Implementation of ACL in Packet Tracer

PROJECT REPORT

18CSE383T – INFORMATION ASSURANCE AND SECURITY

(2018 Regulation)

III Year/ V Semester

Academic Year: 2022 -2023

By

MADAVARAM REDDI VINATHI(RA2011030010133)

P VINAY(RA2011030010138)

Under the guidance of

Dr. SAVARIDASSAN.P

Assistant Professor

Department of Networking and Communications

COLLEGE OF ENGINEERING AND TECHNOLOGY

SCHOOL OF COMPUTING

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Kancheepuram

NOVEMBER 2022

Implementation of ACL in Packet Tracer

BONAFIDE

This is to certify that **18CSE383T – INFORMATION ASSURANCE AND SECURITY mini project report** titled "**Implementation of ACL in Packet Tracer"** is the bonafide work of **Madavaram Reddi Vinathi (RA2011030010133) and P.Vinay (RA2011030010138)** who undertook the task of completing the project within the allotted time.

Signature of the Faculty

Dr. Savaridassan.P

Assistant Professor

Department of NWC

SRM Institute of Science and Technology

Signature of the II Year Academic Advisor

Dr. Annapurani Panaiyappan .K

Professor and Head

Department of NWC

SRM Institute of Science and Technology

TABLE OF CONTENTS

ABSTRACT

This paper relates the part of a cisco packet tracer for a case study to design and simulation virtual local area network. In this case study was carried out aimed at implement broadcast domains into segments, so as to improve network performance. It additionally makes educating simpler, understudies and instructor can make their own particular situation based labs also, gives representation environment cisco packet tracer has part of components to make different situation based labs. The discoveries of this study reason that there are different advantages and focal points of utilizing a cisco packet tracer part of learning fundamental and critical ideas of configuration and reproduction virtual local area network. It is a simple and easy to use device to comprehend different ideas of computer networks.

CHAPTER 1

INTRODUCTION

Access Control Lists (ACL) are used to filter network traffic on Cisco routers. In order to filter network traffic, ACLs control if routed packets have to be forwarded or blocked at the ingress or egress router interface. The router checks each packet to determine whether to forward or drop the packet based on the criteria specified in the ACL applied to the interface.

Two types of IP ACL can be configured in Cisco Packet Tracer 7.2 :

- **Standard ACLs** : This is the oldest ACL type which can be configured on Cisco routers. Traffic is filtered based on the source IP address of IP packets. The access-list number can be any number from 1 to 99. This kind of ACL has to be placed near the destination to avoid blocking legitimate trafic from the source.

```
access-list 1 permit 10.2.25.0 0.0.0.255
access-list 1 deny any.
```

- **Extended ACLs :** Introduced in IOS version 8.3, the extended ACLs are more complex and allow filtering of the IP traffic based on a combination of multiple criterias : source IP address, destination IP address, TCP or UDP port, protocol, ... In numbered ACLs, the access-list number can be any number from 100 to 199 or 2000 to 2699 (available in IOS versions >12.0.1). Such ACLs can also be named access lists in which the ACL number is replaced by a keyword. This kind of ACL has to be placed near the source as it allows fine grained control to ressources accessed. Placing the ACL near the destination will make the trafic travel through the network before beeing blocked, resulting in bandwidth waste.

```
access-list 1 permit ip 10.2.25.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 101 permit icmp any 10.1.0.0 0.0.255.255 echo
access-list 1 deny ip any any.
```

CHAPTER 2

LITERATURE SURVEY

Access control lists

Access control lists (ACLs) are used throughout many IT security policies, procedures, and technologies. An access control list is a list of objects; each entry describes the subjects that may access that object. Any access attempt by a subject to an object that does not have a matching entry on the ACL will be denied. Technologies like firewalls, routers, and any border technical access device are dependent upon access control lists in order to properly function. One thing to consider when implementing an access control list is to plan for and implement a routine update procedure for those access control lists.

