Jaringan *Hotspot* Menggunakan Dua *Radius MikroTik* dan *Ethernet Over Internet Protocol Tunnel*

Taufik Rahman[1,*]

[1] Manajemen Informatika; AMIK BSI Jakarta; Jl. RS. Fatmawati No.24 Jakarta Selatan 12450, (021) 75914750; e-mail: taufik.tkr@bsi.ac.id

* Korespondensi: e-mail: taufik.tkr@bsi.ac.id

Diterima: 24 April 2018 ; Review: 15 Mei 2018; Disetujui: 28 Mei 2018

Cara sitasi: Rahman Taufik. 2018. Jaringan Hotspot Menggunakan Dua *Radius MikroTik* dan *Ethernet Over Internet Protocol Tunnel*. Informatics For Educators and Professionals. 2 (2): 135 – 148.

Abstrak: Koneksi internet dengan jaringan *wireless* sangat rentan dalam hal keamanan, meski sudah menggunakan *password.* Oleh karena itu diperlukan sistem keamanan yang lebih, dimana hanya pengguna legal yang bisa terkoneksi dengan jaringan *wireless.* Pengguna legal terdaftar pada database dengan memiliki id dan *password* yang unik. Unik itu berbeda, informasi sensitif yang digunakan. Pada penelitian ini, bertujuan bagaimana membuat *hotspot* dengan dua *radius-server* pada kantor pusat BSI dioperasikan bersamaan pada mikrotik kampus dan bagaimana menghubungkan kampus BSI dengan kantor pusat. Dengan *user* dan *password* pada dua *radius* yaitu *radius*-bsi dan *radius*-nuri, *split user domain* pada mikrotik kampus dan *Tunnel* EoIP sebagai jaringan vpn nya, mahasiswa, staf dan dosen dapat *Login* hostspot. *User* yang berhasil *Login* masuk ke *user* aktif *hotspot* pada MikroTik RB1000 Kampus dan *Session User Radius Server* MikorTik *user Manager* pada kantor pusat BSI. Demikian pengguna *hotspot* dapat termonitoring dan manajemen *user hotspot* dengan dua *radius server* dapat beroperasi bersamaan pada satu MikroTik pada Kampus.

Kata kunci: *Hotspot*, Jaringan, MikroTik, *Radius*, *Tunnel*

Abstract: *Internet connection with wireless network is very vulnerable in terms of security, even if you already use a password. Therefore more security systems are needed, where only legal users can connect to the wireless network. Legal users are registered on the database with a unique id and password. Unique is different, sensitive information is used. In this study, it aims to create a hotspot with two radius-servers at BSI headquarters operated simultaneously on campus microphones and how to connect BSI campus with headquarters. With user and password on two radiuses ie radius-bsi and radius-parrot, split user domain on campus microtik and EoIP Tunnel as its vpn network, student, staff and lecturer can Login hostspot. Users who successfully Login into the active user hotspot on MikroTik RB1000 Campus and Session User Radius Server MikorTik user Manager at BSI headquarters. Thus hotspot users can be monitored and hotspot user management with two server radios can operate simultaneously on one MikroTik on Campus.*

Keywords*: Hotspot, MikroTik, Network, Radius, Tunnel*

E-ISSN: 2548-3412 ; 135 – 148

1. Pendahuluan

Koneksi internet dengan jaringan *wireless* sangat rentan dalam hal keamanan, meski sudah menggunakan *password.* Oleh karena itu diperlukan sistem keamanan yang lebih, dimana hanya pengguna legal yang bisa terkoneksi dengan jaringan *wireless.* Pengguna legal terdaftar pada database dengan memiliki id dan *password* yang unik. Unik itu berbeda, informasi sensitif yang digunakan. Kelahiran pengguna dapat digunakan dari tanggal bulan dan tahun, dapat dikombinasikan dengan nomer identitas dari organisasi atau institusi. Dengan dua hal tersebut dapat di data dan dibuat sistem identifikasi otentikasi legal pengguna *wireless*, *hotspot*. Karena untuk mengakses jaringan secara *wireless* diperlukan *user* dan *password*.

Permasalahan yang dihadapi bagaimana jika pengguna memiliki dua id dengan *password* yang sama, studi kasus pada mahasiswa dual degree BSI dan STMIK Nusa Mandiri memiliki nim berbeda dan *password* sama. Metode yang baik diantaranya menggunakan 2 *radius* terpisah dengan MikroTik sebagai *server* nya. Kemudian lokasi kampus BSI dan STMIK Nusa Mandiri yang tidak satu bangunan dan terpisahkan oleh jarak, jabodetabek, cikarang, cibitung, cikampek, tasik, bandung, sukabumi, purwokerto, jogja, tegal dan Pontianak. Hal ini dapat menggunakan *Virtual Private Network* melalui jaringan internet.

Penelitian ini menggunakan beberapa referensi yang terkait dengan objek riset utama, antara lain oleh Jennifer Golbeck pada penelitiannya mengatakan banyak perusahaan penyedia layanan internet menawarkan wifi *hotspot* yang di jalankan melalui router nirkabel dirumah pelanggan[Golbeck, 2017].

Wi-Fi *hotspot* adalah produk teknologi jaringan nirkabel yang dapat dengan mudah ditemukan di tempat-tempat umum seperti bandara, kafe, atau pusat perbelanjaan. Selain menawarkan kemudahan dalam koneksi, penggunaan teknologi jaringan nirkabel juga menimbulkan masalah keamanan karena terletak di area terbuka atau publik. Perlu ada mekanisme yang dapat mengontrol akses ke jaringan nirkabel untuk melindunginya dari penyerang atau penyusup[Hermaduanti and Riadi, 2016]

Mengusulkan sistem otentikasi yang menyelesaikan masalah sederhana dan berulang, terjadi antara pengguna jaringan dan orang yang bertanggung jawab atas pemeliharaan jaringan dan dapat mempercepat otentikasi pengguna, melalui otentikasi pengguna berbasis desain jaringan yang dapat mengelola otentikasi jaringan yang tersebar secara terpusat dan fleksibel. Melalui sistem yang diusulkan, ancaman terhadap keamanan akan diminimalkan dan pengguna dan manajer jaringan diantisipasi untuk melepaskan diri dari tugas-tugas sederhana dan berulang pada layanan dan manajemen internet[Yu et al., 2018].

Menyajikan solusi yang berkaitan dengan otentikasi, otorisasi pengguna yang berniat mendapatkan akses ke Internet melalui jaringan aman. Protokol *RADIUS* digunakan untuk mengenkapsulasi paket protokol otentikasi warisan PAP, CHAP, MSCHAPv1, dan MSCHAPv2, sementara algoritma hashing MD4, MD5, asin MD5 dan SHA-1 digunakan untuk memberikan keamanan yang lebih baik untuk kata sandi pengguna[Cristescu et al., 2016].

