**RANCANGAN DAN IMPLEMENTASI SERTA PENGEMBANGAN JARINGAN UJI KOMPETENSI PAKET 4 DENGAN DNS OVER HTTPS, SIMPLE QUEUE DAN DNS BLOCKING**

**Laporan Ini Dibuat untuk**

**Memenuhi Persyaratan Kelulusan dari SMK Bina Informatika**



**Muhammad Fadhlan**

**20.14.2.051**

**Program Keahlian: Teknik Komputer dan Informatika**

**Kompetensi Keahlian: Teknik Komputer dan Jaringan**

**SMK BINA INFORMATIKA BINTARO**

***School of Information Technology and Art***

**2023**

# **DAFTAR ISI**

[**DAFTAR ISI** ii](#_Toc128721993)

[**DAFTAR BAGAN** iii](#_Toc128721994)

[**DAFTAR GAMBAR** iv](#_Toc128721995)

[**DAFTAR TABEL** vii](#_Toc128721996)

[**LEMBAR PENGESAHAAN** viii](#_Toc128721997)

[**KATA PENGANTAR** ix](#_Toc128721998)

[**BAB I PENDAHULUAN** 1](#_Toc128721999)

[**A.** **Latar Belakang** 1](#_Toc128722000)

[**B. Tujuan** 1](#_Toc128722001)

[**C. Manfaat** 2](#_Toc128722002)

[**BAB II PERANCANGAN** 3](#_Toc128722003)

[**A.** **Kerangka berfikir (*Flowchart*)** 3](#_Toc128722004)

[**B.** **Topologi Jaringan Lama** 4](#_Toc128722005)

[**C.** **Identifikasi Masalah** 5](#_Toc128722006)

[**D.** **Analisis Masalah** 5](#_Toc128722007)

[**E.** **Topologi Jaringan Baru** 6](#_Toc128722008)

[**F.** **Daftar Kebutuhan Komponen, *Software*, Bahan, dan Alat** 7](#_Toc128722009)

[**G. Penentuan *IP Address* dan *Interface*** 8](#_Toc128722010)

[**BAB III IMPLEMENTASI & UJI COBA** 9](#_Toc128722011)

[**A.** **Skenario Untuk Kerja** 9](#_Toc128722012)

[**B.** **Langkah pengerjaan** 9](#_Toc128722013)

[**C.** **Skenario Uji Coba** 28](#_Toc128722014)

[**D.** **Daftar Dokumen Pengujian Fungsi Jaringan** 28](#_Toc128722015)

[**BAB IV KESIMPULAN & SARAN** 32](#_Toc128722016)

[**A.** **Kesimpulan** 32](#_Toc128722017)

[**B.** **Saran** 32](#_Toc128722018)

[**DAFTAR PUSTAKA** 33](#_Toc128722019)

# **DAFTAR BAGAN**

Bagan 1: Flowchart kerangka berfikir......................................................................3

# **DAFTAR GAMBAR**

**Gambar 2.1**: Topologi Jaringan Lama....................................................................4

**Gambar 3.1**: Topologi jaringan dari perspektif *router*.............................................9

**Gambar 3.2**: DHCP Client pada ether1 untuk mendapatkan IP Address, DNS dan Gateway dari ISP....................................................................................................10

**Gambar 3.3**: DNS Settings pada Mikrotik.............................................................10

**Gambar 3.4**: DNS Static pada DNS settings..........................................................11

**Gambar 3.5**: Setting NTP Client di router.............................................................12

**Gambar 3.6**: System Clock....................................................................................12

**Gambar 3.7**: IP Address static yang terdefinisi dalam router................................13

**Gambar 3.8**: Konfigurasi firewall NAT.................................................................14

**Gambar 3.10**: Konfigurasi NAT Rule untuk Web Proxy untuk jaringan 192.168.100.0/25....................................................................................................14

**Gambar 3.11**: Konfigurasi NAT Rule untuk Web Proxy untuk jaringan 192.168.100.0/25....................................................................................................14

**Gambar 3.12**: Konfigurasi NAT Rule untuk Web Proxy untuk jaringan 192.168.200.0/24....................................................................................................15

**Gambar 3.13**: Konfigurasi NAT Rule untuk Web Proxy untuk jaringan 192.168.200.0/24....................................................................................................15

**Gambar 3.14**: Konfigurasi NAT Rule untuk DNS Blocking untuk jaringan 192.168.100.0/25....................................................................................................16

**Gambar 3.15**: Konfigurasi NAT Rule untuk DNS Blocking untuk jaringan 192.168.100.0/25....................................................................................................16

**Gambar 3.16**: Konfigurasi NAT Rule untuk DNS Blocking untuk jaringan 192.168.200.0/24....................................................................................................16

**Gambar 3.17**: Konfigurasi NAT Rule untuk DNS Blocking untuk jaringan 192.168.200.0/24....................................................................................................16

**Gambar 3.18**: Konfigurasi NAT Rule untuk jaringan 192.168.200.0/24...............17

**Gambar 3.19**: Konfigurasi NAT Rule untuk jaringan 192.168.200.0/24...............17

**Gambar 3.20**: Konfigurasi NAT Rule untuk jaringan 192.168.200.0/24...............17

**Gambar 3.21**: Konfigurasi NAT Rule untuk jaringan 192.168.100.0/25...............18

**Gambar 3.22**: Konfigurasi NAT Rule untuk jaringan 192.168.100.0/25...............18

**Gambar 3.23**: Konfigurasi Web Proxy untuk jaringan.........................................19

**Gambar 3.24**: Konfigurasi Web Proxy Access.....................................................19

**Gambar 3.25**: Konfigurasi DHCP Server.............................................................20

**Gambar 3.26**: Setting Firewall Rules pada router................................................22

**Gambar 3.27**: Setting Firewall Rules pada router untuk block ICMP 192.168.100.51 – 192.168.100.100 ke 192.168.200.0/24 dan log..........................22

**Gambar 3.28**: Setting Firewall Rules pada router untuk block ICMP 192.168.100.51 – 192.168.100.100 ke 192.168.200.0/24 dan log..........................22

**Gambar 3.29**: Setting Firewall Rules pada router untuk block ICMP 192.168.100.2 – 192.168.100.50 ke Gateway dan Log...................................................................23

**Gambar 3.30**: Setting Firewall Rules pada router untuk block ICMP 192.168.100.2 – 192.168.100.50 ke Gateway dan Log...................................................................23

**Gambar 3.31**: Setting Hotspot pada router...........................................................24

**Gambar 3.32**: User Manager pada router.............................................................25

**Gambar 3.33**: RADIUS Server konfig pada router................................................26

**Gambar 3.34**: Simple Queue pada router...............................................................27

**Gambar 3.35**: Setting SSID pada Access Point.....................................................28

**Gambar 3.36**: Gambar Sebelum dan Sesudah DNS Blocking...............................29

**Gambar 3.37**: Gambar Sebelum dan Sesudah DNS Blocking...............................29

**Gambar 3.38**: Gambar Sebelum dan Sesudah Simple Queue pada jaringan 192.168.100.0/25....................................................................................................30

**Gambar 3.39**: Gambar Sebelum dan Sesudah Simple Queue pada jaringan 192.168.100.0/25....................................................................................................30

**Gambar 3.40**: Gambar Sebelum dan Sesudah Simple Queue pada jaringan 192.168.200.0/24....................................................................................................30

**Gambar 3.41**: Gambar Sebelum dan Sesudah Simple *Queue* pada jaringan 192.168.200.0/24...................................................................*.................................*30

**Gambar 3.42**: Gambar Login Hotspot...................................................................31

**Gambar 3.43**: Gambar *Login Hotspot*..................................................................31

**Gambar 3.44**: Gambar RADIUS Active users.......................................................31

**Gambar 3.45**: Gambar Sebelum dan Sesudah DoH...............................................32

**Gambar 3.46**: Gambar Sebelum dan Sesudah DoH...............................................32

# **DAFTAR TABEL**

Tabel 2.1: Tabel Komponen, Software, Bahan dan Alat...........................................7

**LEMBAR PENGESAHAAN**

Nama Sekolah : SMK Bina Informatika Bintaro

Bidang Keahlian : Teknologi Informasi dan Komunikasi

Kompetensi Keahlian : Teknik Komputer dan Jaringan

Kode : 2145

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **2** | **0** | **1** | **4** | **2** | **0** | **5** | **1** |

Nomor Induk Siswa :

Nama Peserta : Muhammad Fadhlan

Judul : Rancangan Dan Implementasi serta

Pengembangan Jaringan Uji Kompetensi Paket 4 dengan *DNS over HTTPS*, *Simple Queue* dan *DNS Blocking*

# 

# **LEMBAR PENGESAHAAN**

|  |  |
| --- | --- |
| Menyetujui,  Guru Pembimbing  **Zaqi Kurniawan, S.Kom M.Kom**  NIK. 13.22.16.177 | Tangerang Selatan, 03 Maret 2023  Peserta Didik  **Muhammad Fadhlan**  NIS. 20.14.2.051 |
| Mengetahui,  Wakil Kepala Bidang Kependidikan  **Sinta Dewi, S.Pd., M.Kom.**  NIK. 13.07.01.002 | |

# **KATA PENGANTAR**

Puji syukur kita ucapkan kehadirat Tuhan Yang Maha Esa karena telah memberikan rahmat serta hidayah-Nya kepada kita semua sehingga berkatnya saya dapat menyelesaikan makalah tentang "Rancangan Dan Implementasi serta Pengembangan Jaringan Uji Kompetensi Paket 4 dengan *DNS over HTTPS*, *Simple Queue* dan *DNS Blocking*".

