ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"DESARROLLO DE GUIAS DE LABORATORIO VIRTUAL DE FUNDAMENTOS DE REDES UTILIZANDO EL SOFTWARE PACKET TRACER"

DIEGO SEBASTIAN STADLER ROMAN

Sangolquí – Ecuador

2008

CERTIFICACIÓN

Certificamos que el proyecto de grado titulado: "DESARROLLO DE GUIAS DE LABORATORIO VIRTUAL DE FUNDAMENTOS DE REDES UTILIZANDO EL SOFTWARE PACKET TRACER" ha sido desarrollado en su totalidad por el señor Diego Sebastián Stadler Román con cedula de ciudadanía # 171243917-1, bajo nuestra dirección.

_____	_____
Ing. Carlos Romero	Ing. Darwin Aguilar
DIRECTOR	CODIRECTOR

RESUMEN

El Simulador Packet Tracer 4.0, es una herramienta muy útil para el laboratorio de Fundamentos de Redes, porque permite implementar y observar claramente el funcionamiento de las redes sin la necesidad de conectarlas físicamente, y las ventajas que presenta son muy útiles para utilizarlas en la actualidad a nivel mundial.

En el software Packet Tracer se puede realizar la simulación en tiempo real o en tipo de simulación verificando el paso a proceder de cada paquete.

Todas las prácticas realizadas en el simulador Packet Tracer se pueden realizar con componentes reales ósea con su hardware correspondiente sin obtener ningún inconveniente al momento de conectarlos e instalarlos

En las prácticas realizadas empezamos con conexiones básicas como es una conexión entre dos Cpu´s utilizando un cable cruzado, hasta interconectar varios dispositivos de red para una red específica.

En las diferentes practicas se va demostrando lo correspondiente al capitulo, por ejemplo en el capitulo que se trata de las capas del modelo OSI, en la practica se observa el paso a proceder de cada paquete en las diferentes capas del modelo OSI.

En cada capitulo se realiza una prueba de selección múltiple la cual es basada en un software libre en código php, el cual fue adaptado a nuestra necesidad, consiguiendo de este modo una prueba en línea con calificación automática la cual es muy sencilla de manejarla.

DEDICATORIA

Dedico este trabajo de manera muy especial a mi hogar, pues gracias a su apoyo diario, sus palabras de aliento para decirme las cosas y no dejarme caer ante cualquier adversidad.

A toda mi familia mas querida que siempre me han apoyado para el logro de esta meta, mi abuelita querida, mis tíos que siempre estuvieron apoyándome, primos.

A mis amigos y compañeros verdaderos esos que nunca te dejan solo cuando más los necesitas y siempre se encuentran presentes.

AGRADECIMIENTO

Les agradezco de todo corazón a mis padres Alicia y Diego por su amor incondicional y su apoyo, a mis hermanos Gabriela y José Antonio que han estado siempre junto a mí en todo momento. A mis profesores Coordinadores por su orientación y colaboración. A toda mi familia por su apoyo. A mis amigos y a todos aquellos que fueron partícipes para la realización de culminar un peldaño más en mi vida.

PRÓLOGO

El software Packet Tracer, se lo utilizo por la necesidad de tener una herramienta que, a través de las prácticas permita obtener resultados confiables sin tener la necesidad de armar toda la red físicamente.

Muchas veces como estudiantes del Departamento de Eléctrica y Electrónica nos vemos en la necesidad de conseguir todos los componentes físicos de una red, la que necesitamos armar y probar lo cual se vuelve sumamente complicado, por esta razón es sumamente favorable el uso de este software.

En este proyecto de tesis se realiza una recopilación necesaria de información, para un correcto entendimiento y comprensión de cada tema, con una practica dedicada a cada capitulo y con una prueba en red de selección múltiple y con calificación automática.

Finalmente se realiza la culminación del proyecto al tener correcto funcionamiento del software Packet Tracer, en el cual se pueden ejecutar prácticas para tener un mejor entendimiento del trabajo y con los resultados comprobar el por qué son tan importantes el uso del software y su utilización a nivel mundial.

ÍNDICE DE CONTENIDO

ANEXOS

Anexo 1 Banco de Preguntas Capítulo I

Anexo 2 Banco de Preguntas Capítulo II

Anexo 3 Banco de Preguntas Capítulo III

Anexo 4 Banco de Preguntas Capítulo IV

Anexo 5 Banco de Preguntas Capítulo V

Anexo 6 Banco de Preguntas Capítulo VI

Anexo 7 Banco de Preguntas Capítulo VII

INDICE DE TABLAS

INDICE DE FIGURAS

FIGURAS DEL CAPITULO 4:

FIGURAS DEL CAPITULO 5:

FIGURAS DEL CAPITULO 6:

FIGURAS DEL CAPITULO 7:

CAPITULO I

SOFTWARE GENERADOR DE PRUEBAS

1.1 INTRODUCCIÓN

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 aparatos 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.

1.1.1 Creación de preguntas.

Para la creación del banco de preguntas se debe ingresar en la interfaz Web de nuestro programa el cual se encuentra en el siguiente link index.html como se muestra en la figura 1.1. 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 capitulo.

Figura 1.1. Interfaz Web

Ingresamos a la plantilla principal, y colocamos cancelar para la creación de preguntas como se muestra en la figura 1.2

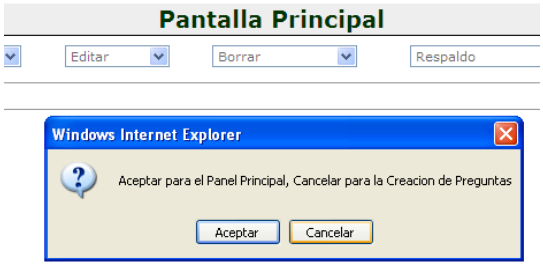


Figura 1.2. Creación de Preguntas

Para la creación de preguntas primero debemos agregar un capitulo como se muestra en la figura 1.3

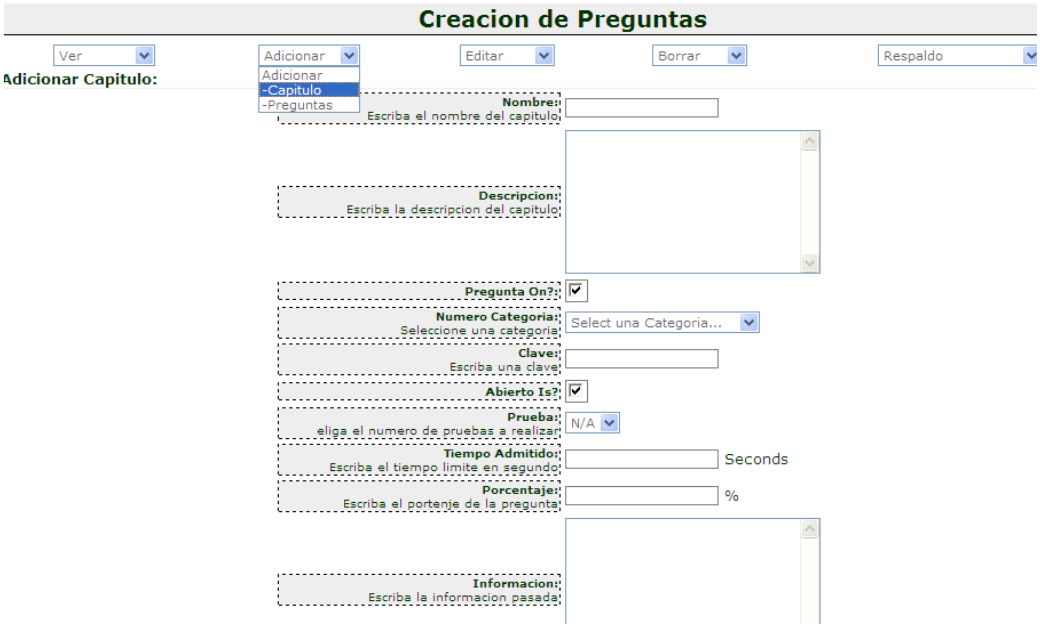


Figura 1.3. Creación Capitulo

En la siguiente pantalla se selecciona adicionar preguntas y se procede a llenar los datos correspondientes como se muestra en la figura 1.4.

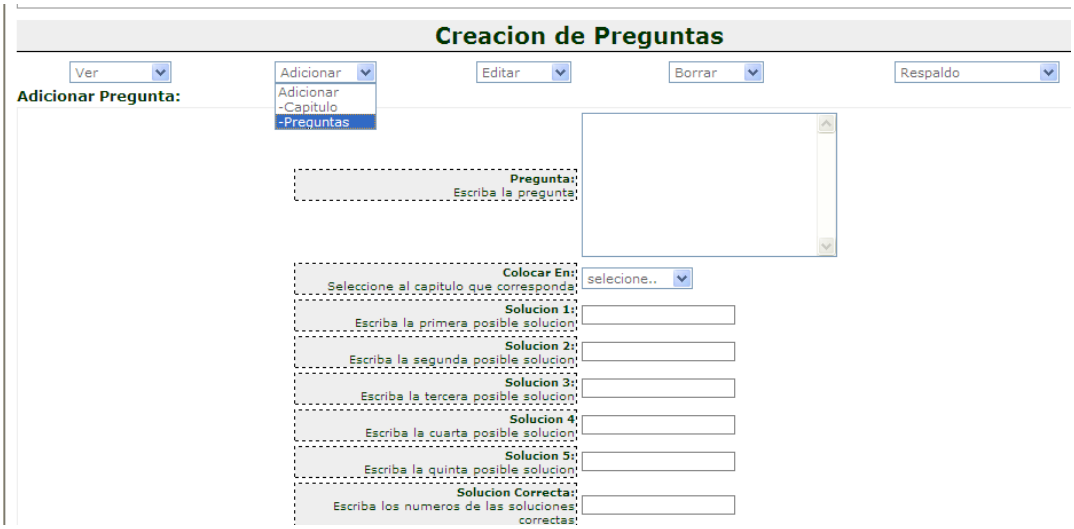


Figura 1.4. Adicionar Pregunta

Al finalizar todos los datos necesarios como se muestra en la figura 1.5 se procede agregar la pregunta, para continuar agregando preguntas se vuelve a realizar los mismos pasos

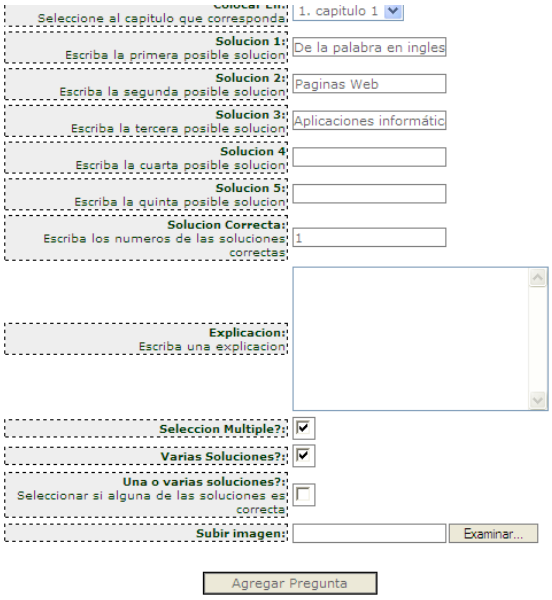


Figura 1.5. Agregar Pregunta

1.1.2. Creación de usuarios

Para la creación de usuarios se debe ingresar en la pantalla principal y proceder a adicionar usuario como se indica en la figura 1.6 y luego se procede a llenar los datos necesarios

Figura 1.6. Creación de usuario

Otra forma de registrar un usuario es en la pantalla de inicio donde puedes hacer clic donde dice no registrado? Como se muestra en la figura 1.7

Figura 1.7. Registrar Usuario

En la figura 1.8 se presenta la siguiente pantalla en la cual usted debe llenar los datos necesarios para poder registrar al usuario

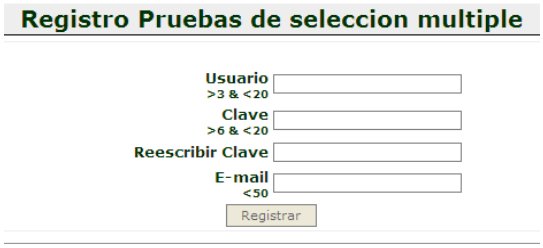


Figura 1.8. Registro Usuario

1.1.3. PRUEBA DE SELECCIÓN MÚLTIPLE

En la pantalla de inicio debe ingresar el nombre de usuario y contraseña como se muestra en la figura 1.9.

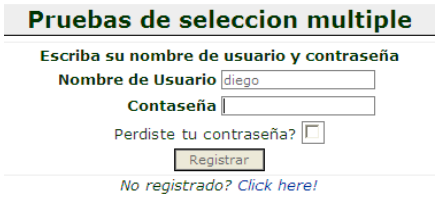


Figura 1.9. Inicio Prueba

Ingresamos en la plantilla de preguntas y se debe elegir el capitulo a que se desea realizar la prueba como se muestra en la figura 1.10.

Figura 1.10. Selección de capitulo

En la siguiente pantalla aparece la prueba a realizarse del capitulo seleccionado como se muestra en la figura 1.11. Se procede a desarrollar la prueba

Figura 1.11 Prueba a realizar

Al terminar de contestar todas las preguntas procede a la calificación automática haciendo clic sobre Corregir prueba 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 1.12

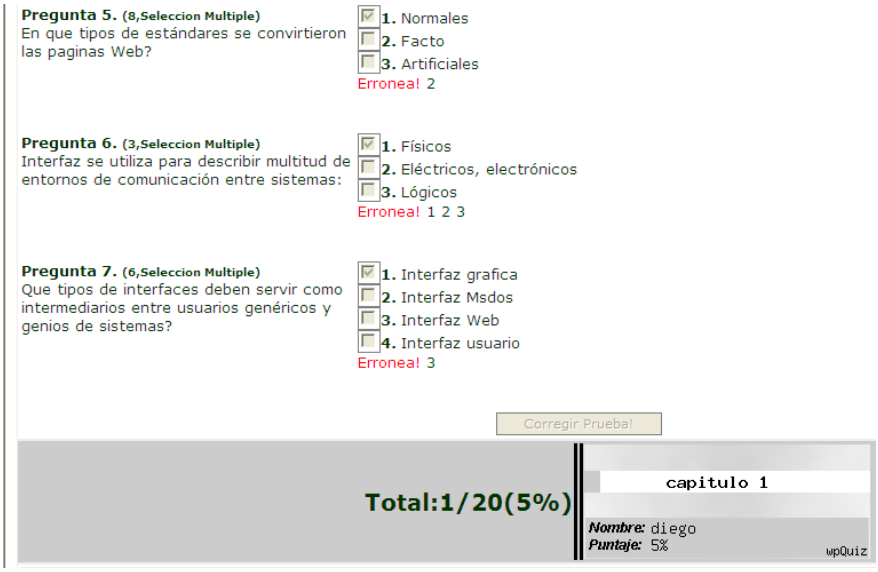


Figura 1.12 Calificación Prueba

CAPITULO II

INTRODUCCIÓN A LAS REDES DE DATOS

2.1. DEFINICIÓN DE REDES DE DATOS

La definición mas 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
- Modems

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 costo/beneficio

2.2. 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)

2.2.1. 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.

2.2.2 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 "lo que no es LAN se considera WAN'.

2.2.3 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 2.1.

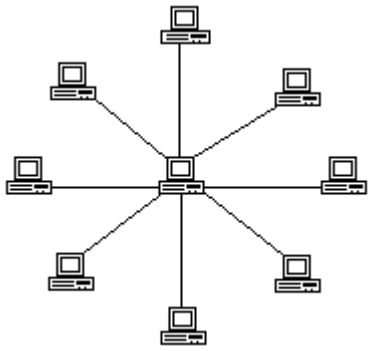


Figura. 2.1. Topología estrella

- **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 (CSMAJCD) "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 esta 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 2.2

Figura 2.2 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 2.3

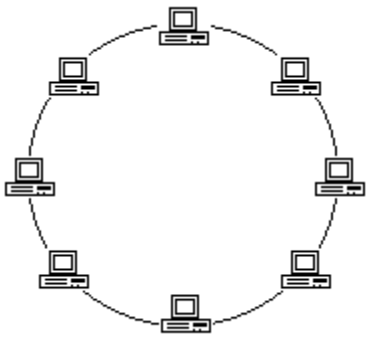


Figura 2.3 Topología Token Ring

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 esta 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.

2.3. TIPOS DE CONEXIONES

2.3.1. 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 usuarios debe ser entrenado para ejecutar tareas administrativas
- Menos Segura
- Todas las máquinas comparten recursos negativamente afectando el desempeño

Figura 2.4 Punto a punto

2.3.2. 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 2.5 Cliente servidor

2.3.3. 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 2.6 Mainframe

2.4. CLASIFICACIÓN DE LAS REDES DE DATOS

2.4.1. 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)

2.4.2. Según el tamaño

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

2.5. 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

2.6. PRUEBAS DE OPCIÓN MÚLTIPLE

El banco de preguntas correspondiente al capitulo se encuentra en anexos.

Para realizar las pruebas de selección múltiple correspondientes a este capitulo se debe correr el programa que se encuentra en el siguiente vinculo index.html, o en http://www.fie-espe.edu.ec/preguntas y luego se procede a ingresar los datos del alumno que va a realizar la prueba como se muestra en la figura 2.7

Figura 2.7. Datos Alumno

Para ingresar a resolver la prueba debemos elegir el capitulo que se va a realizar como se muestra en la figura 2.8 o se debe ingresar a la plantilla de preguntas e elegir igualmente el capitulo deseado.

Figura 2.8. Prueba Capitulo 2

El siguiente paso es realizar la prueba de selección múltiple como se indica en la figura 2.9. Luego de haber respondido a todas las preguntas se procede hacer clic sobre Corregir Prueba para que la prueba sea calificada y corregida automáticamente como se muestra en la figura 2.10

Figura 2.9. Prueba selección múltiple

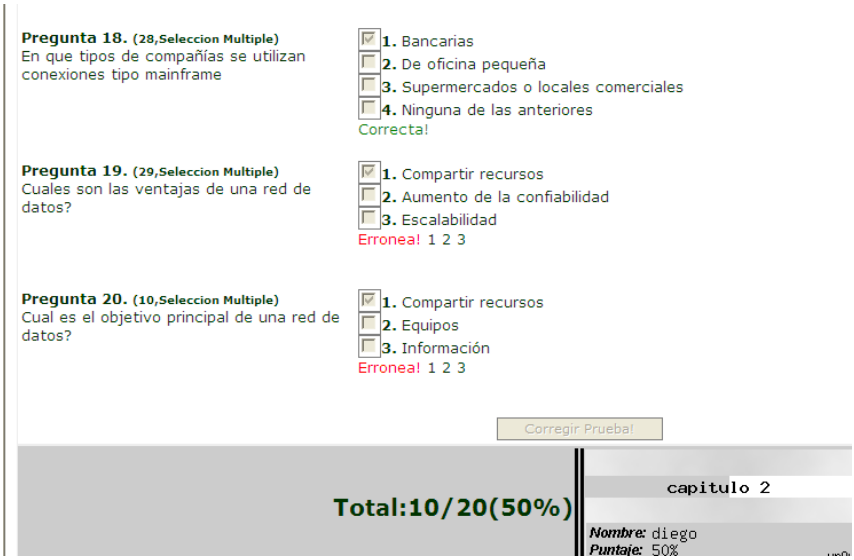


Figura 2.10. Calificación Prueba

CAPITULO III

COMPONENTES FÍSICOS DE UNA RED LAN

3.1. CONCENTRADORES Y TARJETAS DE RED

3.1.1. Concentradores

Un **concentrador** es un dispositivo que permite centralizar el cableado de una red. También conocido con el nombre de *hub*.

Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella.

Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central, llamado también repetidor multipuerto, y existen 3 clases.

- **Pasivo:** No necesita energía eléctrica.
- **Activo:** Necesita alimentación.
- **Inteligente:** También llamados *smart hubs* son *hubs* activos que incluyen microprocesador.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

Conclusiones:

- El concentrador envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

- Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

- Un concentrador funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 megabit/segundo le trasmitiera a otro de 10 megabit/segundo algo se perdería del mensaje. En el caso del ADSL los routers suelen funcionar a 10 megabit/segundo, si lo conectamos a nuestra red casera, toda la red funcionará a 10 megabit/segundo, aunque nuestras tarjetas sean 10/100 megabit/segundo.

- Un concentrador es un dispositivo simple, esto influye en dos características. El precio es barato. Un concentrador casi no añade ningún retardo a los mensajes.

- Los concentradores fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los sniffer. La disponibilidad de switches Ethernet de bajo precio ha dejado obsoletos, pero aún se pueden encontrar en instalaciones antiguas y en aplicaciones especializadas.

3.1.2. Tarjetas de red o NIC (*Network Interface Controller)*

La tarjeta de red es una tarjeta de expansión que permite a una DTE (Data Terminal Equipment) ordenador o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom, etc.). Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, etc.), pero, actualmente el más común es del tipo Ethernet utilizando un interfaz o conector RJ45.

Las tarjetas de red Ethernet pueden variar en función de la velocidad de transmisión, normalmente 10 Mbps ó 10/100 Mbps. Actualmente se están empezando a utilizar las de 1000 Mbps, también conocida como Gigabit Ethernet y en algunos casos 10 Gigabit Ethernet, utilizando también cable de par trenzado, pero de categoría 6, 6e y 7 que trabajan a frecuencias más altas. Otro tipo de adaptador muy extendido hasta hace poco era el que usaba conector BNC.

También son NIC las tarjetas inalámbricas o wireless, las cuales vienen en diferentes variedades dependiendo de la norma a la cual se ajusten, usualmente son 802.11a, 802.11b y 802.11g. Las más populares son la 802.11b que transmite a 11 Mbps con una distancia teórica de 100 metros y la 802.11g que transmite a 54 Mbps.

Cada tarjeta de red tiene un número de identificación único de 48 bits, en hexadecimal llamado MAC (no confundir con Apple Macintosh). Estas direcciones hardware únicas son administradas por el Institute of Electronic and Electrical Engineers (IEEE). Los tres primeros octetos del número MAC son conocidos como OUI identifican a proveedores específicos y son designados por la IEEE.

Se le denomina también **NIC** a un sólo chip de la tarjeta de red, este chip se encarga de servir como interfaz de Ethernet entre el medio físico (por ejemplo un cable coaxial) y el equipo (por ejemplo un PC).

Es un chip usado en computadoras o periféricos tales como las tarjetas de red, impresoras de red o sistemas embebidos para conectar dos o más dispositivos entre sí a través de algún medio, ya sea conexión inalámbrica , cable UTP, cable coaxial, fibra óptica y otros.

3.2. MEDIOS DE TRANSMISIÓN

El medio de transmisión es el soporte físico por el que se va a trasladar la información o datos en forma de señales o magnitudes físicas.
La calidad de transmisión será determinada por las diferentes características del medio por el que se propaga.

3.2.1. Medios magnéticos.

Una de las formas más comunes de transportar datos de una computadora a otra es escribirlos en medios magnéticos; su costo por bit para almacenar la información tiene mayor eficacia en su costo (económico).

- Una cinta de video (Exabyte) puede almacenar 7 GB.
- Una caja de 50 cm puede almacenar 1000 cintas, o 7000 GB.
- En los Estados Unidos se puede mandar una caja de este tipo de cualquier punto a otro en 24 horas.
- El ancho de banda entonces es 648 Mbps. Si el destino es solamente a una hora de distancia, el ancho de banda es más de 15 Gbps.

3.2.2. Par trenzado (*twisted pair*).

El cable de par trenzado es una conexión en la que dos conductores (cables de cobre) son entrelazados para cancelar las interferencias electromagnéticas (IEM) de fuentes externas y la diafonía de los cables adyacentes.

3.2.3. Cable coaxial.

El cable coaxial es un cable formado por dos conductores concéntricos:

- Un conductor central o núcleo, formado por un hilo sólido o trenzado de cobre (llamado positivo o vivo).

- Un conductor exterior en forma de tubo, formado por una malla trenzada de cobre o aluminio o bien por un tubo, en caso de cables semirígidos. Este conductor exterior produce un efecto de blindaje y además sirve como retorno de las corrientes.

El primer conductor está separado del segundo por una capa aislante llamada dieléctrico. De la calidad del dieléctrico dependerá principalmente la calidad del cable.

3.2.4. Fibra óptica.

La fibra óptica es un conductor de ondas en forma de filamento, generalmente de vidrio, aunque también puede ser de materiales plásticos. La fibra óptica es capaz de dirigir la luz a lo largo de su longitud usando la reflexión total interna. Normalmente la luz es emitida por un láser o un LED.

Las fibras son ampliamente utilizadas en telecomunicaciones, ya que permiten enviar gran cantidad de datos a gran velocidad, mayor que las comunicaciones de radio y cable. También se las utiliza para redes locales. Es un medio de transmisión inmune a las interferencias por excelencia pero su costo es elevado.

3.2.5. Además de estos medios de transmisión existen también medios de transmisión inalámbricos. Estos medios de transmisión se generan cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar por el espacio libre.

Toda la comunicación inalámbrica se basa en este principio. Cada medio de transmisión esta definida por una banda de frecuencias dentro de un rango específico en el espectro electromagnético (Véase figura 3.1). La longitud de onda es inversamente proporcional a la frecuencia $\lambda = \frac{c}{f}$.

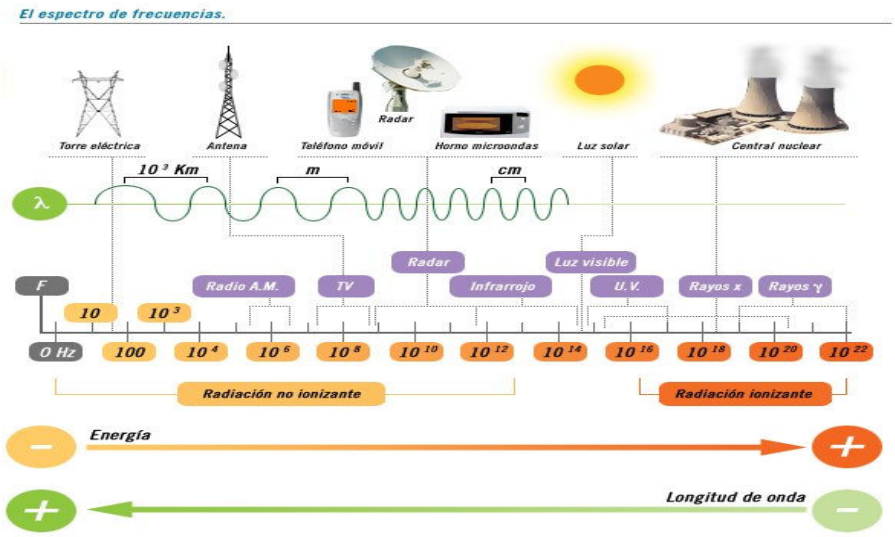


Figura 3.1. Espectro electromagnético *

3.2.6. Radio.

De acuerdo con la distribución del espectro electromagnético a las ondas de radio les corresponde el rango de frecuencias entre 10KHz – 10^9Hz. Estas ondas de radio recorren grandes distancias, y penetran fácilmente en los edificios. En su mayoría las ondas son omnidireccionales.

- Las ondas de frecuencias bajas pasan por los obstáculos, pero el poder disminuye con el cubo de la distancia.
- Las ondas de frecuencias más altas van en líneas rectas. Rebotan en los obstáculos y la lluvia las absorbe.

3.2.7. Microondas.

El rango para este tipo de señales esta entre los siguientes valores 10^9 Hz – 3×10^{11} Hz, es decir, longitudes de onda de entre 30 cm a 1 mm. Antes de la utilización de la fibra óptica formaban el centro del sistema telefónico de larga distancia.

Figura 3.1. Tomada de la dirección siguiente http://www.quimicaweb.net/grupo_trabajo_ccnn_2/tema5/tema5.htm

3.2.8. Infrarrojo.

El rango de frecuencias para este tipos de señales se encuentra entre los siguientes valores 3×10^{11} Hz – $3{,}84\times10^{14}$ Hz. Este medio de transmisión tiene una radiación electromagnética de mayor longitud de onda que las ondas de luz, pero menor que la de las microondas. Su rango de longitudes de onda va desde unos 700 nanómetros hasta 1 milímetro.

3.2.9. Ondas de luz.

Se denominan ondas de luz al rango de frecuencias que se encuentran en el espectro electromagnético entre los siguientes valores $3{,}84\times10^{14}$ Hz – $7{,}89\times10^{14}$ Hz.
A la radiación electromagnética en este rango de longitudes de onda se le denomina ondas de luz y sus límites se encuentran entre los siguientes valores 380 nm - 780 nm.

En el campo de las telecomunicaciones, el **medio de transmisión** constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión.

Los medios de transmisión pueden ser guiados y no guiados. En ambos la transmisión se realiza por medio de ondas electromagnéticas.

En un medio guiado las ondas son conducidas (guiadas) a través de un camino físico, mientras que en uno no guiado el medio solo proporciona un soporte para que las ondas se transmitan, pero no las guía.

Como ejemplo de medios guiados tenemos el cable coaxial, la fibra óptica y los cables de pares.

Entre los no guiados tenemos el aire y el vacío.

Dependiendo de la naturaleza del medio, las características y la calidad de transmisión se verán limitadas de forma distinta. Así en un medio guiado será de éste del que dependerán, principalmente, la velocidad de transmisión, el ancho de banda y el espacio entre repetidores de ser necesario. Sin embargo, en el caso de un medio no guiado resulta

más determinante el espectro de frecuencias de la señal transmitida que el propio medio de transmisión en sí mismo.

3.3. TIPOS DE CABLES Y ESPECIFICACIONES

Actualmente, la gran mayoría de las redes están conectadas por algún tipo de cableado, que actúa como medio de transmisión por donde pasan las señales entre los equipos. Hay disponibles una gran cantidad de tipos de cables para cubrir las necesidades y tamaños de las diferentes redes, desde las más pequeñas a las más grandes, la elección de uno respecto a otro depende del ancho de banda necesario, las distancias existentes y el costo.

Cada tipo de cable tiene sus ventajas e inconvenientes; no existe un tipo ideal. Las principales diferencias entre los distintos tipos de cables radican en la anchura de banda permitida (y consecuentemente en el rendimiento máximo de transmisión), su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la amortiguación de la señal y la distancia recorrida.

Tipos de cables de transmisión: Cable Recto, Cable Coaxial, Cable UTP, Fibra óptica, Cable STP, sin embargo para la instalación de un sistema de cableado estructurado los más recomendados son: UTP, STP y FTP. Todos estos tipos pertenecen a la categoría 5, que de acuerdo con los estándares internacionales pueden trabajar a 100 Mhz, y están diseñados para soportar voz, video y datos. Además de la fibra óptica, que basa su principal atractivo en estas habilidades.

1.- El STP se define con un blindaje individual por cada par, más un blindaje que envuelve a todos los pares. Es utilizado preferentemente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las interferencias electromagnéticas. Aunque con el inconveniente de que es un cable robusto, caro y mas difícil de instalar que un cable UTP.

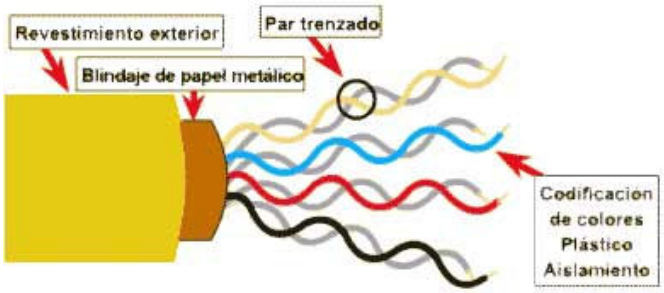


Figura 3.2. Cable STP*

2.- El cable recto de cobre consiste en alambres de cobre forrados con una aislante. Se usa para conectar varios equipos periféricos en distancias cortas y a bajas velocidades de transmisión. Los cables seriales usados para conectar los modems o las impresoras seriales son de este tipo. Este tipo de alambre sufre de interferencia a largas distancias.

Figura 3.3. Cable Recto*

3.- El UTP (par trenzado sin blindar). Es el soporte físico más utilizado en las redes LAN, pues es económico y su instalación es económica y sencilla. Por él se pueden efectuar transmisiones digitales (datos) o analógicas (voz). Consiste en un grupo de conductores de cobre (protegido cada conductor por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la Diafonía. Un cable de par trenzado puede tener pocos o muchos pares; en aplicaciones de datos lo normal es que tengan 4 pares. Uno de sus inconvenientes es la alta sensibilidad que presenta ante interferencias electromagnéticas.

Figura 3.2. Tomada de la dirección siguiente www.alfinal.com/Temas/cableadoestructurado.shtml
Figura 3.3. Tomada de la dirección siguiente www.rginformatica.net/index.php?cPath=77

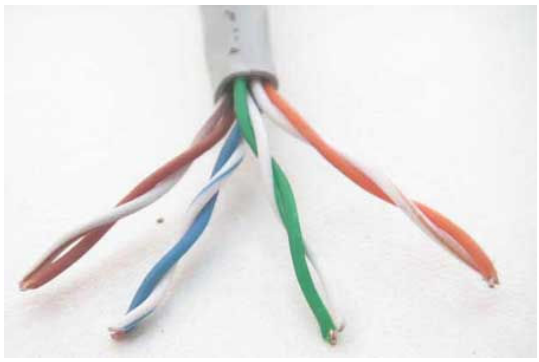


Figura 3.4. Cable UTP*

- **Categorías del cable UTP.** Una categoría de cableado es un conjunto de parámetros técnicos que garantizan un ancho de banda determinado en un canal de comunicaciones de cable de par trenzado. Dentro del cableado estructurado las categorías más comunes son:

    - UTP categoría 1: También llamado *cobre de grado de voz* es un cable UTP definido por el estándar TIA/EIA-568-B creado por la Electronic Industries Alliance (*Alianza de Industrias Electrónicas* o **EIA**) y la Telecommunications Industry Association (*Asociación de la Industria de Telecomunicaciones* o **TIA**). El Cable de Categoría 1 fue diseñado para comunicaciones telefónicas y no es adecuado para la transmisión de datos. Alcanza como máximo una velocidad de 100 Kbps.

Figura 3.5. Cable UTP cat1*

    - UTP categoría 2: Es un tipo de cable de par trenzado no protegido (*unshielded*) definido por el estándar TIA/EIA-568-B. El cable UTP Categoría 2 es utilizado para la transmisión de voz y datos hasta velocidades de 4Mbps. Su principal aplicación es para Token Ring. El cable esta

Figura 3.4. Tomada de la dirección siguiente www.alfinal.com/Temas/cableadoestructurado.shtml
Figura 3.5. Tomada de la dirección siguiente www.tenda.initron.com

compuesto por cuatro pares trenzados de hilo de cobre, como se muestra en la figura 3.6. En la actualidad ya casi no se lo utiliza.

Figura 3.6. Cable UTP cat2*

- UTP categoría 3: Es un cable de par trenzado diseñado para transportar datos de hasta 10 Mbps, con un ancho de banda de 16 MHz. Es parte de una familia de estándares de cables de cobre definido en conjunto por la EIA y la TIA. Los cables de categoría 3 están hechos con conductores calibre 24 AWG y tienen una impedancia característica de 100 W. Entre las principales aplicaciones de los cables de categoría 3 encontramos: voz, Ethernet 10Base-T y Token Ring. Tiene una atenuación de 14.9 dB. La Categoría 3 fue un formato popular de cableado entre administradores de redes en los comienzos de los noventa, pero cayó en popularidad frente al similar pero superior estándar de Cable UTP de Categoría 5.

Figura 3.7. Cable UTP cat3*

- UTP categoría 4: Esta definido para redes de ordenadores tipo anillo como Token Ring con un ancho de banda de hasta 20 Mhz y con una velocidad de 20 Mbps. El cable esta compuesto por cuatro pares trenzados de hilo de cobre. Fue rápidamente reemplazado por el Cable UTP de Categoría 5/5e, debido a su superioridad.

Figura 3.6. Tomada de la dirección siguiente www.usuarioindignado.com
Figura 3.7. Tomada de la dirección siguiente www.animeandcomputers.com

Figura 3.8. Cable UTP cat4*

- UTP categoría 5: Trabajan a una velocidad de hasta 100 Mbps, con un ancho de banda de 100 MHz. Se utiliza en las comunicaciones en redes LAN. Estos cables pueden ser blindados o sin blindar. Tienen 4 pares trenzados de sección AWG24, un aislamiento del conductor de polietileno de alta densidad de 1,5 mm de diámetro, una cubierta de PVC gris, Soporta aplicaciones Gigabit Ethernet.

  La atenuación de este cable depende de la velocidad:

  Velocidad de 4 Mbps → Atenuación de 13 dB
  Velocidad de 10 Mbps → Atenuación de 20 dB (Ethernet)
  Velocidad de 16 Mbps → Atenuación de 25 dB (Token Ring)
  Velocidad de 100 Mbps → Atenuación de 67 dB (Fast Ethernet)

Figura 3.9. Cable UTP cat5*

- UTP Categoría 5e: Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Puede alcanzar velocidades de transmisión de hasta 1Gbs con electrónica especial.

Figura 3.8. Tomada de la dirección siguiente www.pan.fotovista.com
Figura 3.9. Tomada de la dirección siguiente www.todoportatil.com.ve

Figura 3.10. Cable UTP cat5e*

- UTP Categoría 6: Es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es *backward compatible* (compatible con versiones anteriores) con los estándares de Categoría 5/5e y Categoría 3. La Categoría 6 posee características y especificaciones para crosstalk y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (*Gigabit Ethernet*). Tiene un ancho de banda de 250 MHz en cada par. Puede alcanzar velocidades de transmisión de 1Gbps. El cable contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores. Los cables UTP de Categoría 6 son con cable calibre 2*3AWG*. El largo máximo de un cable UTP Cat-6 horizontalmente es de 90 metros (295 pies).

Figura 3.11. Cable UTP cat6*

- UTP Categoría 6A: La especificación ANSI/TIA/EIA-568-B.2-10 indica sistemas de cables llamados Categoría 6 Aumentada "Categoría 6A". La TIA aprobó una nueva especificación estándar de rendimiento mejorados para sistemas con cables trenzados no apantallados (*unshielded*) y cables trenzados apantallados (*Foiled*) que operan a frecuencias de hasta 500 MHz con velocidades de transmisión de hasta 10 Gbps. Soporta una distancia máxima de 100 metros.

Figura 3.10. Tomada de la dirección siguiente www.estec.cl
Figura 3.11. Tomada de la dirección siguiente www.todoportatil.com.ve

Figura 3.12. Cable UTP cat6a*

- UTP Categoría 7: El Cable de Categoría 7, o Cat7, (ISO/IEC 11801:2002 categoría7/claseF), es un estándar de cable para Ethernet y otras tecnologías de interconexión y es compatible con las categorías anteriores como cat5 y cat6. Tiene un ancho de banda de 600 MHz y Puede alcanzar velocidades de transmisión superiores a 10Gbps. El Cat7 posee especificaciones aún más estrictas para crosstalk y ruido en el sistema que Cat6. Para lograr esto, se ha colocado un blindaje para los pares de cable individuales y para el cable entero. El cat7 consta de 4 pares de cables de cobre trenzados. Este cable puede ser colocado un conector eléctrico GG-45 (compatible con RJ-45) como con un conector TERA.

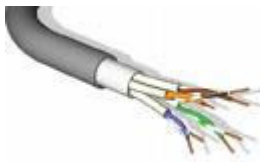


Figura 3.13. Cable UTP cat7*

3.4. ANCHO DE BANDA

El ancho de banda es la diferencia entre la frecuencia máxima y la mínima dentro de un canal. El ancho de banda determina la velocidad de transferencia de los datos por un canal. Lógicamente el ancho de banda limita en gran medida los tipos de transmisiones de cualquier información. Por ejemplo el ancho de banda para radio es lógicamente mas pequeño que el ancho de banda para la transmisión de televisión, debido a que en la transmisión de radio solo se transmite voz y en la transmisión de televisión también se transmiten imágenes. Esta es una de las razones por las que las televisiones digitales usan los satélites para sus transmisiones, estos satélites proveen un ancho de banda enorme en comparación con otros tipos de dispositivos. (Véase figura 3.14).