Merancang dan menerapkan kebijakan keamanan berdasarkan persyaratan dan tuntutan yang disajikan dengan skenario menggunakan peralatan Mikrotik[Pauzhi and Coronel, 2015]

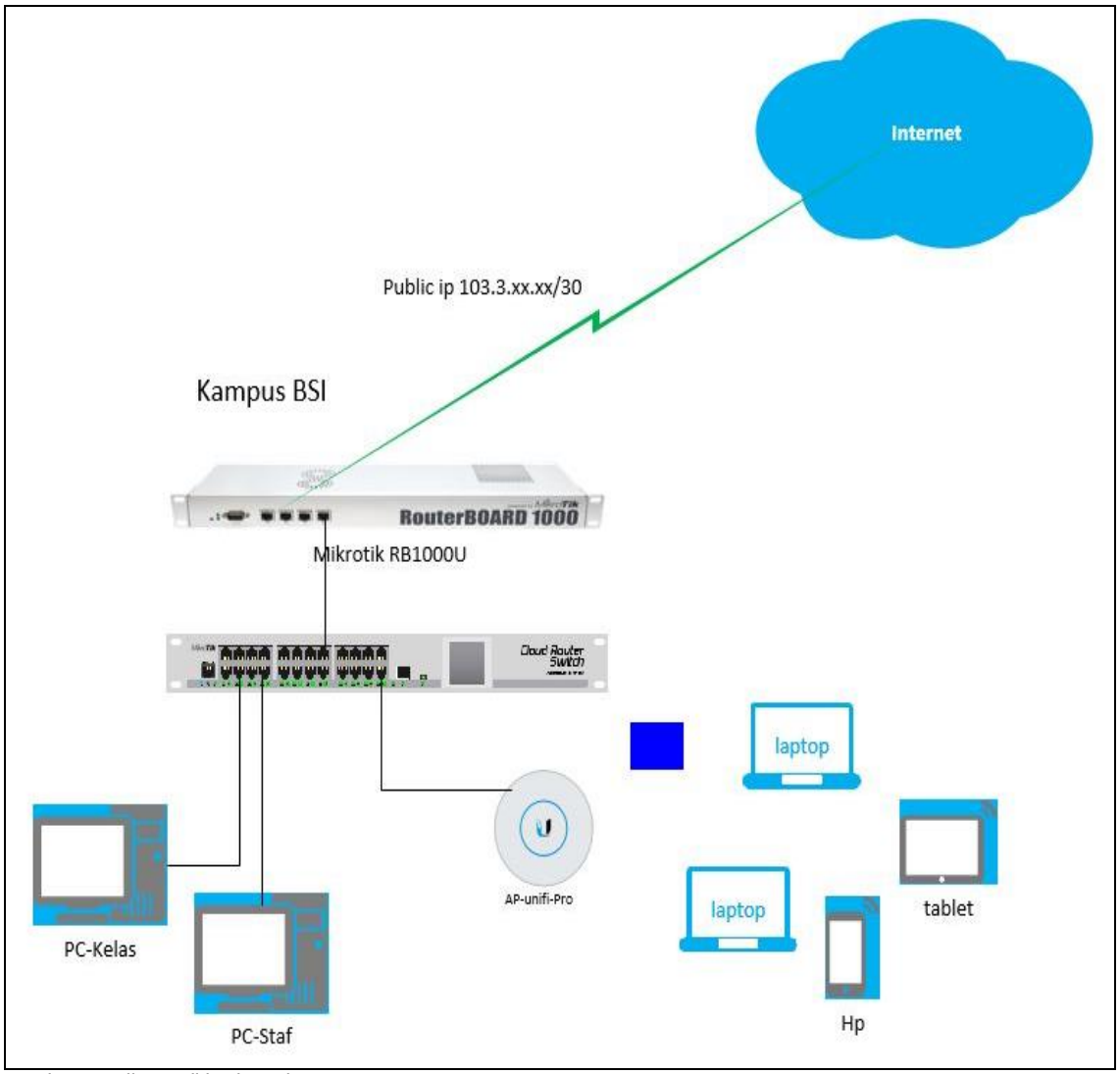
Penerapan keamanan jaringan hotspot menggunakan radius dapat memberikan tingkat keamanan yang cukup baik, serta dapat lebih memudahkan admin jaringan dalam mengelola semua user yang terhubung pada jaringan hotspot[Kuswanto, 2017].

Tujuan dari penelitian untuk membuat otentikasi pada jaringan wireless dalam bentuk *hotspot* dimana pengguna memiliki *user*name sama dengan *password* berbeda yang telah terdaftar pada dua *radius server* mikrotik yang berbeda, dapatkah dua *radius server* beroperasi bersamaan pada satu MikroTik kampus, serta bagaimana menghubungkan jaringan kampus dengan jaringan kantor pusat, sehingga hanya pengguna legal yang dapat koneksi ke internet melalui jaringan *hotspot*.

2. Metode Penelitian

Metode yang digunakan dalam melakukan penelitian ini meliputi beberapa tahap, seperti studi pustaka, analisa kebutuhan, desain, testing, dan implementasi. Studi pustaka merupakan suatu tahap yang bertujuan untuk menelaah masalah secara mendalam yang berkaitan dengan *Hotspot*, maka penulis mencoba melakukan studi pustaka yaitu dengan mengumpulkan data-data teoritis dan mempelajari buku-buku atau literature dengan maksud untuk mendapatkan teori-teori dan bahan-bahan yang berkaitan dengan masalah *Hotspot*,

radius-server dan EoIP *Tunnel*. Tahap selanjutnya yaitu anlisa kebutuhan pada tahap ini dilakukan suatu kegiatan analisa topologi jaringan yang sudah ada pada saat ini dan perencanaan implementasi topologi jaringan yang akan dibuat dalam membangun jaringan VPN dari kampus ke kantor pusat melalui internet, data mahasiswa dan staff dari BSI Group digunakan untuk *user* dan *password Login hotspot*, dan perangkat MikroTik RB1100AHX2 dua unit sebagai *radius server*. Kemudian masuk ke tahap desain, dimana data yang sudah dianalisa pada tahap sebelumnya, pada tahap ini memberikan usulan yang dimaksudkan untuk lebih meningkatkan performansi, efisien dan efektifitas dari jaringan. Pada tahap desain terdapat usulan yang diberikan berupa desain mengenai perangkat, topologi, skema, metode dan konsep yang akan digunakan. Selanjutnya masuk ke tahap pengujian atau *testing*, pada tahap ini semua komponen jaringan diuji keberhasilannya dengan mencoba *user password hotspot* yang terdapat pada *radius server*, juga dengan *user* yang tidak terdaftar. Pengujian jaringan melalui monitoring *user* yang terhubung menggunakan jaringan, pelaporan dan evaluasi. Tahap yang terakhir yaitu implementasi, pada tahap ini penggabungan topologi fisik yang sudah ada dengan topologi yang baru, yang sudah diuji. Dari pembuatan *interface virtual*, setting IP, konfigurasi *routing*, *NAT* untuk *masquerade sub-network* nya, pembuatan *radius*, penambahan *router* pada *server-radius*, mengkoneksikan jaringan dari kampus dengan kantor pusat dilakukan pada tahap ini.



