Simulation of Firewall and Standard Access-Control list Configuration over a TCP/IP Network

BY

OJUAWO O.O

DEPARTMENT OF COMPUTER SCIENCE,
THE FEDERAL POLYTECHNIC, ILARO,
OGUN STATE, NIGERIA.
teemana2000@yahoo.com

PRESENTED AT
THE 5TH NATIONAL CONFERENCE,
ACADEMIC STAFF UNION OF POLYTECHNICS (ASUP),
(ILARO CHAPTER)
THE FEDERAL POLYTECHNIC, ILARO, OGUN STATE
DATE: SUNDAY 16TH – WEDNESDAY 19TH, 2016

Abstract

An internet connection is an entry point for attackers who want to have access to a network. Attackers intercept traffic, send fake data and commands through spoofing of IP addresses. Sometimes, attackers disguise to get into a network have access to sensitive information that could harm the user. Networks are vulnerable because of inherent characteristics of facilitating remote access. Network security has been a preventative measure in protecting the network against unauthorized access. Files, data, and packets are kept safe and protected from authorized access with the help of network security. Network security is accomplished through hardware and software. Information on disk is vulnerable and in transit. Network Security is essential due to the increase in threat of attackers trying to attack Networks. In a network, data is broken down into units called Network Packets. TCP/IP protocol's implementation has serious security flaws despite its usage. Firewall and Access Control List (ACL) has helped in curbing open door policy of the computer systems to attackers over a network. This paper discusses the security aspect of a network and demonstrates the function of Firewall as well as Access Control list within a TCP/IP network using CISCO packet tracer, the configuration of firewall on a TCP/IP network to deny a terminal to have access to the server and other host devices, the function of Dynamic Host Configuration Protocol (DHCP) in automatic allocation of IP addresses to generic machines and configuration of Access Control List (ACL) within a network which consist of a server, a router, a switch and three personal computers.

Keywords: *Firewall, Access control list, packet tracer, TCP/IP.*

1.0 Introduction

Keeping out intruders with the building of walls has been in existence thousands of years back. The introduction of a firewall and access control list within a network has helped in structuring and limiting access to networks for an unauthorized user. Security in PCs is not just affected by network security at the end of the transmission sequence. Vulnerability in the attack should not occur in the communication channel at the point of transmitting data or information. An attacker may focus on the communication channel, get some data, decode and re-insert a false message (Daya, 2013). TCP/IP is the mode of the communication protocol used to connect hosts with a network.

Firewalls limit network access dynamically in which external connections are disallowed or dropped and internal connections are allowed. Access control list (ACL) filters some specific traffics from specific points in a network. ACL can be implemented anywhere on the internal network. This paper discusses the security of a TCP/IP network and the configuration of the firewall as well as ACL over a TCP/IP network using packet tracer.

2.0 Firewalls

A firewall is described as collection components arranged between two networks to filter the traffic between them by the method of some security strategies (Sahare, Joshi & Gehlot 2012). All incoming and outgoing packets go through a firewall which is installed at the private network's entry point and the outside internet (Gouda & Liu, 2007).

Firewalls are mainly categorized into two types. These are a Network-based firewall and Personal firewall. Network-based firewall is generally introduced at the edge of the network that

connects the LAN with broadband access while personal firewall is installed on personal devices or PCs (Hayajneh et al., 2013). A personal firewall can also be called software firewall or desktop firewall.

Most network systems requires firewall to implement trust limits imposed for auditing, operating system security problems, implementing strategies, Prevention of information access and Prevention of information leakage

2.1 Configuration of Firewall on TCP/IP Network

This paper explains the steps taken in the configuration of firewall over a TCP/IP network using packet tracer for the simulation. The aim is to design a TCP/IP network that will deny PC3 access to the server and other host devices.

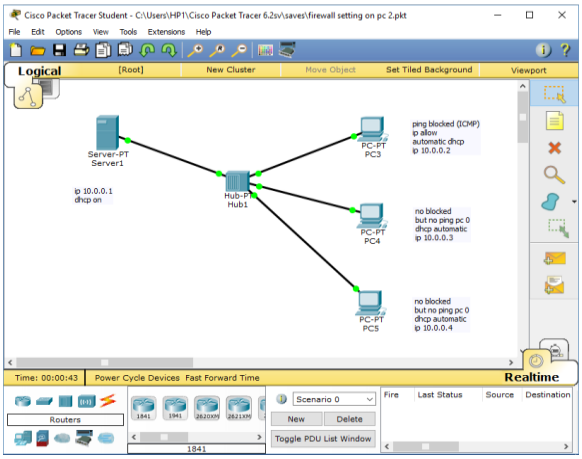

Fig. 1. TCP/IP Network Diagram using Packet Tracer

In Fig. 1 above, the network diagram is created with a server connected to three generic machines (PCs) through the hub with a copper straight through.

