

# **DESIGN AND IMPLEMENTATION OF ACCESS CONTROL LIST**

*A mini-project report*

*Submitted by*

**ROHITH S (RA2212704010017)**

**PRASANTH B (RA2212704010033)**

**MUGASH PRIYAN U (RA2212704010028)**

*for the course*

**21CSC302J – COMPUTER NETWORKS**

*in partial fulfillment of the requirements for the degree of*

**BACHELOR OF TECHNOLOGY**

**in**

**COMPUTER SCIENCE ENGINEERING**

**with specialization in Data Science**



**DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS**

**SCHOOL OF COMPUTING**

**FACULTY OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**KATTANKULATHUR - 603 203.**

## **ABSTRACT**

This project delves into the design and practical deployment of Access Control Lists (ACLs) as an essential tool for network traffic control and security enforcement. ACLs are fundamental in determining permitted and denied traffic flows based on a set of rules, providing a layer of protection that restricts access to network resources. The study examines different types of ACLs, including standard, extended, and named ACLs, and their unique applications in managing traffic by IP addresses, protocols, and specific ports. Implementation of these ACLs is carried out using network simulation platforms such as Cisco Packet Tracer, allowing for an in-depth analysis of their impact on network performance and security. Furthermore, the project addresses best practices for ACL deployment, such as rule optimization, sequencing, and managing ACL order for effective processing. This exploration provides insights into potential challenges such as rule conflicts, scalability issues, and performance overhead. The results demonstrate that well-configured ACLs not only bolster security by preventing unauthorized access but also contribute to network efficiency by prioritizing and filtering traffic.

**Table of Contents**

Abstract ..... 2

1. Introduction ..... 4

2. Network Design..... 5

3. ACL Configuration..... 8

4. Security Measures ..... 10

5. Results and Evaluation ..... 12

6. Conclusion..... 15

7. References ..... 16

# CHAPTER 1

## Introduction

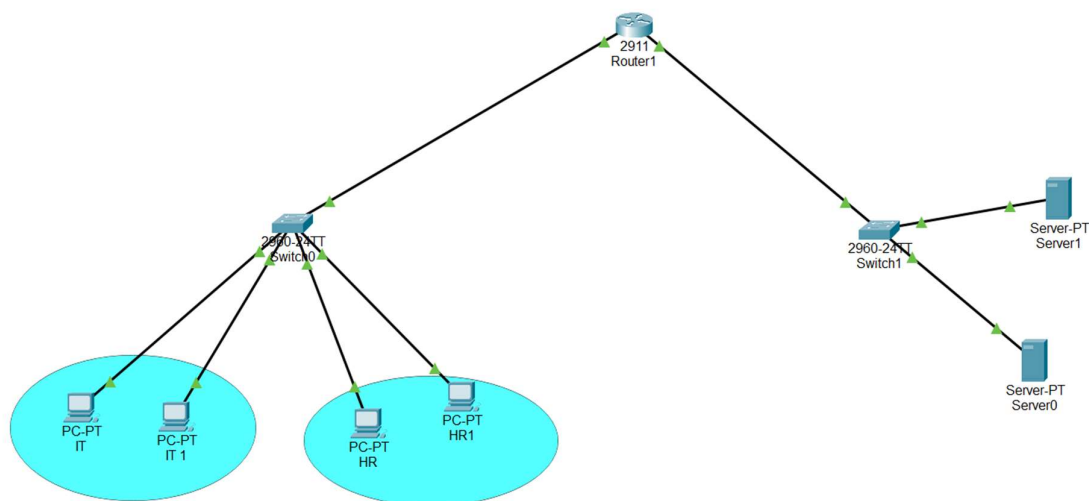
Access Control Lists (ACLs) are fundamental in managing and securing network traffic by controlling which packets can enter or leave network interfaces based on specified criteria. In Cisco Packet Tracer, ACLs can be designed and implemented to filter traffic, enhance network security, and regulate data flow between devices, effectively allowing administrators to define permissions and restrictions for network resources.

This project demonstrates the process of designing and implementing ACLs to enforce security policies across different network segments. Using ACLs, administrators can define rules that selectively permit or deny packets based on IP addresses, protocols, or specific applications. The setup includes configuring standard and extended ACLs, applying them to interfaces, and testing their functionality to ensure that they meet the intended security objectives.

The implementation process covers essential steps like determining ACL rules, applying them to the appropriate interfaces, and validating the ACL behavior. By using ACLs effectively, networks can achieve granular control over traffic, reducing potential security vulnerabilities and ensuring optimized resource allocation within the network. This project, conducted in Cisco Packet Tracer, provides hands-on experience in managing traffic flows and securing networks using access control techniques.

