LAPORAN

PENELITIAN MANDIRI

SENTRALISASI MANAJEMEN HOTSPOT MENGGUNAKAN TRANSPARENT BRIDGE EOIP OVER SSTP

Oleh

I PUTU HARIYADI, M.KOM (0827068001)

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) BUMIGORA MATARAM

DESEMBER 2016

HALAMAN PENGESAHAN

Judul	:	Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge EoIP over SSTP
Peneliti/Pelaksana		
Nama Lengkap	:	I Putu Hariyadi, M.Kom
NIDN	:	0827068001
Jabatan Fungsional	:	Asisten Ahli
Program Studi	:	Teknik Informatika
Nomor HP	:	081936733568
Alamat surel (email)	:	putu.hariyadi@stmikbumigora.ac.id
Perguruan Tinggi	:	STMIK Bumigora

Mataram, 30 Desember 2016

Mengetahui
Ketua LPPM

(Ahmat Adil, M.Sc)
NIP. 96.6.63

Peneliti

(I Putu Hariyadi, M.Kom)
NIDN. 0827068001

RINGKASAN

STMIK Bumigora merupakan perguruan tinggi komputer pertama di provinsi Nusa Tenggara Barat (NTB). Untuk mendukung operasional kampus dan kegiatan perkuliahan baik di ruang kelas dan laboratorium maka STMIK Bumigora membangun infrastruktur jaringan kampus dan menyediakan koneksi Internet bagi civitas akademika. Terdapat 11 titik *hotspot* yang tersebar di lingkungan kampus untuk mempermudah civitas akademika dalam memanfaatkan layanan Internet melalui koneksi nirkabel. Keseluruhan infrastruktur jaringan kampus dan sistem informasi perguruan tinggi dikelola oleh bagian Pusat Teknologi Informasi dan Komunikasi (PusTIK).

Saat ini bagian PusTIK memiliki beberapa permasalahan terkait manajemen dan *monitoring* layanan hotspot kampus antara lain semakin banyaknya titik hotspot yang harus dikelola dengan lokasi yang tersebar di berbagai router Mikrotik membuat proses manajemen hotspot menjadi kompleks, tidak efektif dan efisien. Disamping itu penambahan perangkat *Access Point (AP)* baru untuk mendukung titik hotspot baru memerlukan pengaktifan fitur hotspot pada router Mikrotik yang terhubung secara langsung ke AP. Monitoring atau pengawasan user hotspot yang aktif membutuhkan pengaksesan ke masing-masing router Mikrotik yang mengelola hotspot sehingga antarmukanya terpisah untuk setiap router.

Sentralisasi manajemen *hotspot* kampus STMIK Bumigora menggunakan *transparent bridge EoIP over SSTP* dapat membantu mengatasi permasalahan yang dihadapi oleh bagian PusTIK. *Ethernet over IP (EoIP) Tunneling* merupakan protokol *Mikrotik RouterOS* yang membuat tunnel *Ethernet* diantara *router-router* diatas koneksi IP. *EoIP* tunnel dibangun diatas *tunnel SSTP (EoIP over SSTP)* yang berjenis *Site-to-Site*. *SSTP* merupakan bentuk baru dari *Virtual Private Network (VPN) tunnel* yang menyediakan mekanisme untuk mengenkapsulasi trafik *Point-to-Point Protocol (PPP)* melalui jalur *Secure Socket Layer (SSL)* dari protokol *Hypertext Transfer Protocol Secure (HTTPS).* Selain itu agar hotspot berada dalam satu jaringan maka digunakan fitur *bridging* dari *Mikrotik RouterOS* dengan port anggota berupa *interface EoIP* dan *interface router* yang terhubung secara langsung ke perangkat AP sehingga manajemen dan *monitoring hotspot* terpusat pada satu *router*.

Metodologi penelitian yang digunakan adalah *Network Development Life Cycle (NDLC)*. Dari 6 tahapan yang terdapat pada NDLC, peneliti hanya menggunakan 3 tahapan pertama yaitu *analysis*, *design*, dan *simulation prototyping*. Rancangan jaringan ujicoba menggunakan 8 router, 4 *Access Point (AP)* dan 4 komputer *wireless client*. Skenario ujicoba meliputi manajemen user dan *monitoring user hotspot* di router sentral dan koneksi Internet dari 4 komputer *wireless client* ke setiap AP.

Berdasarkan hasil ujicoba dapat disimpulkan, sentralisasi manajemen dan *monitoring hotspot* dapat dibangun menggunakan teknik *transparent bridge tunnel EoIP over SSTP*. Alamat IP pada *interface SSTP* digunakan sebagai referensi *local* dan *remote address* pembentukan *tunnel EoIP over SSTP*. Penerapan *bridging* pada *interface EoIP* dan *interface* yang terhubung ke perangkat *Access Point* membentuk satu jaringan secara logical sehingga konfigurasi layanan hotspot dapat dilakukan secara terpusat pada satu router.

Kata kunci: *Mikrotik, OSPF, Hotspot, SSTP, EoIP, Bridge*

PRAKATA

Puji syukur peneliti panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmatnya, sehingga **"Laporan Penelitian Mandiri"** ini dapat terselesaikan. Laporan ini memuat tentang hasil dari penelitian yang telah dilakukan, kesimpulan dan saran terkait proses penelitian yang telah dilakukan. Tidak lupa peneliti mengucapkan terimakasih kepada STMIK Bumigora sehingga penelitian ini dapat terlaksana.

Mataram, 30 Desember 2016

Peneliti

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1. Latar Belakang

STMIK Bumigora merupakan perguruan tinggi komputer pertama di provinsi Nusa Tenggara Barat (NTB). Untuk mendukung operasional kampus dan kegiatan perkuliahan baik di ruang kelas dan laboratorium maka STMIK Bumigora membangun infrastruktur jaringan kampus baik menggunakan media kabel maupun nirkabel dan menyediakan koneksi Internet bagi civitas akademika. Terdapat beragam perangkat yang digunakan untuk pembangunan infrastruktur jaringan kampus meliputi 3 unit router Cisco 1841 sebagai router backbone, 1 router Mikrotik RB1000 sebagai gateway ke Internet, 1 router Mikrotik RB1100AHx2 dan 5 router Mikrotik beragam tipe yang tersebar diberbagai lokasi untuk menangani hotspot kampus, 3 Cisco Switch Managable SRW224G4-K9-EU untuk menyediakan layanan *Virtual Local Area Network (VLAN)*. Koneksi Internet menggunakan Internet Service Provider (ISP) Telkom dengan jenis layanan *Indihome* yang memiliki kapasitas *bandwidth* 50 Mbps dan *dedicated connection Astinet* dengan *bandwidth* 1 Mbps. Terdapat 11 titik hotspot yang tersebar di lingkungan kampus untuk mempermudah civitas akademika dalam memanfaatkan layanan Internet melalui koneksi nirkabel. Keseluruhan infrastruktur jaringan kampus dan sistem informasi perguruan tinggi dikelola oleh bagian Pusat Teknologi Informasi dan Komunikasi (PusTIK).

Saat ini bagian PusTIK memiliki beberapa permasalahan terkait manajemen dan *monitoring* layanan hotspot kampus antara lain semakin banyaknya titik hotspot yang harus dikelola dengan lokasi yang tersebar di berbagai router Mikrotik membuat proses manajemen

hotspot menjadi kompleks, tidak efektif dan efisien. Disamping itu penambahan perangkat *Access Point (AP)* baru untuk mendukung titik hotspot baru memerlukan pengaktifan fitur hotspot pada router Mikrotik yang terhubung secara langsung ke AP. Monitoring atau pengawasan user hotspot yang aktif membutuhkan pengaksesan ke masing-masing router Mikrotik yang mengelola hotspot sehingga antarmukanya terpisah untuk setiap router.

PusTIK memiliki harapan terdapat satu sistem yang dapat memusatkan manajemen hotspot kampus sehingga dapat dikelola menggunakan satu antarmuka winbox meskipun hotspot tersebar di banyak router Mikrotik yang tersebar di berbagai lokasi. Selain itu proses manajemen user hotspot dan pengawasan user hotspot yang aktif dapat dimonitoring secara terpusat serta penambahan titik hotspot baru dapat dilakukan dengan konfigurasi minimal sehingga lebih efektif dan efisien.

Sentralisasi manajemen *hotspot* kampus STMIK Bumigora menggunakan *transparent bridge EoIP over SSTP* dapat membantu mengatasi permasalahan yang dihadapi oleh bagian PusTIK. *Ethernet over IP (EoIP) Tunneling* merupakan protokol *Mikrotik RouterOS* yang membuat tunnel *Ethernet* diantara *router-router* diatas koneksi IP [8]. Namun EoIP tidak mendukung fitur keamanan sehingga tunnel EoIP perlu dilewatkan pada tunnel *Secure Socket Tunneling Protocol (SSTP)*. *SSTP* merupakan bentuk baru dari *Virtual Private Network (VPN) tunnel* yang menyediakan mekanisme untuk mengenkapsulasi trafik *Point-to-Point Protocol (PPP)* melalui jalur *Secure Socket Layer (SSL)* dari protokol *Hypertext Transfer Protocol Secure (HTTPS)* [1]. Pengaktifan fitur *bridging* pada *interface EoIP* dan interface *router MikroTik* yang terhubung secara langsung ke perangkat AP membuat jaringan hotspot yang tersebar di beda jaringan dapat digabungkan menjadi satu network secara logical. *Brigde* merupakan perangkat yang digunakan untuk menghubungkan dua jaringan *Ethernet* terpisah menjadi satu *Ethernet* yang

diperluas [6]. Selain itu pembuatan hotspot hanya perlu dilakukan pada interface bridge di satu router yang ditunjuk sebagai sentral yaitu dalam hal ini di router yang difungsikan sebagai *gateway* ke *Internet*.

Dengan adanya sentralisasi manajemen hotspot maka dapat memberikan manfaat berupa pengaktifan fitur hotspot hanya dilakukan pada router yang dipilih sebagai sentral dan proses penambahan titik hotspot baru tidak memerlukan pengaturan hotspot pada router yang terhubung secara langsung pada perangkat AP tersebut. Selain itu manajemen user hotspot meliputi penambahan, perubahan, penghapusan, penggantian sandi, pengawasan user hotspot yang aktif dapat dilakukan dalam satu antarmuka winbox atau terpusat sehingga lebih efektif dan efisien,

1.2. Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah "Bagaimana desain dan implementasi sentralisasi manajemen *hotspot* kampus STMIK Bumigora menggunakan *transparent bridging EoIP over SSTP*?".

1.3. Batasan Masalah

Adapun batasan permasalahan yang diketengahkan pada penelitian ini adalah sebagai berikut:

1. Lokasi penelitian di STMIK Bumigora.
2. Rancangan jaringan ujicoba terdiri dari 8 router dan 4 AP serta 4 komputer Client.
3. Pengujian menggunakan perangkat meliputi:
    a. Router menggunakan Mikrotik RB951Ui-2ND dengan RouterOS versi 6.37.3.
    b. AP menggunakan TP-Link TL-WA5210G.
    c. Sistem operasi pada komputer client adalah Microsoft Windows 10.

4. Protokol *tunneling* menggunakan *SSTP* dengan jenis *Site-to-Site* dan *EoIP* yang dilewatkan pada *SSTP (EoIP over SSTP)*.
5. Menggunakan fitur *bridging* dari *Mikrotik RouterOS* dengan port anggota berupa interface EoIP dan interface router yang terhubung secara langsung ke perangkat AP sehingga hotspot berada dalam satu jaringan.

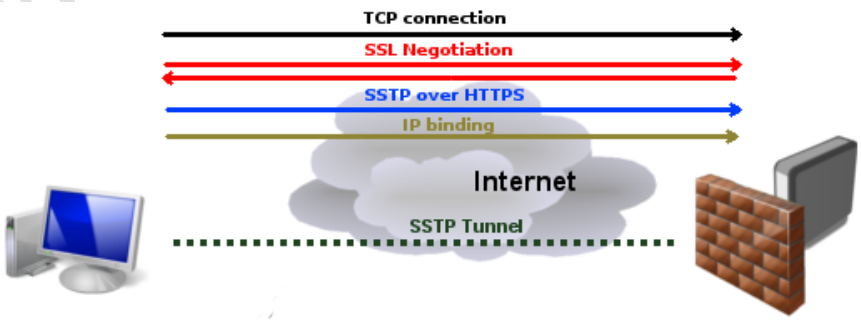
BAB II

TINJAUAN PUSTAKA

2.1. Secure Socket Tunneling Protocol

Secure Socket Tunneling Protocol (SSTP) merupakan bentuk baru dari *Virtual Private Network (VPN) tunnel* dengan fitur yang memungkinkan untuk melewatkan trafik melalui firewall yang memblokir trafik *Point-to-Point Tunneling Protocol (PPTP)* dan *Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPSec)*. SSTP menyediakan mekanisme untuk mengenkapsulasi trafik *Point-to-Point Protocol (PPP)* melalui jalur *Secure Socket Layer (SSL)* dari protokol *Hypertext Transfer Protocol Secure (HTTPS)*. Penggunaan PPP menyediakan dukungan untuk metode otentikasi yang tangguh seperti *Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)*. Penggunaan HTTPS berarti trafik akan melalui *Transmission Control Protocol (TCP)* port 443, port yang umum digunakan untuk mengakses web. SSL menyediakan keamanan tingkat *transport* dengan peningkatan negosiasi kunci, enkripsi dan pengecekan integritas [1].

Proses Koneksi SSTP



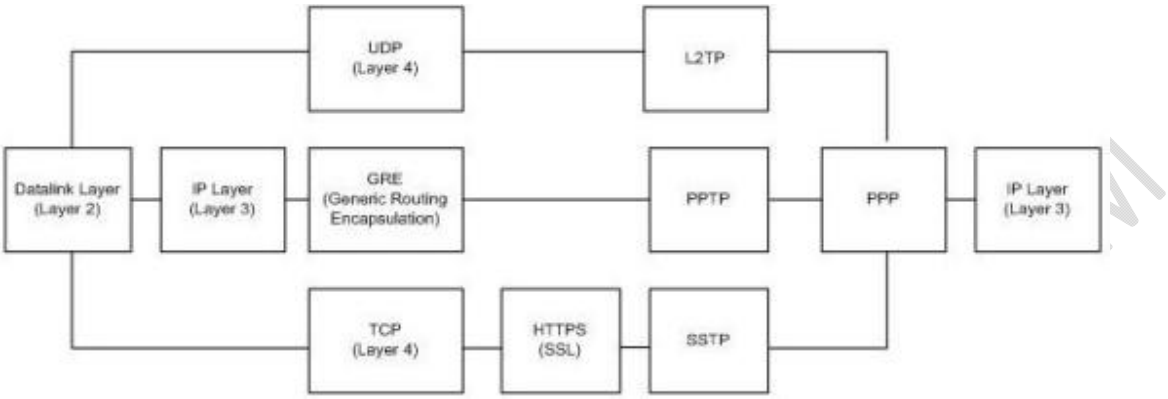
Gambar 2.1 Mekanisme Koneksi SSTP [2]

Tahapan proses koneksi SSTP adalah sebagai berikut [1]:

1. *SSTP Client* membentuk koneksi TCP dengan *SSTP Server* menggunakan TCP port yang secara dinamis dialokasikan pada SSTP Client dan TCP port 443 pada *SSTP Server*.
2. *SSTP Client* mengirim *SSL Client-Hello message* yang mengindikasikan *SSTP Client* ingin membentuk sesi SSL dengan *SSTP Server*.
3. *SSTP Server* mengirim *computer certificate* miliknya ke *SSTP Client*.
4. *SSTP Client* memvalidasi *computer certificate*, menentukan metode enkripsi untuk sesi SSL, membuat kunci sesi SSL dan mengenkripsi dengan *public key* dari *SSTP Server Certificate* dan kemudian mengirimkan kunci sesi SSL dalam bentuk terenkripsi ke *SSTP server*.
5. *SSTP Server* mendekripsi kunci sesi SSL yang terenkripsi dengan *private key* dari *computer certificate*. Keseluruhan komunikasi berikutnya antara *SSTP Client* dan *SSTP Server* dienkripsi dengan metode enkripsi yang telah dinegosiasi dan kunci sesi SSL.
6. *SSTP Client* mengirim pesan permintaan melalui *HTTP over SSL* ke *SSTP Server*.
7. *SSTP Client* menegosiasi sebuah *SSTP tunnel* dengan *SSTP Server*.
8. *SSTP Client* menegosiasi koneksi PPP dengan *SSTP Server*. Negosiasi ini meliputi mengotentikasi *credentials* pengguna menggunakan metode otentikasi PPP dan mengatur *setting* untuk trafik IPv4 atau IPv6.
9. *SSTP Client* mulai mengirim trafik IPv4 atau IPv6 melalui jalur PPP.

Karakteristik dari arsitektur protocol VPN ditunjukkan pada gambar 2.2. Terlihat pada gambar tersebut bahwa SSTP mempunyai *header* tambahan jika dibandingkan dengan dua protocol VPN lainnya. Hal ini karena terdapat enkapsulasi HTTP sebagai tambahan pada *SSTP header*. L2TP

dan PPTP tidak mempunyai *header* pada lapisan *application* yang mengenkapsulasi komunikasi [3].



Gambar 2.2 Arsitektur Protokol VPN [3]

2.2. MikroTik RouterOS

Mikrotik merupakan perusahaan Latvia yang didirikan pada tahun 1996 untuk mengembangkan sistem *router* dan *wireless Internet Service Provider (ISP)*. Pada tahun 1997, Mikrotik membuat sistem operasi RouterOS yang menyediakan stabilitas, fleksibilitas untuk semua jenis data *interfaces* dan *routing* [4]. RouterOS dapat diinstalasi pada *Personal Computer (PC)* yang dapat digunakan untuk menjadikan komputer sebagai *router network* yang handal, mencakup berbagai fitur yang dibuat untuk *IP network* dan jaringan *wireless*, cocok digunakan oleh ISP dan provider hotspot [5]. Selain itu pada tahun 2002, *Mikrotik* membuat hardware *RouterBoard* yang menggunakan sistem operasi RouterOS [4].

2.3. Bridge

Brigde merupakan perangkat yang digunakan untuk menghubungkan dua jaringan *Ethernet* terpisah menjadi satu *Ethernet* yang diperluas [6]. *Bridge* menghubungkan dan mentransfer data antar *Local Area Network (LAN)*. Terdapat 4 (empat) jenis *bridge* antara lain:[7]

a) *Transparent Bridging*

Utamanya ditemukan pada lingkungan *Ethernet* dan kebanyakan digunakan untuk menjembatani jaringan dengan media yang sama. *Bridge* menyimpan table alamat tujuan dan interface keluar (*outbound*).

b) *Source-Route Bridging (SRB)*

Utamanya ditemukan pada lingkungan *Token Ring*. *Bridge* hanya meneruskan frame berdasarkan pada indikator routing yang terdapat pada *frame*. *End station* bertanggungjawab untuk menentukan dan memelihara table dari alamat tujuan dan indikator routing.

c) *Translational Bridging*

Digunakan untuk menjembatani data diantara jenis media yang berbeda. Umumnya digunakan antara *Ethernet* ke *FDDI* atau *Token Ring* ke *Ethernet*.

d) *Source-Route Translational Bridging (SR/TLB)*

Gabungan dari *source-route bridging* dan *transparent bridging* yang memungkinkan komunikasi di lingkungan campuran *Ethernet* dan *Token Ring*. *Translational bridging* tanpa indikator routing antara *Token Ring* dan *Ethernet* disebut juga SR/TLB.

Bridging terjadi pada lapisan *data-link*, yang mengontrol aliran data, menangani kegagalan transmisi, menyediakan pengalamatan fisikal, dan mengatur akses ke media fisik. *Bridge* menganalisa *frame* yang masuk, membuat keputusan untuk meneruskan berdasarkan *frame* tersebut, dan meneruskan *frame* ke tujuannya. Terkadang, seperti SRB, *frame* mengandung keseluruhan jalur ke tujuan. Pada kasus lainnya, seperti *transparent bridging*, *frame* diteruskan satu hop satu waktu menuju tujuan. *Bridge* dapat berupa *local* atau *remote*. *Local bridge*

menyediakan koneksi langsung antara banyak segmen LAN di area yang sama. *Remote bridge* menghubungkan segmen LAN di area yang berbeda, umumnya melalui jalur telekomunikasi.[7]

2.4. Ethernet Over Internet Protocol

Ethernet over IP (EoIP) Tunneling adalah protokol Mikrotik RouterOS yang membuat tunnel Ethernet diantara router-router diatas koneksi IP. Tunnel EoIP dapat berjalan diatas tunnel *IPIP*, *PPTP* atau tunnel lainnya yang memiliki kemampuan mentransport IP. Ketika fungsi *bridging* diaktifkan di router maka semua trafik ethernet (protokol ethernet) akan dibridge seperti ketika terdapat interface fisik ethernet dan kabel yang menghubungkan diantara dua router jika bridging diaktifkan. Protokol ini membuat beberapa skema jaringan yang mungkin dengan interface EoIP yaitu antara lain:[8]

a) Mem-*bridge* LAN melalui Internet.
b) Mem-*bridge* LAN melalui tunnel yang terenkripsi.
c) Mem-*bridge* LAN melalui jaringan wireless ad-hoc 802.11b.

Protocol EoIP mengenkapsulasi *frame Ethernet* pada paket *GRE (IP Protocol number 43)* sama seperti PPTP dan mengirimkannya ke sisi *remote* dari *tunnel EoIP* [8].

2.5. MikroTik Internet Protocol Hotspot

Internet Protocol (IP) Hotspot merupakan sebuah fitur yang terdapat pada *router Mikrotik* yang dapat digunakan sebagai mekanisme untuk mengotentikasi & mengotorisasi pengguna ketika mengakses sumber daya jaringan. *IP Hotspot* tidak menyediakan fitur enkripsi pada trafik. Untuk melakukan login, pengguna dapat menggunakan browser apapun [9].

Mikrotik Hotspot Gateway menyediakan otentikasi bagi client sebelum mengakses jaringan public. Adapun fitur-fitur dari *Hotspot Gateway* adalah sebagai berikut:[10]

a) Metode otentikasi *client* yang berbeda menggunakan *local client database* pada *router* atau *remote RADIUS server*.
b) *Users Accounting* di *database* lokal pada *router* atau pada *remote RADIUS server*.
c) Sistem *wallet-garden* untuk mengijinkan akses ke halaman web tertentu tanpa otorisasi.
d) Modifikasi halaman login yang dapat digunakan untuk menampilkan informasi terkait perusahaan.
e) Perubahan alamat IP *client* secara otomatis atau *transparent* ke alamat yang valid.

BAB III

TUJUAN DAN MANFAAT PENELITIAN

3.1. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah membangun sentralisasi manajemen dan *monitoring hotspot* kampus STMIK Bumigora menggunakan transparent bridging EoIP over SSTP.

