IJCTA, 9(22), 2016, pp. 341-345

Analysis of ACL on various Application Layer Protocols

Shweta yadav, Ravi Shankar Singhal* Ashish Bajpai* Sanjiv Sharma**

Abstract : In this paper we provide security to private network by controlling the flow of incoming and outgoing packets which causes traffic congestion and also concern privacy of network. An ACL is used to define type of traffic and check for allowing or restriction of packet at the router and also limits updating of routing. A comparison is made between the different types of access control lists (ACL) by using various application layer protocols.

Keywords : Access-control Lists (ACL), Standard ACL, Extended ACL, Named ACL.

1. INTRODUCTION

An ACL provides basic level of network security and it has a set of rules to specify the handling of traffic across the router interface (enter or exit).this list commands the router which packet to accept or deny on network on the condition that only one ACL per protocol per interface per direction is applied. If there is no ACL applied over a network than all data frames will get randomly distributed over the network paths and trouble the flow of other data packets hence, causing congestion in traffic by this we see the importance of ACL applied on networks. Here, statements operated in sequential and logical order and different types of ACLs like standard ACL, extended ACL, named ACL is used.

Here we see which ACL works better over network by comparing different ACL using various application layer protocol (TELNET and FTP) using Graphical Network Simulator 3(GNS3) software

2. PERFORMANCE ANALYSIS

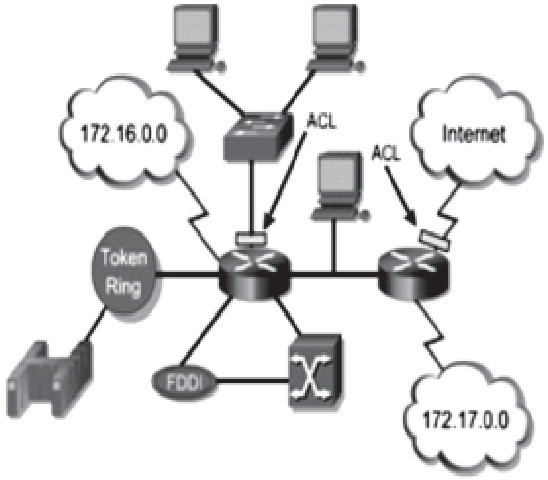


Fig. 1. An arbitrary ACL.

* Dept. of Electronics & Communication Engineering Amity School of Engineering and Technology Uttar Pradesh-201303, India

** Dept. Of Computer science & Engineering, KIET Ghaziabad Utter Pradesh -201206, India syadav3@amity.edu, ashishvirgo12 @gmail.com, ravi247663@gmail.com, sanjiv.sharma@kiet.edu

The numbered access-list and named access-list are two categories of ACL. Numbered access-lists again comprises standard and extended access-lists. A standard access list is based on network subnet or host address and by this its checks source address of the packets and then it permit or deny the packets based on network subnet or host address. To block all the traffic from a network we uses standard access list.

When it comes to packet filtering standard access list fails to cover all the policies that we applied then we make use of extended ACL. The full syntax of the standard IP ACL command for creating the accessing list is:

Router(config)#access-list access-list-number {deny| permit} source_address wildcard_mask

an example for standard ACL to block all traffic except that coming from source 10.1.1.x.

```
interface Ethernet 0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
access-list 1 permit 10.1.1.0 0.0.0.255
```

Now extended access list check for both sourcr and destination addresses for filtering process and based on protocol consist with in a suit(TCP/IP) and port number it filters the traffic. This type of list is widely and oftenly used because it has more granularity than standard access list. It provides good control over network and used where we are more specify about the traffic we want to block. The full syntax of the extended IP ACL command for creating the accessing list is:

Router(config)#access-list access-list-number {deny | permit}[ip| tcp| icmp] source_address source_mask destination_address destination_mask [eq| neq| lt| gt|] port_number

Numbered access list has also various advantages that we can transmit the packets at very high speed and provide more flexibility to implement security policies and here also no need to specify all type of attack in a list as it can filtered out a lots of garbage from their own.

