejemplo, un sitio tiene típicamente un servicio de FTP Anonymous, servicio del Web, y un hub entrante de correo electrónico. Una buena práctica de seguridad consiste en separar las máquinas que proporcionan estos servicios externos de las que realizan servicios internos. Es importante tener límites “fuertes” en la red, preferiblemente firewalls, entre estos dos conjuntos de máquinas.

Por ejemplo, los sitios que tienen un server FTP que permite el comando PORT para establecer conexiones a las máquinas de un tercero deben bloquear el tráfico entre el server FTP y las máquinas que ofrecen servicios que confían en el hostname o la dirección IP para la autenticación. Los ejemplos de tales servicios son rlogin, rsh y NFS. Mientras que un firewall o un filtering router debe prevenir siempre el acceso externo directo a tales servicios, debe también filtrar el tráfico de un server FTP interno que se comporte de esta manera. Esto advierte al server FTP que está siendo utilizado como una máquina de relay para atacar protocolos con mecanismos débiles de autenticación basados en el hostname o la dirección IP.

Los sitios que usan firewall de filtrado dinámico de paquetes dinámico necesitan tomar medidas adicionales para asegurarse de que los comandos PORT de terceros sean bloqueados por el firewall.

6.10. TELNET

TELNET provee acceso de terminal a un sistema. El protocolo incluye provisiones para soportar varios seteos de terminal como ser raw mode, eco de caracteres, etc. Generalmente, el demonio de telnet llama al programa login para autenticar al usuario iniciar la sesión. El mismo provee un nombre de cuenta y una password para el login. Una sesión de telnet puede ocurrir entre dos máquinas de la misma organización o confiables, en ese caso se puede utilizar un secure telnet para encriptar la sesión completa, protegiendo la password y la sesión completa. Pero en la mayoría de los casos, la mayoría de las sesiones de telnet vienen de sistemas no confiables. Es decir, no puede confiar ni en el sistema operativo que hace telnet al nuestro, ni en las redes que intervienen en el proceso.

La password y la sesión entera son fácilmente visibles para los ojos de un espía, típicamente usando sniffers. Una técnica común de hackeo es “pinchar” el programa cliente de telnet, logrando que registre los nombres de usuario y password, e inclusive la sesión entera.

De todas formas, si la red está bajo “sniffing”, es extremadamente sencillo obtener las passwords que circulan por sesiones de telnet. La mejor defensa para este tipo de ataque es el esquema de password de única vez.

Una de las implementaciones de este esquema consiste en que el usuario disponga de un dispositivo programado mediante una clave secreta. El sistema que acepta el login envía un “challenge”, que el usuario digita en su dispositivo. Esto le devuelve la password adecuada para el código “challenge” enviado. Pero esa password que circulo por la red es válida solo para esa sesión, el hacker, si observo la sesión, deberá descifrar cual es el

algoritmo utilizado para que en base al “challenge” variable y una clave secreta que no circula por la red se obtenga la password de única vez.

6.11. SEGURIDAD EN NETBIOS

Los sistemas operativos de Microsoft utilizan para comunicarse entre sí el protocolo NetBIOS (Network Basic Input Output System), desarrollado originalmente por IBM. Este protocolo a su vez debe ir sobre otro de inferior nivel que puede ser uno de los siguientes: NetBEUI, IPX/SPX, TCP/IP; es por ello que se hablará de NetBIOS sobre TCP/IP o NetBIOS sobre NetBEUI. Otras aplicaciones y servicios acceden a la red utilizando directamente IPX/SPX o TCP/IP pero sin utilizar NetBIOS. A la implementación de NetBIOS sobre TCP/IP se la conoce como NBT. NetBIOS nos permite compartir archivos e impresoras en la red Microsoft.

Las situaciones de conectividad frecuentes con las cuales uno se encuentra en la red Microsoft son:

6.11.1.1. *PEQUEÑA RED LAN SIN ACCESO A INTERNET Y SIN INTRA O EXTRANET*

Si se tienen clientes basados en DOS o algún equipo usando LAN Manager, forzosamente se necesita NetBIOS sobre NetBEUI, si además se tiene algún servidor Novell también IPX/SPX aunque no se necesita activar el enlace de NetBIOS sobre IPX/SPX. Si los clientes son todos NT, 95 o Windows 3.x lo más recomendable es NetBIOS sobre IPX/SPX y de paso se tiene acceso a Novell.

6.11.1.2. *REDES LAN CON INTERNET, INTRANET O EXTRANET*

Se necesita claramente TCP/IP, si se desea mayor seguridad se puede usar NetBIOS sobre IPX/SPX y no activar el enlace NetBIOS-TCP/IP, si se tienen clientes DOS o LAN Manager se necesitará NetBEUI en cuyo caso se puede quitar IPX/SPX. Otra opción es usar NetBIOS sobre TCP/IP y filtrar en el router los puertos 135 a 139 o usar un firewall.

6.11.1.3. *REDES WAN*

Se hace necesario NetBIOS sobre TCP/IP, se debe eliminar el resto de los protocolos si no son estrictamente necesarios.

El problema con que se enfrenta es que el usuario muchas veces realiza share de discos en modo read only sin password, cuando no lo hace en modo read write, para compartir sus archivos en la red local. El usuario además cree que sólo lo comparte con gente conocida de su ámbito, por ejemplo.

Pero lo que el ignora, es que si tiene habilitado TCP/IP, NetBIOS se montará encima de TCP/IP, permitiendo que sus shares de disco se vean en TODO INTERNET.

Es más, una situación frecuente es que en una LAN uno de los usuarios haga una conexión dial-up: esto ya basta para que los shares de este usuario sean “vistos” en internet poniendo en potencial riesgo a toda la red.

6.11.1.4. ¿QUÉ HACER?

Los ports usados por el servicio de NetBIOS/TCP (NBT) deben ser IMPERIOSAMENTE filtrados en el router que vincula la LAN con Internet. Además de permitir que un usuario cualquiera de la red acceda a shares de discos de la instalación, la implementación de NBT particularmente en Windows 95 contiene bugs que lo hace vulnerable a ataques del tipo "WinNUKE", como el OOB (Out of Band) bug. Si bien estos ataques no comprometen la integridad de los datos, producen la caída del equipo o de al menos el stack de protocolo, dejando a la máquina aislada.

6.12. DESCRIPCIÓN DE ALGUNAS HERRAMIENTAS DE CONTROL Y SEGUIMIENTO DE ACCESOS

En este apartado se encuentran aquellas herramientas que nos permitirán tener una información - mediante archivos de trazas o logísticos - de todos los intentos de conexión que se han producido sobre nuestro sistema o sobre otro que se haya señalado, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP (herramientas de tipo SATAN).

Este tipo de herramientas nos permite tener un control sobre todos los paquetes que entran por la interfaz de red de la máquina: IP (TCP, UDP) e ICMP, o analizando paquetes a nivel de aplicaciones (TELNET, FTP, SMTP, LOGIN, SHELL, etc.).

Estas herramientas pueden ser utilizadas junto con otras que nos permitan definir desde qué máquinas permite ciertas conexiones y cuales se prohíben. Algunas de las herramientas descritas en este apartado no necesitan estar instaladas en la máquina que se quiere controlar, ya que se puede poner en una máquina cuya interfaz de red funcione en modo promiscuo, permitiendo seleccionar la dirección IP o máquina que se quiere auditar. Algunas de las herramientas descritas en este apartado pueden tener un doble uso. Es decir, nos permiten protegernos ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer los sistemas.

Por eso es importante que el uso de estas herramientas esté restringido - en la manera que se pueda - para que no todo el mundo esté utilizándolas de forma aleatoria y nos oculten realmente un ataque.

También podrán ser utilizadas para realizar seguimientos en la red cuando crea que alguna de las máquinas ha sido comprometida.

6.12.1. HERRAMIENTAS PARA WINDOWS NT

Las herramientas que se nombran, a continuación, son parte de Windows NT.

6.12.1.1. MONITOR DE EVENTOS

Muestra logs del sistema y permite filtrar el display para mostrar cierto tipo de eventos. El log de seguridad incluye violaciones de seguridad, tales como cierres de cuentas, etc.

6.12.1.2. MONITOR DE RED

Permite capturar paquetes de la red y mostrar información sobre ellos.

Esta herramienta puede ser poderosa para monitorear el uso de la red y es muy indicada para la búsqueda de paquetes específicos, a fin de realizar un seguimiento sobre problemas de seguridad.

6.12.1.3. MONITOR DE PERFORMANCE

Este utilitario, es una de las mejores herramientas de NT para optimizar y monitorear la performance del sistema, y tiene algunas herramientas para la seguridad.

6.12.1.4. ERRORES DE PERMISOS DE ACCESOS

Es un contador que muestra la cantidad de veces que los usuarios han probado acceder a archivos sin los permisos indicados. Un número alto, puede indicar que un hacker está buscando acceder a archivos.

6.12.1.5. ERRORES DE LOGON

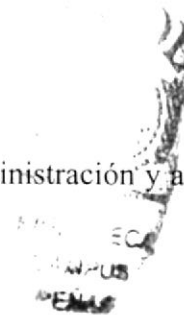
Constituye el número de intentos de ingresar al sistema no válido. Un incremento dramático de éste contador, puede ser indicio de que alguien está tratando de acceder al sistema ó de que se está corriendo un programa para probar password en sucesión.

6.13. PAQUETES PARA WINDOWS

6.13.1. WINDOWS NT RESOURCE KIT

Este paquete de Microsoft tiene varias herramientas para administración y algunas para seguridad.

Las herramientas de seguridad que trae, son:



6.13.1.1. C2CONFIG

Cuando este utilitario es ejecutado muestra una lista de potenciales problemas de seguridad que él encuentra sobre el sistema.

6.13.1.2. DUMPEL

Sirve para convertir la salida del visor de sucesos en otro formato a fin de darle otro tratamiento.

6.13.1.3. PASSPROP

Utilitario para obligar a tener passwords complejas en el sistema. Al correr este utilitario, éste obliga a que las passwords incluyan números, minúsculas y mayúsculas o caracteres de puntuación para que sean válidas.

6.13.1.4. *INTERNET SCANNER*

Este utilitario muestra el mapeo entre las direcciones físicas de las interfaces y su dirección IP.

Vendedor: Internet Security Systems

6.13.1.5. *SCANNT*

Es una herramienta para chequear los passwords sobre el servidor NT. Chequea mediante passwords fáciles de crackear.

Para información recurrir a: www.Ntsecurity.com

6.13.1.6. *NETXRAY*

Es un analizador de protocolo (conocidos como sniffers) que corre bajo Windows NT y provee una muy amigable interface. Entre otras utilidades, permite:

Arquitectura cliente-servidor. Permite anexar copias sobre otra computadora para monitoreo remoto.

Disparos de alertas: genera alertas sobre condiciones especificadas, basadas en errores, utilización y otras características de la red.

Generador de paquetes: permite cargar la red y sondear específicamente la capacidad de testear la habilidad de manejar condiciones extrañas.

6.13.1.7. *SUCK SERVER*

Este programa, escrito por Matthew Strebe, permite establecer puertos TCP/IP absorbidos o no usados sobre los servidores Internet.

Permite ver cuando los hackers están probando atacar a la computadora por servicios que no son provistos.

Obtenible como shareware.

6.13.1.8. *RED BUTTON*

Este programa es una demostración de un serio problema de seguridad de NT. Este bug permite el acceso remoto de más de un registro que podría estar disponible, el resultado es que el acceso remoto puede ser obtenido sin tener password.

Puede ser obtenido como freeware.

6.14. **SÍNTESIS**

A continuación, se presenta, a modo de síntesis un cuadro del algoritmo

Productor-Consumidor y los programas que pueden resolver los problemas que se pueden presentar.

Algoritmo Productor/Consumidor	Programa para ese problema
1)- Interrupción - Disponibilidad	Tcp-wrapper Tcplogger Udplogger Icmplogger Etherscan Nstat Angus Gabriel Nocol Tiger Crack Noshell Tlinux Monitor de performance Windows NT Resource Kit Scan NT NetXRay Suck Server Red Button
2)- Intercepción - Privacidad	Tcp-wrapper Tcplogger Icmplogger Etherscan Topdump ISS Courtney Gabriel Nocol Tiger Crack Cpm Ifstatus Tlinux Monitor de red Windows NT Resource Kit Internet Scanner Scan NT NetXRay Suck Server Red Button

Figura 6-5 Cuadro de síntesis 1

Algoritmo Productor/Consumidor	Programa para ese problema
3)- Modificación - Integridad	Tcp-wrapper Tcplogger Icmplogger Etherscan ISS Gabriel COPS Tiger Isaf osh noshell brinx Monitor de sucesos Windows NT Resource Kit Scan NT Red Button
4)- Producción - Integridad	Tcp-wrapper Tcplogger Icmplogger Etherscan ISS Gabriel COPS Tiger Crack Tripwire Isaf Osh Noshell Tlinux Monitor de sucesos Windows NT Resource Kit Scan NT Red Button

Figura 6-6 Cuadro de síntesis 2





CAPÍTULO 7 NORMAS DE CABLEADO ESTRUCTURADO

7.1 NORMATIVAS DE CABLEADO ESTRUCTURADO



Normativa obligatoria
Recomendación

7.1.1 NORMATIVA 1

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

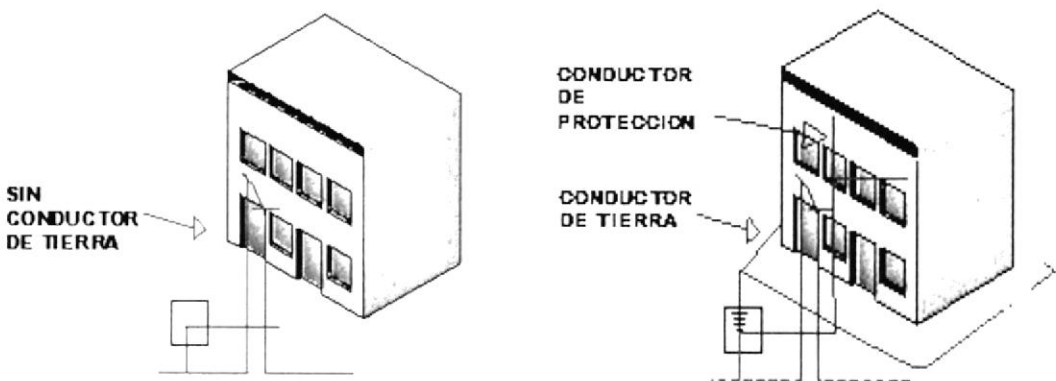


Figura 7-1 Normativa 1

7.1.2 NORMATIVA 2

El cableado horizontal deberá estar configurado como topología estrella con cada salida de telecomunicaciones conectada a un MC o distribuidor de piso.



Figura 7-2 Normativa 2

7.1.3 **NORMATIVA 3** ▲

Se emplearan conexiones cruzadas para conexiones entre cableado horizontal y back bone y para conexiones entre cableado horizontal y equipos con salidas de puertos múltiples.

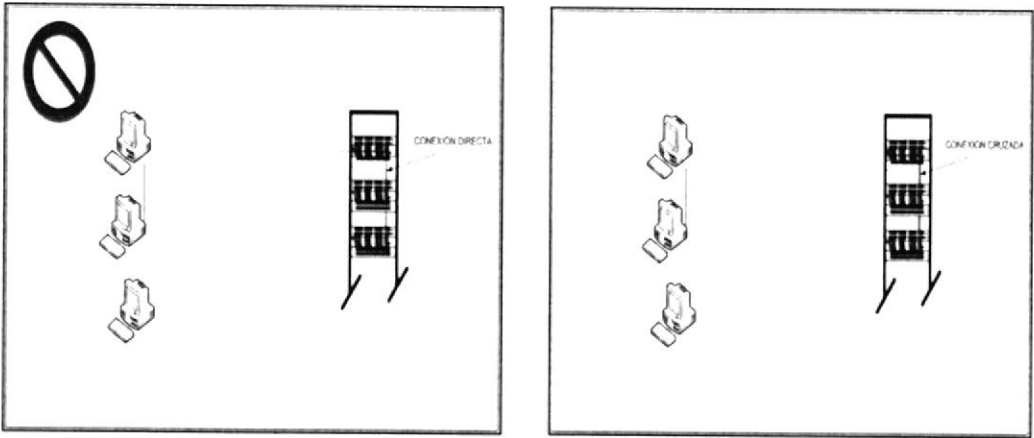


Figura 7-3 Normativa 3

7.1.4 **NORMATIVA 4** ▲

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

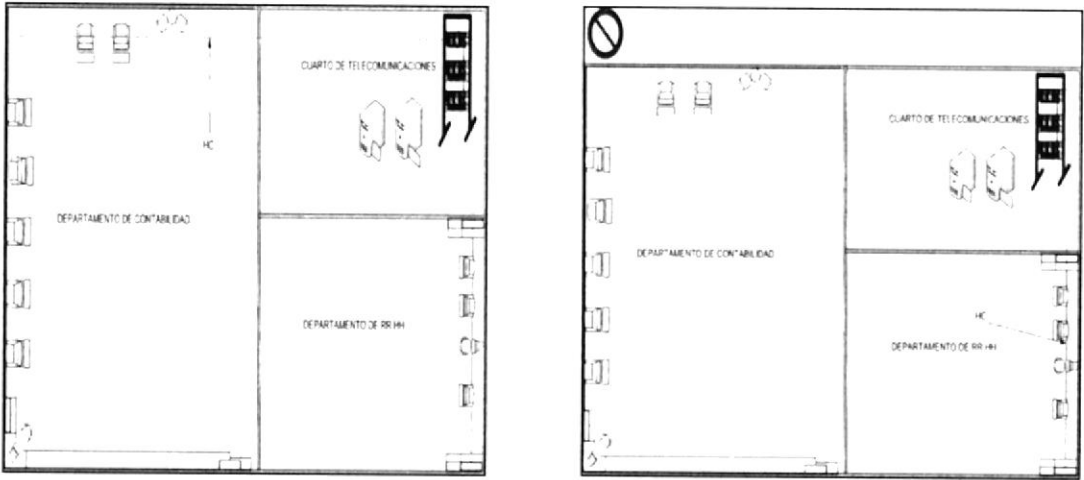


Figura 7-4 Normativa 4

7.1.5 **NORMATIVA 5** ▲

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

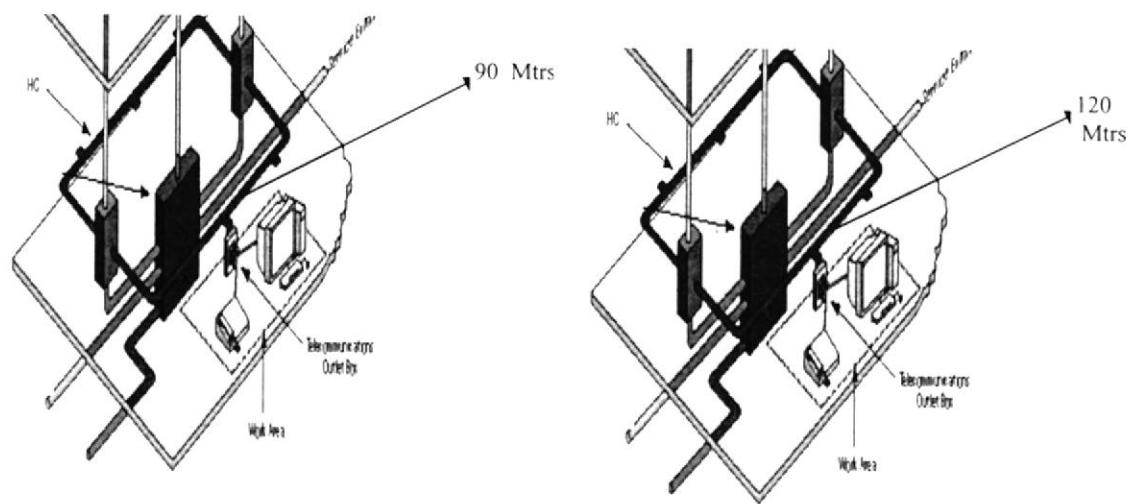


Figura 7-5 Normativa 5



7.1.6 **NORMATIVA 6** ▲

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

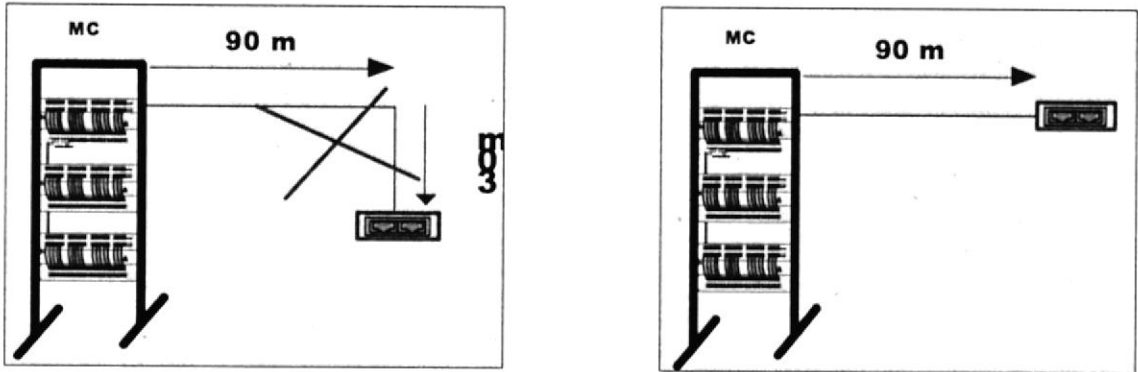


Figura 7-6 Normativa 6

7.1.7 NORMATIVA 7 ▲

La longitud individual o combinada del Patch cord, el par trenzado balanceado 24^a (WE) calibre americano de alambre o fibra óptica utilizado en el HC, no excederá los 5mtrs



