

# Access Control List: Route-Filtering and Traffic Control

**Amith Vishnu<sup>1</sup>, Kavyashree M<sup>2</sup>**

B.E, Department of CSE, BIT, Bangalore, India <sup>1</sup>

Student, MTech, Department of Digital Communication, RVCE, Bangalore, India<sup>2</sup>

**Abstract:** The third layer of the Open System Interconnect (OSI) reference model is the Network Layer. The Network layer handles traffic, addressing and accounting. The network Layer controls the operation of the subnet, deciding which physical path the data should take based on the network conditions, priority of service and other factors. It translates logical addresses, or names into physical address. A router is a layer 3 device and is a networking device that forwards data packets between computer networks. A network is configured with routing protocols-static or dynamic routing because these routing protocols define/specify how the communication packets are forwarded and the route selection process (optimum route selection). In this paper we have considered a network topology in which a certain part of the network is configured with OSPF protocol and enclosed within area 0 and the other part, with routers configured with RIP, version 2. Route redistribution is carried out at the boundary routers of the two sections of the network. Since, OSPF and RIP v2 are entirely different routing protocols; route redistribution is done on the boundary routers belonging to both the sections. Route redistribution [1] allows routes from one routing protocol to be advertised into another routing protocol. Finally, in this paper we configure Access Control List (ACL) on the network. ACL also called Access-List can be configured for all routed network protocols to filter the packets of those protocols as the packets pass through a router. Main function of ACL is to filter network traffic by controlling whether router packets are forwarded or blocked at the router's interfaces and also provide security in the network on which it is configured.

**Keywords:** Open System Interconnect (OSI), reference model, traffic, addressing and accounting, Access Control List (ACL), packets are forwarded or blocked at the router's interfaces and also provide security in the network.

## I. INTRODUCTION

The third layer of OSI reference model called the network layer plays an important role in /plays the following roles

- Routing-Moving data across a series of interconnected networks, selecting an optimum/best route between source and the destination and looking for an alternative route for packet communication in case of any link failure.
- Data Encapsulation-The network layer normally encapsulates messages received from higher layers by placing them into datagram with a network layer header.
- Logical addressing-Translates logical addresses, or names into physical addresses.
- Error handling and diagnostics-Special protocols are used at the network layer to allow devices that are logically connected, or that are trying to route traffic, to exchange information about the status of the hosts on the network or the devices themselves.
- Frame fragmentation-If it determines that a downstream router's Maximum Transmission Unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at destination station.

In this paper we discuss in detail the Access Control List (ACL). ACL are filters that allow or deny certain (specific) routing updates or packets in or out of a network. ACL are used in route filtering and security for the network. ACL can be applied on routers and traffic can be filtered by a network administrator. This can be done by simply permitting or denying network hosts or addresses (IP addresses). ACL's can be configured for all routed network protocols. ACL's provide security for the network by denying certain network hosts or addresses thereby allowing one host to access a part of a network and prevent another host from accessing the same area. In this paper the IP address 1.1.1.1 which is an interface loopback is seen only in the region configured with OSPF and is denied in the region configured with RIPv2 routing protocol. In this paper we also demonstrate the real time applications of ACL's through a small example.

## II. ROUTE REDISTRIBUTION

Route Redistribution [1] allows routes from one routing protocol to be advertised into another routing protocol. A boundary router which is running both the routing protocols and lies in the boundary of two routing domains is called the redistribution point. There must be at least one such router to carry out redistribution of routes between the domains

running different routing protocols. To be plain, it is a simply a translator capable of translating any spoken language in a particular region to another language in the other region. Here the boundary router configured with both the routing protocols existing in the two domains and redistribution command configured on the router is the translator; the two regions are the network regions running two different routing protocols.

Ex: - OSPF [2] in region 1 and RIP v2 in region 2 as shown in figure 1.

### III.ACL – ACCESS CONTROL LIST

Access Control Lists or simply Access-List are a set of permit and deny commands to provide a powerful way to control traffic into and out of a network forwarding packets. A router acts as a packet filter when it forwards or denies packets according to filtering rules as per configuration done by network admin on the interface of the routers. ACL on interface can control two types of traffic- incoming and outgoing traffic to/from a router called inbound and outbound traffic respectively. As a layer 3 device [3], a packet-filtering router uses rules to determine whether to permit or deny traffic based on source and destination IP addresses, source port and destination port, and the protocol of the packet. Figure 2 shows ACL on routers [4].

These are two types of ACL's.

