The Simulation of Access Control List (ACLs) Network Security for Frame Relay Network at PT. KAI Palembang

Kurniati\(^1\), Rahmat Novrianda Dasmen\(^2\)

\(^a\)Teknik Komputer, Universitas Bina Darma
Jenderal A. Yani street number 03 Palembang, Indonesia
\(^1\)kurniati@binadarma.ac.id
\(^2\)rahmat.novrianda.d@gmail.com

Abstract

PT. KAI Palembang is a branch of PT. Kereta Api Indonesia (KAI) Persero located in South Sumatra Province, where PT. KAI Persero is an Indonesian State-Owned Enterprise that organizes railway transportation which provide services including passenger and goods transportation. PT. KAI Palembang has a computer network connected to PT. KAI Persero central is located in Jakarta. Now, PT. KAI Palembang is trying to improve computer network security, where one of them is limiting the access of users who connected to PT. KAI Palembang computer network. This can be done by implementing Access Control Lists (ACLs) and Frame Relay on PT. KAI Palembang computer network. In this research used the Network Development Life Cycle (NDLC) method which has several stages, namely Analysis, Design, Simulation Prototyping, Implementation, Monitoring and Management. This research method is used because the results of this research will be displayed in the Cisco packet tracer simulator. In addition, the results of this research were tested using a ping test between computers to show that the ACLs design had been running well.

Keywords: Network, ACLs, NDLC, Cisco Packet Tracer, ping test

1. Introduction

PT. KAI Palembang is an Indonesian state-owned enterprise located in South Sumatra Province, which provides rail transportation services for both passengers and goods. PT. KAI Palembang has a computer network that was connected to the PT. KAI Persero central computer network located in Jakarta, where the two networks were connected using a router device. A router is a device that will pass IP packets from a network to another network using the addressing and certain protocol method to pass that data packet [1]. IP packets contains IP Address which is a series of binary numbers between 32-bit to 128-bit which is used as the identification address for each host computer on the internet network [2]. Router have function to connect many small networks to a larger network and are called internetwork with TCP / IP technology-based to expand from LAN to WAN and MAN, router also used to connect networks that use different media [3]. Routing needs to be done to the router device so that it can be used, where routing is the process of directing data packets to get the destination from one location to another [4]. To do the routing process, a routing protocol is needed, where the routing protocol is the protocol used in dynamic routing and allows routers to share information about networks and connections between routers [5]. In this research, Enhanced Interior Gateway Routing Protocol (EIGRP) is used, which is a cisco routing protocol that works on cisco routers and on internal route processors that found on layer core switches and cisco distribution layer switches and EIGRP is also a classes and enhanced distance vector protocol [6]. In addition, also need a switch device which have function as a link between the computer network of rooms were located in PT. KAI Palembang. A switch commonly called a smart hub was used to connect between one computer and another computer in a LAN [7].
The problem that occurs in this research is the lower levels of network security, so it is necessary to make efforts to improve computer network security by limiting user access to communication between networks on the PT. KAI Palembang computer network. Therefore, in this research, do the application of Access Control List (ACLs) and Frame Relay on the PT. KAI Palembang computer network. ACLs are a list of licensing or rejection statements that are applied to network addresses or the uppermost protocol layer and ACLs also used to select packets that go in and out of the network [8] while Frame relay is a technology that relies on frame-frame that is forwarded to send data [9], where Frame is a packet data [10]. In order to implement both of these technologies, so necessary to build a Virtual Local Area Network (VLAN) by utilizing router and switch, where VLAN are logical groupings of users and network resources that are connected to determined ports on a switch administratively [11]. VLAN is an option because it regulate networks based on their classification techniques, namely through MAC addressing, ports and so on that make flexible VLAN networks [12]. The entire research was carried out using a Cisco packet tracer simulator, where cisco packet tracer is a simulator of network tools issued by cisco that often used as a medium of learning and training and also often used in computer network simulation research fields [13]. The main purpose of the cisco packet tracer is to provide tools for participants and instructors to be able to understand the principles of computer networking and also build skills in the network configuration field that use cisco [13].

