

Implementation of Standard ACL in a Network thus securing the network from getting accessed by unwanted source IPs

A COURSE PROJECT REPORT

By

Aman Sharma (RA2011030010139)

Sanbeet (RA2011030010134)

Tushar Verma (RA2011030010135)

Kushagra Saxena (RA2011030010128)

Under the guidance of

Dr. Prasath N

Associate Professor, Networks and Communication

In partial fulfilment for the Course

of

18CSC302J - COMPUTER NETWORKS

in Networking And Communications



FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chengalpattu District

NOVEMBER 2022

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this mini project report "Implementation of Standard ACL in a Network thus securing the network by getting accessed from unwanted source IPs is the bonafide work of Aman Sharma(RA2011030010139) and Tushar Verma (RA2011030010135) and Sanbeet (RA2011030010134) and Kushagra Saxena (RA2011030010128) who carried out the project work under my supervision.

SIGNATURE

**Dr. Prasath N
Associate Professor
Department of Networking And Communications
SRM Institute of Science and Technology**

ABSTRACT

A network has to be designed for an organization in such a way that a web browser and local PCs are made. An application for web browsers is hosted by the company on a server that is available to other network hosts(engineers) as well as the permitted (Sales Manager) and not other hosts in the network (Salesman).

On the company's network, the department routers are interconnected so that users may access the server without being blocked. A network for the same was designed using Cisco Packet Tracer version 8.0.0. The requirements were emulated and tested for connectivity.

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor Dr. C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar Dr. S. Ponnusamy**, for his encouragement

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V. Gopal**, for bringing out novelty in all executions.

We would like to express our heartfelt thanks to the Chairperson, School of Computing **Dr. Revathi Venkataraman**, for imparting confidence to complete my course project

We wish to express our sincere thanks to **Course Audit Professor Dr. Annapurani Panaiyappan, Professor and Head, Department of Networking and Communications**, and **Course Coordinators** for their constant encouragement and support.

We are highly thankful to our Course project Faculty **Dr. Prasath N, Associate Professor, Networking And Communications**, for his/her assistance, timely suggestions, and guidance throughout the duration of this course project.

We extend my gratitude to our **Dr. Annapurani Panaiyappan, Professor and Head, Networking And Communications**, and my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

TABLE OF CONTENTS

CHAPTERS

CONTENTS

- | | |
|-----------|--|
| 1. | ABSTRACT |
| 2. | INTRODUCTION |
| 3. | LITERATURE SURVEY |
| 4. | REQUIREMENT ANALYSIS |
| 5. | ARCHITECTURE & DESIGN |
| 6. | IMPLEMENTATION |
| 7. | EXPERIMENT RESULTS & ANALYSIS |
| | 7.1. RESULTS |
| | 7.2. RESULT ANALYSIS |
| 8. | CONCLUSION & FUTURE ENHANCEMENT |
| 9. | REFERENCES |

..

2. INTRODUCTION

Scenario Description

A network has to be designed for a business organization that has some users.

The organization hosts an application on a server that is accessible by the engineers and managers of the organization but not by any other host of the organization. We have to set up a server that listens to all source IPs except the denied ones.

The engineers in the organization will be able to use the server without any restriction since they are directly routed to the same network via the company router. The sales manager in another network can also access it by using the ACL.

The salesman will only know the public address of the company router to connect to the local PCs (Engineers). They can communicate with each other since they are on a public network. But the salesman host cannot communicate with engineers.

3. LITERATURE SURVEY

IoT devices are collecting diverse data, such as electricity consumption, location information, and sensor data, from Internet, sensor networks, and online social networks. The development of IoT search realizes information sharing and improves the efficient use of devices. It can solve the problem of information island, improve the comprehensive utilization rate of social resources, and reduce the production and service costs. However, IoT search also collects, stores and analyses a large amount of private data, while providing convenience to users. Therefore, IoT search is a "double-edged sword". On the one hand, it will bring convenience to people's lives if it is used properly. On the other hand, it's also a serious threaten to personal privacy and national security. Whether IoT search can be widely accepted and popularized depends on its ability of prevent sensitive information leakage. Access control, as the backbone technology to ensure information security, can effectively monitor the access of resources and prevent the unauthorized flow of information. However, IoT search is a relatively new research field, traditional access control methods and techniques cannot fully solve the access control problems faced by IoT search because of node heterogeneity, open environment, multi-party sharing of resources.

