ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMATICA

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"GUIAS PRÁCTICAS DE LABORATORIOS DE NETWORKING DE ACUERDO AL PENSUM VIGENTE PARA LA CARRERA DE INGENIERIA DE SISTEMAS"

WELLINGTON FRANCISCO BARROS SANCHEZ

Sangolquí – Ecuador

2008

DEDICATORIA

A mis Padres, ya que sin su esfuerzo y sacrificio no hubiera podido llegar a culminar mi carrera.

A mi abuelita Mamita Piedad y mis hermanos Wello y Olivita porque siempre estuvieron a mi lado en todo momento apoyándome en lo que fuera necesario.

AGRADECIMIENTO

Un especial Agradecimiento a Dios, quien me ha acompañado y dado la fuerza necesaria para vencer las adversidades en toda mi vida.

A mis Padres, por su apoyo y su dedicación permanente. Gracias al ejemplo demostrado diariamente han hecho de mí un gran profesional; los quiero mucho.

Agradezco a todas las personas que de manera directa e indirecta me han ayudado en la realización de esta tesis y especialmente al Ing. Carlos Romero e Ing. Marcelo Núñez

Agradezco de todo corazón a una persona que estuvo desde el inicio de mi carrera hasta la culminación de la misma, apoyándome en esos momentos difíciles cuando más la necesitaba, gracias Anita Valeria.

PROLOGO

La presente tesis como objetivo desarrollar guías de laboratorios de acuerdo al pensum de la Carrera de Ingeniería de Sistemas para manejo y administración de redes basadas en simuladores o con los equipos necesarios para proporcionar a los estudiantes y docentes la facilidad de simular estos tipos de redes realizando su respectiva programación y poder analizar su funcionamiento.

Moodle un software libre que nos ayudara a implementar un cuestionario de preguntas para que se ejecute un estudio virtual o con las guías prácticas que se implementará, dejara a un lado el aprendizaje lo tradicional

INDICE DE CONTENIDOS

CAPITULO I

1.1. INTRODUCCIÓN 9

1.2. SITUACIÓN ACTUAL 9

1.3. JUSTIFICACIÓN 10

1.5. ALCANCE 11

1.6. HERRAMIENTAS 12

1.7. ESTUDIO DE FACTIBILIDAD 13

CAPITULO II

2.1. MODELO DE REFERENCIA OSI 15

2.2. PROTOCOLOS Y NIVELES 16

2.3. MODELO TCP-IP 18

2.4. Protocolos TCP/IP 20

2.5. Protocolos por capas 20

2.6. Protocolos de Internet 21

2.7. MODELO HÍBRIDO 23

2.8. COMPARACIÓN Y CRÍTICAS 23

2.9. ESTANDARIZACIÓN 26

2.10. CONSIDERACIONES DE DISEÑO 29

2.10.1. Metas del diseño 29

2.11. REDES DE COMUNICACIÓN 33

2.11.1. Por Procesamiento: 33

2.11.2. Por Cubrimiento 35

2.11.3. Por Topología 36

2.12. TIPOS DE CONEXIONES 39
2.12.1.Peer to peer 39
2.12.2.Cliente servidor 40
2.12.3.Mainframe 41
2.13. CLASIFICACIÓN DE LAS REDES DE DATOS 42
2.13.1.Según la tecnología de transmisión 42
2.13.2.Según el tamaño 42
2.14. VENTAJAS DE UNA RED DE DATOS Y CUANTIFICACIÓN DEL IMPACTO SOBRE LAS ORGANIZACIONES 42
2.15. ARQUITECTURA DE LOS ESTÁNDARES IEEE 802 43
2.15.1.División del protocolo IEEE 802 43
2.15.1.1.ETHERNET 802.3 44
2.16. PROTOCOLOS DE ACCESO AL MEDIO (MAC) 45
2.17. CSMA/CD 47
2.18. REDES WLAN 802.11 49
2.18.1.Redes inalámbricas 50
2.18.2.CSMA/CA 51
2.19. ESTRUCTURA DE LA TRAMA ETHERNET 52
2.19.1.La trama Ethernet 52
2.19.2.VLANS 54
2.20. SIMULACIONES DE PRÁCTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER 55
2.20.1.Interfaces y Escenario del Packet Tracer 55
2.20.1.1.Interfaz Standard 56
2.20.1.2.Herramientas 57

2.20.1.3.Dispositivos 57

2.20.1.4.Tráfico 58

2.20.1.5.Explicación del software Packet Tracer 5.0 59

CAPITULO III

3.1. PROTOCOLOS E INTERCONEXION DE REDES 97

3.2. Dispositivos de interconexión de redes. 97

3.2.1. Repetidores 97

3.2.2. Concentradores (Hubs) 99

3.2.3. Puentes (Bridges) 101

3.2.4. ROUTER 105

3.2.5. B-routers 113

3.2.6. Pasarelas (Gateways) 113

CAPITULO IV

4.1. SERVICIOS DE RED 117

4.2. PROTOCOLOS WAN 118

4.2.1. Servicios de conmutación de circuitos 119

4.2.2. Servicios de conmutación de paquetes 119

4.2.3. Capa de Enlace de Datos: Protocolos WAN 120

4.3. CUESTIONARIO DE PREGUNTAS CON MOODLE 121

4.4. ¿QUÉ ES MOODLE? 130

4.4.1. Entornos virtuales de aprendizaje 130

4.4.2. Software libre 131

4.4.3. Características Principales 131

4.4.4. Acceso al sistema o aula virtual 132
4.5. SOFTWARE GENERADOR DE PRUEBAS 133
4.5.1. INTRODUCCIÓN..... 133
4.5.1.1.Interfaz Web 133
4.5.1.2.Creación de preguntas 134
Guía de práctica: Realizar una red Frame Relay utilizando enrutamiento estático 145
Guía de práctica: Realizar una red Frame Relay utilizando enrutamiento dinámico RIP..... 162
Guía de práctica: Realizar un test para una red Frame Relay 178
Guía de práctica: Realizar una red PPP con autentificación CHAP utilizando enrutamiento estático 186
Guía de práctica: Realizar una red PPP con autentificación CHAP utilizando enrutamiento dinámico 197
Guía de práctica: Completar la actividad realizando encapsulamiento PPP con autentificación CHAP..... 209
Guía de práctica: Realizar una red utilizando enrutamiento dinámico OSPF ... 218
Guía de práctica: Completar la actividad realizando enrutamiento OSPF..... 240
Guía de práctica: Realizar dos redes distintas en diferentes interfaces del Packet Tracert con el fin de poderlas comunicar con el MULTIUSER CONECTIO 249
Guía de práctica: Realizar dos redes distintas en diferentes interfaces del Packet Tracer con el fin de poderlas comunicar con el MULTIUSER CONECTION..... 256

CAPITULO V

5.1. CONCLUSIONES..... 263

5.2. RECOMENDACIONES 264

CAPÍTULO I

1.1. INTRODUCCIÓN

El desarrollo de las TIC's ha permitido una rápida convergencia de las telecomunicaciones, captura, transporte almacenamiento y procesamiento de información. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan disponer de medios de comunicación efectivos para controlar su gestión, simplemente oprimiendo una tecla. En cuanto mayor es nuestra habilidad para recolectar, procesar y distribuir información, la demanda de procesamientos más sofisticados crece con mayor rapidez.

El presente trabajo tiene la finalidad de desarrollar guías prácticas de laboratorio que brinde tanto a estudiantes como docentes, la facilidad de comprender como se administran ciertos dispositivos y tecnologías mediante simuladores y equipos relacionados.

Por lo expuesto, el presente documento describirá lo concerniente a un método de aprendizaje práctico en el área de redes, resaltando las ventajas y la productividad que esto representa tanto para el estudiante como para el maestro.

1.2. SITUACIÓN ACTUAL

En la currícula de la carrera de Ingeniería de Sistemas e Informática, actualmente cuenta con asignaturas de REDES, la cual se basa en un temario y no disponen guías prácticas de laboratorios donde el estudiante tenga la facilidad, de desarrollar dicho tema.

Razón por la cual se ve la necesidad de implementar guías practicas de laboratorios para REDES con el fin de que el estudiante como el docente tengan la facilidad de simular dichas redes y tener un mejor entendimiento de cómo funcionaría la aplicación realizada.

1.3. JUSTIFICACIÓN

Las necesidades de tener equipos interconectados en una amplia área geográfica, exige a las empresas y personas en particular, disponer de su escaso tiempo para prepararse para vivir en un mundo competitivo, que hace que los profesionales tengan que capacitarse continuamente, y para lograr esto, se han ido creando nuevas técnicas y herramientas.

Se ha dejado a un lado el aprendizaje tradicional donde el maestro impartía cátedras en forma teórica, y el alumno se limitaba a aprender de él. Hoy por hoy, se le ha dado una responsabilidad más grande al alumno, el maestro se ha convertido en un guía, que enseña al alumno el camino a seguir y éste por sus medios, ya sea con la herramienta o simulador debidamente establecido o con los equipos necesarios para dicha práctica con el fin de alcanzar su meta de aprender y estar a la par con la competencia que tiene alrededor ya que se puede efectuar lo mismo en la vida profesional.

Es necesario entonces para estudiantes y docentes, disponer de guías prácticas de laboratorios que brinde todas las ventajas, con el apoyo de un tutorial que lleve un seguimiento personalizado por parte de los estudiantes, que no tienen la necesidad de estar ligados a un horario. El presente proyecto tiene por objetivo dar ese soporte a los estudiantes y docentes mediante guías prácticas que contenga detalladamente el temario de la asignatura

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

DESARROLLAR GUIAS PRÁCTICAS DE LABORATORIOS PARA NETWORKING DE ACUERDO AL PENSUM VIGENTE PARA LA CARRERA DE INGENIERIA DE SISTEMAS

1.4.2. OBJETIVOS ESPECÍFICOS

- Analizar los requerimientos funcionales y lo que se necesitan para llevar a cabo una simulación para un aprendizaje efectivo.

- Definir las posibles prácticas para cada temario.

- Determinar las características primordiales de la red a simular, para ser aplicada posteriormente en la implementación con la ayuda de las guías prácticas del tema analizado.

- Analizar cada uno de los comandos que se implementaran en la simulación con la ayuda del docente interpretando la guía práctica adquirida.

- Realizar la implementación práctica, en base a los requerimientos que se han encontrado.

1.5. ALCANCE

Desarrollar guías de laboratorios de acuerdo al pensum de la Carrera de Ingeniería de Sistemas para manejo y administración de redes basadas en simuladores o con los equipos necesarios para proporcionar a los estudiantes y

docentes la facilidad de simular estos tipos de redes realizando su respectiva programación y poder analizar su funcionamiento.

Las guías prácticas que se implementará, dejara a un lado el aprendizaje lo tradicional; entre los ítems que se desarrollarán se tiene:

- Introducción, análisis, diseño e implementación de los contenidos de la unidad.
- Introducción de cada uno de los temas detallando lo más relevante.
- Implementación práctica mediante los equipos o simuladores para desarrollar dicho tema.
- El alumno tendrá contacto con los equipos necesarios para dicha simulación, con la ayuda de la guía práctica.
- Analizar los comandos respectivos vistos en la simulación con la ayuda del docente.
- Entender el funcionamiento operacional de la red.
- Foros de debate por parte de los alumnos analizando la funcionalidad de la red.

Básicamente comprenderá todos los temas que se manejan dentro de la asignatura, con la ayuda de las guías prácticas correspondiente al tema.

1.6. HERRAMIENTAS

- Packet Tracer 5.0
- Boson NetSim for CCNP v6.0 Beta3b
- Router SIM
- Dos routers CISCO 2600

- Un switch 3 com
- Un switch CISCO Catalyst 3650
- Un Switch HP

1.7. ESTUDIO DE FACTIBILIDAD

1.7.1. FACTIBILIDAD TÉCNICA

Para el desarrollo de este proyecto de investigación, se utilizará software libre como el Packet Tracer 5.0

La realización de las guías será ejecutada en los computadores personales del autor, no siendo necesaria la adquisición de nuevos.

Características Técnicas de los computadores a usarse:

1) Laptop HP PAVILION zx5000
   Pentium IV de 3.06 GHz
   Memoria RAM de 512 MB
   Disco Duro de 80 GB
   Tarjeta de red 10/100 mbps.
   Tarjeta de red Wireless incorporada
   CD-ROM/ DVD-ROM
   Puertos USB

2) Computadora de escritorio:
   Pentium IV de 2.0 GHz
   Memoria RAM de 512 MB

Disco Duro de 80 GB

Tarjeta de red 10/100 mbps.

Monitor CD-ROM, DVD-ROM, FLOPPY, etc.

1.7.2. FACTIBILIDAD ECONÓMICA

Descripción	Cantidad	Unidad	Valor Unitario	Valor Total
Software Gratuito	1	U	$ 0	$ 0
Materiales Varios	1	GLB	$ 100	$ 100
Una Persona para Desarrollo	4	Meses	$ 500	$ 2.000
			Total	**$ 2.100**

1.7.3. FACTIBILIDAD OPERATIVA

El desarrollo de la presente guía permitirá obtener mayor conocimiento de los temas vistos en clase, y así detectar posibles fallos en la estructura en una red y reaccionar a esos fallos de manera proactiva.

Por tanto el proyecto es factible ya que se posee las herramientas, los conocimientos y la disponibilidad para efectuarlo.

CAPÍTULO II

CONSIDERACIONES DE DISEÑO

Mediante la cobertura de este capítulo es importante que el estudiante tenga conocimientos básicos de cómo se componen las arquitecturas de una red.

2.1. MODELO DE REFERENCIA OSI

Este modelo posee 7 niveles:

- 3 niveles orientados a la aplicación: la aplicación, la presentación y la sesión.
- 1 nivel de transporte.
- 3 últimos niveles orientados a redes: el nivel de red, enlace de datos y físico.

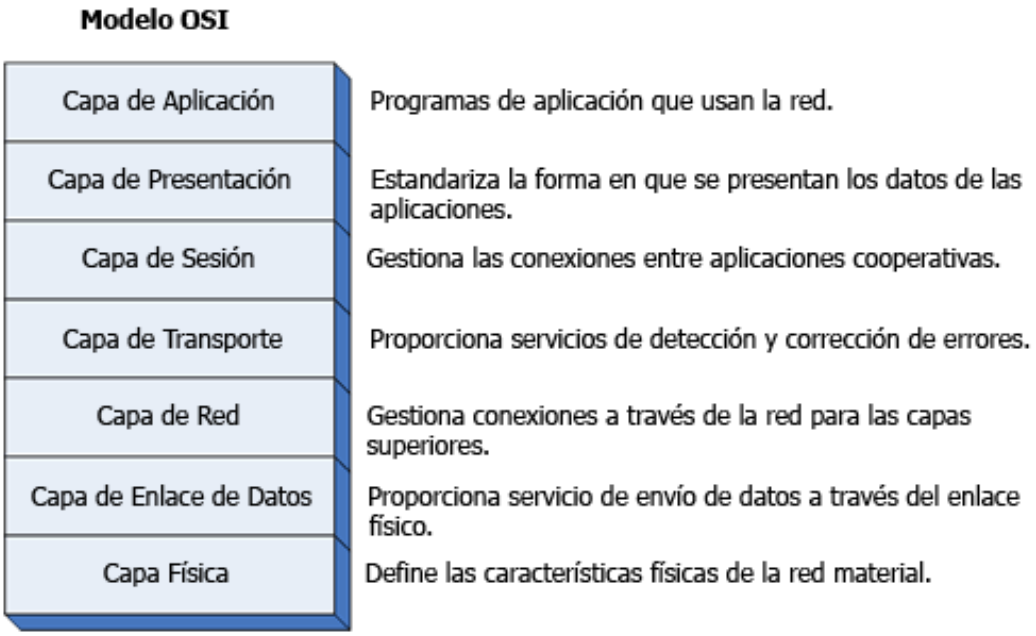

Figura 2.1.1 Modelo OSI

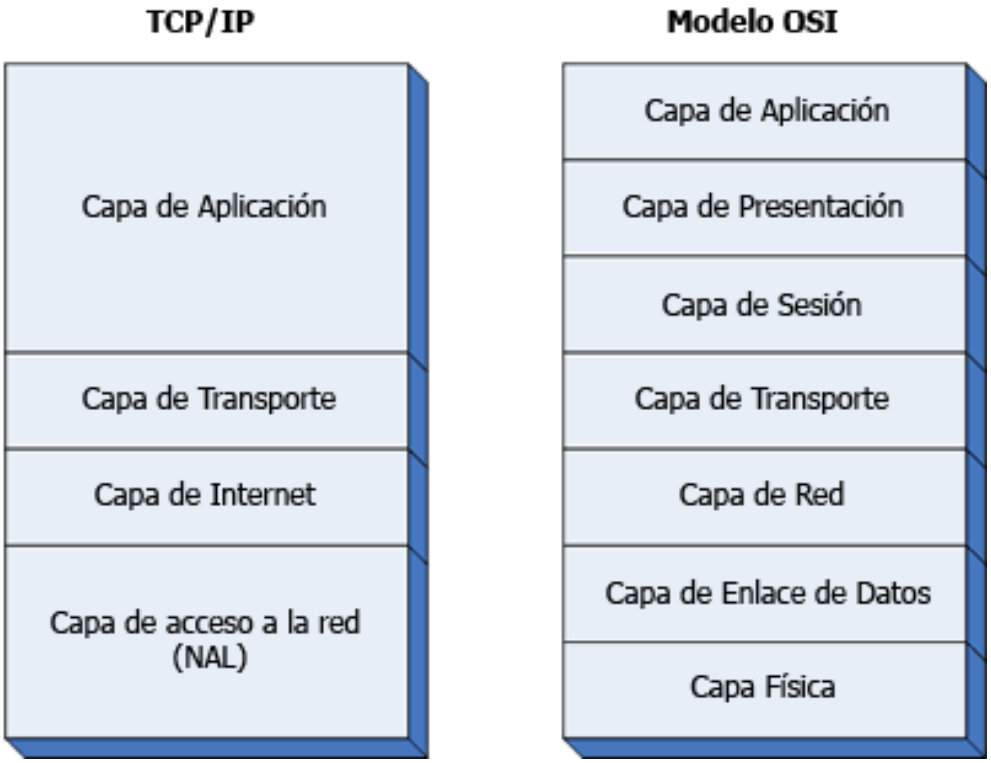

Figura 2.1.2 Modelos OSI y TCP/IP

2.2. PROTOCOLOS Y NIVELES

Niveles

La arquitectura TCP/IP consta de cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).
- Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

- Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- Capa de acceso a la Red: Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

Estos niveles se comunican entre sí a través de daemons (procesos).

Cada equipo que forme parte de la red tendrá implementados los niveles de Red si sigue el modelo OSI.

En diferentes ordenadores el nivel de aplicación solo podrá comunicares con el nivel de aplicación del otro ordenador, así para todos los niveles. Si algún equipo intermedio no tiene todos los niveles de red, el nivel que no esté presente tendrá una comunicación directa con el siguiente equipo que tenga el mismo nivel.

Esta comunicación se hace a través de un solo cable físico por lo tanto la comunicación entre aplicaciones se realiza de la siguiente forma:

- La aplicación realiza una escritura (write) y por lo tanto la aplicación que recibe la información ha de realizar una lectura (read).
- El nivel de presentación encapsula la información de la aplicación y le pone una cabecera con el control de errores y/o flujo creando el PDU del nivel de presentación.
- El nivel de sesión encapsula la PDU de presentación y añade su propia cabecera. La comunicación entre los diferentes niveles se realiza mediante una simple comunicación de procesos.

Así se va formando el PDU definitivo que llega al nivel de enlace, cuyo nivel encapsula el PDU de red le añade su cabecera y la trailer (final del PDU) y lo envía al nivel físico el cual convierte dicha información en señales eléctricas y las envía a través de la red física.

2.3. MODELO TCP-IP

Los niveles de este modelo son:

- Aplicación
- Transporte: TCP-UDP. El TCP ofrece un control de errores (OSI) pero el UDP no ofrece este control de errores, al no utilizar este control tarda menos en realizar la comunicación y por lo tanto es muy útil para aplicaciones en tiempo real.
- Interconexión: IP
- Orientados a red: puede tener todos los niveles que se quieran.

La comunicación entre IP y el nivel de red se realiza mediante drivers.
El nivel de Aplicación realiza las operaciones que se realizaban en los niveles Aplicación, Presentación, Sesión del modelo de referencia OSI.

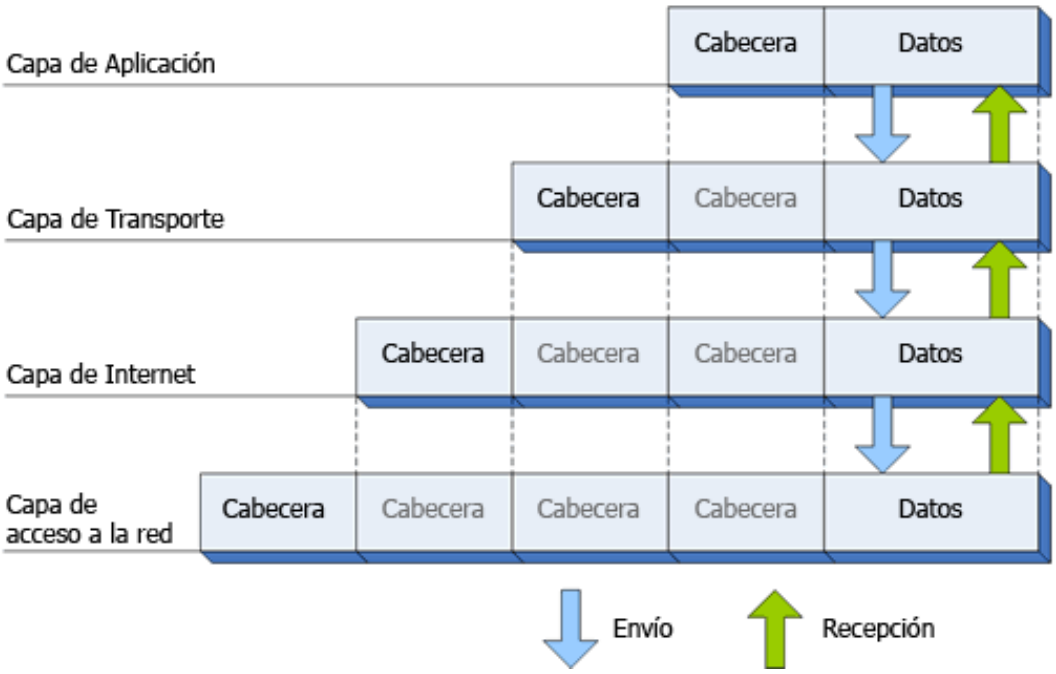

Tabla 2.3.1 Niveles TCP/IP

La arquitectura TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (datagram), y son conjuntos de datos que se envían como mensajes independientes.

2.4. Protocolos TCP/IP

- FTP (File Transfer Protocol). Se utiliza para transferencia de archivos.
- SMTP (Simple Mail Transfer Protocol). Es una aplicación para el correo electrónico.
- TELNET: Permite la conexión a una aplicación remota desde un proceso o terminal.
- RPC (Remote Procedure Call). Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.
- SNMP (Simple Network Management Protocol). Se trata de una aplicación para el control de la red.
- NFS (Network File System). Permite la utilización de archivos distribuidos por los programas de la red.

2.5. Protocolos por capas

TCP/IP, como la mayoría del software de red, está modelado en capas. Esta representación conduce al término pila de protocolos. Se puede usar para situar (pero no para comparar funcionalmente) TCP/IP con otras pilas, como SNA y OSI ("Open System Interconnection"). Las comparaciones funcionales no se pueden extraer con facilidad de estas estructuras, ya que hay diferencias básicas en los modelos de capas de cada una.

Los protocolos de Internet se modelan en cuatro capas, como se puede observar en la figura

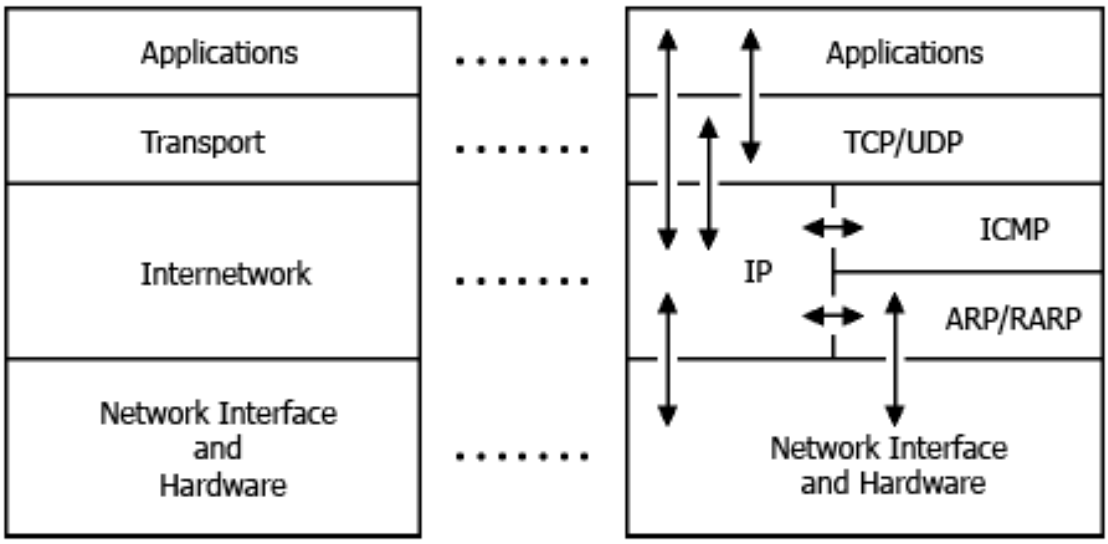

Figura 2.5.1 Protocolos de Internet

2.6. Protocolos de Internet

- Aplicación. Es a un proceso de usuario que coopera con otro proceso en el mismo o en otro host. Ejemplos son TELNET (un protocolo para la conexión remota de terminales), FTP ("File Transfer Protocol") y SMTP ("Simple Mail Transfer Protocol").
- Transporte. Proporciona la transferencia de datos de entre los extremos. Ejemplo son TCP (*orientado a conexión*) y UDP (*no orientado a conexión*).
- Internetwork. También llamada *capa de red*, proporciona la imagen de "red virtual" de Internet (es decir, oculta a los niveles superiores la arquitectura de la red). IP ("Internet Protocol") es el protocolo más importante de esta capa. Es un protocolo *no orientado a conexión que no asume la fiabilidad de las capas inferiores.* No suministra fiabilidad, control de flujo o recuperación de errores. Estas funciones debe proporcionarlas una capa de mayor nivel, bien de transporte con TCP, o de aplicación, si se utiliza UDP como transporte. Una unidad de un mensaje en una red IP se denomina

paquete. Es la unidad básica de información transmitida en redes TCP/IP networks.

- Network Interface. O *capa de enlace* o *capa de enlace de datos*, constituye la interfaz con el hardware de red. Esta interfaz puede proporcionar una entrega fiable, y puede estar orientada a flujo o a paquetes. De hecho, TCP/IP no especifica ningún protocolo aquí, pero puede usar casi cualquier interfaz de red disponible, lo que ilustra la flexibilidad de la capa IP. Ejemplos son IEEE 802.2, X.25 (que es fiable por sí mismo), ATM, FDDI, PRN ("Packet Radio Networks", como AlohaNet) e incluso SNA.

En la figura 2.6.1 Se puede observar el modelo arquitectónico.

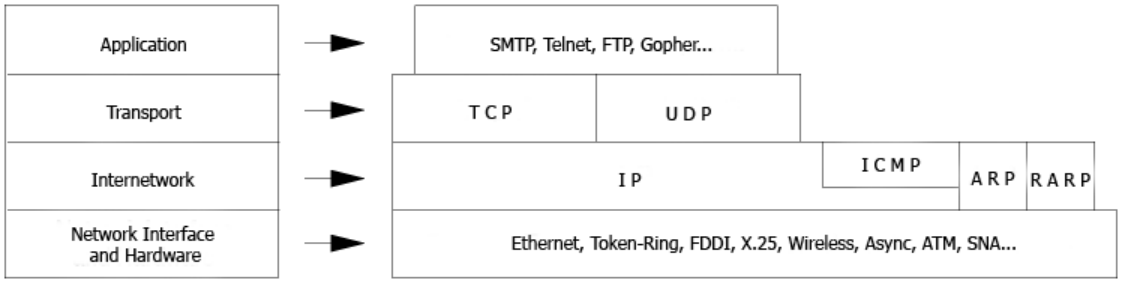

Figura 2.6.1 Modelo arquitectónico

La definición más elemental de una red de datos es la interconexión de dos computadoras cuyo fin principal es el de compartir datos.
Una red es un conjunto de computadoras interconectadas.

Los elementos que pueden ser compartidos en una red son los siguientes:

- Información
- Bases de Datos
- Mensajes y Agendas
- Impresoras
- Faxes
- Módems

Objetivos

- Modificación del viejo concepto de centro de cómputos a los sistemas basados en computadoras interconectadas.
- Viene de la mano de la miniaturización en electrónica.
- Computadoras + comunicaciones = redes de computadoras.
- Computadoras autónomas.
- Interconectadas para intercambiar información.
- Compartir recursos, equipos, información y programas que se encuentren geográficamente dispersos o locales.
- Brindar confiabilidad en la información.
- Transmitir información entre usuarios distantes de manera rápida, segura y económica.
- Obtener una buena relación coste/beneficio

2.7. MODELO HÍBRIDO

El modelo híbrido es el que mantiene el diseño del sitio web original pero cambia los contenidos según el público destinatario. En este modelo los administradores de webs preparan una misma plantilla para todas las lenguas (los mismos colores, tipos de letra, apartados, etc.) y sólo cambian los textos y los enlaces. A veces, sólo se adaptan en los textos cuestiones muy particulares, como por ejemplo las cantidades, los nombres de las personas de contacto o bien los enlaces originales.

2.8. COMPARACIÓN Y CRÍTICAS

TCP y OSI

Los modelos de referencia OSI y TCP/IP tienen mucho en común. Ambos se basan en el concepto de un gran número de protocolos independientes.
También la funcionalidad de las capas es muy similar. Por ejemplo, en ambos modelos las capas por encima de la de transporte, incluida ésta, están ahí para prestar un servicio de transporte de extremo a extremo, independiente de la red, a los procesos que deseen comunicarse. Estas capas forman el proveedor de transporte. También en ambos modelos, las capas encima de la de transporte son usuarios del servicio de transporte orientados a aplicaciones.
A pesar de estas similitudes fundamentales, los dos modelos tienen también muchas diferencias. Es importante notar que aquí estamos comparando los modelos de referencia, no las pilas de protocolos correspondientes.

En el modelo OSI son fundamentales tres conceptos:

1. Servicios.
2. Interfaces.
3. Protocolos.

Es probable que la contribución más importante del modelo OSI sea hacer explícita la distinción entre estos tres conceptos.
Cada capa presta algunos servicios a la capa que se encuentra sobre ella. La definición de servicio dice lo que la capa hace, no cómo es que las entidades superiores tienen acceso a ella o cómo funciona la capa.
La interfaz de una capa les dice a los procesos de arriba cómo acceder a ella; específica cuáles son los parámetros y qué resultados esperar; nada dice tampoco sobre cómo trabaja la capa por dentro.

Finalmente, los protocolos pares que se usan en una capa son asunto de la capa. Ésta puede usar los protocolos que quiera, siempre que consiga que se realice el trabajo (esto es, que provea los servicios que ofrece). La capa también puede cambiar los protocolos a voluntad sin afectar el software de las capas superiores.

Estas ideas ajustan muy bien con las ideas modernas acerca de la programación orientada a objetos. Al igual que una capa, un objeto tiene un conjunto de métodos (operaciones) que los procesos pueden invocar desde fuera del objeto. La semántica de estos métodos define el conjunto de servicios que ofrece el objeto. Los parámetros y resultados de los métodos forman la interfaz del objeto. El código interno del objeto es su protocolo y no está visible ni es de la incumbencia de las entidades externas al objeto.

El modelo TCP/IP originalmente no distinguía en forma clara entre servicio, interfaz y protocolo, aunque se ha tratado de reajustarlo después a fin de hacerlo más parecido a OSI. Por ejemplo, los únicos servicios reales que ofrece la capa de interred son enviar paquete IP y recibir paquete IP. Como consecuencia, en el modelo OSI se ocultan mejor los protocolos que en el modelo TCP/IP y se pueden reemplazar con relativa facilidad al cambiar la tecnología. La capacidad de efectuar tales cambios es uno de los principales propósitos de tener protocolos por capas en primer lugar.

El modelo de referencia se desarrolló antes de que se inventaran los protocolos. Este orden significa que el modelo no se orientó hacia un conjunto específico de protocolos, lo cual lo convirtió en algo muy general. El lado malo de este orden es que los diseñadores no tenían mucha experiencia con el asunto y no supieron bien qué funcionalidad poner en qué capa.

Por ejemplo, la capa de enlace de datos originalmente tenía que ver sólo con redes de punto a punto. Cuando llegaron las redes de difusión, se tuvo que insertar una nueva subcapa en el modelo. Cuando la gente empezó a constituir redes reales haciendo uso del modelo OSI y de los protocolos existentes, descubrió que no cuadraban con las especificaciones de servicio requeridas, de modo que se tuvieron que injertar en el modelo subcapas de convergencia que permitieran tapar las diferencias. Por último, el comité esperaba originalmente que cada país tuviera una red controlada por el gobierno que usara los

protocolos OSI, de manera que no se pensó en la interconexión de redes. Para no hacer el cuento largo, las cosas no salieron como se esperaba.

Lo contrario sucedió con TCP/IP: primero llegaron los protocolos, y el modelo fue en realidad sólo una descripción de los protocolos existentes. No hubo el problema de ajustar los protocolos al modelo, se ajustaban a la perfección. El único problema fue que el modelo no se ajustaba a ninguna otra pila de protocolos: en consecuencia, no fue de mucha utilidad para describir otras redes que no fueran del tipo TCP/IP.

Pasando de temas filosóficos a otros más específicos, una diferencia obvia entre los dos modelos es la cantidad de capas: el modero OSI tiene siete capas y el TCP/IP cuatro. Ambos tienen capas de red, de transpone y de aplicación, pero las otras capas son diferentes.
Otra diferencia se tiene en el área de la comunicación sin conexión frente a la orientada a la conexión. El modelo OSI apoya la comunicación tanto sin conexión como la orientada a la conexión en la capa de red, pero en la capa de transporte donde es más importante (porque el servicio de transporte es visible a los usuarios) lo hace únicamente con la comunicación orientada a la conexión. El modelo TCP/IP sólo tiene un modo en la capa de red (sin conexión) pero apoya ambos modos en la capa de transporte, con lo que ofrece una alternativa a los usuarios. Esta elección es importante sobre todo para los protocolos simples de petición y respuesta.

2.9. ESTANDARIZACIÓN

Estandarización

- Estándares de hecho (de facto)
- Estándares por ley (de jure)
- Estandarización de telecomunicaciones

    - Existen desde 1865
    - ITU (International Telecommunication Union (ex CCITT) agencia de las NNUU desde 1947)
- Sectores:
    - Radiocomunicaciones (ITU-R)
    - Estandarización de las telecomunicaciones (ITU-T)
    - Desarrollo (ITU-D)

Estandarización internacional

- ISO
    - International Standards Organization
    - Organizaciones de estandarización de 89 países
    - Intensa cooperación con ITU
    - Trabajo realizado por "voluntarios"
- IEEE
    - Institute of Electrical and Electronics Engineers, importantes estándares para redes locales
- Etapas de elaboración
    - Método de trabajo: amplio consenso
    - CD - Committee Draft
    - DIS - Draft International Standard
    - IS - International Standard

Estandarización de Internet

- Internet Society elige los miembros de:
    - IAB Internet Architechture Board
    - IRTF
        - Internet Research Borrad
    - IETF

        - Internet Engineering Task Force, que dirige el proceso de creación de estándares
    - RFC
        - Request For Comment (unas 2000)
        - "we reject kings and voting, we believe in rough consensus and running code"

Las *ventajas* de una estandarización son las siguientes:

- Estimula la competitividad (sino hay un monopolio los precios bajan y por lo tanto se facilita el acceso a los usuarios).
- Flexibilidad a la hora de instalar la red (puedes poner equipos de distintos fabricantes). Ejemplo: tarjetas de distintas marcas, etc.

Las *desventajas* son las siguientes:

- Los organismos de estandarización son muy lentos (3 o 4 años aproximados para declarar un estándar).
- Quien compone los organismos de estandarización (empresas: interés por no dejarse aventajar por la competencia; política: comunicación de los votos, universidades)
  Ejemplo: Ethernet! IEEE 802.3
  DIX (Digital-Intel-Xerox)
  Ethernet II! Compatible mediante protocolo
- Demasiados organismos de estandarización.

A continuación veremos unos organismos de estandarización:

- IEEE (Institution of Electrical and Electric Enginers): esta organización declaró el protocolo LAN pero no el LAN-ATM.
- EIA (Electrical Industries Asociation): declaró el cableado estructural.

- CCITT (International Telegraph and Telephone Consultatue Comitte): declaró la telefonía, actualmente esta absorbida por ITU (International Telecomunication Union), esta ultima declaró el ATM y la RDSI (comunicación digital)
- IETF (Internet Engineiring Task Force): declaró el protocolo de Internet.
- ISO (International Standard Org): Modelos de referencia.

2.10. CONSIDERACIONES DE DISEÑO

Diseñar una red siempre ha sido complejo, pero hoy en día la tarea es cada vez más difícil debido a la gran variedad de opciones. A continuación se examinarán las principales metas del diseño de una red, cuales son las prioridades que se adaptan al desarrollo de la red, entre otras cosas. Un efectivo administrador de la red es también un cuidadoso planeador.

2.10.1. Metas del diseño

El diseñador de la red debe siempre preguntarse algunas preguntas básicas de la red antes de que empiece la fase del diseño. ¿ Quién va a usar la red ? ¿ Qué tareas van a desempeñar los usuarios en la red? ¿ Quién va a administrar la red? Igualmente importante ¿ Quién va a pagar por ella? ¿ Quién va a pagar la mantenerla? Cuando esas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más productivo. Estas prioridades se convertirán en las metas del diseño. Vamos a examinar algunas de esas metas clave.

Desempeño (performance): Los tipos de datos procesados pueden determinar el grado de desempeño requerido. Si la función principal de la red es transacciones en tiempo real, entonces el desempeño asume una muy alta

prioridad y desafortunadamente el costo de eleva súbitamente en este trueque desempeño/costo.

Volumen proyectado de tráfico: Algunos equipos de interconexión como los puentes, concentradores pueden ocasionar cuellos de botella (bottlenecks) en las redes con tráfico pesado. Cuando se está diseñando una red se debe de incluir el número proyectado de usuarios, el tipo de trabajo que los usuarios harán, el tipo de aplicaciones que se correrán y el monto de comunicaciones remotas (www, ftp, telnet, VoIP, realaudio, etc). ¿Podrán los usuarios enviar ráfagas cortas de información o ellos podrán enviar grandes archivos? Esto es particularmente importante para determinar el monto de gráficas que se podrán transmitir sobre la red. Si bien un diseñador de red no puede predecir el futuro, éste debe de estar al tanto de las tendencias de la industria. Si un servidor de fax o email va a hacer instalado en la red, entonces el diseñador deberá de anticipar que estos nuevos elementos no afecten grandemente al volumen actual de tráfico de la red.

Expansión futura: Las redes están siempre en continuo creciendo. Una meta del diseño deberá ser planear para el crecimiento de la red para que las necesidades compañía no saturen en un futuro inmediato. Los nodos deberán ser diseñados para que estos puedan ser enlazados al mundo exterior. ¿Cuántas estaciones de trabajo puede soportar el sistema operativo de red? ¿La póliza de precios del vendedor de equipos hace factible la expansión futura? ¿El ancho de banda del medio de comunicación empleado es suficiente para futuro crecimiento de la red? ¿El equipo de comunicaciones tiene puertos disponibles para futuras conexiones?

Seguridad: Muchas preguntas de diseño están relacionadas a la seguridad de la red. ¿Estarán encriptados los datos? ¿Qué nivel de seguridad en los passwords es deseable? ¿Son las demandas de seguridad lo suficientemente grandes para requerir cable de fibra óptica? ¿Qué tipos de sistema de respaldo son requeridos para asegurar que los datos perdidos siempre puedan ser

recuperados? Si la red local tiene acceso a usuarios remotos, ¿Que tipo de seguridad será implementada para prevenir que hackers entren a nuestra red?

Redundancia: Las redes robustas requieren redundancia, sí algún elemento falla, la red deberá por sí misma deberá seguir operando. Un sistema tolerante a fallas debe estar diseñado en la red, de tal manera, si un servidor falla un segundo servidor de respaldo entrará a operar inmediatamente. La redundancia también se aplica para los enlaces externos de la red. Los enlaces redundantes aseguran que la red siga funcionando en caso de que un equipo de comunicaciones falle o el medio de transmisión en cuestión. Es común que compañías tengan enlaces redundantes, si el enlace terrestre falla (por ejemplo, una línea privada), entra en operación el enlace vía satélite o vía microondas. Es lógico que la redundancia cueste, pero a veces es inevitable.

Compatibilidad - hardware & software: La compatibilidad entre los sistemas, tanto en hardware como en software es una pieza clave también en el diseño de una red. Los sistemas deben ser compatibles para que estos dentro de la red puedan funcionar y comunicarse entre sí, por lo que el diseñador de la red, deberá tener cuidado de seleccionar los protocolos mas estándares, sistemas operativos de red, aplicaciones (como un simple procesador de palabras). Así como de tener a la mano el conversor de un formato a otro.

Compatibilidad - organización & gente: Ya una vez que la red está diseñada para ser compatible con el hardware y software existente, sería un gran error si no se considera la organización y el personal de la compañía. A veces ocurre que se tienen sistemas de la más alta tecnología y no se tiene el personal adecuado para operarlos. O lo contrario, se tiene personal con amplios conocimientos y experiencia operando sistemas obsoletos. Para tener éxito, la red deberá trabajar dentro del marco de trabajo de las tecnologías y filosofías existentes.

Costo: El costo que implica diseñar, operar y mantener una red, quizá es uno de los factores por los cuales las redes no tengan la seguridad, redundancia, proyección a futuro y personal adecuado. Seguido ocurre que las redes se adapten al escaso presupuesto y todas las metas del diseño anteriores no se puedan implementar. Los directivos, muchas veces no tienen idea del alto costo que tiene un equipo de comunicaciones, un sistema operativo para múltiple usuarios y muchas veces no piensan en el mantenimiento. El costo involucrado siempre será un factor importante para el diseño de una red.

En la figura 2.10.1.1 es un diagrama de 4 pasos en el proceso de construcción e implementación de una red.

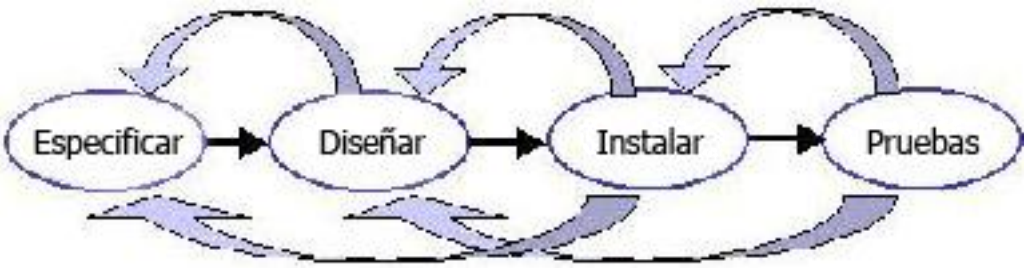

Figura 2.10.1.1

El paso de **Especificación de Requerimientos** es la etapa preliminar y es donde se especifican todos los requerimientos y variables que van a estar presentes en el diseño de una red. La Fase de Diseño, toma los elementos de la Especificación para diseñar la red en base a las necesidades de la organización. Cualquier punto no previsto se revisa y se lleva a la fase anterior de Especificación de Requerimientos. La fase de Instalación se toma "los planos" de la fase de diseño y se empiezan a instalar físicamente los dispositivos y elementos de la red. Cualquier imprevisto se regresa nuevamente a la fase de Diseño o en su caso a la fase de Especificación. La fase de Pruebas es la fase final del proceso y consiste en realizar toda clase de pruebas a la red ya instalada para comprobar o constatar que cumple con las Especificaciones de Requerimientos. Ya realizadas las pruebas con éxito la red está lista para su uso. Cualquier imprevisto, se regresa a las fases anteriores.

2.11. REDES DE COMUNICACIÓN

Una red de comunicación es un esquema de conexión física y lógica, sobre la cual se enlazan varias estaciones, redes o dispositivos de red, con varios fines como:

- Compartir un recurso de hardware y software.
- Procesar información común a todas las estaciones.
- Ejecutar programas multiusuario.
- Anunciar servicios de Internet/intranet (Internet): FTP, Correo, World Wide Web, entre otros.

Las redes se pueden agrupar bajo muchos nombres los cuales representan una característica particular de la red, estos nombres han sido estandarizados por las organizaciones que controlan y emiten las normas, como IETF, ANSI, TIAJE1A, IEEE, CCITT (1TU-T).

Las clasificaciones más importantes son:

- Por el tipo de procesamiento: de procesamiento central y de procesamientos distribuido.
- Por el cubrimiento: Redes de Área Local LAN, redes de área metropolitana MAN y redes de área extendida WAN.
- Por la topología: Bus (Ethernet), Anillo (Token-ring)

2.11.1. Por Procesamiento:

Se clasifican en sistemas de procesamiento central y de procesamiento distribuido.

De Procesamiento Central

Es el sistema de procesamiento que utiliza un anfitrión o Host. El anfitrión se define típicamente en el modelo de computadora centralizada como un sistema informático de tiempo compartido con el que los terminales se comunican y sobre el que descargan el procesamiento. En el entorno IBM, un sistema anfitrión consiste en una computadora central denominada 'Procesador Anfitrión', como el modelo AS400. Estas computadoras centrales ejecutan normalmente el sistema operativo MVS (Multiple Virtual Storage), XA (Extended Architecture) o ESA (Enterprise Systems Architecture). MVS forma parte de la arquitectura de aplicaciones de sistemas (SM, System Application Architecture) de IBM. La característica principal de este tipo de red, es que todo el procesamiento y almacenamiento de información se centraliza en un equipo, que es muy fuerte en este sentido y posee todas la arquitectura adecuada para ejecutar esta tarea en la forma más eficiente.

De Procesamiento Distribuido

En el modelo cliente-servidor, los usuarios trabajan en computadoras denominadas sistemas frontales (front-end) e interaccionan con sistemas servidores denominados posteriores (back-end), que proporcionan servicios tales como el acceso a una base de datos, la gestión de red y el almacenamiento centralizado de archivos. Una red de computadoras ofrece la plataforma de comunicación en la que numerosos clientes pueden interactuar con uno o más servidores. La interacción entre la aplicación que ejecutan los usuarios en sus sistemas frontales y el programa (generalmente una base de datos o un sistema operativo de red) en el servidor posterior se denomina relación cliente-servidor. Esto implica que el usuario dispone de una computadora con su propia capacidad de procesamiento, que ejecuta un programa que puede efectuar la interacción con el usuario y la presentación de la información.

El modelo cliente-servidor se aplica a sistemas operativos de red (NOS). Los sistemas operativos de red, tales como Netware de Novell y Windows NT de Microsoft, están orientados a este modelo puesto que los usuarios situados en las estaciones de trabajo realizan peticiones a los servidores de red.

Estos sistemas operativos ofrecen servicios complementarios e igualmente importantes y hasta imprescindibles en muchos casos, como son los servidores de comunicación con servicios como:

- Servidor de correo, para mensajería interna, y hacia servidores de correo público en ISP.
- Servidor de Web, para publicación de páginas html www, de acceso interno y externo desde cualquier sitio en Internet.
- FTP para descargas seguras de archivos desde la red interna o desde Internet.
- DHCP para realizar dinámicamente direcciones IP a los host dentro de toda la red.
- DNS para resolver nombres o traducir nombres en direcciones IP.
- Proxy para compartir la conexión y dar seguridad al acceso desde Internet, permite abrir sólo los puertos TCP/UDP necesarios para cada estación y definir filtros para salida y utilización de protocolos.

2.11.2. Por Cubrimiento

Se clasifican en LAN, MAN y WAN

Redes de área local (LAN)

Es un segmento de red con estaciones de trabajo y servidores enlazados, o un conjunto de segmentos de red interconectados, por lo general dentro de la misma área como por ejemplo un edificio. La interconexión entre los equipos de

la LAN, se realiza a través de sistemas de cableado estructurado, utilizando como bus activo arreglos de hub o switch.

Redes de Área Metropolitana (MAN)

Es una red que se extiende sobre áreas de ciudades o municipios, y que se interconecta mediante la utilización de facilidades MAN proporcionadas por la compañía de telecomunicaciones local.
Redes de Área Extensa (WAN) Redes que cruzan fronteras interurbanas, interestatales o internacionales. Los enlaces se realizan con los servicios públicos y privados de telecomunicaciones (líneas conmutadas, dedicadas, RDSI, fibra óptica), además de con los enlaces por satélites y microondas.
Hoy en día, se ha popularizado la utilización de las redes LAN y WAN. Los nombres de las redes MAN han adoptado el nombre de WAN, queriéndose decir con esto "o que no es LAN se considera WAN"

2.11.3. Por Topología

Por topología o configuración de interconexión, las redes se pueden clasifican en estrella, bus o anillo. Aunque la topología se refiere tanto a una disposición física como lógica, cuando nos refiramos a la topología de bus y de anillo, estaremos hablando de la disposición lógica.

Estrella

Las estaciones se unen a concentradores y las señales se difunden a todas las estaciones o se pasan de unas a otras. Véase la figura 2.11.3.1

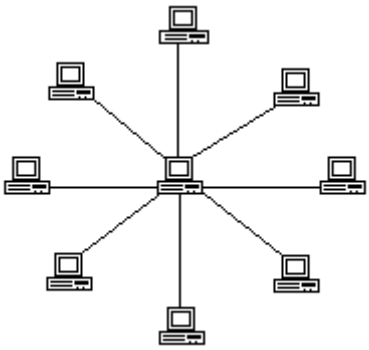

Figura 2.11.3.1 Topología estrella

BUS Ethernet

En esta topología, todos los elementos de la red están interconectados a través de un bus lógico, lo cual lleva a un funcionamiento muy particular. Este tipo de red está ubicada en el nivel de enlace de la capa OSI y se encuentra documentada en la norma Ethernet 802.3 de IEEE. Como el bus es compartido Ethernet necesita verificar la disponibilidad de la portadora (arbitrariedad), para esto se basa en el algoritmo carrier sense multiple access collison detect (CSMA/CD) "acceso múltiple por censado de portadora y detección de colisión", cuya función se resume en los siguientes pasos:

- Escucha y define si alguna trama se recibe.
- Si no hay ninguna trama en el bus Ethernet, entonces transmite.
- Si hay alguna trama en el bus Ethernet, espera y luego escucha de nuevo.
- Mientras está enviando, si una colisión ocurre, para, espera y escucha de nuevo.

Esta tecnología fue creada por Digital Equipement Corporation, Intel y Xerox, con lo cual se llamo inicialmente DIX Ethernet, luego la IEEE realizó mejoras importantes para hoy llamarse simplemente Ethernet, aunque el prefijo DIX no sobra. Véase figura 2.11.3.2

Figura 2.11.3.2 Topología bus

Las redes Ethernet aparecen bajo diferentes nombres, que no hacen más que indicar la velocidad, el tipo de señal a utilizar, el medio y la distancia máxima. Por ejemplo 10Base2, significa que opera a una velocidad de 10Mbps, en banda base, por coaxial y a una distancia máxima de 200métros. 10BaseT, significa 10Mbps, en banda base, por par trenzado y hasta 100 metros.

Ethernet no ha evolucionado tan rápido como los medio físicos que la sustentas, pero si ha alcanzado la suficiente velocidad como para responder a las necesidades de ancho de banda de las aplicaciones actuales. Los desarrollos en hardware y en quipos de concentración y suicheo, la han llevado a convertirse en la red LAN por excelencia. Su velocidad llega inclusive a 1Gigabit por segundo, en lo que se conoce como Gigabit Ethernet.

Anillo Token Ring

En este tipo de topología las señales se pasan de una estación a otra en círculo. La principal norma de esta topología es la red Token Ring. Véase la figura 2.11.3.4

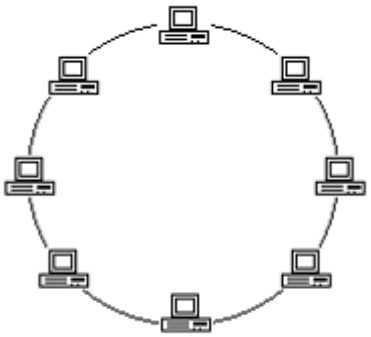

Figura 2.11.3.4 Topología Token Ring

Token Ring es un protocolo de nivel 2 creado por IBM y normalizado por la IEEE como 802.5. Su operación se basa en el paso de un testigo a través del anillo llevando y recogiendo información, como se describe en los siguientes pasos:

- Escucha cuando pasa el testigo.
- Si el testigo está ocupado, escucha al siguiente testigo.
- Si el testigo está libre (id/e), marca el testigo como ocupado (busy), adjunta los datos, y los envía por el anillo.
- Cuando el encabezamiento con el testigo en ocupado regresa al emisor de la trama, después de completar una vuelta completa a través del anillo, el emisor remueve los datos del anillo.
- El dispositivo envía un testigo libre para permitir que otra estación pueda enviar una trama.

Las velocidades de Token Ring son 4 y 16 bps, a pesar de ser una tecnología bastante prometedora en cuanto ancho de banda, no evolucionó lo esperado por lo costoso de su fabricación. Hoy en día, sólo se utiliza entorno IBM, pero con tendencia a desaparecer.

2.12. TIPOS DE CONEXIONES

2.12.1. Peer to peer

Es una red informática que se traduciría al español significa punto a punto, y más conocida como P2P [pedospe], se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comporten simultáneamente como clientes y como servidores de los demás nodos de la red.

Cualquier nodo puede iniciar, detener o completar una transacción compatible. La eficacia de los nodos en el enlace y transmisión de datos puede variar según su configuración local (cortafuegos, NAT, ruteadores, etc.), velocidad de proceso, disponibilidad de ancho de banda de su conexión a la red y capacidad de almacenamiento en disco.

Ventajas de una Red Punto a Punto

- Menos Cara de Implementar.
- No requiere software especializado adicional para la administración.
- No requiere un administrador de red dedicado.

Desventajas de una Red Punto a Punto

- No se puede escalar a redes grandes y la administración se vuelve inmanejable.
- Cada usuario debe ser entrenado para ejecutar tareas administrativas.
- Menos Segura.
- Todas las máquinas comparten recursos negativamente afectando el desempeño.

Figura 2.12.1.1 Punto a punto

2.12.2. Cliente servidor

El modelo cliente-servidor el cual se rige de una arquitectura monolítica donde no hay distribución de tareas entre sí, solo una simple comunicación entre un

usuario y una terminal en donde el cliente y el servidor no pueden cambiar de roles.

Ventajas de una Red Cliente – Servidor

- Provee mayor seguridad.
- Fácil de administrar cuando la red es grande porque la administración es centralizada.
- Todos los datos pueden ser almacenados en una localización central

Desventajas de una Red Cliente – Servidor

- Requiere software caro y especializado para la administración y operación de la red.
- Requiere máquinas servidores más potentes y caras.
- Requiere un administrador profesional.
- Tiene un solo punto de falla. Los datos de usuario no son disponibles si el servidor esta fuera de servicio (Caído)

Figura 2.12.2.1 Cliente servidor

2.12.3. Mainframe

Es una computadora central o mainframe muy potente y costosa usada principalmente por una gran compañía para el procesamiento de una gran cantidad de datos; por ejemplo, para el procesamiento de transacciones bancarias.

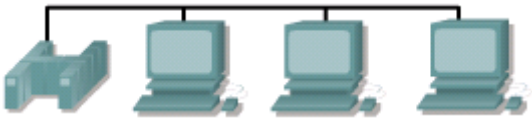

Figura 2.12.3.1 Mainframe

2.13. CLASIFICACIÓN DE LAS REDES DE DATOS

2.13.1. Según la tecnología de transmisión

a) Redes por difusión (broadcast networks)
   - Las estaciones comparten un canal (Ej. Ethernet)

b) Redes punto a punto
   - Enlaces entre equipos (Ej. Conexión por módem)

2.13.2. Según el tamaño

a) LAN (Redes de área local)
b) MAN (Redes de área metropolitana)
c) WAN (Redes de área amplia)

2.14. VENTAJAS DE UNA RED DE DATOS Y CUANTIFICACIÓN DEL IMPACTO SOBRE LAS ORGANIZACIONES

Ventajas

- Compartir recursos
- Aumento de la confiabilidad
- Ahorro (PCs versus Mainframes) Cliente – Servidor
- Escalabilidad
- Medio de comunicación

2.15. ARQUITECTURA DE LOS ESTÁNDARES IEEE 802

En 1980 el IEEE comenzó un proyecto llamado estándar 802 basado en conseguir un modelo para permitir la intercomunicación de ordenadores para la mayoría de los fabricantes. Para ello se enunciaron una serie de normalizaciones que con el tiempo han sido adaptadas como normas internacionales por la ISO. El protocolo 802 está dividido según las funciones necesarias para el funcionamiento de las redes LAN. Cada división se identifica por un número: 802.x:

2.15.1. División del protocolo IEEE 802

- **IEEE 802.** Descripción general y arquitectura.
- **IEEE 802.1** Glosario, gestión de red e Internet working. Relación de estándares, gestión de red, interconexión de redes.
- **IEEE 802.2** Control de enlace lógico (LLC).
- **IEEE 802.3** CSMA/CD. Método de acceso y nivel físico. Ethernet.
- **IEEE 802.4** Token Bus. Método de acceso y nivel físico. Bus con paso de testigo.
- **IEEE 802.5** Token Ring. Método de acceso y nivel físico. Anillo con paso de testigo.
- **IEEE 802.6** Redes de área metropolitana (MAN)
- **IEEE 802.7** Banda Ancha. Aspectos del nivel físico.
- **IEEE 802.8** Recomendaciones fibra óptica.
- **IEEE 802.9** Acceso integrado de voz y datos. Método de acceso y nivel físico. Recomendaciones banda ancha (broadband) Integración voz y datos en LAN
- **IEEE 802.10** Seguridad y privacidad en redes locales. Seguridad
- **IEEE 802.11** Wireless LAN (Redes Inalámbricas). Método de acceso y nivel físico.

- **IEEE 802.12** 100VG-AnyLAN. Método de acceso y nivel físico. LAN's de alta velocidad (Fast Ethernet variante de 802.3)

2.15.1.1. ETHERNET 802.3

CSMA/CD, siglas que corresponden a **Carrier Sense múltiple Access with Collision Detection** (en español, "**Acceso Múltiple con Escucha de Portadora y Detección de Colisiones**"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por eso apareció primeramente la técnica CSMA, que fue posteriormente mejorada con la aparición de CSMA/CD.

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados.

El IEEE 802.3 también define un estándar similar con una ligera diferencia en el formato de las tramas. Todas las adaptaciones del estándar 802.3 tienen una velocidad de transmisión de 10 Mbps con la excepción de 1Base−5, el cual transmite a 1 Mbps pero permite usar grandes tramos de par trenzado. Las topologías más usuales son: 10Base−5; 10Base−2 y 10Base−T, donde el primer número del nombre señala la velocidad en Mbps y el número final a los metros por segmento (multiplicándose por 100). Base viene de banda base (baseband) y Broad de banda ancha (broadband).

Historia:

- Después de ALOHA y el desarrollo del sentido de portador, Xerox PARC construyó un sistema de CSMA/CD de 2,94 Mbps para conectar

más de 100 estaciones de trabajo en un cable de 1 km. Se llamaba Ethernet (red de éter).

- Xerox, DEC, e Intel crearon un estándar para un Ethernet de 10 Mbps. Esto fue el paso para 802.3, que describe una familia de protocolos de velocidades de 1 a 10 Mbps sobre algunos medios.

2.16. PROTOCOLOS DE ACCESO AL MEDIO (MAC)

Una red es un entorno en el que diferentes host y dispositivos comparten un medio de transmisión común. Es necesario por ello establecer técnicas que permitan definir qué host está autorizado para transmitir por el medio común en cada momento. Esto se consigue por medio de una serie de protocolos conocidos con el nombre de Control de Acceso al Medio (protocolos MAC).

Según la forma de acceso al medio, los protocolos MAC pueden ser:

- **Determinísticos**: en los que cada host espera su turno para transmitir. Un ejemplo de este tipo de protocolos determinísticos es Token Ring, en el que por la red circula una especie de paquete especial de datos, denominado **token**, que da derecho al host que lo posée a transmitir datos, mientras que los demás deben esperar a que quede el token libre.
- **No determinísticos**: que se basan en el sistema de "escuchar y transmitir". Un ejemplo de este tipo de protocolos es el usado en las LAN Ethernet, en las que cada host "escucha" el medio para ver cuando no hay ningún host transmitiendo, momento en el que transmite sus datos.

El MAC es el mecanismo encargado del control de acceso de cada estación al medio. El MAC puede realizarse de forma distribuida cuando todas las

estaciones cooperan para determinar cuál es y cuándo debe acceder a la red. También se puede realizar de forma centralizada utilizando un controlador.

El esquema centralizado tiene las siguientes ventajas:

- Puede proporcionar prioridades, rechazos y capacidad garantizada.
- La lógica de acceso es sencilla.
- Resuelve conflictos entre estaciones de igual prioridad.

Los principales inconvenientes son:

- Si el nodo central falla, falla toda la red.
- El nodo central puede ser un cuello de botella.

Las técnicas de control de acceso al medio pueden ser síncronas o asíncronas.

- Las síncronas hacen que la red se comporte como de conmutación de circuitos, lo cual no es recomendable para LAN y WAN.
- Las asíncronas son más aceptables ya que las LAN actúan de forma impredecible y por tanto no es conveniente el mantenimiento de accesos fijos. Las asíncronas se subdividen en 3 categorías: rotación circular, reserva y competición.
    - Rotación circular: se va rotando la oportunidad de transmitir a cada estación, de forma que si no tiene nada que transmitir, declina la oferta y deja paso a la siguiente estación. La estación que quiere transmitir, sólo se le permite una cierta cantidad de datos en cada turno. Este sistema es eficiente cuando casi todas las estaciones quieren transmitir algo, de forma que el tiempo de transmisión se reparte equitativamente. Pero es ineficiente cuando sólo algunas estaciones son las que desean transmitir, ya que se pierde mucho tiempo rotando sobre estaciones que no desean transmitir.

- Reserva: esta técnica es adecuada cuando las estaciones quieren transmitir un largo periodo de tiempo, de forma que reservan ranuras de tiempo para repartirse entre todas las estaciones.
- Competición: en este caso, todas las estaciones que quieren transmitir compiten para poder hacerlo (el control de acceso al medio se distribuyen entre todas las estaciones). Son técnicas sencillas de implementar y eficientes en bajas cargas pero muy ineficientes para cargas altas (cuando hay muchas estaciones que quieren el acceso y además transmiten muchos datos).

2.17. CSMA/CD

Los protocolos de CSMA con la detección de choques son un mejoramiento sobre ALOHA porque aseguran que ninguna estación transmite cuando detecta que el canal está ocupado.

Un segundo mejoramiento es que las estaciones terminan sus transmisiones tan pronto como detectan un choque. Esto ahorra tiempo y ancho de banda. Los protocolos de esta clase se llaman CSMA/CD (Carrier Sense múltiple Access with Collision Detection, o CSMA con la detección de choques).

- Después de detectar un choque, una estación termina su transmisión, espera un período aleatorio, y trata de nuevo.
- Los choques ocurren en el *período de contienda*. La duración de este período determina el retraso y la utilización del canal.

El **CSMA/CD** funciona de la siguiente manera: cuando una computadora desea mandar información primero escucha el cable de la red para revisar que no se esté usando en ese preciso momento (Carrier-Sense). Esto se oye muy sencillo, pero el problema reside en que dos o más computadoras al escuchar que no se está usando el cable pueden mandar al mismo momento su información

(múltiple Access), y como solamente puede haber uno y sólo un mensaje en tránsito en el cable se produce una colisión. Entonces las computadoras detectan la colisión y deciden reenviar su información a un intervalo al azar, es importante que sea al azar ya que si ambas computadoras tuvieran el mismo intervalo fijo se produciría un ciclo vicioso de colisiones y reenvíos (Collision Detection). Así por ejemplo al detectar la colisión una computadora se espera tres milisegundos y la otra cinco milisegundos, siendo obvio que una computadora reenviara en primer lugar y la otra esperará a que el cable este de nuevo sin tránsito.

Evidentemente que en una misma red Ethernet al haber muchas computadoras tratando de enviar datos al mismo tiempo y/o al haber una transferencia masiva de datos se crea un gran porcentaje de colisiones y utilización. Si se pasa del 1% de colisiones y/o 15% de utilización de cable ya se dice que la red está saturada. Además, las señales de este tipo de red tienden a degradarse con la distancia debido a la resistencia, la capacidad u otros factores. Inclusive la señal todavía se puede distorsionar por las interferencias eléctricas exteriores generadas por los motores, las luces fluorescentes y otros dispositivos eléctricos. Cuanto más se aumenta la velocidad de transmisión de los datos. Más susceptible es la señal a degradarse. Por esta razón las normas de Ethernet especifican los tipos de cables, los protectores y las distancias del mismo, la velocidad de transmisión y otros detalles para trabajar y proporcionar un servicio relativamente libre de errores en la mayoría de los entornos.

Las redes Ethernet pueden utilizar diferentes tipos de cableado, cada uno con sus beneficios y problemas. Los tres cableados más comunes son Thinnet, Thicknet, y Twisted Pair (Par trenzado).

- **Thinnet ó 10Base2** puede transmitir datos a 10mbps por Banda Base (señales digitales), pudiendo llegar el cableado hasta 185 metros. Se utiliza cable coaxial RG-58 el cual es bastante barato por lo que a esta red también se le conoce como CheapNet. Un mismo

segmento de cable puede soportar hasta 30 computadoras. Es el más utilizado y recomendado para redes pequeñas. Utiliza la topología local bus, donde un mismo cable recorre todas y cada una de las computadoras.

- **Thicknet ó 10Base5** transmite datos a 10mbps por Banda Base en un cableado que puede alcanzar 500 metros. El cableado es grueso y es utilizado principalmente para largas oficinas o hasta todas las computadoras de un edificio. Del cable principal (backbone) salen cables usualmente Par Trenzado que se conectan a directamente a cada una de las computadoras. Se pueden conectar hasta 100 computadoras con este cableado en un mismo segmento.
- **Twisted Pair ó 10BaseT** transmite datos a 10mbps por Banda Base y utiliza un Hub (concentrador) desde el cual con cable Par Trenzado se conecta cada una de las computadoras quedando en forma similar a estrella. El Hub queda en el centro de la estrella y funciona como "repetidor". El cable desde el Hub hasta la computadora no debe de medir más de 100 metros.

2.18. REDES WLAN 802.11

Una LAN 802.11 está basada en una arquitectura celular, es decir, el sistema está dividido en celdas, donde cada celda (denominada **Basic Service Set**, **BSS**) es controlada por una Estación Base llamada Punto de Acceso (**AP**), aunque también puede funcionar sin la misma en el caso que las máquinas se comuniquen entre ellas. Los Puntos de Acceso de las distintas celdas están conectados a través de algún tipo de red troncal (llamado **Sistema de Distribución**).

La LAN inalámbrica completamente interconectada, incluyendo las distintas celdas, los Puntos de Acceso respectivos y el Sistema de Distribución es

denominada en el estándar como un **Conjunto de Servicio Extendido** (**Extended Service Set**, **ESS**).

En la figura 2.18.1 se puede observar las redes inalámbricas.

Figura 2.18.1 Redes Inalámbricas

2.18.1. Redes inalámbricas

802.11

- Fue especificada para trabajar a 1 y 2 Mbps, en la banda de los 2.4 GHz. Utiliza las técnicas FHSS (Frequency Hopping Spread Spectrum) o DSSS (Direct Sequence Spread Spectrum).

802.11b

- Es una extensión de 802.11 y trabaja también a 5.5 y 11 Mbps, trabaja a 2.4GHz. Utiliza CCK (Complementary Code Keying) con modulación QPSK (Quadrature Phase Shift Keying) y tecnología DSSS (Direct-Sequence Spread Spectrum). La recomendación 802.11b soporta cambios de velocidad dinámicos.

802.11a

- Es una extensión de 802.11b, y trabaja hasta 54 Mbps en la banda de los 5 GHz. Utiliza técnicas de multiplexación ortogonal por división de frecuencia (OFDM), en vez de FHSS o DSSS.