Access control lists (ACLs) are one of the fundamental building blocks of a network configuration. If you fully understand how Access lists are constructed and used, you're well on your way to providing adequate security to your network. However, if you fail to grasp how wildcard masks are used or how order of operation affects Network Address Translation (NAT), then you could very well make your network the next successful target of a hacker. Understanding this topic is important, both for the test and for your career. Unlike many technologies you will learn as a Cisco Certified Network Associate (CCNA) candidate, ACLs are really old. Standard ACLs that match traffic based on source Internet Protocol (IP) address were part of IOS 8.3. Since IOS 9 was introduced in 1992, you know ACLs have been part of securing networks for a very long time. For comparison, the first graphical point-and-click Web browser Mosaic was introduced in 1993.

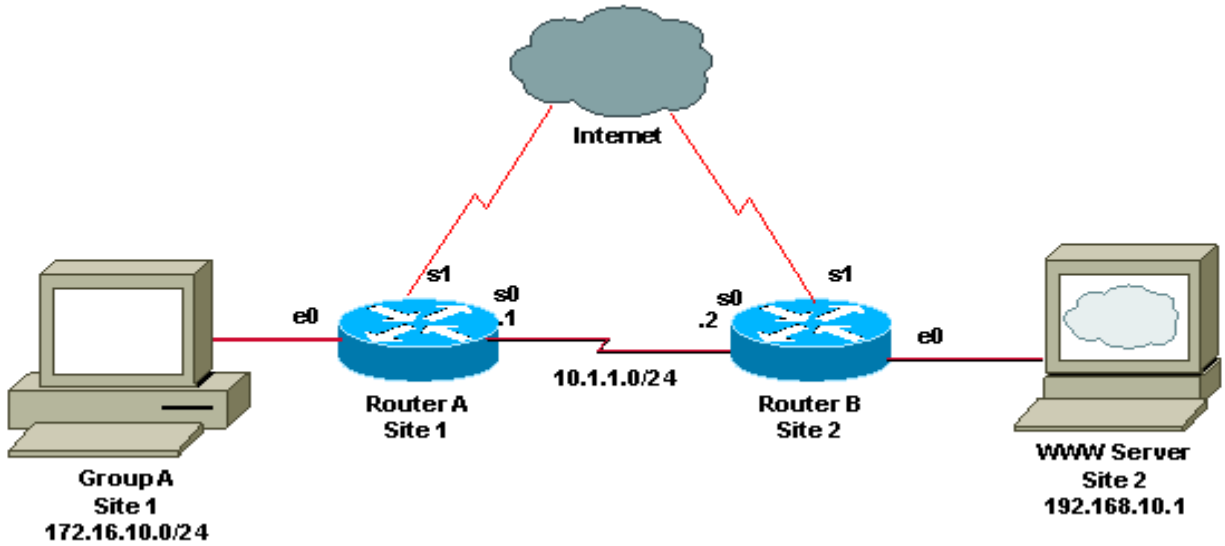
CHAPTER 3

PROPOSED MODEL

3.1 ARCHITECTURE

IMPLEMENTATION OF ACL IN PACKET TRACER

ACL (Access Control List) :-



Access Control Lists “ACLs” are network traffic filters that can control incoming or outgoing traffic.

ACLs work on a set of rules that define how to forward or block a packet at the router’s interface.

An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination.

When you define an ACL on a routing device for a specific interface, all the traffic flowing through will be compared with the ACL statement which will either block it or allow it.

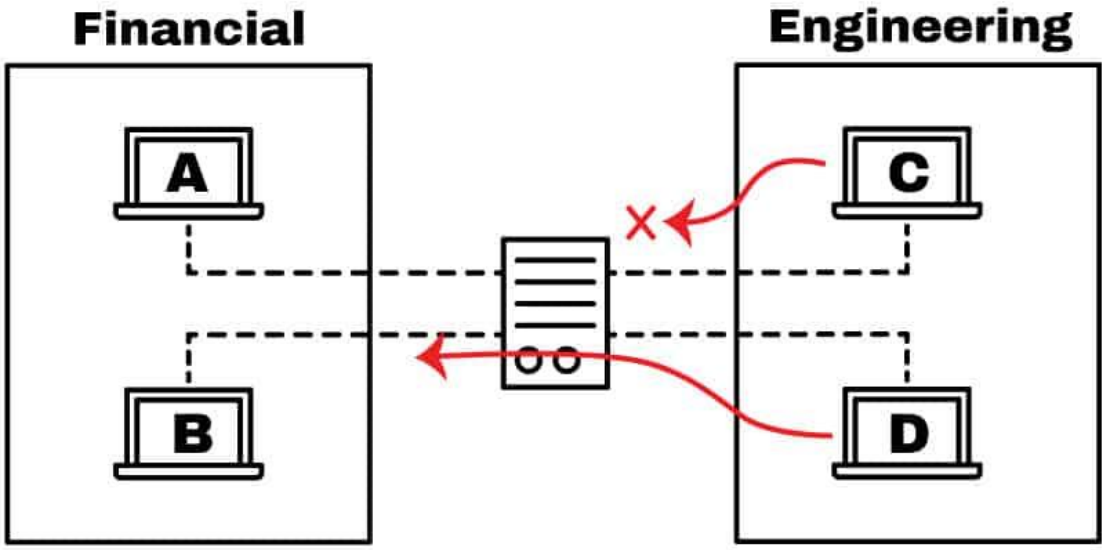
The criteria for defining the ACL rules could be the source, the destination, a specific protocol, or more information.

