ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Escuela de Diseño y Comunicación Visual

Proyecto de Graduación

Previo a la obtención del título de:

Analista de Soporte en Microcomputadores y Programador de Sistemas

Tema:

ESTRUCTURA DE REDES CAMPUS LAS PEÑAS DE LA ESPOL

Manual de Usuario y Configuraciones

Autores:

Manuel Barzola

José Fuentes

Sofía Delgado

Director

Anl. Fabián Barboza

Año 2006

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
ANALISTA DE SOPORTE EN MICROCOMPUTADORES
Y
PROGRAMADOR DE SISTEMAS

TEMA:

ESTRUCTURA DE REDES CAMPUS LAS PEÑAS DE LA ESPOL

MANUAL DE USUARIO Y CONFIGURACIONES

AUTORES:

MANUEL BARZOLA
JOSÉ FUENTES
SOFÍA DELGADO

DIRECTOR:

ANL. FABIÁN BARBOZA

AÑO

2006

AGRADECIMIENTO

A Dios, ya que gracias a el puedo estar en este momento tan importante para mi, a mis padres, ya que gracias a su preocupación, comprensión y amor, ayudaron para que este sueño se haga realidad.
A Rafaela Suquitana, una persona muy especial en mi vida, sin ella fuera difícil haber escrito este agradecimiento.

Manuel Eduardo Barzola Sarmiento

AGRADECIMIENTO

A Dios, por mantenerme sano y dotarme de inteligencia para poder cumplir todo lo que me he propuesto hasta ahora. Por darme tantas alegrías y sentir su amor por medio de las personas que me rodean.
A mi madre Aracely Herrera León que ha sido mi único pilar para conseguir entre otras cosas este Título que con su amor infinito supo guiarme, corregirme y darle sentido a mis esfuerzos.
Gracias mami por tolerar mi mal genio y mi vicio deportivo.
A mi padre por entender todo el tiempo que no pude compartir con él.
A todas las personas que siempre me aconsejaron y llegaron a encontrar un lugar junto a mis padres en mi corazón: Ma. Leonor Proaño, Gilda Gómez, Lidia Martillo, Zoila y Fresia Fuentes, entre otras.
A mis compañeros y amigos, por sus palabras de aliento y su apoyo incondicional: Luís, Ma. De los Ángeles, Evelyn, Erick, Johanna, Jacobo, Priscila, Victor, Silvana, Enzo, Karen, José, Karina, Ronald, Liliana, William, Lorena y especialmente a Manuel y Sofía.

José Stalin Fuentes Herrera

AGRADECIMIENTO

A mi esposo e hijas Adrianita e Isabella, que han soportado y ayudado todo el tiempo que no he podido compartir con ellos por lograr ésta meta.

A mis padres y hermanas que siempre me apoyaron y confiaron en mi capacidad para poder lograr éste gran paso.

Sofia Valentina Delgado Aumala

DEDICATORIA

Dedicar a alguien un trabajo así es difícil, ya que gracias a el, he conocido personas muy importante en mi vida, se lo dedico a todos mis compañeros de tópido, a mis familiares y especialmente a mi madre Ana Sarmiento.

Manuel Eduardo Barzola Sarmiento

DEDICATORIA

A mi madre Aracely Herrera León, por ser la jefa de familia quien tuvo que vigilar por el cuidad, sustento, alimentación, educación y formación de Rosita y mío, a ella va dedicado todo este esfuerzo y triunfo profesional. Gracias mami.

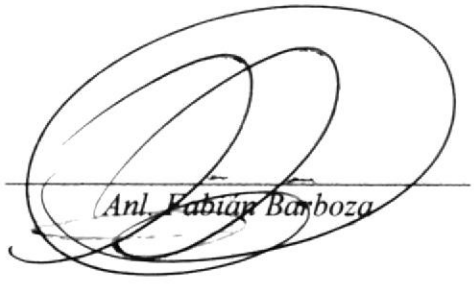
José Fuentes Herrera

DEDICATORIA

A mi esposo, a mis hijas Adrianita e Isabellita, a mis padres Luís Fernando y Juanita Mercedes, y a mis hermanas Katherine, Micaela, Valeria y Alejandra.

Sofía Valentina Delgado Aumala

FIRMA DEL DIRECTOR DEL TÓPICO DE GRADUACIÓN



FIRMA DE LOS AUTORES DEL TÓPICO DE GRADUACIÓN

Manuel Eduardo Barzola Sarmiento

José Stalin Fuentes Herrera

Sofia Valentina Delgado Aumala

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

CAPÍTULO 2 SITUACIÓN ACTUAL

CAPÍTULO 3 SOLUCIÓN PROPUESTA

CAPÍTULO 4 IMPLEMENTACIÓN WAN Y LAN

CAPÍTULO 5 CONFIGURACIÓN DE DISPOSITIVOS

CAPÍTULO 6 CONFIGURACIONES LINUX

ÍNDICE DE TABLAS

CAPÍTULO 3 SOLUCIÓN PROPUESTA

CAPÍTULO 4 CONFIGURACIÓN DE ROUTERS

CAPÍTULO 1

GENERALIDADES

1. GENERALIDADES

1.1 INTRODUCCIÓN

El presente manual de usuario, ha sido elaborado producto de la investigación del análisis de la estructura de la red del Campus Las Peñas de la ESPOL, y a su vez mejorar su infraestructura LAN y optimizar recursos en lo referente a su comunicación WAN.

1.2 A QUIÉN VA DIRIGIDO ÉSTE MANUAL

Éste manual se dirige a los responsables, supervisores y usuarios finales relacionados con el manejo de las redes en el campus Las Peñas de la ESPOL, para ello se detalla sugerencias prácticas basadas en instrucciones que guían a los usuarios brindándoles la forma de operar los dispositivos de enrutamiento, y el arreglo rápido y oportuno de algún inconveniente físico en la red.

En éste manual se ha procurado utilizar un lenguaje flexible, con la perspectiva que tanto personal administrativo y técnico de cada unidad en el campus Las Peñas, pueda involucrarse de manera simple, rápida y oportuna en la comprensión de la estructura de la red del campus las Peñas.

1.3 ¿POR QUÉ ÉSTE MANUAL?

El presente manual contiene una descripción detallada de las configuraciones de los dispositivos de enrutamiento, para poder de manera oportuna conocer como se encuentran comunicados los campus, y a su vez monitorear el rendimiento de la misma.

En resumen, éste manual se diseñó con el objetivo de plantear recomendaciones, en la estructura de la red en el campus Las Peñas, y así poder mantener la información correcta para poder solucionar posibles errores ya sea en comunicación lógica y física.

1.4 ORGANIZACIÓN DEL CONTENIDO DE ÉSTE MANUAL

El manual de usuario contiene una serie de capítulos, los cuales brindan conocimiento de la estructura de la red del Campus las Peñas, y a su vez soluciones que ayuden a la mejor organización de ésta red, para poder monitorear los rendimientos y los accesos de cada unidad, con el transcurso notará que cada uno de los capítulos tiene un propósito específico.

El manual está dividido en 5 capítulos como se detalla a continuación

Capítulo 1 **Generalidades.**
Especifica el contenido del manual y como interpretarlo.

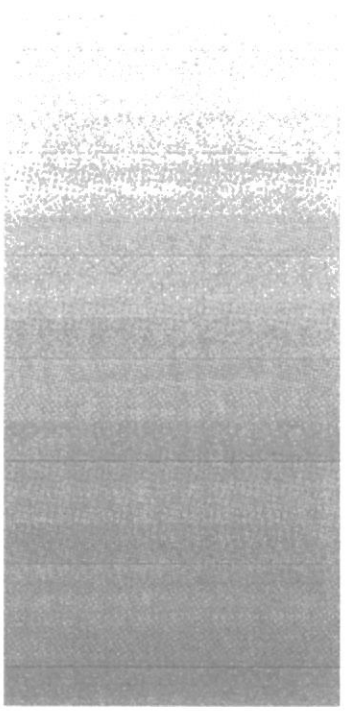
Capítulo 2 **Situación actual.**
La Situación actual del campus Las Peñas con todas sus unidades.

Capítulo 3 **Solución propuesta.**
Especifica las 2 alternativas producto del estudio de éste tópico de graduación.

Capítulo 4 **Implementación WAN y LAN.**
Indica la implementación a nivel de comunicaciones (WAN) y los diagramas de piso (LAN).

Capítulo 5 **Configuración de dispositivos.**
Especifica todas las configuraciones de los dispositivos indicados en la implementación WAN.

Capítulo 6 **Configuración de LINUX.**
Especifica todos los comandos LINUX que se desean implementar en la solución propuesta ofrecida.



CAPÍTULO 2

SITUACIÓN ACTUAL

2. SITUACIÓN ACTUAL

2.1 ANTECEDENTES

La ESPOL fue creada mediante Decreto Ejecutivo No. 1664 expedido por el Presidente de la República Dr. Camilo Ponce Enríquez, el 29 de octubre de 1958. Es una institución de educación superior, persona jurídica de derecho público, sin fines de lucro, autónoma en lo académico, científico, técnico, administrativo, financiero y económico, con capacidad para auto-regularse, buscar la verdad y formular propuestas para el desarrollo humano, sin más restricciones que las señaladas en la constitución y las leyes político y ambiental; hacer investigación, transferencia y extensión de calidad para servir a la sociedad".

La ESPOL inició sus actividades académicas en abril de 1959, con 51 alumnos, 15 profesores y 5 trabajadores. Desde sus inicios su vida académica se articuló a las necesidades del sector productivo y a los principios de la excelencia que requiere el desarrollo del Ecuador.

Las actividades académicas y de investigación se desarrollan en 6 Campus:

2.2 BREVE DESCRIPCIÓN DE CADA CAMPUS

2.2.1 CAMPUS GUSTAVO GALINDO

Tiene una extensión de 724 hectáreas, está ubicado en el Km. 30.5 de la vía Perimetral, es el asiento de la administración central y de la mayoría de las carreras de pregrado que oferta la ESPOL. Su moderna infraestructura es el resultado del Plan de Desarrollo 1983-1992 que se financió con el préstamo BIDESPOL II.

2.2.2 CAMPUS LAS PEÑAS

Tiene una extensión de 2.5 hectáreas, está ubicado al pie del más antiguo barrio de la ciudad. En este campus se realiza una amplia y diversificada vida académica que atiende tanto la formación de pregrado y postgrado, en cuanto a la actualización y mejoramiento profesional.

2.2.3 CENAIM

Está ubicado en San Pedro de Manglaralto, en la ruta del Sol de la Península de Santa Elena, su esfuerzo académico está orientado a potenciar la capacidad productiva del sector acuícola ecuatoriano y por ser un espacio académico internacional.

2.2.4 CAMPUS SANTA ELENA

Está ubicado en la cabecera del cantón del mismo nombre, oferta carreras vinculadas a las Tecnologías Pesquera (PROTEP), Computacional (EDCOM) y Lenguas.

2.2.5 CAMPUS DAULE

Esta ubicado en la parte urbana de dicha ciudad su principal actividad es la agrícola y muy pocas carreras técnicas.

2.2.6 CAMPUS SAMBORONDÓN

Ubicado en Samborondón donde funciona la unidad de EDCOM, cuenta con carreras técnicas como: Análisis de Sistemas y carreras modulares: Análisis de Soporte en Microcomputadores, Programación de Sistemas y Secretariado Ejecutivo.

2.3 MISIÓN

Desde hace más de 40 años contribuimos al desarrollo del Ecuador, formando profesionales idóneos, realizando las investigaciones que el país requiere y prestando los servicios que demanda el sector productivo.

Nuestra misión está cifrada en la obligación moral de preparar recursos humanos que puedan a través de sus gestiones lograr que Ecuador forme parte de la globalización en la que el mundo está inmerso.

2.4 VISIÓN

- Impartir enseñanza en ciencia y en áreas técnicas.
- Formar profesionales en las áreas científica y técnica de nivel superior necesarias para el desarrollo integral del país así como el desarrollar investigación en ciencia y tecnología.
- Efectuar difusión y extensión en las áreas científica y técnica de su competencia.
- Contribuir en la búsqueda de soluciones para la explotación y uso racional de los recursos naturales y energéticos, la preservación del medio ambiente y desarrollar una tecnología autónoma que aporte al mejoramiento de las condiciones de vida y la cultura de la sociedad ecuatoriana

2.5 SITUACIÓN ACTUAL CAMPUS LAS PEÑAS

De los 6 campus, únicamente en los campus Las Peñas y Prosperina existe comunicación realizada por VPN con un ancho de banda de 1 Mbps. En el backbone vertical del Campus Las Peñas, la conexión de los edificios A y G se realizan mediante fibra óptica monomodo a una velocidad de 1 Mb con núcleo 62 micrones, el bloque E del EDCOM se conecta mediante antena microonda unidireccional.

Para la ejecución de éste proyecto nos hemos centrado únicamente en la infraestructura de red del campus Las Peñas, a continuación detallamos las unidades que se encuentran en el campus Las Peñas.

2.6 BACKBONE HORIZONTAL

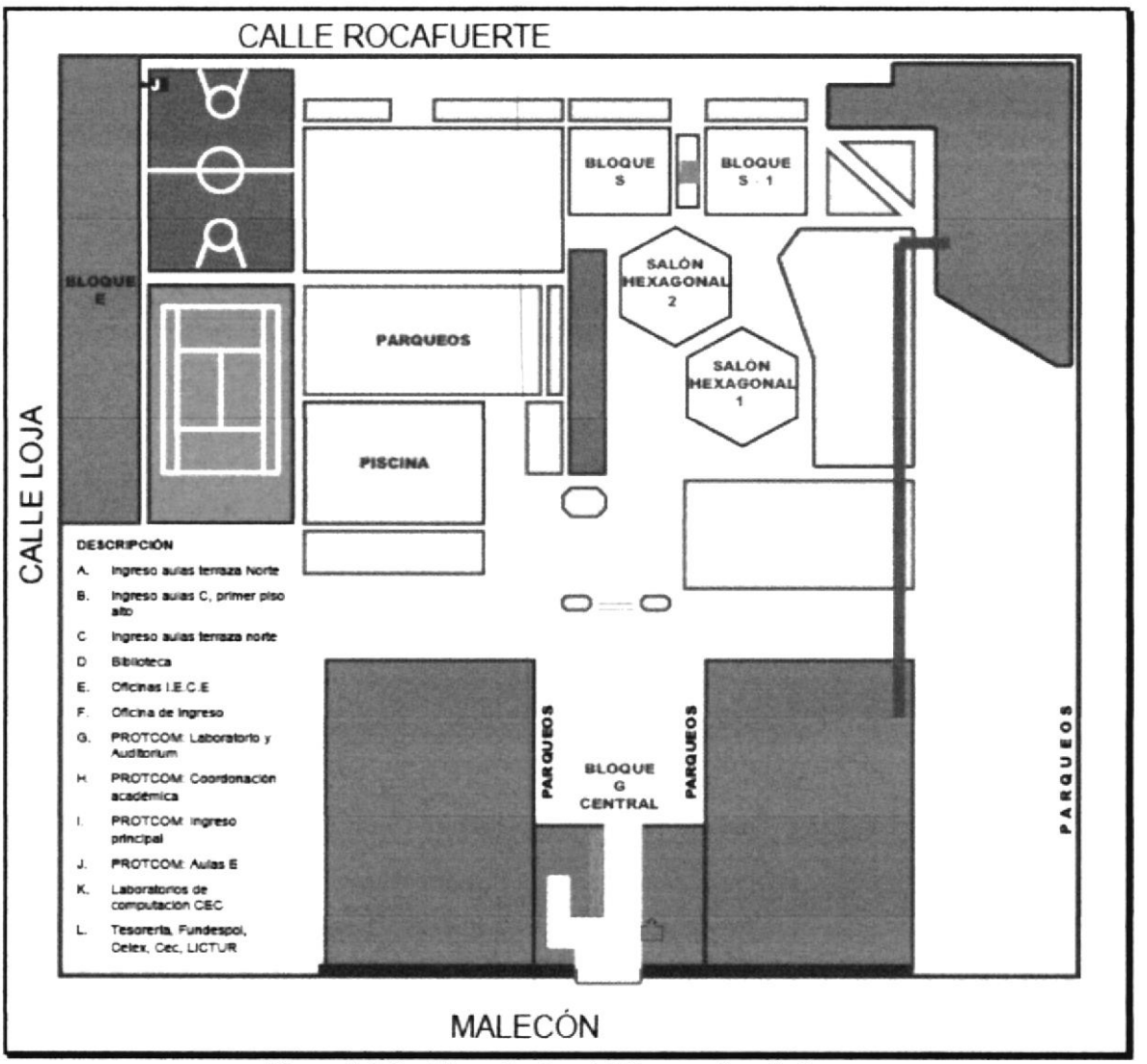


Figura 2.1 Backbone horizontal Campus Las Peñas

2.7 BACKBONE VERTICAL

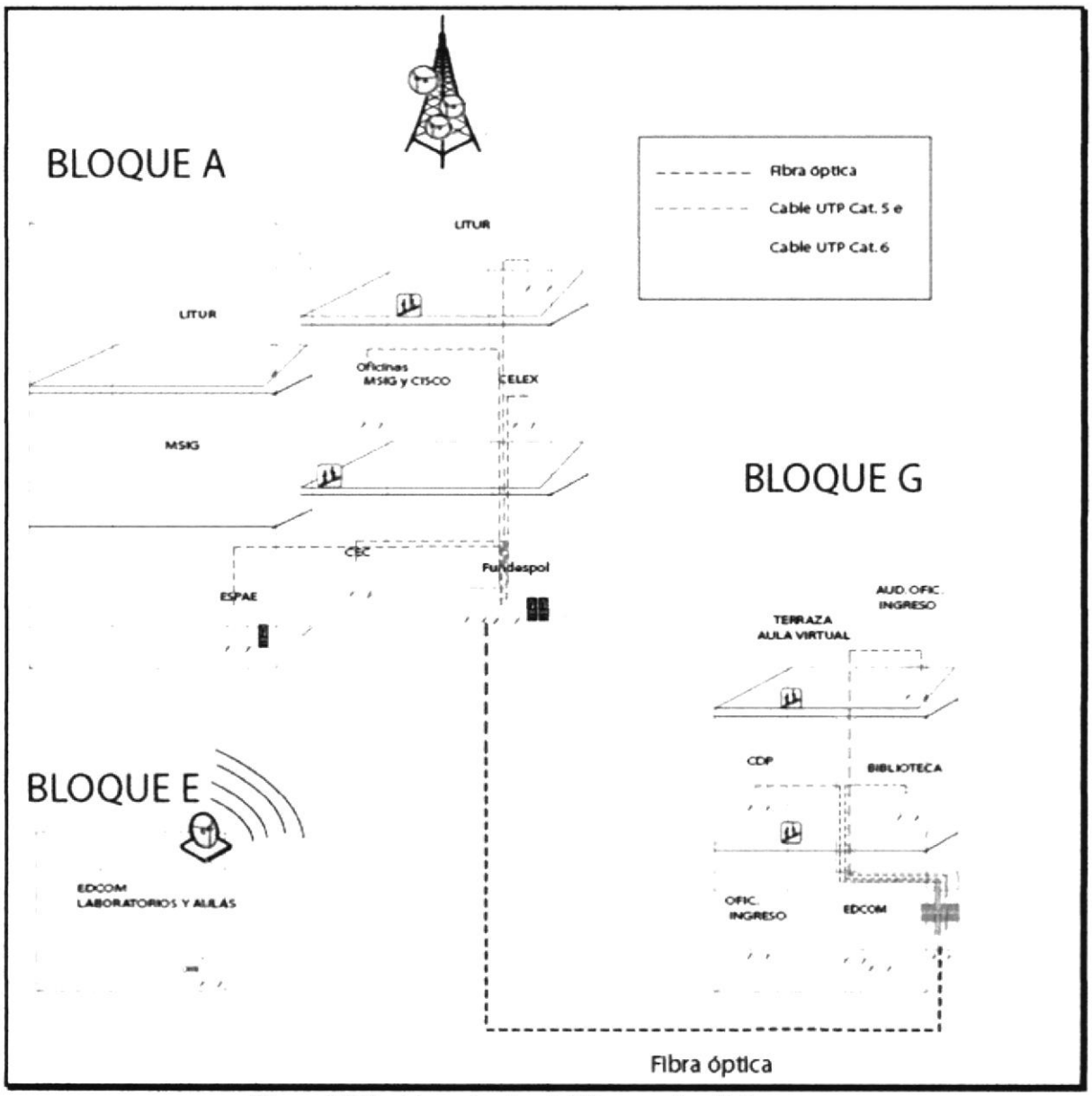


Figura 2.2 Backbone horizontal Campus Las Peñas

2.8 DETALLE SITUACIÓN ACTUAL UNIDADES CAMPUS LAS PEÑAS

2.8.1 FUNDESPOL

Existen 20 Pcs distribuidas en los diferentes departamentos tal como se lo aprecia en el diagrama de piso, actualmente posee una estructura física basada en cable UTP categoría 5 y 5E, en su cableado horizontal, el cableado llega hasta un rack ubicado en el MDF Principal del bloque A.

La distribución del cableado horizontal se encuentra sobre un techo falso, sin ninguna protección esto da lugar a que exista interferencias electromagnéticas y degradación de la señal, afectando la integridad de los datos y el tiempo de respuesta al usuario. Los puntos de red están separados de los puntos eléctricos en la unidad no existe el cumplimiento de los estándares ya que las normas como las del cableado que debe ir en canaletas protegido no se da y los puntos de red no se encuentran certificados actualmente.

2.8.1.1 DIAGRAMA MDF PRINCIPAL

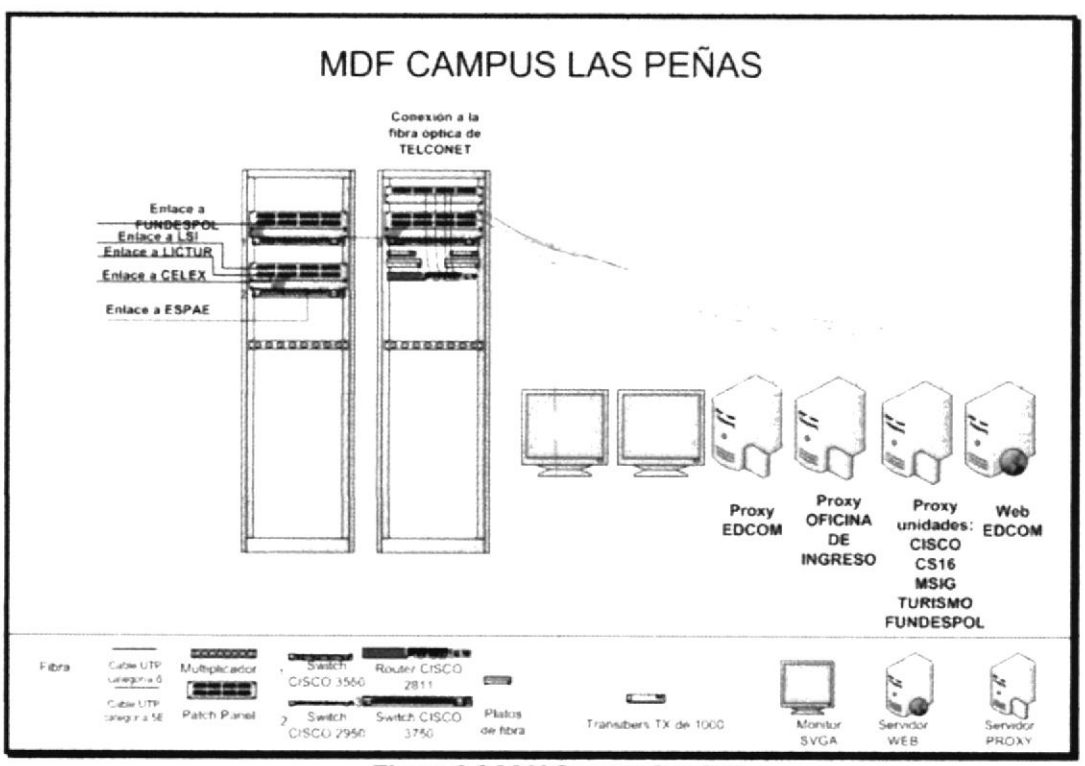


Figura 2.3 Mdf Campus Las Peñas

2.8.1.2 DETALLE DE EQUIPOS

1 Router CISCO 2811.
1 Switch CISCO 2950 10/100 BT de 24 puertos.
1 Switch CISCO 3550 10/100 BT de 24 puertos.
2 Switches 3Com de 10 BT IBM de 24 puertos.
1 Servidor PROXY que abastece al EDCOM.
1 Servidor PROXY que abastece a la Oficina de Ingreso.
1 Servidor PROXY que abastece a ESPAE, LSI, MSIG, TURISMO y FUNDESPOL.
1 Servidor WEB que abastece a EDCOM.
2 Platos de fibra.
5 Transibers TX de 1000.
20 computadoras personales.

2.8.1.3 DIAGRAMA DE PISO

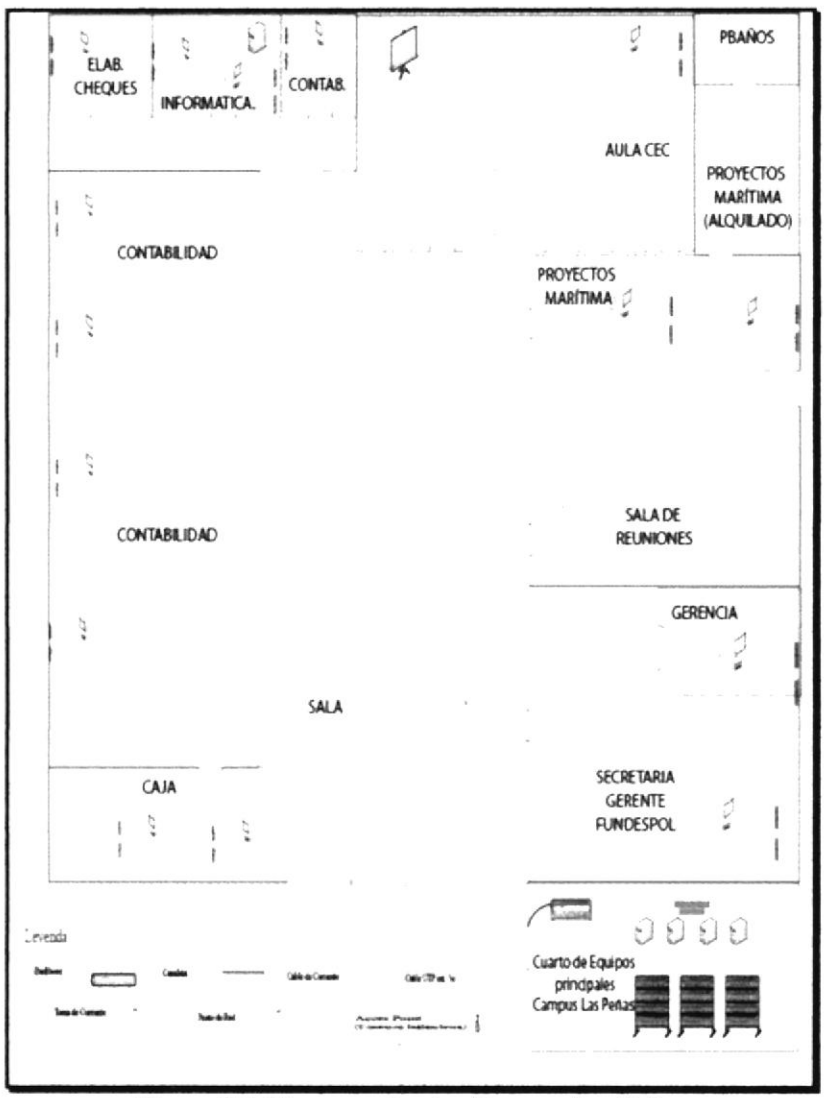


Figura 2.4 Diagrama de piso Campus Las Peñas

2.8.2 OFICINA DE INGRESO

El plan de Cableado es con el estándar T568-B con cable UTP categoría 5 y 5E., los puntos eléctricos están muy distantes a los de red.

2.8.2.1 DIAGRAMA IDF

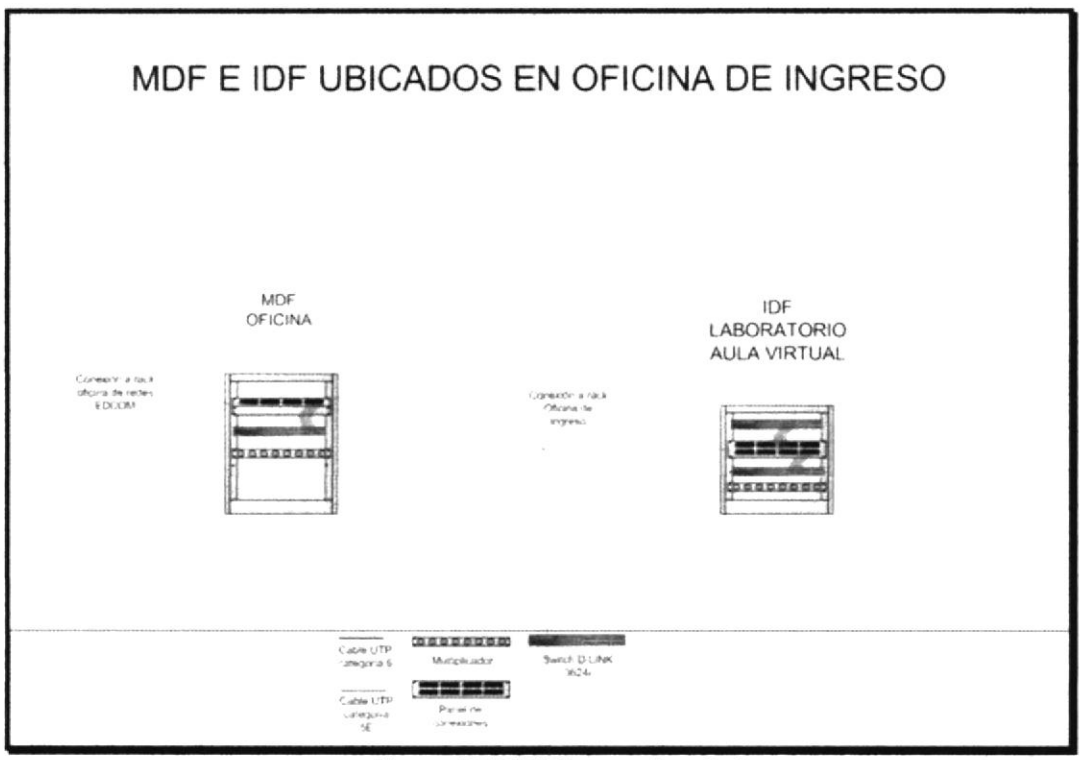


Figura 2.5 Mdf Campus Las Peñas

2.8.2.2 DETALLE DE EQUIPOS

Oficina del director
1 Switch CNET 8 puertos 10 Mbps baseT.

Oficina administrativa
1 Switch D-Link DES1008D 8 puertos 10/100 Mbps baseT.

Cuarto bloque G
1 Switch D-Link DES36241 22 puertos 10/100 Mbps baseT 2 puertos 10/100/1000 Mbps baseT.

Laboratorio semipresencial
Switch DES1024D 24 puertos 10/100 Mbps baseT.
Switch DES1024D 24 puertos 10/100 Mbps baseT.

Auditorio
Switch DES1005D 5 puertos 10/100 Mbps baseT.

2.8.2.3 DIAGRAMA DE PISO OFICINA DE INGRESO

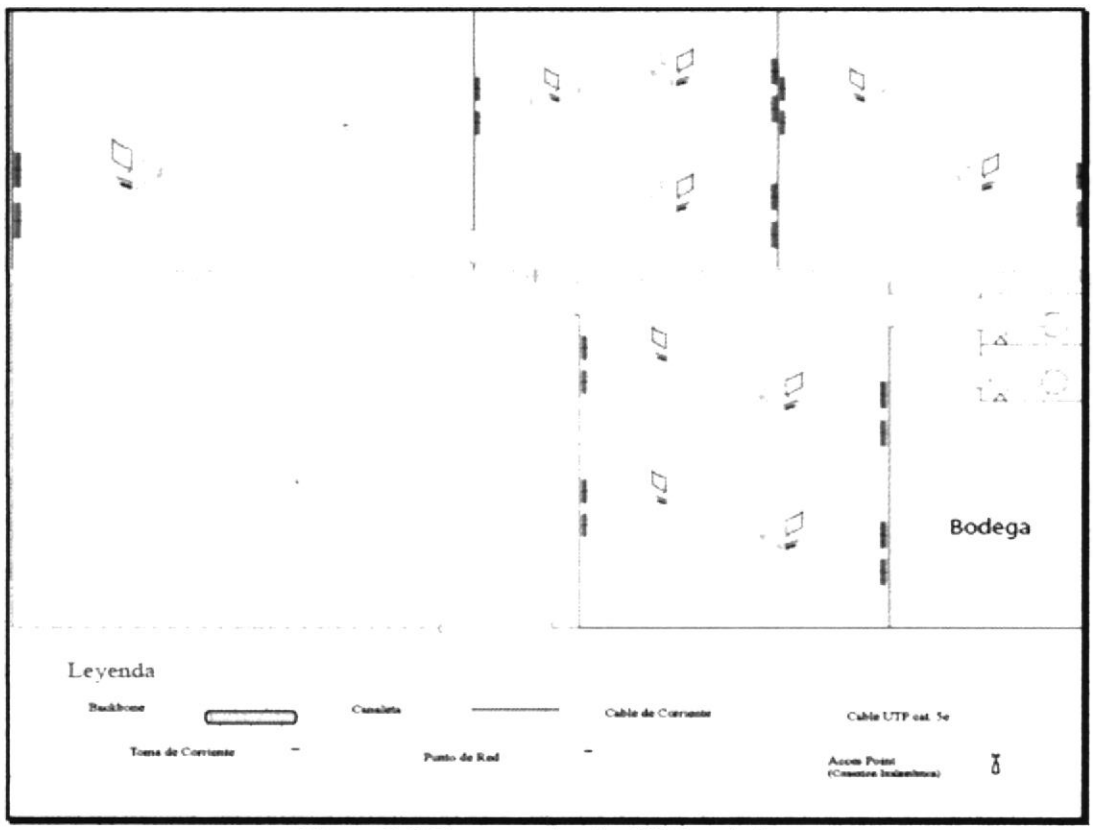


Figura 2.6 Diagrama de piso Oficina de Ingreso

2.8.3 EDCOM

El plan de Cableado es con el estándar T568-B con cable UTP categoría 5 y 5E, el cableado horizontal se encuentra empotrados en los laboratorios G2, G3, G4 en el G7 va por canaletas, El cableado en los departamentos de GAMA, Contabilidad se encuentra por canaletas, la distancia de los puntos eléctricos con los de res en algunos casos es de 5 cm En el Edcom existen alrededor de 264 PCs. En el bloque E hay 3 laboratorios, el cableado estructurado esta por canaletas, el cable es categoría 5e.

2.8.3.1 DIAGRAMA MDF E IDF

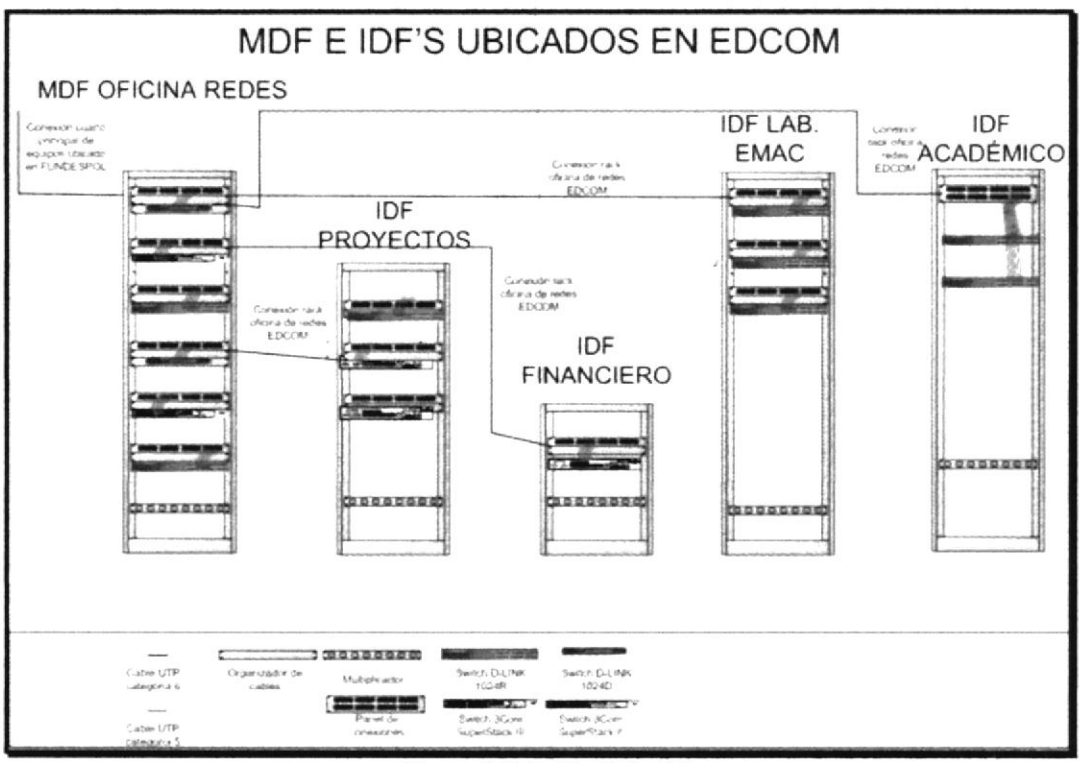


Figura 2.7 Mdf e Idf's Edcom

2.8.3.2 DETALLE DE EQUIPOS

MDF principal

Switch 3Com 3C16471 24 puertos 10/100 Mbps baseT
Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT
Hub 3Com 3C16671 24 puertos 10 Mbps baseT
Switch 3Com 3C16950 24 puertos 10 baseT Mbps 2 puertos 10/100 Mbps baseT
Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT
Switch D-Link 16 puertos 10/100 Mbps baseT

Académico

2 Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT

Proyectos

2 Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT
1 Switch D-Link DES1016R 16 puertos 10/100 Mbps baseT
1 Hub 3Com 3C16671 24 puertos 10 Mbps baseT

IDE
1 Switch D-Link DES1016R 16 puertos 10/100 Mbps baseT

Financiero
1 Switch D-Link DES1016R 16 puertos 10/100 Mbps baseT

Emac Lab
3 Switch D-Link 24 puertos 10/100 Mbps baseT

2.8.3.3 DIAGRAMA DE PISO EDCOM

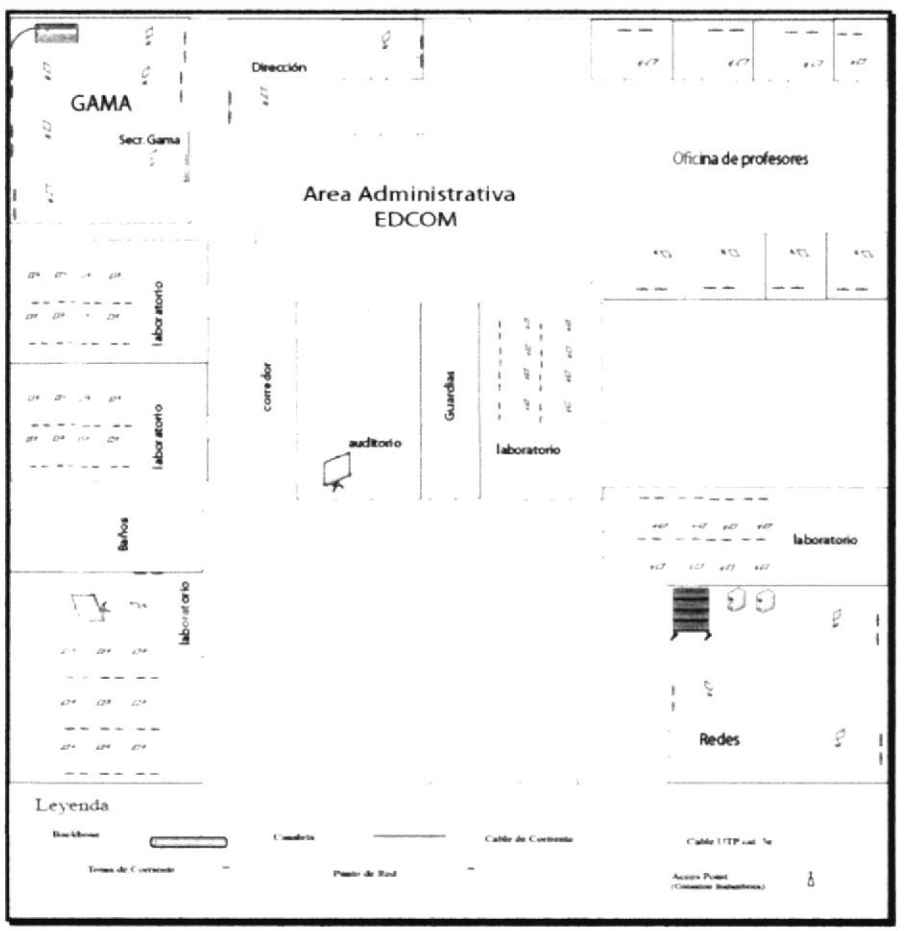


Figura 2.8 Diagrama de piso Edcom

2.8.4 ESPAE

Existen 64 computadoras distribuidas entre el área administrativa y 1 laboratorio, el plan de cableado es con el estándar T568-B con cable UTP categoría 5 y 5E., se encuentra en canaletas y esta debidamente protegido, los puntos de red están separados de los puntos eléctricos a una distancia de 20 cm, los puntos están debidamente certificados y en funcionamiento. Se podría indicar que en esta área si se están dando todos los estándares debidos.

2.8.4.1 DIAGRAMA IDF ESPAE

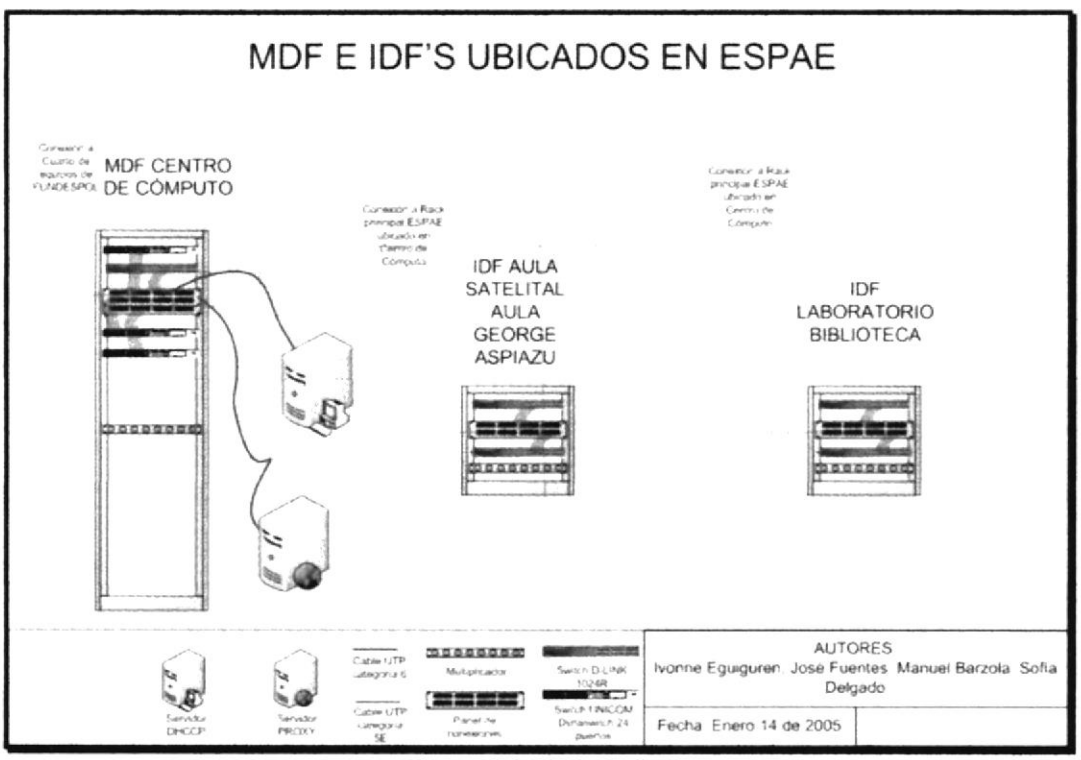


Figura 2.9 Mdf e Idf's Espae

2.8.4.2 DETALLE DE EQUIPOS

Área Centro de Cómputo y Administrativa

1 Switch Dyna Switch/24 24 puertos 10/100 Mbps baseT.
2 Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT.
1 Access Point 3Com office Connect Wireless IEEE 802.11g.
30 computadoras personales.

Laboratorios

2 Switches D-Link DES1024R 24 puertos 10/100 Mbps baseT.
30 computadoras personales.

Aula Satelital

1 Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT.
1 Transceiver 10 baseT-10baseFL.

Aula Ayora Aspiazu
1 Switch D-Link DES1024D 24 puertos 10/100 Mbps baseT.
1 Switch D-Link DES1024D 24 puertos 10/100 Mbps baseT.

Aula hexagonal
1 Hub SMC 3512TP 12 puertos 10baseT.

2.8.4.3 DIAGRAMA DE PISO ESPAE

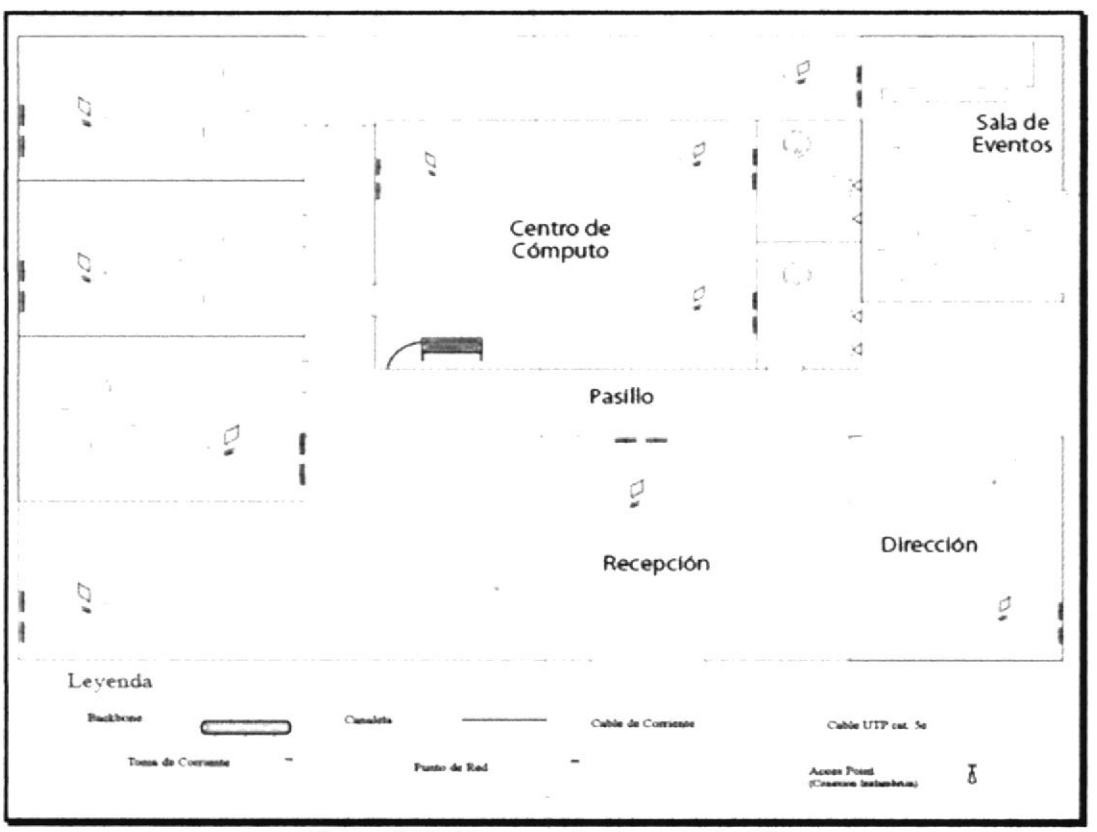


Figura 2.10 Diagrama de piso principal Espae

2.8.5 CEC (CENTRO DE EDUCACIÓN CONTINUA)

Existen en las oficinas alrededor de 12 PCs. Y en el laboratorio alrededor de 30 equipos. El plan de Cableado es con el estándar T568-B con cable UTP categoría 5 y 5E, el cableado horizontal se encuentra por canaletas, los puntos de red mantienen una distancia considerable a los puntos eléctricos.

2.8.5.1 DIAGRAMA IDF

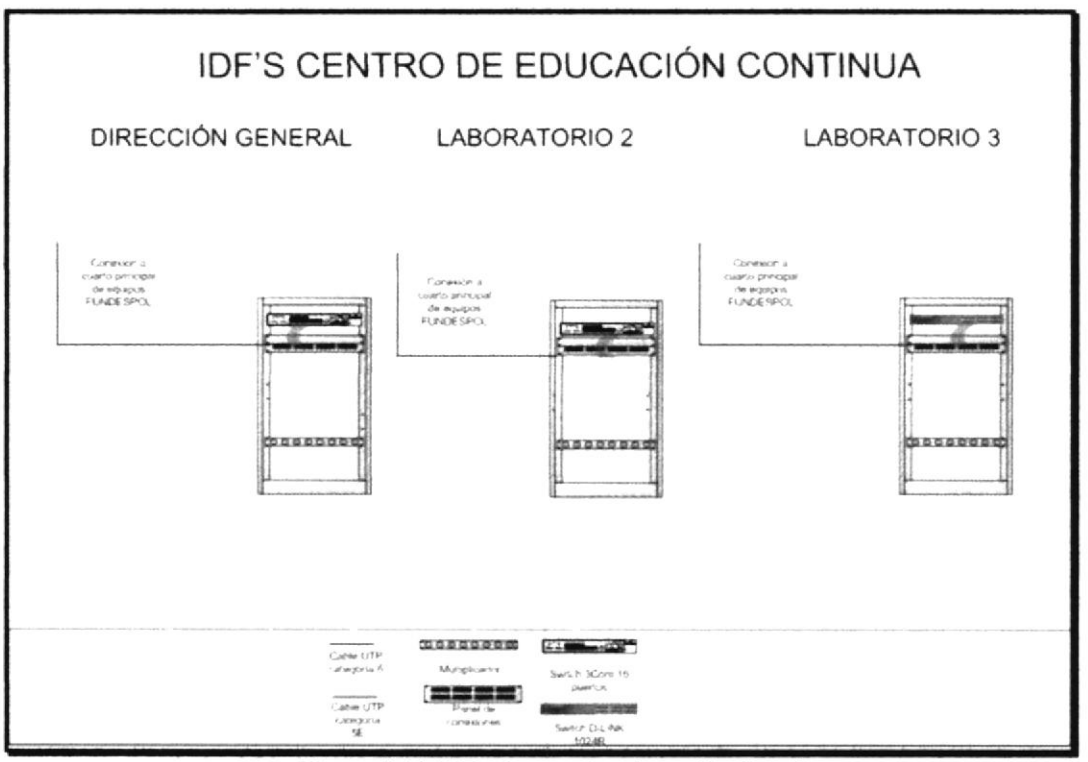


Figura 2.11 Idf's Centro de educación Continua

2.8.5.2 DETALLE DE EQUIPOS

Oficina de dirección

1 Hub D-Link DE-816TP 24 puertos 10/100 Mbps baseT.

Laboratorio 2

1 Hub 3Com 3C16670 24 puertos 10/100 Mbps baseT.

Laboratorio 3

1 Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT.

2.8.5.3 DIAGRAMA DE PISO EDUCACIÓN CONTINUA

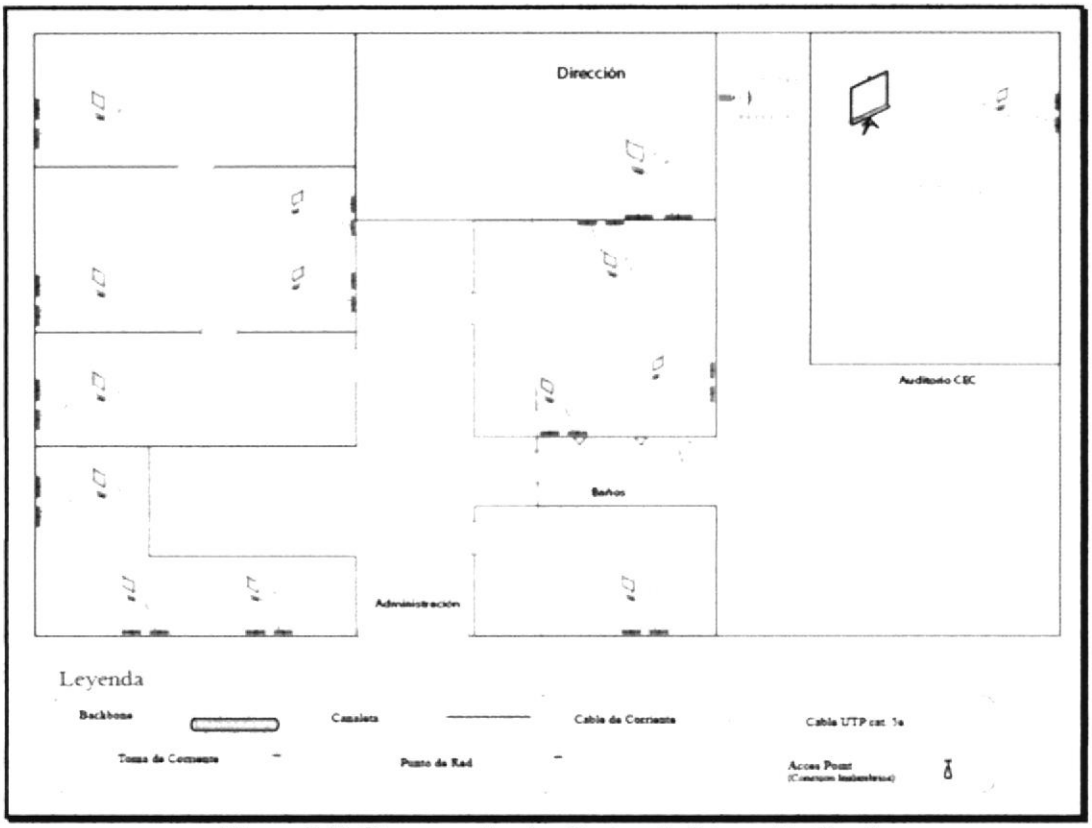


Figura 2.12 Diagrama de piso Centro de Educación Continua

2.8.6 CELEX

El plan de Cableado es con el estándar T568-B con cable UTP categoría 5 y 5E., el cableado horizontal esta protegido por canaletas, los puntos como de red y eléctricos están completamente separados a una distancia de 30cm en otro caso 15cm. Los puntos de red actualmente no están certificados.