Figura 7-7 Normativa 7

7.1.8 NORMATIVA 8 ▲

No se permitirá más de un punto de consolidación dentro del mismo pedido de cable horizontal

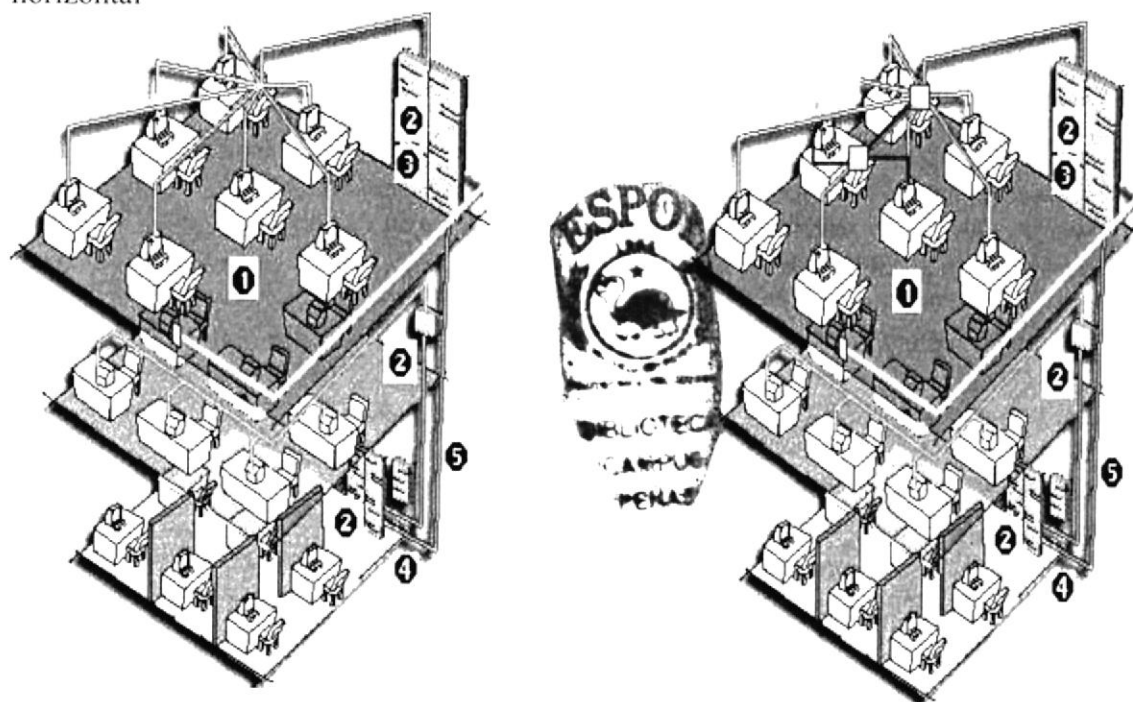


Figura 7-8 Normativa 8

7.1.9 NORMATIVA 9 ▲

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

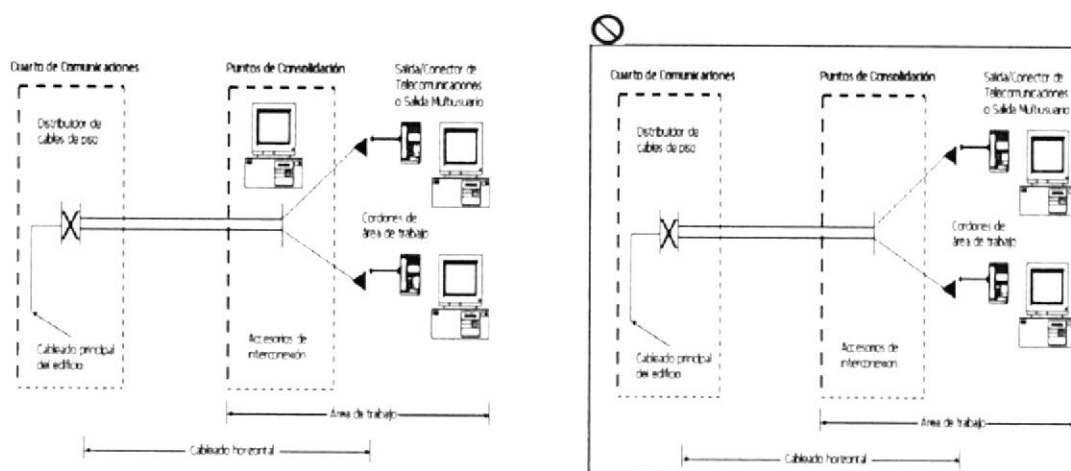


Figura 7-9 Normativa 9

7.1.10 NORMATIVA 10 ▲

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

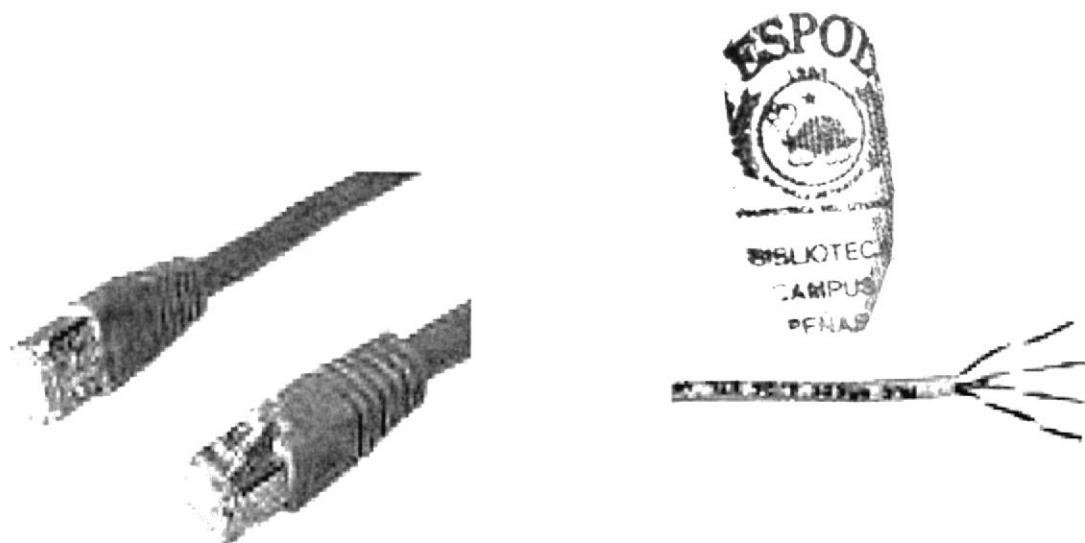


Figura 7-10 Normativa 10

7.1.11 **NORMATIVA 11** ▲

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

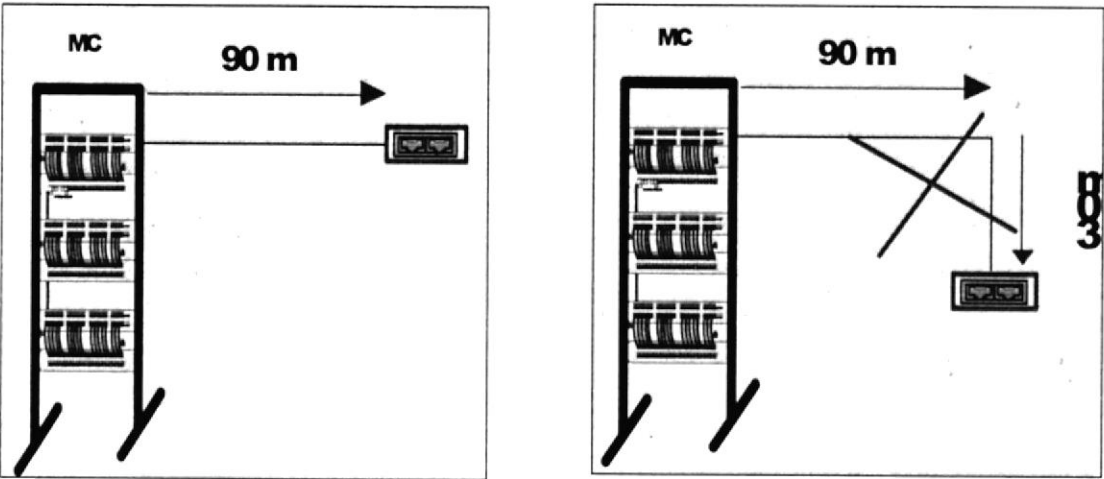


Figura 7-11 Normativa 11

7.1.12 **NORMATIVA 12** ▲

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

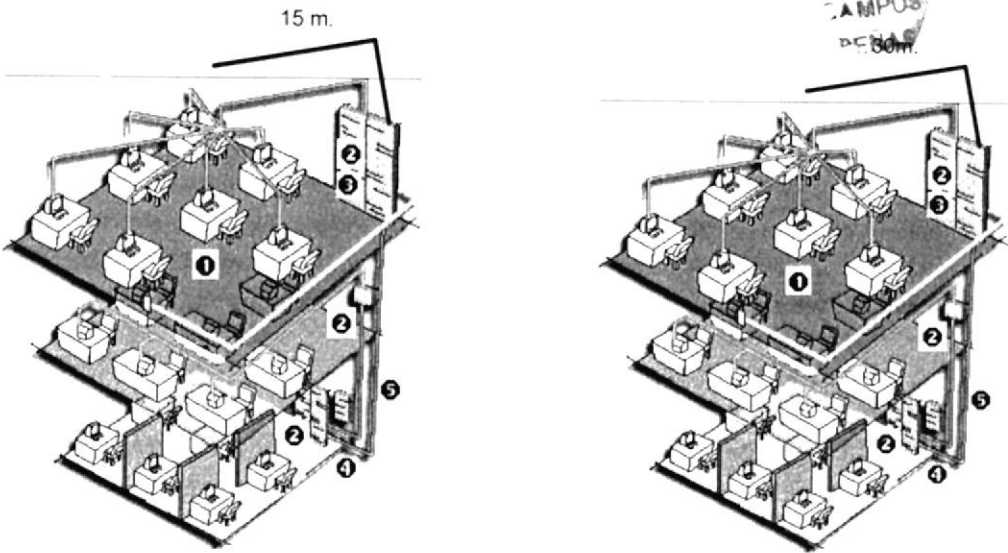


Figura 7-12 Normativa 12

7.1.13 **NORMATIVA 13** ▲

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

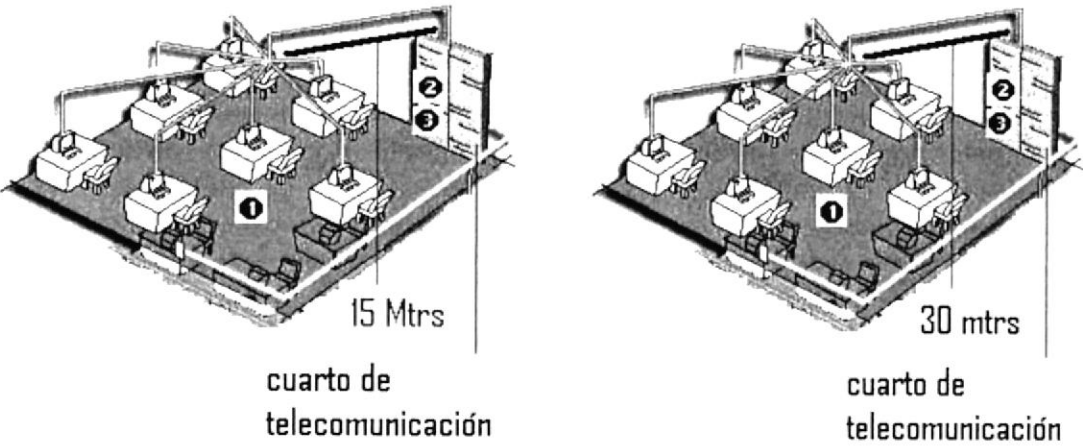


Figura 7-13 Normativa 13

7.1.14 **NORMATIVA 14** ▲

La longitud del canal del cableado horizontal incluyendo los Patch cord de equipos en ambos extremos no excederá los 100m. Independientemente del medio