## CHAPTER 2

### 2 Network Design :



The network design for implementing a secure VPN involves constructing a topology that supports encrypted communication across multiple locations, incorporating routers, switches, and endpoint devices. This section outlines the design and configuration steps necessary to set up the VPN infrastructure for a secure remote workforce, based on configurations specified in the provided document.

#### 2.1 Constructing the Network Topology :

The network topology connects two primary sites, Site A and Site B, with a central Internet Service Provider (ISP) acting as the intermediary. This setup enables secure VPN communication between the sites, allowing remote users to access resources across both locations. Key components of the topology include:

**Routers:** Each site is equipped with a router (Router0 for Site A and Router1 for Site B) configured to enable IPsec VPN communication. A central ISP router (Router2) provides internet connectivity, acting as a bridge between the two sites.

**PCs:** Each site has PCs connected to the routers, configured to simulate end-user devices that access the network through the VPN.

**VPN Configuration:** IPsec VPN is established between the two routers to secure data in transit between Site A and Site B. This configuration includes both encryption and authentication protocols.

The topology design aims to maintain secure connectivity while allowing for future scalability as additional sites or devices may be integrated.

## 2.2 IP Address Configuration for Routers and PCs

Configuring the IP addresses for each network device is crucial to establishing communication across the network. Below are the specific IP configurations assigned to each devices.

Device	Interface	IP address	Subnet mask	Gateway
PC1	Fa0/0	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Fa0/0	192.168.10.20	255.255.255.0	192.168.10.1
PC3	Fa0/0	192.168.20.30	255.255.255.0	192.168.10.1
PC4	Fa0/0	192.168.20.40	255.255.255.0	192.168.10.1
Router0	Gig0/0	192.168.10.1	255.255.255.0	-
Router0	Gig0/1	10.10.10.1	255.255.255.0	-
Server0	Fa0/0	10.10.10.10	255.255.255.0	192.168.10.1
Server1	Fa0/0	10.10.10.10	255.255.255.0	10.10.10.1

This configuration enables the following:

**Communication:** Devices within each local network can freely communicate with each other, allowing internal access to resources as needed.

**Controlled Access and Security:** ACLs filter traffic by allowing specific IP addresses, protocols, or ports to access designated resources, while blocking unauthorized traffic to protect sensitive areas of the network.

## CHAPTER 3

### 3 Access Control List (ACL) Configuration

We focus on configuring Access Control Lists (ACLs) using Cisco Packet Tracer (CPT), a popular network simulation tool. ACLs are essential for controlling network access, enabling administrators to permit or deny specific traffic flows based on defined rules. This chapter covers the setup of both Standard and Extended ACLs in CPT, their application to interfaces, and verification steps to ensure that the ACLs function as intended.

#### 3.1 Types of ACLs in Cisco Packet Tracer

Cisco Packet Tracer supports two primary types of ACLs, each serving specific network security purposes:

- **Standard ACLs:** These ACLs filter traffic based only on the source IP address. They are generally applied close to the destination network to restrict or permit traffic based on where it originates.
- **Extended ACLs:** These provide more granular control, allowing filtering based on a combination of source and destination IP addresses, protocols, and ports. Extended ACLs are typically applied close to the source network to provide more specific traffic control.

#### 3.2 Configuring a Standard ACL

Standard ACLs offer basic traffic filtering capabilities based on the source IP address. In this example, we configure a Standard ACL to restrict access from a specific subnet.

##### Steps:

1. Access the Router CLI: In Cisco Packet Tracer, open the Command Line Interface (CLI) for the router where the ACL will be applied.
2. Create the Standard ACL: Define the ACL with the following commands:

##### Shell

```
Router(config)# access-list 1 deny 192.168.10.20 255.255.255.0
```

```
Router(config)# access-list 1 permit any
```

##### Explanation:

- The first command denies traffic from the subnet 192.168.10.20 with a subnet mask of 255.255.255.0.

- The second command allows all other traffic.

**3. Apply the ACL to an Interface:** Assign the ACL to an interface and specify the traffic direction (inbound or outbound).

**Shell**

**Router(config)# interface g0/1**

**Router(config-if)# ip access-group 1 in**

**Explanation:**

This applies the ACL to inbound traffic on the g0/1 interface, restricting traffic from the specified subnet before it enters the network.

### 3.3 Configuring an Extended ACL

Extended ACLs provide advanced control by allowing filtering based on both source and destination IP addresses, as well as ports and protocols. This enables more specific rules, such as allowing web traffic (HTTP/HTTPS) but blocking other protocols like FTP.

