



**UNIVERSIDAD CATÓLICA DE
SANTIAGO DE GUAYAQUIL**

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

**TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO(A) EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN
EMPRESARIAL**

TEMA:

APLICACIÓN DEL SIMULADOR PACKET TRACER PARA LA REALIZACIÓN
DE PRÁCTICAS EN LA ASIGNATURA TELEMÁTICA I DE LA CARRERA DE
INGENIERIA EN TELECOMUNICACIONES

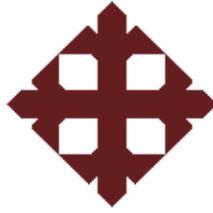
REALIZADO POR:

DIANA JESSENIA BARRAGÁN ROJAS

STEPHANIE SOFÍA JURADO SOLÍS

DIRECTOR:

ING. LUIS PINZÓN BARRIGA



TESIS DE GRADO

**APLICACIÓN DEL SIMULADOR PACKET TRACER PARA LA
REALIZACIÓN DE PRÁCTICAS EN LA ASIGNATURA TELEMÁTICA I DE
LA CARRERA DE INGENIERIA EN TELECOMUNICACIONES**

**Presentada a la Facultad de Educación Técnica para el Desarrollo, Carrera
de Ingeniería en Telecomunicaciones de la Universidad Católica de
Santiago de Guayaquil**

REALIZADO POR:

Diana Jessenia Barragan Rojas

Stephanie Sofía Jurado Solis

Para dar cumplimiento con uno de los requisitos para optar por el título de:
Ingeniero(a) en Telecomunicaciones con Mención en Gestión Empresarial

Ing. Luis Pinzón Barriga

Director de Tesis

Ing.....

Vocal

Ing.....

Vocal

Ing. Manuel Romero Paz

Decano de la Facultad

Ing. Luis Córdoba

Director de Carrera

CERTIFICACIÓN

Certifico que el proyecto de grado titulado “APLICACIÓN DEL SIMULADOR PACKET TRACER PARA LA REALIZACIÓN DE PRÁCTICAS EN LA ASIGNATURA TELEMÁTICA I DE LA CARRERA DE INGENIERIA EN TELECOMUNICACIONES” desarrollado por Diana Jessenia Barragan Rojas y Stephanie Sofía Jurado Solis fue realizado, corregido y terminado, razón por la cual está apto para su presentación y sustentación.

Ing. Luis Pinzón Barriga

DIRECTOR DE TESIS

AGRADECIMIENTO

A nuestro Padre Celestial por darnos vida, fuerza e iluminarnos en cada uno de los pasos emprendidos para culminar nuestra carrera universitaria.

A nuestros padres y familiares por su apoyo incondicional en todas las metas que nos hemos propuesto y por sus sabios consejos para superar cualquier adversidad que se nos ha presentado en este trayecto.

A nuestro Decano, el Ing. Manuel Romero Paz, que con su experiencia y paciencia nos condujo en el desarrollo de nuestro proyecto de tesis, siempre pendiente en cualquier detalle durante la implementación y revisión del mismo.

A todos nuestros profesores que en el transcurso de nuestra carrera supieron brindarnos sus conocimientos para finalmente ponerlos en práctica en nuestra vida profesional.

A nuestros compañeros por compartir con nosotros alegrías, tristezas, experiencias y oportunidades durante todo nuestro ciclo universitario.

DEDICATORIA

Dedicamos este trabajo a todas las personas que nos han apoyado directa e indirectamente y en especial a nuestros padres, que con su ejemplo de amor y constancia, han influido en nuestras personalidades para poner el entusiasmo, dedicación y esfuerzo, para llegar a la culminación de nuestros logros profesionales.

RESUMEN

La presente investigación tiene como propósito principal realizar un análisis al pensum de la Carrera de Ingeniería en Telecomunicaciones de la Facultad de Educación Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil (UCSG), dirigida a la materia Telemática I, para luego incluir un software simulador denominado *Packet Tracer*, en el cual se puedan realizar simulaciones que van desde un simple diseño de una red LAN(*Local Area Network*, Red de Área Local) hasta el diseño de una más compleja con la interacción de los diferentes dispositivos, protocolos y las respectivas topologías, normas y estándares, para luego plasmarlos con componentes reales ósea con su hardware correspondiente sin obtener ningún inconveniente al momento de conectarlos e instalarlos.

Lo cual hace de este software simulador de redes una herramienta importante de enseñanza y aprendizaje para el estudiante de la carrera 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 usarlas en la actualidad a nivel mundial.

El software *Packet Tracer* permite realizar la simulación en tiempo real o en tipo de simulación verificando el recorrido de cada paquete. En las prácticas realizadas empezamos con conexiones básicas como es una conexión entre dos PC's, hasta interconectar varios dispositivos y crear una red específica.

Este procedimiento servirá para la unificación del área teórica y práctica de la materia, es decir poder aplicar los conocimientos adquiridos en el aula de manera rápida y fácil, lo cual permitirá al estudiante llegar a un conocimiento integral de la misma.

ÍNDICE

CAPITULO I

1.....	G
Generalidades del Proyecto	1
1.1.....	I
Introducción.....	1, 2
1.2.....	A
Antecedentes.....	2
1.3.....	J
Justificación.....	3, 4
1.4.....	P
Planteamiento del Problema	4
1.5.....	H
Hipótesis	5
1.6.....	O
Objetivos	5
1.6.1.	O
Objetivo General.....	5
1.6.2.	O
Objetivos Específicos	5, 6

CAPITULO II

2.....	I
Introducción a las Redes e Internet	7
2.1.....	D
Definición de Redes de Datos.....	7,8
2.2.....	I
Internet: Una Red de Redes	8
2.2.1.	I
Internetnetwork	8, 9

2.2.2.	I
Intranet	9
2.3.	C
Comunicación a través de Redes	9, 10
2.3.1.	E
Elementos de una Red	10-13
2.3.1.1.	D
Dispositivos finales y su rol en la red	14
2.3.1.2.	D
Dispositivos intermediarios y su rol en la red	14, 15
2.3.1.3.	M
Medios de red	15, 16
2.4.	R
Redes Múltiples de Múltiples Servicios	17
2.4.1.	R
Redes convergentes	17, 18
2.5.	R
Redes de Comunicación	18, 19
2.5.1.	P
Por Cubrimiento	19
2.5.1.1.	R
Redes de área local (LAN)	19, 20
2.5.1.2.	R
Redes de área extensa (WAN)	20, 21
2.5.1.3.	R
Redes de Área Metropolitana (MAN)	21, 22
2.5.2.	P
Por Topología	22
2.5.2.1.	E
Estrella	22, 23
2.5.2.2.	B
US Ethernet	23-25
2.5.2.3.	A
Anillo Token Ring	25, 26

2.6.....	T
tipos De Conexiones	26
2.6.1.....	P
peer to peer (Punto a punto)	26
2.6.1.1.....	V
ventajas de una Red Punto a Punto.....	27
2.6.1.2.....	D
desventajas de una Red Punto a Punto	27
2.6.2.....	C
cliente servidor	28, 29
2.6.2.1.....	V
ventajas de una Red Cliente – Servidor	29
2.6.2.2.....	D
desventajas de una Red Cliente – Servidor.....	29

CAPITULO III

3.....	M
modelos de capas y protocolos de red	30
3.1.....	M
modelos De Protocolo Y Referencia.....	31, 32
3.1.1.....	M
modelo TCP/IP	31-34
3.1.2.....	M
modelo OSI.....	34-36
3.2.....	C
comparación Entre Modelo OSI Y Modelo TCP/IP	36-38
3.3.....	P
protocolos TCP/IP	38-43
3.4.....	S
servicios E Interfaces	43, 44
3.5.....	T
tipos De Servicio	44, 45

3.6.....	P
limitativas De Servicio	45, 46
3.7.....	E
standarización	46-48

CAPITULO IV

4.....	S
oftware Simulator Packet Tracer	49
4.1.....	D
definición	49
4.2.....	U
utilidad Del <i>Packet Tracer</i>	49, 50
4.3.....	P
propósito	50
4.3.1.....	S
simulador <i>Packet Tracer</i> basado en el aprendizaje.....	51
4.4.....	C
contenido	51
4.4.1.....	E
elementos	51
4.4.2.....	P
principales funcionalidades	52
4.4.3.....	P
protocolos	52
4.5.....	A
actividades Dentro De <i>Packet Tracer</i>	53, 54
4.6.....	B
beneficios de la Simulación Basada en el Aprendizaje	55
4.6.1.....	B
beneficios <i>Packet Tracer</i>	55
4.6.1.1.....	B
beneficios Claves para el Docente	55, 56
4.6.1.2.....	B
beneficios para Estudiantes	56

4.7.....	P
Programa De Simulación Packet Tracer	57
4.7.1.....	D
Descripción General de las opciones gráficas y barras	57-65
4.7.2.....	C
Colocación de Dispositivos.....	66-70
4.7.3.....	M
Modo Simulación (Simulation)	70-72
4.7.4.....	D
Descripción de los controles.....	72-79

CAPITULO V

5.....	S
Simulaciones De Prácticas A Través Del Software Packet Tracer	80
5.1.....	P
Practica # 1: Interconexión de dos CPU's utilizando cable cruzado.....	80-87
5.2.....	P
Practica # 2: Realizar una pequeña red LAN interconectando un switch y un hub	88-94
5.3.....	P
Practica # 3: Realizar una red LAN utilizando un Access Point(AP) y un Switch.....	95-107
5.4.....	P
Practica # 4: Realizar una red LAN en la que se observa las diferentes capas del modelo OSI.....	108-113
5.5.....	P
Practica # 4: Conexión de varios dispositivos de inter conectividad para una red.....	114-119
6.....	C
Conclusiones	120,121
7.....	R
Recomendaciones	121
8.....	G
Glosario	122-124

9.....	B
bibliografía	125, 126

INDICE DE LAS FIGURAS

CAPITULO 2: INTRODUCCION A LAS REDES Y EL INTERNET

Figura 2.1.	Elementos de una red.....	10
Figura 2.2.	Equipos Terminales.....	11
Figura 2.3.	Símbolos de medio de interconexión de redes.....	12
Figura 2.4.	Dispositivos Intermedios.....	12
Figura 2.5.	Reglas, Protocolos.....	13
Figura 2.6.	Medios de Red.....	16
Figura 2.7.	Redes Múltiples.....	17
Figura 2.8.	Red Convergente.....	18
Figura 2.9.	Red de Área Local LAN.....	20
Figura 2.10.	Conexión de 2 LAN mediante una WAN.....	21
Figura 2.11.	Topología Estrella.....	23
Figura 2.12.	Topología Bus.....	23
Figura 2.13.	Topología Anillo.....	25
Figura 2.14.	Red Punto a Punto.....	27

Figura 2.15.	Cliente Servidor.....	29
--------------	-----------------------	----

CAPITULO III: MODELOS DE CAPAS Y PROTOCOLOS DE RED

Figura 3.1.	Modelo OSI y TCP/IP.....	31
Figura 3.2.	Modelo TCP/IP.....	32
Figura 3.3.	Proceso de comunicación.....	34
Figura 3.4.	Modelo OSI.....	35
Figura 3.5.	Comparación del modelo OSI con el modelo TCP/IP.....	38
Figura 3.6.	Protocolo HTTP mediante GET.....	39
Figura 3.7.	Protocolo SMTP y POP3.....	40
Figura 3.8.	Protocolo FTP.....	41
Figura 3.9.	Compartir archivos mediante protocolo SMB.....	42
Figura 3.10.	Proceso Telnet.....	43

CAPITULO IV: SOFTWARE SIMULADOR PACKET TRACER

Figura 4.1.	Simulador Comando IOS.....	53
Figura 4.2.	Tráfico de redes.....	54
Figura 4.3.	Actividades Multiredes.....	54
Figura 4.4.	Simulador Packet Tracer.....	57
Figura 4.5.	Barra Principal.....	58
Figura 4.6.	Opciones Preferences.....	59
Figura 4.7.	Opciones de Administración.....	60
Figura 4.8.	Proceso para agregar una descripción en <i>Packet Tracer</i>	61
Figura 4.9.	Proceso para agregar un fondo en <i>Packet Tracer</i>	61
Figura 4.10.	Visualización de los dispositivos y tipos de conexiones.....	63
Figura 4.11.	Modos Realtime y Simulation.....	64

Figura 4.12.	Visualización Lógica y Física.....	65
Figura 4.13.	Selección del dispositivo (router genérico).....	66
Figura 4.14.	Dispositivo colocado en el espacio de diseño.....	67
Figura 4.15.	Grupo de dispositivos agregados.....	68
Figura 4.16.	Proceso para eliminar un dispositivo.....	68
Figura 4.17.	Descripción para agregar información a la red.....	69
Figura 4.18.	Descripción para obtener información de configuración del router.....	70
Figura 4.19.	Modo Simulación, selección de filtros.....	71
Figura 4.20.	Proceso PDU simple.....	71
Figura 4.21.	Protocolos a seleccionar para el proceso de envío de PDU...	72
Figura 4.22.	Barra de desplazamiento y controles de eventos.....	72
Figura 4.23.	Descripción de controles.....	73
Figura 4.24.	Captura de paquetes desde PC0 a PC1.....	74
Figura 4.25.	Panel para resetear la simulación.....	75
Figura 4.26.	Modo Simulación.....	76
Figura 4.27.	Descripción para crear un nuevo escenario.....	77
Figura 4.28.	Ingreso a Command Prompt.....	78
Figura 4.29.	Ping desde el command de PC0 a PC1.....	78
Figura 4.30.	Respuesta a Ping desde el command de PC0 a PC1.....	79

CAPITULO V: SIMULACIÓN DE PRÁCTICAS A TRAVES SOFTWARE PACKET TRACER

Figura 5.1.	Colocación de 2 PC's en el espacio de trabajo de PT.....	80
Figura 5.2.	Conexión entre las 2 PC's a los puertos Fastethernet.....	81
Figura 5.3.	Conexión entre las 2 PC's con cable cruzado.....	82
Figura 5.4.	Ingreso a IP Configuration.....	82
Figura 5.5.	Direccionamiento de la tarjeta de red de PC0.....	83

Figura 5.6.	Direccionamiento de la tarjeta de red de PC1.....	83
Figura 5.7.	Direccionamiento de la tarjeta de red de PC1.....	84
Figura 4.8.	Ingreso a Command Prompt desde la PC0.....	84
Figura 5.9.	Ping desde la PC0 a la PC1.....	85
Figura 5.10.	Modo simulación – PDU simple.....	85
Figura 5.11.	Paquetes ICMP desde PC0 a PC1.....	86
Figura 5.12.	Transferencia de paquetes exitosa.....	86
Figura 5.13.	Colocación de equipos a utilizarse.....	88
Figura 5.14.	Conexión de PC0, PC1 e impresora al Switch.....	89
Figura 5.15.	Conexión de PC2 y PC3 al hub.....	89
Figura 5.16.	Conexión entre el Switch y el hub.....	90
Figura 5.17.	Verificación de puertos activos.....	90
Figura 5.18.	Direccionamiento de la tarjeta de red de los CPU's	91
Figura 5.19.	Asignación de dirección IP a impresora.....	91
Figura 5.20.	Simulación de transferencia de información.....	92
Figura 5.21.	Simulación de transferencia de información 2 y 3.....	93
Figura 5.22.	Colocación de dispositivos a utilizarse.....	95
Figura 5.23.	Conexión entre dispositivos.....	96
Figura 5.24.	Proceso para ingresar a la tarjeta NIC de PC0.....	97
Figura 5.25.	Direccionamiento de tarjeta de red de PC0.....	97
Figura 5.26.	Asignación de dirección IP.....	98
Figura 5.27.	Verificación de puertos del Switch.....	99
Figura 5.28.	Verificación de puertos del AP.....	100
Figura 5.29.	Configuración de SSID y Password para la red Wireless.....	101
Figura 6.30.	Ingreso a PC Wireless.....	102
Figura 5.31.	Selección de la red configurada en el AP.....	103
Figura 5.32.	Digitación de la clave de acceso a la red.....	103
Figura 5.33.	Computadoras conectadas al AP.....	104
Figura 5.34.	Transferencia de paquetes de PC0 a impresora.....	105

Figura 5.35.	Transferencia de paquetes desde el AP hacia la PC1 y PC2.	105
Figura 5.36.	Transferencia de paquetes desde el switch hacia el AP.....	106
Figura 5.37.	Transferencia de paquetes exitosa.....	107
Figura 5.38.	Colocación y configuración de dispositivos.....	109
Figura 5.39.	Verificación de paquete de datos entre PC1 y PC4.....	110
Figura 5.40.	Visualización capa 3 del modelo OSI.....	111
Figura 5.41.	Visualización capa 2 del modelo OSI.....	111
Figura 5.42.	Visualización de capa 1,2 y 3 del modelo OSI.....	112
Figura 5.43.	Visualización de capa1, 2 y 3 del modelo OSI.....	113
Figura 5.44.	Conexión de equipos.....	115
Figura 5.45.	Direccionamiento IP de los equipos.....	115
Figura 5.46.	Configuración de los Routers.....	116
Figura 5.47.	Transferencia de datos visualización de protocolos.....	118
Figura 5.48.	Finalización de transferencia de paquete.....	118

INDICE DE TABLAS

Tabla 5.1:	Direccionamiento IP.....	108
Tabla 5.2:	Direccionamiento IP de los equipos.....	116
Tabla 5.3:	Direccionamiento IP de los Routers.....	117

CAPITULO I

1 GENERALIDADES DEL PROYECTO

Este capítulo presenta la introducción de este proyecto, los antecedentes y justificativos que permitieron encontrar una mejora en la malla curricular existente de la asignatura de Telemática I, para que de esta manera se complemente la enseñanza por parte del maestro y el aprendizaje por parte del estudiante, planteándose una serie de objetivos específicos para alcanzar el propósito principal de este proyecto de tesis.

1.1 INTRODUCCIÓN

Este tema pretende que se establezcan las funcionalidades básicas generales y avanzadas, acerca del funcionamiento de esta herramienta que provee CISCO. Este simulador sirve para diseñar redes de computadoras, sin la necesidad de tener dispositivos de hardware o software adicionales a la máquina en la que está instalada esta herramienta. Entonces permite crear una o varias redes, permitiendo su configuración real.

Esto agrega un gran valor, pues esta herramienta dispone de interfaces de hardware genéricas y específicas de dicha empresa, no necesitando tener dos computadoras, routers, interfaces, cables, etc., para saber el comportamiento físico y real de una red. Ahorrando así, tiempo en construcción de redes.

Luego de la creación de las redes, es necesario únicamente seguir los pasos sistemáticos que se realizaron en la herramienta, convirtiéndose en una gran ventaja, pues no se necesita tener el espacio físico y todas las computadoras para saber si funciona la red.

En el ámbito estudiantil, el ahorro del movimiento de equipo y a nivel profesional el ahorro de dispositivos de conexión y de tiempo es un factor determinante en cualquier proyecto.

1.2 ANTECEDENTES

Desde sus inicios en la Facultad Técnica, la Ingeniería en Telecomunicaciones no ha incluido en su pensum académico materias de laboratorio en simulación de redes, solo se han enfocado en el aspecto teórico de como diseñar una red de área local o de área extensa, pero esos conocimientos no se han podido complementar debido a la falta de una herramienta práctica para poder plasmar los conocimientos adquiridos.

En la actualidad, la carrera de Ingeniería en Telecomunicaciones en la materia de Telemática I exige varios conocimientos fundamentales para complementar el aprendizaje de la misma, de una manera práctica para un mejor entendimiento y asimilación de los conceptos impartidos en el aula.

Uno de los temas básicos que se maneja en Telemática es como diseñar una red y para esto es necesario tener un conocimiento completo no solo teórico sino también practico para que así al momento de que un estudiante de la carrera de Telecomunicaciones desea realizar u obtener una certificación en redes ya tenga una preparación previa.

Debido a estos antecedentes es necesario manejar y sacarle el mayor provecho a toda herramienta que permita desarrollar habilidades de cómo diseñar redes de pequeñas, medianas o grandes empresas, debido a que en hoy en día hay un enfoque profundo y consecuentemente la necesidad de profesionales con habilidades en redes y su tecnología, facilitando la implementación de una red al momento de realizar un proyecto en la vida profesional.

1.3 JUSTIFICACIÓN

Las redes de la actualidad tienen un impacto significativo en nuestras vidas, ya que cambian la forma de vivir, trabajar y divertirse. Las redes de computadoras (y en especial la red más grande, el Internet) permiten a las personas comunicarse, colaborar e interactuar de maneras totalmente novedosas. Se utiliza la red de distintas formas, entre ellas las aplicaciones Web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y más.

Para pequeñas, medianas o grandes empresas, la comunicación digital de datos, voz y video es esencial para la supervivencia de una empresa. En consecuencia, una red LAN con un diseño apropiado es un requisito fundamental para el emprendimiento y buen desempeño de cualquier compañía. El estudiante o profesional en este campo debe ser capaz de reconocer una red bien diseñada que puede ser LAN, WAN(*Wide Area Network*, Red de Área Extensa), MAN(*Metropolitan Area Network*, Red de Área Metropolitana), etc. y seleccionar los dispositivos apropiados para admitir las especificaciones de las redes de una empresa dependiendo de su tamaño y crecimiento a futuro, por tales razones de vital importancia se plantea el siguiente direccionamiento para la adquisición de un conocimiento integral sobre el tema dentro de la carrera.

Por esta razón el objetivo de esta tesis se enfoca en realizar un análisis del contenido de la materia de Telemática I dentro de la Carrera de Ingeniería en Telecomunicaciones, determinar las falencias en cuanto a la asimilación y entendimiento completo del contenido teórico de la misma y de esta manera proceder con la implementación de una herramienta considerada indispensable (después del análisis previo) para realizar prácticas de laboratorio y se fundamenten en todos los conocimientos teóricos impartidos por el maestro en las aulas.

De acuerdo a esta primera observación del análisis se considera necesario proporcionar a la comunidad estudiantil, en los Laboratorios de Telecomunicaciones, un software simulador de diferentes topologías de redes de área local o de área extensa que provee CISCO denominado *Packet Tracer*, mejorando así el aprendizaje de la materia Telemática I, con un sin número de prácticas a realizarse y simulación en tiempo real, permitiendo al estudiante identificar los diferentes tipos de redes, dispositivos, equipos, protocolos de enrutamiento y demás características propias que involucran al gran mundo de las redes de computadores, convergentes y el internet.

Culminando el trabajo detallado en este estudio, los estudiantes de la Carrera de Ingeniería en Telecomunicaciones tendrán a disponibilidad en su laboratorio la herramienta necesaria para complementar el aprendizaje de la materia Telemática I, siendo ésta una asignatura importante para el buen desempeño del profesional en esta especialidad, ya que hoy en día existe gran competitividad a nivel profesional en el campo del diseño de las redes y el Internet.

En conclusión, la implementación de este software en el Laboratorio de Telecomunicaciones es una solución viable y óptima para contribuir con una mejor enseñanza y entendimiento de la materia Telemática I, debido a que en la actualidad todo gira en torno al mundo de las redes convergentes, la tecnología y el internet, convirtiéndose entonces este software a implementarse en una herramienta fundamental para la asimilación del contenido de esta materia tan importante que servirá a los futuros profesionales en su vida laboral.

1.4 PLANTEAMIENTO DEL PROBLEMA

La necesidad de incorporar un componente práctico en la materia Telemática I de Séptimo Ciclo de la Carrera de Ingeniería en Telecomunicaciones para reforzar y complementar la asimilación y entendimiento de los conocimientos teóricos impartidos por el docente en el aula.

1.5 HIPÓTESIS

El uso de un software que permita simular e implementar los diferentes tipos de redes de área local, área extensa y convergentes entre otros conocimientos relacionados con las redes y el internet vistos teóricamente en la materia de Telemática I, brindará al estudiante la opción de desarrollar un aprendizaje experimental y clarificar mediante diseños prácticos los conocimientos teóricos adquiridos previamente.

1.6 OBJETIVOS

Los objetivos planteados para este proyecto de investigación son los siguientes:

1.6.1 OBJETIVO GENERAL

Aplicar el software simulador de redes *PACKET TRACER* como herramienta de carácter práctico para el programa académico de la asignatura de Telemática I de la Carrera de Ingeniería en Telecomunicaciones.

1.6.2 OBJETIVOS ESPECIFICOS

Los objetivos específicos son los siguientes:

- Analizar el programa y syllabus de la asignatura Telemática I para luego determinar las áreas del mismo que necesitan apoyo práctico.
- Aprender el manejo del simulador *Packet Tracer*.
- Determinar las herramientas de *Packet Tracer* necesarias para desarrollar los temas decididos.
- Utilizar las herramientas más comunes para la manipulación de dispositivos.

- Crear topologías de red mediante la selección de los dispositivos, interconexión y su respectiva ubicación en un área de trabajo, utilizando la interfaz gráfica de *Packet Tracer*.
- Determinar y desarrollar las prácticas que serán realizadas.
- Incluir estas prácticas en el programa de la asignatura Telemática I.

CAPITULO II

2 INTRODUCCION A LAS REDES Y EL INTERNET

En este capítulo se presenta de manera detallada una introducción a las redes de datos/convergentes y sus componentes, sus características, funcionalidades y tipos de conexiones posibles, dependiendo de la topología de red a utilizar, destacando sus ventajas y desventajas al momento de conocer los requerimientos de cualquier área de trabajo que desee implementar una red de datos o convergente.

2.1 DEFINICIÓN DE REDES DE DATOS

Una red de datos es un sistema que enlaza dos o más puntos (terminales) por un medio físico, el cual sirve para enviar o recibir un determinado flujo de información (Anónimo, 2010).

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

- Información.
- Bases de Datos.
- Mensajes y Agendas.
- Impresoras.
- Faxes.
- Modems.

Objetivos de la red de datos:

- 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. (Stadler, 2008)

2.2 INTERNET: UNA RED DE REDES

Aunque existen beneficios por el uso de una LAN o WAN, la mayoría de los usuarios necesitan comunicarse con un recurso u otra red, fuera de la organización local.

Los ejemplos de este tipo de comunicación incluyen:

- enviar un correo electrónico a un amigo en otro país,
- acceder a noticias o productos de un sitio Web,
- obtener un archivo de la computadora de un vecino,
- mensajería instantánea con un pariente de otra ciudad, y
- seguimiento de la actividad de un equipo deportivo favorito a través del teléfono celular.

2.2.1 Internetwork

Una malla global de redes interconectadas (internetworks) cubre estas necesidades de comunicación humanas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo. La internetwork más conocida, ampliamente utilizada y a la que accede el público en general es Internet.

Internet se crea por la interconexión de redes que pertenecen a los Proveedores de servicios de Internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo.

Garantizar la comunicación efectiva a través de esta infraestructura diversa requiere la aplicación de tecnologías y protocolos consistentes y reconocidos comúnmente, como también la cooperación de muchas agencias de administración de redes.

2.2.2 Intranet

El término intranet se utiliza generalmente para referirse a una conexión privada de algunas LAN y WAN que pertenecen a una organización y que está diseñada para que puedan acceder solamente los miembros y empleados de la organización u otros que tengan autorización.

Nota: Es posible que los siguientes términos sean sinónimos: internetwork, red de datos y red. Una conexión de dos o más redes de datos forma una internetwork: una red de redes. También es habitual referirse a una internetwork como una red de datos o simplemente como una red, cuando se consideran las comunicaciones a alto nivel. El uso de los términos depende del contexto y del momento, a veces los términos pueden ser intercambiados.

2.3 COMUNICACIÓN A TRAVES DE REDES

Poder comunicarse en forma confiable con todos en todas partes es de vital importancia para nuestra vida personal y comercial. Para respaldar el envío inmediato de los millones de mensajes que se intercambian entre las personas de todo el mundo, confiamos en una Web de redes interconectadas. Estas redes de información o datos varían en tamaño y capacidad, pero todas las redes tienen cuatro elementos básicos en común:

- reglas y acuerdos para regular cómo se envían, redireccionan, reciben e interpretan los mensajes.
- los mensajes o unidades de información que viajan de un dispositivo a otro,

- una forma de interconectar esos dispositivos, un medio que puede transportar los mensajes de un dispositivo a otro, y
- los dispositivos de la red que cambian mensajes entre sí.

La estandarización de los distintos elementos de la red permite el funcionamiento conjunto de equipos y dispositivos creados por diferentes compañías.

Los expertos en diversas tecnologías pueden contribuir con las mejores ideas para desarrollar una red eficiente sin tener en cuenta la marca o el fabricante del equipo.

2.3.1 Elementos de una red

El diagrama muestra los elementos de una red típica, incluyendo dispositivos, medios y servicios unidos por reglas, que trabajan en forma conjunta para enviar mensajes. Utilizamos la palabra mensajes como un término que abarca las páginas Web, los e-mails, los mensajes instantáneos, las llamadas telefónicas y otras formas de comunicación permitidas por Internet.

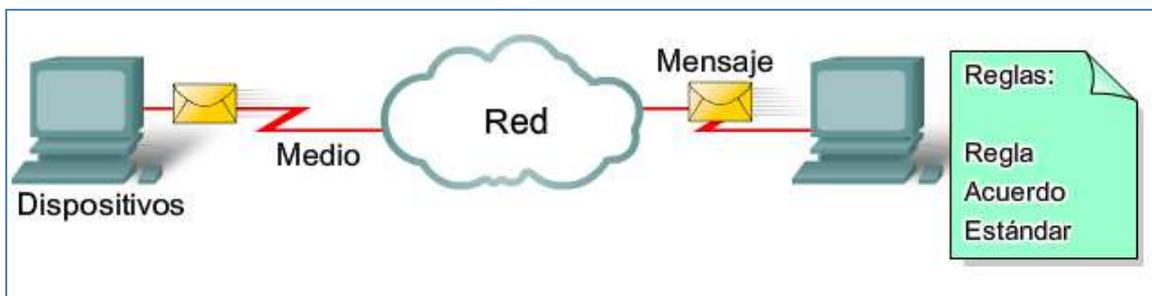


Figura 2.1: Elementos de una red.

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de networking

Por lo que se describe en la figura, los elementos de una red son 4:

- Dispositivos.
- Medio.

- Mensajes.
- Reglas.

En los extremos del diagrama se muestran algunos dispositivos terminales comunes que generalmente originan mensajes que constituyen nuestra comunicación.

Esto incluye diversos tipos de equipos (computadoras, laptops, impresoras etc), servidores y teléfonos IP. En las redes de área local, estos dispositivos generalmente se conectan a través de medios LAN (con cables o inalámbricos).



Figura 2.2: Equipos Terminales

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de networking

En la figura, la gran nube (se utiliza para resumir un grupo de dispositivos de red), puede contener algunos de los dispositivos intermedios más comunes, utilizados para direccionar y administrar los mensajes en la red, como así también otros símbolos comunes de interconexión de redes como lo es el enlace serial (una forma de interconexión WAN, representada por la línea en forma de rayo).



Figura 2.3: Símbolos de medios de interconexión de redes

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de networking

Estos dispositivos intermedios son:

- **Switch:** el dispositivo más utilizado para interconectar redes de área local,
- **Firewall:** proporciona seguridad a las redes.
- **Router:** ayuda a direccionar mensajes mientras viajan a través de una red,
- **Router inalámbrico:** un tipo específico de router que generalmente se encuentra en redes domésticas.

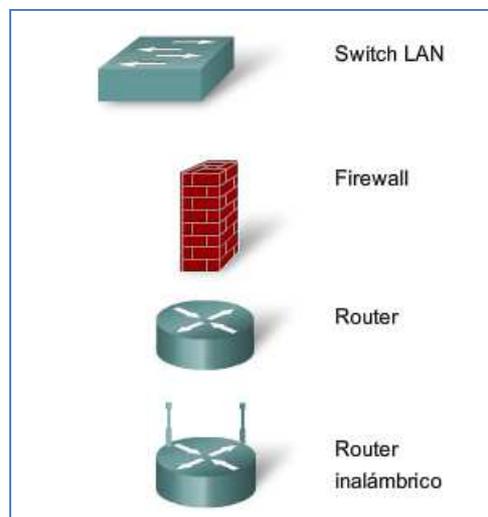


Figura 2.4: Dispositivos Intermedios

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*.

Las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas; estas aplicaciones necesitan servicios para funcionar en la red. Algunos de estos servicios incluyen World Wide Web, e-mail,

mensajería instantánea y telefonía IP. Los dispositivos interconectados a través de medios para proporcionar servicios deben estar gobernados por reglas o protocolos.

En el cuadro se enumeran algunos servicios y un protocolo vinculado en forma más directa con ese servicio. Los protocolos son las reglas que utilizan los dispositivos de red para comunicarse entre sí.

Actualmente el estándar de la industria en redes es un conjunto de protocolos denominado TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP se utiliza en redes comerciales y domésticas, siendo también el protocolo primario de Internet. Son los protocolos TCP/IP los que especifican los mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.

Servicio	Protocolo ("Regla")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Mensaje instantáneo (Jabber; AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Sistema abierto para la comunicación en tiempo real)
Telefonía IP	SIP (Session Initiation Protocol)

Figura 2.5: Reglas = Protocolos

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*.

2.3.1.1 Dispositivos finales y su rol en la red

Los dispositivos de red con los que la gente está más familiarizada se denominan dispositivos finales. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente. Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores Web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Dispositivos móviles de mano (como escáneres de barras inalámbricos, asistentes digitales personales (PDA))

En el contexto de una red, los dispositivos finales se denominan host. Un dispositivo host puede ser el origen o el destino de un mensaje transmitido a través de la red. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia una comunicación, utiliza la dirección del host de destino para especificar dónde debe ser enviado el mensaje.

Los servidores son hosts que tienen software instalado que les permite proporcionar información y servicios, como e-mail o páginas Web, a otros hosts en la red.

2.3.1.2 Dispositivos intermediarios y su rol en la red.

Además de los dispositivos finales con los cuales la gente está familiarizada, las redes dependen de dispositivos intermediarios para proporcionar conectividad y para trabajar detrás de escena y garantizar que los datos fluyan a través de la red.

Estos dispositivos conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork. Los siguientes son ejemplos de dispositivos de red intermediarios:

- dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos),
- dispositivos de internetworking (routers),
- servidores de comunicación y módems, y
- dispositivos de seguridad (firewalls).

La administración de datos mientras fluyen a través de la red también es una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red, para determinar la ruta que deben tomar los mensajes a través de la red. Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- regenerar y retransmitir señales de datos,
- mantener información sobre qué rutas existen a través de la red y de la internetwork,
- notificar a otros dispositivos los errores y las fallas de comunicación,
- direccionar datos por rutas alternativas cuando existen fallas en un enlace,
- clasificar y direccionar mensajes según las prioridades de QoS (calidad de servicio), y
- permitir o denegar el flujo de datos en base a configuraciones de seguridad.

La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

2.3.1.3 Medios de red.

Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son:

- hilos metálicos dentro de los cables,
- fibras de vidrio o plásticas (cable de fibra óptica), y
- transmisión inalámbrica.

La codificación de señal que se debe realizar para que el mensaje sea transmitido es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:

- la distancia en la cual el medio puede transportar exitosamente una señal,
- el ambiente en el cual se instalará el medio,
- la cantidad de datos y la velocidad a la que se deben transmitir, y
- el costo del medio y de la instalación.