The initial step is the configuration of the server by assigning IP address of 10.0.0.1 and subnet mask 255.0.0.0 (a class C IP address) as shown in fig. 2 below.

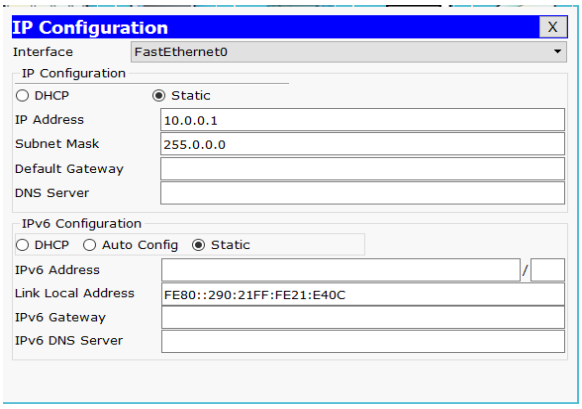

Fig. 2. Server IP address and subnet mask

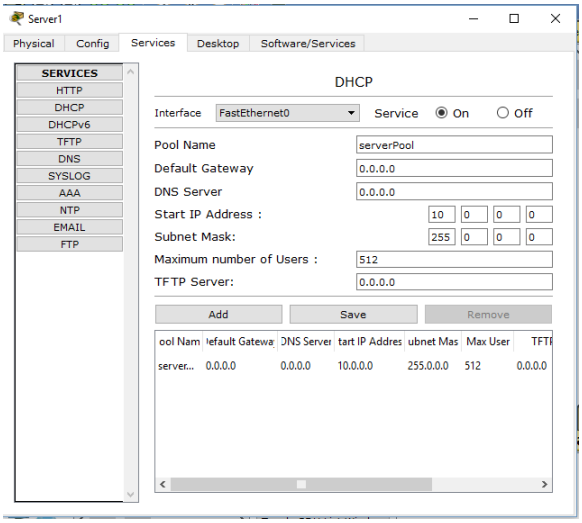

Fig. 3. DHCP Server settings

In fig. 3 above, The Dynamic Host Configuration Protocol (DHCP) is turned on and saved. The DHCP in the server assigns IP address automatically to generic machines from a characterized scope of numbers configured for the network. DHCP issues IP address, subnet mask, default gateway DNS server automatically to a host and stores the information so as not to issue the IP address to another host. After the DHCP issues the IP address to the host (temporarily), the host ask for a renewal of issuance of a new IP address at half time of the duration agreed (least time) by the DHCP. If the DHCP is offline, the host keeps on requesting at a half time until the DHCP responds. IP addresses 10.0.0.2, 10.0.0.3, and 10.0.0.4 are automatically assigned to PC3, PC4,

and PC5 respectively with the DHCP of each PCs turned on in the IP configuration. These are shown in Fig. 4, Fig. 5, and Fig. 6 below.