Figura 3.12. Tomada de la dirección siguiente www.bko.com.ar
Figura 3.13. Tomada de la dirección siguiente www.brand-rex.com

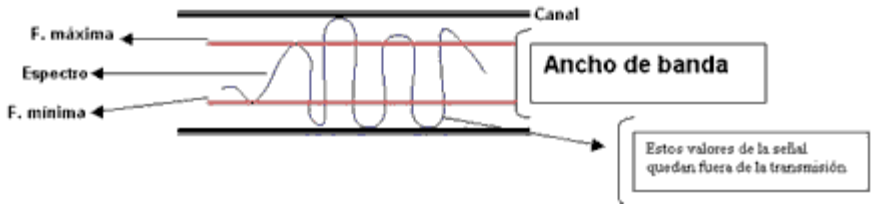


Figura 3.14. Ancho de banda*

Para señales analógicas, el ancho de banda es la anchura, medida en hercios, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Puede ser calculado a partir de una señal temporal mediante el análisis de Fourier.

¿Por qué es importante el ancho de banda?

- El ancho de banda está limitado por los componentes físicos y la tecnología de los medios.
- El ancho de banda no es gratis.
- Los requisitos de ancho de banda están creciendo a un ritmo muy rápido.
- El ancho de banda es fundamental para el rendimiento de la red.

En la siguiente tabla se puede observar las unidades de ancho de banda, su abreviatura y su equivalencia. (Véase tabla 3.1)

Tabla 3.1. Unidades de ancho de banda

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = ~1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = ~1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = ~1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = ~1,000,000,000,000 bps = 10^{12} bps

Figura 3.14. Tomada de la dirección siguiente http://www.ayuda-internet.net/tutoriales/manu-aspectosfisicos/manu-aspectosfisicos.html
Tabla 3.1. Tomada de la bibliografía siguiente Andrew S. Tanenbaum “Computer Networks”, Third Edition, Prentice Hall, 1996

El ancho de banda depende del medio por el que se transmite al igual que de la máxima distancia de cobertura que se requiera; Como se muestra en la tabla 3.2

Tabla 3.2. Ancho de banda y medio de transmisión

Some Typical Media	Bandwidth	Max. Physical Distance
50-Ohm Coaxial Cable (Ethernet 10BASE2, ThinNet)	10-100 Mbps	185m
50-Ohm Coaxial Cable (Ethernet 10BASE5, ThickNet)	10-100 Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 10BASE-T)	10 Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 100BASE-TX)(Fast Ethernet)	100 Mbps	100m
Multimode (62.5/125μm) Optical Fiber 100BASE-FX	100 Mbps	2000m
Singlemode (9/125μm core) Optical Fiber 1000BASE-LX	1000 Mbps (1.000 Gbps)	3000m
Wireless	11 Mbps	a few 100meters

3.5. DISPOSITIVOS DE CONECTIVIDAD

El dispositivo de comunicación más básico de conectividad entre redes es el módem.

Los módems se han convertido en dispositivos habituales y constituyen el equipamiento estándar en la mayoría de los equipos que se venden hoy en día. En realidad, cualquiera que haya utilizado Internet o un PC-fax, ha utilizado un módem. Además de los módems, también se utilizan otros dispositivos para conectar pequeñas LAN en una red de área extensa (WAN). Cada uno de estos dispositivos tiene su propia funcionalidad junto con algunas limitaciones. Simplemente, se pueden utilizar para extender la longitud del medio de red o para proporcionar acceso a una red mundial en Internet. Los dispositivos utilizados para extender las LAN incluyen repetidores, *bridges* (puentes), *routers* (encaminadores), *brouters* (b-encaminadores) y *gateways* (pasarelas).

Tabla 3.2. Tomada de la bibliografía siguiente Andrew S. Tanenbaum “Computer Networks”, Third Edition, Prentice Hall, 1996

3.5.1. Tecnología de módems

Un módem es un dispositivo que permite a los equipos comunicarse a través de una línea telefónica.

Cuando los equipos están demasiado alejados como para conectarse a través de un cable estándar, se puede llevar a cabo la comunicación entre ellos mediante un *módem*. En un entorno de red, los módems actúan como un medio de comunicación entre redes y como una forma de conectar el mundo que existe más allá de la red local.

3.5.2. Funciones básicas de un módem

Los equipos no se pueden conectar a través de una línea telefónica, puesto que éstos se comunican enviando pulsos electrónicos digitales (señales digitales) y una línea telefónica sólo puede enviar ondas analógicas (sonido).

Una señal digital tiene un formato binario. La señal puede tener un valor de 0 ó 1. Una señal analógica se puede representar como una curva suavizada que puede representar un rango infinito de valores.

El módem que se encuentra en el PC emisor convierte las señales digitales en ondas analógicas y transmite estas ondas analógicas a través de la línea telefónica. El módem que recibe la señal, convierte las señales analógicas que le llegan en señales digitales para que las reciba el PC, como se puede observar en la figura 3.15

En otras palabras, un módem emisor *MO*dula las señales digitales en señales analógicas y un módem receptor *DE*modula las señales que recibe en señales digitales.

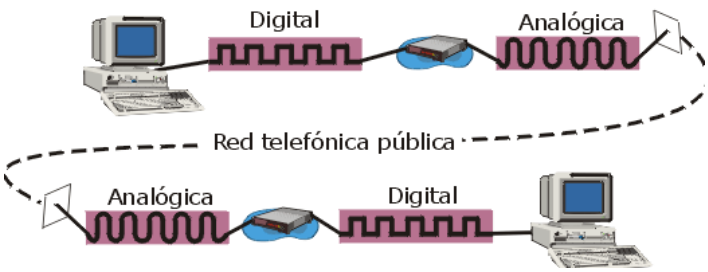


Figura 3.15. Comunicación a través de modems

Figura 3.15. Tomada de la dirección siguiente http://fmc.axarnet.es/redes/tema_07.htm

Tipos de módems

Debido a los distintos entornos de comunicación se requieren diferentes métodos de envío de datos. Estos entornos se pueden dividir en dos áreas relacionadas con el ritmo de las comunicaciones:

- Asíncrona.
- Síncrona.

El tipo de módem que utiliza una red depende de si el entorno es asíncrono o síncrono.

3.6. CABLEADO ESTRUCTURADO

Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus. Las características e instalación de estos elementos se deben hacer en cumplimiento de estándares para que califiquen como cableado estructurado. El apego de las instalaciones de cableado estructurado a estándares trae consigo los beneficios de independencia de proveedor y protocolo (infraestructura genérica), flexibilidad de instalación, capacidad de crecimiento y facilidad de administración.

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

El tendido de cable para una red de área local tiene cierta complejidad cuando se trata de cubrir áreas extensas tales como un edificio de varias plantas. En este sentido hay que tener en cuenta las limitaciones de diseño que impone la tecnología de red de área local que se desea implantar:

- La segmentación del tráfico de red.
- La longitud máxima de cada segmento de red.
- La presencia de interferencias electromagnéticas.
- La necesidad de redes locales virtuales.

Salvando estas limitaciones, la idea del cableado estructurado es simple:

- Tender cables en cada planta del edificio.
- Interconectar los cables de cada planta.

Cableado horizontal o "de planta"

En cada planta se instalan las rosetas (terminaciones de los cables) que sean necesarias en cada dependencia. De estas rosetas parten los cables que se tienden por el suelo (o por el techo) de la planta.

Todos los cables se concentran en el denominado **armario de distribución de planta** o **armario de telecomunicaciones**. Se trata de un bastidor donde se realizan los empalmes de unos cables con otros. En algunos casos, según el diseño que requiera la red, puede tratarse de un elemento activo o pasivo de comunicaciones, es decir, un hub o un switch. En cualquier caso, este armario concentra todos los cables procedentes de una misma planta.

En el cableado estructurado que une los terminales de usuario con los distribuidores de planta no se podrán realizar empalmes.

Este subsistema comprende el conjunto de medios de transmisión (cables, fibras, coaxiales, entre otros.) que unen los puntos de distribución de planta con el conector o conectores del puesto de trabajo. Ésta es una de las partes más importantes a la hora del diseño debido a la distribución de los puntos de conexión en la planta, que no se parece a una red convencional.

Cableado vertical, troncal o backbone

Hay que interconectar todos los armarios de distribución de planta mediante otro conjunto de cables que deben atravesar verticalmente el edificio de planta a planta.

Esto se hace a través de las canalizaciones existentes en el edificio. Si esto no es posible, es necesario habilitar nuevas canalizaciones, aprovechar aberturas existentes (huecos de ascensor o escaleras), o bien, utilizar la fachada del edificio (poco recomendable).

En los casos donde el armario de distribución ya tiene los empalmes de red, el cableado vertical cumple la función de red troncal. Teniendo en cuenta que éste integra el ancho de banda de todas las plantas. Por lo tanto, suele utilizarse otra tecnología con mayor capacidad. Por ejemplo, FDDI o Gigabit Ethernet.

Cuarto principal de equipos y de entrada de servicios

El cableado vertical acaba en una sala donde, de hecho, se concentran todos los cables del edificio. Aquí se sitúa la electrónica de red y otras infraestructuras de telecomunicaciones, tales como pasarelas, puertas de enlace, cortafuegos, central telefónica, recepción de TV por cable o satélite, entre otras.

Subsistemas de Cableado Estructurado

El cableado estructurado está compuesto de varios subsistemas:

- Sistema de cableado vertical.
- Sistema de cableado horizontal.
- Salida de área de trabajo.
- Cuarto o espacio de telecomunicaciones.
- Cuarto o espacio de equipo.
- Cuarto o espacio de entrada de servicios.
- Administración, etiquetado y pruebas.
- Sistema de puesta a tierra para telecomunicaciones.

Normas 568-A y 568-B

La primera revisión del estándar, TIA/EIA-568-A.1-1991, se emitió en 1991 y fue actualizada en 1995. La demanda comercial de sistemas de cableado aumentó fuertemente en aquel período, debido a la aparición de los ordenadores personales y las redes de comunicación de datos, y a los avances en estas tecnologías. El desarrollo de cables de pares cruzados de altas prestaciones y la popularización de los cables de fibra óptica, conllevaron cambios importantes en el estándar, que fue sustituido por el actual conjunto de estándares TIA/EIA-568-B

ANSI/TIA/EIA-568-A (Alambrado de Telecomunicaciones para Edificios Comerciales) El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán.

La norma ANSI/TIA/EIA-568-A publicada en Octubre de 1995 amplia el uso de Cable de Par Trenzado (UTP) y elementos de conexión para aplicaciones en Redes de Área Local (LAN) de alto rendimiento. La edición de la ANSI/TIA/EIA-568-A integra los Boletines Técnicos de Servicio TSB 36 y TSB 40 los cuales prolongan el uso de Cable de Par Trenzado (UTP) en un ancho de banda de hasta 100 MHz.

Esta norma guía la selección de sistemas de cableado al especificar los requisitos mínimos de sistemas y componentes, y describe los métodos de pruebas de campo necesarios para satisfacer las normas.

El contenido de 568-B.3 se refiere a los requerimientos de rendimiento mecánico y de transmisión del cable de fibra óptica, hardware de conexión, y cordones de conexión, incluyen el reconocimiento de la fibra multi-modo y el uso de conectores de fibra de factor de forma pequeño (Small Form Factor - SFF).

La decisión de TIA de publicar la norma 568-B.3 antes de terminar las normas 568-B.1 y 568-B.2 fue motivada por la necesidad de crear conciencia en la industria de las nuevas especificaciones de componentes de fibra. Los temas en las partes uno y dos incluyen la adaptación del modelo de enlace permanente y mejoramiento en precisión de medidas.

Propósito del Estándar EIA/TIA 568-A:

- Establecer un cableado estándar genérico de telecomunicaciones que respaldará un ambiente multiproveedor.
- Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
- Establecer un criterio de ejecución y técnico para varias configuraciones de sistemas de cableado

El estándar especifica:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina
- Topología y distancias recomendadas
- Parámetros de medios de comunicación que determinan el rendimiento
- La vida productiva de los sistemas de telecomunicaciones por cable por más de 10 años (15 actualmente)

TIA/EIA 568-B.3

- Cables de fibra
    - Se reconoce la fibra de 50 mm
    - Se reconocen tanto la fibra multimodo como la monomodo para el área de trabajo
- Conectores de fibra
    - El conector 568SC duplex permanece como estándar en el área de trabajo
    - Otros tipos de conectores pueden ser usados en otro sitios
    - Deben cumplir el estándar de inter apareamiento de TIA/EIA (FOCIS)

Subsistemas de la norma ANSI/TIA/EIA-568-A

De acuerdo a la norma, un sistema de cableado estructurado consiste de 6 subsistemas funcionales:

1. Instalación de entrada, o acometida, es el punto donde la instalación exterior y dispositivos asociados entran al edificio. Este punto puede estar utilizado por servicios de redes públicas, redes privadas del cliente, o ambas. Este es el punto de demarcación entre el portador y el cliente, y en donde están ubicados los dispositivos de protección para sobrecargas de voltaje.
2. El cuarto, local, o sala de máquinas o equipos es un espacio centralizado para el equipo de telecomunicaciones (PBX, equipos de cómputo, conmutadores de imagen, entre otros.) que da servicio a los usuarios en el edificio.
3. El eje de cableado central proporciona interconexión entre los gabinetes de telecomunicaciones, locales de equipo, e instalaciones de entrada. Consiste de cables centrales, interconexiones principales e intermedias, terminaciones mecánicas, y puentes de interconexión. Los cables centrales conectan gabinetes dentro de un edificio o entre edificios.

4. Gabinete de telecomunicaciones es donde terminan en sus conectores compatibles, los cables de distribución horizontal. Igualmente el eje de cableado central termina en los gabinetes, conectado con puentes o cables de puenteo, a fin de proporcionar conectividad flexible para extender los diversos servicios a los usuarios en las tomas o salidas de telecomunicaciones.
5. El cableado horizontal consiste en el medio físico usado para conectar cada toma o salida a un gabinete. Se pueden usar varios tipos de cable para la distribución horizontal. Cada tipo tiene sus propias limitaciones de desempeño, tamaño, costo, y facilidad de uso.
6. El área de trabajo, sus componentes llevan las telecomunicaciones desde la unión de la toma o salida y su conector donde termina el sistema de cableado horizontal, al equipo o estación de trabajo del usuario. Todos los adaptadores, filtros, o acopladores usados para adaptar equipo electrónico diverso al sistema de cableado estructurado, deben ser ajenos a la toma o salida de telecomunicaciones, y están fuera del alcance de la norma 568-A

3.7. SIMULACIONES DE PRÁCTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

3.7.1. Explicación del software Packet Tracer 4.0

El software 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 uso para un usuario novato o intermedio como se puede ver en la figura 3.16

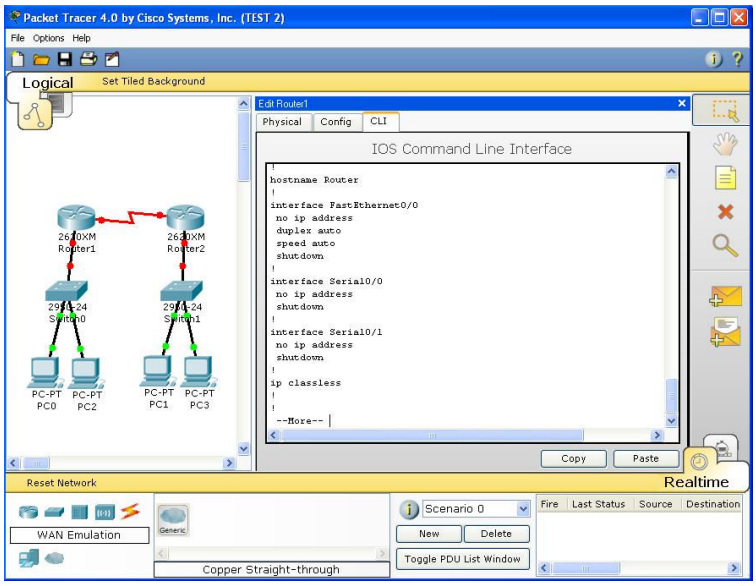


Figura 3.16. Software Packet Tracer

- El software Packet Tracer contiene los siguientes elementos para realizar su simulación:
  - Dispositivos
  - Conexiones
  - Protocolos de enrutamiento
  - Encapsulamiento OSI
  - Condición del enlace
  - Guardar Archivos

- El software Packet Tracer realiza visualización, simulación y animación
  - Creando/conectando dispositivos
  - Removiendo dispositivos/conexiones
  - Creando descripción de redes
  - Locking/unlocking la caja de información

- El software packet tracer 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 3.2

- 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 4.0

- 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

3.7.2 Laboratorios

3.7.2.1. Guía de practica: Interconexión de dos CPU´s utilizando cable cruzado

Correr la simulación correspondiente que se encuentra en el siguiente enlace CAPITULO III\cable cruzado.pka

Objetivo

Conseguir la transferencia de paquetes entre las dos CPU´s.

Procedimiento

1. Iniciar con el software Packet Tracer 4.0. Como se indica en la figura 3.17.

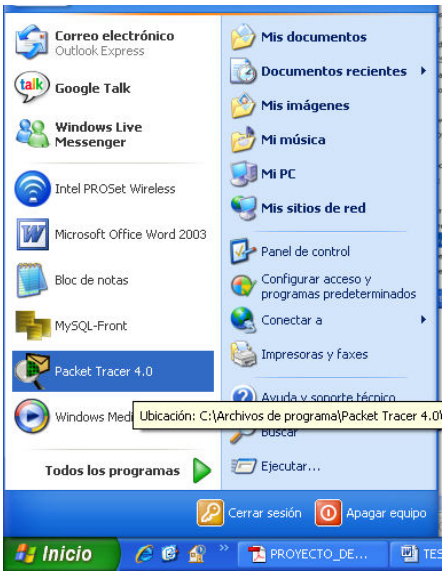


Figura 3.17. Inicio del software Packet Tracer

2. Primero debemos configurar la dirección IP y su respectiva mascara de red para la primera PC, para ello procedemos a dar un clic en la primera CPU para lo cual se abre una pantalla de configuración como se indica en la figura 3.18

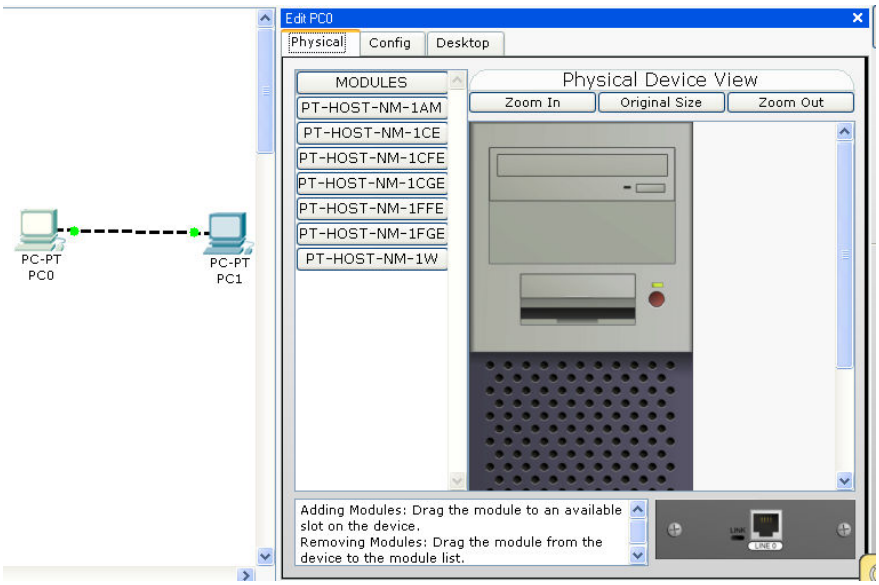


Figura 3.18. Edit PC0

3. En la pantalla que aparece debemos 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 observa en la figura 3.19

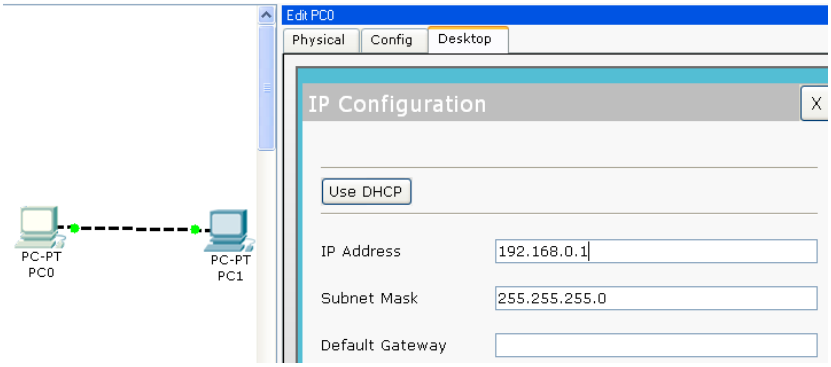


Figura 3.19. PC0

4. Procedemos con la configuración de la dirección IP y su respectiva mascara de red de la segunda PC como se puede observar en la siguiente figura 3.20

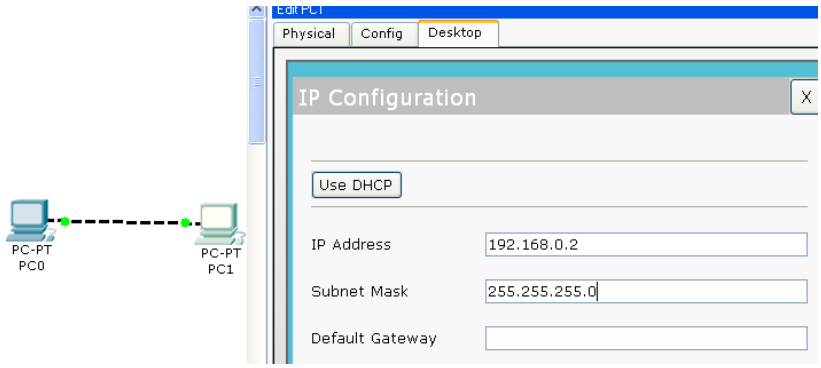


Figura 3.20. PC1

Desarrollo

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 al enviar y recibir los datos, como se puede observar en la figura 3.21

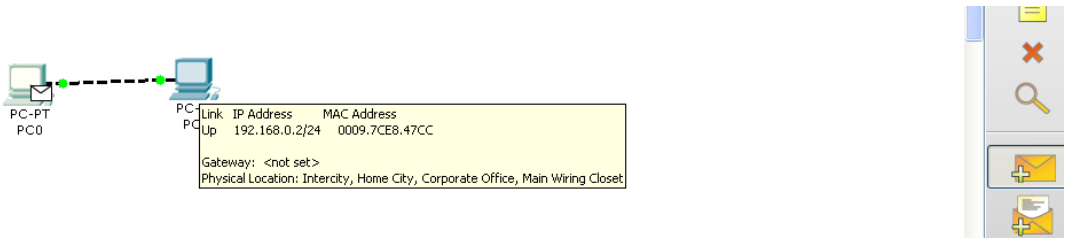


Figura 3.21. Colocación de paquete

2. Procederemos con la respectiva simulación enviando un paquete y comprobando que la conexión correspondiente esta funcionando correctamente, En la figura 3.22 se puede observar claramente como el paquete se traslada de la PC0 a la PC1 sin poseer ningún inconveniente.

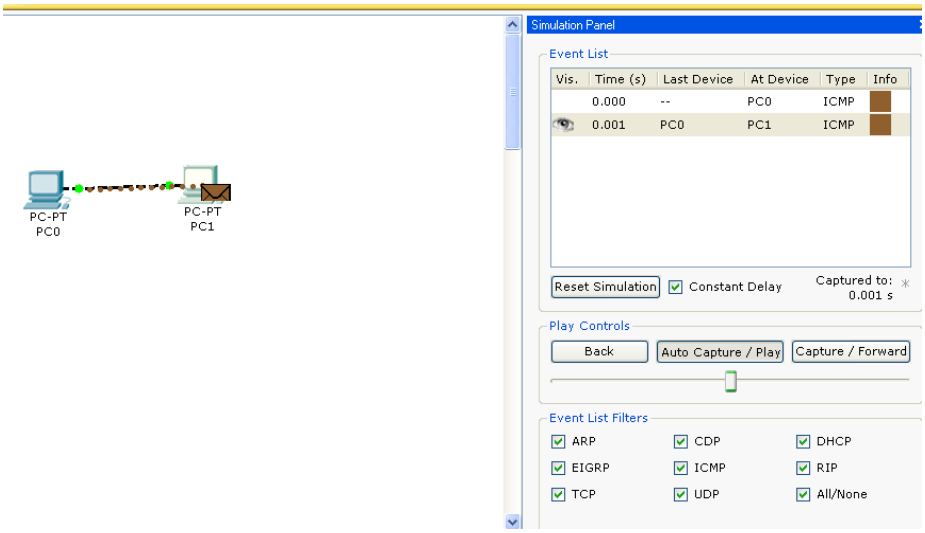


Figura 3.22. Simulación 1

3. En la figura 3.23 se puede observar claramente que el paquete regreso de la PC1 a la PC0 sin obtener ningún problema

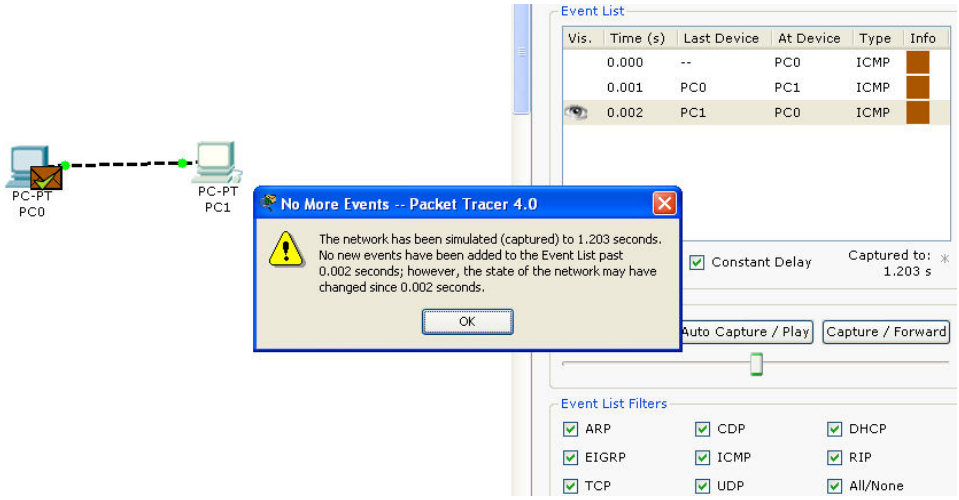


Figura 3.23. Simulación 2

Análisis de resultados

1. Al realizar la simulación para la conexión de dos CPU´s se debe tener muy en cuenta que las dos CPU´s deben estar en la misma red, caso contrario no se podrían enviar ninguna información.

2. En la figura 3.23 se puede observar muy claramente que el paquete regreso al punto de partida, significando que la información fue entregada sin ningún problema a su destino.

Conclusiones

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

2. Con la simulación realizada se cumplieron los objetivos requeridos

3.8. PRUEBAS DE OPCIÓN MÚLTIPLE

El banco de preguntas correspondiente al capitulo se encuentra en anexos.

Para realizar las pruebas de selección múltiple correspondientes a este capitulo se debe correr el programa que se encuentra en el siguiente vinculo index.html, o en http://www.fie-espe.edu.ec/preguntas y luego procedemos a ingresar los datos del alumno que va a realizar la prueba como se muestra en la figura 3.24

Figura 3.24. Datos Alumno

Para ingresar a resolver la prueba debemos elegir el capitulo que se va a realizar como se muestra en la figura 3.25 o se debe ingresar a la plantilla de preguntas e elegir igualmente el capitulo deseado.

Figura 3.25. Prueba Capitulo 3

El siguiente paso es realizar la prueba de selección múltiple como se indica en la figura 3.26. Luego de haber respondido a todas las preguntas se procede hacer clic sobre Corregir Prueba para que la prueba sea calificada y corregida automáticamente como se muestra en la figura 3.27.

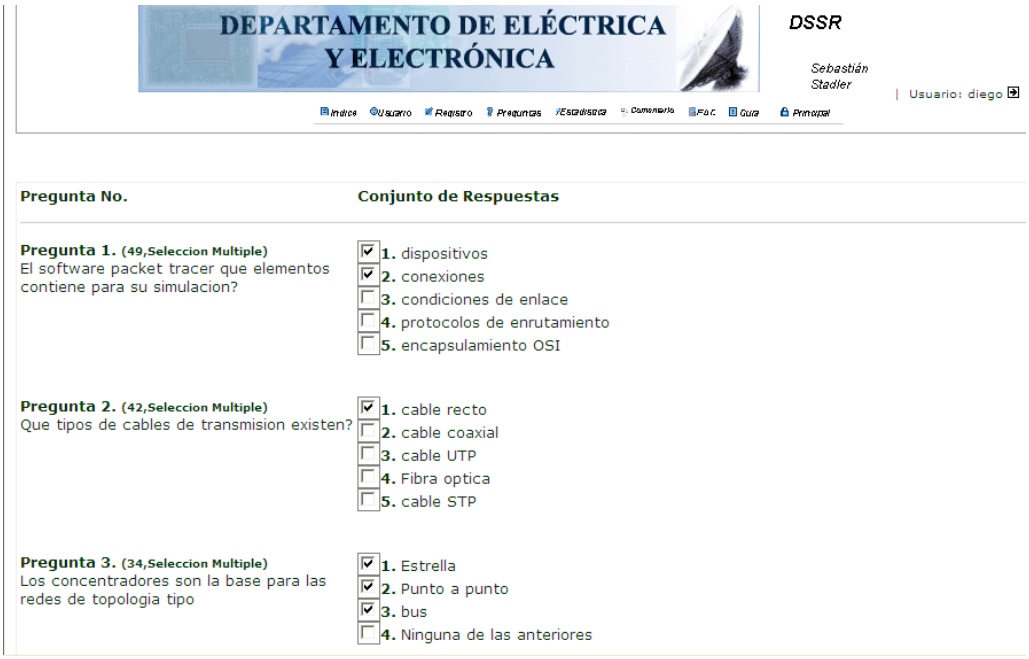


Figura 3.26. Prueba selección múltiple

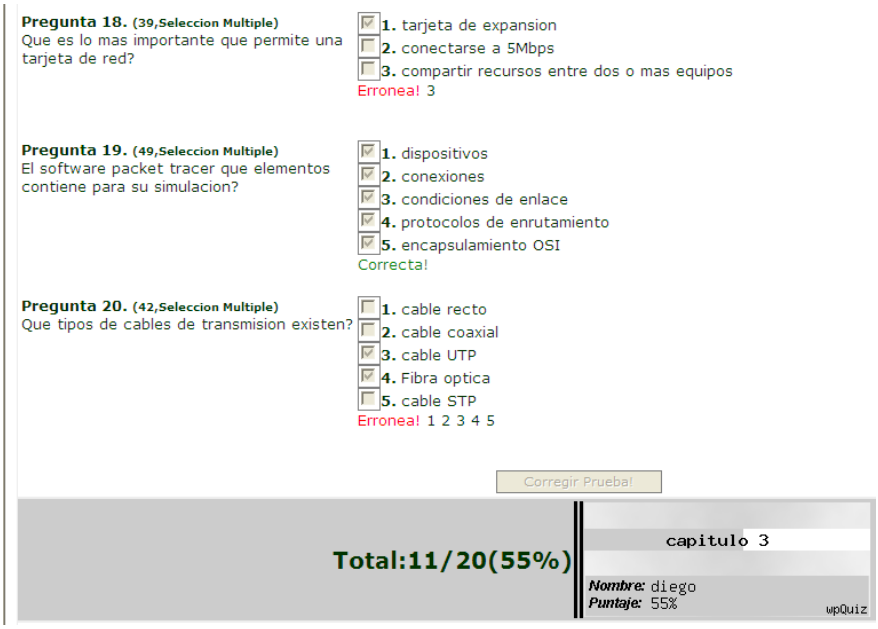


Figura 3.27. Calificación Prueba

CAPITULO IV

REDES LAN

REDES DE ÁREA LOCAL (LAN)

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

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

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.

4.1. 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:

4.1.1. 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)

4.2. 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.

Cables

  - **10Base5** (Ethernet gruesa). Usa un cable coaxial grueso y tiene una velocidad de 10 Mbps.
  - **10Base2** (Ethernet delgada). Usa un cable coaxial delgado. Se hacen las conexiones usando conectores T, que son más fáciles para instalar y más confiables.
  - **10Base-T.** Simplifica la ubicación de rupturas. Cada estación tiene una conexión con un *hub*.
  - **10Base-F.** Usa la fibra óptica. Es cara pero buena para las conexiones entre edificios.

4.3. 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 posee 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 cuál 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).

4.4. 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 este usando en ese precioso momento (Carrier-Sense). Esto se oye muy sencillo, pero el problema reside en que dos o más computadoras al escuchar que no se esta 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 10 Mbps 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 10 Mbps por Banda Base en un cableado que puede alcanzar 500 metros. El cableado es grueso y es utilizado principalmente para grandes 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 10 Mbps 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.

4.5. 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 4.1 se puede observar las redes inalámbricas.

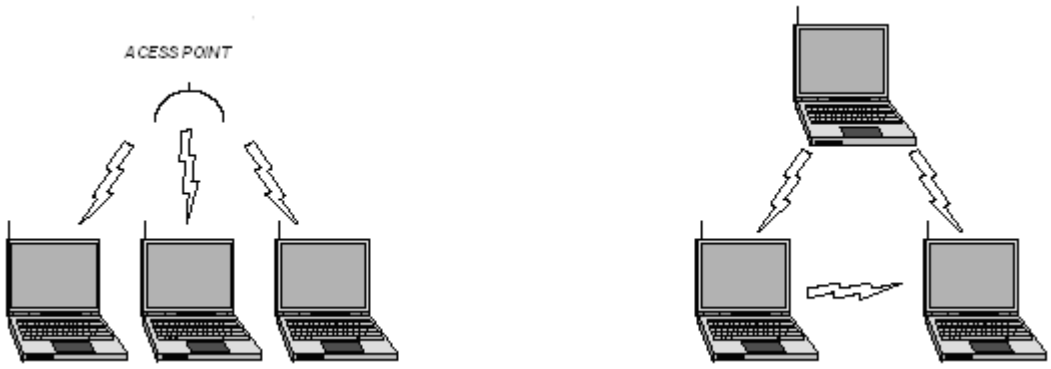


Figura 4.1. Redes inalámbricas

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. 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 múltiplexación 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 múltiplexación ortogonal por división de frecuencia (OFDM).

4.6. CSMA/CA

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

En las redes inalámbricas tenemos dos puntos importantes:

- 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.

4.7. ESTRUCTURA DE LA TRAMA ETHERNET

La trama Ethernet

En la tabla 4.1 se muestra la estructura de trama Ethernet:

Tabla 4.1. Estructura de la trama Ethernet

Campo	Tamaño (Bytes)
Hueco entre tramas	(12)
Preámbulo	7
Delimitador inicio de trama	1
Dirección de destino	6
Dirección de origen	6
Protocolo/Longitud	2
Datos	0-1500
Relleno	0-46
Secuencia de comprobación(CRC)	4

El hueco entre tramas es un período de tiempo en que no se transmite nada, de longitud equivalente a 12 bytes (96 ns a 10 Mb/s) que sirve para separar las tramas. Este hueco entre tramas es el mecanismo empleado en Ethernet para detectar cuando termina la trama anterior, ya que el campo longitud puede no existir y aunque exista no se utilizará en tiempo de captura para averiguar el fin de la trama. El hueco también permite al receptor tomarse un respiro para realizar diversas tareas de mantenimiento (transvase de buffers de la interfaz de red al host, interrupciones a la CPU, etc.) antes de volver a la escucha para capturar la trama siguiente. Para asegurar que se respeta el hueco cuando una estación que va a transmitir detecta el medio libre espera el tiempo equivalente a 12 bytes antes de empezar a transmitir el preámbulo.

El preámbulo está formado por la secuencia 10101010 repetida siete veces, y el delimitador de inicio por la secuencia 10101011. Al ser transmitidos con codificación Manchester a 10Mb/s estos ocho bytes generan una onda cuadrada de 5MHz durante 6,4ms, lo cual permite a los demás ordenadores sincronizar sus relojes con el emisor.

El último bit del delimitador de inicio de trama marca el final del preámbulo y el comienzo de ésta.

Los campos dirección de destino y origen contienen la conocida dirección MAC IEEE de 6 bytes.

El campo protocolo/longitud se interpreta como protocolo cuando el valor es superior a 1536, y como longitud en caso contrario. El primer caso corresponde al antiguo formato DIX, y el segundo al formato 802.3 (actualmente el estándar 802.3 acepta ambos significados).

El campo datos puede tener una longitud entre 0 y 1500 bytes. Cuando su longitud es menor de 46 bytes se añade un relleno para asegurar que la longitud de la trama no es menor de 64 bytes (la trama propiamente dicha abarca desde el campo dirección de destino al CRC, ambos inclusive).

La secuencia de comprobación es un CRC de 32 bits basado en un generador polinómico de grado 32.

Como ya se ha comentado la longitud mínima de trama y la velocidad de la red fijan el diámetro de una Ethernet. De haber mantenido la trama mínima de 64 bytes en Gigabit Ethernet el diámetro máximo habría sido de unos 45ms, inaceptable en la mayoría de situaciones. Para evitar esto la trama Gigabit Ethernet incorpora un segundo relleno denominado extensión de portadora que se añade al final de la trama para garantizar que la longitud mínima nunca sea inferior a 512 bytes (4096 bits). Así el tiempo de ida y vuelta puede ser de hasta 4,096ms (en vez de 0,512ms) y el diámetro puede llegar a 330m. La extensión de portadora no es formalmente parte de la trama Ethernet, por lo que solo existirá mientras ésta viaje por Gigabit Ethernet. En el caso de que una trama con extensión de portadora sea transmitida a una red de 100 o 10 Mb/s la extensión de portadora se

eliminará, e inversamente, si una trama menor de 512 bytes llega a una red Gigabit Ethernet desde Fast Ethernet o Ethernet el conmutador correspondiente añadirá la extensión de portadora necesaria para que la longitud sea de 512 bytes.

4.8. VLANS

Una red de área local (LAN) esta 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 si, 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.

Tipos de VLAN

- **VLAN de puerto central**
  Es en la que todos los nodos de una VLAN se conectan al mismo puerto del switch.

- **VLAN Estáticas**
  Los puertos del switch están ya preasignados a las estaciones de trabajo.

Por puerto

Se configura por una cantidad "n" de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN.

Ventajas:

- Facilidad de movimientos y cambios.
- Microsegmentación y reducción del dominio de Broadcast.
- Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

- Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que esta conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

Por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

Ventajas:

- Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- Multiprotocolo.
- Se pueden tener miembros en múltiples VLANs.

Desventajas:

- Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLANs.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

Por protocolo

Asigna a un protocolo una VLAN. El switch se encarga dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente.

Ventajas:

- Segmentación por protocolo.
- Asignación dinámica.

Desventajas

- Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- No soporta protocolos de nivel 2 ni dinámicos.

Por direcciones IP

Esta basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

Ventajas:

- Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el switch.

Desventajas:

- El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- Perdida de tiempo en la lectura de las tablas.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

Por nombre de usuario

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

Ventajas:

- Facilidad de movimiento de los integrantes de la VLAN.
- Multiprotocolo.

Desventajas:

- En corporaciones muy dinámicas la administración de las tablas de usuarios.

VLAN Dinámicas (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

4.9. HUB Y SWITCH

4.9.1. Hub

- Son repetidores. Trabajan a nivel de la capa física regenerando la señal que reciben por un puerto y transmitiéndola por los demás.
- Son una extensión transparente del bus Ethernet.
- La función principal del Hub es la de repetir la señal que ingresa por cada una de sus “puertas” hacia todas las otras “puertas”, realizando por tanto la “difusión” que requiere Ethernet (y que se daba naturalmente en las topologías de bus sobre cables coaxiales).

- Los Hubs también monitorizan el estado de los enlaces de las conexiones a sus puertas, para verificar que la red funciona correctamente.

