FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

INVESTIGACIÓN, GENERACIÓN Y DESARROLLO DE UN DOCUMENTO GUÍA PARA LABORATORIOS DE LA MATERIA DE REDES LAN DE LA ESCUELA DE TECNOLOGÍAS EN LA UNIVERSIDAD DE LAS AMÉRICAS

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Tecnólogo en Redes y Telecomunicaciones.

Profesor Guía

Ing. Henry Burbano

Autor

Roberto Carlos Herrera Tamayo

Año

2015

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

…….

Henry Burbano

171147608 - 3

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

…….

Roberto Carlos Herrera Tamayo

171889506-1

AGRADECIMIENTOS

Deseo agradecer a DIOS por la oportunidad de permitirme estar en esta instancia tan importante en mi vida, toda la fuerza, valor y constancia para afrontar todos y cada uno de los difíciles momentos que he atravesado.

A mi madre, Mariana Tamayo, a mi padre, Carlos Herrera, quienes me apoyaron en todo momento, sin condiciones, haciéndome una persona con buenos valores y principios.

A mi querido bebe ha sido de gran inspiración para avanzar firmemente en cada paso de mi camino sin titubear.

También quiero agradecer a todas las personas que me han dado su mano para cumplir mi meta como amigos, profesor guía y autoridades de este prestigioso establecimiento.

.

DEDICATORIA

Dedico este trabajo a Dios quien es el que me dio sabiduría para llegar a esta instancia de mi vida y brindándome fuerzas en cada uno de los momentos
en los que necesite.

A mi querida novia y mi hija Eliana MellissaHerrera Valencia quienes fueron mi fortaleza y también base muy importante sirviéndome de inspiración en cada instante.

A mis hermanos que supieron apoyarme en cada momento y acompañándome en mis malos y buenos momentos.

A todas esas personas que con sus consejos hicieron de mí una persona más humilde pero fuerte para llegar a esta instancia de mi vida.

RESUMEN

Hoy en día las REDES LAN han ido creciendo y evolucionando de manera veloz y ágil por ende también su complejidad y exigencia por lo que conviene estar preparado ante cualquier circunstancia con soluciones amplias y eficaces. Por lo cual la elaboración de este documento facilitará administración y control de la de cualquier RED LAN con las respectivas normas y estándares mediante herramientas de fácil uso como Subnetting / VLSM y sin necesidad de inversiones económicas elevadas mejorando la calidad de servicio que se brinda a los usuarios y rendimiento de equipos evitando problemas de congestión por mal uso de los dispositivos.

En el presente trabajo se realiza el uso del software packet tracert por sus cualidades y características que goza para configurar equipos virtuales y así dar a conocer los tipos de comandos, dominar su manejo, permitir conectar equipos, comprobar conectividad y configuraciones remotas sin necesidad de una conexión física.

Además se contribuye con conocimientos de ventajas de implementar una red inalámbrica en lugar de una red cableada realizándolas de tal manera que se pueda comprobar y la persona de manera clara y evidente.

Palabras clave: Red LAN. Subnetting, VLSM, laboratorio, comandos.

ABSTRACT

Today the LAN NETWORKS have been growing and evolving in a fast and agile hence also its complexity and requirement so you should be prepared for any circumstance comprehensive and effective solutions.

The preparation of this document will facilitate the management and control of any LAN NETWORK with the respective rules and standards through easy to use tools without high financial investment by improving the quality of service users are provided and performance equipment avoiding congestion by misuse of the devices.

In this paper the use of the software packet tracert for their qualities and characteristics that enjoys to configure virtual machines and to make known the types of commands, dominate its management, allowing to connect equipment, verify connectivity and remote configurations without requiring performed physical connection.

Furthermore it contributes to knowledge of advantages of implementing a wireless network instead of a wired performing them so that the person can check and clear and conspicuous manner.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

Este proyecto se desarrolla con el objetivo de dar una herramienta de trabajo al docente de la institución y a la vez dotar al alumno de una guía para realizar las prácticas del laboratorio de Redes LAN que se presentarán a continuación.

Las prácticas a desarrollarse servirán de ayuda para fortalecer el conocimiento de otras materias y también serán útiles para desenvolverse en el ámbito laboral, ya que los laboratorios presentados se los realizó a la par con la elaboración del presente Trabajo de Titulación.

CAPITULO I

1. Elaboración de cable directo, cable cruzado y verificación de su funcionamiento en el simulador y PC's**.**

1.1. OBJETIVO GENERAL

Elaborar un cable de red cruzado, directo según las normas TIA/EIA 568A Y TIA/EIA 568B con la respectiva verificación de su funcionamiento en el simulador y PC's.

1.2. OBJETIVOS ESPECÍFICOS

- Conocer las estándares de crimpado según las normas TIA/EIA 568A Y TIA/EIA 568B.
- Realizar la comprobación del cable de red elaborado por el estudiante mediante testeo de calidad.
- Conocer cada uno de los procedimientos para elaborar el laboratorio.

1.3. DESCRIPCIÓN DE EQUIPOS / HERRAMIENTAS / SOFTWARE / MATERIALES

1.3.1. PROVISTOS POR LA UNIVERSIDAD

- Dos computadores
- Simulador de Packet Tracer.

1.3.2. PROVISTOS POR EL ESTUDIANTE

- Conector RJ-45 en categoría 5 y categoría 6
- Protector de conectores
- Tijeras
- Estilete
- Pinza cortadora de cable
- Cable de red UTP.
- Cable de red categoría 5 y categoría 6
- Crimpadora.

1.4. TRABAJO PREPARATORIO

- El estudiante debe consultar previamente y prepararse sobre el funcionamiento del comando ping y un estudio acerca de las clases de direcciones IP con sus respectivas máscaras de subred.
- Conocimiento básico sobre las direcciones IP.

1.5. INTRODUCIÓN / MARCO TEORICO

Un cable de red UTP (Unshielded Twisted Pair, par trenzado sin blindaje) sirve para la comunicación entre dispositivos informáticos como computadores, switches, routers, entre otros, para poder así montar una red de computadoras.

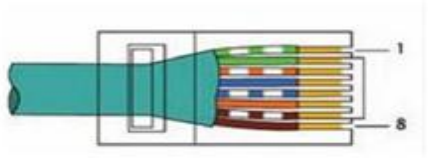


Figura 1. Numeración de pines en conector.
Tomado de Joaquín Andreu Gómez, 2011, p. 121.

1.5.1. Categorías de cables UTP

- Categoría 1: Diseñado para redes telefónicas, utilizado solo para voz.
- Categoría 2: Definido en la norma TIA/EIA-568B, capaz de transmitir hasta 4 Mbps.
- Categoría 3: Definida por la especificación TIA/EIA 568-A. Velocidad de hasta 10 Mbps.
- Categoría 4: Definida por la especificación TIA/EIA 568-A. Velocidad de hasta 16Mbps utilizado en TOKEN RING. Rápidamente reemplazado por la Cat. 6.

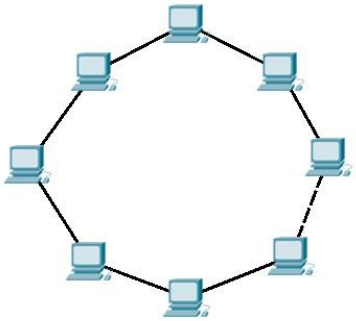


Figura 2. Una estructura o modelo de una red TOKEN RING.
Tomado de Herrera, R. (2014).

- Categoría 5: Definida por la especificación TIA/EIA 568-A. Es un nuevo estándar que soportará velocidades aún mayores de 100 Mbps.
- Categoría 6: Retro-compatible con la categoría con la Cat. 5/5E.

Este tipo de cable está formado por 4 pares de cables entrecruzados entre sí, compensando de esta manera inducciones electromagnéticas producidas por las líneas de los mismos y se encargan de transportar las señales o información.

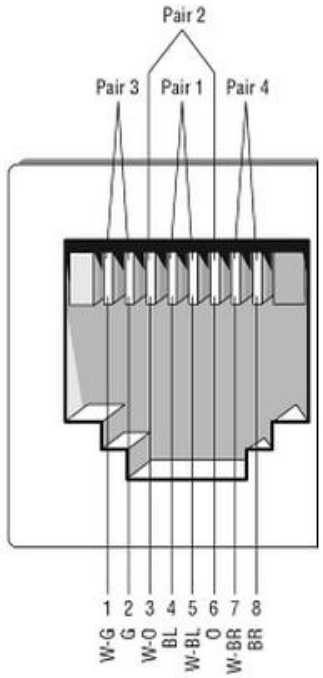
El cable UTP se encuentra resguardado por un recubrimiento de material aislante mientras que los cables están conformados de cobre. Es utilizado comúnmente en redes Ethernet en Cat. 3, 4, 5 y 6 especificados con la norma TIA/EIA 568-A standard.

1.5.2. Conector RJ-45

Figura 3 Conector de red RJ-45.
Tomado de Juan Carlos Martin Castillo, 2012, p. 38.

1.5.3. Normas de crimpado

1.5.3.1. Norma T568A: orden de colores (CABLE CRUZADO)



- Blanco Verde
- Verde
- Blanco Naranja
- Azul
- Blanco Azul
- Naranja
- Blanco Café
- Café

Figura 4. Norma de colores para el crimpado de la norma T568A.
Tomado de Andrew Olivero y Bill Woodward, 2009, p. 75.

Como su nombre lo indica se realiza un intercambio de terminales de transmisión para que del lado de transmisión llegue a la recepción del otro. Para la utilización de éste los equipos deben trabajar en la misma capa de modelo OSI como por ejemplo dos computadores por medio de las tarjetas de red.

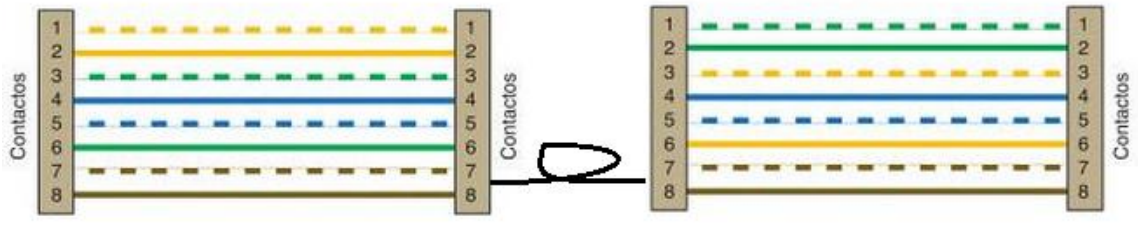
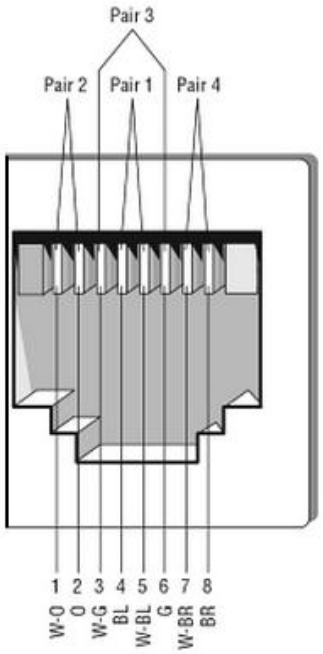


Figura 5. Contactos de un cable de red cruzado.
Tomado de Juan Carlos Martin Castillo, 2012, p. 38.

1.5.3.2. Norma T568B: orden de colores (CABLE DE RED DIRECTO)



- Blanco Naranja
- Naranja
- Blanco Verde
- Azul
- Blanco Azul
- Verde
- Blanco Café
- Café

Figura 6. Norma de colores para el crimpado de la norma T568B.
Tomado de Andrew Olivero y Bill Woodward, 2009, p. 75.

Este tipo de conexión permite realizar una comunicación de dispositivos diferentes, es decir, un computador a un switch o a un router para la salida a internet (si fuera el caso). No habrá problema siempre y cuando se utilice la misma norma de los dos lados del cable.

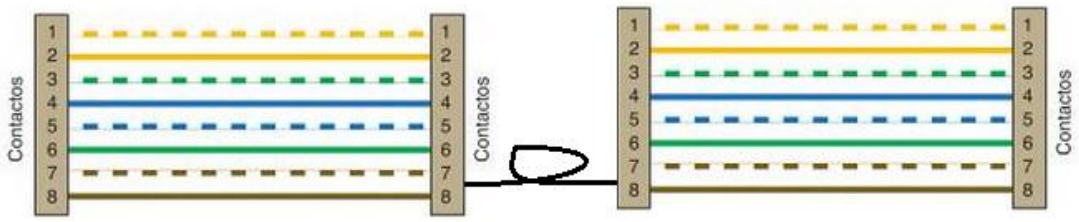


Figura 7. Contactos de un cable de red directo.
Tomado de Juan Carlos Martin Castillo, 2012, p. 38.

1.5.3.2.1. CONEXIONES MDI / MDI-X

El puerto de comunicación RJ-45 contiene una señal de transmisión y una de recepción en un cableado de red informática y toma dos definiciones:

1.5.3.2.2. MDI (Interfaz dependiente del medio):

Éste proporciona la conexión física y eléctrica al medio de transmisión en donde el puerto del dispositivos emisor debe estar conectado con el puerto del dispositivo del receptor, es decir, el puerto MDI de un dispositivo debe estar conectado con el puerto MDIX del otro dispositivo.

Figura 8. Como se intercambian los emisores con receptores para un crimpado.
Tomado de Herrera, R. (2014).

1.5.3.2.3. MDI-X (Interfaz dependiente del medio-Cruzado):

Para la comunicación de dos puertos de la misma configuración (MDI a MDI o MDI-X a MDI-X) se requiere de un cable cruzado que cruce la transmisión y recepción en el cable, de tal forma que estén igualados a nivel del conector. Auto MDI-X detecta de forma automática la conexión del cable y configura la conexión de una manera adecuada, de tal manera que se elimina la necesidad de un cable directo o cruzado para la comunicación de los diferentes dispositivos.

1.6. DESARROLLO DE LA PRÁCTICA:

En este punto se procederá con la elaboración de un cable de red directo para lo cual se debe pelar el cable, retirar el material aislante que recubre a los cables de par trenzados ubicándolos de tal manera que se defina la norma de crimpado que se utilizará en la práctica y con la ayuda de la cortadora de cable UTP cortar de una manera lineal los cables del par trenzado.

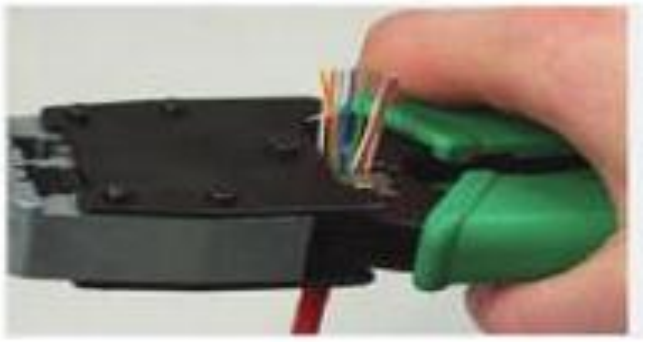


Figura 9. Corte del cable de red.
Tomado de José Carlos Gallego, 2014, p. 106.

Al estar los cables uniformemente cortados es momento de ingresarlos al conector.

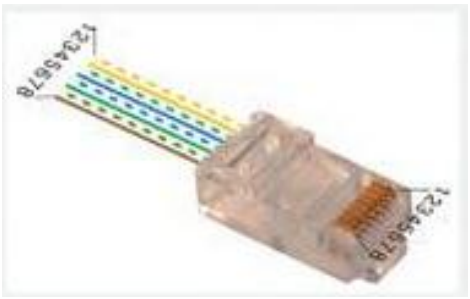


Figura 10. Ingreso de cables al conector.
Tomado de Juan Carlos Martin Castillo, 2012, p. 38.

Se debe tener en cuenta que dentro del conector los terminales del cable deben estar haciendo contacto con los terminales de cobre ubicados al final del conector como se muestra en la figura:

Figura 11. Un conector de red listo para ser crimpado.
Tomado de Herrera, R. (2014).

En este punto es necesario realizar el crimpado correspondiente para la obtención del cable deseado.

Figura 12. Crimpado de cable.
Tomado de Jerri Farris, 2008, p. 57.

Se debe repetir el proceso 1 y 2 del otro extremo del cable para así obtener el cable deseado.

Figura 13. Un cable de red listo para cumplir con sus funciones.
Tomado de Herrera, R. (2014).

Con la ayuda de un testeador de cable de fácil uso y comprensión permiten que los instaladores de red comprueben con exactitud las configuraciones de pin de varios cables de comunicación, transmitiendo señales de prueba a su terminal remota correspondiente para verificar la fiabilidad del cable.

Figura 14. Testeador de cable de red.
Tomado de José Ramón Oliva Haba, 2005, p. 309.

Ahora se procederá con la conexión física de las computadoras por medio de las tarjetas de red con el cable elaborado.

Figura 15. Tarjeta de red.
Tomado de Antonio Pérez Luna, 2012, p. 59.

Conectados físicamente los computadores es momento de realizar la configuración lógica con las direcciones IP y se lo hará presionando en la opción de inicio y posteriormente en panel de control:

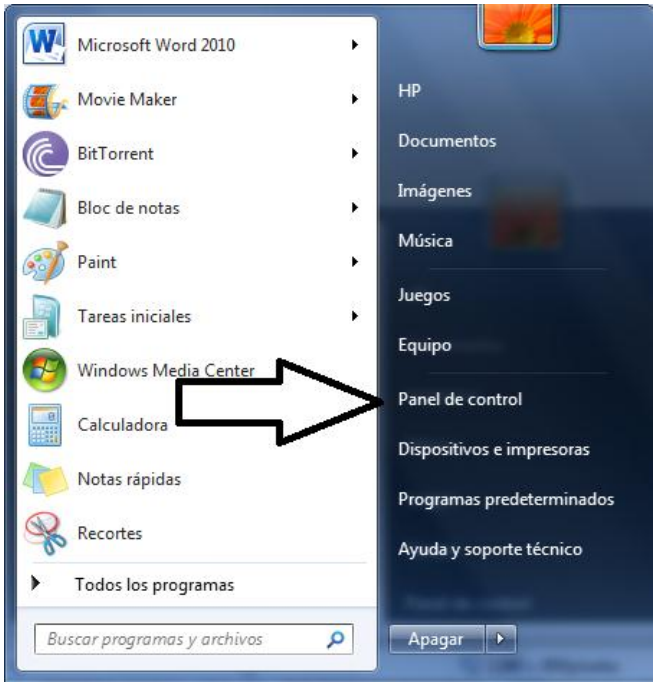


Figura 16. Ventana de inicio.
Tomado de Herrera, R. (2014).

Desplegando una ventana donde se debe seleccionar “Centro de redes y recursos compartidos”.

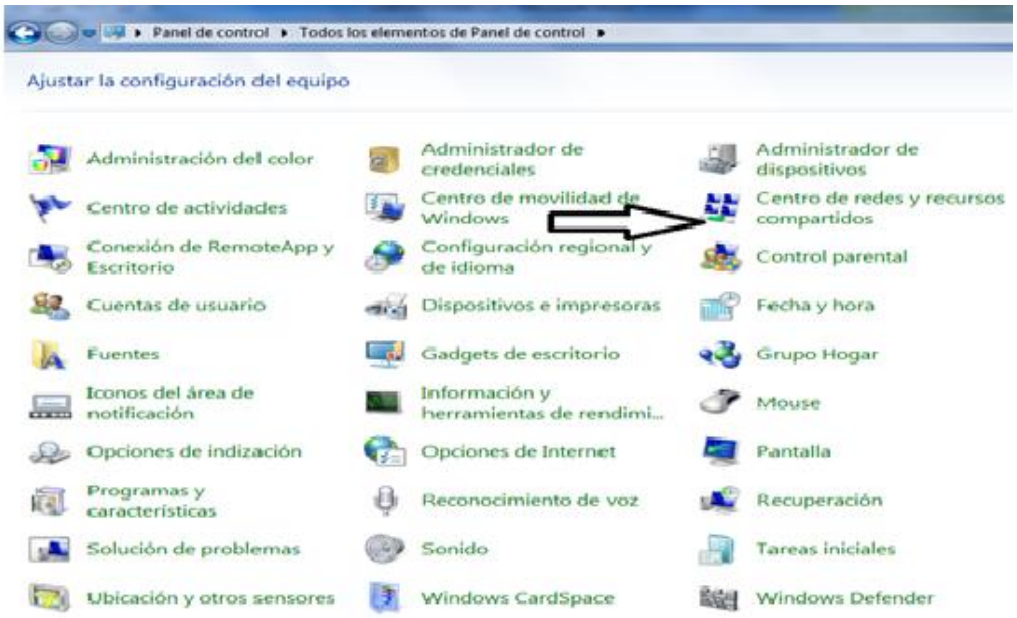


Figura 17. Ventana de Panel de control.
Tomado de Herrera, R. (2014).

Tras pulsar dicha opción de debe seleccionar “cambiar configuración de adaptador y posteriormente el icono a seleccionar es “Conexión de área loca” con clic derecho y seguido de la opción propiedades.

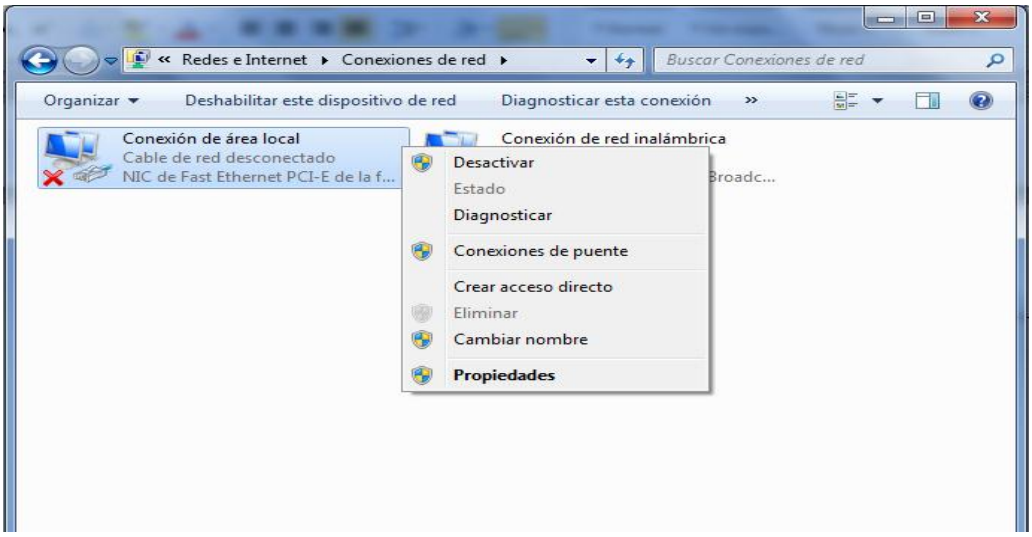


Figura 18. Ventana Conexiones de red.
Tomado de Herrera, R. (2014).

En esta ventana se debe dar clic en la casilla “Protocolo de Internet versión 4 (TCP/IPv4)” y después en “Propiedades”.

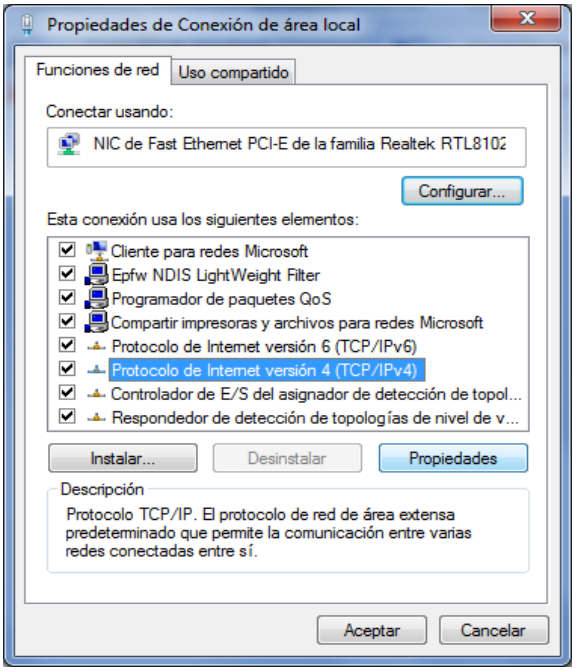


Figura 19. Ventana Propiedades de conexión de área local. Tomado de Herrera, R. (2014).

A continuación se procede a habilitar la opción “Obtener una dirección IP automáticamente” e ingresar la dirección IP 192.168.1.6 y mascara de subred 255.255.255.0

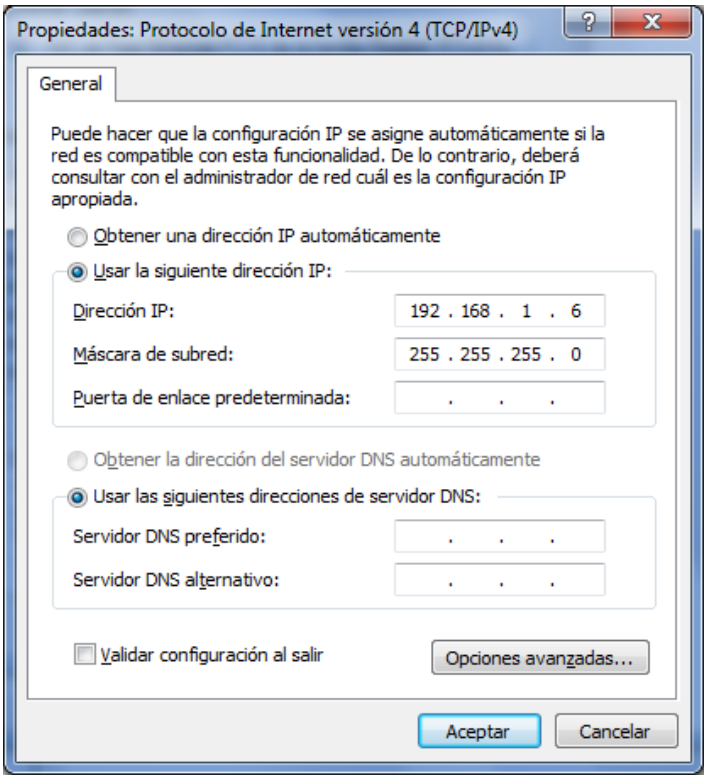


Figura 20. Ventana Propiedades de Protocolo de Internet versión (TCP/IPv4) Tomado de Herrera, R. (2014).

Para finalizar la configuración de los equipos se procederá a dar clic en aceptar, para guardar los cambios efectuados y realizar el mismo procedimiento en la otra estación de trabajo pero la dirección IP que se utilizará para esta será 192.168.1.1 y mascara 255.255.255.0

A continuación se realiza la comprobación de la conexión por medio del comando ping que se lo convoca seleccionando el botón de inicio en el escritorio y posteriormente la opción ejecutar como muestra el siguiente gráfico:

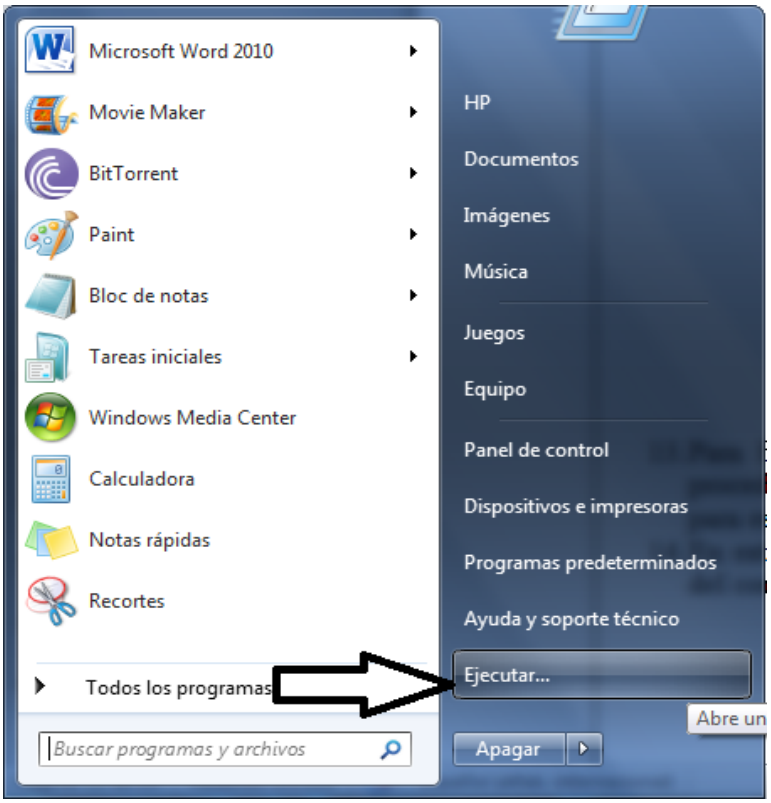


Figura 21. Ventana de opción Ejecutar.
Tomado de Herrera, R. (2014).

Se desplegará una ventana en donde se debe ingresar el siguiente escrito “cmd” y presionar la tecla “ENTER”.

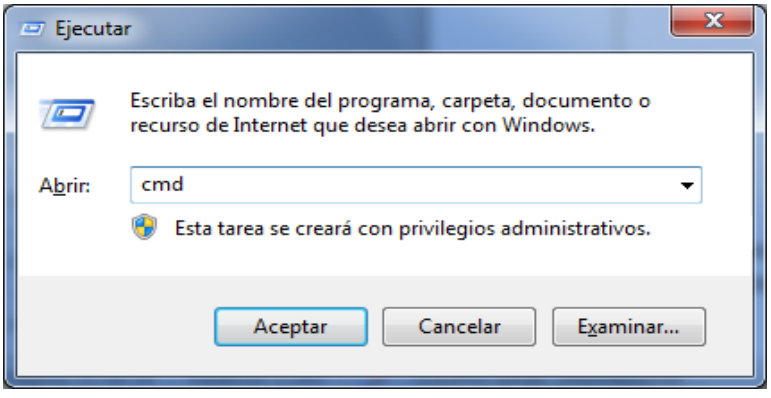


Figura 22. Ventana para ejecución de comandos.
Tomado de Herrera, R. (2014).

En la última pantalla se observa una ventana de DOS, aquí se hará uso del comando "ping" utilizando el computador con IP 192.168.1.6 y digitando "ping 192.168.1.1"

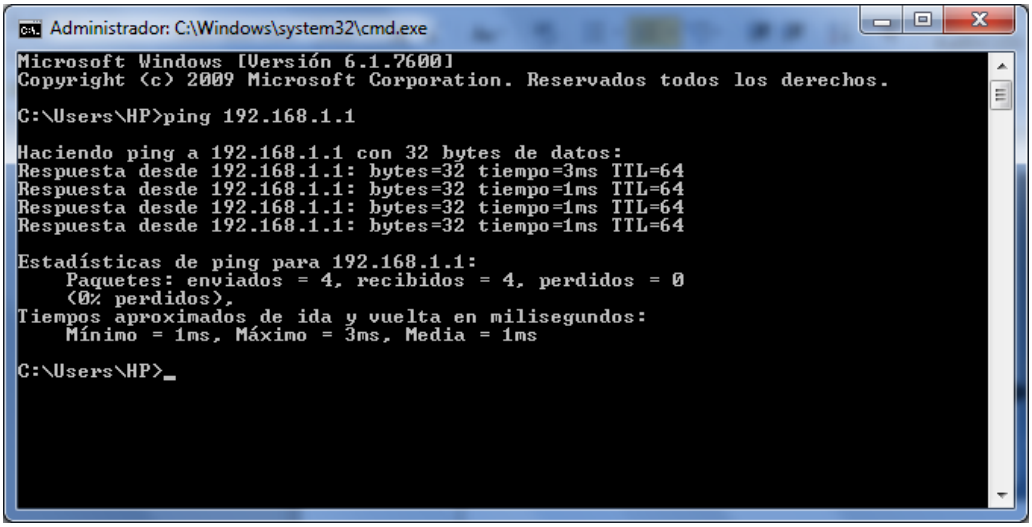


Figura 23. Ejecución de comando ping.
Tomado de Herrera, R. (2014).

La imagen muestra que se envían 4 paquetes con el tiempo que demora en enviarse, demostrando así la conexión que existe de un computador al otro.

1.7. RESULTADO DE LA PRÁCTICA:

El cable de red es muy utilizado y fácil de elaborar permitiendo una conexión segura y práctica, se estableció conexión física sin problemas.

1.8. CONCLUSIONES Y RECOMENDACIONES:

- En este capítulo se dio un vistazo del uso del comando ping y su facilidad para determinar si hay conexión lógica entre equipos tecnológicos como son los computadores utilizados en la práctica.
- Los cables de red o también llamados patch cord hoy en día permiten la comunicación entre los dispositivos ya sean estos directos o cruzados sin necesidad de modificar el código de colores.

- A pesar de que la tecnología avanza el cable de red sigue siendo una conexión segura y muy utilizada.
- El laboratorio se llevó a cabo sin ningún tipo de inconveniente y a satisfacción total de los estudiantes y profesor.

CAPITULO II

2. Demostración, configuración y verificación de los comandos básicos ping, ipconfig, telnet, ftp, tracert en el simulador de Packet Tracert.

2.1. OBJETIVO GENERAL

Mediante el presente laboratorio se procederá a demostrar, configurar y verificar las funciones de los comandos básicos tales como ping, ipconfig, telnet, ftp, tracert en el simulador de Packet Tracer.

2.2. OBJETIVOS ESPECÍFICOS

- Utilizar los comandos básicos de una red para dar soporte de una manera oportuna.
- Conocer cada una de las funcionalidades de los comandos que pueden ser de gran ayuda para resolver inconvenientes de conexión.

2.3. DESCRIPCIÓN DE EQUIPOS / HERRAMIENTAS / SOFTWARE / MATERIALES

2.3.1. PROVISTOS POR LA UNIVERSIDAD

2.3.2. PROVISTOS POR EL ESTUDIANTE

- Simulador de Packet Tracer

2.4. TRABAJO PREPARATORIO

- El estudiante debe consultar previamente el uso y sintaxis de los comandos: ping, ipconfig, telnet, ftp, tracert.
- Conocimiento básico sobre las direcciones IP.

2.5. INTRODUCIÓN / MARCO TEORICO

Un comando es una orden enviada a un computador por parte del usuario indicando a los periféricos una acción/ejecución y obtener una respuesta según el comando enviado.

2.5.1. Comando Ping

El comando ping permite efectuar un test de conectividad. De este modo puede intentar saber qué equipo está fuera de servicio o no. El comando ping utiliza el protocolo ICMP (Internet Control Message Protocol) y se emplea con una dirección de destino IP. El comando ping envía paquetes ICMP de tipo ECHO REQUEST cuya función principal es dar una respuesta con información a una petición realizada.

2.5.1.1. SINTAXIS

Se debe ingresar a simbología del sistema y escribir:

ping X.X.X.X

Las x representan la dirección IP a la cual se desea realizar la comprobación de conectividad y posteriormente presionar la tecla “ENTER”.

La respuesta generada por el otro equipo será:

Respuesta desde X.X.X.X: bytes=32 tiempo=1ms TTL=64

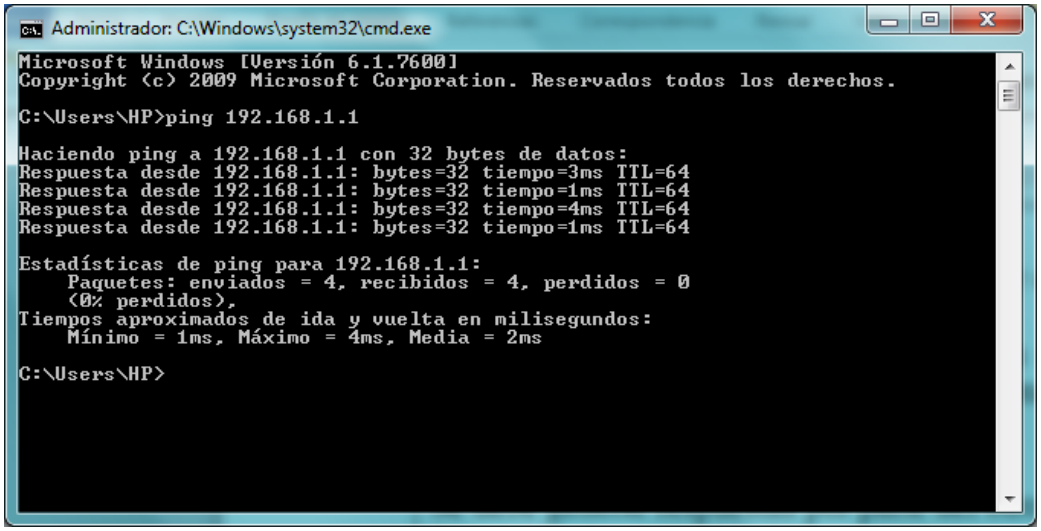


Figura 24. Ventana de comando ping.
Tomado de Herrera, R. (2014).

Cualquier otro mensaje quiere decir que hay un error de conectividad ya sea esta física o lógica. El proceso que realiza el comando ping es el siguiente:

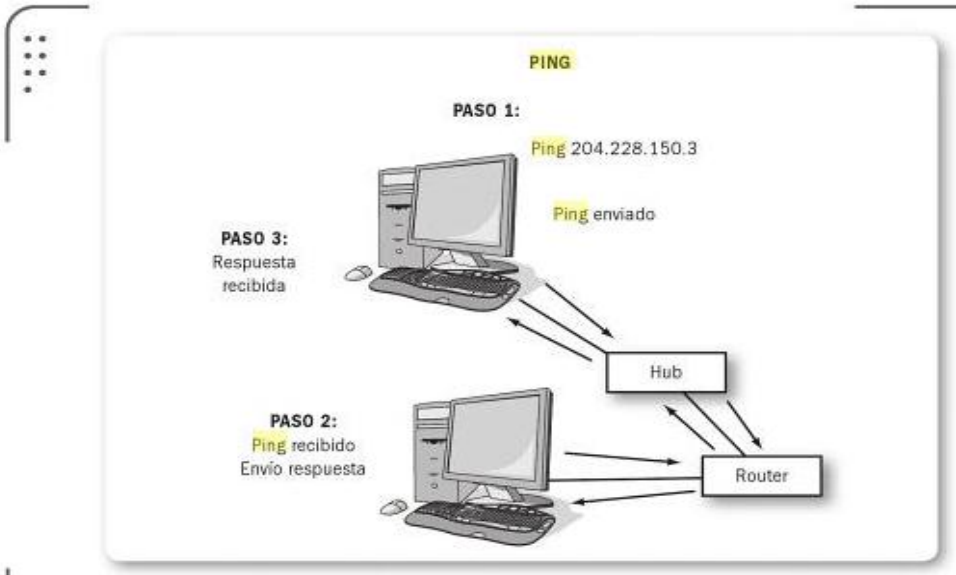


Figura 25. Proceso de comando ping.
Tomado de Gustavo Cabaillero, (2014), p. 193.