- Standard Access- Lists

Standard access lists create filters based on source addresses and are used for sever based filtering. Address based access lists consist of a list of addresses or address ranges and form a statement as to whether access to or from that address is permitted or denied. It ranges from 1 to 99. Figure 3 shows the syntax of configuring standard access list and extended access-list on routers.

- Extended Access- Lists

Extended access lists create filters based on source addresses, destination addresses, protocol, port number and other features and are used for packet based filtering of packets that traverse the network. It ranges from 100-199.

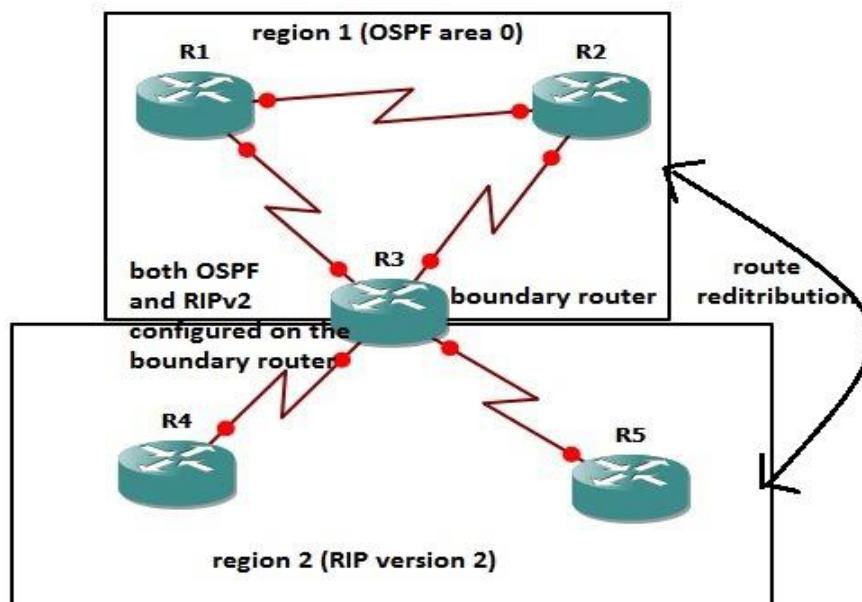


Figure 1 shows OSPF in region 1 and RIP v2 in region 2

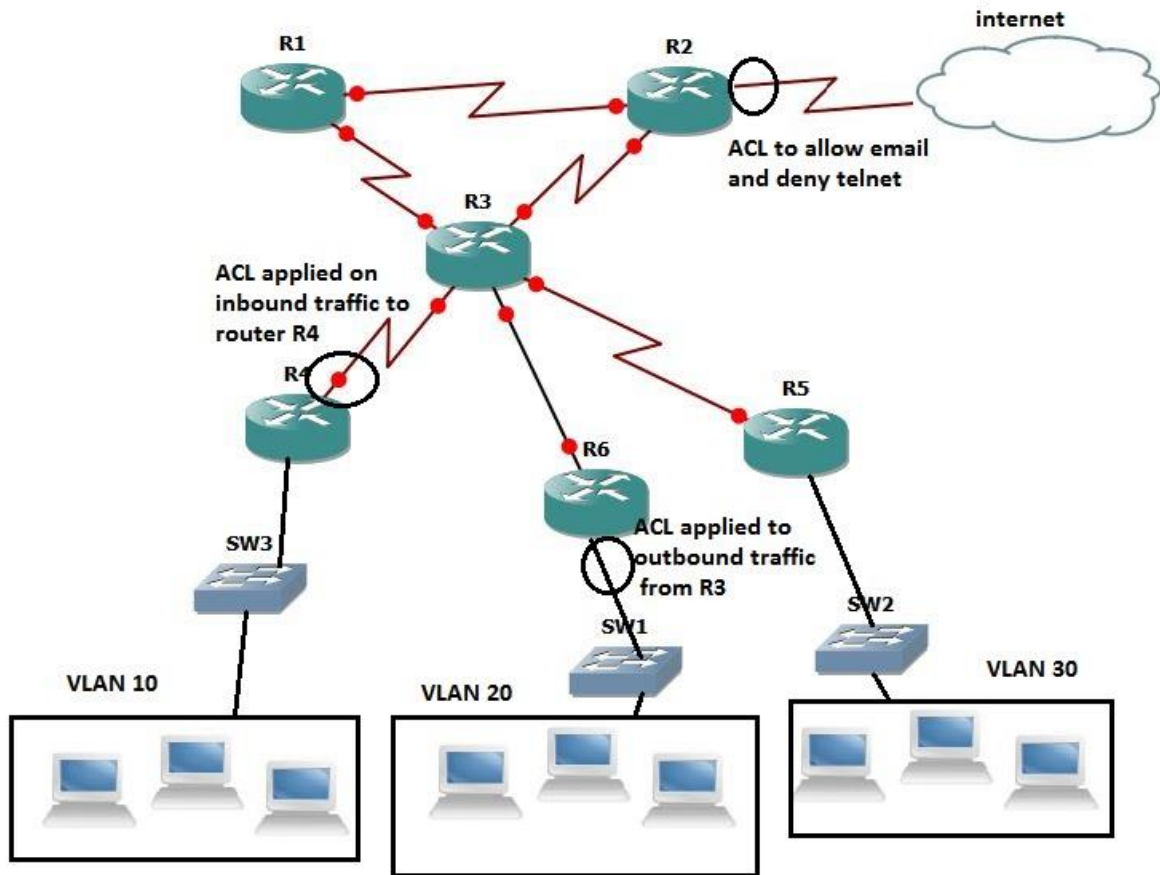


Figure 2 shows ACL on routers.

**standard access-list:**

```
