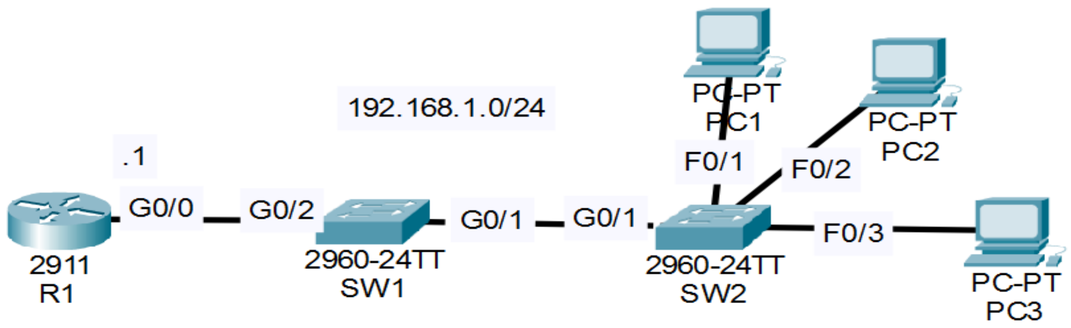
Network Topology:



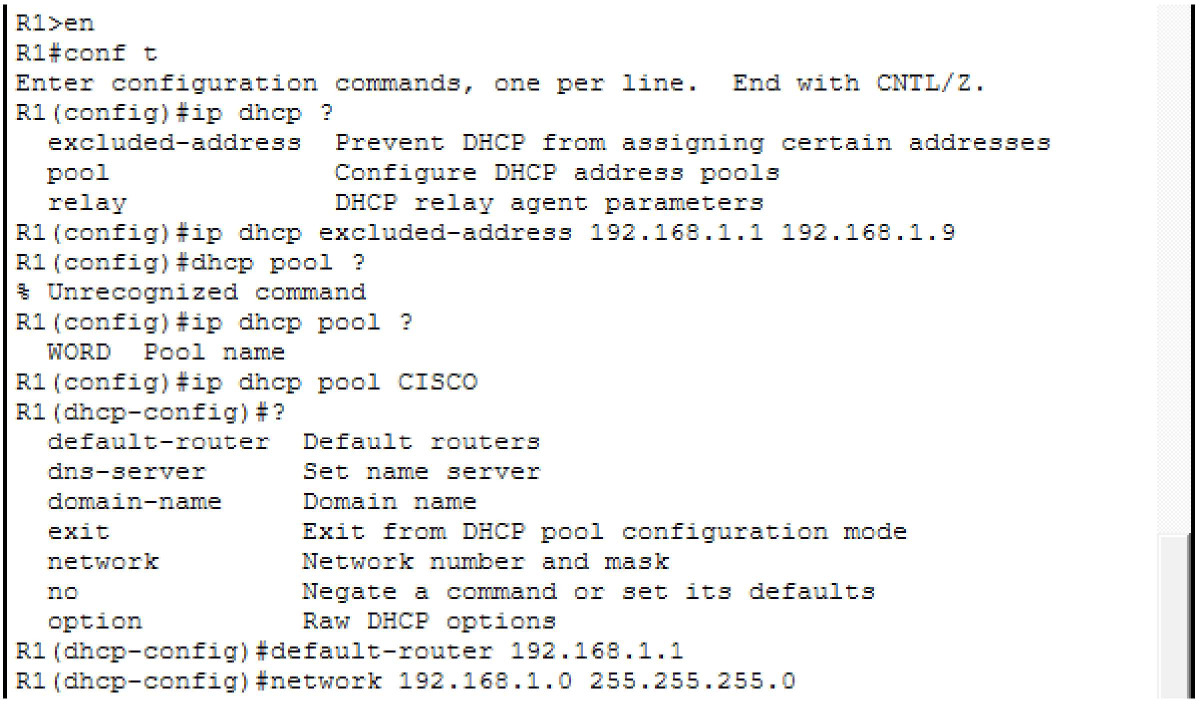
Instructions and actions:

