

**INSTITUTO POLITÉCNICO NACIONAL  
ESCUELA SUPERIOR DE CÓMPUTO**



**Practica 1 Simulación de Red  
Packet tracert**

**Profesor: Ing. Juan J. Alcarazt  
Torres.**

**Alumno : Silva Hernandez Noe Jasiel**

**Grupo: 2CV6**

**Materia : Redes de Computadoras**



**Materia:** Redes de Computadoras.  
**Profesor:** Ing. Juan J. Alcaraz Torres.  
**Tema:** Practica 1

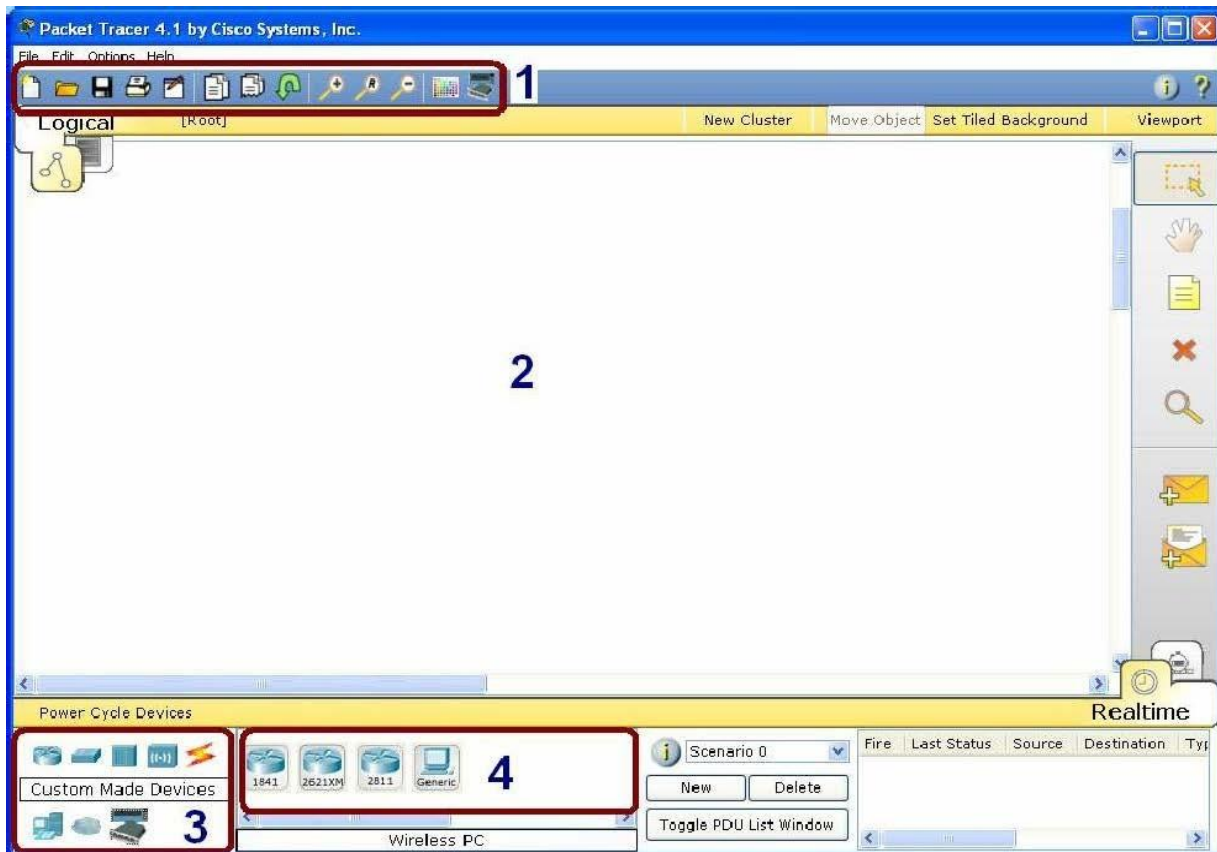
## PACKET TRACER COMO HERRAMIENTA DE SIMULACION

Una de las herramientas más utilizadas en el mundo orientadas a la simulación de redes de datos es Packet Tracer, el cual consiste en un simulador gráfico de redes desarrollado y utilizado por Cisco como herramienta de entrenamiento para obtener la certificación CCNA. Packet Tracer, es un simulador de entorno de redes de comunicaciones de fidelidad media, que permite crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo, utilizando una interfaz gráfica.

Packet Tracer es un simulador que permite realizar el diseño de topologías, la configuración de dispositivos de red, así como la detección y corrección de errores en sistemas de comunicaciones. Ofrece como ventaja adicional el análisis de cada proceso que se ejecuta en el programa de acuerdo a la capa de modelo OSI que interviene en dicho proceso; razón por la cuáles una herramienta de gran ayuda en el estudio y aprendizaje del funcionamiento y configuración de redes telemáticas, adicionalmente, es un programa muy útil para familiarizarse con el uso de los comandos del IOS (El sistema operativo de los dispositivos de red de Cisco).

Esta herramienta software ofrece una interfaz basada en ventanas, la cual ofrece al usuario facilidades para el diseño, configuración y simulación de redes. Presenta tres modos de operación: el primero de estos es el modo topology (topología), que aparece en la ventana de inicio cuando se abre el programa, el otro es el modo simulation (simulación), al cual se accede cuando se ha creado el modelo de la red; finalmente aparece el modo realtime (tiempo real), en donde se pueden programar mensajes SNMP (Ping), para detectar los dispositivos que están activos en la red y si existen algún problema de direccionamiento o tamaño de tramas entre las conexiones. A continuación se describirá brevemente cada uno de los modos de operación de Packet Tracer.

En el Modo Topology, se realizan tres tareas principales, la primera de ellas es el diseño de la red mediante la creación y organización de los dispositivos; por consiguiente en este modo de operación se dispone de un área de trabajo y de un panel de herramientas en donde se encuentran los elementos de red disponibles en Packet Tracer.



En la figura se identifican claramente 4 secciones: la primera consiste en la barra de herramientas con la cual se puede crear un nuevo esquema, guardar una configuración, zoom, entre otras funciones.

La segunda sección corresponde al área de trabajo, sobre la cual se realiza el dibujo del esquema topológico de la red.

La tercera es la sección correspondiente al grupo de elementos disponibles para la implementación de cualquier esquema topológico, el cual incluye: Routers, Switches, Cables para conexión, dispositivos terminales (PCs, impresoras, Servidores), Dispositivos Inalámbricos, entre otros.

La sección 4, lista el conjunto de elementos que hacen parte del dispositivo seleccionado en la sección 3. A continuación se ilustran el conjunto de elementos que hacen parte de cada grupo de dispositivos.



**Routers:** Series 1800, 2600, 2800, Genéricos

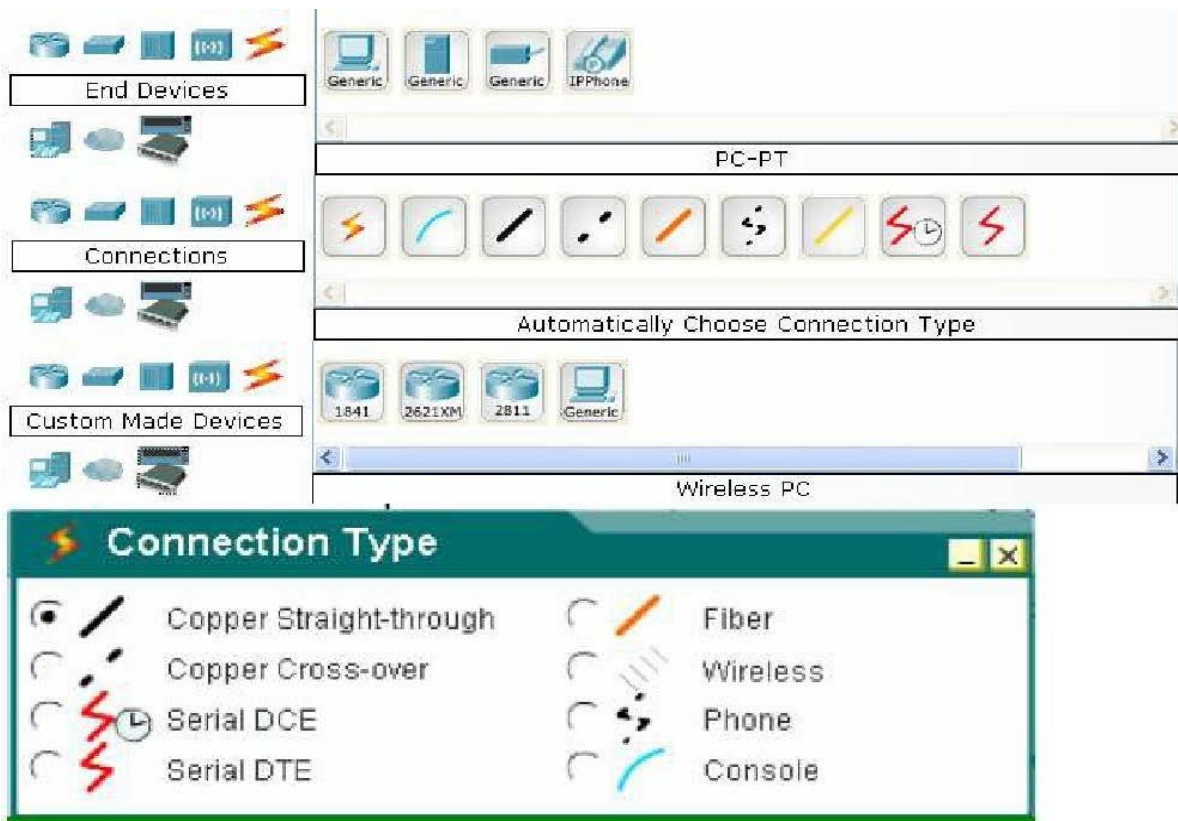
**Switches:** Series 2950, 2960, Genérico, Bridge

**Dispositivos inalámbricos:** Access-Point, Router Inalámbrico

**Tipos de conexiones disponibles:** Cable serial, consola, directo, cruzado, fibra óptica, teléfono, entre otras.

**Dispositivos terminales:** PC, servidores, impresoras, teléfonos IP

**Dispositivos adicionales:** PC con tarjeta inalámbrica



La herramienta está diseñada para orientar al estudiante en su manipulación adecuada.

Dentro del modo de operación topology, existe una herramienta que permite hacer de forma automática, las conexiones entre los dispositivos de la red, ésta opción se activa cuando se selecciona el Simple Mode (modo simple) y esta selección hace que el programa sea el que elija el tipo de enlace, de acuerdo con la conexión que se va a realizar.