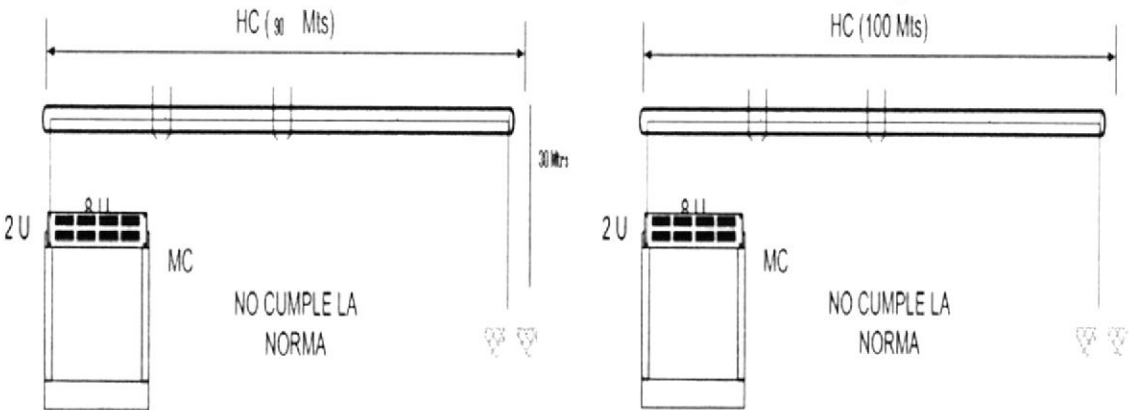


Figura 7-14 Normativa 14

7.1.15 **NORMATIVA 15** ▲

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

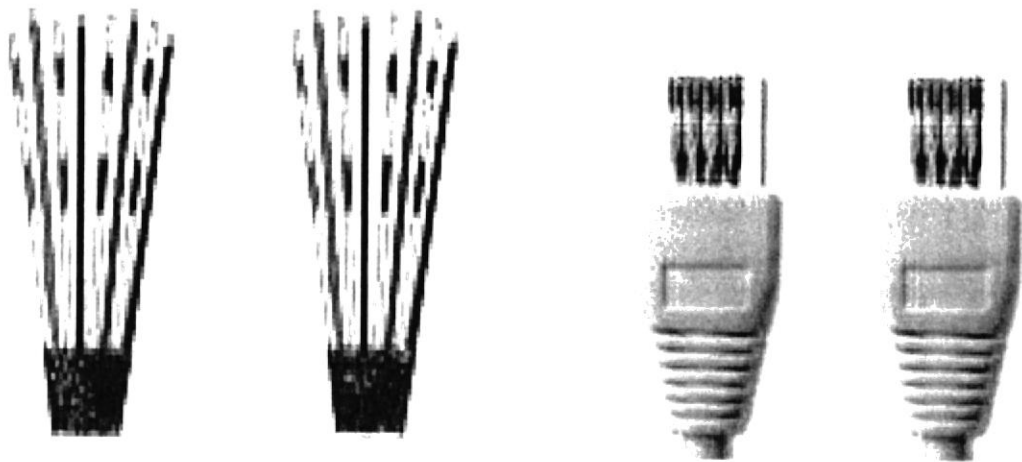


Figura 7-15 Normativa 15

7.1.16 **NORMATIVA 16** ▲

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

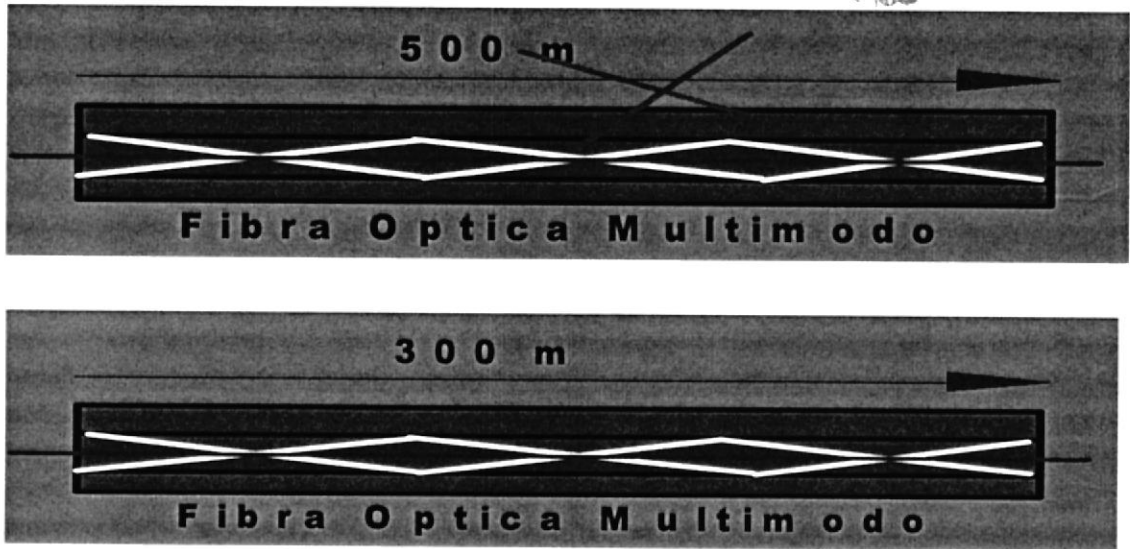


Figura 7-16 Normativa 16

7.1.17 NORMATIVA 17 ▲

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

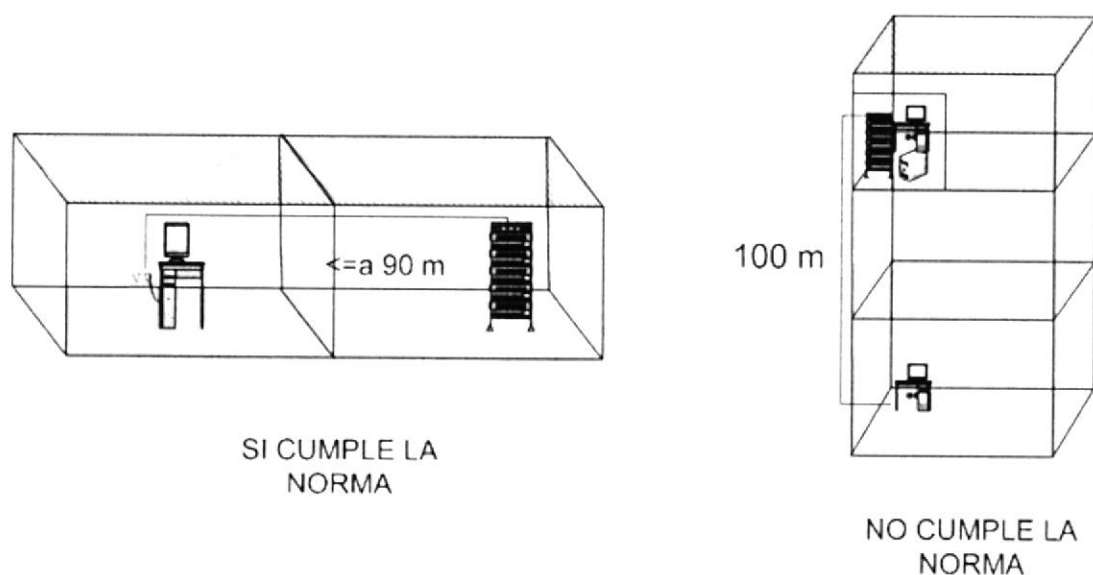


Figura 7-17 Normativa 17

7.1.18 NORMATIVA 18 ▲

Las canalizaciones horizontales de cableado se diseñarán e instalarán para cumplir los requisitos eléctricos y de comunicación, locales, nacionales.

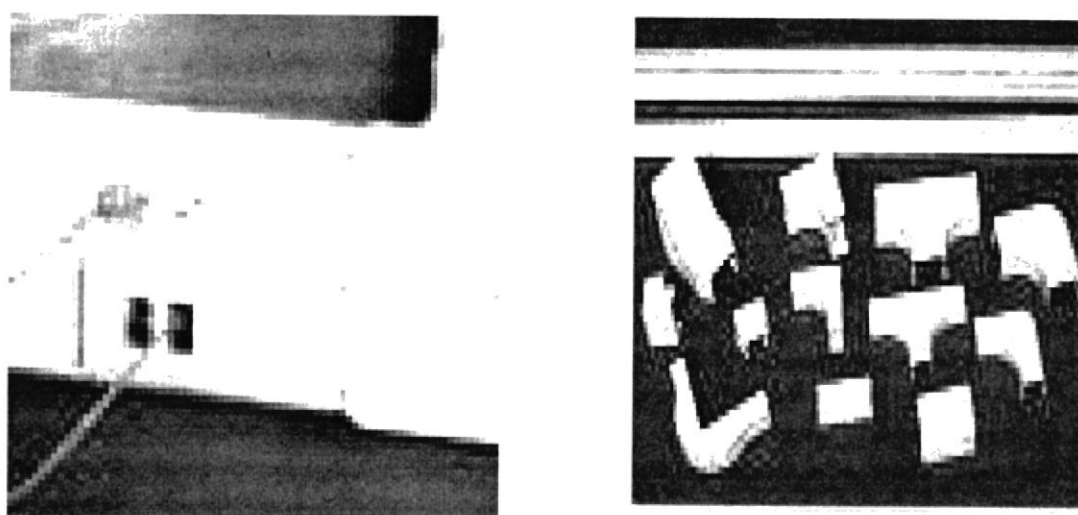


Figura 7-18 Normativa 18

7.1.19 NORMATIVA 19 ▲

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

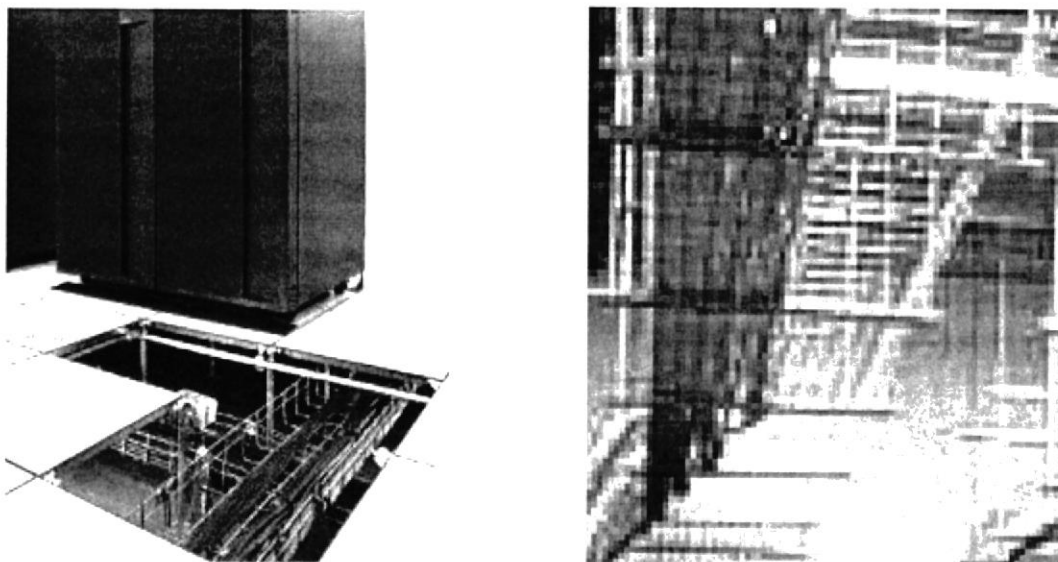


Figura 7-19 Normativa 19

7.1.20 NORMATIVA 20 ▲

Las canalizaciones horizontales deberán mantener un radio mínimo de curvatura para que los cables horizontales se mantengan dentro de las especificaciones del fabricante durante y después de la instalación.

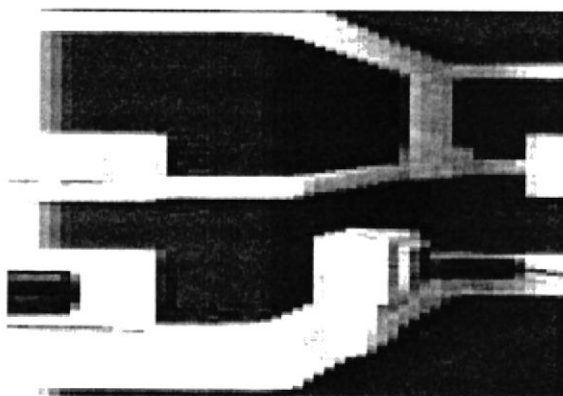


Figura 7-20 Normativa 20

7.1.21 NORMATIVA 21 ▲

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

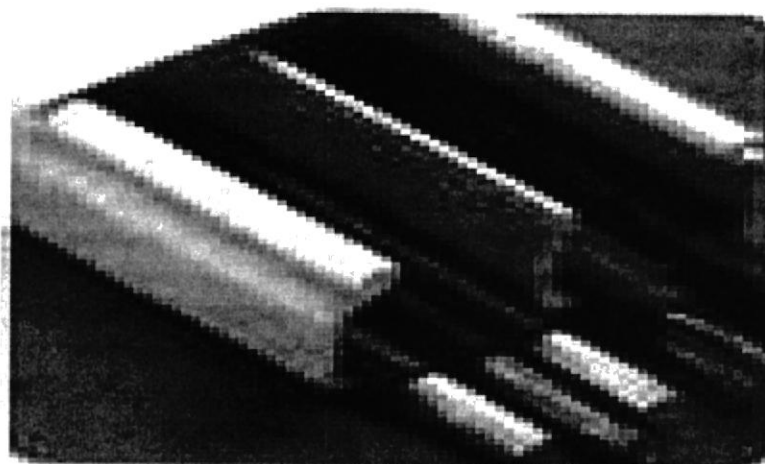


Figura 7-21 Normativa 21

7.1.22 NORMATIVA 22 ▲

El back bone utilizara la topología tipo estrella jerárquica desde el MC hasta el IC

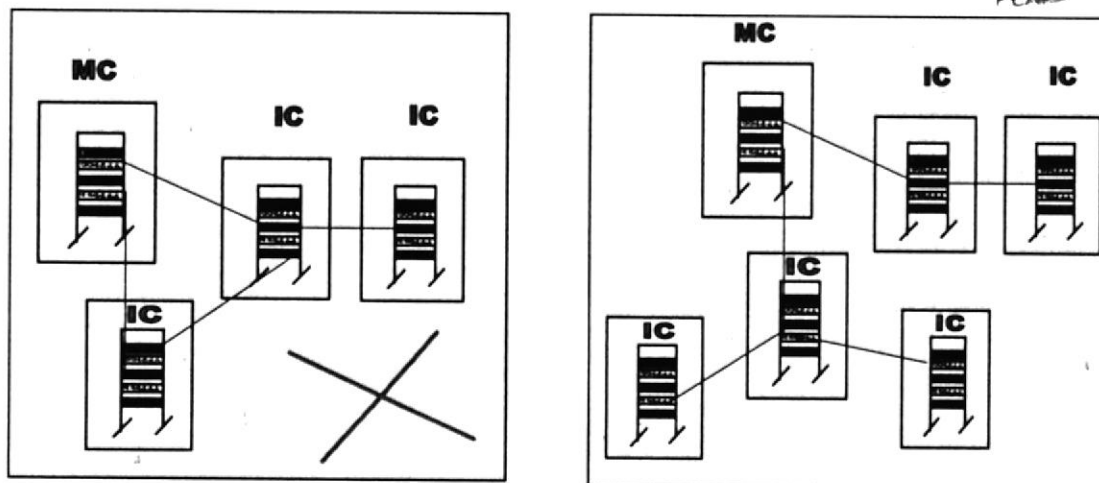


Figura 7-22 Normativa 22

7.1.23

NORMATIVA 23 ▲

Para el tendido del back bone de cada edificio que sea mayor de 90m. de longitud debe proveerse cable de fibra óptica.

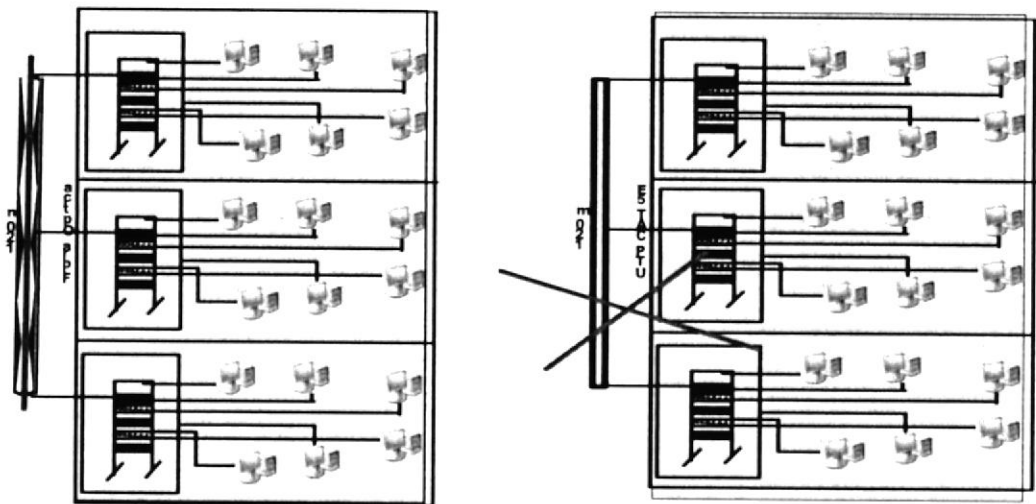


Figura 7-23 Normativa 23

7.1.24

NORMATIVA 24 ▲

La longitud total del canal de cable ente el MC y cualquier H no excederá los siguientes límites:

NOTA#1: Si el back bone de par trenzado balanceado sobrepasa los 100 m. su uso se restringirá para soportar aplicaciones de voz.

LONGITUD	TIPO
3000m.	Fibra óptica monomodo
2000m.	Fibra óptica multimodo
2000m.	Par trenzado balanceado para aplicaciones PVX

Tabla 7-1 Longitud y Tipos de Fibra Óptica



Figura 7-24 Normativa 24

7.1.25 **NORMATIVA 25** ▲

Las canalizaciones de edificio proveerán accesos a todos los cuartos de telecomunicaciones, cuartos de equipos y acometidas localizados en el mismo edificio.

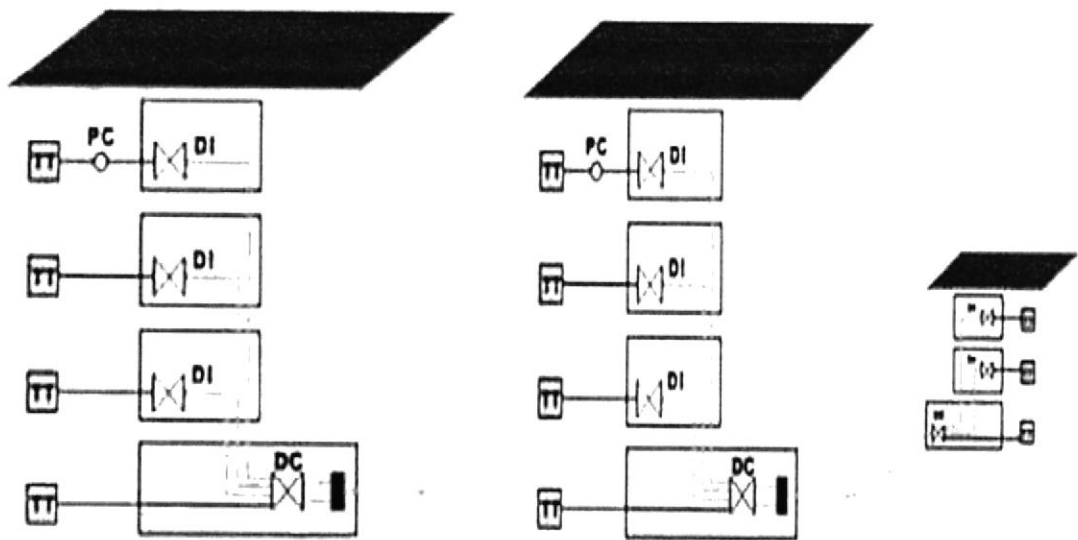


Figura 7-25 Normativa 25

7.1.26 **NORMATIVA 26** ▲

Las canalizaciones no se ubicarán en el ducto de ascensores.

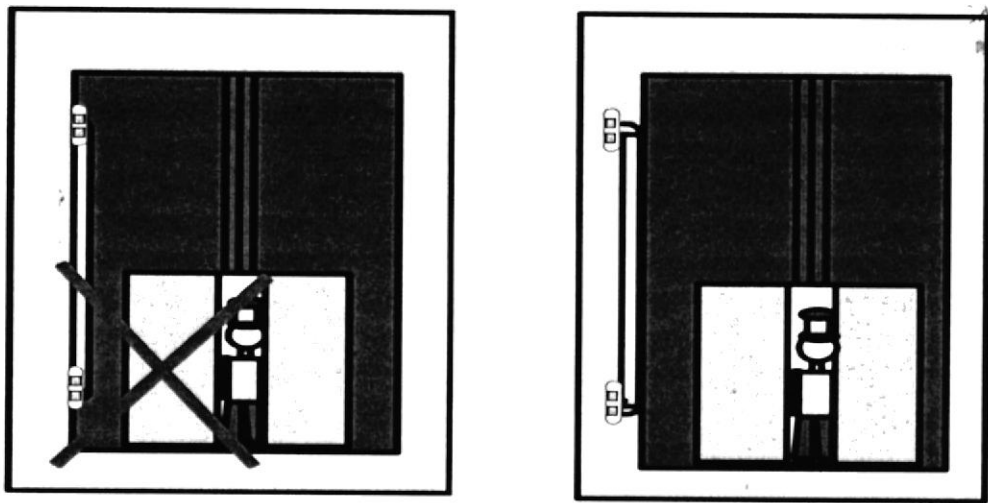


Figura 7-26 Normativa 26

7.1.27 **NORMATIVA 27** ▲

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



Figura 7-27 Normativa 27

7.1.28 **NORMATIVA 28** ▲

El cuarto de telecomunicaciones se usara y equipara para contener equipo de telecomunicación, terminaciones de cable y asociados.