Dalam penyusunan makalah ini, tidak lupa mengucapkan terima kasih kepada semua pihak yang membantu proses pembuatan makalah ini sehingga dapat diselesaikan tepat pada waktunya.

Dalam penyusunan makalah ini saya berharap dapat bermanfaat bagi pembaca, serta menambah wawasannya, saya juga menyadari bahwa dalam penyusunan makalah ini masih terdapat kekurangannya, maka saya mengharapkan kritik dan masukan untuk memperbaiki penyusunan selanjutnya.

Penulis juga ingin mengucapkan terima kasih kepada pihak-pihak yang terkait dalam pembuatan penulisan laporan *Quality Plan* ini, yaitu sebagai berikut.

1. Bapak Esa Hergatama, M. Kom., selaku Kepala SMK Bina Informatika.
2. Ibu Sinta Dewi, S. Pd., M. Kom., selaku Wakil Kepala Sekolah Bidang Kependidikan.
3. Ibu Meta Mustika Sari, M. Pd., selaku Wakil Kepala Sekolah Bidang Pembinaan Peserta Didik.
4. Bapak Zaqi Kurniawan, S. Kom., M. Kom., selaku guru Pembimbing Penulisan Laporan.
5. Bapak Eko Supriyanto, S. Kom., M.M., selaku penguji sidang *Quality Plan*.

**BAB I**

**PENDAHULUAN**

# **BAB I PENDAHULUAN**

## **Latar Belakang**

Dalam dunia *digital* sekarang, sangat penting untuk setiap perusahaan sekarang untuk mempunyai kapabilitas kemampuan jaringan, salah satu nya itu mengamankan jaringan, meratakan pemakaian *bandwidth*, dan blokir *website malware*, semuanya bisa dilakukan dengan menggunakan peralatan seperti *DoH*, *Simple Queue*, dan *DNS Blocking*

*DoH* (*DNS over HTTPS*) adalah sebuah protokol untuk melakukan resolusi

Sistem Penamaan Domain (*DNS*) dengan menggunakan protokol *HTTPS*. Tujuan penggunaan metode ini adalah untuk melindungi privasi dan keamanan pengguna dengan mencegah serangan sadapan / *interception*.

*Simple queue* adalah salah satu fitur dari *RouterBOARD* yang bisa digunakan untuk membatasi penggunaan *bandwidth* pada suatu *network* jadi penggunaan *bandwidth* pada *network* itu rata dan *fair* pada suatu *network*.

*DNS Blocking* adalah suatu teknik yang bisa diartikan sebagai: memblokir

*website* menggunakan *DNS spoofing* (merubah request *DNS* di tengah perjalanan) agar *website* tertentu itu menuju halaman yang kita inginkan

## **B. Tujuan**

**B. Tujuan**

1. **Tujuan Penulisan Laporan**

Tujuan dari penulisan laporan ini antara lain :

1. Untuk memenuhi syarat kelulusan Ujian Kompetensi Kejuruan
2. Untuk meningkatkan kemampuan peserta didik menuangkan keahlian pengerjaan UKK dalam laporan

1

1. **Tujuan *QP***

Tujuan dilaksanakan *QP* antara lain :

1. Untuk membangun kemampuan *critical thinking* dan *problem solving* pada peserta didik
2. Untuk memperbaiki masalah dan mengimprovisasi design pada jaringan UKK.
3. **Tujuan Penambahan Layanan**

Tujuan ditambahkan layanan antara lain :

1. Untuk membuat jaringan lebih susah diretas dengan *DoH*
2. Untuk merata pemakaian *bandwith* pada jaringan dengan *Simple Queue*
3. Untuk membuat jaringan lebih mudah dikontrol dengan *DNS Blocking*

## **C. Manfaat**

**C. Manfaat**

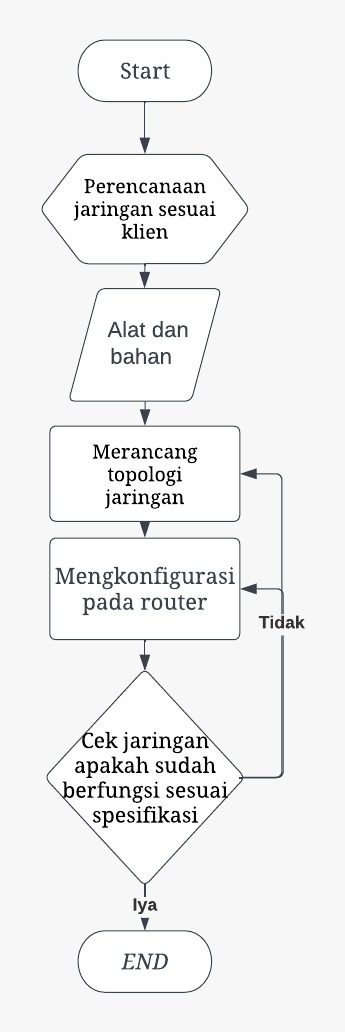
1. Setelah diperlakukan *DNS over HTTPS*, maka jaringan klien itu lebih aman atas manipulasi *website / phishing attack*
2. Setelah diperlakukan *Simple Queue*, maka penggunaan *bandwith* pada jaringan lebih rata dan lebih ideal, jadi satu orang tidak bisa menggambil semua *bandwith* pada jaringanya
3. Setelah diperlakukan *DNS Blocking*, maka pemblokiran *website* - *website* itu bisa dilakukan lebih efektif karena bisa diterapkan untuk *website* menggunakan *HTTPS*

**BAB II**

**PERANCANGAN**

# **BAB II PERANCANGAN**

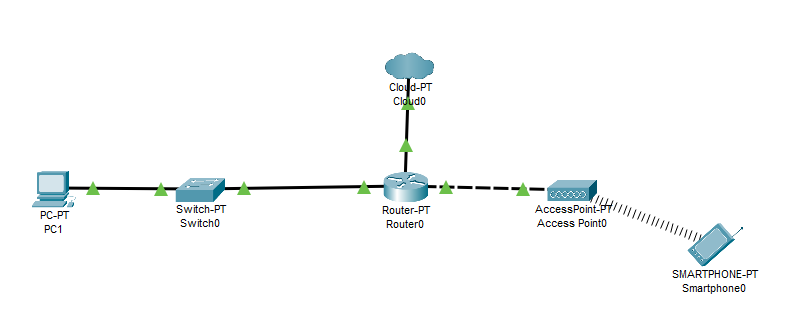
## **Kerangka berfikir (*Flowchart*)**



**Bagan 1: *Flowchart* kerangka berfikir**

3

## **Topologi Jaringan Lama**

**Gambar 2.1: Topologi jaringan lama**

1. Konfigurasi *Router*
2. *DNS* = Dari *ISP*
3. *NTP* = *enabled*
4. *Web Proxy* dan *Cache Administrator* = [muhammad\_fadhlan@smkbi.sch.id](mailto:muhammad_fadhlan@smkbi.sch.id)
5. Jaringan Internet

1. *IP Address* = Sesuai dengan *DHCP Server* dari *ISP*

2. *Gateway* =  Sesuai dengan *DHCP Server* dari *ISP*

1. Jaringan Lokal

1. *IP Address* = 192.168.100.1/25

2. *Network* = 192.168.100.0/25

3. *DHCP Pool* sebanyak 99 *Client*

4. Buat *firewall* agar IP 192.168.100.2-192.168.100.50 tidak dapat *ping* ke *router*

5. Buat *firewall* agar IP 192.168.100.51-192.168.100.100 tidak dapat *ping* ke *client wireless*

6. Buat *rule* agar setiap akses ke *router* tercatat di *logging* dan tersimpan di *disk*

1. Jaringan *Wireless*
   1. *IP Address* = 192.168.200.1/24
   2. *Network* = 192.168.200.0/24
   3. *SSID* = muhammad\_fadhlan@ProxyUKK
   4. *DHCP Pool* sebanyak 99 *client*
   5. 20 *account hotspot* secara *random* di *RADIUS*
   6. *User hotspot* hanya bisa menggunakan internet pada pukul 07.00 - 16.00 (menggunakan *Extra* -> *Time*)
2. Konfigurasi *Web Proxy*
   1. *Blocked host* = [www.linux.org](http://www.linux.org/)
   2. *Blocked path* = \*.mp3
   3. *Blocked path* = \*.mkv

