



**INSTITUTO POLITECNICO NACIONAL**  
**ESCUELA SUPERIOR DE CÓMPUTO (ESCOM)**



**REDES DE COMPUTADORAS**

---

NOMBRE DEL ALUMNO:

- SANTOS MÉNDEZ ULISES JESÚS

NOMBRE DEL MAESTRO:

- JUAN JESÚS ALCARAZ TORRES

PRÁCTICA 1:

- PACKET TRACER COMO HERRAMIENTA DE SIMULACIÓN

## Introducción

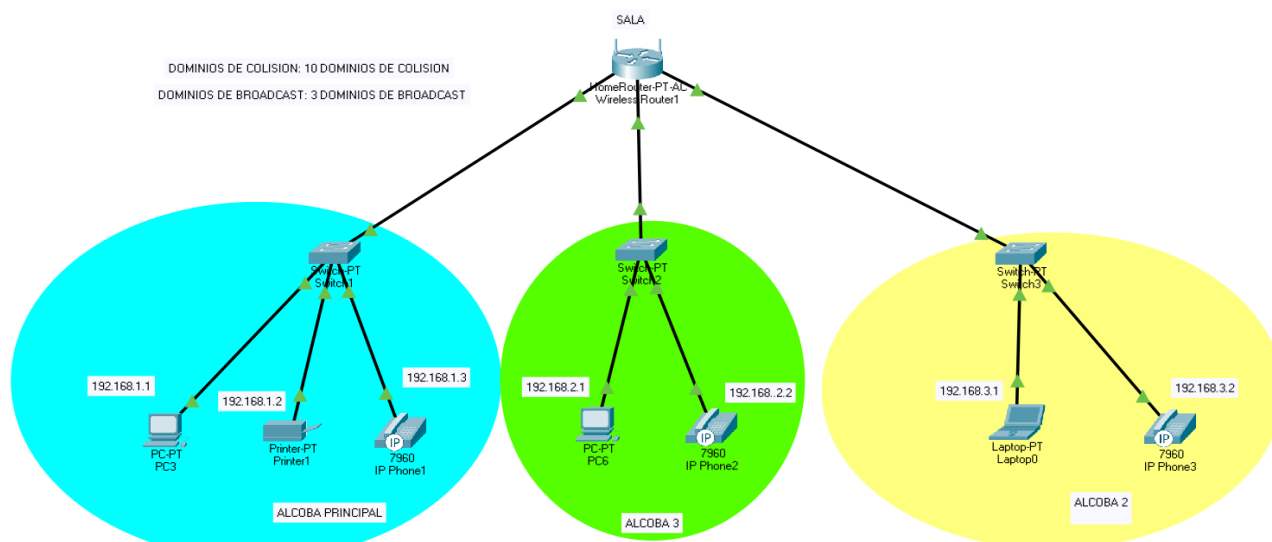
Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA.

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

Packet Tracer 8.0 es la última versión del simulador de redes de Cisco Systems, herramienta fundamental si el alumno está cursando el CCNA o se dedica al networking.



En este programa se crea la topología física y lógica de la red simplemente arrastrando los dispositivos a la pantalla.



## Desarrollo:

- IPCONFIG

IPConfig es una utilidad de línea de comandos que proporciona la configuración TCP-IP de un equipo.

Cuando se utiliza con la opción /all, produce un informe detallado de la configuración de todas las interfaces de red presentes en el equipo, incluyendo los puertos serie configurados en el sistema (RAS).

Las opciones /release [adaptador] y /renew [adaptador] liberan y renuevan respectivamente la dirección IP del adaptador especificado. Si no se especifica adaptador, el comando afectará a todas las direcciones de adaptadores enlazados a TCP/IP.

- PING

Ping es una herramienta que ayuda a verificar la conectividad del equipo a nivel IP. Cuando se detectan errores en la conexión TCP/IP, puede utilizarse el comando ping para enviar a un nombre DNS destino o a una dirección IP una petición ICMP de eco.

Se recomienda realizar un ping inicial a la dirección IP del host destino. Si este resulta con éxito, puede intentarse un ping al nombre simbólico. Si esta última falla, el problema no estará en la conectividad de red, sino en la resolución de nombres.

