CONFIGURATION OF ACCESS CONTROL LIST APPLICATIONS: ROUTE FILTERING AND TRAFFIC CONTROL FOR ENTERPRISE NETWORK DESIGN USING CISCO PACKET TRACER SIMULATION TOOL

Rajamohan Parthasarathy[1*], Murali Krishnan N[2], Ilangovan Perumal[3], Preethy Ayyappan[4], Leelavathi Rajamanickam[5], Syazwina Binti Alias[6]

[1 & 6] Centre for Computer Networks and IoT, Faculty of Engineering, Built Environment and Information Technology, SEGi University, Malaysia.

[2] Faculty of Humanities, Department of Media and Communication, Curtin University, Sarawak Campus, Malaysia.

[3] Faculty of Business, Accountancy, Communication and Hospitality Management, SEGi University, Malaysia.

[4 & 5] Faculty of Engineering, Built Environment and Information Technology, SEGi University, Malaysia.

[*] For correspondence; Tel. + (60) 0183822197, E-mail: *prajamohan@segi.edu.my & parthasarathy_rajamohan@yahoo.com murali.krishnan@curtin.edu.my, Ilangovan@segi.edu.my, ayyappan@segi.edu.my*, leelavathiraj@segi.edu.my, syazwinaalias@segi.edu.my

ABSTRACT *- The third layer of Open System Interconnection (OSI) reference model referred Network Layer. Traffic, addressing, and accounting are all handled by the Network layer. The Network Layer oversees the operations of the subnet, determining which physical path data should travel based on network conditions, service priority, and other criteria. It converts logical addresses, also known as names, to physical addresses. Since routing protocols define/specify how communication packets are routed and the route selection process, a network is configured with static or dynamic routing protocols (optimum route selection). This paper starts by outlining the basics of access control list (ACL) technology, including hardware specifications and software configuration. The paper then goes through the topological structure of enterprise network planning, as well as demonstrating the use of ACL technology in an enterprise network with examples. Both routed network protocols may have an ACL, also known as an Access-List, configured to filter their packets as they pass through a router. An ACL's primary function is to filter data traffic by determining whether router packets should be transferred or prevented at the router's interfaces and provide security.*

Keywords - Access Control List (ACL), Packets Forward, Packets Blocked, Inter-firewall Optimization; IP Packet Filtering.

I. INTRODUCTION

The information in each packet's header is used by routers to make routing decisions. The routing table determines how traffic is routed as it enters a router interface. The router compares "the destination IP internet packet address to routes in the routing database to determine which path is the best fit, and then forwards a packet down that path". In the same way, an access control list may be used to filter traffic. An ACL is a set of IOS commands that filter packets depending on the information in their headers. Routers do not come with ACLs by default. When an ACL is applied to an interface, the router must evaluate all network packets going through it to see if they can be routed. The access control list entries are a series of authorize or deny statements (ACEs).

1.1 Purpose of ACLs

An ACL uses ACEs, which are a sequential array of allowing or refuse to accept statements. ACLs are supported by Cisco routers in both standard and extended forms. Before packets are transmitted to the outside interface, an inbound ACL filters them [1].

Stage 1: "The router observe and understand the packet header and determines the IPv4 address of the source".

Stage 2: "The initial process of the ACLs, the router contrasts the source address of IPv4 to each ACE in sequence".

Stage 3: "If a condition is met, the router executes the command permitting or restricting the packet, and any remaining ACEs in the ACL are ignored".

Stage 4: "The packet is dropped if the source IPv4 address does not match any of the ACL's ACEs because every ACL has an implicit refuse ACE".

1.2 Masks with wildcards

A 32-bit wildcard mask is used by an IPv4 ACE to select which bits of the address to check for a match. The Open Shortest Path First (OSPF) routing system also uses wildcard masks [1]. A wildcard mask uses the ANDing process to determine which bits in an IPv4 address to match, similar to how a subnet mask does. For one host, one subnet, and a set of IPv4 addresses, a wildcard mask is used to filter network data traffic. "Subtracting the subnet mask from 255.255.255 is a viable technique for determining a wildcard mask. Keywords cut down on the amount of keystrokes needed to access the ACL and make ACEs easier to read [1].

1.3 Creation of ACL Guidelines

The number of ACLs that can be applied to a router interface is limited. For example, ACLs can be set to apply to a dual-stacked (IPv4 and IPv6) router interface. One outbound IPv4 ACL, one inbound IPv4 ACL, one inbound IPv6 ACL, and one outbound IPv6 ACL are all present on a router interface. It is not necessary to configure ACLs in both directions [1]. The quantity of ACLs added to the interface, as well as the order in which they are introduced, are defined by the security policy and strategy of the organization. Before configuring an ACL, some provisional planning is required, which includes the best practices listed below. [1]:

- ACLs should be based on the security policy of the company to build, edit, and save all of our ACLs, use a text editor. Using the remark order, to keep track of ACLs.
- Test ACLs on an advancement network prior to conveying them on a creation organization.