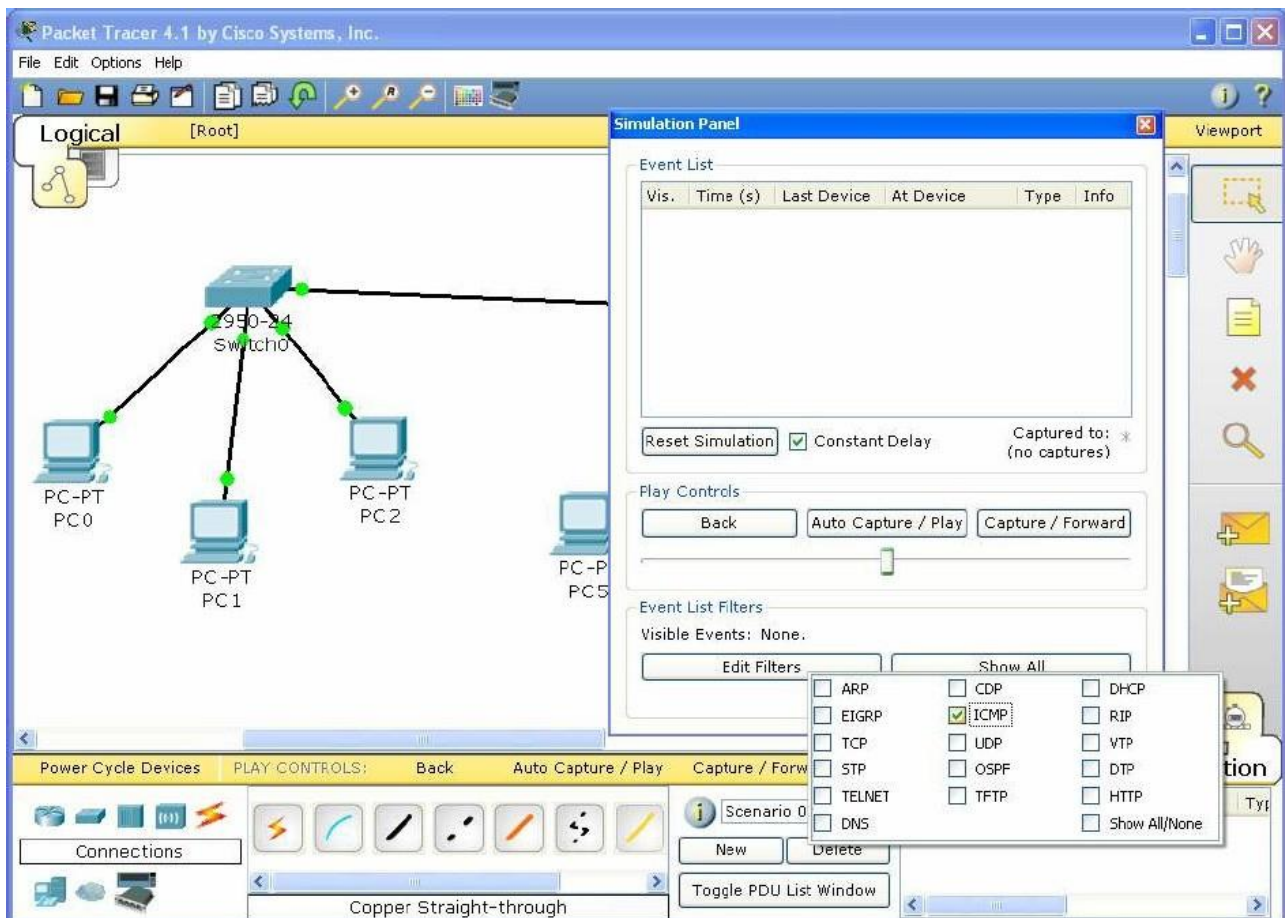
Cuando se desactiva el Simple Mode, el usuario debe seleccionar el enlace y los puertos de los dispositivos por los cuales se efectuará dicha conexión.

Adicionalmente, recomienda que en las primeras experiencias con el programa, se debe trabajar y configurar manualmente los dispositivos y enlaces, es decir con el Simple Mode inactivo; debido a que es así como realmente interactuará el usuario con cada una de las conexiones a la hora de realizar un montaje real con equipos de éste tipo.

En el Modo Simulation, se crean y se programan los paquetes que se van a transmitir por la red que previamente se ha modelado.



Dentro de este modo de operación se visualiza el proceso de transmisión y recepción de infor-



mación haciendo uso de un panel de herramientas que contiene los controles para poner en marcha la simulación.

Una de las principales características del modo de operación simulation, es que permite desplegar ventanas durante la simulación, en las cuales aparece una breve descripción del proceso de transmisión de los paquetes; en términos de las capas del modelo OSI. En la siguiente figura se ilustra un ejemplo en el que se envía un paquete desde el PC0 al PC5



Y finalmente el Modo de operación en tiempo real, está diseñado para enviar pings o mensajes SNMP, con el objetivo de reconocer los dispositivos de la red que están activos, y comprobar que se puedan transmitir paquetes de un host a otro en la red.

Ventajas	Desventajas
El enfoque pedagógico de este simulador, hace que sea una herramienta muy útil como complemento de los fundamentos teóricos sobre redes de comunicaciones.	Es un software propietario, y por ende se debe pagar una licencia para instalarlo.
El programa posee una interfaz de usuario muy fácil de manejar, e incluye documentación y tutoriales sobre el manejo del mismo. Permite ver el desarrollo por capas del proceso de transmisión y recepción de paquetes de datos de acuerdo con el modelo de referencia OSI.	Solo permite modelar redes en términos de filtrado y retransmisión de paquetes.
Permite la simulación del protocolo de enrutamiento RIP V2 y la ejecución del protocolo STP y el protocolo SNMP para realizar diagnósticos básicos a las conexiones entre dispositivos del modelo de la red.	No permite crear topologías de red que involucren la implementación de tecnologías diferentes a Ethernet; es decir, que con este programa no se pueden implementar simulaciones con tecnologías de red como Frame Relay, ATM, XDSL, Satelitales, telefonía celular entre otras.  Ya que su enfoque es pedagógico, el programa se considera de fidelidad media para implementarse con fines comerciales.

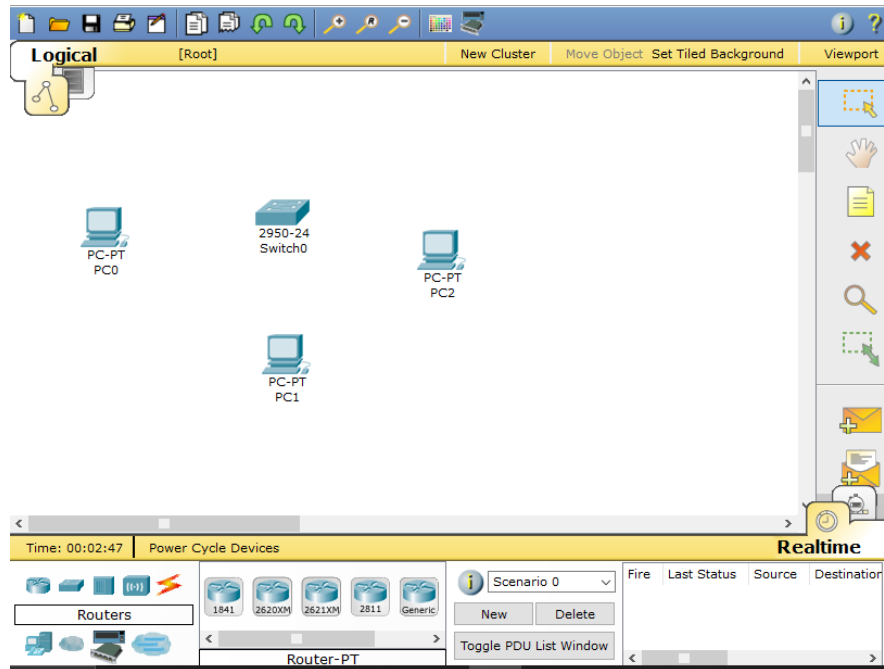
Dentro del modo Realtime, se encuentra el cuadro de registro Ping log, en donde se muestran los mensajes SNMP que han sido enviados y se detalla además el resultado de dicho proceso; con base en este resultado se puede establecer cuál o cuales de los terminales de la red están inactivos, a causa de un mal direccionamiento IP, o diferencias en el tamaño de bits de los paquetes. En la siguiente figura se ilustra claramente un ejemplo de una red, en donde se ingresa a uno de los equipos (PC5) y se hace PING al equipo PC0. Dentro de las ventajas y desventajas que ofrece el uso de Packet Tracer podemos mencionar



