[NC-Rase 18]
DOI: 10.5281/zenodo.1485414

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SIMULATION OF OSPF ROUTING PROTOCOL AND IP TRAFFIC MANAGEMENT WITH ACCESS CONTROL LIST (ACL) USING CISCO PACKET TRACER

Prof. Manjusha. M. Patil[1], Prof. Pravin. V. Thakare[2], Prof. Sagar. R. Deshmukh[3] & Prof. Pranali. P. Chavhan[4]

[1]Department of Electronics & Telecomm.MGI-COET, Shegaon, India
[2&3]Department of Computer Science & Engg. MGI-COET, Shegaon, India
[4]Department of Electronics & Telecomm. MGI-COET, Shegaon, India

ABSTRACT

Network protocols have been created for supporting communication between computers and other types of electronic devices. Routing protocols are the family of network protocols that enable computer routers to communicate with each other and in turn to intelligently forward traffic between their respective networks. Simulation was employed with the use of a packet tracer and authenticated to real time situation with the use of hyper terminal emulator. The simulation process had been validated by the actual setup. Open Shortest Path First (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First. Access Control List (ACL) is a set of commands grouped together to filter the traffic that enters and leaves the interface. In this paper, the routing protocol OSPF has been studied and implemented using 'Cisco Packet tracer'. The results are checked using ping command and the virtual network is created to test the OSPF protocol. This paper also focuses on corroborating the simulated performances of the OSPF routing protocols to actual operations along with simulation of the network using Standard ACL and Extended ACL. The configuration is done using CISCO packet tracer.

Keywords: *Classful IP Addressing, Topology, Configuration, Ping, IP Route, Subnetting, Simulation, OSPF Routing Protocol, Packet Tracer, ACL.*

I. INTRODUCTION

Packet Tracer is virtual networking simulation software developed by Cisco, to learn and understand various concepts in computer networks. Networking devices appear in packet tracer as they look in reality and a student can interact with various networking devices, by customizing the configurations, by turning them on and off etc. Packet Tracer is teaching and learning software and a tool, easy to work with, thus after working with virtual environment, a student gains lot of confidence, when it comes to working in real-time environment. We can track the path of a packet, when it moves from source to destination, and also learn and understand, how to troubleshoot a network, when a packet doesn't reach the destination. Packet Tracer can be used to learn concepts more clearly by creating different scenarios. Since Networking is all about imagination and it's difficult to track movement of packets in a real-time environment, thus various networking concepts can be explained by creating a virtual environment, showing the moment of packets, exactly as it would happen in real-time. Packet tracer can be used to understand the working of various networking devices, their use,a what makes them different and their appropriate use in a designing a network. Packet tracer is a user friendly tool, with various options, where a user can customize and design a network. Various tests can be run, to understand various network failures and how to troubleshoot them in real-time. Simulation of OSPF (Open Shortest Path First) can be done by using Cisco Packet Tracer. IP Traffic Management in network can be controlled though ACL provided by Cisco.

Routing is the selection of the path that the data or packet has been chosen .It mainly depends on the techniques and the number of the devices that are connected to the network. To route a packet we must have the packet destination address (IP) because for packet to reach from one device to other the address of one device must be known such that they can communicate each other and also we want the neighboring devices information and also the topology of the

ISSN 2348 – 8034
Impact Factor- 5.070

network because to study the path (for that we can use ospftechnique).They are three types of routing techniques: Static Routing, Default Routing and Dynamic Routing.

Figure:

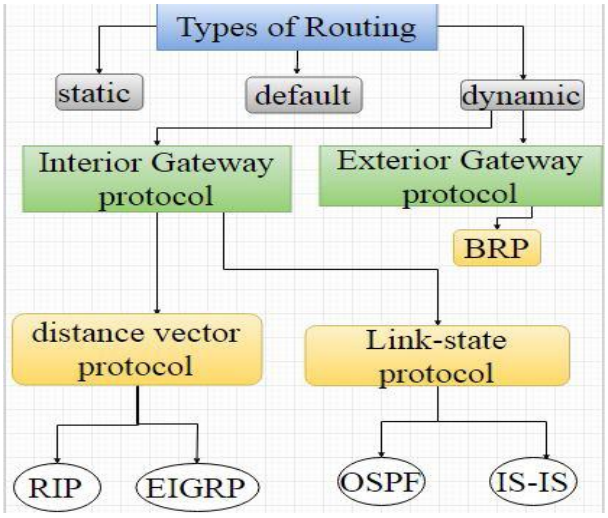

Fig.1: Routing Techniques

OSPF (Open Shortest Path First) is a link state routing protocol that constructs map of the topology and database to calculate the metric for each route and to choose shorter routing routes. Cost is the metric used by this protocol. It is designed for networks which are scalable and to handle a distributed routing table with fast propagation, among routers. There is no hop count limitation so it can be used in large networks. OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e. the protocol which aims at moving the packet within a large autonomous system or routing domain.OSPF uses the concept of Area for hierarchical network design.It is a method of finding the shortest path from one router to another in a local area network (LAN). As long as a network is IP-based, the OSPF algorithm will calculate the most efficient way for data to be transmitted. If there are several routers on a network, OSPF builds a table (or topography) of the router connections. When data is sent from one location to another, this algorithm compares the available options and chooses the most efficient way for the data to be sent. This limits unnecessary delays in data transmission and prevents infinite loops.

Cisco provides Access Control Lists (ACLs) to control the flow of traffic from one interface to the other in the network.These are the filters that enable to control which routing updates or packets are permitted or denied in or out of a network. The ACL commands allow the administrator to deny or permit traffic that enters the interface. ACL also performs other tasks such as restricting telnet, filtering routing information and prioritizing WAN traffic with queuing. A wildcard mask allow to match the range of address in the ACL statements. A router makes two references to ACL such as numbered and named. These references support two types of filtering such as standard and extended. The ACL statements are configured first and then they are activated. In a single ACL number maximum 16000 statements can be created. If we add one statement later, it will get added at the bottom of all statement. Router read ACL top to bottom. If a single ACL is removed then all ACLs created will get removed. The benefits of ACL are as follows:

a. Reduce network traffic and increase network performance.
b. Control the flow of traffic.
c. Take a decision as required.

ISSN 2348 – 8034
Impact Factor- 5.070

II. OSPF TERMS

***Router ID*:** It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

Router priority: It is an 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.

***Designated Router (DR)*:** It is elected to minimize the number of adjacency formed. The role of a designated router is to receive LSA from other router when changes occur. And also to flood the update to other routers under same area. It distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and it will respond to that request with an update.A designated router is elected in each area based on some priority. Non designated routers doesn't exchange routing updates with each other. They sends their update to the DR first. DR router then send updates to other routers.

***Backup Designated Router (BDR)*:** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.Backup Designated Router (BDR) is the deputy of DR. It is also elected during the DR election process. Router with the 2nd highest priority becomes BDR. When the primary designated router (DR) fails BDR take over the role of designated router. During that time 3rd highest router becomes BDR.

Election of Designated Router:
First parameter used to elect the DR &BDR selection is priority. Router's interface with highest priority becomes DR. 2nd highest priority router becomes BDR. When DR router fails /crushes or loses all neighbors, BDR becomes DR and 3rd Highest priority router becomes BDR.This is a contentious process. OSPF priority ranges from 0 to 255. By default, all router is configured with OSPF priority 1. A router configured with ospf priority 1 will never become a DR. When Priority ties, like both router is configured with OSPF priority 100, then Router ID is used to elect the DR. In this case highest router id becomes the DR.DR election is not a preemptive feature .Means, if a DR router ever fails and come back again then it can not become DR. It has to wait until the last router becomes DR. Similarly after an election, if any router is added in the system with highest priority then it will not become DR immediately. If no router ID is configured then router configured with highest loopback interface's IP address becomes DR.If no loopback interface is configured then router with highest physical interface IP address becomes DR.So overall DR election is shown in figure:

Figure:

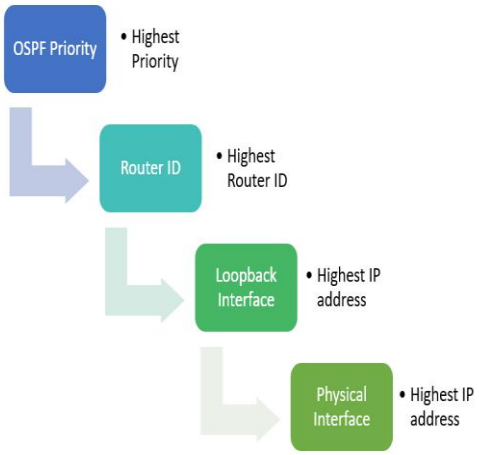

Fig.2:Election of Designated Router

[NC-Rase 18]
DOI: 10.5281/zenodo.1485414
ISSN 2348 – 8034
Impact Factor- 5.070

III. OPEN SHORTEST PATH FIRST (OSPF) ROUTER ROLES

An area is a group of contiguous network and routers. Routers belonging to same area shares a common topology table and area ID. The area ID is associated with router's interface as a router can belong to more than one area. OSPF is a hierarchical routing protocol. It enables better administration and smaller routing tables due to segmentation of entire network into smaller areas. OSPF consists of a backbone (Area 0) network that links all other smaller areas within the hierarchy. There are some roles of router in OSPF