### Ejemplo:

Ping 192.168.1.76

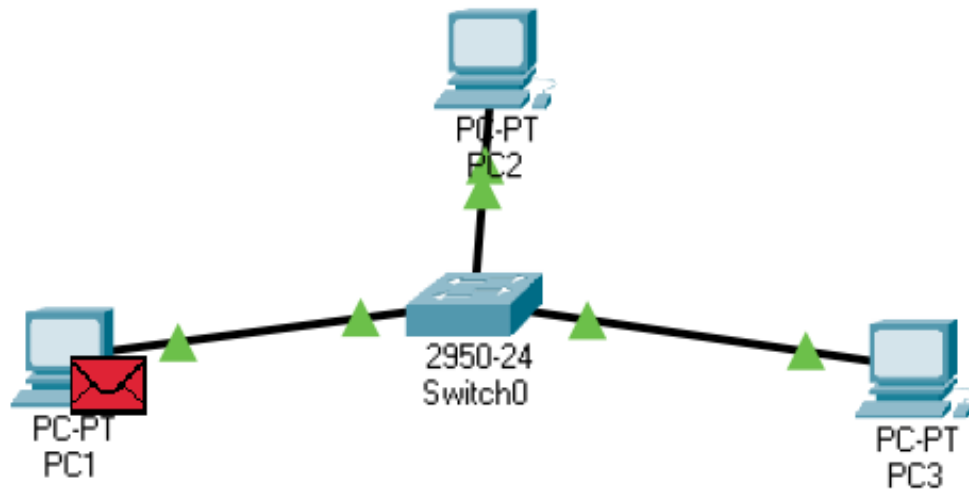
Este comando va de la mano con ipconfig ya que te permite saber tu dirección IP y ping te verifica tu conexión a la red.

- ARP -A

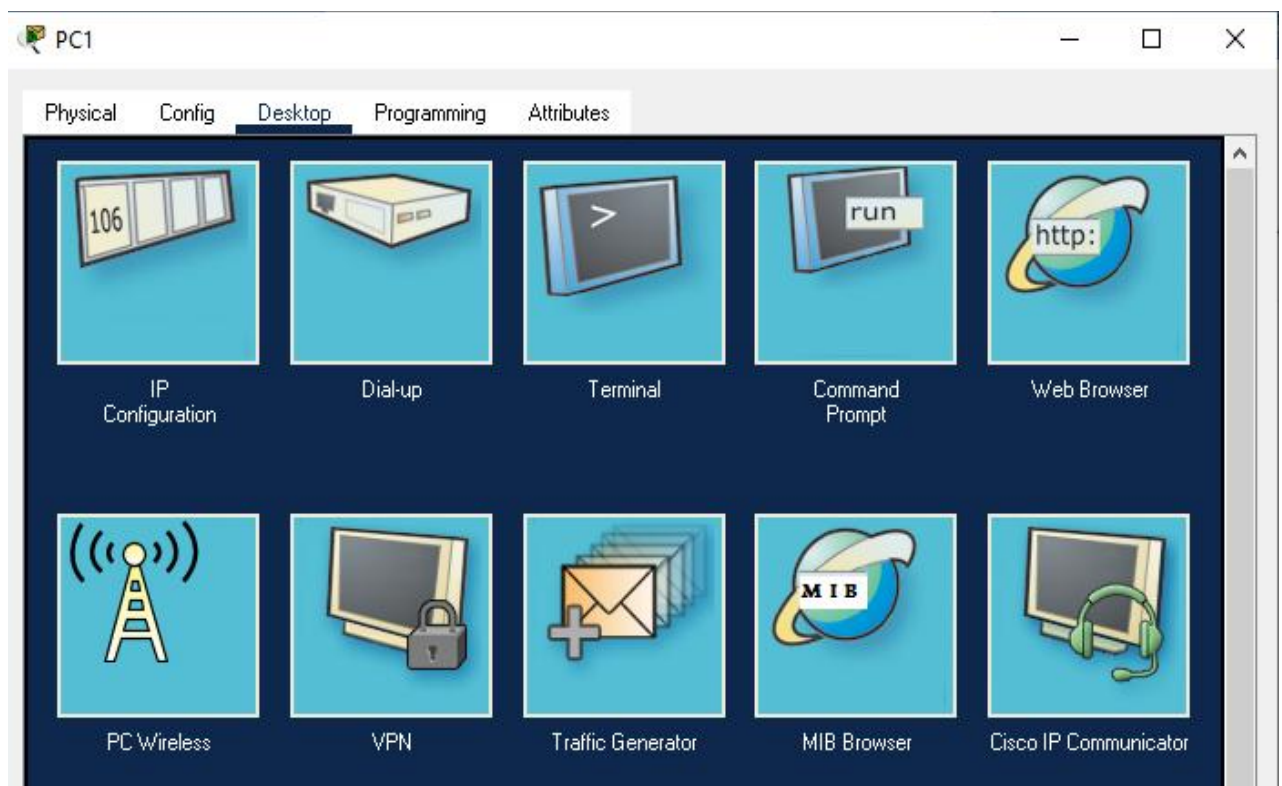
El comando ARP resulta útil para visualizar la caché de resolución de direcciones. Muestra y modifica las tablas de traducción de direcciones IP a direcciones físicas usadas por el protocolo de resolución de direcciones ARP-