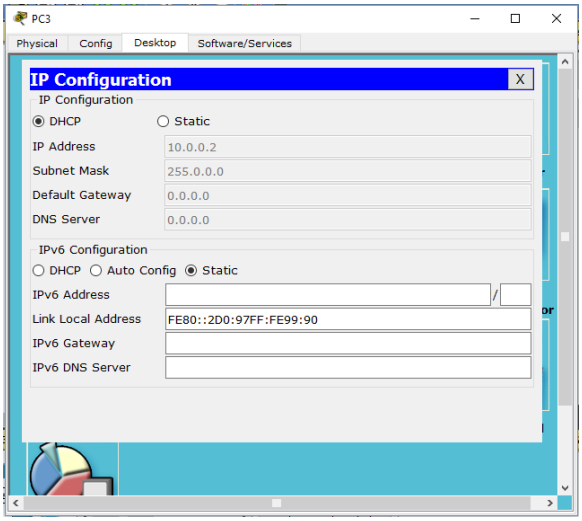

Fig. 4. DHCP assign automatic IP address to PC3

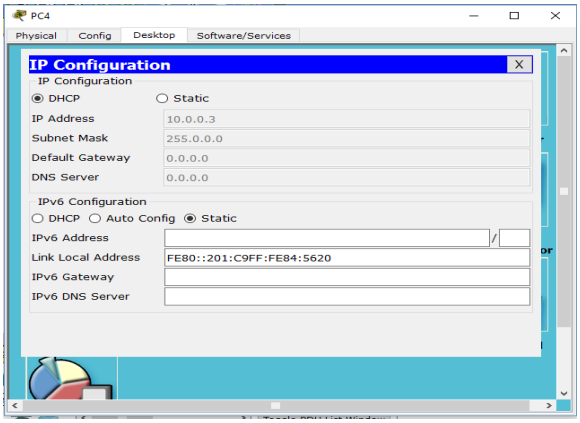

Fig. 5. DHCP assign automatic IP address to PC4

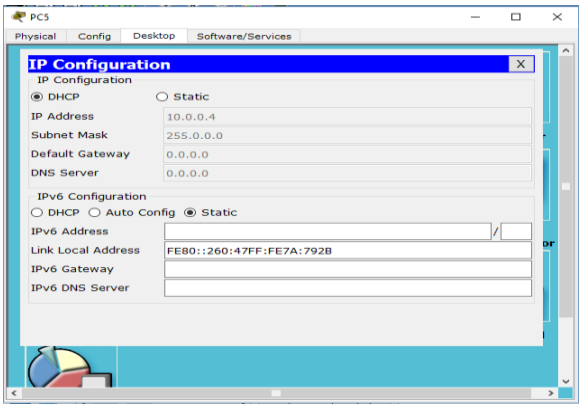

Fig. 6. DHCP assign automatic IP address to PC5

In setting up a firewall, two rules must be observed. The first rule is to deny ICMP and the second rule is to allow IP. In PC3, Firewall is turned on, the action on ICMP is denied and save while the action on IP is allowed and also saved.

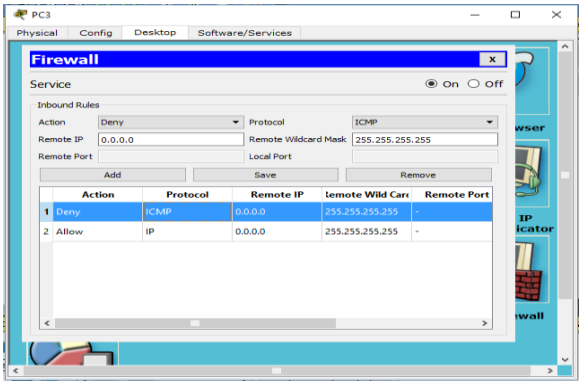

Fig. 7. Firewall configuration on PC3

The remote IP is assigned 0.0.0.0 while the remote wildcard mask is assigned 255.255.255.255. This is shown in fig. 7 above.

Internet Control Message Protocol (ICMP) is used by devices in the network to provide error messages, controls, troubleshooting and debugging. By allowing the IP, it depicts that the hosts can have access to the server through the web server. Denying the ICMP on PC3 means pings sent from or to PC3 through the command prompts of other devices will not be delivered. This shows the configuration of firewall to deny PC3 from communicating with the server and other PCs.

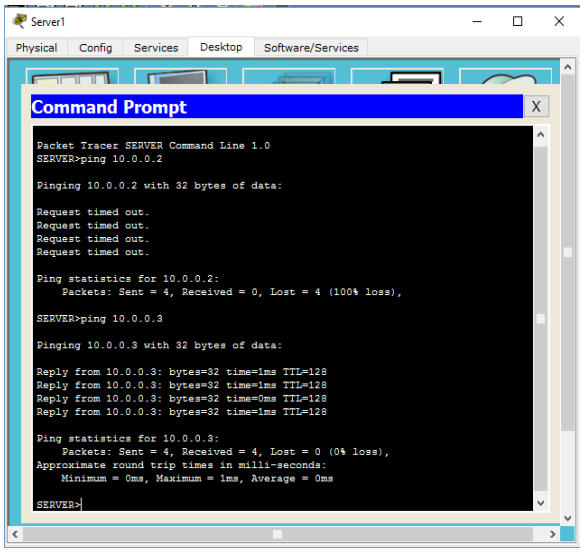

Fig. 8. Pings sent from server to generic devices

Fig. 8 shows the pings sent from the server to PC3 and PC4, four packets was sent to PC3 and all packets were lost. All four packets sent to PC4 are all successful. This shows that access was denied due to the blocked ICMP in PC3.

