

[Home](#) > [About the Journal](#) > [Editorial Team](#)

Editorial Team

Editor-in-Chief:

[Dr. Imam Much Ibnu Subroto](#), Universitas Islam Sultan Agung, Indonesia

[Prof. Franco Frattolillo, Ph.D.](#), (Scopus h-index: 7) University of Sannio, Italy

Managing Editors:

[Dr. Arief Marwanto](#), Universitas Islam Sultan Agung, Indonesia

[Dr. Anton Yudhana](#), Universitas Ahmad Dahlan, Indonesia

Editors:

[Prof. Dr. Liu Xiaosheng](#), Harbin Institute of Technology, China

[Assoc. Prof. Dr. Tole Sutikno](#), (Scopus h-index: 8) Universitas Ahmad Dahlan, Indonesia

[Dr. GA Shaykhian, Ph.D.](#), University of Phoenix, United States

[Dr. Nabil Sultan](#), University Campus Suffolk, United Kingdom

[Dr. Sri Artini Dwi Prasetyowati](#), Universitas Islam Sultan Agung, Indonesia

[Dr. Reza Firsandaya Malik](#), Universitas Sriwijaya, Indonesia

[Dr. Robiah Ahmad](#), Universiti Teknologi Malaysia (UTM), Malaysia

[Dr. Xiao-Yang Liu](#), Shanghai Jiao Tong University, China

[Dr. Yuejin Li](#), Beijing Institute of Petrochemical Technology (BIPT), China

IMPORTANT PAGE

- [Author Guideline](#)
- [Article Template](#)
- [Editorial Boards](#)
- [Online Submissions](#)
- [Publication Ethics](#)
- [Visitor Statistics](#)
- [Contact Us](#)

USER

You are logged in as...
[rahmat_novrianda_d](#)

- [My Journals](#)
- [My Profile](#)
- [Log Out](#)

JOURNAL CONTENT

Search

All

[Search](#)

Browse

- [By Issue](#)
- [By Author](#)
- [By Title](#)
- [Other Journals](#)

INFORMATION

- [For Readers](#)
- [For Authors](#)
- [For Librarians](#)

Table of Contents

Articles

The Decision Support System of the selection of tourist attractions of Bali Island is used Preference method of Organization For Enrichment Evaluation

Eva Zuraidah

Classification of Muslim Woman Student Using Artificial neural network

Ulli Albab, Imam Much Ibnu Subroto, Muhammad Haddin

Fuzzy Logic Based Incubator Temp And Humid Level Controller Prototype

Kuat Supriyadi

The Layer 2 Network Security at SMK Negeri 1 Rantau Alai using DHCP Snooping

Rahmat Novrianda D, Rasmila Rasmila

SIMBOX Identification Using K-Nearest Neighbor Based On Spectrum Analyzer

Agung Suryowibowo, Imam Much Ibnu Subroto, Eka Nuryanto Budi Susila

JSON Implementation with Zlib Compression for Database Efficiency in Handling Dynamic Upload Multiple Images

Rianto Rianto, Alam Rahmatulloh, Iqbal Muhammad Fajar Nuralam

STATCOM Application for Reactive Power Compensation On Distribution of PLTMH Curug Muncar

Ghoni Musyahaer, Muhammad Haddin, Arief Marwanto

- Article Template
- Editorial Boards
- Online Submissions
- Publication Ethics
- Visitor Statistics
- Contact Us

USER

You are logged in as...

rahmat_novrianda_d

- My Journals
- My Profile
- Log Out

JOURNAL CONTENT

Search

All

Search

Browse

- By Issue
- By Author
- By Title
- Other Journals

INFORMATION

- For Readers
- For Authors
- For Librarians

Indexed by:



DOAJ DIRECTORY OF
OPEN ACCESS
JOURNALS

Home > Vol 8, No 1

Journal of Telematics and Informatics

Journal of Telematics and Informatics (e-ISSN: 2303-3703, p-ISSN: 2303-3711) is an interdisciplinary journal of original research and writing in the wide areas of telematics and informatics. The journal encompasses a variety of topics, including but not limited to: The technology of sending, receiving and storing information via telecommunication devices in conjunction with affecting control on remote objects; The integrated use of telecommunications and informatics; Global positioning system technology integrated with computers and mobile communications technology; The use of telematic systems within road vehicles, in which case the term vehicle telematics may be used; The structure, algorithms, behavior, and interactions of natural and artificial systems that store, process, access and communicate information; Develops its own conceptual and theoretical foundations and utilizes foundations developed in other fields; and The social, economic, political and cultural impacts and challenges of information technologies (advertising and the internet, alternative community networks, e-commerce, e-finance, e-governance, globalization and security, green computing, ICT for sustainable development, ICT in healthcare and education, management and policymaking, mobile and wireless communications, peer-to-peer learning, regulation of digital technologies, social networking, special user groups, the 2.0 paradigm, the WWW, etc).