1. Configure R1 as a DHCP server.

   Exclude 192.168.1.1 - 192.168.1.9 from the pool

   Default gateway: R1

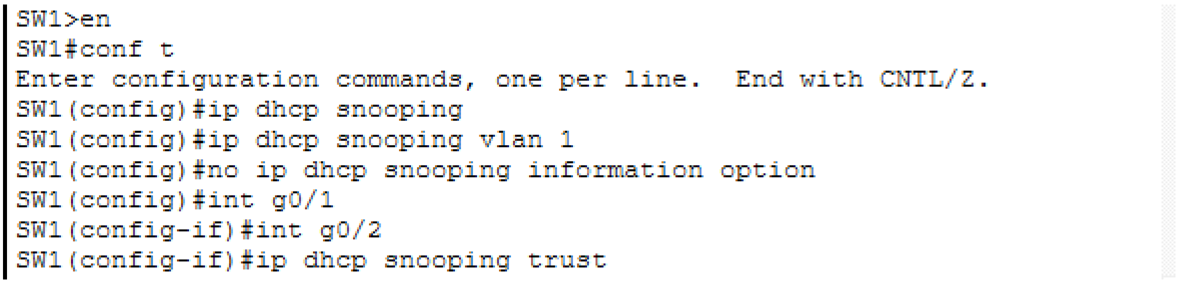
   R1 CLI:



```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp ?
  excluded-address  Prevent DHCP from assigning certain addresses
  pool              Configure DHCP address pools
  relay             DHCP relay agent parameters
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9
R1(config)#dhcp pool ?
% Unrecognized command
R1(config)#ip dhcp pool ?
  WORD  Pool name
R1(config)#ip dhcp pool CISCO
R1(dhcp-config)#?
  default-router  Default routers
  dns-server      Set name server
  domain-name     Domain name
  exit            Exit from DHCP pool configuration mode
  network         Network number and mask
  no              Negate a command or set its defaults
  option          Raw DHCP options
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
```

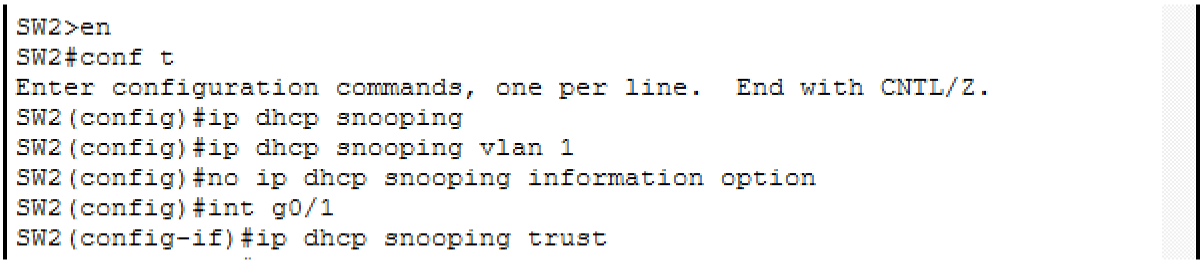
2. Configure DHCP snooping on SW1 and SW2.

   SW1 CLI:



```
SW1>en
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#no ip dhcp snooping information option
SW1(config)#int g0/1
SW1(config-if)#int g0/2
SW1(config-if)#ip dhcp snooping trust
```

   SW2 CLI:

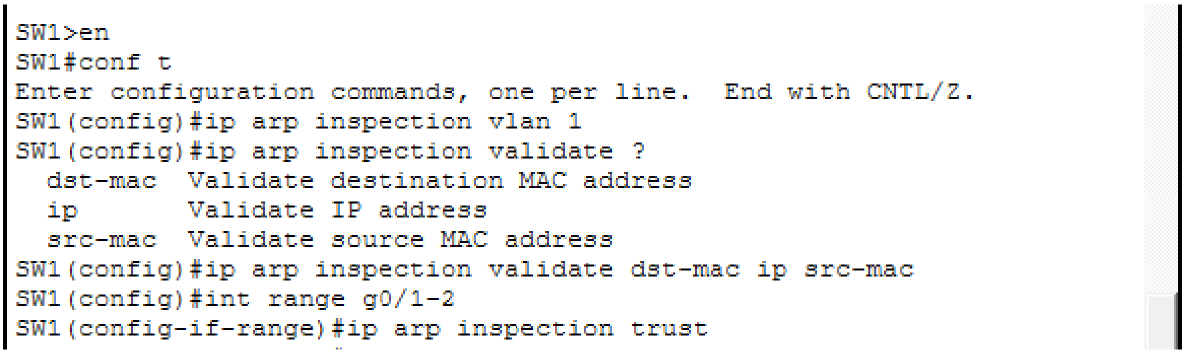


```
SW2>en
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#ip dhcp snooping
SW2(config)#ip dhcp snooping vlan 1
SW2(config)#no ip dhcp snooping information option
SW2(config)#int g0/1
SW2(config-if)#ip dhcp snooping trust
```

3. Configure DAI on SW1 and SW2.
    - Enable all additional validation checks
    - Trust ports connected to a router or a switch

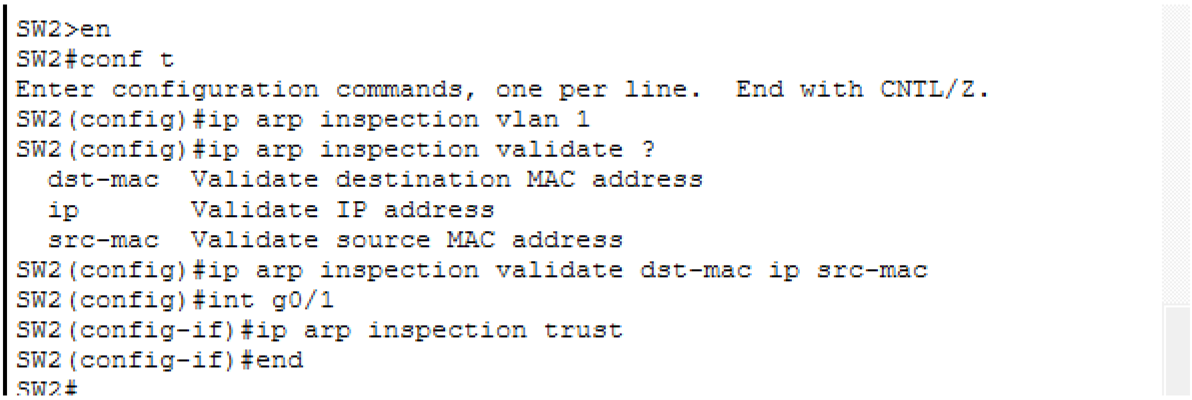
DAI stands for Dynamic ARP Inspection.

