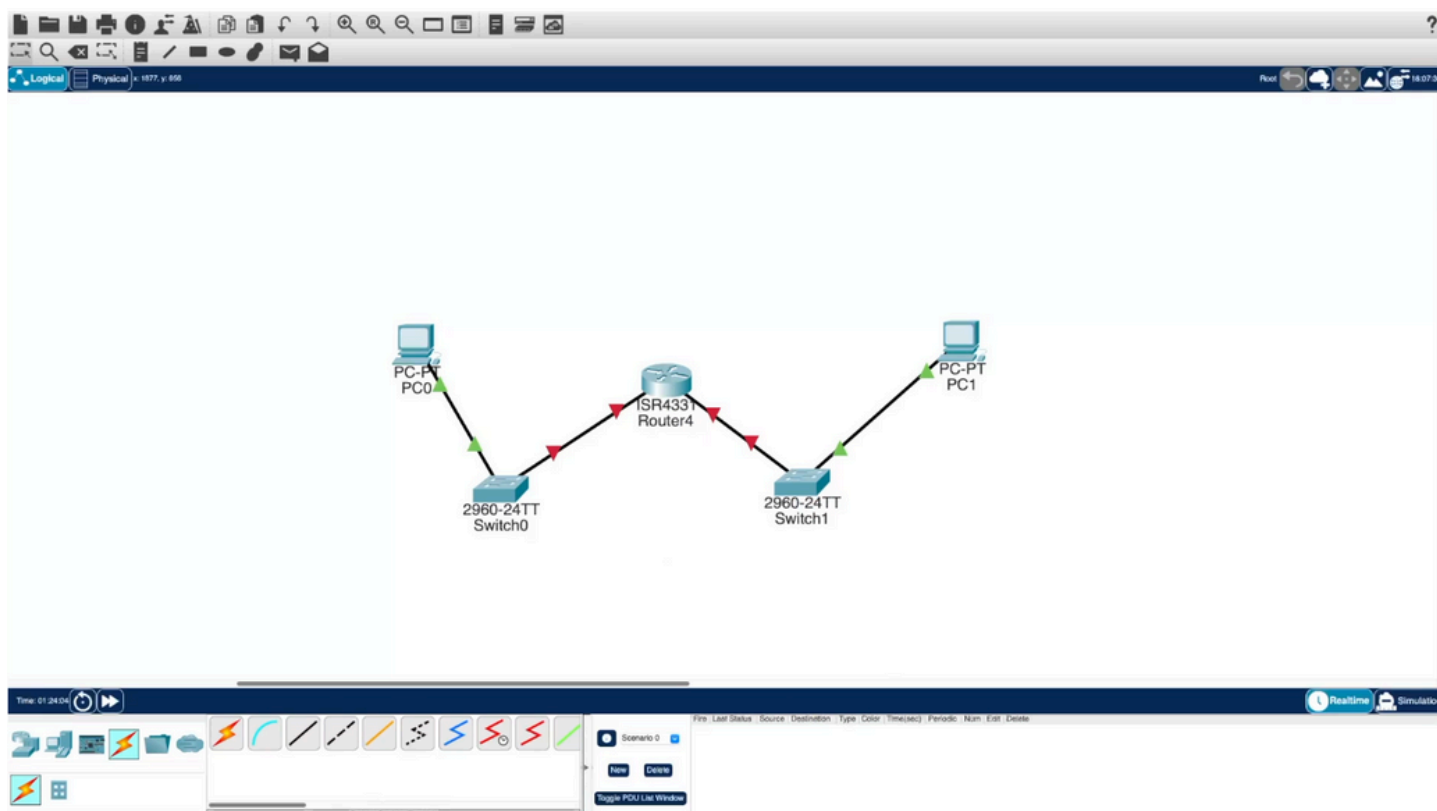
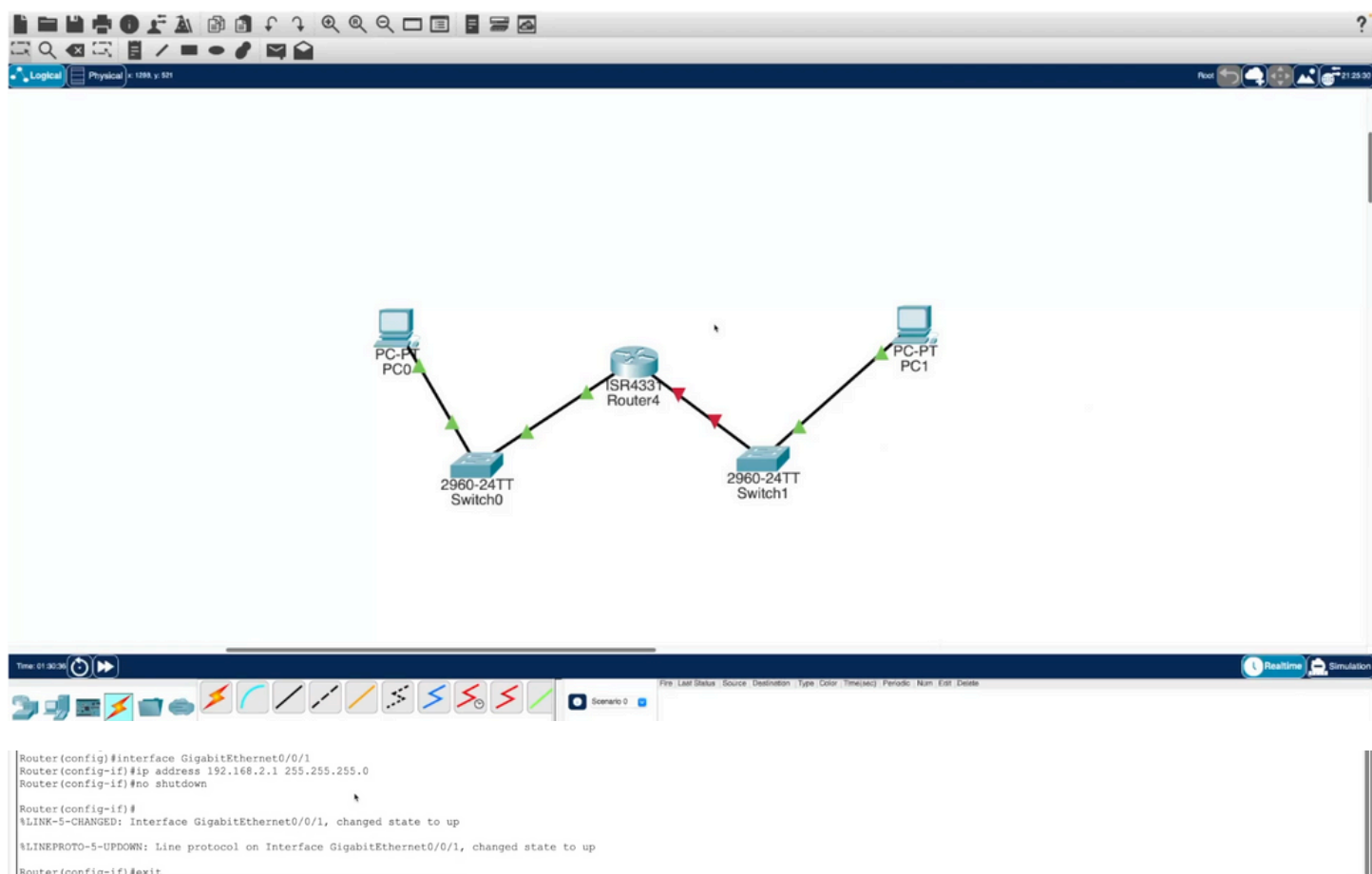


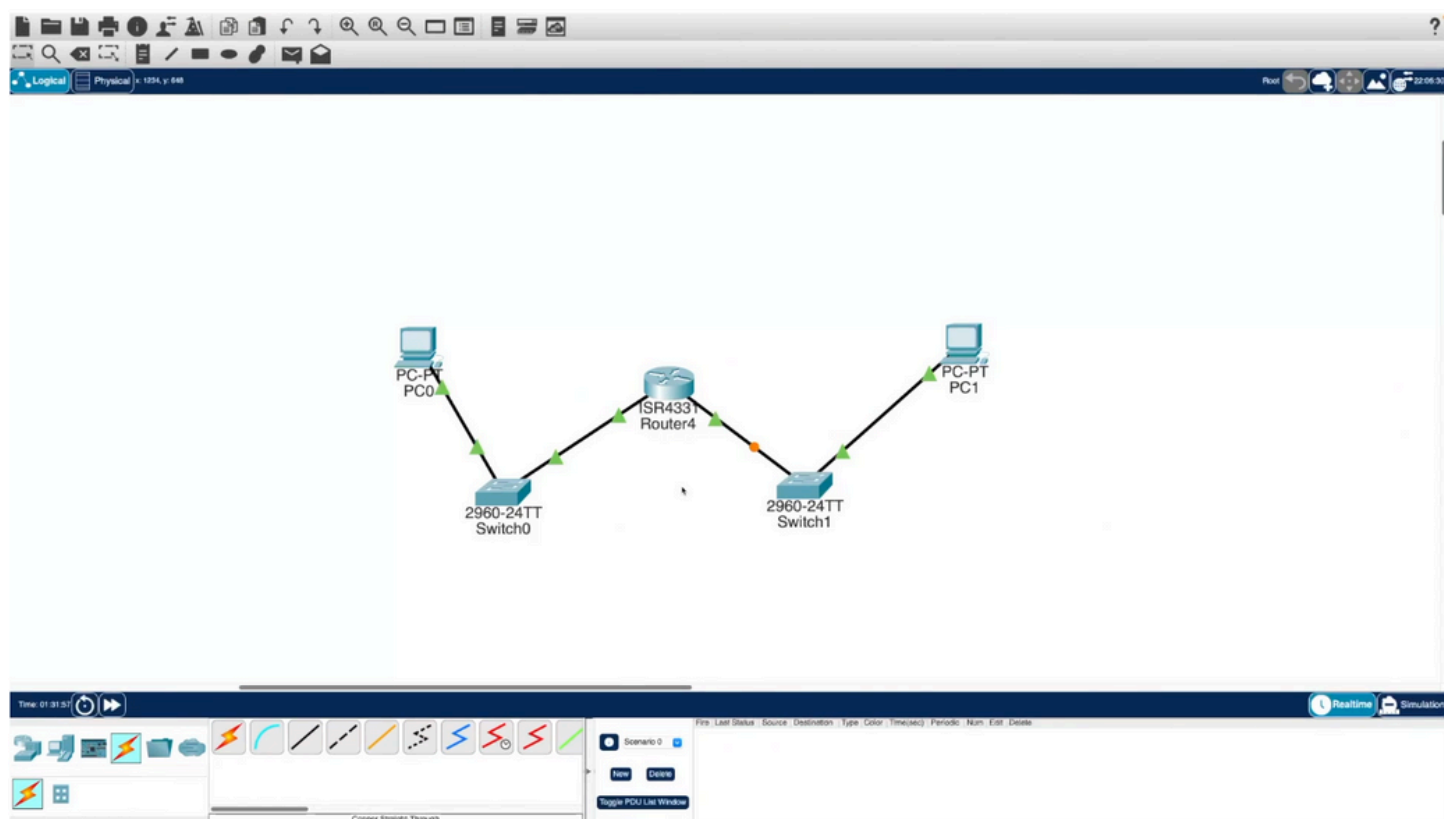
Simulación de firewall usando Packet Tracer de Cisco y la CLI de Cisco para crear las reglas de configuración del router.







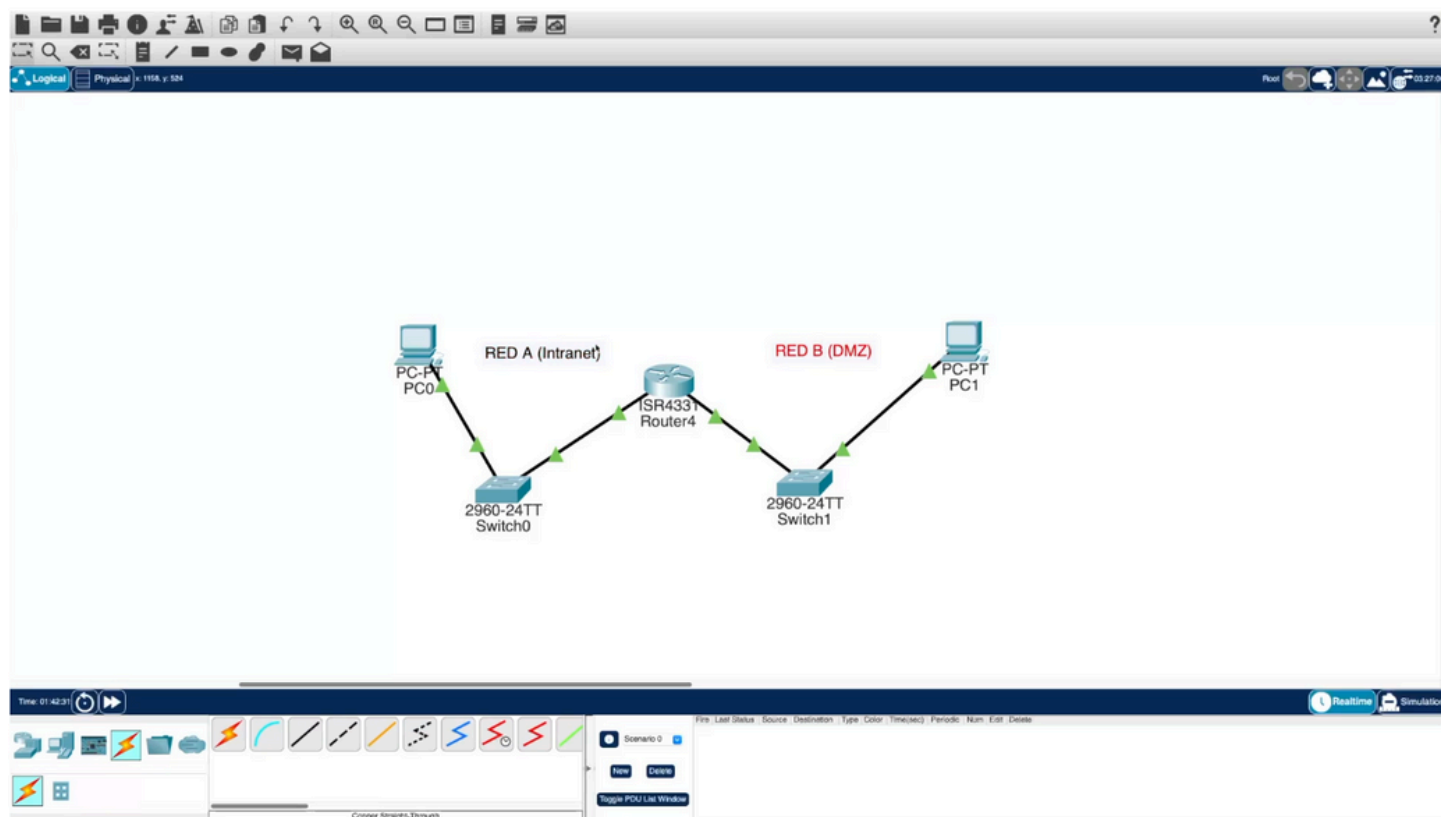