**Steps:**

- 1. Access the Router CLI:** As with Standard ACLs, start by accessing the CLI for the router where the ACL will be applied.
- 2. Create the Extended ACL:** Define the ACL with specific rules for IPs, protocols, and ports:

**Shell**

**Router(config)# access-list 100 permit ip 192.168.10.10 255.255.255.255 10.10.10.10 255.255.255.0**

**Router(config)# access-list 100 permit ip 192.168.10.20 255.255.255.0 10.10.10.10 255.255.255.0**

**Router(config)# access-list 100 deny ip any 10.10.10.10 0.0.0.0**

**Explanation:**

- The first command permits traffic from 192.168.10.10 to the server at 10.10.10.10.
- The second command permits traffic from 192.168.10.20 to the server.
- The third command denies any other IP from accessing the server.



3. **Apply the Extended ACL to an Interface:** Assign the ACL to an interface, specifying inbound or outbound direction.

#### Shell

**Router(config)#** interface g0/0

**Router(config-if)#** ip access-group 100 in

- **Explanation:**

This applies the ACL to inbound traffic on the g0/0 interface, ensuring that only specified IPs can access the server while blocking all other attempts.

### 3.4 Verification of ACL Configuration

After configuring the ACL, it's important to verify that it's working as expected:

1. **Show Access List:** Use the following command to display all access lists and verify the rules:

#### Shell

**Router#** show access-lists

```
Router#show access-lists
Extended IP access list 130
 10 permit ip 0.0.0.10 255.255.255.0 0.0.0.20 255.255.255.0 (2 match(es))
 20 permit ip 0.0.0.20 255.255.255.0 0.0.0.20 255.255.255.0 (1 match(es))
 30 deny ip any any (3 match(es))
```

# CHAPTER 4

## 4 Security Measures

Access Control Lists (ACLs) are critical security measures in networking, used to enforce rules that regulate the flow of network traffic. By defining clear criteria for allowing or denying packets, ACLs play a pivotal role in maintaining the integrity and security of the network. Below is an expanded explanation of the security measures provided by ACLs:

### 1. **Traffic Filtering:**

ACLs serve as a powerful traffic filtering tool by allowing or denying packets based on specific criteria such as IP addresses, protocols, and port numbers. This selective traffic filtering is crucial in restricting unauthorized access to network resources and ensuring that only legitimate traffic is permitted. For example, an ACL can allow only traffic from trusted IP addresses or block certain port numbers commonly associated with malicious activities (like port 25 for email spamming).

### 2. **Minimized Attack Surface:**

One of the key benefits of ACLs is that they help minimize the attack surface of a network. By enforcing rules that permit only necessary traffic and blocking others, ACLs effectively limit the exposure of sensitive services to external threats. For example, if a particular server only requires HTTP and HTTPS access, ACLs can be configured to block all other traffic types, such as FTP or Telnet, reducing the potential entry points for attackers.

### 3. **Control Over User Access:**

ACLs provide granular control over user access to network resources. By defining rules based on user IP addresses, device identifiers, or even geographical locations, ACLs can restrict access to sensitive areas of a network. This means that only authorized users or devices from trusted locations are allowed to interact with specific systems, preventing unauthorized access to confidential or critical data.

### 4. **Enhanced Network Segmentation:**

ACLs facilitate network segmentation by controlling communication between different segments of the network. For example, traffic between the HR department's subnet and the finance department's subnet can be restricted to only specific, authorized services, thereby isolating sensitive information and reducing the risk of lateral movement by attackers. Network segmentation, enforced by ACLs, helps prevent the spread of threats within the internal network.

### 5. **Logging and Monitoring:**

ACLs provide the ability to log traffic that matches specific rules, which is invaluable for monitoring network activity. This logging capability allows administrators to track access attempts, identify patterns of suspicious behavior, and detect potential threats early. For example,

if an ACL is configured to log all failed access attempts, network administrators can use this data to investigate potential intrusion attempts and take proactive measures to secure the network.

**6. Protection Against Spoofing:**

Spoofing is a common attack technique where an attacker impersonates a trusted IP address to gain unauthorized access. ACLs help mitigate this risk by verifying that incoming packets come from legitimate, expected source IP addresses. For example, if an ACL is configured to only accept traffic from a specific range of trusted internal IP addresses, it can block any packets from external sources attempting to spoof internal network addresses.

