ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

IP Traffic Management With Access Control List Using Cisco Packet Tracer

Shipra Suman, Er. Aditi Agrawal

***Abstract*— Access Control List (ACL) is a set of commands grouped together to filter the traffic that enters and leaves the interface. 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. In this paper we have analyzed and simulated the network using Standard ACL and Extended ACL. The configuration is done using CISCO packet tracer.**

Index Terms- ACL, Telnet, Wildcard Mask, Standard ACL, Extended ACL, Packet Tracer

I. INTRODUCTION

Cisco provides Access Control Lists (ACLs) to control the flow of traffic from one interface to the other in the network. ACL also performs other tasks such as restricting telnet, filtering routing information and prioritizing WAN traffic with queuing [7]. 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 [5]. 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.

In this paper Standard ACL and Extended ACL are analyzed and simulated using Cisco Packet Tracer.

II. ACCESS CONTROL LIST

ACL is created in the global configuration mode. After creating the basic group of ACL commands, we need to activate them [6].

In order to filter traffic between interfaces, ACL needs to be activated in Interface Subconfiguration Mode [7]. 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..

The ACL are of two types:

a. Numbered ACL: Unique number is assigned to each ACL.
b. Named ACL: Unique name is assigned to each ACL.

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

or

All Rights Reserved © 2016 IJSETR

permit/deny any any

III. WILDCARD MASKING

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 [2]. 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 1 shows the subnet mask and wildcard mask of Class A,B and C IP addresses.

Table 1. 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

IV. CONFIGURING ACL

The guidelines have to be followed to configure the ACL. The *"access-list"* command is used to create an ACL. The syntax to create an ACL is:

access-list <ACL_#> permit/deny conditions
where,

- *ACL_#* - Allows to group statements into a single list.
- *permit/deny*- Specifies the action to be performed.
- *conditions* - Specifies which packet needs to match for a router to execute an action.

After creating the ACL, it has to be applied to a process in the IOS. In order to activate ACL on the interface, the following syntax is followed:

interface type slot_#/port_#

ip access-group ACL_# in/out
where,

- *in/out* – Specifies the direction of traffic ,whether it is inbound or outbound.

V. STANDARD ACL

The Standard ACLs filters the source IP address in an IP packet. It is also used to restrict telnet access to the router. ACL number for standard ACL range from 1 to 99 and 1300 to 1999. An entry can be created in a standard numbered IP ACL by using the *access-list* command [5]-[7]. The syntax of this command is:

access-list <ACL_#> <permit/deny> <source_IP address> <wildcard mask>
where,

- *source_IP address* – Specifies the IP address of the source.

After creating the standard ACL, it must be activated on the routers interface. The ip access-group command enables to activate the ACL on the interface.
The following steps are followed to activate the standard numbered ACL:

i. Log into the router.
ii. Switch to the privileged mode
iii. Switch to the configured mode.
iv. Type *interface type slot/port* to configure on the router's port.
v. Type *ip access-group ACL_# in/out* to activate the standard numbered ACL on the configured interface.

e.g. access-list 10 deny host 192.168.20.2
access-list 10 permit 192.168.20.0 0.0.0.255
interface fast 0/0
ip access-group 10 out

The figure 1 shows how to specify or place standard ACL in a network.

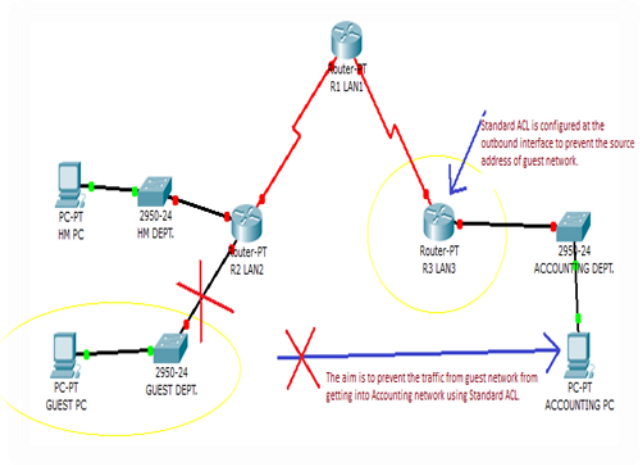

Figure 1. Standard ACL

VI. EXTENDED ACL

The extended ACLs are more flexible in comparison to the standard ACLs [7]. Unlike standard ACLs, extended ACL filter the source and destination IP address, IP protocols such as IP, TCP, UDP, ICMP and protocol information such as port number. The *access-list* command is used to configure an extended ACL. ACL number for extended ACL range from 100 to 199 and 2000 to 2699 [5]. The syntax to configure extended ACL is:

access-list <ACL_#> <permit/deny> <IP protocol> <source IP address> <wildcard mask> <destination IP address> <wildcard mask> <operator> <port_#/name>
where,

- *IP protocol* – Specifies the IP protocol to be matched such as UDP, IGRP, EIGRP and IGMP.
- *operator* – Table 2 shows the operator for TCP and UDP connections [5].

