NETWORK PERFORMANCE OPTIMIZATION USING DYNAMIC ENHANCED INTERIOR ROUTING PROTOCOLS GATEWAY ROUTING PROTOCOL FOR IPv6 (EIGRPv6) AND IPv6 ACCESS CONTROL LIST

Mochamad Wahyudi, Syahril Efendi, Saib Suwilo, M. Safii

1,4) Doctoral Program, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara. Indonesia
2,3) Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Indonesia

mochamad.wahyudi@students.usu.ac.id, syahril1@usu.ac.id, saib@usu.ac.id, m.safii@students.usu.ac.id

Abstract Internet network needs are increasingly rapid in supporting current business needs. This goes hand in hand with requests for IP Address allocations for companies to measure information and business needs. The increasing demand for current IP Address allocation, the fewer the number of IP Addresses available. To fulfill the demand from the use of IP Address, Internet Protocol version 6 (IPv6) or internet protocol was adopted as the next-generation Internet technology. Exchange of IP Address in computer network cannot be separated from the existence of routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) also developed with the use of IPv6 to EIGRP for IPv6 (EIGRPv6). The EIGRPv6 routing concept is designed so well that it is capable of handling table routing that is very large and more efficient than the previous EIGRP. In large-scale computer networks must use good security. One method of network security is the Access Control List (ACL) capable of supporting the performance of IPv6. The application of ACL in this study is able to filter the access of network users by using IPv6 Extended ACL. Based on the results of EIGRPv6 network testing, the average packet delivery time is 7.6ms. And the application of IPv6 ACL is able to limit access to Web Servers, ICMP and FTP Servers properly.

Keywords: IPv6, IP Address version 6, EIGRP for IPv6, EIGRPv6, Access Control List, IPv6 ACL

I. Introduction

The use of internet access is a testament to the success of the information technology field. The development of the internet is very rapid, and makes everything turn into online based. This is also the main factor of the need to use the Internet Protocol Address (IP Address).

To fulfill the demand from the use of IP Address, Internet Protocol version 6 (IPv6) or internet protocol was adopted as the next-generation Internet technology. IPv6 is designed to use 128 bits that are designed beyond the allocation of IPv4 which only uses 32 bits. When viewed from the number of addresses held, IPv6 is able to support as many as 2128 hosts. Readiness to implement IPv6 technology in Indonesia is already at a serious stage, some preparations have been made to the stage of testing static routing and dynamic routing, DNS, web, mail, tunneling, access control lists and BGP [1].

In a computer network that has such heavy traffic, it is required to use several security support features from the network access. Among them are using routing to connect the number of users that are so large and provide security for filtering traffic, such as blocking internet traffic using the Access Control List (ACL). The purpose of this research is to obtain results from the use of Dynamic Enhanced Interior Gateway Routing Protocol (EIGRP) version 6 and the use of IPv6 Access Control List (ACL).
In the previous research, IPv4 extended access list was able to filter packets that passed through the network so that the application of permit and deny permissions can be carried out in accordance with the rules and scenarios designed [2].

II. Theoretical Review

2.1. Internet Protocol

IPv4 (Internet Protocol version 4) is a type of network addressing used in the TCP / IP network protocol that is only capable of addressing as many as 4 billion computer users [3]. The IPv6 protocol is an update protocol from the IPv4 protocol that is capable of using 128bit. Migrating from IPv4 to IPv6 in an instant is not possible due to its very large size and has a greater number than IPv4 [4].

![IPv6 Address](image1)

In Figure 1, the structure of IPv6 is explained which has Global Unicast, Multicast and Anycast. Writing IPv6 is the same as writing a MAC Address that uses Hexadecimal [5].

![Writing of IPv6](image2)

2.2 Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRPv6)

IPv4 routing performance decreases as the routing table size increases. The reason is checking the MTU header on each router and hop switch. The IPv6 routing process is far more efficient than its predecessor, IPv6 has the ability to manage large routing tables [11]. EIGRPv6 is a continuation of EIGRP IPv4 routing. There are different ways to enable EIGRPv6 routing, which is to add the command "ipv6 unicast-routing". Initially, Cisco only served EIGRP for IPv4, IPX and AppleTalk routes. EIGRP architecture easily adapts to Layer 3 protocol and IPv6 usage. How the EIGRPv6 routing protocol works uses a link-local address to find the next next-hop IP. EIGRPv6 is able to find IP Address neighbors even though the neighbors are different subnets [6].

