Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Build the following network in Cisco Packet Tracer.

g0/0/0

g0/0/1

* 2. Configure the interfaces on the router as follows:

*Router(config)#interface g0/0/0*

*Router(config-if)#ip address 192.168.2.1 255.255.255.0*

*Router(config-if)#no shutdown*

*Router(config)#interface g0/0/1*

*Router(config-if)#ip address 192.168.1.1 255.255.255.0*

*Router(config-if)#no shutdown*

* 3. Configure the PCs as follows:
	1. PC1: IP Address 192.168.1.5 subnet mask 255.255.255.0, gateway 192.168.1.1
	2. PC2: IP Address 192.168.1.6 subnet mask 255.255.255.0, gateway 192.168.1.1
	3. PC1: IP Address 192.168.2.5 subnet mask 255.255.255.0, gateway 192.168.2.1

# Classifying Traffic

* 4. Here we will just classify traffic and not really apply any quality of service actions to it. We will create a classification for any web traffic coming into R1 on interface g0/0/1. Type in the following commands:

**First we need to create the rule that specifies web traffic. We do this by creating an access list looking for any traffic on port 80.**

*Router(config)#ip access-list extended WEB\_BROWSING\_ACL*

*Router(config-ext-nacl)#permit tcp any any eq 80*

**Next we create a class (I’ll call it WEB\_BROWSING\_CLASS) and have it match on the access list I just created.**

*Router(config-ext-nacl)class-map WEB\_BROWSING\_CLASS*

*Router(config-cmap)#match access-group name WEB\_BROWSING\_ACL*

**Now create a policy (I’ll call it CLASSIFY\_WEB) and have it use the class map I just created.**

*Router(config-cmap)#policy-map CLASSIFY\_WEB*

*Router(config-pmap)#class WEB\_BROWSING\_CLASS*

**Now it must be applied to an interface, in this case we want to classify the traffic coming into g0/0/1.**

*Router(config-pmap)#interface GigabitEthernet 0/1*

*Router(config-if)#service-policy input CLASSIFY\_WEB*

* 5. Type in the following command:

*Router#show policy-map interface g0/0/1*



How many web packets show up in the class? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 6. Now click on PC2, click on Desktop and select Traffic Generator. Set the following parameters as shown in the screenshot below.
* 7. Click on the Send button below just once. Type in the following command in the router again.

*Router#show policy-map interface g0/0/1*



How many web packets show up in the class? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Marking Traffic

* 8. Now we will give the packets from PC2 a higher priority than the packets coming from PC1. Type in the following commands

**First create the rule:**

*Router(config)#access-list 110 permit ip host 192.168.1.6 any*

**Then create the class called IMPORTANT and have it match on the rule we just created.**

*Router(config)#class-map match-all IMPORTANT*

*Router(config-cmap)# match access-group 110*

**The create a policy called SETDSCP and set any packets from the class IMPORTANT set to “ef” which is a higher priority than the default packets usually set to 0.**

*Router(config-cmap)#policy-map SETDSCP*

*Router(config-pmap)#class IMPORTANT*

*Router(config-pmap-c)# set ip dscp ef*

**Now apply the policy to the interface g0/0/1 where PC2 is attached and on inbound traffic set anything from PC2 to “ef”.**

*Router(config-pmap-c)# interface g0/0/1*

*Router(config-if)#service-policy input SETDSCP*

*Router(config-if)#end*

* 9. Type in the following command:

*Router#show policy-map interface g0/0/1*



How many packets are marked with dscp ef? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 10. Now from PC1, ping PC3. Now run the command *show policy-map interface g0/0/1.* Did the number of packets marked “ef” increase? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Paste your output below.
* 11. Now from PC2, ping PC3. Now run the command *show policy-map interface g0/0/1.* Did the number of packets marked “ef” increase? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Paste your output below.

End of Procedure