2.8.6.1 DIAGRAMA IDF

Figura 2.13 Idf Celex

2.8.6.2 DETALLE DE EQUIPOS

Laboratorio principal

1 Switch 3Com 3C16471 24 puertos 10/100 Mbps baseT.

1 Router Cisco 1700 1 puerto 10/100 Mbps baseT 2 puertos 10 baseT (no se encuentra funcionando).

Laboratorio 1

1 Switch D-Link DES1024R 24 puertos 10/100 Mbps baseT.

Laboratorio 2

1 Access point Orinoco 2.4-5.8 GHZ.

Maestrías

1 Switch D-Link DES1008D 8 puertos 10/100 Mbps baseT.

2.8.6.3 DIAGRAMA DE PISO CELEX

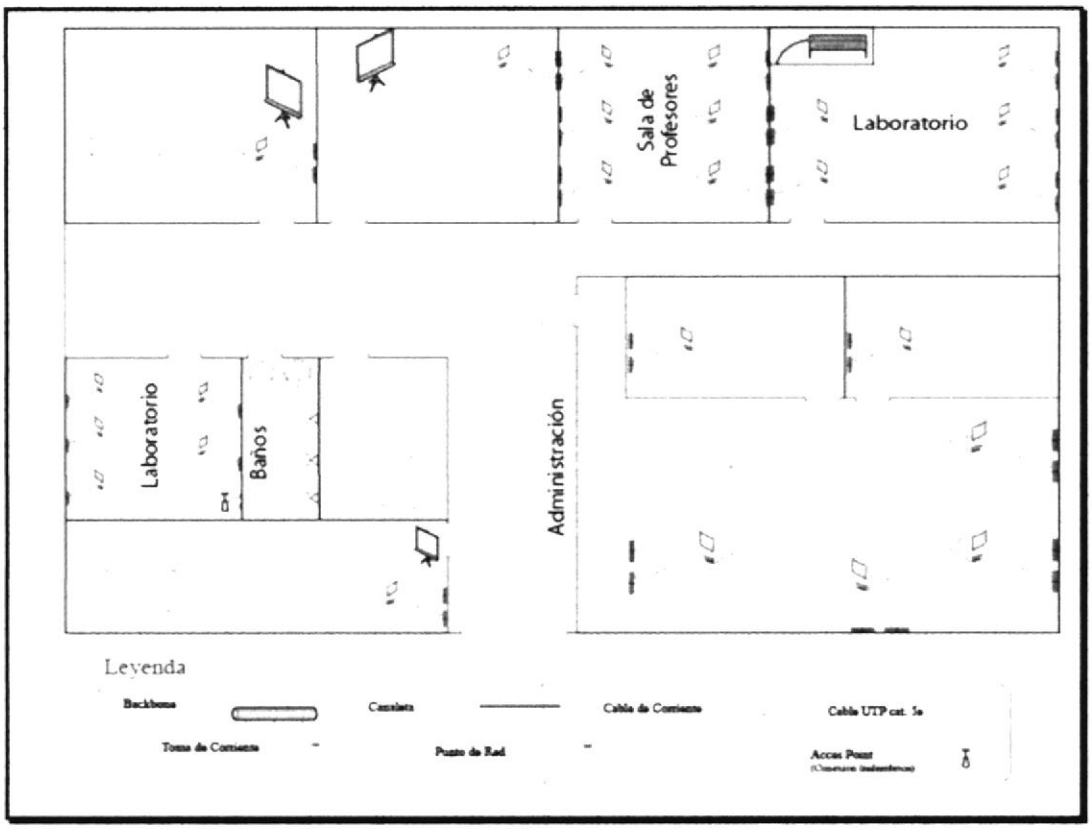


Figura 2.14 Diagrama de piso Celex

2.8.7 LSI (LICENCIATURA EN SISTEMAS DE INFORMACIÓN)

Existen alrededor de 60 PCs entre el área administrativa y laboratorios el plan de cableado es con el estándar T568-B con cable UTP categoría 5 y 5E, el cableado horizontal se encuentra por canaletas, algunos empotrados, los puntos de red mantienen una distancia aproximadamente de 15 cm en otros casos es 30cm. de distancia a los puntos de red

2.8.7.1 DIAGRAMA IDF LSI

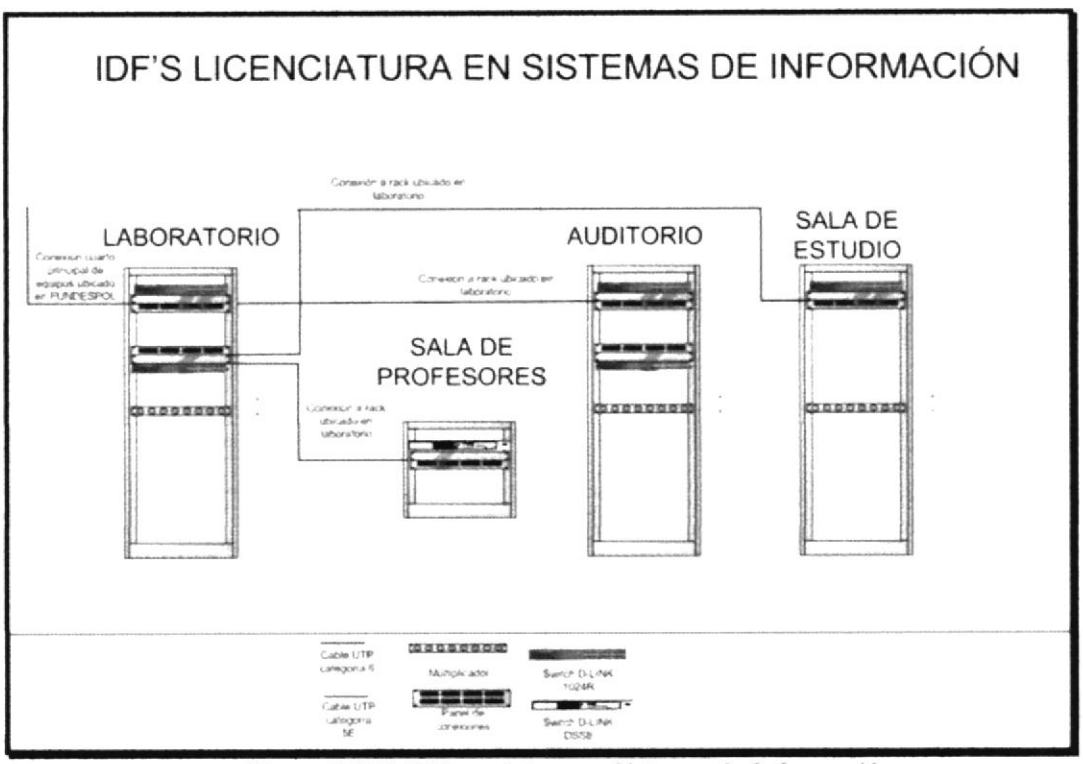


Figura 2.15 Idf Licenciatura en Sistemas de Información

2.8.7.2 DETALLE DE EQUIPOS

Sala de profesores
1 Switch D-Link DSS8+ 8 puertos 10/100 Mbps baseT.

Sala de estudios
1 Switch D-Link DES1024D 24 puertos 10/100 Mbps baseT.

Laboratorio
2 Hub IBM 8224 16 puertos 10 baseT.

Maestría
2 Switch D-Link DES1024D 24 puertos 10/100 Mbps baseT.

2.8.7.3 DIAGRAMA DE PISO LSI

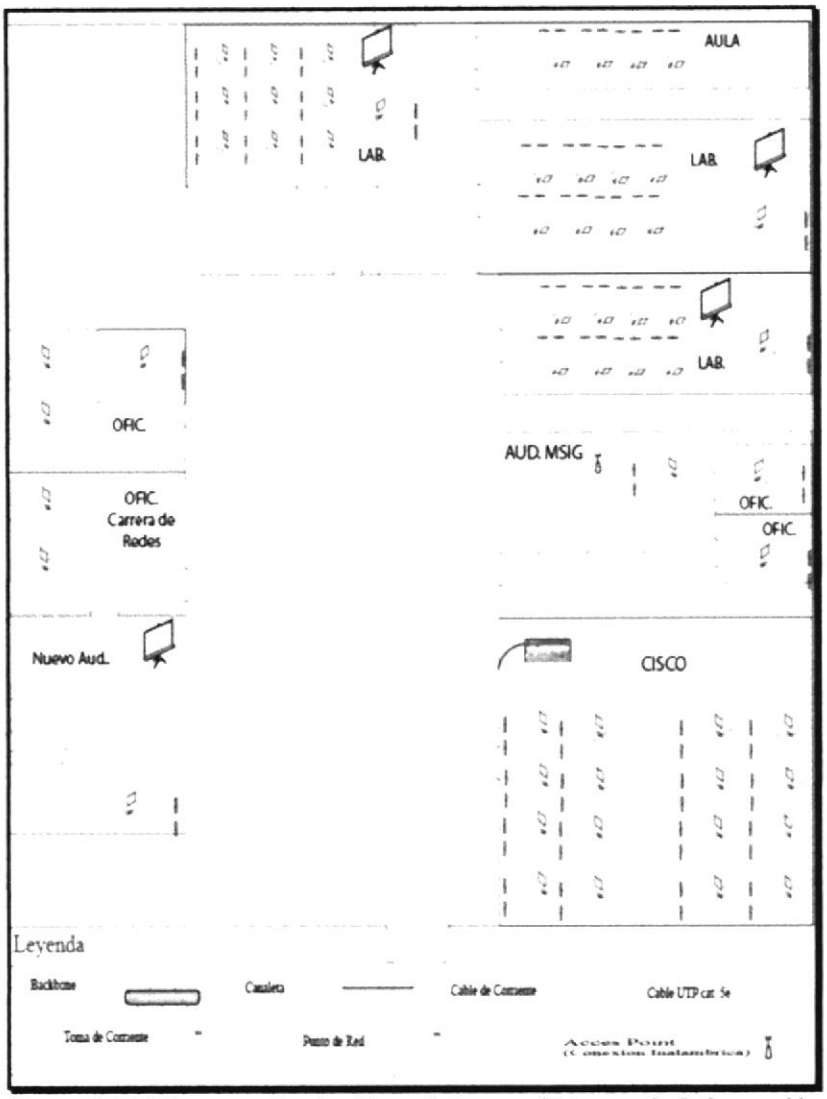


Figura 2.16 Diagrama de piso Licenciatura en Sistemas de Información

2.8.8 LICTUR (LICENCIATURA EN TURISMO)

Existen alrededor de 40 PCs distribuidas entre área administrativa y laboratorio, el plan de Cableado es con el estándar T568-B con cable UTP categoría 5 y 5E, el cableado horizontal se encuentra por canaletas, algunos empotrados, los puntos de red mantienen una distancia aproximadamente de 15 cm en otros casos es 30cm. de distancia a los puntos de red.

2.8.8.1 DIAGRAMA IDF

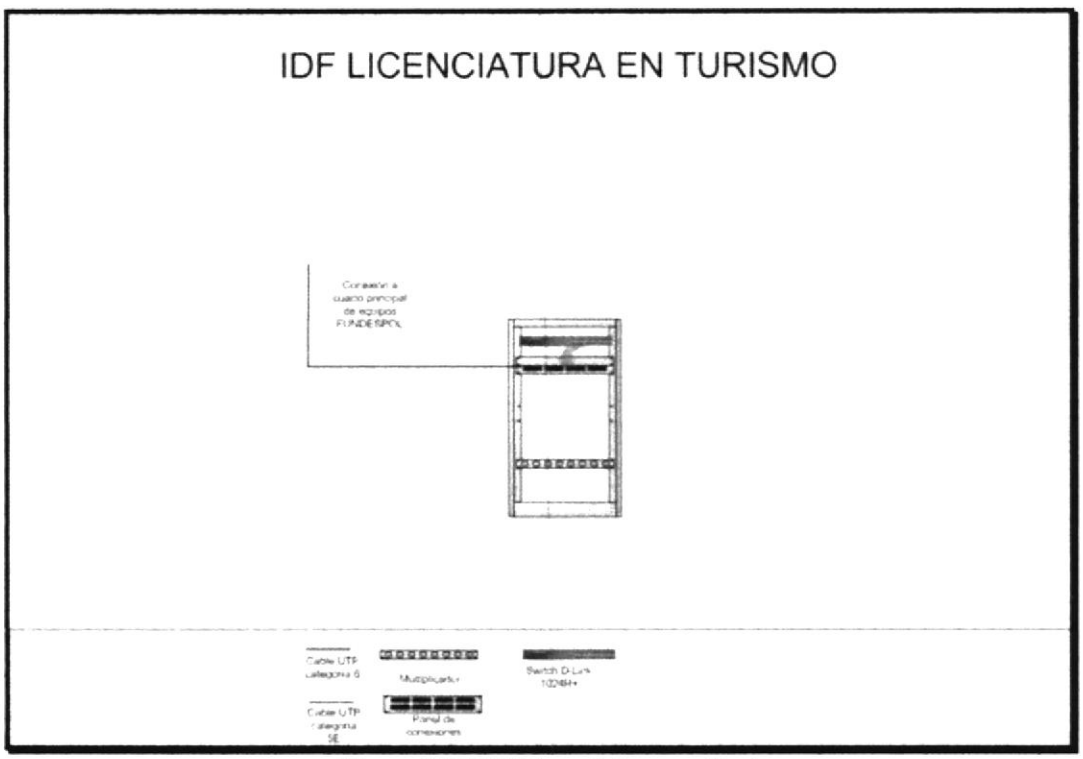


Figura 2.17 Idf Licenciatura en Turismo

2.8.8.2 DETALLE DE EQUIPOS

Laboratorio

1 Hub 3Com TP16C 10/100 base T.

1 Switch D-Link DES1024D 24 puertos 10/100 Mbps baseT.

2.8.8.3 DIAGRAMA DE PISO LICENCIATURA EN TURISMO

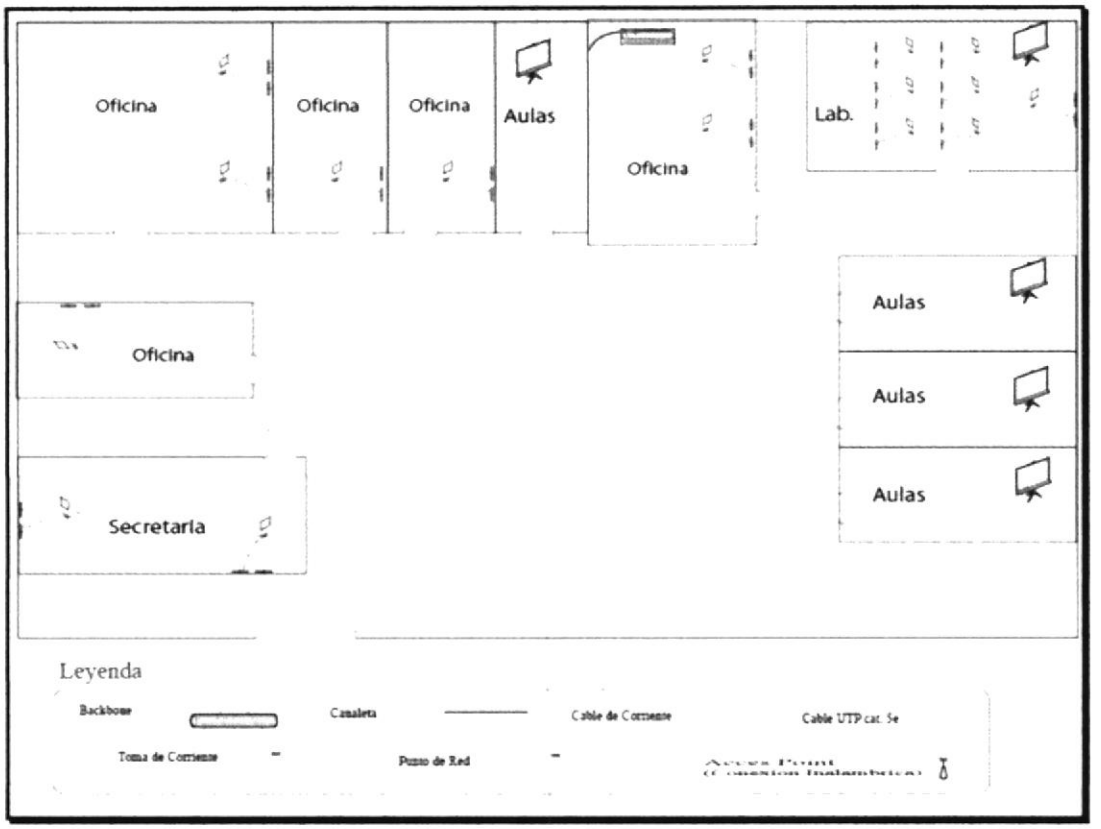


Figura 2.18 Diagrama de piso Licenciatura en Turismo

2.8.9 BIBLIOTECA Y CDP

El plan de Cableado es con el estándar T568-B con cable UTP categoría 5 y 5E, la mayor parte del cableado de la **Biblioteca** no se encuentra debidamente protegido en canaletas sobre todo en los laboratorios.

En el CDP el plan de Cableado es con el estándar T568-B con cable UTP categoría 5 y 5E, todo el cableado horizontal se encuentra en canaletas la mayoría de los puntos son voz y datos, los puntos eléctricos se encuentran muy distantes al de red.

2.8.9.1 DIAGRAMA IDF BIBLIOTECA Y CDP

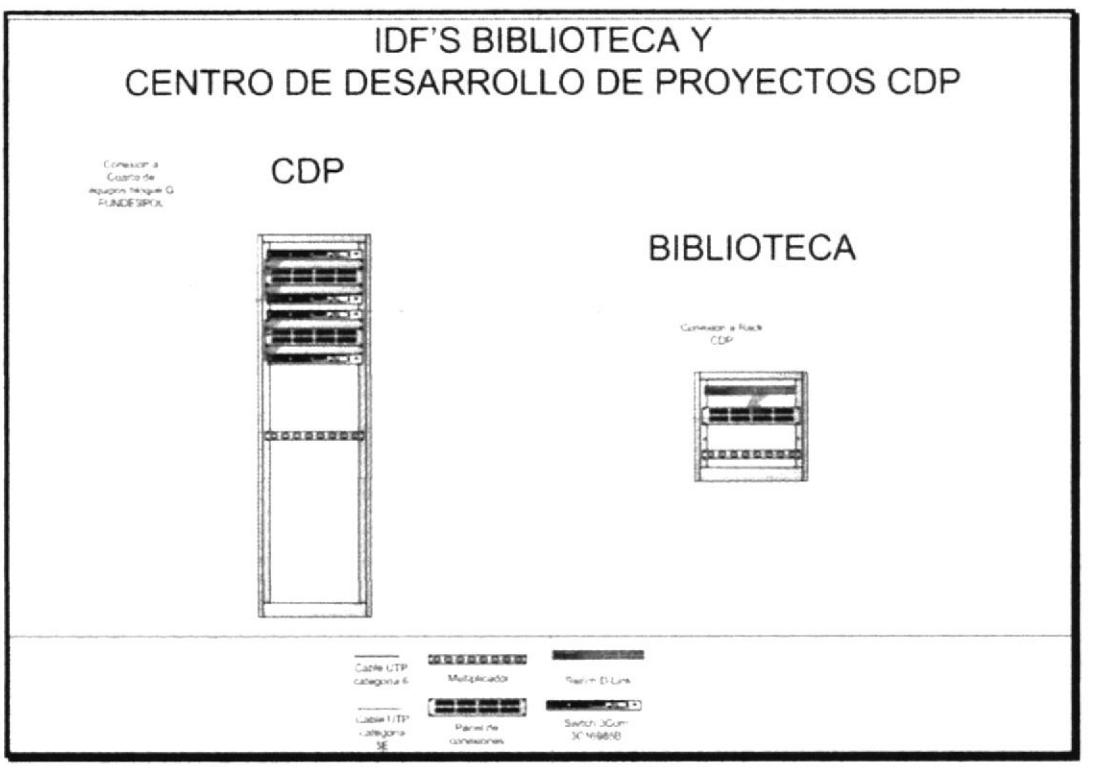


Figura 2.19 Idf's Biblioteca y Centro de Desarrollo de Proyectos

2.8.9.2 DETALLE DE EQUIPOS

CDP - Sala de servidores
4 Switch 3Com 3C16985B 24 puertos 10/100 Mbps baseT.

Biblioteca - Sala de atención
Switch D-link 24 puertos 10/100 Mbps baseT.

2.8.9.3 DIAGRAMA DE PISO BIBLIOTECA Y CDP

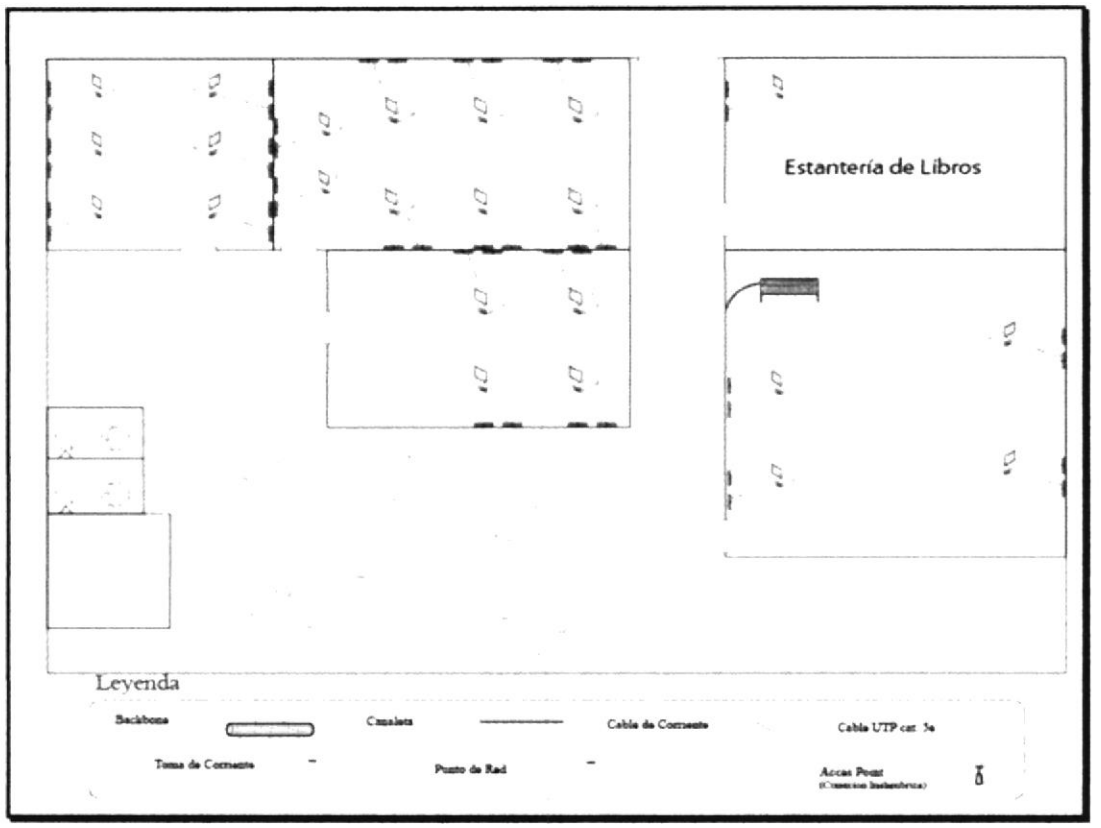


Figura 2.20 Diagrama de piso Biblioteca

CAPÍTULO 3

SOLUCIÓN PROPUESTA

3. SOLUCIÓN PROPUESTA

3.1 PROBLEMAS ENCONTRADOS

3.1.1 PROBLEMAS ORGANIZACIONALES

PROBLEMA	CAUSA	EFECTO
Falta de personal capacitado y a cargo de la administración de la red.	No se realiza capacitación constante al personal encargado. No se pueden solucionar problemas en la red con agilidad ni determinar responsables	Existen personas con falta de conocimientos en el área de redes. Demora en solución de problemas y toma de decisiones.

Tabla 3.1 Problemas organizacionales

3.1.2 PROBLEMAS TÉCNICOS

PROBLEMA	CAUSA	EFECTO	UNIDAD
No se cumple con las normas de cableado estructurado.	Falta de electro-canaletas Los cables del Rack no se encuentran etiquetados. La red no está documentada.	Interferencia electromagnética. No se pueden identificar problemas con facilidad. No hay planos por ser una edificación antigua.	• CEC • Lictur • LSI • ESPAE • Celex • Fundespol • Biblioteca
No existe un enlace de comunicación de respaldo con el Campus Prosperina	No se ha previsto tener éste enlace	Cuando falla el enlace principal no se puede conectar con el Campus Prosperina	• Fundespol
Falta de Firewall's físico.	No se ha implementado sistemas de protección en la red.	Vulnerabilidad en la red.	• Fundespol
Ancho de banda de Internet insuficiente.	Crecimiento en la cantidad de usuarios de la red.	Inconformidad y pérdida de tiempo en la navegación por parte de los usuarios.	Todas las unidades
Colisiones en la red.	Falta de Actualización en los concentradores.	Pérdida de paquetes de información en la red. Velocidad de transmisión compartida entre puertos.	• CEC • Fundespol • Lictur • LSI • ESPAE • Oficina de ingreso • Celex • Biblioteca • CDP

Tabla 3.2 Problemas técnicos

3.2 SOLUCIÓN Y ALCANCE

PROBLEMA	SOLUCIÓN	ALCANCE	UNIDAD
Falta de personal capacitado y a cargo de la administración de la red.	Obtener becas de cursos brindados por la ESPOL al personal que se encargará del funcionamiento de las redes de cada unidad. Contratar a un Jefe de Redes Campus Las Peñas, y delegar responsabilidades específicas para el mejor control de la red.	Mejor solución de problemas y conocimiento en la red. Control de las redes y equipos de comunicación en el campus y en cada unidad eficaz.	• CEC • Lictur • LSI • ESPAE • Oficina de ingreso • Celex • Biblioteca • CDP
No se cumple con las normas de cableado estructurado.	Implementación y adecuación del cableado con sus respectivas normas y estándares, así como la ubicación de los principales equipos de comunicación. Efectuar la respectiva documentación.	Tener un mejor control en la infraestructura del cableado estructurado. Soluciones ágiles al momento de efectuar correcciones en la red.	• CEC • Lictur • LSI • ESPAE • Celex • Biblioteca • CDP
Colisiones en la red.	Adquisición de switchs para reemplazar los hubs existentes.	Adquisición de switchs para reemplazar los hubs existentes.	• CEC • Lictur • LSI • Celex • Biblioteca
Falta de Firewall's fisico.	Adquisición de Firewall´s a nivel de hardware e implementación de los mismos.	Protección en la red a nivel LAN y WAN.	• Mdf Campus Las Peñas
Ancho de banda de Internet insuficiente.	Adquirir un mayor ancho de banda de internet (2 Mbps) para cubrir las necesidades de cada unidad.	Satisfacción en los usuarios de la red al mejorar el acceso a Internet.	• Lictur • LSI • ESPAE • Celex • Biblioteca
No existe un enlace de respaldo a nivel WAN con el Campus Prosperina.	Contratar con el proveedor actual que es Telconet, éste enlace de respaldo el cual será de 768 Kbps.	Comunicación ininterrumpida con el Campus Prosperina.	• Mdf Campus Las Peñas

Tabla 3.3 Solución y alcance

3.3 SOLUCIÓN PROPUESTA ALTERNATIVA 1

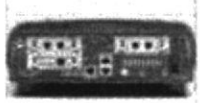
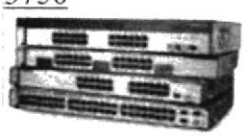
3.3.1 ESTUDIO DE FACTIBILIDADES

3.3.1.1 OBJETIVO

- Mejorar la comunicación WAN gracias a la implementación de dispositivos de enrutamiento de última tecnología
- Protección de la red gracias a la adquisición de firewall físicos.
- Mantener un estándar en la comunicación LAN, con la adquisición de switches e implementación de cableado estructurado debidamente organizado con canaletas.
- Mejorar los servicios Proxy y web Server gracias a la mejora en los servidores

3.3.1.2 FACTIBILIDAD TÉCNICA

3.3.1.2.1 MDF ESPOL PEÑAS

Cant.	Equipo	Descripción	Uso
1	Router CISCO 2600 	-Protocolo de direccionamiento OSPF, BGP-4, IS-IS, RIP-1, RIP-2, IGMP, VRRP, PIM-SM, PIM-DM -Protocolo de interconexión de datos: Ethernet, Fast Ethernet -Red / Protocolo de transporte L2TP, IPSec -Protección firewall, soporte de NAT, VPN, soporte de MPLS -Cumplimiento de normas IEEE 802.1Q	Dispositivo de enrutamiento
1	Router CISCO 1700 	-Memoria RAM 128 MB SDRAM -Memoria Flash 32 MB -Protocolo de direccionamiento OSPF, BGP-4, IS-IS, RIP-1, RIP-2 Cumplimiento de normas IEEE 802.1Q	Dispositivo de enrutamiento
1	Switch CISCO Catalyst 3750 	Opciones Flexibles de Gigabit-uplink, soportando GBIC o 1000 BaseT. 24 Puertos 10/100 respectivamente, junto con 2 puertos Up link de 10/100/1000BaseT. Soporta VLANs, STP, 802.1d, (PVST+), EMI, VTP, MVR, IGMP.	Administración de VLAN's

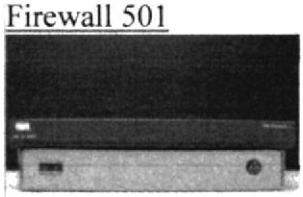
Cant.	Equipo	Descripción	Uso
3	Switch CISCO Catalyst 2950 	Opciones Flexibles de Gigabit-uplink, soportando GBIC o 1000 BaseT. 24 Puertos 10/100 respectivamente, junto con 2 puertos Up link de 10/100/1000BaseT. Soporta el agente de software RMON. Con unidad de rack. Soportan VLANs, STP, 802.1d, (PVST+), EMI, VTP, MVR, IGMP.	Administración de VLAN's
2	Bobinas cat 6 305 mts.	Marca Panduit	Tendido en general
5	Servidor Hp Proliant ML 330 	Procesador Intel Xeon 3.06 GHz/533 MHz - 512KB Memoria tipo PC2100 DDR Memoria: 4 GB Protección de memoria: Advanced ECC Tipo de almacenamiento: Non-hot plug SCSI Puertos para expansion: 5 Puertos removibles de expansión: 3 Controlador de almacenamiento: Single Channel Wide Ultra3 SCSI Adapter (in a PCI slot; SCSI Models)	Servidores PROXY
2	Firewall Cisco Pix Firewall 501 	**Firewall Hardware:** # PIX-515 # 256 MB RAM # 16 MB Flash # CPU Pentium 200 MHz # 2 x Fast Ethernet Interfaces **Firewall Firmware:** # Cisco PIX Firewall Version 5.2(3) – Upgradeable Cisco Secure PIX Firewall BIOS (4.0) #0: Thu Mar 2 22:59:20 PST 2000 Platform PIX-515 Flash=i28F640J5 @ 0x300	Protección entre enlaces Samborondón y Prosperina
20	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.4 Alternativa 1 - Factibilidad Técnica - MDF Espol Peñas

3.3.1.2.2 CDP Y BIBLIOTECA

Cant.	Equipo	Descripción	Uso
4	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	CDP Oficinas administrativas, técnicas y laboratorio
1	Switch D-Link DGS-1216T	El Switch DGS-1216T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Biblioteca
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.5 Alternativa 1 - Factibilidad Técnica - CDP y Biblioteca

3.3.1.2.3 EDCOM

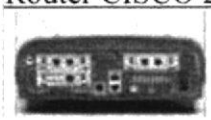
Cant.	Equipo	Descripción	Uso
15	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	MDF EDCOM, Laboratorios bloque G, IDF Académico, IDF Financiero, Laboratorios bloque E, IDE, Laboratorio EMAC
1	Switch D-Link DGS-1216T	El Switch DGS-1216T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	IDF Académico
1	Router CISCO 2600 	-Protocolo de direccionamiento OSPF, BGP-4, IS-IS, RIP-1, RIP-2, IGMP, VRRP, PIM-SM, PIM-DM -Protocolo de interconexión de datos: Ethernet, Fast Ethernet -Red / Protocolo de transporte L2TP, IPSec -Protección firewall, soporte de NAT, VPN, soporte de MPLS -Cumplimiento de normas IEEE 802.1Q	Dispositivo de enrutamiento con FUNDESPOL MDF

Tabla 3.6 Alternativa 1 - Factibilidad Técnica - EDCOM

3.3.1.2.4 ESPAE

Cant.	Equipo	Descripción	Uso
9	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Centro de cómputo, Aula Satelital, Laboratorio, Aula Hexagonal y oficinas administrativas, Biblioteca
1	Switch D-Link DGS-1216T	El Switch DGS-1216T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Aula Hexagonal
2	AIRONET SERIE 1200 CISCO 	Desempeño: 11/54 Mbps -Acceso al medio: DSSS, OFDM-Frecuencia: 2.4 y 5 GHz, banda libre -Equipos base (BS) y satélite (CPE) -Alcance: hasta 30 Km. (con amplificadores) -Antena omni, sectorial, yagi, etc.-Amplificadores RF de 20 Bm / 1w	Biblioteca y Auditorio
130	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.7 Alternativa 1 - Factibilidad Técnica - ESPAE

3.3.1.2.5 CELEX

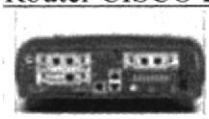
Cant.	Equipo	Descripción	Uso
2	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorios y oficinas administrativas
1	Router CISCO 2600 	-Protocolo de direccionamiento OSPF, BGP-4, IS-IS, RIP-1, RIP-2, IGMP, VRRP, PIM-SM, PIM-DM -Protocolo de interconexión de datos: Ethernet, Fast Ethernet -Red / Protocolo de transporte L2TP, IPSec -Protección firewall, soporte de NAT, VPN, soporte de MPLS -Cumplimiento de normas IEEE 802.1Q	Dispositivo de enrutamiento con FUNDESPOL MDF
2	AIRONET SERIE 1200 CISCO 	Desempeño: 11/54 Mbps -Acceso al medio: DSSS, OFDM -Frecuencia: 2.4 y 5 GHz, banda libre -Equipos base (BS) y satélite (CPE) -Alcance: hasta 30 Km. (con amplificadores) -Antena omni, sectorial, yagi, etc. -Amplificadores RF de 20 dBm / 1w	Aulas
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.8 Alternativa 1 - Factibilidad Técnica - CELEX

3.3.1.2.6 OFICINA DE INGRESO

Can	Equipo	Descripción	Uso
3	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Auditorio y laboratorio de pre-virtual
2	Switch D-Link DGS-108T	El Switch Des-108T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z. Este switch esta equipado para auto negociar velocidades a 10Mbps y 100Mbps.	Oficinas de registro
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.9 Alternativa 1 - Factibilidad Técnica – Oficina de ingreso

3.3.1.2.7 LICTUR

Cant.	Equipo	Descripción	Uso
1	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorio
1	Switch D-Link DGS-1216T	El Switch DGS-1216T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Oficinas administrativas
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización del cableado

Tabla 3.10 Alternativa 1 - Factibilidad Técnica – LICTUR

3.3.1.2.8 CENTRO DE EDUCACIÓN CONTINUA

Cant.	Equipo		Uso
2	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorio
1	Switch D-Link DGS-1216T	El Switch DGS-1216T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Oficinas administrativas
50	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.11 Alternativa 1 - Factibilidad Técnica - CEC

3.3.1.2.9 LSI

Cant.	Equipo		Uso
2	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorios LSI, Laboratorio MSIG, Auditórium
1	Switch D-Link DGS-1216T	El Switch DGS-1216T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Oficinas administrativas
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.12 Alternativa 1 - Factibilidad Técnica - LSI

3.3.1.3 FACTIBILIDAD ECONÓMICA

3.3.1.3.1 COSTO DE HARDWARE

CANTIDAD	DETALLE	UNITARIO	COSTO TOTAL
3	*Router Cisco 2600*	*$1,456.00*	*$4,368.00*
1	*Router Cisco 1700*	*$1,116.70*	*$1,116.70*
2	*Firewall Cisco Pix Firewall 501*	*$821.46*	*$1,642.92*
1	*Switch Cisco 3750*	*$2,750.00*	*$2,750.00*
3	*Switch Cisco 2950*	*$1,435.20*	*$4,305.60*
3	*Access Point Cisco Aironet 1200*	*$600.00*	*$1,800.00*
38	*Switch D-Link DGS1224T 24Ptos.*	*$525.00*	*$19,950.00*
5	*Switch D-Link 16 DGS-1216T Ptos.*	*$320.00*	*$1,600.00*
2	*Switch D-Link 16 DGS-1208T Ptos.*	*$60.00*	*$120.00*
13	*Bobina de 305 m.*	*$250.00*	*$3,250.00*
5	*Servidores Hp Proliant*	*$1,535.90*	*$7,674.50*
350	*mts. de canaleta escalerilla calibre 20*	*$42.00*	*$14,700.00*
	Total Costo de Hardware		***$63,277.72***

Tabla 3.13 Alternativa 1 - Factibilidad Económica - Costo de hardware

3.3.1.3.2 COSTO DE SOFTWARE

DETALLE	UNITARIO	COSTO TOTAL
Sistema operativo LINUX FEDORA CORE 3	*$0.00*	*$0.00*
Total Costo de Software		***$0.00***

Tabla 3.14 Alternativa 1 - Factibilidad Económica - Costo de Software

3.3.1.3.3 COSTOS OPERATIVOS

3.3.1.3.3.1 FASE DE ANÁLISIS LAN Y WAN

CANTIDAD	DETALLE	MESES	INDIVIDUAL	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2*	*$700*	*$1400*

Tabla 3.15 Alternativa 1 - Factibilidad económica - Costos operativos - Fase análisis LAN y WAN

3.3.1.3.3.2 FASE DE DISEÑO E IMPLEMENTACIÓN LAN Y WAN

CANTIDAD	DETALLE	MESES	INDIVIDUAL	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*3*	*$700*	*$2100*
4	*Técnicos en redes*	*2*	*$300*	*$2400*

Tabla 3.16 Alternativa 1 - Costos operativos - Fase implementación LAN y WAN

3.3.1.3.3.3 FASE DE DOCUMENTACIÓN Y PRUEBA LAN Y WAN

CANTIDAD	DETALLE	MESES	INDIVIDUAL	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2*	*$700*	*$1400*
1	*Técnicos en redes*	*1*	*$300*	*$300*
TOTAL COSTOS OPERATIVOS				*$7600*

Tabla 3.17 Alternativa 1 - Factibilidad económica - Costos operativos - Fase documentación y prueba LAN y WAN

3.3.1.3.4 COSTOS TOTALES

TOTAL COSTO DE EQUIPOS	*$63,277.72*
TOTAL COSTOS OPERATIVOS	*$11,200.00*
SUBTOTAL FACTIBILIDAD ECONÓMICA	***$74,477.72***
IMPREVISTOS 10%	***$7,447.77***
TOTAL FACTIBILIDAD ECONÓMICA	***$81,925.49***

Tabla 3.18 Alternativa 1 - Factibilidad económica - Costos totales

3.3.1.3.5 FORMA DE PAGO

La forma de pago para ésta alternativa será el 90% antes de empezar la obra, ya que se necesitará comprar todo el material antes de la implementación de éste proyecto, y el saldo del 10% restante al concluir la misma.

3.3.1.4 FACTIBILIDAD OPERATIVA

3.3.1.4.1 FASE DE ANÁLISIS LAN Y WAN.

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Líder del proyecto, encargado del análisis de la situación actual.

Tabla 3.19 Alternativa 1 - Factibilidad operativa - Fase de análisis LAN y WAN

3.3.1.4.2 FASE DE DISEÑO LAN Y WAN

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Líder del proyecto, encargado del diseño LAN y WAN

Tabla 3.20 Alternativa 1 - Factibilidad operativa - Fase de diseño LAN y WAN

3.3.1.4.3 FASE DE IMPLEMENTACIÓN LAN Y WAN

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Líder, coordinador del grupo
6	Técnicos en Red	Cableado LAN

Tabla 3.21 Alternativa 1 - Factibilidad operativa - Fase de implementación LAN y WAN

3.3.1.4.4 FASE DE DOCUMENTACIÓN

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Elaboración de manuales

Tabla 3.22 Alternativa 1 - Factibilidad operativa - Fase de documentación

3.3.1.4.5 FASE DE PRUEBA

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Pruebas WAN
1	Técnico en redes	

Tabla 3.23 Alternativa 1 - Factibilidad operativa - Fase de prueba

3.3.2 VENTAJAS Y BENEFICIOS ALTERNATIVA 1

3.3.2.1 VENTAJAS

- Protección en la red evitando ingresos maliciosos.
- Aprovechar la adquisición de equipos de comunicación con nueva tecnología para mejorar el rendimiento de red y disminuir las colisiones.
- Mayor rendimiento y velocidad en el acceso a Internet.

3.3.2.2 BENEFICIOS

- Productividad y seguridad en la comunicación.
- Agilidad en reubicación y detección de posibles errores en la comunicación entre unidades.
- Estudiantes satisfechos con Internet más veloz.
- Comunicación ininterrumpida con el Campus Prosperina.

3.3.3 DIAGRAMA DE GANTT

id	Nombre de tarea	Duración	Comienzo	Fin
1	**IMPLEMENTACION CAMPUS LAS PEÑAS**	**152 días**	**jue 01/09/05**	**vie 31/03/06**
2	**Fase de análisis LAN y WAN**	**43 días**	**jue 01/09/05**	**lun 31/10/05**
3	Recopilación de datos	16 días	jue 01/09/05	jue 22/09/05
4	Analizar situación actual	10 días	vie 23/09/05	jue 06/10/05
5	Proponer soluciones	4 días	vie 07/10/05	mié 12/10/05
6	Cotización de dispositivos	7 días	jue 13/10/05	vie 21/10/05
7	Elaborar propuesta	3 días	lun 24/10/05	mié 26/10/05
8	Aceptación de la propuesta	3 días	jue 27/10/05	lun 31/10/05
9	**Fase de diseño de la red**	**59 días**	**mar 01/11/05**	**vie 20/01/06**
10	Diseño LAN	14 días	mar 01/11/05	vie 18/11/05
11	Diseño WAN	8 días	lun 21/11/05	mié 30/11/05
12	Compra de equipos	59 días	mar 01/11/05	vie 20/01/06
13	**Fase de implementación a nivel LAN y WAN**	**53 días**	**vie 18/11/05**	**mar 31/01/06**
14	Cableado de red LAN	46 días	vie 18/11/05	vie 20/01/06
15	Implementación WAN	7 días	lun 23/01/06	mar 31/01/06
16	**Fase de documentación**	**13 días**	**mié 01/02/06**	**vie 17/02/06**
17	Elaboración de manuales de red	13 días	mié 01/02/06	vie 17/02/06
18	**Fase de prueba**	**30 días**	**lun 20/02/06**	**vie 31/03/06**
19	Prueba de cableado estructurado	22 días	lun 20/02/06	mar 21/03/06
20	Prueba de enlace WAN	8 días	mié 22/03/06	vie 31/03/06

Figura 3.1 Alternativa 1 Diagrama de Gantt

3.4 SOLUCIÓN PROPUESTA ALTERNATIVA 2

3.4.1 ESTUDIO DE FACTIBILIDADES

3.4.1.1 OBJETIVO

- Mejorar la comunicación WAN gracias a la implementación de dispositivos de enrutamiento de última tecnología
- Implementar cableado estructurado debidamente organizado con canaletas.
- Optimizar los recursos existentes en cada unidad (switches) para ahorro de dinero.

3.4.1.2 FACTIBILIDAD TÉCNICA

3.4.1.2.1 MDF ESPOL PEÑAS

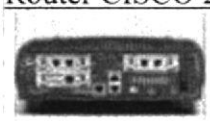
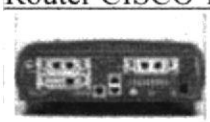
Cant.	Equipo	Descripción	Uso
1	Router CISCO 2600 	-Protocolo de direccionamiento OSPF, BGP-4, IS-IS, RIP-1, RIP-2, IGMP, VRRP, PIM-SM, PIM-DM -Protocolo de interconexión de datos: Ethernet, Fast Ethernet -Red / Protocolo de transporte L2TP, IPSec -Protección firewall, soporte de NAT, VPN, soporte de MPLS -Cumplimiento de normas IEEE 802.1Q	Dispositivo de enrutamiento
1	Router CISCO 1700 	-Memoria RAM 128 MB SDRAM -Memoria Flash 32 MB -Protocolo de direccionamiento OSPF, BGP-4, IS-IS, RIP-1, RIP-2 Cumplimiento de normas IEEE 802.1Q	Dispositivo de enrutamiento
2	Bobinas cat 6 305 mts.	Marca Panduit	Tendido en general
20	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.24 Alternativa 2 - Factibilidad Técnica - MDF Espol Peñas

3.4.1.2.2 CDP Y BIBLIOTECA

Cant.	Equipo	Descripción	Uso
2	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	CDP Oficinas administrativas, técnicas y laboratorio
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.25 Alternativa 2 - Factibilidad Técnica - CDP y Biblioteca

3.4.1.2.3 EDCOM

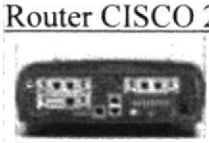
Cant.	Equipo	Descripción	Uso
5	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	MDF EDCOM, Laboratorios bloque G, IDF Académico, IDF Financiero, Laboratorios bloque E, IDE, Laboratorio EMAC
1	Router CISCO 2600 	-Protocolo de direccionamiento OSPF, BGP-4, IS-IS, RIP-1, RIP-2, IGMP, VRRP, PIM-SM, PIM-DM -Protocolo de interconexión de datos: Ethernet, Fast Ethernet -Red / Protocolo de transporte L2TP, IPSec -Protección firewall, soporte de NAT, VPN, soporte de MPLS -Cumplimiento de normas IEEE 802.1Q	Dispositivo de enrutamiento con FUNDESPOL MDF

Tabla 3.26 Alternativa 2 - Factibilidad Técnica - EDCOM

3.4.1.2.4 ESPAE

Cant.	Equipo	Descripción	Uso
5	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Centro de cómputo, Aula Satelital, Laboratorio, Aula Hexagonal y oficinas administrativas, Biblioteca
2	AIRONET SERIE 1200 CISCO 	Desempeño: 11/54 Mbps -Acceso al medio: DSSS, OFDM-Frecuencia: 2.4 y 5 GHz, banda libre -Equipos base (BS) y satélite (CPE) -Alcance: hasta 30 Km. (con amplificadores) -Antena omni, sectorial, yagi, etc.-Amplificadores RF de 20 Bm / 1w	Biblioteca y Auditorio
130	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.27 Alternativa 2 - Factibilidad Técnica - ESPAE

3.4.1.2.5 CELEX

Cant.	Equipo	Descripción	Uso
2	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorios y oficinas administrativas
2	AIRONET SERIE 1200 CISCO 	Desempeño: 11/54 Mbps -Acceso al medio: DSSS, OFDM -Frecuencia: 2.4 y 5 GHz, banda libre -Equipos base (BS) y satélite (CPE) -Alcance: hasta 30 Km. (con amplificadores) -Antena omni, sectorial, yagi, etc. -Amplificadores RF de 20 dBm / 1w	Aulas
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.28 Alternativa 2 - Factibilidad Técnica - CELEX

3.4.1.2.6 OFICINA DE INGRESO

Cant	Equipo	Descripción	Uso
2	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Auditorio y laboratorio de pre-virtual
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.29 Alternativa 2 - Factibilidad Técnica - Oficina de Ingreso

3.4.1.2.7 LICTUR

Cant.	Equipo	Descripción	Uso
2	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorio
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización del cableado

Tabla 3.30 Alternativa 2 - Factibilidad Técnica - LICTUR

3.4.1.2.8 CENTRO DE EDUCACIÓN CONTINUA

Cantidad	Equipo	Descripción	Uso
3	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorio
50	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.31 Alternativa 2 - Factibilidad Técnica - CEC

3.4.1.2.9 LSI

Cantidad	Equipo	Descripción	Uso
3	Switch D-Link DGS-1224T 	El Switch DGS-1224T es compatible con IEEE 802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Ethernet (fibra) y 803.3x control de flujo. Este switch esta equipado para auto negociar velocidades a 10Mbps, 100Mbps y 1000Mbps.	Laboratorios LSI, Laboratorio MSIG, Auditórium
30	mts. Canaleta escalerilla calibre 20 de 12x5 cms	Marca Panduit	Organización general del cableado

Tabla 3.32 Alternativa 2 - Factibilidad Técnica - LSI

3.4.1.3 FACTIBILIDAD ECONÓMICA

3.4.1.3.1 COSTO DE HARDWARE

CANTIDAD	DETALLE	UNITARIO	COSTO TOTAL
2	*Router Cisco 2600*	*$1,456.00*	*$ 2,912.00*
1	*Router Cisco 1700*	*$1,116.70*	*$1,116.70*
4	*Access Point Cisco Aironet 1200*	*$600.00*	*$2,400.00*
24	*Switch D-Link DGS1224T 24Ptos.*	*$525.00*	*$12,600.00*
13	*Bobina de 305 m.*	*$250.00*	*$3,250.00*
350	*mts. de canaleta escalerilla calibre 20*	*$42.00*	*$14,700.00*
	Total Costo de Hardware		***$ 36,978.70***

Tabla 3.33 Alternativa 2 - Factibilidad Económica - Costo de Hardware

3.4.1.3.2 COSTO DE SOFTWARE

DETALLE	UNITARIO	COSTO TOTAL
Sistema operativo LINUX FEDORA CORE 3	*$0.00*	*$0.00*
Total Costo de Software		***$0.00***

Tabla 3.34 Alternativa 2 - Factibilidad Económica - Costo de Software

3.4.1.3.3 COSTOS OPERATIVOS

3.4.1.3.3.1 FASE DE ANÁLISIS LAN Y WAN

CANTIDAD	DETALLE	MESES	INDIVIDUAL	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2*	*$700*	*$1400*

Tabla 3.35 Alternativa 2 - Factibilidad Económica - Costos Operativos - Fase de análisis LAN y WAN

3.4.1.3.3.2 FASE DE DISEÑO E IMPLEMENTACIÓN LAN Y WAN

CANTIDAD	DETALLE	MESES	INDIVIDUAL	COSTO TOTAL
1	*Ing. Telecomunicaciones*	*2.5*	*$700*	*$1750*
4	*Técnicos en redes*	*1.5*	*$300*	*$1800*

Tabla 3.36 Alternativa 2 - Factibilidad Económica - Costos Operativos - Fase de implementación LAN y WAN

3.4.1.3.3.3 FASE DE DOCUMENTACIÓN Y PRUEBA

CANTIDAD	DETALLE	MESES	INDIVIDUAL	COSTO TOTAL
1	*Ing. Telecomunicacione*	*1.5*	*$700*	*$1050*
1	*Técnicos en redes*	*0.5*	*$300*	*$150*
			TOTAL COSTOS OPERATIVOS	*$6150*

Tabla 3.37 Alternativa 2 - Factibilidad Económica - Costos Operativos - Fase de documentación y prueba

3.4.1.3.4 COSTOS TOTALES

TOTAL COSTO DE EQUIPOS	*$ 36,978.70*
TOTAL COSTOS OPERATIVOS	*$6,150.00*
SUBTOTAL FACTIBILIDAD ECONÓMICA	***$ 43,128.70***
IMPREVISTOS 10%	***$4,312.87***
TOTAL FACTIBILIDAD ECONÓMICA	***$ 47,441.57***

Tabla 3.38 Alternativa 2 - Factibilidad Económica - Costos totales

3.4.1.3.5 FORMA DE PAGO

La forma de pago para ésta alternativa será el 90% antes de empezar la obra, ya que se necesitará comprar todo el material antes de la implementación de éste proyecto, y el saldo del 10% restante al concluir la misma.

3.4.1.4 FACTIBILIDAD OPERATIVA

3.4.1.4.1 FASE DE ANÁLISIS LAN Y WAN.

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Líder del proyecto, encargado del análisis de la situación actual.

Tabla 3.39 Alternativa 2 - Factibilidad Operativa - Fase de análisis LAN y WAN

3.4.1.4.2 FASE DE DISEÑO LAN Y WAN

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Líder del proyecto, encargado del diseño LAN y WAN

Tabla 3.40 Alternativa 2 - Factibilidad Operativa - Fase de diseño LAN y WAN

3.4.1.4.3 FASE DE IMPLEMENTACIÓN LAN Y WAN

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Líder, coordinador del grupo
6	Técnicos en Red	Cableado LAN

Tabla 3.41 Alternativa 2 - Factibilidad operativa - Fase de implementación LAN y WAN

3.4.1.4.4 FASE DE DOCUMENTACIÓN

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Elaboración de manuales

Tabla 3.42 Alternativa 2 - Factibilidad operativa - Fase de documentación

3.4.1.4.5 FASE DE PRUEBA

CANTIDAD	CARGO	FUNCIONES
1	Ing. en Elec. y Telecomun.	Pruebas WAN
1	Técnico en redes	

Tabla 3.43 Alternativa 2 - Factibilidad operativa - Fase de prueba

3.4.2 VENTAJAS Y BENEFICIOS ALTERNATIVA 2

3.4.2.1 VENTAJAS

- Aprovechar la adquisición de equipos de comunicación con nueva tecnología para mejorar el rendimiento de red y disminuir las colisiones.
- Mayor rendimiento y velocidad en el acceso a Internet.

3.4.2.2 BENEFICIOS

- Productividad y seguridad en la comunicación.
- Estudiantes satisfechos con Internet más veloz.
- Comunicación ininterrumpida con el Campus Prosperina.