2. Research Methods

The research method used in the current research is the Action Research method wherein this method is described, interpreted and explained a condition at the same time in order to make changes or interventions with the aim of improvement and participation [14]. The following in Figure 1 are the stages of the action research method used:

![METODE ACTION RESEARCH](image)

**Figure 1.** Action Research Method [15]

3. Result and Discussion

3.1. Network Topology Design of PT. KAI Palembang

In Figure 2, below is the result of a topology design that researcher have designed on PT. KAI Palembang computer network, where the researcher added 2 routers and implemented a star-
bus topology with the aim that there were alternative paths could be used if the main line was cut off. The following picture below is the Network Topology that designed using the Cisco packet tracer simulator.

![Network Topology Design in PT. KAI Palembang.](image)

3.2. Virtual Local Area Network (VLAN) mapping

Virtual Local Area Network (VLAN) is a network that connect the same network although different locations with configuration in switch device using the trunking method, the switch is connected with a router to connect a predetermined VLAN network [16]. VLAN mapping is done to ease the Frame Relay configuration and VLAN also divide the device into several rooms based on their functions. The following table below is the VLAN mapping that used in this research:

<table>
<thead>
<tr>
<th>No.</th>
<th>Rooms</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IT and Service Room</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>Safety Room</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Financial and Billing Room</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>Documentation Room</td>
<td>40</td>
</tr>
<tr>
<td>5</td>
<td>Rail and Bridges Room</td>
<td>50</td>
</tr>
<tr>
<td>6</td>
<td>HR and General Room</td>
<td>60</td>
</tr>
</tbody>
</table>
3.3. IP Address Scheme in PT. KAI Palembang
To be able to communicate on a private network or on the internet public network every host on the computer network must be identified by an IP address

<table>
<thead>
<tr>
<th>No.</th>
<th>Rooms</th>
<th>Network address</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IT and Service Room</td>
<td>192.168.1.0/28</td>
<td>192.168.1.2</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.168.1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Safety Room</td>
<td>192.168.2.0/28</td>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.168.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Financial and Billing Room</td>
<td>192.168.6.0/28</td>
<td>192.168.6.2</td>
<td>255.255.255.0</td>
<td>192.168.6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.168.6.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Documentation Room</td>
<td>192.168.5.0/28</td>
<td>192.168.5.2</td>
<td>255.255.255.0</td>
<td>192.168.5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.168.5.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Rail and Bridges Room</td>
<td>192.168.3.0/28</td>
<td>192.168.3.2</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.168.3.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>HR and General Room</td>
<td>192.168.4.0/28</td>
<td>192.168.4.2</td>
<td>255.255.255.0</td>
<td>192.168.4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>192.168.4.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.4. ACLs design
The following table below is the access control list (ACLs) design that will be applied in this research:

<table>
<thead>
<tr>
<th>No.</th>
<th>Rooms</th>
<th>Cannot access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HR and General Room</td>
<td>IT Server</td>
</tr>
<tr>
<td>2</td>
<td>All rooms except the IT room</td>
<td>Internet (ISP)</td>
</tr>
<tr>
<td>3</td>
<td>Financial Room</td>
<td>IT Server</td>
</tr>
</tbody>
</table>

3.5. Frame Relay Design
The researcher designed frame relay from PT. KAI Palembang headed to PT. KAI Central in Jakarta. The researcher added a cloud as a media to connect of two networks with a WAN shell, where the design is as follows
Table 4. Frame Relay Design

<table>
<thead>
<tr>
<th>No.</th>
<th>Router</th>
<th>IP Address</th>
<th>DLCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Palembang</td>
<td>10.1.1.1/24</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>Jakarta</td>
<td>10.1.1.2/24</td>
<td>200</td>
</tr>
</tbody>
</table>

