ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

MANUAL DE USUARIO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ANALISTA DE SOPORTE DE MICROCOMPUTADORES

TEMA:

ARTES GRAFICAS SENEFELDER S.A.

AUTORES

MARIA MONSERRATE ROMERO SUAREZ
CHRISTIAN EDISON MENDEZ CISNEROS

DIRECTOR

ING. FABIAN BARBOZA

AÑO

2010

AGRADECIMIENTO

Agradezco a Dios por haberme ayudado a concluir mi carrera, a mis padres que sin su ayuda y guía no hubiera sido posible este logro, a mi esposa que supo darme su apoyo incondicional.

Christian Edison Méndez Cisneros

AGRADECIMIENTO

Gracias a Dios y a todas aquellas personas que en todo este largo camino recorrido han ayudado a culminar nuestra carrera, a quienes nos alentaron a seguir adelante, nos ayudaron a conocer la clave del éxito, gracias ya que sin ellos no estaríamos aquí. No hay palabras para expresar tanta gratitud, simplemente GRACIAS.

María Monserrate Romero Suárez

DEDICATORIA

Para toda mi familia que hizo posible que llegara a cumplir esta meta, quienes siempre me apoyaron y alentaron para llegar al final, a mis amigos y compañeros que nunca se dieron por vencidos logrando que yo tampoco lo hiciera, a mis maestros que en todo momento pusieron sus conocimientos y enseñanzas a disposición

Christian Edison Méndez Cisneros

DEDICATORIA

Para las 2 personas más importantes en mi vida: mi madre y mi hermano, por el apoyo incondicional y el gran esfuerzo económico que hicieron desde el inicio de mi carrera, por estar a mi lado en todo momento, amigos gracias por compartir conmigo sus conocimientos profesionales cuando era necesario.

María Monserrate Romero Suárez

DECLARACIÓN EXPRESA

La responsabilidad de los hechos, ideas y doctrinas expuestas en este tópico nos corresponde exclusivamente; y el patrimonio intelectual de la misma, al EDCOM de la Escuela Superior Politécnica del Litoral.

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

FIRMA DE LOS MIEMBROS DEL TRIBUNAL DE GRADO

_____

Ing. Fabián Barboza Gilces

_____

Delegado

FIRMA DE LOS AUTORES DEL TÓPICO DE GRADUACIÓN

María Monserrate Romero Suárez

Christian Edison Méndez Cisneros

INTRODUCCIÓN

El presente manual contiene todo el análisis actual, la solución presentada a los problemas, la implementación realizada, configuración de los routers, switches y ACL'S para la empresa Artes Gráficas Senefelder.

Para la elaboración de este manual se realizaron diversos estudios con la finalidad de presentarle a Artes Gráficas Senefelder una buena altenativa a la solución de sus problemas encontrados.

Con este manual el responsable del mantenimiento de la red estará en capacidad de conocer:

- La situación actual que vive la compañía.
- La solución a sus problemas encontrados.
- La implementación realizada.
- La configuración de sus equipos de comunicaciones.

El presente manual consta de cuarenta y tres capítulos.

Este manual se ha diseñado para ser un soporte para el mantenimiento a los equipos de comunicación de la compañía.

- Conocer el análisis de su situación actual.
- Analizar las alternativas para su solución.
- Implementación de sus problemas LAN y WAN.
- Conocer las normas de estandarización utilizadas.
- Conocer la configuración de los equipos de comunicaciones WAN.

INDICE GENERAL

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

CAPITULO 5

CAPITULO 6

CAPITULO 24

CAPITULO 25

CAPITULO 26

CAPITULO 27

CAPITULO 28

CAPITULO 37

CAPITULO 38

CAPITULO 39

CAPITULO 40

CAPITULO 41

CAPITULO 42

CAPITULO 43

TABLA DE GRAFICOS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 6

CAPITULO 7

CAPITULO 8

CAPITULO 22

CAPITULO 23

CAPITULO 25

CAPITULO 26

CAPITULO 27

CAPITULO 28

CAPITULO 29

CAPITULO 30

CAPITULO 42

CAPITULO 43

INDICE DE TABLAS

CAPITULO 2

CAPITULO 3

CAPITULO 4

CAPITULO 5

CAPITULO 10

CAPITULO 11

CAPITULO 12

CAPITULO 16

CAPITULO 17

CAPITULO 1
ESTADO DE SITUACIÓN ACTUAL

ARTES GRAFICAS SENEFELDER S.A.

1 ANTECEDENTES

Artes Gráficas Senefelder C.A. es una empresa ecuatoriana que proporciona a sus clientes una amplia gama de impresos y servicios.

Desde 1921, ha mantenido altos estándares de calidad en las principales categorías de productos. Lidera en la mayoría de los segmentos incluyendo revistas, insertos, libros, catálogos, impresiones especiales, envases pagables, para cajas de camarón, laminado en cartón, valores y formas continuas.

Cuenta con más de 300 colaboradores, manteniendo su compromiso con el recurso humano y tecnológico, para satisfacer las expectativas de los mercados en que compite.

Más que imprimir, Senefelder se orienta a dar soluciones gráficas, estar al día en los cambios tecnológicos y las necesidades del mercado.

Las inversiones de Senefelder en ese rubro han permitido aumentar la productividad, eficiencia y calidad. Conjuntamente con el nivel profesional han constituido una magnífica sinergia para obtener los más altos estándares.

1.1 MISIÓN

Servir a nuestros clientes con soluciones gráficas integrales que les genere valor y resalten la imagen.

1.2 VISIÓN

Liderar el mercado gráfico nacional y fortalecer nuestra presencia en el mercado internacional, brindando productos y servicios de calidad, a través del desarrollo de nuestro recurso humano y la inversión en tecnología de vanguardia.

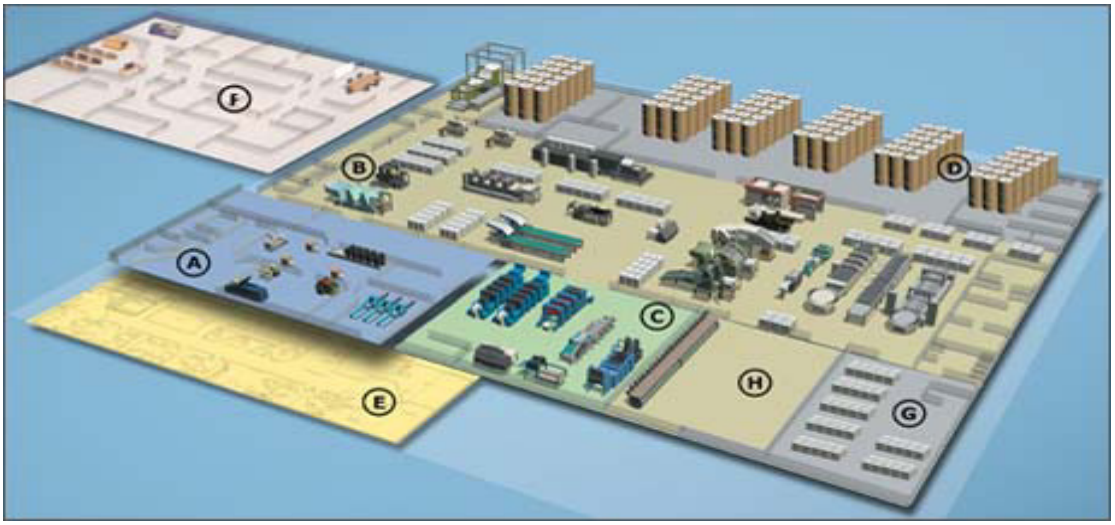


Gráfico 1-1: Instalaciones Senefelder

Leyenda:

A. Área de Valores
B. Litografía
C. Formas continuas
D. Bodegas
E. Administración
F. Arte y preprensa
G. Bodegas y despacho

2 INFRAESTRUCTURA LAN

2.1 Cableado Horizontal

El cableado Horizontal es el cableado que se extiende desde el armario de telecomunicaciones o Rack hasta la estación de trabajo, consta de 146 puntos de Datos CAT6 y 102 puntos de Voz CAT5e. La norma que se ocupa del cableado horizontal es la norma ANSI/TIA/EIA-568-B_ Commercial Building Telecommunications Cabling Standard, poseen un tendido horizontal con cable UTP Cat. 5e (568 B-1) par trenzado, dos pares, sin blindaje de 150 ohmios con conectores RJ45, el más utilizado para las tarjetas Ethernet, que actualmente poseen las estaciones de trabajo de la compañía, con una velocidad de 10/100 mbps, la estructura del cableado permite un radio de curvatura de 1 pulgada.

Cuenta con dos servicios por cada puesto de trabajo, uno de voz y otro de datos, en otros casos solo 1 servicio de dato, y otros dos de dato y uno de voz, actualmente el cableado de telecomunicaciones cruza por encima del cable de energía (techo falso), la distancia es de 15 cm.

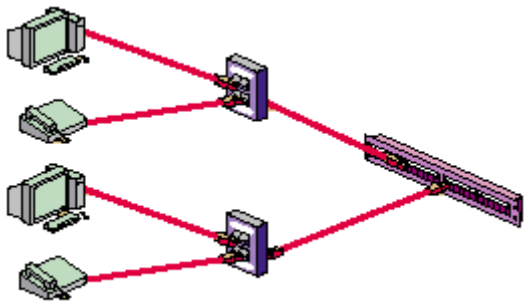


Gráfico 2-1: Dos Conectores por toma

1. Sistema de Cableado marca Siemon para la instalación de 146(Dato) y 102(Voz) puntos de cableado CAT6 y CAT5e respectivamente
2. La Red Lan tiene una velocidad de 1 Mbps.
3. Enlaces de fibra óptica desde el Rack de Telecomunicaciones del Centro de Computo hacia el Rack(HC1) de oficinas Nomina y Rack(HC2) de planta.

4. Enlace de cable multipar desde el MDF Telefónico hacia el Rack(HCl) de oficinas

Nomina y Rack(HC2) de planta

2.2 Infraestructura de Canalización

Dispone de un sistema de backbone de voz y datos, en el primero se utilizo fibra óptica multimodo de 4 hilos de marca COMSCOPE modelo O-004-DA-6F-M04NF con origen en el centro de computo, en el segundo se utilizo cable multipar de 25p de marca SMART LINK modelo SS-201-50C-GY con origen en el MDF ubicado en el centro de computo.

La infraestructura de canalización instalada fue dimensionada considerando la norma ANSÍ EIA/TIA 569, utilizando para ello electro canales y tubería metálica tipo EMT con sus respectivos accesorios de montaje.

2.3 Sistema de Cableado Estructurado de Voz y Datos

El cable UTP no consta de ningún empalme desde el origen (Master Closset) hacia cada uno de los puestos de trabajo. Se utiliza cable UTP, de 8 hilos, soporte de CAT6 de marca SIEMON para DATOS y cable UTP, de 8 hilos, soporte de CAT5e de marca SIEMON para VOZ, para el ruteo del cable en tumbado, tiene un electrocanal galvanizado con tapa de 20cm x lOcm con tapa del cual se derivan tuberías metálicas tipo EMT, la cual termina en una caja de paso que se une a las fundas flexibles metálicas o tubería EMT como bajantes para llegar a los puntos finales.

2.4 Subsistema Área de Trabajo

Posee rastreras metálicas perforadas en las que se encuentran las tomas de cableado conocidas como wall plates, con 1 ó 2 acopladores RJ45 CAT6 y CATSe.

Tienen identificadas las posiciones en los wall plates con nombre y con etiquetas plásticas para diferenciar los servicios (Voz y Datos).

Disponen de Patch Cords RJ45-RJ45 de cable flexible con bota protectora, ensamblados en fábrica, para VOZ y DATO tanto para el usuario como para el Master Closet en Cat6 y Cat5e, de marca SIEMON.

2.5 Subsistema de Administración

Posee 3 racks, 1 de piso cerrado y 2 de pared cerrados para datos y telefónico, de marca QUEST configurado con los siguientes componentes:

2.5.1 Rack de Datos

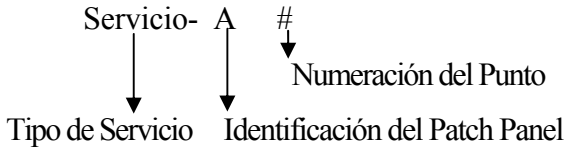
- 6 patch panels para las terminaciones del cableado horizontal de datos, marca SIEMON.
- 1 patch panels para las terminaciones del cableado horizontal de datos (SERVIDORES) marca SIEMON.
- 1 bandeja para terminaciones de fibra óptica de marca SIEMON.
- 8 organizadores horizontales en canaleta 80 x 60 de marca INSELET modelo K-1048.
- 2 organizadores verticales en canaleta 80 x 80 doble lado de marca INSELET OP-256.

2.5.2 Rack de Voz

- 4 patch panels para las terminaciones del cableado horizontal de voz, marca SIEMON.
- 2 patch panels para la terminación del cable multipar 25 pares (desde rack HC1 y HC2), marca SIEMON.
- 4 patch panels para las terminaciones de las extensiones telefónicas, marca NEW LINK.
- 8 organizadores horizontales en canaleta 80 x 60 de marca INSELET modelo K-1048.
- 2 organizadores verticales en canaleta 80 x 80 doble lado de marca INSELET.

2.5.3 Identificación

Todos los elementos de la red pasiva, cables, salidas, distribuidores principales y secundarios estarán identificados, la codificación utilizada es la siguiente:



- **Tipo de Servicio:** Se ha colocado la palabra Voz o Dato dependiendo del servicio que atiende.
- **Identificación del Patch Panel:** Cada patch panel tiene su identificación, así tenemos los patch panel A tanto para el servicio de datos como de Voz.
- **Numeración del Punto:** Se utiliza un número secuencial.

Todos los puntos UTP están probados y certificados, para su correcto funcionamiento, tanto en las oficinas como en la planta, así como los enlaces de FIBRA ÓPTICA.

2.6 Distribución del Cableado Vertical (Backbone)

La distribución del cableado vertical permite la interconexión de cada una de las redes de datos. La interconexión de las redes de datos se hace directamente con el cuarto de cableado principal utilizando cable UTP Cat. 6, esto sucede tanto en la matriz como en las sucursales.

Actualmente sus swichs no son administrables son equipos capa dos y no poseen VLAN's

Este subsistema está constituido por los elementos de conexión asociados y el cable de cobre o fibra óptica que unirá el Cuarto de equipos de Telecomunicaciones principal con el rack de planta baja.

- El tendido de los cables es en topología estrella jerárquica.
- El backbone de datos está compuesto de cable de fibra óptica tipo multimodo tight buffer o loóse tube para las aplicaciones de datos.
- La fibra cumple con las siguientes especificaciones:

Atenuación Máxima:	db/Km. @ 850 nm	1 db/Km @ 1300 nm
Ancho de Banda Mínimo	160MHz-Km@850 nm	500 MHz-Km @ 1300 nm
Apertura numérica:	0.275	

Tabla 1: 3.6.1.1 Tabla de Carácteristicas de la Fibra Optica

- Las terminaciones de la fibra utilizan conectores tipo SC cerámicos de marca FCC
- Para la terminación de la fibra óptica se emplearon bandejas porta cable para fijación
- en rack de marca SIEMON
- El backbone de voz está compuesto por cable multipar telefónico de tipo interior/exterior para aplicaciones de voz, de marca SMART LINK modelo SS-201-50C-GY
- Las terminaciones del cable multipar están conectadas mediante paneles de marca NEWLINK

2.7 ANÁLISIS DE PISO APLICATIVO

2.7.1 EDIFICIO MATRIZ - LITOGRAFIA

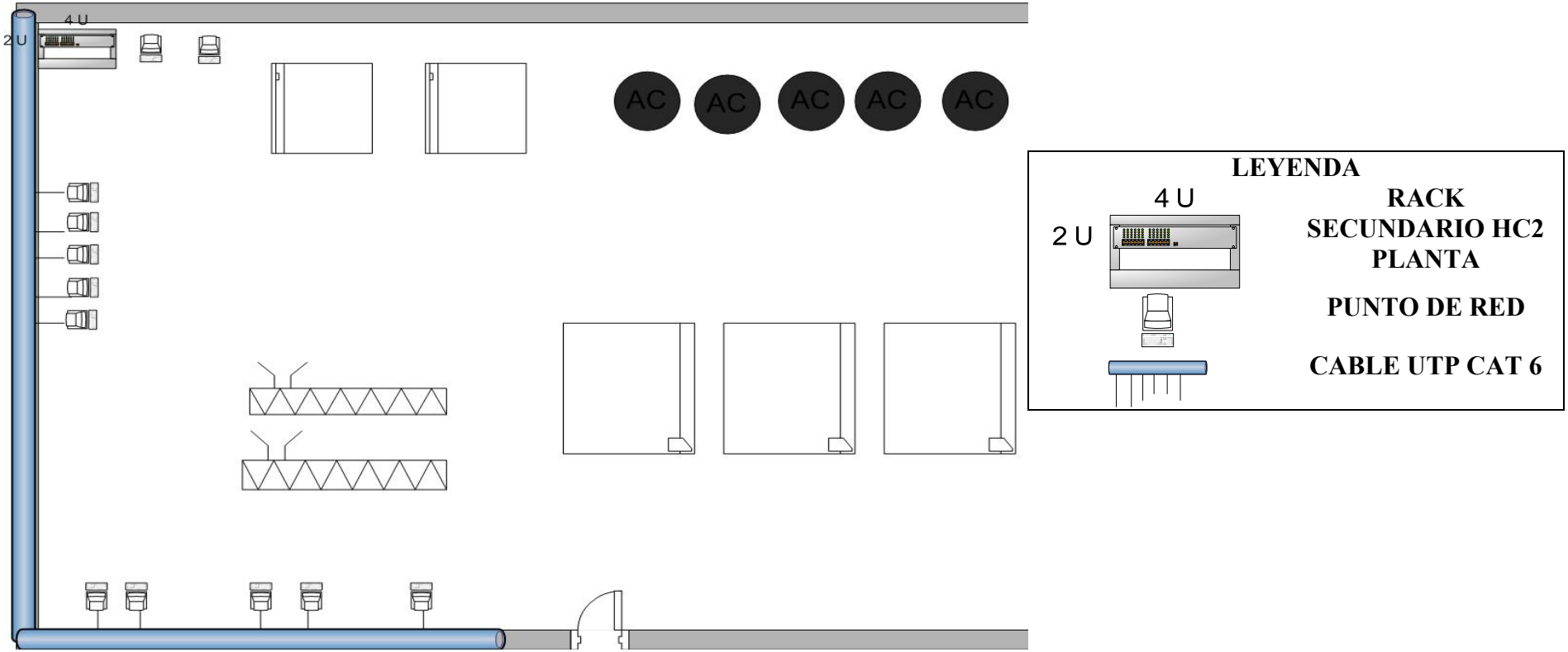
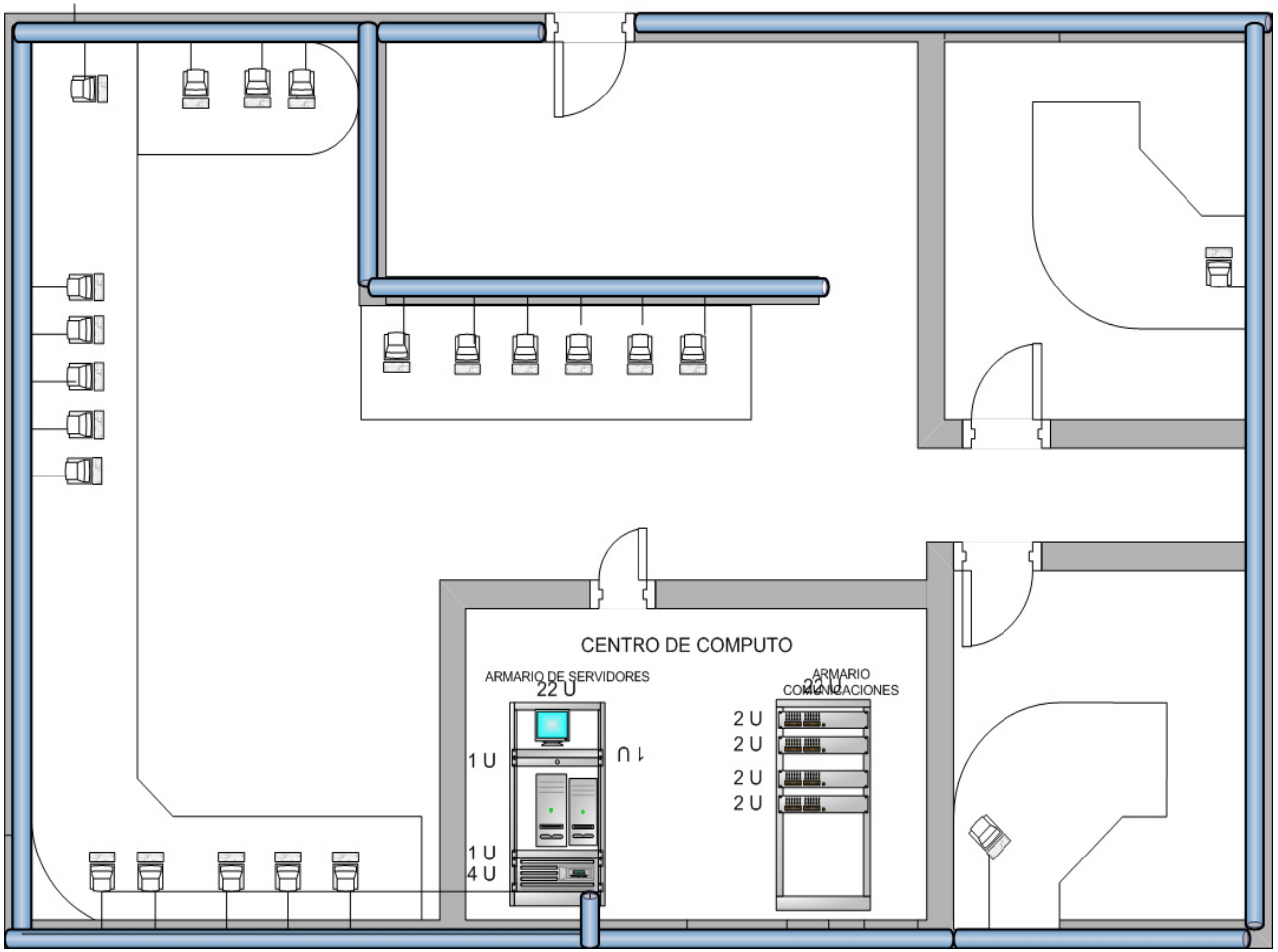


Gráfico 2-2: Planta Baja – Litografía

2.7.2 EDIFICIO MATRIZ – FORMAS CONTINUAS



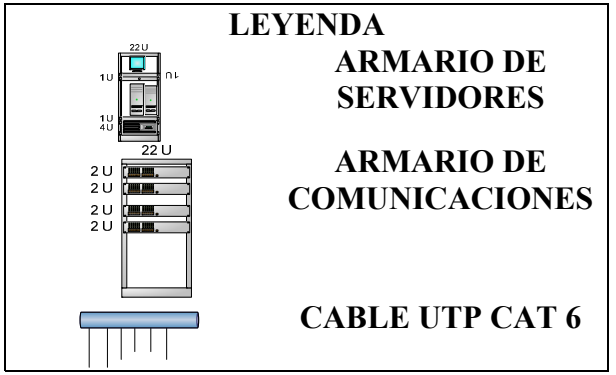
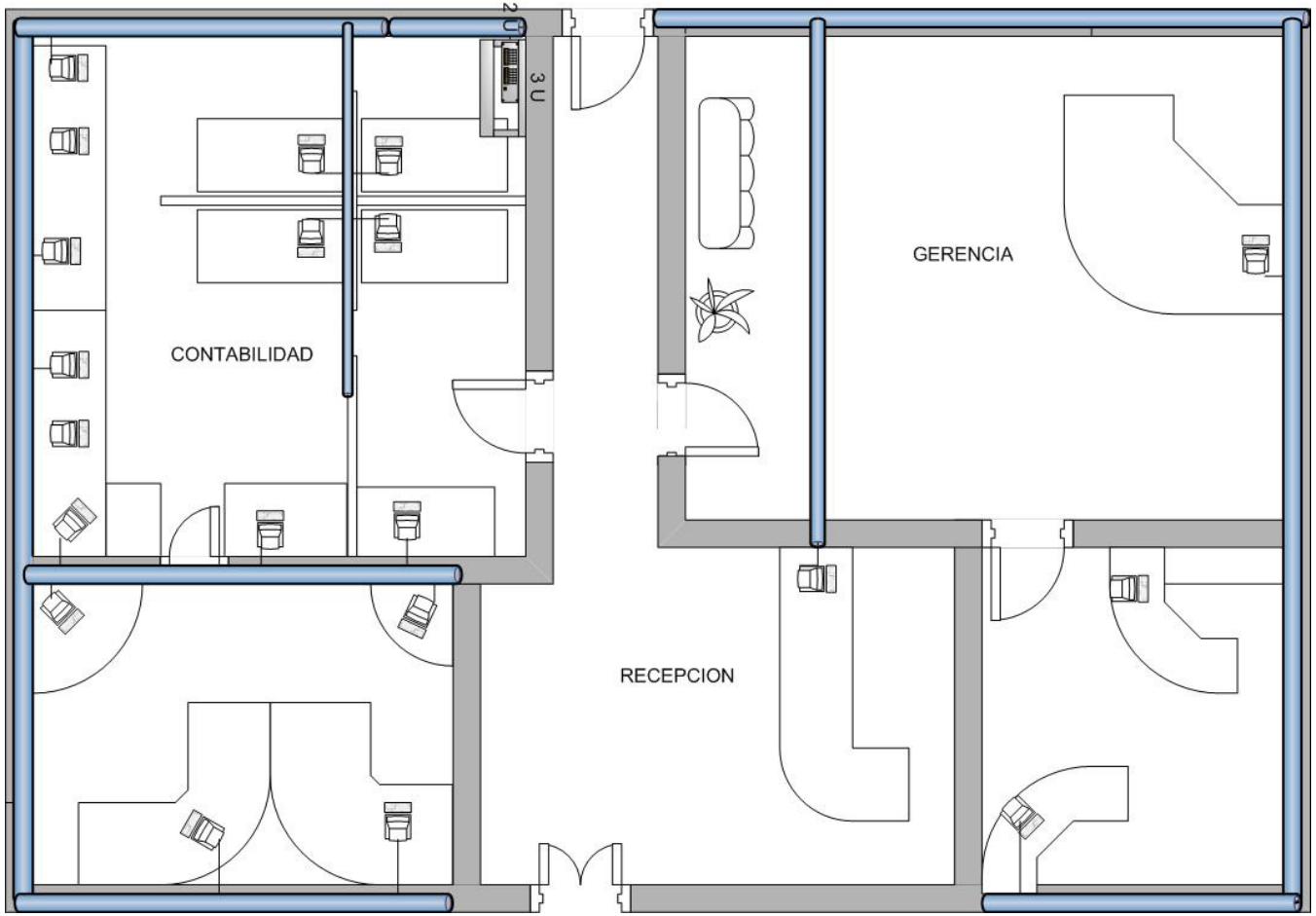


Grafico 2-3: Primer Piso - Formas Continuas

2.7.3 EDIFICIO MATRIZ - ADMINISTRACION



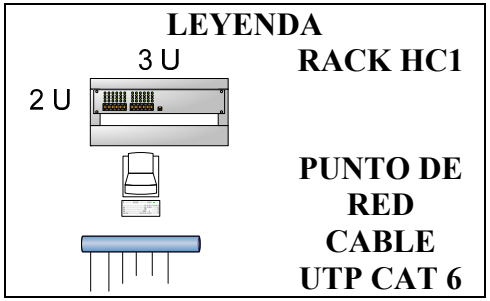


Gráfico 2-4: Planta Baja-Administración

2.7.4 EDIFICIO MATRIZ – ARTE Y PREPRENSA

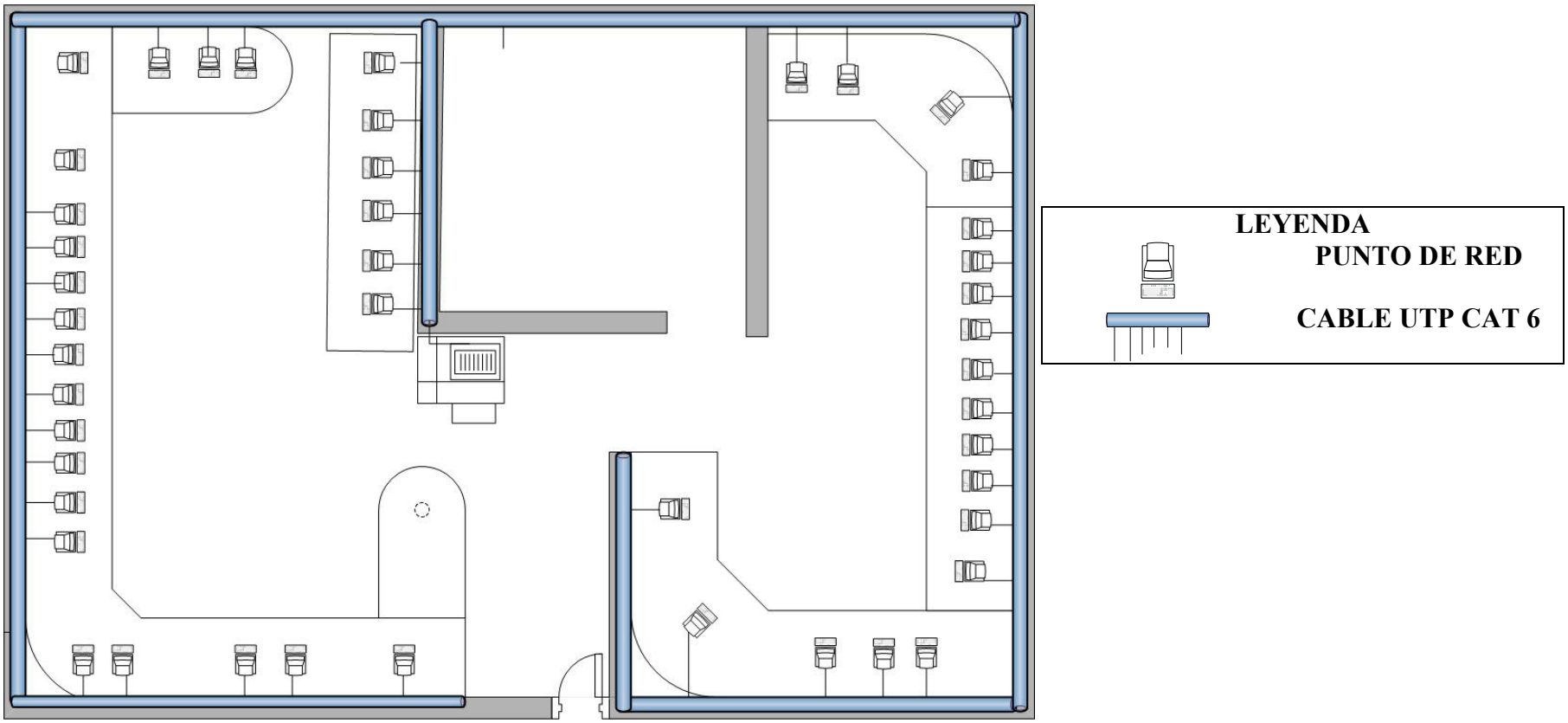


Gráfico 2-5: Primer Piso - Arte y Preprensa

3 ARMARIO Y RACKS DE COMUNICACIONES

3.1 EDIFICIO MATRIZ

3.1.1 PRIMER PISO EDIFICIO MATRIZ

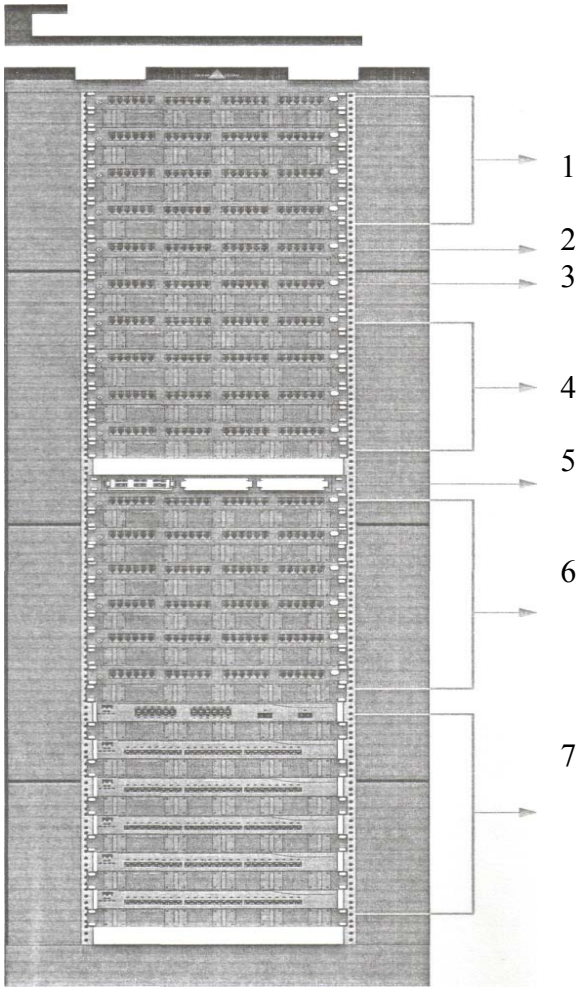


Gráfico 3-1: Armario Comunicaciones Planta Baja Edificio Matriz

Leyenda	
1	**Paneles Extensiones telefónicas**
2	**Distribución Vertical Voz HC1**
3	**Distribución Vertical Voz HC2**
4	**Distribución Horizontal Voz MC**
5	**Distribución Vertical DATO Fibra Optica HC1/HC/2**
6	**Distribución Horizontal Dato MC**
7	**Distribución Switchs de Datos MC**

3.1.2 PLANTA BAJA – ADMINISTRACIÓN

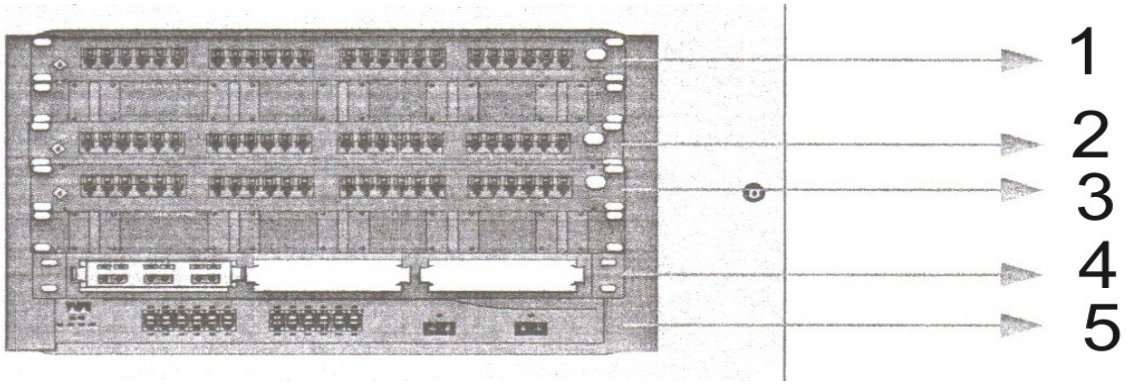


Gráfico 3-2: Planta Baja – Administración

Leyenda	
1	Distribución Horizontal DATO HC1
2	Distribución Vertical Voz HC1
3	Distribución Horizontal Voz desde MC
4	Distribución Vertical DATO Fibra Optica desde MC
5	Distribución Switchs de Datos HC1

3.1.3 PLANTA BAJA - PLANTA

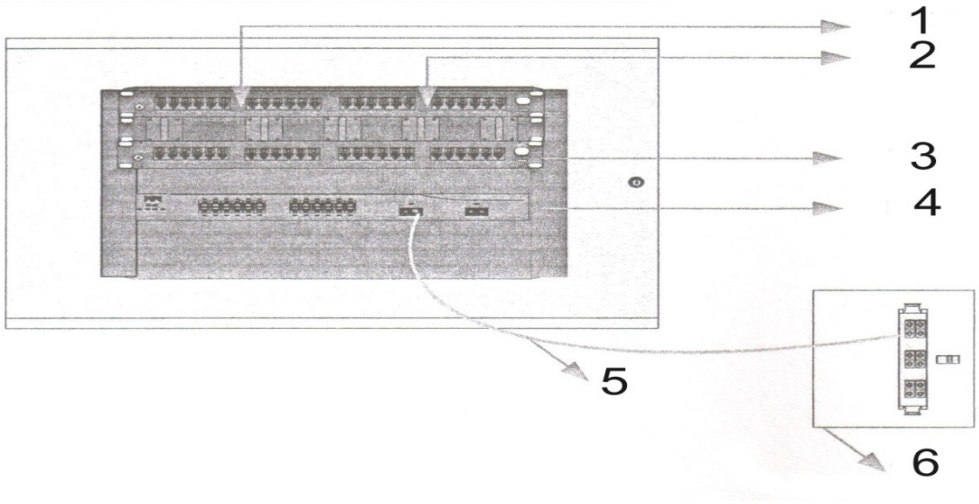


Gráfico 3-3: Planta Baja - Planta

Leyenda	
1	Distribución Horizontal DATO HC1
2	Distribución Vertical Voz HC1
3	Distribución Vertical Voz desde MC
4	Distribución Switchs de Datos HC2
5	Pach Fibra Optica
6	Distribución vertical DATO Fibra Optica desde MC

3.2 DETALLE DE LOS EQUIPOS DE COMUTACIÓN

3.2.1 – SWITCH

EQUIPO	UBICACION	CANTIDAD
Link Sys Cisco SRW2024 24-Port 10/100/1000 Gigabit-Administrable	MATRIZ RACK PRINCIPAL MC-SISTEMAS.	3
LinkSys Cisco SRW2016 16 puertos de 10/100/1000 Mbps	MATRIZ RACK PRINCIPAL MC-SISTEMAS.	1
LinkSys Cisco SR2024 24 Puertos 10/100/1000 Gigabit	MATRIZ RACK PRINCIPAL MC-SISTEMAS.	1
CISCO Catalyst 3750 series 24 puertos - EN, Fast EN, Gigabit EN - 10Base-T, 100Base-TX, 1000Base-T + 4 x SFP (vacías) - 1.5 U - montable en bastidor - apilable	MATRIZ RACK PRINCIPAL MC-SISTEMAS.	1

Tabla 2: 4.2.1.1 Tabla de las Características de los Switchs

3.2.2 HUB

EQUIPO	UBICACION	CANTIDAD
3Com Superstaps dual Speed Hub 500 24 PUERTOS	**MATRIZ** RACK PRINCIPAL MC-SISTEMAS.	1

Tabla 3 :4.2.2.1 Tabla de las Caracteristicas de los Hubs

3.3 ESTACIONES DE TRABAJO

EQUIPO	UBICACION	CANTIDAD
Computadora HP Pentium IV de 3.0 Ghz, Memoria Ram 512 Mb, Disco Duro de 160 Gb Ethernet 100/1000 integrada / DVD Writer / Monitor LCD 17" Sistema Operativo: Windows XP	**VALORES**	40
	LITOGRAFIA	10
	FORMAS CONTINUAS	10
	ADMINISTRACION	30
COMPUTADOR HP ND052LA DX2400 PROCESADOR CORE 2 DUO E2200, MEMORIA RAM 1GB, DISCO DURO 160GB, DVDWRITER, TARJETA DE RED 100/1000 MBPS	**ARTE Y PRE-PRENSA**	20
Power Macintosh G4 (Digital Audio), Procesador PowerPC 7450, 1GB en RAM, Disco Duro de 80GB, DVDWRITER, Unidad ZIP incluida, Ethernet, Modem, 2 puertos USB, 2 puertos Firewire. Sistema Operativo Mac OS 10.3 (Panther)	**ARTE Y PRE-PRENSA**	30

Tabla 4 4.3.1.1 Tabla de las Características de las Estaciones de Trabajo

3.4 SERVIDORES

3.4.1 MATRIZ

CANTIDAD	EQUIPO	UBICACION
1	HP Proliant ML 350 G6 PROCESADOR Quad-Core Intel® Xeon® E5420 (2.26 Ghz) MEMORIA CACHE Memoria cache de 8MB Level 3 MEMORIA RAM 6 GB (3 x 2 GB) de memoria estándar INCORPORA HP Media Altura SATA DVD-ROM Optical Drive 2,4 TB SAS SFF; SFF SATA de 2,0 TB CONECTIVIDAD Total de seis ranuras de expansión, un PCI-Express x16 Gen2 (velocidad x8); Una x8 PCI-Express Gen2 (velocidad x8); Cuatro x8 PCI-Express Gen2 (x4 la velocidad); Opcional PCI-X Expander proporciona otros dos de 64 bits / 100-MHz PCI-X ranuras con una única ranura PCI Express	ARMARIO PRINCIPAL – SISTEMAS (PRIMER PISO)
1	Proliant ML 110G5 HP PROCESADOR Dual-Core Intel® Xeon® E3130 (3.00 GHz) MEMORIA CACHE 6MB MEMORIA RAM 1,00 GB (1 x 1,00 GB) INCORPORA 2 Discos duros HP 160GB 3G SATA 7.2K NHP 3.5" DVD- ROM 16X HP Original Teclado/Mouse CONECTIVIDAD Tarjeta de Red Gigabit NC105i PCI Express Gigabit Ethernet Server Adapter SOPORTE Controladora SATA, RAID 0, 1 support	ARMARIO PRINCIPAL – SISTEMAS (PRIMER PISO)

Tabla 5 4.4.1.1 Tabla de las Carácterísticas de los Servidores

4 INFRAESTRUCTURA WAN

El enlace con las diferentes sucursales es por medio de antenas de Radio las mismas que las provee la empresa Onnet, los cuales se conectan a los dispositivos de comunicación (Rotures). El protocolo de comunicación que utiliza para conectarse con las sucursales Quito y Cuenca es Frame Relay, técnica de comunicación mediante retranmisión de tramas con una frecuencia de 5.8 Ghz

Además posee un sistema de protección Firewall que funciona como cortafuegos, permitiendo o denegando las transmisiones de una red a la otra, no existe un enlace de respaldo entre las sucursales.

