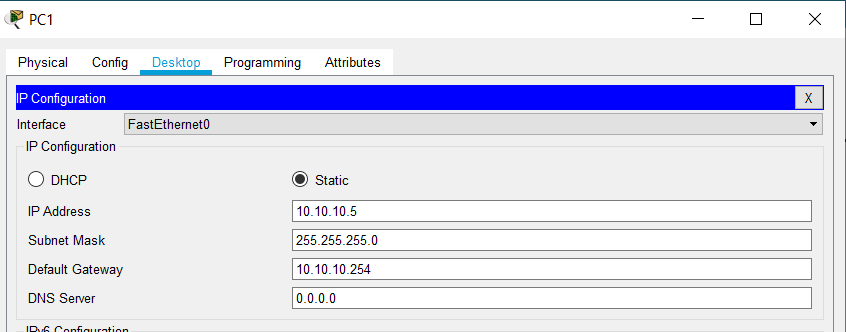
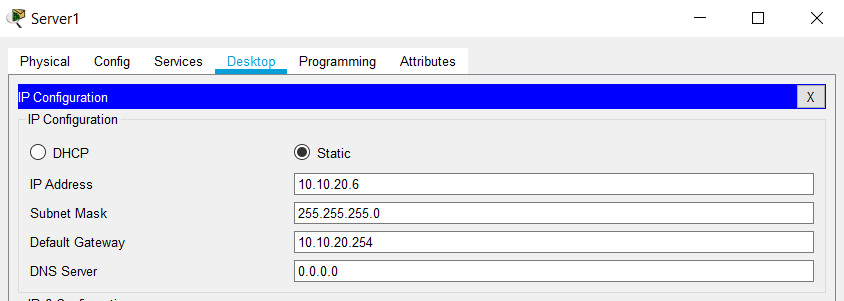


1. **Assign IP addresses to PC, Server and router.**





Router –

Router>enable

Router#configure terminal

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 10.10.30.6 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface FastEthernet1/0

Router(config-if)#ip address 142.3.2.5 255.255.255.0

Router(config-if)#no shutdown

1. **Enter VLAN database data to L3 switch**

Switch>enable

Switch#vlan database

Switch(vlan)#vlan 10 name Students

Switch(vlan)#vlan 20 name Lecturers

Switch(vlan)#exit

Switch(config)#interface vlan10

Switch(config-if)#ip address 10.10.10.254 255.255.255.0

Switch(config-if)#exit

Switch(config)#interface vlan20

Switch(config-if)#ip address 10.10.20.254 255.255.255.0

Switch(config-if)#exit

1. **Enter IP address for L3 switch 0/3 interface**

Switch(config)#interface fa0/3

Switch(config-if)#no switchport

Switch(config-if)#ip address 10.10.30.5 255.255.255.0

Switch(config-if)#exit

1. **Trunk ports as L3 switch’s 0/1 and 0/2 interfaces**

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#exit

Switch(config)#interface fa0/2

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#ip routing

Switch(config)#ip routing

1. **Enter dynamic routing (RIP) details to router**

Switch(config)#router rip

Switch(config-router)#network 10.10.10.0

Switch(config-router)#network 10.10.20.0

Switch(config-router)#network 10.10.30.0

Switch(config-router)#exit

1. **Add VLAN data for both L2 switches and add PC VLAN data to interfaces of L2 switches**

Switch0 Switch>enable

Switch0 Switch#vlan database

Switch0 Switch(vlan)#vlan 10 name Students

Switch0 Switch(vlan)#vlan 20 name Lecturers

Switch0 Switch(vlan)#exit

Switch0 Switch#configure terminal

Switch0 Switch(config)#interface FastEthernet0/1

Switch0 Switch(config-if)#switchport access vlan 10

Switch0 Switch(config-if)#exit

Switch0 Switch(config)#interface FastEthernet1/1

Switch0 Switch(config-if)#switchport access vlan 20

Switch0 Switch(config-if)#exit

Switch0 Switch(config)#interface FastEthernet2/1

Switch0 Switch(config-if)#switchport access vlan 10

Switch1 Switch>enable

Switch1 Switch#vlan database

Switch1 Switch(vlan)#vlan 10 name Students

Switch1 Switch(vlan)#vlan 20 name Lecturers

Switch1 Switch(vlan)#exit

Switch1 Switch#configure terminal

Switch1 Switch(config)#interface FastEthernet0/1

Switch1 Switch(config-if)#switchport access vlan 20

Switch1 Switch(config-if)#exit

Switch1 Switch(config)#interface FastEthernet1/1

Switch1 Switch(config-if)#switchport access vlan 20

Switch1 Switch(config-if)#switchport access vlan 10

1. **Make 3/1 interface of L2 switch and 2/1 interface of other L2 switch as Trunks.**