- El equipo 1 envía una solicitud de respuesta
- El otro equipo 2 recibe la solicitud y responde
- El equipo 1 recibe la respuesta

2.5.2. Comando IPCONFIG.

Este comando proporciona al usuario información esencial de cómo el equipo se encuentra configurado mediante la ejecución del mismo, invocándola desde la línea de comandos digitando “ipconfig”.

Información necesaria como:

- **Descripción:** Nombre del adaptador, dispositivo o tarjeta utilizada en la conexión.
- **Dirección IPv4:** Es la dirección IP asignada al Equipo o dispositivo de red.

- **Servidores DNS:** Generalmente son dos Servidores (Principal y secundario) los encargados de gestionar nombres de los dominios y las direcciones IP de las páginas solicitadas.
- **Dirección MAC**: es una dirección física encargada de identificar físicamente a un dispositivo o hardware al equipo o en otros casos a otros dispositivos, siendo así única en el mundo.
- **Estado de DHCP**: Esta configuración permite al equipo adquirir dinámicamente o aleatoriamente una dirección IP de algún servidor que las asigne.

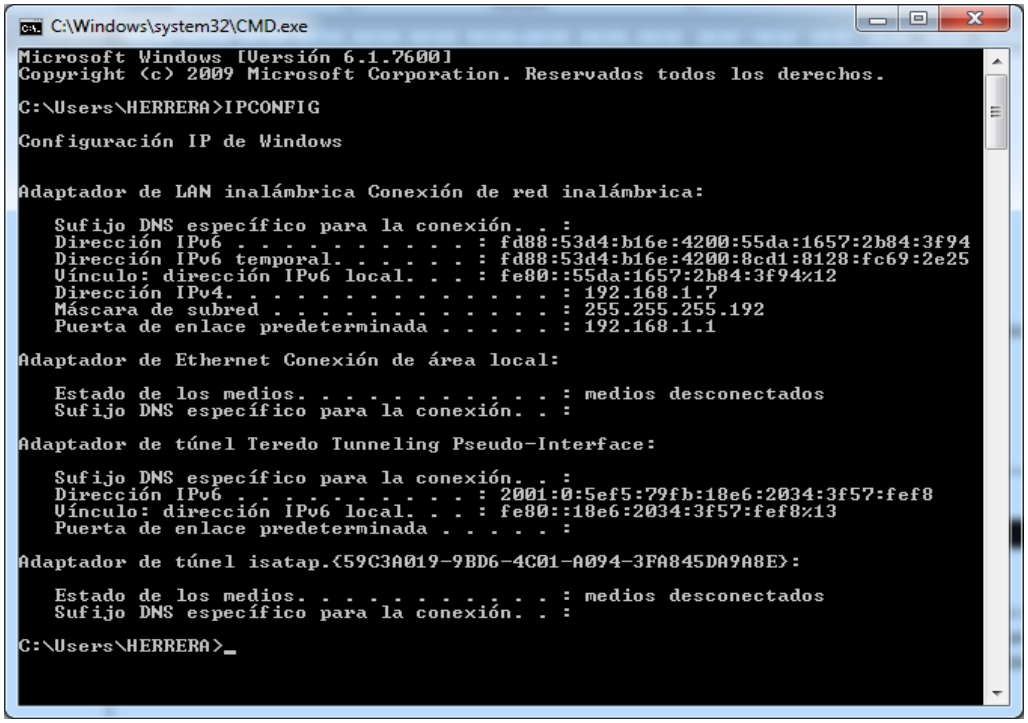


Figura 26. Ejecución de comando IPCONFIG.
Tomado de Herrera, R. (2014).

En el presente gráfico de la figura 3. Se puede observar lo siguiente:

- Dirección IP : 192.168.1.7
- Máscara de red : 255.255.255.192
- Puerta de enlace : 192.168.1.1

2.5.3. Comando TELNET

Como José Dordoigne (2013, pp. 462-462) ya lo dijo "Telnet es un protocolo de emulación de terminal. Establece una sesión entre una estación de trabajo (cliente Telnet) y una máquina remota (servidor Telnet). Se transmite cualquier comando ejecutado en el cliente y se ejecutado en el servidor Telnet".

Como se puede apreciar, Telnet subsiste en varias plataformas como son: UNIX Windows 95, NT y LINUX.

Para iniciar una sesión Telnet se lo hace desde MS-DOS o UNIX de la siguiente manera:

- TELNET XXX.XXX.XXX.XXX (Dirección IP del servidor X) PUERTO

Una vez ingresado en el servidor Telnet se puede ejecutar comandos para alterar o configurar según sea necesario:

- Quit : Cierra cualquier sesión Telnet abierta y sale de telnet.
- Ctrl-z : Suspende telnet.
- Status : Muestra el status de telnet.
- ? [comand]: Proporciona ayuda sobre el comando dado.

2.5.4. Comando FTP (PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS)

Basado en una arquitectura cliente /servidor, éste es un servicio que permite la transferencia de archivos entre dos computadores conectados como programas, archivos, video, música, etc.

- **Un cliente FTP** : Este es el encargado de establecer la conexión y de descargar o subir los archivos al servidor.
- **Un servidor FTP**: Encargado de ejecutar los comandos o peticiones que solicite el cliente FTP.

¿Cómo funciona?

Es necesario ejecutar el programa FTP desde el ordenador y establecer una conexión con Internet. En el servidor FTP se encuentra el “Demonio FTP” encargado de controlar todas las actividades de emisión de información o recepción de datos (descargas). Al entrar en contacto con un servidor FTP mediante el programa FTP, el Demonio FTP le exigirá que indique su usuario y contraseña.

Cuando un cliente desea conectarse a un servidor FTP necesita de los siguientes datos:

- Nombre del servidor : Esta es la IP o nombre del Servidor.
- Puerto: Número del puerto del servidor. Por defecto es el 21.
- Cuenta de Usuario : Nombre de la cuenta de usuario. Hay sitios que permiten la conexión anónima utilizando el nombre de usuario anonymous.
- Clave de acceso: Contraseña.

Cuando se levanta este servicio, el servidor crea el canal de datos de comandos entre su ordenador y el servidor FTP. Esta conexión sirve para enviar comandos del ordenador al servidor FTP, así como para recibir mensajes e información.

2.6. DESARROLLO DE LA PRÁCTICA:

Para aprender el uso de los comandos se hará uso del simulador Packet Tracert previamente el estudiante debió instalar en el computador y así hacer uso de las herramientas que éste pueda proporcionar.

En primer lugar se procederá a ingresar al programa haciendo clic en “Inicio” como se muestra en el siguiente gráfico:

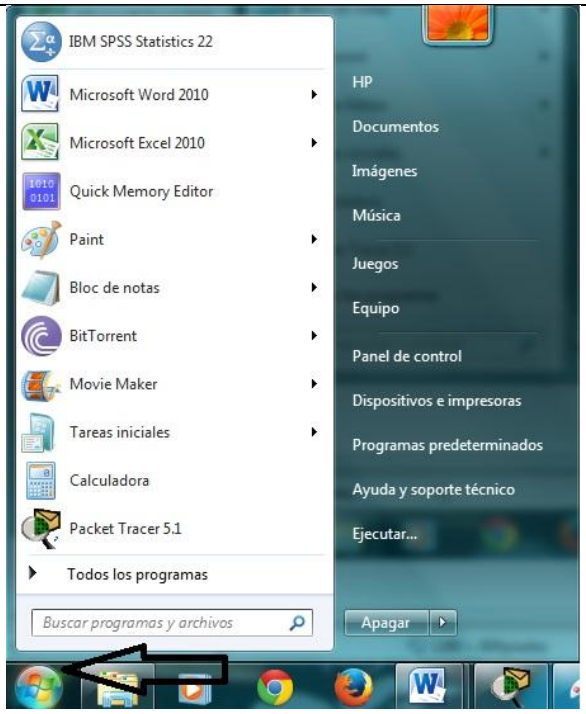


Figura 27. Imagen de botón de inicio en Windows 7. Tomado de Herrera, R. (2014).

Posteriormente dar clic en “Todos los programas”:

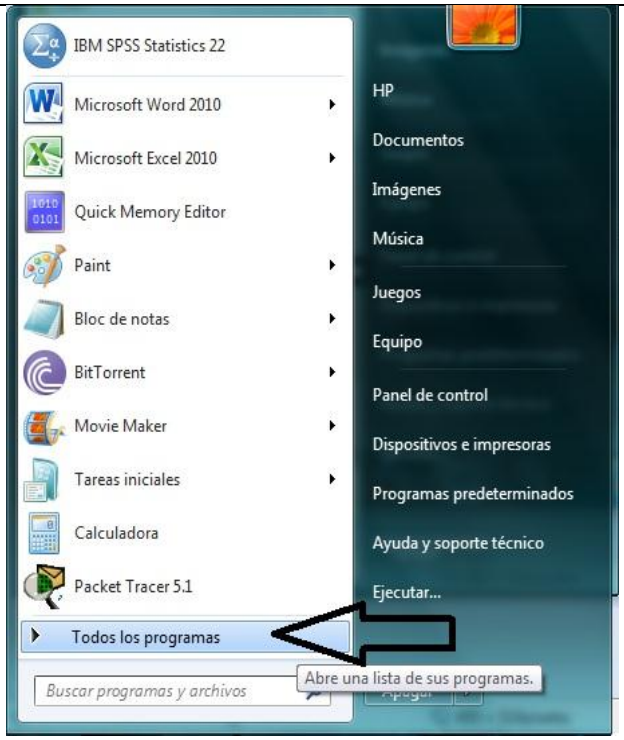


Figura 28. Imagen pestaña de todos los programas. Tomado de Herrera, R. (2014).

Ya en este punto se mostrará la siguiente pestaña y se deberá buscar la opción Packet Tracer y dar clic para ingresar al programa:

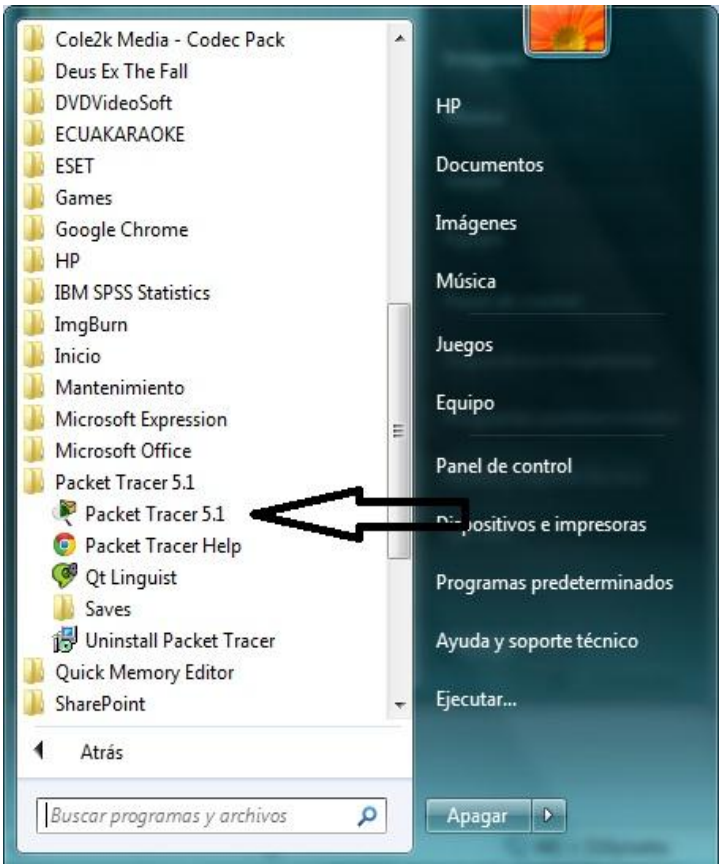


Figura 29. Imagen de opción Packet Tracer.
Tomado de Herrera, R. (2014).

El simulador desplegará una serie de herramientas las cuales se utilizarán en el transcurso del laboratorio y mostrará la siguiente ventana:

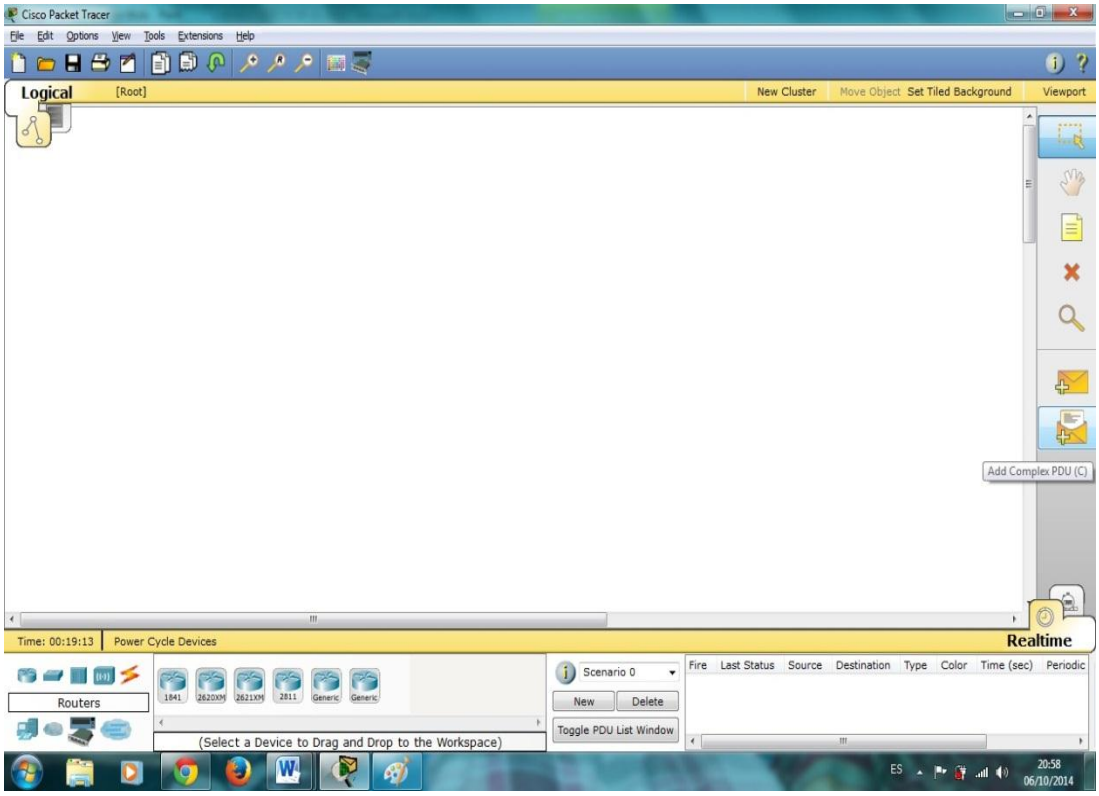


Figura 30. Imagen de Escenario Packet Tracer.
Tomado de Herrera, R. (2014).

A continuación se enlistará las partes, componentes, herramientas que el simulador ofrece para la elaboración del laboratorio y que se utilizarán posteriormente en el transcurso del laboratorio.

Primero se encuentra el escenario o área de trabajo del simulador. Éste sirve para ubicar, como se crea conveniente, todos los elementos/dispositivos de la red que se desee configurar.

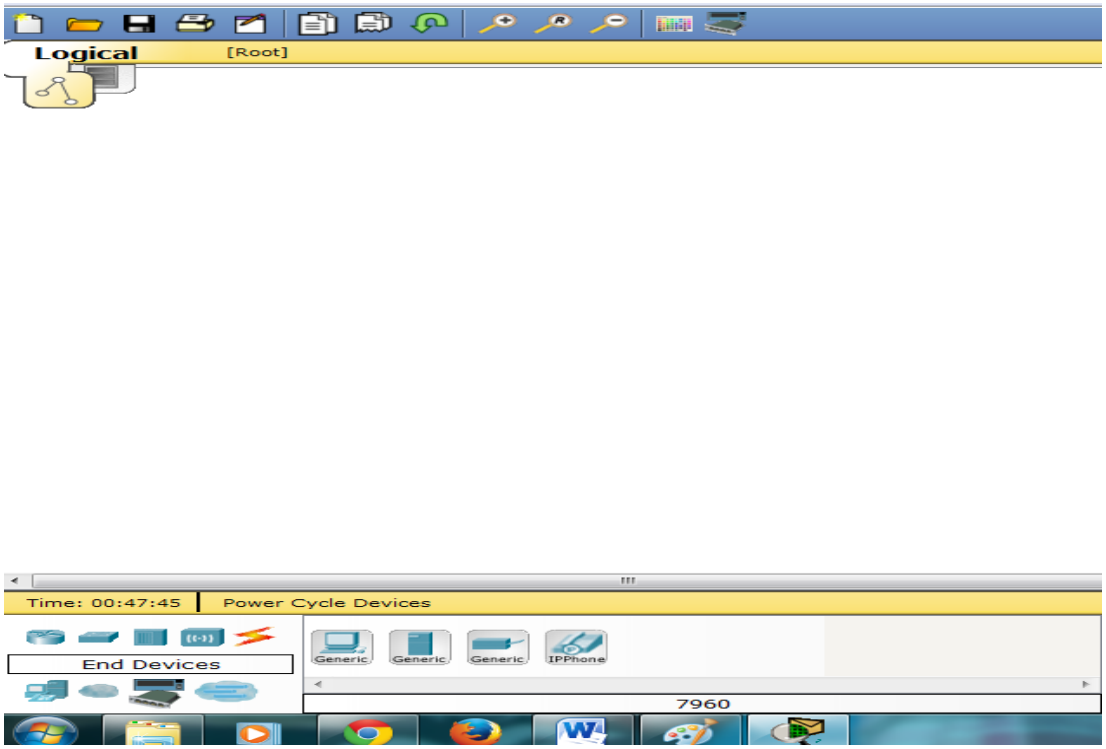


Figura 31. Imagen del simulador de Packet Tracert.
Tomado de Herrera, R. (2014).

Se dispone también de elementos de red en el simulador y están compuestos por routers, switches, hubs, dispositivos inalámbricos, conexiones, dispositivos finales, entre otros.

Figura 32. Imagen de Elementos de Packet tracert.
Tomado de Herrera, R. (2014).

Se puede encontrar un submenú en los elementos disponibles con modelos más específicos para un mejor desempeño en el procedimiento de cualquier laboratorio.

En el submenú de elementos disponibles se puede apreciar:

2.6.1. Routers: (1800, 2600, 2800, genéricos).

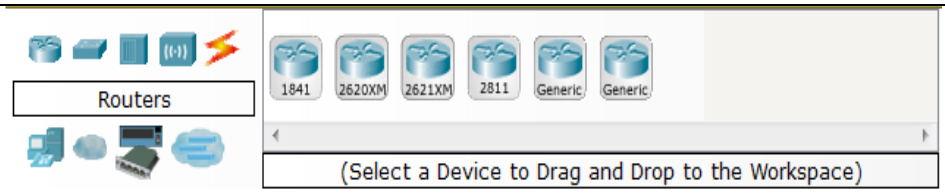


Figura 33. Imagen routers.
Tomado de Herrera, R. (2014).

2.6.2. Switches: series 2950, 2960, genérico y bridge

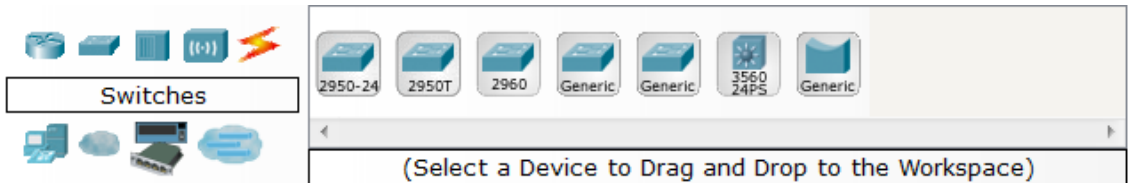


Figura 34. Imagen switches.
Tomado de Herrera, R. (2014).

2.6.3. Dispositivos Inalámbricos: Access Point, Router Inalámbrico.

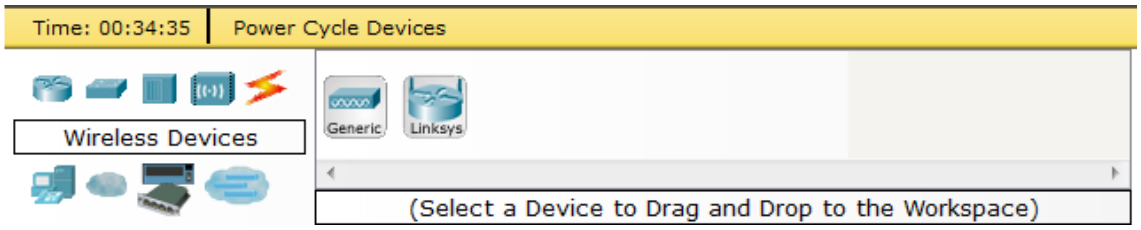


Figura 35. Imagen equipos inalámbricos.
Tomado de Herrera, R. (2014).

2.6.4. Conexiones disponibles: cable serial, consola, directo, cruzado, fibra óptica, etc.

Figura 36. Imagen de Medios de comunicación de red.
Tomado de Herrera, R. (2014).

2.6.5. Dispositivos terminales: Computador, servidores, impresoras, teléfonos IP.

Figura 37. Imagen equipos terminales.
Tomado de Herrera, R. (2014).

Para la elaboración del laboratorio se debe seleccionar un dispositivo desde el submenú y arrastrarlo hacia el escenario quedando de la siguiente manera:

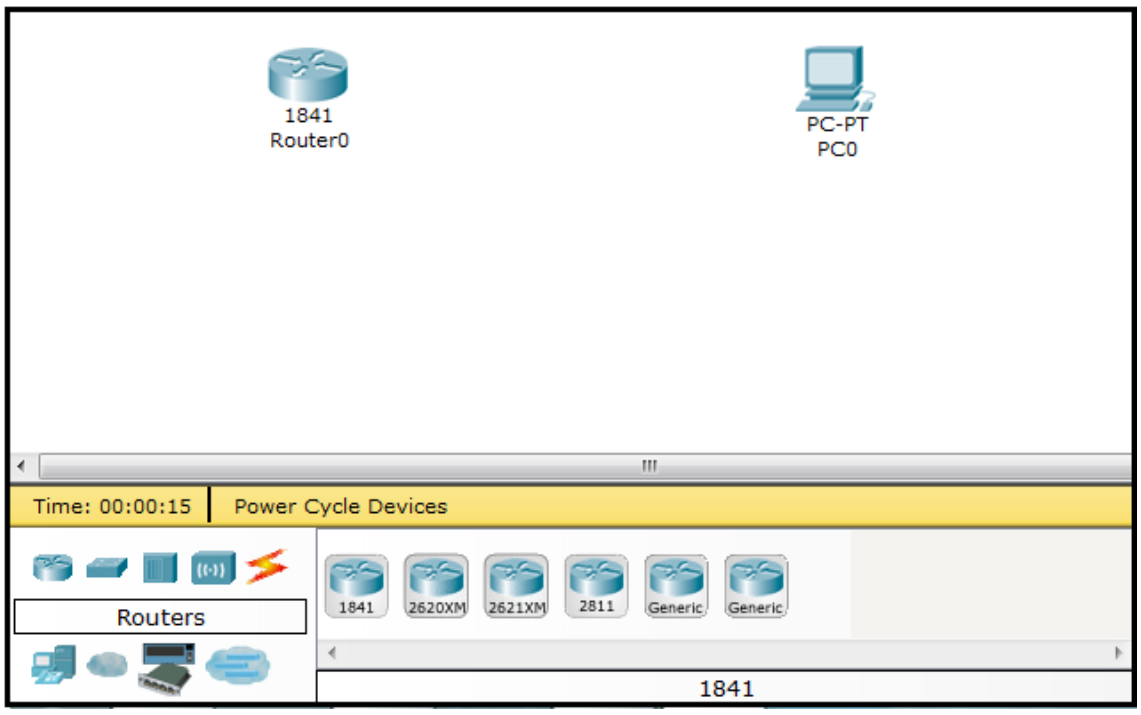


Figura 38. Imagen equipos posicionados en el escenario.
Tomado de Herrera, R. (2014).

Ahora el siguiente paso es agregar una conexión desde los elementos disponibles ítem conexiones y seleccionando opción “CROSS OVER”.

En este punto se debe seleccionar el Router y mostrará un listado de opciones de las cuales se debe escoger FastEthernet0/0:

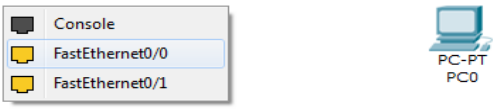


Figura 39. Imagen tipos de conexión de terminales.
Tomado de Herrera, R. (2014).

Ya en este punto lo siguiente será deslizar el puntero del mouse hacia el equipo terminal (el PC) dar clic:

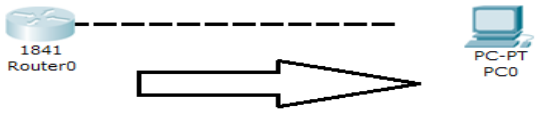


Figura 40. Imagen conexión router hasta PC.
Tomado de Herrera, R. (2014).

Ya aquí el dispositivo seleccionado (PC-PT) mostrará otra ventana en la cual la opción a escoger es “FastEthernet”

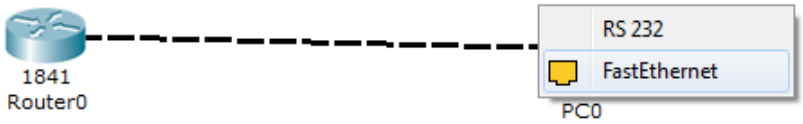


Figura 41. Imagen de co*nexión al otro terminal.*
Tomado de Herrera, R. (2014).

Se observarán los equipos marcados con una señal (puntos rojos) en cada extremo del medio de transmisión indicando que los equipos no tienen conexión pues estos están conectados físicamente más no lógicamente como se muestra en la imagen:

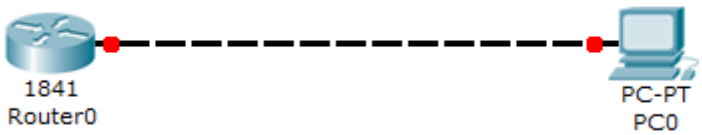


Figura 42. Imagen de equipos conectados con un medio de comunicación.
Tomado de Herrera, R. (2014).

2.6.6. Configuración de equipos en el Simulador

Primero se debe configurar el router con solo seleccionarlo y dirigiendo el mouse hasta la opción “CLI”:

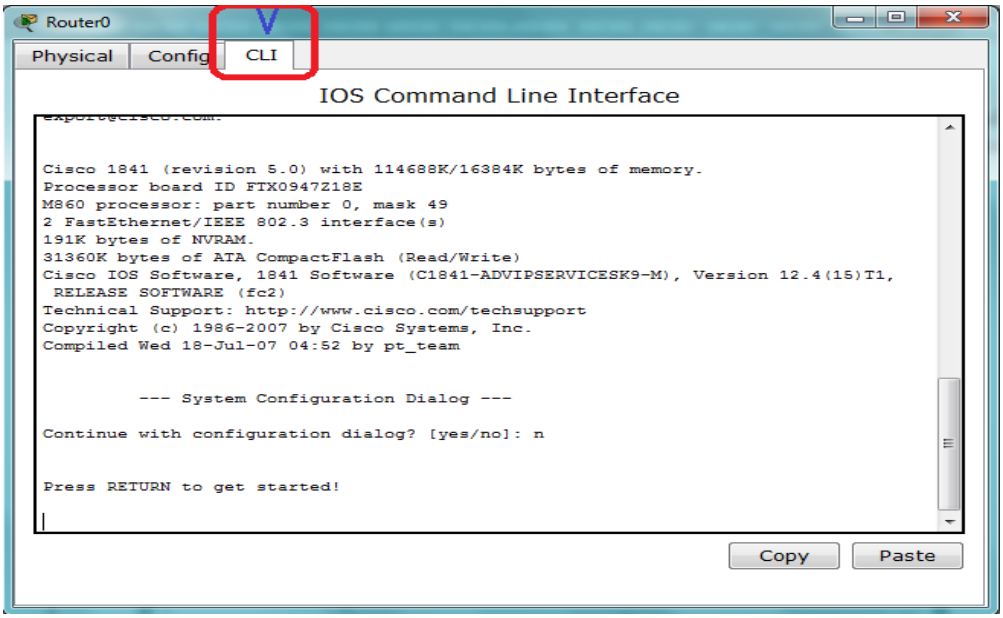


Figura 43. Imagen de terminal.
Tomado de Herrera, R. (2014).

Cabe recalcar que después de cada comando escrito, éste deberá estar seguido de un “ENTER” para la ejecución del mismo.

Para proceder con la configuración se debe dar un Enter y responder con un “no” a la pregunta que planteada “Continue with configuration dialog?” y así se ingresará en modo comando. Ahora se debe ejecutar el comando “enable”:

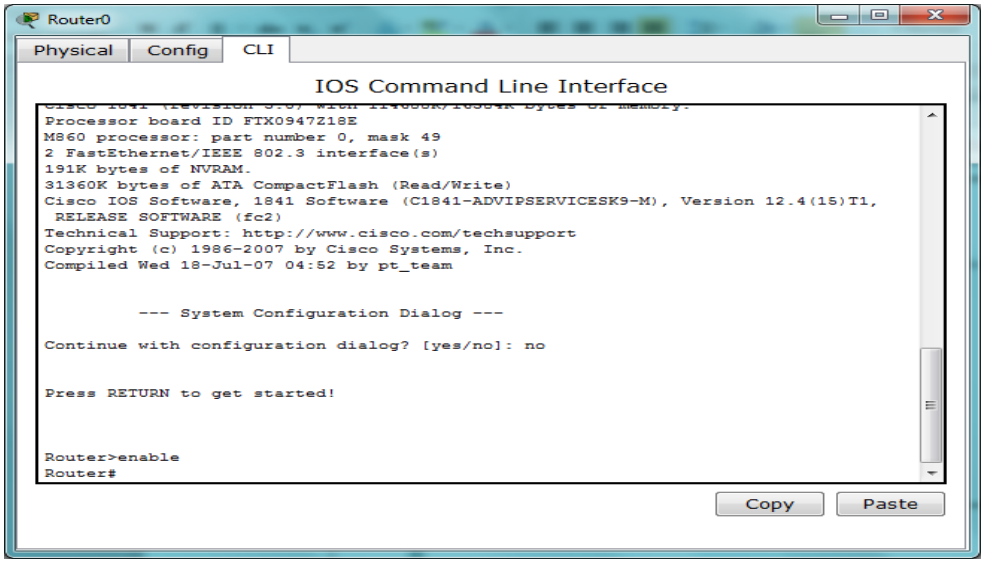


Figura 44. Imagen de acceso al terminal.
Tomado de Herrera, R. (2014).

Si se observa detenidamente se puede notar que después de ejecutar el comando enable el signo “mayor que” > cambia a un numeral #. Esto significa que se puede realizar cualquier cambio en el router con todos los privilegios de Administrador**.**

El siguiente comando a ejecutar es “configure terminal” ingresando de esta manera a la configuración de router:

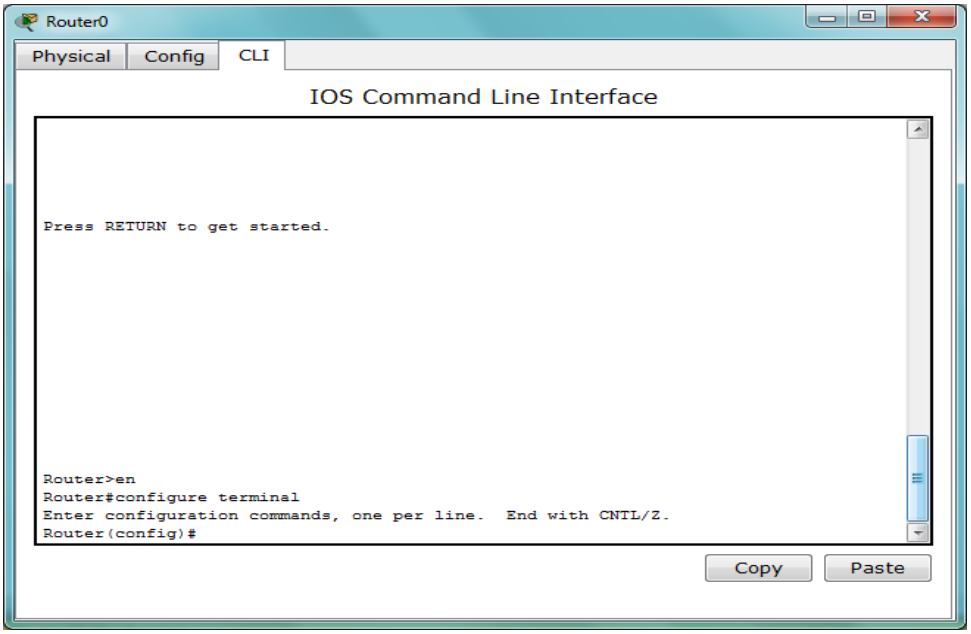


Figura 45. Imagen de administrador en el terminal.
Tomado de Herrera, R. (2014).

El siguiente paso es configurar la interface de la red privada mediante el comando “interface fastethetnet0/0”.

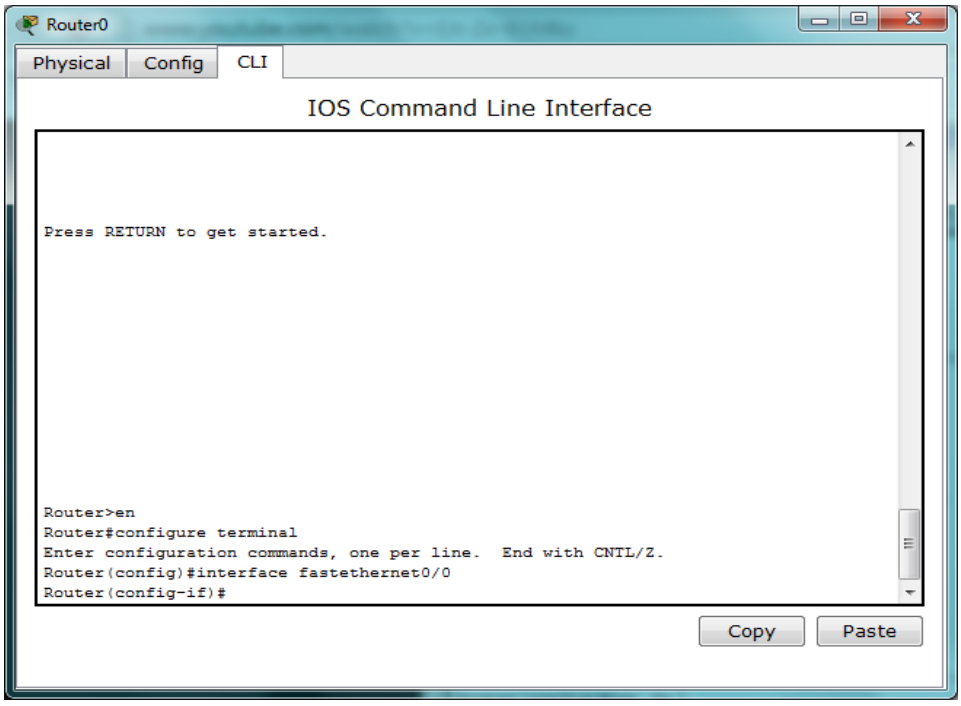


Figura 46. Imagen configuración de interface.
Tomado de Herrera, R. (2014).

Se procede a asignar una dirección IP mediante la sentencia: ip 192.168.0.1 255.255.255.0.

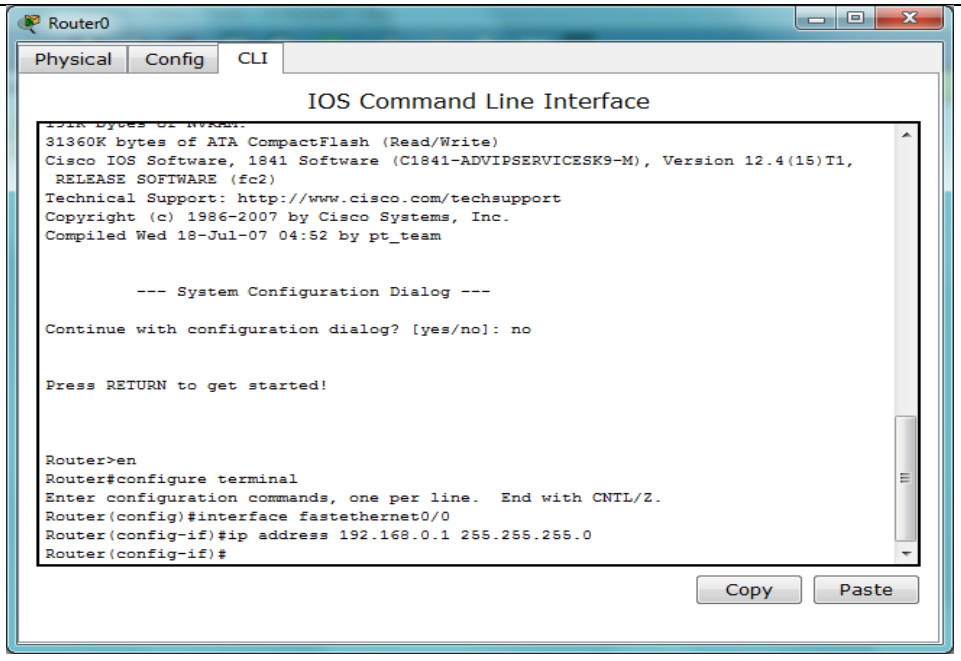


Figura 47. Imagen asignación de IP.
Tomado de Herrera, R. (2014).