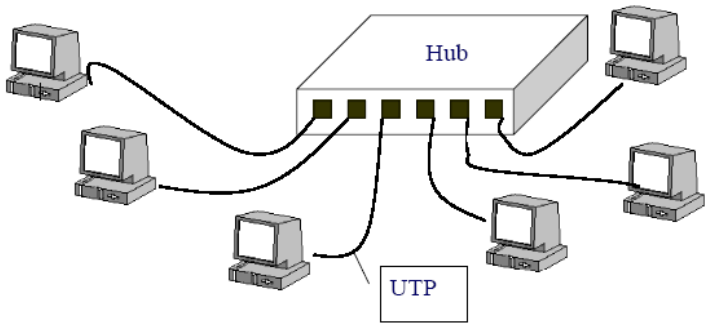


Figura 4.2. Hub

4.9.2. Switch

- Trabajan a nivel de capa 2. Reciben la trama, y luego la transmiten por el puerto que corresponde.
- Cuando una estación envía una trama el switch se graba la ubicación de dicha estación para que tramas posteriores dirigidas a ella sean enviadas solo por ese puerto, lo que mejora la eficiencia de la red. Pero los broadcasts siguen enviándose a todos los puertos.

Figura 4.3. Switch

4.10. SIMULACIONES DE PRÁCTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

4.10.1 Guía de práctica: Realizar una pequeña red LAN interconectando un switch y un hub

Correr la simulación correspondiente que se encuentra en el siguiente enlace CAPITULO IV\switch y hubs.pka

Objetivo

Conseguir la transferencia de paquetes entre las cuatro CPU´s y la impresora que se encuentra conectada en red

Procedimiento

1. Iniciar con el software Packet Tracer 4.0. Como se indica en la figura 4.4.

Figura 4.4. Inicio del software Packet Tracer

2. Primero debemos configurar la dirección IP y su respectiva mascara de red para la primera PC, para ello procedemos a dar un clic en la primera CPU para lo cual se abre una pantalla de configuración como se indica en la figura 4.5

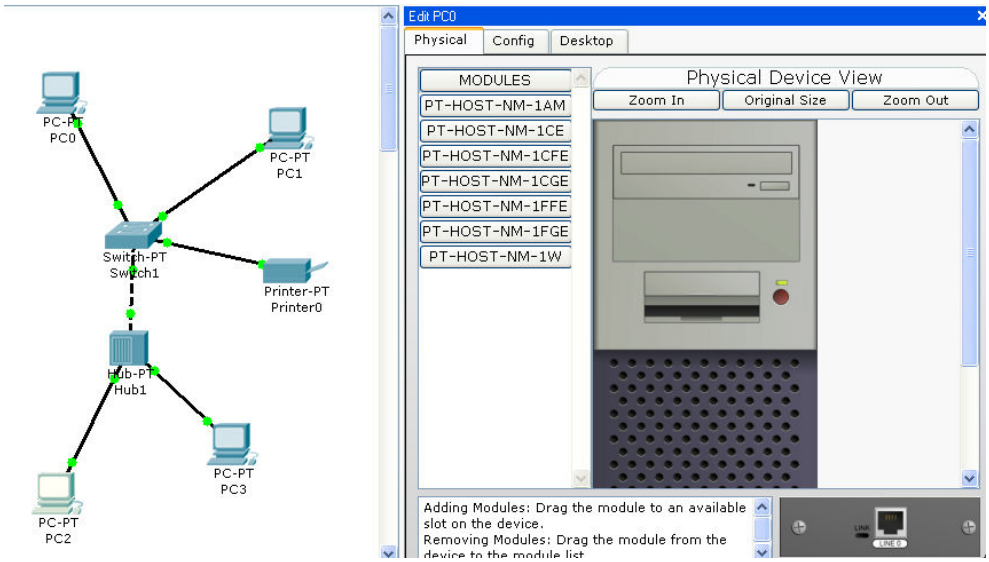


Figura 4.5. Edit PC0

3. En la pantalla que aparece debemos 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 observa en la figura 4.6

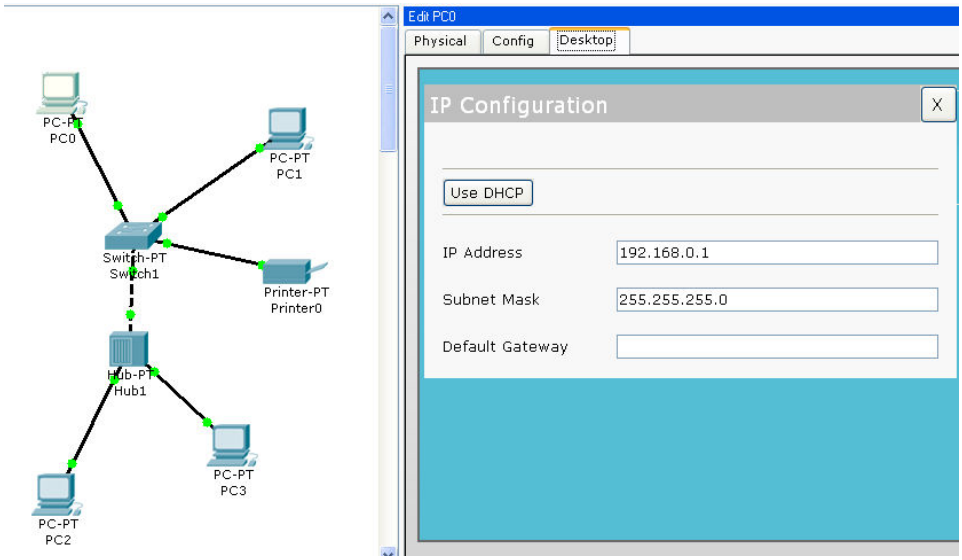


Figura 4.6. PC0

4. El mismo procedimiento será utilizado para la configuración de las siguientes tres CPU´s restantes, colocando las siguientes direcciones IP y mascaras de red como se muestran a continuación:

   - PC1
     - IP Address: 192.168.0.2
     - Subnet Mask: 255.255.255.0

   - PC2
     - IP Address: 192.168.0.3
     - Subnet Mask: 255.255.255.0

   - PC3
     - IP Address: 192.168.0.4
     - Subnet Mask: 255.255.255.0

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 4.7.

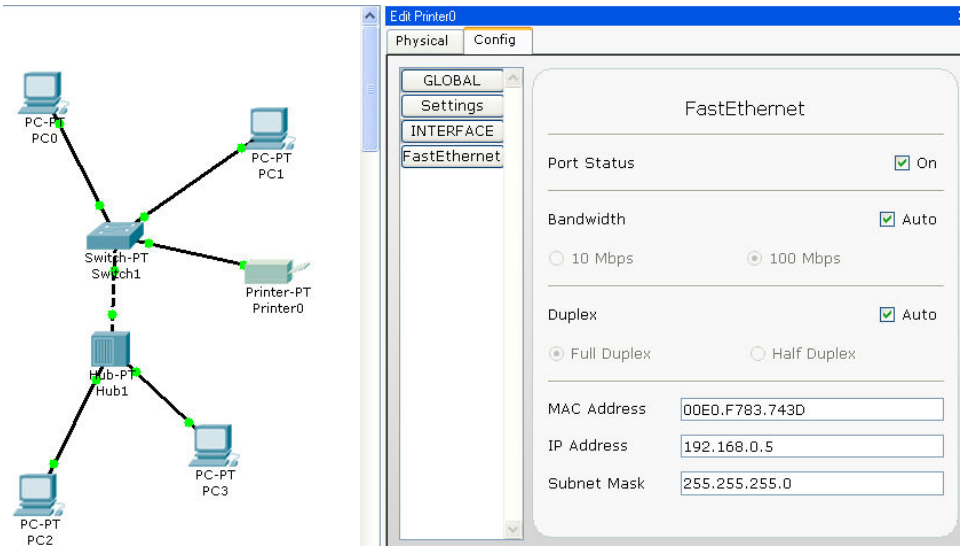


Figura 4.7. Impresora

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 4.8.

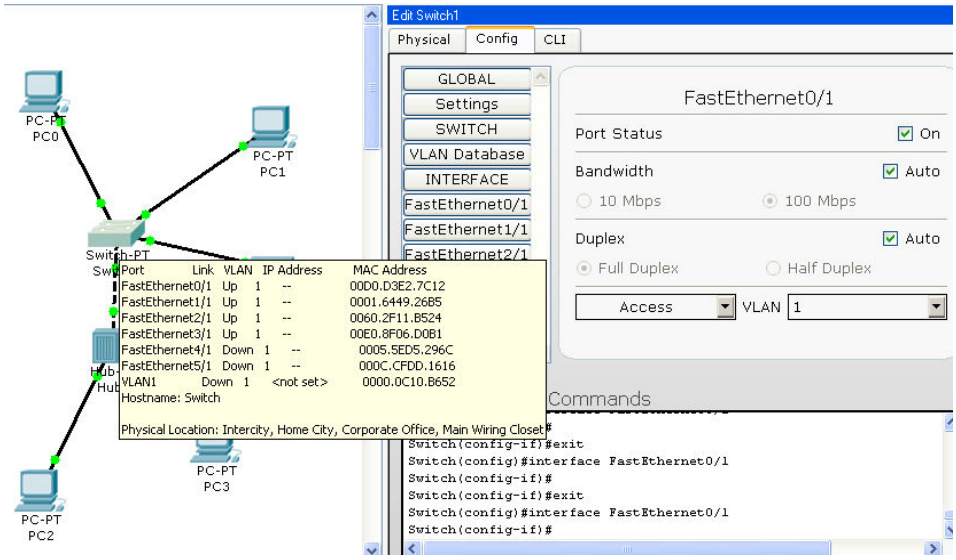


Figura 4.8. Switch1

7. Procedemos a dar un clic sobre el hub y verificamos que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 4.9.

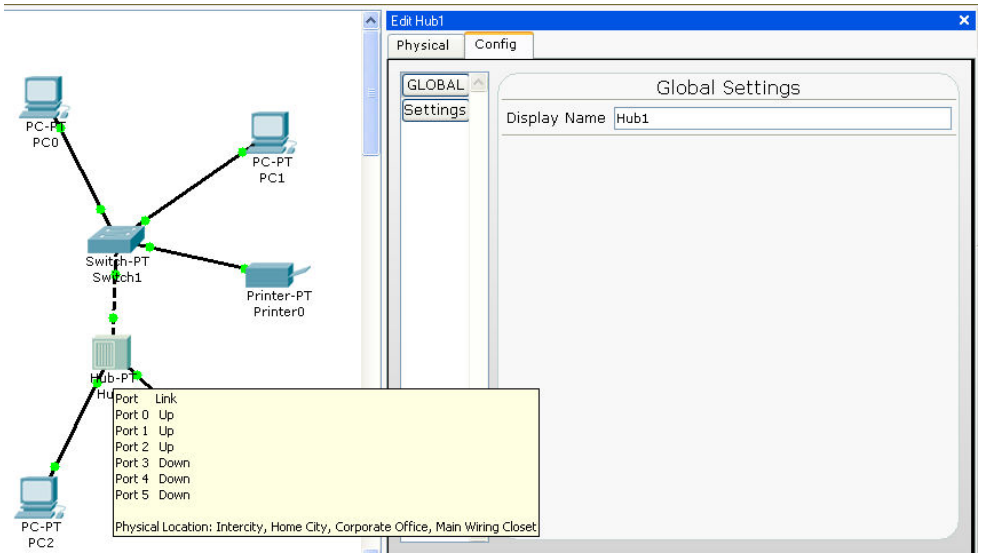


Figura 4.9. Hub1

Desarrollo

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 escenario 0 se va a comprobar la conexión entre la PC0 y la PC1 al enviar y recibir los datos, como se puede observar en la figura 4.10.

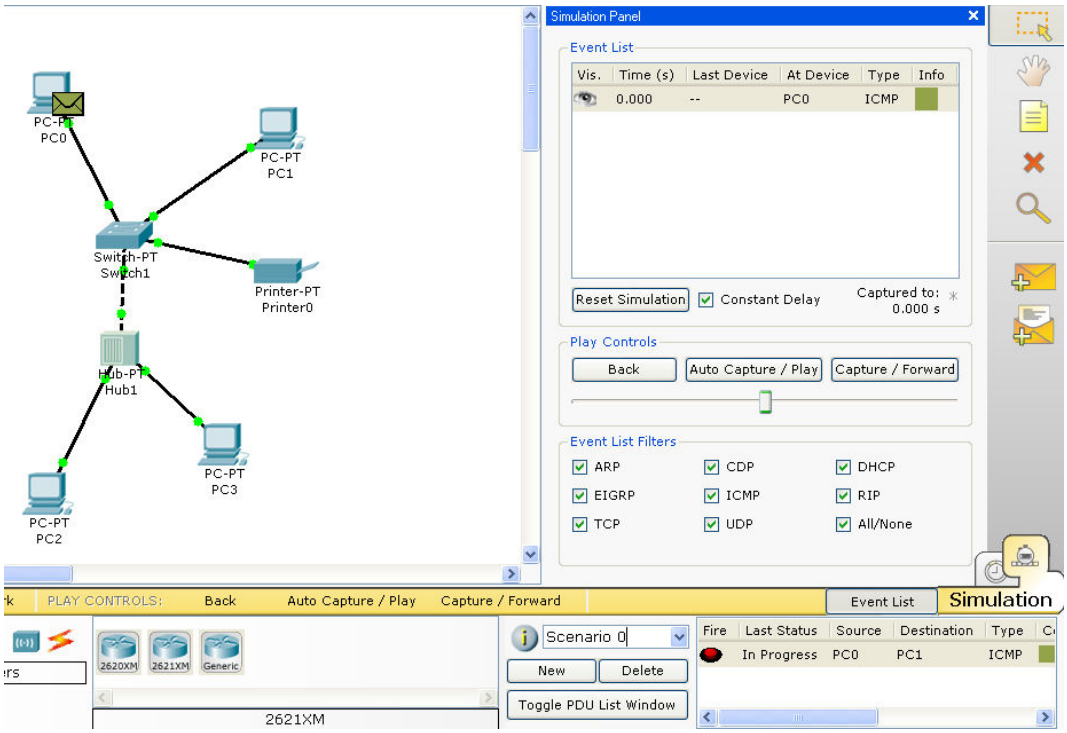


Figura 4.10. Colocación de paquete

2. Procederemos con la respectiva simulación enviando un paquete y comprobando que la conexión correspondiente esta funcionando, En la figura 4.11. se puede observar claramente como el paquete se traslada de la PC0 al Switch1 sin poseer ningún problema.

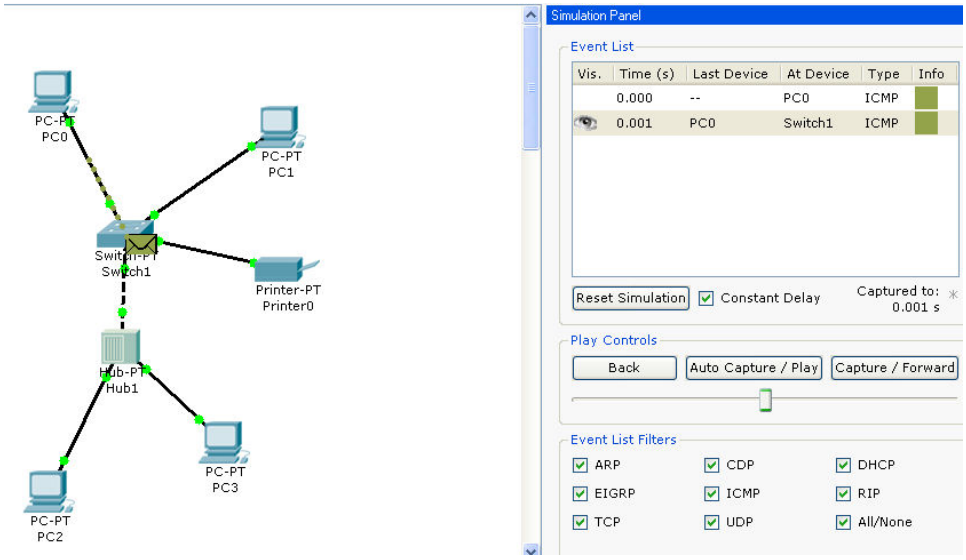


Figura 4.11. Simulación 1

3. En la figura 4.12 se puede observar claramente que el paquete se traslada del switch1 a la PC1 sin obtener ningún problema

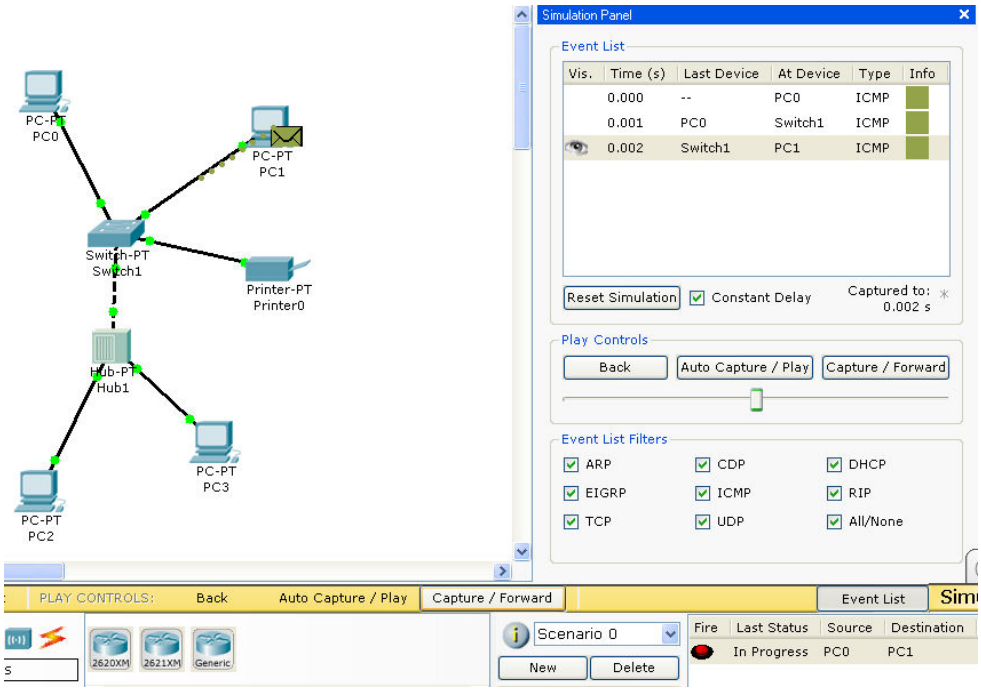


Figura 4.12. Simulación 2

4. En la figura 4.13 se puede observar claramente que el paquete se traslada del PC1 al switch1 sin obtener ningún problema

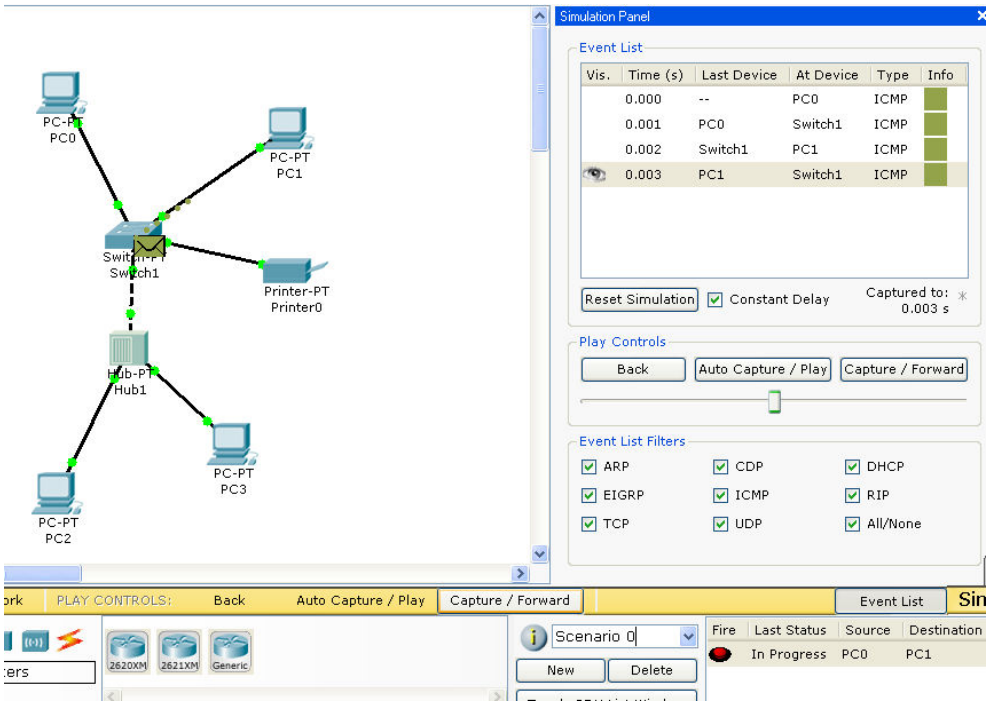


Figura 4.13. Simulación 3

5. En la figura 4.14 se puede observar claramente que el paquete regresa finalmente al PC0 sin obtener ningún inconveniente, eso significa que la información fue transmitida de la PC0 a la PC1

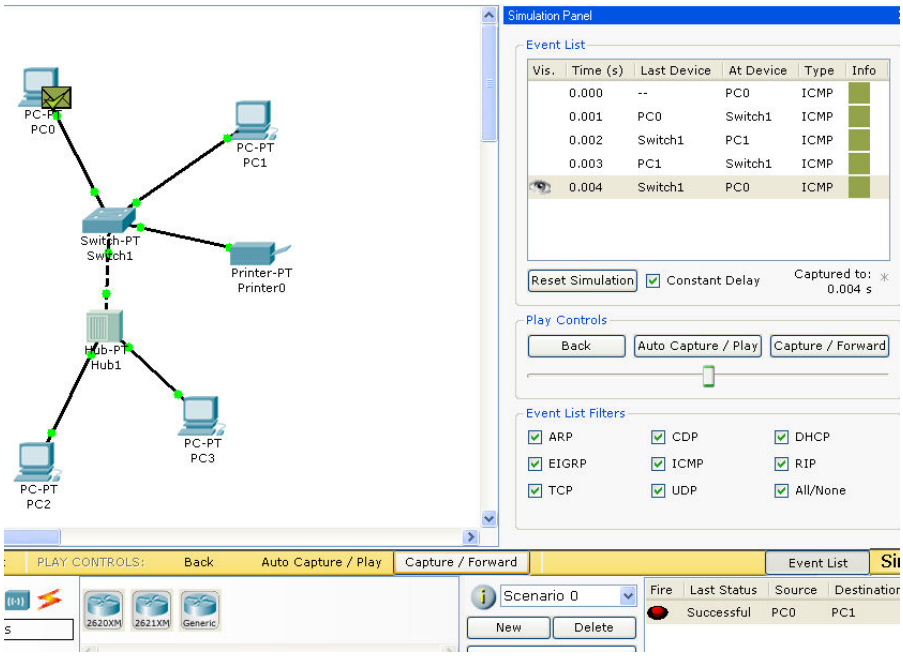


Figura 4.14. Simulación 4

6. Creamos un nuevo escenario llamado Scenario 1 en el cual colocamos un paquete simple señalando el lugar de origen que va hacer la PC2 y el lugar de destino que va hacer la impresora, de esta manera vamos a comprobar que la conexión no tenga problemas, como se puede observar en la figura 4.15.

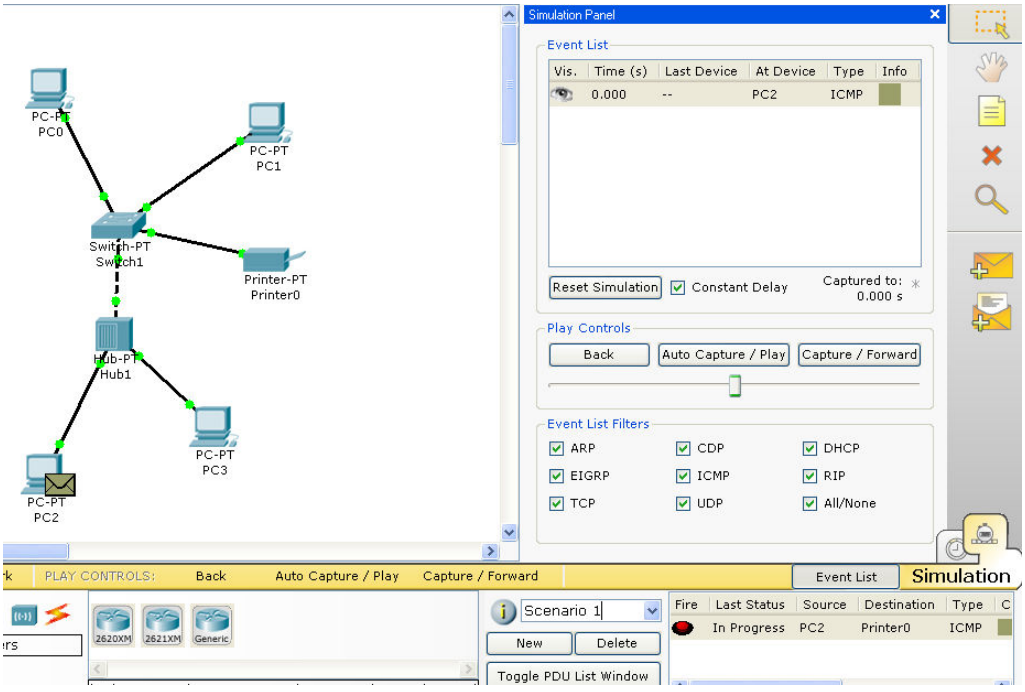


Figura 4.15. Colocación de paquete 1

7. Procederemos con la respectiva simulación enviando un paquete y comprobando que la conexión correspondiente esta funcionando, En la figura 4.16. se puede observar claramente como el paquete se traslada de la PC2 al Hub1 sin poseer ningún problema.

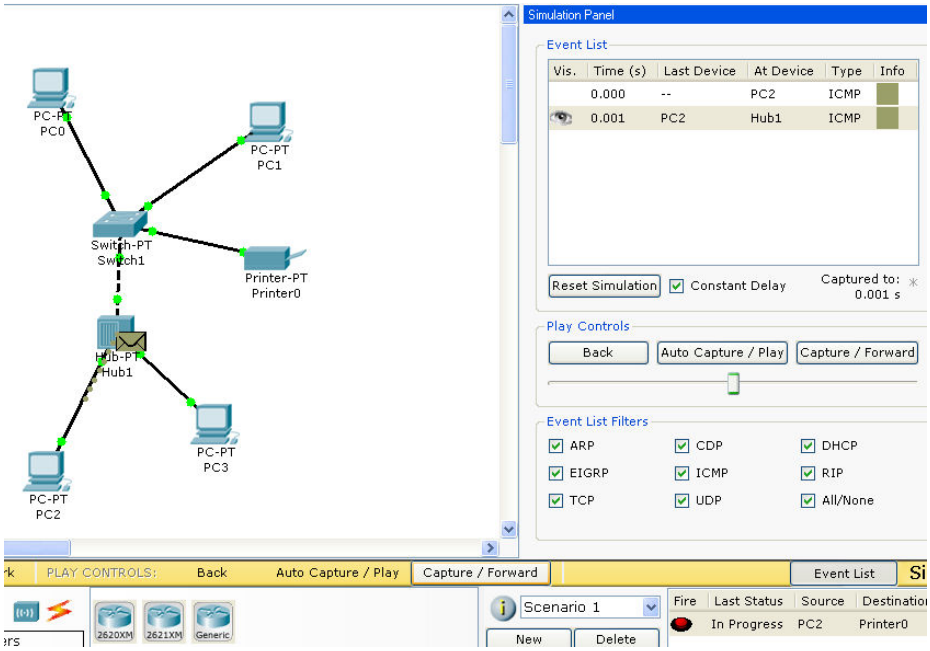


Figura 4.16. Simulación1 1

8. En la figura 4.17 se puede observar claramente que el paquete se traslada del Hub1 al Switch1 sin obtener ningún problema, pero al mismo momento el paquete se transmite también a la PC3 pero el cual es destruido porque ese no es el destino del paquete.

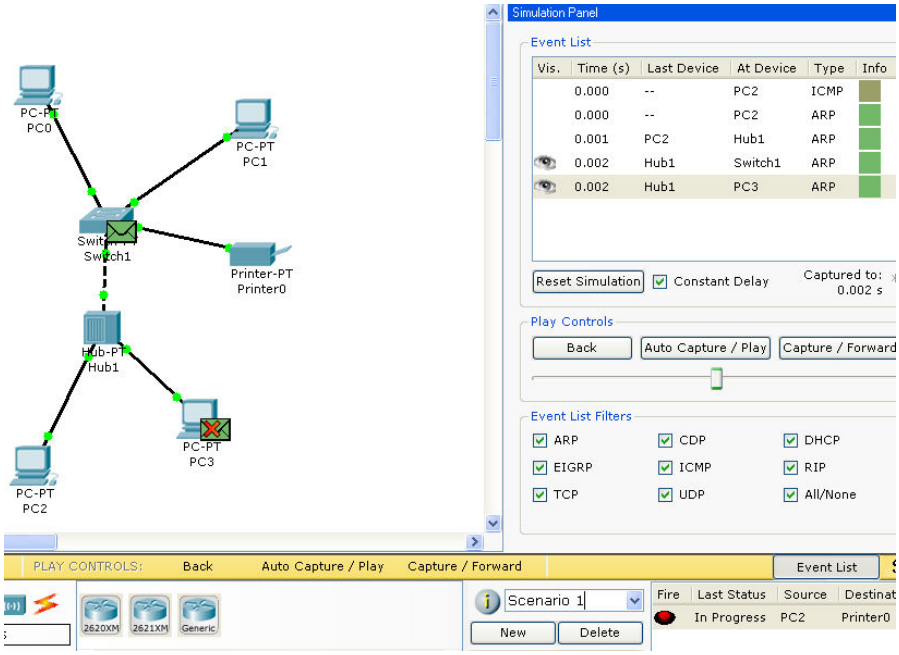


Figura 4.17. Simulación1 2

9. Se debe continuar con la simulación correspondiente hasta que finalmente el paquete regrese a la PC2, confirmando de esta manera que la transferencia de datos es valida, como se puede observar en la figura 4.18. pero al mismo tiempo se observa que es enviado un paquete a la PC3 el mismo que es descartado debido a que ese no es el destino del paquete.

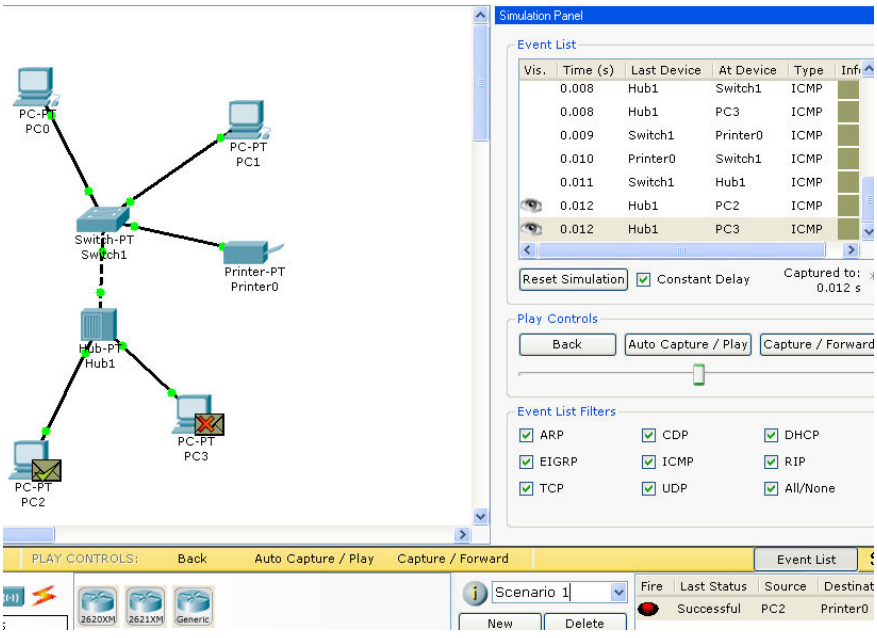


Figura 4.18. Simulación1 3

Análisis de resultados

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

2. En las figuras 4.14 y 4.18 se puede observar muy claramente que el paquete regreso al punto de partida, respectivamente en cada escenario, significando de esa manera que la transferencia de datos es valida en ambos escenarios.

Conclusiones

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

2. Con la simulación realizada se cumplieron los objetivos requeridos

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

4.10.2 Guía de práctica: Realizar una red LAN utilizando un Access Point y un switch

Correr la simulación correspondiente que se encuentra en el siguiente enlace CAPITULO IV\LAN.pka

Objetivo

- Conseguir la transferencia de paquetes entre todas las CPU´s y la impresora que se encuentran conectadas en red
- Verificar la estructura de la trama Ethernet de cada paquete

Procedimiento

1. Iniciar con el software Packet Tracer 4.0. Como se indica en la figura 4.19.

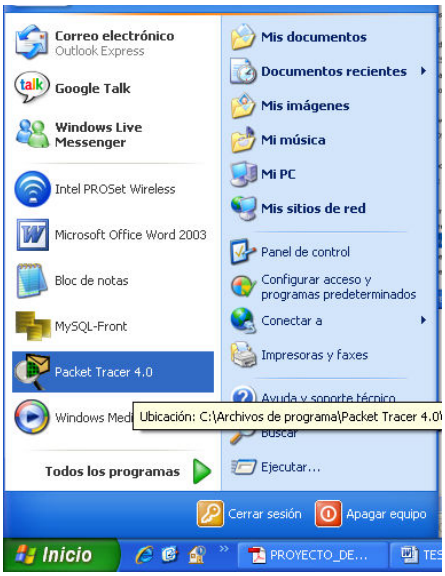


Figura 4.19. Inicio del software Packet Tracer 2

2. Primero debemos configurar la dirección IP y su respectiva mascara de red para la primera PC, para ello procedemos a dar un clic en la primera CPU para lo cual se abre una pantalla de configuración como se indica en la figura 4.20

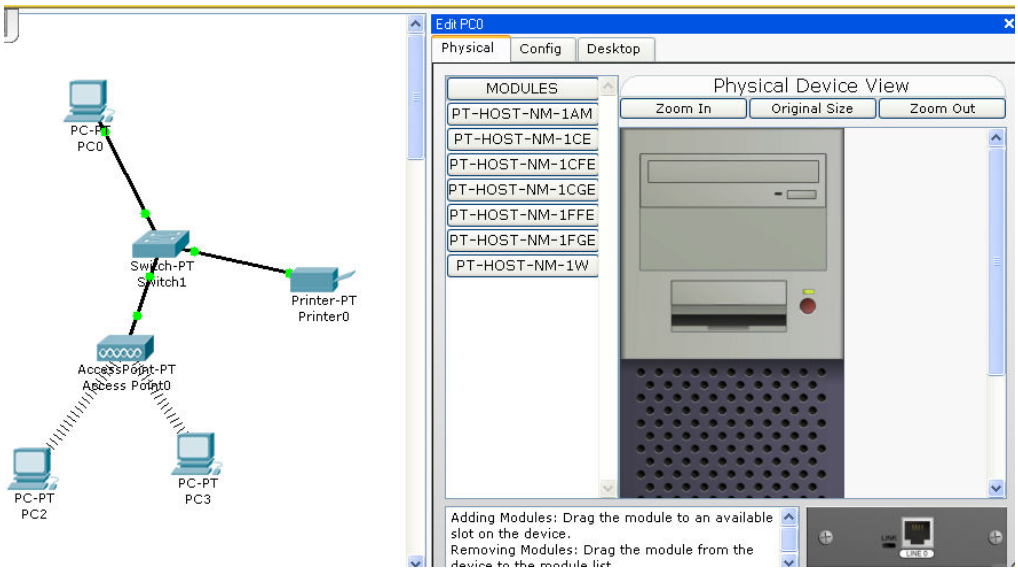


Figura 4.20. Edit PC0 2

3. En la pantalla que aparece debemos 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 observa en la figura 4.21

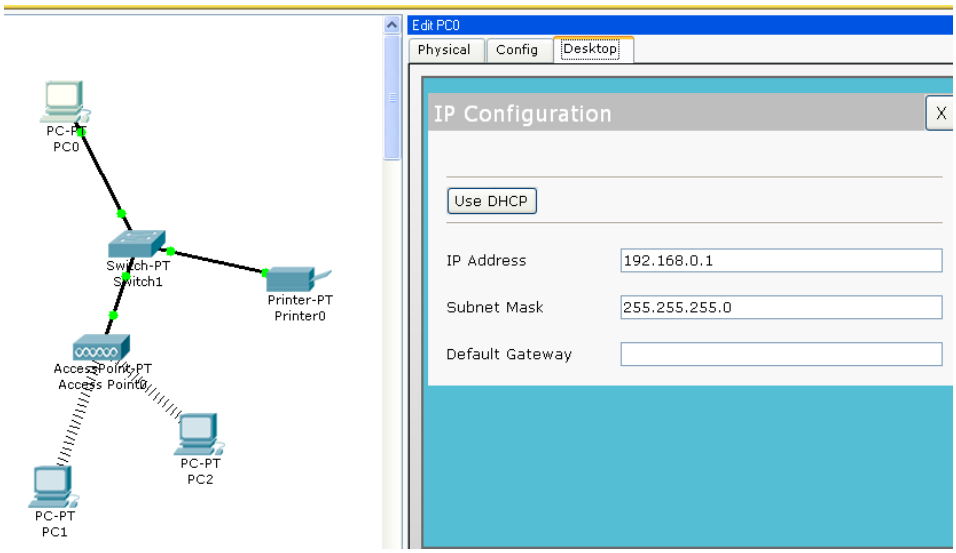


Figura 4.21. PC0 2

4. El mismo procedimiento será utilizado para la configuración de las siguientes dos CPU´s restantes, colocando las siguientes direcciones IP y mascaras de red como se muestran a continuación:
   - PC1
     - IP Address: 192.168.0.2
     - Subnet Mask: 255.255.255.0
   - PC2
     - IP Address: 192.168.0.3
     - Subnet Mask: 255.255.255.0

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 4.22.

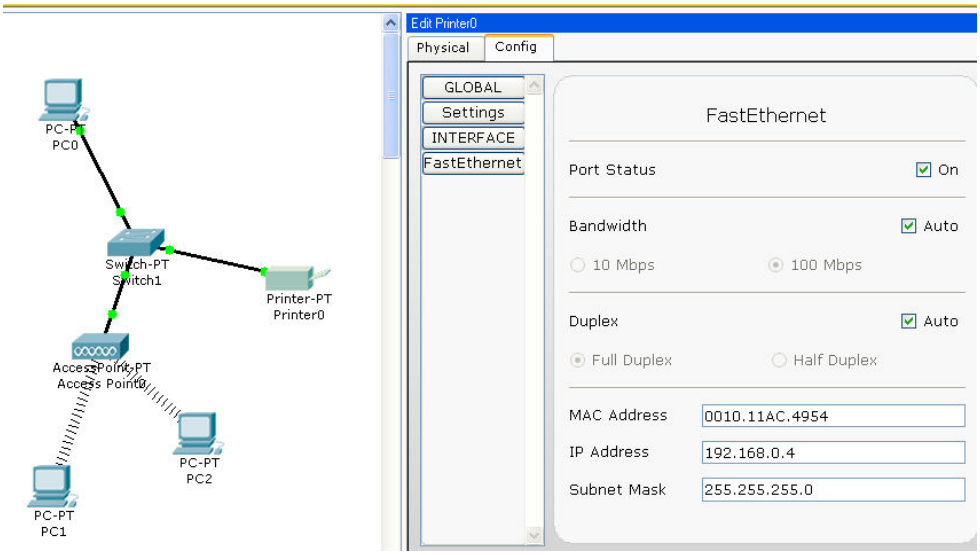


Figura 4.22. Impresora 2

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 4.23.