802.11g

- Es una extensión de 802.11b, y trabaja hasta 54 Mbps en la misma banda que 802.11b (2.4 GHz). Utiliza técnicas de multiplexación ortogonal por división de frecuencia (OFDM).

CSMA/CA (Carrier Sense Multiple Access with Collition Avoidance)

- En las redes inalámbricas es muy dificultoso utilizar mecanismos de detección de colisiones, y por lo tanto se utilizan mecanismos que aseguren la NO existencia de las mismas.
- Se utilizan protocolos del tipo "RTS" – "CTS" para asegurar la disposición del canal durante todo el período de transmisión.

2.18.2. CSMA/CA

Este tipo de problema se presenta cuando dos estaciones transmiten al mismo tiempo y lógicamente abra una colisión. Para solucionar este problema existen dos técnicas diferentes, que son dos tipos de protocolos CSMA: uno es llamado CA - Collision Avoidance, en castellano Prevención de Colisión y el otro CD - Collision Detection, Detección de Colisión. La diferencia entre estos dos enfoques se reduce al envío o no de una señal de agradecimiento por parte del nodo receptor:

- Collision Avoidance (CA): es un proceso en tres fases en las que el emisor:

1. Escucha para ver si la red está libre.
2. Transmite el dato.
3. Espera un reconocimiento por parte del receptor.

Este método asegura así que el mensaje se recibe correctamente. Sin embargo, debido a las dos transmisiones, la del mensaje original y la del reconocimiento del receptor, pierde un poco de eficiencia. Este método se utiliza en la red Ethernet.

2.19. ESTRUCTURA DE LA TRAMA ETHERNET

2.19.1. La trama Ethernet

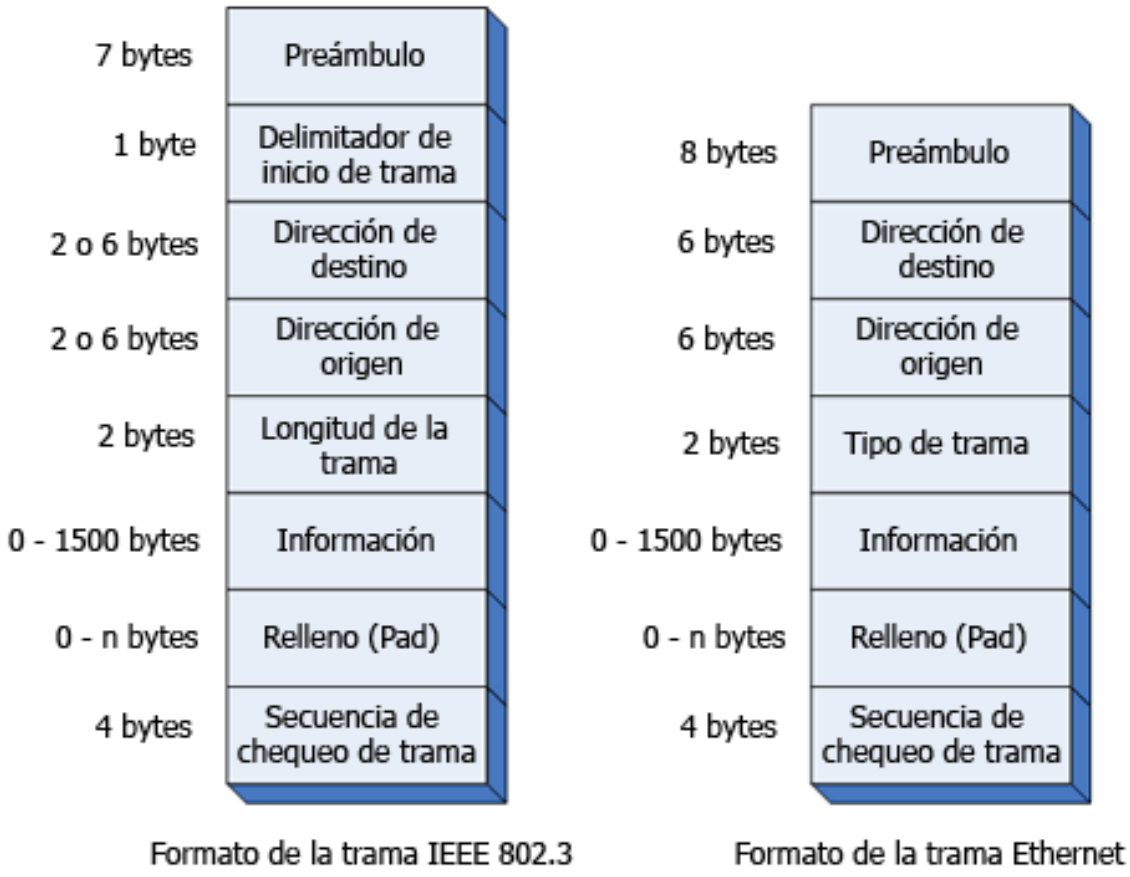

Figura 2.19.1.1 Estructura de la trama Ethernet

Los campos de trama Ethernet e IEEE 802.3 son los siguientes:

Preámbulo: el patrón de unos y ceros alternados les indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de trama (SOF) de la trama IEEE 802.3.

Inicio de trama (SOF): el byte delimitador de IEEE 802.3 finaliza con dos bits 1 consecutivos, que sirven para sincronizar las porciones de recepción de trama de todas las estaciones de la LAN. SOF se especifica explícitamente en Ethernet.

Direcciones destino y origen: vienen determinadas por las direcciones MAC únicas de cada tarjeta de red (6 bytes en hexadecimal). Los primeros 3 bytes de las direcciones son especificados por IEEE según el proveedor o fabricante. El proveedor de Ethernet o IEEE 802.3 especifica los últimos 3 bytes. La dirección origen siempre es una dirección de broadcast única (de nodo único). La dirección destino puede ser de broadcast única, de broadcast múltiple (grupo) o de broadcast (todos los nodos).

Tipo (Ethernet): el tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

Longitud (IEEE 802.3): la longitud indica la cantidad de bytes de datos que sigue este campo.

Datos (Ethernet): una vez que se ha completado el procesamiento de la capa física y de la capa de enlace, los datos contenidos en la trama se envían a un protocolo de capa superior, que se identifica en el campo tipo. Aunque la versión 2 de Ethernet no especifica ningún relleno, al contrario de lo que sucede con IEEE 802.3, Ethernet espera por lo menos 46 bytes de datos.

Datos (IEEE 802.3): una vez que se ha completado el procesamiento de la capa física y de la capa de enlace, los datos se envían a un protocolo de capa superior, que debe estar definido dentro de la porción de datos de la trama. Si los datos de la trama no son suficientes para llenar la trama hasta una cantidad mínima de 64 bytes, se insertan bytes de relleno para asegurar que por lo menos haya una trama de 64 bytes (tamaño mínimo de trama).

Secuencia de verificación de trama (FCS): esta secuencia contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el checksum de verificación de la trama, comprueba que los datos corresponden a un mensaje IP y entonces lo pasa a dicho protocolo (capa de red-Internet) para que lo procese.

Hay que destacar que las direcciones utilizadas por Ethernet no tienen nada que ver con las direcciones de Internet. Las de Internet se le asignan a cada usuario, mientras que las de Ethernet vienen de incluidas de fábrica en la tarjeta de red (NIC).

El formato de trama Ethernet que se utiliza en redes TCP/IP es algo diferente del estándar IEEE 802.3, aquí el campo Longitud no existe (las tarjetas son capaces de detectar automáticamente la longitud de una trama), y en su lugar se emplea el campo Tipo.

2.19.2. VLANS

Una red de área local (LAN) está definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos es el de no poder

tener una confidencialidad entre usuarios de la LAN como pueden ser los directivos de la misma, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no era aprovechado correctamente. La solución a este problema era la división de la LAN en segmentos físicos los cuales fueran independientes entre sí, dando como desventaja la imposibilidad de comunicación entre las LANs para algunos de los usuarios de la misma.
La necesidad de confidencialidad como así el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLANs.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación.

2.20. SIMULACIONES DE PRÁCTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

2.20.1. Interfaces y Escenario del Packet Tracer

Figura 2.20.1.1

Para una mayor comprensión y detalle se dividió las diferentes interfaces. En cada una se encuentra el detalle y uso de cada ítem.

2.20.1.1. Interfaz Standard

Figura 2.20.1.1.1

1) Nuevo / Abrir / Guardar / Imprimir / Asistente para actividades.
2) Copiar / Pegar / Deshacer.
3) Aumentar Zoom / Tamaño original / Reducir Zoom.
4) Dibujar figuras (cuadrados, círculos y líneas).
5) Panel de Dispositivos Personalizados: Sirve para agregar o quitar dispositivos personalizados.

2.20.1.2. Herramientas

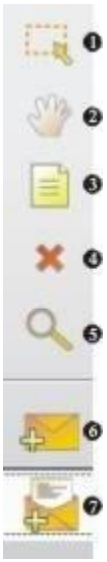

Figura 2.20.1.2.1

1) Puntero. Sirve para seleccionar cualquier ítem o área en el escenario.
2) Sirve para mover el escenario.
3) Sirve para hacer anotaciones en el escenario.
4) Borrar del escenario un ítem.
5) Muestra las tablas del dispositivo (enrutamiento, NAT, ARP, MAC, etc.).
6) Inyecta tráfico simple (ping) de dispositivo a dispositivo.
7) Inyecta tráfico complejo (IP destino, TTL, intervalos, HTTP, Telnet, SNMP, etc).

2.20.1.3. Dispositivos

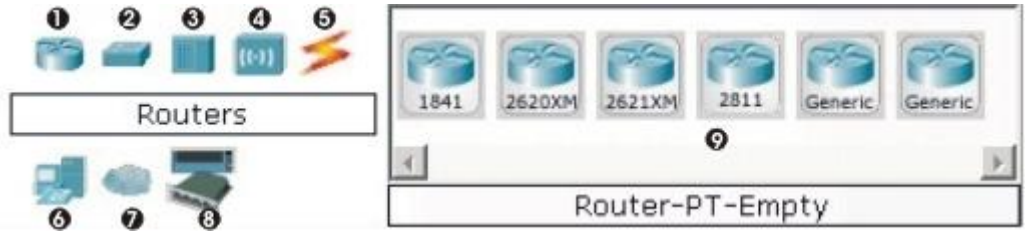

Figura 2.20.1.3.1

1) Routers: Muestra en el panel 9 los modelos de routers disponibles.
2) Switchs: Muestra en el panel 9 los modelos de switchs disponibles.
3) Hubs: Muestra en el panel 9 los modelos de hubs disponibles.
4) Dispositivos Wireless: Muestra en el panel 9 los modelos de dispositivos Wireless disponibles.
5) Medios: Muestra en el panel 9 los medios (serial, fibra, consola, etc) disponibles.
6) Dispositivos Finales: Muestra en el panel 9 los dispositivos finales (impresora, host, server, etc.) disponibles.
7) Emulación WAN: Muestra en el panel 9 las diferentes emulaciones WAN (DSL, módem, cable, etc.) disponibles.
8) Dispositivos Personalizados: Muestra en el panel 9 los diferentes dispositivos personalizados disponibles.
9) Panel de Dispositivos Seleccionados: Muestra los dispositivos disponibles según nuestra selección para utilizar en la topología. Se hace click en el dispositivo que deseamos utilizar y luego click en la parte del escenario que queremos ubicar nuestro dispositivo.

2.20.1.4. Tráfico

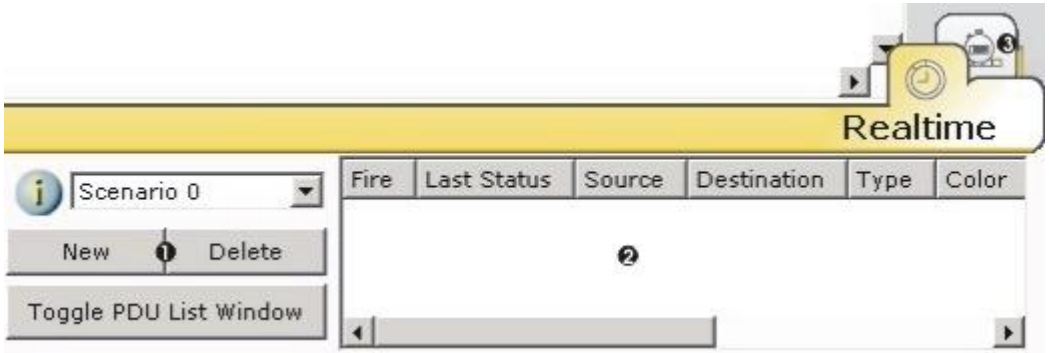

Figura 2.20.1.4.1

1. Crea escenarios para las diferentes PDU.
2. Muestra los resultados de las diferentes PDU.
3. Abre una ventana que muestra las transacciones de diferentes PDU en tiempo real.

Más adelante seguiremos con el armado de topologías y después nos adentraremos en las configuraciones propiamente dichas.

2.20.1.5. Explicación del software Packet Tracer 5.0

Figura 2.20.1.5.1

Packet Tracer es una herramienta interactiva que permite crear redes, configurar dispositivos y conectarlos.

- Sus características principales son la creación de topologías, su modo de simulación y su fácil utilización para un usuario novato o intermedio como se puede ver en la figura 2.20.1.5.2.

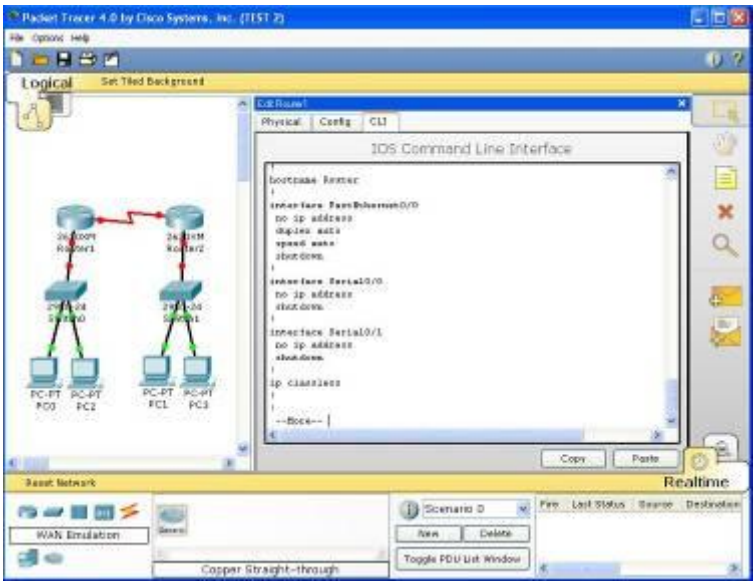

Figura 2.20.1.5.2 Software Packet Tracer

- Contiene los siguientes elementos para realizar su simulación:
  - Dispositivos
  - Conexiones
  - Protocolos de enrutamiento
  - Encapsulamiento OSI
  - Condición del enlace
  - Guardar Archivos
- Realiza visualización, simulación y animación
  - Creando/conectando dispositivos
  - Removiendo dispositivos/conexiones
  - Creando descripción de redes
  - Locking/unlocking la caja de información
- Es un avance muy importante en la enseñanza y aprendizaje.
- Es una herramienta poderosa e interactiva para la enseñanza de las operaciones básicas de varios dispositivos de networking como la capa de enlace de datos y la capa de red del modelo OSI.
- Permite a los usuarios construir sus propias redes de computadoras, y observar el comportamiento de las tramas de datos y paquetes según atraviesen los routers, switches y otros dispositivos.

Características del software Packet Tracer

- Posee la facilidad de la creación de Topologías
  - Solamente arrastrando y soltando dispositivos
  - Posee muchas opciones de interconexión
  - Biblioteca de redes y escenarios
  - Un modo de desafío
- Opciones de Configuración de Dispositivo
  - GUI o switch limitado
  - Configuración de IOS CLI del router
- Actualizaciones de Protocolo
  - RIP v1/v2, STP limitado, rutas por defecto, estáticas y balanceo de carga
  - Soporta por puerto #s, ACLs, VLSM, limited NAT/PAT, DHCP y CDP
- Modo Simulación
  - Examinar bridging, switching, y tablas de enrutamiento.
  - OSI cambios de encapsulación
  - Algoritmos de dispositivo.
- Soporta Novice-Intermediate-User Progression
- Visualización de bridging, switching, y tablas de enrutamiento, encapsulamiento de OSI, estado del enlace
- Capacidades de Ping, Ping extendido y traceroute
- Características de las Capas del Modelo OSI 1, 2, 3 y 4.
- Un Modo de Desafío el cual requiere que el estudiante dirija el paquete tomando decisiones de algoritmo del dispositivo.
- Guardado de Archivo, así las topologías y configuraciones pueden ser compartidas entre instructores y trabajo de colaboración por estudiantes.
- Un Asistente de Actividad, el cual habilita el diseño original, configuración y actividades de troubleshooting para practicar y evaluación formativa.

- Un escenario de Inicialización de Enrutamiento RIP mostrando el desarrollo de tablas de enrutamiento.

Características propuestas del software Packet Tracer 5.0

- Dispositivos
  - Linksys, Seguridad, Wireless, Tecnologías WAN, más routers y switches
- Dinamismo
  - Soporta flujos 2-vías
- Protocolos y Comandos
  - EIGRP, OSPF, más STP, TCP, CDP, PPP, Frame, ISDN
- Instruccional
  - Características de juego, guía instruccional opcional, vista de sniffer.
- GUI
  - Relacionado a la topología física, uso de dispositivos/imágenes reales Cisco, más herramientas, multiusuario, consola de instructor

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

1. Guía de práctica: Realizar una red LAN en la que se observa las diferentes capas del modelo OSI.

1.1. Objetivo

- Verificar el procedimiento de cada paquete en las diferentes capas del modelo OSI.
- Conseguir la transferencia de paquetes entre todas las CPU´s y la impresora que se encuentra conectada en red.

1.2. Procedimiento

1.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1

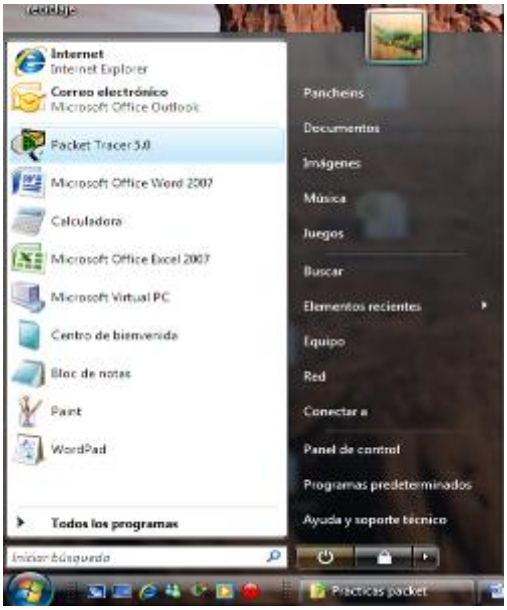

Figura 1.2.1.1 Inicio de Packet Tracer

1.2.2. Primero debemos configurar la dirección IP y su respectiva mascara de red para todas las CPU´s conectadas en la red, para ello procedemos a dar un clic en cada una de las CPU´s de la red, para lo cual se abre una pantalla de configuración como se puede observar en la figura 1.2.2.1

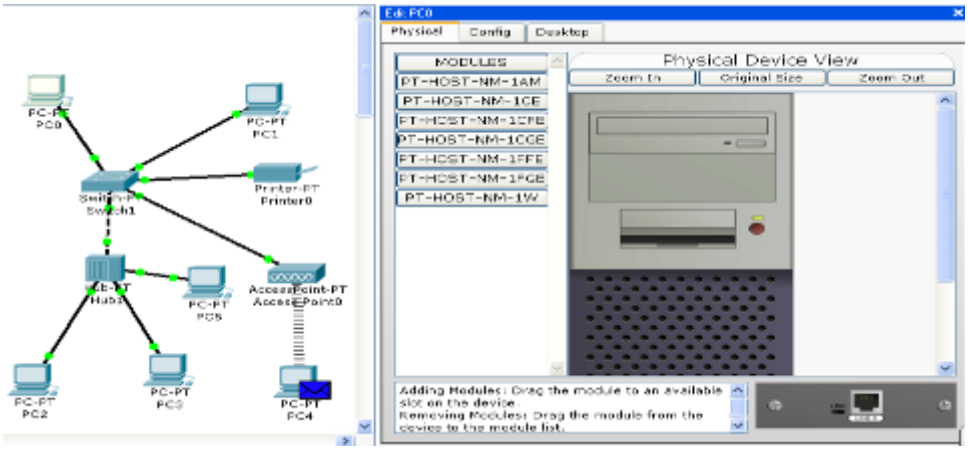

Figura 1.2.2.1 Edit CPU's

1.2.3. En la pantalla que aparece nos debemos dirigir a la pestaña con el nombre de desktop, y luego en IP configuration en la cual procedemos con la configuración de nuestra dirección IP y nuestra mascara de red como se observa en la figura 1.2.3.1

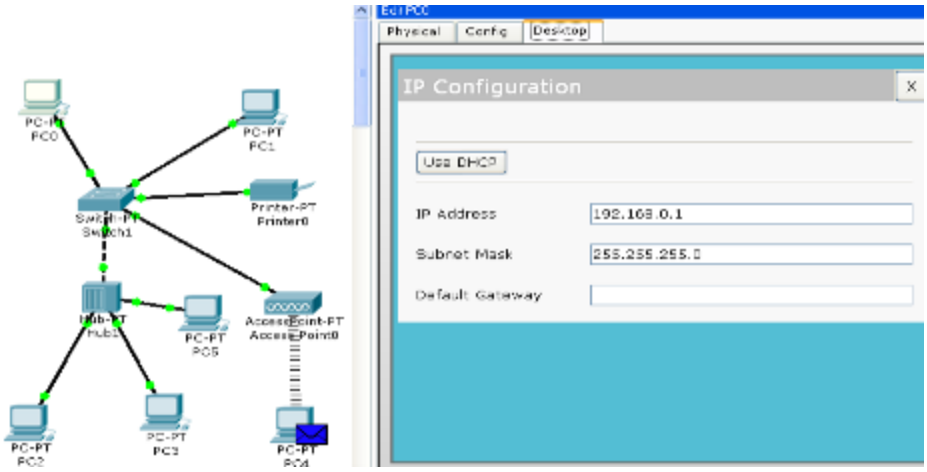

Figura 1.2.3.1 CPU´s

1.2.4. Para realizar la conexión inalámbrica de la computadora PC4 se debe proceder a instalar el dispositivo para la conexión inalámbrica en la CPU como se puede observar en la figura 1.2.4.1

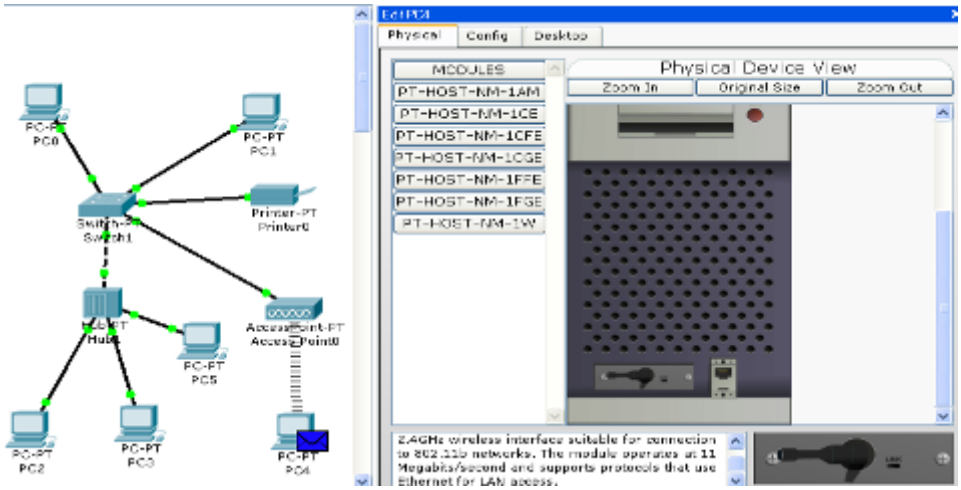

Figura 1.2.4.1 Dispositivo inalámbrico

1.2.5. Procedemos con la configuración de la dirección IP y su respectiva mascara de red de la impresora que se encuentra conectada en red, para ello ingresamos en la parte que dice Fast Ethernet en la plantilla config como se puede observar en la figura 1.2.5.1

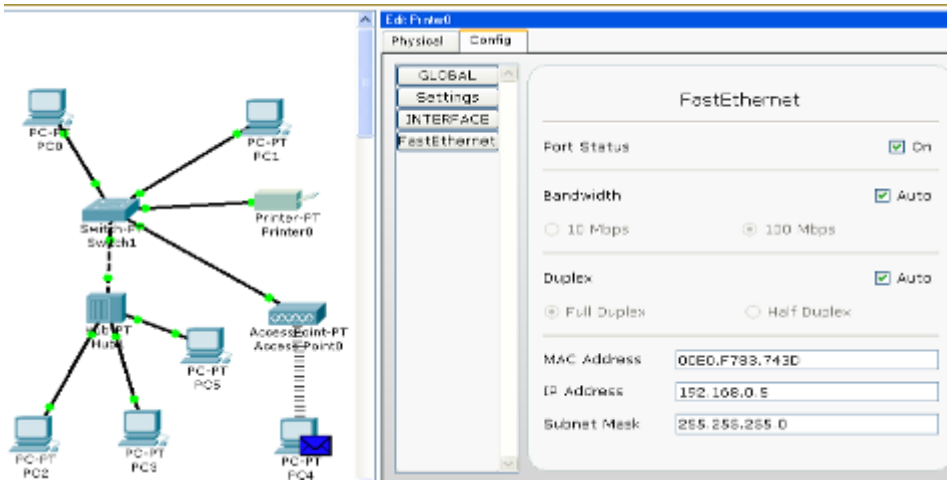

Figura 1.2.5.1 Impresora

1.2.6. Procedemos a dar un clic sobre el switch y verificamos que todos los puertos estén encendidos y funcionando correctamente, para

ello ingresamos en la parte que dice Fast Ethernet en la plantilla config como se puede observar en la figura 1.2.6.1

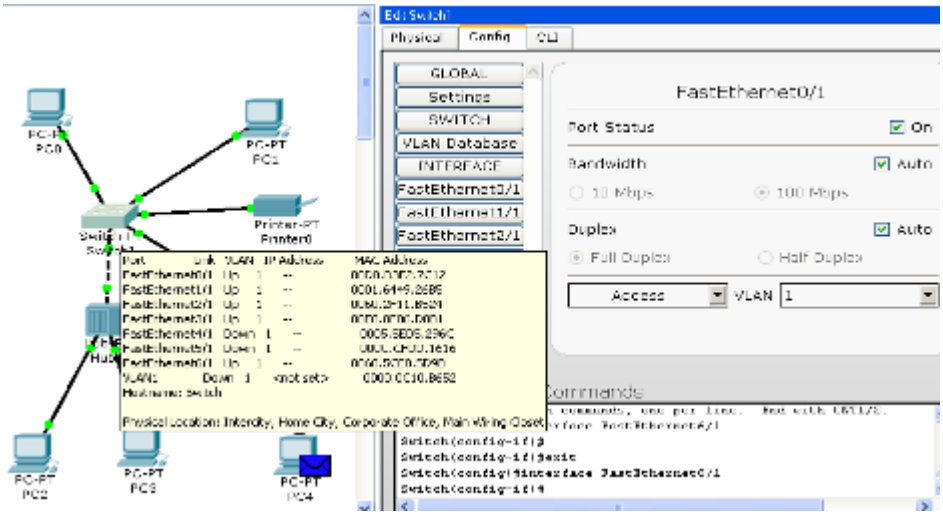

Figura 1.2.6.1 Switch1

1.2.7. Procedemos a dar un clic sobre el Access Point y procedemos a verificar que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 1.2.7.1

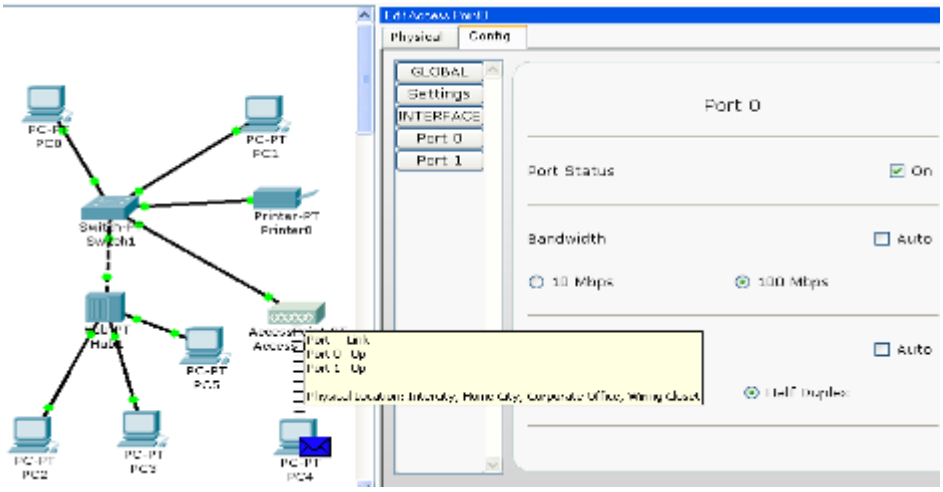

Figura 1.2.7.1 Access Point

1.2.8. Procedemos a dar un clic sobre el Hub y procedemos a verificar que todos los puertos que están conectados se encuentren

encendidos y funcionando correctamente, como se puede observar en la figura 1.2.8.1

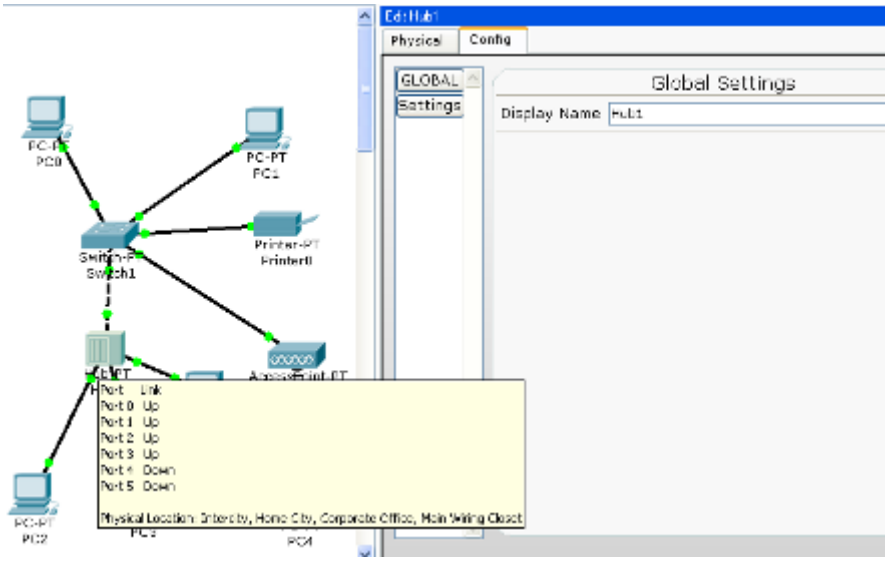

Figura 1.2.8.1 Hub

1.3. Desarrollo

1.3.1. Se coloca un paquete simple señalando el lugar de origen y destino para transferir la información y comprobar que la conexión no tenga problemas, en el escenario0 se va a comprobar la conexión entre la PC4 y la PC1 al enviar y recibir los datos, como se puede observar en la figura 1.3.1.1

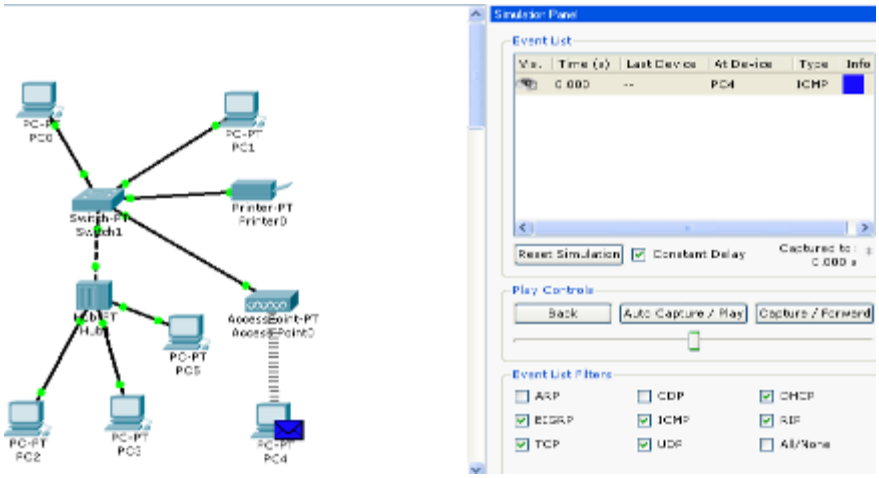

Figura 1.3.1.1 Colocación de paquete

1.3.2. Procederemos con la respectiva simulación enviando un paquete y comprobando que la conexión correspondiente este funcionando, en las figuras 1.3.2.1, 1.3.2.2, 1.3.2.3 y 1.3.2.4 se puede observar las diferentes capas por la que pasa el paquete para ser enviado y su respectivo proceso.

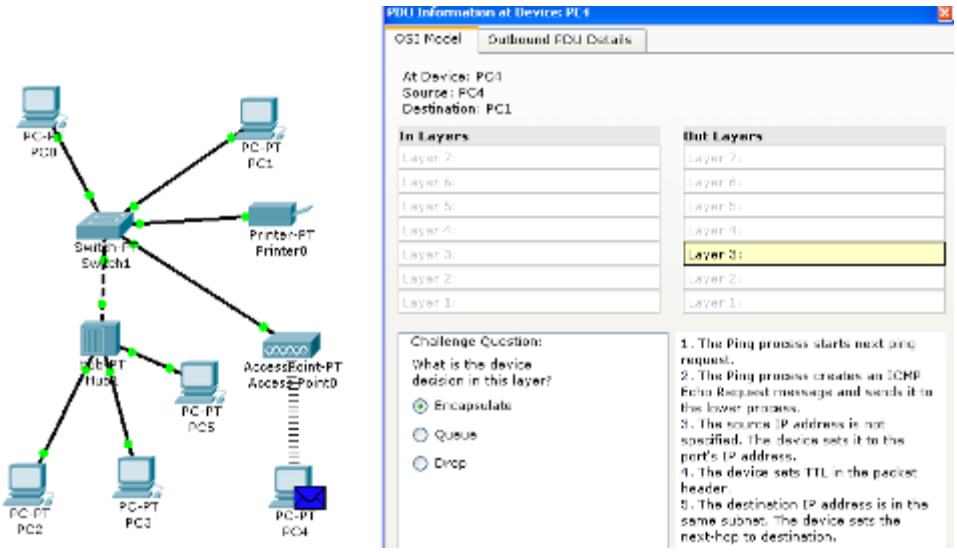

Figura 1.3.2.1 Salida paquete en la capa 3 en PC4

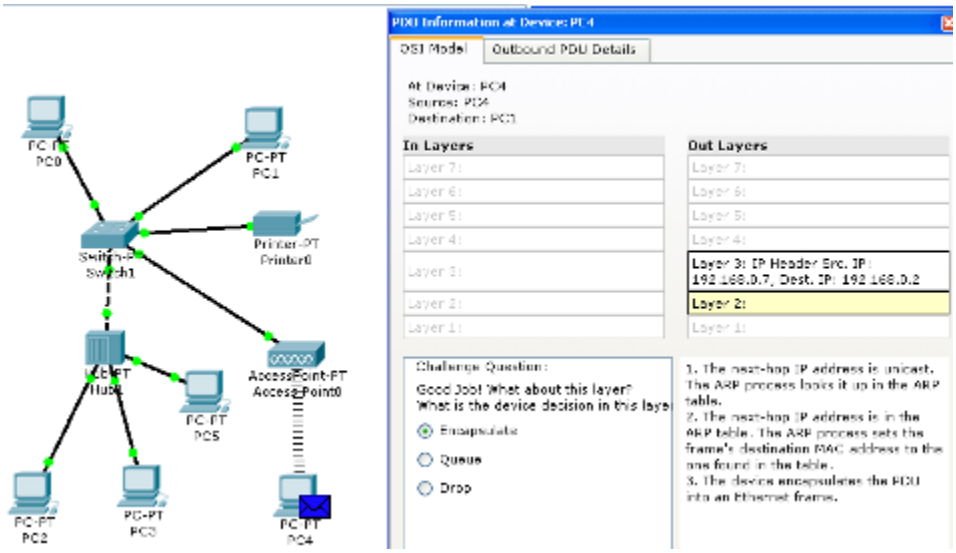

Figura 1.3.2.2 Salida paquete en la capa2 en PC4

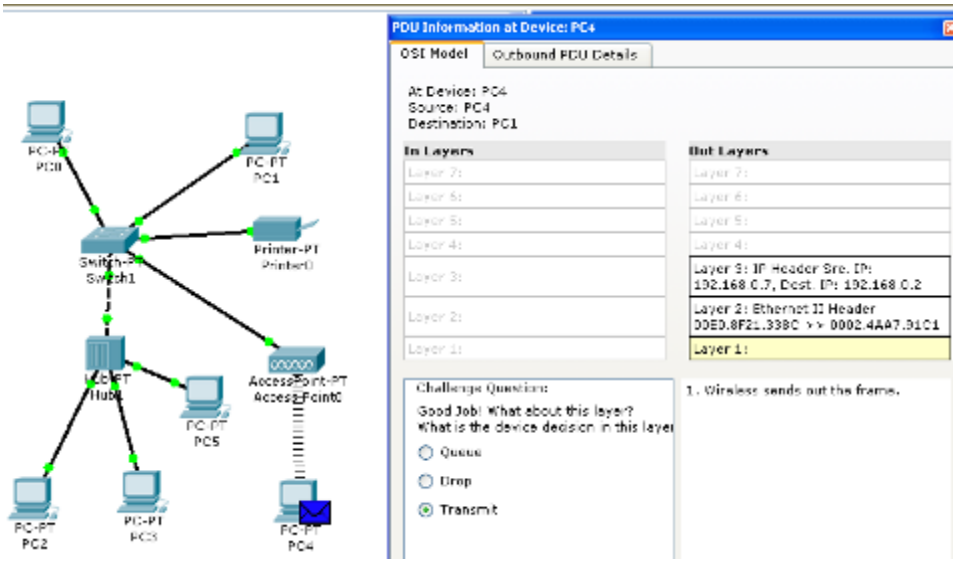

Figura 1.3.2.3 Salida paquete en la capa1 en PC4

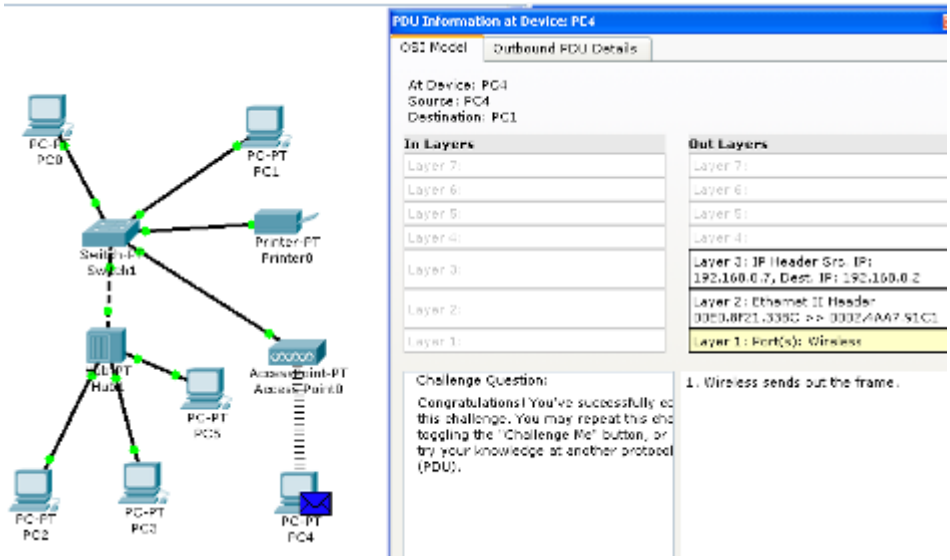

Figura 1.3.2.4 envío paquete en PC4

1.3.3. Procediendo con la respectiva simulación se puede observar claramente en las figuras 1.3.3.1, 1.3.3.2 y 1.3.3.3 que el paquete se traslada de la PC4 al Access Point y también las diferentes capas por la que pasa el paquete para ser enviado y su respectivo proceso.

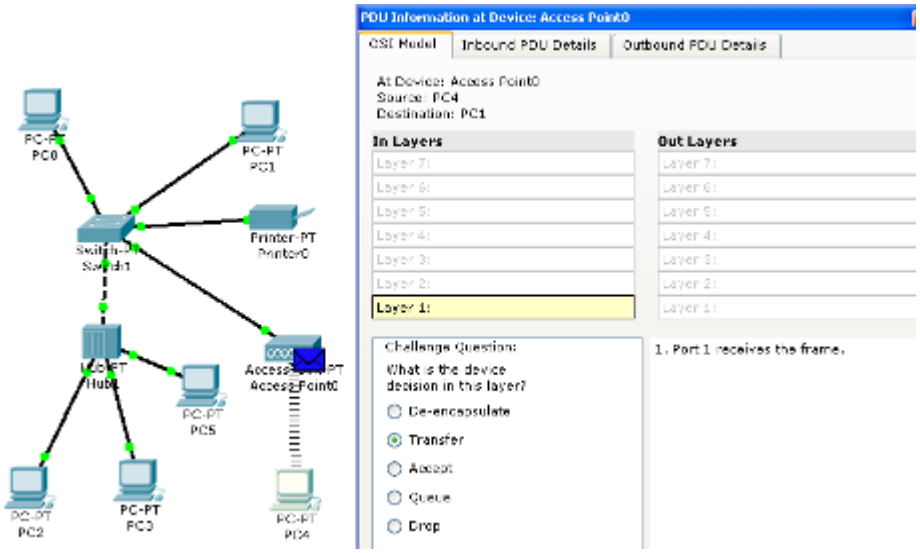

Figura 1.3.3.1 Entrada paquete en la capa1 en Access Point

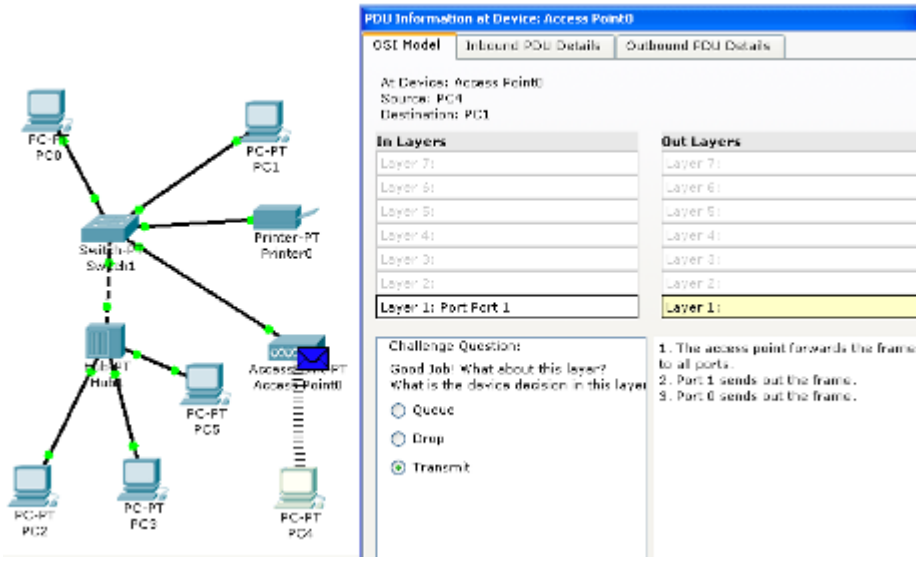

Figura 1.3.3.2 Salida paquete en la capa1 en el Access Point

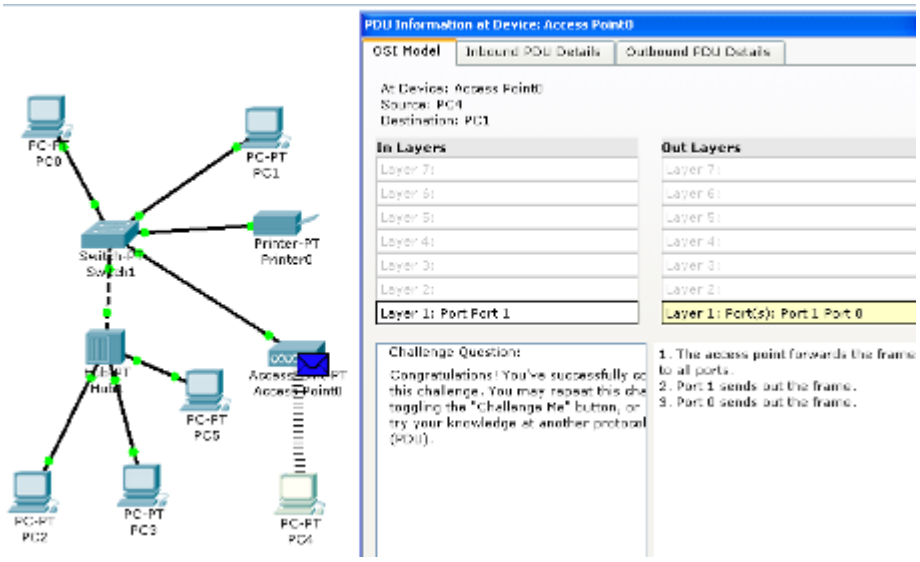

Figura 1.3.3.3 Envío de paquete en el Access Point

1.3.4. Procediendo con la respectiva simulación se puede observar claramente en las figuras 1.3.4.1, 1.3.4.2, 1.3.4.3, 1.3.4.4 y 1.3.4.5 que el paquete se traslada del Access Point al switch y también las diferentes capas por la que pasa el paquete para ser enviado y su respectivo proceso.

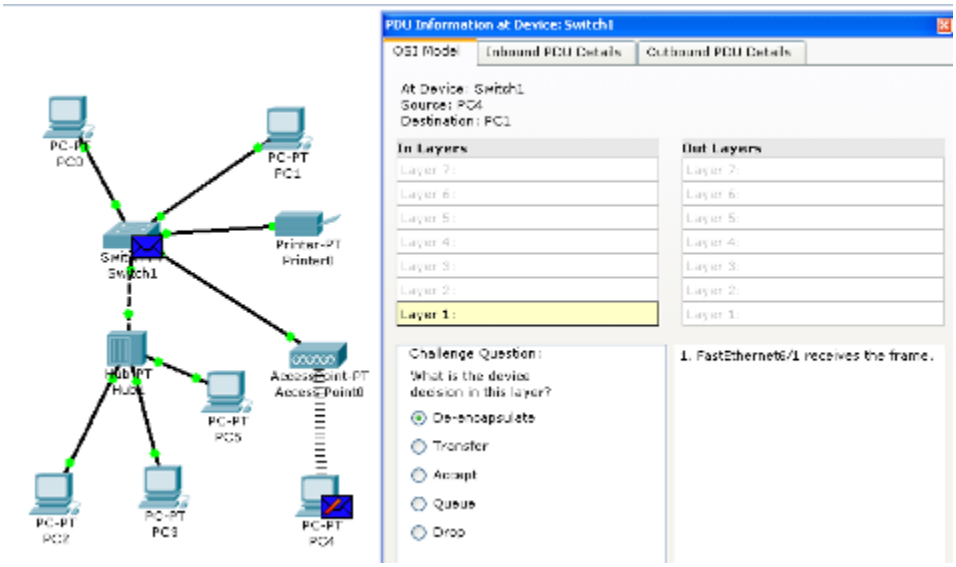

Figura 1.3.4.1 Entrada paquete en la capa1 en el switch

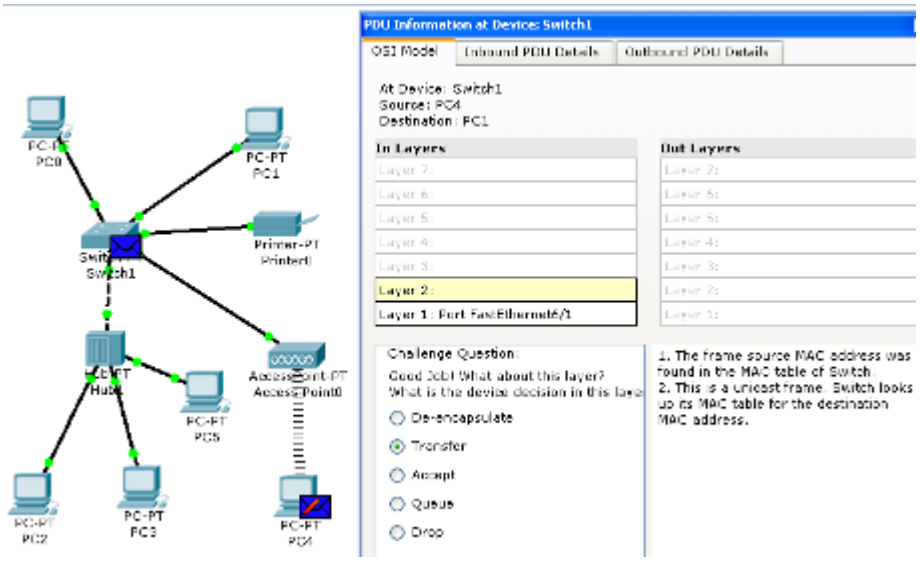

Figura 1.3.4.2 Entrada paquete en la capa2 en el switch

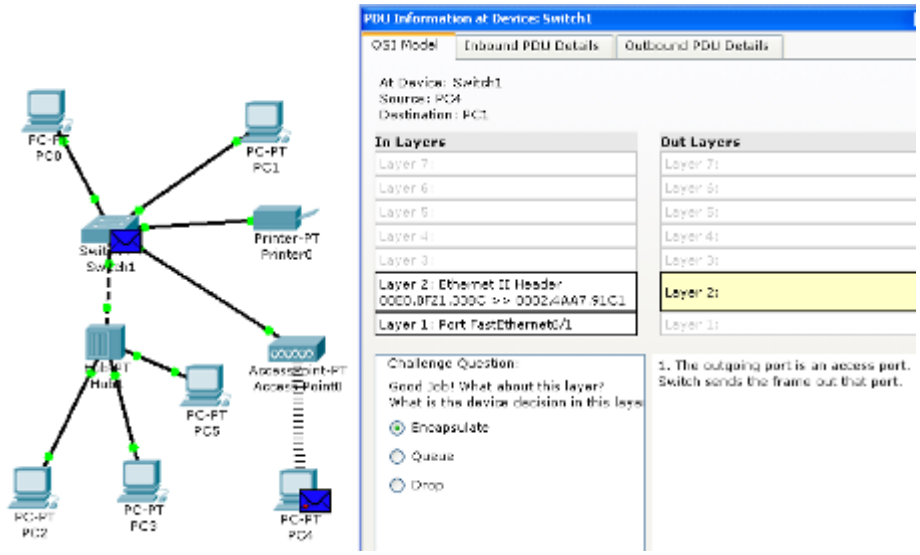

Figura 1.3.4.3 Salida paquete en la capa2 en el switch

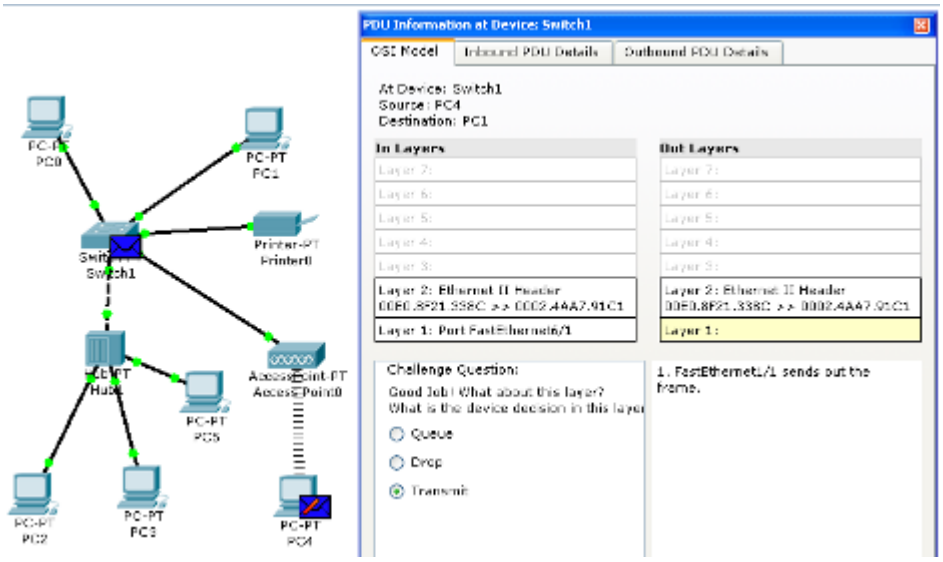

Figura 1.3.4.4 Salida paquete en la capa1 en el switch

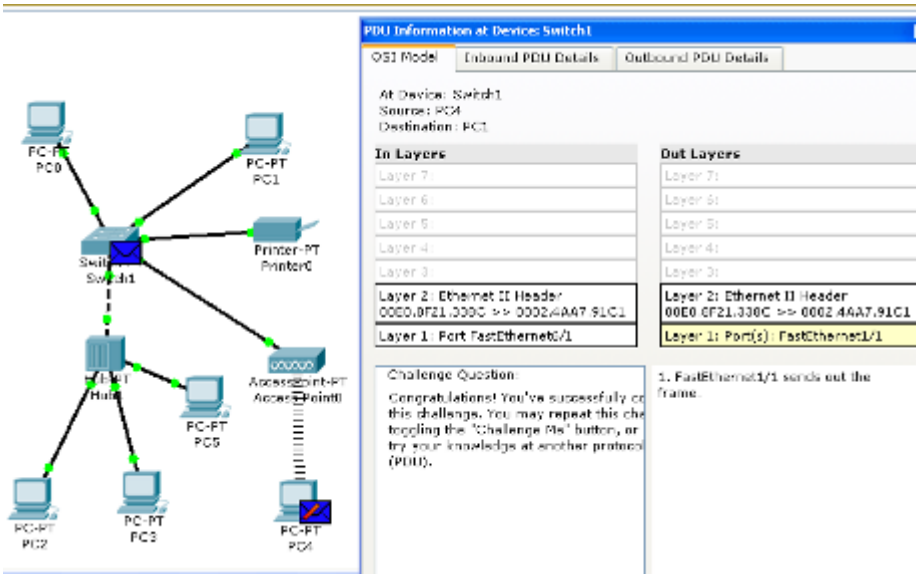

Figura 1.3.4.5 Envío de paquete en el switch

1.3.5. Procediendo con la respectiva simulación se puede observar claramente en las figuras 1.3.5.1, 1.3.5.2, 1.3.5.3, 1.3.5.4, 1.3.5.5, 1.3.5.6 y 1.3.5.7 que el paquete se traslada del switch a la PC1 y también las diferentes capas por las que se procesa el paquete para ser enviado y su respectivo proceso.

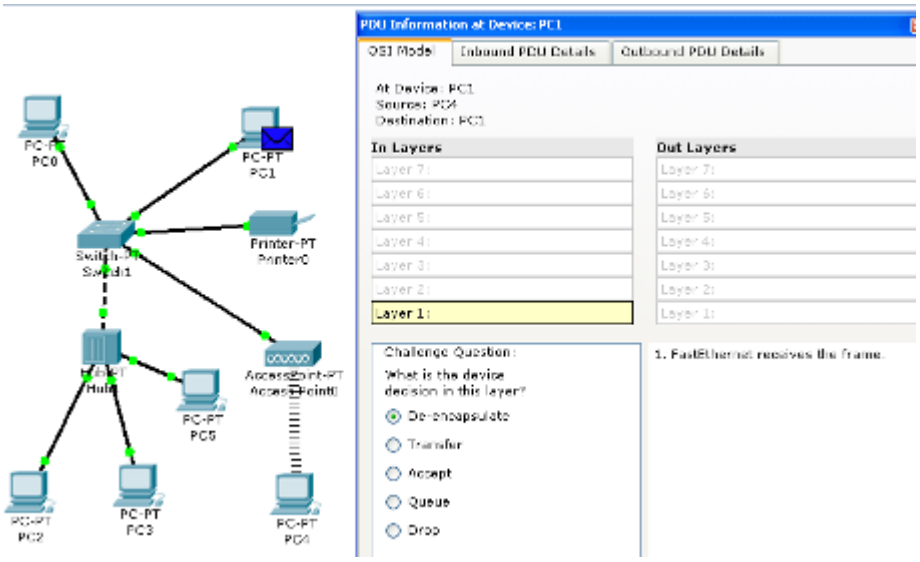

Figura 1.3.5.1 Entrada paquete en la capa1 en PC1

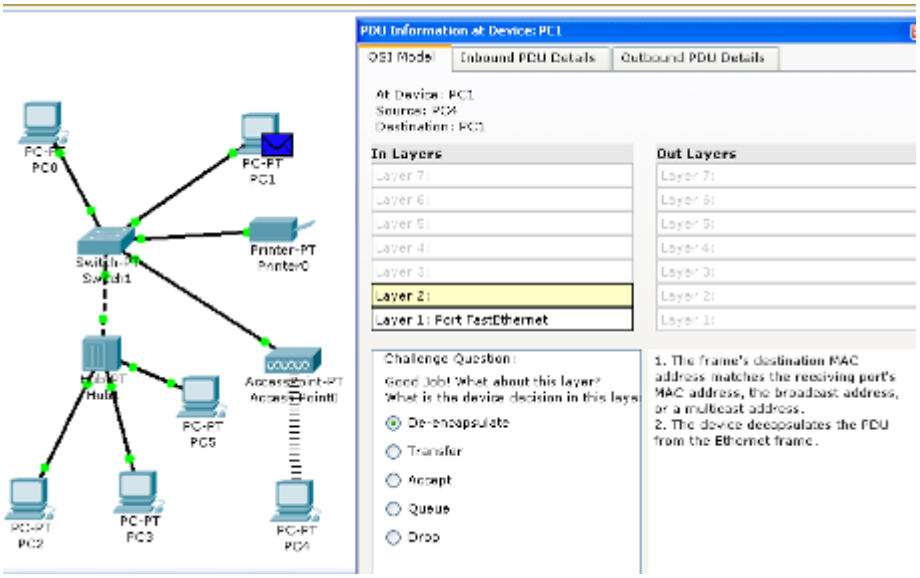

Figura 1.3.5.2 Entrada paquete en la capa2 en PC1

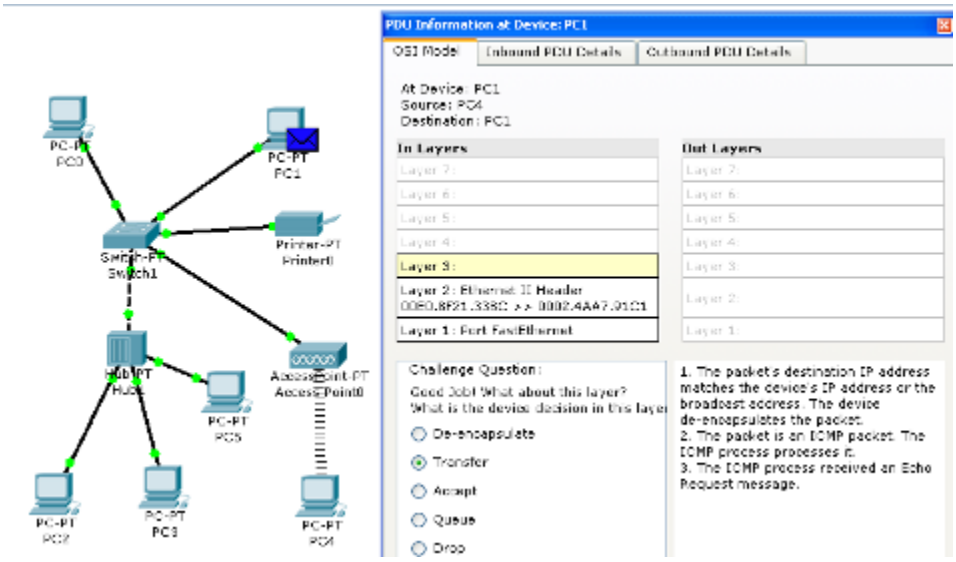

Figura 1.3.5.3 Entrada paquete en la capa3 en PC1

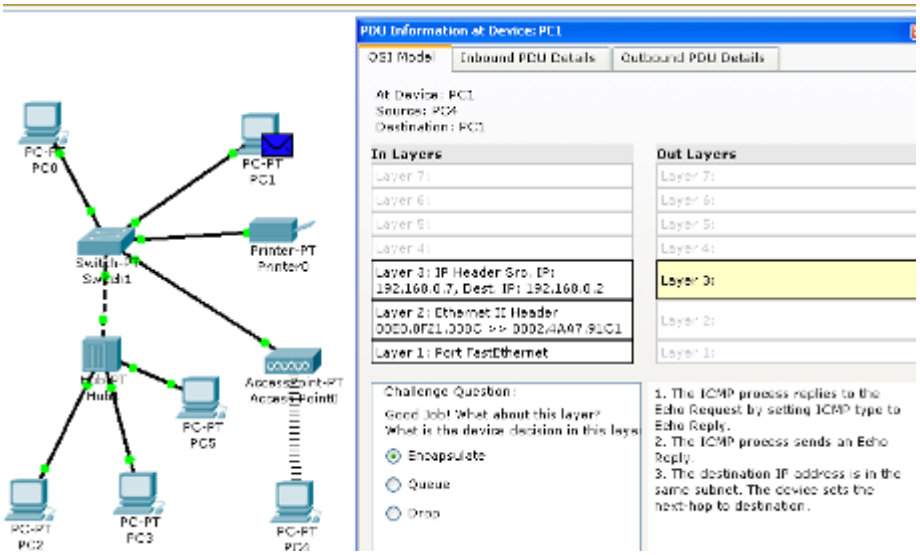

Figura 1.3.5.4 Salida paquete en la capa3 en PC1

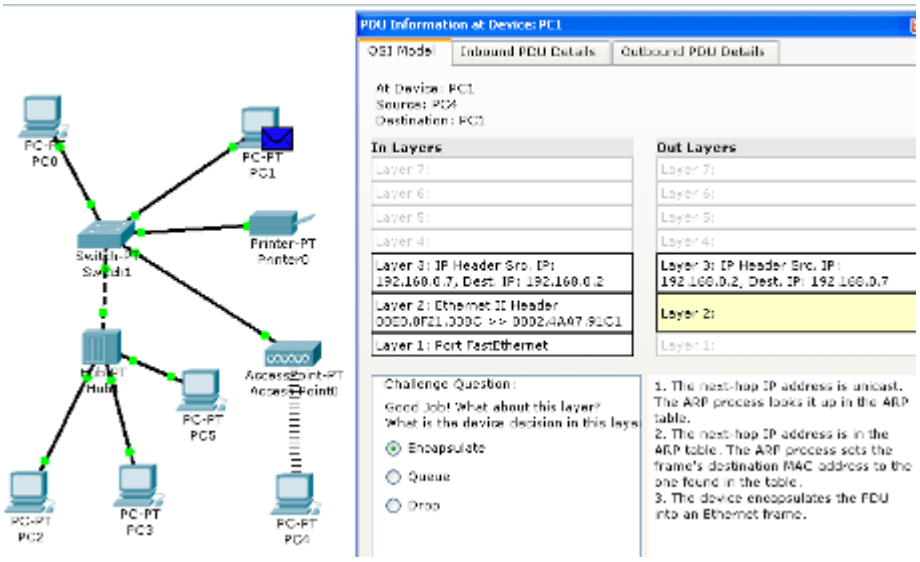

Figura 1.3.5.5 Salida paquete en la capa2 en PC1

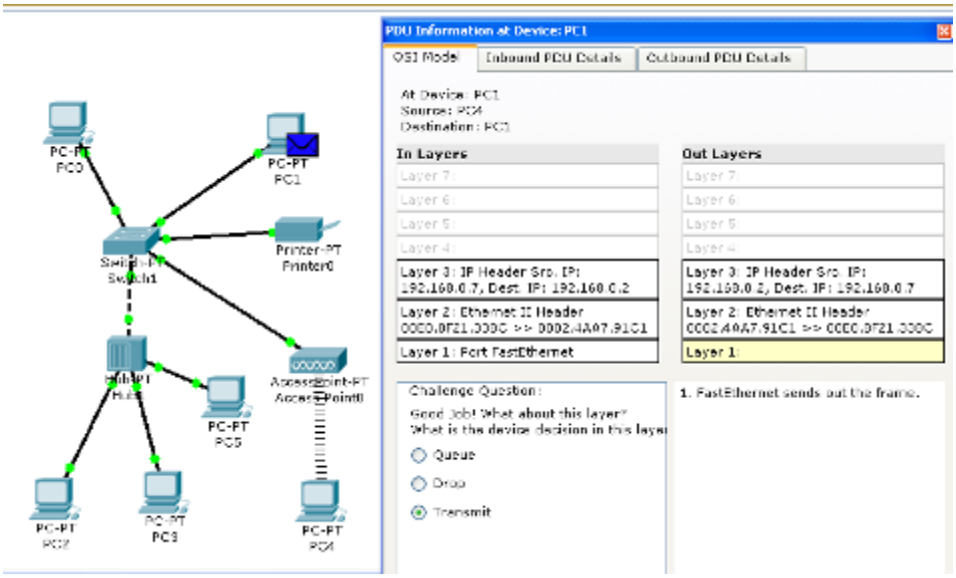

Figura 1.3.5.6 Salida paquete en la capa1 en PC1

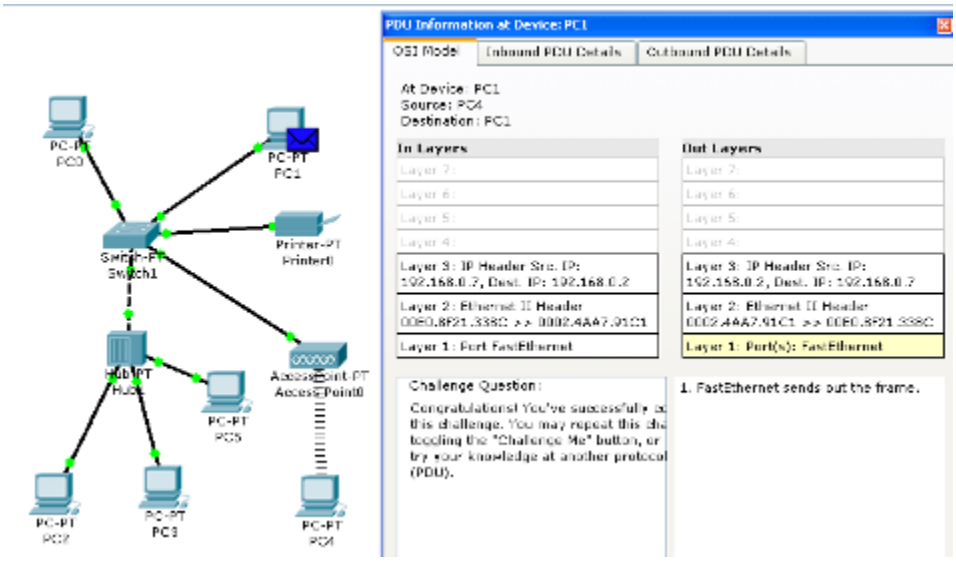

Figura 1.3.5.7 envío Paquete en PC1

1.3.6. Procediendo con la respectiva simulación se puede observar claramente en las figuras 1.3.6.1, 1.3.6.2, 1.3.6.3, 1.3.6.4 y 1.3.6.5 que el paquete se traslada de la PC1 al switch y también las diferentes capas por la que pasa el paquete para ser enviado y su respectivo proceso.