Para que los cambios realizados sean guardados se debe ejecutar el comando “no shutdown”.

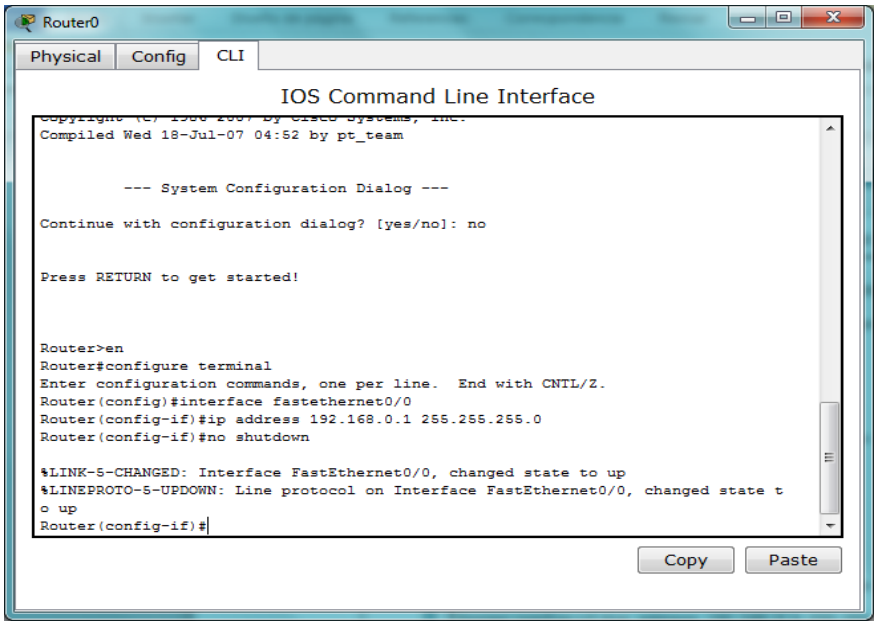


Figura 48. Imagen de no shutdown.
Tomado de Herrera, R. (2014).

Queda verificar los cambios efectuados y la conexión se encuentre funcional presionando ctrl + z hasta regresar a la raíz del prompt y ejecutar el comando: show ip interface brief.

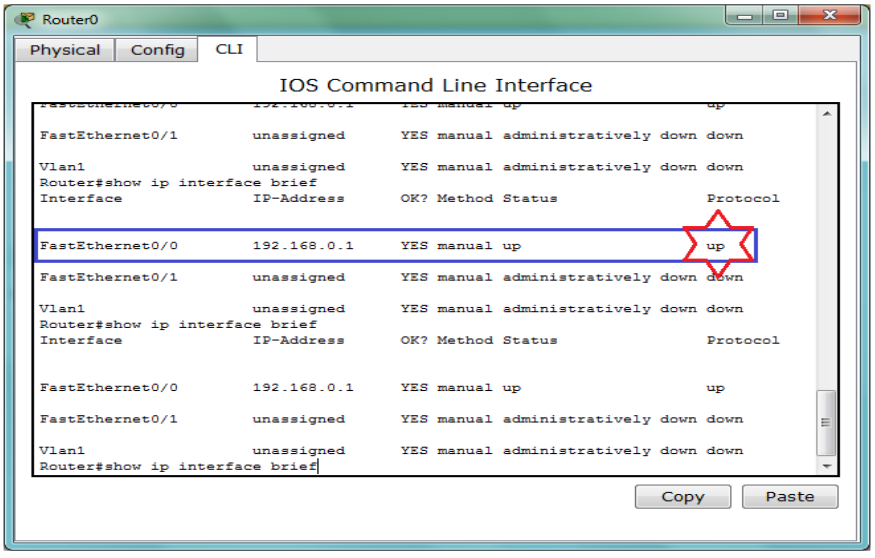


Figura 49. Imagen de interface levantada.
Tomado de Herrera, R. (2014).

Ahora queda configurar el dispositivo PC seleccionándolo y así se mostrará la siguiente ventana con opciones donde la que se debe escoger es “Desktop”.

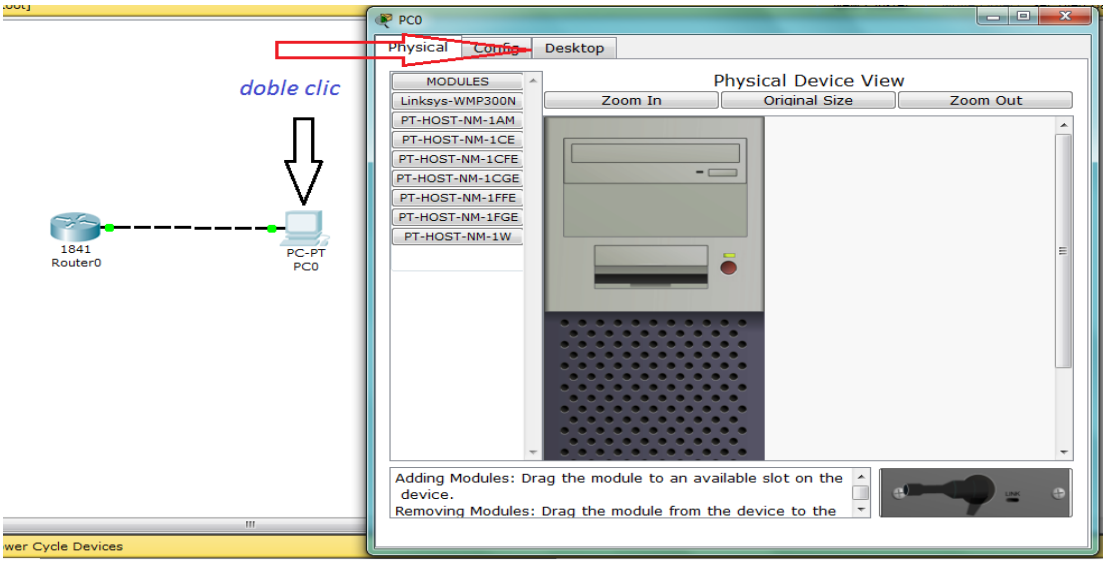


Figura 50.Configuracion de dispositivo.
Tomado de Herrera, R. (2014).

A continuación se asignará la dirección IP 192.168.0.2 y máscara 255.255.255.0. En este caso queda de la siguiente manera:

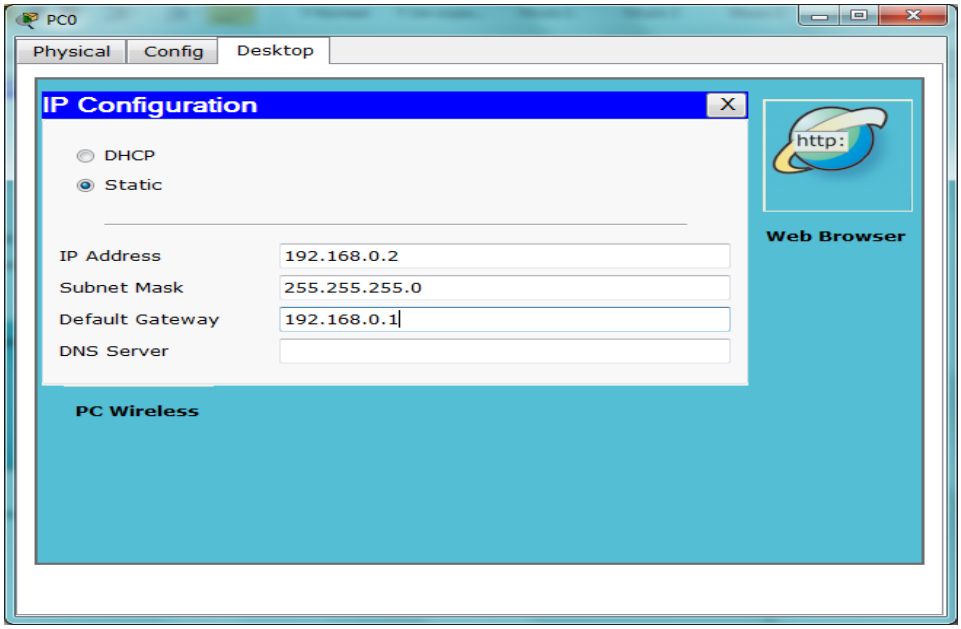


Figura 51. Asignación de IP.
Tomado de Herrera, R. (2014).

2.6.7. USO DE COMANDO IPCONFIG

Se debe ingresar al modo comando en el equipo y ejecutar ipconfig para ver la configuración IP y máscara del equipo indicando que la IP es la asignada anteriormente, con la máscara de red y puerta de enlace como se muestra a continuación:

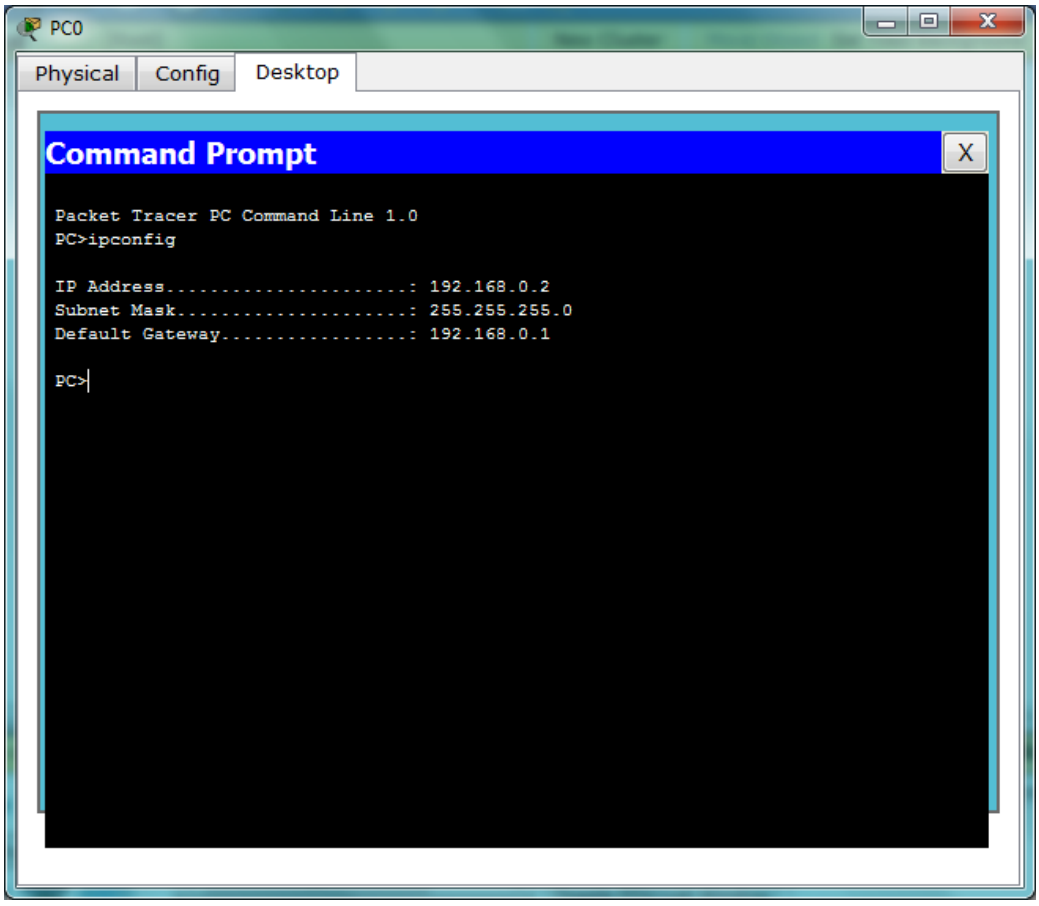


Figura 52. Ejecución de comando IPCONFIG.
Tomado de Herrera, R. (2014).

Como se puede observar en el siguiente gráfico el medio de comunicación ya no tiene los terminales de color rojo sino de cambia a color verde, lo que quiere decir que ya hay comunicación entre los dos equipos.

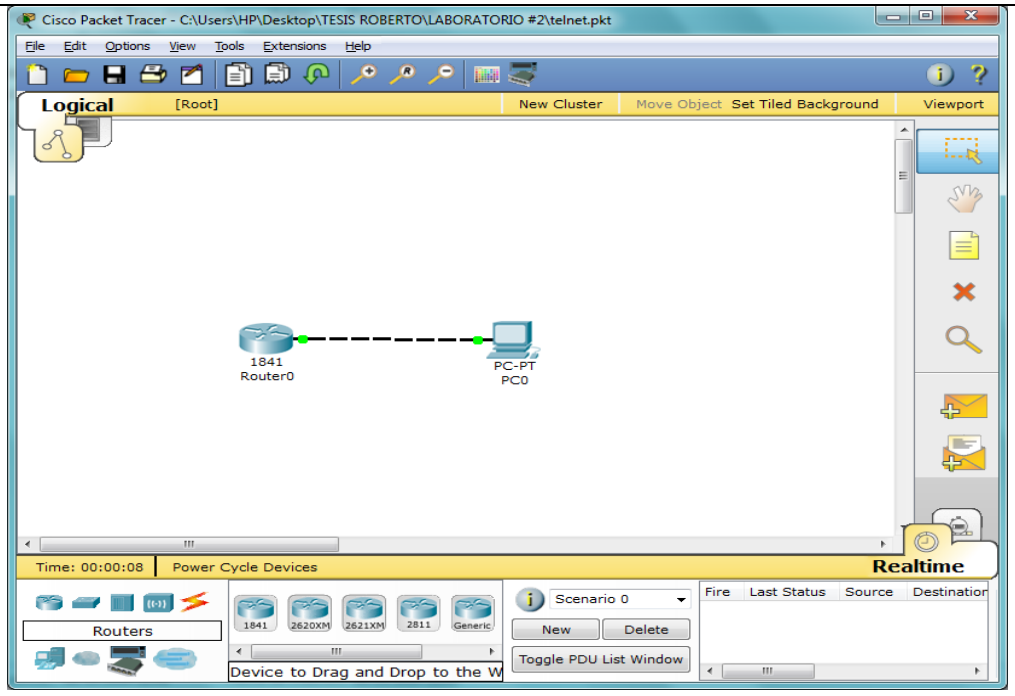


Figura 53. Equipos conectados.
Tomado de Herrera, R. (2014).

2.6.8. USO DE COMANDO PING

Para comprobar la comunicación entre los equipos es necesario ingresar al computador en modo de comando e ingresar a la pestaña “Desktop” como se muestra en la imagen:

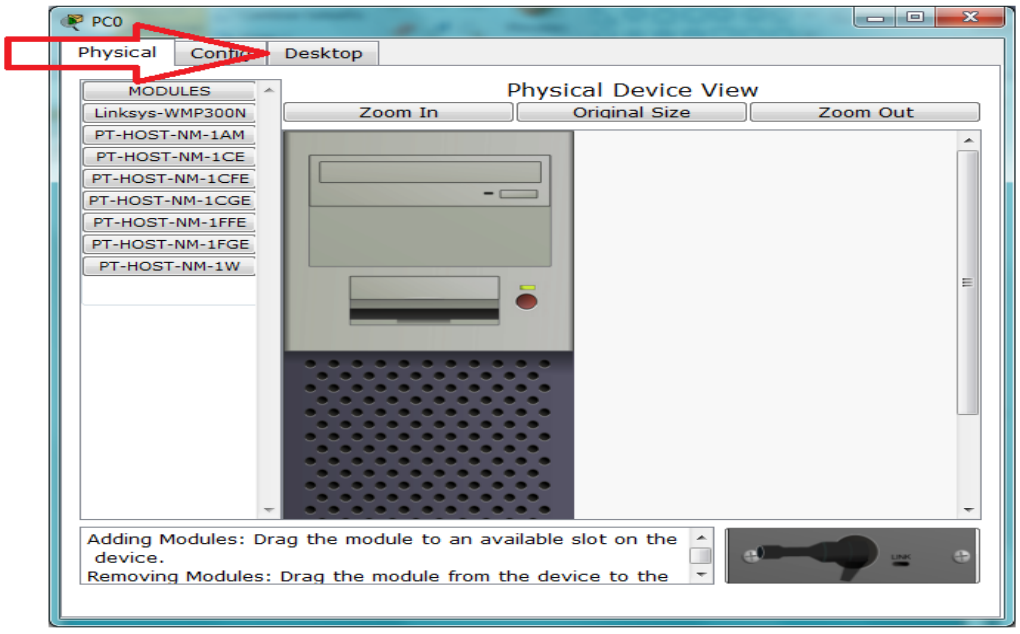


Figura 54. Opciones de dispositivos.
Tomado de Herrera, R. (2014).

En este punto se mostrará una ventana con opciones donde se debe seleccionar “Command Prompt”.

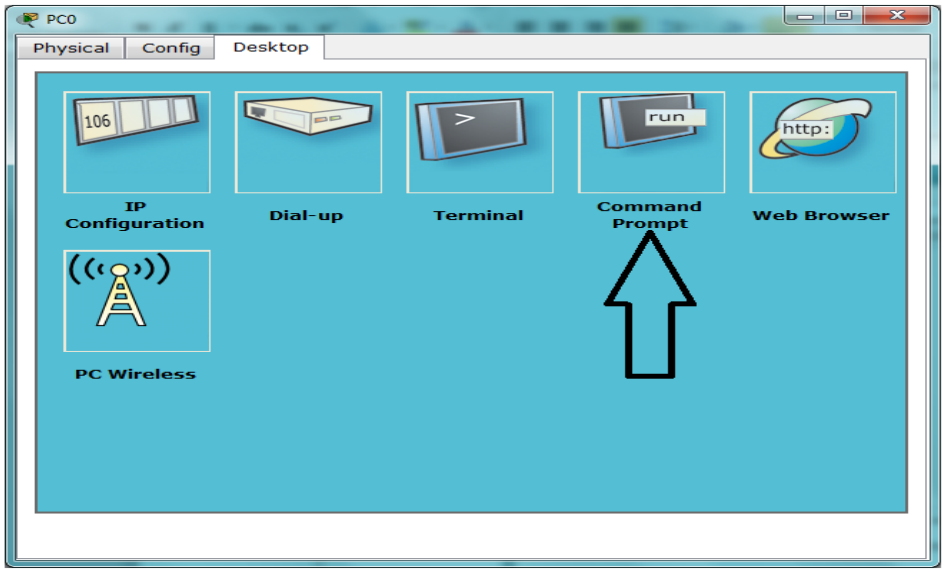


Figura 55. Imagen de ingreso al command Prompt.
Tomado de Herrera, R. (2014).

Ya en esta ventana se debe ejecutar el comando ping de la siguiente manera: ping 192.168.0.1 y el simulador mostrará la conexión exitosa entre los dispositivos.

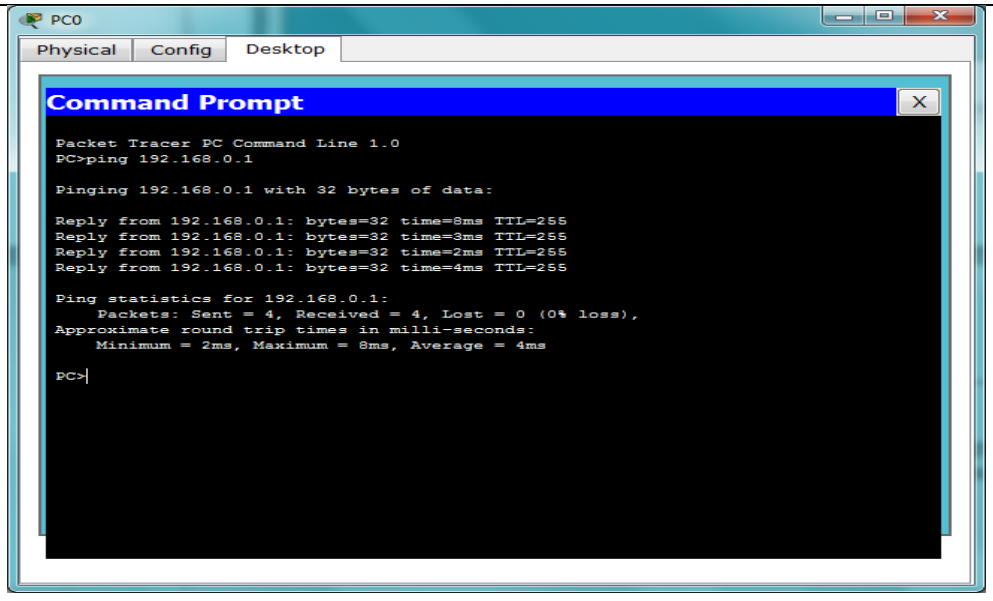


Figura 56. Comando ping succefully.
Tomado de Herrera, R. (2014).

La sintaxis del comando se describe a continuación:

ping [**-t**] [**-a**] [**-n** recuento] [**-l** tamaño] [**-f**] [**-i** TTL] [**-v** TOS] [**-r** recuento] [**-s** recuento] [{**-j** listaHost | **-k** listaHost}] [**-w** tiempoDeEspera] [nombreDestino]

Parámetros:

-t: Con esta sintaxis el comando ping continuará enviando mensajes de solicitud de eco al destino hasta que se le interrumpa presionando CTRL+C.

-a: Especifica que la resolución de nombres inversa se realiza en la dirección IP de destino.

–l tamaño .- Especifica la longitud, en bytes, del campo Datos del mensaje de solicitud de eco enviado. El valor predeterminado es 32. El tamaño máximo es 65.527.

-f Especifica que los mensajes de solicitud de eco se envían con el indicador No fragmentar del encabezado IP establecido como 1. Los enrutadores de la ruta de destino no pueden fragmentar el mensaje de solicitud de eco. Este parámetro resulta útil para solucionar problemas de PMTU (Unidad de transmisión máxima de ruta).

-i TTL Especifica el valor del campo TTL del encabezado IP del mensaje de solicitud de eco enviado. El valor predeterminado es el valor de TTL predeterminado del host. En host Windows XP, normalmente este valor es de 128. El TTL máximo es 255.

-v TOS Especifica el valor del campo TOS (Tipo de servicio) del encabezado IP del mensaje de solicitud de eco enviado. El valor predeterminado es 0. TOS se especifica como un valor decimal que oscila entre 0 y 255.

-r recuento Especifica que la opción Registrar ruta del encabezado IP se utiliza para registrar la ruta que toma el mensaje de solicitud de eco y el mensaje correspondiente de respuesta de eco. Cada salto de la ruta utiliza una entrada de la opción Registrar ruta. Si es posible, especifique un recuento igual o mayor que el número de saltos realizados entre el origen y el destino. El valor de Recuento debe estar entre 1 y 9.

-s Recuento Especifica que la opción Fecha Internet del encabezado IP se utiliza para registrar la hora de llegada del mensaje de solicitud de eco y el mensaje correspondiente de respuesta de eco para cada salto. El valor de Recuento debe estar entre 1 y 4.

Para realizar un ping al destino 10.0.99.221 y resolver 10.0.99.221 a su nombre de host, se debe escribir:

ping -a 10.0.99.221

Para realizar un ping al destino 10.0.99.221 con mensajes de solicitud de eco, cada uno con un campo Datos de 1000 bytes, se debe escribir:

ping -n 10 -l 1000 10.0.99.221

Para realizar ping al destino 10.0.99.221 y registrar la ruta de 4 saltos, se debe escribir:

ping -r 4 10.0.99.221

2.6.9. USO DE COMANDO TELNET

Después de verificar que hay comunicación entre los dispositivos en el simulador, se debe continuar con la configuración del router mediante el comando telnet desde el configure terminal (visto anteriormente) ejecutando el comando “line vty 0 4”:

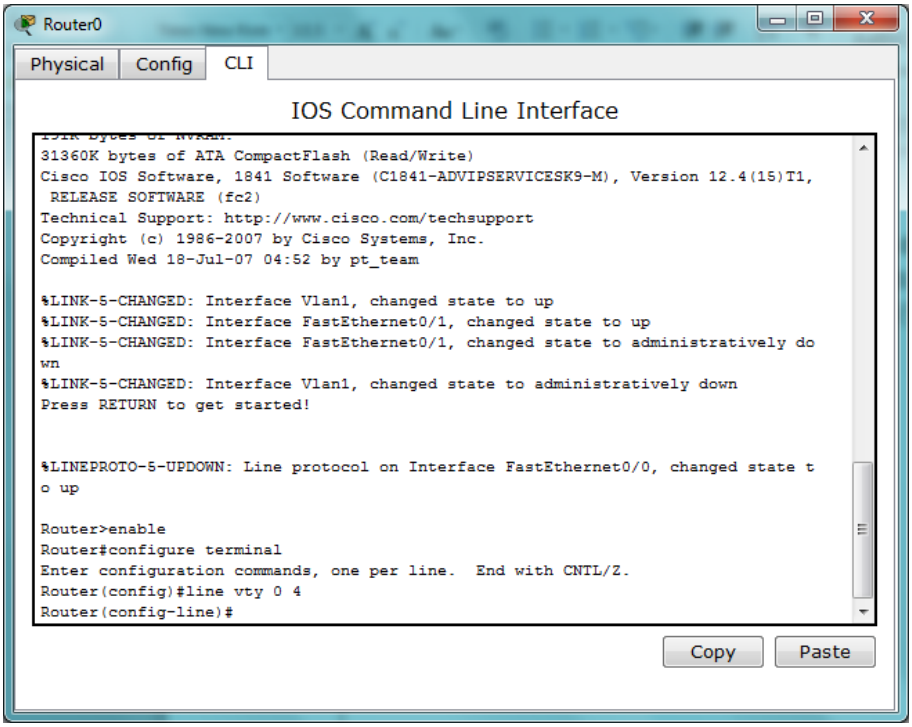


Figura 57. Imagen de configure terminal.
Tomado de Herrera, R. (2014).

Se procede a ejecutar el comando password y “laboratorio” será la contraseña que otorgará o permitirá el acceso como se muestra en la imagen:

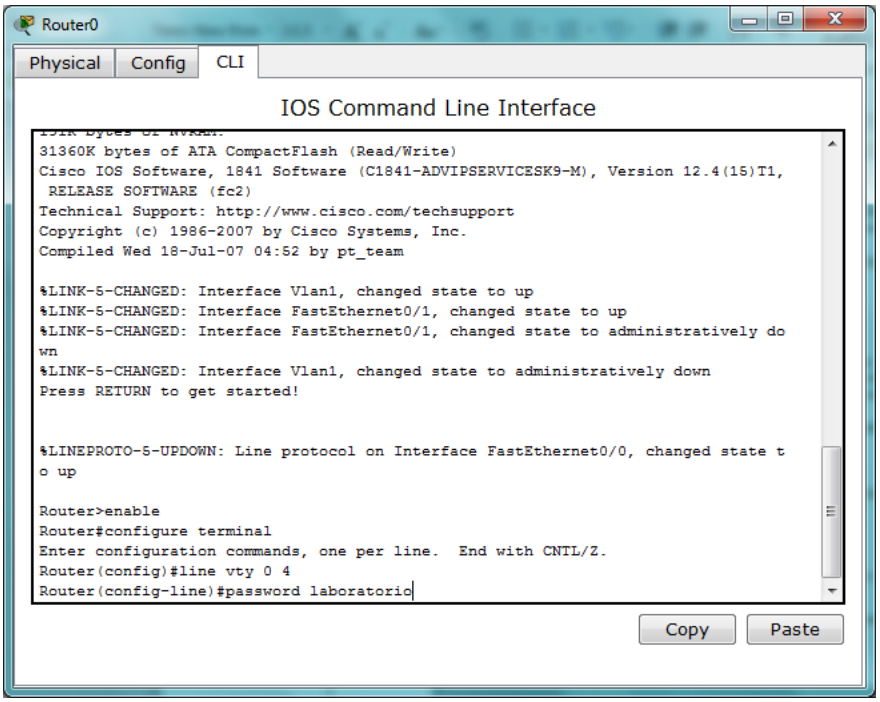


Figura 58. Configuración de password.
Tomado de Herrera, R. (2014).

Posteriormente el comando login seguido de un exit para terminar la configuración.

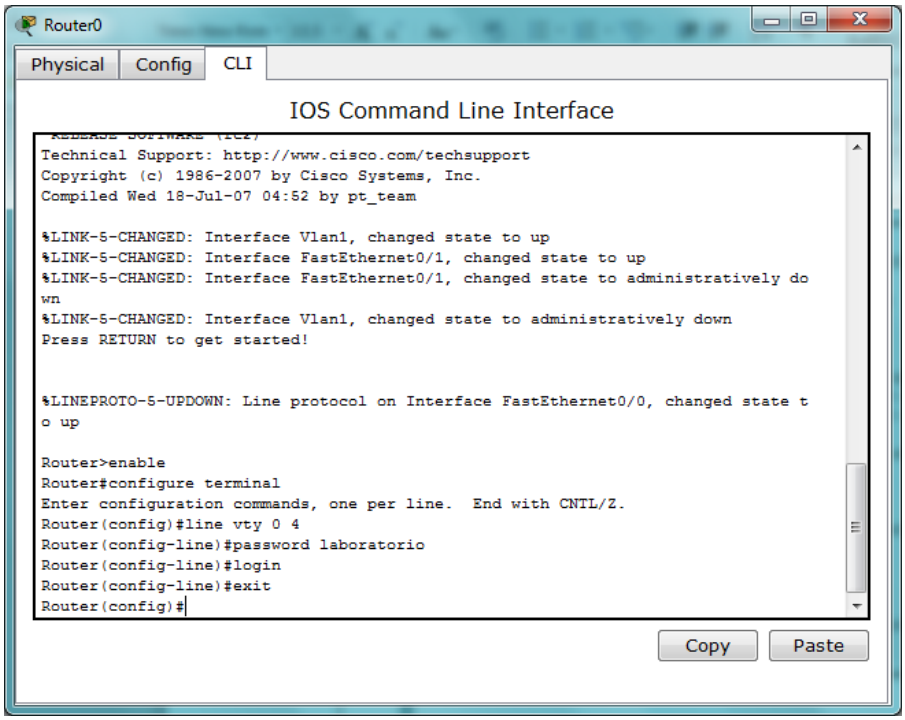


Figura 59. Salida a la raíz del terminal.
Tomado de Herrera, R. (2014).

Finalmente se va a comprobar que la configuración está levantada y funcionando correctamente. Se debe ingresar desde el modo de comando al PC e ingresar remotamente al router para controlarlo remotamente y ahí hacer un ping hacía el PC.

Para ello desde el modo comando, en la PC, se ejecuta el comando telnet seguido de la dirección IP a la que se desea acceder e ingresar como muestra la siguiente figura:

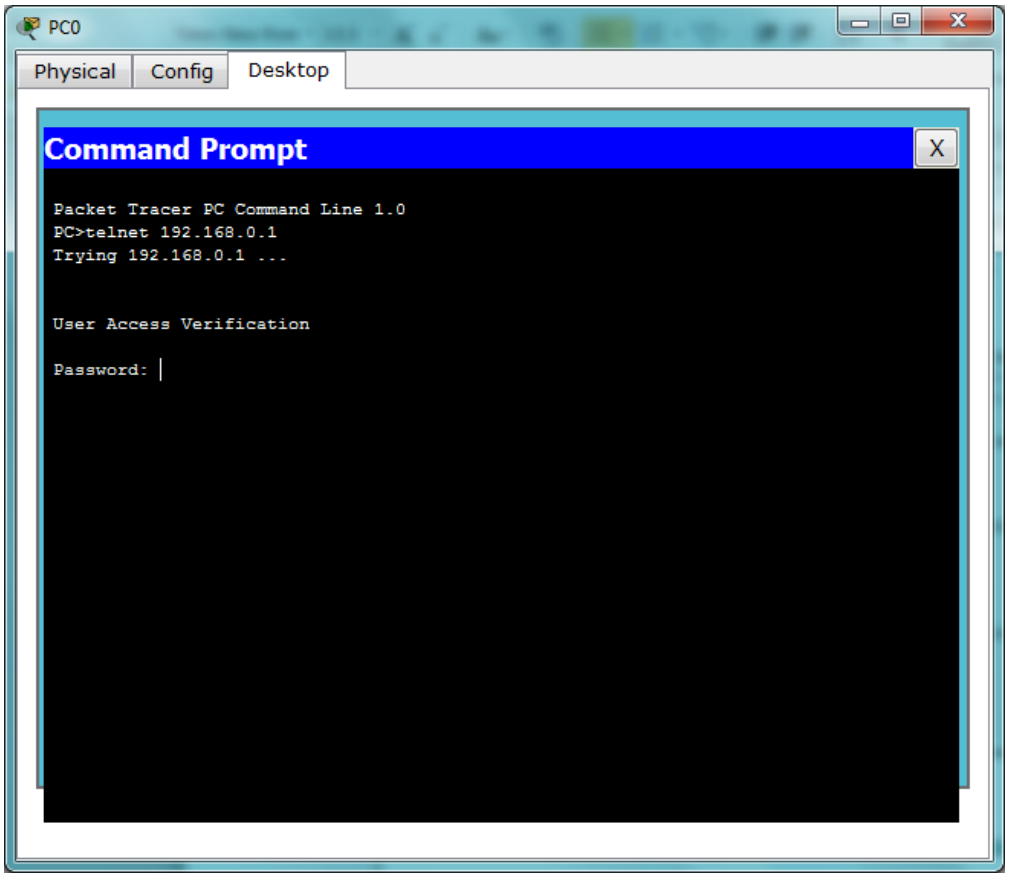


Figura 60. Login de comando telnet.
Tomado de Herrera, R. (2014).

En este punto se puede observar que el ingreso al router está limitado por una contraseña que en este caso es “laboratorio” y que al ingresarla se permitirá el acceso y control total, se debe escribir aunque al momento de digitar no sea mostrada. Para demostrar que el comando telnet si está activo y funcionando correctamente se precede con un ping hacia el PC desde el router y desplegará respuesta.

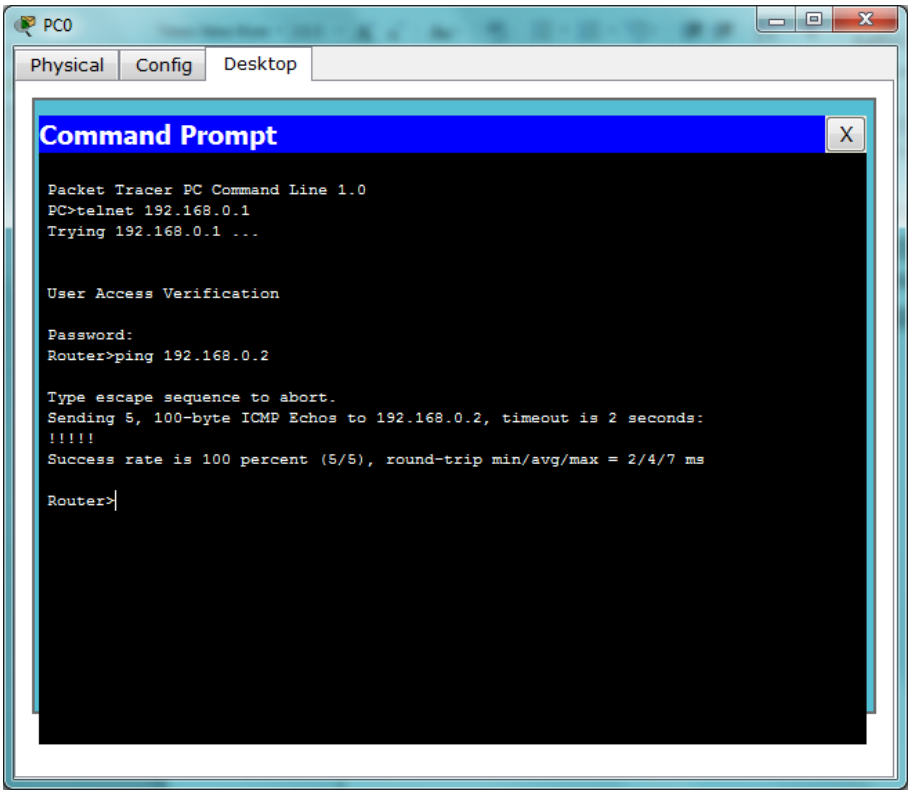


Figura 61. Ingreso al dispositivo remoto.
Tomado de Herrera, R. (2014).

Como se puede observar los paquetes que se enviaron llegaron al computador y se obtuvo respuesta por lo que se puede declarar que la configuración y comunicación de los equipos fue un éxito.