3.4.3 DIAGRAMA DE GANTT

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**IMPLEMENTACIÓN CAMPUS LAS PEÑAS**	**109 días**	**jue 01/09/05**	**mar 31/01/06**
2	**Fase de análisis LAN y WAN**	**43 días**	**jue 01/09/05**	**lun 31/10/05**
3	Recopilación de datos	16 días	jue 01/09/05	jue 22/09/05
4	Analizar situación actual	10 días	vie 23/09/05	jue 06/10/05
5	Proponer soluciones	4 días	vie 07/10/05	mié 12/10/05
6	Cotización de dispositivos	7 días	jue 13/10/05	vie 21/10/05
7	Elaborar propuesta	3 días	lun 24/10/05	mié 26/10/05
8	Aceptación de la propuesta	3 días	jue 27/10/05	lun 31/10/05
9	**Fase de diseño de la red**	**44 días**	**mar 01/11/05**	**vie 30/12/05**
10	Diseño LAN	14 días	mar 01/11/05	vie 18/11/05
11	Diseño WAN	8 días	lun 21/11/05	mié 30/11/05
12	Compra de equipos	30 días	lun 21/11/05	vie 30/12/05
13	**Fase de implementación a nivel LAN y WAN**	**37 días**	**lun 21/11/05**	**mar 10/01/06**
14	Cableado de red LAN	30 días	lun 21/11/05	vie 30/12/05
15	Implementación WAN	7 días	lun 02/01/06	mar 10/01/06
16	**Fase de prueba**	**15 días**	**lun 02/01/06**	**vie 20/01/06**
17	Prueba de cableado estructurado	15 días	lun 02/01/06	vie 20/01/06
18	Prueba de enlace WAN	8 días	mié 11/01/06	vie 20/01/06
19	**Fase de documentación**	**1 día**	**mar 31/01/06**	**mar 31/01/06**
20	Elaboración de manuales	1 día	mar 31/01/06	mar 31/01/06

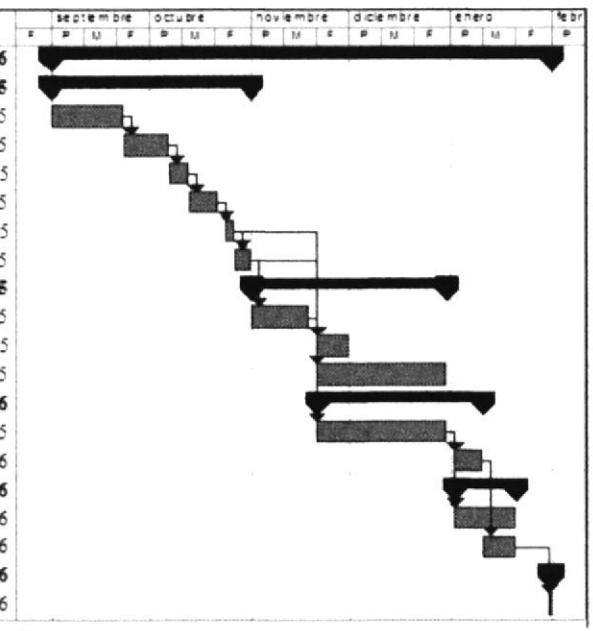


Figura 3.2 Alternativa 2 Diagrama de Gantt

CAPÍTULO 4

IMPLEMENTACIÓN LAN Y WAN

4. IMPLEMENTACIÓN WAN Y LAN

4.1 IMPLEMENTACIÓN WAN ESPOL

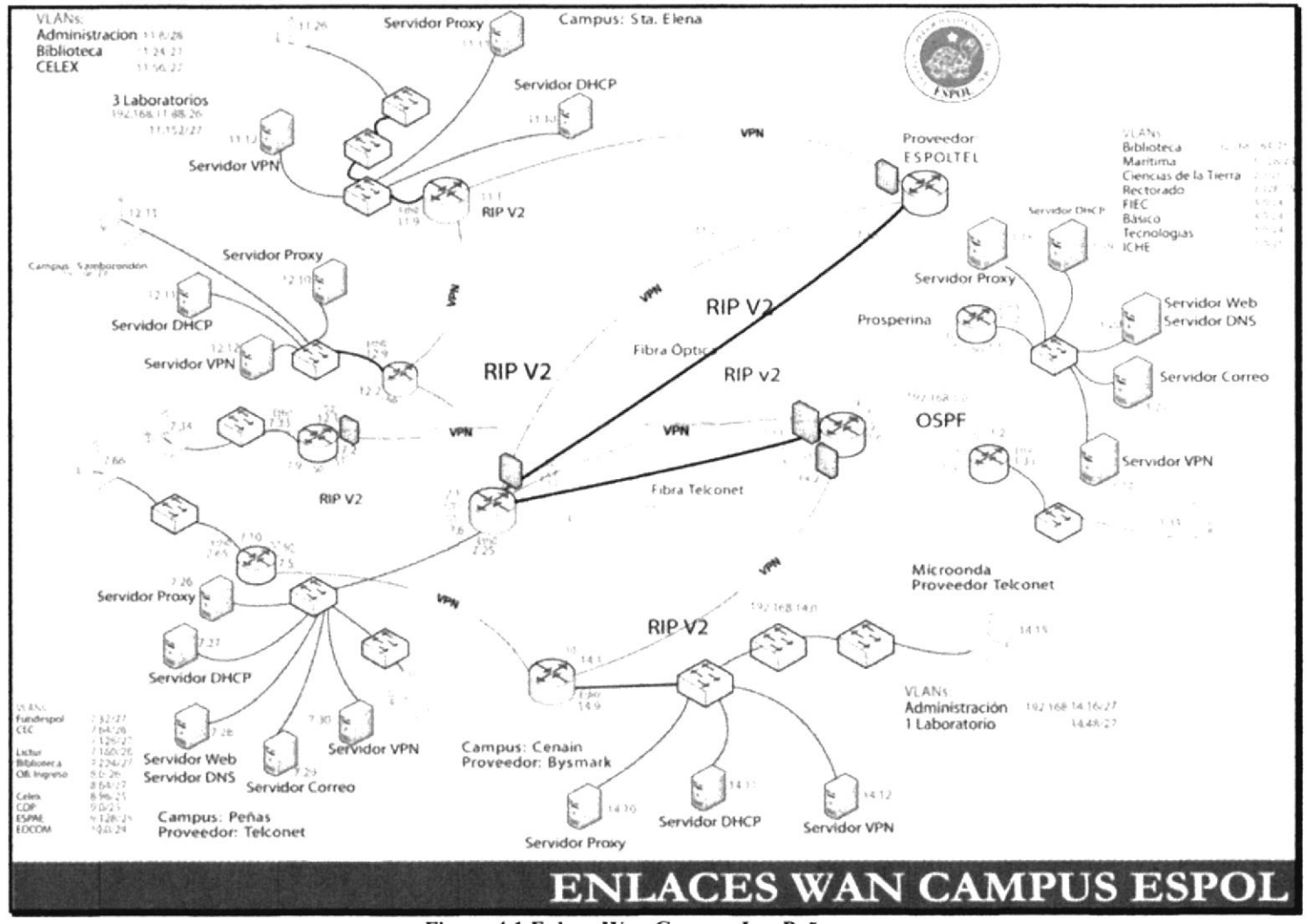


Figura 4.1 Enlace Wan Campus Las Peñas

4.2 IMPLEMENTACIÓN LAN

4.2.1 FUNDESPOL

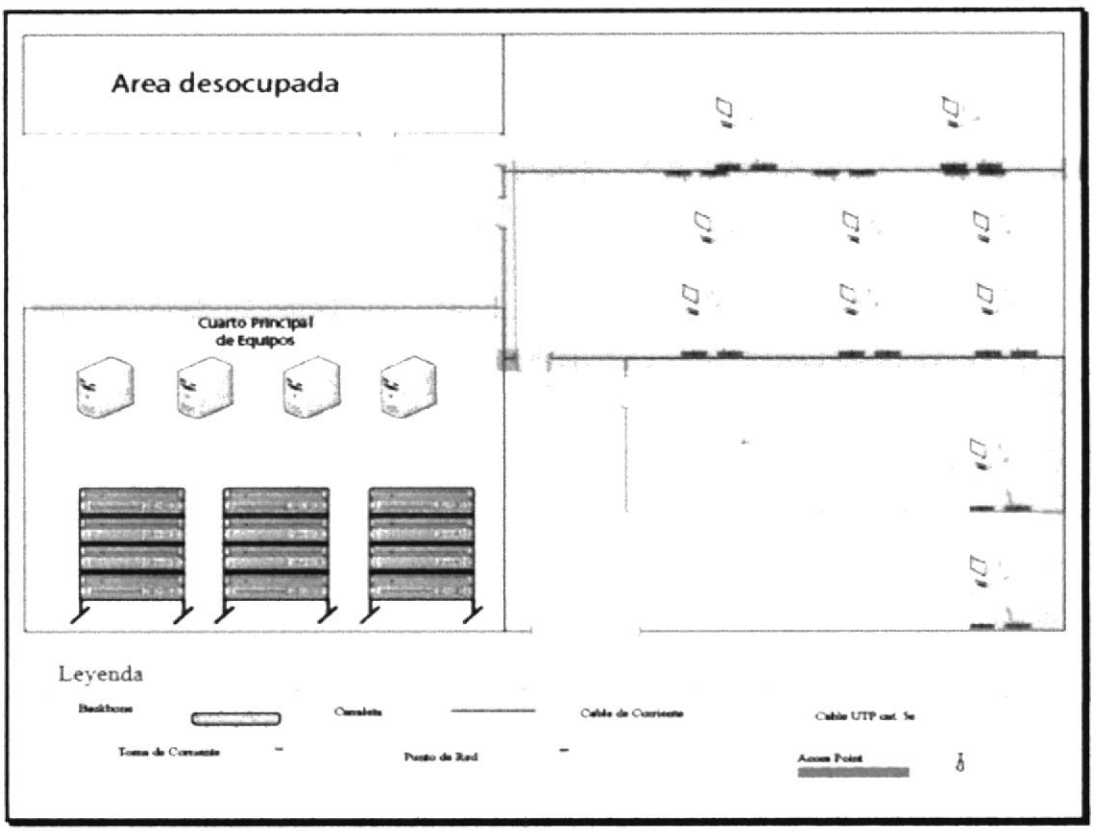


Figura 4.2 Implementación LAN Fundespol

4.2.2 OFICINA DE INGRESO

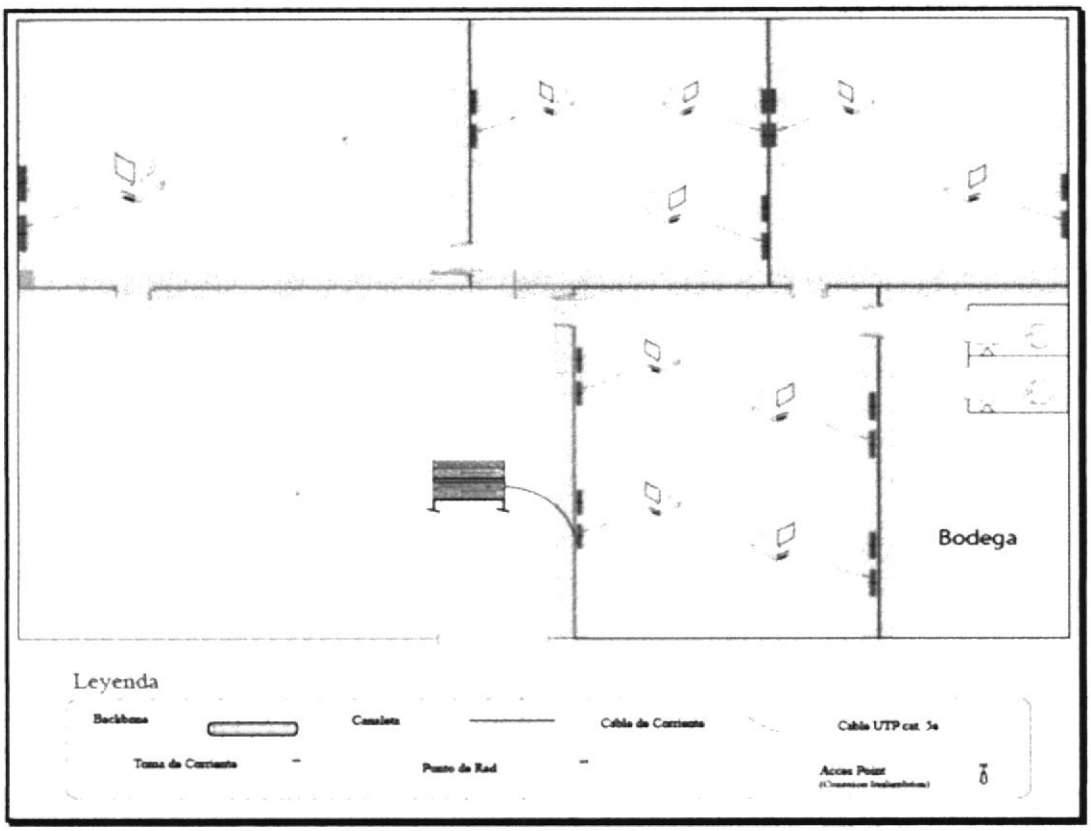


Figura 4.3 Implementación LAN Oficina de ingreso

4.2.3 EDCOM

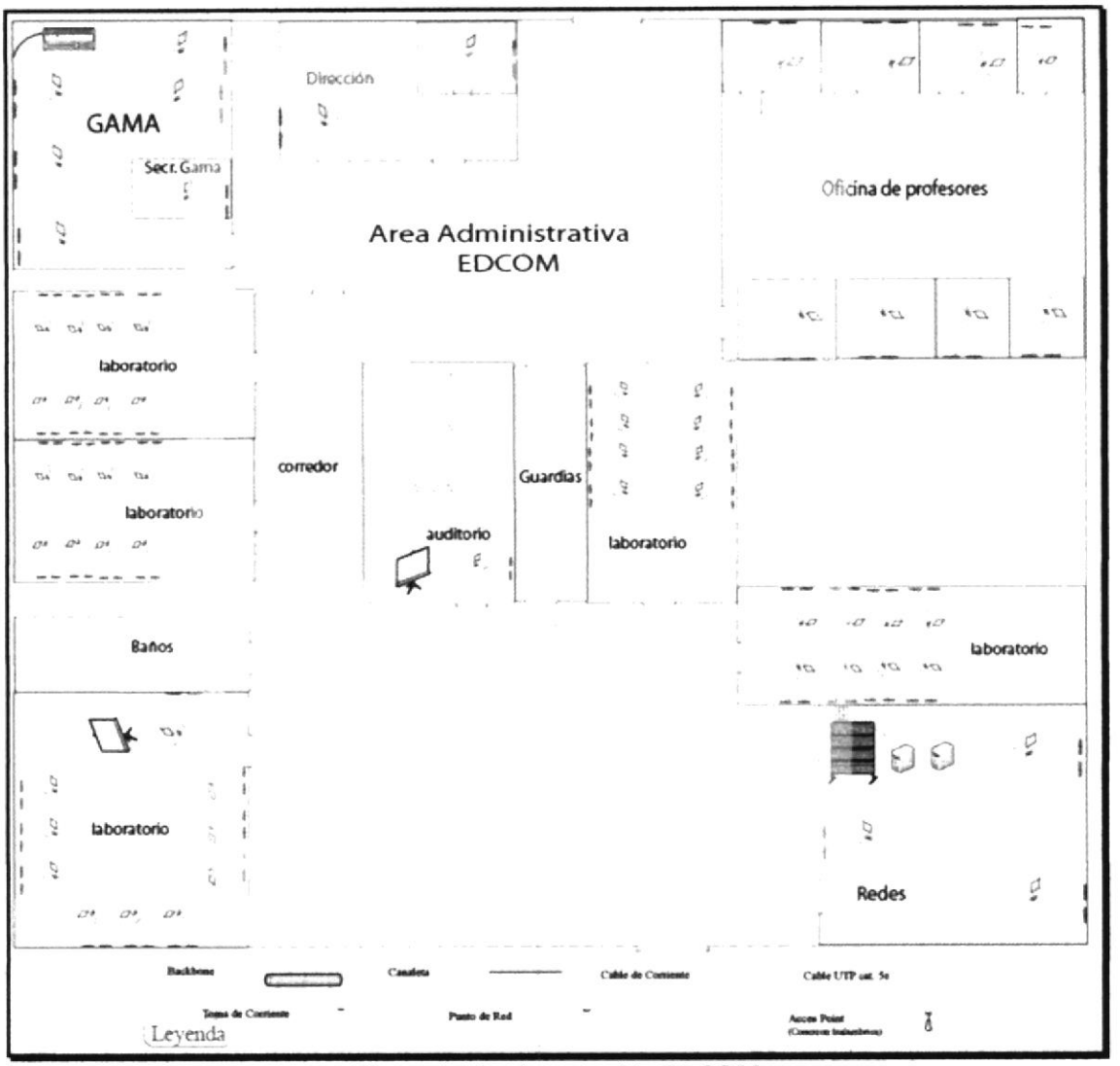


Figura 4.4 Implementación EDCOM

4.2.4 ESPAE

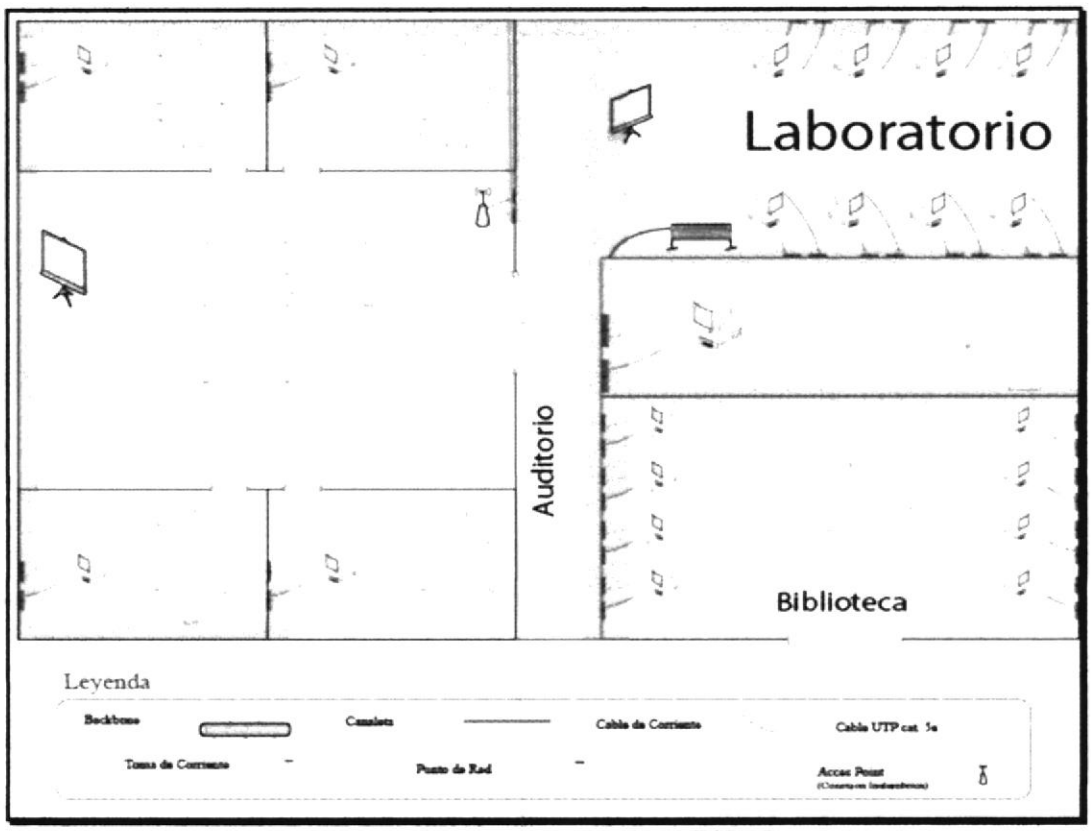


Figura 4.5 Implementación LAN ESPAE

4.2.5 CEC

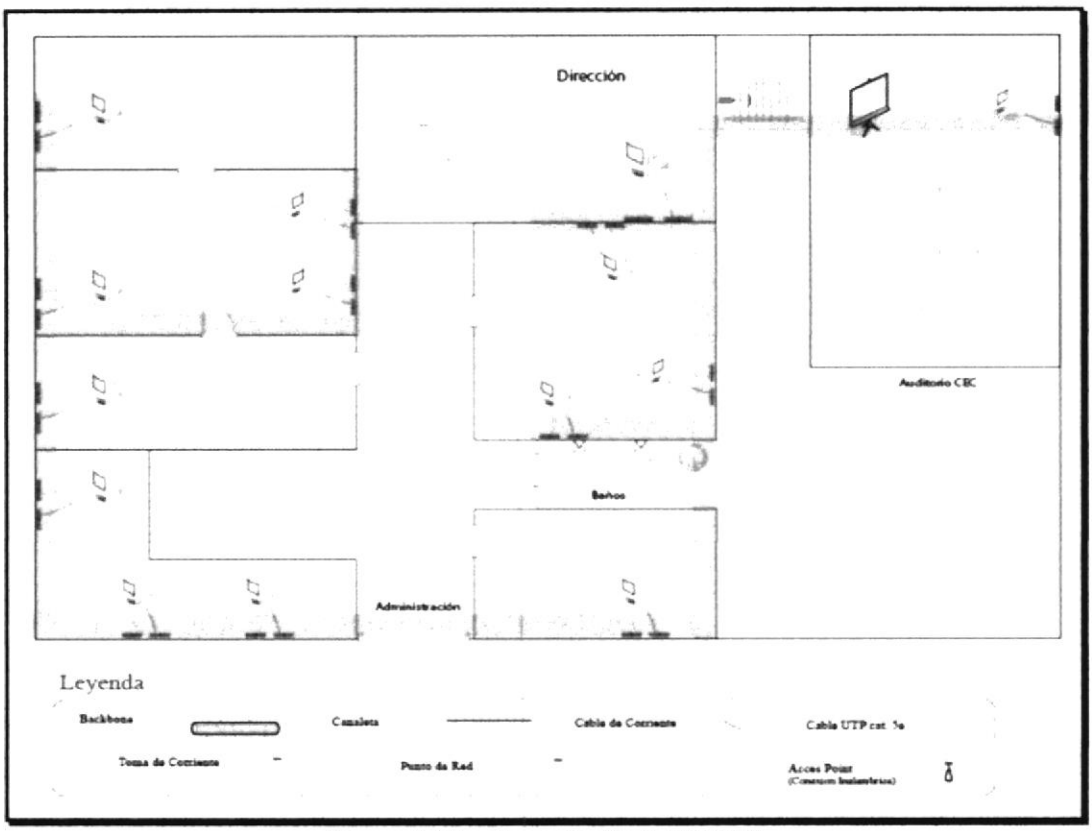


Figura 4.6 Implementación LAN CEC

4.2.6 CELEX

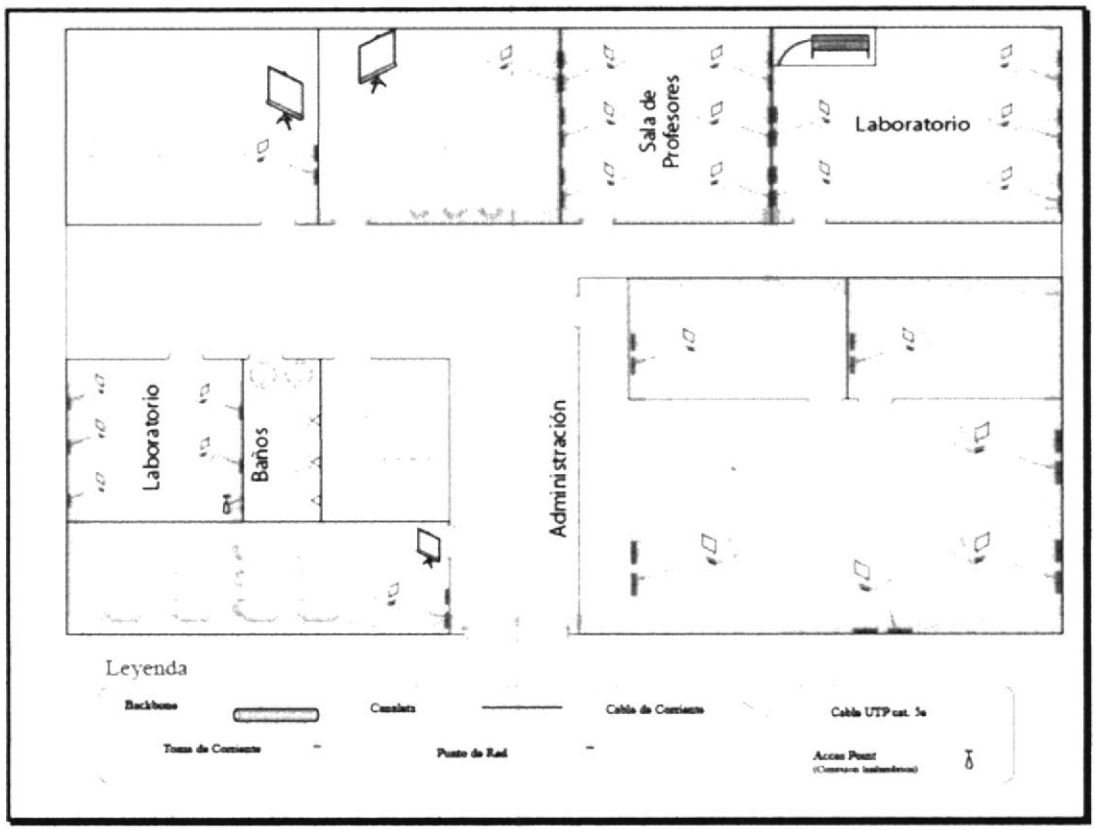


Figura 4.7 Implementación LAN CELEX

4.2.7 LSI

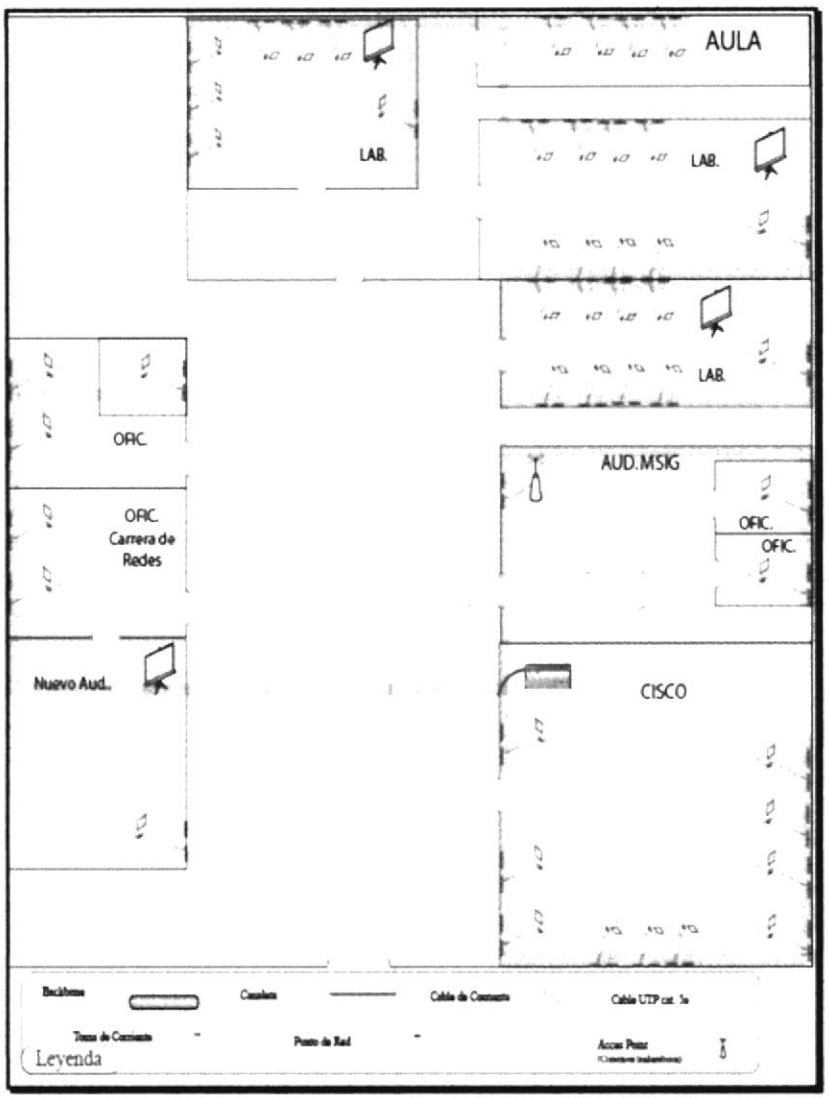


Figura 4.8 Implementación LAN LSI

4.2.8 LICTUR

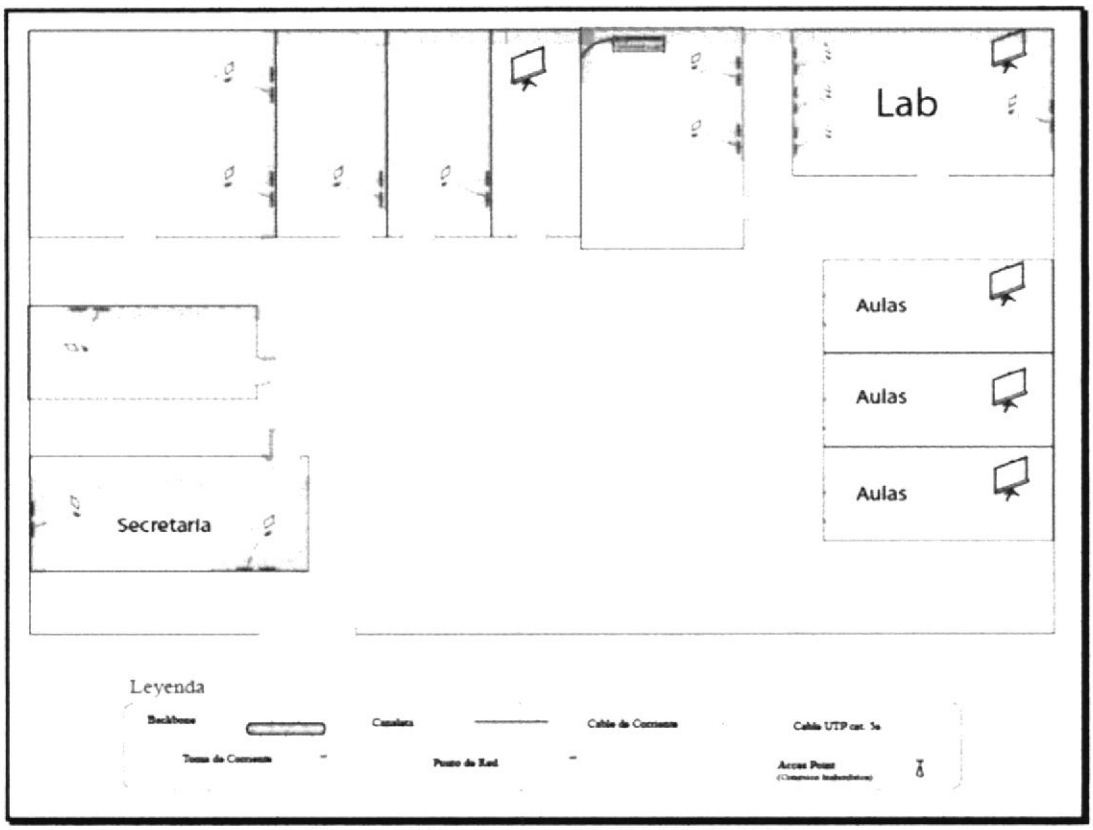


Figura 4.9 Implementación LAN LICTUR

4.2.9 BIBLIOTECA

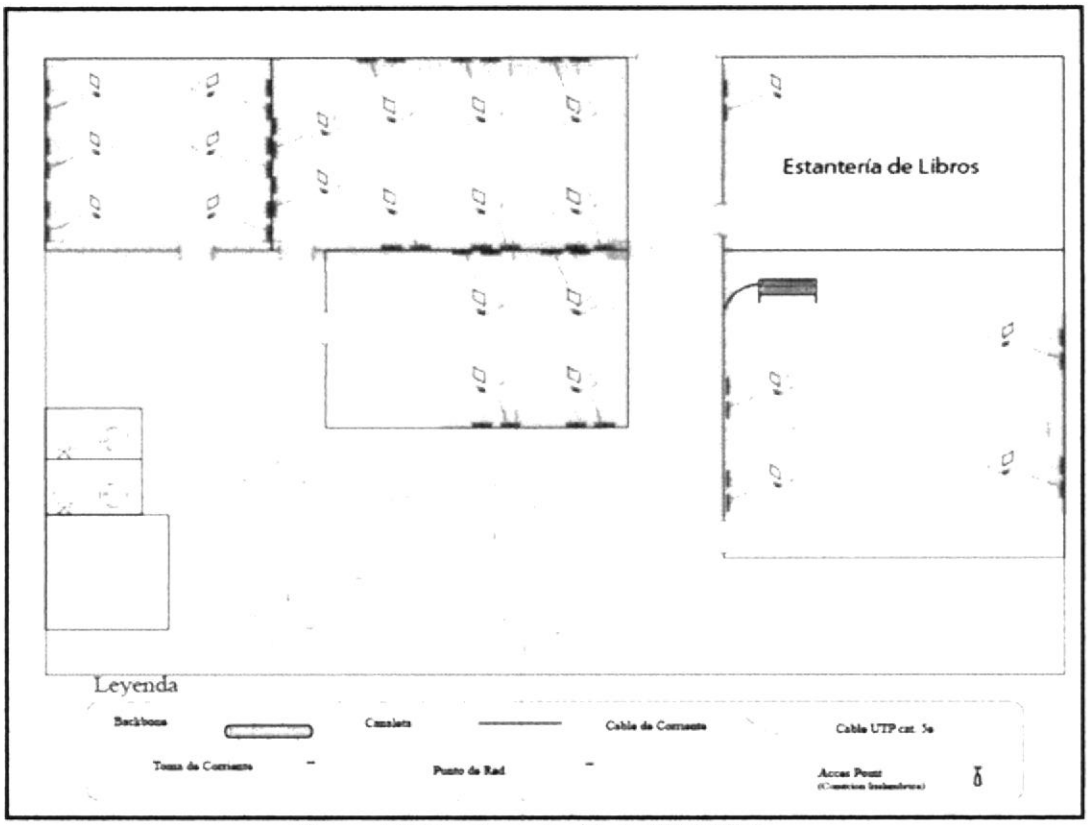


Figura 4.10 Implementación LAN Biblioteca

4.3 CONCLUSIONES

Nuestra finalidad es dar a conocer el estado actual de la estructura de la Red del campus Las Peñas, sugiriendo cambios a nivel de estructura física de la red, orientándonos al cableado estructurado donde pudimos encontrar falencias, y estableciendo un respectivo respaldo a nivel de comunicación entre éste campus y el campus Gustavo Galindo.

Utilizaremos el sistema operativo Linux, el mismo que es de distribución gratuita y uno de los más robustos en el mercado para brindar soporte a todos los usuarios de nuestra red por medio de los diferentes servicios que posee.

Proporcionaremos un respaldo a nivel de comunicaciones entre los campus Las Peñas y Gustavo Galindo (enlace WAN), por medio de creación de VPN (Virtual Private Network), para mayor seguridad en la comunicación.

CAPÍTULO 5

CONFIGURACIÓN DE DISPOSITIVOS

5. CONFIGURACIÓN DE DISPOSITIVOS

5.1 INTRODUCCIÓN A LOS ROUTERS

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

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

5.2 COMPONENTES INTERNOS DEL ROUTER

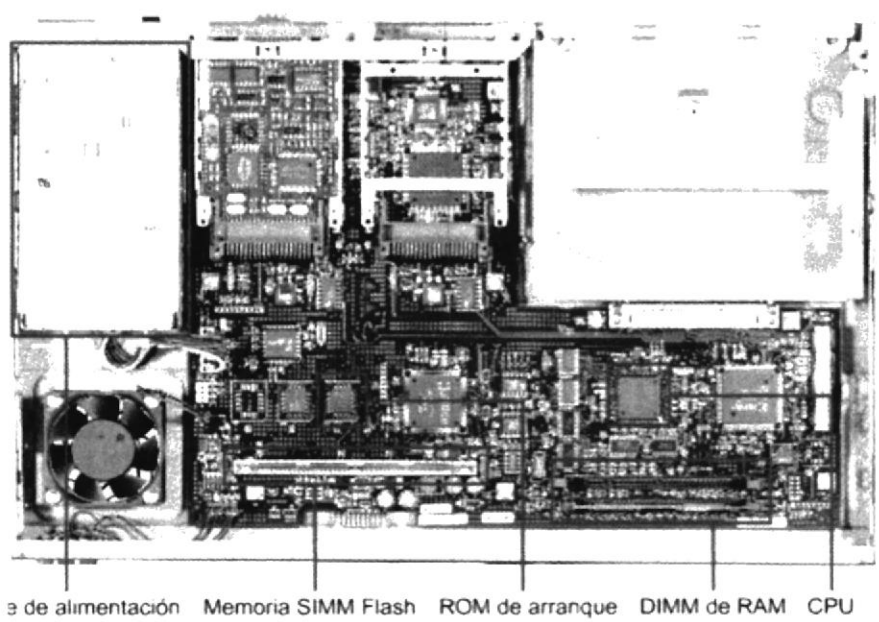


Figura 5.1 Componentes internos del Router

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.

5.3 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.

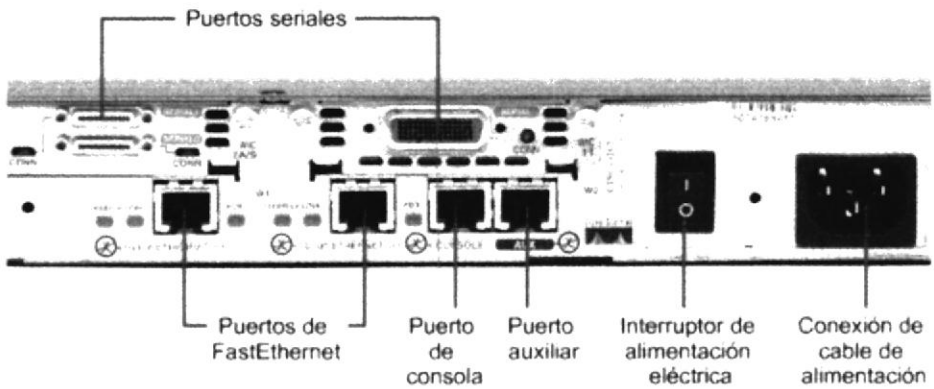


Figura 5.2 Conexiones Externas del Router

5.4 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.

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**.

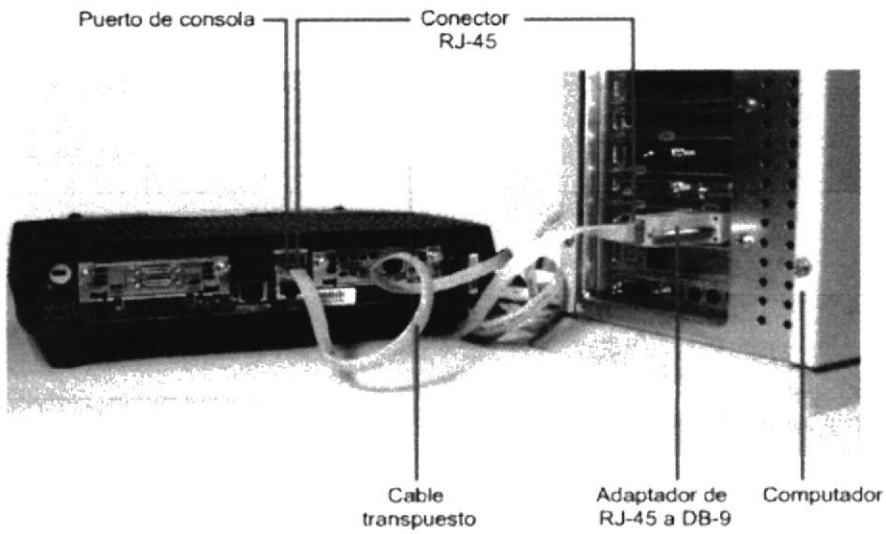


Figura 5.3 Conexiones del puerto de Administración

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.

5.5 CONFIGURACIONES EN EL ROUTER

5.5.1 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:

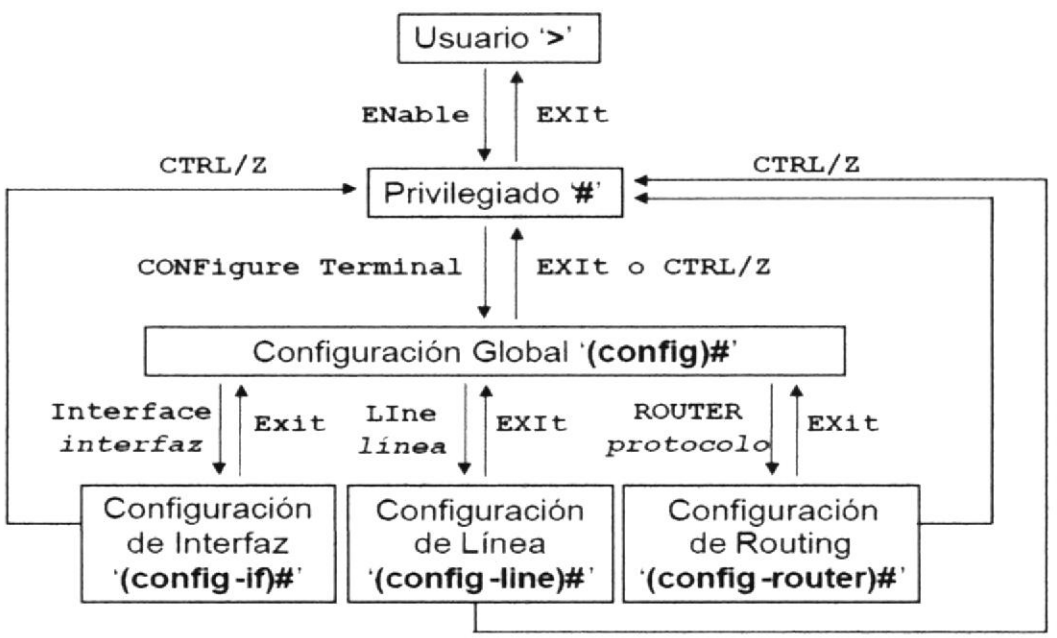


Figura 5.4 Esquema de permisos tipos de usuarios

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
- Sub-interfaces

- 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.

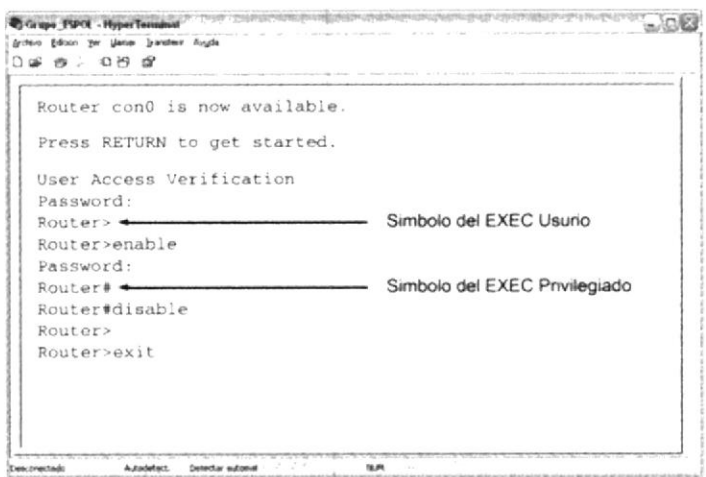


Figura 5.5 Tipos de Interfaz de Usuario

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

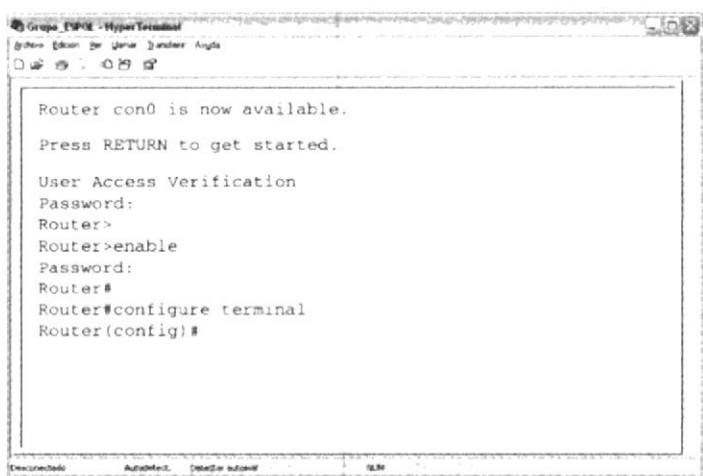


Figura 5.6 Tipos de Interfaz de Usuario

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.

5.5.2 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 el comando hostname seguido del nombre que le queramos asignar al router.
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.

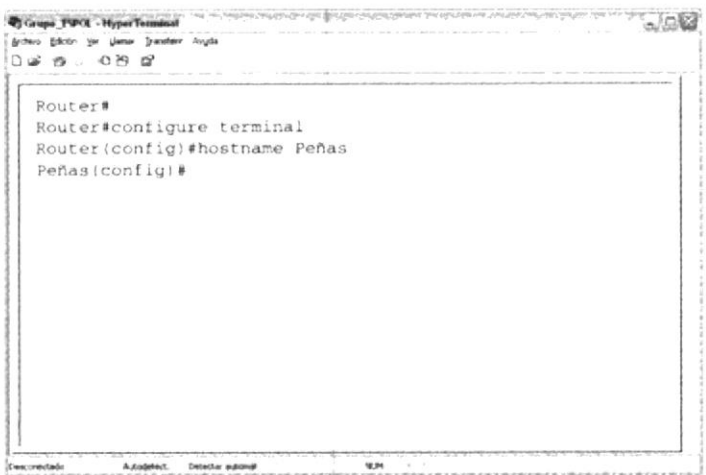


Figura 5.7 Configuración del nombre del Router

5.5.3 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.

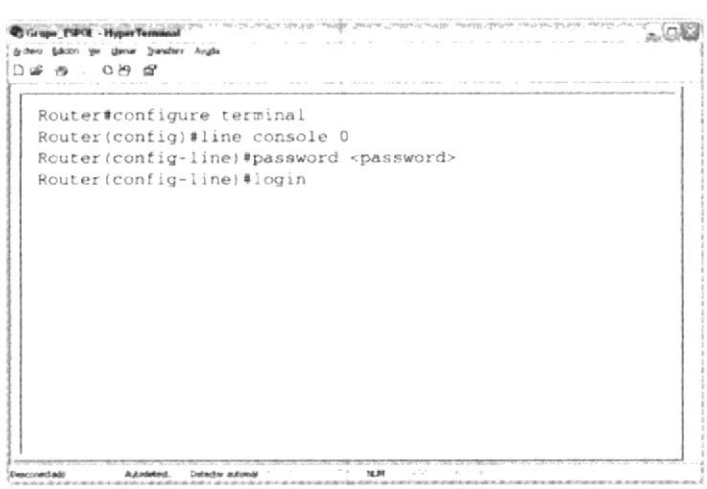


Figura 5.8 Configuración de contraseña del usuario Privilegiado

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:

Figura 5.9 Configuración de contraseña para el acceso remoto por telnet

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:

Figura 5.10 Cifrado de Contraseñas

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:

Figura 5.11 Encriptación de Contraseñas

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.

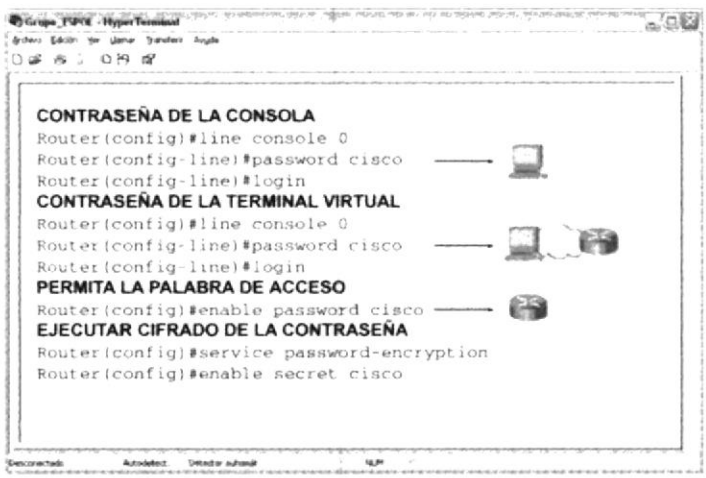


Figura 5.12 Configuración de Contraseñas

5.5.4 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.

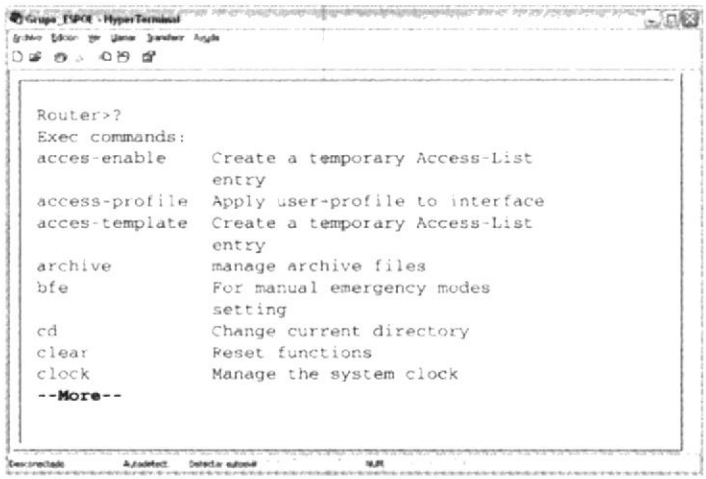


Figura 5.13 Ayuda en la interfaz de línea de comando

Esto se lo puede utilizar con cualquier comando, por ejemplo 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.

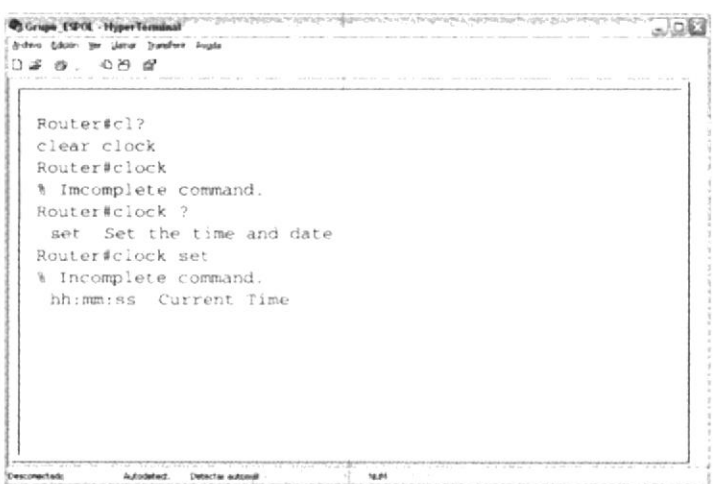


Figura 5.14 Configuración del reloj del router

5.5.5 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.

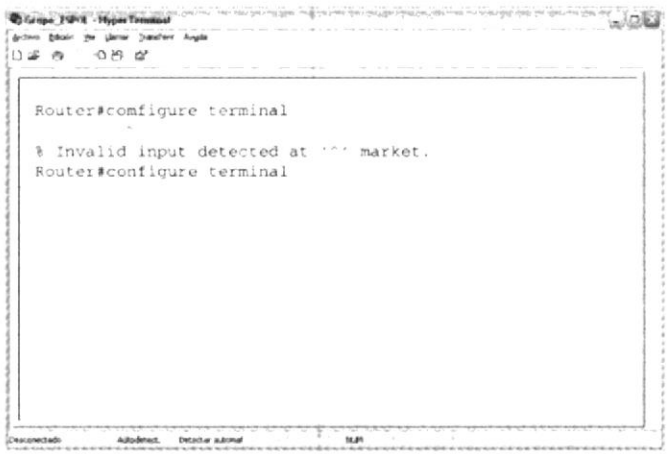


Figura 5.15 Diagnóstico de Fallos

Si una línea de comando es escrita de forma incorrecta y se presiona la tecla *Enter*, 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.

5.6 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:

Figura 5.16 Comando Show Interfaces

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

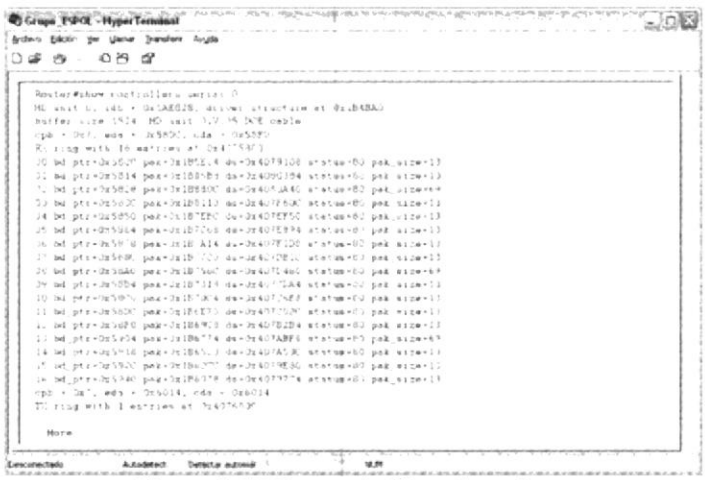


Figura 5.17 Comando Show Interfaces

- **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 router y 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.

5.6.1 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. Configura la dirección de IP mediante los siguientes comandos:

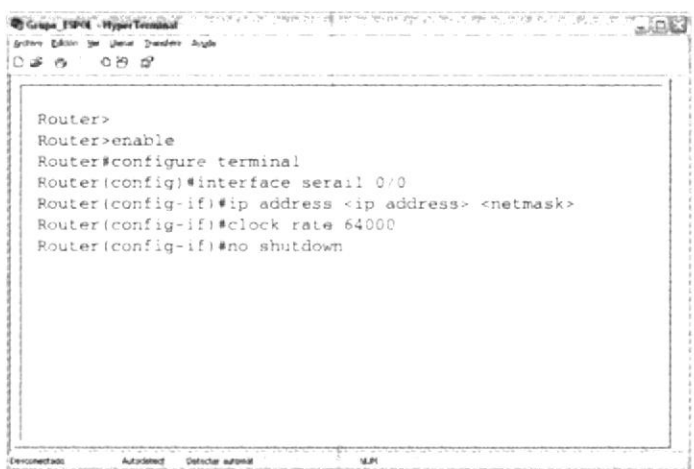


Figura 5.18 Configuración de una interfaz serial DCE

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.

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.

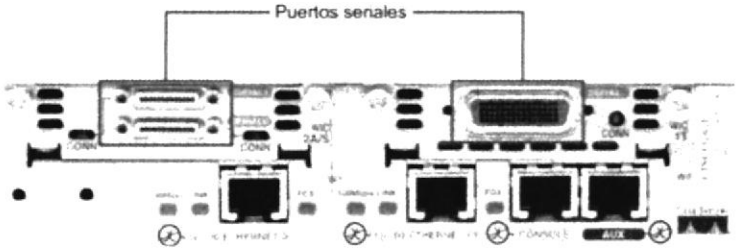


Figura 5.19 Puertos Seriales

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.

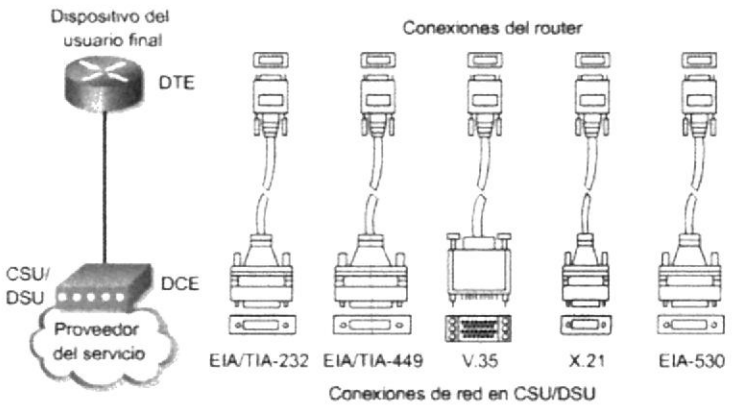


Figura 5.20 Conexiones del Router DCE/DTE

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.

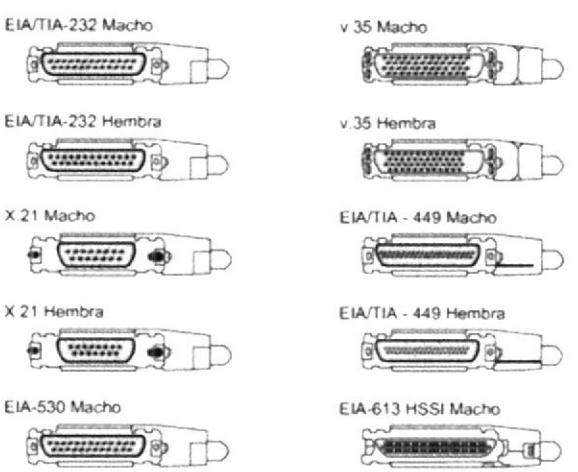


Figura 5.21 Tipos de Seriales de un Router

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:

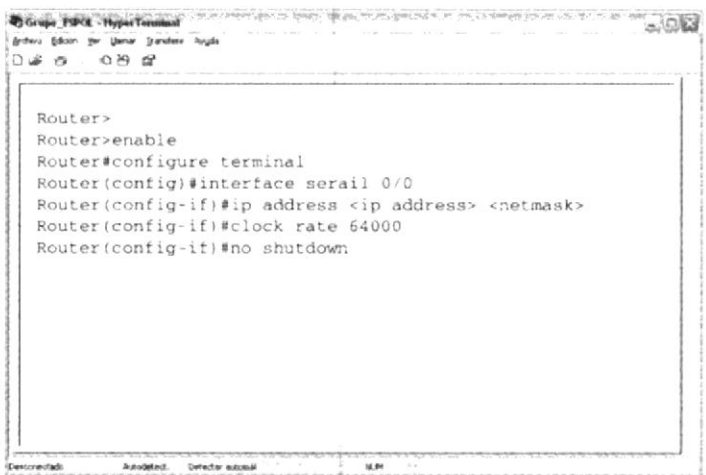


Figura 5.22 Configuración de una interfaz serial DCE

5.6.2 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.

