

Uso del Packet Tracer y Aplicaciones Resueltas

***Victor Andres Ochoa Correa
Ing. de Sistemas***

INTRODUCCIÓN

En este módulo se brinda una introducción general y conceptual sobre diferentes temáticas aplicadas a problemas que se desarrollarán a lo largo del presente módulo. Muchas descripciones serán cualitativas y otras cuantitativas ya que los detalles y aplicaciones propios a la ingeniería así lo exigen para facilitar el proceso de enseñanza-aprendizaje.

El factor clave del presente módulo consiste en el estudio de las Telecomunicaciones y sus aplicaciones principalmente orientadas hacia el uso de herramientas software.

Uno de los principales propósitos de los centros de formación superior es proporcionar una buena formación a sus estudiantes. En esa formación, indudablemente el componente práctico juega un papel imprescindible. Es a través de ella en donde el estudiante reforzará los conceptos teóricos y adquirirá procedimientos fundamentales del área de conocimiento que esté estudiando.

Se puede definir un programa de simulación como un conjunto de instrucciones (software) que se ejecuta sobre un computador (hardware) con el fin de imitar (de manera más o menos realista) el comportamiento de un sistema físico (máquina, proceso, etc.).

Se han realizado diversas experiencias sobre el uso de simuladores y su influencia en el aprendizaje de los estudiantes. La metodología basada en la realización de trabajos de investigación con ayuda de los simuladores, propicia la evolución de las creencias científicas del estudiante hacia un planteamiento más próximo al pensamiento científico

La incorporación del computador en el aula, fundamentada pedagógicamente, no solo supone una mejora en el proceso educativo, sino que se adapta eficazmente a un enfoque constructivista del proceso de enseñanza-aprendizaje

Los simuladores son considerados "herramientas cognitivas", ya que aprovechan la capacidad de control del computador para amplificar, extender o enriquecer la cognición humana. Estas aplicaciones informáticas pueden activar destrezas y estrategias relativas al aprendizaje, que a su vez el estudiante puede usar para la adquisición autorregulada de otras destrezas o de nuevo conocimiento.

Dentro de las principales ventajas que ofrece el uso de simuladores en los procesos de enseñanza, se pueden mencionar:

- ❖ Ofrecen una forma más accesible a los estudiantes de trabajar con diversos equipos, procesos y procedimientos
- ❖ Involucran al estudiante en su aprendizaje, ya que es él el que tendrá que manejar el simulador, observar los resultados y actuar en consecuencia
- ❖ Es una herramienta motivadora
- ❖ Coloca al estudiante ante situaciones próximas a la realidad
- ❖ Se pueden trabajar situaciones difíciles de encontrar en la realidad
- ❖ Al tratarse de un entorno simulado, el estudiante no está expuesto a situaciones peligrosas directamente
- ❖ Supone una forma económica de trabajar con máquinas, procedimientos y procesos actuales y en algunos casos punteros, difícilmente asequibles en la realidad

En los últimos años el desarrollo de los sistemas informáticos ha sido vertiginoso, de manera que hoy día podemos encontrar computadores en

prácticamente todos los ámbitos de la vida cotidiana: en los bancos para la realización de operaciones financieras; en la oficina para procesamiento de textos, consulta de bases de datos y gestión de recursos; en las universidades para la enseñanza y las tareas investigadoras; en la industria para el control de plantas, monitorización de procesos productivos, gestión integrada de las diferentes etapas de fabricación, control de máquinas herramienta, robots y manipuladores, etc.

En el transcurso del módulo se plantearán diferentes situaciones que permitan al estudiante comprender fácilmente cada uno de los temas a tratar y la forma de interacción de cada uno de ellos, aplicado hacia el uso de la tecnología bajo herramientas software de simulación, adquisición de información y medición de parámetros propios del área de las telecomunicaciones.

PACKET TRACER COMO HERRAMIENTA DE SIMULACION

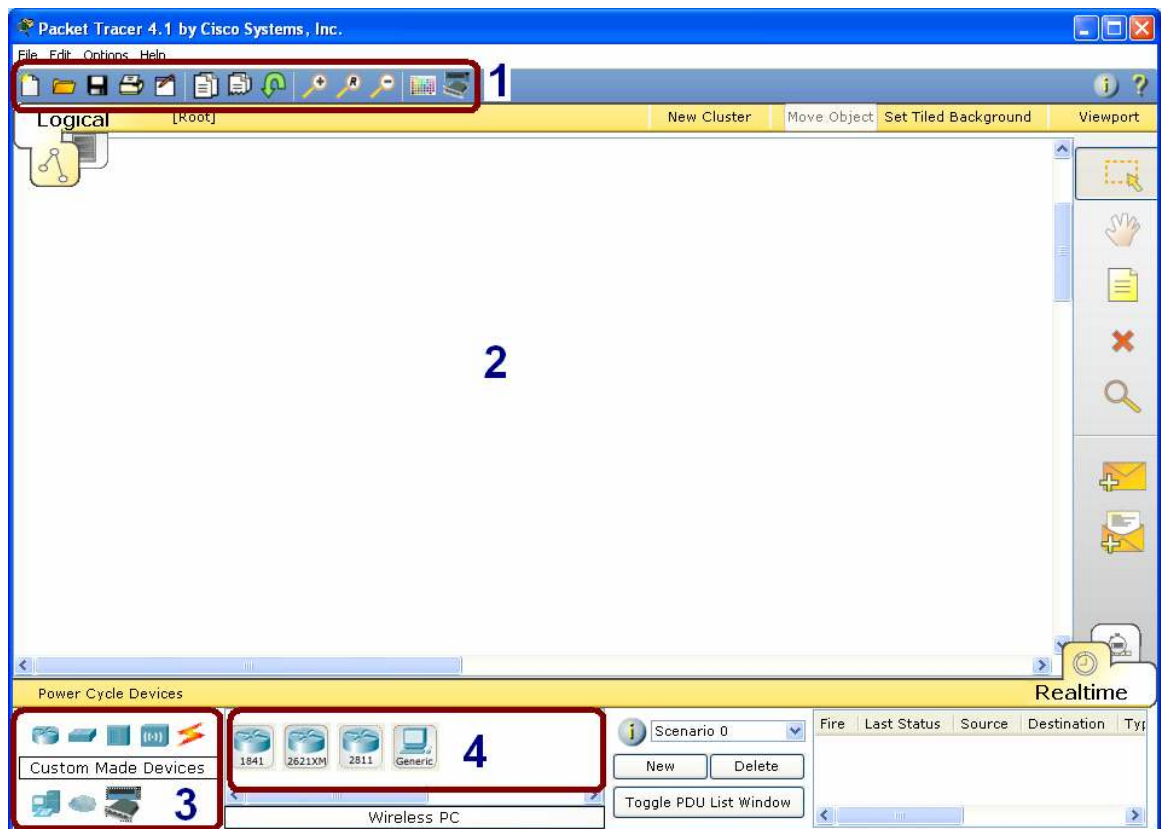
Una de las herramientas más utilizadas en el mundo orientadas a la simulación de redes de datos es Packet Tracer, el cual consiste en un simulador gráfico de redes desarrollado y utilizado por Cisco como herramienta de entrenamiento para obtener la certificación CCNA. Packet Tracer, es un simulador de 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 cuál es 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



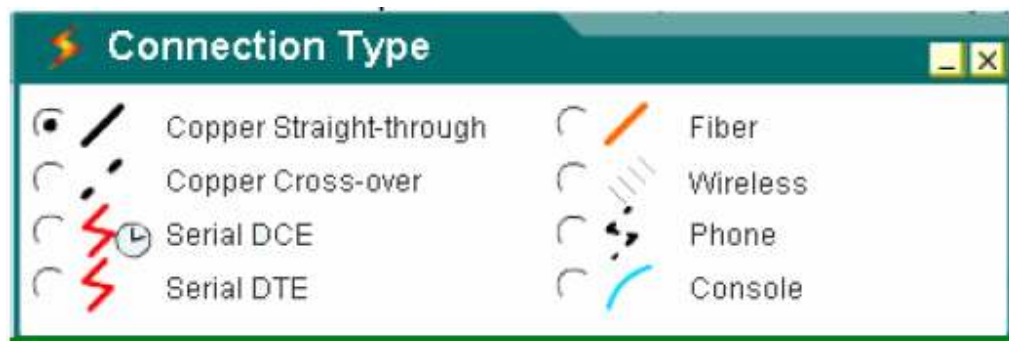
Switches: Series 2950, 2960, Genérico, Bridge



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

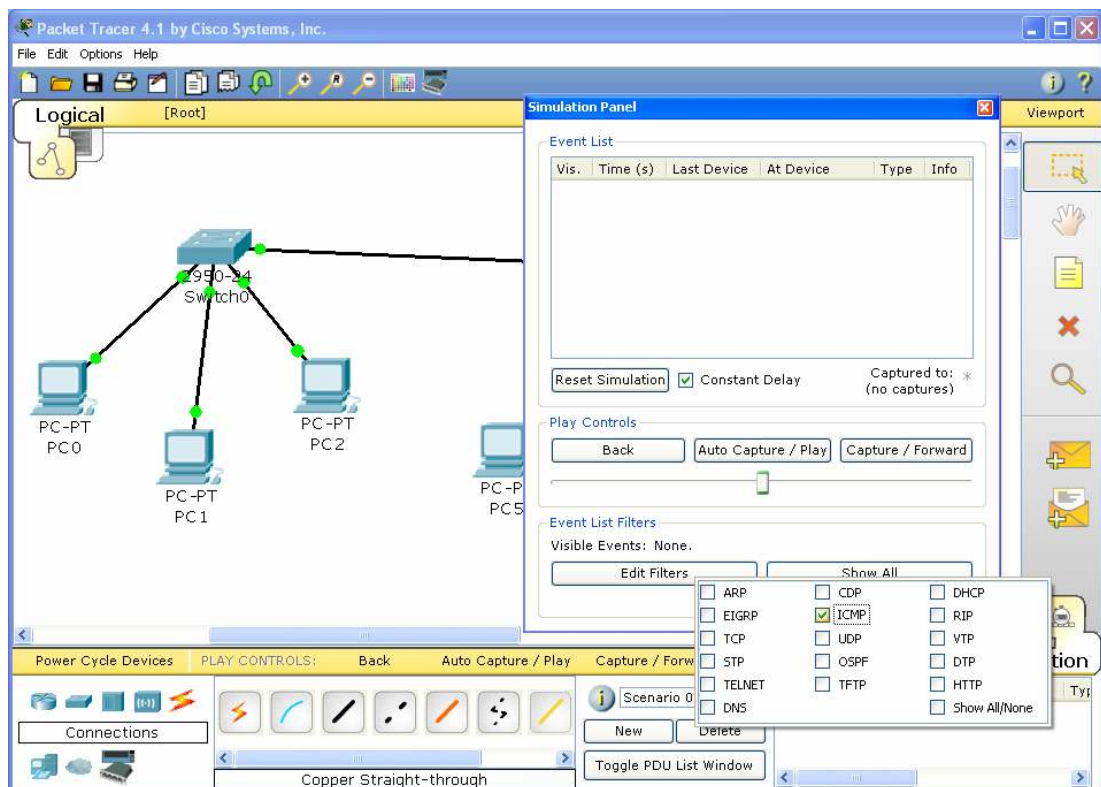


La herramienta está diseñada para orientar al estudiante en su manipulación adecuada. Dentro del modo de operación topology, existe una herramienta que permite hacer de forma automática, las conexiones entre los dispositivos de la red, ésta opción se activa cuando se selecciona el Simple Mode (modo simple) y esta selección hace que el programa sea el que elija 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.

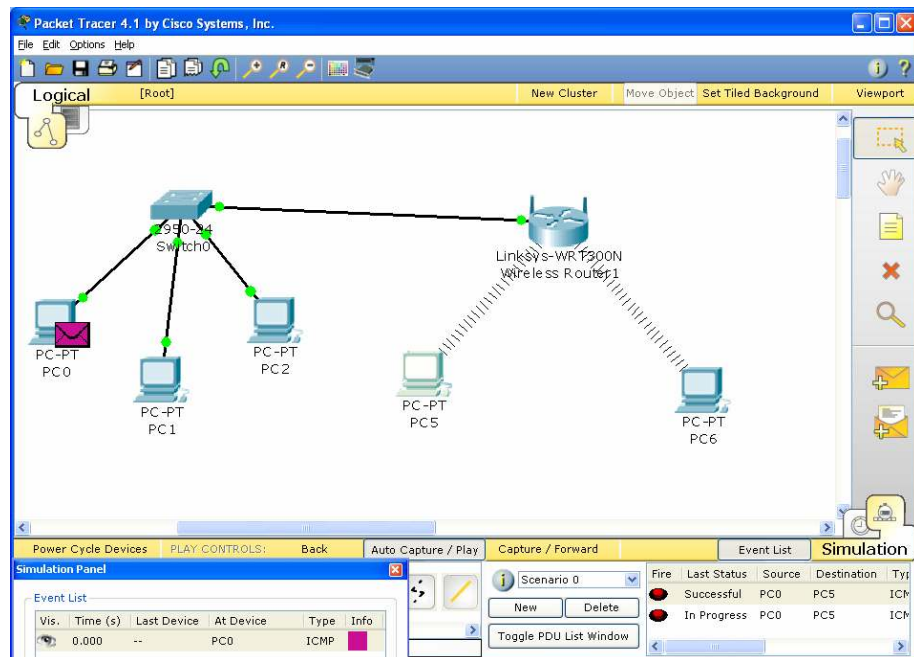
Adicionalmente, se recomienda que en las primeras experiencias con el programa, se debe trabajar y configurar manualmente los dispositivos y enlaces, es decir con el Simple Mode inactivo; debido a que es así como realmente interactuará el usuario con cada una de las conexiones a la hora de realizar un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

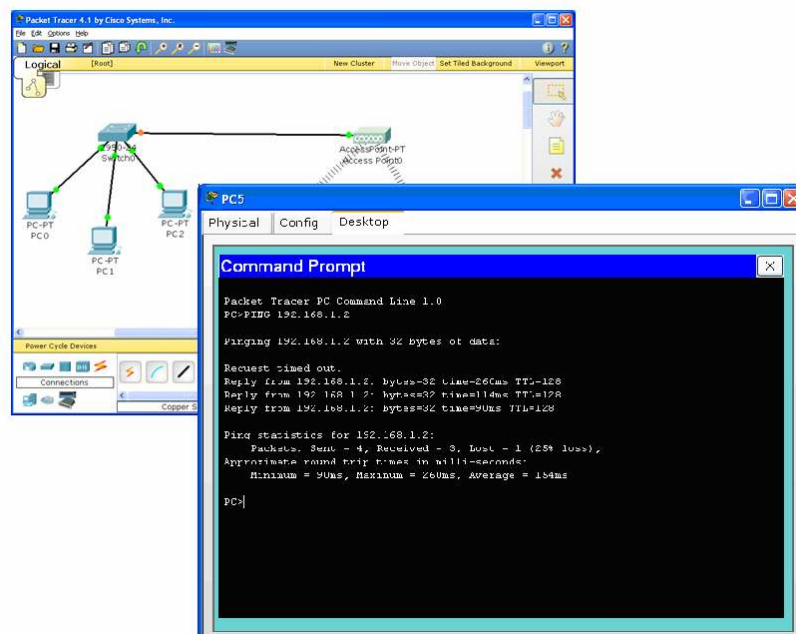


Dentro de este modo de operación se visualiza el proceso de transmisión y recepción de información haciendo uso de un panel de herramientas que contiene los controles para poner en marcha la simulación.