The journal is a collaborative venture between Universitas Islam Sultan Agung (UNISSULA), Universitas Ahmad Dahlan (UAD) and Institute of Advanced Engineering and Science (IAES) Indonesia Section.



IMPORTANT PAGE

- Author Guideline
- Article Template
- Editorial Boards
- Online Submissions
- Publication Ethics
- Visitor Statistics
- Contact Us

USER

You are logged in as...
rahmat_novrianda_d

- My Journals
- My Profile
- Log Out

JOURNAL CONTENT

Search

All ▾

Search

Browse

- By Issue
- By Author
- By Title
- Other Journals

INFORMATION

- For Readers
- For Authors
- For Librarians

The Layer 2 Network Security at SMK Negeri 1 Rantau Alai using DHCP Snooping

Rahmat Novrianda.D, Rasmila

Universitas Bina Darma

Jenderal A. Yani street number 03, telp. (+62 711) 515679 / 515581 / 515582

e-mail: rahmat.novrianda.d@gmail.com

Abstract

SMK Negeri 1 Rantau Alai is located at Ogan Ilir Regency, South Sumatera Province. In this Vocational High School (SMK), there are two majors namely Computer and Network Engineering (TKJ) and Software Engineering (RPL). SMK Negeri 1 Rantau Alai already has a computer network that used to communicate all users for file sharing called Local Area Network (LAN). It has been connected to the internet, but does not have a network security system so it's very vulnerable to hacker intrusion who can do cyber crime. Therefore in this research, researcher built the network security on layer 2 Open System Interconnection (OSI) by utilizing DHCP Snooping technology to avoid cyber crime such as loss of important data from SMK Negeri 1 Rantau Alai database server. To implement DHCP Snooping, researcher need a routerboard Mikrotik device and also a switch that is one of hardware needed on the Data Link Layer. Besides that, Winbox and Putty software are also needed to help in the overall configuration of this research. The results obtained after DHCP snooping configuration done is the ability to recover IP address when converted to Fake IP will be able to return to its original IP address and limit the number of users who can access the internet at SMK 1 Rantau Alai

Keywords: LAN, DHCP Snooping, Switch, Winbox, Putty

1. Introduction

SMK Negeri 1 Rantau Alai is a school located in Rantau Alai, Ogan Ilir Regency, South Sumatra Province. As the only one of public vocational high school in Rantau Alai, there are 2 departments namely Computer and Network Engineering (TKJ) and Software Engineering (RPL). SMK Negeri 1 Rantau Alai also has a computer network called Local Area Network (LAN) and has been connected to the internet network. LAN is a group of computers, there are have several computer units as clients and one computer unit as a data bank or server [1]. SMK Negeri 1 Rantau Alai has problems with network security of important data owned by SMK Negeri 1 Rantau Alai which are susceptible to interference by irresponsible people or called cyber crime. This is be a problem for the school, because there is no authentication that limit permits only for registered users can access the internet of SMK Negeri 1 Rantau Alai, so that any users still connected to the internet network of SMK Negeri 1 Rantau Alai freely. Based on these problems, in this research will increase network security especially on Layer 2 Open System Interconnection (OSI). OSI is a communication standard between entities and consisting of seven layers. These seven layers have different roles and functions and each layer have specifically responsible for the data communication process [2]. Layer 2 OSI is the Data Link Layer that have function to packages data into related frames to hardware [3], then transport through the communication media with a network card, arranges physical layer communication between connection systems and error handling. The Data Link Layer have responsible for creating frames of grouping bits of data. Using MAC addresses for access to the last point, from error correction, flow control and hardware observation [4].

In this research, researcher used DHCP Snooping technology to improve LAN security of SMK Negeri 1 Rantau Alai, especially layer 2 OSI of computer network. Dynamic Host Configuration Protocol (DHCP) is a protocol in computer network that used to manage Internet Protocol (IP) addresses and other configurations such as subnet mask, gateway, which will be assigned to client computers centrally [5]. DHCP snooping is a series of techniques that are

applied to improve DHCP network security. When a DHCP server allocate an IP address to a client on the LAN, DHCP snooping can be configured on the LAN switch to allow only clients with a specific IP and MAC address to have access in the network. With DHCP snooping, information about the IP address and the corresponding MAC address is stored into the database on the switch device [6]. Switch is a simple device with function to connect multiple computers. Switches are identical to HUB, but switches are smarter and have higher performance than HUB [7].