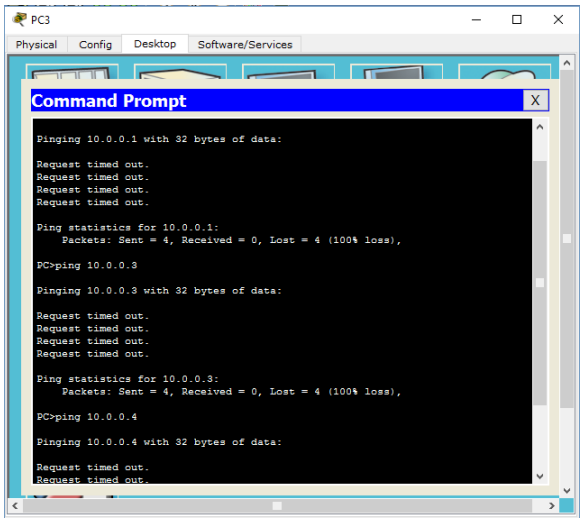

Fig. 9. Pings sent from PC3 to other generic devices

Fig. 9 above shows the pings sent from PC3 to the server and other hosts. All packets sent to other devices were unsuccessful due to the firewall configuration.

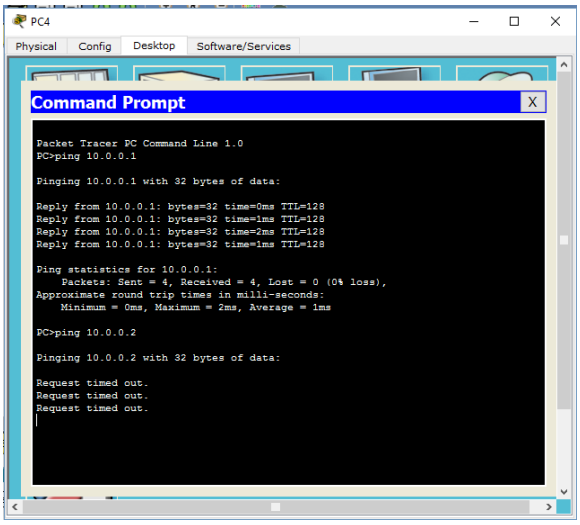

Fig. 10. Pings sent from PC4 to other generic devices

Packets sent from PC4 to the server was successful, which depicts there is communication between both devices while packets sent to PC3 was not successful. This shows that the firewall blocked the packets from getting to its destination.

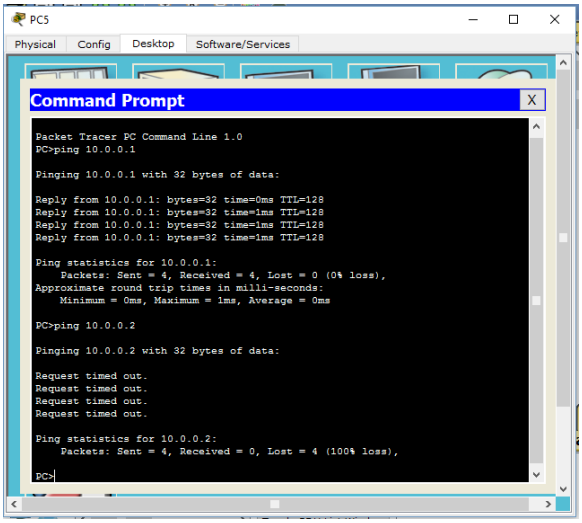

Fig. 11. Pings sent from PC5 to other generic devices

Fig. 11 above shows the packets sent from PC5 to the server and PC3 through the command prompt. The pings sent to the server was successful while pings sent to PC3 was not successful. This depicts that the firewall denies PC5 access to PC3.

3.0 Access-Control List

Access control list (ACL) is a network filter used by the router on some switches to permit and deny flow of data into and from the network interface. The main use of ACL is to provide security to the network. Most networks contain one or more connections to external networks which are a high-security risk (Davies, Comerford & Grout 2012). ACL is arranged at every entry points connecting to a concealed network and the external internet to manage all the inbound and outbound packets (Chate & Chirchi, 2015).