Switch0 Switch(config-if)#exit

Switch0 Switch(config)#interface fa3/1

Switch0 Switch(config-if)#switchport mode trunk

Switch1 Switch(config-if)#exit

Switch1 Switch(config)#interface fa2/1

Switch1 Switch(config-if)#switchport mode trunk

Switch1 Switch(config-if)#exit

1. **Enter dynamic routing (rip) details to router**

Router#configure terminal

Router(config)#router rip

Router(config-router)#network 10.10.30.0

Router(config-router)#network 142.3.2.0

Router(config-router)#exit

1. **Test the computers and servers for ping and traceroute**
2. **Add NAT details to router**

Router>enable

Router#configure terminal

Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255

Router(config)#ip nat pool 4.4.4.10 4.4.4.100 netmask 255.255.255.0

Router(config)#ip nat pool my 4.4.4.10 4.4.4.100 netmask 255.255.255.0

Router(config)#interface fa 0/0

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#interface fa 1/0

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config)#ip nat inside source list 1 pool my

**C. For the L3 switch (Policy 1):**

Switch>enable

Switch#configure terminal

Switch(config)#access-list 2 deny 10.10.10.7

Switch(config)#access-list 2 permit any

Switch(config)#interface fa0/3

Switch(config-if)#ip access-group 2 out

Switch(config-if)#exit

**D.**

**1. For the L3 switch (To remove Policy 1 from L3 switch):**

Switch>enable

Switch#configure terminal

Switch(config)#interface fa 0/3

Switch(config-if)#no ip access-group 2 out

Switch(config-if)#exit

Switch(config)#no access-list 2

Switch(config)#exit

**2. For the Routet (Insert the policy 1)**

Router>enable

Router#configure terminal

Router(config)#access-list 2 deny host 10.10.10.7

Router(config)#access-list 2 permit any

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip access-group 2 in

Router(config-if)#exit

**F.**

**1. For the router (Remove the Policy 1)**

Router>en

Router#configure

Router(config)#interface fa 0/0

Router(config-if)#no ip access-group 2 in

Router(config-if)#exit

Router(config)#no access-list 2

Router(config)#exit

**2. For the router (Insert the Policy 2)**

Router#configure terminal

Router(config)#access-list 3 deny 10.10.10.0 0.0.0.255

Router(config)#access-list 3 permit any

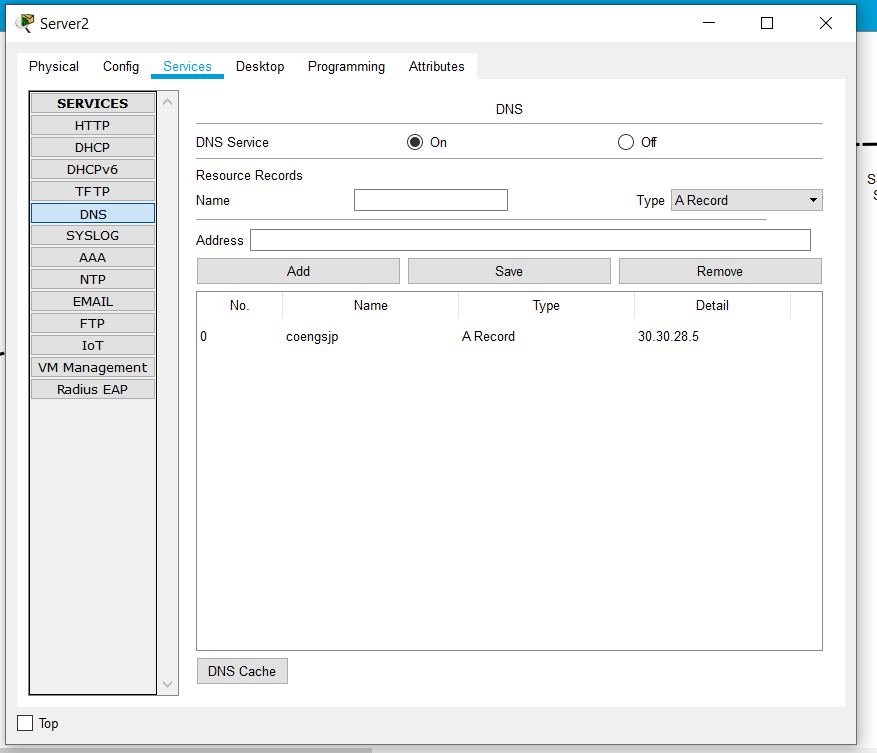
Router(config)#interface fastEthernet 0/0

