Mini Project Report
Submitted by

SUKUMAR(RA2111030010239)
SRINIVASA VARMA(RA2111030010231)
KARTHIKEYA(RA2111030010214)
SASI BHUSHAN(RA2111030010236)

Under the Guidance of

Dr S Murugaanandam

Assistant Professor
(Department of Network and Communications)

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING

with specialization in CSE Cyber Security

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603203
APRIL 2023

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

SRM INSTITUTION OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this lab report titled **“Internet usage control using access control techniques”** is the bonafide work done by SUKUMAR(RA2111030010239), SRINIVASA VARMA(RA2111030010231), KARTHIKEYA(RA2111030010214), SASI BHUSHAN(RA2111030010236),who carried out the lab exercises under my supervision. Certified further, that to the best of my knowledge the work reported here in does not form part of any other work.

SIGNATURE
Dr S Murugaanandam
Computer Communications– Course Faculty.
Assistant Professor.
Department of Network and Communications.

Head of the Department
Dr. Annapurani Panaiyappan. K
Network and Communications

DECLARATION

We, hereby declare that the work presented in this dissertation entitled "Internet usage Control Using Access Control Techniques" has been done by our team, and this dissertation embodies our own work.

SUKUMAR(RA2111030010239)
SRINIVASA VARMA(RA2111030010231)
KARTHIKEYA(RA2111030010214)
SASI BHUSHAN(RA2111030010236)

Internet usage Control Using Access Control Techniques

Abstract: -

In this project we primarily focus on reducing network traffic across network devices using access control lists. It was observed that when the internet usage was very high it creates problems like slow internet, expensive internet bills etc. To solve this problem in our project we have redesigned the network design with the help of extended access control lists.

Objectives:

In this project main aim is to create a access control list which would allow only browsing traffic and all other traffic bound to the internet like FTP, Skype, etc should be blocked.

SOFTWARE USED:-

Cisco Packet Tracer:

- Cisco Packet Tracer is a visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.
- We can also configure each and every router and network with the IP address and tested whether the data transfer is successful or not.
- Using packet tracer we have implemented network topology, assigned routers and switches.

Network Requirements:

The software used is cisco packet tracer and for implementing Internet usage control using access control techniques this prototype we have used 1941 routers which have 8 serial ports, So that it will be easy for us to connect to pc's and we have also used Two 2960-24TT switches all over the network to connect to various pc's among the which are then interconnected to the servers and users. All the serial ports are assigned with IP addresses so they can be recognized between the pc's without confusion.

Design requirement analysis:

The network infrastructure is to support 2 users for prototype design. So 2 desktop computers would be required. To for a network for the computers, a switch would be required .An 1941 router delivers highly secure data, mobility, and application services .Here at the end for implementing the protocol and to check whether our design is working or not, we access the internet through a pc and enter the ip address of the server. Here ip addresses are converted through DNS protocol.

Hardware inventory list –

Devices	Required Nos
PCs	2
Routers	1
Switches	2
Server	01

Network design strategy :

- Web browsing traffic would comprise of the protocols http, https and dns. http and https is used by browsers and dns is used for resolving website names into IP address.
- Without DNS, name resolution would fail and browsing would not work.
- An access list is configured on the E0 interface as inbound which would allow only the protocols listed above and all other traffic is blocked.