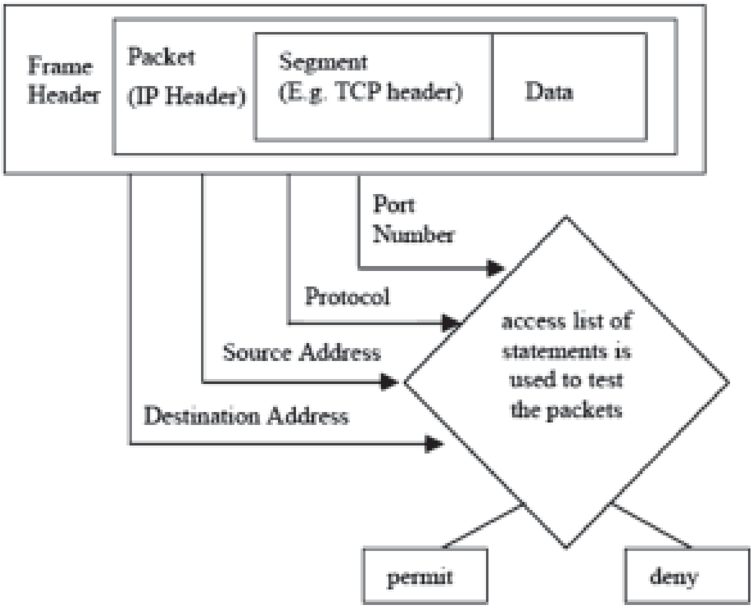


Fig. 2 Format for router and ACLs

A named access lists can be either standard or extended access lists according to the need we can use this type of access list. In this, we can add or delete any statement whereas in numbered access lists if we delete any single statement then whole statements are deleted. We can also give priority to any access lists and according to our need we can change it anytime.

The full syntax of the named IP ACL command for creating the accessing list is:

ip access-list {standard| extended} name

Example given below explains named ACL creation more clearly in order to block all the traffic except the Telnet connection from host 10.1.1.2 to host 172.16.1.1.

```
interface Ethernet 0/0
ip address 10.1.1.1  255.255.255.0
ip access-group in_to_out in
ip access_list extended in_to_out
permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

A. How Acl Works

Firstly, evaluation of packet is done by ACL with top to down approach and then it either permit or deny the packets. When true condition is matched then it stops the further checking of ACL statements. The packets which originated with in the router is cannot be blocked.

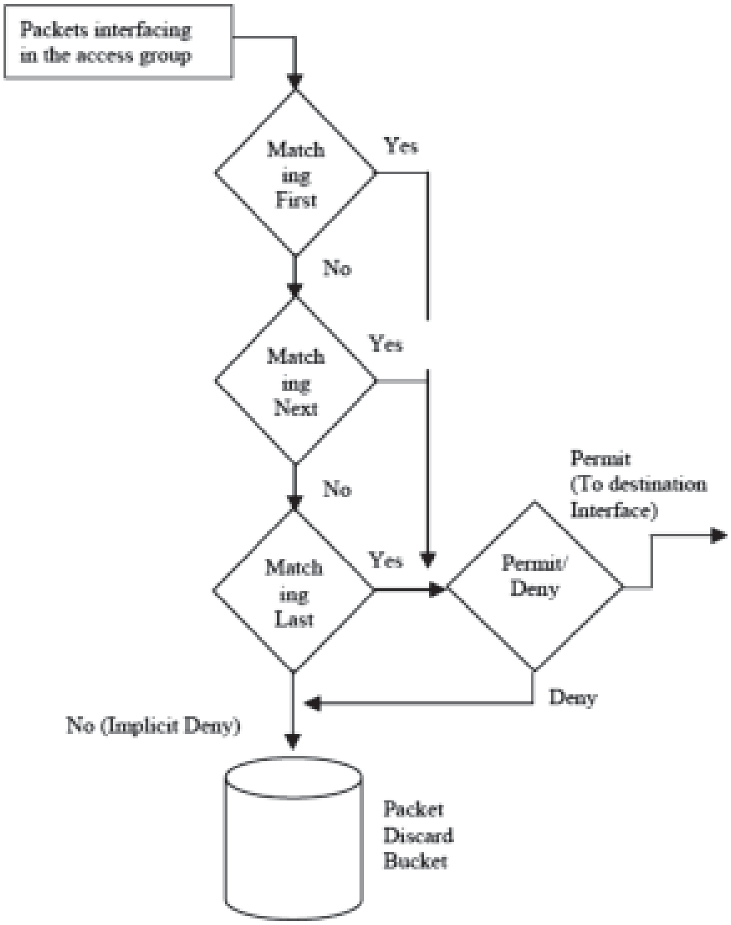


Fig. 3 Flow diagram showing working of ACL

An ACL is created same as if-then statement with every permit statement there is by default denial statement is attached for all other networks which is implicit but here, we need to specify which network will be permitted or not.

2 RESULTS AND DISCUSSIONS

