

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

STMIK Bumigora; Jalan Ismail Marzuki Mataram, (0370) 634498

Jurusan Teknik Informatika, Nusa Tenggara Barat

e-mail: putu.hariyadi@stmikbumigora.ac.id

Abstract

STMIK Bumigora is the first computer college in the province of West Nusa Tenggara (NTB). There are 11 hotspots spread across the campus to provide Internet services through a wireless connection for the academic community. The increasing number of hotspots that must be managed with locations scattered in various Mikrotik routers hence make the process of management and monitoring hotspots become complex, ineffective and inefficient. Centralized campus hotspot management using a transparent bridge EoIP over SSTP can help solve the problems at hand. Ethernet over IP (EoIP) Tunneling is a Mikrotik RouterOS protocol that creates an Ethernet tunnel between routers over IP connections. EoIP tunnel built on SSTP tunnel (EoIP over SSTP) with Site-to-Site type. SSTP is a new form of Virtual Private Network (VPN) tunnel that provides a mechanism for encapsulating Point-to-Point Protocol (PPP) traffic through the SSL path of the HTTPS protocol. The IP address of the SSTP interface is used as the local reference and remote address of the EoIP over SSTP tunnel. The application of bridging on EoIP interfaces and interfaces connected to Access Point devices forms a logical network so that the management and monitoring of hotspot services can be performed centrally on one router.

Keywords— Mikrotik, OSPF, Hotspot, SSTP, EoIP, Bridge

I. PENDAHULUAN

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* 100 Mbps dan *dedicated connection Astinet* dengan *bandwidth* 2 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

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

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*.

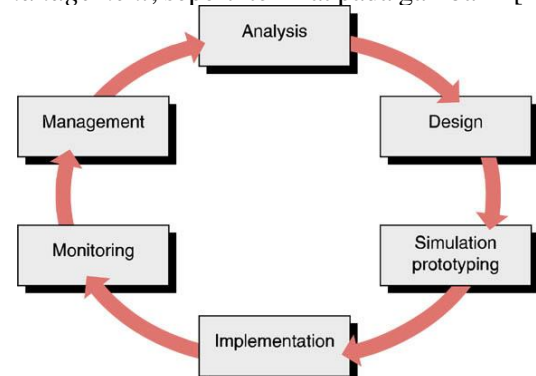
PusTIK memiliki harapan terdapat satu sistem yang dapat memusatkan manajemen *hotspot* kampus sehingga dapat dikelola menggunakan satu antarmuka *winbox* meskipun *hotspot* tersebar di banyak *router Mikrotik* yang tersebar di berbagai lokasi. Selain itu proses manajemen *user hotspot* dan pengawasan *user hotspot* yang aktif dapat di-*monitoring* 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 [1]. 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)* [2]. 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 logikal. *Bridge* merupakan perangkat yang digunakan untuk menghubungkan dua jaringan *Ethernet* terpisah menjadi satu *Ethernet* yang diperluas [3]. 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.

II. 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 1 [4].



Gambar 1 Network Development Life Cycle [4]

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

A. 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 [5]. Sebelum dapat melakukan proses analisis maka terlebih dahulu dilakukan pengumpulan data menggunakan berbagai teknik meliputi observasi, wawancara dan dokumentasi.



Pada tahap ini dilakukan pembuatan rancangan jaringan ujicoba dan rancangan pengalamatan IP serta rancangan *tunnel-id* dari *EoIP* untuk sistem sentralisasi manajemen hotspot kampus. Rancangan jaringan ujicoba untuk sistem sentralisasi manajemen *hotspot* kampus berbasis *transparent bridge EoIP over SSTP*, seperti terlihat pada gambar 2.

routing protocol OSPF dengan area backbone. 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-

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

R8, diperlihatkan menggunakan garis putus-putus berwarna kuning pada gambar 2.