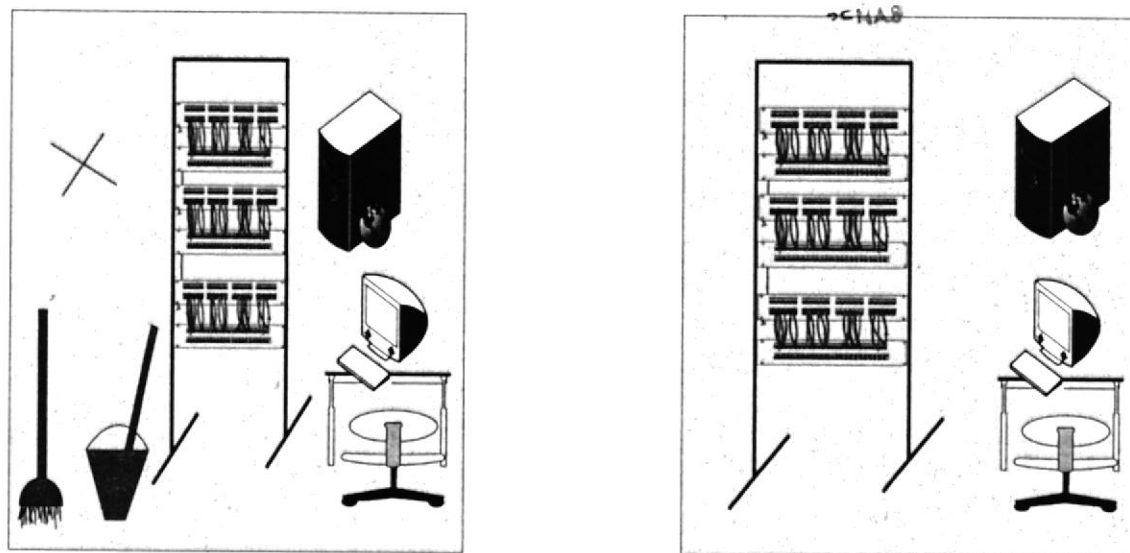


Figura 7-28 Normativa 28

7.1.29 **NORMATIVA 29** ▲

El cuarto de telecomunicaciones estará dedicado a la función de telecomunicaciones. El acceso a los cuartos de telecomunicaciones se restringirá al personal de servicio autorizado y no será compartido por servicios del edificio que puedan interferir con los sistemas de telecomunicaciones

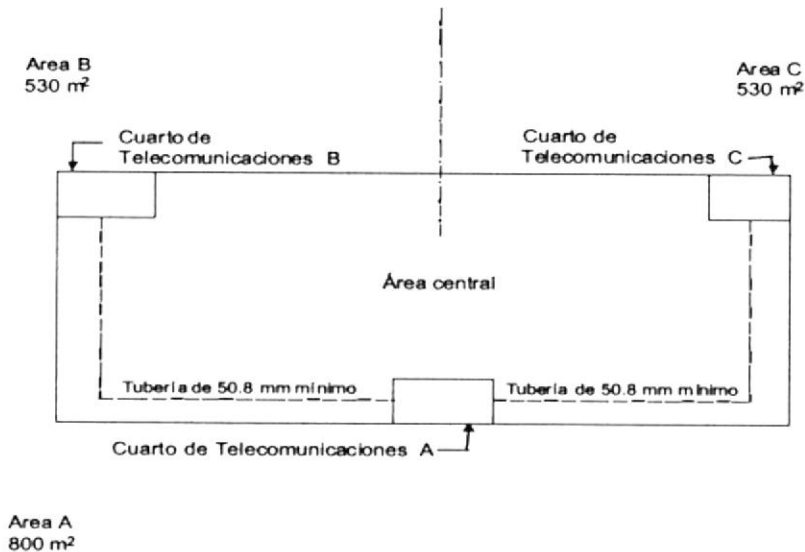


Figura 7-29 Normativa 29



7.1.30 **NORMATIVA 30** ▲

Las instalaciones del cable de puesta a tierra cumplirán los reglamentos y normas aplicables.

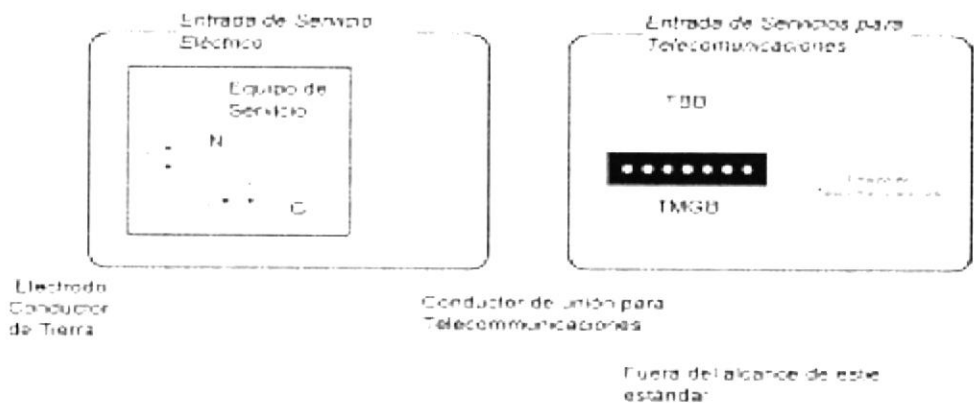


Figura 7-30 Normativa 30

7.1.31 NORMATIVA 31 ▲

Los gabinetes usados como espacios alternativos cumplirán los requisitos de separación tendrán una puerta provista con cerradura y se montará en una ubicación firme.

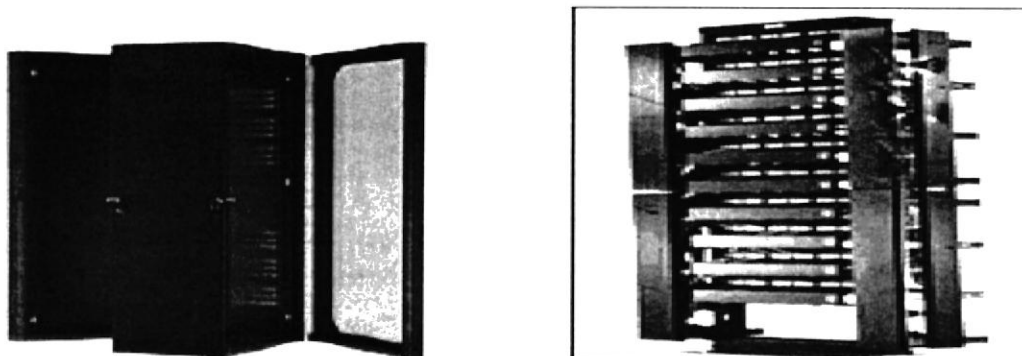


Figura 7-31 Normativa 31

7.1.32 NORMATIVA 32 ▲

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

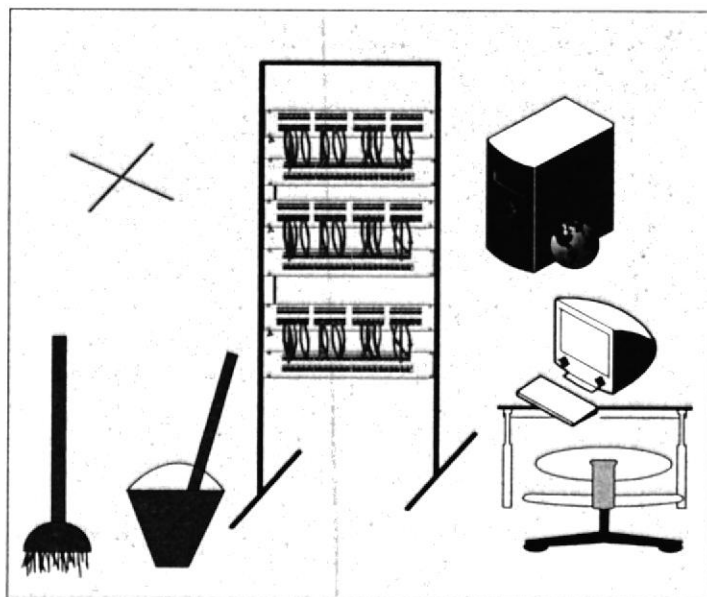


Figura 7-32 Normativa 32

7.1.33 **NORMATIVA 33** ▲

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

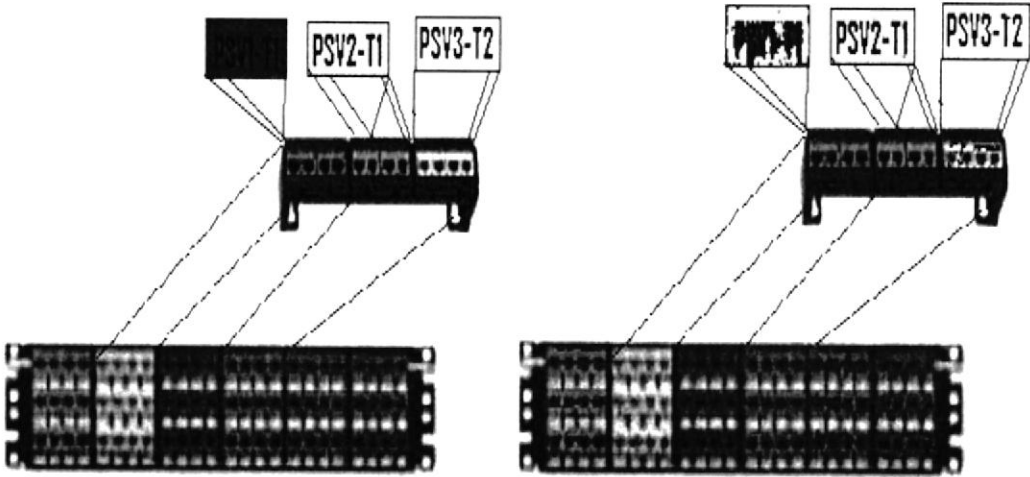


Figura 7-33 Normativa 33

7.1.34 **NORMATIVA 34** ▲

La instalación de gabinetes y Rack deberán proporcionar las separaciones estipuladas en los reglamentos y normas aplicables.

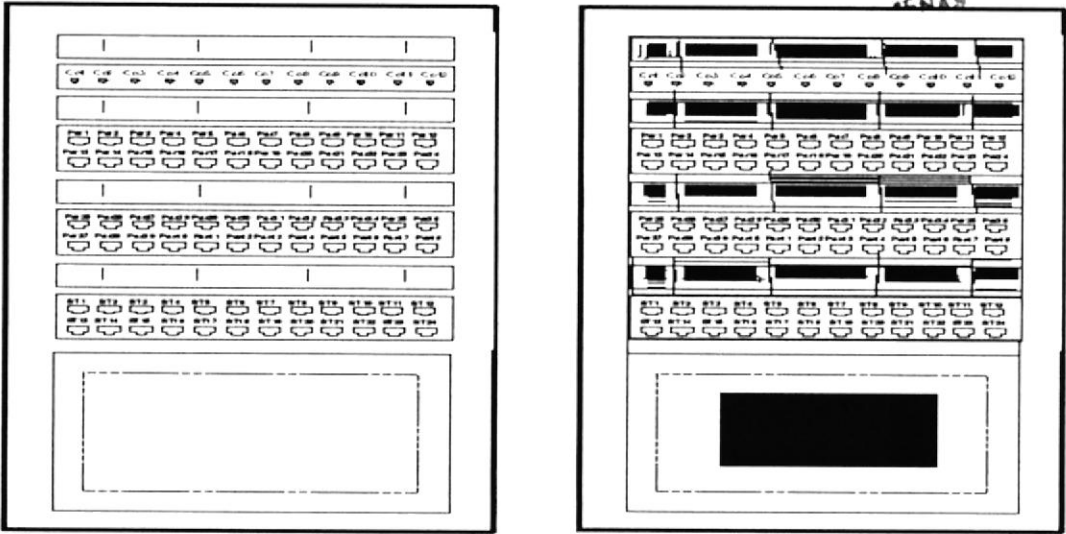


Figura 7-34 Normativa 34

7.1.35 **NORMATIVA 35** ▲

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

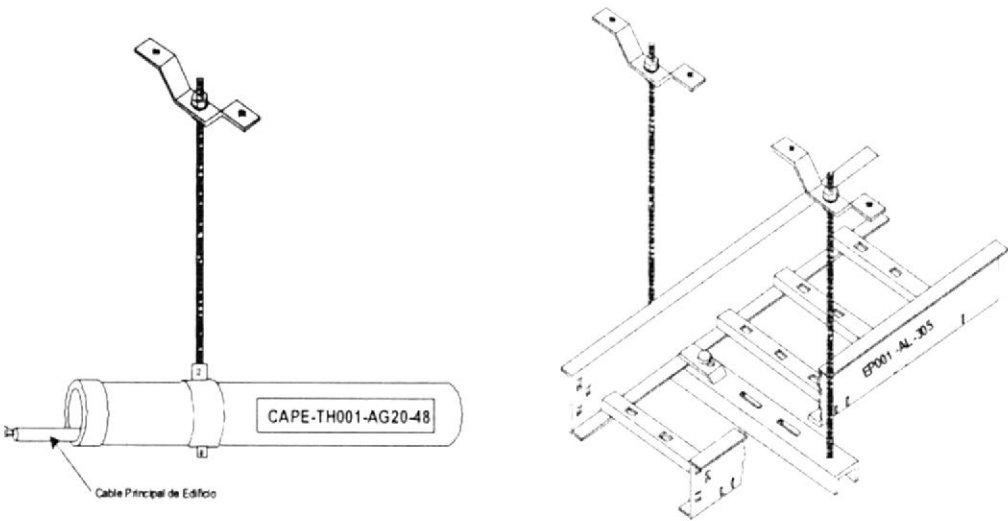


Figura 7-35 Normativa 35

7.1.36 **NORMATIVA 36** ▲

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

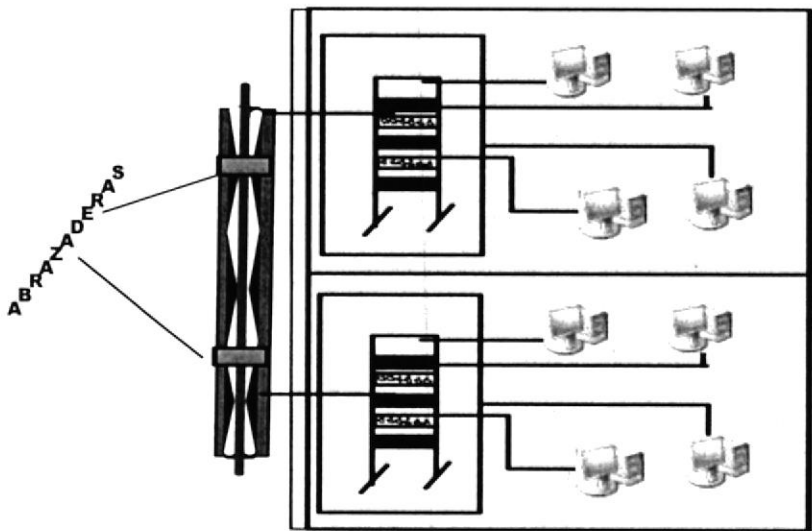


Figura 7-36 Normativa 36

7.1.37 NORMATIVA 37

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

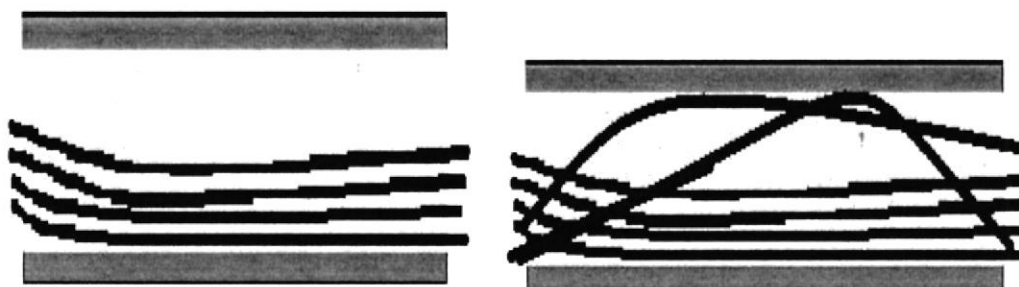


Figura 7-37 Normativa 37

7.1.38 NORMATIVA 38 ▲

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

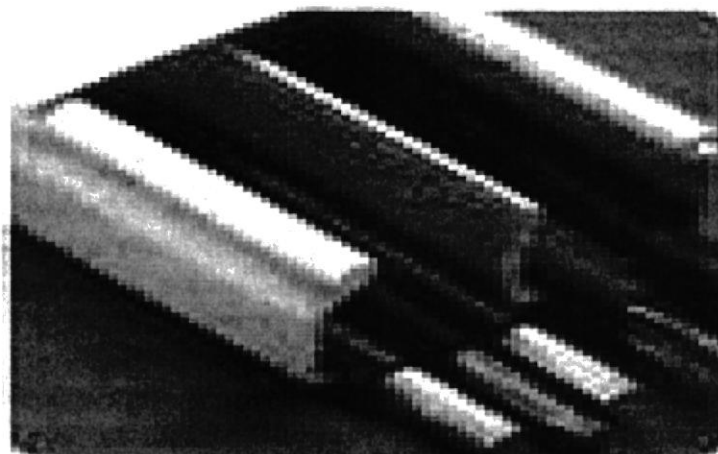


Figura 7-38 Normativa 38

7.1.39 **NORMATIVA 39** ▲

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

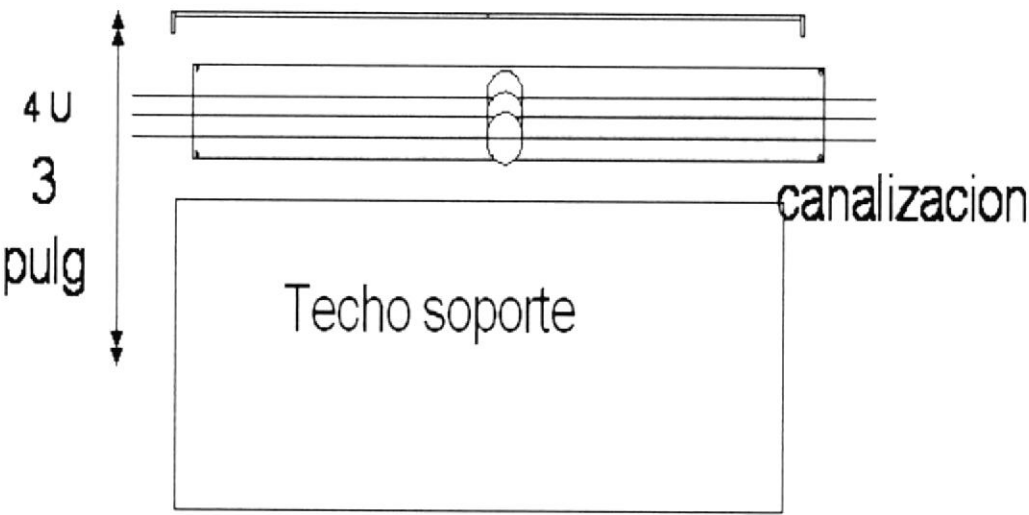


Figura 7-39 Normativa 39



7.1.40 **NORMATIVA 40** ▲

Las tensiones máximas del halado del cable o los radios mínimos de curvatura no pasarán las especificaciones del fabricante.