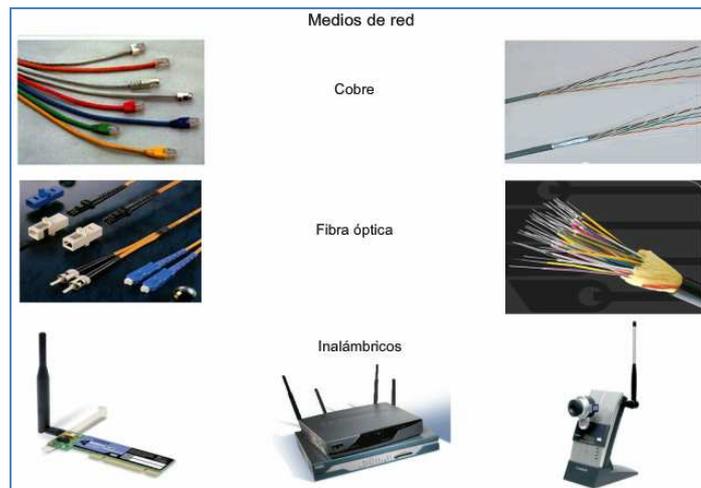


Figura 2.6: Medios de Red

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*.

2.4 REDES MULTIPLES DE MULTIPLES SERVICIOS.

El teléfono tradicional, la radio, la televisión y las redes de datos informáticos tienen su propia versión individual de los cuatro elementos básicos de la red. En el pasado, cada uno de estos servicios requería una tecnología diferente para emitir su señal de comunicación particular. Además, cada servicio tiene su propio conjunto de reglas y estándares para garantizar la comunicación exitosa de su señal a través de un medio específico.

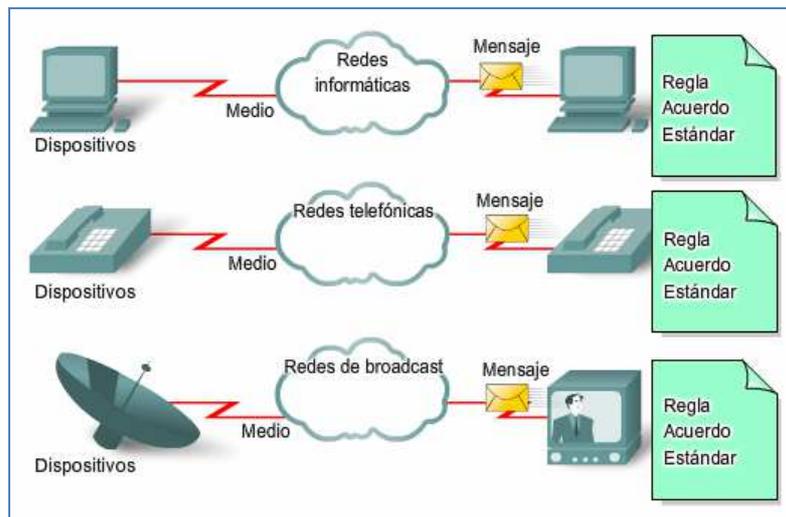


Figura 2.7: Redes Múltiples

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*

2.4.1 Redes convergentes

Los avances de la tecnología nos permiten consolidar esas redes dispersas en una única plataforma: una plataforma definida como una red convergente.

El flujo de voz, vídeo y datos que viajan a través de la misma red elimina la necesidad de crear y mantener redes separadas.

En una red convergente todavía hay muchos puntos de contacto y muchos dispositivos especializados (por ejemplo: computadoras personales, teléfonos, televisores, asistentes personales y registradoras de puntos de venta minoristas) pero una sola infraestructura de red común. (ACADEMY, 2011)

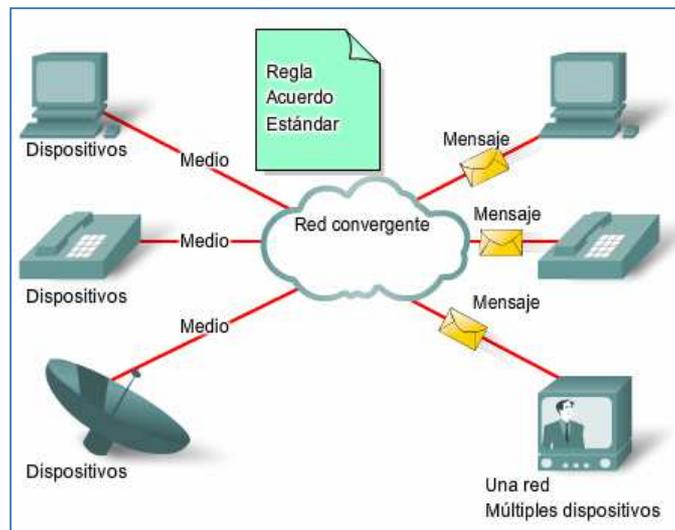


Figura 2.8: Red Convergente

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*

2.5 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, TIA/EIA, IEEE, CCITT (ITU-T).

Las clasificaciones más importantes son:

- **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)

2.5.1 Por Cubrimiento

Se distinguen diferentes tipos de redes (privadas) según su tamaño (en cuanto a la cantidad de equipos), su velocidad de transferencia de datos y su alcance. Generalmente se dice que existen tres categorías de redes y se clasifican en LAN, MAN y WAN. (Stadler, 2008)

2.5.1.1 Redes de área local (LAN)

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina Red de área local (LAN).

Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.

Las infraestructuras de red pueden variar en gran medida en términos de:

- el tamaño del área cubierta,
- la cantidad de usuarios conectados, y
- la cantidad y tipos de servicios disponibles.

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. (ACADEMY, 2011)

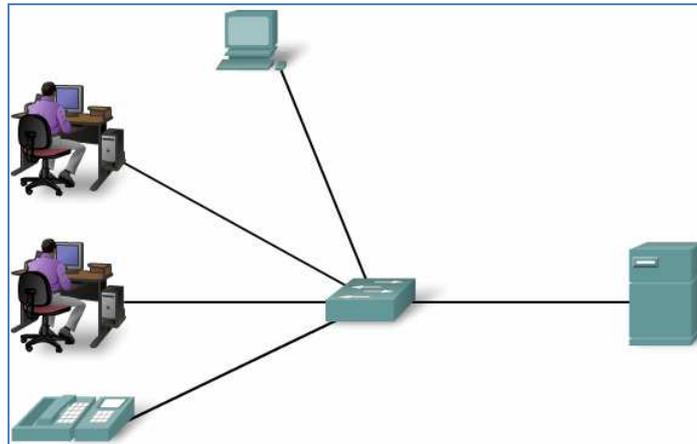


Figura 2.9: Red de Área Local (LAN)

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*

2.5.1.2 Redes de área extensa (WAN)

Una red de área extensa WAN es un sistema de interconexión de equipos informáticos geográficamente dispersos, incluso en continentes distintos.

Las líneas utilizadas para realizar esta interconexión suelen ser parte de las redes públicas de transmisión de datos.

Cuando una compañía o una organización tienen ubicaciones separadas por grandes distancias geográficas, es posible que deba utilizar un proveedor de servicio de telecomunicaciones (TSP) para interconectar las LAN en las distintas ubicaciones. Los proveedores de servicios de telecomunicaciones operan grandes redes regionales que pueden abarcar largas distancias. Tradicionalmente, los TSP transportaban las comunicaciones de voz y de datos en redes separadas. Cada vez más, estos proveedores ofrecen a sus subscriptores servicios de red convergente de información. (Stadler, 2008)

Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que

conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones son controladas por el TSP.

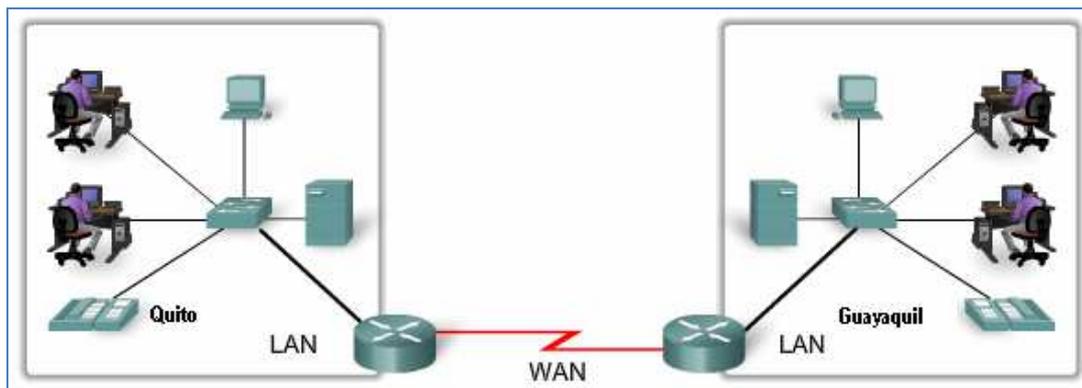


Figura 2.10: Conexión de 2 LAN mediante una WAN

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*.

2.5.1.3 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. (ACADEMY, 2011)

2.5.2 Por Topología

Por topología o configuración de interconexión, las redes se pueden clasificar 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. (Stadler, 2008)

2.5.2.1 Estrella

La topología estrella es una de las topologías más populares de un LAN (Local Area Network). Es implementada conectando cada computadora a un Hub o concentrador central, véase la figura 2.11. El Hub puede ser Activo, Pasivo o Inteligente. Un hub activo es solo un punto de conexión y no requiere energía eléctrica. Un Hub activo (el más común) es actualmente un repetidor con múltiples puertos; impulsa la señal antes de pasarla a la siguiente computadora. Un Hub Inteligente es un hub activo pero con capacidad de diagnóstico, puede detectar errores y corregirlos. (Fire, 2003)

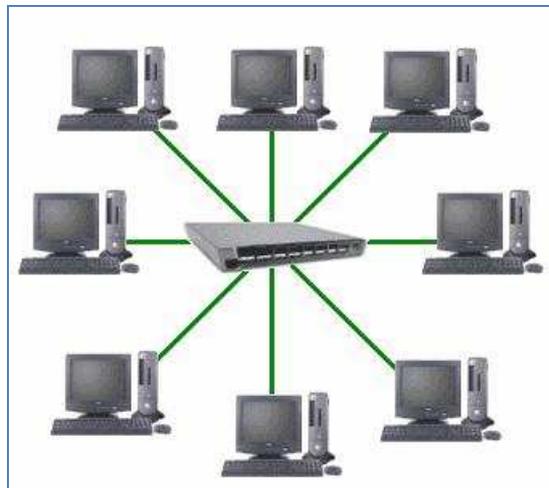


Figura 2.11: Topología Estrella

Fuente: <http://tkmpm2010.blogspot.com/2009/11/tologia-de-red-de-estrella.html>

2.5.2.2 BUS Ethernet

La topología de bus es la manera más simple en la que se puede organizar una red. En la topología de bus, todos los equipos están conectados a la misma línea de transmisión mediante un cable, generalmente coaxial. La palabra "bus" hace referencia a la línea física que une todos los equipos de la red. Véase figura 2.12.

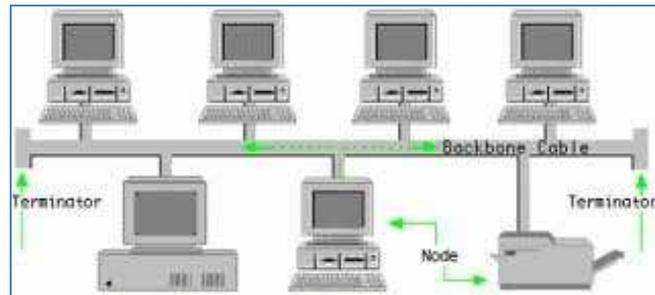


Figura 2.12: Topología Bus

Fuente: http://chemapqpiinformatica.blogspot.com/2011_01_01_archive.html

La ventaja de esta topología es su facilidad de implementación y funcionamiento. Sin embargo, esta topología es altamente vulnerable, ya que si una de las conexiones es defectuosa, esto afecta a toda la red. (Kioskea, 2008)

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 Collision Detect* (CSMA/CD) "acceso múltiple por censado de portadora y detección de colisión", cuya función se resume en los siguientes pasos:

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

Esta tecnología fue creada por Digital Equipment Corporation, Intel y Xerox, con lo cual se llamo inicialmente DIX Ethernet, luego la IEEE realizó mejoras importantes para hoy llamarse simplemente Ethernet.

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 200metros. 10BaseT, significa 10Mbps, en banda base, por par trenzado y hasta 100 metros. (Stadler, 2008)

Ethernet no ha evolucionado tan rápido como los medio físicos que la sustentan, 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 switcheo, 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.

2.5.2.3 Anillo Token Ring

En este tipo de topología las señales se pasan de una estación a otra en círculo. Véase la figura 2.13

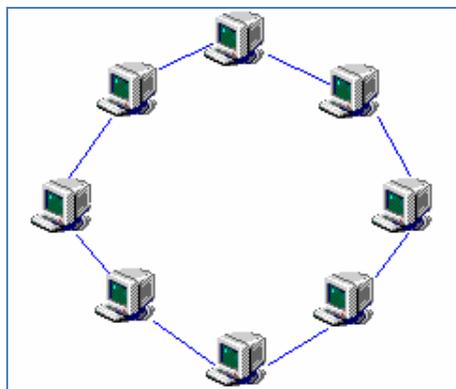


Figura 2.13: Topología Anillo

Fuente: <http://www.google.com.ec/imgres?q=topologia+anillo+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:

- 3 Escucha cuando pasa el testigo
- 4 Si el testigo está ocupado, escucha al siguiente testigo.
- 5 Si el testigo está libre (id/e), marca el testigo como ocupado (busy), adjunta los datos, y los envía por el anillo.
- 6 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.
- 7 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. (Stadler, 2008)

2.6 TIPOS DE CONEXIONES

Las redes también se diferencian por el tipo de conexión que tengan estructurada, entre las que destacamos las siguientes.

2.6.1 Peer to peer (Punto a punto)

Más conocida como P2P, 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. En un ambiente punto a punto, la seguridad es difícil, porque la administración no está centralizada. (Stadler, 2008)

Esta opción se conoce como punto (nodo) a punto, es decir se transmite de un edificio a otro. (Carrasco, 2010)

2.6.1.1 Ventajas de una Red Punto a Punto

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

2.6.1.2 Desventajas de una Red Punto a Punto.

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

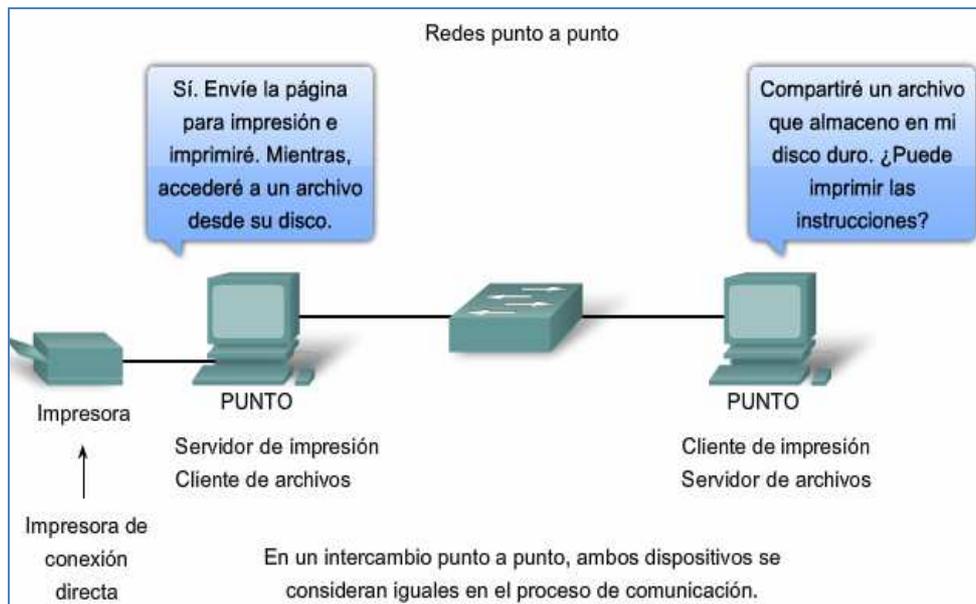


Figura 2.14: Red Punto a Punto

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*

2.6.2 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.

En el modelo cliente-servidor, el dispositivo que solicita información se denomina cliente y el dispositivo que responde a la solicitud se denomina servidor. Los procesos de cliente y servidor se consideran una parte de la capa de Aplicación. El cliente comienza el intercambio solicitando los datos al servidor, que responde enviando uno o más streams de datos al cliente. Los protocolos de capa de Aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Además de la transferencia real de datos, este intercambio puede requerir de información adicional, como la autenticación del usuario y la identificación de un archivo de datos a transferir.

Un ejemplo de una red cliente/servidor es un entorno corporativo donde los empleados utilizan un servidor de e-mail de la empresa para enviar, recibir y almacenar e-mails. El cliente de correo electrónico en la computadora de un empleado emite una solicitud al servidor de e-mail para un mensaje no leído. El servidor responde enviando el e-mail solicitado al cliente.

El flujo de datos puede ser el mismo en ambas direcciones o inclusive ser mayor en la dirección que va del cliente al servidor. Por ejemplo, un cliente puede transferir un archivo al servidor con fines de almacenamiento. La transferencia de datos de un cliente a un servidor se conoce como subida y la de los datos de un servidor a un cliente, descarga. (ACADEMY, 2011)

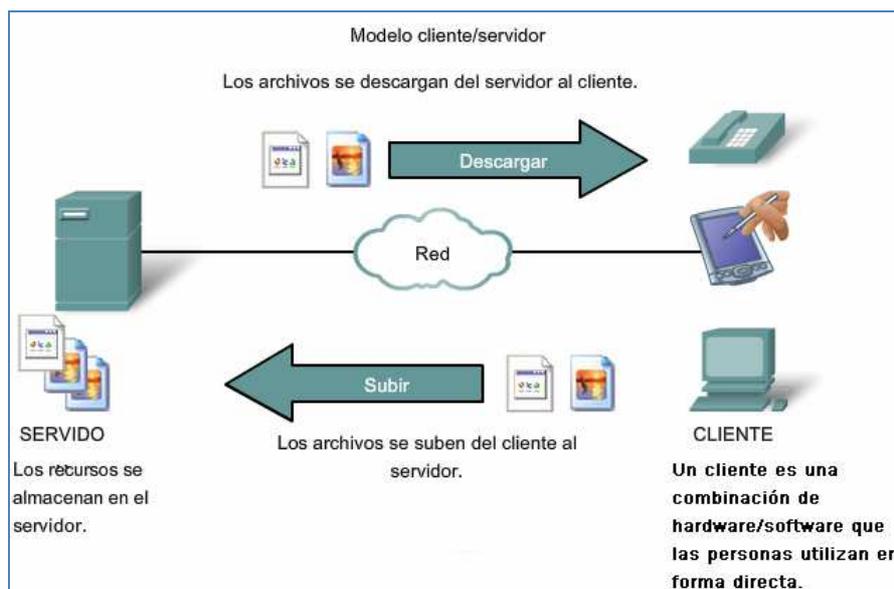


Figura 2.15: Cliente Servidor

Fuente: www.cisco.com: CCNA 1: Aspectos básicos de *networking*

2.6.2.1 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.

2.6.2.2 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). (Stadler, 2008).

CAPITULO III

3 MODELOS DE CAPAS Y PROTOCOLOS DE RED.

Se presenta en este capítulo, la descripción de los protocolos y servicios de red, se da una explicación de los dos modelos de capas básicos para el diseño de redes de datos, recalcando las características de cada uno y las diferencias entre ambos hasta llegar al modelo de red jerárquico, más comúnmente utilizado actualmente para el diseño de redes debido a sus sencilla estructura, sus beneficios y ventajas, facilitando el diseño de cualquier red de datos o convergente.

3.1 MODELOS DE PROTOCOLO Y REFERENCIA

Existen dos tipos básicos de modelos de networking: modelos de protocolo y modelos de referencia.

- **Un modelo de protocolo** proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.
- **Un modelo de referencia** proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red.

El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

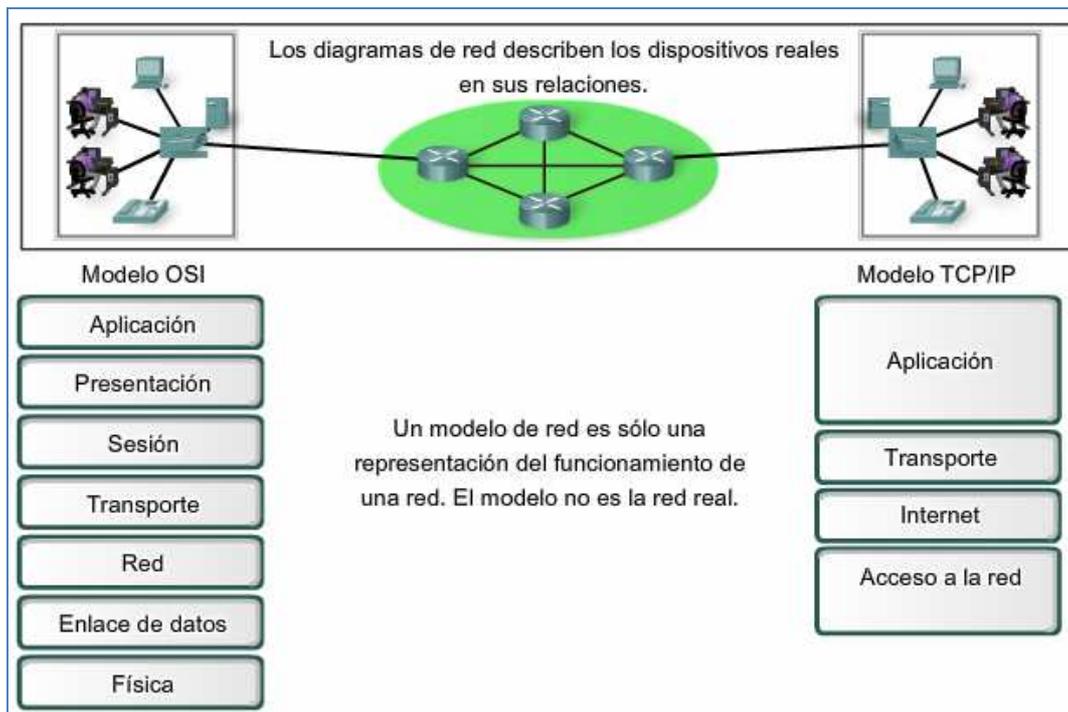


Figura 3.1: Modelo OSI y TCP/IP

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.2

3.1.1 Modelo TCP/IP

Se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo

Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFCS).

Las RFC (Solicitudes de comentarios) también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF). (ACADEMY, 2011)

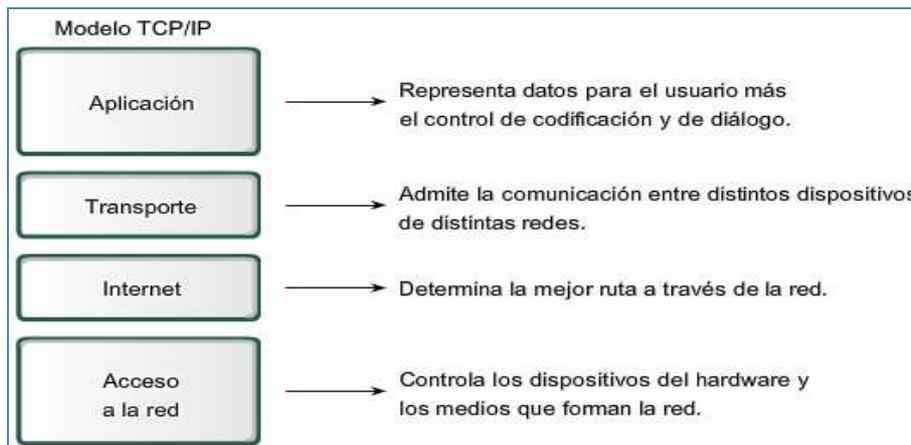


Figura 3.2: Modelo TCP/IP

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.2

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. (Stadler, 2008)

Un proceso completo de comunicación incluye estos pasos:

- Creación de datos a nivel de la capa de aplicación del dispositivo final origen.
- Segmentación y encapsulación de datos cuando pasan por la stack de protocolos en el dispositivo final de origen.
- Generación de los datos sobre el medio en la capa de acceso a la red de la stack
- Transporte de los datos a través de la internetwork, que consiste de los medios y de cualquier dispositivo intermediario.
- Recepción de los datos en la capa de acceso a la red del dispositivo final de destino.
- Desencapsulación y rearmado de los datos cuando pasan por la stack en el dispositivo final.
- Traspaso de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino.

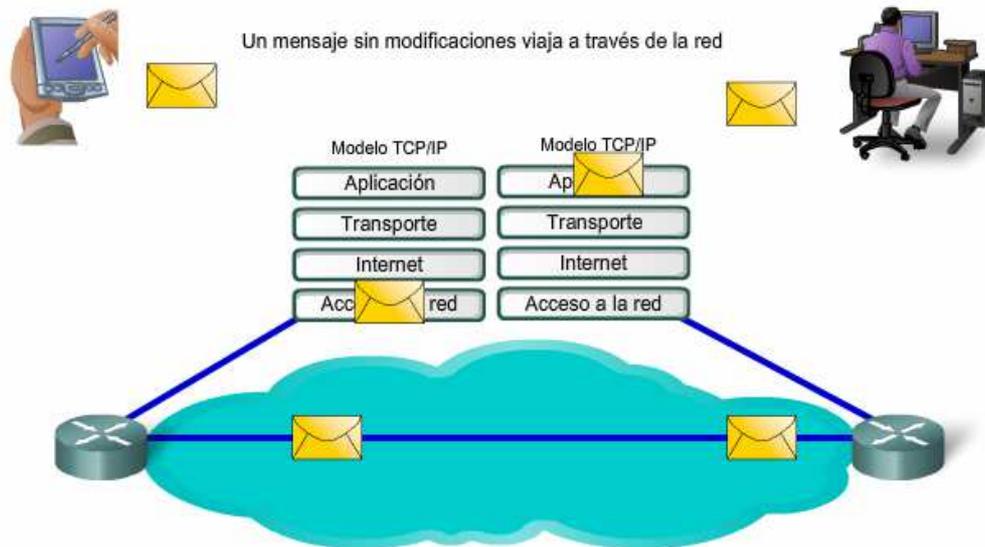


Figura 3.3: Proceso de comunicación.

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.2

3.1.2 Modelo OSI

Inicialmente, el modelo de interconexión de sistemas abiertos (OSI, Open System Inter connection) fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

Lamentablemente, la velocidad a la que fue adoptada la Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas (fig. 3.4) ha realizado aportes importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él.



Figura 3.4: Modelo OSI

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.2

Se describe sintéticamente la función de cada una de las capas del modelo OSI:

- **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.

- **Sesión:** 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 cómo los servicios son implementados realmente. (ACADEMY, 2011)

3.2 COMPARACION ENTRE MODELO OSI Y MODELO TCP/IP

- Los protocolos que forman la suite de protocolos TCP/IP pueden describirse en términos del modelo de referencia OSI.
- En el modelo OSI, la capa Acceso a la red y la capa Aplicación del modelo TCP/IP están subdivididas para describir funciones discretas que deben producirse en estas capas.

- En la capa Acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico.

- Las Capas OSI 1 y 2 analizan los procedimientos necesarios para tener acceso a los medios y los medios físicos para enviar datos por una red.

- La Capa 3 del modelo OSI, la capa Red, se utiliza casi universalmente para analizar y documentar el rango de los procesos que se producen en todas las redes de datos para direccionar y enrutar mensajes a través de una internetwork.

- El Protocolo de Internet (IP) es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la Capa 3.

- La Capa 4, la capa Transporte del modelo OSI, se utiliza para describir servicios o funciones generales que administran conversaciones individuales entre los hosts de origen y de destino.

- En esta capa, los protocolos TCP/IP, Protocolo de control de transmisión (TCP) y Protocolo de datagramas de usuario (UDP) proporcionan la funcionalidad necesaria.

- La capa de aplicación TCP/IP incluye una cantidad de protocolos que proporcionan funcionalidad específica para una variedad de aplicaciones de usuario final.
- Las Capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y programadores de software de aplicación para fabricar productos que necesitan acceder a las redes para establecer comunicaciones, como se observa en la figura 3.5. (Stadler, 2008)

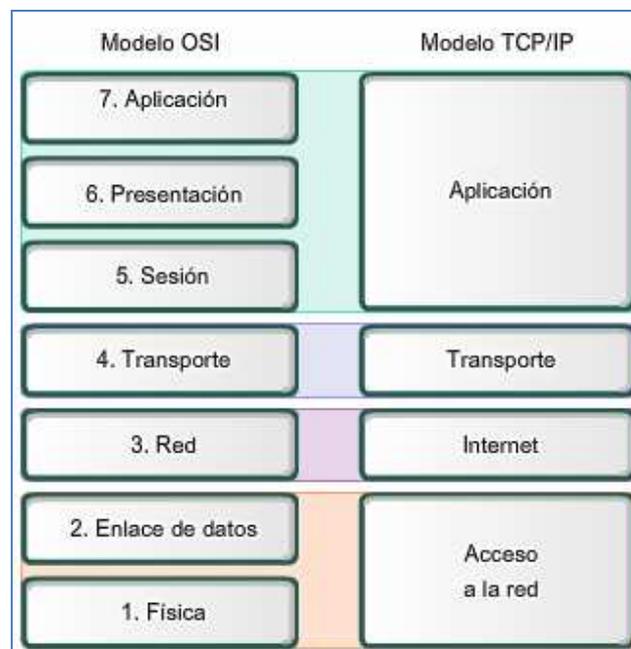


Figura 3.5: Comparación del modelo OSI con el modelo TCP/IP

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.2

3.3 PROTOCOLOS TCP/IP

Los protocolos de capa de aplicación de TCP/IP más conocidos son aquellos que proporcionan intercambio de la información del usuario. Estos protocolos

especifican la información de control y formato necesaria para muchas de las funciones de comunicación de Internet más comunes. Algunos de los protocolos TCP/IP son:

DNS: El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye las consultas sobre formato, las respuestas y los formatos de datos. Las comunicaciones del protocolo DNS utilizan un formato simple llamado mensaje.

HTTP: El protocolo de transferencia de hipertexto uno de los protocolos del grupo TCP/IP, se desarrolló en sus comienzos para publicar y recuperar las páginas HTML, y en la actualidad se utiliza para sistemas de información distribuidos y de colaboración. HTTP se utiliza a través de la World Wide Web para transferencia de datos y es uno de los protocolos de aplicación más utilizados.

HTTP especifica un protocolo de solicitud/respuesta. Cuando un cliente, generalmente un explorador Web, envía un mensaje de solicitud a un servidor, el protocolo HTTP define los tipos de mensajes que el cliente utiliza para solicitar la página Web y envía los tipos de mensajes que el servidor utiliza para responder. Los tres tipos de mensajes más comunes son GET, POST y PUT, como se observa en la figura 3.6.

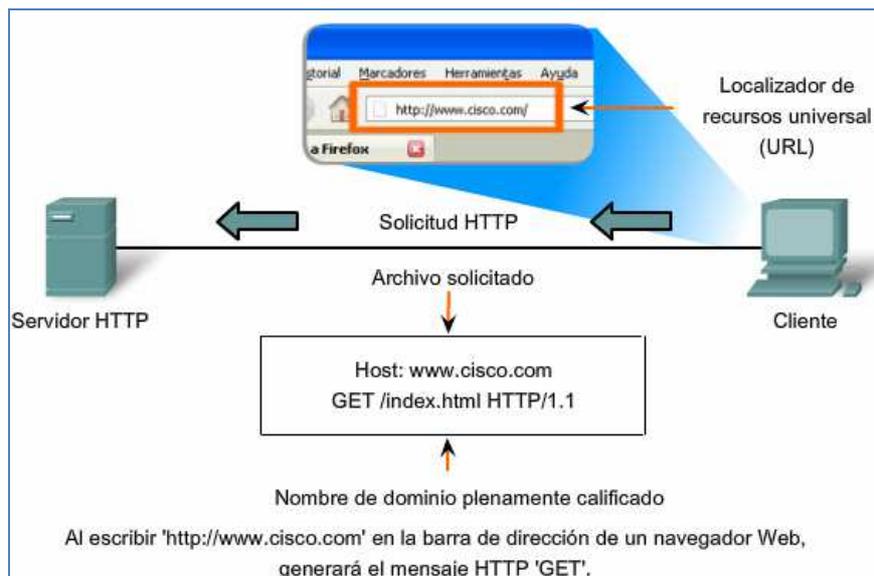


Figura 3.6: Protocolo HTTP mediante GET

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.3

POP y POP3: Protocolo de oficina de correos v.3, son protocolos de envío de correo entrante y protocolos cliente/servidor típicos. Envían e-mails desde el servidor de e-mail al cliente (MUA).

SMTP: El protocolo simple de transferencia de correo, por el contrario, rige la transferencia de e-mails salientes desde el cliente emisor al servidor de e-mail (MDA), como así también el transporte de e-mails entre servidores de e-mail (MTA). SMTP permite transportar e-mails por las redes de datos entre diferentes tipos de software de cliente y servidor, y hace posible el intercambio de e-mails en Internet (Fig.3.7)

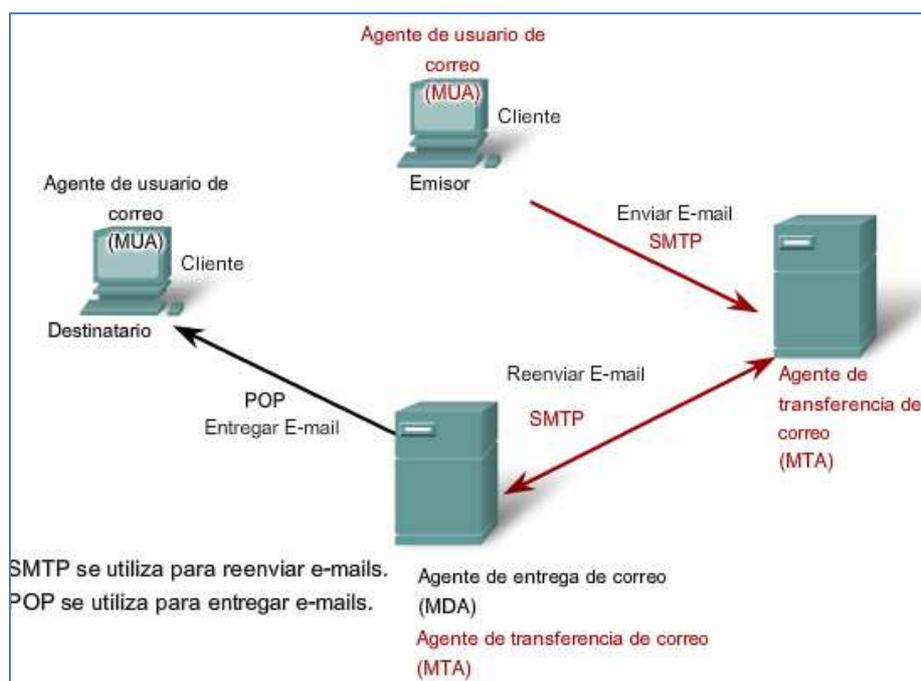


Figura 3.7: Servicios de E-mail – Protocolo SMTP y POP3

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.3

FTP: El protocolo de transferencia de archivos, es otro protocolo de la capa de aplicación comúnmente utilizado. El FTP se desarrolló para permitir las transferencias de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora y se utiliza para cargar y descargar archivos desde un servidor.