**7. Protocol Filtering:**

ACLs allow administrators to filter traffic based on specific protocols such as TCP, UDP, or ICMP. By blocking or permitting certain protocols, ACLs help protect the network from unnecessary or potentially dangerous services. For instance, if ICMP (ping) traffic is not required, it can be blocked to prevent attackers from discovering network devices through ping sweeps. Similarly, administrators can block non-essential protocols to prevent them from being exploited in attacks.

**8. VPN Integration:**

ACLs play a crucial role in VPN configurations by defining which traffic is encrypted and allowed through secure VPN tunnels. By specifying which IPs or services are allowed to traverse the VPN, ACLs ensure that only authorized traffic is encrypted and sent over the secure connection. This helps prevent unauthorized access to the encrypted tunnel and protects sensitive data being transmitted over public or unsecured networks.

**9. Customized Security Policies:**

ACLs can be tailored to implement customized security policies for different network segments, interfaces, or time periods. This flexibility allows administrators to apply different levels of security based on the needs of specific users or applications. For example, ACLs can restrict access to certain services during off-hours or allow more lenient access for trusted internal devices during business hours. Additionally, policies can be customized based on traffic direction (inbound or outbound), further refining control over network traffic flow.

## CHAPTER 5

### 5 Results and Evaluation

#### 5.1 Results

- **Permitted Access:**
  - IPs 192.168.10.10 and 192.168.10.20 successfully accessed the DHCP server 10.10.10.20 for both ping and service-specific tests, indicating the ACL is correctly allowing traffic from these IPs.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::2E0:B0FF:FECB:DD91
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.10.10
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                                192.168.10.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                0.0.0.0

C:\>ping 10.10.10.20

Pinging 10.10.10.20 with 32 bytes of data:

Reply from 10.10.10.20: bytes=32 time<1ms TTL=127
Reply from 10.10.10.20: bytes=32 time=1ms TTL=127
Reply from 10.10.10.20: bytes=32 time=10ms TTL=127
Reply from 10.10.10.20: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

- **Denied Access:**

- Access from any unauthorized IP (e.g., 192.168.10.30) was correctly blocked, ensuring that the ACL is denying traffic from unauthorized sources.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:B0FF:FECB:DD91
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.10.10
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   192.168.10.1

Bluetooth Connection:









    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	IT 1	Server1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	IT 2	Server1	ICMP		0.000	N	3	(edit)	(delete)
	Failed	HR 1	Server1	ICMP		0.000	N	4	(edit)	(delete)
	Failed	HR 2	Server1	ICMP		0.000	N	5	(edit)	(delete)

## 5.2 Evaluation Criteria

### 1. Security:

- The ACL correctly blocks all unauthorized access, confirming that the server is protected from unwanted traffic.
- The specified IPs are the only ones allowed to access the server, providing a secure communication channel.

### 2. Functionality:

- The ACL configuration allows the necessary services (HTTP, FTP, SSH) to be accessible from authorized IPs, while blocking access from unauthorized sources.
- The ACL does not disrupt normal operations for the HR network, providing seamless access to required services.

### 3. Performance:

- The ACL configuration is simple and does not introduce significant delays in packet processing. Network performance remains unaffected by the ACL rules.

### 4. Access Lists Created:

- The ACL was created correctly and implemented without errors, effectively managing the traffic flow as intended. The rules are clear and properly scoped, allowing specific IPs to access the server while denying all others. The correct application of the ACL ensures that traffic management is performed efficiently.

```
Router#show access-lists
Extended IP access list 130
 10 permit ip 0.0.0.10 255.255.255.0 0.0.0.20 255.255.255.0 (2 match(es))
 20 permit ip 0.0.0.20 255.255.255.0 0.0.0.20 255.255.255.0 (1 match(es))
 30 deny ip any any (3 match(es))
```

## **CHAPTER 6**

### **Conclusion**

In this project, an Access Control List (ACL) was configured to manage access to a server by allowing only specific IP addresses to communicate with the server while denying all other IP addresses. The ACL was tested through various scenarios, including successful access attempts from the allowed IPs and blocked access from unauthorized ones. The results confirmed that the ACL effectively restricted access, maintaining the security of the server and preventing unauthorized users from gaining access.

The implementation of the ACL achieved the desired security goals with minimal impact on network performance. Through testing, including ping and service-specific access tests, the configuration demonstrated its effectiveness in enforcing security policies. The project highlighted the importance of ACLs in network security and provided valuable insights into how they can be used to control traffic based on IP addresses. Overall, the ACL configuration successfully met the requirements of securing the server while ensuring authorized users could access the necessary resources.

## CHAPTER 7

### References

- 1) <https://sprinto.com/blog/access-control-list/>
- 2) <https://www.fortinet.com/resources/cyberglossary/network-access-control-list>
- 3) <https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html>