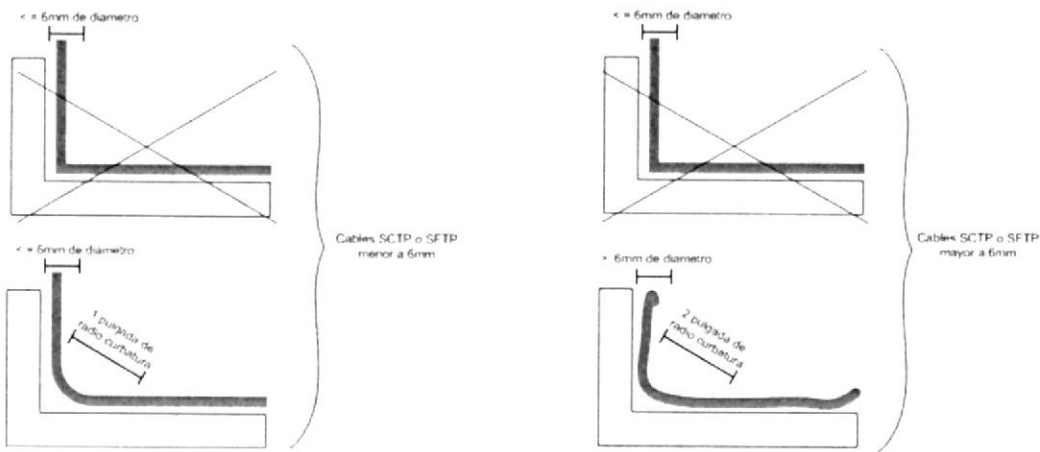


Figura 7-40 Normativa 40

7.1.41 NORMATIVA 41 ▲

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

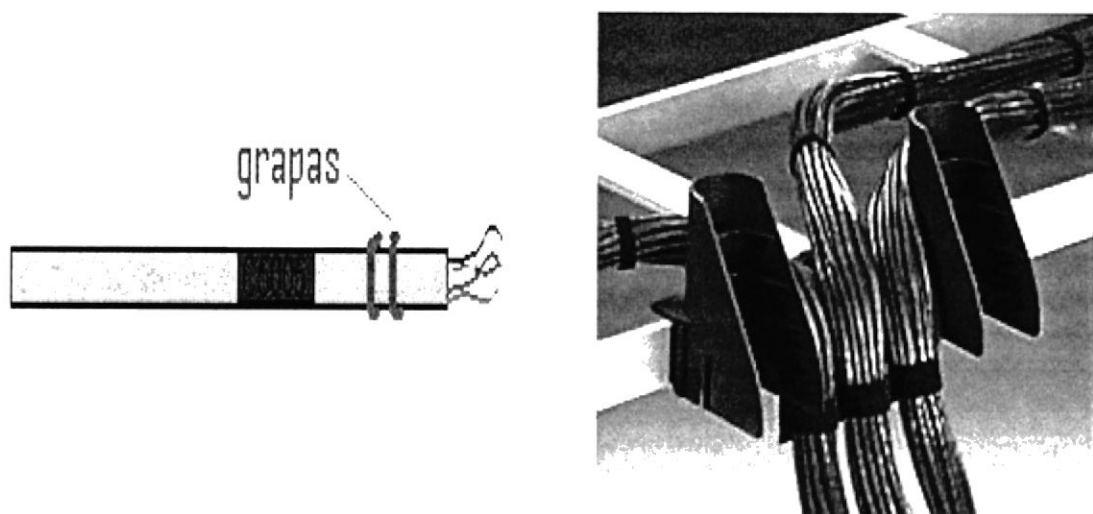


Figura 7-41 Normativa 41

7.1.42 NORMATIVA 42 ▲

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

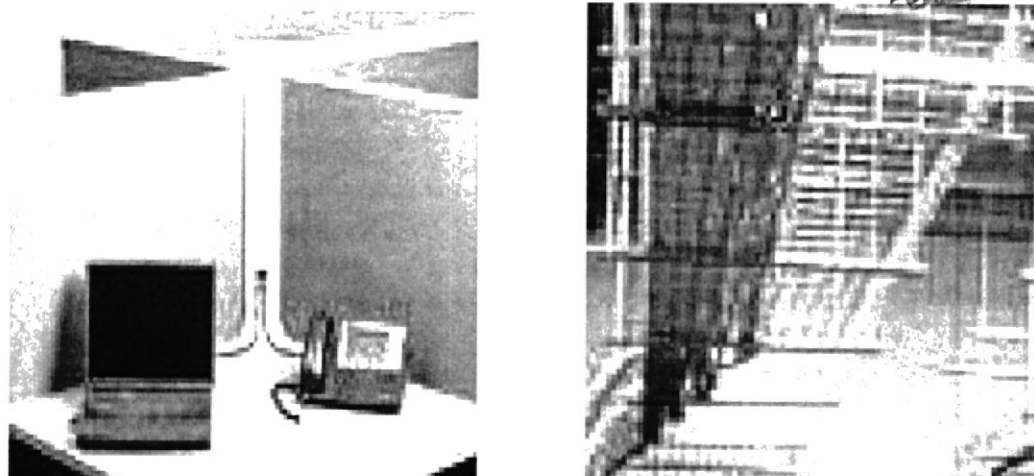


Figura 7-42 Normativa 42

7.1.43 **NORMATIVA 43** ▲

El radio mínimo de curvatura, en condiciones de no tensión (cuando el cable solo es colocado, no halado.), será de una pulgada para SCTP o SFTP de diámetro menor o igual a 6mm. (0.25 inch).

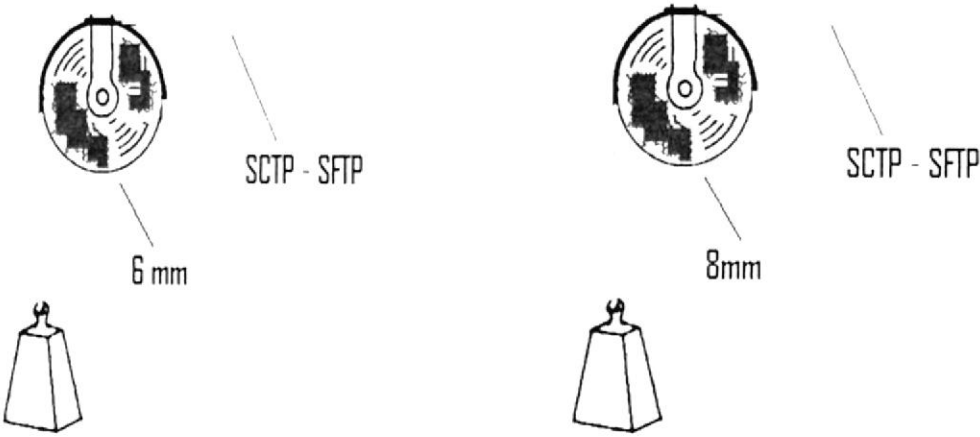


Figura 7-43 Normativa 43

7.1.44 **NORMATIVA 44** ▲

El radio mínimo de curvatura para cable horizontal de 2 y 4 fibras será de 1 pulgada bajo condiciones de no tensión y de 2 pulgadas bajo condiciones de tensión, en donde la tensión máxima de halado permitida será de 222 newton (libra - fuerza).

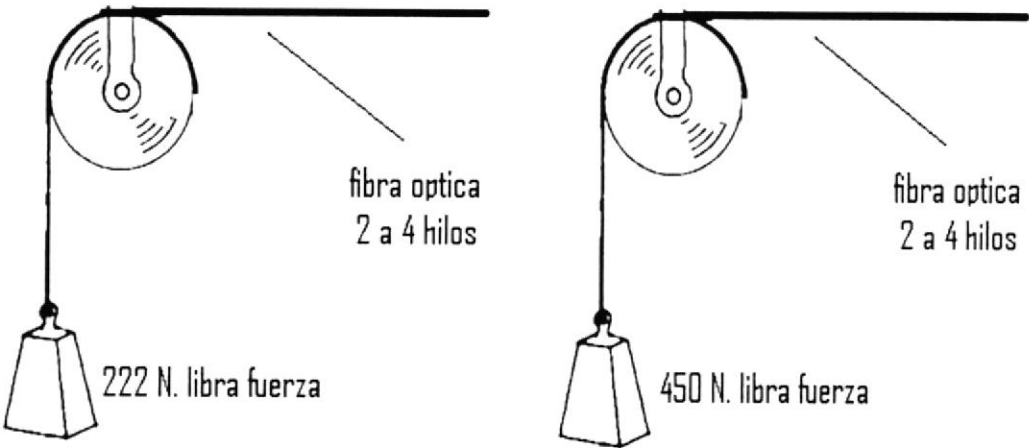


Figura 7-44 Normativa 44

7.1.45 NORMATIVA 45 ▲

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

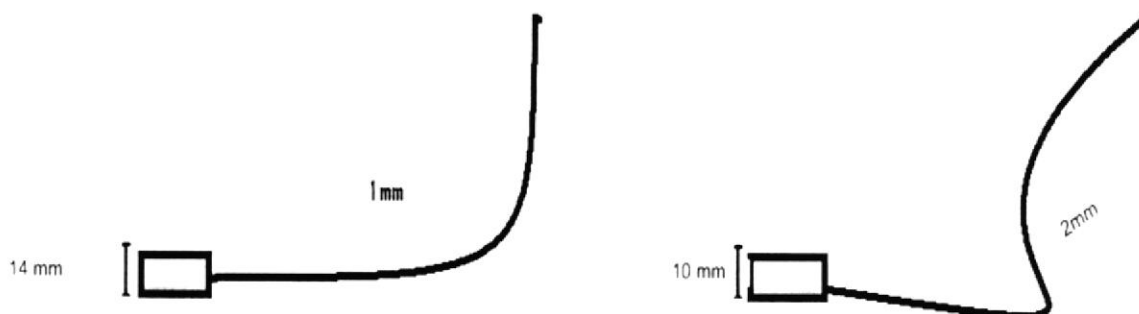


Figura 7-45 Normativa 45

7.1.46 NORMATIVA 46 ▲

El radio de curvatura para el cable de back bone de fibra óptica externa no será menor a 10 veces el diámetro externo del cable bajo condiciones de no tensión y no menor a 20 veces el diámetro externo del cable bajo condiciones de tensión, en donde la tensión de halado permitido es menor a 2600 newton (600 libras - fuerza).

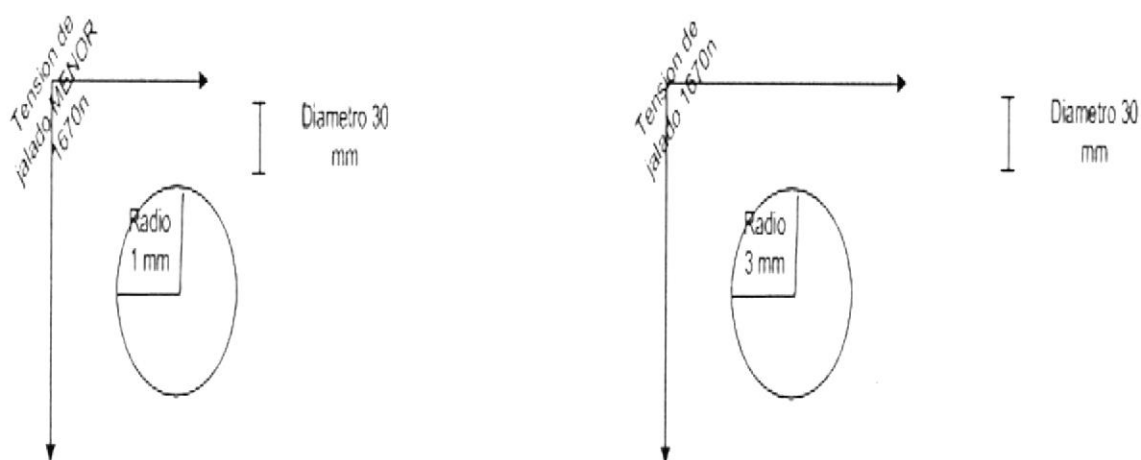
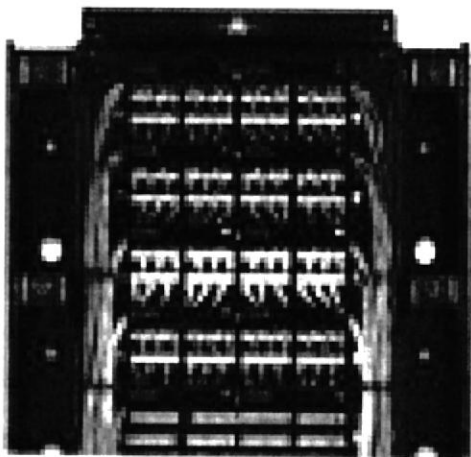


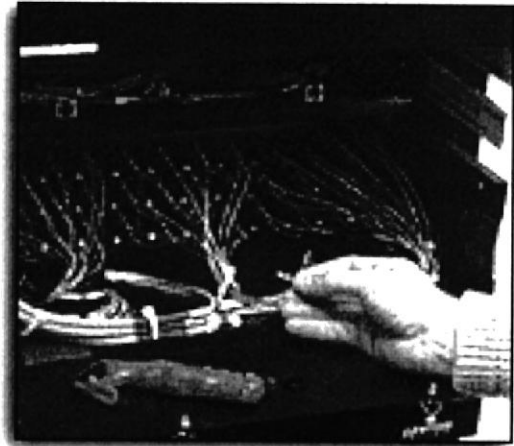
Figura 7-46 Normativa 46

7.1.47 **NORMATIVA 47** ▲

El cable que corra entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará expuesto en el área de trabajo ni en otros espacios de accesos públicos.



EN EL RACK



INTERPERIE

Figura 7-47 Normativa 47

7.1.48 **NORMATIVA 48** ▲

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

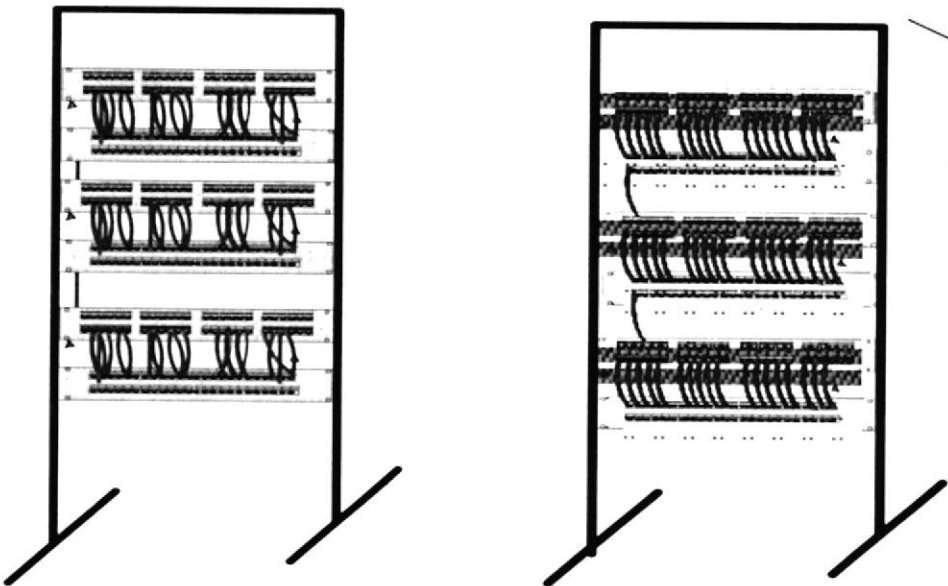


Figura 7-48 Normativa 48



7.1.49 **NORMATIVA 49** ▲

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

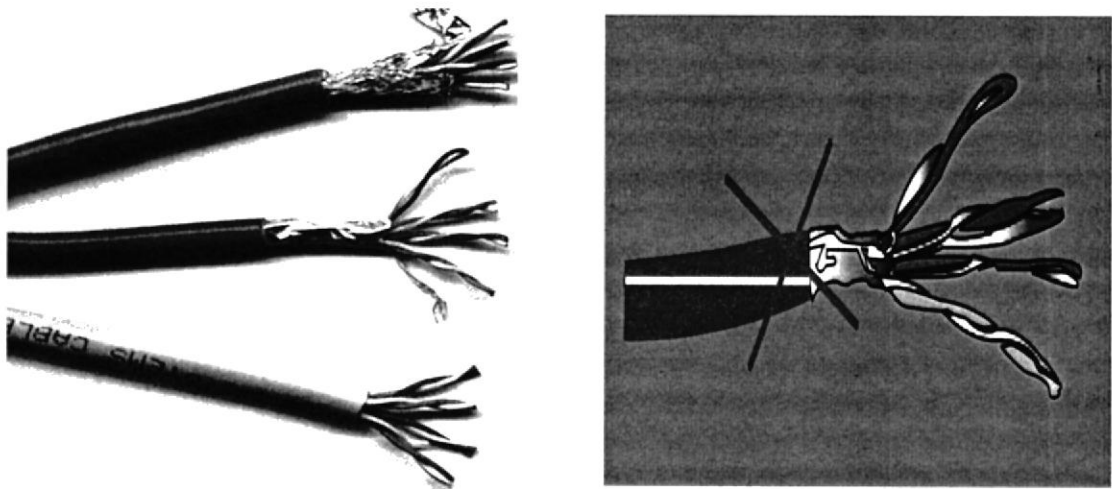


Figura 7-49 Normativa 49

7.1.50 **NORMATIVA 50** ▲

La cantidad máxima de desentrelazado de cada par resultan de de la terminación en el hardware de conexión, será de 13mm. Para cables de categoría 5E o mayor, y de 75mm. Para cable de categoría 3.