1.4 IPv4 Access Control Lists (ACLs) Types

IPv4 ACLs are classified into two types: There are two types of ACLs: standard ACLs and extended ACLs. Packets are allowed or denied by standard ACLs only based on their IPv4 originating address. Extended ACLs allow or deny packets based on their source and destination IPv4 addresses, protocol type, source and destination TCP or UDP ports, and other factors [1].

- "The ACLs standard values are 1 to 99 and 1300 to 1999 [1]".
- "Extended ACLs are defined as numbers ranging from 100 to 199 and 2000 to 2699 [1]".

Named ACLs" are the preferred method of configuring ACLs. ACLs, both regular and extended, can be used to get more information about how they work. Any ACL should be placed at the most convenient area. Extended ACLs should be placed as close to the source of the filtered traffic as possible. Unwanted traffic is thus dismissed close to the source network, avoiding the need to traverse communications network infrastructure. Standard ACLs should be placed as close to the destination as possible. The "permit" or "deny" decision will be made based on the stated source address if a standard ACL was applied to the traffic source, regardless of the traffic destination. The ACL's location can be determined by the scope of organizational control, network bandwidth, and ease of configuration [1].

1.5 Filtering of packets anion and operation of ACL

"Packet filtering restricts network access by analyzing incoming and outgoing network packets before forwarding or deleting them based on preset criteria. Layer 3 or Layer 4 packet filtering is possible[1]". "An ACL is a set of rules that offer you additional control over packets that come in through the router's inbound interfaces, packets that are relayed through the router, and packets that leave through the router's outgoing interfaces [1]". ACLs for inbound and outbound traffic can be built independently.

Until packets are forwarded to the outward interface, they are filtered by an inward ACL. If a packet is discarded, an inbound ACL is beneficial because it avoids the overhead of routing lookups. If the ACL allows it, a packet is evaluated for routing. When the network linked to an inbound interface is the only source of packets that need to be inspected, inbound ACLs are the best technique to filter them [1].

Regardless of the incoming interface, an outgoing ACL filters packets after they have been routed. Incoming packets are forwarded to the outward interface, where they are handled by the outbound ACL. When the same filter is applied to packets coming from several inbound interfaces before leaving the same outbound interface, outbound ACLs are the best option. An ACL has a specified behavior when it is applied to an interface. When traffic reaches a router interface with an inbound standard IPv4 ACL configured, for example, these are the operational steps [1]:

Step 1: The router obtains the source IPv4 address from the packet header.

Step 2: The router checks the source IPv4 address to each ACE in order, starting at the top of the ACL.

Step 3: If a match is found, the router will execute the instruction, permitting or disallowing the packet, and the other ACEs in the ACL will not be checked.

Step 4: "If any of the ACL's ACEs do not match the source IPv4 address, the packet is deleted, because all ACLs have an implicit deny ACE."

The last ACE statement in an ACL is invariably an inferred deny that blocks all traffic. This statement is implicitly implied at the end of an ACL by default, despite the fact that it is hidden and not presented in the settings.

II. RELATED WORK

The use of rule reordering to reduce packet classification latency has been proposed. Ordered ACLs have been shown to minimize packet processing time in studies [2]. The study, "on the other hand, did not account for possible inconsistencies between different ACL laws. Individual rule reordering and disputes are not addressed in a later paper" [3], which does reference rule reordering but only in a simplified way by grouping related laws into classes.

Algorithmic techniques were used to find anomalies in firewall datasets [3]. Based on research, a strategy was presented for applying early rejection rules for the most often matched traffic, with sophisticated adjustments when traffic patterns altered. There have been several proposals for storing filtering rules in non-linear data structures, which allows for faster lookup rates than linear lists. The rules are translated into a decision tree in order to achieve this [4]. Hash tables are frequently used to classify packets with a single memory lookup, but their worst-case exponential space complexity limits their utility in devices with restricted memory bandwidth [5].

Ternary Content Addressable Memory (TCAM) has created hardware solutions to the latency issue (TCAMs). In a single memory lookup, these run a concurrent test of all packet filter rules and return the first one that matches. TCAMs are usually found only in the most expensive higher-end core routers models [6-8]. The majority of the research has focused on individual routers, with very little attention paid to packet filter enhancement in a single domain. When a packet traverses numerous packet filters within a domain, several forms of anomalies have been recognized as being comparable to those seen in single sets of filtering rules. [9]. Binary decision diagrams (BDDs) were used to search for anomalies in distributed firewalls using static analysis techniques, allowing the construction of a firewall analysis tool to be made possible [10].

A system for finding and removing redundancy between two nearby firewalls in neighboring domains under separate administrative control has been devised [11]. The protocol allows firewalls to share filtering information without exposing surrounding firewalls' content, which could represent a security risk. On a range of real-world and virtual firewalls, the protocol was put to the test, and it was determined that up to 49% of duplicate rules can be securely deleted [12]. Guarddog [13] is an example of a program that "automatically conducts the translation of a security policy into a set of regulations for usage in routers" outside of manufacturer specifications, but "little work has been done on domain optimization".

The Access Control List is discussed in depth in this article (ACL). ACLs are filters that enable or prevent particular (specific) routing changes or packets from entering or leaving a network.