ACLs are common in routers or firewalls, but they can also configure them in any device that runs in the network, from hosts, network devices, servers, etc.

An access control list (ACL) contains rules that grant or deny access to certain digital environments. Every packet that attempts to enter or leave a router must be tested against each rule in the ACL until a match is found. If no match is found, then it will be denied.

when a packet is sent out, it must know where it's going (destination) and where it came from (source). So, it contains a source and destination IP address. The router looks at this information to determine if it matches any of the rules in its ACL.

If a router cannot find a match between the information in an ACL and the information in the packet that is attempting to enter it, the packet is denied .implicitly.



There are two types of ACLs:

- **Standard ACL**
- **Extended ACL**

(A) Standard ACL - Standard Access lists match only based on the source IP address of the packet.

(B) Extended ACL - Extended Access lists can match on source and destination address, in addition to port, protocol, and many other fields.

What Are The Components of An ACL?

The implementation for ACLs is pretty similar in most routing platforms, all of which have general guidelines for configuring them.

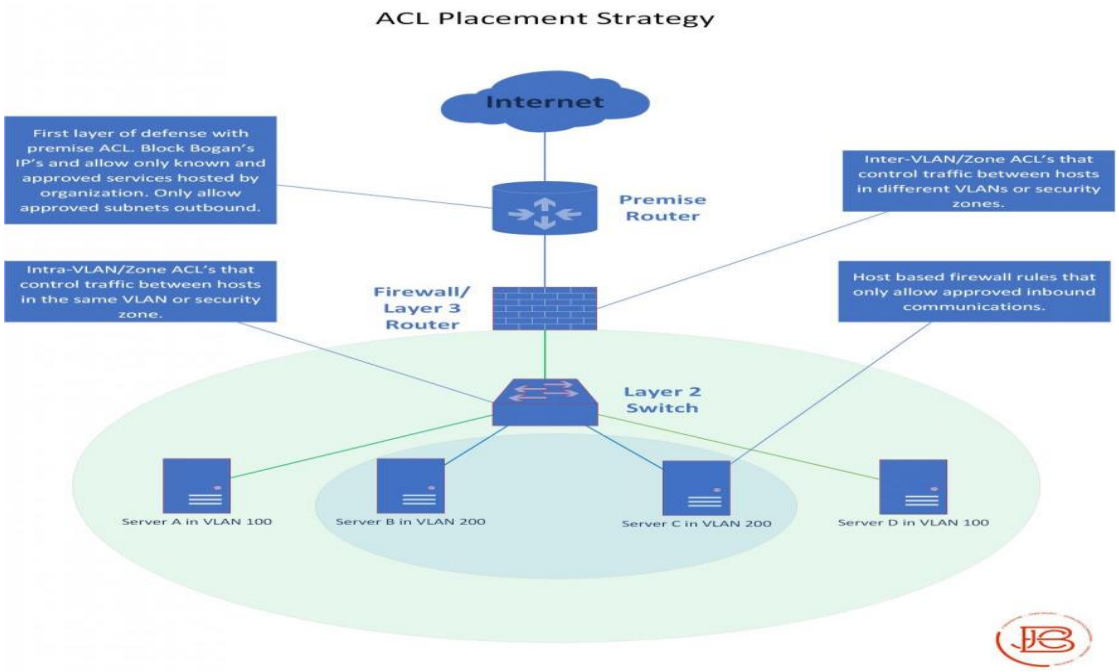
Remember that an ACL is a set of rules or entries. You can have an ACL with single or multiple entries, where each one is supposed to do something, it can be to permit everything or block nothing.