4.1 DETALLE DE LOS EQUIPOS DE ENRUTAMIENTO

4.1.1 ROUTER

CANTIDAD	EQUIPO	UBICACIÓN
1	Router CISCO 2600 Form Factor 19" Rack Mount (Up to 2RU) DRAM (default) 256 MB DRAM(maximum) 256 MB Flash (default) up 32 MB Flash (Maximum) up to 128 MB Support for High Speed WICs (HWICs) No LAN PORTS UP TO 2 10/100 Integrated Inline Power/ PoE Support No USB Ports No Console Port (Up to 115.2 Kbps) 1 Auxiliary Port (Up to 115.2 Kbps) 1	**MATRIZ** RACK PRINCIPAL MC-SISTEMAS.
1	COMPUTADOR PC GENERICO P4 3.0 GHZ, MEMORIA RAM 1 GB, DISCO DURO 160 GB, TARJETA DE RED 100/1000 MBPS SISTEMA OPERATIVO CENTOS	**MATRIZ** RACK PRINCIPAL MC-SISTEMAS.

Tabla 6 5.1.1.1 Tabla de las Características de los Routers

5 SEGURIDAD

CANTIDAD	EQUIPO	UBICACIÓN
1	Firewall Global Technologies Asociates Inc. GB-800	**MATRIZ** RACK PRINCIPAL MC-SISTEMAS.

Tabla 7 6.1.1.1 Tabla de Firewall

6 COMUNICACIÓN WAN

6.1 ENLACE DE DATOS

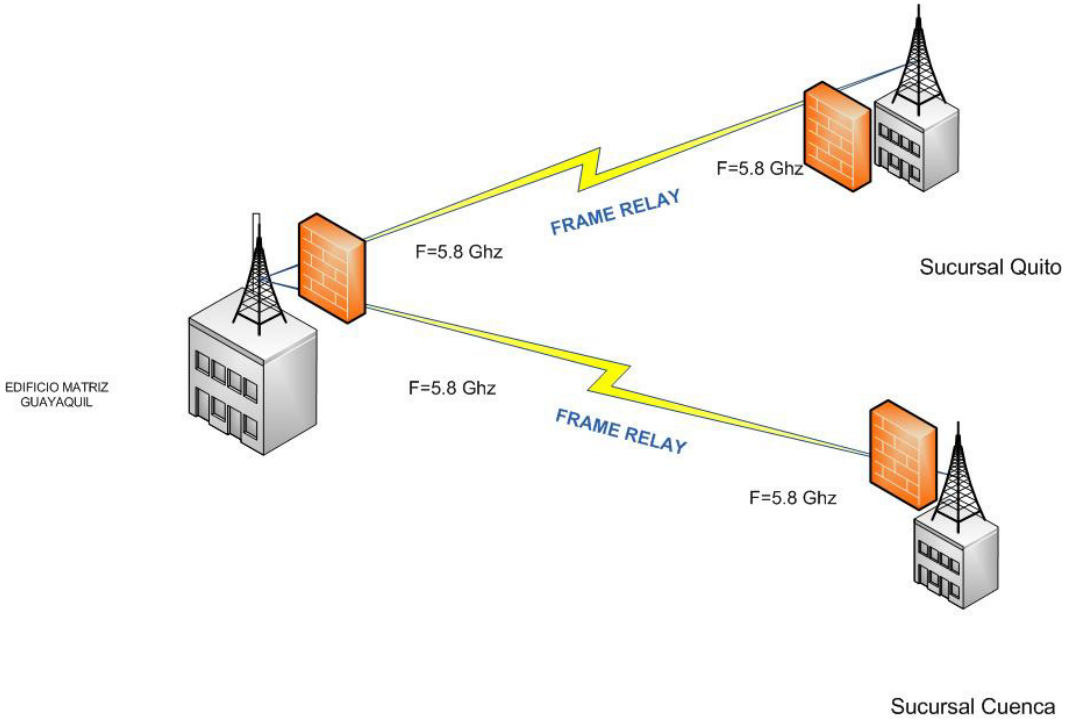


Gráfico 6-1: Enlace de Datos

Leyenda	
ANTENA MICROONDA	
ENLACE SERIAL	
FIREWALL	

7 RECEPCIÓN DE INTERNET DE LA MATRIZ

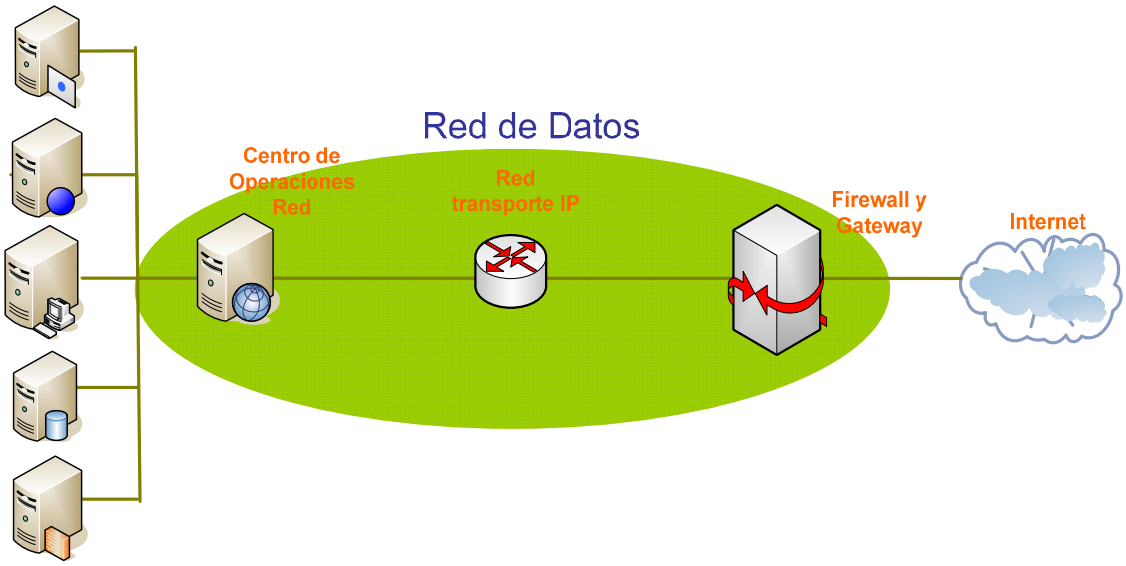


Gráfico 7-1: Recepción de internet

Leyenda	
SERVIDORES	
ROUTER	
FIREWALL	
INTERNET	

8 ENLACE WAN DE MEDIOS

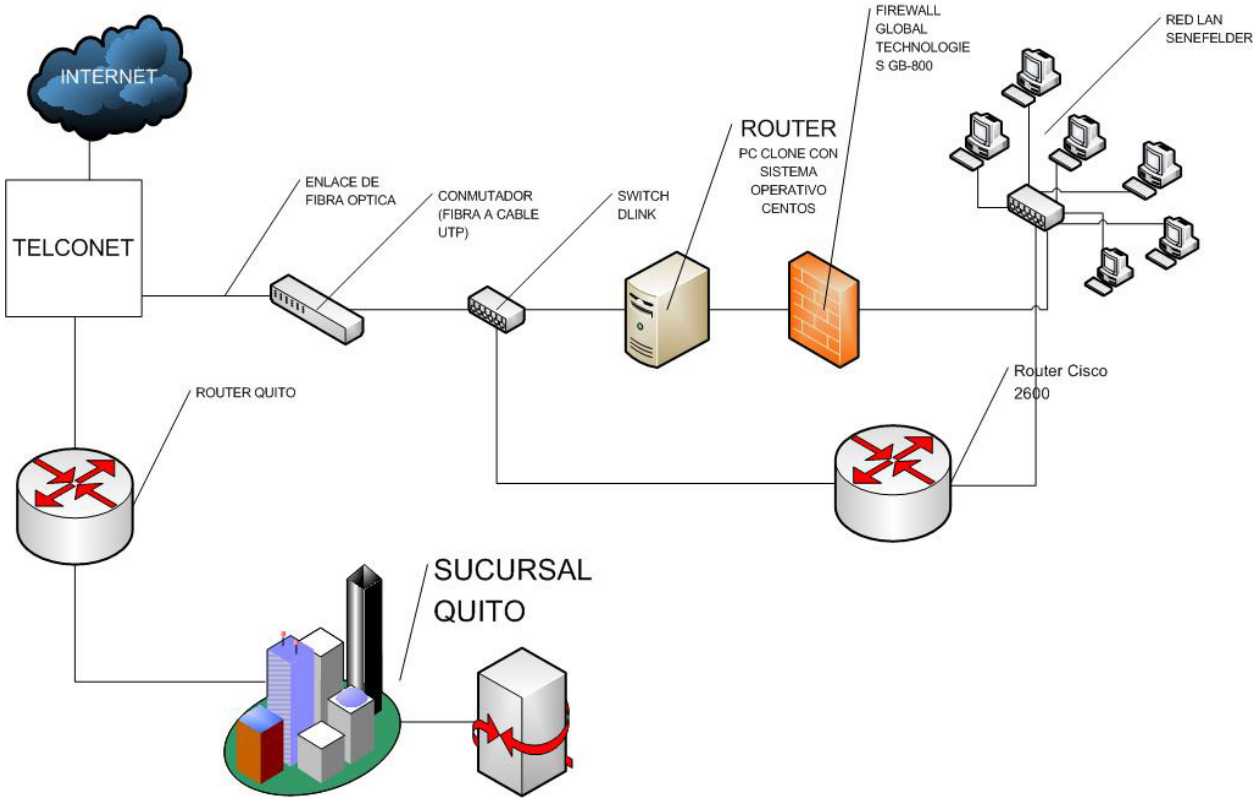


Gráfico 8-1: Enlace de Medios

Leyenda	
ROUTER: PC CLONE CON SISTEMA OPERATIVO CENTOS	
ROUTER: CISCO 2600	
FIREWALL GLOBAL TECHNOLOGIES GB-800	
INTERNET PROVEEDOR ONNET	

9 PROBLEMAS ENCONTRADOS EN LA MATRIZ

Dentro del análisis realizado a la empresa hemos encontrado los siguientes problemas:

1. Falta de capacitación al personal encargado de le red LAN.

2. La red de conexión LAN no está segmentada en VLANS.

3. No existe un enlace de respaldo para la conexión WAN.

4. Colisiones en la red debido al uso de un hub.

5. Constantemente se pierde la conexión de la red Wan debido al mal funcionamiento del Equipo de Computo que realiza las funciones de router.

CAPITULO 2

SOLUCIÓN PROPUESTA

10 SOLUCION PROPUESTA

10.1 PROBLEMAS ENCONTRADOS

10.1.1 PROBLEMAS ORGANIZACIÓNALES

PROBLEMA	CAUSA	EFECTO	SUCURSAL
Falta de capacitación al personal encargado de le red LAN	No existe presupuesto en la empresa	Se demora en solucionar un problema de red.	MATRIZ QUITO CUENCA

Tabla 8 11.1.1.1 Tabla de Problemas Organizacionales

10.1.2 PROBLEMAS TECNICOS

PROBLEMA	CAUSA	EFECTO	SUCURSAL
La red de conexión LAN no está segmentada en VLANS	No hay un swich dónde se puedan crear VLAN para departamentos	Congestionamiento en la red.	MATRIZ QUITO CUENCA
No existe un enlace de respaldo para la conexión WAN	Falta de conocimiento por parte del personal encargado de la red.	Falla en el enlace principal de conexión WAN	MATRIZ QUITO CUENCA

Tabla 9 11.1.2.1 Tabla de Problemas Técnicos

10.1.3 PROBLEMAS TECNICOS

PROBLEMA	CAUSA	EFECTO	SUCURSAL
Colisiones en la red	En la red LAN existe un Hub	Perdidas en la transmisión de paquetes, lentitud la red.	MATRIZ QUITO CUENCA
Constantemente se pierde la conexión de la red Wan	Se ha asignado un dispositivo que realiza la terea de un Router	Problema de comunicación Wan.	MATRIZ

Tabla 10 11.1.3.1 Tabla de Problemas Técnicos

10.2 SOLUCIÓN PROPUESTA

PROBLEMA	SOLUCIÓN	ALCANCE	SUCURSAL
1. No existe VLANs creadas en los departamentos de las sucursales	Adquisición de equipos de conmutación (swich) con soporte a VLAN.	Disminuyen los dominios de broadcast, mejora el rendimiento general de la red.	MATRIZ QUITO CUENCA
2. No hay enlace de respaldo Wan	Contratar otro proveedor de enlace de datos	En caso de que se pierda la comunicación en un proveedor el otro proveedor está vigente para continuar el enlace de datos	MATRIZ QUITO CUENCA
3. Colisiones en la red.	Adquisición de swich para reemplazar los hub	Mejora la transmisión de datos en la red interna, y control de colisiones	MATRIZ QUITO CUENCA
4. Router basado en un computador clone con sistema operativo centos	Adquirir un Router	Mejora en la comunicación hacia la red Wan, al emplear un equipo diseñado para ruteo.	MATRIZ

Tabla 11 11.2.1.1 Tabla de Solución Propuesta

11 ESTUDIO DE LA FACTIBILIDAD ALTERNATIVA 1

11.1 OBJETIVOS

Dentro de los objetivos principales apreciaremos una mejor administración de la red, infraestructura de punta en la comunicación LAN y WAN, se crearan VLANs que reducirán los dominios de broadcast y trafico y obtendremos mejor tiempo de respuesta en la red interna.

Dentro de esta alternativa hemos enfocado el problema del enlace de respaldo solicitando al proveedor de última milla una total garantía en sus equipos. El proveedor para el enlace de respaldo en esta alternativa es la empresa Pacifictel.

11.2 FACTIBILIDAD TECNICA

DESCRIPCIÓN DEL EQUIPO	CARACTERÍSTICAS	CANTIDAD	UBICACIÓN
	Cisco 2821 Integrated Service Router ISR	1	Matriz
	Switch Cisco Catalyst 2950G-24	3	Matriz Sucursales

Tabla 12 12.2.1.1 Tabla de Factibilidad Técnica

11.3 FACTIBILIDAD ECONOMICA

11.3.1 COSTO DE HARDWARE

CANTIDAD	*DESCRIPCION*	*P. UNITARIO*	*TOTAL*
1	Cisco 2821 Integrated Service Router ISR **Memoria Ram**: 256 Mb/1 Gb (Max.) **Protocolos Soportados:** OSPF, RIP-1, RIP-2, IS-IS **Interfaces:** 2 por Red-Ethernet 10-T/100Tx/1000T- RJ-45 - 2 x USB. Protección firewall, asistencia Técnica VPN. **Soporte:** 802.1q-802.1p – IPV4-IPV6	5400	5400
3	Switch Cisco Catalyst 2950G-24 **Memoria Ram:** 16 Mb Sdram. 24 puertos – 10/T100Tx Dúplex pleno, concentración de enlaces, apilable. **Normas:** IEEE 802.3, IEEE 802.1q, IEEE 802.1p.	550	1650
		TOTAL	**7050**

Tabla 13 12.3.1.1 Tabla de Costo de Hardware

11.3.2 COSTO DE ENLACE DE RESPALDO

(INCLUYE ALQUILER DE EQUIPOS ULTIMA MILLA)

DESCRIPCION	*C. Mensual*	*TOTAL ANUAL*
Enlace Fibra Óptica GYE- QUITO 256 Kbps (Pacifictel)	250	3.000
Instalación		250
Enlace Fibra Óptica GYE- CUENCA 256Kbps (Pacifictel)	250	3.000
Instalación		250
(*) Incluído Impuestos	TOTAL	***$ 6.500**

Tabla 14 12.3.2.1 Tabla de Costo Enlace de Respaldo

12 COSTOS OPERATIVOS

12.1 FASE DE ANALISIS

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*10*	*$266.66*

Tabla 15 13.1.1.1 Tabla de Fase de Análisis

12.2 FASE DE DISEÑO

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*4*	*$106.66*

Tabla 16 13.2.1.1 Tabla de Fase de Diseño

12.3 FASE DE IMPLEMENTACIÓN

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2*	*$53.33*
2	*Técnicos de redes*	*2*	*$23.33*

Tabla 17 13.3.1.1 Tabla de Fase de Implementación

12.4 FASE DE PRUEBA

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2*	*$53.33*
2	*Técnico de redes*	*2*	*$23.33*

Tabla 18 13.4.1.1 Tabla de Fase de Prueba

12.5 FASE DE DOCUMENTACIÓN

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*10*	*$266.66*
Total Costos Operativos			*$793.30*

Tabla 19 13.5.1.1 Tabla de Fase de Documentación

TOTAL COSTO DE EQUIPOS	*$7.050*
TOTAL ENLACE DE RESPALDO	*$6.500*
SERVICIOS PROFESIONALES	*$793.30*
SUBTOTAL FACTIBILIDAD ECONÓMICA	***$14,343.30***
IVA 12%	***1,721.20***
TOTAL	***$ 16,064.50***

13 VENTAJAS Y BENEFICIOS

13.1 VENTAJAS

- Aprovechar la adquisición de equipos de conmutación y enrutamiento de nueva tecnología, para mejorar el rendimiento de la red, evitar colisiones y perdidas de datos.
- Mejorar el servicio de respaldo a nivel Wan.
- Localización e identificación de fallos en la red.

13.2 BENEFICIOS

- Eficacia Organizacional
- Ponemos la información vital al alcance de todos los empleados con acceso a ella.
- Mejora organizacional con efectos directos en la satisfacción de los usuarios y clientes.
- Se optimizaran los recursos administrativos.

14 CONDICIONES DE LA OFERTA

Forma de pago: 60% a la firma del contrato – 40% contra entrega del trabajo realizado

Validez de la oferta: 15 días

15 GARANTÍAS

Los equipos de comunicaciones WAN, gozarán de una garantía de tres años.

La garantía de la implementación iniciará a partir de la firma del acta de recepción correspondiente por el lapso de 1 año. El proveedor asumirá el compromiso dar soporte sin costo alguno durante el período de la garantía al cliente.

16 ESTUDIO DE LAS FACTIBILIDAD

16.1 ALTERNATIVA 2

16.1.1 Objetivos

Dentro de los objetivos se diseña un sistema rápido y fiable que vaya de acuerdo a las demandas de crecimiento de las nuevas tecnologías de comunicación, la administración y gestión de una red sencilla y la centralización de su administración son claves en el desarrollo empresarial al mismo tiempo que debemos proyectarnos a un largo plazo.

En esta alternativa enfatizamos el contrato del servicio de ultima milla al proveedor Interactive para el enlace de respaldo.

16.2 FACTIBILIDAD TECNICA

Descripción del equipo	Características	Cantidad	Ubicación
3Com® Router 5682 	**Puertos:** Uno de consola, uno serie AUX; ocho ranuras para MIM **Interfaces WAN:** RDSI, ADSL, E1, T1, T3, E3, serie de alta velocidad, X.25, Frame Relay, HDLC/SDLC **Interfaces de LAN:** Ethernet 10/100, 10/100/1000 **Routing de WAN:** IP, IPX, OSPF, BGP-4, IS-IS Integrado, RIP V1/V2, Routing Estático, VPN MPLS L2 y L3 **Seguridad:** VPN (L2TP, GRE, IPSec), Stateful Firewall, ACLs, NAT, RADIUS, certificados X.509	1	Matriz
Switch 3Com 2226 	Switch Administrable 3Com 2226 24 Port 10/100 mbps	3	Matriz y Sucursales

Tabla 20 17.2.1.1 Tabla de Factibilidad Técnica

16.3 FACTIBILIDAD ECONÓMICA

16.3.1 COSTO DE HARDWARE

A continuación detallamos la factibilidad Económica de nuestra propuesta.

CANTIDAD	*DESCRIPCION*	*P. UNITARIO*	*TOTAL*
1	3Com® Router 5682	$ 2.500	$ 2.500
3	Switch Administrable 3Com 2226 24 Port 10/100 mbps **Memoria Ram:** 16 Mb Sdram. 24 puertos – 10/100mbps Half y Full Duplex, soporte a Vlan, MDI/MDIX. **Normas:** IEEE 802.1q, IEEE 802.1p.	$ 290	$ 870
		TOTAL	**$ 3.370**

Tabla 21 17.3.1.1 Tabla de Costo de Hardware

16.3.2 COSTO DE ENLACE DE RESPALDO

(INCLUYE ALQUILER DE EQUIPOS ULTIMA MILLA)

DESCRIPCION	*C. Mensual*	*TOTAL ANUAL*
Enlace Fibra Óptica GYE- QUITO 256 Kbps (Interactive)	190	2.280
Instalación		300
Enlace Fibra Óptica GYE-CUENCA 256Kbps (Interactive)	190	2.280
Instalación		300
(*) Incluído Impuestos	TOTAL	***$ 5.160**

Tabla 22 17.3.2.1 Tabla de Costo de Enlace de Respaldo

17 COSTOS OPERATIVO

17.1 FASE DE ANALISIS

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*10*	*$266.66*

Tabla 23 18.1.1.1 Tabla de Fase de Análisis

17.2 FASE DE DISEÑO

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*4*	*$106.66*

Tabla 24 18.2.1.1 Tabla de Diseño

17.3 FASE DE IMPLEMENTACIÓN

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2*	*$53.33*
2	*Técnicos de redes*	*2*	*$23.33*

Tabla 25 18.3.1.1 Tabla de Fase de Implementación

17.4 FASE DE PRUEBA

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2*	*$53.33*
2	*Técnico de redes*	*2*	*$23.33*

Tabla 26 18.4.1.1 Tabla de Fase de Prueba

17.5 FASE DE DOCUMENTACIÓN

CANTIDAD	DETALLE	DIAS	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*10*	*$266.66*
Total Costos Operativos			*$793.30*

Tabla 27 18.5.1.1 Tabla de Fase de Documentación

TOTAL COSTO DE EQUIPOS	*$.3.370,00*
TOTAL ENLACE ANUAL	**$5.160.00**
TOTAL COSTOS OPERATIVOS	*$793.30*
SUBTOTAL	***9,323.30***
Iva	***1,118.80***
FACTIBILIDAD ECONÓMICA	***$ 10442.10***

18 VENTAJAS Y BENEFICIOS DE LA SOLUCIÓN PROPUESTA

18.1 VENTAJAS

- Incremento de la seguridad en la red.
- Enlaces efectivos.
- Disminución de broadcast en la red.
- Rapidez, fiabilidad y seguridad en las comunicaciones

18.2 BENEFICIOS

- Eficacia Organizacional
- Ponemos la información vital al alcance de todos los empleados con acceso a ella.
- Mejora organizacional con efectos directos en la satisfacción de los usuarios y clientes.
- Se optimizaran los recursos administrativos.

19 CONDICIONES DE LA OFERTA

Forma de pago: 50% al inicio de la etapa de diseño para la compra de los equipos y el 50% contra entrega del trabajo y la completa satisfacción del cliente.

Validez de la oferta: 30 días

20 GARANTÍAS

Los equipos de comunicaciones WAN, gozarán de una garantía de tres años en lo equipos de comunicación.

Se ofrece seis meses en garantía de equipos LAN y tres meses en las configuraciones, sin costo alguno para el cliente.

21 GRAFICO GANTT

Ver Anexos.

CAPITULO 3
MANUAL DE CONFIGURACIÓN DE ROUTERS Y SWITCHES

22 CONFIGURACION ROUTER

Antes de empezar a configurar conoceremos un poco sobre el concepto de que es un router y las diferentes partes que lo conforman:

22.1 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.

22.2 COMPONENTES INTERNOS DEL ROUTER

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

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

RAM: La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Por lo general, la RAM se divide de forma lógica en memoria del procesador principal y memoria compartida de entrada/salida (I/O). Las interfaces de almacenamiento temporal de los paquetes comparten la memoria de I/O compartida. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más Módulos de memoria en línea doble (DIMM).

Tiene las siguientes características y funciones:

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

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

La NVRAM tiene las siguientes características y funciones:

Almacena el archivo de configuración inicial.

Retiene el contenido cuando se apaga o reinicia el router.

Memoria flash: La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco.

Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En

otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los Módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.

La memoria flash tiene las siguientes características y funciones:

Guarda la imagen del sistema operativo (IOS)

Permite que el software se actualice sin retirar ni reemplazar chips en el procesador.

Retiene el contenido cuando se apaga o reinicia el router.

Puede almacenar varias versiones del software IOS.

Es un tipo de ROM programable, que se puede borrar electrónicamente (EEPROM).

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

La memoria de sólo lectura (ROM) tiene las siguientes características y funciones:

Guarda las instrucciones para el diagnóstico de la prueba al inicio (POST).

Guarda el programa bootstrap y el software básico del sistema operativo.

Requiere del reemplazo de chips que se pueden conectar en el motherboard para las actualizaciones del software.

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

Las interfaces LAN pueden ser configuraciones fijas o modulares.

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

Las interfaces tienen las siguientes características y funciones:

Conectan el router a la red para permitir que las tramas entren y salgan.

Pueden estar en el motherboard o en un módulo aparte.

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

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

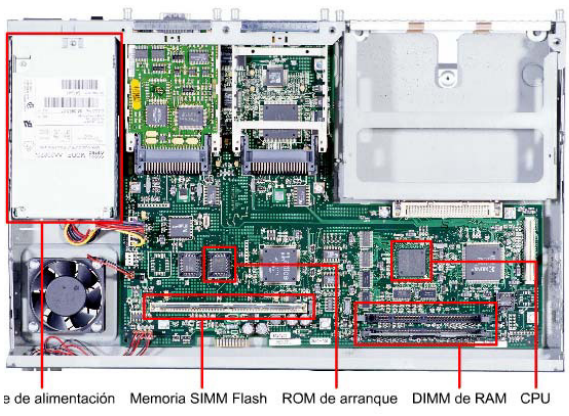


Gráfico 22-1:Componentes Internos del Router

22.3 CONEXIONES EXTERNAS DEL ROUTER

La función de los puertos de administración es diferente a la de las otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red por donde se transmiten los paquetes. El puerto de administración proporciona una conexión basada en texto

para la configuración y diagnóstico de fallas del router. Los puertos auxiliares y de consola constituyen las interfaces de administración comunes. Estos son puertos seriales asíncronos EIA-232. Están conectados a un puerto de comunicaciones de un computador. El computador debe ejecutar un programa de emulación de Terminal para iniciar la sesión basada en texto con el router. A lo largo de esta sesión, el administrador de la red puede administrar el dispositivo.

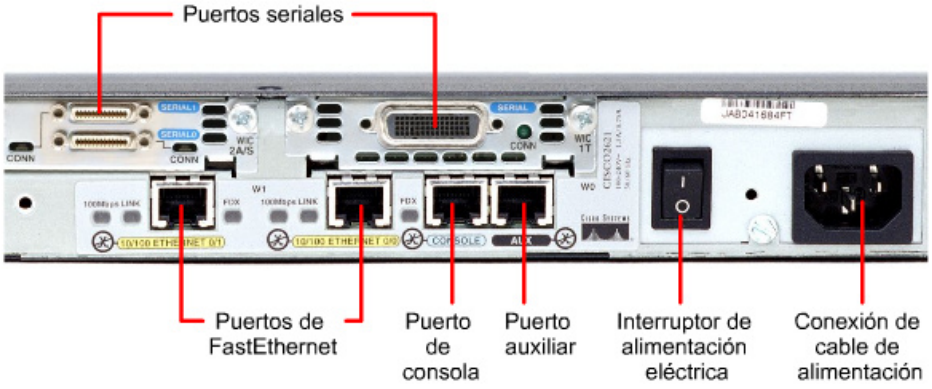


Gráfico 22-2: Conexiones Externas del Router

22.4 CONEXIONES DEL PUERTO DE ADMINISTRACIÓN

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

Cuando el router entra en servicio por primera vez, los parámetros de networking no están configurados. Por lo tanto, el router no puede comunicarse con ninguna red.

Para prepararlo para la puesta en marcha y configuración iniciales, conecte una terminal

ASCII RS-232 o un computador que emule una terminal ASCII terminal al puerto de consola del sistema. Entonces, se podrán ingresar los comandos de configuración para poner en marcha el router.

Una vez que la configuración inicial se ha introducido en el router a través del puerto de consola o auxiliar, entonces, se puede conectar el router a la red para realizar un

diagnóstico de fallas o monitoreo. Además, el router puede configurarse desde un lugar remoto haciendo telnet a una línea de terminal virtual o marcando el número de un módem conectado al puerto de consola o auxiliar del router.

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

Siga los pasos a continuación para conectar una terminal al puerto de consola del router:

Conecte la terminal mediante un cable transpuesto RJ-45 a RJ-45 y un adaptador RJ-45 a DB-9 o RJ-45 a DB-25.

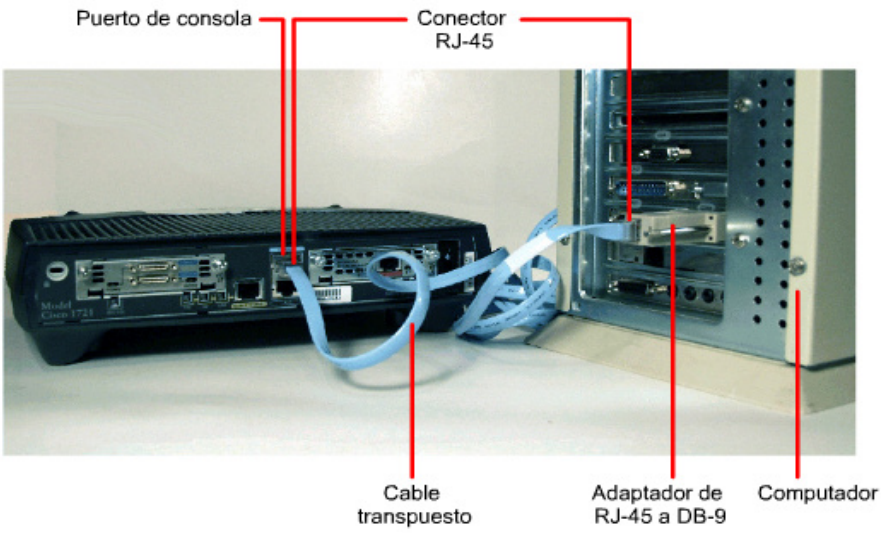


Gráfico 22-3: Conexiones del Puerto de Administración

Generalmente para que se pueda configurar un router el administrador del equipo debe ingresar a una interfaz de usuario, el acceso a ésta puede ser mediante una Terminal o

accesando remotamente, pero para este caso de estudio accesaremos a través de una Terminal.

22.5 PROCEDIMIENTO

Utilizando el HyperTerminal debe conectarse al router y establecer una sesión de consola.

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

PASOS A SEGUIR:

1.- Click izquierdo en la pestaña de inicio en el Escritorio de Windows o bien presione la tecla de Windows (Banderita)

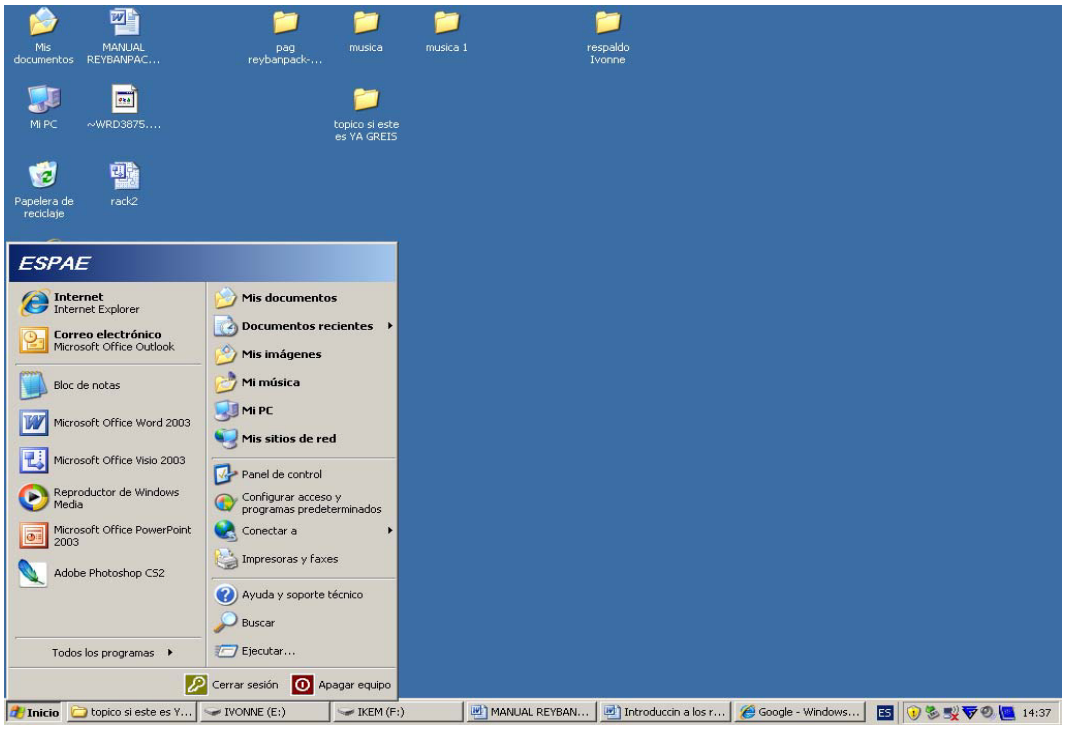


Gráfico 22-4: Conexión al Router por medio del Hiper Terminal

2.- Click izquierdo en la pestaña de Todos los Programas

Se nos despliega un menú con todos los programas instalados en nuestra PC.

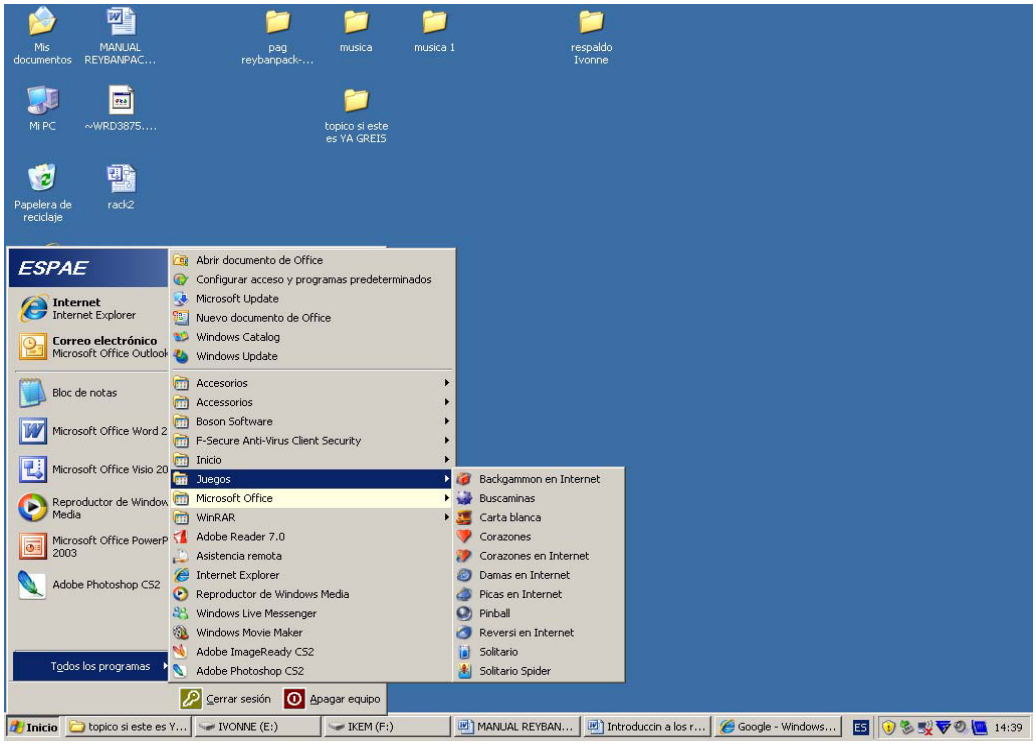


Gráfico 22-5: Conexión al Router por medio del Hiper Terminal

3.- Buscamos en el menú que se desplegó la pestaña llamada "Accesorios". Esta pestaña a su vez nos seguirá desplegando un sub-menú.