ACLs are used in route filtering and network protection. ACLs can be added to routers, and network administrators can filter traffic. ACLs provide network protection by refusing access to specific network hosts or addresses, allowing one host to access a section of the network while denying another host access [14].

2.1 Router Redistribution

Path Redistribution [15] enables routes from one routing protocol to be marketed in another. The redistribution point is a boundary router that runs all routing protocols and is located at the intersection of two routing domains. At least one of these routers is needed to redistribute routes between domains using different routing protocols. The translator is the boundary router, which is equipped with both the routing protocols used in the two domains and the redistribution command.

2.2 ACL Standards and Configuration Commands

On a router or switch port, the Cisco Access Control List (ACL) is a traffic filtering system that uses a set of filtering rules to filter traffic. Based on the ACL's conditions, a packet is either allowed or denied further movement.

IP, IPX, AppleTalk, XNS, DECnet, and other routed protocols work with Cisco ACLs. Only TCP/IP-based ACLs will be discussed [1]. There are two kinds of access lists: standard access control lists and extended access control lists according to TCP/IP traffic filtering ACLs [1].

2.3 The Standard ACL command syntax format.

"access-list *access-list-number* {permit|deny} {host|source source-wildcard|any'' [1]

Example of Standard ACL:

"access-list 10 permit 192.168.2.0 0.0.0.255"

This list accepts addresses in the range 192.168.2.0 to 192.168.2.255. Each access list must be identifiable by a name or a number assigned to the protocol's access list when configuring access lists on a router [1].

2.4 The IP Extended ACL command syntax format

"access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence]" [1]

Example of Extended ACL:

"access-list 110 - Applied to traffic leaving the office (access-list 110) (outgoing)"

"access-list 110 permit tcp 192.128.2.0 0.0.0.255 any eq 80"

Traffic from any 192.128.2.0 network address is allowed to pass through ACL 110. According to the 'any' assertion, any traffic can flow to any destination address as long as it goes through port 80.

2.5 The syntax of a router interface ACL command.

The ACL must then be applied to the GUI after it has been defined (inbound or outbound). The following is the syntax for adding an ACL to a router interface:

"interface <interface>"

"ip access-group {number|name} {in|out}"

A name or a number may be used to specify an Access List. The ACL is applied to inbound traffic by "in," and the ACL is applied to outbound traffic by "out". Router interface ACL eg.:

"Router(config)#interface serial 0"

"Router(config-if)#ip access-group 10 out"

III. NETWORK TOPOLOGY DESIGN METHODS AND ACL COMMAND CONFIGURATIONS

A network associate protects the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. This API should not be accessible via a web browser from any other hosts on the LAN or the Core. All other traffic should be allowed because this site provides many business tools and other resources on the Finance Web Server. Create a three-statement numbered access-list for the Finance Web Server that only requires host C web access, and then apply it. The Finance Web Server will not be accessible through the internet from any other hosts. All other types of traffic are allowed. By selecting the appropriate host, you can gain access to the router CLI. All passwords have been changed to "cisco" for the time being. The IP address for the Core link is "198.18.196.65".

The computers in the Hosts LAN have been assigned the IP addresses 192.168.33.1 – 192.168.33.254. The IP 192.168.33.1, 192.168.33.2, 192.168.33.3, and 192.168.33.4 are the addresses of Host PC A, Host PC B, Host PC C, and Host PC D. The servers in the Server LAN have been assigned the IP addresses 172.22.242.17 – 172.22.242.30. The Finance Web Server's IP address is 172.22.242.23. The Public Web Server's IP address is 172.22.242.17.

The following functions must be configured in addition to the primary configuration of the router.

- The first task is to set up ACLs so that host C can connect to the Finance Web Server through the Internet.
- The second task is to prevent other hosts from accessing the Finance web server through the Internet.
- The third task is just to allow all other traffic to pass through.
- The fourth task is to configure the ACL to the Fa0/1 interface (outbound direction)