2.6.10. USO DE COMANDO FTP (File Transfer Protocol)

Para entender mejor el manejo y uso de FTP se realizará una práctica en el simulador de packet tracer donde se deberá tener la siguiente estructura configurando los equipos como se realizó anteriormente:

Red "A"

Computador 1	: 192.168.1.2	255.255.255.0
Computador 2	: 192.168.1.3	255.255.255.0
Interface Router Fa0/0	: 192.168.1.1	255.255.255.0

Un switch

Red “B”

Un servidor	: 192.168.2.2	255.255.255.0
Interface Router Fa0/1	: 192.168.2.1	255.255.255.0

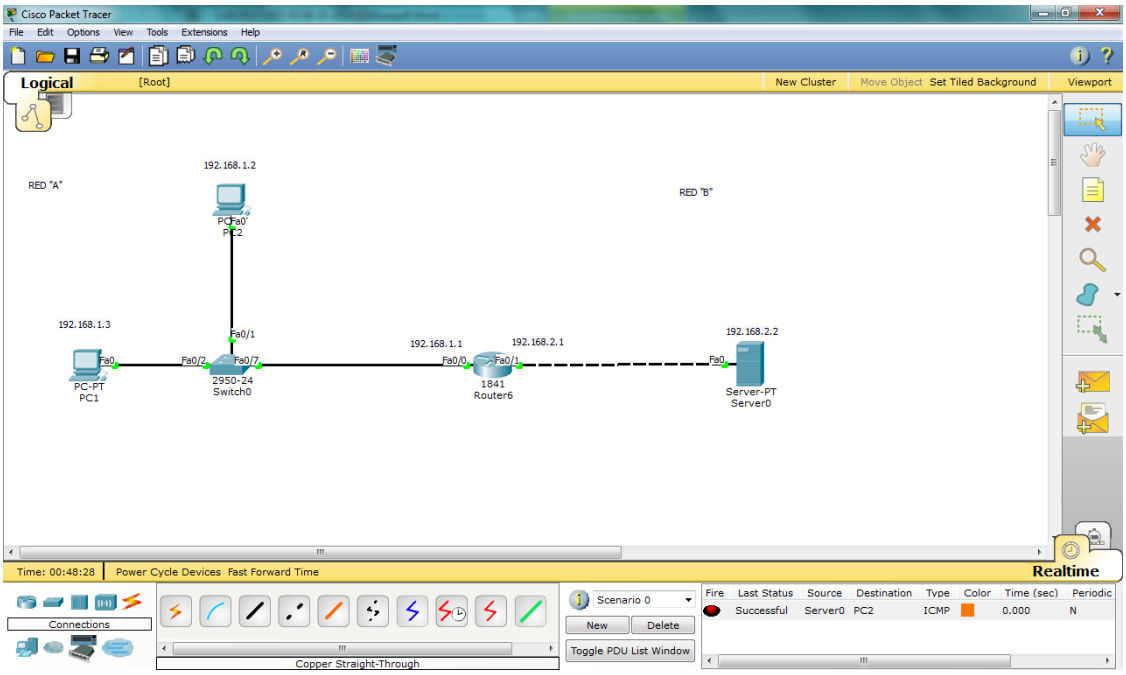


Figura 62. Interfaces de equipos.
Tomado de Herrera, R. (2014).

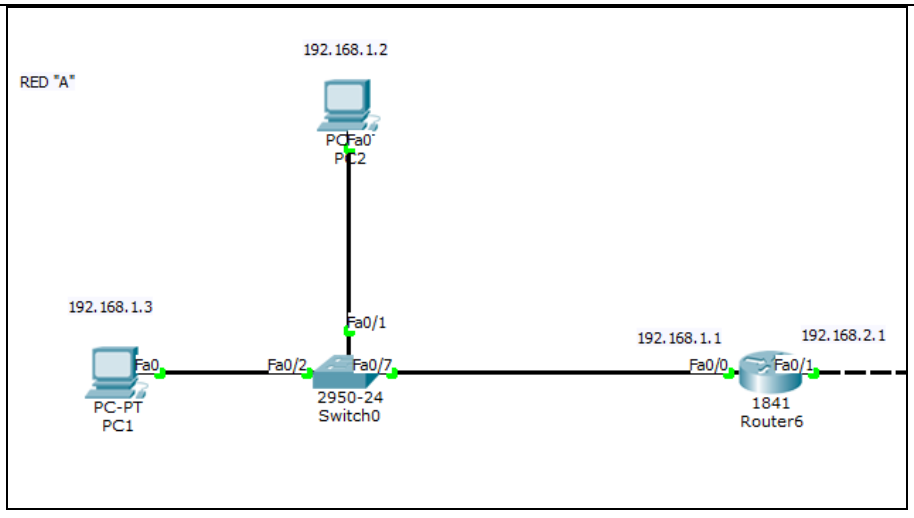


Figura 63. Interface Red A.
Tomado de Herrera, R. (2014).

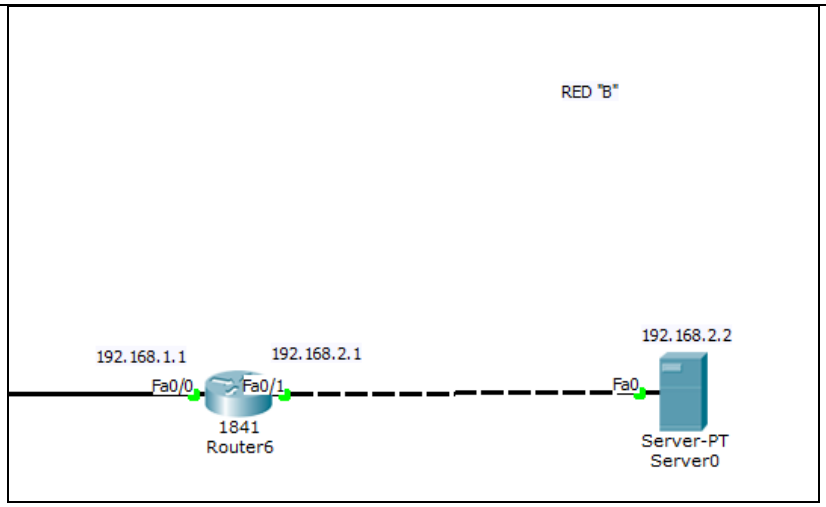


Figura 64. Red B.
Tomado de Herrera, R. (2014).

En este momento se procederá con la configuración del servidor simplemente dando clic en el dispositivo para que se muestre la ventana y seleccionar la pestaña “Config”:

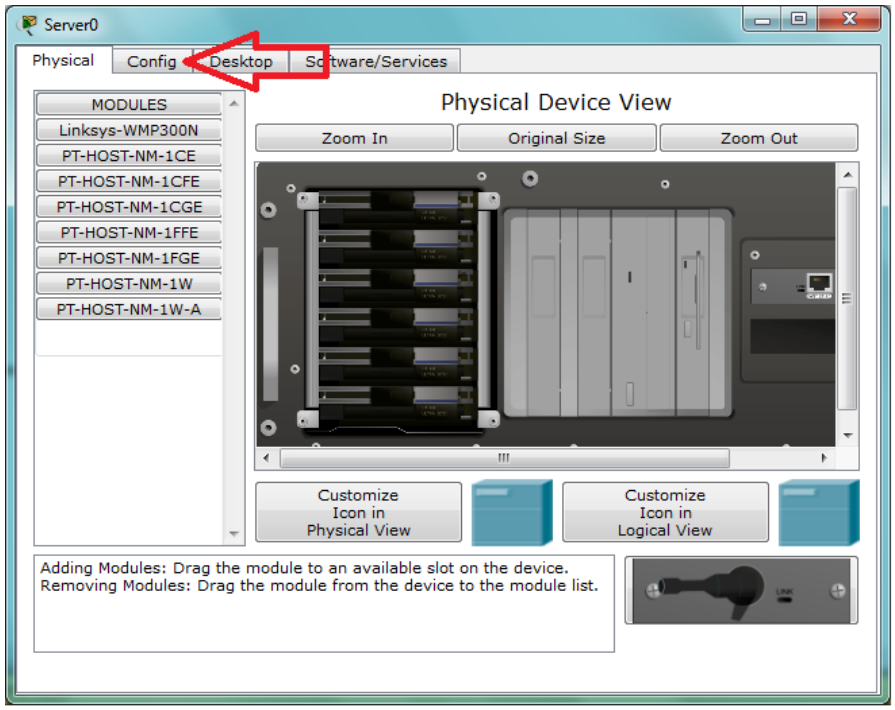


Figura 65. Configuración de terminal.
Tomado de Herrera, R. (2014).

Se despliega la siguiente ventana donde la opción a escoger será “FTP”

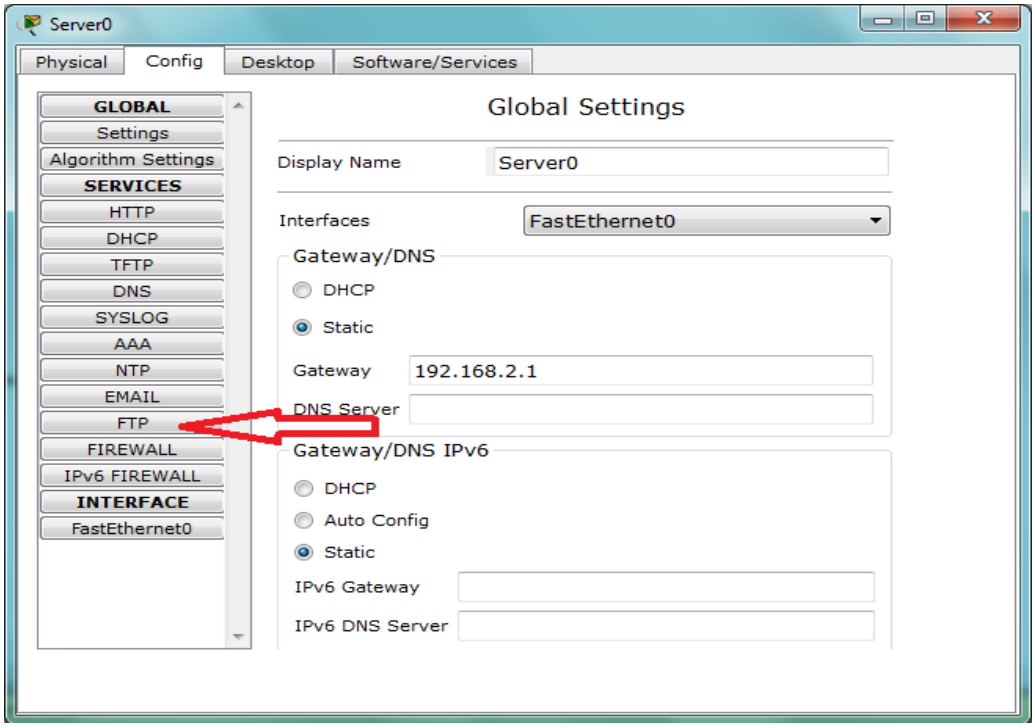


Figura 66. Configuración FTP.
Tomado de Herrera, R. (2014).

Posteriormente desplegará una ventana con varias opciones en donde se debe ingresar un nombre de usuario y un password (en este caso será servidorftp como usuario y 1234 como password) éstos servirán para poder realizar el login de tal manera que se transfieran los datos. Se debe activar las opciones: Write, Read, Delete, Rename, List y dar clic en el símbolo “+”.

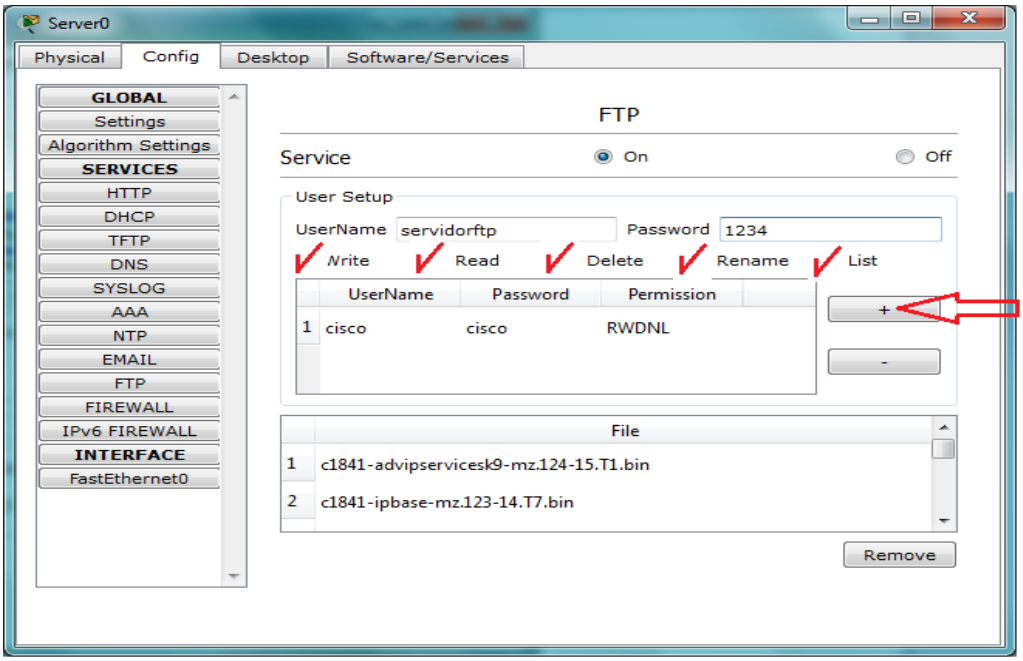


Figura 67. Activar permisos.
Tomado de Herrera, R. (2014).

Quedará una ventana de la siguiente manera:

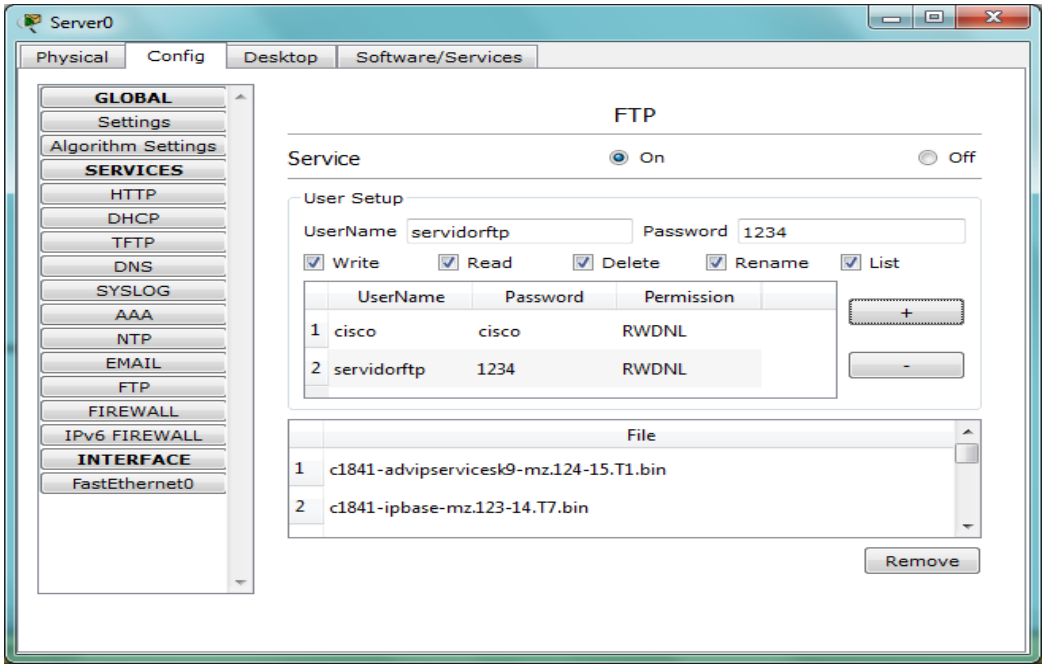


Figura 68. Servicio configurado.
Tomado de Herrera, R. (2014).

Ahora queda configurar el router para que se autentique con el servidor FTP, hay que tener en cuenta que los datos de usuario y password deben ser exactos a aquellos que se configuró en el servidor. Ahora queda ingresar al router en el terminal y ejecutar los comandos:

ip ftp username servidor ftp

ip ftp password 1234

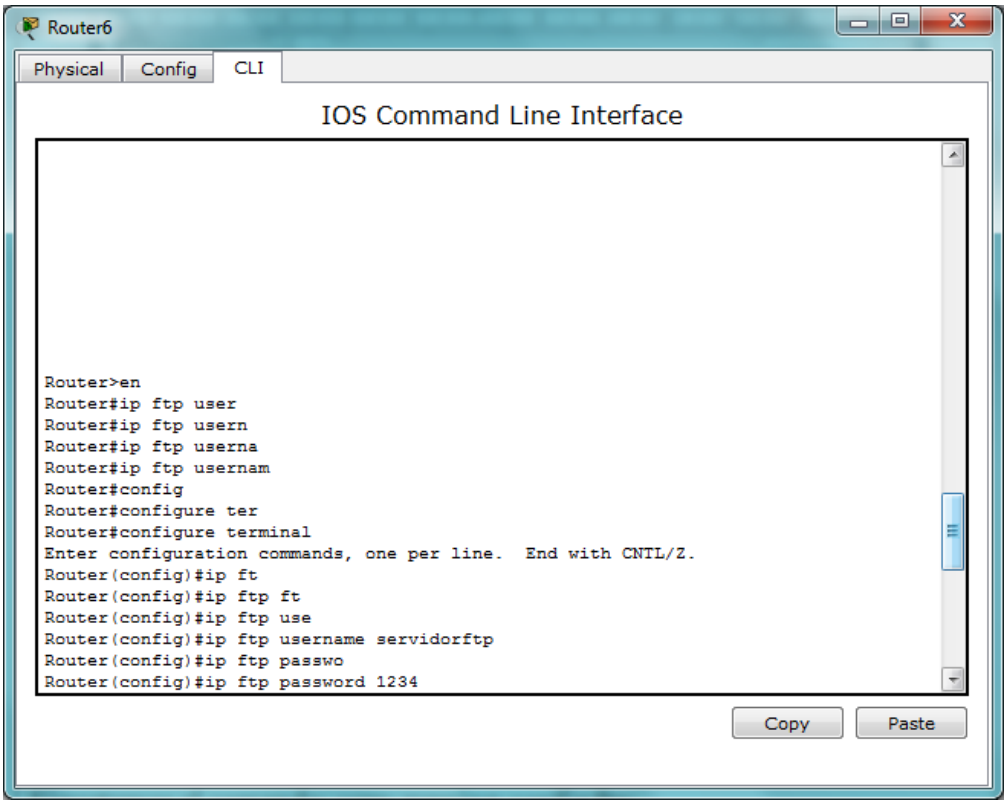


Figura 69. Configuración ftp.
Tomado de Herrera, R. (2014).

Se procederá a realizar una copia de la configuración en el servidor FTP ejecutando el comando: copy running-config ftp:

En esta línea solicitará la IP del servidor ftp donde se desea guardar el archivo respaldo de configuración, se procede a insertarla de la siguiente manera:

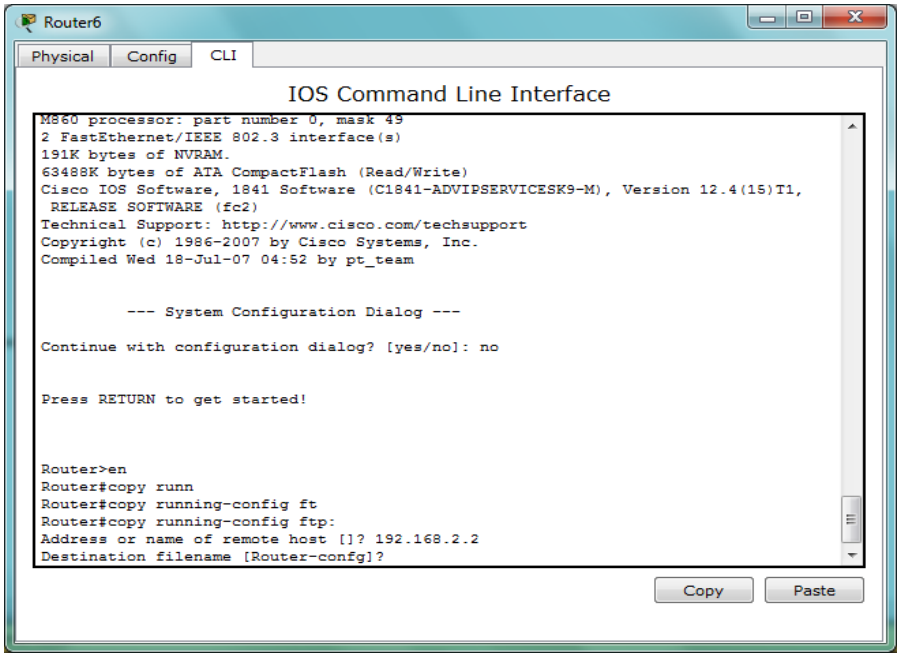


Figura 70. Respaldo de configuración.
Tomado de Herrera, R. (2014).

El nombre que se ingresara en este caso será respaldo_ftp y ejecutarlo.

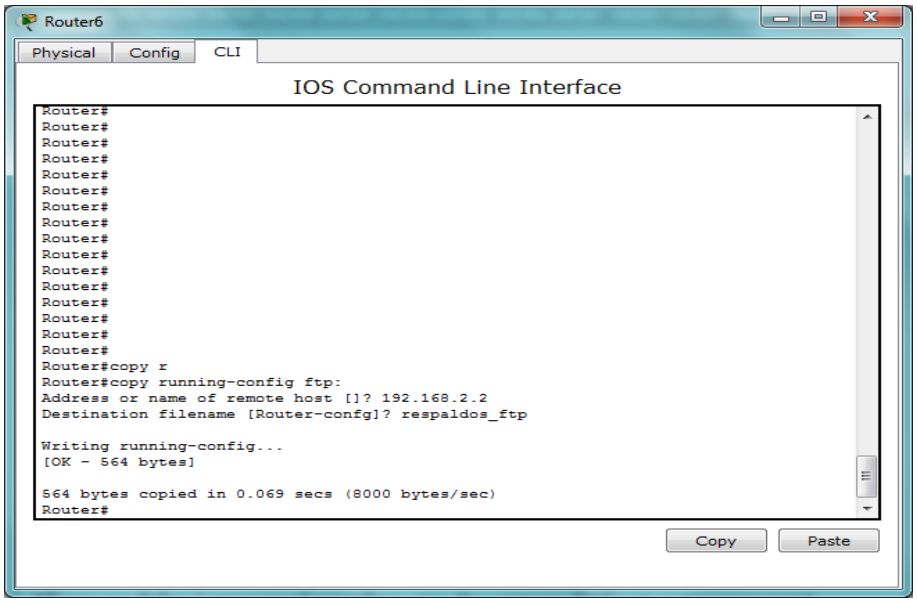


Figura 71. Se sube archivo a servidor.
Tomado de Herrera, R. (2014).

En este punto indicará que el archivo subió correctamente y se puede verificar desde el servidor:

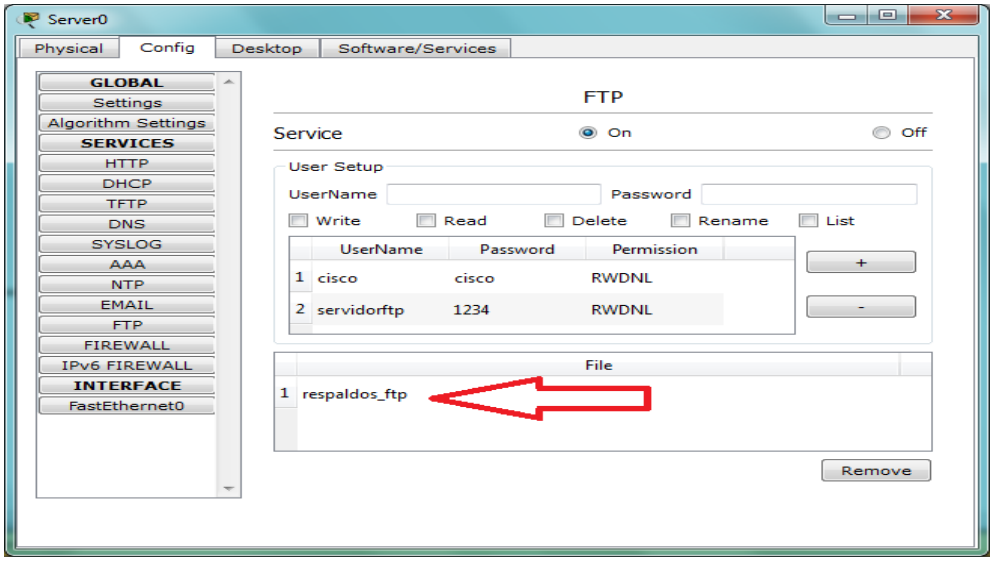


Figura 72. Archivo subido.
Tomado de Herrera, R. (2014)

Ya aquí se realizará la descarga desde el computador 1 en la red “A” desde el servidor, solo con ingresar al modo comando y ejecutando el comando ftp + ip, se podrá observar que el promt a cambiado por ftp>. Significa que se logró ingresar al servidor: ftp 192.168.2.2

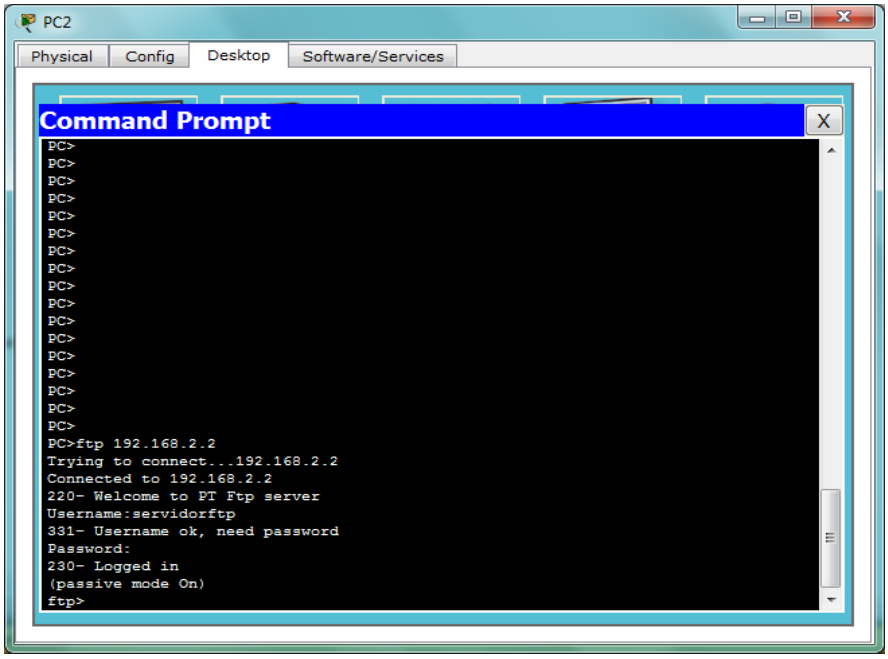


Figura 73. Acceso a FTP server.
Tomado de Herrera, R. (2014).

Con el comando dir se podrá enlistar los archivos alojados en el servidor mostrando el archivo respaldos_ftp.

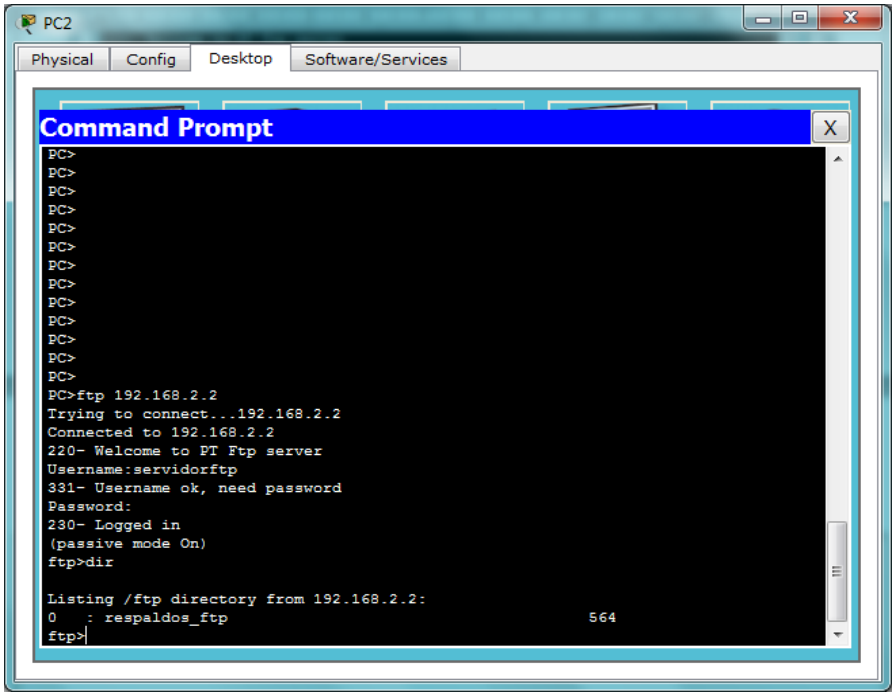


Figura 74. Listado de archivos disponibles.
Tomado de Herrera, R. (2014).

Para descargar el archivo al equipo local se debe ejecutar el comando get [nombre del archivo] como se muestra a continuación:

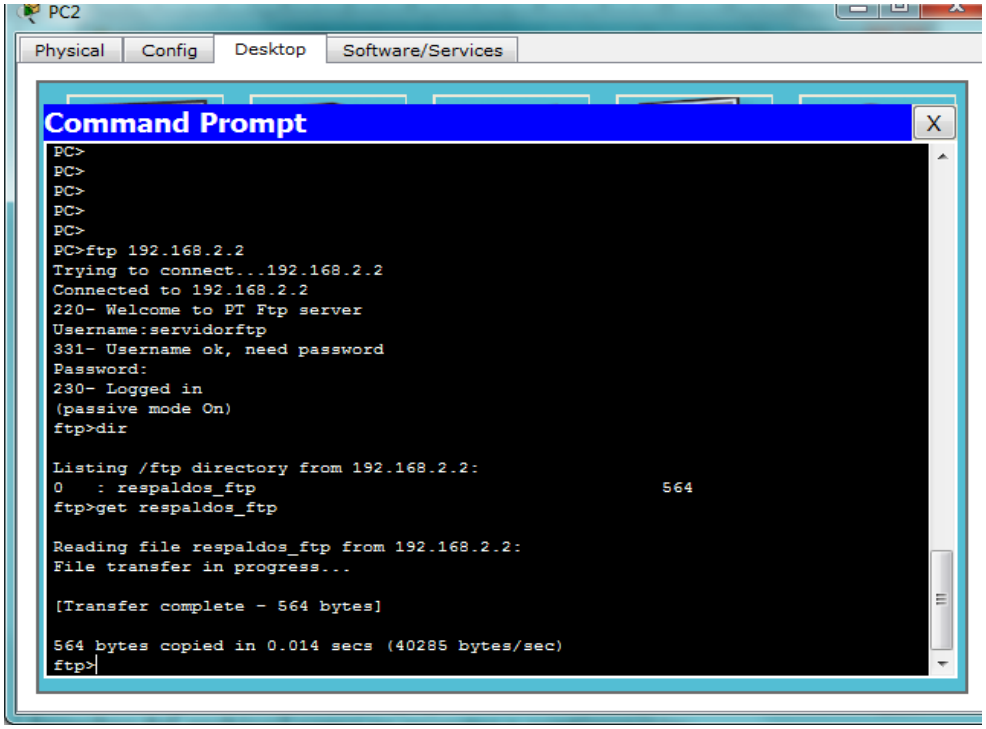


Figura 75. Archivo enlistado.
Tomado de Herrera, R. (2014).

En la ventana anterior se puede observar que el archivo se copió o transfirió correctamente.

Lo siguiente será verificar que el archivo se encuentre en el equipo. Para ello hay que ejecutar el comando quit para salir del servidor hacia el equipo local y ejecutar el comando dir para mostrar el archivo:

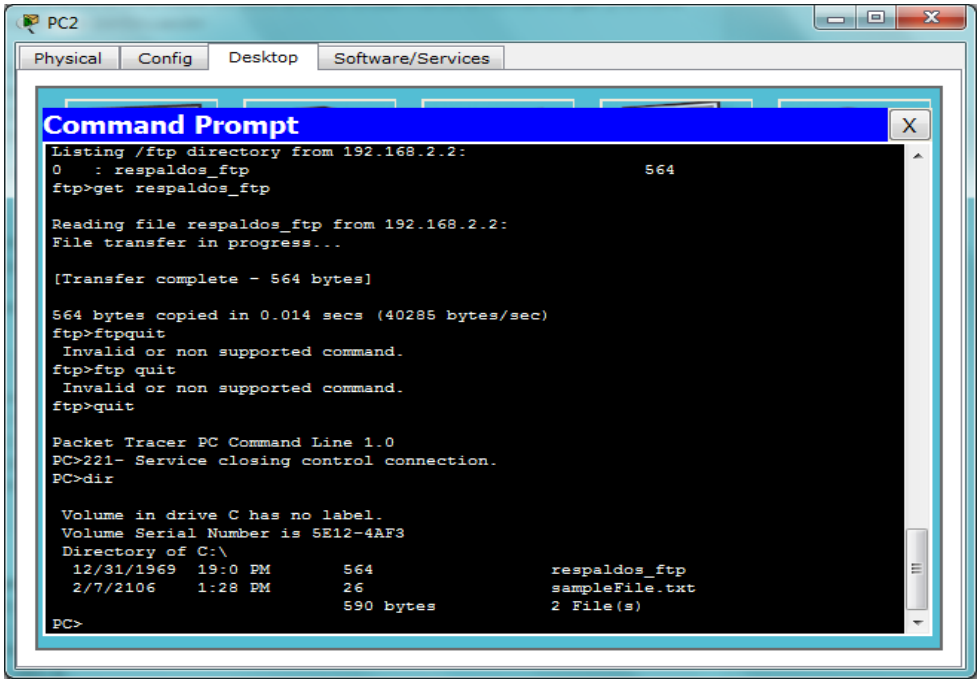


Figura 76. Comando dir.
Tomado de Herrera, R. (2014).

Con esto ha quedado demostrado la conexión y transferencia de archivos desde un computador, cualquiera que sea de la red “A”, hacia el servidor.

2.7. RESULTADO DE LA PRÁCTICA

- Aprendizaje en el manejo de comandos ping, ipconfig, telnet, ftp, tracert.
- El laboratorio se llevó a cabo sin ningún tipo de inconveniente y funcionando correctamente en el proceso.
- Pruebas realizadas en el simulador permitiendo al estudiante identificar cada una de las funciones de los comandos mencionados siendo un éxito total.

2.8. CONCLUSIONES Y RECOMENDACIONES

- En este capítulo se dio un vistazo del uso del comando ping y su facilidad para determinar si hay conexión lógica entre equipos tecnológicos como son los computadores utilizados en la práctica.

- El laboratorio se llevó a cabo sin ningún tipo de inconveniente y a satisfacción total de los estudiantes y profesor demostrando conexión remota hasta equipos en distintos lugares.
- Existen comandos que permiten administrar una red de manera remota y obtener información de su configuración en la red.
- Mediante el comando FTP se puede obtener información remota desde equipos lejanos mediante una configuración realmente fácil.

CAPITULO III

3. Realizar la configuración de una red utilizando la herramienta de subneting, con la misma cantidad de computadores pero en distintas redes virtuales y demostrando conectividad entre las redes virtuales.

3.1. OBJETIVO GENERAL

Configurar una red con la herramienta de subneting, con la misma cantidad de computadores pero en distintas redes virtuales y demostrar conectividad entre las redes.

3.2. OBJETIVOS ESPECÍFICOS

- Dividir una red en partes iguales modificando la máscara de red.
- Optimizar la red con solo segmentar la red y obtener un mejor rendimiento.

3.3. DESCRIPCIÓN DE EQUIPOS / HERRAMIENTAS / SOFTWARE / MATERIALES

3.3.1. PROVISTOS POR LA UNIVERSIDAD

- Simulador de Packet Tracert
- Equipos de laboratorio

3.4. TRABAJO PREPARATORIO

- El estudiante debe tener conocimientos en numeración binaria y decimal para el entendimiento y desarrollo de las prácticas.

3.5. INTRODUCIÓN / MARCO TEORICO

3.5.1. SUBNETTING

Como Eduardo Collado Cabeza (2009, pp. 28) ya lo dijo “La estructura física y lógica de la red debe permitir el flujo de datos de la empresa”.

Para el correcto funcionamiento y flujo de estos datos los equipos deben permanecer en la misma red lógica.

Como José Huidobro (2007, pp. 227) ya lo dijo “El subnetting consiste en la creación de varias redes lógicas a partir de una sola clase de direcciones IP, reduciendo así el coste que supondría la obtención de otra clase de direcciones”.

El rango de direcciones IP asignados en una red, siempre contiene dos direcciones no utilizables para los host que determinan el inicio y fin de las direcciones IP o sus rangos llamadas RED y Broadcast.

3.5.2. Máscara De Red

La máscara de red determina un rango de red, es decir, el número de direcciones IP’s dentro de una red o subred. Dada una dirección IP, una máscara de red y un cálculo se puede determinar el rango de red al que pertenece el dispositivo u ordenador.

Una máscara de red está compuesta por 4 octetos de 8 bits cada uno.

255.255.255. 0 = 11111111. 11111111. 11111111.00000000

3.5.3. Tabla Exponencial:

Esta tabla permitirá realizar el cálculo de las direcciones IP’s disponibles en una subred.

Máscara de red		**Máscara de red (bits)**
255.255.255.0	=>	11111111 . 11111111 . 11111111 . 0

Octeto decimal		**Octeto Binario (Bit Octeto)**
255	=>	11111111

Es necesario saber cómo está compuesto un octeto en la máscara de red. Por tal motivo se procederá con la revisión de una sencilla tabla la cual se muestra a continuación:

Tabla 1. Tabla exponencial de valores de bits que conforman el octeto de máscara de red

Bit Octeto	1	1	1	1	1	1	1	1
Exponente	7	6	5	4	3	2	1	0
Base	2	2	2	2	2	2	2	2
Resultado	128	64	32	16	8	4	2	1

.

Nota: Cada bit octeto de la máscara de red debe estar representado por la base 2 y elevado a un exponente en secuencia empezando desde cero (0), para así obtener varios resultados, los cuales sumados proporcionarán el resultado buscado; al momento de realizar los cálculos hay que tomar en cuenta que en los bits octeto que estén en 0 no serán tomados en cuenta pues no representan ningún valor.

En el ejemplo de la tabla el cálculo sería:

1 + 2 + 4 + 8 +16 + 32 + 64 + 128 = 255

El resultado es 255, valor representado en decimal, en la máscara de red.

3.6. DESARROLLO DE LA PRÁCTICA

En primer lugar se debe determinar los parámetros a utilizarse en el laboratorio, definiendo:

Creación de 4 subredes (64 IPS cada una)

La IP a utilizar será: 192.168.1.0 (clase C).

Por el hecho de que se utiliza una dirección clase C significa que solo se puede modificar el primer octeto en la máscara de red definiendo así las subredes como muestra la imagen:

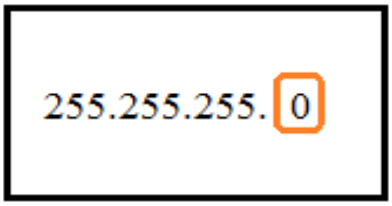


Figura 77. Imagen de una máscara de red.
Tomado de Herrera, R. (2014).