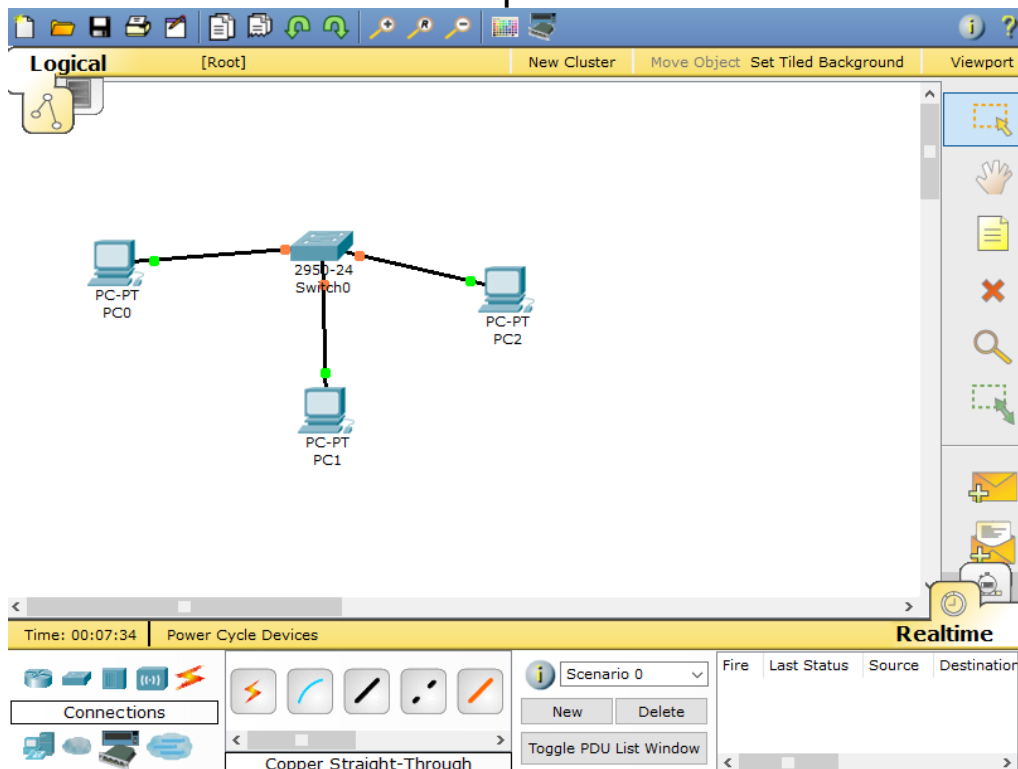


# DESARROLLO

Agregando pc's genericas

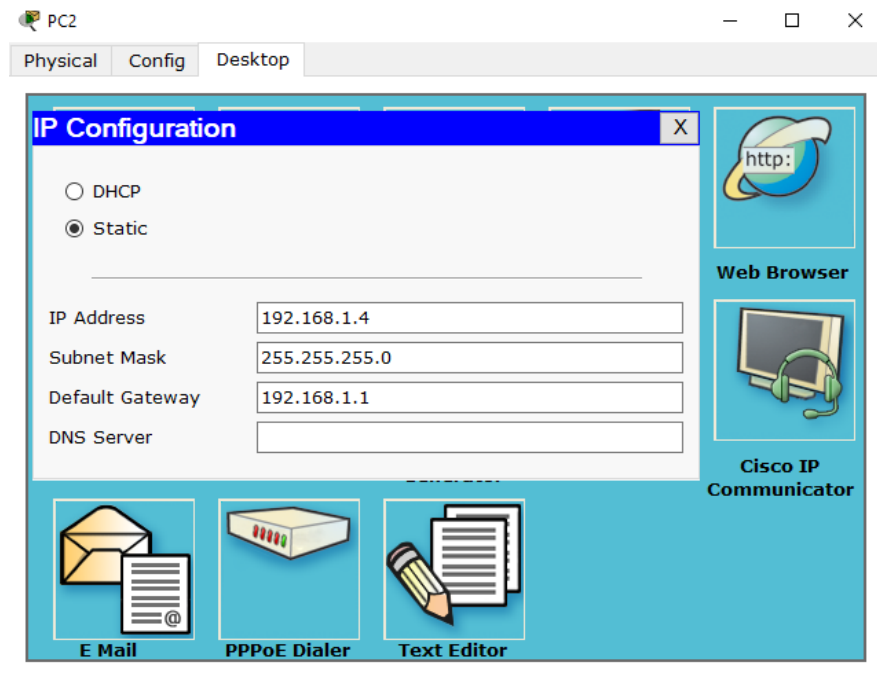


Cableando pc's al switch



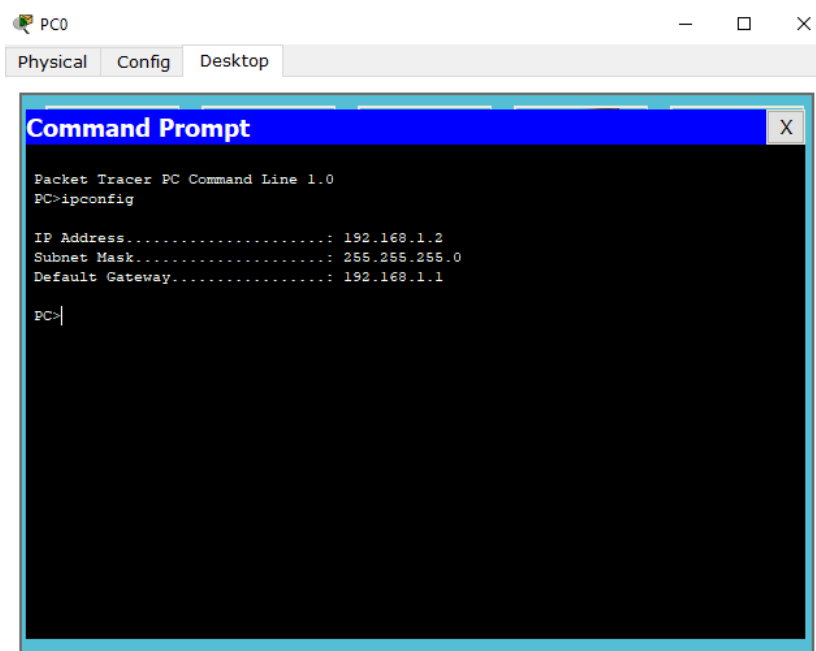


a cada pc se le establece una dirección IP además de un default Gateway y la Subnet Mask se establece por defecto



## Probando comando IPCONFIG

En donde se identifican los parámetros del host correspondientes a la dirección IP, la máscara de Subred y la dirección de Gateway

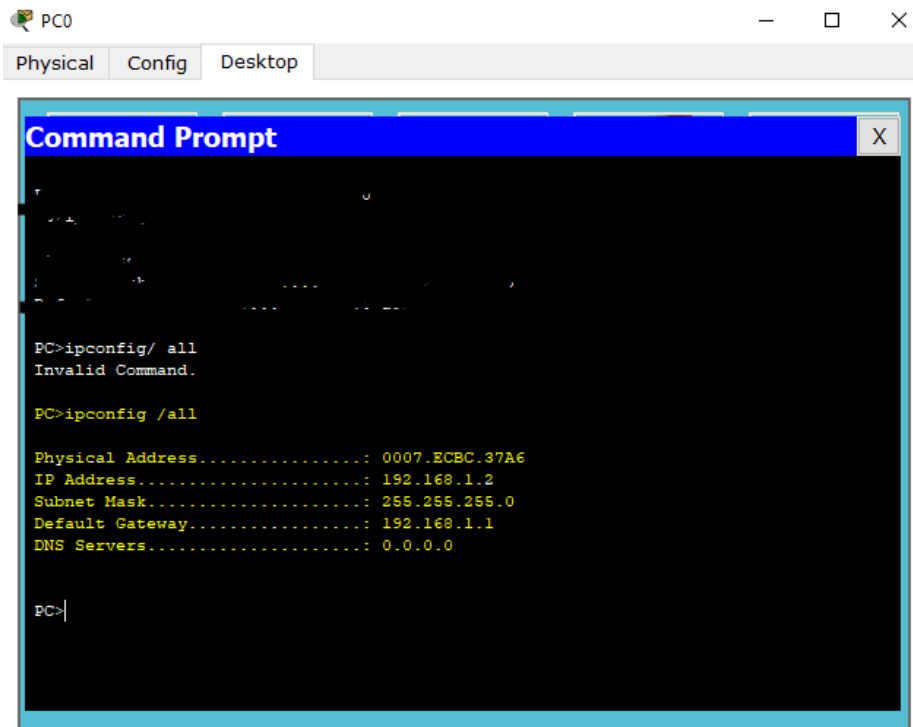






## Comando IPCONFIG/ ALL

En donde se evidencia no solo los parámetros mencionados anteriormente, sino que además incluye la dirección física del equipo conocida como MAC y la dirección del servidor de dominio DNS.



```
PC0
Physical Config Desktop

Command Prompt

PC>ipconfig/ all
Invalid Command.

PC>ipconfig /all

Physical Address.....: 0007.ECBC.37A6
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 0.0.0.0

PC>
```



## Probando conexión entre dispositivos

### Comando PING

Para verificar que existe una comunicación entre los diferentes equipos que hacen parte de la red, simplemente se selecciona uno de ellos y se le hace un ping

```
PC2
Physical Config Desktop

Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=13ms TTL=128
Reply from 192.168.1.4: bytes=32 time=16ms TTL=128
Reply from 192.168.1.4: bytes=32 time=16ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 11ms

PC>
```

En la imagen se ve que se enviaron 4 paquetes y se recibieron 4 por lo cual quiere decir que si hay conexión