Ahora la otra también se ha completado (verde).



Ahora vamos a crear la ACL (access list) y configurarla con sus reglas, dando acceso primero con permit, luego limitamos el acceso con deny. También limitamos el ip que no entre en esta regla con ip any any. Ahora que la ACL está creada tenemos que aplicarla.

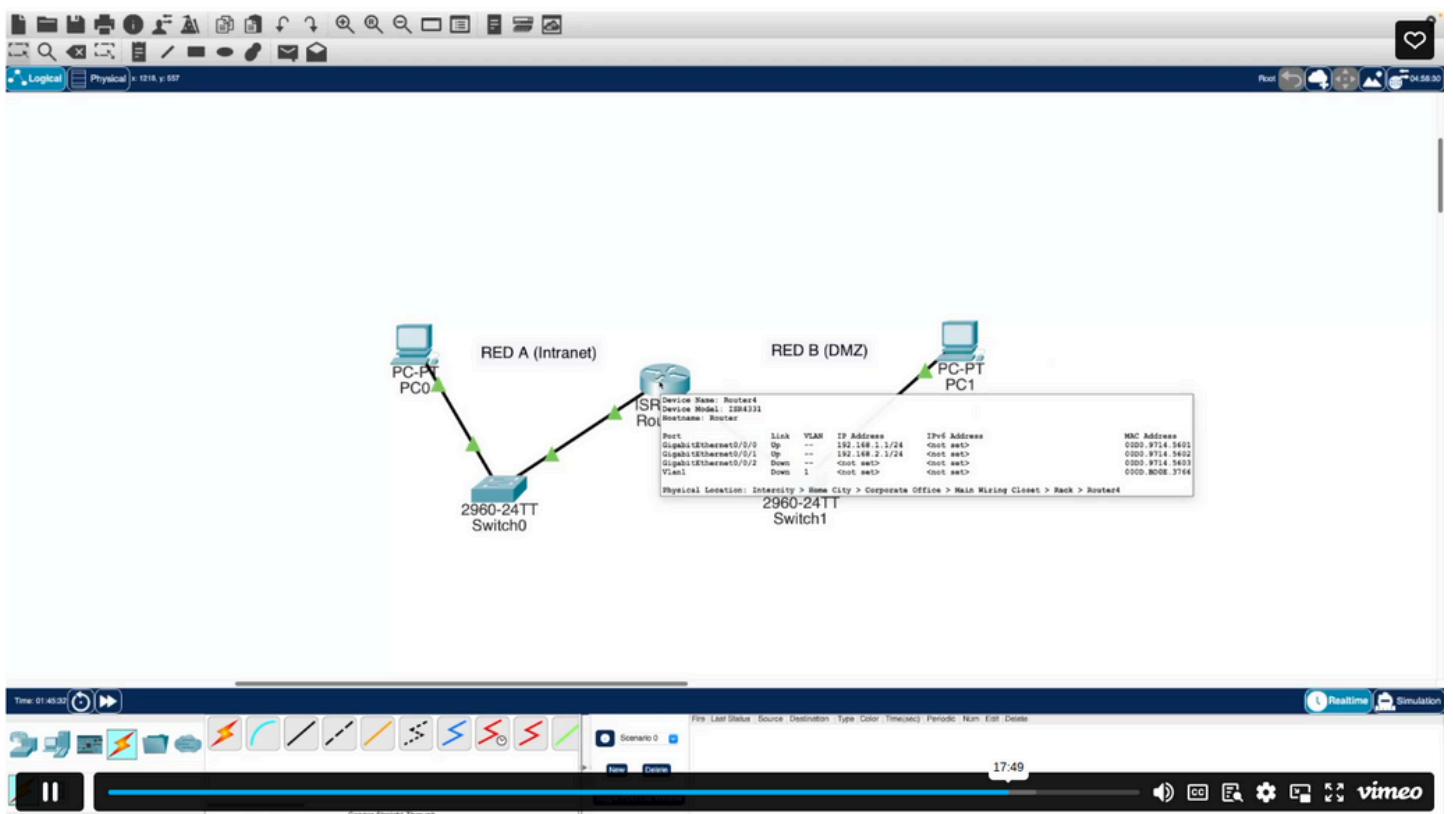
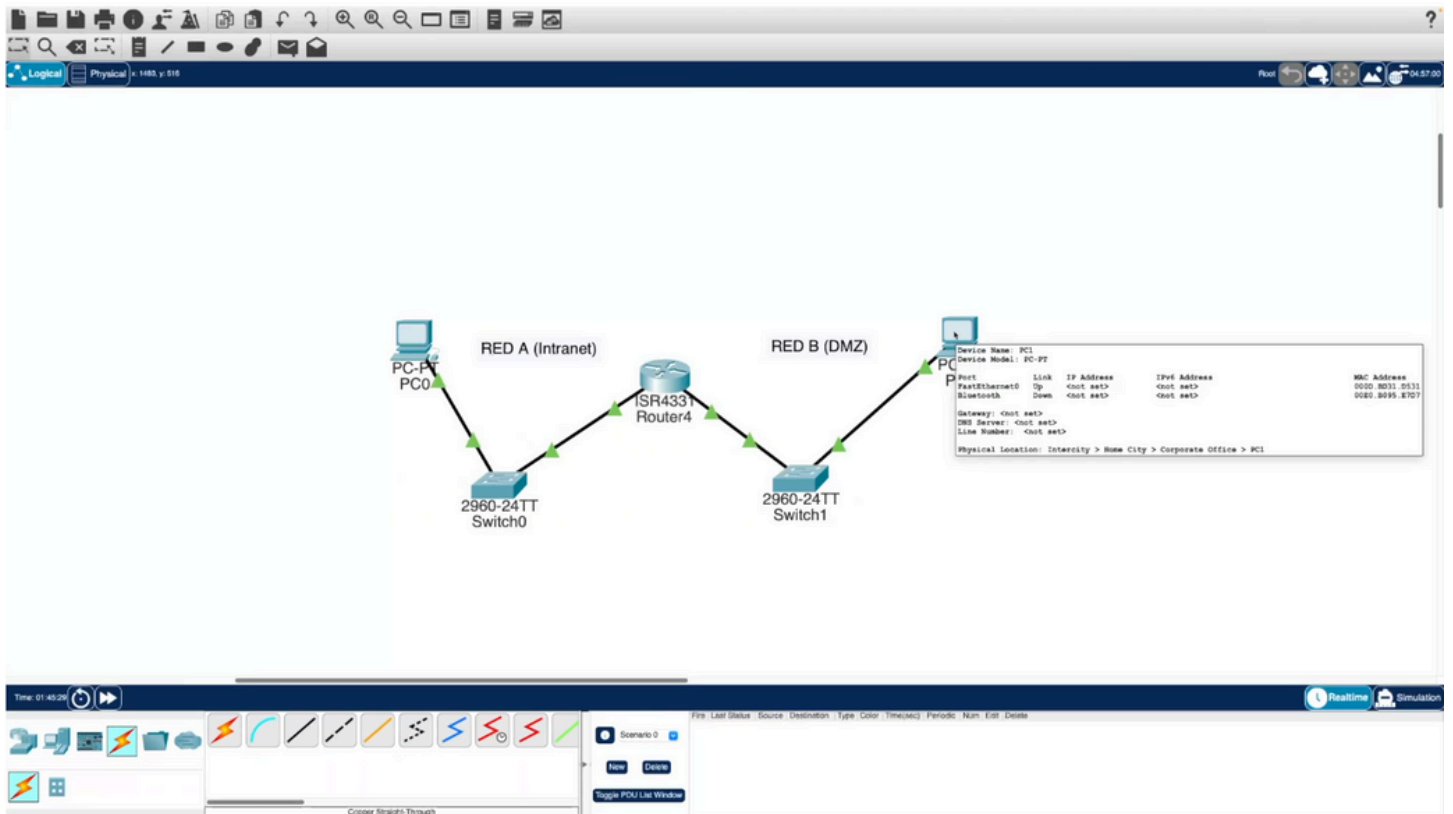
```
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

Ahora haremos las pruebas, recordemos que la red A es el pc de la izquierda con el switch (la intranet), y la red B es