Para transferir los archivos en forma exitosa, el FTP requiere de dos conexiones entre cliente y servidor: una para comandos y respuestas, otra para la transferencia real de archivos.

El cliente establece la primera conexión con el servidor en TCP puerto 21. Esta conexión se utiliza para controlar el tráfico, que consiste en comandos del cliente y respuestas del servidor.

El cliente establece la segunda conexión con el servidor en TCP puerto 20. Esta conexión es para la transferencia real de archivos y se crea cada vez que se transfiere un archivo (Fig.3.8).

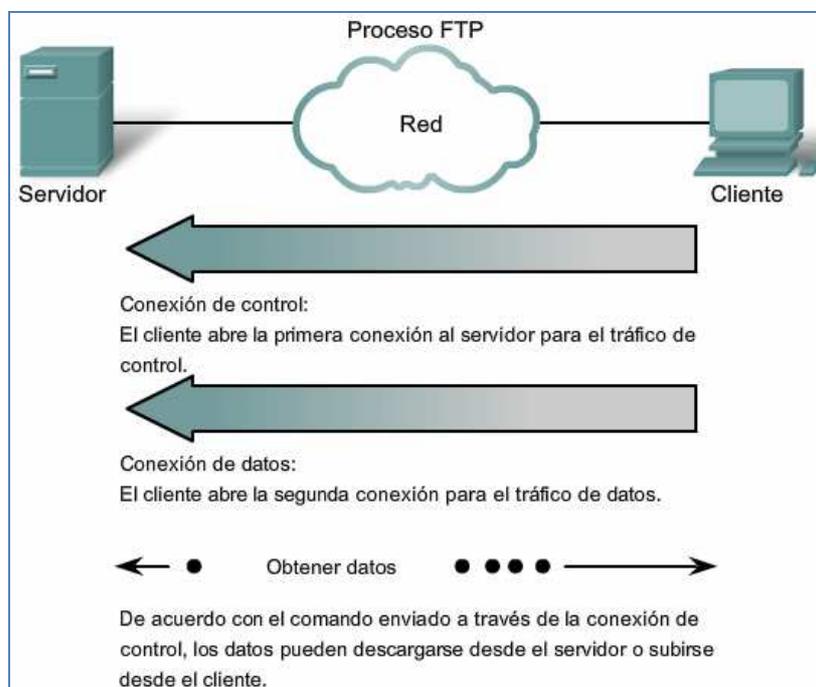


Figura 3.8: Proceso FTP

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.3

DHCP: El Protocolo de configuración dinámica de host permite a los dispositivos de una red obtener direcciones IP y demás información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, gateways y otros parámetros de redes IP.

DHCP permite a un host obtener una dirección IP en forma dinámica cuando se conecta a la red.

SMB: El Bloque de mensajes del servidor es un protocolo cliente-servidor para compartir archivos.

El protocolo SMB describe el acceso al sistema de archivos y la manera en que los clientes hacen solicitudes de archivos. Además describe la comunicación entre procesos del protocolo SMB. Todos los mensajes SMB comparten un mismo formato. Este formato utiliza un encabezado de tamaño fijo seguido por un parámetro de tamaño variable y un componente de datos.

Los mensajes SMB pueden:

- Iniciar, autenticar y terminar sesiones
- Controlar el acceso a archivos e impresoras
- Permitir a una aplicación enviar o recibir mensajes hacia o desde otro dispositivo.

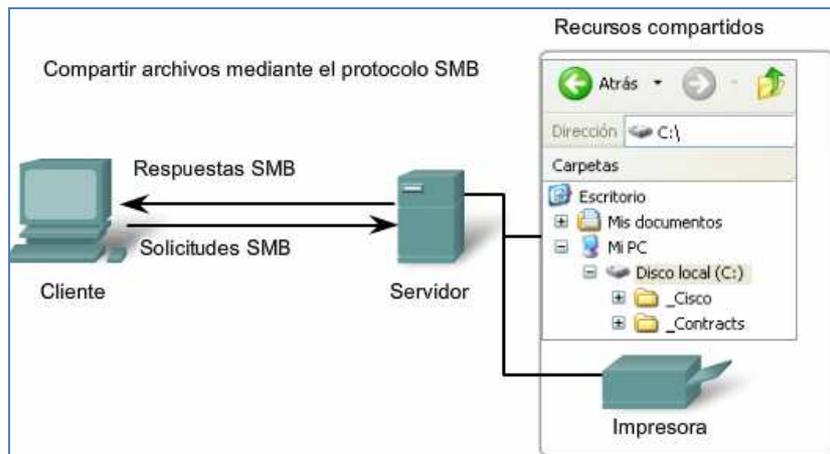


Figura 3.9: Compartir archivos mediante protocolo SMB

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.3

Telnet: Es un protocolo cliente-servidor y especifica cómo se establece y se termina una sesión VTY. Además proporciona la sintaxis y el orden de los comandos utilizados para iniciar la sesión Telnet, como así también los comandos de control que pueden ejecutarse durante una sesión. Cada comando Telnet consiste en por lo menos dos bytes. (ACADEMY, 2011)



Figura 3.10: Proceso Telnet

Fuente: www.cisco.com: CCNA 1: Aspectos Básicos de Networking/Cap.3

3.4 SERVICIOS E INTERFACES

➤ **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.

3.5 TIPOS DE SERVICIO

➤ **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.

3.6 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

3.7 ESTANDARIZACIÓN

A continuación se detalla brevemente los tipos de estandarizaciones.

- 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 Architecture Board
 - ✓ IRTF
- ❖ Internet Research Board
 - ✓ IETF: Internet Engineering Task Force, que dirige el proceso de creación de estándares
- RFC: Request For Comment

Ventajas:

- 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.

Desventajas:

- Los organismos de estandarización son muy lentos (3 o 4 años aproximados para declarar un estándar).
- Quien compone los organismos de estandarización (empresas: interés por no dejarse aventajar por la competencia; política: comunicación de los votos, universidades)

Ejemplo:

Ethernet! IEEE 802.3

- Demasiados organismos de estandarización. (Stadler, 2008)

CAPITULO IV

4 SOFTWARE SIMULADOR *PACKET TRACER*

Se presenta en este capítulo, de manera minuciosa en qué consiste el software simulador de redes *Packet Tracer*, sus características, beneficios tanto para los estudiantes como para los docentes y se explica de manera gráfica su utilidad y fácil manejo, detallando la función de cada uno de sus componentes, convirtiéndose en un práctico manual.

4.1 DEFINICION

Packet Tracer es una herramienta de aprendizaje y simulación de redes interactiva, que permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. *Packet Tracer* se enfoca en apoyar mejor los protocolos de redes.

Ofrece una combinación única de experiencias realistas de simulación, visualización, evaluación compleja, capacidades de la actividad de creación y oportunidades de colaboración multiusuario. (Cisco Packet Tracer)

Packet Tracer tiene una amplia gama de lenguajes, los cuales pueden ser adquiridos. Todo esto representa una mayor comodidad en la representación textual, con un formato adecuado a cada país.

4.2 UTILIDAD DEL *PACKET TRACER*

El Simulador *Packet Tracer* es una herramienta muy útil, porque permite implementar y observar claramente el funcionamiento de las redes sin 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 es decir con su hardware correspondiente sin obtener ningún inconveniente al momento de conectarlos e instalarlos. (Salazar)

Esta herramienta tiene la capacidad de configuración de routers a nivel de comandos, que implementa IOS, el sistema de CISCO, como la configuración mediante botones y habilitaciones de cuadros de selección. Todo esto es para las configuraciones de diferentes routers. En el caso de dispositivos finales, como las PC's no cuenta más que con el uso de comandos como PING, para realizar

pruebas de envío de paquetes entre computadoras. La configuración de una PC es a nivel de llenado de cuadros de texto con la información necesaria.

4.3 PROPÓSITO

Este software tiene el propósito de ser usado como un simulador educativo que brinda exposición a la interfaz comando – línea de los dispositivos de Cisco para practicar y aprender por descubrimiento.

Existen varias actualizaciones, *Packet Tracer 5.3.0* es la última versión del simulador de redes de *Cisco Systems*.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego realizando un doble click en ellos se puede ingresar a sus consolas de configuración. Una vez completada la configuración física y lógica de la red, también se puede hacer simulaciones de conectividad (*pings, traceroutes, etc.*) todo ello desde la misma consola incluida. (Anonimo2, 2009)

4.3.1 Simulador *Packet Tracer* basado en el aprendizaje

Las características innovadoras ayudan a los estudiantes y docentes a resolver problemas y aprender conceptos en un entorno social atractivo y dinámico.

Permite a los docentes enseñar y demostrar fácilmente complejos conceptos técnicos y el diseño de sistemas de redes simples y extensas. También ayuda a los estudiantes a desarrollar importantes habilidades del siglo 21.

4.4 CONTENIDO

A continuación se detallan los elementos que contiene el software *Packet Tracer*.

4.4.1 Elementos

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.

4.4.2 Principales funcionalidades

Entre las principales características del *Packet Tracer* se encuentran las siguientes:

- Soporte para Windows (2000, XP, Vista) y Linux (Ubuntu y Fedora).
- Permite configuraciones multiusuario y colaborativas en tiempo real.
- Soporte para IPv6, OSPF multiárea, redistribución de rutas, RSTP, SSH y *Switches* multicapa.
- Áreas de trabajos lógicos y físicos.

- El tiempo real y simulación de los modos.
- Comando de usuario amigable interfaz de línea de comandos (CLI).
- Lista de eventos globales (analizador de paquetes).
- LAN, conmutación, TCP / IP, ruteo y protocolos WAN.
- Soporte de plataformas múltiples.
- Soporte para múltiples idiomas.
- Ayuda integrada y Tutoriales.

4.4.3 Protocolos

El software *Packet Tracer* soporta los siguientes protocolos:

- HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP y DNS.
- TCP/UDP, IPv4, IPv6, ICMPv4 e ICMPv6.
- RIP, EIGRP, OSPF Multiárea, enrutamiento estático y redistribución de rutas.
- Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP.
- ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP. (Cisco Packet Tracer)

4.5 ACTIVIDADES DENTRO DE *PACKET TRACER*

El *Packet Tracer* permite realizar las siguientes actividades:

- Simulación
 - Visualización
 - Colaboración (Cisco Packet Tracer)
- **Simulación de comandos IOS(Sistema Operativo de Cisco)**

En la figura 4.1 se presenta la simulación de algunos comandos del IOS de Cisco ejecutados en el CLI (Interfaz de Línea de Comandos) del *Paket Tracer*.

```
R1
Physical Config CLI
IOS Command Line Interface

User Access Verification

Password:
Password:
Password:

Router1>ena
Password:

Router1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      192.168.7.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.7.0/25 is directly connected, FastEthernet0/0
C      192.168.7.128/26 is directly connected, FastEthernet0/1
Router1#
```

Figura 4.1: Simulador Comandos IOS.

Fuente: Manual CISCO, www.cisco.com

➤ Visualización del tráfico de paquetes en las Redes

En la figura 4.2 se presenta el diseño de una red con 3 enlaces WAN y 3 redes LAN, en la cual mediante la simulación en tiempo real que *Packet Tracer* permite, se observa el tráfico de la red, como fluctúan los paquetes de información transmitidos entre usuarios de las redes LAN.



Figura 4.2: Tráfico de Redes.

Fuente: CCNA 1: Conceptos básicos sobre *networking*

➤ **Colaboración en actividades de múltiples redes**

En la figura 4.3 se presenta como interactúan múltiples usuarios de múltiples redes mediante la simulación en tiempo real.

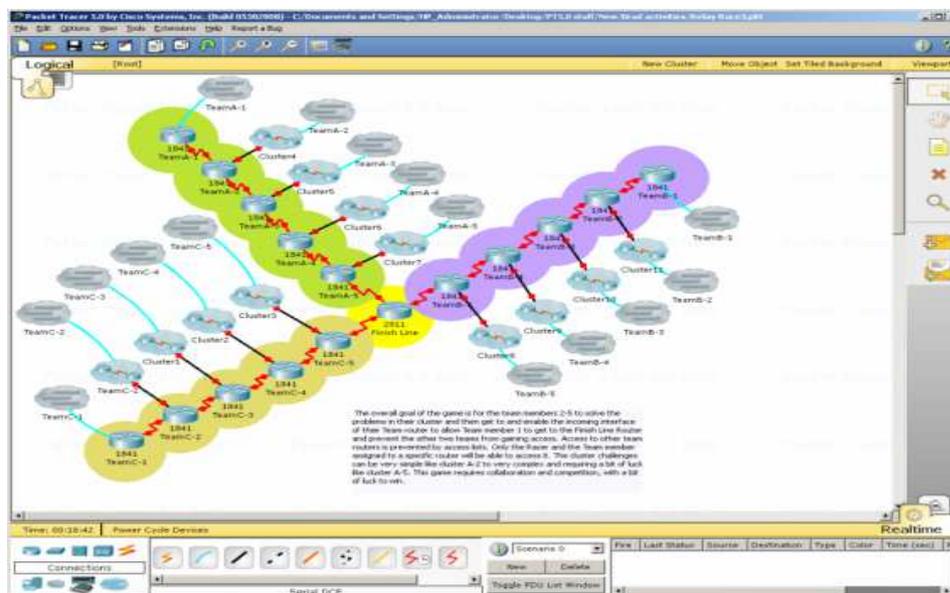


Figura 4.3: Actividades Multi-redes

Fuente: CCNA 1: Conceptos básicos de *networking*.

4.6 Beneficios de la Simulación Basada en el Aprendizaje

Los estudiantes que exploran y experimentan con el simulador *Packet Tracer* desarrollan la curiosidad intelectual y el pensamiento crítico. *Packet Tracer* es de gran riqueza visual, en el entorno de simulación facilita la comprensión de los conceptos de tecnología compleja.

Los estudiantes que solucionan problemas de redes con *Packet Tracer* desarrollan habilidades para resolver problemas. Los estudiantes que diseñan y construyen redes virtuales utilizando *Packet Tracer* mejoran sus habilidades de innovación y creatividad.

El uso de este software hace que la tecnología de enseñanza y aprendizaje en red sea más fácil. No pretende sustituir las experiencias con equipos reales, sino más bien complementarlas.

4.6.1 Beneficios *Packet Tracer*

El software *Packet Tracer* hace que la enseñanza sea más fácil proporcionando un entorno libre y multi-usuario para que los docentes puedan enseñar fácilmente conceptos técnicos complejos.

Facilita el aprendizaje al proporcionar una simulación realista y visualización del entorno para la exploración, la experimentación y la explicación. Profesores y estudiantes pueden crear sus propias redes virtuales "red mundos" para la enseñanza y el aprendizaje de conceptos de redes y tecnologías.

4.6.1.1 Beneficios Claves para el Docente

Entre algunos beneficios que proporciona el uso de este software para los docentes, se tiene los siguientes:

- Capacidad para enseñar conceptos complejos de redes.
- La demostración de tecnologías y configuraciones.
- Se utiliza para conferencias de demostración, individual y grupo de laboratorios, tareas, evaluaciones, juegos, diseño de redes, las tareas de resolución de problemas y el modelado, el reforzamiento de las actividades prácticas de laboratorio, estudios de casos.
- Equipo de suplementos en el aula y proporciona oportunidades de aprendizaje complementarias que no son posibles en el aula solo.
- Apoya procesos de aprendizaje social a través de la colaboración y la competencia multiusuario.

4.6.1.2 Beneficios para Estudiantes

Entre algunos beneficios que brinda el uso de este software a los estudiantes, se tiene:

- Proporciona una práctica libre y entorno de visualización para el diseño, configuración y solución de problemas de entornos de red.
- Observa los paquetes virtuales en tiempo real a medida que viajan a través de su red.
- Permite la práctica fuera del aula y el laboratorio (ordenadores personales, ordenadores portátiles).
- Crear y configurar mucho más grande que las topologías posibles con el equipo físico disponible.
- Proporciona un rico entorno de aprendizaje más allá de las prácticas estándar de tecnología de redes de instrucción.
- Proporciona una valiosa experiencia práctica para ayudar a tener éxito en el aula y en el trabajo. (Cisco Packet Tracer)

4.7 PROGRAMA DE SIMULACION *PACKET TRACER*

A continuación se describe detalladamente cómo funciona el simulador *Packet Tracer*.

4.7.1 Descripción General de las opciones gráficas y barras.

En esta primera fase se presentará de forma detallada la función que cumple cada opción gráfica y cada ítem descrito en las barras de herramienta y menú de *Packet Tracer*, para poder brindar al lector una visión fácil de utilización del software.

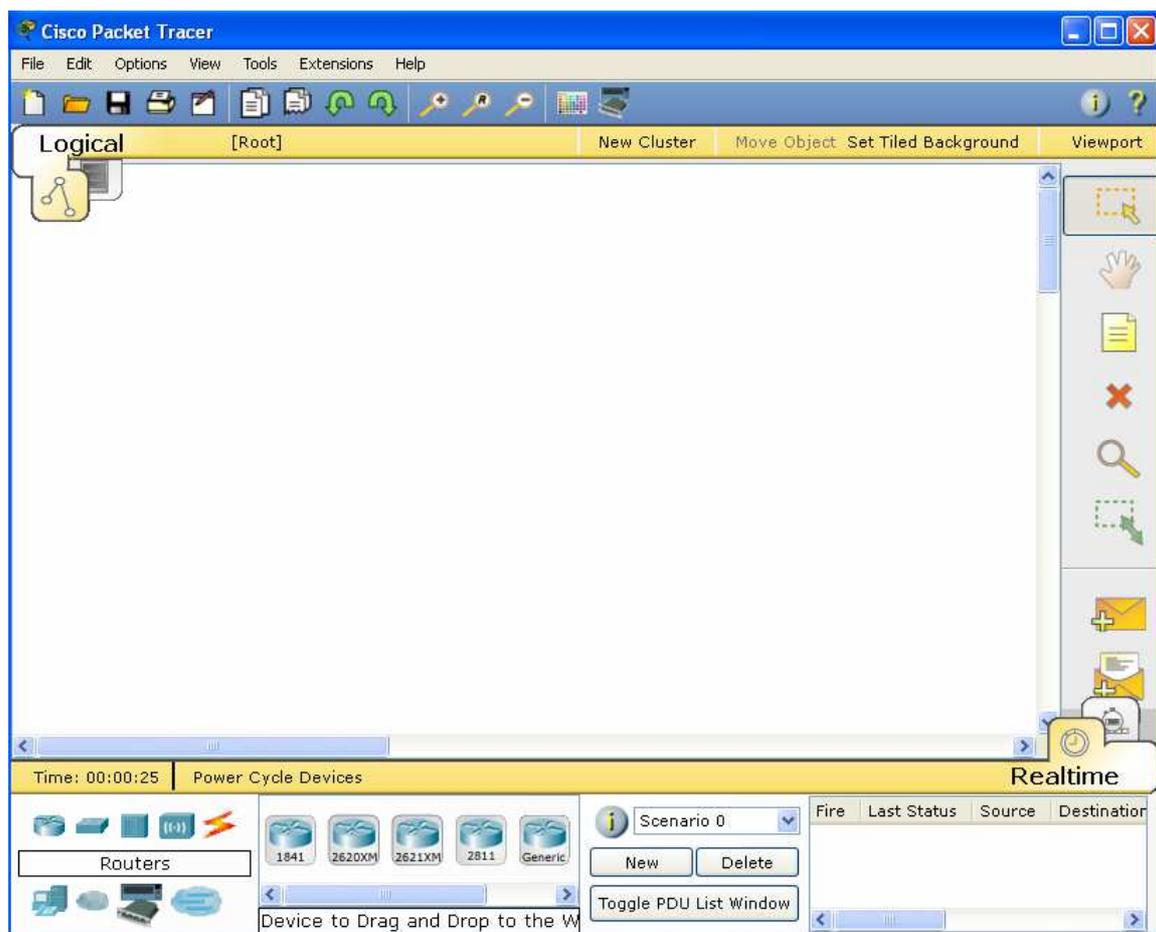


Figura 4.4: Simulador *Packet Tracer*

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Esta como otras herramientas dispone de sus menús principales, entre los cuales están FILE,OPTIONS,TOOLS y HELP, además de contar con una barra de uso rápido que contiene las opciones de nuevo escenario (NEW), abrir un escenario (OPEN), guardar cambios en un escenario (SAVE), imprimir un escenario (PRINT) y un asistente de actividades (ACTIVITY WIZARD).

En el menú FILE, se encuentran las opciones descritas en la barra de uso rápido, con la única diferencia que se encuentra la opción de guardar como (SAVE AS).

En el menú OPTIONS, se encuentra la opción PREFERENCES, que maneja la personalización de la herramienta, *Packet Tracer*.

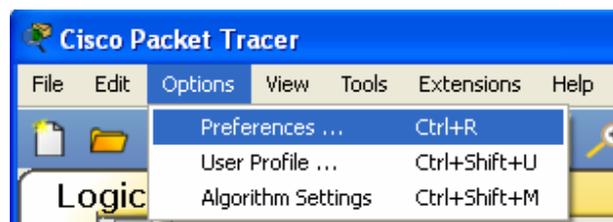


Figura 4.5: Barra Principal

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Al seleccionar esta opción se despliega un cuadro de diálogo, en el cual dispone de dos pestañas, una de las cuales tiene el título INTERFACE en donde se puede habilitar o deshabilitar las opciones de Animación, Sonido y Etiquetas. Además de la seleccionar el idioma que dispone la herramienta.

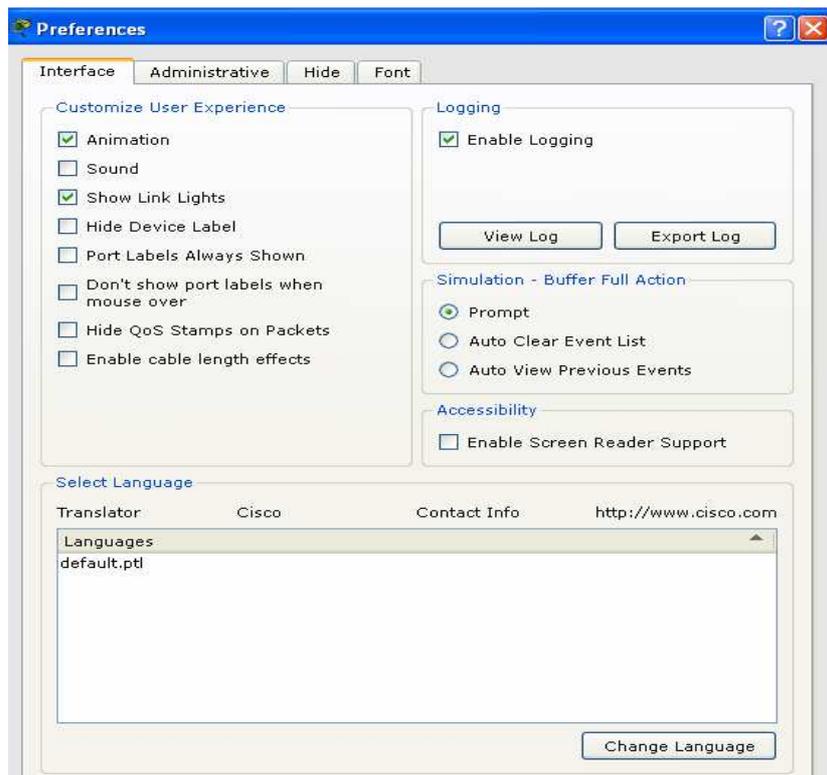


Figura 4.6: Opción Preferences

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

La otra, con el título ADMINISTRATIVE provee opciones adicionales de administración. Entre las cuales dispone de un password y su confirmación para futuros accesos a la herramienta. Al igual que la habilitación y deshabilitación del password. Dispone además de la opción de agregar o remover distintos fondos.

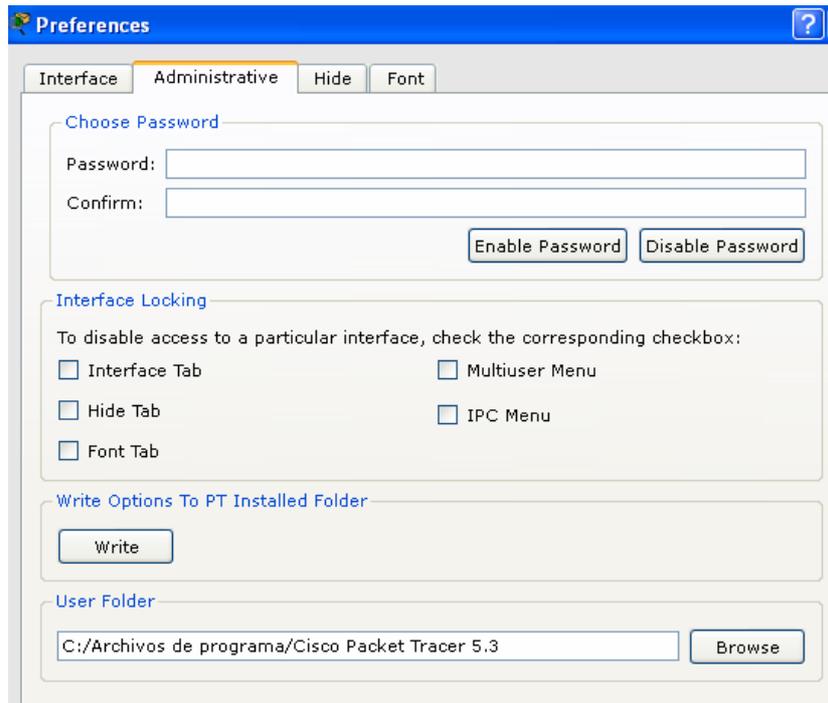


Figura 4.7: Opciones de Administración.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Una forma esencial de agregar información relativa a la red que construimos, está disponible en el cuadro de información, en la parte derecha de la barra de acceso rápido.

El círculo color rojo muestra la ubicación del botón que activa esta opción de agregar una descripción.

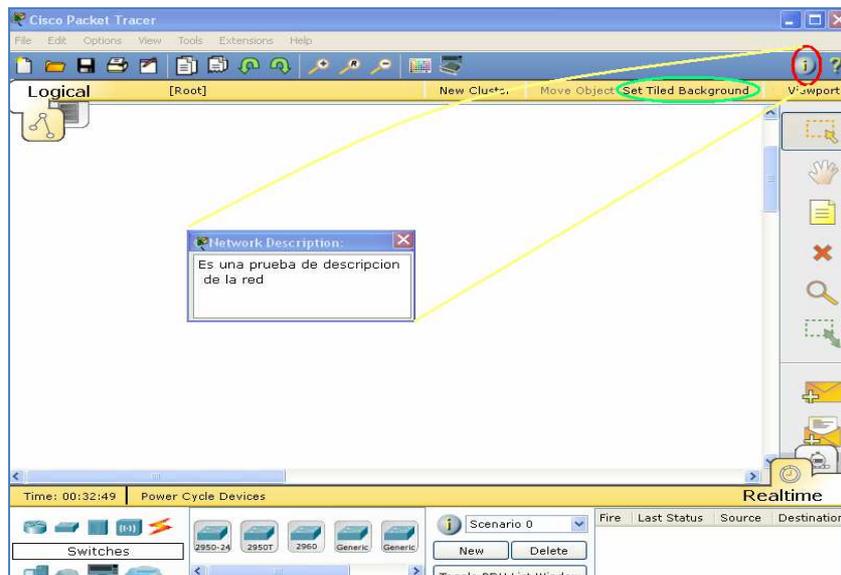


Figura 4.8: Proceso para agregar una descripción en *Packet Tracer*

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

La opción de Set Tiled Background, seleccionada en el óvalo color verde, permite agregar un fondo, sea cualquier imagen cargada desde el menú options preferences. Se despliega un cuadro de dialogo, en el cual seleccionamos la imagen, con el botón apply, se coloca como fondo, y con el botón reset, se limpia el área de trabajo.

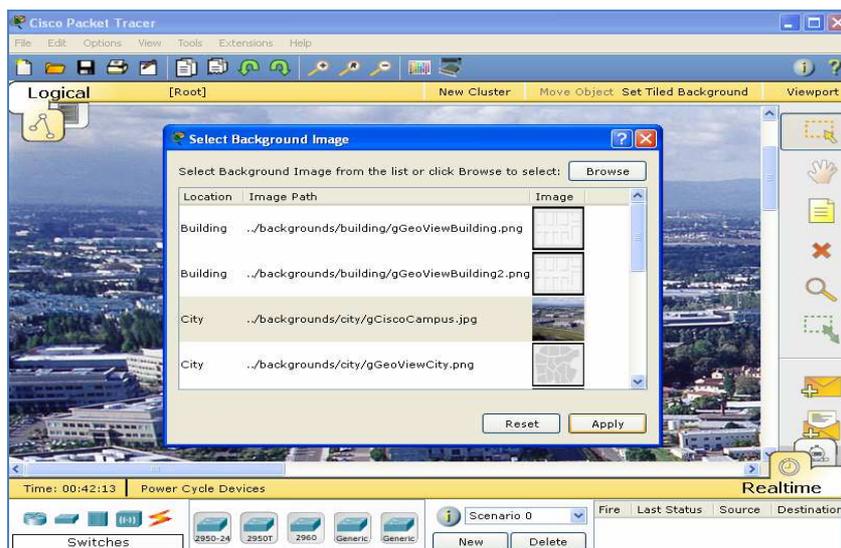
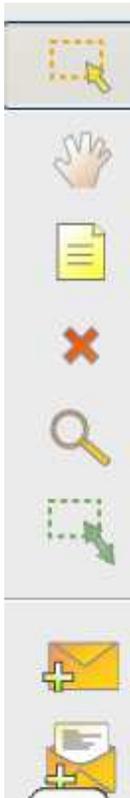


Figura 4.9: Proceso para agregar un fondo en *Packet Tracer*

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

La barra de acceso común provee herramientas para la manipulación de los dispositivos, las cuales se detallan a continuación.

El orden de descripción es el mismo orden en que aparecen los iconos de la barra.



1. Selección de dispositivos y conexiones, no selecciona conexiones wireless.
2. Movimiento de Rejilla, moviliza los dispositivos alrededor del área de trabajo.
3. Notas, permite agregar notas que enriquecen de conocimiento, del área de trabajo.
4. Eliminar, permite eliminar cualquier dispositivo, conexión (excepto wireless) y notas.
5. Inspector, permite visualizar la tabla correspondiente al dispositivo
6. seleccionado, entre ellas ARP, MAC y ROUTER.
7. Mensaje Simple UDP, permite crear paquete del tipo ICMP entre dispositivos.
8. Mensaje Complejos UDP, permite crear paquetes personalizados entre dispositivos.

En la parte inferior izquierda, aparecen una serie de dispositivos que pueden ser agregados.

Por ejemplo, se selecciona el router, a la par aparece una serie de routers, entre ellos destacan los específicos de CISCO y un genérico. En el caso de los hubs, solo se dispone de genéricos.

Las conexiones tienen todas las conocidas, desde automáticas, que detectan el tipo correcto entre dispositivos, hasta punto a punto (Cooper Straight - through), cruzadas (Cooper Cross - over), consola (console), fibra óptica (fiber), teléfono (telephone), Serial DCE y Serial DTE.

Entre los últimos por mencionar tenemos a los dispositivos que van conectados entre sí, es decir pc's, servidores, impresoras, siendo genéricas todas estas.

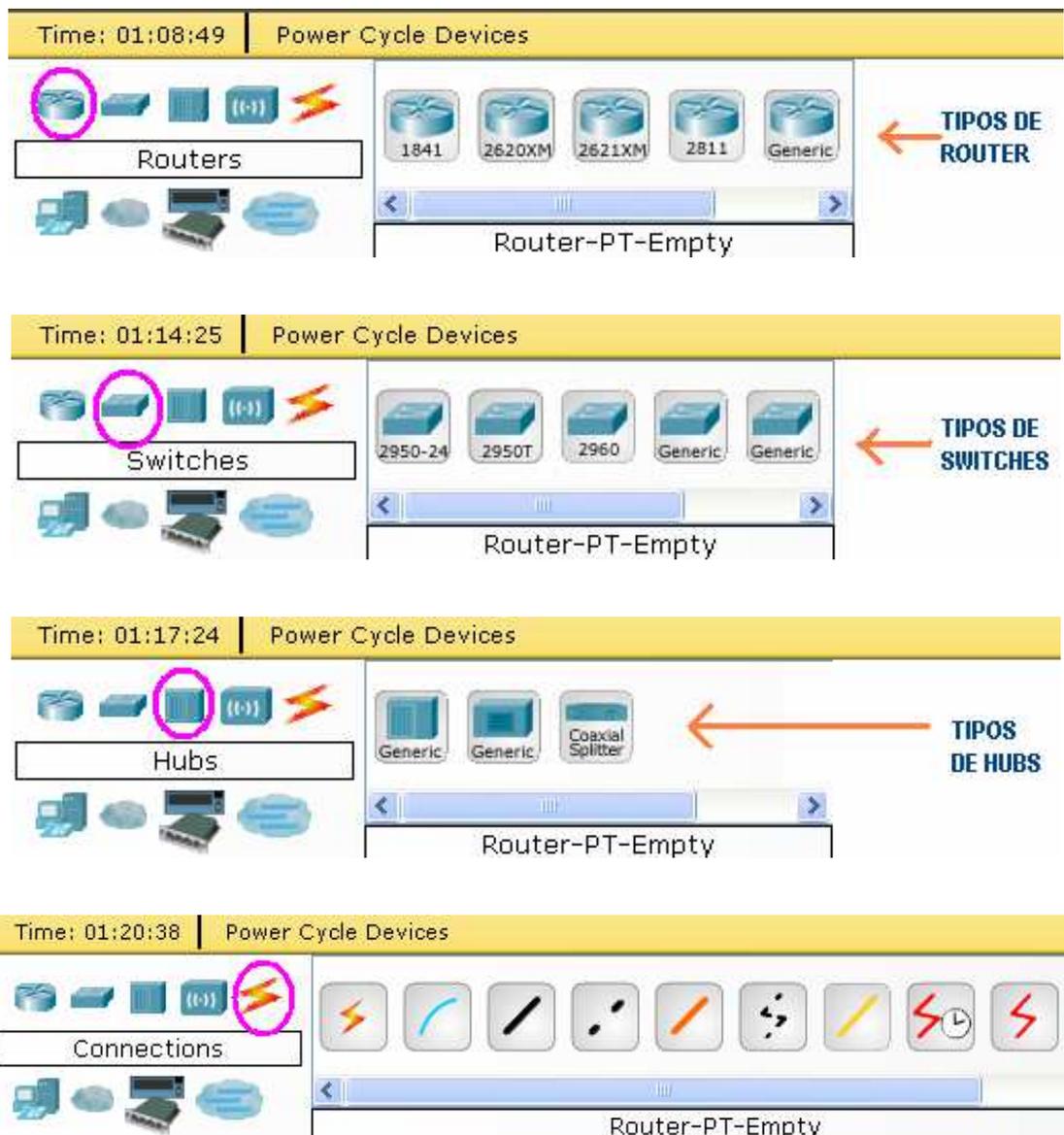


Figura 4.10: Visualización de los dispositivos y tipos de conexiones.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Por último, al seleccionar algún tipo de dispositivo, el nombre del dispositivo aparece en la parte inferior central, por ejemplo, en la figura anterior, se ha seleccionado Dispositivos Finales (End Devices), y el cursor está sobre la figura de la pc, es ese momento que aparece como nombre del dispositivo "PC-PT".