![Network Scheme](image3)
EIGRP routing is Cisco proprietary, recently Cisco also published EIGRP as RFC [7]. If seen in Figure 3, it is explained that there are 3 routers that are connected to each other using EIGRPv6 dynamic routing.

### 2.3 Access Control List (ACL)

ACL is a package grouping based on categories. The use of ACL is very helpful in controlling network traffic [8]. The use of ACL can determine packet traffic on a computer network whether the package is blocked or forwarded to the destination. IPv6 Function ACL Standard is expanded to support filtering data packet traffic based on IPv6 usage. Writing IPv6 ACL if seen in Figure 4, by detailing the source and destination using keywords permit, deny, remark and other keywords [9].

#### Table 1

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td></td>
<td>53</td>
</tr>
<tr>
<td>tftp</td>
<td></td>
<td>69</td>
</tr>
<tr>
<td>ntp</td>
<td></td>
<td>123</td>
</tr>
<tr>
<td>radius account</td>
<td></td>
<td>1646 or 1813</td>
</tr>
<tr>
<td>radius auth</td>
<td></td>
<td>1645 or 1812</td>
</tr>
<tr>
<td>snmp</td>
<td></td>
<td>161</td>
</tr>
<tr>
<td>snmp-trap</td>
<td></td>
<td>162</td>
</tr>
<tr>
<td>syslog</td>
<td></td>
<td>514</td>
</tr>
<tr>
<td>ftp</td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>ftp-data</td>
<td></td>
<td>21</td>
</tr>
<tr>
<td>ssh</td>
<td></td>
<td>22</td>
</tr>
<tr>
<td>telnet</td>
<td></td>
<td>23</td>
</tr>
<tr>
<td>smtp</td>
<td></td>
<td>25</td>
</tr>
<tr>
<td>tasacs-ds</td>
<td></td>
<td>65</td>
</tr>
<tr>
<td>www</td>
<td></td>
<td>80</td>
</tr>
<tr>
<td>sftp</td>
<td></td>
<td>115</td>
</tr>
<tr>
<td>http</td>
<td></td>
<td>143</td>
</tr>
<tr>
<td>wbem-http</td>
<td></td>
<td>5988</td>
</tr>
<tr>
<td>wbem-https</td>
<td></td>
<td>5989</td>
</tr>
</tbody>
</table>
Errors in configuring the ACL can make the network down. For this reason, carefulness is needed in setting up the network to the network, host to network and host to host.

III. Research methods

This research uses Cisco Packet Trecer simulation software using Router 2911 / K9 with Cisco IOS version 15.1 and does not reduce specifications like the original router. In the EIGRP Protocol for IPv6 (EIGRPv6) Routing network and IPv6 ACL the author uses 3 routers which will be used to perform EIGRPv6 dynamic routing and use one server as the destination of ACL filtering.

IV. Research Results and Discussion

4.1 EIGRPv6 Configuration

4.1.1 Configuring EIGRPv6 R1

To enable EIGRPv6 routing against R1, you can use the command:

```
ipv6 unicast-routing
ipv6 router eigrp 1
eigrp router-id 1.1.1.1
no shutdown
```

While the commands used to implement EIGRPv6 routing into the interface can use the command:

```
interface GigabitEthernet0/0
ipv6 eigrp 1

interface GigabitEthernet0/1
ipv6 eigrp 1
interface GigabitEthernet0/2
ipv6 eigrp 1
```