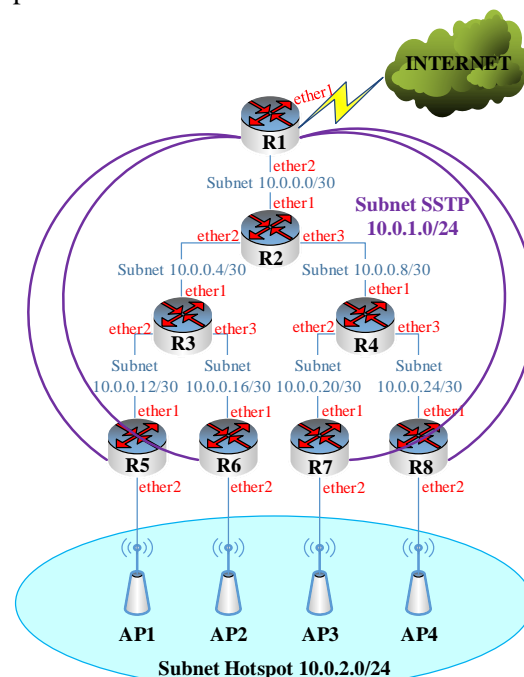
Pada *router R1* dilakukan pembuatan *interface bridge* dengan port anggota keseluruhan *interface EoIP*, sedangkan pada *router R5-R8* dilakukan pula pembuatan *interface bridge* dengan port anggota *interface EoIP* dan *interface ether2* yang terhubung secara langsung ke perangkat AP. *Interface bridge*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

Rancangan 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 1.

Tabel 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
8.	10.0.1.0/24	Dialokasikan untuk <i>SSTP tunnel</i>
9.	10.0.2.0/24	Dialokasikan untuk subnet <i>hotspot</i>

Alokasi alamat subnet pada rancangan jaringan ujicoba, seperti terlihat pada gambar 3. Secara detail pengalamatan IP yang dialokasikan pada setiap *interface* dari *router* dan *Access Point*, seperti terlihat pada tabel 2.



Gambar 3 Alokasi Pengalamatan IP Per Subnet

Tabel 2 Pengalamatan IP Router dan Access Point

N o.	Per angkat	Inter face	Alamat IP	Gate way
1.	Router R1	Ether 2	10.0.0.1/30	
2.	Router R2	Ether 1	10.0.0.2/30	
3.		Ether 2	10.0.0.5/30	
4.		Ether 3	10.0.0.9/30	
5.	Router R3	Ether 1	10.0.0.6/30	
6.		Ether 2	10.0.0.13/30	
7.		Ether 3	10.0.0.17/30	
8.	Router R4	Ether 1	10.0.0.10/30	

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

9.		Ether 2	10.0.0.2 1/30	
10.		Ether 3	10.0.0.2 5/30	
11.	Router R5	Ether 1	10.0.1.1 4/30	
12.	Router R6	Ether 1	10.0.1.1 8/30	
13.	Router R7	Ether 1	10.0.1.2 2/30	
14.	Router R8	Ether 1	10.0.1.2 6/30	
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 3. Router yang bertindak sebagai *SSTP Server* adalah router *R1*, sedangkan router yang bertindak sebagai *SSTP Client* adalah *R5*, *R6*, *R7* dan *R8*.

Tabel 3 SSTP User

No.	Username	Local - address	Remote- address	Deskripsi
1.	R5@stmik bumigora. local	10.0.1 .1	10.0. 1.5	R1- R5
2.	R6@stmik bumigora. local		10.0. 1.6	R1- R6
3.	R7@stmik bumigora. local		10.0. 1.7	R1- R7
4.	R8@stmik bumigora. 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. Sedangkan 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 5.

Tabel 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

Tabel 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

C. Tahap Simulation Prototyping

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

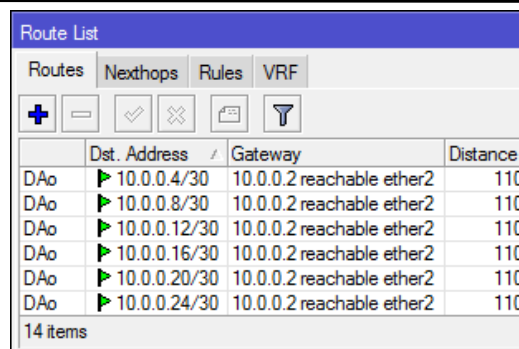
I Putu Hariyadi

Tahap *simulation prototyping* dibagi menjadi dua bagian yaitu konfigurasi dan ujicoba baik verifikasi konfigurasi maupun skenario. Konfigurasi dilakukan di keseluruhan router yang terlibat meliputi konfigurasi dasar pengalamatan IP, *routing protocol OSPF*, *DNS*, *NTP Client*, *Time Zone*, *SSTP tunnel*, *EoIP tunnel* dan *interface bridge* serta *hotspot*. Sedangkan ujicoba dibagi menjadi 2 (dua) jenis yaitu verifikasi konfigurasi dan ujicoba berbasis skenario. Verifikasi konfigurasi 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*. Sedangkan ujicoba berbasis skenario terdiri dari 7 (tujuh) 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*.