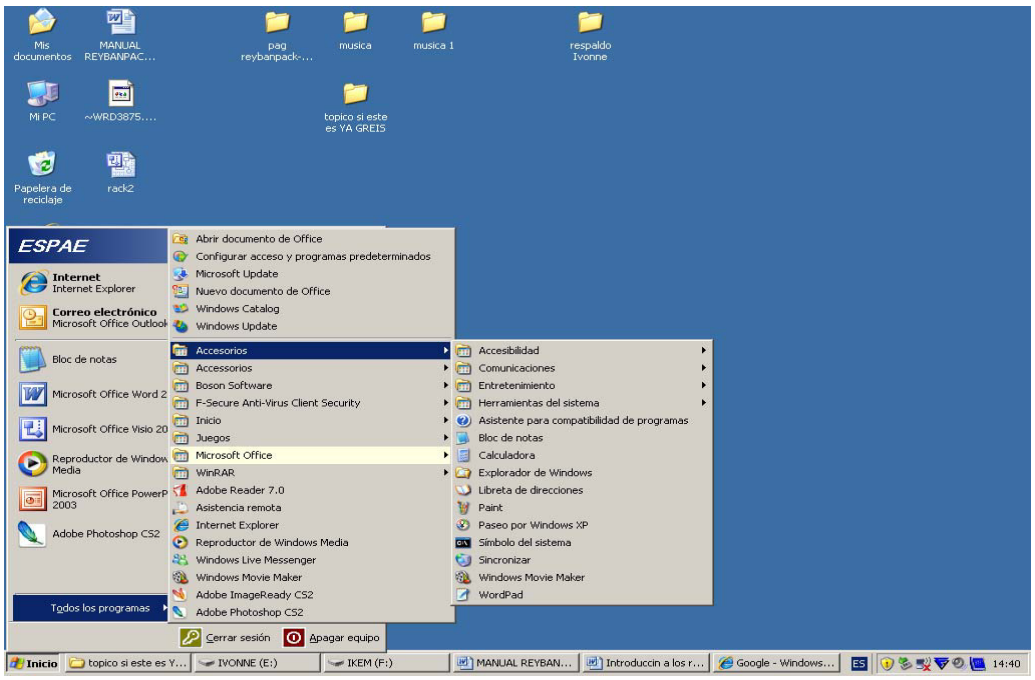


Gráfico 22-6: Conexión al Router por medio del Hiper Terminal

4.- Click en la pestaña llamada "Comunicaciones".

Aquí veremos algunas opciones de conexión hacia equipos remotos.

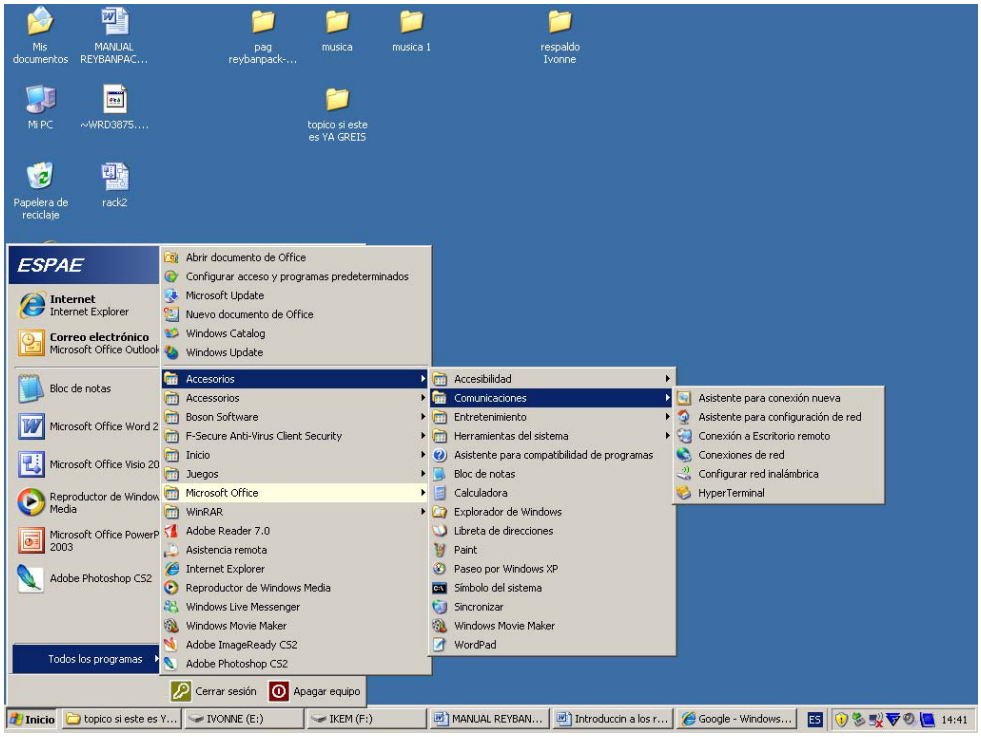


Gráfico 22-7: Conexión al Router por medio del Hiper Terminal

5.- Click en la pestaña llamada "HyperTerminal"

Una vez ya en el sub-menú de Comunicaciones, damos click en la pestaña de HyperTerminal que va a ser nuestra vía visual para el acceso al Router.

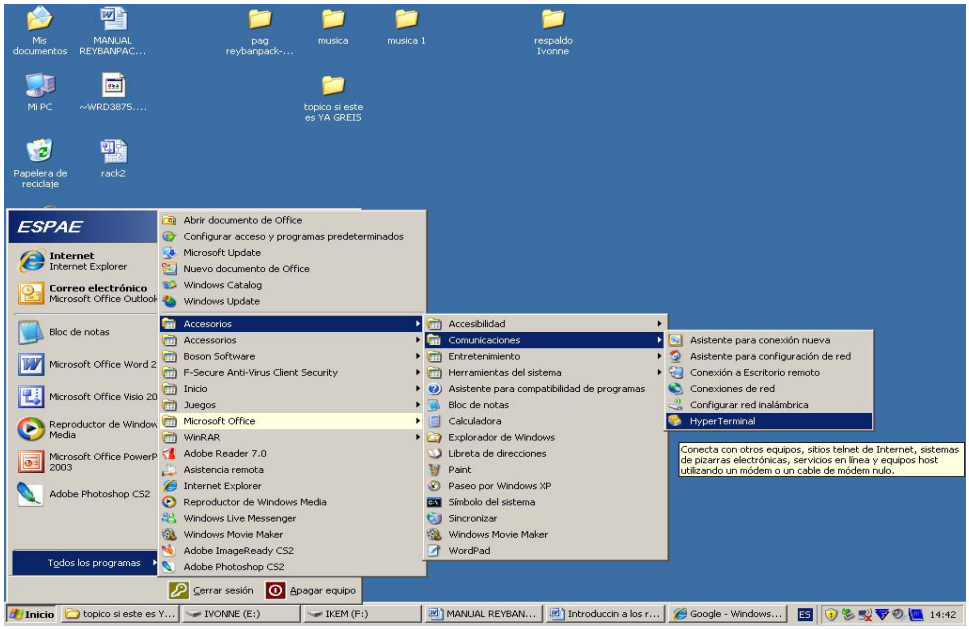


Gráfico 22-8: Conexión al Router por medio del Hiper Terminal

6.- Inmediatamente luego de haber dado click en la pestaña de HyperTerminal nos aparecerá una pequeña venta de Descripción de la Conexión, aquí le damos un nombre y le asignamos un tipo a la conexión.

El nombre de la conexión puede ser cualquiera, pero se recomienda algo que este relacionado a lo que esta trabajando, en este caso le pondremos Grupo_ESPOL.

Luego debajo de donde ubicamos el nombre de la conexión se encuentra una pequeña barra con una serie de iconos, cada una es para un tipo de conexión diferente.

Para nuestra conexión escogeremos el primer icono y daremos click en aceptar o simplemente damos <ENTER>

Si damos click en cancelar se cerrará la ventana de Descripción de la conexión, si se desea volver a ingresar se deberá seguir los pasos que detallamos para abrir la HyperTerminal.

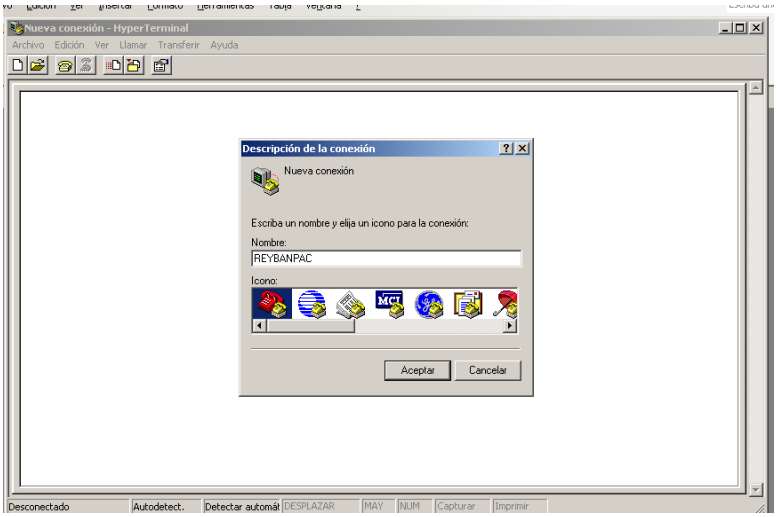


Gráfico 22-9: Configuración Puerto Com Hiper Terminal

7.- Escogemos el puerto con el cual nos vamos a conectar al Router, por lo general es el puerto COM1 y luego damos click en aceptar o presionamos la tecla <ENTER> para pasar al siguiente paso.

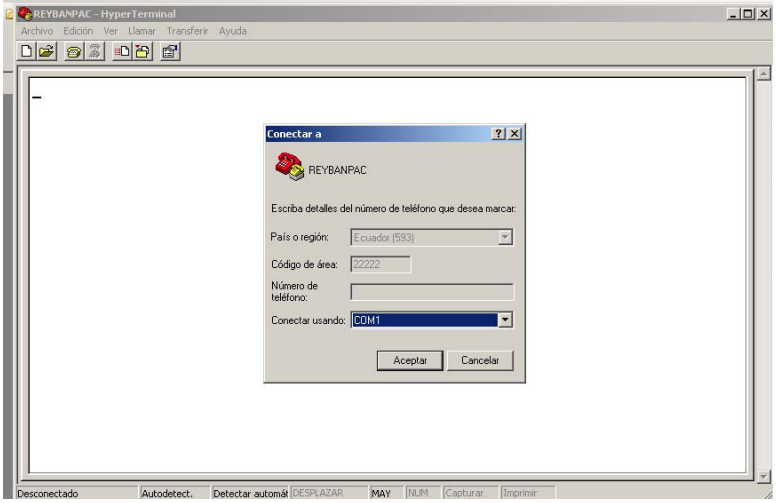


Gráfico 22-10: Configuración Puerto Com Hiper Terminal

Depende del medio que escojamos se habilitarán y deshabilitarán, o hasta pueden cambiar las propiedades de la conexión, en este caso al escogeremos la conexión usando COM1 se deshabilitarán las demás opciones.

Si damos click en cancelar automáticamente la venta se cerrará y habrá que cerrar también la venta que está detrás dando click en la cruz ubicada en la parte superior derecha, si nos pide guardar le ponemos no, ya que aún no hemos hecho nada que justifique guardar la conexión.

8.- Configuramos las propiedades del puerto COM1 según los parámetros:

a. 9600bps
b. 8 bits de datos
c. Ninguno (paridad)
d. 1 (Bit de parada)
e. Ninguno (Control de flujo)

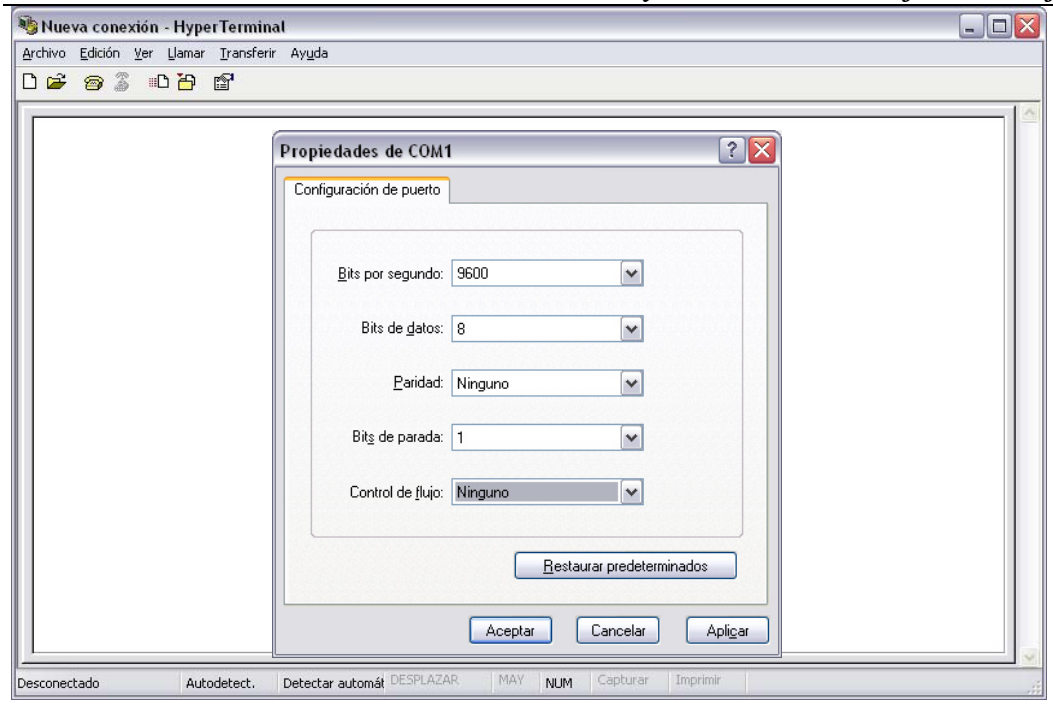


Gráfico 22-11: Configuración Puerto Com Hiper Terminal

9.- Empecemos a configurar

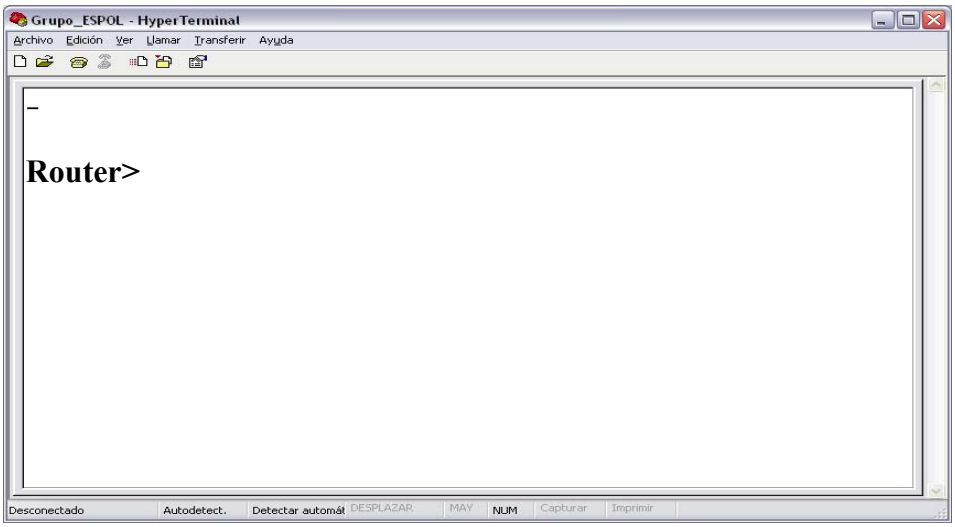


Gráfico 22-12: Configuración Puerto Com Hiper Terminal

23 MODOS DE INTERFAZ DE USUARIO

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

El IOS suministra un servicio de intérprete de comandos, denominado comando ejecutivo (EXEC). Luego de ingresar un comando, el EXEC lo valida y ejecuta.

Como característica de seguridad, el software Cisco IOS divide las sesiones EXEC en dos niveles de acceso. Estos niveles son el modo EXEC usuario y el modo EXEC privilegiado. El modo EXEC privilegiado también se denomina el modo enable. Las siguientes son las características resaltantes del modo EXEC usuario y del modo EXEC privilegiado:

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

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

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

A continuación veremos un esquema de los diferentes usuarios a y los permisos que tiene cada uno:

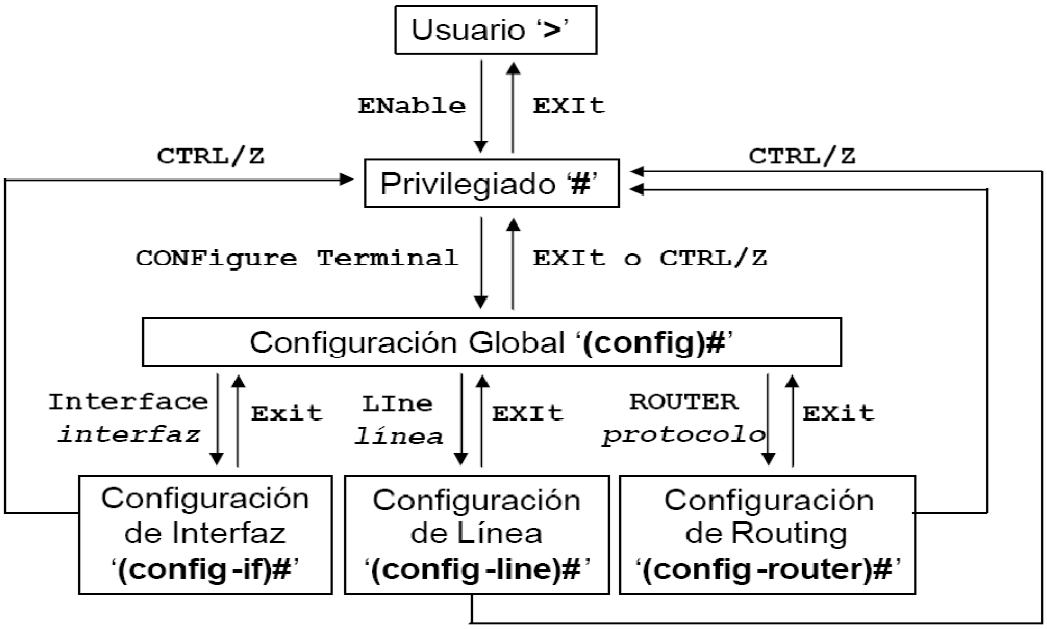


Gráfico 23-1: Esquema Usuarios y Privilegios

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

- Interfaces
- Subinterfaces
- Línea
- Router
- Mapas de enrutamiento

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

Para ingresar al modo EXEC privilegiado, escriba enable o su abreviatura ena. Esto puede hacer que el router pida al usuario una contraseña, que se haya fijado con anterioridad.

```
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router> <-------- Símbolo del modo usuario
Router>enable
Password:
Router# <-------- Símbolo del modo privilegiado
Router#disable
Router>
Router>exit
```

Los comandos del modo de configuración global se utilizan en un router para ejecutar comandos de configuración que afectan al sistema como un todo.

Router#configure terminal

Router(config)#

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

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

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

Al escribir exit desde alguno de estos modos de configuración específicos, el router regresa al modo de configuración global. Al presionar Control-Z, se sale por completo del modo de configuración y el router vuelve al modo EXEC privilegiado.

24 CONFIGURACIÓN DEL NOMBRE DE ROUTER

Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante los siguientes comandos:

Router(config)#hostname Matriz

Matriz(config)#

Al presionar la tecla Enter, la petición de entrada ya no mostrará el nombre de host por defecto ('Router'), sino el nombre de host que se acaba de configurar, 'Tokio', en el ejemplo anterior.

25 CONFIGURACIÓN DE CONTRASEÑAS DE ROUTER

Las contraseñas restringen el acceso a los routers. Se debe siempre configurar contraseñas para las líneas de terminales virtuales y para la línea de consola. Las contraseñas también se usan para controlar el acceso al modo EXEC privilegiado, a fin de que sólo los usuarios autorizados puedan hacer cambios al archivo de configuración. Aunque es opcional, se recomienda configurar una contraseña para la línea de comando. Los siguientes comandos se utilizan para fijar dicha contraseña.

Router#configure terminal
Router(config)#line console 0
Router(config-line)#password <password>
Router(config-line)#login

Se debe fijar contraseñas en una o más de las líneas de terminales virtuales (VTY), para habilitar el acceso remoto de usuarios al router mediante Telnet. Normalmente, los routers Cisco permiten cinco líneas de VTY identificadas del 0 al 4, aunque según el hardware particular, puede haber modalidades diferentes para las conexiones de VTY. Se suele usar la misma contraseña para todas las líneas, pero a veces se reserva una línea mediante una contraseña exclusiva, para que sea posible el acceso al router aunque haya demanda de más de cuatro conexiones.

Los siguientes comandos se utilizan para establecer contraseñas en las líneas de VTY:

Router#configure terminal

Router(config)#line vty 0 4

(config-line)#password<password>

Router(config-line)#login

Los comandos enable password y enable secret se utilizan para restringir el acceso al modo EXEC privilegiado. El comando enable password se utiliza sólo si no se ha configurado previamente enable secret. Se recomienda habilitar siempre enable secret, ya que a diferencia de enable password, la contraseña estará siempre cifrada. Estos son los comandos que se utilizan para configurar las contraseñas:

Router(config)#enable password <password>

Router(config)#enable secret<password>

En ocasiones es deseable evitar que las contraseñas se muestren en texto sin cifrar al ejecutar los comandos show running-config o show startup-config. El siguiente comando se utiliza para cifrar las contraseñas al mostrar los datos de configuración:

Router(config)#service password-encryption

El comando service password-encryption aplica un cifrado débil a todas las contraseñas sin cifrar. El comando enable secret <password> usa un fuerte algoritmo MD5 para cifrar.

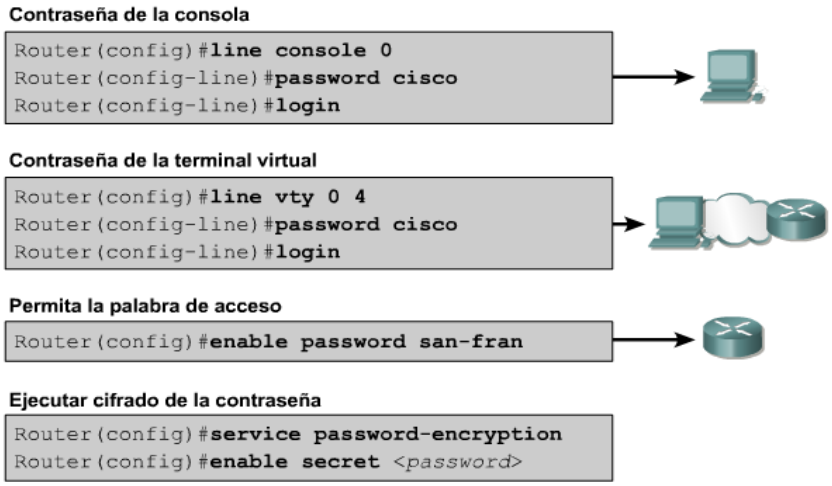


Gráfico 25-1: Configuración de Contraseñas del Router

25.1 AYUDA MEDIANTE EL TECLADO EN LA INTERFAZ DE LÍNEA DE COMANDO

Al escribir un signo de interrogación (?) en la petición de entrada del modo usuario o del modo privilegiado, aparece una útil lista de los comandos disponibles. Observe el "--More--" (Más) que aparece en la parte inferior de la pantalla de muestra. La pantalla muestra varias líneas a la vez. La petición de entrada "--More--" que aparece en la parte inferior de la pantalla indica que hay más pantallas disponibles.

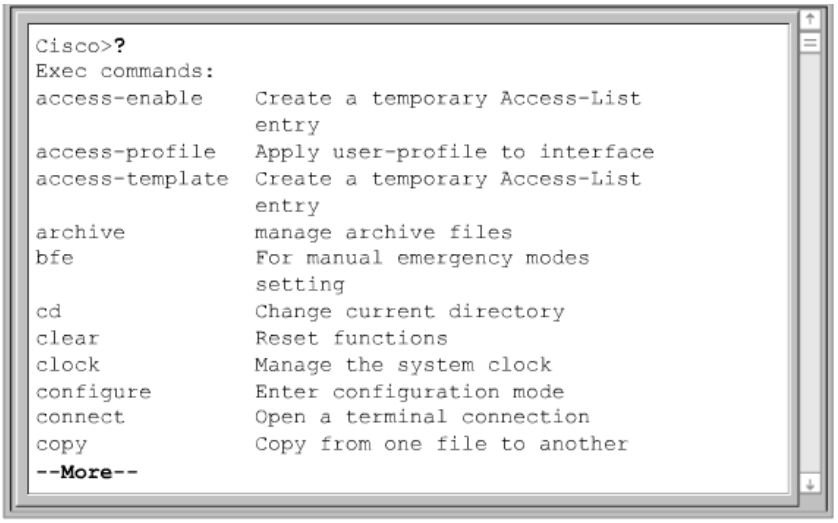


Gráfico 25-2: Ayuda mediante el teclado en la interfaz de la línea de Comando

Si un usuario desea configurar el reloj del router pero no sabe cuál es el comando adecuado, puede usar la función de ayuda para conocer cuál es el comando correcto. El ejercicio siguiente ilustra uno de los muchos usos de la función de ayuda.

La tarea es configurar el reloj del router. Considere que no conoce el comando correspondiente, y efectúe lo siguiente:

Paso 1 Use ? para encontrar el comando adecuado para configurar el reloj. El resultado de la ayuda indica que se requiere el comando clock (reloj).

Paso 2 Verifique la sintaxis para hacer cambios en la hora.

Paso 3 Introduzca la hora actual en horas, minutos y segundos, tal como se muestra en la Figura. El sistema indica que se debe suministrar información adicional para completar el comando.

```
Cisco#cl?
clear  clock
Cisco#clock
% Incomplete command.
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
```

25.2 DIAGNÓSTICO DE FALLAS DE LOS ERRORES DE LÍNEA DE COMANDOS

Los errores de línea de comandos se producen principalmente debido a errores de tecleado. Si un comando es escrito de forma incorrecta, la interfaz del usuario muestra el error mediante un indicador de error (^). El símbolo "^"aparece en el punto de la cadena del comando donde se introdujo el comando, palabra clave o argumento incorrecto. El indicador de ubicación del error y el sistema de ayuda interactiva permiten al usuario localizar y corregir fácilmente los errores de sintaxis.

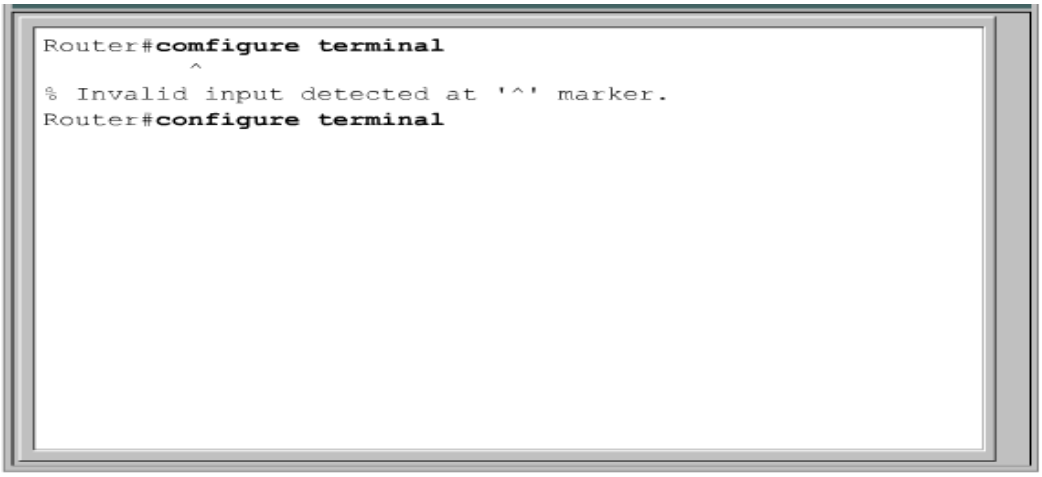


Gráfico 25-3: Diagnostico de fallas de los errores de línea de comando

Si una línea de comando es escrita de forma incorrecta y se presiona la tecla Intro, se puede presionar la tecla flecha-arriba para reescribir el último comando. Use las teclas flecha-derecha e izquierda para mover el cursor hasta el lugar donde se cometió el error. Luego escriba la corrección necesaria. Si es necesario eliminar algo, use la tecla retroceso.

25.3 USO DE LOS COMANDOS SHOW

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

show interfaces: Muestra las estadísticas completas de todas las interfaces del router. Para ver las estadísticas de una interfaz específica, ejecute el comando show interfaces seguido de la interfaz específica y el número de puerto. Por ejemplo:

Router#show interfaces serial 0/1

show controllers serial: Muestra información específica de la interface de hardware. El comnado debe incluir el número de puerto y/o de ranura de la interfaz. Por ejemplo:

Router#show controllers serial 0/1

show clock: Muestra la hora fijada en el router.

show hosts: Muestra la lista en caché de los nombres de host y sus direcciones.

show users: Muestra todos los usuarios conectados al router.

show history: Muestra un historial de los comandos ingresados.

show flash: Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí.

show version: Despliega la información acerca del routery de la imagen de IOS que esté corriendo en al RAM. Este comando también muestra el valor del registro de configuración del router.

show ARP: Muestra la tabla ARP del router.

show protocols: Muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado.

show startup-configuration: Muestra el archivo de configuración almacenado en la NVRAM.

show running-configuration: Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.

25.4 EL COMANDO SHOW VERSION

El comando show version muestra información acerca de la versión del software Cisco IOS en uso en el router. Esto incluye el registro de configuración y el registro de arranque.

```
GAD#show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version
12.2(11)P, RELEASE SOFTWARE (fc1)
… <output omitted>…
ROM: System Bootstrap, Version 11.1(10)AA, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
ROM: 1700 Software (C1700-BOOT-R), Version
11.1(10)AA, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
GAD uptime is 3 weeks 6 days 2 hours, 11 minutes
System restarted by power-on
System image file is "flash:c1700-bnsy-l.122-
11.p", booted via flash
cisco 1721 (68360) processor (revision C) with
3584K/512K bytes of memory.
Processor board ID 12014633, with hardware
```

La Figura muestra la siguiente información acerca del comando show version:

Versión e información descriptiva del IOS

Versión de la ROM de bootstrap

Versión de la ROM de arranque

Tiempo de actividad del router

Último método de reinicio

Ubicación y nombre del archivo de imagen del sistema

Use el comando show version para identificar la imagen del IOS del router y la fuente de arranque.

25.5 CONFIGURACIÓN DE UNA INTERFAZ SERIAL

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

1. Ingrese al modo de configuración global

2. Ingrese al modo de configuración de interfaz
3. Especifique la dirección de la interfaz y la máscara de subred
4. Si el cable de conexión es DCE, fije la velocidad de sincronización. Omita este paso si el cable es DTE.
5. Active la interfaz.

A cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP. Configure la dirección de IP mediante los siguientes comandos:

Router(config)#**interface serial 0/0**
Router(config-if)#**ip address** <*ip address*> <*netmask*>

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

Para cada tipo de servicio WAN, el equipo terminal del abonado (CPE), a menudo un router, es el equipo terminal de datos (DTE). Este se conecta al proveedor del servicio por medio de un dispositivo del equipo de transmisión de datos (DCE), en general, un módem o una unidad de servicio de canal/unidad de servicio de datos (CSU/DSU). Este dispositivo se usa para convertir los datos del DTE a una forma aceptable para el proveedor del servicio WAN.

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

Los routers Cisco pueden usar diferentes conectores para las interfaces seriales. La interfaz de la izquierda es una interfaz serial inteligente. La interfaz de la derecha es una conexión DB-60. Esto hace que la selección del cable serial que conecta el sistema de la red a los dispositivos seriales sea una parte fundamental de la configuración de una WAN.

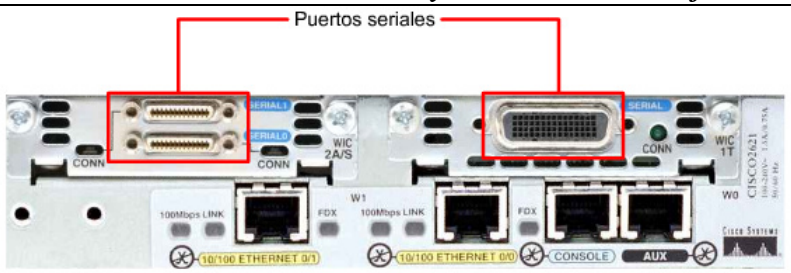


Gráfico 25-4: Interfaces del Router

El DTE y el DCE son dos tipos de interfaces seriales que los dispositivos usan para comunicarse. La diferencia clave entre los dos es que el dispositivo DCE proporciona la señal reloj para las comunicaciones en el bus. La documentación del dispositivo debe especificar si es DTE o DCE.

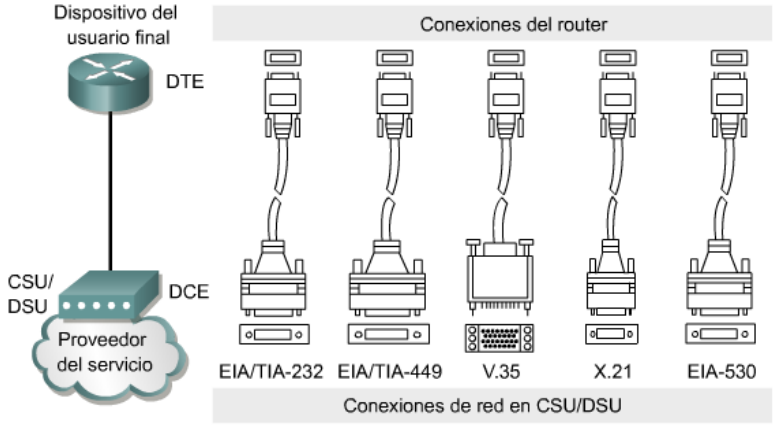


Gráfico 25-5: Conexiones del Router

Cada dispositivo podría requerir un estándar serial diferente. Cada estándar define las señales del cable y especifica el conector del extremo del cable. Siempre se debe consultar la documentación del dispositivo para obtener información sobre el estándar de señalización.

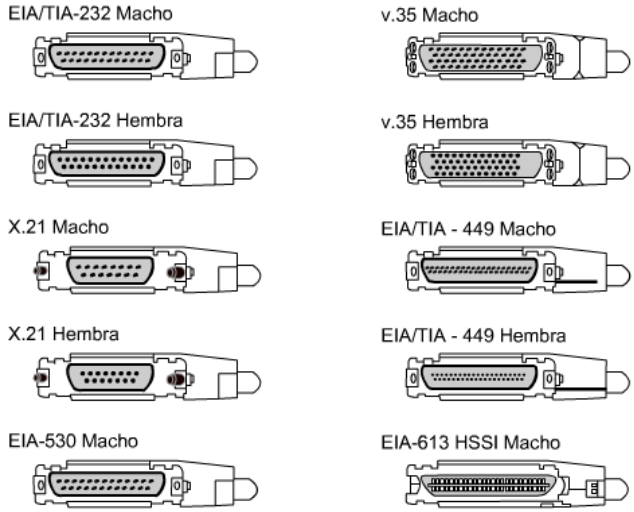


Gráfico 25-6: Tipos de conectores seriales

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

En los enlaces seriales interconectados directamente, un extremo debe considerarse como un DCE y debe proporcionar la señal de sincronización. Se activa la sincronización y se fija la velocidad mediante el comando clock rate. Las velocidades de sincronización disponibles (en bits por segundo) son: 56000, 64000, 72000, etc... No obstante, es posible que algunas de estas velocidades no estén disponibles en algunas interfaces seriales, según su capacidad.

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ingresa el comando no shutdown. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o de diagnóstico de fallas, se utiliza el comando shutdown para desactivarla.

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

Router(config)#**interface serial 0/0**
Router(config-if)#**clock rate 64000**
Router(config-if)#**no shutdown**

25.6 CONFIGURACIÓN DE UNA INTERFAZ ETHERNET

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

Para configurar una interfaz Ethernet, siga estos pasos:

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

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ejecuta el comando no shutdown. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o diagnóstico de fallas, se utiliza el comando shutdown para desactivarla.

25.7 DESCRIPCIÓN DE INTERFACES

La descripción de las interfaces se emplea para indicar información importante, como puede ser la relativa a un router distante, el número de un circuito, o un segmento de red específico. La descripción de la interfaz puede ayudar a un usuario de red a recordar información específica de la interfaz, como por ejemplo, a cuál red atiende dicha interfaz. La descripción es sólo un comentario escrito acerca de la interfaz.

Router#**configure terminal**
Router(config)#**interface ethernet 0**
Router(config-if)#**ip address 200.0.10.9 255.255.255.248**
Router(config-if)# **description edificio matriz**
Router(config-if)#**no shutdown**

25.8 ENRUTAMIENTO ESTÁTICO

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:
El administrador de red configura la ruta.

El router instala la ruta en la tabla de enrutamiento.

Los paquetes se enrutan de acuerdo a la ruta estática.

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

Ejemplo:

Router#**configure terminal**
Router(config)#**ip route 192.168.16.33 255.255.255.0 s0**

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 o el siguiente salto, como se muestra a continuación:

Router(config)#**ip route 192.168.16.0 255.255.255.0 172.16.4.1 130**

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.

25.9 ENRUTAMIENTO POR DEFECTO

Las rutas por defecto se usan para enviar paquetes a destinos que no coinciden con los de ninguna de las otras rutas en la tabla de enrutamiento. Generalmente, los routers están configurados con una ruta por defecto para el tráfico que se dirige a la Internet, ya que a menudo resulta poco práctico e innecesario mantener rutas hacia todas las redes de la Internet.

En realidad, una ruta por defecto es una ruta estática especial que utiliza este formato:

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

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

Siga estos pasos para configurar rutas por defecto.

1. Ingrese al modo de configuración global.
2. Ejecute el comando ip route con 0.0.0.0 como la dirección de red de destino y 0.0.0.0 como máscara de subred. La opción address para la ruta por defecto puede ser la interfaz del router local que está conectado a las redes externas, o puede ser la dirección IP del router del siguiente salto. En la mayoría de los casos, es preferible especificar la dirección IP del router del siguiente salto.
3. Salga del modo de configuración global.
4. Guarde la configuración activa en la NVRAM mediante el comando copy running-config sartup-config.

Router#**configure terminal**
Router(config)#**ip route 0.0.0.0 0.0.0.0 s0**
Router(config)#**exit**
Router#**copy running-config startup-config**

25.10 ENRUTAMIENTO DINÁMICO

El enrutamiento dinámico significa que el router va averiguando las rutas para llegar al destino por medio de actualizaciones periódicas enviadas desde otros routers.

25.11 INTRODUCCIÓN A LOS PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento son diferentes a los protocolos enrutados tanto en su función como en su tarea.

Un protocolo de enrutamiento 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)
- protocolo de enrutamiento exterior por vector-distancia(BGP)

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

Ejemplos de protocolos enrutados:

- Protocolo Internet (IP)
- Intercambio de paquetes de internetwork (IPX)

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos. Cuando todos los routers de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia.