3.2. Manfaat Penelitian

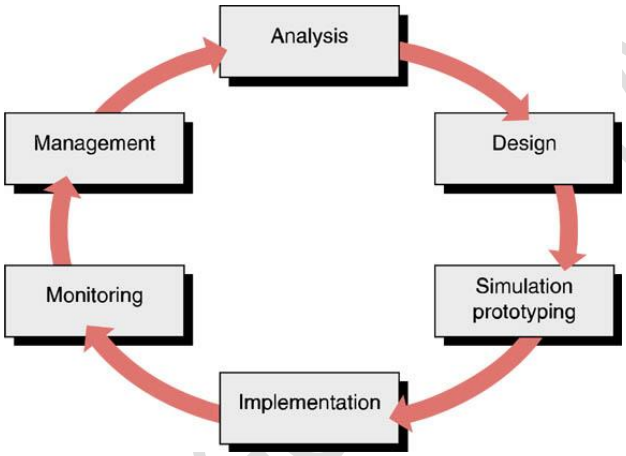
Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Membantu bagian PusTIK dalam mengkonfigurasi sentralisasi manajemen dan *monitoring hotspot* kampus STMIK Bumigora.
2. Pengaktifan fitur hotspot hanya dilakukan pada router yang dipilih sebagai sentral dan proses penambahan titik hotspot baru tidak memerlukan pengaturan hotspot pada router yang terhubung secara langsung pada perangkat AP tersebut sehingga meminimalisasi konfigurasi *hotspot* yang harus dilakukan.
3. Manajemen user hotspot meliputi penambahan, perubahan, penghapusan, penggantian sandi, pengawasan user hotspot yang aktif dapat dilakukan dalam satu antarmuka winbox atau terpusat sehingga lebih efektif dan efisien.
4. Menambah wawasan dan pengetahuan terkait sistem *hotspot*, *bridging* dan *protocol tunneling EoIP* serta *SSTP*.

BAB IV

METODE PENELITIAN

Metode penelitian yang digunakan adalah *Network Development Life Cycle (NDLC)*. NDLC terdiri dari 6 (enam) tahapan meliputi *analysis*, *design*, *simulation prototyping*, *implementation*, *monitoring* dan *management*, seperti terlihat pada gambar 3.1 [11].



Gambar 4.1 Network Development Life Cycle [11]

Dari 6 tahapan yang terdapat pada NDLC, peneliti hanya menggunakan 3 tahapan pertama yaitu *analysis*, *design* dan *simulation prototyping*.

4.1. Tahap Analysis

Pada tahap ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa terhadap topologi/jaringan yang sudah ada saat ini [12]. Sebelum dapat melakukan proses analisis maka terlebih dahulu dilakukan pengumpulan data menggunakan berbagai teknik meliputi observasi, wawancara dan dokumentasi. Berdasarkan analisis terhadap data yang telah dikumpulkan maka diperoleh hasil sebagai berikut:

1. Terdapat beragam perangkat yang digunakan untuk pembangunan infrastruktur jaringan kampus meliputi:
    a) 3 unit router Cisco 1841 sebagai router backbone,
    b) 1 router Mikrotik RB1000 sebagai gateway ke Internet,
    c) 1 router Mikrotik RB1100AHx2 dan 5 router Mikrotik beragam tipe yang tersebar diberbagai lokasi untuk menangani hotspot kampus,
    d) 3 Cisco Switch Managable SRW224G4-K9-EU untuk menyediakan layanan *Virtual Local Area Network (VLAN)*.
2. Koneksi Internet menggunakan Internet Service Provider (ISP) Telkom dengan jenis layanan *Indihome* yang memiliki kapasitas *bandwidth* 50 Mbps dan *dedicated connection Astinet* dengan *bandwidth* 1 Mbps.
3. Terdapat 11 titik hotspot yang tersebar di lingkungan kampus yang dapat dimanfaatkan oleh civitas akademika untuk mengakses Internet melalui koneksi nirkabel.
4. Bagian Pusat Teknologi Informasi dan Komunikasi (PusTIK) bertanggungjawab dalam mengelola infrastruktur jaringan kampus dan sistem informasi perguruan tinggi.
5. Bagian PusTIK memiliki beberapa permasalahan terkait manajemen dan *monitoring* layanan hotspot kampus meliputi:
    a) Proses manajemen hotspot menjadi kompleks, tidak efektif dan efisien seiring dengan semakin banyaknya titik hotspot yang harus dikelola dengan lokasi yang tersebar di berbagai router Mikrotik.
    b) Penambahan perangkat *Access Point (AP)* baru untuk mendukung titik hotspot baru memerlukan pengaktifan fitur hotspot pada router Mikrotik yang terhubung secara langsung ke AP.

c) Monitoring atau pengawasan user hotspot yang aktif membutuhkan pengaksesan ke masing-masing router Mikrotik yang mengelola hotspot sehingga antarmukanya terpisah untuk setiap router.

6. Bagian PusTIK memiliki harapan meliputi:
   a) Adanya satu sistem yang dapat memusatkan manajemen hotspot kampus sehingga dapat dikelola menggunakan satu antarmuka winbox meskipun hotspot tersebar di banyak router Mikrotik yang tersebar di berbagai lokasi.
   b) Proses manajemen user hotspot dan pengawasan user hotspot yang aktif dapat dimonitoring secara terpusat.
   c) Penambahan titik hotspot baru dapat dilakukan dengan konfigurasi minimal sehingga lebih efektif dan efisien.

Berdasarkan hasil analisis tersebut, mendorong penulis untuk melakukan penelitian tentang sentralisasi manajemen dan *monitoring hotspot* kampus STMIK Bumigora menggunakan *transparent bridge EoIP over SSTP* sebagai solusi dalam mengatasi permasalahan yang dihadapi oleh bagian PusTIK.

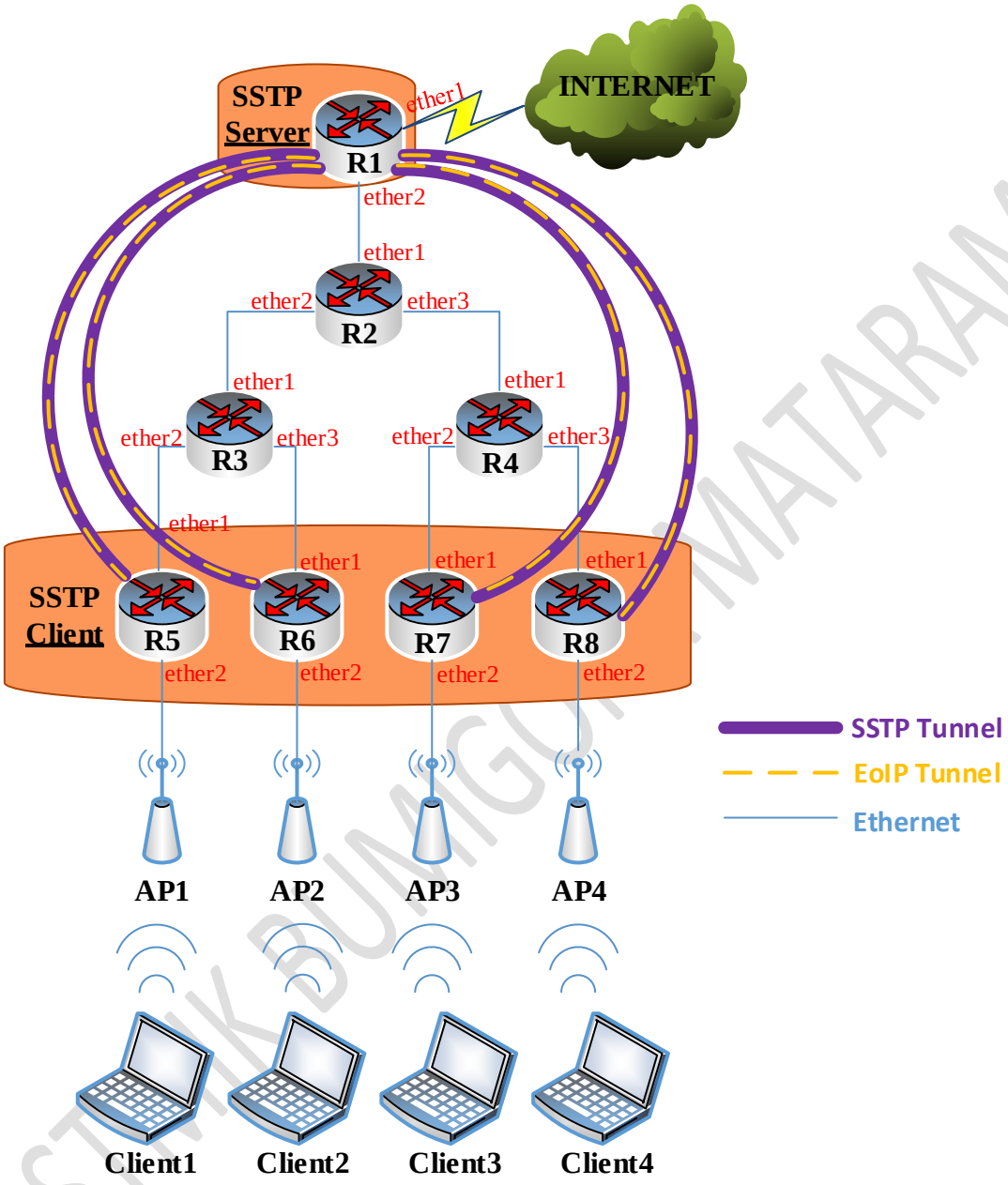
4.2. Tahap Desain

Pada tahap ini dilakukan desain atau merancang jaringan ujicoba dan rancangan pengalamatan IP serta rancangan *tunnel-id* dari *EoIP* untuk sistem sentralisasi manajemen hotspot kampus.

4.2.1. Rancangan Jaringan Ujicoba

Rancangan jaringan ujicoba untuk sistem sentralisasi manajemen *hotspot* kampus berbasis *transparent bridge EoIP over SSTP*, seperti terlihat pada gambar 4.1. Rancangan jaringan ujicoba ini terdiri dari 8 router Mikrotik (*R1-R8*), 4 perangkat *Access Point*

(*AP1-AP4*), dan 4 laptop sebagai *wireless client* (*Client1-Client4*). Pada keseluruhan router diaktifkan *routing protocol OSPF* dengan *area backbone*.



Gambar 4.2 Rancangan Jaringan Ujicoba

Router R1 ditunjuk sebagai router sentral manajemen *hotspot* dan bertindak sebagai *gateway* untuk koneksi Internet bagi jaringan lokal serta sebagai *SSTP Server*. 4 (empat) perangkat AP masing-masing terpasang pada *interface ether2* dari *router R5, R6, R7* dan *R8*. *Router R5-R8* difungsikan sebagai *SSTP Client*. *Tunnel SSTP* dibangun antara *router R1-R5,*

R1-R6, R1-R7 dan *R1-R8*, diperlihatkan menggunakan garis berwarna ungu pada gambar 4.2. Selanjutnya dibangun *tunnel EoIP* didalam *tunnel SSTP* yang telah ada antara *router R1-R5, R1-R6, R1-R7* dan *R1-R8*, diperlihatkan menggunakan garis putus-putus berwarna kuning pada gambar 4.2.

Pada *router R1* dilakukan pembuatan *interface bridge* dengan *port anggota* keseluruhan *interface EoIP*, sedangkan pada *router R5-R8* dilakukan pula pembuatan *interface bridge* dengan port anggota *interface EoIP* dan *interface ether2* yang terhubung secara langsung ke perangkat AP. *Interface bridge* digunakan untuk membuat jaringan hotspot yang tersebar di beda jaringan dapat digabungkan menjadi satu network secara logical. Selanjutnya dilakukan pengaktifan fitur hotspot hanya pada router sentral.

4.2.2. Rancangan Pengalamatan IP

Pengalamatan IP untuk keseluruhan jaringan ujicoba menggunakan alamat *network Class* A yaitu 10.0.0.0/8 yang di *subnetting* sesuai kebutuhan jumlah pengalamatan per subnetnya, seperti terlihat pada tabel 4.1.

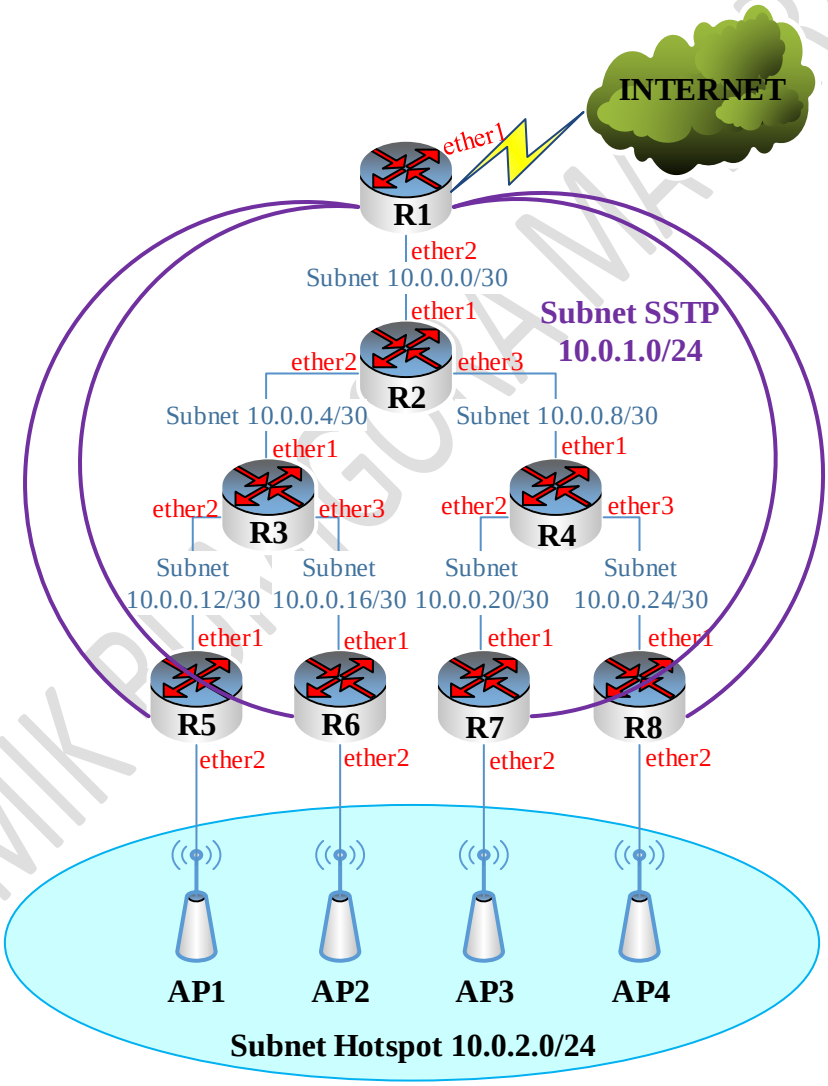
Tabel 4.1 Alokasi Alamat Subnet

No.	Alamat Subnet	Deskripsi
1.	10.0.0.0/30	Dialokasikan untuk subnet router R1-R2
2.	10.0.0.4/30	Dialokasikan untuk subnet router R2-R3
3.	10.0.0.8/30	Dialokasikan untuk subnet router R2-R4
4.	10.0.0.12/30	Dialokasikan untuk subnet router R3-R5
5.	10.0.0.16/30	Dialokasikan untuk subnet router R3-R6
6.	10.0.0.20/30	Dialokasikan untuk subnet router R4-R7
7.	10.0.0.24/30	Dialokasikan untuk subnet router R4-R8

Tabel 4.1 Lanjutan

No.	Alamat Subnet	Deskripsi
8.	10.0.1.0/24	Dialokasikan untuk *SSTP tunnel*
9.	10.0.2.0/24	Dialokasikan untuk subnet *hotspot*

Alokasi alamat subnet pada rancangan jaringan ujicoba, seperti terlihat pada gambar 4.3.



Gambar 4.3 Alokasi Pengalamatan IP Per Subnet

Secara detail pengalamatan IP yang dialokasikan pada setiap *interface* dari *router* dan *Access Point*, seperti terlihat pada tabel 4.2.

Tabel 4.2 Pengalamatan IP Router dan Access Point

No.	Nama Perangkat	Interface	Alamat IP	Gateway
1.	*Router R1*	Ether2	10.0.0.1/30	
2.	*Router R2*	Ether1	10.0.0.2/30	
3.		Ether2	10.0.0.5/30	
4.		Ether3	10.0.0.9/30	
5.	*Router R3*	Ether1	10.0.0.6/30	
6.		Ether2	10.0.0.13/30	
7.		Ether3	10.0.0.17/30	
8.	*Router R4*	Ether1	10.0.0.10/30	
9.		Ether2	10.0.0.21/30	
10.		Ether3	10.0.0.25/30	
11.	*Router R5*	Ether1	10.0.1.14/30	
12.	*Router R6*	Ether1	10.0.1.18/30	
13.	*Router R7*	Ether1	10.0.1.22/30	
14.	*Router R8*	Ether1	10.0.1.26/30	
15.	*Access Point AP1*	LAN	10.0.2.2/24	10.0.2.1
16.	*Access Point AP2*		10.0.2.3/24	
17.	*Access Point AP3*		10.0.2.4/24	
18.	*Access Point AP4*		10.0.2.5/24	

Rancangan user yang dibuat pada SSTP Server untuk digunakan ketika otentikasi dari router yang bertindak SSTP Client, seperti terlihat pada tabel 4.3. *Router* yang bertindak sebagai *SSTP Server* adalah *router R1*, sedangkan *router* yang bertindak sebagai *SSTP Client* adalah *R5, R6, R7* dan *R8*. Sandi untuk keseluruhan user SSTP adalah "12345678".

Tabel 4.3 SSTP User

No.	Username	Local-address	Remote-address	Deskripsi
1.	R5@stmikbumigora.local	10.0.1.1	10.0.1.5	R1-R5
2.	R6@stmikbumigora.local		10.0.1.6	R1-R6
3.	R7@stmikbumigora.local		10.0.1.7	R1-R7
4.	R8@stmikbumigora.local		10.0.1.8	R1-R8

Rancangan alamat IP untuk tunnel local dan remote address yang digunakan ketika pembentukan tunnel EoIP antara router R1 dengan R5, R6, R7, R8 dan sebaliknya, seperti terlihat pada tabel 4.4.

Tabel 4.4 EoIP Tunnel Local Dan Remote Address

No.	Local-address	Remote-address	Deskripsi
1.	10.0.1.1	10.0.1.5	*Tunnel router* R1-R5
2.	10.0.1.1	10.0.1.6	*Tunnel router* R1-R6
3.	10.0.1.1	10.0.1.7	*Tunnel router* R1-R7
4.	10.0.1.1	10.0.1.8	*Tunnel router* R1-R8
5.	10.0.1.5	10.0.1.1	*Tunnel router* R5-R1
6.	10.0.1.6	10.0.1.1	*Tunnel router* R6-R1
7.	10.0.1.7	10.0.1.1	*Tunnel router* R7-R1
8.	10.0.1.8	10.0.1.1	*Tunnel router* R8-R1

4.2.3. Rancangan Tunnel-id EoIP

Adapun rancangan *tunnel-id* untuk *EoIP* yang digunakan ketika pembentukan *tunnel* dari *router R1-R5, R1-R6, R1-R7,* dan *R1-R8*, seperti terlihat pada tabel 4.5.

Tabel 4.5 EoIP Tunnel-id

No.	Tunnel-ID	Deskripsi
1.	5	*Tunnel router* R1-R5
2.	6	*Tunnel router* R1-R6
3.	7	*Tunnel router* R1-R7
4.	8	*Tunnel router* R1-R8

4.3. Tahap Simulation Prototyping

Tahap *simulation prototyping* dibagi menjadi dua bagian yaitu konfigurasi dan ujicoba baik verifikasi konfigurasi maupun skenario.

4.3.1 Konfigurasi

Konfigurasi dilakukan di keseluruhan router yang terlibat meliputi konfigurasi dasar pengalamatan IP, *routing protocol OSPF*, *table routing*, DNS, *NTP Client*, *Time Zone*, *SSTP tunnel*, *EoIP tunnel* dan *interface bridge* serta *hotspot*.

4.3.2 Ujicoba

Ujicoba dibagi menjadi 2 (dua) jenis yaitu:

1. Verifikasi Konfigurasi

   Verifikasi dilakukan di keseluruhan router yang terlibat meliputi verifikasi konfigurasi pengalamatan IP, *routing protocol OSPF*, *table routing*, DNS, *NTP Client*, *Time Zone*, *SSTP tunnel*, *EoIP tunnel* dan *interface bridge* serta *hotspot*.

2. Skenario

Terdapat 7 skenario yang digunakan untuk mengujicoba konfigurasi meliputi manajemen *user hotspot* di *router R1,* koneksi Internet dari *router R1, Client1, Client2, Client3* dan *Client4* serta *monitoring user hotspot*.

BAB V

HASIL DAN LUARAN YANG DICAPAI

Bab ini membahas tentang hasil konfigurasi dan ujicoba serta analisa terhadap hasil ujicoba.

5.1 Konfigurasi

Konfigurasi terdiri dari 5 (lima) bagian yaitu konfigurasi dasar, konfigurasi *routing protocol OSPF*, konfigurasi *NTP Client*, konfigurasi *SSTP*, konfigurasi *EoIP* dan *Bridge* serta konfigurasi *hotspot*.

5.1.1 Konfigurasi Dasar

Konfigurasi dasar dilakukan pada 8 (delapan) *router MikroTik* meliputi pengaturan *hostname* sebagai identitas dari *router* dan pengalamatan IP pada *interface*. Khusus untuk *router* R1 dilakukan pula konfigurasi *Point-to-Point over Ethernet* (*PPPoE) Client* untuk dapat terkoneksi ke ISP dan *Network Address Translation (NAT)* untuk berbagi pakai koneksi Internet dengan host-host di jaringan local serta konfigurasi sebagai *DNS Server* bagi jaringan lokal. Selain itu pada *router* selain R1 juga dilakukan pengaturan *Domain Name System (DNS) Client* agar dapat mengakses layanan *Internet* menggunakan nama domain.

5.1.1.1 Konfigurasi Dasar Pada Router R1

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R1 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R1
```

2. Mengatur *PPPoE Client* untuk mengkoneksikan ke *Internet Service Provider (ISP)*.

```
[admin@R1] > interface pppoe-client add name=pppoe-out1
             interface=ether1          user=username@isp
             password=password     add-default-route=yes
             use-peer-dns=yes disabled=no
```

3. Mengatur NAT untuk berbagi pakai koneksi Internet.

```
[admin@R1] > ip firewall nat add chain=srcnat out-
             interface=pppoe-out1 action=masquerade
```

4. Mengatur pengalamatan IP pada *interface ether2*.

```
[admin@R1] > ip address add address=10.0.0.1/30
             interface=ether2
```

5. Mengatur sebagai *DNS Server*.

```
[admin@R1] > ip dns set allow-remote-requests=yes
```

5.1.1.2 Konfigurasi Dasar Pada Router R2

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R2 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R2
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@R2] > ip address add address=10.0.0.2/30
             interface=ether1
```

3. Mengatur pengalamatan IP pada *interface ether2*.

```
[admin@R2] > ip address add address=10.0.0.5/30
             interface=ether2
```

4. Mengatur pengalamatan IP pada *interface ether3*.

```
[admin@R2] > ip address add address=10.0.0.9/30
                interface=ether3
```

5. Mengatur *DNS Client*.

```
[admin@R2] > ip dns set servers=10.0.0.1
```

5.1.1.3 Konfigurasi Dasar Pada Router R3

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R3 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R3
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@R3] > ip address add address=10.0.0.6/30
                interface=ether1
```

3. Mengatur pengalamatan IP pada *interface ether2*.