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 hosts a otro(s) en la red.



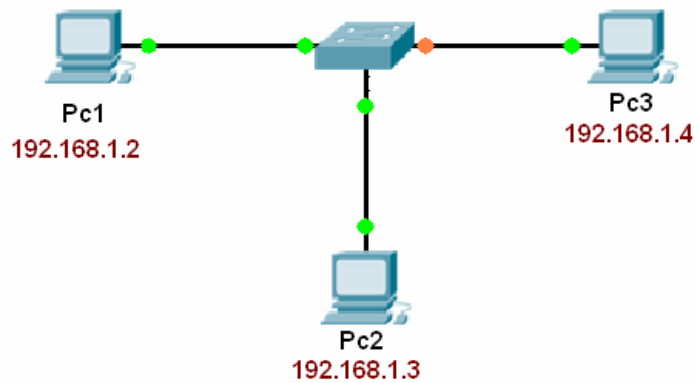
Dentro del modo Realtime, se encuentra el cuadro de registro Ping log, en donde se muestran los mensajes SNMP que han sido enviados y se detalla además el resultado de dicho proceso; con base en este resultado se puede establecer cuál o cuales de los terminales de la red están inactivos, a causa de un 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:

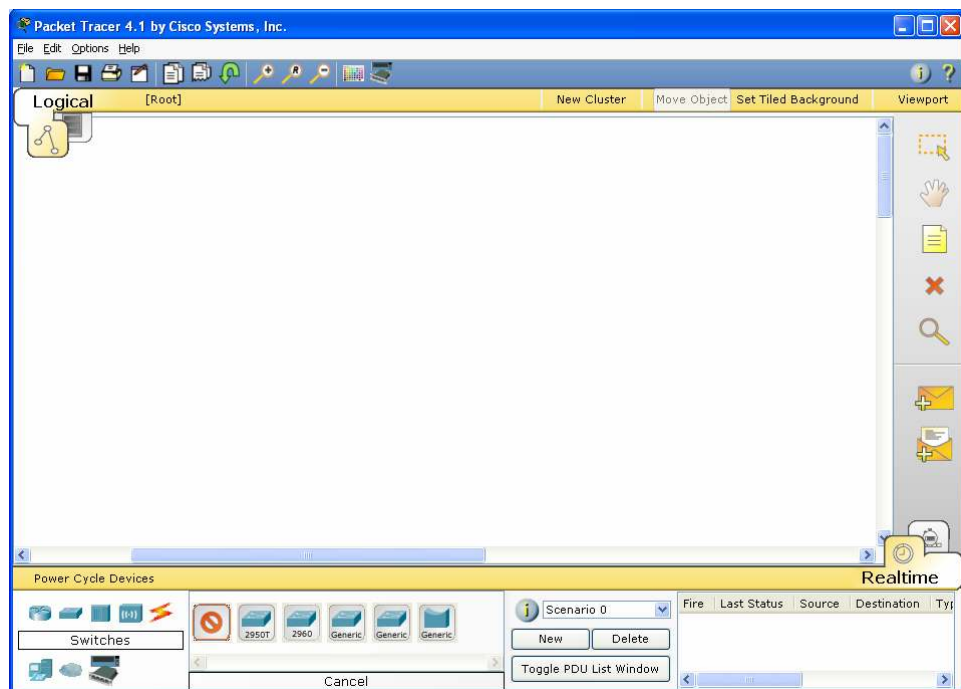
Ventajas	Desventajas
El enfoque pedagógico de este simulador, hace que sea una herramienta muy útil como complemento de los fundamentos teóricos sobre redes de comunicaciones.	Es un software propietario, y por ende se debe pagar una licencia para instalarlo.
El programa posee una interfaz de usuario 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.

Primera aplicación

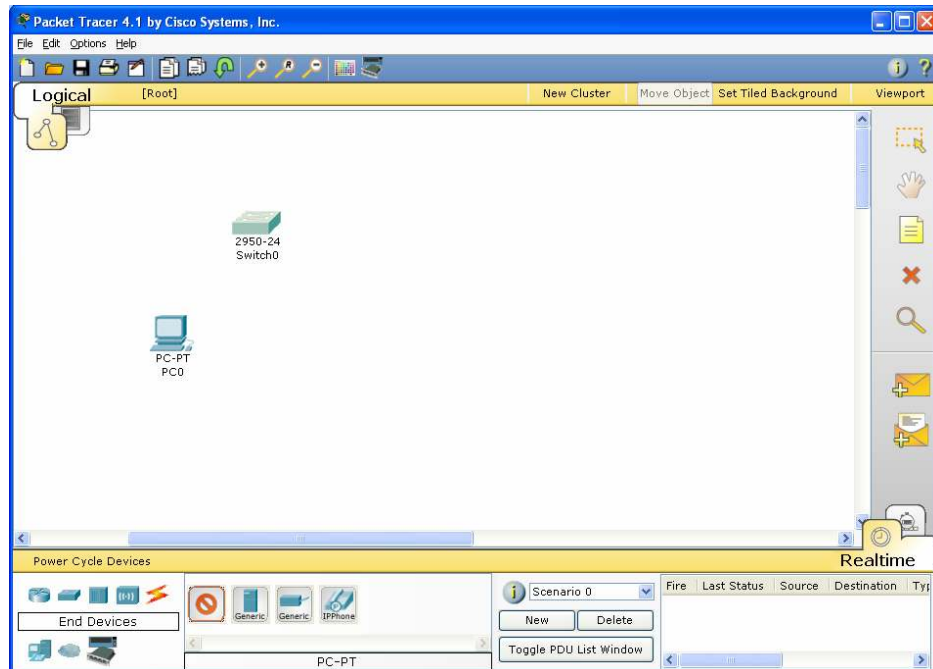
Utilizando la herramienta de simulación PACKET TRACER, se desea implementar la siguiente estructura de red.



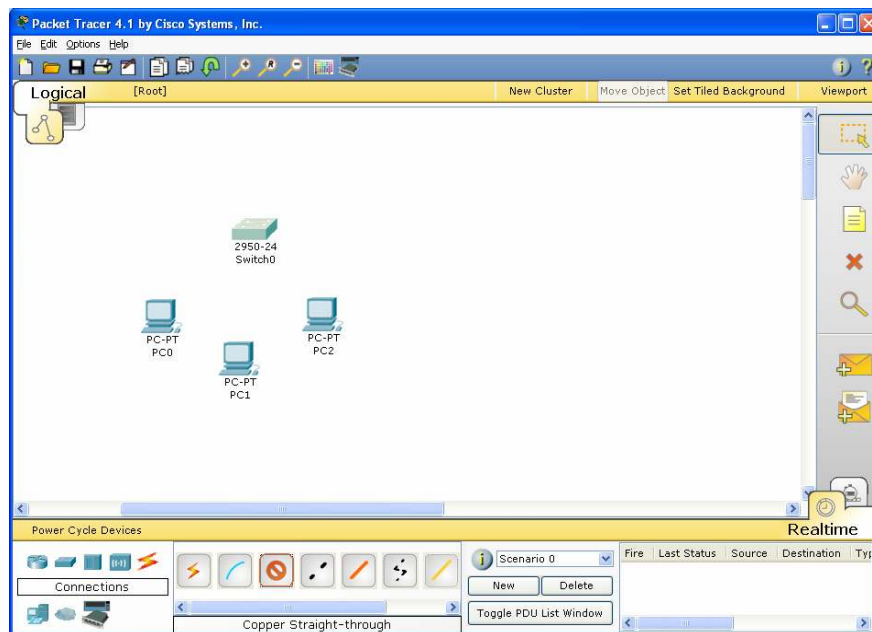
Paso 1: Ingresar a la herramienta Packet Tracer y seleccionar la referencia de Switch 2950-24 el cual se encuentra en el menú Switches, tal como se ilustra en la figura



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



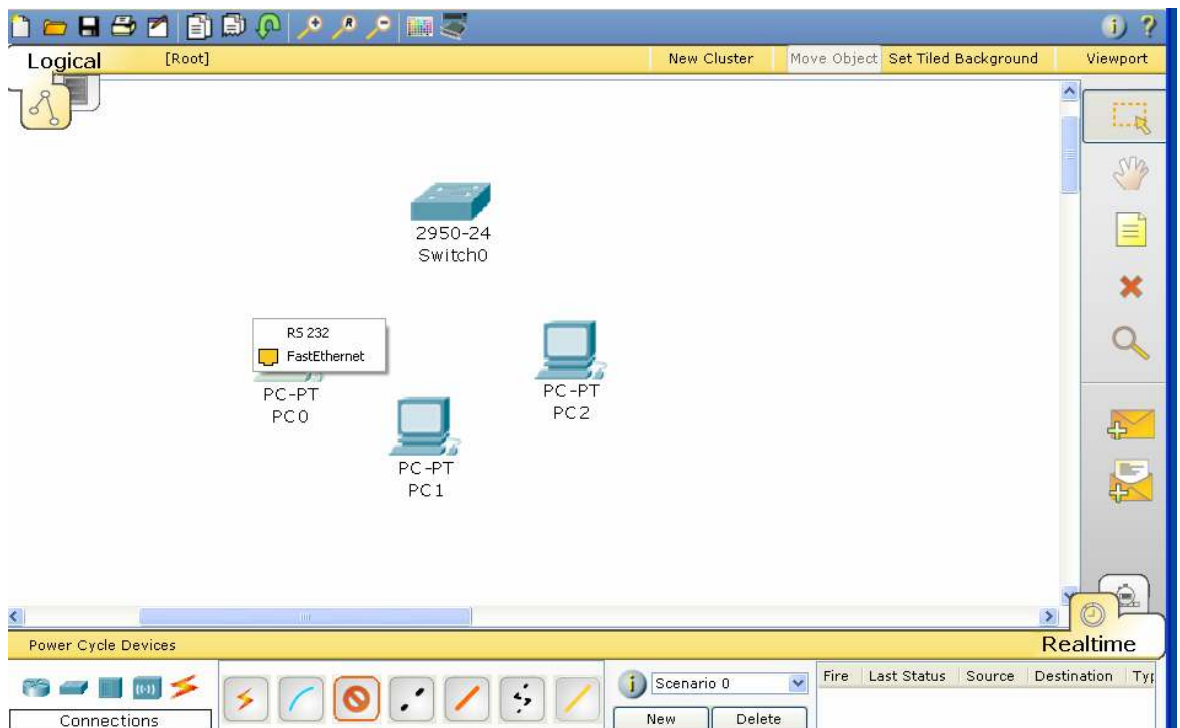
Repetir el paso anterior dos veces, completando con ello los tres Pcs requeridos en el esquema



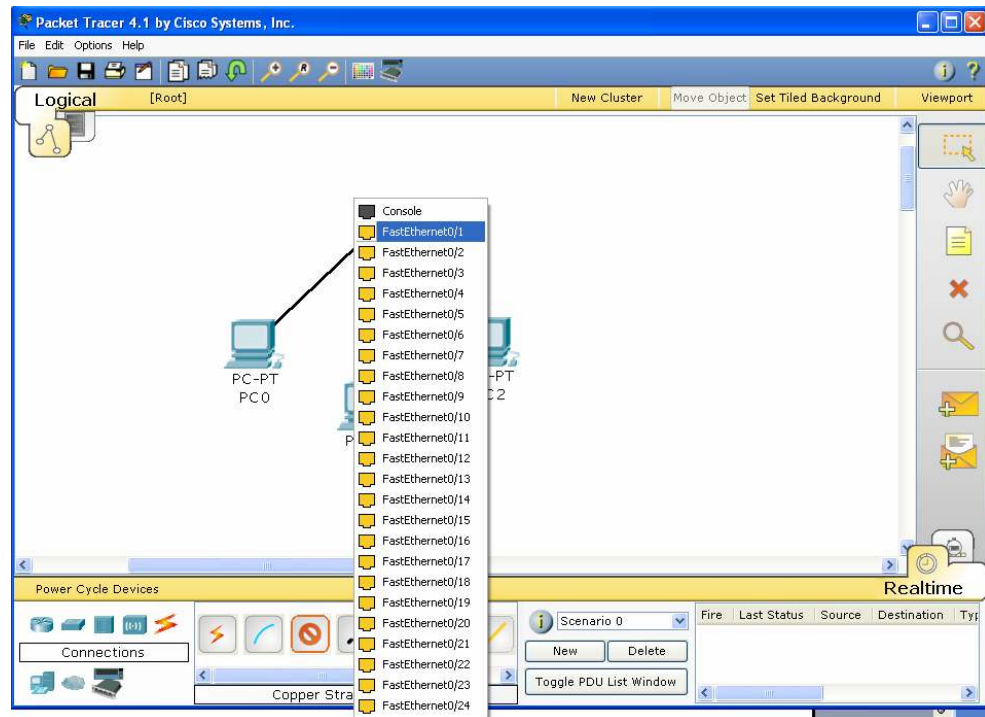
Paso 3:

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.