Hay dos modos en las redes concretadas, en el **modo real**, en donde se crean las configuraciones y se dispone la posición de los dispositivos; y el **modo simulación** en el cual se pone a andar la o las redes armadas.

Se puede cambiar entre los diferentes modos, esto está en la parte inferior derecha. El modo real (Realtime) es representado por un reloj, y el modo simulación (Simulation) es representado con un cronometro.

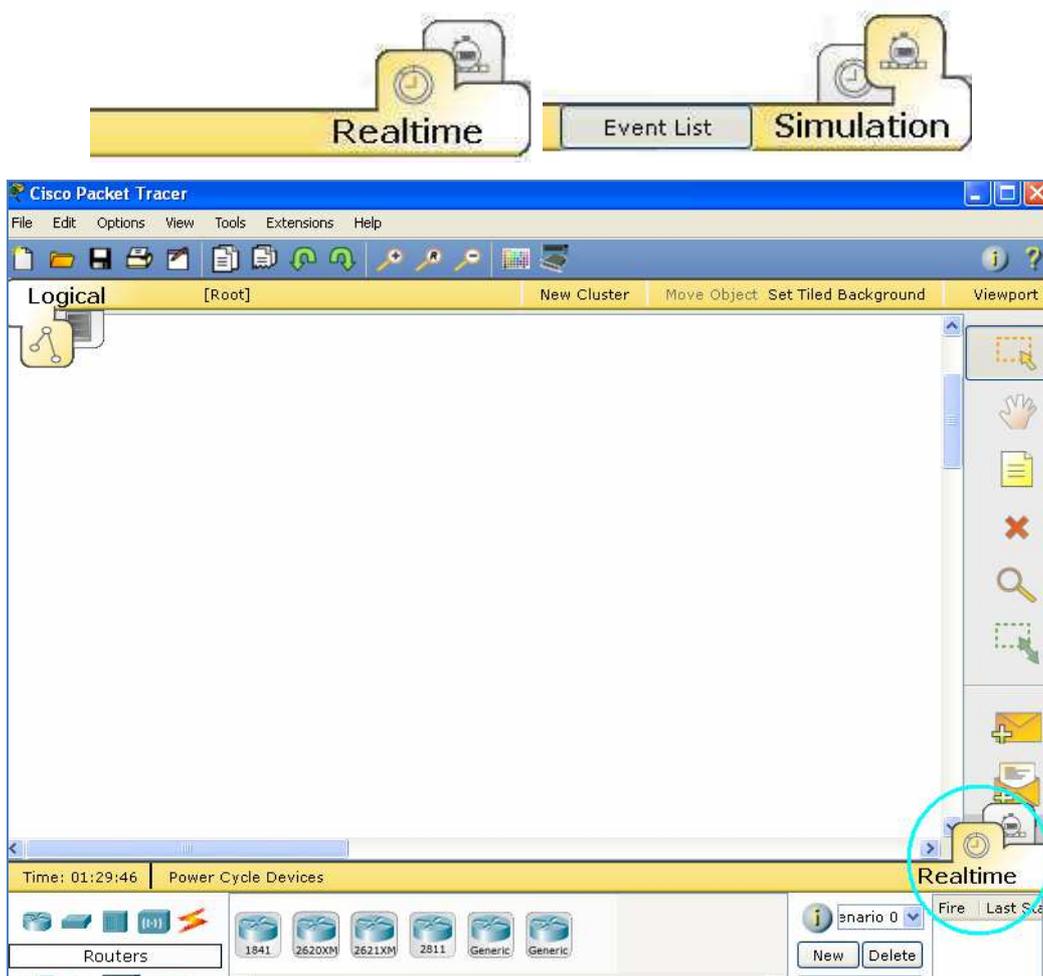


Figura 4.11: Modos Realtime y Simulation

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Existen dos vistas, la lógica y la física. En la vista lógica se agregan todos los dispositivos, y en la vista física la disposición de las redes, una vista de ciudad,

departamento y oficina. Estas pueden ser alternadas por las opciones que aparecen en la barra. Estas vistas pueden ser cambiadas en la barra que aparece en la parte de debajo de la barra de acceso rápido.

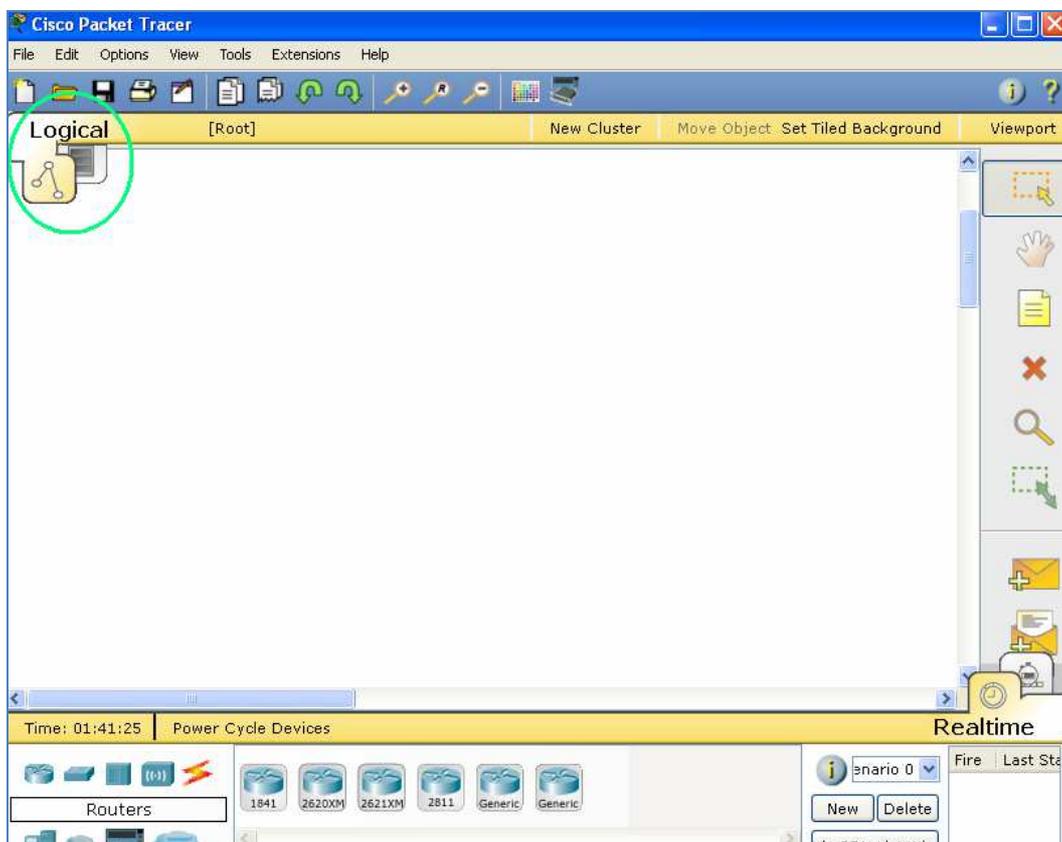
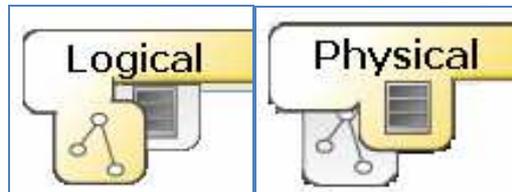


Figura 4.12: Visualización Lógica y Física

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

4.7.2 Colocación de Dispositivos.

Como se menciona anteriormente, para poder agregar un dispositivo, tal como un router, switch, computadora, etc.; es necesario únicamente dar un clic simple

sobre el dispositivo que deseamos y colocar en el área de trabajo. Notaremos que al dar un clic sobre el dispositivo el curso cambia de una flecha a un signo más. Si deseamos colocar más de un dispositivo del mismo tipo, la tarea puede volverse tediosa, pero para ello únicamente debe presionar la tecla CTRL antes de seleccionar el dispositivo, notara que ahora el cursor permanece con el signo más, después de agregar el primer dispositivo. En ese momento podrá agregar cuantos dispositivos desee, del mismo que selecciono. Para terminar pulse la tecla ESC, o bien dando un clic sobre el botón del dispositivo que selecciono. El botón debe estar de la siguiente forma con una diagonal invertida de fondo . La siguiente ilustración muestra como agregar un router, de forma individual y en forma conjunta.

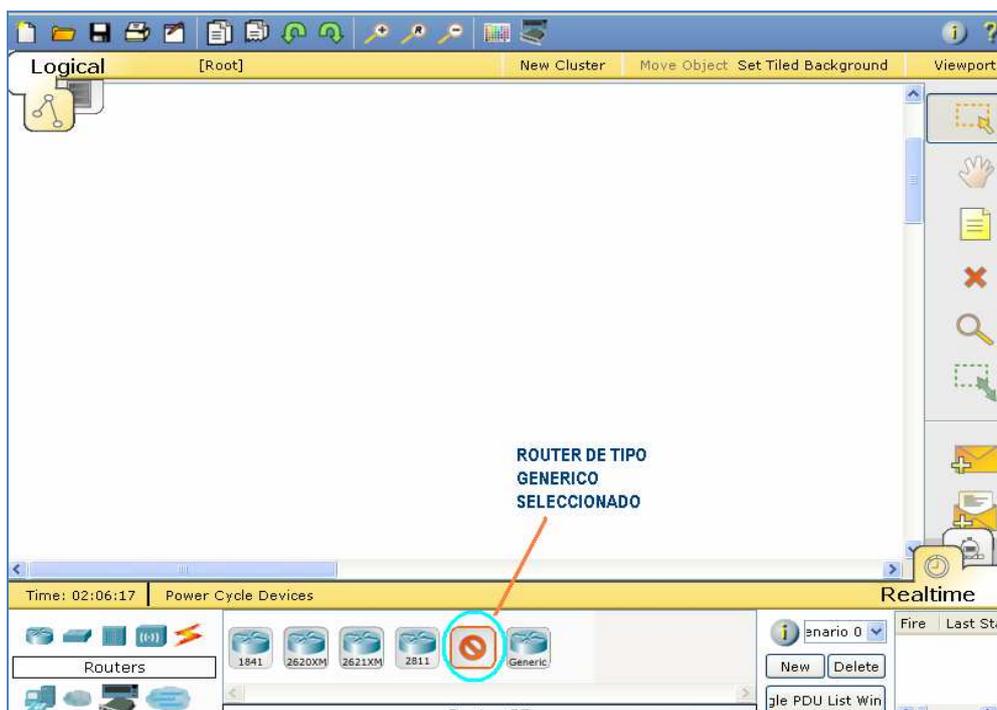


Figura 4.13: Selección del dispositivo (router genérico)

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Después de agregar el primer router genérico, el cursor cambia a una flecha y el botón seleccionado se coloca con la figura del router. Esto se muestra en la siguiente ilustración.

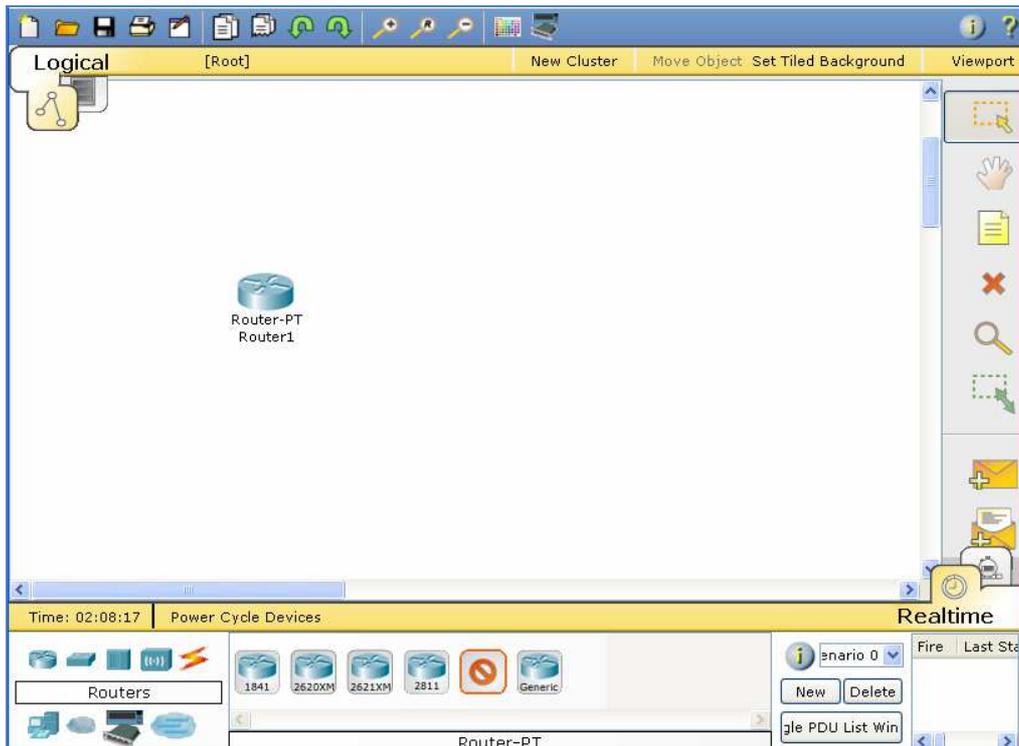


Figura 4.14: Dispositivo colocado en el espacio de diseño.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para eliminar cualquier dispositivo, es necesario seleccionarlo y luego dirigirnos a la barra común, dar un clic en el botón identificado con una equis.

Nota: La barra común se encuentra en la parte derecha central de la ventana.

Otra forma de eliminar algún dispositivo es oprimiendo la tecla DEL, el cursor tendrá el aspecto del signo más, y luego podrá seleccionar el dispositivo que desee. También puede seleccionar un grupo de dispositivos, y repetir cualquier de los dos pasos mencionados anteriormente.

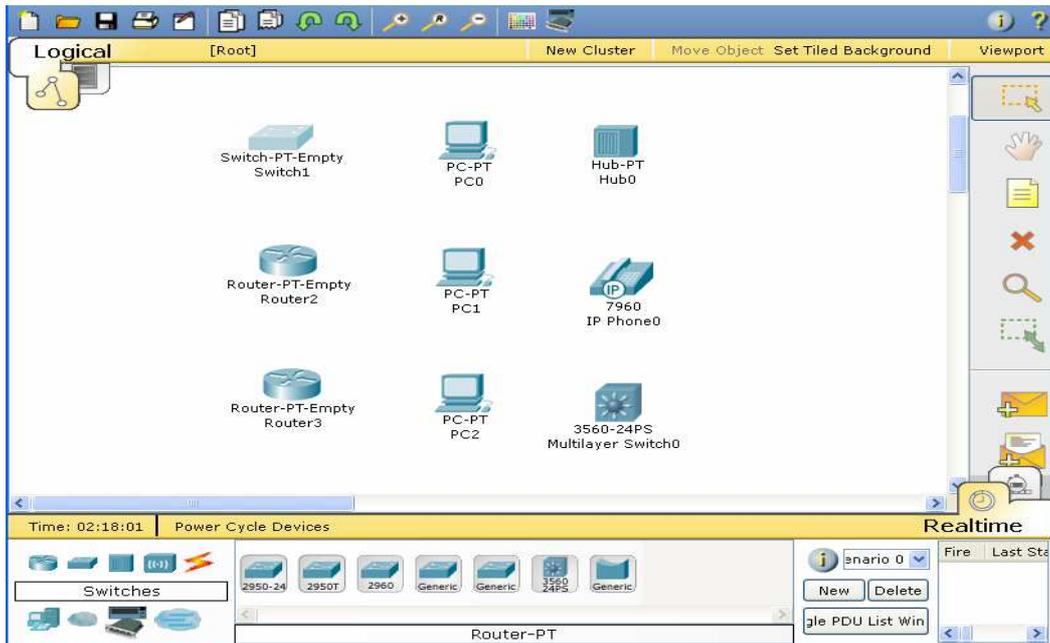


Figura 4.15: Grupo de dispositivos agregados.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Se desea eliminar el dispositivo Hub0. Solamente aceptar la confirmación.



Figura 4.16: Proceso para eliminar un dispositivo.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Si la topología de la red es demasiado grande, la herramienta será útil para mover grandes distancias. Se encuentra en la barra común de herramientas. Para utilizar coloque el curso de la manita en el área de trabajo, de un clic, y sin soltar arrástrelo, verá que la maquina se torna en forma empuñada.

Una forma de agregar información sustancial a las redes, es la herramienta notas, que se encuentra en la barra común de herramientas.

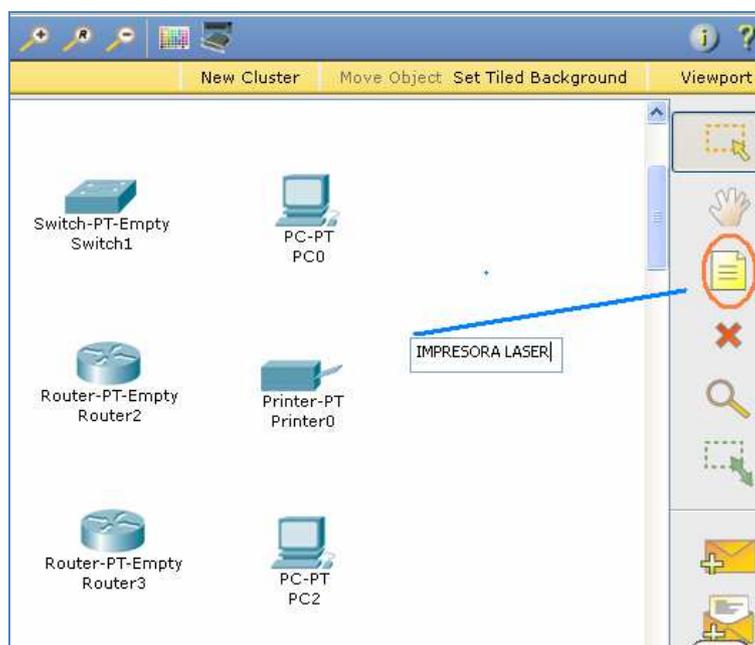


Figura 4.17: Descripción para agregar información a la red.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Otra herramienta útil, es el inspector que sirve para visualizar las tablas ARP, MAC y ROUTING de cada uno de los dispositivos utilizados. De un clic sobre esta herramienta situada en la barra de herramientas comunes, en la parte central derecha de la ventana, y el cursor tendrá la apariencia de una lupa, entonces seleccione con un clic simple el dispositivo y se le preguntara por el tipo de tabla, debe seleccionar la que necesite, y entonces se desplegara un cuadro de texto con la información de la tabla.

Otra forma de obtener información acerca de routers, por ejemplo es situar el cursor sobre el dispositivo y esperar a que se despliegue la información, claro que al mover el cursor la información desaparecerá. Recuerde que para que muestre esta información de manera temporal se debe estar en el modo selección de dispositivos, botón que se encuentra en la barra de herramientas comunes, situada en la parte central derecha. La flecha que aparece en la imagen no aparecer en la herramienta, es únicamente para indicar de qué router hemos seleccionado.

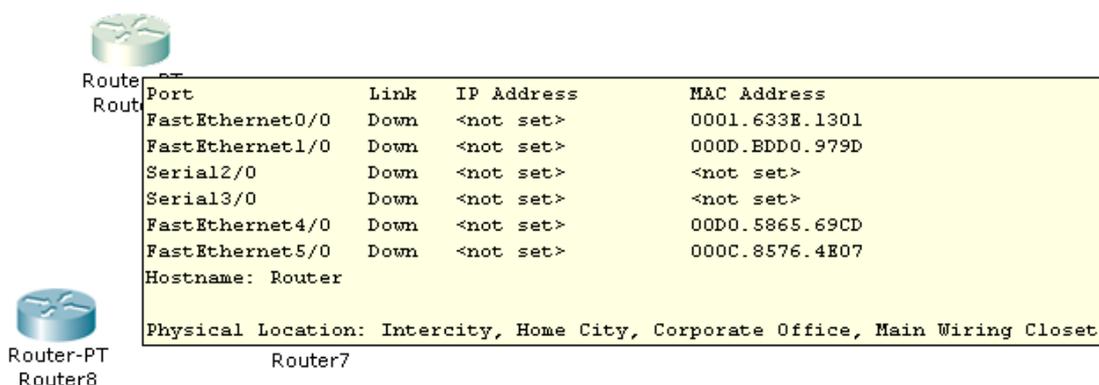


Figura 4.18: Descripción para obtener información de configuración del router.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

4.7.3 Modo Simulación (Simulation)

En el modo simulación, podrá ver animaciones de cómo se envían paquetes UDP, del tipo ICMP y paquetes personalizados. El modo real fue el modo en el que se realizó toda la configuración de los routers.

- **PDU Simple**

Diríjase a la parte inferior derecha, de un clic en donde dice *simulation*, con un cronómetro como dibujo, y aparecerá lo siguiente.

Aparecerá un cuadro donde podremos elegir el tipo de filtro que deseemos. Al inicio se encuentran todos los filtros activados, podemos activar/desactivar todos juntos, al seleccionar la opción All/None.

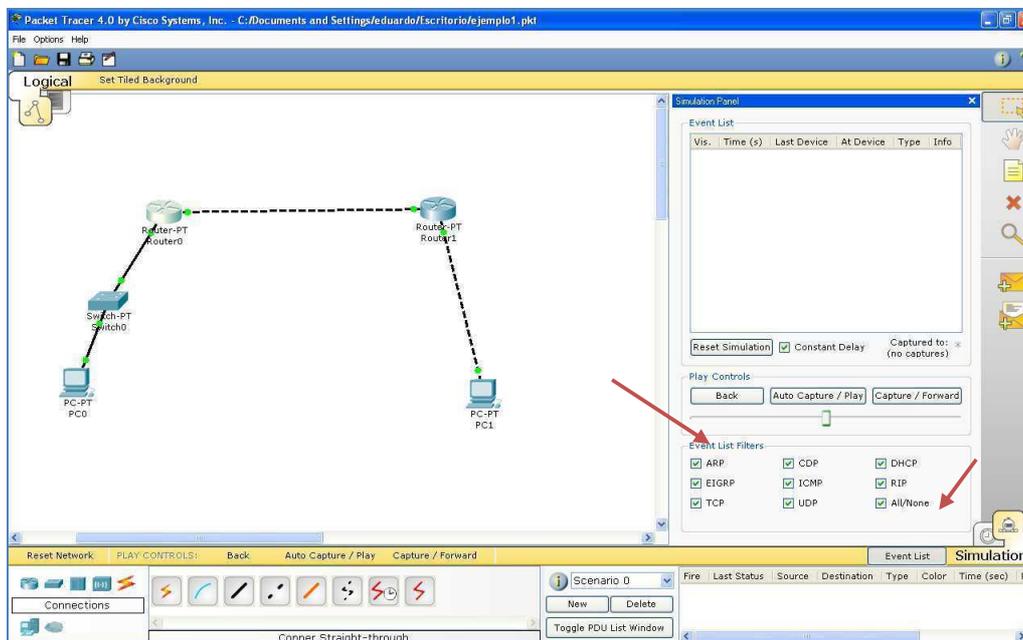


Figura 4.19: Modo Simulación, selección de filtros.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Enviaremos un paquete de tipo simple (Simple PDU), este botón se encuentra en la barra de herramientas comunes, es el sobre cerrado con un signo más en su parte izquierda. Se le determina el origen (PC0) y el destino (PC1).

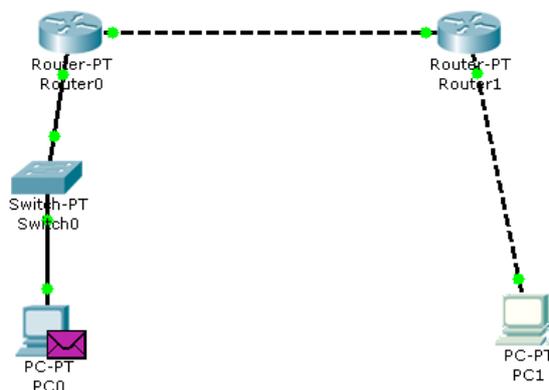


Figura 4.20: Proceso PDU simple.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Ahora debemos seleccionar el filtro, los paquetes que deseamos visualizar en la captura de datos que existirá cuando empieza la animación, el envío del paquete de la PC0 a la PC1. En la casilla All/None, podrá seleccionar o deseleccionar todos los paquetes

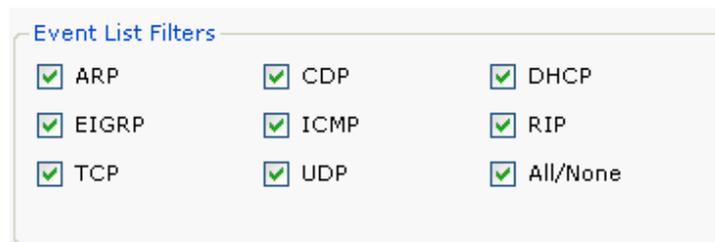


Figura 4.21: Protocolos a seleccionar para el proceso de envío de PDU

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para este ejemplo, dejaremos todos los paquetes seleccionados. La animación cuenta con una velocidad relativamente baja, para mostrar todos los pasos; pero puede modificarse con la barra de desplazamiento, con ella podrá aumentar o disminuir la velocidad con la que ocurren los eventos de envío y recepción, dicha barra se encuentra en Play Control. En ella también se encuentran los botones Back, Auto Capture / Play y Capture / Forward.

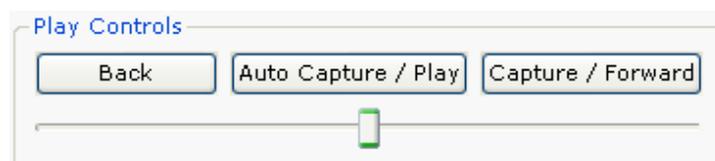


Figura 4.22: Barra de desplazamiento y controles de eventos.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

4.7.4 Descripción de los controles:

- **Capture / Forward:** Tiene como funcionalidad, iniciar la captura de paquetes de forma manual y de paso a paso en un tiempo determinado hacia delante.

- **Auto Capture / Play:** Funciona de manera similar que el anterior control, solamente que ahora la captura de paquetes se realiza automáticamente. Y va de forma directa el envío de paquetes.
Para detenerse la captura de paquetes y animación, debe de pulsarse sobre este botón, una vez iniciado el evento de animación y captura.
- **Back:** Retrocede hacia atrás un paso, y funciona para cualquier modalidad de las detalladas anteriormente (Capture / Forward y Auto Capture / Play).

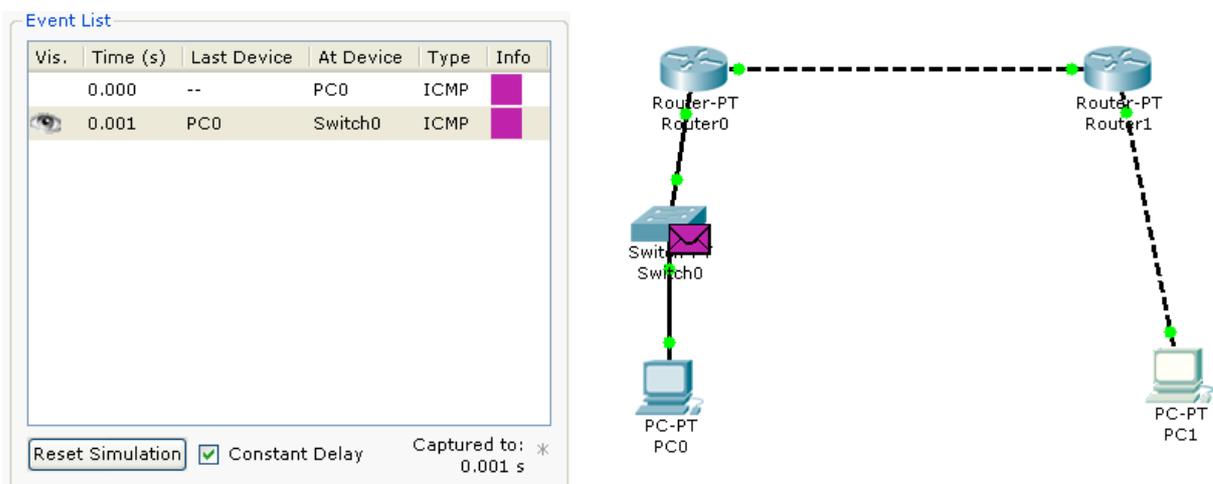


Figura 4.23: Descripción de controles

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

La ilustración anterior muestra el momento en que se pulsa por primera vez el botón Capture / Forward, y se visualiza cómo va el paquete de la PC0 hacia el Switch0, además muestra la lista de eventos ocurrido, que tiene como información mostrada, un pequeño ojo que muestra por donde está el paquete en ese preciso momento, el tiempo el segundo que ha transcurrido, el último dispositivo en el que se encuentra, el dispositivo en donde se encuentra, el tipo de paquete y la información, que está marcada con un cuadrado de cierto color correspondiente al tipo de paquete en operación.

Ahora procederemos a la captura manual de los paquetes, desde el inicio (PC0) hasta el fin (PC1). Las ilustraciones siguientes, muestran el proceso. Si se ve con

atención, el paquete desde el dispositivo donde se encuentre va desapareciendo y la apareciendo en el siguiente dispositivo, además que se muestra la ruta a seguir antes de proceder a desaparecer y a reaparecer.

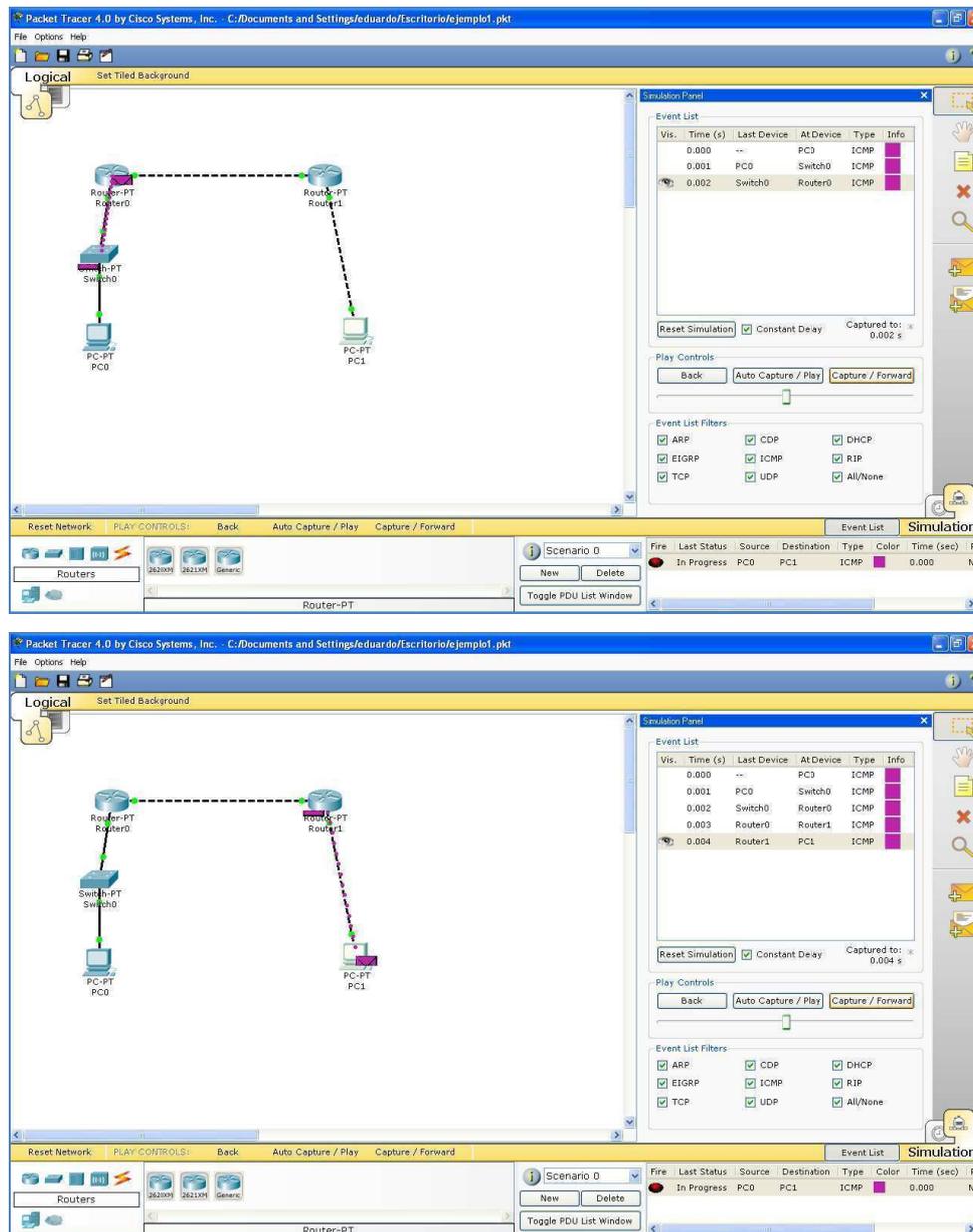


Figura 4.24: Captura de paquetes desde PC0 a PC1

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

La siguiente ilustración muestra la lista de eventos cuando el filtro de paquetes está activado, después que ha terminado la captura respectiva. En la parte inferior aparece un botón con el título 'Reset Simulation', que es el encargado de reiniciar cualquier tipo de captura de paquetes, manual o automática.

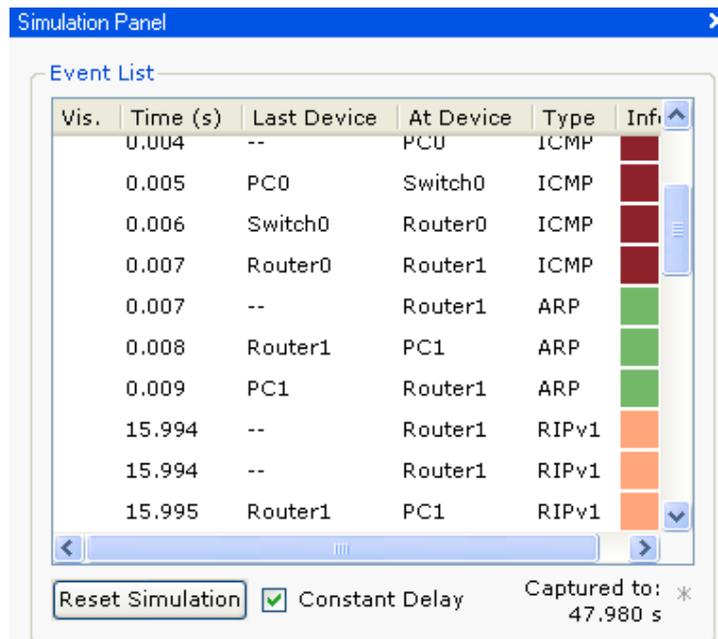


Figura 4.25: Panel para resetear la simulación.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

En la barra inferior, como se muestra a continuación, tendrá un acceso rápido cuando se tenga activa la operación de simulación, que sirve para ocultar o aparecer todos estos cuadros de información.