3.1 Router Enterprise Network Topology Model with ACL

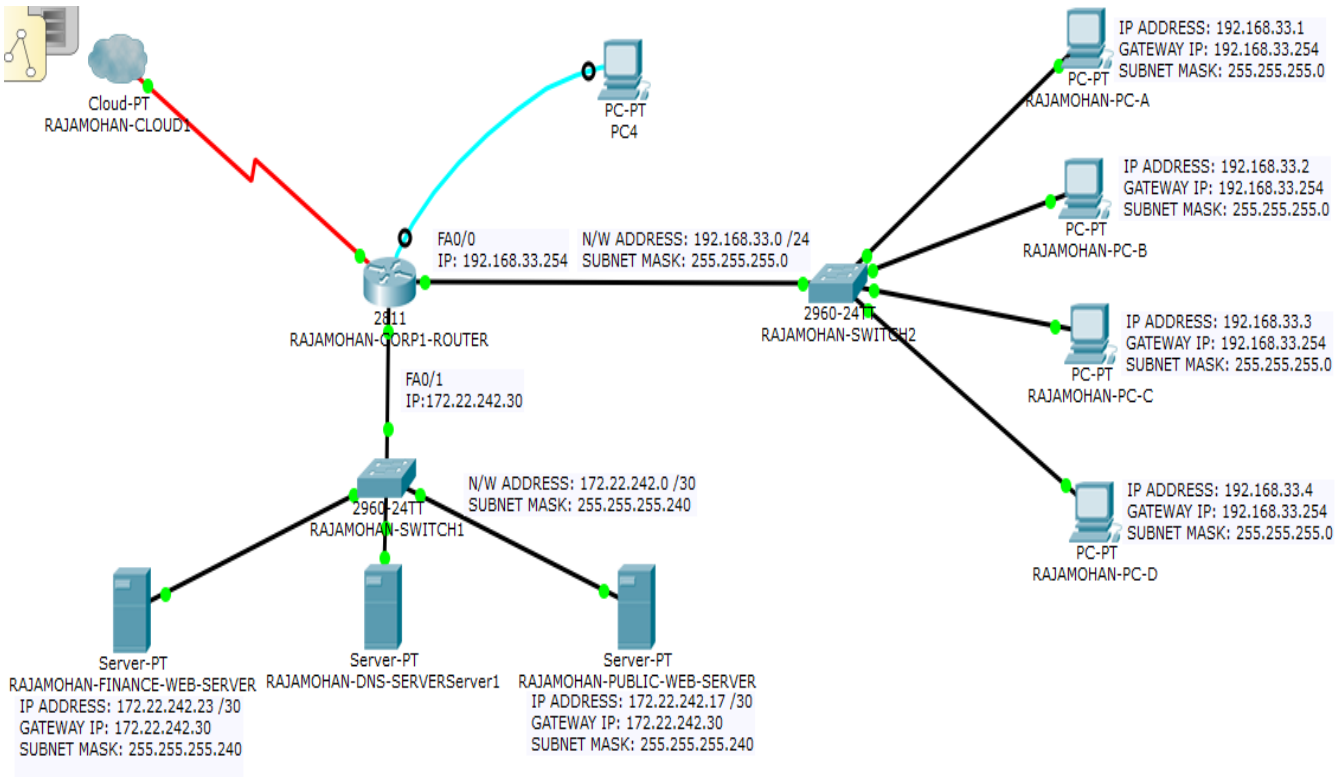
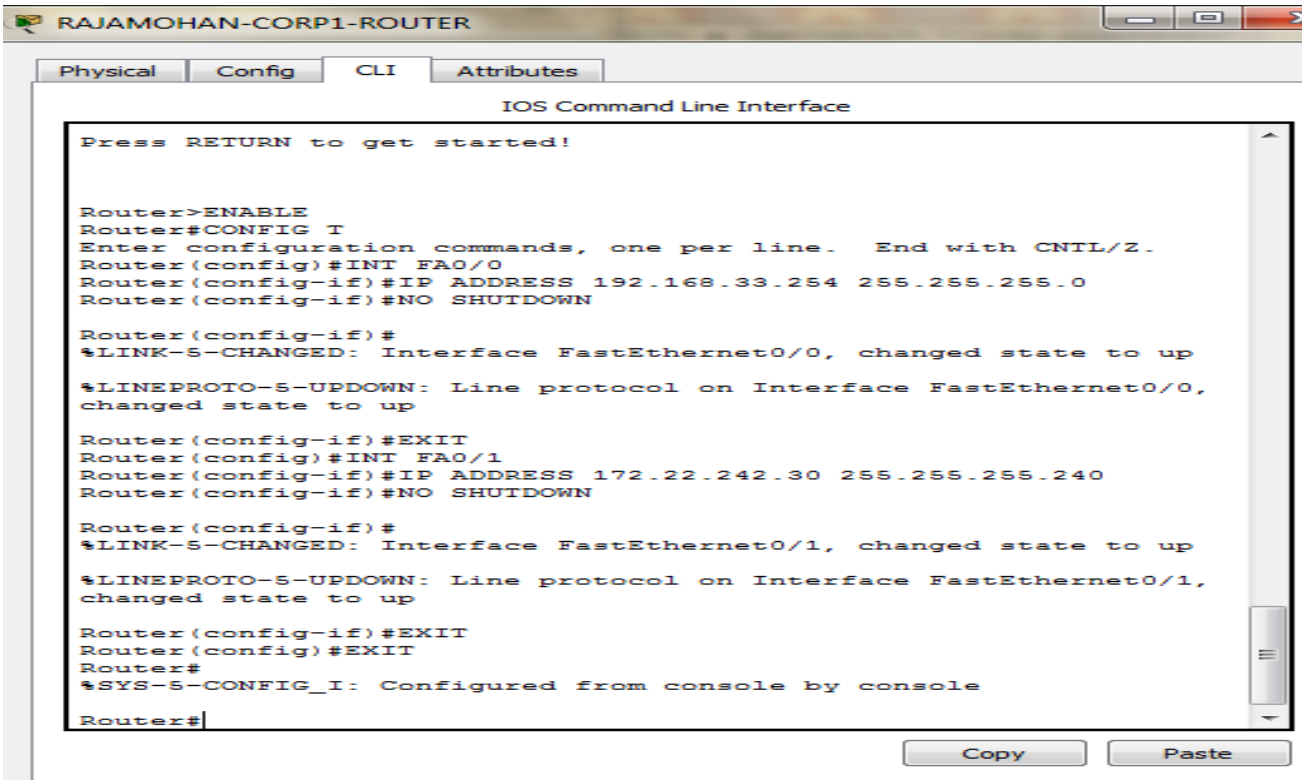
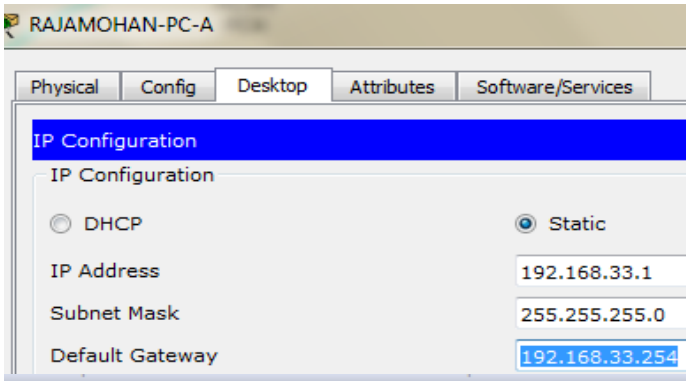