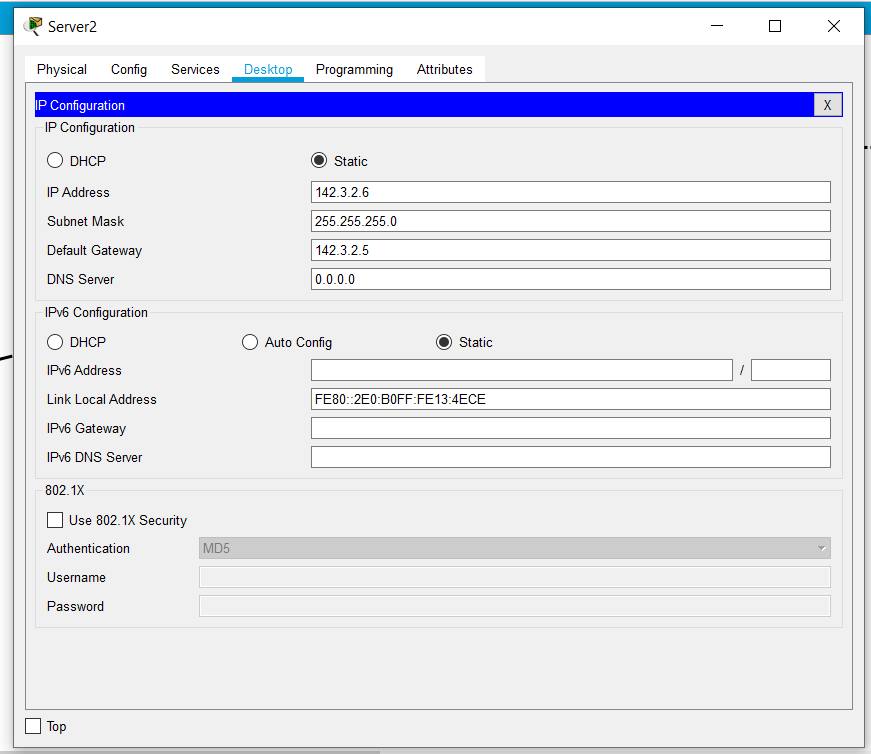
Router(config-if)#ip access-group 3 in

Router(config-if)#exit

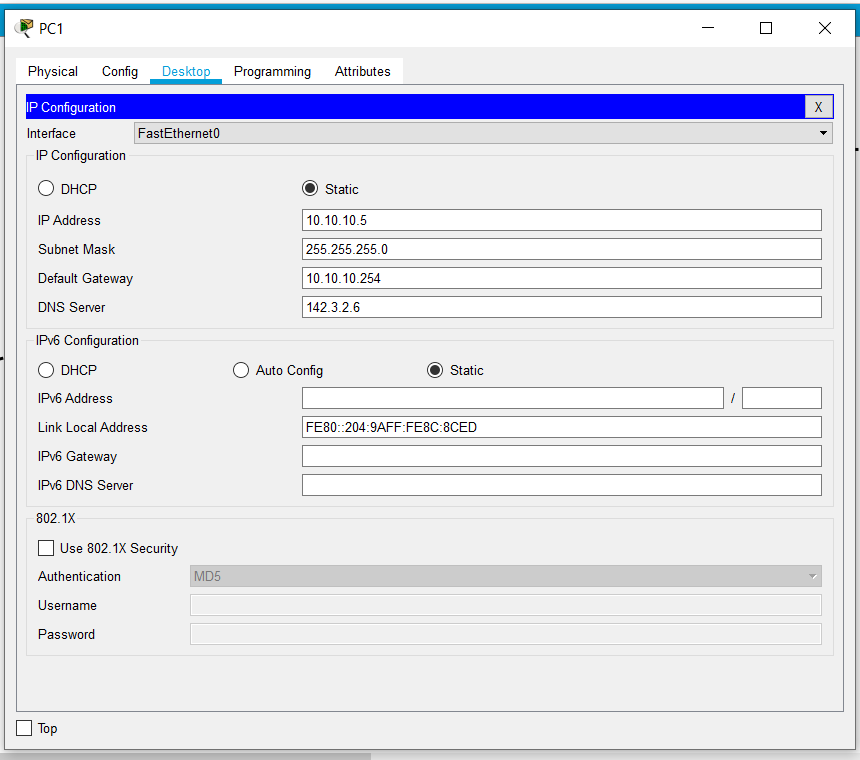
**G.**

**1. Turn on DNS of server and assign a name**





**2. Add DNS to PC and servers**



**3. Remove Policy 2 from router**

Router>enable

Router#configure terminal

Router(config)#interface fa0/0

Router(config-if)#no ip access-group 3 in

Router(config-if)#exit

Router(config)#no access-list 3

Router(config)#exit

0/0 in – As router’s 1/0 is nat, so we are not able to find correct IP addresses

Need static, rip and copy run all to save ACLS

**4. Enter Policy 3 to router**

Router>enable

Router#show access-lists

Router#configure

Router(config)#ip route 0.0.0.0 0.0.0.0 142.3.2.6

Router(config)#ip route 10.10.0.0 255.255.0.0 10.10.30.5

Router(config)#exit

Router#configure terminal

Router(config)#access-list 110 permit udp 10.0.0.0 0.255.255.255 any eq domain

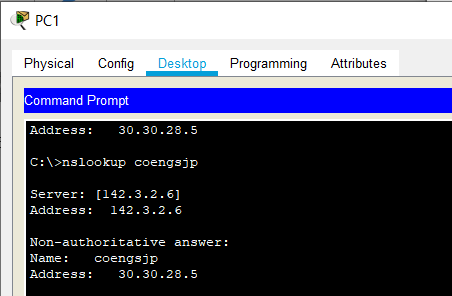
Router(config)#access-list 110 permit tcp 10.0.0.0 0.255.255.255 any eq www