III. HASIL DAN PEMBAHASAN

A. Hasil Konfigurasi

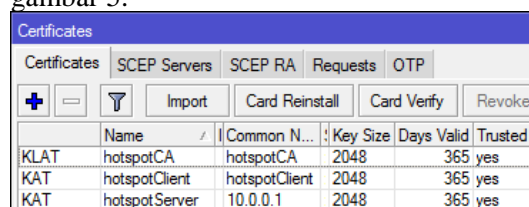
Konfigurasi terdiri dari 5 (lima) bagian yaitu konfigurasi dasar, konfigurasi *routing protocol OSPF*, konfigurasi *NTP Client*, konfigurasi *SSTP*, konfigurasi *EoIP* dan *Bridge* serta konfigurasi *hotspot*. Konfigurasi dasar dan *routing protocol OSPF* serta *NTP Client* dilakukan pada 8 (delapan) *router Mikrotik*. Hasil dari konfigurasi dasar dan *OSPF* dapat dilihat dengan menampilkan informasi routing tabel dari router. Sebagai contoh pada *router R1*, seperti terlihat pada gambar 4.



	Dst. Address	Gateway	Distance
DAo	10.0.0.4/30	10.0.0.2 reachable ether2	110
DAo	10.0.0.8/30	10.0.0.2 reachable ether2	110
DAo	10.0.0.12/30	10.0.0.2 reachable ether2	110
DAo	10.0.0.16/30	10.0.0.2 reachable ether2	110
DAo	10.0.0.20/30	10.0.0.2 reachable ether2	110
DAo	10.0.0.24/30	10.0.0.2 reachable ether2	110

Gambar 4 Routing Table Router R1

Konfigurasi *SSTP* terdiri dari 2 bagian yaitu *SSTP Server* yang dilakukan pada *router R1* dan *SSTP Client* yang dilakukan pada *router R5*, *R6*, *R7* dan *R8*. Konfigurasi *SSTP Server* yang dilakukan pada *router R1* adalah membuat *template* untuk *Certificate Authority (CA)*, *Server Certificate* dan *Client Certificate*, melakukan *Sign Certificate (CA, Server, Client)* dan mengatur *Certificate Revocation Lists (CRL)* *Uniform Resource Locator (URL)* menggunakan alamat IP 10.0.0.1 yang merupakan alamat IP internal dari *Server* serta mengatur *trusted* pada *CA*, *Server* dan *Client Certificate*. Hasil pembuatan *template* dan pengaturan *CRL* serta *trusted certificate*, seperti terlihat pada gambar 5.



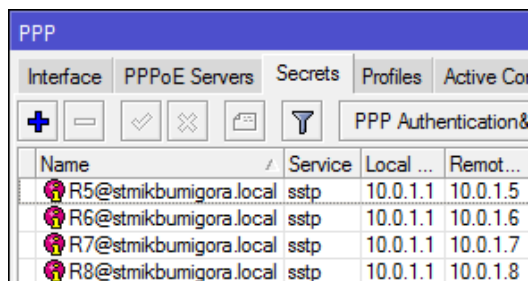
Name	Common Name	Key Size	Days Valid	Trusted
KLAT hotspotCA	hotspotCA	2048	365	yes
KAT hotspotClient	hotspotClient	2048	365	yes
KAT hotspotServer	10.0.0.1	2048	365	yes

Gambar 5 Template CA, Server dan Client Certificate

Client Certificate dan *CA Certificate* yang telah berhasil dibuat, selanjutnya di *export* untuk digunakan pada *router* yang bertindak sebagai *SSTP Client* yaitu *R5*, *R6*, *R7* dan *R8*. Selain itu pada *router R1* juga dilakukan pembuatan akun pengguna untuk koneksi dari *router R5*, *R6*, *R7* dan *R8* yang bertindak sebagai *SSTP Client* ke *router R1* yang bertindak sebagai *SSTP Server* dan dan mengaktifkan *SSTP Server*. Hasil pembuatan akun, seperti terlihat pada gambar 6.