--en la sig imagen se hará ping a una IP que no esta en al red

```
PC2
Physical Config Desktop

Command Prompt
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=97ms TTL=128
Reply from 192.168.1.2: bytes=32 time=47ms TTL=128
Reply from 192.168.1.2: bytes=32 time=63ms TTL=128
Reply from 192.168.1.2: bytes=32 time=62ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 97ms, Average = 67ms

PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

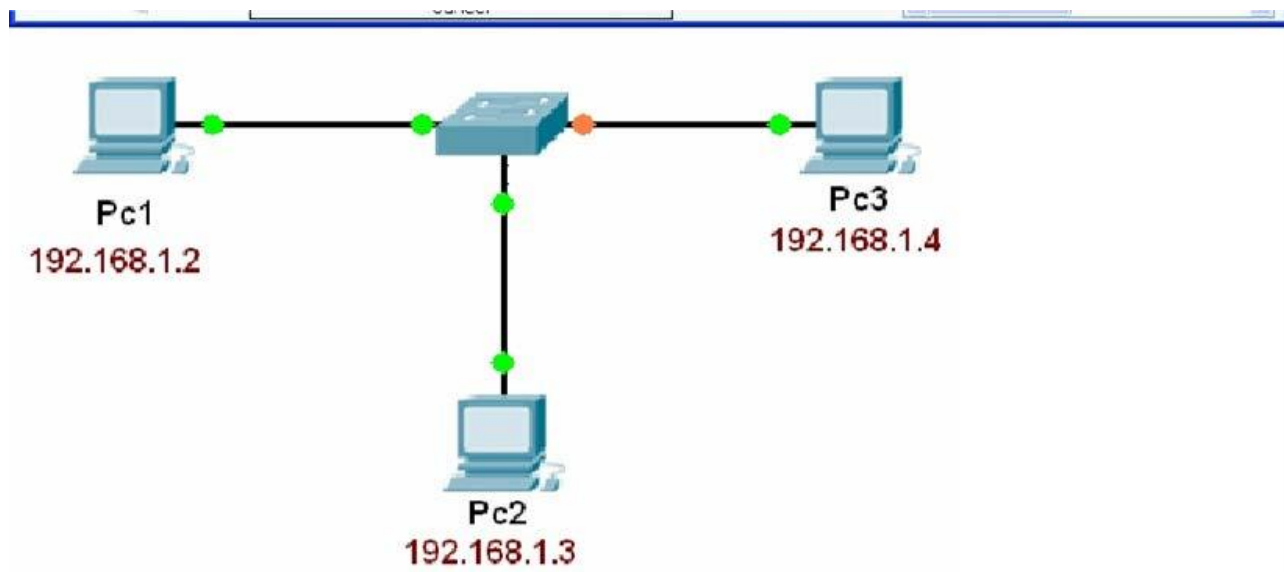
Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

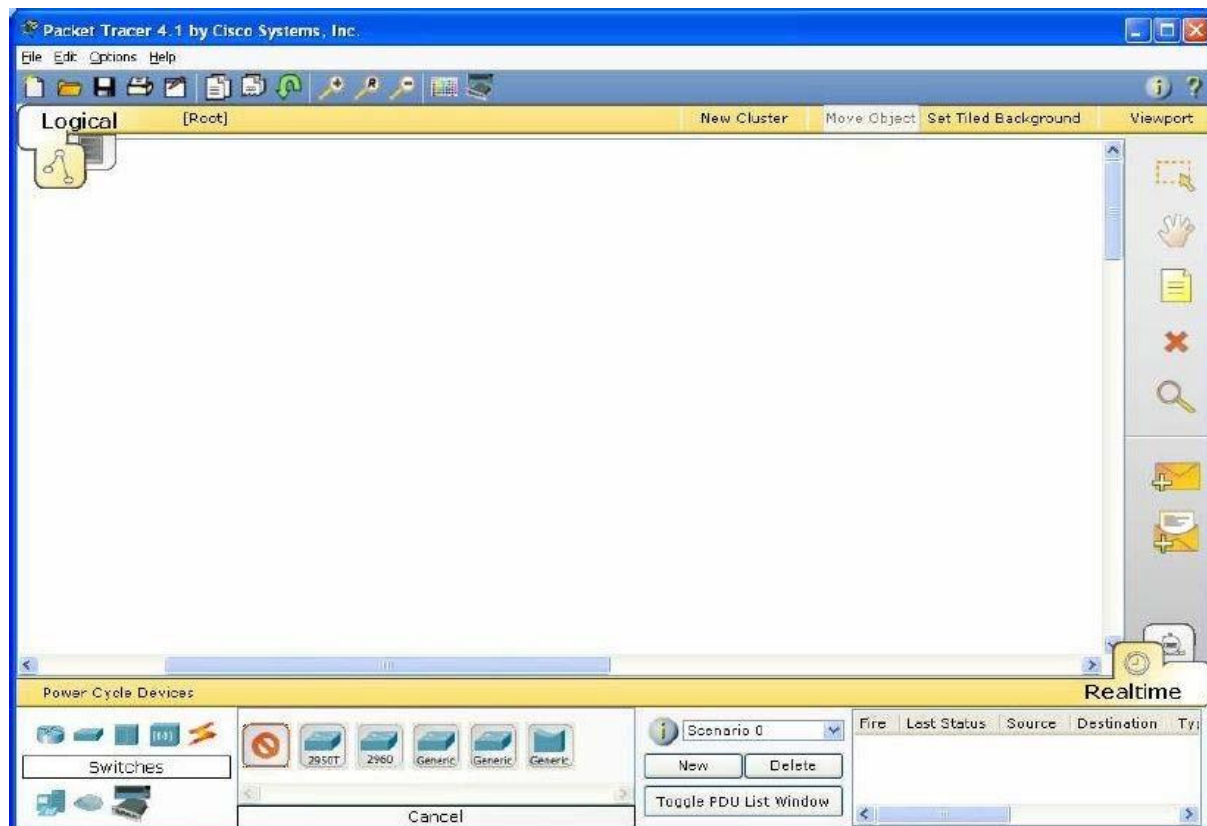


## Primera aplicación

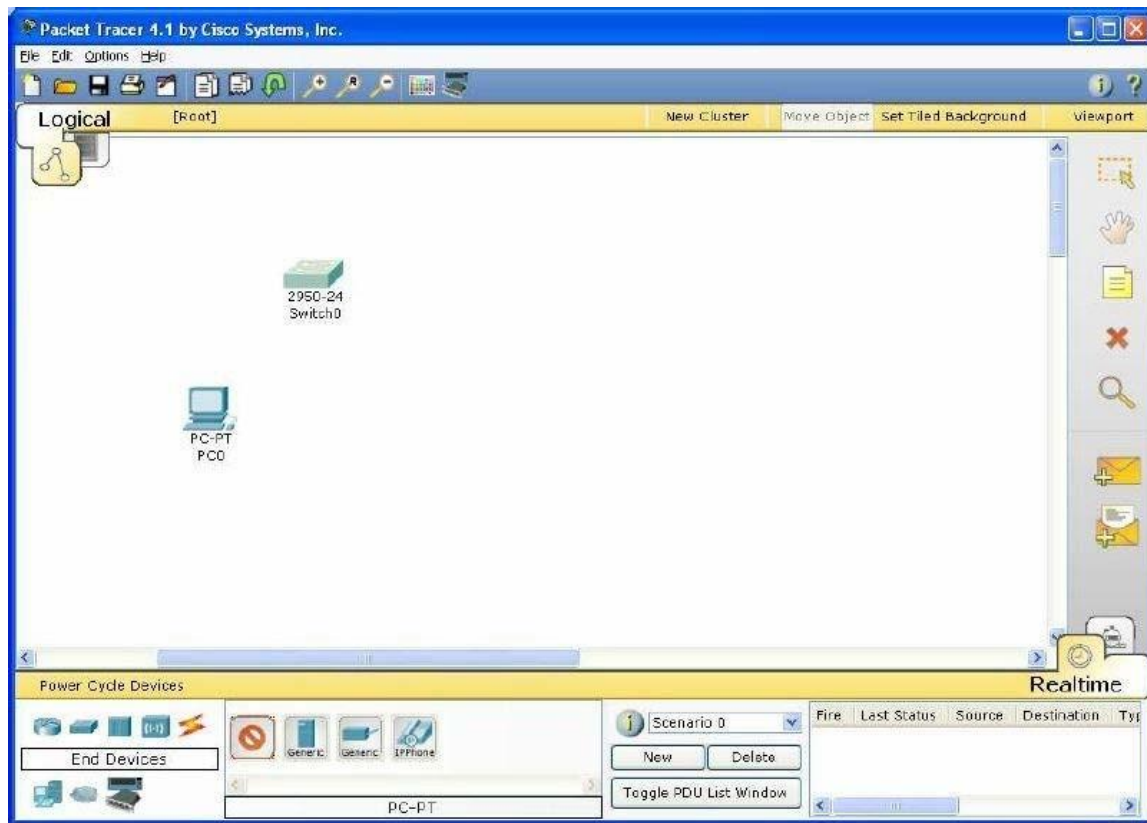
Utilizando la herramienta de simulación packet tracer, se desea implementar la siguiente estructura de red.



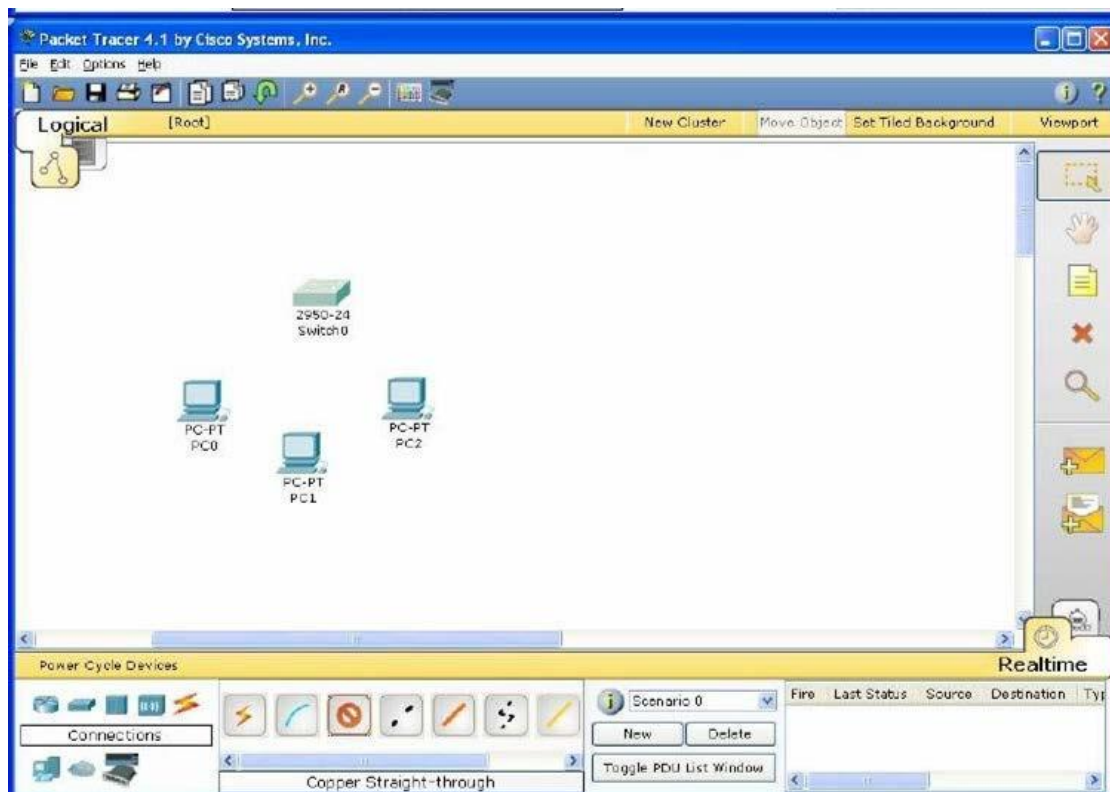
Paso 1: Ingresar a la herramienta Packet Tracer y seleccionar la referencia de Switch 2950-24 el cual se encuentra en el menú Switches, tal como se ilustra en la figura



Paso 2: En el menú End Devices, seleccionar la opción PC-PT y dibujar el primer PC, tal como se indica en la figura.



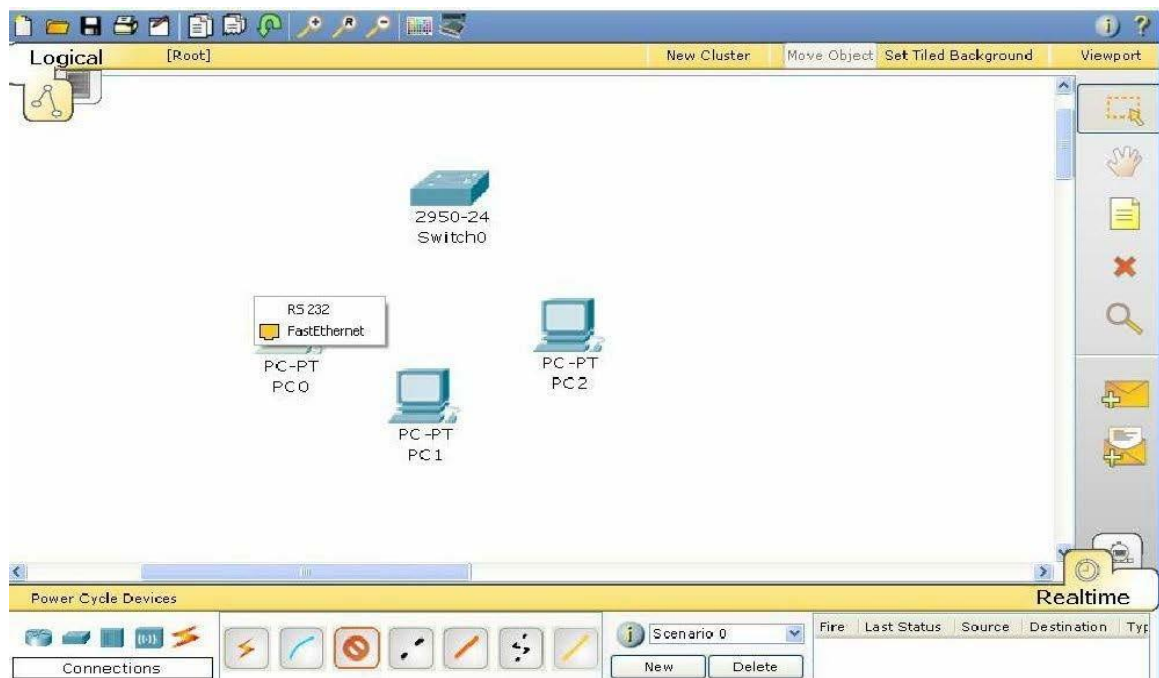
Repetir el paso anterior dos veces, completando con ello los tres Pcs requeridos en el esquema



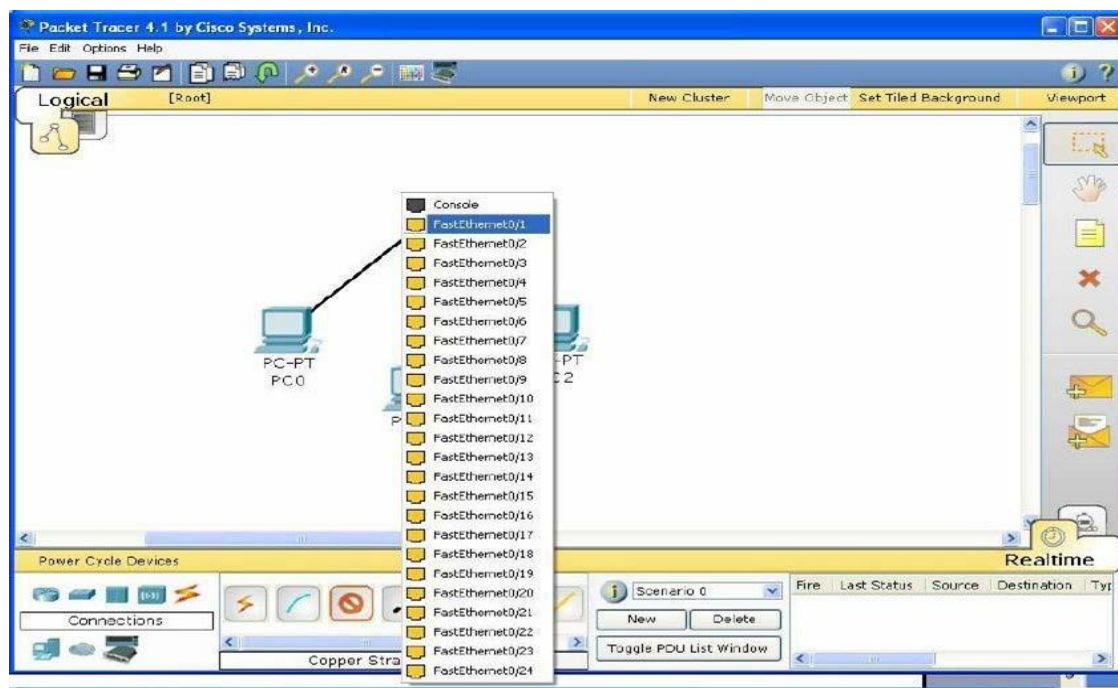


Paso 3: En la opción Connections del menú de elementos, escoger la opción Copper Straight through, la cual corresponde a un cable de conexión directa requerido en éste caso para conectar un Pc a un Switch.

Hecho esto, se debe seleccionar el primer PC, hacer click con el botón derecho del Mouse y escoger la opción Fastethernet, indicando con ello que se desea establecer una conexión a través de la tarjeta de red del equipo.



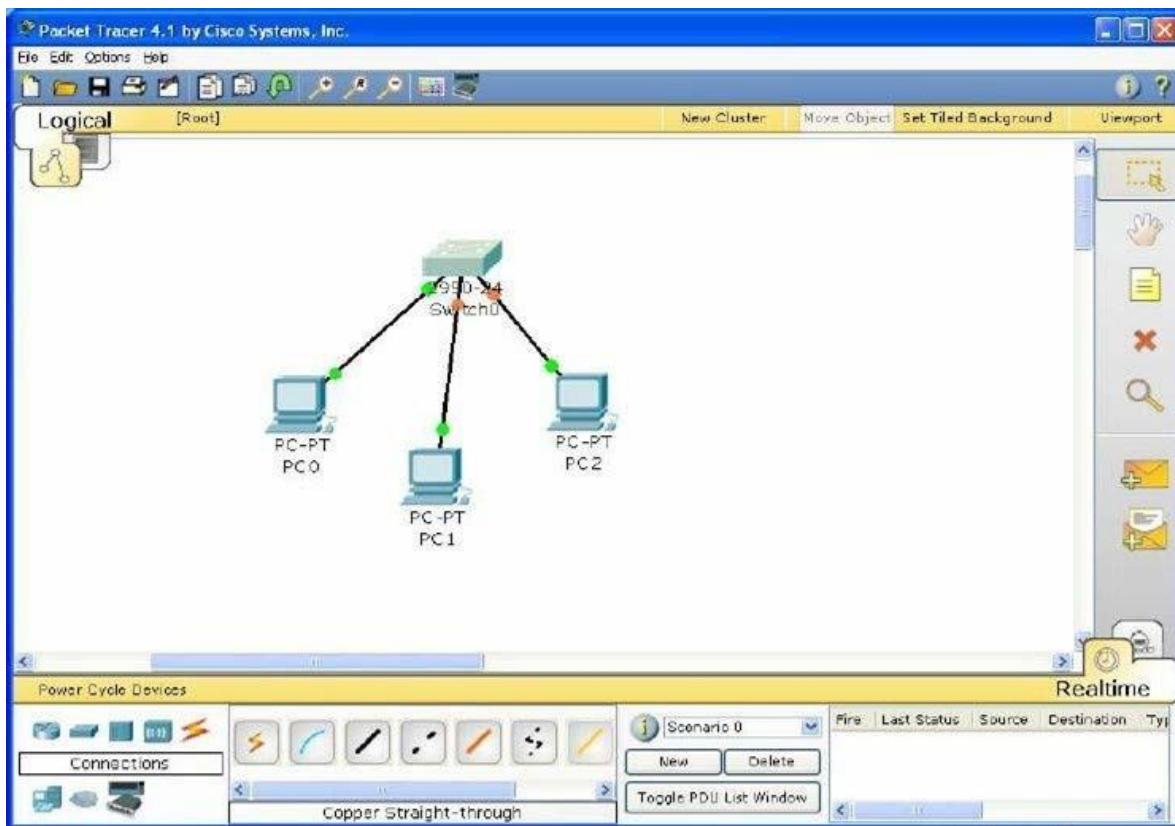