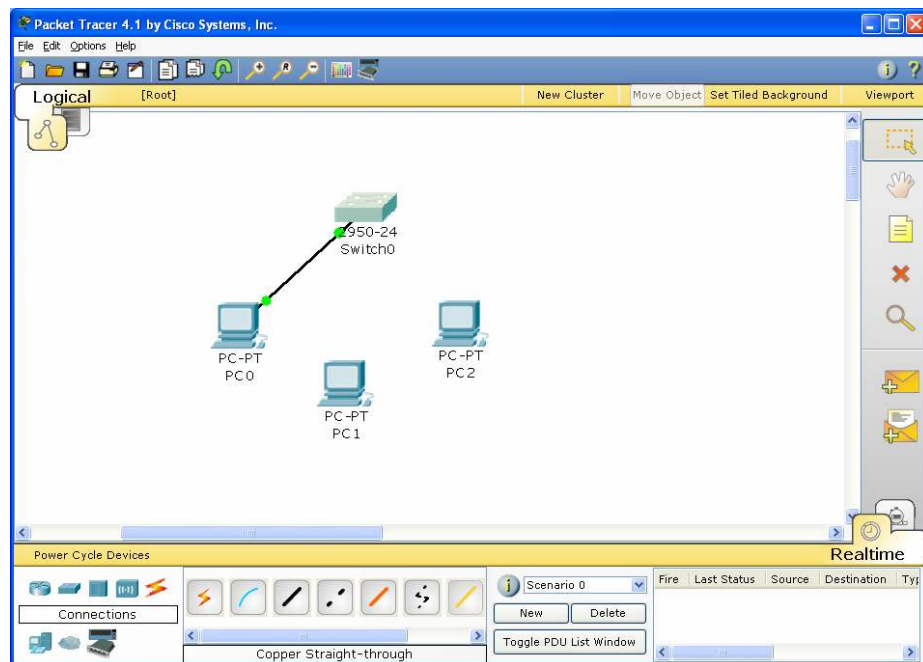
Hecho esto, se debe seleccionar el primer PC, hacer click con el botón derecho del Mouse y escoger la opción Fastethernet, indicando con ello que se desea establecer una conexión a través de la tarjeta de red del equipo.

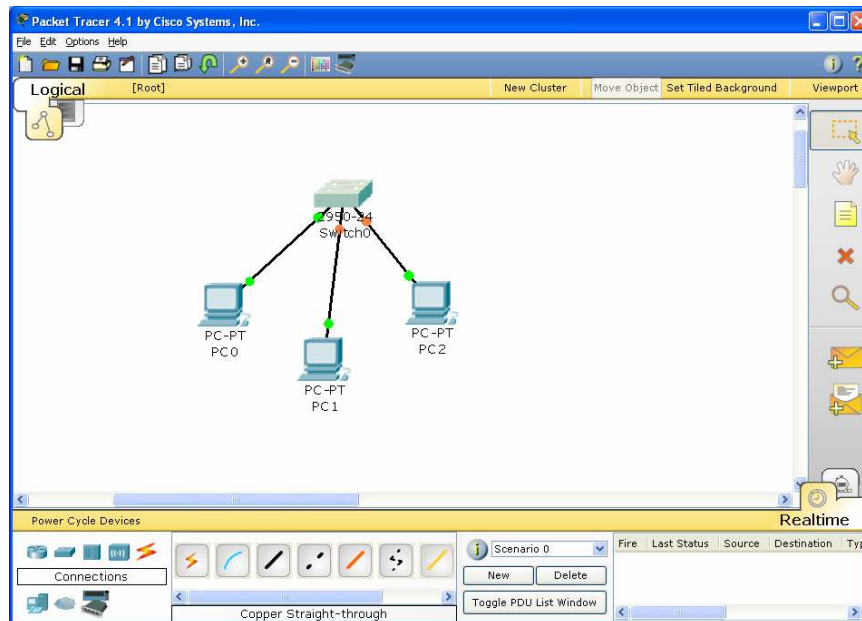


Paso 4: Después de seleccionar la opción Fastethernet en el primer Pc, arrastrar el Mouse hasta el Switch, hacer clic sobre él y seleccionar el puerto sobre el cual se desea conectar el Pc1, en nuestro caso corresponde al puerto Fastethernet 0/1.

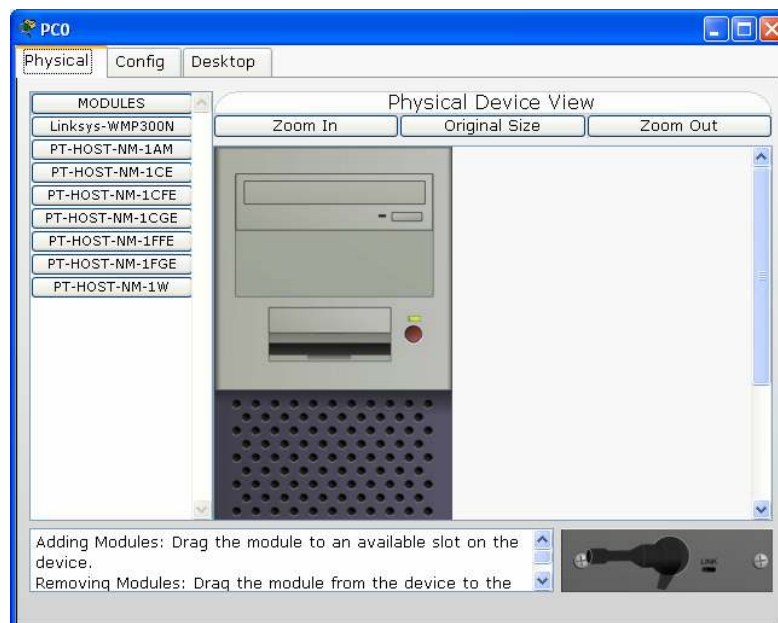


El resultado de lo anterior se refleja en la siguiente figura, lo cual se debe repetir con cada uno de los Pcs que hacen parte del diseño.



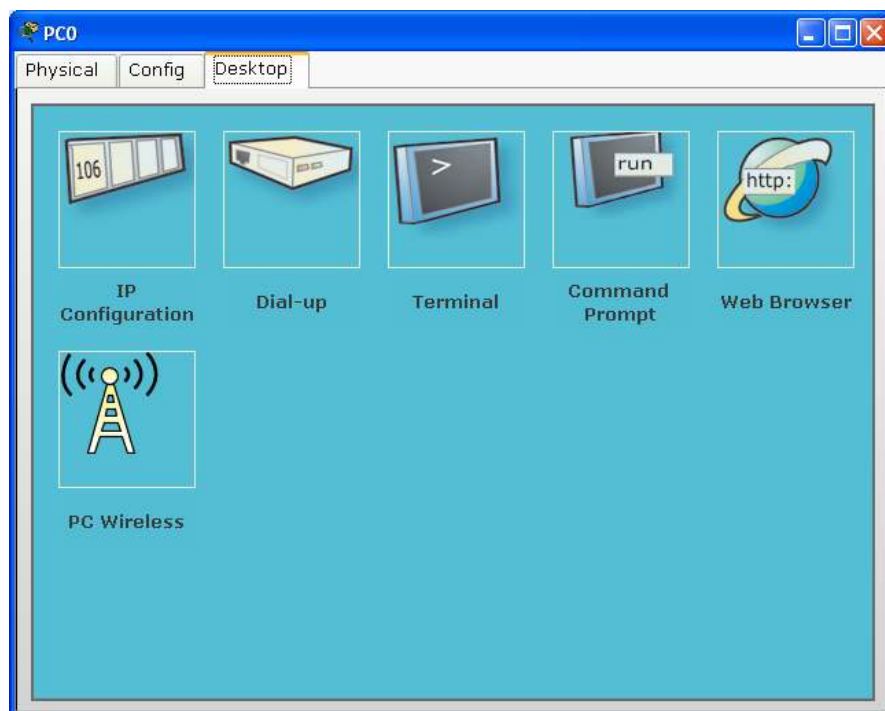


Paso 5: Después de realizar cada una de las conexiones, se deben configurar cada una de las direcciones IP según los criterios de diseño. Para ello, se selecciona el primer PC y se hace doble clic sobre él. Apareciendo el formulario que se ilustra en la siguiente figura, el cual corresponde a la apariencia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



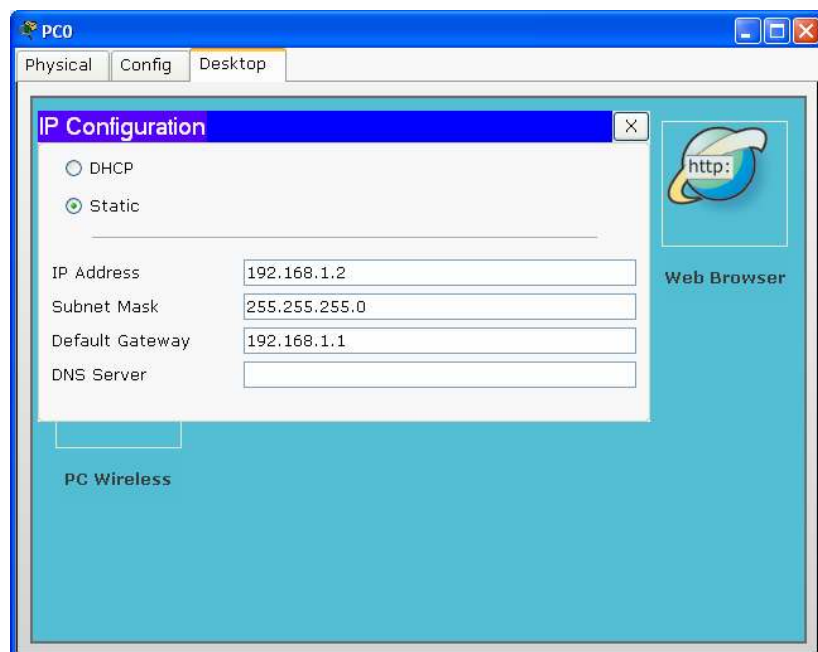
En la parte superior aparecen tres opciones, las cuales permiten realizar diversas funciones sobre el equipo en particular. La primera opción **Physical**, permite configurar parámetros físicos del PC, tales como la inclusión o exclusión de componentes hardware propios de red. La segunda opción **Config**, 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 más

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.



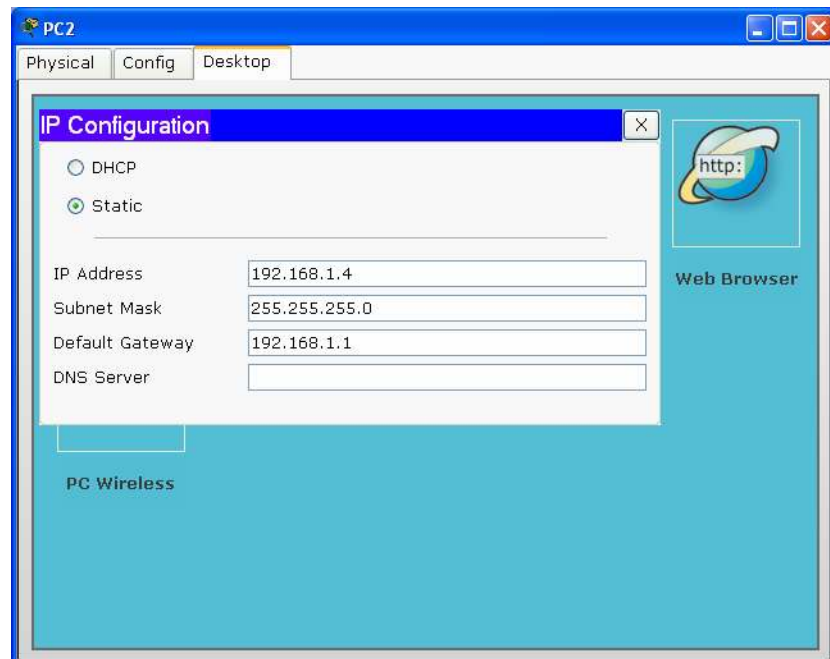
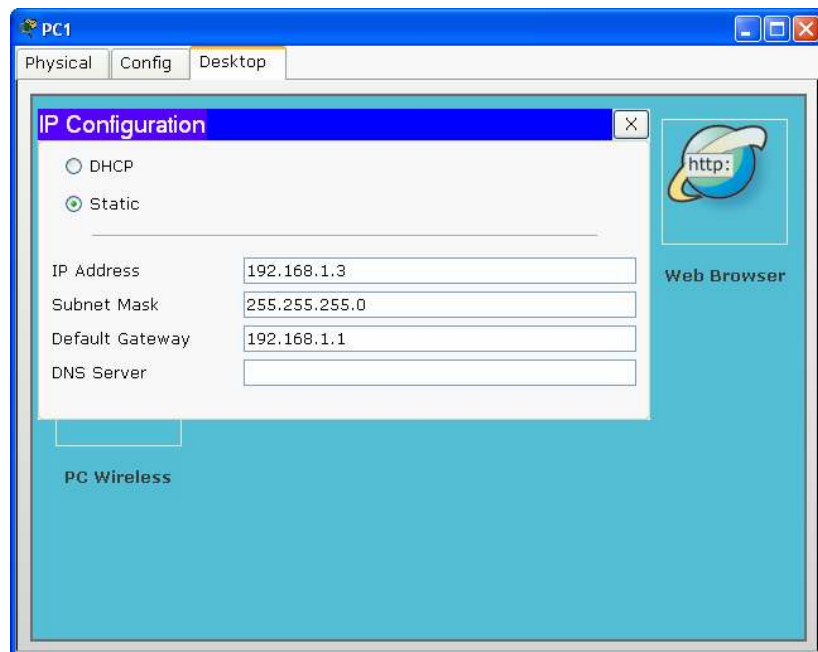
Allí se definen la dirección IP del computador, la cual corresponde a la dirección 192.168.1.2; se toma como máscara de subred la máscara por defecto para una clase C la cual corresponde al valor 255.255.255.0 y finalmente se define la dirección de gateway o puerta de enlace, ésta dirección corresponde 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