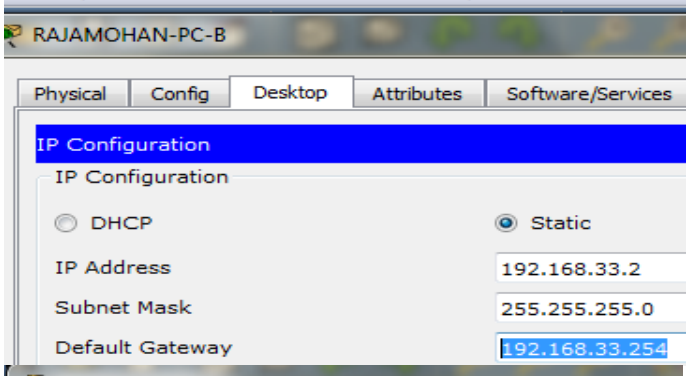
Fig. 1. ACL Part of Full Topology

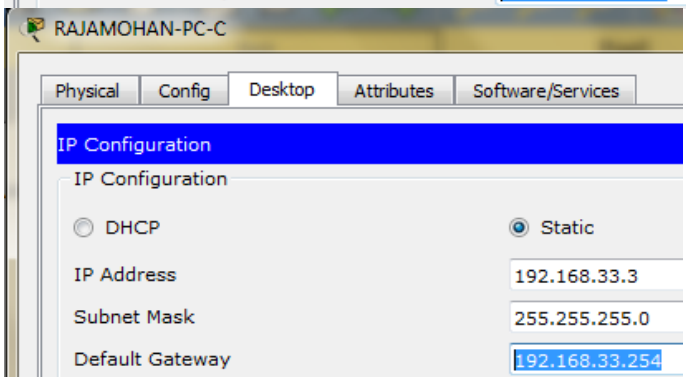
3.2 Router Basic Configurations

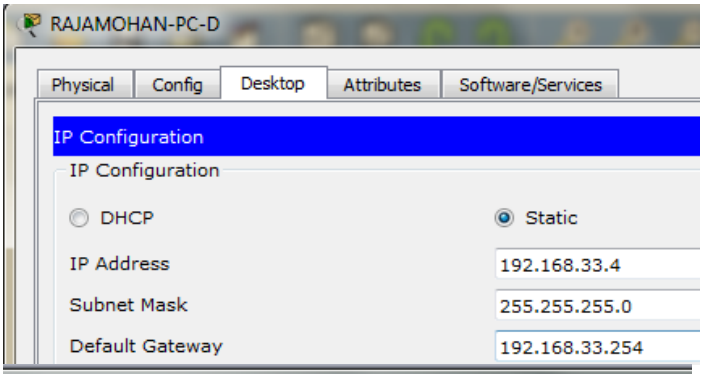


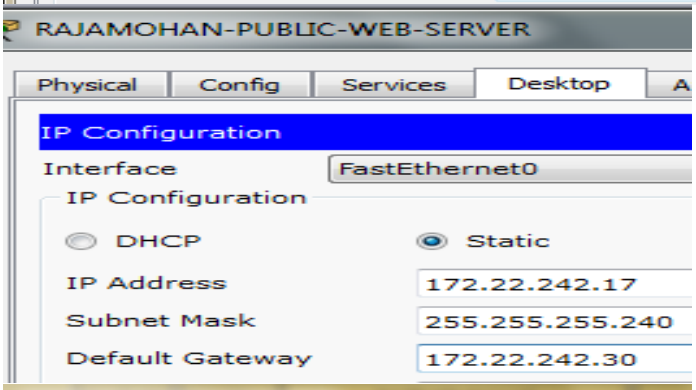
3.3 IP Configurations of PC A, PC B, PC C, PC D, Financial Web Server and Public Web Server