All Rights Reserved © 2016 IJSETR

- *port_#/name* – Specifies the TCP/UDP port names or numbers. Table 3 and 4 shows TCP and UDP port names and numbers respectively [5].

Table 2. Operators for TCP and UDP Connection

Operator	Description
lt	Less than
gt	Greater than
neq	Not equal to
eq	Equal to
range	Range of port numbers

Table 3. TCP Port Names and Numbers

Name	Command Parameter	Number
FTP Data	ftp-data	20
FTP Control	ftp	21
Telnet	telnet	23
SMTP	Smtp	25
WWW	www	80

Table 4. UDP Port Names and Numbers

Name	Command Parameter	Number
DNS Query	dns	53
TFTP	tftp	69
SNMP	Snmp	161
IP RIP	Rip	520

The figure 2 shows how to specify or place extended ACL in a network.

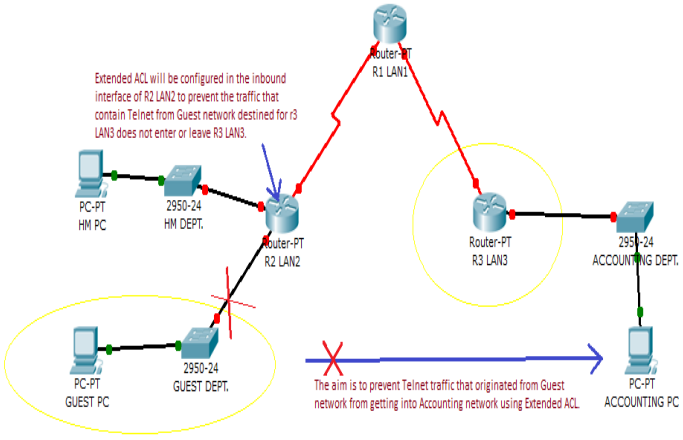

Figure 2. Extended ACL

VII. CONFIGURATION USING CISCO PACKET TRACER SIMULATOR

A virtual networking model comprising of CISCO routers was developed by using Cisco Packet Tracer simulator as shown in figure 3 [1].

Networking Model Algorithm:

In this network model we have implemented Routing Information Protocol. We have used many components such as routers, switches and made physical connection by using copper straight through cables and serial DCE cables for fast ethernet and serial ports [4].

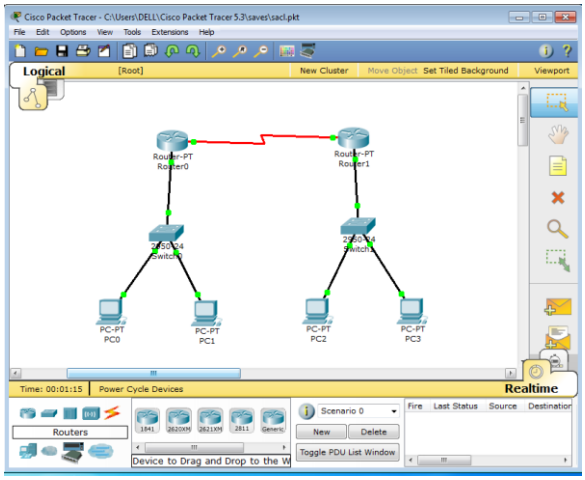

Figure 3.Networking Model in Cisco Packet Tracer

The algoritm for Standard ACL as well as Extended ACL are discussed below:

A. Standard ACL:

First step is to configure the CISCO Routers.