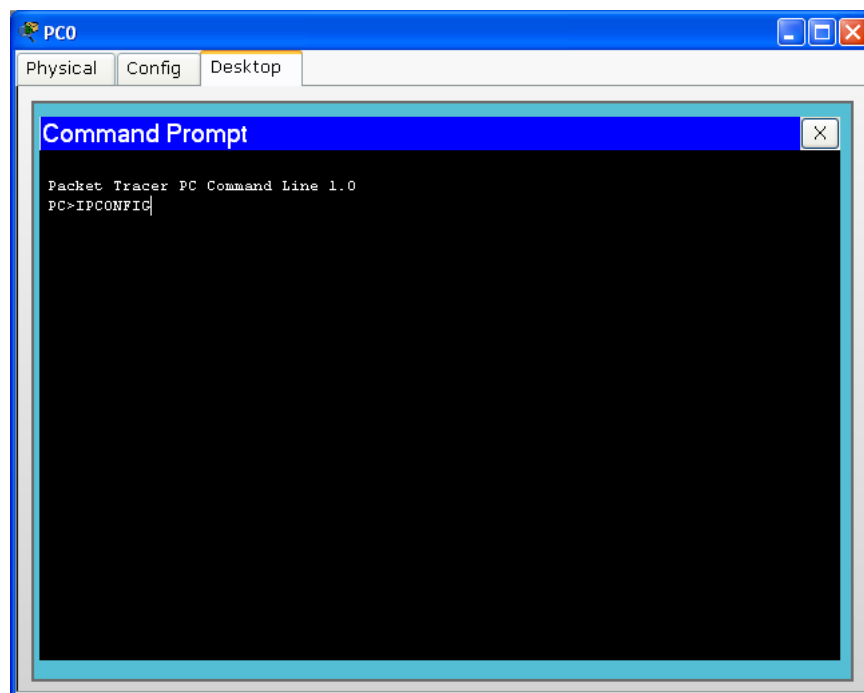
Este paso se repite para cada uno de los host o computadores que hacen parte del diseño, teniendo en cuenta que en cada uno de ellos, el único parámetro

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 evidencia claramente esto.

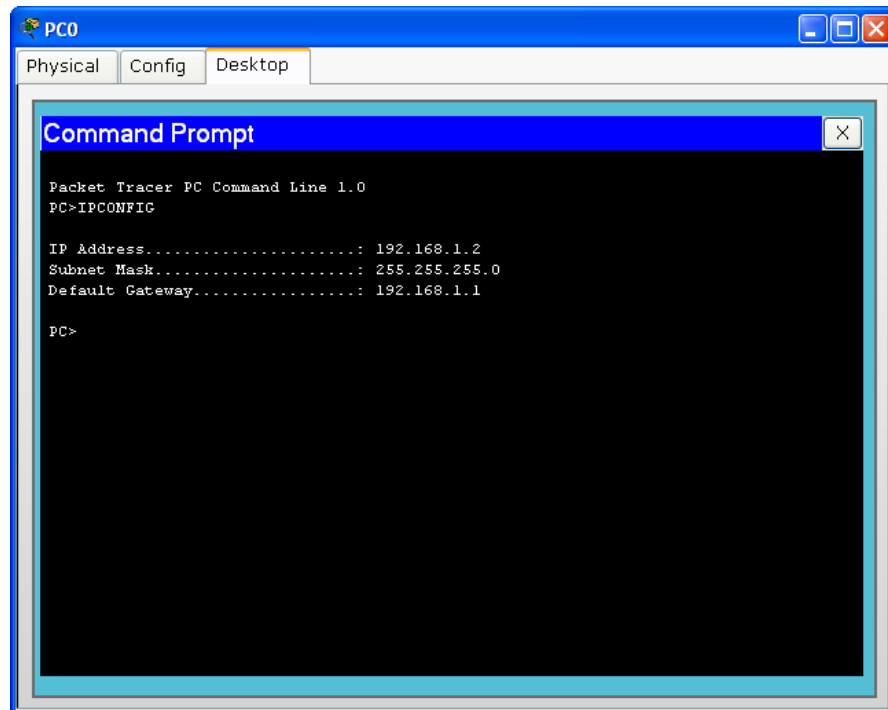


Paso 6:

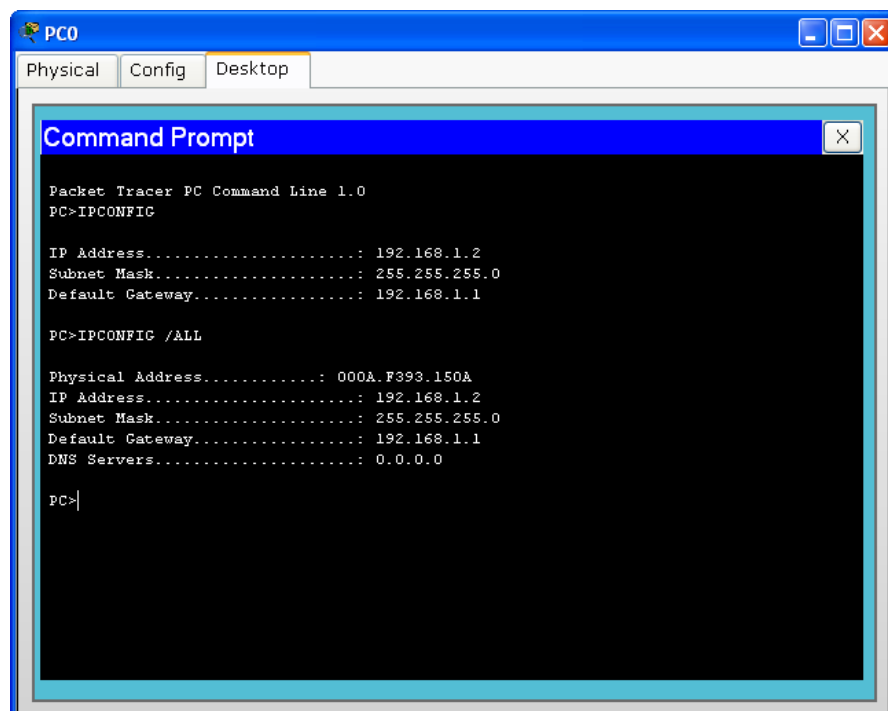
Si se desea verificar la configuración de un computador en particular, simplemente se selecciona el Host, se escoge la opción Desktop, seleccionamos la opción **Command prompt**, la cual visualiza un ambiente semejante al observado en el sistema operativo DOS. Allí escribimos IPCONFIG y pulsamos enter.



El resultado de ello se visualiza 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

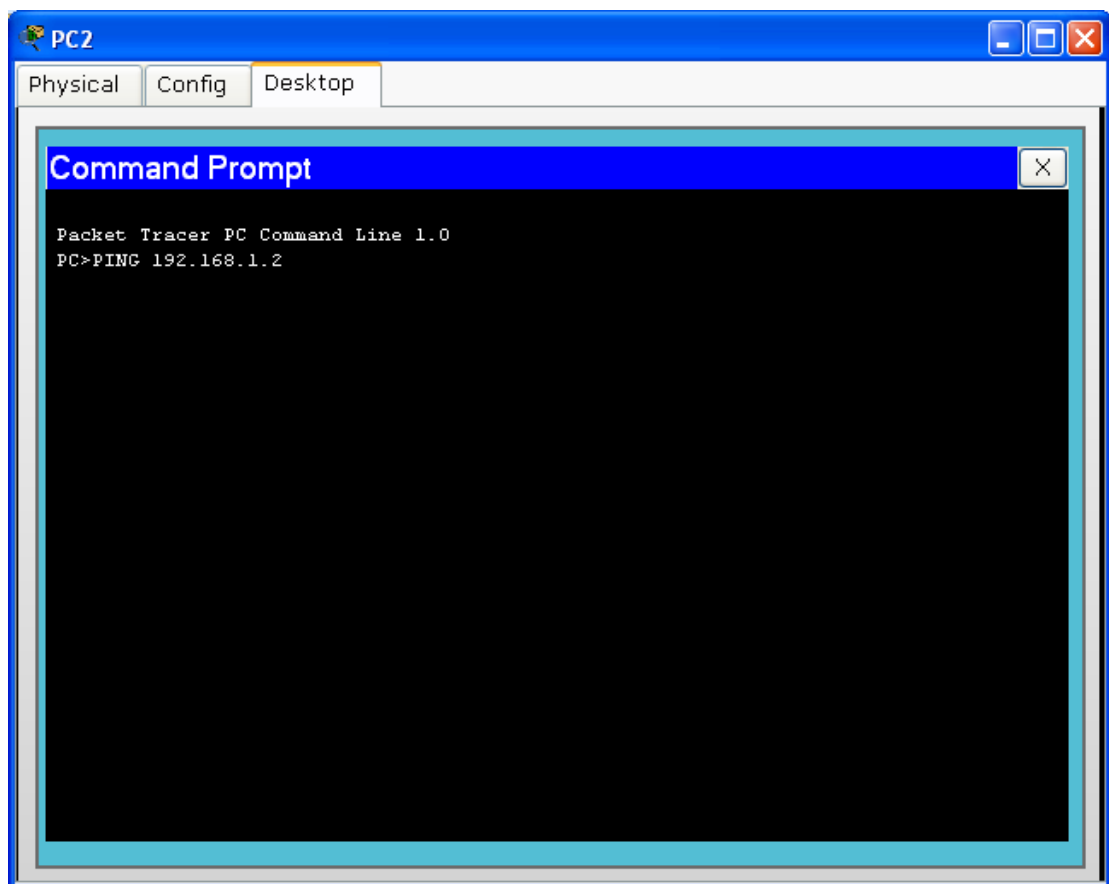


Si el comando introducido es IPCONFIG/ALL, el resultado es el observado en la siguiente figura.



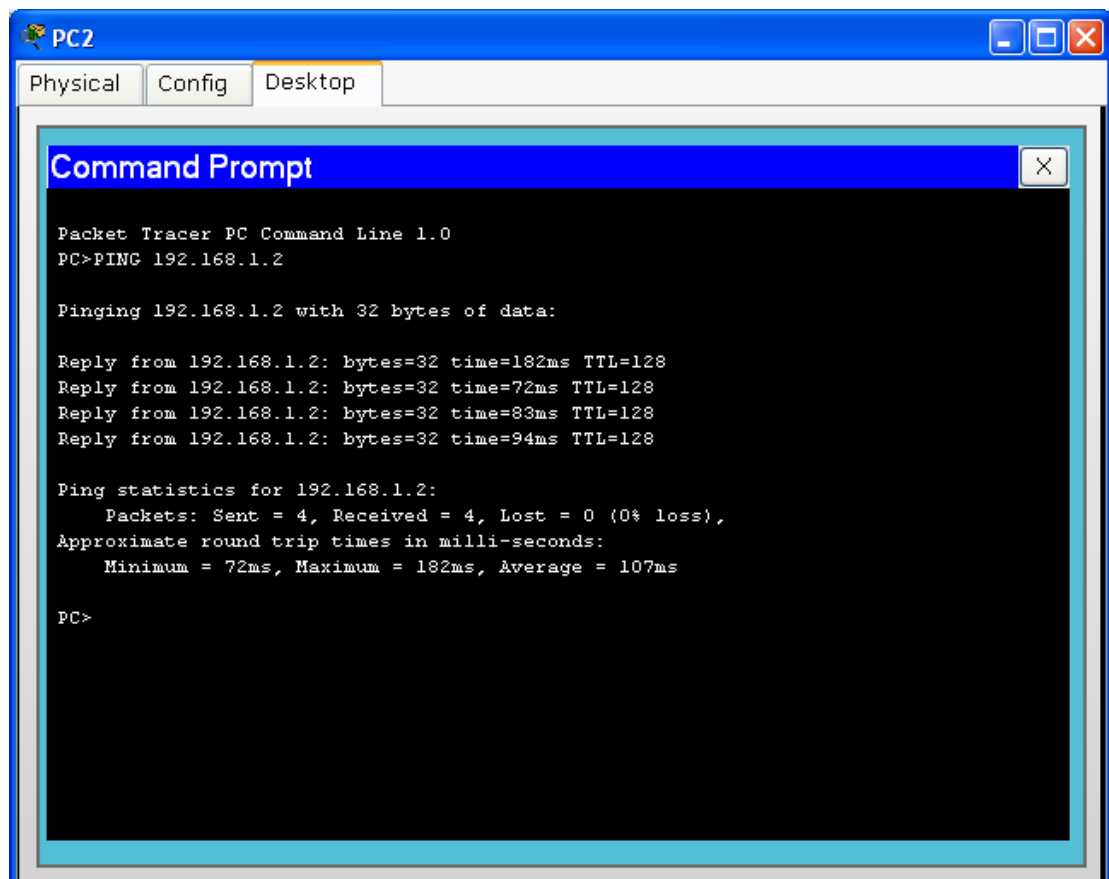
En donde se evidencia no solo los parámetros mencionados anteriormente, sino que además incluye la dirección física del equipo conocida como MAC y la dirección del servidor de dominio DNS.