In this [survey\[1\]](#), he present a thorough analysis of the current state-of-the-art technologies of access control for IoT search. We also provide an overview of the research challenges in access control. Such as, IoT search needs to integrate data from different data sources, so how to dynamic division of authorization for different data sources and integrate different access control policies are big challenges. The next section describes the background of access control for IoT search, which includes development history of access control and the Attribute-based access control (ABAC) model.

this [survey\[2\]](#) provides convenience to people, IoT search uses a large amount of authorized personal privacy data. However, the protection of these privacy data is not enough. Once the privacy data is leaked, it may bring huge losses to the organizations. Access control technology ensures that resources can only be accessed by authorized users according to the pre-defined access control policy, so it can prevent unauthorized access to privacy information.

In [Survey\[3\]](#) around 2000, with the development of Internet and increasing large-scale applications of information system in enterprises, the traditional models of access control (i.e. DAC, MAC and its extension models) are difficult to handle complex application layer access requirements. To solve this problem, Role-Based Access Control (RBAC) [5] is prosed to restricting system access to authorized users. The components of RBAC (i.e. role-permissions, user-role and role-role relationships) make it

simple to perform user assignments. Figure 1 shows the relationship between roles and users in RBAC model. RBAC can be used to facilitate administration of security in large organizations, and meeting the information integrity requirements of information systems. RBAC is different from MAC and DAC, however it can enforce these policies without any complication

Temporal-RBAC (TRBAC) [8] is an extension of RBAC model, which supports periodic role enabling, disabling, and temporal dependencies by using role triggers. Concept Usage Control (UCON) was developed in [9], which enables finer-grained control over usage of digital objects than that of traditional access control policies and models.

This **survey [4]** Fast development of new computing environments such as IOT search brings big challenges to the applications of access control technology. Traditional closed environment-oriented access control models (i.e. DAC, MAC, RBAC) are not adapt to the new computing environments. In this case, Attribute-Based Access Control (ABAC) [6] is proposed as an emerging form of access control, where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions [7]. The concept of role is very common in real life. Ferraiolo and Kuhn first introduced it into the Information System Access Control Research Institute in 1992 and named it RBAC [5]. Such Different from the traditional access control models which manual assignment of roles, ownership, or security labels by a system administrator, ABAC allows for the creation of access policies based on the existing attributes of the users and objects in the system. The advantages of ABAC can effectively solve the problem of fine-grained access control in dynamic large-scale environment. ABAC is an ideal access control model in new computing environment, and has broad application prospects.

4. REQUIREMENTS

4.1 Requirement Analysis

From the given scenario, we draw the following requirements:

1. Identifying the appropriate hardware which would be used (Cisco Packet Tracer)
2. The users in the organization should have full access to the server.
3. TCP/IP Network design with IP addressing

4.2 Hardware Requirement

From the given scenario, we draw the following requirements:

For Company XYZ):

For the developer Sector:

Hardware Required:

1x Switches

1x Router

3x PCs (Engineers)

1x Web server

For Sales Sector:

Hardware Required:

1x Router

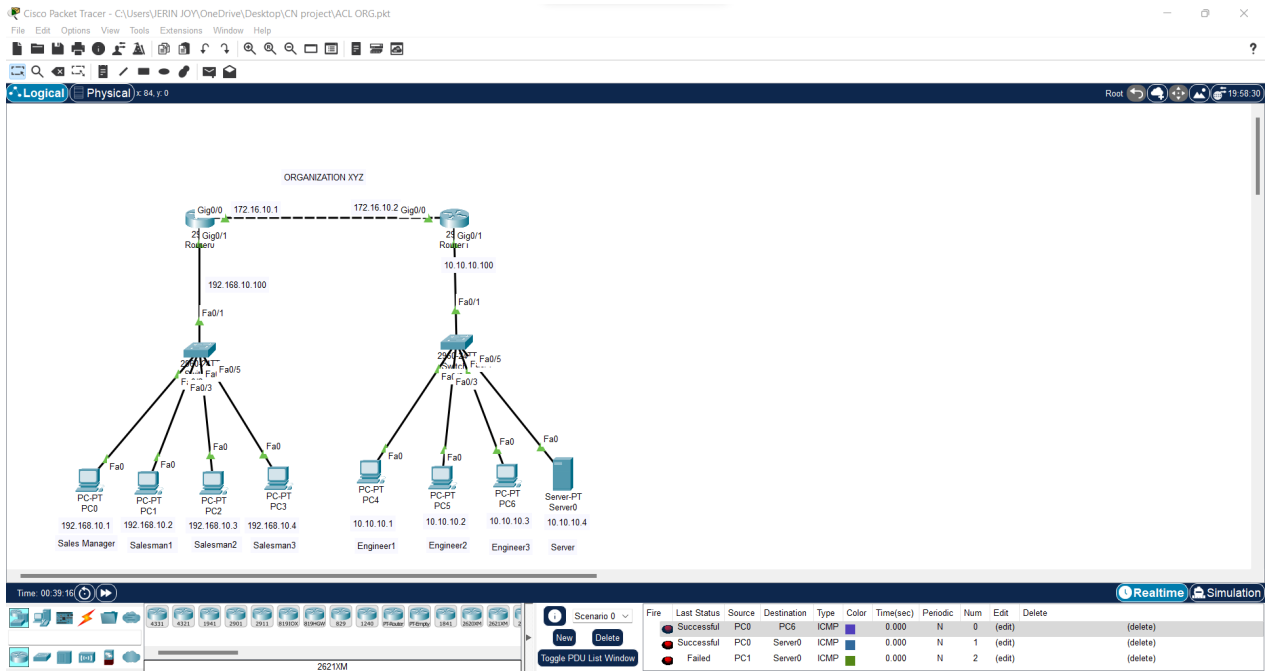
1x Switch (Broadband Switch)

4x End Devices (Public Network PCs)

5. ARCHITECTURE AND DESIGN

5.1 Network Architecture

The network architecture is as follows:



The architecture consists of three major networks:

- Company Network(s)
- Sales Sector
- Developer Sector

6. IMPLEMENTATION

6.1 Address Table

The address table is as follows:

Device	Interface	Address
Server	Fa0	10.10.10.4
Router 0	Gig 0/1 / switch	192.168.10.100
	Gig0/0	172.16.10.1
Router 1	Gig 0/1	10.10.10.100
	Gig0/0 / switch	172.16.10.2
Sales Manager	Fa0	192.168.10.1
Salesman1	Fa0	192.168.10.2
Salesman2	Fa0	192.168.10.3
Salesman3	Fa0	192.168.10.4
Engineer1	Fa0	10.10.10.1
Engineer2	Fa0	10.10.10.2
Engineer3	Fa0	10.10.10.3

