A CN PBL Report

On

# Internet Usage Control Using Access Control Techniques

Submitted by

Mr. Kunal Amare (C-55)

Miss. Pradnya Mane (C-58)

Miss. Sanjana Sawant (C-59)

Miss. Namrata Mane (C-67)

Mr. Harshwardhan Patil (C-72)

**Under the Guidance of**

Mr. S.S. Palkar

**Department of Computer Science and Engineering**

**KIT’s College of Engineering (Autonomous), Kolhapur.**

**2020-2021**

# Acknowledgement

We would like to express our deep gratitude to Mr. S.S.Palkar Asst.Professor, KIT’s College of Engineering, Kolhapur, for providing this opportunity to carry out the PBL of Computer Networks. We are grateful to all faculties for providing academic inputs, guidance and encouragement throughout this period. We would like to express a deep sense of gratitude and thank Mr. S. S. Palkar without whose permission, wise counsel and able guidance, it would have not been possible to carry out our PBL in this manner.
Finally, we express my indebtedness to all who have directly or indirectly contribute to the successful completion of our PBL.

# List of Figures

## Table of Content

# 1. Introduction

ACLs, known for their ability to filter traffic as it either comes into or leaves an interface.

ACLs are basically a set of commands, grouped together by a number or name, that are used to filter traffic entering or leaving an interface. ACL commands define specifically which traffic is permitted and denied. ACLs are created in Global Configuration mode. By default, switches break up collision domains and routers break up broadcast domains. By using ACL, the internet traffic will be filtered, the router will allow or deny any specified protocol in the router configuration. The web browsing traffic would comprise of protocols HTTP, HTTPS, DNS. DNS is used for resolving websites names into IP address while HTTP and HTTPS are used by browsers.

## 1.1 Problem Statement

The increased internet usage in LAN or WAN may create problems like slow internet, threat to security and expensive internet bills. To solve this problem, the network would be redesigned such that it would allow only browsing traffic and all other traffic bound to the internet would be blocked. With a good Wi-Fi router, there are several ways to control internet access, both at home and at the office. Not only can you control who can access the internet from your router, you can also block websites, limit the hours of access, throttle bandwidth and even block rogue access points from hijacking your network. Although the administrative options on a router vary with different models and manufacturers, usually, the best place to start is to look for the router's parental controls. Even routers designed for small businesses have parental controls, so controlling internet access at home is often the same as controlling it at work.

## 1.2 Project Purpose

This project is aimed to reduce the internet usage in a particular network. For this we use Access Control List (ACL). The main idea of using ACL is to provide security, to reduce internet usage and make it less vulnerable to unwanted and dangerous traffic. The project focuses on improving security by using ACL, that is we can deny specific routing updates or provide traffic flow control. In this way, the project will be reducing the incoming traffic into the network and hence reduce internet usage.

## 1.3 Project Scope

This project involves controlling Internet usage using access control techniques. Access list criteria could be the source address of the traffic, the destination address of the traffic, or other information. Basically, control list is group of statements where each statement has specific pattern found in packet of IP. When a packet comes through an interface associated with access list, list is scanned from top to bottom order. Cisco provides basic traffic filtering capabilities with ACL. All routed network protocols can be configured to filter the packets with help of access lists. By defining access list, we define criteria that are applied to each packet which is processed by router. Decision to permit or deny that particular protocol will be taken by router. In traditional Local Area Network, the sending host uses the Address Resolution Protocol (ARP) to determine the MAC address associated with the destination IP address as Traffic sent to an IP address in the same subnet stays within local area network.

## 1.4 System Analysis

### 1.4.1 Existing System

In a traditional local area network (LAN), hosts are connected by a network of hubs and switches. The switches cooperate to construct a spanning tree for delivering traffic. Each switch forwards Ethernet frames based on its destination MAC address. If the switch contains no forwarding-table entry for the frame’s destination MAC address, the switch floods each frame over the entire spanning tree.

A switch learns how to reach a MAC address by remembering the incoming link for frames sent by that MAC address and creating a mapping between the MAC address and that port. To connect to the rest of the enterprise net- work (and the rest of the Internet), the island of Ethernet switches connects to IP routers that forward traffic to and from remote hosts. Each host interface in the LAN has an IP address from a common IP prefix (or set of prefixes). Traffic sent to an IP address in the same subnet stays within the LAN; the sending host uses the Address Resolution Protocol (ARP) to determine the MAC address associated with the destination IP address. For traffic destined to remote IP addresses, the host forwards the packets to the gateway router, which forwards packets further toward their destinations.