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

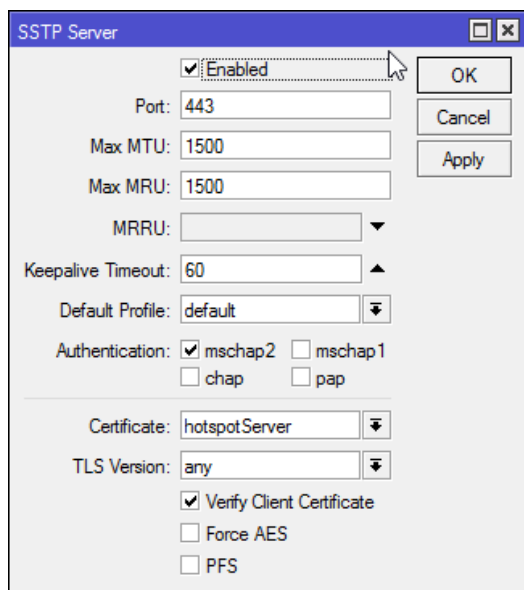


Name	Service	Local ...	Remot...
R5@stmikbumigora.local	sstp	10.0.1.1	10.0.1.5
R6@stmikbumigora.local	sstp	10.0.1.1	10.0.1.6
R7@stmikbumigora.local	sstp	10.0.1.1	10.0.1.7
R8@stmikbumigora.local	sstp	10.0.1.1	10.0.1.8

Gambar 6 Akun SSTP Client

Terdapat beberapa parameter yang harus dikonfigurasi ketika mengaktifkan *SSTP Server*, seperti terlihat pada gambar 7 yaitu antara lain:

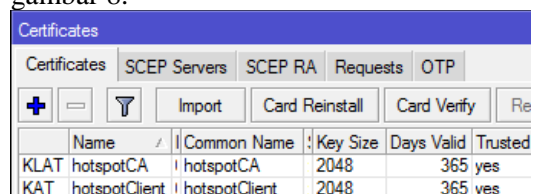
- Menandai parameter *Enabled*.
- Memilih *Certificate* yang digunakan untuk menentukan nama *Server Certificate* yang digunakan yaitu "*hotspotServer*".
- Menandai *Verify Client Certificate* yang digunakan agar server melakukan pengecekan *Client Certificate* termasuk dalam *certificate chain* yang sama.
- Memilih *Authentication* yang digunakan untuk menentukan metode otentikasi yang diterima oleh *SSTP Server* yaitu *mschap2*.



Gambar 7 Pengaktifan SSTP Server

Konfigurasi *SSTP Client* dilakukan pada 4 (empat) *router* yaitu *router R5, R6, R7* dan *R8*. Konfigurasi yang dilakukan pada *SSTP Client* adalah menyalin file *CA* dan *Client Certificate* dari *router R1* ke *router R5, R6, R7* dan *R8*.

File CA dan *Client Certificate* yang telah disalin kemudian di *import* serta disesuaikan penamaan filenya, seperti terlihat pada gambar 8.



Name	Common Name	Key Size	Days Valid	Trusted
KLAT hotspotCA	hotspotCA	2048	365	yes
KAT hotspotClient	hotspotClient	2048	365	yes

Gambar 8 Import File CA dan Client Certificate

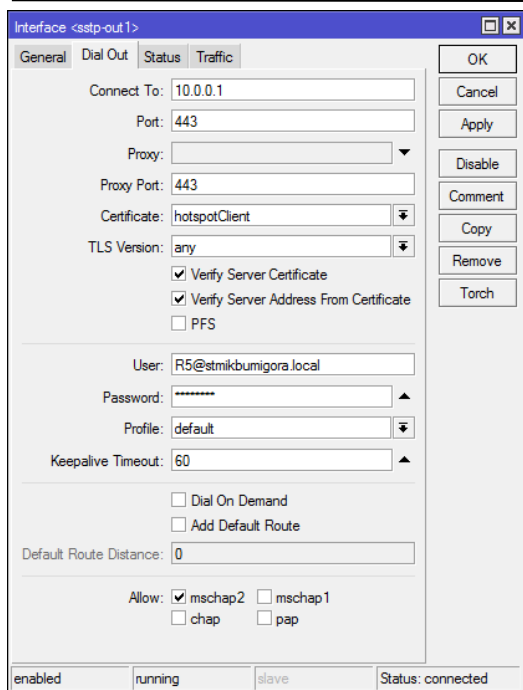
Selanjutnya dilakukan pembuatan *interface SSTP Client* yang digunakan untuk koneksi dari setiap *router* ke *R1*. Hasil pembuatan *interface SSTP Client* pada *router R5*, seperti terlihat pada gambar 9.