The two main types of ACL configuration are (Kaushik, Tomar & Poonam, 2014):

- Standard ACL: this permits or denies packets in view of the IP address and it has a range of 1 – 99 standard ACL IDs, which can also be in strings.
- Extended ACL: it permits or denies packets in view of protocol information and IP address of the source and destination. Extended ACL performs this process based on the IP protocol, source IP address, destination IP address, source UDP or TCP port, and destination UDP or TCP source.

3.1 **Configuration of ACL on TCP/IP Network.**

The aim of this configuration is to set up an ACL on the router to block PC1 from communication with other generic devices. The network consists of a server, a router, a switch and three PCs. The server is connected to the router with copper cross-over wire. The router is connected to the switch via a copper straight-through wire and also the switch is connected to the three PCs via the copper straight-through wire. The simulation diagram is shown in Fig. 12 below.

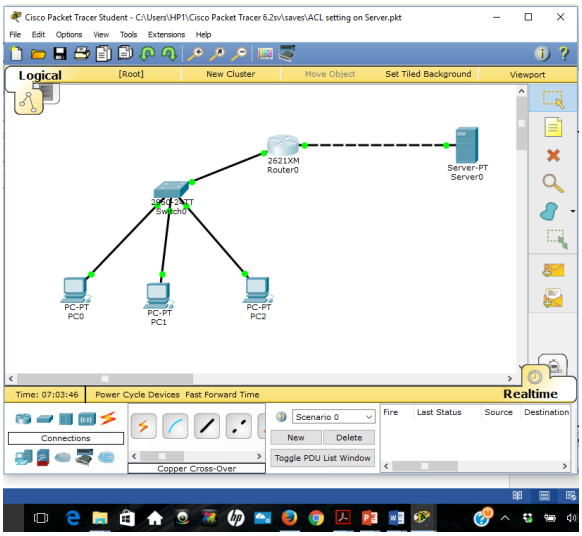

Fig. 12. TCP/IP Network Diagram using Packet Tracer

IP addresses of 1192.168.10.1 with a subnet mask of 255.255.255.0 were assigned to PC0. PC1 has an IP address of 192.168.10.2 with a subnet mask of 255.255.255.0 while IP address of 198.168.10.3 with a subnet mask of 255.255.255.0 was assigned to PC2. The IP configuration of each PCs is shown in Fig. 13, Fig. 14 and Fig. 15 below