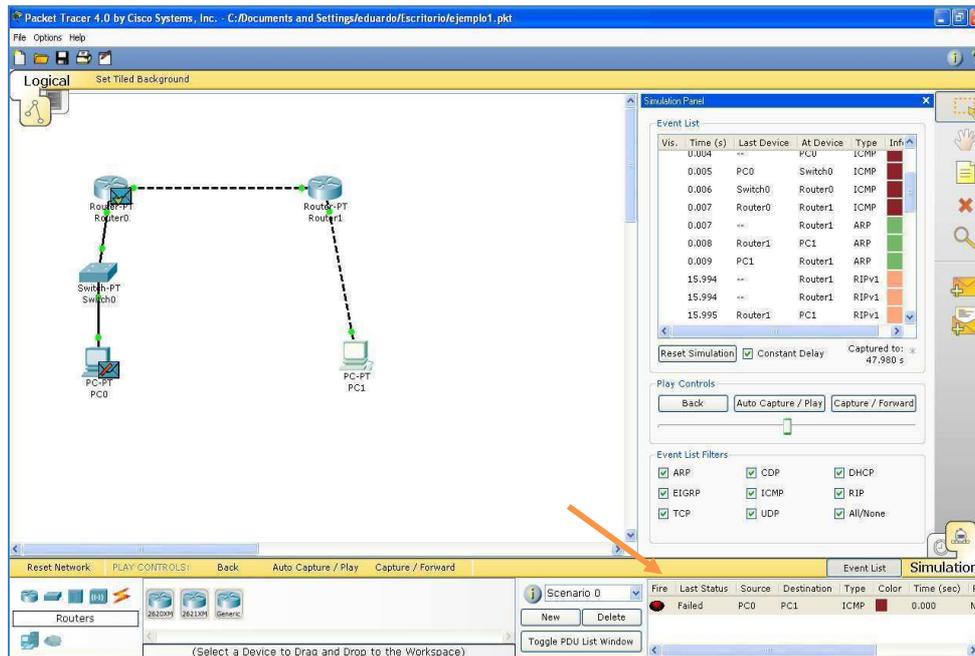


Figura 4.26: Modo Simulación.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Esta barra presenta la misma funcionalidad que el cuadro que aparece cuando se inicia el modo simulación, y es una barra para llevar el control del momento en que se desea capturar los datos, y no mostrar en ese momento la información generada por la captura.

El botón que está marcado en el ovalo naranja, oculta o muestra toda la información capturada. Existe en esta misma barra un botón denominado 'Reset Network' que es la encargada de romper los ciclos que existiesen en la red, pero además de esto pide una confirmación para eliminar la configuración que existe en la red, perdiendo así todas las configuraciones realizadas, esto es en los ficheros de running-config.



Una vez realizada la captura de paquetes, se puede alterar los paquetes que se han captura, es decir realizar un filtro de otros paquetes de los cuales no fue señalada la captura.

Ahora regresemos al inicio. Pueden crearse diferentes escenarios, para realizar las simulaciones, y para ello localizamos la siguiente barra. Donde podrá crear un nuevo escenario con el botón **New**, borrar algún escenario con el botón **Delete** y dar información relevante con el botón que tiene el icono de la letra i; si se agrega esta información, aparecerá un cuadro donde podrá ingresarla, solamente necesitar cerrar esta ventanita para poder guardar la información.

Creamos un nuevo escenario, para mostrar el siguiente ejemplo, dejamos el nombre por default, Scenario 1. Al realizar esta operación, notara que la lista de eventos capturas es nueva para cada escenario creado.

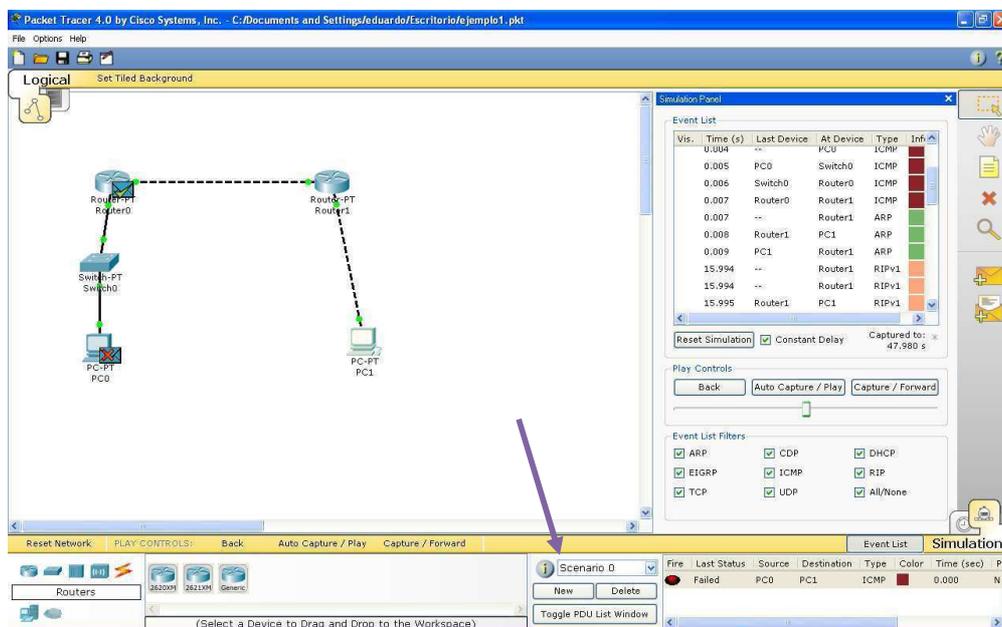


Figura 4.27: Descripción para crear un nuevo escenario.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Ahora seleccionamos la PC0, y nos dirigimos a la opción de **Command Prompt**. Ahora escribimos la dirección ip de la PC1. Todos los cuadros de información se acomodan para mostrarse, pero podrá hacer doble clic sobre alguno de ellos, en este caso el que muestra la lista de eventos, y vera como se coloca en una nueva posición, fuera de la rendija de la ventana principal.

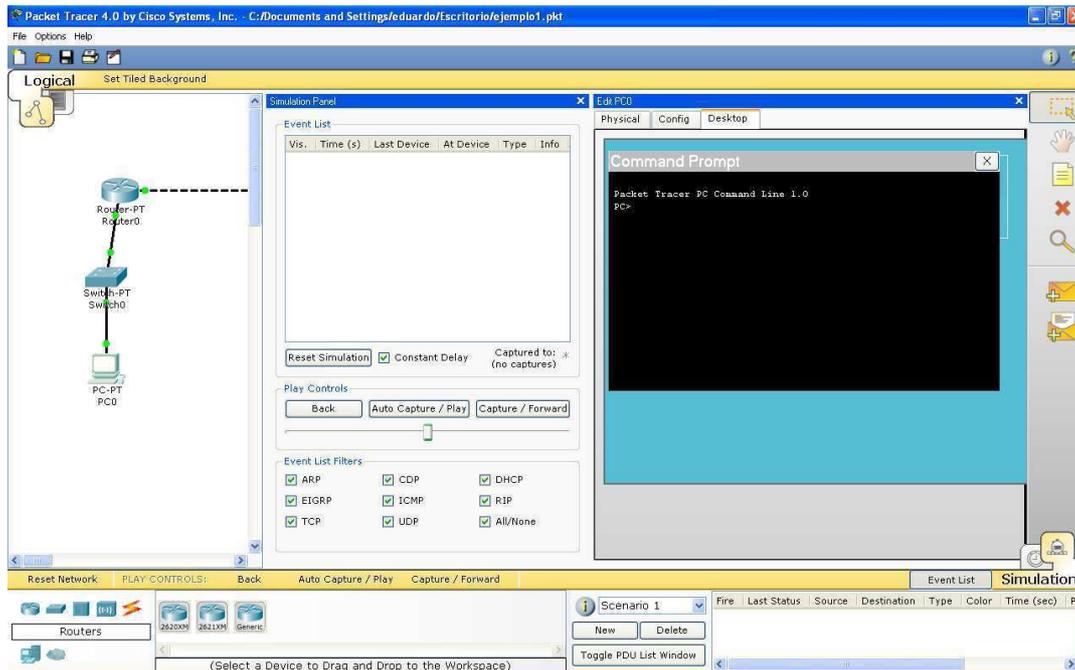


Figura 4.28: Ingreso a Command Prompt

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

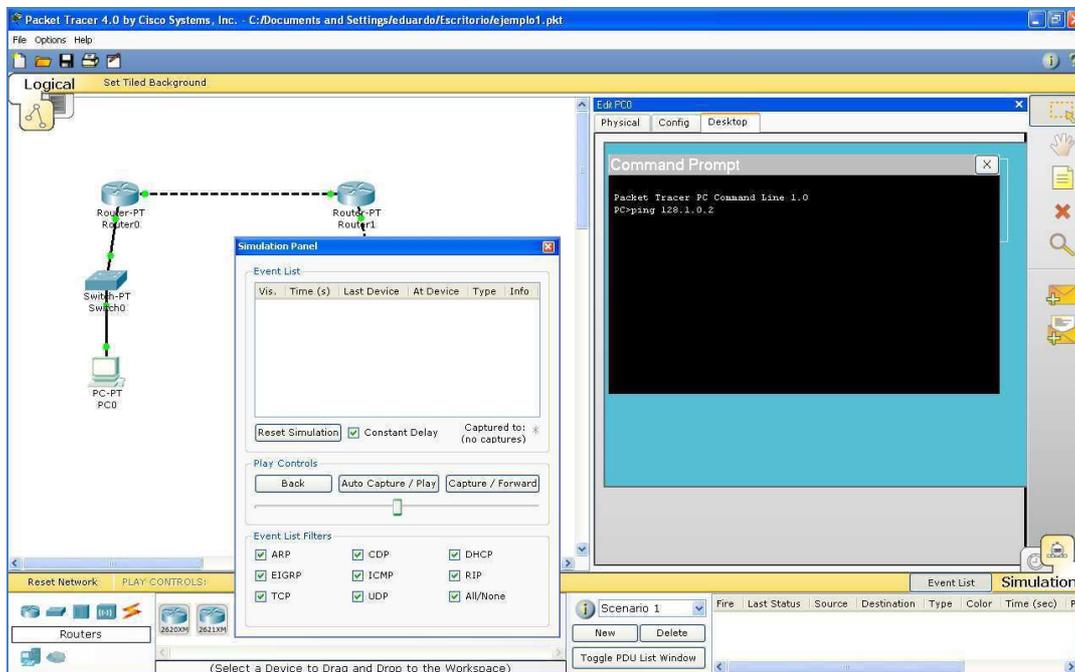


Figura 4.29: Ping desde el command de PC0 a PC1

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

El tipo de filtro seleccionado debe ser del tipo ICMP, para este ejemplo

Después que presione la tecla ENTER notara que no empieza la secuencia de la respuesta, y esto se debe a que no nos encontramos en el modo real, y por lo tanto debemos de iniciar la captura de paquetes, en forma automática o manual, pero en este caso será automática, para ver su comportamiento de manera rápida. Una vez que el paquete ha sido enviado y se devuelve la confirmación, este ha sido marcado de un color diferente, aunque sean del mismo tipo de paquete.

En la ilustración, vemos que los paquetes son del tipo ICMP y cuando se envían son de un color diferente que cuando ya es recibida la respuesta en la misma computadora, la emisora del mensaje. Podrá terminar de ver las cuatro REPLY que se dan al momento de hacer un ping, o detenerse en cualquier momento la animación. Recuerde que podrá reiniciar la simulación en cualquier momento.

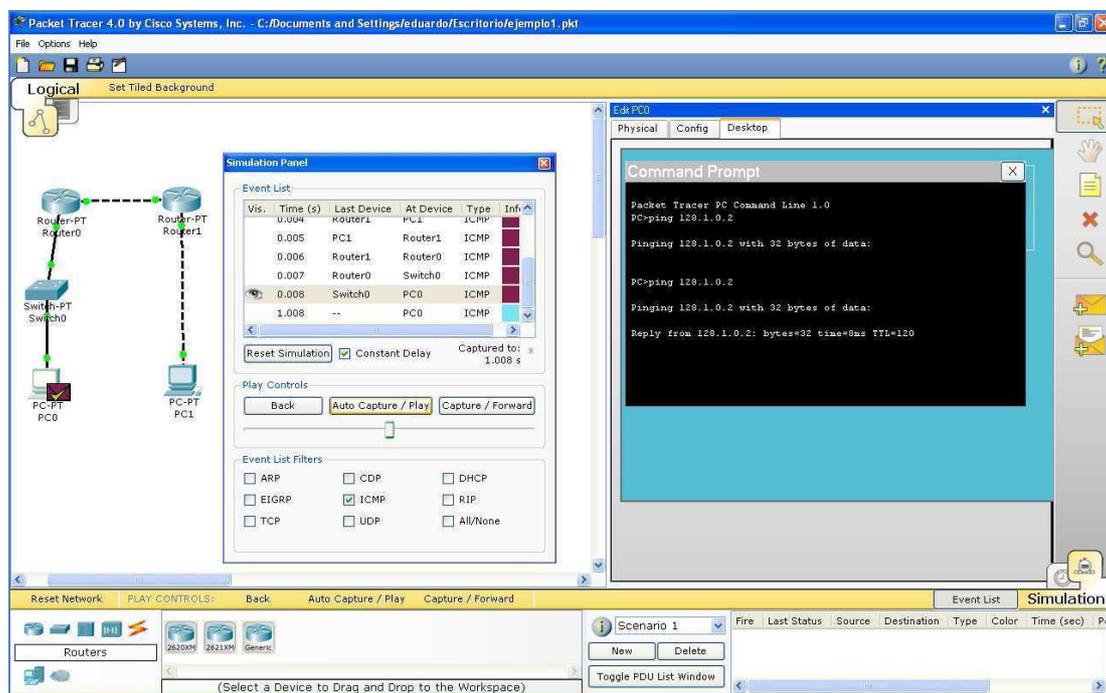


Figura 4.30: Respuesta a Ping desde el command de PC0 a PC1

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

CAPITULO V

5 SIMULACIONES DE PRÁCTICAS A TRAVÉS DEL SOFTWARE *PACKET TRACER*

A continuación presentamos algunas prácticas realizadas con el software *Packet Tracer* desde la creación de interconexiones simples entre dispositivos hasta obtener una red en la que interactúan varios elementos y comparten información.

5.1. Practica # 1: Interconexión de dos CPU's utilizando cable cruzado

➤ **Objetivo:** Conseguir la transferencia de paquetes entre las dos PC's.

➤ **Procedimiento:**

Iniciamos el software *Packet Tracer* versión 5.3.0 y colocamos 2 PC's genéricas en el espacio de trabajo, como se observa en la fig. 5.1.

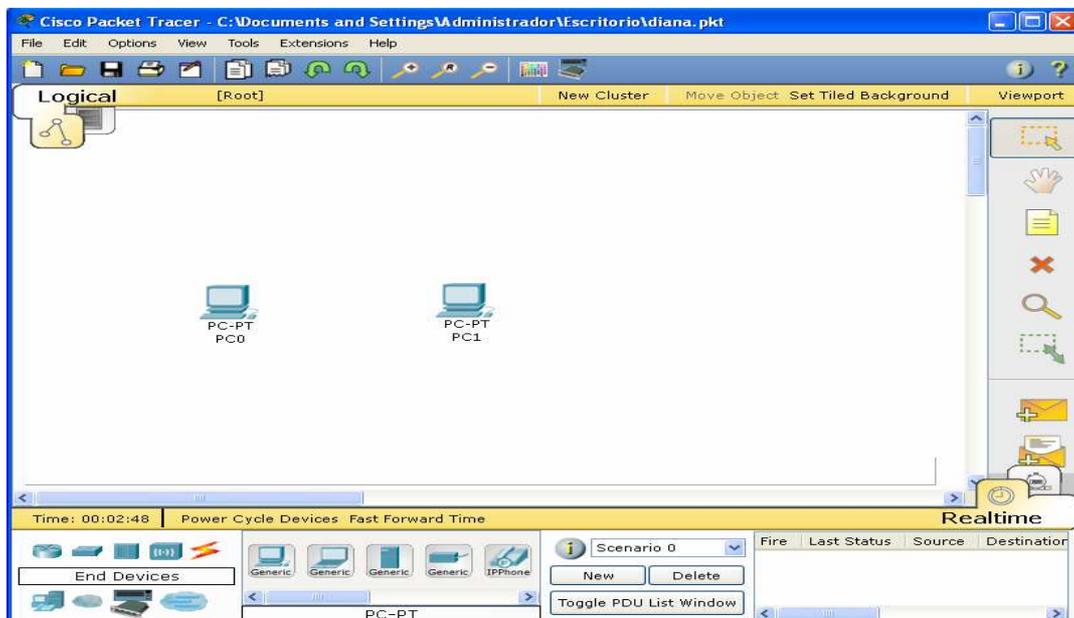


Figura 5.1: Colocación de 2 PC's en el espacio de trabajo de PT

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Tenemos 2 computadoras similares a la que se denominará PC0 y PC1 respectivamente.

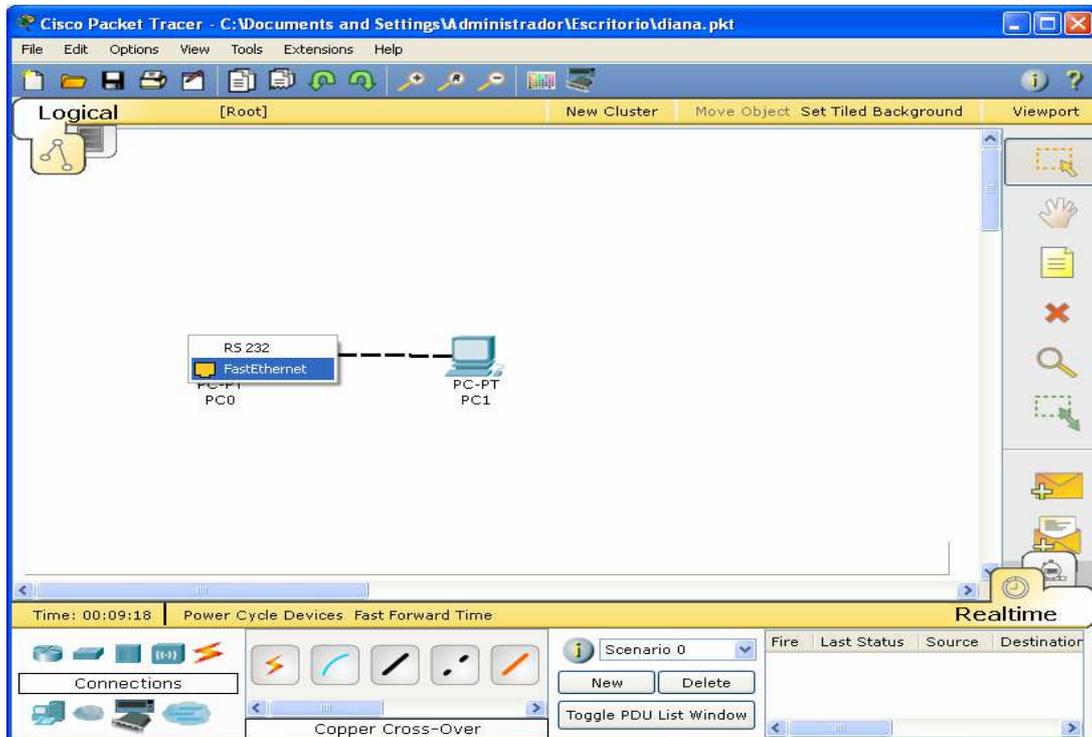


Figura 5.2: Conexión entre las 2 PC's a los puertos Fastethernet

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

En la parte inferior del *Packet Tracer* en el icono **Conexions** ⚡ donde se encuentran los diferentes tipos de cables que se tienen para interconectar los equipos de una red de telecomunicaciones, seleccionamos un cable cruzado  , para realizar esta práctica, cada extremo del cable irá en el puerto FasEthernet de cada CPU. Fig. 5.2

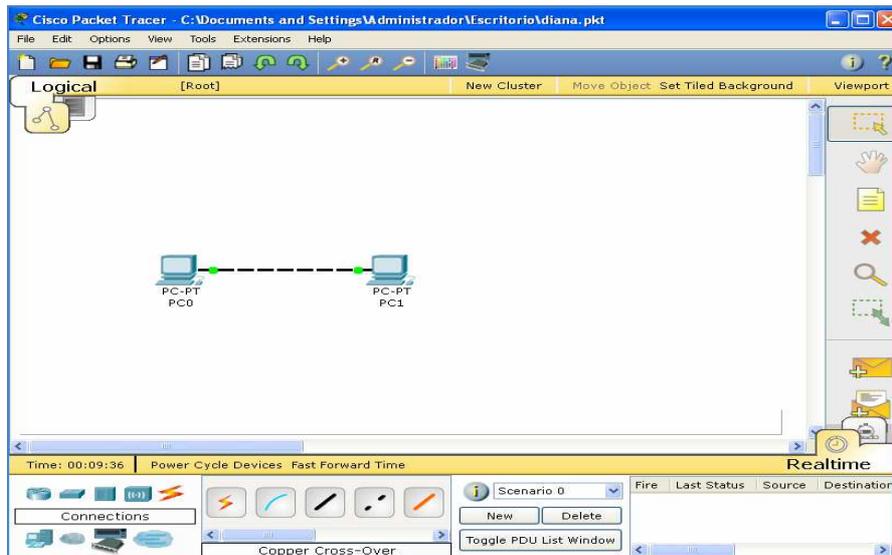


Figura 5.3: Conexión entre las 2 PC's con cable cruzado.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Ahora tenemos la conexión entre los dos CPU's, pero existe un inconveniente la información no puede ser transmitida entre estos 2 equipos. Fig. 5.3

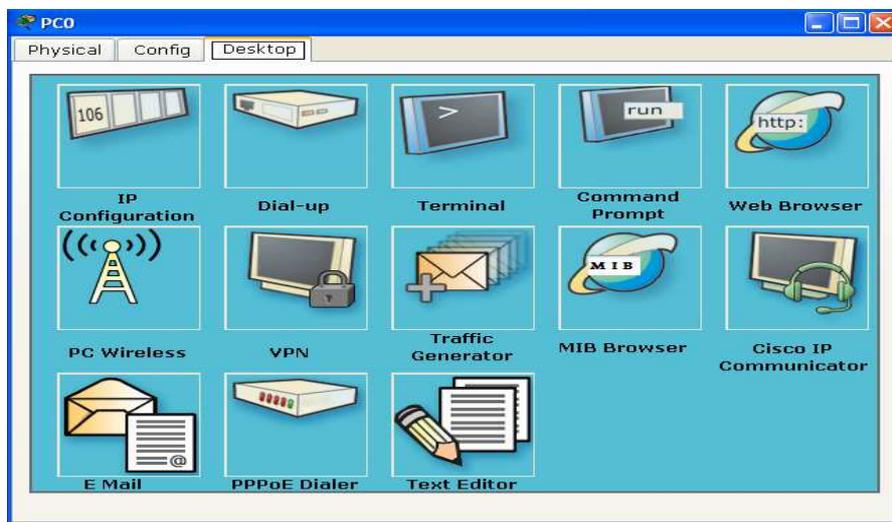


Figura 5.4: Ingreso a IP Configuration

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

El siguiente paso es el direccionamiento de la tarjeta de red de cada una de las computadoras, seleccionamos la PC0, donde se abre una nueva ventana, en la

parte superior elegimos la pestaña **Desktop**, y luego la opción **IP Configurartion**.
Fig. 5.4.

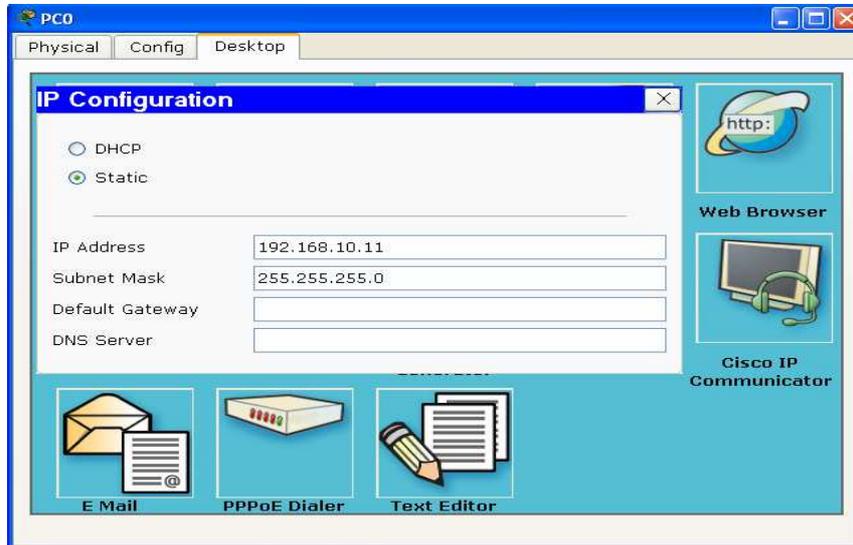


Figura 5.5: Direccionamiento de la tarjeta de red de PC0

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Seleccionamos la opción de direccionamiento estático **Static**, Luego asignamos una dirección Ip y mascara de subred. Fig. 5.5

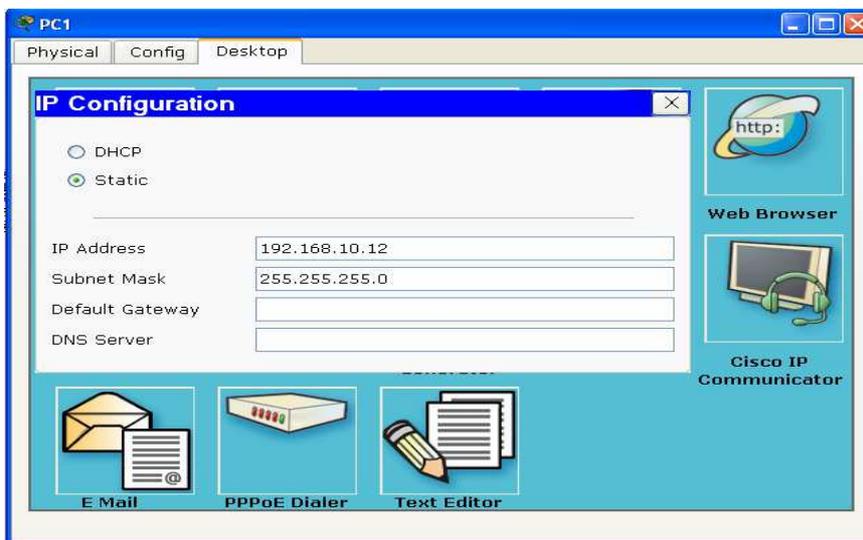


Figura 5.6: Direccionamiento de la tarjeta de red de PC1

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

De igual manera lo hacemos en la PC1, cabe recalcar que las direcciones IP deben ser de una misma red para que pueda existir una transferencia de datos exitosa. Fig. 5.6

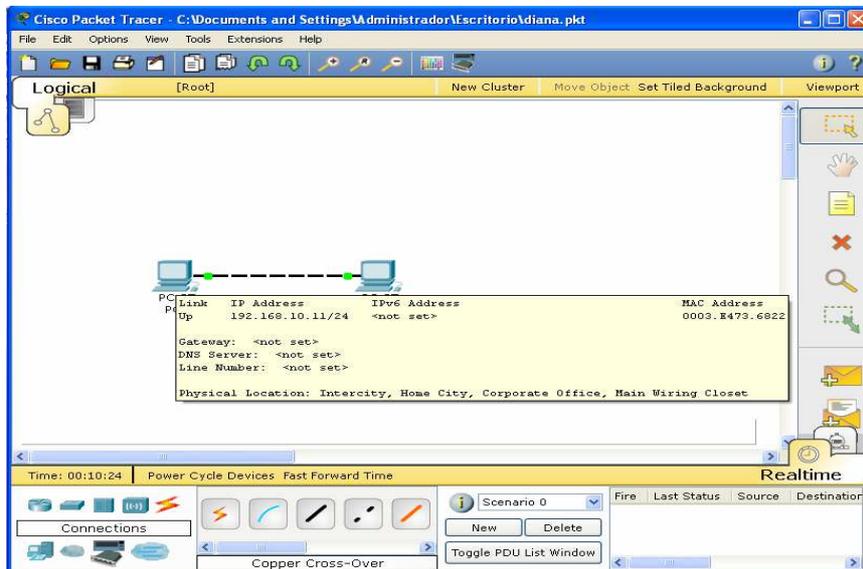


Figura 5.7: Direccionamiento de la tarjeta de red de PC1

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

En este momento las 2 PC's pueden transferir información, tienen configurada una dirección IP con su respectiva máscara de subred. Fig. 5.7

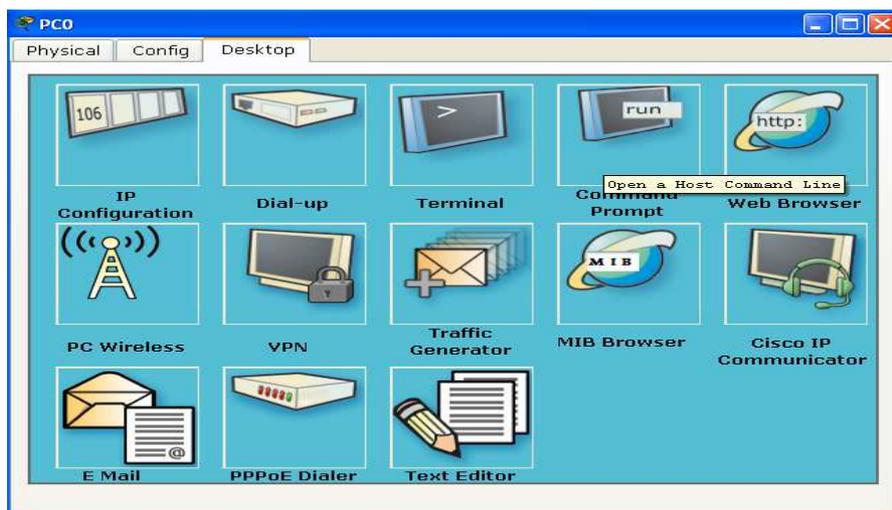


Figura 5.8: Ingreso a Command Prompt desde la PC0

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para poder comprobar que existe comunicación al 100% entre los equipos nos dirigimos a cualquiera de las dos computadoras a la opción **Desktop** y luego **Command Prompt** para realizar un Ping a la dirección IP de la otra PC. Fig. 5.8

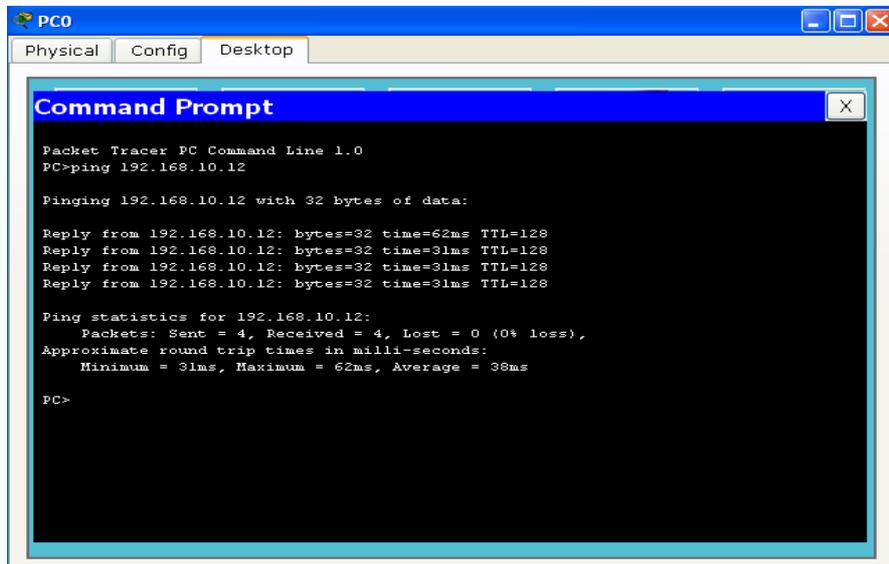


Figura 5.9: Ping desde la PC0 a la PC1

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Hacemos un ping a la dirección IP de la otra PC y el resultado es exitoso. Fig. 5.9

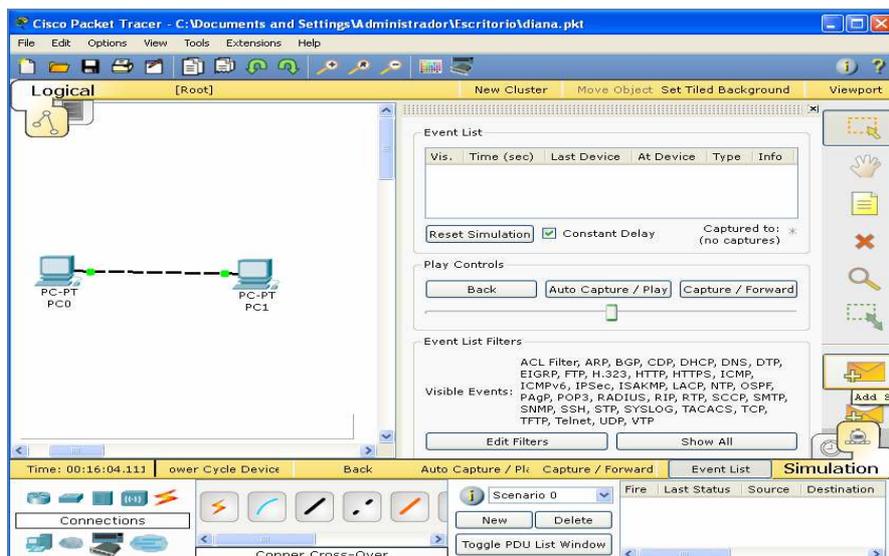


Figura 5.10: Modo simulación – PDU simple

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para realizar una simulación de cómo se transmite un paquete de datos seleccionamos la opción **Simulation** que se encuentra en la parte inferior derecha del *Packet Tracer*, luego agregamos un **PDU simple** tanto en la PC0 como la PC1. Fig. 5.10

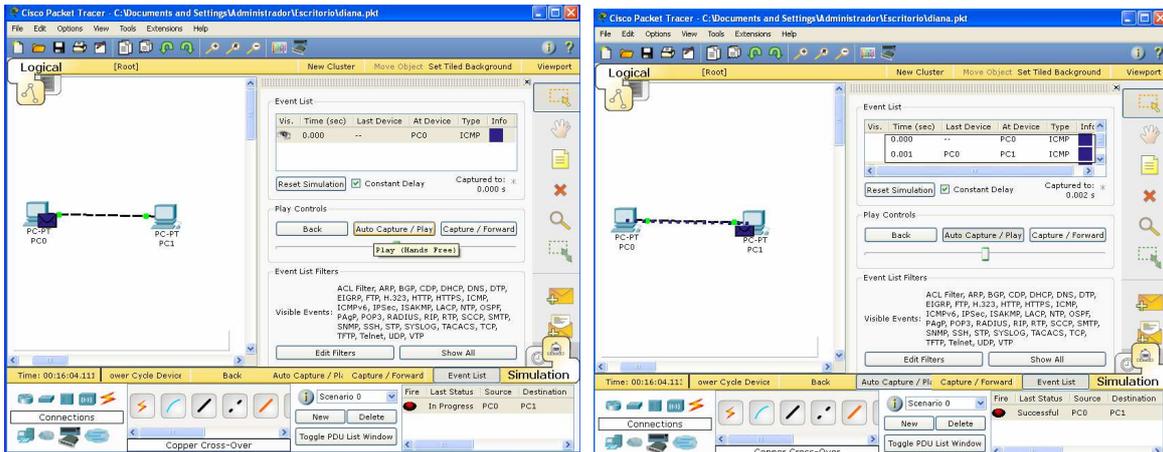


Figura 5.11: Modo simulación – Paquetes ICMP desde PC0 a PC1

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Seleccionamos la opción **Auto Capture/Play**, para empezar la simulación y vemos como el paquete es transmitido de una PC a otra, en la parte superior derecha se puede observar los protocolos que se están utilizando. Fig. 5.11

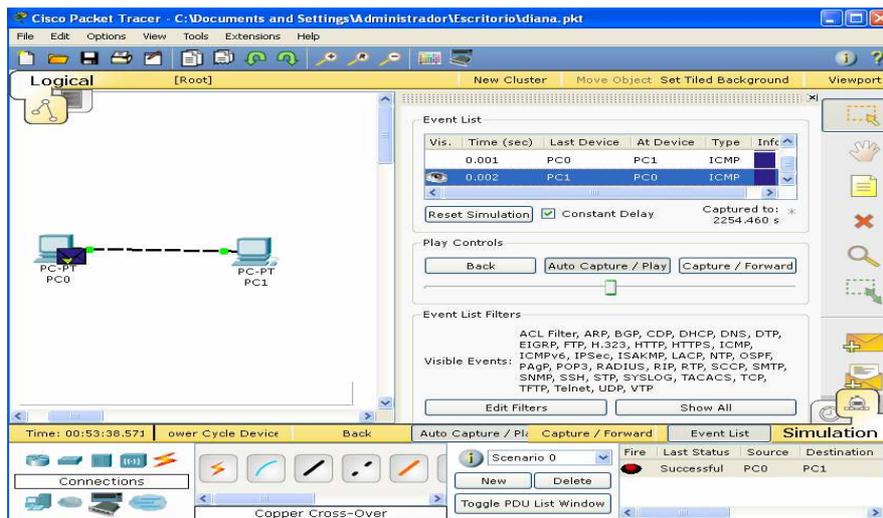


Figura 5.12: Transferencia de paquetes exitosa.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Por último vemos que la transferencia del paquete fue exitosa.