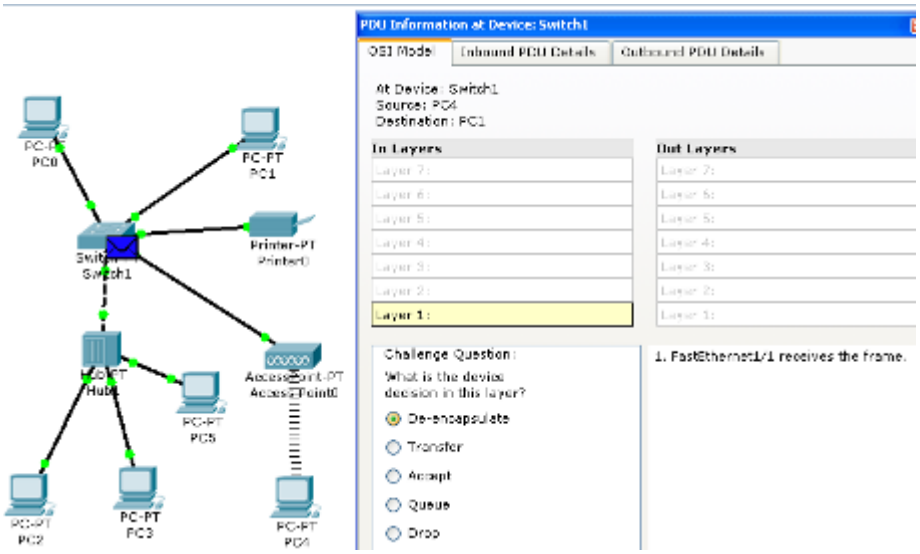

Figura 1.3.6.1 Entrada paquete en la capa1 en switch

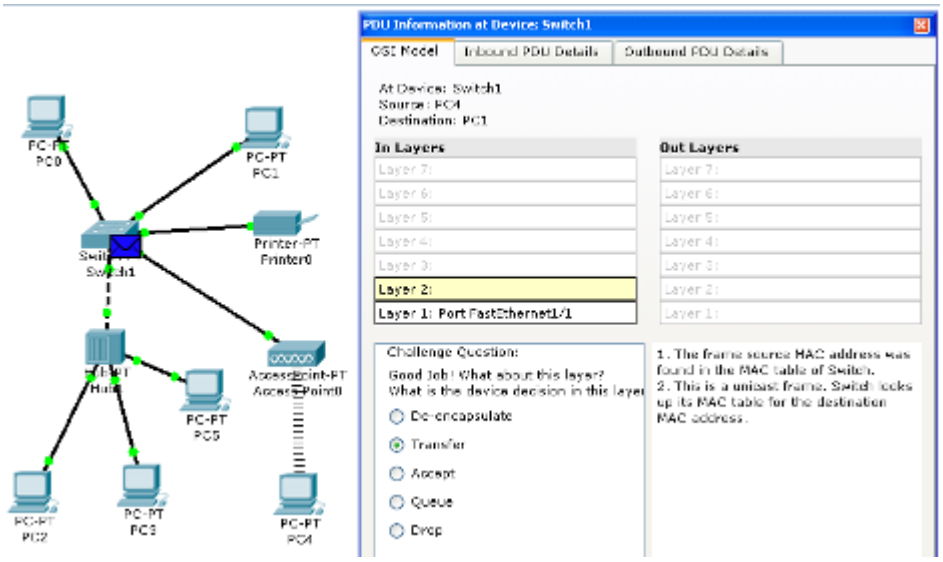

Figura 1.3.6.2 Entrada paquete en la capa2 en switch

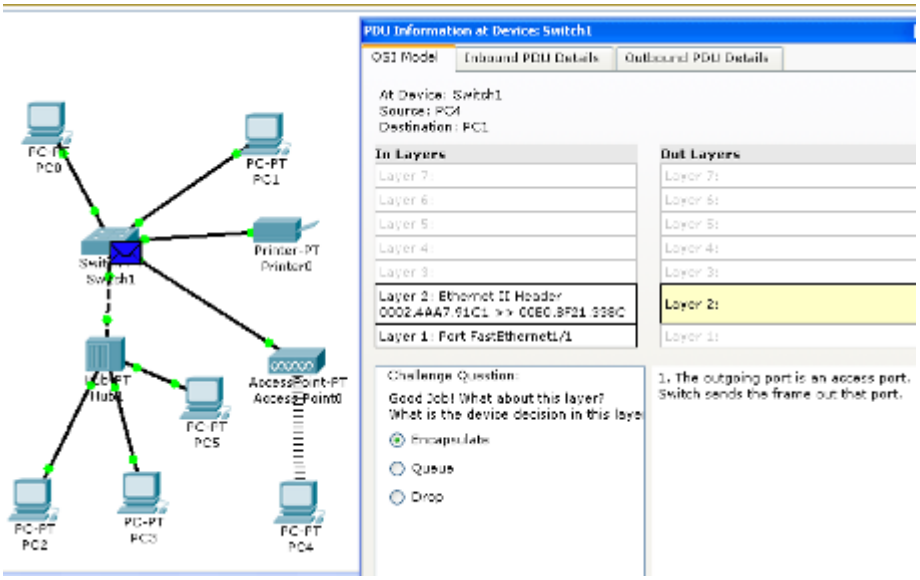

Figura 1.3.6.3 Salida paquete en la capa2 en switch

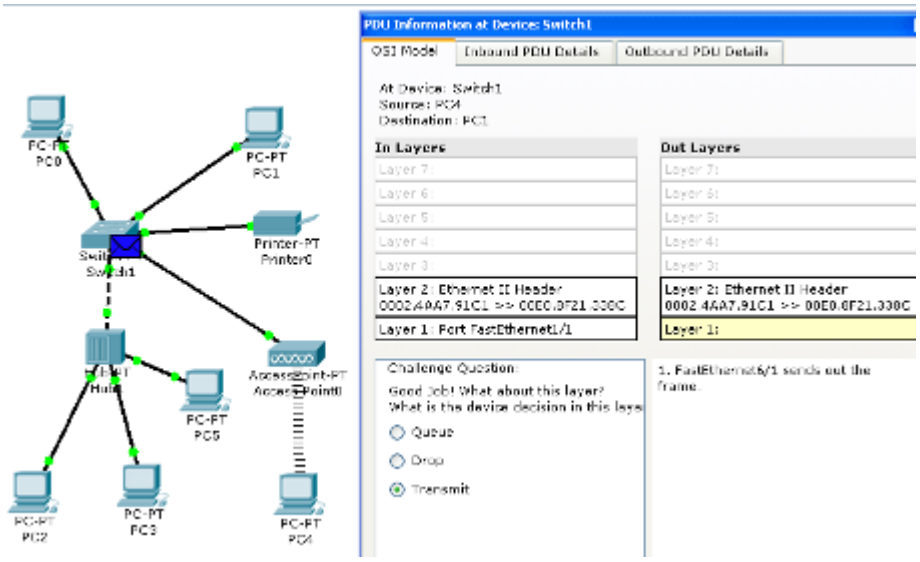

Figura 1.3.6.4 Salida paquete en la capa1 en switch

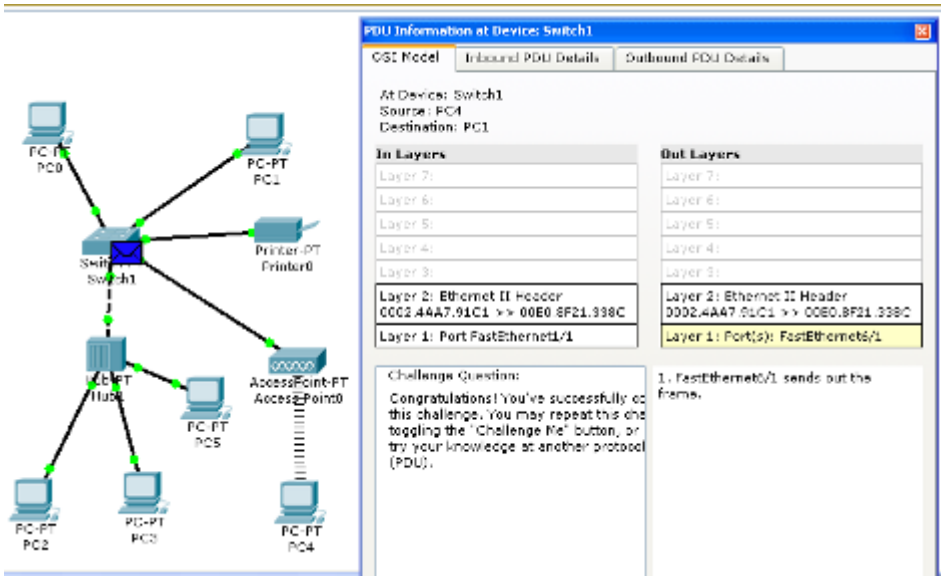

Figura 1.3.6.5 Envío de paquete en switch

1.3.7. Procediendo con la respectiva simulación se puede observar claramente en las figuras 1.3.7.1, 1.3.7.2 y 1.3.7.3 que el paquete se traslada del switch al Access Point y también las diferentes capas por la que pasa el paquete para ser enviado y su respectivo proceso.

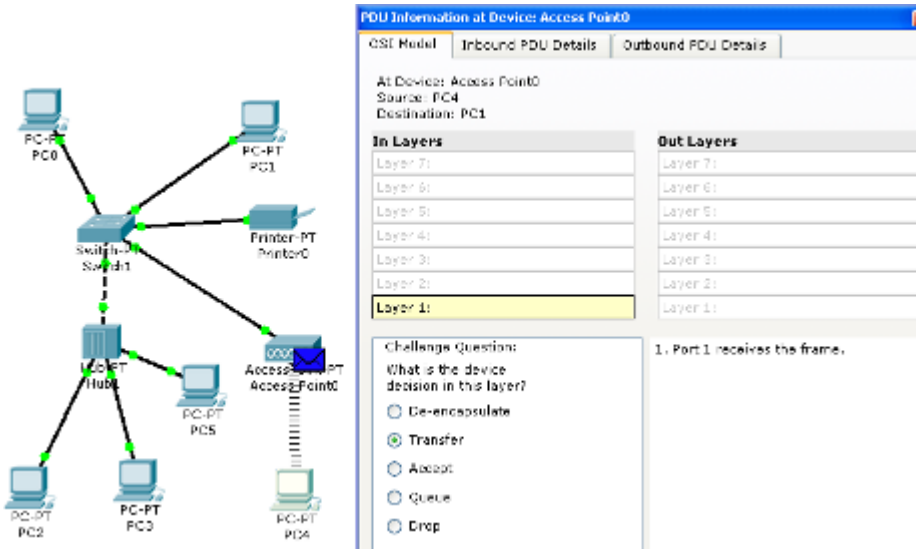

Figura 1.3.7.1 Entrada paquete en la capa1 en Access Point

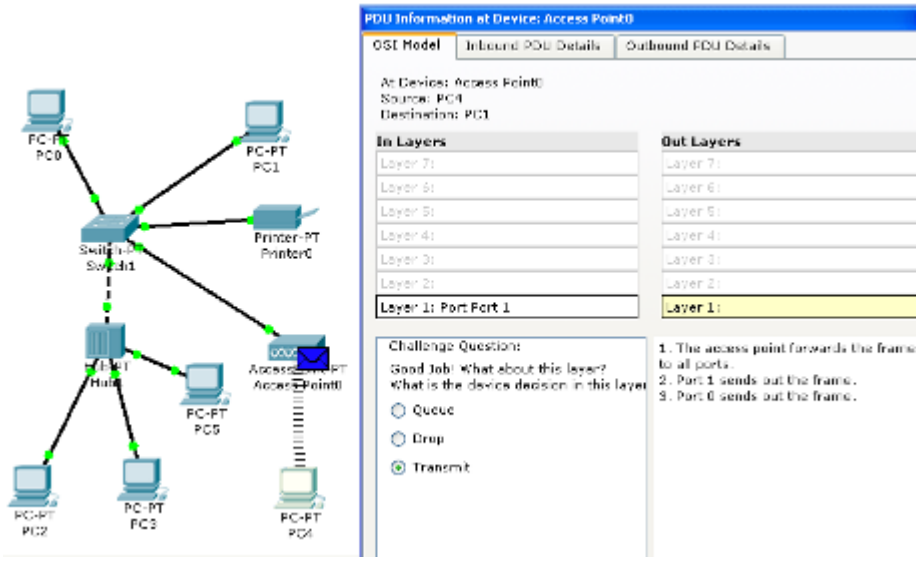

Figura 1.3.7.2 Salida paquete salida en la capa1 en Access Point

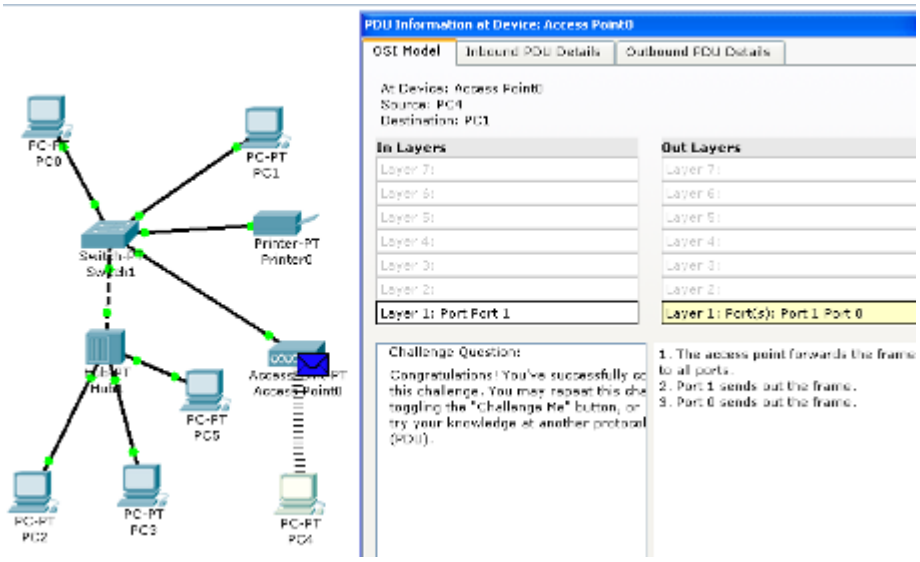

Figura 1.3.7.3 Envío de paquete en Access Point

1.3.8. Procediendo con la respectiva simulación se puede observar claramente en las figuras 1.3.8.1, 1.3.8.2 y 1.3.8.3 que el paquete se traslada del Access Point a la PC4 y también las diferentes capas por la que pasa el paquete para ser enviado y su respectivo proceso.

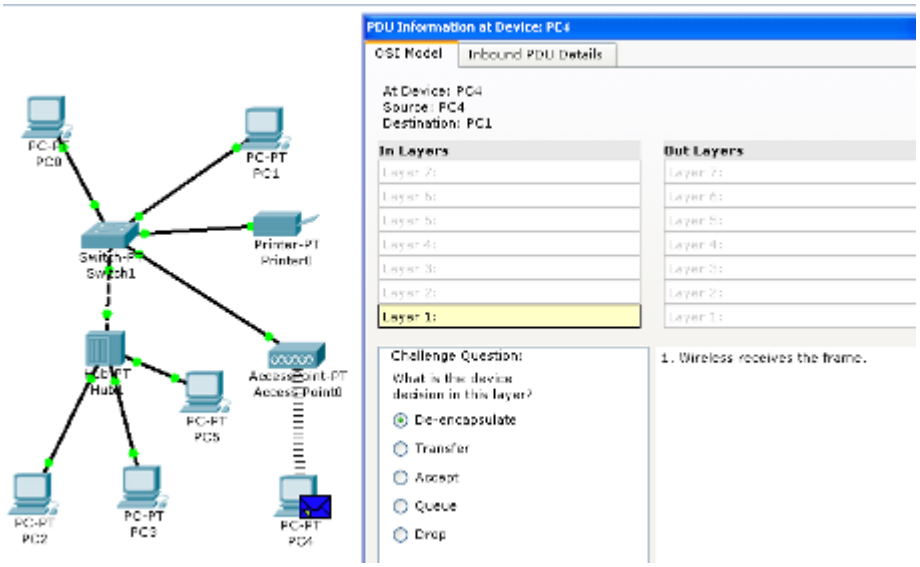

Figura 1.3.8.1 Entrada paquete en la capa1 en PC4

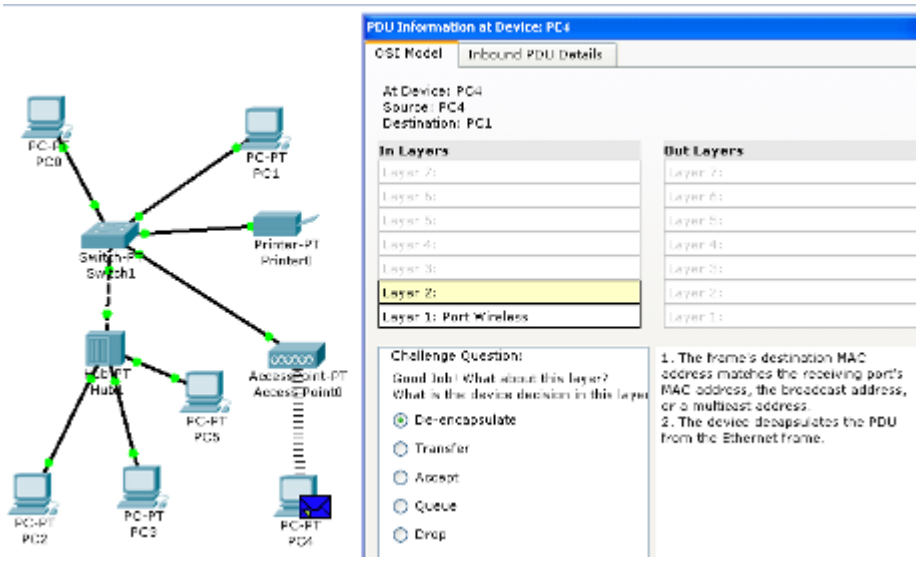

Figura 1.3.8.2 Entrada paquete en la capa2 en PC4

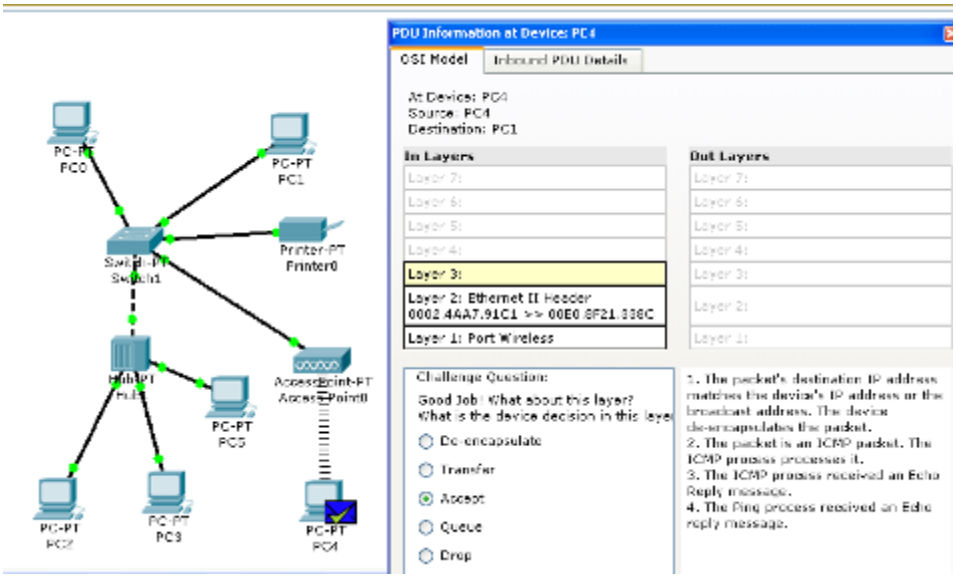

Figura 1.3.8.3 Entrada paquete en la capa3 en PC4

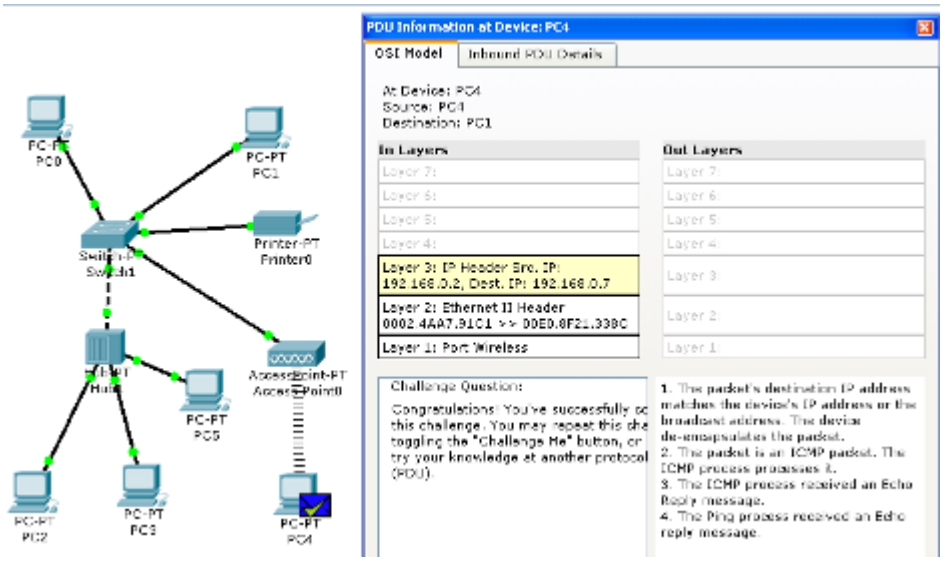

Figura 1.3.8.4 Paquete recibido en PC4

1.4. Análisis de resultados

1.4.1. Se puede observar en la simulación que el switch utilizado traba hasta en una capa2 del modelo OSI

1.4.2. En las CPU´s se puede observar claramente como el paquete trabaja hasta una capa3 del modelo OSI

1.4.3. Al realizar la simulación de la red se debe tener muy en cuenta que todos los elementos de la red deben estar en la misma red, caso contrario no se podrían enviar ninguna información.

1.5. Conclusiones

1.5.1. Las graficas de la simulación permitieron observar que los paquetes se trasladaron sin ningún problema por la red

1.5.2. Con la simulación realizada se cumplieron los objetivos requeridos

1.5.3. Se puede observar muy claramente que la red se encuentra funcionando correctamente con todos sus elementos

2. Guía de práctica: Realizar 4 subredes de una clase tipo B con conectividad vía Wireless

2.1. Objetivo

- Realizar cuatro subredes para una clase tipo B
- Conseguir la transferencia de paquetes entre todas las subredes de la clase B
- Realizar con la conectividad con PC vía wireless

2.2. Procedimiento

2.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[1]

2.2.2. Primero debemos realizar los cálculos correspondientes para realizar las cuatro subredes que se va a utilizar de una clase tipo B. Para ello elegimos una red de tipo B y procedemos a dividirlo como se muestra a continuación en la figura 2.2.2.1

Dividamos la red 147.156.0.0 (clase B) en cuatro subredes:

	16 bits	2 bits	14 bits
	147 . 156	Subred	Host
Máscara:	11111111 . 11111111 .	11	000000 . 00000000
	255 . 255 .	192	. 0

Bits subred	Subred	Máscara	Rango
00 (0)	147.156.0.0	255.255.192.0	147.156.0.0 – 147.156.63.255
01 (64)	147.156.64.0	255.255.192.0	147.156.64.0 – 147.156.127.255
10 (128)	147.156.128.0	255.255.192.0	147.156.128.0 – 147.156.191.255
11 (192)	147.156.192.0	255.255.192.0	147.156.192.0 – 147.156.255.255

Figura 2.2.2.1 Cuatro subredes de una clase B

2.2.3. Luego procedemos con la configuración de la dirección IP y su respectiva mascara de red para todas las PC´s de la red, como se ha venido mostrando en las prácticas anteriores, tomando en cuenta que cada sección le vamos a tomar como una subred, para ello procedemos a dar un clic en una CPU para lo cual se abre una pantalla de configuración en la cual nos dirigirnos a la pestaña con el nombre de desktop, y luego en IP configuration en la cual procedemos con la configuración de nuestra dirección IP y nuestra mascara de red como se puede observar en la figura 2.2.3.1

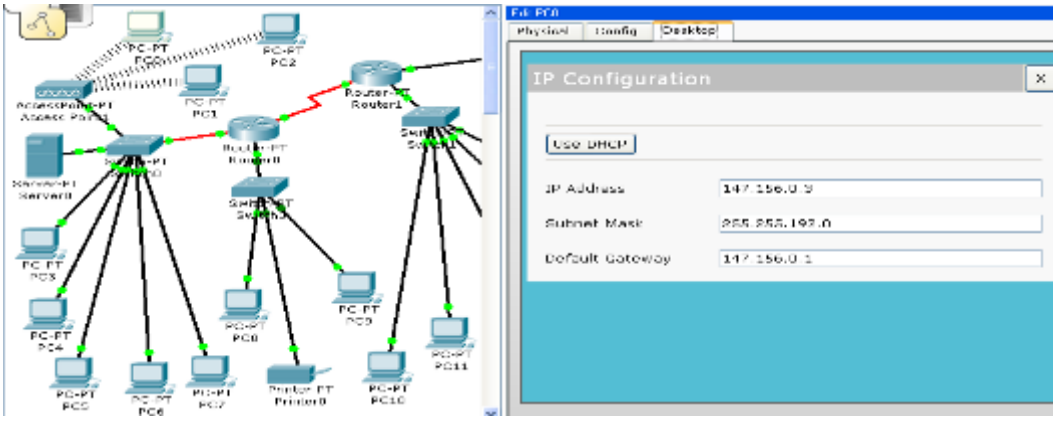

Figura 2.2.3.1 Edit PC0

2.2.4. En las CPU´s PC0, PC1 y PC2 se debe realizar el respectivo cambio de la tarjeta inalámbrica para su funcionamiento como se indica en la figura 2.2.4.1

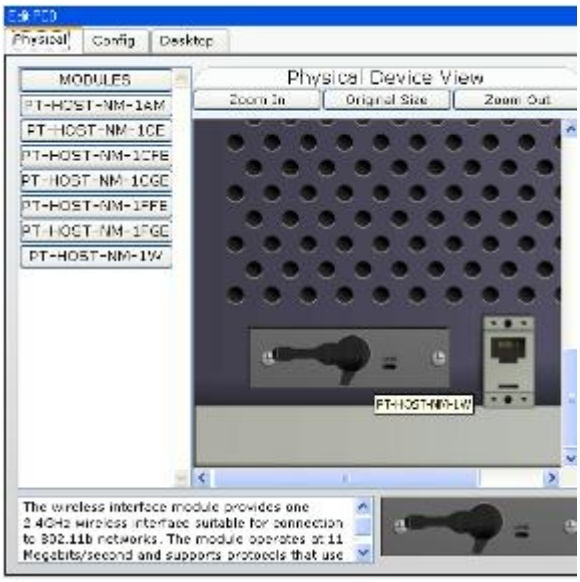

Figura 2.2.4.1 Tarjeta inalámbrica

2.2.5. Procedemos con la configuración de la dirección IP y su respectiva mascara de red del servidor que se encuentra conectada en red, para ello ingresamos en la parte que dice Fast Ethernet en la plantilla config como se puede observar en la figura 2.2.5.1

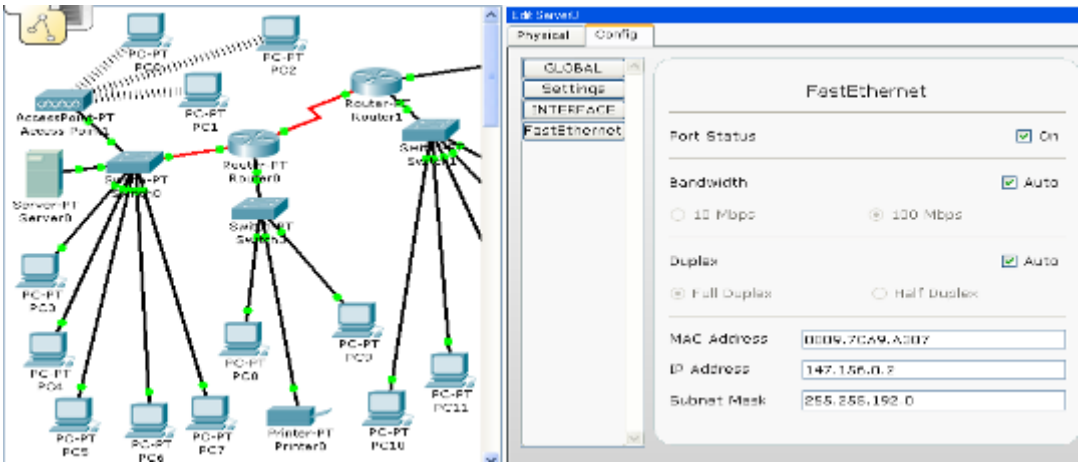

Figura 2.2.5.1 Servidor

2.2.6. Procedemos con la configuración de la dirección IP y su respectiva mascara de red de la impresora que se encuentra conectada en red, para ello ingresamos en la parte que dice Fast Ethernet en la plantilla config como se puede observar en la figura 2.2.6.1

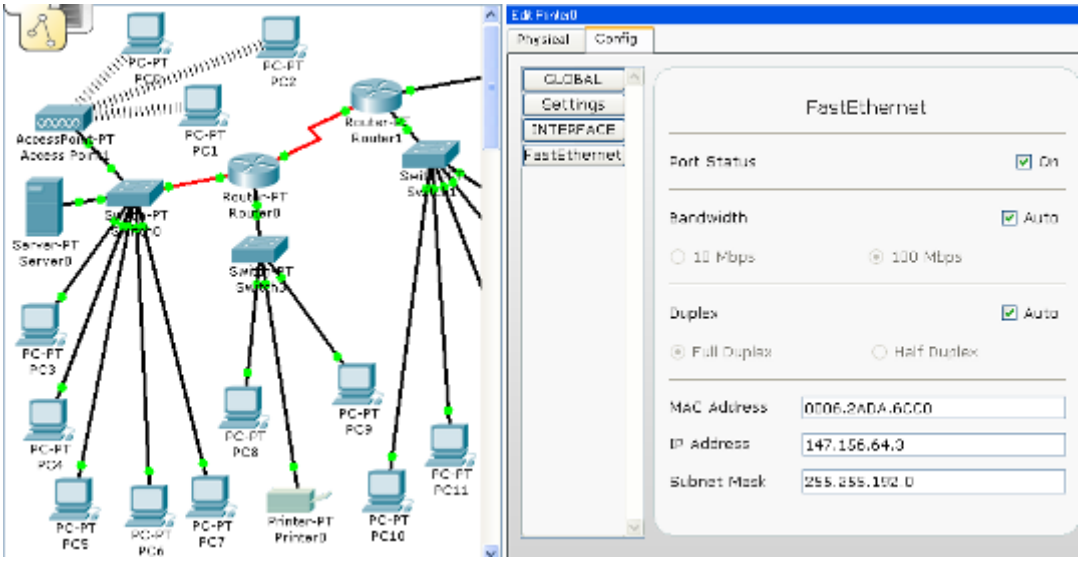

Figura 2.2.6.1 Impresora

2.2.7. Procedemos a dar un clic sobre el Access Point y procedemos a verificar que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 2.2.7.1

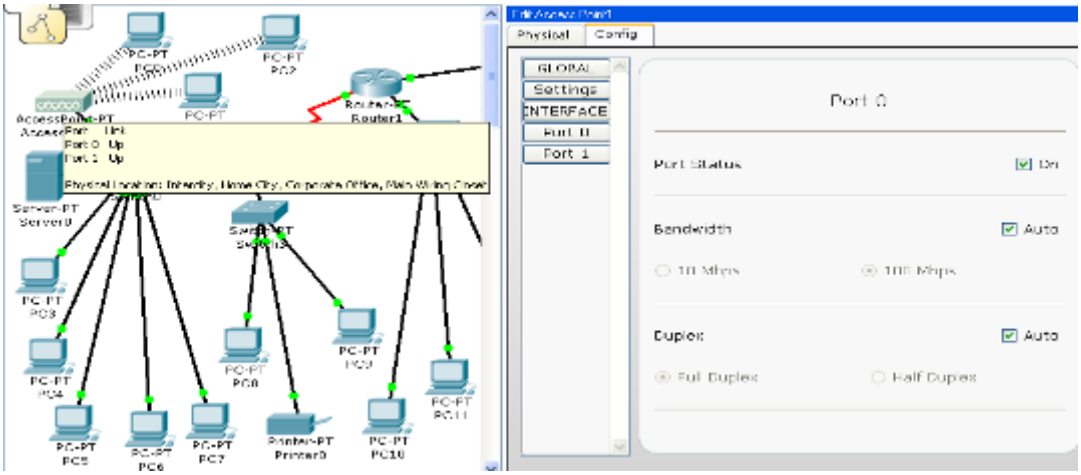

Figura 2.2.7.1 Access Point

2.2.8. Procedemos a dar un clic sobre los Routers y verificamos que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 2.2.8.1

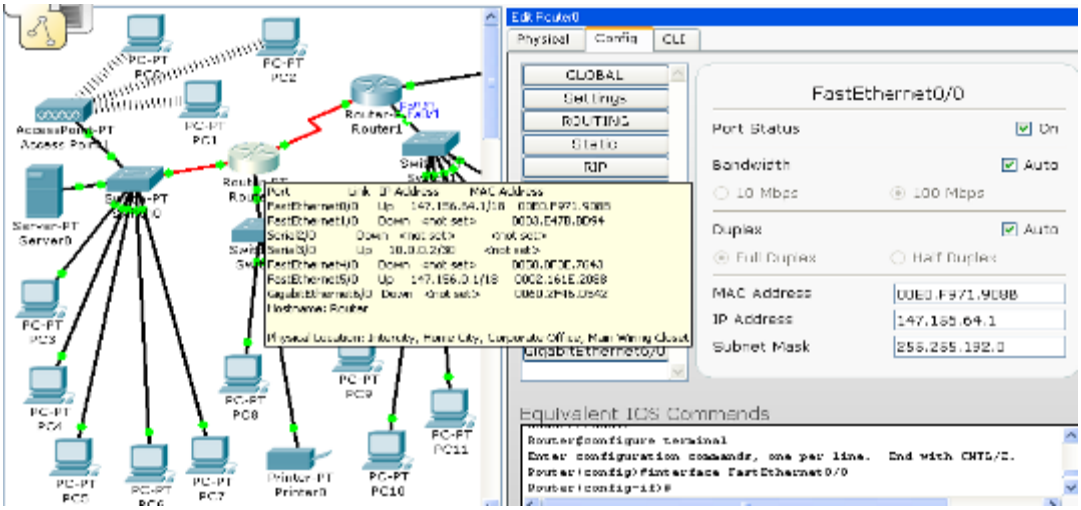

Figura 2.2.8.1 Routers

2.2.9. Procedemos a dar un clic sobre los switchs y verificamos que todos los puertos estén encendidos y funcionando correctamente, para ello ingresamos en la parte que dice Fast Ethernet en la plantilla config como se puede observar en la figura.

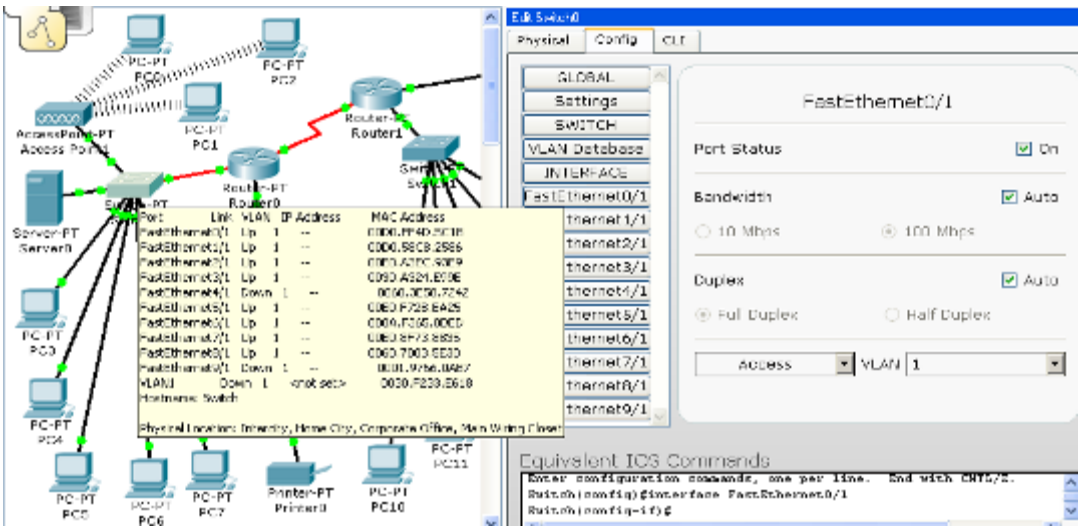

Figura 2.2.9.1 Switchs

2.3. Desarrollo

2.3.1. Para comprobar su funcionamiento colocamos un paquete simple señalando el lugar de origen y destino para la transferencia de información, en el scenario 0 se va a comprobar la conexión entre la

PC0 y la PC10 al enviar y recibir los datos, como se puede observar en la figura 2.3.1.1

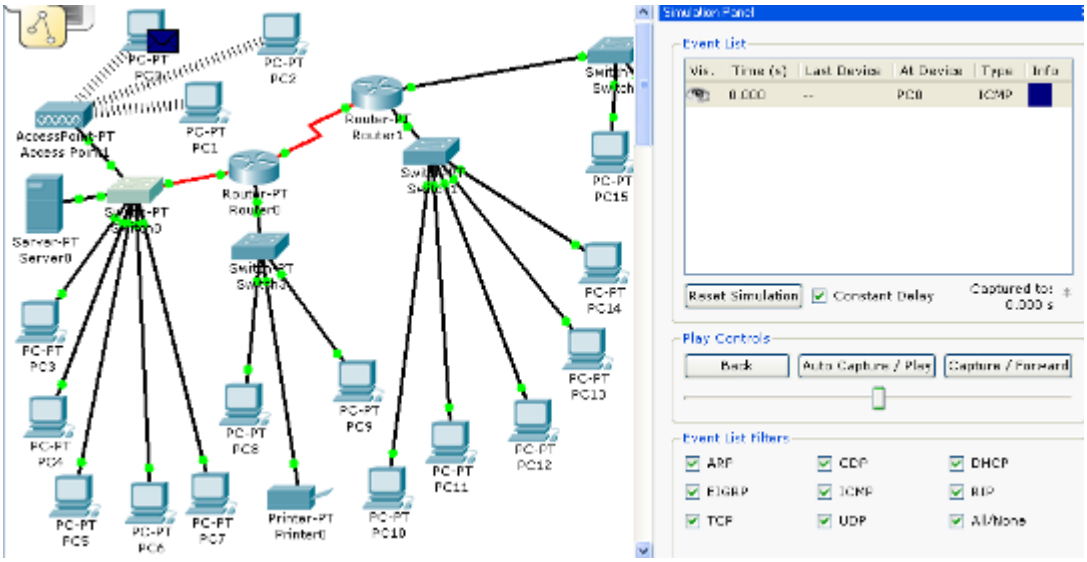

Figura 2.3.1.1 Colocación de paquete

2.3.2. En las figuras 2.3.2.1, 2.3.2.2, 2.3.2.3, 2.3.2.4, 2.3.2.5 y 2.3.2.6 a continuación, se puede observar con su respectiva simulación del paquete que se va trasladándose paso a paso por cada uno de los dispositivos de la red hasta que finalmente llega a la PC10 comprobando de esta manera que la conexión correspondiente está funcionando.

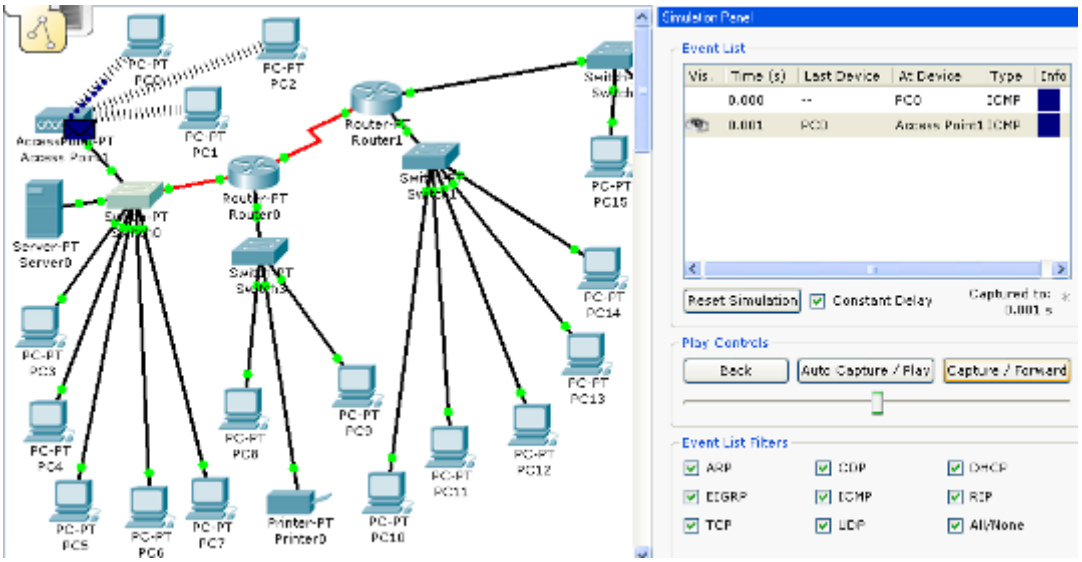

Figura 2.3.2.1 Simulación 1

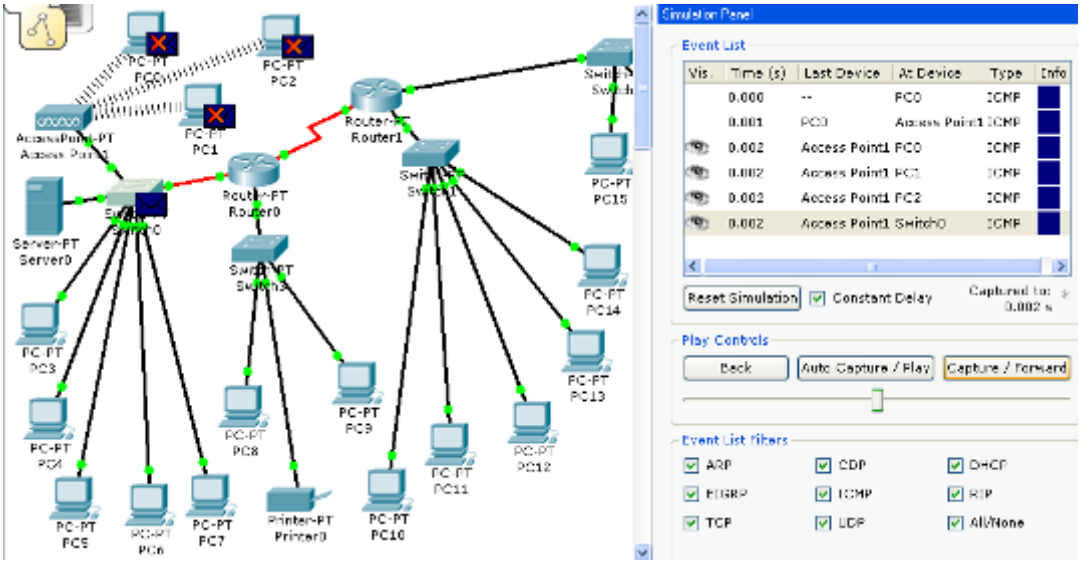

Figura 2.3.2.2 Simulación 2

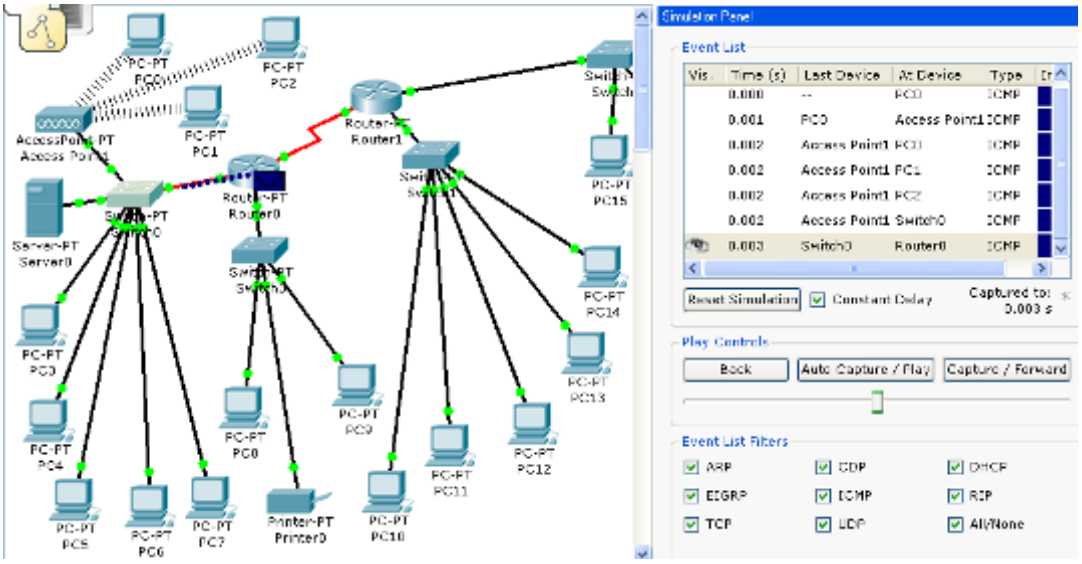

Figura 2.3.2.3 Simulación 3

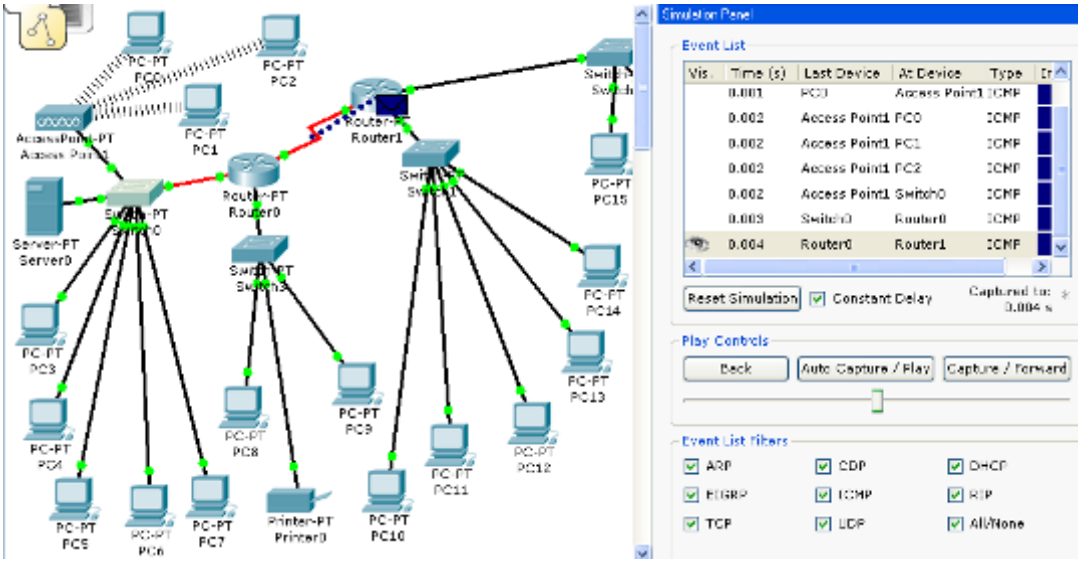

Figura 2.3.2.4 Simulación 4

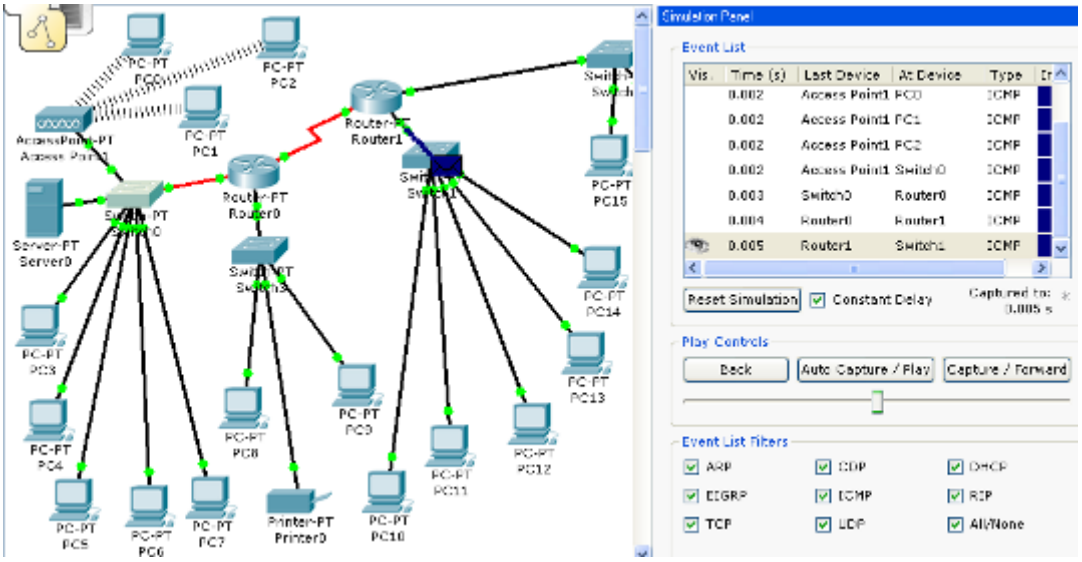

Figura 2.3.2.5 Simulación 5

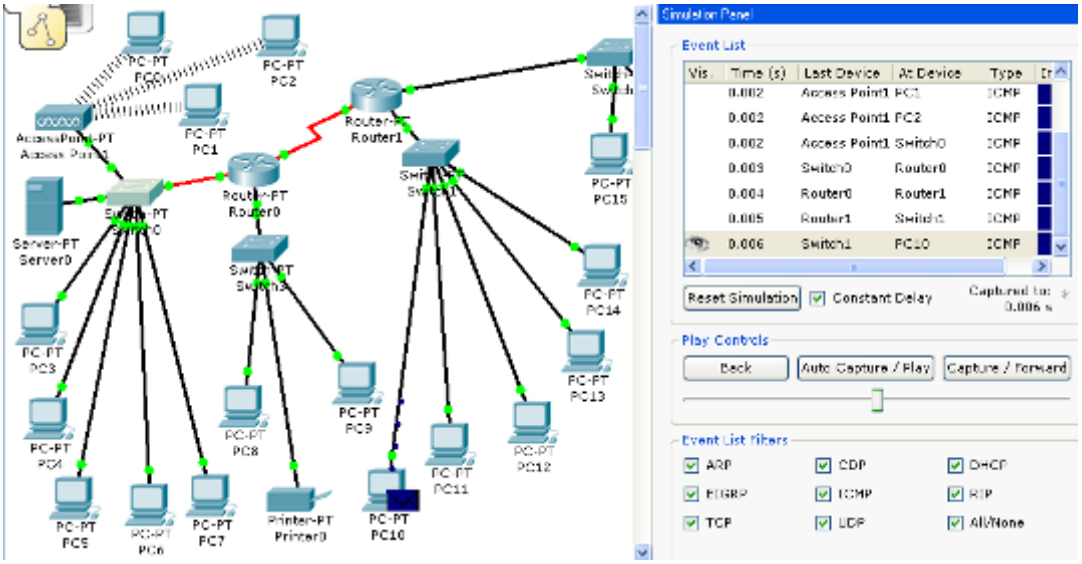

Figura 2.3.2.6 Simulación 6

2.3.3. En las figuras 2.3.3.1, 2.3.3.2, 2.3.3.3, 2.3.3.4, 2.3.3.5 y 2.3.3.6 a continuación se observa que el paquete se traslada de la PC10 a la PC0 paso a paso por cada uno de los dispositivos de la red hasta que finalmente llega a la PC0 comprobando de esta manera que la conexión entre la PC0 y la PC10 se encuentra funcionando correctamente.

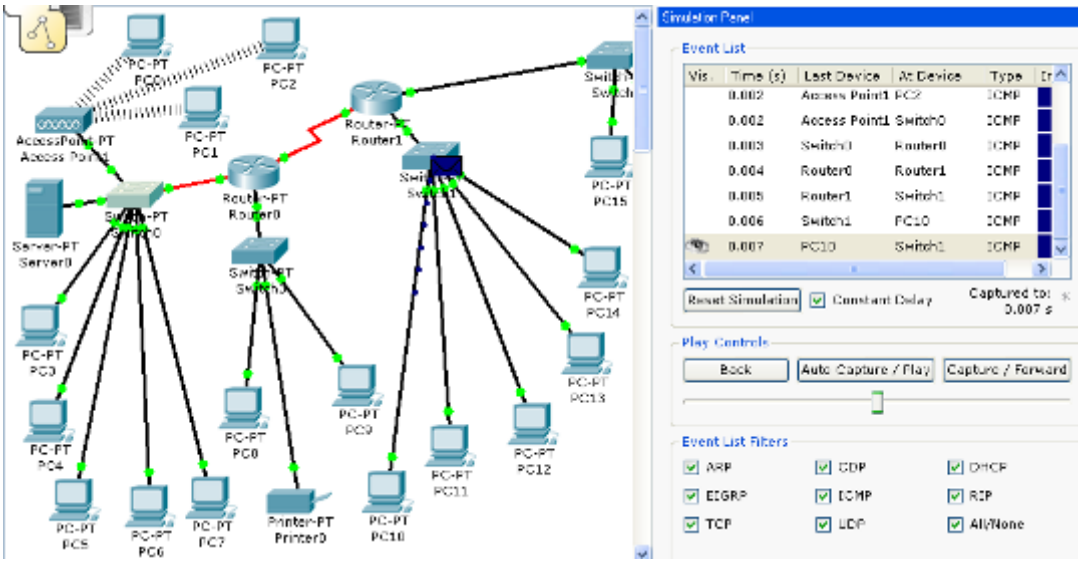

Figura 2.3.3.1 Simulación 7

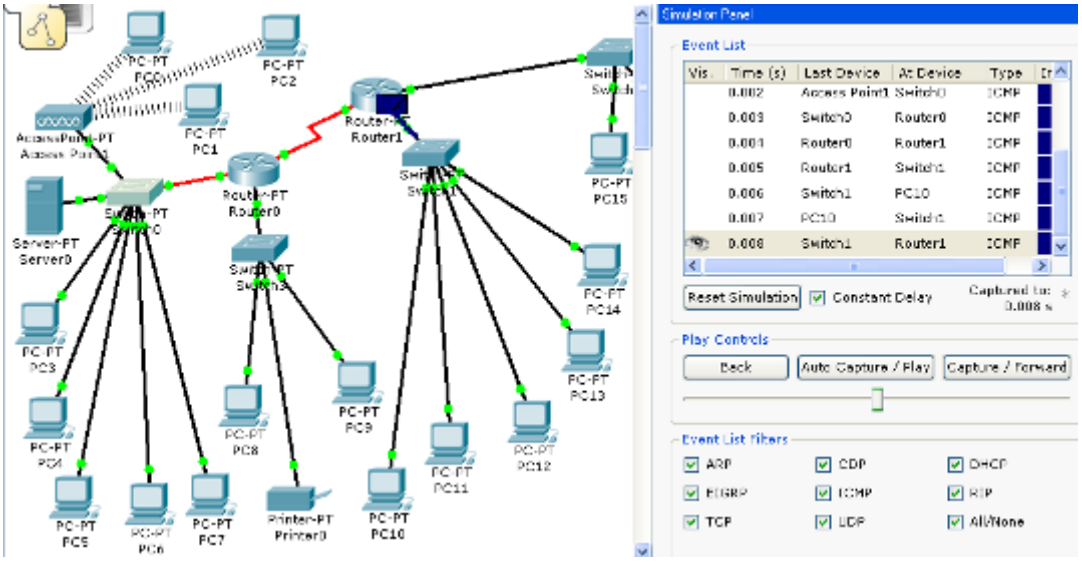

Figura 2.3.3.2 Simulación 8

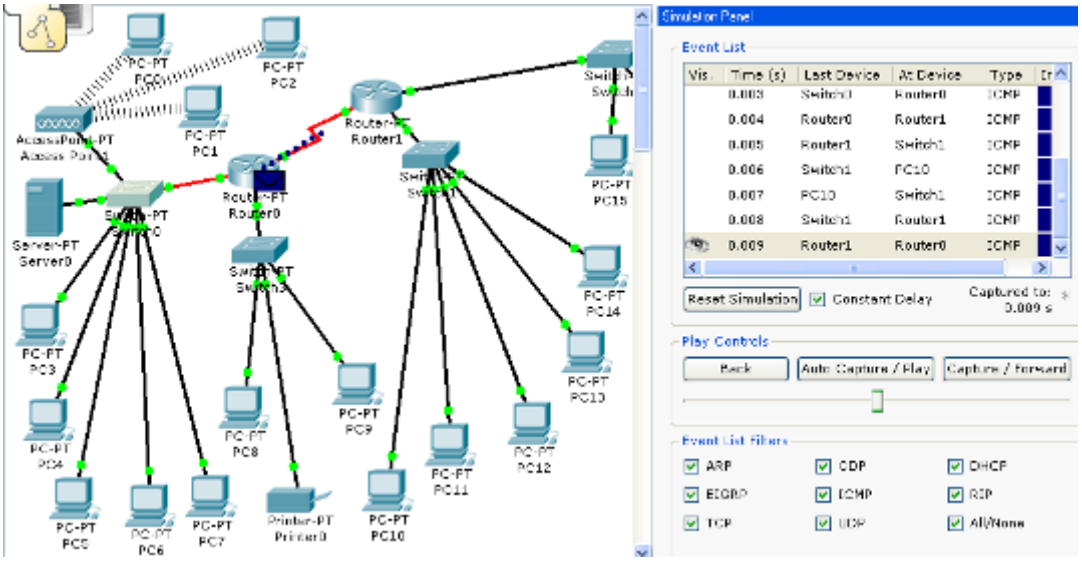

Figura 2.3.3.3 Simulación 9

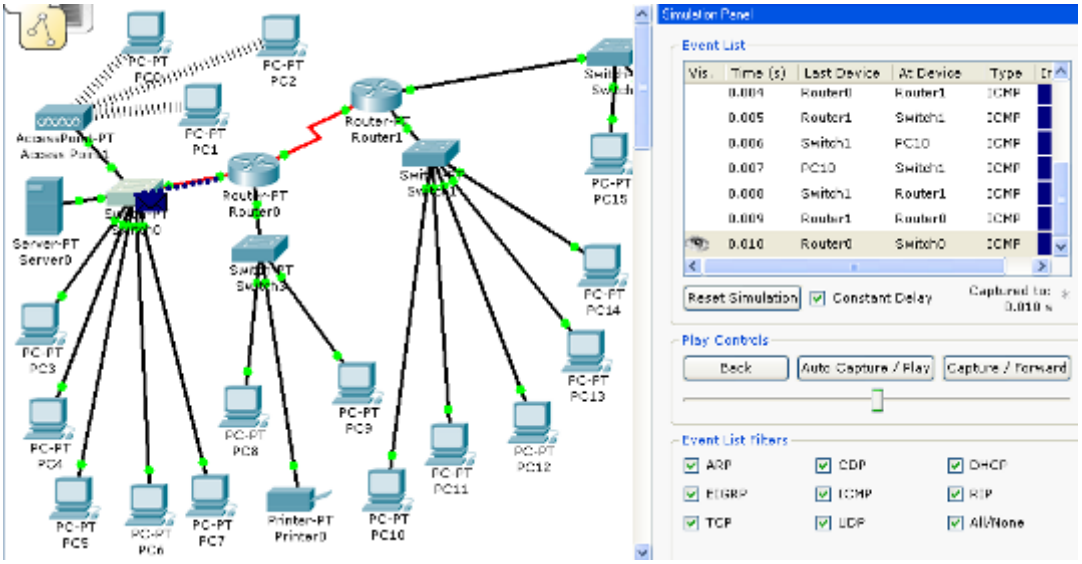

Figura 2.3.3.4 Simulación 10

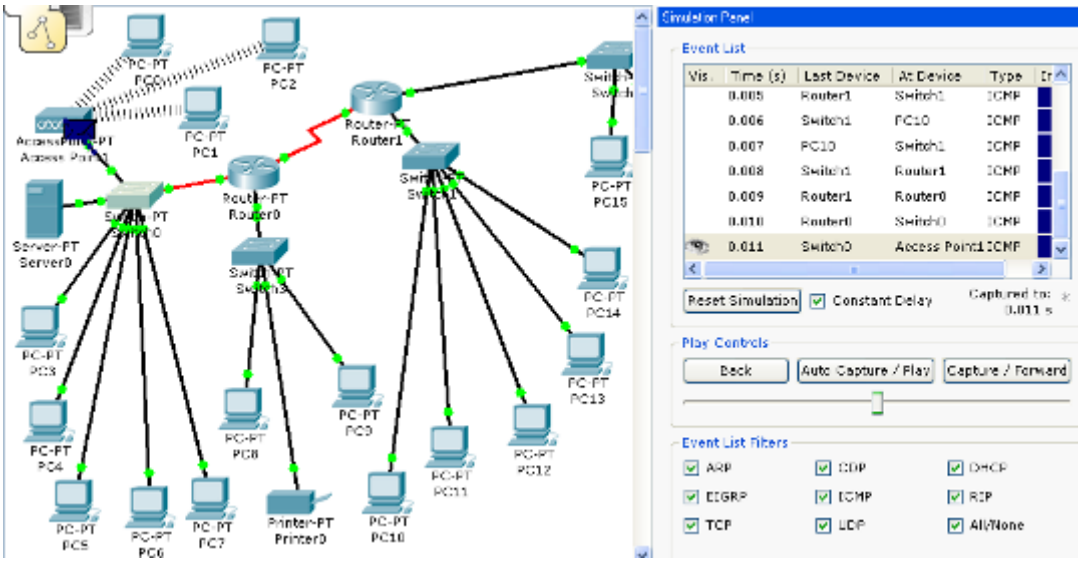

Figura 2.3.3.5 Simulación 11

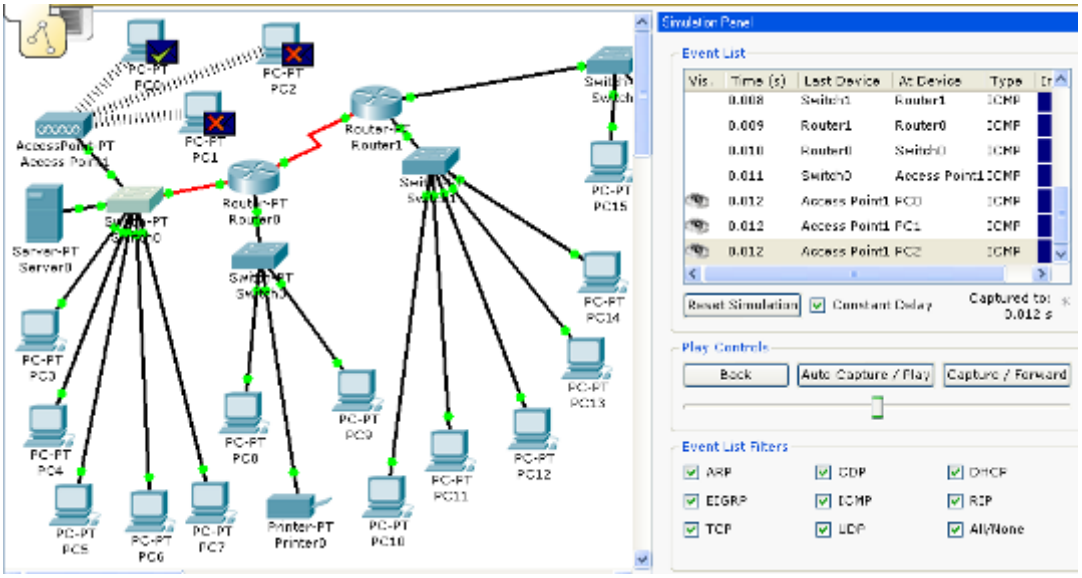

Figura 2.3.3.6 Simulación 12

2.4. Análisis de resultados

2.4.1. En la figuras se realizaron las subdivisiones de las subredes de la clase tipo B, la cual usamos para configurar las distintas PC´s y para cada switch usaremos una subred distinta.

2.4.2. Se muestran claramente que el paquete fue enviado y recibido correctamente a su destino, confirmando de esta manera que la conexión se encuentra en perfecto estado.

2.4.3. En nuestro caso se debe conectar con cable serial cuando se conecta dos ruteadores, y se puede conectar con cable directo o fibra óptica entre los ruteadores y los switch como se muestra en nuestro caso.

2.5. Conclusiones

2.5.1. Se puede ver claramente en las graficas que las subredes de la clase B funcionan correctamente al trasladar la información de una subred a otra sin ningún inconveniente

2.5.2. Con la simulación realizada se cumplieron los objetivos requeridos transmitiendo datos por toda la red.

2.5.3. En las graficas de la simulación se pueden observar muy claramente que todos los paquetes se trasladaron sin ningún problema por toda la red.

CAPÍTULO III

3.1. PROTOCOLOS E INTERCONEXION DE REDES

Al momento de diseñar una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes.

El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario y visible para el administrador de la red. Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

3.2. Dispositivos de interconexión de redes.

3.2.1. Repetidores

El repetidor es un elemento que permite la conexión de dos tramos de red, teniendo como función principal regenerar eléctricamente la señal, para permitir alcanzar distancias mayores manteniendo el mismo nivel de la señal a lo largo de la red. De esta forma se puede extender, teóricamente, la longitud de la red hasta el infinito.

Un repetidor interconecta múltiples segmentos de red en el nivel físico del modelo de referencia OSI. Por esto sólo se pueden utilizar para unir dos redes que tengan los mismos protocolos de nivel físico.

Los repetidores no discriminan entre los paquetes generados en un segmento y los que son generados en otro segmento, por lo que los paquetes llegan a todos los nodos de la red. Debido a esto existen más riesgos de colisión y más posibilidades de congestión de la red.

Se pueden clasificar en dos tipos:

- Locales: cuando enlazan redes próximas.
- Remotos: cuando las redes están alejadas y se necesita un medio intermedio de comunicación.

Normalmente la utilización de repetidores está limitada por la distancia máxima de la red y el tamaño máximo de cada uno de los segmentos de red conectados. En las redes Ethernet, por problemas de gestión de tráfico en la red, no deben existir más de dos repetidores entre dos equipos terminales de datos, lo que limita la distancia máxima entre los nodos más lejanos de la red a 1.500 m. (enlazando con dos repetidores tres segmentos de máxima longitud, 500 m).

Ventajas

- Incrementa la distancia cubierta por la RAL.
- Retransmite los datos sin retardos.
- Es transparente a los niveles superiores al físico.

Desventajas

- Incrementa la carga en los segmentos que interconecta.
- Los repetidores son utilizados para interconectar RALs que estén muy próximas, cuando se quiere una extensión física de la red. La tendencia actual es dotar de más inteligencia y flexibilidad a los repetidores, de tal forma que ofrezcan capacidad de gestión y soporte de múltiples medios físicos, como Ethernet sobre par trenzado (10BaseT), ThickEthernet (10Base5), ThinEthernet (10Base2), TokenRing, fibra óptica, etc.

3.2.2. Concentradores (Hubs)

El término concentrador o hub describe la manera en que las conexiones de cableado de cada nodo de una red se centralizan y conectan en un único dispositivo. Se suele aplicar a concentradores Ethernet, Token Ring, y FDDI (Fiber Distributed Data Interface) soportando módulos individuales que concentran múltiples tipos de funciones en un solo dispositivo. Normalmente los concentradores incluyen ranuras para aceptar varios módulos y un panel trasero común para funciones de encaminamiento, filtrado y conexión a diferentes medios de transmisión (por ejemplo Ethernet y TokenRing). Los primeros hubs o de "primera generación" son cajas de cableado avanzadas que ofrecen un punto central de conexión conectado a varios puntos. Sus principales beneficios son la conversión de medio (por ejemplo de coaxial a fibra óptica).

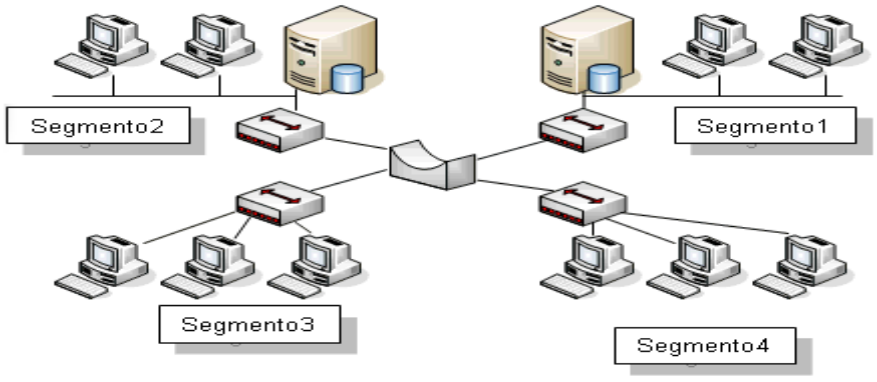

Figura 3.2.2.1

Los hubs inteligentes de "segunda generación" basan su potencial en las posibilidades de gestión ofrecidas por las topologías radiales (TokenRing y Ethernet). Tiene la capacidad de gestión, supervisión y control remoto, dando a los gestores de la red la oportunidad de ofrecer un período mayor de funcionamiento de la red gracias a la aceleración del diagnóstico y solución de problemas. Sin embargo tienen limitaciones cuando se intentan emplear como herramienta universal de configuración y gestión de arquitecturas complejas y heterogéneas.