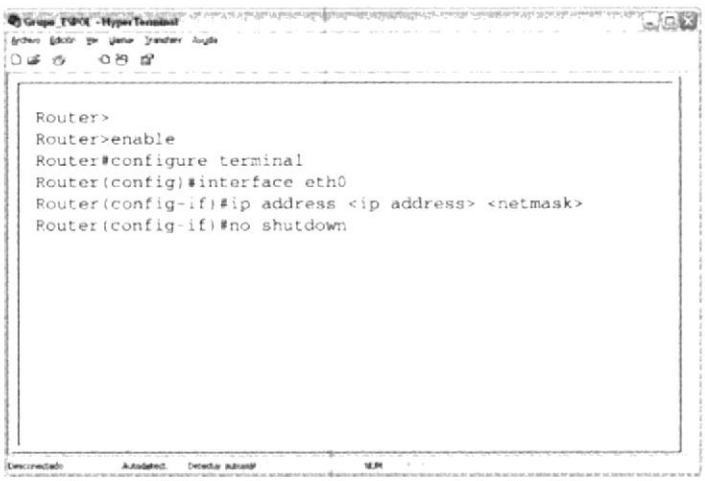


Figura 5.23 Configuración de una interfaz Ethernet

5.6.3 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.

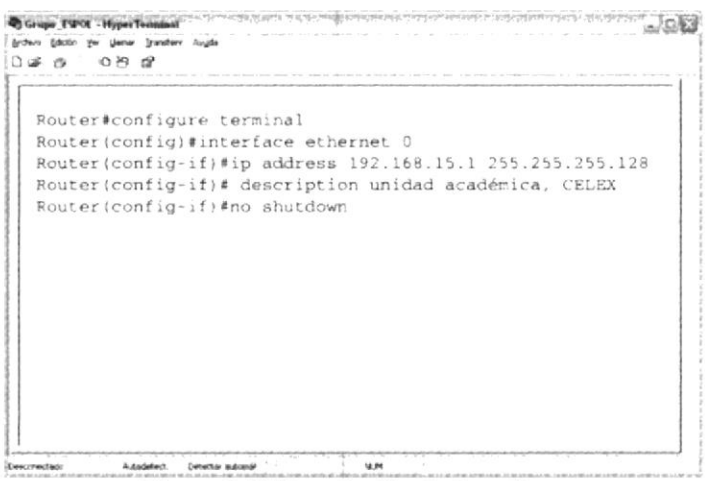


Figura 5.24 Descripción de Interfaces

5.6.4 CONFIGURACIÓN DEL MENSAJE DEL DÍA (MOTD)

Ingrese al modo de configuración global para configurar un texto como mensaje del día (MOTD). Use el comando banner motd, seguido de un espacio y un delimitador, como por ejemplo el signo numeral (#). Escriba el mensaje del día (MOTD) seguido de un espacio y de nuevo el delimitador.

Siga estos pasos para crear y mostrar un mensaje del día:

1. Ingrese al modo de configuración global, mediante el comando **configure terminal**.
2. Escriba el comando **banner motd#** Solo personal autorizado **#**.
3. Guarde los cambios mediante el comando **copy running-config startup-config**

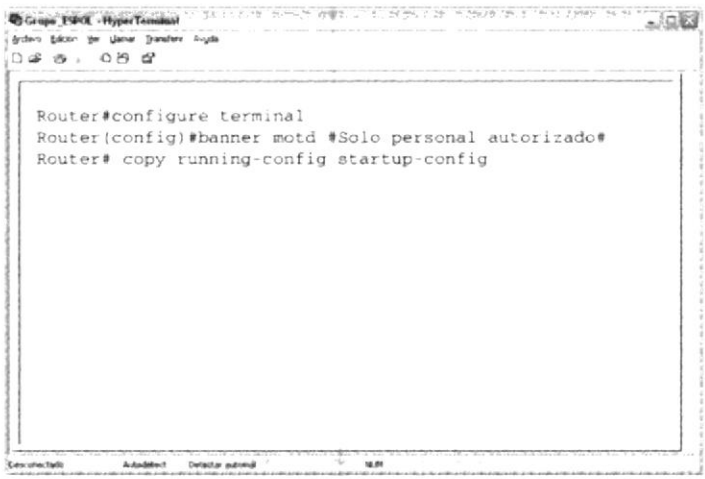


Figura 5.25 Configuración de mensaje del Día

5.7 CONFIGURACIÓN DE TABLAS DE HOST

Para asignar nombres de host a direcciones, primero ingrese al modo de configuración global. Ejecute el comando ip host seguido del nombre de destino y todas las direcciones de IP con las que se puede llegar al dispositivo.

El procedimiento para configurar la tabla de host es:

1. Ingrese al modo de configuración global en el router.
2. Ejecute el comando **ip host** seguido del nombre del router y todas las direcciones de IP asociadas con las interfaces en cada router.
3. Repita el proceso, hasta que todos los routers de la red hayan sido configurados.
4. Guarde la configuración en la NVRAM.

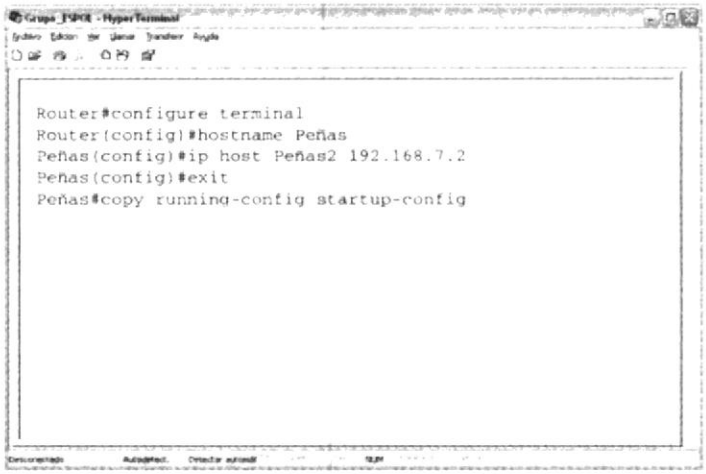


Figura 5.26 Configuración de tablas de host

5.7.1 ENRUTAMIENTO

5.7.1.1 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**.

Figura 5.27 Configuración de enrutamiento estático

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:

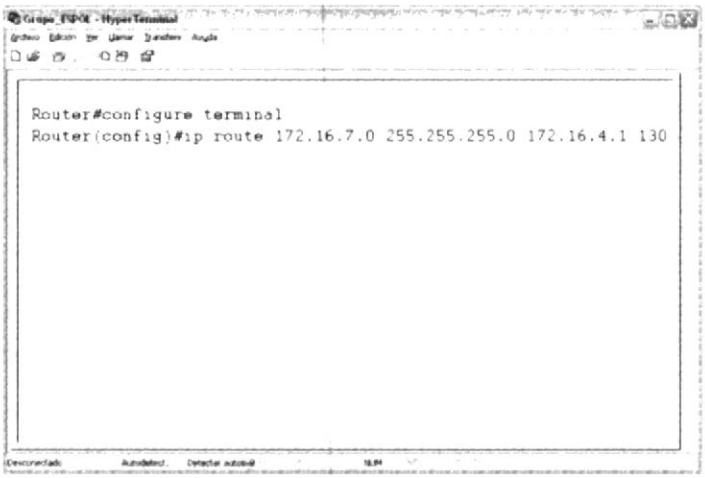


Figura 5.28 Configuración de enrutamiento estático 2

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta. A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

5.7.1.2 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 startup-config.**

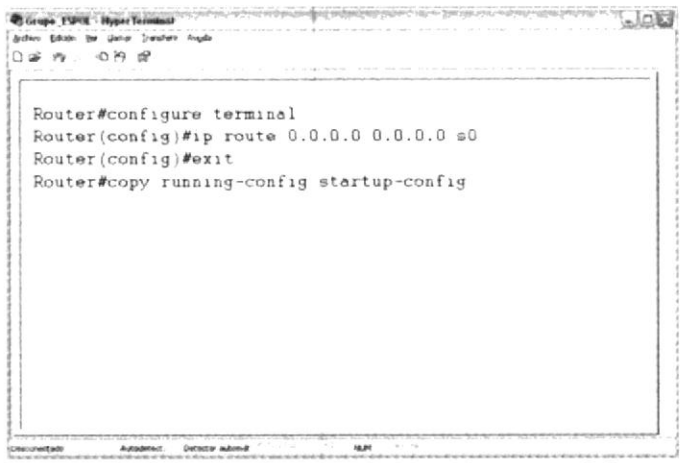


Figura 5.29 Configuración de enrutamiento por defecto

5.7.1.3 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.

5.7.1.3.1 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.

5.7.1.3.1.1 TIPOS DE 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 bVlan ceo 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.

5.7.1.4 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).

Para configurar RIP v1 empezamos digitando el comando **router** el cual 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:

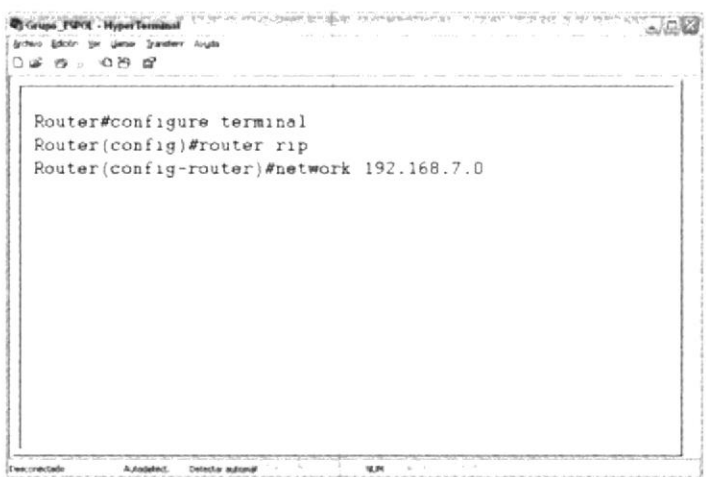


Figura 5.30 Configuración de Protocolo Rip v1

5.7.1.4.1 MEJORAS EN RIP V2

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

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.

Un ejemplo de configuración de enrutamiento rip versión 2 es:

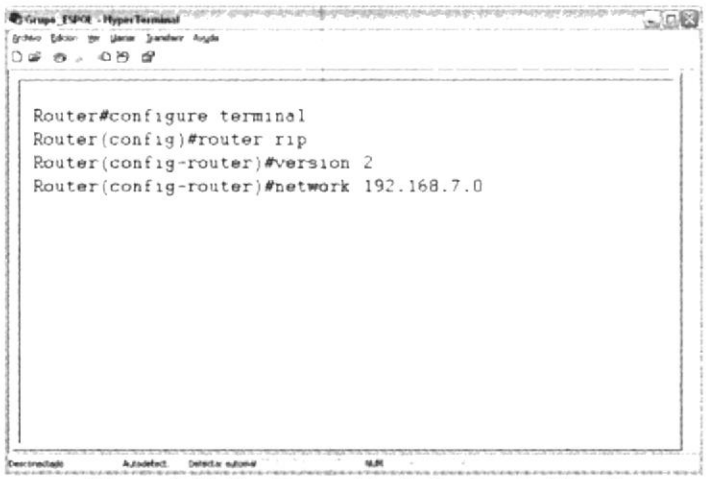


Figura 5.31 Configuración de Protocolo Rip v2

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.

Figura 5.32 Comando Show ip route

5.7.1.5 PROTOCOLOS DE ENRUTAMIENTO DE ESTADO DE ENLACE

Los algoritmos de estado de 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 rutas 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 de enlace no patentado. Las características clave del OSPF son las siguientes:

- Es un protocolo de enrutamiento de estado de 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.

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

OSPF ofrece soluciones a los siguientes problemas:

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

5.7.1.5.1.1 TIPOS DE REDES 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.

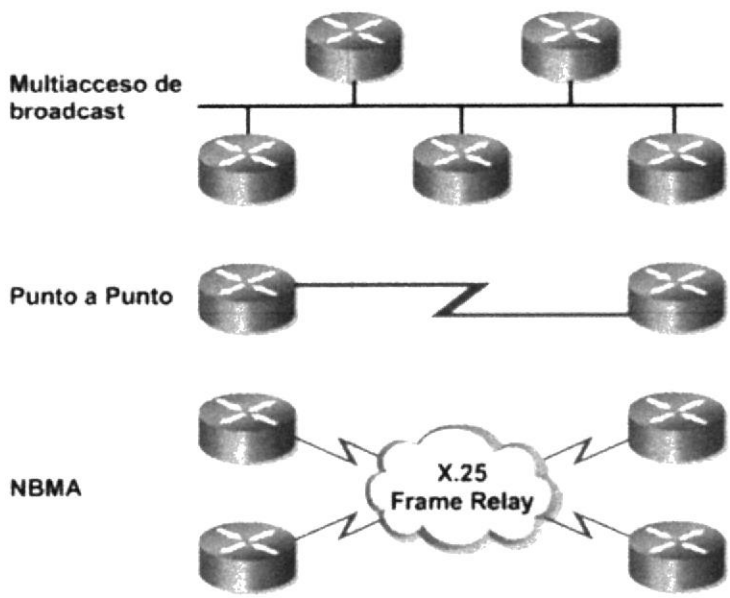


Figura 5.33 Tipos de red OSPF

5.7.1.5.1.2 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.

Figura 5.34 Configuración del Protocolo de enrutamiento OSPF

5.7.1.5.1.3 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 192.168.7.1 255.255.255.255**

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.

Figura 5.35 Configuración de la interfaz loopback

5.7.1.5.1.4 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.

Figura 5.36 Modificación de la métrica de los costos de OSPF

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 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.

Figura 5.37 Modificación de la métrica de los costos de OSPF

5.7.1.5.1.5 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:

Figura 5.38 Configuración de los temporizadores OSPF

5.7.1.5.1.6 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.

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

Figura 5.39 Comando Show ip protocol

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.

Figura 5.40 Comando show ip route

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.

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.

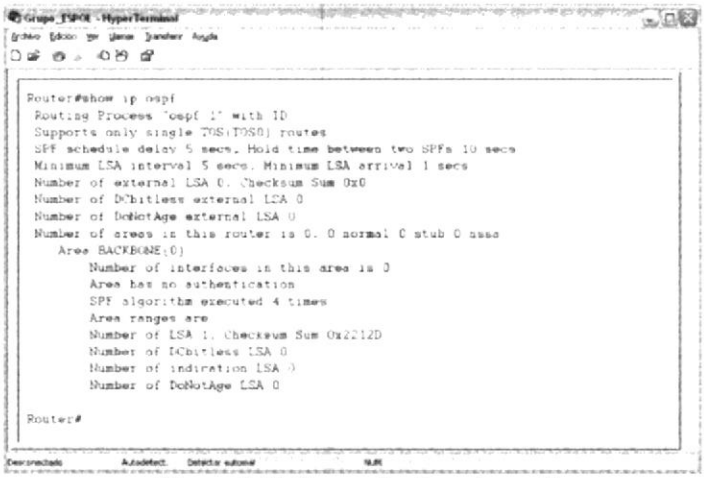


Figura 5.41 Comando show ip ospf

Show ip ospf neighbor detail. – Este comando muestra un listado detallado de vecinos, sus prioridades y estados.

Show ip ospf database.- Esto muestra el contenido de la base de datos topológica que mantiene el router y el ID del proceso OSPF.

5.7.2 LISTAS DE CONTROL DE ACCESO (ACL'S)

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

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

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

Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX). Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

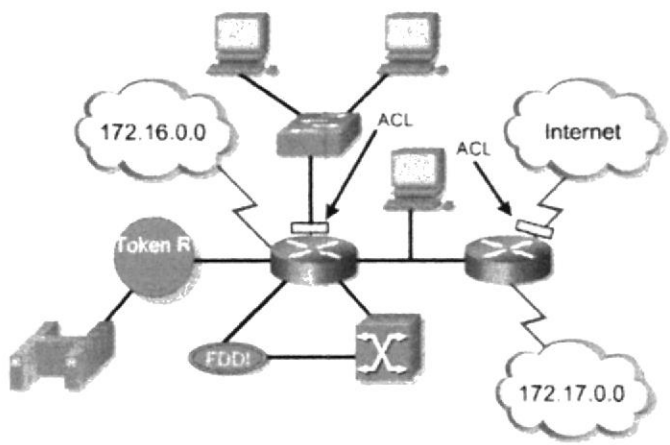


Figura 5.42 Grafico de ubicación de ACL's

5.7.2.1 FUNCIONAMIENTO DE LAS ACL

El orden en el que se ubican las sentencias de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL.

Una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo. Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice **deny any** (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea deny any no sea visible como última línea de una ACL, está ahí y no permitirá que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada. Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el deny any al final de las ACL para reforzar la presencia dinámica de la prohibición implícita deny.

5.7.2.2 CREACIÓN DE LAS ACL

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

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

Tabla 5.1 Rangos para crear una ACL

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.

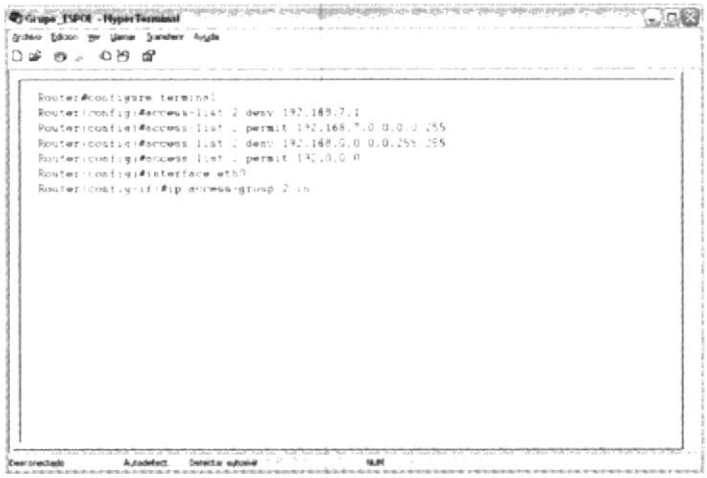


Figura 5.43 Borrar ACL`s

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.

Figura 5.44 Borrar ACL`s

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

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

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

Se la puede escribir como:

Router(config)#access-list 1 **permit any**

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

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

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

Se la puede escribir como:

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

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

5.7.2.4 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.

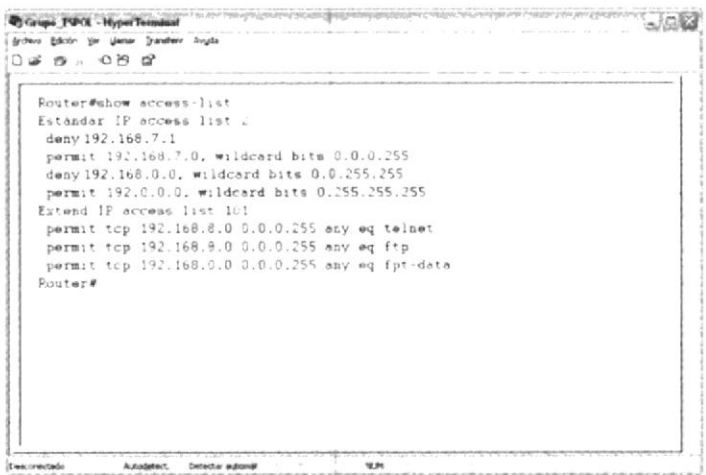


Figura 5.45 Verificación de las ACL's

5.7.3 TIPOS DE ACL'S

5.7.3.1 ACL ESTÁNDAR

En la versión 12.0.1 del IOS de Cisco, se usaron por primera vez números adicionales (1300 al 1999) para las ACL's estándar pudiendo así proveer un máximo posible de 798 ACL's estándar adicionales, a las cuales se les conoce como ACL's IP expandidas. (También entre 1300 y 1999 en IOS recientes) En la primera sentencia ACL, cabe notar que no hay máscara wildcard. En este caso donde no se ve ninguna lista, se utiliza la máscara por defecto, que es la 0.0.0.0. Esto significa que toda la dirección debe concordar o que esta línea en la ACL no aplica y el router debe buscar una concordancia en la línea siguiente de la ACL.

La sintaxis completa del comando ACL estándar es:

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

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

Figura 5.46 Utilización del comando remark

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**}

5.7.3.2 ACL EXTENDIDA

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

Es posible configurar múltiples sentencias en una sola ACL. Puede haber tanta cantidad de sentencias de condición como sean necesarias, siendo la única limitación la memoria disponible en el router.

La sintaxis de una sentencia ACL extendida puede ser muy extensa y a menudo, se vuelve engorrosa en la ventana terminal. Las wildcards también tienen la opción de utilizar las palabras clave **host** o **any** en el comando.

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

Las operaciones lógicas pueden especificarse como igual (eq), desigual (neq), mayor a (gt) y menor a (lt) 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.

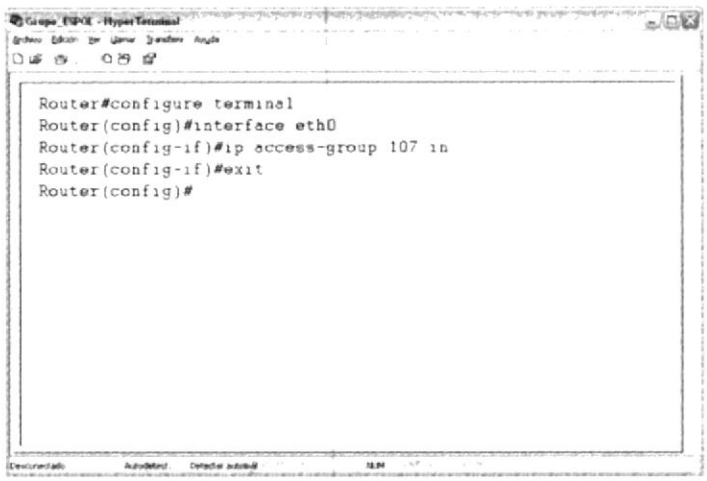


Figura 5.47 Implementación acl extendida en la interfaz.

5.7.3.3 UBICACIÓN DE LA 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 donde 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.

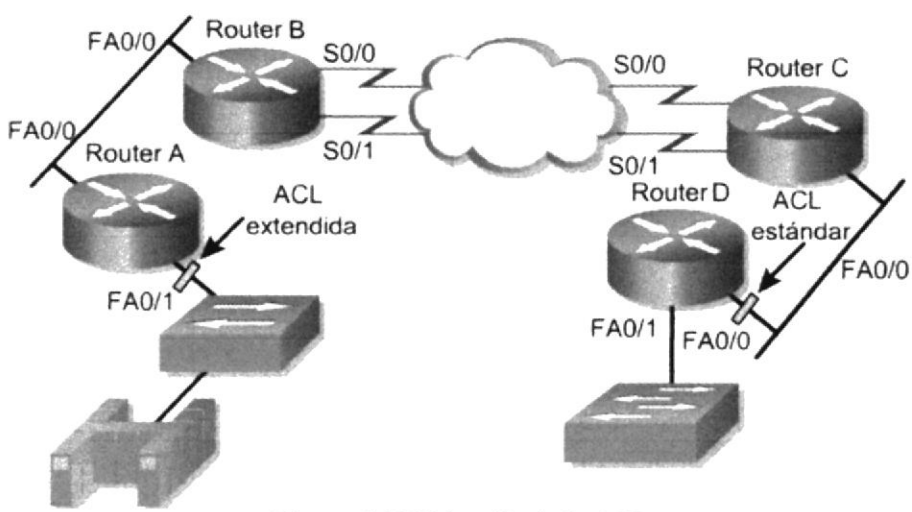


Figura 5.48 Ubicación de la ACL

5.7.4 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 ACL's para cada protocolo de red configurado en las interfaces del router.

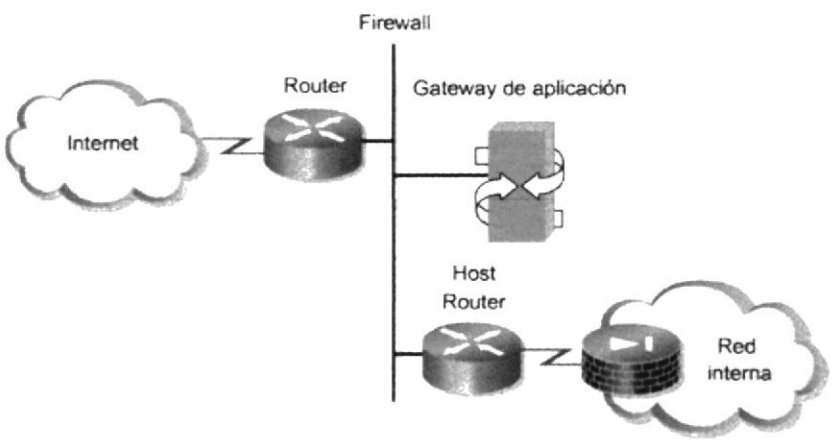


Figura 5.49 Implementación de Firewall

5.8 PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE ROUTERS (GRUPO – ESPOL)

Ahora pasaremos a configurar paso a paso los diferentes Routers de la red ESPOL.

5.8.1 CONEXIÓN DE UNA TERMINAL CON LA CONSOLA DEL ROUTER

Antes de empezar, tenemos que tener claro que nuestra conexión se realizará a través de la Aplicación HyperTerminal de Windows.

> **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. Con un cable transpuesto **RJ-45** a **RJ-45** y un adaptador **RJ-45** a **DB-9** o **RJ-45** a **DB-25** conectar de una Terminal (PC – Personal Computer) al puerto de consola del Router.
2. Abrimos la aplicación HyperTerminal siguiendo los siguientes pasos.
   - En el Escritorio de Windows clic con el botón izquierdo en el menú "Inicio"

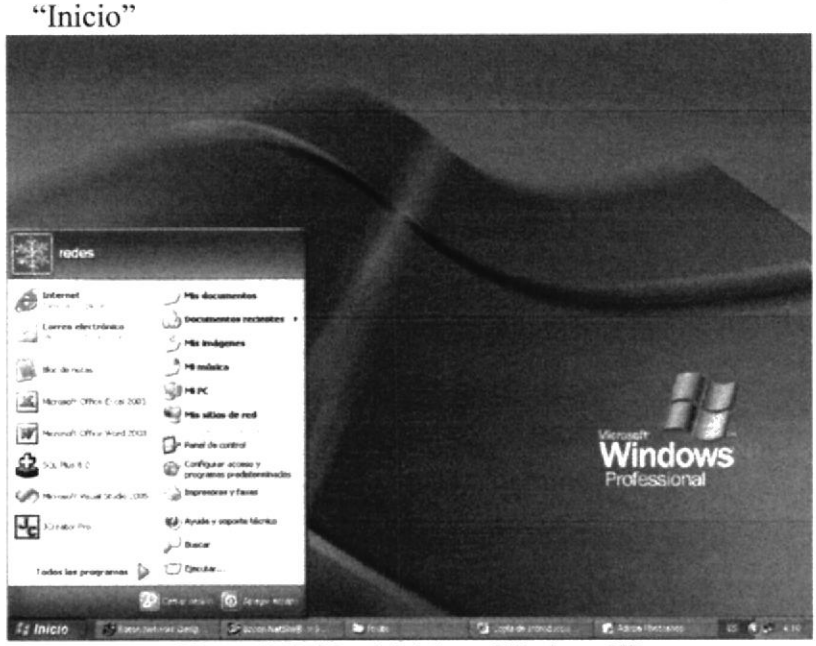


Figura 5.50 Menú Inicio en Windows XP

   - En el menú desplegable buscar la opción **"Todos los Programas"** o **"Programas"** según la versión y dar un clic con el botón izquierdo la cual desplegará otro pequeño submenú.

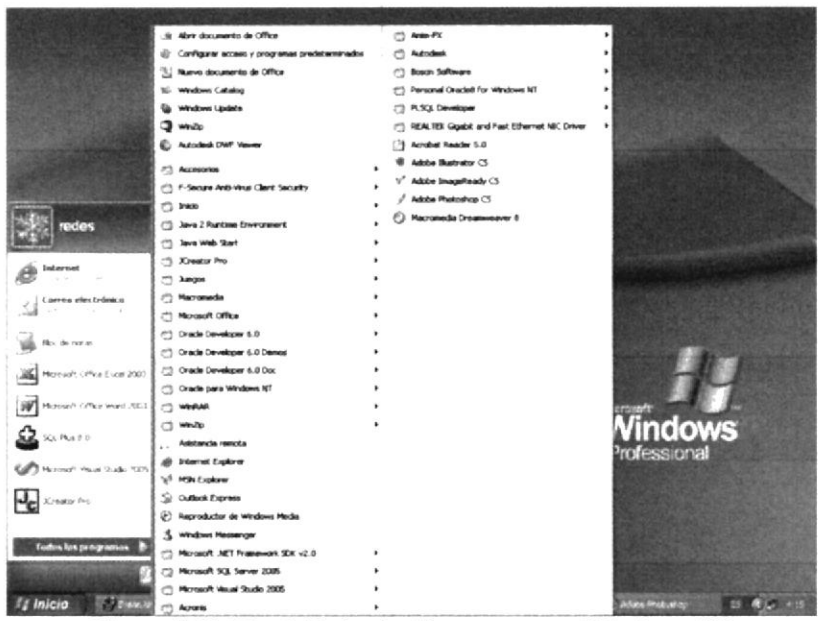


Figura 5.51 Menú Todos los Programas en Windows XP

- En este submenú buscar la opción **"Accesorios"** y dar un clic izquierdo, la cual hará acceder a un nuevo nivel de submenú.

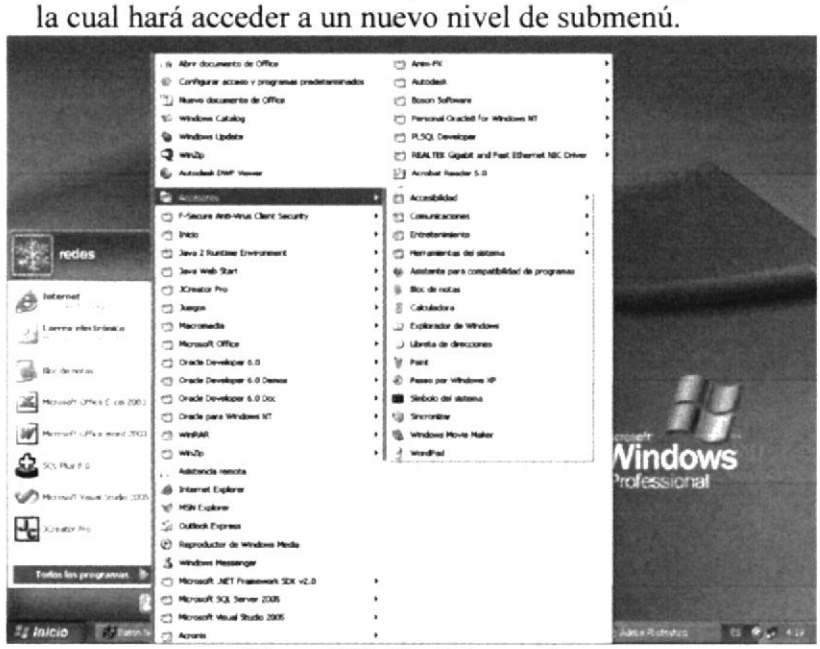


Figura 5.52 Menú Accesorios

- En este submenú aparecerán algunas de las herramientas que proporciona Windows, y la que interesa es la de Comunicaciones, dar clic izquierdo.

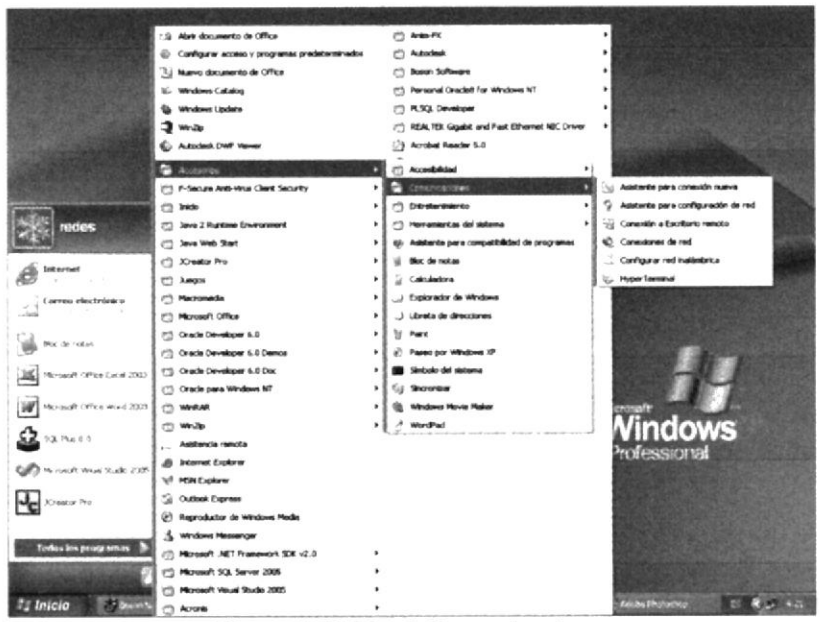


Figura 5.53 Menú Comunicaciones

- Buscar la aplicación de HyperTerminal en el submenú que se desplegó y dar clic izquierdo.

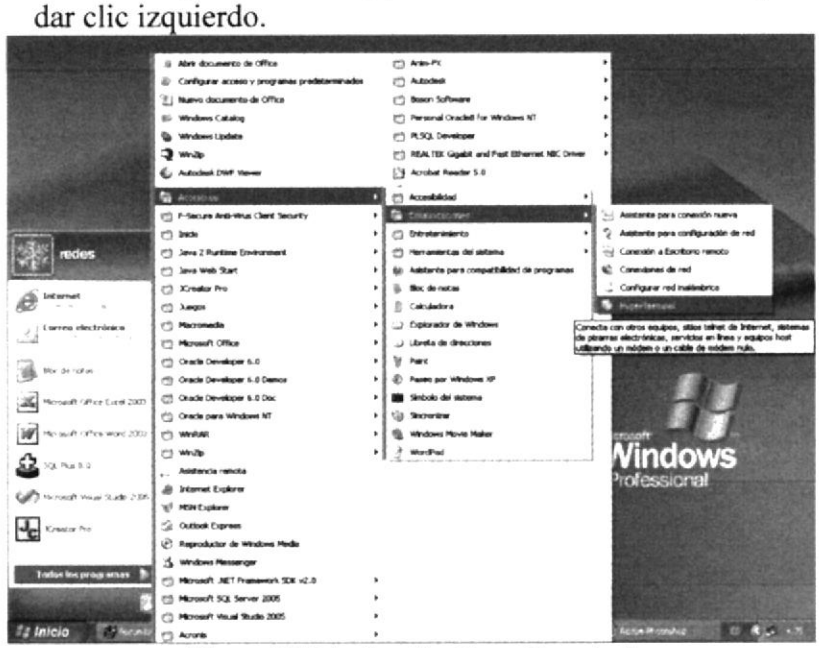


Figura 5.54 Aplicación HyperTerminal

3. Una vez que se ha encontrado dar clic izquierdo en el menú de HyperTerminal, si es la primera vez que se accede a esta aplicación, aparecerá una ventana de Advertencia, donde se recomienda establecer la Aplicación HyperTerminal como programa predeterminado de Telnet.

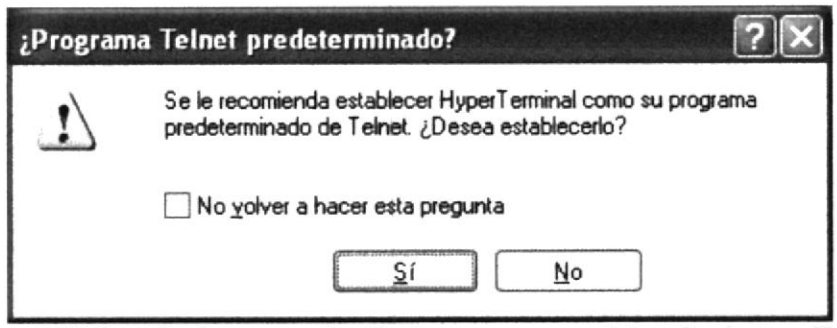


Figura 5.55 Pantalla de recomendación de programa predeterminado para Telnet

- La primera opción es si se desea volver a ver esta pregunta la próxima vez que se acceda al HyperTerminal. Esta opción no afectará en lo más mínimo a nuestra conexión.
- Ahora presenta dos opciones de respuesta referente a la recomendación que hace Windows, si se acepta **"Sí"** automáticamente aparecerá una ventana, la cual solicita cierta información para una conexión mediante un MODEM; pero como este no es el caso simplemente **"cancelamos",** y automáticamente aparecerá la ventana de **"Descripción de conexión"** de la HyperTerminal.

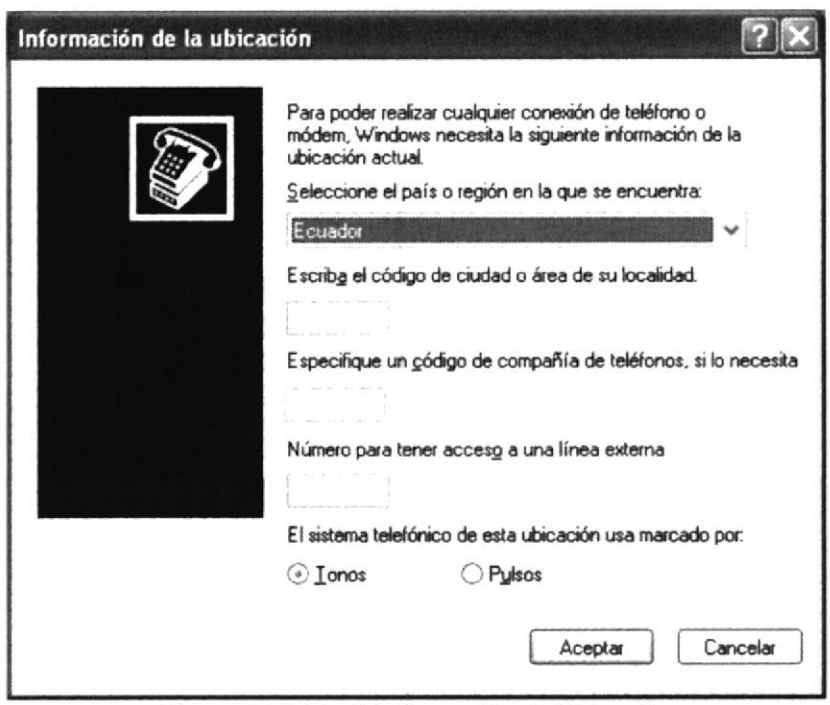


Figura 5.56 Menú Información de Ubicación

- Si en un caso en la ventana que Windows recomienda establecer a la aplicación HyperTerminal como predeterminada para Telnet, se la cancela, automáticamente aparecería la ventana de **"Descripción de la conexión"** de la HyperTerminal.

Figura 5.57 Pantalla de Descripción de la conexión de la HyperTerminal

4. En la ventana de **"Descripción de la conexión"** de la HyperTerminal pide un nombre y un icono para la conexión.
   - El nombre puede ser cualquiera, en este caso se llamará Grupo_ESPOL.
   - Cada icono es un tipo de conexión diferente, para este caso utilizar el primero, el que viene marcado por default.
   - Si se llena los datos que pide la ventana de **"Descripción de conexión"** y da clic en aceptar, automáticamente aparecerá la venta de **"Conectar a"**

Figura 5.58 Pantalla Descripción de la conexión

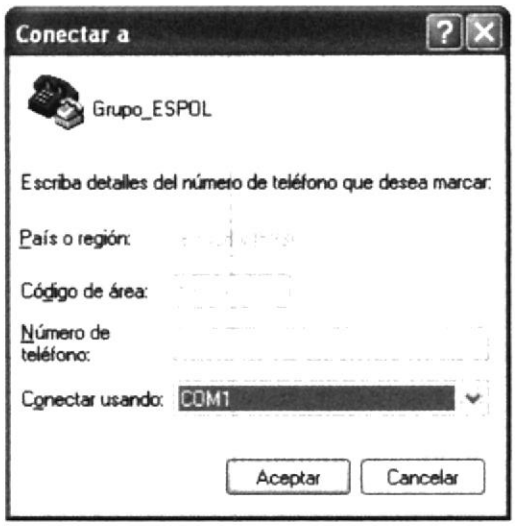


Figura 5.59 Pantalla Conectar a

5. En la ventana de **"Conectar a"** aparte de la opción **"Conectar usando"** las demás vendrán deshabilitadas, y en la opción habilitada escoger por medio de que puerto del computador y conectarse al router, por lo general es el puerto COM1, y viene por default. Desplegando la caja de texto se podrá ver los diferentes puertos disponibles del PC.

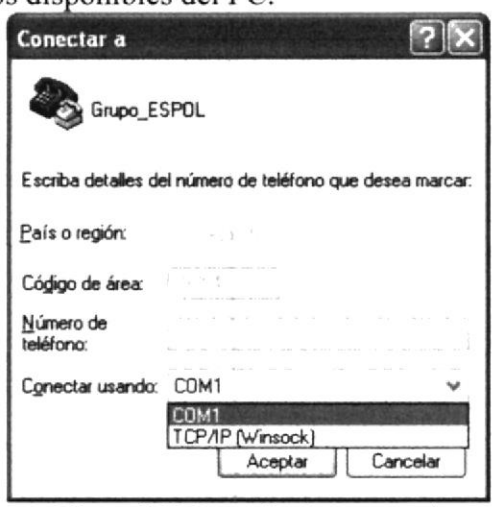


Figura 5.60 Pantalla Conectar a 2

- Si se cancela la ventana de **"Conectar a",** automáticamente se cerrará y quedará activa la ventana de **"Nueva Conexión – HyperTerminal"**, y se procederá a cerrarlo según lo explicado antes.
- Si se acepta, aparecerá una ventana de **"Propiedades del COM1"**, estas son la propiedades del puerto que se escoge para conectarse con el Router.

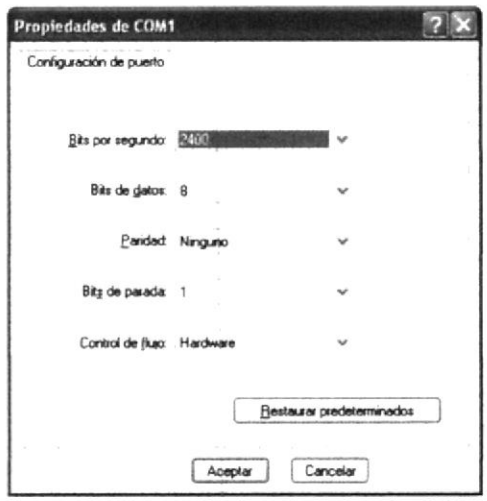


Figura 5.61 Pantalla Propiedades de COM1

6. En la ventana de **"Propiedades de COM1",** se debe configurar según las especificaciones dadas a continuación.
   - 9600 bps
   - 8 bits de datos
   - Ninguno (paridad)
   - 1 (Bit de parada)
   - Ninguno (Control de flujo)

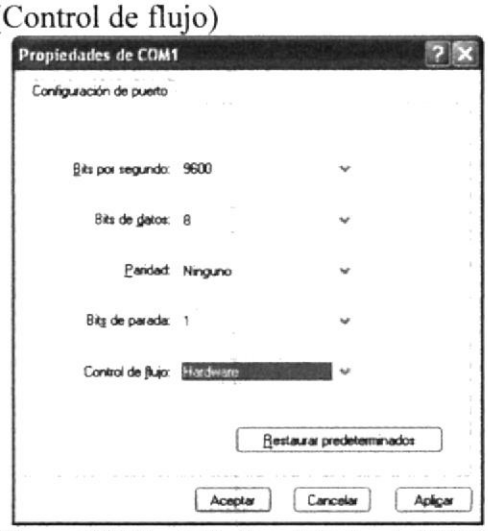


Figura 5.62 Pantalla Propiedades de COM1

   a. La pantalla de **"Propiedades de COM1"** proporciona 3 diferentes opciones: Restaurar Predeterminados, Aceptar, Cancelar y Aplicar. Cada una tiene una función diferente. Si se da clic izquierdo en el botón **Restaurar Predeterminados,** las propiedades del COM1 regresarán a las que estaban cuando recién se abrió la ventana.
   b. La segunda opción es **"Aplicar",** esta opción establecerá las opciones que se están configurando, pero aun no los hará surtir efecto.
   c. La otra opción es la ventana de **"Propiedades de COM1"** es la de **"Aceptar"**, esta opción surtirá efecto las opciones configuradas, inclusive se podrá obviar el paso de primero **"Aplicar"** y luego **"Aceptar".** Una vez dado clic en **"Aceptar"** conectarse inmediatamente al **Router.**

Figura 5.63 Pantalla Inicio de Interfaz con el Router

d. La tercera y ultima opción es la de **"Cancelar",** si se da clic aquí automáticamente la ventana se cerrará y se activará la ventana de **"Nueva Conexión - HyperTerminal",** luego se la cierra según lo requerido y ya aprendido.

5.8.2 CONFIGURACIONES EN CADA ROUTER

5.8.2.1 CONFIGURACIÓN DEL ROUTER SANTA ELENA

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

Acceso al modo de Configuración principal.

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)# exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname STA_ELENA

Sirve para asignarle un nombre al router (STA_ELENA)

STA_ELENA(config)#

Creación de Contraseñas

STA_ELENA #enable

Ingresar al modo EXEC privilegiado

STA_ELENA #configure terminal

Ingresar al modo de configuración global

STA_ELENA (config)#

STA_ELENA (config)#line console 0

Ingresar a configurar la consola

STA_ELENA (config-line)#password cisco

Asignar una contraseña a la consola

STA_ELENA (config-line)#login

Petición de contraseña

STA_ELENA (config-line)#exit

Salir de la configuración de la consola

STA_ELENA (config)#line vty 0 4

Ingresar a configurar la Terminal virtual

STA_ELENA (config-line)#password cisco

Asignar una contraseña a la Terminal virtual

STA_ELENA (config-line)#login

Petición de contraseña

STA_ELENA (config-line)#exit

Salir de la configuración de la Terminal virtual

STA_ELENA (config)#line aux 0

Ingresar a configurar el puerto auxiliar

STA_ELENA (config-line)#password cisco

Asignar una contraseña al puerto auxiliar

STA_ELENA (config-line)#login

Petición de contraseña

STA_ELENA (config-line)#exit

Salir de la configuración del puerto auxiliar

STA_ELENA (config)#

STA_ELENA (config)#enable password cisco

Agregar una contraseña para ingresar al router

STA_ELENA (config)#enable secret cisco

Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.

STA_ELENA (config)#interface FastEthernet 0

Ingresar a la interfaz que se va a configurar

STA_ELENA (config-if)#ip address 192.168.11.9 255.255.255.240

Asignar una dirección ip con su respectiva máscara

STA_ELENA (config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

STA_ELENA (config-if)#exit

Salir de la configuración de la interfaz

STA_ELENA (config)#interface serial 0

Ingresar a la interfaz que se va a configurar

STA_ELENA (config-if)#ip address 192.168.11.1 255.255.255.252

Asignar una dirección ip con su respectiva máscara

STA_ELENA (config-if)#clock rate 64000

Asignar el valor para el sincronizador del reloj

STA_ELENA (config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

STA_ELENA (config-if)#exit

Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento RIPV2

STA_ELENA #configure terminal

Ingresar al modo de configuración global

STA_ELENA (config)#router rip

Habilitar el protocolo de enrutamiento a configurar

STA_ELENA (config-router)#version 2

Asignar la version del protocolo ya asignado

STA_ELENA (config-router)#network 192.168.11.0

Asignar la dirección de la red

STA_ELENA (config-router)#exit

Salir de la configuración del protocolo de enrutamiento

STA_ELENA (config)#

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

STA_ELENA #configure terminal
Ingresar al modo de configuración global
STA_ELENA (config)#no router rip
Desactiva el protocolo de enrutamiento rip
STA_ELENA (config)#

Guardar configuración

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

STA_ELENA #copy running-config startup-config
Guardar una copia de la configuración a la NVRAM

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

Configuración de Listas de Acceso
Bloquear toda la subred 192.168.11.0/27, excepto el servidor con la siguiente ip 192.168.11.3

STA_ELENA # configure terminal
Ingresar al modo de configuración global
STA_ELENA (config)# access-list 1 permit host 192.168.11.3
Asignar permiso a un host específico
STA_ELENA (config)# access-list 1 deny 192.168.11.0 0.0.0.31
Negar el acceso a la red a las demás ip's
STA_ELENA (config)# access-list 1 permit any
Colocar una línea implícita para ésta acl
STA_ELENA (config)# exit
Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

STA_ELENA # configure terminal
Ingresar al modo de configuración global
STA_ELENA (config)# interface fast-Ethernet 0/0
Ingresar a la interfaz que se va a asignar la acl
STA_ELENA (config)# ip access-group 1 in
Levantar la acl de manera entrante

ACL extendida

STA_ELENA # configure terminal

Ingresar al modo de configuración global

STA_ELENA (config)#access-list 101 permit ip host 192.168.11.10 host 192.168.11.3

Asignar permiso a un host específico

STA_ELENA (config)#access-list 101 deny ip 192.168.11.0 0.0.0.255 host 192.168.11.3

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

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

Colocar una línea implícita para ésta acl

STA_ELENA (config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

STA_ELENA # configure terminal

Ingresar al modo de configuración global

STA_ELENA (config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

STA_ELENA (config)# ip access-group 101 in

Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.11.3. Denegar todo lo demás.

STA_ELENA # configure terminal

Ingresar al modo de configuración global

STA_ELENA (config)# access-list 120 permit tcp host 192.168.11.10 host 192.168.11.3 any eq telnet

Ingresar a la interfaz que se va a asignar la acl

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

Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

STA_ELENA # configure terminal

Ingresar al modo de configuración global

STA_ELENA (config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

STA_ELENA (config)# ip access-group 101 in

Levantar la acl de manera entrante

STA_ELENA con0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER SANTA ELENA

User Access Verification
Password:
STA_ELENA>enable
Password:
STA_ELENA#show running-config

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

Current configuration:

Configuración actual del switch

!

version 12.0

Versión del Sistema Operativo del Router

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

Servicio de encriptación de contraseña no esta activo

!

hostname STA_ELENA

!

enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/

Indica que la contraseña de ingreso al switch se encuentra encriptada

!

ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!

key chain private

Clave privada en la autenticación de Rip

key 1

Inicialización de la autenticación de Rip

key-string 234

Cadena de autenticación de Rip

!

!!

interface Ethernet0

Tipo de Interfaz

ip address 192.168.11.9 255.255.255.252

Dirección IP y máscara de la interfaz

no ip directed-broadcast

interface Serial0

Tipo de Interfaz

description Esta serial se conecta con el Router de ESPOLTEL

Pequeña descripción de la conexión de la interfaz

ip address 192.168.11.1 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast

ip rip authentication mode md5

ip rip authentication key-chain private

no ip mroute-cache

clockrate 64000

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

!

interface Serial1

Tipo de la interfaz
no ip address
Esto significa que no tiene ninguna ip asignada
no ip directed-broadcast
shutdown
Esto describe el estado de la interfaz, Up(Levantada) o Down (Caída)
!
router rip
Protocolo de Enrutamiento
version 2
Versión del protocolo de Enrutamiento
network 192.168.11.0
Redes configuradas con el protocolo de Enrutamiento Rip
!
ip classless
Indica acceso a las redes no remotas con máscara de sub red diferente
!
banner motd ^CBIENVENIDO AL ROUTER SANTA ELENA^C
Indica el mensaje de Bienvenida del Router
!
line con 0
password topico
Contraseña para línea de comandos
login
transport input none
line 1 8
line aux 0
password topico
login
line vty 0 4
password topico
Contraseña para Telnet
login
!
end
STA_ELENA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Descripción de Protocolos usados
Gateway of last resort is not set
192.168.11.0/30 is subnetted, 1 subnets
C 192.168.11.0 is directly connected, Serial0
Especifica que esta interfaz esta conectada directamente mediante la serial 0
STA_ELENA#

5.8.2.2 CONFIGURACIÓN DEL ROUTER ESPOLTEL

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

Acceso al modo de Configuración principal.

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)# exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname ESPOLTEL

Sirve para asignarle un nombre al router (ESPOLTEL)

ESPOLTEL(config)#

Creación de Contraseñas

ESPOLTEL#enable

Ingresar al modo EXEC privilegiado

ESPOLTEL#configure terminal

Ingresar al modo de configuración global

ESPOLTEL(config)#

ESPOLTEL(config)#line console 0

Ingresar a configurar la consola

ESPOLTEL(config-line)#password cisco

Asignar una contraseña a la consola

ESPOLTEL(config-line)#login

Petición de contraseña

ESPOLTEL(config-line)#exit

Salir de la configuración de la consola

ESPOLTEL(config)#line vty 0 4

Ingresar a configurar la Terminal virtual

ESPOLTEL(config-line)#password cisco

Asignar una contraseña a la Terminal virtual

ESPOLTEL(config-line)#login

Petición de contraseña

ESPOLTEL(config-line)#exit

Salir de la configuración de la Terminal virtual

ESPOLTEL(config)#line aux 0

Ingresar a configurar el puerto auxiliar

ESPOLTEL(config-line)#password cisco
Asignar una contraseña al puerto auxiliar
ESPOLTEL(config-line)#login
Petición de contraseña
ESPOLTEL(config-line)#exit
Salir de la configuración del puerto auxiliar
ESPOLTEL(config)#
ESPOLTEL(config)#enable password cisco
Agregar una contraseña para ingresar al router
ESPOLTEL(config)#enable secret cisco
Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.
ESPOLTEL(config)#interface serial 0
Ingresar a la interfaz que se va a configurar
ESPOLTEL(config-if)#ip address 192.168.7.18 255.255.255.252
Asignar una dirección ip con su respectiva máscara
ESPOLTEL(config-if)#clock rate 64000
Asignar el valor para el sincronizador del reloj
ESPOLTEL(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
ESPOLTEL(config-if)#exit
Salir de la configuración de la interfaz
ESPOLTEL(config)#interface serial 1
Ingresar a la interfaz que se va a configurar
ESPOLTEL(config-if)#ip address 192.168.11.2 255.255.255.252
Asignar una dirección ip con su respectiva máscara
ESPOLTEL(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
ESPOLTEL(config-if)#exit
Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento RIPV2
ESPOLTEL#configure terminal
Ingresar al modo de configuración global
ESPOLTEL(config)#router rip
Habilitar el protocolo de enrutamiento a configurar
ESPOLTEL(config-router)#version 2
Asignar la version del protocolo ya asignado
ESPOLTEL(config-router)#network 192.168.7.0
ESPOLTEL(config-router)#network 192.168.11.0
Asignar la dirección de la red
ESPOLTEL(config-router)#exit
Salir de la configuración del protocolo de enrutamiento
ESPOLTEL(config)#

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

ESPOLTEL#configure terminal
Ingresar al modo de configuración global
ESPOLTEL(config)#no router rip
Desactiva el protocolo de enrutamiento rip
ESPOLTEL(config)#

Guardar configuración

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

ESPOLTEL#copy running-config startup-config
Guardar una copia de la configuración a la NVRAM

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

ESPOLTELcon0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER ESPOLTEL

User Access Verification

Password:
ESPOLTEL>enable
Password:
ESPOLTEL#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del Router
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
Servicio de encriptación de contraseña no esta activo
!
hostname ESPOLTEL
!
enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/

Indica que la contraseña de ingreso al switch se encuentra encriptada

!

ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!

key chain private

Clave privada en la autenticación de Rip

key 1

Inicialización de la autenticación de Rip

key-string 234

Cadena de autenticación de Rip

!

!!

interface Serial0

Tipo de Interfaz

description Esta serial se conecta con el Router de ESPOLTEL

Pequeña descripción de la conexión de la interfaz

ip address 192.168.7.18 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast

ip rip authentication mode md5

ip rip authentication key-chain private

no ip mroute-cache

clockrate 64000

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

!

interface Serial1

Tipo de Interfaz

description Esta serial se conecta con el Router de ESPOLTEL

Pequeña descripción de la conexión de la interfaz

ip address 192.168.11.2 255.255.255.252

Dirección IP y máscara de dicha interfaz

no ip directed-broadcast

!

router rip

Protocolo de Enrutamiento

version 2

Versión del protocolo de Enrutamiento

network 192.168.7.0

network 192.168.11.0

Redes configuradas con el protocolo de Enrutamiento Rip

!

ip classless

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

!

banner motd ^CBIENVENIDO AL ROUTER ESPOLTEL^C

Indica el mensaje de Bienvenida del Router

!

line con 0
password topico
Contraseña para línea de comandos
login
transport input none
line 1 8
line aux 0
password topico
login
line vty 0 4
password topico
Contraseña para Telnet
login
!
end
ESPOLTEL#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, * - candidate default
U - per-user static route, o – ODR
Descripción de Protocolos usados

Gateway of last resort is not set

192.168.11.0/30 is subnetted, 1 subnets
R 192.168.7.0 is directly connected, Serial1
C 192.168.11.0 is directly connected, Serial0
Especifica que esta interfaz esta conectada directamente mediante la serial 0 y serial 1
ESPOLTEL#

5.8.2.3 CONFIGURACIÓN DEL ROUTER PEÑAS_1

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

Acceso al modo de Configuración principal.

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

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname PEÑAS_1

Sirve para asignarle un nombre al router (PEÑAS_1)

PEÑAS_1(config)#

Creación de Contraseñas

PEÑAS_1#enable

Ingresar al modo EXEC privilegiado

PEÑAS_1#configure terminal

Ingresar al modo de configuración global

PEÑAS_1(config)#

PEÑAS_1(config)#line console 0

Ingresar a configurar la consola

PEÑAS_1(config-line)#password cisco

Asignar una contraseña a la consola

PEÑAS_1(config-line)#login

Petición de contraseña

PEÑAS_1(config-line)#exit

Salir de la configuración de la consola

PEÑAS_1(config)#line vty 0 4

Ingresar a configurar la Terminal virtual

PEÑAS_1(config-line)#password cisco

Asignar una contraseña a la Terminal virtual

PEÑAS_1(config-line)#login

Petición de contraseña

PEÑAS_1(config-line)#exit

Salir de la configuración de la Terminal virtual

PEÑAS_1(config)#line aux 0

Ingresar a configurar el puerto auxiliar

PEÑAS_1(config-line)#password cisco

Asignar una contraseña al puerto auxiliar

PEÑAS_1(config-line)#login

Petición de contraseña

PEÑAS_1(config-line)#exit

Salir de la configuración del puerto auxiliar

PEÑAS_1(config)#

PEÑAS_1(config)#enable password cisco

Agregar una contraseña para ingresar al router

PEÑAS_1(config)#enable secret cisco

Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.

PEÑAS_1(config)#interface FastEthernet 0

Ingresar a la interfaz que se va a configurar

PEÑAS_1(config-if)#ip address 192.168.7.25 255.255.255.240
Asignar una dirección ip con su respectiva máscara
PEÑAS_1(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
PEÑAS_1(config-if)#exit
Salir de la configuración de la interfaz
PEÑAS_1(config)#interface serial 0
Ingresar a la interfaz que se va a configurar
PEÑAS_1(config-if)#ip address 192.168.7.1 255.255.255.252
Asignar una dirección ip con su respectiva máscara
PEÑAS_1(config-if)#clock rate 64000
Asignar el valor para el sincronizador del reloj
PEÑAS_1(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
PEÑAS_1(config-if)#exit
Salir de la configuración de la interfaz
PEÑAS_1(config)#interface serial 1
Ingresar a la interfaz que se va a configurar
PEÑAS_1(config-if)#ip address 192.168.7.17 255.255.255.252
Asignar una dirección ip con su respectiva máscara
PEÑAS_1(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
PEÑAS_1(config-if)#exit
Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento RIPV2

PEÑAS_1Configure terminal
Ingresar al modo de configuración global
PEÑAS_1(config)#router rip
Habilitar el protocolo de enrutamiento a configurar
PEÑAS_1(config-router)#version 2
Asignar la version del protocolo ya asignado
PEÑAS_1(config-router)#network 192.168.7.0
Asignar la dirección de la red
PEÑAS_1(config-router)#exit
Salir de la configuración del protocolo de enrutamiento
PEÑAS_1(config)#

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

PEÑAS_1#configure terminal
Ingresar al modo de configuración global
PEÑAS_1(config)#no router rip
Desactiva el protocolo de enrutamiento rip
PEÑAS_1(config)#

Configuración de Listas de Acceso

Bloquear toda la subred 192.168.7.0/28, excepto el servidor con la siguiente ip 192.168.7.3

PEÑAS_1# configure terminal

Ingresar al modo de configuración global

PEÑAS_1(config)# access-list 1 permit host 192.168.7.3

Asignar permiso a un host específico

PEÑAS_1(config)# access-list 1 deny 192.168.7.24 0.0.0.15

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

PEÑAS_1(config)# access-list 1 permit any

Colocar una línea implícita para ésta acl

PEÑAS_1(config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

PEÑAS_1# configure terminal

Ingresar al modo de configuración global

PEÑAS_1(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PEÑAS_1(config)# ip access-group 1 in

Levantar la acl de manera entrante

ACL extendida

PEÑAS_1# configure terminal

Ingresar al modo de configuración global

PEÑAS_1(config)#access-list 101 permit ip host 192.168.7.10 host 192.168.7.3

Asignar permiso a un host específico

PEÑAS_1(config)#access-list 101 deny ip 192.168.7.24 0.0.0.15 host 192.168.7.3

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

PEÑAS_1(config)#access-list 101 permit ip any any

Colocar una línea implícita para ésta acl

PEÑAS_1(config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PEÑAS_1# configure terminal

Ingresar al modo de configuración global

PEÑAS_1(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PEÑAS_1(config)# ip access-group 101 in

Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.7.3. Denegar todo lo demás.

PEÑAS_1# configure terminal

Ingresar al modo de configuración global

PEÑAS_1(config)# access-list 120 permit tcp host 192.168.7.10 host 192.168.7.3 any eq telnet

Ingresar a la interfaz que se va a asignar la acl

PEÑAS_1(config)#access-list 120 deny any any

Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PEÑAS_1# configure terminal

Ingresar al modo de configuración global

PEÑAS_1(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PEÑAS_1(config)# ip access-group 101 in

Levantar la acl de manera entrante

Guardar configuración

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

PEÑAS_1#copy running-config startup-config

Guardar una copia de la configuración a la NVRAM

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

PEÑAS_1con0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER PEÑAS_1

User Access Verification

Password:
PEÑAS_1>enable
Password:
PEÑAS_1#show running-config

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

Current configuration:

Configuración actual del switch

!
version 12.0

Versión del Sistema Operativo del Router

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

Servicio de encriptación de contraseña no esta activo

```
!
hostname PEÑAS_1
!
enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/
```

Indica que la contraseña de ingreso al switch se encuentra encriptada

```
!
ip subnet-zero
```

Sirve para utilizar la ip inicial al momento de subnetear

```
!
key chain private
```

Clave privada en la autenticación de Rip

```
 key 1
```

Inicialización de la autenticación de Rip

```
  key-string 234
```

Cadena de autenticación de Rip

```
!
!!
interface Ethernet0
```

Tipo de Interfaz

```
 ip address 192.168.7.25 255.255.255.240
```

Dirección IP y máscara de la interfaz

```
 no ip directed-broadcast
!
!!
interface Serial0
```

Tipo de Interfaz

```
 description Esta serial se conecta con el Router de PEÑAS_1
```

Pequeña descripción de la conexión de la interfaz

```
 ip address 192.168.7.1 255.255.255.252
```

Dirección IP y máscara de dicha interfaz

```
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain private
 no ip mroute-cache
 clockrate 64000
```

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

```
!
interface Serial1
```

Tipo de Interfaz

```
 description Esta serial se conecta con el Router de PEÑAS_1
```

Pequeña descripción de la conexión de la interfaz

```
 ip address 192.168.7.17 255.255.255.252
```

Dirección IP y máscara de dicha interfaz

```
 no ip directed-broadcast
!
router rip
        Protocolo de Enrutamiento
 version 2
        Versión del protocolo de Enrutamiento
 network 192.168.7.0
        Redes configuradas con el protocolo de Enrutamiento Rip
!
ip classless
        Indica acceso a las redes no remotas con máscara de sub red diferente
!
banner motd ^CBIENVENIDO AL ROUTER PEÑAS_1^C
        Indica el mensaje de Bienvenida del Router
!
line con 0
password topico
        Contraseña para línea de comandos
 login
 transport input none
line 1 8
line aux 0
 password topico
 login
line vty 0 4
 password topico
        Contraseña para Telnet
 login
!
end
```

PEÑAS_1#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, * - candidate default
       U - per-user static route, o – ODR
           Descripción de Protocolos usados

Gateway of last resort is not set

    192.168.7.0/30 is subnetted, 3 subnets
R       192.168.7.4 [120/1] via 192.168.7.2, 00:00:14, Serial0
C       192.168.7.0 is directly connected, Serial0
C       192.168.7.16 is directly connected, Serial1
        Especifica que esta interfaz esta conectada directamente mediante la serial 0 y
        serial 1
PEÑAS_1#
```

5.8.2.4 CONFIGURACIÓN DEL ROUTER PEÑAS_2

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

Acceso al modo de Configuración principal.

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)# exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname PEÑAS_2

Sirve para asignarle un nombre al router (PEÑAS_2)

PEÑAS_2(config)#

Creación de Contraseñas

PEÑAS_2#enable

Ingresar al modo EXEC privilegiado

PEÑAS_2#configure terminal

Ingresar al modo de configuración global

PEÑAS_2(config)#

PEÑAS_2(config)#line console 0

Ingresar a configurar la consola

PEÑAS_2(config-line)#password cisco

Asignar una contraseña a la consola

PEÑAS_2(config-line)#login

Petición de contraseña

PEÑAS_2(config-line)#exit

Salir de la configuración de la consola

PEÑAS_2(config)#line vty 0 4

Ingresar a configurar la Terminal virtual

PEÑAS_2(config-line)#password cisco

Asignar una contraseña a la Terminal virtual

PEÑAS_2(config-line)#login

Petición de contraseña

PEÑAS_2(config-line)#exit

Salir de la configuración de la Terminal virtual

PEÑAS_2(config)#line aux 0

Ingresar a configurar el puerto auxiliar

PEÑAS_2(config-line)#password cisco

Asignar una contraseña al puerto auxiliar

PEÑAS_2(config-line)#login

Petición de contraseña

PEÑAS_2(config-line)#exit

Salir de la configuración del puerto auxiliar

PEÑAS_2(config)#

PEÑAS_2(config)#enable password cisco

Agregar una contraseña para ingresar al router

PEÑAS_2(config)#enable secret cisco

Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.

PEÑAS_2(config)#interface FastEthernet 0

Ingresar a la interfaz que se va a configurar

PEÑAS_2(config-if)#ip address 192.168.7.65 255.255.255.224

Asignar una dirección ip con su respectiva máscara

PEÑAS_2(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

PEÑAS_2(config-if)#exit

Salir de la configuración de la interfaz

PEÑAS_2(config)#interface serial 0

Ingresar a la interfaz que se va a configurar

PEÑAS_2(config-if)#ip address 192.168.7.5 255.255.255.252

Asignar una dirección ip con su respectiva máscara

PEÑAS_2(config-if)#clock rate 64000

Asignar el valor para el sincronizador del reloj

PEÑAS_2(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

PEÑAS_2(config-if)#exit

Salir de la configuración de la interfaz

PEÑAS_2(config)#interface serial 1

Ingresar a la interfaz que se va a configurar

PEÑAS_2(config-if)#ip address 192.168.7.2 255.255.255.252

Asignar una dirección ip con su respectiva máscara

PEÑAS_2(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

PEÑAS_2(config-if)#exit

Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento RIPV2

PEÑAS_2#configure terminal

Ingresar al modo de configuración global

PEÑAS_2(config)#router rip

Habilitar el protocolo de enrutamiento a configurar

PEÑAS_2(config-router)#version 2

Asignar la version del protocolo ya asignado

PEÑAS_2(config-router)#network 192.168.7.0

Asignar la dirección de la red

PEÑAS_2(config-router)#exit
Salir de la configuración del protocolo de enrutamiento
PEÑAS_2(config)#

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

PEÑAS_2#configure terminal
Ingresar al modo de configuración global
PEÑAS_2(config)#no router rip
Desactiva el protocolo de enrutamiento rip
PEÑAS_2(config)#

Configuración de Listas de Acceso

Bloquear toda la subred 192.168.7.0/27, excepto el servidor con la siguiente ip 192.168.7.70

PEÑAS_2# configure terminal
Ingresar al modo de configuración global
PEÑAS_2(config)# access-list 1 permit host 192.168.7.70
Asignar permiso a un host específico
PEÑAS_2(config)# access-list 1 deny 192.168.7.64 0.0.0.31
Negar el acceso a la red a las demás ip's
PEÑAS_2(config)# access-list 1 permit any
Colocar una línea implícita para ésta acl
PEÑAS_2(config)# exit
Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

PEÑAS_2# configure terminal
Ingresar al modo de configuración global
PEÑAS_2(config)# interface fast-Ethernet 0/0
Ingresar a la interfaz que se va a asignar la acl
PEÑAS_2(config)# ip access-group 1 in
Levantar la acl de manera entrante

ACL extendida

PEÑAS_2# configure terminal
Ingresar al modo de configuración global
PEÑAS_2(config)#access-list 101 permit ip host 192.168.7.68 host 192.168.7.70
Asignar permiso a un host específico
PEÑAS_2(config)#access-list 101 deny ip 192.168.7.64 0.0.0.31 host 192.168.7.70
Negar el acceso a la red a las demás ip's
PEÑAS_2(config)#access-list 101 permit ip any any
Colocar una línea implícita para ésta acl
PEÑAS_2(config)# exit
Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PEÑAS_2# configure terminal
Ingresar al modo de configuración global
PEÑAS_2(config)# interface fast-Ethernet 0/0
Ingresar a la interfaz que se va a asignar la acl
PEÑAS_2(config)# ip access-group 101 in
Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.7.70
Denegar todo lo demás.

PEÑAS_2# configure terminal
Ingresar al modo de configuración global
PEÑAS_2(config)# access-list 120 permit tcp host 192.168.7.68 host 192.168.7.70 any eq telnet
Ingresar a la interfaz que se va a asignar la acl
PEÑAS_2(config)#access-list 120 deny any any
Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PEÑAS_2# configure terminal
Ingresar al modo de configuración global
PEÑAS_2(config)# interface fast-Ethernet 0/0
Ingresar a la interfaz que se va a asignar la acl
PEÑAS_2(config)# ip access-group 101 in
Levantar la acl de manera entrante

Guardar configuración

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

PEÑAS_2#copy running-config startup-config
Guardar una copia de la configuración a la NVRAM

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

PEÑAS_2con0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER PEÑAS_2

User Access Verification

Password:
PEÑAS_2>enable
Password:
PEÑAS_2#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del Router
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
Servicio de encriptación de contraseña no esta activo
!
hostname PEÑAS_2
!
enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/
Indica que la contraseña de ingreso al switch se encuentra encriptada
!
ip subnet-zero
Sirve para utilizar la ip inicial al momento de subnetear
!
key chain private
Clave privada en la autenticación de Rip
key 1
Inicialización de la autenticación de Rip
key-string 234
Cadena de autenticación de Rip
!
!!
interface Ethernet0
Tipo de Interfaz
ip address 192.168.7.65 255.255.255.224
Dirección IP y máscara de la interfaz
no ip directed-broadcast
!
!!
interface Serial0
Tipo de Interfaz
description Esta serial se conecta con el Router de PEÑAS_2
Pequeña descripción de la conexión de la interfaz
ip address 192.168.7.5 255.255.255.252
Dirección IP y máscara de dicha interfaz

```
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain private
 no ip mroute-cache
 clockrate 64000
```
Indica la velocidad del puerto en bits por segundo Lo encontramos en la DCE.
```
!
interface Serial1
```
Tipo de Interfaz
```
 description Esta serial se conecta con el Router de PEÑAS_2
```
Pequeña descripción de la conexión de la interfaz
```
 ip address 192.168.7.2 255.255.255.252
```
Dirección IP y máscara de dicha interfaz
```
 no ip directed-broadcast
!
router rip
```
Protocolo de Enrutamiento
```
 version 2
```
Versión del protocolo de Enrutamiento
```
 network 192.168.7.0
```
Redes configuradas con el protocolo de Enrutamiento Rip
```
!
ip classless
```
Indica acceso a las redes no remotas con máscara de sub red diferente
```
!
banner motd ^CBIENVENIDO AL ROUTER PEÑAS_2^C
```
Indica el mensaje de Bienvenida del Router
```
!
line con 0
password topico
```
Contraseña para línea de comandos
```
 login
 transport input none
line 1 8
line aux 0
 password topico
 login
line vty 0 4
 password topico
```
Contraseña para Telnet
```
 login
!
end
```
PEÑAS_2#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, * - candidate default
U - per-user static route, o – ODR
Descripción de Protocolos usados

Gateway of last resort is not set

192.168.7.0/30 is subnetted, 3 subnets
C 192.168.7.0 is directly connected, Serial0
C 192.168.7.16 is directly connected, Serial1
R 192.168.7.4 [120/1] via 192.168.7.1, 00:00:14, Serial1
Especifica que esta interfaz esta conectada directamente mediante la serial 0 y serial 1
PEÑAS_2#

5.8.2.5 CONFIGURACIÓN DEL ROUTER SAMBORONDÓN

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

Acceso al modo de Configuración principal.

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)# exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname SAMBORONDON

Sirve para asignarle un nombre al router (SAMBORONDON)

SAMBORONDON(config)#

Creación de Contraseñas

SAMBORONDON#enable

Ingresar al modo EXEC privilegiado

SAMBORONDON#configure terminal

Ingresar al modo de configuración global

SAMBORONDON(config)#

SAMBORONDON(config)#line console 0

Ingresar a configurar la consola

SAMBORONDON(config-line)#password cisco

Asignar una contraseña a la consola

SAMBORONDON(config-line)#login

Petición de contraseña

SAMBORONDON(config-line)#exit

Salir de la configuración de la consola

SAMBORONDON(config)#line vty 0 4

Ingresar a configurar la Terminal virtual

SAMBORONDON(config-line)#password cisco

Asignar una contraseña a la Terminal virtual

SAMBORONDON(config-line)#login

Petición de contraseña

SAMBORONDON(config-line)#exit

Salir de la configuración de la Terminal virtual

SAMBORONDON(config)#line aux 0

Ingresar a configurar el puerto auxiliar

SAMBORONDON(config-line)#password cisco
Asignar una contraseña al puerto auxiliar
SAMBORONDON(config-line)#login
Petición de contraseña
SAMBORONDON(config-line)#exit
Salir de la configuración del puerto auxiliar
SAMBORONDON(config)#
SAMBORONDON(config)#enable password cisco
Agregar una contraseña para ingresar al router
SAMBORONDON(config)#enable secret cisco
Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.

SAMBORONDON(config)#interface FastEthernet 0
Ingresar a la interfaz que se va a configurar
SAMBORONDON(config-if)#ip address 192.168.12.65 255.255.255.224
Asignar una dirección ip con su respectiva máscara
SAMBORONDON(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
SAMBORONDON(config-if)#exit
Salir de la configuración de la interfaz
SAMBORONDON(config)#interface serial 1
Ingresar a la interfaz que se va a configurar
SAMBORONDON(config-if)#ip address 192.168.12.2 255.255.255.252
Asignar una dirección ip con su respectiva máscara
SAMBORONDON(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
SAMBORONDON(config-if)#exit
Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento RIPV2

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)#router rip
Habilitar el protocolo de enrutamiento a configurar
SAMBORONDON(config-router)#version 2
Asignar la version del protocolo ya asignado
SAMBORONDON(config-router)#network 192.168.12.0
Asignar la dirección de la red
SAMBORONDON(config-router)#exit
Salir de la configuración del protocolo de enrutamiento
SAMBORONDON(config)#

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

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)#no router rip

Desactiva el protocolo de enrutamiento rip
SAMBORONDON(config)#

Configuración de Listas de Acceso
Bloquear toda la subred 192.168.12.0/27, excepto el servidor con la siguiente ip 192.168.12.70

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)# access-list 1 permit host 192.168.12.70
Asignar permiso a un host específico
SAMBORONDON(config)# access-list 1 deny 192.168.12.64 0.0.0.31
Agregar el acceso a la red a las demás ip's
SAMBORONDON(config)# access-list 1 permit any
Colocar una línea implícita para ésta acl
SAMBORONDON(config)# exit
Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)# interface fast-Ethernet 0/0
Ingresar a la interfaz que se va a asignar la acl
SAMBORONDON(config)# ip access-group 1 in
Levantar la acl de manera entrante

ACL extendida

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)#access-list 101 permit ip host 192.168.12.68 host 192.168.12.70
Asignar permiso a un host específico
SAMBORONDON(config)#access-list 101 deny ip 192.168.12.64 0.0.0.31 host 192.168.12.70
Negar el acceso a la red a las demás ip's
SAMBORONDON(config)#access-list 101 permit ip any any
Colocar una línea implícita para ésta acl
SAMBORONDON(config)# exit
Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)# interface fast-Ethernet 0/0
Ingresar a la interfaz que se va a asignar la acl
SAMBORONDON(config)# ip access-group 101 in
Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.12.70
Denegar todo lo demás.

SAMBORONDON#configure Terminal
Ingresar al modo de configuración global
SAMBORONDON(config)# access-list 120 permit tcp host 192.168.12.68 host 192.168.12.70 any eq telnet
Ingresar a la interfaz que se va a asignar la acl
SAMBORONDON(config)#access-list 120 deny any any
Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)# interface fast-Ethernet 0/0
Ingresar a la interfaz que se va a asignar la acl
SAMBORONDON(config)# ip access-group 101 in
Levantar la acl de manera entrante

Guardar configuración

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

SAMBORONDON#copy running-config startup-config
Guardar una copia de la configuración a la NVRAM

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

SAMBORONDONcon0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER SAMBORONDON

User Access Verification

Password:
SAMBORONDON>enable
Password:
SAMBORONDON#show running-config

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

Current configuration:

Configuración actual del switch

!

version 12.0

Versión del Sistema Operativo del Router

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

Servicio de encriptación de contraseña no esta activo

!

hostname SAMBORONDON

!

enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/

Indica que la contraseña de ingreso al switch se encuentra encriptada

!

ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!

key chain private

Clave privada en la autenticación de Rip

key 1

Inicialización de la autenticación de Rip

key-string 234

Cadena de autenticación de Rip

!

!!

interface Ethernet0

Tipo de Interfaz

ip address 192.168.12.65 255.255.255.224

Dirección IP y máscara de la interfaz

no ip directed-broadcast

!

!!

interface Serial0

Tipo de la interfaz

no ip address

Esto significa que no tiene ninguna ip asignada

no ip directed-broadcast

shutdown

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

!

interface Serial1

Tipo de Interfaz

description Esta serial se conecta con el Router de SAMBORONDON

Pequeña descripción de la conexión de la interfaz

ip address 192.168.12.2 255.255.255.252

Dirección IP y máscara de dicha interfaz
no ip directed-broadcast
!
router rip
Protocolo de Enrutamiento
version 2
Versión del protocolo de Enrutamiento
network 192.168.12.0
Redes configuradas con el protocolo de Enrutamiento Rip
!
ip classless
Indica acceso a las redes no remotas con máscara de sub red diferente
!
banner motd ^CBIENVENIDO AL ROUTER SAMBORONDON^C
Indica el mensaje de Bienvenida del Router
!
line con 0
password topico
Contraseña para línea de comandos
login
transport input none
line 1 8
line aux 0
password topico
login
line vty 0 4
password topico
Contraseña para Telnet
login
!
end

SAMBORONDON#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, * - candidate default
U - per-user static route, o – ODR
Descripción de Protocolos usados

Gateway of last resort is not set
92.168.12.0/30 is subnetted, 1 subnets
C 192.168.12.0 is directly connected, Serial1
Especifica que esta interfaz esta conectada directamente mediante la serial 0 y serial 1
SAMBORONDON#

5.8.2.6 CONFIGURACIÓN DEL ROUTER PROSPE_1

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

Acceso al modo de Configuración principal.

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)# exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname PROSPE_1

Sirve para asignarle un nombre al router (PROSPE_1)

PROSPE_1(config)#

Creación de Contraseñas

PROSPE_1#enable

Ingresar al modo EXEC privilegiado

PROSPE_1#configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)#

PROSPE_1(config)#line console 0

Ingresar a configurar la consola

PROSPE_1(config-line)#password cisco

Asignar una contraseña a la consola

PROSPE_1(config-line)#login

Petición de contraseña

PROSPE_1(config-line)#exit

Salir de la configuración de la consola

PROSPE_1(config)#line vty 0 4

Ingresar a configurar la Terminal virtual

PROSPE_1(config-line)#password cisco

Asignar una contraseña a la Terminal virtual

PROSPE_1(config-line)#login

Petición de contraseña

PROSPE_1(config-line)#exit

Salir de la configuración de la Terminal virtual

PROSPE_1(config)#line aux 0

Ingresar a configurar el puerto auxiliar

PROSPE_1(config-line)#password cisco

Asignar una contraseña al puerto auxiliar

PROSPE_1(config-line)#login

Petición de contraseña

PROSPE_1(config-line)#exit

Salir de la configuración del puerto auxiliar

PROSPE_1(config)#

PROSPE_1(config)#enable password cisco

Agregar una contraseña para ingresar al router

PROSPE_1(config)#enable secret cisco

Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.

PROSPE_1(config)#interface FastEthernet 0

Ingresar a la interfaz que se va a configurar

PROSPE_1(config-if)#ip address 192.168.1.33 255.255.255.224

Asignar una dirección ip con su respectiva máscara

PROSPE_1(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

PROSPE_1(config-if)#exit

Salir de la configuración de la interfaz

PROSPE_1(config)#interface serial 0

Ingresar a la interfaz que se va a configurar

PROSPE_1(config-if)#ip address 192.168.1.1 255.255.255.252

Asignar una dirección ip con su respectiva máscara

PROSPE_1(config-if)#clock rate 64000

Asignar el valor para el sincronizador del reloj

PROSPE_1(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

PROSPE_1(config-if)#exit

Salir de la configuración de la interfaz

PROSPE_1(config)#interface serial 1

Ingresar a la interfaz que se va a configurar

PROSPE_1(config-if)#ip address 192.168.7.14 255.255.255.252

Asignar una dirección ip con su respectiva máscara

PROSPE_1(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

PROSPE_1(config-if)#exit

Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento OSPF

El Protocolo de enrutamiento OSPF debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red, lo Habilitar utilizando:

PROSPE_1#configure Terminal

Ingresar al modo de configuración global

PROSPE_1(config)#router ospf 0

Habilitar el protocolo de enrutamiento a configurar

PROSPE_1(config-router)#network 192.168.1.0 0.0.0.3 area 0

PROSPE_1(config-router)#network 192.168.1.32 0.0.0.31 area 0

Asignar la dirección de la red, wildcard y área respectiva

Al mismo tiempo configuraremos la distribución del protocolo de enrutamiento Rip.

PROSPE_1(config-router)#redistributed rip subnets

Distribuimos ospf hacia las subredes rip.

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

PROSPE_1#configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)#no router ospf 0

Desactiva el protocolo de enrutamiento ospf

PROSPE_1(config)#exit

Salir del modo de configuración global

Configuración de Protocolo de Enrutamiento RIP

El Protocolo de enrutamiento RIP debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de errores, lo Habilitar utilizando:

PROSPE_1#configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)#router rip

Habilitar el protocolo de enrutamiento a configurar

PROSPE_1(config-router)#version 2

Asignar la version del protocolo ya asignado

PROSPE_1(config-router)#network 192.168.7.0

Asignar la dirección de la red

PROSPE_1(config-router)#default-metric 10

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

PROSPE_1(config-router)#exit

Salir del modo de configuración de protocolo

Al mismo tiempo configuraremos la distribución del protocolo de enrutamiento OSPF.

PROSPE_1(config-router)#redistributed ospf 0

Distribuimos rip hacia las redes ospf

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

PROSPE_1#configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)#no router rip

Desactiva el protocolo de enrutamiento rip

PROSPE_1(config)#exit

Salir del modo de configuración global

PROSPE_1#

Configuración de Listas de Acceso

Bloquear toda la subred 192.168.1.0/27, excepto el servidor con la siguiente ip 192.168.1.40

PROSPE_1# configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)# access-list 1 permit host 192.168.1.40

Asignar permiso a un host específico

PROSPE_1(config)# access-list 1 deny 192.168.1.32 0.0.0.31

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

PROSPE_1(config)# access-list 1 permit any

Colocar una línea implícita para ésta acl

PROSPE_1(config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

PROSPE_1# configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PROSPE_1(config)# ip access-group 1 in

Levantar la acl de manera entrante

ACL extendida

PROSPE_1# configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)#access-list 101 permit ip host 192.168.1.35 host 192.168.1.40

Asignar permiso a un host específico

PROSPE_1(config)#access-list 101 deny ip 192.168.1.32 0.0.0.31 host 192.168.1.40

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

PROSPE_1(config)#access-list 101 permit ip any any

Colocar una línea implícita para ésta acl

PROSPE_1(config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PROSPE_1# configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PROSPE_1(config)# ip access-group 101 in

Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.1.40 Denegar todo lo demás.

PROSPE_1# configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)# access-list 120 permit tcp host 192.168.1.35 host 192.168.1.40 any eq telnet

Ingresar a la interfaz que se va a asignar la acl

PROSPE_1(config)#access-list 120 deny any any

Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PROSPE_1# configure terminal

Ingresar al modo de configuración global

PROSPE_1(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PROSPE_1(config)# ip access-group 101 in

Levantar la acl de manera entrante

Guardar configuración

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

PROSPE_1#copy running-config startup-config

Guardar una copia de la configuración a la NVRAM

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

1PROSPE_1con0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER PROSPE_1

User Access Verification

Password:
PROSPE_1>enable
Password:
PROSPE_1#show running-config

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

Current configuration:

Configuración actual del switch

!
version 12.0

Versión del Sistema Operativo del Router

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

Servicio de encriptación de contraseña no esta activo

```
!
hostname PROSPE_1
!
enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/
```

Indica que la contraseña de ingreso al switch se encuentra encriptada

```
!
ip subnet-zero
```

Sirve para utilizar la ip inicial al momento de subnetear

```
!
key chain private
```

Clave privada en la autenticación de Rip

```
 key 1
```

Inicialización de la autenticación de Rip

```
  key-string 234
```

Cadena de autenticación de Rip

```
!
!!
interface Ethernet0
```

Tipo de Interfaz

```
 ip address 192.168.1.33 255.255.255.224
```

Dirección IP y máscara de la interfaz

```
 no ip directed-broadcast
!
!!
interface Serial0
```

Tipo de Interfaz

```
 description Esta serial se conecta con el Router de PROSPE_1
```

Pequeña descripción de la conexión de la interfaz

```
 ip address 192.168.1.1 255.255.255.252
```

Dirección IP y máscara de dicha interfaz

```
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain private
 no ip mroute-cache
 clockrate 64000
```

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

```
!
interface Serial1
```

Tipo de Interfaz

```
 description Esta serial se conecta con el Router de PROSPE_1
```

Pequeña descripción de la conexión de la interfaz

```
 ip address 192.168.7.14 255.255.255.252
```

Dirección IP y máscara de dicha interfaz

```
 no ip directed-broadcast
!
router ospf 1
 log-adjacency-changes
        Se utiliza cuando ocurren cambios en los routers vecinos
 redistribute rip subnets
        Distribuye protocolo ospf hacia las subredes de rip
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.1.32 0.0.0.31 area 0
        Redes configuradas con el protocolo de Enrutamiento OSPF
 !
router rip
        Protocolo de Enrutamiento
 version 2
        Versión del protocolo de Enrutamiento
 redistribuye ospf 1
        Distribuye protocolo rip hacia las redes ospf
 network 192.168.7.0
        Redes configuradas con el protocolo de Enrutamiento Rip
default-metric 10
        Métrica para el enrutamiento de paquetes de ospf a rip
!
ip classless
        Indica acceso a las redes no remotas con máscara de sub red diferente
!
banner motd ^CBIENVENIDO AL ROUTER PROSPE_1^C
        Indica el mensaje de Bienvenida del Router
!
line con 0
password topico
        Contraseña para línea de comandos
 login
 transport input none
line 1 8
line aux 0
 password topico
 login
line vty 0 4
 password topico
        Contraseña para Telnet
 login
!
end
```

PROSPE_1#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, * - candidate default
U - per-user static route, o – ODR
Descripción de Protocolos usados

Gateway of last resort is not set

192.168.7.0/30 is subnetted, 1 subnets
R 192.168.7.12 is directly connected, Serial1
192.168.1.0/30 is subnetted, 1 subnets
O 192.168.1.0 is directly connected, Serial0
Especifica que esta interfaz esta conectada directamente mediante la serial 0 y serial 1
PROSPE_1#

5.8.2.7 CONFIGURACIÓN DEL ROUTER PROSPE_2

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

Acceso al modo de Configuración principal.

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

Configuración de los nombres de los Routers

Router>enable
Ingresar al modo EXEC privilegiado
Router#configure terminal
Ingresar al modo de configuración global
Router(config)#hostname PROSPE_2
Sirve para asignarle un nombre al router (PROSPE_2)
PROSPE_2(config)#

Creación de Contraseñas

PROSPE_2#enable
Ingresar al modo EXEC privilegiado
PROSPE_2#configure terminal
Ingresar al modo de configuración global
PROSPE_2(config)#
PROSPE_2(config)#line console 0
Ingresar a configurar la consola
PROSPE_2(config-line)#password cisco
Asignar una contraseña a la consola

PROSPE_2(config-line)#login
Petición de contraseña
PROSPE_2(config-line)#exit
Salir de la configuración de la consola
PROSPE_2(config)#line vty 0 4
Ingresar a configurar la Terminal virtual
PROSPE_2(config-line)#password cisco
Asignar una contraseña a la Terminal virtual
PROSPE_2(config-line)#login
Petición de contraseña
PROSPE_2(config-line)#exit
Salir de la configuración de la Terminal virtual
PROSPE_2(config)#line aux 0
Ingresar a configurar el puerto auxiliar
PROSPE_2(config-line)#password cisco
Asignar una contraseña al puerto auxiliar
PROSPE_2(config-line)#login
Petición de contraseña
PROSPE_2(config-line)#exit
Salir de la configuración del puerto auxiliar
PROSPE_2(config)#
PROSPE_2(config)#enable password cisco
Agregar una contraseña para ingresar al router
PROSPE_2(config)#enable secret cisco
Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.

PROSPE_2(config)#interface FastEthernet 0
Ingresar a la interfaz que se va a configurar
PROSPE_2(config-if)#ip address 192.168.2.1 255.255.255.224
Asignar una dirección ip con su respectiva máscara
PROSPE_2(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
PROSPE_2(config-if)#exit
Salir de la configuración de la interfaz
PROSPE_2(config)#interface serial 0
Ingresar a la interfaz que se va a configurar
PROSPE_2(config-if)#ip address 192.168.1.5 255.255.255.252
Asignar una dirección ip con su respectiva máscara
PROSPE_2(config-if)#clock rate 64000
Asignar el valor para el sincronizador del reloj
PROSPE_2(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
PROSPE_2(config-if)#exit
Salir de la configuración de la interfaz
PROSPE_2(config)#interface serial 1
Ingresar a la interfaz que se va a configurar
PROSPE_2(config-if)#ip address 192.168.1.2 255.255.255.252

Asignar una dirección ip con su respectiva máscara

PROSPE_2(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

PROSPE_2(config-if)#exit

Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento OSPF

El Protocolo de enrutamiento OSPF debe habilitarse antes de llevar a cabo cualquiera de los comandos de diagnóstico de la red, lo Habilitar utilizando:

PROSPE_2#configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)#router ospf 0

Habilitar el protocolo de enrutamiento a configurar

PROSPE_2(config-router)#network 192.168.1.0 0.0.0.3 area 0

PROSPE_2(config-router)#network 192.168.1.4 0.0.0.3 area 0

PROSPE_2(config-router)#network 192.168.2.0 0.0.0.31 area 0

Asignar la dirección de la red, wildcard y área respectiva

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

PROSPE_2#configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)#no router ospf 0

Desactiva el protocolo de enrutamiento ospf

PROSPE_2(config)#exit

Salir del modo de configuración global

Configuración de Listas de Acceso

Bloquear toda la subred 192.168.2.0/27, excepto el servidor con la siguiente ip 192.168.2.15

PROSPE_2# configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)# access-list 1 permit host 192.168.2.15

Asignar permiso a un host específico

PROSPE_2(config)# access-list 1 deny 192.168.2.0 0.0.0.31

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

PROSPE_2(config)# access-list 1 permit any

Colocar una línea implícita para ésta acl

PROSPE_2(config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

PROSPE_2# configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PROSPE_2(config)# ip access-group 1 in

Levantar la acl de manera entrante

ACL extendida

PROSPE_2# configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)#access-list 101 permit ip host 192.168.2.10 host 192.168.2.15

Asignar permiso a un host específico

PROSPE_2(config)#access-list 101 deny ip 192.168.2.0 0.0.0.31 host 192.168.2.15

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

PROSPE_2(config)#access-list 101 permit ip any any

Colocar una línea implícita para ésta acl

PROSPE_2(config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PROSPE_2# configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PROSPE_2(config)# ip access-group 101 in

Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.2.15
Denegar todo lo demás.

PROSPE_2# configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)# access-list 120 permit tcp host 192.168.2.10 host 192.168.2.15 any eq telnet

Ingresar a la interfaz que se va a asignar la acl

PROSPE_2(config)#access-list 120 deny any any

Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

PROSPE_2# configure terminal

Ingresar al modo de configuración global

PROSPE_2(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

PROSPE_2(config)# ip access-group 101 in

Levantar la acl de manera entrante

Guardar configuración

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

PROSPE_2#copy running-config startup-config
Guardar una copia de la configuración a la NVRAM

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

PROSPE_2con0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER PROSPE_2

User Access Verification

Password:
PROSPE_2>enable
Password:
PROSPE_2#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del Router
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
Servicio de encriptación de contraseña no esta activo
!
hostname PROSPE_2
!
enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/
Indica que la contraseña de ingreso al switch se encuentra encriptada
!
ip subnet-zero
Sirve para utilizar la ip inicial al momento de subnetear
!
key chain private
Clave privada en la autenticación de Rip
key 1
Inicialización de la autenticación de Rip
key-string 234
Cadena de autenticación de Rip
!

```
!!
interface Ethernet0
        Tipo de Interfaz
 ip address 192.168.2.1 255.255.255.224
        Dirección IP y máscara de la interfaz
 no ip directed-broadcast
!
!!
interface Serial0
        Tipo de Interfaz
 description Esta serial se conecta con el Router de PROSPE_2
        Pequeña descripción de la conexión de la interfaz
 ip address 192.168.1.5 255.255.255.252
        Dirección IP y máscara de dicha interfaz
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain private
 no ip mroute-cache
 clockrate 64000
       Indica la velocidad del puerto en bits por segundo Lo encontramos en la DCE.
!
interface Serial1
        Tipo de Interfaz
 description Esta serial se conecta con el Router de PROSPE_2
        Pequeña descripción de la conexión de la interfaz
 ip address 192.168.1.2 255.255.255.252
        Dirección IP y máscara de dicha interfaz
 no ip directed-broadcast
!
router ospf 1
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.1.4 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.31 area 0
        Redes configuradas con el protocolo de Enrutamiento OSPF
!
ip classless
        Indica acceso a las redes no remotas con máscara de sub red diferente
!
banner motd ^CBIENVENIDO AL ROUTER PROSPE_2^C
        Indica el mensaje de Bienvenida del Router
!
line con 0
password topico
        Contraseña para línea de comandos
 login
 transport input none
line 1 8
line aux 0
```

```
 password topico
 login
line vty 0 4
 password topico
```
Contraseña para Telnet
```
 login
!
end
```

PROSPE_2#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, * - candidate default
       U - per-user static route, o – ODR
```
Descripción de Protocolos usados
```
Gateway of last resort is not set

    192.168.1.0/30 is subnetted, 2 subnets
R       192.168.1.0 is directly connected, Serial1
R       192.168.1.4 is directly connected, Serial0
```
Especifica que esta interfaz esta conectada directamente mediante la serial 0 y serial 1
```
PROSPE_2#
```

5.8.2.8 CONFIGURACIÓN DEL ROUTER CENAIM

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

Acceso al modo de Configuración principal.

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)# exit

Salir un nivel

Router#

Configuración de los nombres de los Routers

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#hostname CENAIM

Sirve para asignarle un nombre al router (CENAIM)

CENAIM(config)#

Creación de Contraseñas

CENAIM#enable

Ingresar al modo EXEC privilegiado

CENAIM#configure terminal

Ingresar al modo de configuración global

CENAIM(config)#

CENAIM(config)#line console 0

Ingresar a configurar la consola

CENAIM(config-line)#password cisco

Asignar una contraseña a la consola

CENAIM(config-line)#login

Petición de contraseña

CENAIM(config-line)#exit

Salir de la configuración de la consola

CENAIM(config)#line vty 0 4

Ingresar a configurar la Terminal virtual

CENAIM(config-line)#password cisco

Asignar una contraseña a la Terminal virtual

CENAIM(config-line)#login

Petición de contraseña

CENAIM(config-line)#exit

Salir de la configuración de la Terminal virtual

CENAIM(config)#line aux 0

Ingresar a configurar el puerto auxiliar

CENAIM(config-line)#password cisco

Asignar una contraseña al puerto auxiliar

CENAIM(config-line)#login

Petición de contraseña

CENAIM(config-line)#exit

Salir de la configuración del puerto auxiliar

CENAIM(config)#

CENAIM(config)#enable password cisco

Agregar una contraseña para ingresar al router

CENAIM(config)#enable secret cisco

Agregar una contraseña encriptada para ingresar al router

Configuración de las Interfaces.

CENAIM(config)#interface FastEthernet 0

Ingresar a la interfaz que se va a configurar

CENAIM(config-if)#ip address 192.168.14.9 255.255.255.224

Asignar una dirección ip con su respectiva máscara

CENAIM(config-if)#no shutdown

Habilitar la interfaz para que pueda funcionar

CENAIM(config-if)#exit

Salir de la configuración de la interfaz

CENAIM(config)#interface serial 0
Ingresar a la interfaz que se va a configurar
CENAIM(config-if)#ip address 192.168.14.1 255.255.255.252
Asignar una dirección ip con su respectiva máscara
CENAIM(config-if)#clock rate 64000
Asignar el valor para el sincronizador del reloj
CENAIM(config-if)#no shutdown
Habilitar la interfaz para que pueda funcionar
CENAIM(config-if)#exit
Salir de la configuración de la interfaz

Configuración de Protocolo de Enrutamiento RIPV2

CENAIM#configure terminal
Ingresar al modo de configuración global
CENAIM(config)#router rip
Habilitar el protocolo de enrutamiento a configurar
CENAIM(config-router)#version 2
Asignar la version del protocolo ya asignado
CENAIM(config-router)#network 192.168.14.0
Asignar la dirección de la red
CENAIM(config-router)#exit
Salir de la configuración del protocolo de enrutamiento
CENAIM(config)#

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

CENAIM#configure terminal
Ingresar al modo de configuración global
CENAIM(config)#no router rip
Desactiva el protocolo de enrutamiento rip
CENAIM(config)#

Configuración de Listas de Acceso

Bloquear toda la subred 192.168.14.0/27, excepto el servidor con la siguiente ip 192.168.14.10

CENAIM# configure terminal
Ingresar al modo de configuración global
CENAIM(config)# access-list 1 permit host 192.168.14.10
Asignar permiso a un host específico
CENAIM(config)# access-list 1 deny 192.168.14.8 0.0.0.31
Negar el acceso a la red a las demás ip's
CENAIM(config)# access-list 1 permit any
Colocar una línea implícita para ésta acl
CENAIM(config)# exit
Salir del modo de configuración global

Posteriormente se levantará la acl estándar en la interfaz correspondiente.

CENAIM# configure terminal

Ingresar al modo de configuración global

CENAIM(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

CENAIM(config)# ip access-group 1 in

Levantar la acl de manera entrante

ACL extendida

CENAIM# configure terminal

Ingresar al modo de configuración global

CENAIM(config)#access-list 101 permit ip host 192.168.14.15 host 192.168.14.10

Asignar permiso a un host específico

CENAIM(config)#access-list 101 deny ip 192.168.14.8 0.0.0.31 host 192.168.14.10

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

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

Colocar una línea implícita para ésta acl

CENAIM(config)# exit

Salir del modo de configuración global

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

CENAIM# configure terminal

Ingresar al modo de configuración global

CENAIM(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

CENAIM(config)# ip access-group 101 in

Levantar la acl de manera entrante

Permitir tráfico "ping" (ICMP) desde un host específico al servidor 192.168.14.10
Denegar todo lo demás.

CENAIM# configure terminal

Ingresar al modo de configuración global

CENAIM(config)# access-list 120 permit tcp host 192.168.14.15 host 192.168.14.10 any eq telnet

Ingresar a la interfaz que se va a asignar la acl

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

Colocar una línea implícita para ésta acl

Posteriormente se levantará la acl extendida en la interfaz correspondiente.

CENAIM# configure terminal

Ingresar al modo de configuración global

CENAIM(config)# interface fast-Ethernet 0/0

Ingresar a la interfaz que se va a asignar la acl

CENAIM(config)# ip access-group 101 in

Levantar la acl de manera entrante

Guardar configuración

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

CENAIM#copy running-config startup-config
Guardar una copia de la configuración a la NVRAM

Lo que se le indica al router con esta instrucción es que el contenido del archivo **running-config** se copie en el **startup-config**. El archivo **running-config** se encuentra en memoria RAM y el **startup-config** se almacena en memoria **NVRAM**, así si se pierde el fluido eléctrico la configuración que se tenia se recuperará de la memoria **NVRAM (startup-config).**
CENAIMcon0 is now available
Press RETURN to get started.

BIENVENIDO AL ROUTER CENAIM

User Access Verification
Password:
CENAIM>enable
Password:
CENAIM#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz especifica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del Router
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
Servicio de encriptación de contraseña no esta activo
!
hostname CENAIM
!
enable secret 5 $1$8Ow2$BAv1G3dGyyZ3usjGfTNPx/
Indica que la contraseña de ingreso al switch se encuentra encriptada
!
ip subnet-zero
Sirve para utilizar la ip inicial al momento de subnetear
!
key chain private
Clave privada en la autenticación de Rip
key 1

Inicialización de la autenticación de Rip
key-string 234
Cadena de autenticación de Rip
!
!!
interface Ethernet0
Tipo de Interfaz
ip address 192.168.14.9 255.255.255.224
Dirección IP y máscara de la interfaz
no ip directed-broadcast
!
!!
interface Serial0
Tipo de Interfaz
description Esta serial se conecta con el Router de CENAIM
Pequeña descripción de la conexión de la interfaz
ip address 192.168.14.1 255.255.255.252
Dirección IP y máscara de dicha interfaz
no ip directed-broadcast
ip rip authentication mode md5
ip rip authentication key-chain private
no ip mroute-cache
clockrate 64000
Indica la velocidad del puerto en bits por segundo Lo encontramos en la DCE.
!
interface Serial0
Tipo de la interfaz
no ip address
Esto significa que no tiene ninguna ip asignada
no ip directed-broadcast
shutdown
Esto describe el estado de la interfaz, Up(Levantada) o Down (Caída)
!
router rip
Protocolo de Enrutamiento
version 2
Versión del protocolo de Enrutamiento
network 192.168.14.0
Redes configuradas con el protocolo de Enrutamiento Rip
!
ip classless
Indica acceso a las redes no remotas con máscara de sub red diferente
!
banner motd ^CBIENVENIDO AL ROUTER CENAIM^C
Indica el mensaje de Bienvenida del Router
!
line con 0
password topico

Contraseña para línea de comandos

```
 login
 transport input none
line 1 8
line aux 0
 password topico
 login
line vty 0 4
 password topico
```

Contraseña para Telnet

```
 login
!
end
```

CENAIM#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, * - candidate default
       U - per-user static route, o – ODR
```

Descripción de Protocolos usados

```
Gateway of last resort is not set

    192.168.14.0/30 is subneTted, 1 subnets
C       192.168.14.0 is directly connected, Serial1
R       192.168.1.4/24 [120/1] via 192.168.14.2, 00:00:12, Serial1
```

Especifica que esta interfaz esta conectada directamente mediante la serial 0 y serial 1