## **Identifikasi Masalah**

1. *Request DNS* tidak terenkripsi
2. *Web proxy* tidak efektif untuk *block HTTPS*
3. Penggunaan *bandwidth* untuk setiap pengguna tidak dibatasi

## **Analisis Masalah**

1. Karena *request DNS* tidak terenkripsi ketika keluar dari *router* maka bisa disadap dan diubah oleh orang lain seperti *hacker* dan badan pemerintah seperti Kominfo, maka kita *enable DoH* dengan menggunakan *resolver* seperti https://8.8.8.8/dns-query
2. Karena *website* yang kita ingin *block* itu menggunakan *HTTPS*, maka tidak efektif hanya menggunakan *web proxy*, maka kita menambah *entry* ke *DNS Static*
3. Karena jaringan lokal dan *wireless* itu tidak dibatasi berapa banyak pemakaian *bandwidth* nya, maka satu perangkat bisa ambil semua *bandwith* dan meninggalkan hanya sedikit untuk perangkat lainya, maka kita menambahkan *Simple Queue* untuk membataskan penggunaan *bandwidth* perangkat

## **Topologi Jaringan Baru**

Semua konfigurasi baru itu adalah tambahan ke konfigurasi lama.

1. Konfigurasi *Router*
   1. *Setting DNS* di *Router*:
      1. *DoH Server URL*: https://8.8.8.8/dns-query
   2. *Simple Queue*
      1. 192.168.100.0/25
         1. Target 20 Mbps *Download*
         2. Target 8 Mbps *Upload*
      2. 192.168.200.0/24
         1. Target 25 Mbps *Download*
         2. Target 10 Mbps *Upload*
   3. *DHCP Server*
      1. 192.168.100.1/25
         1. *DNS Server* 192.168.100.1
      2. 192.168.200.1/24
         1. *DNS Server* 192.168.200.1
   4. *Firewall NAT*
      1. *Chain*: dstnat
         1. *Src Address*: 192.168.100.0/25
         2. *Protocol*: udp
         3. *dstport*: 53
         4. *Action*: netmap, *to address* 192.168.100.1 *port* 53
      2. *Chain*: dstnat
         1. *Src Address*: 192.168.200.0/24
         2. *Protocol*: udp
         3. *dstport*: 53
         4. *Action*: netmap, *to address* 192.168.200.1 *port* 53
   5. *DNS Static*
      1. linux.org = NXDOMAIN

## **Daftar Kebutuhan Komponen, *Software*, Bahan, dan Alat**

**Tabel 2.1: Tabel *Komponen*, *Software*, Bahan dan Alat**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Nama  Alat/Bahan/Komponen | Spesifikasi Minimal | Jumlah | Keterangan |
|  | Alat |  |  |  |
| 1 | *Crimping Tool* | Standar | 1 Buah | Untuk kabel *RJ45* |
| 2 | *Cable Tester* | Standar | 1 Buah | Untuk kabel *RJ45* |
|  | Komponen |  |  |  |
| 1 | *PC Client* | *CPU*: *Dual Core* i3-4170  *RAM*: 4GB  *Storage Non Removable*: 256GB  *NIC*: 100Mbps  *Monitor* 14’’ | 1 *unit* | Untuk pengujian jaringan lokal |
| 2 | *RouterBOARD* | hEX | 1 *unit* | Untuk *router* jaringan |
| 3 | *Switch Unmanageable* | 5 *port* | 1 *unit* | Agar bisa menghubungkan lebih dari 1 perangkat ke jaringan lokal |
| 4 | *Smartphone Client* | 2GB *RAM*  16GB *Storage internal* | 1 *unit* | Untuk pengujian jaringan *wireless* |
| 5 | *Access Point* | 100Mbps | 1 *unit* | Diperlukan karena *router*nya tidak mendukung *wireless* |
|  | Bahan |  |  |  |
| 1 | Kabel *UTP* | Cat 5e | 3 Meter |  |
| 2 | Konektor *RJ45* | Cat 5e | 8 Buah |  |
| 3 | Koneksi Internet | Tidak ada *login page*  50Mbps |  |  |
|  | *Software* |  |  |  |
| 1 | *Software* untuk *Router* | *RouterOS* versi 7 |  |  |
| 2 | *Software* untuk *PC Client* | *Browser*: *Firefox* / *Chrome*  OS: *Windows* 10 |  |  |
| 3 | *Software* untuk *Smartphone* | *OS*: *Android* atau *iOS* *Browser*: Chrome / Firefox |  |  |

## **G. Penentuan *IP Address* dan *Interface***

1. *Router*
   1. Ether1 (internet)
      1. *Ip address* = Sesuai dengan *DHCP Server* dari *ISP*
   2. Ether2 (jaringan lokal)
      1. *Ip address* = 192.168.100.1
      2. *Network* = 192.168.100.0/25
   3. Ether3 (jaringan *wireless*)
      1. *Ip address* = 192.168.200.1
      2. *Network* = 192.168.200.0/24
2. *PC*

*PC* terhubung ke jaringan lokal, jadi mendapatkan *IP* secara dinamis dari *router*

1. *Smartphone*

*Smartphone* terkoneksi ke jaringan *wireless*, jadi mendapatkan *IP* secara dinamis dari *router*

**BAB III**

**IMPLEMENTASI & UJI COBA**

# **BAB III IMPLEMENTASI & UJI COBA**

## **Skenario Untuk Kerja**

Di dalam kegiatan ini saya bertindak sebagai *Network* *system* *administrator*, yang mengatur dan mengkonfigurasi jaringannya berdasarkan permintaan dari klien dan melakukan modifikasi berdasarkan pencarian tentang teknologi yang membuat jaringan lebih baik.

## **Langkah pengerjaan**

1. Pemasangan kabel pada *port router*:



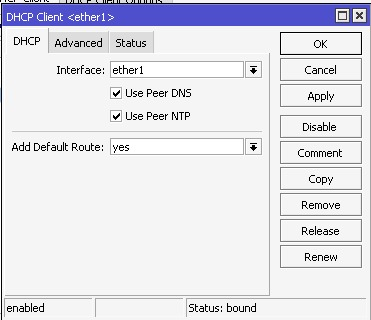
**Gambar 3.1: Topologi jaringan dari perspektif *router***

Berdasarkan perencanaan pada halaman sebelumnya, bisa ditentukan bahwa pada:

1. Ether1: Disambung ke sumber internet atau *ISP*
2. Ether2: Disambung ke *switch* jaringan lokal
3. Ether3: Disambung ke *access point*

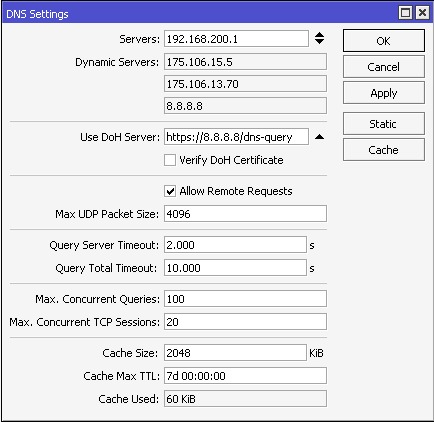
9

1. *Setting* *DNS* dan *DHCP client* pada *router*:



**Gambar 3.2: *DHCP Client* pada ether1 untuk mendapatkan**

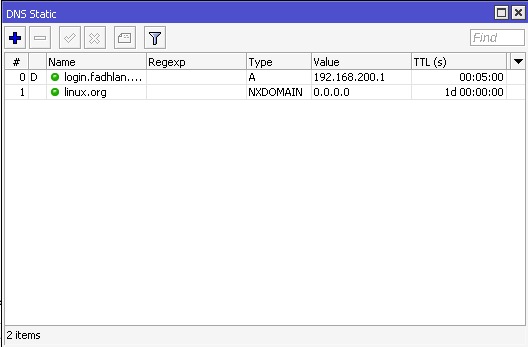
***IP Address*, *DNS* dan *Gateway* dari *ISP***



**Gambar 3.3: *DNS Settings* pada *Mikrotik***

Pada langkah ini, *DHCP Client* ditambahkan agar *router*nyamendapatkan *IP Address*, *DNS*, dan *Gateway* dari sumber internet */ ISP*.