el pc de la derecha con su switch (la DMZ). Hemos habilitado el tráfico de la red A a la red B pero no hemos creado el acceso para que vaya de la red B a la red A. Es el principio de las DMZ, que ella puede comunicarse con los demás pero éstos no pueden comunicarse con la DMZ. Testeemos éstas reglas.



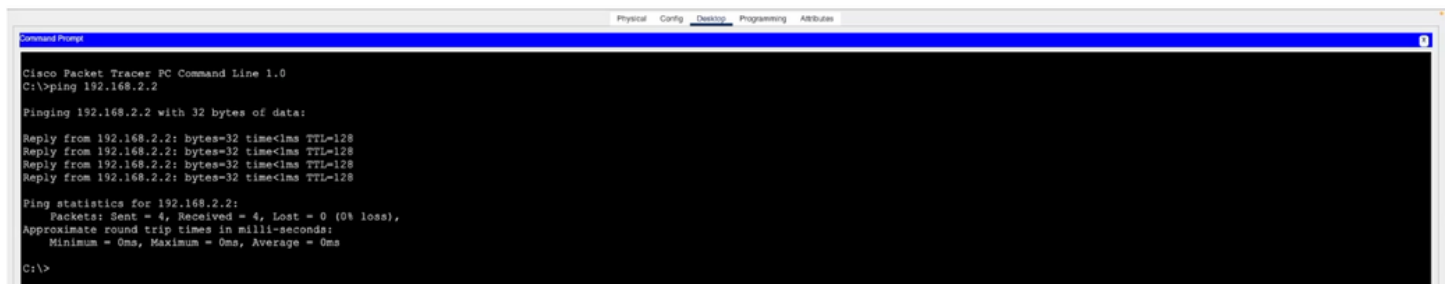
Asignamos una ip al pc de la red A.





Ahora que hay ip en ambos pc y hay conectividad podemos hacer la primera prueba.

De la red A a la red B se puede hacer ping, tal y cómo lo habíamos previsto.



```
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

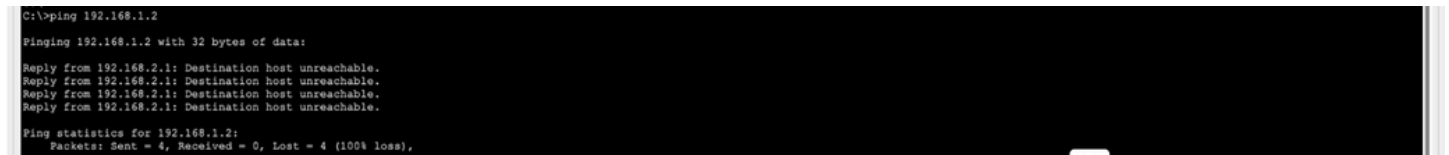
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

De la red B a la red A no se envía el ping, así que tal y cómo hemos configurado no llegan los paquetes.



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```