Sumber: Hasil Penelitian(2017)

Gambar 1. Topologi Jaringan Kampus Bina Sarana Informatika

E-ISSN: 2548-3412 ; 135 – 148

3. Hasil dan Pembahasan

Pada bagian ini, dijelaskan hasil penelitian dan pada saat yang sama diberikan pembahasan yang komprehensif. Hasil dapat disajikan dalam angka, grafik, tabel dan lain-lain yang membuat pembaca memahami dengan mudah. Pembahasan dapat dibuat dalam beberapa sub-bab.

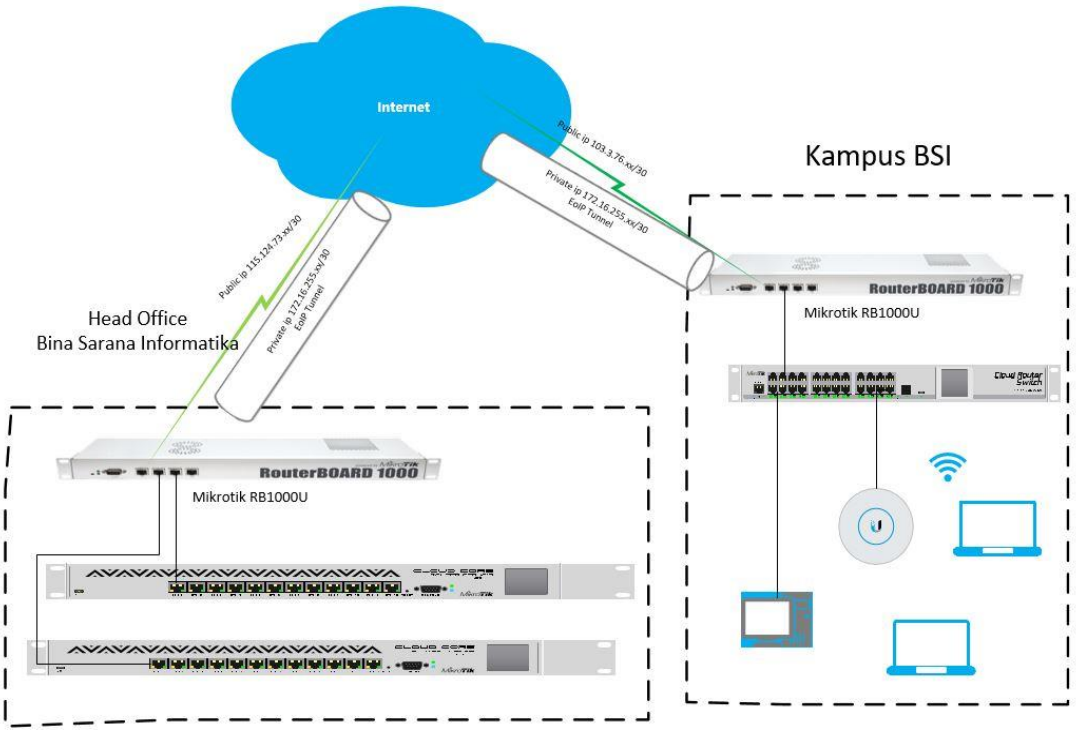
Dalam penelitian ini mengambil studi kasus jaringan wireless yang dijadikan *hotspot* pada salah satu kampus BSI Group sebagai metode autentikasi nya menggunakan *radius server* dengan MikroTik Cloud Core Router yang berada di kantor pusat BSI. Tahapan dalam implementasi nya sebagai berikut.

3.1. Analisa Permasalahan

Pada kampus Bina Sarana Informatika terdapat jaringan wireless pada gambar 1, untuk akses dibutuhkan *password* yang sudah dibuat oleh technical support menggunakan WPA Personal dan di share ke staff, dosen dan adm kemudian ke mahasiswa. Permasalahan nya adalah tidak diketahui identitas pengguna internet pada jaringan wireless sehingga jika terjadi pelanggaran keamanan, penggunaan bandwidth berlebih tidak dapat terdeteksi. Oleh karena nya dibuatlah sistem *hotspot* untuk otentikasi pada jaringan wireless. Selanjutnya agar penggunaan jaringan *hotspot* dapat dimonitoring dari kantor pusat BSI, maka dibuatlah *radius server* menggunakan MikroTik Cloud Core Router sebanyak dua unit karena terdapat mahasiswa dual degree BSI dan STMIK Nusa Mandiri yang memiliki nomor induk berbeda dengan *password* yang sama yaitu tahun bulan dan tanggal lahir mahasiswa. Untuk koneksi dari kampus ke kantor pusat menggunakan *Virtual Private Network* dengan membuat EoIP *Tunnel*.

3.2. Desain

Pada bagian desain dimulai membuat topologi jaringan pada gambar 2, pembuatan ip address, vpn dengan EoIP *Tunnel*, network address translation, *routing* pada MikroTik RouterBoard Kampus dan MikroTik Kantor Pusat BSI. Instalasi packet *user-Manager* dan memasukkan ip router kampus pada MikroTik Cloud Core Router, konfigurasi *hotspot* pada MikroTik Kampus.



Sumber: Hasil Penelitian (2018)

Gambar 2. Jaringan *Hotspot* kampus BSI dengan dua *Radius* MikroTik melalui EoIP *Tunnel*

Koneksi jaringan kantor pusat BSI dengan kampus menggunakan vpn melalui jaringan internet dengan *Tunnel* EoIP. *Tunnel* EoIP dibangun pada *router* MikroTik RB1000 dikedua sisi sebagai *interface virtual*.
Interface virtual pada MikroTik kantor pusat BSI dapat dilihat dengan CLI (Command Line *Interface*) menggunakan Putty dengan SSH pada ip router nya sebagai berikut,
Konfigurasi *interface* EoIP *Tunnel*

```
[taufik@MT_kantorpusat] > interface eoip pr
Flags: X - disabled, R - running
 0  R name="eoip-to-kampus" mtu=1500 actual-mtu=1500 l2mtu=65535
      mac-address=02:AE:65:C0:FC:6D arp=enabled arp-timeout=auto
      loop-protect=default loop-protect-status=off
      loop-protect-send-interval=5s loop-protect-disable-time=5m
      local-address=0.0.0.0 remote-address=103.3.xx.xx Tunnel-id=141
      dscp=inherit clamp-tcp-mss=no dont-fragment=no allow-fast-path=no
```

Interface virtual pada MikroTik kampus BSI sebagai berikut,

```
[taufik@MT_Kampus] > interface eoip pr
Flags: X - disabled, R - running
 0  R name="eoip-to-kantorpusat" mtu=1500 actual-mtu=1500 l2mtu=65535
      mac-address=02:96:21:AF:BC:25 arp=enabled local-address=0.0.0.0
      remote-address=115.124.xx.xx Tunnel-id=141 dscp=inherit clamp-tcp-mss=no
      dont-fragment=no allow-fast-path=no
```

Kemudian *interface* EoIP *Tunnel* diberikan ip address untuk dapat berkomunikasi pada keduanya.

```
[taufik@MT_Kampus] > ip address pr
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.10.0.1/26       10.10.0.0       vlan1
 1   10.10.1.1/25       10.10.1.0       vlan10
 2   10.10.2.1/25       10.10.2.0       vlan20
 3   10.10.3.1/25       10.10.3.0       vlan30
 4   10.10.4.1/25       10.10.4.0       vlan40
 5   10.10.5.1/25       10.10.5.0       vlan50
 6   10.10.6.1/25       10.10.6.0       vlan60
 7   10.10.7.1/25       10.10.7.0       vlan70
 8   10.10.8.1/25       10.10.8.0       vlan80
 9   10.10.9.1/25       10.10.9.0       vlan90
10   10.10.10.1/25      10.10.10.0      vlan100
11   172.16.xx.254/24   172.16.xx.0     vlan200
12   172.16.255.xx/30   172.16.255.xx   eoip-to-kantorpusat
13   103.3.xx.xx/29     103.3.xx.xx     ether1-isp
14   10.100.100.1/27    10.100.100.0    vlan500
15   10.168.100.1/26    10.168.100.0    vlan600
```

Jika pada ip address terdapat x artinya ujung ip address tersebut disembunyikan untuk keamanan.