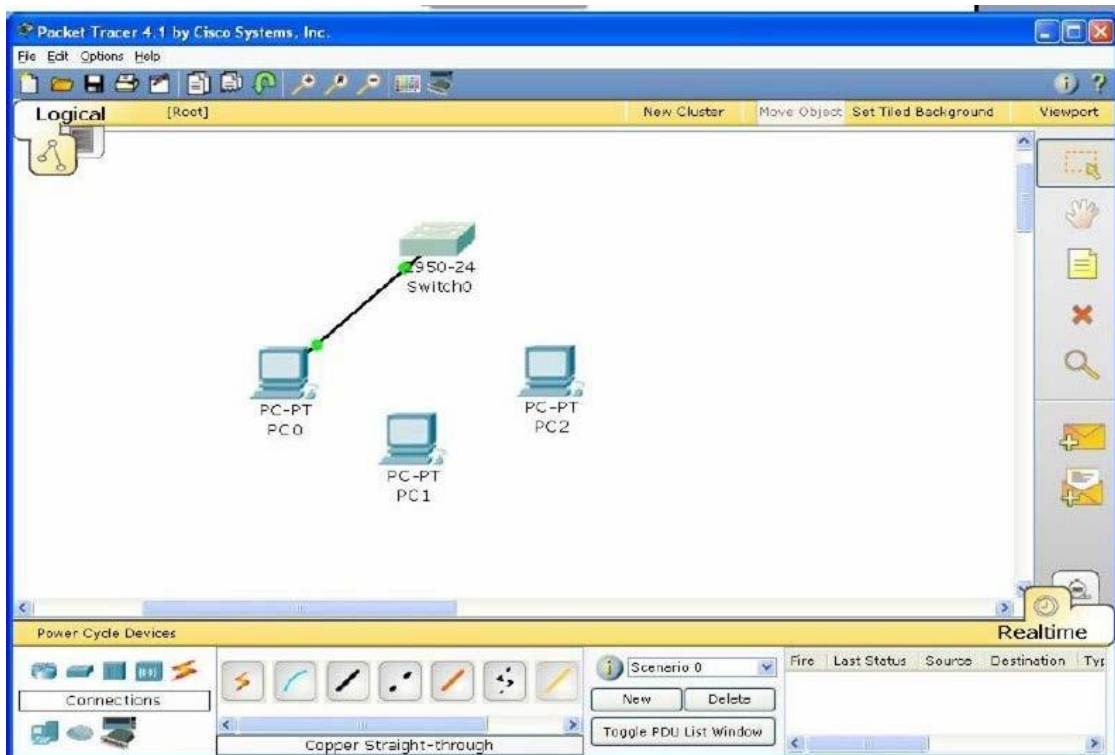
Paso 4: Después de seleccionar la opción Fastethernet en el primer Pc, arrastrar el Mouse hasta el Switch, hacer clic sobre él y seleccionar el puerto sobre el cual se desea conectar el Pc1, en nuestro caso corresponde al puerto Fastethernet 0/1.





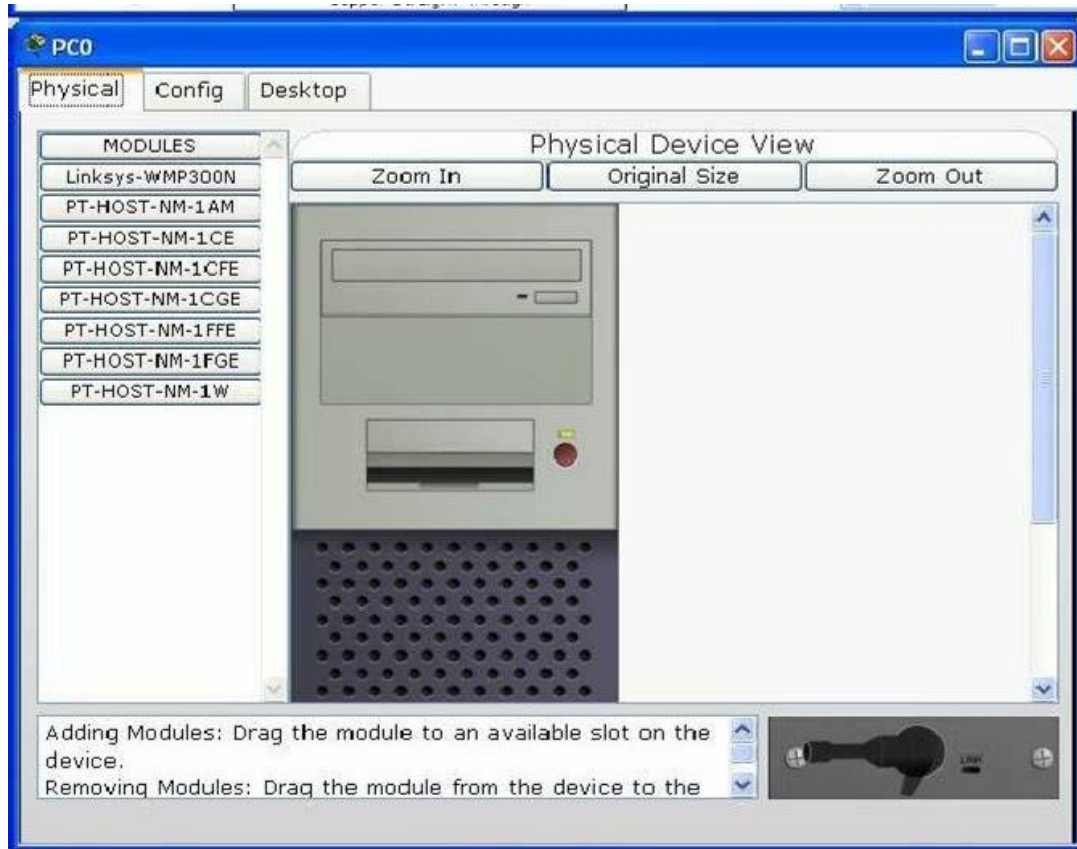


El resultado de lo anterior se refleja en la siguiente figura, lo cual se debe repetir con cada uno de los Pcs que hacen parte del diseño.



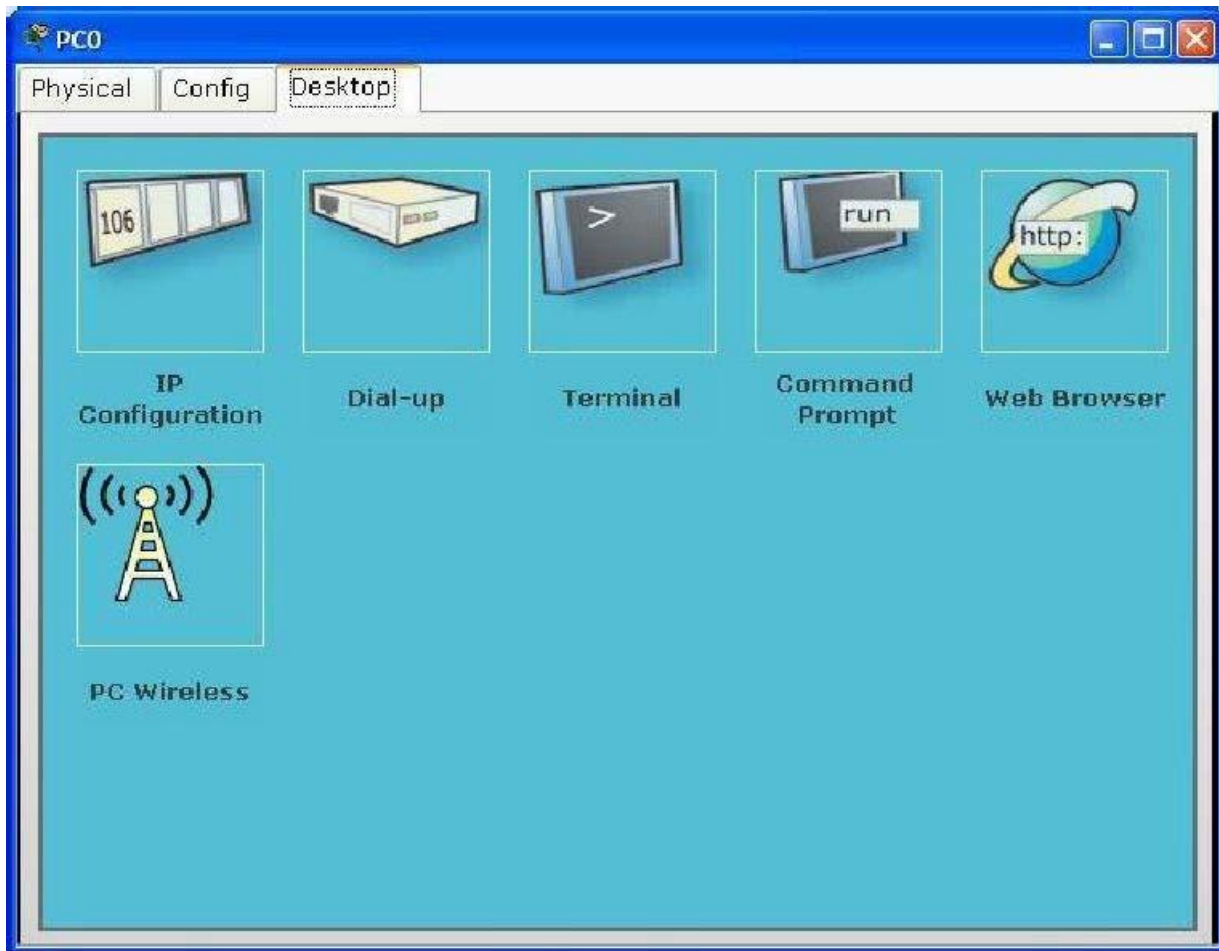


Paso 5: Después de realizar cada una de las conexiones, se deben configurar cada una de las direcciones IP según los criterios de diseño. Para ello, se selecciona el primer PC y se hace doble clic sobre él. Apareciendo el formulario que se ilustra en la siguiente figura, el cual corresponde a la apariencia física de un computador.



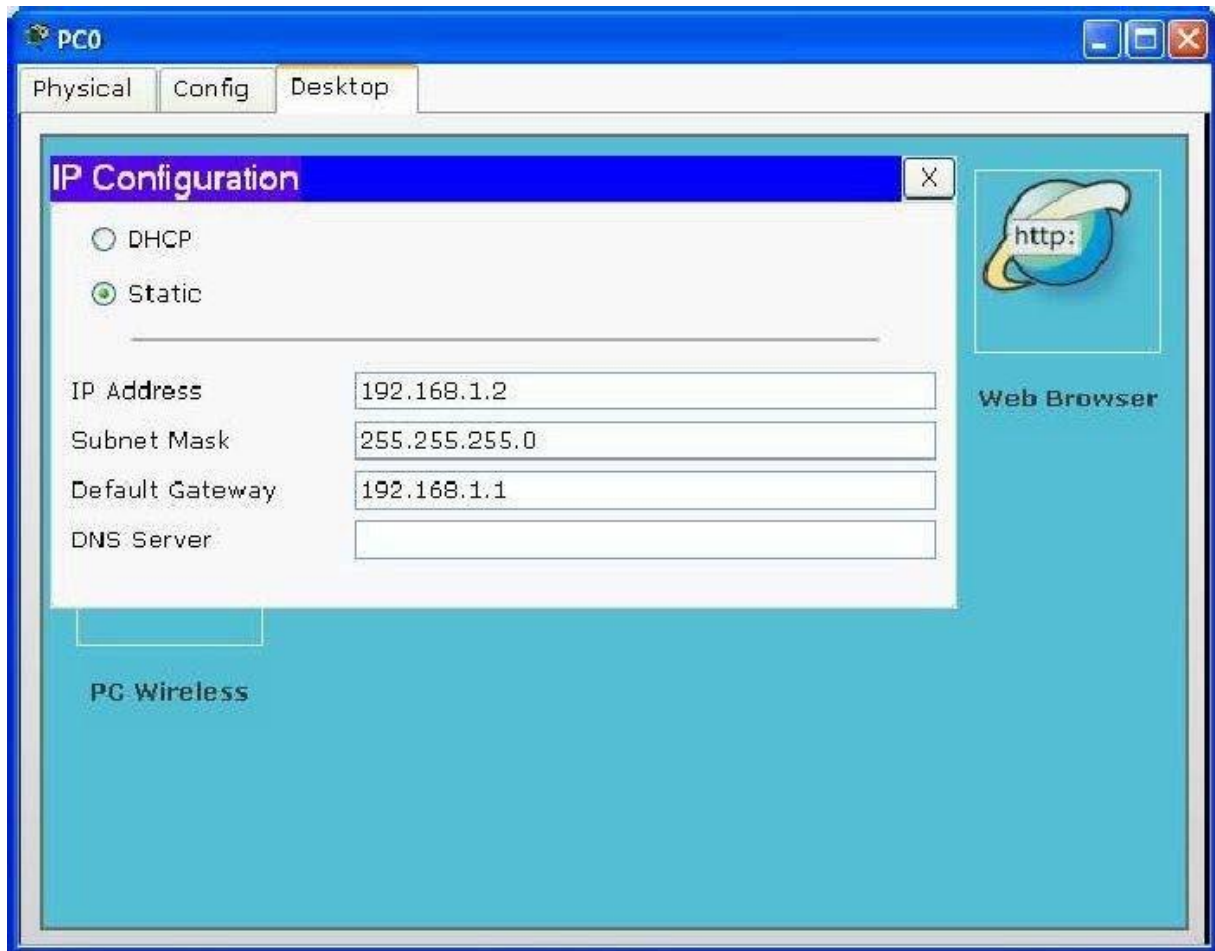
En la parte superior aparecen tres opciones, las cuales permiten realizar diversas funciones sobre el equipo en particular. La primera opción Physical, permite configurar parámetros físicos del PC, tales como la inclusión o exclusión de componentes hardware propios de red. La segunda opción Config, permite configurar parámetros globales tales como un direccionamiento estático o dinámico y la tercera opción Desktop, permite realizar operaciones de funcionamiento y configuración de la red tales como: Dirección IP, máscara de red, dirección de gateway, dirección DNS, ejecutar comandos como PING, TELNET, IPCONFIG, entre otras funciones.

Como en éste paso se requiere la configuración de los parámetros lógicos de red tales como la dirección IP, máscara de red y dirección Gateway se escoge la opción 3 (Desktop), en donde posteriormente se selecciona la opción IP Configuration tal como se ilustra en la figura.