```
[admin@R3] > ip address add address=10.0.0.13/30
                interface=ether2
```

4. Mengatur pengalamatan IP pada *interface ether3*.

```
[admin@R3] > ip address add address=10.0.0.17/30
                interface=ether3
```

5. Mengatur *DNS Client*.

```
[admin@R3] > ip dns set servers=10.0.0.1
```

5.1.1.4 Konfigurasi Dasar Pada Router R4

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R4 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R4
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@R4] > ip address add address=10.0.0.10/30
                interface=ether1
```

3. Mengatur pengalamatan IP pada *interface ether2*.

```
[admin@R4] > ip address add address=10.0.0.21/30
                interface=ether2
```

4. Mengatur pengalamatan IP pada *interface ether3*.

```
[admin@R4] > ip address add address=10.0.0.25/30
                interface=ether3
```

5. Mengatur *DNS Client*.

```
[admin@R4] > ip dns set servers=10.0.0.1
```

5.1.1.5 Konfigurasi Dasar Pada Router R5

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R5 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R5
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@R5] > ip address add address=10.0.0.14/30
                interface=ether1
```

3. Mengatur *DNS Client*.

```
[admin@R5] > ip dns set servers=10.0.0.1
```

5.1.1.6 Konfigurasi Dasar Pada Router R6

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R6 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R6
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@R6] > ip address add address=10.0.0.18/30
                interface=ether1
```

3. Mengatur *DNS Client*.

```
[admin@R6] > ip dns set servers=10.0.0.1
```

5.1.1.7 Konfigurasi Dasar Pada Router R7

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R7 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R7
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@R7] > ip address add address=10.0.0.22/30
                interface=ether1
```

3. Mengatur *DNS Client*.

```
[admin@R7] > ip dns set servers=10.0.0.1
```

5.1.1.8 Konfigurasi Dasar Pada Router R8

Adapun langkah-langkah konfigurasi dasar yang dilakukan pada *router* R8 adalah sebagai berikut:

1. Mengubah *hostname*.

```
[admin@MikroTik] > system identity set name=R8
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@R8] > ip address add address=10.0.0.26/30
                    interface=ether1
```

3. Mengatur *DNS Client*.

```
[admin@R8] > ip dns set servers=10.0.0.1
```

5.1.2 Konfigurasi Routing Protokol OSPF

Konfigurasi *routing protokol OSPF* dilakukan pada 8 (delapan) *router MikroTik* yaitu *R1, R2, R3, R4, R5, R6, R7* dan *R8.*

5.1.2.1 Konfigurasi Routing Protokol OSPF Pada Router R1

Adapun langkah-langkah konfigurasi *routing protocol OSPF* pada *router* R1 adalah sebagai berikut:

1. Mengaktifkan *routing protocol OSPF* dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.0/30 dan area *backbone.*

```
[admin@R1] > routing ospf network add network=10.0.0.0/30
                area=backbone
```

2. Mendistribusikan *default route* menggunakan *metric type 1* agar *router OSPF* lainnya seperti R2, R3, R4, R5, R6, R7 dan R8 agar dapat merutekan paket data dengan tujuan diluar dari jaringan local yaitu Internet melalui router R1.

```
[admin@R1] > routing ospf instance set distribute-
                default=always-as-type-1 default
```

5.1.2.2 Konfigurasi Routing Protokol OSPF Pada Router R2

Pengaktifan *routing protocol OSPF* pada *router* R2 dilakukan dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.0/30, 10.0.0.4/30, 10.0.0.8/30 dan area *backbone* menggunakan perintah berikut:

```
[admin@R2] > routing ospf network add network=10.0.0.0/30
             area=backbone
[admin@R2] > routing ospf network add network=10.0.0.4/30
             area=backbone
[admin@R2] > routing ospf network add network=10.0.0.8/30
             area=backbone
```

5.1.2.3 Konfigurasi Routing Protokol OSPF Pada Router R3

Pengaktifan *routing protocol OSPF* pada *router* R3 dilakukan dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.4/30, 10.0.0.12/30, 10.0.0.16/30 dan area *backbone* menggunakan perintah berikut:

```
[admin@R3] > routing ospf network add network=10.0.0.4/30
             area=backbone
[admin@R3] > routing ospf network add network=10.0.0.12/30
             area=backbone
[admin@R3] > routing ospf network add network=10.0.0.16/30
             area=backbone
```

5.1.2.4 Konfigurasi Routing Protokol OSPF Pada Router R4

Pengaktifan *routing protocol OSPF* pada *router* R4 dilakukan dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.8/30, 10.0.0.20/30, 10.0.0.24/30 dan area *backbone* menggunakan perintah:

```
[admin@R4] > routing ospf network add network=10.0.0.8/30
             area=backbone
```

```
[admin@R4] > routing ospf network add network=10.0.0.20/30
             area=backbone
[admin@R4] > routing ospf network add network=10.0.0.24/30
             area=backbone
```

5.1.2.5 Konfigurasi Routing Protokol OSPF Pada Router R5

Pengaktifan *routing protocol OSPF* pada *router* R5 dilakukan dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.12/30 dan area *backbone* menggunakan perintah berikut:

```
[admin@R5] > routing ospf network add network=10.0.0.12/30
             area=backbone
```

5.1.2.6 Konfigurasi Routing Protokol OSPF Pada Router R6

Pengaktifan *routing protocol OSPF* pada *router* R6 dilakukan dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.16/30 dan area *backbone* menggunakan perintah berikut:

```
[admin@R6] > routing ospf network add network=10.0.0.16/30
             area=backbone
```

5.1.2.7 Konfigurasi Routing Protokol OSPF Pada Router R7

Pengaktifan *routing protocol OSPF* pada *router* R7 dilakukan dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.20/30 dan area *backbone* menggunakan perintah berikut:

```
[admin@R7] > routing ospf network add network=10.0.0.20/30
             area=backbone
```

5.1.2.8 Konfigurasi Routing Protokol OSPF Pada Router R8

Pengaktifan *routing protocol OSPF* pada *router* R8 dilakukan dengan mendefinisikan alamat jaringan dan area dimana OSPF beroperasi yaitu 10.0.0.24/30 dan area *backbone* menggunakan perintah berikut:

```
[admin@R8] > routing ospf network add network=10.0.0.24/30
             area=backbone
```

5.1.3 Konfigurasi NTP Client

Konfigurasi *NTP Client* dilakukan pada keseluruhan *router MikroTik* untuk mensinkronisasi waktu dengan *NTP Server* di *Internet* yaitu **0.id.pool.ntp.org** dan **1.asia.ntp.org** menggunakan perintah berikut:

```
> system ntp client set enabled=yes server-dns-
  names=0.id.pool.ntp.org,1.asia.pool.ntp.org
```

5.1.4 Konfigurasi SSTP

Konfigurasi *SSTP* terdiri dari 2 bagian yaitu *SSTP Server* yang dilakukan pada *router R1* dan *SSTP Client* yang dilakukan pada *router R5, 56, R7* dan *R8.*

5.1.4.1 Konfigurasi SSTP Server Pada Router R1

Adapun langkah-langkah konfigurasi *SSTP Se*rver yang dilakukan pada *router R1* adalah sebagai berikut:

1. Membuat *template* untuk *Certificate Authority (CA).*

```
[admin@R1] > certificate add name=hotspotCA common-
             name=hotspotCA country=ID state="Nusa
             Tenggara Barat" locality=Mataram
             organization="STMIK Bumigora" unit=PusTIK
             key-usage=key-cert-sign,crl-sign
```

2. Membuat *template* untuk *Server Certificate*.

```
[admin@R1] > certificate add name=hotspotServer common-
             name=10.0.0.1 country=ID state="Nusa
             Tenggara Barat" locality=Mataram
             organization="STMIK Bumigora" unit=PusTIK
```

3. Membuat *template* untuk *Client Certificate*.

```
[admin@R1] > certificate add name=hotspotClient common-
             name=hotspotClient country=ID state="Nusa
             Tenggara Barat" locality=Mataram
             organization="STMIK Bumigora" unit=PusTIK
```

4. Melakukan *Sign Certificate* untuk CA dan mengatur *Certificate Revocation Lists (CRL) Uniform Resource Locator (URL)* menggunakan alamat IP 10.0.0.1 yang merupakan alamat IP internal dari *Server*.

```
[admin@R1] > certificate sign hotspotCA ca-crl-
             host=10.0.0.1 name=hotspotCA
```

5. Melakukan *Sign Certificate* untuk *Server Certificate*.

```
[admin@R1] > certificate sign hotspotServer ca=hotspotCA
             name=hotspotServer
```

6. Melakukan *Sign Certificate* untuk *Client Certificate*.

```
[admin@R1] > certificate sign hotspotClient ca=hotspotCA
             name=hotspotClient
```

7. Mengatur *trusted* pada *CA*, *Server* dan *Client Certificate*.

```
[admin@R1] > certificate set hotspotCA trusted=yes
[admin@R1] > certificate set hotspotServer trusted=yes
[admin@R1] > certificate set hotspotClient trusted=yes
```

8. Melakukan *export Client Certificate* dan *CA Certificate* dengan *key* sebagai contoh "**12345678**" yang nantinya akan digunakan pada *router* yang bertindak sebagai *SSTP Client* yaitu R5, R6, R7 dan R8.

```
[admin@R1] > certificate export-certificate hotspotCA
             export-passphrase=12345678
[admin@R1] > certificate export-certificate hotspotClient
             export-passphrase=12345678
```

9. Membuat akun pengguna untuk koneksi dari *router R5* yang bertindak sebagai *SSTP Client* ke *router R1* yang bertindak sebagai *SSTP Server*.

```
[admin@R1] > ppp secret add name=R5@stmikbumigora.local
             password=12345678 service=sstp local-
             address=10.0.1.1 remote-address=10.0.1.5
```

10. Membuat akun pengguna untuk koneksi dari *router R6* yang bertindak sebagai *SSTP Client* ke *router R1* yang bertindak sebagai *SSTP Server*.

```
[admin@R1] > ppp secret add name=R6@stmikbumigora.local
             password=12345678 service=sstp local-
             address=10.0.1.1 remote-address=10.0.1.6
```

11. Membuat akun pengguna untuk koneksi dari *router R7* yang bertindak sebagai *SSTP Client* ke *router R1* yang bertindak sebagai *SSTP Server*.

```
[admin@R1] > ppp secret add name=R7@stmikbumigora.local
             password=12345678 service=sstp local-
             address=10.0.1.1 remote-address=10.0.1.7
```

12. Membuat akun pengguna untuk koneksi dari *router R8* yang bertindak sebagai *SSTP Client* ke *router R1* yang bertindak sebagai *SSTP Server*.

```
[admin@R1] > ppp secret add name=R8@stmikbumigora.local
             password=12345678 service=sstp local-
             address=10.0.1.1 remote-address=10.0.1.8
```

13. Mengaktifkan *SSTP Server*.

```
[admin@R1] > interface sstp-server server set enabled=yes
             certificate=hotspotServer verify-client-
             certificate=yes authentication=mschap2
```

Penjelasan *properties*:

a) `enabled=yes`, digunakan untuk mengaktifkan SSTP Server.

b) `certificate=hotspotServer`, digunakan untuk menentukan nama Server Certificate yang digunakan yaitu hotspotServer.

c) `verify-client-certificate=yes`, digunakan agar server melakukan pengecekan *Client Certificate* termasuk dalam *certificate chain* yang sama.

d) `authentication=mschap2`, digunakan untuk menentukan metode otentikasi yang diterima oleh *SSTP Server* yaitu *mschap2*.

5.1.4.2 Konfigurasi SSTP Client

Konfigurasi *SSTP Client* dilakukan pada 4 (empat) *router* yaitu *router R5, R6, R7* dan *R8*.

5.1.4.2.1 Konfigurasi SSTP Client Pada Router R5

Adapun langkah-langkah konfigurasi *SSTP Client* yang dilakukan pada *router R5* adalah sebagai berikut:

1. Menyalin file *CA* dan *Client Certificate* dari *router R1* ke *router R5*.

```
[admin@R5] > /tool fetch address=10.0.0.1 src-
             path="cert_export_hotspotCA.crt"
```

```
                    user=admin password="" mode=ftp port=21
                    dst-path="cert_export_hotspotCA.crt"
                    keep-result=yes
[admin@R5]    >    /tool    fetch    address=10.0.0.1    src-
                    path="cert_export_hotspotCA.key"
                    user=admin password="" mode=ftp port=21
                    dst-path="cert_export_hotspotCA.key"
                    keep-result=yes
[admin@R5]    >    /tool    fetch    address=10.0.0.1    src-
                    path="cert_export_hotspotClient.key"
                    user=admin password="" mode=ftp port=21
                    dst-
                    path="cert_export_hotspotClient.key"
                    keep-result=yes
[admin@R5]    >    /tool    fetch    address=10.0.0.1    src-
                   path="cert_export_hotspotClient.crt"
                   user=admin password="" mode=ftp port=21
                   dst-
                   path="cert_export_hotspotClient.crt"
                   keep-result=yes
```

2. Melakukan *import file CA* dan *Client Certificate*. *Passphrase* atau *key* untuk proses *import* menggunakan nilai key ketika proses *export certificate* yaitu "**12345678**".

```
[admin@R5]      >      certificate      import      file-
                        name=cert_export_hotspotCA.crt
passphrase: ********
     certificates-imported: 1
```

```
     private-keys-imported: 0
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
[admin@R5]      >      certificate      import      file-
                        name=cert_export_hotspotClient.cr
                        t
passphrase: ********
     certificates-imported: 1
     private-keys-imported: 0
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
[admin@R5]      >      certificate      import      file-
                        name=cert_export_hotspotCA.key
passphrase: ********
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0

[admin@R5]      >      certificate      import      file-
                        name=cert_export_hotspotClient.ke
                        y
passphrase: ********
```

```
      certificates-imported: 0
      private-keys-imported: 1
             files-imported: 1
        decryption-failures: 0
  keys-with-no-certificate: 0
```

3. Mengubah nama file hasil *import file CA* dan *Client Certificate*.

```
[admin@R5] > certificate set 0 name=hotspotCA
[admin@R5] > certificate set 1 name=hotspotClient
```

4. Membuat *interface SSTP Client* yang digunakan untuk koneksi dari *router R5* ke *R1*.

```
[admin@R5] > interface sstp-client add
           authentication=mschap2
           certificate=hotspotClient connect-to=10.0.0.1
           disabled=no name=sstp-out1 password=12345678
           user=R5@stmikbumigora.local verify-server-
           certificate=yes
```

Penjelasan *properties*:

a) `authentication=mschap2`, digunakan untuk menentukan metode otentikasi yang diterima yaitu *mschap2*.

b) `certificate=hotspotClient`, digunakan untuk menentukan nama *Client Certificate* yang digunakan yaitu *hotspotClient*.

c) `connect-to=10.0.0.1`, digunakan untuk menentukan alamat IP dari *SSTP Server* yaitu 10.0.0.1.

d) `disabled=no`, digunakan untuk mengaktifkan *SSTP Client*.

e) `name=sstp-out1`, digunakan untuk menentukan nama deskripsi untuk *interface* yang dibuat yaitu "*sstp-out1*".

f) `password=12345678,` digunakan untuk menentukan sandi yang akan digunakan untuk otentikasi yaitu "*12345678*".

g) `user=R5@stmikbumigora.local,` digunakan untuk menentukan nama pengguna yang akan digunakan untuk otentikasi yaitu "*R5@stmikbumigora.local*".

h) `verify-server-certificate=yes`, digunakan agar client melakukan pengecekan *certificate* termasuk dalam *certificate chain* yang sama dengan *Server Certificate*.

5.1.4.2.2 Konfigurasi SSTP Client Pada Router R6

Adapun langkah-langkah konfigurasi *SSTP Client* yang dilakukan pada *router R6* adalah sebagai berikut:

1. Menyalin file *CA* dan *Client Certificate* dari *router R1* ke *router R6*.

```
[admin@R6] > /tool fetch address=10.0.0.1 src-
             path="cert_export_hotspotCA.crt"
             user=admin password="" mode=ftp port=21
             dst-path="cert_export_hotspotCA.crt"
             keep-result=yes
[admin@R6] > /tool fetch address=10.0.0.1 src-
             path="cert_export_hotspotCA.key"
             user=admin password="" mode=ftp port=21
             dst-path="cert_export_hotspotCA.key"
             keep-result=yes
[admin@R6] > /tool fetch address=10.0.0.1 src-
             path="cert_export_hotspotClient.key"
             user=admin password="" mode=ftp port=21
```

```
                    dst-
                    path="cert_export_hotspotClient.key"
                    keep-result=yes
[admin@R6]  >  /tool  fetch  address=10.0.0.1  src-
                    path="cert_export_hotspotClient.crt"
                    user=admin password="" mode=ftp port=21
                    dst-
                    path="cert_export_hotspotClient.crt"
                    keep-result=yes
```

2. Melakukan *import file CA* dan *Client Certificate*. *Passphrase* atau *key* untuk proses *import* menggunakan nilai key ketika proses *export certificate* yaitu "**12345678**".

```
[admin@R6]      >      certificate      import      file-
                        name=cert_export_hotspotCA.crt
passphrase: ********
     certificates-imported: 1
     private-keys-imported: 0
          files-imported: 1
      decryption-failures: 0
  keys-with-no-certificate: 0
[admin@R6]      >      certificate      import      file-
                        name=cert_export_hotspotClient.cr
                        t
passphrase: ********
     certificates-imported: 1
     private-keys-imported: 0
            files-imported: 1
```

```
       decryption-failures: 0
  keys-with-no-certificate: 0
[admin@R6]      >      certificate      import      file-
                        name=cert_export_hotspotCA.key
passphrase: ********
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0

[admin@R6]      >      certificate      import      file-
                       name=cert_export_hotspotClient.ke
                       y
passphrase: ********
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
```

3. Mengubah nama file hasil import file CA dan Client Certificate.

```
[admin@R6] > certificate set 0 name=hotspotCA
[admin@R6] > certificate set 1 name=hotspotClient
```

4. Membuat *interface SSTP Client* yang digunakan untuk koneksi dari *router R6* ke *R1*.

```
[admin@R6]      >      interface      sstp-client      add
             authentication=mschap2
```

```
certificate=hotspotClient connect-to=10.0.0.1
disabled=no name=sstp-out1 password=12345678
user=R6@stmikbumigora.local verify-server-
certificate=yes
```

Penjelasan *properties*:

a) `authentication=mschap2`, digunakan untuk menentukan metode otentikasi yang diterima yaitu *mschap2*.

b) `certificate=hotspotClient`, digunakan untuk menentukan nama *Client Certificate* yang digunakan yaitu *hotspotClient*.

c) `connect-to=10.0.0.1`, digunakan untuk menentukan alamat IP dari *SSTP Server* yaitu 10.0.0.1.

d) `disabled=no`, digunakan untuk mengaktifkan *SSTP Client*.

e) `name=sstp-out1`, digunakan untuk menentukan nama deskripsi untuk *interface* yang dibuat yaitu "*sstp-out1*".

f) `password=12345678`, digunakan untuk menentukan sandi yang akan digunakan untuk otentikasi yaitu "*12345678*".

g) `user=R6@stmikbumigora.local`, digunakan untuk menentukan nama pengguna yang akan digunakan untuk otentikasi yaitu "*R6@stmikbumigora.local*".

h) `verify-server-certificate=yes`, digunakan agar client melakukan pengecekan *certificate* termasuk dalam *certificate chain* yang sama dengan *Server Certificate*.

5.1.4.2.3 Konfigurasi SSTP Client Pada Router R7

Adapun langkah-langkah konfigurasi *SSTP Client* yang dilakukan pada *router R7* adalah sebagai berikut:

1. Menyalin file *CA* dan *Client Certificate* dari *router R1* ke *router R7*.

```
[admin@R7] > /tool fetch address=10.0.0.1 src-
path="cert_export_hotspotCA.crt"
user=admin password="" mode=ftp port=21
dst-path="cert_export_hotspotCA.crt"
keep-result=yes
[admin@R7] > /tool fetch address=10.0.0.1 src-
path="cert_export_hotspotCA.key"
user=admin password="" mode=ftp port=21
dst-path="cert_export_hotspotCA.key"
keep-result=yes
[admin@R7] > /tool fetch address=10.0.0.1 src-
path="cert_export_hotspotClient.key"
user=admin password="" mode=ftp port=21
dst-
path="cert_export_hotspotClient.key"
keep-result=yes
[admin@R7] > /tool fetch address=10.0.0.1 src-
path="cert_export_hotspotClient.crt"
user=admin password="" mode=ftp port=21
dst-
path="cert_export_hotspotClient.crt"
keep-result=yes
```

2. Melakukan *import file CA* dan *Client Certificate*. *Passphrase* atau *key* untuk proses *import* menggunakan nilai key ketika proses *export certificate* yaitu "**12345678**".

```
[admin@R7] > certificate import file-
                        name=cert_export_hotspotCA.crt
passphrase: ********
     certificates-imported: 1
     private-keys-imported: 0
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
[admin@R7] > certificate import file-
                        name=cert_export_hotspotClient.cr
                        t
passphrase: ********
     certificates-imported: 1
     private-keys-imported: 0
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
[admin@R7] > certificate import file-
                        name=cert_export_hotspotCA.key
passphrase: ********
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
```

```
[admin@R7]      >      certificate      import      file-
                        name=cert_export_hotspotClient.ke
                        y
passphrase: ********
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
```

3. Mengubah nama file hasil import file CA dan Client Certificate.

```
[admin@R7] > certificate set 0 name=hotspotCA
[admin@R7] > certificate set 1 name=hotspotClient
```

4. Membuat *interface SSTP Client* yang digunakan untuk koneksi dari *router R7* ke *R1*.

```
[admin@R5]      >      interface      sstp-client      add
            authentication=mschap2
            certificate=hotspotClient connect-to=10.0.0.1
            disabled=no name=sstp-out1 password=12345678
            user=R7@stmikbumigora.local    verify-server-
            certificate=yes
```

Penjelasan *properties*:

a) `authentication=mschap2`, digunakan untuk menentukan metode otentikasi yang diterima yaitu *mschap2*.

b) `certificate=hotspotClient`, digunakan untuk menentukan nama *Client Certificate* yang digunakan yaitu *hotspotClient*.

c) `connect-to=10.0.0.1,` digunakan untuk menentukan alamat IP dari *SSTP Server* yaitu 10.0.0.1.

d) `disabled=no`, digunakan untuk mengaktifkan *SSTP Client*.

e) `name=sstp-out1,` digunakan untuk menentukan nama deskripsi untuk *interface* yang dibuat yaitu "*sstp-out1*".

f) `password=12345678,` digunakan untuk menentukan sandi yang akan digunakan untuk otentikasi yaitu "*12345678*".

g) `user=R7@stmikbumigora.local,` digunakan untuk menentukan nama pengguna yang akan digunakan untuk otentikasi yaitu "*R7@stmikbumigora.local*".

h) `verify-server-certificate=yes`, digunakan agar client melakukan pengecekan *certificate* termasuk dalam *certificate chain* yang sama dengan *Server Certificate*.

5.1.4.2.4 Konfigurasi SSTP Client Pada Router R8

Adapun langkah-langkah konfigurasi *SSTP Client* yang dilakukan pada *router R8* adalah sebagai berikut:

1. Menyalin file *CA* dan *Client Certificate* dari *router R1* ke *router R8*.