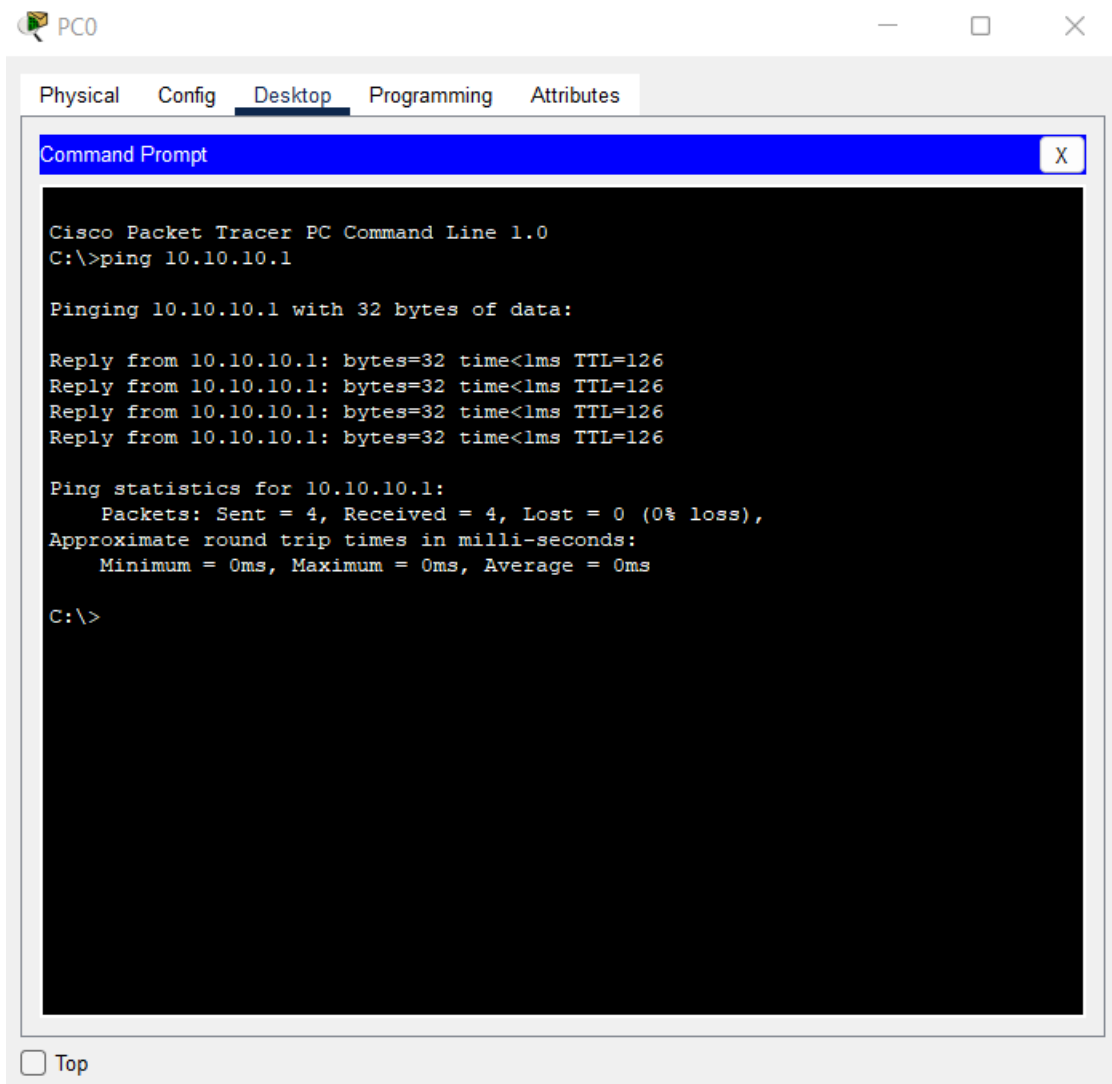
The Access Control List contains the entire broadband network. Any request from that network is translated to the private IP of the server.

Static Routing is used on all the routers to interconnect the networks.

7. RESULTS AND DISCUSSION

7.1 Result:

The network connections were checked by ping requests and sales manager can access server



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named PC0. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with Desktop selected. The Command Prompt window displays the output of a ping command to 10.10.10.1. The output shows four successful replies with 32 bytes of data, a time of less than 1ms, and a TTL of 126. The ping statistics show 4 packets sent, 4 received, and 0% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time<1ms TTL=126
Reply from 10.10.10.1: bytes=32 time<1ms TTL=126
Reply from 10.10.10.1: bytes=32 time<1ms TTL=126
Reply from 10.10.10.1: bytes=32 time<1ms TTL=126