Here, simulation result showing that permission on specific allplication layer protocol TELNET or FTP can be created. Whereas, in extended access list it cannot be done. With named access list any application layer protocol is applied. It can also be seen that meanwhile access control list is providing basic security, traffic prioritising, reduced updations and blocking of traffic.

Table 1. Simulation Results of Different ACLs

Parameters	*Standard ACL*	*Extended ACL*	*Named ACL*
IP Range	1-99	100-199	Not numbered
Prioritization	Not possible	Not possible	Possible
ACL Placement	Closest to the destination address	closest to the source address destination address	Either at source address or

In fig 4, standard access list denying host and the results are given below:

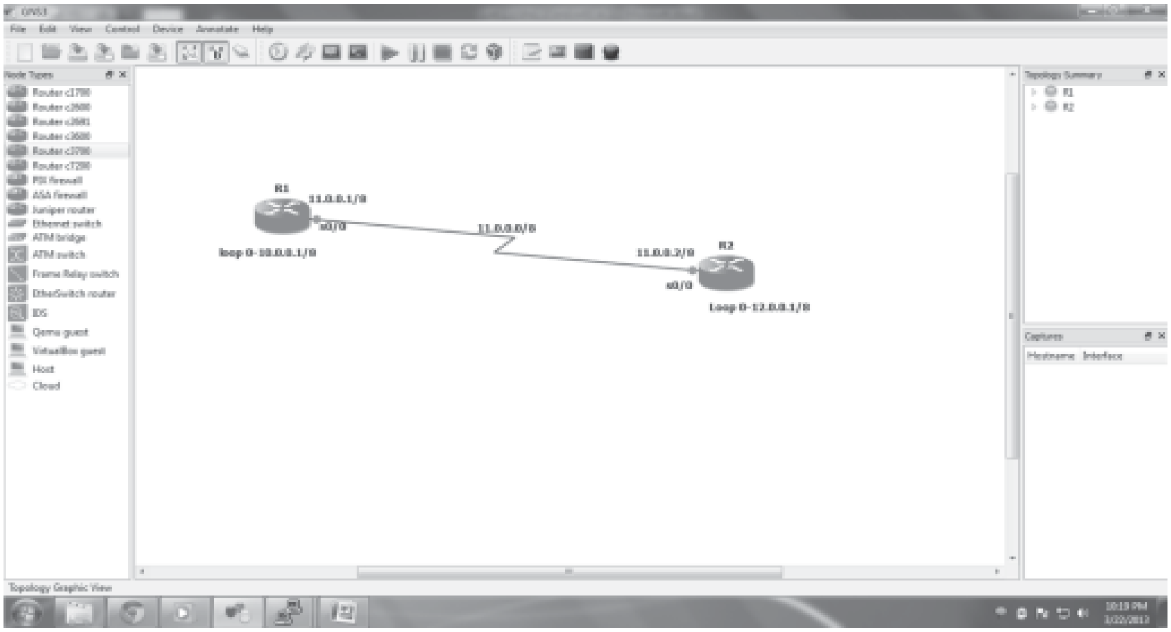
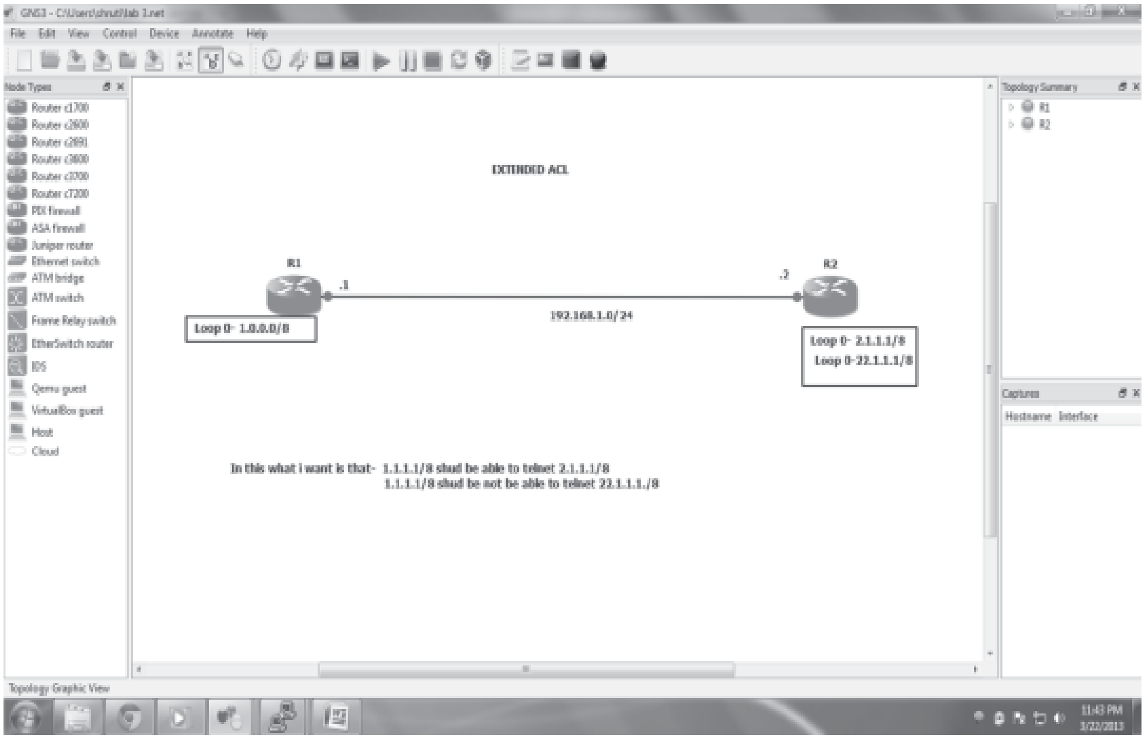
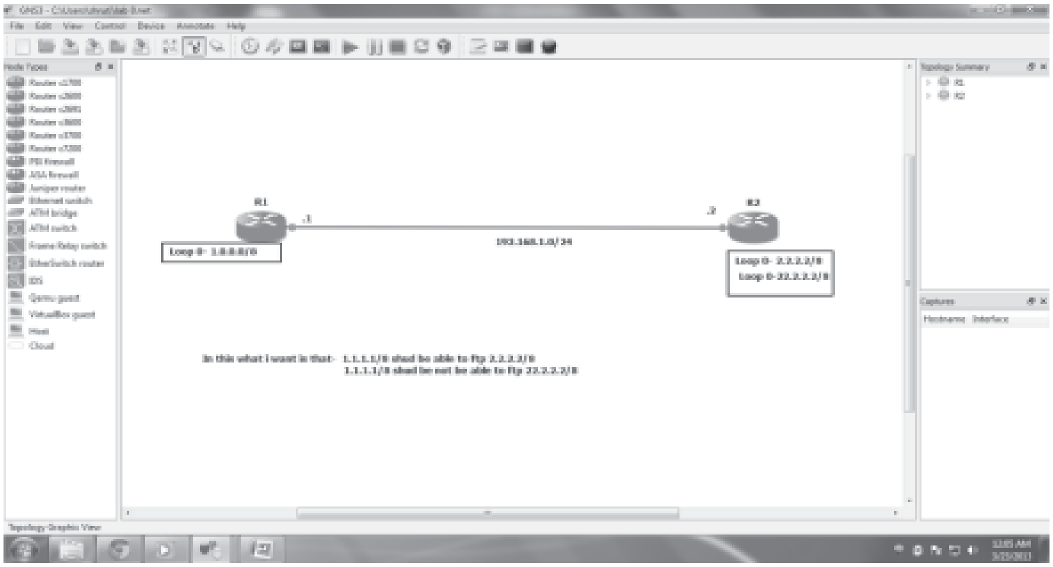


Fig. 4. Screenshot of denying a host using Standard Access List



In this what I want is that- 1.1.1.1/8 shud be able to telnet 2.1.1.1/8
1.1.1.1/8 shud be not be able to telnet 22.1.1.1./8

Fig. 5. Screenshot of denying a host from Telnet using Extended Access List



In this what i want is that- 1.1.1.1/8 shud be able to ftp 2.2.2.2/8
1.1.1.1/8 shud be not be able to ftp 22.2.2.2/8

Fig. 6. Screenshot of denying a host from FTP using Extended Access List