IP address pada MikroTik kantor pusat BSI adalah sebagai berikut,

```
[taufik@MT_kantorpusat] > ip address  pr
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   115.124.xx.xx/30   115.124.xx.xx   ether1@ISP-kantorpusat
 1   172.16.255.xx/30   172.16.255.xx   eoip-to-Kampus
 2   172.16.10.1/24     172.16.10.0     vlan@Server
```

Selanjutnya *routing* yang terdapat pada MikroTik kantor pusat dan Kampus.

```
[taufik@MT_kantorpusat] > ip route pr
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
```

E-ISSN: 2548-3412 ; 135 – 148

```
B - blackkantorpusatle, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  ;;; Gateway ISP
        0.0.0.0/0          115.124.xx.xx               1
 1 A S  ;;; route to bsi kampus
        172.16.xx.0/24                 172.16.255.xx           1
 2 ADC  115.124.xx.xx/30  115.124.xx.xx  ethernet1@isp...       0
 3 ADC  172.16.10.0/24    172.16.10.1    vlan@Server          0
 4 ADC  172.16.255.xx/30  172.16.255.xx  eoip-to-Kampus              0
[taufik@MT_Kampus] > ip route pr
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  ;;; Gateway to ISP
        0.0.0.0/0                      103.3.xx.xx
 1 ADC  10.10.0.0/26       10.10.0.1       vlan1
 2 ADC  10.10.1.0/25       10.10.1.1       vlan10
 3 ADC  10.10.2.0/25       10.10.2.1       vlan20
 4 ADC  10.10.3.0/25       10.10.3.1       vlan30
 5 ADC  10.10.4.0/25       10.10.4.1       vlan40
 6 ADC  10.10.5.0/25       10.10.5.1       vlan50
 7 ADC  10.10.6.0/25       10.10.6.1       vlan60
 8 ADC  10.10.7.0/25       10.10.7.1       vlan70
 9 ADC  10.10.8.0/25       10.10.8.1       vlan80
10 ADC  10.10.9.0/25       10.10.9.1       vlan90
11 ADC  10.10.10.0/25      10.10.10.1      vlan100
12 ADC  10.100.100.0/27    10.100.100.1    vlan500
13 ADC  103.3.xx.xx/29     103.3.xx.xx     ether1-isp
14 ADC  172.16.xx.0/24     172.16.xx.254   vlan200
15 A S  ;;; route to dwsa
        172.16.10.0/24                 172.16.255.xx
16 ADC  172.16.255.xx/30 172.16.255.xx eoip-to-kantorpusat
17 ADC  10.168.100.0/26    10.168.100.1    vlan600
```

3.3. Implementasi

Selanjutnya implementasi *hotspot* pada MikroTik Kampus dengan memilih *interface*, dapat menggunakan *interface* fisik atau Ethernet juga bisa pada *interface virtual* seperti vlan. Pada kampus BSI *Login hotspot* juga digunakan untuk perkuliahan di kelas. Dengan memilih SSID sesuai dengan nama ruang kelas, misal : R 201 itu untuk perkuliahan pada ruang 201. Oleh karena itu, jumlah *interface* vlan bergantung pada jumlah ruang kelas pada kampus BSI.

Pembuatan *hotspot server* pada kampus terdapat 12 *hotspot server* pada tampilan menggunakan terminal pada menu winbox setelah *Login*:

Konfigurasi *Hotspot Server*

```
[taufik@MT_Kampus] > ip hotspot print detail
Flags: X - disabled, I - invalid, S - HTTPS
 0      name="hs-vlan10" interface=vlan10 address-pool=dhcp_pool2 profile=hsprof1 idle-
timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-
name=10.100.1.1  proxy-status="running"
 1      name="hs-vlan20" interface=vlan20 address-pool=dhcp_pool3 profile=hsprof1 idle-
timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-
name=10.100.1.1 proxy-status="running"
 2      name="hs-vlan30" interface=vlan30 address-pool=dhcp_pool4 profile=hsprof1 idle-
timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-
name=10.100.1.1     proxy-status="running"
 3      name="hs-vlan40" interface=vlan40 address-pool=dhcp_pool5 profile=hsprof1 idle-
timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-
name=10.100.1.1     proxy-status="running"
```

4 name="hs-vlan50" interface=vlan50 address-pool=dhcp_pool6 profile=hsprof1 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.100.1.1 proxy-status="running"
5 name="hs-vlan60" interface=vlan60 address-pool=dhcp_pool7 profile=hsprof1 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.100.1.1 proxy-status="running"
6 name="hs-vlan70" interface=vlan70 address-pool=dhcp_pool8 profile=hsprof1 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.100.1.1 proxy-status="running"
7 name="hs-vlan80" interface=vlan80 address-pool=dhcp_pool9 profile=hsprof1 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.100.1.1 proxy-status="running"
8 name="hs-vlan90" interface=vlan90 address-pool=dhcp_pool10 profile=hsprof1 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.100.1.1 proxy-status="running"
9 name="hs-vlan100" interface=vlan100 address-pool=dhcp_pool11 profile=hsprof1 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.100.1.1 proxy-status="running"
10 name="hs-vlan500" interface=vlan500 address-pool=dhcp_pool13 profile=hsprof3 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.100.100.1 proxy-status="running"
11 name="hs-vlan600" interface=vlan600 address-pool=dhcp_pool14 profile=hsprof4 idle-timeout=5m keepalive-timeout=none Login-timeout=none addresses-per-mac=1 ip-of-dns-name=10.168.100.1 proxy-status="running"