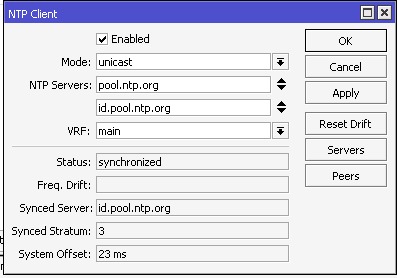
Setelah *DHCP Client* ditambah dan sudah *bound*, maka bisa lanjut ke langkah berikutnya yaitu megecek ketika *DNS server* sudah didapati, berada di *IP* → *DNS*, dan pada langkah ini, ditambah juga server *DoH* kita yaitu *Google*: <https://8.8.8.8/dns-query>



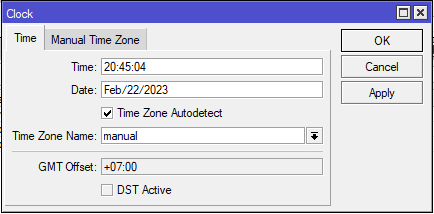
**Gambar 3.4*: DNS Static* pada *DNS settings***

Setelah konfigurasi *DHCP Client*, dilanjutkan dengan konfigurasi *DNS Static* untuk *blocking* *website*, bisa dikonfigurasi di *IP* → *DNS* → *Static*, dan kita *add domain / subdomain* yang akan di *block*. Dalam spesifikasi yang akan di block itu linux.org, jadi tekan add dan di Name itu linux.org dan Type itu NXDOMAIN.

1. *Setting* *NTP* pada *router*



**Gambar 3.5: *Setting NTP Client* di *router***

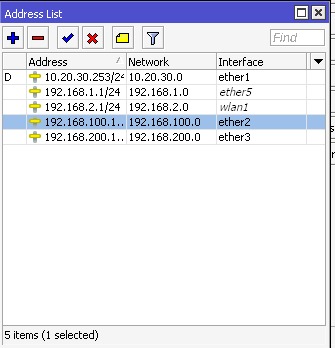
**Gambar 3.6:*****System Clock***

Pada langkah ini, *NTP Client* ditambahkan agar *router-*nya mendapatkan waktu akurat dari *server* jadi peraturan *Time* bekerja dengan benar.

Di *System* → *NTP Client* → *NTP Servers*, ditambah entry: pool.ntp.org dan id.pool.ntp.org, yaitu adalah *server NTP* yang *reliable* dan digunakan untuk sinkronisasi waktu pada perangkat.

Sebelum tekan *OK*, harus di cek dulu zona waktu pada *router*nya, bisa dilakukan di *System* → *Clock* → *Manual Time Zone* dan ditentukan berdasarkan posisi, untuk WIB itu +07:00, setelah konfigurasi itu tekan *OK* di Clock terus *NTP Client*.

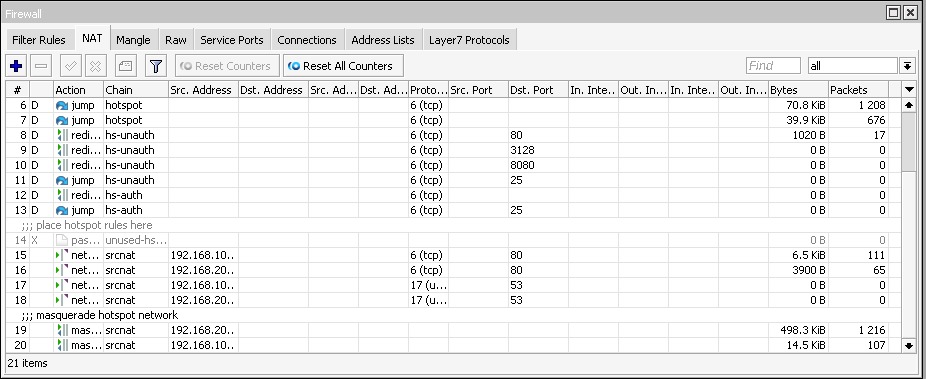
1. *Setting IP Static* di *router*



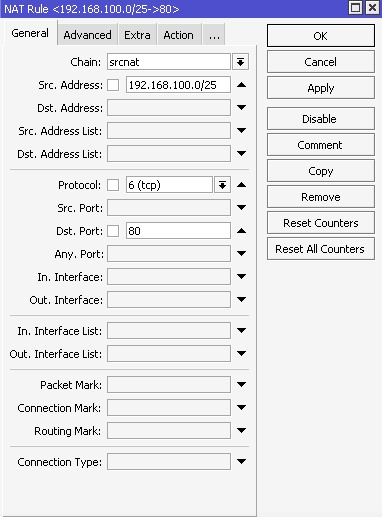
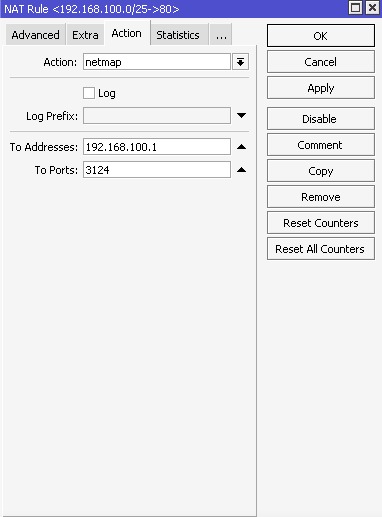
**Gambar 3.7: *IP Address static* yang terdefinisi dalam *router***

Pada langkah ini, *IP Address* dikonfigurasi di *router* berdasarkan perencanaan jaringan yaitu:

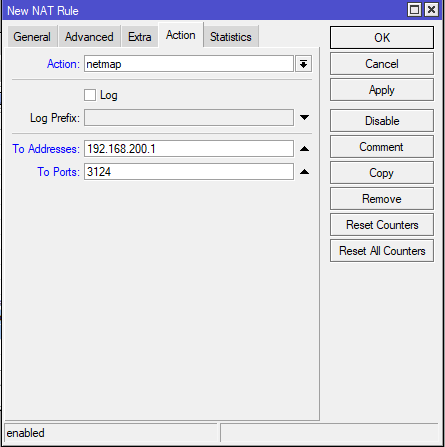
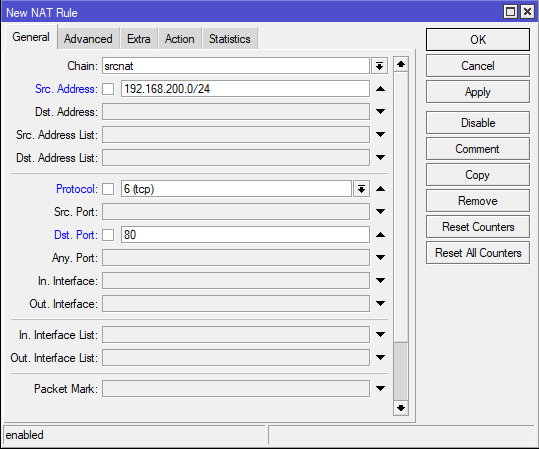
* 1. Ether1 (internet)
     1. *Ip address* = Sesuai dengan *DHCP Server* dari *ISP*
  2. Ether2 (jaringan lokal)
     1. *Ip address* = 192.168.100.1
     2. *Network* = 192.168.100.0/25
  3. Ether3 (jaringan *wireless*)
     1. *Ip address* = 192.168.200.1
     2. *Network* = 192.168.200.0/24