3.6.1. CREACIÓN DE LA PRIMERA SUBRED

A continuación se debe determinar el número de hosts en cada una de las subredes que se desea. Se necesitan 4 subredes en el laboratorio por lo que hay que la siguiente fórmula será de gran ayuda:

$$2^n - 2 > \text{Número de hosts}$$

En la fórmula “n” representa el exponente que ayudará a determinar el número de bits o host que se necesite para la creación de la subred mientras que se resta 2 pues un rango de IP’s necesita de una dirección de red y broadcast para delimitar las subredes.

En el presente caso el exponente a utilizar será 6 quedando como resultado 64 hosts.

$$64 - 2 > 62$$

En este punto se puede observar que se dispone de 62 IP’s las cuales son utilizables para cada uno de los dispositivos que se necesitan para interconectar entre sí a nuestra subred.

Se procederá a trabajar con los bits de la máscara de red para entender mejor el funcionamiento del subnetting.

El exponente 6 indica que se debe tomar los 6 últimos bits del primer octeto y para los host que se marcará de color rojo mientras que los dos bits de color azul determinan la máscara que se necesita para la configuración del laboratorio y se calcula con la tabla exponencial mencionada anteriormente.

11111111. 11111111. 11111111.11000000

Tabla 2. Tabla para el cálculo de una máscara de red.

	Octeto	**Octeto**	**Octeto**	**Octeto**
IP RED	192	168	1	0
Bits	11111111	11111111	11111111	11000000
Máscara	255	255	255	192

Realizado el cálculo y como resultado de máscara de red 192 se puede saber que se dispone de 4 Subredes de 64 IP's cada una y conformadas de la siguiente manera:

Tabla 3. Lista de direcciones IP disponibles, red y broadcast.

RED	**BROADCAST**	**IP's válida desde**	**IP's válida hasta**	**IP's Válidas**
0	63	1	62	62
64	127	65	122	62
128	191	125	190	62
192	255	193	254	62

Por consiguiente:

- La dirección IP será : 192.168.1.0
- Rango de IP : 192.168.1.1 hasta 192.168.1.62
- Máscara de red : 255.255.255.192 // 26
- Número de IP válidas : 62
- Número de Subredes : 4

3.6.2. PACKET TRACER

En este punto se hará uso del simulador para demostrar la conectividad de los equipos. Se debe montar el siguiente escenario:

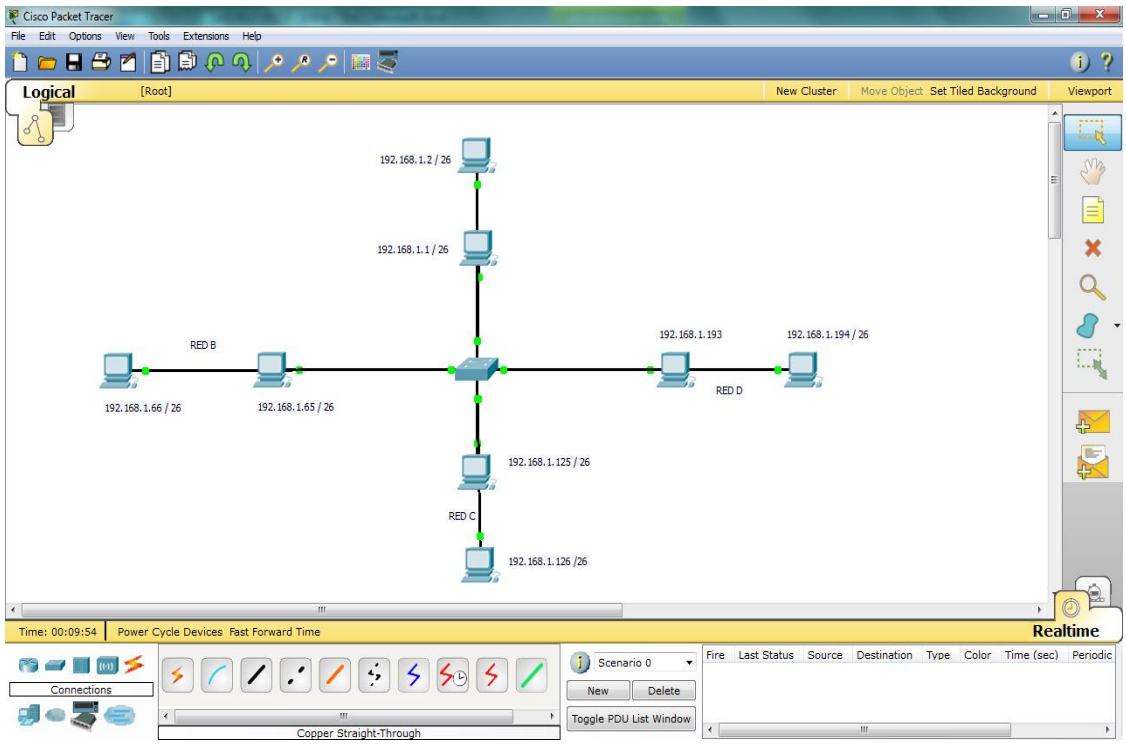


Figura 78. Imagen de la estructura necesaria para elaborar el laboratorio. Tomado de Herrera, R. (2014).

En el presente escenario hay 1 red LAN la cual esta segmentada en 4 subredes ordenadas y bien definidas.

Red A, B, C Y D: compuesto por dos computadores los cuales están en el mismo rango de IP's para comprobar la conectividad de cada dispositivo en su misma red y en diferentes.

Red A: En este momento se procederá con la comprobación de la conectividad entre los computadores de la RED A.

En este caso utilizar el comando ping entre computadores que se encuentran en el mismo rango como son: el computador 1 (192.168.1.1 /26) con el computador 2 (192.168.1.2 /26).

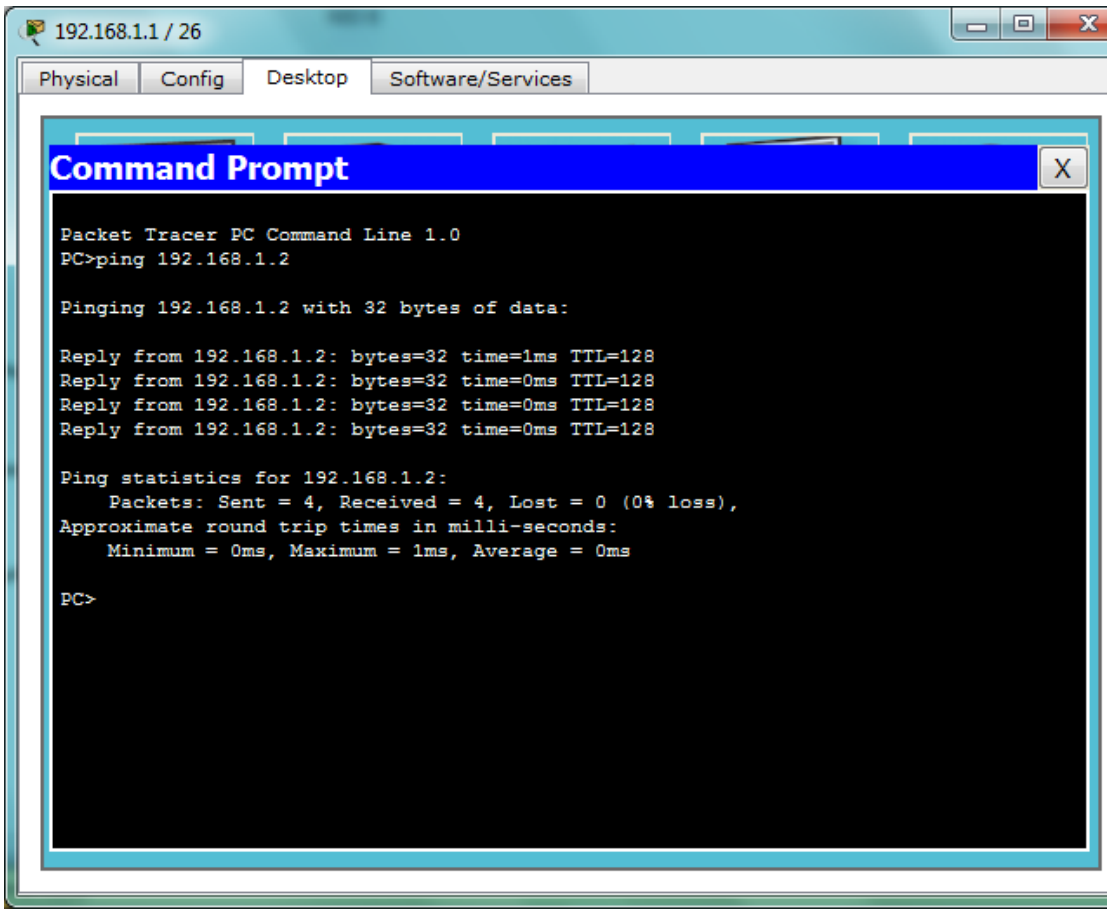


Figura 79. Prueba de conectividad entre equipos mediante el comando PING. Tomado de Herrera, R. (2014).

Como se puede observar si hay conexión entre los dos computadores en la misma red.

Ahora queda demostrar que no hay conexión entre en computador 2 (192.168.1.2 /26) con el computador 3 (192.168.1.65 /26) que se encuentra en otro rango de dirección IP u otra Subred.

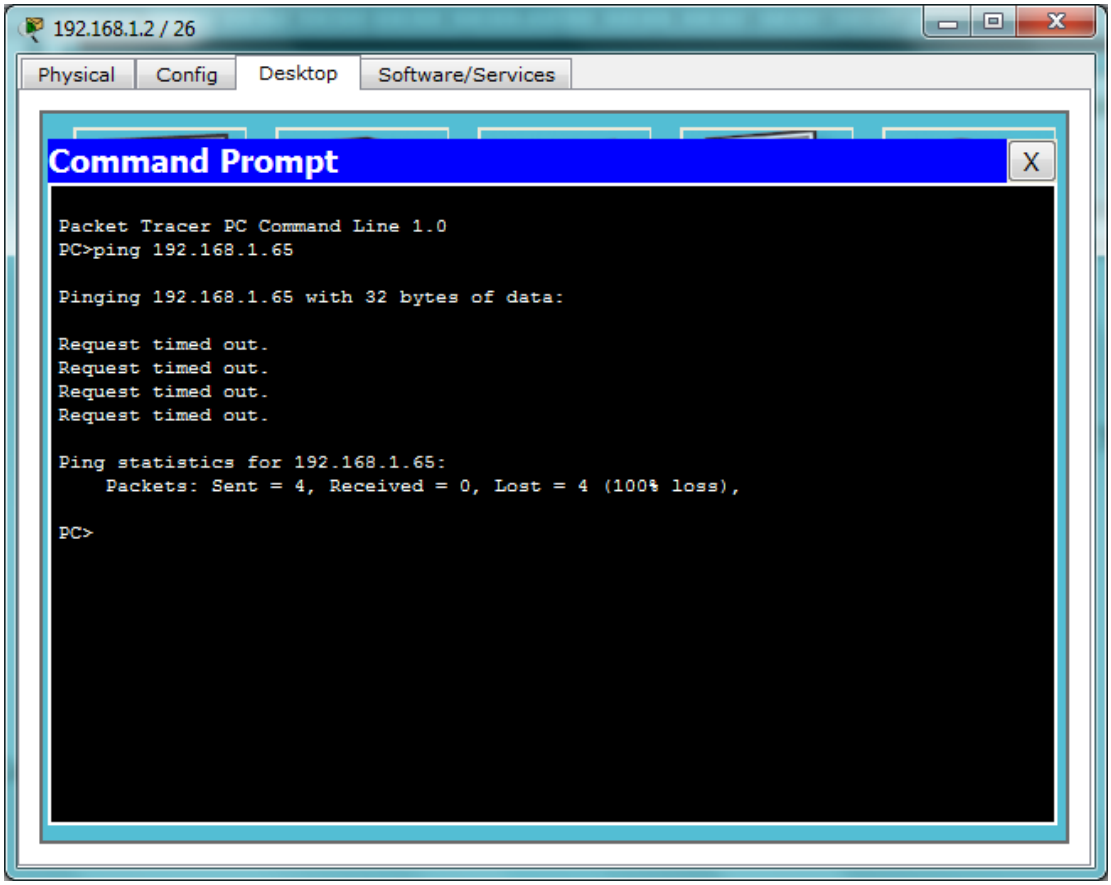


Figura 80. Prueba de conectividad entre equipos mediante el comando PING. Tomado de Herrera, R. (2014).

Como se pudo apreciar en la imagen la conectividad es nula y así queda demostrado que no hay ningún tipo de conexión.

El mismo procedimiento se puede realizar con las demás subredes y el resultado sería el mismo. No hay conectividad entre equipos que se encuentren en una subred diferente.

3.7. RESULTADO DE LA PRÁCTICA

Si los equipos pertenecen a una subred diferente con otra máscara de red no podrán tener conectividad con otras subredes lo cual es de gran ayuda para delimitar departamentos y tenerlos bien definidos en una empresa por ejemplo: área de contabilidad, gerencia, RRHH, etc.

3.8. CONCLUSIONES Y RECOMENDACIONES

- Se pudo apreciar que la máscara de red es la encargada de determinar los números de subredes.
- El laboratorio se llevó a cabo sin ningún tipo de inconveniente siendo un éxito.

CAPITULO IV

4. Realizar la configuración y segmentar los equipos de una red que la conforman mediante el uso de VLSM en distintos números de equipos en cada una de las redes virtuales y demostrando su conectividad en el laboratorio de la Universidad De Las Américas.

4.1. OBJETIVO GENERAL

Configurar y segmentar los equipos de una red que la conforman mediante el uso de VLSM en distintos números de quipos en cada una de las redes virtuales y demostrando su conectividad en el laboratorio de la Universidad de las Américas.

4.2. OBJETIVOS ESPECÍFICOS

- Explotar los beneficios y características que contribuyen las VLAN.
- Identificar el funcionamiento de las VLAN's.
- Configurar VLAN's básicas.

4.3. DESCRIPCIÓN DE EQUIPOS / HERRAMIENTAS / SOFTWARE / MATERIALES

4.3.1. PROVISTOS POR LA UNIVERSIDAD

- Simulador de Packet Tracert
- Equipos del laboratorio de la Universidad de las Américas.

4.4. TRABAJO PREPARATORIO

- El estudiante debe consultar previamente y prepararse sobre el funcionamiento del comando ping y un estudio acerca de las clases de direcciones IP con sus respectivas máscaras de subred.
- Conocimiento básico sobre las direcciones IP.

4.5. INTRODUCIÓN / MARCO TEORICO

Como Eduardo Collado Cabeza (2009, pp. 36) ya lo dijo "La utilización de VLSM dentro de las redes de la organización responde a que rara vez las

organizaciones tienen repartidos de forma uniforme los hosts, entonces utilizan VLSM para adecuar la estructura de su red a las necesidades de la empresa.

4.6. DESARROLLO DE LA PRÁCTICA

Para el desarrollo del laboratorio hay que determinar los parámetros que se utilizarán, definiendo:

4.6.1. Creación de 3 redes virtuales

- La primera subred será de 32 hosts
- La segunda subred será de 14 hosts
- La tercera subred será de 8 hosts
- La IP a utilizar será: 192.168.1.0 (clase C).

4.6.2. CREACIÓN DE LA PRIMERA SUBRED DE 32 HOSTS.

Se debe utilizar la fórmula:

$2^n - 2 >$ Número de hosts

$64 - 2 > 62$

11111111. 11111111. 11111111.11000000

Realizado el cálculo y como resultado de máscara de red 192 se puede saber que:

Por consiguiente:

- La dirección IP será : 192.168.1.0
- Rango de IP : 192.168.1.1 hasta 192.168.1.62
- Máscara de red : 255.255.255.192 // 26
- Número de IP válidas : 62
- Número de Subredes : 4

Tabla 4 Rango de direcciones IP's de red y broadcast de la red mencionada.

Rango	
Desde	Hasta
0	63
64	127
128	191
192	255

4.6.3. CREACIÓN DE LA SEGUNDA SUBRED DE 14 HOSTS.

Por consiguiente:

- La dirección IP será : 192.168.1.0
- Rango de IP : 192.168.1.1 hasta 192.168.1.14
- Máscara de red : 255.255.255.240 // 28
- Número de IP válidas : 14
- Número de Subredes : 16

Tabla 5. Rango de direcciones IP's de red y broadcast de la red mencionada.

Rangos	
Desde	Hasta
0	14
15	29
30	44
45	59
60	74
75	89
90	104
105	119
120	134
135	149
150	164
165	179

Rangos	
180	194
195	209
210	224
225	239
240	254

4.6.4. CREACIÓN DE LA TERCERA SUBRED DE 5 HOSTS.

Por consiguiente:

- La dirección IP será : 192.168.1.0
- Rango de IP : 192.168.1.1 hasta 192.168.1.6
- Máscara de red : 255.255.255.248 // 29
- Número de IP válidas : 6
- Número de Subredes : 32

4.6.5. PACKET TRACER

En este punto se hará uso del simulador para demostrar la conectividad de los equipos. Se debe montar el siguiente escenario:

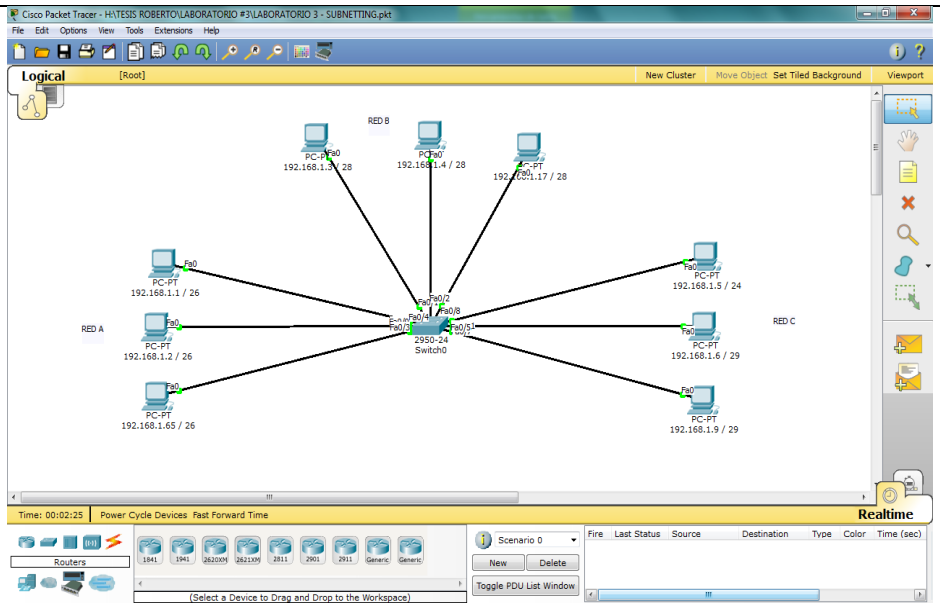


Figura 81. Imagen de estructura de la red para realizar la práctica. Tomado de Herrera, R. (2014).

En el presente escenario hay 1 red LAN la cual esta segmentada en 3 subredes:

- Cada subred se encuentra ordenada y bien definida.
- Red A, B, C: compuesto por tres computadores, dos de los cuales están en el mismo rango de IP's; el tercer computador se encuentra en un rango diferente para comprobar la conectividad de cada dispositivo.

4.6.5.1. Comprobación de conectividad en equipos de la misma red

Red A: En este momento se procederá con la comprobación de la conectividad entre los computadores de la RED A.

Se utilizará el comando ping y comprobar la conectividad entre computadores que se encuentran en el mismo rango como son: el computador 1 (192.168.1.1 /26) con el computador 2 (192.168.1.2 /26).

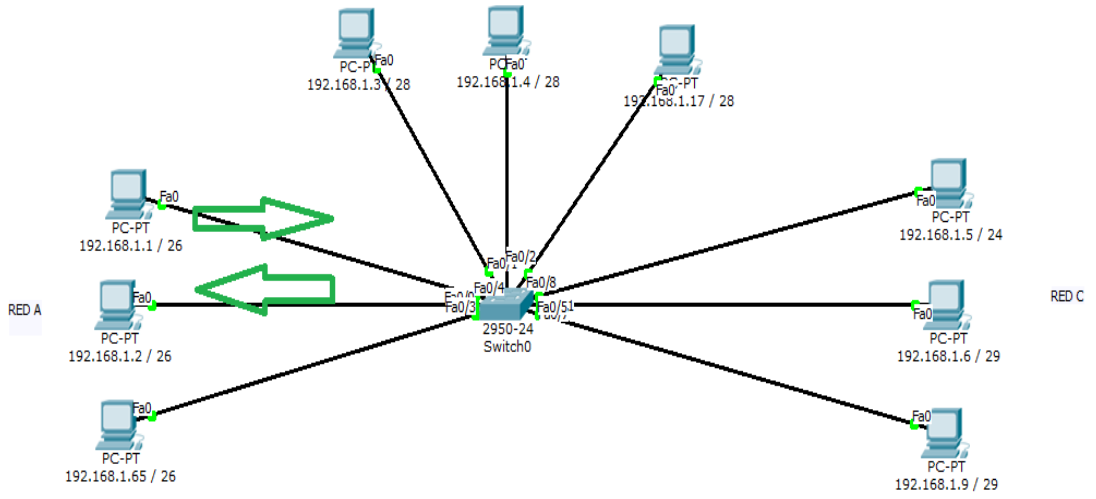


Figura 82. Prueba de conectividad entre equipos.
Tomado de Herrera, R. (2014).

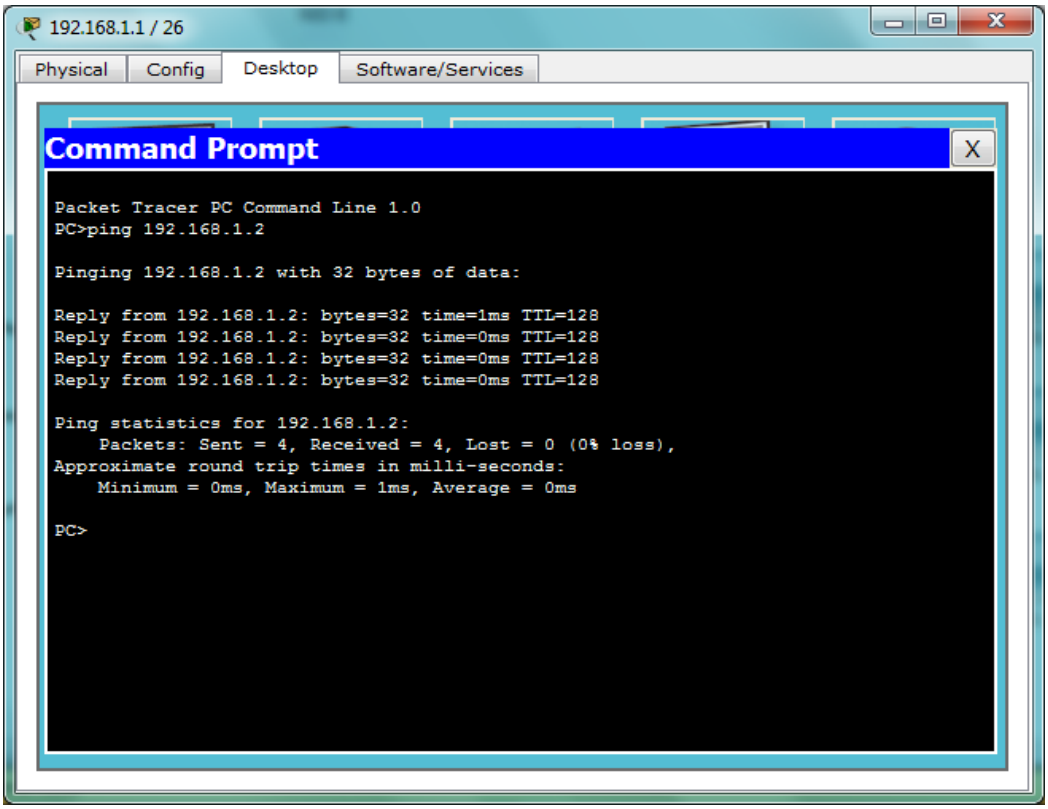


Figura 83. Prueba de conectividad mediante el comando PING.
Tomado de Herrera, R. (2014).

Como se puede observar si hay conexión entre estos equipos.

4.6.5.2. Comprobación de conectividad

Ahora queda demostrar que no hay conexión entre en computador 2 (192.168.1.2 /26) con el computador 3 (192.168.1.65 /26) que se encuentra en otro rango de dirección IP u otra Subred.

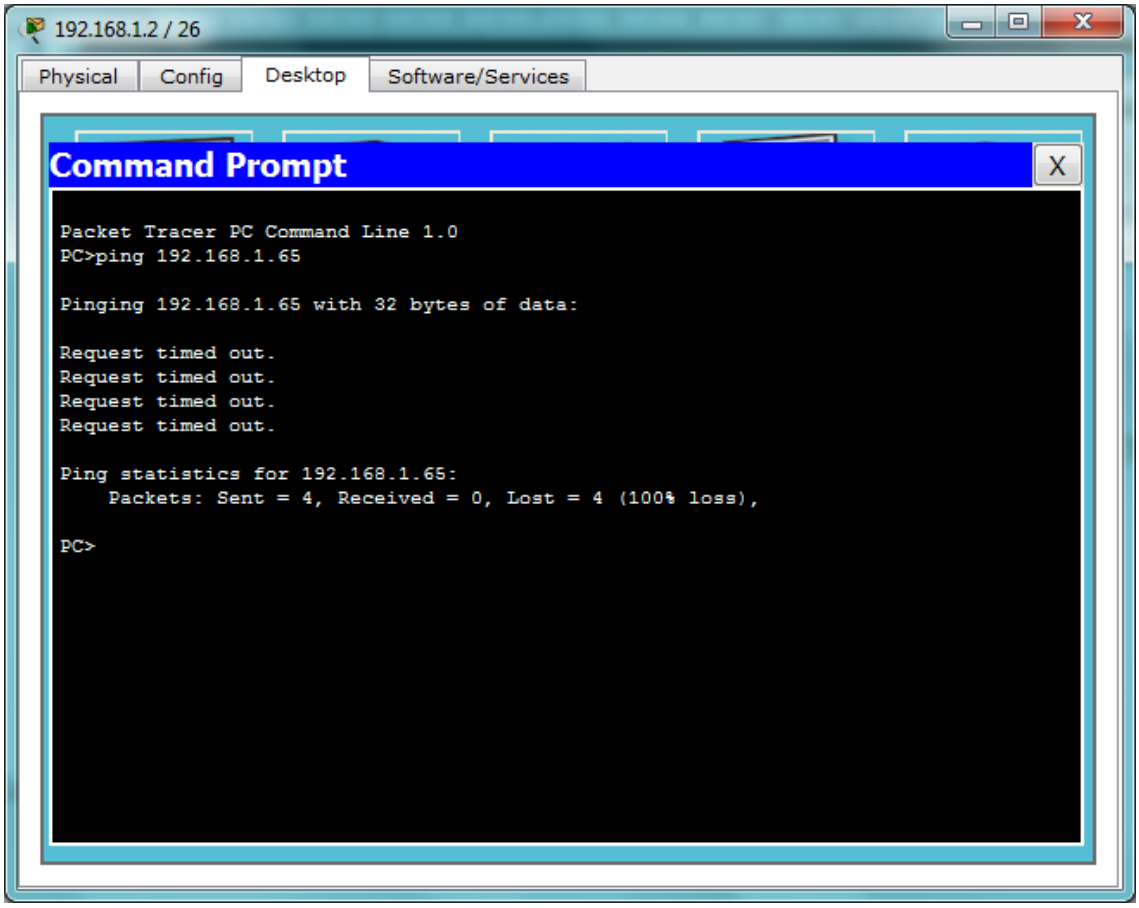


Figura 84. Imagen de conectividad entre equipos de otras subredes. Tomado de Herrera, R. (2014).

Como se puede apreciar en la imagen la conectividad es nula y así queda demostrado que no hay ningún tipo de conexión.

El mismo procedimiento se puede realizar con las demás subredes y el resultado sería el mismo. No hay conectividad entre equipos que se encuentren en una subred diferente a la suya.

4.7. RESULTADO DE LA PRÁCTICA

- La comunicación fue satisfactoria en equipos de una misma red más no en los que se encontraban en alguna diferente.
- El estudiante tiene un manejo práctico y óptimo de segmentación de redes virtuales.

- Optimización de una red.

4.8. CONCLUSIONES Y RECOMENDACIONES

- En esta práctica se pudo observar que las subredes pueden tener diferente su capacidad para un mejor desempeño de la red
- El laboratorio se llevó a cabo sin ningún tipo de inconveniente y a satisfacción total de los estudiantes y profesor.

CAPITULO V

5. Configuración de una red inalámbrica en el laboratorio de la universidad de las américas.

5.1. OBJETIVO GENERAL

Realizar la configuración de una red inalámbrica en el laboratorio de la Universidad de las Américas.

5.2. OBJETIVOS ESPECÍFICOS

El estudiante tendrá la capacidad y destreza de implementar una red inalámbrica en cualquier otra red donde el cable de red no alcance.

5.3. DESCRIPCIÓN DE EQUIPOS / HERRAMIENTAS / SOFTWARE / MATERIALES

5.3.1. PROVISTOS POR LA UNIVERSIDAD

- Router inalámbrico
- Equipos de computación o computadores del laboratorio con tarjetas inalámbricas.

5.4. TRABAJO PREPARATORIO

El estudiante para la elaboración del presente laboratorio debe conocer las causas que pueden perjudicar la conexión desde el emisor al receptor.

5.5. INTRODUCIÓN / MARCO TEORICO

Como Gallego (2014, pp. 94) ya lo dijo “Las redes inalámbricas (WLAN) sustituyen una gran parte de la conexión cableada por emisores y receptores de ondas.”

Las redes inalámbricas son integradas cada vez más a las redes de hoy en día evitando así el cableado y permitiendo un coste más bajo.

Las comunicaciones inalámbricas utilizan ondas electromagnéticas o medios no guiados para realizar la comunicación entre dispositivos a largas distancias a través de antenas.

(Flickenger, 2008, pp. 4) “La tecnología principal utilizada actualmente para la construcción de redes inalámbricas de bajo costo es la familia de los protocolos 802.11, también conocida en muchos circuitos como WI-FI. La familia de protocolos de radio 802.11 (802.11a, 802.11b, 802.11g y 802.11n) han adquirido una gran popularidad.”

5.5.1. 802.11a

(García, 2010, pp. 130) “Aprobada en 1999, funciona en frecuencia de 5Ghz y ofrece velocidades de hasta 54Mbit/s en Europa no está disponible ya que se utiliza para redar militar”.

5.5.2. 802.11b

(García, 2010, pp. 130) “Aprobada en 1999, funciona a 2.4GHz y proporciona velocidades de hasta 11Mbits/s. Hoy en día es obsoleta.”

5.5.3. 802.11g

(García, 2010, pp. 130) “aprobada en 2003, funciona a 2.4Ghz y proporciona velocidades de hasta 54Mbit/s. Compatible con 802.11b/g.”

5.5.4. 802.11n

(García, 2010, pp. 130) “Aún no completada ni ratificada, ofrecerá velocidades de hasta 600Mbit/s. Los estándares 802.11b y 802.11g utilizan la banda de 2,4GHz – 2.5 GHz. En esta banda se definieron 11 canales utilizables por los equipos WIFI, los cuales pueden configurarse de acuerdo a necesidades particulares.”

Como García (2010, P. 131) ya lo dijo “Los dispositivos de conectividad inalámbrica están compuestos por:

Puntos de acceso: es un dispositivo que permite la conexión inalámbrica de un equipo móvil con la red. Generalmente los punto de acceso tienen como función principal permitir la conectividad con la red, delegando la terea de enrutamiento y direccionamiento a servidores, routers y switches.”

Puntos de extensión: Como García (2010, pp. 131) ya lo dijo “Extiende el alcance de la red inalámbrica retransmitiendo las señales de un equipo, Punto de Acceso a otro punto de extensión. Los puntos de extensión no se conectan a la red Ethernet. La finalidad de los puntos de extensión es encadenarse para pasar los datos entre un Punto de Acceso, Punto de extensión y Computadores lejanos de modo que se construye un puente entre ambos. Los metros que cubren dichos aparatos van en función de los obstáculos (Edificios, Paredes, Puertas) a sortear, pero lo normal son 100 metros en interior y 300 metros en exterior. Los puntos de Extensión tienen incorporado una tarjeta Ethernet para poder ser configurados vía Navegador, pero no es necesario ser conectados a la red inalámbrica cuando ya están configurados y funcionando y normalmente maneja el estándar IEEE 802.11”.

Figura 85. Ejemplo esquemático de una red WIFI. Tomado de García Francisco, 2010, p.131.

Nota: En la imagen se puede apreciar el punto de acceso (router) y el punto de extensión Access Point.

5.6. DESARROLLO DE LA PRÁCTICA

En primer lugar se procede a conectar el computador al puerto LAN del router por medio de un patch cord y configurarlos en la misma red lógica.

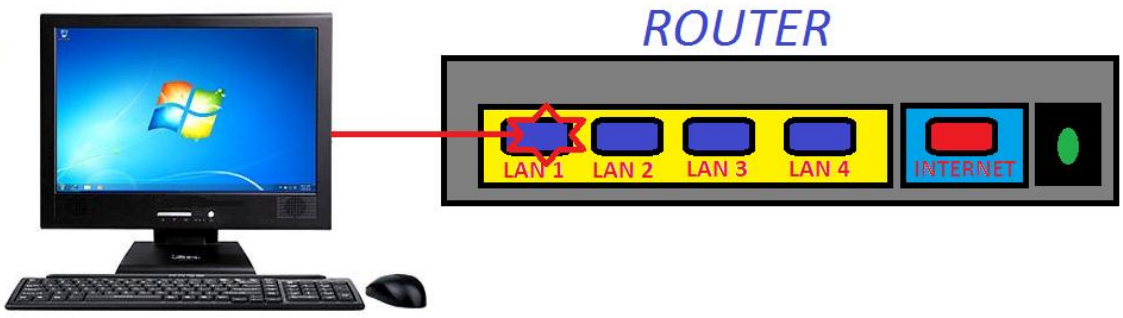


Figura 86. Conexión física de un computador hasta el puerto LAN de un router. Tomado de Herrera, R. (2014)

Ahora queda verificar en la posterior del router la información proporcionada en el mismo como dirección IP, nombre de usuario y contraseña necesarios para llevar a cabo la configuración del equipo y desarrollo del laboratorio.

A continuación se debe ingresar al navegador y ubicar la barra de dirección o URL como se muestra en la siguiente imagen:

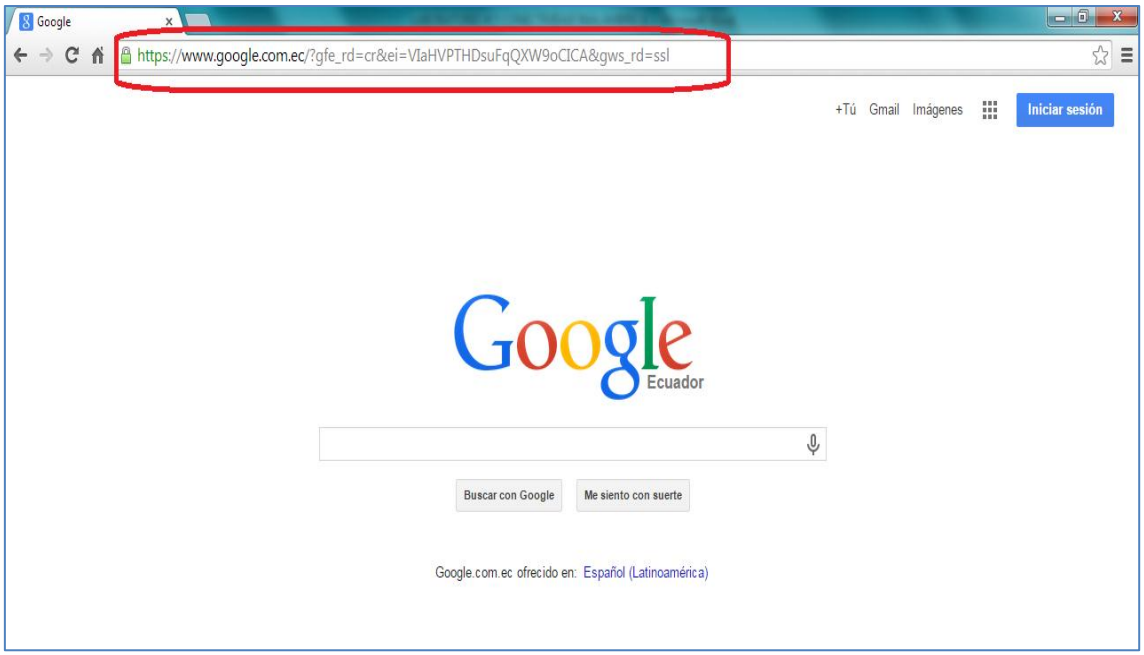


Figura 87. Muestra de la ubicación de la barra URL en el Navegador Google Chrome.
Tomado de Herrera, R. (2014).

Queda reemplazar la dirección en el URL por la dirección IP del Router que este caso es 192.168.1.1 y presionar ENTER.

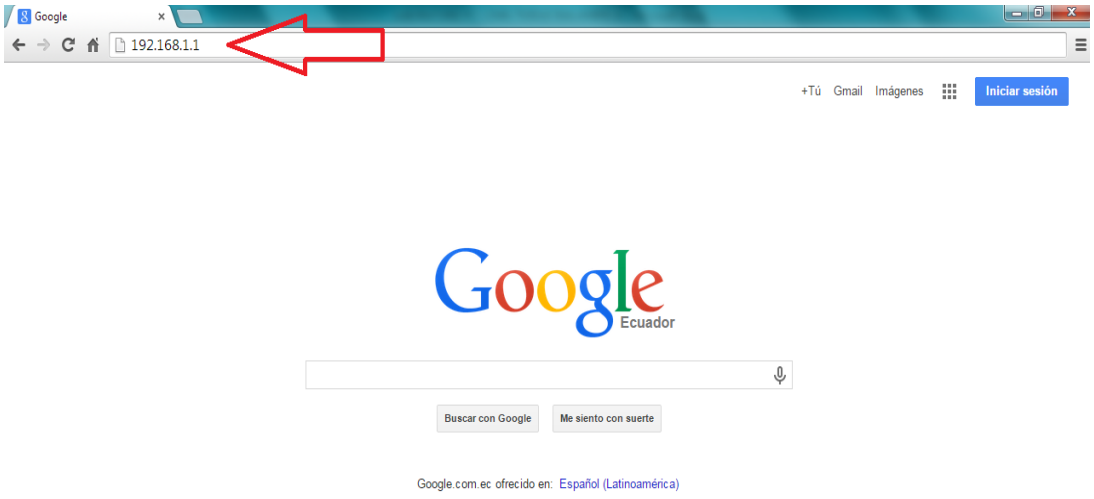


Figura 88. Ingreso de la dirección IP en la barra URL del navegador.
Tomado de Herrera, R. (2014).