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 image shows a screenshot of a Packet Tracer PC Command Prompt window. The window has a blue title bar with the text 'PC2' and standard window controls. Below the title bar are three tabs: 'Physical', 'Config', and 'Desktop', with 'Desktop' being the active tab. The main area of the window is a black terminal with white text. The text shows the execution of a 'PING' command to the IP address 192.168.1.2. It displays four successful replies with varying round-trip times (72ms, 182ms, 83ms, and 94ms) and a TTL of 128. Finally, it shows the ping statistics: 4 packets sent, 4 received, 0% loss, with an average round-trip time of 107ms.

```
Packet Tracer PC Command Line 1.0
PC>PING 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

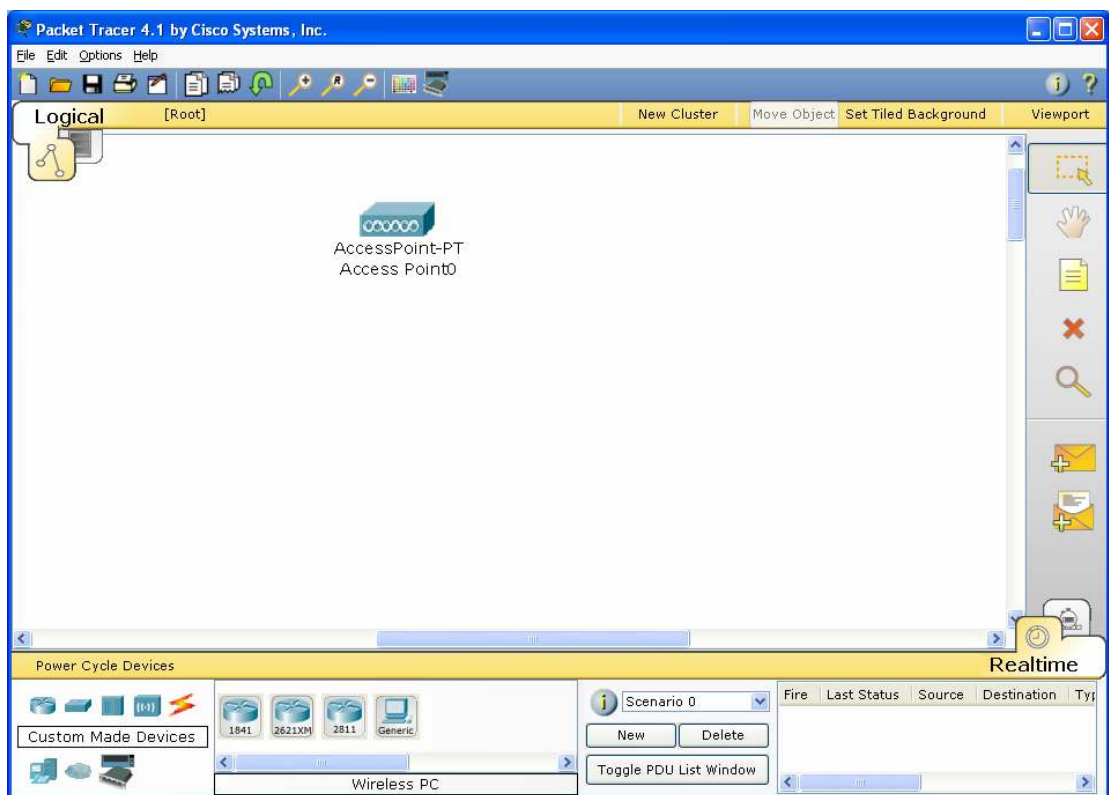
Reply from 192.168.1.2: bytes=32 time=182ms TTL=128
Reply from 192.168.1.2: bytes=32 time=72ms TTL=128
Reply from 192.168.1.2: bytes=32 time=83ms TTL=128
Reply from 192.168.1.2: bytes=32 time=94ms TTL=128

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

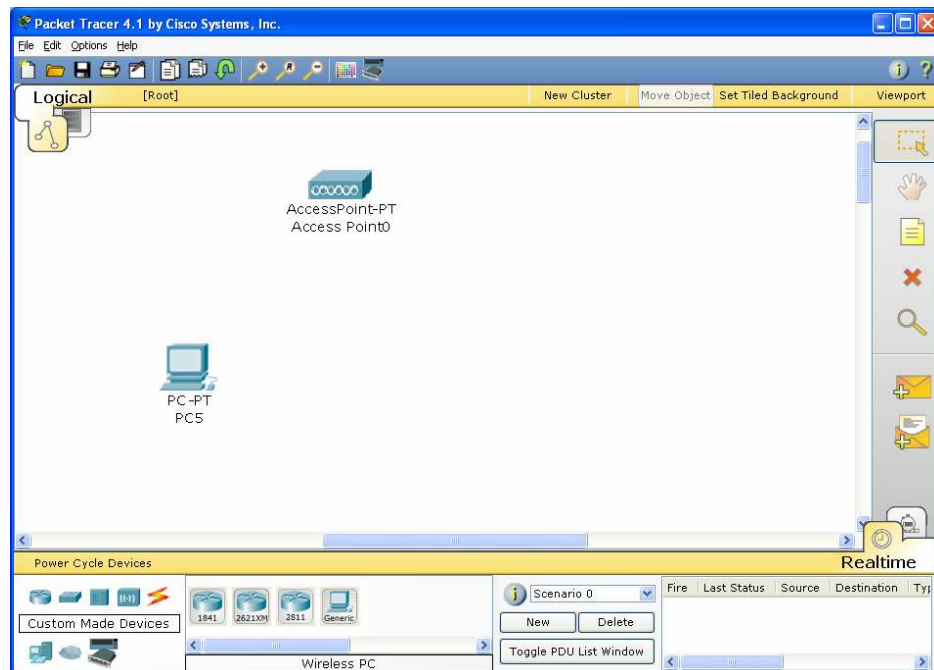
PC>
```


PACKET TRACER Y LAS REDES INALÁMBRICAS

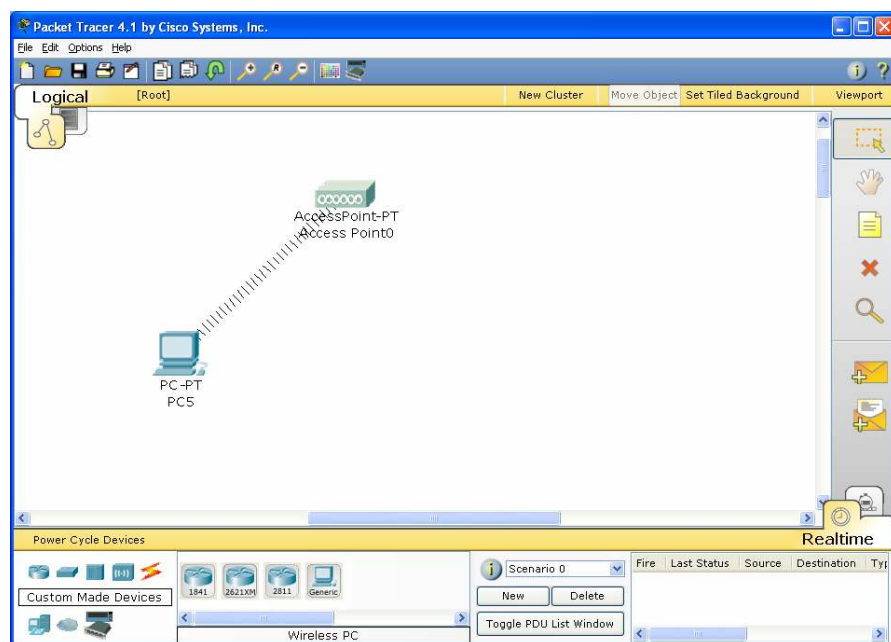
Anteriormente se utilizó Packet Tracer como herramienta de simulación de redes de datos en forma cableada; sin embargo, también es posible utilizarlo como herramienta de simulación para redes inalámbricas. A continuación se hará un montaje bastante básico de una red inalámbrica, el cual será mejorado en capítulos posteriores.



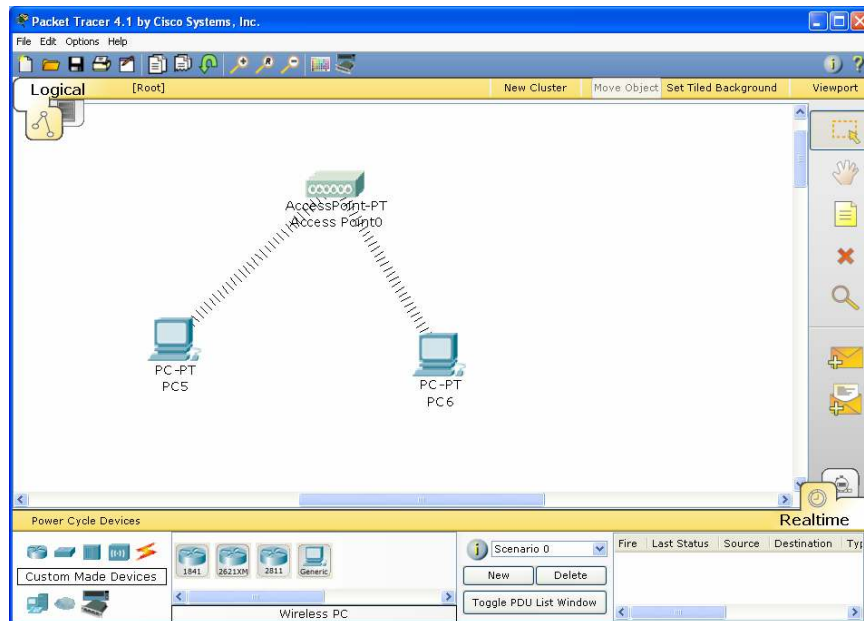
Se desea implementar una red Lan en forma inalámbrica, constituida por dos equipos mediante el uso de un Access Point. Para ello, lo primero es dibujar el access point, el cual se encuentra en el menú Wireless. Tal como se ilustra en la figura anterior.



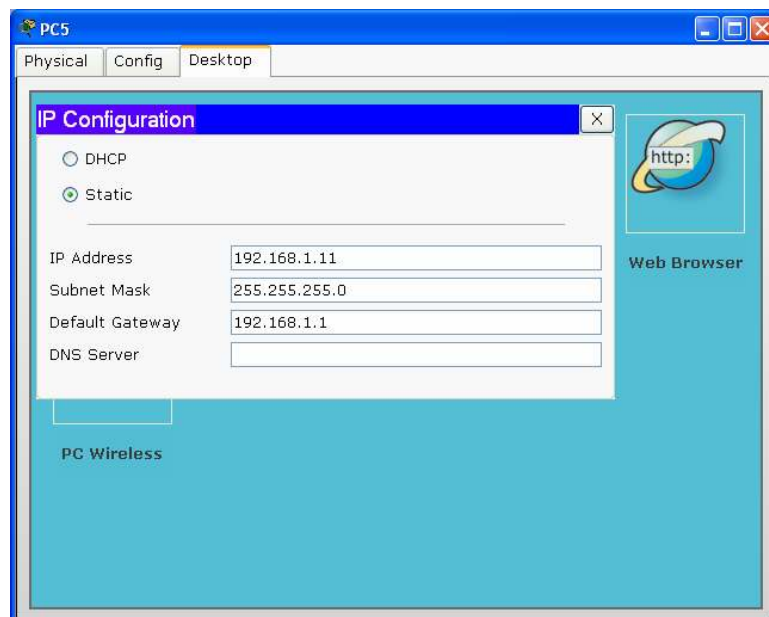
Posteriormente se dibujan los dos PCs con tarjeta inalámbrica, los cuales se encuentran ya configurados en la opción **Custom Made Devices**, el cual al dibujarlo comienza a negociar con el access point hasta establecer una conexión inalámbrica con él, tal como se muestra en la siguiente figura.



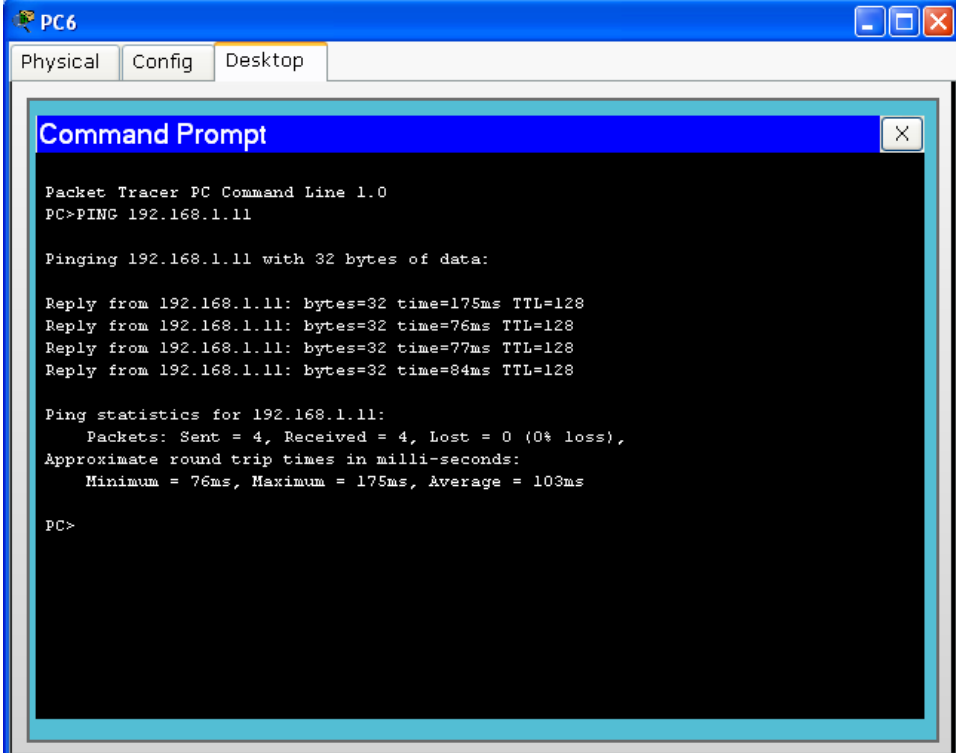
Se realiza el mismo proceso incluyendo ahora el nuevo PC y el resultado es el siguiente:



Sin embargo, el hecho de que existe una conexión no significa que exista una comunicación completa.