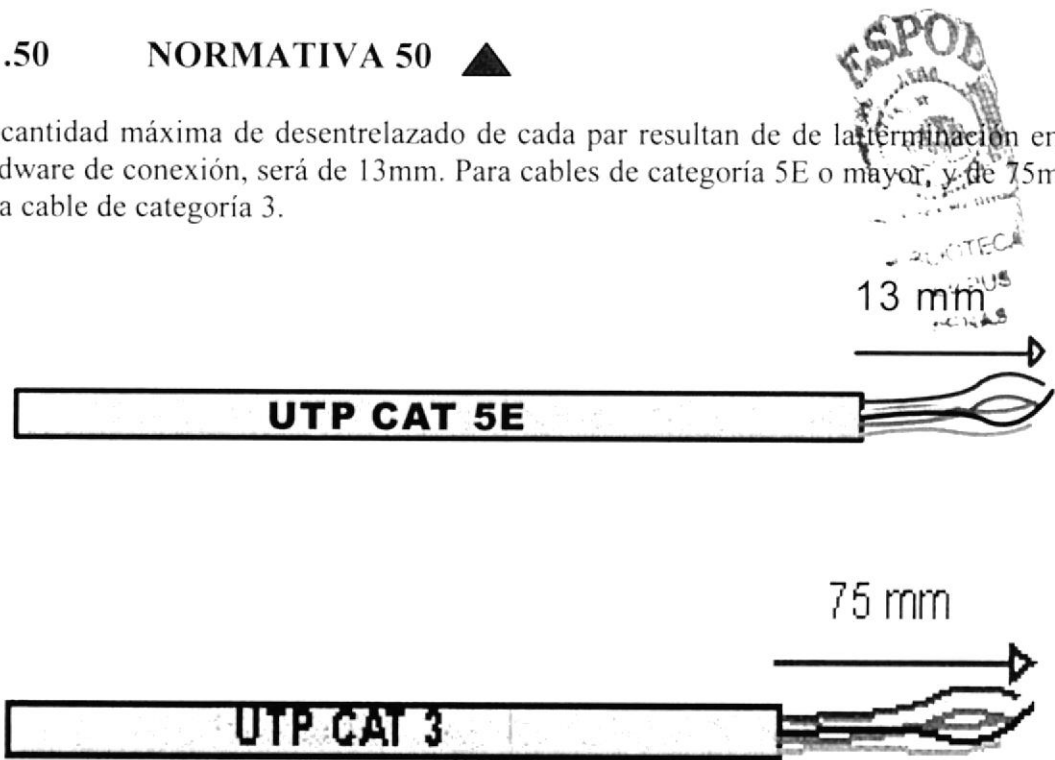


Figura 7-50 Normativa 50

7.1.51 **NORMATIVA 51** ▲

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

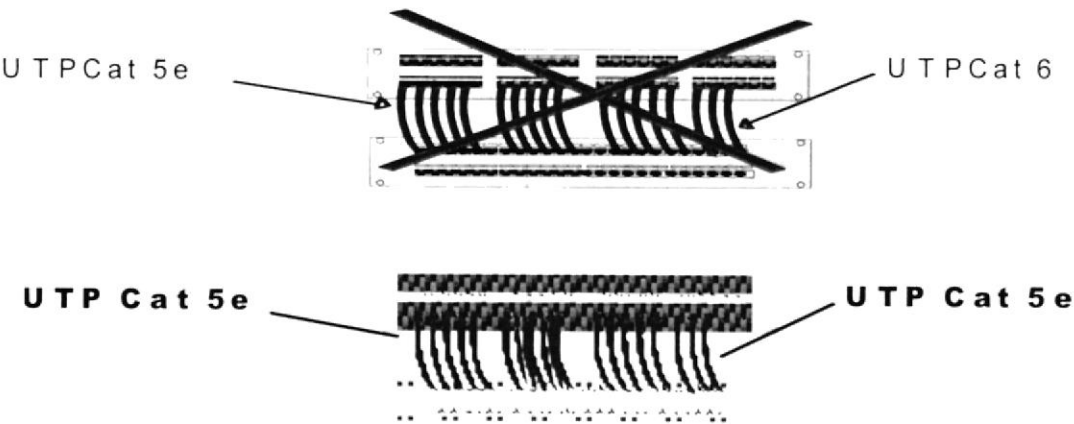


Figura 7-51 Normativa 51

7.1.52 **NORMATIVA 52** ▲

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

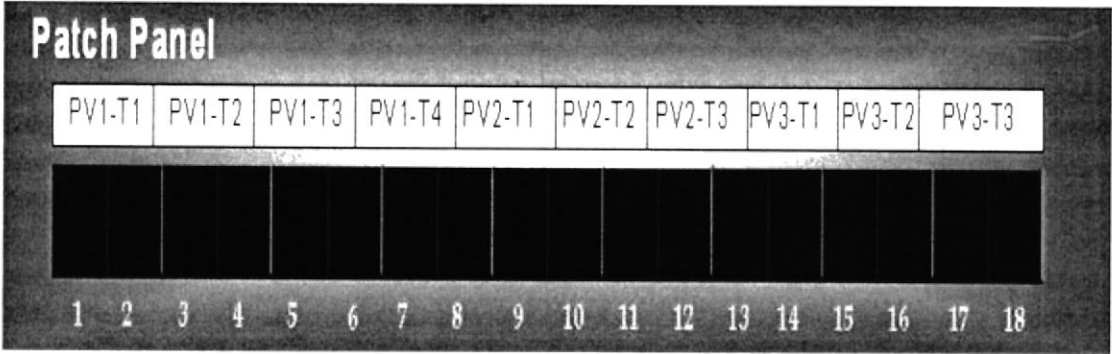


Figura 7-52 Normativa 52



7.1.53

NORMATIVA 53 ▲

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

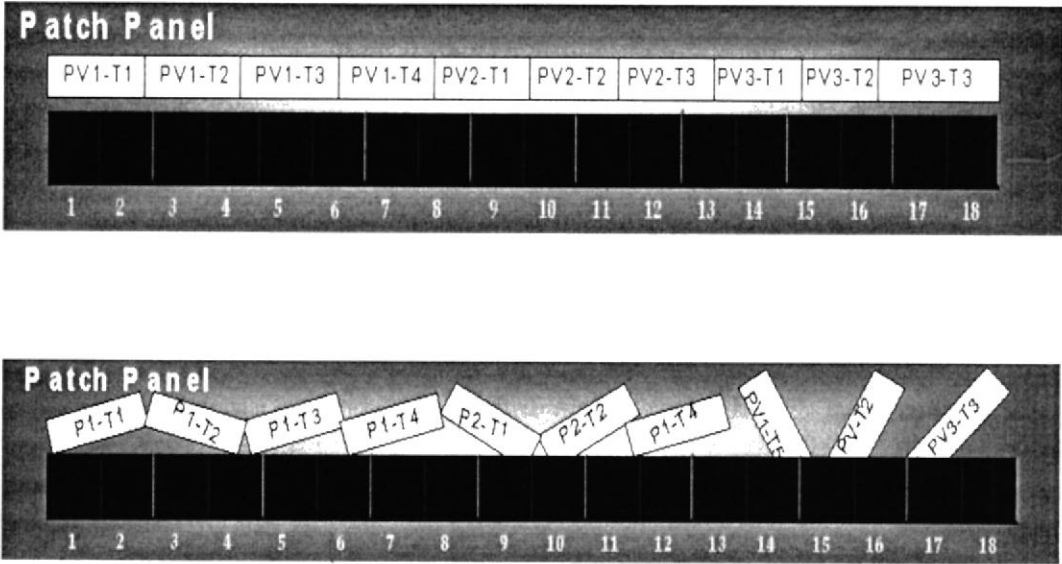


Figura 7-53 Normativa 53

7.1.54

NORMATIVA 54 ▲

El rotulado deberá ser legible y permanecer firmemente unido dentro del periodo de garantía (5 años dependiendo del fabricante).

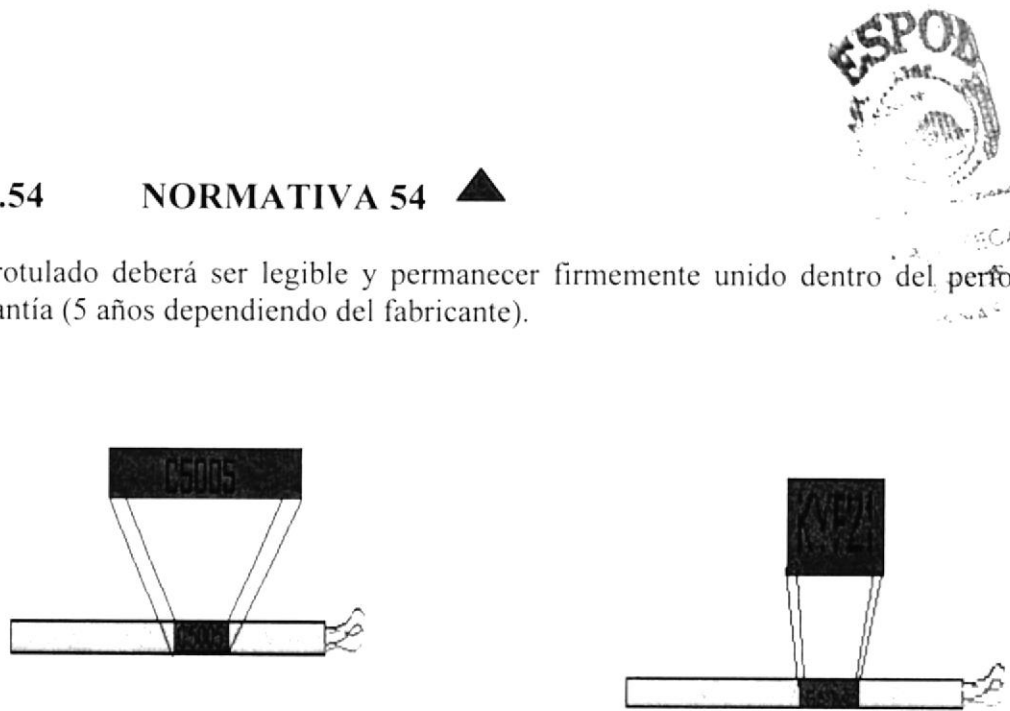


Figura 7-54 Normativa 54

7.1.55 **NORMATIVA 55** ▲

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

DESCRIPCIÓN	IDENTIFICADOR
Cable #9 de fibra óptica multimodo	FOM009
Cable #5 de utp cat 5e	C5005

Tabla 7-2 Cables con identificador

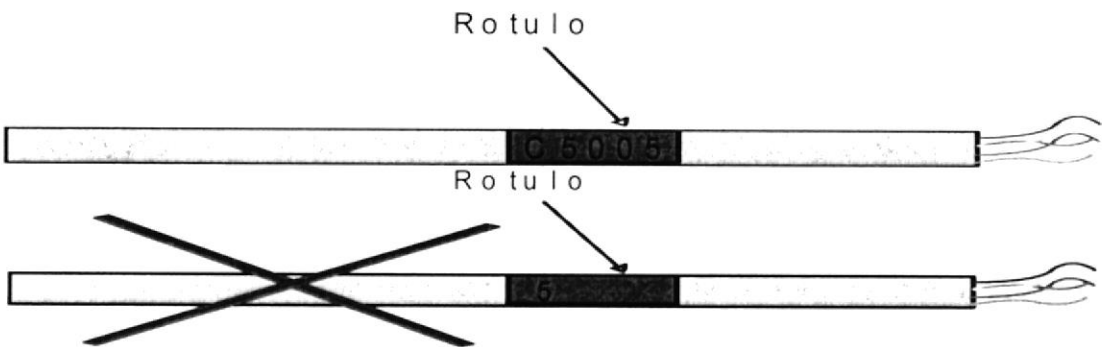


Figura 7-55 Normativa 55



7.1.56 **NORMATIVA 56** ▲

Los cables de los subsistemas horizontales de back bone deberán rotularse en cada extremo. La etiqueta puede ser colocada a 30cm. Del extremo del cable, esta marca deberá permanecer en el cable después de terminar la instalación.

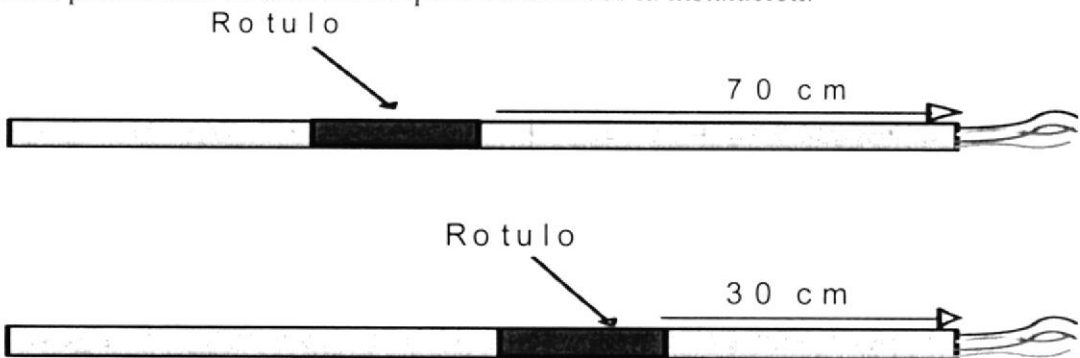


Figura 7-56 Normativa 56

7.1.57 RECOMENDACIÓN 1

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

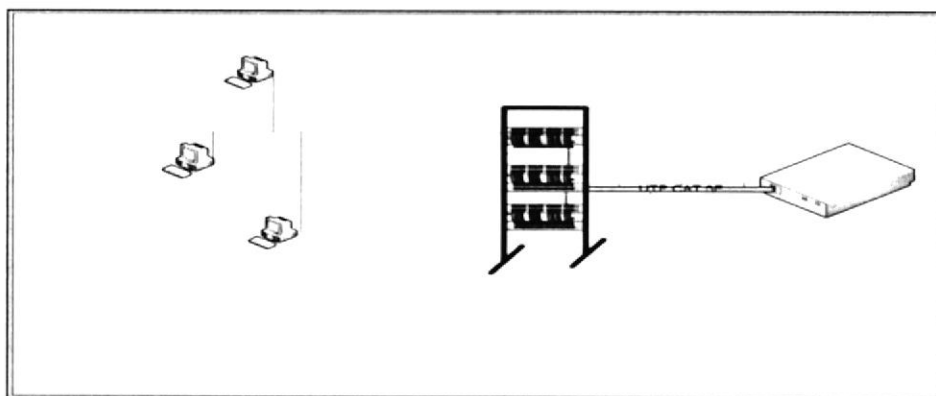


Figura 7-57 Recomendación 1

7.1.58 RECOMENDACIÓN 2

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

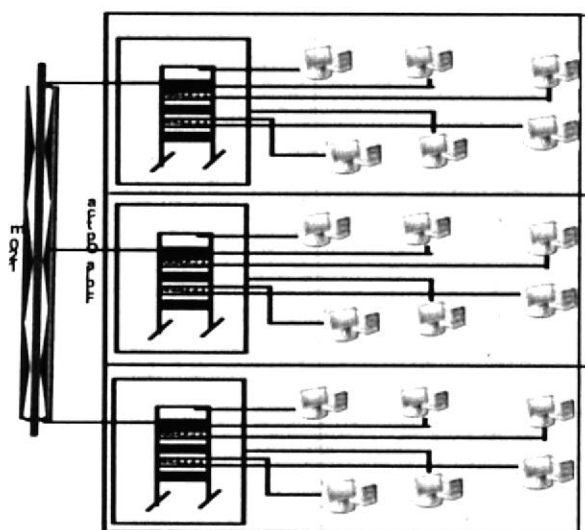


Figura 7-58 Recomendación 2



7.1.59 RECOMENDACIÓN 3

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

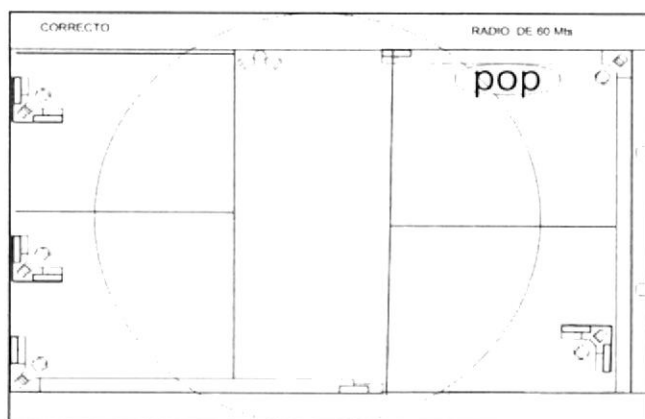


Figura 7-59 Recomendación 3

7.1.60 RECOMENDACIÓN 4

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



Figura 7-60 Recomendación 4

7.1.61

RECOMENDACIÓN 5

△

Se recomienda un mínimo de 2 salidas de categoría 6 por cada área de trabajo individual con el fin de soportar las numerosas complicaciones por operación sobre cableado por par trenzado.

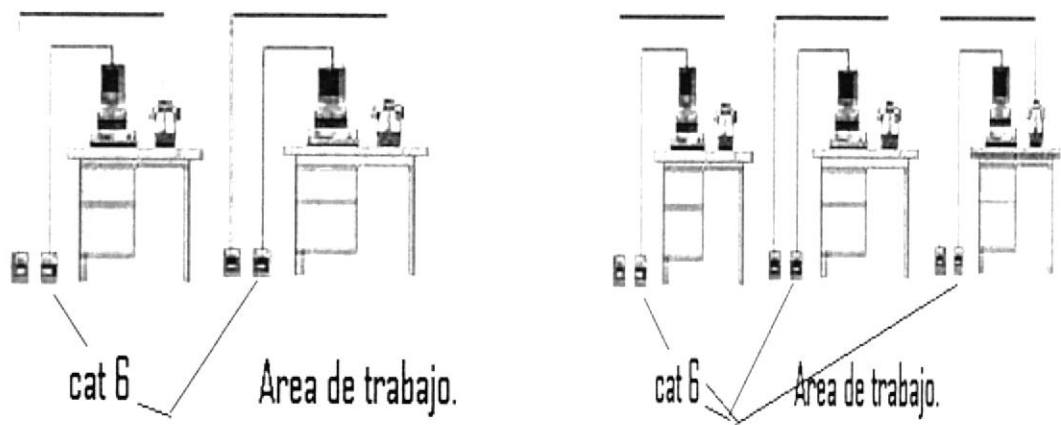


Figura 7-61 Recomendación 5

7.1.62

RECOMENDACIÓN 6

△

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

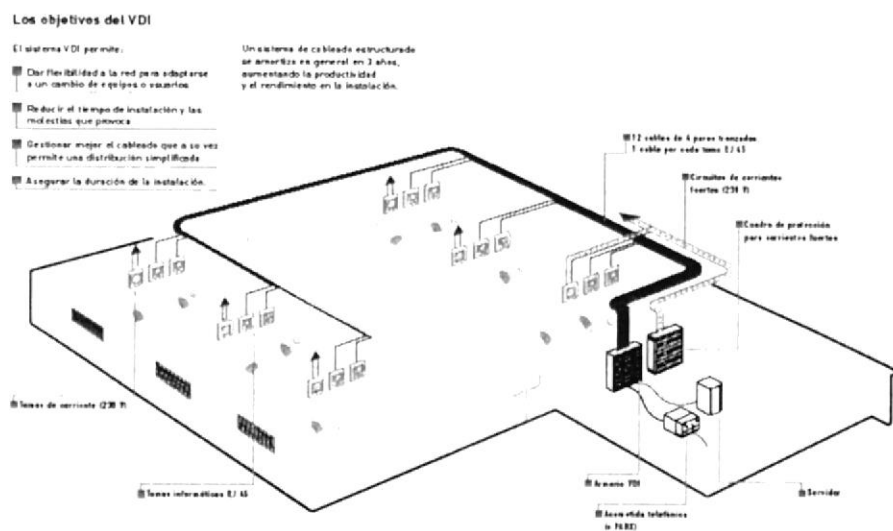


Figura 7-62 Recomendación 6

7.1.63 RECOMENDACIÓN 7

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

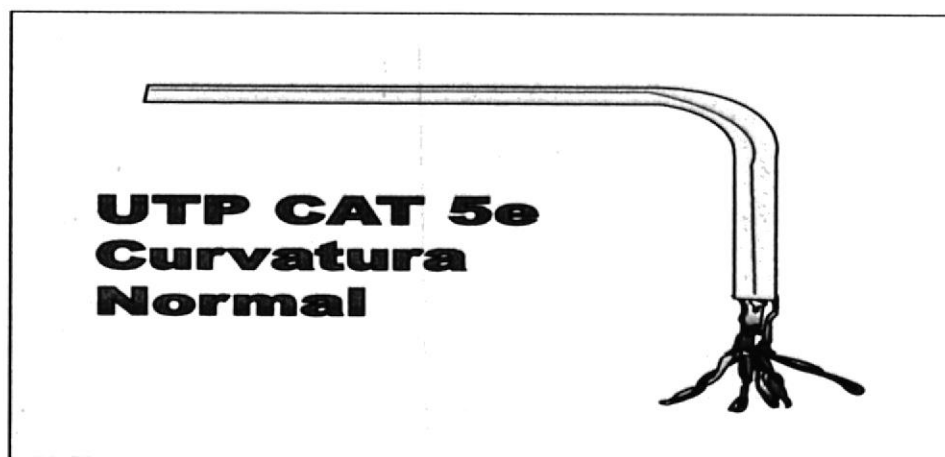


Figura 7-63 Recomendación 7

7.1.64 RECOMENDACIÓN 8

Ningún segmento del canal contendrá más de dos curvas de 90° entre puntos de acceso.