25.12 PROTOCOLOS DE ENRUTAMIENTO POR VECTOR-DISTANCIA

Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro. Estas actualizaciones periódicas entre routers informan de los cambios de topología. Los algoritmos de vector-distancia no permiten que un router conozca la topología exacta de una red, ya que cada router solo ve a sus routers vecinos.

Las actualizaciones de las tablas de enrutamiento se producen al haber cambios en la topología. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada una de las redes indicadas en la tabla.

La habilitación del enrutamiento de paquetes de IP, requiere fijar parámetros tanto globales como de enrutamiento. Las tareas globales incluyen la selección de un protocolo de enrutamiento, por ejemplo: RIP, IGRP, EIGRP o OSPF. La tarea principal del modo configuración de enrutamiento es indicar los números IP de la red. El enrutamiento dinámico utiliza comunicaciones broadcast y multicast con los otros routers. La métrica de enrutamiento ayuda a los routers a encontrar la mejor ruta hacia cada red o subred.

25.13 PROTOCOLOS DE ENRUTAMIENTO

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

Es un protocolo de enrutamiento por vector-distancia.

Utiliza el número de saltos como métrica para la selección de rutas.

Si el número de saltos es superior a 15, el paquete es desechado.

Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

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

Es un protocolo de enrutamiento por vector-distancia.

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

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

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

Es un protocolo mejorado de enrutamiento por vector-distancia.

Utiliza 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.

26 CONFIGURACIÓN DEL ENRUTAMIENTO

El comando router inicia el proceso de enrutamiento.

El comando network es necesario, ya que permite que el proceso de enrutamiento determine cuáles son las interfaces que participan en el envío y la recepción de las actualizaciones de enrutamiento.

Un ejemplo de configuración de enrutamiento es:

router(config)#**router rip**
router(config-router)#**network 192.168.13.0**

26.1 PROTOCOLO DE ENRUTAMIENTO RIP

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 Version 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 enmascaramiento de subredes de longitud variable (VLSM).

Un ejemplo de configuración de enrutamiento rip versión 2 es:

Router#**configure terminal**
router(config)#**router rip**
router(config-router)#**version 2**
router(config-router)#**network 192.168.13.0**

Entre las tareas opcionales se encuentran:

- Aplicar compensaciones a la métrica de enrutamiento.
- Ajustar los temporizadores.
- Especificar una versión de RIP.
- Habilitar la autenticación de RIP.
- Configurar el resumen de las rutas en una interfaz.
- Verificar el resumen de las rutas IP.
- Inhabilitar el resumen automático de rutas.

El comando show ip route se puede utilizar para verificar que las rutas recibidas por los routers RIP vecinos estén instaladas en la tabla de enrutamiento. Examine el resultado del comando y busque las rutas RIP que señaladas con "R". Recuerde que la red tardará algún tiempo en converger, de modo que puede que no aparezcan las rutas de forma inmediata.

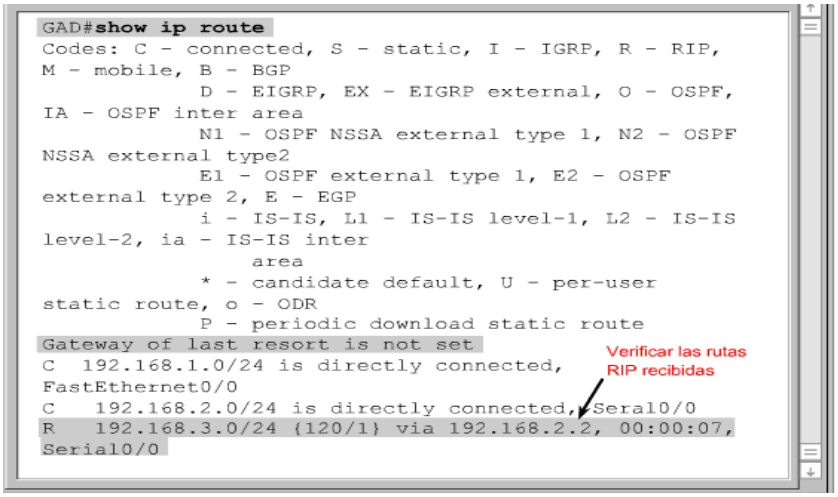


Gráfico 26-1: Show IP Route

26.2 PROTOCOLOS DE ENRUTAMIENTO DE ESTADO DEL ENLACE

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

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

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

Es un protocolo de enrutamiento de estado del enlace.

Es un protocolo de enrutamiento público (open Standard).

Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.

Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

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

Es un protocolo de enrutamiento exterior por vector-distancia.

Se usa entre ISPs o entre los ISPs y sus clientes.

Se usa para enrutar el tráfico de Internet entre sistemas autónomos.

26.3 PROTOCOLO DE ENRUTAMIENTO OSPF

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

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

OSPF es apropiado para Internet Works 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

26.4 TIPOS DE RED OSPF

Las interfaces OSPF reconocen tres tipos de redes:

Multiacceso de broadcast como por ejemplo Ethernet.

Redes punto a punto.

Multiacceso sin broadcast (NBMA), como por ejemplo Frame Relay.

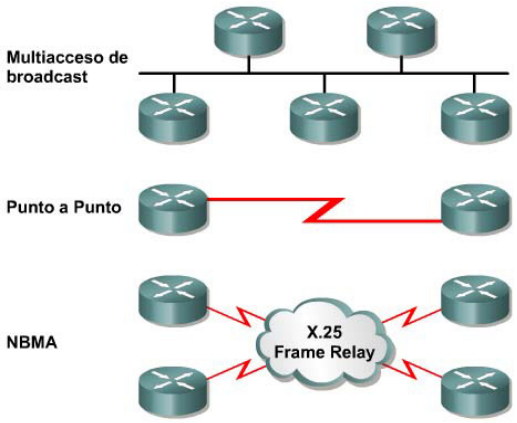


Gráfico 26-2:Tipos de Red OSPF

26.5 PROTOCOLO HELLO DE OSPF

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete hello y sigue enviando hellos a intervalos regulares.

Las reglas de intercambio de paquetes hello de OSPF se denominan protocolo Hello.

En la capa 3 del modelo OSI, los paquetes hello se direccionan hacia la dirección multicast 224.0.0.5. Esta dirección equivale a "todos los routers OSPF". Los routers OSPF utilizan los paquetes hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los Hellos se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes NBMA, como por ejemplo Frame Relay, el tiempo por defecto es de 30 segundos.

En las redes multiacceso el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR).El paquete hello transmite información para la cual todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

La configuración de OSPF requiere que el proceso de enrutamiento OSPF esté activo en el router con las direcciones de red y la información de área especificadas.

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

Router(config)#**router ospf** *process-id*

El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en el router. Se pueden iniciar varios procesos OSPF en el mismo router. El número puede tener cualquier valor entre 1 y 65.535.

Las redes IP se publican de la siguiente manera en OSPF:

Router(config-router)#**network** *address wildcard-mask* **area** *area-id*

Dirección.-Esta puede ser la dirección de red, subred o de la interfaz. 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.

26.6 DIRECCIÓN DE LOOPBACK OSPF

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

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

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

Router(config)#**interface loopback** *number*
Router(config-if)#**ip address 192.168.13.100 255.255.255.255**

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

```
! Create the loopback 0 interface
Sydney3(config)#interface loopback 0
Sydney3(config-if)#ip address 192.168.31.33
255.255.255.255
Sydney3(config-if)#exit
! Remove loopback 0 interface
Sydney3(config)#no interface loopback 0
Sydney3(config)#
01:47:27: %LINK-5-CHANGED: Interface Loopback0, changed
state to administratively down
```

Gráfico 26-3: Dirección de Loopback en OSPF

26.7 MODIFICACIÓN DE LA MÉTRICA DE COSTOS DE OSPF

OSPF utiliza el costo como métrica para determinar la mejor ruta. Un costo se asocia con el lado de salida de cada interfaz de router. Los costos también se asocian con datos de enrutamiento derivados en forma externa. Por lo general, el costo de ruta se calcula mediante la fórmula 10^8/ancho de banda, donde el ancho de banda se expresa en bps.

Resulta esencial para la operación correcta de OSPF que se establezca el ancho de banda de interfaz correcto. El ancho de banda por defecto para las interfaces seriales Cisco es 1,544 Mbps o 1544 kbps.

Router(config)#**interface fastEthernet 0/0**
Router(config-if)#**bandwidth 100**

Es posible cambiar el costo para afectar el resultado de los cálculos de costo OSPF. Una situación se produce al utilizar Gigabit Ethernet. Con la configuración por defecto, se asigna el valor de costo más bajo (1) a un enlace de 100 Mbps. En una situación con con enlaces Gigabit Ethernet y 100-Mbps, los valores de costo por defecto podrían hacer que el enrutamiento tome una ruta menos deseable a menos que estos se ajusten. El número de costo se puede establecer entre 1 y 65.535.

Utilice el siguiente comando de configuración de interfaz para establecer el costo del enlace:

Router(config)#**interface fastEthernet 0/0**
Router(config-if)#**ip ospf cost 1**

26.8 CONFIGURACIÓN DE LA AUTENTICACIÓN DE OSPF

Por defecto, un router confía en que la información de enrutamiento proviene de un router que debería estar enviando información. Un router también confía en que la información no haya sido alterada a lo largo de la ruta.

Para garantizar esta confianza, los routers de un área específica pueden configurarse para autenticarse entre sí.

Cada interfaz OSPF puede presentar una clave de autenticación para que la usen los routers que envían información de OSPF hacia otros routers del segmento. La clave de autenticación, conocida como contraseña, es un secreto compartido entre los routers. Esta clave se utiliza para generar los datos de autenticación en el encabezado del paquete de OSPF. La contraseña puede contener hasta ocho caracteres. Utilice la siguiente sintaxis de comando para configurar la autenticación de OSPF:

Router(config-if)#**ip ospf authentication-key** *password*

Una vez configurada la contraseña, se debe habilitar la autenticación:

Router(config-router)#**area** *area-number* **authentication**

Con la autenticación sencilla, se envía la contraseña como texto sin cifrar. Esto significa que se puede decodificar fácilmente si un husmeador de paquetes captura un paquete de OSPF.Se recomienda cifrar la información de autenticación. Para enviar la información de autenticación cifrada y asegurar mayor seguridad, se utiliza la palabra clave message-digest.

La palabra clave MD5 especifica el tipo de algoritmo de hash de message-digest a utilizar y el campo de tipo de cifrado se refiere al tipo de cifrado, donde 0 significa ninguno y 7 significa propietario.

Utilice la sintaxis del modo de comando de configuración de interfaz:

Router(config-if)#**ip ospf message-digest-key** *key-id encryption-type* **md5** *key*

El key-id es un identificador y toma un valor en el intervalo de 1 a 255. Key es una contraseña alfanumérica de hasta dieciséis caracteres. Los routers vecinos deben usar el mismo identificador clave con el mismo valor clave.

Se configura lo siguiente en el modo de configuración del router:
Router(config-router)#**area** *area-id* **authentication message-digest**

La autenticación MD5 crea un message-digest. Un message-digest son datos cifrados en base a la contraseña y el contenido del paquete. El router receptor utiliza la contraseña compartida y el paquete para recalcular el digest. Si los digests coinciden, el router considera que el origen y el contenido del paquete no han sido alterados. El tipo de autenticación identifica qué clase de autenticación, de haber alguna, se está utilizando. En el caso de la autenticación del message-digest, el campo de datos de autenticación contiene el key-id y la longitud del message-digest que se ha adjuntado al paquete. El message-digest es como una filigrana que no se puede falsificar.

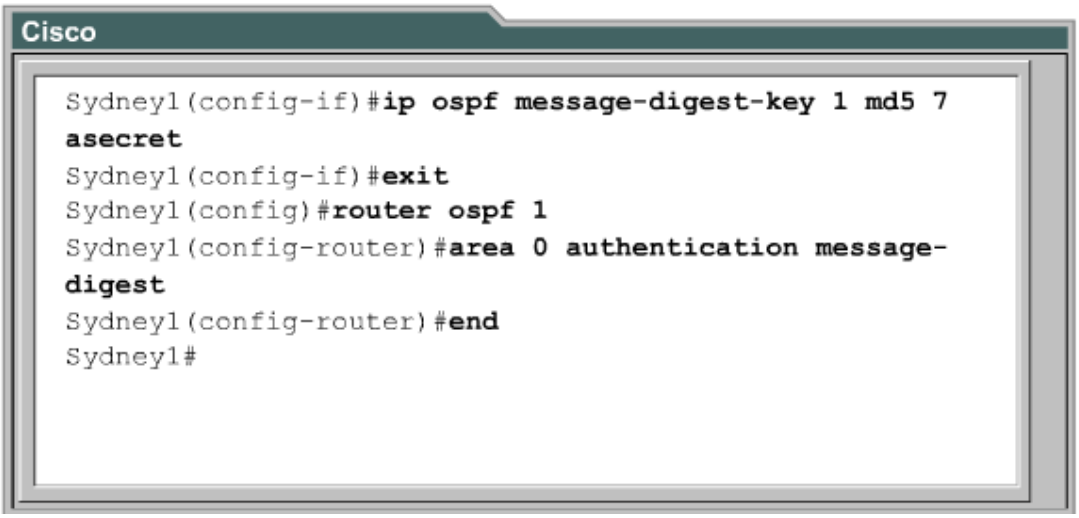


Gráfico 26-4: Configuración de la autenticación de OSPF

26.9 CONFIGURACIÓN DE LOS TEMPORIZADORES OSPF

Los routers OSPF deben tener los mismos intervalos hello y los mismos intervalos muertos para intercambiar información. Por defecto, el intervalo muerto es de cuatro veces el valor del intervalo hello. Esto significa que un router tiene cuatro oportunidades de enviar un paquete hello antes de ser declarado muerto.

En las redes OSPF de broadcast, el intervalo hello por defecto es de 10 segundos y el intervalo muerto por defecto es de 40 segundos. En las redes que no son de broadcast, el intervalo hello por defecto es de 30 segundos y el intervalo muerto por defecto es de 120 segundos. Estos valores por defecto dan como resultado una operación eficiente de OSPF y muy pocas veces necesitan ser modificados.

Un administrador de red puede elegir estos valores de temporizador. Se necesita una justificación de que el rendimiento de red OSPF mejorará antes de cambiar los temporizadores. Estos temporizadores deben configurarse para que coincidan con los de cualquier router vecino.

Para configurar los intervalos hello y muertos de una interfaz, utilice los siguientes comandos:

Router(config-if)#**ip ospf hello-interval** *seconds*
Router(config-if)#**ip ospf dead-interval** *seconds*

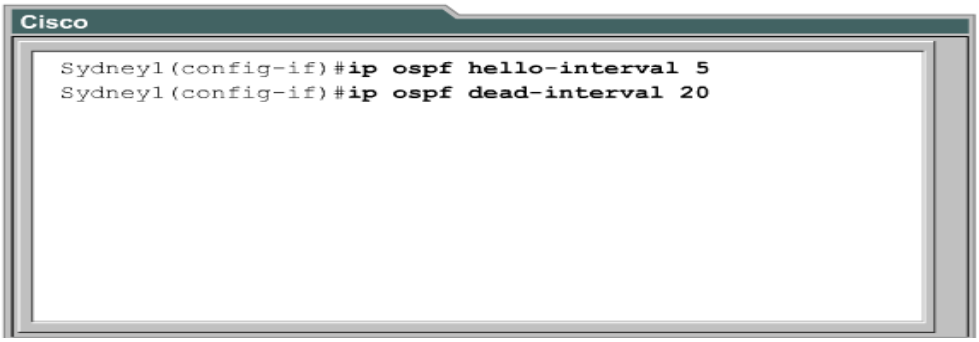


Gráfico 26-5: Configuración a de los Temporizadores OSPF

27 VERIFICACIÓN DE CONFIGURACIÓN OSPF

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

27.1 Show ip protocol

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

27.2 Show ip route

Esto muestra las rutas que el router conoce y describe como se conocieron. Ésta es una de las mejores maneras para determinar la conectividad entre el router local y el resto de la red.

27.3 Show ip ospf interface

Esto verifica que las interfaces se hayan configurado en la áreas planificadas. Si no se especifica una dirección loopback, la interfaz con la dirección más alta se considera como el ID del router.

Además proporciona los intervalos de temporización como el intervalo hello y muestra las adyacencias del router.

27.4 Show ip ospf

Muestra la cantidad de veces en que se ha usado el algoritmo SPF. También muestra el intervalo de actualización de estado de enlace si no se han producido cambios topológicos.

27.5 Show ip ospf neighbor detail

Este comando muestra un listado detallado de vecinos, sus prioridades y estados.

27.6 Show ip ospf database

Esto muestra el contenido de la base de datos topológica que mantiene el router y el ID del proceso OSPF.

27.7 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.

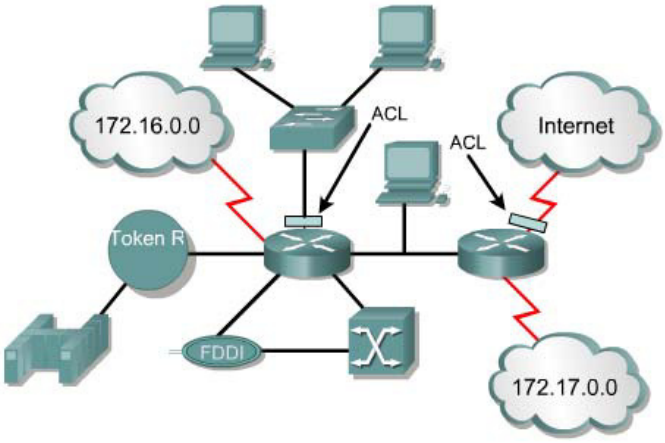


Gráfico 27-1: *V*erificación de Configuración OSPF

28 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. Si 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.

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

PROTOCOLO	INTERVALO
IP	1-99, 1300-1999
IP EXTENDIDO	100-199, 2000-2699
APPLE TALK	600-699
IPX	800-899
IPX EXTENDIDO	900-999

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.

Gráfico 28-1: ACL

Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando no access-list list-number y entonces proceder a crear una nueva ACL.

```
Router(config)#no access-list 2
```

28.2 FUNCIÓN DE LA MÁSCARA WILDCARD

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

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

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones any y host. Para explicarlo de forma sencilla, la opción any reemplaza la dirección IP con 0.0.0.0 y la máscara wildcard por 255.255.255.255. Esta opción concuerda con cualquier dirección con la que se la compare. La máscara 0.0.0.0 reemplaza la opción host.

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

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

Se la puede escribir como:

Router(config)#access-list 1 permit any

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

Se la puede escribir como:

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

28.3 VERIFICACIÓN DE LAS ACL

El comando show ip interface muestra información de la interfaz IP e indica si se ha establecido alguna ACL. El comando show access-lists muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número ACL como opción a este comando. El comando show running-config también revela las listas de acceso en el router y la información de asignación de interfaz.

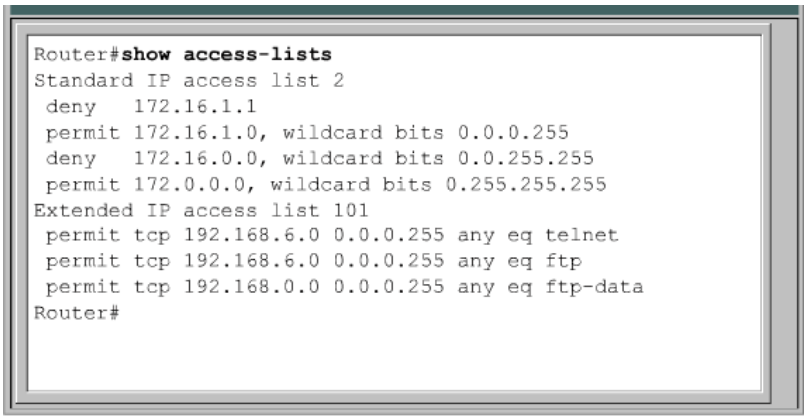


Gráfico 28-2: Verificación de las ACL

28.4 ACL estándar

En la versión 12.0.1 del IOS de Cisco, se usaron por primera vez números adicionales (1300 al 1999) para las ACLs estándar pudiendo así proveer un máximo posible de 798 ACLs estándar adicionales, a las cuales se les conoce como ACLs 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. Por ejemplo, no es suficientemente claro cual es el propósito del siguiente comando: access-list 1 permit 192.168.15.15. Es mucho más fácil leer un comentario acerca de un comando para entender sus efectos, así como sigue:

access-list 1 remark Permit only karix workstation through
access-list 1 permit 192.168.7.1

La forma no de este comando se utiliza para eliminar una ACL estándar. Ésta es la sintaxis:

Router(config)#**no access-list***access-list-number*

El comando ip access-group relaciona una ACL existente a una interface:

Router(config)#**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

Gráfico 28-3: ACL estándar

28.5 ACL extendidas

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 qué 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) aquéllas 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.

El formato del comando es:

Router(config)#**interface eth0**

```
Router(config-if)#ip access-group 107 in
Router(config-if)#exit
Router(config)#
```

28.6 Ubicación de las ACL

Las ACL se utilizan para controlar el tráfico, filtrando paquetes y eliminando el tráfico no deseado de la red. Otra consideración importante a tener en cuenta al implementar la ACL es dónde se ubica la lista de acceso. Si las ACL se colocan en el lugar correcto, no sólo es posible filtrar el tráfico sino también toda la red se hace más eficiente. Si se tiene que filtrar el tráfico, la ACL se debe colocar en un lugar donde mejore la eficiencia de forma significativa.

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. Por ejemplo, una ACL estándar se debe colocar en Fa0/0 del Router D para evitar el tráfico desde el Router A.

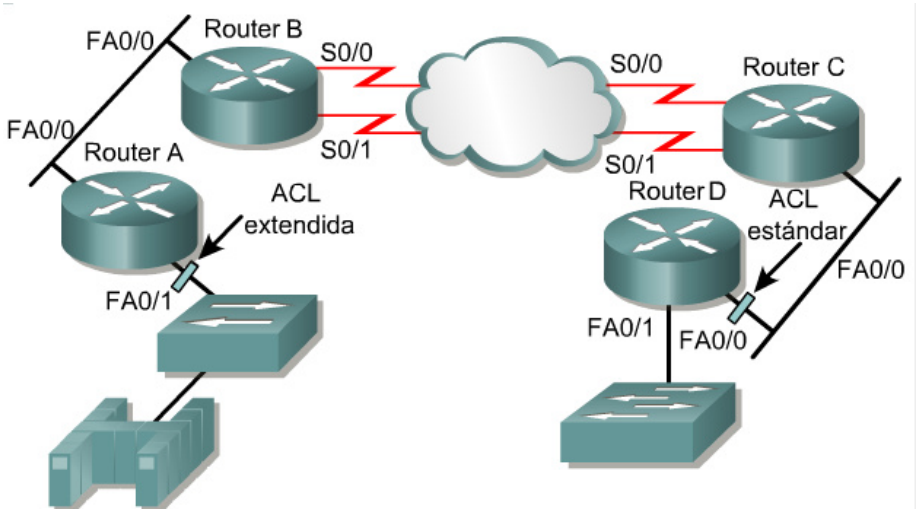


Gráfico 28-4: Ubicación de las ACL

29 Firewalls

Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos. En la mayoría de los casos, los intrusos provienen de la Internet mundial y de las miles de redes remotas que interconecta. Normalmente, un firewall de red se compone de varias máquinas diferentes que funcionan al mismo tiempo para impedir el acceso no deseado e ilegal.

Se deben utilizar ACL en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet. Esto permite el control del tráfico entrante o saliente de alguna parte específica de la red interna. El router firewall proporciona un punto de aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada.

Se necesita configurar las ACL en routers fronterizos, que son aquellos situados en las fronteras de la red, para brindar mayor seguridad. Esto proporciona protección básica contra la red externa u otra parte menos controlada de la red, en un área más privada de la red. En estos routers fronterizos, es posible crear ACLs para cada protocolo de red configurado en las interfaces del router.

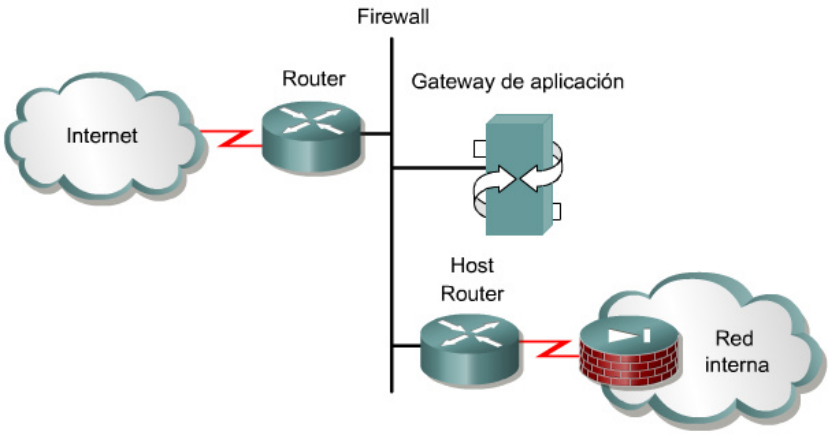


Gráfico 29-1: Firewalls

30 GRAFICO WAN

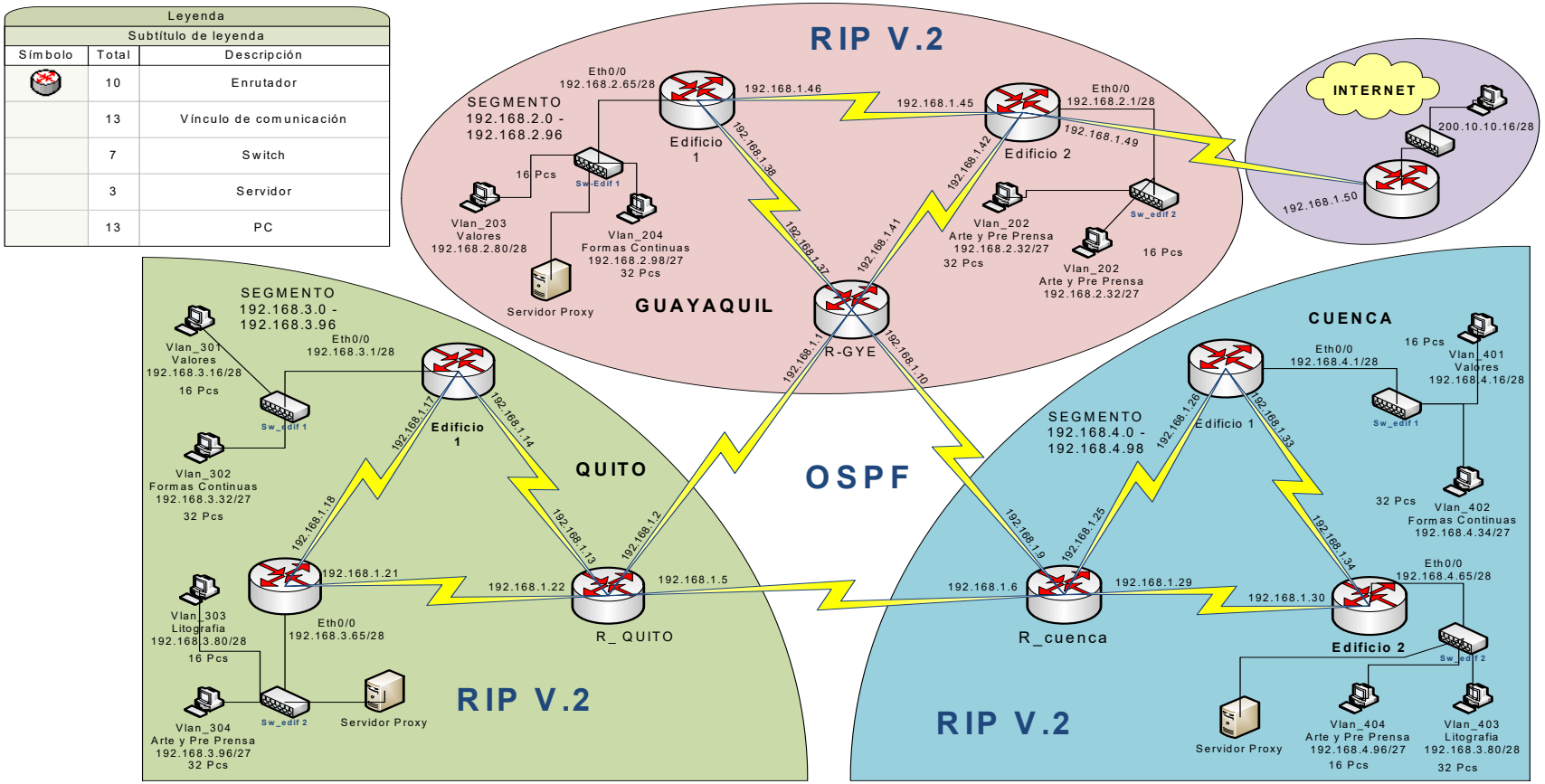


Gráfico 30-1: Grafico WAN

31 CONFIGURACION DE ROUTER

31.1 CONFIGURACIÓN DEL ROUTER GUAYAQUIL

31.1.1 Acceso al modo de Configuración principal.

Router>enable →*Ingresa al modo EXEC privilegiado*
Router#configure terminal →*Configura la terminal manualmente desde la terminal de consola*
Router(config)# exit → *Estando en el modo de configuración global o cualquiera de sus submodos regresa al modo anterior. Estando en los modos EXEC Usuario o EXEC Privilegiado, cierra la sesión*
Router#

31.1.2 Configuración de los nombres del Router

Router>enable
Router#configure terminal
Router(config)#hostname *GUAYAQUIL* → *Modifica el nombre del router.*
GUAYAQUIL(config)#

31.1.3 Creación de Contraseñas

GUAYAQUIL #enable
GUAYAQUIL #configure terminal
GUAYAQUIL**(config)#**
GUAYAQUIL **(config)#**line console 0 → *Identifica una línea específica para la configuración e inicia el modo de reunión de comandos de configuración.*
GUAYAQUIL **(config-line)#**password cisco → *Asigna la contraseña a ser solicitada en el momento de la conexión*
GUAYAQUIL **(config-line)#l**ogin → *Habilita la verificación de contraseña en el momento de la conexión.*
GUAYAQUIL **(config-line)#**exit
GUAYAQUIL **(config)#**line vty 0 4 → *indica la interfaz telnet, 0 el número de la interfaz y 4 la cantidad máxima de conexiones múltiples a partir de 0, en este caso se permiten 5 conexiones múltiples.*
GUAYAQUIL **(config-line)#**password cisco
GUAYAQUIL **(config-line)#**login
GUAYAQUIL **(config)#**enable password cisco → *Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio.*
GUAYAQUIL **(config-line)#***exit*

31.2 CONFIGURACIÓN DE LAS INTERFACES.

Para configurar una dirección IP a una interfaz de red, sea serial o fastEthernet, se debe pasar del modo de configuración global a un modo especifico que es el de interfaz, éste se reconoce porque el prompt visualiza lo siguiente **(config- if)**.

El comando que le permite asignar una dirección IP es **"ip address <dirIP> <mask>"**. Cuando esta configurando una interfaz tiene que tener en cuenta que las interfaces en los routers por defecto vienen administrativamente abajo **(vienen en un status shutdown)**; como administradores de la red y de la configuración del router es usted el responsable de subir la interfaz **(comando "no shutdown")**.

Las interfaces vienen por lo general según el modelo de Router, según el que estemos utilizando o el que necesitemos. El Router que vamos a utilizar en el QUEVEDO tiene 2 seriales y una FastEthernet, a continuación veremos la configuración de las mismas.

31.2.1 CONFIGURACIÓN DE LA INTERFAZ SERIAL 1/0

GUAYAQUIL **(config)#**interface serial 1/0 → *Configura un tipo de interfaz y entra al modo de configuración de interfaz.*
GUAYAQUIL **(config-if)#**ip address 192.168.1.37 255.255.255.252 → *Asigna una dirección y una máscara de subred e inicia el procesamiento IP en una interfaz.*
GUAYAQUIL **(config-if)#**clock rate 64000 → *Configura la velocidad de reloj para las conexiones de hardware en interfaces seriales, como módulos de interfaz de red y procesadores de interfaz a una velocidad de bits aceptable.*
GUAYAQUIL **(config-if)#**no shutdown → *Reinicia una interfaz desactivada*
GUAYAQUIL **(config-if)#**exit

31.2.2 CONFIGURACIÓN DE LA INTERFAZ SERIAL 1/1

GUAYAQUIL **(config)#**interface serial 1/1

GUAYAQUIL **(config-if)#**ip address 192.168.1.1 255.255.255.252

GUAYAQUIL **(config-if)#**clock rate 64000

GUAYAQUIL **(config-if)#**no shutdown

GUAYAQUIL **(config-if)#**exit *interfaz*

31.2.3 CONFIGURACIÓN DE LA INTERFAZ SERIAL 1/2

GUAYAQUIL **(config)#**interface serial 1/2

GUAYAQUIL **(config-if)#**ip address 192.168.1.41 255.255.255.252

GUAYAQUIL **(config-if)#**clock rate 64000

GUAYAQUIL **(config-if)#**no shutdown

***GUAYAQUIL* (config-if)#**exit

31.2.4 CONFIGURACIÓN DE LA INTERFAZ SERIAL 1/3

***GUAYAQUIL* (config)#**interface serial 1/3

***GUAYAQUIL* (config-if)#**ip address 192.168.1.10 255.255.255.252

***GUAYAQUIL* (config-if)#**no shutdown

***GUAYAQUIL* (config-if)#**exit

31.3 CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO RIPV2

El Protocolo de enrutamiento RIP de habilitarse antes de llevar a cabo cualquiera de los comandos, lo habilitamos utilizando el comando:

***GUAYAQUIL* (config)#**router rip → *Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. En este caso RIP*
***GUAYAQUIL* (config-router)#**version 2 → *Versión del protocolo de enrutamiento*
***GUAYAQUIL* (config-router)#**network 192.168.1.36 → *Redes que operaran dentro del protocolo RIP V2.*

Para deshabilitar el Protocolo de enrutamiento RIP se utilizar el comando "**no router rip".**

***GUAYAQUIL* #**configure terminal
***GUAYAQUIL* (config)#**no router rip → *elimina el protocolo aplicado*
***GUAYAQUIL* (config)#**

RIP puede configurarse para procesar paquetes de Versión 1 o Versión 2, el modo predefinido es Versión 1. Si ninguna versión se especifica, entonces RIP tendrá como valor predefinido la Versión 1. Si RIP se pone a Versión 2, la configuración de "Versión 2" se desplegará, pero la configuración de "Versión 1" no se desplegará mientras no se especifique que se utiliza Versión 1.

Para nuestro caso de estudio utilizaremos la versión que es la más utilizada.

***GUAYAQUIL* #**configure terminal
***GUAYAQUIL* (config)#**router rip
***GUAYAQUIL* (config-router)#**version 2
***GUAYAQUIL* (config-router)#**network 192.168.1.36

***GUAYAQUIL* (config-router)#**network 192.168.1.40
***GUAYAQUIL* (config-router)#**redistribute ospf 1 metric 1 → *Redistribuir redes Rip a OSPF*
***GUAYAQUIL* (config-router)#**exit → *Salir de configuración actual*
***GUAYAQUIL* (config)# exit** → *Salir de Configuración Global*
***GUAYAQUIL* # Wr** → *Guarda la configuración actual al Archivo de Inicio.*

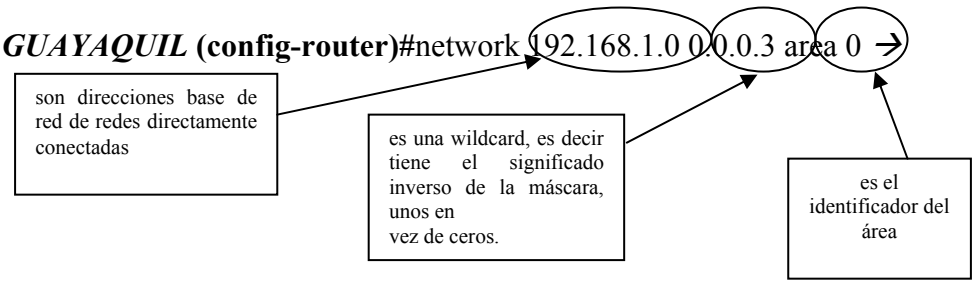
En la configuración luego de habilitar **RIP** y poner la versión, configuramos las redes a las que se podrá comunicar **RIP** con el comando "**network",** luego salimos con el comando **"exit".**

31.4 CONFIGURACIÓN DE PROTOCOLO OSPF

A continuación detallaremos el proceso de configuración del protocolo OSPF en la sucursal Guayaquil.

***GUAYAQUIL* (config)#**router ospf 1 → *Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. En este caso OSPF1*

***GUAYAQUIL* (config-router)#**network 192.168.1.0 0.0.0.3 area 0 →



***GUAYAQUIL* (config)#**redistribute rip subnets → *Redistribuyendo Redes OSPF hacia RIP*
***GUAYAQUIL* (config)#**exit

En la configuración luego de habilitar **OSPF**, configuramos las redes a las que se podrá comunicar **OSPF** con el comando "**network",** luego salimos con el comando **"exit".**

31.5 GUARDAR CONFIGURACIÓN

Para guardar los cambios que vaya realizando en el router utilice el siguiente comando:

***GUAYAQUIL* #**copy running-config startup-config

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 tenia se recuperará de la memoria **NVRAM (startup-config).**

31.6 SHOW RUNNING-CONFIG DEL ROUTER GUAYAQUIL

GUAYAQUIL#Show Running-config → *Muestra el contenido del archivo de configuración activo*

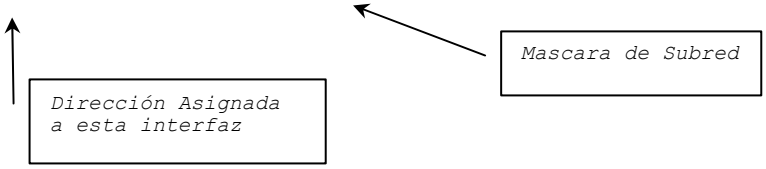
Building configuration...

