LAB-B00K=2

Name = Jay Vasani

Student ID =8885487

Course code =INFO1435

Professor name =Manpreet Kaur

Due date = 2023-07-05

# Table of Contents

[Table of Contents 2](#_Toc48746339)

OSPF routing configuration [3](#_Toc48746340)

[Description 3](#_Toc48746342)

[observation 3](#_Toc48746344)

[screenshots 4](#_Toc48746344)

[reflection 9](#_Toc48746344)

[PACKET FILTERING CONFIGURATION 10](#_Toc48746344)

[description 10](#_Toc48746344)

[observation 10](#_Toc48746344)

[screenshots 12](#_Toc48746346)

[Reflection 15](#_Toc48746346)

**OSPF ROUTING CONFIGURATION**

**DESCRIPTION:**

This lab is all about configuring the OSPF dynamic routing protocol on the routers and getting to know about which DR and BDR. In this lab I have made the topology as per the scematics and then configured OSPF to see the neighbors and give permission to all the routers to send traffic to every network.

**OBSERVATION:**

* At first, I created the topology as per the scematics. And for that I have used the 2960 switch and given name by my condor id (for example S1-JV)
* I used the 2911 router and connected all of them with Fast Ethernet and GigabitEthernet ports.
* After that I assigned the IP address to the routers on the designated ports and no shut all the interfaces.
* After that I configured the RID on each router as per scematics
* I used the command “router-id 192.168.255.254” to configure the router id on R1.
* To enable OSPF routing on each router I have entered “router ospf 1” command on config mode.
* After that I configured each router to include directly connected networks in OSPF area 0.
* For R4 I have entered the command “router ospf 1” and after that “network 192.168.222.0 0.0.0.255 area 0” to include network in area 0.
* After that I verified that all the networks are in the routing table of each router by entering “show ip route” command
* I also found that R1 is DR for the network and R2 is BDR.
* The R1 is the highest priority router of this networks that is the reason why it is the DR (designated router)
* The R2 is the second highest priority router of this networks that is the reason why it is the BDR (backup designated router)
* After that I shut down the interface on R2 which is 192.168.22.1.
* After that I observed the routing table of R1 and found that 192.168.22.0 is not on that because the interface connects to that network is shut down.
* The R3 is the BDR for the network because I just shut the interface down which was BDR before and now the second highest priority of my network is R3.
* After that I brought up the interface which I shut down and I found that it is appeared in routing table of R1. This is because OSPF adjacencies between R1 and R2 are reestablished.

**SCREENSHOTS:**

This screenshot shows DR-BDR on R1 before the shut down command and also shows routing table.

A screenshot of a computer

Description automatically generated

This screenshot shows DR-BDR on R2 before the shut down command and also shows routing table.

A screenshot of a computer

Description automatically generated

This screenshot shows DR-BDR on R3 before the shut down command and also shows routing table.

A computer screen shot of a computer program

Description automatically generated

This screenshot shows DR-BDR on R4 before the shut down command and also shows routing table.

A screenshot of a computer

Description automatically generated

This is R1 after shutting the interface down on R2 which shows that now R3 is the BDR and it also not showing the interface which is shut down.

A close-up of a number

Description automatically generated

A screenshot of a computer program

Description automatically generated

After bringing that interface up I found that that interface again apperad in th routing table of R1

A screenshot of a computer

Description automatically generated

**REFLECTION:**

Overall, this lab is all about getting knowledge about OSPF dynamic routing protocol and it gives basic information about RID. Having hands on experience finding DR and BDR shutting the interfaces down and then observing the routing table. And this also gives the knowledge of how OSPF dynamically control the routing table.

**PACKET FILTERING CONFIGURATION**

**DESCRIPTION:**

This lab is all about getting hands-on to the access control list and creating standard and extended access control lists. This lab includes the access and deny options while traffic going to the server. At the end I got the network where plant PC can only send web traffic to the server and the staff PC can send every traffic to the server.

**OVERVIEW:**

* First, I have created the topology as per the scematics and given the ip to the PC and server.
* I used 54 in place of 121 which is the first 2 Digits of my condor ID.
* I used 87 in place of 122 which is the last 2 Digits of my condor ID.
* I used the same IP as per scematics because there is no replacement of 18.
* After that I assigned the IP to the designated ports of the router so that I can ping all of the devices.

STANDARD:

* After that I created the standard ACL so that it will only allow traffic from staff PC to reach the server. And the traffic coming from plant PC will be dropped.
* For that I entered the further commands.

A computer screen shot of a computer program

Description automatically generated

* In these commands I just gave permit to the staff network and the other networks will automatically be denied to access the server.
* I chose the gigabit Ethernet 0/2 which is connected to the server and I entered the command “ip access-group BLOACK\_PLANT out” on that interface.
* I chose the outbound because it will take the packet to the router but not allow to pass the router and it will be dropped at router interface.
* After that checked that only staff PC can ping the server where plant PC cannot.
* For another approach while using the standard ACL is when I can use the “deny 10.105.54.0 0.0.0.255” instead of the permit command.
* This will basically prevent the traffic coming from the plant and the other networks will automatically be allowed to send traffic to the server.

EXTENDED:

* I created the extended ACL which only allows web access from the plant PC and the other traffic from that network will be dropped. Also the staff PC can send any kind of traffic.
* For that I entered further commands.
* A computer screen shot of a computer program

  Description automatically generated
* In these commands I just gave permission to plant to send tcp traffic and denied the other traffic from that
* At the end I entered “permit any” which basically allow any kind of traffic from the other devices.
* I chose the gigabit Ethernet 0/2 which is connected to the server, and I entered the command “ip access-group BLOACK\_PLANT out” on that interface.
* I chose the outbound because it will take the packet to the router but not allow to pass the router and it will be dropped at router interface.
* For the other approach I can use this

#permit tcp any 10.106.18.0 0.0.0.255 eq www

#deny ip 10.105.54.0 0.0.0.255 any

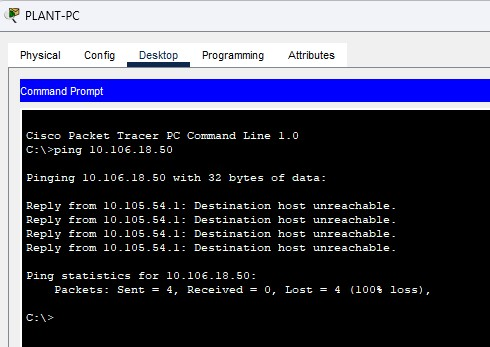
#permit ip 10.105.87.0 0.0.0.255 any

#deny ip any any

* Where first I permitted web access from plant pc then deny all other traffic from that
* After that I permitted all the traffic from staff pc
* And after that I denied all the other traffic from any other devices.

**SCREENSHOTS:**

This shows that the server is unreachable from plant pc



This shows that I can ping server from staff pc

A computer screen shot of a black screen

Description automatically generated

This shows staff pc have web access to server

A screenshot of a computer

Description automatically generated

This shows plant pc have web access to server

A screenshot of a computer

Description automatically generated

This is the both access list I have created

A screenshot of a computer

Description automatically generated

**REFLECTION:**

This lab gives knowledge about how the big organizations work where they only give access to some data to the clients and how we can restrict the user from getting access to some specific department. I also got hands-on experience of allowing and denying specific traffic while using standard and extended access control lists.