Department of Computer Science and Engineering

Computer Networks

Internet Usage Control using Access Control Techniques

Prepared by,

C55 Kunal Amare

C58 Pradnya Mane

C59 Sanjana Sawant

C67 Namrata Mane

C72 Harshwardhan Patil

Internet Usage Control Using Access Control Techniques

Problem Statement:

- In LAN or WAN problems like slow internet, threat to security and expensive internet bills are created due to increased internet usage.
- To solve these problems, network would be redesigned such that it would allow only browsing traffic(HTTP,HTTPS and DNS).
- All other traffic bound to the internet would be blocked.

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 solve problems like slow internet, expensive bills and make it less vulnerable to unwanted, dangerous traffic.
- By using ACL, 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.

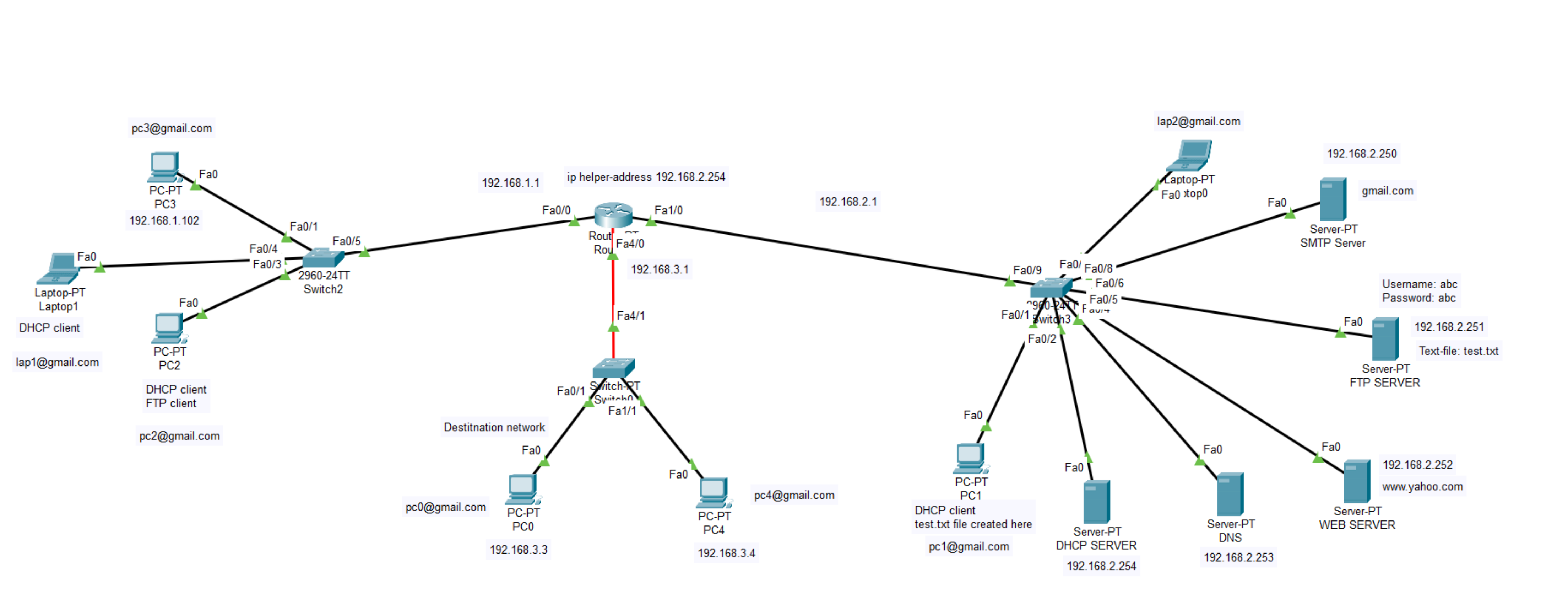
Existing System:

- In a traditional local area network (LAN), hosts are connected by a network of hubs and switches.
- 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 towards their destinations.

Limitations :

- There are some limitations of existing system-
- Privacy Violations- It is difficult to make the system secure from hackers and also LAN administrator can check personal data files of user.
- Larger network becomes difficult to manage as traffic increase on network.
- The unnecessary searches and downloads can slow down the system. This possesses greater risk of Malware and virus which suffering through useless websites.
- Not suitable for traffic-intensive applications.

Proposed System:



- Access list can be configured for all network protocols to filter the packets .
- In access list, we define criteria that are applied to each packet that is processed by router.
- The router will decide whether to permit or deny that protocol.
- We are trying to control who can access internet from router, also can block websites, limit the hours of access.
- Web browsing traffic would comprise of the protocols HTTP, HTTPS, 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 router interface as outbound which would allow only the protocols listed above and all other traffic is blocked.

Advantages:

- Limit 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 the same group can send broadcast message 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 need.

- ACL provides control over the traffic as it can permit or deny according to the need of network.
- The migration cost of stations is reduced as it move by using software.

ACL

- An access control list (ACL) is a list of access control entries (ACE).

- The direction of filtering the traffic is classified into:

i. 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.

ii. 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

ACL

The ACLs supports the following types:

i. Standard ACL: ACL is applied on destination router. It permits or deny the packet on the basis of source addresses only.

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

In this project, extended ACL is used in order to filter the traffic based on its type.

Router Configuration

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

Router Configuration explained

- 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.

Conclusion

- ACL can be configured on the router interface to reduce the internet usage.
- The ACL configured on the outbound of the router filters only the browsing traffic into the destination network.
- This reduces the amount of data used in the network considerably.
- Also, it reduces the security threats.
- Further, people belonging to that same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.