```
[admin@R8] > /tool fetch address=10.0.0.1 src-
             path="cert_export_hotspotCA.crt"
             user=admin password="" mode=ftp port=21
             dst-path="cert_export_hotspotCA.crt"
             keep-result=yes
[admin@R8] > /tool fetch address=10.0.0.1 src-
             path="cert_export_hotspotCA.key"
             user=admin password="" mode=ftp port=21
```

```
                    dst-path="cert_export_hotspotCA.key"
                    keep-result=yes
[admin@R8]    >    /tool    fetch    address=10.0.0.1    src-
                    path="cert_export_hotspotClient.key"
                    user=admin password="" mode=ftp port=21
                    dst-
                    path="cert_export_hotspotClient.key"
                    keep-result=yes
[admin@R8]    >    /tool    fetch    address=10.0.0.1    src-
                    path="cert_export_hotspotClient.crt"
                    user=admin password="" mode=ftp port=21
                    dst-
                    path="cert_export_hotspotClient.crt"
                    keep-result=yes
```

2. Melakukan *import file CA* dan *Client Certificate*. *Passphrase* atau *key* untuk proses *import* menggunakan nilai key ketika proses *export certificate* yaitu "**12345678**".

```
[admin@R8]    >    certificate    import    file-
                    name=cert_export_hotspotCA.crt
passphrase: ********
      certificates-imported: 1
     private-keys-imported: 0
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
```

```
[admin@R8]      >      certificate      import      file-
                        name=cert_export_hotspotClient.cr
                        t
passphrase: ********
     certificates-imported: 1
     private-keys-imported: 0
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
[admin@R8]      >      certificate      import      file-
                        name=cert_export_hotspotCA.key
passphrase: ********
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0

[admin@R8]      >      certificate      import      file-
                        name=cert_export_hotspotClient.ke
                        y
passphrase: ********
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
```

```
keys-with-no-certificate: 0
```

3. Mengubah nama file hasil import file CA dan Client Certificate.

```
[admin@R8] > certificate set 0 name=hotspotCA
[admin@R8] > certificate set 1 name=hotspotClient
```

4. Membuat *interface SSTP Client* yang digunakan untuk koneksi dari *router R8* ke *R1*.

```
[admin@R8] > interface sstp-client add
           authentication=mschap2
           certificate=hotspotClient connect-to=10.0.0.1
           disabled=no name=sstp-out1 password=12345678
           user=R5@stmikbumigora.local verify-server-
           certificate=yes
```

Penjelasan *properties*:

a) `authentication=mschap2`, digunakan untuk menentukan metode otentikasi yang diterima yaitu *mschap2*.

b) `certificate=hotspotClient`, digunakan untuk menentukan nama *Client Certificate* yang digunakan yaitu *hotspotClient*.

c) `connect-to=10.0.0.1`, digunakan untuk menentukan alamat IP dari *SSTP Server* yaitu 10.0.0.1.

d) `disabled=no`, digunakan untuk mengaktifkan *SSTP Client*.

e) `name=sstp-out1`, digunakan untuk menentukan nama deskripsi untuk *interface* yang dibuat yaitu "*sstp-out1*".

f) `password=12345678`, digunakan untuk menentukan sandi yang akan digunakan untuk otentikasi yaitu "*12345678*".

g) `user=R8@stmikbumigora.local,` digunakan untuk menentukan nama pengguna yang akan digunakan untuk otentikasi yaitu "*R8@stmikbumigora.local*".

h) `verify-server-certificate=yes`, digunakan agar client melakukan pengecekan *certificate* termasuk dalam *certificate chain* yang sama dengan *Server Certificate*.

5.1.5 Konfigurasi EoIP dan Bridge

Konfigurasi *EoIP* dan *Bridge* dilakukan pada 4 (empat) *router* yaitu *router* R1, R5, R6, R7 dan R8.

5.1.5.1 Konfigurasi EoIP dan Bridge Pada Router R1

Adapun langkah-langkah konfigurasi *EoIP* dan *Bridge* yang dilakukan pada *router R1* adalah sebagai berikut:

1. Membuat *interface EoIP tunnel* dari *router R1* ke *R5*.

```
[admin@R1] > interface eoip add name=eoip-R1-R5 tunnel-id=5
             local-address=10.0.1.1                remote-
             address=10.0.1.5 comment="EoIP dari R1 ke R5"
             disabled=no
```

Keterangan *properties*:

a) `Name` : nama pengenal interface EoIP yang dibuat yaitu "*eoip-R1-R5*".

b) `Tunnel-id` : metode untuk mengidentifikasi *tunnel* yang harus unik untuk masing-masing *tunnel EoIP* dan harus sesuai dengan sisi *tunnel* lainnya. Nilainya dapat berupa *integer* antara 0-65536, dan untuk *tunnel* dari R1 ke R5 diatur dengan nilai "5".

c) `Local-address` : alamat IP sumber dari tunnel lokal yaitu 10.0.1.1.

d) `Remote-address` : alamat IP dari tunnel EoIP lawan atau sisi remote yaitu 10.0.1.5.

e) `Comment` : deskripsi atau keterangan singkat terkait interface EoIP yang dibuat yaitu "*EoIP dari R1 ke R5*".

f) `Disabled` : mengatur agar interface diaktifkan.

2. Membuat *interface EoIP tunnel* dari *router R1* ke *R6*.

```
[admin@R1] > interface eoip add name=eoip-R1-R6 tunnel-id=6
             local-address=10.0.1.1          remote-
             address=10.0.1.6 comment="EoIP dari R1 ke R6"
             disabled=no
```

Keterangan *properties*:

a) `Name` : nama pengenal interface EoIP yang dibuat yaitu "*eoip-R1-R6*".

b) `Tunnel-id` : metode untuk mengidentifikasi *tunnel* yang harus unik untuk masing-masing *tunnel EoIP* dan harus sesuai dengan sisi *tunnel* lainnya. Nilainya dapat berupa *integer* antara 0-65536, dan untuk *tunnel* dari R1 ke R5 diatur dengan nilai "6".

c) `Local-address` : alamat IP sumber dari tunnel lokal yaitu 10.0.1.1.

d) `Remote-address` : alamat IP dari tunnel EoIP lawan atau sisi remote yaitu 10.0.1.6.

e) `Comment` : deskripsi atau keterangan singkat terkait interface EoIP yang dibuat yaitu "*EoIP dari R1 ke R6*".

f) `Disabled` : mengatur agar interface diaktifkan.

3. Membuat *interface EoIP tunnel* dari *router R1* ke *R7*.

```
[admin@R1] > interface eoip add name=eoip-R1-R7 tunnel-id=7
             local-address=10.0.1.1          remote-
```

```
address=10.0.1.7 comment="EoIP dari R1 ke R7"
disabled=no
```

Keterangan *properties*:

a) `Name` : nama pengenal interface EoIP yang dibuat yaitu "*eoip-R1-R7*".

b) `Tunnel-id` : metode untuk mengidentifikasi *tunnel* yang harus unik untuk masing-masing *tunnel EoIP* dan harus sesuai dengan sisi *tunnel* lainnya. Nilainya dapat berupa *integer* antara 0-65536, dan untuk *tunnel* dari R1 ke R7 diatur dengan nilai "7".

c) `Local-address` : alamat IP sumber dari tunnel lokal yaitu 10.0.1.1.

d) `Remote-address` : alamat IP dari tunnel EoIP lawan atau sisi remote yaitu 10.0.1.7.

e) `Comment` : deskripsi atau keterangan singkat terkait interface EoIP yang dibuat yaitu "*EoIP dari R1 ke R7*".

f) `Disabled` : mengatur agar interface diaktifkan.

4. Membuat *interface EoIP tunnel* dari *router R1* ke *R8*.

```
[admin@R1] > interface eoip add name=eoip-R1-R8 tunnel-id=8
local-address=10.0.1.1 remote-
address=10.0.1.8 comment="EoIP dari R1 ke R8"
disabled=no
```

Keterangan *properties*:

a) `Name` : nama pengenal interface EoIP yang dibuat yaitu "*eoip-R1-R8*".

b) `Tunnel-id` : metode untuk mengidentifikasi *tunnel* yang harus unik untuk masing-masing *tunnel EoIP* dan harus sesuai dengan sisi *tunnel* lainnya. Nilainya dapat berupa *integer* antara 0-65536, dan untuk *tunnel* dari R1 ke R5 diatur dengan nilai "8".

c) `Local-address` : alamat IP sumber dari tunnel lokal yaitu 10.0.1.1.

d) `Remote-address` : alamat IP dari tunnel EoIP lawan atau sisi remote yaitu 10.0.1.8.

e) `Comment` : deskripsi atau keterangan singkat terkait interface EoIP yang dibuat yaitu "*EoIP dari R1 ke R8*".

f) `Disabled` : mengatur agar interface diaktifkan.

5. Membuat *interface bridge* dengan nama "*bridgeHotspot*" yang digunakan untuk *hotspot*.

```
[admin@R1] > interface bridge add name=bridgeHotspot
```

6. Menambahkan *interface EoIP* dengan "*eoIP-R1-R5*" sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R1] > interface bridge port add bridge=bridgeHotspot
             interface=eoip-R1-R5
```

7. Menambahkan *interface EoIP* dengan "*eoIP-R1-R6*" sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R1] > interface bridge port add bridge=bridgeHotspot
             interface=eoip-R1-R6
```

8. Menambahkan *interface EoIP* dengan "*eoIP-R1-R7*" sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R1] > interface bridge port add bridge=bridgeHotspot
             interface=eoip-R1-R7
```

9. Menambahkan *interface EoIP* dengan "*eoIP-R1-R8*" sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R1] > interface bridge port add bridge=bridgeHotspot
             interface=eoip-R1-R8
```

5.1.5.2 Konfigurasi EoIP dan Bridge Pada Router R5

Adapun langkah-langkah konfigurasi *EoIP* dan *Bridge* yang dilakukan pada *router R5* adalah sebagai berikut:

1. Membuat *interface EoIP tunnel* dari *router R5* ke *R1*.

```
[admin@R5] > interface eoip add name=eoip-R5-R1 tunnel-id=5
             local-address=10.0.1.5              remote-
             address=10.0.1.1 comment="EoIP dari R5 ke R1"
             disabled=no
```

2. Membuat *interface bridge* dengan nama "*bridgeHotspot*".

```
[admin@R5] > interface bridge add name=bridgeHotspot
```

3. Menambahkan *interface Eoip* dengan nama "*eoip-R5-R1*" sebagai *port* anggota dari *interface bridge "bridgeHotspot"*.

```
[admin@R5] > interface bridge port add bridge=bridgeHotspot
             interface=eoip-R5-R1
```

4. Menambahkan *interface ether2* sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R5] > interface bridge port add bridge=bridgeHotspot
             interface=ether2
```

5.1.5.3 Konfigurasi EoIP dan Bridge Pada Router R6

Adapun langkah-langkah konfigurasi *EoIP* dan *Bridge* yang dilakukan pada *router R6* adalah sebagai berikut:

1. Membuat *interface EoIP tunnel* dari *router R6* ke *R1*.

```
[admin@R6] > interface eoip add name=eoip-R6-R1 tunnel-id=6
             local-address=10.0.1.6              remote-
```

```
address=10.0.1.1 comment="EoIP dari R6 ke R1"
disabled=no
```

2. Membuat *interface bridge* dengan nama "*bridgeHotspot*".

```
[admin@R6] > interface bridge add name=bridgeHotspot
```

3. Menambahkan *interface Eoip* dengan nama "*eoip-R6-R1*" sebagai *port* anggota dari *interface bridge "bridgeHotspot"*.

```
[admin@R6] > interface bridge port add bridge=bridgeHotspot
interface=eoip-R6-R1
```

4. Menambahkan *interface ether2* sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R6] > interface bridge port add bridge=bridgeHotspot
interface=ether2
```

5.1.5.4 Konfigurasi EoIP dan Bridge Pada Router R7

Adapun langkah-langkah konfigurasi *EoIP* dan *Bridge* yang dilakukan pada *router R7* adalah sebagai berikut:

1. Membuat *interface EoIP tunnel* dari *router R7* ke *R1*.

```
[admin@R7] > interface eoip add name=eoip-R7-R1 tunnel-id=7
local-address=10.0.1.7 remote-
address=10.0.1.1 comment="EoIP dari R7 ke R1"
disabled=no
```

2. Membuat *interface bridge* dengan nama "*bridgeHotspot*".

```
[admin@R7] > interface bridge add name=bridgeHotspot
```

3. Menambahkan *interface Eoip* dengan nama "*eoip-R7-R1*" sebagai *port* anggota dari *interface bridge "bridgeHotspot"*.

```
[admin@R7] > interface bridge port add bridge=bridgeHotspot
             interface=eoip-R7-R1
```

4. Menambahkan *interface ether2* sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R7] > interface bridge port add bridge=bridgeHotspot
             interface=ether2
```

5.1.5.5 Konfigurasi EoIP dan Bridge Pada Router R8

Adapun langkah-langkah konfigurasi *EoIP* dan *Bridge* yang dilakukan pada *router R8* adalah sebagai berikut:

1. Membuat *interface EoIP tunnel* dari *router R8* ke *R1*.

```
[admin@R8] > interface eoip add name=eoip-R8-R1 tunnel-id=8
             local-address=10.0.1.8 remote-
             address=10.0.1.1 comment="EoIP dari R8 ke R1"
             disabled=no
```

2. Membuat *interface bridge* dengan nama "*bridgeHotspot*".

```
[admin@R8] > interface bridge add name=bridgeHotspot
```

3. Menambahkan *interface Eoip* dengan nama "*eoip-R8-R1*" sebagai *port* anggota dari *interface bridge "bridgeHotspot"*.

```
[admin@R8] > interface bridge port add bridge=bridgeHotspot
             interface=eoip-R8-R1
```

4. Menambahkan *interface ether2* sebagai *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R8] > interface bridge port add bridge=bridgeHotspot
             interface=ether2
```

5.1.6 Konfigurasi DHCP Server

Adapun langkah-langkah konfigurasi *DHCP Server* yang dilakukan pada router R1 adalah sebagai berikut:

1. Mengatur pengalamatan IP pada *interface bridge "bridgeHotspot"*.

```
[admin@R1] > ip address add address=10.0.2.1/24
                interface=bridgeHotspot
```

2. Mengatur *IP Pool* dengan nama "*poolHotspot*" dan menentukan ruang alamat IP yang akan disewakan ke *DHCP client* yaitu dari alamat 10.0.2.25 sampai dengan 10.0.2.254.

```
[admin@R1] > ip pool add name=poolHotspot ranges=10.0.2.25-
             10.0.2.254
```

3. Mengatur *IP DHCP Server Network* untuk menentukan parameter TCP/IP yang didistribusikan ke *DHCP Client* meliputi alamat jaringan 10.0.2.0/24, *server DNS* 10.0.2.1 *gateway* untuk komunikasi antar jaringan 10.0.2.1 dan *netmask* /32.

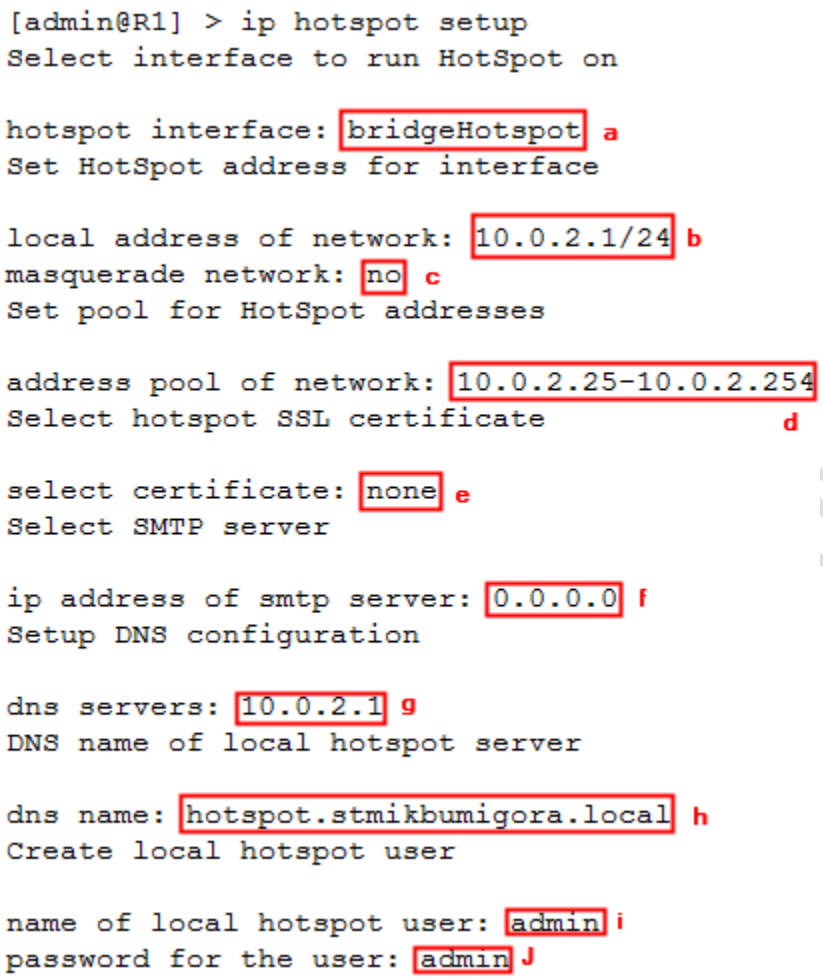
```
[admin@R1] > ip dhcp-server network add address=10.0.2.0/24
             dns-server=10.0.2.1        gateway=10.0.2.1
             netmask=32
```

4. Mengatur IP DHCP Server