Por tal razón es indispensable definir en cada uno de los PCs una dirección IP, la cual por el momento se harán de manera estática. A los PCs se les configurará con las direcciones IP 192.168.1.11 y 192.168.1.12, utilizando máscara por defecto y dirección de Gateway 192.168.1.1 tal como se ilustra en las figuras anteriores



The image shows a screenshot of a Packet Tracer PC Command Prompt window. The window has a blue title bar with the text "PC6" and standard window controls. Below the title bar are three tabs: "Physical", "Config", and "Desktop". The "Desktop" tab is selected, and a "Command Prompt" window is open within it. The Command Prompt has a black background with white text. The text shows the execution of a ping command to 192.168.1.11, including the packet statistics and round trip times.

```
Packet Tracer PC Command Line 1.0
PC>PING 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

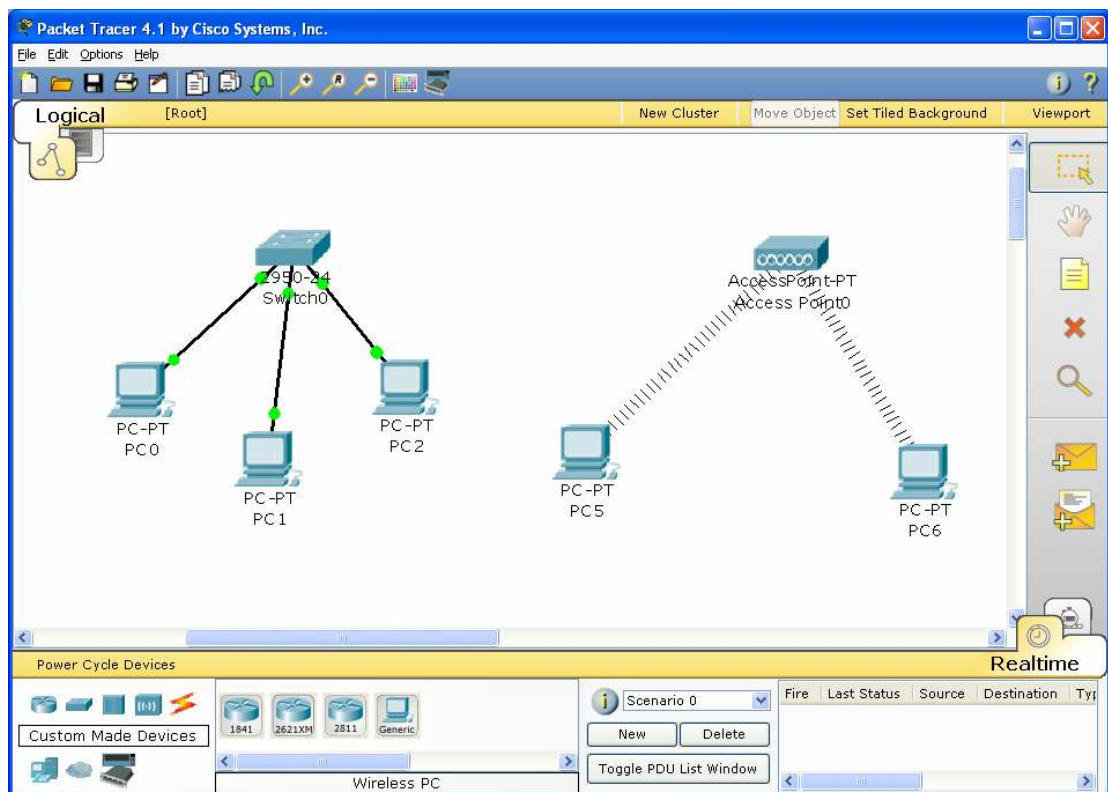
Reply from 192.168.1.11: bytes=32 time=175ms TTL=128
Reply from 192.168.1.11: bytes=32 time=76ms TTL=128
Reply from 192.168.1.11: bytes=32 time=77ms TTL=128
Reply from 192.168.1.11: bytes=32 time=84ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 76ms, Maximum = 175ms, Average = 103ms

PC>
```

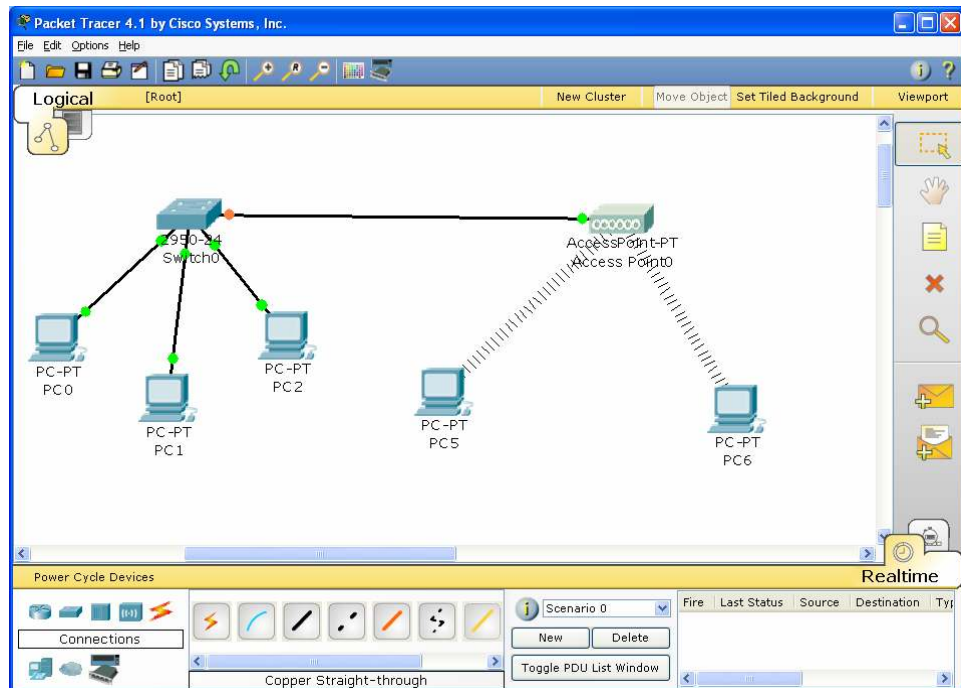
A fin de verificar la comunicación entre los equipos, realizamos un PING a la dirección 192.168.1.11 y listo.

Hasta aquí simplemente se ha implementado una red inalámbrica básica, sin embargo, muchas veces es necesario interconectar redes inalámbricas cableadas con redes inalámbricas. A continuación un ejemplo al respecto.



Integrando el ejemplo anterior junto con el primer ejemplo de interconexión de host en forma cableada y utilizando las mismas direcciones IP, se obtiene el esquema anterior.

Sin embargo, para que exista comunicación entre los equipos de la red cableada y los equipos de la red inalámbrica, debe existir una conexión física entre los equipos concentradores, es decir, entre el Switch y el Acces point. Por tal razón, es necesario conectar a éstos dos dispositivos mediante un cable de conexión directa. Tal como se ilustra en la siguiente figura.



El resultado de interconexión se ve reflejado en la siguiente gráfica mediante el uso del comando PING

The screenshot shows the 'PC5' window with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the results of a PING command. The text in the Command Prompt is as follows:

```
Packet Tracer PC Command Line 1.0
PC>PING 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=260ms TTL=128
Reply from 192.168.1.2: bytes=32 time=114ms TTL=128
Reply from 192.168.1.2: bytes=32 time=90ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 90ms, Maximum = 260ms, Average = 154ms

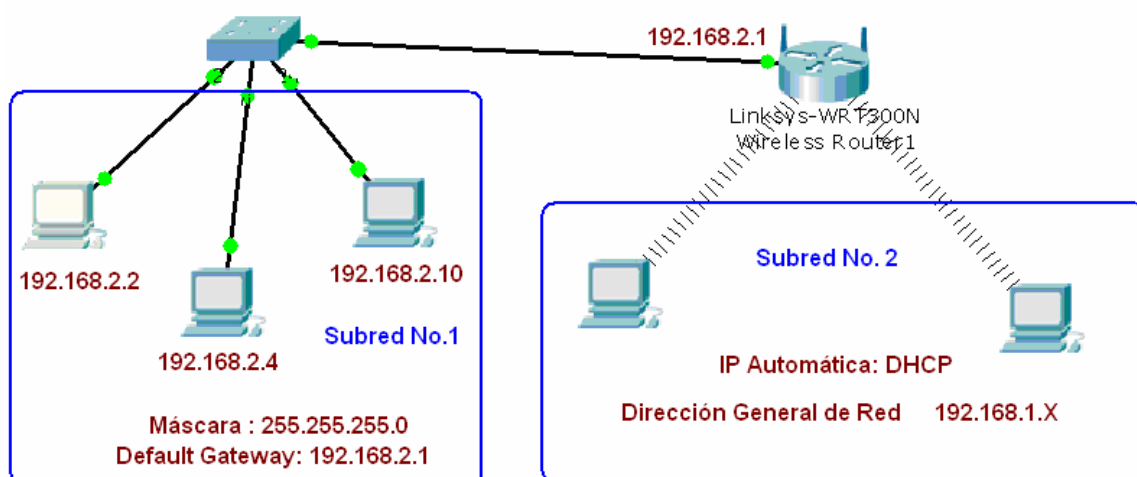
PC>|
```

Uso de la herramienta Packet Tracer, simulando una red híbrida controlada por un Router Inalámbrico

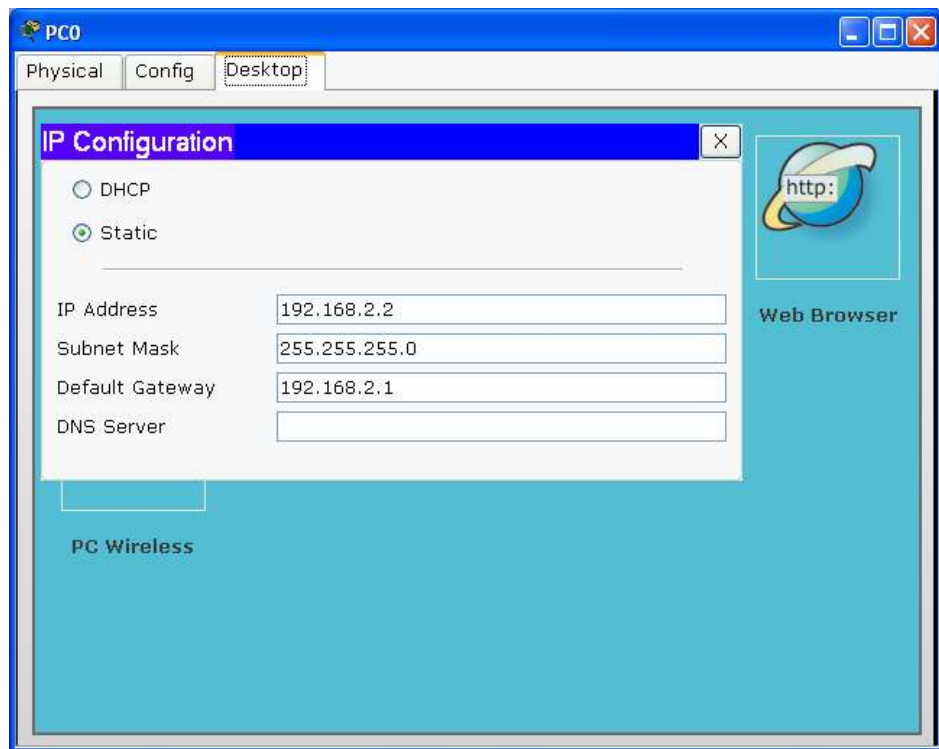
En prácticas anteriores se realizó el montaje de una red híbrida en donde se utilizaba como dispositivos concentradores un switch y un Access Point. Sin embargo, éste sistema presentaba una limitante la cual consistía en que solamente se podían comunicar entre sí siempre y cuando los equipos pertenezcan a la misma subred.

En éste caso, los equipos que hacen parte de la red cableada pertenecen a una dirección de subred diferente a los equipos que pertenecen a la red inalámbrica. Adicionalmente, se aprovechará la oportunidad para configurar los equipos de tal forma que los host pertenecientes a la LAN cableada utilicen direccionamiento IP estático y los host de la WLAN (Wireless LAN) utilicen direccionamiento IP dinámico bajo el uso del protocolo DHCP.