En este punto la pantalla mostrará el login del router donde solicitará Usuario y Password los cuales se deben ingresar:

- Username: admin
- Password: 1234

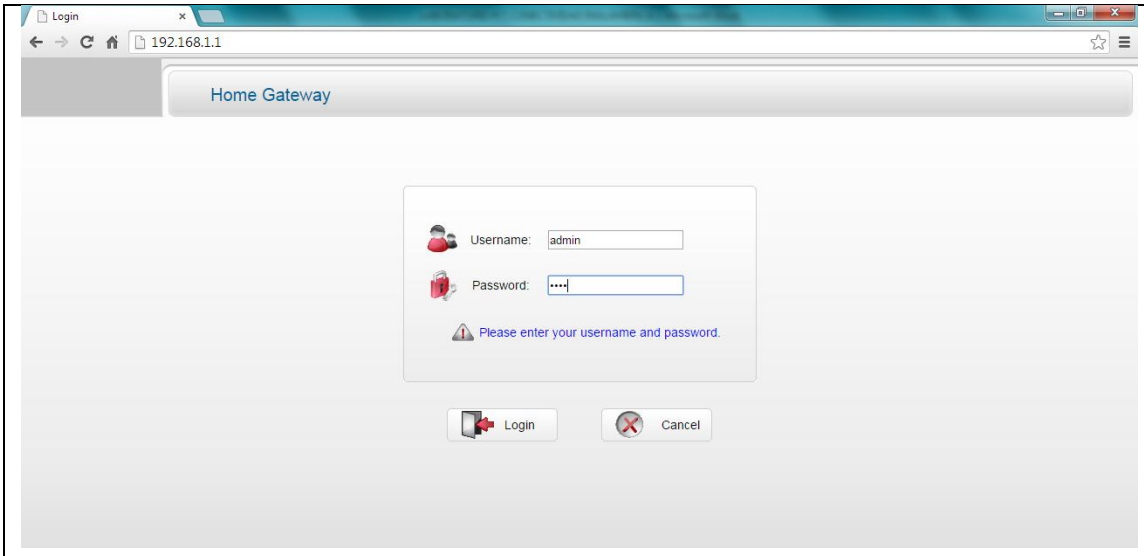


Figura 89. Pantalla de login para el acceso al router.
Tomado de Herrera, R. (2014).

Después de ingresar los datos solicitados para el ingreso al router, éste automáticamente presentará la pantalla con el estado e información de cómo está actualmente configurado. En este punto se escoge la opción “Basic”.

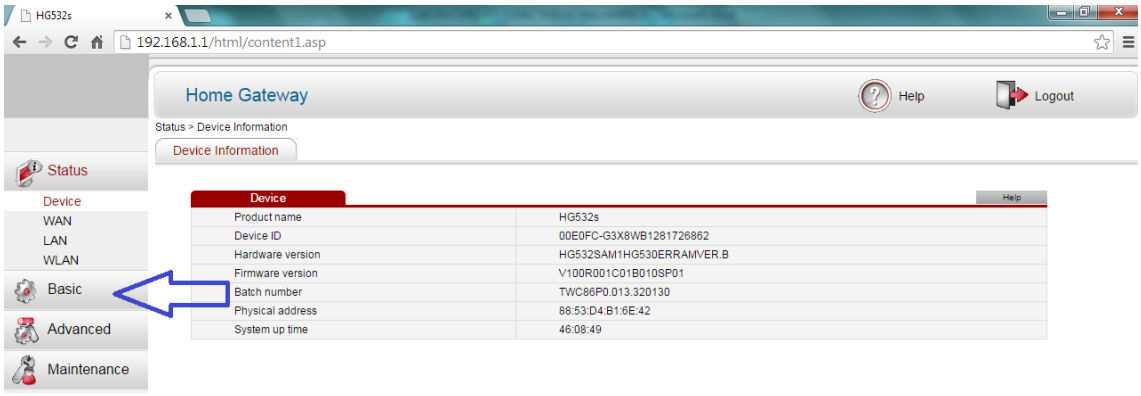


Figura 90. Lista de configuración del router y selección de la opción Basic.
Tomado de Herrera, R. (2014).

Ya en esta interfaz, se desplegará una ventana donde se debe escoger WLAN e identificar los campos:

5.6.1. SSID

Es el Nombre que se asignará a la red inalámbrica para ser identificada.

5.6.2. WPA pre-shared key

Es la contraseña que se desea asignar a la red para poder tener acceso.

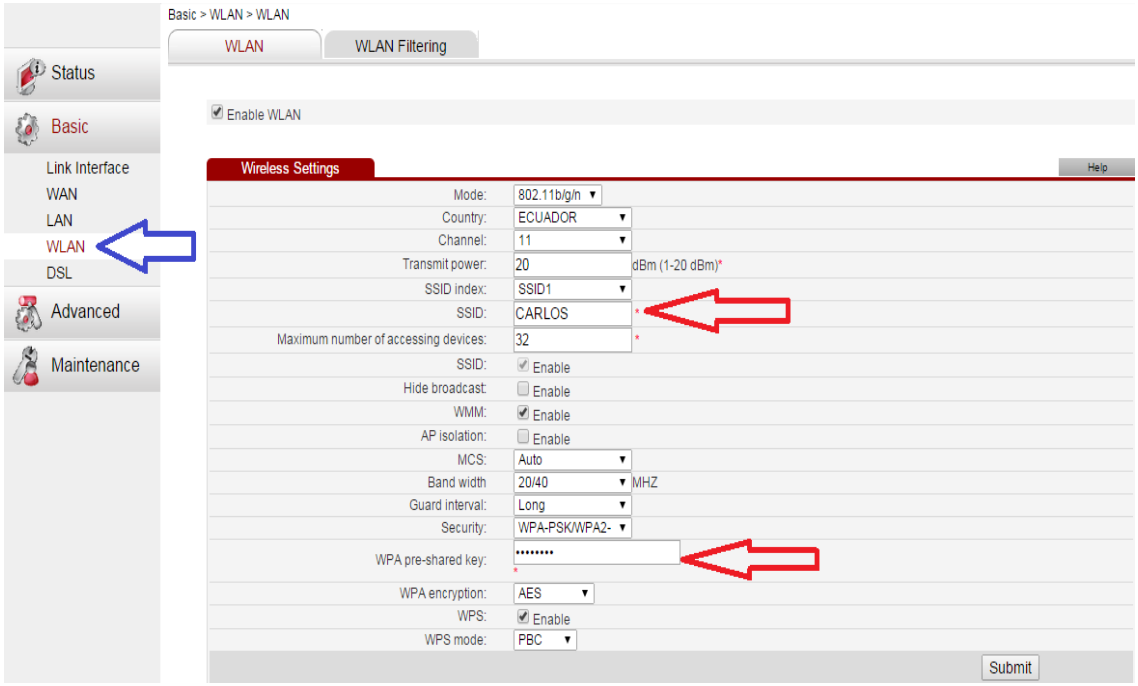


Figura 91. Campos disponibles para modificar el SSID y contraseña para el acceso a la red wifi.
Tomado de Herrera, R. (2014).

Ya identificados los campos se los puede modificar como se desee, para el laboratorio el SSID: CARLOS password: 1234567890. Para salvar la información se debe cliquear en el botón submit.

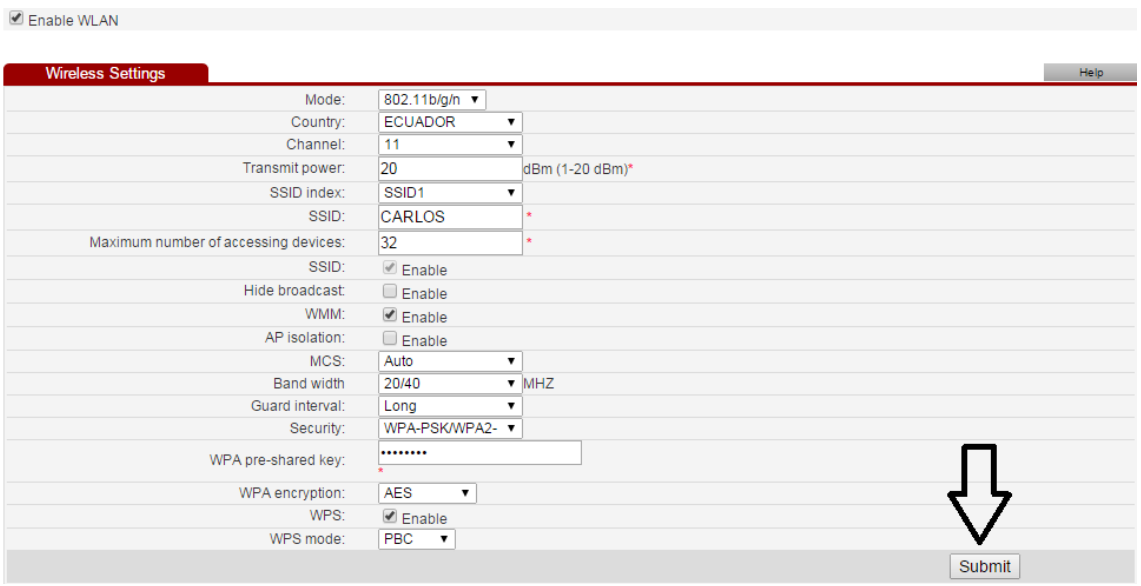


Figura 92. Imagen de selección del botón Submit y guardar la configuración. Tomado de Herrera, R. (2014).

Es momento es posible ingresar desde cualquier dispositivo pero en laboratorio se lo hará desde un portátil que incluye una tarjeta de red inalámbrica, para ello icono de wireless debe ser seleccionado con un clic.

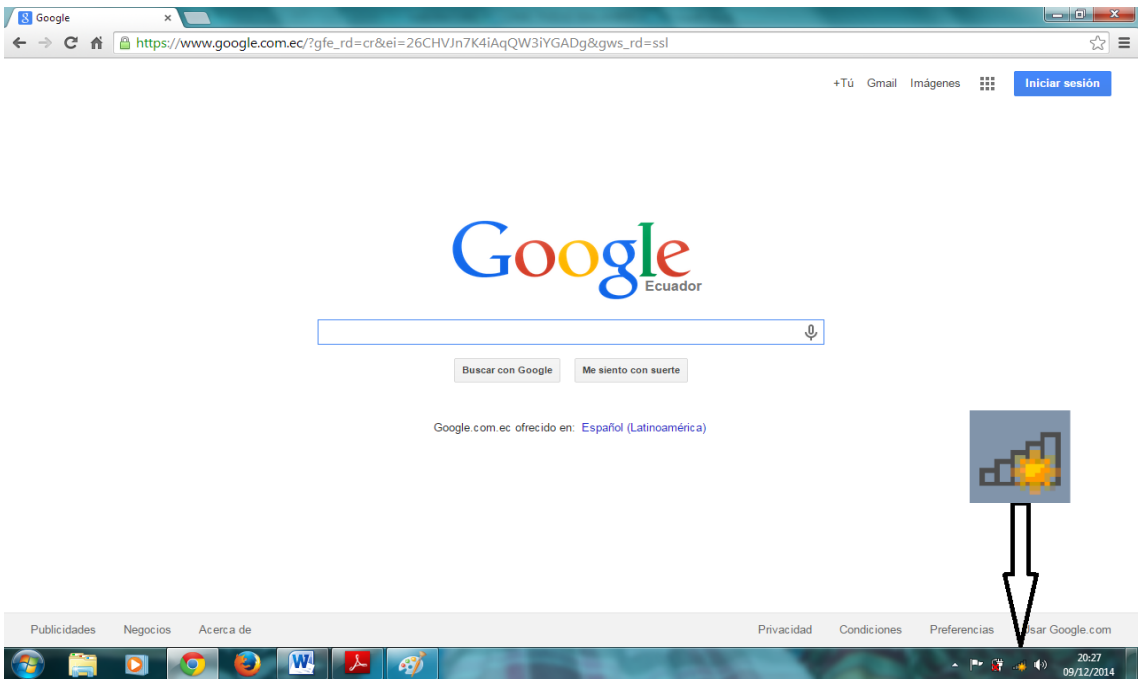


Figura 93. Muestra del icono wireless en el escritorio de Windows 7. Tomado de Herrera, R. (2014).

En este momento se desplegará una ventana con las redes disponibles o detectadas. Se procede a seleccionar la red CARLOS, presionar el botón conectar y para así ingresar el password 1234567890 permitiendo el acceso a la red.

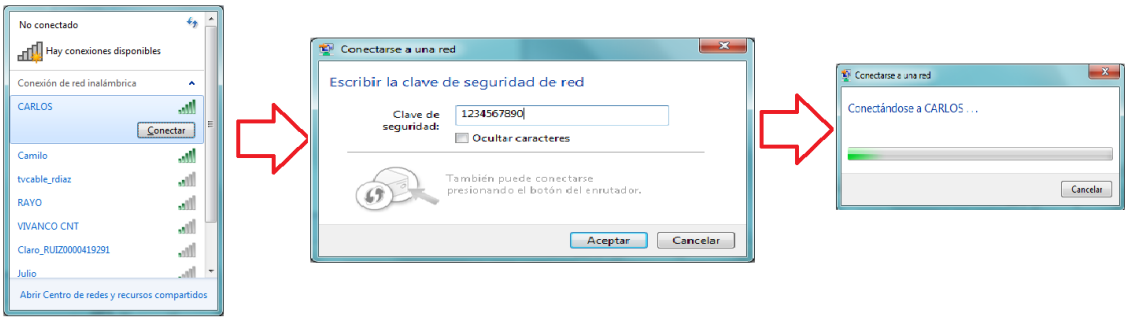


Figura 94. Ciclo por el que conlleva ingresar, seleccionar la red e ingresar la contraseña para acceder a una red inalámbrica.
Tomado de Herrera, R. (2014).

Ahora el icono de Wireless cambia como se muestra en la imagen denotando que la conexión está completa y la conectividad hacia el router es un éxito.

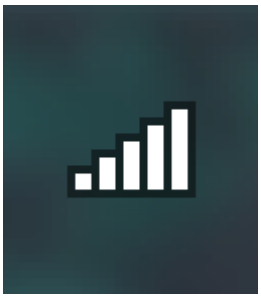


Figura 95. Estado de la conexión por medio de wireless exitosa. Herrera, R. (2014)

Finalmente para comprobar la conexión hay que realizar un ping hacia el router desde el computador portátil las veces que sean necesarias y desde varios puntos para evidenciar que la conexión es continua y no se pierde por moverlo de un lugar a otro. El comando a ejecutar será: ping 192.168.1.1

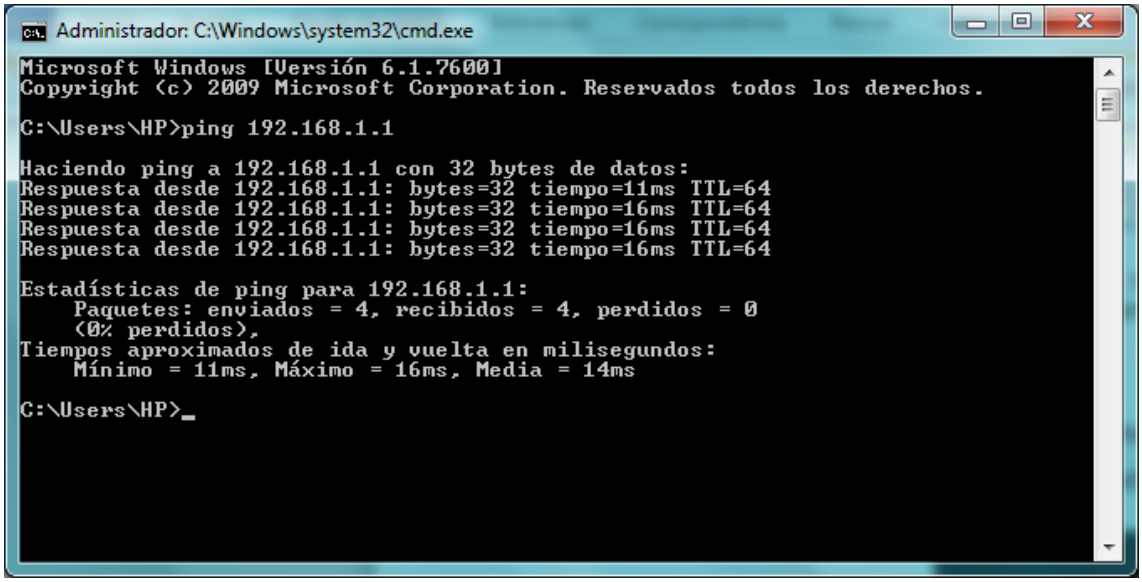


Figura 96. Ejecución de comando ping mostrando una conexión exitosa hacia el destino.
Tomado de Herrera, R. (2014).

5.7. RESULTADO DE LA PRÁCTICA

- El dispositivo no perdió la señal al momento de trasportar de un lugar a otro.
- La intensidad de la señal desciende o baja mientras el dispositivo se aleja del router.
- Se pudo conectar a la red inalámbrica los dispositivos que soportan una conexión wireless o wifi.

5.8. CONCLUSIONES Y RECOMENDACIONES

- La instalación en el laboratorio es más fácil y rápida que una cableada.
- El mantenimiento no es costoso por la infraestructura.
- La conexión puede verse afectada por cambios atmosféricos o de otros emisores de microonda.

CAPITULO VI

6. Realizar un análisis de tráfico en el laboratorio de la universidad de las américas mediante la captura de paquetes con el programa wireshark.

6.1. OBJETIVO GENERAL

Analizar el tráfico en el laboratorio de la Universidad de las Américas mediante la captura de paquetes con el programa Wireshark.

6.2. OBJETIVOS ESPECÍFICOS

- Dar a conocer como una herramienta tan fácil de usar puede realizar mejorías notorias en el rendimiento de una red congestionada.
- Describir el procedimiento de implementación y utilización del programa.
- Inspeccionar que sucede en la red y así determinar problemas y vulnerabilidades.

6.3. DESCRIPCIÓN DE EQUIPOS / HERRAMIENTAS / SOFTWARE / MATERIALES

6.3.1. PROVISTOS POR LA UNIVERSIDAD

- Equipos de computación del laboratorio de la Universidad de las Américas.

6.3.2. PROVISTOS POR EL ESTUDIANTE

- Software Wireshark.

6.4. TRABAJO PREPARATORIO

- El estudiante previamente debe disponer de internet para la descarga del programa Wireshark para la elaboración del laboratorio caso contrario del instalador.

6.5. INTRODUCIÓN / MARCO TEORICO

En la última década los equipos tecnológicos han avanzado de manera gigantesca y consigo el software el cual proporciona maravillosas herramientas

para un mejor desempeño, control y rendimiento de los mismos en una oficina, empresa y hasta en el hogar.

Se realizó la elección del programa Wireshark por sus múltiples beneficios y ventajas que éste ofrece pues es multiplataforma y software libre, ideal para la elaboración del presente laboratorio.

Como Zeas (2011, pp. 17) ya lo dijo “Wireshark es un analizador de protocolos utilizado para realizar el análisis, captura de paquetes de datos y solucionar problemas en redes de comunicaciones cuenta con todas las características estándares de un analizador de protocolos”.

6.5.1. Protocolo ARP

Este protocolo se encarga de transforma direcciones IP a direcciones MAC. El cliente averigua con broadcast en la red ¿quién tiene dirección IP a.b.c.d? y el servidor responde con su dirección MAC. Para permitir que esto pueda hacerse el valor de 0x8006 se coloca en la cabecera de la trama indicando al destino que se trata de un paquete ARP.

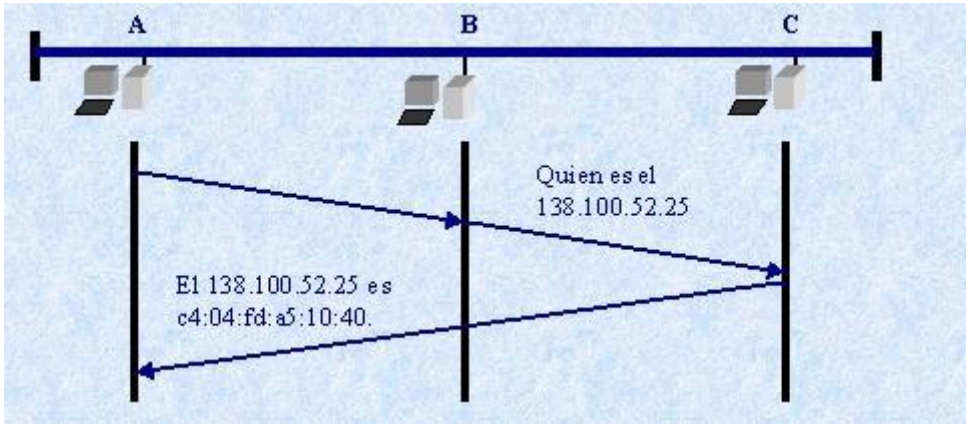


Figura 97. Funcionamiento de protocolo ARP.
Tomado de Herrera, R. (2014).

6.6. DESARROLLO DE LA PRÁCTICA

En primer lugar se debe ingresar a un navegador de internet e ingresar a la página web y seleccionar el sistema operativo que se dispone para la instalación: https://www.wireshark.org/download.html.

Seleccionar el sistema operativo que se dispone y comenzará la descarga del archivo instalador.

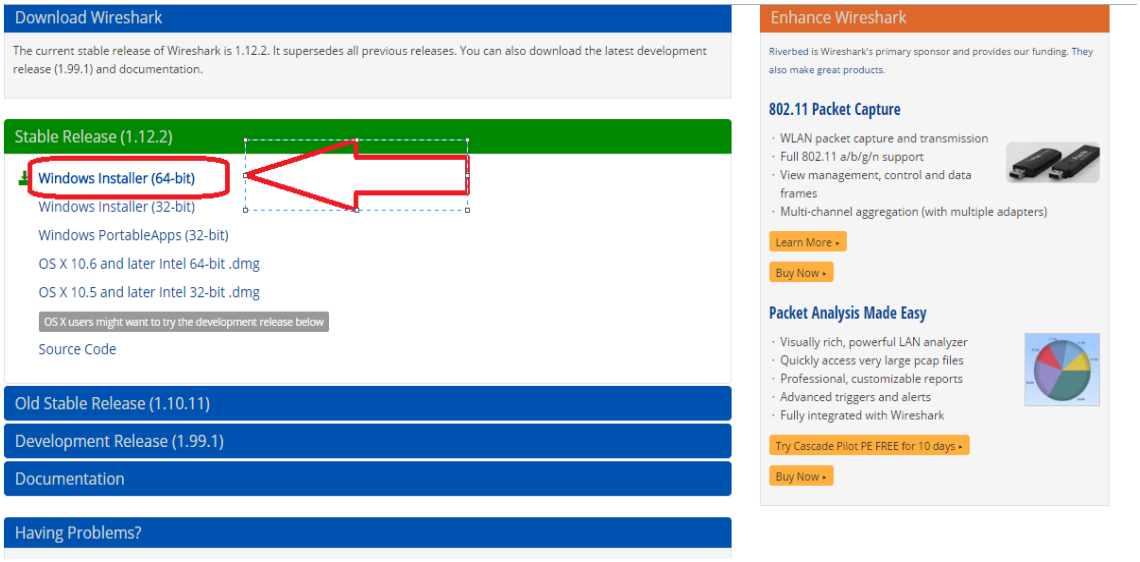


Figura 98. Imagen tomada de la página web oficial de Wireshark seleccionando el sistema operativo.
Recuperado el 16 de diciembre de 2014 de la página web: https://www.wireshark.org/

Figura 100. Icono instalador de Wireshark.
Recuperado el 16 de diciembre de 2014 de la página web: https://www.wireshark.org/

Posterior a la descarga se procede con la ejecución del archivo instalador el cual muestra la siguiente ventana donde la opción a elegir es “Next”:

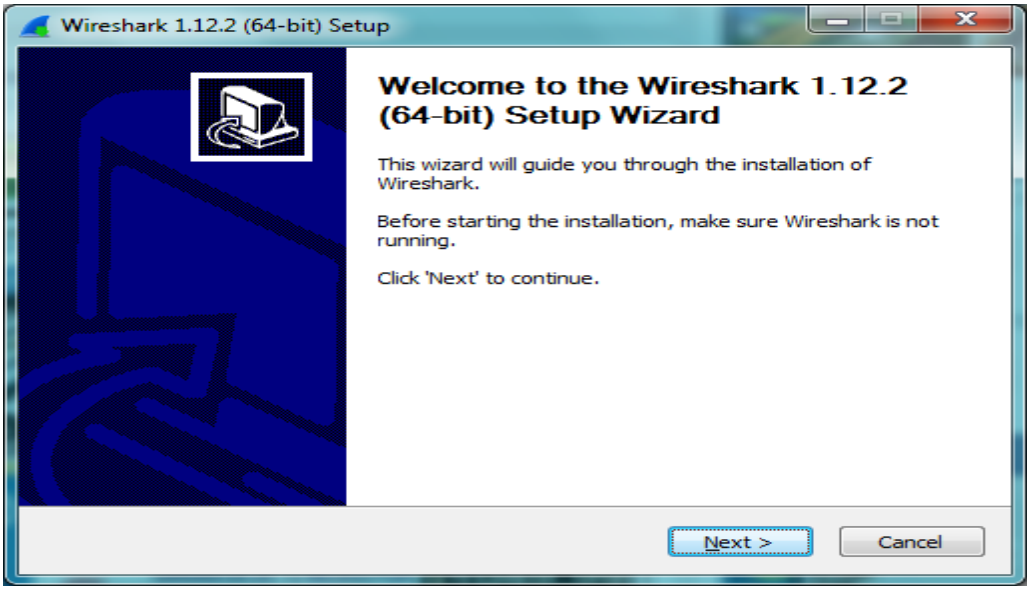


Figura 99. Ventana de Wizard del programa Wireshark.
Tomado de Herrera, R. (2014).

A continuación seleccionar el botón “I Agree” aceptando los términos y condiciones:

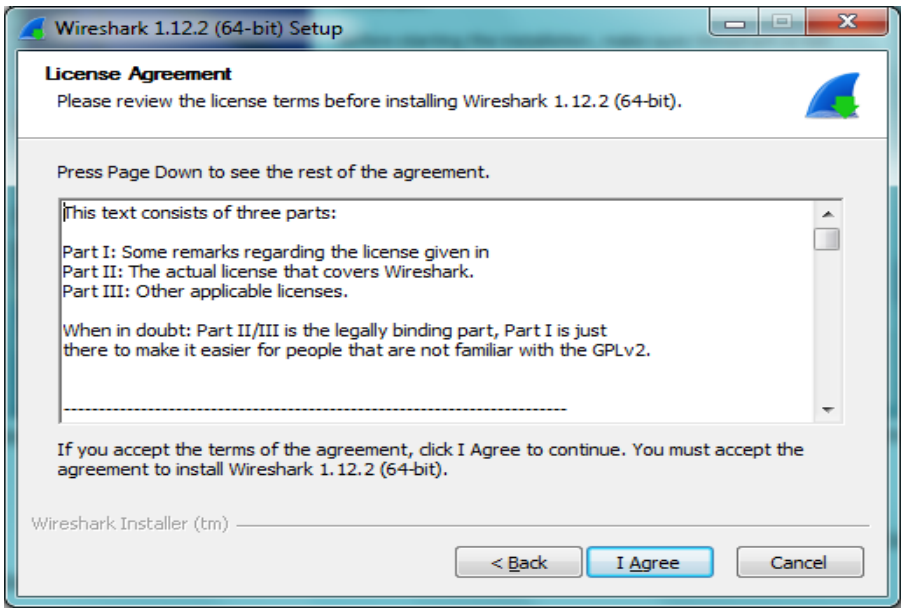


Figura 100. Acuerdo de licencia para proseguir con la instalación.
Tomado de Herrera. R. (2014).

En este punto queda seleccionar las todas las opciones y herramientas que se utilizarán más adelante y posteriormente presionar el botón “Next”:

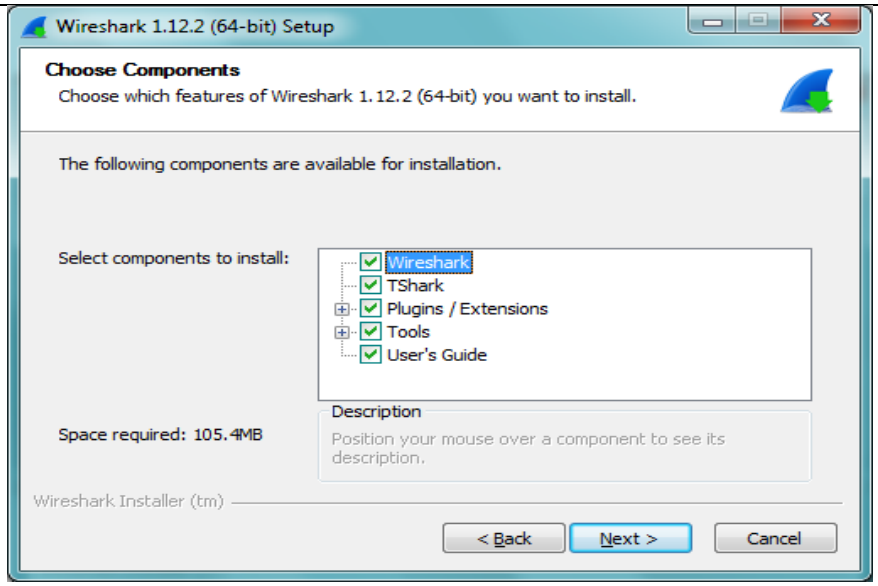


Figura 101. Herramientas y librerías necesarias para el uso posterior del programa.
Tomado de Herrera. R. (2014).

Ahora queda habilitar las extensiones para su correcto funcionamiento:

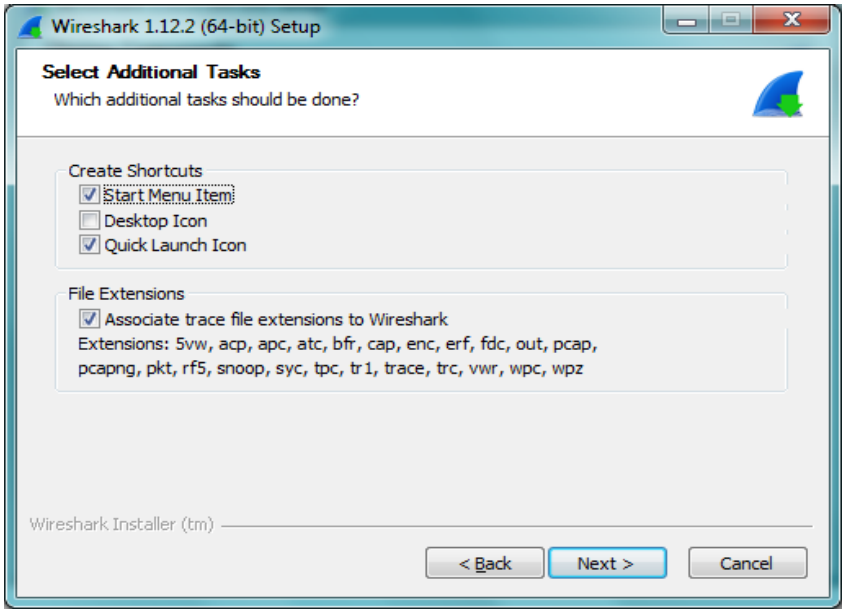


Figura 104. Archivo de extensiones del programa Wireshark.
Tomado de Herrera, R. (2014).

En esta ventana indica la ubicación de instalación. Se deja el default:

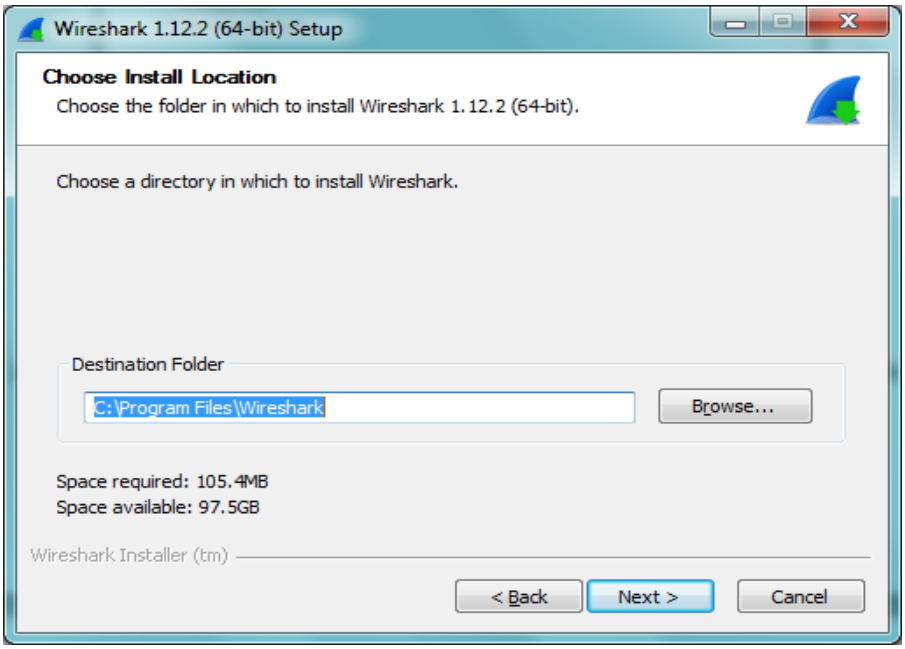


Figura 102. Destino donde se instalarán los archivos para el funcionamiento de Wireshark.
Tomado de Herrera, R. (2014).

Para proseguir con la instalación es necesario habilitar “Install winPcap”:

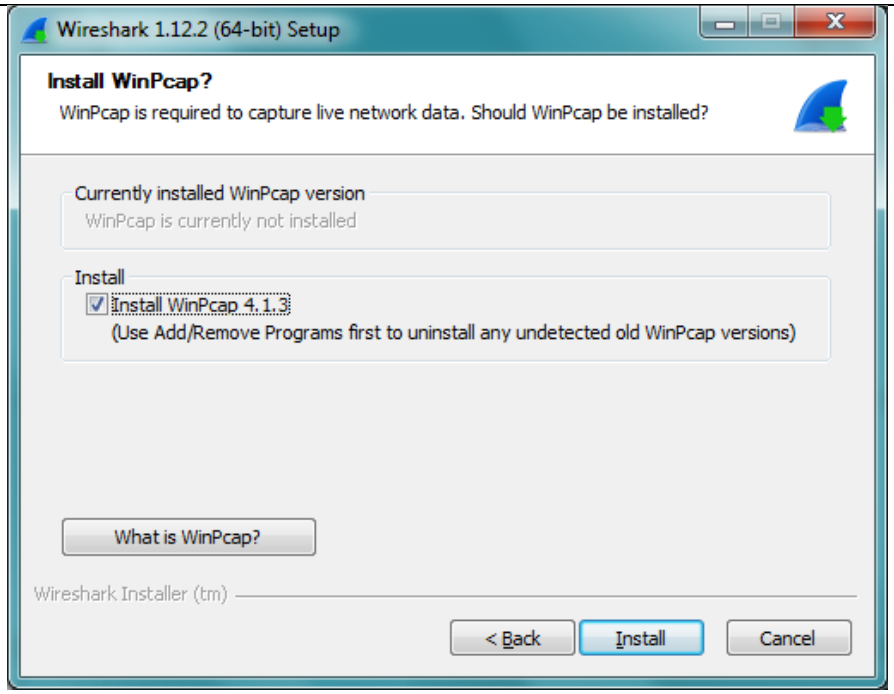


Figura 103. Instalación de WinPcap.
Tomado de Herrera, R. (2014).

