# STANDARD ACCESS CONTROL LIST

A COURSE PROJECT REPORT

By

Under the guidance of   
**SUJATHA MURUGAN***In partial fulfilment for the Course*

of

18CSC381T - CRYPTOGRAPHY

in NWC



**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 "**STANDARD ACCESS CONTROL LIST**" is the bonafide work of **SHARAN.K (RA2011030010062), PAKAZHAVAN (RA2011030010067), RAAGUL VIGNESH.R (RA2011030010088), VISHWA (RA2011030010105), MADAR HUSSAIN KHAN (RA2011030010109)** who carried out the project work under my supervision.

# SIGNATURE

SUJATHA MURUGAN

ASSOCIATE PROFESSOR

**NWC**

SRM Institute of Science and Technology

# 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 my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project

We wish to express my 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 my Course project Faculty **SUJATHA MURUGAN ,** **ASSOCIATE** **PROFESSOR**, **NWC,** for his/herassistance, timely suggestion and guidance throughout the duration of this course project.

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 PAGE NO.

* + - 1. **ABSTRACT**
      2. **INTRODUCTION**
      3. **REQUIREMENT ANALYSIS**
      4. **ARCHITECTURE & DESIGN**
      5. **IMPLEMENTATION**
      6. **ACCESS CONTROL LIST IMPLEMENTATION**
      7. **CONCLUSION**

1. **INTRODUCTION**

Access control lists 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.

On a computer system, certain users have different levels of privilege, depending on their role. For example, a user logged in as network administrator may have read, write and edit permissions for a sensitive file or other resource. By contrast, a user logged in as a guest may only have read permissions.

Access control lists can help organize traffic to improve network efficiency and to give network administrators granular control over users on their computer systems and networks. ACLs can also be used to improve network security by keeping out malicious traffic.

**ABSTRACT:**

An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network.

Each system resource has a security attribute that identifies its access control list. The list includes an entry for every user who can access the system. The most common privileges for a file system ACL include the ability to read a file or all the files in a directory, to write to the file or files, and to execute the file if it is an executable file or program. ACLs are also built into network interfaces and operating systems (OSes), including Linux and Windows.

**REQUIREMENTS**

* 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. Users on the internet should be able to access only https on the WEB server.

3. Users on the internet should have access only to the public IP address of the server and not the private IP address.

4. The users in the organization should have full access to the server.

5. TCP/IP Network design with IP addressing

6. Features and configuration required on the hardware with explanation

We need to configure a network design keeping the following requirements in mind.

* 1. **Hardware Requirement**

From the given scenario, we draw the following requirements:

For UNIVERSITY SRM (Private Network):

Hardware Required:

3x Server – PT Primary Server

2x Router (For address)

2x Switches:

1x STUDENT SIDE Switch

1x ADMIN SIDE Switch

7x End Devices:

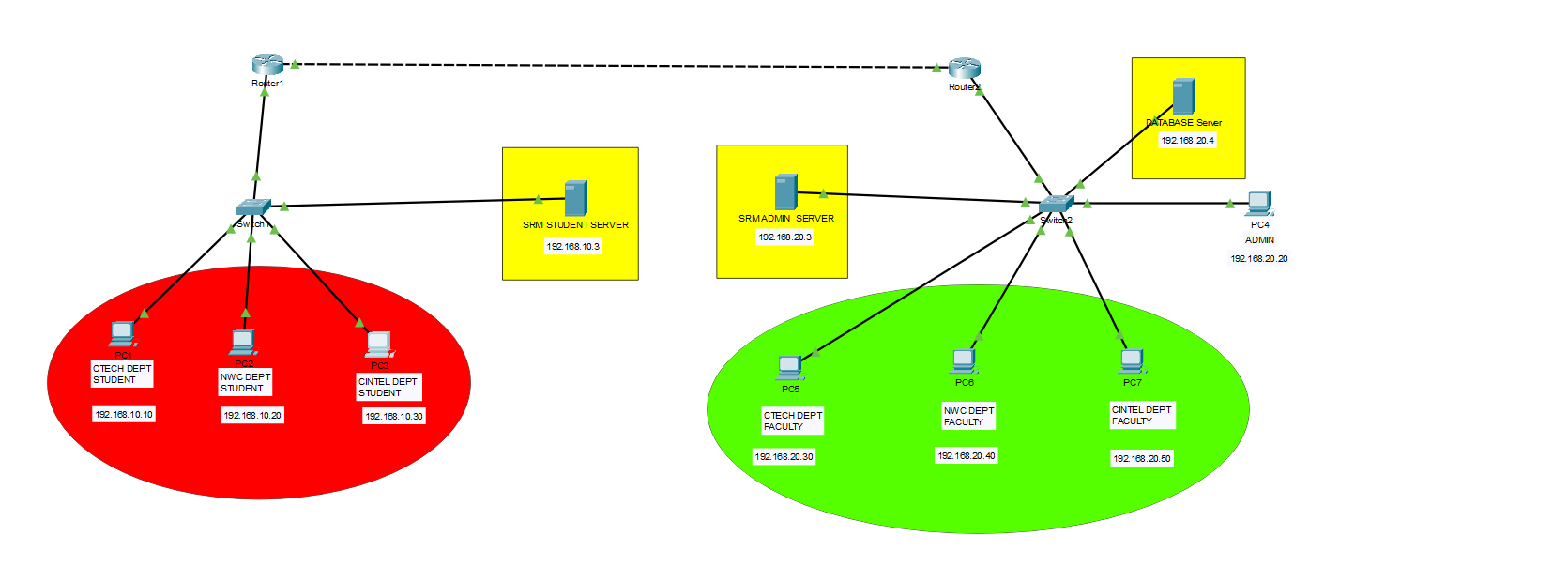
3x PCs for STUDENT

1x PCs for ADMIN

3x PCs for FACULTY

1. **ARCHITECTURE AND DESIGN**
   1. **Network Architecture**

The network architecture is as follows:



The architecture consists of three major networks:

* UNIVERSITY Network(s)
* PRIVATE Internet
* Network maintained by the Internet Service Provider

These networks are interconnected with each other with varying degrees (discussed in the implementation chapter).

1. **IMPLEMENTATION**

* 1. **Address Table**

The address table is as follows:

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **Address** |
| STUDENT Server  ADMIN Server  Data base Server | Fa0  Fa0  Fa0 | 192.168.10.3  192.168.20.3  192.168.20.4 |
| Students PC | Fa0/0 | 192.168.10.10 to 192.168.10.30 |
| Faculty PC | Fa0 | 192.168.20.30 |
| Fa0/0 | 192.168.20.50 |
|  | Fa0/0 | 192.168.20.40 |
| Admin PC | Fa0/0 | 192.168.20.20 |

The university Router has NAT configured with an ACL.

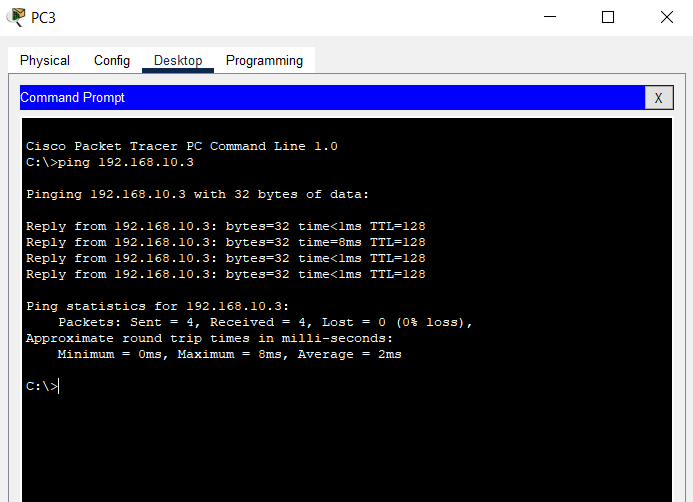
The Access Control List contains the entire broadband network. Any request from that network is translated to the private IP of the server.

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

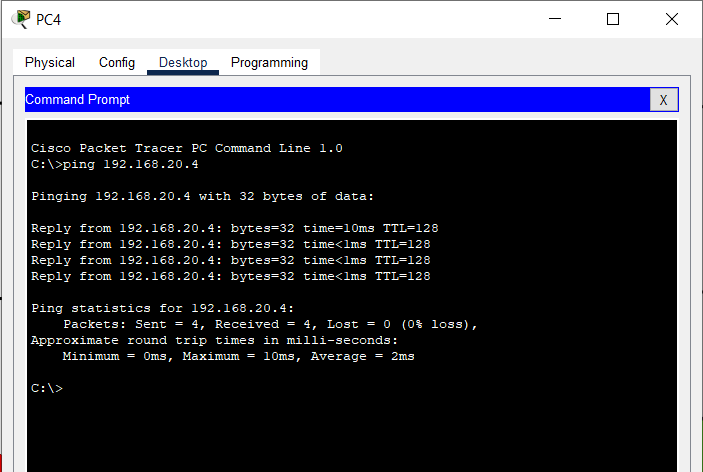
1. **RESULTS AND DISCUSSION**
   1. **Connection Check**

The network connections were checked by ping requests:

STUDENTS PC:

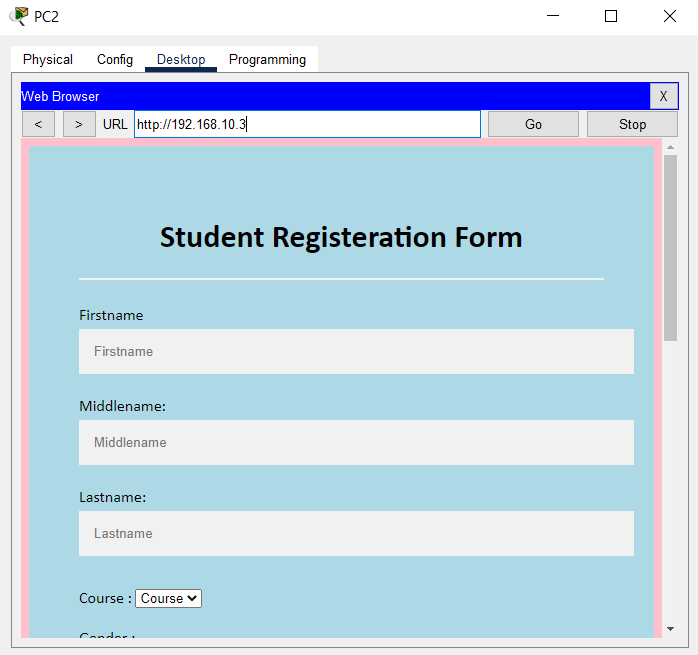
****

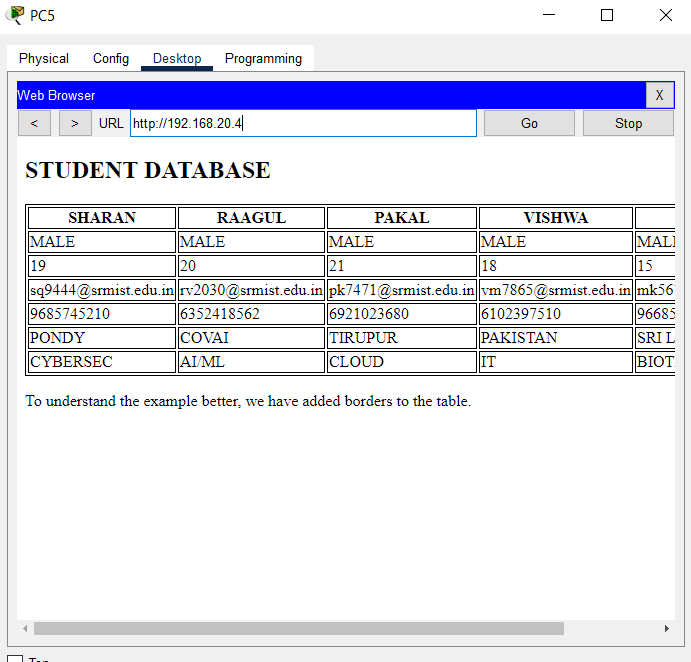
**ADMIN PC**

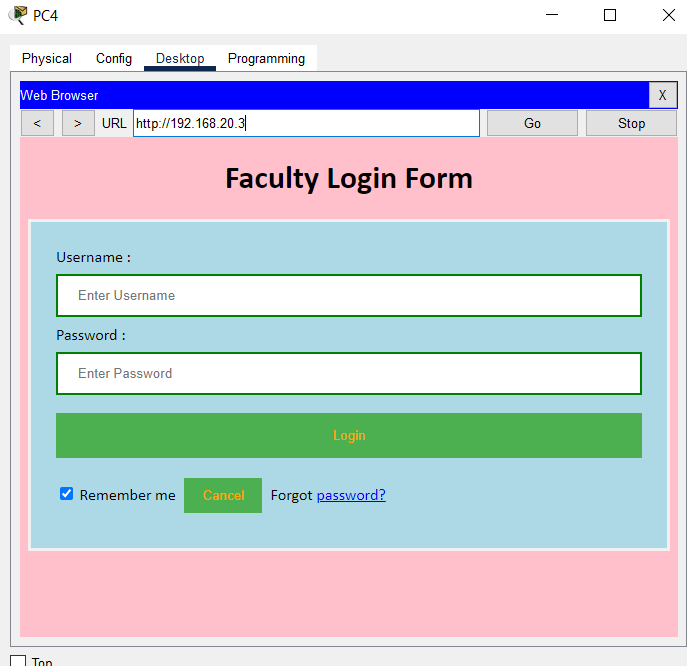
****

* 1. **HTTPS Check**

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







**ACCESS CONTROL LIST IMPLEMENTATION:**

router(config)#interface f0/1

router(config-if) #ip access-group 10 out

router(config)#**ip access-list standard**{access-list-name}

**Deny:**

router(config)#access-list 10 deny 192.168.10.10 0.0.0.255

router(config)#access-list 10 deny 192.168.10.20 0.0.0.255

router(config)#access-list 10 deny 192.168.10.30 0.0.0.255

**Permit:**

router(config)#access-list 10 deny 192.168.20.30 0.0.0.255

router(config)#access-list 10 deny 192.168.20.40 0.0.0.255

router(config)#access-list 10 deny 192.168.20.50 0.0.0.255

**CONCLUSION:**

HENCE THE ACCESS CONTROL LIST HAS BEEN IMPLEMENTED IN THE STUDENT AND THE ADMIN SERVER SUCCESSFULLY .