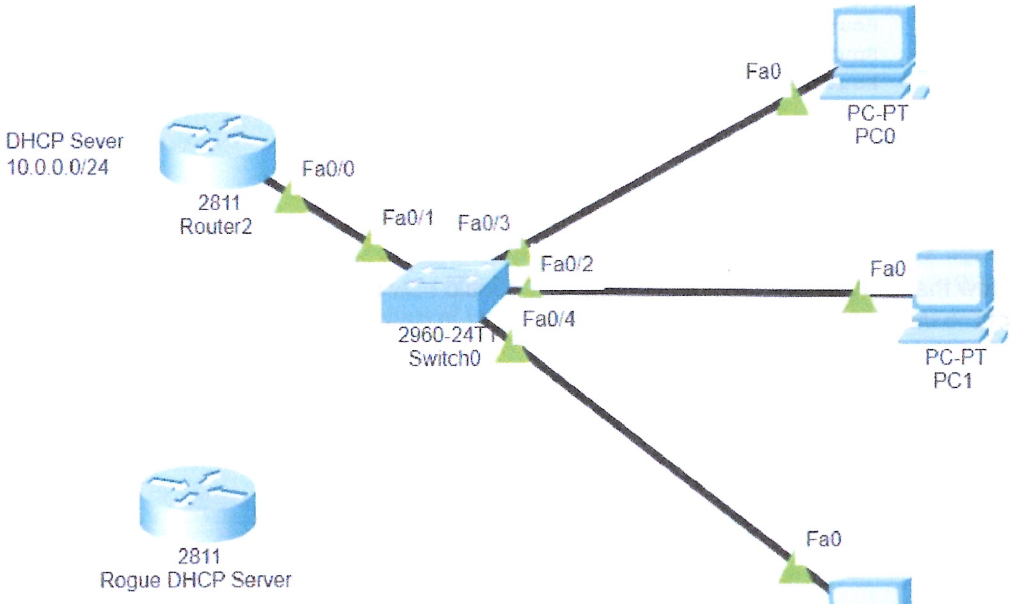
IFT 266 Introduction to Network Information Communication Technology

Lab 17

DHCP Snooping

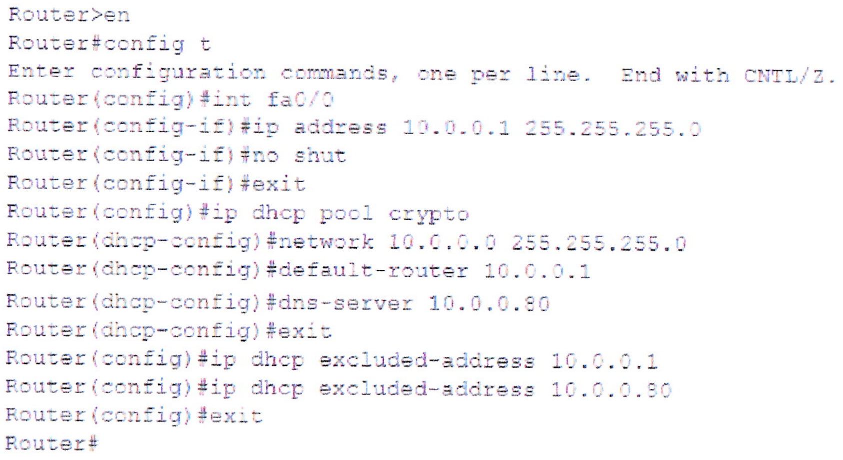
After you complete each step, put an 'x' in the completed box
or
Attach a screenshot where prompted

1. Create the following network topology on Packet Tracer



Completed ☒

2. We will now configure Router 2 to act as the legitimate DHCP server.



```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip dhcp pool crypto
Router(dhcp-config)#network 10.0.0.0 255.255.255.0
Router(dhcp-config)#default-router 10.0.0.1
Router(dhcp-config)#dns-server 10.0.0.80
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 10.0.0.1
Router(config)#ip dhcp excluded-address 10.0.0.80
Router(config)#exit
Router#
```