De esta manera podemos observar de una manera práctica y simple como es la interconexión de 2 CPU's utilizando cable cruzado y todo lo que implica la transferencia de un paquete.

➤ **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 5.12 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.

5.2. Practica # 2: Realizar una pequeña red LAN interconectando un switch y un hub.

- **Objetivo:** Conseguir la transferencia de paquetes entre las cuatro PC's y la impresora que se encuentra conectada en red.

- **Procedimiento:**

Iniciamos el software *Packet Tracer* versión 5.3.0 y colocamos los dispositivos en el espacio de trabajo, como se observa en la fig. 5.13.

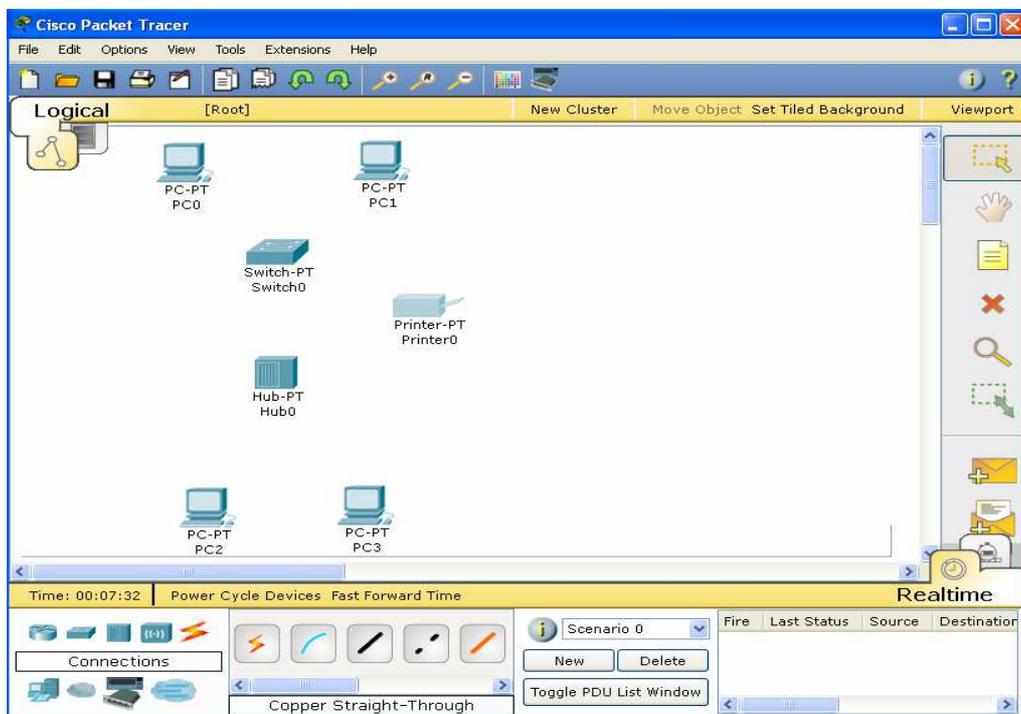


Figura 5.13: Colocación de equipos a utilizarse.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Se posee 4 computadoras, 1 switch, 1 hub, y 1 impresora, las cuales se las quiere poner en una misma red, es decir una pequeña LAN. Fig. 5.13

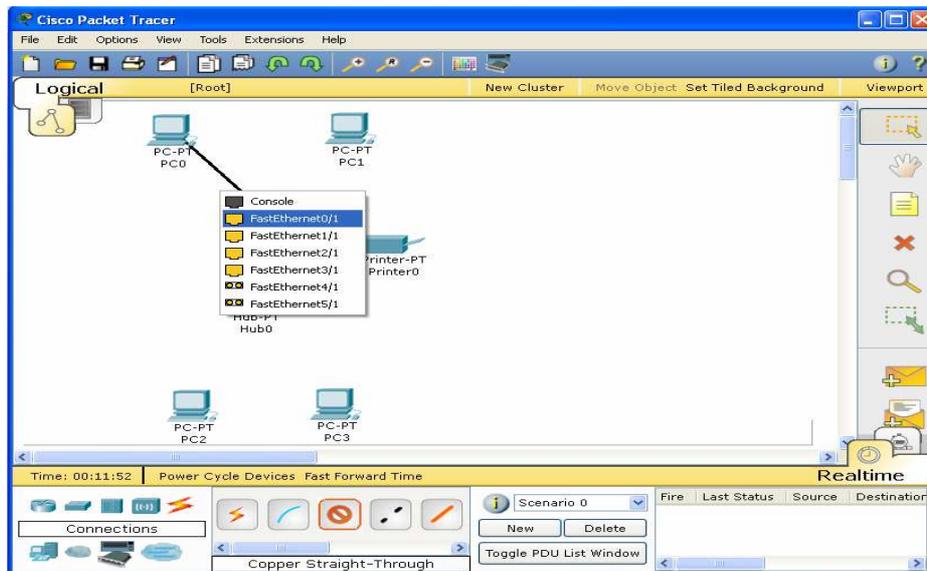


Figura 5.14: Conexión de PC0, PC1 e impresora al Switch

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para conectar un CPU a un Switch se utiliza un cable directo, En la PC0 conectamos al puerto FastEthernet, y en el Switch conectamos a uno de los puertos FastEthernet del Switch, de igual manera hacemos este procedimiento para conectar el PC1 y la impresora con los puertos libres del Switch. Fig. 5.14

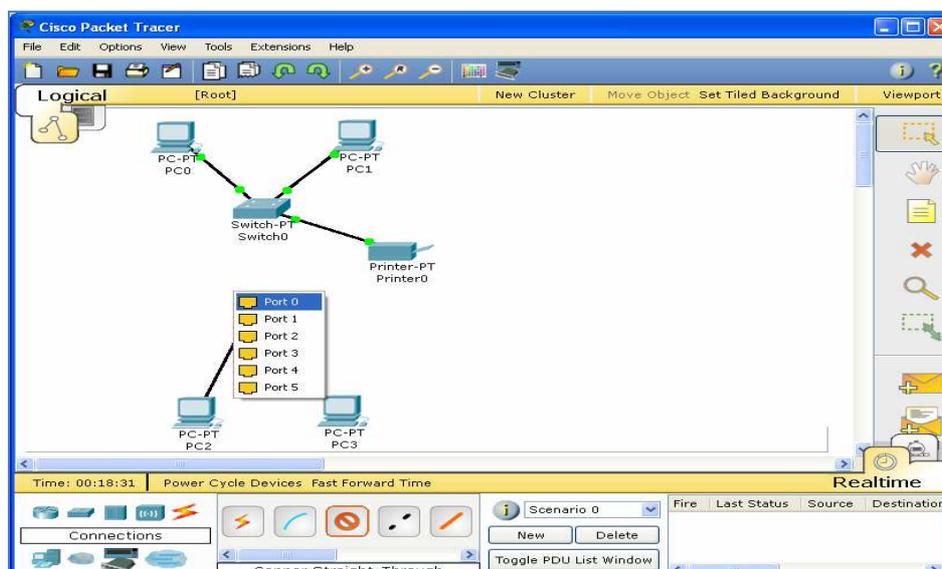


Figura 5.15: Conexión de PC2 y PC3 al hub

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para conectar un CPU a un hub el proceso es casi similar al anterior paso, con la diferencia de que el hub no tiene puertos FastEthernet. Fig. 5.15

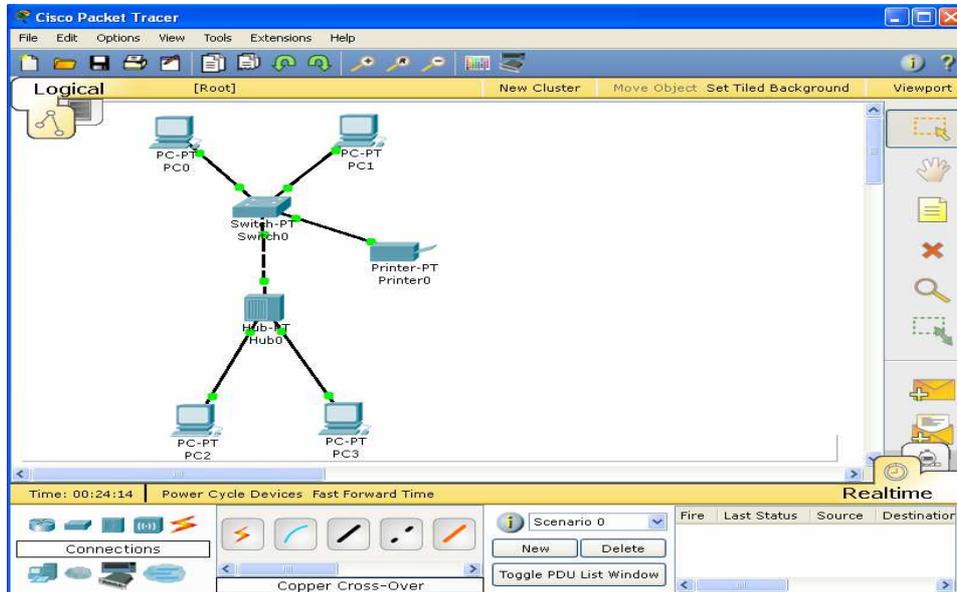


Figura 5.16: Conexión entre el Switch y el hub

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para conectar el Switch y el hub utilizamos un cable cruzado, y de esta manera tenemos la conexión física de nuestra pequeña LAN. Fig. 5.16

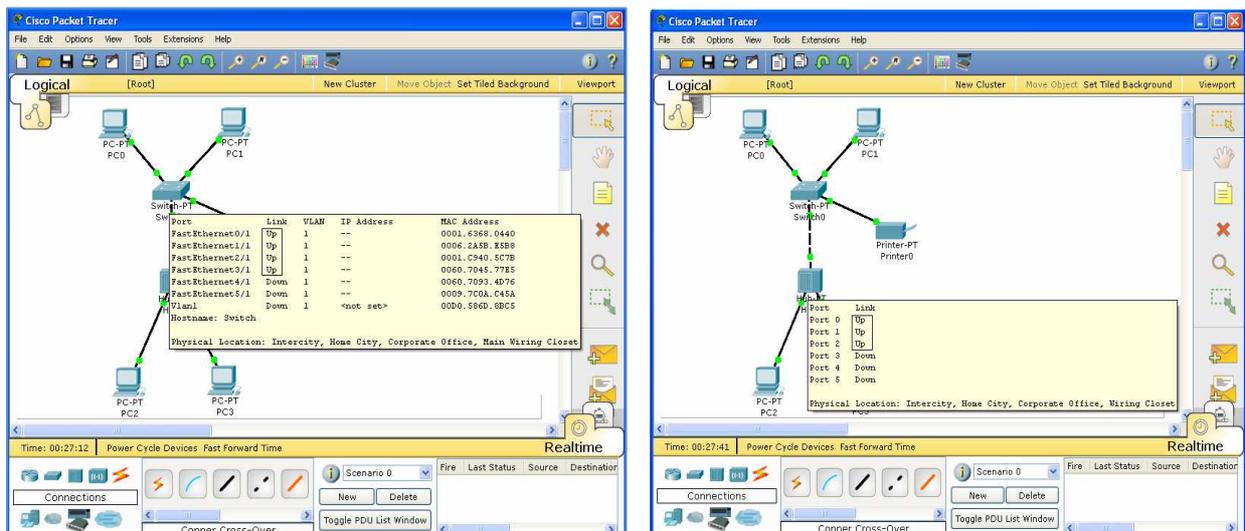


Figura 5.17: Verificación de puertos activos

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para verificar que los puertos tanto del Switch como del hub están Up, colocamos el cursor sobre el equipo para notar el estado de los puertos. Fig. 5.17.

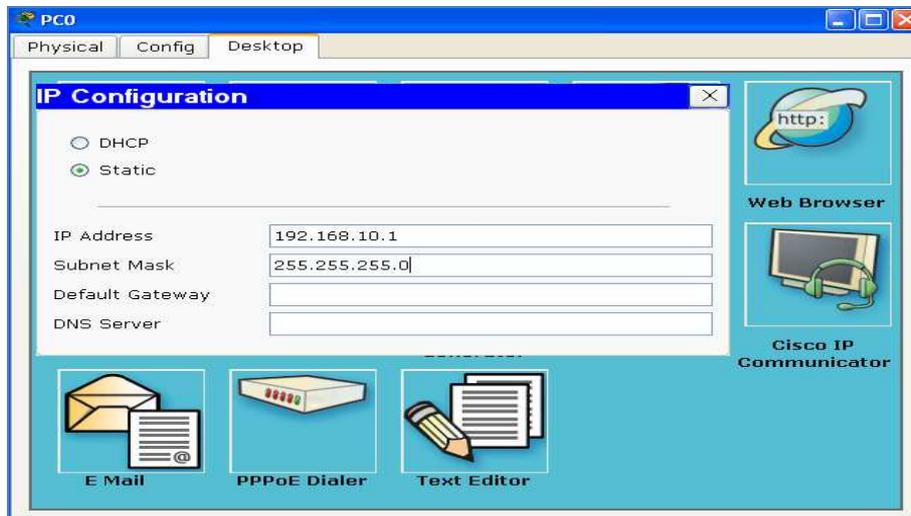


Figura 5.18: Direccionamiento de la tarjeta de red de los CPU's
Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Luego de la conexión física de la LAN, se procede al direccionamiento de la tarjeta de red de cada una de las computadoras, la dirección IP va desde la 192.168.10.1 hasta 192.168.10.4 con su máscara de subred 255.255.255.0 respectivamente. Fig. 5.18.

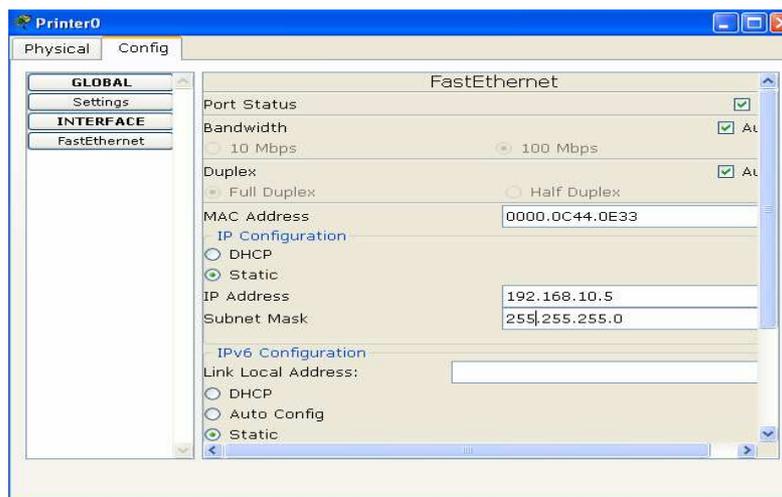


Figura 5.19: Asignación de dirección IP a impresora
Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Para que la impresora se encuentre dentro de la misma LAN seleccionamos este equipo, luego ubicamos la opción de configuración y seleccionamos la opción FastEthernet, asignamos la dirección IP 192.168.10.5 y la máscara de subred 255.255.255.0 respectivamente y de esta manera todos los equipos están interconectados lógicamente dentro de la misma LAN. Fig. 5.19.

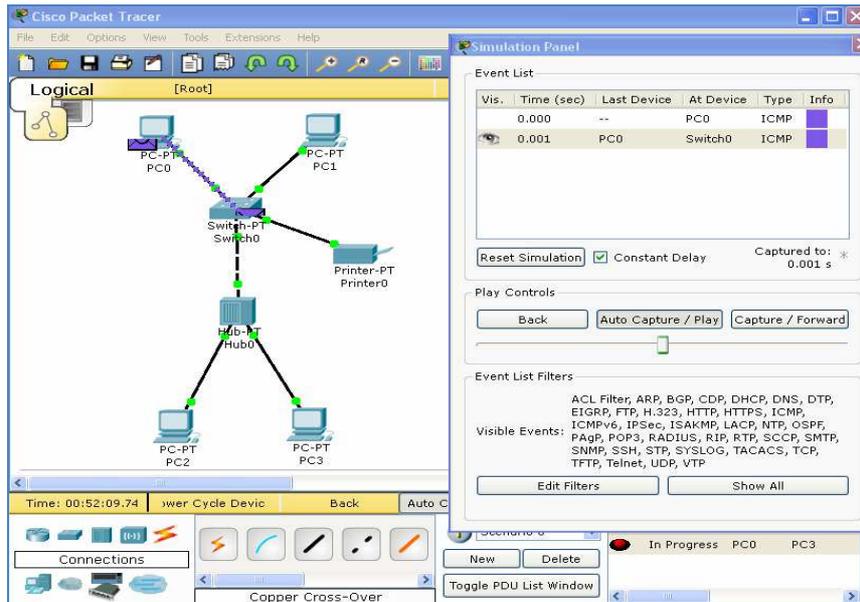


Figura 5.20: Simulación de transferencia de información

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Aquí se puede notar como comienza la transferencia de información y los protocolos que se está utilizando para una comunicación entre la PC0 y PC3. Fig. 5.20.

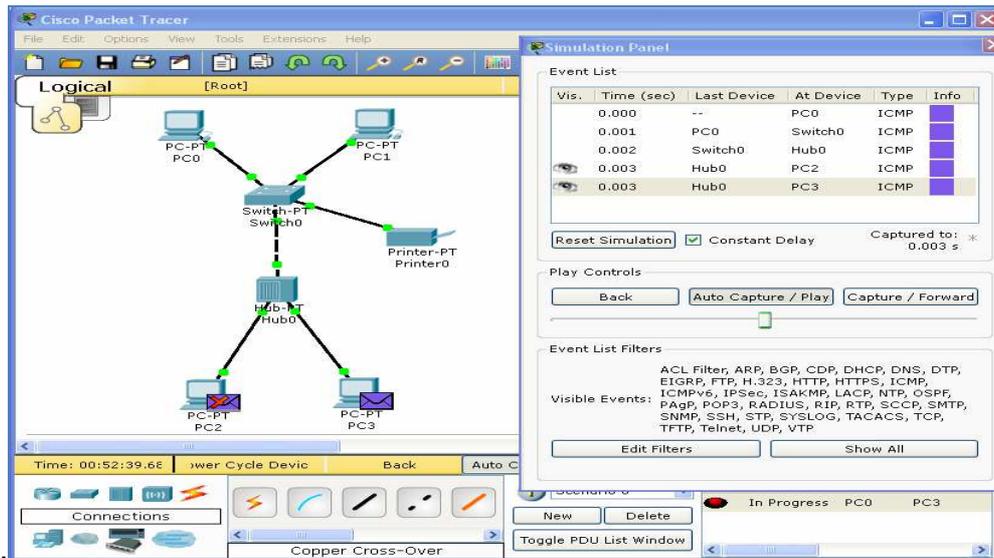


Figura 5.21: Simulación de transferencia de información 2

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Se puede observar claramente que el paquete se traslada del Switch al hub sin obtener ningún problema, pero al mismo momento el paquete se transmite también a la PC2 pero el cual es destruido porque ese no es el destino del paquete. Fig. 5.21.

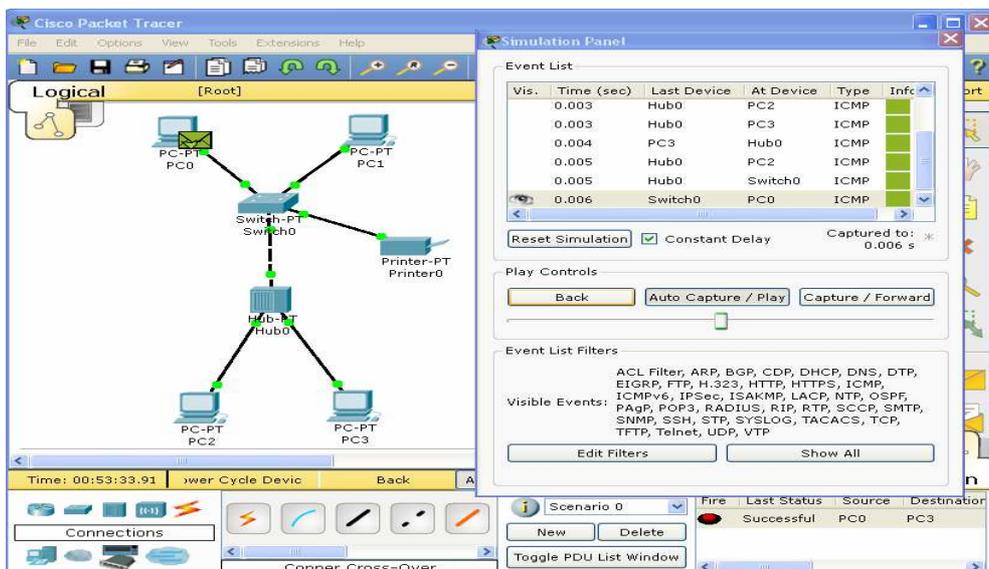


Figura 5.21: Simulación de transferencia de información 3

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Por último la PC0 recibió la confirmación de que el paquete fue entregado a su destino PC3.

➤ **Análisis de resultados**

- 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.
- En la figura 5.21 se puede observar muy claramente que el paquete regreso al punto de partida, significando de esa manera que la transferencia de datos es válida.

Conclusiones

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

5.3. Practica # 3: Realizar una red LAN utilizando un Access Point(AP) y un Switch

➤ Objetivos:

- 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:

Iniciamos el software *Packet Tracer* versión 5.3.0 y colocamos los siguientes dispositivos en el espacio de trabajo: 1 switch, 1 Access Point, 3 PC's y una impresora como se observa en la fig. 5.22.

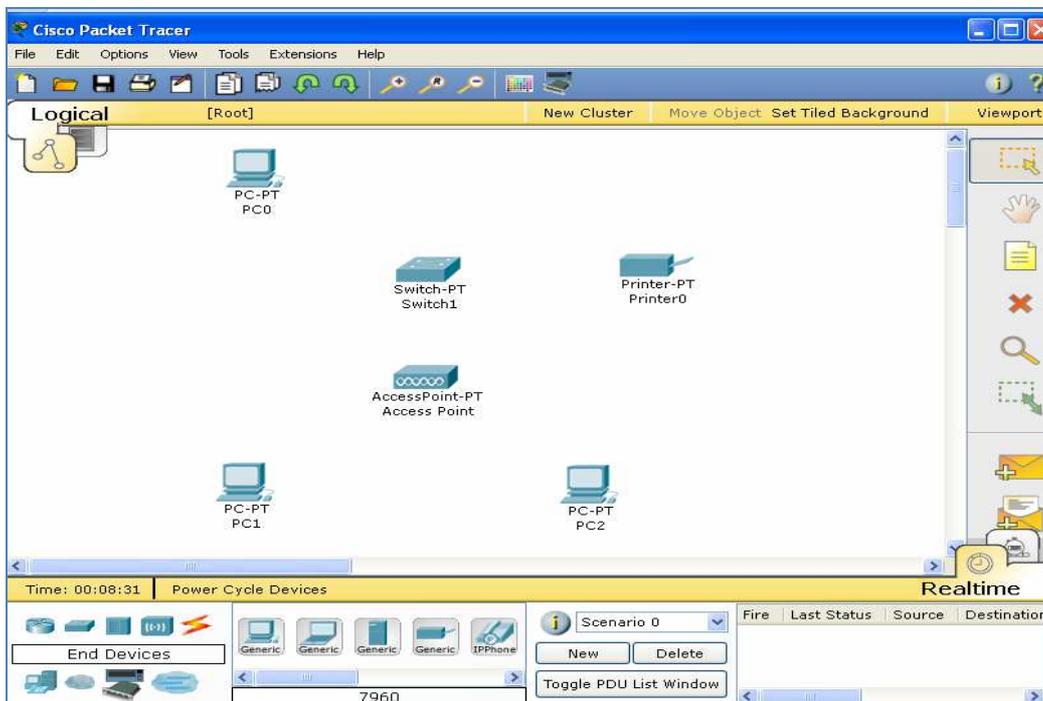


Figura 5.22: Colocación de dispositivos a utilizarse.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Conectamos con cable directo los puertos FastEthernet de la PC0 y la impresora a los puertos Fa0/1, Fa1/1 del switch respectivamente y conectamos el puerto 0 del AP al puerto F2/1 del switch, como se muestra en la fig. 5.23

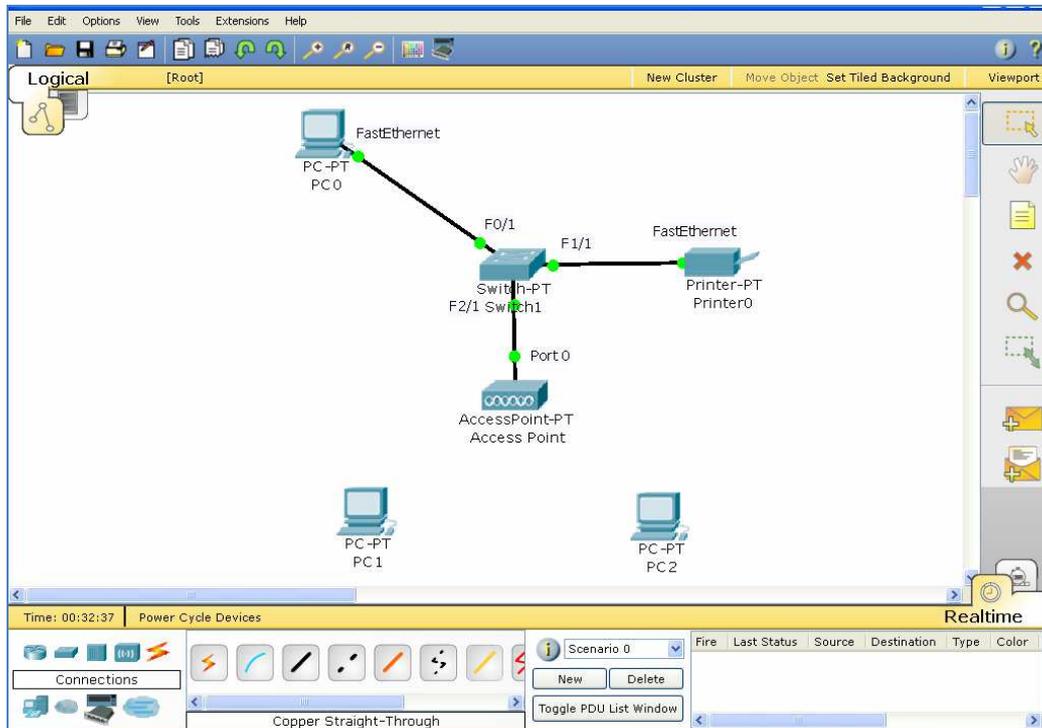


Figura 5.23: Conexión entre dispositivos.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Ahora se procede a configurar la dirección IP y su respectiva máscara de red para la PC0, para ello procedemos a dar un clic en la primera CPU para lo cual se abre una pantalla de configuración.

En la pantalla que aparece debemos dirigirnos a la pestaña con el nombre de **Desktop**, y luego en **IP Configuration** (Fig. 5.24) en la cual procedemos a colocar la dirección IP asignada a esa PC y su respectiva máscara de subred, como se observa en la figura 5.25.

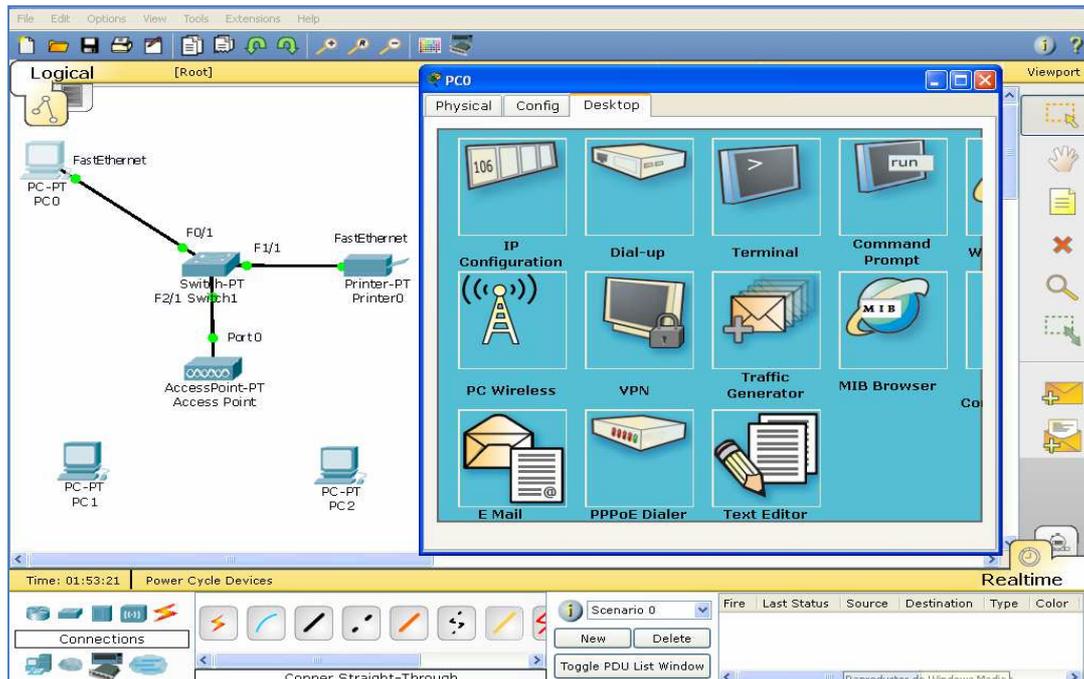


Figura 5.24: Proceso para ingresar a la tarjeta NIC de PC0

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

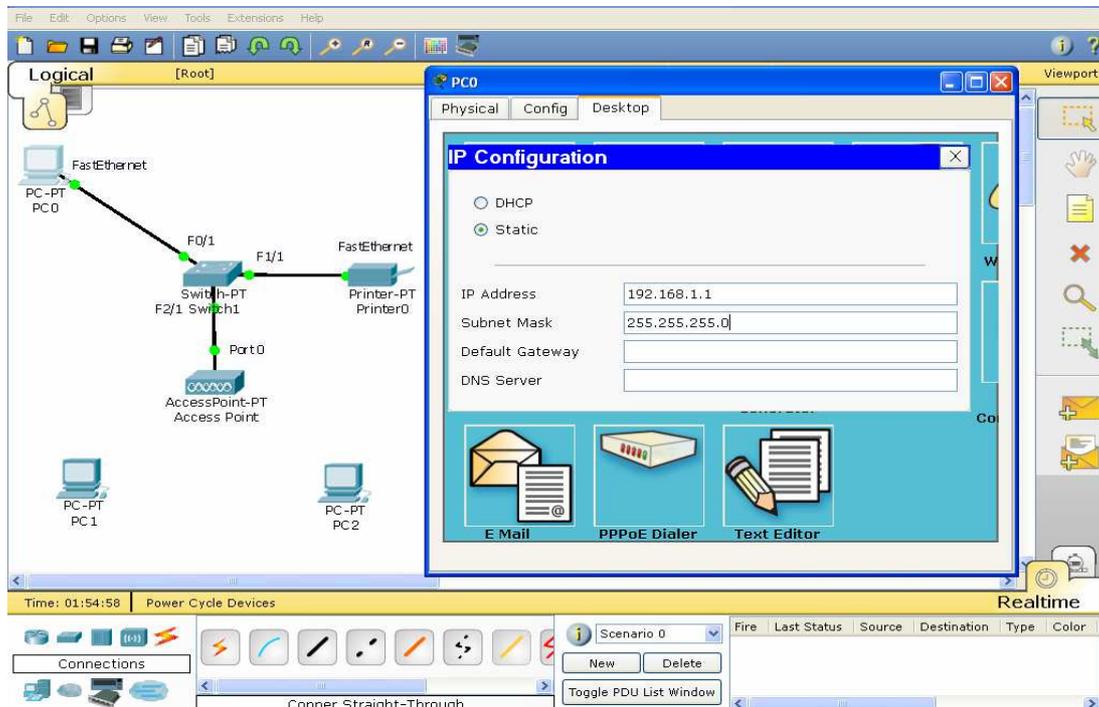


Figura 5.25: Direccinamiento de tarjeta de red de PC0

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

El mismo procedimiento será utilizado para la configuración de la tarjeta de red de PC1 y PC2, colocando las siguientes direcciones IP y máscaras de red como se muestran a continuación:

- **PC1**

IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0

- **PC2**

IP Address: 192.168.1.3
Subnet Mask: 255.255.255.0

A continuación procedemos con la configuración de la dirección IP de la impresora con su respectiva máscara de subred, para lo cual damos clic en la impresora y nos dirigimos a la pestaña **Config**, luego a **FastEthernet** y colocamos de manera estática la dirección IP y la máscara como se observa en la figura 5.26.