When you define an ACL entry, you'll need necessary information.

1. **Sequence Number:**
   Identify an ACL entry using a number.
2. **ACL Name:**
   Define an ACL entry using a name. Instead of using a sequence of numbers, some routers allow a combination of letters and numbers.
3. **Remark:**
   Some Routers allow you to add comments into an ACL, which can help you to add detailed descriptions.
4. **Statement:**
   Deny or permit a specific source based on address and wildcard mask. Some routing devices, such as Cisco, configure an implicit deny statement at the end of each ACL by default.
5. **Network Protocol:**
   Specify whether deny/permit IP, IPX, ICMP, TCP, UDP, NetBIOS, and more.
6. **Source or Destination:**
   Define the Source or Destination target as a Single IP, a Address Range (CIDR), or all Addresses.
7. **Log:**
   Some devices are capable of keeping logs when ACL matches are found.
8. **Other Criteria:**
   Advanced ACLs allow you to use control traffic through the Type of Service (ToS), IP precedence, and differentiated services codepoint (DSCP) priority.

Why do we use ACL's?

- They are used for controlling permissions to a computer system or computer network.
- They are used to filter traffic in and out of a specific device.
- Those devices can be network devices that act as network gateways or endpoint devices that users access directly.



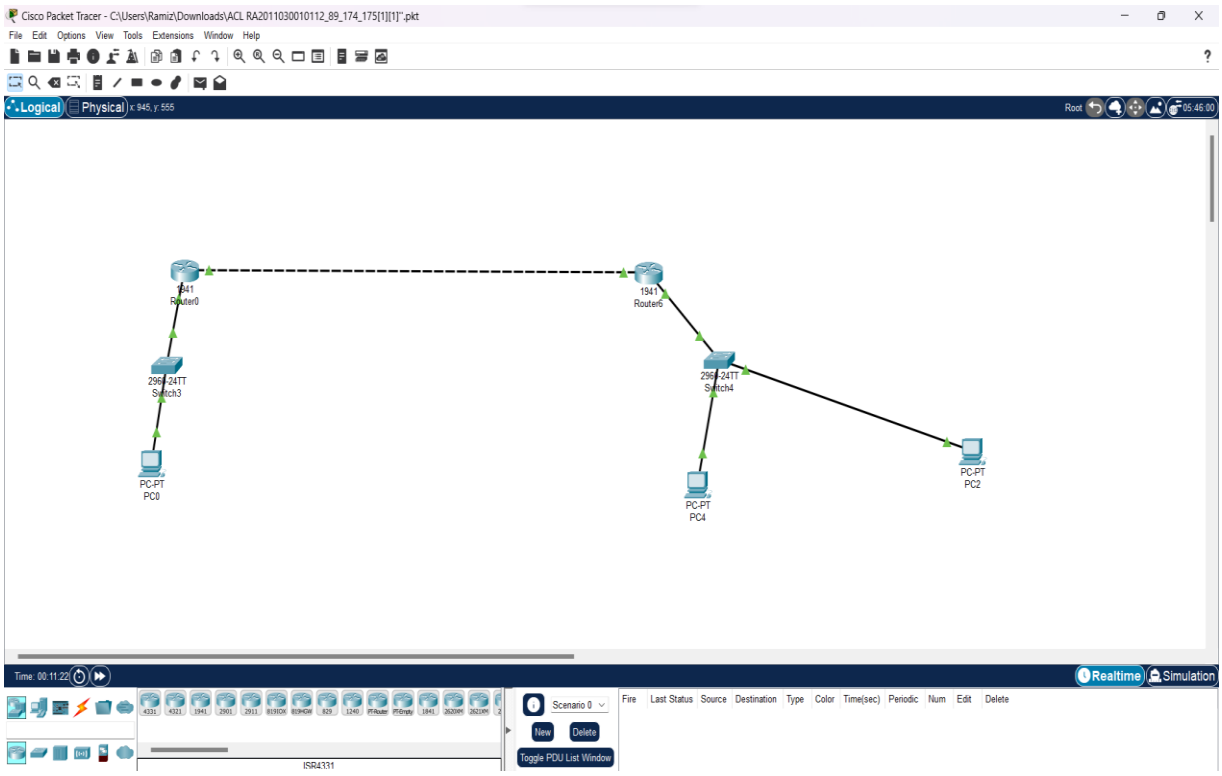
Routing Table:

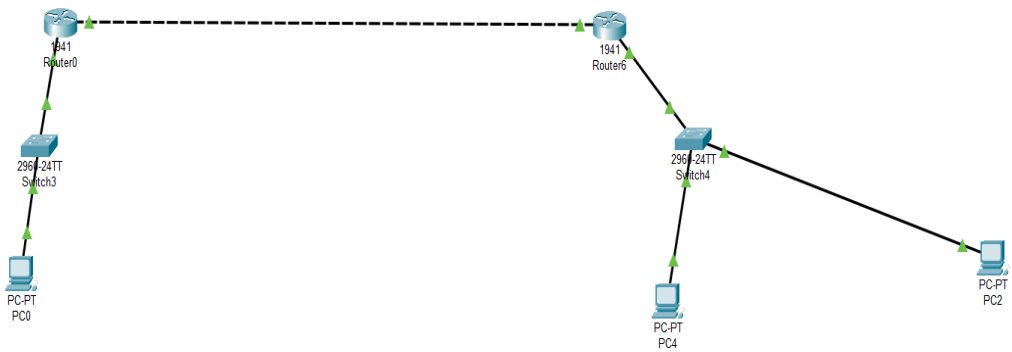
Device / Interface	IP Address	Connected with
Router0 (Fa0/0)	192.168.3.1	Switch0
Router0 (Fa0/1)	192.168.1.1	Switch0
PC0	192.168.1.10	Switch0
PC1	192.168.1.20	Switch0
Router1 (Fa0/0)	192.168.3.2	Switch1
Router1 (Fa0/1)	192.168.2.1	Switch1

PC2	192.168.2.42	Switch1

3.2 EXPLANATION OF THE PROPOSED MODEL

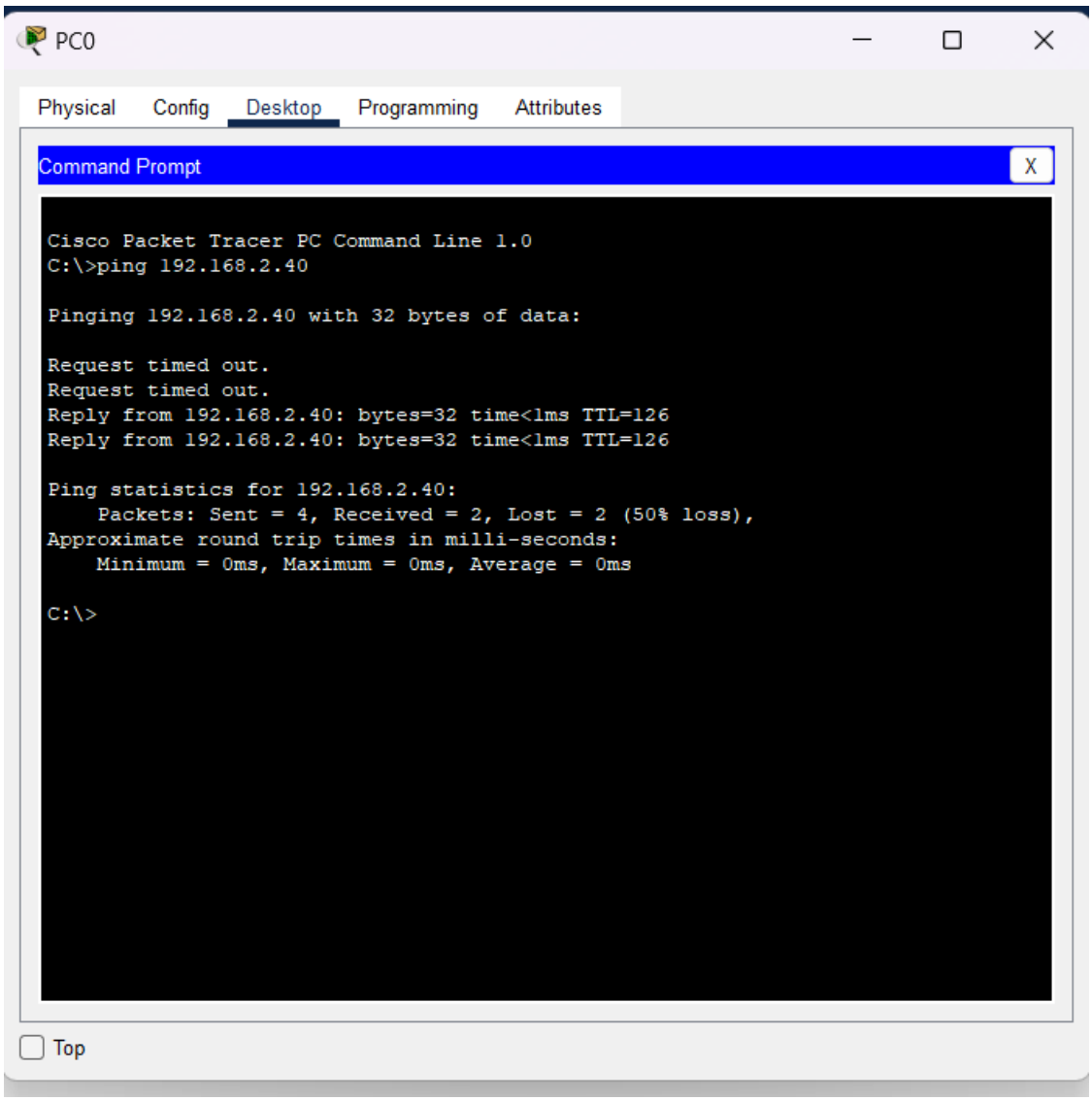
ACL Design:



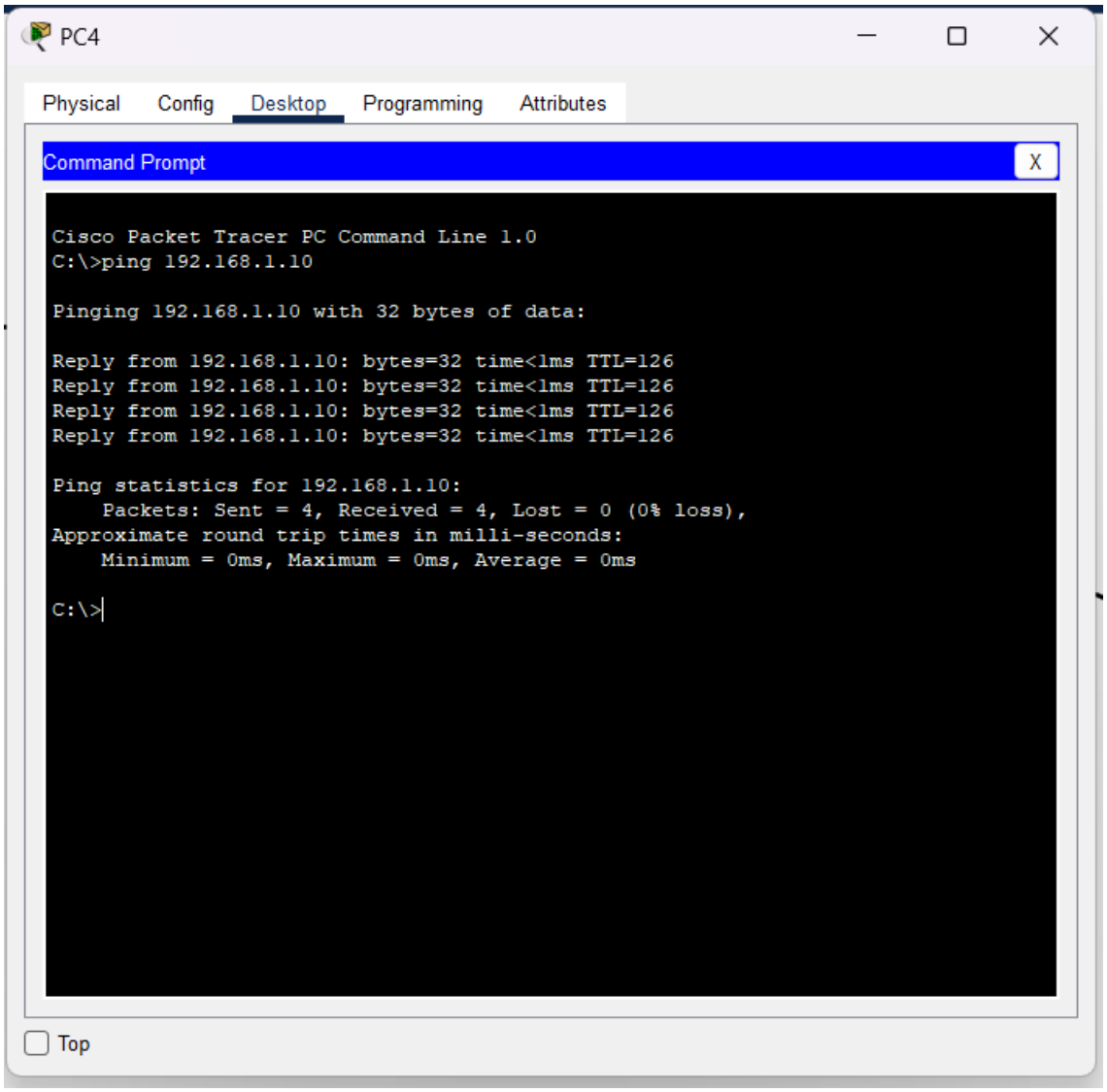


Before ACL:

1. **From PC0**



2. From PC1


PC4
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

ACL Implementation:

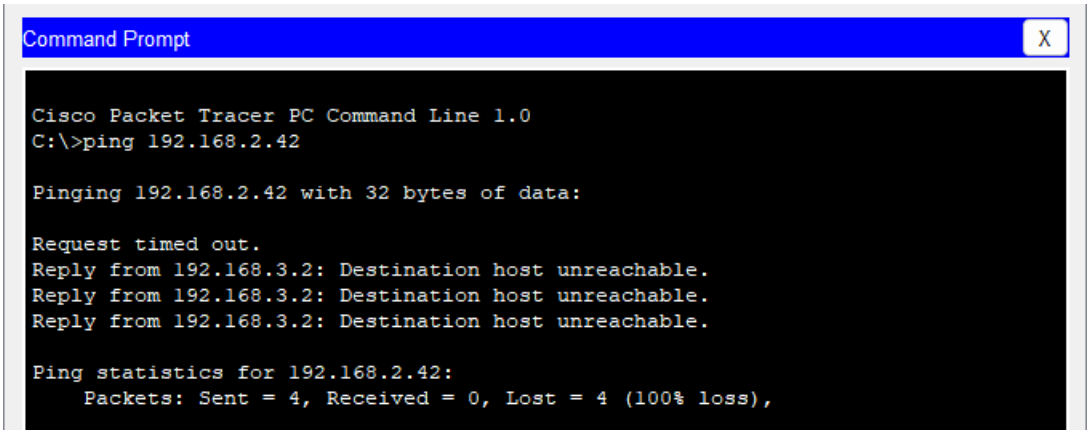
```
Router(config)#access-list 1 permit ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
Router(config)#access-list 1 permit any
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show run
Building configuration...

Current configuration : 736 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX15242LLW-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.3.1
!
ip flow-export version 9
!
!
access-list 1 deny host 192.168.1.20
access-list 1 permit any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end


Router#
Router#show access-lists
Standard IP access list 1
    10 deny host 192.168.1.20
    20 permit any

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/1
Router(config-if)#access-group ?
% Unrecognized command
Router(config-if)#access-group
                  ^
% Invalid input detected at '^' marker.

Router(config-if)#ip access-group ?
  <1-199>  IP access list (standard or extended)
  WORD     Access-list name
Router(config-if)#ip access-group
% Incomplete command.
Router(config-if)#ip access-group 1 ?
  in   inbound packets
  out  outbound packets
Router(config-if)#ip access-group 1 out
Router(config-if)#ex
Router(config)#
```

CHAPTER 4

RESULTS

1. Access Denied:



CHAPTER 5

CONCLUSION

Access Control Lists play a crucial role in traffic flow control and the network's security at large. This makes the network less vulnerable to unwanted and dangerous traffic.

REFERENCES

https://www.computernetworkingnotes.com/ccna-study-guide/configure-standard-access-control-list-step-by-step-guide.amp.html