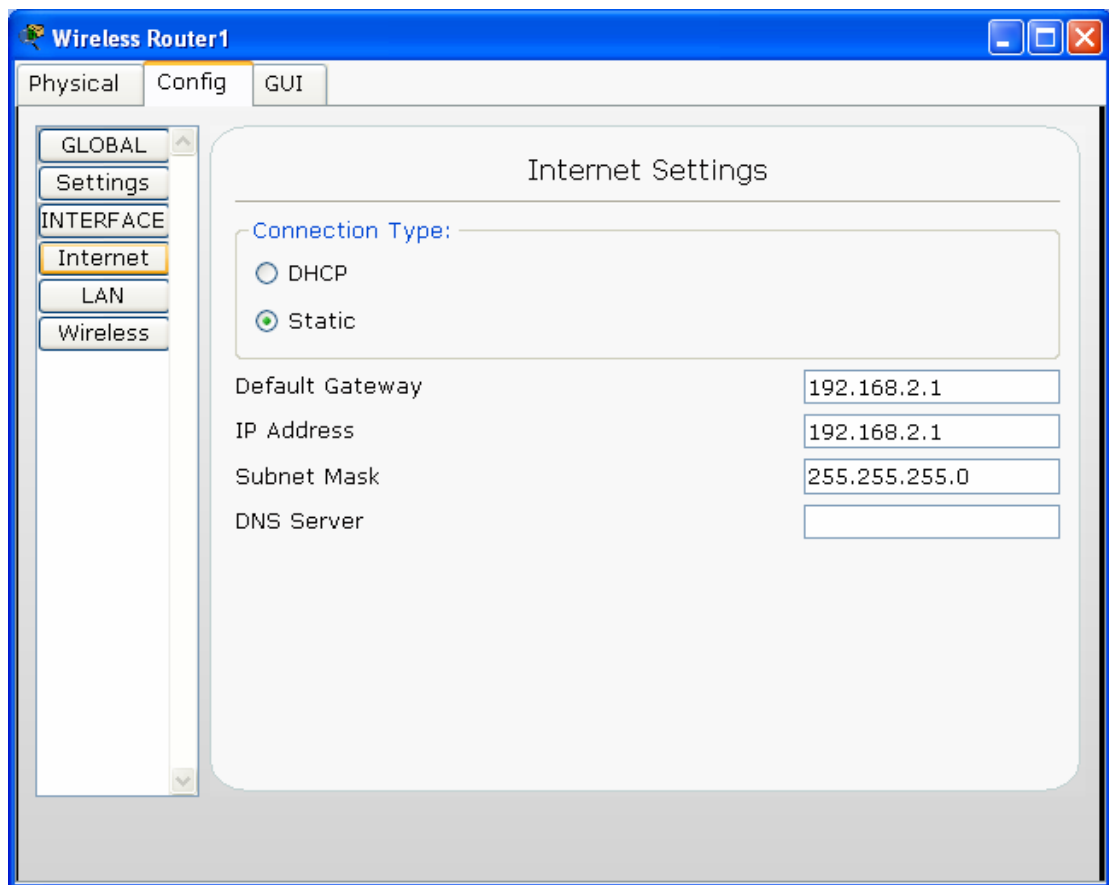
El esquema topológico es el siguiente:



En la figura se indica claramente las direcciones IP requeridas para la subred cableada, las cuales pertenecen a la dirección de subred : 192.168.2.0; la subred inalámbrica trabajará bajo el uso del protocolo DHCP distribuyendo las direcciones IP a los host propios de la dirección de subred: 192.168.1.0



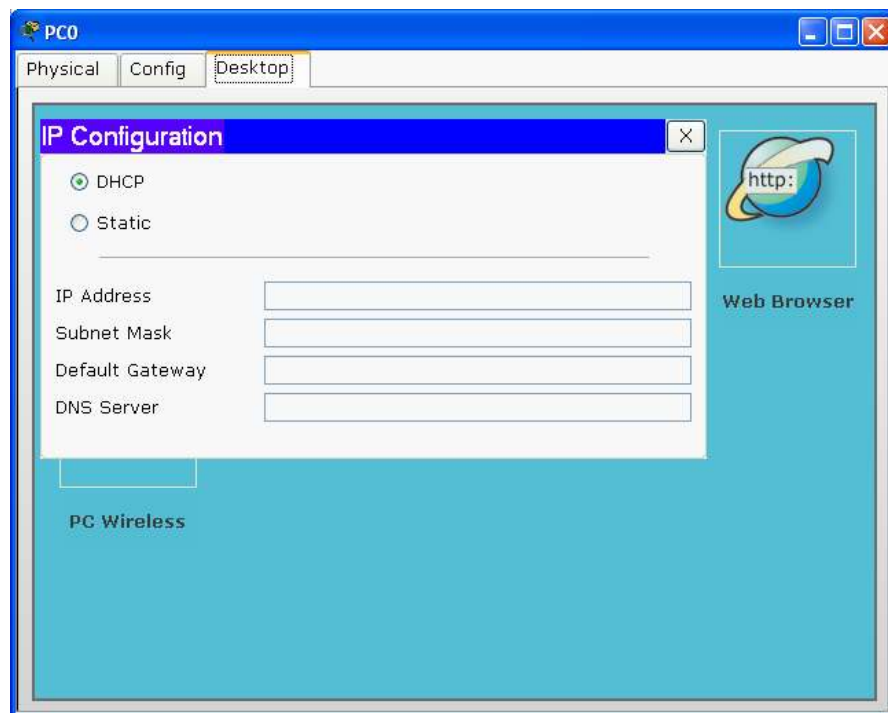
En vista de lo anterior, lo primero que se debe hacer es configurar las direcciones IP, máscara de Subred y Default Gateway en cada uno de los equipos que hacen parte de la red cableada, según los criterios de diseño, tal como se ilustra en la figura anterior.



Como en éste caso se hace uso de un Router Inalámbrico, hay necesidad de configurar la dirección de gateway, la cual es la aquella dirección que utilizarán los host para acceder a otras subredes, en éste caso, para acceder a la subred 192.168.1.0

Cuando se realizar la conexión física entre el Switch y el Router Inalámbrico, se hace a través de la interfaz de INTERNET; sobre la cual se debe configurar la dirección de gateway tal como se ilustra en la figura anterior.

Después de configura los parámetros correspondientes a la red cableada, se inicia la configuración de la red inalámbrica de la siguiente forma:



Cada uno de los host que hacen parte de la red inalámbrica se deben configurar utilizando el protocolo DHCP, tal como se ilustra en la figura anterior, el cual se encargará de adjudicar según sus criterios las direcciones IP a cada uno de los Host.

Sin embargo, es importante comprender en qué lugar se deben definir aquellos parámetros que rigen la distribución de direcciones IP, propias de la red inalámbrica. En la siguiente figura se ilustra éste proceso.

Se selecciona el Router inalámbrico, se escoge la opción GUI sobre la cual de definen los siguientes parámetros:

The screenshot shows the 'Wireless Router1' configuration window with the 'Config' tab selected. The 'Network Setup' section is active, displaying the following settings:

- Router IP:** 192.168.1.1
- Subnet Mask:** 255.255.255.0
- DHCP Server:** Enabled (radio button selected)
- DHCP Reservation:** (button)
- Start IP Address:** 192.168.1.100
- Maximum number of Users:** 50
- IP Address Range:** 192.168.1.100 - 149
- Client Lease Time:** 0 minutes (0 means one day)
- Static DNS 1:** 0.0.0.0
- Static DNS 2:** 0.0.0.0
- Static DNS 3:** 0.0.0.0

IP Address: 192.168.1.1 (Gateway subred inalámbrica)

Subset Mask (Máscara de subred): 255.255.255.0

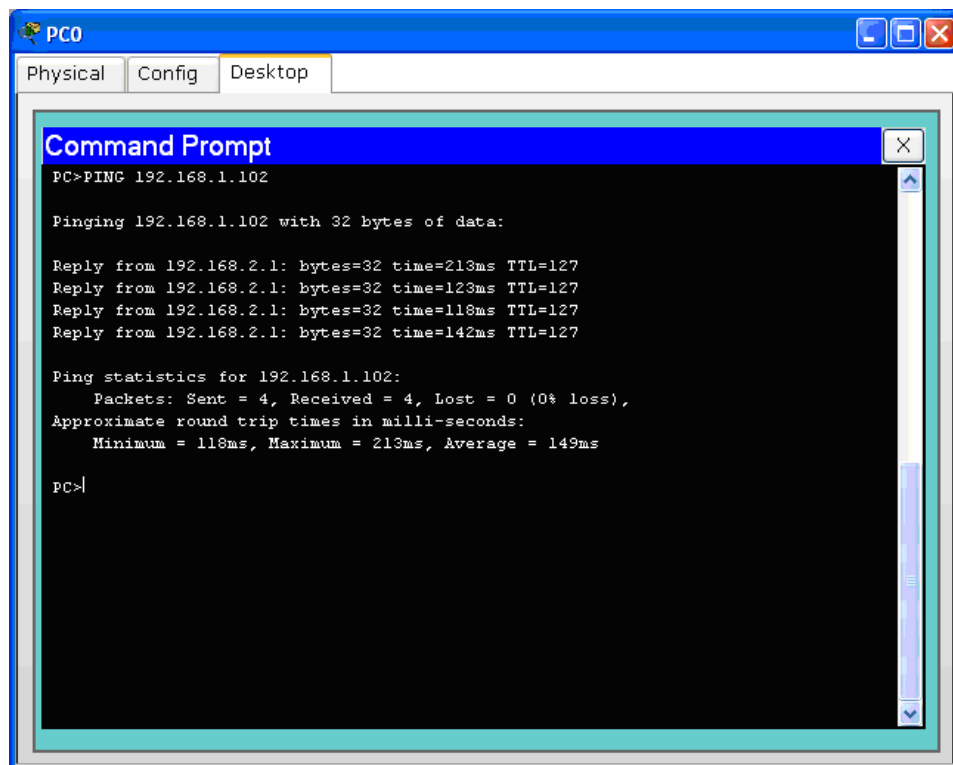
DHCP Enabled : Indicando que se utilizará el protocolo DHCP

Stara IP Address: 192.168.1.100 (Dirección inicial para la adjudicación de direcciones IP en forma automática)

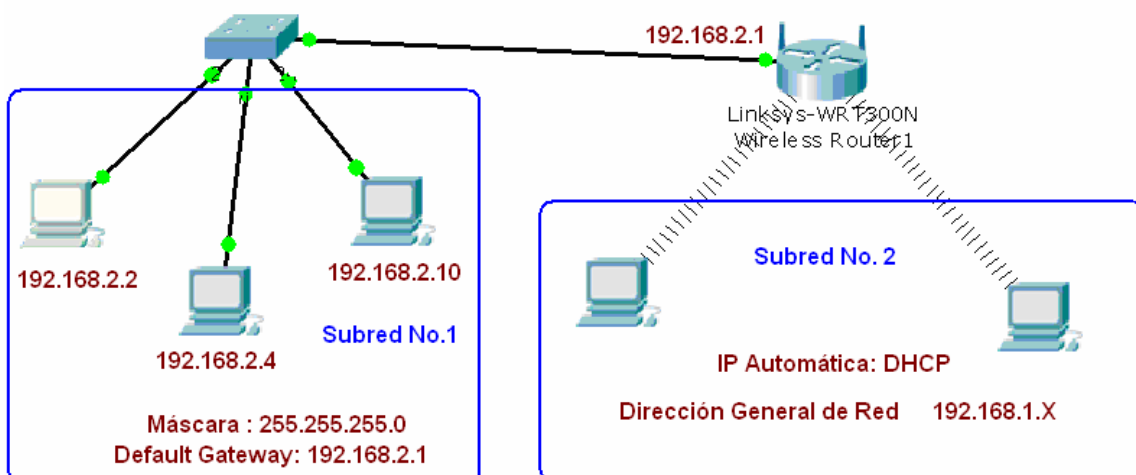
Número máximo de usuarios: 50

Rango de direcciones IP para distribución: 192.168.1.100 – 192.168.1.149

A continuación se verifica la comunicación entre un equipo de la red cableada y un host inalámbrico, específicamente, desde la dirección 192.168.2.2 (LAN Cableada) a la dirección 192.168.1.102 (LAN Inalámbrica)



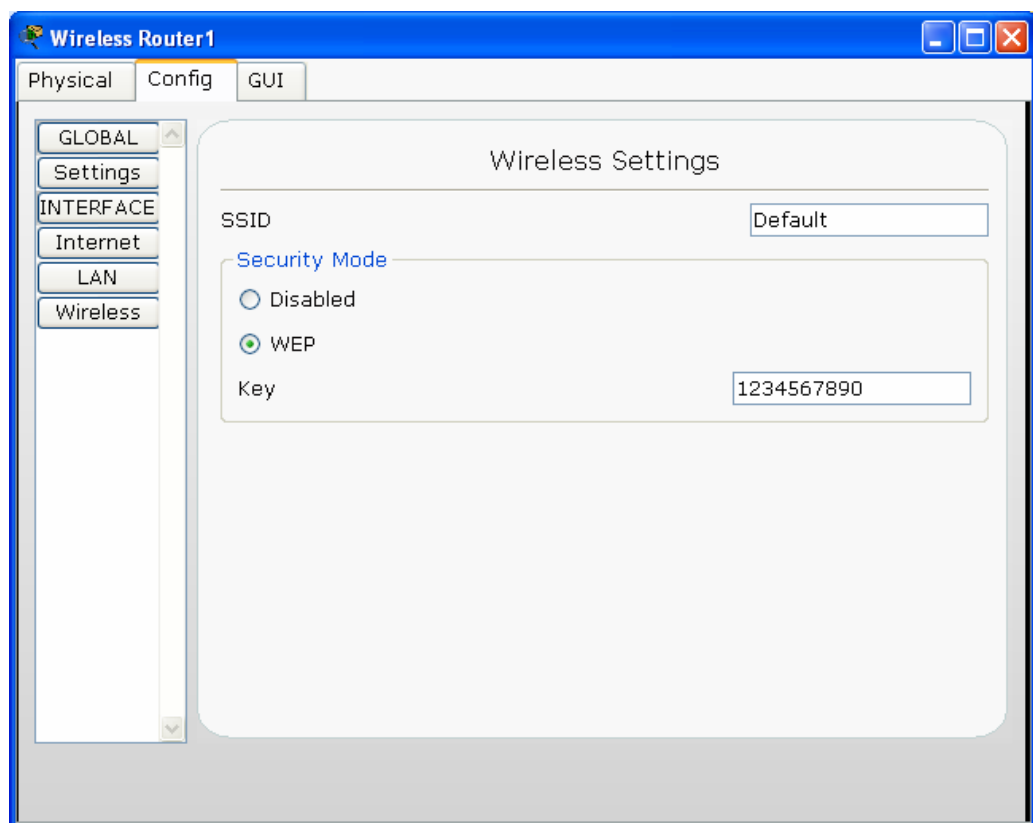
Uso del Protocolo WEP en redes Inalámbricas



Utilizando el mismo esquema de red anterior, tal como se ilustra en la figura, seleccionamos el router inalámbrico y nos ubicamos en la sección Config. Allí

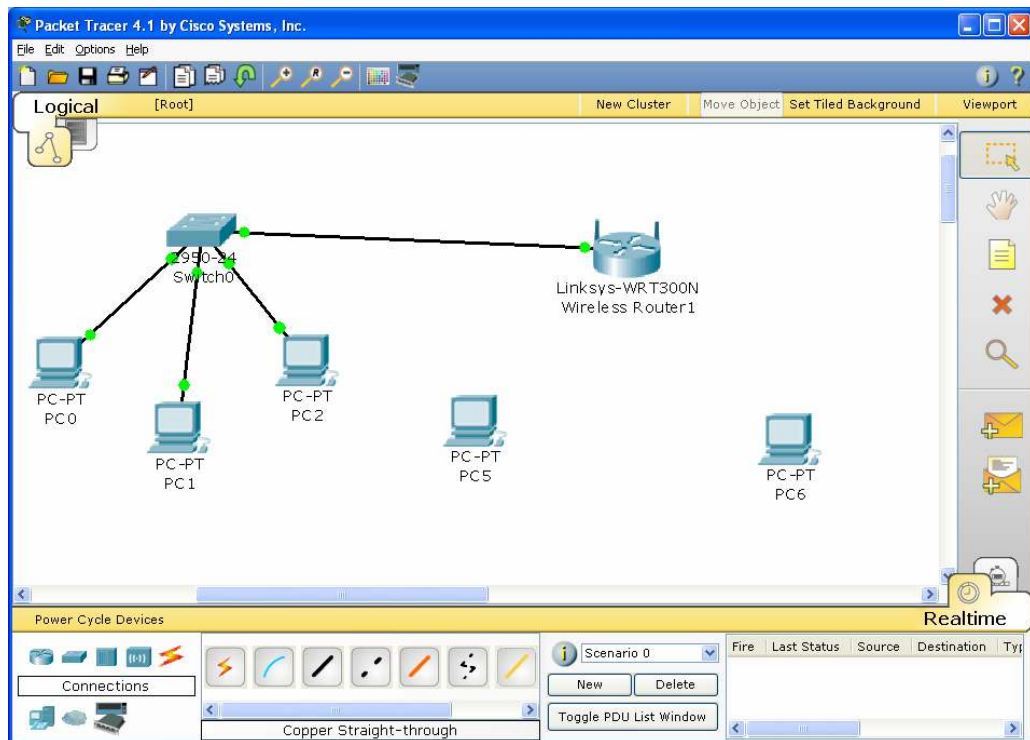
se encuentra establecido el modo de Seguridad a utilizar, el cual por defecto se encuentra deshabilitado.