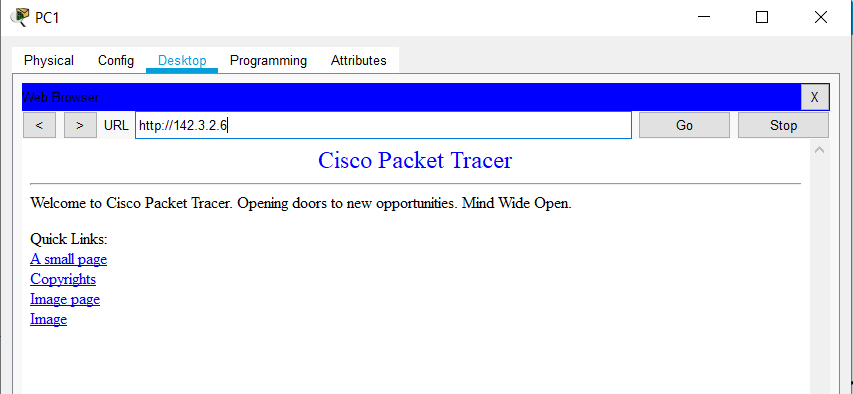
Router(config)#interface fa0/0

Router(config-if)#ip access-group 110 in

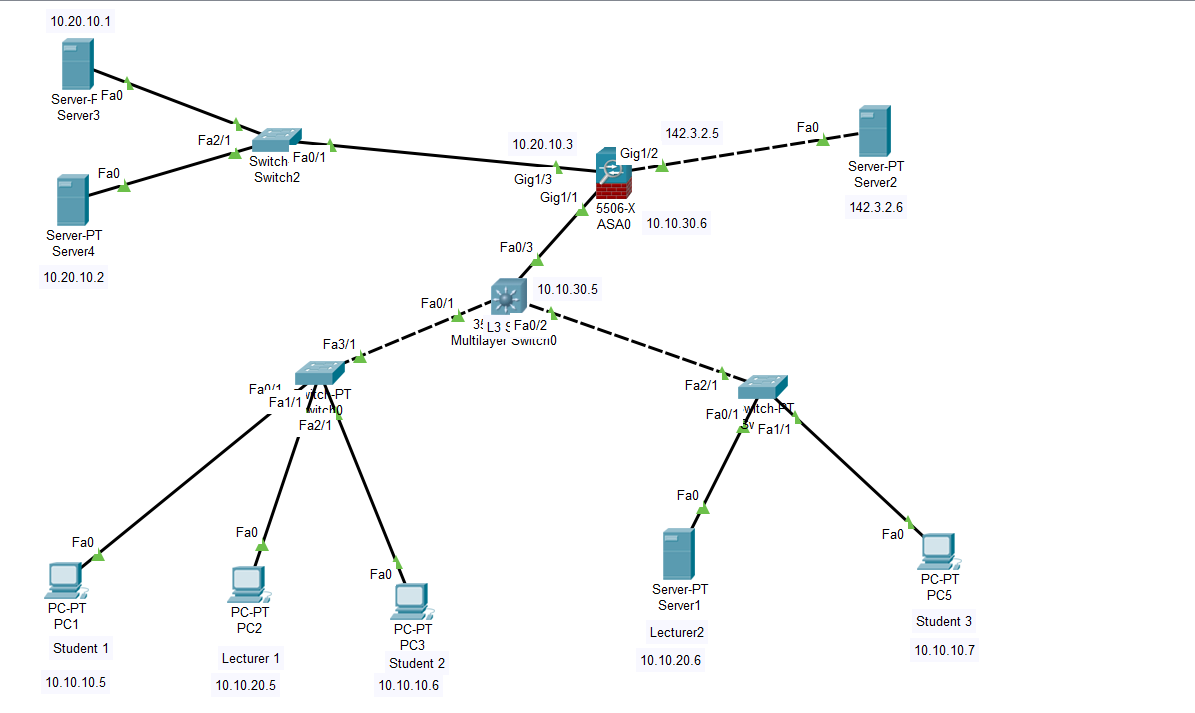
Router(config-if)#exit

Router#copy running-config startup-config





**H.**



**For the ASA5506;**

1. **Assign IP addresses**

ciscoasa#conf t

ciscoasa(config)#int g1/1

ciscoasa(config-if)#nameif inside

ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#ip address 10.10.30.6 255.255.255.0

ciscoasa(config-if)#exit

ciscoasa(config)#int g1/2

ciscoasa(config-if)#nameif outside

INFO: Security level for "outside" set to 0 by default.

ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#ip address 142.3.2.5 255.255.255.0

ciscoasa(config-if)#exit

ciscoasa(config)#

ciscoasa(config)#int g 1/3

ciscoasa(config-if)#nameif dmz

INFO: Security level for "dmz" set to 0 by default.

ciscoasa(config-if)#security-level 50

ciscoasa(config-if)#ip address 10.20.10.3 255.255.255.0

ciscoasa(config-if)#exit

ciscoasa(config)#

1. **Configure NAT to Allow Hosts to Go Out to the Internet**

ciscoasa(config)#object network dmz-subnet

ciscoasa(config-network-object)#subnet 10.20.10.0 255.255.255.0

ciscoasa(config-network-object)#nat (dmz,outside) dynamic interface

ciscoasa(config-network-object)#exit

ciscoasa#conf t

ciscoasa(config)#object network inside-subnet

ciscoasa(config-network-object)#subnet 10.10.0.0 255.255.255.0

ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

ciscoasa(config-network-object)#exit

ciscoasa#

1. **Configure NAT to access web server from the internet**

ciscoasa#conf t

ciscoasa(config)#object network webserver1

ciscoasa(config-network-object)#host 10.20.10.1

ciscoasa(config-network-object)#nat (dmz,outside) static 142.3.2.100

ciscoasa(config-network-object)#exit

ciscoasa#conf t

ciscoasa(config)#object network webserver2

ciscoasa(config-network-object)#host 10.20.10.2

ciscoasa(config-network-object)#nat (dmz,outside) static 142.3.2.101

1. **Configure ACL**

ciscoasa#conf t

ciscoasa(config)#access-list in\_reply extended permit icmp any any echo-reply

ciscoasa(config)#access-list in\_reply extended permit icmp any any unreachable

ciscoasa(config)#

ciscoasa(config)#object network webserver-external-ip

ciscoasa(config-network-object)#host 142.3.2.100

ciscoasa(config-network-object)#exit

ciscoasa#conf t

ciscoasa(config)#access-list in\_reply extended permit tcp any object webserver1 eq www

ciscoasa(config)#access-list in\_reply extended permit tcp any object webserver2 eq www

ciscoasa(config)#access-list in\_reply extended permit tcp any host 142.3.2.100 eq www

ciscoasa(config)#access-list in\_reply extended permit tcp any host 142.3.2.101 eq www

ciscoasa(config)#access-group in\_reply in interface outside

1. **Enter dynamic routing**

ciscoasa(config)#router rip

ciscoasa(config-router)#network 10.0.0.0

ciscoasa(config-router)#network 142.3.2.0

ciscoasa(config-router)#exit

ciscoasa(config)#access-list inside\_web extended permit tcp any any eq www

1. **Insert access group**

ciscoasa#conf t

ciscoasa(config)#access-list 110 extended permit tcp 10.10.0.0 255.255.0.0 any eq www

ciscoasa(config)#access-list 110 extended permit tcp any eq www 10.10.0.0 255.255.0.0

ciscoasa(config)#access-list 110 extended permit tcp any eq www 10.20.10.0 255.255.255.0

ciscoasa(config)#access-list 110 extended permit tcp any host 142.3.2.101 eq www

ciscoasa(config)#access-list 110 extended permit tcp any host 142.3.2.100 eq www

ciscoasa(config)#access-list 120 extended permit tcp any eq www 10.10.0.0 255.255.0.0

ciscoasa(config)#access-list 130 extended permit tcp any eq www 10.20.10.0 255.255.255.0