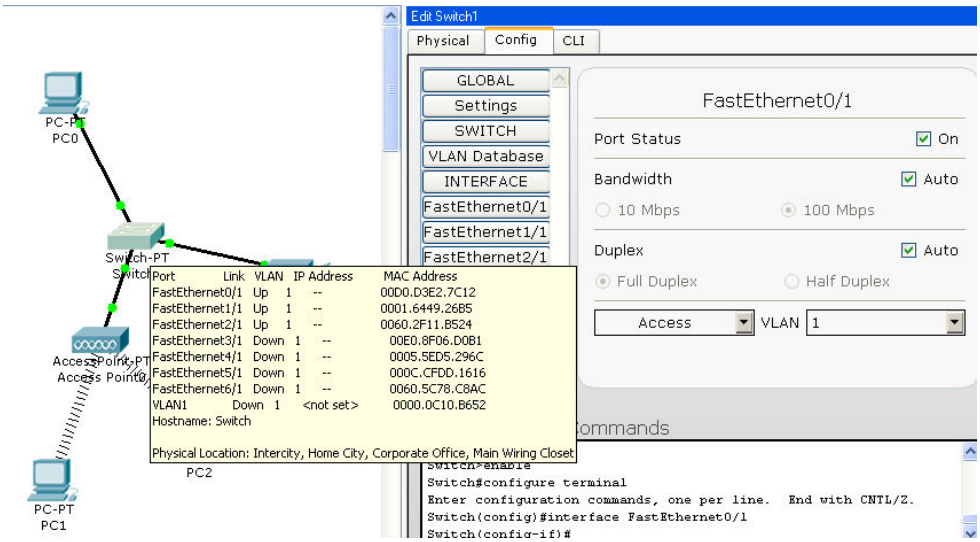


Figura 4.23. Switch1 2

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 4.24.

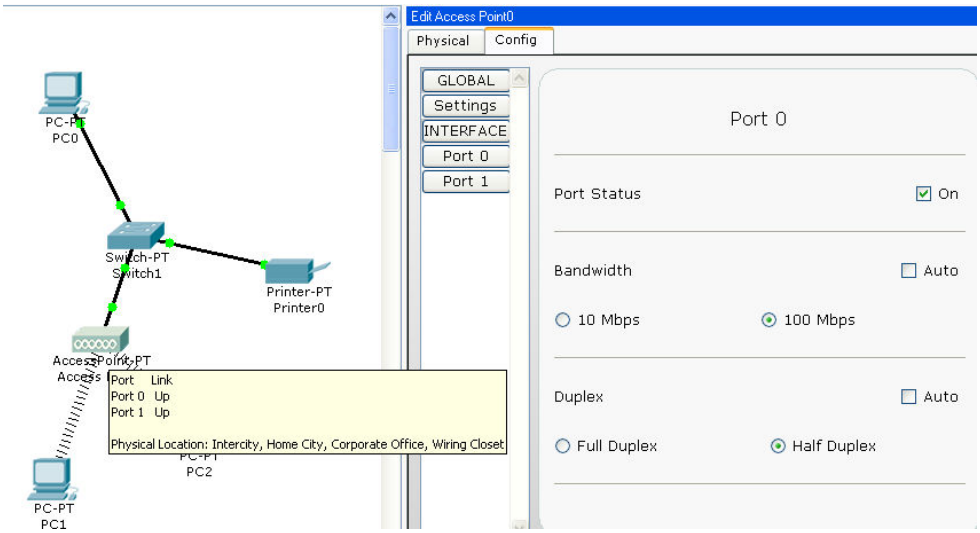


Figura 4.24. Access Point 2

Desarrollo

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 PC2 y la Impresora al enviar y recibir los datos, como se puede observar en la figura 4.25.

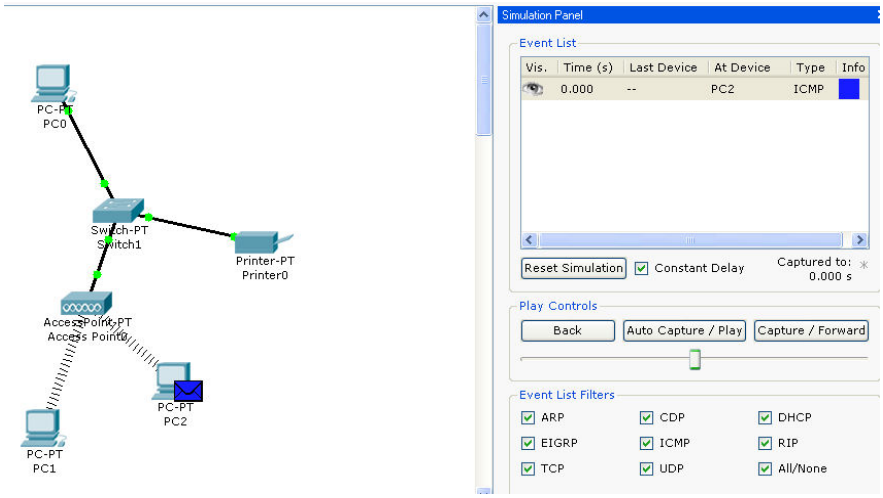


Figura 4.25. Colocación de paquete 2

2. Procederemos con la respectiva simulación enviando un paquete y comprobando que la conexión correspondiente este funcionando, en la figura 4.26. se puede observar los detalles del paquete

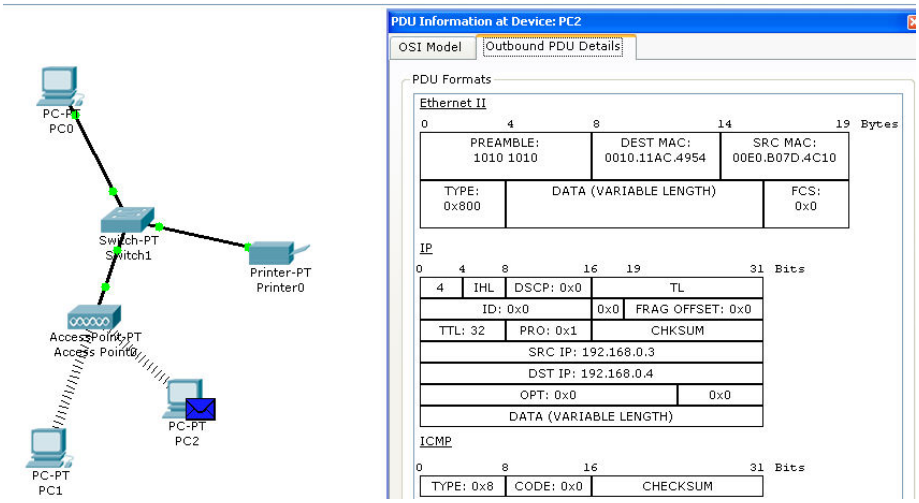


Figura 4.26 Detalles paquete en la PC2

3. Se puede observar claramente en la figura 4.27 que el paquete se traslada de la PC2 al Access Point sin obtener ningún inconveniente y los detalles correspondientes del paquete de entrada y salida.

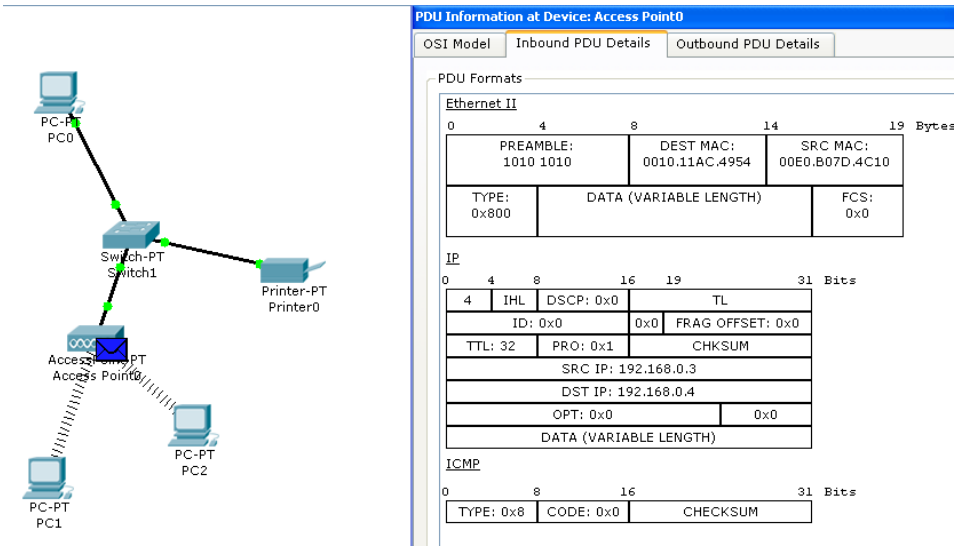


Figura 4.27. Simulación2 1

4. En la figura 4.28 se puede observar claramente que el paquete se traslada del Access Point al switch1 sin obtener problemas y los detalles correspondientes al paquete de entrada y salida, se puede observar también que los paquetes que son enviados a la PC1 y PC2 son eliminados porque ese no es su destino.

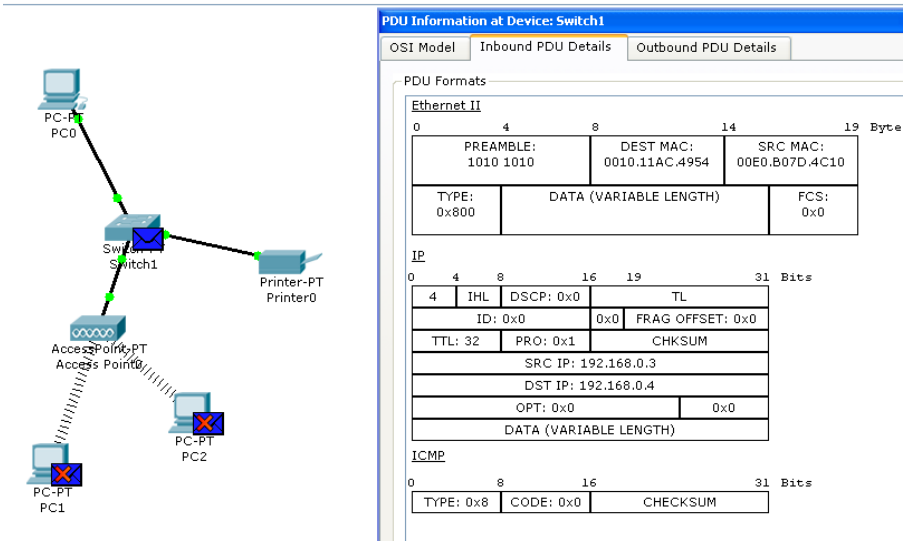


Figura 4.28. Simulación2 2

5. En la figura 4.29 se puede observar claramente que el paquete se traslada del switch1 a la impresora sin obtener ningún problema, y también se puede observar los detalles del paquete de entrada, y en la figura 4.30 se observa los detalles del paquete de salida

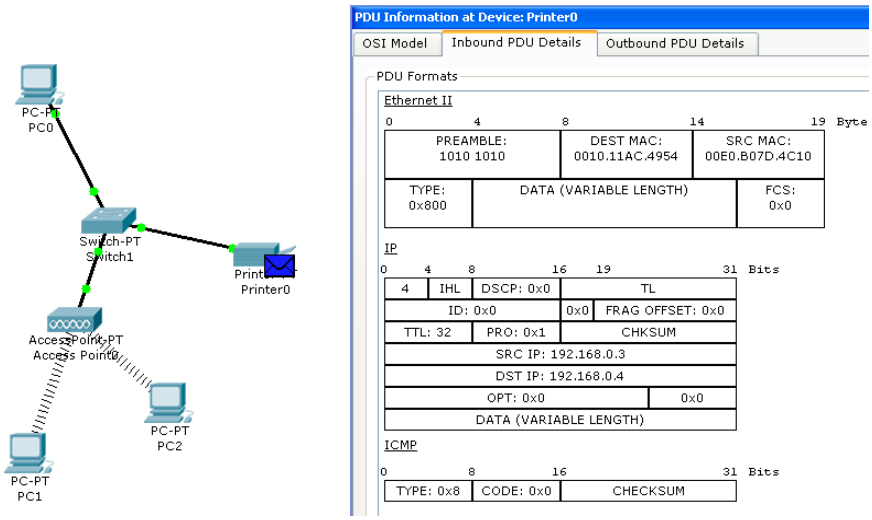


Figura 4.29. Simulación2 3

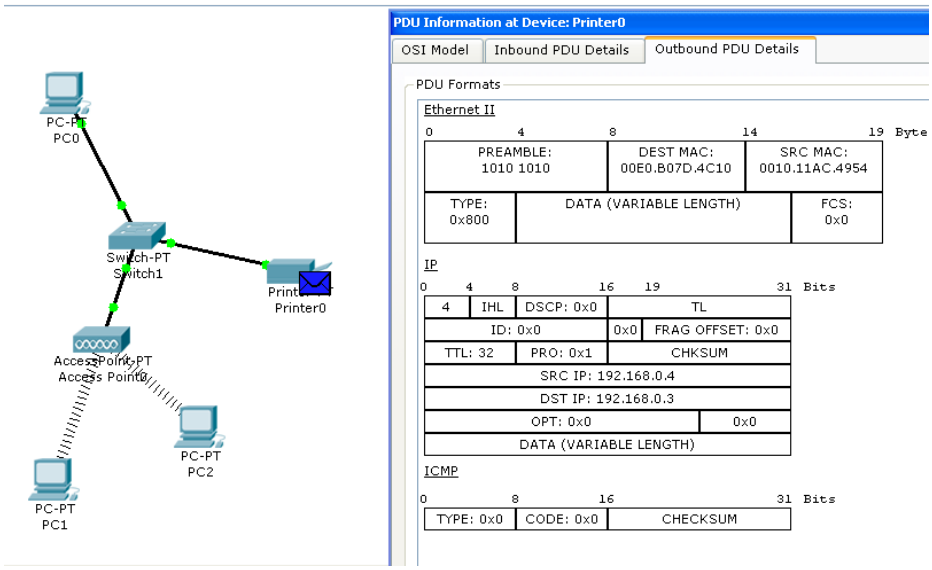


Figura 4.30. Detalles paquete de salida

6. Se debe continuar con la simulación correspondiente hasta que finalmente el paquete regrese a la PC2, confirmando de esta manera que la transferencia de datos es valida, como se puede observar en la figura 4.31. pero al mismo tiempo se observa que es enviado un paquete a la PC1 el mismo que es descartado debido a que ese no es el destino del paquete.

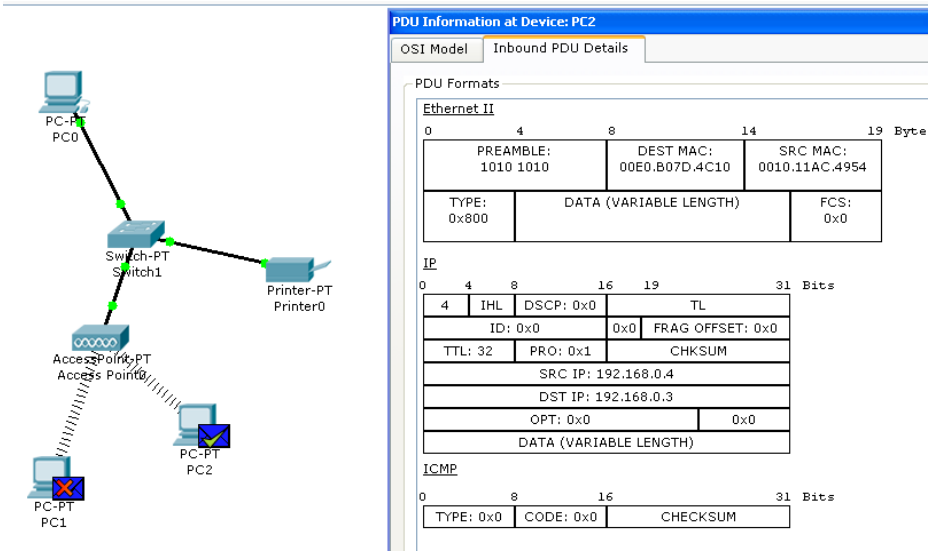


Figura 4.31. Simulación2 4

Análisis de resultados

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

2. En la figura 4.31 se puede observar muy claramente que el paquete regreso al punto de partida, significando que la información fue entregada sin ningún problema a su destino.

Conclusiones

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

2. Con la simulación realizada se cumplieron los objetivos requeridos

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

4.11. PRUEBAS DE OPCIÓN MÚLTIPLE

El banco de preguntas correspondiente al capitulo se encuentra en anexos.

Para realizar las pruebas de selección múltiple correspondientes a este capitulo se debe correr el programa que se encuentra en el siguiente vinculo index.html, o en http://www.fie-espe.edu.ec/preguntas y luego procedemos a ingresar los datos del alumno que va a realizar la prueba como se muestra en la figura 4.32

Figura 4.32. Datos Alumno

Para ingresar a resolver la prueba debemos elegir el capitulo que se va a realizar como se muestra en la figura 4.33 o se debe ingresar a la plantilla de preguntas e elegir igualmente el capitulo deseado.

Figura 4.33. Prueba Capitulo 4

El siguiente paso es realizar la prueba de selección múltiple como se indica en la figura 4.34. Luego de haber respondido a todas las preguntas se procede hacer clic sobre Corregir Prueba para que la prueba sea calificada y corregida automáticamente como se muestra en la figura 4.35.

Figura 4.34. Prueba selección múltiple

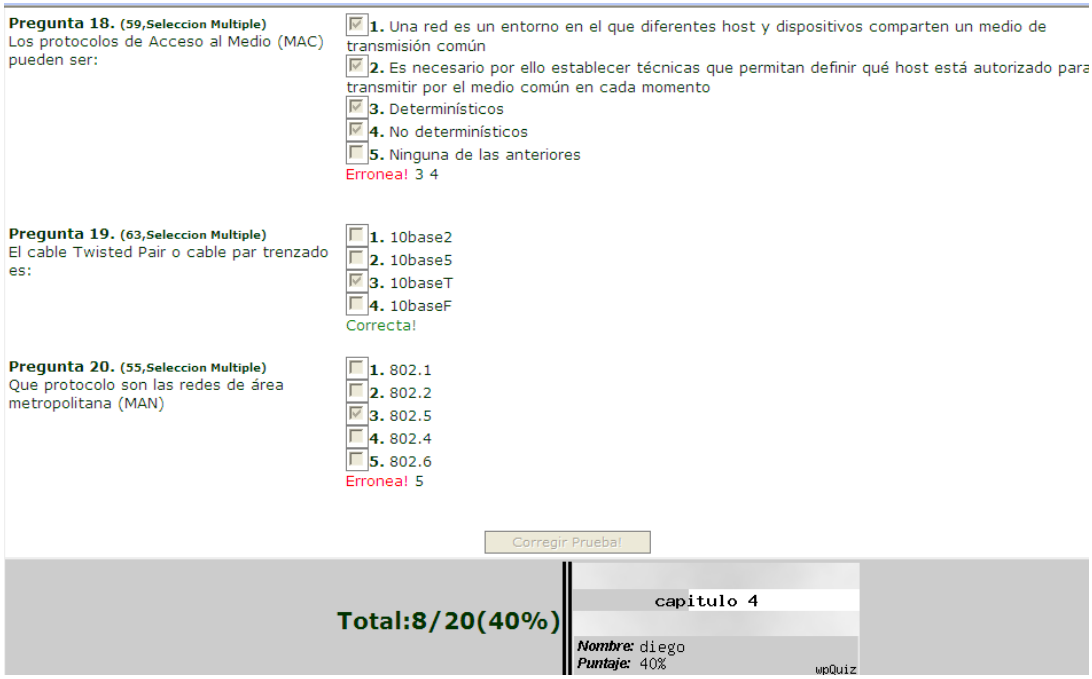


Figura 4.35. Calificación Prueba

CAPITULO V

PROTOCOLOS Y SERVICIO DE RED.

5.1. MODELO DE CAPAS

En 1984, la Organización Internacional de Estandarización (ISO) desarrolló un modelo de referencia llamado **OSI (Open Systems Interconectiòn**, Interconexión de sistemas abiertos). El cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. A este se lo conoce como el modelo de siete capas que son:

- Aplicación: Esta se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación.
- Presentación: Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Esta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos.
- Sección: Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación.
- Transporte: Esta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario.
- Red: Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final.
- Enlace: Realiza la verificación de errores, retransmisión, control fuera del flujo y la secuenciación de la capacidades que se utilizan en la capa de red.
- Físico: Se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.

En el modelo OSI el propósito de cada capa es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de como los servicios son implementados realmente. Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora como se observa en la figura 5.1.

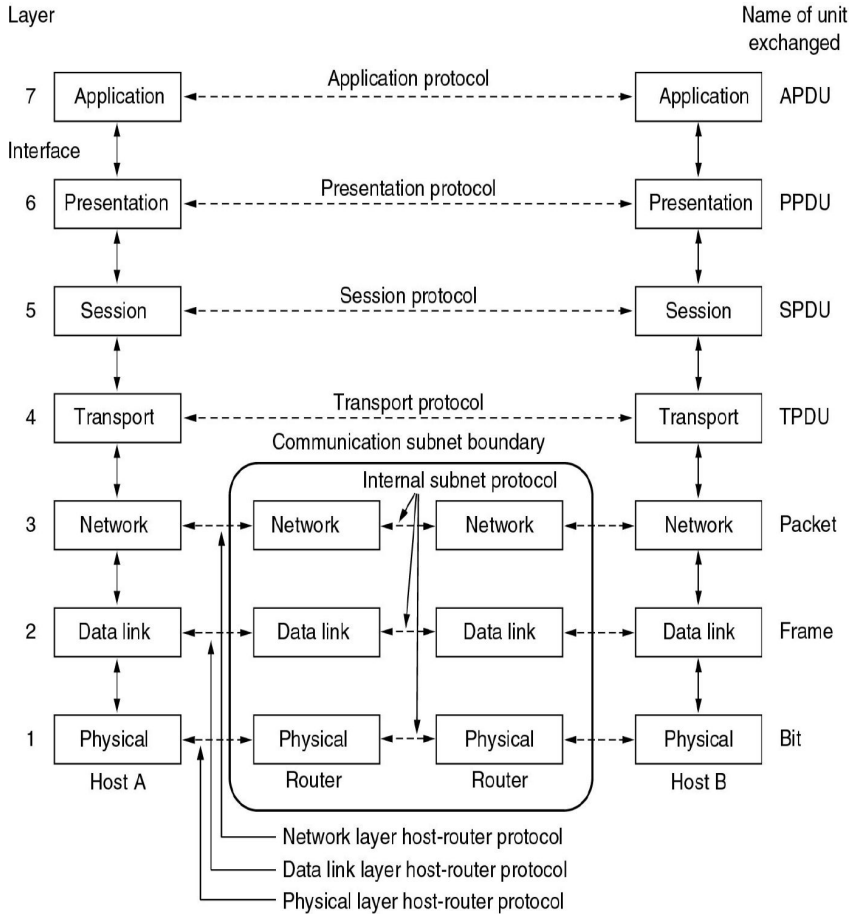


Figura 5.1. Capas modelo OSI*

Figura 5.1. Tomada de la dirección siguiente http://antares.itmorelia.edu.mx/~jcolivar/cursos/rc071q/cap1.pdf

En la figura 5.2 se pueden observar las capas de los modelos OSI y TCP/IP

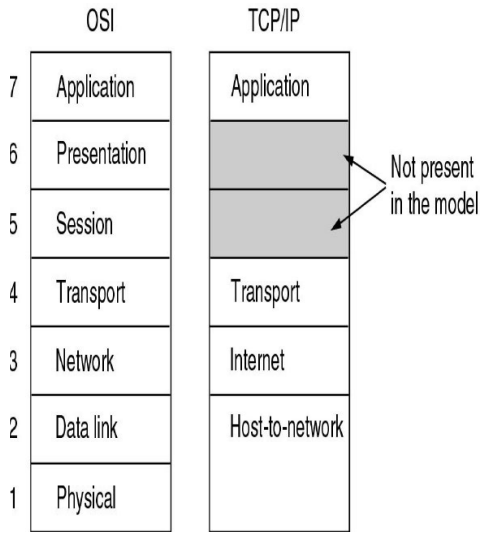


Figura 5.2. Modelos OSI y TCP/IP

5.2. PROTOCOLOS Y NIVELES

5.2.1. Niveles

El modelo TCP/IP consta de cinco 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.
- 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.
- Físico: Análogo al nivel físico del modelo OSI.

Figura 5.2. Tomada de la dirección siguiente http://antares.itmorelia.edu.mx/~jcolivar/cursos/rc071q/cap1.pdf

En la tabla 5.1 se puede observar los cinco niveles de la arquitectura TCP/IP

Tabla 5.1. Niveles TCP/IP

NIVEL DE APLICACIÓN
NIVEL DE TRANSPORTE
NIVEL DE INTERNET
NIVEL DE RED
NIVEL FÍSICO

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.

5.2.2. 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.

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 5.3:

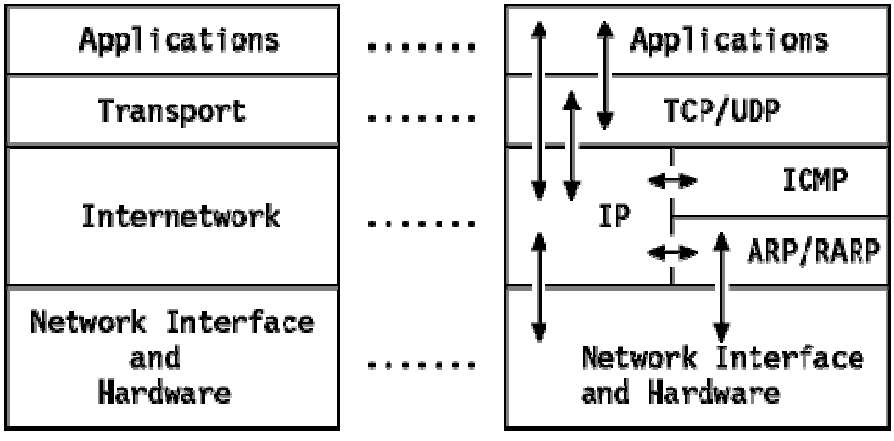


Figura 5.3. Protocolos de internet

Figura 5.3. Tomada de la dirección siguiente http://ditec.um.es/laso/docs/tut-tcpip/3376c21.html

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 datagrama IP. 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 5.4. Se puede observar el modelo arquitectónico.

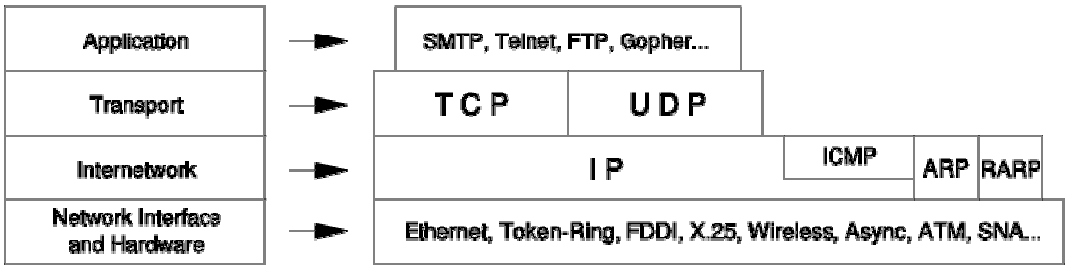


Figura 5.4. Modelo arquitectónico

Figura 5.4. Tomada de la dirección siguiente http://ditec.um.es/laso/docs/tut-tcpip/3376c21.html

5.3. INTERFACES Y SERVICIOS

Servicio

- Conjunto de primitivas (operaciones) que un nivel o capa provee al nivel superior. El servicio define que operaciones pueden ejecutar el nivel superior, pero no dice como se implementan.
- La entidad N desarrolla un servicio para el nivel N+1, en este caso el nivel N es un proveedor del servicio y la capa N+1 es usuario del servicio.
- Es importante diferenciar entre un protocolo y un servicio: un nivel ofrece determinado servicio al nivel superior el cual es implementado usando determinado protocolo.
- La transferencia de información entre niveles pares realmente es virtual ya que el flujo real de información se realiza a través de los servicios ofrecidos por el nivel inmediatamente inferior. Este proceso se repite hasta llegar al nivel físico donde se presenta una transmisión real.

Interface

- Punto entre dos capas adyacentes. La interface define un conjunto de reglas, primitivas y operaciones de intercambio de información entre niveles adyacentes dentro del mismo host. Define los servicios que ofrece la capa inferior a la superior.
- Los servicios están disponibles a través de los puntos de acceso al servicio (SAP). Los SAPs de la capa N es el punto donde la capa N+1 puede acceder servicios. Cada SAP tiene un identificador que lo hace único. Por ejemplo: en el caso de Telefonía, los SAP son los conectores que se encuentran en la pared para poner el teléfono.
- Para que haya comunicación entre las capas, la superior pasa una Unidad de Datos de Interfaz (IDU), la cual está compuesta por una unidad de datos del servicio (SDU) e información de control. Luego la capa n se encarga de agregar la información de la SDU en una unidad de datos del protocolo (PDU).
- Encabezados (Headers): Información de control (PCI: Protocol Control Information) que cada capa agrega a los datos que recibe de la capa superior (SDU).

- Límites del tamaño de mensajes: Las diferentes arquitecturas presentan límites del tamaño de los mensajes dependiendo del nivel o capa.

5.4. TIPOS DE SERVICIOS

Orientados a la conexión:

Un servicio O.C. es aquel que posee tres fases:

- Conexión (Connect)
- Transferencia (Data)
- Desconexión (Disconnect)

Características del servicio:

- Servicio Confiable
- Garantiza la conexión lógica
- Corrección de errores
- Los mensajes poseen una secuencia
- Puede establecer conexiones PERMANENTES o TEMPORALES
- Puede ofrecer mecanismos de control de flujo.

No orientados a la conexión:

Un servicio N.O.C es aquel que solo posee la fase de transferencia de datos:

- Transferencia (Data).

Características del servicio:

- Mejor esfuerzo
- No hay garantía de entrega
- No hay corrección de errores
- Los mensajes pueden ser perdidos, duplicados entregados en desorden
- No hay secuencia
- Se conoce como servicios DATAGRAMA

5.5. PRIMITIVAS DE SERVICIO

Un servicio se especifica formalmente mediante un conjunto de primitivas

- Las primitivas son las operaciones disponibles para el usuario del servicio
- Son indicaciones para que el servicio haga algo o para que avise si la entidad par hace algo

Ejemplos:

- CONNECT.request
- CONNECT.indication
- CONNECT.response
- CONNECT.confirm
- DATA.request
- DATA.indication
- DISCONNECT.request
- DISCONNECT.indication

5.6. MODELO DE REFERENCIA OSI

Este modelo posee tres 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 y físico.

Estos niveles se comunican entre si 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 este 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 tail (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.

Las funciones que desempeñan los diferentes niveles son las siguientes:

- *Nivel A*: ofrece servicios de transferencia de archivos, gestión de correo electrónico, etc. Ofrece la posibilidad de crear sus propios servicios.
- *Nivel P*: está relacionado con la representación sintáctica de los datos (presentación de los datos). También está relacionado con la seguridad informática, es decir, con temas de encriptación.
- *Nivel S*: sincroniza las aplicaciones, por ejemplo cuando hay una caída de la red y al poco tiempo vuelve este nivel hace que las aplicaciones funcionen correctamente.
- *Nivel T*: intenta realizar una conexión correcta para esto realiza el control de flujo y de errores.
- *Nivel R*: busca rutas para llegar al destino, y da un identificador de red (dirección de ordenador y de interconexión)
- *Nivel E*: ofrece un servicio libre y seguro realizando el control de flujo y errores, pero a través de los terminales intermedios. Los niveles R no aseguran que haya errores y por eso se realiza aquí, también, el control de flujo y errores.
- *Nivel F*: se ocupa de la electrónica y mecánica, tipologías, etc.

5.7. 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 A realiza las operaciones que se realizaban en los niveles A, P, S del modelo de referencia OSI.

5.8. 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.

5.9. 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.

5.9.1. Comparación

Aporte fundamental del modelo OSI: **conceptos**

- Servicios
    - Definen las funciones de una capa
- Interfaces
    - Como las capas superiores acceden a los servicios de las capas interiores
- Protocolos
    - El mecanismo por el cual las parejas de entidades se comunican. Es un problema interno de las capas.

5.10. 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, estándares para redes

- 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 Board
  - 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 no 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 (se puede poner equipos de distintos fabricantes). Ejemplo: tarjetas de distintas marcas.

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: I+D...)

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 (Instituction 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

5.11. SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

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

Correr la simulación correspondiente que se encuentra en el siguiente enlace CAPITULO V\modelo osi.pka

Objetivo

- Verificar el comportamiento 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

Procedimiento

1. Iniciar con el software Packet Tracer 4.0. Como se indica en la figura 5.5.

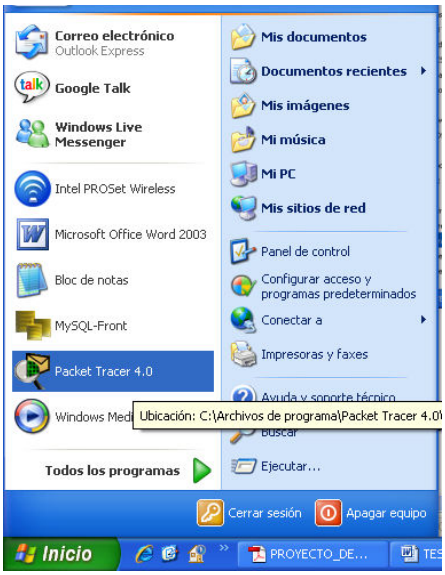


Figura 5.5. Inicio del software Packet Tracer

2. 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 5.6.

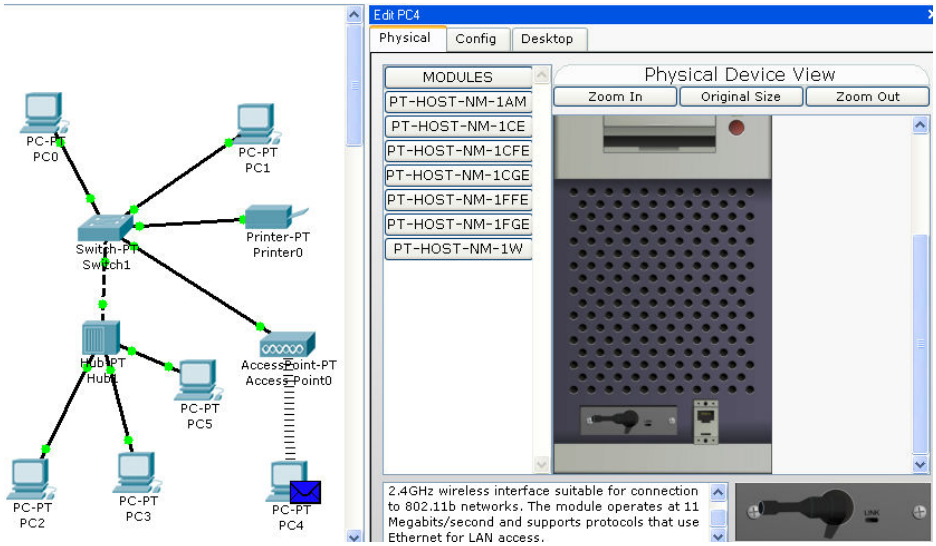


Figura 5.6. Dispositivo inalámbrico

3. 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 5.7

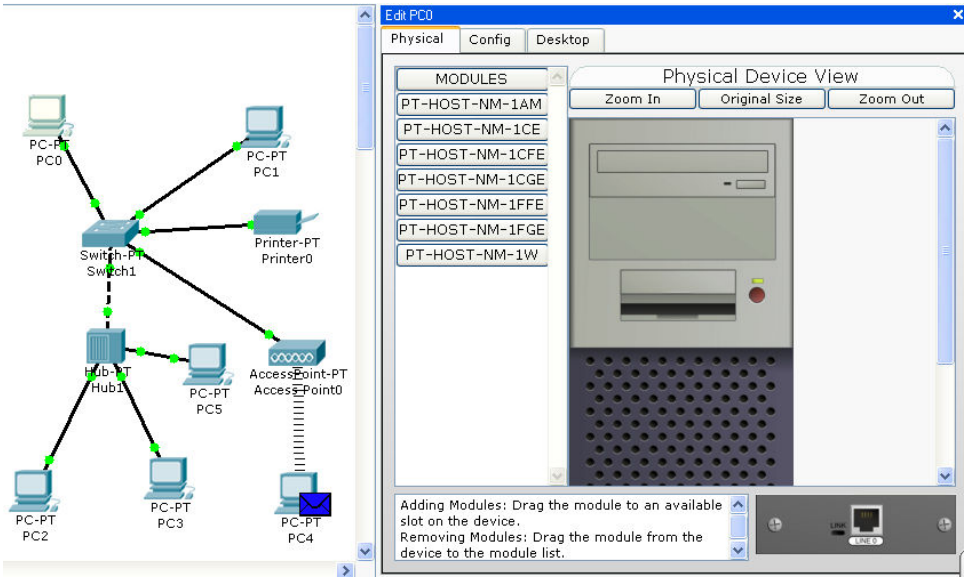


Figura 5.7. Edit CPU´s

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 y nuestra mascara de red como se observa en la figura 5.8

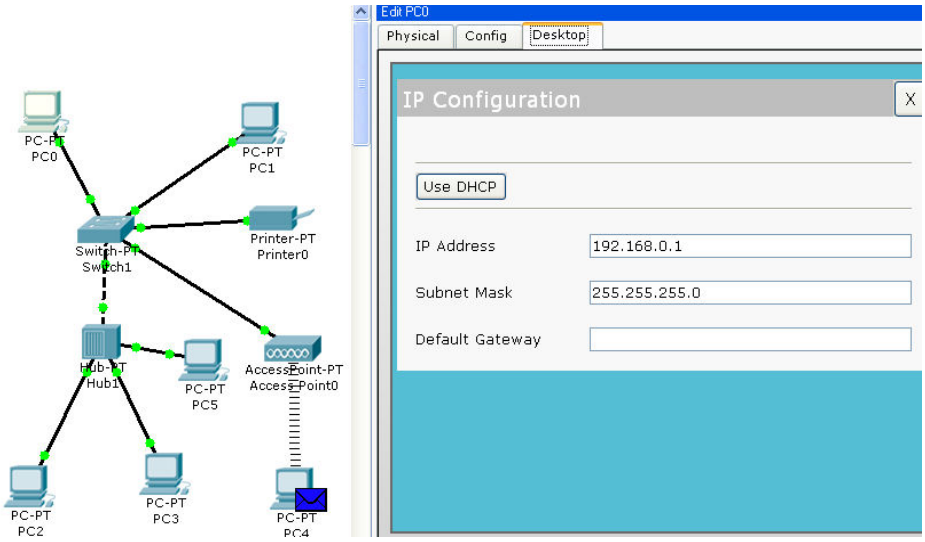


Figura 5.8. CPU´s

5. El mismo procedimiento será utilizado para la configuración de las cinco CPU´s restantes, colocando las siguientes direcciones IP y mascaras de red como se muestran a continuación:

- PC1
  - IP Address: 192.168.0.2
  - Subnet Mask: 255.255.255.0

- PC2
  - IP Address: 192.168.0.3
  - Subnet Mask: 255.255.255.0

- PC3
  - IP Address: 192.168.0.4
  - Subnet Mask: 255.255.255.0

- PC4
  - IP Address: 192.168.0.7
  - Subnet Mask: 255.255.255.0

- PC5
  - IP Address: 192.168.0.8
  - Subnet Mask: 255.255.255.0

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 5.9.