3.6. VLAN Configure on switch in the IT room

To give the identity of a VLAN or VLAN identity number is called a VLAN ID. Used to mark related VLAN, by configuring it as follows:

![IOS Command Line Interface](image)

3.6. VLAN Configure on switch in the IT room

To give the identity of a VLAN or VLAN identity number is called a VLAN ID. Used to mark related VLAN, by configuring it as follows:

1) Configure the access link interface to the PC

The interface configuration to the PC aim to access the VLAN ID that was created on the switch. Then to connect the interface using an access link command used to connect a computer with switch access links is a configured switch port.

Switch (config) #int fa0/2
Switch (config-if) #switchport access vlan 10
Switch (config-if) #switchport mode access
Switch (config) #int fa0 / 3
Switch (config-if) #switchport access vlan 20
Switch (config-if) #switchport mode access
Switch (config) #int fa0 / 4
Switch (config-if) #switchport access vlan 30
Switch (config-if) #switchport mode access
Switch (config-if) #int fa0 / 5
Switch (config-if) #switchport access vlan 40
Switch (config-if) #switchport mode access
Switch (config-if) #int fa0 / 6
Switch (config-if) #switchport access vlan 50
Switch (config-if) #switchport mode access
Switch (config-if) #int fa0/7
Switch (config-if) #switchport access vlan 60
Switch (config-if) #switchport mode access
Switch (config-if) #ex

2) Setting interconnection between VLAN

![IOS Command Line Interface]

**Figure 4.** Setting interconnection between VLAN
3.7. Frame Relay Configuration

Frame Relay have function for communication between branches of the company, for example the branch office PT. KAI Palembang wants to communicate with the PT. KAI central in Jakarta and the communication process become more simple.

1) Palembang Router Configuration

![Palembang Router Configuration](image)

**Figure 5. Palembang Router Configuration**

2) Jakarta Router Configuration

![Jakarta Router Configuration](image)

**Figure 6. Jakarta Router Configuration**
3) Cloud configuration

Cloud is a combination of the computer technology used (computing) in a network with internet-based development (cloud) that has a function to run programs or applications through connected computers at the same time, but not all are connected through the internet using cloud computing. This cloud-based computer is a technology that makes the internet the central server for managing data and user applications. This technology allows users to run programs without installation and allows users to access their personal data through computers with internet access. As well as the benefits of cloud in everyday life can store all data on the server centrally, data security, high flexibility and scalability and long-term investment.

a) Port to the Palembang Router

![Port to the Palembang Router](image1)

**Figure 7.** Port to the Palembang Router

b) Port to Jakarta Router

![Port to Jakarta Router](image2)

**Figure 8.** Port To the Jakarta Router
c) Connect frame relay from Palembang to Jakarta

![Figure 9. Frame Relay From Palembang to Jakarta](image)

### 3.8. EIGRP Routing Configuration

Each router that is in one domain has an identical database to each other, so that large network can be broken down into smaller areas and react very quickly to changes that occur on the network. Here is the configuration:

```plaintext
RouterPLB (config) #router eigrp 10
RouterPLB (config-router) #no auto-summary
RouterPLB (config-router) #network 192.168.1.0 0.0.0.255
RouterPLB (config-router) #network 192.168.2.0 0.0.0.255
RouterPLB (config-router) #network 192.168.3.0 0.0.0.255
RouterPLB (config-router) #network 192.168.4.0 0.0.0.255
RouterPLB (config-router) #network 192.168.5.0 0.0.0.255
RouterPLB (config-router) #network 192.168.6.0 0.0.0.255
RouterPLB (config-router) #network 100.10.1.0 0.0.0.255
RouterPLB (config-router) #network 10.10.10.0 0.0.0.255
RouterPLB (config-router) #network 20.20.20.0 0.0.0.255
RouterPLB (config-router) #end
RouterPLB # wr
```