Konfigurasi *Hotspot* Profile

[taufik@MT_Kampus] > *ip hotspot profile pr*
*Flags: * - default*
*0 * name="default" hotspot-address=0.0.0.0 dns-name="" html-directory=hotspot rate-limit="" http-proxy=0.0.0.0:0 smtp-server=0.0.0.0 Login-by=http-chap split-user-domain=no use-radius=no*
1 name="hsprof1" hotspot-address=10.10.1.1 dns-name="hotspot.bsi.ac.id" html-directory=hotspot rate-limit="" http-proxy=0.0.0.0:0 smtp-server=0.0.0.0 Login-by=http-chap split-user-domain=no use-radius=no
2 name="hsprof2" hotspot-address=10.100.100.1 dns-name="hotspot.bsi.ac.id" html-directory=hotspotbsi rate-limit="" http-proxy=0.0.0.0:0 smtp-server=0.0.0.0 Login-by=http-chap split-user-domain=yes use-radius=yes radius-accounting=yes radius-interim-update=received nas-port-type=wireless-802.11 radius-default-domain="radius-bsi" radius-location-id="" radius-location-name="" radius-mac-format=XX:XX:XX:XX:XX:XX
3 name="hsprof3" hotspot-address=10.168.100.1 dns-name="hotspot.nusamandiri.ac.id" html-directory=hotspotnusamandiri rate-limit="" http-proxy=0.0.0.0:0 smtp-server=0.0.0.0 Login-by=http-chap split-user-domain=yes use-radius=yes radius-accounting=yes radius-interim-update=received nas-port-type=wireless-802.11 radius-default-domain="radius-nuri" radius-location-id="" radius-location-name="" radius-mac-format=XX:XX:XX:XX:XX:XX

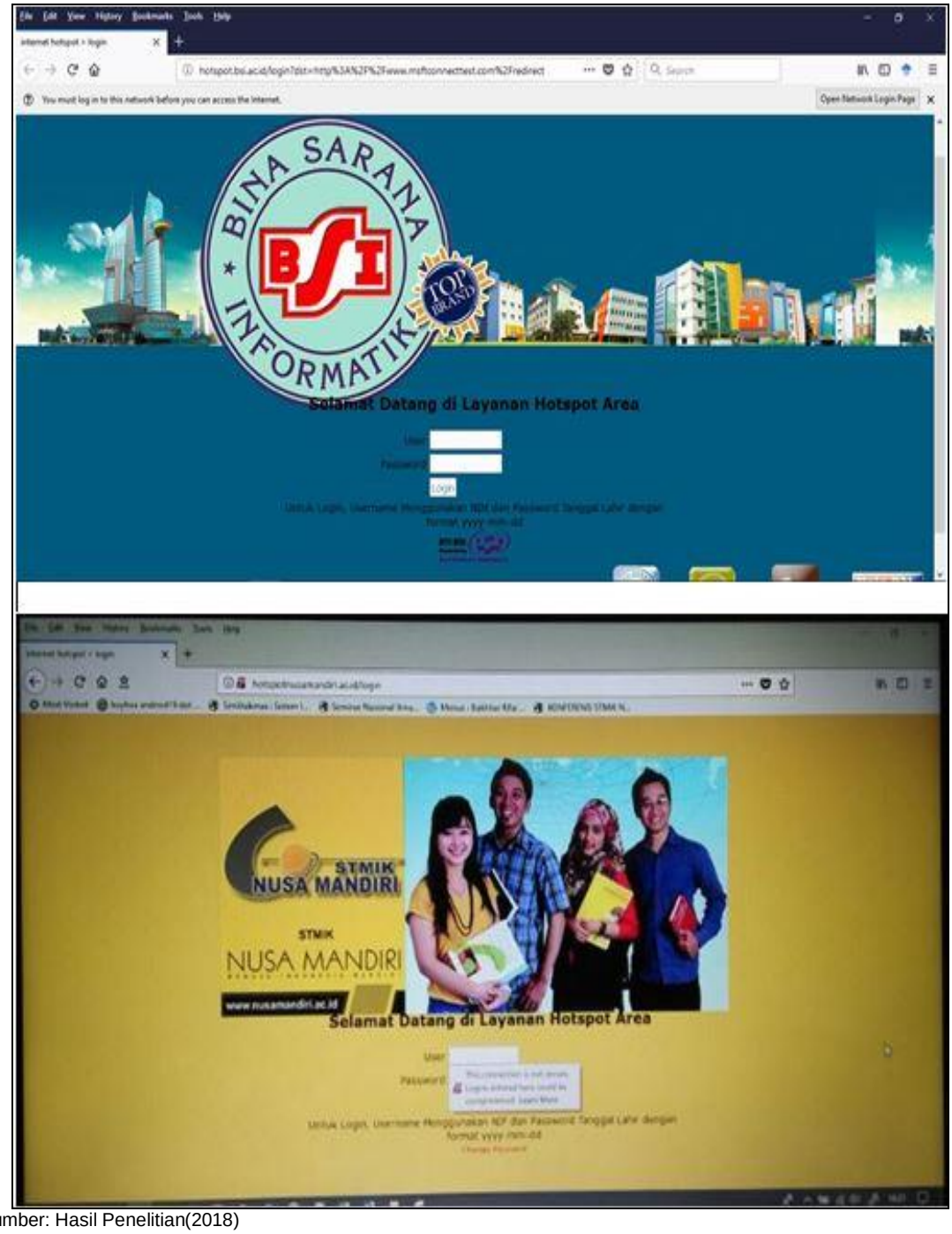
Pada *hotspot* profile number 2 dan 3 pada *radius*-default-domain ditambahkan ”*radius*-bsi” dan ”*radius*-nuri”, untuk memanggil *radius server* nya.

[taufik@MT_Kampus] > radius pr detail without-paging
Flags: X - disabled
0 service=*Login*,hotspot called-id="" domain="radius-bsi" address=172.16.192.10 secret="password" authentication-port=1812 accounting-port=1813 timeout=3000ms accounting-backup=no realm="" src-address=172.16.100.254
1 service=*Login*,hotspot called-id="" domain="radius-nuri" address=172.16.10.12 secret="password" authentication-port=1812 accounting-port=1813 timeout=3000ms accounting-backup=no realm="" src-address=172.16.100.254

Pada gambar 3, tampilan awal untuk penggunaan koneksi ke jaringan wireless, jika memilih SSID BSI maka akan muncul halaman *Login hotspot* yang atas, kemudian untuk SSID Nusa Mandiri akan muncul laman *Login hotspot* dengan logo STMIK Nusa Mandiri. Selanjutnya

E-ISSN: 2548-3412 ; 135 – 148

jika *Login* berhasil maka akan di direct ke laman mahasiswa.kampus.id dari kelas melalui AP-Unifi untuk perkuliahan.