Current configuration : 1345 bytes → *Tamaño en Bytes del archivo de configuración del router*
!
version 12.4 → *muestra la Version del IOS*
no service password-encryption→*Indica que no esta habilitado la encriptación del password.*
!
hostname GUAYAQUIL → *Nombre del Router*

!
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0 → *Clave encriptada*
enable password cisco → *Clave del Router*

!
ip ssh version 1→*Indica que se está utilizando el protocolo seguro ssh v. 1*
!
interface FastEthernet0/0 → *Puerto Ethernet del router*
 no ip address →*Esta interface no tiene asignado ninguna dirección ip*
 duplex auto → *Modo duplex automático*
 speed auto → *Velocidad de transferencia automática*
 shutdown → *La interfaz FastEthernet no está activada*
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0 → *ingresa al Submodo de Configuración de Interfaz*

ip address 192.168.1.37 255.255.255.252



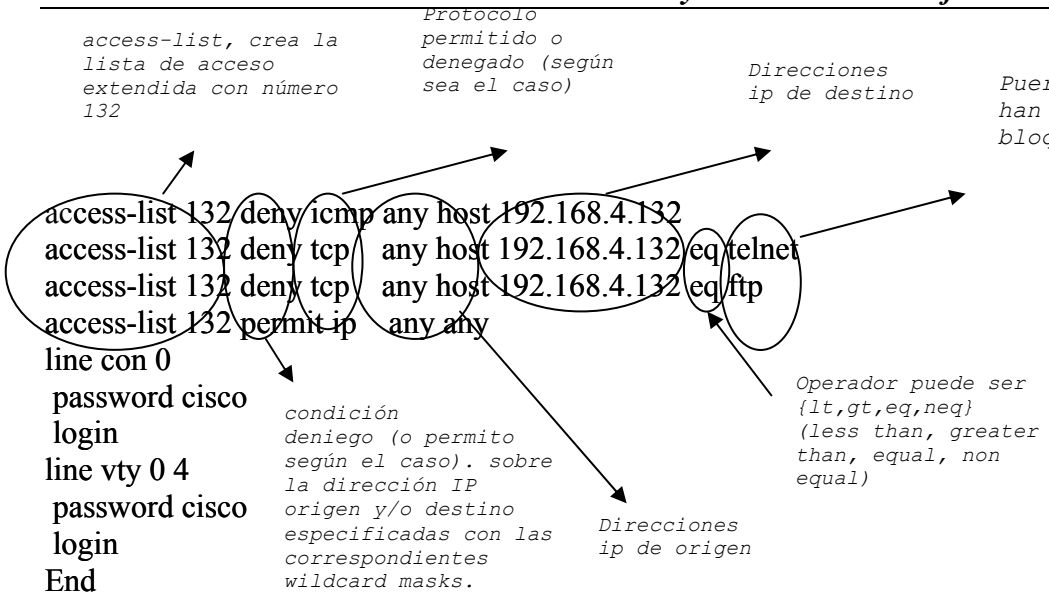
clock rate 64000 → *Velocidad de Reloj asignada a esta interfaz.*
!
interface Serial1/1

ip address 192.168.1.1 255.255.255.252
!
interface Serial1/2
ip access-group 132 out → *asigna la lista de acceso 132 sobre el protocolo IP sobre la interfaz de entrada o de salida donde se ejecuta dicho comando.*

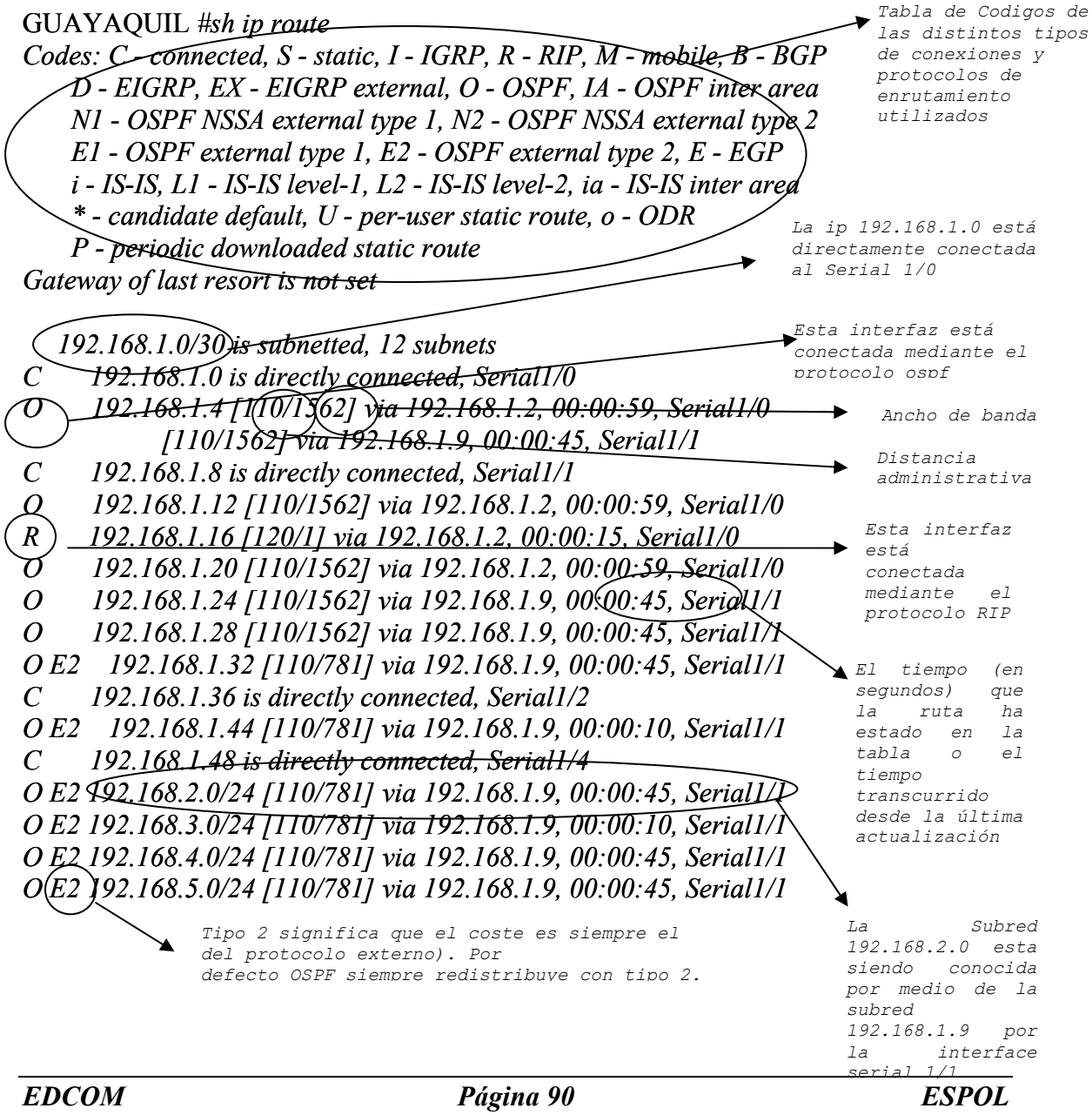
ip address 192.168.1.41 255.255.255.252
clock rate 64000
!
interface Serial1/3
ip address 192.168.1.10 255.255.255.252
clock rate 64000
!
interface Vlan1
no ip address → *La ip de esta interface no tiene asignada una ip.*
shutdown
!

router ospf 1
log-adjacency-changes → *los mensajes serán enviados a la consola y almacenados en un archivo log.*
redistribute rip subnets → *Redistribuir redes OSPF1 a Rip*
network 192.168.1.0 0.0.0.3 area 0
!
router rip
version 2
redistribute ospf 1 metric 1
network 192.168.1.0

!
ip classless → *Este commando se refiere al tratamiento de la tabla de enrutamiento es decir de como la tabla escoge la mejor ruta para un paquete de destino.*



31.7 SHOW IP ROUTE DEL ROUTER GUAYAQUIL



32 CONFIGURACIÓN DEL ROUTER GUAYAQUIL EDIFICIO 1

32.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

32.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER GUAYAQUIL EDIFICIO 1

Router>enable
Router#configure terminal
Router(config)#hostname Guayaquil_E1
Guayaquil_E1 (config)#

32.3 CREACIÓN DE CONTRASEÑAS

Router>enable
Guayaquil_E1 #enable
Guayaquil_E1 #configure terminal
Guayaquil_E1 (config)#
Guayaquil_E1 (config)#line console 0
Guayaquil_E1 (config-line)#password cisco
Guayaquil_E1 (config-line)#login
Guayaquil_E1 (config-line)#exit
Guayaquil_E1 (config)#line vty 0 4
Guayaquil_E1 (config-line)#password cisco
Guayaquil_E1 (config-line)#login
Guayaquil_E1 (config)#enable password cisco
Guayaquil_E1 (config-line)#exit

32.4 CONFIGURACIÓN DE LAS INTERFACES.

32.4.1 CONFIGURANDO LA INTERFAZ SERIAL 1/0

Guayaquil_E1 (config)#interface serial 1/0
Guayaquil_E1 (config-if)#ip address 192.168.1.38 255.255.255.252
Guayaquil_E1 (config-if)#no shutdown
Guayaquil_E1 (config-if)#exit

32.4.2 CONFIGURANDO LA INTERFAZ SERIAL 1/1

Guayaquil_E1 (config)#interface serial 1/1
Guayaquil_E1 (config-if)#ip address 192.168.1.46 255.255.255.252
Guayaquil_E1 (config-if)#clock rate 64000
Guayaquil_E1 (config-if)#no shutdown
Guayaquil_E1 (config-if)#exit

32.4.3 CONFIGURANDO LA INTERFAZ FASTETHERNET

Guayaquil_E1 (config)#interface FastEthernet 0/0
Guayaquil_E1 (config-if)#ip address 192.168.2.65 255.255.255.240
Guayaquil_E1 (config-if)#no shutdown
Guayaquil_E1 (config-if)#exit

32.5 CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO RIPV2

El Protocolo de enrutamiento debe habilitarse antes de llevar a cabo cualquiera de los comandos, lo habilitamos utilizando el comando:

Guayaquil_E1 (config)#router rip
Guayaquil_E1 (config-router)# version 2
Guayaquil_E1 (config-router)# network 192.168.1.36
Guayaquil_E1 (config-router)# network 192.168.1.44
Guayaquil_E1 (config-router)# network 192.168.2.64
Guayaquil_E1 (config-router)#exit
Guayaquil_E1 (config) #exit
Guayaquil_E1#wr

32.6 SHOW RUNNING-CONFIG ROUTER GUAYAQUIL EDIFICIO 1

Guayaquil_E1#Show running-config
Building configuration...

Current configuration : 1095 bytes
!
version 12.4
no service password-encryption
!
hostname Guayaquil_E1
!
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!

```
!
!
!
ip ssh version 1
!
interface FastEthernet0/0
 ip address 192.168.2.65 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/0.2 → modo de configuración del subinterfaz 2
 encapsulation dot1Q 204 → Se está empleando el encapsulado 802.1Q
 ip address 192.168.2.81 255.255.255.240→Dirección ip y Mascara asignada a esta subinterfaz.
ip access-group 141 in
!
interface FastEthernet0/0.3
 encapsulation dot1Q 205
 ip address 192.168.2.97 255.255.255.224
ip access-group 142 in
!
interface FastEthernet0/0.4
 encapsulation dot1Q 206
ip address 192.168.2.131 255.255.255.240
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown


!
interface Serial1/0
 ip address 192.168.1.38 255.255.255.252
!
interface Serial1/1
 ip address 192.168.1.46 255.255.255.252
 clock rate 64000
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```

```
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
!
ip classless
!
access-list 141 deny icmp host 192.168.2.82 host 192.168.2.132
access-list 141 deny tcp host 192.168.2.82 host 192.168.2.132 eq telnet
access-list 141 deny tcp host 192.168.2.82 host 192.168.2.132 eq ftp
access-list 141 permit ip any any
access-list 142 deny icmp host 192.168.2.98 host 192.168.2.132
access-list 142 deny tcp host 192.168.2.98 host 192.168.2.132 eq telnet
access-list 142 deny tcp host 192.168.2.98 host 192.168.2.132 eq ftp
access-list 142 permit ip any any
no cdp run
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
!
End
```

32.7 SHOW IP ROUTE ROUTER GUAYAQUIL EDIFICIO 1

```
Guayaquil_E1#Show Ip Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 10 subnets
R       192.168.1.0 [120/1] via 192.168.1.37, 00:00:24, Serial1/0
R       192.168.1.4 [120/2] via 192.168.1.37, 00:00:24, Serial1/0
R       192.168.1.8 [120/1] via 192.168.1.37, 00:00:24, Serial1/0
R       192.168.1.12 [120/2] via 192.168.1.37, 00:00:24, Serial1/0
R       192.168.1.16 [120/3] via 192.168.1.37, 00:00:24, Serial1/0
R       192.168.1.28 [120/2] via 192.168.1.37, 00:00:24, Serial1/0
R       192.168.1.32 [120/3] via 192.168.1.37, 00:00:24, Serial1/0
C       192.168.1.36 is directly connected, Serial1/0
C       192.168.1.44 is directly connected, Serial1/1
```

```
R       192.168.1.48 [120/1] via 192.168.1.45, 00:00:10, Serial1/1
    192.168.2.0/24 is variably subnetted, 4 subnets, 3 masks
R       192.168.2.0/24 [120/1] via 192.168.1.45, 00:00:10, Serial1/1
C       192.168.2.64/28 is directly connected, FastEthernet0/0
C       192.168.2.80/28 is directly connected, FastEthernet0/0.2
C       192.168.2.96/27 is directly connected, FastEthernet0/0.3
R    192.168.3.0/24 [120/3] via 192.168.1.37, 00:00:24, Serial1/0
R    192.168.4.0/24 [120/3] via 192.168.1.37, 00:00:24, Serial1/0
R    200.10.10.0/24 [120/2] via 192.168.1.45, 00:00:10, Serial1/1
```

33 CONFIGURACIÓN DEL ROUTER GUAYAQUIL EDIFICIO 2

33.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

33.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER GUAYAQUIL EDIFICIO 2

Router>enable
Router#configure terminal
Router(config)#hostname Guayaquil_E2
Guayaquil_E2(config)#

33.3 CREACIÓN DE CONTRASEÑAS

Router>enable
Guayaquil_E2#enable
Guayaquil_E2 #configure terminal
Guayaquil_E2 (config)#
Guayaquil_E2 (config)#line console 0
Guayaquil_E2 (config-line)#password cisco
Guayaquil_E2 (config-line)#login
Guayaquil_E2 (config-line)#exit
Guayaquil_E2 (config)#line vty 0 4
Guayaquil_E2 (config-line)#password cisco
Guayaquil_E2 (config-line)#login
Guayaquil_E2 (config)#enable password cisco
Guayaquil_E2 (config-line)#exit

33.4 CONFIGURACIÓN DE LAS INTERFACES.

33.4.1 CONFIGURANDO LA INTERFAZ SERIAL 1/0

Guayaquil_E2 (config)#interface serial 1/0
Guayaquil_E2 (config-if)#ip address 192.168.1.45 255.255.255.252
Guayaquil_E2 (config-if)#no shutdown
Guayaquil_E2 (config-if)#exit

33.4.2 CONFIGURANDO LA INTERFAZ SERIAL 1/1

Guayaquil_E2 (config)#interface serial 1/1
Guayaquil_E2 (config-if)#ip address 192.168.1.42 255.255.255.252
Guayaquil_E2 (config-if)#no shutdown
Guayaquil_E2 (config-if)#exit

33.4.3 CONFIGURANDO LA INTERFAZ SERIAL 1/2

Guayaquil_E2 (config)#interface serial 1/2
Guayaquil_E2 (config-if)#ip address 192.168.1.49 255.255.255.252
Guayaquil_E2 (config-if)#clock rate 64000
Guayaquil_E2 (config-if)#no shutdown
Guayaquil_E2 (config-if)#exit

33.4.4 CONFIGURANDO LA INTERFAZ FASTETHERNET

Guayaquil_E2 (config)#interface FastEthernet 0/0
Guayaquil_E2 (config-if)#ip address 192.168.2.1 255.255.255.240
Guayaquil_E2 (config-if)#no shutdown
Guayaquil_E2 (config-if)#exit

33.5 CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO RIPV2

El Protocolo de enrutamiento debe habilitarse antes de llevar a cabo cualquiera de los comandos, lo habilitamos utilizando el comando:

Guayaquil_E2 (config)#router rip
Guayaquil_E2 (config-router)# version 2
Guayaquil_E2 (config-router)# network 192.168.1.44
Guayaquil_E2 (config-router)# network 192.168.1.40
Guayaquil_E2 (config-router)# network 192.168.1.48
Guayaquil_E2 (config-router)# network 192.168.2.0

Guayaquil_E2 (config-router)#exit
Guayaquil_E2 (config) #exit
Guayaquil_E2#wr

33.6 SHOW RUNNING-CONFIG ROUTER GUAYAQUIL EDIFICIO 2

```
Guayaquil_E2#Show Running-config
Building configuration...

Current configuration : 1234 bytes
!
version 12.4
no service password-encryption


!
hostname Guayaquil_E2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!

ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 201
 ip address 192.168.2.17 255.255.255.240
!
interface FastEthernet0/0.3
 encapsulation dot1Q 202
 ip address 192.168.2.33 255.255.255.224
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 192.168.1.45 255.255.255.252
ip access-group 131 out
!
interface Serial1/1
```

```
 ip address 192.168.1.42 255.255.255.252
!
interface Serial1/2
 ip address 192.168.1.49 255.255.255.252
 clock rate 64000
!
interface Serial1/3
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown


!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
!
ip classless
access-list 131 deny icmp any host 192.168.2.132
access-list 131 deny tcp any host 192.168.2.132 eq telnet
access-list 131 deny tcp any host 192.168.2.132 eq ftp
access-list 131 permit ip any any
!
no cdp run
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
!
end
```

33.7 SHOW IP ROUTE ROUTER GUAYAQUIL EDIFICIO 2

```
Guayaquil_E2#Show Ip Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```
     192.168.1.0/30 is subnetted, 10 subnets
R       192.168.1.0 [120/2] via 192.168.1.46, 00:00:00, Serial1/0
R       192.168.1.4 [120/3] via 192.168.1.46, 00:00:00, Serial1/0
R       192.168.1.8 [120/2] via 192.168.1.46, 00:00:00, Serial1/0
R       192.168.1.12 [120/3] via 192.168.1.46, 00:00:00, Serial1/0
R       192.168.1.16 [120/4] via 192.168.1.46, 00:00:00, Serial1/0
R       192.168.1.28 [120/3] via 192.168.1.46, 00:00:00, Serial1/0
R       192.168.1.32 [120/4] via 192.168.1.46, 00:00:00, Serial1/0
R       192.168.1.36 [120/1] via 192.168.1.46, 00:00:00, Serial1/0
C       192.168.1.44 is directly connected, Serial1/0
C       192.168.1.48 is directly connected, Serial1/2
     192.168.2.0/24 is variably subnetted, 4 subnets, 3 masks
R       192.168.2.0/24 [120/1] via 192.168.1.46, 00:00:00, Serial1/0
C       192.168.2.0/28 is directly connected, FastEthernet0/0
C       192.168.2.16/28 is directly connected, FastEthernet0/0.2
C       192.168.2.32/27 is directly connected, FastEthernet0/0.3
R    192.168.3.0/24 [120/4] via 192.168.1.46, 00:00:00, Serial1/0
R    192.168.4.0/24 [120/4] via 192.168.1.46, 00:00:00, Serial1/0
R    200.10.10.0/24 [120/1] via 192.168.1.50, 00:00:23, Serial1/2
```

34 CONFIGURACIÓN DEL ROUTER ISP

34.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

34.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER ISP

Router>enable
Router#configure terminal
Router(config)#hostname Guayaquil_E2
***ISP* (config)#**

34.3 CREACIÓN DE CONTRASEÑAS

Router>enable
***ISP*#**enable
***ISP*#**configure terminal
***ISP*(config)#**
***ISP*(config)#**line console 0
***ISP*(config-line)#**password cisco
***ISP*(config-line)#l**ogin
***ISP*(config-line)#**exit

***ISP*(config)#**line vty 0 4
***ISP*(config-line)#**password cisco
***ISP*(config-line)#**login
***ISP*(config)#**enable password cisco
***ISP*(config-line)#**exit
ISP #configure terminal
ISP **(config)#**hostname ISP
***ISP*(config)#**

34.4 CONFIGURACIÓN DE LAS INTERFACES.

34.4.1 CONFIGURACIÓN DE LA INTERFAZ SERIAL 1/0

***ISP*(config)#**interface serial 1/0
***ISP*(config-if)#**ip address 192.168.1.50 255.255.255.252
***ISP*(config-if)#**no shutdown
***ISP*(config-if)#**exit

34.4.2 CONFIGURACIÓN DE LA INTERFAZ FASTETHERNET

***SP*(config)#**interface FastEthernet 0/0
***ISP*(config-if)#**ip address 200.10.10.1 255.255.255.240
***ISP*(config-if)#**no shutdown
***ISP*(config-if)#**exit

34.5 CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO RIPV2

El Protocolo de enrutamiento debe habilitarse antes de llevar a cabo cualquiera de los comandos, lo habilitamos utilizando el comando:

ISP (config)#router rip
ISP (config-router)# version 2
ISP (config-router)# network 192.168.1.48
ISP (config-router)# network 200.10.10.0
ISP (config-router)#exit
ISP (config)#wr

34.6 SHOW RUNNING-CONFIG DEL ROUTER ISP

ISP#Show Running-config
Building configuration...

Current configuration : 1108 bytes
!

```
version 12.4
no service password-encryption
!
hostname ISP


!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 200.10.10.1 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 501
 ip address 200.10.10.17 255.255.255.240
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 192.168.1.50 255.255.255.252
ip access-group 130 out
!
interface Serial1/1
 no ip address
 shutdown
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.1.0
```

```
 network 200.10.10.0


!
ip classless
access-list 130 deny icmp host 200.10.10.18 host 192.168.4.132
access-list 130 deny tcp host 200.10.10.18 host 192.168.4.132 eq telnet
access-list 130 deny tcp host 200.10.10.18 host 192.168.4.132 eq ftp
access-list 130 permit ip any any
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
!
end
```

34.7 SHOW IP ROUTE DEL ROUTER ISP

```
ISP#Show Ip Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 10 subnets
R       192.168.1.0 [120/3] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.4 [120/4] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.8 [120/3] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.12 [120/4] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.16 [120/5] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.28 [120/4] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.32 [120/5] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.36 [120/2] via 192.168.1.49, 00:00:21, Serial1/0
R       192.168.1.44 [120/1] via 192.168.1.49, 00:00:21, Serial1/0
C       192.168.1.48 is directly connected, Serial1/0
R    192.168.2.0/24 [120/1] via 192.168.1.49, 00:00:21, Serial1/0
R    192.168.3.0/24 [120/5] via 192.168.1.49, 00:00:21, Serial1/0
R    192.168.4.0/24 [120/5] via 192.168.1.49, 00:00:21, Serial1/0
     200.10.10.0/28 is subnetted, 2 subnets
```

C 200.10.10.0 is directly connected, FastEthernet0/0
C 200.10.10.16 is directly connected, FastEthernet0/0.2

35 CONFIGURACIÓN DEL ROUTER QUITO

35.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

35.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER QUITO

Router>enable
Router> configure terminal
Router(config)#hostname *Quito*
***Quito*(config)#**

35.3 CREACIÓN DE CONTRASEÑAS

Quito#enable
Quito #configure Terminal
Quito (config)#
Quito (config)#line console 0
Quito (config-line)#password cisco
Quito (config-line)#login
Quito (config-line)#exit
Quito (config)#line vty 0 4
Quito (config-line)#password cisco
Quito (config-line)#login
Quito (config-line)#exit
Quito (config)#
Quito (config)#enable password cisco
Quito (config)#enable secret cisco

35.4 CONFIGURACIÓN DE LAS INTERFACES.

35.4.1 CONFIGURACION DE LA INTERFAZ SERIAL 1/0

Quito(config)#interface serial 1/0
Quito(config-if)#ip address 192.168.1.5 255.255.255.252
Quito (config-if)#exit
Quito (config-if)#clock rate 64000
Quito (config-if)#no shutdown

35.4.2 CONFIGURACION DE LA INTERFAZ SERIAL 1/1

Quito (config)#interface serial 1/1
Quito (config-if)#ip address 192.168.1.2 255.255.255.252
Quito (config-if)#no shutdown
Quito (config-if)#exit

35.4.3 CONFIGURACION DE LA INTERFAZ SERIAL 1/2

Quito (config)#interface serial 1/2
Quito (config-if)#ip address 192.168.1.13 255.255.255.252
Quito (config-if)#clock rate 64000
Quito (config-if)#no shutdown
Quito(config-if)#exit

35.4.4 CONFIGURACION DE LA INTERFAZ SERIAL 1/3

Quito (config)#interface serial 1/3
Quito (config-if)#ip address 192.168.1.22 255.255.255.252
Quito (config-if)#clock rate 64000
Quito (config-if)#no shutdown
Quito (config-if)#exit

35.5 CONFIGURACIÓN DE PROTOCOLO RIPV2

El Protocolo de enrutamiento RIP de habilitarse antes de llevar a cabo cualquiera de los comandos, lo habilitamos utilizando el comando:

Quito #configure terminal
Quito (config)# exit
Quito # wr
Quito (config)#router rip
Quito (config-router)#network 192.168.1

En la configuración luego de habilitar **RIP** y poner la versión, configuramos las redes a las que se podrá comunicar **RIP** con el comando "**network",** luego salimos con el comando **"exit".**

Quito#configure terminal
Quito(config)#router rip
Quito(config-router)#version 2
Quito(config-router)#network 192.168.1.12
Quito(config-router)#network 192.168.1.20
Quito(config-router)#redistribute ospf 1 metric 1
Quito(config-router)#exit
Quito(config)# exit
Quito# Wr

35.6 CONFIGURACIÓN DE PROTOCOLO OSPF

A continuación detallaremos el proceso de configuración del protocolo OSPF en la sucursal Quito.

Quito (config)#router ospf 1
Quito (config-router)# network 192.168.1.4 0. 0. 0.3 area 0
Quito(config-router)#*redistribute* rip subnets
Quito((config-router)# exit
Quito(config)# exit
Quito# Wr

35.7 SHOW RUNNING-CONFIG SUCURSAL QUITO

Quito*>enable*
Quito*#Show run*

Building configuration...

Current configuration : 2355 bytes
!
version 12.4
!
hostname Quito
!
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
ip ssh version 1

!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown

```
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 192.168.1.2 255.255.255.252
ip access-group 102 out

!
interface Serial1/1
ip address 192.168.1.5 255.255.255.252
ip access-group 101 out
clock rate 64000
!
interface Serial1/2

ip address 192.168.1.13 255.255.255.252
ip access-group 135 in
clock rate 64000
!
interface Serial1/3

 ip address 192.168.1.22 255.255.255.252
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
redistribute rip subnets
 network 192.168.1.4 0.0.0.3 area 0
!
router rip
 version 2
 redistribute ospf 1  metric 1
 network 192.168.1.0


!
ip classless
!
access-list 101 deny icmp any host 192.168.1.1
access-list 101 deny icmp any host 192.168.1.10
access-list 101 deny icmp any host 192.168.1.37
access-list 101 deny icmp any host 192.168.1.41
access-list 101 deny tcp any host 192.168.1.1 eq telnet
```

```
access-list 101 deny tcp any host 192.168.1.10 eq telnet
access-list 101 deny tcp any host 192.168.1.37 eq telnet
access-list 101 deny tcp any host 192.168.1.41 eq telnet
access-list 101 deny tcp any host 192.168.1.1 eq ftp
access-list 101 deny tcp any host 192.168.1.10 eq ftp
access-list 101 deny tcp any host 192.168.1.37 eq ftp
access-list 101 deny tcp any host 192.168.1.41 eq ftp
access-list 101 permit ip any any
access-list 102 deny icmp any host 192.168.2.132
access-list 102 deny tcp any host 192.168.2.132 eq telnet
access-list 102 deny tcp any host 192.168.2.132 eq ftp
access-list 102 permit ip any any
access-list 135 deny icmp host 192.168.3.18 host 192.168.4.132
access-list 135 deny icmp host 192.168.3.34 host 192.168.4.132
access-list 135 deny tcp host 192.168.3.18 host 192.168.4.132 eq telnet
access-list 135 deny tcp host 192.168.3.34 host 192.168.4.132 eq telnet
access-list 135 deny tcp host 192.168.3.18 host 192.168.4.132 eq ftp
access-list 135 deny tcp host 192.168.3.34 host 192.168.4.132 eq ftp
access-list 135 permit ip any any
!
no cdp run
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
End
```

35.8 SHOW IP ROUTE SUCURSAL QUITO

```
Quito#Show Ip Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 10 subnets
C       192.168.1.4 is directly connected, Serial1/0
C       192.168.1.12 is directly connected, Serial1/2
C       192.168.1.20 is directly connected, Serial1/3
R       192.168.1.24 [120/3] via 192.168.1.6, 00:00:11, Serial1/0
R       192.168.1.28 [120/3] via 192.168.1.6, 00:00:11, Serial1/0
O E2    192.168.1.32 [110/781] via 192.168.1.6, 00:46:10, Serial1/0
```

O E2 192.168.1.36 [110/781] via 192.168.1.6, 00:53:32, Serial1/0
O E2 192.168.1.40 [110/781] via 192.168.1.6, 00:53:32, Serial1/0
R 192.168.1.44 [120/1] via 192.168.1.6, 00:02:44, Serial1/0
[120/1] via 192.168.1.14, 00:02:44, Serial1/2
[120/1] via 192.168.1.21, 00:02:44, Serial1/3
R 192.168.1.48 [120/1] via 192.168.1.6, 00:02:44, Serial1/0
[120/1] via 192.168.1.14, 00:00:10, Serial1/2
R 192.168.2.0/24 [120/1] via 192.168.1.6, 00:02:44, Serial1/0

[120/1] via 192.168.1.21, 00:02:44, Serial1/3
[120/1] via 192.168.1.14, 00:02:44, Serial1/2
O E2 192.168.4.0/24 [110/781] via 192.168.1.6, 00:46:10, Serial1/0
R 200.10.10.0/24 [120/1] via 192.168.1.6, 00:01:31, Serial1/0
[120/1] via 192.168.1.21, 00:01:31, Serial1/3
[120/1] via 192.168.1.14, 00:01:31, Serial1/2

36 CONFIGURACIÓN DEL ROUTER QUITO EDIFICIO 1

36.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

36.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER QUITO EDIFICIO 1

Router>enable
Router#configure terminal
Router(config)#hostname QuitoEdificio1
QuitoEdificio1(config)#

36.3 CREACION DE CONTRASEÑAS

QuitoEdificio1#enable
QuitoEdificio1 #configure Terminal
QuitoEdificio1 (config)#
QuitoEdificio1 (config)#line console 0
QuitoEdificio1 (config-line)#password cisco
QuitoEdificio1 (config-line)#login
QuitoEdificio1 (config-line)#exit
QuitoEdificio1 (config)#line vty 0 4
QuitoEdificio1 (config-line)#password cisco
QuitoEdificio1 (config-line)#login
QuitoEdificio1 (config-line)#exit
QuitoEdificio1 (config)#

QuitoEdificio1 (config)#enable password cisco

36.4 CONFIGURACIÓN DE LAS INTERFACES.

36.4.1 CONFIGURACION DE LA INTERFAZ SERIAL 1/0

QuitoEdificio1(config)#interface serial 1/0
QuitoEdificio1 (config-if)#ip address 192.168.1.14 255.255.255.252
QuitoEdificio1 (config-if)#no shutdown
QuitoEdificio1 (config-if)#exit

36.4.2 CONFIGURACION DE LA INTERFAZ SERIAL 1/1

QuitoEdificio1 (config)#interface serial 1/1
QuitoEdificio1 (config-if)#ip address 192.168.1.17 255.255.255.252
QuitoEdificio1 (config-if)#no shutdown
QuitoEdificio1 (config-if)#exit

36.4.3 CONFIGURACION DE LA INTERFAZ FASTETHERNET 0/0

QuitoEdificio1 (config)#interface FastEthernet 0/0
QuitoEdificio1 (config-if)#ip address 192.168.3.1 255.255.255.240
QuitoEdificio1(config-if)#no shutdown
QuitoEdificio1(config-if)#exit

36.5 CONFIGURACIÓN DE PROTOCOLO RIPV2

QuitoEdificio1#configure terminal
QuitoEdificio1 (config)#router rip
QuitoEdificio1 (config-router)#version 2
QuitoEdificio1 (config-router)#network 192.168.1.12
QuitoEdificio1 (config-router)#network 192.168.1.16
QuitoEdificio1 (config-router)#network 192.168.3.0
QuitoEdificio1 (config-router)#exit
QuitoEdificio1 (config)# exit
QuitoEdificio1#Wr

36.6 SHOW RUNNING-CONFIG ROUTER QUITO EDIFICIO 1

QuitoEdificio1#Show Running-config
Building configuration...

Current configuration : 1202 bytes
!

```
version 12.4
no service password-encryption
!
hostname QuitoEdificio1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
!
ip ssh version 1


!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 301
 ip address 192.168.3.17 255.255.255.240
!
interface FastEthernet0/0.3
 encapsulation dot1Q 302
 ip address 192.168.3.33 255.255.255.224
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 192.168.1.14 255.255.255.252
!
interface Serial1/1
ip address 192.168.1.17 255.255.255.252
ip access-group 115 out
!
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```

```
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.3.0
!



ip classless
access-list 115 deny icmp any host 192.168.4.132
access-list 115 deny tcp any host 192.168.4.132 eq telnet
access-list 115 deny tcp any host 192.168.4.132 eq ftp
access-list 115 permit ip any any
!
no cdp run
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
End
```

36.7 SHOW IP ROUTE ROUTER QUITO EDIFICIO 1

```
QuitoEdificio1#Show Ip Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 12 subnets
R       192.168.1.4 [120/1] via 192.168.1.13, 00:00:27, Serial1/0
R       192.168.1.8 [120/1] via 192.168.1.18, 00:02:00, Serial1/1
                    [120/1] via 192.168.1.13, 00:02:00, Serial1/0
C       192.168.1.12 is directly connected, Serial1/0
C       192.168.1.16 is directly connected, Serial1/1
R       192.168.1.20 [120/1] via 192.168.1.13, 00:02:15, Serial1/0
                     [120/1] via 192.168.1.18, 00:00:25, Serial1/1
R       192.168.1.24 [120/1] via 192.168.1.18, 00:02:00, Serial1/1
                     [120/1] via 192.168.1.13, 00:02:00, Serial1/0
R       192.168.1.28 [120/1] via 192.168.1.18, 00:02:00, Serial1/1
                     [120/1] via 192.168.1.13, 00:02:00, Serial1/0
R       192.168.1.32 [120/1] via 192.168.1.13, 00:02:00, Serial1/0
```

```
                [120/1] via 192.168.1.18, 00:02:00, Serial1/1
R       192.168.1.36 [120/1] via 192.168.1.18, 00:02:00, Serial1/1
                [120/1] via 192.168.1.13, 00:02:00, Serial1/0
R       192.168.1.40 [120/1] via 192.168.1.18, 00:02:00, Serial1/1
                [120/1] via 192.168.1.13, 00:02:00, Serial1/0
R       192.168.1.44 [120/1] via 192.168.1.18, 00:02:00, Serial1/1
                [120/1] via 192.168.1.13, 00:02:00, Serial1/0
R       192.168.1.48 [120/4] via 192.168.1.13, 00:02:15, Serial1/0
R    192.168.2.0/24 [120/4] via 192.168.1.13, 00:02:15, Serial1/0
     192.168.3.0/24 is variably subnetted, 4 subnets, 3 masks
R       192.168.3.0/24 [120/1] via 192.168.1.18, 00:00:25, Serial1/1
                [120/1] via 192.168.1.13, 00:01:22, Serial1/0
C       192.168.3.0/28 is directly connected, FastEthernet0/0
C       192.168.3.16/28 is directly connected, FastEthernet0/0.2
C       192.168.3.32/27 is directly connected, FastEthernet0/0.3
R    192.168.4.0/24 [120/1] via 192.168.1.18, 00:02:00, Serial1/1
                [120/1] via 192.168.1.13, 00:02:00, Serial1/0
R    200.10.10.0/24 [120/5] via 192.168.1.13, 00:02:15, Serial1/0
```

37 CONFIGURACIÓN DEL ROUTER QUITO EDIFICIO 2

37.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

37.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER QUITO EDIFICIO 2

Router>enable
Router#configure terminal
Router(config)#hostname QuitoEdificio2
QuitoEdificio2(config)#

37.3 CREACION DE CONTRASEÑAS

QuitoEdificio2#enable
QuitoEdificio2 #configure Terminal
QuitoEdificio2 (config)#
QuitoEdificio2 (config)#line console 0
QuitoEdificio2 (config-line)#password cisco
QuitoEdificio2 (config-line)#login
QuitoEdificio2 (config-line)#exit
QuitoEdificio2 (config)#line vty 0 4
QuitoEdificio2 (config-line)#password cisco
QuitoEdificio2 (config-line)#login

QuitoEdificio2 (config-line)#exit
QuitoEdificio2 (config)#
QuitoEdificio2 (config)#enable password cisco

37.4 CONFIGURACIÓN DE LAS INTERFACES.

37.4.1 CONFIGURACION DE LA INTERFAZ SERIAL 1/0

QuitoEdificio2(config)#interface serial 1/0
QuitoEdificio2 (config-if)#ip address 192.168.1.21 255.255.255.252
QuitoEdificio2 (config-if)#no shutdown
QuitoEdificio2 (config-if)#exit

37.4.2 CONFIGURACION DE LA INTERFAZ SERIAL 1/1

QuitoEdificio2 (config)#interface serial 1/1
QuitoEdificio2 (config-if)#ip address 192.168.1.18 255.255.255.252
QuitoEdificio2 (config-if)#clock rate 64000
QuitoEdificio2 (config-if)#no shutdown
QuitoEdificio2 (config-if)#exit

37.4.3 CONFIGURACION DE LA INTERFAZ FASTETHERNET 0/0

QuitoEdificio2 (config)#interface FastEthernet 0/0
QuitoEdificio2 (config-if)#ip address 192.168.3.65 255.255.255.240
QuitoEdificio2(config-if)#no shutdown
QuitoEdificio2(config-if)#exit

37.5 CONFIGURACIÓN DE PROTOCOLO RIPV2

QuitoEdificio2#configure terminal
QuitoEdificio2 (config)#router rip
QuitoEdificio2 (config-router)#version 2
QuitoEdificio2 (config-router)#network 192.168.1.16
QuitoEdificio2 (config-router)#network 192.168.1.20
QuitoEdificio2 (config-router)#network 192.168.3.64

QuitoEdificio2 (config-router)#exit
QuitoEdificio2(config)# exit
QuitoEdificio2#Wr

37.6 SHOW RUNNING-CONFIG ROUTER QUITO EDIFICIO 2

QuitoEdificio2#Show Running-config
Building configuration...
Current configuration : 2529 bytes
!
version 12.4
no service password-encryption

```
!
hostname QuitoEdificio2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
ip ssh version 1
!

interface FastEthernet0/0
 ip address 192.168.3.65 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 303
 ip address 192.168.3.81 255.255.255.240
ip access-group 137 in
!
interface FastEthernet0/0.3
 encapsulation dot1Q 304
 ip address 192.168.3.97 255.255.255.224
ip access-group 136 in
!
interface FastEthernet0/0.4
 encapsulation dot1Q 305
 ip address 192.168.3.131 255.255.255.240
 ip access-group 120 out
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
ip address 192.168.1.21 255.255.255.252
ip access-group 118 out
!
interface Serial1/1
ip address 192.168.1.18 255.255.255.252
ip access-group 119 in
 clock rate 64000
!
interface Serial1/2
 no ip address
 shutdown



!
```

```
interface Serial1/3
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.3.0
!
ip classless
!
access-list 118 deny icmp any host 192.168.2.132
access-list 118 deny tcp any host 192.168.2.132 eq telnet
access-list 118 deny tcp any host 192.168.2.132 eq ftp
access-list 118 permit ip any any
access-list 119 deny icmp any host 192.168.3.132
access-list 119 deny tcp any host 192.168.3.132 eq telnet
access-list 119 deny tcp any host 192.168.3.132 eq ftp
access-list 119 permit ip any any
access-list 120 deny icmp host 192.168.3.82 host 192.168.3.132
access-list 120 deny icmp host 192.168.3.98 host 192.168.3.132
access-list 120 deny tcp host 192.168.3.82 host 192.168.3.132 eq telnet
access-list 120 deny tcp host 192.168.3.98 host 192.168.3.132 eq telnet
access-list 120 deny tcp host 192.168.3.82 host 192.168.3.132 eq ftp
access-list 120 deny tcp host 192.168.3.98 host 192.168.3.132 eq ftp
access-list 120 permit ip any any
access-list 136 deny icmp host 192.168.3.98 host 192.168.4.132
access-list 136 deny tcp host 192.168.3.98 host 192.168.4.132 eq telnet
access-list 136 deny tcp host 192.168.3.98 host 192.168.4.132 eq ftp
access-list 136 permit ip any any
access-list 137 deny icmp host 192.168.3.82 host 192.168.4.132
access-list 137 deny tcp host 192.168.3.82 host 192.168.4.132 eq telnet
access-list 137 deny tcp host 192.168.3.82 host 192.168.4.132 eq ftp
access-list 137 permit ip any any
no cdp run
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
End
```