1. Configure the EIGRP Router on the JKT Router
   - RouterJKT (config) #router eigrp 10
   - RouterJKT (config-router) #no auto-summary
   - RouterJKT (config-router) #network 20.20.20.0 0.0.0.255
   - RouterJKT (config-router) #end

2. Configuring the EIGRP Router on the ISP Router
   - RouterISP (config) #router eigrp 10
   - RouterISP (config-router) #no auto-summary
   - RouterISP (config-router) #network 10.10.10.0 0.0.0.255
   - RouterISP (config-router) #end

This testing phase is intended to find out whether the Access Control List (ACLs) configuration has been running properly according to the ACLs design table that has been presented previously. Following are some examples of ping test from several computer clients on the PT. KAI Palembang computer network:
3.9. Ping test from HR and General Room to Lampung Router
To be able to test the connection from HR and general room to the Lampung Router, the researcher ping the HR and general room client to the Lampung Router IP address: 101.11.10.2. The following results can be seen in the picture below.

![Ping test from HR and General Room to Lampung Router](image)

**Figure 10.** Ping test on HR and General Room to Lampung Router

3.10. Ping test from IT Room to an ISP Router (Internet).
To be able to test the connection from the IT room to the ISP, the researcher ping the IT Room client to the ISP IP address: 10.20.30.2. The following results can be seen in the picture below.

![Ping test from IT Room to an ISP Router (Internet)](image)

**Figure 11.** Ping test IT Room to an ISP Router (Internet)
3.11. Ping test from Financial Room to the Lampung Router
To be able to test the connection from the Financial room to the Lampung Router, the researcher ping the Financial room client to the Lampung Router IP address: 101.11.10.2. The following results can be seen in the picture below.

![Ping test Financial Room to the Lampung Router](image1)

Figure 12. Ping test Financial Room to the Lampung Router

3.12. Ping test from Documentation Room to the ISP Router (Internet)
To be able test the connection from Documentation Room to the ISP, the researcher ping the Documentation room client to the ISP IP address: 10.20.30.2. The following results can be seen in the picture below.

![Ping test Documentation Room to the ISP Router (Internet)](image2)

Figure 13. Ping test Documentation Room to the ISP Router (Internet)
3.13. Ping test from IT Room to the Billing Room

![Figure 14. Ping test IT Room to the Billing Room](image)

From the results of connection testing between several clients on the PT. KAI Palembang computer network that has been obtained above, it can be seen that the Access Control List (ACLs) configuration has run according to the ACLs design table (Table 3). Can be seen in table 5 below:

<table>
<thead>
<tr>
<th>No.</th>
<th>Testing</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ping test on HR and General Room to Lampung Router</td>
<td>not connected</td>
</tr>
<tr>
<td>2</td>
<td>Ping test IT Room to an ISP Router (Internet)</td>
<td>connected</td>
</tr>
<tr>
<td>3</td>
<td>Ping test Financial Room to the Lampung Router</td>
<td>not connected</td>
</tr>
<tr>
<td>4</td>
<td>Ping test Documentation Room to the ISP Router (Internet)</td>
<td>not connected</td>
</tr>
<tr>
<td>5</td>
<td>Ping test IT Room to the Billing Room</td>
<td>connected</td>
</tr>
</tbody>
</table>

4. Conclusion

This research use the Network Development Life Cycle (NDLC) method, where the NDLC method stages that have been carried out in this research are Analysis, Design and Simulation Prototyping so that the next stages such as Implementation, Monitoring and Management can be carried out by next researchers. From the final results of this research which the connection testing between several clients on PT. KAI Palembang computer network show that the
application of Access Control Lists (ACLs) can limit a user's access to communication, where only users who are registered in the users list database are permitted through ACLs configuration that can connect and communicate. That way, the results of this research can be used as a solution for the network security problems faced by PT. KAI Palembang.

References