De esta manera dará inicio a instalación de librerías, posteriormente mostrará la ventana de instalación de WinCap:

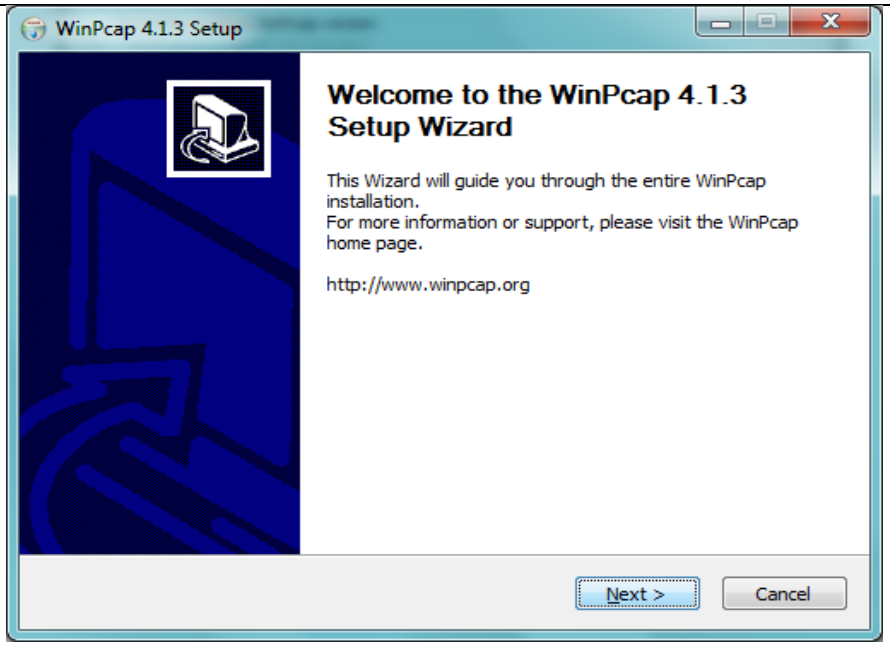


Figura 104. Wizard de instalación de WinPcap.
Tomado de Herrera, R. (2014)

Leer y aceptar los términos y condiciones de WinPcap:

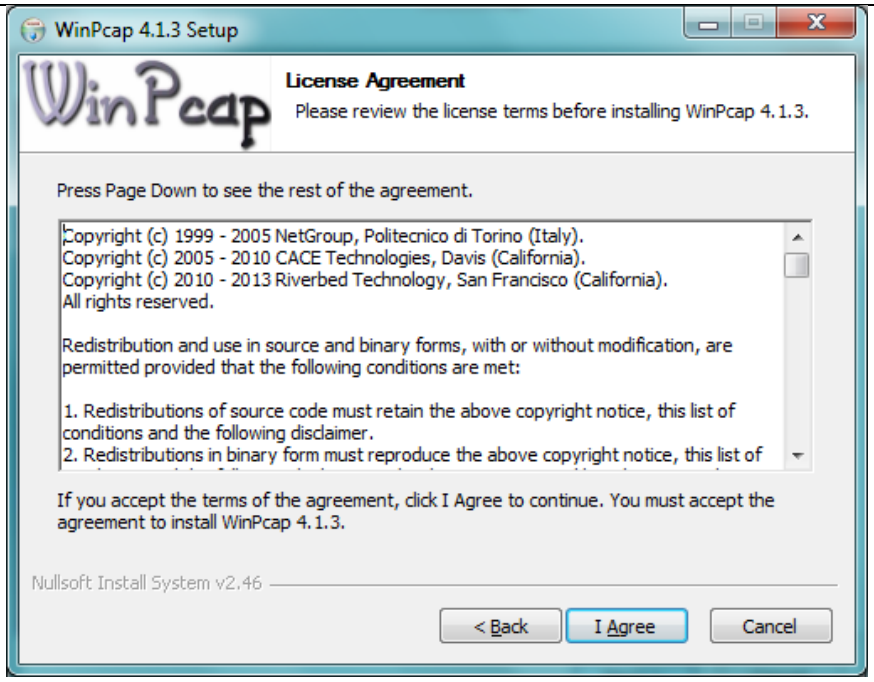


Figura 105. Términos y condiciones de WinPcap.
Tomado de Herrera, R. (2014).

Seleccionar la opción de inicio automático de WinPcap y siguiente:

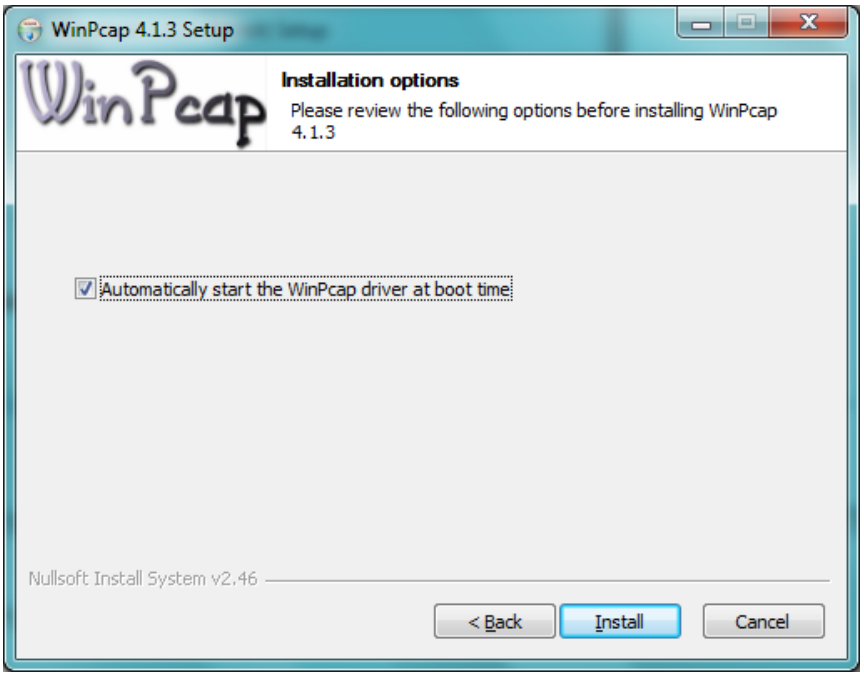


Figura 106. Opción para el inicio automático de WinPcap.
Tomado de Herrera, R. (2014).

Se completará la instalación deWinPcap y seleccionar finalizar:

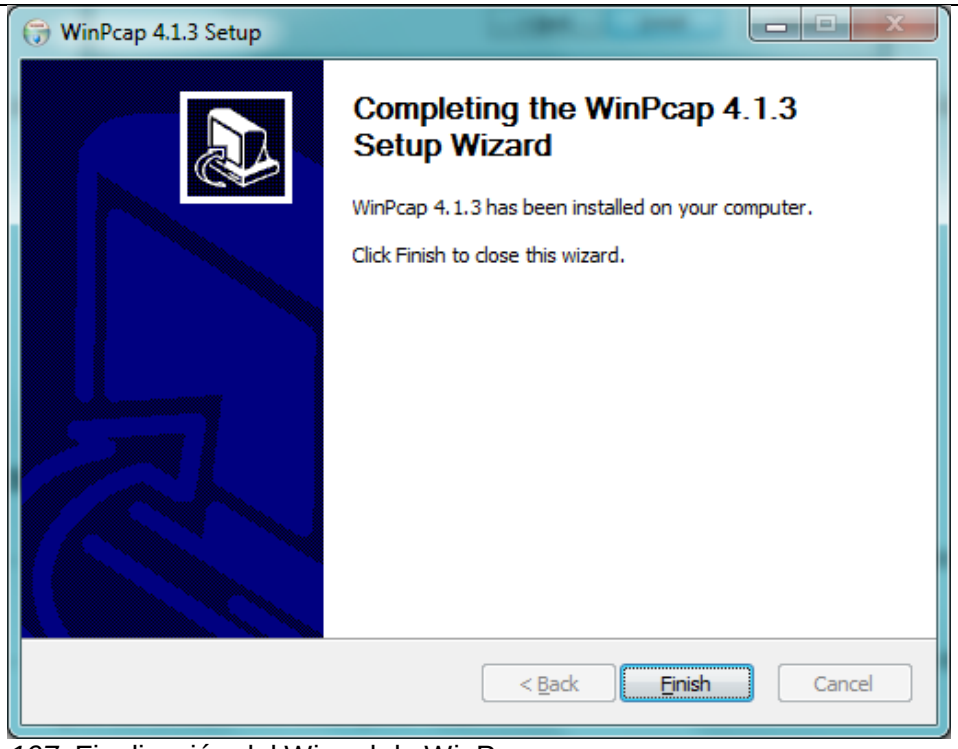


Figura 107. Finalización del Wizard de WinPcap.
Tomado de Herrera, R. (2014).

Para finalizar la instalación se debe seleccionar “Next” y posteriormente finalizar:

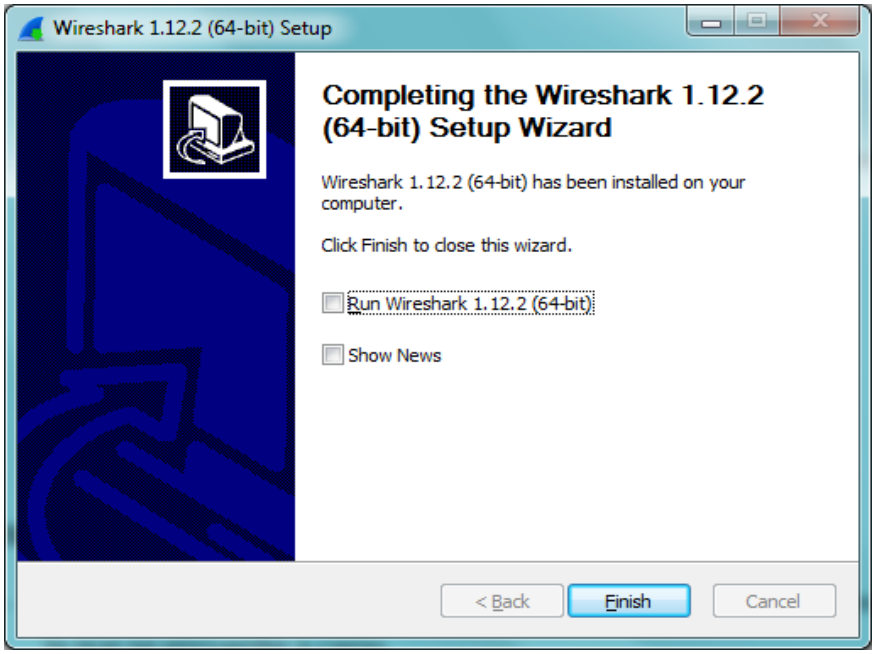


Figura 1081. Finalización del wizard de Wireshark.
Tomado de Herrera, R. (2014).

En este momento se debe proceder a acceder al programa desde el menú Inicio – Todos los programas – Wireshark (Windows 7) donde se desplegará la siguiente pantalla:

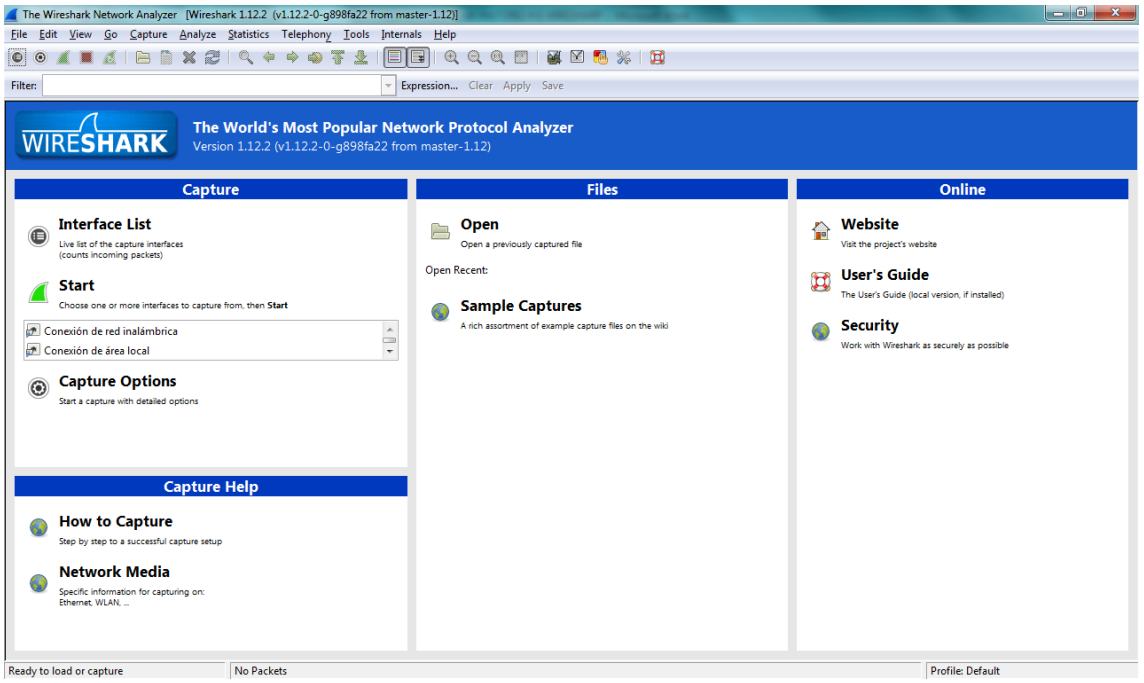


Figura 109. Pantalla inicial de Wireshark.
Tomado de Herrera, R. (2014).

6.6.1. Partes y herramientas de Wireshark.

6.6.1.1. Menú Principal

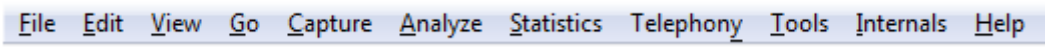


Figura 110. Menú principal Wireshark.
Tomado de Herrera, R. (2014).

- File : Opciones para la modificación de archivos.
- Edit : Aplicar cambios en los paquetes.
- View : Editar despliegue del dato capturado.
- Go : Permite desplazamiento de un paquete a otro.
- Capture: Inicia o captura la captura de paquetes.
- Analyze: Edita los filtros, flujo de información (paquetes), etc.
- Statics: Define estadísticas del data obtenido.
- Help : Menú de ayuda.

6.6.1.2. Barra de herramientas

Figura 111. Acceso rápido a funciones de Wireshark.
Tomado de Herrera, R. (2014).

6.6.1.3. Barra de filtro

Figura 112. Filtro de los paquetes.
Tomado de Herrera, R. (2014).

6.6.1.4. Panel de paquetes

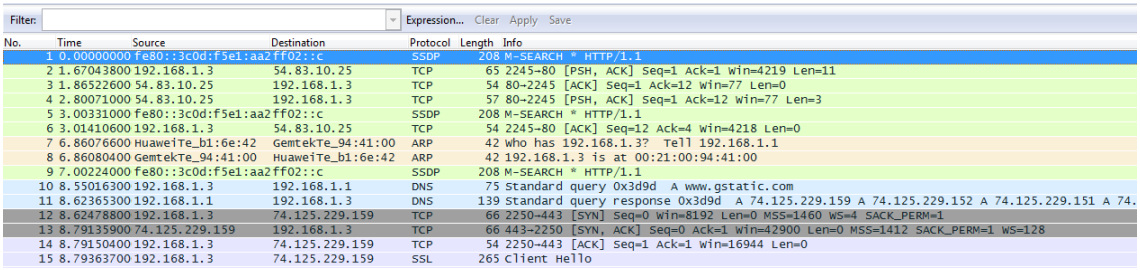


Figura 113. Imagen de paquetes capturados.
Tomado de Herrera, R. (2014).

- No: Item de paquete capturado.
- Time:Tiempo de captura del paquete.
- Source: Fuente u origen de paquete.
- Destination: Dirección destino del paquete.
- Protocol: Protocolo del paquete.
- Info: Información adicional del paquete capturado.

6.6.2. ANALISIS DE TRÁFICO A LA PAGINA WEB ww.facebook.com

Una vez instalado el programa se procede a seleccionar la opción Conexión de red inalámbrica y posteriormente Start:

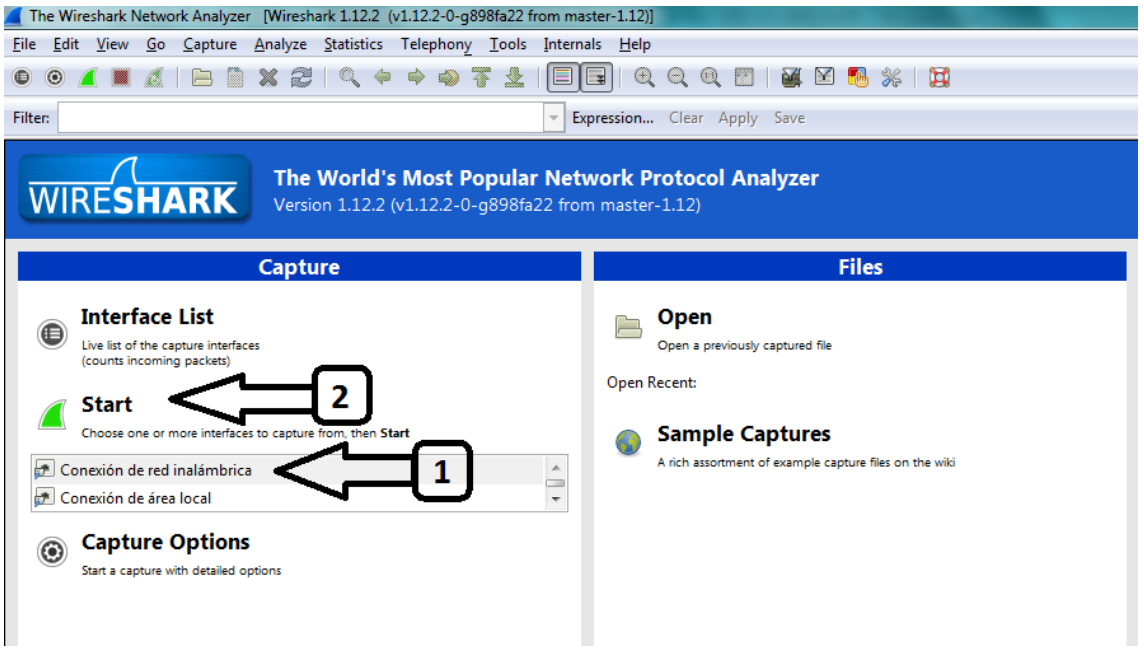


Figura 114. Selección de adaptador de red e iniciar la captura de paquetes. Tomado de Herrera, R. (2014).

Posteriormente Wiresharp realizará la captura de paquetes que se encuentren transitando en la red.

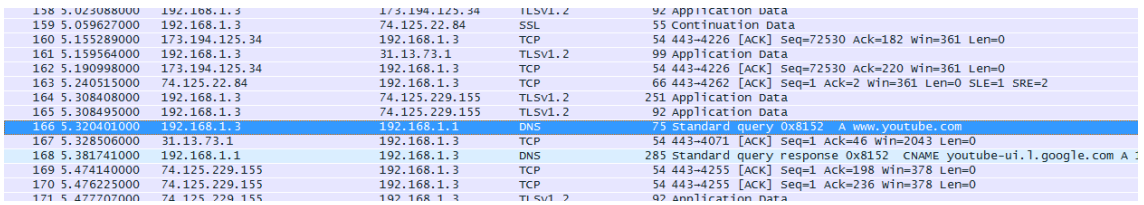
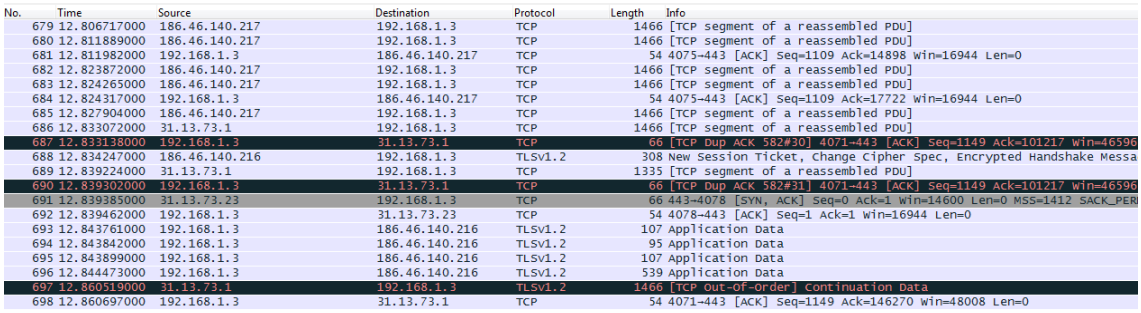


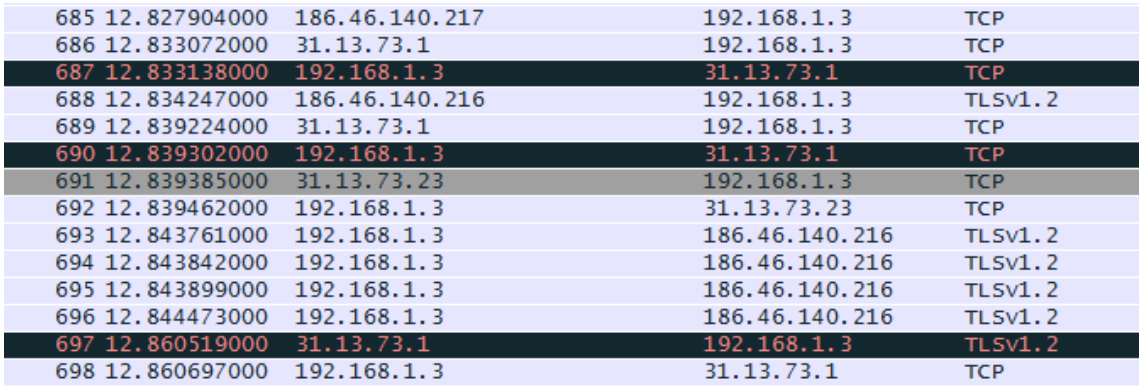
Figura 115. Tráfico en la red.
Tomado de Herrera, R. (2014).

En la imagen 117 se puede observar que el host con dirección 192.168.1.3 se encuentra realizando una solicitud o realizando conexión (petición DNS) a www.youtube.com la cual perjudica el rendimiento de la red o velocidad de Internet.



No.	Time	Source	Destination	Protocol	Length	Info
679	12.806717000	186.46.140.217	192.168.1.3	TCP	1466	[TCP segment of a reassembled PDU]
680	12.811889000	186.46.140.217	192.168.1.3	TCP	1466	[TCP segment of a reassembled PDU]
681	12.811982000	192.168.1.3	186.46.140.217	TCP	54	4075→443 [ACK] Seq=1109 Ack=14898 Win=16944 Len=0
682	12.823872000	186.46.140.217	192.168.1.3	TCP	1466	[TCP segment of a reassembled PDU]
683	12.824265000	186.46.140.217	192.168.1.3	TCP	1466	[TCP segment of a reassembled PDU]
684	12.824317000	192.168.1.3	186.46.140.217	TCP	54	4075→443 [ACK] Seq=1109 Ack=17722 Win=16944 Len=0
685	12.827904000	186.46.140.217	192.168.1.3	TCP	1466	[TCP segment of a reassembled PDU]
686	12.833072000	31.13.73.1	192.168.1.3	TCP	1466	[TCP segment of a reassembled PDU]
687	12.833138000	192.168.1.3	31.13.73.1	TCP	66	[TCP Dup ACK 582#30] 4071→443 [ACK] Seq=1149 Ack=101217 Win=46596
688	12.834247000	186.46.140.216	192.168.1.3	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Messa
689	12.839224000	31.13.73.1	192.168.1.3	TCP	1335	[TCP segment of a reassembled PDU]
690	12.839302000	192.168.1.3	31.13.73.1	TCP	66	[TCP Dup ACK 582#31] 4071→443 [ACK] Seq=1149 Ack=101217 Win=46596
691	12.839385000	31.13.73.23	192.168.1.3	TCP	66	443→4078 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1412 SACK_PER
692	12.839462000	192.168.1.3	31.13.73.23	TCP	54	4078→443 [ACK] Seq=1 Ack=1 Win=16944 Len=0
693	12.843761000	192.168.1.3	186.46.140.216	TLSv1.2	107	Application Data
694	12.843842000	192.168.1.3	186.46.140.216	TLSv1.2	95	Application Data
695	12.843899000	192.168.1.3	186.46.140.216	TLSv1.2	107	Application Data
696	12.844473000	192.168.1.3	186.46.140.216	TLSv1.2	539	Application Data
697	12.860519000	31.13.73.1	192.168.1.3	TLSv1.2	1466	[TCP Out-Of-Order] Continuation Data
698	12.860697000	192.168.1.3	31.13.73.1	TCP	54	4071→443 [ACK] Seq=1149 Ack=146270 Win=48008 Len=0

Figura 116. Captura de paquetes en la red.
Tomado de Herrera, R. (2014).



685 12.827904000	186.46.140.217	192.168.1.3	TCP
686 12.833072000	31.13.73.1	192.168.1.3	TCP
687 12.833138000	192.168.1.3	31.13.73.1	TCP
688 12.834247000	186.46.140.216	192.168.1.3	TLSv1.2
689 12.839224000	31.13.73.1	192.168.1.3	TCP
690 12.839302000	192.168.1.3	31.13.73.1	TCP
691 12.839385000	31.13.73.23	192.168.1.3	TCP
692 12.839462000	192.168.1.3	31.13.73.23	TCP
693 12.843761000	192.168.1.3	186.46.140.216	TLSv1.2
694 12.843842000	192.168.1.3	186.46.140.216	TLSv1.2
695 12.843899000	192.168.1.3	186.46.140.216	TLSv1.2
696 12.844473000	192.168.1.3	186.46.140.216	TLSv1.2
697 12.860519000	31.13.73.1	192.168.1.3	TLSv1.2
698 12.860697000	192.168.1.3	31.13.73.1	TCP

Figura 117. Gráfico informativo de paquetes en la red mostrando comunicación entre un host hacia internet.
Tomado de Herrera, R. (2014)

En la imagen 120 se puede apreciar que la dirección IP (192.168.1.3) presenta comunicación constante con otra dirección IP (31.13.73.1). Se procede a realizar la ejecución del comando tracert a la dirección IP 31.13.73.1 para identificar su procedencia.

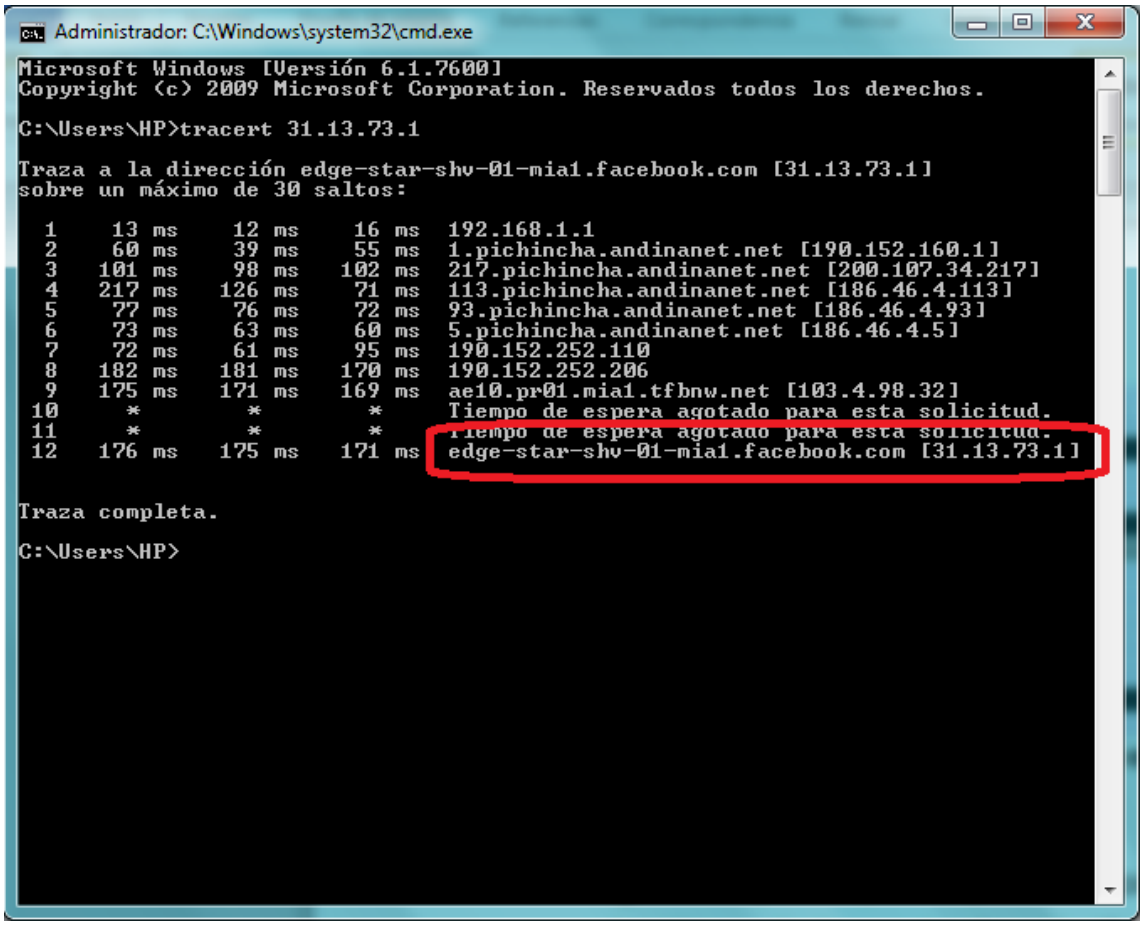


Figura 118. Ejecución de comando tracert a la IP que se desea conocer.
Tomado de Herrera, R. (2014).

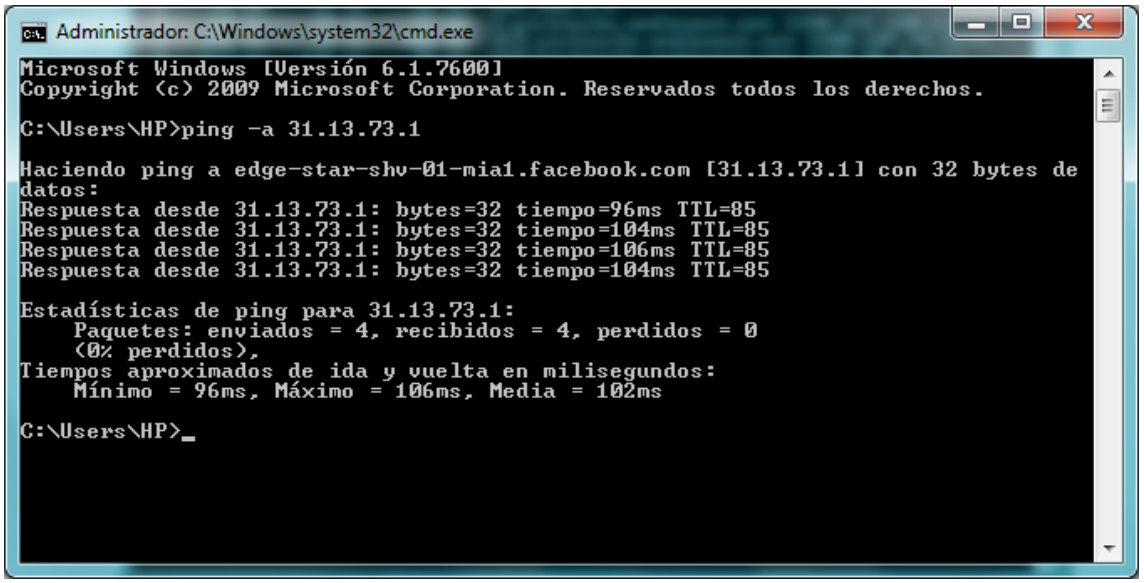


Figura 119. Ejecución del comando ping –a.
Tomado de Herrera, R. (2014)

Como se puede confirmar en el programa existe comunicación permanente desde un host hacia la página web www.facebook.com lo que causa que la red baje su rendimiento en el sentido de velocidad de internet y que no sea necesaria para una institución educativa.

6.7. RESULTADO DE LA PRÁCTICA

- El estudiante con facilidad podrá determinar el rendimiento de la red en la que se encuentre a cargo.
- Con una simple herramienta se es capaz de determinar el estado en la que se encuentre cualquier red.
- Conocimiento del tráfico que circula en la red.

6.8. CONCLUSIONES Y RECOMENDACIONES

- En un pequeño momento determinado se pudo analizar el tipo de tráfico.
- No se necesita de una inversión de alto costo pues una herramienta tan fácil de usar puede realizar grandes resultados.
- Un paquete de datos capturado contiene información que puede ser analizada.

CAPITULO VII

7. Realizar en el simulador de Packet tracer la configuración de un servidor DHCP con el protocolo de internet versión 4 (ipv4) y configuración un router para el protocolo de internet versión 6 (ipv6).

7.1. OBJETIVO GENERAL

En el simulador de Packet Tracer realizar la configurar de un servidor DHCP con el Protocolo de Internet versión 4 (IPv4) y configurar un router para el Protocolo de Internet versión 6 (IPv6).

7.2. OBJETIVOS ESPECÍFICOS

Realizar configuraciones básicas para la comprensión del funcionamiento del servicio DHCP en IPv4 e IPv5.

7.3. DESCRIPCIÓN DE EQUIPOS / HERRAMIENTAS / SOFTWARE / MATERIALES

7.3.1. PROVISTOS POR LA UNIVERSIDAD

- Router
- Computador (escritorio)
- Computador portátil

7.3.2. PROVISTOS POR EL ESTUDIANTE

- Simulador de Packet Tracer
- Patch cord

7.4. TRABAJO PREPARATORIO

- El estudiante previamente debe disponer del simulador instalado en el equipo o computador a utilizar para la elaboración del laboratorio.

7.5. INTRODUCIÓN / MARCO TEORICO

Como Gómez, (2010, pp. 12) ya lo dijo “El protocolo de configuración dinámica de Anfitrión o DHCP es un protocolo de red TCP/IP que permite a los nodos de una red obtener sus parámetros de configuración automáticamente.

Se trata de un protocolo de tipo cliente/servidor en el que, generalmente, un servidor posee unos rangos de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento qué interfaz ha estado en posesión de esa IP, por asociación a su MAC (Media Access Control), cuanto tiempo la ha tenido y a quien se la ha asignado después."

7.6. DESARROLLO DE LA PRÁCTICA

7.6.1. Configuración de IPv4

En primer lugar se procederá con la configuración del IPv4 en el simulador de Packet Tracer donde se necesita tener el siguiente escenario con los equipos que se muestran a continuación:

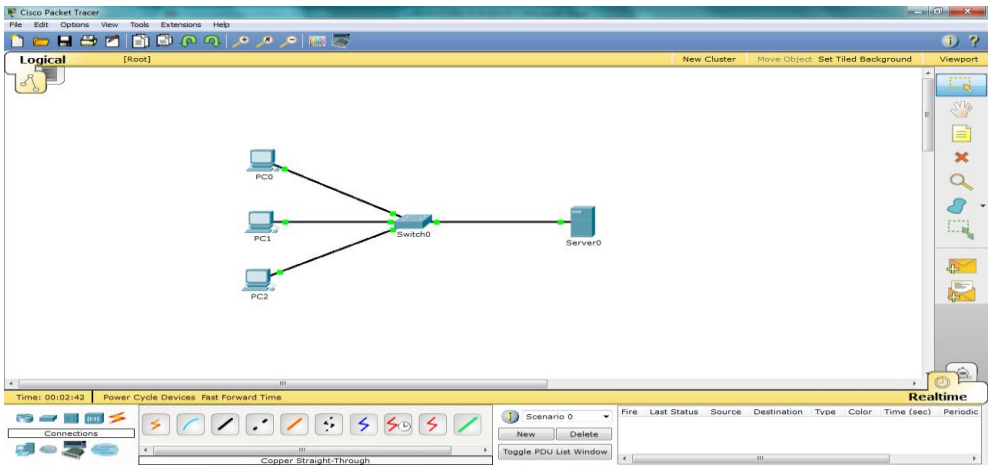


Figura 120. Escenario con tres computadores, un switch y un servidor necesarios para el desarrollo del laboratorio.
Tomado de Herrera, R. (2014).

A continuación se debe ingresar al servidor para su configuración, desde la opción Config y posteriormente seleccionando el botón DHCP:

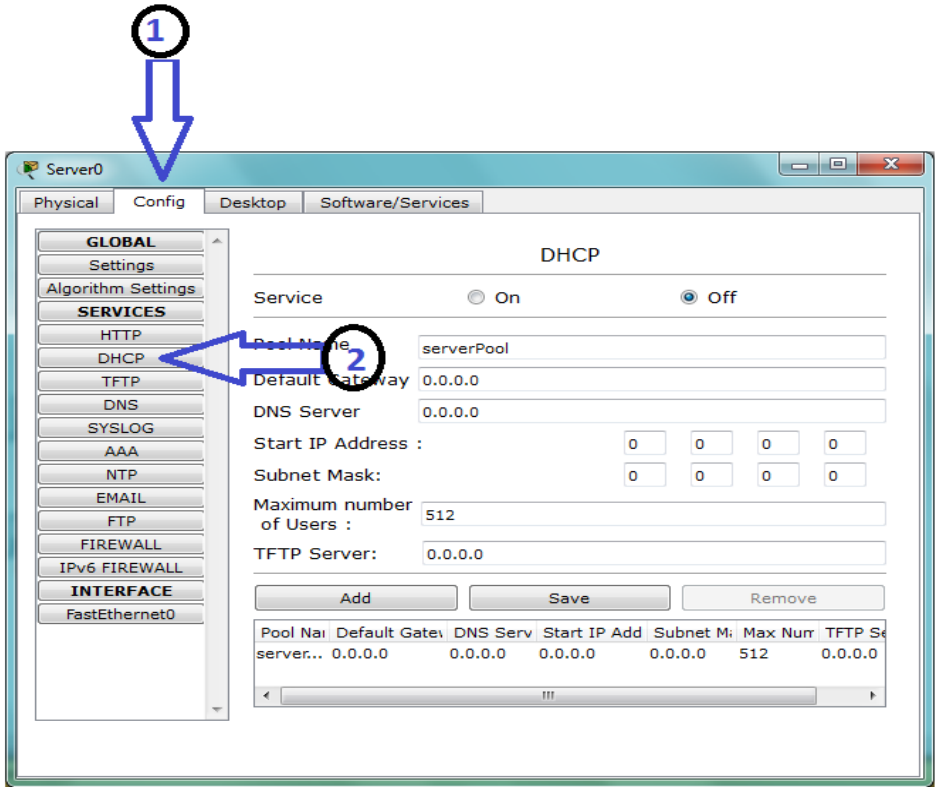


Figura 121. Selección servicio DHCP.
Tomado de Herrera, R. (2014).

Tras realizar los pasos anteriores el simulador mostrará las opciones de configuración del servicio DHCP.