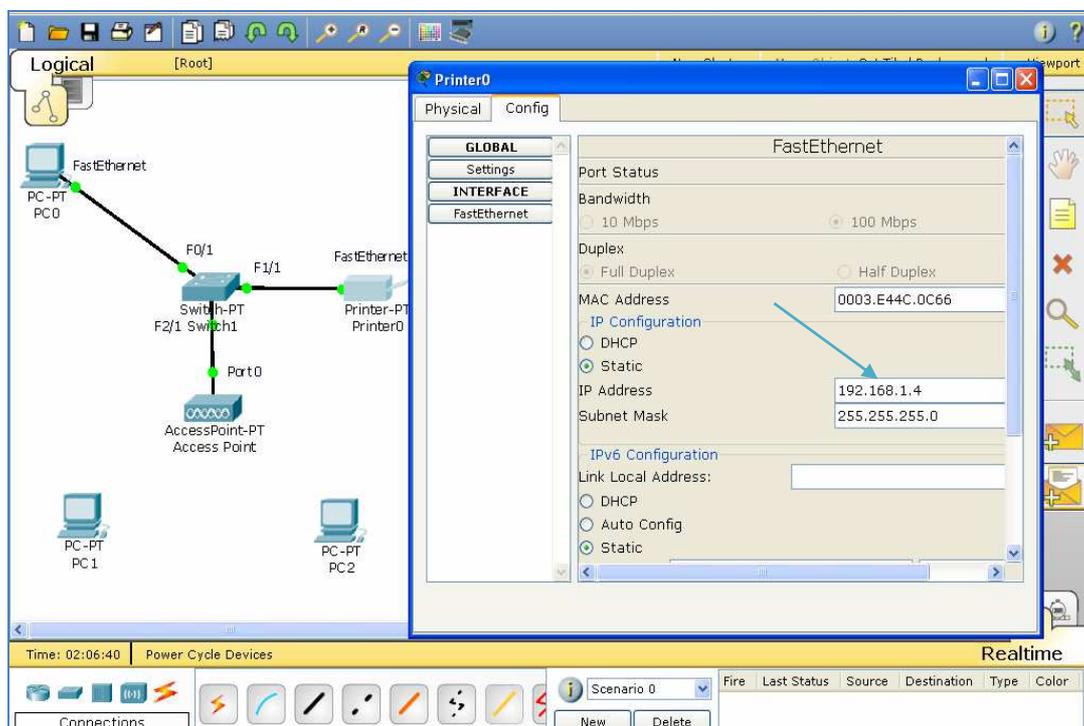


Figura 5.26: Asignación de dirección IP a la impresora.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

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 **FastEthernet** en la pestaña **Config** como se puede observar en la figura 5.27.

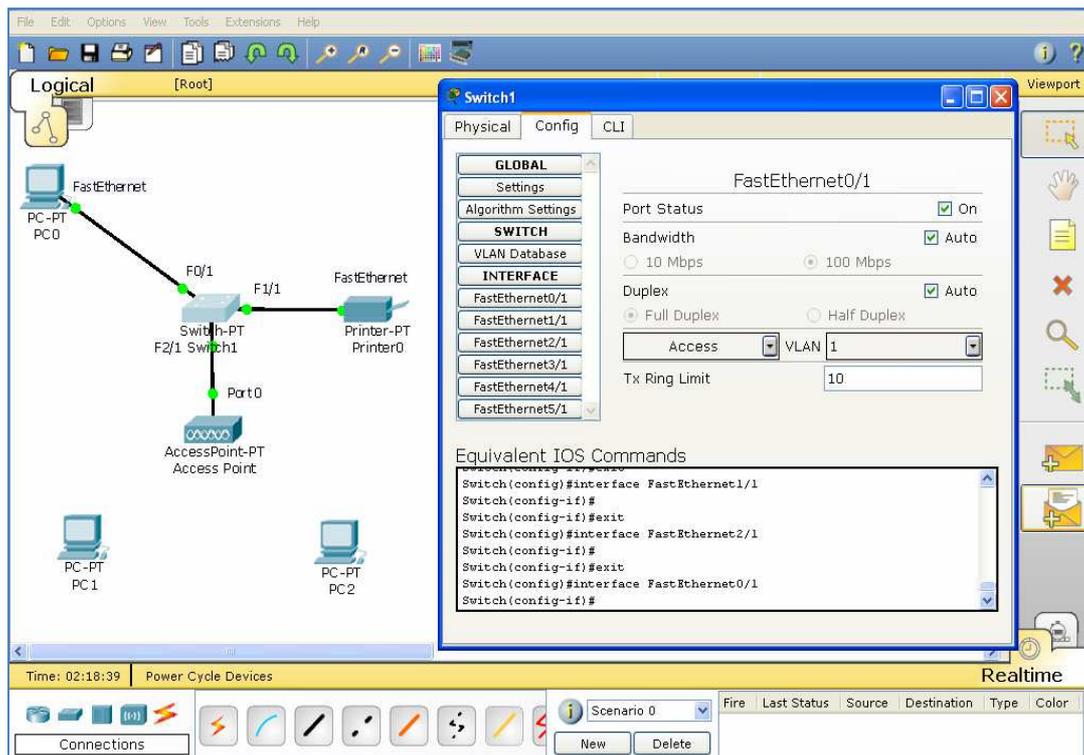


Figura 5.27: Verificación de puertos del Switch

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Procedemos a dar un clic sobre el AP y procedemos a verificar que todos los puertos que están conectados se encuentren encendidos y funcionando correctamente, como se puede observar en la figura 5.28.

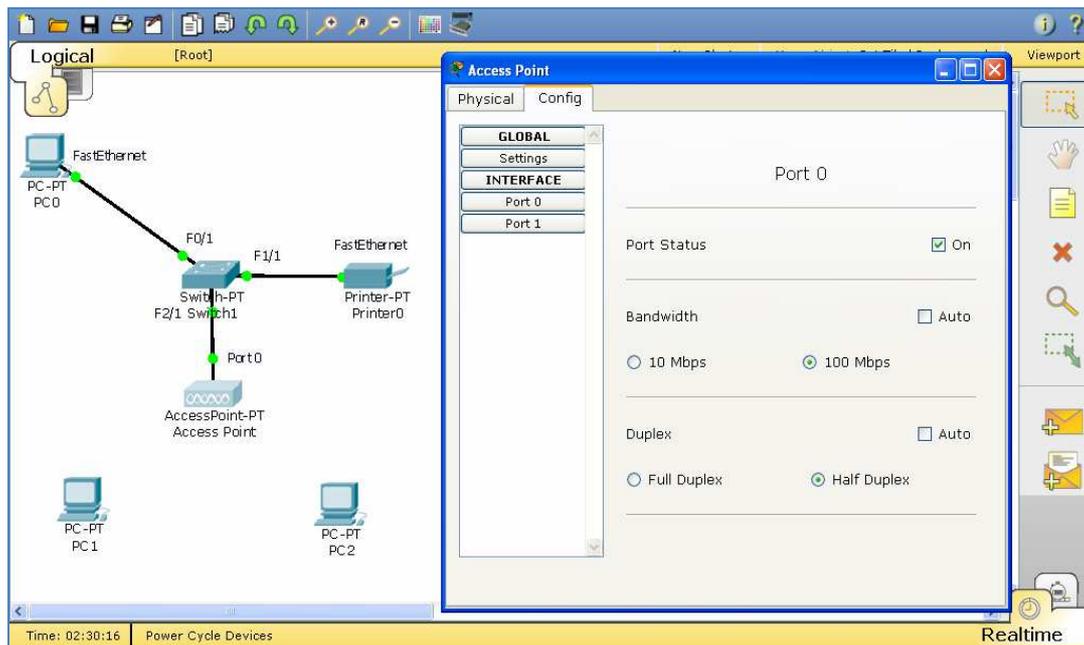


Figura 5.28: Verificación de puertos del AP

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Ahora damos clic en el Access Point y nos dirigimos a la pestaña **Config** y seleccionamos **Port 1** y procedemos a configurar el nombre de la red inalámbrica (SSID) que para efecto de esta práctica será **CISCO** y para evitar infiltraciones de otros usuarios a la red la protegemos con una contraseña **cisco1234**, como se observa en la figura 5.29.

Nota: Para proteger la red con una contraseña de autenticación, primero seleccionamos la opción **WPA-PSK** y ahí se nos habilita la opción **Passphrase** y colocamos la clave que debe tener mínimo 8 caracteres.

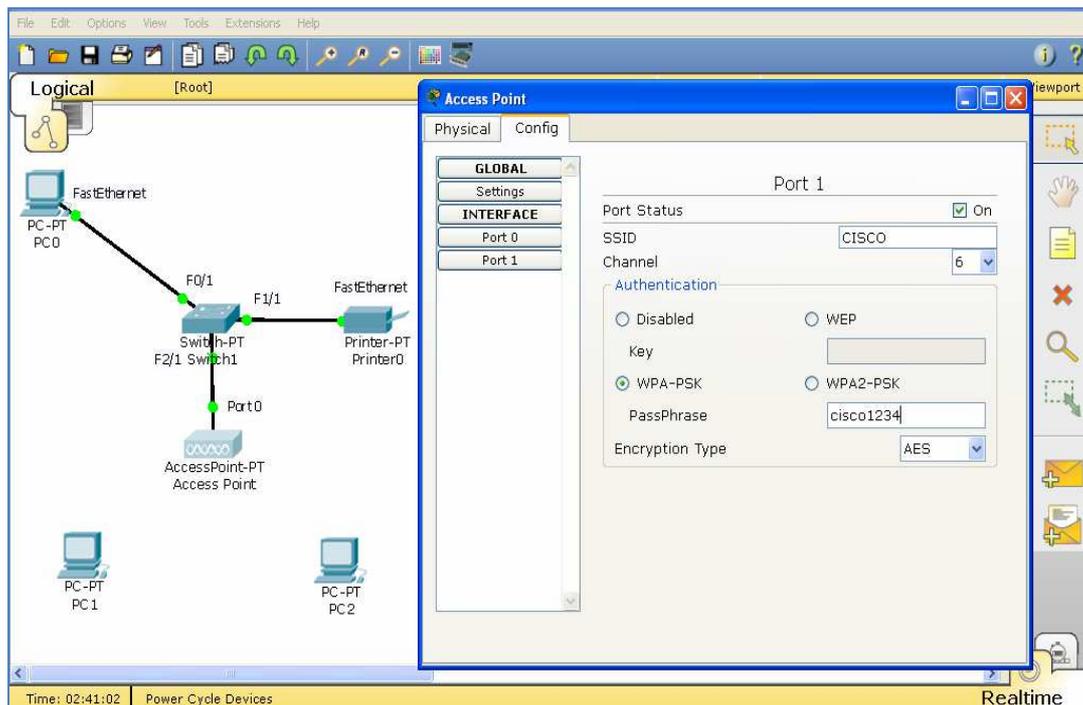


Figura 5.29: Configuración de SSID y Password para la red Wireless.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Luego para que las PC1 y PC2 puedan conectarse a la red wireless CISCO que acabamos de configurar en el AP, debemos primero quitarle la tarjeta NIC Fast Ethernet e insertarle la NIC inalámbrica.

Paso 1. Quitar la NIC Fast Ethernet de PC1 y PC2.

- Haga clic en la **PC** y luego en la ficha **Physical**.
- En la vista de dispositivos físicos se muestra una imagen del equipo PC. Haga clic en el botón de encendido para apagar el equipo PC.
- Quite la NIC Fast Ethernet. Para ello, arrástrela hacia la esquina inferior derecha de la ventana. La NIC se encuentra en la parte inferior de la máquina.

Paso 2. Instalar la NIC inalámbrica en PC1 y PC2.

- En **Modules**, busque Linksys-WMP300N y arrástrelo y colóquelo donde se encuentra la NIC Fast Ethernet.
- Vuelva a encender la alimentación.

Este proceso se lo realiza en ambas PC's para luego conectarlas a la red wireless CISCO.

Para lo cual, damos clic en la PC, nos dirigimos a la pestaña **Desktop**, luego a **PC Wireless** (Fig.5.30) y damos clic en la pestaña **connect** y aparece la redes inalámbricas disponibles, seleccionamos la red **CISCO** y damos clic en el botón **connect** (Fig.5.31) que está en la parte derecha y nos muestra la ventana de autenticación para acceder a la red solicitando la contraseña cisco1234 antes configurada en el AP, la digitamos en el espacio **Pre-Shared Key** y damos clic en connect. (Fig.5.32.)

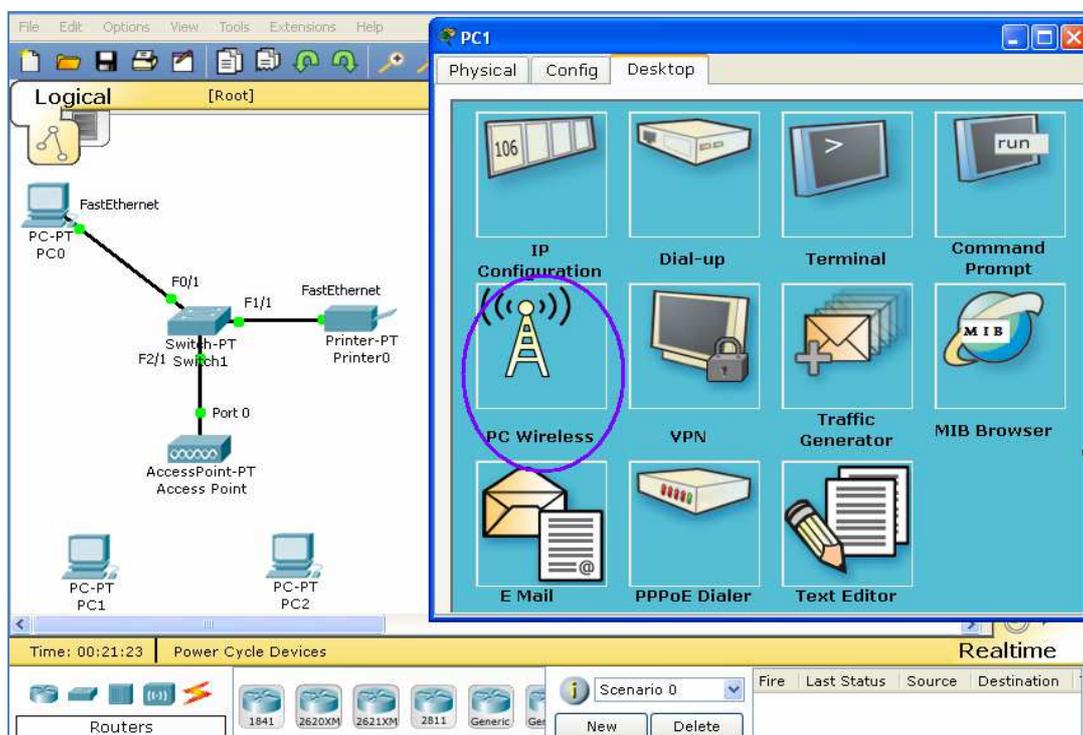


Figura 5.30: Ingreso a PC Wireless

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

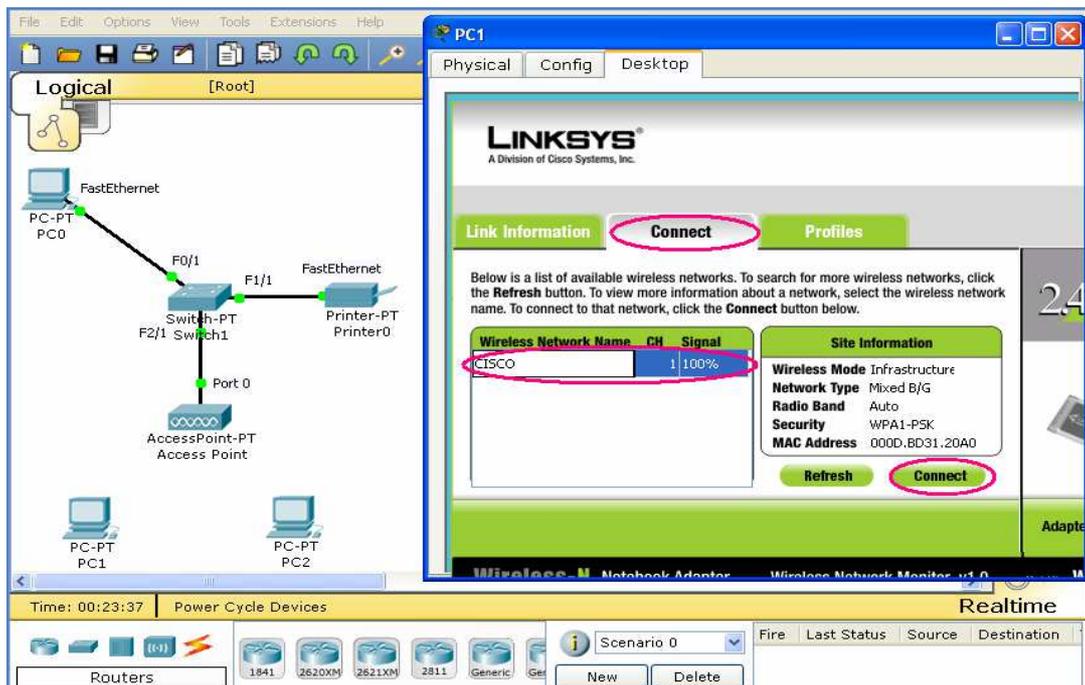


Figura 5.31: Selección de la red configurada en el AP
Fuente: Software Cisco *Packet Tracer* versión 5.3.0

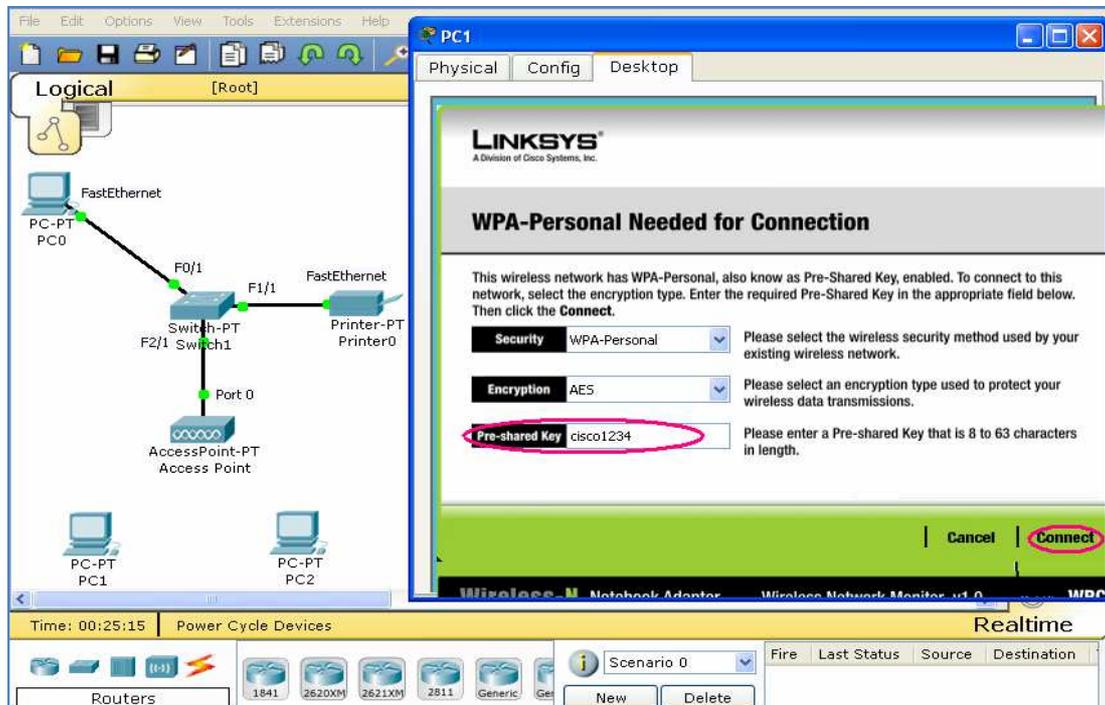


Figura 5.32: Digitación de la clave de acceso a la red.
Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Este proceso se lo realiza de igual manera en ambas computadoras PC1 y PC2 y al final se muestran las líneas de conexión wireless de forma exitosa entre cada una de las PC y el AP, como se muestra en la figura 5.33.

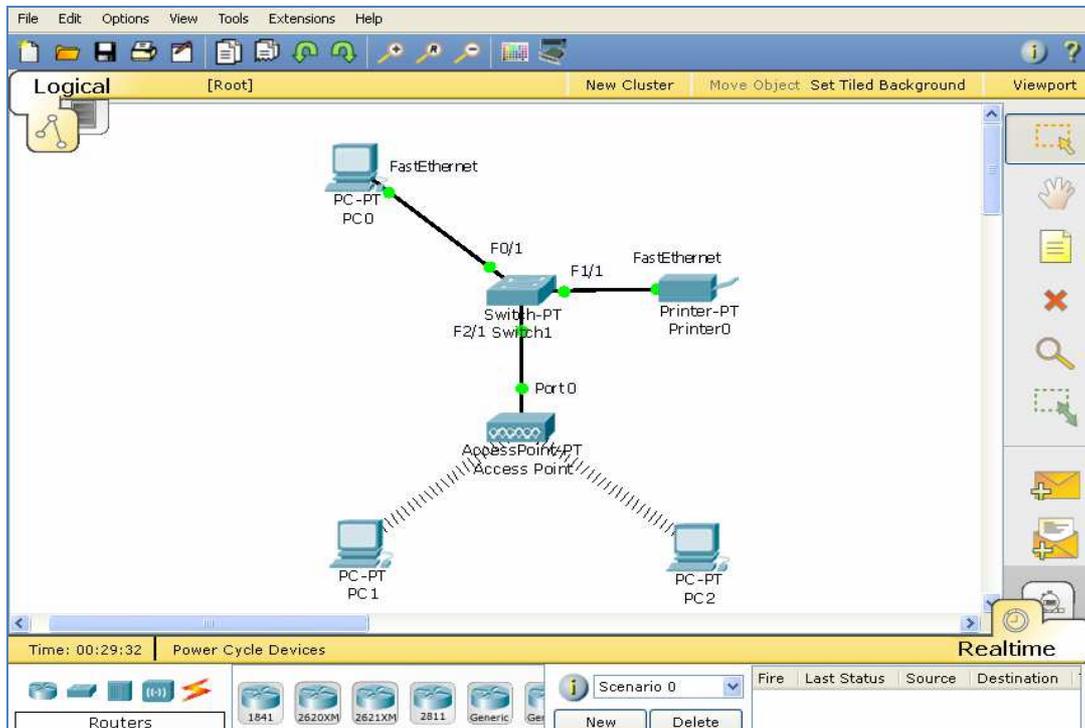


Figura 5.33: Computadoras conectadas al AP

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Empezamos a trabajar en modo de simulación. Ahora para transferir la información y comprobar que la conexión no tenga problemas se coloca un paquete simple señalando el lugar de origen y destino, en este primer escenario se va a comprobar la conexión entre la PC0 y la Impresora al enviar y recibir los datos, se observa en la figura 6.34 el trayecto del paquete PDU desde PC0 a la impresora, haciendo puente en el switch.

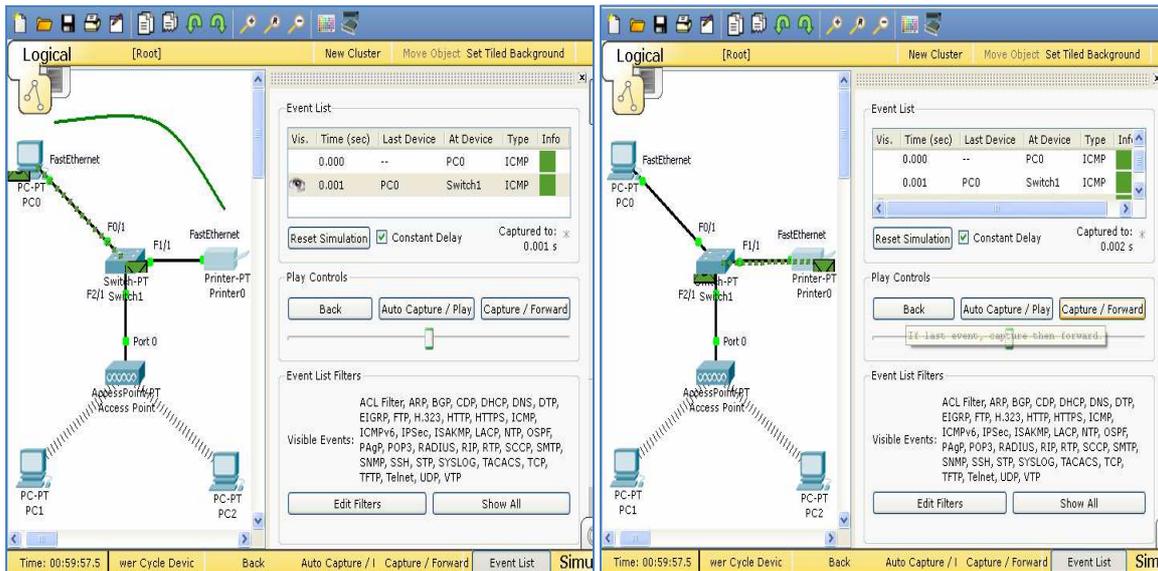


Figura 5.34: Transferencia de paquetes de PC0 a impresora.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Se puede observar claramente en la figura 5.35 la transferencia de paquetes desde el AP hacia la PC1 y PC2 sin obtener ningún inconveniente.

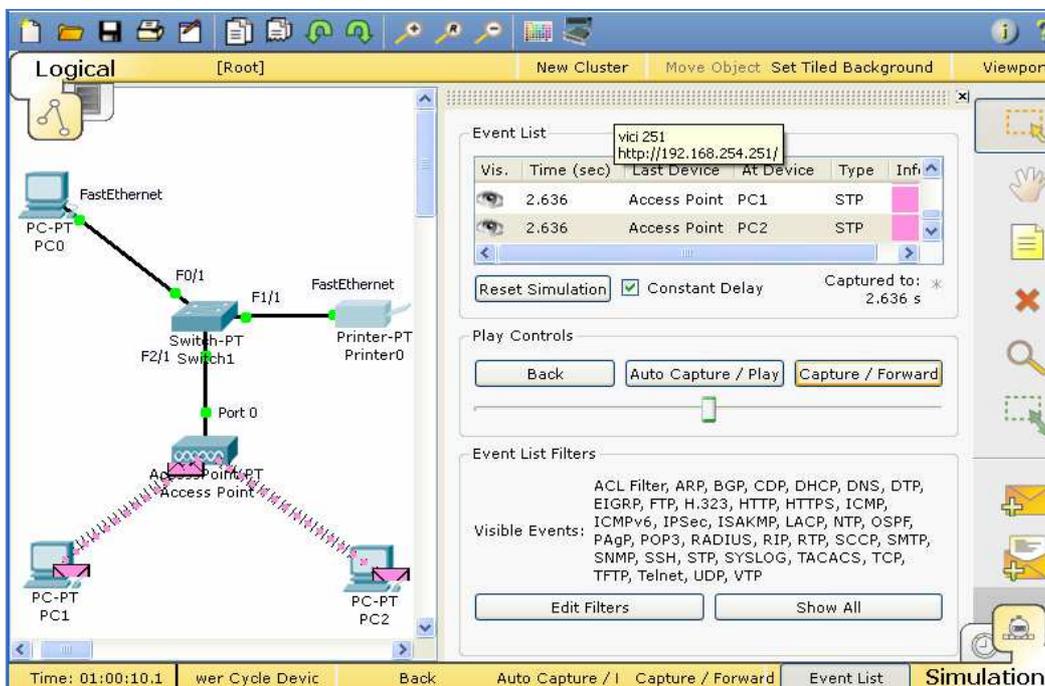


Figura 5.35: Transferencia de paquetes desde el AP hacia la PC1 y PC2.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

En la figura 5.36 se puede observar claramente que el paquete se traslada del switch 1 al Access Point sin obtener problemas y los detalles correspondientes al paquete de entrada y salida.

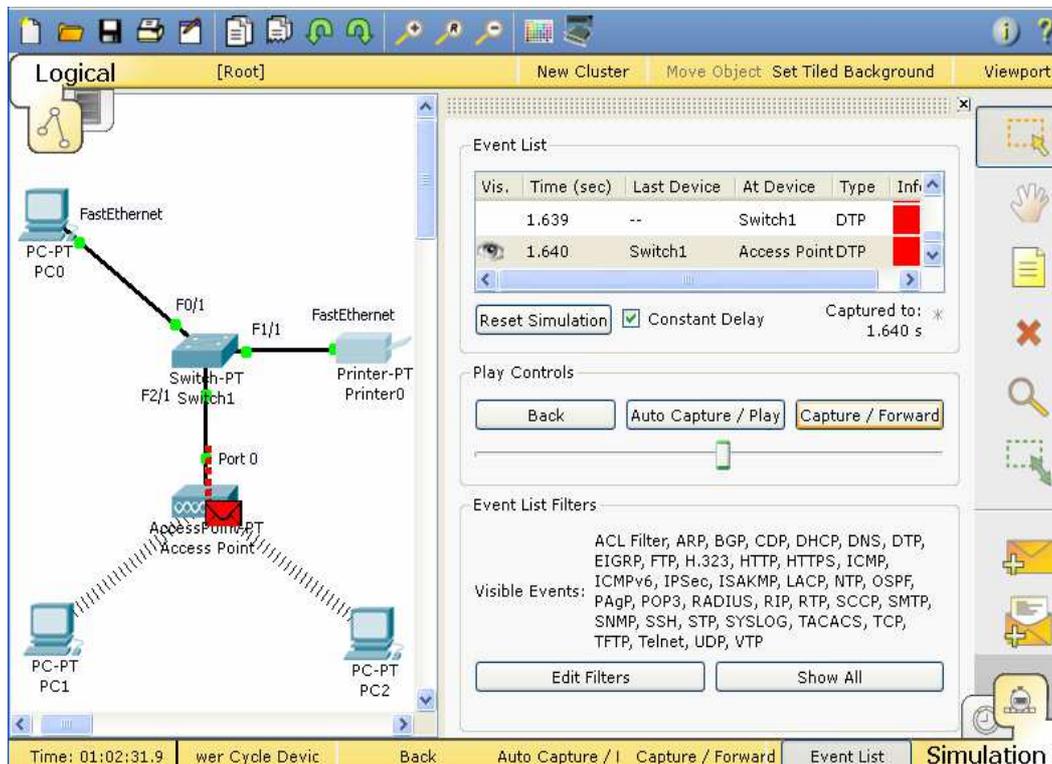


Figura 5.36: Transferencia de paquetes desde el switch hacia el AP

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

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 válida, como se puede observar en la figura 5.37.

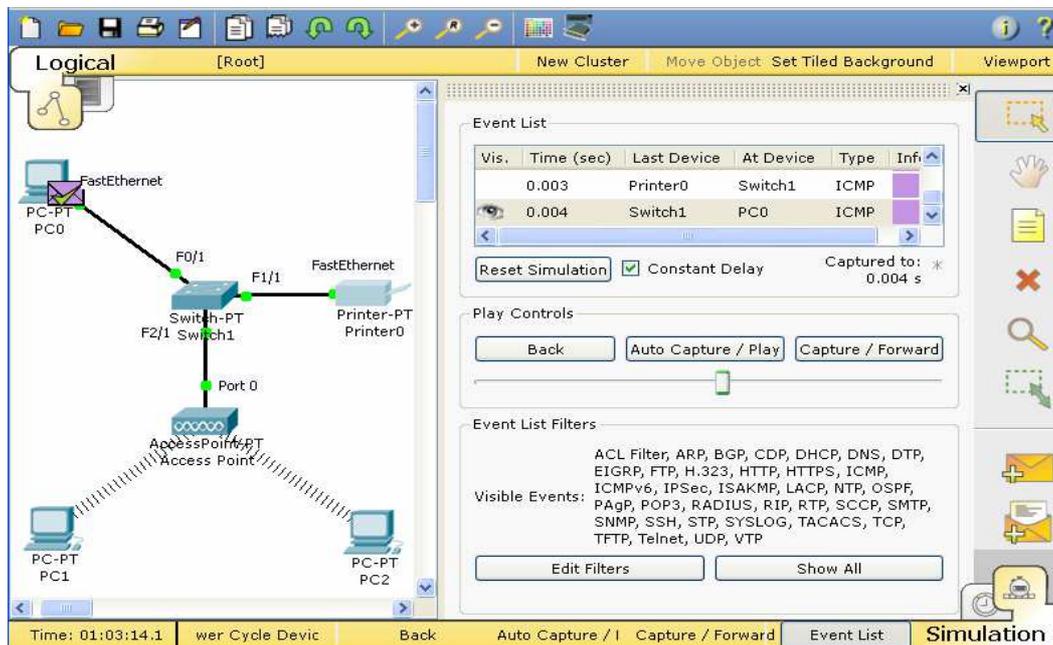


Figura 5.37: Transferencia de paquetes exitosa.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

➤ Análisis de resultados

- 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.
- En la figura 5.37 se puede observar claramente que el paquete regreso al punto de partida, significando que la información fue entregada sin ningún problema a su destino.

➤ Conclusiones

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

5.4. Practica # 4: Realizar una red LAN en la que se observa las diferentes capas del modelo OSI

➤ **Objetivos:**

- 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:**

Iniciamos el software *Packet Tracer* versión 5.3.0 y colocamos los siguientes dispositivos en el espacio de trabajo: En esta red LAN intervienen 6 CPU's, 1 switch, 1 hub, 1 impresora y 1 Access Point.

Las configuraciones son idénticas a la de las prácticas anteriores, conectamos todos los equipos, asignamos las direcciones IP que se muestra en la tabla 5.1 a todas las computadoras, incluso la PC que está conectada de forma inalámbrica mediante un Access Point también se le asigna una dirección IP para que se encuentre lógicamente en la misma red LAN.

TABLA DE DIRECCIONAMIENTO IP		
EQUIPO	DIRECCION IP	MASCARA DE SUBRED
PC0	192.168.10.1	255.255.255.0
PC1	192.168.10.2	255.255.255.0
PC2	192.168.10.3	255.255.255.0
PC3	192.168.10.4	255.255.255.0
PC4	192.168.10.6	255.255.255.0
PC5	192.168.10.7	255.255.255.0
IMPRESORA	192.168.10.5	255.255.255.0

Tabla 5.1: Direccionamiento IP

Se procede a verificar la conectividad, todos los puertos deben estar activos en el switch, hub, AP, y realizamos un ping de cualquiera de las PC hacia otra incluso la PC que está conectada de forma inalámbrica, como se observa en la figura 5.38.