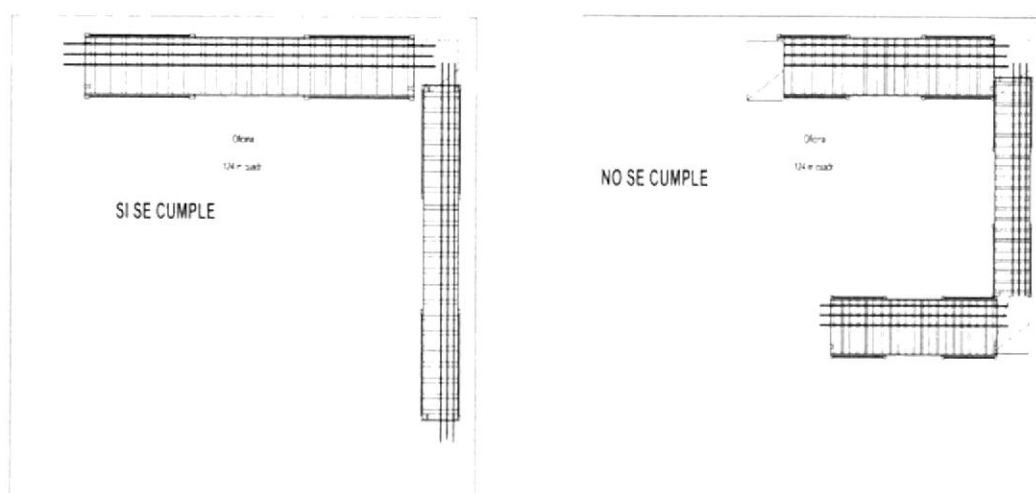


Figura 7-64 Recomendación 8

7.1.65 RECOMENDACIÓN 9

Se recomienda que se provean como mínimo 2 hilos de fibra óptica para cada aplicación conocida a atenderse por el sistema de back bone de edificio durante su periodo de planificación. Debe preverse un factor de crecimiento del 100%.

APLICACIÓN	NUMERO DE HILOS DE FIBRA
VOZ	2
VIDEO	2
LAN	2
CRECIMIENTO	6
TOTAL	12

Tabla 7-3 Uso de Hilos de fibra Óptica



Figura 7-65 Recomendación 9

7.1.66 RECOMENDACIÓN 10

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

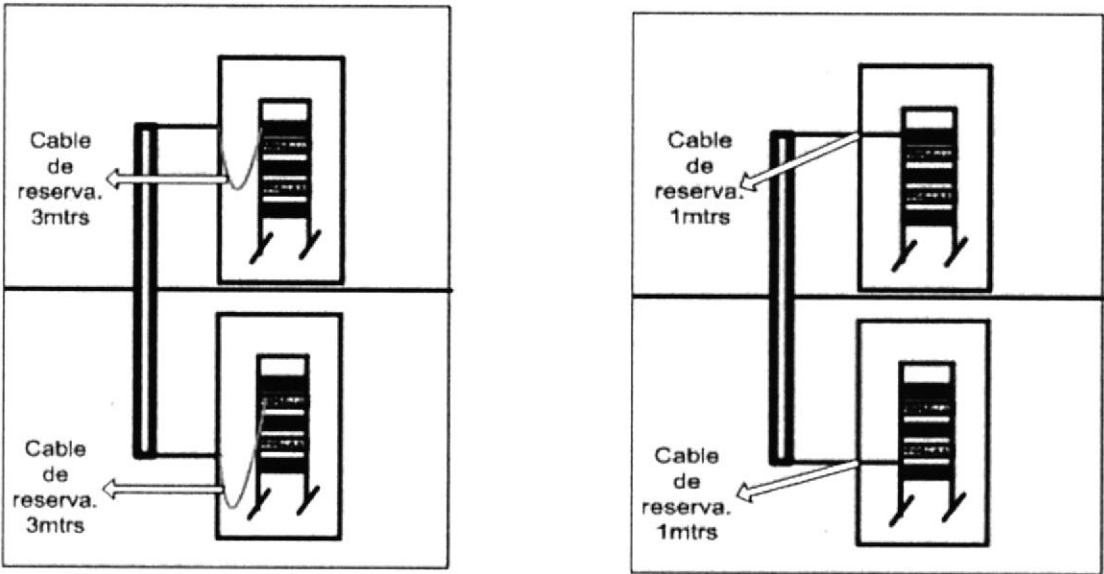


Figura 7-66 Recomendación 10

7.1.67 RECOMENDACIÓN 11

Los acabados en el cuarto de telecomunicaciones deberán ser de color claro para mejorar la iluminación del mismo.



Figura 7-67 Recomendación 11





ANEXO

GLOSARIO DE TERMINOS

GLOSARIO DE TÉRMINOS

A

Ancho de Banda: La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también se usa para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

Arp: Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Comparar con RARP.

Asignación de direcciones: Técnica que permite que distintos protocolos interoperen traduciendo direcciones desde un formato a otro. Por ejemplo, al enrutar IP a través de una red Frame Relay, las direcciones IP se deben mapear a las direcciones Frame Relay de modo que los paquetes IP se puedan transmitir por la red. Ver también resolución de direcciones.

B

Banda Ancha: Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica. Comparar con banda ancha.

Broadcast: Envío de información en cualquier formato a más de un lugar de destino

Banda Base: Característica de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha. Ver la diferencia con banda ancha. Término utilizado en la WWW.

Bps: (Bits per Second). Medida que representa la rapidez con que los bits de datos se transmiten a través de un medio de comunicaciones. Por ejemplo: un módem de 28.8 Kbps es capaz de transferir 28.800 bits por segundo.

Bit: (Binary Digit ó Dígito Binario). Es un dígito en base 2, es decir, 0 ó 1. Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

Byte: Unidad de medida de la cantidad de información en formato digital. Usualmente un byte consiste de 8 bits. Un bit es un cero (0) o un uno (1). Esa secuencia de números (byte) puede simbolizar una letra o un espacio (un carácter). Un kilobyte (Kb) son 1024 bytes y un Megabyte (Mb) son 1024 Kilobytes.

Bloqueo: En un sistema de conmutación, una condición en el que no hay ninguna ruta disponible para completar un circuito. El término también se usa para describir una

situación en la que no se puede iniciar una actividad hasta que la otra no se haya completado.

C

Cable blindado: Cable que posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

Cable coaxial: Cable compuesto por un conductor cilíndrico exterior hueco que rodea un conductor de alambre interno-único. En la actualidad se usan dos tipos de cable coaxial en la LAN: cable de 50 ohmios, que se usa para la señalización digital, y cable de 75 ohmios que se usa para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro, sin embargo no es susceptible a la interferencia electromagnética y es capaz de brindar velocidades de datos más altas.

Cable neutro: Cable de circuito que se conecta a la conexión a tierra en la central de energía y en el transformador.

Cableado backbone: Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN. Ver cableado vertical.

Cableado de Categoría 1: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 1 se usa para comunicaciones telefónicas y no es adecuado para transmitir datos. Comparar con cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 2: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 3: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 3 se usa en las redes 10BASE-T y puede transmitir datos a velocidades de hasta 10 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 4: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 4 se usa en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 5: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 4. Ver también EIA/TIA-568B UTP.

Caché: Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso más rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los accesos a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

Canaleta decorativa: Tipo de canal montado en la pared que tiene una cubierta removible que se usa para admitir el cableado horizontal. La canaleta decorativa es lo suficientemente grande como para contener dos cables.

Canaleta: Un tipo de canal adosado a la pared que tiene una cubierta removible para dar apoyo al cableado horizontal. La canaleta es lo suficientemente grande como para contener varios cables.

Capa física: La Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Capa de control de enlace de datos: La Capa 2 del modelo de arquitectura SNA. Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

Capa de red: La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

Capa de transporte: La Capa 4 del modelo de referencia OSI. Esta capa es responsable de la comunicación confiable de red entre nodos finales. La capa de transporte suministra mecanismos para establecer, mantener y terminar los circuitos virtuales, detección y recuperación de errores de transporte y control del flujo de información.

Capa de sesión: La Capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de capa de presentación.

Capa de servicios de presentación: La Capa 6 del modelo de arquitectura SNA. Esta capa suministra administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Corresponde aproximadamente a la capa de presentación del modelo OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control física, capa de servicios de transacción y capa de control de transmisión.

Capa de aplicación: La Capa 7 del modelo de referencia OSI. Esta capa suministra servicios a los procesos de aplicación (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de Terminal) que están fuera del modelo OSI. La capa de aplicación identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos que se requieren para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos. Corresponde aproximadamente a la capa de servicios de transacción del modelo SNA. Ver también capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

Cliente: Nodo que solicita servicios a un servidor.

Colisión: En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

Cola: Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

Conector RJ: Conector macho registrado. Conectores estándar que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ.

Costo: Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.

Consola: DTE a través del cual se introducen los comandos en un host.

Correo electrónico: Aplicación de red utilizada ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.

CSMA/CD: Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

Click: Acción de presionar y soltar rápidamente el botón del mouse (ratón).

Cliente: Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para

trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

Computador: Es un dispositivo electrónico compuesto básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

Contraseña ó Password: Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los Sistemas y recursos de la computadora.

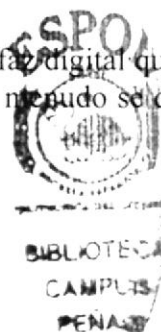
CPU; (Centra] Processirjg Unit ó Unidad central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

Cuadro de Diálogo: Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

Cuadro de Texto: Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de diálogo, el cuadro de texto puede estar en blanco o contener texto.

Cursor: Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo carácter a visualizar cuando se pulse uñatéela.

CSU: Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con el loop telefónico digital local. A menudo se denomina, de forma conjunta con DSU, como CSU/DSU.



D

Db: Decibelios

Dominio: En Internet, una parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía.

DCE: Equipo de comunicación de datos (expansión EIA) o equipo de terminación de circuito de datos (expansión ITU-T). El dispositivo y las conexiones de una red de comunicaciones que abarca el extremo de la red de la interfaz usuario a red. El DCE proporciona una conexión física con la red, envía tráfico y suministra una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE. Comparar con DTE.

Descifrado: La aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando por lo tanto los datos a su estado original, no cifrado.

Dato: Son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

DTE: Equipo de terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario-red que actúa como origen de datos, destino de datos o ambas. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y por lo general usa señales de temporización generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadores, traductores de protocolo y multiplexores.

Directorio: En D.O.S., una lista de nombres de archivo que contiene toda la información de los archivos almacenados. A partir de Windows 95 este término se reemplazó por CARPETA.

Dirección: Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico* (emáil address); "IP" y (direccion de Internet) y "dirección hardware".

Dirección del Protocolo de Internet (dirección IP): Dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red con Protocolo de control de transmisión/Protocolo Internet (TCP/IP). Número único que consta de 4 partes separadas por puntos. Una dirección IP se suele representar en una flotación decimal con puntos que indica cada octeto (ocho bits o un byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 172.16.255.255.

Cada computadora conectada a Internet tiene un único número de IP. Si la máquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem).

Disco Rígido: Unidad de almacenamiento permanente de información. Éste es el que guarda la información cuando apagamos la computadora. Aquí se guardan la mayoría de los programas y el sistema operativo. Su capacidad de almacenamiento se mide en Megabytes (Mb) o Gigabytes (Gb), en donde $1024 \text{ Mb} = 1 \text{ Gb}$.

Disquete: Dispositivo que puede insertarse y extraerse en una unidad de disco.

DNS: (Domain Name System ó Sistema de Nombres de Dominio). El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de éstos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes son: .COM (comercial - empresas), .EDU (educación, centros docentes), .ORG (organización sin ánimo de lucro), .NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejército USA). La mayoría de los países tienen un dominio propio. Por ejemplo, AR (Argentina) .PY (Paraguay), .US (Estados Unidos de América), .ES (España), .AU (Australia), etc.

Dominio: (Domain Name). Nombre único que identifica a un sitio de Internet. Los nombres de dominio tienen 2 o más secciones, separadas por puntos. La sección de la izquierda es la más específica, y la de la derecha, la más general. Una computadora particular puede tener más de un nombre de dominio, pero un nombre de dominio se refiere únicamente a una PC.

Download ó descargar: En Internet es el proceso de transferir información desde un servidor de información a la propia PC.

Documentación: Manual escrito que detalla el manejo de un sistema o pieza de hardware.

Doble Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón) dos veces, sin desplazarlo. Esta acción sirve para ejecutar una determinada aplicación, como por ejemplo: inicializarla.

DSU: Unidad de servicio de datos. Dispositivo que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión como, por ejemplo, TI y El.

DVD: (Digital Versatile Disc ó Disco Versátil Digital). Disco que sirve para almacenar más datos de contenido digital, como música o video, que un CD. Un DVD guarda un mínimo de 4.7 Gigabytes (el tamaño de una película de cine).

E

EI: Estándar Europeo equivalente al americano TI. Los circuitos EI y TI. Los dos usan canales de 64 Kbps, pero el TI tiene 24 mientras que el EI tiene 32 canales.

EIA/TIA-568: Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

Encapsulamiento: El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

Emulación de terminal: Aplicación de red en la que un computador ejecuta software que la hace aparecer ante un host remoto como una terminal conectada directamente.

Enrutamiento: Proceso para encontrar una ruta hacia un host destino. El enrutamiento en redes de gran tamaño es muy complejo dada la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ethernet: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3. Ver también IOBASE2, IOBASE5, IOBASE-F, IOBASE-T, IOBase36 e IEEE 802.3.

Elemento de Pantalla: Partes que constituyen una ventana o cuadro de diálogo como por ejemplo: la barra de título, los botones de "Maximizar" y "Minimizar", los bordes de las ventanas y las barras de desplazamiento.

Escritorio: Fondo de la pantalla sobre la cual aparecen ventanas, iconos y cuadros de diálogo.

Estación de trabajo: Computador de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. Llamadas así para distinguirlas de los que se conocen como servidores.

Expandir: Mostrar los niveles de directorio ocultos del árbol de directorios. Con el administrador de archivos es posible expandir un solo nivel de directorio, una rama del árbol de directorio o todas las ramas a la vez.

Explorador: Llamado también explorador Web. Interfaz cliente que permite al usuario ver documentos HTML en el World Wide Web, en otra red o en su propio equipo; seguir los hipervínculos y transferir archivos. Un ejemplo es Microsoft Internet Explorer.

Extensión: Está compuesto por un punto y un sufijo de hasta tres caracteres situados al final de un nombre de archivo. La extensión suele indicar el tipo de archivo o directorio.

F

Fibra monomodo: Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único. Ver también fibra multimodo.

Fibra multimodo: Fibra óptica que permite la propagación de múltiples frecuencias de luz.

Firewall: Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Fluctuación de fase: Distorsión analógica de la línea de comunicación provocada por la variación de una señal de sus posiciones de temporización de referencia. La fluctuación de fase puede provocar la pérdida de datos, especialmente a altas velocidades.

Flujo de datos: Todos los datos que se transmiten a través de la línea de comunicaciones en una sola operación de lectura o escritura.
Frecuencia: Cantidad de ciclos, medidos en hercios, de una señal de corriente alterna por unidad de tiempo.

FTP: Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP, que se usa para transferir archivos entre nodos de la red. El FTP se define en la RFC 959.

Full dúplex: Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora.

G

Gateway: En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función, y gateway se refiere a un dispositivo con fines especiales que ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra.

Gateway fronterizo: Router que se comunica con routers de otros sistemas autónomos.

Giga: Prefijo que indica un múltiplo de 1.000 millones, o sea 10⁹. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 1.073.741.824.

Grupo de trabajo: Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

H

Hardware: Son todos los componentes físicos que componen una PC.

Hercio: Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

Hexadecimal: Base 16. Representación numérica que usa los dígitos 0 a 9, con su significado habitual, y las letras A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, luego $16A2=256$, etc.

Host: Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

HTML: (HyperText Markup Language). Lenguaje utilizado para crear los documentos de hipertexto que se emplean en la WWW. Los documentos HTML son simples archivos de texto que contienen instrucciones (llamadas tags) entendibles por el Navegador (Browser).

HTTP: (HyperText Transport Protocol). Protocolo utilizado para transferir archivos de hipertexto a través de Internet. Requiere de un programa "cliente" de HTTP en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la WWW.

Hub: Dispositivo de hardware o software que contiene módulos de red y equipo de internetwork múltiples, independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen, las señales que se envían a través de ellos).

1

IEEE: Instituto de ingenieros eléctricos y electrónicos. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN del IEEE son los estándares de LAN predominantes en el mundo actual.

IEEE 802.1: Especificación del IEEE que describe un algoritmo que evita los loops de capa dos mediante la creación de un spanning tree. El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo de Digital y el algoritmo IEEE 802.1 no son exactamente los mismos, ni tampoco son compatibles.

IEEE 802.12: Estándar LAN del IEEE que especifica la capa física y la subcapa MAC de la capa de enlace de datos. El IEEE 802.12 usa el esquema de acceso a los medios de prioridad de demanda a 100 Mbps a través de una diversidad de medios físicos. Ver también 100 VG-Any LAN.

IEEE 802.2: Protocolo LAN del IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 administra errores, entramado,

control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se usa en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3: Protocolo LAN del IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 usa acceso CSMA/CD a diversas velocidades sobre diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican las implementaciones de Fast Ethernet. Las variantes físicas de la especificación IEEE 802.3 original incluyen IOBASE2, IOBASE5, IOBASE-F, IOBASE-T y IOBroad36. Las variantes físicas de Fast Ethernet incluyen IOBASE-T, IOBASE-T4y IOBASE-X.

Icono: Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc.

IDF: Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

Impresora: Dispositivo de salida, cuya funcionalidad es transcribir/pasar un documento (imagen y/o texto) desde el ordenador (procesador de textos, bloc de notas, visor de imágenes, etc.) a un medio físico, generalmente papel, mediante el uso de cinta, cartuchos de tinta o también con tecnología láser.

Impresora de Inyección a tinta: Crean imágenes directamente sobre el papel al rociar tinta a través de unas pequeñas boquillas, su calidad de impresión es bastante alta.

Impresora Predeterminada: Impresora que se utiliza si se elige el comando Imprimir, no habiendo especificado antes la impresora que se desea utilizar. Solo puede haber una impresora predeterminada, que debe ser la que se utilice con mayor frecuencia.