Configuration of Router0 using RIP protocol is as follows:

Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s2/0
Router(config-if)#ip add 192.168.10.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down
Router(config-if)#int f0/0
Router(config-if)#ip add 192.168.20.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#router rip
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0

All Rights Reserved © 2016 IJSETR

```
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#write memory
Building configuration...
[OK]
```

Configuration of Router1 using RIP protocol is as follows:

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#int s2/0
Router(config-if)#ip add 192.168.10.2 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown

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

Router(config-if)#int f0/0
Router(config-if)#ip add
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial2/0, changed state to up
192.168.30.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

Router(config-if)#router rip
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.30.0
Router(config-router)#exit
Router(config)#access-list 10 deny host 192.168.20.2
Router(config)#access-list 10 permit 192.168.20.0 0.0.0.255
Router(config)#interface fast 0/0
Router(config-if)#ip access-group 10 out
Router(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
Router#write memory
Building configuration...
[OK]
Router#
```

Configuration of PC:

Figure 4 shows the configuration of PC0.

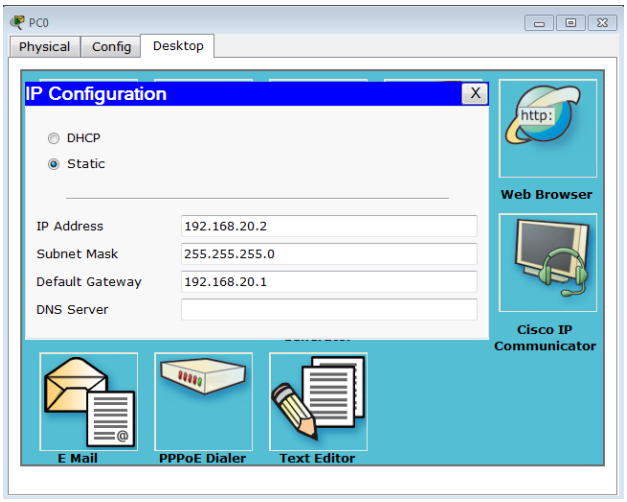

Figure 4. Configuring PC0

B. Extended ACL:

Similar to standard ACL firstly routers are configured and then extended numbered ACL is congifured. Figure 5 shows the network model for extended ACL.

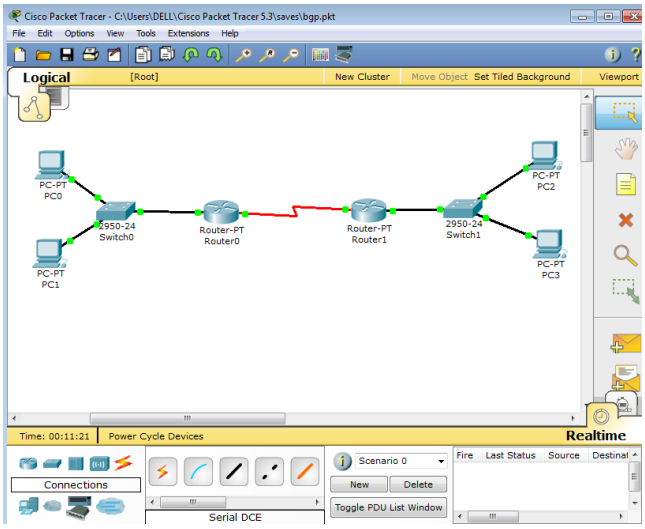

Figure 5. Extended ACL

Configuration of Router0 using RIP protocol is as follows:

```
Router>en
Router#config  t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#int s2/0
Router(config-if)#ip add 10.10.10.1 255.0.0.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to
down
Router(config-if)#int f0/0
Router(config-if)#ip add 20.20.20.1 255.0.0.0
Router(config-if)#no shutdown
```


All Rights Reserved © 2016 IJSETR

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#exit
Router(config)#access-list 101 deny tcp host 20.20.20.2 10.10.10.2 0.255.255.255 eq telnet
Router(config)#access-list 101 permit tcp 20.0.0.0 0.255.255.255 10.10.10.2 0.255.255.255 eq telnet
Router(config)#access-list 101 permit ip any any
Router(config)#int f0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Configuration of Router1 using RIP protocol is as follows:

Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s2/0
Router(config-if)#ip add 10.10.10.2 255.0.0.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown

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

Router(config-if)#int f0/0
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
ip add 30.30.30.1 255.0.0.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 30.0.0.0
Router(config-router)#line vty 0 4
Router(config-line)#password 1234
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable secret qwerty
Router(config)#

Verify the Telnet access:

Figure 6 shows that when the host i.e. PC1 connected to Router0 tries to telnet serial port connected to Router1, the access-list permits the host to route the packets.

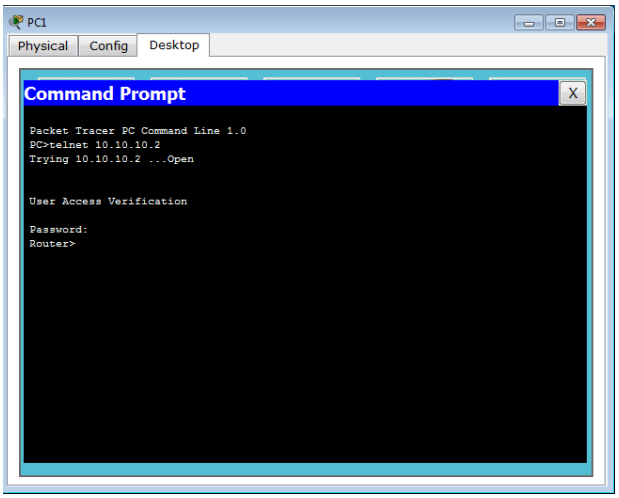

Figure 6. Router0 host can Telnet Router1

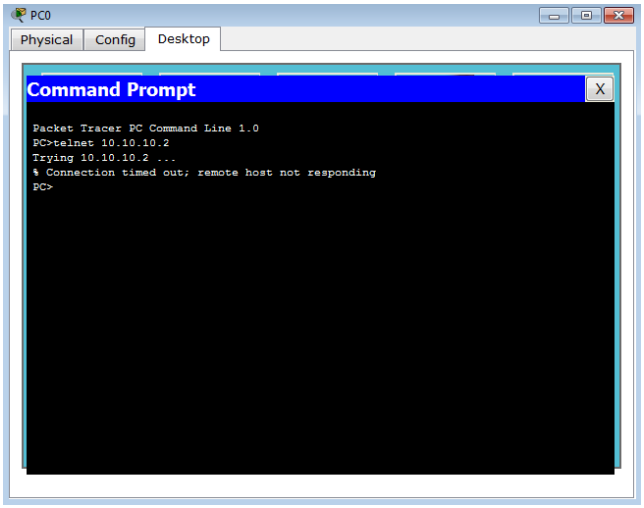

Figure 7. Router0 can't Telnet Router1

Figure 7 shows that when the host i.e. PC0 connected to Router0 tries to telnet serial port connected to Router1, the access-list denies the host to route the packets.

VIII. CONCLUSION AND FUTURE SCOPE

This paper shows the configuration of standard ACL and extended ACL on the router. The standard ACL create filters based on source addresses only and are used for server based filtering, where as extended ACL provide more security by creating filters based on source addresses as well as destination addresses, protocol and port number. The extended ACL in this paper used TCP/IP protocol. Routing Information Protocol (RIP) is used for routing the packets.

In future work, more IP protocols such as UDP, ICMP and IP can be used in extended ACL. Apart from RIP routing protocols , EIGRP, OSPF and BGP routing protocols can be used for routing packets.

All Rights Reserved © 2016 IJSETR

REFERENCES

[1] Pritesh K. Jain, Manoj Sindhwani, S. Sachdeva, "Comparative Study of Routing Protocols with Subnetting Implementation in Cisco Packet Tracer", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 12, dec. 2014.

[2] S. Pozo, A.J. Varela-Vaca, and R.M. Gasca.,"A quadratic, complete, and minimal consistency diagnosis process for firewall acls", *Advanced Information Networking and Applications (AINA), 24th IEEE International Conference* , pages 1037-1046, april 2010.

[3] David E. Taylor."Survey and taxonomy of packet classification techniques."*ACM Computing Surveys*, Vol. 37, No. 3, 2005. Pages 238-275

[4] A. Velte and T. Velte."Cisco: A Beginner's Guide", *McGraw-Hill Inc.* 3rd edition (2004).

[5] Cisco Systems Inc. *http://www.cisco.com*

[6] 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.

[7] Lammle, Todd. (2011). *Cisco Certified Network Associate Study Guide*, *Wiley Publishing*, Inc., Seventh Edition.

Shipra Suman, PG Student, Department of Electronics and Communication Engineering, SHIATS, Allahabad, India

Er. Aditi Agrawal, Assistant Professor, Department of Electronics And Communication Engineering, SHIATS, Allahabad, India

.

All Rights Reserved © 2016 IJSETR