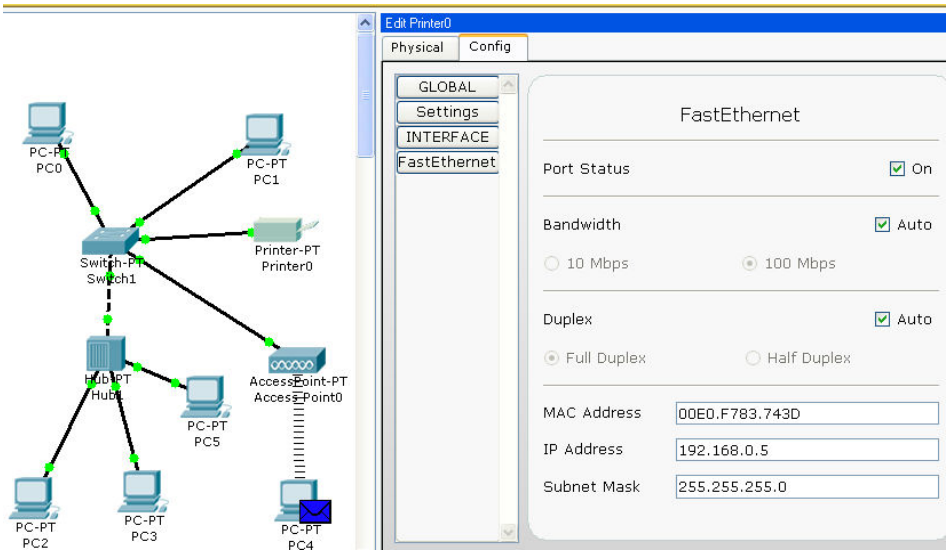


Figura 5.9. Impresora

7. 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 5.10.

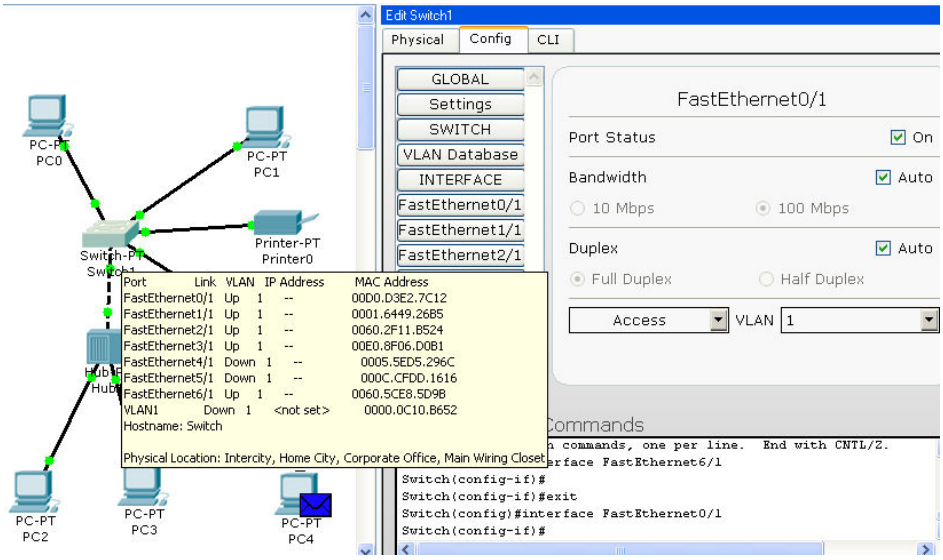


Figura 5.10. Switch1

8. Se procede 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 5.11.

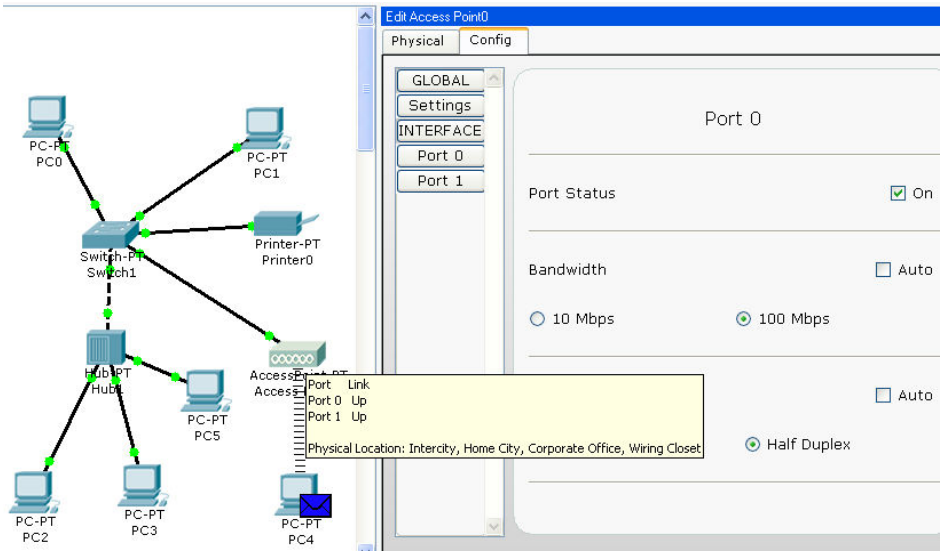


Figura 5.11. Access Point

9. 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 5.12.

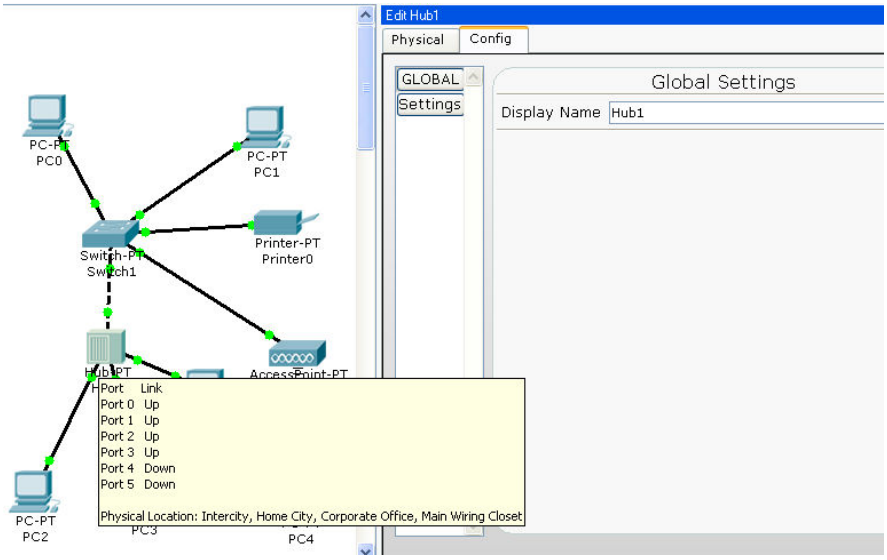


Figura 5.12. Hub

Desarrollo

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 5.13.

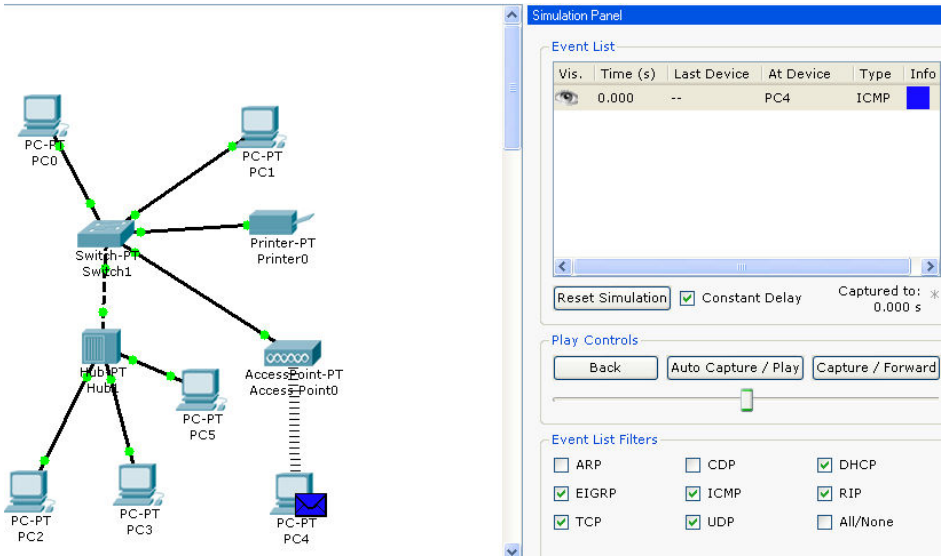


Figura 5.13. Colocación de paquete

2. Procederemos con la respectiva simulación enviando un paquete y comprobando que la conexión correspondiente este funcionando, en las figuras 5.14., 5.15, 5.16 y 5.17. se puede observar las diferentes capas por la que pasa el paquete para ser enviado y su respectivo comportamiento. Como se observa en la figura 5.14 para que el paquete salga de la PC4 debe atravesar las diferentes capas del modelo OSI, en este caso el paquete se encuentra en la capa tres, en la cual se le debe encapsular al paquete para que pueda pasar a la capa dos y así sucesivamente.

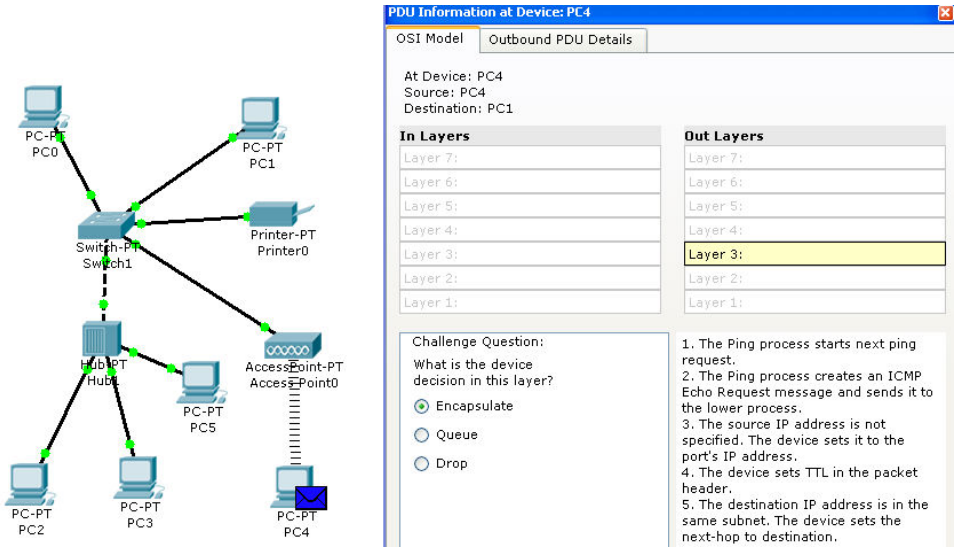


Figura 5.14 Salida paquete en la capa 3 en PC4

3. Como se puede observar en la figura 5.15 el paquete de la PC4 se encuentra en la capa dos, en la cual se le debe encapsular al paquete para que pueda pasar a la capa uno y así seguir con su comportamiento.

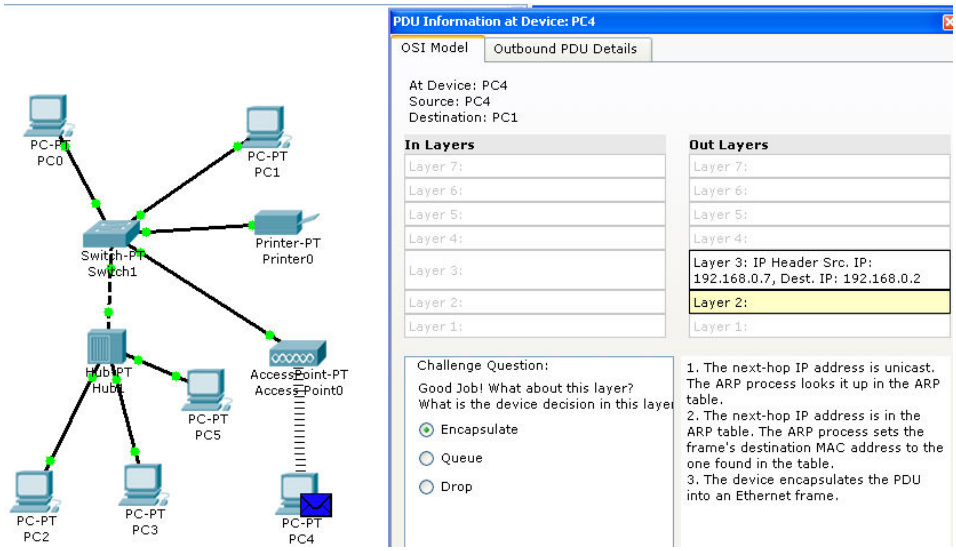


Figura 5.15 Salida paquete en la capa2 en PC4

4. Como se puede observar en la figura 5.16 el paquete de la PC4 se encuentra en la capa uno, en la cual se le debe transmitir al paquete para que pueda ser enviado hacia el Access Point en un paso posterior.

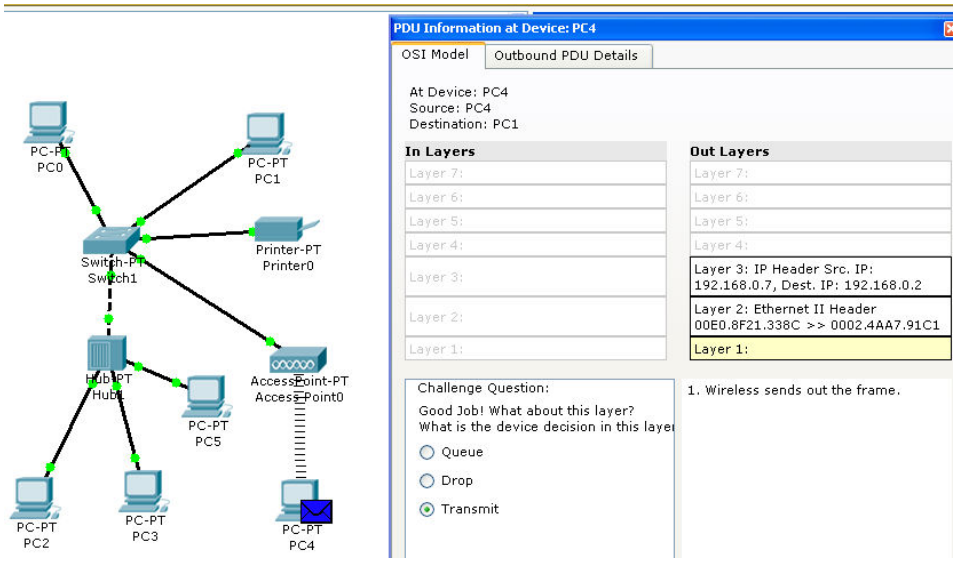


Figura 5.16 Salida paquete en la capa1 en PC4

5. Como se puede observar en la figura 5.17 el paquete de la PC4 se encuentra listo para el envío hacia el Access Point.

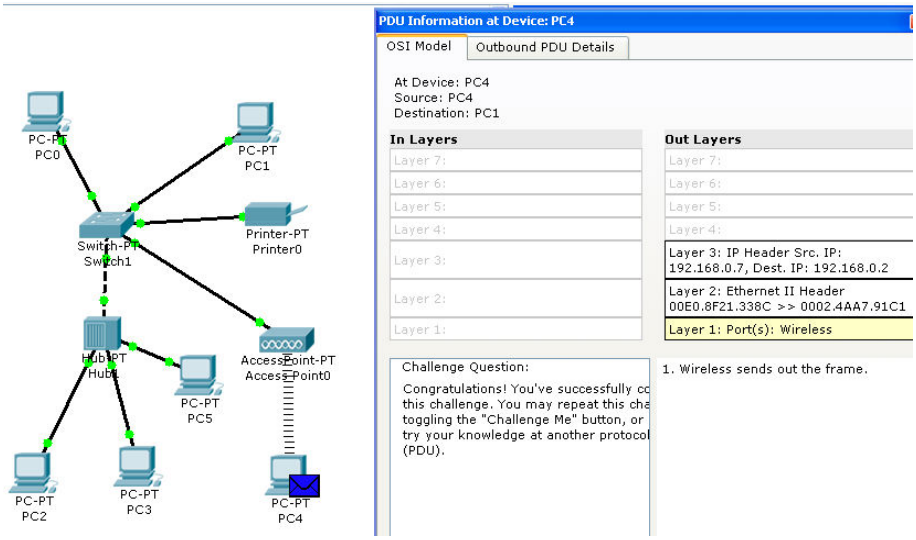


Figura 5.17 Envío paquete en PC4

6. Se debe continuar con la simulación correspondiente verificando el comportamiento del paquete en cada elemento de la red y en cada capa del modelo OSI, hasta que finalmente el paquete llegue a la PC1 que es su destino y luego regrese a la PC4 para que de esta manera sea confirmada que la transferencia de datos es valida, como se puede observar en la figura 5.18.

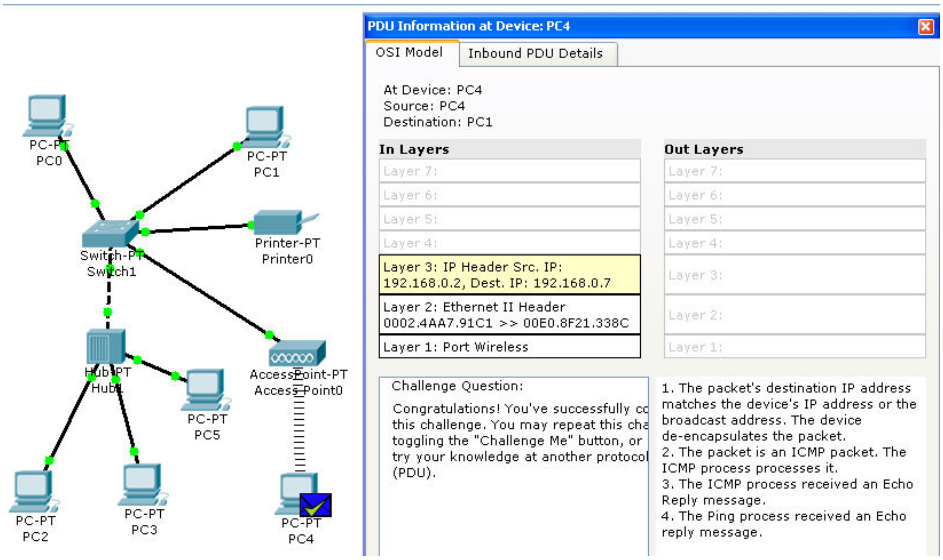


Figura 5.18 Paquete recibido en PC4

Análisis de resultados

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

2. Se puede verificar el comportamiento del paquete en las CPU´s observando claramente como el paquete llega hasta una capa3 del modelo OSI.

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

Conclusiones

1. En las gráficas de la simulación se pudo verificar el comportamiento de cada paquete en las diferentes capas del modelo OSI.

2. En las gráficas de la simulación se permitió observar que la red se encuentra funcionando correctamente gracias a la transferencia de paquetes en la misma.

3. Se puede observar muy claramente que la red se encuentra funcionando correctamente con todos los dispositivos que se encuentran conectados en la misma.

5.12. PRUEBAS DE OPCIÓN MÚLTIPLE

El banco de preguntas correspondiente al capitulo se encuentra en anexos.

Para realizar las pruebas de selección múltiple correspondientes a este capitulo se debe correr el programa que se encuentra en el siguiente vinculo index.html, o en http://www.fie-espe.edu.ec/preguntas y luego procedemos a ingresar los datos del alumno que va a realizar la prueba como se muestra en la figura 5.19

Figura 5.19. Datos Alumno

Para ingresar a resolver la prueba debemos elegir el capitulo que se va a realizar como se muestra en la figura 5.20 o se debe ingresar a la plantilla de preguntas e elegir igualmente el capitulo deseado.

Figura 5.20. Prueba Capitulo 5

El siguiente paso es realizar la prueba de selección múltiple como se indica en la figura 5.21. Luego de haber respondido a todas las preguntas se procede hacer clic sobre Corregir Prueba para que la prueba sea calificada y corregida automáticamente como se muestra en la figura 5.22.

Figura 5.21. Prueba selección múltiple

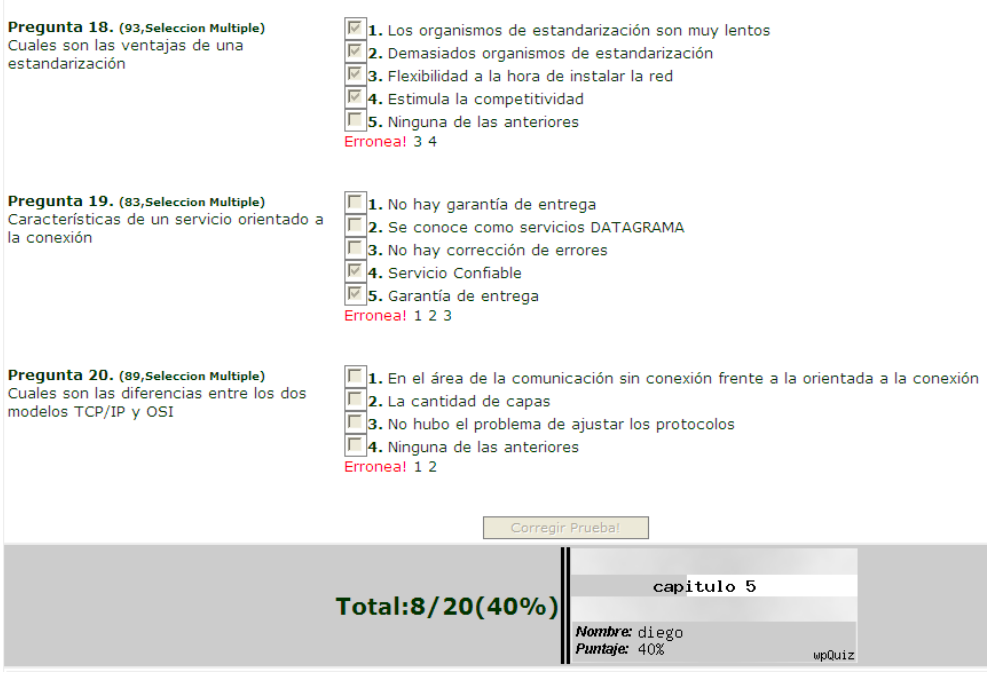


Figura 5.22. Calificación Prueba

CAPITULO VI

DISPOSITIVOS DE CONECTIVIDAD E ÍNTER CONECTIVIDAD

6.1. BRIDGE

Al igual que un repetidor, un bridge puede unir segmentos o grupos de trabajo LAN. Sin embargo, un bridge puede, además, dividir una red para aislar el tráfico o los problemas. Por ejemplo, si el volumen del tráfico de uno o dos equipos o de un departamento está sobrecargando la red con los datos y ralentizan todas las operaciones, el bridge podría aislar a estos equipos o al departamento.

Los bridges se pueden utilizar para:

- Extender la longitud de un segmento.
- Proporcionar un incremento en el número de equipos de la red.
- Reducir los cuellos de botella del tráfico resultantes de un número excesivo de equipos conectados.
- Dividir una red sobrecargada en dos redes separadas, reduciendo la cantidad de tráfico en cada segmento y haciendo que la red sea más eficiente.
- Enlazar medios físicos diferentes como par trenzado y Ethernet coaxial.

Los bridges trabajan a nivel de enlace de datos del modelo de referencia OSI y, por tanto, toda la información de los niveles superiores no está disponible para ellos. Más que distinguir entre un protocolo y otro, los bridges pasan todos los protocolos que aparecen en la red.

Los bridges trabajan en el nivel MAC (capa2) y, por ello, algunas veces se conocen como Bridges de nivel MAC.

Un bridge de nivel MAC:

- Escucha todo el tráfico.
- Comprueba las direcciones origen y destino de cada paquete.
- Construye una tabla de encaminamiento, donde la información está disponible.
- Reenvían paquetes de la siguiente forma:
  - Si el destino no aparece en la tabla de encaminamiento, el bridge reenvía el paquete a todos los segmentos.
  - Si el destino aparece en la tabla de encaminamiento, el bridge reenvía el paquete al segmento correspondiente (a menos que este segmento sea también el origen).

Un bridge funciona considerando que cada nodo de la red tiene su propia dirección. Un bridge reenvía paquetes en función de la dirección del nodo destino. Realmente, los bridges tienen algún grado de inteligencia puesto que aprenden a dónde enviar los datos. Cuando el tráfico pasa a través del bridge, la información sobre las direcciones de los equipos se almacenan en la RAM del bridge. El bridge utiliza esta RAM para generar una tabla de encaminamiento en función de las direcciones de origen.

Inicialmente, la tabla de encaminamiento del bridge está vacía. Cuando los nodos transmiten los paquetes, la dirección de origen se copia en la tabla de encaminamiento. Con esta información de la dirección, el bridge identifica qué equipos están en cada segmento de la red.

Figura 6.1. Bridge

Figura 6.1. Tomada de la dirección siguiente www.ciao.it/3Com__597638

Creación de la tabla de encaminamiento. Los bridges generan sus tablas de encaminamiento en función de las direcciones de los equipos que han transmitido datos en la red. Los bridges utilizan, de forma específica, las direcciones de origen (dirección del dispositivo que inicia la transmisión) para crear una tabla de encaminamiento.

Cuando el bridge recibe un paquete, la dirección de origen se compara con la tabla de encaminamiento. Si no aparece la dirección de origen, se añade a la tabla. A continuación, el bridge compara la dirección de destino con la base de datos de la tabla de encaminamiento.

Si la dirección de destino está en la tabla de encaminamiento y aparece en el mismo segmento de la dirección de origen, se descarta el paquete. Este filtrado ayuda a reducir el tráfico de la red y aislar segmentos de la red.

Si la dirección de destino está en la tabla de encaminamiento y no aparece en el mismo segmento de la dirección de origen, el bridge envía el paquete al puerto apropiado que permite alcanzar la dirección de destino.

Si la dirección de destino no está en la tabla de encaminamiento, el bridge envía el paquete a todos sus puertos, excepto al puerto desde donde se originó el envío.

Resumiendo, si un bridge conoce la localización del nodo de destino, envía el paquete a dicha localización. Si no conoce el destino, envía el paquete a todos los segmentos, en la figura 6.2 se puede observar un bridge conectado en red.

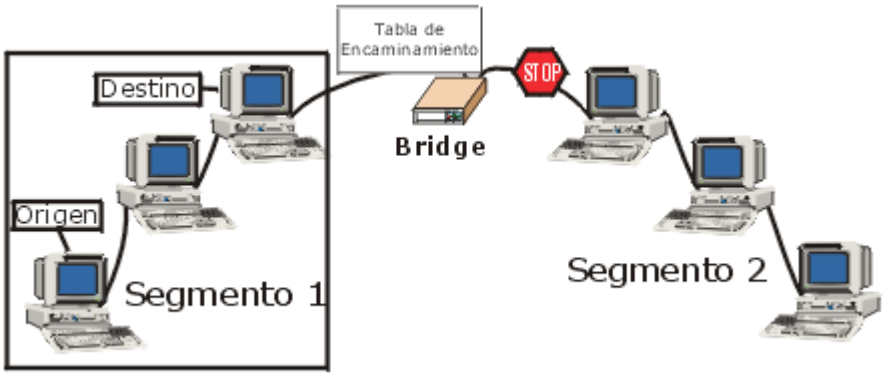


Figura 6.2. Red interconectada utilizando un bridge

Figura 6.2. Tomada de la dirección siguiente http://carinalusso.iespana.es/Dispositivos%20de%20red.htm

Segmentación del tráfico de red. Un bridge puede segmentar el tráfico mediante su tabla de encaminamiento. Un equipo en el segmento 1 (origen), envía datos a otro equipo (destino) también localizado en el segmento 1. Si la dirección de destino está en la tabla de encaminamiento, el bridge puede determinar que el equipo destino está también en el segmento 1. Dado que los equipos origen y destino están en el mismo segmento 1, se tiene que el paquete no se reenvía a través del bridge al segmento 2, como se puede observar en la figura 6.2.

Por tanto, los bridges pueden utilizar las tablas de encaminamiento para reducir el tráfico de la red controlando los paquetes que se envían al resto de los segmentos. Este control (o restricción) del flujo del tráfico de red se conoce como "segmentación del tráfico de red".

Una red grande no está limitada a un solo bridge. Se pueden utilizar múltiples bridge para combinar diferentes redes pequeñas en una red más grande.

Los bridges tienen todas las características de los repetidores, pero también proporcionan más ventajas. Ofrecen mejor rendimiento de red que los repetidores. Las redes unidas por bridges se han dividido y, por tanto, un número menor de equipos compiten en cada segmento por los recursos disponibles.

Visto de otra forma, si una gran red Ethernet se dividió en dos segmentos conectados por un bridge, cada red nueva transportaría un número menor de paquetes, tendríamos menos colisiones y operaría de forma mucho más eficiente. Aunque cada red estaría separada, el bridge pasaría el tráfico apropiado entre ellas.

Un bridge puede constituir una pieza de equipamiento autónoma, independiente (un bridge externo) o se puede instalar en un servidor. Si el sistema operativo de red (NOS) lo admite, puede instalar una o más tarjetas de red (NIC) generando un bridge interno.

Su popularidad en grandes redes se debe a que:

- Son sencillos de instalar y transparentes a los usuarios.
- Son flexibles y adaptables.
- Son relativamente baratos.

Repetidores

Un repetidor es la expresión mínima de un concentrador, o dicho con más propiedad, podemos afirmar que un concentrador es un repetidor multipuerto. Los repetidores, con solo dos puertos, diseñados según las especificaciones IEEE 802.3, actúan como una parte del cableado de la red, ya que transfieren los paquetes recibidos de un extremo al otro, independientemente de su contenido, su origen y su destino, es decir, de un modo totalmente transparente e indiscriminado. Nos permiten interconectar dos o más segmentos incluso con diferentes tipos de cableado, permitiéndonos, de este modo, sobrepasar el número máximo de nodos o la longitud máxima permitidas por segmento.

Se encargan de regenerar las señales y resincronizar los segmentos, e incluso de desconectar a aquellos que funcionan inadecuadamente, permitiendo así que el resto de la red siga trabajando. Por supuesto, el uso de repetidores también esta limitado, ya que generan un pequeño retraso, que en caso de prolongarse por varios repetidores consecutivos, impediría el adecuado funcionamiento de la red y la perdida de los paquetes que circulan por la misma; entre dos nodos cualesquiera de la red, pueden existir un máximo de cuatro repetidores, lo que equivale a cinco segmentos, y además en un máximo de tres de ellos pueden conectarse otros nodos (es decir dos de los cinco segmentos sólo pueden ser empleados para la interconexión entre repetidores).

La velocidad a la que transmiten los paquetes es siempre la misma que la de la propia red. Los repetidores actúan, según el modelo OSI, a nivel físico (capa 1).

Diferencias entre bridge y repetidor

Los bridges trabajan a un nivel superior del modelo OSI que los repetidores. Esto significa que los bridges tienen más inteligencia que los repetidores y pueden tener más características relativas a los datos en las cuentas.

Mientras que los bridges parecen repetidores en el sentido que pueden regenerar los datos, este proceso se lleva a cabo a nivel de paquete. Esto significa que los bridges pueden enviar paquetes sobre distancias más largas utilizando una variedad de medios de larga distancia.

6.2. SWITCH

Un Switch es un dispositivo de Networking situado en la capa 2 del modelo de referencia OSI (no confundir con ISO: Organización Internacional para la Normalización).

En esta capa además se encuentran las NIC (Network Interface Card; Placa de Red) pueden ser inalámbricas y los Bridges (Puentes).

Comunes (PCI) Para conexión con medios físicos (cables) e inalámbricas.

Placas para puerto PMCIA (Para computadoras portátiles), para medios físicos e inalámbricos.

La capa 2 del modelo de referencia OSI es la capa de Enlace de datos, esta capa proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Un switch, al igual que un bridge (puente), es un dispositivo de la capa 2. De hecho, el switch se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto. La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, así hacen que la LAN sea mucho más eficiente. Los switches hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos. Esto hace que la LAN sea más lenta.

A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión (pueden ser de 8, 12, 24 o 48, o conectando 2 de 24 en serie), dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red).

La diferencia entre un hub y un switch está dada por lo que sucede dentro de cada dispositivo.

El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total.

6.3. 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. Este dispositivo se conoce como router.

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 costo 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 costo.

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.

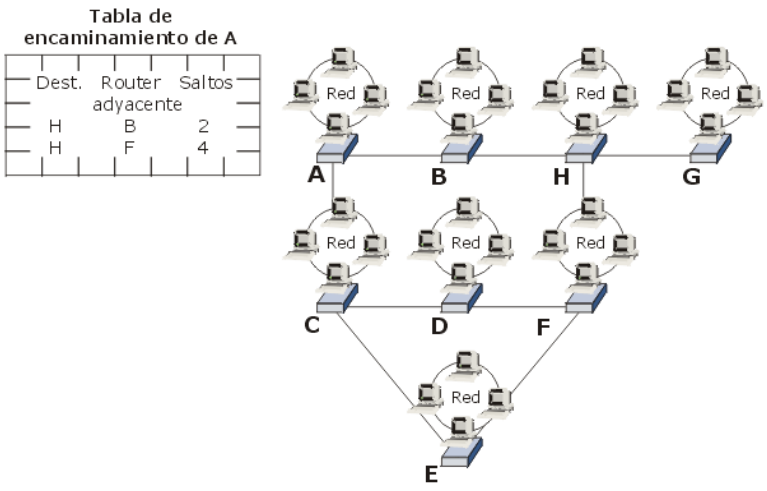


Figura 6.3. Tabla de encaminamiento de un router

Figura 6.3. Tomada de la dirección siguiente http://www.entrebits.cl/foros/networking/3331-routers.html

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 routers

Los tipos principales de routers son:

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

  - **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.

  - **Características**
    - Configuración manual del primer router. Detectan automáticamente redes y routers adicionales.
    - Pueden seleccionar una ruta en función de factores tales como costo 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

Los bridges y los routers se configuran para realizar las mismas cosas: enviar paquetes entre redes y enviar datos a través de los enlaces WAN, lo que plantea una cuestión importante: cuándo utilizar un bridge y cuando utilizar un router.

El bridge, que trabaja en el subnivel MAC del nivel de enlace de datos del modelo OSI, como se puede observar en la figura 6.4, 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.

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 6.4, 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.

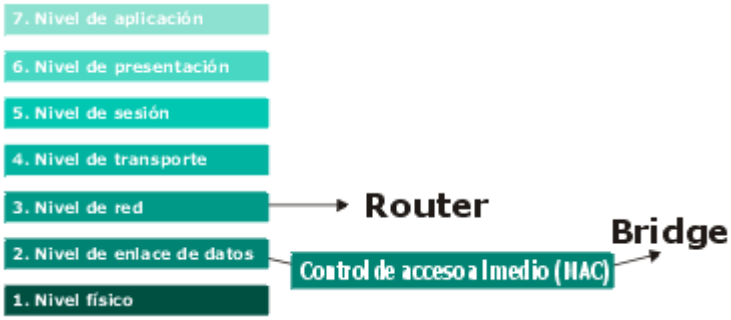


Figura 6.4. Capas Bridge, Router

Múltiples caminos. Un bridge sólo puede reconocer un único camino entre las redes. Un router puede buscar diferentes caminos activos y determinar en un momento determinado cuál resulta más adecuado.

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 6.5.

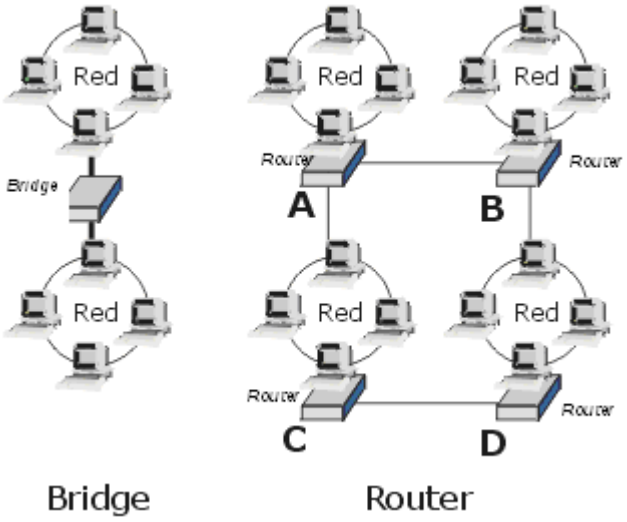


Figura 6.5. Caminos Router, Bridge

Figura 6.4. Tomada de la dirección siguiente http://carinalusso.iespana.es/Dispositivos%20de%20red.htm
Figura 6.5. Tomada de la dirección siguiente http://www.entrebits.cl/foros/networking/3332-diferencias-entre-bridges-y-routers.html

Conclusión:

- 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).

B-routers

Un brouter 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.

6.4. GATEWAY

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 referencia 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.

6.5. SIMULACIONES DE PRACTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

6.5.1. Guía de práctica: Conexión de varios dispositivos de interconectividad para una red

Correr la simulación correspondiente que se encuentra en el siguiente enlace CAPITULO VI\dispositivos de interconectividad.pka

Objetivo

- Conseguir la transferencia de paquetes entre todos los dispositivos de interconexión conectados a las red

Procedimiento

1. Iniciar con el software Packet Tracer 4.0. Como se indica en la figura 6.6.

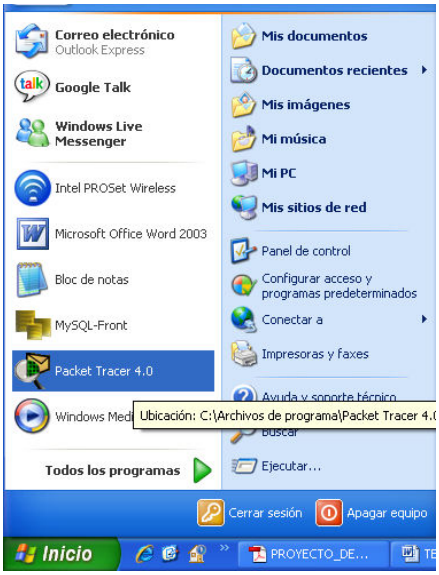


Figura 6.6. Inicio del software Packet Tracer

2. Primero debemos configurar la dirección IP y su respectiva mascara de red para todas las PC´s de la red, como se a mostrado en las practicas anteriores, 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, nuestra mascara de red y el Gateway como se puede observar en la figura 6.7.

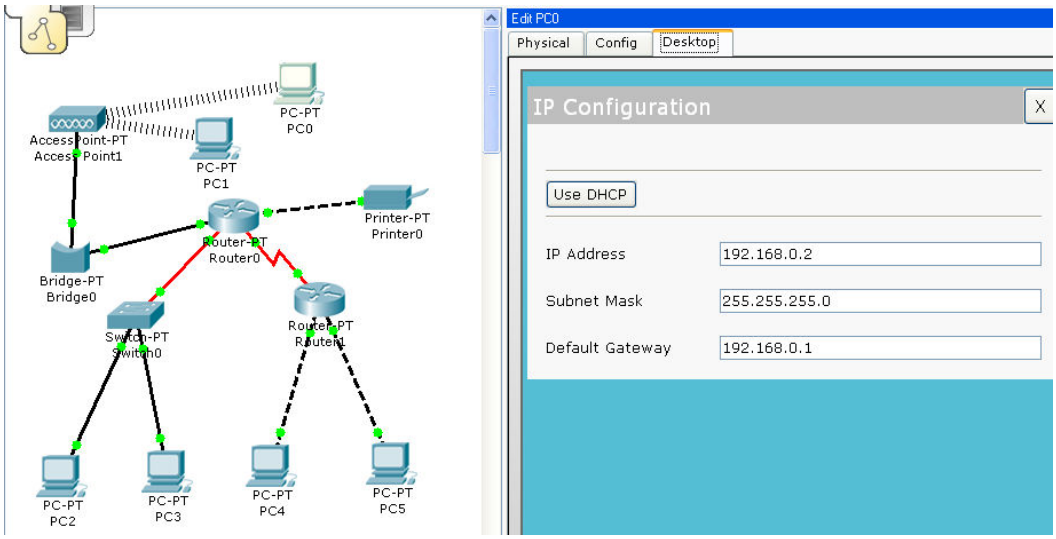


Figura 6.7. Edit PC0

3. El mismo procedimiento será utilizado para la configuración de las siguientes cinco CPU´s restantes, colocando las siguientes direcciones IP, mascaras de red y gateway como se muestran a continuación:
   - PC1
     - IP Address: 192.168.0.3
     - Subnet Mask: 255.255.255.0
     - Gateway: 192.168.0.1
   - PC2
     - IP Address: 192.168.3.2
     - Subnet Mask: 255.255.255.0
     - Gateway: 192.168.3.1
   - PC3
     - IP Address: 192.168.3.3
     - Subnet Mask: 255.255.255.0
     - Gateway: 192.168.3.1
   - PC4
     - IP Address: 192.168.1.2
     - Subnet Mask: 255.255.255.0
     - Gateway: 192.168.1.1
   - PC5
     - IP Address: 192.168.2.2
     - Subnet Mask: 255.255.255.0
     - Gateway: 192.168.2.1
4. En las CPU´s PC0 y PC1 se debe realizar el respectivo cambio de la tarjeta inalámbrica para su funcionamiento como se indica en la figura 6.8.