SW1 CLI:



```
SW1>en
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#ip arp inspection vlan 1
SW1(config)#ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP address
  src-mac  Validate source MAC address
SW1(config)#ip arp inspection validate dst-mac ip src-mac
SW1(config)#int range g0/1-2
SW1(config-if-range)#ip arp inspection trust
```

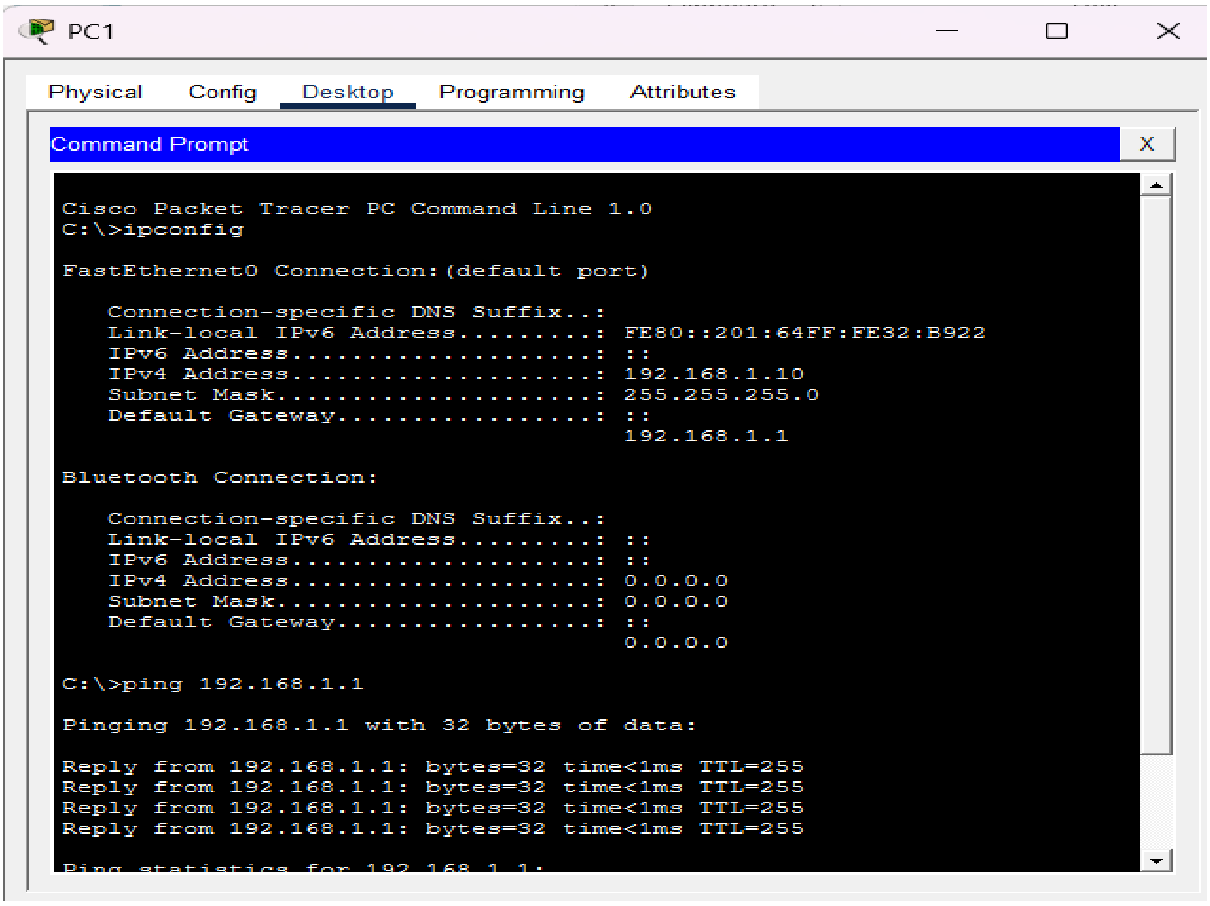
SW2 CLI:



```
SW2>en
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#ip arp inspection vlan 1
SW2(config)#ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP address
  src-mac  Validate source MAC address
SW2(config)#ip arp inspection validate dst-mac ip src-mac
SW2(config)#int g0/1
SW2(config-if)#ip arp inspection trust
SW2(config-if)#end
SW2#
```

4. Check

PC1 Command Prompt:



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:64FF:FE32:B922
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.1

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

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
```