In this research also requires Mikrotik routerboard device and 2 software such as Winbox and Putty to assist of overall configuration required for built DHCP snooping. DHCP snooping allows only those ports on switch to respond DHCP Requests which are configured for it. DHCP categorizes ports into trusted and untrusted ports [8]. Winbox is a utility used to remote the Mikrotik routerboard server in GUI (Graphical User Interface) mode [9] and Putty is a utility in CLI (Command Line Interface) mode which is a remote console / terminal software that used remote access to the computers and network devices using SSH, Telnet or serial [10].

2. Research Method

Explaining research chronological, including research design, research procedure (in the form of algorithms, Pseudocode or other), how to test and data acquisition [1], [3]. The description of the course of research should be supported references, so the explanation can be accepted scientifically [2], [4].

In this current research use the NDLC (Network Development Life Cycle) method, which is a approach in data communication using a cycles that have no beginning and ending for building a network [11]. This method have six stages, namely analysis, design, simulation prototyping, implementation, monitoring and management [12].

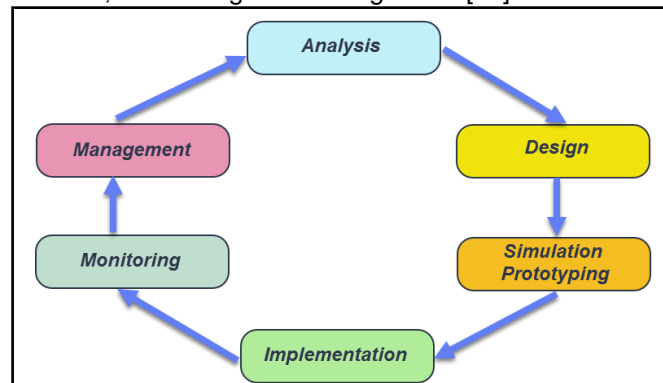


Figure 1. Network Development Life Cycle (NDLC) Method

- a. Analysis
In this stage, the researcher conducted a network topology survey and analysis of the problems at SMK Negeri 1 Rantau Alai and obtained information that SMK Negeri 1 Rantau Alai computer network was connected to the internet but did not have network security and user access limit.
- b. Design
Based on obtained data previously, the SMK Negeri 1 Rantau Alai network topology is designed using the existing network topology design application in this stage.
- c. Simulation Prototype
Simulation prototyping is used to test whether the overall configuration is successful or not. In this stage, configuration is performed on the Mikrotik routerboard and switch by utilizing Winbox and Putty software.
- d. Implementation
In this stage, the overall configuration that has been tested in the previous stage is applied to Mikrotik routerboard and switches device owned by SMK Negeri 1 Rantau Alai network computer.
- e. Monitoring
Monitoring is always carried out on the IP address of users who is connected to the SMK Negeri 1 Rantau Alai computer network. In addition, it also monitors the number of users who are connected to the internet actively.

f. Management

This stage is the last stage of NDLC method, management is carried out for maintenance, repair and development of the layer 2 network security at SMK Negeri 1 Rantau Alai.

3. Results and Analysis

3.1. Network Topology of SMK Negeri 1 Rantau Alai

Design of SMK Negeri 1 Rantau Alai network topology can be see on Fig. 2. with addition of several parts needed so that monitoring and maintenance process can be run optimally.

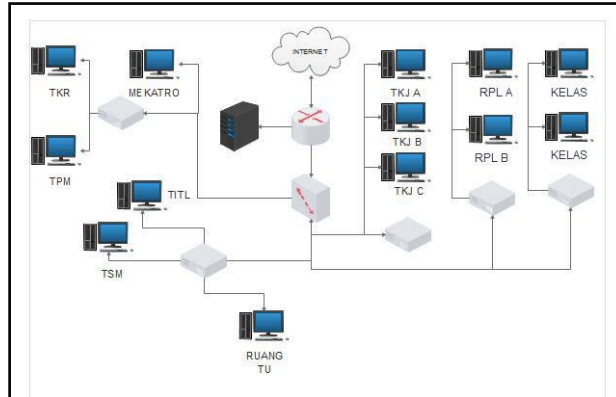


Figure 2. Network Topology of SMK Negeri 1 Rantau Alai

3.2. Configure Internet on Winbox

There are results of the DHCP Internet configuration steps on Mikrotik routerboard, i.e.:

- a. In Winbox software, select the Interfaces menu then enter the Internet name

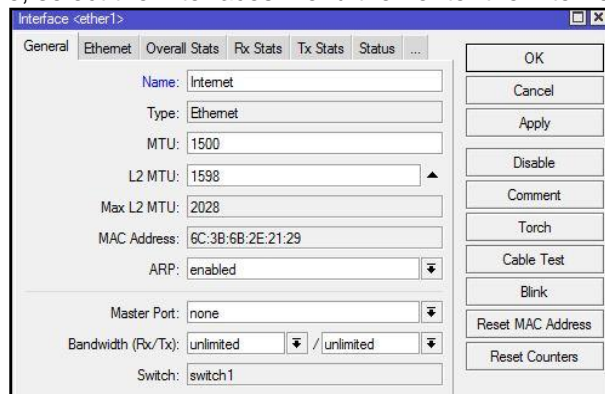


Figure 3. Making Internet Interfaces

- b. After that, select the IP menu then select Addresses, then the address list dialog box will appear and enter the IP address

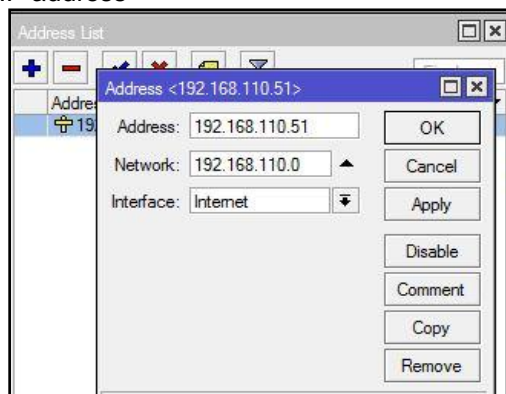


Figure 4. Enter an internet IP address

- c. Next, select the DNS settings, then configure the DNS servers.

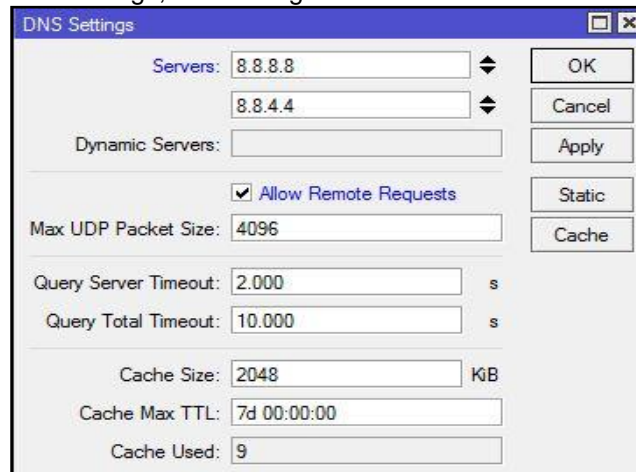


Figure 5. Configure the DNS servers

- d. In winbox software, select IP then Firewall and then NAT settings

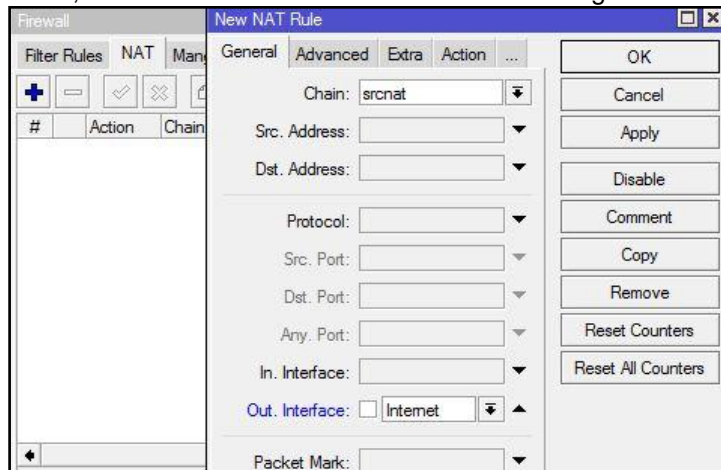


Figure 6. Choosing an Out Interface Internet

- e. Next, select out interface internet, select action and then select masquerade. After that press ok.

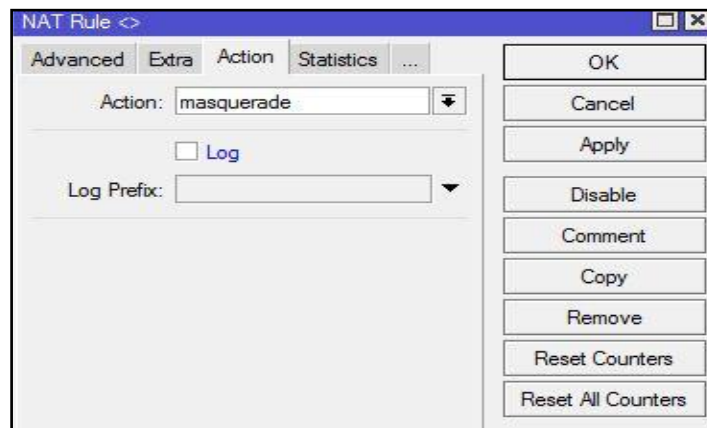


Figure 7. Determining masquerade on NAT rule

3.3. Configure the TKJ DHCP Server on Winbox

The steps was taken on the configuration of the TKJ DHCP server with Winbox software, i.e :

- a. In Winbox software, select the Interfaces menu then enter the TKJ name.