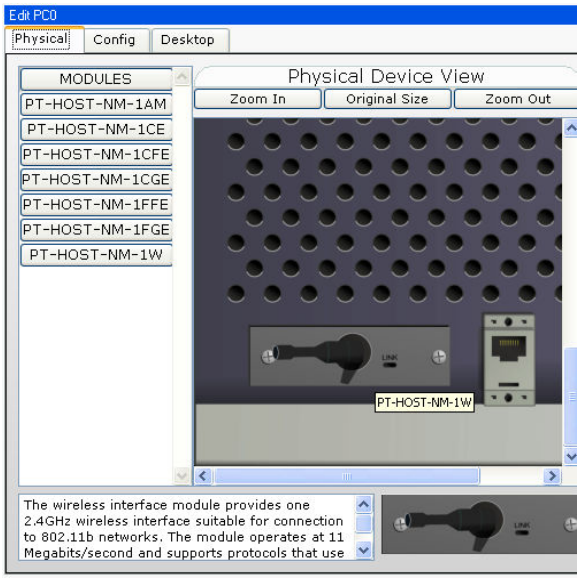


Figura 6.8. Tarjeta inalámbrica

5. Procedemos con la configuración de la dirección IP y su respectiva máscara 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 6.9.

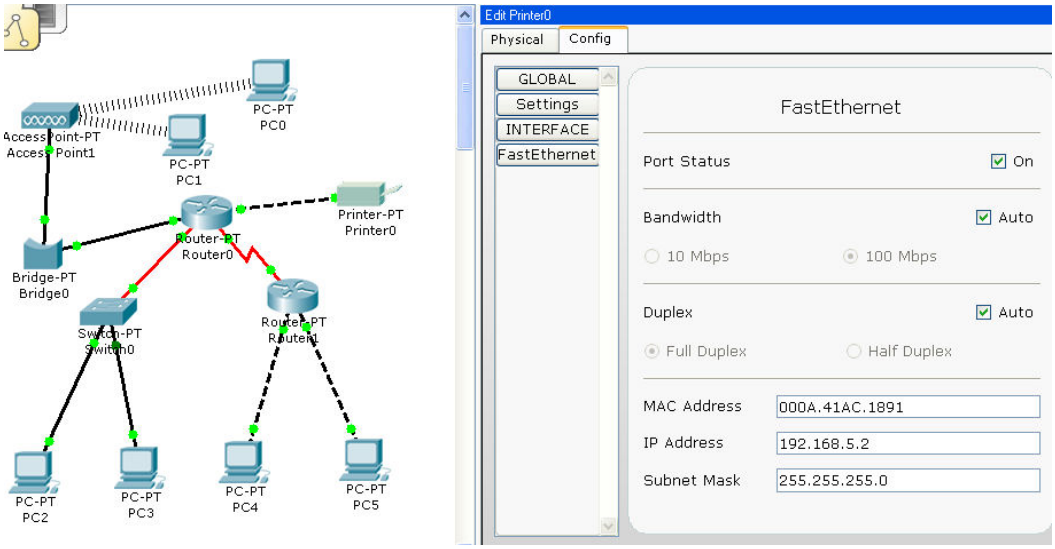


Figura 6.8. Configuración IP de la impresora

6. 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 6.10.

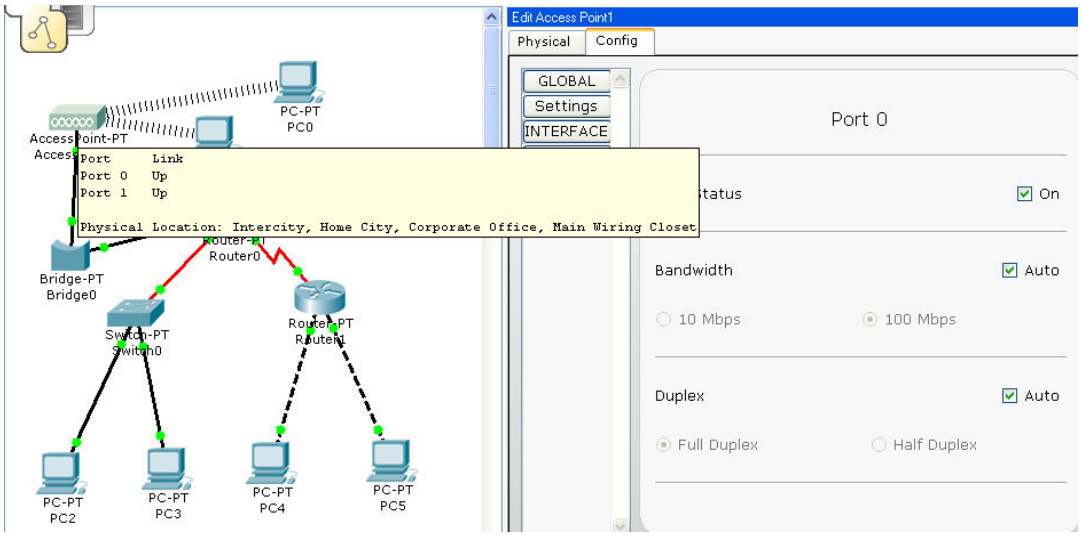


Figura 6.10. Verificación Access Point

7. Procedemos a dar un clic sobre el Bridge y procedemos a verificar que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 6.11.

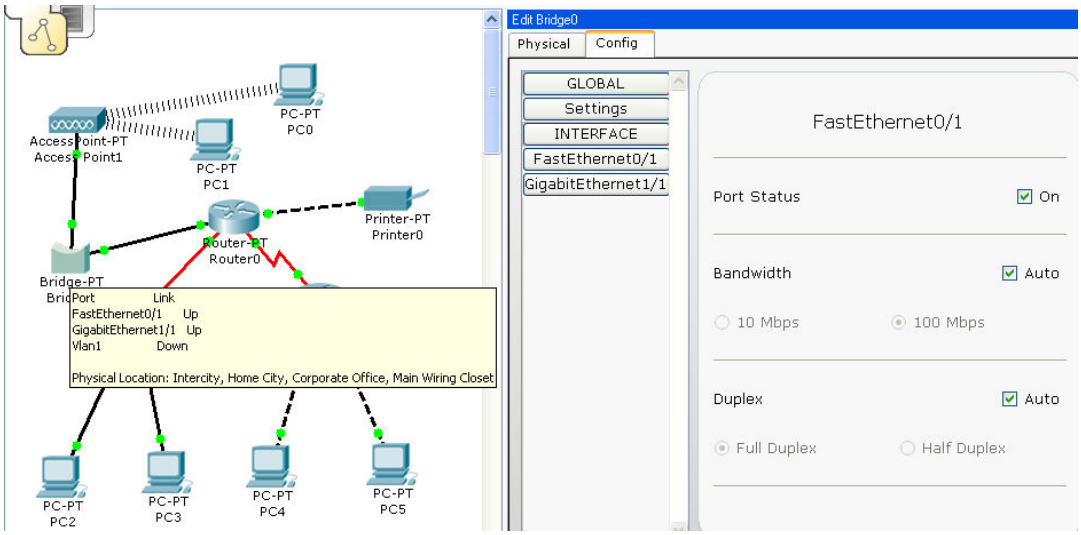


Figura 6.11. Verificación Bridge

8. Procedemos a dar un clic sobre el Router0 y procedemos a verificar que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 6.12.

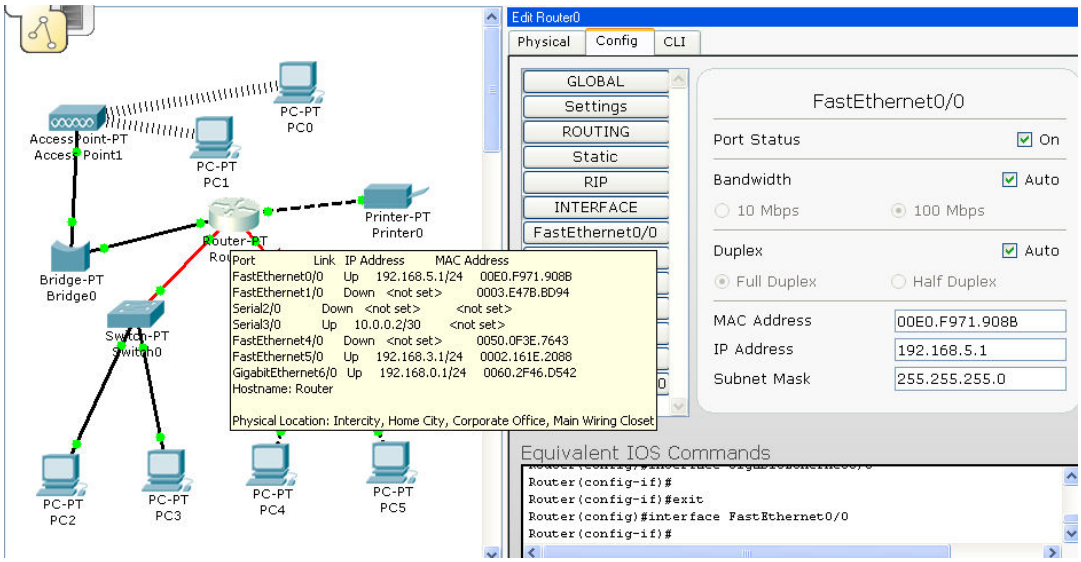


Figura 6.12. Verificación Router0

9. 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 6.13.

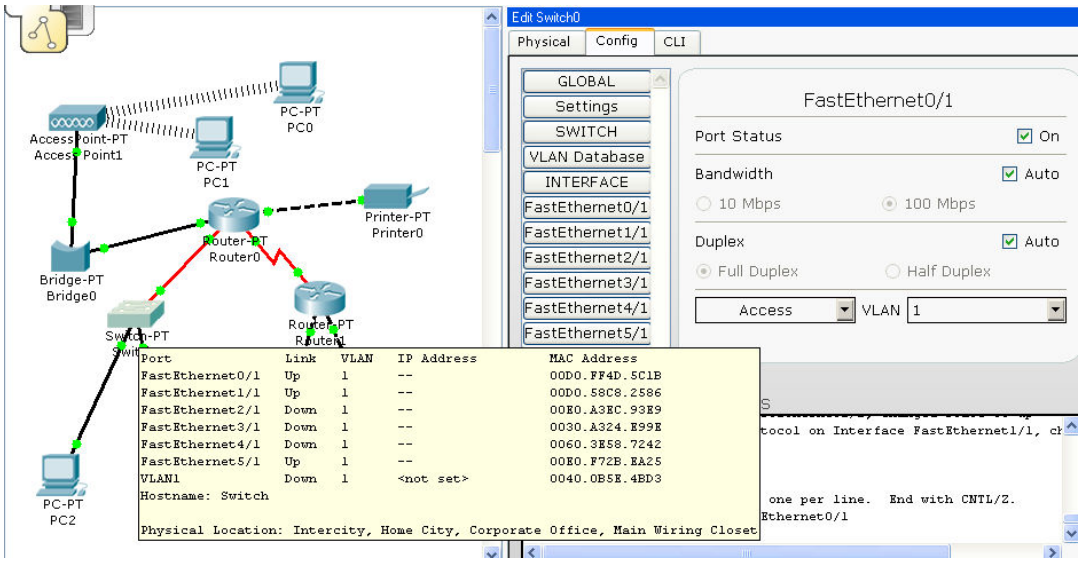


Figura 6.13. Verificación Switch0

10. Procedemos a dar un clic sobre el Router1 y procedemos a verificar que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 6.14.

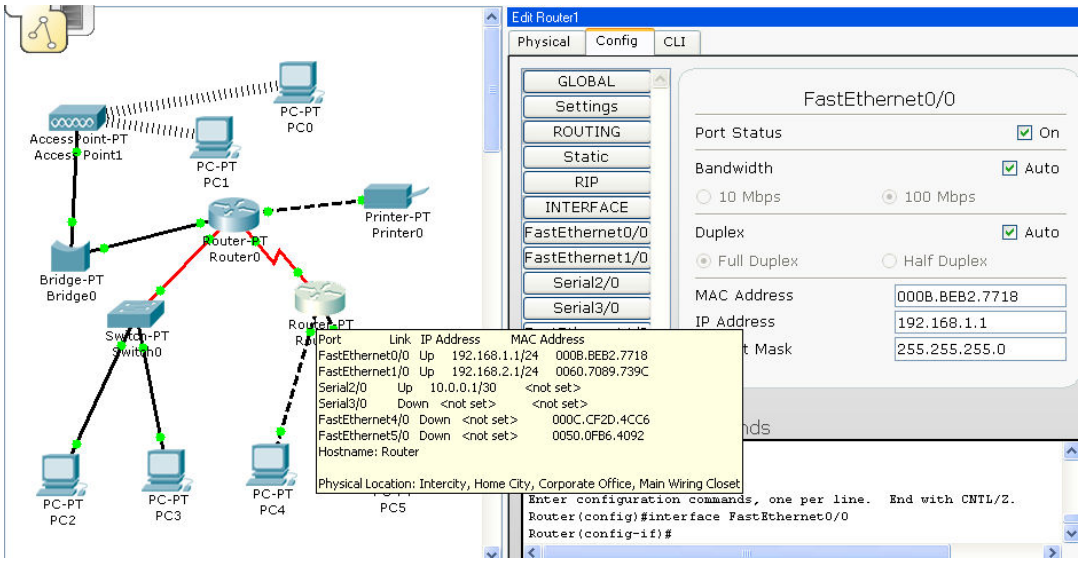


Figura 6.14. Verificación Router1

Desarrollo

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 Scenario 0 se va a comprobar la conexión entre la PC0 y la PC3 al enviar y recibir los datos, como se puede observar en la figura 6.15.

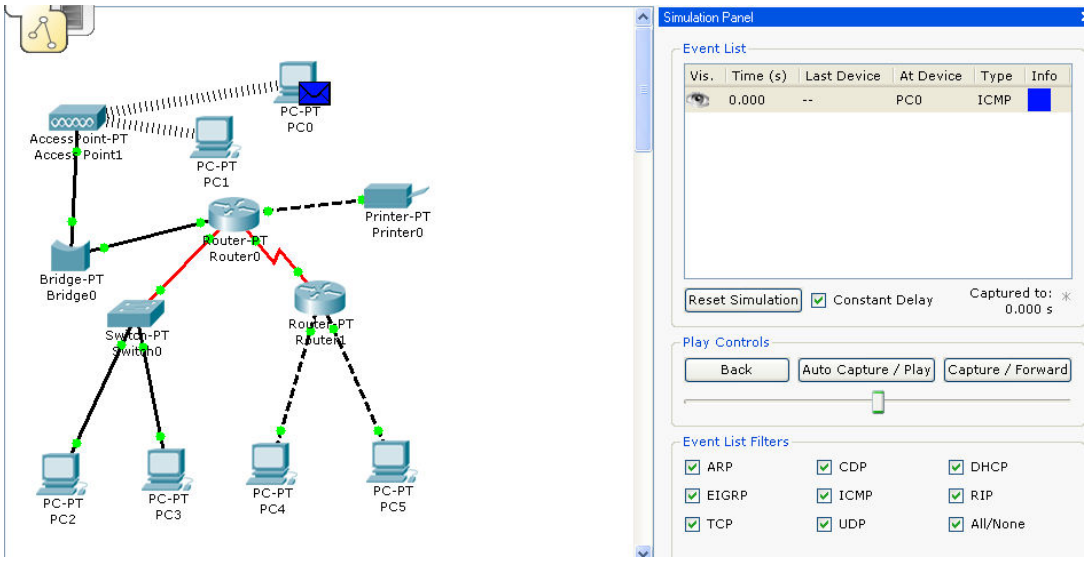


Figura 6.15. Colocación de paquete a ser transmitido

2. En la figura 6.16. Se puede observar claramente que con la simulación correspondiente el paquete se va trasladándose en este caso de la PC0 al Access Point comprobando de esta manera que la conexión se encuentra funcionando correctamente.

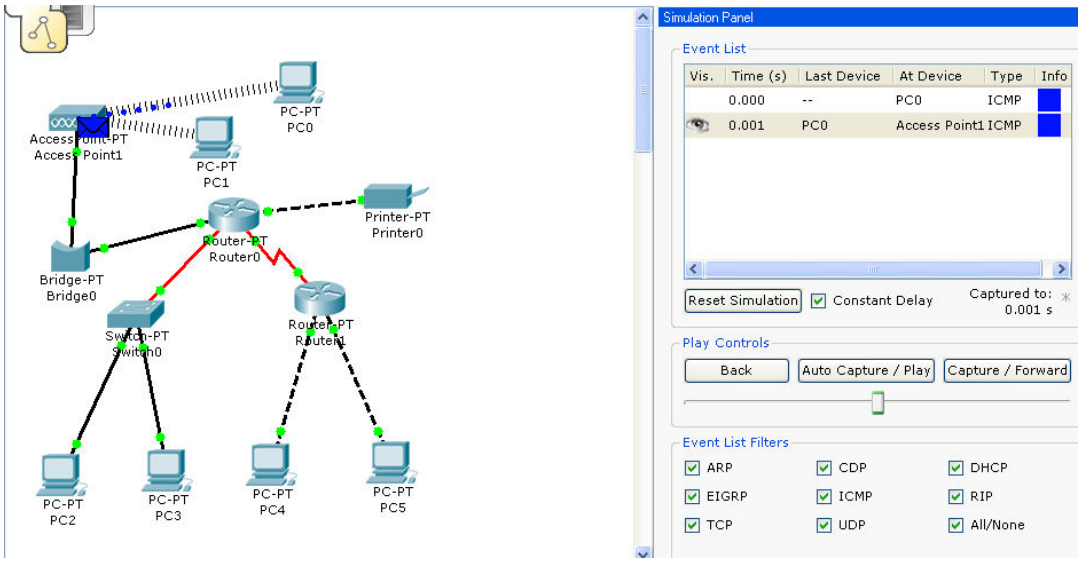


Figura 6.16. Simulación 1

3. Se debe continuar con la simulación correspondiente hasta que finalmente el paquete regrese a la PC0, confirmando de esta manera que la transferencia de datos es valida, como se puede observar en la figura 6.17. pero al mismo tiempo se observa que es enviado un paquete a la PC1 el mismo que es descartado debido a que ese no es el destino del paquete.

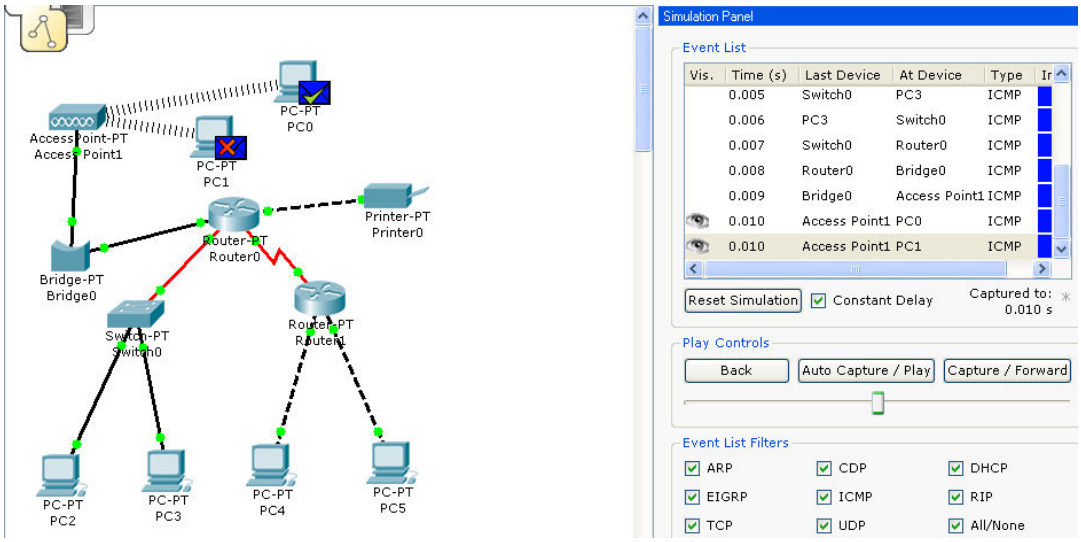


Figura 6.17. Simulación 2

Análisis de resultados

1. En la grafica 6.17 se muestra claramente que el paquete fue enviado y recibido a su destino, confirmando de esta manera que la conexión se encuentra en perfecto estado.

2. En nuestro caso se conectara con un cable serial DCE V.35 cuando se conecta dos ruteadores.

3. En nuestro caso se conecto con fibra entre el ruteador y el switch y entre el ruteador y el bridge es una conexión GigabitEthernet.

Conclusiones

1. Se puede observar muy claramente que la red se encuentra funcionando correctamente con todos los dispositivos de interconectividad que se encuentran conectados en la misma.

2. Con la simulación realizada se cumplieron los objetivos requeridos transmitiendo datos por todos los dispositivos conectados en la red.

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

4. En la figura 6.17 se observa que el paquete ha regresado al punto de partida (PC0), comprobando de esta manera que la conexión entre PC0 y PC3 se encuentra funcionando correctamente.

6.6. PRUEBAS DE OPCIÓN MÚLTIPLE

El banco de preguntas correspondiente al capitulo se encuentra en anexos.

Para realizar las pruebas de selección múltiple correspondientes a este capitulo se debe correr el programa que se encuentra en el siguiente vinculo index.html, o en http://www.fie-espe.edu.ec/preguntas y luego procedemos a ingresar los datos del alumno que va a realizar la prueba como se muestra en la figura 6.18

Figura 6.18. Datos Alumno

Para ingresar a resolver la prueba debemos elegir el capitulo que se va a realizar como se muestra en la figura 6.19 o se debe ingresar a la plantilla de preguntas e elegir igualmente el capitulo deseado.

Figura 6.19. Prueba Capitulo 6

El siguiente paso es realizar la prueba de selección múltiple como se indica en la figura 6.20. Luego de haber respondido a todas las preguntas se procede hacer clic sobre Corregir Prueba para que la prueba sea calificada y corregida automáticamente como se muestra en la figura 6.21.

Figura 6.20. Prueba selección múltiple

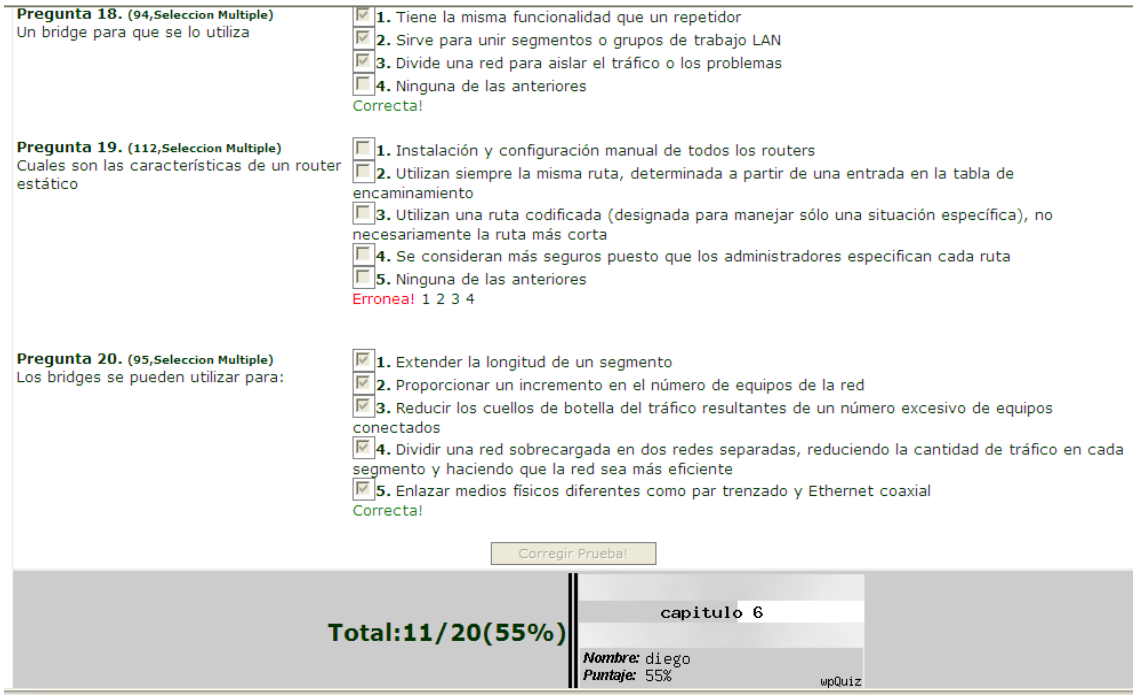


Figura 6.21. Calificación Prueba

CAPITULO VII

TCP-IP

7.1. DIRECCIONES IPV4 E IPV6

7.1.1. Direcciones Ipv4

IPv4 es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

Una dirección IPv4 se representa mediante un número binario de 32 bits. Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto puede ser entre 0 y 255 (el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255 en total).

Ejemplo de representación de dirección IPv4: *192.168.0.1*

IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido el Internet (mucho más de lo que se esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos, ya hace varios años se pudo comprobar que escaseaban las direcciones IPv4.Esta limitación ayudó a estimular el impulso hacia IPv6.

En la tabla 7.1. Se puede observar el Datagrama de las direcciones IPv4

Tabla 7.1. Datagrama IPv4

Versión	Lon Cab	DS (DiffServ)	Longitud Total			
Identificación			Res.	DF	MF	Desplazam. de Fragmento
Tiempo de vida (TTL)	Protocolo		Checksum			
Dirección de origen						
Dirección de destino						
Opciones (de 0 a 40 bytes)						

Descripción de cada cuadro del datagrama:

- **Versión**: 4.
- **Longitud Cabecera**: en palabras de 32 bits (mínimo 5, máximo 15).
- **DS (Differentiated Services):** Para Calidad de Servicio (QoS).
- **Longitud total**: en bytes, máximo 65535 (incluye la cabecera).
- **Campos de Fragmentación**: Identificación, DF, MF, Desplaz. Fragmento.
- **Tiempo de vida (TTL):** cuenta saltos hacia atrás (se descarta cuando es cero).
- **Checksum**: comprueba toda la cabecera (pero no los datos).

7.1.2. Direcciones Ipv6

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits, el equivalente a unos $3.4x10^{38}$ hosts direccionables. La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

El cambio más drástico de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores.

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF.

Ejemplo: *2001:123:4:ab:cde:3403:1:63*

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera y los datos.

La cabecera está en los primeros 40 bytes del paquete y contiene las direcciones de origen y destino (128 bits cada una), la versión de IP (4 bits), la clase de tráfico (8 bits, Prioridad del Paquete), etiqueta de flujo (20 bits, manejo de la Calidad de Servicio), longitud del campo de datos (16 bits), cabecera siguiente (8 bits), y límite de saltos (8 bits, Tiempo de Vida). Después viene el campo de datos, con los datos que transporta el paquete, que puede llegar a 64k de tamaño en el modo normal, o más con la opción "jumbo payload".

En IPv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en IPv4 en donde los routers pueden fragmentar un paquete. En IPv6, las opciones también se salen de la cabecera estándar y son especificadas por el campo "Cabecera Siguiente" (*Next Header*), similar en funcionalidad en IPv4 al campo Protocolo. Un ejemplo: en IPv4 uno añadiría la opción "ruta fijada desde origen" (*Strict Source and Record Routing*) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo "Cabecera Siguiente" indicando que una cabecera de encaminamiento es la siguiente en venir. La cabecera de encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete, e indicar que, por ejemplo, la cabecera TCP será la siguiente. Este procedimiento es análogo al de AH y ESP en IPsec para IPv4 (que aplica a IPv6 de igual modo, por supuesto).

En la tabla 7.2. Se puede observar el Datagrama de las direcciones IPv6

Tabla 7.2. Datagrama IPv6

Version	Prioridad	Etiqueta de flujo
Longitud	Siguiente cabecera	Limite de existencia
Direccion de Origen		
Direcion de Destino		

Resumen:

- **Direcciones:** Pasa a direcciones de 128 bits.
- **Eficiencia:** Simplifica cabeceras. Omite checksum. Estructura jerárquica, reduce tablas de routing.
- **Seguridad:** Incorpora mecanismos de privacidad y validación mediante criptografía.
- **Calidad de Servicio (QoS):** Previsto soporte de tráfico en tiempo real.
- **Multicast:** Mejora soporte.
- **Sencillez:** Posibilidad de autoconfiguración de equipos.
- **Movilidad:** Permite movilidad manteniendo dirección.
- **Evolución:** Contempla mecanismo para futuras opciones.
- **Compatibilidad:** puede coexistir con IPv4, pero no son compatibles.

7.2. DIRECCIONAMIENTO IP

7.2.1. Direccionamiento en Redes

Normalmente debería haber una dirección por cada nivel, pero hay niveles internos que no necesitan, por lo tanto las direcciones necesarias para alcanzar una maquina remota son tres:

- Una dirección para identificar la *aplicación*: conocida como puerto, TCP/IP o A-SAP (Service Access Point).
- Dirección de *Internet* (IP). Identifica la red y el ordenador (la identificación de ordenador, en esta dirección solo es interesante para ordenadores conectados a la misma red).

- Dirección *física* o hardware, identifica la dirección propia de la tarjeta de red (identificador del ordenador real "MAC").

Las direcciones de Internet pueden ser simbólicas o numéricas. La forma simbólica es más fácil de leer, por ejemplo: minombre@tcpip.com. La forma numérica es un número binario sin signo de 32 bits, habitualmente expresado en forma de números decimales separados por puntos. Por ejemplo, 128.167.5.8 es una dirección de Internet válida. La forma numérica es usada por el software de IP. La función de mapeo entre los dos la realiza el *DNS (Domain Name System)*. Primeramente examinaremos la forma numérica, denominada dirección IP.

La dirección IP

Para ser capaz de identificar una máquina en Internet, a cada interfaz de red de la máquina o host se le asigna una dirección, la *dirección IP*, o *dirección de Internet*. Cuando la máquina está conectada a más de una red se le denomina *"multi-homed"* y tendrá una dirección IP por cada interfaz de red. La dirección IP consiste en un par de números:
IP dirección = <número de red <número de interfaz de red.

- La parte de la dirección IP correspondiente al *número de red* está administrada centralmente por el InterNIC (Internet Network Information Center) y es única en toda la Internet.
- Las direcciones IP son números de 32 bits representados habitualmente *en formato decimal* (la representación decimal de cuatro valores binarios de 8 bits concatenados por puntos). Por ejemplo*128.2.7.9* es una dirección IP, donde 128.2 es el número de red y 7.9 el de la interfaz de red. Las reglas usadas para dividir una dirección de IP en su parte de red y de interfaz de red se explican a continuación.

El formato binario para la dirección IP 128.2.7.9 es:

10000000 00000010 00000111 00001001

Las direcciones IP son usadas por el protocolo IP para definir únicamente un host en la red. Los datagramas IP (los paquetes de datos elementales intercambiados entre máquinas) se transmiten a través de alguna red física conectada a la interfaz de la máquina y cada uno de ellos contiene la *dirección IP de origen* y *la dirección IP de destino*. Para enviar un

datagrama a una dirección IP de destino determinada la dirección de destino de ser traducida o mapeada a una dirección física. Esto puede requerir transmisiones en la red para encontrar la dirección física de destino.

- Los primeros bits de las direcciones IP especifican como el resto de las direcciones deberían separarse en sus partes de red y de interfaz.
- Los términos *dirección de red* y *netID* se usan a veces en vez de número de red, pero el término formal, utilizado en RFC 1166, es número de red. Análogamente, los términos *dirección de host* y *hostID* se usan ocasionalmente en vez de número de host.

Hay cinco clases de direcciones IPv4 las cuales se observa en la figura 7.1.

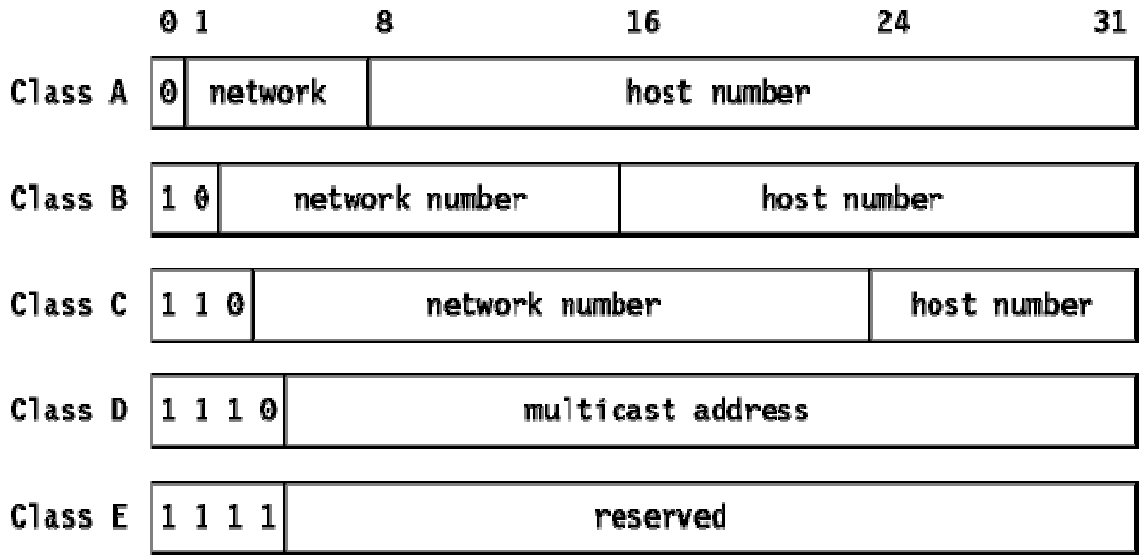


Figura 7.1. Clases asignadas de direcciones IPv4 de internet

Nota: Dos de los números de red de cada una de las clases A, B y C, y dos de los números de host de cada red están preasignados: los que tienen todos los bits a 0 y los que tienen todos los bits a 1.

- Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes (veremos posteriormente que de cada par de direcciones de red y de

host, dos tienen un significado especial). Los restantes 24 bits se emplean para el número de host, de modo que cada red tiene hasta 16,777,214 hosts.

- Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16382 redes de hasta 65534 hosts cada una.
- Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2,097,150 redes de hasta 254 hosts cada una.
- Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada.
- Las direcciones de clase E se reservan para usos en el futuro

Es obvio que una dirección de clase A sólo se asignará a redes con un elevado número de hosts, y que las direcciones de clase C son adecuadas para redes con pocos hosts. Sin embargo, esto significa que las redes de tamaño medio (aquellas con más de 254 hosts o en las que se espera que en el futuro haya más de 254 hosts).

7.3. DIRECCIONES PÚBLICAS Y PRIVADAS

7.3.1. Direcciones IP especiales

Como se ha señalado anteriormente, cualquier componente de una dirección IP con todos sus bits a 1 o a 0 tiene un significado especial:

Con todos los bits a 0 significa: “este”, direcciones IP con número de host=0 o direcciones IP con número de red=0 y sólo se usa cuando el valor real no se conoce. Esta forma de expresar direcciones se utiliza con direcciones IP fuente, cuando el host trata de determinar sus direcciones IP por medio de un servidor remoto. El host puede incluir su número de host, si lo conoce, pero no su número de red o subred.

Con todos los bits a 1 significa "todos": todas las redes o todos los hosts. Por ejemplo, 128.2.255.255 (una dirección de clase B con número de host 255.255) significar "todos los host de la red 128.2". Esta forma de expresar direcciones se emplea en mensajes de broadcast.

Hay otra dirección de especial importancia: el número de red de clase A con todos los bits a 1, 127, se reserva para la *dirección de loopback*. Todo lo que se envíe a una dirección con 127 como valor del byte de mayor orden, por ejemplo 127.0.0.1, no debe encaminarse a través de la red, sino directamente del controlador de salida al de entrada.

En las siguientes tablas se puede observar muy claramente, por ejemplo en la tabla 7.2 se observa su dirección, su significado y un ejemplo y en la tabla 7.3 se puede observar su red y su uso.

Tabla 7.2. Dirección, significado y ejemplo

Dirección	Significado	Ejemplo
255.255.255.255	Broadcast en la propia red o subred	
0.0.0.0	Identifica al host que envía el datagrama	Usado en BOOTP
Host a ceros	Identifica una red (o subred)	147.156.0.0
Host a unos	Broadcast en esa red (o subred)	147.156.255.255
Red a ceros	Identifica un host en la propia red (o subred)	0.0.1.25
127.0.0.1	Dirección Loopback	
224.0.0.1	Todos los hosts multicast	

Tabla 7.3. Red y uso

Red o rango	Uso
127.0.0.0	Reservado (fin clase A)
128.0.0.0	Reservado (ppio. Clase B)
191.255.0.0	Reservado (fin clase B)
192.0.0.0	Reservado (ppio. Clase C)
224.0.0.0	Reservado (ppio. Clase D)
240.0.0.0 – 255.255.255.254	Reservado (clase E)
10.0.0.0	Privado
172.16.0.0 – 172.31.0.0	Privado
192.168.0.0 – 192.168.255.0	Privado

7.4. MÁSCARAS

Una máscara de red es un conjunto de cuatro números separados por puntos. Cada número se representa normalmente como el equivalente decimal de un número binario de 8 bits, lo que significa que cada número puede tomar valores entre 0 (todos los bits en cero) y 255 (todos los bits en uno). Cada dirección IP consiste de dos partes (la dirección de red y el número de máquina). La máscara de red se usa para determinar el tamaño de cada una de estas partes. Las posiciones de los bits en uno de la máscara se consideran parte del espacio reservado para la dirección de red, mientras que los bits que están puestos a cero se consideran parte del espacio apartado para el número de máquina.

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Mediante la máscara de red una computadora podrá saber si debe enviar los datos dentro o fuera de la red. Por ejemplo, si el router tiene la IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una IP que empiece por 192.168.1 va para la red local y todo lo que va a otras IPS, para fuera (internet, otra red local mayor...).

Supongamos que tenemos un rango de direcciones IP desde 10.0.0.0 hasta 10.255.255.255. Si todas ellas formaran parte de la misma red, su máscara de red sería: 255.0.0.0. También se puede escribir como 10.0.0.0/8

Como la máscara consiste en una secuencia de unos y ceros, los números permitidos para representar la secuencia son los siguientes: 0, 128, 192, 224, 240, 248, 252, 254, y 255.

La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y los bits de host usados por las subredes. Así, en esta forma de representación (10.0.0.0/8) el 8 sería la cantidad de bits puestos a 1 que contiene la máscara en binario, comenzando desde la izquierda. Para el ejemplo dado (/8), sería 11111111.00000000.00000000.00000000 y en su representación en decimal sería 255.0.0.0.

Una máscara de red representada en binario son 4 octetos de bits (11111111.11111111.11111111.11111111).

Ejemplo:
8bit x 4 octetos = 32 bit. (11111111.11111111.11111111.11111111 = 255.255.255.255)
8bit x 3 octetos = 24 bit. (11111111.11111111.11111111.00000000 = 255.255.255.0)
8bit x 2 octetos = 16 bit. (11111111.11111111.00000000.00000000 = 255.255.0.0)
8bit x 1 octetos = 8 bit. (11111111.00000000.00000000.00000000 = 255.0.0.0)

En el ejemplo 10.0.0.0/8, según lo explicado anteriormente, indicaría que la máscara de red es 255.0.0.0

Las máscaras, se utilizan como validación de direcciones realizando una operación AND lógica entre la dirección IP y la máscara para validar al equipo cosa que permite realizar una verificación de la dirección de la Red y con un OR y la mascara negada se obtiene la dirección del broadcasting, como se observa en la figura 7.2.