Los nuevos hubs de "tercera generación" ofrecen proceso basado en arquitectura RISC (Reduced Instructions Set Computer) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios buses independientes Ethernet, TokenRing, FDDI y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación. A un hub Ethernet se le denomina "repetidor multipuerta". El dispositivo repite simultáneamente la señal a múltiples cables conectados en cada uno de los puertos del hub. En el otro extremo de cada cable está un nodo de la red, por ejemplo un ordenador personal. Un hub Ethernet se convierte en un hub inteligente (smart hub) cuando puede soportar inteligencia añadida para realizar monitorización y funciones de control.

Los concentradores inteligentes (smart hub) permiten a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporcionan una estructura de crecimiento ordenado de la red. La capacidad de gestión remota de los hubs inteligentes hace posible el diagnóstico remoto de un problema y aísla un punto con problemas del resto de la RAL, con lo que otros usuarios no se ven afectados.

El tipo de hub Ethernet más popular es el hub 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento

también se encarga de desconectar las salidas cuando se produce una situación de error

3.2.3. Puentes (Bridges)

Son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado no local. Al distinguir los tráficos locales y no locales, estos elementos disminuyen el mínimo total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a la congestión de la red.

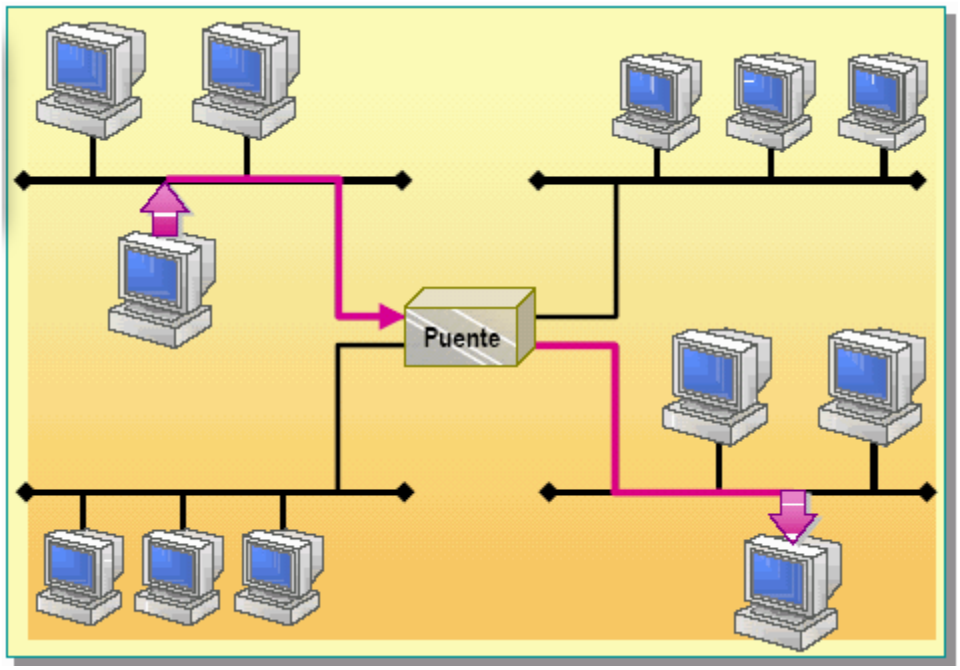

Figura 3.2.3.1

Operan en el Nivel de Enlace del modelo de referencia OSI, en el nivel de trama MAC (Medium Access Control, Control de Acceso al Medio) y se utilizan para conectar o extender redes similares, es decir redes que tienen protocolos idénticos en los dos niveles inferiores OSI, (como es TokenRing con TokenRing, Ethernet con Ethernet, etc) y conexiones a redes de área extensa.

Se encargan de filtrar el tráfico que pasa de una a otra red según la dirección

de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas.

Las redes conectadas a través de bridge aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece a uno u otro segmento.

Un bridge ejecuta tres tareas básicas:

- Aprendizaje de las direcciones de nodos en cada red.
- Filtrado de las tramas destinadas a la red local.
- Envío de las tramas destinadas a la red remota.

Se distinguen dos tipos de bridge:

- Locales: sirven para enlazar directamente dos redes físicamente cercanas.
- Remotos o de área extensa: se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas.

Se puede realizar otra división de los bridges en función de la técnica de filtrado y envío (bridging) que utilicen:

- Spanning Tree Protocol Bridge o Transparent Protocol Bridge (Protocolo de Arbol en Expansión o Transparente, STP).

Spanning Tree Protocol (STP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos, Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las

conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de lazos. STP es transparente a las estaciones de usuario.

Cuando hay lazos en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast y multicast, al no existir ningún campo TTL (Time To Live, Tiempo de Vida) en la Capa 2, tal y como ocurre en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos casos la red queda inutilizada. Un router, por el contrario, si podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de lazos. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Estos bridges deciden qué paquetes se filtran en función de un conjunto de tablas de direcciones almacenadas internamente. Su objetivo es evitar la formación de lazos entre las redes que interconecta. Se emplea normalmente en entornos Ethernet.

- Source Routing Protocol Bridge (Bridge de Protocolo de Encaminamiento por Emisor, SRP).
- El emisor ha de indicar al bridge cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en entornos TokenRing.
- Source Routing Transparent Protocol Bridge (Bridge de Protocolo de Encaminamiento por Emisor Transparente, SRTP).

Este tipo de bridges pueden funcionar en cualquiera de las técnicas anteriores.

Ventajas

- Fiabilidad. Utilizando bridges se segmentan las redes de forma que un fallo sólo imposibilita las comunicaciones en un segmento.
- Eficiencia. Segmentando una red se limita el tráfico por segmento, no influyendo el tráfico de un segmento en el de otro.
- Seguridad. Creando diferentes segmentos de red se pueden definir distintos niveles de seguridad para acceder a cada uno de ellos, siendo no visible por un segmento la información que circula por otro.
- Dispersión. Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los bridges permiten romper esa barrera de distancias.

Desventajas

- Son ineficientes en grandes interconexiones de redes, debido a la gran cantidad de tráfico administrativo que se genera.
- Pueden surgir problemas de temporización cuando se encadenan varios bridges.
- Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

Las aplicaciones de los bridges está en soluciones de interconexión de RALs similares dentro de una interconexión de redes de tamaño pequeño-medio, creando una única red lógica y obteniendo facilidad de instalación, mantenimiento y transparencia a los protocolos de niveles superiores. También son útiles en conexiones que requieran funciones de filtrado. Cuando se quiera interconectar pequeñas redes.

3.2.4. ROUTER

En un entorno que está formado por diferentes segmentos de red con distintos protocolos y arquitecturas, el bridge podría resultar inadecuado para asegurar una comunicación rápida entre todos los segmentos. Una red de esta complejidad necesita un dispositivo que no sólo conozca las direcciones de cada segmento, sino también, que sea capaz de determinar el camino más rápido para el envío de datos y filtrado del tráfico de difusión en el segmento local.

Los routers trabajan en el nivel de red del modelo de referencia OSI. Esto significa que pueden conmutar y encaminar paquetes a través de múltiples redes. Realizan esto intercambiando información específica de protocolos entre las diferentes redes. Los routers leen en el paquete la información de direccionamiento de las redes complejas teniendo acceso a información adicional, puesto que trabajan a un nivel superior del modelo OSI en comparación con los bridges.

Los routers pueden proporcionar las siguientes funciones de un bridge:

- Filtrado y aislamiento del tráfico.
- Conexión de segmentos de red.

Los routers tienen acceso a más información en los paquetes de la que tienen los bridges y utilizan esta información para mejorar la entrega de los paquetes. Los routers se utilizan en redes complejas puesto que proporcionan una mejor gestión del tráfico. Los routers pueden compartir con otro router el estado y la información de encaminamiento y utilizar esta información para evitar conexiones lentas o incorrectas.

¿Cómo funcionan los routers?

Los routers mantienen sus propias tablas de encaminamiento, normalmente constituidas por direcciones de red; también se pueden incluir las direcciones de los hosts si la arquitectura de red lo requiere. Para determinar la dirección de destino de los datos de llegada, las tablas de encaminamiento incluyen:

- Todas las direcciones de red conocidas.
- Instrucciones para la conexión con otras redes.
- Los posibles caminos entre los routers.
- El coste de enviar los datos a través de estos caminos.

Un router utiliza sus tablas de encaminamiento de datos para seleccionar la mejor ruta en función de los caminos disponibles y del coste.

La tabla de encaminamiento que mantiene un bridge contienen las direcciones del subnivel MAC para cada nodo, mientras que la tabla de encaminamiento que mantiene un router contiene números de red. Aunque los fabricantes de ambos tipos de equipamiento han seleccionado utilizar el término «tabla de encaminamiento», tienen diferente significado para cada uno de los dispositivos.

Los routers requieren direcciones específicas. Entienden sólo los números de red que les permiten comunicarse con otros routers y direcciones NIC locales. Los routers no conversan con equipos remotos. Cuando los routers reciben paquetes destinados a una red remota, los envían al router que gestiona la red de destino. En algunas ocasiones esto constituye una ventaja porque significa que los routers pueden:

- Segmentar grandes redes en otras más pequeñas.
- Actuar como barrera de seguridad entre los diferentes segmentos.

- Prohibir las tormentas de difusión, puestos que no se envían estos mensajes de difusión.

Los routers son más lentos que los bridges, puesto que deben realizar funciones complejas sobre cada paquete. Cuando se pasan los paquetes de router a router, se separan las direcciones de origen y de destino del nivel de enlace de datos y, a continuación, se vuelven a generar. Esto activa a un router para encaminar desde una red Ethernet TCP/IP a un servidor en una red Token Ring TCP/IP.

Dado que los routers sólo leen paquetes direccionados de red, no permiten pasar datos corruptos a la red. Por tanto, al no permitir pasar datos corruptos ni tormentas de difusión de datos, los routers implican muy poca tensión en las redes.

Los routers no ven la dirección del nodo de destino, sólo tienen control de las direcciones de red. Los routers pasarán información sólo si conocen la dirección de la red. Esta capacidad de controlar el paso de datos a través del router reduce la cantidad de tráfico entre las redes y permite a los routers utilizar estos enlaces de forma más eficiente que los bridges.

La utilización de un esquema de direccionamiento basado en router permite a los administradores poder dividir una gran red en muchas redes separadas, y dado que los routers no pasan e incluso controlan cada paquete, actúan como una barrera de seguridad entre los segmentos de la red. Esto permite reducir bastante la cantidad de tráfico en la red y el tiempo de espera por parte de los usuarios.

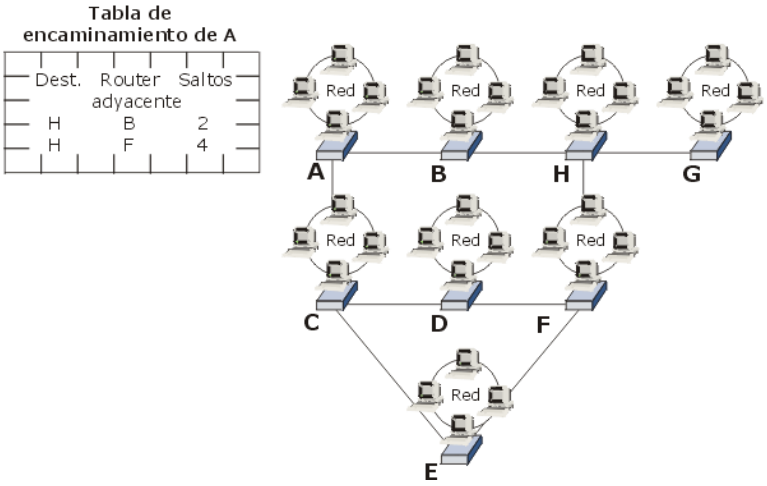

Figura 3.2.4.1 Router

Protocolos que permiten encaminar

No todos los protocolos permiten encaminar.

Los protocolos que encaminan son:

- DECnet.
- Protocolo de Internet (IP).
- Intercambio de paquetes entre redes (IPX).
- OSI.
- Sistema de red de Xerox (XNS).
- DDP (Apple Talk).

Los protocolos que no pueden encaminar son:

- Protocolo de transporte de área local (LAT), un protocolo de Digital Equipment Corporation.
- NetBEUI (Interfaz de usuario extendida NetBIOS).

Los routers pueden utilizar en la misma red múltiples protocolos.

Un router puede escuchar una red e identificar las partes que están ocupadas. Esta información la utiliza para determinar el camino sobre el que envía los datos. Si un camino está ocupado, el router identifica un camino alternativo para poder enviar los datos.

Un router decide el camino que seguirá el paquete de datos determinando el número de saltos que se generan entre los segmentos de red. Al igual que los bridges, los routers generan tablas de encaminamiento y las utilizan en los siguientes algoritmos de encaminamiento:

- **OSPF** (Primer camino abierto más corto) es un algoritmo de encaminamiento basado en el estado del enlace. Los algoritmos de estado de enlace controlan el proceso de encaminamiento y permiten a los routers responder rápidamente a modificaciones que se produzcan en la red.
- **RIP** (Protocolo de información de encaminamiento) utiliza algoritmos con vectores de distancia para determinar la ruta. El Protocolo de control de transmisión/Protocolo de Internet (TCP/IP) e IPX admite RIP.
- **NLSP** (Protocolo de servicios de enlace NetWare) es un algoritmo de estado de enlace a utilizar con IPX.

Tipos de Enrutamiento

Los tipos principales de enrutamiento son:

- **Estático**. Los routers estáticos requieren un administrador para generar y configurar manualmente la tabla de encaminamiento y para especificar cada ruta.

  Se presentan las siguientes características:

- Instalación y configuración manual de todos los routers
- Utilizan siempre la misma ruta, determinada a partir de una entrada en la tabla de encaminamiento
- Utilizan una ruta codificada (designada para manejar sólo una situación específica), no necesariamente la ruta más corta.
- Se consideran más seguros puesto que los administradores especifican cada ruta

- **Dinámico**. Los routers dinámicos se diseñan para localizar, de forma automática, rutas y, por tanto, requieren un esfuerzo mínimo de instalación y configuración. Son más sofisticados que los routers estáticos, examinan la información de otros routers y toman decisiones a nivel de paquete sobre cómo enviar los datos a través de la red.

  Se presentan las siguientes características:

  - Configuración manual del primer router. Detectan automáticamente redes y routers adicionales.
  - Pueden seleccionar una ruta en función de factores tales como coste y cantidad del tráfico de enlace.
  - Pueden decidir enviar paquetes sobre rutas alternativas.
  - Pueden mejorar la seguridad configurando manualmente el router para filtrar direcciones específicas de red y evitar el tráfico a través estas direcciones.

Diferencias entre bridges y routers

El bridge, que trabaja en el subnivel MAC del nivel de enlace de datos del modelo OSI, como se puede observar en la figura 3.2.4.2, utiliza sólo la dirección del nodo. Para ser más específicos, un bridge trata de localizar una dirección del subnivel MAC en cada paquete. Si el bridge reconoce la dirección,

mantiene el paquete o lo reenvía al segmento apropiado. Si el bridge no reconoce la dirección, envía el paquete a todos los segmentos excepto al segmento del cual ha partido el paquete.

Un bridge es de capa 2 y hace un direccionamiento estático y el router es capa 3, y hace direccionamiento lógico. El bridge hace conmutación mientras que el router hace enrutamiento.

Primero, el bridge reconoce o no la dirección del subnivel MAC del paquete y, a continuación, envía el paquete.

Difusión. El envío de paquetes es la clave para entender las diferencias que plantean los bridges y los routers. Con los bridges, los datos de difusión enviados se dirigen a cada equipo desde todos los puertos del bridge, excepto desde el puerto a través del cual ha llegado el paquete. Es decir, cada equipo de todas las redes (excepto la red local a partir de la cual se ha generado la difusión) recibe un paquete de difusión. En las redes pequeñas esto puede que no tenga mucho impacto, pero en una red grande se puede generar el suficiente tráfico de difusión que provoque una bajada de rendimiento de la red, incluso filtrando las direcciones de la misma.

El router, que trabaja a nivel de red, como se puede observar en la figura 3.2.4.2, y tiene en cuenta más información que el bridge, determinando no sólo qué enviar, sino también dónde enviarlo. El router reconoce no sólo una dirección, al igual que el bridge, sino también un tipo de protocolo. De forma adicional, el router puede identificar las direcciones de otros routers y determinar los paquetes que se envían a otros routers.

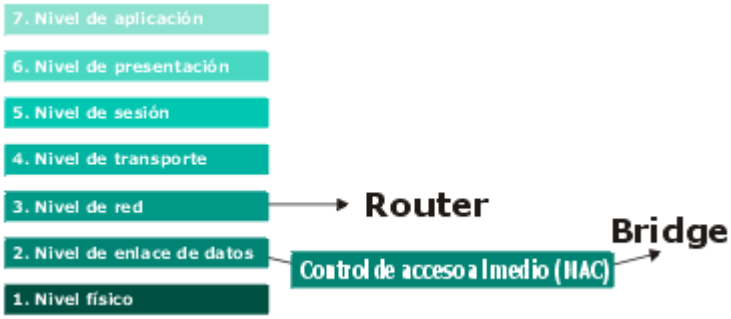

Figura 3.2.4.2 Capas Bridge, Router

Múltiples caminos. Si un router A realiza una transmisión que necesita enviarse al router D, puede enviar el mensaje al router C o al B, y el mensaje será enviado al router D. Los routers tienen la posibilidad de evaluar ambos caminos y decidir la mejor ruta para esta transmisión, como se puede observar en la figura 3.2.4.3

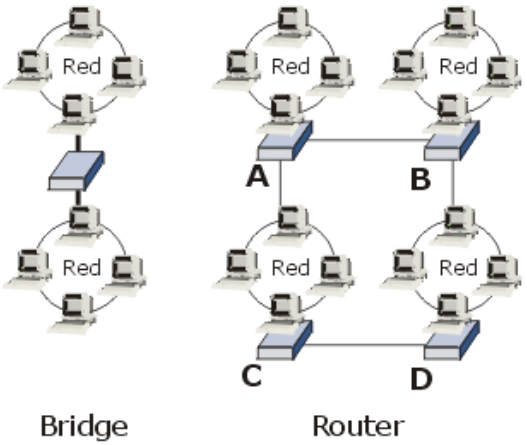

Figura 3.2.4.3 Caminos Router, Bridge

Conclusiones

- El bridge reconoce sólo las direcciones locales a subnivel MAC (las direcciones de las NIC en su propio segmento). Los routers reconocen direcciones de red.
- El bridge difunde (envía) todo lo que no reconoce y lo envía a todas las direcciones que controla, pero sólo desde el puerto apropiado.
- El router trabaja sólo con protocolos encaminables.

- El router filtra las direcciones. Envía protocolos particulares a direcciones determinadas (otros routers).

3.2.5. B-routers

Un b-router combina las cualidades de un bridge y un router. Un brouter puede actuar como un router para un protocolo y como un bridge para el resto.

Los b-routers pueden:

- Encaminar protocolos encaminables seleccionados.
- Actuar de bridge entre protocolos no encaminables.
- Proporcionar un mejor coste y gestión de interconexión que el que proporcionan los bridges y routers por separado.

3.2.6. Pasarelas (Gateways)

Estos dispositivos están pensados para facilitar el acceso entre sistemas o entornos soportando diferentes protocolos. Operan en los niveles más altos del modelo de referencia OSI (Nivel de Transporte, Sesión, Presentación y Aplicación) y realizan conversión de protocolos para la interconexión de redes con protocolos de alto nivel diferentes.

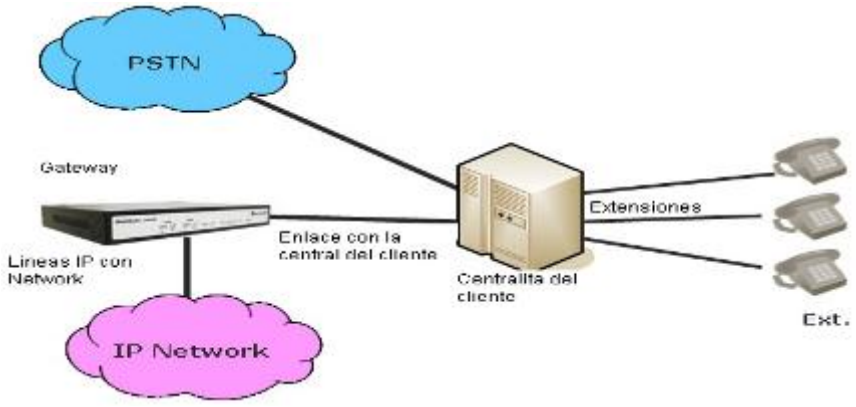

Figura 3.2.4.4

Los gateways activan la comunicación entre diferentes arquitecturas y entornos. Se encargan de empaquetar y convertir los datos de un entorno a otro, de forma que cada entorno pueda entender los datos del otro entorno. Un gateway empaqueta información para que coincida con los requerimientos del sistema destino. Los gateways pueden modificar el formato de un mensaje para que se ajuste al programa de aplicación en el destino de la transferencia. Por ejemplo, los gateways de correo electrónico, como el X.400, reciben mensajes en un formato, los formatean y envían en formato X.400 utilizado por el receptor, y viceversa.

Un gateway enlaza dos sistemas que no utilizan los mismos:

- Protocolos de comunicaciones.
- Estructuras de formateo de datos.
- Lenguajes.
- Arquitectura.

Los gateways interconectan redes heterogéneas; por ejemplo, pueden conectar un servidor Windows NT de Microsoft a una Arquitectura de red de los sistemas IBM (SNA). Los gateways modifican el formato de los datos y los adaptan al programa de aplicación del destino que recibe estos datos.

Los gateways son de tarea específica. Esto significa que están dedicados a un tipo de transferencia. A menudo, se referencian por su nombre de tarea (gateway Windows NT Server a SNA).

Un gateway utiliza los datos de un entorno, desmantela su pila de protocolo anterior y empaqueta los datos en la pila del protocolo de la red destino.

Para procesar los datos, el gateway:

- Desactiva los datos de llegada a través de la pila del protocolo de la red.
- Encapsula los datos de salida en la pila del protocolo de otra red para permitir su transmisión.

Algunos gateways utilizan los siete niveles del modelo OSI, pero, normalmente, realizan la conversión de protocolo en el nivel de aplicación. No obstante, el nivel de funcionalidad varía ampliamente entre los distintos tipos de gateways.

Una utilización habitual de los gateways es actuar como traductores entre equipos personales y mini equipos o entornos de grandes sistemas. Un gateway en un host que conecta los equipos de una LAN con los sistemas de mini equipo o grandes entornos (mainframe) que no reconocen los equipos conectados a la LAN.

En un entorno LAN normalmente se diseña un equipo para realizar el papel de gateway. Los programas de aplicaciones especiales en los equipos personales acceden a los grandes sistemas comunicando con el entorno de dicho sistema a través del equipo gateway. Los usuarios pueden acceder a los recursos de los grandes sistemas sólo cuando estos recursos están en sus propios equipos personales.

Normalmente, los gateways se dedican en la red a servidores. Pueden utilizar un porcentaje significativo del ancho de banda disponible para un servidor, puesto que realizan tareas que implican una utilización importante de recursos, tales como las conversiones de protocolos. Si un servidor gateway se utiliza para múltiples tareas, será necesario adecuar las necesidades de ancho de banda y de RAM o se producirá una caída del rendimiento de las funciones del servidor.

Los gateways se consideran como opciones para la implementación, puesto que no implican una carga importante en los circuitos de comunicación de la red y realizan, de forma eficiente, tareas muy específicas.

CAPITULO IV

4.1. SERVICIOS DE RED

Entre los protocoles que tenemos para la administración de redes el más importante es el protocolo SNMP, a continuación hare una pequeña introducción de este protocolo.

SNMP (Simple Network Management Protocol), en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP, protocolo del mundo UNIX, y que ha llegado a convertirse en un estándar. Surge a raíz del interés mostrado por la IAB (Internet Activities Board) en encontrar un protocolo de gestión que fuese válido para la red Internet, dada la necesidad del mismo debido a las grandes dimensiones que estaba tomando. Los tres grupos de trabajo que inicialmente se formaron llegaron a conclusiones distintas, siendo finalmente el SNMP (RFC 1098) el adoptado, incluyendo éste algunos de los aspectos más relevantes presentados por los otros dos: HEMS (High-Level Management System) y SGMP (Simple Gateway Monitoring Protocol).

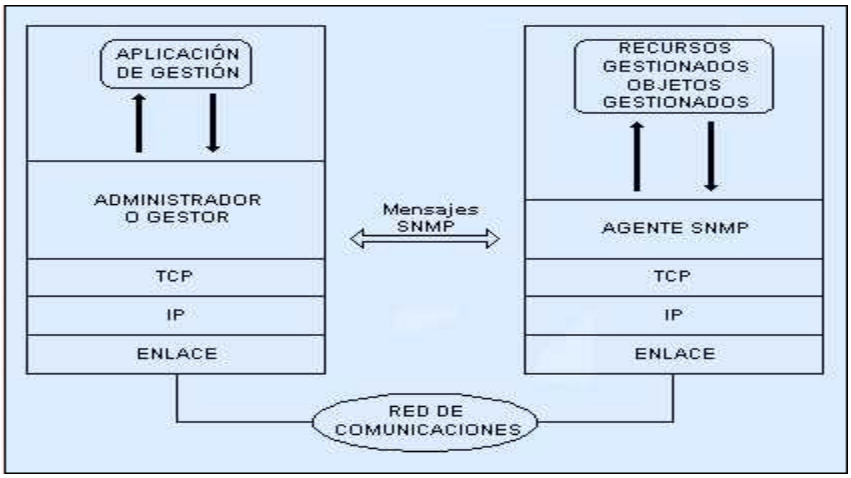

Figura 4.1.1

SNMP se sitúa en el tope de la capa de transporte de la pila OSI, o por encima de la capa UDP de la pila de protocolos TCP/IP. Siempre en la capa de transporte. Gráficamente se podría ver así:

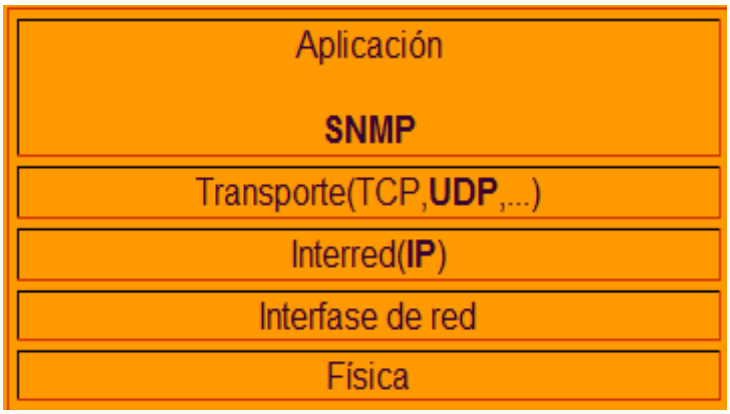

Figura 4.1.2

4.2. PROTOCOLOS WAN

Una red de área amplia o WAN (Wide Area Network), se extiende sobre un área geográfica extensa, a veces un país o un continente; contiene un número variado de hosts dedicadas a ejecutar programas de usuario (de aplicación). Las hosts están conectadas por una de subred comunicación, o simplemente subred. El trabajo de la subred es conducir mensajes de una host a otra.

En muchas redes WAN, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (circuitos, canales o troncales) mueven bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para reenviarlos. Aunque no existe una terminología estándar para designar estas computadoras, se les denomina nodos conmutadores de paquetes, sistemas

intermedios y centrales de conmutación de datos. También es posible llamarles simplemente enrutadores.

4.2.1. Servicios de conmutación de circuitos

En una conexión de conmutación de circuitos se establece un canal dedicado, denominado circuito, entre dos puntos por el tiempo que dura la llamada. El circuito proporciona una cantidad fija de ancho de banda durante la llamada y los usuarios sólo pagan por esa cantidad de ancho de banda el tiempo que dura la llamada.

Las conexiones de conmutación de circuitos tienen dos serios inconvenientes. El primero es que debido a que el ancho de banda en estas conexiones es fijo, no manejan adecuadamente las avalanchas de tráfico, requiriendo frecuentes retransmisiones. El segundo inconveniente es que estos circuitos virtuales sólo tienen una ruta, sin caminos alternativos definidos. Por esta razón cuando una línea se cae, es necesario que un usuario intervenga reencamine el tráfico manualmente o se detiene la transmisión.

4.2.2. Servicios de conmutación de paquetes

Los servicios de conmutación de paquetes suprimen el concepto de circuito virtual fijo. Los datos se transmiten paquete a paquete a través del entramado de la red o nube, de manera que cada paquete puede tomar un camino diferente a través de la red. Como no existe un circuito virtual predefinido, la conmutación de paquetes puede aumentar o disminuir el ancho de banda según sea necesario, pudiendo manejar adecuadamente las avalanchas de paquetes de forma adecuada. Los servicios de conmutación de paquetes son capaces de enrutar los paquetes, evitando las líneas caídas o congestionadas, debido a los múltiples caminos en la red.

4.2.3. Capa de Enlace de Datos: Protocolos WAN

Las tramas más comunes en la capa de enlace de datos, asociadas con las líneas seriales sincrónicas se enumeran a continuación:

- Synchronous Data Link Control (SDLC). Es un protocolo orientado a dígitos desarrollado por IBM. SDLC define un ambiente WAN multipunto que permite que varias estaciones se conecten a un recurso dedicado. SDLC define una estación primaria y una o más estaciones secundarias. La comunicación siempre es entre la estación primaria y una de sus estaciones secundarias. Las estaciones secundarias no pueden comunicarse entre sí directamente.
- High-Level Data Link Control (HDLC). Es un estándar ISO. HDLC no pudo ser compatible entre diversos vendedores por la forma en que cada vendedor ha elegido cómo implementarla. HDLC soporta tanto configuraciones punto a punto como multipunto.
- Link Access Procedure Balanced (LAPB). Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de marcos así como también para intercambio, retransmitición, y reconocimiento de marcos.
- Frame Relay. Utiliza los recursos digitales de alta calidad donde sea innecesario verificar los errores LAPB. Al utilizar un marco simplificado sin mecanismos de corrección de errores, Frame Relay puede enviar la información de la capa 2 muy rápidamente, comparado con otros protocolos WAN.
- Point-to-Point Protocol (PPP). Descrito por el RFC 1661, dos estándares desarrollados por el IETF. El PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.
- X.25. Define la conexión entre una terminal y una red de conmutación de paquetes.

- Integrated Services Digital Network (ISDN). Un conjunto de servicios digitales que transmite voz y datos sobre las líneas de teléfono existentes.
- Asynchronous Transfer Mode (ATM) Modo de Transferencia Asíncrona es capaz de transferir voz, video y datos a través de redes privadas y públicas. Tiene una arquitectura basada en celdas más bien que una basada en tramas

4.3. CUESTIONARIO DE PREGUNTAS CON MOODLE

Para instalar moodle tenemos que tener instalado un servidor web, y en este caso instalamos WAMP SERVER 2.0

Wamp es una forma de mini-servidor que puede ejecutarse en casi cualquier sistema operativo Windows. Wamp incluye Apache 2, PHP 5 (SMTP puertos son discapacitados) y MySQL (phpMyAdmin y SQLitemanager se instalan para gestionar sus bases de datos) preinstalados.

4.3.1. Ejecutamos el instalador de Wamp Server 2. La instalación se basa en un asistente normal que nos solicitará varios datos típicos de instalaciones, como que aceptemos los términos de la licencia. Luego nos saldrá la ventana para acabar que marcaremos que ejecute Wamp Server inmediatamente.

Figura 4.3.1 WampServer2 Setup Wizard

4.3.2. Si todo ha funcionado, en 1 minuto más podremos comprobar si PHP 5 está funcionando en nuestro ordenador. Sólo tendríamos que encender los servicios. Para ello WampServer2 tiene un panel de control que se accede desde un icono de programa residente de la barra de tareas. Tiene una forma rara, como un cuentakilómetros. Lo veremos la figura 4.3.2.1

Figura 4.3.2.1 Icono de WampServer2

Ahora, para comprobar que los servicios funcionan sólo nos queda abrir un navegador. Vamos a escribir la siguiente dirección URL en la barra de direcciones:

http://localhost

Entonces nos tiene que salir la página de inicio del servidor Apache con PHP 5, personalizada por Wamp, como se muestra en la figura 4.3.2.2

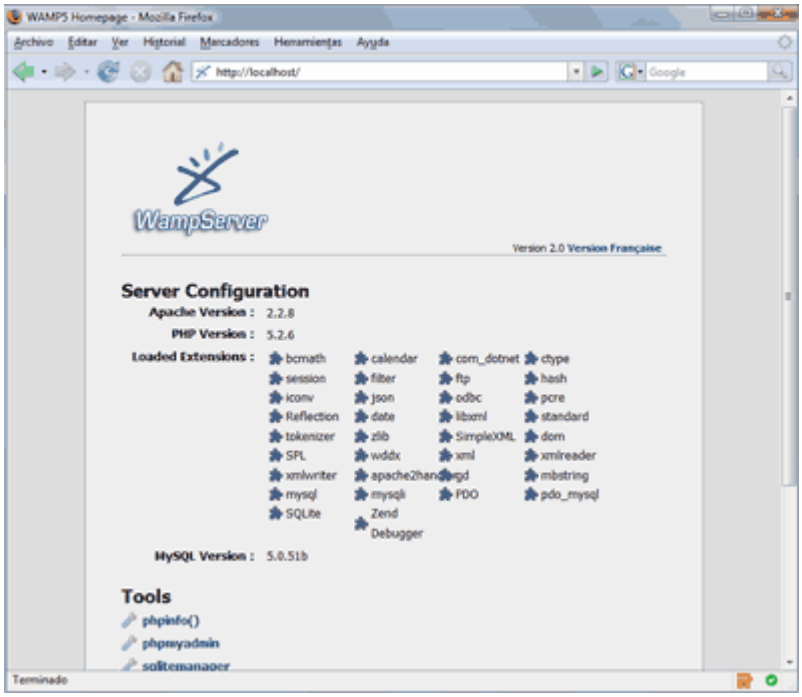

Figura 4.3.2.2

Si no sale nada puede que haya habido un problema o un error al iniciar los servicios, generalmente el Apache, que utiliza el puerto 80 que a veces está ocupado por otro programa como Skype o IIS

Ahora podremos colocar en nuestro servidor todas las páginas PHP que queramos probar o los proyectos que hayamos creado anteriormente. El directorio donde generalmente se localiza la raíz de publicación es:

C:\wamp\www

Y es exactamente en esta carpeta donde deberíamos poner nuestra carpeta moodle para comenzar con la instalación

C:\wamp\www\moodle

4.3.3. Seleccionamos el idioma en que queremos que se realice la instalación

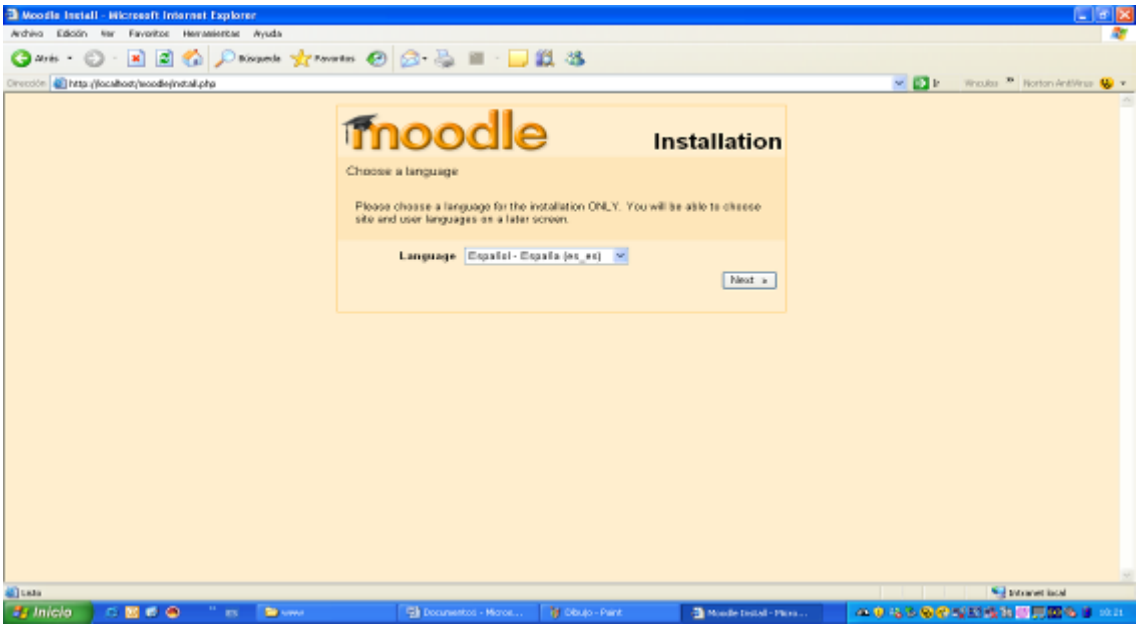

Figura 4.3.3.1

4.3.4. Como el moodle necesita que tengamos instalado PHP, hace una verificación si tenemos instalado correctamente

Figura 4.3.4.1

4.3.5. Ponemos en path en donde se van a guardar los archivos de configuración del el moodle.

Figura 4.3.5.1

4.3.6. Tendremos una pantalla donde nos indica el motor de base de datos que vamos a utilizar donde tendremos que digitar el usuario y proveer una contraseña

Figura 4.3.6.1

4.3.7. El sistema verifica si están al día las comprobaciones del Servidor

Figura 4.3.7.1

4.3.8. Tenemos que habilitar todas las extensiones faltantes del PHP

Figura 4.3.8.1

4.3.9. Luego se concluye la instalación del moodle

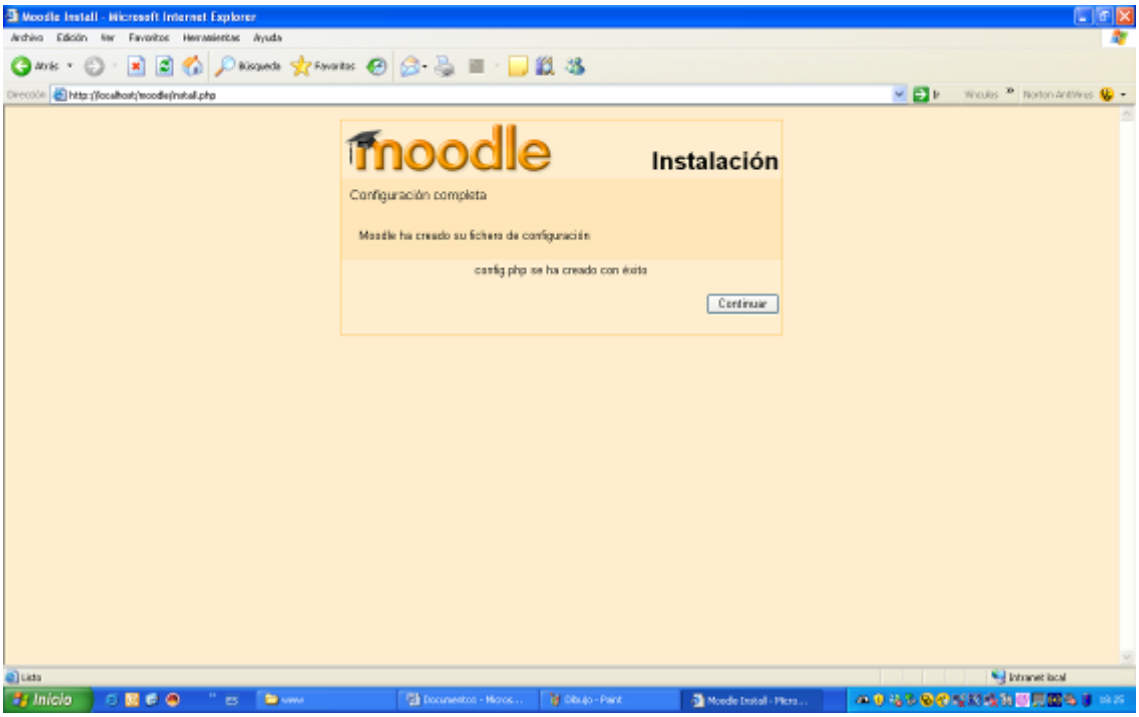

Figura 4.3.9.1

4.3.10. Luego el moodle nos indica que ingresemos un nombre y contraseña para el administrador del sistema, completar los datos personales del administrador.

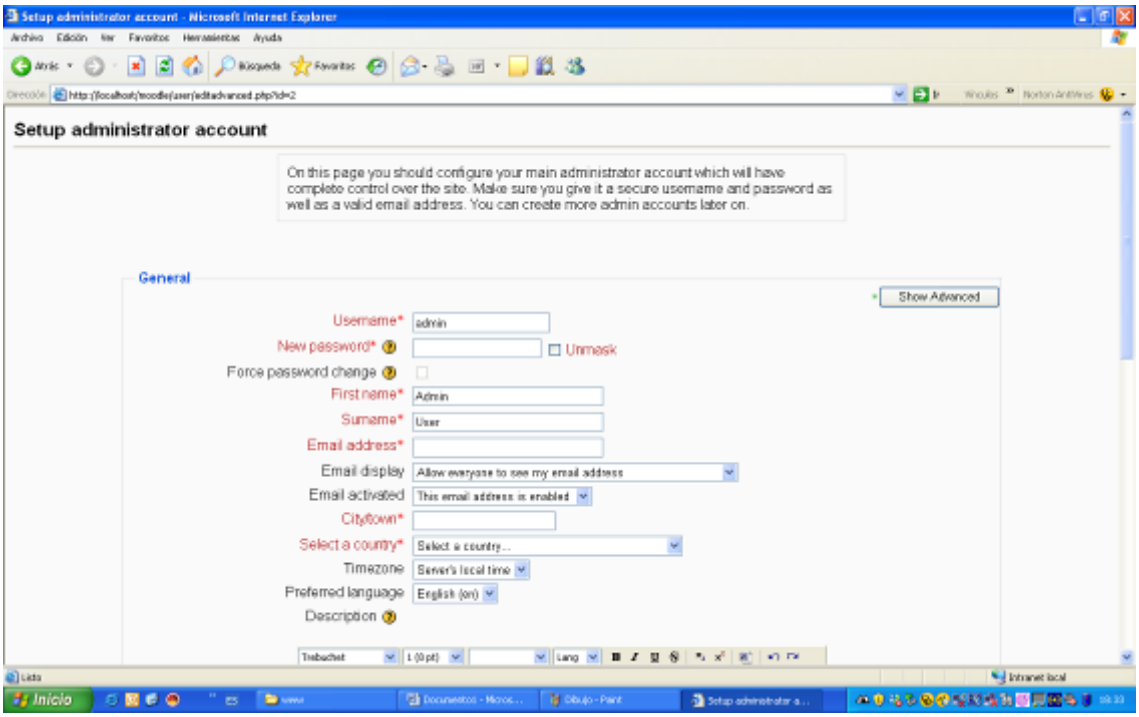

Figura 4.3.10.1

4.3.11. Configuramos la pantalla principal del moodle, al entrar al sistema

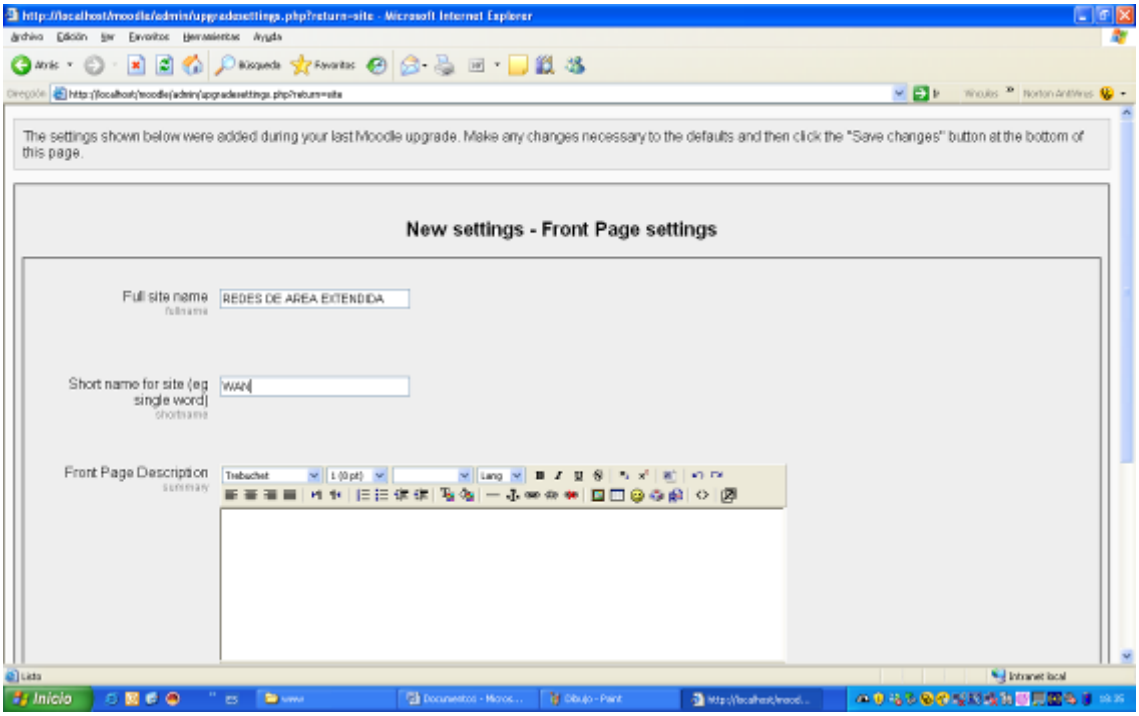

Figura 4.3.11.1

4.3.12. Y por último tendremos una pantalla donde ya podemos hacer la configuración del moodle.

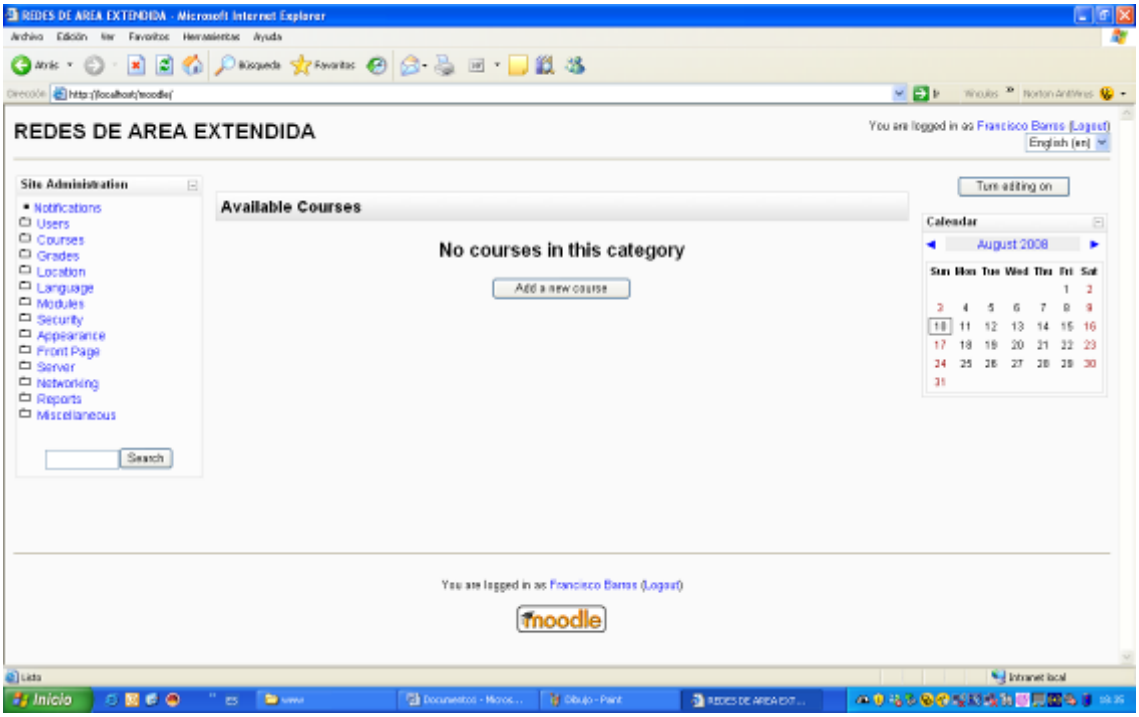

Figura 4.3.12.1

4.4. ¿QUÉ ES MOODLE?

4.4.1. Entornos virtuales de aprendizaje

Técnicamente, **Moodle** es una aplicación que pertenece al grupo de los Gestores de Contenidos Educativos (**LMS**, *Learning Management Systems*), también conocidos como Entornos de Aprendizaje Virtuales (**VLE**, *Virtual Learning Managements*).

De una manera más coloquial, podemos decir que Moodle es una aplicación para crear y gestionar plataformas educativas, es decir, espacios donde un centro educativo, institución o empresa, gestiona recursos educativos proporcionados por unos docentes y organiza el acceso a esos recursos por los estudiantes, y además permite la comunicación entre todos los implicados (alumnado y profesorado).

La palabra Moodle, en inglés, es un acrónimo para Entorno de Aprendizaje Dinámico Modular, Orientado a Objetos (*Modular Object-Oriented Dynamic Learning Environment*)

4.4.2. Software libre

Moodle se distribuye gratuitamente como Software Libre (Open Source), bajo Licencia pública GNU. Esto significa que Moodle tiene derechos de autor (copyright), pero que tenemos algunas libertades: podemos copiar, usar y modificar Moodle siempre que aceptemos proporcionar el código fuente a otros, no modificar la licencia original y los derechos de autor, y aplicar esta misma licencia a cualquier trabajo derivado de él.

Es fácil de instalar en casi cualquier plataforma con un servidor Web que soporte PHP. Sólo requiere que exista una base de datos . Con su completa abstracción de bases de datos, soporta las principales marcas de bases de datos (en especial MySQL). Finalmente, es importante destacar que, al ser Moodle una aplicación Web, el usuario sólo necesita para acceder al sistema un ordenador con un navegador Web instalado (Mozilla Firefox, Internet Explorer, o cualquier otro) y una conexión a Internet. Por supuesto, también se necesita conocer la dirección Web (URL) del servidor donde Moodle se encuentre alojado y disponer de una cuenta de usuario registrado en el sistema.

4.4.3. Características Principales

- Entorno de aprendizaje modular y dinámico orientado a objetos, sencillo de mantener y actualizar.
- Excepto el proceso de instalación, no necesita prácticamente de "mantenimiento" por parte del administrador.
- Dispone de una interfaz que permite crear y gestionar cursos fácil-mente.
- Los recursos creados en los cursos se pueden reutilizar.

- La inscripción y autenticación de los estudiantes es sencilla y segura.
- Resulta muy fácil trabajar con él, tanto para el profesorado como el alumnado.
- Detrás de él hay una gran comunidad que lo mejora, documenta y apoya en la resolución de problemas.
- Está basado en los principios pedagógicos constructivistas: el aprendizaje es especialmente efectivo cuando se realiza compartiéndolo con otros

4.4.4. Acceso al sistema o aula virtual

Moodle es una aplicación Web a la que se accede por medio de cualquier navegador Web (Mozilla Firefox, Internet Explorer, Opera, etc.). Esto quiere decir que, además de disponer de conexión a Internet, tendremos que conocer la dirección Web (URL) del servidor donde se encuentre alojado Moodle.

Para poder acceder al sistema deberemos estar registrados como usuario del mismo. Los datos de la cuenta de usuario se introducen en el bloque Entrar (la posición de este bloque puede variar dependiendo de cómo se haya configurado esta página). Si no está accesible directamente, hay que hacer clic en el enlace Entrar que se encuentra habitualmente en la parte superior derecha, tal como se indica en la figura 4.4.4.1

Figura 4.4.4.1

4.5. SOFTWARE GENERADOR DE PRUEBAS

4.5.1. INTRODUCCIÓN

4.5.1.1. Interfaz Web

La Real Academia Española define el término interfaz (de la palabra inglés interface, superficie de contacto) como una conexión física y funcional entre dos aparatos o sistemas independientes. Generalizando esta definición, dados dos sistemas cualesquiera que se deben comunicar entre ellos la interfaz será el mecanismo, entorno o herramienta que hace posible dicha comunicación.

Esta definición es amplia en sí misma, utilizándose para describir multitud de entornos de comunicación entre sistemas físicos, eléctricos, electrónicos y lógicos, utilizándose por ejemplo para referirse a los procedimientos físicos y lógicos que permiten relacionarse a dos capas diferentes de la arquitectura de comunicaciones en red TCP/IP, a cualquier dispositivo que permite establecer una comunicación entre dos arquitecturas de diferente naturaleza o a

determinados componentes de software que habilitan el entendimiento correcto entre dos aplicaciones u objetos lógicos.

Cuando uno de los sistemas que se comunican es un ser humano pasamos al concepto de interfaz de usuario. Por un lado tenemos un sistema físico o informático y por otro a una persona que desea interaccionar con él, darle instrucciones concretas, siendo la interfaz de usuario la herramienta que entiende a ambos y es capaz de traducir los mensajes que se intercambian.

Las páginas web supusieron la aparición de las interfaces web, interfaces gráficas de usuario con unos elementos comunes de presentación y navegación que pronto se convirtieron en estándares de facto. Este tipo de interfaces deben servir de intermediarias entre unos usuarios genéricos, no acostumbrados generalmente al uso de aplicaciones informáticas, y unos sistemas de información y procesos transaccionales que corren por debajo, debiendo posibilitar la localización de la información deseada, el entendimiento claro de las funcionalidades ofrecidas, la realización práctica de tareas específicas por parte de los usuarios y la navegación intuitiva por las diferentes páginas que forman el sitio web.

4.5.1.2. Creación de preguntas

4.5.1.2.1. Para la creación del banco de preguntas se debe ingresar en la interfaz web de nuestro programa como se muestra en la figura en el cual se debe ingresar el nombre de usuario y su respectiva contraseña, en este caso procedemos a ingresar el de administrador para poder crear las preguntas caso contrario solo puede entrar como alumno y rendir las respectivas pruebas correspondientes a cada capítulo.

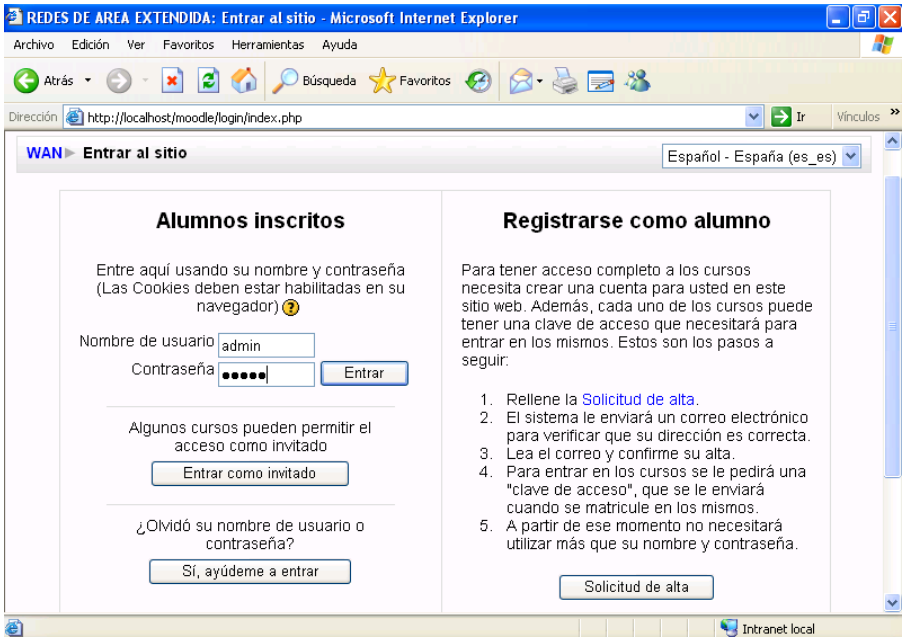

Figura 4.5.1.2.1 Interfaz Web

4.5.1.2.2. Para la creación de preguntas primero debemos agregar un curso como se muestra en la figura 4.5.1.2.2.1

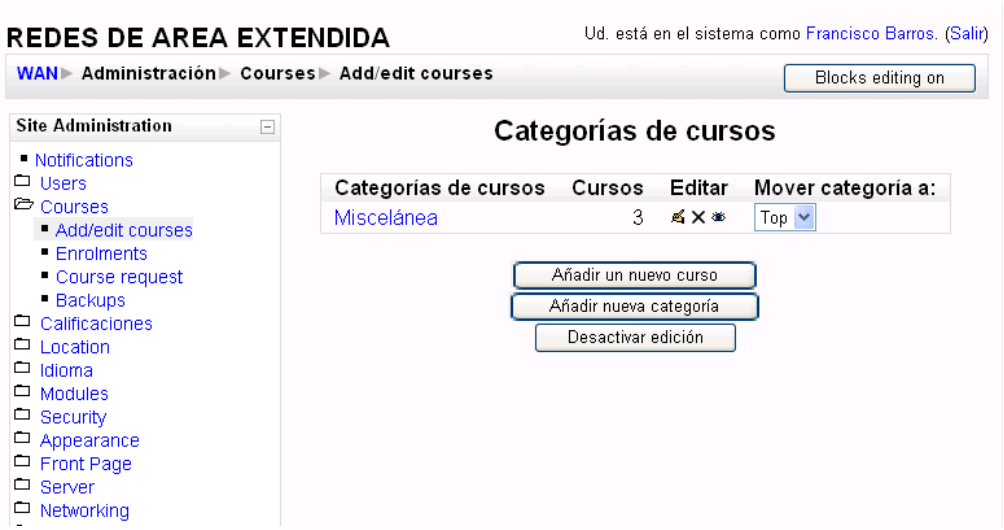

Figura 4.5.1.2.2.1 Creación del curso

4.5.1.2.3. En la siguiente pantalla se selecciona Añadir nuevo curso y se procede a llenar los datos correspondientes a la configuración de dicho curso

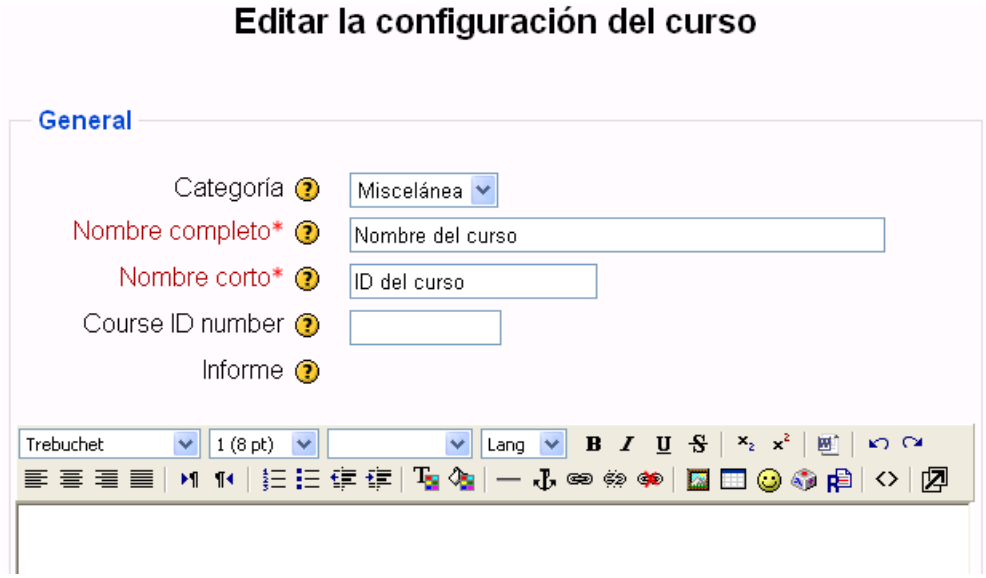

Figura 4.5.1.2.3.1 Edición de la configuración del curso

4.5.1.2.4. En nuestro caso añadimos el siguiente curso como se muestra en la figura 4.5.1.2.4.1

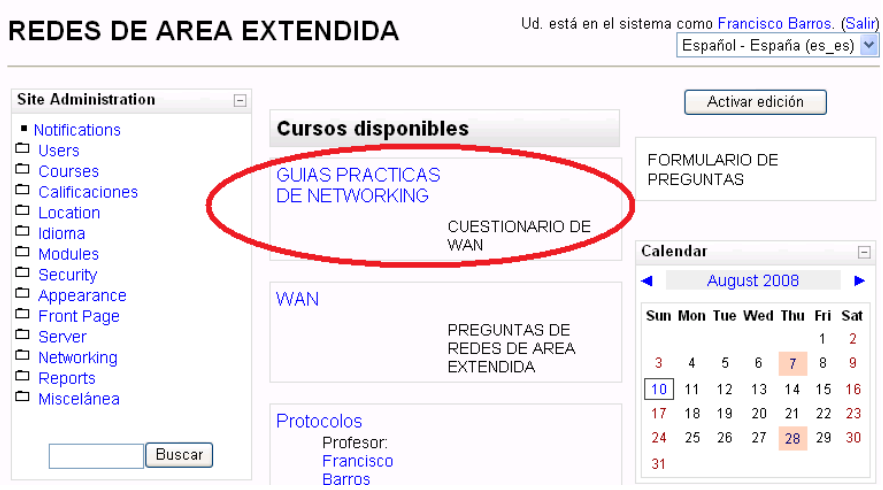

Figura 4.5.1.2.4.1 Adición de curso

4.5.1.2.5. Para ingresar las preguntas entramos al curso creado y nos dirigimos a la pestaña de preguntas como se indica en la figura 4.5.1.2.5.1

Figura 4.5.1.2.5.1 Adición de preguntas

4.5.1.2.6. En el cuadro que se nos despliega seleccionamos la modalidad de las preguntas que en nuestro caso escogemos Preguntas de Opción Múltiple, como se muestra en la figura 4.5.1.2.6.1

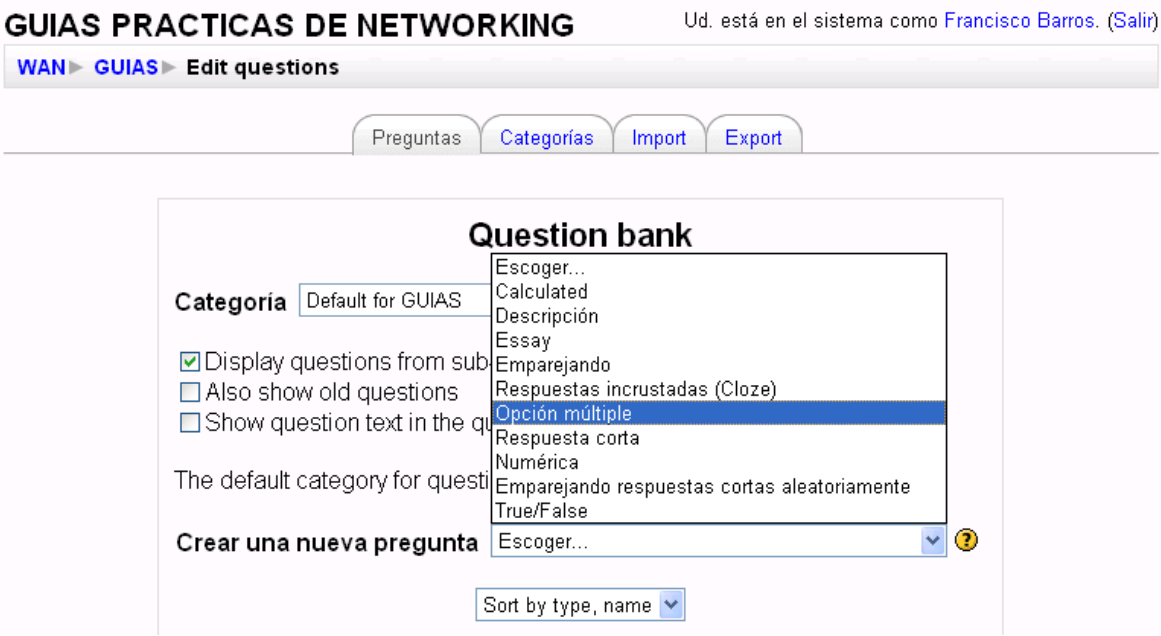

Figura 4.5.1.2.6.1 Adición de preguntas

4.5.1.2.7. Al finalizar todos los datos necesarios para las preguntas se nos despliega un cuadro como se muestra en la figura 4.5.1.2.7.1,

para continuar agregando preguntas se vuelve a realizar los mismos pasos

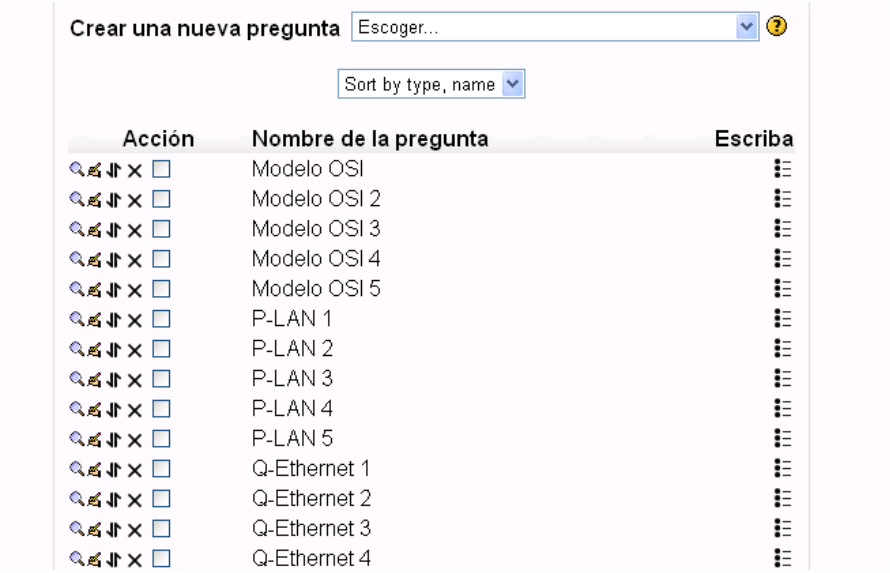

Figura 4.5.1.2.7.1 Pregunta Disponibles

4.5.1.2.8. Una vez realizada las preguntas necesarias procedemos agregar las preguntas al Curso, Volvemos a la pantalla principal, ingresamos al curso que creamos y Activamos la Edición para poder agregar nuestras preguntas

Figura 4.5.1.2.8.1

4.5.1.2.9. Se nos despliega una pantalla en el cual seleccionamos Agregar cuestionario como se muestra en la figura 4.5.1.2.9.1

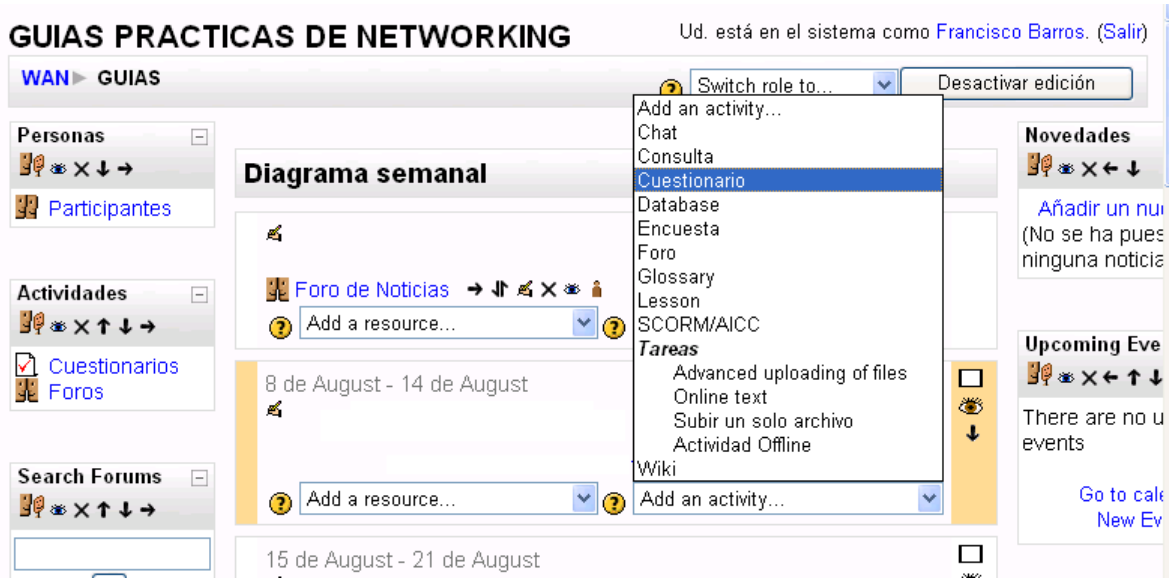

Figura 4.5.1.2.9.1

4.5.1.2.10. Una vez seleccionada las preguntas que deseamos a nuestro Quiz nos aparecerá el curso ya con nuestras preguntas listas para ser vistas por nuestros usuarios