```
CENAIM#
```

5.9 INTRODUCCIÓN A LOS SWITCHES

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.

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. La configuración básica del switch, las actualizaciones de IOS y la recuperación de contraseñas son capacidades esenciales del administrador de red.

5.9.1 CONFIGURACIÓN DE SWITCHES

Se procederá ahora con la configuración de los Switches.

5.9.1.1 MODOS DE INTERFAZ USUARIO

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

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

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

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

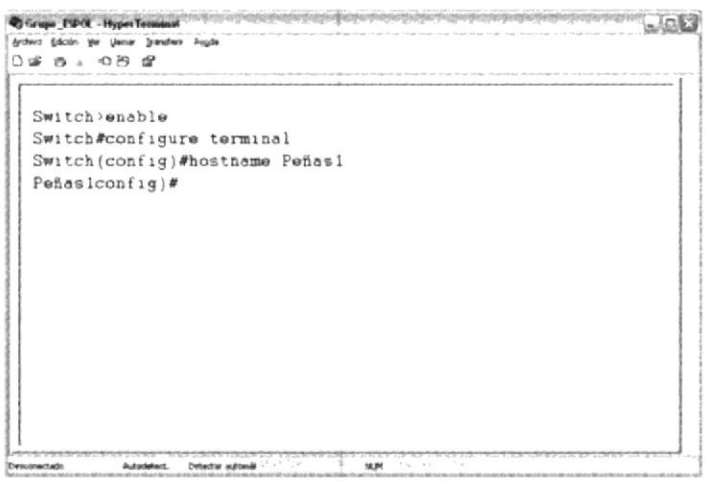


Figura 5.64 Modos de Usuario

5.9.1.2 CONFIGURACIÓN DE CONTRASEÑAS

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

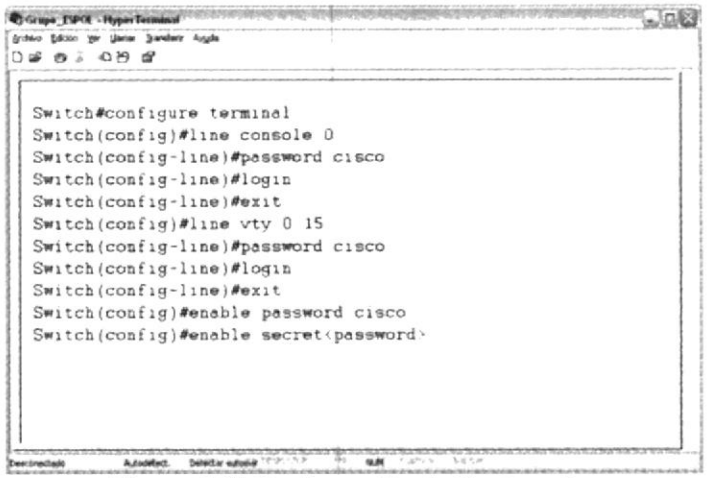


Figura 5.65 Configuración de Contraseñas

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

5.9.1.3 EXAMINANDO EL COMANDO HELP EN LA CLI DEL SWITCH

En esta página se explica de qué manera el comando help se utiliza en la CLI de los switches Cisco.

La CLI de los switches Cisco es muy similar a la CLI de los routers Cisco.

Introduzca un signo de interrogación (?) para emitir el comando help. Cuando se introduce este comando en el indicador del sistema, aparece una lista de comandos disponibles para el modo de comandos actual.

El comando **help** es muy flexible. Para obtener una lista de comandos que empiecen con una determinada secuencia de caracteres, introduzca estos caracteres seguidos inmediatamente por el signo de interrogación (**?**).

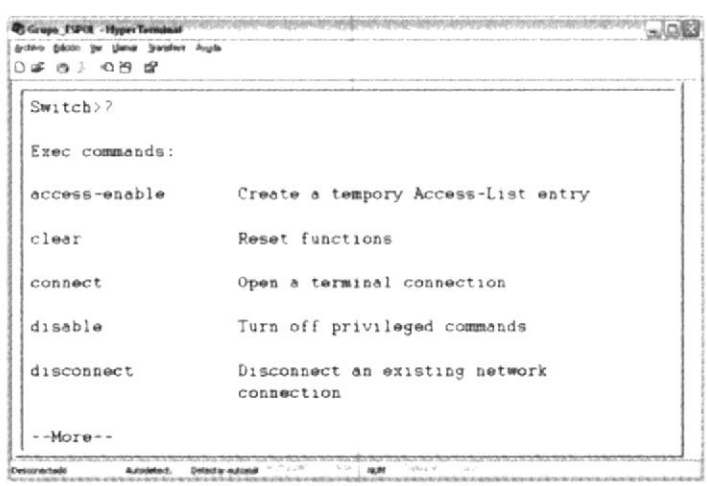


Figura 5.66 Comando Help

5.9.1.4 ASPECTOS BÁSICOS DE LAS VLAN

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

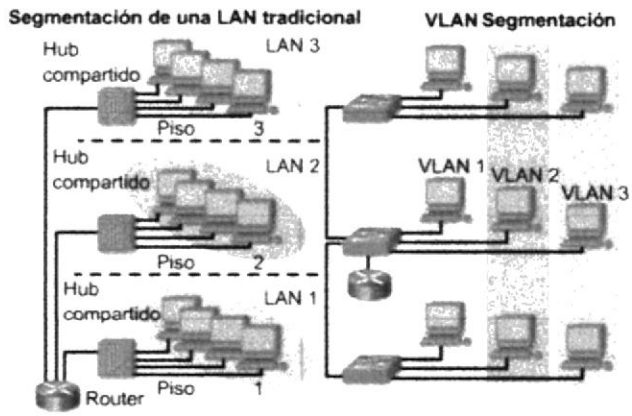


Figura 5.67 Comparación de una LAN tradicional y una VLAN

Las VLAN se configuran en el switch a través del software. Debido a la cantidad de implementaciones de VLAN que compiten entre sí es posible que deba requerirse el uso de un software propietario por parte del fabricante del switch. La agrupación de puertos y usuarios en comunidades de interés, conocidos como organizaciones VLAN, puede obtenerse mediante el uso de un solo switch o una conexión más potente entre los switches ya conectados dentro de la empresa. Al agrupar puertos y usuarios en varios switches, las VLAN pueden abarcar infraestructuras contenidas en un solo edificio o en edificios interconectados. Las VLAN ayudan a utilizar con efectividad el ancho de banda dado que comparten el mismo dominio de broadcast o la misma red de Capa 3. Las VLAN optimizan la acumulación y uso del ancho de banda. Las VLAN se disputan el mismo ancho de banda aunque los requisitos del ancho de banda pueden variar considerablemente según el grupo de trabajo o el departamento.

A continuación, 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.

5.9.1.5 CONFIGURACIÓN DE VLAN POR DEFECTO

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

Figura 5.68 Configuración de Vlan por defecto

5.9.1.6 CREACIÓN DE VLAN'S

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

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

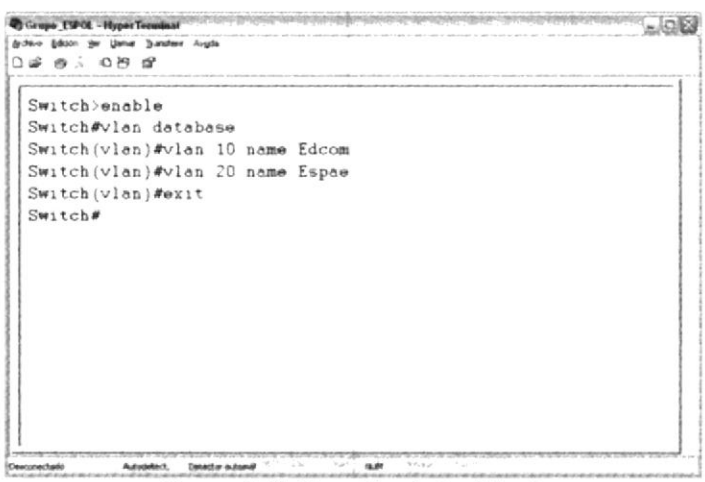


Figura 5.69 Creación de las Vlan's

5.9.1.7 BORRADO DE VLAN'S

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

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

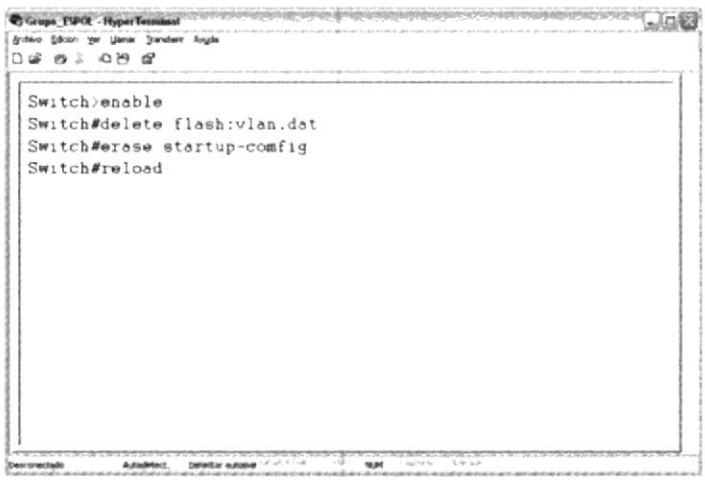


Figura 5.70 Borrado de las Vlan's

5.9.1.8 ASIGNACIÓN DE VLAN'S A LOS PUERTOS

Figura 5.71 Asignación de vlan´s a los puertos

5.9.1.9 ENRUTAMIENTO ENTRE VLAN

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

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

Figura 5.72 Enlace Troncal

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

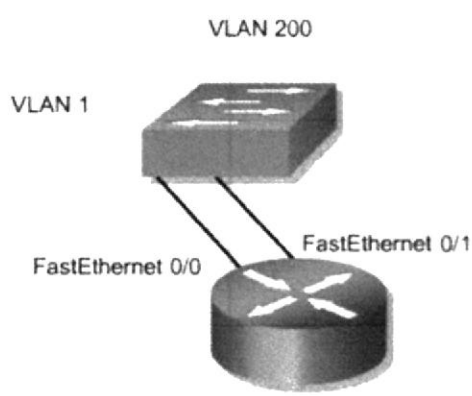


Figura 5.73 Enlace Switch - Router

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

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

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

5.9.1.10 INTERFACES FÍSICAS Y LÓGICAS

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

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

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

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

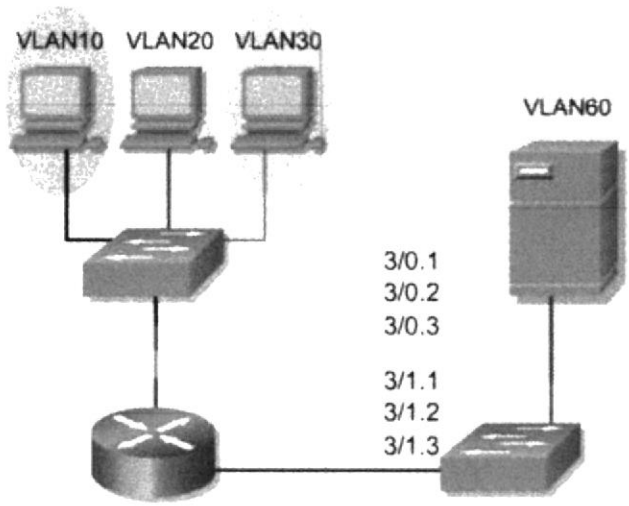


Figura 5.74 Interfaces físicas y lógicas

La ventaja principal del uso del enlace troncal es una reducción en la cantidad de puertos de router y switch que se utiliza. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de router conectado a un enlace troncal puede ampliarse hasta un número mucho más alto de VLAN que el diseño de "un enlace por VLAN".

5.9.1.11 ASIGNAR SWITCH DE TIPO SERVER

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

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

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

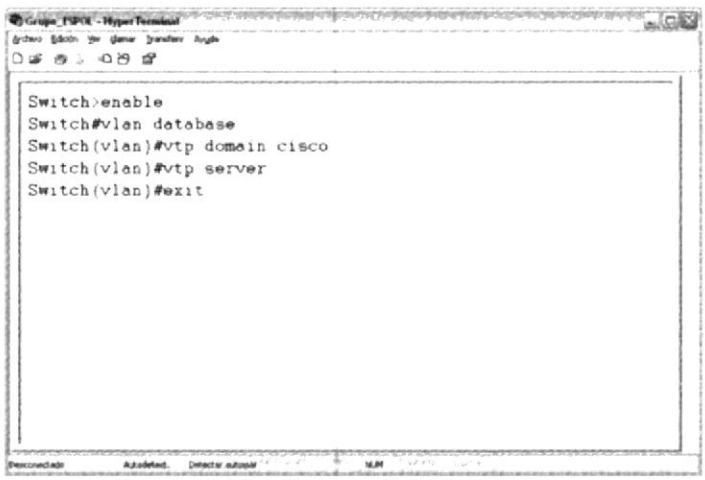


Figura 5.75 Asignar switch de tipo server

5.9.1.12 CONFIGURACIÓN DE UN ENRUTAMIENTO ENTRE DISTINTAS VLAN

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

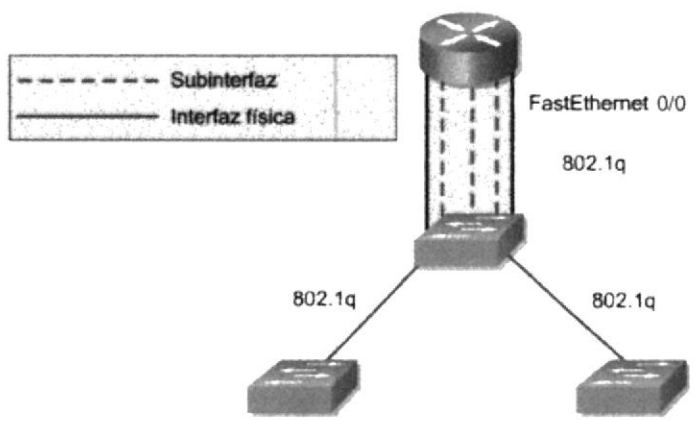


Figura 5.76 Enrutamiento entre distintas vlan's

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

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

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

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

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

Port-number identifica la interfaz física y ***subinterface-number*** identifica la interfaz virtual (Vlan).

El router debe poder comunicarse con el switch utilizando un protocolo de enlace troncal estandarizado. Esto significa que ambos dispositivos conectados entre sí deben comprenderse. Para definir el encapsulamiento de la VLAN, introduzca el comando **encapsulation** en el modo de configuración de interfaz.

Router(config-if)#encapsulation dot1q Vlan -number

Vlan-number identifica la VLAN para la cual la subinterfaz transportará el tráfico. Se agrega un ID de VLAN a la trama sólo cuando la trama está destinada a una red no local. Cada paquete de VLAN transporta el ID de VLAN dentro del encabezado del paquete.

Para asignar una dirección IP a la interfaz, introduzca el siguiente comando en el modo de configuración de interfaz.

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

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

Figura 5.77 Configuración de enrutamiento entre distintas vlan's

5.9.1.13 PROCEDIMIENTO PASO A PASO PARA LA CONFIGURACIÓN DE SWITCH (GRUPO – ESPOL)

Ahora pasaremos a configurar paso a paso los diferentes Switch de la red ESPOL.

5.9.1.13.1CONEXIÓN DE UNA TERMINAL CON LA CONSOLA DEL SWITCH

Antes de empezar, tenemos que tener claro que nuestra conexión se realizará a través de la Aplicación HyperTerminal de Windows.

> **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:

7. Con un cable transpuesto **RJ-45** a **RJ-45** y un adaptador **RJ-45** a **DB-9** o **RJ-45** a **DB-25** conectar de una Terminal (PC – Personal Computer) al puerto de consola del Switch.
8. Abrimos la aplicación HyperTerminal siguiendo los siguientes pasos.
   - En el Escritorio de Windows damos clic con el botón izquierdo en el menú llamada "Inicio"

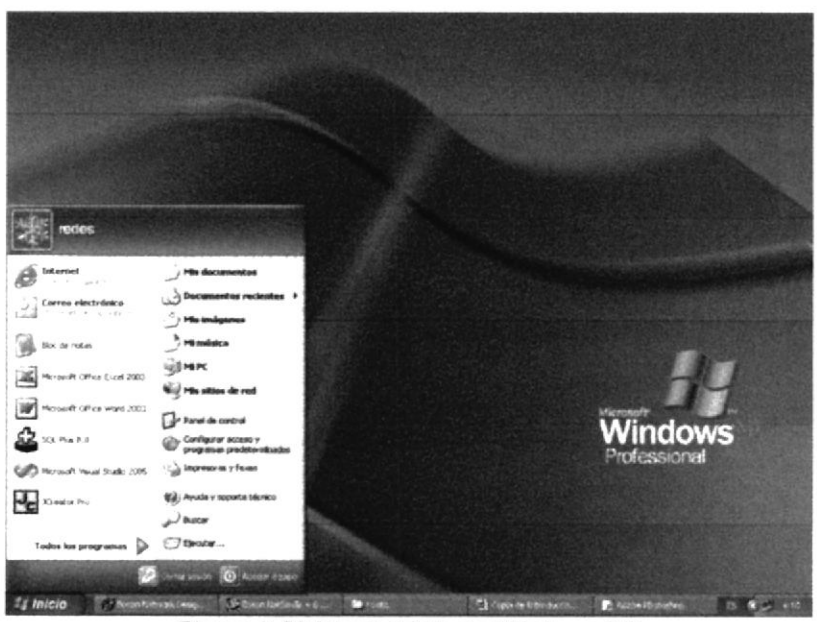


Figura 5.78 Menú Inicio de Windows XP

   - En el menú desplegable buscar la opción **"Todos los Programas"** o **"Programas"** según la versión y dar un clic con el botón izquierdo la cual desplegará otro pequeño submenú.

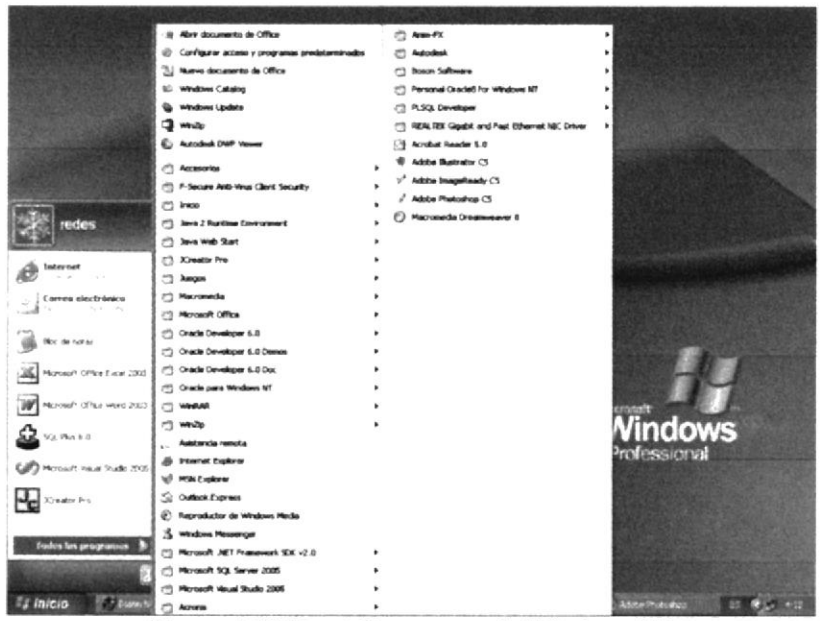


Figura 5.79 Menú Programas de Windows XP

- En este submenú buscar el menú **"Accesorios"** y dar un clic izquierdo, la cual hará acceder a un nuevo nivel de submenú.

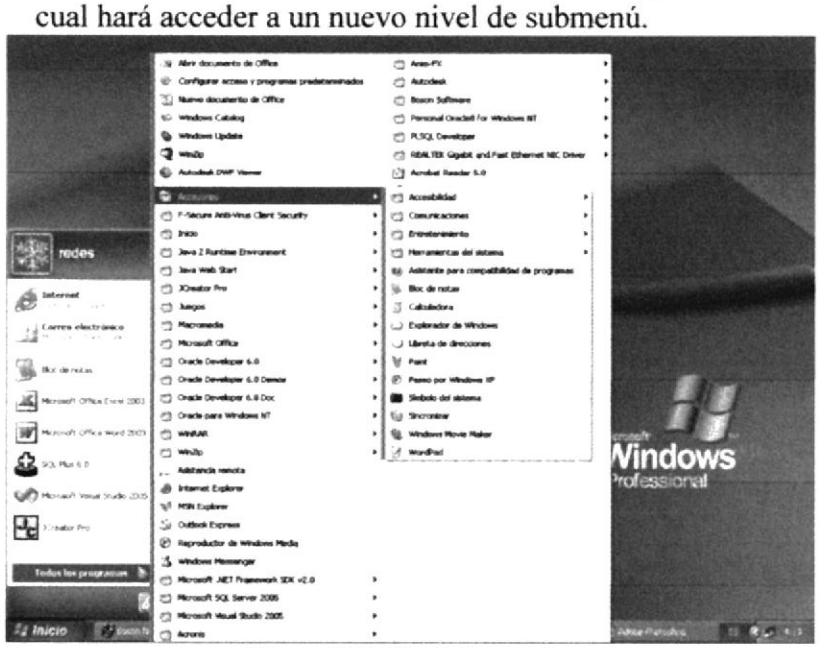


Figura 5.80 Menú Accesorios

- En este submenú aparecerán algunas de las herramientas que proporciona Windows, y la que interesa es la de Comunicaciones, dar clic izquierdo.

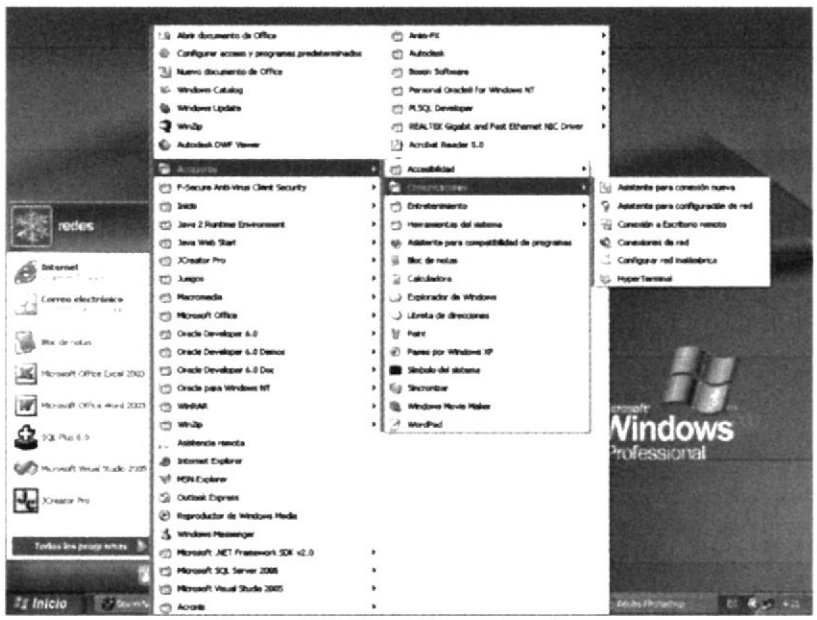


Figura 5.81 Menú Comunicaciones

- Buscar la aplicación de HyperTerminal en el submenú que se desplegó y dar clic izquierdo.

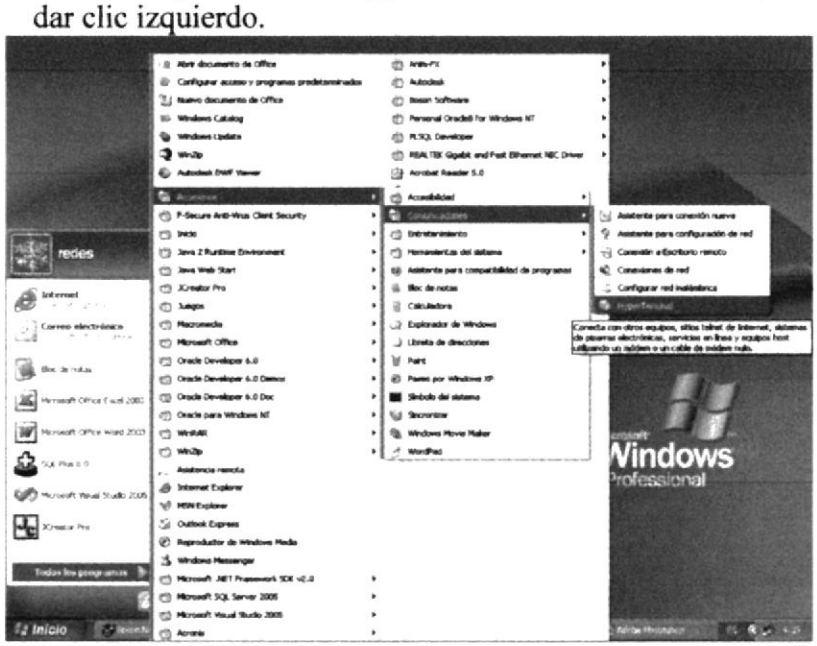


Figura 5.82 Aplicación HyperTerminal

9. Una vez que se ha encontrado dar clic izquierdo en la opción de HyperTerminal, si es la primera vez que se accede a esta aplicación, aparecerá una ventana de Advertencia, donde se recomienda establecer la Aplicación HyperTerminal como programa predeterminada de Telnet.

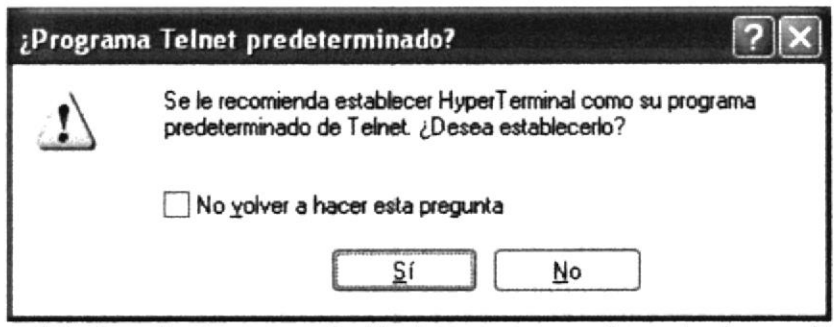


Figura 5.83 Pantalla de recomendación de programa predeterminado para Telnet

- La primera opción es si se desea volver a ver esta pregunta la próxima vez que se acceda a la HyperTerminal. Esta opción no afectará en lo más mínimo a nuestra conexión.
- Ahora presenta dos opciones de respuesta referente a la recomendación que hace Windows, si se acepta **"Sí"** automáticamente aparecerá una ventana, la cual solicita cierta información para una conexión mediante un MODEM; pero como este no es el caso simplemente **"cancelamos",** y automáticamente aparecerá la ventana de **"Descripción de conexión"** de la HyperTerminal.

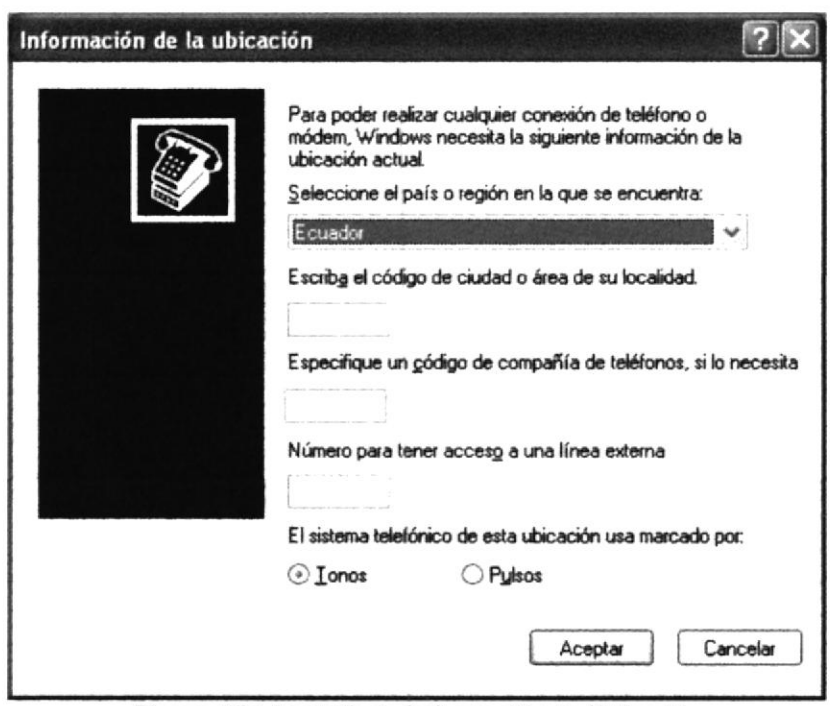


Figura 5.84 Pantalla de Información de Ubicación

- Si en un caso en la ventana que Windows recomendaba establecer a la aplicación HyperTerminal como predeterminada para Telnet, la cancelábamos, automáticamente aparecería la ventana de **"Descripción de la conexión"** de la HyperTerminal.

Figura 5.85 Pantalla de Descripción de la conexión de la HyperTerminal

10. En la ventana de **"Descripción de la conexión"** de la HyperTerminal pide un nombre y un icono para la conexión.

- El nombre puede ser cualquiera, en este caso le llamaremos Grupo_ESPOL.
- Cada icono es un tipo de conexión diferente, para este caso utilizaremos el primero, el que viene marcado por default.

- Si llenamos los datos que pide la ventana de **"Descripción de conexión"** y damos aceptar, automáticamente aparecerá la venta de **"Conectar a"**

Figura 5.86 Pantalla Descripción de la conexión

Figura 5.87 Pantalla Conectar a

11. En la ventana de **"Conectar a"** aparte de la opción **"Conectar usando"** las demás vendrán deshabilitadas, y en la opción habilitada escogeremos por medio de que puerto del computador se conectará al router, por lo general es el puerto COM1, y viene por default. Desplegando la caja de texto podremos ver los diferentes puertos disponibles del PC.

Figura 5.88 Pantalla Conectar a 2

- Si cancelamos la ventana de **"Conectar a",** automáticamente se cerrará y quedará activa la ventana de **"Nueva Conexión – HyperTerminal"**, y procedemos a cerrarlo según lo explicado antes.
- Si aceptamos, no aparecerá una ventana de **"Propiedades del COM1"**, estas son la propiedades del puerto que escogimos para conectarnos con el Router.

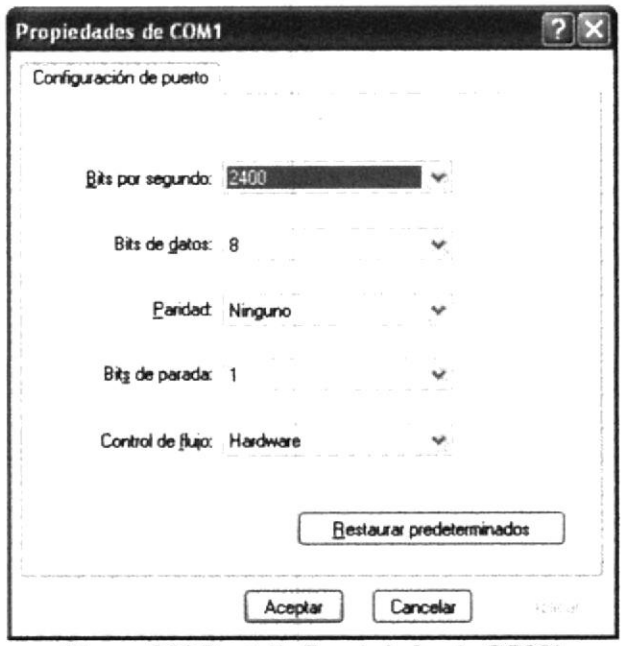


Figura 5.89 Pantalla Propiedades de COM1

12. En la ventana de **"Propiedades de COM1",** debemos configurar según las especificaciones dadas a continuación.
    - 9600 bps
    - 8 bits de datos
    - Ninguno (paridad)
    - 1 (Bit de parada)
    - Ninguno (Control de flujo)

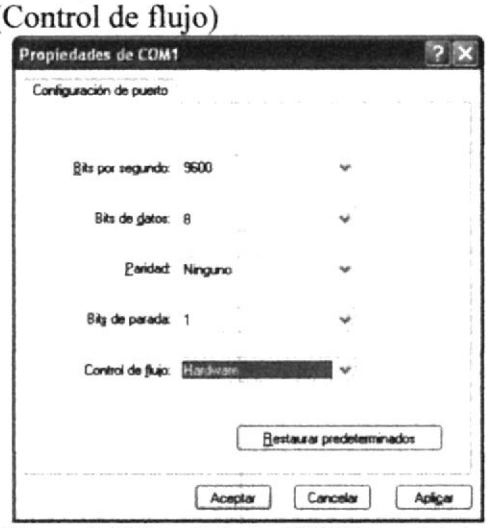


Figura 5.90 Propiedades COM1 cambiadas

a. La pantalla de **"Propiedades de COM1"** proporciona 3 diferentes opciones: Restaurar Predeterminados, Aceptar, Cancelar y Aplicar. Cada una tiene una función diferente. Si damos clic izquierdo en el botón **Restaurar Predeterminados,** las propiedades del COM1 regresarán a las que estaban cuando recién se abrió la ventana.

b. La segunda opción es **"Aplicar",** esta opción establecerá las opciones que se están configurando, pero aun no los hará surtir efecto.

c. La otra opción que aparece es la ventana de **"Propiedades de COM1"** es la de **"Aceptar"**, esta opción surtirá efecto las opciones configuradas, inclusive podemos obviar el paso de primero **"Aplicar"** y luego **"Aceptar".** Una vez dado clic en **"Aceptar"** se conectará inmediatamente al **Switch.**

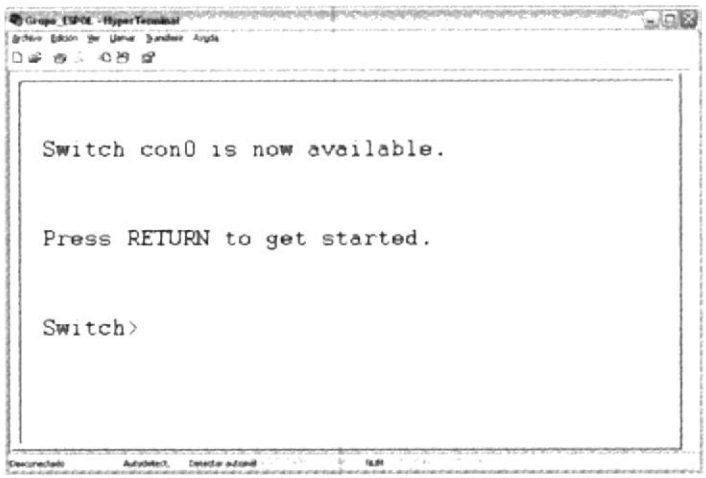


Figura 5.91 Pantalla Inicio de Interfaz con el Router

d. La tercera y ultima opción es la de **"Cancelar",** si damos clic aquí automáticamente se la ventana se cerrará y se activará la ventana de **"Nueva Conexión - HyperTerminal",** luego la cerramos según lo requerido y ya aprendido.

5.9.1.14 CONFIGURACIÓN DEL SWITCH PEÑAS_1

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

Acceso al modo de Configuración principal.

Switch>enable

Ingresar al modo EXEC privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch(config)#exit

Salir un nivel

Configuración de los nombres de los Peñas_1s

Peñas_1>enable

Ingresar al modo EXEC privilegiado

Peñas_1#configure terminal

Ingresar al modo de configuración global

Peñas_1(config)#hostname peñas1

Sirve para asignarle un nombre al Peñas_1 (Peñas1)

Peñas1config)#

Configuración de Contraseñas

Peñas_1#configure terminal
Ingresar al modo de configuración global
Peñas_1(config)#line console 0
Ingresar a configurar la consola
Peñas_1(config-line)#password <password>
Asignar una contraseña a la consola
Peñas_1(config-line)#login
Peñas_1(config-line)#exit
Salir de la configuración de la consola
Peñas_1(config)#line vty 0 15
Ingresar a configurar la Terminal virtual
Peñas_1(config-line)#password <password>
Asignar una contraseña a la Terminal virtual
Peñas_1(config-line)#login
Peñas_1(config-line)#exit
Salir de la configuración de la Terminal virtual
Peñas_1(config)#enable password<password>
Agregar una contraseña para ingresar al router
Peñas_1(config)#enable secret<password>
Agregar una contraseña encriptada para ingresar al router

Creación de VLAN's

Peñas_1>enable
Ingresar al modo de configuración global
Peñas_1#vlan database
Ingresar al modo de configuración de vlan's
Peñas_1(Vlan)#Vlan 10 name Edcom
Asignar un número referencial y un nombre a la Vlan que se va a crear
Peñas_1(Vlan)#Vlan 20 name Espae
Asignar un número referencial y un nombre a la Vlan que se va a crear
Peñas_1(Vlan)#exit
Salir del modo configuración de Vlan
Peñas_1#

Asignación de VLAN's a los puertos

Peñas_1>enable
Ingresar al modo EXEC privilegiado
Peñas_1#configure terminal
Ingresar al modo de configuración global
Peñas_1(config)#
Peñas_1(config)#interface fastethernet 0/2
Ingresar a la interfaz puerto que se va a configurar
Peñas_1(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
Peñas_1(config-if)#switchport access Vlan 10
Asignar el puerto a la Vlan 10
Peñas_1(config-if)#exit
Peñas_1(config)#interface fastethernet 0/4
Ingresar a la interfaz puerto que se va a configurar
Peñas_1(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan

Peñas_1(config-if)#switchport access vlan 20
Asignar el puerto a la Vlan 20
Peñas_1(config-if)#exit

Asignar Peñas_1 de Tipo Server

Peñas_1>enable
Ingresar al modo EXEC privilegiado
Peñas_1#vlan database
Ingresar al modo de configuración de Vlan
Peñas_1(Vlan)#vtp domain cisco
Asignar un dominio vtp al Peñas_1
Peñas_1(Vlan)#vtp server
Configurar de modo server el Peñas_1
Peñas_1(Vlan)#exit
Salir al modo de configuración global

Configuración de un enrutamiento entre distintas VLAN (Router Peñas_1)

Router>enable
Ingresar al modo EXEC privilegiado
Router#configure terminal
Ingresar al modo de configuración global
Router(config)#interface FastEthernet 0/0.1
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 10
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 10
Router(config-subif)#ip address 192.168.7.1 255.255.255.0
Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.20
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 20
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 20
Router(config-subif)#ip address 192.168.7.65 255.255.255.0
Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#exit
Salir del modo de configuración global
Router#copy runn-config startup-config
Guardar una copia de la configuración a la NVRAM

Switch _Peñas1con0 is now available

Press RETURN to get started.

BIENVENIDO AL Switch_Peñas1

User Access Verification

Password:
Switch_Peñas1>enable
Password:

Switch_Peñas1#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del switch
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
El servicio de encriptación de contraseña no esta activo
!
hostname Switch_Peñas1
Nombre del switch
!
enable secret 5 1/GbR$LBaLnR1hq1.CeffXBwKw40
Indica que la contraseña de ingreso al switch se encuentra encriptada
!
!
!
!
ip subnet-zero
Sirve para utilizar la ip inicial al momento de subnetear
!
!
!

interface FastEthernet0/1
Puertos físicos del switch, aquí se verifica a que Vlan pertenece
!
interface FastEthernet0/2
switchport access vlan 10
Puerto asignado a la Vlan 10
!
interface FastEthernet0/3
switchport access vlan 10
Puerto asignado a la Vlan 10
!

```
interface FastEthernet0/4
switchport access vlan 20
        Puerto asignado a la Vlan 20
!
interface FastEthernet0/5
 switchport access vlan 20
        Puerto asignado a la Vlan 20
!
interface FastEthernet0/6
        Puerto sin configurar
!
interface FastEthernet0/7
        Puerto sin configurar
!
interface FastEthernet0/8
        Puerto sin configurar
!
interface FastEthernet0/9
        Puerto sin configurar
!
interface FastEthernet0/10
        Puerto sin configurar
!
interface FastEthernet0/11
        Puerto sin configurar
!
interface FastEthernet0/12
        Puerto sin configurar
!
interface FastEthernet0/13
        Puerto sin configurar
!
interface FastEthernet0/14
        Puerto sin configurar
!
interface FastEthernet0/15
        Puerto sin configurar
!
interface FastEthernet0/16
        Puerto sin configurar
!
interface FastEthernet0/17
        Puerto sin configurar
!
interface FastEthernet0/18
        Puerto sin configurar
!
interface FastEthernet0/19
```

Puerto sin configurar
!
interface FastEthernet0/20
Puerto sin configurar
!
interface FastEthernet0/21
Puerto sin configurar
¡
interface FastEthernet0/22
Puerto sin configurar
!
interface FastEthernet0/23
Puerto sin configurar
!
interface FastEthernet0/24
Puerto sin configurar
!
interface GigabitEthernet0/1
Puerto que transmite a 10/100/1000, sin configurar
!
interface GigabitEthernet0/2
!
interface VLAN1
Puerto 1 del switch, Vlan de administración o defecto por donde salen los demás puertos si no tuvieran ninguna Vlan asignada)

ip address 192.168.7.2 255.255.255.0
Dirección ip asignada a la Vlan por defecto del switch
no ip directed-broadcast
no ip route-cache
!
ip default-gateway 192.168.7.1
Dirección ip por la cual saldrán todos los puertos del switch hacia otras subredes
!
line con 0
Contraseña para la línea de comandos
password cisco
login
line vty 0 15
Contraseña para telnet
password cisco
login
!
End
Switch_Peñas1#show Vlan
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------

```
1    default                active    Fa0/1, Fa0/6, Fa0/7, Fa0/8,
                                      Fa0/9, 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, Gi0/1, Gi0/2
```

Número de puertos asignados a la Vlan de administración

```
10   Edcom                  active  Fa0/2, Fa0/3
```

Puertos asignados y activos a la Vlan Edcom

```
20   Espae                  active    Fa0/4, Fa0/5
```

Puertos asignados y activos a la Vlan Espae

```
1002 fddi-default                active
```

Vlan para red fddi active

```
1003 token-ring-default          active
```

Vlan para red token ring 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
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

5.9.1.15 CONFIGURACIÓN DEL SWITCH STA_ELENA

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

Acceso al modo de Configuración principal.

Switch>enable

Ingresar al modo EXEC privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch(config)#exit

Salir un nivel

Configuración de los nombres de los Sta_Elena

Sta_Elena>enable

Ingresar al modo EXEC privilegiado

Sta_Elena#configure terminal

Ingresar al modo de configuración global

Sta_Elena(config)#hostname Sta_Elena
Sirve para asignarle un nombre al Switch (Sta_Elena)
Sta_Elena #

Configuración de Contraseñas

Sta_Elena#configure terminal
Ingresar al modo de configuración global
Sta_Elena(config)#line console 0
Ingresar a configurar la consola
Sta_Elena(config-line)#password <password>
Asignar una contraseña a la consola
Sta_Elena(config-line)#login
Sta_Elena(config-line)#exit
Salir de la configuración de la consola
Sta_Elena(config)#line vty 0 15
Ingresar a configurar la Terminal virtual
Sta_Elena(config-line)#password <password>
Asignar una contraseña a la Terminal virtual
Sta_Elena(config-line)#login
Sta_Elena(config-line)#exit
Salir de la configuración de la Terminal virtual
Sta_Elena(config)#enable password<password>
Agregar una contraseña para ingresar al router
Sta_Elena(config)#enable secret<password>
Agregar una contraseña encriptada para ingresar al router

Creación de VLAN's

Sta_Elena>enable
Ingresar al modo de configuración global
Sta_Elena#vlan database
Ingresar al modo de configuración de vlan's
Sta_Elena(Vlan)#Vlan 10 name Celex
Asignar un número referencial y un nombre a la Vlan que se va a crear
Sta_Elena(Vlan)#Vlan 20 name Biblioteca
Asignar un número referencial y un nombre a la Vlan que se va a crear
Sta_Elena(Vlan)#exit
Salir del modo configuración de Vlan
Sta_Elena#

Asignación de VLAN's a los puertos

Sta_Elena>enable
Ingresar al modo EXEC privilegiado
Sta_Elena#configure terminal
Ingresar al modo de configuración global
Sta_Elena(config)#
Sta_Elena(config)#interface fastethernet 0/2
Ingresar a la interfaz puerto que se va a configurar
Sta_Elena(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
Sta_Elena(config-if)#switchport access Vlan 10

Asignar el puerto a la Vlan 10

Sta_Elena(config-if)#exit

Sta_Elena(config)#interface fastethernet 0/4

Ingresar a la interfaz puerto que se va a configurar

Sta_Elena(config-if)# switchport mode access

Ingresar al modo de configuración para asignar la Vlan

Sta_Elena(config-if)# switchport access vlan 20

Asignar el puerto a la Vlan 20

Sta_Elena(config-if)#exit

Asignar Sta_Elena de Tipo Server

Sta_Elena>enable

Ingresar al modo EXEC privilegiado

Sta_Elena#vlan database

Ingresar al modo de configuración de Vlan

Sta_Elena(Vlan)#vtp domain cisco

Asignar un dominio vtp al Sta_Elena

Sta_Elena(Vlan)#vtp server

Configurar de modo server el Sta_Elena

Sta_Elena(Vlan)#exit

Salir al modo de configuración global

Configuración de un enrutamiento entre distintas VLAN (Router Sta_Elena)

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#interface FastEthernet 0/0.1

Ingresar a la sub-interfaz que se va a configurar

Router(config-subif)#encapsulation dot1q 10

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

Router(config-subif)#ip address 192.168.11.25 255.255.255.0

Asignar una dirección ip con su respectiva máscara

Router(config-subif)#exit

Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.20

Ingresar a la sub-interfaz que se va a configurar

Router(config-subif)#encapsulation dot1q 20

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

Router(config-subif)#ip address 192.168.11.57 255.255.255.0

Asignar una dirección ip con su respectiva máscara

Router(config-subif)#exit

Salir de la configuración de la sub-interfaz

Router(config)#exit

Salir del modo de configuración global

Router#copy runn-config startup-config

Guardar una copia de la configuración a la NVRAM

Sta_Elenacon0 is now available
Press RETURN to get started.

BIENVENIDO AL SWITCH Sta_Elena

User Access Verification

Password:
Sta_Elena >enable
Password:

Sta_Elena#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del switch
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
El servicio de encriptación de contraseña no esta activo
!
hostname Switch_Sta_Elena
Nombre del switch
!
enable secret 5 1/GbR$LBaLnR1hq1.CeffXBwKw40
Indica que la contraseña de ingreso al switch se encuentra encriptada
!
!
!
!
ip subnet-zero
Sirve para utilizar la ip inicial al momento de subnetear
!
!
!
interface FastEthernet0/1
Puertos fisicos del switch, aquí se verifica a que Vlan pertenece
!
interface FastEthernet0/2
switchport access Vlan 10
Puerto asignado a la Vlan 10
!
interface FastEthernet0/3
switchport access vlan 10

Puerto asignado a la Vlan 10
!
interface FastEthernet0/4
switchport access vlan 20
Puerto asignado a la Vlan 20
!
interface FastEthernet0/5
switchport access vlan 20
Puerto asignado a la Vlan 20
!
interface FastEthernet0/6
Puerto sin configurar
!
interface FastEthernet0/7
Puerto sin configurar
!
interface FastEthernet0/8
Puerto sin configurar
!
interface FastEthernet0/9
Puerto sin configurar
!
interface FastEthernet0/10
Puerto sin configurar
!
interface FastEthernet0/11
Puerto sin configurar
!
interface FastEthernet0/12
Puerto sin configurar
!
interface FastEthernet0/13
Puerto sin configurar
!
interface FastEthernet0/14
Puerto sin configurar
!
interface FastEthernet0/15
Puerto sin configurar
!
interface FastEthernet0/16
Puerto sin configurar
!
interface FastEthernet0/17
Puerto sin configurar
!
interface FastEthernet0/18
Puerto sin configurar

```
!
interface FastEthernet0/19
        Puerto sin configurar
!
interface FastEthernet0/20
        Puerto sin configurar
!
interface FastEthernet0/21
        Puerto sin configurar
!
interface FastEthernet0/22
        Puerto sin configurar
!
interface FastEthernet0/23
        Puerto sin configurar
!
interface FastEthernet0/24
        Puerto sin configurar
!
interface GigabitEthernet0/1
        Puerto que transmite a 10/100/1000, sin configurar
!
interface GigabitEthernet0/2
!
interface VLAN1
        Puerto 1 del switch, Vlan de administración o defecto por donde salen los
        demás puertos si no tuvieran ninguna Vlan asignada)

 ip address 192.168.11.2 255.255.255.0

        Dirección ip asignada a la Vlan por defecto del switch
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 192.168.11.1
        Dirección ip por la cual saldrán todos los puertos del switch hacia otras
        subredes
!
line con 0
        Contraseña para la línea de comandos
 password cisco
 login
line vty 0  15
        Contraseña para telnet
password cisco
 login
!
End
```

Sta_Elena#show Vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/6, Fa0/7, Fa0/8,
                                                 Fa0/9, 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, Gi0/1, Gi0/2
```

Número de puertos asignados a la Vlan de administración

```
10   Celex                             active    Fa0/2, Fa0/3
```

Puertos asignados y activos a la Vlan Celex

```
20   Biblioteca                        active    Fa0/4, Fa0/5
```

Puertos asignados y activos a la Vlan Biblioteca

```
1002 fddi-default                      active
```

Vlan para red fddi active

```
1003 token-ring-default                active
```

vlan para red token ring 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
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

5.9.1.16 CONFIGURACIÓN DEL SWITCH SAMBORONDON

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

Acceso al modo de Configuración principal.

Switch>enable

Ingresar al modo EXEC privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch(config)#exit

Salir al modo de configuración global

Configuración de nombre del Switch SAMBORONDON

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

Configuración de Contraseñas

SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)#line console 0
Ingresar a configurar la consola
SAMBORONDON(config-line)#password <password>
Asignar una contraseña a la consola
SAMBORONDON(config-line)#login
SAMBORONDON(config-line)#exit
Salir de la configuración de la consola
SAMBORONDON(config)#line vty 0 15
Ingresar a configurar la Terminal virtual
SAMBORONDON(config-line)#password <password>
Asignar una contraseña a la Terminal virtual
SAMBORONDON(config-line)#login
SAMBORONDON(config-line)#exit
Salir de la configuración de la Terminal virtual
SAMBORONDON(config)#enable password<password>
Agregar una contraseña para ingresar al router
SAMBORONDON(config)#enable secret<password>
Agregar una contraseña encriptada para ingresar al router

Creación de VLAN's

SAMBORONDON>enable
Ingresar al modo de configuración global
SAMBORONDON#vlan database
Ingresar al modo de configuración de vlan's
SAMBORONDON(Vlan)#Vlan 10 name Edcom
Asignar un número referencial y un nombre a la Vlan que se va a crear
SAMBORONDON(Vlan)#exit
Salir del modo configuración de Vlan
SAMBORONDON#

Asignación de VLAN's a los puertos

SAMBORONDON>enable
Ingresar al modo EXEC privilegiado
SAMBORONDON#configure terminal
Ingresar al modo de configuración global
SAMBORONDON(config)#

SAMBORONDON(config)#interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

SAMBORONDON(config-if)#switchport mode access

Ingresar al modo de configuración para asignar la Vlan

SAMBORONDON(config-if)#switchport access vlan 10

Asignar el puerto a la Vlan 10

SAMBORONDON(config-if)#exit

Asignar SAMBORONDON de Tipo Server

SAMBORONDON>enable

Ingresar al modo EXEC privilegiado

SAMBORONDON#vlan database

Ingresar al modo de configuración de Vlan

SAMBORONDON(Vlan)#vtp domain cisco

Asignar un dominio vtp al SAMBORONDON

SAMBORONDON(Vlan)#vtp server

Configurar de modo server el SAMBORONDON

SAMBORONDON(Vlan)#exit

Salir al modo de configuración global

Configuración de un enrutamiento entre distintas VLAN (Router SAMBORONDON)

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#interface FastEthernet 0/0.1

Ingresar a la sub-interfaz que se va a configurar

Router(config-subif)#encapsulation dot1q 1

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

Router(config-subif)#ip address 192.168.12.9 255.255.255.240

Asignar una dirección ip con su respectiva máscara

Router(config-subif)#exit

Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.2

Ingresar a la sub-interfaz que se va a configurar

Router(config-subif)#encapsulation dot1q 10

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

Router(config-subif)#ip address 192.168.12.33 255.255.255.224

Asignar una dirección ip con su respectiva máscara

Router(config-subif)#exit

Salir de la configuración de la sub-interfaz

Router(config)#exit

Salir del modo de configuración global

Router#copy runn-config startup-config

Guardar una copia de la configuración a la NVRAM

SAMBORONDONcon0 is now available
Press RETURN to get started.

BIENVENIDO AL SWITCH SAMBORONDON

User Access Verification

Password:
SAMBORONDON >enable
Password:

SAMBORONDON#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del switch
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
El servicio de encriptación de contraseña no esta activo
!
hostname SAMBORONDON
Nombre del switch
!
enable secret 5 1/GbR$LBaLnR1hq1.CeffXBwKw40
Indica que la contraseña de ingreso al switch se encuentra encriptada
!
!
!
!
ip subnet-zero
Sirve para utilizar la ip inicial al momento de subnetear
!
!
!
interface FastEthernet0/1
Puerto asignado a la Vlan Administración
!
interface FastEthernet0/2
switchport access vlan 10
Puerto asignado a la Vlan 10
!
interface FastEthernet0/3

switchport access vlan 10
Puerto asignado a la Vlan 10
!
interface FastEthernet0/4
Puerto sin configurar
!
interface FastEthernet0/5
Puerto sin configurar
!
interface FastEthernet0/6
Puerto sin configurar
!
interface FastEthernet0/7
Puerto sin configurar
!
interface FastEthernet0/8
Puerto sin configurar
!
interface FastEthernet0/9
Puerto sin configurar
!
interface FastEthernet0/10
Puerto sin configurar
!
interface FastEthernet0/11
Puerto sin configurar
!
interface FastEthernet0/12
Puerto sin configurar
!
interface FastEthernet0/13
Puerto sin configurar
!
interface FastEthernet0/14
Puerto sin configurar
¡
interface FastEthernet0/15
Puerto sin configurar
!
interface FastEthernet0/16
Puerto sin configurar
!
interface FastEthernet0/17
Puerto sin configurar
!
interface FastEthernet0/18
Puerto sin configurar
!

```
interface FastEthernet0/19
        Puerto sin configurar
!
interface FastEthernet0/20
        Puerto sin configurar
!
interface FastEthernet0/21
        Puerto sin configurar
!
interface FastEthernet0/22
        Puerto sin configurar
!
interface FastEthernet0/23
        Puerto sin configurar
!
interface FastEthernet0/24
        Puerto sin configurar
!
interface GigabitEthernet0/1
        Puerto que transmite a 10/100/1000, sin configurar
!
interface GigabitEthernet0/2
!
interface VLAN1
        Puerto 1 del switch, Vlan de administración o defecto por donde salen los
        demás puertos si no tuvieran ninguna Vlan asignada)

 ip address 192.168.12.2 255.255.255.0

        Dirección ip asignada a la Vlan por defecto del switch
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 192.168.12.1
        Dirección ip por la cual saldrán todos los puertos del switch hacia otras
        subredes
!
line con 0
        Contraseña para la línea de comandos
 password cisco
 login
line vty 0  15
        Contraseña para telnet
password cisco
 login
!
End
```

SAMBORONDON#show Vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/6, Fa0/7, Fa0/8,
                                                 Fa0/9, 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, Gi0/1, Gi0/2
```

Número de puertos asignados a la Vlan de administración

```
10   Edcom                             active    Fa0/2, Fa0/3
```

Puertos asignados y activos a la Vlan Edcom

```
1002 fddi-default                      active
```

Vlan para red fddi active

```
1003 token-ring-default                active
```

vlan para red token ring 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
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

5.9.1.17 CONFIGURACIÓN DEL SWITCH CENAIM

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

Acceso al modo de Configuración principal.

Switch>enable

Ingresar al modo EXEC privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch(config)#exit

Salir al modo de configuración global

Configuración de nombre del Switch CENAIM

CENAIM>enable

Ingresar al modo EXEC privilegiado

CENAIM#configure terminal
Ingresar al modo de configuración global
CENAIM(config)#hostname CENAIM
Sirve para asignarle un nombre al CENAIM (CENAIM)
CENAIM#

Configuración de Contraseñas

CENAIM#configure terminal
Ingresar al modo de configuración global
CENAIM(config)#line console 0
Ingresar a configurar la consola
CENAIM(config-line)#password <password>
Asignar una contraseña a la consola
CENAIM(config-line)#login
CENAIM(config-line)#exit
Salir de la configuración de la consola
CENAIM(config)#line vty 0 15
Ingresar a configurar la Terminal virtual
CENAIM(config-line)#password <password>
Asignar una contraseña a la Terminal virtual
CENAIM(config-line)#login
CENAIM(config-line)#exit
Salir de la configuración de la Terminal virtual
CENAIM(config)#enable password<password>
Agregar una contraseña para ingresar al router
CENAIM(config)#enable secret<password>
Agregar una contraseña encriptada para ingresar al router

Creación de VLAN's

CENAIM>enable
Ingresar al modo de configuración global
CENAIM#vlan database
Ingresar al modo de configuración de vlan's
CENAIM(Vlan)#Vlan 10 name Marítima
Asignar un número referencial y un nombre a la Vlan que se va a crear
CENAIM(Vlan)#exit
Salir del modo configuración de Vlan
CENAIM#

Asignación de VLAN's a los puertos

CENAIM>enable
Ingresar al modo EXEC privilegiado
CENAIM#configure terminal
Ingresar al modo de configuración global
CENAIM(config)#

CENAIM(config)#interface fastethernet 0/2

Ingresar a la interfaz puerto que se va a configurar

CENAIM(config-if)#switchport mode access

Ingresar al modo de configuración para asignar la Vlan

CENAIM(config-if)#switchport access vlan 10

Asignar el puerto a la Vlan 10

CENAIM(config-if)#exit

Asignar CENAIM de Tipo Server

CENAIM>enable

Ingresar al modo EXEC privilegiado

CENAIM#vlan database

Ingresar al modo de configuración de Vlan

CENAIM(Vlan)#vtp domain cisco

Asignar un dominio vtp al CENAIM

CENAIM(Vlan)#vtp server

Configurar de modo server el CENAIM

CENAIM(Vlan)#exit

Salir al modo de configuración global

Configuración de un enrutamiento entre distintas VLAN (Router CENAIM)

Router>enable

Ingresar al modo EXEC privilegiado

Router#configure terminal

Ingresar al modo de configuración global

Router(config)#interface FastEthernet 0/0.1

Ingresar a la sub-interfaz que se va a configurar

Router(config-subif)#encapsulation dot1q 1

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

Router(config-subif)#ip address 192.168.14.9 255.255.255.240

Asignar una dirección ip con su respectiva máscara

Router(config-subif)#exit

Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.2

Ingresar a la sub-interfaz que se va a configurar

Router(config-subif)#encapsulation dot1q 10

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

Router(config-subif)#ip address 192.168.12.33 255.255.255.224

Asignar una dirección ip con su respectiva máscara

Router(config-subif)#exit

Salir de la configuración de la sub-interfaz

Router(config)#exit

Salir del modo de configuración global

Router#copy runn-config startup-config

Guardar una copia de la configuración a la NVRAM

CENAIMcon0 is now available

Press RETURN to get started.

BIENVENIDO AL SWITCH CENAIM

User Access Verification

Password:
CENAIM >enable
Password:

CENAIM#show running-config
Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class.
Current configuration:
Configuración actual del switch
!
version 12.0
Versión del Sistema Operativo del switch
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
El servicio de encriptación de contraseña no esta activo
!
hostname CENAIM
Nombre del switch
!
enable secret 5 1/GbR$LBaLnR1hq1.CeffXBwKw40
Indica que la contraseña de ingreso al switch se encuentra encriptada
!
!
!
!
ip subnet-zero
Sirve para utilizar la ip inicial al momento de subnetear
!
!
!
interface FastEthernet0/1
Puerto asignado a la Vlan Administración
!
interface FastEthernet0/2
switchport access vlan 10
Puerto asignado a la Vlan 10
!
interface FastEthernet0/3

switchport access vlan 10
Puerto asignado a la Vlan 10
!
interface FastEthernet0/4
Puerto sin configurar
!
interface FastEthernet0/5
Puerto sin configurar
!
interface FastEthernet0/6
Puerto sin configurar
!
interface FastEthernet0/7
Puerto sin configurar
!
interface FastEthernet0/8
Puerto sin configurar
!
interface FastEthernet0/9
Puerto sin configurar
!
interface FastEthernet0/10
Puerto sin configurar
!
interface FastEthernet0/11
Puerto sin configurar
!
interface FastEthernet0/12
Puerto sin configurar
!
interface FastEthernet0/13
Puerto sin configurar
!
interface FastEthernet0/14
Puerto sin configurar
¡
interface FastEthernet0/15
Puerto sin configurar
!
interface FastEthernet0/16
Puerto sin configurar
!
interface FastEthernet0/17
Puerto sin configurar
!
interface FastEthernet0/18
Puerto sin configurar
!

```
interface FastEthernet0/19
        Puerto sin configurar
!
interface FastEthernet0/20
        Puerto sin configurar
!
interface FastEthernet0/21
        Puerto sin configurar
!
interface FastEthernet0/22
        Puerto sin configurar
!
interface FastEthernet0/23
        Puerto sin configurar
!
interface FastEthernet0/24
        Puerto sin configurar
!
interface GigabitEthernet0/1
        Puerto que transmite a 10/100/1000, sin configurar
!
interface GigabitEthernet0/2
!
interface VLAN1
        Puerto 1 del switch, Vlan de administración o defecto por donde salen los
        demás puertos si no tuvieran ninguna Vlan asignada)

 ip address 192.168.14.2 255.255.255.0

        Dirección ip asignada a la Vlan por defecto del switch
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 192.168.14.1
        Dirección ip por la cual saldrán todos los puertos del switch hacia otras
        subredes
!
line con 0
        Contraseña para la línea de comandos
 password cisco
 login
line vty 0  15
        Contraseña para telnet
password cisco
 login
!
End
```

CENAIM#show Vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/6, Fa0/7, Fa0/8,
                                                 Fa0/9, 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, Gi0/1, Gi0/2
```

Número de puertos asignados a la Vlan de administración

```
10   Marítima                          active    Fa0/2, Fa0/3
```

Puertos asignados y activos a la Vlan Marítima

```
1002 fddi-default                      active
```

Vlan para red fddi active

```
1003 token-ring-default                active
```

vlan para red token ring 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
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

5.9.1.18 CONFIGURACIÓN DEL SWITCH PROSPERINA

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

Acceso al modo de Configuración principal.