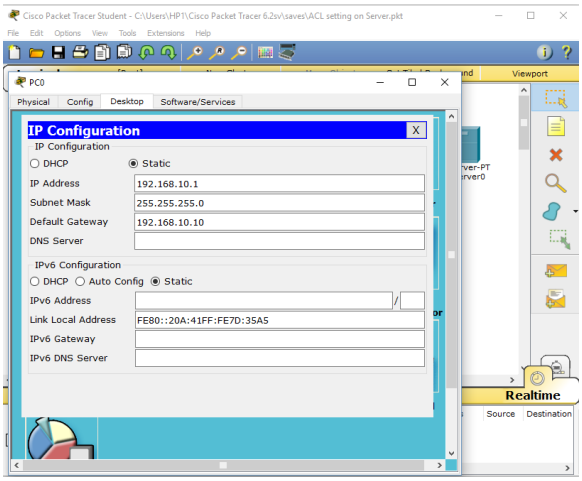

Fig. 13. IP configuration of PC0

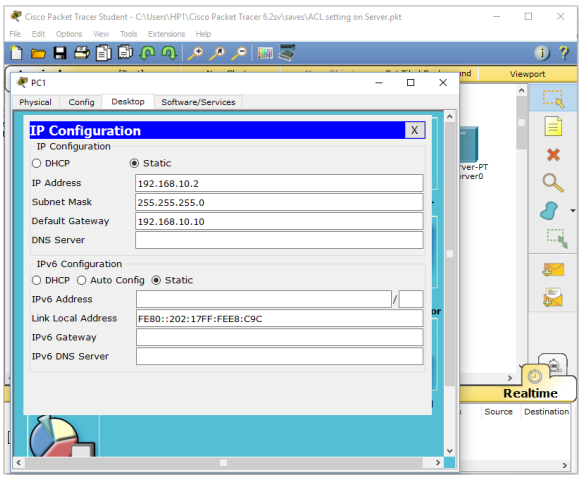

Fig. 14. IP configuration of PC1

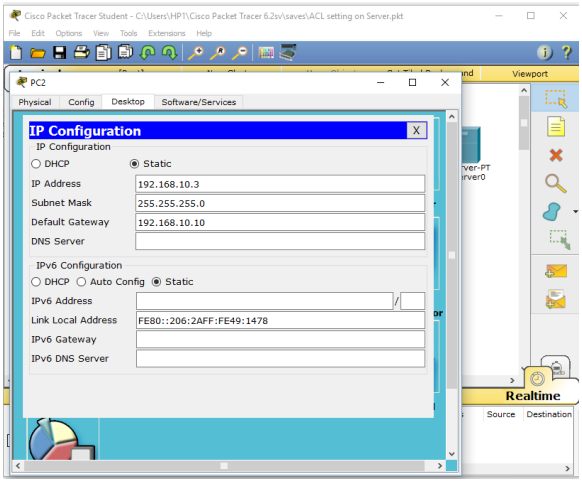

Fig. 15. IP address configuration of PC2

The following stage is to assign an IP address to the router which will serve as a default gateway to the three PCs and to configure the router to enable connection between the router and the switch by entering the commands in the command line interface (CLI) if the router. This is shown in Fig. 16 below.

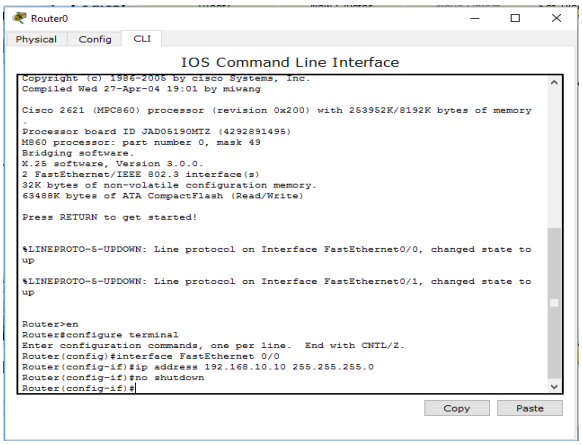

Fig. 16. Internal IP address configuration of Router

The router is assigned an internal IP address of 198.128.10.10 which serve as a default gateway to the three PCs.

The next step is to enable a connection between the router and the server by entering the commands through the router's CLI and assigning an external IP address of 10.10.10.10 to the router. This is shown in Fig. 17 below.

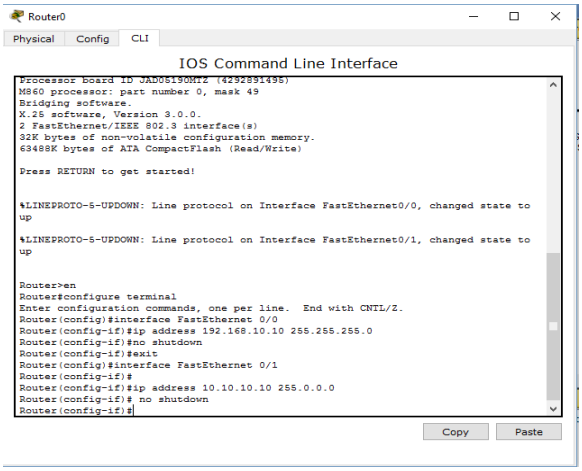

Fig. 17 External IP address Configuration of Router

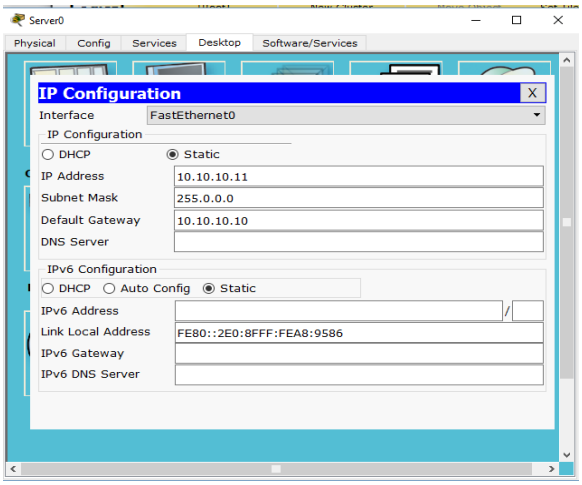

Fig 18. IP configuration of the server

The server is then assigned an IP address of 10.10.10.11 with a subnet mask of 255.0.0.0 and default gateway 10.10.10.10 as shown in Fig. 18 above. The job of the default gateway is to connect the subnet network to other computers.