**-a:** Muestra las entradas actuales de ARP preguntando por los datos del protocolo. Si se especifica dir\_IP, se muestran las direcciones IP y Física sólo para el equipo especificado. Cuando ARP se utiliza en más de una interfaz de red, entonces se muestran entradas para cada tabla ARP.

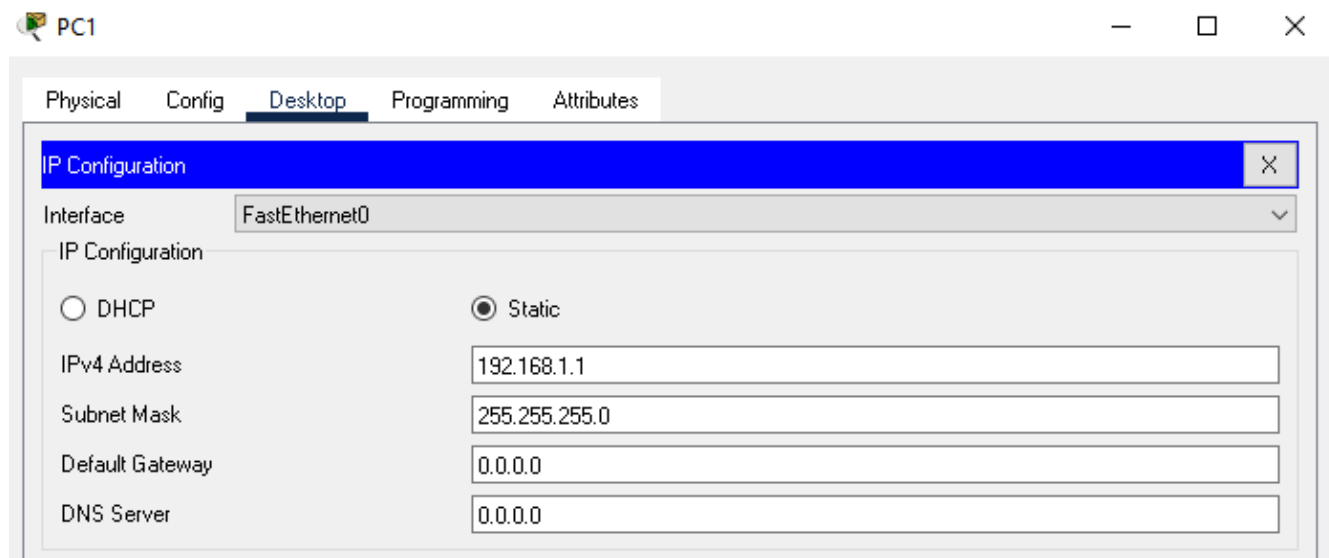
1. Se construyó la siguiente red con ayuda de packet tracer.



2. Se configuro la red IP en cada computadora accediendo al apartado de escritorio.



3. En la sección de interface de la configuración de IP, se ingresa la dirección IPv4, en automático se configura la máscara de subred.



4. Se hacen los pasos anteriores en cada una de las computadoras, posteriormente se ingresan algunos comandos en la consola del equipo del que estamos hablando, esto se hace en el command prompt que en Windows sería el CMD.