1. *Setting Web Proxy* dan *Firewall NAT* di *router*

**Gambar 3.8: Konfigurasi *firewall NAT***

**Gambar 3.10, 3.11: Konfigurasi *NAT Rule* untuk *Web Proxy* untuk jaringan 192.168.100.0/25**

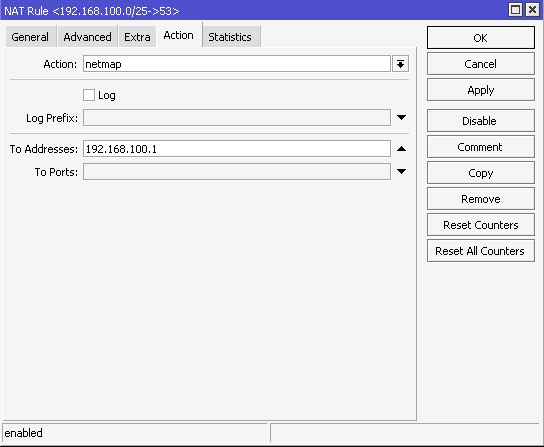
**

**Gambar 3.12, 3.13: Konfigurasi *NAT Rule* untuk *Web Proxy* untuk jaringan 192.168.200.0/24**

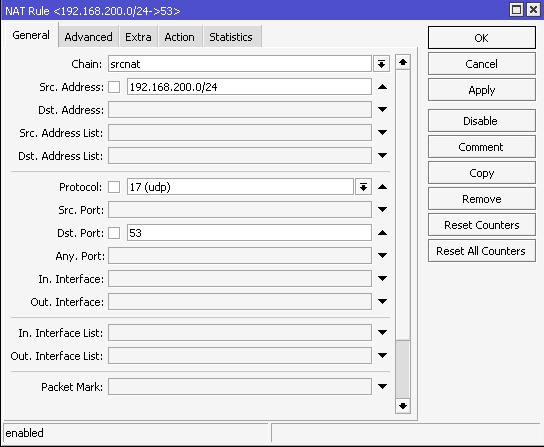
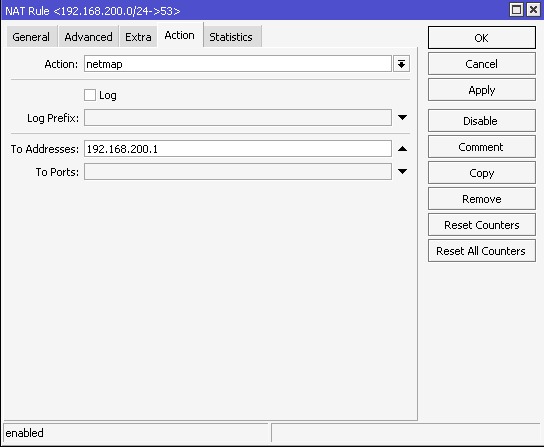
Pada langkah ini, ditambahkan peraturan *NAT* di *IP* → *Firewall* → *NAT*, agar *Web Proxy*, *DNS Blocking* dan Akses Internet bekerja.

Untuk *Web Proxy* ditambahkan dua *NAT rule* yaitu:

* + 1. *Chain*: dstnat
       1. *Src Address*: 192.168.100.0/25
       2. *Protocol*: *tcp*
       3. *dstport*: 80
       4. *Action*: netmap, *to address* 192.168.100.1 *port* 3124
    2. *Chain*: dstnat
       1. *Src Address*: 192.168.200.0/24
       2. *Protocol*: *tcp*
       3. *dstport:* 80
       4. *Action*: netmap, *to address* 192.168.200.1 port 3124

Untuk *DNS Blocking* ditambahkan *NAT rule* 2 juga yaitu:

**Gambar 3.14, 3.15 : Konfigurasi *NAT Rule* untuk *DNS Blocking* untuk jaringan 192.168.100.0/25**



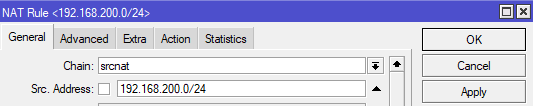
**Gambar 3.16, 3.17 : Konfigurasi *NAT Rule* untuk *DNS Blocking* untuk jaringan 192.168.200.0/24**

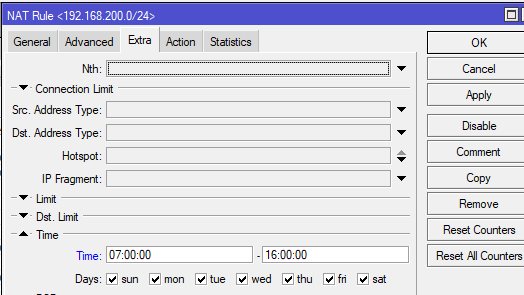
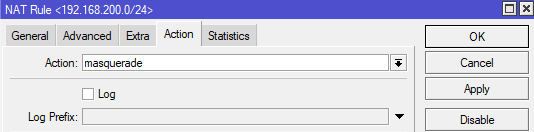
*NAT Rulenya* ditambahkan agar fitur *DNS Blocking* bekerja, karena *DNS Blocking* itu cara berfungsinya dengan *redirect* semua *DNS request* ke *gateway*

Untuk *DNS Blocking* ditambahkan dua *NAT rule* yaitu:

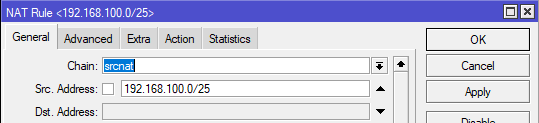
* + 1. *Chain*: dstnat
       1. *Src Address*: 192.168.100.0/25
       2. *Protocol*: *udp*
       3. *dstport*: 53
       4. *Action*: netmap, *to address* 192.168.100.1 port 53
    2. *Chain*: dstnat
       1. *Src Address*: 192.168.200.0/24
       2. *Protocol*: *udp*
       3. *dstport*: 53
       4. *Action*: netmap, *to address* 192.168.200.1 port 53

Setelah semua *NAT rule* ditambahkan, jaringan masih belum bisa berfungsi karena belum dibolehkan untuk akses internet, agar bisa akses Internetditambahkan *NAT rule* berikut:





**Gambar 3.18, 3.19, 3.20: Konfigurasi *NAT Rule* untuk jaringan 192.168.200.0/24**

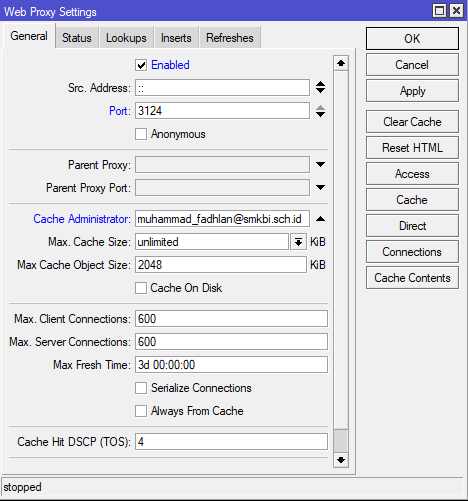
****

****

**Gambar 3.21, 3.22: Konfigurasi *NAT Rule* untuk jaringan 192.168.100.0/24**

* + 1. *Chain*: srcnat
       1. *Src Address*: 192.168.100.0/25
       2. *Action*: masquerade
    2. *Chain*: srcnat
       1. *Src Address*: 192.168.200.0/24
       2. *Time*: Semua hari, dari waktu 07:00:00 – 16:00:00
       3. *Action*: masquerade

Setelah semua *NAT rule* ditambahkan, dan *NAT Rule* untuk internetditambahkan, maka dilanjutkan untuk konfigurasi *Web Proxy*, yang berada di *IP* → *Web Proxy:*

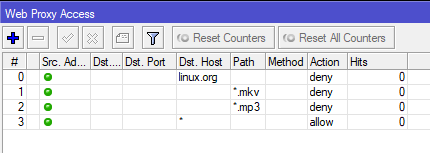


**Gambar 3.23: Konfigurasi *Web Proxy* untuk jaringan**

*Web proxy* untuk memblokir *website HTTP*, dan dikonfigurasi sebagai berikut:

* + 1. *Enabled*:
    2. *Port:* 3124
    3. *Cache Administrator*: [muhammad\_fadhlan@smkbi.sch.id](mailto:muhammad_fadhlan@smkbi.sch.id)

Setelah konfigurasi berikut, dilanjutkan dengan *Access*, dan didalam sini, dimasukkan semua *website* yang akan di *block*:

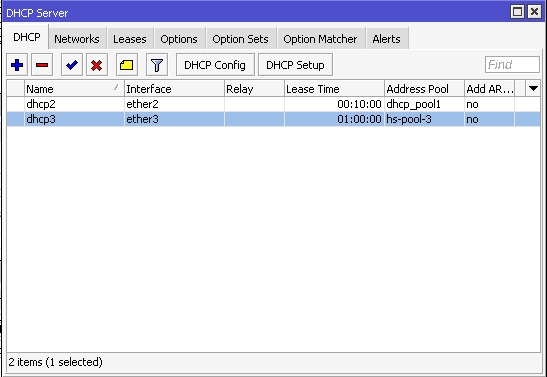


**Gambar 3.24: Konfigurasi *Web Proxy Access***

* + 1. *Dst Host*: linux.org
       1. *Action*: deny
    2. *Dst Host*: kosong
       1. *Path*: \*.mkv
       2. *Action*: deny
    3. *Dst Host*: kosong
       1. *Path*: \*.mp3
       2. *Action*: deny
    4. *Dst Host*: \*
       1. *Action*: allow

Setelah dikonfigurasi *Web Proxy Access*, dan *Web Proxy*, tekan *OK* pada *Web Proxy*.