Terdapat beberapa parameter yang harus dikonfigurasi antara lain:

- Connect To*: digunakan untuk menentukan alamat IP dari *SSTP Server* yaitu 10.0.0.1.
- Certificate*: digunakan untuk menentukan nama *Client Certificate* yang digunakan yaitu *hotspotClient*.
- Verify Server Certificate* yang digunakan agar client melakukan pengecekan *certificate* termasuk dalam *certificate chain* yang sama dengan *Server Certificate*.
- User*: digunakan untuk menentukan nama pengguna yang akan digunakan untuk otentikasi yaitu *R5@stmikbumigora.local*.
- Password*: digunakan untuk menentukan sandi yang akan digunakan untuk otentikasi.
- Authentication* yang digunakan untuk menentukan metode otentikasi yang diterima yaitu *mschap2*.

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi



Gambar 9 Interface SSTP Client di Router R5

Konfigurasi *EoIP* dan *Bridge* dilakukan pada 4 (empat) router yaitu router *R1*, *R5*, *R6*, *R7* dan *R8*. Hasil dari pembuatan interface *Bridge* dan pengaturan *bridge port* untuk interface *EoIP* tunnel dari router *R1* ke *R5*, *R6*, *R7* dan *R8*, seperti terlihat pada gambar 10.

Interface	Bridge	P...	P...	Role
teoip-R1-R5	bridgeHotspot	80	10	designated port
teoip-R1-R6	bridgeHotspot	80	10	designated port
teoip-R1-R7	bridgeHotspot	80	10	designated port
teoip-R1-R8	bridgeHotspot	80	10	designated port

Gambar 10 Interface Bridge Port di Router R1

Terdapat beberapa parameter yang harus dikonfigurasi ketika pembuatan interface *EoIP* tunnel, sebagai contoh dari router *R1* ke *R5* antara lain Name: nama pengenalan interface *EoIP* yang dibuat yaitu "eoip-R1-R5", Tunnel-id: metode untuk mengidentifikasi tunnel yang harus unik untuk masing-masing tunnel *EoIP* dan harus sesuai dengan sisi tunnel lainnya dimana nilainya dapat berupa integer antara

0-65536 dan untuk tunnel dari *R1* ke *R5* diatur dengan nilai "5", Local-address: alamat IP sumber dari tunnel lokal yaitu 10.0.1.1, Remote-address: alamat IP dari tunnel *EoIP* lawan atau sisi remote yaitu 10.0.1.5. Sedangkan konfigurasi *EoIP* dan *Bridge* yang dilakukan pada router *R5*, *R6*, *R7* dan *R8* adalah membuat interface *EoIP* tunnel dari setiap router hanya ke *R1*, membuat interface *bridge* dan menambahkan interface *EoIP* sebagai port anggota dari interface *bridge* serta menambahkan interface *ether2* sebagai port anggota dari interface *bridge*. Sebagai contoh pada router *R5*, hasil konfigurasinya terlihat seperti pada gambar 11.

Interface	Bridge	P...	P...	Role
teoip-R5-R1	bridgeHotspot	80	10	root port
ether2	bridgeHotspot	80	10	designated port

Gambar 11 Interface Bridge Port di Router R5

Konfigurasi *DHCP* Server dan *Hotspot* dilakukan pada interface *Bridge* "bridgeHotspot" pada router *R1* sehingga setiap client memperoleh pengalamatan IP secara dinamis dan harus melakukan proses otentikasi login hotspot terlebih dahulu sebelum dapat mengakses Internet. Koneksi Internet dapat dilakukan oleh client melalui 4 (empat) perangkat AP yang dikonfigurasi menggunakan SSID yang sama yaitu "STMIK Bumigora".