Primero se hace uso del comando ipconfig

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:43FF:FE45:B0A1
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0
```

Después se utiliza el comando ping

```
C:\>ping
Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms 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 = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Después se usa el comando arp -a

```
C:\>arp -a
    Internet Address      Physical Address      Type
    192.168.1.2           0007.ec0b.6dl8       dynamic

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

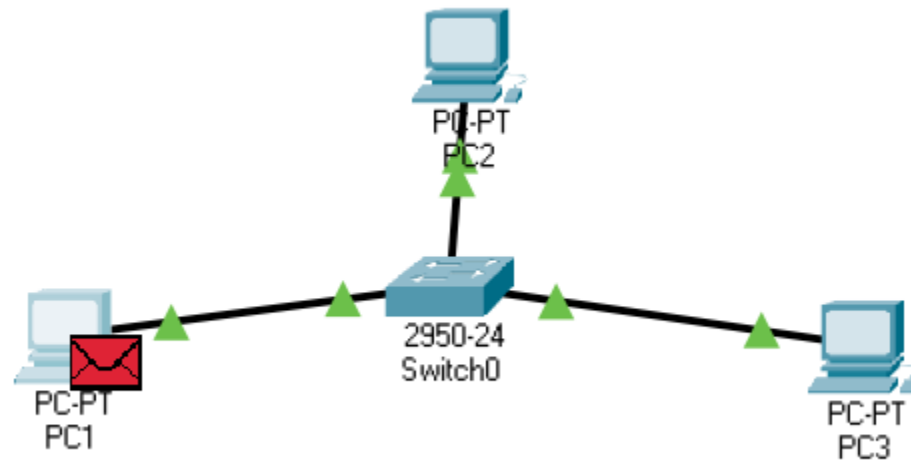
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

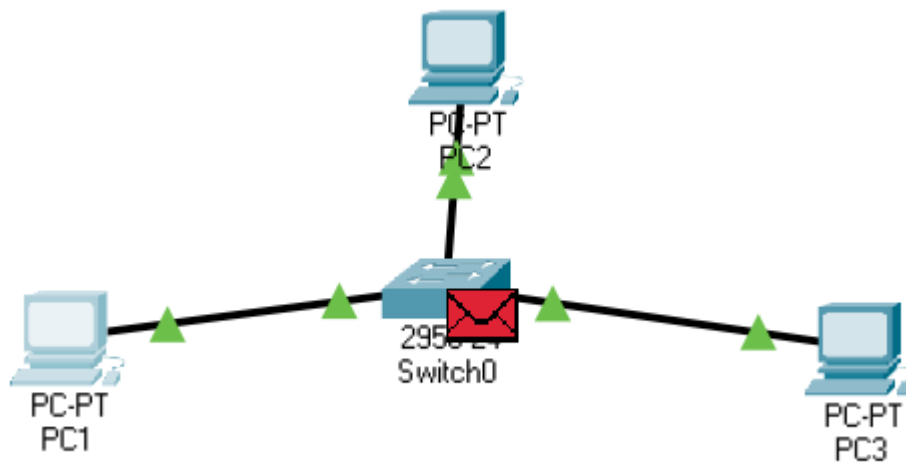
C:\>arp -a
    Internet Address      Physical Address      Type
    192.168.1.2           0007.ec0b.6dl8       dynamic
    192.168.1.3           000c.cfa6.ccb3       dynamic

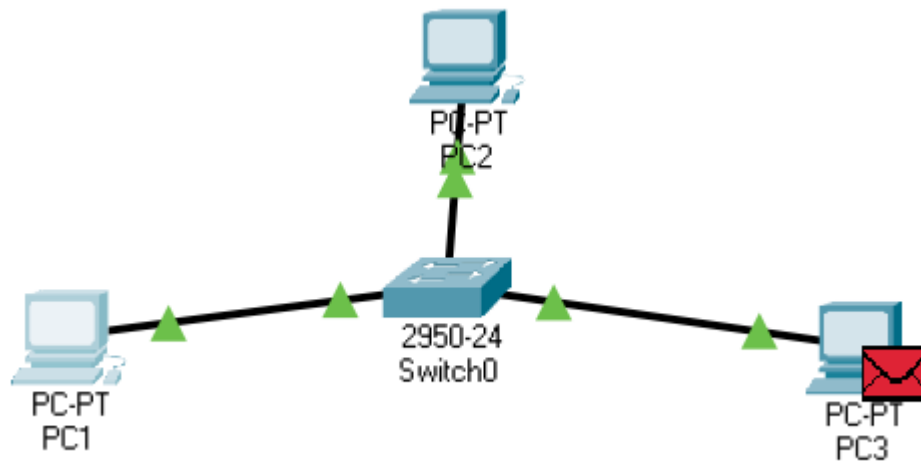
C:\>
```