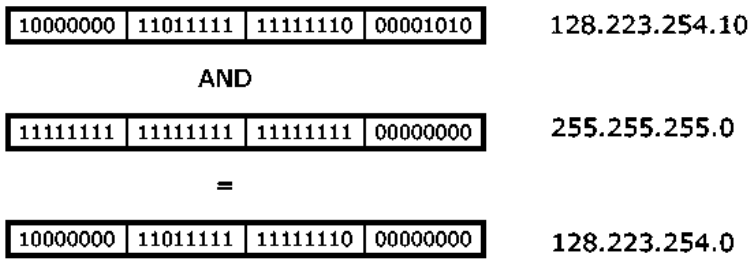


Figura 7.2. Máscara de red

7.5. SUBREDES Y SUPERREDES

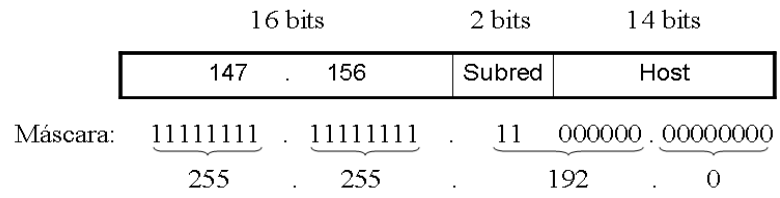
7.5.1. Subredes

- La máscara identifica que parte de la dirección es red-subred y que parte es host.
- Si la parte host es cero la dirección es la de la propia subred.
- La dirección con la parte host toda a unos esta reservada para broadcast en la subred.
- En cada subred hay siempre dos direcciones reservadas, la primera y la última.

Ejemplo:

En la figura 7.3. se puede observar un ejemplo de subred en la cual se va a dividir una red de clase B en cuatro subredes

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



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 7.3. Subredes clase B

En la siguiente tabla 7.3. se realiza las subredes para una clase C, explicando el número de subredes, número de host, su máscara, entre otras.

Tabla 7.3. Subredes clase C

Bits Subred	Nº subredes	Nº subredes	Bits host	Nº hosts	Máscara	Último byte de la máscara en binario
0	0	0	8	254	255.255.255.0	00000000
1	0	2	7	126	255.255.255.128	10000000
2	2	4	6	62	255.255.255.192	11000000
3	6	8	5	30	255.255.255.224	11100000
4	14	16	4	14	255.255.255.240	11110000
5	30	32	3	6	255.255.255.248	11111000
6	62	64	2	2	255.255.255.252	11111100
7	126	128	1	0	255.255.255.254	11111110
8	254	256	0	0	255.255.255.255	11111111

Debido al crecimiento explosivo de Internet, el uso de direcciones IP asignadas se volvió demasiado rígido para permitir cambiar con facilidad la configuración de redes locales. Estos cambios podían ser necesarios cuando:

- Se instala una nueva red física.
- El crecimiento del número de hosts requiere dividir la red local en dos o más redes.
- Para evitar tener que solicitar direcciones IP adicionales en estos casos, se introdujo el concepto de *subred*.

El número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. Esta segunda red se denomina *subred*. La red principal consiste ahora en un conjunto de subredes y la dirección IP se interpreta como número de red, número de subred, número de host

La combinación del número de subred y del host suele denominarse "dirección local" o parte local. La creación de subredes se implementa de forma que es transparente a redes remotas. Un host dentro de una red con subredes es consciente de la existencia de estas, pero un host de una red distinta no lo es, sigue considerando la parte local de la dirección IP como un número de host.

La división de la parte local de la dirección IP en números de subred y de host queda a libre elección del administrador local, cualquier serie de bits de la parte local se puede tomar para la subred requerida. La división se efectúa empleando una *máscara de subred* que es un número de 32 bits. Los bits a cero en esta máscara indican posiciones de bits correspondientes al número de host, y los que están a uno, posiciones de bits correspondientes al número de subred. Las posiciones de la máscara pertenecientes al número de red se ponen a uno pero no se usan. Al igual que las direcciones IP, las máscaras de red suelen expresarse en formato decimal.

El tratamiento especial de "todos los bits a cero" y "todos los bits a uno" se aplica a cada una de las tres partes de dirección IP con subredes del mismo modo que a una dirección IP que no las tiene. Por ejemplo, una red de clase B con subredes, que tiene un parte local de 16 bits, podría hacer uso de uno de los siguientes esquemas:

- El primer byte es el número de subred, el segundo el de host. Esto proporciona 254 (256 menos dos, al estar los valores 0 y 255 reservados) posibles subredes, de 254 hosts cada una. La máscara de subred es 255.255.255.0.

- Los primeros 12 bits se usan para el número de subred, y los 4 últimos para el de host. Esto proporciona 4094 posibles subredes (4096 menos 2), pero sólo 14 host por subred. La máscara de subred es 255.25.255.240. Hay muchas otras posibilidades.

Mientras el administrador es totalmente libre de asignar la parte de subred a la dirección local de cualquier forma legal, el objetivo es asignar un *número* de bits al número de subred y el resto a la dirección local. Por tanto, es corriente usar un bloque de bits contiguos al comienzo de la parte local para el número de subred ya que así las direcciones son más legibles (esto es particularmente cierto cuando la subred ocupa 8 o 16 bits). Con este enfoque, cualquiera de las máscaras anteriores es buena, pero no máscaras como 255.255.252.252 o 255.255.255.15.

Tipos de "subnetting"

Hay dos tipos de "subnetting": estático y de longitud variable (dinámico).
El de longitud variable es el más flexible de los dos. El tipo de "subnetting" disponible depende del protocolo de encaminamiento en uso, el IP nativo sólo soporta "subnetting" estático, al igual que el ampliamente utilizado RIP. Sin embargo, la versión 2 del protocolo RIP soporta además "subnetting" de longitud variable.

"Subnetting" estático

El "subnetting" estático consiste en que todas las subredes de la red dividida empleen la misma máscara de red. Esto es simple de implementar y de fácil mantenimiento, pero implica el desperdicio de direcciones para redes pequeñas. Por ejemplo, una red de cuatro hosts que use una máscara de subred de 255.255.255.0 desperdicia 250 direcciones IP. Además, hace más difícil reorganizar la red con una máscara nueva. Hoy en día, casi todos los hosts y routers soportan "subnetting" estático.

"Subnetting" de longitud variable (dinámico)

Cuando se utiliza "subnetting" de longitud variable, las subredes que constituyen la red pueden hacer uso de diferentes máscaras de subred. Una subred pequeña con sólo unos pocos hosts necesita una máscara que permita acomodar sólo a esos hosts. Una subred con muchos puede requerir una máscara distinta para direccionar esa elevada cantidad de hosts. La posibilidad de asignar máscaras de subred de acuerdo a las necesidades individuales de cada subred ayuda a conservar las direcciones de red. Además, una subred se puede dividir en dos añadiendo un bit a la máscara. El resto de las subredes no se verán afectadas por el cambio. No todos los hosts y routers soportan "subnetting" de longitud variable.

Mezclando "subnetting" estático y de longitud variable

A primera vista, parece que la presencia de un host que sólo puede manejar "subnetting" estático impediría utilizar "subnetting" de longitud variable en cualquier punto de la red. Afortunadamente no es este el caso. Siempre que los routers entre las subredes que tengan distintas máscaras usen "subnetting" de longitud variable, los protocolos de encaminamiento son capaces de ocultar la diferencia entre máscaras de subred a cada host de una subred. Los hosts pueden seguir usando encaminamiento IP básico y desentenderse de las complejidades del "subnetting", que quedan a cargo de routers dedicados a tal efecto.

7.5.2 Superredes

Una red se denomina *SUPERRED cuando la máscara de CIDR contiene menos bits a unos que la máscara por omisión de la red*. Es decir, con una máscara más corta en cuanto al número de *unos* que la máscara natural (255.255.252.0 es menor que 255.255.255.0 o lo que es lo mismo 22 es menor que 24), la red se define como una *superred*. Por tanto, cuando una entidad IP detecte lo anterior en una entrada de la tabla de encaminamiento, sabe que no está ante una dirección de red sino, ante una dirección de superred *(prefijo común + bloque CIDR)* que resume un bloque de direcciones adyacentes de red. Consecuentemente, las máquinas (de usuario y routers) que usan el direccionamiento de superred necesitan un software de encaminamiento no convencional que entienda los correspondientes rangos de direcciones

Para evitar terminar con el espacio de direcciones de IP de la clase B y poder hacer un uso más óptimo del espacio de direccionamiento en función del número de máquinas que, en realidad, se desea conectar; se ha creado el concepto de SUPERRED o CIDR (encaminamiento entre dominios sin clase) que se basa en una técnica que permite resumir un conjunto variable de direcciones IP contiguas de red de una clase en una misma dirección de IP de red de esa clase para, por un lado, disponer de un espacio de direccionamiento superior sin necesidad de solicitar una dirección de rango superior y, por otro lado, evitar que las tablas de encaminamiento, y los mensajes para una actualización dinámica de éstas entre routers contiguos, crezcan demasiado.

En la figura 7.4. se puede observar un ejemplo de formato y bloque CIDR. El *CIDR* es el número de direcciones de red contiguas que conforman el bloque o grupo de direcciones que se desea resumir en una sola dirección de red.

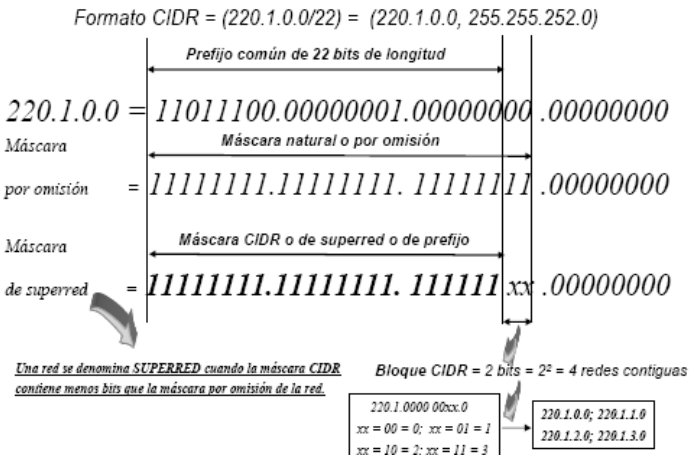


Figura 7.4. Ejemplo de formato y bloque CIDR

Las superredes se definen mediante máscaras, igual que las subredes

Ejemplo:

Red 195.100.16.0/21 (máscara 255.255.248.0)

Incluye desde 195.100.16.0/24 hasta 195.100.23.0/24

También se puede partir en trozos más pequeños partes de una clase A (de las que quedan libres). Por eso esta técnica se llama CIDR (Classless InterDomain Routing).

Resumen:

Problema: agotamiento del espacio de direcciones IP.

Causa: Clase A inaccesible, Clase B excesiva, C demasiado pequeña. Muchas organizaciones solicitaban clases B y usaban solo una pequeña parte.

Solución: asignar grupos de clases C a una organización.

Nuevo problema: explosión de las tablas de rutas.

Nueva solución: considerar un grupo contiguo de redes clase C como una sola red. Hacer superredes.

En la figura 7.5. se muestra muy claramente para donde se crean las superredes y las subredes.

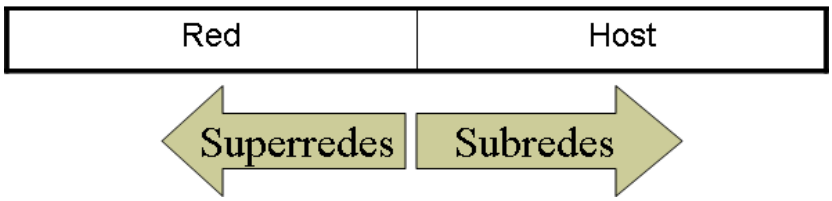


Figura 7.5. Superredes y Subredes

7.6. PROTOCOLOS DE CONTROL DE RED

La Internet tiene varios protocolos de control al nivel de red entre los cuales tenemos los siguientes:

- ICMP (Internet Control Message Protocol). Ejemplos de paquetes: No se puede alcanzar el destino, la vida de un paquete expiró, valor ilegal en el encabezamiento, paquete de bloqueo (no usado más), paquete de eco o respuesta.
- ARP (Address Resolution Protocol). En una LAN es difícil mantener la correspondencia entre las direcciones de IP y las direcciones de LAN (por ejemplo, en una Ethernet hay direcciones de 48 bits). El protocolo ARP permite que una máquina haga un broadcast para preguntar qué dirección local pertenece a alguna dirección de IP. En esta manera no se necesita una tabla de configuración, que simplifica la administración.
- RARP (Reverse ARP). Permite que una máquina que acaba de bootear pueda encontrar su dirección de IP.

- Hay también el protocolo BOOTP, cuyos mensajes son de UDP y se pueden reenviar sobre ruteadores.

7.7. SIMULACIONES DE PRÁCTICAS A TRAVÉS DEL SOFTWARE PACKET TRACER

7.7.1. Guía de práctica: Realizar 4 subredes de una clase tipo B

Correr la simulación correspondiente que se encuentra en el siguiente enlace CAPITULO VII\subredes clases B.pka

Objetivo

- Realizar cuatro subredes para una clase tipo B
- Conseguir la transferencia de paquetes entre todas las subredes de la clase B

Procedimiento

1. Iniciar con el software Packet Tracer 4.0. Como se indica en la figura 7.6.

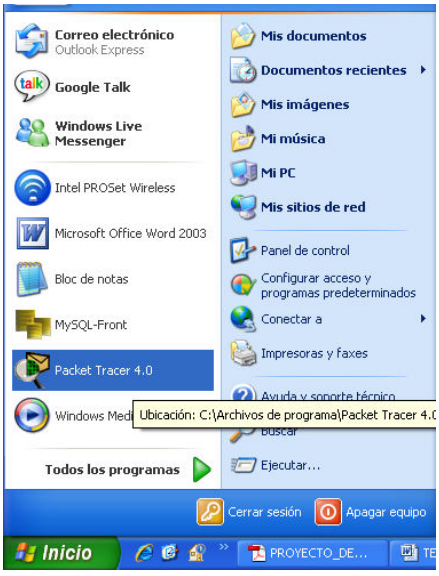


Figura 7.6. Inicio del software Packet Tracer

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 7.7.

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 7.7. Cuatro subredes de una clase B

3. Procedemos con la configuración de las CPU´s para lo cual damos un clic en la PC0 para que se abra una pantalla de configuración en la cual nos dirigirnos a la pestaña con el nombre de Desktop, y luego en IP Configuration en la que procedemos con la configuración de nuestra dirección IP, nuestra mascara de red y el respectivo gateway como se puede observar en la figura 7.8. El mismo procedimiento será utilizado para la configuración de las siguientes 18 CPU´s restantes, con la configuración que se muestra a continuación:

- PC1
  - IP Address: 147.156.0.4
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.0.1

- PC2
  - IP Address: 147.156.0.5
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.0.1

- PC3
  - IP Address: 147.156.0.6
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.0.1

- PC4
  - IP Address: 147.156.0.7
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.0.1

- PC5
  - IP Address: 147.156.0.8
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.0.1

- PC6
  - IP Address: 147.156.0.9
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.0.1

- PC7
  - IP Address: 147.156.0.10
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.0.1

- PC8
  - IP Address: 147.156.64.2
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.64.1

- PC9
  - IP Address: 147.156.64.4

- Subnet Mask: 255.255.192.0
- Gateway: 147.156.64.1

- PC10
  - IP Address: 147.156.128.2
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.128.1

- PC11
  - IP Address: 147.156.128.3
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.128.1

- PC12
  - IP Address: 147.156.128.4
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.128.1

- PC13
  - IP Address: 147.156.128.5
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.128.1

- PC14
  - IP Address: 147.156.128.6
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.128.1

- PC15
  - IP Address: 147.156.192.2
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.192.1

- PC16
  - IP Address: 147.156.192.3
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.192.1

- PC17
  - IP Address: 147.156.192.4
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.192.1

- PC18
  - IP Address: 147.156.192.5
  - Subnet Mask: 255.255.192.0
  - Gateway: 147.156.192.1

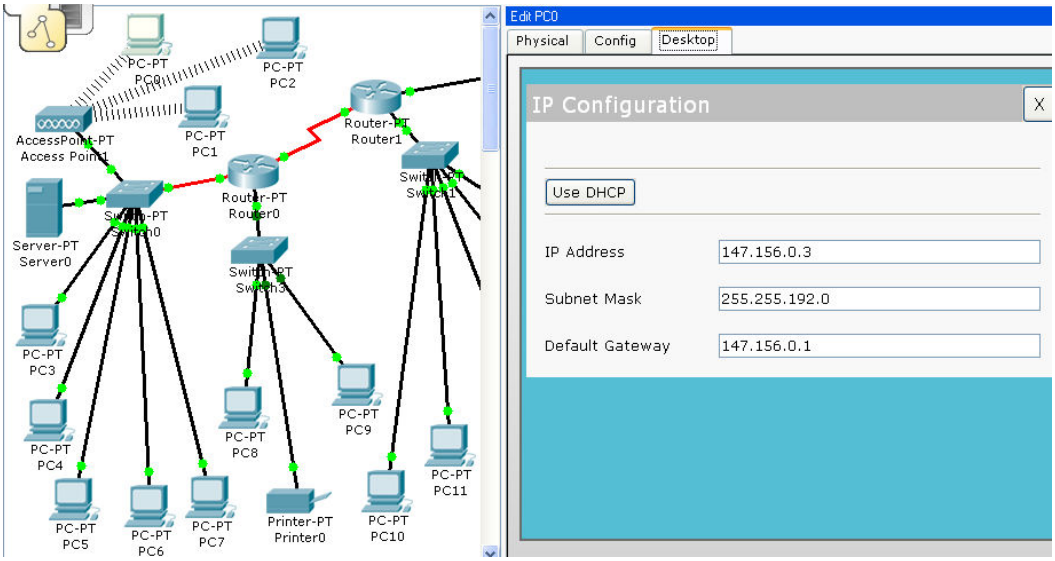


Figura 7.8. Edit PC0

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 7.9.

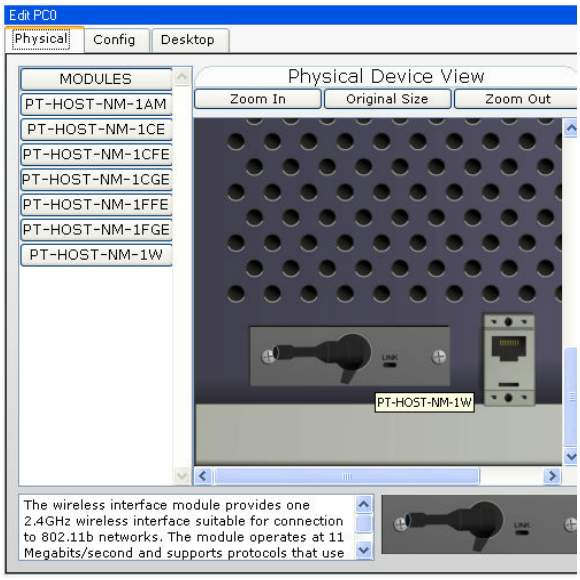


Figura 7.9. Tarjeta inalámbrica

5. Procedemos con la configuración de la dirección IP y su respectiva máscara 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 7.10.

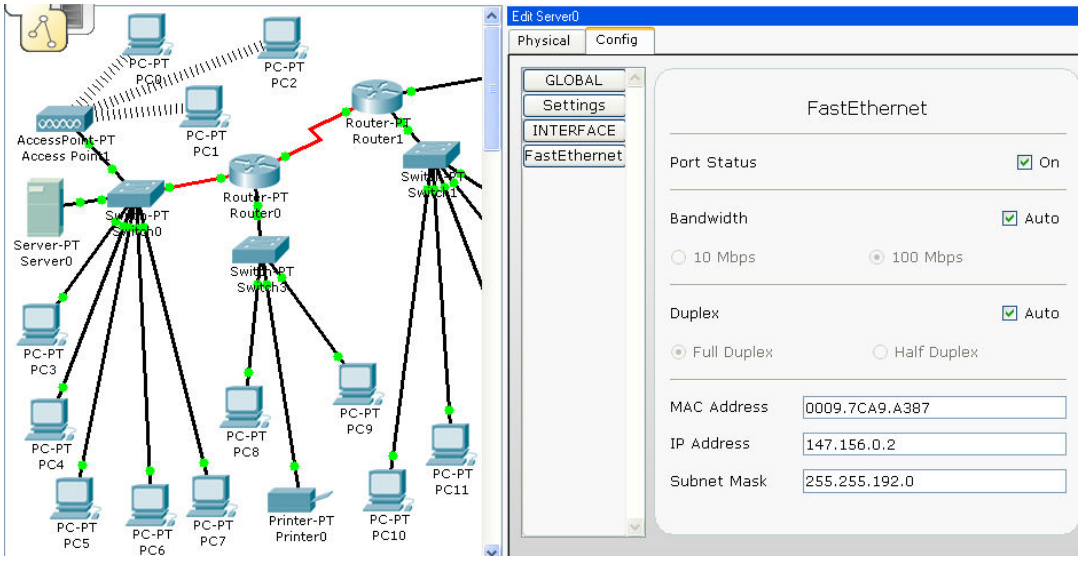


Figura 7.10. Configuración del Servidor

6. Procedemos con la configuración de la dirección IP y su respectiva máscara 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 7.11.

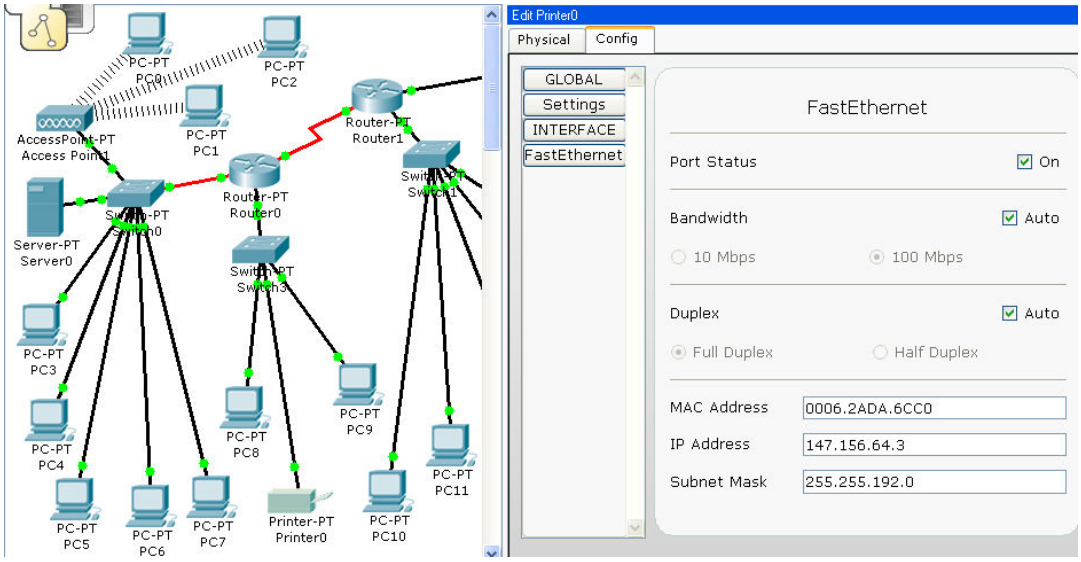


Figura 7.11. Configuración Impresora

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 7.12.

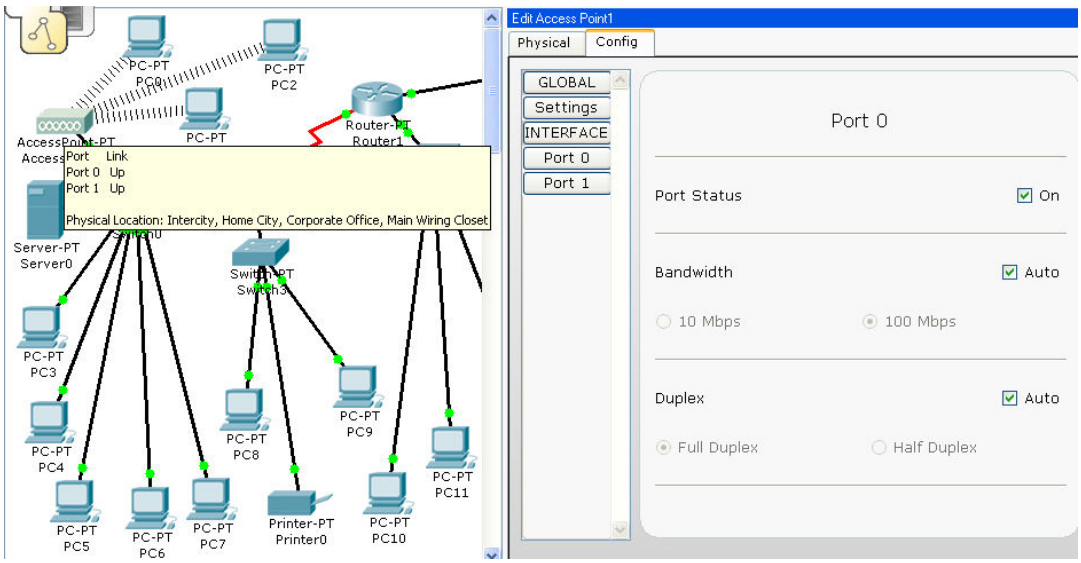


Figura 7.12. Verificación Access Point

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 7.13.

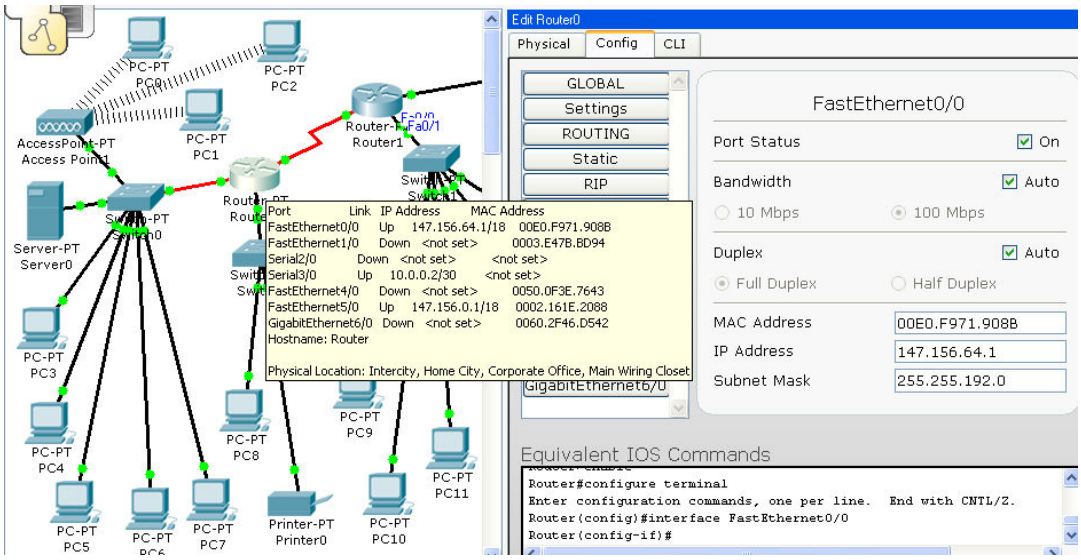


Figura 7.13. Verificación Routers

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 7.14.

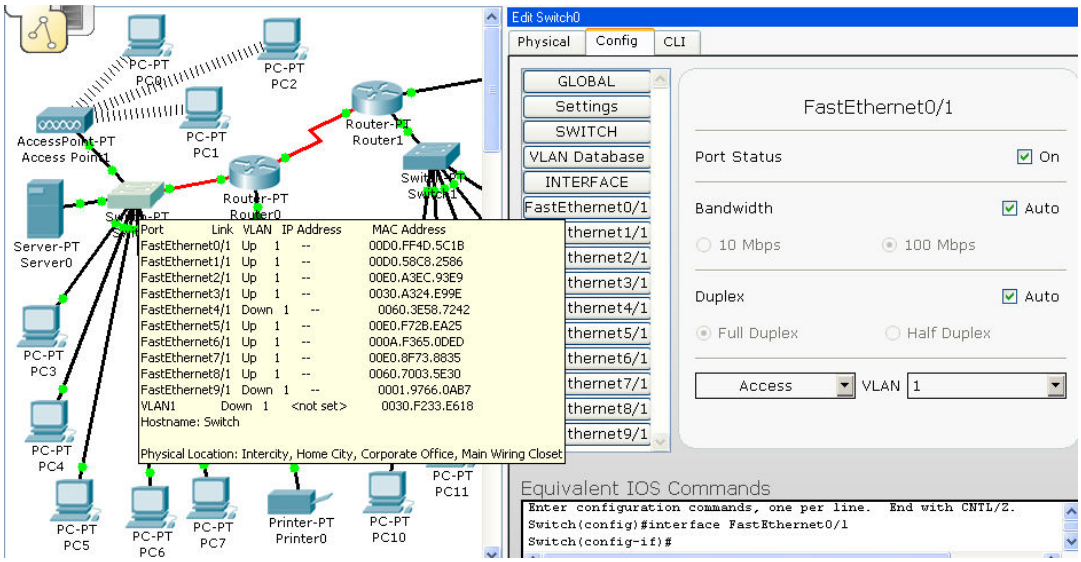


Figura 7.14. Verificación Switchs

Desarrollo

1. Para comprobar su funcionamiento colocamos un paquete simple señalando el lugar de origen y destino para la transferencia de información, en el escenario 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 7.15.

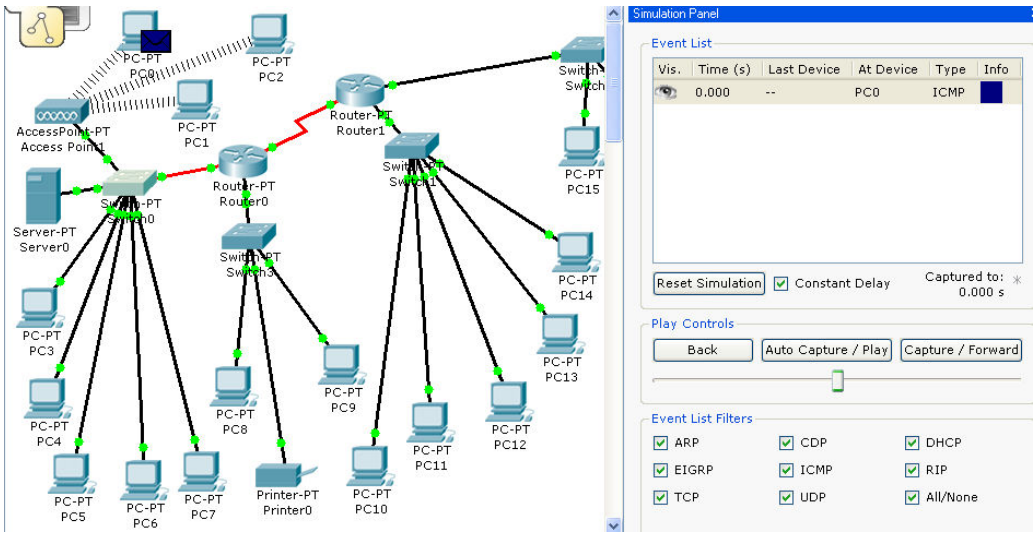


Figura 7.15. Colocación de paquete

2. En la figura 7.16. Se puede observar claramente que el paquete se ha trasladado de la PC0 al Access Point de la red comprobando de esta manera que la conexión correspondiente esta funcionando.

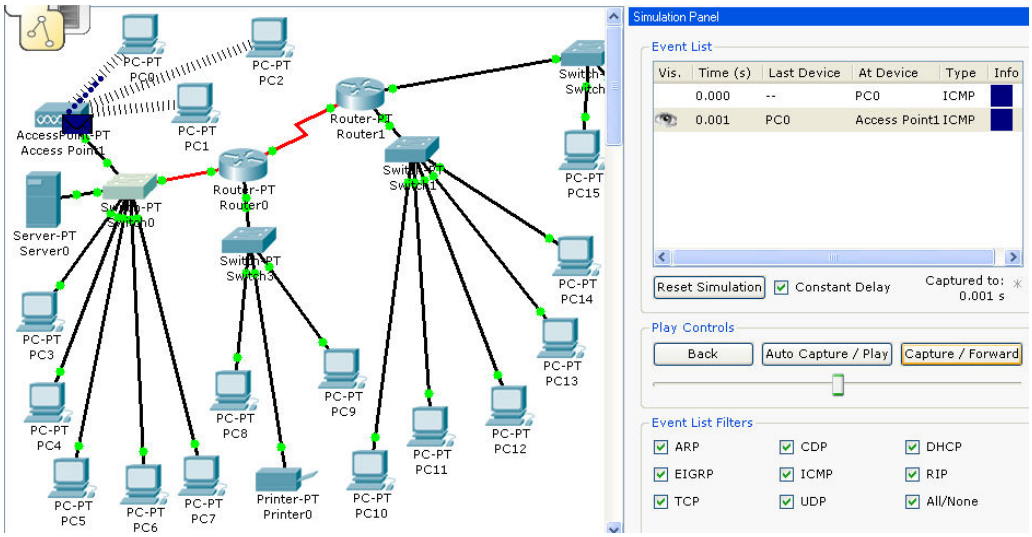


Figura 7.16. Simulación 1

3. En la figura 7.17. Se puede observar claramente que el paquete se ha trasladado del Access Point al Switch comprobando de esta manera que la conexión correspondiente se encuentra funcionando correctamente. Pero al mismo tiempo se puede observar en esta grafica que los paquetes enviados hacia la PC0, PC1 y PC2 son eliminados inmediatamente.

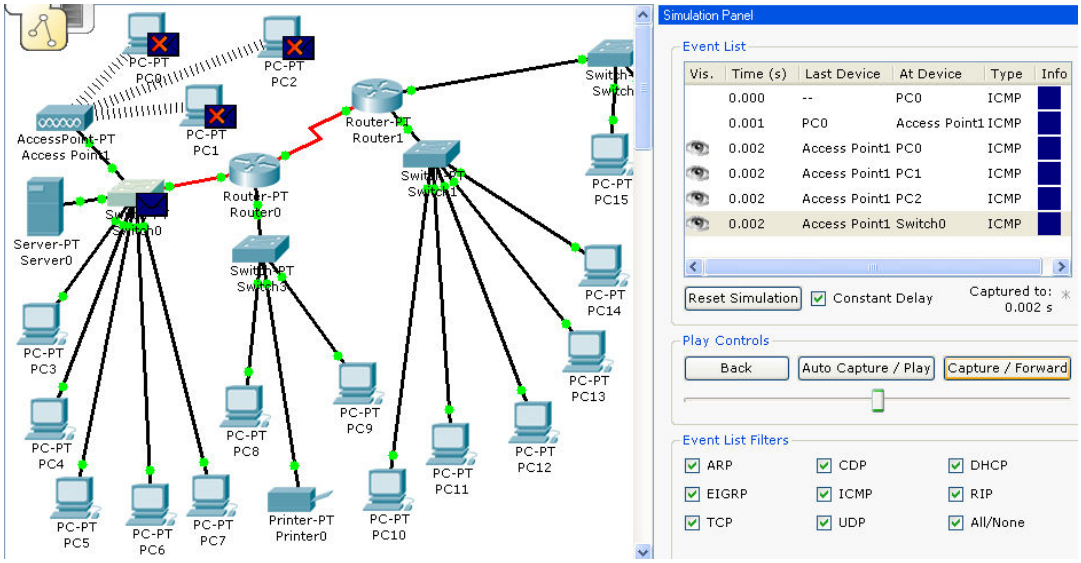


Figura 7.17. Simulación 2

4. Se debe continuar con la simulación correspondiente como se ha indicado en prácticas anteriores hasta que finalmente el paquete regrese a la PC0 (origen), confirmando de esta manera que la transferencia de datos es valida en la red, como se puede observar en la figura 7.18. Al mismo tiempo se observa en la grafica que los paquetes enviados a la PC1 y PC2 son descartados debido a que ese no es su destino.

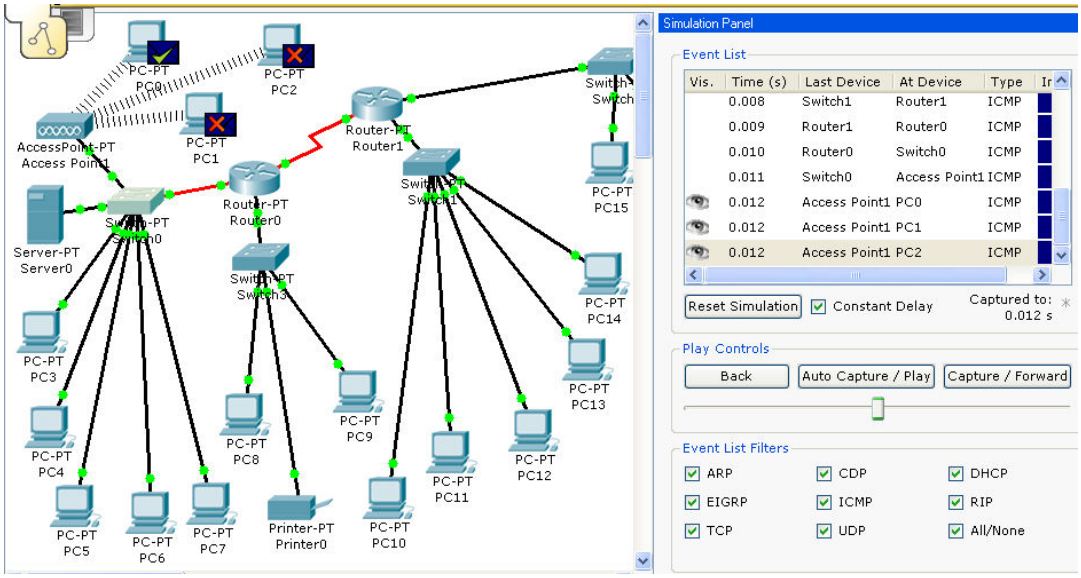


Figura 7.18. Simulación 3

Análisis de resultados

1. En la figura 7.7. se realiza las subdivisiones de las subredes de la clase tipo B, la cual usamos para configurar las distintas PC´s como se puede observar en la figura 7.8. y para cada switch usaremos una subred distinta.

2. En la figura 7.18 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.

3. En nuestro caso se debe conectar con cable serial V.35 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.

Conclusiones

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

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

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

7.8. PRUEBAS DE OPCIÓN MÚLTIPLE

El banco de preguntas correspondiente al capitulo se encuentra en anexos.

Para realizar las pruebas de selección múltiple correspondientes a este capítulo se debe correr el programa que se encuentra en el siguiente vinculo index.html o en http://www.fie-espe.edu.ec/preguntas, y luego procedemos a ingresar los datos del alumno que va a realizar la prueba como se muestra en la figura 7.19

Figura 7.19. Datos Alumno

Para ingresar a resolver la prueba debemos elegir el capítulo que se va a realizar como se muestra en la figura 7.20 o se debe ingresar a la plantilla de preguntas e elegir igualmente el capítulo deseado.

Figura 7.20. Prueba Capitulo 7

El siguiente paso es realizar la prueba de selección múltiple como se indica en la figura 7.21. Luego de haber respondido a todas las preguntas se procede hacer clic sobre Corregir Prueba para que la prueba sea calificada y corregida automáticamente como se muestra en la figura 7.22.