ciscoasa(config)#access-group 110 in interface outside

ciscoasa(config)#access-group 130 in interface dmz

ciscoasa(config)#access-group 120 in interface inside

ciscoasa(config)#exit

1. **Insert static routing**

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 142.3.2.6

ciscoasa(config)#route inside 10.10.0.0 255.255.0.0 10.10.30.5

ciscoasa(config)#exit

1. **Access list**

ciscoasa(config)#access-list 130 extended permit udp any any

ciscoasa(config)#access-list 120 extended permit udp any any

ciscoasa(config)#access-list 110 extended permit udp any any

ciscoasa(config)#access-group 130 in interface dmz

ciscoasa(config)#access-group 120 in interface inside

ciscoasa(config)#access-group 110 in interface outside

ciscoasa(config)#exit

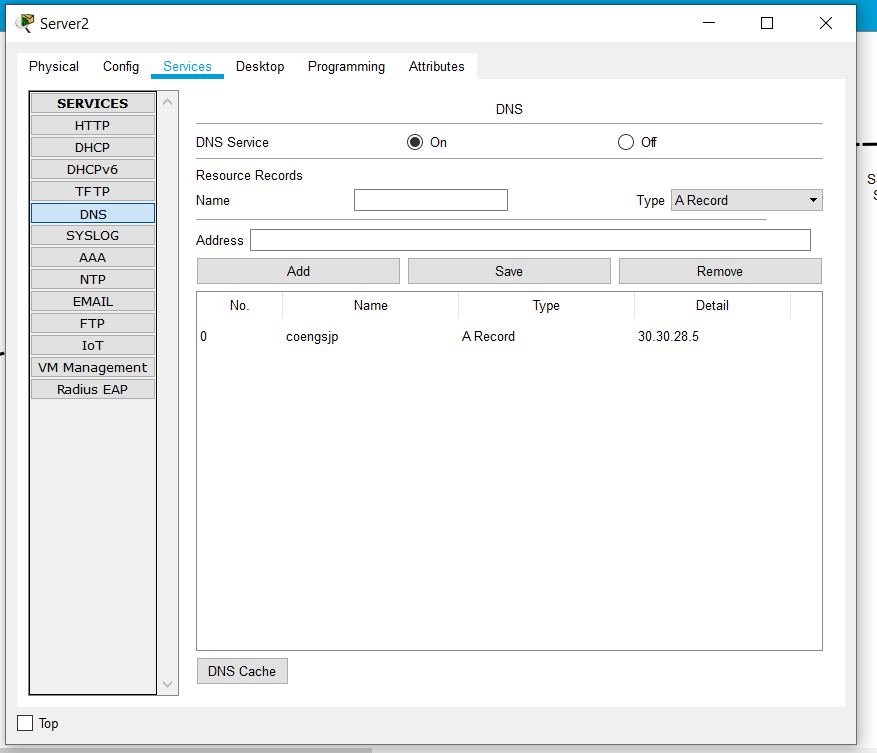
ciscoasa#configure terminal

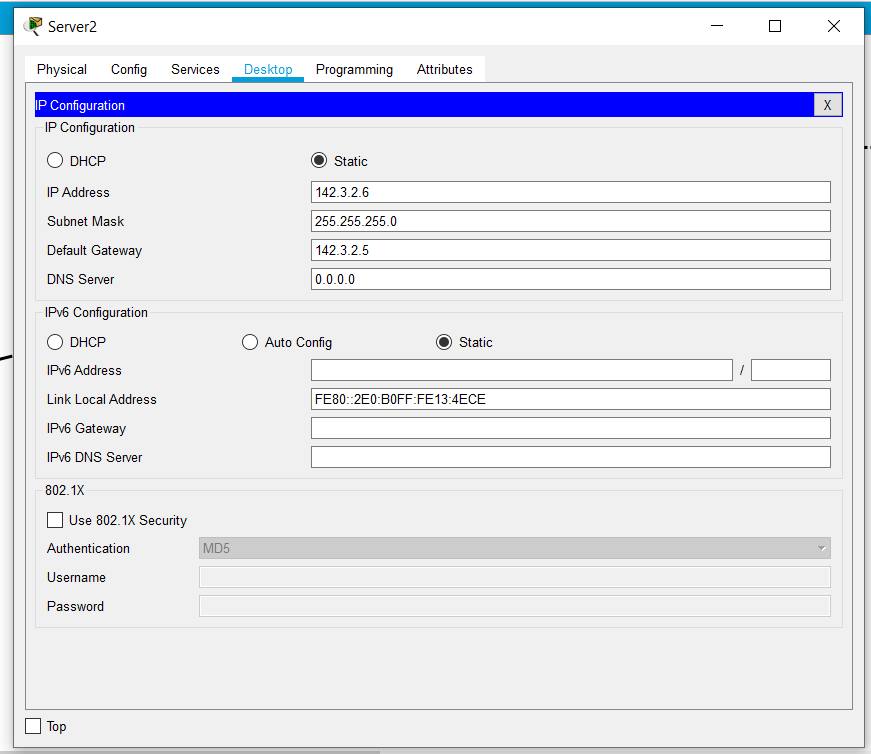
ciscoasa(config)#access-list 130 extended permit tcp 10.20.10.0 255.255.255.0 eq www 10.10.0.0 255.255.0.0