5. Se procede a hacer una simulación con un paquete de datos que se comunica con otra computadora, se observa que el paquete cambia de lugar, pasando primero por el switch y posteriormente pasa hacia la otra PC, a su vez este mensaje regresa como confirmación que el paquete fue recibido.



El paquete de datos que se encuentra en la PC1 se dirige hacia la PC3





6. Se pueden acceder los comandos anteriores en el CMD de Windows o en el SO que estés trabajando.

- ipconfig

```
Microsoft Windows [Versión 10.0.19041.867]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\ulise>ipconfig

Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::7ce9:7a01:4be2:cb4f%13
    Dirección IPv4. . . . . : 192.168.1.76
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.254
```



- ping

```
C:\Users\ulise>ping

Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
        [-4] [-6] nombre_destino

Opciones:
-t          Hacer ping al host especificado hasta que se detenga.
            Para ver estadísticas y continuar, presione
            Ctrl-Interrumpir; para detener, presione Ctrl+C.
-a          Resolver direcciones en nombres de host.
-n count    Número de solicitudes de eco para enviar.
-l size     Enviar tamaño de búfer.
-f          Establecer marca No fragmentar en paquetes (solo IPv4).
-i TTL      Período de vida.
-v TOS      Tipo de servicio (solo IPv4. Esta opción está desusada y
            no tiene ningún efecto sobre el campo de tipo de servicio
            del encabezado IP).
-r count    Registrar la ruta de saltos de cuenta (solo IPv4).
-s count    Marca de tiempo de saltos de cuenta (solo IPv4).
-j host-list Ruta de origen no estricta para lista-host (solo IPv4).
-k host-list Ruta de origen estricta para lista-host (solo IPv4).
-w timeout  Tiempo de espera en milisegundos para cada respuesta.
-R          Usar encabezado de enrutamiento para probar también
            la ruta inversa (solo IPv6).
            Por RFC 5095 el uso de este encabezado de enrutamiento ha
            quedado en desuso. Es posible que algunos sistemas anulen
            solicitudes de eco si usa este encabezado.
-S srcaddr  Dirección de origen que se desea usar.
-c compartment Enrutamiento del identificador del compartimiento.
-p          Hacer ping a la dirección del proveedor de Virtualización
            de red de Hyper-V.
-4          Forzar el uso de IPv4.
-6          Forzar el uso de IPv6.
```

- arp -a

```
C:\Users\ulise>arp -a

Interfaz: 192.168.1.76 --- 0xd
Dirección de Internet      Dirección física      Tipo
192.168.1.64               bc-ff-eb-81-f7-2d     dinámico
192.168.1.66               88-79-7e-0b-ff-1a     dinámico
192.168.1.68               dc-ef-ca-f0-0d-ca     dinámico
192.168.1.70               68-a3-c4-a3-e8-78     dinámico
192.168.1.73               dc-74-a8-e2-5f-bc     dinámico
192.168.1.77               5e-2c-41-e8-6a-5b     dinámico
192.168.1.254              18-4a-6f-18-25-fc     dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff     estático
224.0.0.22                 01-00-5e-00-00-16     estático
224.0.0.251                01-00-5e-00-00-fb     estático
224.0.0.252                01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático
```

## **Conclusión**

En conclusión la práctica me permitió ver el funcionamiento de este simulador de redes, a ubicar los elementos de comunicación pertenecientes a capas así como ver los dispositivos que se pueden conectar por medio de cables, a su vez me permitió ver los comandos que se ingresan para conocer datos sobre nuestra red, como MAC y dirección IP, se demostró con el CMD de Windows que esos comandos si son de uso general para conocer cierta información de nuestra red.