Switch>enable

Ingresar al modo EXEC privilegiado

Switch#configure terminal

Ingresar al modo de configuración global

Switch(config)#exit

Salir al modo de configuración global

Configuración de nombre del Switch PROSPERINA

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

Configuración de Contraseñas

PROSPERINA#configure terminal
Ingresar al modo de configuración global
PROSPERINA(config)#line console 0
Ingresar a configurar la consola
PROSPERINA(config-line)#password <password>
Asignar una contraseña a la consola
PROSPERINA(config-line)#login
PROSPERINA(config-line)#exit
Salir de la configuración de la consola
PROSPERINA(config)#line vty 0 15
Ingresar a configurar la Terminal virtual
PROSPERINA(config-line)#password <password>
Asignar una contraseña a la Terminal virtual
PROSPERINA(config-line)#login
PROSPERINA(config-line)#exit
Salir de la configuración de la Terminal virtual
PROSPERINA(config)#enable password<password>
Agregar una contraseña para ingresar al router
PROSPERINA(config)#enable secret<password>
Agregar una contraseña encriptada para ingresar al router

Creación de VLAN's

PROSPERINA>enable
Ingresar al modo de configuración global
PROSPERINA#vlan database
Ingresar al modo de configuración de vlan's
PROSPERINA(Vlan)#Vlan 10 name Biblioteca
Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#Vlan 20 name Marítima
Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#Vlan 30 name C_Tierra
Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#Vlan 40 name Rectorado
Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#Vlan 50 name FIEC
Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#Vlan 60 name Básico
Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#Vlan 70 name Tecnologías
Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#Vlan 80 name ICHE

Asignar un número referencial y un nombre a la Vlan que se va a crear
PROSPERINA(Vlan)#exit
Salir del modo configuración de Vlan
PROSPERINA#

Asignación de VLAN's a los puertos

PROSPERINA>enable
Ingresar al modo EXEC privilegiado
PROSPERINA#configure terminal
Ingresar al modo de configuración global
PROSPERINA(config)#
PROSPERINA(config)#interface fastethernet 0/2
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access Vlan 10
Asignar el puerto a la Vlan 10
PROSPERINA(config-if)#exit
Salir al modo de configuración de la interfaz
PROSPERINA(config)#interface fastethernet 0/3
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access Vlan 20
Asignar el puerto a la Vlan 20
PROSPERINA(config-if)#exit
Salir al modo de configuración de la interfaz

PROSPERINA(config)#interface fastethernet 0/4
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access Vlan 30
Asignar el puerto a la Vlan 30
PROSPERINA(config-if)#exit
Salir al modo de configuración de la interfaz

PROSPERINA(config)#interface fastethernet 0/5
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access Vlan 40
Asignar el puerto a la Vlan 40
PROSPERINA(config-if)#exit
Salir al modo de configuración de la interfaz

PROSPERINA(config)#interface fastethernet 0/6
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access Vlan 50
Asignar el puerto a la Vlan 50
PROSPERINA(config-if)#exit

Salir al modo de configuración de la interfaz

PROSPERINA(config)#interface fastethernet 0/7
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access Vlan 60
Asignar el puerto a la Vlan 60
PROSPERINA(config-if)#exit
Salir al modo de configuración de la interfaz

PROSPERINA(config)#interface fastethernet 0/8
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access vlan 70
Asignar el puerto a la Vlan 70
PROSPERINA(config-if)#exit
Salir al modo de configuración de la interfaz

PROSPERINA(config)#interface fastethernet 0/9
Ingresar a la sub- interfaz o puerto que se va a configurar
PROSPERINA(config-if)#switchport mode access
Ingresar al modo de configuración para asignar la Vlan
PROSPERINA(config-if)#switchport access vlan 80
Asignar el puerto a la Vlan 80
PROSPERINA(config-if)#exit
Salir al modo de configuración de la interfaz

Asignar PROSPERINA de Tipo Server

PROSPERINA>enable
Ingresar al modo EXEC privilegiado
PROSPERINA#vlan database
Ingresar al modo de configuración de Vlan
PROSPERINA(Vlan)#vtp domain cisco
Asignar un dominio vtp al PROSPERINA
PROSPERINA(Vlan)#vtp server
Configurar de modo server el PROSPERINA
PROSPERINA(Vlan)#exit
Salir al modo de configuración global

Configuración de un enrutamiento entre distintas VLAN (Router PROSPERINA1)

Router>enable
Ingresar al modo EXEC privilegiado
Router#configure terminal
Ingresar al modo de configuración global
Router(config)#interface FastEthernet 0/0.1
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 1
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.1.33 255.255.255.224
Asignar una dirección ip con su respectiva máscara

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

Router(config)#interface FastEthernet 0/0.2
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 10
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 10
Router(config-subif)#ip address 192.168.1.65 255.255.255.192
Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.3
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 20
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.1.128 255.255.255.128

Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.4
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 30
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.2.1 255.255.255.128

Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.5
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 40
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.2.130 255.255.255.128

Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.6
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 50
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.3.1 255.255.255.0

Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit

Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.7
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 60
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.4.1 255.255.255.0

Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.8
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 70
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.5.0 255.255.255.0

Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#interface FastEthernet 0/0.9
Ingresar a la sub-interfaz que se va a configurar
Router(config-subif)#encapsulation dot1q 80
Asignar el tipo de encapsulamiento a utilizar asociado a la Vlan 1
Router(config-subif)#ip address 192.168.6.1 255.255.255.0

Asignar una dirección ip con su respectiva máscara
Router(config-subif)#exit
Salir de la configuración de la sub-interfaz

Router(config)#exit
Salir del modo de configuración global
Router#copy runn-config startup-config
Guardar una copia de la configuración a la NVRAM

PROSPERINAcon0 is now available
Press RETURN to get started.

BIENVENIDO AL SWITCH PROSPERINA

User Access Verification

Password:
PROSPERINA >enable
Password:

PROSPERINA#show running-config

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

Current configuration:

Configuración actual del switch

!

version 12.0

Versión del Sistema Operativo del switch

no service pad

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

El servicio de encriptación de contraseña no esta activo

!

hostname PROSPERINA

Nombre del switch

!

enable secret 5 1/GbR$LBaLnR1hq1.CeffXBwKw40

Indica que la contraseña de ingreso al switch se encuentra encriptada

!

!

!

!

ip subnet-zero

Sirve para utilizar la ip inicial al momento de subnetear

!

!

!

interface FastEthernet0/1

Puerto asignado a la Vlan Administración

!

interface FastEthernet0/2

switchport access vlan 10

Puerto asignado a la Vlan 10

!

interface FastEthernet0/3

switchport access vlan 20

Puerto asignado a la Vlan 20

!

interface FastEthernet0/4

switchport access vlan 30

Puerto asignado a la Vlan 30

!

interface FastEthernet0/5

switchport access vlan 40

Puerto asignado a la Vlan 40

!

interface FastEthernet0/6

switchport access vlan 50

```
        Puerto asignado a la Vlan 50
!
interface FastEthernet0/7
        switchport access vlan 60
        Puerto asignado a la Vlan 60
!
interface FastEthernet0/8
        switchport access vlan 70
        Puerto asignado a la Vlan 70
!
interface FastEthernet0/9
        switchport access vlan 80
        Puerto asignado a la Vlan 80
!
interface FastEthernet0/10
        Puerto sin configurar
!
interface FastEthernet0/11
        Puerto sin configurar
!
interface FastEthernet0/12
        Puerto sin configurar
!
interface FastEthernet0/13
        Puerto sin configurar
!
interface FastEthernet0/14
        Puerto sin configurar
¡
interface FastEthernet0/15
        Puerto sin configurar
!
interface FastEthernet0/16
        Puerto sin configurar
!

interface FastEthernet0/17
        Puerto sin configurar
!
interface FastEthernet0/18
        Puerto sin configurar
!
interface FastEthernet0/19
        Puerto sin configurar
!
interface FastEthernet0/20
        Puerto sin configurar
!
```

interface FastEthernet0/21
Puerto sin configurar
!
interface FastEthernet0/22
Puerto sin configurar
!
interface FastEthernet0/23
Puerto sin configurar
!
interface FastEthernet0/24
Puerto sin configurar
!
interface GigabitEthernet0/1
Puerto que transmite a 10/100/1000, sin configurar
!
interface GigabitEthernet0/2
!
interface VLAN1
Puerto 1 del switch, Vlan de administración o defecto por donde salen los demás puertos si no tuvieran ninguna Vlan asignada

ip address 192.168.1.34 255.255.255.0

Dirección ip asignada a la Vlan por defecto del switch
no ip directed-broadcast
no ip route-cache
!
ip default-gateway 192.168.1.33
Dirección ip por la cual saldrán todos los puertos del switch hacia otras subredes
!
line con 0
Contraseña para la línea de comandos
password cisco
login
line vty 0 15
Contraseña para telnet
password cisco
login
!
End

PROSPERINA#show Vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, 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, Gi0/1, Gi0/2
Número de puertos asignados a la Vlan de administración

10 Biblioteca active Fa0/2
Puerto asignado y activo a la Vlan Biblioteca
20 Marítima active Fa0/3
Puerto asignado y activo a la Vlan Marítima

30 C_Tierra active Fa0/4
Puerto asignado y activo a la Vlan C_Tierra

40 Rectorado active Fa0/5
Puerto asignado y activo a la Vlan Rectorado

50 FIEC active Fa0/6
Puerto asignado y activo a la Vlan FIEC

60 Básico active Fa0/7
Puerto asignado y activo a la Vlan Básico

70 Tecnologías active Fa0/8
Puerto asignado y activo a la Vlan Tecnología

80 ICHE active Fa0/9
Puerto asignado y activo a la Vlan ICHE

1002 fddi-default active
Vlan para red fddi active
1003 token-ring-default active
Vlan para red token ring 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
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

CAPÍTULO 6

CONFIGURACIÓN DE LINUX

6. CONFIGURACIÓN DE LINUX

6.1 SAMBA

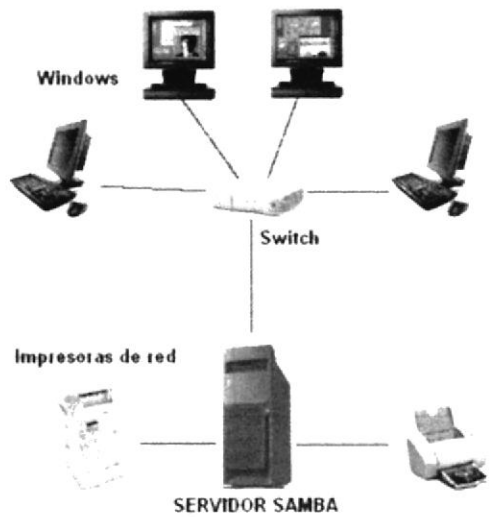


Figura 6.1 Como funciona SAMBA

SMB (acrónimo de Server Message Block). La interconectividad entre un equipo con Linux instalado y el resto de los equipos en red en una oficina con alguna versión de Windows es importante, ya que esto permitirá compartir archivos e impresoras. Esta interconectividad se consigue exitosamente a través de SAMBA.

6.1.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- No tener habilitado el firewall de Linux.
- Haber instalado el paquete samba el cual se verifica con el comando **rpm –q samba.**

6.1.2 CONFIGURACIÓN

1. Verificar si el paquete de samba esta instalado, caso contrario digitar el comando setup y elija la opción Servicios del Sistema y habilitar network, smb.
   rpm –q samba

   A continuación están las tres opciones a seguir:
   1. Utilizar el comando ifconfig,
      ```
      Ifconfig eth0 192.168.17.1 netmask 255.255.255.248 up
      ```
   2. Utilizar el comando netconfig que sería en interfaz gráfica

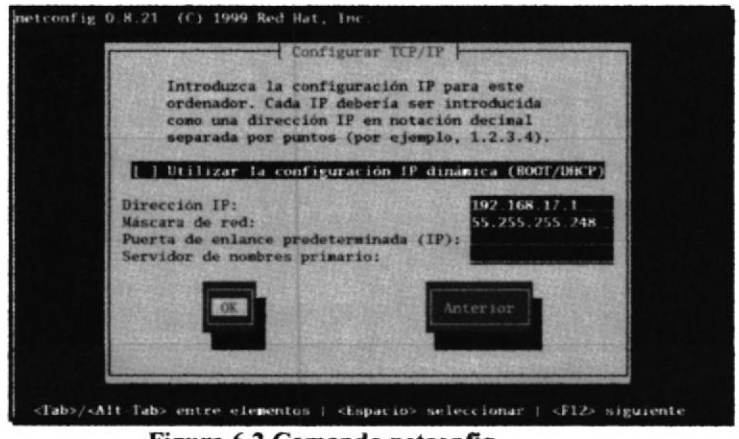


Figura 6.2 Comando netconfig

3. Configurar al archivo ifcfg-eth0 para cambiar la ip
   `vi /etc/sysconfig/network-scripts/ifcfg-eth0`
   Salir guardando los cambios con: wq.

4. Levantar los servicios de la network.
   `Service network start`

5. Si hay un tipo de error se digita lo siguiente:
   `Service network restart`

2. Configurar el archivo smb.conf.
   `vi /etc/samba/smb.conf`

   En las secciones del smb.conf

   Las secciones GLOBAL, SHARE, PRINTER son parecidas a las secciones existentes en el fichero `/etc/smb.conf`, que se presenta como un fichero .ini habitual del mundo Windows.

   Global Settings

   La sección GLOBAL contiene variables generales que se aplican al total de los recursos puestos a disposición del servidor de SMB. Esta sección contiene también información de identificación del servidor dentro de la red NetBIOS: grupo de trabajo, nombre e identificador. Esta sección contiene también los modos de funcionamiento de Samba.

6.1.3 CONFIGURACIÓN DE LOS PARÁMETROS GLOBALES

Identificar el servidor
Primero hay que elegir algunos parámetros de funcionamiento del servidor, para que se integre bien en la red.

El campo **workgroup**, permite elegir el grupo de trabajo del que el servidor Samba hace parte.

```
workgroup = ESPOL (Grupo de trabajo)
```

El campo **netbios name**, permite definir el nombre de la máquina, no como un nombre de DNS, sino como un nombre de resolución de nombres propio del protocolo NetBIOS.

```
netbios name = LINUX SERVER (Descripción del servidor)
```

Los menús **hosts allow** y **host deny** permiten controlar el acceso a los recursos de ciertas máquinas.

```
host allow = [registrar las ip de las pc]
```

El campo **server string**, permite elegir la descripción que acompaña al nombre del servidor en la lista de recursos anunciados.

El campo **interfaces** permite identificar la o las tarjetas de red que enlazan el servidor con el grupo de trabajo.

Share Definitions

La sección SHARE contiene la lista de particiones de disco efectuadas por la máquina. Se aconseja primero crear la partición compartida y después precisar para cada partición sus propiedades particulares.

```
[home]
   coment = Home Directories**
   browseable = no
   writable = yes
   path = /nombre_carpeta (adicionar)
```

El campo **coment indica un comentario del recurso.

El campo **browseable** indica que este recurso debe ser anunciado por nmbd, y por tanto ser visible para todos los usuarios.

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

El campo **valid users** limita el acceso a ciertos usuarios, ya que para cada recurso es posible restringir el acceso a ciertos usuarios. Para cada una de las líneas de recursos compartidos en /etc/smb.conf, se podrá añadir la línea:

```
valid users = usuario1, usuario2
```

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

- Salir con :wq para guardar los cambios.

3. Crear el directorio que contendrá los archivos a compartir.

```
mkdir <nombre_directorio>
```

4. Ingresar al directorio.
```
cd <nombre _directorio>
```

5. Crear un archivo de texto para la verificar su funcionamiento.
```
touch nombre.txt
```

6. Dar todos los permisos para el archivo a compartir.
```
chmod +777 nombre.txt
```

7. Dar todos los permisos para el directorio a compartir.
```
chmod +777 <nombre _directorio>
```

8. Salir al directorio raíz.
```
cd /
```

9. Crear los usuarios que anteriormente se registraron en valid user.
```
adduser usuario
```

10. Crear las contraseñas para el usuario.
```
passwd usuario
```

11. Asignar una contraseña para los usuarios para hacer uso del servicio de samba
```
smb passwd -a usuario
```

12. Iniciar los servicios de samba, xinetd y network.
```
service smb start
service xinetd start
service network start
```

6.1.4 CONFIGURACIÓN EN WINDOWS

Pasos a seguir en la estación de trabajo con sistema operativo windows:

1. Acceder a la máquina Linux por dirección ip.

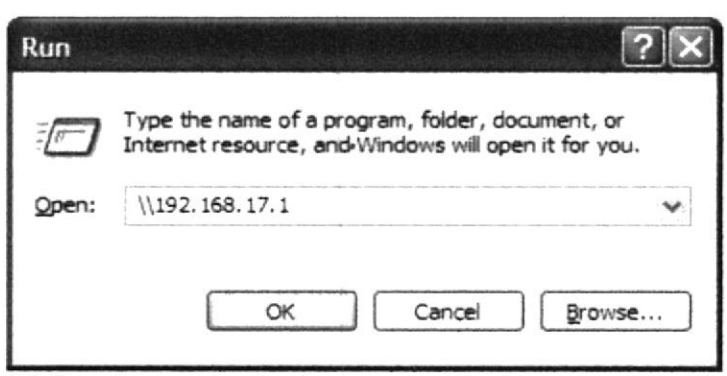


Figura 6.3 Con el comando ejecutar ir a una máquina por su dirección ip

2. Ingresar nuestro usuario samba con su clave

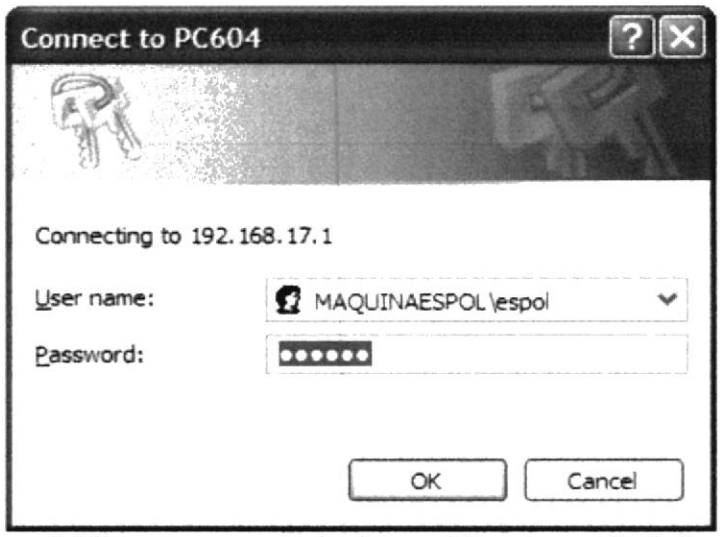


Figura 6.4 Conectarse a una máquina con Linux por medio de Samba

3. Ingresar a recursos compartidos en el servidor Samba Linux

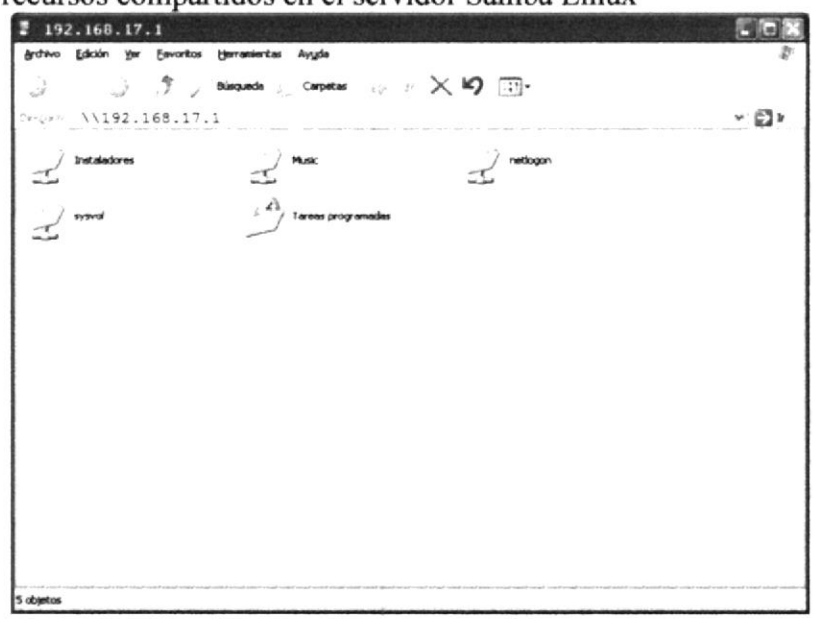


Figura 6.5 Visualización de una máquina con Linux con el servicio samba

6.2 DNS

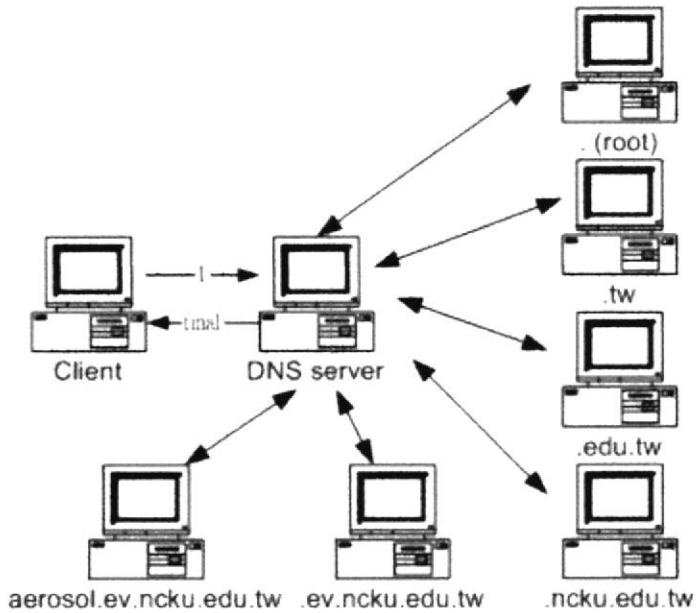


Figura 6.6 Como funciona DNS

Un **DNS** (Domain Name Server) es un conjunto de protocolos y servicios (base de datos distribuida) que permiten a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP. Por ejemplo, si la dirección IP del sitio FTP de proxy es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.ve y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente los DNS nacieron de la necesidad de recordar fácilmente los sitios visitados o a visitar y sustituir el antiguo sistema de identificación de "host" en internet que consistía en un gran archivo donde estaban almacenados los nombres y las direcciones ips de cada nodo de la red con el cual se podía establecer comunicación.

6.2.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Tener deshabilitado el firewall.
- Haber instalado el paquete bind el cual se verifica con el comando **rpm –q bind.**

6.2.2 CONFIGURACIÓN

1. Verificar la instalación del paquete del DNS.
   rpm –qa bind

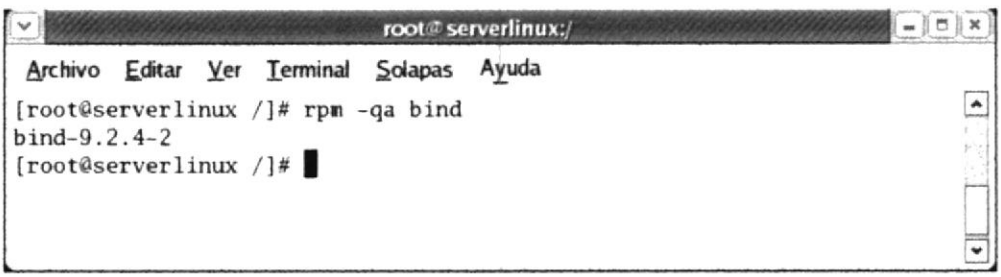


Figure 6.7 Verificar si el servicio de DNS está habilitado

2. Configurar el archivo named.conf.
   vi /etc/ named.conf
   Realizar los siguientes pasos:
   - Copiar estas líneas
   en zone "localhost" IN {
   type master;
   file "nombre.zone";
   allow-update {nome};
   };

   - Realizar los siguientes cambios
   en zone "espol.com"{
   type master; ***
   notify no; **
   file "espol.com"; *
   allow-update{none};
   };

Figure 6.8 Cambios en el archivo espol.com

***Los parámetros en esta sección como **type**, indican si se tratará de un servidor principal (master) o secundario (slave) de la zona.

Agregar el parámetro **notify para que se notifiquen los cambios a los servidores secundarios.

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

- Salir con :wq para guardar los cambios.

3. Ingresar a la ruta
   cd /var/named/chroot/var/named/

4. Listar el contenido con el comando **ls** y debe aparecer localhost.zone

5. Realizar una copia del contenido del archivo localhost.zone al espol.com.
   cp localhost.zone espol.com

6. Editar el archive espol.com
   `vi espol.com`

   Realizar los siguientes cambios.

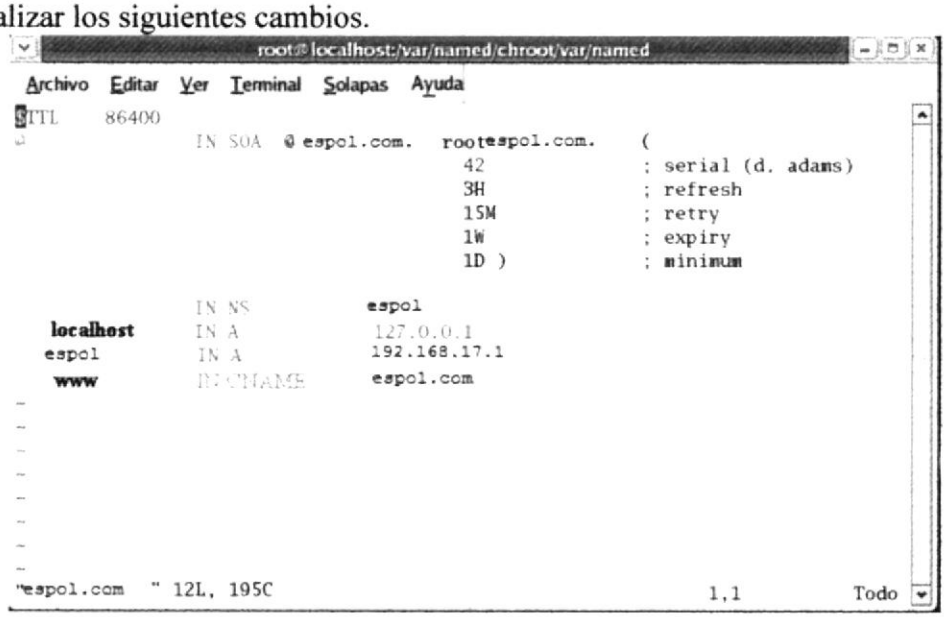


Figure 6.9 Edición del comando espol.com

Registros de recursos

A especifica la dirección real IP
NS apunta a una posición específica del servidor de nombres
CNAME el nombre canónico para un alias
SOA marca el principio de la zona de autoridad (dominio, dirección del responsable de zona, Número de serie.....)

@ Al principio de línea de los archivos de zona indica que no se necesita nombre.

7. Iniciar los servicios del bind.

```
service named start
```

8. Para cambiar la configuración del servidor dns local en Linux se debe ingresar al archivo resolv.conf.
```
vi /etc/ resolv.conf
```

9. Hacer ping a la dirección ip del servidor y también a la dirección DNS que se ha creado, cualquiera de las 3 siguientes líneas puede ser utilizada.
```
ping 192.168.17.1
ping www.espol.com
ping espol.com
```

   Si da respuesta es porque su configuración esta bien realizada.

6.2.3 CONFIGURACIÓN EN WINDOWS

Agregar a la configuración de la tarjeta de red la dirección ip del servidor DNS.

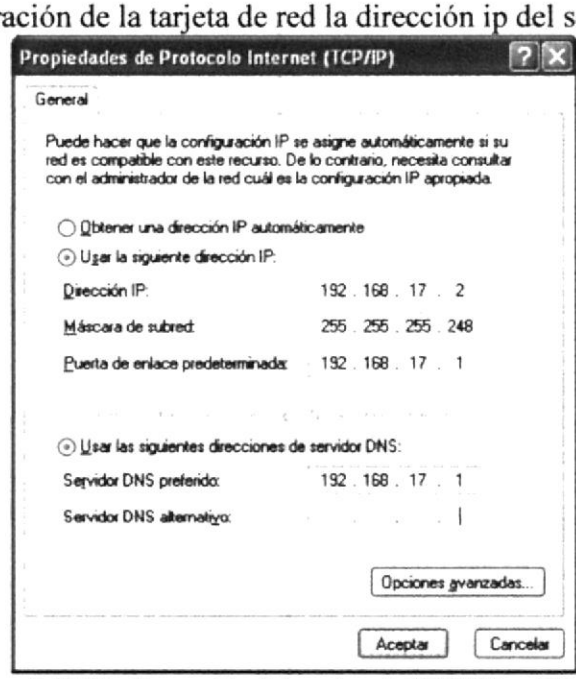


Figura 6.10 Configuración del protocolo TCP/IP en Windows

Una vez que se ha asignado la dirección ip en la máquina de Windows, se podrá hacer ping a la dirección ip del servidor y también a la dirección creada www.espol.com

6.3 WEB SERVER

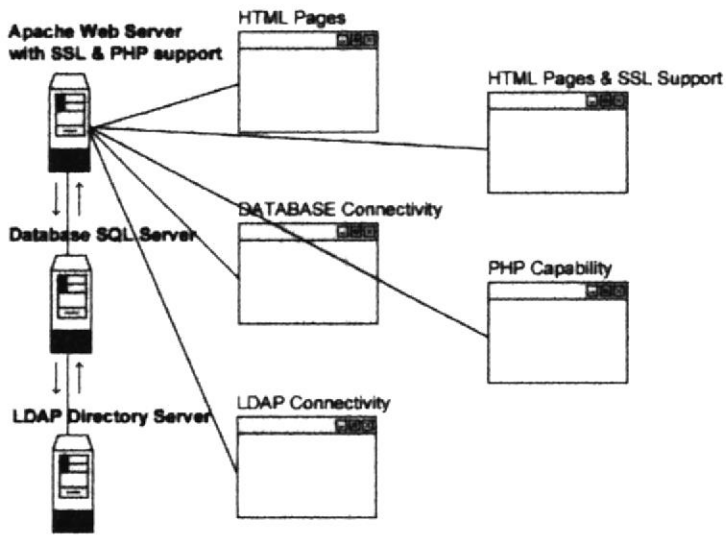


Figura 6.11 Como funciona Web Server

Usted podrá disponer de su página o páginas web sin limitación de dominios, ni espacio en disco duro, sin límite de transferencia, y con todos los dominios hospedados y redirigidos que desee.

6.3.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Tener deshabilitado el firewall.
- Haber instalado el paquete httpd el cual se verifica con el comando **rpm –q httpd**
- Tener levantado el servidor DNS

6.3.2 CONFIGURACIÓN

1. Verificar la instalación del paquete de web server
   `rpm -qa httpd`

2. Configurar al archivo httpd.conf que se encuentra en la siguiente ruta
   `vi /etc/httpd/conf/httpd.conf`

3. Buscar las siguientes líneas y descomentarlas.

   `Listen 80`

   Permite habilitar el puerto 80 que es el que se encarga de todo lo que se refiere al servicio httpd.

   `DocumentRoot "/var/www/html"`

Permite indicar la ruta donde se cargará la página web a utilizar..

```
Directory Index index.html index.doc
```

Indica como se llama el archivo principal para cargar la página web.

```
NameVirtualHost *:80
```

Indica el puerto que debe escuchar como una máquina virtual.

En el parámetro **directory index** se agrega el nombre y la extensión del archivo que se va a crear en el caso que no se encuentra especificado

4. Copiar el párrafo del <virtual host *:80> -- <virtual host >, descomentar las líneas necesarias y realizar los siguientes cambios:

```
<virtual host * :80>
   server admin        root@ localhost.localdomain
   document root      /var/www/html/sitio_espol
   server name www.espol.com
</virtual host>
```

5. Ingresar a la ruta especificada en el document root.
   `cd /var/www/html/`

6. Digitando el comando ls, verificar las carpetas que han sido creadas

7. Crear la carpeta donde será ubicada la página.
   `mkdir  sitio_espol`

8. Ingresar a la carpeta
   `cd sitio_espol`

9. Crear un archivo con extensión html para verificar funcionamiento.
   `vi index.html`

10. Iniciar los servicios del httpd
    `service httpd start`

6.3.3 CONFIGURACIÓN EN WINDOWS

Ingresar al explorador de Windows, menú Herramientas y elegir Opciones de Internet.

Figura 6.12 Acceso a la configuración de la página web por medio de Windows XP

Dentro de opciones de Internet escoger la pestaña Conexiones, configuración de la red LAN.

Figura 6.13 Pestaña Conexiones del Internet Explorer

Colocar la dirección del servidor y el puerto de comunicación en este caso para Web Server es el 80.

Figura 6.14 Configuración del servidor Proxy para acceder a la página creada

Acceder al sitio web mediante nuestro navegador. Recordar que se debe haber asignado la dirección DNS en nuestra máquina Windows.

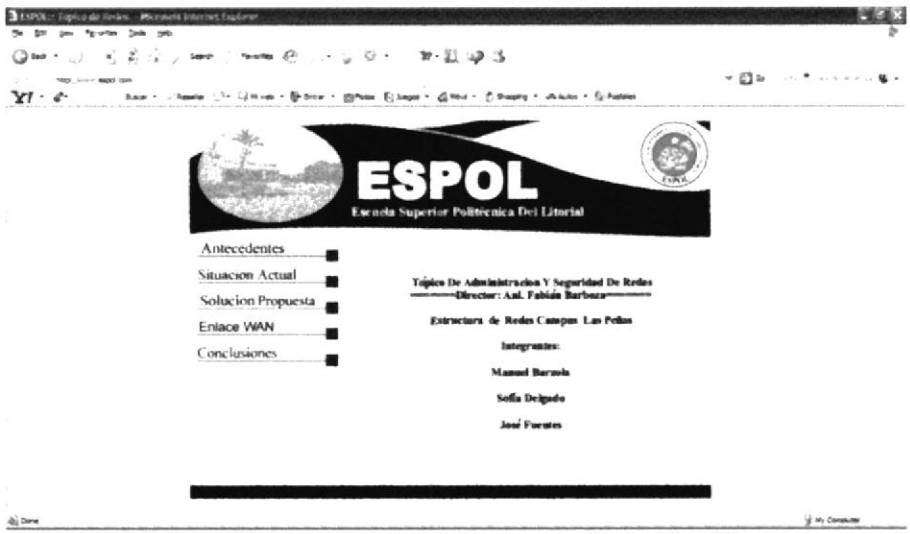


Figura 6.15 Acceso a una página por medio de Web Server

6.4 SERVIDOR DE CORREO

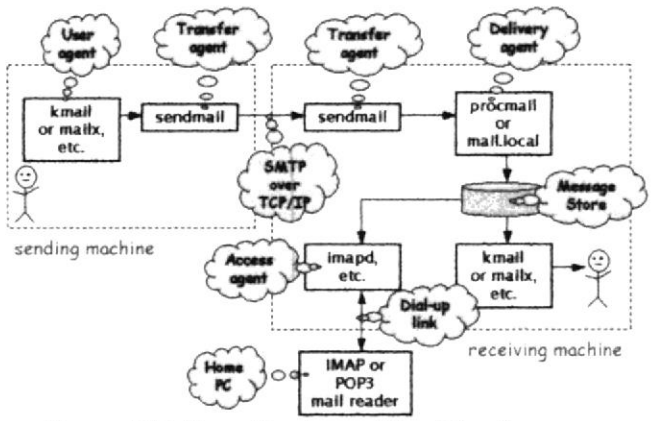


Figura 6.16 Como funciona el Servidor de correo

Mail Server es un servidor de mail que trabaja con los servicios dovecot y sendmail, con los protocolos POP3 y SMTP que utilizan los puertos 110 y 25 respectivamente, que soporta un número ilimitado casillas de mail, y listas de correo.

Sendmail es el agente de transporte de correo más común de Internet en los sistemas Linux. Aunque actúa principalmente como MTA (Mail Transport Agent), que son los encargados de transferir los mail a su correcto destino.

Un servidor de correo es una aplicación que permite enviar mensajes de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

SMTP, Simple Mail Transfer Protocol: Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

POP, Post Office Protocol: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

IMAP, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario (como el caso de Mozilla Mail, Evolution, Microsoft Outlook). Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario.

6.4.1 REQUERIMIENTOS

- Tener una PC instalado el sistema operativo Linux Fedora Core 3, con su respectiva tarjeta de red.
- Tener deshabilitado el firewall.
- Haber instalado el paquete sendmail el cual se verifica con el comando **rpm –q sendmail.**
- Haber instalado el paquete dovecot el cual se verifica con el comando **rpm –q dovecot.**

6.4.2 CONFIGURACIÓN

1. Configurar tarjeta de red.
   Ejm: `ifconfig eth0 192.168.17.1 mask 255.255.255.0 up`
   O también se puede utilizar el comando Netconfig

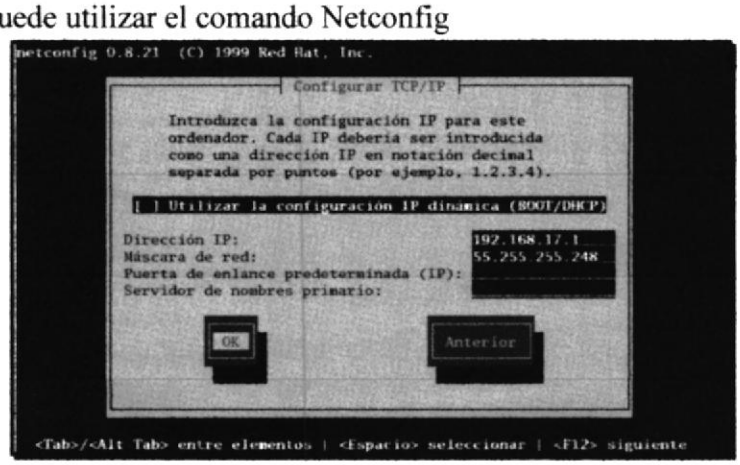


Figure 6.17 Comando netconfig

2. Comprobar si esta instalado el servicio sendmail y dovecot, si no instalarlo.
   `rpm -qa sendmail`
   `rpm -qa dovecot`

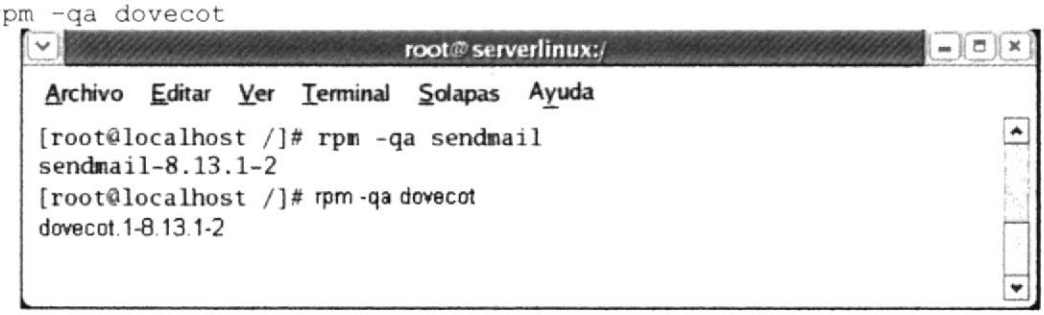


Figure 6.18 Comprobar servicios sendmail y dovecot

3. Configurar archivo del servicio Sendmail
   `vi /etc/mail/sendmail.cf`

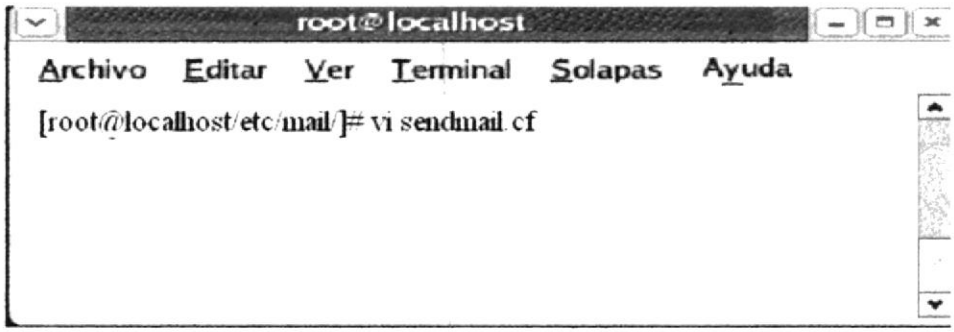


Figure 6.19 Ejecutar el comando vi sendmail.cf

Agregar los parámetros y salir con **:wq** para guardar los cambios.

- En `Cwlocalhost` cambiar por `Cwespol.com`
- `# SMTP daemon options`
  `O DaemonPortOptions=Port=smtp,Addr=0.0.0.0, Name=MTA`
- `# SMTP client options`
  `O ClientPortOptions=Family=inet,Addr=0.0.0.0`

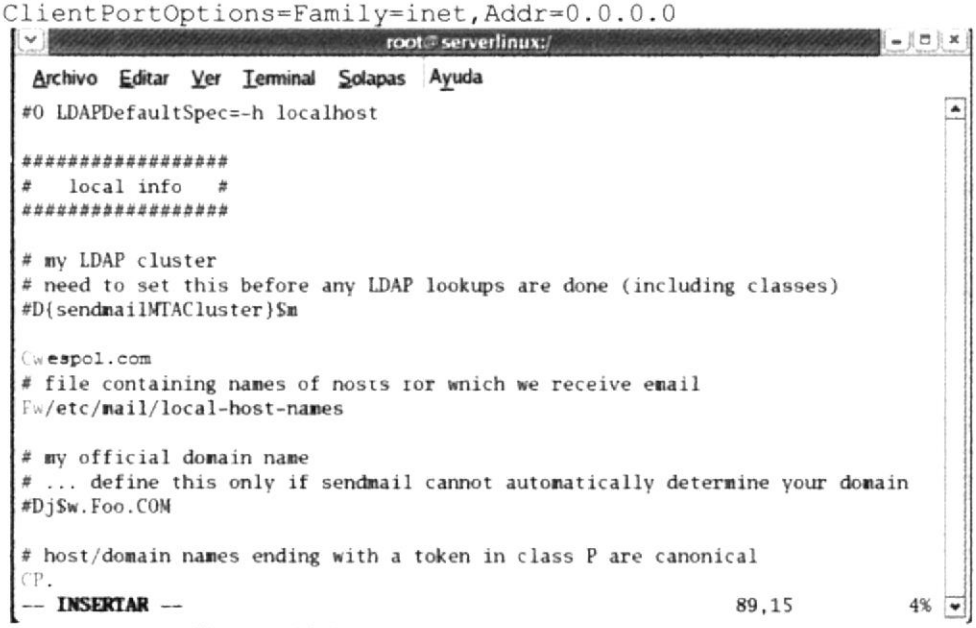


Figure 6.20 Edición del comando sendmail.cf

4. Configurar archivo del servicio Dovecot
   `vi /etc/dovecot.conf`

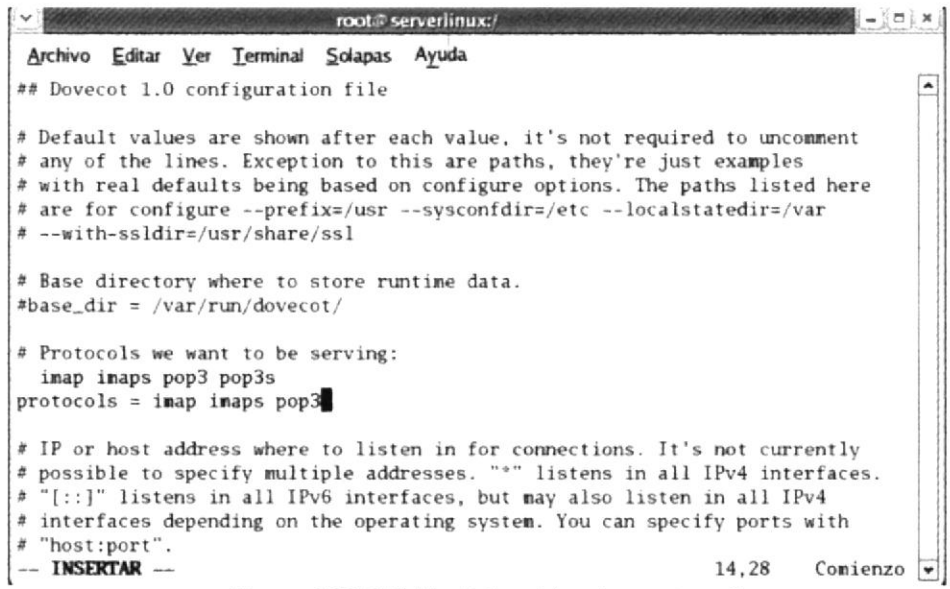


Figure 6.21 Edición del archivo dovecot.conf

Descomentar la línea, agregar los parámetros y salir con :wq para guardar los cambios.

```
protocols = imap imaps pop3
```

5. Iniciar servicios.

```
service sendmail restart
service dovecot restart
```

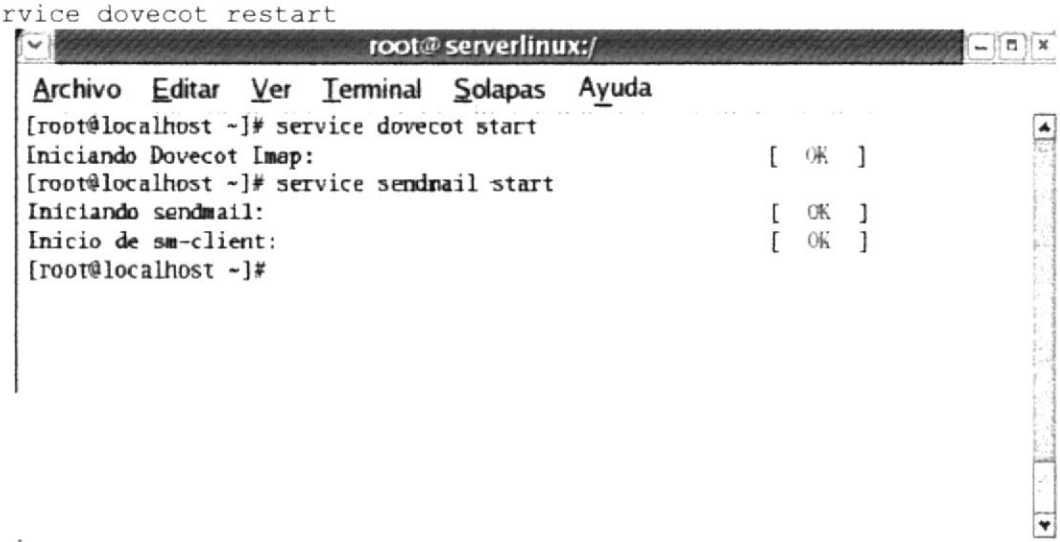


Figure 6.22 Ejecución del comando service dovecot y sendmail restart

6. Comprobar los puertos abiertos

```
netstat -an | more, o netstat -plan | more
```

Deben estar escuchando los puertos 25 (SMTP) y el 110 (POP3)

7. Configurar el archivo network

```
vi /etc/sysconfig/network

NETWORKING=yes
HOSTNAME=espol.com (mismo de Cw)
```

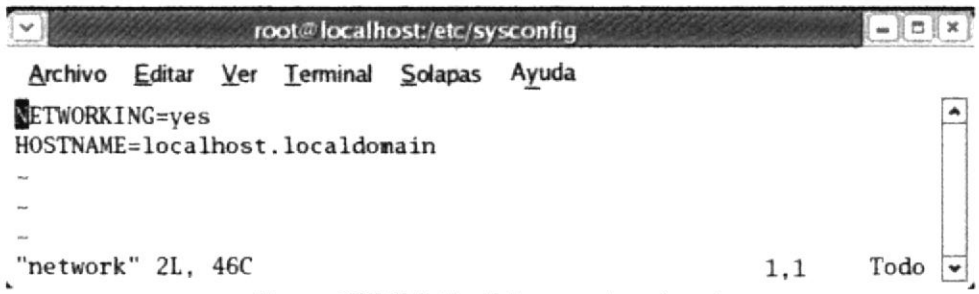


Figure 6.23 Edición del comando network

8. Iniciar el servicio del network
   ```
   service network start
   ```

9. Reiniciar el equipo

10. Configurar los clientes

NOTA:

- Para verificar se envía un mail al root
  ```
  [root@localhost~]# mail root@espol.com
  Subject: nombre_usuario
  ```
  Finalizar el mensaje con punto
  ```
  .
  cc:/nombre_usuario2
  ```

- Para verificar un mail desde el usuario administrador
  ```
  [root@localhost~]# su -
  [root@localhost/root]# mail
  ```

- Para verificar correos de otros usuarios
  ```
  [root@localhost/sofia]# mail -u sofia
  ```

- Para cambiar de usuario
  ```
  [root@localhost/sofia]# su - jose
  [root@localhost/jose]# su - regresa al root pidiendo clave.
  ```

6.4.3 CONFIGURACIÓN EN WINDOWS

Pasos a seguir en la estación de trabajo con sistema operativo windows:

1. Proceder a configurar el Outlook Express, dando clic en inicio y elegir la opción de correo electrónico (Outlook Express) dentro del menú inicio de Windows XP

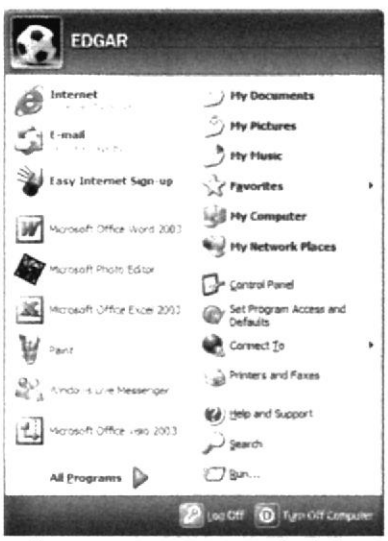


Figura 6.24 Cómo acceder a programa que administra el correo electrónico

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

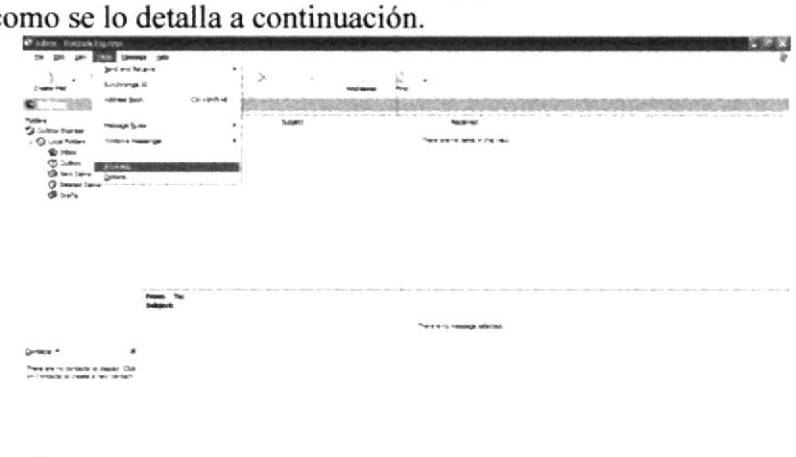


Figura 6.25 Como ingresar para configurar una cuenta de correo electrónico mediante Outlook Express

3. Aparecerá la siguiente pantalla a manera de un asistente para poder configurar la nueva cuenta de correo electrónico, en la cual se dará clic en agregar y posteriormente elegir la opción correo.

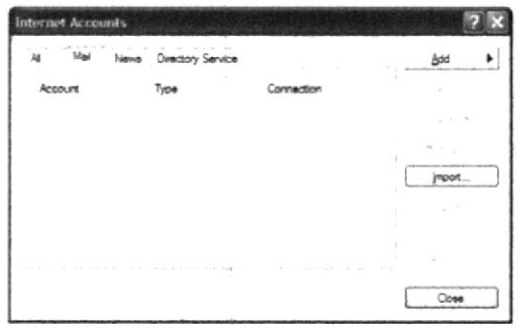


Figura 6.26 Pestaña Mail para configurar una cuenta de correo electrónico

4. Después Ingresar en Agregar nueva cuenta de correo electrónico la misma que indicará que nombre desea que aparezca en la cuenta de correo, luego se irá a la siguiente pantalla dando clic en siguiente

Figura 6.27 Primera pantalla de configuración de una cuenta de correo electrónico

5. Se colocará nuestra dirección de correo asociado al usuario que creamos en Linux, clic en siguiente.

Figura 6.28 Segunda pantalla de configuración de una cuenta de correo electrónico

6. Se especifica el servidor de correo entrante (POP3) y el servidor de correo saliente (SMTP), en este caso los dos son la misma dirección del servidor Linux, luego clic en siguiente

Figura 6.29 Tercera pantalla de configuración de una cuenta de correo electrónico

7. Ingresar el nombre de usuario y contraseña proporcionado por el servidor Linux, clic en siguiente

Figura 6.30 Cuarta pantalla de configuración de una cuenta de correo electrónico

8. Clic en finalizar para verificar que la información escrita anteriormente esta correcta.

Figura 6.31 Pantalla de finalización de configuración de una cuenta de correo electrónico

9. Terminada la configuración se visualizará una pantalla con las cuentas de correo que existen, a la vez la cuenta que esta como predeterminada en este caso 192.168.17.1 .

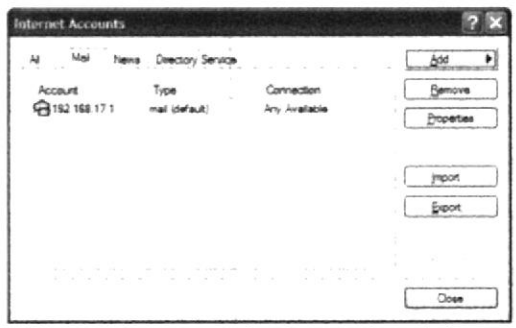


Figura 6.32 Listado de cuentas de correo electrónico configuradas

10. Ahora podrá enviar y recibir mensajes de correos de los usuarios creados en nuestro servidor Linux.

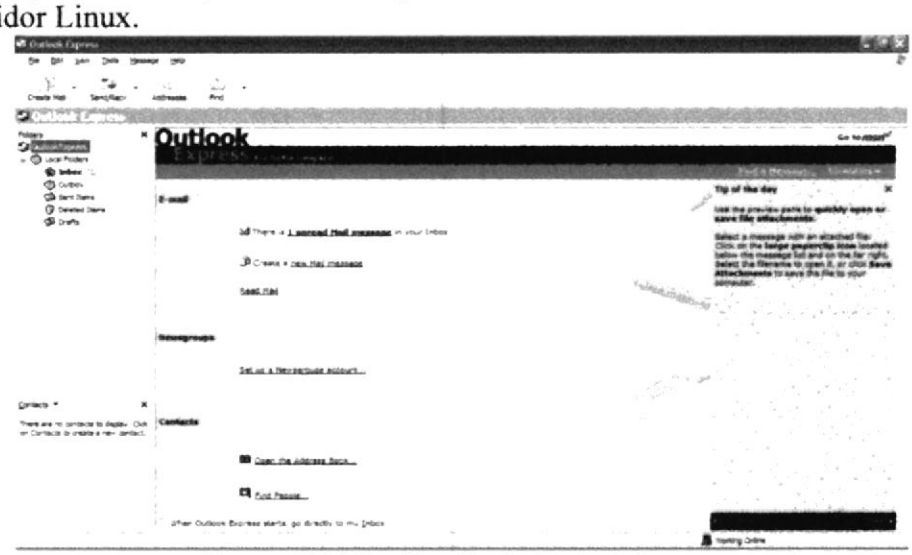


Figura 6.33 Visualización de Outlook Express

11. Para realizar la prueba de envío y recepción de mensajes de correo en el Outlook Express presione el botón enviar y recibir mensajes en la barra de herramientas y saldrá una pantalla donde se muestra la búsqueda de los mensajes que son enviados y recibidos.