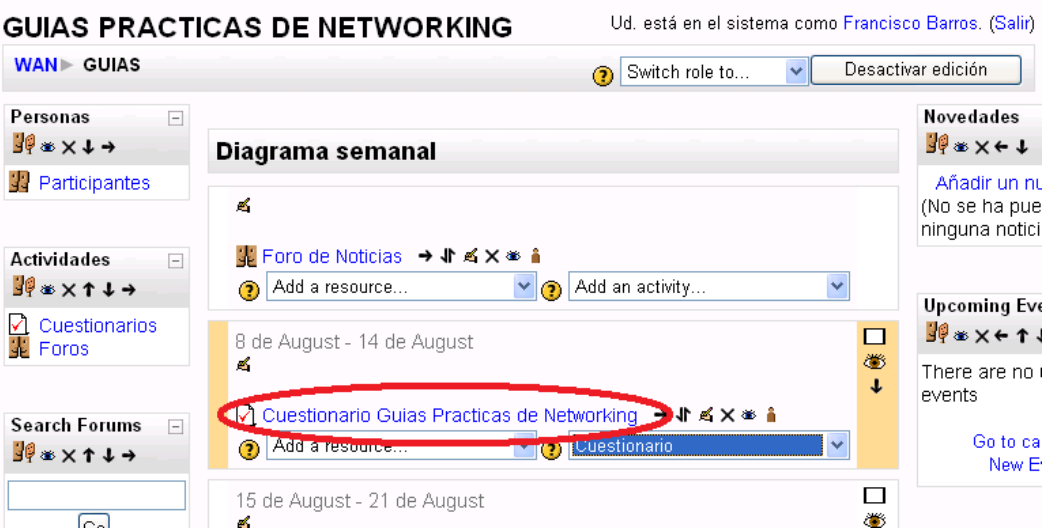

Figura 4.5.1.2.10.1

4.5.1.3. Creación de usuarios

4.5.1.3.1. Para la creación de usuarios se debe ingresar en la pantalla principal y proceder a adicionar usuario como se indica en la figura 4.5.1.3.1.1 y luego se procede a llenar los datos necesarios

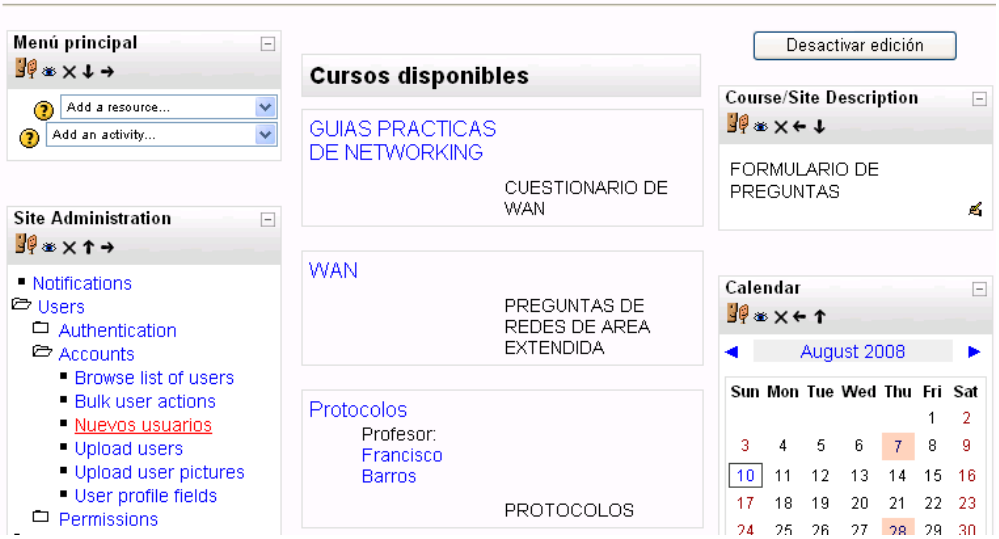

Figura 4.5.1.3.1.1 Creación de usuario

4.5.1.3.2. En la figura 4.5.1.3.2.1 se presenta la siguiente pantalla en la cual usted debe llenar los datos necesarios para poder registrar al usuario

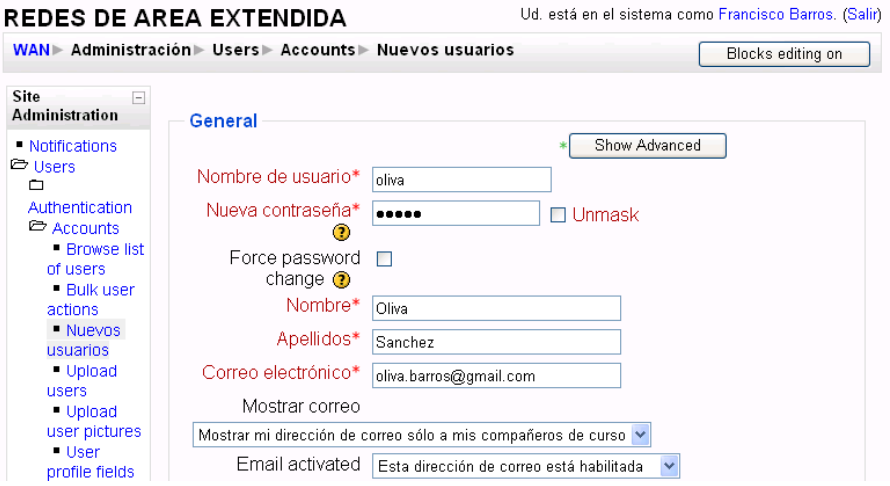

Figura 4.5.1.3.2.1 Registro Usuario

4.5.1.4. PRUEBA DE SELECCIÓN MÚLTIPLE

4.5.1.4.1. En la pantalla de inicio debe ingresar el nombre de usuario y contraseña de algún usuario creado como se muestra en la figura 4.5.1.4.1.1

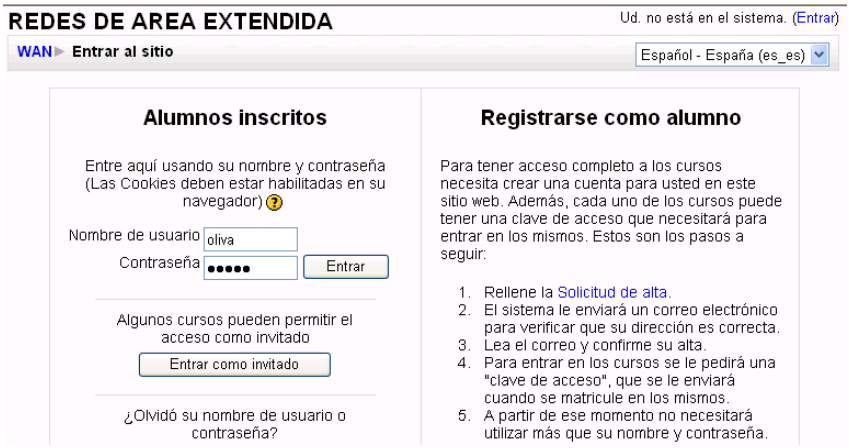

Figura 4.5.1.4.1.1 Inicio Prueba

4.5.1.4.2. Ingresamos en la plantilla de preguntas y se debe elegir el curso a que se desea realizar la prueba como se muestra en la figura 4.5.1.4.2.1

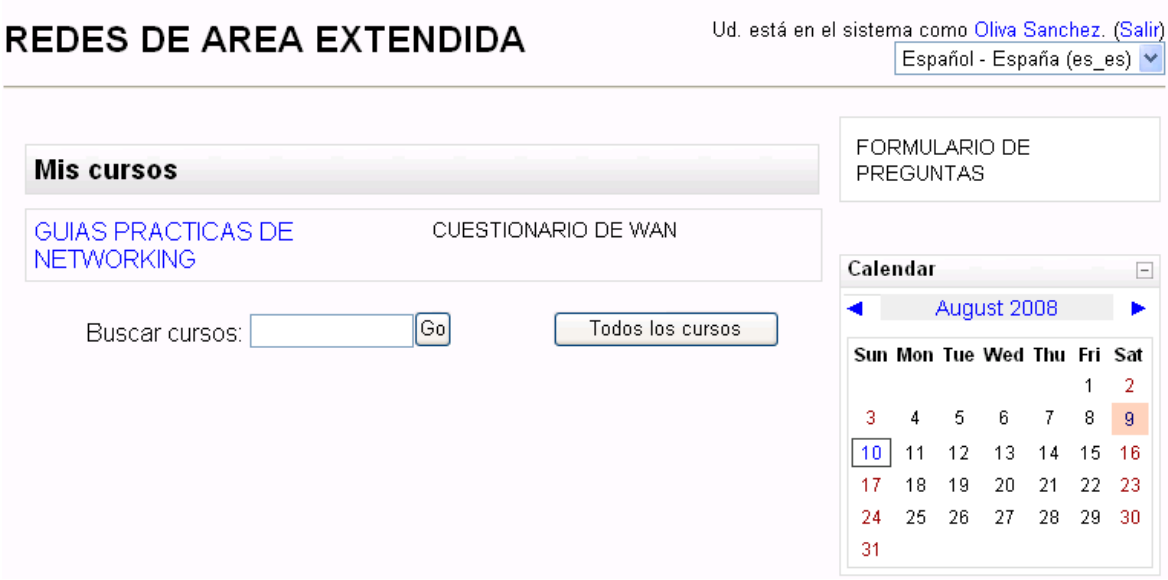

Figura 4.5.1.4.2.1 Selección de Curso

4.5.1.4.3. En esta pantalla seleccionamos el Cuestionario dependiendo de la fecha de creación

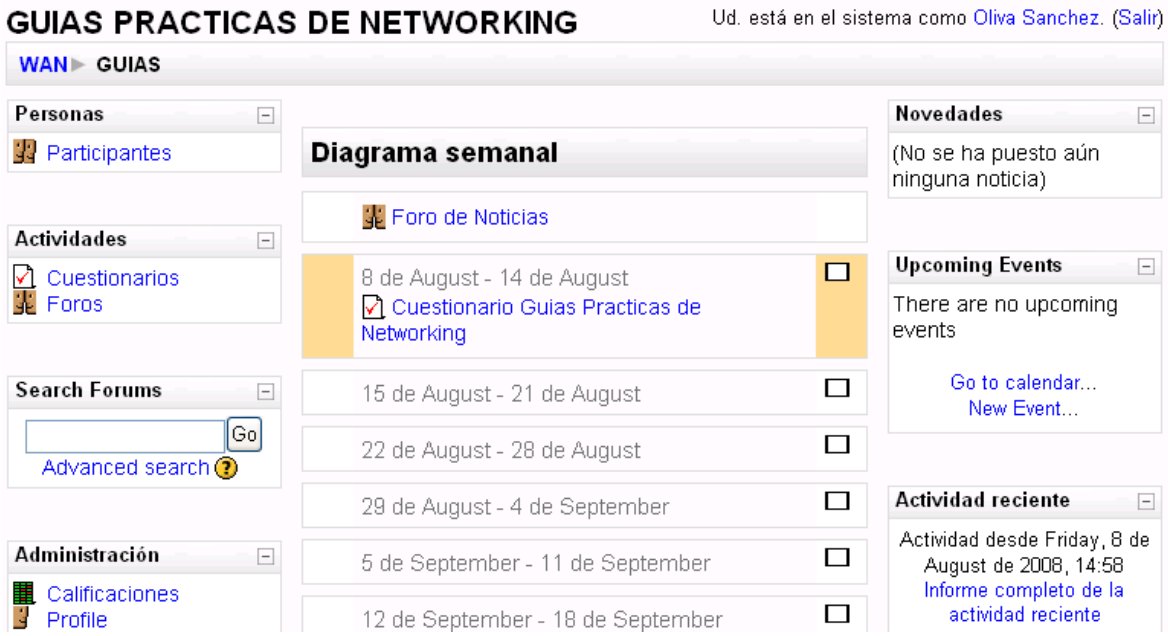

Figura 4.5.1.4.3.1 Selección de Curso

4.5.1.4.4. Una vez seleccionado el Cuestionario tendremos un WARNING que dice que vamos a realizar ya el test

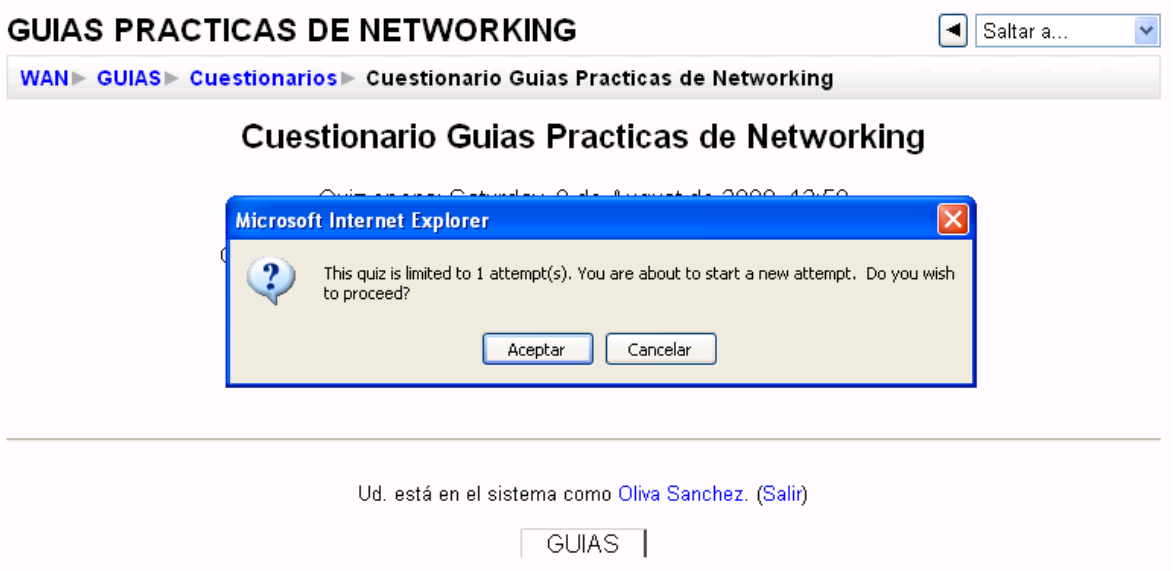

Figura 4.5.1.4.4.1 Confirmación del Examen

4.5.1.4.5. En la siguiente pantalla aparece la prueba a realizarse del capítulo seleccionado como se muestra en la figura 4.5.1.4.5.1. Se procede a desarrollar la prueba

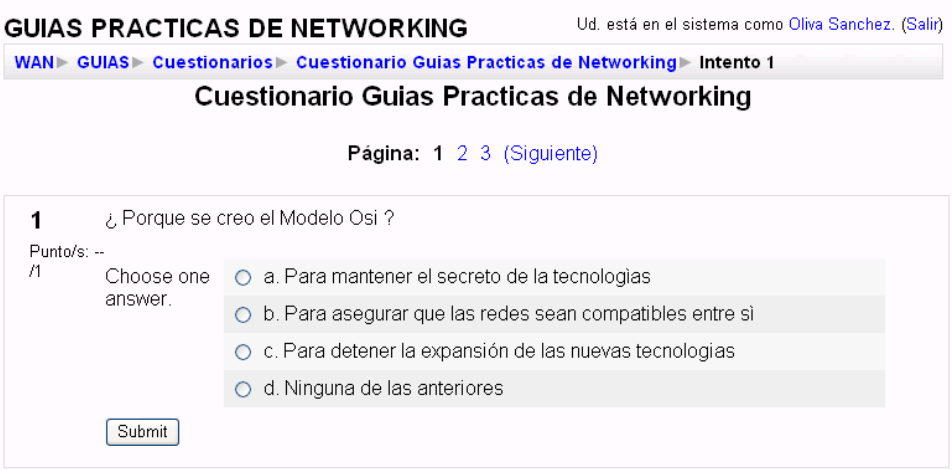

Figura 4.5.1.4.5.1 Prueba a realizar

4.5.1.4.6. Al terminar de contestar todas las preguntas procede a la calificación automática haciendo clic sobre submit Answer y

automáticamente el programa le muestra cuales de sus preguntas fueron correctas e incorrectas con su respectivo total de buenas y en porcentaje como se muestra en la figura

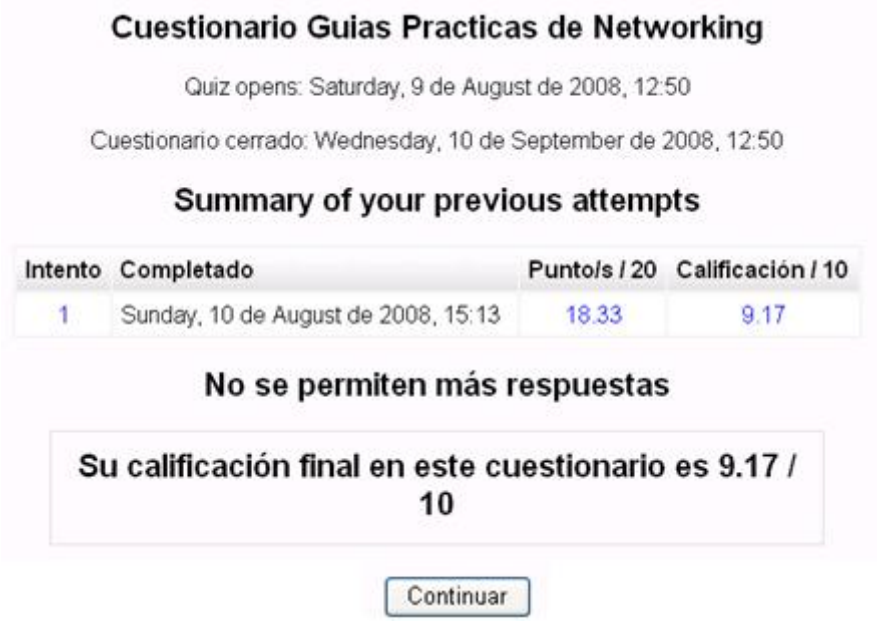

Figura 4.5.1.4.6.1 Calificación Prueba

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

3. Guía de práctica: Realizar una red Frame Relay utilizando enrutamiento estático

3.1. Objetivo

- Realizar una red Frame Relay entableciendo las PVC para cada una de las redes interconectadas
- Establecer enrutamiento estático en cada uno de los ruteadores

3.2. Procedimiento

3.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[2]

3.2.2. Realizamos la topología de red como se muestra en la figura en cual estamos utilizando una nube frame relay

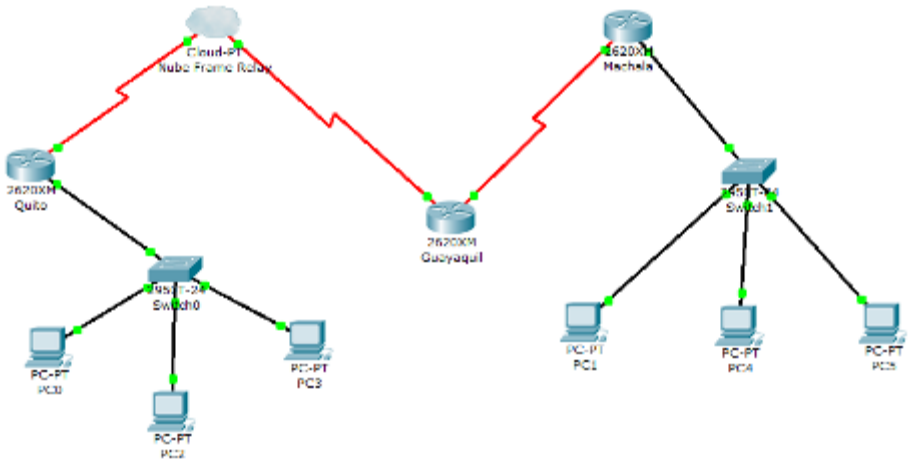

Figura 3.2.2.1

[2] Guía de práctica: Realizar una red LAN en la que se observa las diferentes capas del modelo OSI

3.2.3. Debemos configurar la dirección IP y su respectiva mascara de red para todas las CPU´s conectadas en la red, para ello procedemos a dar un clic en cada una de las CPU´s de la red, para lo cual se abre una pantalla de configuración como se puede observar en la figura

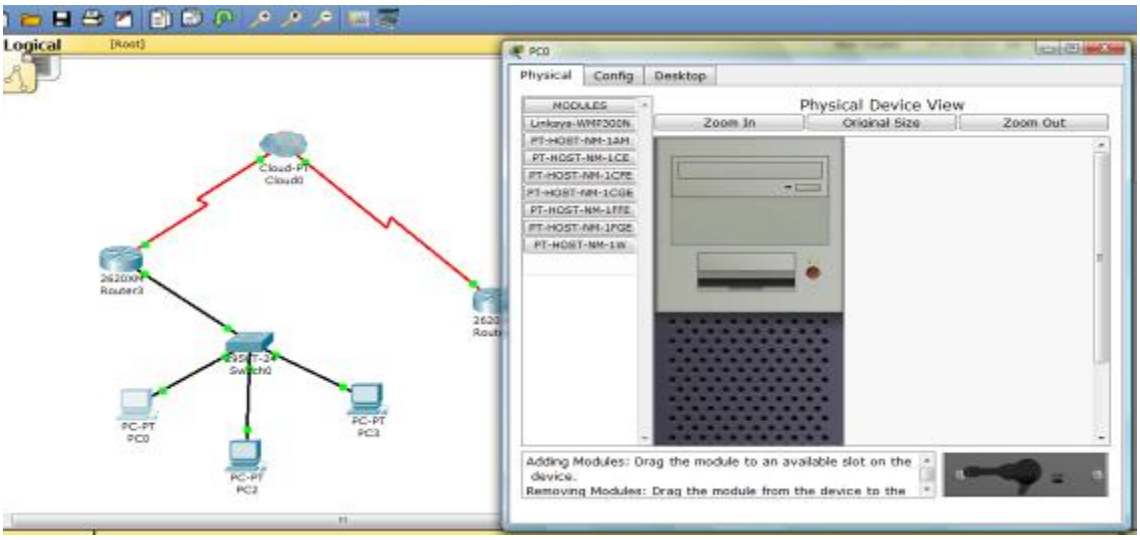

Figura 3.2.3.1 Edit CPU's

3.2.4. En la pantalla que aparece nos debemos dirigir a la pestaña con el nombre de desktop, y luego en IP configuration en la cual procedemos con la configuración de nuestra dirección IP con el respectivo Gateway para poder acceder a otras redes y nuestra mascara de red como se observa en la figura

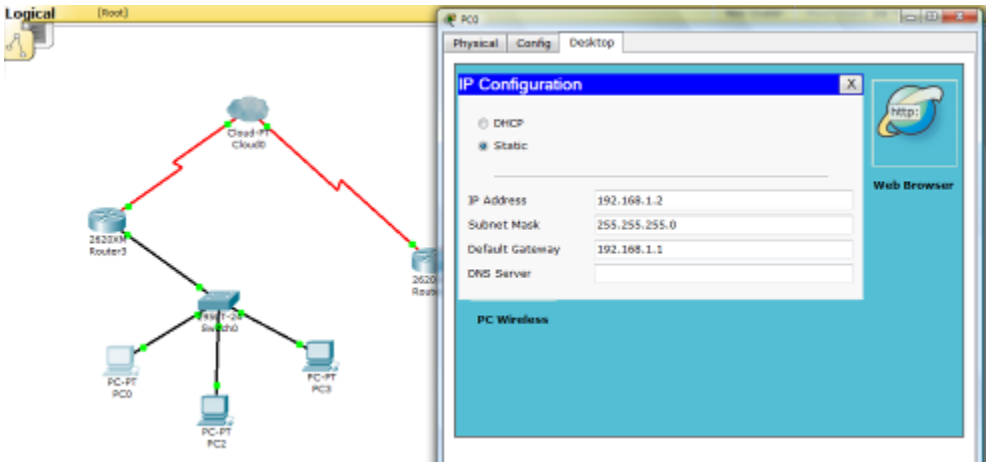

Figura 3.2.4.1 CPU's

3.2.5. Lo mismo la ips para la otro sector de la red.

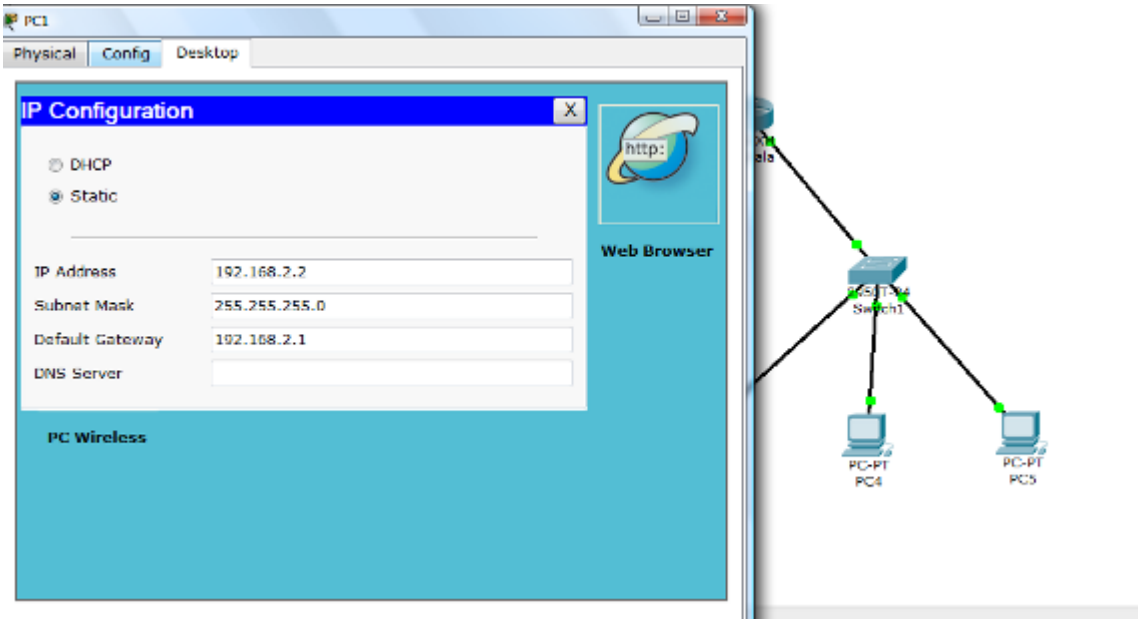

Figura 3.2.5.1

3.2.6. Para realizar la configuración de los ruteadores Quito, Guayaquil, Machala, es importante indicar que debemos insertar la tarjeta WIC 1T como se muestra en la figura para este procedimiento el ruteador se debe encontrar apagado y encenderlo posteriormente

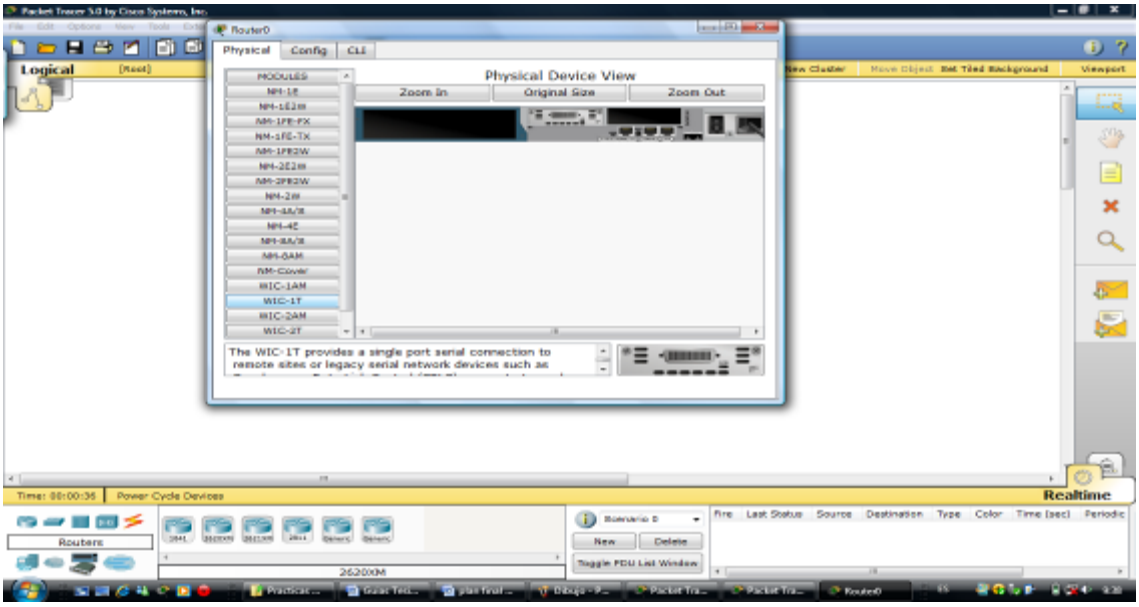

Figura 3.2.6.1 Interfaz Serial

3.2.7. Procedemos con la configuración del Ruteador Quito con el cual utilizaremos el modelo 2620XM.

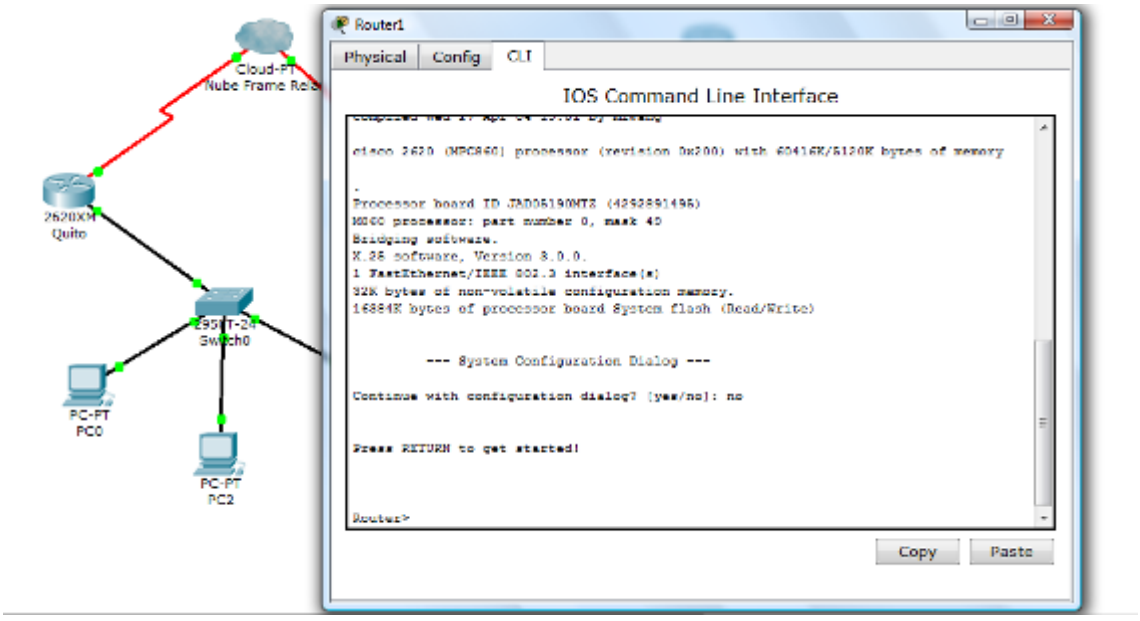

Figura 3.2.7.1

3.2.7.1. Ponemos nombre al ruteador

Router>enable

Router#conf t

Router(config)#hostname Quito

3.2.7.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Quito(config)#int f0/0
Quito(config-if)#ip address 192.168.1.1 255.255.255.0
Quito(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Quito(config-if)#exit

3.2.7.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

Quito(config)#int s0/0
Quito(config-if)#ip address 172.16.4.1 255.255.0.0
Quito(config-if)#encapsulation frame-relay ietf
Quito(config-if)#frame-relay lmi-type ansi
Quito(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Quito(config-if)# exit

3.2.7.4. Configuramos las rutas estáticas en el equipo local

Quito(config)# ip route 10.0.0.0 255.0.0.0 172.16.4.2
Quito(config)# ip route 192.168.2.0 255.255.255.0 172.16.4.2

Quito#wr
Building configuration...
[OK]
Quito#

NOTA: Los ruteadores que se conectan a la Nube Frame Relay se la debe configurar como Interfaces DTE

3.2.7.5. Como último paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

```
Quito#sh running-config
Building configuration...

Current configuration : 451 bytes
!
version 12.2
no service password-encryption
!
hostname Quito
!
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0


duplex auto
 speed auto
!
```

```
interface Serial0/0
 ip address 172.16.4.1 255.255.0.0
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
!
ip classless
ip route 10.0.0.0 255.0.0.0 172.16.4.2
ip route 192.168.2.0 255.255.255.0 172.16.4.2
!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end


Quito#
```

3.2.8. Procedemos con la configuración del Ruteador Guayaquil con el cual utilizaremos el modelo 2620XM, con interfaces seriales

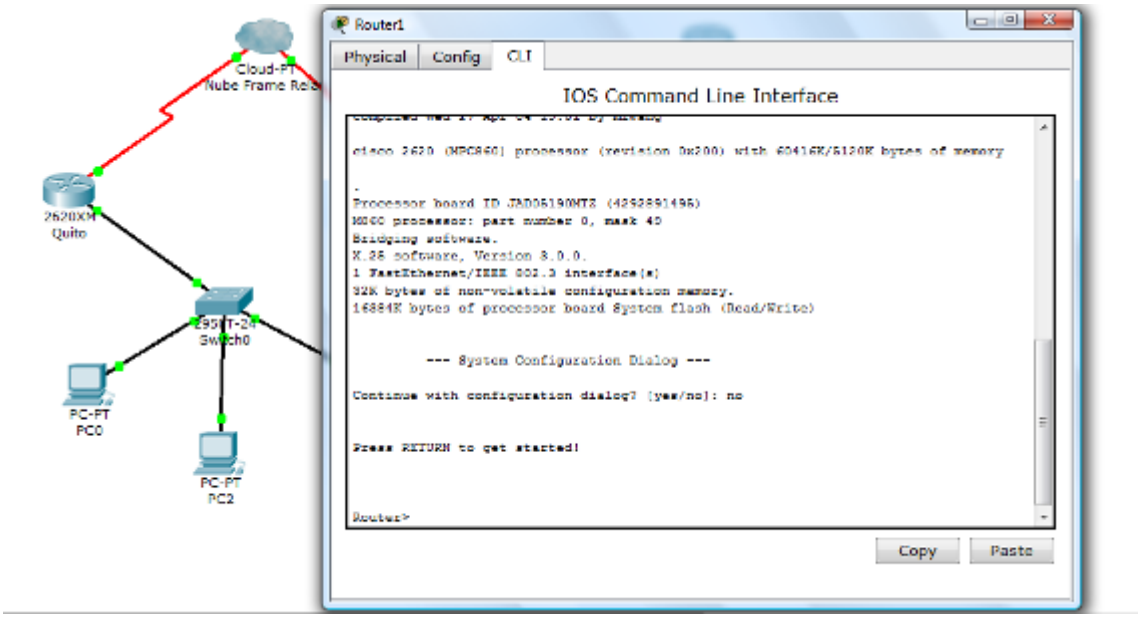

Figura 3.2.8.1

3.2.8.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Guayaquil

3.2.8.2. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

Guayaquil(config)#int s0/0
Guayaquil(config-if)#ip address 172.16.4.2 255.255.0.0
Guayaquil(config-if)#encapsulation frame-relay ietf
Guayaquil(config-if)#frame-relay lmi-type ansi
Guayaquil(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Guayaquil (config-if)# exit

Guayaquil(config)#int s0/1
Guayaquil(config-if)#ip address 10.0.0.1 255.0.0.0

Guayaquil(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Guayaquil (config-if)# exit

3.2.8.3. Configuramos las rutas estáticas en el equipo local

Guayaquil(config)# ip route 192.168.1.0 255.255.255.0 172.16.4.1
Guayaquil(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
Guayaquil#wr
Building configuration...
[OK]
Guayaquil #

NOTA: Los ruteadores que se conectan a la Nube Frame Relay se la debe configurar como Interfaces DTE

3.2.8.4. Como último paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

Guayaquil#sh running-config
Building configuration...

Current configuration : 500 bytes
!
version 12.2
no service password-encryption
!
hostname Guayaquil
!
!

```
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 172.16.4.2 255.255.0.0
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
!
interface Serial0/1
 ip address 10.0.0.1 255.0.0.0
!
ip classless
ip route 192.168.1.0 255.255.255.0 172.16.4.1
ip route 192.168.2.0 255.255.255.0 10.0.0.2
!
!
!
!
!
line con 0
line vty 0 4
 login
!
```

!

end

Guayaquil#

3.2.9. Procedemos con la configuración del Ruteador Machala con el cual utilizaremos el modelo 2620XM.

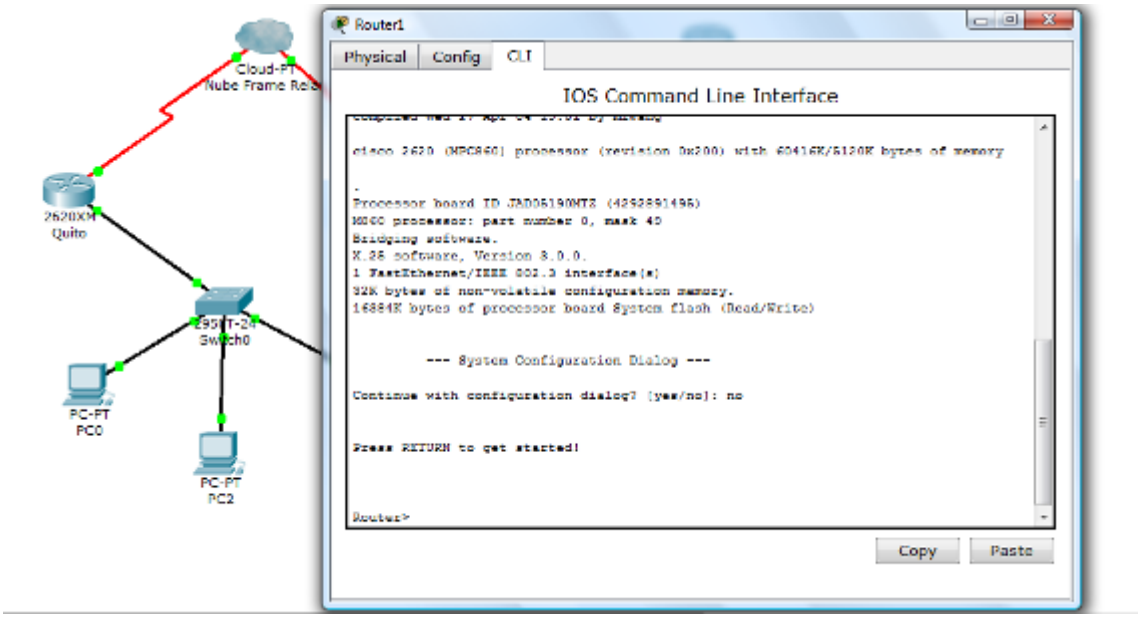

Figura 3.2.9.1

3.2.9.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Machala

3.2.9.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Machala(config)#int f0/0
Machala(config-if)#ip address 192.168.2.1 255.255.255.0

```
Machala(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Machala(config-if)#exit
```

3.2.9.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

```
Machala(config)#int s0/0
Machala(config-if)#ip address 10.0.0.2 255.0.0.0
Machala(config-if)#clock rate 56000
Machala(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Machala(config-if)# exit
```

Configuramos las rutas estáticas en el equipo local

```
Machala(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
Machala(config)# ip route 172.16.0.0 255.255.0.0 10.0.0.1
Machala#wr
Building configuration...
[OK]
Machala#
```

3.2.9.4. Como último paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

```
Machala#sh running-config
Building configuration...

Current configuration : 408 bytes
```

```
!
version 12.2
no service password-encryption
!
hostname Machala
!
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.0.0.2 255.0.0.0
 clock rate 56000
!
ip classless
ip route 192.168.1.0 255.255.255.0 10.0.0.1
ip route 172.16.0.0 255.255.0.0 10.0.0.1
!
!
!
line con 0
line vty 0 4
 login
!
```

!

end

Machala#

3.2.10. Procedemos con la configuración de la Nube Frame Relay

3.2.10.1. Lo que primero debemos realizar en la Nube es limitar los DLCI en los seriales dependiendo del router conectado y el nombre que vamos a utilizar con fines administrativos. En este caso nos dirigimos a la Serial0 donde está conectado directamente con el Router de Quito.

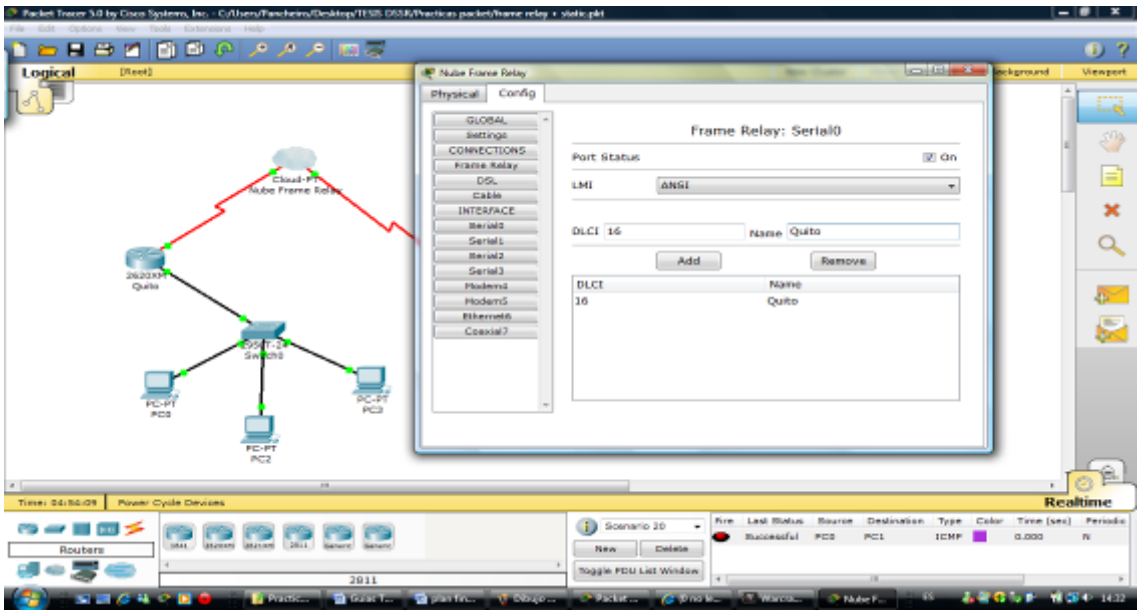

Figura 3.2.10.1.1

3.2.10.2. Posteriormente lo mismo para la Serial1 donde se encuentra conectado directamente con el Router de Guayaquil.

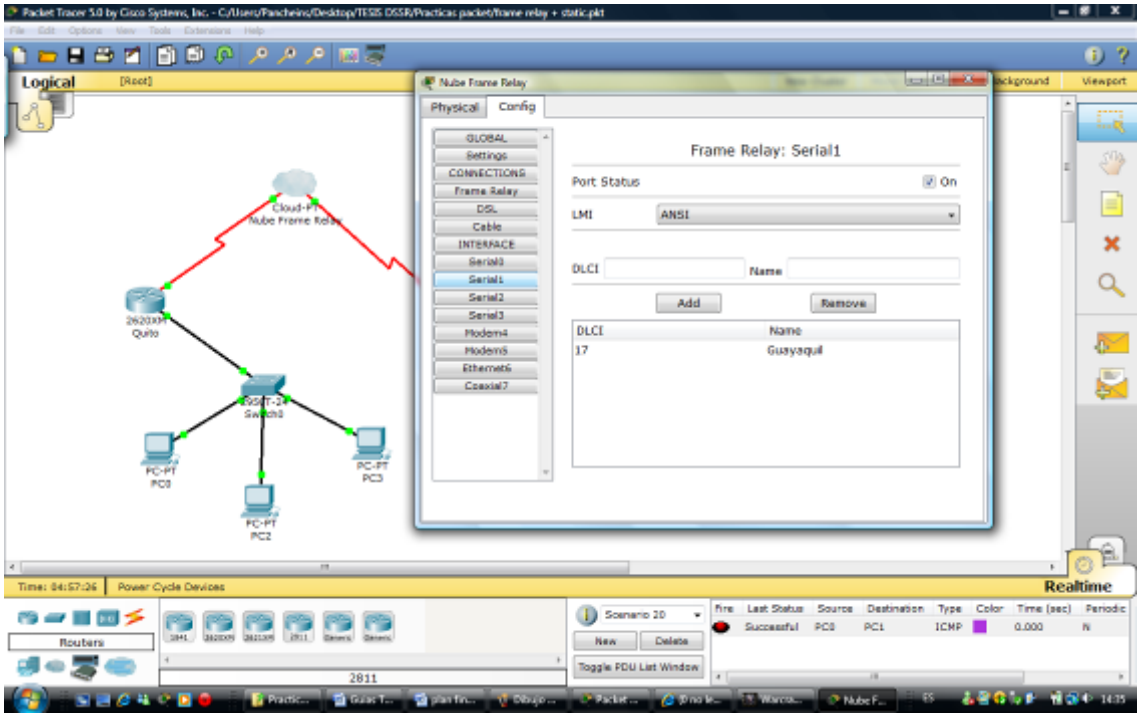

Figura 3.2.10.2.1

3.2.10.3. Y como último paso en la Nube Frame Relay direccionamos la PVC o el túnel virtual entre el Router de Quito y el Router de Guayaquil tal cual se muestra la figura.

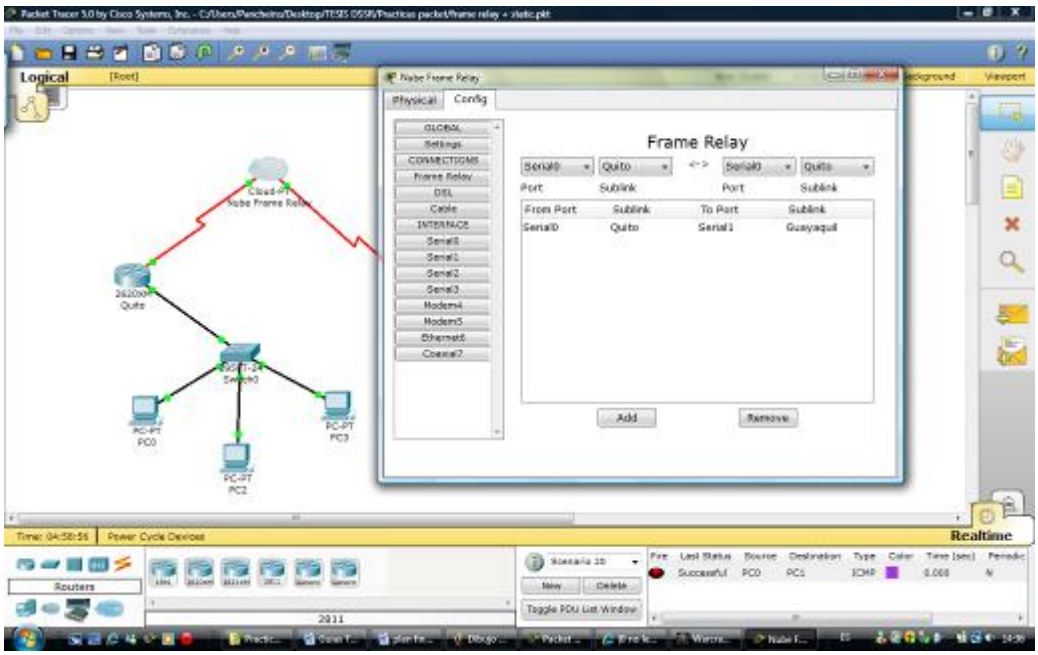

Figura 3.2.10.3.1

3.3. Análisis de resultados

3.3.1. Hacemos ping a una estación de trabajo vía command prompt

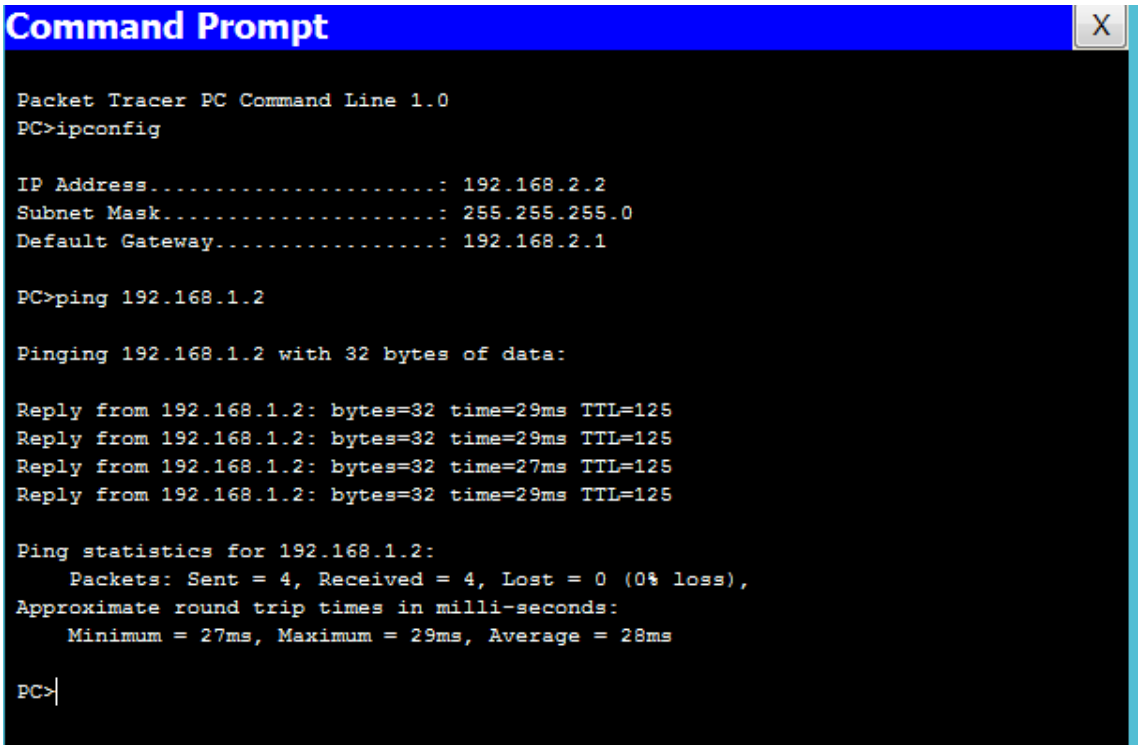

Figura 3.3.1.1

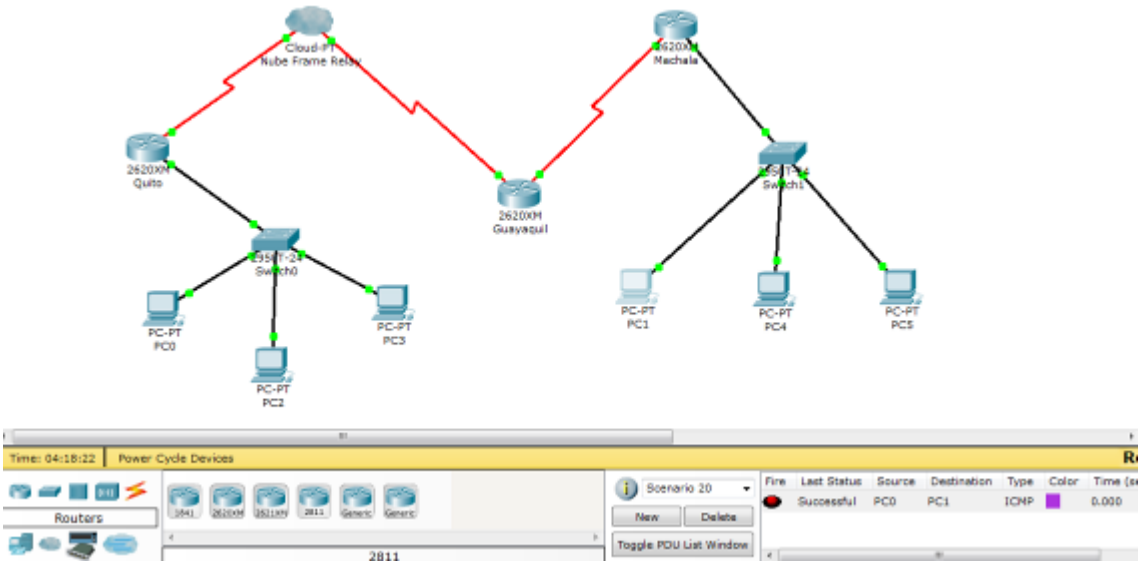

Figura 3.3.1.2

3.4. Análisis de resultados

- Se puede observar en la simulación que podemos hacer ping desde la PC0 hasta la PC1
- Al realizar la simulación de la red se debe tener muy en cuenta que todos routers estén configurados debidamente el enrutamiento caso contrario no se podrían enviar ninguna información.

3.5. Conclusiones

- Las graficas de la simulación permitieron observar que los paquetes se trasladaron sin ningún problema por la red
- Con la simulación realizada se cumplieron los objetivos requeridos
- Se puede observar muy claramente que la red se encuentra funcionando correctamente con todos sus elementos

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

4. Guía de práctica: Realizar una red Frame Relay utilizando enrutamiento dinámico RIP

4.1. Objetivo

- Realizar una red Frame Relay entableciendo las PVC para cada una de las redes interconectadas
- Establecer enrutamiento dinámico en cada uno de los ruteadores

4.2. Procedimiento

4.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[3]

4.2.2. Realizamos la topología de red como se muestra en la figura en cual estamos utilizando una nube frame relay

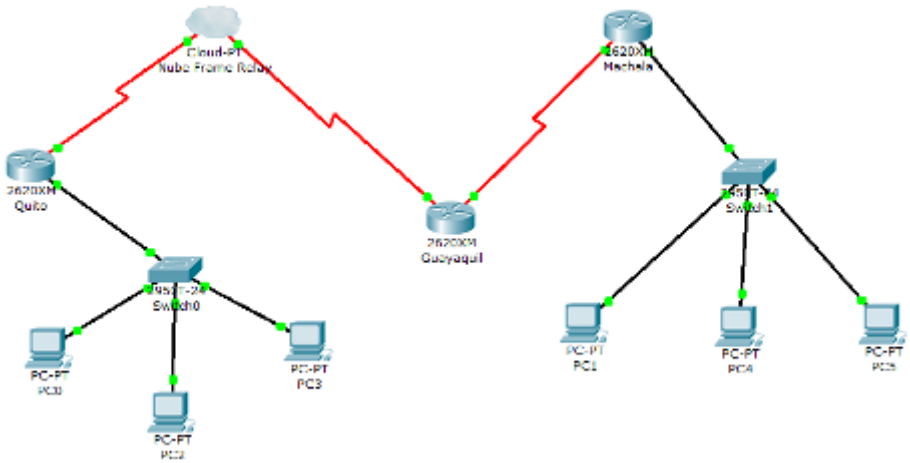

Figura 4.2.2.1

4.2.3. Debemos configurar la dirección IP y su respectiva mascara de red para todas las CPU´s conectadas en la red, para ello procedemos a dar un clic en cada una de las CPU´s de la red, para lo cual se abre una pantalla de configuración como se puede observar en la figura

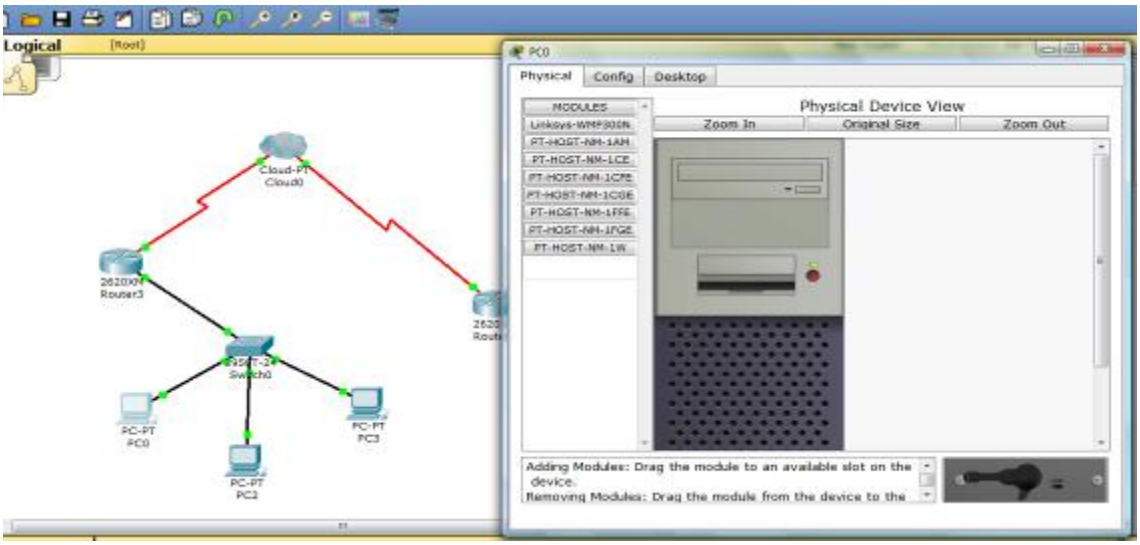

Figura 4.2.3.1 Edit CPU's

4.2.4. En la pantalla que aparece nos debemos dirigir a la pestaña con el nombre de desktop, y luego en IP configuration en la cual procedemos con la configuración de nuestra dirección IP con el respectivo Gateway para poder acceder a otras redes y nuestra mascara de red como se observa en la figura

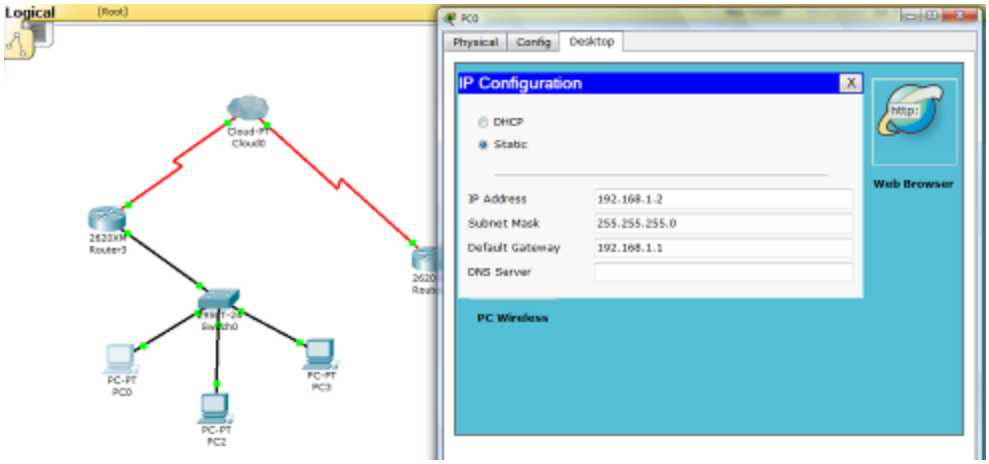

Figura 4.2.4.1 CPU's

4.2.5. Lo mismo la ips para el otro sector de la red.

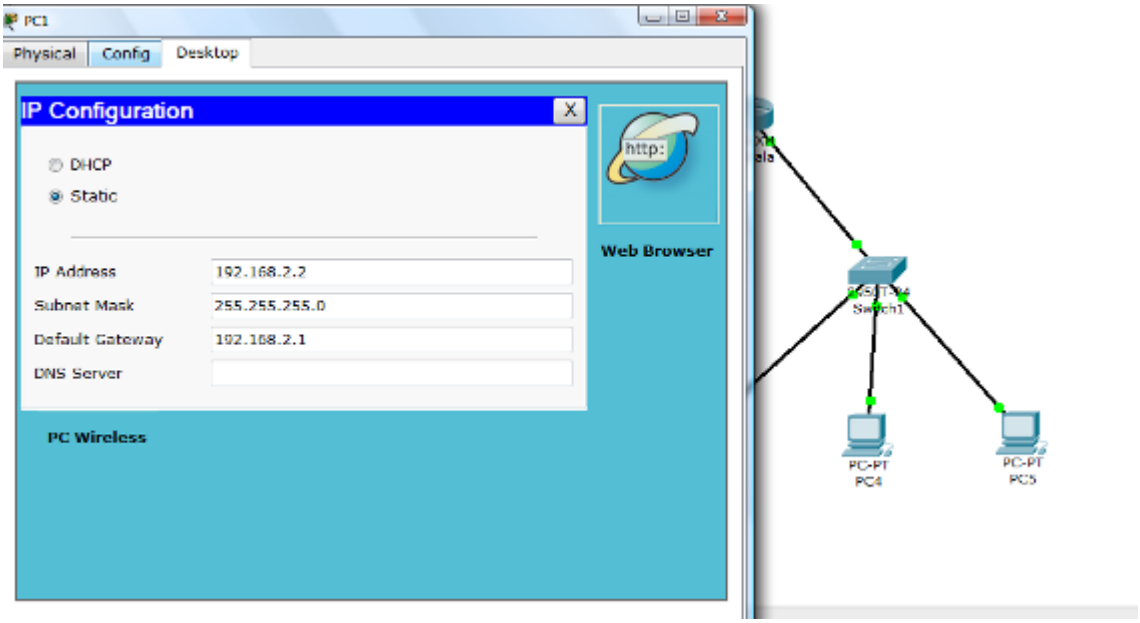

Figura 4.2.5.1

4.2.6. Para realizar la configuración de los ruteadores Quito, Guayaquil, Machala, es importante indicar que debemos insertar la tarjeta WIC 1T como se muestra en la figura para este procedimiento el ruteador se debe encontrar apagado y encenderlo posteriormente

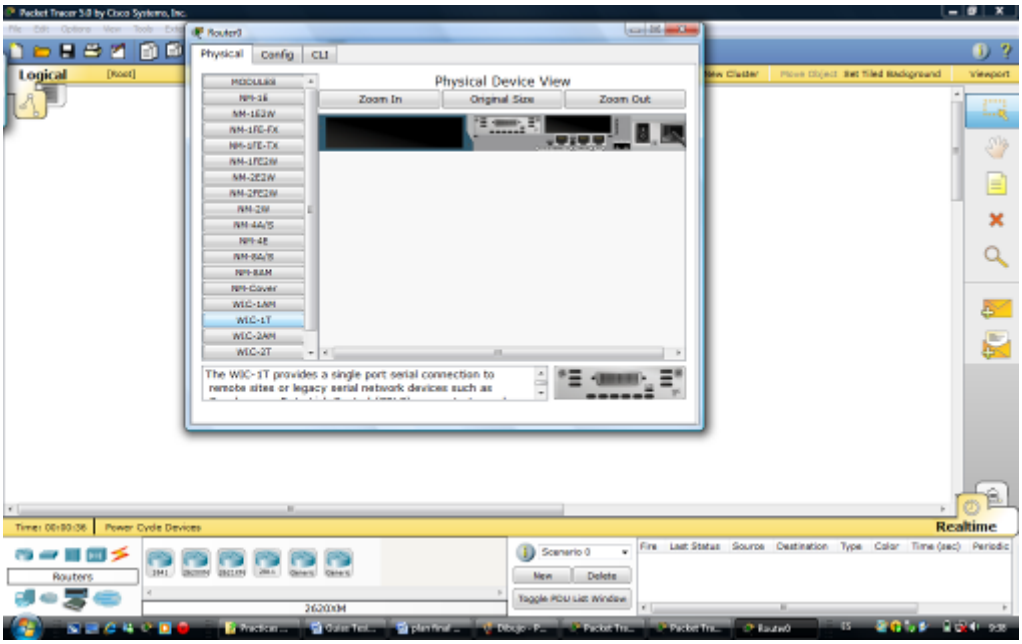

Figura 4.2.6.1 Interfaz Serial

4.2.7. Procedemos con la configuración del Ruteador Quito con el cual utilizaremos el modelo 2620XM.

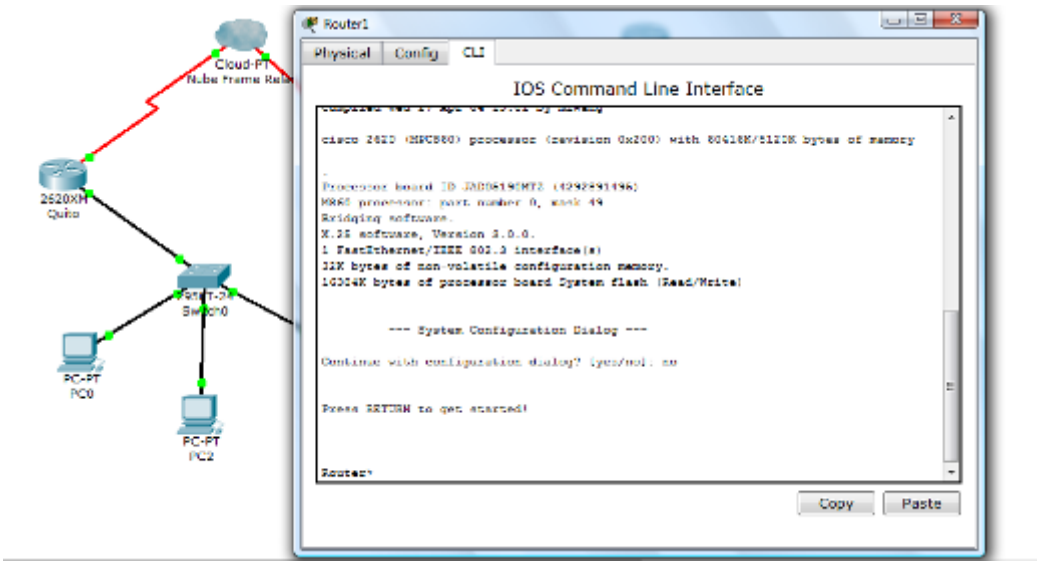

Figura 4.2.8.1

4.2.7.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Quito

4.2.7.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Quito(config)#int f0/0
Quito(config-if)#ip address 192.168.1.1 255.255.255.0
Quito(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Quito(config-if)#exit

4.2.7.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

Quito(config)#int s0/0
Quito(config-if)#ip address 172.16.4.1 255.255.0.0
Quito(config-if)#encapsulation frame-relay ietf
Quito(config-if)#frame-relay lmi-type ansi
Quito(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Quito(config-if)# exit

4. Configuramos las rutas estáticas en el equipo local

Quito(config)#router rip
Quito(config-router)#network 172.16.0.0
Quito(config-router)#network 192.168.1.0

Quito#wr
Building configuration...
[OK]
Quito#

NOTA: Los ruteadores que se conectan a la Nube Frame Relay se la debe configurar como Interfaces DTE

4.2.7.4. Como último paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

Quito#sh running-config
Building configuration...

```
Current configuration : 289 bytes
!
version 12.2
no service password-encryption
!
hostname Quito
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
router rip
 network 172.16.0.0
 network 192.168.1.0
!
ip classless
!
!
line con 0
line vty 0 4
 login
!
!
end
Quito#
```

4.2.8. Procedemos con la configuración del Ruteador Guayaquil con el cual utilizaremos el modelo 2620XM, con interfaces seriales

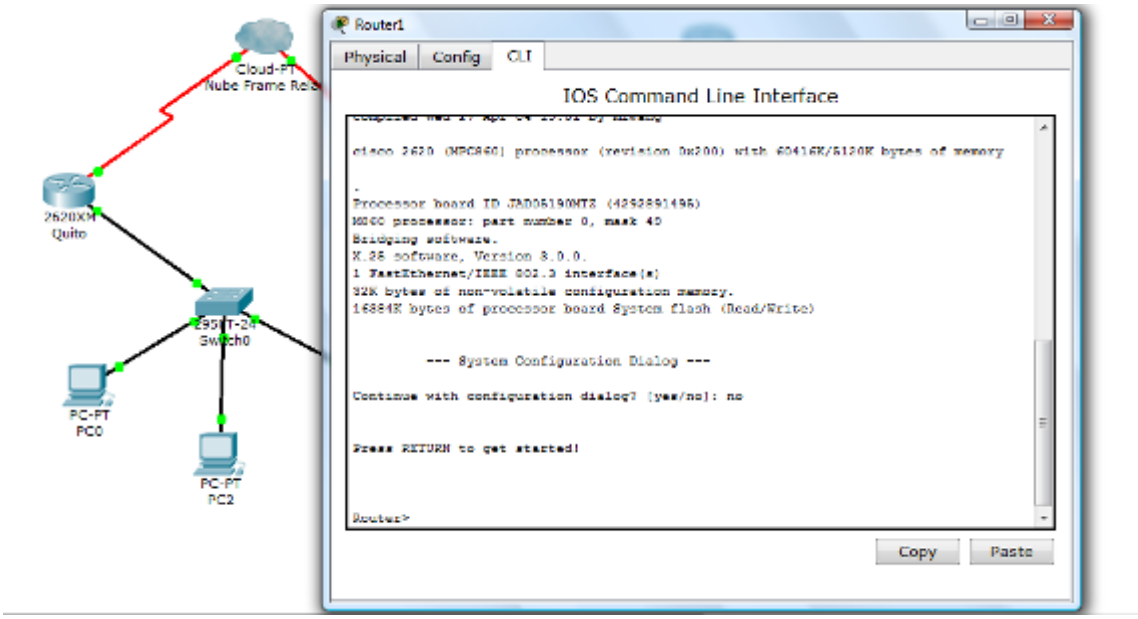

Figura 4.2.7.5.1

4.2.8.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Guayaquil

4.2.8.2. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

Guayaquil(config)#int s0/0
Guayaquil(config-if)#ip address 172.16.4.2 255.255.0.0
Guayaquil(config-if)#encapsulation frame-relay ietf
Guayaquil(config-if)#frame-relay lmi-type ansi
Guayaquil(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up

Guayaquil (config-if)# exit

Guayaquil(config)#int s0/1
Guayaquil(config-if)#ip address 10.0.0.1 255.0.0.0
Guayaquil(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Guayaquil (config-if)# exit

4.2.8.3. Configuramos las rutas estáticas en el equipo local

Guayaquil(config)#router rip
Guayaquil(config-router)#network 172.16.0.0
Guayaquil(config-router)#network 10.0.0.0
Guayaquil#wr
Building configuration...
[OK]
Guayaquil #

NOTA: Los ruteadores que se conectan a la Nube Frame Relay se la debe configurar como Interfaces DTE

4.2.8.4. Como último paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

Guayaquil#sh running-config
Building configuration...