In Fig. 19 below, the ACL is being set up in the router's CLI to deny PC1 to communicate with the server and permit any other host to communicate with the server. The first rule is to deny PC1 to communicate with the server with the command <deny> <host> <192.168.10.2>. The second rule is to allow any other host to communicate with the server. The command is <permit> <any>.

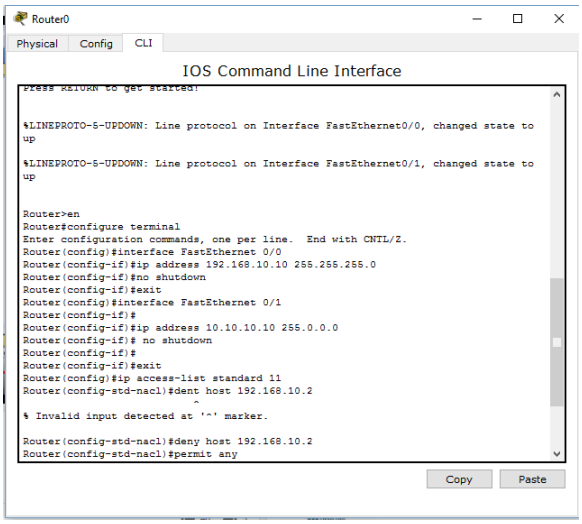

Fig. 19. ACL configuration in Router's CLI

The results of the pings sent from PC0, PC1, and PC2 are shown in Fig. 20, Fig. 21, and Fig. 22 respectively.

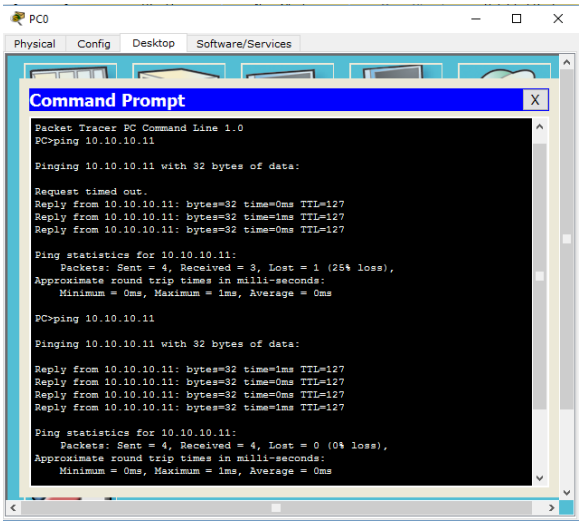

Fig. 20 Ping sent from PC0 to the server

From the above figure, all packets sent from PC0 to the server was received. This depicts that there is communication between the server and PC0.

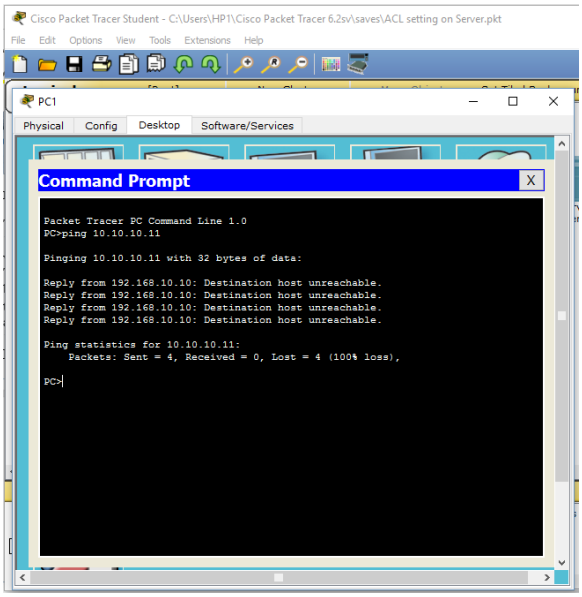

Fig. 21 Ping sent from PC1 to the server

From Fig. 21 above, all packets sent from PC1 to the server was not successful. This shows the effectiveness of the ACL configured in the router to deny access to PC1.