4.1.2 Configuration R2

To enable EIGRPv6 on R2 you can use the command:

```
ipv6 unicast-routing
```

Table 2

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv6</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>G0/0</td>
<td>2001:0db8:11:1/64</td>
<td>FEC0:1</td>
</tr>
<tr>
<td></td>
<td>G0/1</td>
<td>2001:0db8:11:1/64</td>
<td>FEC0:1</td>
</tr>
<tr>
<td></td>
<td>G0/2</td>
<td>2001:0db8:11:1/64</td>
<td>FEC0:1</td>
</tr>
<tr>
<td>R2</td>
<td>G0/0</td>
<td>2001:0db8:11:1/64</td>
<td>FEC0:2</td>
</tr>
<tr>
<td></td>
<td>G0/1</td>
<td>2001:0db8:11:1/64</td>
<td>FEC0:2</td>
</tr>
<tr>
<td>R3</td>
<td>G0/0</td>
<td>2001:0db8:11:1/64</td>
<td>FEC0:3</td>
</tr>
<tr>
<td></td>
<td>G0/1</td>
<td>2001:0db8:11:1/64</td>
<td>FEC0:3</td>
</tr>
<tr>
<td>PC1</td>
<td>NIC</td>
<td>2001:0db8:10:1/64</td>
<td>FEC0:1</td>
</tr>
<tr>
<td>PC2</td>
<td>NIC</td>
<td>2001:0db8:10:1/64</td>
<td>FEC0:1</td>
</tr>
<tr>
<td>PC3</td>
<td>NIC</td>
<td>2001:0db8:10:1/64</td>
<td>FEC0:1</td>
</tr>
<tr>
<td>PC4</td>
<td>NIC</td>
<td>2001:0db8:10:1/64</td>
<td>FEC0:1</td>
</tr>
<tr>
<td>SERVER</td>
<td>NIC</td>
<td>2001:0db8:10:30:30</td>
<td>FEC0:3</td>
</tr>
</tbody>
</table>
ipv6 router eigrp 1
eigrp router-id 2.2.2.2
no shutdown
!
interface GigabitEthernet0/0
 ipv6 eigrp 1
interface GigabitEthernet0/1
 ipv6 eigrp 1

4.1.3 Configuring R3
The routing configuration used for R3 is not much different from the routing configuration used in R1 and R2.

ipv6 unicast-routing
ipv6 router eigrp 1
eigrp router-id 2.2.2.2
no shutdown
!
interface GigabitEthernet0/0
 ipv6 eigrp 1
interface GigabitEthernet0/1
 ipv6 eigrp 1

4.2 EIGRPv6 Connectivity Test
4.2.1 Routing Table
The Routing Table can be used to monitor IPv6 routes. If you look at figure 5, picture 6, and picture 7, there are codes with the initials "D" that mean EIGRP.

R1 # sh ipv6 route

    IPv6 Routing Table - 3 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
D - Direct, O - OSPF intra, O* - OSPF inter, O1 - OSPF ext 1, O2 - OSPF ext 2
O9 - OSPF NSSA ext 1, O11 - OSPF NSSA ext 2
O2 - BGP, E2 - EIGRP external
C 2001:0db8:1::/64 [90]
   via GigabitEthernet0/0, directly connected
L 2001:0db8:1::1/128 [0/0]
   via GigabitEthernet0/0, directly connected
   2001:0db8:1:2::/64 [90/0]
   via GigabitEthernet0/0, directly connected
   2001:0db8:1::1/128 [0/0]
   via GigabitEthernet0/0, directly connected
C 2001:0db8:1:3:/64 [90/0]
   via GigabitEthernet0/0, directly connected
L 2001:0db8:1:4::1/128 [0/0]
   via GigabitEthernet0/0, receive
C 2001:0db8:1::1/128 [0/0]
   via GigabitEthernet0/0, receive
L 2001:0db8:1:2::1/128 [0/0]
   via GigabitEthernet0/0, receive
L 2001:0db8:1:3::1/128 [0/0]
   via GigabitEthernet0/0, receive
L 2001:0db8:1:4::1/128 [0/0]
   via GigabitEthernet0/0, receive

Figure 5. R1 Routing Table

R2 # sh ipv6 route
4.2.2 ICMP Connectivity Test

Testing can be done by sending ICMP packets from PC1, PC2, PC3, and PC4 to the Server shown in Figure 8.

The next test is sending an ICMP packet from IPv6: 2001: DB8: 1: 10 :: / 64 heading to IPv6: 2001: DB8: 1 :: 30 :: / 64. Tests were carried out in five packages to get the average time needed for transferring data packages. The results obtained from the test can be seen in Figure 9.