Figure:

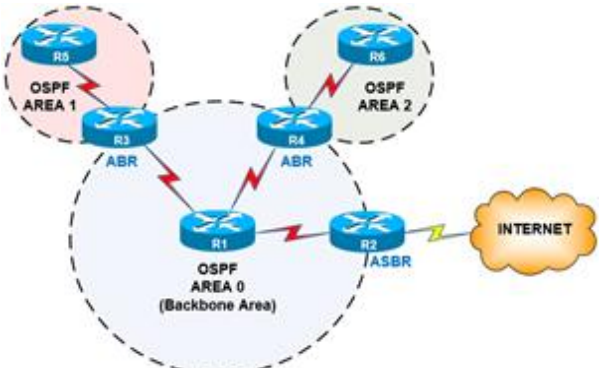

Fig.3:OSPF Router Roles

Areas: An area consists of routers that have been administratively grouped together. Usually, an area as a collection of contiguous IP subnetted networks. Routers that are totally connected to networks within the area. Within an area, all routers have identical topological databases.

Backbone Area: An OSPF backbone area consists of all routers in area 0, and all area border routers (ABRs).The backbone distributes routing information between different areas.

Backbone router: The area 0 is known as backbone area and the routers in area 0 are known as backbone routers. If the routers exists partially in the area 0 then also it is a backbone router.

Internal router: An internal router is a router which have all of its interfaces in a single area.

Area Boundary Router (ABR):The router which connects backbone area with another area is called Area Boundary Router. It belongs to more than one area. The ABRs therefore maintain multiple link-state databases that describe both the backbone topology and the topology of the other areas

Area Summary Border Router/Autonomous System BoundaryRouter: Routers that exchange routing information with routers in other Autonomous Systems are called ASBRs .When an OSPF router is connected to a different protocol like EIGRP, or Border Gateway Protocol, or any other routing protocol then it is known as AS. The router which connects two different AS (in which one of the interface is operating OSPF) is known as Area Summary Border Router. These routers perform redistribution. ASBRs run both OSPF and another routing protocol, such as RIP or BGP. ASBRs advertise the exchanged external routing information throughout their AS.

IV. OSPF LINK STATE PACKET TYPES

OSPF routers generate packets of information that are exchanged with neighboring routers. These packets are designed for several purposes such as forming neighbor relations between routers, calculating cost and best path for

a specific route and more. All OSPF packets share a common OSPF Header of 24-bytes. This header allows the receiving router to validate and process the packets. The format of common OSPF header is:

Figure:

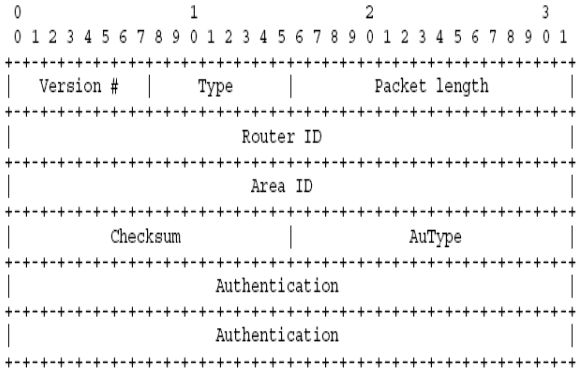

Fig.4: Common OSPF Header

The following is a list of the most frequently used OSPF packets:
Link State Advertisement (LSA): The primary means of communication between OSPF routers, it's the packet that carries all fundamental information about the topology and is flooded between areas to performdifferent functions, there are 11 types of LSA packets**.**

Link State Database (LSDB): **LSDB** packet contains all updated link-state information exchanged among the network, and all routers within the same area have **i**dentical LSDB, and when two routers form new neighbor adjacency, they sync their LSDB to be fully adjacent.***Link State Request (LSR)****:* Once neighbor adjacency is formed and LSDB is exchanged, neighbor routers may locate a missing LSDB information, they then send a request packet to claim the missing piece, and neighbors receive this packet and respond with **LSU**.***Link State Update (LSU)****:* A response packet sends a specific piece of LSDB information requested by an OSPF neighbor via LSR packet.***Link State Acknowledgment (LSACK)****:* The router that sends the LSR packet confirms receiving the LSU from neighbor by sending a confirmation packet acknowledging receiving the requested LSUs.