```
[admin@R1] > ip dhcp-server add add-arp=yes address-
             pool=poolHotspot              disabled=no
             interface=bridgeHotspot     lease-time=3h
             name=dhcpHotspot
```

5.1.7 Konfigurasi Hotspot

Pengaktifan fitur hotspot pada router R1 dapat dilakukan dengan mengeksekusi perintah "`ip hotspot setup`", seperti terlihat pada gambar 5.1.



Gambar 5.1 IP Hotspot Setup

Keterangan:

a) `Hotspot interface`: menentukan pada *interface* dimana *hotspot* bekerja, yaitu "*bridgeHotspot*".

b) `Local address of network`: menentukan alamat *gateway* dari *Hotspot*, yaitu "10.0.2.1/24".

c) `Masquerade network`: menonaktifkan fitur masquerade pada jaringan hotspot yaitu "*no*".

d) `Address pool of network`: menentukan jangkauan ruang alamat IP yang didistribusikan ke client DHCP yaitu "*10.0.2.25-10.0.2.254*".

e) `Select certificate`: menonaktifkan fitur otorisasi HTTPS pada hotspot yaitu "*none*" .

f) `IP address of smtp server`: mengabaikan penentuan alamat IP dari server SMTP yaitu "0.0.0.0" .

g) `Dns servers`: menentukan alamat IP dari Server DNS, yaitu "10.0.2.1" .

h) `Dns name`: menentukan nama domain untuk *hotspot server* yang dibuat, diperlukan nama domain lengkap yaitu "*hotspot.stmikbumigora.local*".

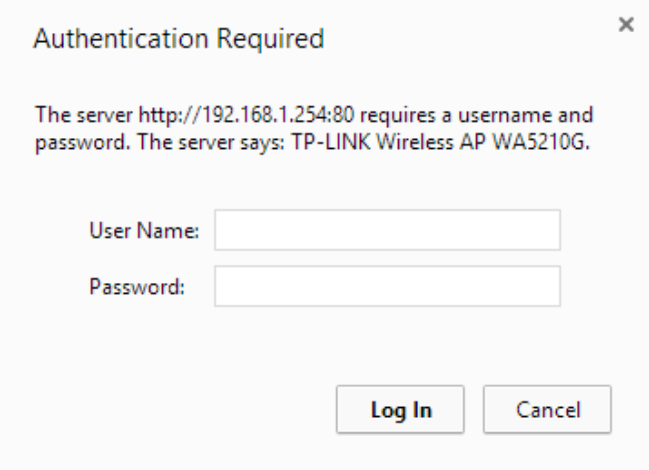
i) `Name of local hotspot user`: menentukan nama login user *hotspot* pertama yang dibuat, yaitu dengan nama "*admin*".

j) `Password for the user`: menentukan sandi login user *hotspot* pertama yang dibuat, yaitu "*admin*".

5.1.8 Konfigurasi Access Point

Terdapat 4 (empat) perangkat *Access Point (AP)* yang digunakan yaitu *AP1*, *AP2*, *AP3* dan *AP4*. Adapun langkah-langkah konfigurasi yang dilakukan pada keseluruhan perangkat AP adalah sebagai berikut:

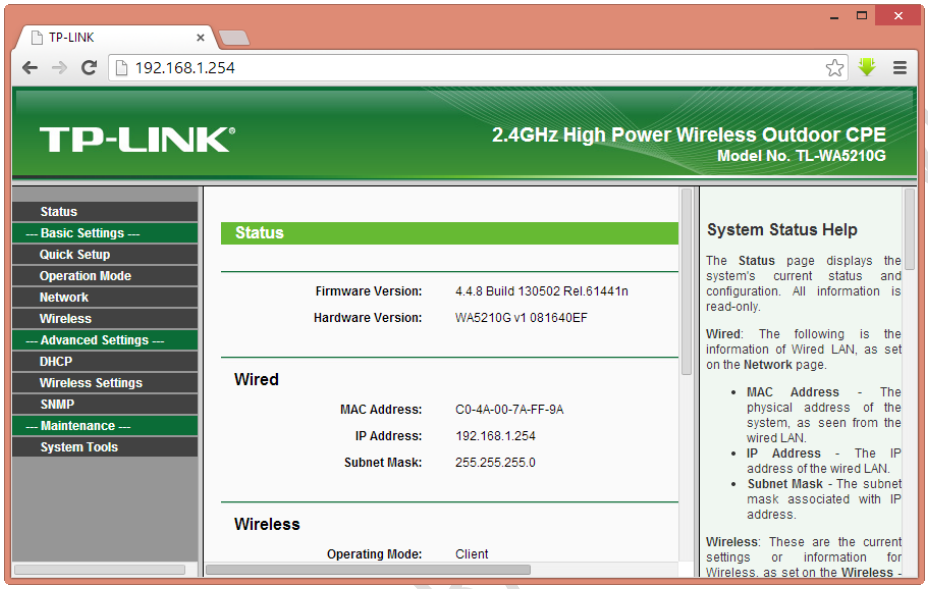
1. Mengakses halaman administrasi dari AP dengan mengakses alamat IP **192.168.1.254** maka selanjutnya akan tampil halaman login, seperti terlihat pada gambar 5.2.



Gambar 5.2 Halaman Login Administrasi AP

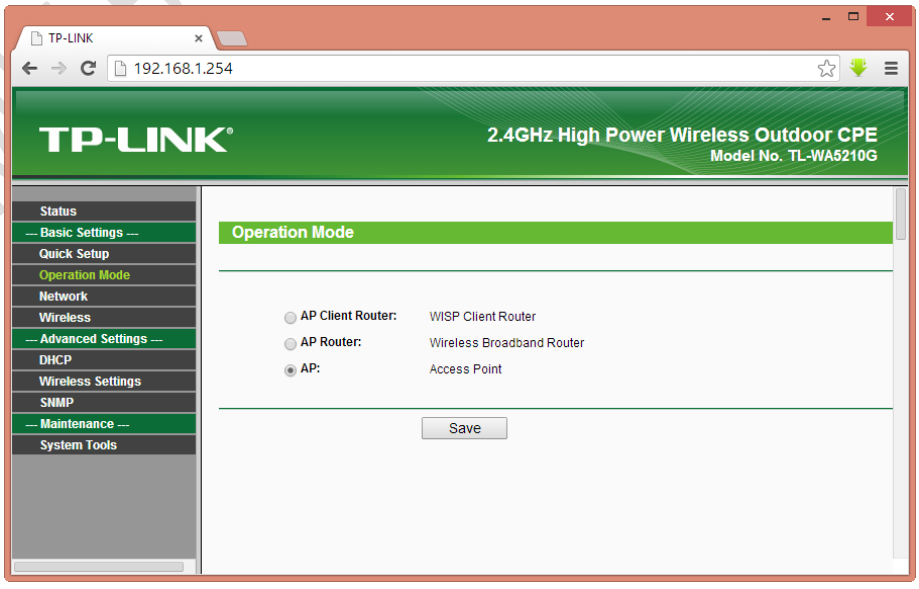
Proses login dapat dilakukan dengan melengkapi inputan parameter **User Name:** dan inputan parameter **Password:** menggunakan nilai "**admin**" serta memilih tombol **Log In**.

2. Tampil halaman administrasi dari *Access Point*, seperti terlihat pada gambar 5.3.



Gambar 5.3 Halaman Administrasi AP

3. Mengatur mode operasi dengan memilih menu "*Operation Mode"* pada pilihan menu navigasi di panel sebelah kiri. Pada panel detail akan tampil pengaturan *Operation Mode*, seperti terlihat pada gambar 5.4.

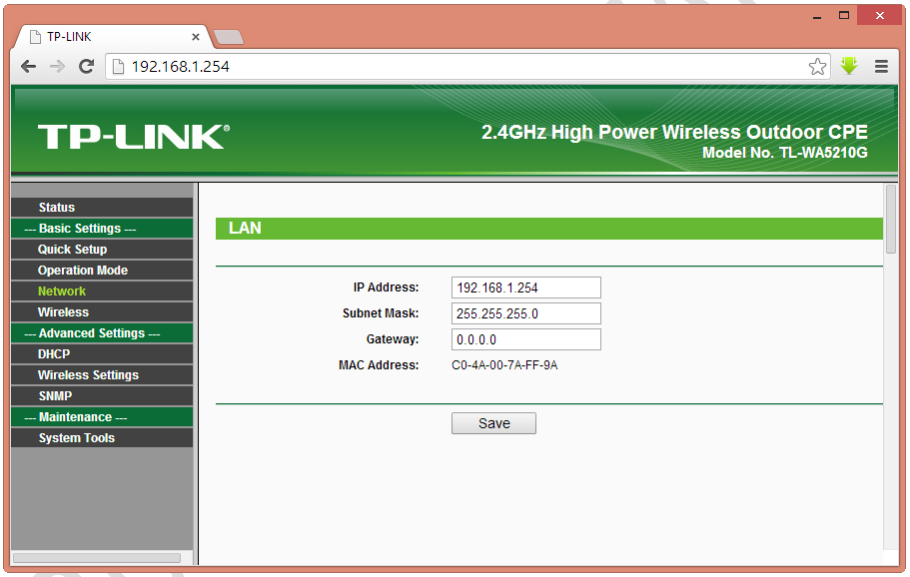


Gambar 5.4 Operation Mode

Pilih **AP: Access Point** untuk memfungsikan sebagai *Access Point* dan menyimpan perubahan konfigurasi dengan menekan tombol **Save**.

4. Mengatur pengalamatan IP untuk mengakses ke halaman administrasi *Access Point* sehingga dapat dimanajemen secara jarak jauh. Pada panel sebelah kiri pilih **Network**, maka pada panel sebelah kanan akan tampil pengaturan **LAN** seperti terlihat pada gambar 5.5. Terdapat beberapa parameter yang harus diatur antara lain:

    a) **IP Address**, digunakan untuk menentukan alamat IP. Masing-masing AP memiliki alamat IP, seperti terlihat pada tabel 5.1.



Gambar 5.5 LAN

Tabel 5.1 Pengalamatan IP dari AP

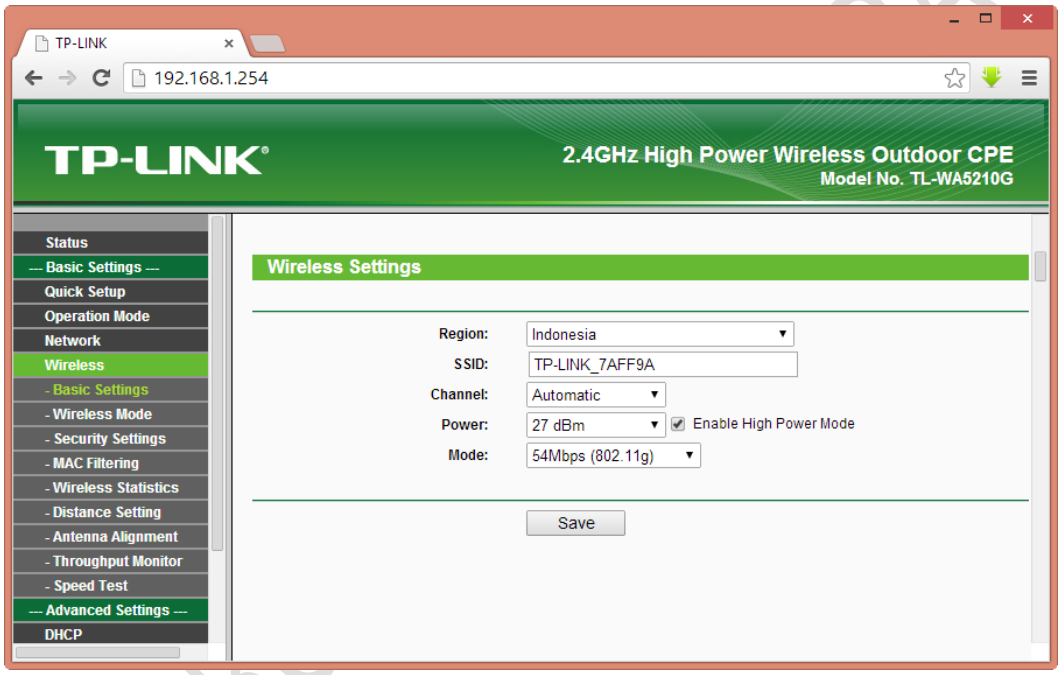
No.	Nama Perangkat	Alamat IP
1.	AP1	10.0.2.2
2.	AP2	10.0.2.3
3.	AP3	10.0.2.4
4.	AP4	10.0.2.5

b) **Subnet Mask**, digunakan untuk menentukan alamat subnetmask yaitu **255.255.255.0**.

c) **Gateway**, digunakan untuk menentukan alamat *default gateway* untuk komunikasi antar jaringan, masukkan **10.0.2.1**.

Menyimpan perubahan dengan menekan tombol **Save**.

5. Mengatur fitur **Wireless**. Pada panel sebelah kiri pilih **Wireless**, maka pada panel detail akan tampil pengaturan **Wireless Settings** seperti terlihat pada gambar 5.6.



Gambar 5.6 Wireless Settings

Terdapat beberapa parameter yang harus diatur antara lain:

a) **Region**, digunakan untuk menentukan pilihan Negara, pilih **Indonesia**.

b) **SSID**, digunakan untuk menentukan nama pengenal jaringan nirkabel yang dibuat, masukkan **STMIK Bumigora**.

c) **Channel**, digunakan untuk menentukan channel wireless, pilih **Automatic**.

d) **Power**, digunakan untuk menentukan *transmit power* dari *Access Point*, pilih **27 dBm** dan aktifkan pilihan **Enable High Power Mode** untuk meningkatkan unjuk kerja.

e) Mode, digunakan untuk menentukan mode wireless, pilih **54Mbps (802.11g)**.

Hasil dari pengaturan isian masing-masing parameter terlihat seperti pada gambar berikut:

Gambar 5.7 Hasil Pengaturan Wireless Settings

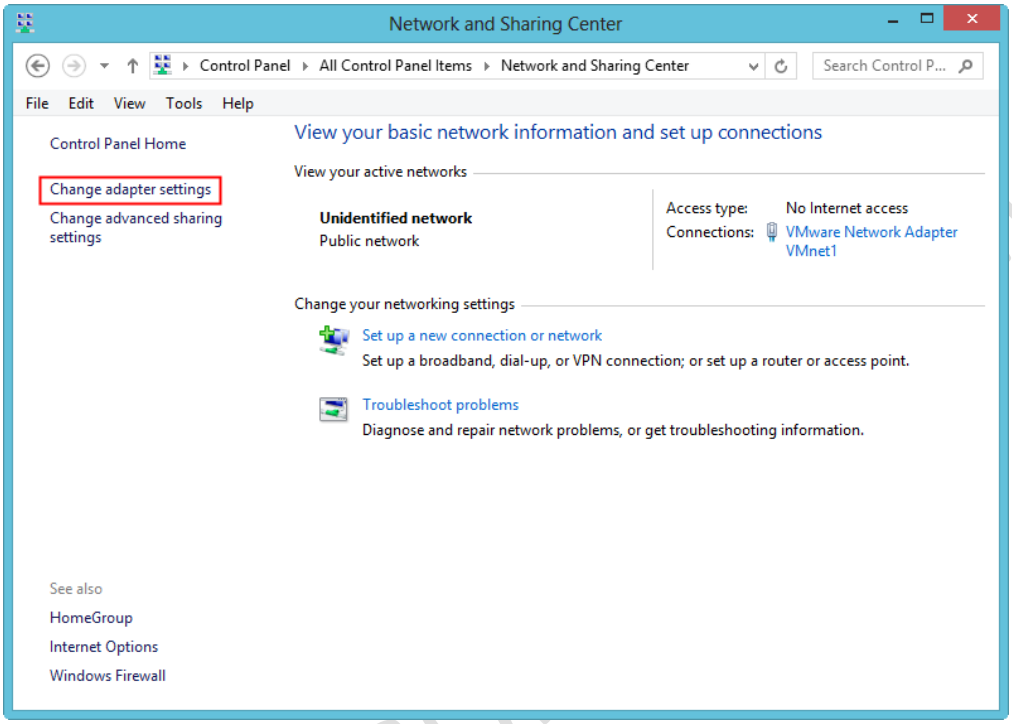
Menyimpan perubahan dengan menekan tombol **Save**.

5.1.9 Konfigurasi DHCP Client Pada Komputer Client Hotspot

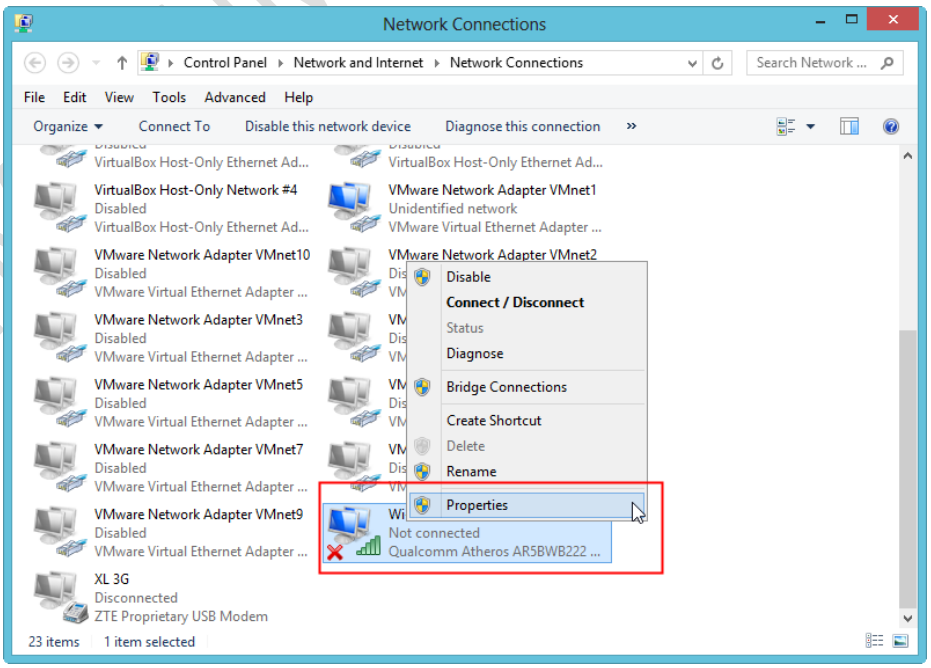
Adapun langkah-langkah konfigurasi DHCP Client yang dilakukan pada komputer Client Hotspot dengan sistem operasi Windows adalah sebagai berikut:

1. Mengakses *Network and Sharing Center* pada *Control Panel*.
2. Pada panel sebelah kiri dari kotak dialog *Network and Sharing Center* yang tampil, pilih *Change adapter Settings*, seperti terlihat pada gambar 5.8.
3. Mengakses *Properties* dari *Wi-Fi Adapter* pada kotak dialog *Network Connections* yang tampil, seperti terlihat pada gambar 5.9.

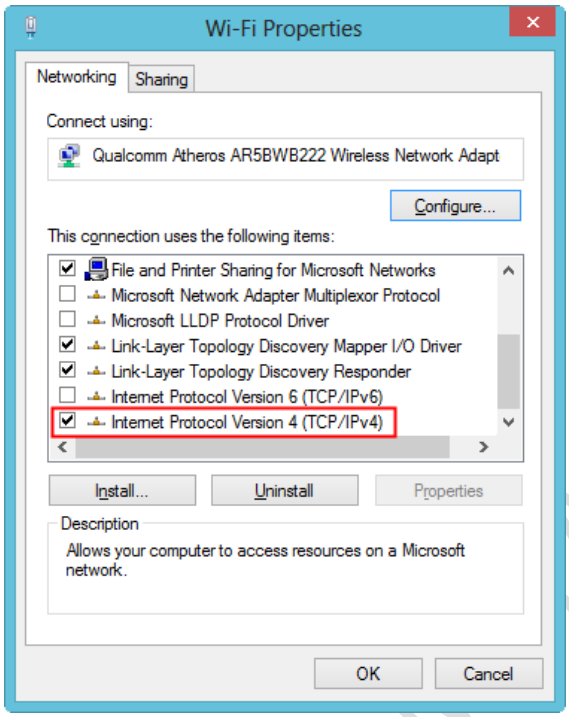
4. Tampil kotak dialog *Wi-Fi Properties*. Pada bagian "*This connection uses the following items:*" pilih "*Internet Protocol Version 4 (TCP/IPv4)*" dan tombol *Properties*, seperti terlihat pada gambar 5.10.



Gambar 5.8 Network and Sharing Center

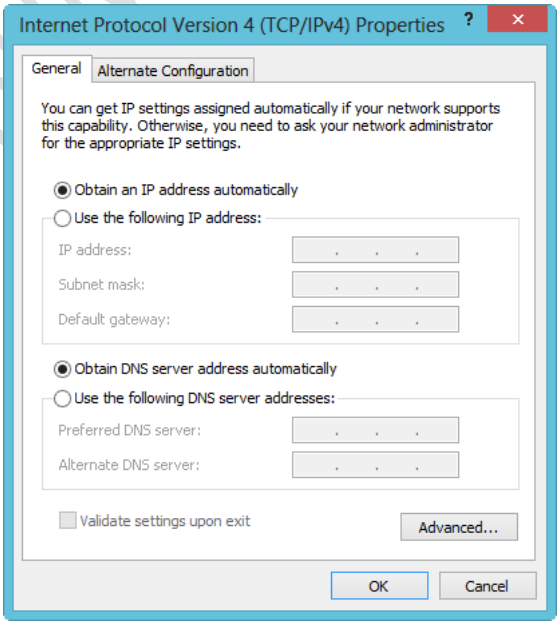


Gambar 5.9 Network Connections



Gambar 5.10 Wi-Fi Properties

5. Tampil kotak dialog "*Internet Protocol Version 4 (TCP/IPv4) Properties*". Pilih "*Obtain an IP address automatically"* dan "*Obtain DNS server address automatically"*, seperti terlihat pada gambar 5.11.



Gambar 5.11 Internet Protocol Version 4 (TCP/IPv4) Properties

Menyimpan pengaturan dengan menekan tombol *OK*.

5.2 Ujicoba

Ujicoba terdiri dari 2 (dua) bagian yaitu verifikasi konfigurasi dan ujicoba berbasis skenario.

5.2.1 Verifikasi Konfigurasi

Verifikasi konfigurasi dilakukan pada keseluruhan router meliputi konfigurasi dasar, *routing protocol OSPF*, *NTP Client*, *SSTP*, *EoIP*, *Bridge*, *DHCP Server* dan *Hotspot*.

5.2.1.1 Verifikasi Konfigurasi Pada Router R1

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada router R1 adalah sebagai berikut:

1. Menampilkan informasi interface *PPPoE Client*.

```
[admin@R1] > interface pppoe-client print
Flags: X - disabled, R - running
 0  R name="pppoe-out1" max-mtu=auto max-mru=auto mrru=disabled
      interface=ether1 user="username@isp" password="password"
      profile=default keepalive-timeout=60 service-name=""
      ac-name="" add-default-route=yes default-route-distance=0
      dial-on-demand=no use-peer-dns=yes allow=pap,chap,mschap1,
      mschap2
```

2. Menampilkan informasi pengalamatan IP pada *interface*.

```
[admin@R1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 192.168.0.2/32     192.168.0.1     pppoe-out1
 1   10.0.0.1/30        10.0.0.0        ether2
```

3. Menampilkan informasi pengaturan *routing ospf network*.

```
[admin@R1] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.0/30        backbone
```

4. Menampilkan informasi table *routing*.

```
[admin@R1] > ip route print
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 ADS  0.0.0.0/0                          192.168.0.1               0
 1 ADC  10.0.0.0/30        10.0.0.1        ether2                    0
 2 ADo  10.0.0.4/30                        10.0.0.2                110
 3 ADo  10.0.0.8/30                        10.0.0.2                110
 4 ADo  10.0.0.12/30                       10.0.0.2                110
 5 ADo  10.0.0.16/30                       10.0.0.2                110
 6 ADo  10.0.0.20/30                       10.0.0.2                110
 7 ADo  10.0.0.24/30                       10.0.0.2                110
 8 ADC  192.168.0.1/32     192.168.0.2     pppoe-out1                0
```

5. Menampilkan informasi pengaturan *route redistribution* untuk *default route*.

```
[admin@R1] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=0.0.0.0 distribute-default=always-as-type-1
      redistribute-connected=no redistribute-static=no redistribute-rip=no
      redistribute-bgp=no redistribute-other-ospf=no metric-default=1
      metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

6. Menampilkan informasi pengaturan *IP Firewall NAT* untuk berbagi pakai koneksi *Internet*.

```
[admin@R1] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade out-interface=pppoe-out1
```

7. Menampilkan informasi pengaturan sebagai DNS Server bagi jaringan lokal.

```
[admin@R1] > ip dns print
                  servers:
            dynamic-servers: 192.168.0.1
  allow-remote-requests: yes
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
              cache-size: 2048KiB
           cache-max-ttl: 1w
              cache-used: 9KiB
```

8. Menampilkan informasi pengaturan NTP Client.

```
[admin@R1] > system ntp client print
       enabled: yes
  server-dns-names: 0.id.pool.ntp.org,1.asia.pool.ntp.org
          mode: unicast
     poll-interval: 16s
     active-server: 203.89.31.13
```

9. Menampilkan informasi pengaturan *time zone*.

```
[admin@R1] > system clock print
              time: 23:04:06
              date: dec/26/2016
  time-zone-autodetect: yes
      time-zone-name: Asia/Makassar
          gmt-offset: +08:00
          dst-active: no
```

10. Menampilkan informasi *CA*, *Server* dan *Client Cerficate* yang telah dibuat.

```
[admin@R1] > certificate print detail
Flags: K - private-key, D - dsa, L - crl, C - smart-card-key, A - authority,
I - issued, R - revoked, E - expired, T - trusted
 0 K L A  T name="hotspotCA" country="ID" state="Nusa Tenggara Barat"
           locality="Mataram" organization="STMIK Bumigora" unit="PusTIK"
           common-name="hotspotCA" key-size=2048 days-valid=365 trusted=yes
           key-usage=key-cert-sign,crl-sign ca-crl-host="10.0.0.1"
           serial-number="49D07361387A785A"
           fingerprint="ec90623df41f46f3778cc4a599f93a4c6647fac68af749ed0aaceeb72aa6fc44"
           invalid-before=dec/27/2016 12:39:01 invalid-after=dec/27/2017 12:39:01

 1 K   A  T name="hotspotServer" country="ID" state="Nusa Tenggara Barat"
           locality="Mataram" organization="STMIK Bumigora" unit="PusTIK"
           common-name="10.0.0.1" key-size=2048 days-valid=365 trusted=yes
           key-usage=digital-signature,key-encipherment,data-encipherment,
           key-cert-sign,crl-sign,tls-server,tls-client ca=hotspotCA
           serial-number="4330ADAB12EC9701"
           fingerprint="3a2b1789fff0e40fc32aba242048fe7f80f7d6b3d278777b6e07c48ebb062085"
           invalid-before=dec/27/2016 12:40:49 invalid-after=dec/27/2017 12:40:49

 2 K   A  T name="hotspotClient" country="ID" state="Nusa Tenggara Barat"
           locality="Mataram" organization="STMIK Bumigora" unit="PusTIK"
           common-name="hotspotClient" key-size=2048 days-valid=365 trusted=yes
           key-usage=digital-signature,key-encipherment,data-encipherment,key-cert-sign,
           crl-sign,tls-server,tls-client ca=hotspotCA serial-number="73D0DEDCA8AFD695"
           fingerprint="083612a48252c6d5233298aadb7c7514832bb60bb39b48991652526065e4b433"
           invalid-before=dec/27/2016 12:41:16 invalid-after=dec/27/2017 12:41:16
```

11. Menampilkan informasi *file* hasil *export CA* dan *Client Certificate*.

```
[admin@R1] > file print
 # NAME                                                                TYPE
 0 skins                                                               directory
 1 cert_export_hotspotClient.crt                                       .crt file
 2 cert_export_hotspotClient.key                                       .key file
 3 cert_export_hotspotCA.crt                                           .crt file
 4 cert_export_hotspotCA.key                                           .key file
 5 R1.backup                                                           backup
 6 R1.rsc                                                              script
 7 auto-before-reset.backup                                            backup
 8 pub                                                                 directory
 9 R1-compact.rsc                                                      script
```

12. Menampilkan informasi pengaturan akun *SSTP Client*.

```
[admin@R1] > ppp secret print
Flags: X - disabled
 #   NAME                    SERVICE CALLER-ID  PASSWORD  PROFILE  REMOTE-ADDRESS
 0   R5@stmikbumigora.local  sstp               12345678  default  10.0.1.5
 1   R6@stmikbumigora.local  sstp               12345678  default  10.0.1.6
 2   R7@stmikbumigora.local  sstp               12345678  default  10.0.1.7
 3   R8@stmikbumigora.local  sstp               12345678  default  10.0.1.8
```