Sumber: Hasil Penelitian(2018)

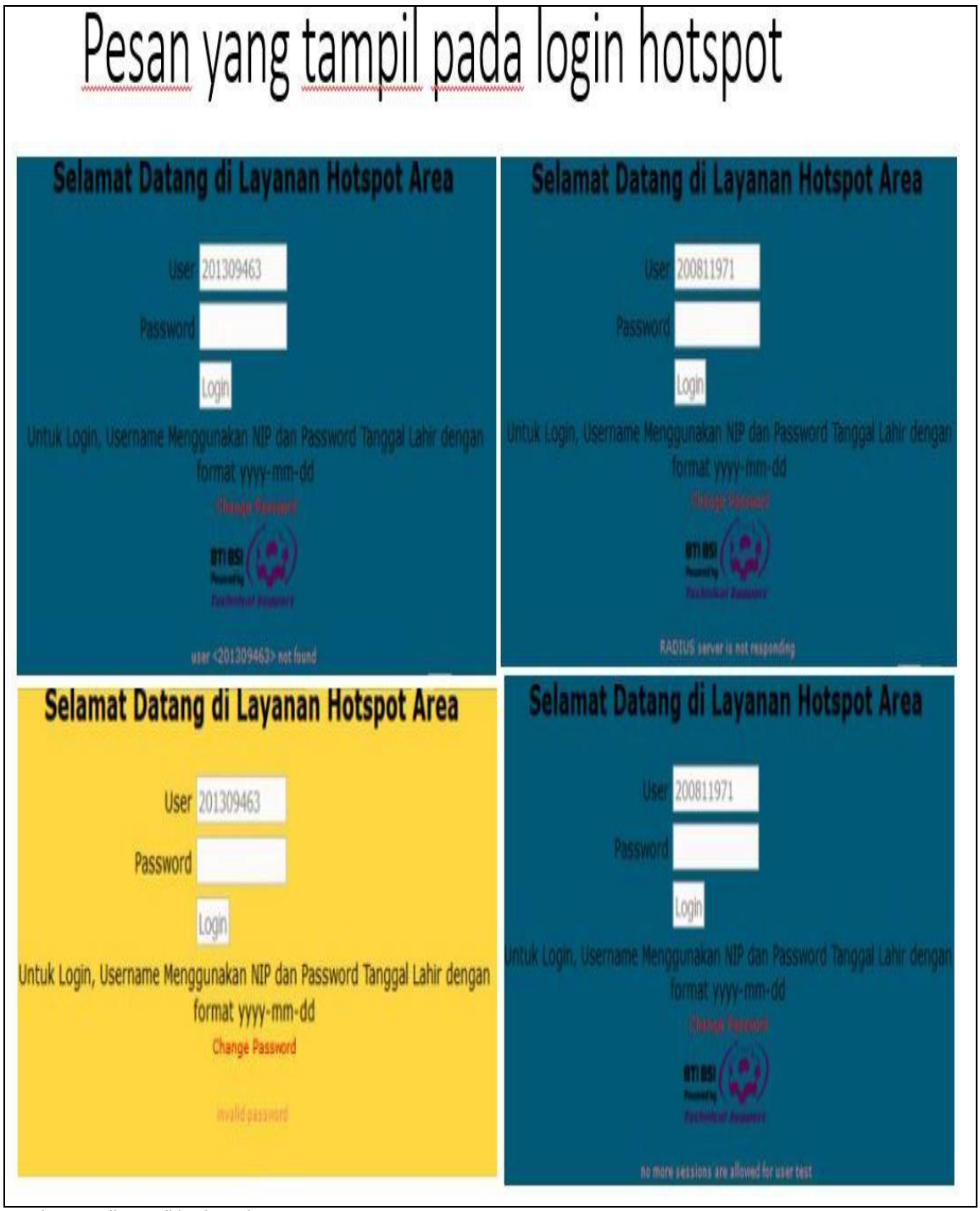
Gambar 3. Halaman *Login Hotspot*

Sedangkan untuk penggunaan internet, jika berhasil *Login hotspot* dari AP-Unifi Pro akan di direct ke laman http://bsi.ac.id. Konfigurasi *radius* pada mikrotik kampus untuk *Login* dan *hotspot* nya dengan nama domain *radius*-bsi ip address 172.16.192.10 dan *radius*-nuri ip address 172.16.192.12, keduanya dimasukkan *password*(secret) *Radius-server* pada MikroTik Cloud Core Router Kantor Pusat Bina Sarana Informatika. Port otentikasi dan accounting yang digunakan harus sesuai mengikuti port *radius* pada MikroTik kampus. *Radius server* pada

MikroTik disebut MikroTik *User Manager*, terkoneksinya *router* mikrotik yang akan mengakses *user* dan *password* legal sehingga bisa terkoneksi ke jaringan internet.

3.4. Testing

Pada tahap testing yang dilakukan adalah menguji menggunakan *user* dan *password* yang tidak terdaftar pada *radius-server*, menguji koneksi mikrotik kampus dengan *radius-server*.



Sumber: Hasil Penelitian(2018)

Gambar 4. Pesan *error* pada *Login hotspot*

E-ISSN: 2548-3412 ; 135 – 148

Pada gambar 4 adalah tampilan beberapa pesan *error* pada *Login hotspot*, antara lain ;
Pertama, *User* <20139463> *not found*, bahwa *user* 20139463 (contoh) tidak ditemukan pada *radius-server*
Kedua, *Invalid Password*, bahwa *password* yang dimasukkan salah
Ketiga, *RADIUS Server is not responding*, bahwa tidak terjadi koneksi antara MikroTik kampus dengan MikroTik Cloud Core Router sebagai *radius-server*.
Keempat, *No more sessions are allowed for user test*, bahwa tidak ada session lebih yang diijinkan untuk *user* test, artinya satu *user* hanya untuk satu perangkat yang *Login hotspot*.

3.5. Manajemen

Selanjutnya pada tahap manajemen adalah monitoring *user* yang telah terkoneksi ke *hotspot*. Terdapat dua antarmuka menggunakan port 80 atau http untuk konfig *radius server* yang terdapat di Kantor Pusat BSI:
http://172.16.192.10/*userman* untuk domain *radius*-bsi
http://172.16.192.12/*userman* untuk domain *radius*-nuri

Data mikrotik kampus yang diijinkan masuk ke *radius*-bsi *server* MUM (MikroTik *User Manager*) adalah:
[taufik@*Radius*_Bsi] > *tool user-Manager router pr detail without-paging*
Flags: X - disabled
0 customer=admin name="kampus" ip-address=12.12.0.2 shared-secret="Password" log=auth-fail use-coa=yes coa-port=3799
1 customer=admin name="radius-bsi" ip-address=127.0.0.1 shared-secret="Password" log=auth-fail use-coa=yes coa-port=3799
2 customer=admin name="hotspotdwsa" ip-address=172.16.155.119 shared-secret="Password" log=auth-ok,auth-fail,acct-ok,acct-fail use-coa=yes coa-port=3799
3 customer=admin name="bandung" ip-address=172.16.160.1 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
4 customer=admin name="Bogor" ip-address=172.16.80.254 shared-secret="Password" log=auth-ok,auth-fail use-coa=no coa-port=3799
5 customer=admin name="Pontianak" ip-address=172.16.156.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
6 customer=admin name="kramat18" ip-address=172.16.28.1 shared-secret="Password" log=auth-ok,auth-fail use-coa=no coa-port=3799
7 customer=admin name="Bekasi" ip-address=172.16.168.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
8 customer=admin name="Cileubut" ip-address=172.16.132.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
9 customer=admin name="BSD" ip-address=172.16.136.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
10 customer=admin name="Cengkareng" ip-address=172.16.96.252 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
11 customer=admin name="Cibitung" ip-address=172.16.188.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
12 customer=admin name="Cikampek" ip-address=172.16.88.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
13 customer=admin name="Cikarang" ip-address=172.16.255.26 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
14 customer=admin name="Dewi Sartika B" ip-address=172.16.255.166 shared-secret="Password" log=auth-fail use-coa=yes coa-port=3799
15 customer=admin name="Fatmawati" ip-address=172.16.8.1 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
16 customer=admin name="Ciledug B" ip-address=172.16.100.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
17 customer=admin name="Jatiwaringin" ip-address=172.16.255.10 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
18 customer=admin name="Jogja" ip-address=172.16.120.253 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700