37.7 SHOW IP ROUTE ROUTER QUITO EDIFICIO 2

```
QuitoEdificio2#Show Ip Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 10 subnets
R       192.168.1.0 [120/2] via 192.168.1.17, 00:00:17, Serial1/1
R       192.168.1.4 [120/2] via 192.168.1.17, 00:00:17, Serial1/1
R       192.168.1.8 [120/3] via 192.168.1.17, 00:00:17, Serial1/1
R       192.168.1.12 [120/1] via 192.168.1.17, 00:00:17, Serial1/1
C       192.168.1.16 is directly connected, Serial1/1
R       192.168.1.28 [120/3] via 192.168.1.17, 00:00:17, Serial1/1
R       192.168.1.32 [120/4] via 192.168.1.17, 00:00:17, Serial1/1
R       192.168.1.36 [120/3] via 192.168.1.17, 00:00:17, Serial1/1
R       192.168.1.44 [120/4] via 192.168.1.17, 00:00:17, Serial1/1
R       192.168.1.48 [120/5] via 192.168.1.17, 00:00:17, Serial1/1
R    192.168.2.0/24 [120/4] via 192.168.1.17, 00:00:17, Serial1/1
     192.168.3.0/24 is variably subnetted, 4 subnets, 3 masks
R       192.168.3.0/24 [120/1] via 192.168.1.17, 00:00:17, Serial1/1
C       192.168.3.64/28 is directly connected, FastEthernet0/0
C       192.168.3.80/28 is directly connected, FastEthernet0/0.2
C       192.168.3.96/27 is directly connected, FastEthernet0/0.3
R    192.168.4.0/24 [120/4] via 192.168.1.17, 00:00:17, Serial1/1
R    200.10.10.0/24 [120/6] via 192.168.1.17, 00:00:17, Serial1/1
```

38 CONFIGURACIÓN DEL ROUTER CUENCA

38.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

38.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER CUENCA

Router>enable
Router#configure terminal
Router(config)#hostname *CUENCA*
***CUENCA*(config)#**

38.3 CREACION DE CONTRASEÑAS

CUENCA #enable
CUENCA #configure terminal
CUENCA **(config)#**
CUENCA **(config)#**line console 0
CUENCA **(config-line)#**password cisco
CUENCA **(config-line)#l**ogin
CUENCA **(config-line)#**exit
CUENCA **(config)#**line vty 0 4
CUENCA **(config-line)#**password cisco
CUENCA **(config-line)#**login
CUENCA **(config-line)#**password cisco
CUENCA **(config)#**enable password cisco
CUENCA **(config-line)#**exit

38.4 CONFIGURACION DE LAS INTERFACES

38.4.1 CONFIGURACION DE LA INTERFAZ SERIAL 1/0

CUENCA **(config)#**interface serial 1/0
CUENCA **(config-if)#**ip address 192.168.1.9 255.255.255.252
CUENCA **(config-if)#**no shutdown
CUENCA **(config-if)#**exit

38.4.2 CONFIGURACION DE LA INTERFAZ SERIAL 1/1

CUENCA **(config)#**interface serial 1/1
CUENCA **(config-if)#**ip address 192.168.1.6 255.255.255.252
CUENCA **(config-if)#**no shutdown
CUENCA **(config-if)#**exit

38.4.3 CONFIGURACION DE LA INTERFAZ SERIAL 1/2

CUENCA **(config)#**interface serial 1/2
CUENCA **(config-if)#**ip address 192.168.1.25 255.255.255.252
CUENCA **(config-if)#**clock rate 64000
CUENCA **(config-if)#**no shutdown
CUENCA **(config-if)#**exit

38.4.4 CONFIGURACION DE LA INTERFAZ SERIAL 1/3

CUENCA **(config)#**interface serial 1/3

***CUENCA* (config-if)**#ip address 192.168.1.29 255.255.255.252
***CUENCA* (config-if)**#clock rate 64000
***CUENCA* (config-if)**#no shutdown
***CUENCA* (config-if)**#exit

38.5 CONFIGURACIÓN DE PROTOCOLO RIPV2

El Protocolo de enrutamiento RIP de habilitarse antes de llevar a cabo cualquiera de los comandos, lo habilitamos utilizando el comando:

***CUENCA* (config)**#router rip
***CUENCA* (config-router)**#version 2
***CUENCA* (config-router)**#network 192.168.1.24
***CUENCA* (config-router)**#network 192.168.1.28
***CUENCA* (config-router)**#redistribute ospf1 metric 1
***CUENCA* (config-router)**#exit

38.6 CONFIGURACIÓN DE PROTOCOLO OSPF

***CUENCA* (config)**#router ospf 1
***CUENCA* (config-router)**#network 192.168.1.8 0.0.0.3
***CUENCA* (config-router)**#redistribute rip subnets
***CUENCA* (config-router)**#exit
***CUENCA* (config)**#

38.7 SHOW RUNNING-CONFIG ROUTER CUENCA

```
Router#Show Running-config
Building configuration...
Current configuration : 1845 bytes
!
version 12.4
no service password-encryption
!
hostname Router
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco

ip ssh version 1
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 192.168.1.6 255.255.255.252
ip access-group 112 out
!
interface Serial1/1
 ip address 192.168.1.9 255.255.255.252
ip access-group 103 out
 clock rate 64000
!
interface Serial1/2
 ip address 192.168.1.29 255.255.255.252
 clock rate 64000
!
interface Serial1/3
 ip address 192.168.1.25 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 redistribute rip subnets
 network 192.168.1.8 0.0.0.3 area 1
!
router rip
 version 2
 redistribute ospf 1  metric 1
 network 192.168.1.0
!
ip classless
!
access-list 103 deny icmp any host 192.168.1.1
access-list 103 deny icmp any host 192.168.1.10
access-list 103 deny icmp any host 192.168.1.37
access-list 103 deny icmp any host 192.168.1.41
access-list 103 deny tcp any host 192.168.1.1 eq telnet
access-list 103 deny tcp any host 192.168.1.10 eq telnet
access-list 103 deny tcp any host 192.168.1.37 eq telnet
access-list 103 deny tcp any host 192.168.1.41 eq telnet
access-list 103 deny tcp any host 192.168.1.1 eq ftp
access-list 103 deny tcp any host 192.168.1.10 eq ftp
access-list 103 deny tcp any host 192.168.1.37 eq ftp
access-list 103 deny tcp any host 192.168.1.41 eq ftp
access-list 103 permit ip any any
```

```
access-list 112 deny icmp any host 192.168.2.132
access-list 112 deny tcp any host 192.168.2.132 eq telnet
access-list 112 deny tcp any host 192.168.2.132 eq ftp
access-list 112 permit ip any any
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
!
End
```

38.8 SHOW IP ROUTE ROUTER CUENCA

```
Cuenca#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 12 subnets
O       192.168.1.0 [110/1562] via 192.168.1.10, 01:19:26, Serial1/0
                    [110/1562] via 192.168.1.5, 01:19:26, Serial1/1
C       192.168.1.4 is directly connected, Serial1/1
C       192.168.1.8 is directly connected, Serial1/0
O       192.168.1.12 [110/1562] via 192.168.1.5, 01:19:26, Serial1/1
R       192.168.1.16 is possibly down, routing via 192.168.1.10, Serial1/0
                     is possibly down, routing via 192.168.1.5, Serial1/1
O       192.168.1.20 [110/1562] via 192.168.1.5, 01:19:26, Serial1/1
C       192.168.1.24 is directly connected, Serial1/2
C       192.168.1.28 is directly connected, Serial1/3

R       192.168.1.32 [120/1] via 192.168.1.30, 00:00:13, Serial1/3
                     [120/1] via 192.168.1.26, 00:00:21, Serial1/2
O       192.168.1.36 [110/1562] via 192.168.1.10, 01:19:26, Serial1/0
O E2    192.168.1.44 [110/781] via 192.168.1.10, 00:04:42, Serial1/0
O       192.168.1.48 [110/1562] via 192.168.1.10, 01:19:26, Serial1/0
O E2 192.168.2.0/24 [110/781] via 192.168.1.10, 00:45:05, Serial1/0
O E2 192.168.3.0/24 [110/781] via 192.168.1.5, 00:49:15, Serial1/1
O E2 192.168.4.0/24 [110/781] via 192.168.1.6, 00:46:10, Serial1/0
R    200.10.10.0/24 [120/1] via 192.168.1.6, 00:01:31, Serial1/0
```

[120/1] via 192.168.1.21, 00:01:31, Serial1/3
[120/1] via 192.168.1.14, 00:01:31, Serial1/2

39 CONFIGURACIÓN DEL ROUTER CUENCA EDIFICIO 1

39.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

39.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER CUENCA EDIFICIO 1

Router>enable
Router#configure terminal
Router(config)#hostname EDIFICIO 1
EDIFICIO1(config)#

39.3 CREACION DE CONTRASEÑAS

EDIFICIO1#enable
EDIFICIO1#configure terminal
EDIFICIO1 (config)#
EDIFICIO1 (config)#line console 0
EDIFICIO1 (config-line)#password cisco
EDIFICIO1 (config-line)#login
EDIFICIO1 (config)#enable password cisco
EDIFICIO1 (config-line)#exit
EDIFICIO1 (config)#line vty 0 4
EDIFICIO1 (config-line)#password cisco
EDIFICIO1 (config-line)#login
EDIFICIO1 (config)#enable password cisco
EDIFICIO1 (config-line)#exit
EDIFICIO1 (config)#

39.4 CONFIGURACION DE LAS INTERFACES

39.4.1 CONFIGURACION DE LA INTERFAZ SERIAL 1/0

EDIFICIO1 (config)#interface serial 1/0
EDIFICIO1 (config-if)#ip address 192.168.1.26 255.255.255.252
EDIFICIO1 (config-if)#no shutdown
EDIFICIO1 (config-if)#exit

39.4.2 CONFIGURACION DE LA INTERFAZ SERIAL 1/1

EDIFICIO1 (config)#interface serial 1/1
EDIFICIO1 (config-if)#ip address 192.168.1.33 255.255.255.252
EDIFICIO1 (config-if)#clock rate 64000
EDIFICIO1 (config-if)#no shutdown
EDIFICIO1 (config-if)#exit

39.4.3 CONFIGURACION DE LA INTERFAZ FASTETHERNET 0/0

EDIFICIO1 (config)#interface FastEthernet 0/0
EDIFICIO1 (config-if)#ip address 192.168.4.1 255.255.255.240
EDIFICIO1 (config-if)#no shutdown
EDIFICIO1 (config-if)#exit

39.5 CONFIGURACIÓN DE PROTOCOLO RIPV2

EDIFICIO1 #configure terminal
EDIFICIO1 (config)#router rip
EDIFICIO1 (config-router)#version 2
EDIFICIO1 (config-router)#network 192.168.1.24
EDIFICIO1 (config-router)#network 192.168.1.32
EDIFICIO1 (config-router)#network 192.168.4.0
EDIFICIO1 (config-router)#exit
EDIFICIO1 (config)#

39.6 SHOW RUNNING-CONFIG ROUTE CUENCA EDIFICIO 1

```
EDIFICIO1#Show Running-config
Building configuration...

Current configuration : 1215 bytes
!
version 12.4
no service password-encryption
!
hostname EDIFICIO1
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
ip ssh version 1
```

```
!
!
interface FastEthernet0/0
 ip address 192.168.4.1 255.255.255.240
 duplex auto
 speed auto
!


interface FastEthernet0/0.2
 encapsulation dot1Q 401
 ip address 192.168.4.17 255.255.255.240
!
interface FastEthernet0/0.3
 encapsulation dot1Q 402
 ip address 192.168.4.33 255.255.255.224
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 192.168.1.26 255.255.255.252
!
interface Serial1/1
 ip address 192.168.1.33 255.255.255.252
ip access-group 111 out
 clock rate 64000
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.4.0
!
ip classless
access-list 111 deny icmp any host 192.168.3.132
access-list 111 deny tcp any host 192.168.3.132 eq telnet
```

```
access-list 111 deny tcp any host 192.168.3.132 eq ftp
access-list 111 permit ip any any
!
no cdp run
!


line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
!
End
```

39.7 SHOW IP ROUTE ROUTER CUENCA EDIFICIO 1

```
EDIFICIO1#Show Ip Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 10 subnets
R       192.168.1.0 [120/3] via 192.168.1.34, 00:00:15, Serial1/1
R       192.168.1.4 [120/2] via 192.168.1.34, 00:00:15, Serial1/1
R       192.168.1.8 [120/2] via 192.168.1.34, 00:00:15, Serial1/1
R       192.168.1.12 [120/3] via 192.168.1.34, 00:00:15, Serial1/1
R       192.168.1.16 [120/4] via 192.168.1.34, 00:00:15, Serial1/1
R       192.168.1.28 [120/1] via 192.168.1.34, 00:00:15, Serial1/1
C       192.168.1.32 is directly connected, Serial1/1
R       192.168.1.36 [120/3] via 192.168.1.34, 00:00:15, Serial1/1
R       192.168.1.44 [120/4] via 192.168.1.34, 00:00:15, Serial1/1
R       192.168.1.48 [120/5] via 192.168.1.34, 00:00:15, Serial1/1
R    192.168.2.0/24 [120/4] via 192.168.1.34, 00:00:15, Serial1/1
R    192.168.3.0/24 [120/4] via 192.168.1.34, 00:00:15, Serial1/1
     192.168.4.0/24 is variably subnetted, 4 subnets, 3 masks
R       192.168.4.0/24 [120/1] via 192.168.1.34, 00:00:15, Serial1/1
C       192.168.4.0/28 is directly connected, FastEthernet0/0
C       192.168.4.16/28 is directly connected, FastEthernet0/0.2
C       192.168.4.32/27 is directly connected, FastEthernet0/0.3
R    200.10.10.0/24 [120/6] via 192.168.1.34, 00:00:15, Serial1/1
```

40 CONFIGURACIÓN DEL ROUTER CUENCA EDIFICIO 2

40.1 ACCESO AL MODO DE CONFIGURACIÓN PRINCIPAL

Router>enable
Router#configure terminal
Router(config)# exit
Router#

40.2 CONFIGURACIÓN DEL NOMBRE DEL ROUTER CUENCA EDIFICIO 2

Router>enable
Router#configure terminal
Router(config)#hostname EDIFICIO 1
EDIFICIO2(config)#

40.3 CREACION DE CONTRASEÑAS

EDIFICIO2#enable
EDIFICIO2#configure terminal
EDIFICIO2 (config)#
EDIFICIO2 (config)#line console 0
EDIFICIO2 (config-line)#password cisco
EDIFICIO2(config-line)#login
EDIFICIO2(config)#enable password cisco
EDIFICIO2(config-line)#exit
EDIFICIO2(config)#line vty 0 4
EDIFICIO2(config-line)#password cisco
EDIFICIO2(config-line)#login
EDIFICIO2(config)#enable password cisco
EDIFICIO2(config-line)#exit
EDIFICIO2(config)#

40.4 CONFIGURACION DE LAS INTERFACES

40.4.1 CONFIGURACION DE LA INTERFAZ SERIAL 1/0

EDIFICIO2 (config)#interface serial 1/0
EDIFICIO2 (config-if)#ip address 192.168.1.30 255.255.255.252

EDIFICIO2 (config-if)#no shutdown
EDIFICIO2 (config-if)#exit

40.4.2 CONFIGURACION DE LA INTERFAZ SERIAL 1/1

EDIFICIO2 (config)#interface serial 1/1
EDIFICIO2 (config-if)#ip address 192.168.1.34 255.255.255.252
EDIFICIO2 (config-if)#no shutdown
EDIFICIO2 (config-if)#exit

40.4.3 CONFIGURACION DE LA INTERFAZ FASTETHERNET 0/0

EDIFICIO1 (config)#interface FastEthernet 0/0
EDIFICIO1 (config-if)#ip address 192.168.4.65 255.255.255.240
EDIFICIO1 (config-if)#no shutdown
EDIFICIO1 (config-if)#exit

40.5 CONFIGURACIÓN DE PROTOCOLO RIPV2

EDIFICIO2 #configure terminal
EDIFICIO2 (config)#router rip
EDIFICIO2 (config-router)#version 2
EDIFICIO2 (config-router)#network 192.168.1.28
EDIFICIO2 (config-router)#network 192.168.1.32
EDIFICIO2 (config-router)#network 192.168.4.64
EDIFICIO2 (config-router)#exit
EDIFICIO2 (config)#

40.6 SHOW RUNNING-CONFIG ROUTER CUENCA EDIFICIO 2

EDIFICIO2#Show Running-config
Building configuration...

Current configuration : 2044 bytes
!
version 12.4
no service password-encryption
!
hostname EDIFICIO2
!!
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
ip ssh version 1
!

```
!
interface FastEthernet0/0
 ip address 192.168.4.65 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 403
 ip address 192.168.4.81 255.255.255.240
!
interface FastEthernet0/0.3
 encapsulation dot1Q 404
 ip address 192.168.4.97 255.255.255.224
!
interface FastEthernet0/0.4
 encapsulation dot1Q 405
 ip address 192.168.4.131 255.255.255.240
 ip access-group 114 out
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial1/0
 ip address 192.168.1.30 255.255.255.252
ip access-group 110 out
!


interface Serial1/1
 ip address 192.168.1.34 255.255.255.252
ip access-group 113 in
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
router rip
 version 2
 network 192.168.1.0
 network 192.168.4.0
!
```

```
ip classless
access-list 110 deny icmp any host 192.168.2.132
access-list 110 deny tcp any host 192.168.2.132 eq telnet
access-list 110 deny tcp any host 192.168.2.132 eq ftp
access-list 110 permit ip any any
access-list 113 deny icmp any host 192.168.4.132
access-list 113 deny tcp any host 192.168.4.132 eq telnet
access-list 113 deny tcp any host 192.168.4.132 eq ftp
access-list 113 permit ip any any
access-list 114 deny icmp host 192.168.4.82 host 192.168.4.132
access-list 114 deny icmp host 192.168.4.98 host 192.168.4.132
access-list 114 deny tcp host 192.168.4.82 host 192.168.4.132
access-list 114 deny tcp host 192.168.4.82 host 192.168.4.132 eq telnet
access-list 114 deny tcp host 192.168.4.98 host 192.168.4.132 eq telnet
access-list 114 deny tcp host 192.168.4.82 host 192.168.4.132 eq ftp
access-list 114 deny tcp host 192.168.4.98 host 192.168.4.132 eq ftp
access-list 114 permit ip any any
!
no cdp run
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
end
```

41 CONFIGURACIÓN DE ACCESS LIST (ACL)

41.1 ACL EXTENDIDA GUAYAQUIL

access-list (número) (deny | permit) (ip origen) (ip destino)

access-list 132 deny icmp any host 192.168.4.132

Bloquear el ping de cualquier subred a la PC con la IP 192.168.4.132
Bloquear el protocolo TELNET de cualquier subred a la PC con la IP 192.168.4.132
Bloquear el protocolo FTP de cualquier subred a la PC con la IP 192.168.4.132

Puertos que han sido bloqueados.

Comando Access List

```
GUAYAQUIL (config)# access-list 132 deny icmp any host 192.168.4.132
GUAYAQUIL (config)# access-list 132 deny tcp any host 192.168.4.132 eq telnet
GUAYAQUIL (config)# access-list 132 deny tcp any host 192.168.4.132 eq ftp
GUAYAQUIL (config)# access-list 132 permit ip any any
GUAYAQUIL (config)#exit
```

Comando

Número de Access List extendida 100-199

Permite o deniega el ingreso al paquete

IP origen

IP destino

Operador puede ser {lt,gt,eq,neq} (less than, greater than, equal, non equal)

41.1.1 IP Access-Group

El comando IP Access-Group agrupa una ACL existente a una interfaz.
In /Out: Selecciona si la ACL se aplica sobre la interfaz para paquetes de entrada o salida. Sino especifica si es de entrada o salida, la opción por defecto es out.
Se agruparan las ACL dentro del grupo 132 creado en la Subinterfaz 1/2 del router GUAYAQUIL

```
GUAYAQUIL (config)# interface serial 1/2
GUAYAQUIL (config-if)# ip access-group 132 out
GUAYAQUIL (config-if)# exit
```

Identifica que estamos agregando la ACL l al grupo 132 interfaz serial de salida

41.2 ACL EXTENDIDA GUAYAQUIL EDIFICIO1

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear la PC con la IP 192.168.2.82, hacia el Servidor del Edificio 1 con la siguiente IP 192.168.2.132
Bloquear el protocolo TELNET y el protocolo FTP.

GUAYAQUIL edif1 (config)# access-list 141 deny icmp host 192.168.2.82 host 192.168.2.132
GUAYAQUIL edif1 (config)# access-list 141 deny tcp host 192.168.2.82 host 192.168.2.132 eq telnet
GUAYAQUIL edif1 (config)# access-list 141 deny tcp host 192.168.2.82 host 192.168.2.132 eq ftp
GUAYAQUIL edif1 (config)# access-list 141 permit ip any any

Bloquear la PC con la IP 192.168.2.98, hacia el Servidor del Edificio 1 con la siguiente IP 192.168.2.132
Bloquear el protocolo TELNET y el protocolo FTP.

GUAYAQUIL edif1 (config)# access-list 142 deny icmp host 192.168.2.98 host 192.168.2.132
GUAYAQUIL edif1 (config)# access-list 142 deny tcp host 192.168.2.98 host 192.168.2.132 eq telnet
GUAYAQUIL edif1 (config)# access-list 142 deny tcp host 192.168.2.98 host 192.168.2.132 eq ftp
GUAYAQUIL edif1 (config)# access-list 142 permit ip any any

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

GUAYAQUIL edif1(config)# interface FastEthernet0/0.2
GUAYAQUIL edif1(config)# ip access-group 141 in
GUAYAQUIL edif1(config)# exit

GUAYAQUIL edif1(config)# interface FastEthernet0/0.3
GUAYAQUIL edif1(config)# ip access-group 142 in
GUAYAQUIL edif1(config)# exit

41.3 ACL EXTENDIDA IPS

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear el ping el protocolo Telnet y FTP a la PC con la IP 200.10.10.18 del Router del ISP hacia la red de Cuenca.

ISP (config)# *access-list 130 deny icmp host 200.10.10.18 host 192.168.4.132*
ISP (config)# *access-list 130 deny tcp host 200.10.10.18 host 192.168.4.132 eq telnet*
ISP (config)# *access-list 130 deny tcp host 200.10.10.18 host 192.168.4.132 eq ftp*
ISP (config)# *access-list 130 permit ip any any*

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

ISP (config)# interface Serial 1/0
ISP (config)# ip access-group 130 out
ISP (config)# exit

41.4 ACL EXTENDIDA QUITO

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear el ping el protocolo Telnet y FTP a la red del router de Quito desde cualquier punto de la red.

QUITO(config)# access-list 101 deny icmp any host 192.168.1.1
QUITO(config)# access-list 101 deny icmp any host 192.168.1.10
QUITO(config)# access-list 101 deny icmp any host 192.168.1.37
QUITO(config)# access-list 101 deny icmp any host 192.168.1.41
QUITO(config)# access-list 101 deny tcp any host 192.168.1.1 eq telnet
QUITO(config)# access-list 101 deny tcp any host 192.168.1.10 eq telnet
QUITO(config)# access-list 101 deny tcp any host 192.168.1.37 eq telnet
QUITO(config)# access-list 101 deny tcp any host 192.168.1.41 eq telnet
QUITO(config)# access-list 101 deny tcp any host 192.168.1.1 eq ftp
QUITO(config)# access-list 101 deny tcp any host 192.168.1.10 eq ftp
QUITO(config)# access-list 101 deny tcp any host 192.168.1.37 eq ftp
QUITO(config)# access-list 101 deny tcp any host 192.168.1.41 eq ftp

QUITO(config)# access-list 101 permit ip any any
QUITO(config)# access-list 102 deny icmp any host 192.168.2.132
QUITO(config)# access-list 102 deny tcp any host 192.168.2.132 eq telnet
QUITO(config)# access-list 102 deny tcp any host 192.168.2.132 eq ftp
QUITO(config)# access-list 102 permit ip any any
QUITO(config)# access-list 135 deny icmp host 192.168.3.18 host 192.168.4.132
QUITO(config)# access-list 135 deny icmp host 192.168.3.34 host 192.168.4.132
QUITO(config)# access-list 135 deny tcp host 192.168.3.18 host 192.168.4.132 eq telnet
QUITO(config)# access-list 135 deny tcp host 192.168.3.34 host 192.168.4.132 eq telnet
QUITO(config)# access-list 135 deny tcp host 192.168.3.18 host 192.168.4.132 eq ftp
QUITO(config)# access-list 135 deny tcp host 192.168.3.34 host 192.168.4.132 eq ftp

QUITO(config)# access-list 135 permit ip any any

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

QUITO (config)# interface Serial 1/0
QUITO (config)# ip access-group 102 out
QUITO (config)# exit

QUITO (config)# interface Serial 1/1
QUITO (config)# ip access-group 101 out
QUITO (config)# exit

QUITO (config)# interface Serial 1/2
QUITO (config)# ip access-group 135 in
QUITO (config)# exit

41.5 ACL EXTENDIDA QUITO EDIFICIO1

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear el ping el protocolo Telnet y FTP a la PC con la IP 192.168.4.132 del Router del edificio 1 en Quito desde cualquier punto de la red.

QUITO_E1(config)# access-list 115 deny icmp any host 192.168.4.132
QUITO_E1(config)# access-list 115 deny tcp any host 192.168.4.132 eq telnet
QUITO_E1(config)# access-list 115 deny tcp any host 192.168.4.132 eq ftp
QUITO_E1(config)# access-list 115 permit ip any any

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

QUITO_E1 (config)# interface Serial 1/1
QUITO_E1 (config)# ip access-group 115 out
QUITO_E1 (config)# exit

41.6 ACL EXTENDIDA QUITO EDIFICIO2

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear el ping el protocolo Telnet y FTP al Servidor con la IP 192.168.3.132 del Router del edificio 2 en Quito desde cualquier punto de la red.

QUITO_E2 (config)# *access-list 118 deny icmp any host 192.168.2.132*
QUITO_E2 (config)# *access-list 118 deny tcp any host 192.168.2.132 eq telnet*
QUITO_E2 (config)# *access-list 118 deny tcp any host 192.168.2.132 eq ftp*
QUITO_E2 (config)# *access-list 118 permit ip any any*
QUITO_E2 (config)# *access-list 119 deny icmp any host 192.168.3.132*

QUITO_E2 (config)# *access-list 119 deny tcp any host 192.168.3.132 eq telnet*
QUITO_E2 (config)# *access-list 119 deny tcp any host 192.168.3.132 eq ftp*
QUITO_E2 (config)# *access-list 119 permit ip any any*
QUITO_E2 (config)# *access-list 120 deny icmp host 192.168.3.82 host 192.168.3.132*
QUITO_E2 (config)# *access-list 120 deny icmp host 192.168.3.98 host 192.168.3.132*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.82 host 192.168.3.132 eq telnet*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.98 host 192.168.3.132 eq telnet*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.82 host 192.168.3.132 eq ftp*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.98 host 192.168.3.132 eq ftp*
QUITO_E2 (config)# *access-list 120 permit ip any any*
QUITO_E2 (config)# *access-list 136 deny icmp host 192.168.3.98 host 192.168.4.132*
QUITO_E2 (config)# *access-list 136 deny tcp host 192.168.3.98 host 192.168.4.132 eq telnet*
QUITO_E2 (config)# *access-list 136 deny tcp host 192.168.3.98 host 192.168.4.132 eq ftp*
QUITO_E2 (config)# *access-list 136 permit ip any any*
QUITO_E2 (config)# *access-list 137 deny icmp host 192.168.3.82 host 192.168.4.132*
QUITO_E2 (config)# *access-list 137 deny tcp host 192.168.3.82 host 192.168.4.132 eq telnet*
QUITO_E2 (config)# *access-list 137 deny tcp host 192.168.3.82 host 192.168.4.132 eq ftp*

QUITO_E2 (config)# *access-list 137 permit ip any any*
QUITO_E2 (config)# *access-list 118 deny icmp any host 192.168.2.132*
QUITO_E2 (config)# *access-list 118 deny tcp any host 192.168.2.132 eq telnet*
QUITO_E2 (config)# *access-list 118 deny tcp any host 192.168.2.132 eq ftp*
QUITO_E2 (config)# *access-list 118 permit ip any any*
QUITO_E2 (config)# *access-list 119 deny icmp any host 192.168.3.132*
QUITO_E2 (config)# *access-list 119 deny tcp any host 192.168.3.132 eq telnet*
QUITO_E2 (config)# *access-list 119 deny tcp any host 192.168.3.132 eq ftp*
QUITO_E2 (config)# *access-list 119 permit ip any any*
QUITO_E2 (config)# *access-list 120 deny icmp host 192.168.3.82 host 192.168.3.132*
QUITO_E2 (config)# *access-list 120 deny icmp host 192.168.3.98 host 192.168.3.132*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.82 host 192.168.3.132 eq telnet*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.98 host 192.168.3.132 eq telnet*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.82 host 192.168.3.132 eq ftp*
QUITO_E2 (config)# *access-list 120 deny tcp host 192.168.3.98 host 192.168.3.132 eq ftp*
QUITO_E2 (config)# *access-list 120 permit ip any any*
QUITO_E2 (config)# *access-list 136 deny icmp host 192.168.3.98 host 192.168.4.132*
QUITO_E2 (config)# *access-list 136 deny tcp host 192.168.3.98 host 192.168.4.132 eq telnet*

QUITO_E2 (config)# *access-list 136 deny tcp host 192.168.3.98 host 192.168.4.132 eq ftp*
QUITO_E2 (config)# *access-list 136 permit ip any any*
QUITO_E2 (config)# *access-list 137 deny icmp host 192.168.3.82 host 192.168.4.132*
QUITO_E2 (config)# *access-list 137 deny tcp host 192.168.3.82 host 192.168.4.132 eq telnet*
QUITO_E2 (config)# *access-list 137 deny tcp host 192.168.3.82 host 192.168.4.132 eq ftp*
QUITO_E2 (config)# *access-list 137 permit ip any any*

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

QUITO_E2 (config)# interface FastEthernet 0/0.2
QUITO_E2 (config)# ip access-group 137 in
QUITO_E2 (config)# exit

QUITO_E2 (config)# interface FastEthernet 0/0.3
QUITO_E2 (config)# ip access-group 136 in
QUITO_E2 (config)# exit

QUITO_E2 (config)# interface FastEthernet 0/0.4
QUITO_E2 (config)# ip access-group 120 out
QUITO_E2 (config)# exit

QUITO_E2 (config)# interface Serial 1/0
QUITO_E2 (config)# ip access-group 118 out
QUITO_E2 (config)# exit
QUITO_E2 (config)# interface Serial 1/1
QUITO_E2 (config)# ip access-group 119 in
QUITO_E2 (config)# exit

41.7 ACL EXTENDIDA CUENCA

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear el ping el protocolo Telnet y FTP a la red del router de Cuenca desde cualquier punto de la red.

CUENCA access-list 103 deny icmp any host 192.168.1.1
CUENCA access-list 103 deny icmp any host 192.168.1.10
CUENCA access-list 103 deny icmp any host 192.168.1.37
CUENCA access-list 103 deny icmp any host 192.168.1.41
CUENCA access-list 103 deny tcp any host 192.168.1.1 eq telnet
CUENCA access-list 103 deny tcp any host 192.168.1.10 eq telnet

```
CUENCA access-list 103 deny tcp any host 192.168.1.37 eq telnet
CUENCA access-list 103 deny tcp any host 192.168.1.41 eq telnet
CUENCA access-list 103 deny tcp any host 192.168.1.1 eq ftp
CUENCA access-list 103 deny tcp any host 192.168.1.10 eq ftp
CUENCA access-list 103 deny tcp any host 192.168.1.37 eq ftp
CUENCA access-list 103 deny tcp any host 192.168.1.41 eq ftp
CUENCA access-list 103 permit ip any any
CUENCA access-list 112 deny icmp any host 192.168.2.132
CUENCA access-list 112 deny tcp any host 192.168.2.132 eq telnet
CUENCA access-list 112 deny tcp any host 192.168.2.132 eq ftp
CUENCA access-list 112 permit ip any any
```

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

```
CUENCA (config)# interface Serial 1/0
CUENCA (config)# ip access-group 112 out
CUENCA (config)# exit

CUENCA (config)# interface Serial 1/1
CUENCA (config)# ip access-group 103 out
CUENCA (config)# exit
```

41.8 ACL EXTENDIDA CUENCA EDIFICIO1

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear el ping el protocolo Telnet y FTP a la PC con la IP 192.168.3.132 del Router del edificio 1 en Cuenca desde cualquier punto de la red.

```
CUENCA_E1(config)# access-list 111 deny icmp any host 192.168.3.132
CUENCA_E1(config)# access-list 111 deny tcp any host 192.168.3.132 eq telnet
CUENCA_E1(config)# access-list 111 deny tcp any host 192.168.3.132 eq ftp
CUENCA_E1(config)# access-list 111 permit ip any any
```

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

```
CUENCA_E1(config)# interface Serial 1/1
CUENCA_E1(config)# ip access-group 111 out
CUENCA_E1(config)# exit
```

41.9 ACL EXTENDIDA CUENCA EDIFICIO2

Sintaxis:

access-list (número) (deny | permit) (ip origen) (ip destino)

Bloquear el ping el protocolo Telnet y FTP a la PC con la IP 192.168.2.132 del Router del edificio 2 en Cuenca desde cualquier punto de la red.

CUENCA_E2(config)# *access-list 110 deny icmp any host 192.168.2.132*
CUENCA_E2(config)# *access-list 110 deny tcp any host 192.168.2.132 eq telnet*
CUENCA_E2(config)# *access-list 110 deny tcp any host 192.168.2.132 eq ftp*
CUENCA_E2(config)# *access-list 110 permit ip any any*
CUENCA_E2(config)# *access-list 113 deny icmp any host 192.168.4.132*
access-list 113 deny tcp any host 192.168.4.132 eq telnet
access-list 113 deny tcp any host 192.168.4.132 eq ftp
access-list 113 permit ip any any
access-list 114 deny icmp host 192.168.4.82 host 192.168.4.132
access-list 114 deny icmp host 192.168.4.98 host 192.168.4.132
access-list 114 deny tcp host 192.168.4.82 host 192.168.4.132
access-list 114 deny tcp host 192.168.4.82 host 192.168.4.132 eq telnet
access-list 114 deny tcp host 192.168.4.98 host 192.168.4.132 eq telnet
access-list 114 deny tcp host 192.168.4.82 host 192.168.4.132 eq ftp
access-list 114 deny tcp host 192.168.4.98 host 192.168.4.132 eq ftp
access-list 114 permit ip any any

Posteriormente levantaremos nuestra ACL extendida en la interfaz correspondiente.

CUENCA_E2(config)# interface FastEthernet 0/0.4
CUENCA_E2(config)# ip access-group 114 out
CUENCA_E2(config)# exit

CUENCA_E2(config)# interface Serial 1/0
CUENCA_E2(config)# ip access-group 110 out
CUENCA_E2(config)# exit

CUENCA_E2(config)# interface Serial 1/1
CUENCA_E2(config)# ip access-group 113 out
CUENCA_E2(config)# exit

42 SWITCHES

Un switch denominado en el idioma castellano se la llama tambien "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 Interconection). Un conmutador o swicht se interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Gráfico 42-1: Switches

Switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

42.1 OBJETIVOS DEL DISEÑO DE LAN

El primer paso en el diseño de una LAN es establecer y documentar los objetivos de diseño. Estos objetivos son específicos para cada organización o situación. Esta página describirá los requisitos de la mayoría de los diseños de red:

- **Funcionalidad:** La red debe funcionar. Es decir, debe permitir que los usuarios cumplan con sus requisitos laborales. La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonables.
- **Escalabilidad:** La red debe poder aumentar de tamaño. Es decir, el diseño original debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.
- **Adaptabilidad:** La red debe diseñarse teniendo en cuenta futuras tecnologías. La red no debería incluir elementos que limiten la implementación de nuevas tecnologías a medida que éstas van apareciendo.
- **Facilidad de administración:** La red debe estar diseñada para facilitar su monitoreo y administración, con el objeto de asegurar una estabilidad de funcionamiento constante.

  La Actividad de Medios Interactivos ayudará a los estudiantes a familiarizarse con los cuatro objetivos de diseño principales

  En la página siguiente se analizan algunas de las consideraciones del diseño de una LAN.

42.2 EL DISEÑO DE CAPA 2

El propósito de los dispositivos de la Capa 2 en la red es conmutar tramas basadas en sus direcciones MAC destino, ofrecer detección de errores y reducir la congestión en la red. Los dos dispositivos de networking de Capa 2 más comunes son los puentes y switches LAN. Los dispositivos de la Capa 2 determinan el tamaño de los dominios de colisión.

Las colisiones y el tamaño de los dominios de colisión son dos factores que afectan de forma negativa el rendimiento de una red. La microsegmentación de la red reduce el tamaño de los dominios de colisión y reduce las colisiones. La microsegmentación se implementa a través del uso de puentes y switches. El objetivo es aumentar el rendimiento de un grupo de trabajo o de un backbone.

Los switches se pueden utilizar junto con hubs para suministrar el nivel de rendimiento adecuado para distintos usuarios y servidores.

Otra característica importante de un switch LAN es la forma en que puede asignar ancho de banda por puerto. Esto permite ofrecer más ancho de banda para el

cableado vertical, los uplinks y los servidores. Este tipo de conmutación se conoce como conmutación asimétrica. La conmutación asimétrica proporciona conexiones de conmutación entre puertos con distinto ancho de banda por ejemplo, una combinación de puertos de 10 Mbps y de 100 Mbps. La conmutación simétrica ofrece conexiones conmutadas entre puertos de ancho de banda similar.

La capacidad deseada de un tendido de cable vertical es mayor que la de un tendido de cable horizontal. La instalación de un switch LAN en MDF e IDF, permite al tendido de cable vertical administrar el tráfico de datos que se transmiten desde el MDF hasta el IDF. Los tendidos horizontales entre el IDF y las estaciones de trabajo utilizan UTP Categoría 5e. Una derivación de cableado horizontal debería ser superior a 100 metros (328 pies). En un entorno normal, 10 Mbps es lo adecuado para la derivación del cableado horizontal. Los switches LAN asimétricos permiten la mezcla de los puertos 10-Mbps y 100-Mbps en un solo switch.