### 1.4.2 Limitations of Existing System

- Privacy Violations: It is difficult to make the system secure from hackers, novices or industrial espionage. Also, The LAN administrator can see and check personal data files of each and every LAN user. Moreover, he can view the computer and internet history of the LAN user.
- As traffic increases on a network the performance degrades unless it is designed properly. The larger the network becomes difficult to manage.
- Perhaps the unnecessary Searches or Downloads can drastically slow down the system.
- This possesses the greater risk of Malware and Virus suffering through the useless websites can cause the installation of malware which can eventually turns into financial loss.
- Not suitable for traffic-intensive applications. In case the rate of traffic on the LAN goes up the efficiency of the LAN goes down. It becomes backbreaking activity to control such traffic.

### 1.4.3 Proposed System

We are planning to use access control techniques to control internet usage. Access lists can be configured for all routed network protocols to filter the packets of different type of protocols as the packets pass through a router. When we define an access list, we define criteria that are applied to each packet that is processed by the router. The router will decide whether to permit or deny that protocol. We are trying to control who can access the internet from router, also can block websites, limit the hours of access, even block rogue access points from hijacking the network.

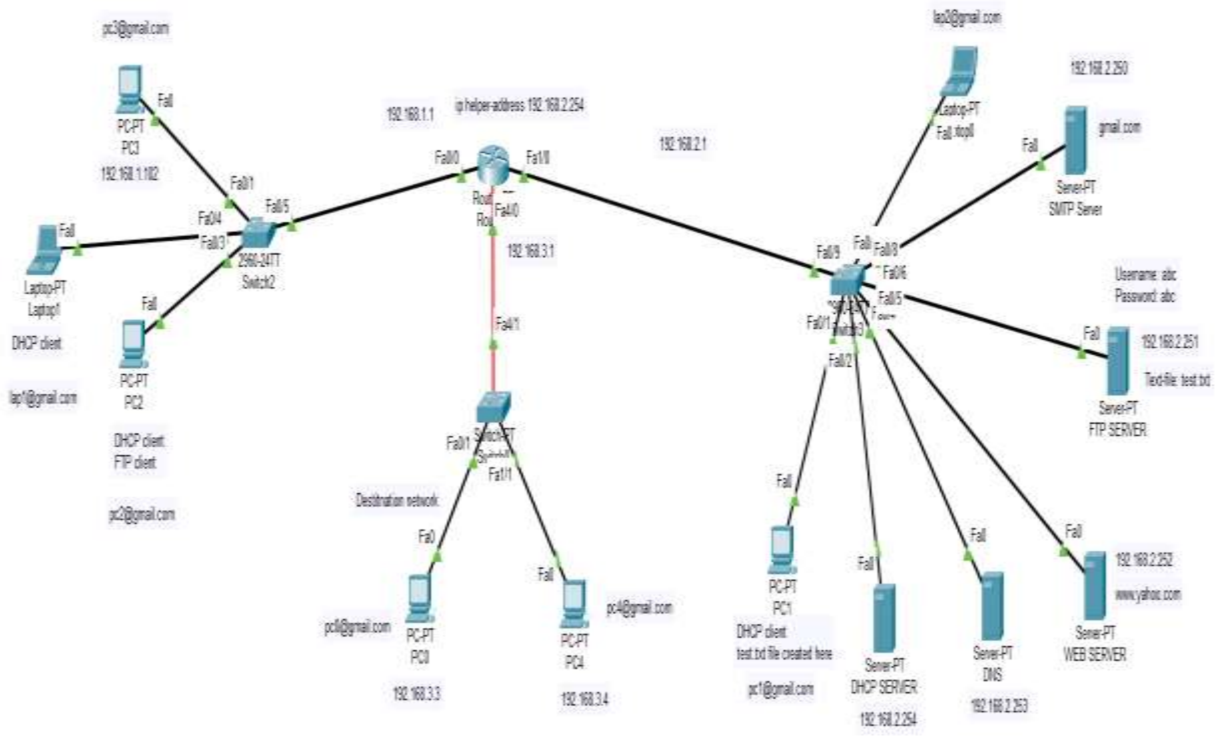

*Figure 1: Network design*

### 1.4.4 Advantages of Proposed System

- The ACL limits the network traffic to increase network performance.
- This reduces the internet usage for unwanted traffic. The filtering strategy in place at the network edges reduces many of the risks associated with direct network attacks.
- People belonging to that same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.
- It provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network. ACL provides control over the traffic as it can permit or deny according to the need of network.
- Cost and time reduction - LAN can reduce the migration cost of stations going from one group to another Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software.
- Security – It provides an extra measure of security.