Current configuration : 459 bytes
!
version 12.2

```
no service password-encryption
!
hostname Guayaquil
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 172.16.4.2 255.255.0.0
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
!
interface Serial0/1
 ip address 10.0.0.1 255.0.0.0
!
router rip
 network 10.0.0.0
 network 172.16.0.0
!
ip classless
!
!
line con 0
line vty 0 4
 login
```

!

!

end

Guayaquil#

4.2.9. Procedemos con la configuración del Ruteador Machala con el cual utilizaremos el modelo 2620XM.

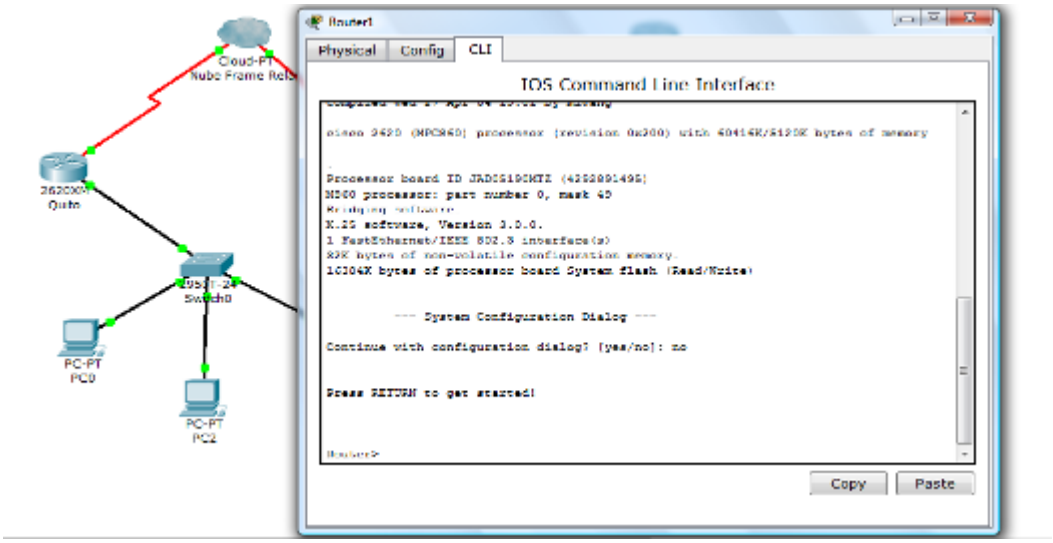

Figura 4.2.9.1

4.2.9.1. Ponemos nombre al ruteador

Router>enable

Router#conf t

Router(config)#hostname Machala

4.2.9.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Machala(config)#int f0/0

Machala(config-if)#ip address 192.168.2.1 255.255.255.0

Machala(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Machala(config-if)#exit

4.2.9.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

Machala(config)#int s0/0
Machala(config-if)#ip address 10.0.0.2 255.0.0.0
Machala(config-if)#clock rate 56000
Machala(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Machala(config-if)# exit

4.2.9.4. Configuramos las rutas estáticas en el equipo local

Machala(config)#router rip
Machala(config-router)#network 192.16.2.0
Machala (config-router)#network 10.0.0.0
Machala#wr
Machala#

4.2.9.5. Como último paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

Machala#sh running-config
Building configuration...

Current configuration : 373 bytes
!
version 12.2

```
no service password-encryption
!
hostname Machala
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.0.0.2 255.0.0.0
 clock rate 56000
!
router rip
 network 10.0.0.0
 network 192.168.2.0
!
ip classless
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

Machala#

4.2.10. Procedemos con la configuración de la Nube Frame Relay

4.2.10.1. Lo que primero debemos realizar en la Nube es limitar los DLCI en los seriales dependiendo del router conectado y el nombre que vamos a utilizar con fines administrativos. En este caso nos dirigimos a la Serial0 donde está conectado directamente con el Router de Quito.

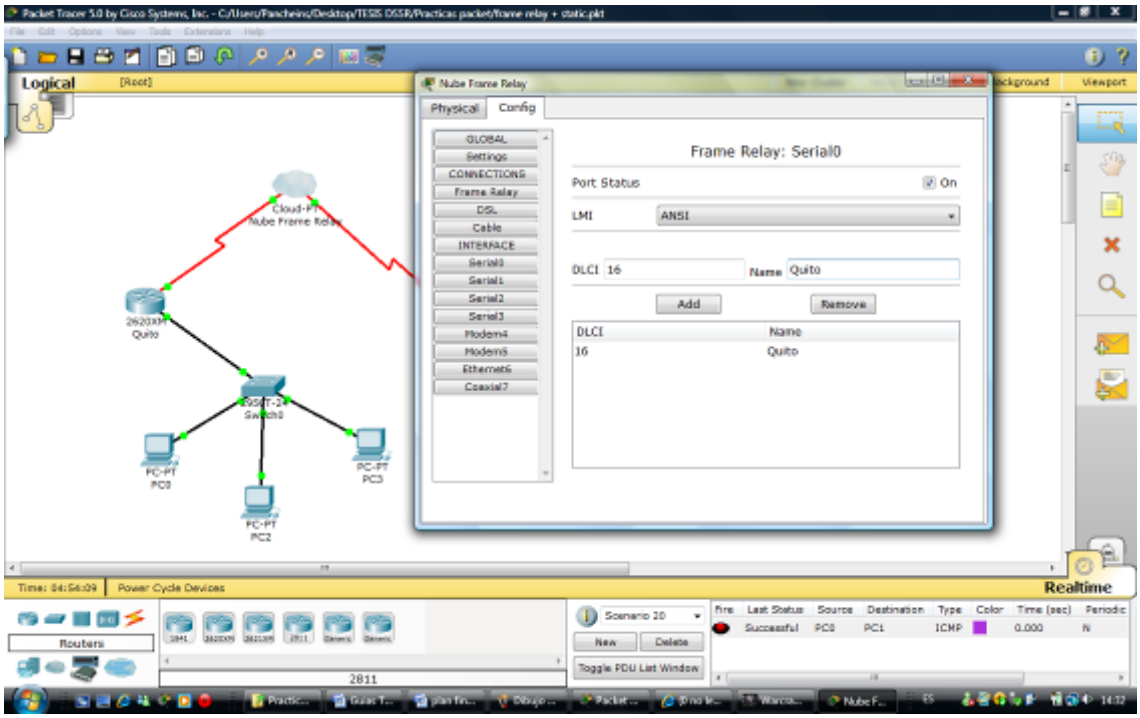

Figura 4.2.10.1

4.2.10.2. Posteriormente lo mismo para la Serial1 donde se encuentra conectado directamente con el Router de Guayaquil.

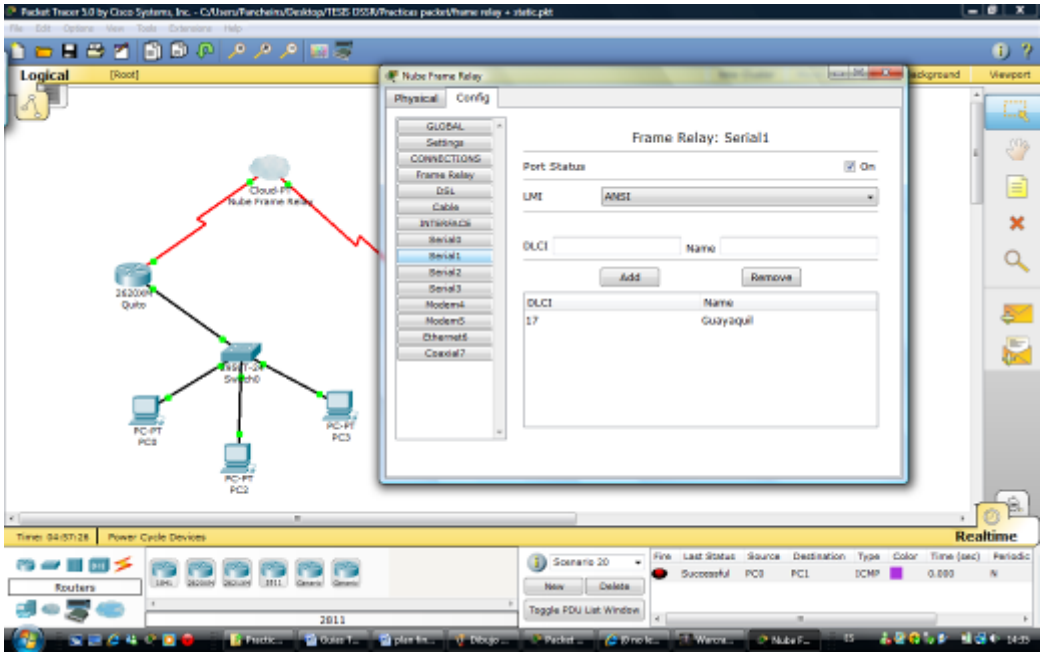

Figura 4.2.10.2.1

4.2.10.3. Y como último paso en la Nube Frame Relay direccionamos la PVC o el túnel virtual entre el Router de Quito y el Router de Guayaquil tal cual se muestra la figura.

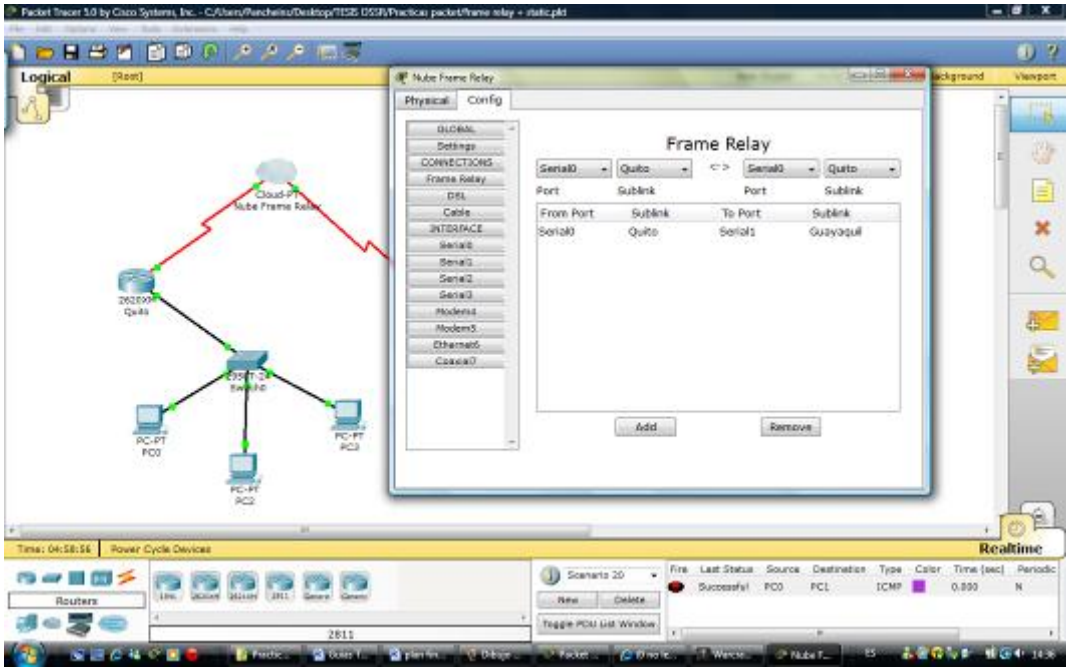

Figura 4.2.10.3.1

4.3. Análisis de resultados

4.3.1. Hacemos ping a una estación de trabajo vía command prompt

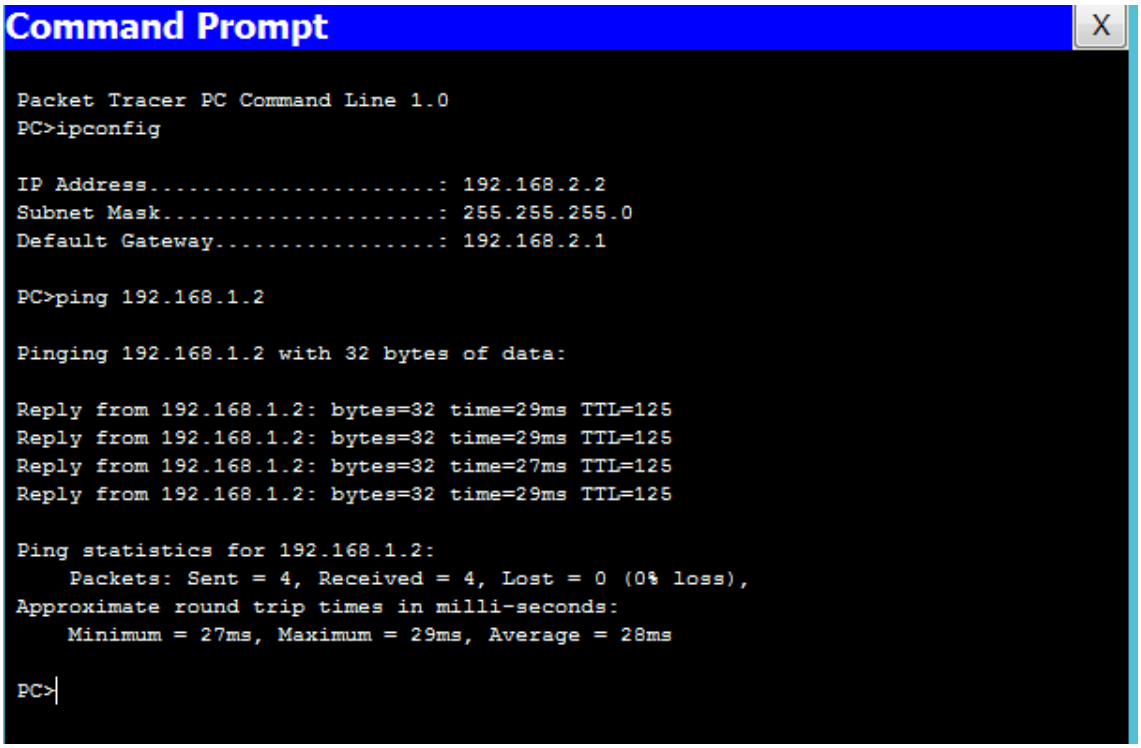

Figura 4.3.1.1

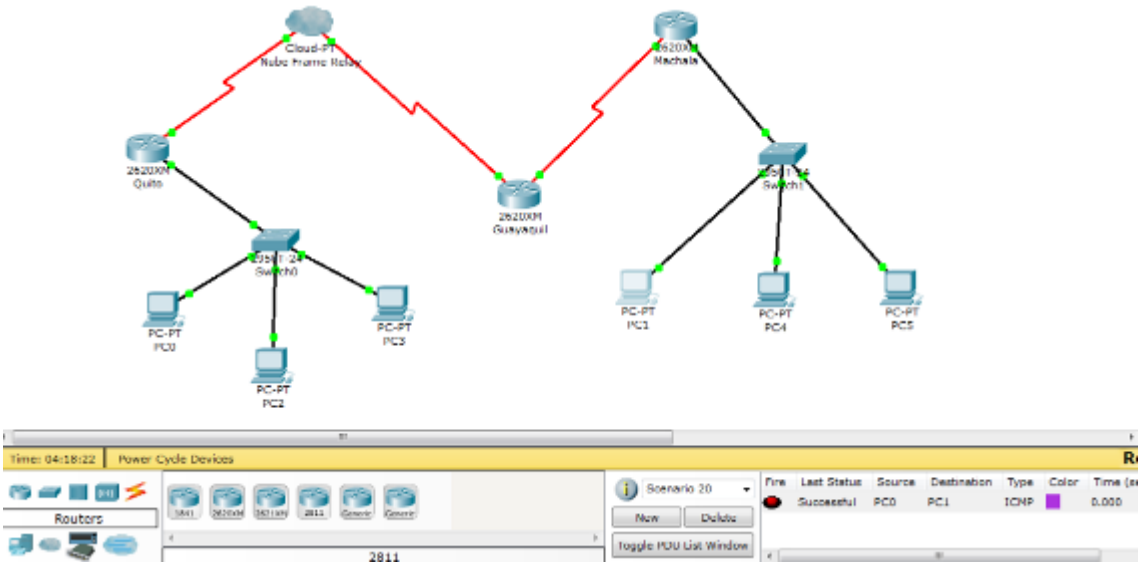

Figura 4.3.2.1

4.4. Análisis de resultados

- Se puede observar en la simulación que podemos hacer ping desde la PC0 hasta la PC1
- Al realizar la simulación de la red se debe tener muy en cuenta que todos routers estén configurados debidamente el enrutamiento caso contrario no se podrían enviar ninguna información.

4.5. Conclusiones

- Las graficas de la simulación permitieron observar que los paquetes se trasladaron sin ningún problema por la red
- Con la simulación realizada se cumplieron los objetivos requeridos
- Se puede observar muy claramente que la red se encuentra funcionando correctamente con todos sus elementos

4.6. Recomendaciones

- En las redes Frame Relay es recomendable hacer la configuración del camino virtual una vez culminada la topología con sus respectivas interfaces subidas y configuradas
- Cuando se configura la PVC es importante tener el mapa de conectividad de donde desea el administrador de la red transmitir los paquetes

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

5. Guía de práctica: Realizar un test para una red Frame Relay

5.1. Objetivo

- Realizar un test para una red Frame Relay entableciendo las PVC para cada una de las redes interconectadas

5.2. Procedimiento

5.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[4]

5.2.2. Utilizamos la topología de red como se muestra en la figura en cual estamos utilizando una nube frame relay

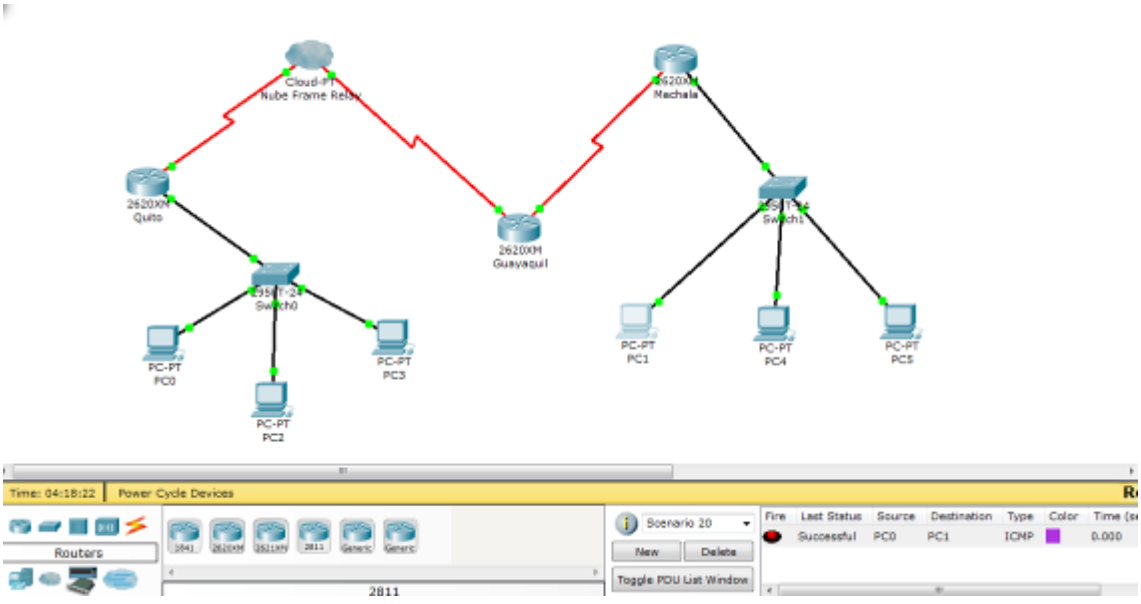

Figura 5.2.2.1

5.2.3. Abrimos un nuevo documento Packet Tracer y abrimos un Activity Wizard, tendríamos una pantalla como se muestra en la figura.

Figura 5.2.3.1

5.2.4. Nos muestra una pantalla de lo que significa una ACTIVIDAD y todos los pasos que debemos seguir para la creación, en la parte de Instrucciones tenemos que digitar cual es el procedimiento de la actividad, tal como se muestra en la figura.

Figura 5.2.4.1

5.2.5. En el siguiente paso Answer Network, creamos la red respuesta pero en este caso importamos la red ya que fue creada anteriormente, en cual solo procedemos activar a la Nube Frame Relay ya que ahí se va a realizar la actividad.

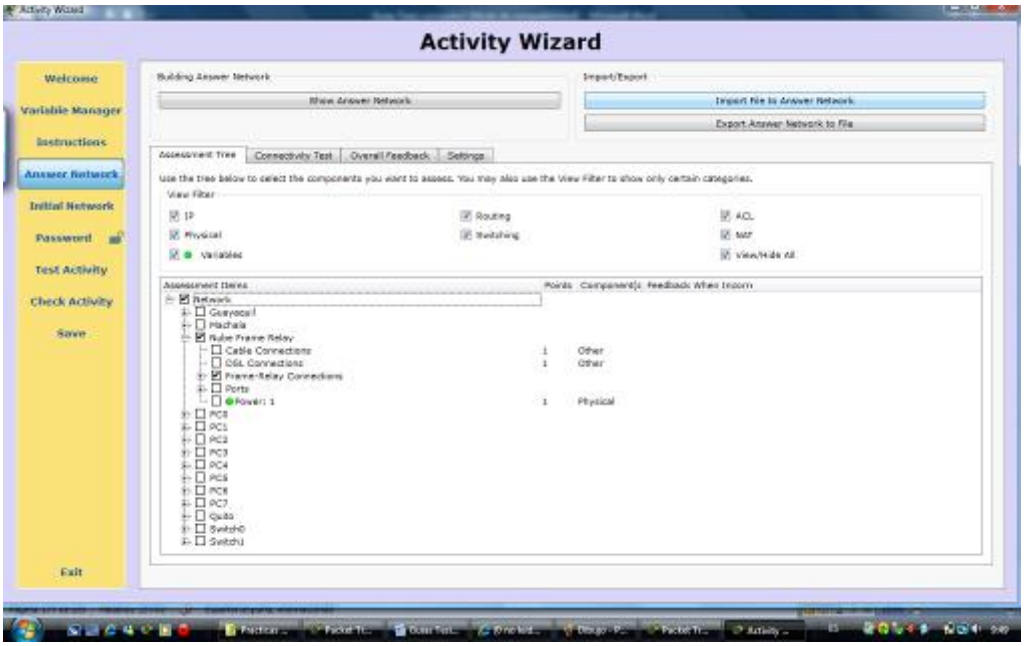

Figura 5.2.5.1

5.2.6. Otra pestaña importante que debemos tener en cuenta es la parte de Overall Feedback, ya que aquí digitamos los mensajes una vez concluida la activad.

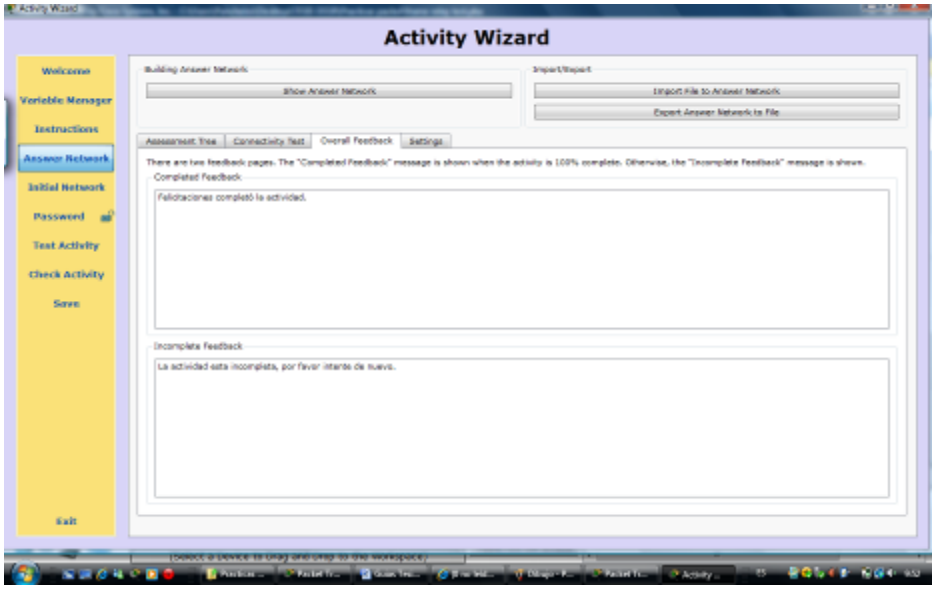

Figura 5.2.6.1

5.2.7. En el siguiente paso Inicial Network, creamos la red inicial pero en este caso importamos la red, que se deberá crear al PVC en la Nube Frame Relay

Figura 5.2.7.1

5.2.8. Y para completar la actividad SAVE, le grabamos como frame relay test y el path del archivo.

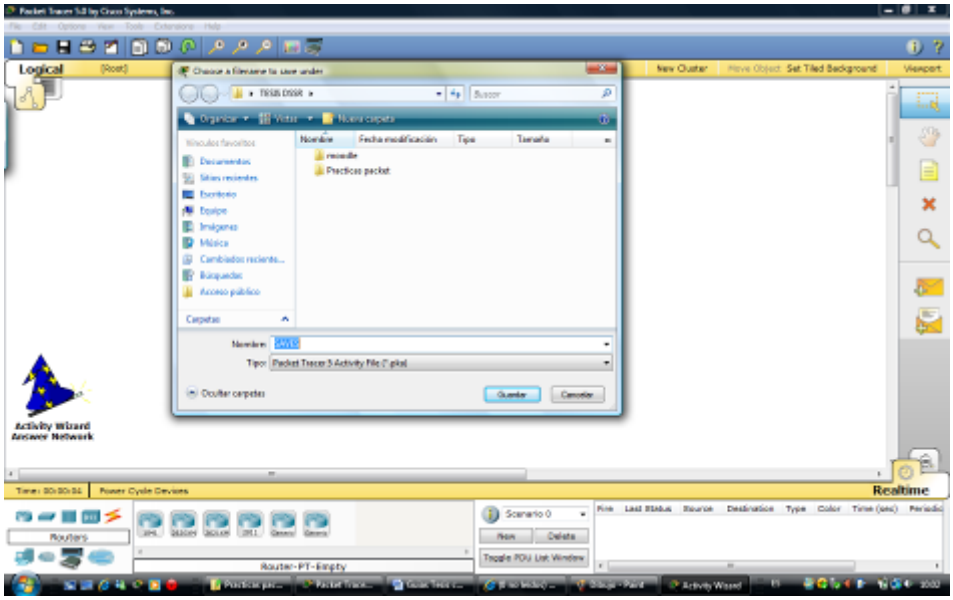

Figura 5.2.8.1

5.2.9. Una vez grabado abrimos el archivo "frame relay.pka", y nos muestra la siguiente pantalla.

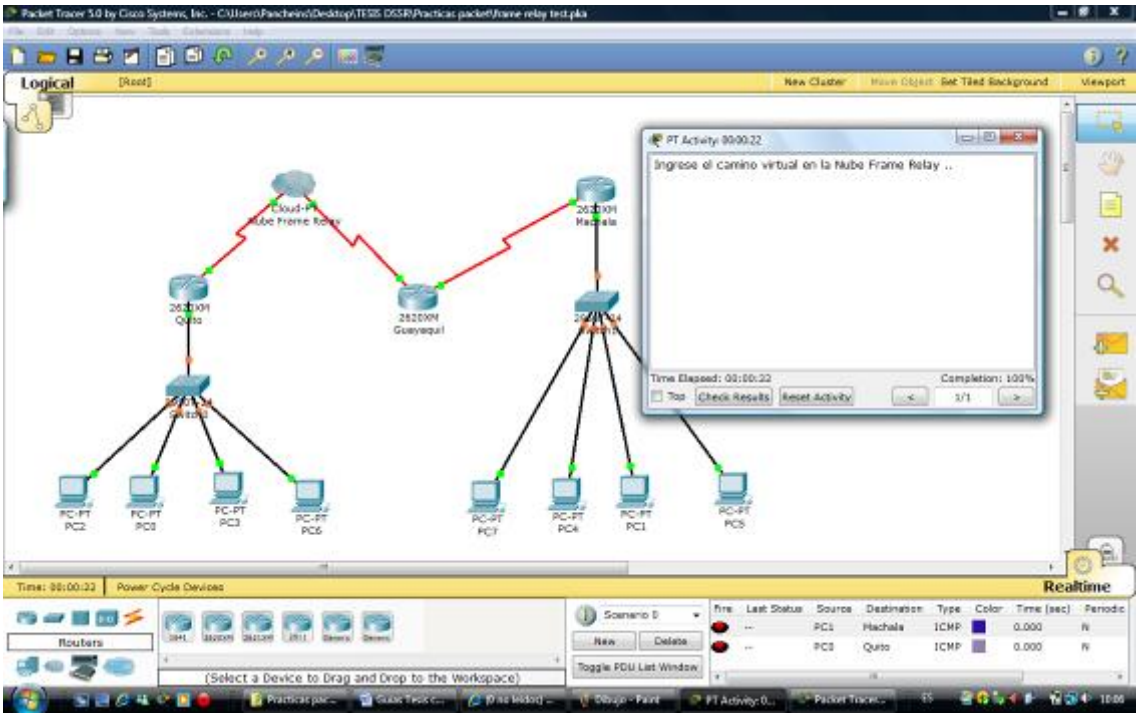

Figura 5.2.10.1

5.2.10. Con el fin de verificar los mensajes si la actividad está completa hacemos click donde dice Check Result

Figura 5.2.10.1

5.2.11. Como siguiente damos click Reset Activity, o ponemos OK

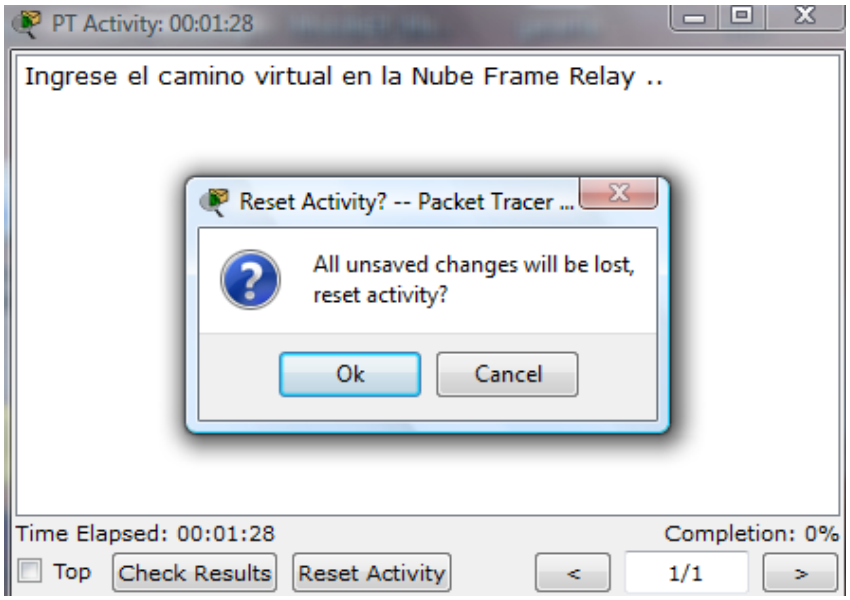

Figura 5.2.11.1

5.2.12. En este paso nos dirigimos a la configuración de la Nube Frame Relay, y damos cuenta la el camino virtual no se encuentra creado tal como se muestra en la figura.

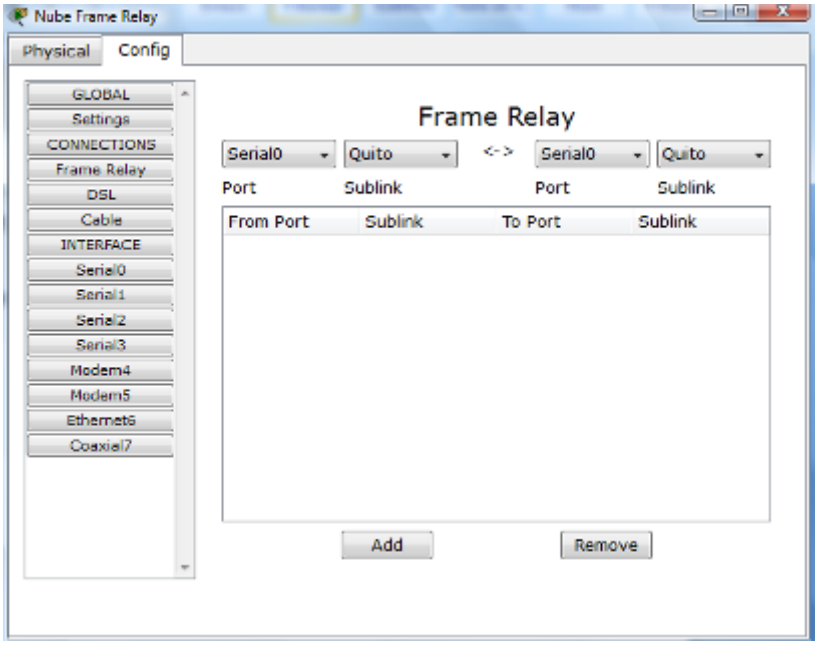

Figura 5.2.12.1

5.2.13. Entonces creamos el camino virtual Serial0 Quito <-> Serial1 Guayaquil y damos click en ADD. Como se muestra en la figura 5.2.13.1

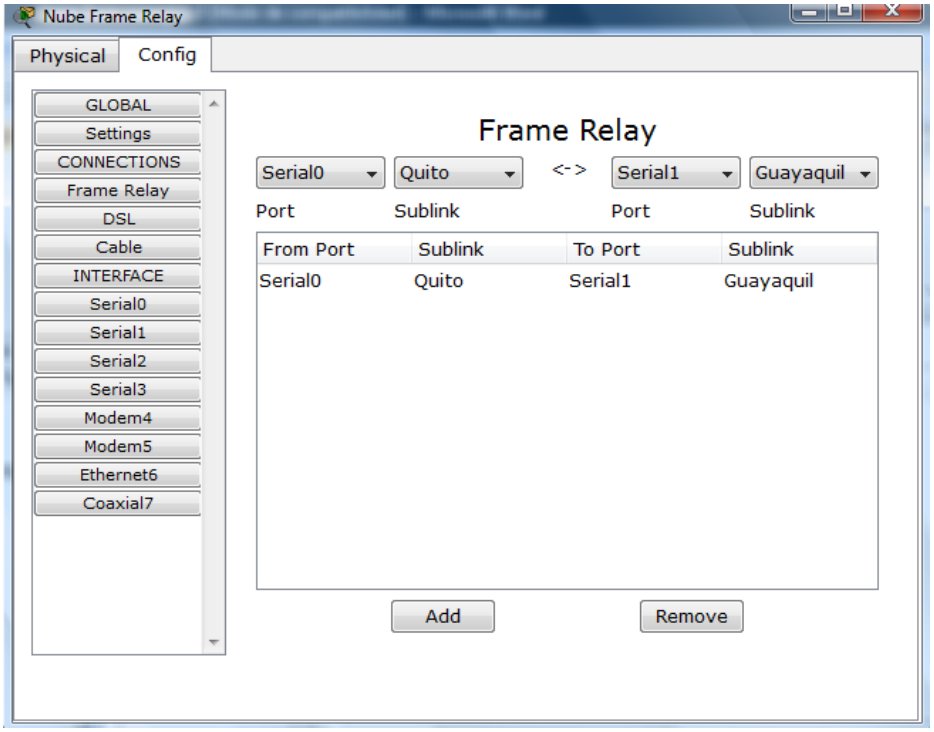

Figura 5.2.13.1

5.2.14. Posteriormente damos tiempo hasta que la red converja totalmente probamos conectividad entre los dispositivos, y posteriormente damos click en Check Result, y finalmente nos muestra una pantalla que la actividad se completo satisfactoriamente.

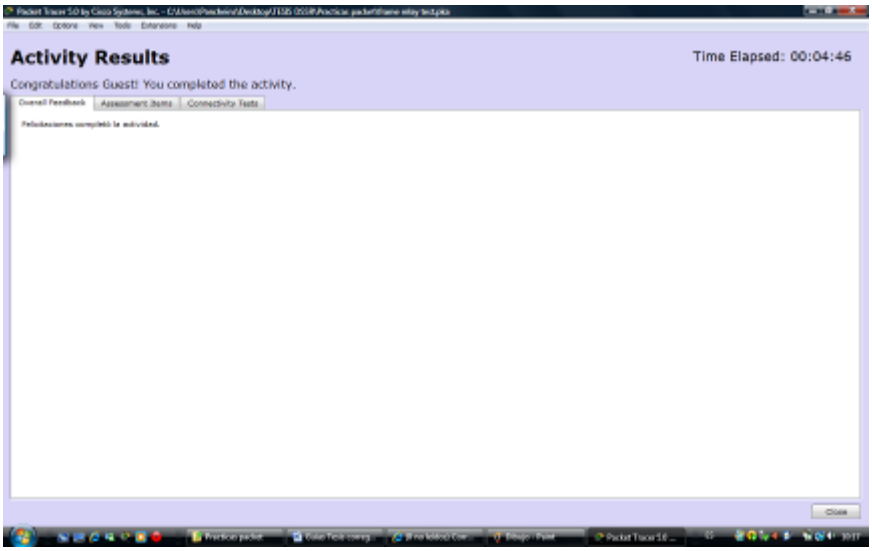

Figura 5.2.14.1

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

6. Guía de práctica: Realizar una red PPP con autentificación CHAP utilizando enrutamiento estático

6.1. Objetivo

- Realizar una red PPP con autentificación CHAP para cada uno de los ruteadores
- Establecer enrutamiento estático en cada ruteador

6.2. Procedimiento

6.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[5]

6.2.2. Realizamos la topología de red como se muestra en la figura 6.2.2.1 en cual estamos utilizando ruteadores modelo 2650

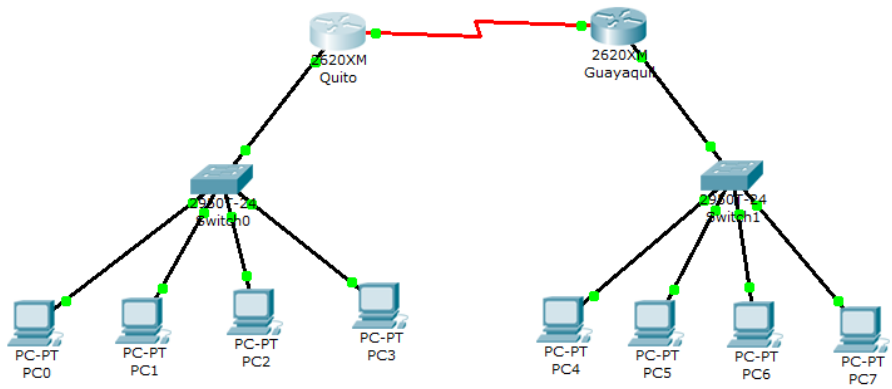

Figura 6.2.2.1

6.2.3. Debemos configurar la dirección IP y su respectiva mascara de red para todas las CPU´s conectadas en la red con la siguiente dirección

192.188.53.0/27, para ello procedemos a dar un clic en cada una de las CPU´s de la red, para lo cual se abre una pantalla de configuración como se puede observar en la figura

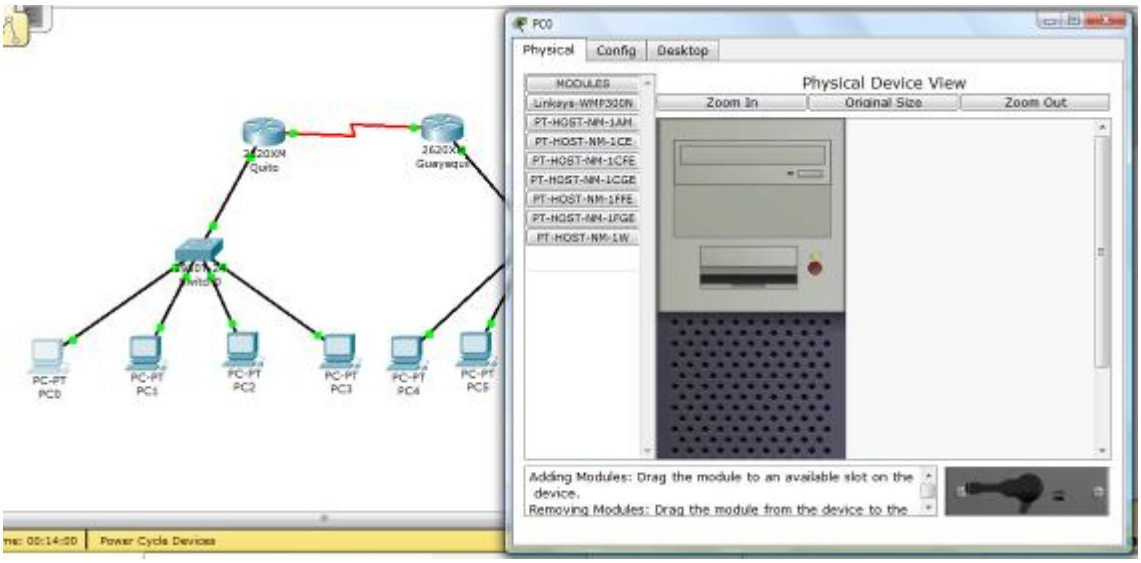

Figura 6.2.3.1 Edit CPU´s

6.2.4. En la pantalla que aparece nos debemos dirigir a la pestaña con el nombre de desktop, y luego en IP configuration en la cual procedemos con la configuración de nuestra dirección IP con el respectivo Gateway para poder acceder a otras redes y nuestra mascara de red como se observa en la figura

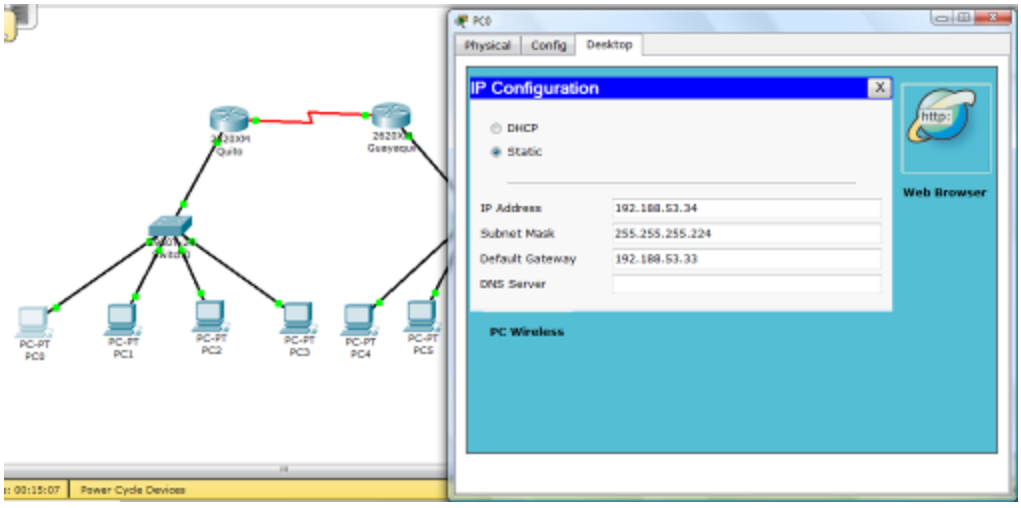

Figura 6.2.4.1 CPU's

6.2.5. Lo mismo la ips para el otro sector de la red.

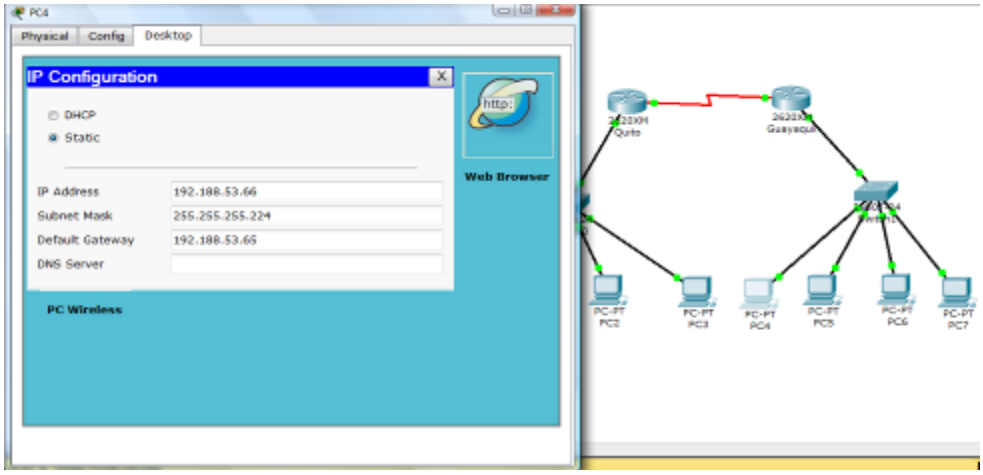

Figura 6.2.5.1

6.2.6. Para realizar la configuración de los ruteadores Quito, Guayaquil, es importante indicar que debemos insertar la tarjeta WIC 1T como se muestra en la figura para este procedimiento el ruteador se debe encontrar apagado y encenderlo posteriormente

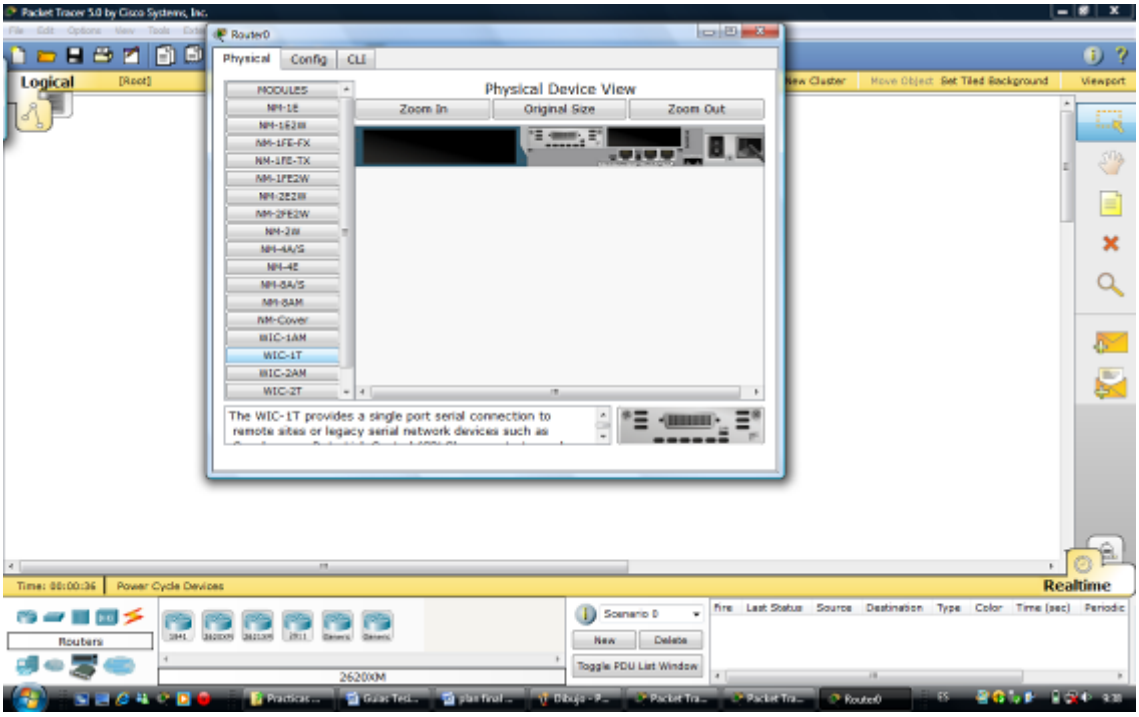

Figura 6.2.6.1 Interfaz Serial

6.2.7. Procedemos con la configuración del Ruteador Quito con el cual utilizaremos el modelo 2620XM.

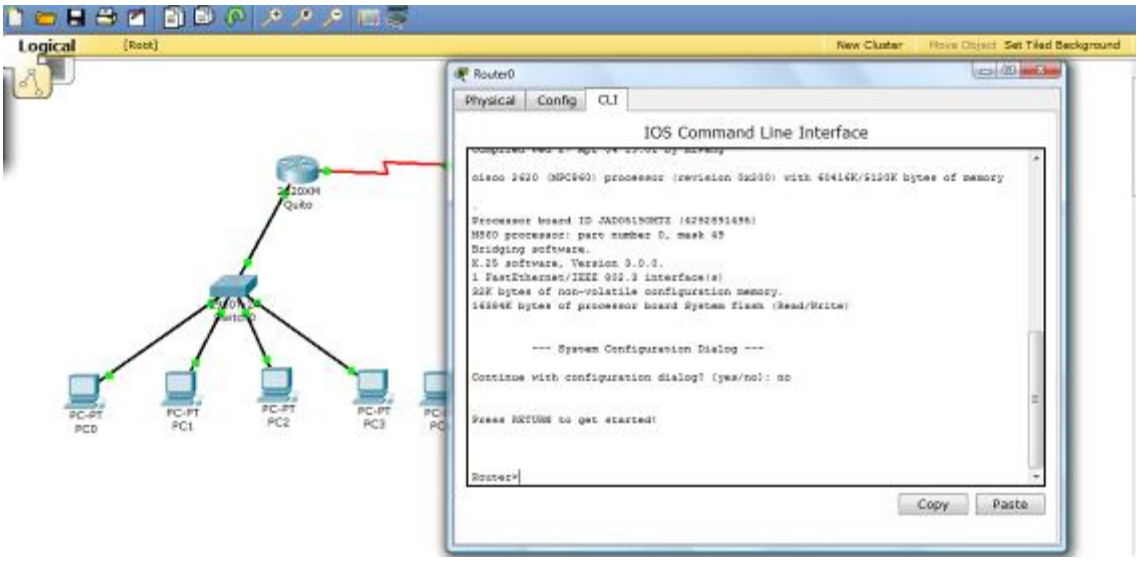

Figura 6.2.7.1

6.2.7.1. Ponemos nombre al ruteador

```
Router>enable
Router#conf t
Router(config)#hostname Quito
```

6.2.7.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

```
Quito(config)#int f0/0
Quito(config-if)#ip address 192.188.53.33 255.255.255.224
Quito(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Quito(config-if)#exit
```

6.2.7.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

```
Quito(config)#int s0/0
Quito(config-if)#ip address 192.188.53.97 255.255.255.224
Quito(config-if)#encapsulation ppp
Quito(config-if)#clock rate 56000
Quito(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Quito(config-if)# exit

Quito(config)#username Guayaquil password wan
Quito(config)#int s0/0
Quito(config-if)#ppp authentication chap
```

6.2.7.4. Configuramos las rutas estáticas en el equipo local

```
Quito(config)# ip route 192.188.53.64 255.255.255.224 192.188.53.98

Quito#wr
Building configuration...
[OK]
Quito#
```

6.2.7.5. El siguiente paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

```
Quito#sh running-config
Building configuration...
```

```
Current configuration : 468 bytes
!
version 12.2
no service password-encryption
!
hostname Quito
!
!
!
!

username Guayaquil password 0 wan
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.188.53.33 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.188.53.97 255.255.255.224
 encapsulation ppp
 ppp authentication chap
 clock rate 56000
!
ip classless
ip route 192.188.53.64 255.255.255.224 192.188.53.98
!
!
```

!

line con 0

line vty 0 4

login

!

!

end

Quito#

6.2.8. Procedemos con la configuración del Ruteador Guayaquil con el cual utilizaremos el modelo 2620XM, con interfaces seriales

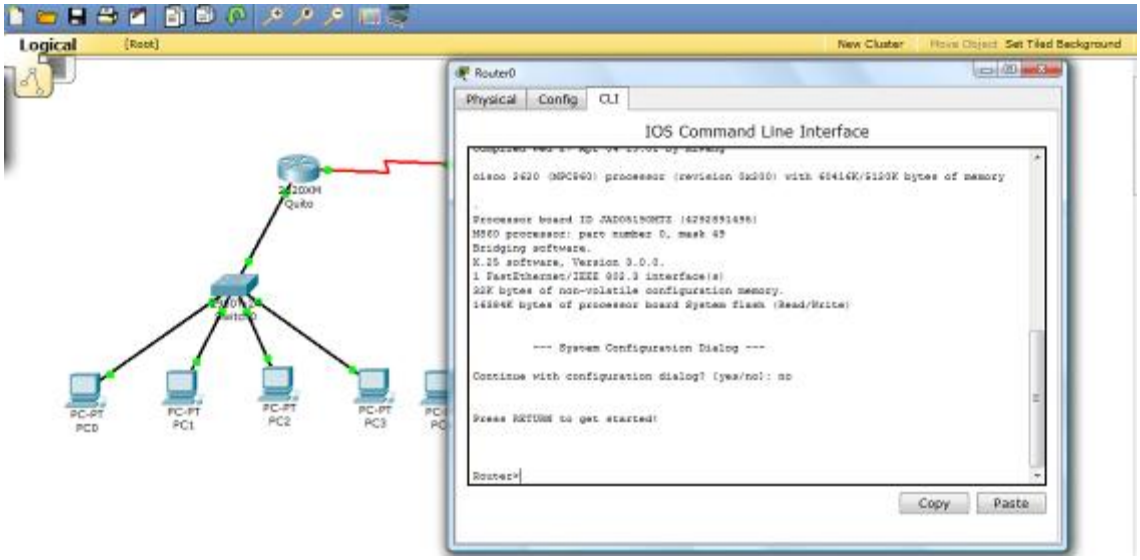

Figura 6.2.8.1

6.2.8.1. Ponemos nombre al ruteador

Router>enable

Router#conf t

Router(config)#hostname Guayaquil

6.2.8.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

```
Guayaquil(config)#int f0/0
Guayaquil(config-if)#ip address 192.188.53.65 255.255.255.224
Guayaquil(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Guayaquil(config-if)#exit
```

6.2.8.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

```
Guayaquil(config)#int s0/0
Guayaquil(config-if)#ip address 192.188.53.98 255.255.255.224
Guayaquil(config-if)#encapsulation ppp
Guayaquil(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Guayaquil(config-if)# exit

Guayaquil(config)#username Quito password wan
Guayaquil(config)#int s0/0
Guayaquil(config-if)#ppp authentication chap
```

6.2.8.4. Configuramos las rutas estáticas en el equipo local

```
Guayaquil(config)# ip route 192.188.53.32 255.255.255.224
192.188.53.97
Guayaquil#wr
Building configuration...
[OK]
Guayaquil#
```

6.2.8.5. Mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

```
Guayaquil#sh running-config
Building configuration...

Current configuration : 450 bytes
!
version 12.2
no service password-encryption
!
hostname Guayaquil
!
!
!
username Quito password 0 wan
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.188.53.65 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.188.53.98 255.255.255.224
 encapsulation ppp
 ppp authentication chap
!
ip classless
```

ip route 192.188.53.32 255.255.255.224 192.188.53.97

!

!

!

line con 0

line vty 0 4

login

!

!

end

Guayaquil#

6.3. Análisis de resultados

6.3.1. Hacemos ping a una estación de trabajo vía command prompt

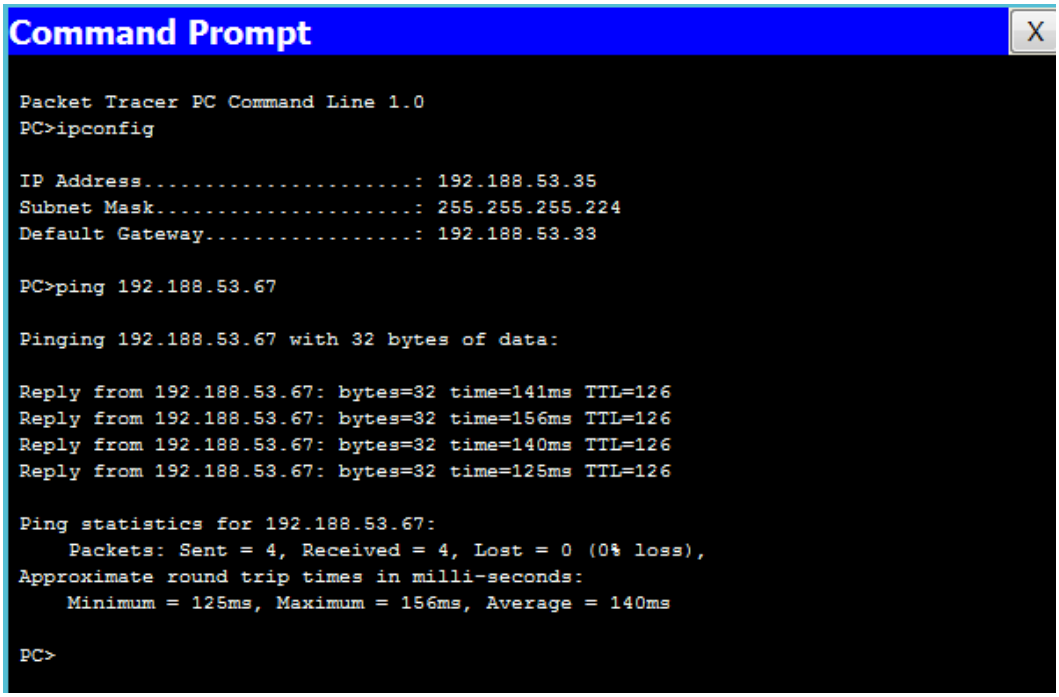

Figura 6.3.1.1

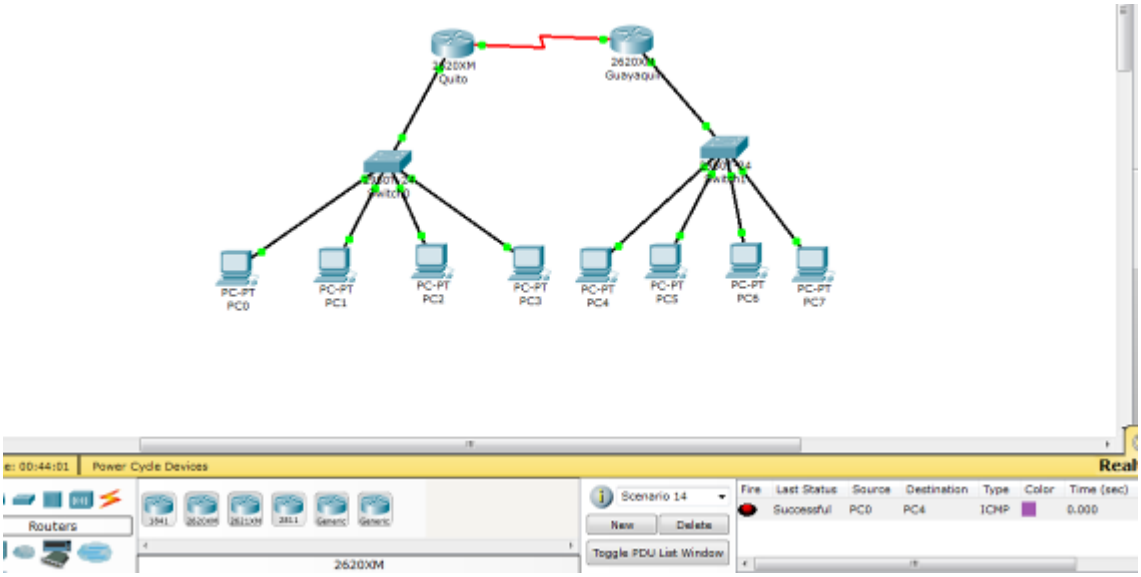

Figura 6.3.1.2

6.4. Análisis de resultados

- Se puede observar en la simulación que podemos hacer ping desde la PC0 hasta la PC4
- Al realizar la simulación de la red se debe tener muy en cuenta que todos routers estén configurados debidamente el enrutamiento y la autentificación caso contrario no se podrían enviar ninguna información.

6.5. Conclusiones

- Las graficas de la simulación permitieron observar que los paquetes se trasladaron sin ningún problema por la red
- Con la simulación realizada se cumplieron los objetivos requeridos

7. Guía de práctica: Realizar una red PPP con autentificación CHAP utilizando enrutamiento dinámico

7.1. Objetivo

- Realizar una red PPP con autentificación CHAP para cada uno de los ruteadores
- Establecer enrutamiento dinámico en cada ruteador

7.2. Procedimiento

7.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[6]

7.2.2. Realizamos la topología de red como se muestra en la figura en cual estamos utilizando ruteadores modelo 2650

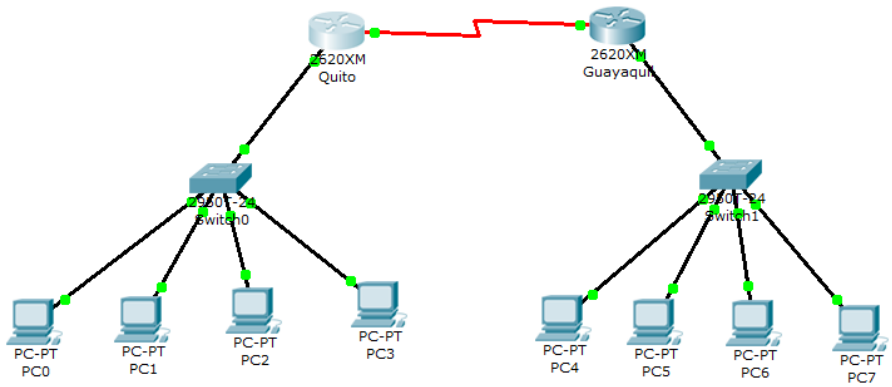

Figura 7.2.2.1

7.2.3. Debemos configurar la dirección IP y su respectiva mascara de red para todas las CPU´s conectadas en la red con la siguiente dirección 192.188.53.0/27, para ello procedemos a dar un clic en cada una de las CPU´s de la red, para lo cual se abre una pantalla de configuración como se puede observar en la figura

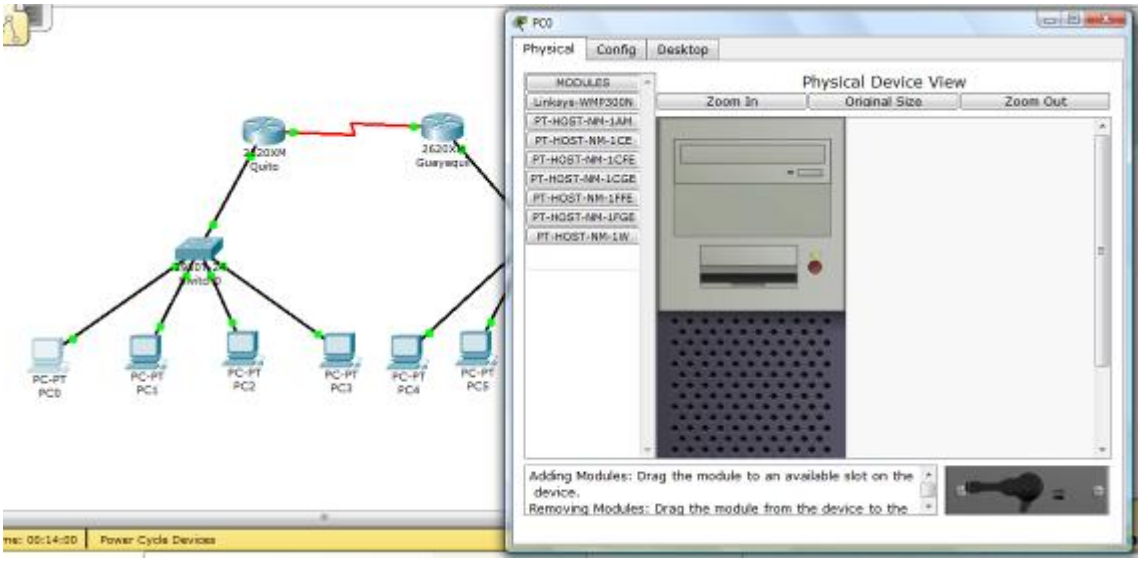

Figura 7.2.3.1 Edit CPU's

7.2.4. En la pantalla que aparece nos debemos dirigir a la pestaña con el nombre de desktop, y luego en IP configuration en la cual procedemos con la configuración de nuestra dirección IP con el respectivo Gateway para poder acceder a otras redes y nuestra mascara de red como se observa en la figura

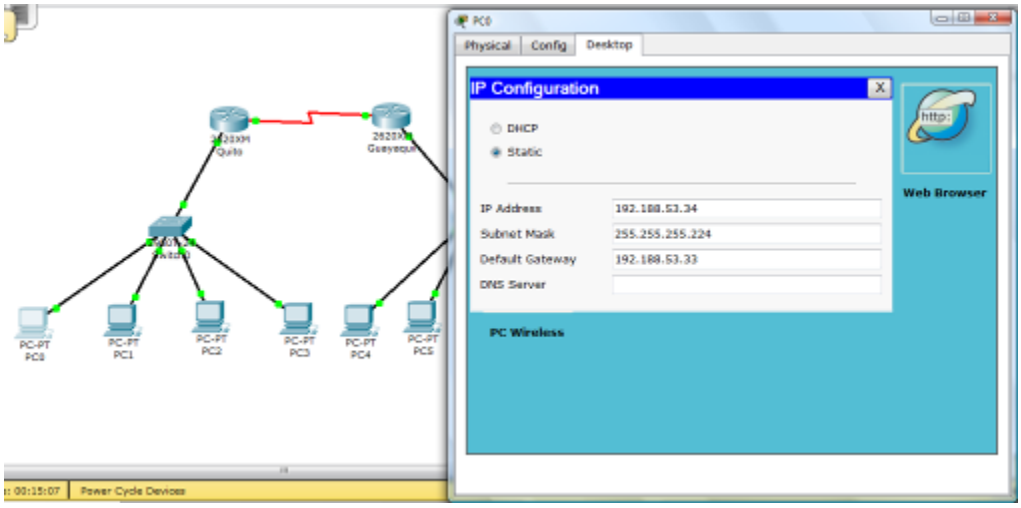

Figura 7.2.4.1 CPU's

7.2.5. Lo mismo la ips para la otro sector de la red.

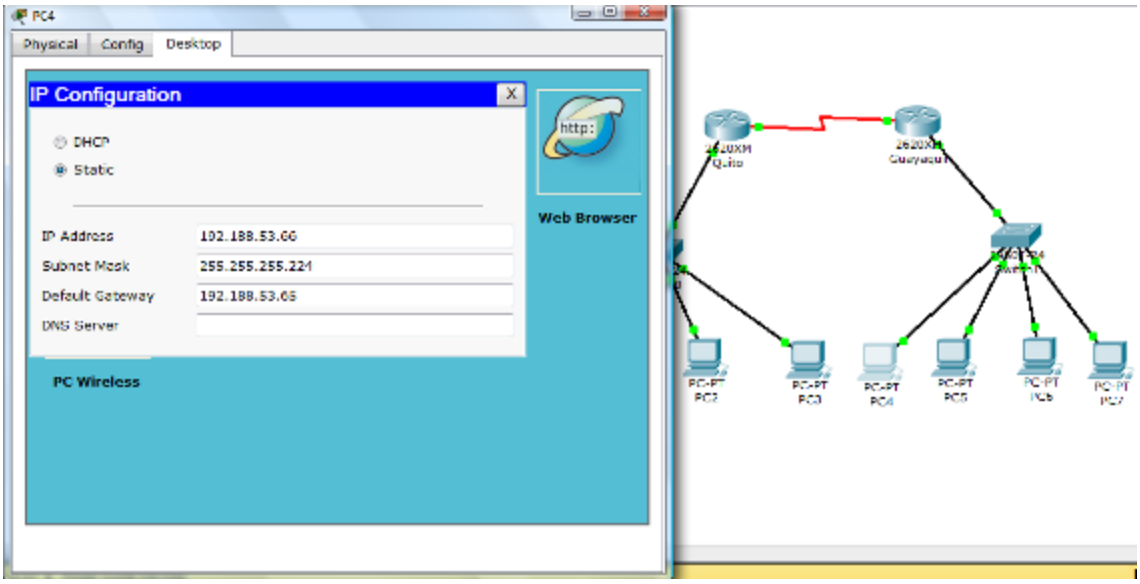

Figura 7.2.5.1

7.2.6. Para realizar la configuración de los ruteadores Quito, Guayaquil, es importante indicar que debemos insertar la tarjeta WIC 1T como se muestra en la figura para este procedimiento el ruteador se debe encontrar apagado y encenderlo posteriormente

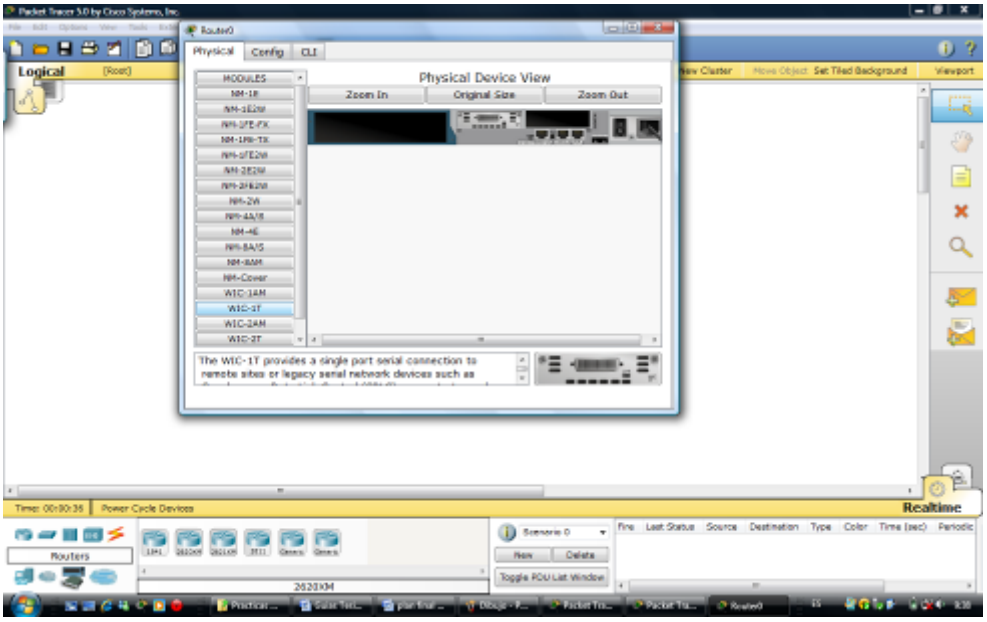

Figura 7.2.6.1 Interfaz Serial

7.2.7. Procedemos con la configuración del Ruteador Quito con el cual utilizaremos el modelo 2620XM.

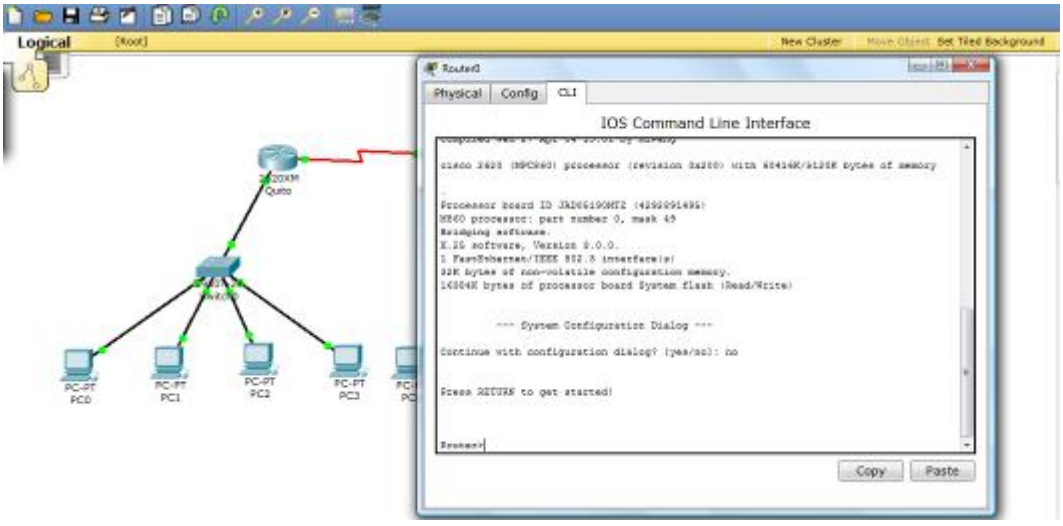

Figura 7.2.7.1

7.2.7.1. Ponemos nombre al ruteador

```
Router>enable
Router#conf t
Router(config)#hostname Quito
```

7.2.7.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

```
Quito(config)#int f0/0
Quito(config-if)#ip address 192.188.53.33 255.255.255.224
Quito(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Quito(config-if)#exit
```

7.2.7.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

```
Quito(config)#int s0/0
Quito(config-if)#ip address 192.188.53.97 255.255.255.224
Quito(config-if)#encapsulation ppp
Quito(config-if)#clock rate 56000
Quito(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Quito(config-if)# exit
```

```
Quito(config)#username Guayaquil password wan
Quito(config)#int s0/0
Quito(config-if)#ppp authentication chap
```

7.2.7.4. Configuramos las rutas dinámicas en el equipo local

```
Quito(config)#router rip
Quito(config-router)#network 192.188.53.0
```

```
Quito#wr
Building configuration...
```

[OK]
Quito#

7.2.7.5. El siguiente paso de la configuración del router mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

```
Quito#sh running-config
Building configuration...