1. *Setting DHCP Server* pada *Router*

****

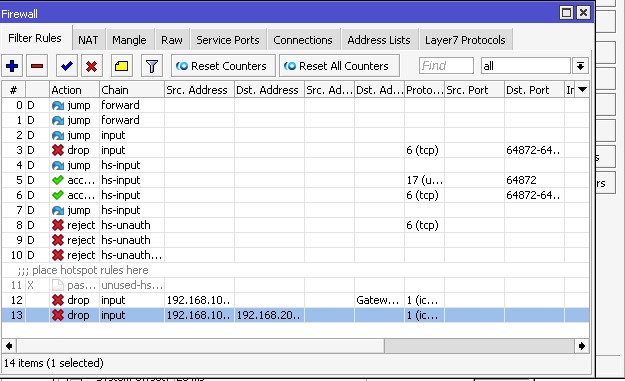
**Gambar 3.25: Konfigurasi *DHCP Server***

*DHCP Server* itu penting agar setiap klien di jaringan mendapatkan *IP Address* secara otomatis, dan tidak perlu konfigurasi secara manual semua perangkat pada jaringanya

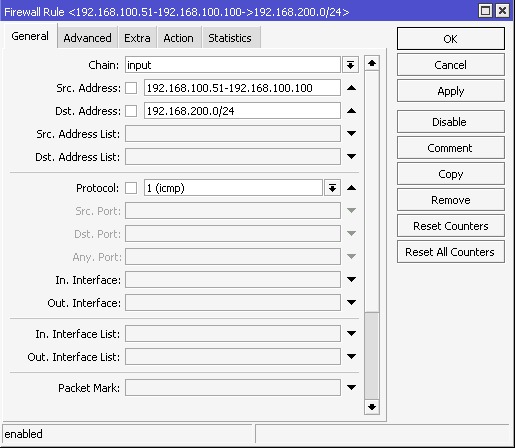
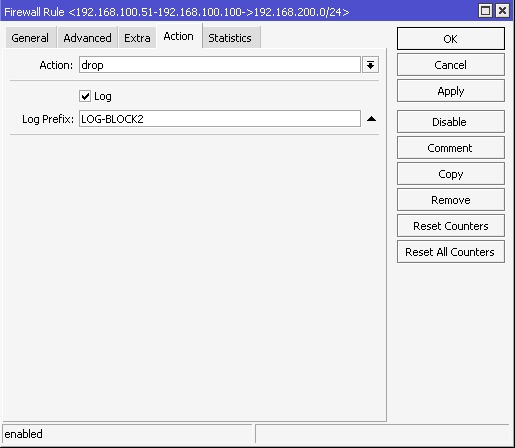
Pada langkah ini, *DHCP Server* dikonfigurasi menggunakan *DHCP Setup*:

* + 1. Ether2
       1. *DHCP Address Space*: 192.168.100.0/25
       2. *Gateway for DHCP Network*: 192.168.100.1
       3. *Addresses to Give Out*: 192.168.100.2-192.168.100.100
       4. *DNS Servers*: 192.168.100.1
       5. *Lease Time*: 00:10:00
    2. Ether3
       1. *DHCP Address Space*: 192.168.200.0/24
       2. *Gateway for DHCP Network*: 192.168.200.1
       3. *Addresses to Give Out*: 192.168.200.2-192.168.200.100
       4. *DNS Servers*: 192.168.200.1
       5. *Lease Time*: 00:10:00

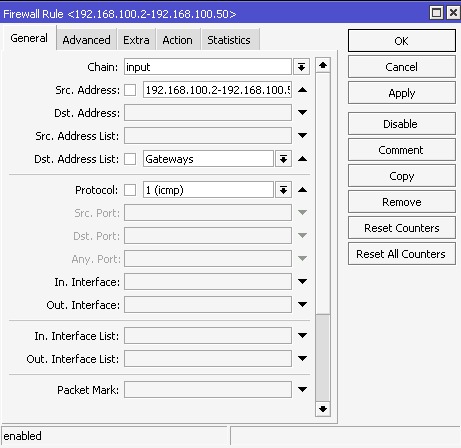
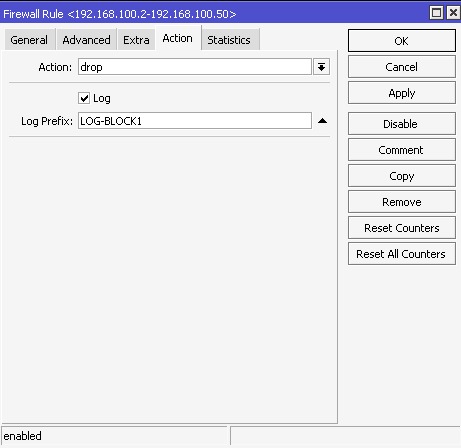
1. *Setting Firewall Filter Rules* pada *router*



**Gambar 3.26: Setting *Firewall Rules* pada *router***



**Gambar 3.27, dan 3.28: Setting *Firewall Rules* pada *router* untuk *block ICMP* 192.168.100.51 – 192.168.100.100 ke 192.168.200.0/24 dan *log***

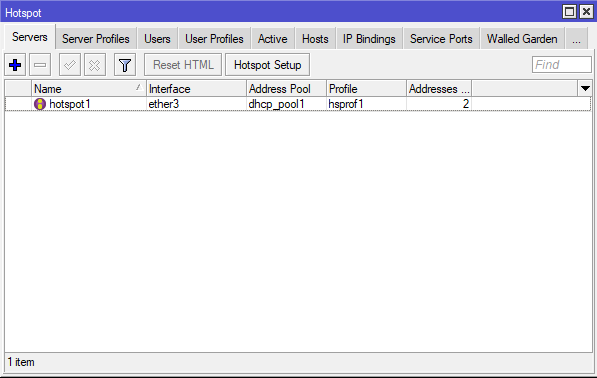


**Gambar 3.29, dan 3.30: Setting *Firewall Rules* pada *router* untuk *block ICMP* 192.168.100.2 – 192.168.100.50 ke *Gateway* dan *Log***

Pada langkah ini, *Firewall Rules* dibuat untuk memblokir *ICMP* / *Ping* ke *gateway* dan perangkat spesifik agar *hacker* lebih susah retas jaringan:

* + 1. *Chain*: input
       1. *Src Address*: 192.168.100.51 – 192.168.100.100
       2. *Dst Address*: 192.168.200.0/24
       3. *Protocol*: *ICMP*
       4. *Action*: drop, *Log*: LOG-BLOCK2
    2. *Chain*: input
       1. *Src Address*: 192.168.100.2 – 192.168.100.50
       2. *Dst Address* *List*: Gatways (192.168.100.1 dan 192.168.200.1)
       3. *Protocol*: *ICMP*
       4. *Action*: drop, *Log*: LOG-BLOCK1

1. *Setting RADIUS* dan *Hotspot* pada *router*

****

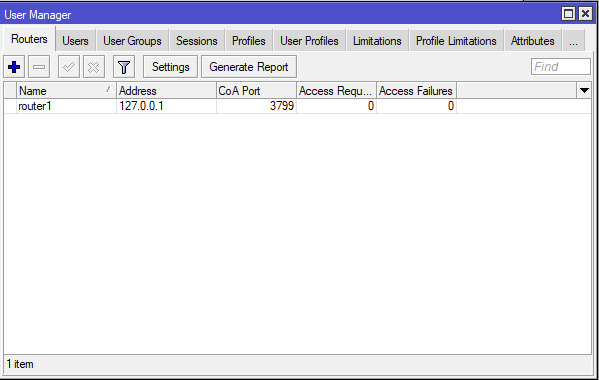
**Gambar 3.31: Setting *Hotspot* pada *Router***

*Hotspot* itu gunakan pada sebuah jaringan agar bisa mengatur siapa yang bisa menggunakan *Wi-Fi Hotspot* dengan *login* atau dengan *voucher.*

Pada langkah ini, *Hotspot* dikonfigurasi menggunakan *Hotspot Setup*:

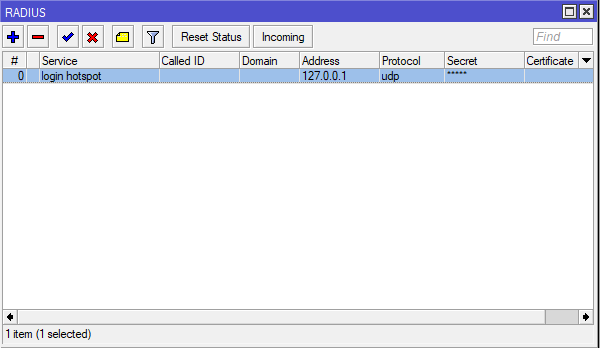
Ether3

* + - 1. *Local Address of Network*: 192.168.200.1/24
      2. *Masquerade Network*: off
      3. *Addresses Pool of Network*: 192.168.200.2-192.168.200.100
      4. *Select certificate*: none
      5. *IP Address of SMTP Server*: 0.0.0.0
      6. *DNS Servers*: 192.168.200.1
      7. *DNS Name*: login.fadhlan.hotspot

Setelah konfigurasi *Hotspot*, dilanjut dengan konfigurasi *RADIUS* dan *User Manager* server, agar *management user* lebih mudah:

**Gambar 3.32: *User Manager* pada *router***

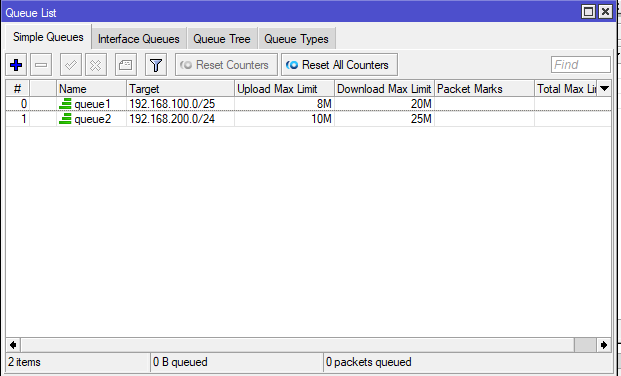
* + 1. *Settings*
       1. *Enabled* =
    2. *Routers* → Add
       1. *Shared Secret*: muhammad\_fadhlan@PROXYUKK
    3. *Users* → *Add Batch Users*
       1. *Number of Users*: 20

Setelah *User Manager* dikonfigurasi, dilanjut konfigurasi *server* *RADIUS*:

**Gambar 3.33: *RADIUS Server* konfig pada *router***

Setelah konfigurasi *User Manager*, dilanjut dengan konfigurasi *RADIUS*, karena *User Manager* perlu *server RADIUS* untuk manajemen akun:

* + 1. *Incoming*
       1. *Accept* =
    2. *Add*
       1. *Service* = [ hotspot [ login
       2. *Address* = 127.0.0.1
       3. *Protocol* = *udp*
       4. *Secret* = muhammad\_fadhlan@PROXYUKK

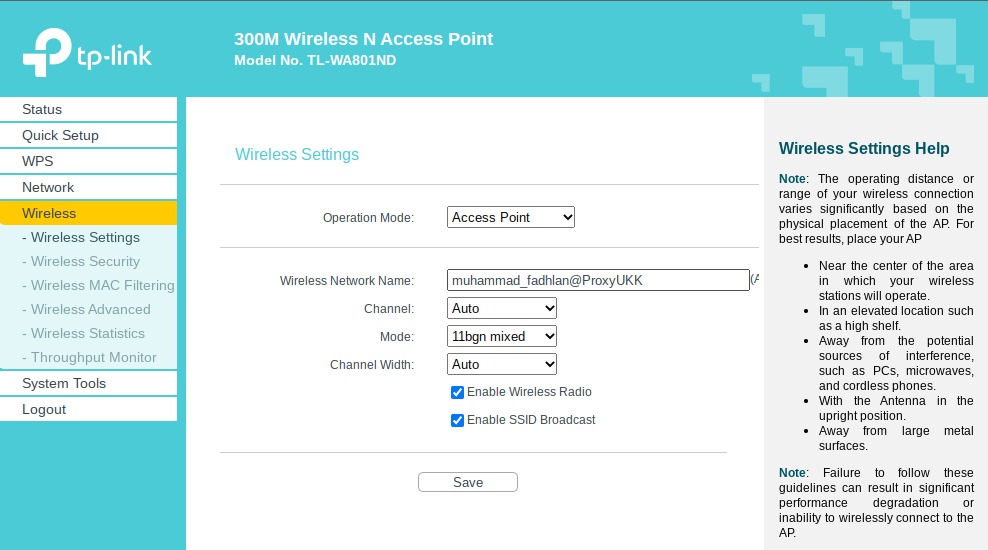
1. *Setting Simple Queue* pada *Router*

**Gambar 3.34:*Simple Queue* pada *Router***

Konfigurasi *Simple Queue* itu dilakukan agar penggunaan *bandwidth* pada jaringan itu rata dan adil:

* + 1. 192.168.100.0/25
       1. Target 20 Mbps *Download*
       2. Target 8 Mbps *Upload*
    2. 192.168.200.0/24
       1. Target 25 Mbps *Download*
       2. Target 10 Mbps *Upload*

1. *Setting SSID* pada *AP*



**Gambar 3.35: *Setting SSID* pada *Access Point***

Pada langkah ini, *SSID* pada *AP* dikonfigurasi sesuai soal, untuk membuka kontrol panel pertama koneksi ke *AP* dengan *SSID* dan *Password* dibawah *AP*nya. Terus di *Wireless Settings* diberi nama muhammad\_fadhlan@ProxyUKK dan tekan *Save*.

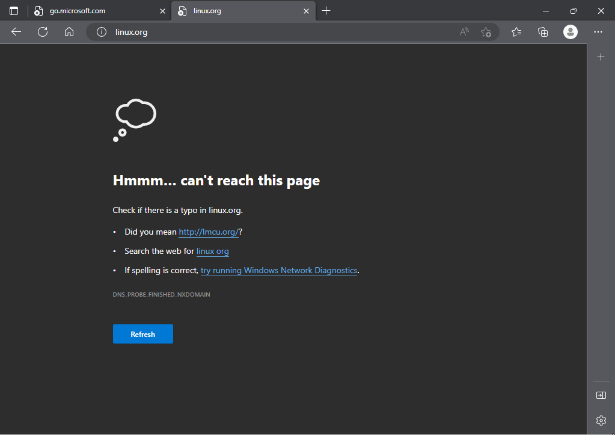
## **Skenario Uji Coba**

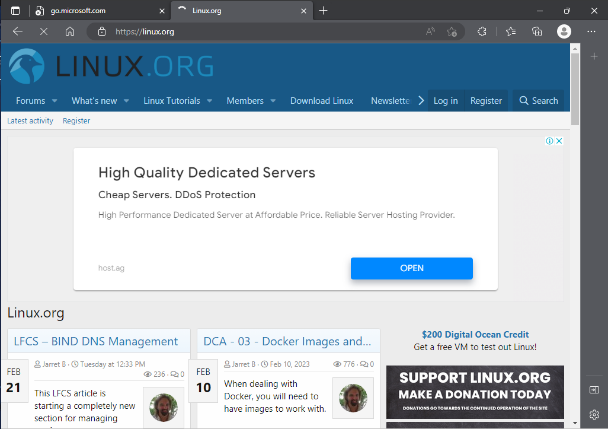
Untuk mengukur kestabilan jaringan, maka digunakan simulasi menggunakan *Mikrotik* 7.4, *Windows* 10 (64 bit), *Winbox* v3.35, *VirtualBox* v7.0, dan Microsoft Edge yang mengacu pada hasil dari rancangan jaringan.

*Software* ini digunakan karena sesuai dengan kebutuhan. Selain itu juga penggunannya yang mudah dimengerti oleh *user.* Dari hasil simulasi yang dibuat maka diambil beberapa sampel dan tes untuk mengukur keberhasilan *services*, efektifitas, dan, kinerja jaringan. Berikut adalah metode yang digunakan untuk uji coba topologi jaringan yang telah dibuat.