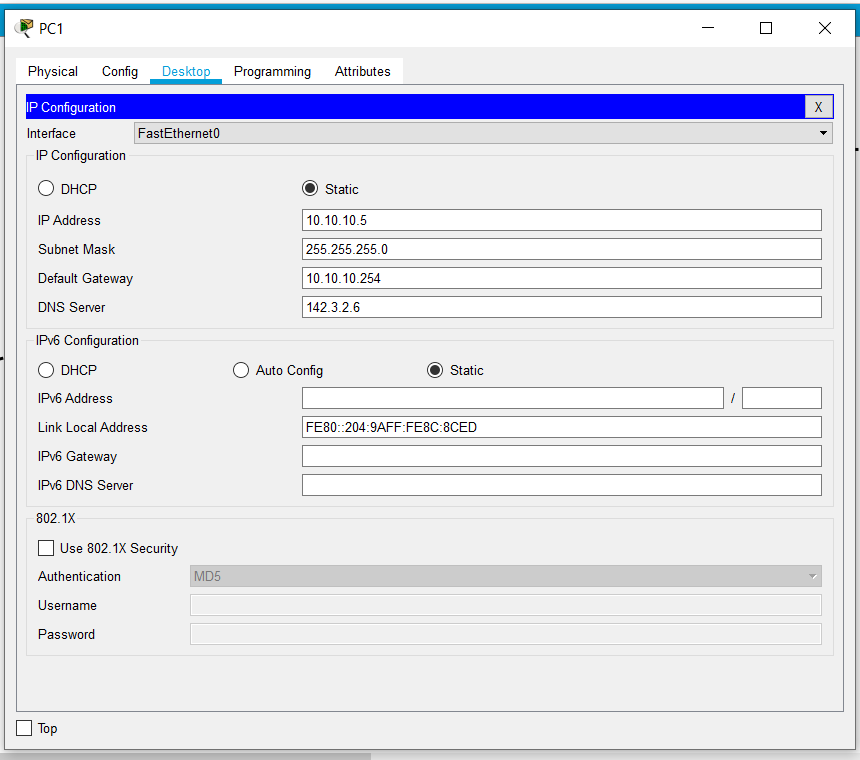
Tue Dec 8 18:52:01 2020 ASA0 ciscoasa(config)#access-group 130 in interface dmz

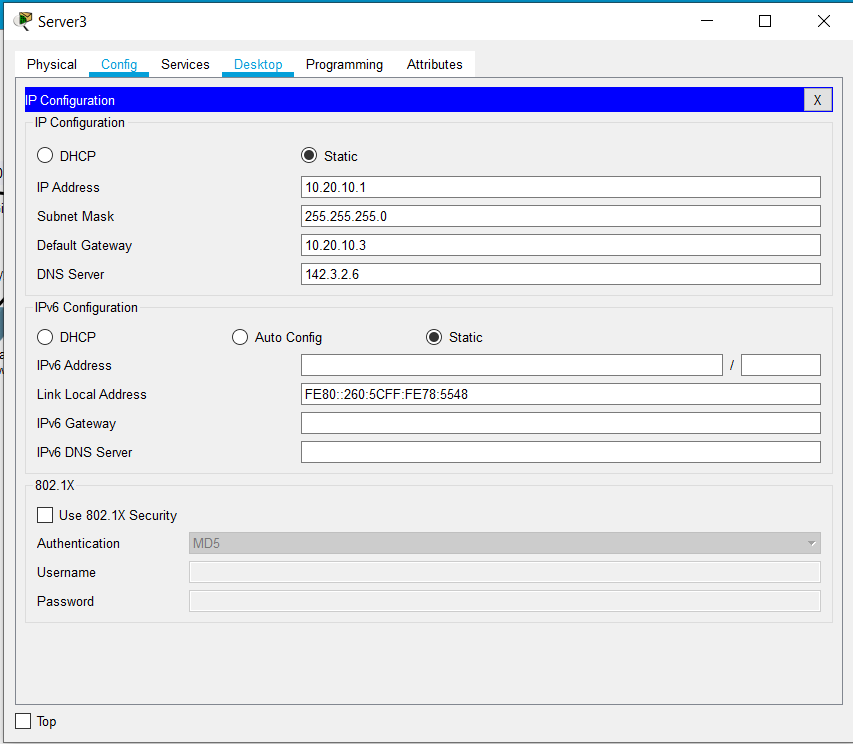
ciscoasa#copy running-config startup-config