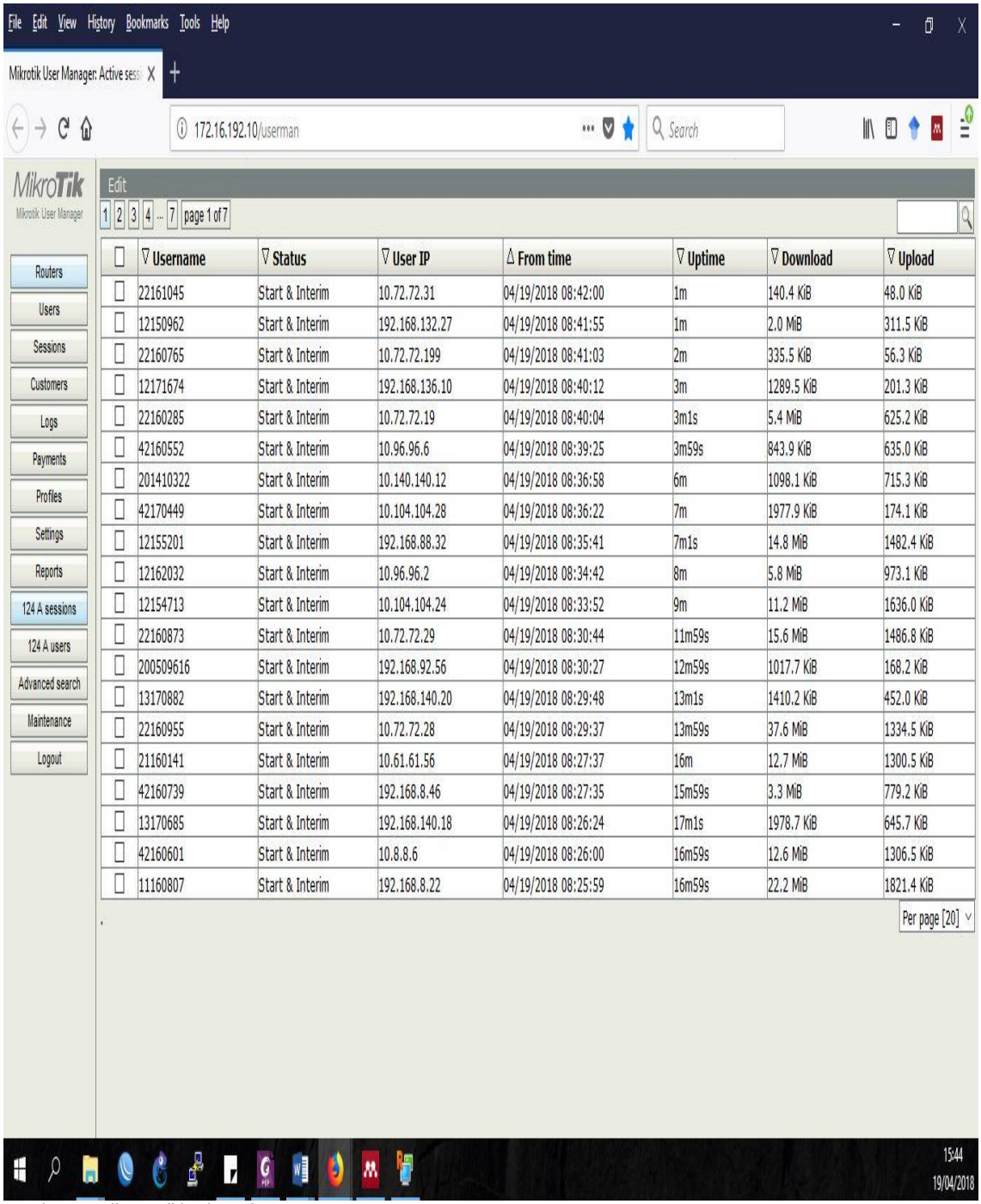
19 customer=admin name="Kaliabang" ip-address=172.16.196.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
20 customer=admin name="Kalimalang" ip-address=172.16.104.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
21 customer=admin name="Karawang" ip-address=172.16.84.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
22 customer=admin name="Margonda" ip-address=172.16.255.86 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
23 customer=admin name="Pemuda" ip-address=172.16.255.194 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
24 customer=admin name="Purwokerto" ip-address=172.16.13.3 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
25 customer=admin name="Salemba 22" ip-address=172.16.255.94 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
26 customer=admin name="Salemba 45" ip-address=172.16.255.98 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
27 customer=admin name="Sukabumi" ip-address=172.16.144.1 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
28 customer=admin name="Cemerlang" ip-address=172.16.13.10 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
29 customer=admin name="TNA" ip-address=172.16.48.1 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
30 customer=admin name="TNB" ip-address=172.16.52.1 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
31 customer=admin name="Tasik" ip-address=172.16.108.1 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
32 customer=admin name="Tegal" ip-address=172.16.13.6 shared-secret="Password" log=auth-fail use-coa=no coa-port=1700
33 customer=admin name="Warung Jati" ip-address=172.16.13.7 shared-secret="Password" log=auth-fail use-coa=no coa-port=17000

Data router kampus yang didaftarkan pada radius-nuri server pada kantor pusat Bina Sarana Informatika sebagai berikut:
[taufik@Radius-Nuri] > tool user-Manager router pr detail without-paging
Flags: X - disabled
0 customer=admin name="radius-nuri" ip-address=127.0.0.1 shared-secret="Password" log=auth-ok,auth-fail,acct-ok,acct-fail use-coa=yes coa-port=3799
1 customer=admin name="kramat18" ip-address=172.16.28.1 shared-secret="Password" log=auth-ok,auth-fail,acct-ok,acct-fail use-coa=no coa-port=3799
2 customer=admin name="kampus" ip-address=13.13.0.2 shared-secret="Password" log=auth-ok,auth-fail,acct-ok,acct-fail use-coa=no coa-port=3799
3 customer=admin name="wrj" ip-address=172.16.164.1 shared-secret="Password" log=auth-ok,auth-fail,acct-ok,acct-fail use-coa=no coa-port=3799
4 customer=admin name="TNB" ip-address=172.16.52.1 shared-secret="Password" log=auth-ok,auth-fail,acct-ok,acct-fail use-coa=no coa-port=3799
5 customer=admin name="Ciledug B" ip-address=172.16.100.254 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799
6 customer=admin name="Jatiwaringin" ip-address=172.16.255.10 shared-secret="Password" log=auth-fail use-coa=no coa-port=3799

User aktif pada *radius*, Setelah proses input *router* mikrotik pada *radius-server*, maka *user* berhasil *Login* akan masuk ke Session-*user* dan dapat dikatakan sebagai *user* aktif. *User* berhasil *Login* jika *user* dan *password* benar terdapat pada *radius-server*, kemudian *user* dan *password* digunakan pada 1 perangkat (laptop atau gadget). Jika akan berpindah perangkat, maka *user* terlebih dahulu harus logout pada perangkat yang sedang digunakan.