13. Menampilkan informasi pengaturan *SSTP Server*.

```
[admin@R1] > interface sstp-server server print
                    enabled: yes
                       port: 443
                    max-mtu: 1500
                    max-mru: 1500
                       mrru: disabled
          keepalive-timeout: 60
            default-profile: default
             authentication: mschap2
                certificate: hotspotServer
  verify-client-certificate: yes
                  force-aes: no
                        pfs: no
               tls-version: any
```

14. Menampilkan informasi SSTP Client yang terkoneksi dengan SSTP Server.

```
[admin@R1] > interface sstp-server print
Flags: X - disabled, D - dynamic, R - running
 #     NAME                              USER          MTU CLIENT-ADDRESS UPTIME   ENCODING
 0  DR <sstp-R5@stmikbumigora.local>  R5@stmikb... 1500 10.0.0.14      46m27s  RC4
 1  DR <sstp-R6@stmikbumigora.local>  R6@stmikb... 1500 10.0.0.18      20m46s  RC4
 2  DR <sstp-R7@stmikbumigora.local>  R7@stmikb... 1500 10.0.0.22      5m52s   RC4
 3  DR <sstp-R8@stmikbumigora.local>  R8@stmikb... 1500 10.0.0.26      41s     RC4
```

15. Menampilkan informasi monitoring status tunnel antara router R1 dengan R5.

```
[admin@R1] > interface sstp-server monitor 0
          status: connected
          uptime: 5m4s
            user: R5@stmikbumigora.local
       caller-id: 10.0.0.14
        encoding: RC4
             mtu: 1500
  local-address: 10.0.1.1
 remote-address: 10.0.1.5
```

16. Menampilkan informasi monitoring status tunnel antara router R1 dengan R6.

```
[admin@R1] > interface sstp-server monitor 1
          status: connected
          uptime: 1m52s
            user: R6@stmikbumigora.local
       caller-id: 10.0.0.18
        encoding: RC4
             mtu: 1500
  local-address: 10.0.1.1
 remote-address: 10.0.1.6
```

17. Menampilkan informasi monitoring status tunnel antara router R1 dengan R7.

```
[admin@R1] > interface sstp-server monitor 2
          status: connected
          uptime: 6m8s
            user: R7@stmikbumigora.local
       caller-id: 10.0.0.22
        encoding: RC4
             mtu: 1500
  local-address: 10.0.1.1
 remote-address: 10.0.1.7
```

18. Menampilkan informasi monitoring status tunnel antara router R1 dengan R8.

```
[admin@R1] > interface sstp-server monitor 3
          status: connected
          uptime: 1m
            user: R8@stmikbumigora.local
       caller-id: 10.0.0.26
        encoding: RC4
             mtu: 1500
  local-address: 10.0.1.1
 remote-address: 10.0.1.8
```

19. Memverifikasi koneksi dari *router R1* sebagai *SSTP Server* ke alamat IP dari *interface SSTP Client* pada *router R5*.

```
[admin@R1] > ping 10.0.1.5
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.5                                   56  64 1ms
    1 10.0.1.5                                   56  64 1ms
    2 10.0.1.5                                   56  64 2ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms
```

20. Memverifikasi koneksi dari *router R1* sebagai *SSTP Server* ke alamat IP dari *interface* *SSTP Client* pada *router R6*.

```
[admin@R1] > ping 10.0.1.6
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.6                                   56  64 1ms
    1 10.0.1.6                                   56  64 1ms
    2 10.0.1.6                                   56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms
```

21. Memverifikasi koneksi dari *router R1* sebagai *SSTP Server* ke alamat IP dari *interface* *SSTP Client* pada *router R7*.

```
[admin@R1] > ping 10.0.1.7
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.7                                   56  64 1ms
    1 10.0.1.7                                   56  64 1ms
    2 10.0.1.7                                   56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms
```

22. Memverifikasi koneksi dari *router R1* sebagai *SSTP Server* ke alamat IP dari *interface* *SSTP Client* pada *router R8*.

```
[admin@R1] > ping 10.0.1.8
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.8                                   56  64 2ms
    1 10.0.1.8                                   56  64 1ms
    2 10.0.1.8                                   56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms
```

23. Menampilkan informasi *interface EoIP* yang dibuat untuk *tunneling* dari *router R1* ke *router R5, R6, R7* dan *R8*.

```
[admin@R1] > interface eoip print
Flags: X - disabled, R - running
 0    ;;; EoIP dari R1 ke R5
      name="eoip-R1-R5" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:DB:E1:E4:85:9F
      arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
      loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.1
      remote-address=10.0.1.5 tunnel-id=5 keepalive=10s,10 dscp=inherit
      clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes

 1    ;;; EoIP dari R1 ke R6
      name="eoip-R1-R6" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:29:4D:1E:5D:45
      arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
      loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.1
      remote-address=10.0.1.6 tunnel-id=6 keepalive=10s,10 dscp=inherit
      clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes

 2    ;;; EoIP dari R1 ke R7
      name="eoip-R1-R7" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:5A:A6:BE:6D:F0
      arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
      loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.1
      remote-address=10.0.1.7 tunnel-id=7 keepalive=10s,10 dscp=inherit
      clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes

 3    ;;; EoIP dari R1 ke R8
      name="eoip-R1-R8" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:71:88:D2:00:AB
      arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
      loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.1
      remote-address=10.0.1.8 tunnel-id=8 keepalive=10s,10 dscp=inherit
      clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes
```

24. Menampilkan informasi bridge "*bridgeHotspot*" yang dibuat untuk hotspot.

```
[admin@R1] > interface bridge print
Flags: X - disabled, R - running
 0  R name="bridgeHotspot" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled
      arp-timeout=auto mac-address=00:00:00:00:00:00 protocol-mode=rstp priority=0x8000
      auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s forward-delay=15s
      transmit-hold-count=6 ageing-time=5m
```

25. Menampilkan informasi *bridge port* yang menjadi *port* anggota dari *interface bridge* "*bridgeHotspot*".

```
[admin@R1] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #    INTERFACE                                                        BRIDGE
 0    eoip-R1-R5                                                       bridgeHotspot
 1    eoip-R1-R6                                                       bridgeHotspot
 2    eoip-R1-R7                                                       bridgeHotspot
 3    eoip-R1-R8                                                       bridgeHotspot
```

26. Menampilkan informasi pengalamatan IP yang diatur pada interface bridge "*bridgeHotspot*".

```
[admin@R1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    10.0.0.1/30        10.0.0.0        ether2
 1 D  192.168.0.2/32     192.168.0.1     pppoe-out1
 2 D  10.0.1.1/32        10.0.1.5        <sstp-R5@stmikbumigora.local>
 3 D  10.0.1.1/32        10.0.1.6        <sstp-R6@stmikbumigora.local>
 4 D  10.0.1.1/32        10.0.1.7        <sstp-R7@stmikbumigora.local>
 5 D  10.0.1.1/32        10.0.1.8        <sstp-R8@stmikbumigora.local>
 6    10.0.2.1/24        10.0.2.0        bridgeHotspot
```

27. Menampilkan informasi pengaturan *IP Pool*.

```
[admin@R1] > ip pool print
 # NAME           RANGES
 0 poolHotspot    10.0.2.25-10.0.2.254
```

28. Menampilkan informasi pengaturan *IP DHCP Server Network*.

```
[admin@R1] > ip dhcp-server network print
 # ADDRESS            GATEWAY         DNS-SERVER      WINS-SERVER     DOMAIN
 0 10.0.2.0/24        10.0.2.1        10.0.2.1
```

29. Menampilkan informasi pengaturan *IP DHCP Server*.

```
[admin@R1] > ip dhcp-server print
Flags: X - disabled, I - invalid
 #    NAME          INTERFACE       RELAY  ADDRESS-POOL    LEASE-TIME ADD-ARP
 0    dhcpHotspot   bridgeHotspot         poolHotspot     3h         yes
```

30. Menampilkan informasi pengaturan *IP Hotspot*.

```
[admin@R1] > ip hotspot print
Flags: X - disabled, I - invalid, S - HTTPS
 #    NAME       INTERFACE       ADDRESS-POOL    PROFILE   IDLE-TIMEOUT
 0    hotspot1   bridgeHotspot   poolHotspot     hsprof1   5m
```

31. Menampilkan informasi *user* pada *IP Hotspot*.

```
[admin@R1] > ip hotspot user print
Flags: * - default, X - disabled, D - dynamic
 #   SERVER                                NAME            ADDRESS  PROFILE    UPTIME
 0 * ;;; counters and limits for trial users
                                           default-trial                       0s
 1                                         admin                    default    0s
```

5.2.1.2 Verifikasi Konfigurasi Pada Router R2

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada router R2 adalah sebagai berikut:

1. Menampilkan informasi pengalamatan IP pada interface.

```
[admin@R2] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.2/30        10.0.0.0        ether1
 1   10.0.0.5/30        10.0.0.4        ether2
 2   10.0.0.9/30        10.0.0.8        ether3
```

2. Menampilkan informasi pengaturan *routing ospf network.*

```
[admin@R2] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.0/30        backbone
 1   10.0.0.4/30        backbone
 2   10.0.0.8/30        backbone
```

3. Menampilkan informasi *table routing.*

```
[admin@R2] > ip route print
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 ADo  0.0.0.0/0                          10.0.0.1                110
 1 ADC  10.0.0.0/30        10.0.0.2        ether1                    0
 2 ADC  10.0.0.4/30        10.0.0.5        ether2                    0
 3 ADC  10.0.0.8/30        10.0.0.9        ether3                    0
 4 ADo  10.0.0.12/30                       10.0.0.6                110
 5 ADo  10.0.0.16/30                       10.0.0.6                110
 6 ADo  10.0.0.20/30                       10.0.0.10               110
 7 ADo  10.0.0.24/30                       10.0.0.10               110
```

4. Menampilkan informasi pengaturan *DNS Client*.

```
[admin@R2] > ip dns print
                servers: 10.0.0.1
        dynamic-servers:
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
              cache-size: 2048KiB
           cache-max-ttl: 1w
              cache-used: 9KiB
```

5. Menampilkan informasi pengaturan *NTP Client*.

```
[admin@R2] > system ntp client print
          enabled: yes
  server-dns-names: 0.id.pool.ntp.org,1.asia.pool.ntp.org
              mode: unicast
```

6. Menampilkan informasi pengaturan *timezone*.

```
[admin@R2] > system clock print
                time: 23:07:41
                date: dec/26/2016
  time-zone-autodetect: yes
        time-zone-name: Asia/Makassar
            gmt-offset: +08:00
            dst-active: no
```

5.2.1.3 Verifikasi Konfigurasi Pada Router R3

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada *router R3* adalah sebagai berikut:

1. Menampilkan informasi pengalamatan IP pada *interface*.

```
[admin@R3] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.6/30        10.0.0.4        ether1
 1   10.0.0.13/30       10.0.0.12       ether2
 2   10.0.0.17/30       10.0.0.16       ether3
```

2. Menampilkan informasi pengaturan *routing ospf network*.

```
[admin@R3] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.4/30        backbone
 1   10.0.0.12/30       backbone
 2   10.0.0.16/30       backbone
```

3. Menampilkan informasi *table routing*.

```
[admin@R3] > ip route print
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 ADo  0.0.0.0/0                          10.0.0.5                110
 1 ADo  10.0.0.0/30                        10.0.0.5                110
 2 ADC  10.0.0.4/30        10.0.0.6        ether1                    0
 3 ADo  10.0.0.8/30                        10.0.0.5                110
 4 ADC  10.0.0.12/30       10.0.0.13       ether2                    0
 5 ADC  10.0.0.16/30       10.0.0.17       ether3                    0
 6 ADo  10.0.0.20/30                       10.0.0.5                110
 7 ADo  10.0.0.24/30                       10.0.0.5                110
```

4. Menampilkan informasi pengaturan *DNS Client*.

```
[admin@R3] > ip dns print
                  servers: 10.0.0.1
        dynamic-servers:
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
              cache-size: 2048KiB
           cache-max-ttl: 1w
              cache-used: 9KiB
```

5. Menampilkan informasi pengaturan *NTP Client*.

```
[admin@R3] > system ntp client print
           enabled: yes
  server-dns-names: 0.id.pool.ntp.org,1.asia.pool.ntp.org
              mode: unicast
     poll-interval: 16s
     active-server: 203.89.31.13
```

6. Menampilkan informasi pengaturan *timezone*.

```
[admin@R3] > system clock print
                  time: 23:10:24
                  date: dec/26/2016
  time-zone-autodetect: yes
         time-zone-name: Asia/Makassar
             gmt-offset: +08:00
             dst-active: no
```

5.2.1.4 Verifikasi Konfigurasi Pada Router R4

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada *router R4* adalah sebagai berikut:

1. Menampilkan informasi pengalamatan IP pada interface.

```
[admin@R4] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.10/30       10.0.0.8        ether1
 1   10.0.0.21/30       10.0.0.20       ether2
 2   10.0.0.25/30       10.0.0.24       ether3
```

2. Menampilkan informasi pengaturan *routing ospf network.*

```
[admin@R4] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.8/30        backbone
 1   10.0.0.20/30       backbone
 2   10.0.0.24/30       backbone
```

3. Menampilkan informasi *table routing*.

```
[admin@R4] > ip route print
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 ADo  0.0.0.0/0                          10.0.0.9                110
 1 ADo  10.0.0.0/30                        10.0.0.9                110
 2 ADo  10.0.0.4/30                        10.0.0.9                110
 3 ADC  10.0.0.8/30        10.0.0.10       ether1                    0
 4 ADo  10.0.0.12/30                       10.0.0.9                110
 5 ADo  10.0.0.16/30                       10.0.0.9                110
 6 ADC  10.0.0.20/30       10.0.0.21       ether2                    0
 7 ADC  10.0.0.24/30       10.0.0.25       ether3                    0
```

4. Menampilkan informasi pengaturan *DNS Client*.

```
[admin@R4] > ip dns print
                  servers: 10.0.0.1
        dynamic-servers:
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
              cache-size: 2048KiB
            cache-max-ttl: 1w
              cache-used: 9KiB
```

5. Menampilkan informasi pengaturan *NTP Client*.

```
[admin@R4] > system ntp client print
          enabled: yes
  server-dns-names: 0.id.ntp.pool.org,1.asia.ntp.pool.org
              mode: unicast
     poll-interval: 16s
     active-server: 64.99.80.121
```

6. Menampilkan informasi pengaturan *timezone*.

```
[admin@R4] > system clock print
                  time: 07:11:35
                  date: dec/27/2016
  time-zone-autodetect: yes
        time-zone-name: Asia/Makassar
            gmt-offset: +08:00
            dst-active: no
```

5.2.1.5 Verifikasi Konfigurasi Pada Router R5

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada *router R5* adalah sebagai berikut:

1. Menampilkan informasi pengalamatan IP pada interface.

```
[admin@R5] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.14/30       10.0.0.12       ether1
```

2. Menampilkan informasi pengaturan *routing ospf network.*

```
[admin@R5] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.12/30       backbone
```

3. Menampilkan informasi *table routing*.

```
[admin@R5] > ip route print
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 ADo  0.0.0.0/0                          10.0.0.13               110
 1 ADo  10.0.0.0/30                        10.0.0.13               110
 2 ADo  10.0.0.4/30                        10.0.0.13               110
 3 ADo  10.0.0.8/30                        10.0.0.13               110
 4 ADC  10.0.0.12/30       10.0.0.14       ether1                    0
 5 ADo  10.0.0.16/30                       10.0.0.13               110
 6 ADo  10.0.0.20/30                       10.0.0.13               110
 7 ADo  10.0.0.24/30                       10.0.0.13               110
```

4. Menampilkan informasi pengaturan *DNS Client*.

```
[admin@R5] > ip dns print
                  servers: 10.0.0.1
         dynamic-servers:
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
                cache-size: 2048KiB
           cache-max-ttl: 1w
                cache-used: 9KiB
```

5. Menampilkan informasi pengaturan *NTP Client*.

```
[admin@R5] > system ntp client print
           enabled: yes
  server-dns-names: 0.id.ntp.pool.org,1.asia.ntp.pool.org
                mode: unicast
     poll-interval: 16s
     active-server: 64.99.80.121
```

6. Menampilkan informasi pengaturan *timezone*.

```
[admin@R5] > system clock print
                  time: 23:13:23
                  date: dec/26/2016
  time-zone-autodetect: yes
         time-zone-name: Asia/Makassar
             gmt-offset: +00:00
             dst-active: no
```

7. Menampilkan informasi *file CA* dan *Client Certificate*.

```
[admin@R5] > file print
 # NAME                                                                TYPE
 0 skins                                                               directory
 1 auto-before-reset.backup                                            backup
 2 cert_export_hotspotCA.crt                                           .crt file
 3 cert_export_hotspotCA.key                                           .key file
 4 cert_export_hotspotClient.crt                                       .crt file
 5 cert_export_hotspotClient.key                                       .key file
 6 R5.backup                                                           backup
 7 R5.rsc                                                              script
 8 pub                                                                 directory
 9 R5-compact.rsc                                                      script
```

8. Menampilkan informasi *Certificate* yang telah di *import*.

```
[admin@R5] > certificate print
Flags: K - private-key, D - dsa, L - crl, C - smart-card-key, A - authority, I - issued,
R - revoked, E - expired, T - trusted
 #          NAME           COMMON-NAME   SUBJECT-ALT-NAME FINGERPRINT
 0 K L A  T hotspotCA      hotspotCA                      ec90623df41f46f3778cc4a599f93...
 1 K   A  T hotspotClient  hotspotClient                  083612a48252c6d5233298aadb7c7...
```

9. Menampilkan informasi *interface SSTP Client*.

```
[admin@R5] > interface sstp-client print
Flags: X - disabled, R - running
 0  R name="sstp-out1" max-mtu=1500 max-mru=1500 mrru=disabled connect-to=10.0.0.1:443
      http-proxy=0.0.0.0:443 certificate=hotspotClient verify-server-certificate=yes
      verify-server-address-from-certificate=yes user="R5@stmikbumigora.local"
      password="12345678" profile=default keepalive-timeout=60 add-default-route=no
      dial-on-demand=no authentication=mschap2 pfs=no tls-version=any
```

10. Menampilkan informasi *monitoring* status *tunnel* antara *router R5* dengan *R1*.

```
[admin@R5] > interface sstp-client monitor sstp-out1
         status: connected
         uptime: 1m22s
       encoding: RC4
            mtu: 1500
  local-address: 10.0.1.5
 remote-address: 10.0.1.1
```

11. Memverifikasi koneksi dari *SSTP Client* ke *SSTP Server*.

```
[admin@R5] > ping 10.0.1.1
SEQ HOST                                     SIZE TTL TIME  STATUS
  0 10.0.1.1                                   56  64 1ms
  1 10.0.1.1                                   56  64 1ms
  2 10.0.1.1                                   56  64 2ms
  sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms
```

12. Menampilkan informasi *interface EoIP* untuk tunneling dari router R5 ke R1.

```
[admin@R5] > interface eoip print
Flags: X - disabled, R - running
 0  R ;;; EoIP dari R5 ke R1
     name="eoip-R5-R1" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:CD:09:DD:05:03
     arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
     loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.5
     remote-address=10.0.1.1 tunnel-id=5 keepalive=10s,10 dscp=inherit
     clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes
```

13. Menampilkan informasi interface *bridge*.

```
[admin@R5] > interface bridge print
Flags: X - disabled, R - running
 0  R name="bridgeHotspot" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled
     arp-timeout=auto mac-address=00:00:00:00:00:00 protocol-mode=rstp
     priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s
     forward-delay=15s transmit-hold-count=6 ageing-time=5m
```

14. Menampilkan informasi *interface bridge port*.

```
[admin@R5] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #     INTERFACE   BRIDGE          PRIORITY  PATH-COST    HORIZON
 0     eoip-R5-R1  bridgeHotspot   0x80         10        none
 1     ether2      bridgeHotspot   0x80         10        none
```

5.2.1.6 Verifikasi Konfigurasi Pada Router R6

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada *router R6* adalah sebagai berikut:

1. Menampilkan informasi pengalamatan IP pada interface.

```
[admin@R6] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.18/30       10.0.0.16       ether1
```

2. Menampilkan informasi pengaturan *routing ospf network.*

```
[admin@R6] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.16/30       backbone
```

3. Menampilkan informasi *table routing*.

```
[admin@R6] > ip route print
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 ADo  0.0.0.0/0                          10.0.0.17               110
 1 ADo  10.0.0.0/30                        10.0.0.17               110
 2 ADo  10.0.0.4/30                        10.0.0.17               110
 3 ADo  10.0.0.8/30                        10.0.0.17               110
 4 ADo  10.0.0.12/30                       10.0.0.17               110
 5 ADC  10.0.0.16/30       10.0.0.18       ether1                    0
 6 ADo  10.0.0.20/30                       10.0.0.17               110
 7 ADo  10.0.0.24/30                       10.0.0.17               110
```

4. Menampilkan informasi pengaturan *DNS Client*.

```
[admin@R6] > ip dns print
                  servers: 10.0.0.1
        dynamic-servers:
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
              cache-size: 2048KiB
           cache-max-ttl: 1w
              cache-used: 9KiB
```

5. Menampilkan informasi pengaturan *NTP Client*.

```
[admin@R6] > system ntp client print
           enabled: yes
  server-dns-names: 0.id.ntp.pool.org,1.asia.ntp.pool.org
              mode: unicast
     poll-interval: 16s
     active-server: 64.99.80.121
```

6. Menampilkan informasi pengaturan *timezone*.

```
[admin@R6] > system clock print
                  time: 07:16:35
                  date: dec/27/2016
  time-zone-autodetect: yes
        time-zone-name: Asia/Makassar
            gmt-offset: +08:00
            dst-active: no
```

7. Menampilkan informasi *file CA* dan *Client Certificate*.

```
[admin@R6] > file print
 # NAME                                                                TYPE
 0 skins                                                               directory
 1 cert_export_hotspotClient.key                                       .key file
 2 cert_export_hotspotCA.crt                                           .crt file
 3 cert_export_hotspotCA.key                                           .key file
 4 cert_export_hotspotClient.crt                                       .crt file
 5 R6.backup                                                           backup
 6 R6.rsc                                                              script
 7 auto-before-reset.backup                                            backup
 8 pub                                                                 directory
 9 R6-compact.rsc                                                      script
```

8. Menampilkan informasi *Certificate* yang telah di *import*.

```
[admin@R6] > certificate print
Flags: K - private-key, D - dsa, L - crl, C - smart-card-key, A - authority, I - issued,
R - revoked, E - expired, T - trusted
 #          NAME           COMMON-NAME    SUBJECT-ALT-NAME FINGERPRINT
 0 K L A  T hotspotCA      hotspotCA                       ec90623df41f46f3778cc4a599f93...
 1 K   A  T hotspotClient  hotspotClient                   083612a48252c6d5233298aadb7c7...
```