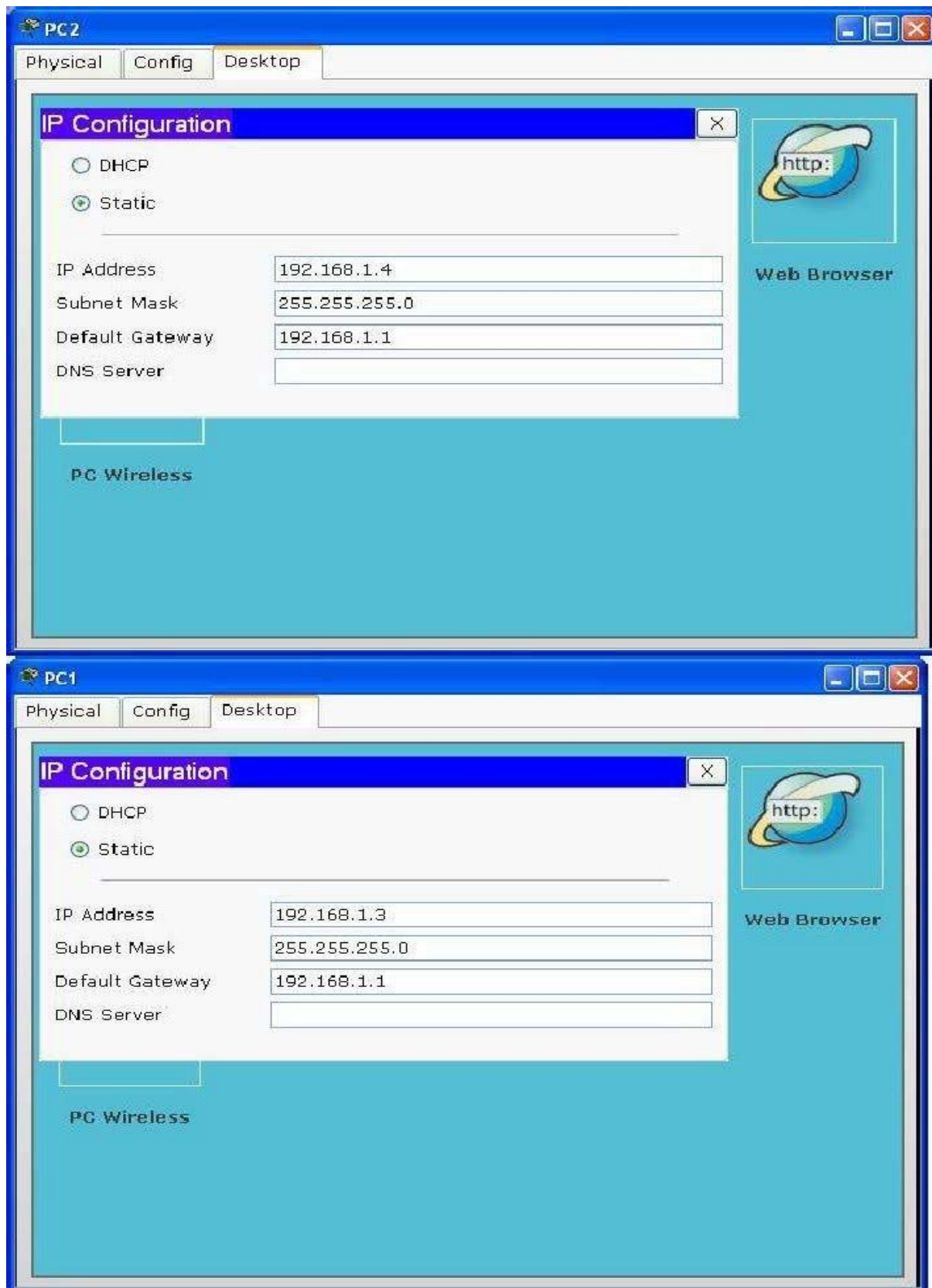


Allí se definen la dirección IP del computador, la cual corresponde a la dirección 192.168.1.2; se toma como máscara de subred la máscara por defecto para una clase C la cual corresponde al valor 255.255.255.0 y finalmente se define la dirección de gateway o puerta de enlace, ésta dirección corresponde a la dirección sobre la cual los computadores de la red tratarán de acceder cuando requieran establecer comunicación con otras redes a través de un dispositivo capa 3 (Router), la cual por criterios de diseño corresponde a la primera dirección IP de la red: 192.168.1.1

Adicionalmente, en éste caso se desea trabajar bajo el modelo de configuración IP estática y no bajo la alternativa del protocolo DHCP, el cual establece en forma automática la dirección IP a un host o computador de la red, acorde con la disponibilidad de direcciones IP existentes en la red a fin de optimizar su uso; ésta alternativa es muy utilizada en redes inalámbricas Wifi

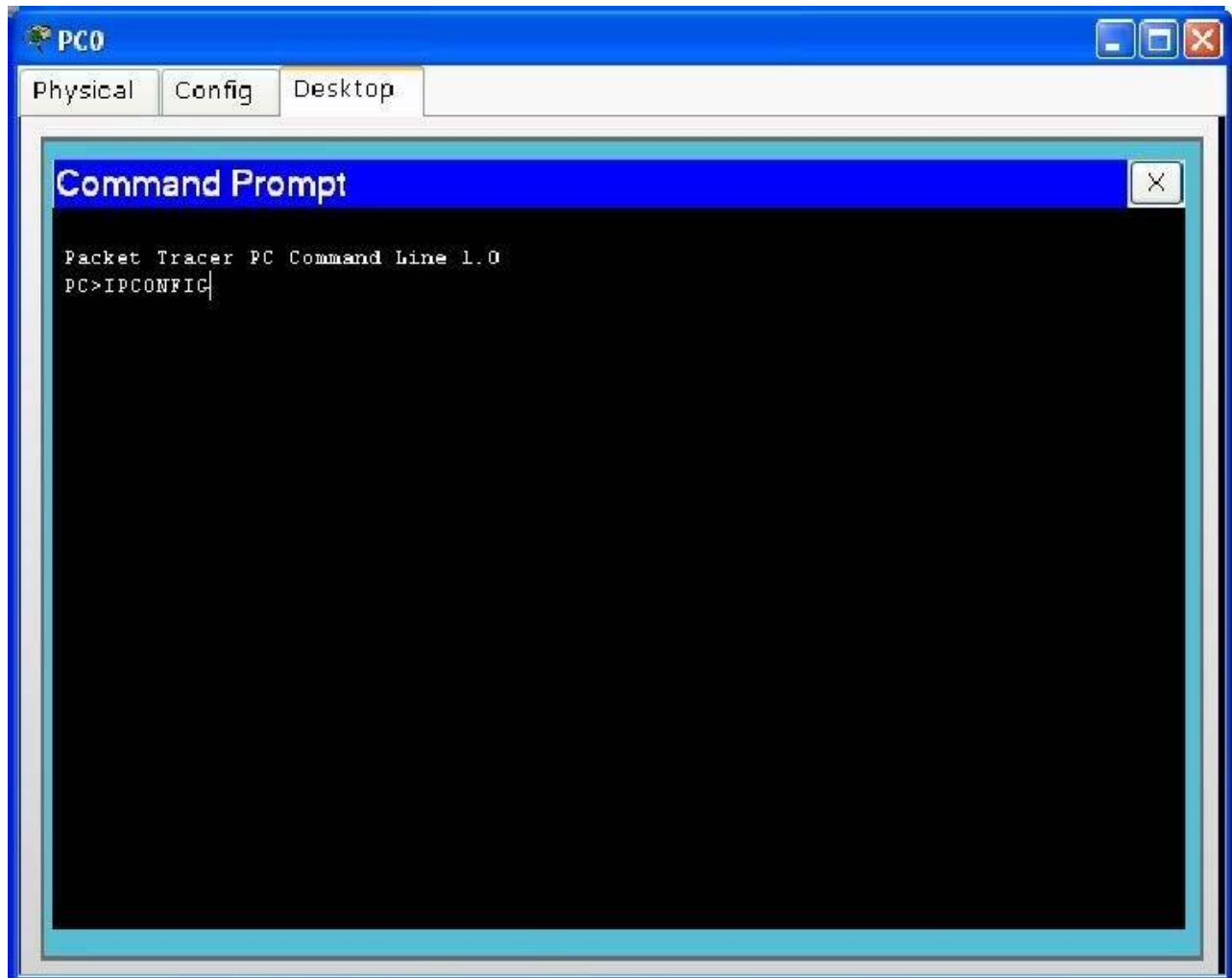


Este paso se repite para cada uno de los host o computadores que forman parte del diseño, teniendo en cuenta que en cada uno de ellos, el único parámetro que varía será la dirección IP; la máscara de subred y la dirección de gateway permanecen constantes debido a que todos los equipos pertenecen a la misma subred. En las dos figuras siguientes se muestra claramente esto.

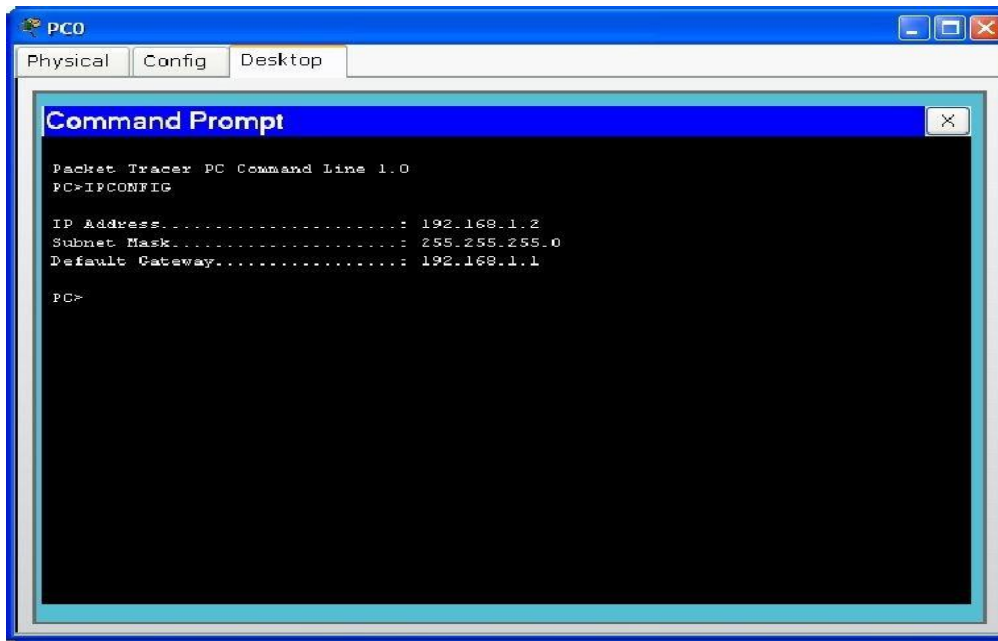




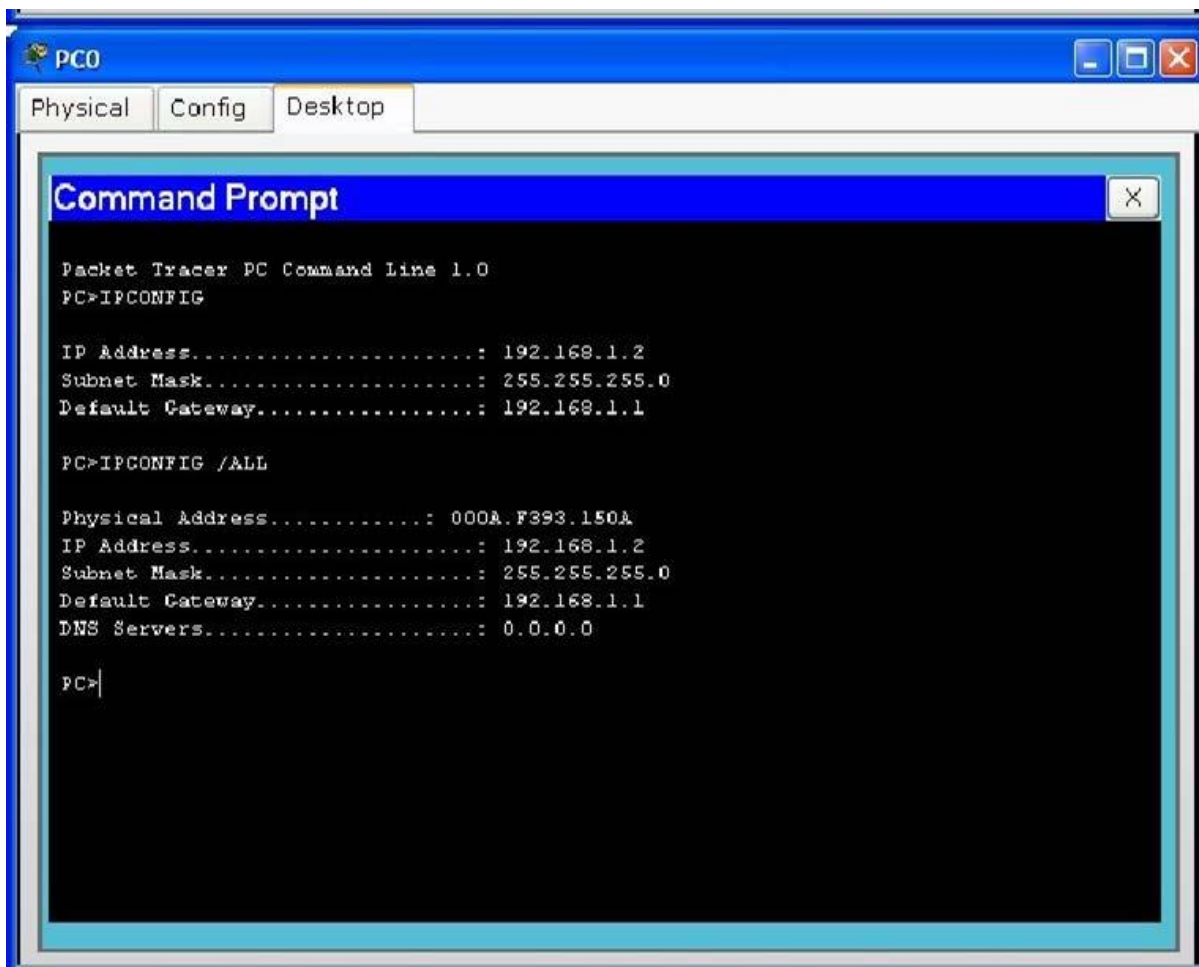
Paso 6: Si se desea verificar la configuración de un computador en particular, simplemente se selecciona el Host, se escoge la opción Desktop, seleccionamos la opción Command prompt, la cual visualiza un ambiente semejante al observado en el sistema operativo DOS. Allí escribimos IPCONFIG y pulsamos enter.