En éste caso en particular, seleccionamos WEP y establecemos la contraseña o Key, la cual será utilizada por el router inalámbrico y los PCs para encriptar su información bajo el uso de éste protocolo. Vale la pena mencionar que ésta contraseña deberá ser de al menos 10 caracteres. Existen herramientas software especializadas en generar éste tipo de contraseñas teniendo en cuenta criterios de seguridad mayores a los que usualmente poseen las contraseñas convencionales.

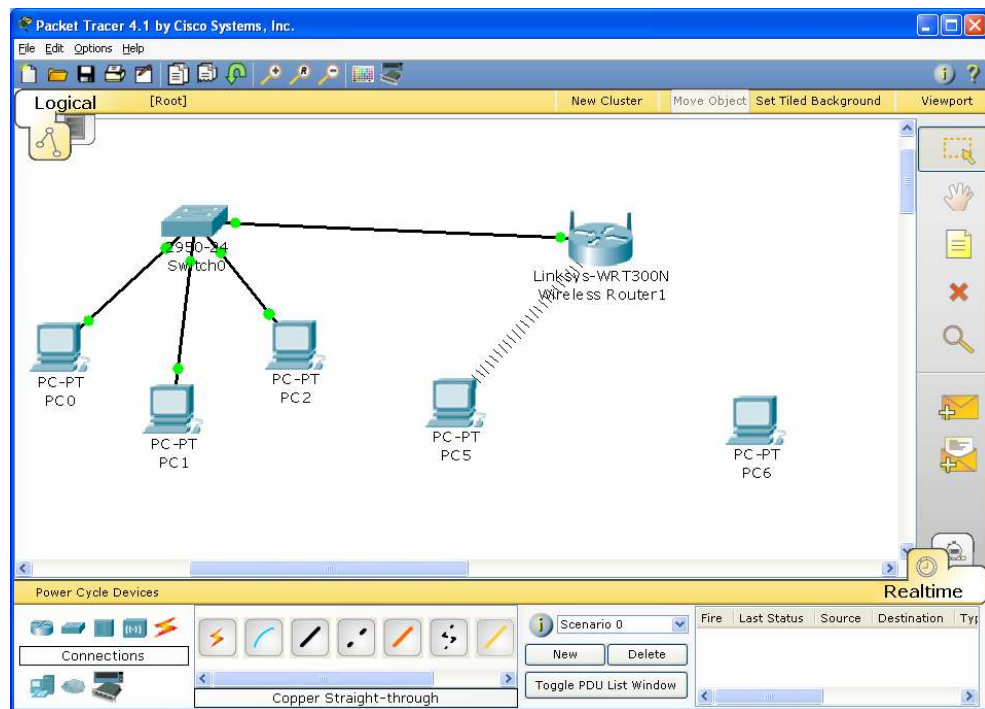
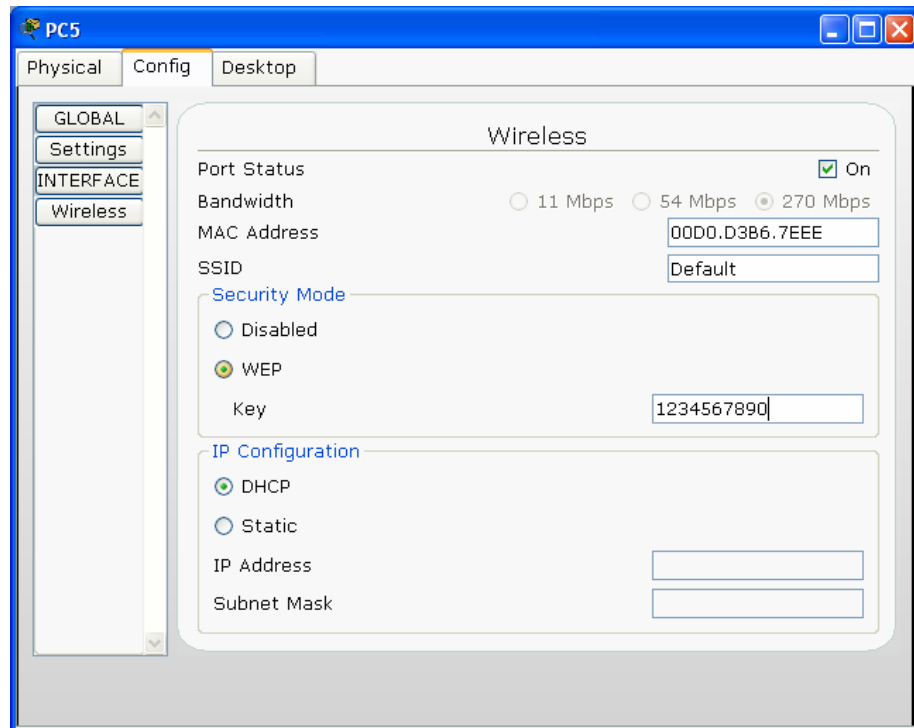


Obsérvese, que si activamos el protocolo WEP en el router, los equipos o host no establecerán comunicación con él hasta que en cada uno de ellos no se defina que se utilizará éste protocolo y se defina la misma contraseña de

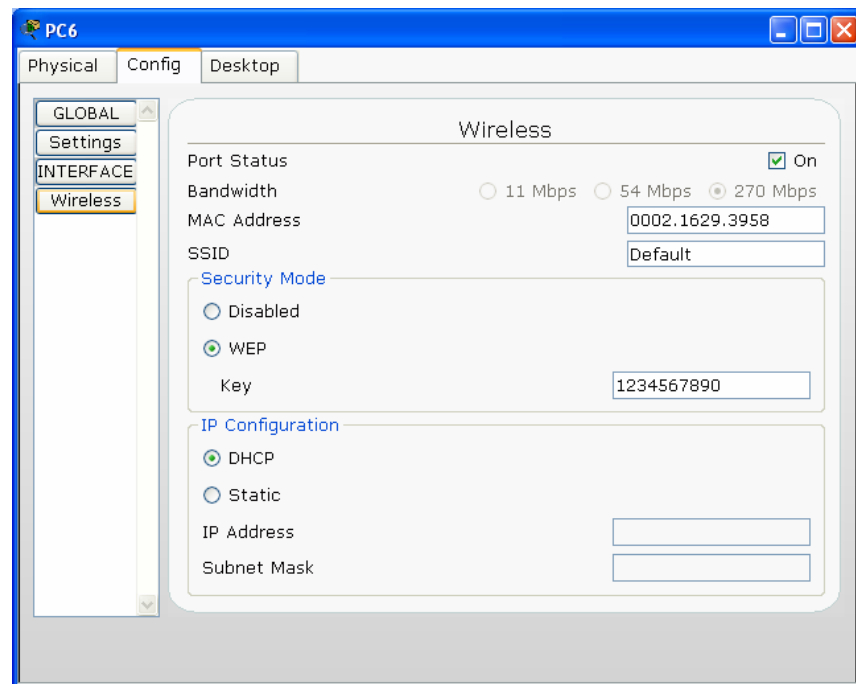
encriptación configurada en el router. En la siguiente figura se ilustra claramente ésta situación. En la primer figura se evidencia que ninguno de los host inalámbricos presenta comunicación con el Router, y tan pronto ésta configuración se realiza en uno de los PCs, automáticamente inicia el proceso de comunicación demostrado en la tercera figura.



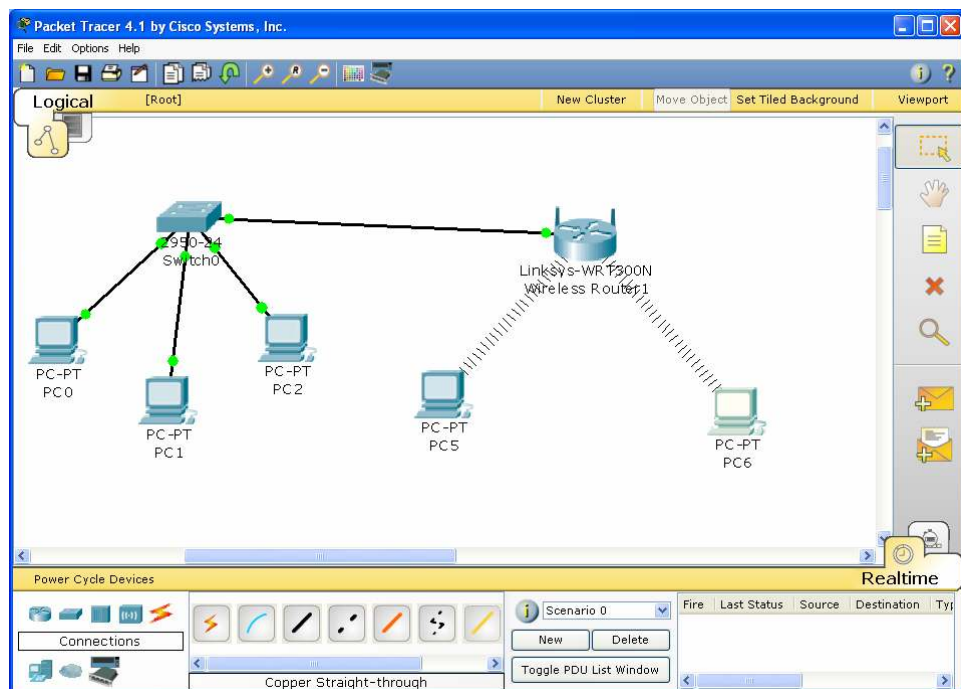
En la siguiente figura se ilustra la configuración en uno de los PCs



Configurando el segundo PC inalámbrico



En donde finalmente queda configurada la red de la siguiente forma:



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 ENCRYPTACIÓN: 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 Certificadores 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.

REFERENCIA BIBLIOGRAFICAS

ANSI/IEEE Std 802.11g. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. Estados Unidos: Institute of Electrical and Electronics Engineers, 2003. ISBN 0-7381-3701-4 SS95134.

ATHEROS COMMUNICATIONS INC. 802.11 Wireless LAN Performance. Doc. 991-00002-006. Sunnyvale, CA. 2003

CHEUNG, David y PRETTIE Cliff. A Path Loss Comparison Between the 5 GHz UNII Band (802.11a) and the 2.4 GHz ISM Band (802.11b), Inter Labs, Intel Corporation, Enero 2002.

DE LUQUE Luis, DÍAZ Irina, VASQUEZ Sandra. Predicción del nivel de intensidad de señal recibid RSSI en una red inalámbrica 802.11b mediante un modelo neuronal. Proyecto de Grado. E3T UIS. Bucaramanga 2005.

Marcelo Najnudel. "ESTUDO DE PROPAGAÇÃO EM AMBIENTES FECHADOS PARA O PLANEJAMENTO DE WLANS". Río de Janeiro, Febrero de 2004.

STALLINGS William. Wireless Communications and Networks. Prentice - Hall. Estados Unidos 2006.

TANENBAUM Andrew. Redes de Computadores. Pearson Education. México 2003.

VILLAROEL Carlos, RODRÍGUEZ Angie, VALLE Julio. Diseño de una red de área local inalámbrica. Universidad de Tarapacá Departamento de Electrónica. Arica, Chile 2003.

YUTACA, Hayacawa. Sistemas de medida wireless LAN y software específico. Revista Española de Electrónica. Barcelona. Marzo de 2003.

ETHERREAL Network Analyzer. Disponible en Internet, URL <<http://www.ethereal.com>>, Enero 2004.

BARBERO, Lucas. Tutorial Ethereal. Universidad Tecnológica nacional 2006

JANGEUN, Jun y MIHAIL, Sichitiu. "The Nominal Capacity of Gíreles Mesh Networks", IEEE Wireless Communications Magazine, Oct. 2003.

LIN Yu-Ju, LATCHMAN Haniph y NEWMAN Richard. "A Comparative Performance Study of Wireless and Power Line Networks", IEEE Communications Magazine, Abril 2003.

<http://www.amp.co/networking/warranty.html>

<http://www.cintel.org.com.co>

<http://www.linksys.com>

<http://www.cisco.com>

<http://www.trendware.com>

<http://www.wi-fi.org>

<http://www.wi-fiplanet.com/tutorials/article.php/1116311>. 2003

<http://www.programas-gratis.net>

<http://www.wikipedia.com>

<http://www.monografias.com>

<http://www.3com.com>

<http://www.upv.com>