9. Menampilkan informasi *interface SSTP Client*.

```
[admin@R6] > interface sstp-client print
Flags: X - disabled, R - running
 0  R name="sstp-out1" max-mtu=1500 max-mru=1500 mrru=disabled connect-to=10.0.0.1:443
      http-proxy=0.0.0.0:443 certificate=hotspotClient verify-server-certificate=yes
      verify-server-address-from-certificate=yes user="R6@stmikbumigora.local"
      password="12345678" profile=default keepalive-timeout=60 add-default-route=no
      dial-on-demand=no authentication=mschap2 pfs=no tls-version=any
```

10. Menampilkan informasi *monitoring* status *tunnel* antara *router R6* dengan *R1*.

```
[admin@R6] > interface sstp-client monitor sstp-out1
          status: connected
          uptime: 29s
        encoding: RC4
             mtu: 1500
  local-address: 10.0.1.6
 remote-address: 10.0.1.1
```

11. Memverifikasi koneksi dari *SSTP Client* ke *SSTP Server*.

```
[admin@R6] > ping 10.0.1.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.1                                   56  64 1ms
    1 10.0.1.1                                   56  64 1ms
    2 10.0.1.1                                   56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms
```

12. Menampilkan informasi *interface EoIP* untuk tunneling dari router R6 ke R1.

```
[admin@R6] > interface eoip print
Flags: X - disabled, R - running
 0  R ;;; EoIP dari R6 ke R1
     name="eoip-R6-R1" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:F7:60:27:F3:09
     arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
     loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.6
     remote-address=10.0.1.1 tunnel-id=6 keepalive=10s,10 dscp=inherit
     clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes
```

13. Menampilkan informasi interface *bridge*.

```
[admin@R6] > interface bridge print
Flags: X - disabled, R - running
 0  R name="bridgeHotspot" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto
     mac-address=00:00:00:00:00:00 protocol-mode=rstp priority=0x8000 auto-mac=yes
     admin-mac=00:00:00:00:00:00 max-message-age=20s forward-delay=15s transmit-hold-count=6
     ageing-time=5m
```

14. Menampilkan informasi *interface bridge port*.

```
[admin@R6] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #     INTERFACE   BRIDGE          PRIORITY  PATH-COST    HORIZON
 0     eoip-R6-R1  bridgeHotspot   0x80         10        none
 1     ether2      bridgeHotspot   0x80         10        none
```

5.2.1.7 Verifikasi Konfigurasi Pada Router R7

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada *router R7* adalah sebagai berikut:

1. Menampilkan informasi pengalamatan IP pada interface.

```
[admin@R7] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.22/30       10.0.0.20       ether1
```

2. Menampilkan informasi pengaturan *routing ospf network.*

```
[admin@R7] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.20/30       backbone
```

3. Menampilkan informasi *table routing.*

```
[admin@R7] > ip route print
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 ADo  0.0.0.0/0                          10.0.0.21               110
 1 ADo  10.0.0.0/30                        10.0.0.21               110
 2 ADo  10.0.0.4/30                        10.0.0.21               110
 3 ADo  10.0.0.8/30                        10.0.0.21               110
 4 ADo  10.0.0.12/30                       10.0.0.21               110
 5 ADo  10.0.0.16/30                       10.0.0.21               110
 6 ADC  10.0.0.20/30       10.0.0.22       ether1                    0
 7 ADo  10.0.0.24/30                       10.0.0.21               110
```

4. Menampilkan informasi pengaturan *DNS Client*.

```
[admin@R7] > ip dns print
                  servers: 10.0.0.1
        dynamic-servers:
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
            cache-size: 2048KiB
          cache-max-ttl: 1w
             cache-used: 9KiB
```

5. Menampilkan informasi pengaturan *NTP Client*.

```
[admin@R7] > system ntp client print
          enabled: yes
  server-dns-names: 0.id.pool.ntp.org,1.asia.pool.ntp.org
              mode: unicast
     poll-interval: 16s
     active-server: 103.20.91.62
```

6. Menampilkan informasi pengaturan *timezone*.

```
[admin@R7] > system clock print
                  time: 23:18:39
                  date: dec/26/2016
  time-zone-autodetect: yes
        time-zone-name: Asia/Makassar
            gmt-offset: +08:00
            dst-active: no
```

7. Menampilkan informasi *file CA* dan *Client Certificate*.

```
[admin@R7] > file print
 # NAME                                                                TYPE
 0 skins                                                               directory
 1 auto-before-reset.backup                                            backup
 2 cert_export_hotspotClient.key                                       .key file
 3 cert_export_hotspotCA.crt                                           .crt file
 4 cert_export_hotspotCA.key                                           .key file
 5 cert_export_hotspotClient.crt                                       .crt file
 6 R7.rsc                                                              script
 7 pub                                                                 directory
 8 R7.backup                                                           backup
 9 R7-compact.rsc                                                      script
```

8. Menampilkan informasi *Certificate* yang telah di *import*.

```
[admin@R7] > certificate print
Flags: K - private-key, D - dsa, L - crl, C - smart-card-key, A - authority, I - issued,
R - revoked, E - expired, T - trusted
 #          NAME           COMMON-NAME    SUBJECT-ALT-NAME  FINGERPRINT
 0 K L A  T hotspotCA      hotspotCA                        ec90623df41f46f3778cc4a599f93...
 1 K    A  T hotspotClient  hotspotClient                   083612a48252c6d5233298aadb7c7...
```

9. Menampilkan informasi *interface SSTP Client*.

```
[admin@R7] > interface sstp-client print
Flags: X - disabled, R - running
 0  R name="sstp-out1" max-mtu=1500 max-mru=1500 mrru=disabled connect-to=10.0.0.1:443
      http-proxy=0.0.0.0:443 certificate=hotspotClient verify-server-certificate=yes
      verify-server-address-from-certificate=yes user="R7@stmikbumigora.local"
      password="12345678" profile=default keepalive-timeout=60 add-default-route=no
      dial-on-demand=no authentication=mschap2 pfs=no tls-version=any
```

10. Menampilkan informasi *monitoring* status *tunnel* antara *router R7* dengan *R1*.

```
[admin@R7] > interface sstp-client monitor sstp-out1
          status: connected
          uptime: 18s
        encoding: RC4
             mtu: 1500
  local-address: 10.0.1.7
 remote-address: 10.0.1.1
```

11. Memverifikasi koneksi dari *SSTP Client* ke *SSTP Server*.

```
[admin@R7] > ping 10.0.1.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.1                                   56  64 1ms
    1 10.0.1.1                                   56  64 1ms
    2 10.0.1.1                                   56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms
```

12. Menampilkan informasi *interface EoIP* untuk tunneling dari *router R7* ke *R1*.

```
[admin@R7] > interface eoip print
Flags: X - disabled, R - running
 0  R ;;; EoIP dari R7 ke R1
     name="eoip-R7-R1" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:90:C2:93:9B:DC
     arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
     loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.7
     remote-address=10.0.1.1 tunnel-id=7 keepalive=10s,10 dscp=inherit
     clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes
```

13. Menampilkan informasi interface *bridge*.

```
[admin@R7] > interface bridge print
Flags: X - disabled, R - running
 0  R name="bridgeHotspot" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled
     arp-timeout=auto mac-address=00:00:00:00:00:00 protocol-mode=rstp
     priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00
     max-message-age=20s forward-delay=15s transmit-hold-count=6
     ageing-time=5m
```

14. Menampilkan informasi *interface bridge port*.

```
[admin@R7] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #     INTERFACE   BRIDGE          PRIORITY  PATH-COST    HORIZON
 0     eoip-R7-R1  bridgeHotspot   0x80         10        none
 1     ether2      bridgeHotspot   0x80         10        none
```

5.2.1.8 Verifikasi Konfigurasi Pada Router R8

Adapun langkah-langkah verifikasi konfigurasi yang dilakukan pada *router R8* adalah sebagai berikut:

1. Menampilkan informasi pengalamatan IP pada interface.

```
[admin@R8] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.26/30       10.0.0.24       ether1
```

2. Menampilkan informasi pengaturan *routing ospf network*.

```
[admin@R8] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   10.0.0.24/30       backbone
```

3. Menampilkan informasi *table routing*.

```
[admin@R8] > ip route print
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 ADo  0.0.0.0/0                          10.0.0.25               110
 1 ADo  10.0.0.0/30                        10.0.0.25               110
 2 ADo  10.0.0.4/30                        10.0.0.25               110
 3 ADo  10.0.0.8/30                        10.0.0.25               110
 4 ADo  10.0.0.12/30                       10.0.0.25               110
 5 ADo  10.0.0.16/30                       10.0.0.25               110
 6 ADo  10.0.0.20/30                       10.0.0.25               110
 7 ADC  10.0.0.24/30       10.0.0.26       ether1                    0
```

4. Menampilkan informasi pengaturan *DNS Client*.

```
[admin@R8] > ip dns print
                  servers: 10.0.0.1
        dynamic-servers:
  allow-remote-requests: no
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
                cache-size: 2048KiB
          cache-max-ttl: 1w
             cache-used: 9KiB
```

5. Menampilkan informasi pengaturan *NTP Client*.

```
[admin@R8] > system ntp client print
          enabled: yes
  server-dns-names: 0.id.ntp.pool.org,1.asia.ntp.pool.org
                mode: unicast
     poll-interval: 16s
     active-server: 64.99.80.121
```

6. Menampilkan informasi pengaturan *timezone*.

```
[admin@R8] > system clock print
                  time: 07:20:47
                  date: dec/27/2016
  time-zone-autodetect: yes
        time-zone-name: Asia/Makassar
            gmt-offset: +08:00
            dst-active: no
```

7. Menampilkan informasi *file CA* dan *Client Certificate*.

```
[admin@R8] > file print
 # NAME                                                                TYPE
 0 skins                                                               directory
 1 auto-before-reset.backup                                            backup
 2 cert_export_hotspotClient.key                                       .key file
 3 cert_export_hotspotCA.crt                                           .crt file
 4 cert_export_hotspotCA.key                                           .key file
 5 cert_export_hotspotClient.crt                                       .crt file
 6 R8.backup                                                           backup
 7 R8.rsc                                                              script
 8 pub                                                                 directory
 9 R8-compact.rsc                                                      script
```

8. Menampilkan informasi *Certificate* yang telah di *import*.

```
[admin@R8] > certificate print
Flags: K - private-key, D - dsa, L - crl, C - smart-card-key, A - authority, I - issued,
R - revoked, E - expired, T - trusted
 #          NAME          COMMON-NAME    SUBJECT-ALT-NAME FINGERPRINT
 0 K L A  T hotspotCA     hotspotCA                       ec90623df41f46f3778cc4a599f93...
 1 K   A  T hotspotClient hotspotClient                   083612a48252c6d5233298aadb7c7...
```

9. Menampilkan informasi *interface SSTP Client*.

```
[admin@R8] > interface sstp-client print
Flags: X - disabled, R - running
 0    name="sstp-out1" max-mtu=1500 max-mru=1500 mrru=disabled connect-to=10.0.0.1:443
      http-proxy=0.0.0.0:443 certificate=hotspotClient verify-server-certificate=yes
      verify-server-address-from-certificate=yes user="R8@stmikbumigora.local"
      password="12345678" profile=default keepalive-timeout=60 add-default-route=no
      dial-on-demand=no authentication=mschap2 pfs=no tls-version=any
```

10. Menampilkan informasi *monitoring* status *tunnel* antara *router R8* dengan *R1*.

```
[admin@R8] > interface sstp-client monitor sstp-out1
         status: connected
         uptime: 4s
       encoding: RC4
            mtu: 1500
  local-address: 10.0.1.8
 remote-address: 10.0.1.1
```

11. Memverifikasi koneksi dari *SSTP Client* ke *SSTP Server*.

```
[admin@R8] > ping 10.0.1.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.1                                   56  64 1ms
    1 10.0.1.1                                   56  64 1ms
    2 10.0.1.1                                   56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms
```

12. Menampilkan informasi *interface EoIP* untuk *tunneling* dari *router R8* ke *R1*.

```
[admin@R8] > interface eoip print
Flags: X - disabled, R - running
 0  R ;;; EoIP dari R8 ke R1
     name="eoip-R8-R1" mtu=auto actual-mtu=1458 l2mtu=65535 mac-address=FE:7E:73:0F:07:C0
     arp=enabled arp-timeout=auto loop-protect=default loop-protect-status=off
     loop-protect-send-interval=5s loop-protect-disable-time=5m local-address=10.0.1.8
     remote-address=10.0.1.1 tunnel-id=8 keepalive=10s,10 dscp=inherit
     clamp-tcp-mss=yes dont-fragment=no allow-fast-path=yes
```

13. Menampilkan informasi interface *bridge*.

```
[admin@R8] > interface bridge print
Flags: X - disabled, R - running
 0  R name="bridgeHotspot" mtu=auto actual-mtu=1458 l2mtu=65535 arp=enabled arp-timeout=auto
     mac-address=FE:7E:73:0F:07:C0 protocol-mode=rstp priority=0x8000 auto-mac=yes
     admin-mac=00:00:00:00:00:00 max-message-age=20s forward-delay=15s transmit-hold-count=6
     ageing-time=5m
```

14. Menampilkan informasi *interface bridge port*.

```
[admin@R8] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #     INTERFACE   BRIDGE          PRIORITY  PATH-COST    HORIZON
 0     eoip-R8-R1  bridgeHotspot   0x80         10        none
 1     ether2      bridgeHotspot   0x80         10        none
```

5.2.2 Skenario

Terdapat 7 skenario yang digunakan untuk mengujicoba konfigurasi meliputi manajemen *user hotspot* di *router R1*, koneksi *Internet* dari *router R1*, *Client1*, *Client2*, *Client3* dan *Client4* serta *monitoring user hotspot*.

5.2.2.1 Koneksi Internet dari Router R1

Adapun langkah-langkah yang dilakukan untuk mengujicoba skenario koneksi Internet dari *router R1* adalah sebagai berikut:

1. Memverifikasi koneksi ke alamat IP dari ISP yang merupakan alamat IP *default gateway* atau *default route* dari *router R1*.

```
[admin@R1] > ping 192.168.0.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.0.1                                56  64 0ms
    1 192.168.0.1                                56  64 0ms
    2 192.168.0.1                                56  64 0ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

2. Memverifikasi koneksi ke beberapa situs di Internet sebagai contoh *google.com* dan *stmikbumigora.ac.id*.

```
[admin@R1] > ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 118.98.30.167                              56 127 11ms
    1 118.98.30.167                              56 127 10ms
    2 118.98.30.167                              56 127 10ms
    sent=3 received=3 packet-loss=0% min-rtt=10ms avg-rtt=10ms max-rtt=11ms

[admin@R1] > ping stmikbumigora.ac.id
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 45.32.117.34                               56 127 38ms
    1 45.32.117.34                               56 127 35ms
    2 45.32.117.34                               56 127 35ms
    sent=3 received=3 packet-loss=0% min-rtt=35ms avg-rtt=36ms max-rtt=38ms
```

Hasil verifikasi menunjukkan koneksi ke situs tersebut berhasil dilakukan.

5.2.2.2 Manajemen User Hotspot di Router R1

Adapun langkah-langkah yang dilakukan untuk mengujicoba skenario manajemen *user hotspot* di *router R1* adalah sebagai berikut:

1. Membuat *user hotspot* dengan nama *"user1", "user2", "user3"* dan *"user4"* dan password *"12345678"* untuk keseluruhan *user*.

```
[admin@R1] > ip hotspot user add name=user1 password=12345678
[admin@R1] > ip hotspot user add name=user2 password=12345678
[admin@R1] > ip hotspot user add name=user3 password=12345678
[admin@R1] > ip hotspot user add name=user4 password=12345678
```

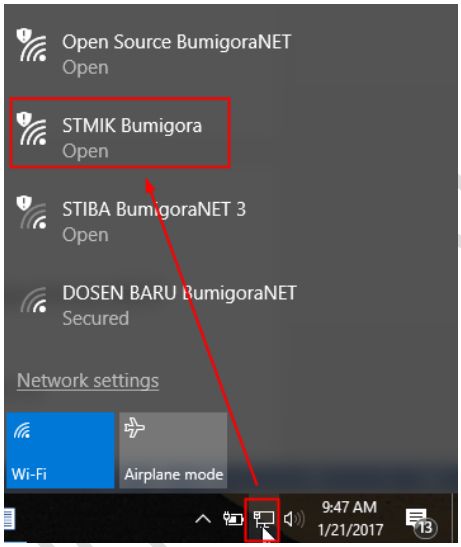
2. Menampilkan informasi *user hotspot* yang telah dibuat.