Completed ☒

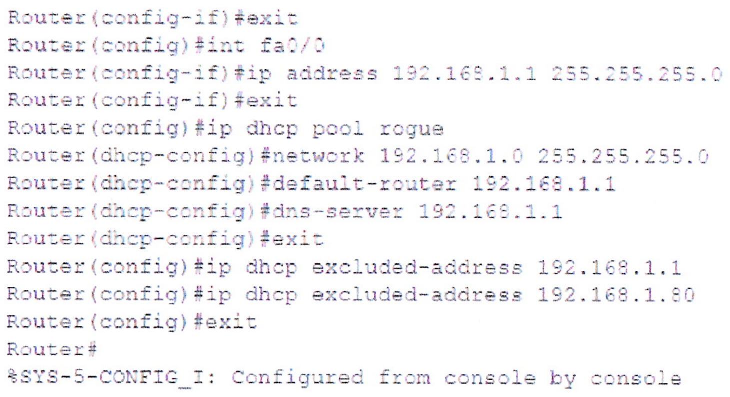
3. Now that DHCP has been configured, you should now be able to assign IP configuration details to each of the three PCs using DHCP.

Insert a screenshot PC0 configuration details below.

4. All the PCs can now communicate with other. Make sure that is the case by having PC0 ping PC1.

Completed ☒

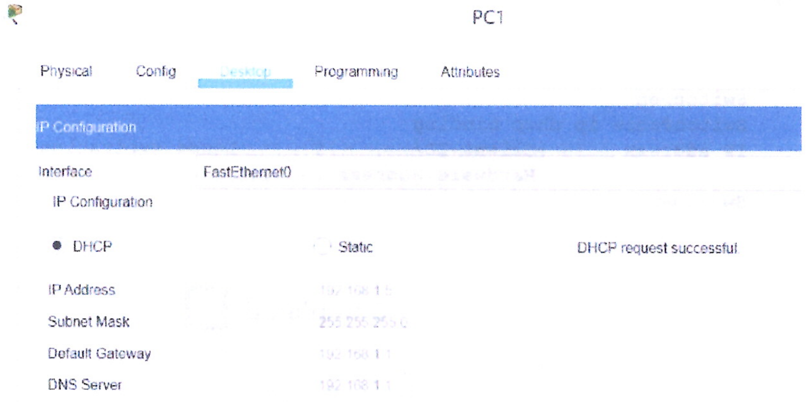
5. Connect the rogue DHCP server (router) to the network switch and configure it as shown below.



```
Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#ip dhcp pool rogue
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#ip dhcp excluded-address 192.168.1.80
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Completed ☒

6. Reconfigure the PCs with their IP configuration details (change it to static and back again to automatic/DHCP) and there a good chance they will receive a valid IP address from the rogue DHCP server (e.g. 192.168.1.x) but it not part of your network (10.0.0.0) as in the image below.



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful

IP Address 192.168.1.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 192.168.1.1

Completed ☒

7. A device (e.g. PC1 as in image in step 6) that requests the IP address will normally take the IP address that gets sent to it first. In this case, the rogue DHCP server.

   This is done to deny clients from working or route their traffic through a sniffer in order to extract private information.

   Easiest solution = DHCP Snooping

   DHCP Snooping tells the switch that DHCP responses may only come from certain ports.
   This port would be the trusted DHCP server.

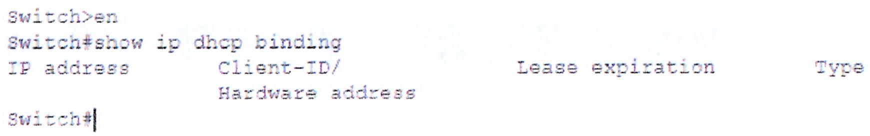
   In our topology, the trusted port would be FA0/1 (connects legitimate DHCP server to switch).
   Remainder of the ports (fa0/2, fa0/3 and fa0/4) are untrusted ports.

   Completed ☒

8. We will now configure DHCP snooping on the switch as DHCP snooping is not enabled by default.

   Before we start the switch configuration, we will run the "show ip dhcp binding" command which shows us that none of the IP addresses are binded with any of the hardware addresses.

   The binding table is stored locally in memory but can be exported to TFTP server is required.

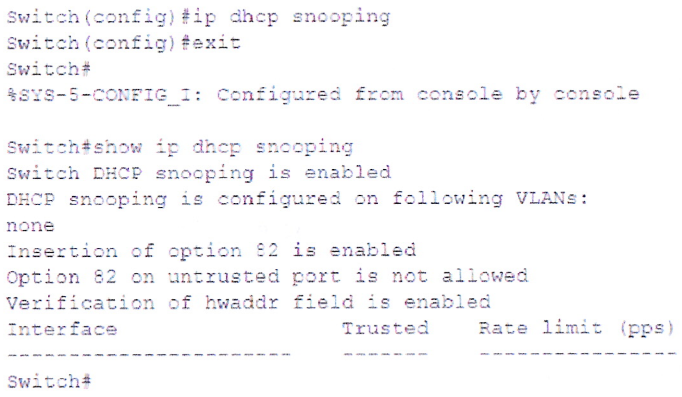