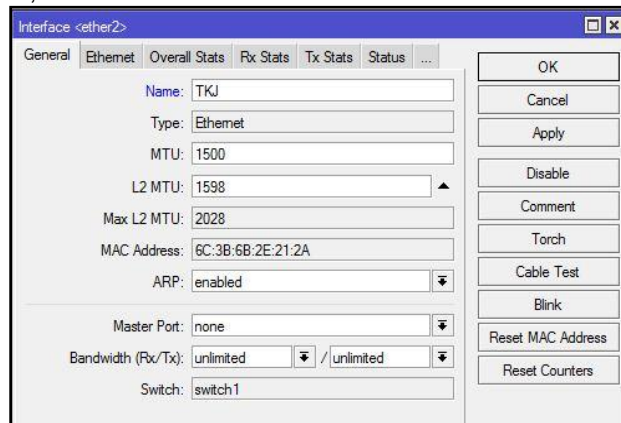


Figure 8. Creating TKJ interfaces

- b. After that, select the IP menu then select addresses and then the address list dialog box appear, so enter the IP address

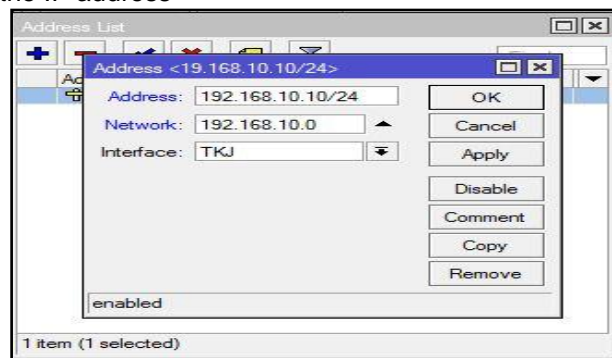


Figure 9. Enter the TKJ IP address

- c. Select winbox then select the IP menu and then choose DHCP server.
- d. After that, the DHCP server configuration dialog box appear. Select DHCP setup.
- e. Then, the DHCP setup dialog box appear, in this section select the interface that is connected to the TKJ.

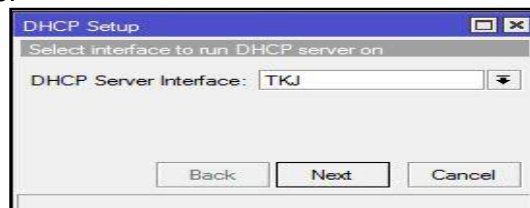


Figure 10. Choosing Ethernet to be used as a TKJ

- f. Next, give the IP address for the interface that is connected to the switch. After that, select the next button.

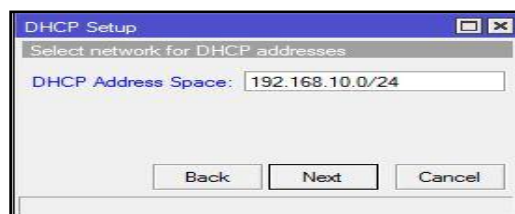


Figure 11. Determine the TKJ IP address

- g. After that, the address pool configuration appear. In this stage, determine the IP address range for TKJ A, TKJ B, and TKJ C. Then next

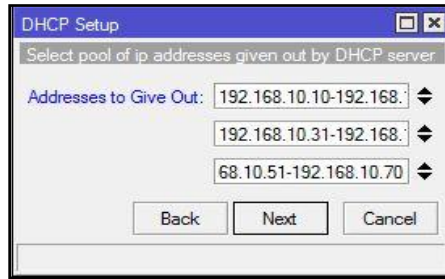


Figure 12. TKJ IP Pool Range

- h. Next, the DNS server configuration appear and then enter the DNS server. Then next.

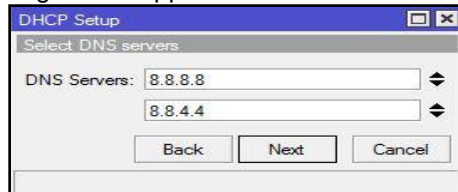


Figure 13. DNS server for TKJ

- i. After that, configure the SMTP Server IP, enter the specified lease time. Then next.

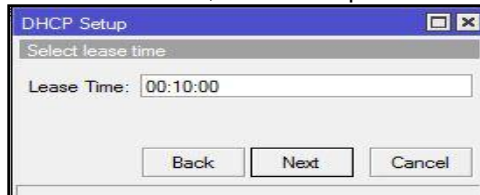


Figure 14. Determine the lease time for TKJ

- j. After creating the TKJ DHCP server IP on Winbox, researcher does a test to find out whether the DHCP IP was configured successfully.