```
[admin@R1] > ip hotspot user print
Flags: * - default, X - disabled, D - dynamic
 #    SERVER     NAME                ADDRESS         PROFILE   UPTIME
 0 * ;;; counters and limits for trial users
                 default-trial                                  0s
 1               admin                               default    0s
 2               user1                               default    0s
 3               user2                               default    0s
 4               user3                               default    0s
 5               user4                               default    0s
```

5.2.2.3 Koneksi Internet Dari Client1

Adapun langkah-langkah yang dilakukan untuk scenario ujicoba koneksi Internet dari *Client1* adalah sebagai berikut:

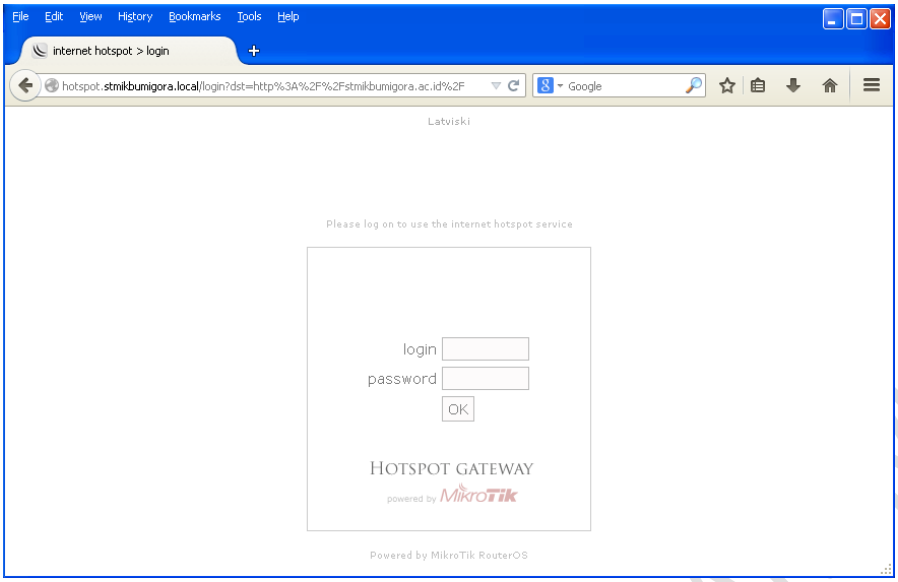
1. Menghubungkan *Client1* ke *hotspot* dengan cara memilih penanda *Network Connection* pada bagian pojok kanan dari *task bar* sistem operasi *Windows* dan memilih *SSID "STMIK Bumigora"*, seperti terlihat pada gambar 5.12.



Gambar 5.12 Network Connection Windows

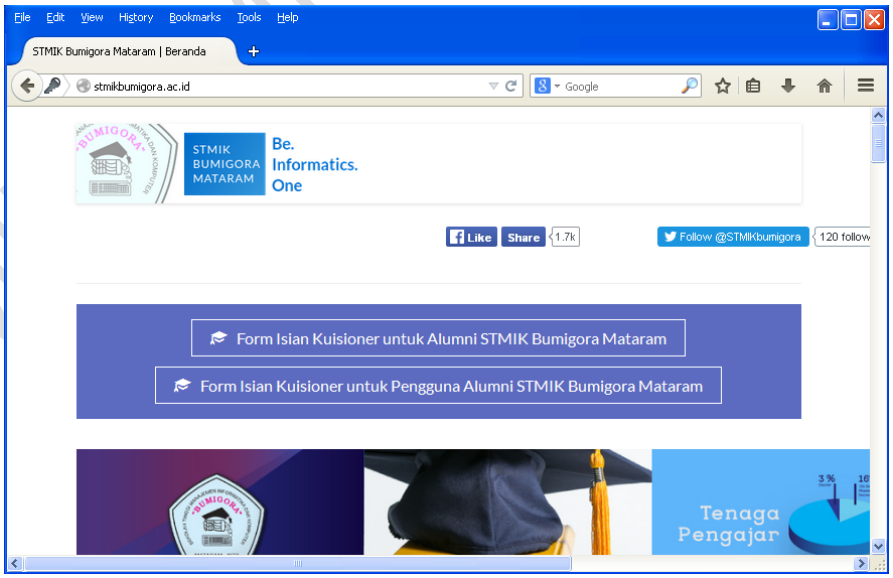
Pilih tombol *Connect* pada *SSID "STMIK Bumigora"* untuk menghubungkan ke *hotspot* tersebut.

2. Mengakses salah satu situs di Internet sebagai contoh situs STMIK Bumigora dengan alamat "*stmikbumigora.ac.id"* melalui browser, seperti terlihat pada gambar 5.13.



Gambar 5.13 Halaman Login Hotspot

Sebelum koneksi Internet dapat dilakukan maka pengguna akan diarahkan terlebih dahulu ke halaman otentikasi login hotspot. Login menggunakan *username* "*user1*" dengan *password* "*12345678*". Setelah otentikasi login hotspot berhasil dilakukan maka pengguna akan diarahkan kembali ke situs yang diakses, seperti terlihat pada gambar 5.14.

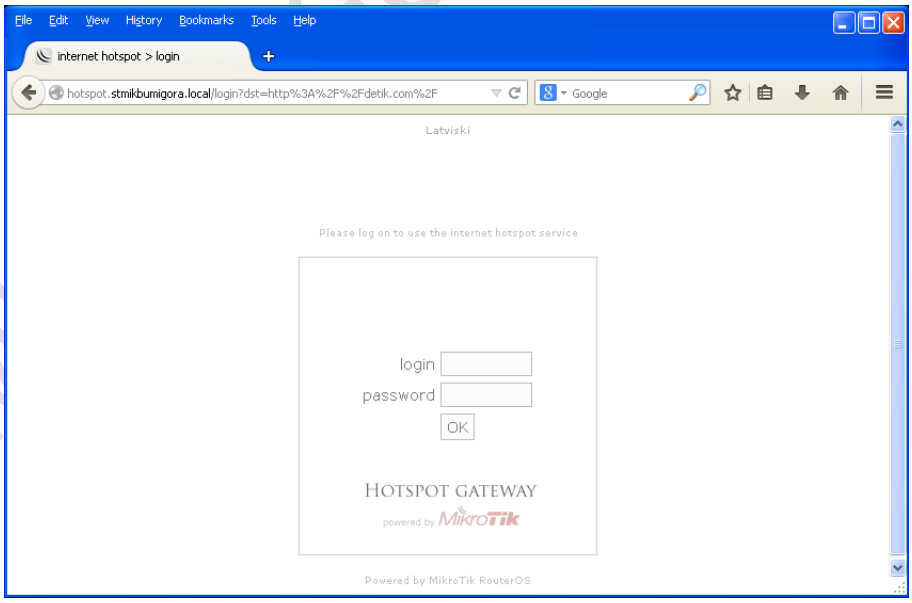


Gambar 5.14 Situs STMIK Bumigora

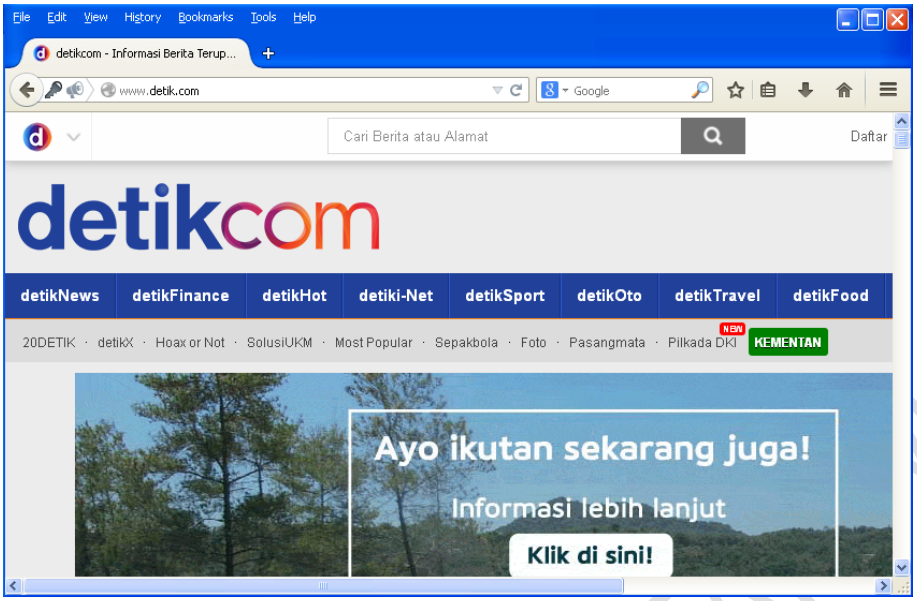
5.2.2.4 Koneksi Internet Dari Client2

Adapun langkah-langkah yang dilakukan untuk scenario ujicoba koneksi Internet dari *Client2* adalah sebagai berikut:

1. Menghubungkan *Client2* ke *hotspot* menggunakan cara yang sama dengan Client1 yaitu dengan cara memilih penanda *Network Connection* pada bagian pojok kanan dari *task bar* sistem operasi *Windows* dan memilih *SSID "STMIK Bumigora"*. Pilih tombol *Connect* pada *SSID "STMIK Bumigora"* untuk menghubungkan ke *hotspot* tersebut.
2. Mengakses salah satu situs di Internet sebagai contoh situs Detik dengan alamat "*detik.com"* melalui browser. Sebelum koneksi Internet dapat dilakukan maka pengguna akan diarahkan terlebih dahulu ke halaman otentikasi login hotspot, seperti terlihat pada gambar 5.15. Login menggunakan *username* "*user2*" dengan *password* "*12345678*". Setelah otentikasi berhasil dilakukan maka pengguna akan diarahkan kembali ke situs yang diakses, seperti terlihat pada gambar 5.16.



Gambar 5.15 Halaman Login Hotspot

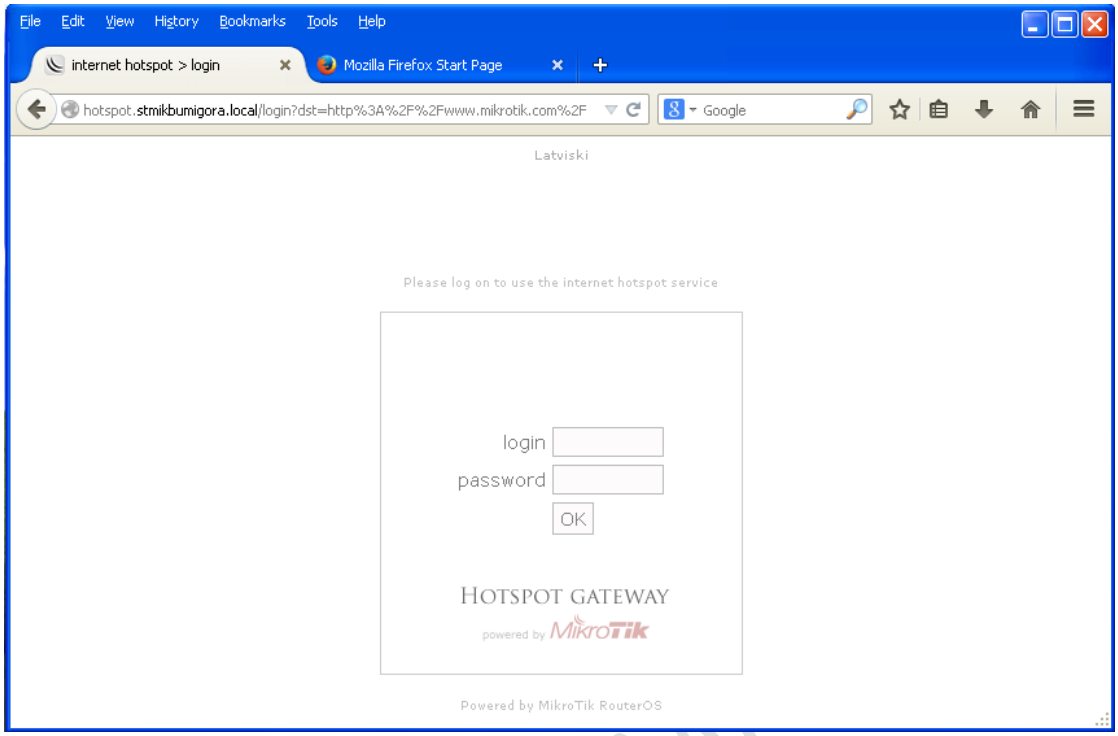


Gambar 5.16 Situs Detik

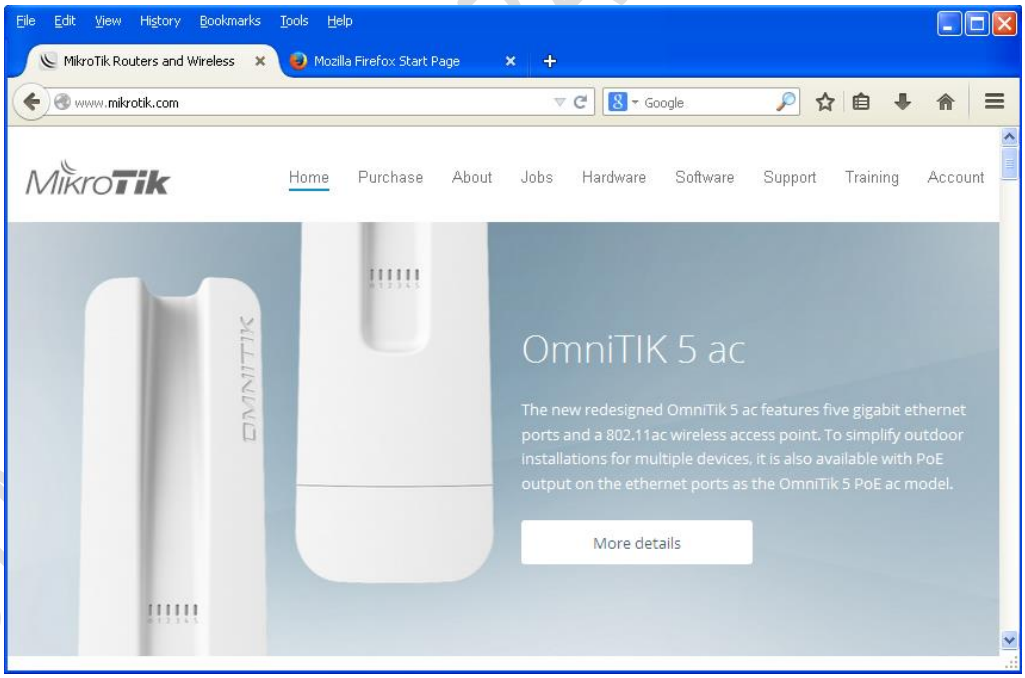
5.2.2.5 Koneksi Internet Dari Client3

Adapun langkah-langkah yang dilakukan untuk scenario ujicoba koneksi Internet dari *Client3* adalah sebagai berikut:

1. Menghubungkan *Client3* ke *hotspot* menggunakan cara yang sama dengan Client1 yaitu dengan cara memilih penanda *Network Connection* pada bagian pojok kanan dari *task bar* sistem operasi *Windows* dan memilih *SSID "STMIK Bumigora"*. Pilih tombol *Connect* pada *SSID "STMIK Bumigora"* untuk menghubungkan ke *hotspot* tersebut.
2. Mengakses salah satu situs di Internet sebagai contoh situs Mikrotik dengan alamat "*mikrotik.com"* melalui browser. Sebelum koneksi Internet dapat dilakukan maka pengguna akan diarahkan terlebih dahulu ke halaman otentikasi login hotspot, seperti terlihat pada gambar 5.17. Login menggunakan *username* "*user3*" dengan *password* "*12345678*". Setelah otentikasi berhasil dilakukan maka pengguna akan diarahkan kembali ke situs yang diakses, seperti terlihat pada gambar 5.18.



Gambar 5.17 Halaman Login Hotspot

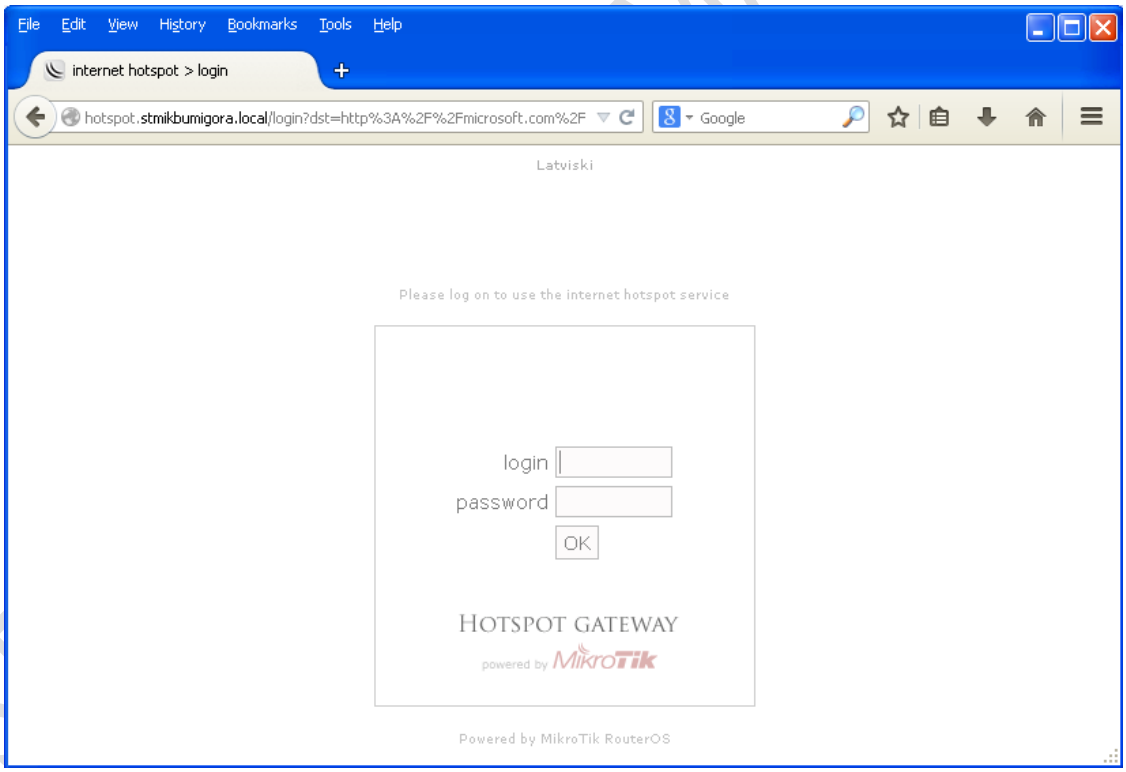


Gambar 5.18 Situs Mikrotik

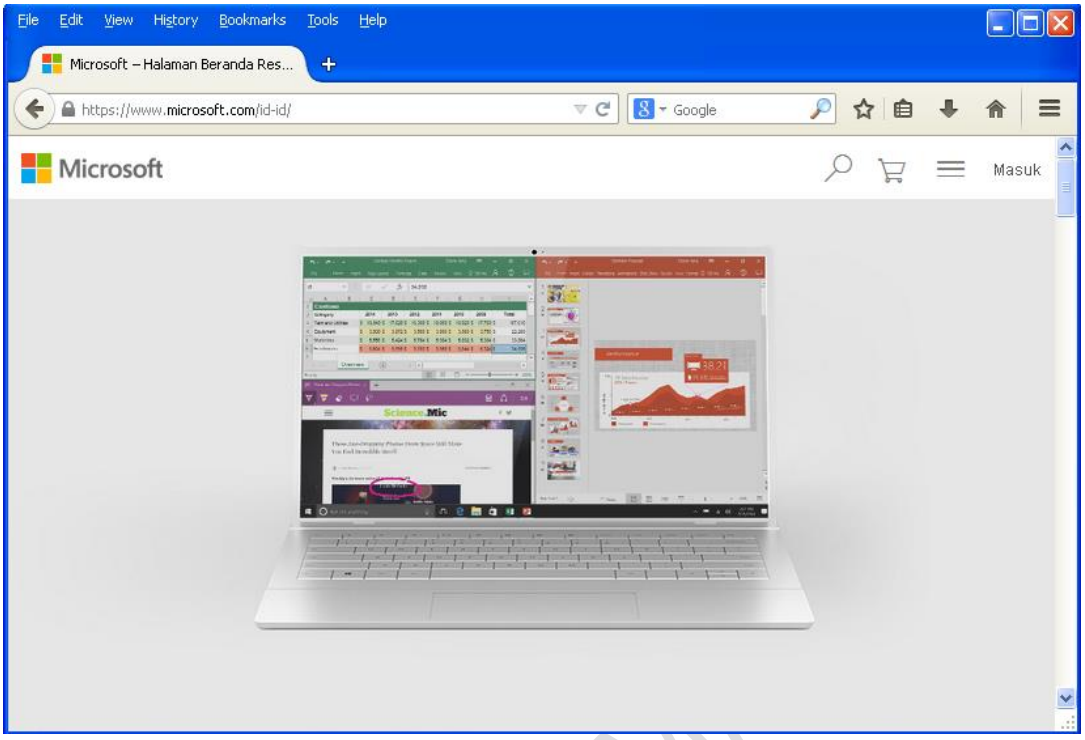
5.2.2.6 Koneksi Internet Dari Client4

Adapun langkah-langkah yang dilakukan untuk scenario ujicoba koneksi Internet dari *Client4* adalah sebagai berikut:

1. Menghubungkan *Client4* ke *hotspot* menggunakan cara yang sama dengan Client1 yaitu dengan cara memilih penanda *Network Connection* pada bagian pojok kanan dari *task bar* sistem operasi *Windows* dan memilih *SSID "STMIK Bumigora"*. Pilih tombol *Connect* pada *SSID "STMIK Bumigora"* untuk menghubungkan ke *hotspot* tersebut.
2. Mengakses salah satu situs di Internet sebagai contoh situs Mikrotik dengan alamat "*mikrotik.com"* melalui browser. Sebelum koneksi Internet dapat dilakukan maka pengguna akan diarahkan terlebih dahulu ke halaman otentikasi login hotspot, seperti terlihat pada gambar 5.19. Login menggunakan *username* "*user4*" dengan *password* "*12345678*". Setelah otentikasi berhasil dilakukan maka pengguna akan diarahkan kembali ke situs yang diakses, seperti terlihat pada gambar 5.20.



Gambar 5.19 Halaman Login Hotspot



Gambar 5.20 Situs Microsoft

5.2.2.7 Monitoring User Hotspot

Untuk menampilkan informasi *user hotspot* yang sedang aktif (*monitoring*) dapat dilakukan dengan mengeksekusi perintah berikut:

```
[admin@R1] > ip hotspot active print
Flags: R - radius, B - blocked
 #    USER    ADDRESS         UPTIME  SESSION-TIME-LEFT IDLE-TIMEOUT
 0    user4   10.0.2.243      7m21s
 1    user3   10.0.2.244      29m23s
 2    user2   10.0.2.245      1m49s
 3    user1   10.0.2.254      1m47s
```

Terlihat terdapat 4 user yang sedang aktif menggunakan layanan hotspot.

5.3 Analisa Hasil Ujicoba

Berdasarkan ujicoba yang telah dilakukan maka dapat diperoleh hasil analisa sebagai berikut:

1. *Internet connection sharing* dikonfigurasi pada *router R1* dengan memanfaatkan fitur *IP Firewall NAT* pada *Mikrotik RouterOS* dengan *chain* "*srcnat*" yang diterapkan pada

out interface PPPoE Client yang mengkoneksikan ke ISP sehingga seluruh host di jaringan lokal dapat terhubung ke Internet.

2. *Router R1* difungsikan sebagai *DNS server* sehingga dapat melayani permintaan resolusi pemetaan nama domain bagi *client hotspot*.
3. *Route redistribution default route* diterapkan pada *routing protocol OSPF router R1* agar router lainnya di jaringan local memiliki informasi *default route* pada routing tabelnya sehingga dapat merutekan paket data keluar dari alamat network jaringan local yaitu Internet.
4. Pengaturan *NTP Client* dapat mensinkronisasi waktu sistem pada keseluruhan router dengan *NTP Server* di *Internet*.
5. *Mikrotik RouterOS* dapat digunakan untuk membuat sertifikat SSL, dimana sertifikat ini diperlukan ketika penerapan SSTP di *router R1, R5, R6, R7* dan *R8*.
6. *Router R1* berfungsi sebagai *SSTP Server*, sedangkan *router R5, R6, R7* dan *R8* difungsikan sebagai *SSTP Client* karena hanya 4 (empat) *router* ini yang terhubung secara langsung ke perangkat *Access Point*.
7. *EoIP tunnel* dibangun diatas *SSTP tunnel* dengan referensi alamat IP yang digunakan oleh *interface SSTP Server* dan *Client*, dimana alamat IP ini diterapkan pada *properties local-address* dan *remote-address* dari *interface EoIP*.
8. Nilai *tunnel-id* pada *EoIP* harus unik untuk setiap *tunnel* karena digunakan sebagai metode untuk mengidentifikasi *tunnel*.
9. *Interface bridge* dibuat pada router R1, R5, R6, R7 dan R8 dengan *bridge port* berupa *interface EoIP* dan *ether2* yang terhubung ke perangkat *Access Point* sehingga layanan hotspot membentuk sebuah LAN.

10. Layanan *hotspot* diterapkan pada *interface bridge* "*bridgeHotspot*" pada *router R1* sehingga setiap client harus melakukan proses otentikasi login hotspot terlebih dahulu sebelum dapat mengakses Internet.
11. Koneksi Internet dapat dilakukan oleh setiap *client* yang terhubung ke setiap perangkat *Access Point* dengan *SSID* yang sama yaitu "STMIK Bumigora".
12. Keseluruhan client hotspot berada dalam satu alamat jaringan yaitu 10.0.2.0/24 meskipun terkoneksi melalui perangkat *Access Point* yang berbeda.

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil konfigurasi dan ujicoba serta analisa terhadap hasil ujicoba yang telah dilakukan maka dapat diambil kesimpulan sebagai berikut:

1. Sentralisasi manajemen dan *monitoring hotspot* dapat dibangun menggunakan teknik *transparent bridge tunnel EoIP over SSTP*.
2. Alamat IP pada *interface SSTP* digunakan sebagai referensi *local* dan *remote address* pembentukan *tunnel EoIP over SSTP*.
3. Penerapan *bridging* pada *interface EoIP* dan *interface* yang terhubung ke perangkat *Access Point* membentuk satu jaringan secara logical sehingga konfigurasi layanan hotspot dapat dilakukan secara terpusat pada satu router.

6.2 Saran

Adapun saran-saran untuk pengembangan penelitian ini lebih lanjut adalah sebagai berikut:

1. Menganalisa unjuk kerja jaringan atau *Quality of Service (QoS)* terkait penggunaan *transparent bridge tunnel EoIP over SSTP* pada *hotspot*.
2. Menganalisa fitur keamanan terkait penerapan *transparent bridge tunnel EoIP over SSTP* pada *hotspot*.
3. Membandingkan *QoS* dan fitur keamanan terkait penerapan sentralisasi *hotspot* berbasis *transparent bridge tunnel EoIP over SSTP* dengan teknik lainnya seperti *transparent bridge tunnel EoIP over PPTP* dan *Multiprotocol Label Switching (MPLS) Virtual Private LAN Service (VPLS).*

4. Mengembangkan aplikasi manajemen dan *monitoring* sentralisasi *hotspot* berbasis *transparent bridge tunnel EoIP over SSTP* sehingga proses manajemen dan pengawasan lebih efektif dan efisien.

DAFTAR REFERENSI

[1] Microsoft. 2007. *SSTP Remote Access Step-by-Step Guide: Deployment*. *https://technet.microsoft.com/en-us/library/cc731352(v=ws.10).aspx*. Diakses tanggal 30 Nopember 2016

[2] Mikrotik. 2016. *Manual:Interface/SSTP*. *http://wiki.mikrotik.com/wiki/Manual:Interface/SSTP*. Diakses tanggal 1 Desember 2016

[3] Tom Shinder. 2008. *Configuring Windows Server 2008 as a Remote Access SSL VPN Server (Part 1)*. *http://techgenix.com/Configuring-Windows-Server-2008-Remote-Access-SSL-VPN-Server-Part1*. Diakses tanggal 2 Desember 2016

[4] Mikrotik. 2016. *About*. *http://www.mikrotik.com/aboutus*. Diakses tanggal 2 Desember 2016

[5] Mikrotik Indonesia. 2016. *Homepage*. *http://mikrotik.co.id*. Diakses tanggal 3 Desember 2016

[6] WikiBooks. 2016. *Switches, Routers, Bridges and LANs/Bridges*. *https://en.wikibooks.org/wiki/Switches,_Routers,_Bridges_and_LANs/Bridges*. Diakses tanggal 15 Desember 2016

[7] Cisco. 2005. *Configuring Transparent Bridging*. *http://www.cisco.com/c/en/us/support/docs/ibm-technologies/source-route-transparent-srt-bridging/10676-37.html*. Diakses tanggal 20 Desember 2016

[8] Mikrotik. 2015. *Manual:Interface/EoIP*. *http://wiki.mikrotik.com/wiki/Manual:Interface/EoIP*. Diakses tanggal 4 Desember 2016

[9] Mikrotik. 2015. *Manual:Hotspot Introduction*. *http://wiki.mikrotik.com/wiki/Manual: Hotspot_Introduction*. Diakses tanggal 5 Desember 2016

[10] Mikrotik. 2016. *Manual:IP/Hotspot*. *http://wiki.mikrotik.com/wiki/Manual:IP/Hotspot*. Diakses tanggal 5 Desember 2016

[11] James E.Goldman dan Phillip T. Rawles. 2004. *The Network Development Life Cycle*. *http://higheredbcs.wiley.com/legacy/college/goldman/0471346403/lecture_slides/ch10.ppt ?newwindow=true*. Diakses tanggal 6 Desember 2016

[12] Deris Stiawan. 2009. *Fundamental Internetworking Development & Life Cycle*. *http://unsri.ac.id/upload/arsip/network_development_cycles.pdf*, Diakses tanggal 7 Desember 2016