V. FEATURES OF PACKET TRACER

Packet creates a simulation environment where a student gets visualization experience. An instructor can set up an activity wizard to assess the students by giving them different grades. There is also a multi-user feature, where students at different physical locations can work together on the same project, assignment or lab. Packet tracer has both Logical and physical workspace to create customized scenario based labs and it has got both Real-time and simulation Modes to understand various networking concepts, the same way as it would have happened in real-time. Packet tracer also has got user friendly GUI and CLI interfaces, which are easy to work with and doesn't need any experience or expertise. Another most important feature of packet tracer is that it can support multiple languages and it is platform independent. It is an open-source software which can be downloaded free of cost from the internet. Packet tracer also helps to understand the concept of logical troubleshooting and it can also be used for case studies. There are integrated tutorials along with the software to understand use of various features of packet tracer. It also supports group and individual labs, homework, exams, games, problem solving etc. Workspaces: There are two types of work space Logical Work-space: It allows users to build logical network topologies and various devices can be dragged and dropped to logical workspace. Physical work-space: It allows a user to create a network, the way as it would look in real world, and has the capability of geographical representation, where different networking devices can be shown as connected at different locations of the city. Modes: There are two types Modes

Real-time Mode*:*The devices in a network behave as real devices do and look similar to real devices.

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485414 Impact Factor- 5.070

Simulation Mode: In this mode, a student can see and control time intervals, to learn how to troubleshoot network failures.

Cisco Packet Tracer includes the following features:

- Makes learning easier by providing a realistic network simulation and visualization environment.
- Provides authoring of learning activities, tasks, labs, and complex assessments.
- Supplements real equipment and enables extended learning opportunities beyond physical classroom limitations.
- Simulates continuous real-time updates of underlying network logic and activities.
- Promotes social learning through a network-capable (peer-to-peer) application with opportunities for multiuser competition, remote instructor-student interactions, social networking, and gaming.
- Supports the majority of protocols and technologies.

VI. TOPOLOGY FOR SIMULATION OF OSPF

We considered thatthe network model that contains two routers, two switches, four computers (end devices).The Cisco packet Tracker is used for this simulation of OSPF routing technique. The connection between the two routers is done by using Serial DCE cable and for computer toswitch we use the copper straight-through cable. The Network model is shown below:

Figure:

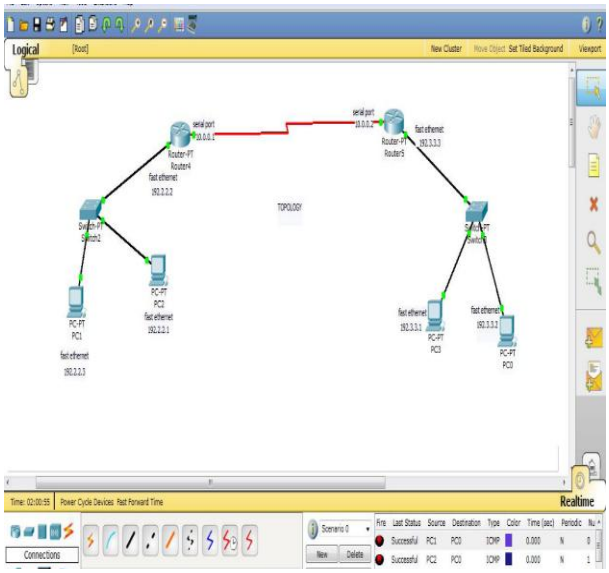

Fig.5: Network Model for Simulation of OSPF

Subnetting: Subnet allows administrators to divide their private network into virtually defined segments. Subnets provide a lot of benefits for network administrators and ultimately users, by making administration and routing more efficient such as: subnetting prevents unnecessary broadcasts, increases security options, simplifies administration and controls growth. Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class. Classless Inter Domain Routing (CIDR) provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class IP address can be used to have smaller sub-networks which provide better network management capabilities. In the simulated performance evaluation of the three routing protocols, a packet tracer had been used.