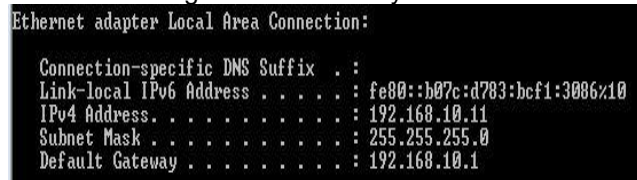


Figure 15. Testing TKJ DHCP server IP

3.4. Configure RPL DHCP Server in Winbox

The steps taken in configure the RPL DHCP server on Winbox are same as configure the TKJ DHCP server on Winbox above, but have different in the allocation of IP addresses, i.e.:

- a. In Winbox software, select the Interfaces menu then enter the RPL name.

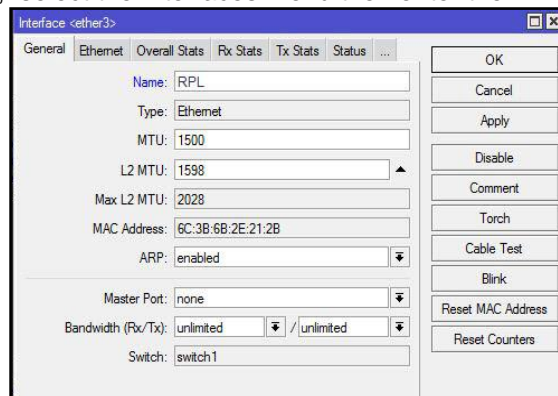


Figure 16. Creating RPL interfaces

- b. In winbox software, select the IP menu then select addresses
- c. Then the address list dialog box appear and then enter the IP address

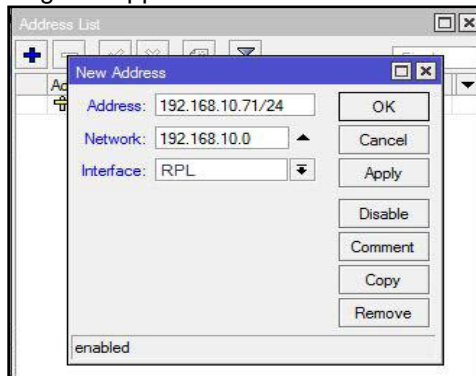


Figure 17. Enter the RPL IP address

- d. Below is the specified IP address for RPL

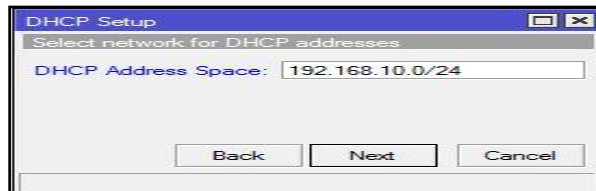


Figure 18. specifies the RPL IP address

- e. Different from TKJ, RPL only has RPL A and RPL B, so there are only 2 ranges of IP addresses.

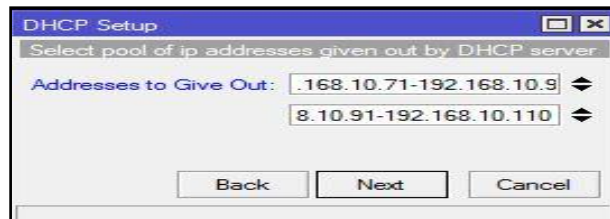


Figure 19. RPL IP Pool Range

- f. For the configuration of the DNS server and the SMTP server IP on RPL same as the configuration of TKJ. After all of RPL DHCP server IP configuration on Winbox has been done, researcher does a test to find out whether the DHCP IP was configured successfully.

```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . . :
Link-local IPv6 Address . . . . . : fe80::b07c:d783:bcf1:3086%10
IPv4 Address. . . . . : 192.168.10.72
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
```

Figure 20. Testing RPL DHCP server IP

3.5. Configure DHCP Snooping

After creating the DHCP server IP has been done, researcher configure DHCP snooping on the switch. By using VLAN 1, there are several used ports in configuration.

- a. Configure DHCP snooping trust, trust have function to secure the IP address to avoid from fake IP or attackers.

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int f0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#int f0/3
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ex
Switch(config)#
```

Figure 21. Configure DHCP Snooping Trust

```

C:\Users\CISCO>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1: The system cannot find the file specified.

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    IPv4 Address. . . . . : 192.168.10.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
  
```

Figure 22. DHCP Snooping Trust Result

- b. DHCP snooping limit rate configuration, limit rate have function to determine which number of users can enter the computer network.