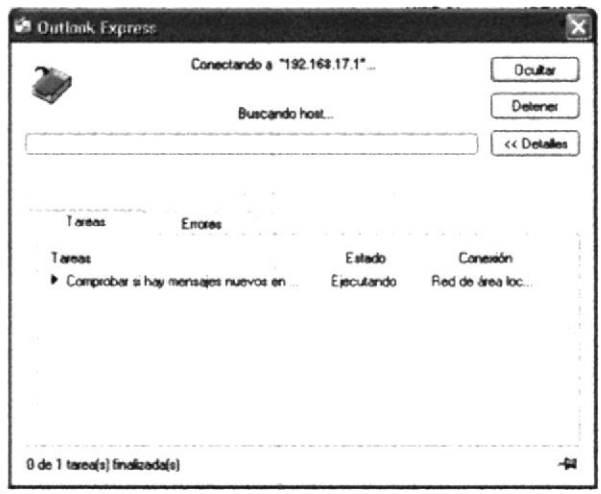


Figura 6.34 Buscando el servidor de correo electrónico

6.5 PROXY

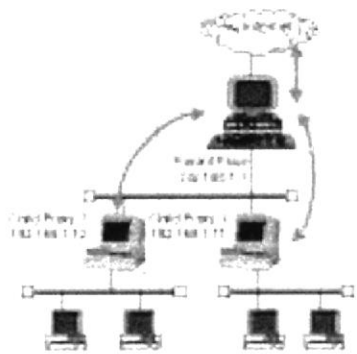


Figura 6.35 Como funciona Proxy

Con un servidor proxy disminuirá el tráfico de internet en su empresa ya que almacena el contenido de las páginas web e imágenes por donde los usuarios navegan. De esta forma, si cualquier otro usuario solicita una página ya visualizada por otro usuario, no es necesario descargarla nuevamente de internet (si no ha variado su contenido, el cual, es descargado nuevamente de internet) ya que la caché servirá las páginas.

Con un servidor proxy/cache estándar, usted puede limitar las páginas web que no quiere que visualice los usuarios, o indicar únicamente, las páginas que quiere que visualice. Estas limitaciones se pueden personalizar para cada uno de los usuarios.

6.5.1 REQUERIMIENTOS

- Haber instalado el paquete squid el cual se verifica con el comando **rpm –q squid**
- Tener deshabilitado el firewall.

6.5.2 CONFIGURACIÓN

1. Tener configurado el DNS y un WEB SERVER
2. Comprobar IP del servidor
   ```
   ifconfig
   ```
3. Comprobar si esta instalado el servicio squid
   ```
   rpm -q squid
   ```
4. Configurar el archivo squid
   ```
   vi /etc/squid/squid.conf
   ```

   ```
   http_port 8080                                  línea 53
   cache_men 16 MB                                 línea 468
   cache_dir ufs /var/spool/squid 100 16 256       línea 666
   cache_access_log /var/log/squid/access_log
   ```

```
acl red  src 192.168.17.0/255.255.255.0          línea 1680
acl Safe_ports web      8080
```

El parámetro **http_port**, en squid el puerto por defecto es el 3128 para atender peticiones pero puede especificarse otro, o más de uno.

- Proxy Transparente: utiliza el puerto 80 y redirecciona peticiones.
- Proxy Convencional: los usuraos suelen traer por defecto el puerto 8080 (Servicio de Cacheo de www).

El parámetro **cache_men,** establece la cantidad de memoria para Objetos en Tránsito, Objetos Hot y Objetos navegantes almacenados en caché. Debido a que los datos se almacenan en bloques de 4 kb por defecto se asignan 8 MB.

El parámetro **cache_dir,** debido a que entre más extensa la caché del disco más objetos almacena éste, y por lo tanto utilizará menos ancho de banda, será por defecto 100 MB.

El parámetro **cache_access_log,** sirve para monitorear la actividad de los hosts que tenga a cargo el Proxy.

5. Incluir las listas en las reglas de control de acceso
   ```
   http_acces allow red web                    línea 1742
   ```

6. Reiniciar el servicio
   ```
   service squid start
   ```

7. Configurar el cliente
   - Agregar dirección ip
   - En el explorador Habilitar servidor proxy:
     ```
     Ip del servidor          puerto 8080
     ```

6.5.3 CONFIGURACIÓN EN WINDOWS

1. Ingresar al explorador de Windows, elegir Menú Herramientas, y luego Opciones de Internet.

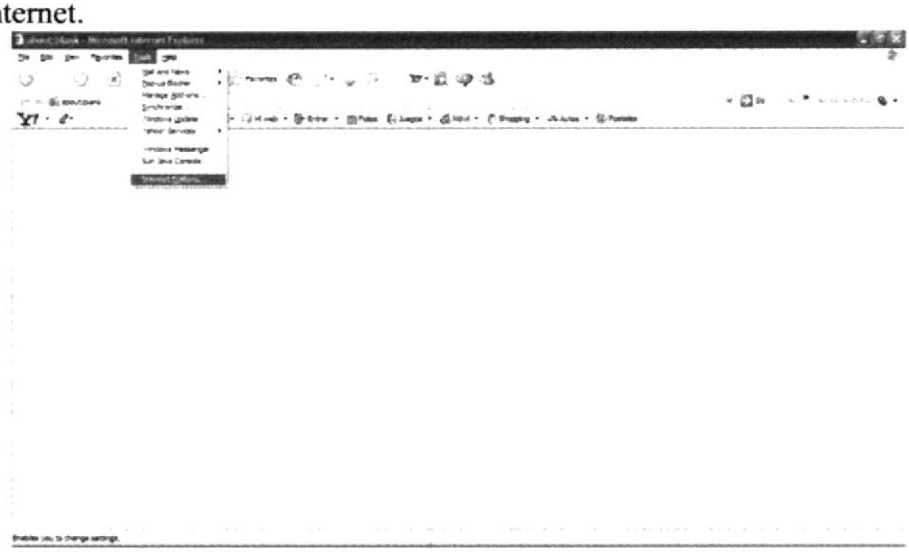


Figura 6.36 Cómo configurar servicio proxy para acceso a Internet

2. Dentro de Opciones de Internet escoger la pestaña Conexiones, y Configuración de la red LAN.

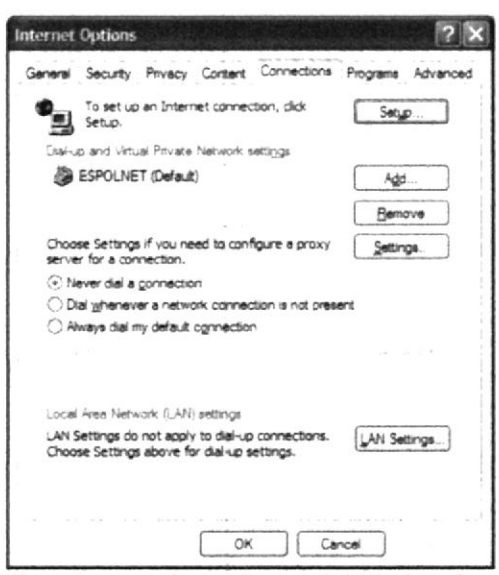


Figura 6.37 Pestaña conexiones dentro del Explorador de windows

3. En esta pantalla colocar la dirección del servidor y el puerto de comunicación en este caso para proxy es el 8080.

Figura 6.38 Botón Configuración Proxy dentro de la pestaña Conexiones del Explorador de Windows

4. Se carga la página www.espol.com, la misma que debe de estar configurada previamente en DNS y WEB SERVER.

Figura 6.39 Pantalla de autenticación de Proxy

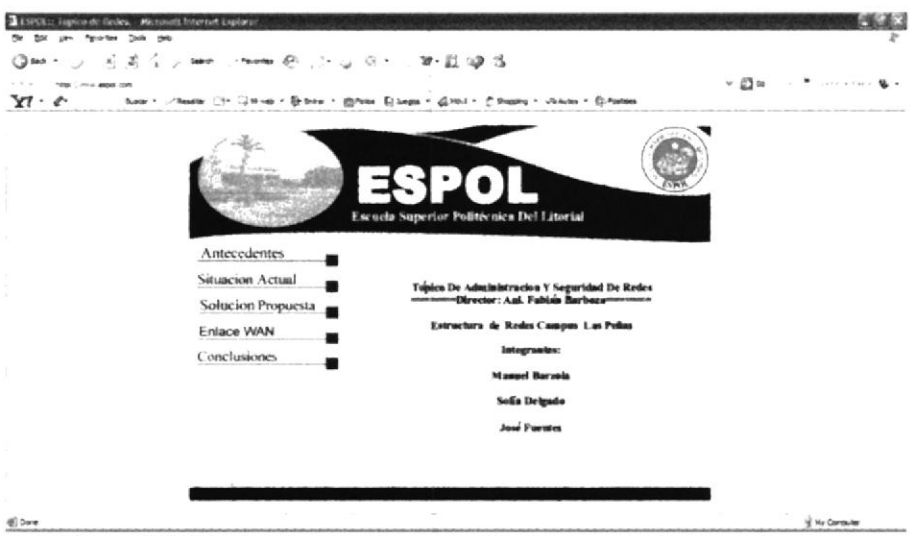


Figura 6.40 Página ingresado por medio Proxy creada por web server

6.5.3.1 DENEGAR ACCESOS POR HORA

1. Incluir las listas de control de acceso (acl)
   `acl (nombre de la lista) time (día) (hora inicio)-(hora fin)`
   ejm: `acl matutino time A 12:00-12:10` línea 1694
   `acl (nombre de la regla) src (ip de la red o la máquina a restringir)/` ejm: `acl cliente src 192.168.17.2/` línea 1695
   Los días están determinados por las letras

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

   Pueden combinarse los días
   La hora inicio y hora fin debe ser asignados en formato 24:00
2. Incluir las listas en las reglas de control de acceso
   `http_acces deny cliente matutino` línea 1742
3. Iniciar el servicio
   `service squid start`

6.5.3.2 ACCESO CON AUTENTICACIÓN (PASSWORD)

1. Crear archivo claves
   `touch /etc/squid/claves`
2. Levantar permisos al archivo
   `chmod 600 /etc/squid/claves`
3. Cambiar de propietario al archivo
   `chown squid:squid /etc/squid/claves`
4. Asignar contraseña
   `htpasswd /etc/squid/claves (usuario existente)`
5. Configurar el archivo squid

6.5.3.2.1 ESPECIFICAR RUTA DEL PROGRAMA BÁSICO DE PARÁMETROS DE AUTENTIFICACIÓN Y RUTA DE CONTRASEÑAS

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/clav
```

6. Incluir lista de control de acceso
   `acl password proxy_auth REQUIRED`

7. Incluir regla de control de acceso
   `http_access allow cliente password`

8. Reiniciar el servicio
   `service squid restart`

6.5.3.3 DENEGAR PÁGINAS PROHIBIDAS

1. Configurar el archivo squid

2. Incluir lista de control de acceso
   ```
   acl prohibidos src "/sitios/denegados"
   ```

3. Incluir regla de control de acceso
   ```
   http_access deny red prohibidos
   ```

4. Crear directorio y archivo de sitios prohibidos
   ```
   mkdir /sitios
   cd /sitios
   touch denegados
   ```
5. Editar archivo de páginas prohibidas
   ```
   vi /sitios/denegados
         www.xxx.com
         www.hardcore.com
         www.playboy.com
         www.triplex.com
   ```
   Salir con: wq para guardar los cambios del archivo

6. Reiniciar el servicio
   service squid restart

6.6 SEGURIDADES – FIREWALL

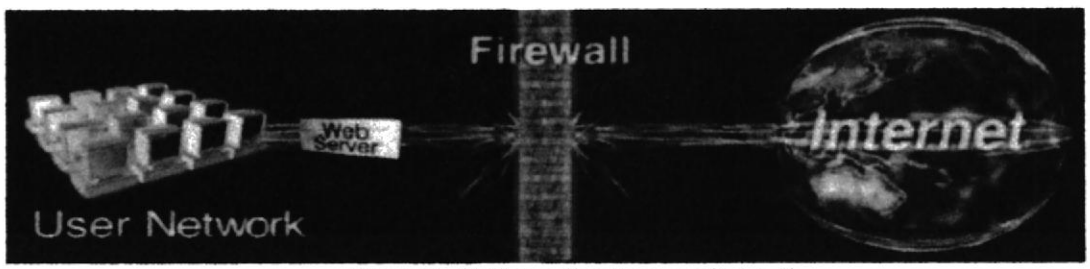


Figure 6.41 Como funciona un firewall

Un firewall es un dispositivo que filtra el tráfico entre redes, puede ser un dispositivo físico o un software sobre un sistema operativo.

Es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta.

Dependiendo de los servicios configurados en el servidor (web, correo, archivo, etc), y tras un exhaustivo análisis de la utilización, rendimiento del servidor y de la red interna se configura un firewall en el mismo servidor para tal fin.

Existen 3 tipos de reglas:
INPUT = ENTRADA AL SERVIDOR
OUTPUT = SERVIDOR HACIA FUERA
FORDWARD = REDIRECCIONAR

6.6.1 CONFIGURACIÓN

1. Bloquear PING

```
iptables -A INPUT -s 192.168.17.0/24 -d 192.168.17.27/32 -p icmp -j
DROP
iptables -A INPUT -s 192.168.17.0/24 -d 192.168.17.27/32 -p icmp -j
REJECT
```

Figura 6.42 Bloqueo de ping

2. Bloquear TELNET

```
iptables -A INPUT -s 192.168.17.0/24 -d 192.168.17.27/32 -p tcp --
dport 23 - j DROP
```

Figura 6.43 Bloqueo de telnet

3. Bloquear FTP

```
iptables -A INPUT -s 192.168.17.0/24 -d 192.168.17.27/32 -p tcp --
dport 21 -j DROP
```

6.7 DHCP

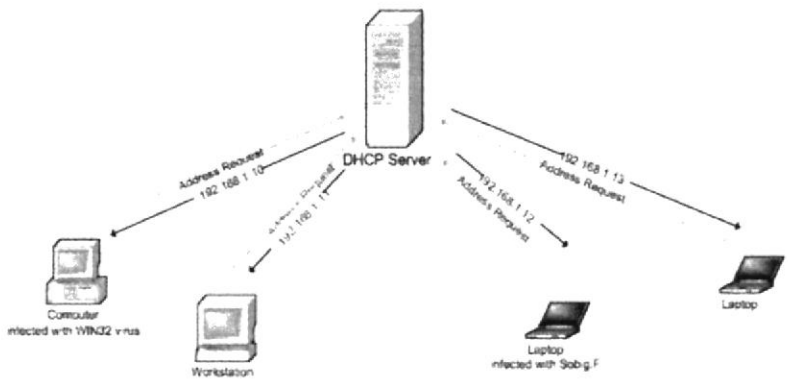


Figura 6.44 Como funciona DHCP

DHCP son las siglas que identifican a un protocolo, empleado para que los hosts (clientes), en una red, puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS, entre otros. El servicio DHCP permite acelerar y facilitar la configuración de muchos ordenadores en una red, evitando en gran medida los posibles errores humanos.

6.7.1 REQUERIMIENTOS

- Haber instalado el paquete dhcpd el cual se verifica con el comando **rpm –q dhcpd.**

- Tener deshabilitado los firewall (cortafuegos), esto se verifica digitando setup en la terminal y se elige configuración de firewall y se podrá verificar el estado.

6.7.2 CONFIGURACIÓN

1. Verificar si el paquete del dhcp esta instalado.
   ```
   rpm  -q dhcp
   ```

2. Crear el archivo dhcp.conf de la siguiente manera
   ```
   cp /usr/share/doc/dhcp-3.01/dhcpd.conf.sample etc/dhcpd.conf
   ```

3. Configurar el archivo dhcpd.conf
   ```
   vi  /etc/dhcpd.conf
   ```

   - En la línea subnet se asigna el segmento de red con su respectiva máscara.
     ```
     Subset 192.168.17.0 netmask 255.255.255.0
     ```
   - Opcional colocar la línea del gateway
     ```
     Option routers 192.168.17.8
     Option subset-mask 255.255.255.0
     ```
   - Digitar la dirección del DNS
     ```
     Option domain-name-servers 192.168.17.1
     ```
   - Definir el rango de IP desde - hasta
     ```
     Range dynamic-bootp 192.168.17.66 192.168.17.100
     ```

- Salir con :wq para guardar los cambios.

4. Se debe crear un archivo en la siguiente ruta que es donde se guardaran todas las direcciones ip asignadas por dhcp.
```
touch /var/lib/dhcp/dhcpd.leases
```

5. Para añadir dhcp al arranque del sistema, ejecute:
```
chkconfig dhcpd on
```

6. Verificar el estado del proceso de dhcp cada vez que se realice una cambio.
```
pgrep dhcp
```

7. Iniciar el servicio del dhcpd
```
service dhcpd restart
```

6.7.3 WINDOWS

Configurar en windows la ip dinámica en la estación de trabajo

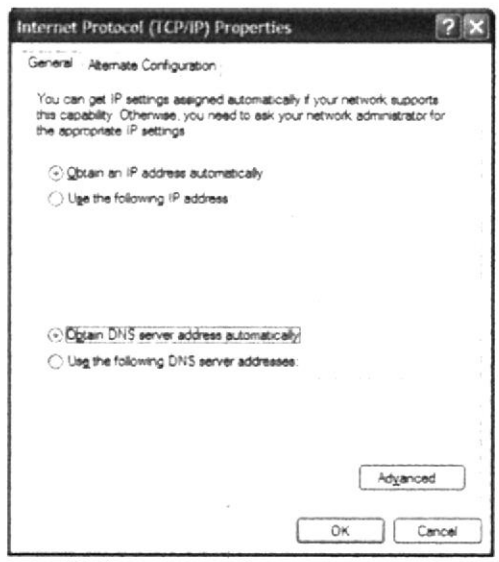


Figura 6.45 Como se configura el protocolo TCP/IP

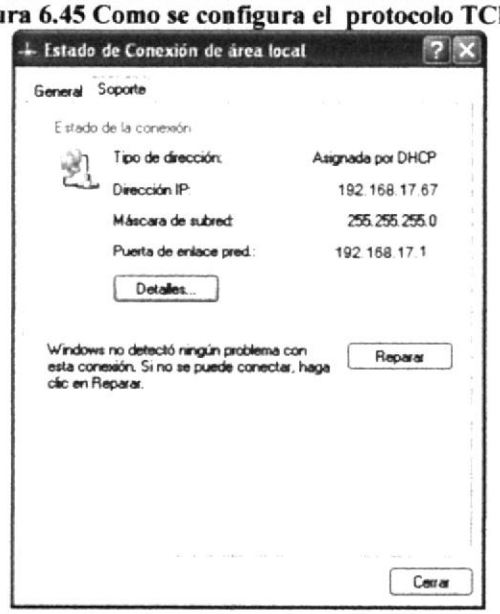
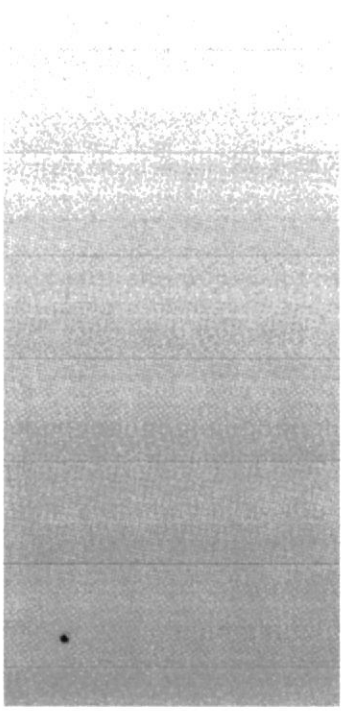


Figura 6.46 Como se ha asignado una dirección IP por medio de DHCP



ANEXOS

GLOSARIO

GLOSARIO

0-9

10 mbps: Millones de bits por segundo unidad de velocidad de transferencia de información.

10 base T: Especificación Ethernet de banda base de 10 Mbps que usa dos pares de cables de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y el otro para recibir datos. 10BASE-T, que forma parte de la especificación IEEE 802.3, tiene una limitación de distancia de aproximadamente 100 metros por segmento. Ver también Ethernet e IEEE 802.3.

10 base-F: Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BASE-FB, 10BASE-FL y 10BASE-FP para Ethernet sobre cableado de fibra óptica. Ver también 10BASE-FB, 10BASE-FL, 10BASE-FP y Ethernet.

100 base FX: Especificación Fast Ethernet de banda base de 100 Mbps que usa dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una temporización de señal adecuada, el enlace 100BASE-FX no puede exceder una longitud de 400 metros. Basado en el estándar IEEE 802.3. Ver también 100BASE-X, Fast Ethernet e IEEE 802.3.

10 base-F: Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BASE-FB, 10BASE-FL y 10BASE-FP para Ethernet sobre cableado de fibra óptica. Ver también 10BASE-FB, 10BASE-FL, 10BASE-FP y Ethernet.

10 base-FB: Especificación Ethernet de banda base de 10 Mbps que usa cableado de fibra óptica. 10BASE-FB forma parte de la especificación IEEE 10BASE-F. No se utiliza para conectar estaciones de usuario pero, en cambio, suministra un backbone de señalización síncrona que permite que segmentos y repetidores adicionales se conecten a la red. Los segmentos 10BASE-FB pueden tener hasta 2000 metros de largo. Ver también 10BASE-F y Ethernet.

10 base-FL: Especificación Ethernet de banda base de 10 Mbps que usa cableado de fibra óptica. 10BASE-FL forma parte de la especificación IEEE 10BASE-F y, aunque puede interoperar con FOIRL, está diseñado para reemplazar a la especificación FOIRL. Los segmentos 10BASE-FL pueden tener hasta 1000 metros de largo si se usan con FOIRL, y hasta 2000 metros si se usan exclusivamente con 10BASE-FL. Ver también 10BASE-F, Ethernet, y FOIRL.

10 base-FP: Especificación Ethernet de banda base de fibra pasiva de 10 Mbps que usa cableado de fibra óptica. La 10BASE-FP forma parte de la especificación IEEE 10BASE-F. Organiza una cantidad de computadores en una topología en estrella sin necesidad de usar repetidores. Los segmentos 10BASE-FP pueden tener hasta 500 metros de largo. Ver también 10BASE-F y Ethernet.

A

Ancho de Banda: La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también se usa para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

ARP: Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Comparar con RARP.

Asignación de direcciones: Técnica que permite que distintos protocolos interoperen traduciendo direcciones desde un formato a otro. Por ejemplo, al enrutar IP a través de una red Frame Relay, las direcciones IP se deben mapear a las direcciones Frame Relay de modo que los paquetes IP se puedan transmitir por la red. Ver también resolución de direcciones.

B

Banda Ancha: Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica. Comparar con banda ancha.

Broadcast: Envío de información en cualquier formato a mas de un lugar de destino

Banda Base: Característica de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha. Ver la diferencia con banda ancha. Término utilizado en la WWW

Bps: (Bits per Second). Medida que representa la rapidez con que los bits de datos se transmiten a través de un medio de comunicaciones. Por ejemplo: un módem de 28.8 Kbps es capaz de transferir 28.800 bits por segundo.

Bit: (Binary Digit ó Dígito Binario). Es un dígito en base 2,es decir, 0 ó 1.Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

Byte: Unidad de medida de la cantidad de información en formato digital. Usualmente un byte consiste de 8 bits. Un bit es un cero (0) o un uno (1). Esa secuencia de números (byte) pueden simbolizar una letra o un espacio (un carácter). Un kilobyte (Kb) son 1024 bytes y un Megabyte (Mb) son 1024 Kilobytes.

Bloqueo: En un sistema de conmutación, una condición en al que no hay ninguna ruta disponible para completar un circuito. El término también se usa para describir una situación en la que no se puede iniciar una actividad hasta que la otra no se haya completado.

C

Cable blindado: cable que posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

Cable coaxial: cable compuesto por un conductor cilíndrico exterior hueco que rodea un conductor de alambre interno único. En la actualidad se usan dos tipos de cable coaxial en la LAN: cable de 50 ohmios, que se usa para la señalización digital, y cable de 75 ohmios que se usa para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro, sin embargo no es susceptible a la interferencia electromagnética y es capaz de brindar velocidades de datos más altas.

Cable neutro: Cable de circuito que se conecta a la conexión a tierra en la central de energía y en el transformador.

Cableado backbone: Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN. Ver cableado vertical.

Cableado de Categoría 1: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 1 se usa para comunicaciones telefónicas y no es adecuado para transmitir datos. Comparar con cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 2 : Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568By UTP.

Cableado de Categoría 3: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 3 se usa en las redes 10BASE-T y puede transmitir datos a velocidades de hasta 10 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 4: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 4 se usa en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 5: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de

Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 4. Ver también EIA/TIA-568By UTP.

Caché: Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso más rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los accesos a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

Canaleta decorativa Tipo de canal montado en la pared que tiene una cubierta removible que se usa para admitir el cableado horizontal. La canaleta decorativa es lo suficientemente grande como para contener dos cables.

Canaleta: Un tipo de canal adosado a la pared que tiene una cubierta removible para dar apoyo al cableado horizontal. La canaleta es lo suficientemente grande como para contener varios cables.

Capa física: La Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Capa de control de enlace de datos: La Capa 2 del modelo de arquitectura . Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

Capa de red: La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

Capa de transporte: La Capa 4 del modelo de referencia OSI. Esta capa es responsable de la comunicación confiable de red entre nodos finales. La capa de transporte suministra mecanismos para establecer, mantener y terminar los circuitos virtuales, detección y recuperación de errores de transporte y control del flujo de información.

Capa de sesión: La Capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de capa de presentación.

Capa de presentación: La Capa 6 del modelo de arquitectura OSI. Esta capa suministra administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Corresponde aproximadamente a la capa de presentación del modelo OSI.

Capa de aplicación: La Capa 7 del modelo de referencia OSI. Esta capa suministra servicios a los procesos de aplicación (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de terminal) que están fuera del modelo OSI. La capa de aplicación identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos que se requieren para conectarse con ellos),

sincroniza las aplicaciones cooperantes y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos.

CD: Detección de portadora. Señal que indica si una interfaz está activa. También, una señal generada por un módem que indica que se ha conectado una llamada.

Cliente: Nodo que solicita servicios a un servidor.

Colisión: En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

Cola: Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

Conector RJ: Conector macho registrado. Conectores estándar que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ

Costo: Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.

Consola: DTE a través del cual se introducen los comandos en un host.

Correo electrónico: Aplicación de red utilizada ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.

CSMA/CD: Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón).

Cliente: Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

Computador: Es un dispositivo electrónico compuesto básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

Contraseña ó Password: Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los Sistemas y recursos de la computadora.

CPU: (Central Processing Unit ó Unidad central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

Cuadro de Diálogo: Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

Cuadro de Texto: Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de diálogo, el cuadro de texto puede estar en blanco o contener texto.

Cursor: Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo caracter a visualizar cuando se pulse una tecla.

CSU: Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con el loop telefónico digital local. A menudo se denomina, de forma conjunta con DSU, como CSU/DSU.

D

Db: Decibelios

Dominio: En Internet, una parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía.

DCE: equipo de comunicación de datos. Equipo de comunicación de datos (expansión EIA) o equipo de terminación de circuito de datos (expansión ITU-T). El dispositivo y las conexiones de una red de comunicaciones que abarca el extremo de la red de la interfaz usuario a red. El DCE proporciona una conexión física con la red, envía tráfico y suministra una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE. Comparar con DTE.

Descifrado: La aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando por lo tanto los datos a su estado original, no cifrado.

Dato: Son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

DTE: Equipo de terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario-red que actúa como origen de datos, destino de datos o ambas. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y por lo general usa señales de temporización generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadores, traductores de protocolo y multiplexores.

Directorio: En D.O.S., una lista de nombres de archivo que contiene toda la información de los archivos almacenados. A partir de Windows 95 este término se reemplazó por CARPETA.

Dirección: Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico" (email address); "IP" (dirección Internet); y "dirección hardware".

Dirección del Protocolo de Internet (dirección IP): Dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red con Protocolo de control de transmisión/Protocolo Internet (TCP/IP). Número único que consta de 4 partes separadas por puntos. Una dirección IP se suele representar en una notación decimal con puntos que indica cada octeto (ocho bits o un byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 172.16.255.255.

Cada computadora conectada a Internet tiene un único número de IP. Si la máquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem).

Disco Rígido: Unidad de almacenamiento permanente de información. Éste es el que guarda la información cuando apagamos la computadora. Aquí se guardan la mayoría de los programas y el sistema operativo. Su capacidad de almacenamiento se mide en Megabytes (Mb) o Gigabytes (Gb), en donde 1024 Mb = 1Gb.

Disquete: Dispositivo que puede insertarse y extraerse en una unidad de disco.

DNS: (Domain Name System ó Sistema de Nombres de Dominio). El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de éstos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes son: .COM (comercial - empresas), .EDU (educación, centros docentes), .ORG (organización sin ánimo de lucro), . NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejército USA). La mayoría de los países tienen un dominio propio. Por ejemplo, AR (Argentina) .PY (Paraguay), .US (Estados Unidos de América), .ES (España), ..AU (Australia), etc.

Dominio: (Domain Name). Nombre único que identifica a un sitio de Internet. Los nombres de dominio tienen 2 o más secciones, separadas por puntos. La sección de la

izquierda es la más específica, y la de la derecha, la más general. Una computadora particular puede tener más de un nombre de dominio, pero un nombre de dominio se refiere únicamente a una PC.

Download ó descargar: En Internet es el proceso de transferir información desde un servidor de información a la propia PC.

Documentación: Manual escrito que detalla el manejo de un sistema o pieza de hardware.

Doble Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón) dos veces, sin desplazarlo. Esta acción sirve para ejecutar una determinada aplicación, como por ejemplo: inicializarla.

DSU: Unidad de servicio de datos. Dispositivo que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión como, por ejemplo, T1 y E1. La DSU también es responsable de funciones tales como

DVD: (Digital Versatile Disc ó Disco Versátil Digital). Disco que sirve para almacenar más datos de contenido digital, como música o video, que un CD. Un DVD guarda un mínimo de 4.7 Gigabytes (el tamaño de una película de cine).

E

E1: Estándar Europeo equivalente al americano T1. Los circuitos E1 y T1. Los dos usan canales de 64 Kbps, pero el T1 tiene 24 mientras que el E1 tiene 32 canales.

EIA/TIA-568: Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

Encapsulamiento: El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

Emulación de terminal: Aplicación de red en la que un computador ejecuta software que la hace aparecer ante un host remoto como una terminal conectada directamente.

Enrutamiento: Proceso para encontrar una ruta hacia un host destino. El enrutamiento en redes de gran tamaño es muy complejo dada la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ethernet: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3. Ver también 10BASE2, 10BASE5, 10BASE-F, 10BASE-T, 10Broad36 e IEEE 802.3.

Elemento de Pantalla: Partes que constituyen una ventana o cuadro de diálogo como por ejemplo: la barra de título, los botones de "Maximizar" y "Minimizar", los bordes de las ventanas y las barras de desplazamiento.

Escritorio: Fondo de la pantalla sobre la cual aparecen ventanas, iconos y cuadros de diálogo.

Estación de trabajo: Computador de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. Llamadas así para distinguirlas de los que se conocen como servidores.

Expandir: Mostrar los niveles de directorio ocultos del árbol de directorios. Con el administrador de archivos es posible expandir un solo nivel de directorio, una rama del árbol de directorio o todas las ramas a la vez.

Explorador: Llamado también explorador Web. Interfaz cliente que permite al usuario ver documentos HTML en el World Wide Web, en otra red o en su propio equipo; seguir los hipervínculos y transferir archivos. Un ejemplo es Microsoft Internet Explorer.

Extensión: Está compuesto por un punto y un sufijo de hasta tres caracteres situados al final de un nombre de archivo. La extensión suele indicar el tipo de archivo o directorio.

F

Fibra monomodo: Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único. Ver también fibra multimodo.

Fibra multimodo: Fibra óptica que permite la propagación de múltiples frecuencias de luz.

Firewall: Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Fluctuación de fase: Distorsión analógica de la línea de comunicación provocada por la variación de una señal de sus posiciones de temporización de referencia. La fluctuación de fase puede provocar la pérdida de datos, especialmente a altas velocidades.

Flujo de datos: Todos los datos que se transmiten a través de la línea de comunicaciones en una sola operación de lectura o escritura.

Frecuencia: Cantidad de ciclos, medidos en hercios, de una señal de corriente alterna por unidad de tiempo.

FTP: Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP, que se usa para transferir archivos entre nodos de la red. El FTP se define en la RFC 959.

Full duplex: Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora.

G

Gateway: En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función, y gateway se refiere a un dispositivo con fines especiales que ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra.

Gateway fronterizo: Router que se comunica con routers de otros sistemas autónomos.

Giga: Prefijo que indica un múltiplo de 1.000 millones, o sea 10^9. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 2^{30}, o sea 1.073.741.824.

Grupo de trabajo: Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

H

Hardware: Son todos los componentes físicos que componen una PC.

Hercio: Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

Hexadecimal: Base 16. Representación numérica que usa los dígitos 0 a 9, con su significado habitual, y las letras A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, luego 16^2=256, etc.

Host : Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

HTML: (HyperText Markup Language). Lenguaje utilizado para crear los documentos de hipertexto que se emplean en la WWW. Los documentos HTML son simples archivos de texto que contienen instrucciones (llamadas tags) entendibles por el Navegador (Browser).

HTTP: (HyperText Transport Protocol). Protocolo utilizado para transferir archivos de hipertexto a través de Internet. Requiere de un programa "cliente" de HTTP en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la WWW.

Hub: Dispositivo de hardware o software que contiene módulos de red y equipo de internetwork múltiples, independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen, las señales que se envían a través de ellos).

I

IEEE: Instituto de ingenieros eléctricos y electrónicos. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN del IEEE son los estándares de LAN predominantes en el mundo actual.

IEEE 802.1: Especificación del IEEE que describe un algoritmo que evita los loops de capa dos mediante la creación de un spanning tree. El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo de Digital y el algoritmo IEEE 802.1 no son exactamente los mismos, ni tampoco son compatibles.

IEEE 802.12: Estándar LAN del IEEE que especifica la capa física y la subcapa MAC de la capa de enlace de datos. El IEEE 802.12 usa el esquema de acceso a los medios de prioridad de demanda a 100 Mbps a través de una diversidad de medios físicos. Ver también 100VG-Any LAN.

IEEE 802.2: Protocolo LAN del IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 administra errores, entramado, control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se usa en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3: Protocolo LAN del IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 usa acceso CSMA/CD a diversas velocidades sobre diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican las implementaciones de Fast Ethernet. Las variantes físicas de la especificación IEEE 802.3 original incluyen 10BASE2, 10BASE5, 10BASE-F, 10BASE-T y 10Broad36. Las variantes físicas de Fast Ethernet incluyen 100BASE-T, 100BASE-T4 y 100BASE-X.

Icono: Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc.

IDF: Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

Impresora: Dispositivo de salida, cuya funcionalidad es transcribir/pasar un documento (imagen y/o texto) desde el ordenador (procesador de textos, bloc de notas, visor de

imágenes, etc.) a un medio físico, generalmente papel, mediante el uso de cinta, cartuchos de tinta o también con tecnología láser.

Impresora de Inyección a tinta: Crean imágenes directamente sobre el papel al rociar tinta a través de una pequeñas boquillas, su calidad de impresión es bastante alta.

Impresora Predeterminada: Impresora que se utiliza si se elige el comando Imprimir, no habiendo especificado antes la impresora que se desea utilizar. Sólo puede haber una impresora predeterminada, que debe ser la que se utilice con mayor frecuencia.

Información: Es lo que se obtiene del procesamiento de datos, es el resultado final.

Informática cliente-servidor: Término que se usa para describir los sistemas de red informáticos distribuidos (de procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: cliente (front end) y servidor (back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos actuales.

Internetwork: Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red.

IP: Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad. Documentado en la RFC 791.

IP access-group: Comando que enlaza una lista de acceso existente con una interfaz de salida.

IP host: Comando que se usa para crear una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.

IP multicast: Técnica de enrutamiento que permite que el tráfico IP se propague desde un origen hacia un número de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, se envía un paquete a un grupo de multicast que se identifica mediante una sola dirección de grupo de destino IP.

IPX: Intercambio de paquetes de internetworking. Protocolo de capa de red (Capa 3) de NetWare que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

Interfaz: Una conexión e interacción entre hardware, software y usuario, es decir, como la plataforma o medio de comunicación entre usuario o programa.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

Intranet: Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno.

ISO: Organización Internacional de Normalización. Organización internacional que es responsable por una amplia gama de estándares, incluyendo aquellos relevantes para el networking. ISO desarrolló el modelo de referencia OSI, un modelo de referencia de networking sumamente popular.

J

Jumper: Término que se usa para los cables de interconexión que se encuentran en el armario de cableado.

K

Kbps: (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit esta formado por mil bits.

Kilobyte: Es el equivalente a 1024 bytes.

L

LAN: Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido. Comparar con MAN y WAN.

Latencia: Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir tambien sucede en el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

LED: Diodo emisor de luz. Dispositivo semiconductor que emite luz producida por la conversión de energía eléctrica. Las lámparas de estado en los dispositivos de hardware generalmente son LED.

Línea de acceso telefónico: Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

Línea de comunicación: Enlace físico (como, por ejemplo, un cable o circuito de teléfono) que conecta uno o más dispositivos con uno o más dispositivos.

Línea de mira: Característica de determinados sistemas de transmisión como, por ejemplo, los sistemas láser, de microondas e infrarrojos, en los que no puede existir ninguna obstrucción en la ruta directa entre el transmisor y el receptor.

Línea dedicada: Línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir. Ver también línea arrendada.

Lista de acceso: Lista que mantienen los routers Cisco para controlar el acceso hacia o desde el router para diversos servicios (por ejemplo, para evitar que los paquetes que tienen una determinada dirección IP salgan de una interfaz específica del router).

LSA: Publicación de estado de enlace. Paquete de broadcast que usan los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de la ruta. Los routers receptores usan las LSA para mantener sus tablas de enrutamiento

Login: Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del password, el login no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

M

MAC: Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

MICIP: Protocolo de capa de red que encapsula paquetes IP en DDS o transmisión a través de AppleTalk.

Malla: Topología de red en la que los dispositivos se organizan de una manera administrable, segmentada, con varias interconexiones, a menudo redundantes, ubicadas estratégicamente entre nodos de la red. Ver también malla completa y malla parcial.

Malla completa: Término que describe a una red en la que los dispositivos están organizados en una topología de malla, en la que cada nodo de la red tiene un circuito físico o un circuito virtual que lo conecta a todos los otros nodos de la red. Una malla completa brinda una gran cantidad de redundancia pero, dado que su implementación puede resultar excesivamente cara, generalmente se la reserva para los backbones de la red. Ver también malla y malla parcial.

MAN: Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

MAP: Protocolo de automatización de fabricación. Arquitectura de red creada por General Motors para satisfacer las necesidades específicas las instalaciones fabriles. El MAP especifica una LAN de transmisión de tokens similar a IEEE 802.4. Ver también IEEE 802.4.

Mapa de cableado: Característica suministrada por la mayoría de los analizadores de cable. Se usa para probar las instalaciones de cableado de par trenzado, y muestra cuáles hilos están conectados a cuáles pines, en conectores macho y hembra.

Mapa de topología: Herramienta para administrar un switch ATM LightStream 2020 que examina una red y muestra el estado de sus nodos y enlaces troncales. El mapa de topología es una aplicación basada en HP OpenView que se ejecuta en un NMS.

Máscara de red: Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

Máscara wildcard: Cantidad de 32 bits que se usan de forma conjunta con una dirección IP para determinar cuáles son los bits de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

MD5: Message Digest 5. Algoritmo que se usa para la autenticación de mensajes en SNMP v.2. El MD5 verifica la integridad de la comunicación, autentica el origen y controla la puntualidad. Ver también SNMP2.

MDF: Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

Megabyte (MB): 1.048.576 bytes; 1.024 Kilobytes.

Megahertz: Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

Memoria RAM: Memoria de acceso aleatorio cuyo contenido permanecerá presente mientras el computador permanezca encendido.

Memoria ROM: Memoria de sólo lectura. Chip de memoria que sólo almacena permanentemente instrucciones y datos de los fabricantes.

Métrica: Método por el cual un algoritmo de enrutamiento determina que una ruta es mejor que otra. Esta información se guarda en las tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de comunicación, retardo, número de saltos, carga, MTU, costo de la ruta y confiabilidad.

Microonda: este enlace esta constituido por dos transceptores de radio provistos de antenas parabólicas que se apuntan directamente entre si. La radio puede transportar transmisiones punto a punto de muchos anchos de banda. Su alcance varia según el tamaño de la antena, el clima en la zona y la magnitud de la potencia emitida contemplando todos estos conjuntos la señal puede llegar hasta 80 Km.

Módem: (Modulator,Demodulator). Dispositivo que se conecta a la computadora y a la línea telefónica y que permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

Mouse: Permite convertir el movimiento de la mano en desplazamiento de un cursor sobre la pantalla.

Multicast: la multidifusión (multicast) permite que grupos de usuarios seleccionados reciban la misma transmisión de datos en una red los cuales están identificados por una única dirección de grupo de destino IP.

N

Navegador de Web: Aplicación de cliente de hipertexto basada en GUI como, por ejemplo, Mosaic, que se usa para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a través de la WWW e Internet. Ver también hipertexto, Internet, Mosaic y WWW.

NBP: Protocolo de enlace de denominación. Protocolo AppleTalk de nivel de transporte que convierte un nombre dado en forma de una cadena de caracteres en una dirección de internetwork.

NET: Título de entidad de red. Direcciones de red, definidas por la arquitectura de red ISO.

NetBIOS: Sistema básico de entrada/salida de red. API que usan las aplicaciones de una LAN IBM para solicitar servicios de procesos de red de nivel inferior. Estos servicios pueden incluir establecimiento y terminación de sesión y transferencia de información

NetWare: NOS distribuido de uso generalizado desarrollado por Novell. Suministra acceso remoto transparente a archivos, y muchos otros servicios de red distribuida.

Networking: Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NIC: Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

NOS: Sistema operativo de red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos. Los ejemplos de NOS incluyen LAN Manager, NetWare, NFS y VINES.

Número de host: Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

Número de red: Parte de una dirección IP que especifica la red a la que pertenece el host.

Número de saltos: Métrica de enrutamiento que se usa para medir la distancia entre un origen y un destino. El RIP usa el número de saltos como su única métrica.

NVRAM: RAM no volátil. RAM que retiene su contenido cuando una unidad se apaga. En los productos Cisco, la NVRAM se usa para guardar la información de configuración.

Nodo: En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma.

Nombre de usuario: La secuencia de caracteres que lo identifica. Al conectarse a una computadora, generalmente necesita proporcionar su nombre y contraseña de usuario. Esta información se usa para verificar que la persona está autorizada para usar el Sistema.

O

Operador de red: Persona que monitorea y controla una red de forma continua, ejecutando tareas como

Oscilación: Señal secundaria superpuesta a la onda de 60 Hz. Tiene una magnitud que varía entre el 15% y el 100% del voltaje normal de la línea de alimentación. Ver sobrevoltaje, pico y baja de voltaje.

OSI: Interconexión de sistemas abiertos. Programa internacional de normalización creado por la ISO y la UIT-T para desarrollar estándares de interconexión que faciliten la interoperabilidad de equipos de múltiples proveedores.

OSINET: Asociación internacional diseñada para promover OSI en las arquitecturas de los proveedores.

OSPF: Versión abierta del algoritmo "Primero la ruta libre más corta". Algoritmo de enrutamiento IGP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad Internet. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga. El OSPF deriva de una versión inicial del protocolo ISIS

P

PAD: Ensamblador/desensamblador de paquetes. Dispositivo que se usa para conectar dispositivos simples (como terminales de modo de carácter) a una red, los cuales no admiten toda la funcionalidad de un protocolo específico. Los PAD almacenan los datos en el búfer de los PAD y ensamblan y desensamblan los paquetes que se envían a dichos dispositivos finales.

Panel de conexión: Conjunto de ubicaciones de pin y puertos que se puede montar en un bastidor o una consola de pared en el armario de cableado. Los paneles de conexión actúan como conmutadores que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

Paquete de choque: Paquete que se envía al transmisor para informarle que hay congestión y que debe reducir su velocidad de envío.

Par trenzado: Medio de transmisión de relativa baja velocidad compuesto por dos cables aislados dispuestos en un patrón en espiral regular. Los cables pueden ser blindados o no blindados. El uso del par trenzado es común en aplicaciones de telefonía y es cada vez más común en las redes de datos. Ver también STP y UTP.

Paradiafonía: Energía de interferencia transferida de un circuito a otro.

PBX: Central telefónica privada. Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas y públicas.

PCI: Información de control de protocolo. Información de control que se agrega a los datos del usuario para formar un paquete OSI.

Pila de protocolo: Conjunto de protocolos de comunicación relacionados que operan de forma conjunta y, como un grupo, cumplen con la comunicación en alguna o en las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo y, a menudo, un solo protocolo de la pila se dirige a una cantidad de capas a la vez. El TCP/IP es un protocolo de pila típico.

Ping: Abreviatura para Packet Internet Groper o Packet Inter-network Groper, una utilidad que se usa para determinar si una dirección IP en particular está disponible. Funciona enviando un paquete a la dirección especificada y esperando una respuesta. El PING se usa principalmente para diagnosticar las fallas de las conexiones de Internet.

Plan de distribución: Diagrama simple que indica dónde están ubicados los tendidos de cable y la cantidad de habitaciones hacia las que se dirigen.

POP: Punto de presencia. Punto de presencia es el punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y el servicio de distribución principal del edificio.

Portadora: Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos. Ver también modulación.

POST: Autocomprobación de encendido. Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando ese dispositivo se enciende.

Protocolo de enrutamiento: Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. Los ejemplos de protocolos de enrutamiento incluyen el IGRP, el OSPF y el RIP.

Puerto: Interfaz de un dispositivo de internetworking (como, por ejemplo, un router).
En terminología IP, un proceso de capa superior que recibe información de las capas inferiores.
Un conector hembra de un panel de conexión el cual acepta el mismo tamaño de conector que el de un RJ45. Los cables de conexión se usan en estos puertos para realizar interconexiones entre los computadores conectados al panel. Es esta interconexión conexión la que permite la operación de la LAN.

Página Web: Documento de World Wide Web. Una página Web suele consistir en un archivo HTML, con sus archivos asociados de gráficos y secuencias de comandos, en un directorio determinado de un equipo concreto (y, por tanto, identificable mediante una dirección URL).

Periféricos: Cualquier dispositivo de hardware conectado a una computadora.

Pixel: (PICture cELL). Es la parte más pequeña de una pantalla de video, constituido por uno o más puntos que se consideran como una unidad. Es por tanto, el bloque de construcción de imágenes.

Protocolo: Método por el que los equipos se comunican en Internet. El protocolo más común en el World Wide Web es HTTP. Otros protocolos de Internet incluyen FTP, Gopher y telnet. El protocolo forma parte de la dirección URL completa de un recurso.

Proveedor: Institución o empresa que provee acceso a uno o varios servicios de Internet.

R

RAM: Memoria de acceso directo aleatorio. Memoria volátil que puede ser leída y escrita por un microprocesador.

Red: Conjunto de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red de conexión única: Red que tiene una sola conexión con un router.

Redireccionar: Parte de los protocolos ICMP y ES-IS que permiten que un router le indique a un host que puede ser más efectivo usar otro router.

Redistribución: Permitir que la información de enrutamiento detectada a través de un protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento. A veces denominada redistribución de ruta.

Redundancia: En internetworking, la duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los dispositivos,

servicios o conexiones redundantes puedan ejecutar el trabajo de aquellos que han fallado. Ver también sistema redundante.

Rendimiento: Velocidad de la información que llega a, y posiblemente atraviesa, un punto particular de un sistema de red.

Repetidor: Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red.

Retardo: El tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. También, el tiempo que se requiere para mover un paquete desde el origen hacia el destino a través de una ruta específica.

RF: Radiofrecuencia. Término genérico que se usa para referirse a frecuencias que corresponden a transmisiones radioeléctricas. Las redes de televisión por cable y de banda ancha usan tecnología RF.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

RIP: Protocolo de información de enrutamiento. IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet.

RMON: Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitoreo remoto de los dispositivos conectados a la red.

ROM: Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.

Ruta estática: Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

Ruta por defecto: Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

S

Segmento: La sección de una red limitada por puentes, routers o switches. Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

SMTP: Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico.

Sondeo: Método de acceso en el que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

Switch: Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI:

Switch LAN: Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches LAN envían tráfico basándose en las direcciones MAC. Esta variedad de switch LAN a veces de denomina switch de trama. Los switches LAN a menudo se clasifican de acuerdo con el método que usan para enviar tráfico: conmutación de paquetes por método de corte y conmutación de paquetes por almacenamiento y envío. Los switches multicapas son un subconjunto inteligente de los switches LAN.

Servidor: Computadora o programa que brinda un servicio específico al "cliente", que se ejecuta en otras computadoras. El término puede referirse tanto a un equipo de una red que envía archivos o ejecuta aplicaciones para otros equipos de la red; el software que se ejecuta en el equipo servidor y que efectúa la tarea de servir archivos y ejecutar aplicaciones; o bien, en la programación orientada a objetos, un fragmento de código que intercambia información con otro fragmento de código cuando se pide.

SO: (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software: Todos los componentes no físicos de una PC (Programas).

T

T1: Servicio de portadora de WAN digital. T1 transmite datos con formato DS-1 a 1.544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o B8ZS. Comparar con E1. Ver también AMI, B8ZS y DS-1.

Tabla de enrutamiento: Tabla que se guarda en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas hacia destinos de red en particular y, en algunos casos, las métricas asociadas con esas rutas.

TFTP: Protocolo de Transferencia de Archivos Trivial. Versión simplificada del FTP que permite que los archivos se transfieran desde un computador a otra a través de una red.

Terminal: Dispositivo simple en el que los datos se pueden introducir o recuperar desde una red. Generalmente, las terminales tienen un monitor y un teclado pero no tienen ningún procesador ni unidad de disco local.

Topología: Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

Topología de anillo: Topología de red que consta de un conjunto de repetidores conectados entre sí mediante enlaces de transmisiones unidireccionales para formar un solo bucle cerrado. Cada estación de la red se conecta a la red en el repetidor. Aunque lógicamente están organizadas en anillo, las topologías de anillo a menudo están organizadas en una estrella de bucle cerrado.

Topología de bus: Arquitectura LAN lineal en la que las transmisiones de las estaciones de red se propagan a lo largo del medio y son recibidas por todas las otras estaciones.

Topología en árbol: Topología LAN similar a la topología bus, salvo que las redes en árbol pueden tener ramificaciones con múltiples nodos. Las transmisiones desde una estación atraviesan la longitud del medio y son recibidas por todas las otras estaciones.

Topología en estrella: Topología LAN en la que los puntos de terminación de una red se conectan a un switch central común mediante enlaces punto a punto. Una topología de anillo que está organizada como estrella implementa una estrella de loop cerrado unidireccional en lugar de enlaces punto a punto.

Topología en estrella jerárquica: Topología en estrella extendida en la que un hub central se conecta a través de cableado vertical con otros hubs que dependen del mismo.

Transceiver: Unidad de conexión al medio. Dispositivo que se usa en las redes Ethernet e IEEE 802.3 que suministra la interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que se puede incorporar a una estación o puede ser un dispositivo individual, ejecuta funciones de capa física, incluyendo la conversión de datos digitales desde la interfaz Ethernet, detección de colisiones e inyección de bits en la red.

TIA: Asociación de la Industria de las Telecomunicaciones. Organización que desarrolla estándares relacionados con las tecnologías de telecomunicaciones.

Tunneling: Arquitectura que está diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.

Tarjeta de Interfaz de Red: (NIC). Dispositivo a través del cual computadoras de una red transmiten y reciben datos.

TCP/IP: (Transmisor Control Protocol/Internet Protocol). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

Telnet: Protocolo que permite al usuario de Internet conectarse y escribir comandos en un equipo remoto vinculado a Internet como si el usuario estuviera utilizando un terminal de texto conectado directamente al equipo. Forma parte del conjunto de protocolos TCP/IP.

Tiempo Real: Método para procesar la información en cuanto se recibe.

U

Unicast: En redes conmutadas ethernet, transferencia de archivos/paquetes entre dos entidades. Una difusión única puede iniciarla un servidor a una estación de trabajo, una estación a un servidor, una estación a una impresora o cualquier otra unidad única hacia otra entidad

UPS: (Uninterruptible Power Supply ó Suministro de Energía Ininterrumpida). Es un estabilizador electrónico que está preparado para suplir al computador cuando se presenten caídas de energía o cambios de voltaje.

URL: (Universal Resource Locator ó Localizador de Recursos Universal). Identifica de manera única la ubicación de un equipo, directorio o archivo en Internet. La dirección URL también indica el protocolo de Internet apropiado, como HTTP o FTP. Por ejemplo: http://www.microsoft.com.

USB: Tecnología que facilita la conexión de periféricos a la computadora. Esta reconoce automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo, ya que se conecta a la parte trasera de la PC a un enchufe especial (puerto USB). La tarjeta madre debe tener esta tecnología en su CHIPSET para poder conectar dispositivos de este tipo.

UTP: Cable de para trenzado no apantallado, lo que significa que no tiene envoltura alrededor del grupo de conductores. Estos cables se usan principalmente en redes de voz y datos

Usuario: Cualquier individuo que interactúa con el computador a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con el computador a nivel profesional.

V

Vector: Segmento de datos de un mensaje SNA. Un vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

Virtualización: Proceso que se usa para implementar una red basada en segmentos de red virtuales. Los dispositivos se conectan a segmentos virtuales independientemente de su ubicación física y de su conexión física con la red.

VLAN: LAN virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.

VLSM: Máscara de subred de longitud variable. Capacidad de especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

VTP: Protocolo de terminal virtual. Aplicación ISO para establecer una conexión de terminal virtual a través de una red.

Virus: Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan, se propagan a través de cualquier medio de almacenamiento, o a través de la LAN, o de la misma Internet.

W

WAN: Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

WorkGroup Director: Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroup Director se ejecuta en estaciones de trabajo UNIX, ya sea como una aplicación independiente o integrada con otra plataforma de administración de red basada en SNMP, brindando un sistema de gestión poderoso y transparente para los productos de grupo de trabajo de Cisco.

WWW: World Wide Web. Gran red de servidores de Internet la cual suministra servicios de hipertexto y otros a terminales que ejecutan aplicaciones de clientes como, por ejemplo, un navegador de Web. Ver también navegador de Web.

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.

X

X Windows: Protocolo que interconecta estaciones de trabajo de interfaz gráfica de usuario con programas servidores de aplicaciones que utiliza TCP/IP

Z

Zona de autoridad: Asociada con DNS, la zona de autoridad es una sección del árbol del nombre de dominio para el que un servidor de nombre es la autoridad.