Current configuration : 449 bytes
!
version 12.2
no service password-encryption
!
hostname Quito
!
!
!
!
!
username Guayaquil password 0 wan
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.188.53.33 255.255.255.224
 duplex auto
 speed auto
!
```

```
interface Serial0/0
 ip address 192.188.53.97 255.255.255.224
 encapsulation ppp
 ppp authentication chap
 clock rate 56000
!
router rip
 network 192.188.53.0
!
ip classless
!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end

Quito#
```

7.2.8. Procedemos con la configuración del Ruteador Guayaquil con el cual utilizaremos el modelo 2620XM, con interfaces seriales

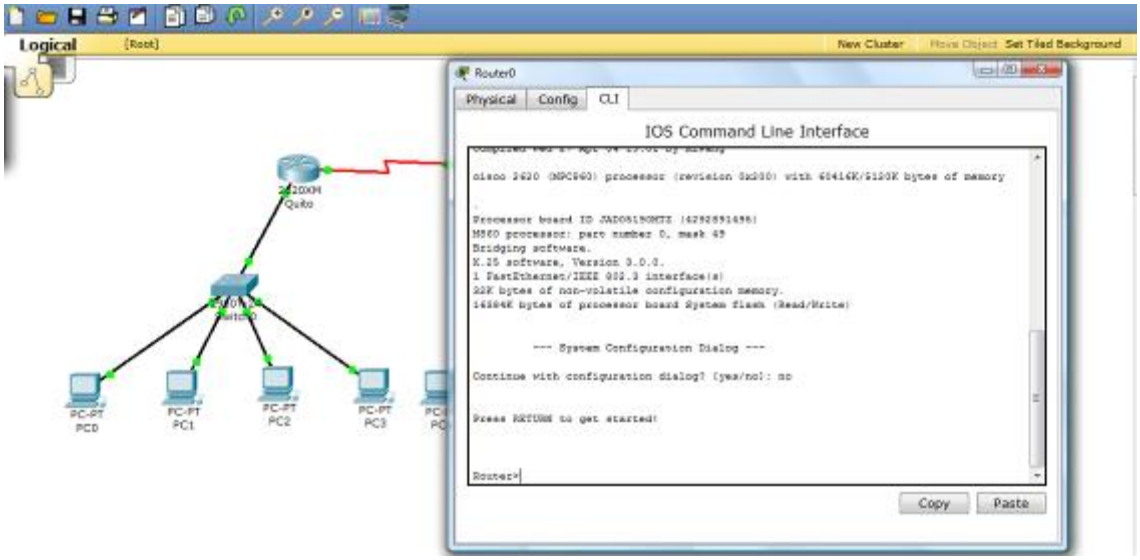

Figura 7.2.8.1

7.2.8.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Guayaquil

7.2.8.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Guayaquil(config)#int f0/0
Guayaquil(config-if)#ip address 192.188.53.65 255.255.255.224
Guayaquil(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Guayaquil(config-if)#exit

7.2.8.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente y la encapsulación que va a utilizar nuestra red

Guayaquil(config)#int s0/0
Guayaquil(config-if)#ip address 192.188.53.98 255.255.255.224

```
Guayaquil(config-if)#encapsulation ppp
Guayaquil(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Guayaquil(config-if)# exit

Guayaquil(config)#username Quito password wan
Guayaquil(config)#int s0/0
Guayaquil(config-if)#ppp authentication chap
```

7.2.8.4. Configuramos las rutas dinámicas en el equipo local

```
Guayaquil(config)#router rip
Guayaquil(config-router)#network 192.188.53.0
Building configuration...
[OK]
Guayaquil#
```

7.2.8.5. Mostramos toda la configuración con el comando show running-config, donde nos indica todo lo que hemos realizado en el dispositivo local

```
Guayaquil#sh running-config
Building configuration...

Current configuration : 431 bytes
!
version 12.2
no service password-encryption
!
hostname Guayaquil
!
!
```

```
!
username Quito password 0 wan
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 192.188.53.65 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.188.53.98 255.255.255.224
 encapsulation ppp
 ppp authentication chap
!
router rip
 network 192.188.53.0
!
ip classless
!
!
!
line con 0
line vty 0 4
 login
!
!
Guayaquil#
```

7.3. Análisis de resultados

7.3.1. Hacemos ping a una estación de trabajo vía command prompt

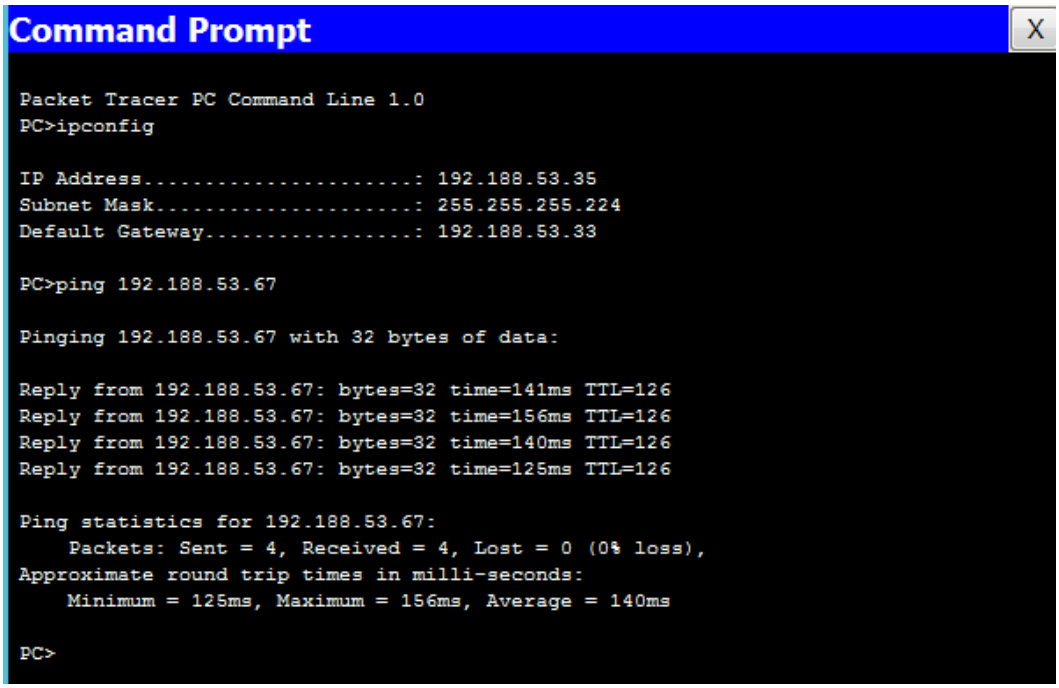

Figura 7.3.1.1

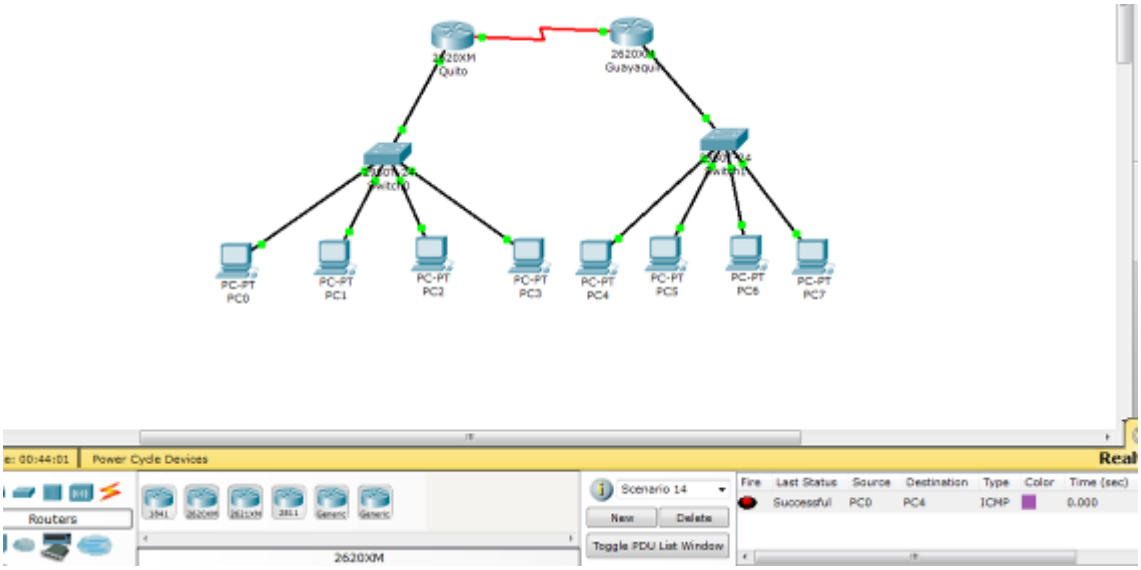

Figura 7.3.1.2

7.4. Análisis de resultados

- Se puede observar en la simulación que podemos hacer ping desde la PC0 hasta la PC4
- Al realizar la simulación de la red se debe tener muy en cuenta que todos routers estén configurados debidamente el enrutamiento y la autentificación caso contrario no se podrían enviar ninguna información.

7.5. Conclusiones

- Las gráficas de la simulación permitieron observar que los paquetes se trasladaron sin ningún problema por la red
- Con la simulación realizada se cumplieron los objetivos requeridos
- Se observo que se demoro 30s en converger la red ya que se encuentra configurado RIP

7.6. Recomendaciones

- Para estos tipos de redes es recomendable efectuar la configuración LAN y por ultimo hacer la configuración WAN ya que pueden tener problemas de conectividad
- Para la autentificación es preferible usar el nombre del ruteador al cual se quiere hacer el enlace ya que puede haber problemas de nombre o de password

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

8. Guía de práctica: Completar la actividad realizando encapsulamiento PPP con autentificación CHAP

8.1. Objetivo

- Completar la actividad realizando encapsulamiento PPP con autentificación CHAP

8.2. Procedimiento

8.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[7]

8.2.2. Realizamos la topología de red como se muestra en la figura 8.2.2.1

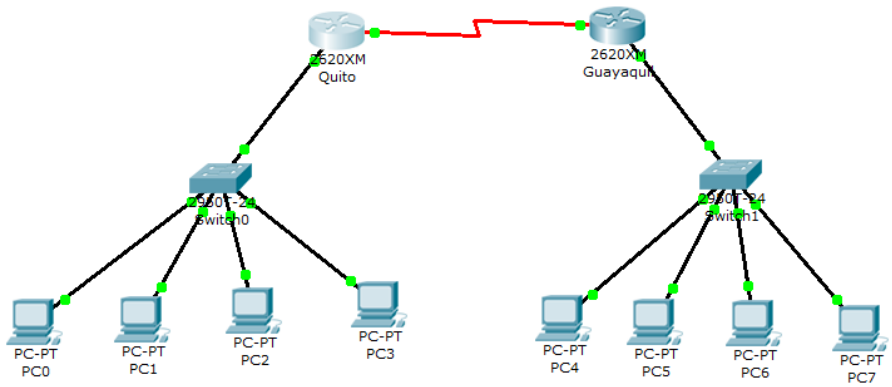

Figura 8.2.2.1

8.2.3. Abrimos un nuevo documento Packet Tracer y abrimos un Activity Wizard, tendríamos una pantalla como se muestra en la figura.

Figura 8.2.3.1

8.2.4. Nos muestra una pantalla de lo que significa una ACTIVIDAD y todos los pasos que debemos seguir para la creación, en la parte de Instrucciones tenemos que digitar cual es el procedimiento de la actividad, tal como se muestra en la figura.

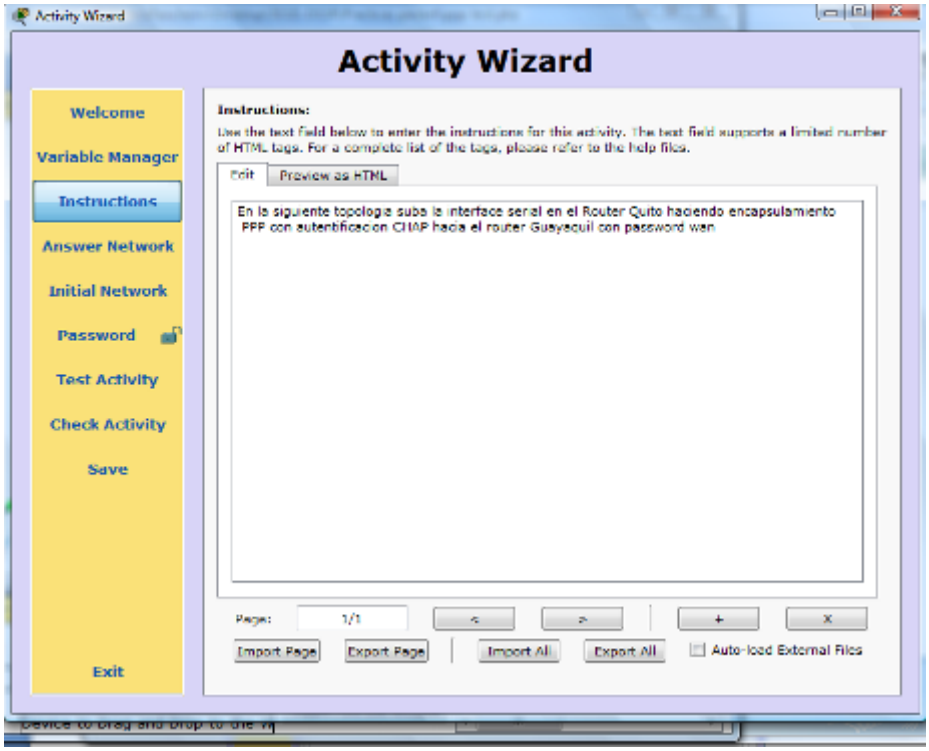

Figura 8.2.4.1

8.2.5. En el siguiente paso Answer Network, creamos la red respuesta pero en este caso importamos la red ya que fue creada anteriormente, en cual solo procedemos activar al Router Quito ya que ahí se va a realizar la actividad.

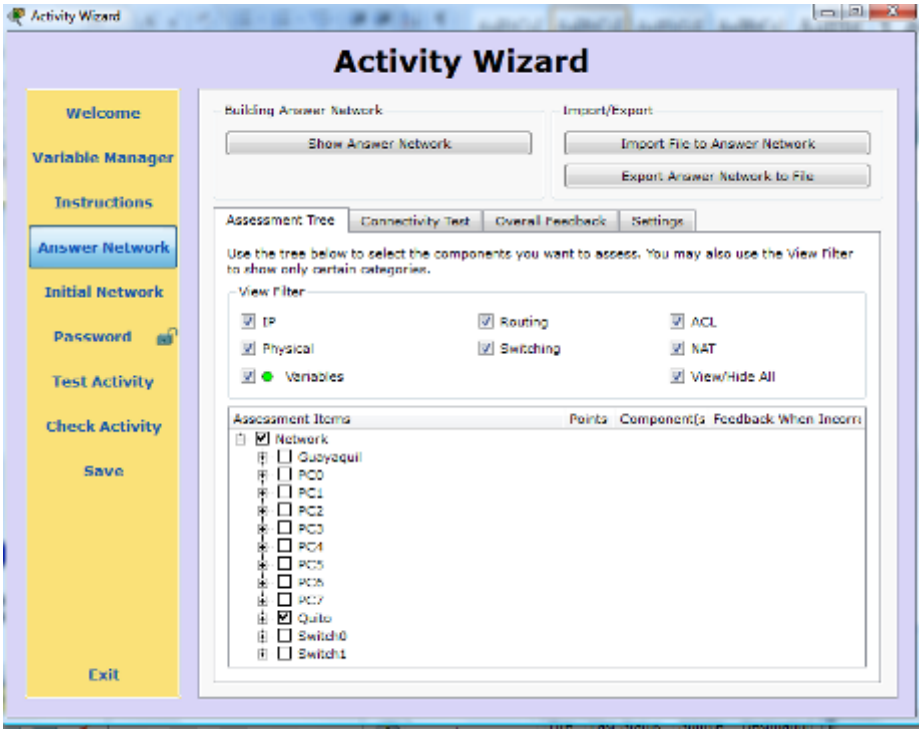

Figura 8.2.5.1

8.2.6. Otra pestaña importante que debemos tener en cuenta es la parte de Overall Feedback, ya que aquí digitamos los mensajes una vez concluida la activad.

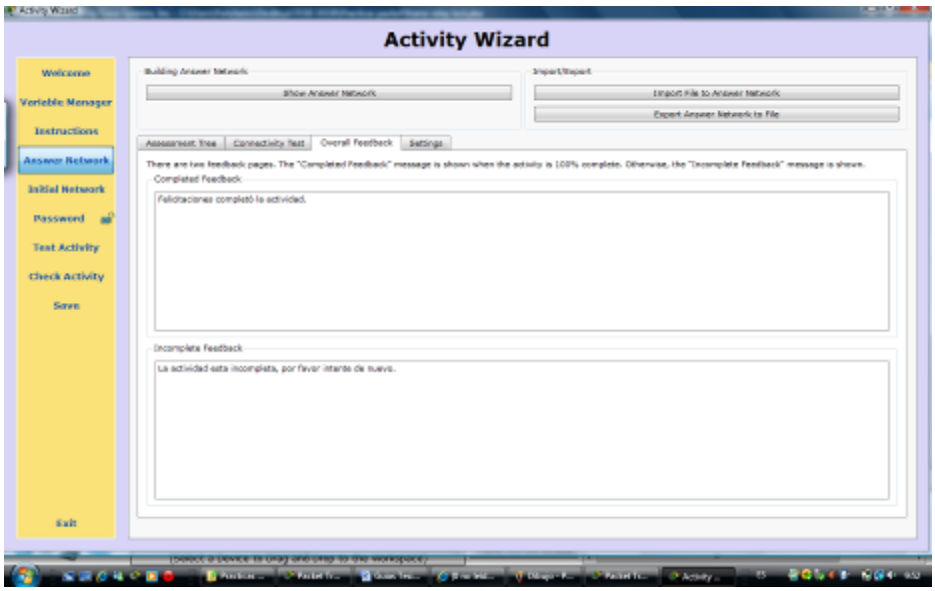

Figura 8.2.6.1

8.2.7. En el siguiente paso Inicial Network, creamos la red inicial pero en este caso importamos la red, que se deberá crear el respectivo encapsulamiento.

Figura 8.2.7.1

8.2.8. Y para completar la actividad SAVE, le grabamos como ppt test.

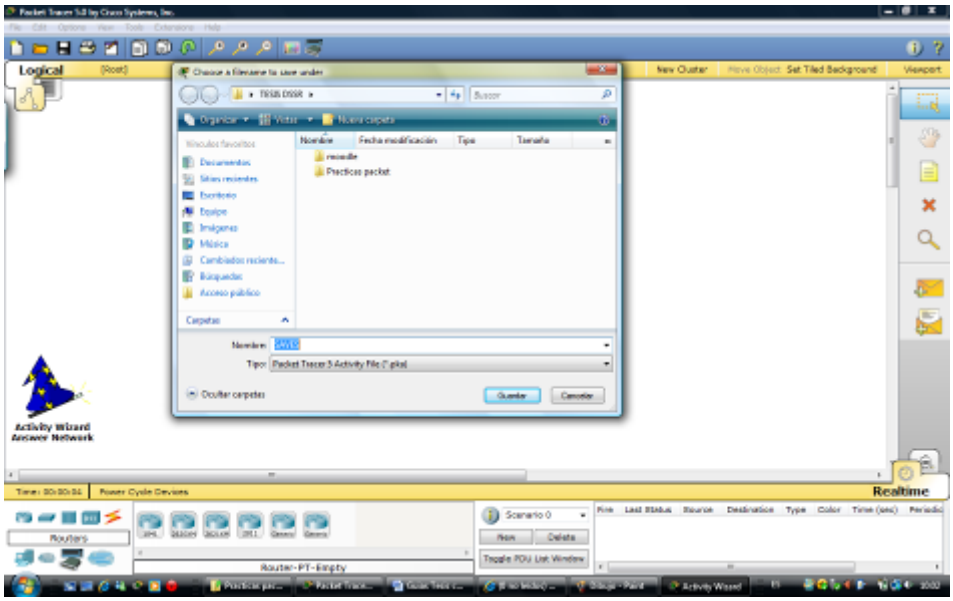

Figura 8.2.8.1

8.2.9. Una vez grabado abrimos el archivo "ppp test.pka", y nos muestra la siguiente pantalla.

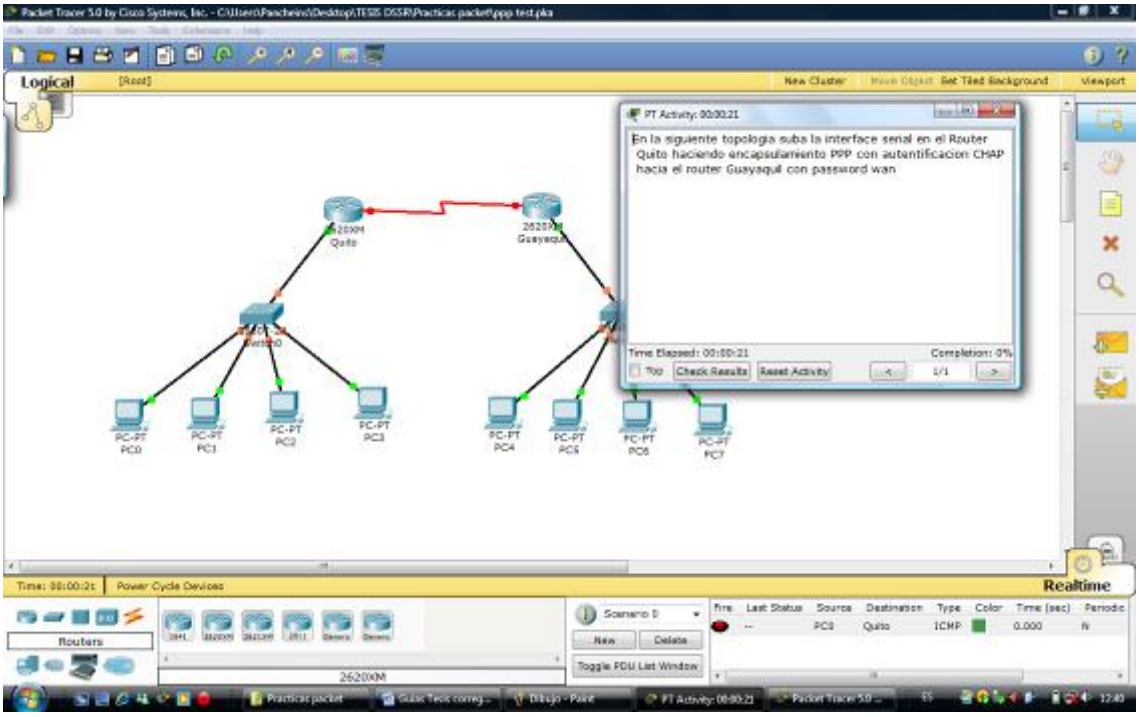

Figura 8.2.9.1

8.2.10. Con el fin de verificar los mensajes si la actividad está completa hacemos click donde dice Check Result

Figura 8.2.10.1

8.2.11. Como siguiente damos click Reset Activity, o ponemos OK

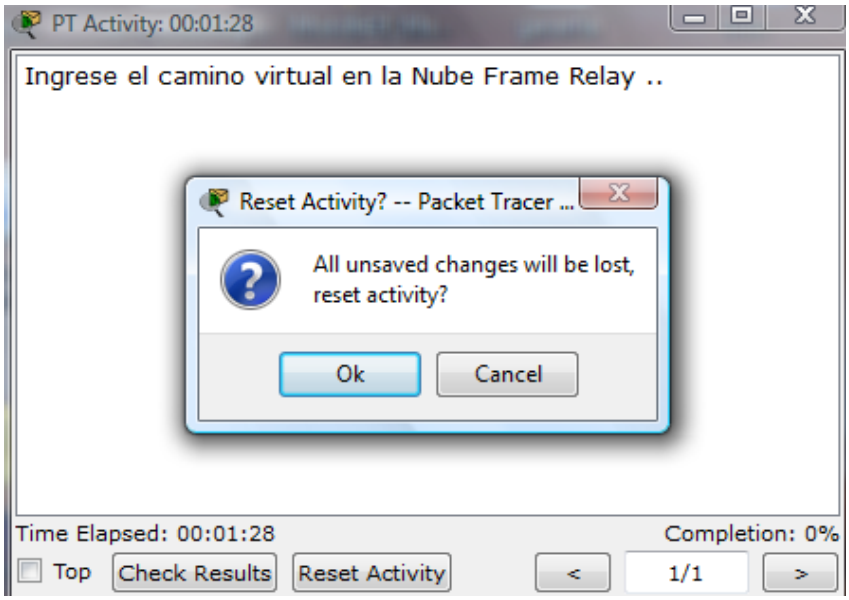

Figura 8.2.11.1

8.2.12. En este paso nos dirigimos a la configuración del router Quito, y tal como se muestra en la figura.

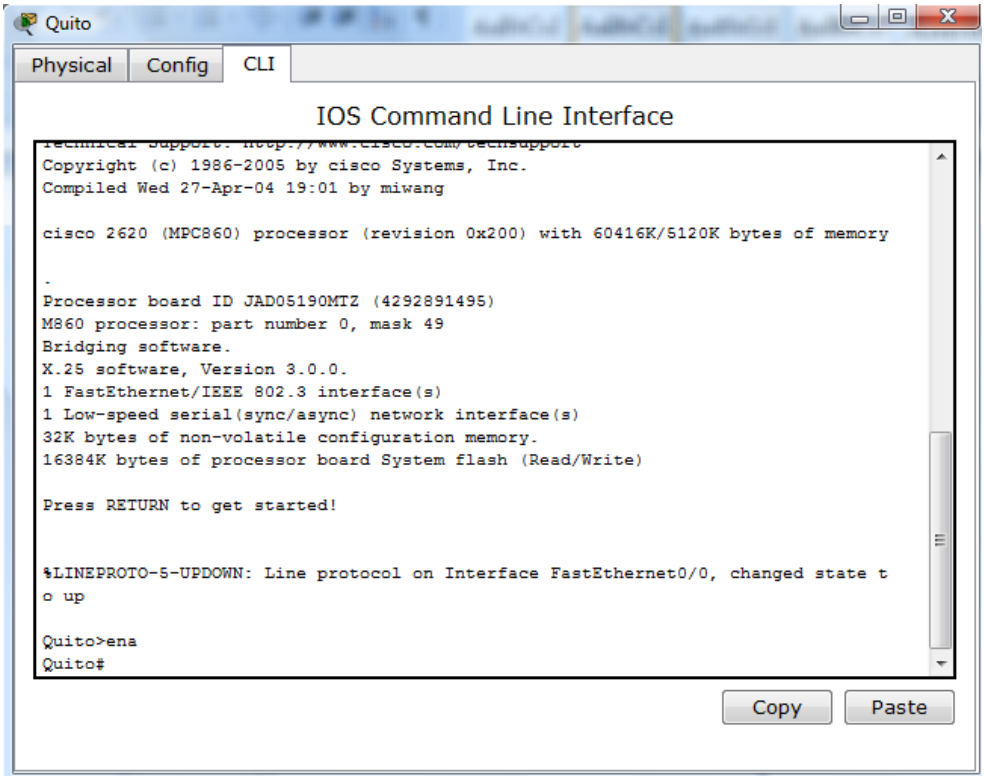

Figura 8.2.12.1

8.2.12.1. Entonces procedemos a la configuración del router Quito, con su respectivo encapsulamiento y autentificación

Quito#conf t
Quito(config-if)#encapsulation ppp
Quito(config-if)#ppp authentication chap
Quito(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Quito(config-if)#exit
Quito(config)#username Guayaquil password wan
Quito(config)#

8.2.12.2. Posteriormente damos tiempo hasta que la red converja totalmente probamos conectividad entre los dispositivos, y posteriormente damos click en Check Result, y finalmente nos

muestra una pantalla que la actividad se completo satisfactoriamente.

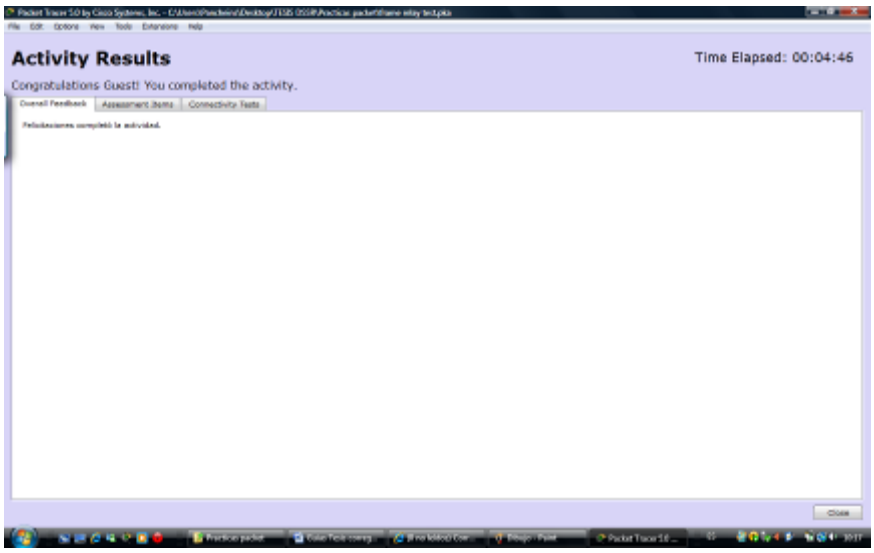

Figura 8.2.12.2.1

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

9. Guía de práctica: Realizar una red utilizando enrutamiento dinámico OSPF

9.1. Objetivo

Realizar una red utilizando el protocolo de enrutamiento OSPF

9.2. Procedimiento

9.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[8]

9.2.2. Realizamos la topología de red como se muestra en la figura en cual estamos utilizando ruteadores modelo 2620 y Switch 2950

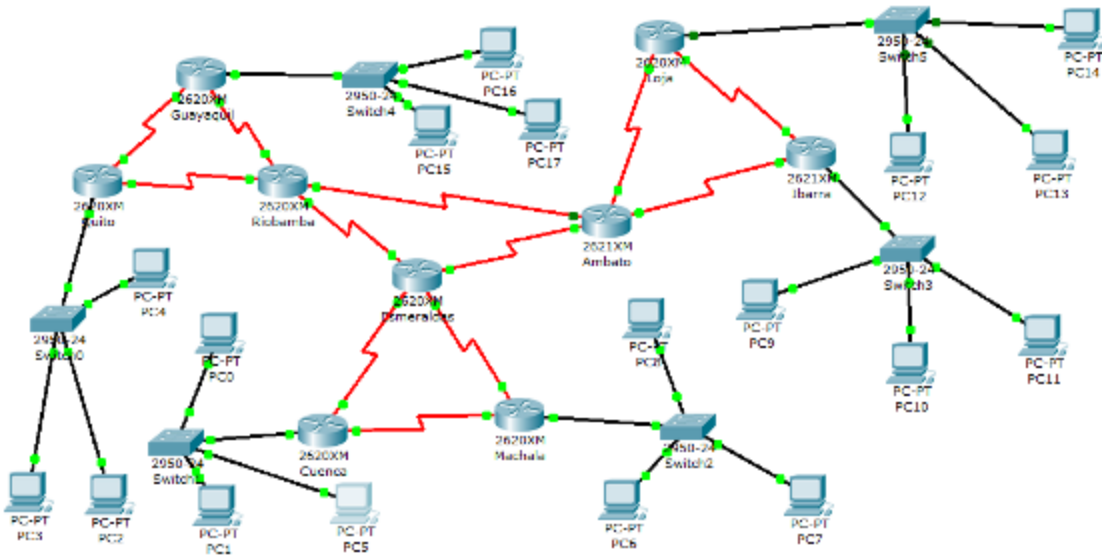

Figura 9.2.2.1

9.2.3. Debemos configurar la dirección IP y su respectiva mascara de red para todas las CPU´s conectadas en la red con la siguiente dirección 192.168.1.0/29, para ello procedemos a dar un clic en cada una de las CPU´s de la red, para lo cual se abre una pantalla de configuración como se puede observar en la figura

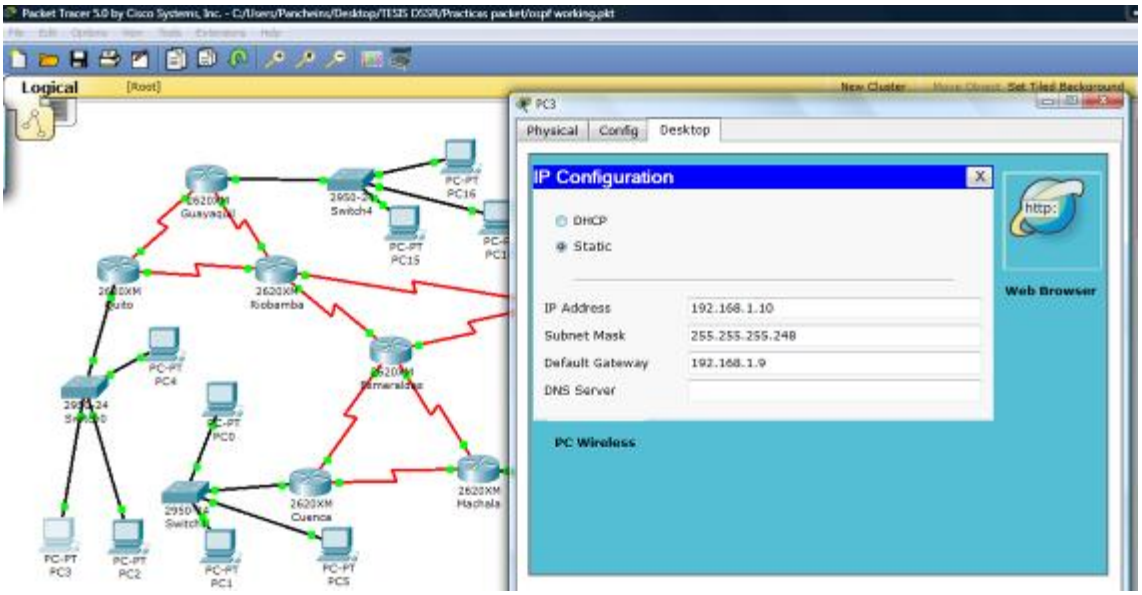

Figura9.2.3.1 Edit CPU's

9.2.4. En la pantalla que aparece nos debemos dirigir a la pestaña con el nombre de desktop, y luego en IP configuration en la cual procedemos con la configuración de nuestra dirección IP con el respectivo Gateway para poder acceder a otras redes y nuestra mascara de red como se observa en la figura

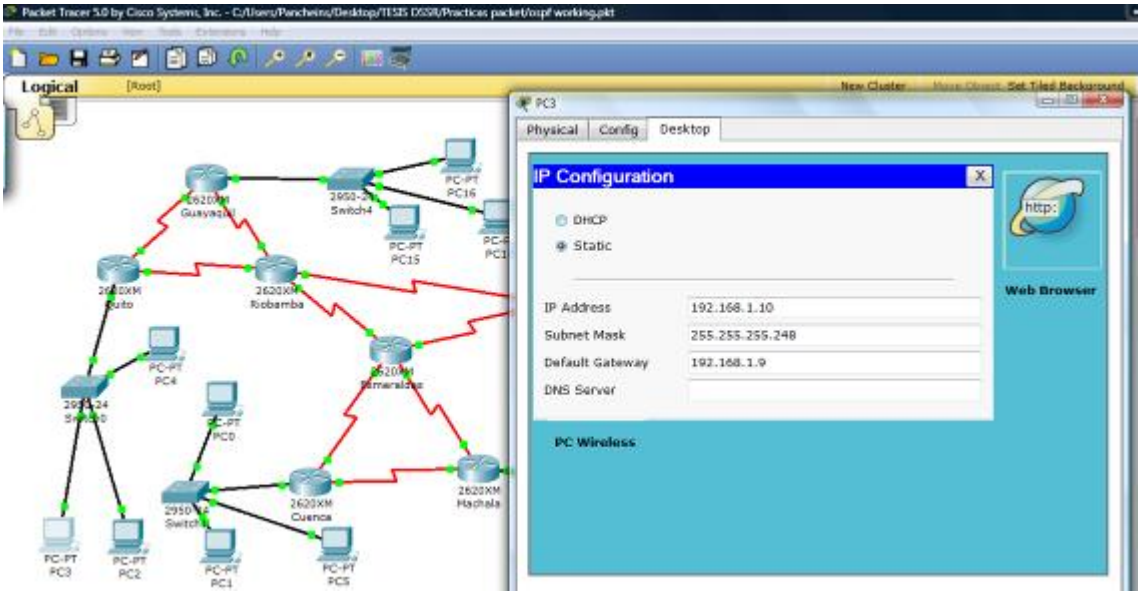

Figura 9.2.4.1 CPU's

9.2.5. Se distribuye las direcciones de red lo mas convenientemente posible para cada una de las estaciones de trabajo.

9.2.6. Para realizar la configuración de los ruteadores es importante indicar que debemos insertar la tarjeta WIC 1T como se muestra en la figura para este procedimiento el ruteador se debe encontrar apagado y encenderlo posteriormente

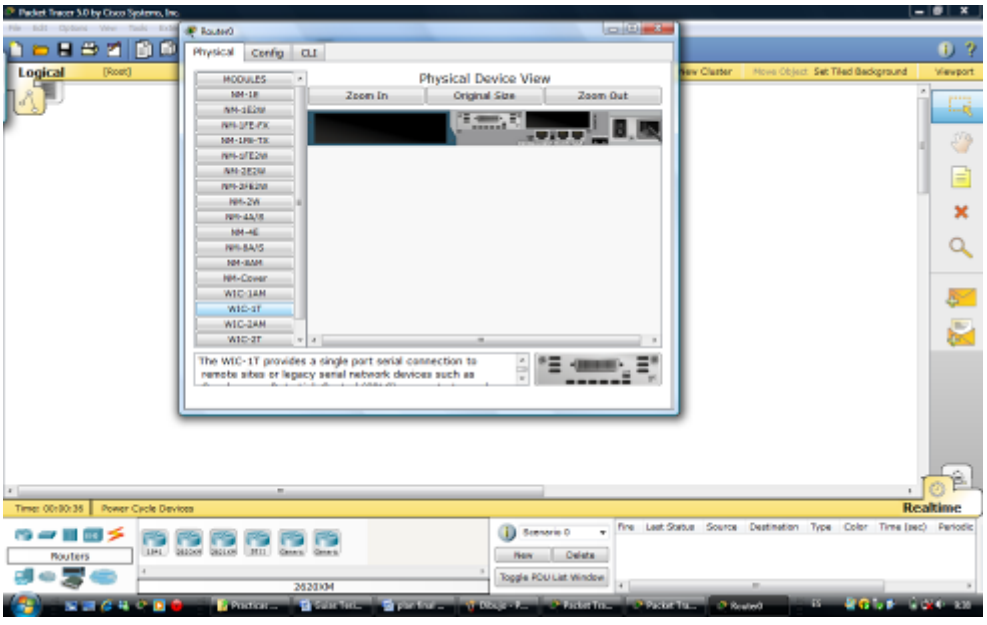

Figura 9.2.6.1 Interfaz Serial

9.2.7. Procedemos con la configuración del Ruteador Quito con el cual utilizaremos el modelo 2620XM.

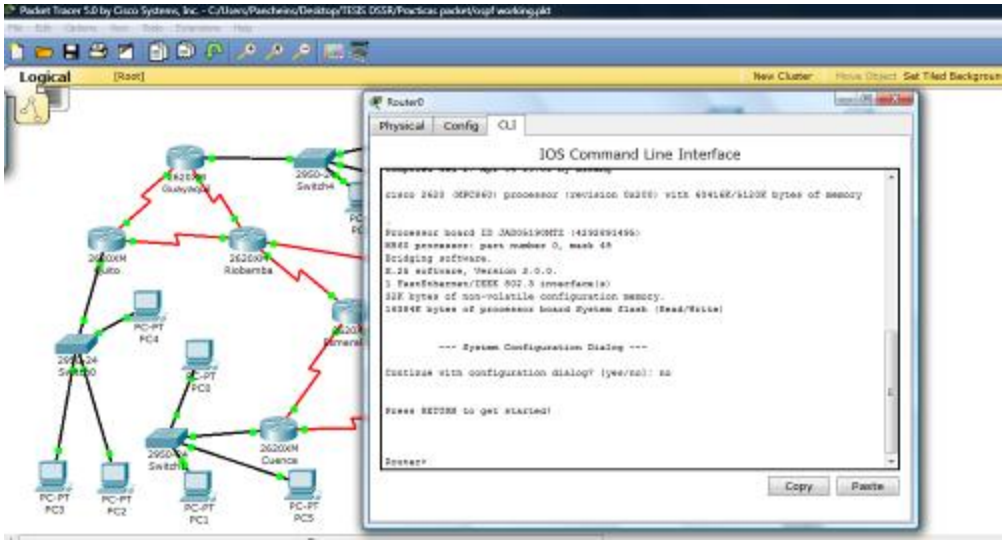

Figura 9.2.7.1

9.2.7.1. Ponemos nombre al ruteador

```
Router>enable
Router#conf t
Router(config)#hostname Quito
```

9.2.7.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

```
Quito(config)#int f0/0
Quito(config-if)#ip address 192.168.1.9 255.255.255.248
Quito(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Quito(config-if)#exit
```

9.2.7.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

Quito(config)#int s0/0
Quito(config-if)#ip address 192.168.1.58 255.255.255.248
Quito(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Quito(config-if)# exit

Quito(config)#int s0/1
Quito(config-if)#ip address 192.168.1.65 255.255.255.248
Quito(config-if)#clock rate 56000
Quito(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Quito(config-if)# exit

9.2.7.4. Configuramos las rutas dinámicas en el equipo local

Quito(config)#router ospf 1
Quito(config-router)# network 192.168.1.8 0.0.0.7 area 0
Quito(config-router)# network 192.168.1.56 0.0.0.7 area 0
Quito(config-router)# network 192.168.1.64 0.0.0.7 area 0
Quito#wr
Building configuration...
[OK]
Quito#

9.2.8. Procedemos con la configuración del Ruteador Guayaquil con el cual utilizaremos el modelo 2620XM, con interfaces seriales

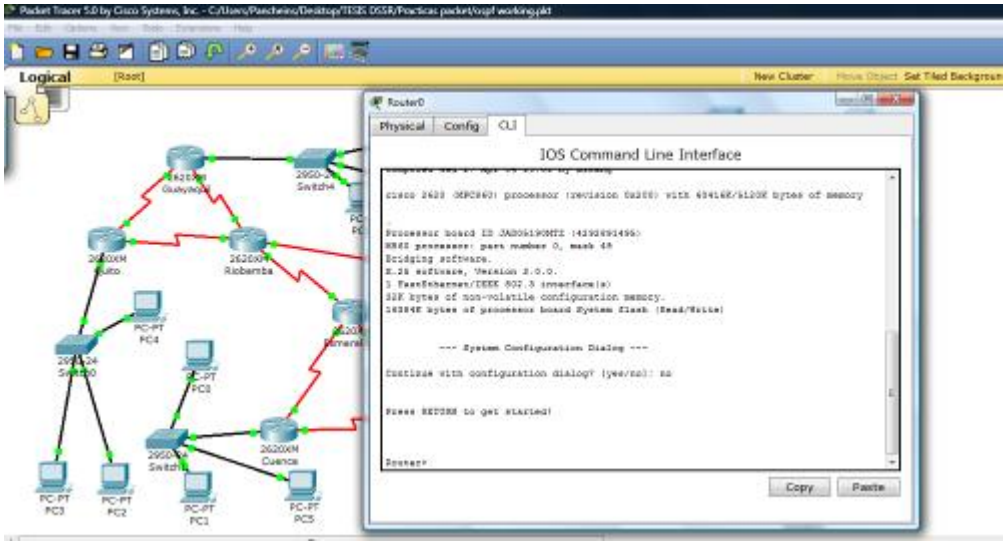

Figura 9.2.8.1

9.2.8.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Guayaquil

9.2.8.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Guayaquil(config)#int f0/0
Guayaquil(config-if)#ip address 192.168.1.17 255.255.255.248
Guayaquil(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Guayaquil(config-if)#exit

9.2.8.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

Guayaquil(config)#int s0/0
Guayaquil(config-if)#ip address 192.168.1.57 255.255.255.248

Guayaquil(config-if)#clock rate 56000

Guayaquil(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0, changed state to up

Guayaquil(config-if)# exit

Guayaquil(config)#int s0/1

Guayaquil(config-if)#ip address 192.168.1.73 255.255.255.248

Guayaquil(config-if)#clock rate 56000

Guayaquil(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1, changed state to up

Guayaquil(config-if)# exit

4. Configuramos las rutas dinámicas en el equipo local

Guayaquil(config)#router ospf 1

Guayaquil(config-router)# network 192.168.1.16 0.0.0.7 area 0

Guayaquil(config-router)# network 192.168.1.56 0.0.0.7 area 0

Guayaquil(config-router)#network 192.168.1.72 0.0.0.7 area 0

Guayaquil#

9.2.9. Procedemos con la configuración del Ruteador Riobamba con el cual utilizaremos el modelo 2620XM, con interfaces seriales

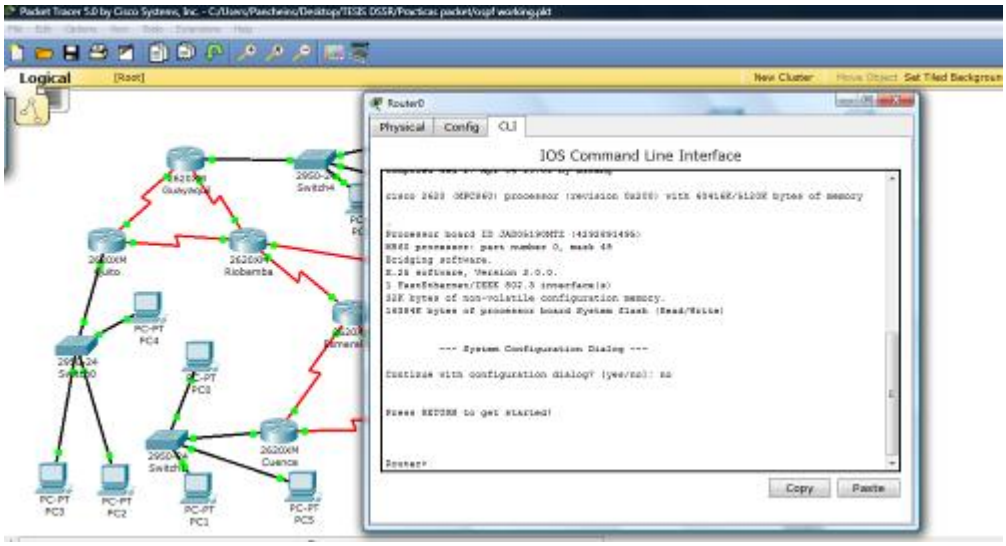

Figura 9.2.9.1

9.2.9.1. Ponemos nombre al ruteador

```
Router>enable
Router#conf t
Router(config)#hostname Riobamba
```

9.2.9.2. Ingresamos a la interfaz Serial ponemos la ip que va a utilizar nuestra red

```
Riobamba(config)#int s0/0
Riobamba(config-if)#ip address 192.168.1.74 255.255.255.248
Riobamba(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Riobamba(config-if)# exit

Riobamba (config)#int s0/1
Riobamba (config-if)#ip address 192.168.1.66 255.255.255.248
Riobamba (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Riobamba (config-if)# exit

Riobamba(config)#int s1/0
Riobamba(config-if)#ip address 192.168.1.81 255.255.255.248
Riobamba(config)#clock rate 56000
Riobamba(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to up
Riobamba(config-if)# exit

Riobamba(config)#int s1/1
Riobamba(config-if)#ip address 192.168.1.89 255.255.255.248
```

Riobamba(config)#clock rate 56000

Riobamba(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial1/1, changed state to up

Riobamba(config-if)# exit

9.2.9.3. Configuramos las rutas dinámicas en el equipo local

Riobamba(config)#router ospf 1

Riobamba(config-router)# network 192.168.1.64 0.0.0.7 area 0

Riobamba(config-router)# network 192.168.1.80 0.0.0.7 area 0

Riobamba(config-router)# network 192.168.1.88 0.0.0.7 area 0

Riobamba(config-router)#network 192.168.1.72 0.0.0.7 area 0

Riobamba#

9.2.10. Procedemos con la configuración del Ruteador Esmeraldas con el cual utilizaremos el modelo 2620XM, con interfaces seriales adicionales

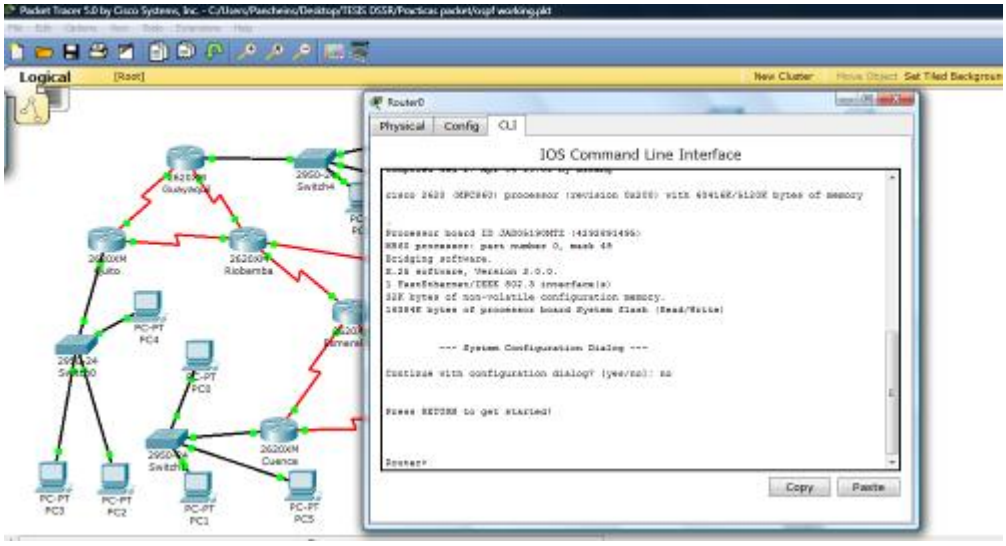

Figura 9.2.10.1

9.2.10.1. Ponemos nombre al ruteador

```
Router>enable
Router#conf t
Router(config)#hostname Esmeraldas
```

9.2.10.2. 2. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

```
Esmeraldas(config)#int s0/0
Esmeraldas(config-if)#ip address 192.168.1.97 255.255.255.248
Esmeraldas(config)#clock rate 56000
Esmeraldas(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Esmeraldas(config-if)# exit

Esmeraldas(config)#int s0/1
Esmeraldas(config-if)#ip address 192.168.1.82 255.255.255.248
Esmeraldas(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Esmeraldas(config-if)# exit

Esmeraldas(config)#int s1/0
Esmeraldas(config-if)#ip address 192.168.1.105 255.255.255.248
Esmeraldas(config)#clock rate 56000
Esmeraldas(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to up
Esmeraldas(config-if)# exit

Esmeraldas(config)#int s1/1
Esmeraldas(config-if)#ip address 192.168.1.121 255.255.255.248
Esmeraldas(config)#clock rate 56000
Esmeraldas(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/1, changed state to up
```

Esmeraldas(config-if)# exit

9.2.10.3. Configuramos las rutas dinámicas en el equipo local

Esmeraldas(config)#router ospf 1
Esmeraldas(config-router)# network 192.168.1.96 0.0.0.7 area 0
Esmeraldas(config-router)# network 192.168.1.80 0.0.0.7 area 0
Esmeraldas(config-router)# network 192.168.1.104 0.0.0.7 area 0
Esmeraldas(config-router)#network 192.168.1.120 0.0.0.7 area 0
Esmeraldas #

9.2.11. Procedemos con la configuración del Ruteador Cuenca con el cual utilizaremos el modelo 2620XM.

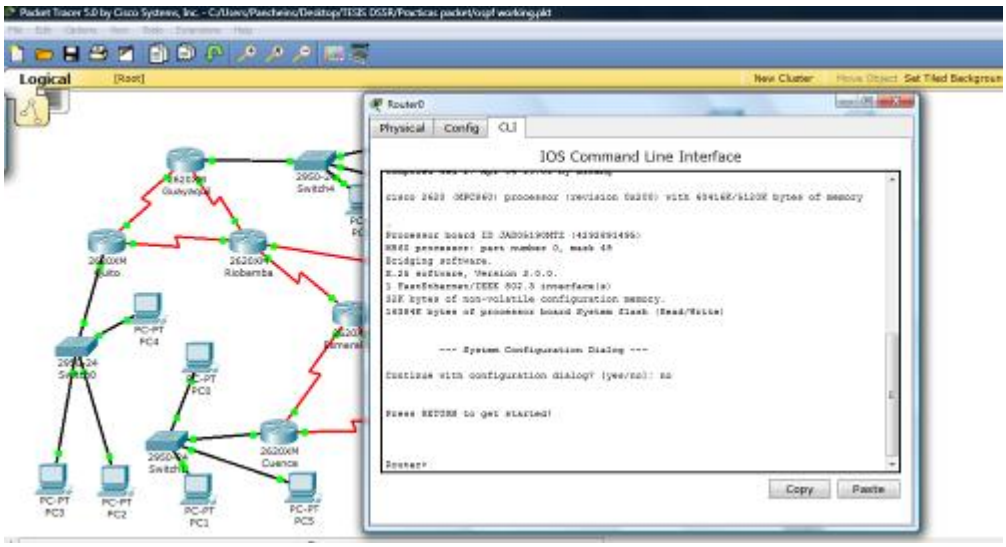

Figura 9.2.11.1

9.2.11.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Cuenca

9.2.11.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

```
Cuenca(config)#int f0/0
Cuenca(config-if)#ip address 192.168.1.25 255.255.255.248
Cuenca(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Cuenca(config-if)#exit
```

9.2.11.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

```
Cuenca(config)#int s0/0
Cuenca(config-if)#ip address 192.168.1.113 255.255.255.248
Cuenca(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Cuenca(config-if)# exit

Cuenca(config)#int s0/1
Cuenca(config-if)#ip address 192.168.1.106 255.255.255.248
Cuenca(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Cuenca(config-if)# exit
```

9.2.11.4. Configuramos las rutas dinámicas en el equipo local

```
Cuenca(config)#router ospf 1
Cuenca(config-router)# network 192.168.1.24 0.0.0.7 area 0
Cuenca(config-router)# network 192.168.1.104 0.0.0.7 area 0
Cuenca(config-router)# network 192.168.1.12 0.0.0.7 area 0
Cuenca#wr
```

9.2.12. Procedemos con la configuración del Ruteador Machala con el cual utilizaremos el modelo 2620XM.

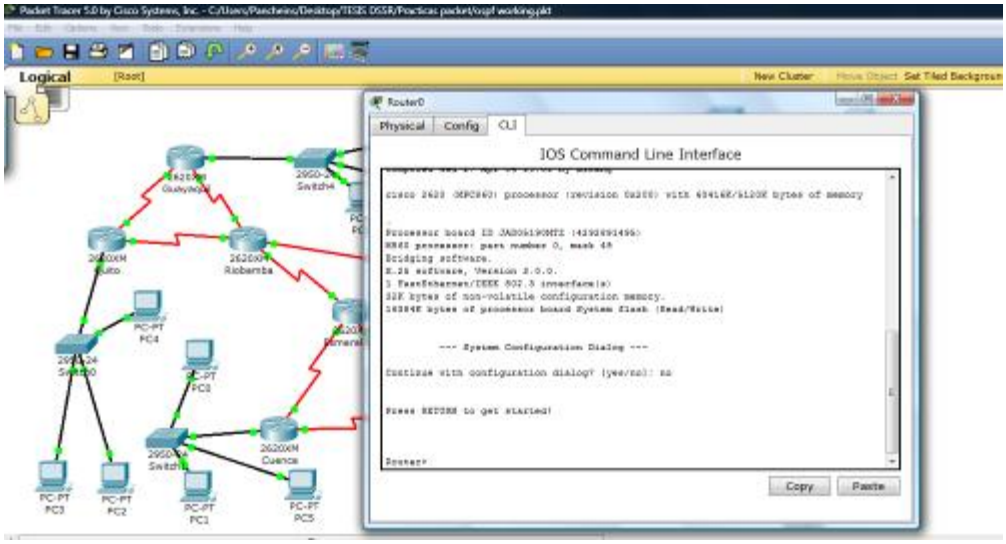

Figura 9.2.12.1

9.2.12.1. Ponemos nombre al ruteador

```
Router>enable
Router#conf t
Router(config)#hostname Machala
```

9.2.12.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

```
Machala(config)#int f0/0
Machala(config-if)#ip address 192.168.1.33 255.255.255.248
Machala(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Machala(config-if)#exit
```

9.2.12.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

```
Machala(config)#int s0/0
Machala(config-if)#ip address 192.168.1.114 255.255.255.248
Machala(config-if)#clock rate 56000
Machala(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Machala(config-if)# exit

Machala(config)#int s0/1
Machala(config-if)#ip address 192.168.1.122 255.255.255.248
Machala(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Machala(config-if)# exit
```

9.2.12.4. Configuramos las rutas dinámicas en el equipo local