```

Switch(config)#int f0/1
Switch(config-if)#ip dhcp sn
Switch(config-if)#ip dhcp snooping limit rate 4
  
```

Figure 23. DHCP Snooping Limit Rate Configuration

```

C:\Users\User>ipconfig /release

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media disconnected.
An error occurred while releasing interface Local Area Connection : An address has not yet been associated with the network endpoint.

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

C:\Users\User>ipconfig /renew

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media disconnected.
An error occurred while renewing interface Local Area Connection : unable to contact your DHCP server. Request has timed out.
An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.
  
```

Figure 24. DHCP Snooping Limit Rate Result

From Fig. 24. above, show the DHCP snooping limit rate result. Limit rate have function as a limitation of the user, if the user exceeds the limit rate capacity or offer of the user then the next user will be disconnected automatically from computer network.

3.6. DHCP Snooping Trust Testing

Researcher configure the TKJ network, port f0/1 is the LAN port of the router that is connected to the switch and port f0/2 is the TKJ port that is connected to the HUB.

```

Administrator: C:\Windows\system32\cmd.exe

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
IPv4 Address. . . . . : 192.168.10.23
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

tunnel adapter isatap.{83BF6489-C103-4C27-9771-8EBB205487A9}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
tunnel adapter Teredo Tunneling Pseudo-Interface:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\CISCO>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    Default Gateway . . . . . : 

tunnel adapter isatap.{83BF6489-C103-4C27-9771-8EBB205487A9}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
tunnel adapter Teredo Tunneling Pseudo-Interface:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\CISCO>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    IPv4 Address. . . . . : 10.10.10.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1
  
```

Figure 25. Show TKJ DHCP before trust

On Fig. 25., show the TKJ server IP address is 192.168.10.0/24 changes to fake IP 10.10.10.0/24. After configure DHCP snooping trust on TKJ network at port f0/1 and f0/2, then

do release and renew on command prompt to get a new DHCP, so fake IP changes back to the original TKJ IP address, i.e.:

```

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    IPv4 Address. . . . . : 10.10.10.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 

C:\Users\CISCO>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface
System cannot find the file specified.

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    Default Gateway . . . . . : 

Tunnel adapter isatap.{83BF6489-C103-4C27-9771-8EBB205487A9}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 

C:\Users\CISCO>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface
System cannot find the file specified.

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    IPv4 Address. . . . . : 192.168.10.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

```

Figure 26. TKJ DHCP renew after Result trust

After that, researcher also configure the RPL network, port f0/1 is the LAN port of the router that is connected to the switch and port f0/3 is RPL port that is connected to the HUB.

```

Connection-specific DNS Suffix . . . : 
Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
IPv4 Address. . . . . : 192.168.10.82
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

Tunnel adapter isatap.{83BF6489-C103-4C27-9771-8EBB205487A9}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 

C:\Users\CISCO>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface
System cannot find the file specified.

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    Default Gateway . . . . . : 

Tunnel adapter isatap.{83BF6489-C103-4C27-9771-8EBB205487A9}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : 

C:\Users\CISCO>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface
System cannot find the file specified.

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::d910:ecb1:8c87:26d6%11
    IPv4 Address. . . . . : 10.10.10.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1

```

Figure 27. Show RPL DHCP before trust

On Fig. 27. above, show the RPL server IP address is 192.168.10.0/24 changes to fake IP 10.10.10.0/24. After configure DHCP snooping trust on RPL network at port f0/1 and port f0/3, then release and renew on command prompt to get a new DHCP, so fake IP changes back to the original RPL server IP address as shown below:

```

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d910:ech1:8c87:26d6%11
IPv4 Address. . . . . : 192.168.10.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

Tunnel adapter isatap.{83BF6489-C103-4C27-9771-8EBB205487A9}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\CISCO>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface
System cannot find the file specified.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d910:ech1:8c87:26d6%11
IPv4 Address. . . . . :
Subnet Mask . . . . . :
Default Gateway . . . . . :

Tunnel adapter isatap.{83BF6489-C103-4C27-9771-8EBB205487A9}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\CISCO>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface
System cannot find the file specified.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d910:ech1:8c87:26d6%11
IPv4 Address. . . . . : 192.168.10.76
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

```

Figure 28. RPL DHCP renew result after trust

3.7. DHCP Snooping Limit Rate Testing

In this test, researcher configure the limit rate on port f0/1 which is the connecting port from switch to router. For example of this test is limited only for 4 users who can connect to the LAN of SMK Negeri 1 Rantau Alai. After configure the limit rate, then researcher does a test to see the obtained result after the limit rate configuration has been done, as shown below:

```

C:\Users\CISCO>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d910:ech1:8c87:26d6%11
IPv4 Address. . . . . : 192.168.10.82
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

```

Figure 29. DHCP on user 1