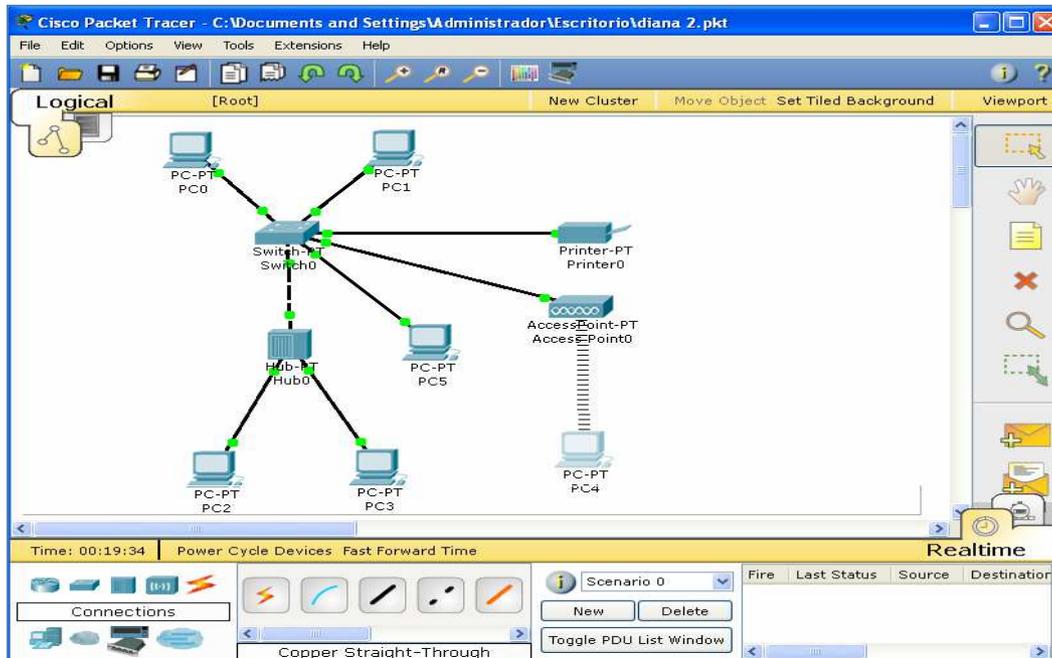


Figura 5.38: Red LAN – Colocación y configuración de dispositivos

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Se coloca un paquete de datos 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 PC4 y la PC1 al enviar y recibir los datos, como se observa en la figura 5.39

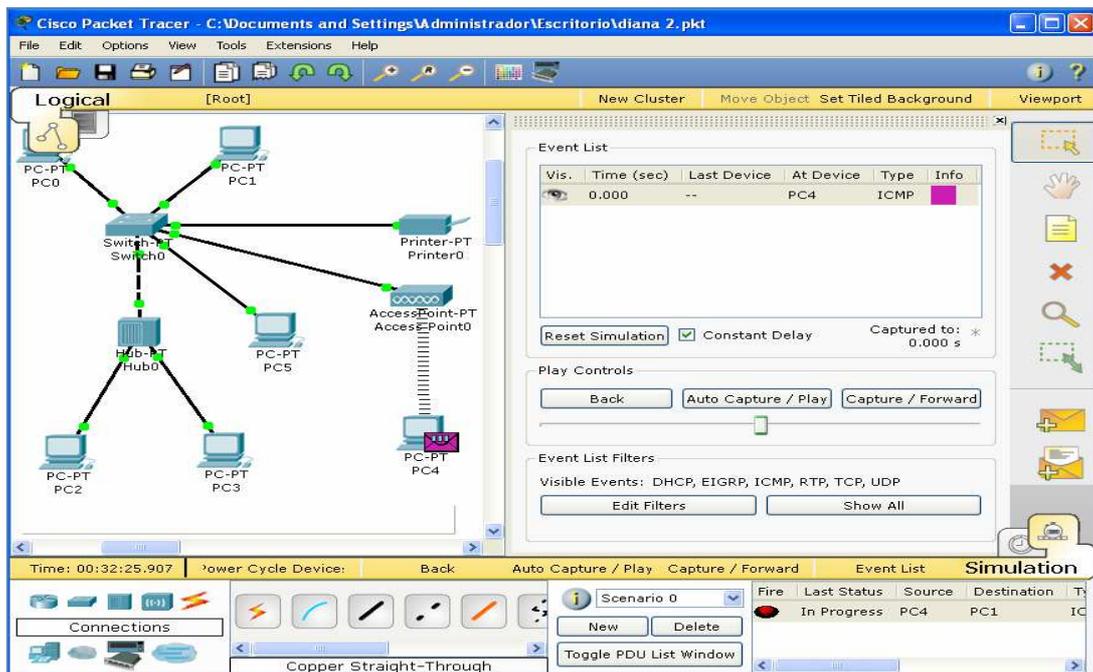


Figura 5.39: Verificación de paquete de datos entre PC1 y PC4.

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Procederemos con la respectiva simulación enviando un paquete y comprobando que la conexión correspondiente este funcionando, se puede observar las diferentes capas por la que pasa el paquete para ser enviado y su respectivo comportamiento, 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, como se observa en la figura 5.40

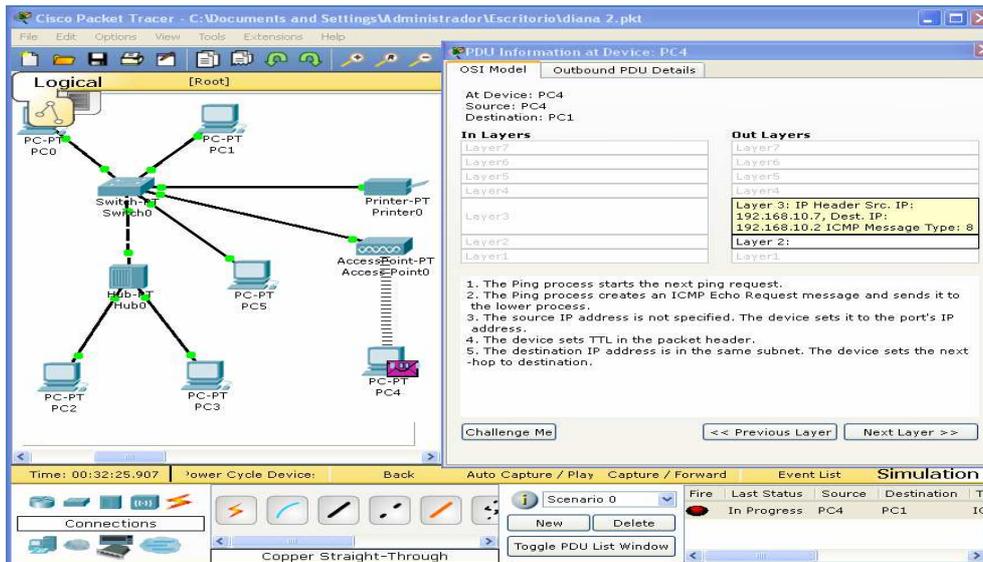


Figura 5.40: Visualización capa 3 del modelo OSI

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

En este caso el paquete se encuentra en la capa dos, en la cual se le debe encapsular al paquete para que pueda pasar a la capa uno, como se observa en la figura 5.41

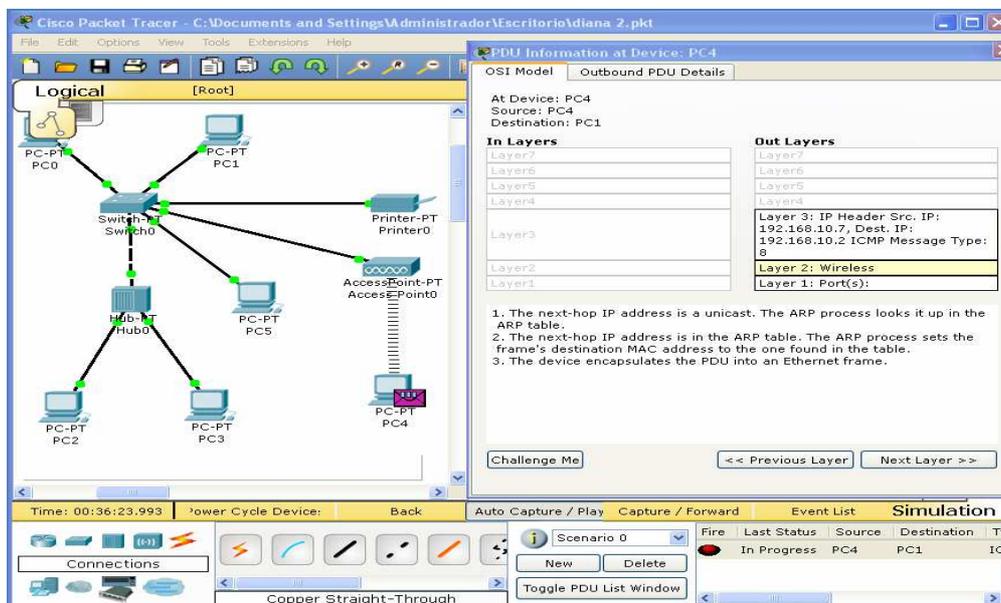


Figura 5.41: Visualización capa 2 del modelo OSI

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Cuando el paquete se encuentra en la mitad del camino podemos observar que intervienen la capa 1 y 2 del modelo OSI, y se visualiza el puerto FastEthernet y la dirección MAC que se asocian en este proceso, como se observa en la figura 5.42.

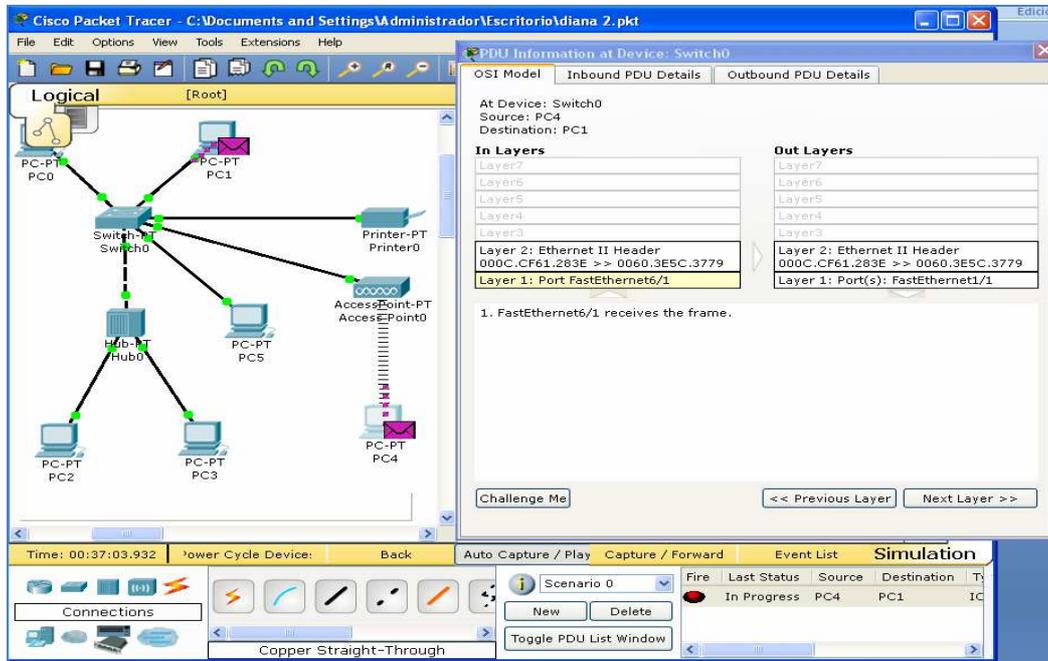


Figura 5.42: Visualización de capa 1,2 y 3 del modelo OSI

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

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 válida, como se observa en la figura 5.43

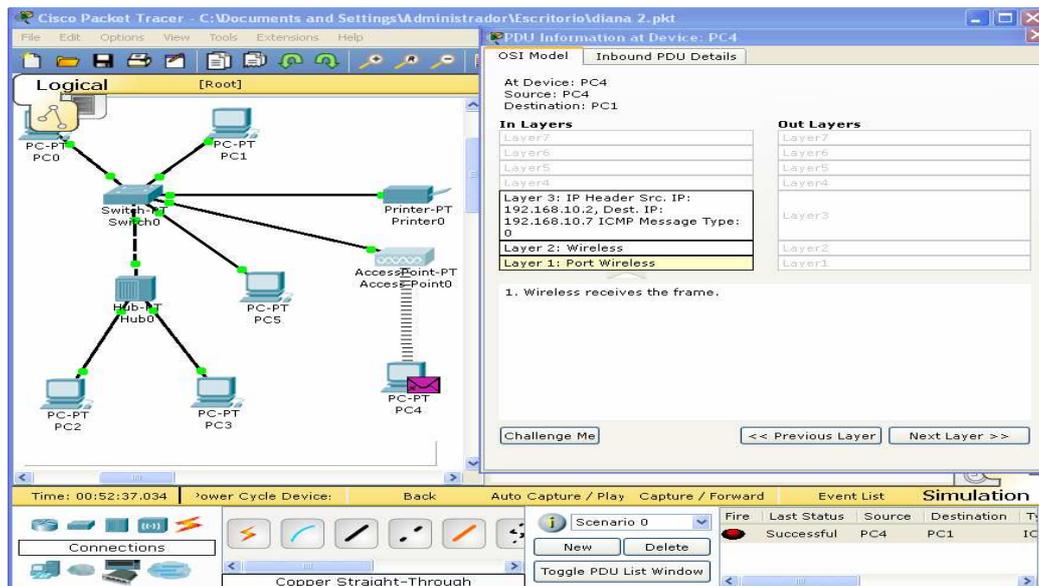


Figura 5.43: Visualización de capa 1, 2 y 3 del modelo OSI

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

➤ **Análisis de resultados**

- Se puede observar en la simulación que el Switch utilizado trabaja hasta en una capa 2 del modelo OSI
- Se puede verificar el comportamiento del paquete en las CPU's observando claramente como el paquete llega hasta una capa 3 del modelo OSI.
- 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**

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

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

5.5. Practica # 5: Conexión de varios dispositivos de inter conectividad para una red

➤ **Objetivo:**

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

➤ **Procedimiento:**

En esta práctica conectaremos varios dispositivos entre los cuales se tendrá 2 PC con tarjeta de red inalámbrica, 4 PC normales, 1 impresora, 1 Access point, 1 bridge, 1 Switch y 2 routers.

Cabe recalcar que existen dos aspectos nuevos que no se han visto en las anteriores prácticas, como son la conexión entre el router 0 con el Switch que se hace mediante fibra óptica; este tipo de material no se utiliza siempre para la conexión de estos dos equipos pero en esta práctica se utiliza este medio de transmisión para dar a conocer que el simulador *Packet Tracer* posee todas las características para simular una topología de red similar a la realizada en una empresa.

Por último tenemos la conexión entre los router 0 y router 1 que se hace mediante cable serial DCE(conexión WAN), en este caso cuando se vaya a conectar 2 routers para simular una red WAN siempre se va a utilizar este tipo de cable serial ya sea DCE o DTE.

Verificamos que todos los puertos de los equipos estén conectados y funcionando correctamente, como se observa en la figura 5.44

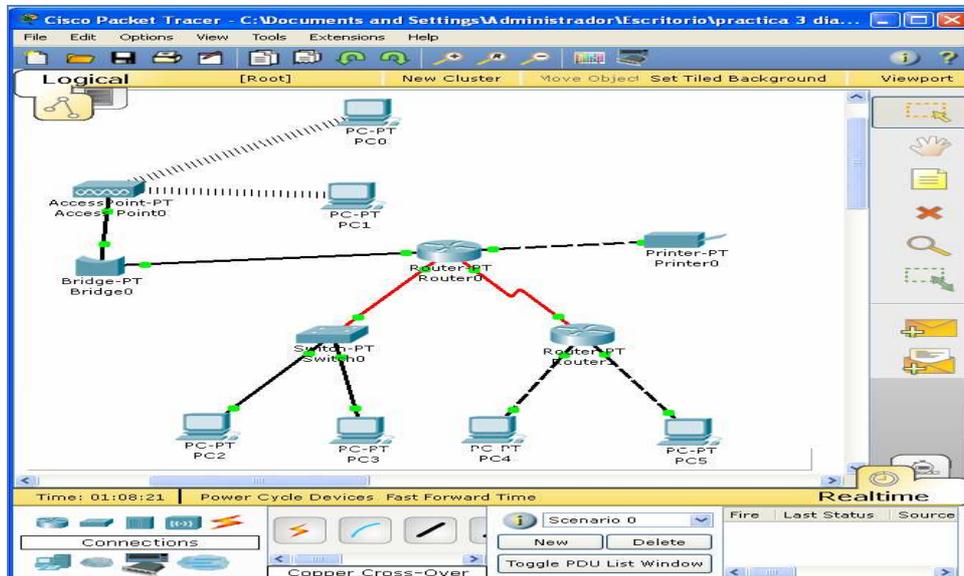


Figura 5.44: Conexión de equipos

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

Primero debemos configurar la dirección IP y su respectiva máscara de red para todas las PC's y la impresora con los datos que se indican en la tabla 5.2, en este caso configuramos también la opción del Gateway para las PC's, como se observa en la figura 5.45.

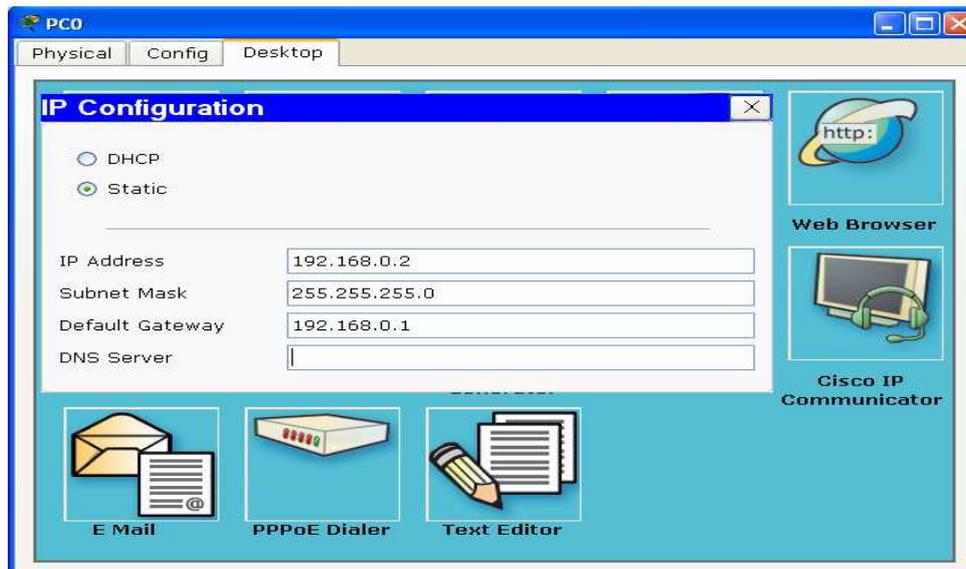


Figura 5.45: Direccionamiento IP de los equipos

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

TABLA DE DIRECCIONAMIENTO IP			
EQUIPO	DIRECCION IP	MASCARA DE SUBRED	GATEWAY
PC0	192.168.0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.3.2	255.255.255.0	192.168.3.1
PC3	192.168.3.3	255.255.255.0	192.168.3.1
PC4	192.168.1.2	255.255.255.0	192.168.1.1
PC5	192.168.2.2	255.255.255.0	192.168.2.1
IMPRESORA	192.168.10.5	255.255.255.0	

Tabla 5.2: Direccionamiento IP de los equipos

Procedemos a configurar los routers, damos clic en el router 0, seleccionamos las pestaña **Config** y ubicamos el puerto al que debemos asignar la dirección IP y la máscara de subred correspondiente, de igual manera hacemos con el router 1 como se observa en la figura 5.46.

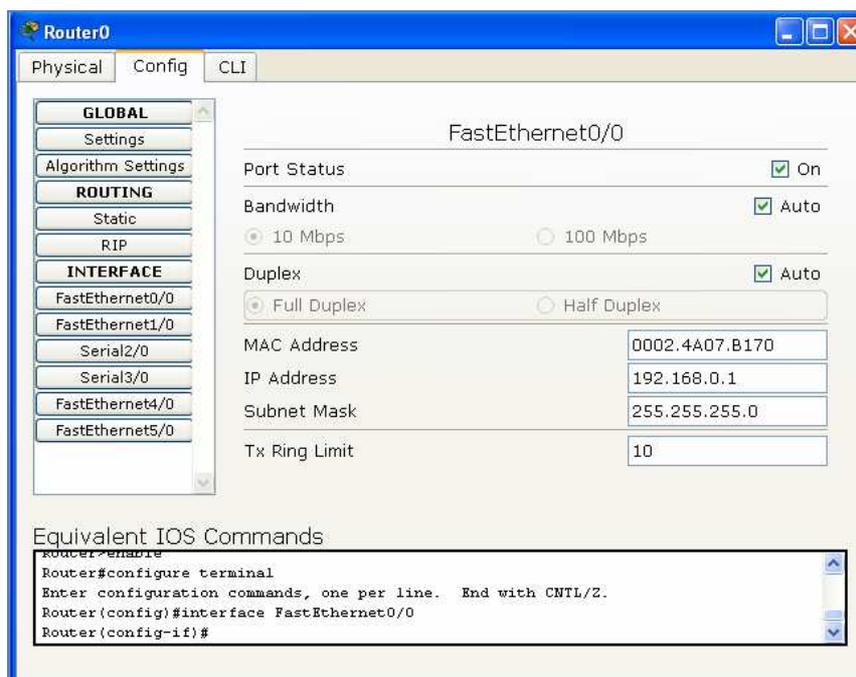


Figura 5.46: Configuración de los Routers

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

ROUTER 0		
Puerto	Dirección IP	Mascara de subred
FastEthernet 0/0	192.168.0.1	255.255.255.0
FastEthernet 1/0	192.168.5.1	255.255.255.0
FastEthernet 4/0	192.168.3.1	255.255.255.0
Serial 2/0	10.0.0.2	255.255.255.252
ROUTER 1		
Puerto	Dirección IP	Mascara de subred
FastEthernet 0/0	192.168.1.1	255.255.255.0
FastEthernet 1/0	192.168.2.1	255.255.255.0
Serial 2/0	10.0.0.1	255.255.255.252

Tabla 5.3: Direccionamiento IP de los Routers

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.

Se puede observar claramente que con la simulación correspondiente el paquete se va trasladando, en este caso, de la PC0 al Access Point comprobando de esta manera que la conexión se ha establecido correctamente.

Así mismo se observa en la parte derecha los protocolos que se están utilizando y los equipos que intervienen, como se observa en la figura 5.47

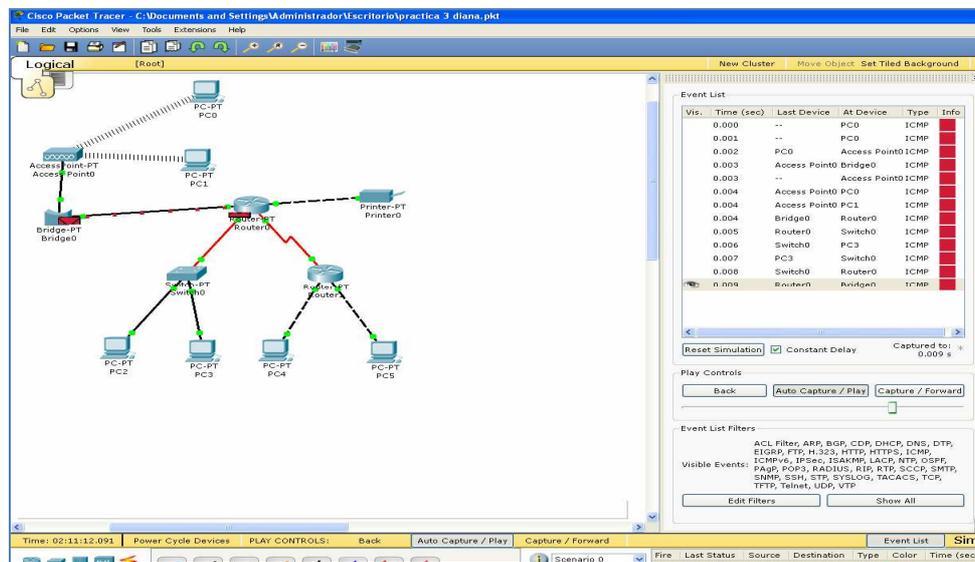


Figura 5.47: Transferencia de datos visualización de protocolos

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

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 válida, 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, como se observa en la figura 5.48

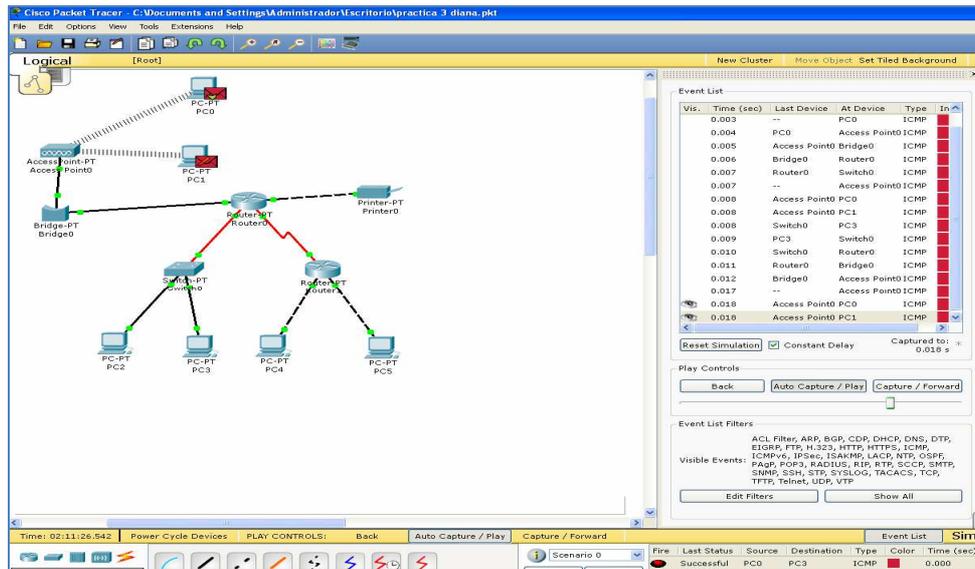


Figura 5.48: Finalización de transferencia de paquete

Fuente: Software Cisco *Packet Tracer* versión 5.3.0

➤ Análisis de resultados

- En la grafica 5.48 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.
- En nuestro caso se conectara con un cable serial DCE V.35 cuando se conecta dos ruteadores.
- 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

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

- Con la simulación realizada se cumplieron los objetivos requeridos transmitiendo datos por todos los dispositivos conectados en la red.
- En las gráficas de simulación se pueden observar muy claramente que todos los paquetes se trasladaron sin ningún problema por toda la red.
- En la figura 5.48 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. CONCLUSIONES

Después de haber realizado el estudio respectivo para la aplicación del simulador de redes *Packet Tracer* como herramienta de carácter práctico para el programa académico de la asignatura de Telemática I de la carrera de Ingeniería de Telecomunicaciones podemos concluir lo siguiente:

El resultado obtenido al realizar este proyecto de tesis fue proveer a los laboratorios de Telecomunicaciones de la Facultad Técnica de un software para simular redes de datos y de comunicaciones en tiempo real, facilitando a los estudiantes el aprendizaje del contenido de la materia de Telemática I y la interacción con el diseño de redes que coadyuvan el desarrollo profesional.

El Simulador *Packet Tracer* 5.3.0, es una herramienta muy útil para el laboratorio de Telecomunicaciones, 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 emplearlas en la actualidad a nivel mundial, debido a que 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 y de esta manera hacer las correcciones necesarias y verificar si resulta viable su respectiva implementación.

Para ejecutar este proyecto de investigación fue necesario analizar detalladamente el contenido de la asignatura Telemática I y de esta manera poder detectar las áreas que necesitaban apoyo práctico.

Para ejecutar el software simulador de redes *Packet Tracer* en los laboratorios de Telecomunicaciones fue necesario instruirnos en el manejo adecuado de la herramienta, para lo cual realizamos las investigaciones respectivas obteniendo un resultado satisfactorio.

Una vez aprendido el manejo completo del software, empezamos a crear topologías de red mediante la selección de los dispositivos de interconexión y su respectiva ubicación en un área de trabajo, utilizando la interfaz gráfica de *Packet Tracer*, para así hacer demostraciones y prácticas explicando la importante utilidad de esta herramienta para simular redes de datos en tiempo real, siendo un aporte sustancial para la integración global del conocimiento de los estudiantes.

En síntesis este proyecto de investigación sobre la factibilidad de la aplicación del software *Packet Tracer* mediante prácticas para así complementar el aprendizaje de la materia Telemática I fue culminado con éxito, cumpliendo a cabalidad lo mencionado en los *items* anteriores, para de esta manera obtener como resultado una mejor asimilación del conocimiento teórico.

Las conclusiones detalladas anteriormente demuestran que se cumplieron todos los objetivos específicos establecidos para este proyecto y que el conjunto de los mismos ha permitido cumplir el objetivo general planteado para resolver el problema que se determinó inicialmente.

7. RECOMENDACIONES

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.

Se recomienda que se sigan elaborando tesis de este tipo en el Laboratorio de Telecomunicaciones, de esta forma los alumnos que ya terminamos nuestros estudios dejamos un aporte sustancial para nuestros compañeros que continúan en esta carrera.

Es importante actualizar la versión del software *Packet Tracer*, debido a que Cisco System avanza a pasos agigantados a nivel mundial y trae consigo muchas mejoras e incomparables beneficios en el desarrollo de simuladores de redes de datos.

8. GLOSARIO

ARP: *Address Resolution Protocol* o Protocolo de resolución de direcciones.

CCITT: Consultative Committee for International Telegraphy and Telephony ó Comité Consultivo Internacional Telegráfico y Telefónico.

CD: Committee Draft.

CDP: *Cisco Discovery Protocol* o Protocolo de descubrimiento de Cisco.

CLI: *Command Line Interface* o Interfaz de Línea de Comandos.

CSMA/CD: Carrier Sense Multiple Access ó Acceso Múltiple por Detección de Portadora y detección de Colisiones.

DHCP: Protocolo de configuración dinámica de host.

DIS: Draft International Standard.

DNS: *Domain Name System* o Sistema de nombres de dominio.

DSSS: Direct-Sequence Spread Spectrum.

DTP: *Dynamic Trunking Protocol*.

EIGRP: *Enhanced Interior Gateway Routing Protocol* o Protocolo de enrutamiento de gateway e interior mejorado.

HDLC: *High-Level Data Link Control* o Control de enlace síncrono de datos.

HTTP: *HyperText Transfer Protocol*.

IAB: Internet Architecture Board.

IBM: International Business Machines.

ICMP: *Internet Control Message Protocol* o Protocolo de Mensajes de Control de Internet.

IDU: Interface Data Unit ó Unidad de Datos de Interfaz.

IETF: Internet Engineering Task Force.

IOS: *Internetwork Operating System* o Sistema Operativo de Interconexión de Redes.

IP: Protocolo de Internet.

IPv6: Protocolo de Internet versión 6.

IS: International Standard

LAN: *Local Area Network* o Red de Area Local.

LLC: Control de Enlace Lógico.

MAC: Medio Access Control ó Control de Acceso al Medio.

MACs: *Media Access Control* o Control de Acceso al Medio.

MAN: *Metropolitan Area Network* o Red de Area Metropolitana.

MIMO: Multiple-input Multiple-output ó Múltiple entrada múltiple salida

NAT: *Network Address Translation* o Traducción de Direcciones de Red.

NS: Lotus Notes.

OFDM: Orthogonal Frequency Division Multiplexing ó Multiplexación por División de Frecuencia Ortogonal.

OSI: *Open System Interconnection*.

OSPF: *Open Shortest Path First*.

P2P: Peer to Peer ó Punto a Punto.

PAgP: *Port Aggregation Protocol*.

PCI: Protocol Control Information ó Protocolo de Control de la Información.

PDA: Asistentes Digitales Personales.

PDU: *Packet Data Unit*.

PPP: *Point to point Protocol* o Protocolo Punto a Punto.

QoS: Calidad de Servicio.

RDSI: Red Digital de Servicios Integrados.

RF: Radiofrecuencia

RIP: *Routing Information Protocol* o Protocolo de Enrutamiento de Información.

RSTP: *Rapid Spanning Tree Protocol*.

RSTP: *Rapid Spanning Tree Protocol*.

SAP: Service Access Point ó Punto de Acceso al Servicio.

SDU: Service Data Unit ó Unidad de Datos de Servicio.

SSH: *Secure Shell* o Capa segura.

STP: *Shielded Twisted Pair* o Cable par trenzado apantallado.

TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet.

TCP: *Transport Control Protocol*.

TELNET: *TELEcommunication NETwork*.

TFTP: *Trivial File Transfer Protocol* o Protocolo de Transferencia de Archivos Trivial.

UDP: *User Datagram Protocol* o Protocolo de Datagrama de Usuario.

UDP: *User Datagram Protocol*.

UTP: Unshielded twisted pair ó Cable de Par Trenzado.

VoIP: Voice over Internet Protocol ó Voz sobre Protocolo de Internet.

VTP: *VLAN Trunking Protocol*.

WAN: *Wide Area Net work* o *Red de Area Extensa*

WWW: World Wide Web.

XP: *Xtreme Programmig*.

9. BIBLIOGRAFIA

Academy, C. 3. (26 de 03 de 2010). *Switching VLAN and Wireless*. Recuperado el 30 de 09 de 2011, de Switching VLAN and Wireless:

<http://cisco.net.es/spanish/ccna3.html>

ACADEMY, C. C. (22 de 03 de 2011). *Cisco.net*. Recuperado el 08 de 08 de 2011, de Cisco.net: <http://cisco.net.es/spanish/ccna1.html>

Anónimo. (11 de 02 de 2010). *Redes de datos LAN*. Recuperado el 12 de 08 de 2011, de Redes de datos LAN:

http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan.pdf

Anonimo2. (14 de 05 de 2009). *Manual de Packet Tracer*. Recuperado el 22 de 10 de 2011, de Manual de Packet Tracer:

<http://fcp.unach.mx/manuales/download/packet4.pdf>

Carrasco, I. (18 de 02 de 2010). *Solo Redes*. Recuperado el 30 de 09 de 2011, de Tipo de conexión de redes: <http://soloredes-izhela.blogspot.com/2010/02/tipos-de-conexion-de-redes.html>

Cisco Packet Tracer. (s.f.). Recuperado el 24 de Julio de 2011, de Cisco:
http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

Fire, A. (12 de 08 de 2003). *Topologías de Redes*. Recuperado el 18 de 09 de 2011, de Topología Estrella:
<http://www.angelfire.com/cantina/alegre0/topologiaestrella.htm>

Introducción a Packet Tracer. (s.f.). Recuperado el 22 de Julio de 2011, de Comunicación de Datos I:
<http://www.udb.edu.sv/Academia/Laboratorios/electronica/Comunicacion%20de%20Datos%20I/guia4CDAI.pdf>

Kioskea. (26 de 10 de 2008). *Topología de redes*. Recuperado el 15 de 09 de 2011, de Topología Bus: <http://es.kioskea.net/contents/initiation/topologi.php3>

Manual de Packet Tracer 4.0. (s.f.). Recuperado el 01 de Agosto de 2011, de <http://fcp.unach.mx/manuales/download/packet4.pdf>

Salazar, M. (s.f.). *Cisco Networking Academy*. Recuperado el 22 de Julio de 2011, de http://gtts.ehu.es/TWiki/bin/viewfile/Main/MoisesSalazarMaldonado?rev=1;filename=1.7.1_Desaf%EDo_de_integraci%F3n_de_habilidades__Introducci%F3n_a_

Stadler, D. (2008). *Desarrollo de Guías de Laboratorio Virtual de Fundamentos de Redes utilizando el software Packet Tracer*. Recuperado el 01 de Agosto de 2011, de ESPE-Escuela Superior Politécnica del Ejercito:
<http://www3.espe.edu.ec:8700/bitstream/21000/129/1/T-ESPE-017998.pdf>