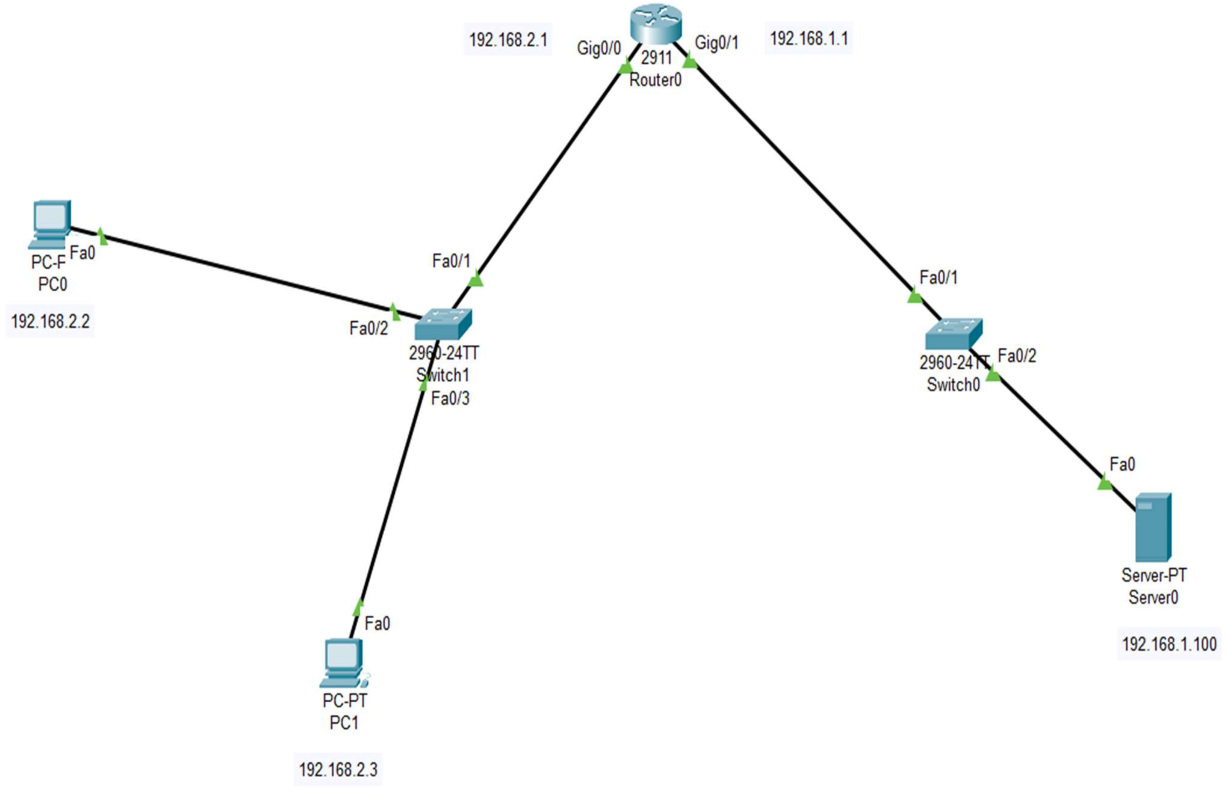
Access Control List:-

- Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

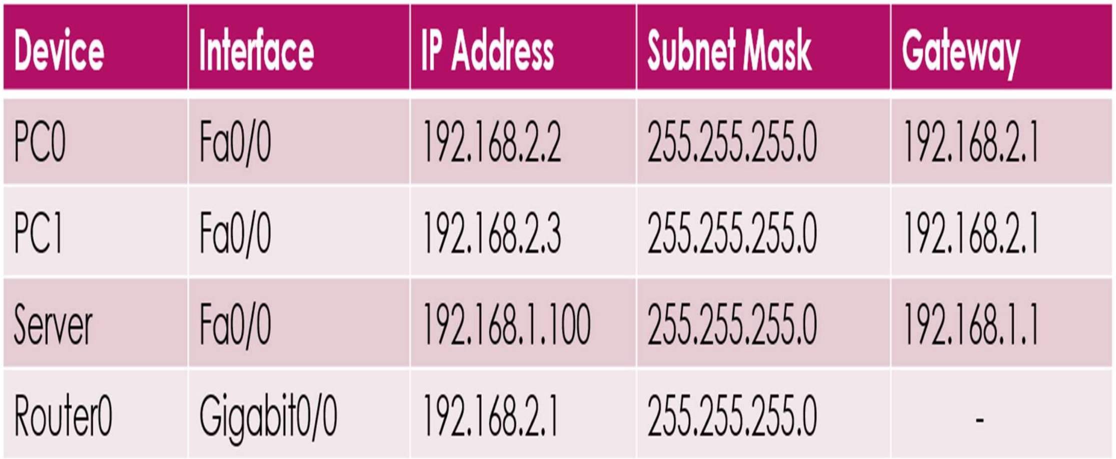
- Types of ACL – There are two main different types of Access-list namely:

- Standard Access-list – These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.
- Extended Access-list – These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