ISSN 2348 – 8034
Impact Factor- 5.070

Configuring the network model using OSPF:

IP address assign in PC's:

Firstly, computers (pc's) must be assign ip address as follows

Figure:

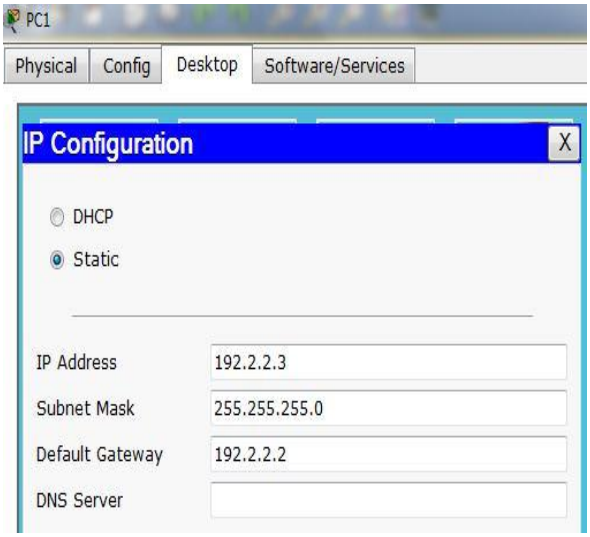

Fig.6: show the assign of ip address in pc1

The remaining PC should be configured in the same manner as the PC1
PC2: IP Address 192.2.2.1,Subnet Mask 255.255.255.0, Default Gateway 192.2.2.2
PC3: IP Address 192.3.3.1, Subnet Mask 255.255.255.0, Default Gateway 192.3.3.3
PC0: IP Address 192.3.3.2, Subnet Mask 255.255.255.0, Default Gateway 192.3.3.3
In the all above pc's the default gateway is the fast Ethernet ip address of the routers they are connected with there, Ethernet ports using copper straight through cable. After the connections are performed physically, configuring the router need to be done. In figure 5, router4 is configured as follows:

```
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 192.2.2.2 255.255.255.0
Router(config-if)#int s2/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#clock rate 64000
Router(config-if)#exit
Router(config)#router ospf 7
Router(config-router)#network 10.0.0.0 0.255.255.255 area 7
Router(config-router)#
00:23:49: %OSPF-5-ADJCHG: Process 7, Nbr 10.0.0.2 on Serial2/0 from LOADING to F
ULL, Loading Done
```

[NC-Rase 18]
DOI: 10.5281/zenodo.1485414
ISSN 2348 – 8034
Impact Factor- 5.070

After that the router 5 needs to configure using OSPF:

```
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 192.3.3.3 255.255.255.0
Router(config-if)#int s2/0
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

Router(config-if)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router(config)#router ospf 7
Router(config-router)#network 10.0.0.0 0.255.255.255 area 7
Router(config-router)#exit
```

Above configuration shown the router5 in CLI (command line interface).After the above code is done there is link-up line protocol is made there such that the OSPF has done. In the above the fa0/0 is the Fast Ethernet, and S2/0 is the serial port. Router ospf 7 the '7' gives the area and thus must be same for all the router such that they all are in the same domain. The area code may be any number.

Examing the configuration

The network model that is implemented has verified using ping command from any pc's that attached to the router. Here we are using the pc1 and pinging the address to the another pc0. The result is shown in the below figure

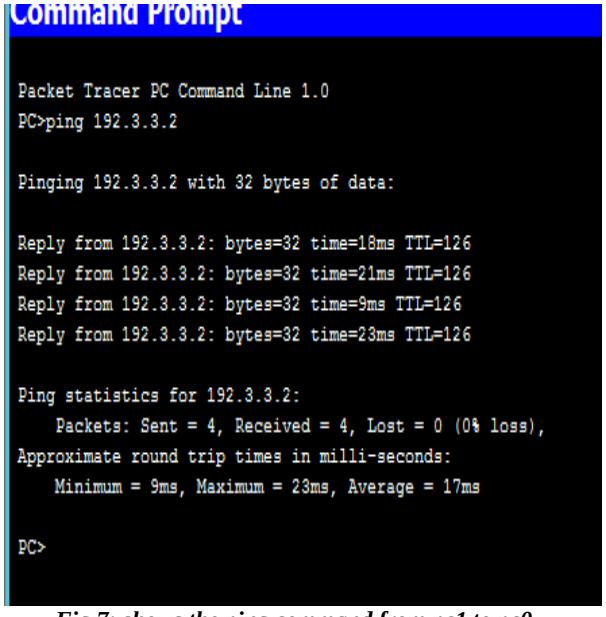

Fig.7: shows the ping command from pc1 to pc0

Routing is used to trace the path for the network and in this paper we implemented the virtual network model using cisco packet tracer. There are different types of routing techniques are there but due to the usage and area of necessity we use the require one. The OSPF is used for the area where more routers are used and also large network usage. It mainly use is that it has unlimited hop count and Irrespective of other techniques it uses a concept of area to ease management and traffic control.