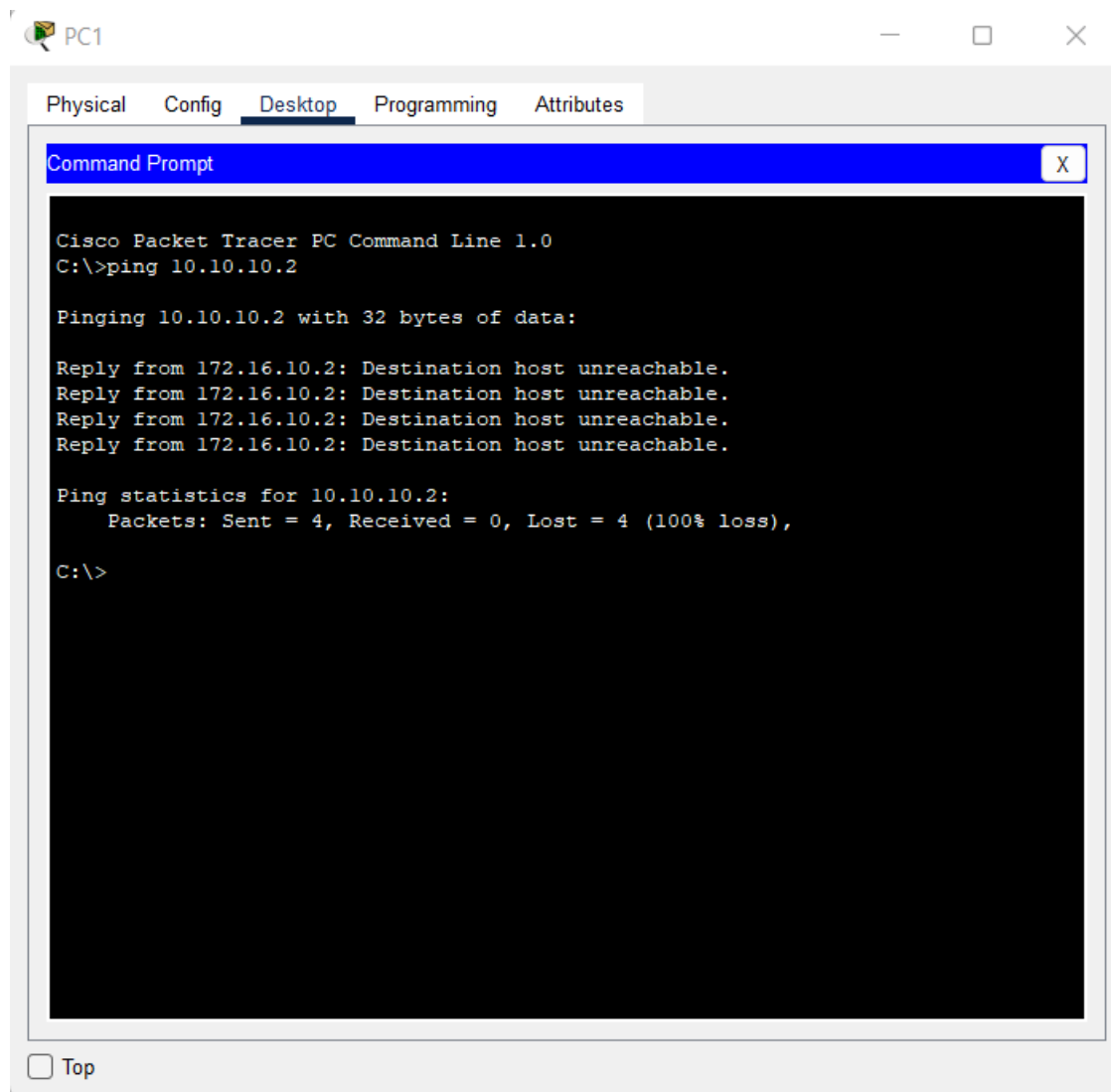
Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