router(config)#access-list{1-99} {permit/deny} source-addr
[source-wildcard]
```

**extended access-list:**

```
router(config)#access-list {100-199} {permit/deny} protocol
source-addr [source-wildcard] [operator operand]
destination- addr [destination-wildcard] [operator operand]
[established]
```

Figure 3 shows the syntax of configuring standard access list and extended access-list on routers

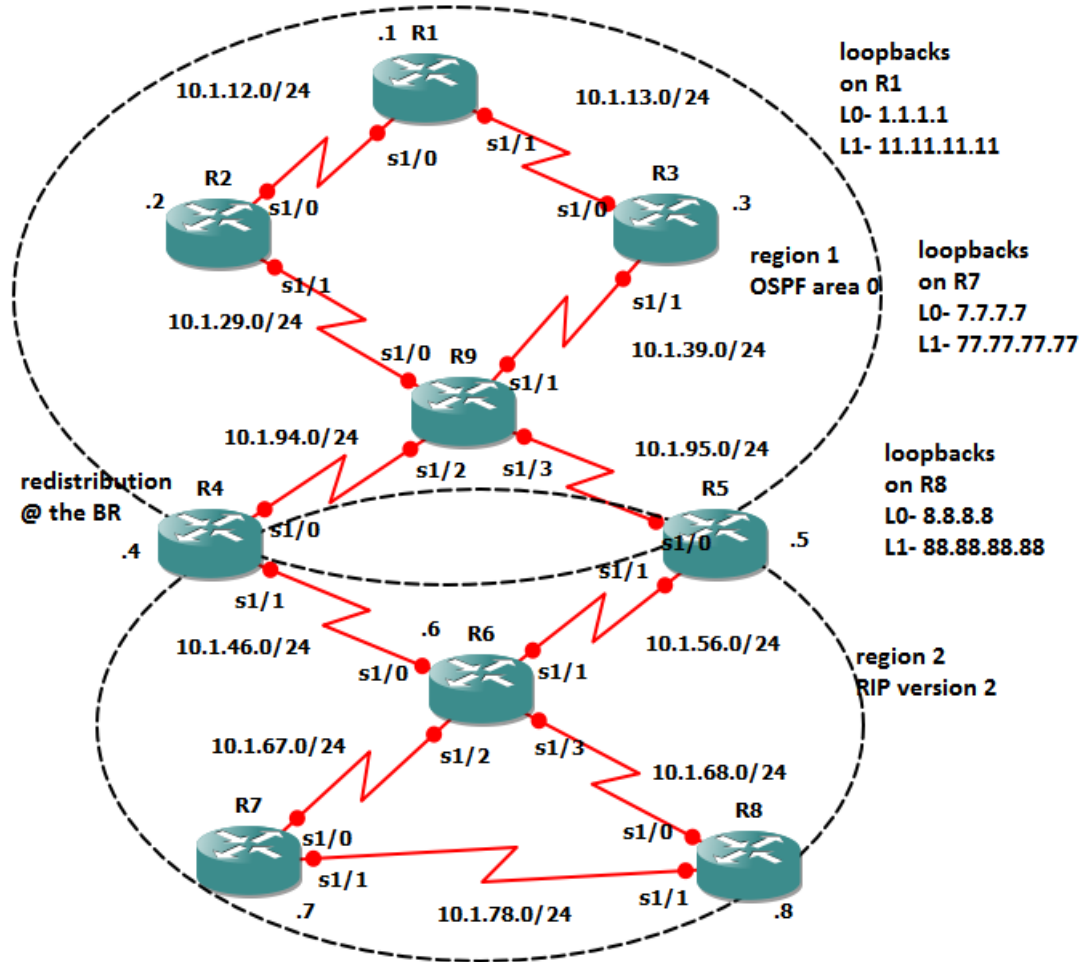
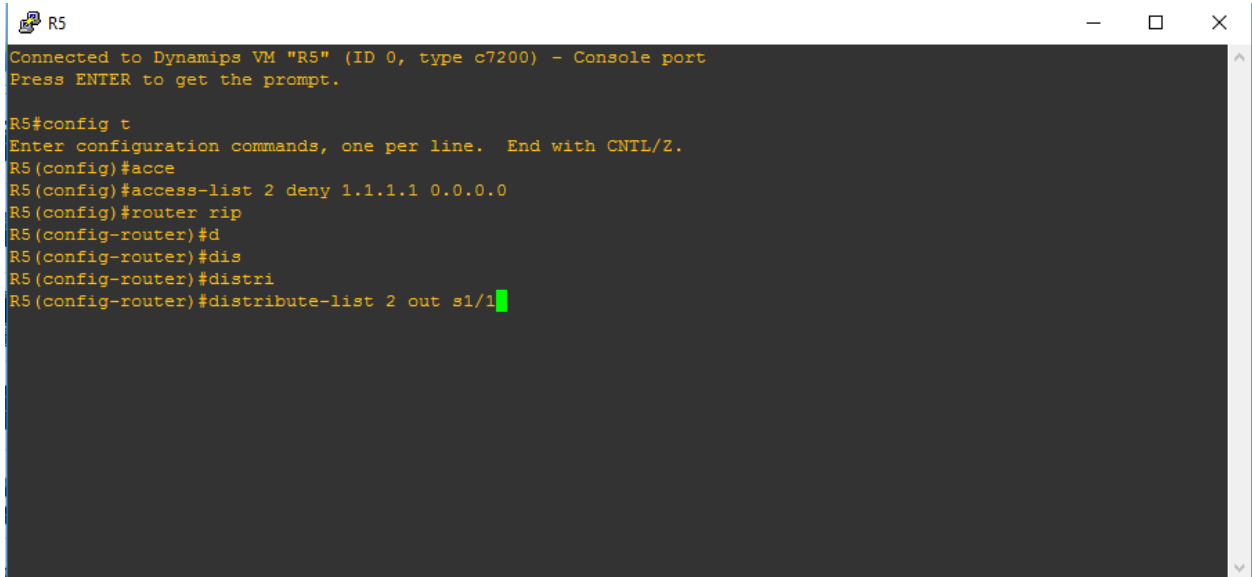