**Assign DNS to server 2 and other Pcs and servers (server 1, server 3, server 4) as part 2g.**



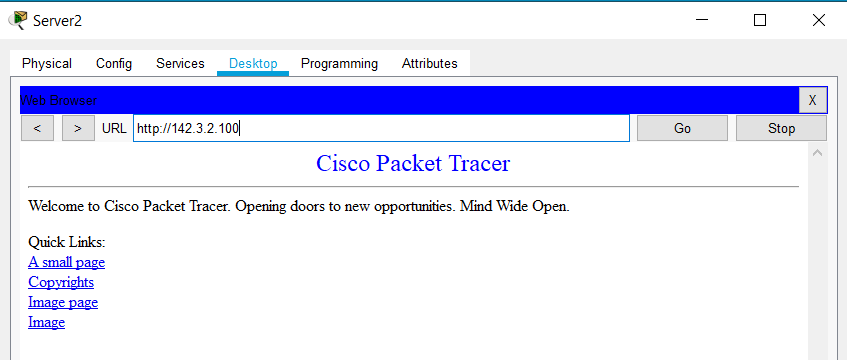




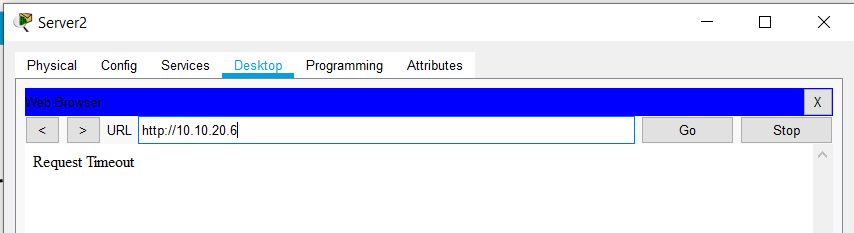


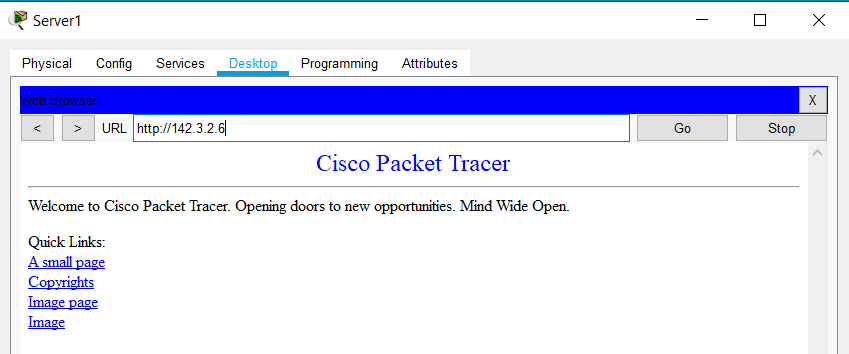
**Test**

 Test HTTP connectivity from Server2 (public) to a DMZ web server (http://142.3.2.100).

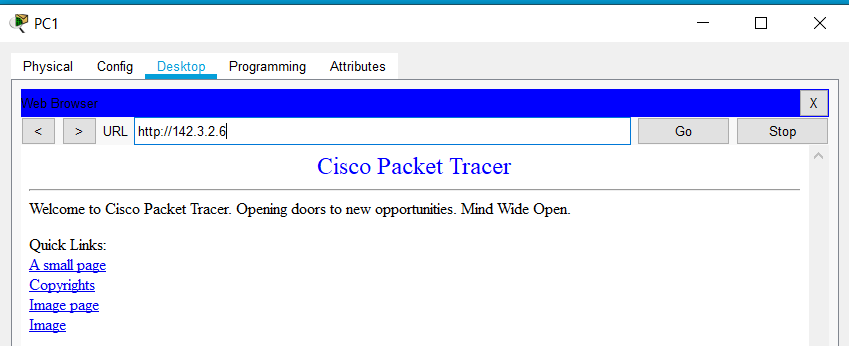


 Test HTTP connectivity from Server2 (public) to Server1 (internal).

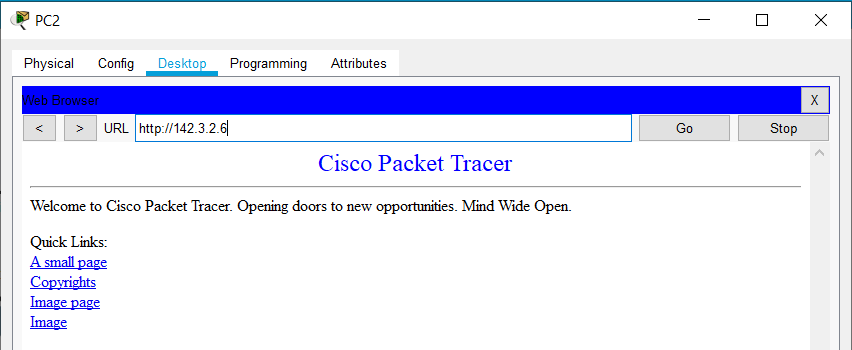




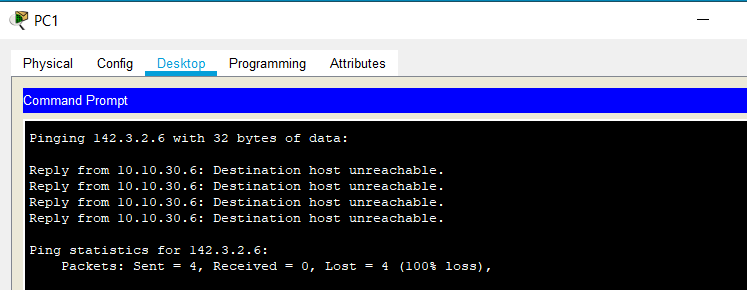
 Access the web server on Server2 from PC1 (Student).



 Access the web server on Server2 from PC2 (Lecturer).



 Ping/traceroute from PC1 to Server2.



**More;**