El resultado de ello se muestra claramente en la siguiente figura, en donde se identifican los parámetros del host correspondientes a la dirección IP, la máscara de Subred y la dirección de Gateway



Si el comando introducido es IPCONFIG/ALL, el resultado es el observado en la siguiente figura.

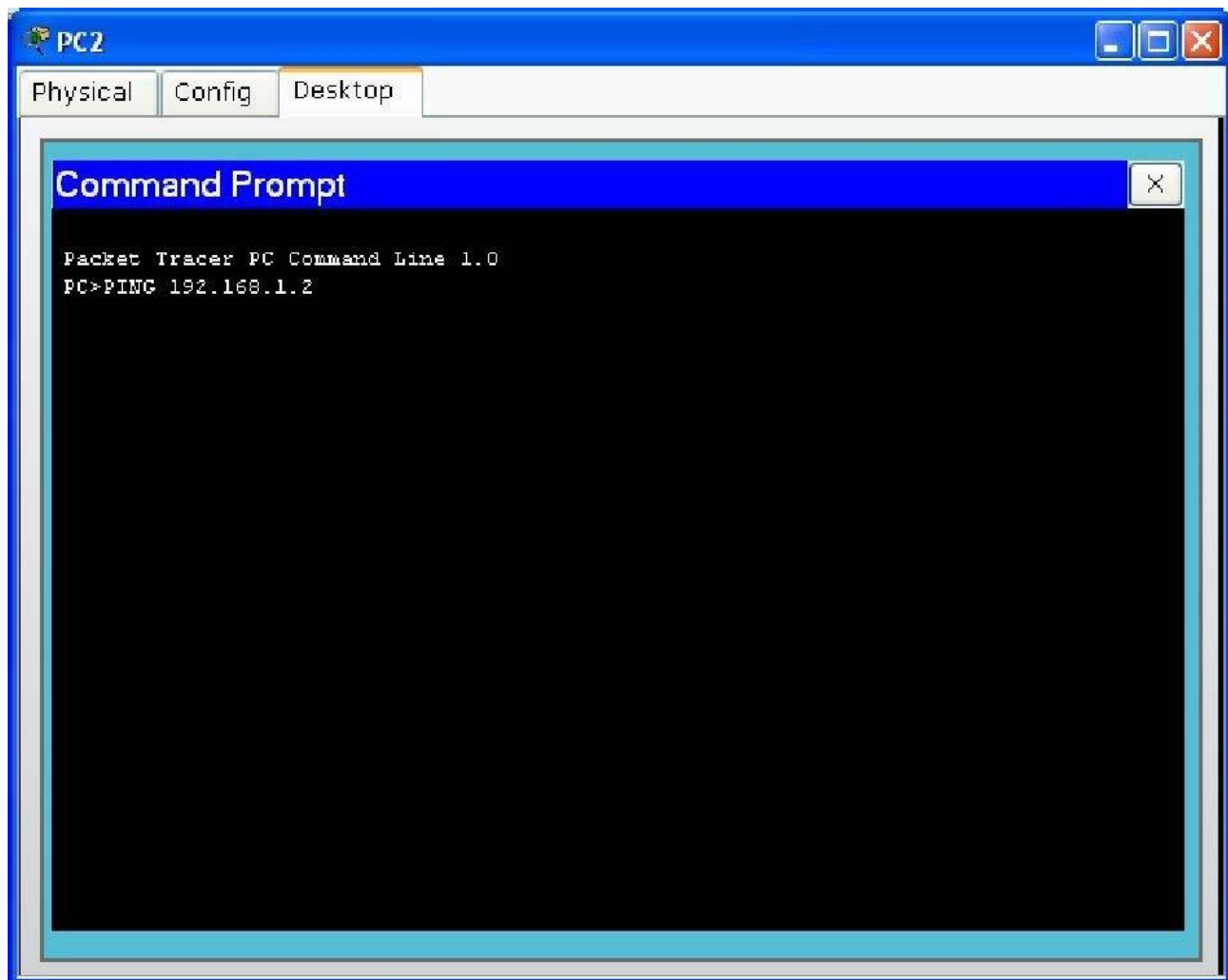






En donde se evidencia no solo los parámetros mencionados anteriormente, sino que además incluye la dirección física del equipo conocida como MAC y la dirección del servidor de dominio DNS.

Paso 7: Para verificar que existe una comunicación entre los diferentes equipos que hacen parte de la red, simplemente se selecciona uno de ellos; en éste caso en particular se seleccionó el PC2 con el fin de establecer comunicación con el equipo que posee la dirección IP 192.168.1.2.



Para ello se ejecuta el comando PING acompañado de la dirección IP sobre la cual se desea establecer comunicación tal como se indica en la figura anterior.

El resultado de ello se observa en la siguiente figura, en donde se constata claramente que se enviaron 4 paquetes de información y 4 paquetes fueron recibidos a satisfacción.



The screenshot shows a Packet Tracer PC Command Line window for a device named PC2. The window has three tabs: Physical, Config, and Desktop. The Desktop tab is active, displaying a black command prompt with white text. The text shows the execution of the 'ping 192.168.1.2' command, which returns four successful replies with varying times and a TTL of 128. Ping statistics are also displayed, showing 0% loss and an average round trip time of 107ms.