```
Machala(config)#router ospf 1
Machala(config-router)# network 192.168.1.32 0.0.0.7 area 0
Machala(config-router)# network 192.168.1.20 0.0.0.7 area 0
Machala(config-router)# network 192.168.1.112 0.0.0.7 area 0
Machala#wr
```

9.2.13. Procedemos con la configuración del Ruteador Ambato con el cual utilizaremos el modelo 2620XM, con interfaces seriales adicionales

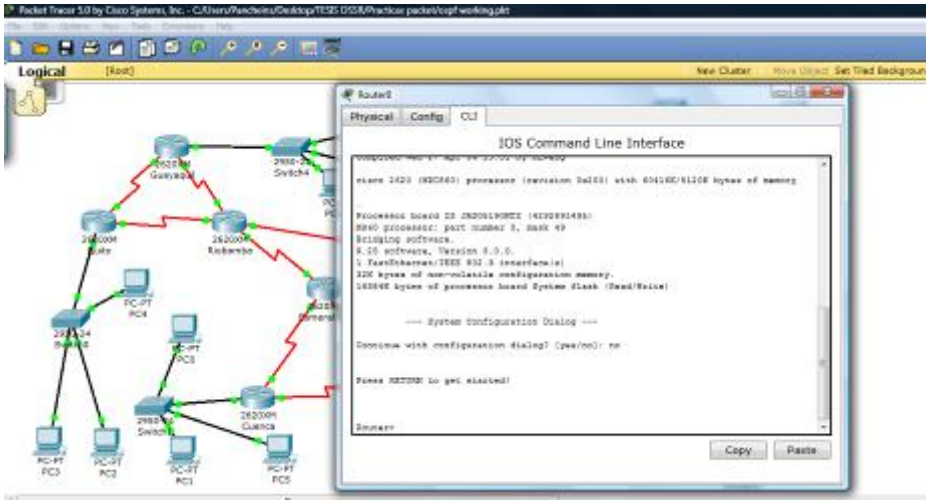

Figura 9.2.13.1

9.2.13.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Ambato

9.2.13.2. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

Ambato(config)#int s0/0
Ambato(config-if)#ip address 192.168.1.98 255.255.255.248
Ambato(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Ambato(config-if)# exit

Ambato(config)#int s0/1
Ambato(config-if)#ip address 192.168.1.90 255.255.255.248
Ambato(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Ambato(config-if)# exit

Ambato(config)#int s1/0
Ambato(config-if)#ip address 192.168.1.130 255.255.255.248
Ambato(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to up
Ambato(config-if)# exit

Ambato(config)#int s1/1
Ambato(config-if)#ip address 192.168.1.138 255.255.255.248
Ambato(config-if)#no shutdown

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

9.2.13.3. Configuramos las rutas dinámicas en el equipo local

Ambato(config)#router ospf 1
Ambato(config-router)# network 192.168.1.96 0.0.0.7 area 0
Ambato(config-router)# network 192.168.1.88 0.0.0.7 area 0
Ambato(config-router)# network 192.168.1.136 0.0.0.7 area 0
Ambato(config-router)#network 192.168.1.128 0.0.0.7 area 0
Ambato#

9.2.14. Procedemos con la configuración del Ruteador Loja con el cual utilizaremos el modelo 2620XM.

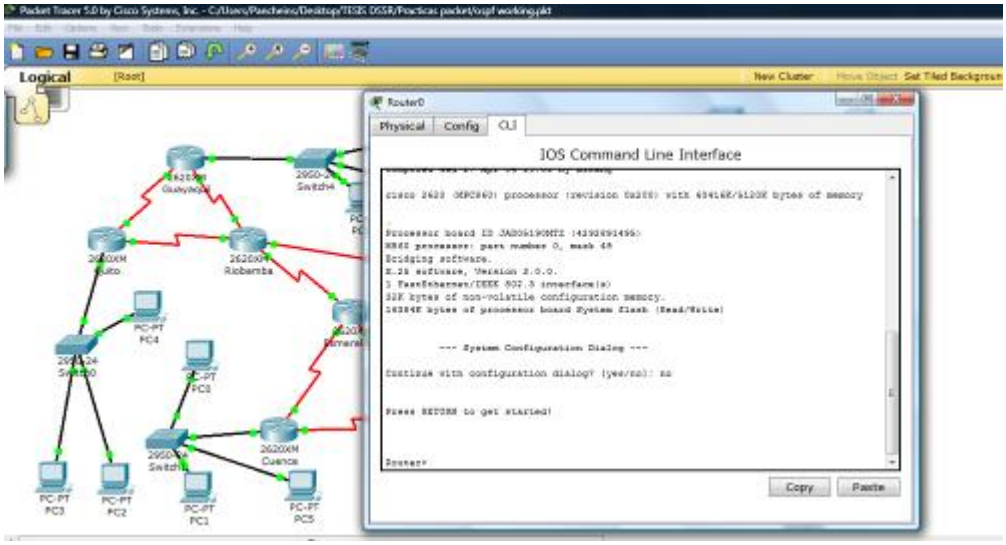

Figura 9.2.14.1

9.2.14.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Loja

9.2.14.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Loja(config)#int f0/0
Loja(config-if)#ip address 192.168.1.49 255.255.255.248
Loja(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Loja(config-if)#exit

9.2.14.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

Loja (config)#int s0/0
Loja (config-if)#ip address 192.168.1.145 255.255.255.248

Loja (config-if)#clock rate 56000
Loja (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Loja (config-if)# exit

Loja(config)#int s0/1
Loja(config-if)#ip address 192.168.1.129 255.255.255.248
Loja(config-if)#clock rate 56000
Loja(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Loja(config-if)# exit

9.2.14.4. Configuramos las rutas dinámicas en el equipo local

Loja (config)#router ospf 1
Loja (config-router)# network 192.168.1.48 0.0.0.7 area 0
Loja (config-router)# network 192.168.1.144 0.0.0.7 area 0
Loja (config-router)# network 192.168.1.128 0.0.0.7 area 0
Loja #wr

9.2.15. Procedemos con la configuración del Ruteador Ibarra con el cual utilizaremos el modelo 2620XM.

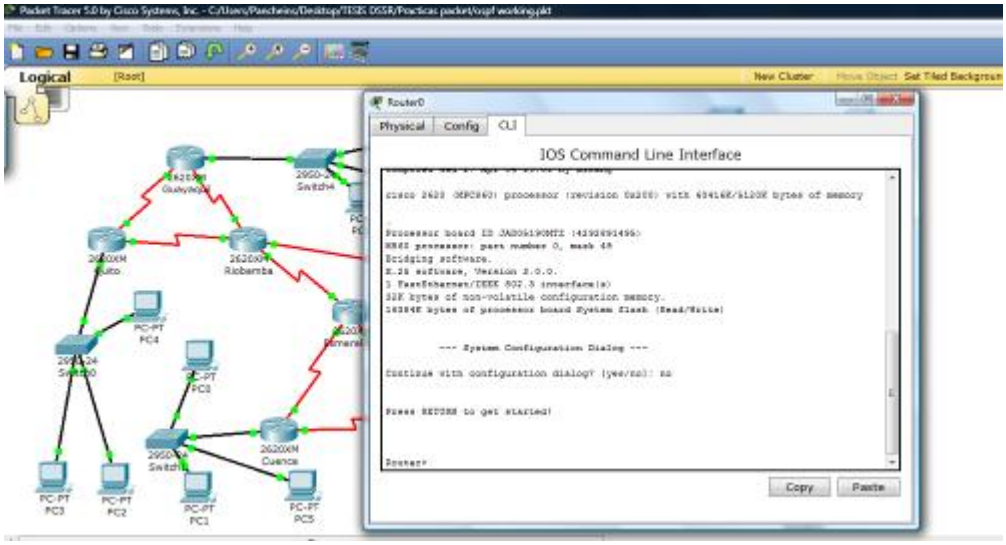

Figura 9.2.15.1

9.2.15.1. Ponemos nombre al ruteador

Router>enable
Router#conf t
Router(config)#hostname Ibarra

9.2.15.2. Ingresamos a la interfaz Fast Ethernet y ponemos la ip correspondiente

Ibarra (config)#int f0/0
Ibarra (config-if)#ip address 192.168.1.41 255.255.255.248
Ibarra (config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Ibarra (config-if)#exit

9.2.15.3. Ingresamos a la interfaz Serial ponemos la ip correspondiente que va a utilizar nuestra red

Ibarra(config)#int s0/0
Ibarra(config-if)#ip address 192.168.1.137 255.255.255.248

Ibarra(config-if)#clock rate 56000
Ibarra(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
Ibarra(config-if)# exit

Ibarra(config)#int s0/1
Ibarra(config-if)#ip address 192.168.1.146 255.255.255.248
Ibarra(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
Ibarra(config-if)#exit

9.2.15.4. Configuramos las rutas dinámicas en el equipo local

Ibarra(config)#router ospf 1
Ibarra(config-router)# network 192.168.1.40 0.0.0.7 area 0
Ibarra(config-router)# network 192.168.1.136 0.0.0.7 area 0
Ibarra(config-router)# network 192.168.1.144 0.0.0.7 area 0
Ibarra#wr

9.3. Análisis de resultados

9.3.1. Hacemos ping a una estación de trabajo vía command prompt

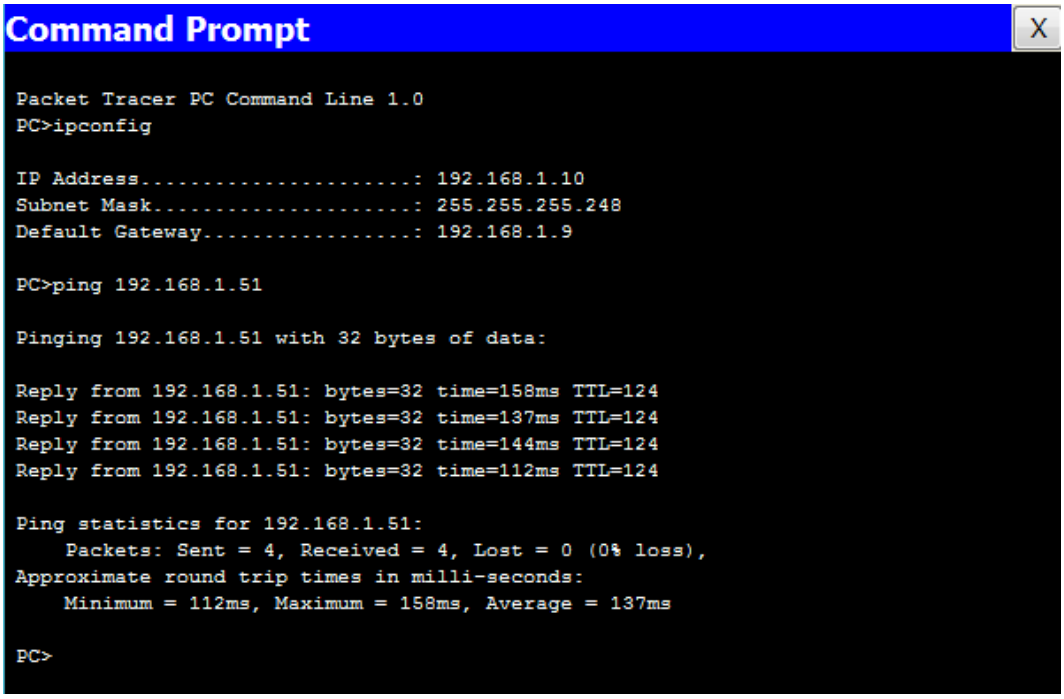

Figura 9.3.1.1

9.4. Análisis de resultados

- Se puede observar en la simulación que podemos hacer ping desde la PC3 hasta la PC14
- Al realizar la simulación de la red se debe tener muy en cuenta que todos routers estén configurados debidamente el enrutamiento y la autentificación caso contrario no se podrían enviar ninguna información.

9.5. Conclusiones

- Las gráficas de la simulación permitieron observar que los paquetes se trasladaron sin ningún problema por la red
- Con la simulación realizada se cumplieron los objetivos requeridos
- Se observo que se demoro en converger la red ya que se encuentra configurado con OSPF

9.6. Recomendaciones

- Como recomendación al hacer estos tipos de redes es tener las direcciones de red bien claras al rato de la configuración
- Es importante recalcar que se debe configurar primero todo lo que son enlaces lan y posteriormente con los enlaces wan
- Es recomendable tener un mapa de direcciones para equivocarse al rato de saber si los equipos son DTE o DCE

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

10. Guía de práctica: Completar la actividad realizando enrutamiento OSPF

10.1. Objetivo

- Completar la actividad realizando enrutamiento OSPF

10.2. Procedimiento

10.2.1. Iniciar con el software Packet Tracer 5.0. Como se indica en la figura 1.2.1.1[9]

10.2.2. Realizamos la topología de red como se muestra en la figura 10.2.2.1

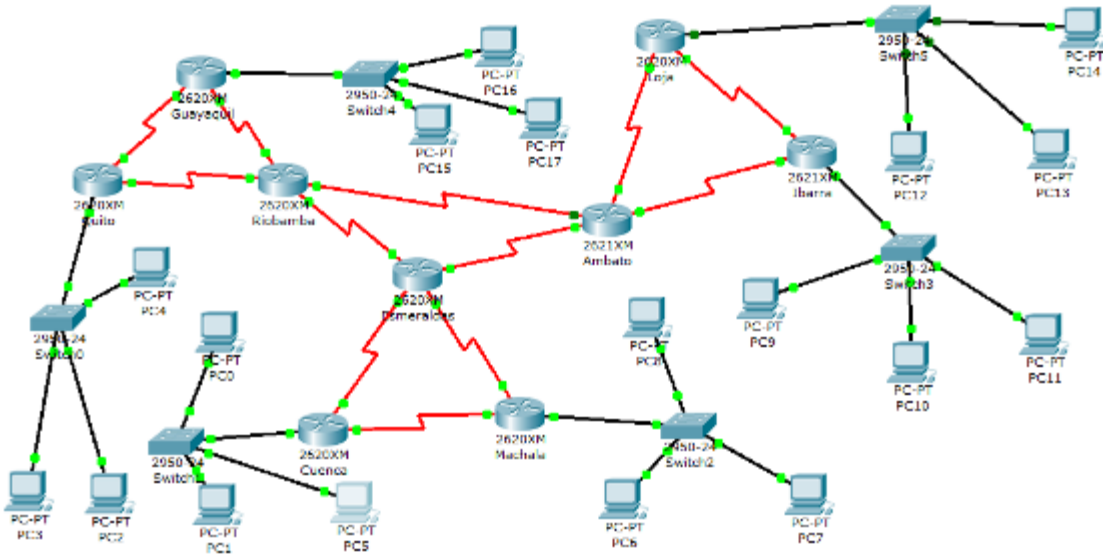

Figura 10.2.2.1

10.2.3. Abrimos un nuevo documento Packet Tracer y abrimos un Activity Wizard, tendríamos una pantalla como se muestra en la figura.

Figura 10.2.3.1

10.2.4. Nos muestra una pantalla de lo que significa una ACTIVIDAD y todos los pasos que debemos seguir para la creación, en la parte de Instrucciones tenemos que digitar cual es el procedimiento de la actividad, tal como se muestra en la figura.

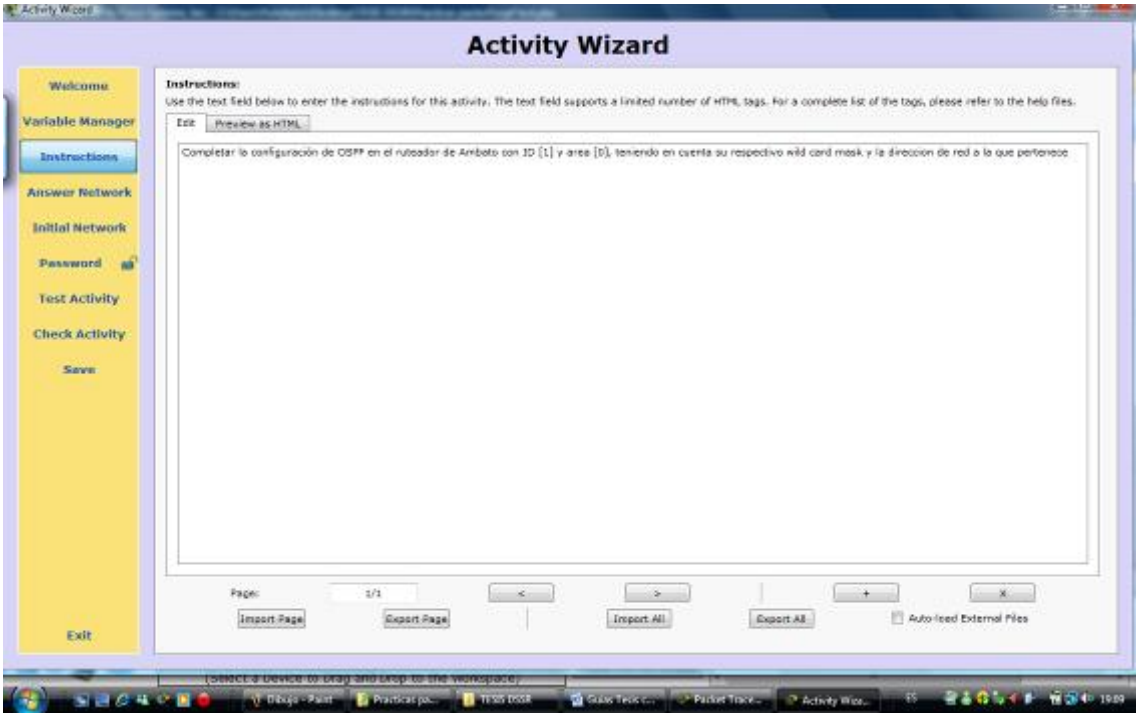

Figura 10.2.4.1

10.2.5. En el siguiente paso Answer Network, creamos la red respuesta pero en este caso importamos la red ya que fue creada anteriormente, se bloquea todos los dispositivos y en cual solo procedemos activar al Router Ambato ya que ahí se va a realizar la actividad.

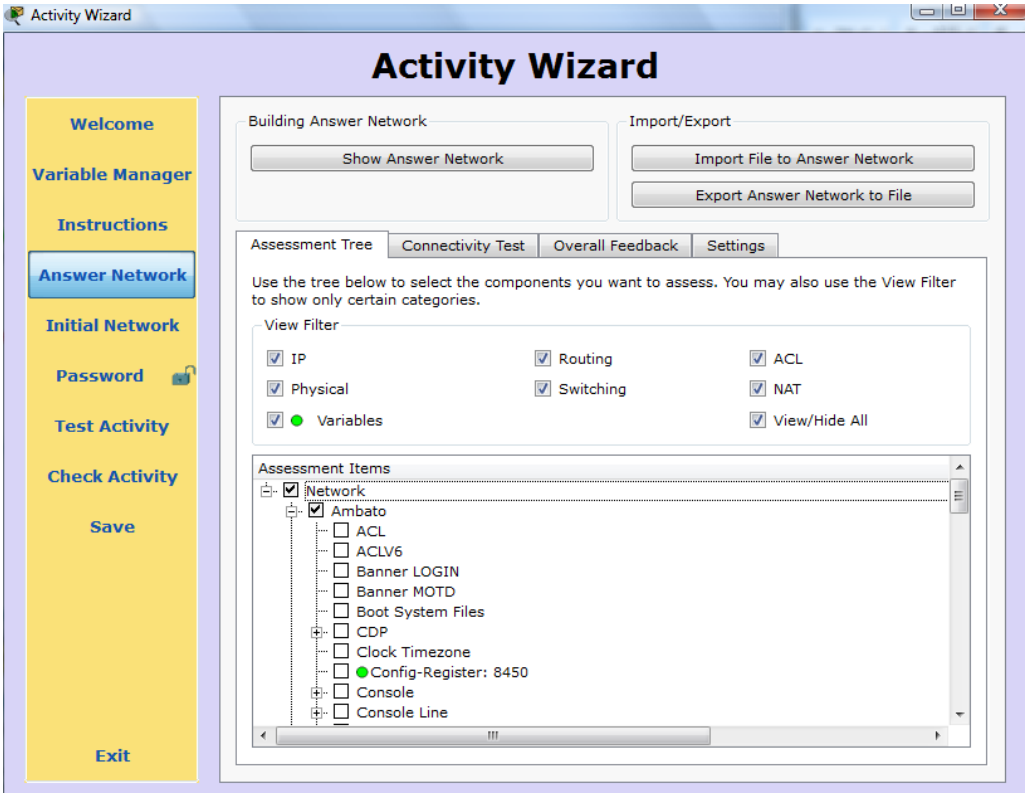

Figura 10.2.5.1

10.2.6. En parte de Overall Feedback se nos despliega dos cuadros, y que aquí digitamos los mensajes una vez concluida o no la activad.

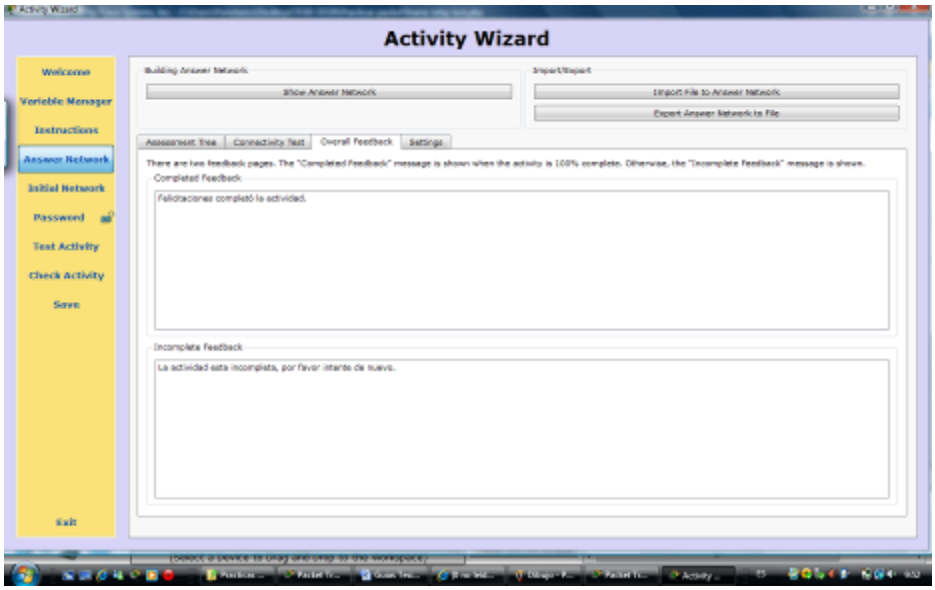

Figura 10.2.6.1

10.2.7. En el siguiente paso Inicial Network, creamos la red inicial pero en este caso importamos la red, que se deberá crear la respectiva actividad.

Figura 10.2.7.1

10.2.8. Y para completar la actividad SAVE, le grabamos como ospf test.

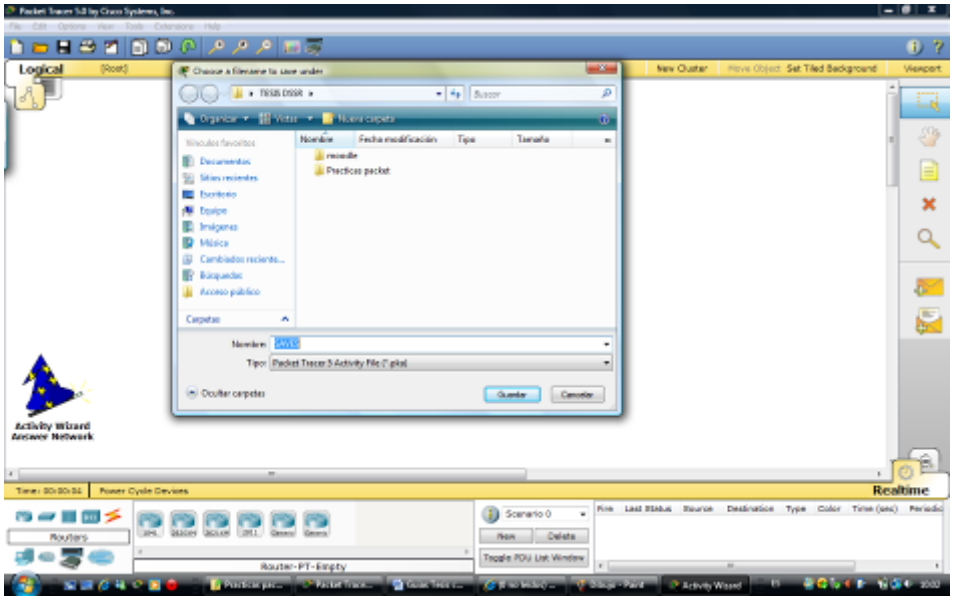

Figura 10.2.8.1

10.2.9. Una vez grabado abrimos el archivo "ospf test.pka", y nos muestra la siguiente pantalla.

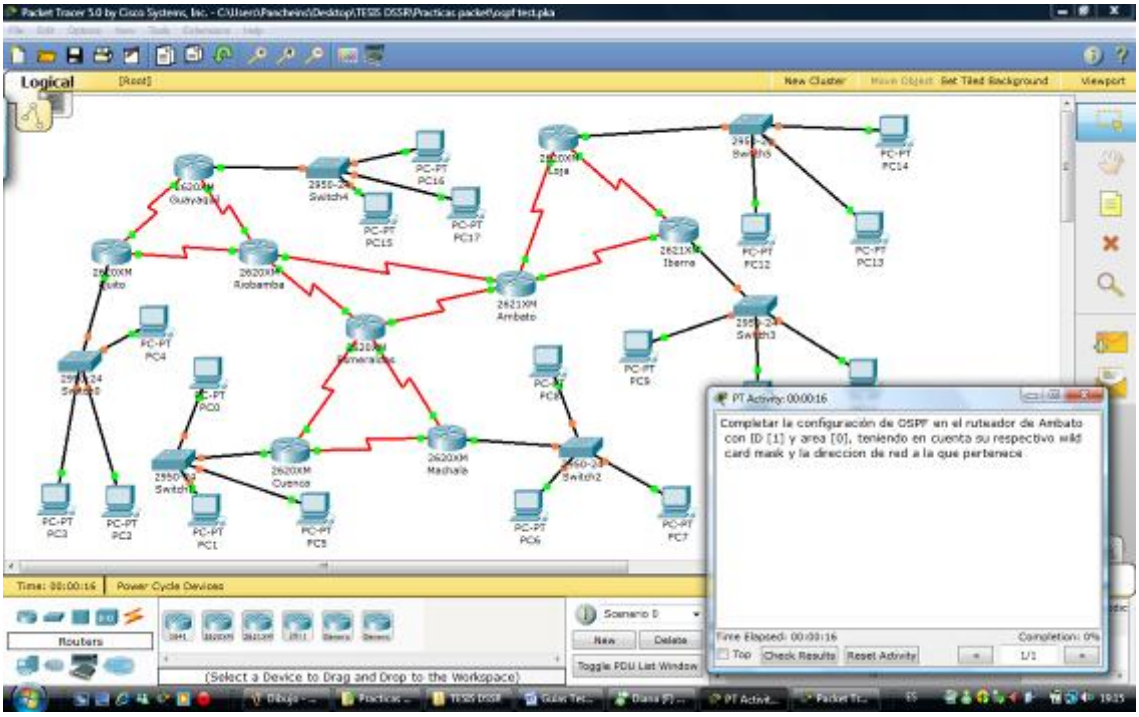

Figura 10.2.10.1

10.2.10. Con el fin de verificar los mensajes si la actividad está completa hacemos click donde dice Check Result

Figura 10.2.10.1

10.2.11. Como siguiente damos click Reset Activity, o ponemos OK

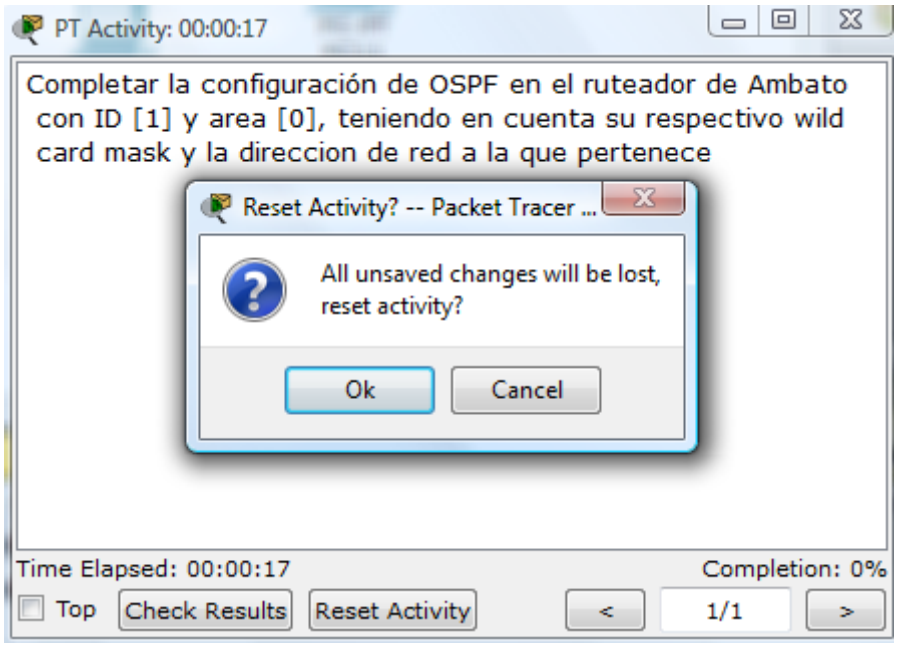

Figura 10.2.11.1

10.2.12. En este paso nos dirigimos a la configuración del router Ambato, y tal como se muestra en la figura.

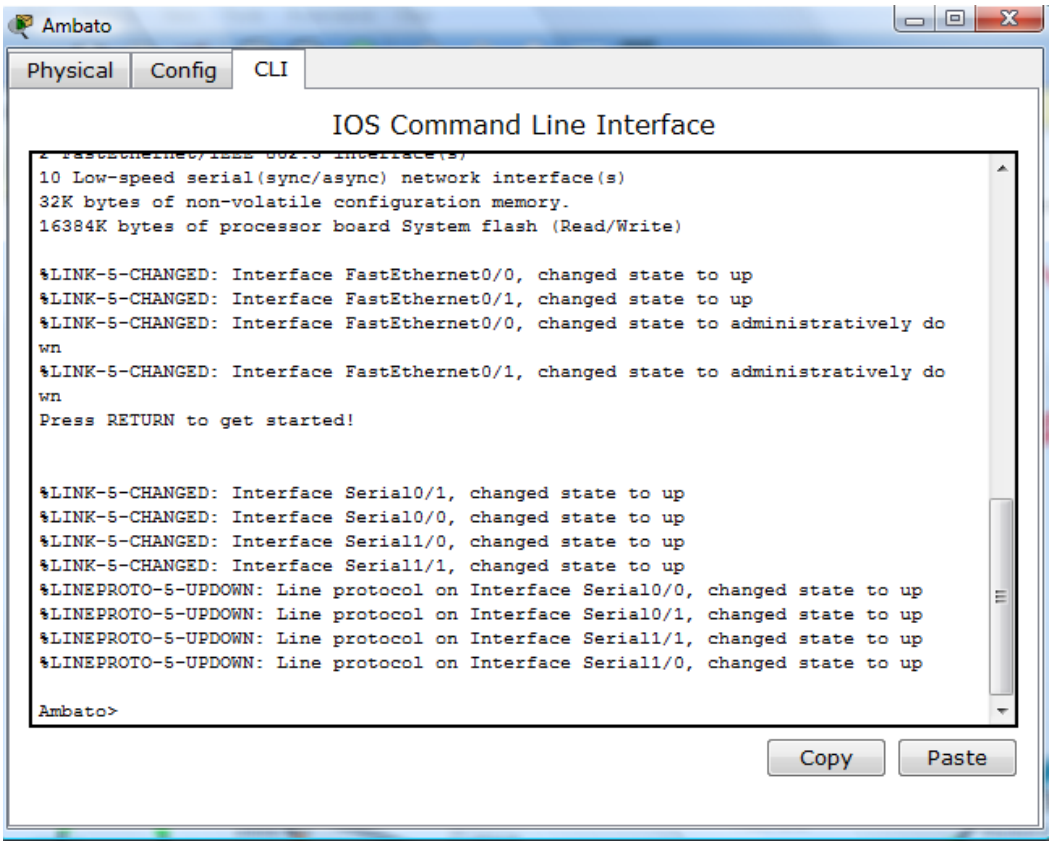

Figura 10.2.12.1

10.2.12.1. Entonces procedemos a la configuración del router Ambato, con enrutamiento OSPF ID [1] y área [0]

Ambato>enable
Ambato#conf t
Ambato(config)#router ospf 1
Ambato(config-router)#network 192.168.1.96 0.0.0.7 area 0
Ambato(config-router)#network 192.168.1.88 0.0.0.7 area 0
Ambato(config-router)#network 192.168.1.128 0.0.0.7 area 0
Ambato(config-router)#network 192.168.1.136 0.0.0.7 area 0
Ambato(config-router)#

10.2.12.2. Posteriormente damos tiempo hasta que la red converja totalmente probamos conectividad entre los

dispositivos, y posteriormente damos click en Check Result, y finalmente nos muestra una pantalla que la actividad se completo satisfactoriamente.

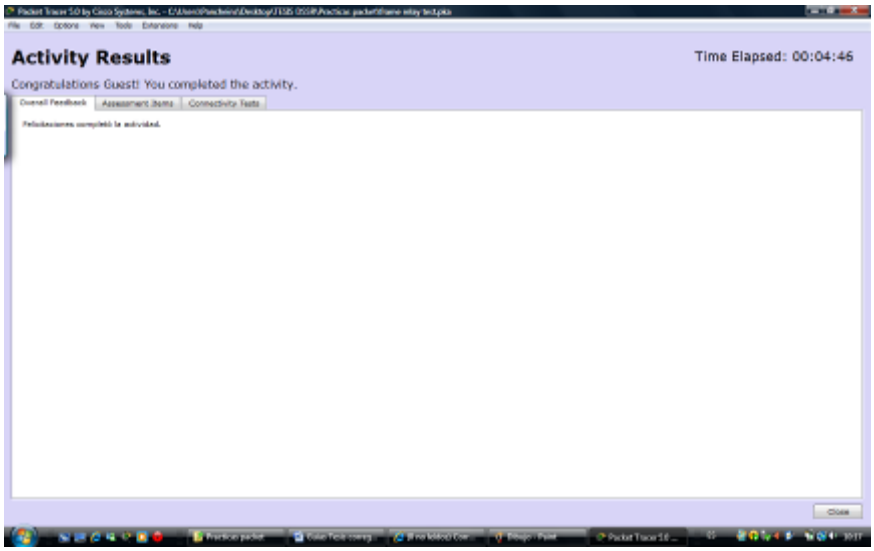

Figura 10.2.12.2.1

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

11. Guía de práctica: Realizar dos redes distintas en diferentes interfaces del Packet Tracer con el fin de poderlas comunicar con el MULTIUSER CONECTION

11.1. Objetivo

- Realizar dos redes en distintas interfaces con el fin de poder simular una red wan

11.2. Procedimiento

11.2.1. Realizamos la topología de red que tenga conectividad en cada uno de los dispositivos como se muestra en la figura

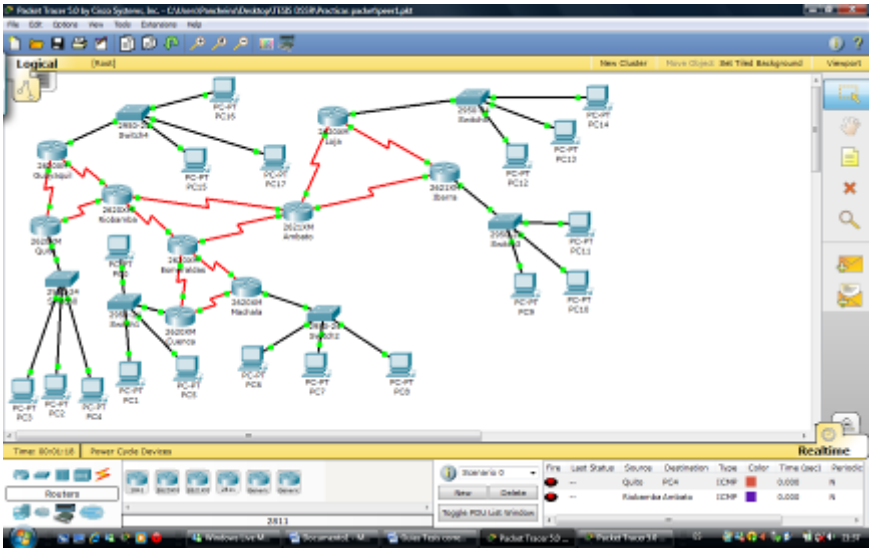

Figura 11.2.1

11.2.2. Realizamos otra red que tenga conectividad en caso uno de los dispositivos es importante recalcar que no tienen que tener las mismas ips de la red anterior

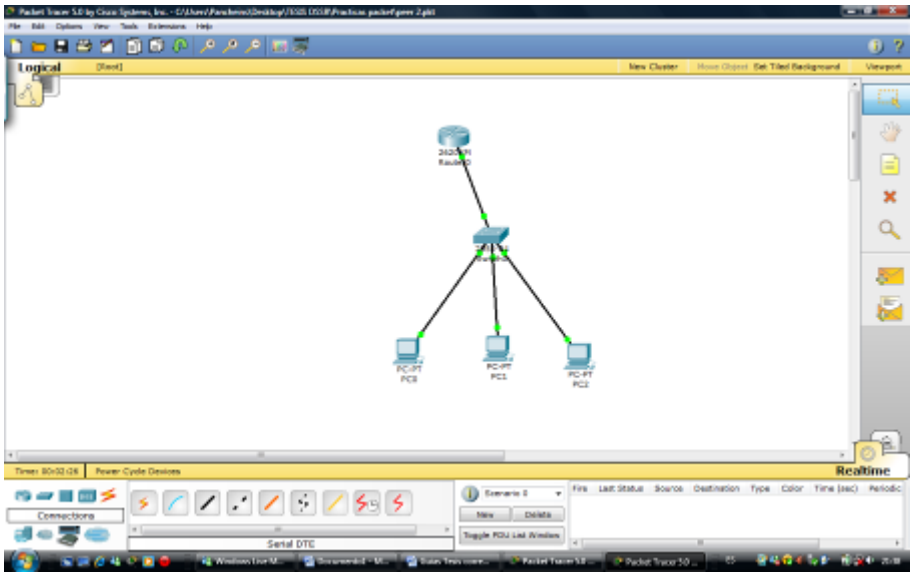

Figura 11.2.2.1

11.2.3. Como siguiente paso, en la segunda red insertamos una Multiuser Conection tal como se muestra en la figura

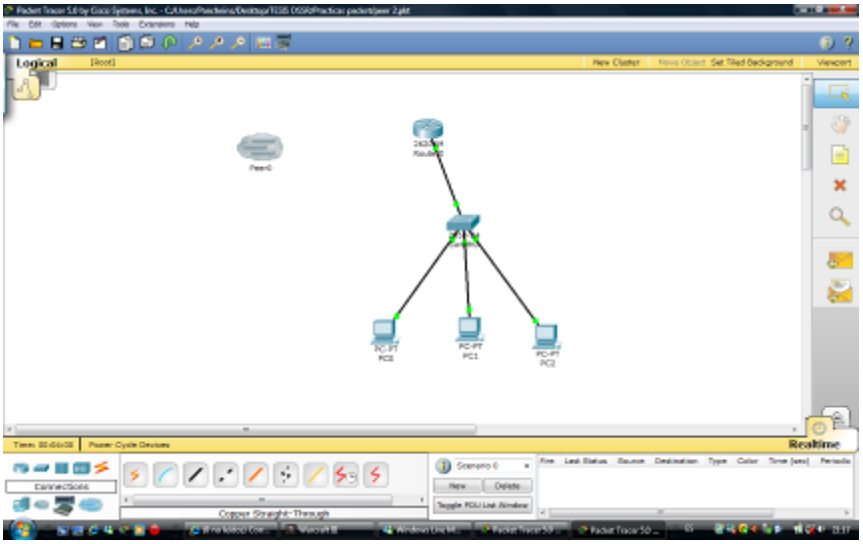

Figura 11.2.3.1

11.2.4. Consecuentemente se nos despliega una pantalla en la cual digitamos localhost o la ip de la computadora remota si estamos en red con otro dispositivo pero en nuestro caso localhost ya se va a

realizar localmente la conexión y luego el puerto por el cual se va habilitar, y con password "cisco", y finalmente Connect,

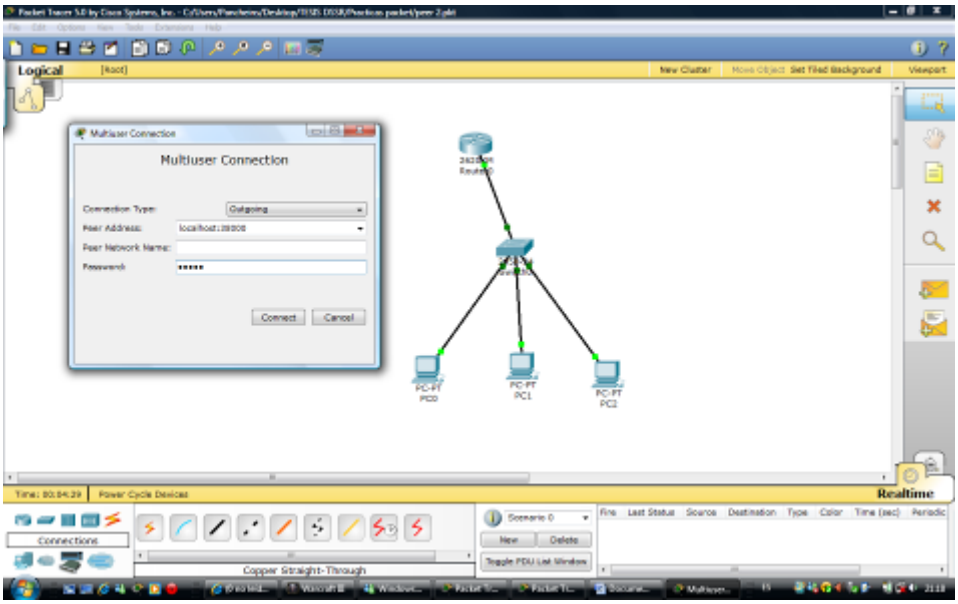

Figura 11.2.4.1

11.2.5. Posteriormente en la primera red se nos despliega un mensaje que un equipo remoto desea conectarse, lo cual aceptamos, tal como se muestra en la figura

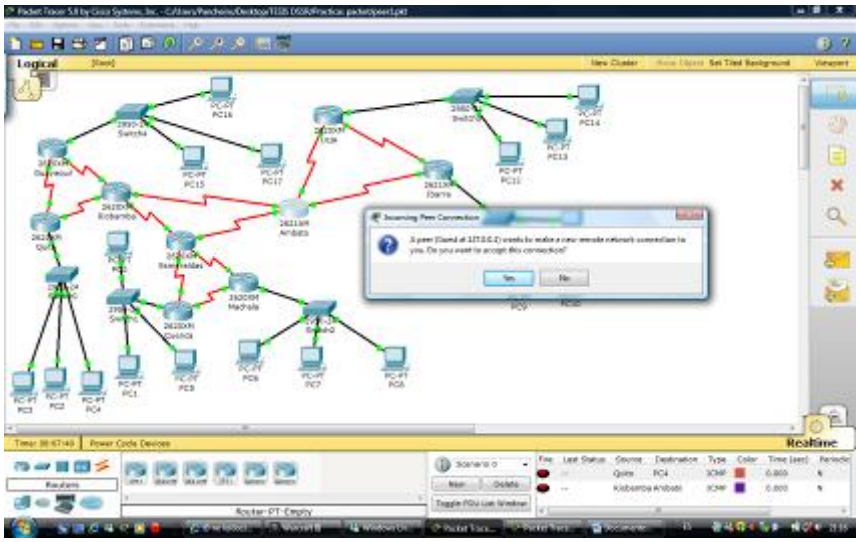

Figura 11.2.5.1

11.2.6. Con lo cual se nos crea la nube peer que va hacer la conectividad entre los dispositivos

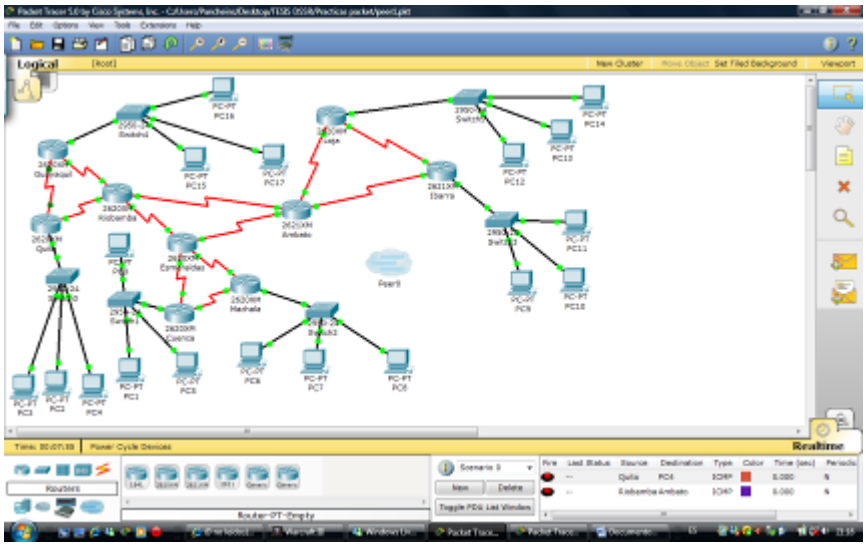

Figura 11.2.6.1

11.2.7. Nos dirigimos a la segunda red y creamos un nuevo enlace para que se puedan comunicar los dispositivos

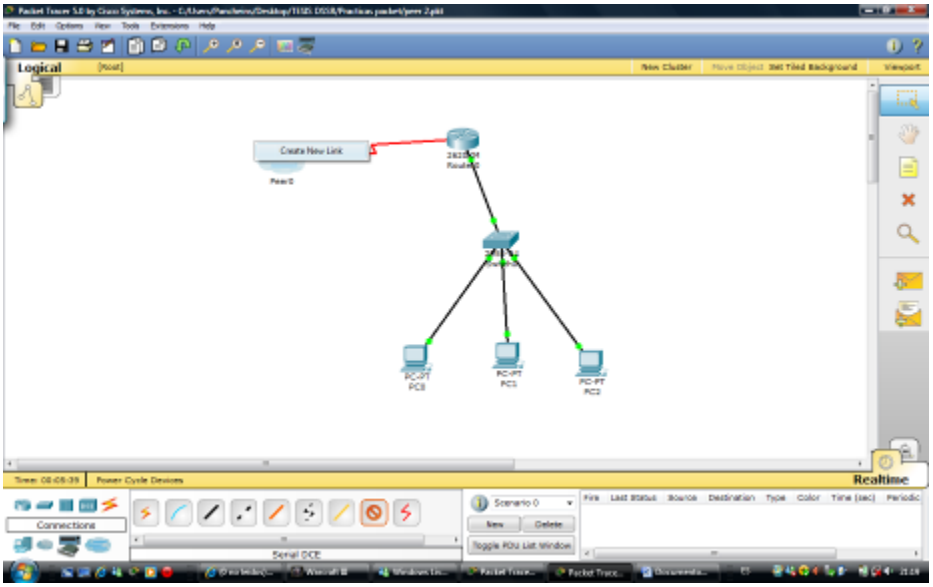

Figura 11.2.7.1

11.2.8. En la primera red hacemos lo mismo pero en este caso nos muestra la pantalla que existe un enlace opcional que es de nuestro ruteador remoto

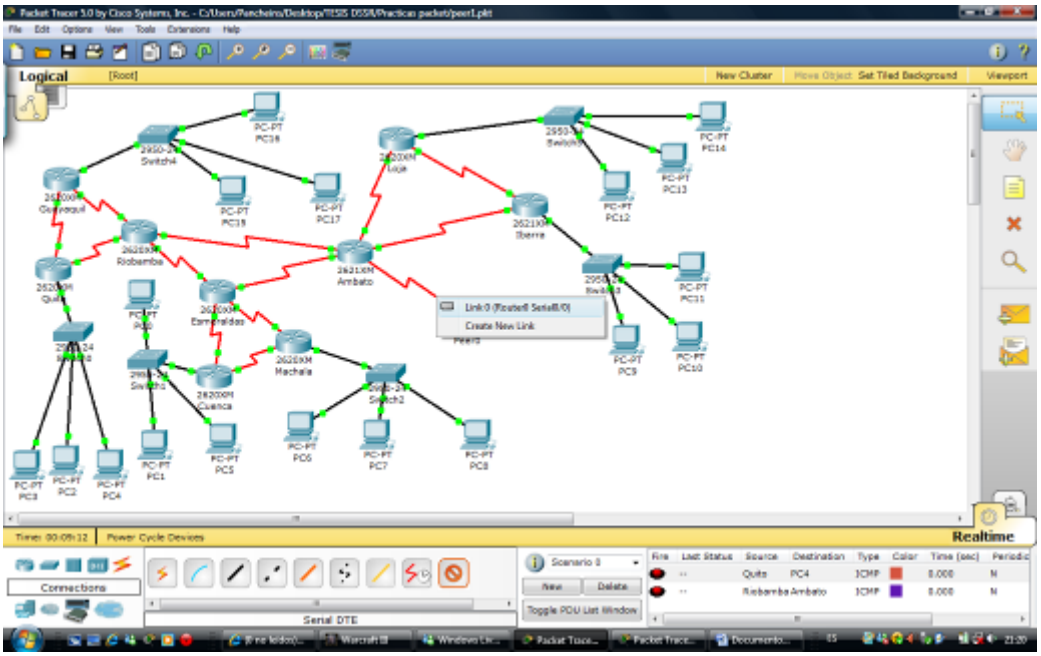

Figura 11.2.8.1

11.2.9. Finalmente se suben nuestros enlaces y existe conectividad en cada uno de nuestros dispositivos

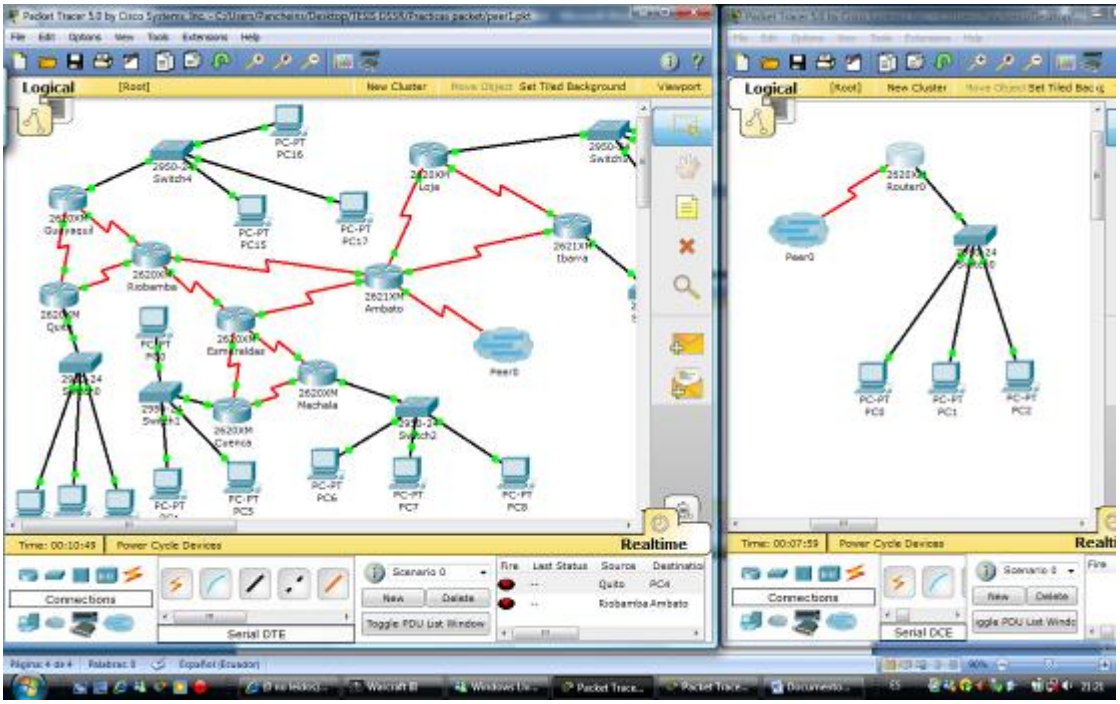

Figura 11.2.10.1

11.3. Análisis de resultados

- Se pudo hacer ping desde la estación de trabajo de la primera red hasta la otra red que se encuentra en otra interface del Packet Tracer
- Al realizar la simulación de la red se debe tener muy en cuenta que todos routers estén configurados debidamente las ips ya que no se pueden repetir con la segunda red.

11.4. Conclusiones

- Las redes se completaron y existió conectividad en las distintas interfaces con la ayuda de las Conexiones para Múltiples Usuarios
- Con la simulación realizada se cumplieron los objetivos requeridos
- Se puede observar muy claramente que la red se encuentra funcionando correctamente con todos sus elementos

11.5. Recomendaciones

- Tener a la mana un mapa de direcciones ips con el fin de que no se repitan las direcciones al momento de crear las dos redes en las diferentes interfaces
- Es importante recalcar que cuando se configura la Conexión para Múltiples Usuarios se debe establecer con anterioridad la clave que se a utilizar para la conexión remota
- Para la conexión remota es primordial que sea con clave ya que podemos tener abiertos varios archivos PKT que deseen conectarse a dicha red
- Al momento de la conexión remota es importante habilitar en el firewall el puerto que vamos a utilizar ya que tendríamos problemas al momento de la configuración.

SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

12. Guía de práctica: Realizar dos redes distintas en diferentes interfaces del Packet Tracer con el fin de poderlas comunicar con el MULTIUSER CONECTION

12.1. Objetivo

- Realizar dos redes en distintas interfaces con el fin de poder simular una red wan

12.2. Procedimiento

12.2.1. Realizamos la topología de red que tenga conectividad en cada uno de los dispositivos como se muestra en la figura

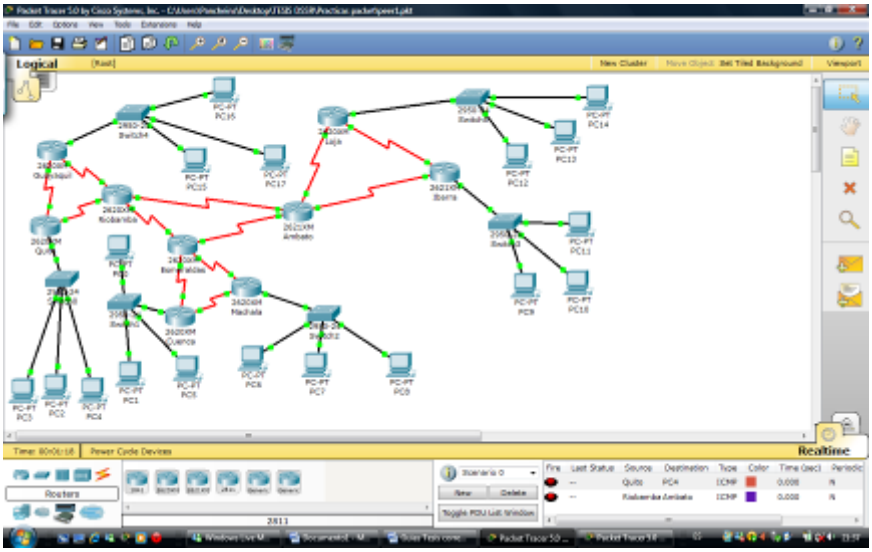

Figura 12.2.1.1

12.2.2. Realizamos otra red que tenga conectividad en caso uno de los dispositivos es importante recalcar que no tienen que tener las mismas ips de la red anterior

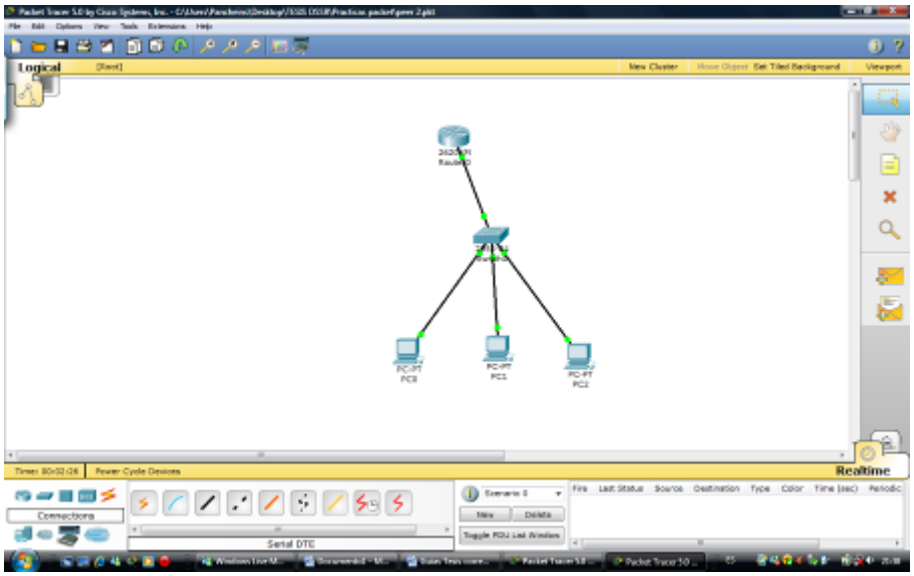

Figura 12.2.2.1

12.2.3. Como siguiente paso, en la segunda red insertamos una Multiuser Conection tal como se muestra en la figura

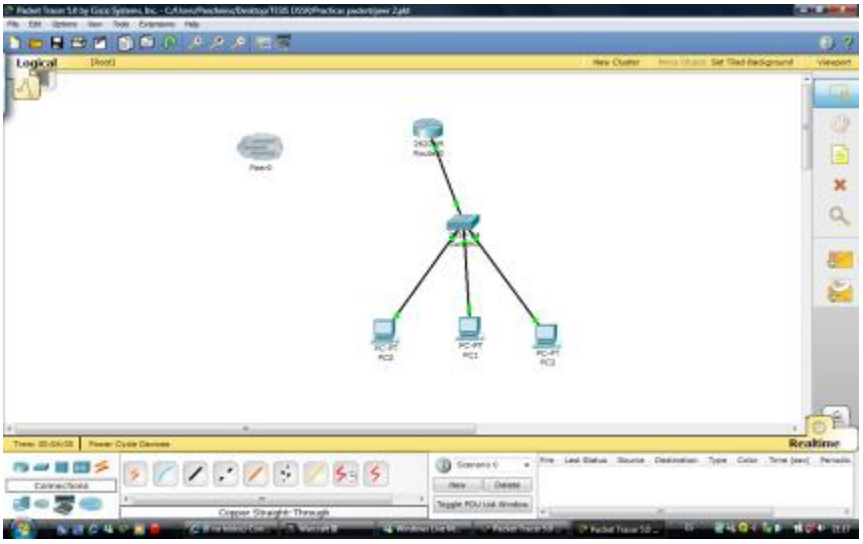

Figura 12.2.3.1

12.2.4. Consecuentemente se nos despliega una pantalla en la cual digitamos localhost o la ip de la computadora remota si estamos en red con otro dispositivo pero en nuestro caso localhost ya se va a

realizar localmente la conexión y luego el puerto por el cual se va habilitar, y con password "cisco", y finalmente Connect,

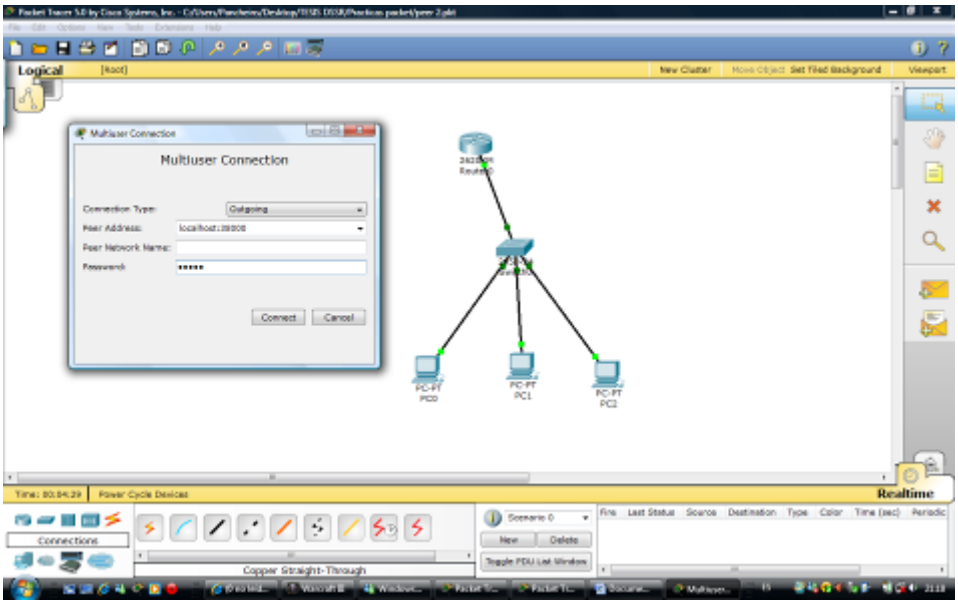

Figura 12.2.4.1

12.2.5. Posteriormente en la primera red se nos despliega un mensaje que un equipo remoto desea conectarse, lo cual aceptamos, tal como se muestra en la figura

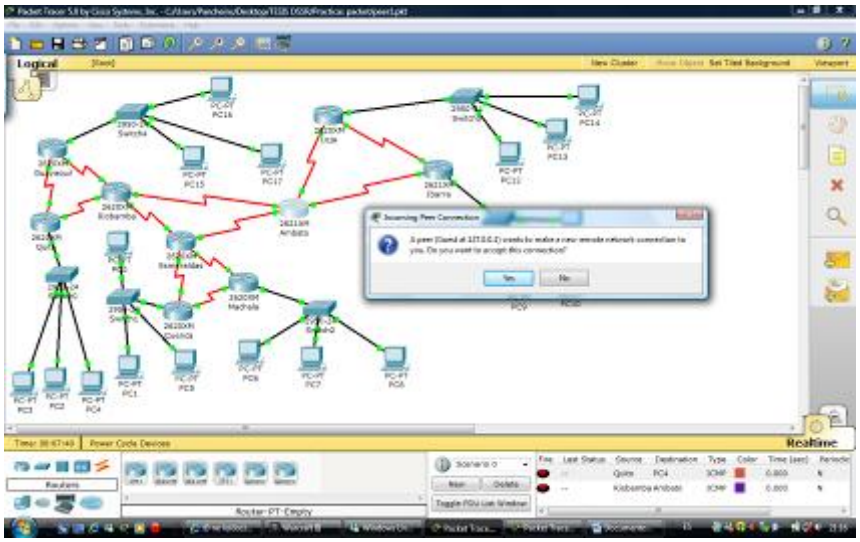

Figura 12.2.5.1

12.2.6. Con lo cual se nos crea la nube peer que va hacer la conectividad entre los dispositivos

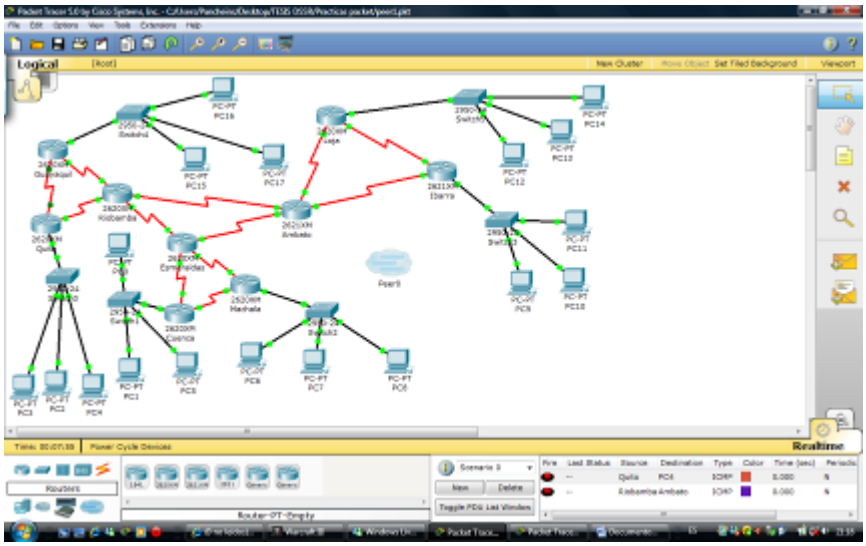

Figura 12.2.6.1

12.2.7. Nos dirigimos a la segunda red y creamos un nuevo enlace para que se puedan comunicar los dispositivos

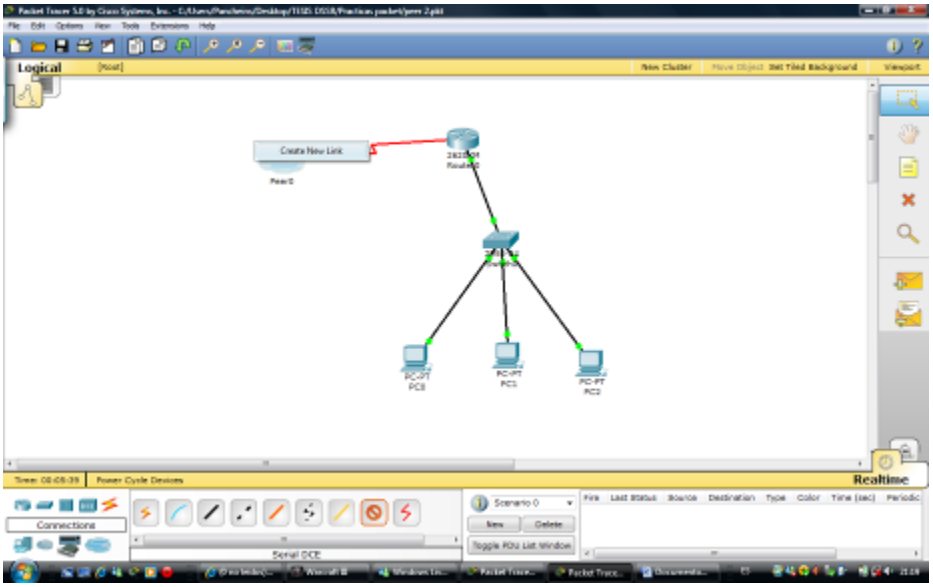

Figura 12.2.7.1

12.2.8. En la primera red hacemos lo mismo pero en este caso nos muestra la pantalla que existe un enlace opcional que es de nuestro ruteador remoto

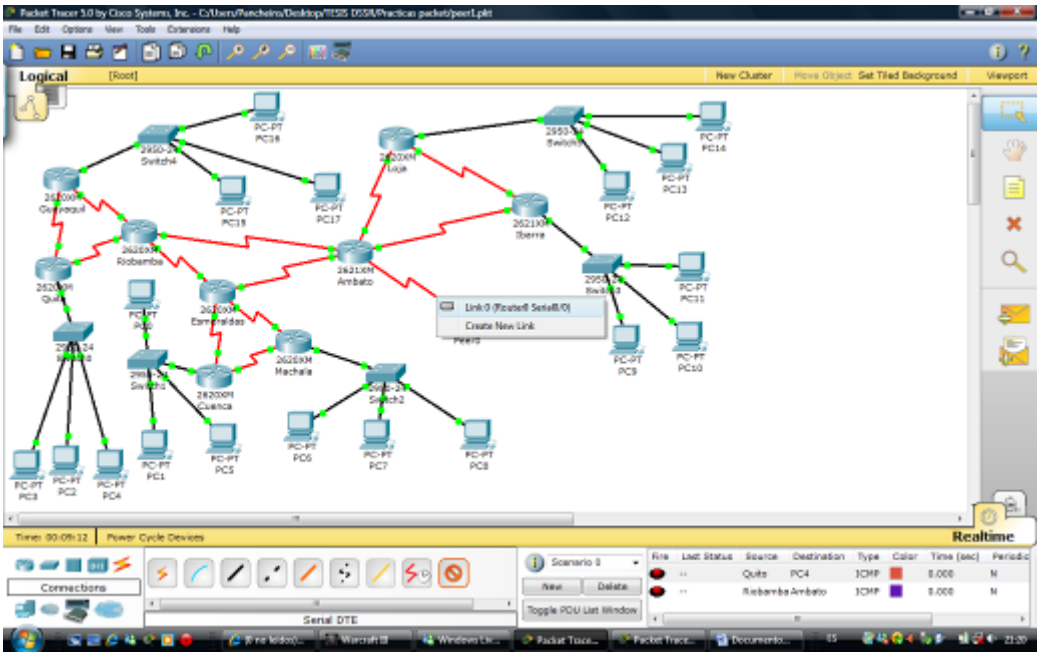

Figura 12.2.8.1

12.2.9. Finalmente se suben nuestros enlaces y existe conectividad en cada uno de nuestros dispositivos

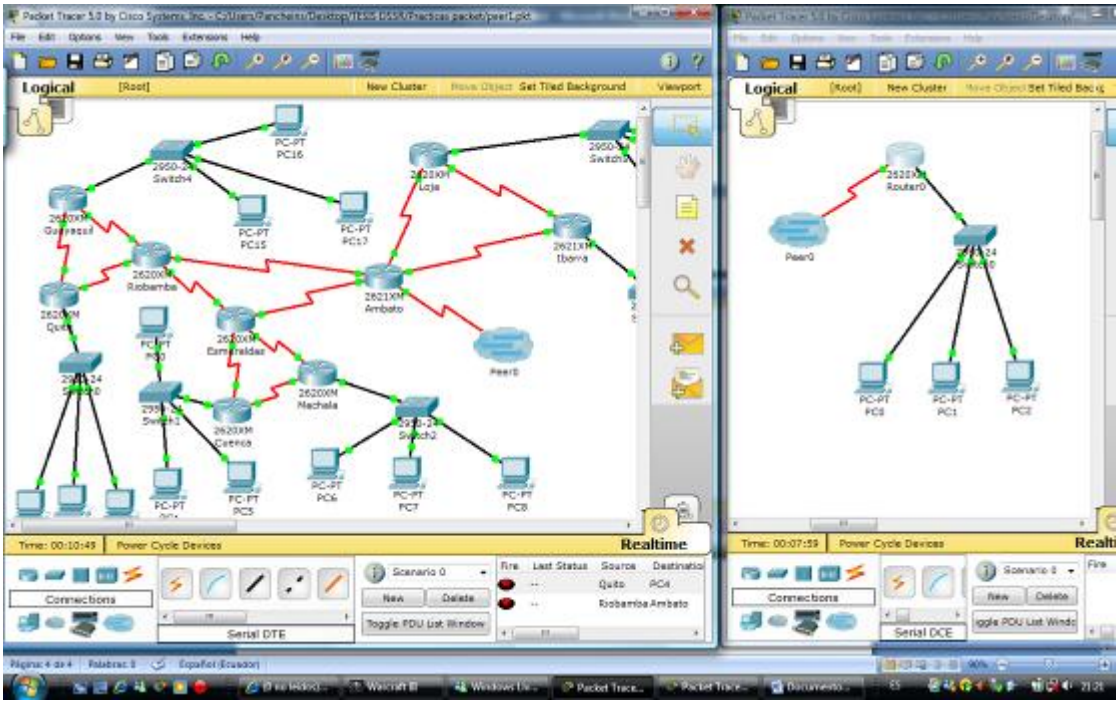

Figura 12.2.2.9.1

12.3. Análisis de resultados

- Se pudo hacer ping desde la estación de trabajo de la primera red hasta la otra red que se encuentra en otra interface del Packet Tracer
- Al realizar la simulación de la red se debe tener muy en cuenta que todos routers estén configurados debidamente las ips ya que no se pueden repetir con la segunda red.

12.4. Conclusiones

- Las redes se completaron y existió conectividad en las distintas interfaces con la ayuda de las Conexiones para Múltiples Usuarios
- Con la simulación realizada se cumplieron los objetivos requeridos
- Se puede observar muy claramente que la red se encuentra funcionando correctamente con todos sus elementos

12.5. Recomendaciones

- Tener a la mana un mapa de direcciones ips con el fin de que no se repitan las direcciones al momento de crear las dos redes en las diferentes interfaces
- Es importante recalcar que cuando se configura la Conexión para Múltiples Usuarios se debe establecer con anterioridad la clave que se a utilizar para la conexión remota
- Para la conexión remota es primordial que sea con clave ya que podemos tener abiertos varios archivos PKT que deseen conectarse a dicha red
- Al momento de la conexión remota es importante habilitar en el firewall el puerto que vamos a utilizar ya que tendríamos problemas al momento de la configuración.

CAPÍTULO V

5.1. CONCLUSIONES

- Se llegó a concluir la utilización del presente proyecto con el fin de llegar a un aprendizaje de mayor nivel por parte de los alumnos pues tendrán la oportunidad de practicar lo aprendido a través de las guías afianzando y solidificando sus conocimientos.

- Se analizó que dentro de las capacidades de cada estudiante de Ingeniería de Sistemas de la ESPE existe el conocimiento y el razonamiento necesario para elaborar proyectos que incluyan análisis, diseño e implementación de un servidor de educación virtual que permita a la ESPE crecer en tecnología y reflejar el auto aprendizaje con sus estudiantes

- Se determinó que existen diferentes tipos de redes de comunicaciones, las características que componen cada una ayudan a definir un concepto claro de ellas. La redes de área extendida cubren una área mucho más extensa como una ciudad o un país, la topología, tipos de enlaces de conexión -fibra óptica, enlaces punto a punto, inalámbricas -, protocolos de comunicación -IPv6, FDDI, SDLC, HDLC, -que manejen influirá para la velocidad con la que se transfieren los datos

5.2. RECOMENDACIONES

- Se recomienda la utilización del presente proyecto con el fin de llegar a un aprendizaje de mayor nivel por parte de los alumnos pues tendrán la oportunidad de practicar lo aprendido a través de las guías afianzando y solidificando sus conocimientos.

- Se recomienda aplicar esta metodología de estudio a todas las asignaturas, pues el estudiante tiene la posibilidad de interactuar de mejor forma con la parte teórica aprendida y palpar de mejor forma los resultados.

- El presente modo de educación es una manera fácil de acceder a los recursos necesarios para el aprendizaje, pues al tratarse de educación virtual y de acuerdo al manejo de los contenidos a nivel web, tanto tutores como estudiantes tienen un libre acceso a través de Internet.