Información: Es lo que se obtiene del procesamiento de datos, es el resultado final.

Informática cliente-servidor: Término que se usa para describir los sistemas de red informáticos distribuidos (de procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: cliente (front end) y servidor (back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos actuales.

Internetwork: Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red.

IP: Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad. Documentado en la RFC 791.

IP access-group: Comando que enlaza una lista de acceso existente con una interfaz de salida.

IP host: Comando que se usa para crear una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.

IP multicast: Técnica de enrutamiento que permite que el tráfico IP se propague desde un origen hacia un número de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, se envía un paquete a un grupo de multicast que se identifica mediante una sola dirección de grupo de destino IP.

IPX: Intercambio de paquetes de internetworking. Protocolo de capa de red (Capa 3) de NetWare que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

Interfaz: Una conexión e interacción entre hardware, software y usuario, es decir, como la plataforma o medio de comunicación entre usuario o programa.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

Intranet: Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno.

ISO: Organización Internacional de Normalización. Organización internacional que es responsable por una amplia gama de estándares, incluyendo aquellos relevantes para el networking. ISO desarrolló el modelo de referencia OSI, un modelo de referencia de networking sumamente popular.

J

Jumper: Término que se usa para los cables de interconexión que se encuentran en el armario de cableado.

K

Kbps: (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit está formado por mil bits.

Kilobyte: Es el equivalente a 1024 bytes.

L

LAN: Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de



enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido. Comparar con MAN y WAN.

Latencia: Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir también sucede en el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

LED: Diodo emisor de luz. Dispositivo semiconductor que emite luz producida por la conversión de energía a eléctrica. Las lámparas de estado en los dispositivos de hardware generalmente son LED.

Línea de acceso telefónico: Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

Línea de comunicación: Enlace físico (como, por ejemplo, un cable o circuito de teléfono) que conecta uno o más dispositivos con uno o más dispositivos.

Línea de mira: Característica de determinados sistemas de transmisión como, por ejemplo, los sistemas láser, de microondas e infrarrojos, en los que no puede existir ninguna obstrucción en la ruta directa entre el transmisor y el receptor.

Línea dedicada: Línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir. Ver también línea arrendada.

Lista de acceso: Lista que mantienen los routers Cisco para controlar el acceso hacia o desde el router para diversos servicios (por ejemplo, para evitar que los paquetes que tienen una determinada dirección IP salgan de una interfaz específica del router).

LSA: Publicación de estado de enlace. Paquete de broadcast que usan los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de la ruta. Los routers receptores usan las LSA para mantener sus tablas de enrutamiento.

Login: Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del password, el login no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

M

MAC: Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

MICIP: Protocolo de capa de red que encapsula paquetes IP en DDS o transmisión a través de AppleTalk.

Malla: Topología de red en la que los dispositivos se organizan de una manera administrable, segmentada, con varias interconexiones, a menudo redundantes, ubicadas estratégicamente entre nodos de la red. Ver también malla completa y malla parcial.

Malla completa: Término que describe a una red en la que los dispositivos están organizados en una topología de malla, en la que cada nodo de la red tiene un circuito físico o un circuito virtual que lo conecta a todos los otros nodos de la red. Una malla completa brinda una gran cantidad de redundancia pero, dado que su implementación puede resultar excesivamente cara, generalmente se la reserva para los backbones de la red. Ver también malla y malla parcial.

MAN: Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

MAP: Protocolo de automatización de fabricación. Arquitectura de red creada por General Motors para satisfacer las necesidades específicas las instalaciones fabriles. El MAP especifica una LAN de transmisión de tokens similar a IEEE 802.4. Ver también IEEE 802.4. –

Mapa de cableado: Característica suministrada por la mayoría de los analizadores de cable. Se usa para probar las instalaciones de cableado de par trenzado, y muestra cuáles hilos están conectados a cuáles pines, en conectores macho y hembra.

Mapa de topología: Herramienta para administrar un switch ATM LightStream 2020 que examina una red y muestra el estado de sus nodos y enlaces troncales. El mapa de topología es una aplicación basada en HP OpenView que se ejecuta en un NMS.

Máscara de red: Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

Máscara wildcard: Cantidad de 32 bits que se usan de forma conjunta con una dirección IP para determinar cuáles son los bits de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

MDF: Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

Megabyte (MB): 1.048.576 bytes; 1.024 Kilobytes.

Megahertz: Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

Memoria RAM: Memoria de acceso aleatorio cuyo contenido permanecerá presente mientras el computador permanezca encendido.

Memoria ROM: Memoria de sólo lectura. Chip de memoria que sólo almacena permanentemente instrucciones y datos de los fabricantes.

Microonda: este enlace esta constituido por dos transceptores de radio provistos de antenas parabólicas que se apuntan directamente entre si. La radio puede transportar transmisiones punto a punto de muchos anchos de banda. Su alcance varia según el tamaño de la antena, el clima en la zona y la magnitud de la potencia emitida contemplando todos estos conjuntos la señal puede llegar hasta 80 Km.

Módem: (Modulator, Demodulator). Dispositivo que se conecta a la computadora y a la linea telefónica y que permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

Mouse: Permite convertir el movimiento de la mano en desplazamiento de un cursor obre la pantalla.

Multicast: la multidifusión (multicast) permite que grupos de usuarios seleccionados reciban la misma transmisión de datos en una red los cuales están identificados por una mica dirección de grupo de destino IP.

N



Navegador de Web: Aplicación de cliente de hipertexto basada en GUI como, por ejemplo, Mosaic, que se usa para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a través de la WWW e Internet. Ver también hipertexto, Internet, Mosaic y WWW.

NBP: Protocolo de enlace de denominación. Protocolo AppleTalk de nivel de transporte que convierte un nombre dado en forma de una cadena de caracteres en una dirección de internetwork.

NET: Título de entidad de red. Direcciones de red, definidas por la arquitectura de red ISO.

NetBIOS: Sistema básico de entrada/salida de red. API que usan las aplicaciones de una LAN IBM para solicitar servicios de procesos de red de nivel inferior. Estos servicios pueden incluir establecimiento y terminación de sesión y transferencia de información

NetWare: NOS distribuido de uso generalizado desarrollado por Novell. Suministra acceso remoto transparente a archivos, y muchos otros servicios de red distribuida.

Networking: Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NIC: Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

NOS: Sistema operativo de red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos. Los ejemplos de NOS incluyen LAN Manager, NetWare, NFS y VINES.

Número de host: Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

Número de red: Parte de una dirección IP que especifica la red a la que pertenece el host.

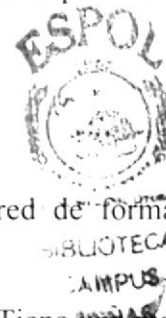
Número de saltos: Métrica de enrutamiento que se usa para medir la distancia entre un origen y un destino. El RIP usa el número de saltos como su única métrica.

NVRÁM: RAM no volátil. RAM que retiene su contenido cuando una unidad se apaga. En los productos Cisco, la NVRAM se usa para guardar la información de configuración.

Nodo: En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma.

Nombre de usuario: La secuencia de caracteres que lo identifica. Al conectarse a una computadora, generalmente necesita proporcionar su nombre y contraseña de usuario. Esta información se usa para verificar que la persona está autorizada para usar el Sistema.

O



Operador de red: Persona que monitorea y controla una red de forma continua, ejecutando tareas varias.

Oscilación: Señal secundaria superpuesta a la onda de 60 Hz. Tiene una magnitud que varía entre el 15% y el 100% del voltaje normal de la línea de alimentación. Ver sobrevoltaje, pico y baja de voltaje.

OSI: Interconexión de sistemas abiertos. Programa internacional de normalización creado por la ISO y la UIT-T para desarrollar estándares de interconexión que faciliten la interoperabilidad de equipos de múltiples proveedores.

OSINET: Asociación internacional diseñada para promover OSI en las arquitecturas de los proveedores.

OSPF: Versión abierta del algoritmo "Primero la ruta libre más corta". Algoritmo de enrutamiento TOP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad Internet. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga. El OSPF deriva de una versión inicial del protocolo ISIS.

P

PAD: Ensamblador/desamblador de paquetes. Dispositivo que se usa para conectar dispositivos simples (como terminales de modo de carácter) a una red, los cuales no admiten toda la funcionalidad de un protocolo específico. Los PAD almacenan los datos en el búfer de los PAD y ensamblan y desensamblan los paquetes que se envían a dichos dispositivos finales.

Panel de conexión: Conjunto de ubicaciones de pm y puertos que se puede montar en un bastidor o una consola de pared en el armario de cableado. Los paneles de conexión actúan como conmutadores que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

Paquete de choque: Paquete que se envía al transmisor para informarle que hay congestión y que debe reducir su velocidad de envío.

Par trenzado: Medio de transmisión de relativa baja velocidad compuesto por dos cables aislados dispuestos en un patrón en espiral regular. Los cables pueden ser blindados o no blindados. El uso del par trenzado es común en aplicaciones de telefonía y es cada vez más común en las redes de datos. Ver también STP y UTP.

Paradiafonía: Energía de interferencia transferida de un circuito a otro.

PBX: Central telefónica privada. Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas y públicas.

PCI: Información de control de protocolo. Información de control que se agrega a los datos del usuario para formar un paquete OSI.

Pila de protocolo: Conjunto de protocolos de comunicación relacionados que operan de forma conjunta y, como un grupo, cumplen con la comunicación en alguna o en las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo y, a menudo, un solo protocolo de la pila se dirige a una cantidad de capas a la vez. El TCP/IP es un protocolo de pila típico.

Ping: Abreviatura para Packet Internet Groper o Packet Inter-network Groper, una utilidad que se usa para determinar si una dirección IP en particular está disponible. Funciona enviando un paquete a la dirección especificada y esperando una respuesta. El PING se usa principalmente para diagnosticar las fallas de las conexiones de Internet.

Plan de distribución: Diagrama simple que indica dónde están ubicados los tendidos de cable y la cantidad de habitaciones hacia las que se dirigen.

POP: Punto de presencia. Punto de presencia es el punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y el servicio de distribución principal del edificio.

Portadora: Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos. Ver también modulación.

POST: Autocomprobación de encendido. Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando ese dispositivo se enciende.

Protocolo de enrutamiento: Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. Los ejemplos de protocolos de enrutamiento incluyen el IGRP, el OSPF y el RIP.

Puerto: Interfaz de un dispositivo de internetworking (como, por ejemplo, un router) En terminología ip, un proceso de capa superior que recibe información de las capas Inferiores. Un conector hembra de un panel de conexión el cual acepta el mismo tamaño de conector que el de un rj45. Los cables de conexión se usan en estos puertos para realizar interconexiones entre los computadores conectados al panel. Es esta interconexión la que permite la operación de la lan.

Página Web: Documento de World Wide Web. Una página Web suele consistir en un archivo HTML, con sus archivos asociados de gráficos y secuencias de comandos, en un directorio determinado de un equipo concreto (y, por tanto, identificable mediante una dirección URL).

Periféricos: Cualquier dispositivo de hardware conectado a una computadora.

Pixel: (PICture cELL). Es la parte más pequeña de una pantalla de video, constituido por uno o más puntos que se consideran como una unidad. Es por tanto el bloque de construcción de imágenes.

Protocolo: Método por el que los equipos se comunican en Internet. El protocolo más común en el World Wide Web es HTTP. Otros protocolos de Internet incluyen FTP, Gopher y telnet. El protocolo forma parte de la dirección URL completa de un recurso.

Proveedor: Institución o empresa que provee acceso a uno o varios servicios de Internet.

R

RAM: Memoria de acceso directo aleatorio. Memoria volátil que puede ser leída y escrita por un microprocesador.

Red: Conjunto de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red de conexión única: Red que tiene una sola conexión con un router

Redireccionar: Parte de los protocolos ICMP y ES-IS que permiten que un router le indique a un host que puede ser más efectivo usar otro router.

Redistribución: Permitir que la información de enrutamiento detectada a través de un protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento. A veces denominada redistribución de ruta.

Redundancia: En internetworking, la duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan ejecutar el trabajo de aquellos que han fallado. Ver también sistema redundante.

Rendimiento: Velocidad de la información que llega a, y posiblemente atraviesa, un punto particular de un sistema de red.

Repetidor: Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red.

Retardo: El tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. También, el tiempo que se requiere para mover un paquete desde el origen hacia el destino a través de una ruta específica.

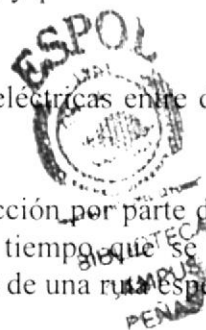
RF: Radiofrecuencia. Término genérico que se usa para referirse a frecuencias que corresponden a transmisiones radioeléctricas. Las redes de televisión por cable y de banda ancha usan tecnología RF.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

RIP: Protocolo de información de enrutamiento. IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet.

RMON: Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitoreo remoto de los dispositivos conectados a la red.

ROM: Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.



Ruta estática: Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

Ruta por defecto: Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

S

Segmento: La sección de una red limitada por puentes, routers o switches. Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

SMTP: Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico

Sondeo: Método de acceso en el que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

Switch: Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

Switch LAN: Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches LAN envían tráfico basándose en las direcciones MAC. Esta variedad de switch LAN a veces se denomina switch de trama. Los switches LAN a menudo se clasifican de acuerdo con el método que usan para enviar tráfico: conmutación de paquetes por método de corte y conmutación de paquetes por almacenamiento y envío. Los switches multicapas son un subconjunto inteligente de los switches LAN.

Servidor: Computadora o programa que brinda un servicio específico al "cliente", que se ejecuta en otras computadoras. El término puede referirse tanto a un equipo de una red que envía archivos o ejecuta aplicaciones para otros equipos de la red; el software que se ejecuta en el equipo servidor y que efectúa la tarea de servir archivos y ejecutar aplicaciones; o bien, en la programación orientada a objetos, un fragmento de código que intercambia información con otro fragmento de código cuando se pide.

SO: (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software: Todos los componentes no físicos de una PC (Programas).

T

TI: Servicio de portadora de WAN digital. TI transmite datos con formato DS-1 a 1.544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o B8ZS. Comparar con El. Ver también AMI, B8ZS y DS-1.

Tabla de enrutamiento: Tabla que se guarda en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas hacia destinos de red en particular y, en algunos casos, las métricas asociadas con esas rutas.

TFTP: Protocolo de Transferencia de Archivos Trivial. Versión simplificada del FTP que permite que los archivos se transfieran desde un computador a otra a través de una red.

Terminal: Dispositivo simple en el que los datos se pueden introducir o recuperar desde una red. Generalmente, las terminales tienen un monitor y un teclado pero no tienen ningún procesador ni unidad de disco local.

Topología: Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

Topología de anillo: Topología de red que consta de un conjunto de repetidores conectados entre sí mediante enlaces de transmisiones unidireccionales para formar un solo bucle cerrado. Cada estación de la red se conecta a la red en el repetidor. Aunque lógicamente están organizadas en anillo, las topologías de anillo a menudo están organizadas en una estrella de bucle cerrado.

Topología de bus: Arquitectura LAN lineal en la que las transmisiones de las estaciones de red se propagan a lo largo del medio y son recibidas por todas las otras estaciones.

Topología en árbol: Topología LAN similar a la topología bus, salvo que las redes en árbol pueden tener ramificaciones con múltiples nodos. Las transmisiones desde una estación atraviesan la longitud del medio y son recibidas por todas Las otras estaciones.

Topología en estrella: Topología LAN en la que los puntos de terminación de una red se conectan a un switch central común mediante enlaces punto a punto. Una topología de anillo que está organizada como estrella implementa una estrella de loop cerrado unidireccional en lugar de enlaces punto a punto.

Topología en estrella jerárquica: Topología en estrella extendida en la que un hub central se conecta a través de cableado vertical con otros hubs que dependen del mismo.

Transceiver: Unidad de conexión al medio. Dispositivo que se usa en las redes Ethernet e IEEE 802.3 que suministra la interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que se puede incorporar a una estación o puede ser un dispositivo individual, ejecuta funciones de capa física, incluyendo la conversión

de datos digitales desde la interfaz Ethernet, detección de colisiones e inyección de bits en la red.

Tunneling: Arquitectura que está diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.

Tarjeta de Interfaz de Red: (NIC). Dispositivo a través del cual computadoras de una red transmiten y reciben datos.

TCP/IP: (Transmisor Control Protocol/Internet Protocol). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

Telnet: Protocolo que permite al usuario de Internet conectarse y escribir comandos en un equipo remoto vinculado a Internet como si el usuario estuviera utilizando un terminal de texto conectado directamente al equipo. Forma parte del conjunto de protocolos TCP/IP.

Tiempo Real: Método para procesar la información en cuanto se recibe.

U

Unicast: En redes conmutadas ethernet, transferencia de archivos/paquetes entre dos entidades. Una difusión única puede iniciarla un servidor a una estación de trabajo, una estación a un servidor, una estación a una impresora o cualquier otra entidad única hacia otra entidad

UPS: (Uninterruptible Power Supply ó Suministro de Energía Ininterrumpida). Es un estabilizador electrónico que está preparado para suplir al computador cuando se presenten caídas de energía o cambios de voltaje.

URL: (Universal Resource Locator ó Localizador de Recursos Universal). Identifica de manera única la ubicación de un equipo, directorio o archivo en Internet. La dirección URL también indica el protocolo de Internet apropiado, como HTTP o FTP. Por ejemplo: <http://www.microsoft.com>.

USB: Tecnología que facilita la conexión de periféricos a la computadora. Esta reconoce automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo, ya que se conecta a la parte trasera de la PC a un enchufe especial (puerto USB). La tarjeta madre debe tener esta tecnología en su CHIPSET para poder conectar dispositivos de este tipo.

UTP: Cable de para trenzado no apantallado, lo que significa que no tiene envoltura alrededor del grupo de conductores. Estos cables se usan principalmente en redes de voz y datos

Usuario: Cualquier individuo que interactúa con el computador a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con el computador a nivel profesional.

V

Vector: Segmento de datos de un mensaje SNA. Un vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

Virtuatización: Proceso que se usa para implementar una red basada en segmentos de red virtuales. Los dispositivos se conectan a segmentos virtuales independientemente de su ubicación física y de su conexión física con la red.

VLAN: LAN virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.

VLSM: Máscara de subred de longitud variable. Capacidad de especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

VTP: Protocolo de terminal virtual. Aplicación ISO para establecer una conexión de terminal virtual a través de una red.

Virus: Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan, se propagan a través de cualquier medio de almacenamiento, o a través de la LAN, o de la misma Internet.



W

WAN: Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

WorkGroup Director: Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroup Director se ejecuta en estaciones de trabajo UNIX, ya sea como una aplicación independiente o integrada con otra plataforma de administración de red basada en SNMP, brindando un sistema de gestión poderoso y transparente para los productos de grupo de trabajo de Cisco.

WWW: World Wide Web. Gran red de servidores de Internet la cual suministra servicios de hipertexto y otros a terminales que ejecutan aplicaciones de clientes como, por ejemplo, un navegador de Web. Ver también navegador de Web.