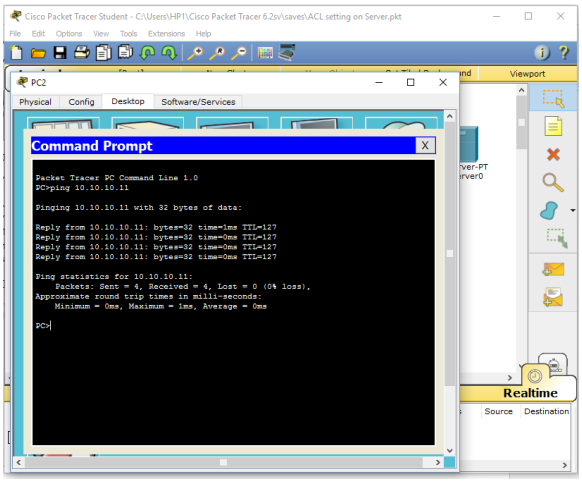

Fig. 22. Ping sent from PC2 to the server

From Fig. 22, all packets sent from PC2 was delivered successfully. This shows the effect of the <permit> <any> command to allow all other hosts to communicate with the server.

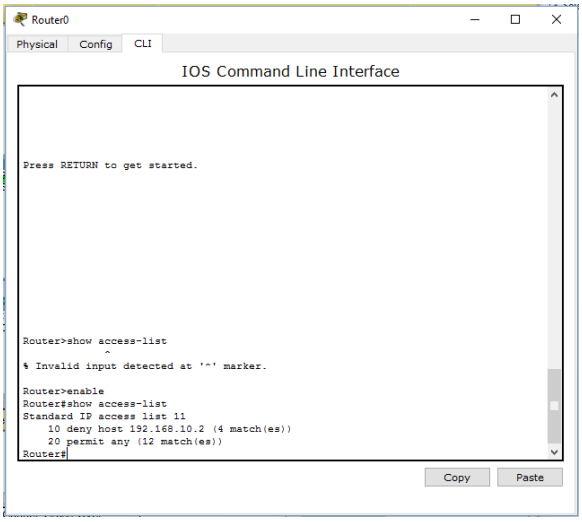

Fig. 23 show access-list command

The show access-list command shows the four packets denied from host 192.168.10.2 and twelve packets received by the server from other hosts.

4.0 Conclusion

This paper has been able to simulate the configuration of firewall and ACL to restrict access to a TCP/IP network. The firewall configuration was established in the server whereby PC3 was denied access to the server and other hosts. The automatic allocation of IP addresses through the DHCP was established. This paper also shows how ICMP was denied PC3 to send packets to other generic devices while IP was allowed for the hosts to access the server through the web browser.

Access Control Line (ACL) was also configured on a TCP network which consists of a server, a router, a switch and three PCs. The ACL was established on the router to show the process of blocking unauthorized access to the server. PC1 was denied access and the results were shown above. Sending TCP packets through the firewall without TCP 3-way handshake will fail on the firewall but the TCP packets will pass through the router with ACL set up. This gives firewall an edge over ACL. Firewall is more efficient that the ACL in terms of controlling traffic. Most firewalls perform inspection on network while ACL is just “deny” and “allow” process.

5.0 References

Chate, A.B. & Chirchi, V.R. 2015, “Access Control List Provides Security in Network”, *International Journal of Computer Applications*, vol. 121, no. 22

Davies, J.N., Comerford, P. & Grout, V. 2012, "Principles of Eliminating Access Control Lists within a Domain", *Future Internet,* vol. 4, no. 2, pp. 413-429.

Daya, B. 2013, "Network security: History, importance, and future", *University of Florida Department of Electrical and Computer Engineering.*

Gouda, M.G. & Liu, A.X. 2007, "Structured firewall design", *Computer Networks,* vol. 51, no. 4, pp. 1106-1120.

Hayajneh, T., Mohd, B.J., Itradat, A. & Quttoum, A.N. 2013, "Performance and information security evaluation with firewalls", *International Journal of Security and its Applications,* vol. 7, no. 6, pp. 355-372.

Kaushik, M., Tomar, A. & Poonam 2014, “Access Control List Implementation in Private Network”, *International Journal of Information & Communication Technology*, vol. 4, no. 14, pp. 1361-1366

Sahare, S., Joshi, M. & Gehlot, M. 2012, "A survey paper: Data security in local networks using distributed firewalls", *International Journal on Computer Science and Engineering,* vol. 4, no. 9, pp. 1617.