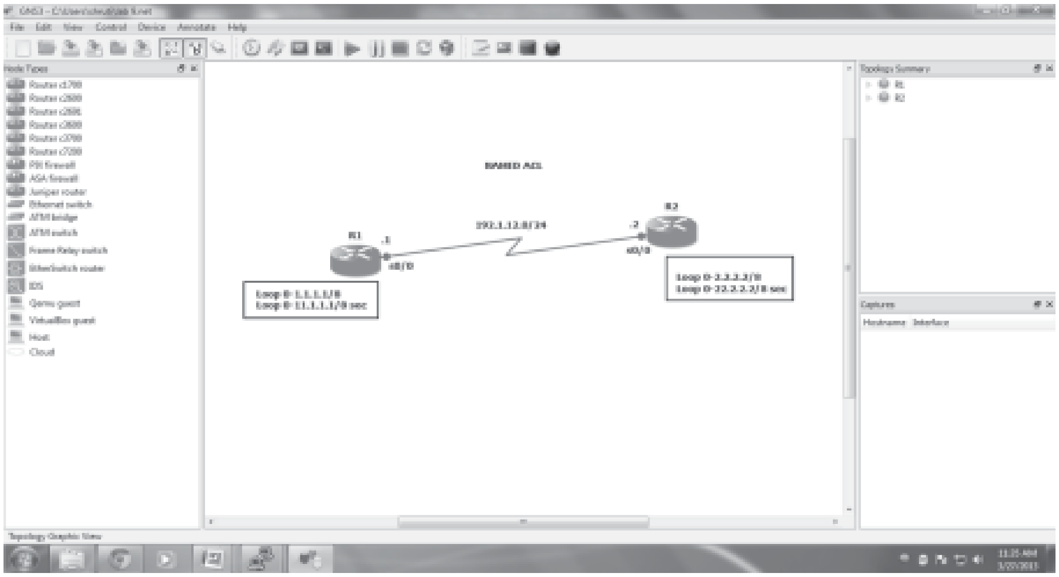


Fig. 7. Screenshot of denying a host from Telnet using Named Access List.

4. CONCLUSIONS

Different ACL have been compared and it has been observed that standard access list is failed to create permission on specific protocols but same can be done by extended and named access list.

5. REFERENCES

1. Coynek, E. J., Sandhu, R. S., Feinsteink, H. L., and Youman, C. E., (1996). “Different Access Control Models IEEE Computer”, Volume 29, Number 2, February 1996, pp. 38-47.
2. National Institute of Standards and Technology, (2004). Special Publication 800-12: An Introduction to Computer Security- The NIST Handbook.
3. Miao Zhao, Huiling Zhu, V.O.K. Li, Yuanyuan Yang, “Contention Based Prioritized Opportunistic Medium Access Control in Wireless LANs” in Proc. IEEE ICC 2006, pp. 3820-3825.
4. Solms, S. H., and Isak, M., (1994). “The management of computer security profiles using a role-oriented approach” Computers and Security, 13(8): pp. 673-680.[5]Trent, J. and Tidswell, J.E., (2001). Practical safety in flexible access control models. ACM Transactions Information and System Security, 4(2) pp. 158-190.