TOPOLOGY DIAGRAM:-



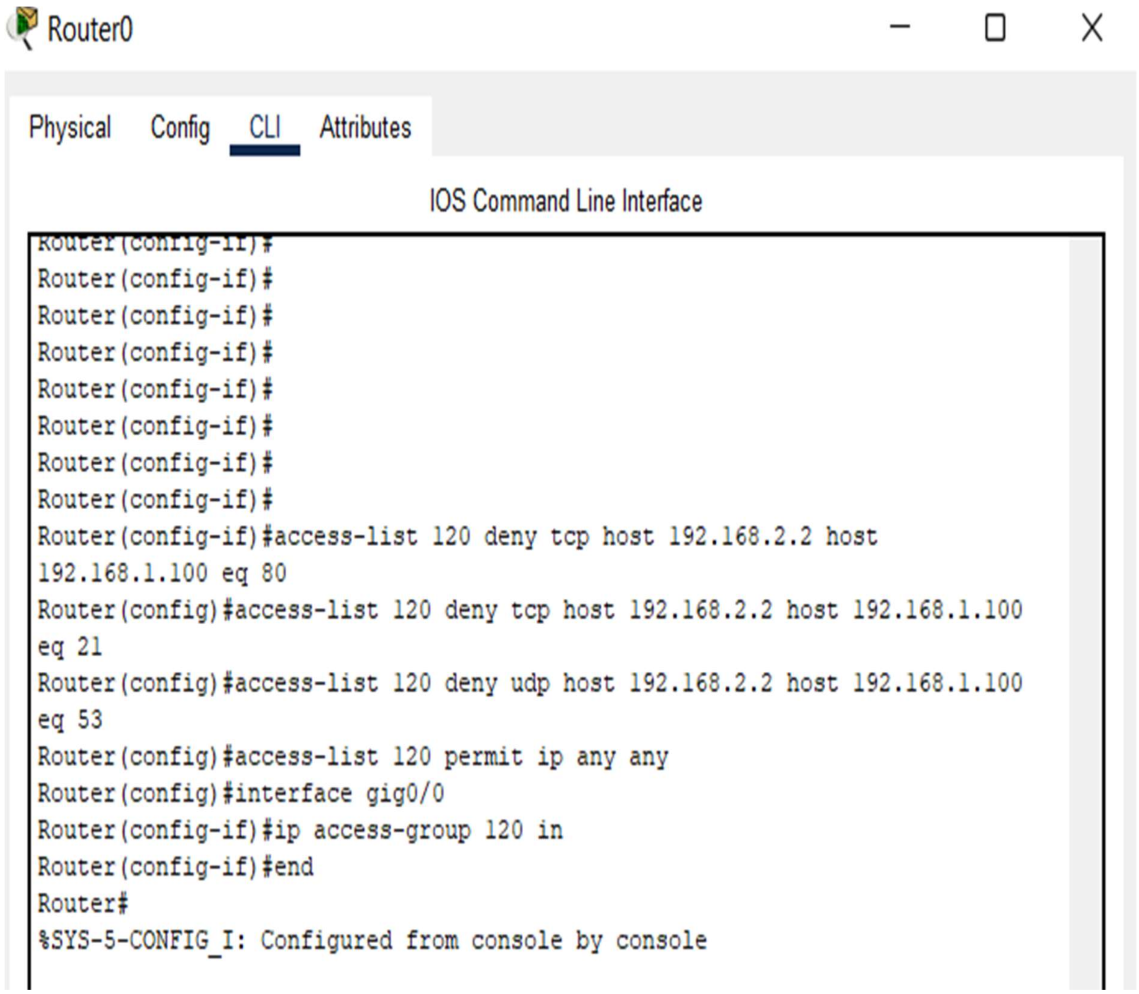
ADDRESSING TABLE:-



Device	Interface	IP Address	Subnet Mask	Gateway
PC0	Fa0/0	192.168.2.2	255.255.255.0	192.168.2.1
PC1	Fa0/0	192.168.2.3	255.255.255.0	192.168.2.1
Server	Fa0/0	192.168.1.100	255.255.255.0	192.168.1.1
Router0	Gigabit0/0	192.168.2.1	255.255.255.0	-

Router Configuration:-

- An extended ACL is configured on the E0 interface as inbound, the detail of which is shown below.
- Router(config)# #access-list 120 deny tcp host 192.168.2.2 host 192.168.1.100 eq 80
- Router(config)# # access-list 120 deny tcp host 192.168.2.2 host 192.168.1.100 eq 21
- Router(config)# #access-list 120 deny udp host 192.168.2.2 host 192.168.1.100 eq 53
- Router(config)# #access-list 120 permit ip any any
- Router(config)# interface gig0/0
- Router(config-if)#ip access-group 120 in



```
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#access-list 120 deny tcp host 192.168.2.2 host
192.168.1.100 eq 80
Router(config)#access-list 120 deny tcp host 192.168.2.2 host 192.168.1.100
eq 21
Router(config)#access-list 120 deny udp host 192.168.2.2 host 192.168.1.100
eq 53
Router(config)#access-list 120 permit ip any any
Router(config)#interface gig0/0
Router(config-if)#ip access-group 120 in
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Router Configuration Explained:-

- The first line configures the ACL to allow TCP port 80 for http communication.
- The second line configures the ACL to allow TCP port 443 for allowing https communication.
- The 3rd line configures the ACL to allow TCP port 443 for allowing https communication.
- The 4th line goes to the interface of the router.
- The 5th line applies the ACL as inbound.
- The implicit deny functionality of Cisco ACL would ensure that all other protocols are denied automatically.
- The configurations would ensure that only http, https and dns traffic is allowed from the network 192.168.2.0/24 to the E0 interface through which packets bound for the internet travel.
- This would ensure that users would be unable to access any other type of traffic apart from the protocols listed above.

CONCLUSION –

In the world of technology, there are vast numbers of users' communicating with different devices in different languages. That also includes many ways in which they transmit data along with the different software they implement. So, communicating worldwide will not be possible if there were no fixed 'standards' that will govern the way user communicates for data as well as the way our devices treat those data.Some of them are TCP,UDP,Internet Protocol, Hyper Text Transfer Protocol (HTTP),FTP etc. DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.So we access all these protocols or standards we generally use internet in our daily life.

In our project in order to decrease the internet traffic we have used Access Control Lists and the network topology has been redesigned in such a way that browsing traffic is allowed and remaining traffic is blocked.

References:-

- https://www.geeksforgeeks.org/

  For gathering information regarding access control lists concept.

- https://www.tutorialspoint.com/index.html

  For gathering information related to_various protocols used in internet.

- https://www.netacad.com/courses/packet-tracer

  For designing the network topology in cisco packet tracer.

- https://www.javatpoint.com/

  For gathering information regarding DNS protocol.