## 1.5 Definitions, Acronyms, Abbreviation

1) ACL - Access Control List. An access control list (ACL) is a list of access control entries (ACE) that will perform packet filtering to control the movement of packets through a network.
2) ACE - Access Control Entry. An access control entry specifies the access or auditing permission to an object.
3) HTTP - Hypertext Protocol. It is the foundation of any data exchange on the web.
4) DNS - Domain Name System. It translates domain names into IP addresses.
5) TCP - Transmission Control Protocol. It is a communication standard that enables application programs and computing devices to exchanges messages over a network.
6) MAC Address – Media Access Control Address.
7) LAN – Local Area Network.
8) WAN – Wide Area Network.
9) ARP – Address Resolution Protocol.
10) IP – Internet Protocol.
11) DoS – Denial of Service

## 1.6 Overview

The increased internet usage in LAN or WAN may create problems like slow internet, threat to security and expensive internet bills. To solve this problem, the network would be redesigned such that it would allow only browsing traffic and all other traffic bound to the internet would be blocked. For this purpose, we are using Access Control Lists (ACL). Access control lists are used to filter traffic within a routed network is a critical network security practice. In ACL, the contact list is a group of statements. Each statement defines a pattern that would be found in an IP packet. As each packet comes through an interface with an associated access list, the list is scanned from top to bottom in the exact order that it was entered for a pattern that matches the incoming packet. Access list criteria could be the source address of the traffic, the destination address of the traffic, or other information. Cisco provides basic traffic filtering capabilities with access control lists. Access lists can be configured for all routed network protocols to filter the packets of different type of protocols as the packets pass through a router. When we define an access list, we define criteria that are applied to each packet that is processed by the router. The router will decide whether to permit or deny that protocol. The standard ACL create filters based on source addresses only and are used for server-based filtering, whereas extended ACL provide more security by creating filters based on source addresses as well as destination addresses, protocol and port number. Risk of direct network attack is reduced by filtering strategy. ACL's provide network administrator with ability to block traffic at key points within a network. Access control list at WAN and LAN will guard against infected systems from attacking on other sites.

# 2. The Overall Descriptions

## 2.1 Product Perspective

In this project, the network is designed in such a way that the internet usage of that network would be significantly reduced. Access control lists (ACLs) perform packet filtering to control the movement of packets through a network. A level of security for network access specifies which areas of the server/network/service can be accessed by a user and which cannot. Granular monitoring of the traffic exiting and entering the system.

An access control list (ACL) contains rules that grant or deny access to certain digital environments.

- ACL limits the network traffic to increase network performance and speed.

- This initiates in lowering the internet usage for unwanted traffic. The filtering strategy in place at the network edges that helps in reducing many of the risks associated with direct network attacks.

- People belonging to that same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.

- It provides security since the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network. ACL provides control over the traffic as it can permit or deny according to the need of network user.

- Cost and time reduction - LAN can reduce the migration cost of stations going from one group to another Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software.

## 2.2 Product Function

Routing security has received varying levels of attention over the past several years and has recently begun to attract more attention specifically on the public Internet. Despite this new attention, however, the area most open to attack is on the routing systems within any enterprise network. An enterprise routing infrastructure can easily be attacked and other attacks designed to corrupt or change the routing tables with the following results:

- Traffic redirection - In this attack, the adversary is able to redirect traffic, enabling the attacker to modify traffic in transit or simply sniff packets.
- Router DoS- Attacking the routing process can result in a crash of the router or a severe degradation of service.
- Routing protocol DoS- Similar to the attack previously described against a whole router, a routing protocol attack could be launched to stop the routing process from functioning properly.
- Unauthorized route prefix origination- This attack aims to introduce a new prefix into the route table that shouldn't be there. The attacker might do this to get a covert attack network to be routable throughout the victim network

There are some primary attack methods for the above attacks –

1. Configuration modification of existing routers-
2. Sending excess packets to routing protocol process
3. Modification of valid routing protocol message

The above attack methods are avoided in this project by following ways-

1. Configuration modification of existing routers- To counter configuration of existing router, the router must be secure.