La nueva tarea consiste en determinar el número de puertos de 10 Mbps y 100 Mbps que se necesitan en el MDF y cada IDF. Esto se logra revisando los requisitos del usuario para la cantidad de derivaciones de cable horizontal por habitación y la cantidad de derivaciones totales en cualquier área de captación. Esto incluye la cantidad de tendidos de cable vertical. Por ejemplo, digamos que los requisitos para el usuario establecen que se deben instalar cuatro tendidos de cable horizontal en cada habitación. El IDF que brinda servicios a un área de captación abarca 18 habitaciones. Por lo tanto, cuatro derivaciones en cada una de las 18 habitaciones es igual a 4x18 ó 72 puertos de switch LAN.

El tamaño de un dominio de colisión se determina por la cantidad de hosts que se conectan físicamente a cualquier puerto en el switch. Esto también afecta la cantidad de ancho de banda de la red que está disponible para cualquier host. En una situación ideal, hay solamente un host conectado a un puerto de switch LAN. El dominio de colisión consistiría solamente en el host origen y el host destino.

El tamaño del dominio de colisión sería de dos. Debido al pequeño tamaño de este dominio de colisión, prácticamente no se producen colisiones cuando alguno de los dos hosts se comunica con el otro. Otra forma de implementar la conmutación LAN es instalar hubs de LAN compartidos en los puertos del switch. Esto permite a varios hosts conectarse a un solo puerto de switch. Todos los hosts conectados al

hub de LAN compartido comparten el mismo dominio de colisión y el mismo ancho de banda

. Esto significa que las colisiones podrían producirse con más frecuencia.

Los hubs de medios compartidos, generalmente, se utilizan en un entorno de switch LAN para crear más puntos de conexión al final de los tendidos de cableado horizontal.

Los hubs de medios compartidos, generalmente, se utilizan en un entorno de switch LAN para crear más puntos de conexión al final de los tendidos de cableado horizontal. Ésta es una situación aceptable pero que debe tomarse con precaución. Los dominios de colisión deben mantenerse pequeños y el ancho de banda hacia el host se debe suministrar de acuerdo con las especificaciones establecidas en la fase de requisitos del proceso de diseño de red.

En la página siguiente se analizan algunos temas de diseño de la Capa 3.

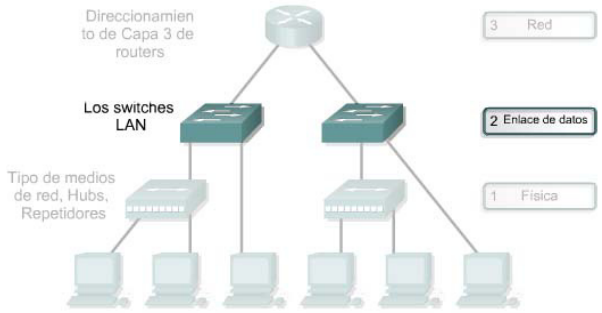


Gráfico 42-2: El diseño de Capa 2

42.3 SWITCHES DE CAPA DE ACCESO

Los switches de la capa de acceso operan en la Capa 2 del modelo OSI y ofrecen servicios como el de asociación de VLAN. El principal propósito de un switch de capa de acceso es permitir a los usuarios finales el acceso a la red. Un switch de capa de acceso debe proporcionar esta funcionalidad con bajo costo y una alta densidad de puerto.

Los siguientes switches Cisco se utilizan comúnmente en la capa de acceso:

- Serie Catalyst 1900
- Serie Catalyst 2820
- Serie Catalyst 2950
- Serie Catalyst 4000
- Serie Catalyst 5000

El switch de las series Catalyst 1900 ó 2820 es un dispositivo de acceso efectivo para redes de campus medias o pequeñas. El switch serie Catalyst 2950 ofrece acceso efectivo para servidores y usuarios que requieren un alto ancho de banda. Esto se logra con puertos de switch adaptados para Fast Ethernet. Los switches serie Catalyst 4000 y 5000 incluyen puertos Gigabit Ethernet y son dispositivos de acceso efectivos para una mayor cantidad de usuarios en redes de campus más grandes.

42.4 SWITCHES DE LA CAPA DE DISTRIBUCIÓN

En esta página se explican las características y funciones de los switches de la capa de distribución.

Los switches de la capa de distribución son los puntos de totalización de múltiples switches de la capa de acceso. El switch debe poder adecuarse al monto total del tráfico desde los dispositivos de la capa de acceso.

El switch de la capa de distribución debe tener un alto rendimiento, dado que es un punto en el cual se encuentra delimitado el dominio de broadcast. La capa de distribución combina el tráfico VLAN y es un punto focal para las decisiones de política sobre flujo de tráfico.

Por estas razones, los switches que residen en la capa de distribución operan tanto en la Capa 2 como en la Capa 3 del modelo OSI. Los switches en esta capa se conocen como switches multicapa. Estos switches multicapa combinan las funciones de un router y de un switch en un dispositivo. Están diseñados para conmutar el tráfico a fin de obtener un rendimiento mayor que el de un router estándar. Si no tienen un módulo de router asociado, entonces, se utiliza un router externo para la función de la Capa 3.

Los siguientes switches de Cisco son adecuados para la capa de distribución:

- Catalyst 2926G
- Familia Catalyst 5000
- Familia Catalyst 6000

42.5 DESCRIPCIÓN GENERAL DE LA CAPA DE DISTRIBUCIÓN

En esta página se describe la capa de distribución y su propósito. La capa de distribución de la red se encuentra entre las capas de acceso y núcleo. Ayuda a definir y separar el núcleo. El propósito de esta capa es ofrecer una definición fronteriza en la cual se puede llevar a cabo la manipulación de paquetes. Esta capa segmenta las redes en dominios de broadcast. Se pueden aplicar políticas y las listas de control de acceso pueden filtrar los paquetes. La capa de distribución aísla los problemas de red para los grupos de trabajo en los cuales se producen. La capa de distribución también evita que estos problemas afecten la capa núcleo. Los switches en esta capa operan en la Capa 2 y Capa 3. A continuación presentamos algunas de las funciones de la capa de distribución en una red conmutada:

- Unificación de las conexiones del armario de cableado
- Definición de dominio de broadcast/multicast
- Enrutamiento VLAN
- Cualquier transición de medio que deba producirse
- Seguridad

La página siguiente describe los switches de capa de distribución.

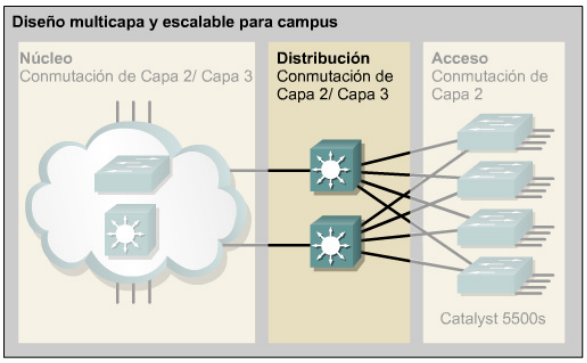


Gráfico 42-3: Descripción General de la Capa de Distribución

42.6 SEGMENTACIÓN

La segmentación se trata de dividir un segmento de red en varias direcciones osea direcciones IP con la finalidad que estas ip sehan utilizada en varias maquinas que se encuentra conectadas en la red, esta direccion ip no se puede repetirse en la red ya que produce problemas de direccion de ip en la red.

42.7 CONFIGURACIÓN DE SWICH

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

Un hub es un tipo más antiguo de dispositivo de concentración que también dispone de varios puertos. Sin embargo, los hubs son inferiores a los switches dado que todos los dispositivos conectados a un hub comparten el ancho de banda y tienen el mismo dominio de colisión. Otra desventaja de los hubs es que sólo operan en modo half-duplex. En modo half-duplex, los hubs sólo pueden enviar o recibir datos en determinado momento pero no pueden hacer las dos cosas al mismo tiempo. Los switches pueden operar en modo full-duplex, lo que significa que pueden enviar y recibir datos simultáneamente.

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

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

Los nuevos switches tienen una configuración preestablecida con valores de fábrica. Esta configuración rara vez cumple con las necesidades de los administradores de red. Los switches se pueden configurar y administrar desde una interfaz de línea de comando (CLI). Los dispositivos de red también se pueden configurar y administrar a través de una interfaz y un navegador basados en web.

Los administradores de red deben familiarizarse con todas las tareas relacionadas con la administración de redes con switches. Algunas de estas tareas incluyen el mantenimiento del switch y de su IOS. Otras tareas incluyen la administración de interfaces y tablas para lograr una operación óptima, confiable y segura. La configuración básica del switch, las actualizaciones de IOS y la recuperación de contraseñas son capacidades esenciales del administrador de red.

42.8 ARRANQUE FÍSICO DEL SWITCH CATALYST

En esta página se explican las características, funciones y el arranque de los switches.

Los switches son computadoras dedicadas y especializadas que contienen una unidad de procesamiento central (CPU), memoria de acceso aleatorio (RAM), y un sistema

operativo. Los switches generalmente poseen varios puertos a los cuales los hosts se pueden conectar así como puertos especializados para fines de administración. Los switches se pueden administrar y la configuración se puede visualizar y cambiar mediante el puerto de consola.

Los switches generalmente no tienen interruptores para encenderlos o apagarlos. Simplemente se conectan o se desconectan de una fuente de energía eléctrica.

En la Figura aparecen algunos switches de la serie Cisco Catalyst 2900. Existen modelos de 12 puertos, 24 puertos y 48 puertos. Los dos switches principales en la Figura son switches simétricos de configuración fija que ofrecen FastEthernet en todos los puertos o una combinación de puertos de 10Mbps y 100Mbps. Los siguientes tres switches son modelos asimétricos con dos puertos fijos Gigabit Ethernet de fibra o cobre. Los cuatro switches de la parte inferior son modelos asimétricos con ranuras modulares de Convertidor de Interfaz Gigabit (GBIC), que pueden alojar una serie de opciones de medios de cobre y de fibra.

42.9 INDICADORES LED DEL SWITCH

El panel frontal de un switch tiene varias luces que ayudan a controlar la actividad y desempeño del sistema. Esas luces se llaman diodos emisores de luz (LED). En esta página se analizan los LED que se encuentran en la parte frontal de un switch:

- LED del sistema
- LED de suministro remoto de energía (RPS)
- LED de modo de puerto
- LED de estado de puerto

El LED del sistema analiza si el sistema está recibiendo energía y está funcionando correctamente.

El LED RPS indica si se está utilizando o no el suministro de energía remota.

Los LED de modo indican el estado del botón Mode (Modo). Los modos se utilizan para determinar de qué manera se interpretan los LED de estado de puerto. Para seleccionar o cambiar el modo de puerto, presione el botón Mode (Modo) reiteradas veces hasta que los LED de modo indiquen el modo deseado.

En la página siguiente se explica de qué manera los LED se utilizan para verificar la funcionalidad de un switch.

42.10 RESULTADO DE ARRANQUE INICIAL DESDE EL SWITCH

En esta página se explica de qué manera se puede usar HyperTerminal para verificar y configurar un switch.

Para poder configurar o verificar el estado de un switch, conecte una computadora al switch para establecer una sesión de comunicación. Utilice un cable transpuesto (rollover) para conectar el puerto de consola de la parte trasera del switch a un puerto COM en la parte trasera de la computadora.

Inicie HyperTerminal en la computadora. Aparece una ventana de diálogo. Primero debe otorgarse un nombre a la conexión al configurar por primera vez la comunicación de HyperTerminal con el switch.

Seleccione el puerto COM al cual el switch está conectado desde el menú desplegable y haga clic en el botón OK. Aparece otra ventana de diálogo. Establezca los parámetros tal como aparecen en la Figura y haga clic en el botón OK.

Conecte el switch al tomacorriente. El resultado del arranque inicial desde el switch debe aparecer en la pantalla de HyperTerminal. Este resultado muestra información sobre el switch, detalles sobre el estado de la POST y datos de hardware del switch.

Una vez que el switch ha arrancado y completado la POST, aparecen indicadores de diálogo de Configuración del Sistema. El switch se puede configurar manualmente con o sin ayuda del diálogo de Configuración del Sistema. El diálogo de Configuración del Sistema del switch es mucho más simple que el de los routers.

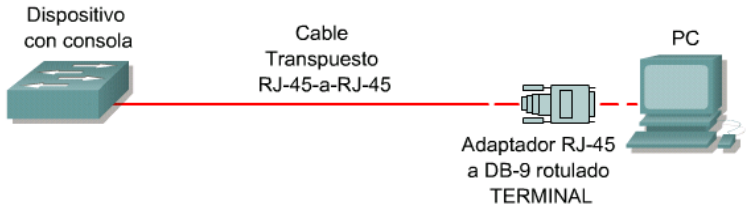


Gráfico 42-4: Resultado de arranque inicial desde el Switch

42.11 MODOS DE COMANDO DE LOS SWITCH

En esta página sea analizan dos modos de comando de switch. El modo por defecto es el modo EXEC usuario. El modo EXEC usuario se reconoce por su indicador, que termina en un carácter de "mayor que" (>). Los comandos disponibles en el modo EXEC usuario se limitan a los que cambian las configuraciones de terminal, realizan pruebas básicas y muestran información del sistema. La Figura describe los comandos show que están disponibles en el modo EXEC usuario.

El comando enable se utiliza para entrar al modo EXEC privilegiado desde el modo EXEC usuario. El modo EXEC privilegiado también se reconoce por su indicador, que termina con el carácter numeral (#).

El conjunto de comandos del modo EXEC privilegiado incluye el comando configure así como todos los comandos del modo EXEC usuario. El comando configure permite el acceso a otros modos de comando. Dado que estos modos se utilizan para configurar el switch, el acceso al modo EXEC privilegiado debe protegerse con contraseña para evitar el uso no autorizado. Si se establece una contraseña, se le solicita a los usuarios que introduzcan esa contraseña para poder acceder al modo EXEC privilegiado. La contraseña no aparece en pantalla y distingue entre mayúsculas y minúsculas.

Comandos	Descripción
`show version`	Proporciona información de versión del software y hardware. Se usa para ver exactamente cuáles son los módulos y el software en uso.
`show flash:`	Muestra información acerca de la flash: sistema de archivos.
`show mac-address-table`	Muestra el contenido de la tabla de envío MAC.
`show controllers ethernet-controller`	Proporciona información de tramas descartadas, tramas diferidas, errores de alineación, colisiones, etc.

Gráfico 42-5: Modos de Comando de los Switch

42.12 ADMINISTRACIÓN DE LA TABLA DE DIRECCIONES MAC

En esta página se explica de qué manera los switches crean y administran las tablas de direcciones MAC.

Los switches examinan la dirección origen de las tramas que se reciben en los puertos para aprender la dirección MAC de las estaciones de trabajo o las PC conectadas a estos. Estas direcciones MAC aprendidas se registran luego en una tabla de direcciones MAC. Las tramas que tienen una dirección MAC destino, que se ha registrado en la tabla, se pueden conmutar hacia la interfaz correcta.

El comando show mac-address-table se puede introducir en el modo EXEC privilegiado para examinar las direcciones que un switch ha aprendido.

Un switch aprende en forma dinámica y mantiene miles de direcciones MAC. Para preservar la memoria y para una operación optima del switch, las entradas aprendidas se pueden descartar de la tabla de direcciones MAC. Es posible que se hayan eliminado máquinas de un puerto, se hayan apagado o trasladado a otro puerto en el mismo switch o en un switch diferente. Esto puede provocar confusión al momento de enviar las tramas.

Por todas estas razones, si no se ven tramas con una dirección aprendida anteriormente, la entrada de direcciones MAC se descarta automáticamente o expiran después de 300 segundos.

En lugar de esperar que una entrada dinámica expire, los administradores de red pueden utilizar el comando clear mac-address-table en el modo EXEC privilegiado. Las entradas de direcciones MAC configuradas por los administradores de red también se pueden eliminar con este comando. Este método para borrar entradas de tabla permite eliminar de forma inmediata las direcciones no válidas.

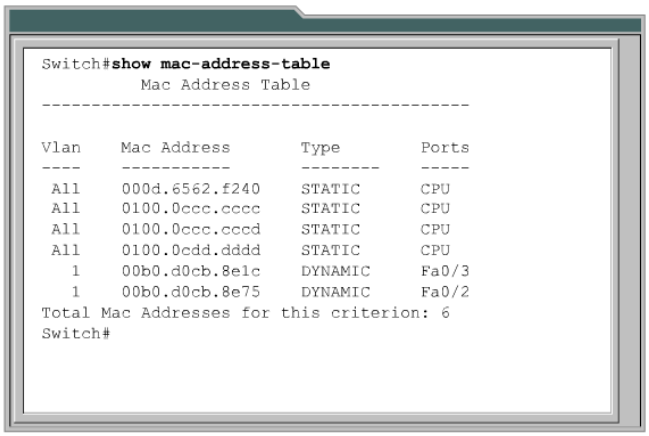


Gráfico 42-6: Administración De la Tabla de Direcciones MAC

42.13 CONFIGURACIÓN DE SEGURIDAD DE PUERTO

En esta página se explica por qué la seguridad de puerto es importante y de qué manera se la configura en un switch Catalyst 2900.

La seguridad de la red es una responsabilidad importante para los administradores de red. Se puede acceder a los puertos de switch de la capa de acceso a través de los conectores de red del cableado estructurado. Cualquier persona puede enchufar una PC o computadora portátil a uno de esos conectores de red. Éste es un posible punto de entrada a la red por parte de usuarios no autorizados. Los switches ofrecen una función que se conoce como seguridad de puertos. Es posible limitar la cantidad de direcciones que se pueden aprender en una interfaz. El switch se puede configurar para realizar una acción si ésta se supera.

Las direcciones MAC seguras se pueden configurar de forma estática. Sin embargo, la tarea de configurar direcciones MAC seguras es compleja y por lo general con una elevada tendencia a los errores.

Un enfoque alternativo es establecer una seguridad de puertos en una interfaz de switch. La cantidad de direcciones MAC por puerto se puede limitar a 1. La primera dirección aprendida de forma dinámica por el switch se convierte en dirección segura.

Para revertir la seguridad del puerto en una interfaz utilice la forma no del comando .

Para verificar el estado de seguridad de un puerto, se utiliza el comando show port security.

42.14 ADMINISTRACIÓN DEL ARCHIVO IOS DEL SWITCH

En esta página se enseña a los estudiantes cómo documentar y mantener los archivos de configuración operacional de los dispositivos de red.

Los administradores de red deben documentar y mantener los archivos de configuración operacional de los dispositivos de red. Debe realizarse una copia de seguridad del archivo de configuración actual en un servidor o en un disco. Esta documentación no sólo es esencial sino también muy útil en caso de que se necesite restaurar la configuración.

También debe realizarse una copia de seguridad del IOS en un servidor local. Entonces se puede recargar el IOS en la memoria flash si es necesario.

42.15 VLANs

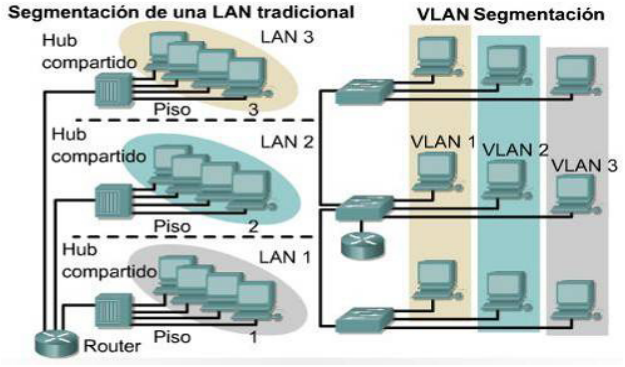


Gráfico 42-7: VLANS

Una VLAN es una agrupación lógica de dispositivos o usuarios que se pueden agrupar por función, departamento o aplicación, sin importar su ubicación física.
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 A continuación, presentamos algunos de los temas de configuración de las VLAN:

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

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

42.16 DOMINIOS DE BROADCAST CON VLAN Y ROUTERS

En esta página se explica de qué manera se enrutan los paquetes entre diferentes dominios de broadcast.

Una VLAN es un dominio de broadcast que se crea en uno o más switches. El diseño de red en las Figuras y requiere de tres dominios de broadcast separados.

La Figura muestra como los tres dominios de broadcast se crean usando tres switches. El enrutamiento de capa 3 permite que el router mande los paquetes a tres dominios de broadcast diferentes.

En la Figura , se crea una VLAN con un router y un switch. Existen tres dominios de broadcast separados. El router enruta el tráfico entre las VLAN mediante enrutamiento de Capa 3. El switch en la Figura envía tramas a las interfaces del router cuando se presentan ciertas circunstancias:

- Si es una trama de broadcast
- Si está en la ruta a una de las direcciones MAC del router

Si la Estación de Trabajo 1 de la VLAN de Ingeniería desea enviar tramas a la Estación de Trabajo 2 en la VLAN de Ventas, las tramas se envían a la dirección MAC Fa0/0 del router. El enrutamiento se produce a través de la dirección IP de la interfaz del router Fa0/0 para la VLAN de Ingeniería.

Si la Estación de Trabajo 1 de la VLAN de Ingeniería desea enviar una trama a la Estación de Trabajo 2 de la misma VLAN, la dirección MAC de destino de la trama es la de la Estación de Trabajo 2.

La implementación de VLAN en un switch hace que se produzcan ciertas acciones:

- El switch mantiene una tabla de puenteo separada para cada VLAN.
- Si la trama entra en un puerto en la VLAN 1, el switch busca la tabla de puenteo para la VLAN 1.

- Cuando se recibe la trama, el switch agrega la dirección origen a la tabla de puenteo si es desconocida en el momento.

- Se verifica el destino para que se pueda tomar una decisión de envío.
- Para aprender y enviar se realiza la búsqueda en la tabla de direcciones para esa VLAN solamente.

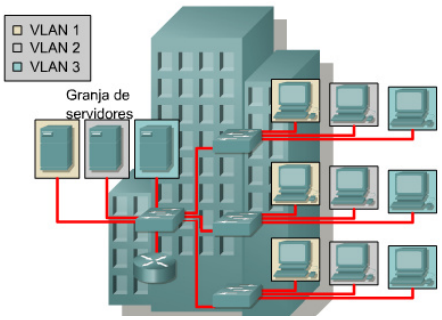


Gráfico 42-8: Dominios de Broadcast con vlan y routers

42.17 VENTAJAS DE LAS VLAN

Las VLAN permiten que los administradores de red organicen las LAN de forma lógica en lugar de física. Ésta es una ventaja clave. Esto permite que los administradores de red realicen varias tareas:

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad

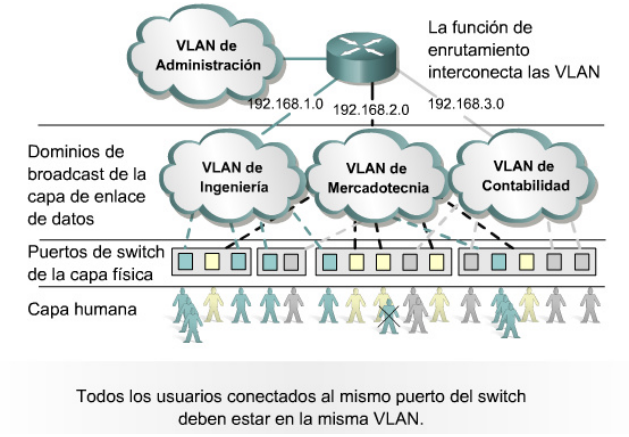


Gráfico 42-9: Ventajas de las Vlans

42.18 TIPOS DE VLAN

En esta página se describen tres asociaciones básicas de VLAN que se utilizan para determinar y controlar de qué manera se asigna un paquete: -

- VLAN basadas en puerto
- VLAN basadas en direcciones MAC
- VLAN basadas en protocolo
- La cantidad de VLAN en un switch varía según diversos factores:
- Patrones de tráfico
- Tipos de aplicaciones
- Necesidades de administración de red
- Aspectos comunes del grupo

El esquema de direccionamiento IP es otra consideración importante al definir la cantidad de VLAN en un switch.

Por ejemplo, una red que usa una máscara de 24 bits para definir una subred tiene en total 254 direcciones de host permitidas en una subred. Dado que es altamente recomendada una correspondencia de uno a uno entre las VLAN y las subredes IP, no puede haber más de 254 dispositivos en una VLAN. También se recomienda que las VLAN no se extiendan fuera del dominio de Capa 2 del switch de distribución.

Existen dos métodos principales para el etiquetado de tramas: el enlace Inter-Switch (ISL) y 802.1Q. ISL es un protocolo propietario de Cisco y antiguamente era el más común, pero está siendo reemplazado por el etiquetado de trama estándar IEEE 802.1Q.

A medida que los paquetes son recibidos por el switch desde cualquier dispositivo de estación final conectado, se agrega un identificador único de paquetes dentro de cada encabezado. Esta información de encabezado designa la asociación de VLAN de cada paquete. El paquete se envía entonces a los switches o routers correspondientes sobre la base del identificador de VLAN y la dirección MAC. Al alcanzar el nodo destino, el ID de VLAN es eliminado del paquete por el switch adyacente y es enviado al dispositivo conectado. El etiquetado de paquetes brinda un mecanismo para controlar el flujo de broadcasts y aplicaciones, mientras que no interfiere con la red y las aplicaciones.

La emulación de LAN (LANE) es una forma en que una red de Modo de Transferencia Asíncrona (ATM) simula una red Ethernet.

No hay etiquetado en LANE, pero la conexión virtual utilizada implica un ID de VLAN.

42.19 VERIFICACIÓN DE LA CONFIGURACIÓN DE VLAN

En esta página se explica de qué manera se pueden usar los comandos show vlan, show vlan brief, o show vlan id id_number para verificar las configuraciones de VLAN.

Se aplican los siguientes hechos a las VLAN:

- Una VLAN creada permanece sin usar hasta que se la asigna a puertos de switch.

Todos los puertos Ethernet son asignados a VLAN 1 por defecto.

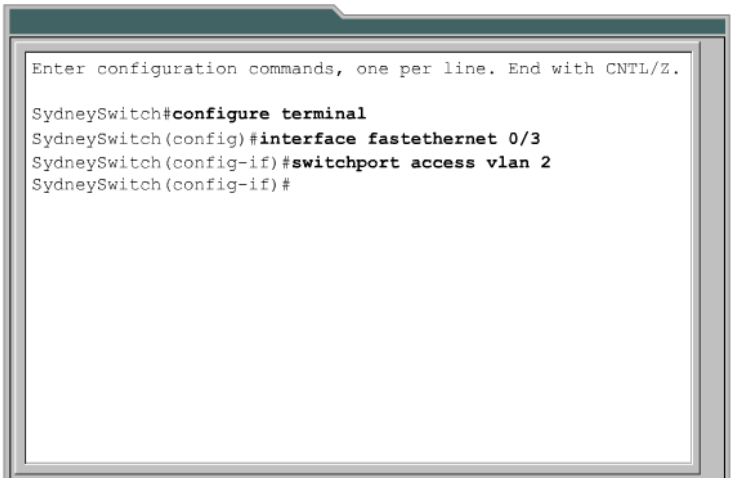


Gráfico 42-10: Verificación de la configuración de VLAN

42.20 CÓMO GUARDAR LA CONFIGURACIÓN DE VLAN

En esta página se enseña a los estudiantes cómo crear un archivo de texto de una configuración de VLAN para usarla como copia de seguridad.

Resulta útil mantener una copia de la configuración de VLAN como archivo de texto, especialmente si se necesita hacer copias de seguridad o auditorías.

Los valores de configuración del switch se pueden copiar en un servidor TFTP con el comando **copy running-config tftp**.

Como alternativa, se puede usar la función de captura de HyperTerminal junto con los comandos show running-config y show vlan para guardar los valores de configuración

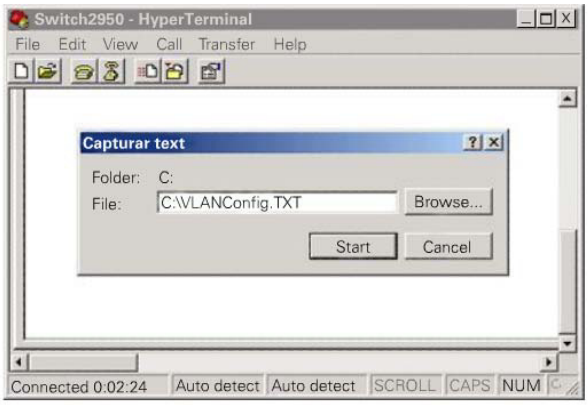


Gráfico 42-11: Como guardar la configuración de la Vlan

42.21 SITUACIONES DE DIAGNÓSTICO DE FALLAS DE LAS VLANS

Los administradores de red pueden hacer el diagnóstico de fallas de redes conmutadas de manera eficiente después de aprender las técnicas y adaptarlas a las necesidades de la empresa. La experiencia es la mejor manera de mejorar estas capacidades.

En esta página se describen tres situaciones de diagnóstico de fallas de VLAN relacionadas con los problemas que se presentan más comúnmente. Cada una de estas situaciones contiene un análisis del problema y su posterior resolución. Mediante el uso de comandos específicos apropiados y la reunión de información significativa de los resultados, se puede completar el proceso de diagnóstico de fallas.

No se puede establecer un enlace troncal entre un switch y un router

Cuando existan dificultades con una conexión de enlace troncal entre un switch y un router, tenga en cuenta las siguientes causas posibles:

- Asegúrese de que el puerto esté conectado y no reciba ningún error de capa física, alineación o secuencia de verificación de trama (FCS). Esto puede hacerse con el comando show interface en el switch.

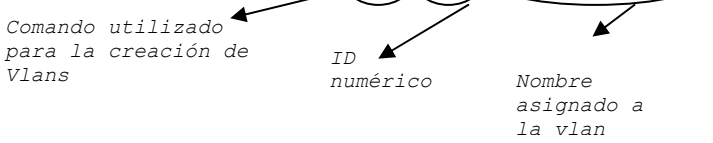
- Verifique que el duplex y la velocidad se encuentren correctamente configurados entre el switch y el router. Esto puede hacerse con el comando show interface status en el switch o el comando show interfaces en el router.
- Configure la interfaz física del router con una subinterfaz por cada VLAN que enrute el tráfico. Verifique esto introduciendo el comando IOS show interfaces. Asegúrese también de que cada subinterfaz en el router tenga el tipo de encapsulamiento, número de VLAN, dirección IP y máscara de subred correctos configurado. Esto puede hacerse con los comandos IOS show interfaces o show running-config.
- Confirme que el router esté ejecutando una versión del IOS que admita enlaces troncales. Esto se puede realizar con el comando show version.

43 CONFIGURACIÓN DE LOS SWITCHS

43.1 CONFIGURACION DE SWITCH DE LA SUCURSAL GUAYAQUIL EDIFICIO 1

43.1.1 CREACION DE LAS VLANS

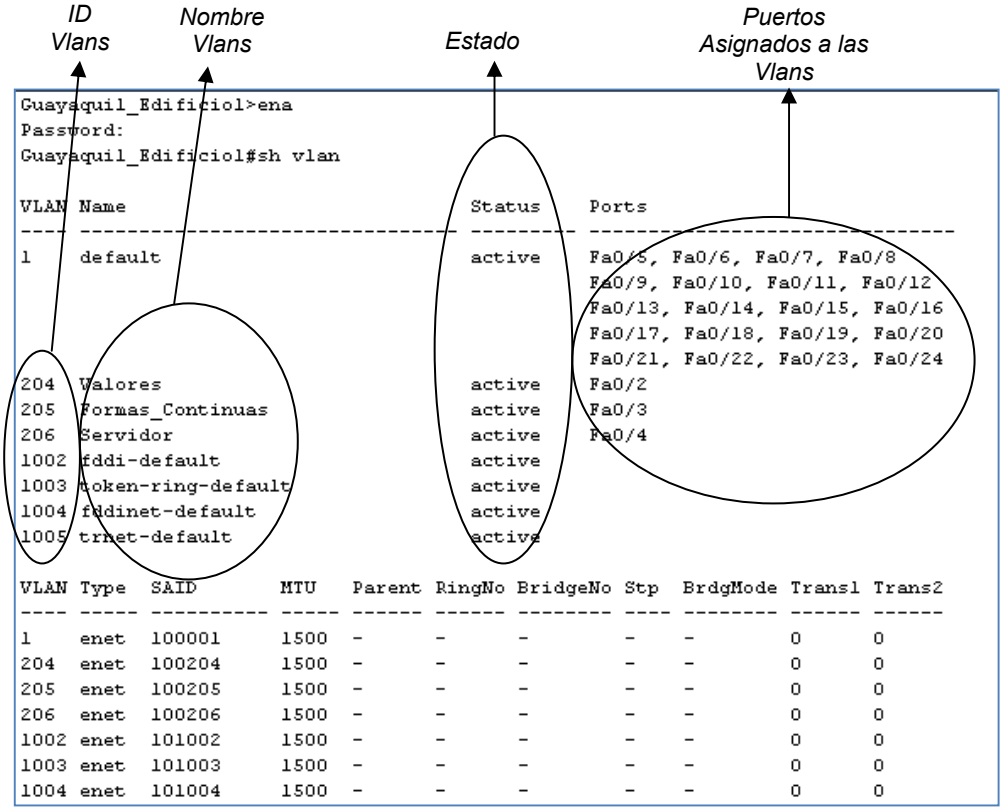
Guayaquil_Edificio1#vlan DAtabase → *Accesa a la Data Base VLan*
Guayaquil_Edificio1 (VLAN)#vlan 204 name Valores



Guayaquil_Edificio1 (VLAN)# Exit
Guayaquil_Edificio1 (VLAN)#vlan 205 name Formas_Continuas
VLAN 205 added:
Name: Formas_Continuas
Guayaquil_Edificio1 (vlan)#exit
APPLY completed.
Exiting....

43.1.2 SHOW VLAN DE SWITCH GUAYAQUIL_EDIFICIO1

Guayaquil_Edificio1 #show vlan → *Verifica la configuración de la VLAN*




```
Guayaquil_Edificiol>ena
Password:
Guayaquil_Edificiol#sh vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
204  Valores                             active    Fa0/2
205  Formas_Continuas                    active    Fa0/3
206  Servidor                            active    Fa0/4
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
204  enet  100204     1500  -      -      -        -    -        0      0
205  enet  100205     1500  -      -      -        -    -        0      0
206  enet  100206     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
```

Gráfico 43-1: Show vlan del swicth Guayaquil Edificio 1

43.1.3 ASIGNACION DE VLANS A LOS PUERTOS DEL SWITCH GUAYAQUIL_EDIFICIO1

Guayaquil_Edificio1(CONFIG)#interface fastethernet 0/1 → *Accesando Interfaz fast ethernet*
Guayaquil_Edificio1(CONFIG-IF)#switchport mode trunk →*Definir un puerto en modo runcado*
Guayaquil_Edificio1(CONFIG-IF)#exit → *Saliendo de la Interfaz*
Guayaquil_Edificio1(CONFIG)#interface fastethernet 0/2
Guayaquil_Edificio1(config-if)#*Switchport Access Vlan 204* → *Asignar Vlan a la Interfaz*
Guayaquil_Edificio1(CONFIG-IF)#exit
Guayaquil_Edificio1(CONFIG)#interface fastethernet 0/2
Guayaquil_Edificio1(config-if)#*Switchport Access Vlan 205*
Guayaquil_Edificio1(CONFIG-IF)#exit
Guayaquil_Edificio1(CONFIG)

43.2 CONFIGURACION DE SWITCH DE LA SUCURSAL GUAYAQUIL EDIFICIO 2

43.2.1 CREACION DE LAS VLANS

Guayaquil_Edificio2#vlan DAtabase
Guayaquil_Edificio2 (VLAN)#vlan 201 name Litografia
VLAN 201 added:
Name: Valores
Guayaquil_Edificio2 (VLAN)#vlan 202 name Arte_Prensa
VLAN 202 added:
Name: Formas_Continuas
Guayaquil_Edificio2 (vlan)#exit
APPLY completed.
Exiting....