```

C:\Users\CISCO>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d910:ech1:8c87:26d6%11
IPv4 Address. . . . . : 192.168.10.76
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

```

Figure 30. DHCP on user 2

```

C:\Users\CISCO>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::a8f6:3977:f1b6:7a0b%11
IPv4 Address. . . . . : 192.168.10.73
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

```

Figure 31. DHCP on user 3

```
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::302f:77b3:149:5f2b%11
    IPv4 Address. . . . . : 192.168.10.74
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
```

Figure 32. DHCP on user 4

```
C:\Users\CISCO>ipconfig /renew

Windows IP Configuration

An error occurred while renewing interface Local Area Connection : unable to contact your DHCP server. Request has timed out.
An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.
```

Figure 33. DHCP on user 5

On Fig. 29, 30, 31 and 32 show that 4 users obtain DHCP IP, while on fig. 33 show that the 5th user cannot access to the computer network or not obtain a DHCP IP as a client. When the user or client exceeds the maximum limit as configured in the limit rate, then the new user connected to the router directly will be disconnected automatically

4. Conclusion

From the results of the research that has been done, researcher can be concluded that increasing network security can also be done on OSI layer 2, namely the Data Link Layer which associated with the switch device. The used security enhancement in this research is DHCP snooping technology, with done several configurations, then DHCP snooping trust can be built which serves to help restore the IP address that changed to Fake IP back to the original IP address. Furthermore, also built the DHCP snooping limit rate which useful to limit users who can connect to the SMK Negeri 1 Rantau Alai computer network. Therefore, the level of network security at SMK Negeri 1 Rantau Alai can be increase and can avoid interference from hackers or other irresponsible person

References

- [1] Nasution, Surya Darma. "Penerapan Metode Linier Kongruen dan Algoritma Vigenère Chiper Pada Aplikasi Sistem Ujian Berbasis LAN." *Pelita Informatika: Informasi dan Informatika* 4.1 (2013).
- [2] Lestaringati, Susmini I., and Fathur Rozak. "Pembangunan aplikasi monitoring jaringan berbasis web menggunakan simple network management protocol (SNMP)." *Majalah Ilmiah UNIKOM* 12.2 (2014).
- [3] Februariyanti, Hery. "Perancangan Pengindeks Kata pada Dokumen Teks menggunakan Aplikasi Berbasis Web." *Dinamik-Jurnal Teknologi Informasi* 18.2 (2013).
- [4] DITYA, KUSUMA ANGGAR. "Perancangan Jaringan Diskless Menggunakan Program CCBoot (Studi Kasus Pada Game Center PHDNET Semarang)." *Skripsi, Fakultas Ilmu Komputer*(2014).
- [5] Widodo, Triyogatama Wahyu, and Sigit Diantoro. "Auto-Configuration of Wireless Sensor Networks on Area Border Pole." *IJEIS (Indonesian Journal of Electronics and Instrumentation Systems)* 4.1 (2014): 79-90.
- [6] Tamsir Ariyadi, Tamsir. "Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN)." *Jurnal Sistem Komputer Musi Rawas (JUSIKOM)* 2.01 (2017): 28-36.

-
- [7] Permana, Agus Aan Jiwa. "Pengembangan Lab Komputer Sederhana Berbasis Jaringan Multipoint Menggunakan Switch Sebagai Sarana Penunjang Proses Pembelajaran." *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)* 3.2 (2014): 51-57.
- [8] Khan, Mohsin, Saleh Alshomrani, and Shahzad Qamar. "Investigation of DHCP packets using Wireshark." *International Journal of Computer Applications* 63.4 (2013).
- [9] Fitriastuti, Fatsyahrina, and Dodi Prasetyo Utomo. "Implementasi Bandwidth Management dan Firewall System Menggunakan Mikrotik OS 2.9. 27." *Jurnal Teknik4 4* (2014).
- [10] Taftazanie, Shofa, Agung Budi Prasetijo, and Eko Didik Widiyanto. "Aplikasi Pemantau Perangkat Jaringan Berbasis Web Menggunakan Protokol SNMP dan Notifikasi SMS." *Jurnal Teknologi dan Sistem Komputer* 5.2 (2017): 62-68.
- [11] Novrianda, Rahmat. "Rancang bangun keamanan jaringan wireless pada stiper sriwigama Palembang dengan radius server." *Jurnal Maklumatika* 4.1 (2017).
- [12] Novrianda, Rahmat. "Implementasi authentication Captive Portal pada Wireless Local Area Network PT. Rikku Mitra Sriwijaya." *Register: Jurnal Ilmiah Teknologi Sistem Informasi* 4.2 (2018): 67-80.