VII. ACCESS CONTROL LIST

ACL is created in the global configuration mode. After creating the basic group of ACL commands, we need to activate them. In order to filter traffic between interfaces, ACL needs to be activated in Interface Sub configuration Mode. Thus the direction of filtering the traffic is classified into:

a. Inbound:The traffic is filtered as it enters the interface. If the ACL is set as inbound, the router compares the incoming packet with the interface ACL before it leaves the interface.

***b. Outbound*:** The traffic is filtered as it leaves the interface. . If the ACL is set as outbound, the router forwards the received packet to the exit interface where the packet is compared with the interface ACL.

Wildcard mask

Wildcard mask are used for matching a range of IP addresses in ACL, instead of manually entering it. Also, wildcards are used with access lists to specify host, network or a range of addresses. It is similar to an inverted subnet mask. In order to match IP address of a packet with the ACL statement, a wildcard is created by inverting the bit values of the subnet mask. Table shows the subnet mask and wildcard mask of Class A, B and C IP addresses.

Table:

Table1. Subnet Mask and Wildcard Mask of Class A, B and C IP Addresses

CLASS	SUBNET MASK	WILDCARD MASK
A	255.0.0.0	0.255.255.255
B	255.255.0.0	0.0.255.255
C	255.255.255.0	0.0.0.255

The ACLs supports the following types:

***a. Standard ACL*:** ACL is applied on destination router. It permits or deny the packet on the basis of source addresses only.

b. Extended ACL:ACL is applied on source router. It permits or deny the packet on the basis of source as well as destination addresses. If a single host is to be permitted or denied into a network the syntax is: permit/deny <source IP address><wildcard mask>or permit/deny host <source IP address>e.g. permit/deny 192.168.10.10 0.0.0.255 or permit/deny host 192.168.10.10 If a single network is to be permitted or denied into a network the syntax is: permit/deny <Network ID><wildcard mask>e.g. permit/deny 192.168.10.0 0.0.0.255 If the whole network is to be permitted or denied, the syntax is: permit/deny 255.255.255.255 255.255.255.255

Standard Access-List Configuration

A Standard ACL can use only the source IP address in an IP packet to filter thenetwork traffic. Standard access lists are typically used to permit or deny an entire host or network. They cannot be used to filter individual protocol or services such as FTP and Telnet. In the technical explanation, the standard ACL supports only source address. To create a standard access list on a Cisco router, the following command is used from the router's global configurationmode: R1(config)# access-list

ACL_NUMBER permit|deny IP_ADDRESS WILDCARD_MASK
Using the host keyword to specify the host we want to permit or deny:
R1(config)# access-list ACL_NUMBER permit|deny host IP_ADDRESS

Once the access list is created, it needs to be applied to an interface. By using the ip access-group ACL_NUMBER in|out interface subcommand. in and out keywords specify in which direction you are activating the ACL. in means that ACL is applied to the traffic coming into the interface, while the out keyword means that the ACL is applied to the traffic leaving the interface.Consider the following network topology,

Figure:

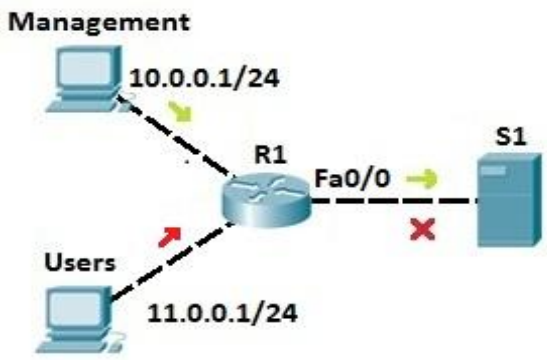

Fig.8: Configuration of Standard Access List

We want to allow traffic from the management LAN to the server S1. First, we need to write an ACL to permit traffic from LAN 10.0.0.0/24 to S1. We can use the following command on R1
R1(config)#access-list 1 permit 10.0.0.0 0.0.0.255
The command above permits traffic from all IP addresses that begin with 10.0.0.0 we could also target the specific host by using the host keyword:
R1(config)#access-list 1 permit host 10.0.0.1
The command above permits traffic only from the host with the IP address of 10.0.0.1.
Next, we will deny traffic from the Users LAN (11.0.0.0/24):
R1(config)#access-list 1 deny 11.0.0.0 0.0.0.255
Next, we need to apply the access list to an interface. It is recommended to place the standard access lists as close to the destination as possible. In our case, this is the Fa0/0 interface on R1. Since we want to evaluate all packets trying to exit out Fa0/0, we will specify the outbound direction with the out keywordR1(config-if)#ip access-group 1 out
At the end of each ACL there is an implicit deny all statement. This means that all traffic not specified in earlier ACL statements will be forbidden, so the second ACL statement (access-list 1 deny 11.0.0.0 0.0.0.255) was not even necessary

Extended Access-List Configuration

To be more precise when matching a certain network traffic, extended access lists are used. With extended access lists, we can match more information. The numbers are in ranges from 100 to 199 and from 2000 to 2699.
Two steps are required to configure extended access lists:

1. Configure extended access lists using the following command:(config) access list NUMBER permit|deny IP_PROTOCOL SOURCE_ADDRESS WILDCARD_MASK [PROTOCOL_INFORMATION] DESTINATION_ADDRESS WILDCARD_MASK PROTOCOL_INFORMATION
2. apply an access list to an interface using the following command:

(config) ip access-group ACL_NUMBER in | out

To better understand the usefulness of extended access lists, consider the following example,

ISSN 2348 – 8034
Impact Factor- 5.070

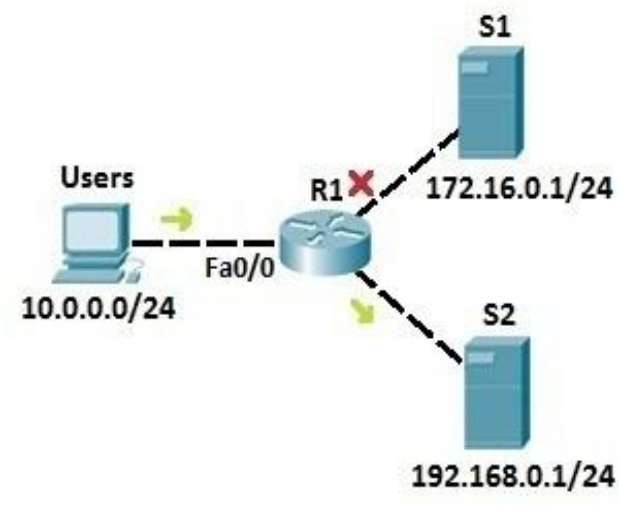

Fig.9: Configuration of Extended Access List

We want Users from the network 10.0.0.0/24 to be able to access the server S2 (IP address 192.168.0.1) and prevent them from accessing server S1 (IP address 172.16.0.1/24). First, we need to configure an access list to permit Users the access to server S2:

```
R1(config)#access-list 100 permit ip 10.0.0.0 0.0.0.255 192.168.0.1 0.0.0.0
```

Next, we need to deny Users the right to access S1 by using the deny statement:

```
R1(config)#access-list 100 deny ip 10.0.0.0 0.0.0.255 172.16.0.1 0.0.0.0
```

nally, we need to apply the access list to the interface on R1:

```
R1(config)#int fa0/0
R1(config-if)#ip access-group 100 in
```

Here is another example of using extended access lists. In this example we will use extended ACLs to filter traffic by the port used.

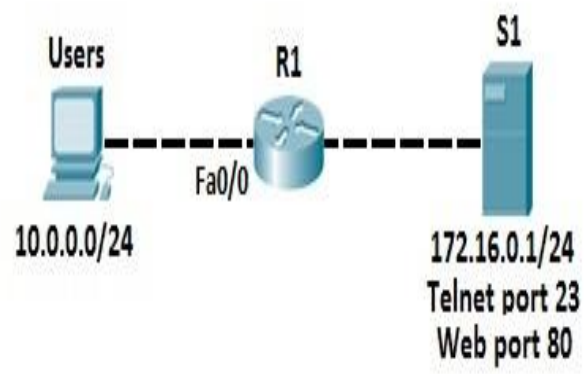

Fig10:Configuration of Extended Access List to Filter the Traffic by Port

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485414 Impact Factor- 5.070

Again, we have the Users network (10.0.0.0/24). On the right side, we have a server that serves as a web server, listening on port 80. We need to permit Users to access web sites on S1, but we also need to deny other type of access, for example the Telnet access. First, we need to allow traffic from Users network to the web server port of 80. We can do that by using the following command:

```
R1(config)#access-list 100 permit tcp 10.0.0.0 0.0.0.255 172.16.0.1 0.0.0.0 eq 80
```