1. Hardware Uji Coba
   1. TP LINK Access Point (TL-WR840N)
   2. RouterBOARD hEX
   3. PC Client
   4. Switch Unmanageable
2. Software Uji Coba
   1. Mikrotik RouterOS v7.4
   2. User Manager 5
   3. Windows 10
   4. Winbox 3.55
   5. Virtual Box v7.0
   6. Microsoft Edge

## **Daftar Dokumen Pengujian Fungsi Jaringan**

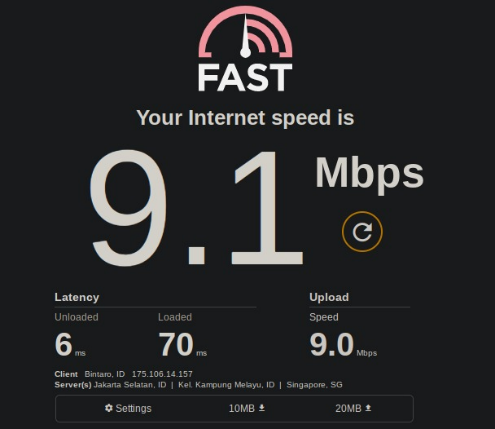
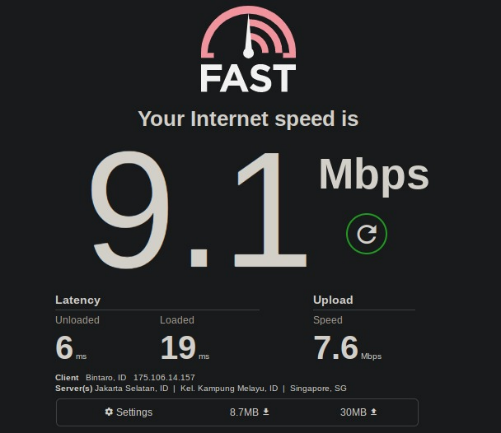
* 1. *DNS Blocking*



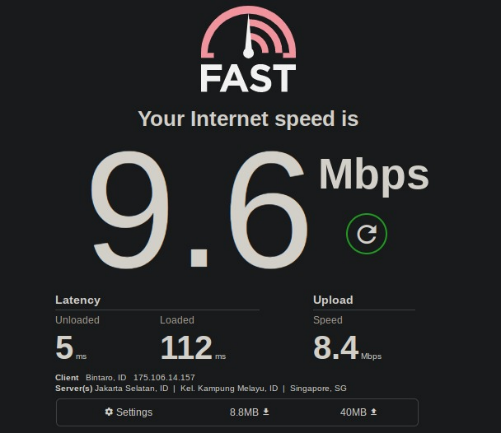
**Gambar 3.36 dan 3.37: Gambar Sebelum dan Sesudah *DNS Blocking***

Bisa dilihat dari gambar diatas, sebelum, dan sesudah diperlakukan *DNS Blocking*. Sebelumnya klien bisa buka *website* terblockir dan sesudahnya, klien tidak bisa buka *website* terblockir.

* 1. *Simple Queue*

**

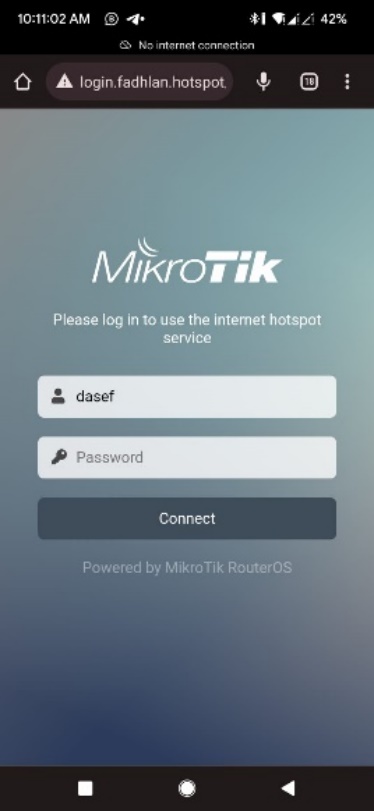
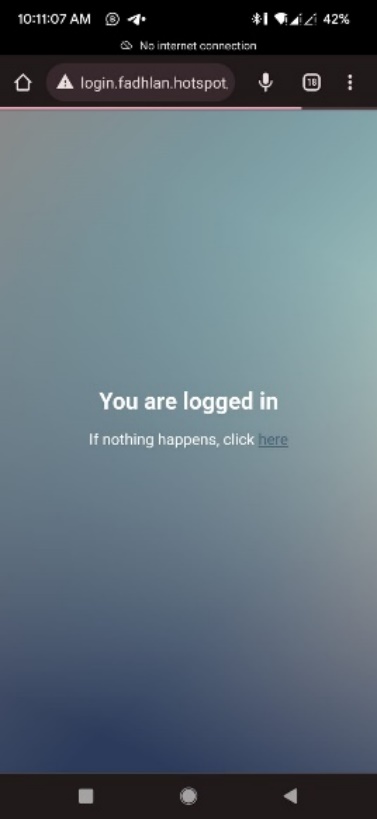
**Gambar 3.38 dan 3.39: Gambar Sebelum dan Sesudah *Simple Queue* pada jaringan 192.168.100.0/25**

**

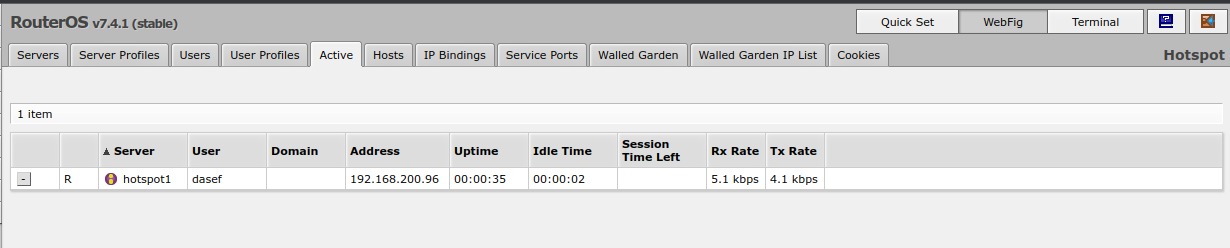
**Gambar 3.40 dan 3.41: Gambar Sebelum dan Sesudah *Simple Queue* pada jaringan 192.168.200.0/24**

Bisa dilihat dari gambar diatas, sebelum, dan sesudah diperlakukan *Simple Queue*. Sebelumnya klien bisa gunakan semua *bandwith*, dan sesudahnya tidak.

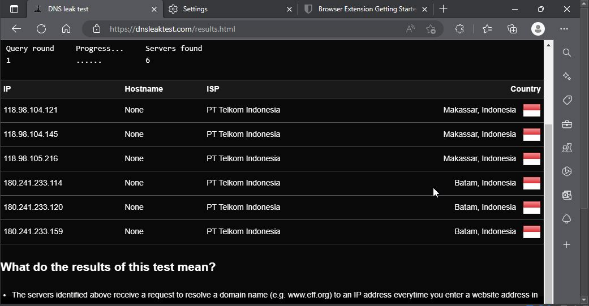
* 1. *Hotspot* dan *RADIUS*

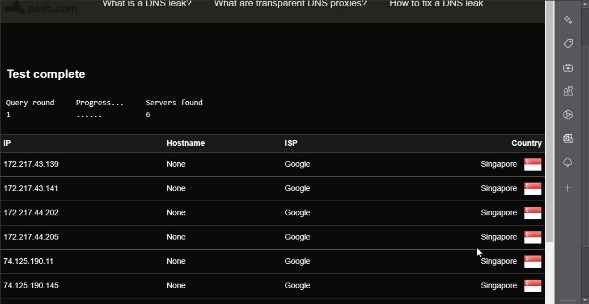


**Gambar 3.42 dan 3.43: Gambar *Login Hotspot***



**Gambar 3.44: *Gambar RADIUS Active users***

* 1. *DNS over HTTPS*

**

**Gambar 3.45 dan 3.46: Gambar Sebelum dan Sesudah *DoH***

Bisa dilihat dari gambar diatas, sebelum, dan sesudah diperlakukan *DNS over HTTPS*, sebelumnya tidak bisa buka *website* tertentu, dan sesudahnya bisa.

**BAB IV**

**KESIMPULAN & SARAN**

# **BAB IV KESIMPULAN & SARAN**

## **Kesimpulan**

Dapat disimpulkan dari laporan UKK diatas bahwa pembangunan jaringan itu adalah salah satu keperluan yang penting pada zaman sekarang, dan peralatan jaringan yang modern seperti *DoH*, *Simple Queue*, dan *DNS Blocking* dapat meningkat kemampuan teknologi pada perusahaan.

Dengan semua peralatan ini, maka jaringan bisa lebih efisien, lebih rata pemakaian bandwidth, dan lebih aman.

## **Saran**

Saran perbaikan penulisan untuk sekolah:

* 1. Sekolah seharusnya memberikan lebih banyak waktu untuk perbaikan dengan cara dedikasikan waktu yang khusus untuk revisi
  2. Sekolah seharusnya memberikan revisi lebih cepat agar waktunya tidak tertekan

Saran pengembangan toplogi adalah:

1. Seharusnya topologi diolah lebih banyak jadi bisa lebih baik dari sekarang

32

**DAFTAR PUSTAKA**

# **DAFTAR PUSTAKA**

Admin. “*DNS over HTTPS di Mikrotik RouterOS*”. Citraweb. 03 Maret 2023. <https://citraweb.com/artikel/390>