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>MINIMUM</th>
<th>MAXIMUM</th>
<th>AVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8:1:10::/64</td>
<td>2001:DB8:1:30::/64</td>
<td>1ms</td>
<td>25ms</td>
<td>14ms</td>
</tr>
<tr>
<td>12ms</td>
<td></td>
<td></td>
<td>24ms</td>
<td>15ms</td>
</tr>
<tr>
<td>0ms</td>
<td></td>
<td></td>
<td>1ms</td>
<td>0ms</td>
</tr>
<tr>
<td>0ms</td>
<td></td>
<td></td>
<td>0ms</td>
<td>0ms</td>
</tr>
<tr>
<td>0ms</td>
<td></td>
<td></td>
<td>13ms</td>
<td>9ms</td>
</tr>
</tbody>
</table>

Figure 9. ICMP Package Delivery

4.3 HTTP ACL Block Configuration

In this first scenario we will limit access to the web server. Web servers can only be accessed from the local network if connected using interface g0 / 2 on the R1 interface (2001: DB8: 1: 11 :: 1/64) or can only be accessed via PC3 and PC4 according to Figure 3. The client is connected to networks outside the g0 / 2 interface cannot be connected to the web server. The following is the configuration of the ACL that is used to filter HTTP and HTTPS on R1:

```
ipv6 access-list BLOCK-HTTP
```
deny tcp any host 2001:DB8:1:30::30 eq www
deny tcp any host 2001:DB8:1:30::30 eq 443
permit ipv6 any any
!

After configuring the creation of IPv6 ACL, the next is registering an interface that is not permitted to communicate with the web server.

```plaintext
! interface GigabitEthernet0/1
tcp traffic-filter BLOCK-HTTP in
!
```

This command is used to limit access to interface g0/1 (PC1 and PC2) in communicating with the web server.

4.4 HTTP Block Connectivity Test

![HTTP filtering on PC2 (Deny)](image)

HTTP filtering is running as needed. If you look at Figure 10, PC2 cannot access the web server. Meanwhile, PC3 can access the web server shown in figure 11.

![ACL Permit](image)

4.5 Configuration of ICMP ACL Block

ICMP packet filtering is very important in the implementation of computer networks, using ACLs by blocking ICMP packets can avoid Denial-of-Service (DOS) attacks. To implement the ICMP packet block we use R3 or the router closest to the server, the following commands are used:

```plaintext
! ipv6 access-list BLOCK-ICMP
deny icmp any any
permit ipv6 any any
!
```
This command is used to activate the IPv6 ACL Block ICMP. Next is register the GigabitEthernet0 / 0 interface into the ACL.

```
interface GigabitEthernet0/0
  ipv6 traffic-filter BLOCK-ICMP out
```

**4.6 ICMP Block Connectivity Test**

If previously the client can communicate with sending ICMP data packets to the server in accordance with Figure 8. After the implementation of the ACL to perform ICMP filtering, all clients are confirmed to be unable to test connectivity using ping (ICMP) shown in figure 12.

![Figure 12. ICMP filtering](image)

**4.7 Configuration of ACL Block FTP**

Filtering access to FTP servers can be used to limit access from the client to transfer data. To restrict access to the FTP protocol, we use R1 by using the command:

```
ipv6 access-list BLOCK-FTP
  deny tcp any host 2001:DB8:1:30::30 eq 20
  deny tcp any host 2001:DB8:1:30::30 eq ftp
  permit ipv6 any any
```

```
interface GigabitEthernet0/2
  ipv6 traffic-filter BLOCK-FTP in
```

This configuration is used to block FTP protocol access on interface g0 / 2 which is connected to PC3 and PC4.

**4.8 ACL Block FTP Connectivity Test**

![Figure 13. FTP Permit (PC1)](image)

In Figure 13, it can be explained that PC1 can access FTP Server with the address 2001: DB8: 1: 30 :: 30. Whereas, PC3 with IPv6 Address 2001: DB8: 1: 11 :: 10 cannot access the FTP Server according to figure 14.
From the network security system implemented, PC1 and PC2 are only allowed to access FTP servers. While PC3 and PC4 are only given access to Web Servers.

V. Conclusion

1. The use of ACL can limit the access rights of clients who want to be connected to a computer network.
2. Using ACLs by blocking ICMP packets can avoid Denial-of-Service (DOS) attacks.
3. Network optimization using EIGRPv6 routing can be increased more specifically.

VI. Bibliography