```
PC2
Physical Config Desktop
Command Prompt
Packet Tracer PC Command Line 1.0
PC>PING 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=182ms TTL=128
Reply from 192.168.1.2: bytes=32 time=72ms TTL=128
Reply from 192.168.1.2: bytes=32 time=83ms TTL=128
Reply from 192.168.1.2: bytes=32 time=94ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 72ms, Maximum = 182ms, Average = 107ms

PC>
```



## CONCLUSION:

Por medio de esta practica nos podemos dar a la idea de como hacer una red super sencilla con tal solo un dispositivo que funcione como un switch y unos cuantos cables de red conectados a este.

Además de otorgarle una IP a cada PC y que estas puedan tener comunicación entre ellas, esto nos ahorra tiempo ya que si se quiere hacer algo a las 3 PC, en vez de hacerlo 1 por 1 se hace la red y el trabajo se simplifica



## GLOSARIO

**AAA:** Abreviatura de Autenticación (Authentication), Autorización (Authorization) y Contabilidad (Accounting), sistema en redes IP para qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

**ACCOUNTING:** Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión.

**AD HOC:** Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso.

**AES:** También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bits desarrollado por los belgas Joan Daemen y Vincent Rijmen.

**ALGORITMO DE ENCRIPCIÓN:** Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales.

**ATAQUES A PASSWORDS:** Es un intento de obtener o descifrar una contraseña legítima de usuario.

**ATAQUE DE DICCIONARIO:** Método empleado para romper la seguridad de los sistemas basados en contraseñas en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático.

**ATAQUE DE FUERZA BRUTA:** Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas).

**AUDITORÍA:** Análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos.

**AUTENTICACIÓN:** Es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña.

**AUTORIZACIÓN:** Es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. **BRIDGE:** Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.

**CHAP** (Challenge Handshake Authentication Protocol): Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, lo cual lo hace un protocolo mucho más seguro que el PAP.

**CIFRADO:** Proceso para transformar la información escrita en texto simple a texto codificado.

**CIFRADO ASIMÉTRICO:** Cifrado que permite que la clave utilizada para cifrar sea diferente a la utilizada para descifrar.



**CIFRADO DE ARCHIVOS:** Transformación de los contenidos texto simple de un archivo a un formato ininteligible mediante algún sistema de cifrado.

**CLIENTE INALÁMBRICO:** Todo dispositivo susceptible de integrarse en una red inalámbrica como PDAs, portátiles, cámaras inalámbricas, impresoras.

**CLAVE DE CIFRADO:** Serie de números utilizados por un algoritmo de cifrado para transformar texto sin cifrar que se puede leer directamente en datos cifrados y viceversa.

**CONFIDENCIALIDAD:** Garantizar que la información sea asequible sólo a aquellas personas autorizadas a tener acceso a ella.

**CONTROL DE ACCESOS:** Se utiliza para restringir el acceso a determinadas áreas del computador, de la red, etc.

**EAP** - Protocolo de Autenticación Extensible (Extensible Authentication Protocol): Extensión del Protocolo Punto a Punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación.

**ESTÁNDAR:** Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos.

**FAST** (Flexible Authentication Secure Tunneling): Protocolo de seguridad WLAN del tipo EAP. Impide los denominados ataques de diccionario por fuerza bruta enviando una autenticación de contraseña entre el cliente WLAN y el punto de acceso inalámbrico a través de un túnel cifrado seguro. Elimina la necesidad de instalar servidores separados para tratar los certificados digitales empleados en otro sistema de seguridad WLAN (como el PEAP).

**HOT SPOT:** Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles) que proporciona servicios de red inalámbrica de banda ancha a visitantes móviles.

**IEEE:** Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización entre otras actividades, su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales

**INFRAESTRUCTURA:** Topología de una red inalámbrica que consta de dos elementos básicos: estaciones clientes inalámbricos y puntos de acceso. ISP: Proveedor de Servicios de Internet.

**LEAP** (Lightweight Extensible Authentication Protocol): Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección.

**MAC** - Dirección de Control de Acceso al Medio (Media Access Control Address): Dirección hardware de 6 bytes (48 bits) única que identifica cada tarjeta de una red y se representa en notación hexadecimal.



**MD5:** Algoritmo de cifrado de 128-bits del tipo EAP empleado para crear firmas digitales.

**802.11:** Familia de estándares desarrollados por la IEEE para tecnologías de red inalámbricas.

**802.11a:** Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz.

**802.11b:** Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 11 Mbps en una banda de 2.4 GHz. Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. No es compatible con el 802.11a pues funciona en otra banda de frecuencia. 802.11e: Estándar destinado a mejorar la calidad de servicio en Wi-Fi. Es de suma importancia para la transmisión de voz y video.

**802.11g:** Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz. Una de sus ventajas es la compatibilidad con el estándar 802.11b. 802.11i: Estándar de seguridad para redes Wi-Fi aprobado a mediados de 2004. En el se define al protocolo de encriptación WPA2 basado en el algoritmo AES.

**802.11n:** Estándar para conseguir mayores velocidades de transmisión para Wi-Fi. Estas serán superiores a 100 Mbps.

**802.16:** Estándar de transmisión inalámbrica conocido como WIMAX. Es compatible con Wi-Fi. La tecnología permite alcanzar velocidades de transmisión de hasta 70 Mbits en una banda de frecuencias entre 10 GHz y 66 GHz.

**802.16d:** Estándar de transmisión inalámbrica WIMAX que suministra una velocidad de entre 300 Kbps y 2 Mbps en una banda de frecuencia de 2GHz a 11GHz. Se utiliza para el cubrimiento de la "primer milla".

**802.1x:** Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

**PAP** - Protocolo de Autenticación de Contraseñas(Password Authentication Protocol): El método más básico de autenticación, en el cual el nombre de usuario y la contraseña se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión.

**PEAP** (Protected Extensible Authentication Protocol): Protocolo del tipo EAP para la transmisión de datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red Wi-Fi empleando sólo certificados del lado servidor creando un túnel SSL/TLS cifrado entre el cliente y el servidor de autenticación.

**PKI** - Infraestructura de Clave Pública: Sistema de certificados digitales, Autoridades Certificadoras y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet.

**PUNTO DE ACCESO (AP):** Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles tanto para centralización como para enrutamiento.





**RADIUS** (Remote Authentication Dial-In User Service): Sistema de autenticación y contabilidad empleado por la mayoría de proveedores de servicios de Internet (ISPs).

**RAS** - Servidor de Acceso Remoto: Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta.

**ROUTER**: Es un conmutador de paquetes que opera en el nivel de red del modelo OSI, proporciona un control del tráfico y funciones de filtrado; está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP.

**ROAMING**: En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad

**SERVIDOR DE AUTENTICACIÓN (AS)**: Servidor que gestiona las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos.

**SISTEMA DE CIFRADO**: Colección completa de algoritmos que tienen su propia denominación en función de las claves que utilizan para cifrar.

**SNIFFERS**: Programa y/o dispositivo que monitorea la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información.

**SSID**: Identificador de red inalámbrica, similar al nombre de la red pero a nivel Wi-Fi.

**TKIP** - Protocolo de Integridad de Clave Temporal: Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

**VLAN** - Red de Área Local Virtual: Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares.

**WAN** – Red de Área Amplia: Tipo de red compuesta por dos o más redes de área local (LANs).

**WARCHALKING**: Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

**WARDRIVING**: Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar puntos de acceso inalámbrico.

**WARSPAMMING**: Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.

**WEP** – Privacidad Equivalente a Cableado: Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se



transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del Vector de inicialización IV), de 128 bits (104 bits más 24 bits del vector de inicialización IV). Wi-Fi (Wireless Fidelity): Es el nombre comercial con el cual se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.

**WIMAX** - Interoperabilidad Mundial para Acceso por Microondas: Es un estándar de transmisión inalámbrica de datos (802.MAN) proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa entre el punto transmisor y el receptor.

**WPA** - Acceso Protegido Wi-Fi: Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado).

**WPA2** – Protocolo de Aplicación Inalámbrica: Protocolo de seguridad para redes Wi-Fi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Puntos de Acceso de última generación.