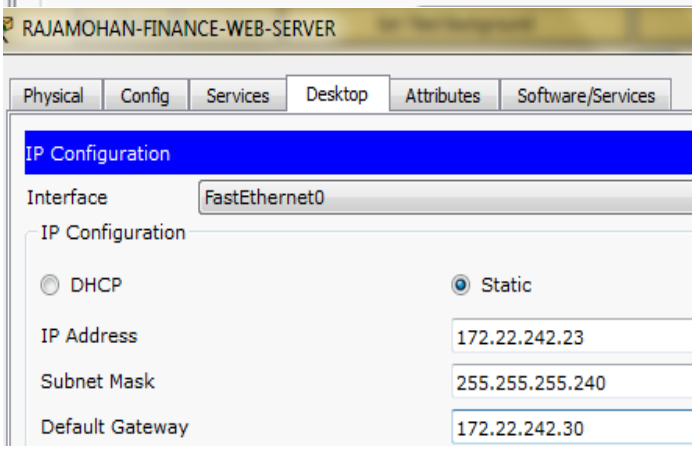








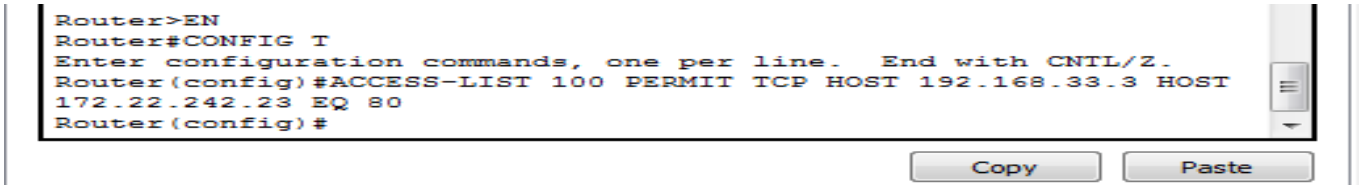




3.4 ACL allow host C to Finance Web Server via Web

Required Command RAJAMOHAN-CORP1-ROUTER:

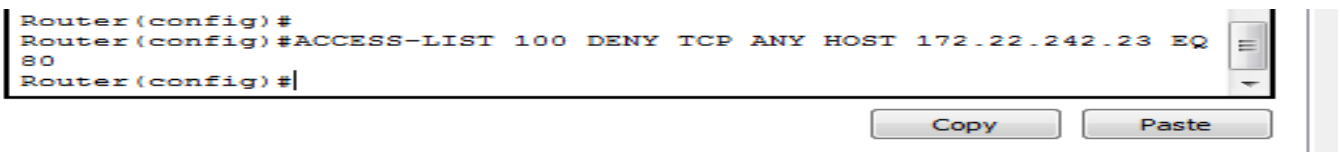
"ACCESS-LIST 100 PERMIT TCP HOST 192.168.33.3 HOST 172.22.242.23 EQ 80"



3.5 Deny other hosts access to Finance Web Server via Web (i.e) other PCs not able to access Finance Web Server

Required Command in RAJAMOHAN-CORP1-ROUTER:

"ACCESS-LIST 100 DENY TCP ANY HOST 172.22.242.23 EQ 80"



3.6 Allow all other traffic is permitted

Required Command RAJAMOHAN-CORP1-ROUTER:

"ACCESS-LIST 100 PERMIT IP ANY ANY"

```
Router(config)#
Router(config)#ACCESS-LIST 100 PERMIT IP ANY ANY
```

Copy Paste

3.7 Apply this ACL to Fa0/1 interface (outbound direction)

Required Command RAJAMOHAN-CORP1-ROUTER:

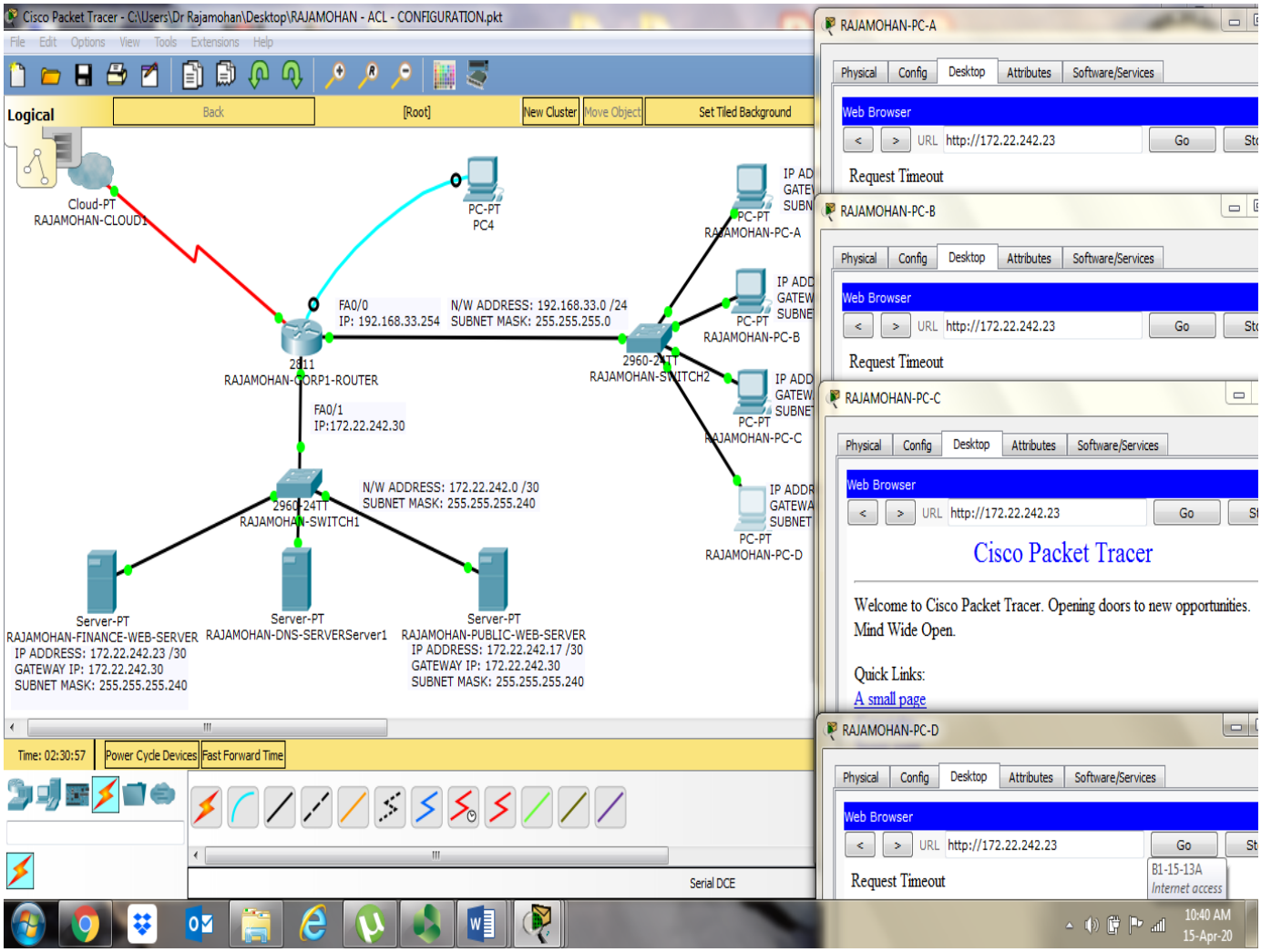
"Router(config)#INT FA0/1"
"Router(config-if)#IP ACCESS-GROUP 100 OUT"
"Router(config-if)#EXIT"

```
Router(config)#
Router(config)#INT FA0/1
Router(config-if)#IP ACCESS-GROUP 100 OUT
Router(config-if)#EXIT
Router(config)#EXIT
Router#
```

IV. RESULTS AND FINDING

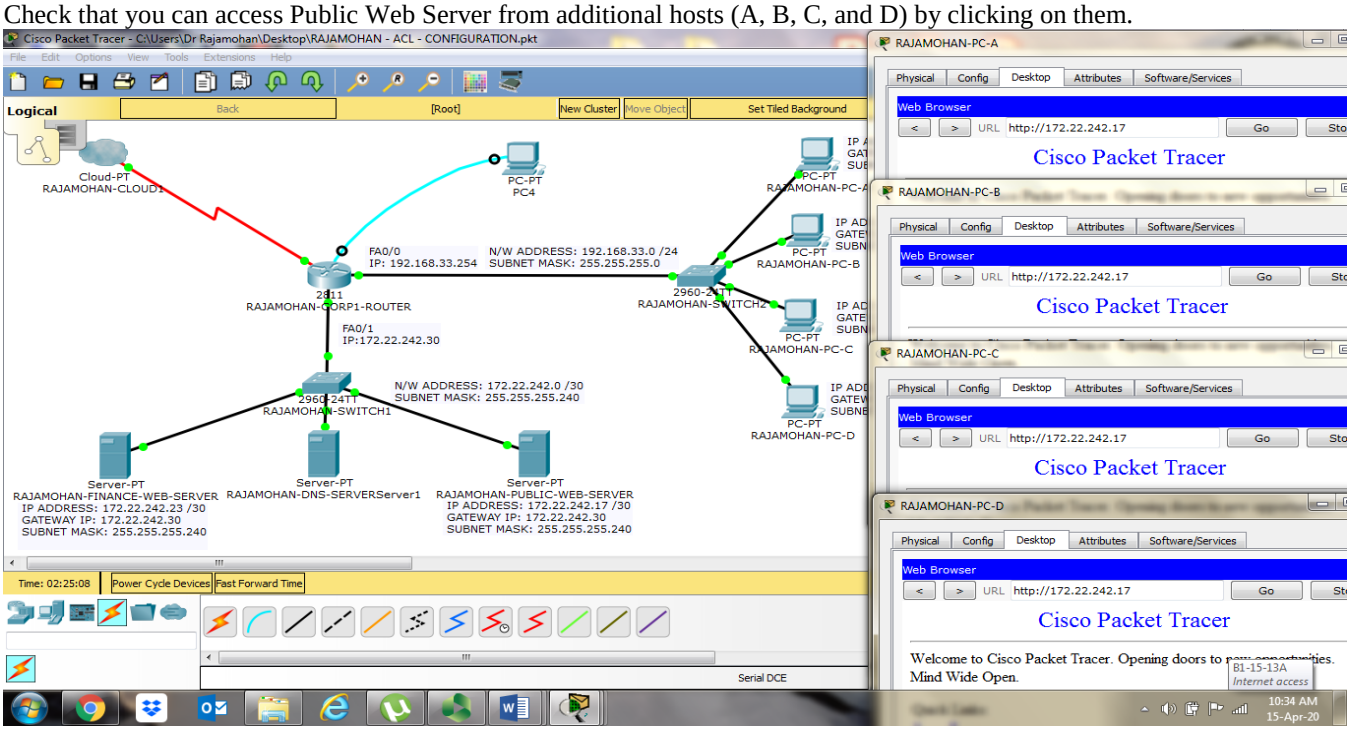
4.1 Verification on Finance Web Server IP: "http://172.22.242.23"