Figure 4 shows the network topology of interest.

```

R4
*Aug 9 14:34:27.519: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Aug 9 14:34:27.523: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Aug 9
R4#14:34:27.851: %SNMP-5-COLDSTART: SNMP agent on host R4 is undergoing a cold start
R4#
*Aug 9 14:34:36.179: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
R4#
R4#
R4#
R4#
R4#
R4#
R4#config
Configuring from terminal, memory, or network [terminal]? config t
?Must be "terminal", "replace", "memory" or "network"
R4#config t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#access
R4(config)#access-list 1 deny 1.1.1.1
*Aug 9 14:35:56.163: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R4(config)#access-list 1 deny 1.1.1.1 0.0.0.0
R4(config)#router rip
R4(config-router)#distribute-list 1 out s1/1
  
```

Figure 5 shows the ACL configuration of router R4.



```

R5
Connected to Dynamips VM "R5" (ID 0, type c7200) - Console port
Press ENTER to get the prompt.

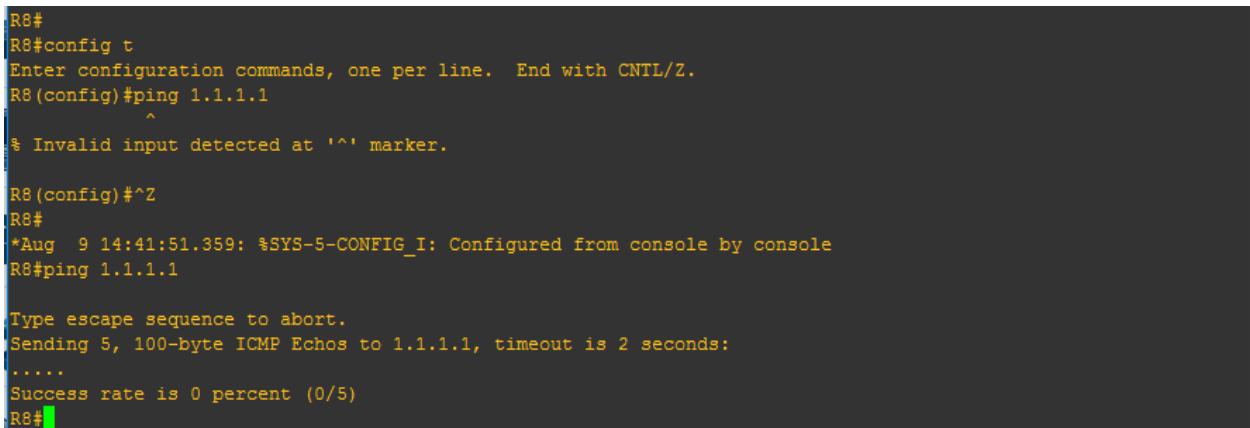
R5#config t
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#acce
R5(config)#access-list 2 deny 1.1.1.1 0.0.0.0
R5(config)#router rip
R5(config-router)#d
R5(config-router)#dis
R5(config-router)#distri
R5(config-router)#distribute-list 2 out s1/1

```

Figure 6 shows the ACL configuration of router R5

#### IV. NETWORK TOPOLOGY

Figure 4 shows the network topology of interest. The entire topology is divided into two regions or sections [5]. Region 1 consists of router R1, R2, R3, R9, R4 and R5 configured with OSPF routing protocol and area 0. The other region consists of routers R7, R6 and R8 configured with RIP, version 2 protocol. R4 and R5 are made the boundary routers and run both OSPF routing protocol and RIP v2 routing protocol both of which are internal gateway protocols [6] and dynamic routing protocols. Suppose region 1 and region 2 are merged due to an agreement signed for a merger, two regions run two different protocols and route redistribution need to be done on the boundary routers. Route redistribution allows routes from one region running a routing protocol to be advertised in another region running a different routing protocol. Now ACLs need to be applied on the network for traffic filtering and security. In this paper we apply outbound ACL on s1/1 interface of router R4 and s1/1 interface of router R5. Figure 5 and 6 shows the ACL configuration of R4 and R5 respectively.



```

R8#
R8#config t
Enter configuration commands, one per line. End with CNTL/Z.
R8(config)#ping 1.1.1.1
^
% Invalid input detected at '^' marker.

R8(config)#^Z
R8#
*Aug 9 14:41:51.359: %SYS-5-CONFIG_I: Configured from console by console
R8#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R8#

```

Figure 7 shows the implementation of ACL on R4 by ping test

#### V. RESULTS AND FINDINGS

When an attempt was made to ping router R8 through interface loopback 1.1.1.1, the ping failed because IP address 1.1.1.1 is denied by applying ACL at the interface s1/1 of router R4 and R5 (outbound traffic). But IP 1.1.1.1 is seen in the OSPF region and not in the region configured with RIP. Figure 7 shows the implementation of ACL on R4 by ping test.

**VI. CONCLUSIONS**

Access Control List or simply Access-Lists are a set of statements/commands configured on a router, routing packets at layer 3 by selecting the optimum path between source and destination, selected by the routing protocol. ACLs limit network traffic to increase network performance. ACLs configured on a network provide traffic flow control by restricting the delivery of routing update. It also provides additional security by denying host or IP addresses and is very simple to configure.

**REFERENCES**

- [1] Route Redistribution-A Case Study - ijarccce- [www.ijarccce.com/upload/2017/june-17/IJARCCCE%2042.pdf](http://www.ijarccce.com/upload/2017/june-17/IJARCCCE%2042.pdf)
- [2] Open Shortest Path First- A Case Study - ijarccce- [www.ijarccce.com/upload/2017/june-17/IJARCCCE%2096.pdf](http://www.ijarccce.com/upload/2017/june-17/IJARCCCE%2096.pdf)
- [3] Open Shortest Path First - Router Alley- [www.routeralley.com/guides/ospf.pdf](http://www.routeralley.com/guides/ospf.pdf)
- [4] Configuring IP Access Lists - Cisco- <https://www.cisco.com/c/en/us/support/docs/security/ios.../23602-confaccesslists.html>
- [5] Conceptual Study of Wireless BAN using Bluetooth/IEEE 802.11n - DOI-10.17148/IJARCCCE.2016.51184
- [6] Open Shortest Path First (OSPF) Routing Protocol and the Use of Virtual-Links-DOI10.17148/IJARCCCE.2017.6733-  
<http://www.ijarccce.com/upload/2017/july-17/IJARCCCE%2033.pdf>