Figura 7.21. Prueba selección múltiple

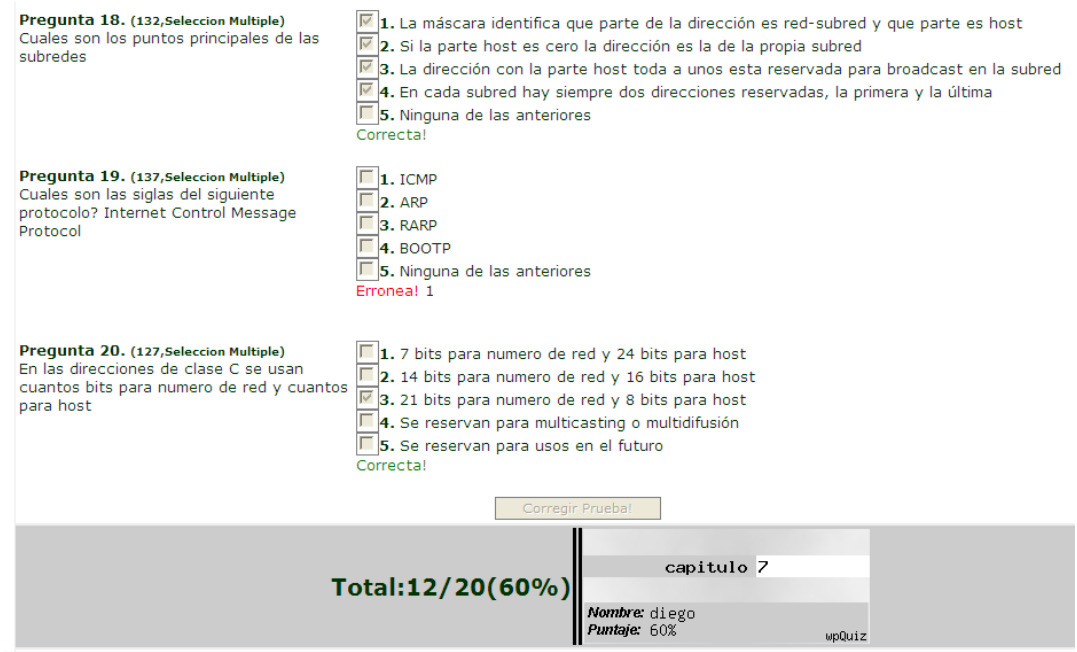


Figura 7.22. Calificación Prueba

CONCLUSIONES Y RECOMENDACIONES

- El Simulador Packet Tracer 4.0, es una herramienta muy útil para el laboratorio de Fundamentos de Redes, porque permite implementar y observar claramente el funcionamiento de las redes sin la necesidad de conectarlas físicamente, y las ventajas que presenta son muy útiles para utilizarlas en la actualidad a nivel mundial.
- El software Packet Tracer, se lo utilizo por la necesidad de tener una herramienta que, a través de las prácticas permita obtener resultados confiables sin tener la necesidad de armar toda la red físicamente.
- Los simuladores constituyen una gran ayuda para determinar la efectividad de un sistema a ser analizado, mediante las prácticas en donde se puede observar la eficiencia de la red, logrando comprobar así las ventajas, por lo que resulta ser muy viable su respectiva implementación.
- El software packet tracer es una herramienta muy útil para observar el comportamiento que tendría en la práctica y su funcionamiento al realizar la conexión de las redes de computadoras.
- Las gráficas en las prácticas, dan una clara muestra de lo necesario que es utilizar un simulador antes de crear toda la red física sin haber hecho los respectivos análisis.
- Como estudiantes del Departamento de Eléctrica y Electrónica nos vemos en la necesidad de conseguir todos los componentes físicos de una red, la que necesitamos armar y probar lo cual se vuelve sumamente complicado, por esta razón es sumamente favorable el uso de este software.
- La implementación de este proyecto en la ESPE no tiene costo debido a que se utilizo un software libre para la creación de la prueba de selección múltiple y además ya se encuentra instalada y lista para usarse en el servidor de la ESPE, y el packet tracer utilizado es un software libre de cisco system.
- Es recomendable que los alumnos se familiaricen con programas de este tipo para realizar sus simulaciones y comprobar resultados antes de crear físicamente una red.

- Es recomendable que se sigan elaborando tesis para el Departamento de Eléctrica y Electrónica, de esta forma los alumnos que ya terminamos nuestros estudios dejamos un aporte para nuestros compañeros que continúan en esta carrera.
- La prueba de selección múltiple aquí creada se la puede implementar fácilmente para varias materias del departamento de eléctrica y electrónica en un futuro muy cercano.

ANEXOS

ANEXOS

Anexo 1 Banco de Preguntas Capítulo I

Anexo 2 Banco de Preguntas Capítulo II

Anexo 3 Banco de Preguntas Capítulo III

Anexo 4 Banco de Preguntas Capítulo IV

Anexo 5 Banco de Preguntas Capítulo V

Anexo 6 Banco de Preguntas Capítulo VI

Anexo 7 Banco de Preguntas Capítulo VII

Anexo 1: Banco de Preguntas Capítulo I

1. La real academia española define el término interfaz como?
    a. **Palabra en ingles interface.**
    b. Paginas Web.
    c. Aplicaciones informáticas.

2. Interfaz se utiliza para describir multitud de entornos de comunicación entre sistemas:
    a. **Físicos.**
    b. **Eléctricos, electrónicos.**
    c. **Lógicos.**

3. Que procedimiento permiten relacionarse a dos capas diferentes de la arquitectura TCP/IP?
    a. Web.
    b. Medios físicos.
    c. **Interfaz.**

4. Cuando unos de los sistemas que se comunican es un ser humano cual es el concepto de interfaz?
    a. Interfaz Web.
    b. **Interfaz usuario.**
    c. Interfaz grafica.
    d. Interfaz MsDos.

5. Que tipos de interfaces deben servir como intermediarios entre usuarios genéricos y genios de sistemas?
    a. Interfaz grafica.
    b. Interfaz MsDos.
    c. **Interfaz Web.**
    d. Interfaz usuario.

6. Para posibilitar la información deseada se debe utilizar la interfaz?
    a. **Web.**
    b. Usuario.
    c. MsDos.
    d. Gráfica.

7. En que tipos de estándares se convirtieron las paginas Web?
    a. Normales.
    b. **Facto.**
    c. Artificiales.

Anexo 2: Banco de Preguntas Capítulo II

1. La definición más elemental de redes de datos es?
    a. La comunicación de varias computadoras.
    b. La interconexión de dos computadoras.
    c. Compartir recursos.

2. Cual es el objetivo principal de una red de datos?
    a. Compartir recursos.
    b. Conectar equipos.
    c. Compartir información.

3. Que es una red de comunicación?
    a. Esquema lógico.
    b. Es un esquema de conexión física y lógica.
    c. Conexión física.

4. Las redes de comunicación pueden:
    a. Compartir recursos de hardware y software.
    b. Procesar información común.
    c. Ejecutar programas multiusuario.
    d. Todas las anteriores.

5. Las clasificaciones más importantes de las redes son:
    a. Por el tipo de procesamiento.
    b. Por el cubrimiento.
    c. Por la topología.
    d. Todas las anteriores.

6. Las redes se clasifican en sistemas de procesamiento
    a. Central.
    b. Distribuido.

7. Las redes se clasifican según su cubrimiento en:
    a. LAN.
    b. WAN.
    c. MAN.

8. Las siglas LAN significan:
    a. Redes de área metropolitana.
    b. Redes de área extensa.
    c. Redes de área local.

9. Hoy en día a que se les denomina redes WAN
    a. Redes LAN.
    b. **Redes MAN.**
    c. Ninguna de las anteriores.

10. Las redes se clasifican según su topología en:
    a. Estrella.
    b. Bus.
    c. Anillo.
    d. Todas las anteriores.

11. En que tipo de topología se utiliza el algoritmo carrier sense multiple access collison detect (CSMA/CD)
    a. Estrella.
    b. Bus.
    c. Anillo.

12. En las redes Ethernet 10BaseT, significa:
    a. 10Mbps, en banda base, por par trenzado y hasta 100 metros.
    b. 100Mbps, en banda base, por coaxial y hasta 200 metros.
    c. 10Mbps, en banda base, por coaxial y hasta 100 metros.
    d. 100Mbps, en banda base, por par trenzado y hasta 10 metros.

13. En las redes Ethernet 10Base2, significa:
    a. 10Mbps, en banda base, por par trenzado y hasta 100 metros.
    b. 100Mbps, en banda base, por coaxial y hasta 200 metros.
    c. 10Mbps, en banda base, por coaxial y hasta 200 metros.
    d. 100Mbps, en banda base, por par trenzado y hasta 10 metros.

14. Token Ring es un protocolo de nivel 2 creado por IBM y normalizado por la IEEE como:
    a. 802.11.
    b. 802.2.
    c. 802.5.
    d. 802.11a.

15. Qué tipos de conexiones existen?
    a. Mainframe.
    b. Punto a punto.
    c. Cliente servidor.
    d. Todas las anteriores.

16. Cuáles son las ventajas de una red punto a punto?
    a. Menos cara de implementar.
    b. No requiere software especializado adicional para la administración.
    c. No requiere un administrador de red dedicado.
    d. Todas las anteriores.

17. Cuáles son las desventajas de una Red Punto a Punto?
    a. Todas las máquinas comparten recursos negativamente afectando el desempeño.
    b. Cada usuario no debe ser entrenado para ejecutar tareas administrativas.
    c. Menos segura.

18. Cuáles son las ventajas de una Red Cliente - Servidor
    a. Provee mayor seguridad.
    b. Fácil de administrar cuando la red es grande porque la administración es centralizada.
    c. Todos los datos pueden ser almacenados en una localización central.
    d. Todas las anteriores.

19. Cuáles son las desventajas de una Red Cliente – Servidor?
    a. Requiere software caro y especializado para la administración y operación de la red.
    b. Requiere máquinas servidores más potentes y caras.
    c. Tiene un solo punto de falla. Los datos de usuario no son disponibles si el servidor esta fuera de servicio (Caído).

20. En qué tipos de compañías se utilizan conexiones tipo mainframe?
    a. Bancarias.
    b. De oficina pequeña.
    c. Supermercados o locales comerciales.
    d. Ninguna de las anteriores.

21. Cuáles son las ventajas de una red de datos?
    a. Compartir recursos.
    b. Aumento de la confiabilidad.
    c. Escalabilidad.

Anexo 3: Banco de Preguntas Capítulo III

1. Qué clases de repetidores multipuerto existen?
    a. Pasivo.
    b. Activo.
    c. **Inteligente.**

2. Un concentrador en el modelo OSI opera a nivel de la capa?
    a. Transporte.
    b. Física.
    c. Enlace.
    d. Red.
    e. Sección.

3. La disponibilidad de switches Ethernet de bajo precio y su funcionamiento similar han dejado obsoletos a los?
    a. Router.
    b. **Concentradores.**
    c. Gateway.
    d. Bridge.

4. A un concentrador se le conoce también como?
    a. Switch.
    b. Hub.
    c. Bridge.
    d. Router.
    e. Gateway.

5. Los concentradores son la base para las redes de topología tipo
    a. Estrella.
    b. Punto a punto.
    c. Bus.
    d. Ninguna de las anteriores.

6. Un concentrador envía la información a todos los ordenadores?
    a. Si.
    b. No.
    c. En algunos casos.

7. Qué sucede cuando dos ordenadores envían información al mismo tiempo?
    a. Colisión.
    b. Perdida de paquetes.
    c. Nada.

8. A qué velocidad funciona un concentrador?
    a. A una velocidad fija.
    b. A la velocidad del dispositivo mas lento de la red.
    c. A la velocidad del dispositivo mas rápido de la red.

9. Qué características tiene un concentrador que es un dispositivo simple?
    a. No añade retardos a los mensajes.
    b. Su precio es barato.
    c. No eran muy comunes.
    d. Se siguen usando.

10. Qué es lo mas importante que permite una tarjeta de red?
    a. Tarjeta de expansión.
    b. Conectarse a 5Mbps.
    c. **Compartir recursos entre dos o mas equipos.**

11. Cuáles son las diferentes tarjetas de Ethernet que se diferencian por su velocidad de transmisión?
    a. 10Mbps.
    b. 10 Gigabit.
    c. **1000Mbps.**

12. Qué tipos de tarjetas inalámbricas existen?
    a. 8802.11ª.
    b. 8802.11b.
    c. **8802.11g.**

13. Qué tipos de cables de transmisión existen?
    a. **Cable recto.**
    b. **Cable coaxial.**
    c. **Cable UTP.**
    d. **Fibra óptica.**
    e. **Cable STP.**

14. Los cables UTP, STP y FTP a que categoría pertenecen?
    a. Categoría 4.
    b. **Categoría 5.**
    c. Categoría 6.
    d. Categoría 6e.
    e. Categoría 7.

15. Un cable UTP categoría 2 empleado para la transmisión de voz y datos cuantos Mbps transmite?
    a. 10Mbps.
    b. 8Mbps.
    c. 6Mbps.
    d. **4Mbps.**
    e. 2Mbps.

16. Un cable UTP categoría 5 puede soportar comunicación de hasta?
    a. 20Mbps.
    b. 50Mbps.
    c. 80Mbps.
    d. **100Mbps.**
    e. 150Mbps.

17. Porqué es importante el ancho de banda?
    a. **El ancho de banda está limitado por la física y la tecnología.**
    b. **El ancho de banda no es gratis.**
    c. **Los requisitos de ancho de banda están creciendo a un ritmo muy rápido.**
    d. **El ancho de banda es fundamental para el rendimiento de la red.**
    e. Ninguna de las anteriores.

18. El ancho de banda es fundamental para el rendimiento de la red?
    a. Switch.
    b. Router.
    c. Módem.
    d. Hub.
    e. **Ninguna de las anteriores.**

19. En qué tipos se dividen los distintos entornos de comunicación para el envío de datos?
    a. **Asíncrona.**
    b. **Sincrona.**
    c. Ninguna de las anteriores.

20. El software packet tracer que elementos contiene para su simulación?
    a. **Dispositivos.**
    b. **Conexiones.**
    c. **Condiciones de enlace.**
    d. **Protocolos de enrutamiento.**
    e. **Encapsulamiento OSI.**

21. El software packet tracer puede realiza visualización, simulación y animación
    a. **Creando/conectando dispositivos.**
    b. **Removiendo dispositivos/conexiones.**
    c. **Creando descripción de redes.**
    d. **Locking/unlocking la caja de información.**
    e. Ninguna de las anteriores.

Anexo 4: Banco de Preguntas Capítulo IV

1. Qué protocolo se refiere a glosario, gestión de red e Internet working. Relación de estándares, gestión de red, interconexión de redes?
    a. **802.1.**
    b. 802.2.
    c. 802.3.
    d. 802.4.
    e. 802.5.

2. Qué protocolo es CSMA/CD. Método de acceso y nivel físico. Ethernet?
    a. 802.1.
    b. 802.2.
    c. **802.3.**
    d. 802.4.
    e. 802.5.

3. Qué protocolo es Token Bus. Método de acceso y nivel físico. Bus con paso de testigo?
    a. 802.1.
    b. 802.2.
    c. 802.3.
    d. **802.4.**
    e. 802.5.

4. Qué protocolo es Token Ring. Método de acceso y nivel físico. Anillo con paso de testigo?
    a. 802.1.
    b. 802.2.
    c. 802.3.
    d. 802.4.
    e. **802.5.**

5. Qué protocolo son las redes de área metropolitana (MAN)?
    a. 802.1.
    b. 802.2.
    c. 802.5.
    d. 802.4.
    e. **802.6.**

6. Qué protocolo son las wireless LAN (Redes Inalámbricas). Método de acceso y nivel físico?
    a. 802.10.
    b. **802.11.**
    c. 802.13.
    d. 802.12.
    e. 802.9.

7. CSMA/CD, siglas que corresponden a Carrier Sense múltiple Access with Collision Detection es el protocolo N.-
    a. 802.1.
    b. 802.2.
    c. **802.3.**
    d. 802.4.
    e. 802.5.

8. Las topologías más usuales en Ethernet 802.3 son:
    a. 1Base−5.
    b. **10Base−5.**
    c. **10Base−2.**
    d. **10Base−T.**

9. Los protocolos de Acceso al Medio (MAC) pueden ser:
    a. Una red es un entorno en el que diferentes host y dispositivos comparten un medio de transmisión común.
    b. Es necesario por ello establecer técnicas que permitan definir qué host está autorizado para transmitir por el medio común en cada momento.
    c. **Determinísticos.**
    d. **No determinísticos.**
    e. Ninguna de las anteriores.

10. El esquema centralizado tiene ventajas, cuales son:
    a. **Puede proporcionar prioridades, rechazos y capacidad garantizada.**
    b. **La lógica de acceso es sencilla.**
    c. **Resuelve conflictos entre estaciones de igual prioridad.**
    d. Ninguna de las anteriores.

11. Las técnicas de control de acceso al medio asíncronas se subdividen en categorías, cuales son?
    a. **Rotación circular.**
    b. **Reserva.**
    c. **Competición.**
    d. Ninguna de las anteriores.

12. Las redes Ethernet pueden utilizar diferentes tipos de cableado, cada uno con sus beneficios y problemas. Cuales son los tres cableados más comunes?
    a. **Tinte.**
    b. **Thicknet.**
    c. **Twisted pair.**
    d. Fibra óptica.
    e. Coaxial.

13. El cable Twisted Pair o cable par trenzado es:
    a. 10base2.
    b. 10base5.
    c. **10baseT.**
    d. 10baseF.

14. Las Redes WLAN 802.11 se dividen en:
    a. **802.11a.**
    b. **802.11.**
    c. **802.11g.**
    d. **802.11b.**
    e. Ninguna de las anteriores.

15. El protocolo CSMA se divide en técnicas diferentes de detección cuales son?
    a. **CA - Collision Avoidance, en castellano Prevención de Colisión.**
    b. **CD - Collision Detection, Detección de Colisión.**

16. Collision Avoidance (CA) realiza un proceso en las que el emisor realiza los siguientes pasos.
    a. Nada.
    b. **Escucha para ver si la red está libre.**
    c. **Transmite el dato.**
    d. **Espera un reconocimiento por parte del receptor.**

17. Qué significa el hueco entre tramas?
    a. **Un período de tiempo en que no se transmite nada.**
    b. **Tiene una longitud equivalente a 12 bytes (96 ns a 10 Mb/s).**
    c. **Sirve para separar las tramas.**
    d. **Detecta cuando termina la trama anterior.**
    e. Ninguna de las anteriores.

18. Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados como son:
    a. **Hub.**
    b. **Bridges.**
    c. **Switch.**
    d. **Estaciones de trabajo.**
    e. Concentradores.

19. Cuáles son las ventajas de conectar una VLAN por puertos?
    a. **Facilidad de movimientos y cambios.**
    b. **Microsegmentación y reducción del dominio de Broadcast.**
    c. **Multiprotocolo.**
    d. Administración.
    e. Ninguna de las anteriores.

20. Cuáles son las ventajas de conectar un VLAN por dirección MAC?
    a. **Facilidad de movimientos.**
    b. Problemas de rendimiento y control de Broadcast.
    c. **Se pueden tener miembros en múltiples VLANs.**
    d. Complejidad en la administración.
    e. **Multiprotocolo.**

21. Qué ventajas tiene conectar una VLAN por protocolos?
    a. Problemas de rendimiento y control de Broadcast.
    b. **Asignación dinámica.**
    c. No soporta protocolos de nivel 2 ni dinámicos.
    d. **Segmentación por protocolo**.

Anexo 5: Banco de Preguntas Capítulo V

1. Entre las capas del modelo OSI se encuentran:
    a. Aplicación.
    b. Presentación.
    c. Sección.
    d. Transporte.
    e. Red.

2. Qué capas del modelo OSI no se encuentran en el modelo TCP/IP?
    a. Presentación.
    b. Sección.
    c. Aplicación.
    d. Transporte.

3. En la capa de aplicación se incluyen protocolos destinados a proporcionar servicios, tales como:
    a. Correo electrónico (SMTP).
    b. Transferencia de ficheros (FTP).
    c. Conexión remota (TELNET).
    d. **Protocolo HTTP (*Hypertext Transfer Protocol*)**.

4. Cuáles son los niveles de la arquitectura TCP/IP?
    a. Nivel de aplicación.
    b. Nivel de transporte.
    c. Nivel de Internet.
    d. Nivel de red.
    e. Nivel físico.

5. De los siguientes protocolos cuales perteneces a TCP/IP?
    a. **FTP (File Transfer Protocol).**
    b. **SMTP (Simple Mail Transfer Protocol).**
    c. **SNMP (Simple Network Management Protocol).**
    d. **NFS (Network File System).**
    e. **TELNET.**

6. Los protocolos de Internet se modelan en cuales capas de las siguientes:
    a. **Aplicación.**
    b. **Transporte.**
    c. **Internetwork.**
    d. **Network Interface.**
    e. Ninguna de las anteriores.

7. Qué es una interface?
    a. **Es un conjunto de reglas, primitivas y operaciones de intercambio de información entre niveles adyacentes dentro del mismo host.**
    b. **Define los servicios que ofrece la capa inferior a la superior.**
    c. **Es el punto entre dos capas adyacentes.**
    d. Ninguna de las anteriores.

8. Para que exista comunicación entre las capas se debe proceder con cuales de las siguientes sugerencias:
    a. **Unidad de Datos de Interfaz (IDU).**
    b. **Unidad de datos del servicio (SDU).**
    c. **Unidad de datos del protocolo (PDU).**
    d. Ninguna de las anteriores.

9. Un servicio Orientado a la conexión qué fases posee:
    a. Confiable.
    b. **Conexión.**
    c. Corrección de errores.
    d. **Desconexión.**
    e. **Transferencia.**

10. Características de un servicio orientado a la conexión
    a. **Puede establecer conexiones permanentes o temporales.**
    b. **Los mensajes poseen secuencia y siempre llegan en orden.**
    c. **Servicio Confiable.**
    d. **Garantía de entrega.**
    e. **Corrección de errores.**

11. Un servicio No Orientado a la conexión que fases posee:
    a. Confiable.
    b. Conexión.
    c. Corrección de errores.
    d. Desconexión.
    e. **Transferencia.**

12. Características de un servicio orientado a la conexión
    a. **No hay garantía de entrega.**
    b. **Se conoce como servicios DATAGRAMA.**
    c. **No hay corrección de errores.**
    d. Servicio Confiable.
    e. Garantía de entrega.

13. Algunos ejemplos de primitivas de servicio son:
    a. **CONNECT.response.**
    b. **CONNECT.confirm.**
    c. **DATA.request.**
    d. **DATA.indication.**
    e. **DISCONNECT.request.**

14. El modelo de referencia OSI tiene 3 niveles orientados a la aplicación cuales son:
    a. El nivel de red.
    b. Enlace.
    c. Aplicación.
    d. Presentación.
    e. Sesión.

15. El modelo de referencia OSI tiene niveles orientados a redes cuales son:
    a. **El nivel de red.**
    b. **Enlace.**
    c. **Físico.**
    d. **Aplicación.**
    e. **Sesión.**

16. Los niveles del modelo TCP/IP son:
    a. **Aplicación.**
    b. Sección.
    c. **Transporte.**
    d. **Interconexión.**
    e. **Orientados a red.**

17. En el modelo OSI son fundamentales tres conceptos cuales son:
    a. **Servicios.**
    b. **Interfaces.**
    c. **Protocolos.**
    d. Transporte.
    e. Aplicación.

18. Cuáles son las diferencias entre los dos modelos TCP/IP y OSI?
    a. **En el área de la comunicación sin conexión frente a la orientada a la conexión.**
    b. **La cantidad de capas.**
    c. No hubo el problema de ajustar los protocolos.
    d. Ninguna de las anteriores.

19. Cuáles son las criticas fundamentales del modelo OSI?
    a. Mala temporización.
    b. Mala tecnología.
    c. Mala implementación.
    d. Mala política.
    e. Faltan conceptos.

20. Cuáles son las criticas fundamentales del modelo TCP/IP?
    a. Mala temporización.
    b. Mala tecnología.
    c. Faltan conceptos.
    d. No define capas 1 y 2.
    e. **Muchos protocolos de aficionados.**

21. Cuáles son los puntos fundamentales de la estandarización?
    a. Estándares de hecho (de facto).
    b. Estándares por ley (de jure).
    c. Estandarización de telecomunicaciones.
    d. Sectores.
    e. Ninguna de las anteriores.

22. Cuáles son las *ventajas* de una estandarización?
    a. Los organismos de estandarización son muy lentos.
    b. Demasiados organismos de estandarización.
    c. Flexibilidad a la hora de instalar la red.
    d. **Estimula la competitividad.**
    e. Ninguna de las anteriores.

Anexo 6: Banco de Preguntas Capítulo VI

1. Un bridge para qué se lo utiliza?
    a. **Tiene la misma funcionalidad que un repetidor.**
    b. **Sirve para unir segmentos o grupos de trabajo LAN.**
    c. **Divide una red para aislar el tráfico o los problemas.**
    d. Ninguna de las anteriores.

2. Los bridges se pueden utilizar para:
    a. **Extender la longitud de un segmento.**
    b. **Proporcionar un incremento en el número de equipos de la red.**
    c. **Reducir los cuellos de botella del tráfico resultantes de un número excesivo de equipos conectados.**
    d. **Dividir una red sobrecargada en dos redes separadas, reduciendo la cantidad de tráfico en cada segmento y haciendo que la red sea más eficiente.**
    e. **Enlazar medios físicos diferentes como par trenzado y Ethernet coaxial.**

3. Un bridge de nivel MAC que funciones realiza?
    a. **Escucha todo el tráfico.**
    b. **Comprueba las direcciones origen y destino de cada paquete.**
    c. **Construye una tabla de encaminamiento, donde la información está disponible.**
    d. **Reenvían paquetes.**
    e. Ninguna de las anteriores.

4. Para qué se utiliza la creación de la tabla de encaminamiento?
    a. **La dirección de origen se compara con la tabla de encaminamiento. Si no aparece la dirección de origen, se añade a la tabla.**
    b. **El bridge compara la dirección de destino con la base de datos de la tabla de encaminamiento.**
    c. **Si la dirección de destino está en la tabla de encaminamiento y aparece en el mismo segmento de la dirección de origen, se descarta el paquete.**
    d. **Si la dirección de destino está en la tabla de encaminamiento y no aparece en el mismo segmento de la dirección de origen, el bridge envía el paquete al puerto apropiado que permite alcanzar la dirección de destino.**
    e. **Si la dirección de destino no está en la tabla de encaminamiento, el bridge envía el paquete a todos sus puertos, excepto al puerto desde donde se originó el envío.**

5. A qué se le conoce como segmentación del tráfico de red?
    a. **Cuando los Bridges los utilizar las tablas de encaminamiento para reducir el tráfico de la red.**
    b. **Controlando los paquetes que se envían al resto de los segmentos.**
    c. La dirección de origen se compara con la tabla de encaminamiento. Si no aparece la dirección de origen, se añade a la tabla.
    d. El bridge compara la dirección de destino con la base de datos de la tabla de encaminamiento.
    e. Ninguna de las anteriores.

6. Cuáles son las ventajas de utilizar un bridges en lugar de los repetidores?
    a. **Ofrecen mejor rendimiento de red.**
    b. **Un número menor de equipos compiten en cada segmento por los recursos disponibles.**
    c. **Se pueden utilizar múltiples bridge para combinar diferentes redes pequeñas en una red más grande.**
    d. **Se tiene menos colisiones y operaría de forma mucho más eficiente.**
    e. ninguna de las anteriores.

7. Su popularidad en grandes redes se debe a que?
    a. **Son sencillos de instalar y transparentes a los usuarios.**
    b. **Son relativamente baratos.**
    c. **Son flexibles y adaptables.**
    d. Son relativamente caros.
    e. Ninguna de las anteriores.

8. Un Switch que es un dispositivo de Networking esta situado en qué capa del modelo de referencia OSI?
    a. 1.
    b. **2.**
    c. 3.
    d. 4.
    e. 5.

9. La capa 2 del modelo OSI es la capa de Enlace de datos, esta capa proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico) que son:
    a. **La topología de red.**
    b. **El acceso a la red.**
    c. **La notificación de errores.**
    d. **Entrega ordenada de tramas.**
    e. **Control de flujo.**

10. Cuáles son las diferencias entre el hub y el switch?
    a. **Los switches toman decisiones basándose en las direcciones MAC.**
    b. **Los hubs no toman ninguna decisión.**
    c. **Los switches hacen que la LAN sea mucho más eficiente.**
    d. **El hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar todos los datos.**
    e. Ninguna de las anteriores.

11. El router es un dispositivo que?
    a. **Se utiliza en una red de alta complejidad.**
    b. **Conoce las direcciones de cada segmento.**
    c. **Es capaz de determinar el camino más rápido para el envío de datos.**
    d. **Facilita con el filtrado del tráfico de difusión en el segmento local.**
    e. Ninguna de las anteriores.

12. Los routers pueden proporcionar las siguientes funciones de un bridge
    a. Pueden conmutar y encaminar paquetes.
    b. **Filtrado y aislamiento del tráfico.**
    c. Trabajan a un nivel superior del modelo OSI.
    d. **Conexión de segmentos de red.**
    e. Ninguna de las anteriores.

13. Cómo funcionan los routers?
    a. **Mantienen sus propias tablas de encaminamiento.**
    b. **Tablas constituidas por direcciones de red.**
    c. **Incluir las direcciones de los host.**
    d. **Determinar la dirección de destino de los datos de llegada.**
    e. Ninguna de las anteriores.

14. Las tablas de encaminamiento de los router incluyen?
    a. **Todas las direcciones de red conocidas.**
    b. **Instrucciones para la conexión con otras redes.**
    c. **Los posibles caminos entre los routers.**
    d. **El costo de enviar los datos a través de estos caminos.**
    e. Ninguna de las anteriores.

15. Por qué en algunas ocasiones un router constituye una ventaja?
    a. **Segmentar grandes redes en otras más pequeñas.**
    b. Incluir las direcciones de los host.
    c. Actuar como barrera de seguridad entre los diferentes segmentos.
    d. Prohibir las tormentas de difusión, puestos que no se envían estos mensajes de difusión.
    e. Ninguna de las anteriores.

16. Algunos protocolos que permiten encaminar son?
    a. **DECnet.**
    b. **Protocolo de Internet (IP).**
    c. **Intercambio de paquetes entre redes (IPX).**
    d. NetBEUI (Interfaz de usuario extendida NetBIOS).
    e. **OSI.**

17. Algunos protocolos que no permiten encaminar son?
    a. **Protocolo de transporte de área local (LAT), un protocolo de Digital Equipment Corporation.**
    b. Protocolo de Internet (IP).
    c. Intercambio de paquetes entre redes (IPX).
    d. **NetBEUI (Interfaz de usuario extendida NetBIOS).**
    e. OSI.

18. De los siguientes nombres cuales son algoritmos de encaminamiento?
    a. **OSPF.**
    b. **RIP**.
    c. **NLSP**.
    d. OSI.
    e. P2P.

19. Cuáles son las características de un router estático?
    a. **Instalación y configuración manual de todos los routers.**
    b. **Utilizan siempre la misma ruta, determinada a partir de una entrada en la tabla de encaminamiento.**
    c. **Utilizan una ruta codificada (designada para manejar sólo una situación específica), no necesariamente la ruta más corta.**
    d. **Se consideran más seguros puesto que los administradores especifican cada ruta.**
    e. Ninguna de las anteriores.

20. Cuáles son las características de un router dinámico?
    a. **Configuración manual del primer router. Detectan automáticamente redes y routers adicionales.**
    b. **Pueden seleccionar una ruta en función de factores tales como costo y cantidad del tráfico de enlace.**
    c. **Pueden decidir enviar paquetes sobre rutas alternativas.**
    d. **Pueden mejorar la seguridad configurando manualmente el router para filtrar direcciones específicas de red y evitar el tráfico a través estas direcciones.**
    e. Ninguna de las anteriores.

21. Los b-routers pueden?
    a. **Encaminar protocolos encaminables seleccionados.**
    b. **Actuar de bridge entre protocolos no encaminables.**
    c. **Proporcionar un mejor coste y gestión de interconexión que el que proporcionan los bridges y routers por separado.**
    d. Ninguna de las anteriores.

22. En pocas palabras un gateway enlaza dos sistemas que no utilizan los mismos?
    a. **Protocolos de comunicaciones.**
    b. **Estructuras de formateo de datos.**
    c. **Lenguajes.**
    d. **Arquitectura.**
    e. Ninguna de las anteriores.

23. El Gateway para procesar los datos deba seguir unos pasos cuales son?
    a. **Desactiva los datos de llegada a través de la pila del protocolo de la red.**
    b. **Encapsula los datos de salida en la pila del protocolo de otra red para permitir su transmisión.**
    c. Ninguna de las anteriores.

Anexo 7: Banco de Preguntas Capitulo VII

1. Cuáles de los siguientes nombres se encuentran en un datagrama de IPv4?
    a. **Versión.**
    b. **Longitud Cabecera.**
    c. **DS (Differentiated Services).**
    d. **Longitud total.**
    e. **Campos de Fragmentación.**

2. Cuáles de los siguientes nombres a continuación son mejoras de IPv6 sobre IPv4?
    a. **Direcciones.**
    b. **Eficiencia.**
    c. **Seguridad.**
    d. **Multicast.**
    e. **Sencillez.**

3. Cuáles son los fines de utilizar IPv6?
    a. **Autoconfiguración y movilidad.**
    b. **Opciones encadenadas.**
    c. **Reducir el tamaño de las tablas de ruteo.**
    d. **Simplificar el protocolo.**
    e. **Usar tipos distintos de servicio.**

4. Cuáles son las direcciones necesarias para alcanzar una maquina remota?
    a. Dirección de red.
    b. **Dirección para identificar la *aplicación.***
    c. **Dirección de *Internet.***
    d. Dirección de transporte.
    e. **Dirección *física* o hardware.**

5. Una dirección IP esta subdividido en?
    a. **Numero de red.**
    b. Multi homed.
    c. DNS (Domain Name System).
    d. **Numero de interfaz de red.**
    e. Ninguna de las anteriores.

6. Las direcciones IP pueden ser?
    a. Normales.
    b. **Simbólicas.**
    c. **Numéricas.**
    d. Habituales.
    e. Ninguna de las anteriores.

7. En el término formal, utilizado en RFC 1166, como mas se le conoce al número de red?
    a. Dirección IP.
    b. Dirección física.
    c. **NetID.**
    d. **Dirección de red.**
    e. Ninguna de las anteriores.

8. Cuáles son las clases de direcciones IP que existen?
    a. **Clase A.**
    b. **Clase B.**
    c. **Clase C.**
    d. **Clase D.**
    e. **Clase E.**

9. En las direcciones de clase A se usan cuantos bits para numero de red y cuantos para host?
    a. **7 bits para numero de red y 24 bits para host.**
    b. 14 bits para numero de red y 16 bits para host.
    c. 21 bits para numero de red y 8 bits para host.
    d. Se reservan para multicasting o multidifusión.
    e. Se reservan para usos en el futuro.

10. En las direcciones de clase B se usan cuantos bits para numero de red y cuantos para host?
    a. 7 bits para numero de red y 24 bits para host.
    b. 14 bits para numero de red y 16 bits para host.
    c. 21 bits para numero de red y 8 bits para host.
    d. Se reservan para multicasting o multidifusión.
    e. Se reservan para usos en el futuro.

11. En las direcciones de clase C se usan cuantos bits para numero de red y cuantos para host?
    a. 7 bits para numero de red y 24 bits para host.
    b. 14 bits para numero de red y 16 bits para host.
    c. 21 bits para numero de red y 8 bits para host.
    d. Se reservan para multicasting o multidifusión.
    e. Se reservan para usos en el futuro.

12. En las direcciones de clase D se usan cuantos bits para numero de red y cuantos para host?
    a. 7 bits para numero de red y 24 bits para host.
    b. 14 bits para numero de red y 16 bits para host.
    c. 21 bits para numero de red y 8 bits para host.
    d. Se reservan para multicasting o multidifusión.
    e. Se reservan para usos en el futuro.

13. En las direcciones de clase E se usan cuantos bits para numero de red y cuantos para host?
    a. 7 bits para numero de red y 24 bits para host.
    b. 14 bits para numero de red y 16 bits para host.
    c. 21 bits para numero de red y 8 bits para host.
    d. Se reservan para multicasting o multidifusión.
    e. Se reservan para usos en el futuro.

14. Para qué nos sirve la mascara de red de una computadora al rato de enviar un paquete?
    a. Para saber si debe enviar los datos dentro de la red.
    b. Para saber si debe enviar los datos fuera de la red.
    c. Para indicar a los dispositivos qué parte de la IP es el número de la red.
    d. Para indicar a los dispositivos qué parte de la IP es correspondiente al host.
    e. Ninguna de las anteriores.

15. Cuál es su función de la mascara de red?
    a. Para saber si debe enviar los datos dentro de la red.
    b. Para saber si debe enviar los datos fuera de la red.
    c. Para indicar a los dispositivos qué parte de la IP es el número de la red.
    d. Para indicar a los dispositivos qué parte de la IP es correspondiente al host.
    e. Ninguna de las anteriores.

16. Cuáles son los puntos principales de las subredes?
    a. **La máscara identifica que parte de la dirección es red-subred y que parte es host.**
    b. **Si la parte host es cero la dirección es la de la propia subred.**
    c. **La dirección con la parte host toda a unos esta reservada para broadcast en la subred.**
    d. **En cada subred hay siempre dos direcciones reservadas, la primera y la última.**
    e. Ninguna de las anteriores.

17. Qué tipos de subnetting existen?
    a. Longitud fija.
    b. **Estático.**
    c. Diferencial.
    d. **Longitud variable.**
    e. Ninguna de las anteriores.

18. Una red se denomina *SUPERRED cuando la máscara de CIDR contiene?*
    a. Mas bits que la mascara original.
    b. Igual bits que la mascara original.
    c. **Menos bits a unos que la máscara por omisión de la red.**
    d. Menos bytes.
    e. Ninguna de las anteriores.

19. Algunos de los protocolos de control al nivel de red son?
    a. **ICMP.**
    b. **ARP.**
    c. **RARP.**
    d. **BOOTP.**
    e. Ninguna de las anteriores.

20. Cuáles son las siglas del siguiente protocolo? Address Resolution Protocol?
    a. ICMP.
    b. **ARP.**
    c. RARP.
    d. BOOTP.
    e. Ninguna de las anteriores.

21. Cuáles son las siglas del siguiente protocolo? Internet Control Message Protocol?
    a. **ICMP.**
    b. ARP.
    c. RARP.
    d. BOOTP.
    e. Ninguna de las anteriores.

REFERENCIAS BIBLIOGRÁFICAS

- http://www.gratisweb.com/alricoa/contenido.htm
- http://www.geocities.com/v.iniestra/apuntes/dipl_redes/70-058.html
- http://es.encarta.msn.com/encyclopedia_961520284_2/Redes_de_comunicación.html
- http://es.wikipedia.org
- http://www.arqhys.com/arquitectura/cables-tipos.html
- http://fmc.axarnet.es/redes/tema_07.htm
- www.netacad.uat.edu.mx
- http://standards.ieee.org/regauth/oui/oui.txt.
- http://mx.geocities.com/reco202eq1/Trabajo_3.htm
- http://fmc.axarnet.es/redes/tema_02.htm
- http://www.csi.map.es/csi/silice/Cablead6.html
- http://www.pchardware.org/redes/redes_ethernet.php
- http://pdf.rincondelvago.com/ethernet-e-802_3.html
- http://alumno.ucol.mx/al971848/public_html/IEEE.htm
- http://docente.ucol.mx/al970310/public_html/CSMA.htm
- http://www.tech-faq.com/lang/es/vlan.shtml
- http://www.textoscientificos.com/redes/redes-virtuales
- http://ditec.um.es/laso/docs/tut-tcpip/3376c21.html
- http://personales.upv.es/rmartin/TcpIp/cap02s14.html
- http://html.rincondelvago.com/redes_19.html
- http://usuarios.lycos.es/janjo/janjo1.html
- http://ditec.um.es/laso/docs/tut-tcpip/3376c21.html
- http://www.adslzone.net/adsl_router-faq.html
- http://carinalusso.iespana.es/Dispositivos%20de%20red.htm
- http://www.consulintel.es/html/Tutoriales/Articulos/tecn_conm.html
- http://www.entrebits.cl/foros/networking/3332-diferencias-entre-bridges-y-routers.html
- http://www.entrebits.cl/foros/networking/3331-routers.html
- http://ditec.um.es/laso/docs/tut-tcpip/3376c22.html#address
- http://halley.ls.fi.upm.es/~jyaguez/pdfs/LIbrosuperred.pdf

FECHA DE ENTREGA

El proyecto de grado titulado: DESARROLLO DE GUIAS DE LABORATORIO VIRTUAL DE FUNDAMENTOS DE REDES UTILIZANDO EL SOFTWARE PACKET TRACER fue entregado al departamento de eléctrica y electrónica de la ESPE y reposa en la escuela Politécnica del Ejercito desde:

Sangolquí, a _____ del 2008

ELABORADO POR:

_____
Diego Sebastián Stadler Román
171243917-1

AUTORIDADES:

_____
Ing. Gonzalo Olmedo
Coordinador de carrera