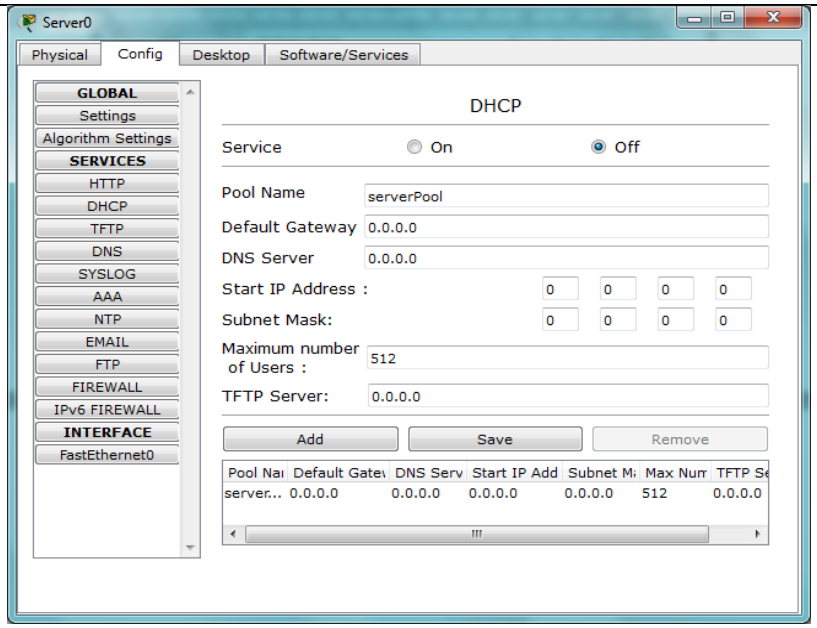


Figura 122. Imagen con las opciones de configuración del servidor DHCP. Tomado de Herrera, R. (2014).

7.6.1.1.1. Opciones de configuración del servidor DHCP.

7.6.1.1.2. Pool Name

- Nombre que se asignará al servidor.

7.6.1.1.3. Default Gateway

- Es la IP de la puerta de enlace el cual funciona como intermediario para comunicar una red con otra.

7.6.1.1.4. Start IP Address

- Es inicio del rango de IP que se desea configurar.

7.6.1.1.5. Subnet Mask

- Máscara de red

La configuración del servidor debe quedar de la siguiente manera:

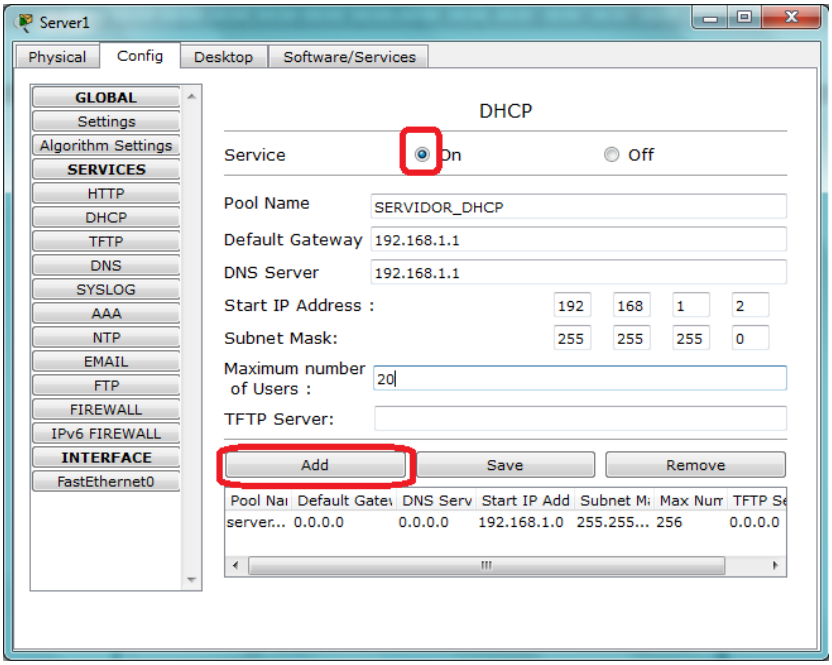


Figura 123. Imagen con la configuración necesaria para el servicio DHCP. Tomado de Herrera, R. (2014).

7.6.1.2. Configuración para el laboratorio

7.6.1.2.1. Nombre del servidor

- Servidor_DHCP

7.6.1.2.2. Default Gateway

- 192.168.1.1

7.6.1.2.3. Inicio de rango IP's

- 192.168.1.2

7.6.1.2.4. Mascara de red

- 255.255.255.0

7.6.1.2.5. Numero max de usuarios

- 20

Queda presionar en el botón On para activar el servicio, en el botón Add para salvar la configuración y así se adicionará en la parte inferior la siguiente línea:

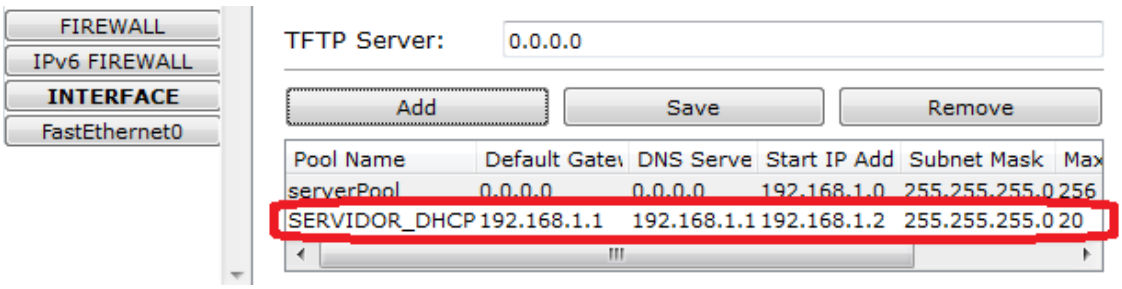


Figura 124. Línea agregada posterior a seleccionar el botón Add.
Tomado de Herrera, R. (2014).

En este punto se debe ingresar una dirección IP al servidor:

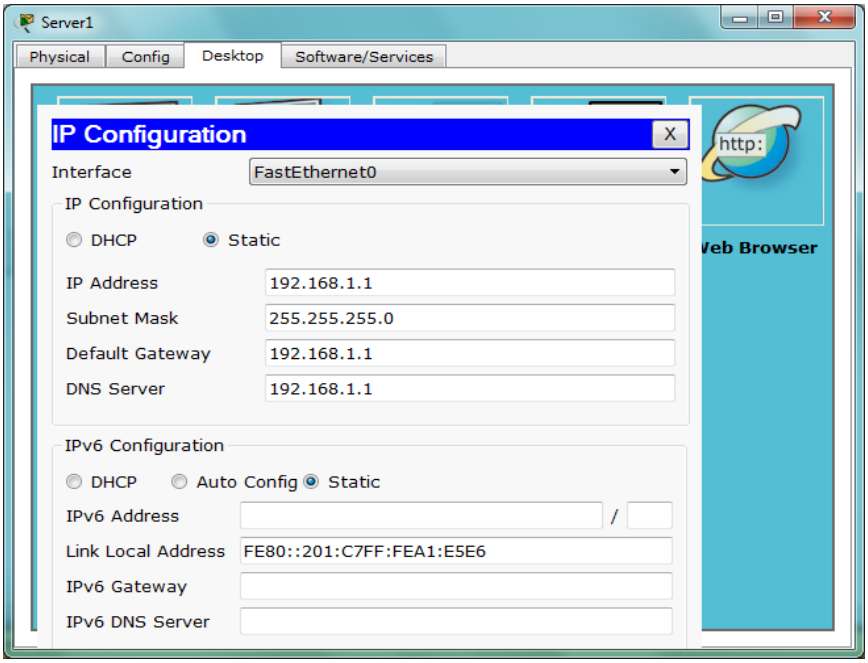


Figura 125. Configuración de IP del servidor.
Tomado de Herrera, R. (2014).

Para continuar con la configuración es necesario activar el servicio DHCP en cada nodo activándolo desde la IP seleccionando la opción DHCP:

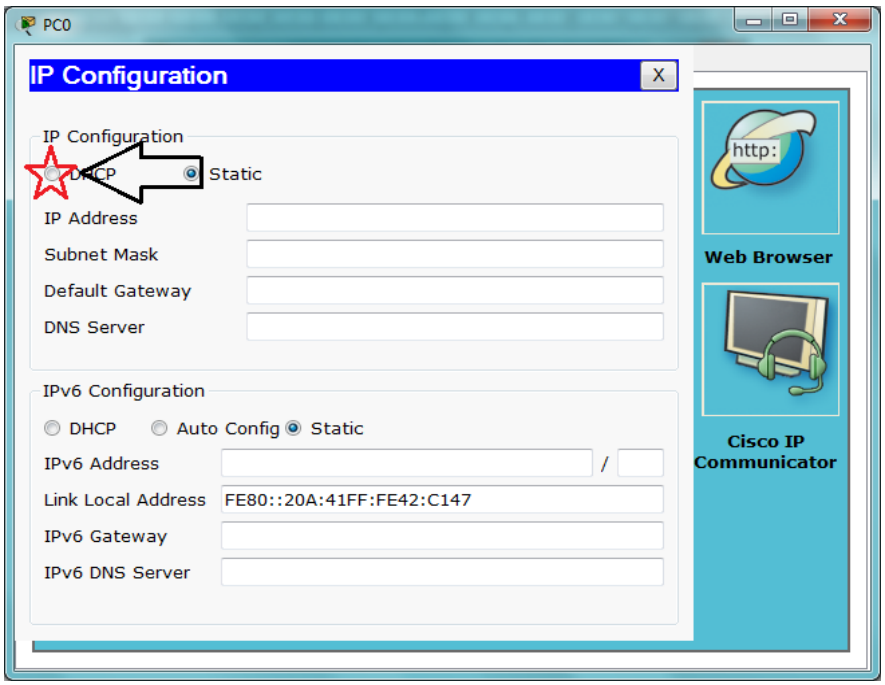


Figura 126. Activación del servicio DHCP en un host.
Tomado de Herrera, R. (2014).

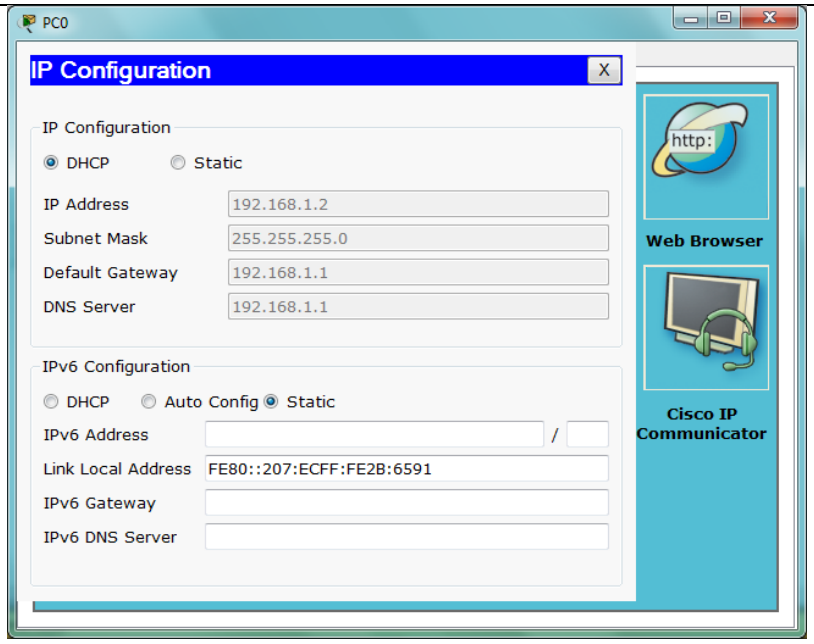


Figura 127. Servicio DHCP en un host activado y trabajando.
Tomado de Herrera, R. (2014).

Como resultado, el host recibe automáticamente la configuración desde el servidor y para confirmar la conectividad se realizar un ping hacia la IP 192.1681.1 (servidor).

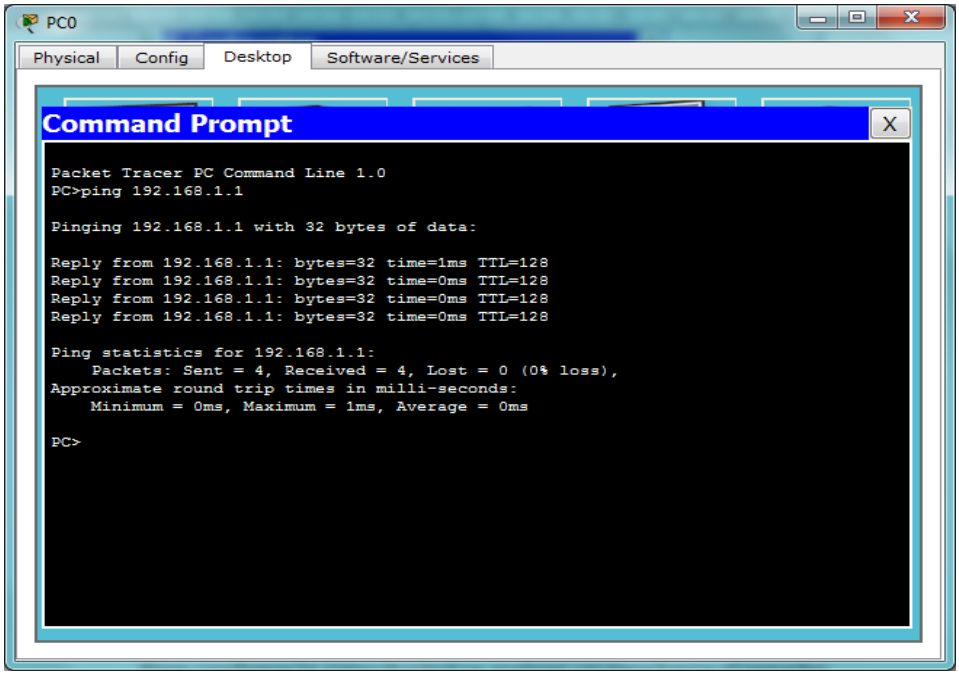


Figura 128. Ejecución del comando ping hacia el servidor.
Tomado de Herrera, R. (2014).

7.6.2. Configuración de IPv6.

Este protocolo es el siguiente paso de protocolo IPv4, cuyas características principales son:

- **Mayor espacio de direccionamiento:** Las direcciones pasan de 32 a 128 bits, es decir, 2 elevado a la 32 (4.294.967.296) direcciones.
- **Autoconfiguración:** permiten a los ordenadores conectados a una red asignarles su configuración de conectividad rápidamente.

Ejemplo:

- la web de www.hotmail.com en IPv4 es 193.110.128.200
- en IPv6 la IP de nuestra web es 2002:450:9:10::71, siendo su representación completa 2002:0450:0009:0010:0000:0000:0000:0071

En primer lugar se debe procede a la conexión física entre el computador y el router Billion por medio del cable de red o patch core hacia un puerto LAN.

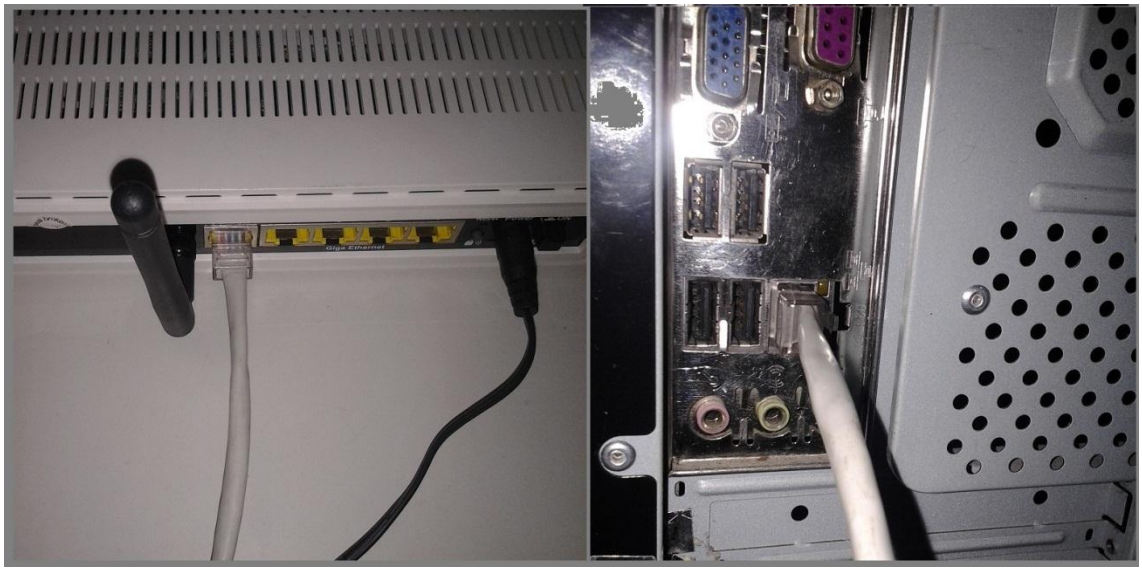


Figura 129. Conexión física por medio de un cable de red entre el router y el computador.
Tomado de Herrera, R. (2014).

Inmediatamente se realiza esta conexión aparecerá un mensaje indicando que la configuración actual no es apta para el correcto funcionamiento.

Figura 130. Mensaje informativo de un problema en la configuración del router al computador con Windows 7.
Tomado de Herrera, R. (2014).

El siguiente paso será ingresar a un navegador, en este caso se lo hará desde el Google Chrome donde automáticamente se direccionará a la configuración del router donde para acceder solicitará el usuario y contraseña.

- User : admin
- Password: admin

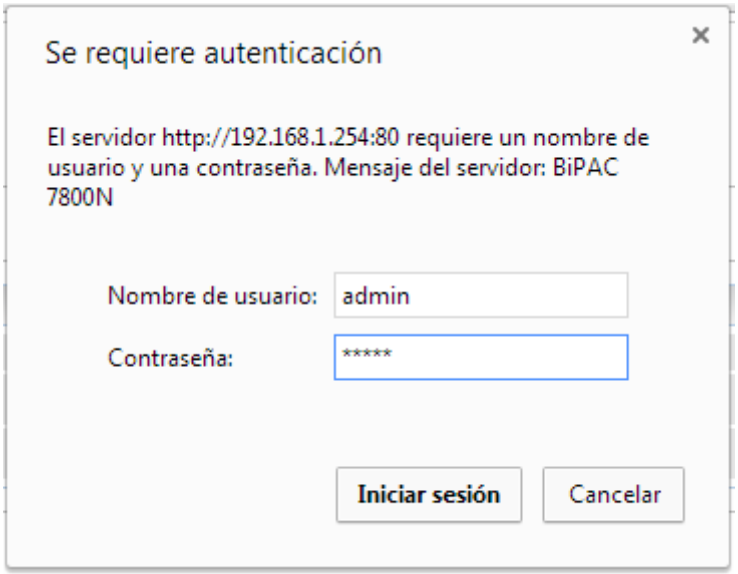


Figura 131. Campos para el ingreso de usuario y password para el acceso al router y configuración.
Tomado de Herrera, R. (2014).

En este punto el navegador direccionará al equipo a la configuración del router donde la opción a escoger es Advanced.

Figura 132. Selección de opción Advance para la configuración básica del router.
Tomado de Herrera, R. (2014).

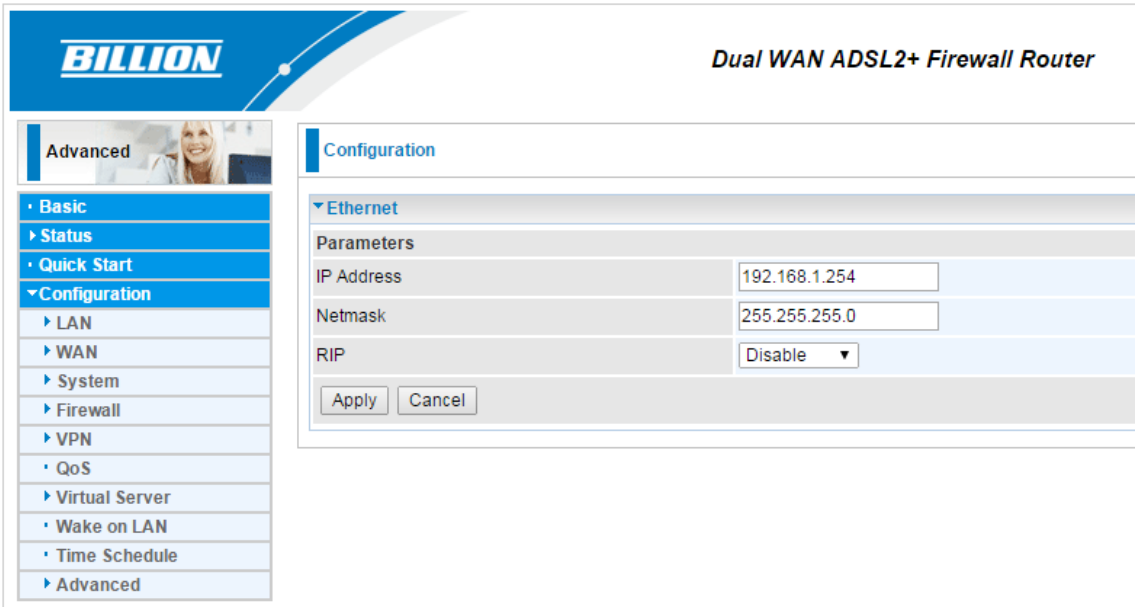


Figura 133. Campos para el ingreso de usuario y password para el acceso al router y configuración.
Tomado de Herrera, R. (2014).

En la presente ventana se debe seleccionar la opción Configutation donde se procederá a configurar la red LAN y el servicio DHCP que se necesita para la elaboración del laboratorio.

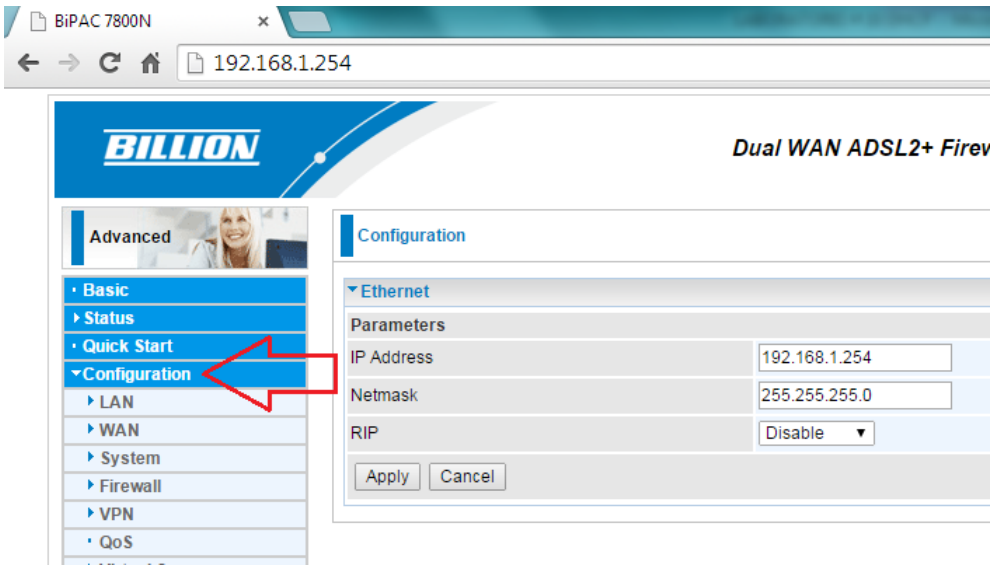


Figura 134. Campos para el ingreso de usuario y password para el acceso al router y configuración.
Tomado de Herrera, R. (2014).

7.6.3. Configuración RED LAN

A continuación se realizará la configuración de la red LAN por lo que se tiene que realizar los siguientes pasos:

- Escoger opción LAN
- Ethernet
- Mantener la IP por 192.168.1.254

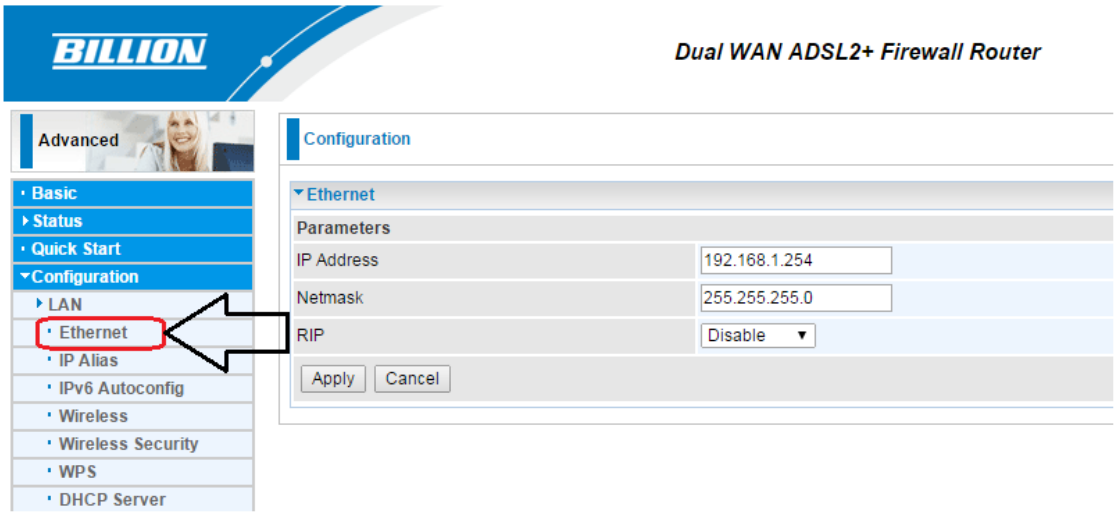


Figura 135. Selección de opción LAN y opciones de configuración. Tomado de Herrera, R. (2014).

A continuación se debe proceder a la configuración de Wireless solamente seleccionándola como se muestra en la imagen 17:

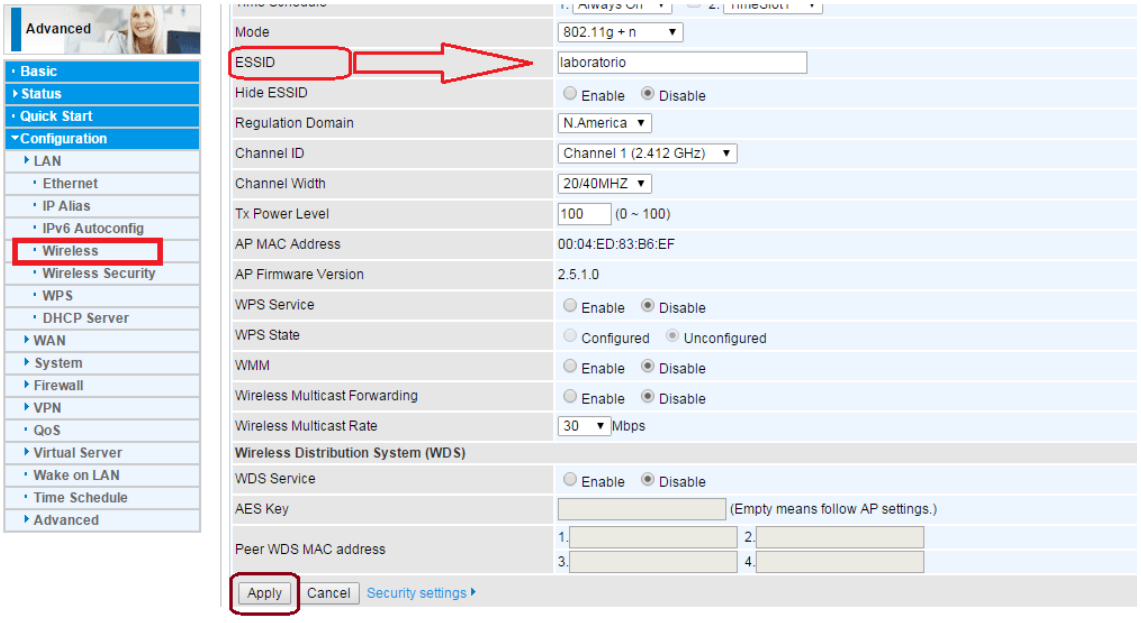


Figura 136. Configuración de SSID de wireless. Tomado de Herrera, R. (2014).

Como se muestra en la imagen 17 el único campo que hay que cambiar es el del SSID que se muestra, cambiarlo por “laboratorio” (sin comillas) y presionar el botón Apply.

Ahora la opción a escoger es IPv6 Autoconfig, habilitar la opción Enable, posteriormente dar clic en el botón Apply seguido de la opción Save Config para salvar la configuración que hasta el momento se ha realizado.

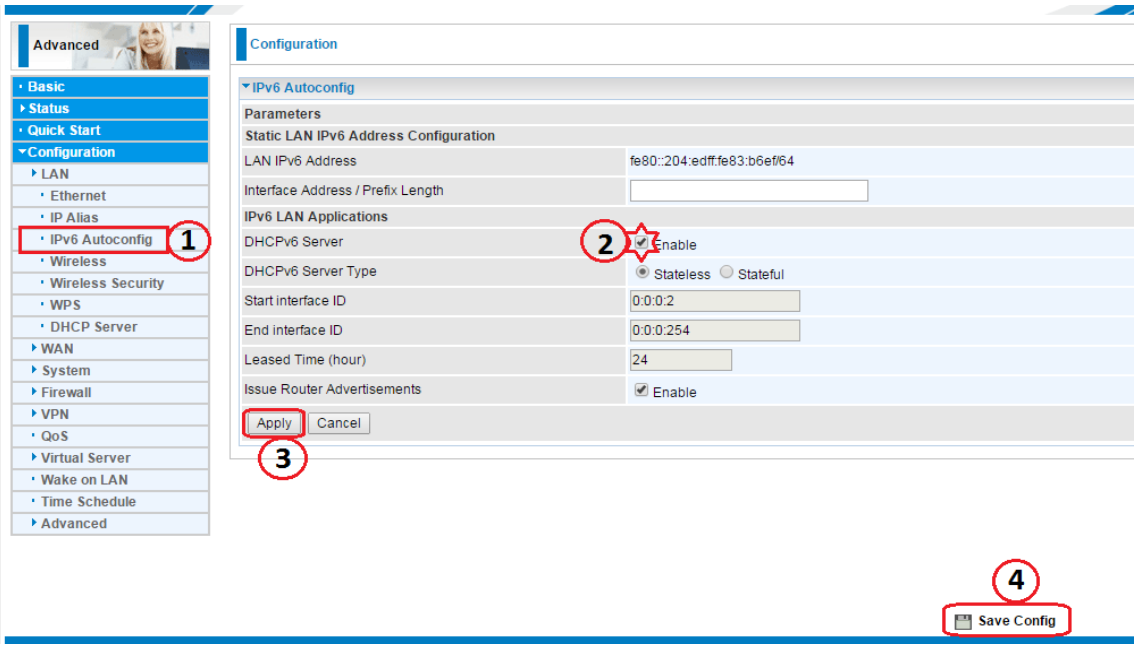


Figura 137. Pasos a seguir para la activación del servicio DHCP en IPv6. Tomado de Herrera, R. (2014).

En este momento es necesario hacer uso de otro computador (Laptop) y realizar la ejecución del comando ipconfig y así observar la configuración de la IP antes de ingresar a la red del router.

El servicio DHCP es un protocolo utilizado para asignar automáticamente a terminales una configuración necesaria para estar comunicados entre sí.

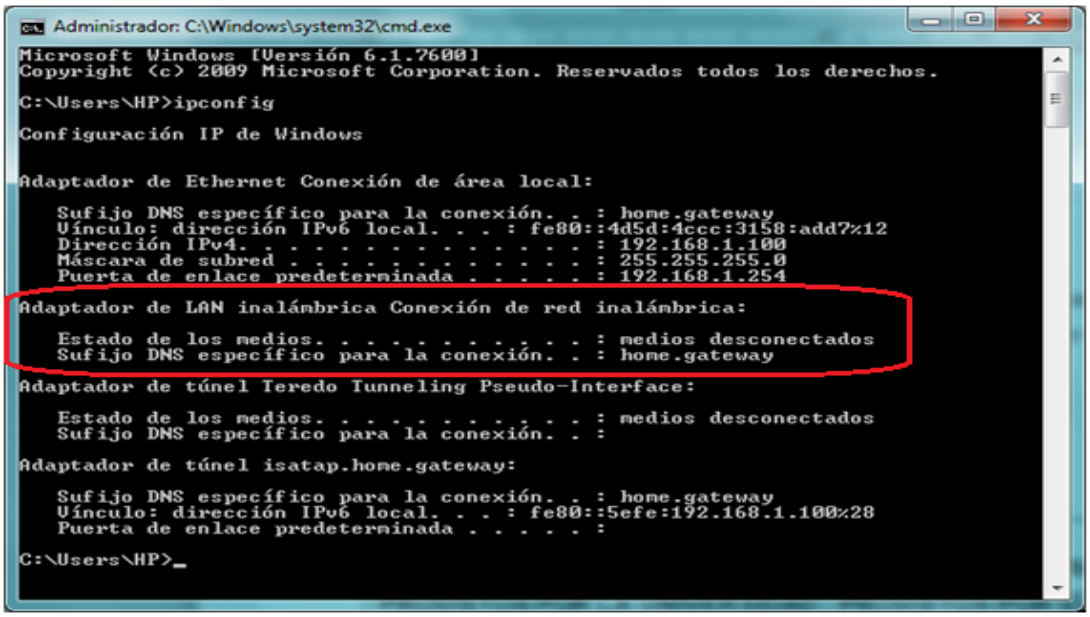


Figura 138. Ventana de comando ipconfig en ejecución y mostrando la configuración del equipo.
Tomado de Herrera, R. (2014).

La conexión por wifi será el próximo paso a seguir ubicando y seleccionando la red laboratorio.

Figura 139. Estado de conexión inalámbrica.
Tomado de Herrera, R. (2014).

Para culminar se debe ejecutar nuevamente el comando ipconfig para comprobar el estado de la dirección IPv6.

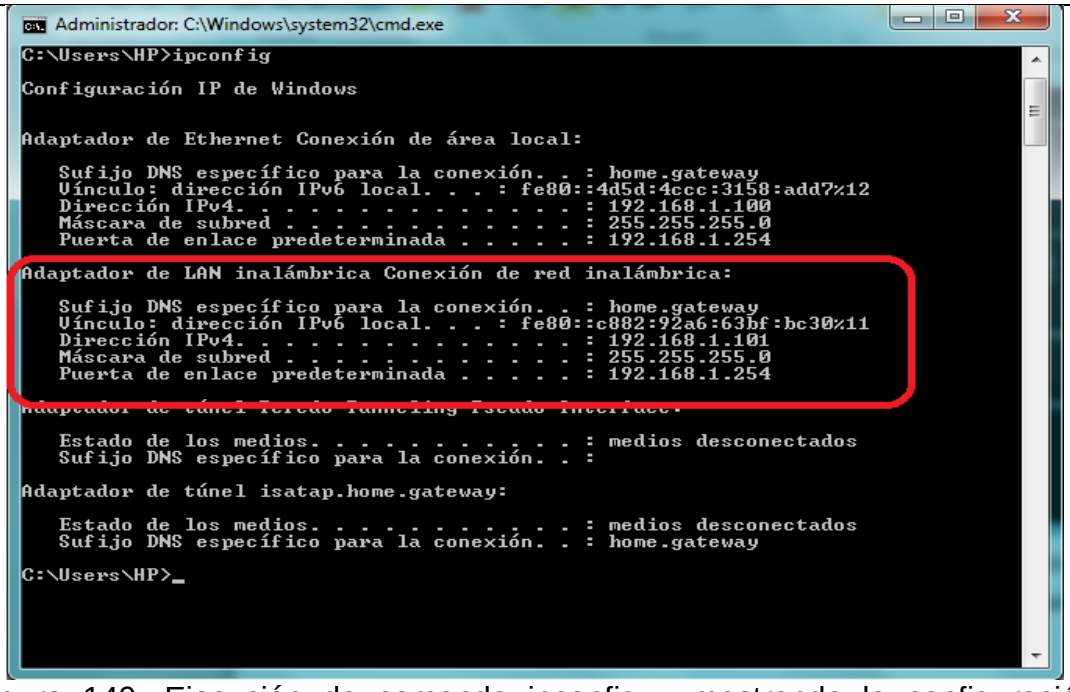


Figura 140. Ejecución de comando ipconfig y mostrando la configuración después de conectar a la red laboratorio.
Tomado de Herrera, R. (2014).

En este punto se puede apreciar que el IPv6 se encuentra levantado y asignó de manera automática la configuración.

7.7. RESULTADO DE LA PRÁCTICA

- Por medio de este servicio los equipos del simulador reciben una configuración automáticamente.
- Configuración DHCP en router.
- Configuración de servicio DHCP.
- Manejo de simulador.

7.8. CONCLUSIONES Y RECOMENDACIONES

- El laboratorio funcionó con éxito y el comando ping comprobó la conectividad.
- Las IP’s de los servidores o equipos están seguros.
- No habrá conflicto de IP’s pues el servidor se encarga de gestionarlas.
- Reutilización de direcciones IP’s.

REFERENCIAS

Andrew, O., Woodward, B. (2009). Cabling the complete guide to copper and Fiber-Optic Networking, Indianapolis, Indiana: Editex.

Caballeiro, G, (2012). Redes wi-fi (1ª ed.). Buenos Aires, Argentina: Dalaga S.A.

Collado, E. (2009). Fundamentos de Routing. Madrid, España: Lulu.com.

Collado, E. (2009). Fundamentos de Routing. Madrid, España: Lulu.com.

Dordoigne, J, (2013). Redes informáticas (4ª ed.). Barcelona, España: Ediciones Eni.

Flickenger, R. (2008). Redes inalámbricas en los países en desarrollo: una guía práctica para planificar y construir infraestructuras de telecomunicaciones de bajo costo (2ª ed.). Gran Bretaña, Inglaterra: Hacker Friendly LLC.

Gallego,J. (2014). Operaciones auxiliares para la configuración y la explotación. (1ªed.). Madrid, España: Editex.

García, F. (2010). Videovigilancia: CCTV usando vídeos IP (1ª ed.). Málaga, España: Fundación Vértice Emprende.

Gómez, J. (2010). Servicios en Red. Madrid, España: Editex.

Huidobro, M. (2007). Sistemas Telemáticos. Madrid, España: Parainfo.

José Ramón Oliva Haba, Custodia Manjavacas Zarco, Pedro Luis Martin Márquez. (2014). Montaje y mantenimiento de equipos. (2ª ed.). Madrid, España: Paraninfo S.A.

Martín, J. Alba, J. (2012). Infraestructuras comunes de telecomunicaciones en viviendas y edificios, (4 ª ed). España: Library of Congress Cataloging-in- Publication Data.

Zeas, R. (2011). Análisis y captura de paquetes de datos en una red mediante la herramienta Wireshark. Quito, Ecuador: Handle System.