E-ISSN: 2548-3412 ; 135 – 148

User berhasil *Login* masuk pada *radius-server* seperti pada gambar 5, *user Login* pada *radius*-bsi. Pada *radius*-nuri akan disimpan dan ditampilkan jika *user* berhasil *Login* pada ip 172.16.192.12/*userman* pada tab *session*.



Username	Status	User IP	From time	Uptime	Download	Upload
22161045	Start & Interim	10.72.72.31	04/19/2018 08:42:00	1m	140.4 KiB	48.0 KiB
12150962	Start & Interim	192.168.132.27	04/19/2018 08:41:55	1m	2.0 MiB	311.5 KiB
22160765	Start & Interim	10.72.72.199	04/19/2018 08:41:03	2m	335.5 KiB	56.3 KiB
12171674	Start & Interim	192.168.136.10	04/19/2018 08:40:12	3m	1289.5 KiB	201.3 KiB
22160285	Start & Interim	10.72.72.19	04/19/2018 08:40:04	3m1s	5.4 MiB	625.2 KiB
42160552	Start & Interim	10.96.96.6	04/19/2018 08:39:25	3m59s	843.9 KiB	635.0 KiB
201410322	Start & Interim	10.140.140.12	04/19/2018 08:36:58	6m	1098.1 KiB	715.3 KiB
42170449	Start & Interim	10.104.104.28	04/19/2018 08:36:22	7m	1977.9 KiB	174.1 KiB
12155201	Start & Interim	192.168.88.32	04/19/2018 08:35:41	7m1s	14.8 MiB	1482.4 KiB
12162032	Start & Interim	10.96.96.2	04/19/2018 08:34:42	8m	5.8 MiB	973.1 KiB
12154713	Start & Interim	10.104.104.24	04/19/2018 08:33:52	9m	11.2 MiB	1636.0 KiB
22160873	Start & Interim	10.72.72.29	04/19/2018 08:30:44	11m59s	15.6 MiB	1486.8 KiB
200509616	Start & Interim	192.168.92.56	04/19/2018 08:30:27	12m59s	1017.7 KiB	168.2 KiB
13170882	Start & Interim	192.168.140.20	04/19/2018 08:29:48	13m1s	1410.2 KiB	452.0 KiB
22160955	Start & Interim	10.72.72.28	04/19/2018 08:29:37	13m59s	37.6 MiB	1334.5 KiB
21160141	Start & Interim	10.61.61.56	04/19/2018 08:27:37	16m	12.7 MiB	1300.5 KiB
42160739	Start & Interim	192.168.8.46	04/19/2018 08:27:35	15m59s	3.3 MiB	779.2 KiB
13170685	Start & Interim	192.168.140.18	04/19/2018 08:26:24	17m1s	1978.7 KiB	645.7 KiB
42160601	Start & Interim	10.8.8.6	04/19/2018 08:26:00	16m59s	12.6 MiB	1306.5 KiB
11160807	Start & Interim	192.168.8.22	04/19/2018 08:25:59	16m59s	22.2 MiB	1821.4 KiB

Sumber: Hasil Penelitian(2018)

Gambar 5. Session dan Active *User* pada *Radius-server*

Hasil *user hotspot* yang berhasil *Login* masuk ke *radius-server* dan *router* mikrotik kampus, berikut *user hotspot* yang berhasil *Login* pada mikrotik kampus:
[taufik@MT_Kampus] > *ip hotspot active pr detail Flags: R - radius, B - blocked*

0 R server=hs-vlan500 user="199707225" address=10.8.8.13 mac-address=DC:85:DE:46:3A:EA Login-by="http-chap" uptime=1m24s session-time-left=58m36s
1 R server=hs-vlan500 user="11142421" address=10.8.8.22 mac-address=78:E4:00:00:D2:A0 Login-by="http-chap" uptime=53m37s session-time-left=6m23s
2 R server=hs-vlan500 user="12152660" address=10.8.8.24 mac-address=1C:77:F6:EC:C2:47 Login-by="http-chap" uptime=21m37s session-time-left=38m23s
3 R server=hs-vlan500 user="42161059" address=10.8.8.28 mac-address=C4:0B:CB:FF:5C:4E Login-by="http-chap" uptime=5m50s session-time-left=54m10s

Konfigurasi *Radius* agar dapat monitoring pada mikrotik kampus sebagai berikut:

```
[taufik@MT_Kampus] > radius monitor
numbers: 0
         pending: 0
        requests: 58373
         accepts: 54126
         rejects: 1470
         resends: 8344
        timeouts: 2777
    bad-replies: 17  last-request-rtt: 50ms


[taufik@MT_Kampus] > radius monitor
numbers: 1
         pending: 0
        requests: 24714
         accepts: 23500
         rejects: 586
         resends: 1882
        timeouts: 628
    bad-replies: 2  last-request-rtt: 80ms
```

Pada MikroTik kampus *radius* monitor akan memiliki hasil yang berbeda karena bergantung dari banyak nya *user* yang menggunakan *hotspot*, berhasil *Login* atau status *user* pun mempengaruhi monitoring *radius*.

4. Kesimpulan

Dengan *user* dan *password* pada dua *radius server* yaitu *radius*-bsi dan *radius*-nuri, *split user domain* pada mikrotik kampus dan *Tunnel* EoIP sebagai jaringan vpn nya, mahasiswa, staf dan dosen dapat *Login* hostspot. *User Login* dengan *user*name dan *password* yang terdaftar *radius server* masuk ke *user* aktif *hotspot* pada MikroTik RB1000 Kampus dan *Session User Radius Server* MikroTik Cloud Core Router *user Manager* pada Kantor Pusat Bina Sarana Informatika. Demikian pengguna *hotspot* dapat termonitoring dan manajemen *user hotspot* dengan dua *radius server* dapat beroperasi bersamaan pada satu MikroTik pada Kampus. Pengembangan untuk penelitian selanjutnya EoIP *Tunnel* dapat diriset dengan hal yang lainnya seperti monitoring syslog.

Referensi

Cristescu GC, Croitoru V, Sorici V. 2016. Implementing an AAA-RADIUS solution based on legacy authentication protocols. 2016 12th Int. Symp. Electron. Telecommun. ISETC 2016 - Conf. Proc.: 75–80.

Golbeck J. 2017. User Concerns with Personal Routers Used as Public Wi-fi hotspots. 571–576.

Hermaduanti N, Riadi I. 2016. Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN. J. Theor. Appl. Inf. Technol. 93: 287–296.

Kuswanto H. 2017. Sistem Autentikasi Hotspot Menggunakan Radius Server Mikrotik Router. INFORMATICS Educ. Prof. 2: 43–50.

Pauzhi W, Coronel J. 2015. Security for WISP through Mikrotik equipment Mikrotik). In: 2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON). Santiago, Chile, p 229–233.

E-ISSN: 2548-3412 ; 135 – 148

Yu Y, Park K, Kim D. 2018. Study On Port Based On User Authentication System Using IEEE 802.1X. J. Theor. Appl. Inf. Technol. 96: 1711–1721.