TCP keyword, we can filter packets by source and destination ports. In the example above, we have permitted traffic originating from the 10.0.0.0 network to the host 172.16.0.1 on the port 80. The last part of the statement, eq 80, specifies the destination port of 80.Now we need to disable telnet traffic from the network 10.0.0.0 to 172.16.0.1. To do that, we need to create a deny statement:

```
R1(config)#access-list 100 deny tcp 10.0.0.0 0.0.0.255 172.16.0.1 0.0.0.0 eq 23
```

Next, we need to apply our access list to the interface:

```
R1(config)#int fa0/0
R1(config-if)#ip access-group 100 in
```

Since at the end of each access list there is an explicit deny all statement, the second ACL statement was not really necessary. After applying an access list, every traffic not explicitly permitted will be denied.

VIII. CONCLUSION

The OSPF used for the area where more routers are used and also large network usage. Using areas, OSPF network can be logically segmented to improve administration and decrease the size of routing tables. It gather all link state data available to build a topology map of all available paths in its network and then save the information in its topology database. It uses the link state algorithm. From the information gathered, it will calculate the best shortest path to each reachable subnet/network using an algorithm. It contains a topology table included the entire road map of the network with all available OSPF routers and calculated best and alternative paths.

Access Control Lists are a set of rules used most commonly to filter network traffic. They are used on network devices with packet filtering compatibilities. They provides traffic flow control by restricting the delivery of routing updates. Controls which type of traffic are forwarded or blocked by the router. By using standard access list we can filter only on the source IP address of a packet. These types of access list are not as powerful as extended access lists, but they are less processor intensive for the router. Extended access lists are more complex to configure and consume more CPU time than the standard access lists, but they allow a much more granular level of control.

IX. FUTURE SCOPE

Apart from RIP, OSPF routing protocols EIGRP and BGP routing protocols can be used for routing the packets. More IP protocols such as UDP, ICMP and IP can be used in extended ACLs.

REFERENCES

1. *Andrew Smith,Colin Bluck, Multiuser Collaborative Practical Learning Using Packet Tracer, IEEE Xplore,may 2010(11291357)*
2. *Hirokazu Sayama ; Noriaki Yoshiura,"Test tool for equivalence of access control list",IEEE Xplore.Nov 2012(13151581)*
3. *Garima Jain, Nasreen Noorani, Nisha Kiran, Sourabh Sharma, Designing & simulation of topology network using Packet Tracer, International Research Journal of Engineering and Technology (IRJET), 2(2), 2015.*
4. *Petcu, D.; Iancu, B.; Peculea, A.; Dadarlat, V.; Cebuc, E., "Integrating Cisco Packet Tracer with Moodle platform: Support for teaching and automatic evaluation," Networking in Education and Research, 2013 RoEduNet International Conference 12th Edition , vol., no., pp.1,6, 26-28 Sept. 2013*

ISSN 2348 – 8034
Impact Factor- 5.070

5. *IP Routing: OSPF Configuration Guide, Cisco IOS Release 12.4T by Americas Headquarters Cisco Systems, Inc.*
6. *M. Ericsson, M. G. C. Resende, and P. M. Pardalos.A genetic algorithm for the weight setting problem in ospf routing. J. of Comb. Opt., 6:299–333,2002.*
7. *http://www.sis.pitt.edu/~icucart/networking_basics/networking_topology.html*
8. *Nahush Kulkarni , Harsh Kothari , Hardik Ashar , Sanchit Patil,"Access Control List" International Journal for Research in Applied Science & Engineering Technology (IJRASET),vol 3, ISSN: 2321-9653,nov 2015*
9. *Sharat Kaushik, Anita Tomar, Poonam, "Access Control List Implementation in a Private Network", International Journal of Information & Computation Technology, Vol. 4, No. 14, 2014, pp. 1361-1366.*
10. *Cisco Systems Inc. http://www.cisco.com*