```
Switch>en
Switch#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
Switch#
```

Completed ☒

9. To enable DHCP Snooping, we use the global command “ip dhcp snooping” command.

   To verify that DHCP snooping is enabled, we can run the “show ip dhcp snooping” command.



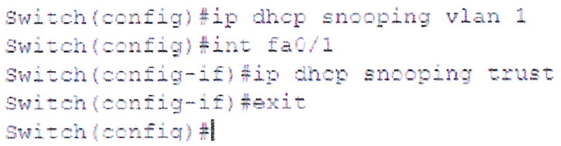
```
Switch(config)#ip dhcp snooping
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
Switch#
```

Completed ☒

10. We will now configure the VLANs that you want to protect using the “ip dhcp snooping VLAN 1” command.

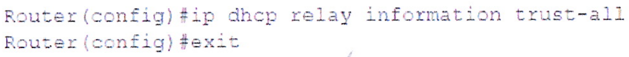
    DHCP is built on the concept of using 1 or more trusted ports (i.e. fa0/1) that have being identified as having a legitimate DHCP server attached.



```
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#
```

Completed ☒

11. One more command is required on the legitimate DHCP server (router) – “ip dhcp relay information trust-all”



```
Router(config)#ip dhcp relay information trust-all
Router(config)#exit
```

Completed ☒

12. As clients communicate on the network, the switch builds a binding table. This binding table is a database that lists the clients MAC address, DHCP assigned address, switch port, VLAN and remaining DHCP leased time.

    Now go back into each of the 3 (three) PCs and reconfigure the PCs with their IP configuration details (change it to static and back again to automatic/DHCP).

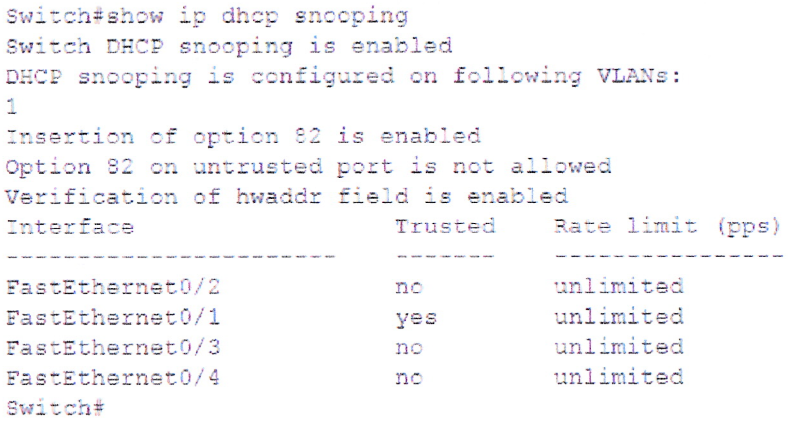
    This time you will only receive the correct IP address in the range 10.0.0.0 network as only the legitimate DHCP server is assigning IPs to the clients.

Completed ☒

13. We will now run the "show ip dhcp snooping" command on the switch.

    The switch filters any DHCP server messages from untrusted ports i.e. fa0/2, fa0/3 and fa0/4 in order to protect the integrity of legitimate DHCP server and their operation.

    Fa0/1 is the only trusted port among all the ports as the remaining are untrusted.



```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                   Trusted    Rate limit (pps)
-----------------------     -------    ----------------
FastEthernet0/2             no         unlimited
FastEthernet0/1             yes        unlimited
FastEthernet0/3             no         unlimited
FastEthernet0/4             no         unlimited
Switch#
```

Completed ☒

14. Now add 2 more PCs to the original topology and configure them using DHCP.

    They should receive their details for the 10.0.0.0 network thus the trusted DHCP server.

Completed ☒

15. Go back into the switch and once again run the "show ip dhcp snooping" command to confirm the addition of the two untrusted ports.

    Fa0/1 should still be the only trusted port.

    Insert a screenshot of the result of the "show ip dhcp snooping" command which should show Fa0/1 as the only trusted port and now with five (5) untrusted ports.

↓