☐ Top

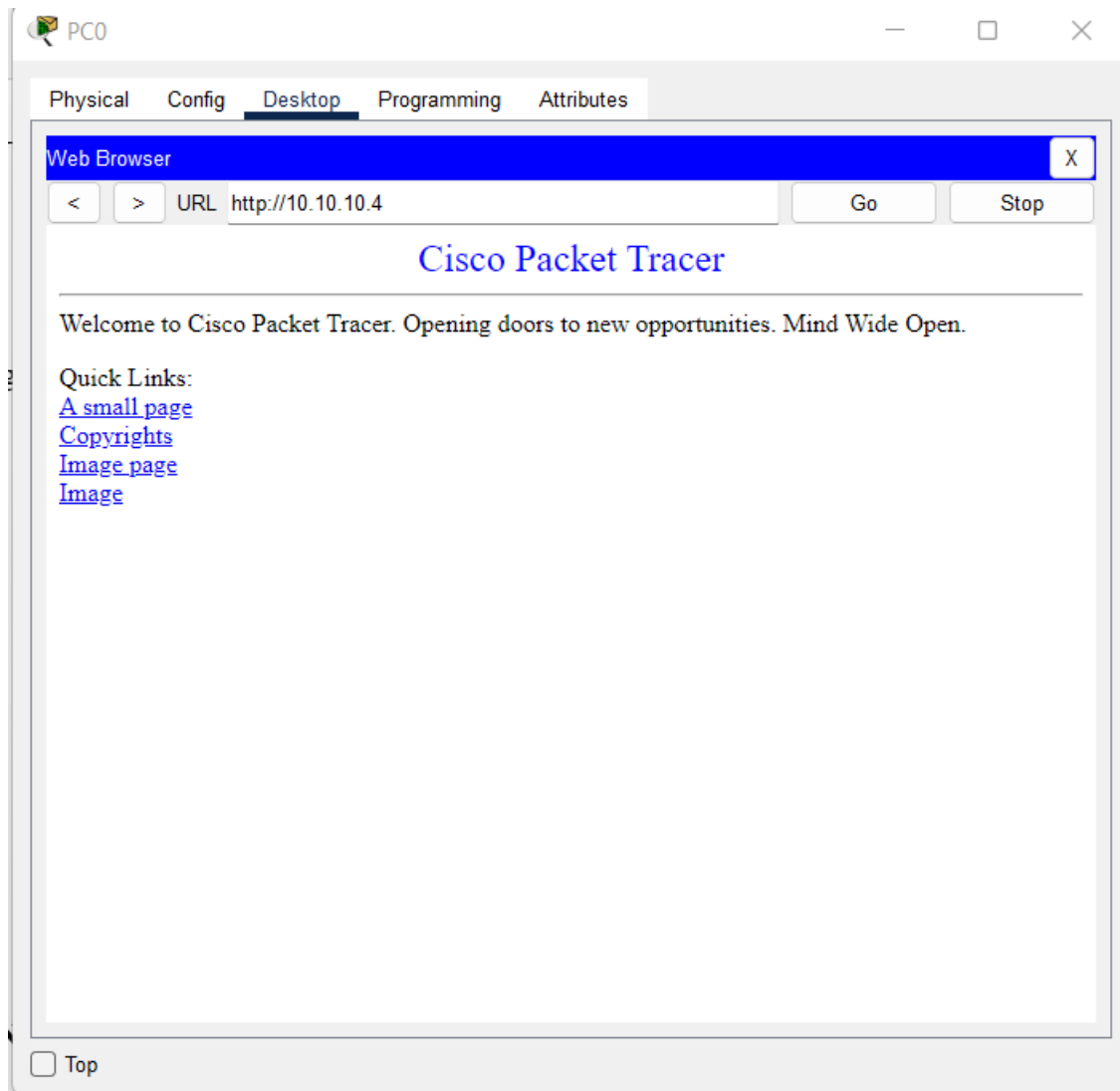
7.2 Result Analysis

SALESMAN DENIED:

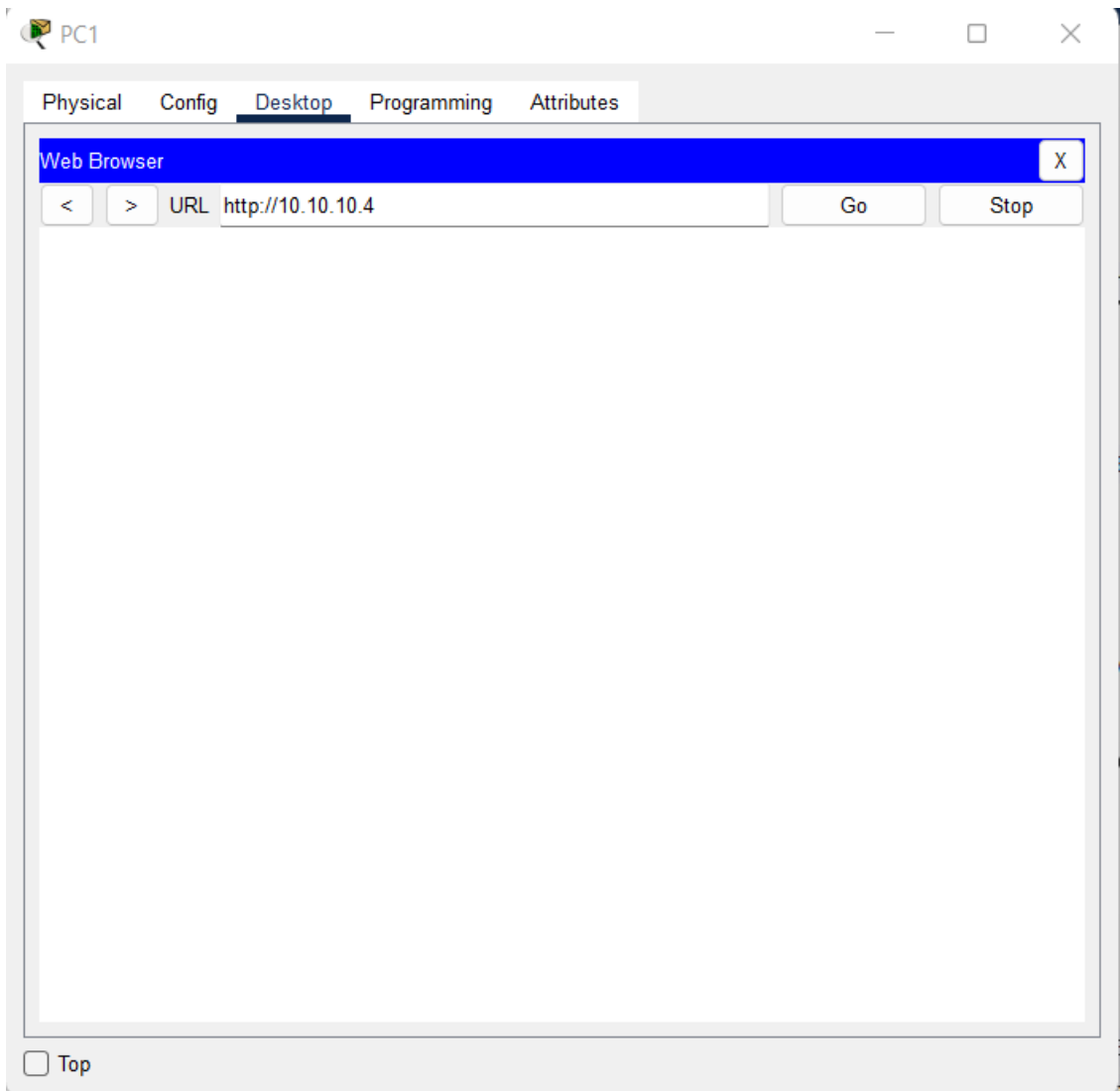


1.1 HTTPS Server Check

The server access was checked with HTTPS by using a browser by Sales manager:



Salesman are not able to access the HTTPS servers



8. CONCLUSION AND FUTURE ENHANCEMENT

From the above project, we implemented, demonstrated, and verified Standard ACL within an Organization. Now, as you already know there is an implicit deny at the end of every access list which means that if the traffic doesn't match any of the rules of the access list then the traffic will be dropped. By specifying any means that source having any IP address traffic will reach the Server except the traffic which it matches the above rules that you have made

Additionally, we can make the salesman communicate with engineers according to configuring Access control lists. And we can make ACL more specific using extended ACL.

9. REFERENCES:

1. <https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL>
2. <https://www.imperva.com/learn/data-security/access-control-list-acl/>
3. <https://www.geeksforgeeks.org/access-lists-acl/>
4. https://en.wikipedia.org/wiki/Access-control_list
5. https://en.wikipedia.org/wiki/Access-control_list
6. <https://www.youtube.com/watch?v=1puoq1N0qWI>
7. <https://www.youtube.com/watch?v=oYXsrNQBsuw&t=500s>
8. <https://www.youtube.com/watch?v=TihpWhQQsOM&t=203s>