43.2.2 SHOW VLAN DE SWITCH GUAYAQUIL_EDIFICIO1

Guayaquil_Edificio2 #show vlan → *Verifica la configuración de la VLAN*

```
Guayaquil_Edificio2#Show Vlan

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

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

Gráfico 43-2: Show vlan del swicth Guayaquil Edificio 2

43.2.3 ASIGNACION DE VLANS A LOS PUERTOS DEL SWITCH GUAYAQUIL_EDIFICIO1

Guayaquil_Edificio2(CONFIG)#in fastethernet 0/1
Guayaquil_Edificio2(CONFIG-IF)#switchport mode trunk
Guayaquil_Edificio2(CONFIG-IF)#exit
Guayaquil_Edificio2(CONFIG)#in fastethernet 0/2
Guayaquil_Edificio2(config-if)#*Switchport Access Vlan 201* → *Asignar Vlan a la Interfaz*
Guayaquil_Edificio2(CONFIG-IF)#exit → *Salir de la interfaz*
Guayaquil_Edificio2(CONFIG)#in fastethernet 0/2 → *Accesando Interfaz*

Guayaquil_Edificio2(config-if)#*Switchport Access Vlan 202* → *Asignar Vlan a la Interfaz*
Guayaquil_Edificio2(CONFIG-IF)#exit → *Salir de la interfaz*
Guayaquil_Edificio2(CONFIG)

43.3 CONFIGURACION DE SWITCH DE LA SUCURSAL QUITO EDIFICIO 1

43.3.1 CREACION DE LAS VLANS

Quito_Edificio1#vlan Database → *Crear Vlan*
Quito_Edificio1 (VLAN)#vlan 301 name Valores
VLAN 301 added:
Name: Valores → *Asignar Nombre de la VLAN*
Quito_Edificio1 (VLAN)#vlan 302 name Formas_Continuas
VLAN 302 added:
Name: Formas_Continuas
Quito_Edificio1 (vlan)#exit → *Salir de la configuración*
APPLY completed.
Exiting....

43.3.2 SHOW VLAN DE SWITCH QUITO_EDIFICIO1

Quito_Edificio1 #show vlan → *Verifica la configuración de la VLAN*

ID Vlans *Nombre Vlans* *Estado* *Puertos Asignados a las Vlans*

```
Quito_Edificio1#Show Vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
301  enet  100301     1500  -      -      -        -    -        0      0
302  enet  100302     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
1005 enet  101005     1500  -      -      -        -    -        0      0
```

Gráfico 43-3: SHOW VLAN DE SWITCH QUITO_EDIFICIO1

43.3.3 ASIGNACION DE VLANS A LOS PUERTOS DEL SWITCH QUITO_EDIFICIO1

Quito_Edificio1(CONFIG)#in fastethernet 0/1 → *Accesando Interfaz*
Quito_Edificio1(CONFIG-IF)#switchport mode trunk →*Definir un puerto Truncado*
Quito_Edificio1(CONFIG-IF)#exit → *Saliendo de la Interfaz*
Quito_Edificio1(CONFIG)#in fastethernet 0/2 → *Accesando Interfaz*
Quito_Edificio1(config-if)#*Switchport Access Vlan 301* → *Asignar Vlan a la Interfaz*
Quito_Edificio1(CONFIG-IF)#exit → *Salir de la interfaz*
Quito_Edificio1(CONFIG)#in fastethernet 0/2 → *Accesando Interfaz*
QuIto_Edificio1(config-if)#*Switchport Access Vlan 302* → *Asignar Vlan a la Interfaz*
Quito_Edificio1(CONFIG-IF)#exit → *Salir de la interfaz*
Quito_Edificio1(CONFIG)

43.4 CONFIGURACION DE SWITCH DE LA SUCURSAL QUITO EDIFICIO 2

43.4.1 CREACION DE LAS VLANS

Sw_Edificio2#vlan DAtabase
Sw_Edificio2 (VLAN)#vlan 303 name Litografia
VLAN 303 added:
Name: Litografia
Sw_Edificio2(VLAN)#vlan 304 name Arte_Prensa
VLAN 304 added:
Name: Arte_Prensa
Sw_Edificio2 (vlan)#exit
APPLY completed
Exiting....

43.4.2 SHOW VLAN DE SWITCH SW_EDIFICIO2

Sw_Edificio2#*Show Vlan*

```
Sw_Edificio2#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
303  Litografia                        active    Fa0/2
304  Arte_Prensa                       active    Fa0/3
305  Servidores                        active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
303  enet  100303     1500  -      -      -        -    -        0      0
304  enet  100304     1500  -      -      -        -    -        0      0
305  enet  100305     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
1005 enet  101005     1500  -      -      -        -    -        0      0
```

Gráfico 43-4: SHOW VLAN DE SWITCH SW_EDIFICIO2

43.4.3 ASIGNACION DE VLANS A LOS PUERTOS DEL SWITCH SW_EDIFICIO2

Sw_Edificio2(CONFIG)#in fastethernet 0/1
Sw_Edificio2(CONFIG-IF)#switchport mode trunk
Sw_Edificio2(CONFIG-IF)#exit
Sw_Edificio2(CONFIG)#in fastethernet 0/2
Sw_Edificio2(config-if)#*Switchport ACcess Vlan 303*
Sw_Edificio2(CONFIG-IF)#exit
Sw_Edificio2(CONFIG)#in fastethernet 0/2
Sw_Edificio2(config-if)#*Switchport ACcess Vlan 304*
Sw_Edificio2(CONFIG-IF)#exit
Sw_Edificio2(CONFIG)

43.5 CONFIGURACION DE SWITCH DE LA SUCURSAL CUENCA EDIFICIO 1

43.5.1 CREACION DE LAS VLANS

Cuenca_Edificio1#vlan DAtabase
Cuenca_Edificio1 (VLAN)#vlan 401 name Valores
VLAN 401 added:

Name: Valores → *Asignar Nombre de la VLAN*
Cuenca_Edificio1 (VLAN)#vlan 402 name Formas_Continuas
VLAN 402 added:
Name: Formas_Continuas
Cuenca_Edificio1 (vlan)#exit → *Salir de la configuración*
APPLY completed.
Exiting....

43.5.2 SHOW VLAN DE SWITCH CUENCA_EDIFICIO1

Cuenca_Edificio1#Show Vlan

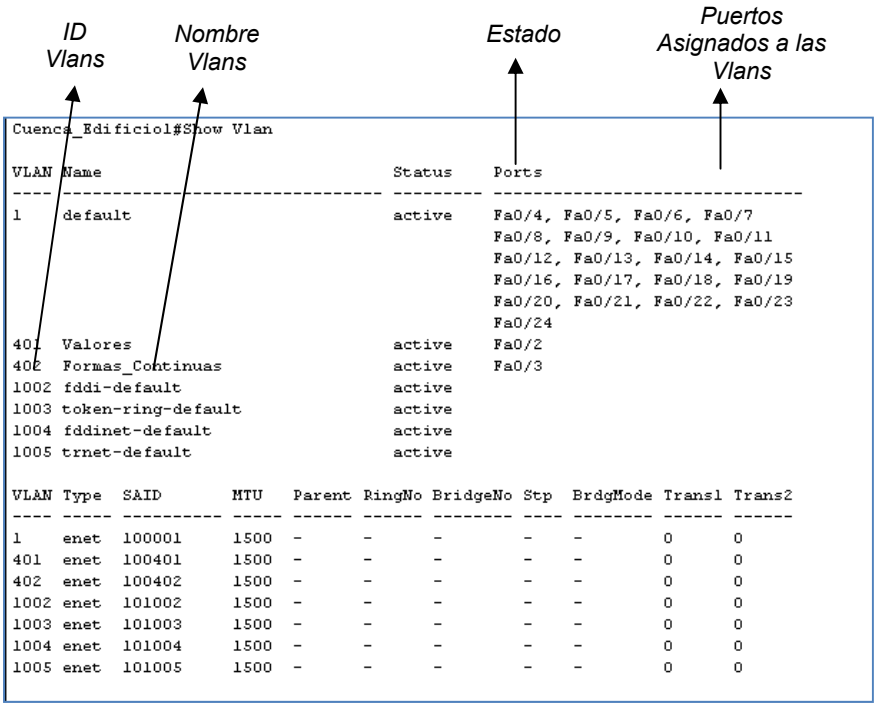


Gráfico 43-5:Show Vlan de Switch Cuenca_Edificio1

43.5.3 ASIGNACION DE VLANS A LOS PUERTOS DEL SWITCH CUENCA_EDIFICIO1

Cuenca_Edificio1 (CONFIG)#in fastethernet 0/1 → *Accesando Interfaz*
Cuenca_Edificio1 (CONFIG-IF)#switchport mode trunk →*Definir un puerto Truncado*
Cuenca_Edificio1 (CONFIG-IF)#exit → *Saliendo de la Interfaz*
Cuenca_Edificio1 (CONFIG)#in fastethernet 0/2 → *Accesando Interfaz*
Cuenca_Edificio1 (config-if)#*Switchport Access Vlan 401* → *Asignar Vlan a la Interfaz*
Cuenca_Edificio1 (CONFIG-IF)#exit → *Salir de la interfaz*
Cuenca_Edificio1 (CONFIG)#in fastethernet 0/2 → *Accesando Interfaz*
Cuenca_Edificio1 (config-if)#*Switchport Access Vlan 402* → *Asignar Vlan a la Interfaz*
Cuenca_Edificio1 (CONFIG-IF)#exit → *Salir de la interfaz*
Cuenca_Edificio1 (CONFIG)

43.6 CONFIGURACION DE SWITCH DE LA SUCURSAL CUENCA EDIFICIO 2

43.6.1 CREACION DE LAS VLANS

Cuenca_Edificio2#vlan DAtabase
Cuenca_Edificio2 (VLAN)#vlan 403 name Litografia
VLAN 403 added:
Name: Litografia
Cuenca_Edificio2 (VLAN)#vlan 404 name Arte_Prensa
VLAN 404 added:
Name: Arte_Prensa
Cuenca_Edificio2 (vlan)#exit
APPLY completed
Exiting....

43.6.2 SHOW VLAN DE SWITCH CUENCA EDIFICIO 2

Cuenca_Edificio2*#Show Vlan*

```
Cuenca_Edificio2#Show Vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
403  enet  100403     1500  -      -      -        -    -        0      0
404  enet  100404     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
1005 enet  101005     1500  -      -      -        -    -        0      0
```

Gráfico 43-6: Show Vlan de Switch Cuenca Edificio2

43.6.3 ASIGNACION DE VLANS A LOS PUERTOS DEL SWITCH CUENCA EDIFICIO 2

Cuenca_Edificio2 (CONFIG)#in fastethernet 0/1
Cuenca_Edificio2 (CONFIG-IF)#switchport mode trunk
Cuenca_Edificio2 (CONFIG-IF)#exit
Cuenca_Edificio2 (CONFIG)#in fastethernet 0/2
Cuenca_Edificio2 (config-if)#*Switchport ACcess Vlan 403*
Cuenca_Edificio2 (CONFIG-IF)#exit
Cuenca_Edificio2 (CONFIG)#in fastethernet 0/2
Cuenca_Edificio2 (config-if)#*Switchport ACcess Vlan 404*
Cuenca_Edificio2 (CONFIG-IF)#exit
Cuenca_Edificio2 (CONFIG)

GLOSARIO DE TÉRMINOS TÉCNICOS

44 GLOSARIO DE TÉRMINOS TÉCNICOS

A

ACL.- es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

B

BROADCAST.- en castellano difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo. En una red de broadcast la cuestión principal es como determinar quien usa un canal para el cual existe competencia. Los protocolos para esto pertenecen a un subnivel del nivel de enlace que se llama el subnivel de MAC (Medium Access Control, o control de acceso al medio). Es muy importante en las LANs, que normalmente usan canales de broadcast.

BROADCAST.- transmisión de un paquete que será recibido por todos los dispositivos en una red.

C

CABLE SPT (PAR TRENZADO BLINDADO) .- con una única protección alrededor de todos los alambres. Este cable es muy común. Es aún algo flexible y no es muy costoso. Las posibilidades de interferencias de radio son reducidas.
CABLE UTP (Unshielded Twisted Pair, par trenzado no apantallado).- Es el más simple y empleado, sin ningún tipo de pantalla adicional y con una impedancia característica de 100 Ohmios. El conector más frecuente con el UTP es el RJ45, aunque también puede usarse otro (RJ11, DB25,DB11,etc), dependiendo del adaptador de red. cable par trenzado es de los más antiguos en el mercado y en algunos tipos de aplicaciones es el más común. Consiste en dos alambres de cobre o a veces de aluminio, aislados con un grosor de 1 mm aproximado. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multipares de pares trenzados (de 2, 4, 8, hasta 300 pares).

CABLEADO ESTRUCTURADO.- El cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

CABLEADO HORIZONTAL.- es el cableado que se extiende desde el armario de telecomunicaciones o Rack hasta la estación de trabajo

CABLEADO VERTICAL.- permite la interconexión de cada una de las redes de datos

COMPUTADOR.- Una computadora (del inglés computer, y éste del latín computare -calcular-), también denominada ordenador o computador, es una máquina electrónica que recibe y procesa datos para convertirlos en información útil. Una computadora es una colección de circuitos integrados y otros componentes relacionados que puede ejecutar con exactitud, rapidez y de acuerdo a lo indicado por un usuario o automáticamente por otro programa, una gran variedad de secuencias o rutinas de instrucciones que son ordenadas, organizadas y sistematizadas en función a una amplia gama de aplicaciones prácticas y precisamente determinadas, proceso al cual se le ha denominado con el nombre de programación y al que lo realiza se le llama programador.
CONTROL DE FLUJO.- hay controles de flujo de parada y espera o de ventana deslizante . El control de flujo es necesario en varios protocolos o capas , ya que el problema de saturación del receptor se puede producir en cualquier capa del protocolo .

D

DIRECCIONAMIENTO.- cada estación o dispositivo intermedio de almacenamiento debe tener una dirección única. A su vez, en cada terminal o sistema final puede haber varios agentes o programas que utilizan la red, por lo que cada uno de ellos tiene asociado un puerto.
DOMINIO DE BROADCAST.- Es un área lógica en una red de ordenadores en la que cualquier ordenador conectado a la red puede transmitir directamente a cualquier otro en el dominio sin precisar ningún dispositivo de encaminamiento, dado que comparten la misma subred, dirección de puerta de enlace y están en la misma VLAN (VLAN por defecto o instalada).

E

ESTÁNDARES PARA REDES DE LA IEEE:

ETHERNET.- Ethernet es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama descrito más abajo, aunque no tenga CSMA/CD como método de acceso al medio.

F

FIBRA OPTICA MULTIMODO.- La fibra óptica multimodo es adecuada para distancias cortas, como por ejemplo redes LAN o sistemas de video vigilancia. Su nombre proviene del hecho de que transporta múltiples modos de forma simultánea, ya que este tipo de fibra se caracteriza por tener un diámetro del núcleo mucho mayor que las fibras monomodo.

I

IEEE 802.1 .-Estándar que especifica la relación de los estándares IEEE y su interacción con los modelos OSI de la ISO, así como las cuestiones de interconectividad y administración de redes.

IEEE 802.12.- Se prevé la posibilidad de que el Fast EtherNet, adémdum de 802.3, se convierta en el IEEE 802.12.

IEEE 802.2 .- Control lógico de enlace (LLC), que ofrece servicios de "conexión lógica" a nivel de capa 2.

IEEE 802.3 10Base2.- Este estándar describe un bus de red el cual puede transmitir datosa una velocidad de 10 Mbs sobre un cable coaxial de banda base del tipo Thin en una distancia máxima de 200 mts.

IEEE 802.3 10Base5.- El estándar para bus IEEE 802.3 originalmente fue desarrollado para cable coaxial de banda base tipo Thick como muna norma para EtherNet, especificación a la cual se hace referencia como 10Base5 y describe un bus de red de compuesto por un cable coaxial de banda base de tipo thick el cual puede transmitir datos a una velocidad de 10Mbs. sobre un máximo de 500 mts.

IEEE 802.3 10BaseT.- Este estándar describe un bus lógico 802.3 CSMA/CD sobre un cableado de 4 pares trenzados el cual esta configurado físicamente como una estrella distribuida, capas de transmitir datos a 10 Mbs en un máximo de distancia de 100 mts.

IEEE 802.3 STARLAN.- El comité IEEE 802 desarrllo este estándar para una red con protocolo CSMA el cual hace uso de una topología de estrella agrupada en la cual las estrellas se enlazan con otra.

IEEE 802.3.- El comité de la IEEE 802. 3 definió un estándar el cual incluye el formato del paquete de datos para EtherNet, el cableado a usar y el máximo de distancia alcanzable para este tipo de redes.

IEEE 802.4 .-Define una red de topología usando el método de acceso al medio de Token Paassing.

IEEE 802.5 Token Ring.- Este estándar define una red con topología de anillo la cual usa token (paquete de datos) para transmitir información a otra.

IEEE 802.6.- Red de área metropolitana (MAN), basada en la topologia popuesta por la University of Western Australia, conocida como DQDB (Distribuited Queue Dual Bus) DQDB utiliza un bus dual de fibra óptica como medio de transmisión.

INTERNET.- Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

L

LAS REDES.- interconectan computadoras con distintos sistemas operativos, ya sea dentro de una empresa u organización (LANs) o por todo el mundo (WANs, Internet).

P

PROTOCOLO.- es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.
PUERTO SERIAL.- Es una interfaz de comunicaciones de datos digitales, frecuentemente utilizado por computadoras y periféricos, en donde la información es transmitida bit a bit enviando un solo bit a la vez, en contraste con el puerto paralelo que envía varios bits simultáneamente.
PUERTO.- En la informática, un puerto es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir. Dicha interfaz puede ser de tipo físico, o puede ser a nivel de software (por ejemplo, los puertos que permiten la transmisión de datos entre diferentes ordenadores) (ver más abajo para más detalles), en cuyo caso se usa frecuentemente el término puerto lógico.

R

RED LAN.- es la abreviatura de Local Area Network (Red de Área Local o simplemente Red Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc; para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

RED WAN.- acrónimo de la expresión en idioma inglés Wide Area Network, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

ROUTER.- El enrutador (calco del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

S

SERVIDOR.- En informática, un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.
SWITCH.- Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

T

TOPOLOGÍA ESTRELLA EXTENDIDA.- La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

U

UN RACK (O SOPORTE METÁLICO).- Es una estructura de metal muy resistente, generalmente de forma cuadrada de aproximadamente 3 mts de alto por 1 mt de ancho, en donde se colocan los equipos regeneradores de señal y los Patch-Panels, estos son ajustados al rack sobre sus orificios laterales mediante tornillos.

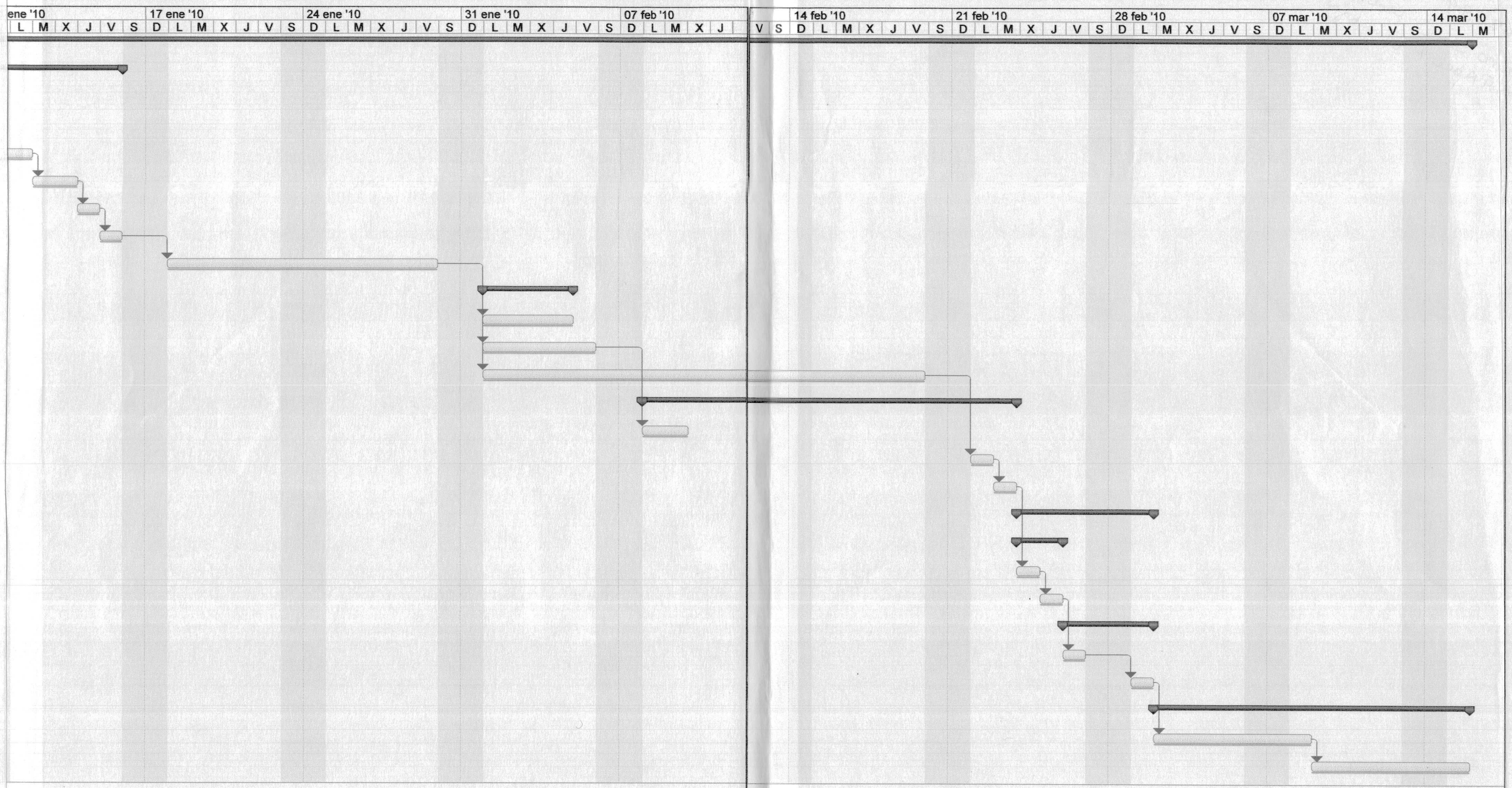
V

VLAN.- Acrónimo de Virtual LAN, 'red de área local virtual', es un método de crear redes lógicamente independientes dentro de una misma red física.

ANEXOS

45 GRÁFICA DE GANTT

Id	Nombre de tarea	Duración	Comienzo	Prede	Fin
1	**PROYECTO SENEFELDER**	**51 días**	**lun 04/01/10**		**lun 15/03/10**
2	**FASE DE ANÁLISIS DE LAN Y WAN**	**10 días**	**lun 04/01/10**		**vie 15/01/10**
3	Recopilación de datos	2 días	lun 04/01/10		mar 05/01/10
4	Analizar la situación actual de la red lan	2 días	mié 06/01/10	3	jue 07/01/10
5	Proponer soluciones	2 días	vie 08/01/10	4	lun 11/01/10
6	Cotización de dispositivos de conmutación y	2 días	mar 12/01/10	5	mié 13/01/10
7	Elaborar la propuesta	1 día	jue 14/01/10	6	jue 14/01/10
8	Presentar la propuesta	1 día	vie 15/01/10	7	vie 15/01/10
9	Aceptacion de la propuesta	10 días	lun 18/01/10	8	vie 29/01/10
10	**FASE DE DISEÑO DE LA RED**	**4 días**	**lun 01/02/10**		**jue 04/02/10**
11	Diseño WAN	4 días	lun 01/02/10	9	jue 04/02/10
12	compra de Dispositivos LAN	5 días	lun 01/02/10	9	vie 05/02/10
13	Compra de Equipos Wan	15 días	lun 01/02/10	9	vie 19/02/10
14	**FASE DE IMPLEMENTACIÓN**	**12 días**	**lun 08/02/10**		**mar 23/02/10**
15	Implementacion dispositivos Lan	2 días	lun 08/02/10	12	mar 09/02/10
16	Enlace Wan MATRIZ-Quito	1 día	lun 22/02/10	13	lun 22/02/10
17	Enlace Wan MATRIZ_Sucursal	1 día	mar 23/02/10	16	mar 23/02/10
18	**Fase de Prueba**	**4 días**	**mié 24/02/10**		**lun 01/03/10**
19	**Prueba Lan**	**2 días**	**mié 24/02/10**		**jue 25/02/10**
20	Prueba de configuración de	1 día	mié 24/02/10	17	mié 24/02/10
21	Prueba de configuración de	1 día	jue 25/02/10	20	jue 25/02/10
22	**Prueba Wan**	**2 días**	**vie 26/02/10**		**lun 01/03/10**
23	Prueba enlace Wan Matriz-Quito	1 día	vie 26/02/10	21	vie 26/02/10
24	Prueba enlace Wan Matriz-Cuenca	1 día	lun 01/03/10	23	lun 01/03/10
25	**FASE DE DOCUMENTACIÓN**	**10 días**	**mar 02/03/10**		**lun 15/03/10**
26	Elaborar Documentación de Configuraciones Lan	5 días	mar 02/03/10	24	lun 08/03/10
27	Elaboración de Documentación Wan	5 días	mar 09/03/10	26	lun 15/03/10



Proyecto: gran_topico
Fecha: mar 22/06/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito exteTarea
División

Proyecto: gran_topico
Fecha: mar 22/06/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito exteTarea
División

Proyecto: gran_topico
Fecha: mar 22/06/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito exteTarea
División

```
PAGE   1
// JOB
LOG DRIVE   CART SPEC   CART AVAIL  PHY DRIVE
   0000         000F        000F        0000
V2 M10   ACTUAL  8K  CONFIG  8K
// XEQ PCS     10
*FILES(1,NETID),(2,CALEN),(3,SYRED),(4,SYREG),(5,SYOUR),
*FILES(202,DIREC),(203,PROCS),(204,PWIWI),(205,WIWIW),(208,MILES)
*LOCALDELFI,DMF,MPWIF
*LOCALFLOOK,PRNTZ,PRNZ,WRTYZ
*LOCALLSLF,COMLS,PRNTZ,PRNZ
*LOCALPRPT,CNTRL,DDT,CALSD,CALSF,WRTYZ
*LOCALRESAG,DRP,DRTC,OP,HPP
*LOCALSR,DATSW,NEWLN,VASIT
*LOCALWSP,VASIJ,ALPMO,NEWLN,PRNZ
*LOCALZPWIF,PRNTZ,PRNZ

A       G
B2525    2JAN80  2JAN80 PROYECTO DE CONSTRUCCION DE LINEA DE 69 KV     2JAN80 1
C2525   1  1JAN80   1MAY80 24MAY80 24JUL80 10AUG80   90CT80 120CT80   2NOV80   3NOV80
C2525   1 25DEC80   1JAN81   1MAY81 24MAY81 24JUL81 10AUG81   90CT81 120CT81   2NOV81
C2525   1  3NOV81 25DEC81   1JAN82   1MAY82 24MAY82 24JUL82 10AUG82   90CT82 120CT82
     0  0  0    0  0    0  0    0  0    0  0    0  0    0  0    0  0    0  0    0  0
 ERROR 12041     TYPE  I
THERE ARE     27 HOLIDAYS + NON-WORK DAYS FOR NET  2525
    IN DAY NUMBERS FROM 01 MAR 64 (HOLIDAYS ARE POSITIVE,SPEC. DAYS ARE NEG.), AS FOLLOWS-
  5784  5905  5928  5989  6006  6066  6069  6090  6091  6143  6150  6270  6293  6354  6371  6431  6434  6455  6456  6508
  6515  6635  6658  6719  6736  6796  6799
D          1 GERENTE GENERAL      2 GERENTE TECNICO      3 ING SUPERVISOR
D          4 CONT TOPOGRAFIA      5 ASESOR JURIDICO      6 CONT DISENO
D          7 CONT CONSTRUC.       8 CONT POSTES          9 BODEGUERO
D         10 CONT MAT LOCAL.     11 CONT MAT IMPORT     12 GRUA
D         13 TRAYLER             14 GRUPO A             15 GRUPO B
D         16 GRUPO C             17 GRUPO D             18 GRUPO E
D         19 GRUPO F             20 GRUPO G1            21 GRUPO G2
D         22 GRUPO H             23 GRUPO I             24 GRUPO J
D         25 GRUPO K1            26 GRUPO K2            27 GRUPO L
D         28 GRUPO M             0                      0
E        1    PLANIFICACION      1    2    3    4    5   14   15    0    0    0
E        2    DISENO             1    2    6   16    0    0    0    0    0    0
E        3    ADQ MATERIALES     1    2    5   17    0    0    0    0    0    0
E        4    CONSTRUCCION       6    8    9   12   13    0    0    0    0    0
F2525      0    0  0    0 0                    0    0    4    4 5 44    7 7
G2525    0000001 COMIENZO DEL PROYECTO                                  00500
G2525    0000002 PLANEACION DEL PROYECTO                              1500510
G2525    0000003 APROBACION PRESUPUESTO INICIAL                       1500510
G2525    0000100 SELECCION CONTRATISTA LEVANTAMIENTO TOPOGRA.         1000510
G2525    0000160 OBTENCION MAPAS INST. GEOGRAFICO MILITAR              500510
G2525    0000170 ESTUDIO DE PROYECCION DE LA DEMANDA                  6000510
G2525    0000180 CONTRATO ESTUDIO TOPOGRAFICO                          300510
G2525    0000200 SELECCION EN PAPEL RUTAS PRELIMINARES                 300510
G2525    0000300 RECONOCIMIENTO DEL TERRENO RUTAS PRELIMINAR.          300510
G2525    0000400 OBTENCION PERMISOS DERECHO DE VIA                    3000510
G2525    0000500 TRAZADO PRELIMINAR RUTA SELECCIONADA                 4500510
G2525    0000600 TRAMITAR INDEMNIZACIONES                             6000510
G2525    0000700 PRESENTACION LEVANT. TOPOGRAF. PRELIMINAR             100510
G2525    0000800 FIJACION DEFINITIVA DE LA RUTA                        300510
G2525    0000900 FICTICIA                                               00000
G2525    0001000 ELABORACION INFORME DE FACTIBILIDAD                  1500510
G2525    0001100 APROBACION INFORME DE FACTIBILIDAD                    300510
G2525    0001200 APROBACION PRESUPUESTO DE DISENO                     1500510
G2525    0001300 LEVANTAMIENTO TOPOGRAFICO RUTA DEFINITIVA            8400510
G2525    0001400 ELABORACION PLANOS Y CALCULO LIBRETA                 1000510
G2525    0001500 PRESENTACION ESTUDIO LEVANT. TOPOGRAFICO              100510
```

```
G2525    0001600 APROBACION ESTUDIO TOPOGRAFICO                    300510
G2525    0001700 PREPARACION DOCUMENTOS CONTRATO DE DISENO        1000510
G2525    0001800 OBTENCION FINANCIACION DE LA CONSTRUCCION        6000510
G2525    0001900 CONCURSO DE OFERTAS DISENO DE LINEA              4000510
G2525    0002000 PRESENTACION DE OFERTAS                           100510
G2525    0002100 ANALISIS Y ADJUDICACION CONTRATO DE DIDENO        500510
G2525    0002200 ELABORACION DISENO MECANICO Y ELECTRICO          3000510
G2525    0002300 PRESENTACION DISENO                               100510
G2525    0002350 APROBACION DE FINANCIACION PARA CONSTRUCCION      300510
G2525    0002400 APROBACION DISENO                                 300510
G2525    0002600 PREPARACION DOCUMENTOS COMPRA MATER. LOCALES     1700510
G2525    0002700 PREPARACION DOCUMENTOS COMPRA MATER. IMPORT.     1700510
G2525    0002800 PREPARACION DOCUMENTOS CONTRATO CONST. LINEA     1000510
G2525    0002900 PREPARACION DOCUMENTOS COMPRA DE POSTES          1700510
G2525    0003000 LICITACION MATERIALES LOCALES                    3500510
G2525    0003100 LICITACION MATERIALES IMPORTACION                3500510
G2525    0003200 LICITACION CONSTRUCCION DE LINEA                 6000510
G2525    0003300 LICITACION POSTES                                3500510
G2525    0003400 ANALISIS DE OFERTAS MATERIALES LOCALES            500510
G2525    0003500 ANALISIS DE OFERTAS MATERIALES IMPORTACION        500510
G2525    0003600 ANALISIS Y ADJUDICACION CONTRATO CONSTRUC.       1000510
G2525    0003700 ANALISIS DE OFERTAS DE POSTES                     500510
G2525    0003800 ADJUDICACION DE OFERTAS Y CONTRATO MAT LOCAL     1000510
G2525    0003950 FABRICACION ENTREGA Y RECEPCION MAT LOCALES      9000510
G2525    0003900 ADJUDICACION DE OFERTAS Y CONTRATO MAT IMPOR     1000510
G2525    0003950 FABRICACION ENTREGA Y RECEPCION MAT IMPORT.     12000510
G2525    0004000 ADJUDICACION DE OFERTAS Y CONTRATO DE POSTES     1000510
G2525    0004100 FABRICACION DE POSTES                           12000510
G2525    0004200 OBTENCION VIVIENDA Y BODEGA DE CAMPO              500510
G2525    0004300 REPLANTEO DE LA RUTA                             8400510
G2525    0004400 TRASLADO DE PERSONAL                              100510
G2525    0004500 DESBROCE DE LA RUTA                              7000510
G2525    0004600 INSTALACION DE FAENAS                             100510
G2525    0004700 EXCAVACION                                       6600510
G2525    0004800 TRANSPORTE Y REGADO DE POSTES                    8000510
G2525    0004900 TRANSPORTE DE MATERIALES                        15200510
G2525    0005000 PARADA DE POSTES Y PUESTA A TIERRA               7820510
G2525    0005100 EXCAVACION Y ARMADO DE TENSORES                  5500510
G2525    0005200 VESTIDO DE POSTES                                6500510
G2525    0005300 TENDIDO CABLE DE GUARDIA                         8400510
G2525    0005400 TENDIDO DE CONDUCTORES                          16800510
G2525    0005500 REVISION FINAL                                   3500510
G2525    0005600 ENTREGA DE LA LINEA                               100510
G2525    0005700 FIN DEL PROYECTO                                   00500
H  0*                                                               00000
H2525    0000002  0000001        0*          0*          0*
H2525    0000003  0000002        0*          0*          0*
H2525    0000100  0000003        0*          0*          0*
H2525    0000160  0000003        0*          0*          0*
H2525    0000170  0000003        0*          0*          0*
H2525    0000180  0000100        0*          0*          0*
H2525    0000200  0000160        0*          0*          0*
H2525    0000300  0000180        0*  0000200 0*          0*
H2525    0000400  0000300        0*          0*          0*
H2525    0000500  0000300        0*          0*          0*
H2525    0000600  0000400 SP 2000*          0*          0*
H2525    0000700  0000500        0*          0*          0*
H2525    0000800  0000600        0*  0000700 0*          0*
H2525    0000900  0000170        0*          0*          0*
H2525    0001000  0000800        0*  0000900 0*          0*
H2525    0001100  0001000        0*          0*          0*
H2525    0001200  0001100        0*          0*          0*
H2525    0001300  0001200        0*          0*          0*
H2525    0001400  0001300        0*          0*          0*
H2525    0001500  0001400        0*          0*          0*
H2525    0001600  0001500        0*          0*          0*
H2525    0001700  0001600        0*          0*          0*
H2525    0001800  0001600        0*          0*          0*
H2525    0001900  0001700        0*          0*          0*
H2525    0002000  0001900        0*          0*          0*
H2525    0002100  0002000        0*          0*          0*
H2525    0002200  0002100        0*          0*          0*
H2525    0002300  0002200        0*          0*          0*
H2525    0002350  0001800        0*          0*          0*
H2525    0002400  0002300        0*  0002350 0*          0*
H2525    0002600  0002400        0*          0*          0*
H2525    0002700  0002400        0*          0*          0*
H2525    0002800  0002400        0*          0*          0*
H2525    0002900  0002400        0*          0*          0*
H2525    0003000  0002600        0*          0*          0*
```


SISTEMAS DE CONTROL C. A.
SISTEMAS DE CONTROL C. A.

H2525	0003100	0002700		0.				0.			0.				
H2525	0003200	0002800		0.				0.			0.				
H2525	0003300	0002900		0.				0.			0.				
H2525	0003400	0003000		0.				0.			0.				
H2525	0003500	0003100		0.				0.			0.				
H2525	0003600	0003200		0.				0.			0.				
H2525	0003700	0003300		0.				0.			0.				
H2525	0003800	0003400		0.				0.			0.				
H2525	0003850	0003800		0.				0.			0.				
H2525	0003900	0003500		0.				0.			0.				
H2525	0003950	0003900		0.				0.			0.				
H2525	0004000	0003700		0.				0.			0.				
H2525	0004100	0004000		0.				0.			0.				
H2525	0004200	0003600		0.				0.			0.				
H2525	0004300	0003600		0.				0.			0.				
H2525	0004400	0004200		0.				0.			0.				
H2525	0004500	0004300	SP	600.				0.			0.				
H2525	0004600	0004400		0.	0004500			0.			0.				
H2525	0004700	0004600		0.				0.			0.				
H2525	0004800	0004100	SP	4000.				0.			0.				
H2525	0004900	0003850		0.	0003950			0.	0004600		0.				
H2525	0005000	0004800	SP	1070.	0004700	SP	1000.	0.			0.				
H2525	0005100	0004900	SP	8000.	0005000	SP	2500.	0.			0.				
H2525	0005200	0005100	SP	500.				0.			0.				
H2525	0005300	0005200	SP	3000.				0.			0.				
H2525	0005400	0005300	SP	3000.				0.			0.				
H2525	0005500	0005400		0.				0.			0.				
H2525	0005600	0005500		0.				0.			0.				
H2525	0005700	0005600		0.				0.			0.				
K 0*				0.				0.			0.				

K2525	0000002	10	10	20	10	00	0	00	0	0.
K2525	0000003	10	10	00	0	00	0	00	0	0.
K2525	0000100	10	10	20	10	00	0	00	0	10000.
K2525	0000160	140	10	00	0	00	0	00	0	1000.
K2525	0000170	140	10	00	0	00	0	00	0	0.
K2525	0000180	10	10	40	10	50	10	00	0	0.
K2525	0000200	20	10	140	10	00	0	00	0	0.
K2525	0000300	30	10	40	10	20	10	00	0	15000.
K2525	0000400	50	10	00	0	00	0	00	0	0.
K2525	0000500	40	10	150	10	00	0	00	0	201600.
K2525	0000600	50	10	00	0	00	0	00	0	300000.
K2525	0000700	40	10	00	0	00	0	00	0	0.
K2525	0000800	20	10	30	10	00	0	00	0	0.
K2525	0001000	140	10	00	0	00	0	00	0	0.
K2525	0001100	10	10	20	10	00	0	00	0	0.
K2525	0001200	10	10	00	0	00	0	00	0	0.
K2525	0001300	40	10	150	10	00	0	00	0	546000.
K2525	0001400	40	10	150	10	00	0	00	0	151200.
K2525	0001600	10	10	20	10	00	0	00	0	0.
K2525	0001700	10	10	20	10	50	10	00	0	10000.
K2525	0001800	10	10	00	0	00	0	00	0	0.
K2525	0001900	10	10	50	10	00	0	00	0	20000.
K2525	0002100	10	10	20	10	50	10	170	10	0.
K2525	0002200	60	10	160	10	00	0	00	0	756000.
K2525	0002400	10	10	20	10	00	0	00	0	0.
K2525	0002600	10	10	20	10	00	0	00	0	0.
K2525	0002700	10	10	20	10	00	0	00	0	0.
K2525	0002800	10	10	20	10	50	10	00	0	0.
K2525	0002900	10	10	20	10	00	0	00	0	0.
K2525	0003000	170	10	00	0	00	0	00	0	10000.
K2525	0003100	170	10	00	0	00	0	00	0	10000.
K2525	0003200	170	10	00	0	00	0	00	0	20000.
K2525	0003300	170	10	00	0	00	0	00	0	10000.
K2525	0003400	10	10	170	10	00	0	00	0	0.
K2525	0003500	10	10	170	10	00	0	00	0	0.
K2525	0003600	170	10	10	10	20	10	00	0	0.
K2525	0003700	10	10	170	10	00	0	00	0	0.
K2525	0003800	170	10	10	10	50	10	00	0	0.
K2525	0003850	100	10	90	10	00	0	00	0	*********
K2525	0003900	170	10	10	10	50	10	00	0	0.
K2525	0003950	110	10	90	10	00	0	00	0	3172120.
K2525	0004000	170	10	10	10	50	10	00	0	0.
K2525	0004100	80	10	00	0	00	0	00	0	6705061.
K2525	0004200	70	10	00	0	00	0	00	0	30000.
K2525	0004300	40	10	150	10	00	0	00	0	168000.
K2525	0004400	30	10	70	10	00	0	00	0	2000.
K2525	0004500	70	10	190	10	00	0	00	0	252000.
K2525	0004600	30	10	70	10	00	0	00	0	0.
K2525	0004700	70	10	200	10	210	10	00	0	0.
K2525	0004800	80	10	120	10	130	10	180	10	609400.

```
K2525    0024900     70  10    30  10    230  10    90  10    492450.
K2525    0005000     70  10    30  10    220  10   120  10   2717900.
K2525    0005100     70  10    30  10    240  10    00   0    385000.
K2525    0005200     70  10    30  10    250  10   260  10    684250.
K2525    0005300     70  10    30  10    270  10    00   0    504000.
K2525    0005400     70  10    30  10    280  10    00   0   5439421.
K2525    0005500     70  10    30  10     00   0    00   0     34000.
K2525    0005600     10  10    70  10     00   0    00   0         0.
L    0*              00   0    00   0     00   0    00   0         0.
L2525    0000001 0 COMIENZO DEL PROYECTO
L2525    0001100 0 APROBACION INFORME DE FACTIBILIDAD
L2525    0002400 0 APROBACION DISENO
L2525    0004600 0 INSTALACION DE FAENAS
L2525    0005700 0 FIN DEL PROYECTO
    0*           0
```