"Simply double-click on host C to launch its web browser. Type to see if you have permission to visit Finance Web Server. http://172.22.242.23 into the address box. You should be able to access it if your setup is right. Make sure you can't connect to Finance Web Server from any other servers. (A, B, and D) by clicking on them. To open the web browser on host C, Simply double-click on it. Type http://172.22.242.23 into the address box to see if you're able to access Finance Web Server".



4.2 Verification on Public Web Server IP: "http://172.22.242.17"

Check that you can access Public Web Server from additional hosts (A, B, C, and D) by clicking on them.



v. CONCLUSIONS

Access Control Lists, or simply Access-Lists, are a series of statements/commands that are configured on a router to route packets at layer 3 by choosing mainly on the routing protocol, the best-effort path between the source and destination routing. To improve network efficiency, ACLs restrict network traffic. ACLs on a network limit the distribution of routing updates, allowing traffic flow to be regulated. It also adds protection by refusing access to certain hosts or IP addresses, and it's very easy to set up.

REFERENCES

[1] Cisco Press, ACL Concepts, Enterprise Networking, Security, and Automation Companion Guide (CCNAv7) By Cisco Networking Academy, (2020).

[2] Bukhatwa, F.; Patel, A. Effects of Ordered Lists in Firewalls. In *Proceedings of International Conference (IADIS)*, Algarve, Portugal,. 5–8 (2003).

[3] El-Atawy, A.; Hamed, H.; Al-Shaer, E. Adaptive Statistical Optimization Techniques for Firewall Packet Filtering. In *Proceedings of IEEE INFOCOM*, Barcelona, Spain, 23–29(2006).

[4] Singh, S.; Baboescu, F.; Varghese, G.; Wang, J. Packet classification using multidimensional cutting. In *Proceedings of ACM SIGCOMM '03*, Karlsruhe, Germany, 25–27(2003).

[5] Varghese, G. *Network Algorithmics*; 1st ed.; Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 75(2005).

[6] Meiners, C.R.; Liu, A.X.; Torng, E. TCAM razor: A systematic approach towards minimizing packet classifiers in TCAMs. *IEEE/ACM Trans. Netw. 18*, 490–500(2010).

[7] Meiners, C.R.; Liu, A.X.; Torng, E. *Hardware-Based Classification for High-Speed Internet Routers*; 1st ed.; Springer: Berlin/Heidelberg, Germany, 2(2010).

[8] Liu, A.X.; Meiners, C.R.; Yun, Z. All-Match Based Complete Redundancy Removal for Packet Classifiers in TCAMs. In *Proceedings of IEEE INFOCOM 2008. The 27th Conference on Computer Communications*, Phoenix, AZ, USA,13–18(2008)..

[9] Alfaro, J.G.; Cuppens, F.; Cuppens-Boulahia, N. Complete analysis of configuration rules to guarantee reliable network security policies. *Int. J. Inf. Secur. 7*, 103–122*(2008).*

[10] Al-Shaer, E.; Hamed, H.; Boutaba, R.; Hasan, M. Conflict classification and analysis of distributed firewall policies. *IEEE J. Sel. Areas Commun. 23*, 2069–2084(2005).

[11] Kim, S.; Lee, H. Classifying rules by in-out traffic direction to avoid security policy anomaly. *Trans. Internet Inf. Syst. 4*, 671–690(2010),.

[12] Alfaro, J.G.; Cuppens, F.; Cuppens-Boulahia, N. Analysis of Policy Anomalies on Distributed Network Security Setups. *Lecture Notes Comput. Sci. 4189*, 496–511(2006).

[13] Alfaro, J.G.; Cuppens, F.; Cuppens-Boulahia, N. Aggregating and Deploying Network Access Control Policies. In *Proceedings of The Second International Conference on Availability, Reliability and Security (ARES 2007)*, Vienna, Austria, 10–13(2007).

[14] John N. Davies, Paul Comerford and Vic Grout, Principles of Eliminating Access Control Lists within a Domain, Future Internet. 4, 413-429 (2012)..

[15] Vishesh S, Chethan M Yadav, Nagaraj Manjunath Moger, Chiranjeevi S, Akshay Bhat, Gagan M, Route Redistribution-A Case Study, International Journal of Advanced Research in Computer and Communication Engineering, 6(6), 236-241(2017).