2. Sending excess packets to routing protocol process- Malformed packets are nearly impossible to stop without participation of router vendor. Here routing protocol implementations have to use, for dealing with malformed messages or packets.

3. Modification of valid message – Message authentication can help to prevent the modification of valid routing protocol message.

## 2.3 User Characteristics

Access control lists (ACLs) identify traffic flows by one or more characteristics, including source and destination IP address, IP protocols and other parameters, depending on type of ACL. The network is designed in such way that it would allow only browsing traffic and all other type of traffic bound to the internet would be blocked. In this project, only HTTP, HTTPS and DNS protocols would be filtered into the system. This means that the users would be able to access only the browsing traffic and all other traffic would be denied. However, all the users within the LAN would be able to send and receive all types of traffic and the broadcast messages. If we want to allow all user to access network for one or more particular addresses then we need to deny those particular addresses and then all other will permit. This type of network design increase network security and reduces the internet/data usage by avoiding unwanted traffic from other networks.

This type of network design is beneficial to private networks or organizations using single LAN for communication. Thus, such type of technique reduces problems like internet usage in LAN, threat to security and expensive bills.

# 3.Specific Requirements

## 3.1 Functional Requirements –Access Control List (ACL)

An access control list (ACL) is a list of access control entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee.

ACL is created in the global configuration mode. After creating the basic group of ACL commands, we need to activate them. In order to filter traffic between interfaces, ACL needs to be activated in Interface Sub configuration Mode. Thus, the direction of filtering the traffic is classified into:

a. Inbound: The traffic is filtered as it enters the interface. If the ACL is set as inbound, the router compares the incoming packet with the interface ACL before it leaves the interface.
b. Outbound: The traffic is filtered as it leaves the interface. If the ACL is set as outbound, the router forwards the received packet to the exit interface where the packet is compared with the interface ACL.

The ACLs are of two types:

a. Numbered ACL: Unique number is assigned to each ACL.
b. Named ACL: Unique name is assigned to each ACL.

The ACLs supports the following types:

a. Standard ACL: ACL is applied on destination router. It permits or deny the packet on the basis of source addresses only.
b. Extended ACL: ACL is applied on source router. It permits or deny the packet on the basis of source as well as destination addresses.

## Configuring ACL

The “access-list” command is used to create an ACL. The syntax to create an ACL is:

*access-list <ACL_#> permit/deny conditions*

where,

- ACL_# - Allows to group statements into a single list.
- permit/deny - Specifies the action to be performed.
- Conditions - Specifies which packet needs to match for a router to execute an action.

After creating the ACL, it has to be applied to a process in the IOS. In order to activate ACL on the interface, the following syntax is followed:

*interface type slot_#/port_#*

*ip access-group ACL_# in/out*

where,

- in/out – Specifies the direction of traffic, whether it is inbound or outbound.

# 4. Environmental Setup

## Router Configuration

An extended ACL is configured on the E0 interface as inbound, the detail of which is as follows:

```
1)  Router>en
2)  Router#config t
3)  Router(config)#access-list 100 permit tcp any any eq www
4)  Router(config)#access-list 100 deny ip  any any
5)  Router(config)#interface fa4/0
6)  Router(config)#ip access-group 100 out
```

**Router configuration explained**

The network designed using these ACL commands would ensure that users would be unable to access any other type of traffic apart from the protocols listed above.

- We enable router configuration by using command “en” and “config t”.
- On third line, we create an access list numbered 100, and permit traffic of type www from any source to any destination in the network.
- On fourth line, we deny all other type of traffic.
- On fifth line, we configure the interface of FastEthernet 4/0.
- On sixth line, we create an access-group and apply it on the interface.

# 5. References

- International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 5, May 2016.
- David E. Taylor. “Survey and taxonomy of packet classification techniques.” *ACM Computing Surveys*, Vol. 37, No. 3, 2005. Pages 238-275.
- Cisco Systems Inc. *http://www.cisco.com*
- https://protechgurus.com/configure-standard-acl-cisco-router/
- https://ipcisco.com/lesson/standard-access-list-configuration-with-packet-tracer-2/
- A Flexible Generative Model for Preference Aggregation.