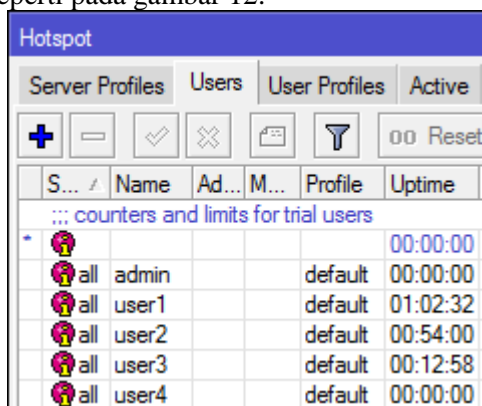
B. Hasil Ujicoba

Terdapat 7 (tujuh) 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. Skenario ujicoba manajemen user hotspot di router *R1* dapat dilakukan dengan mengakses fitur IP Hotspot melalui winbox. Hasil manajemen user hotspot berupa penambahan 4 (empat) akun hotspot masing-masing dengan nama

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

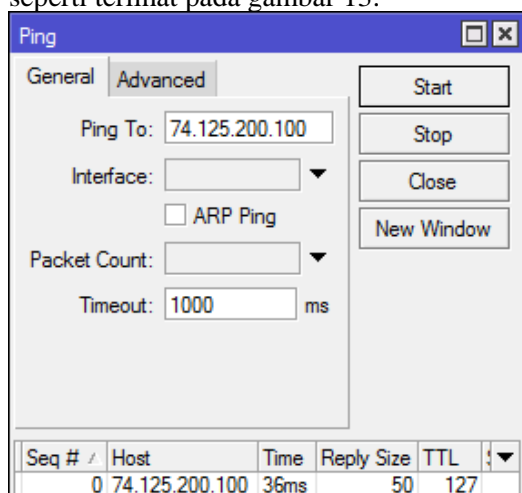
user1, *user2*, *user3* dan *user4*, terlihat seperti pada gambar 12.



S...	Name	Ad...	M...	Profile	Uptime
... counters and limits for trial users					
*					00:00:00
all	admin			default	00:00:00
all	user1			default	01:02:32
all	user2			default	00:54:00
all	user3			default	00:12:58
all	user4			default	00:00:00

Gambar 12 Manajemen User Hotspot

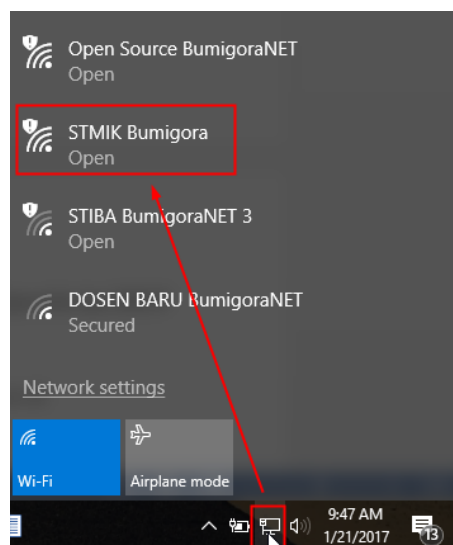
Hasil dari skenario ujicoba koneksi *Internet* di *router R1* menggunakan tool *ping* ke “*google.com*” dengan IP 74.125.200.100, seperti terlihat pada gambar 13.



Seq #	Host	Time	Reply Size	TTL
0	74.125.200.100	36ms	50	127

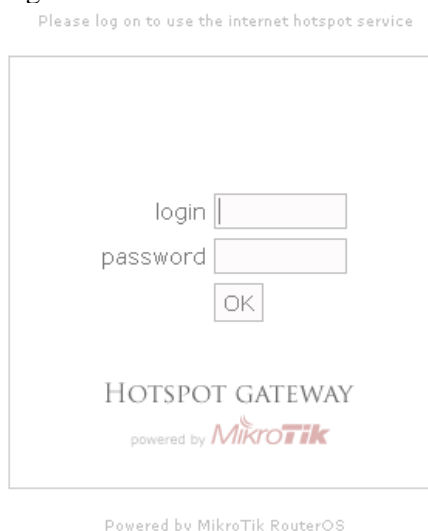
Gambar 13 Verifikasi Koneksi Internet dari router R1

Skenario ujicoba koneksi *Internet* dari *Client1*, *Client2*, *Client3* dan *Client4*, diawali dengan menghubungkan masing-masing *Client* ke *hotspot* melalui setiap perangkat AP dengan *SSID* yang sama yaitu “*STMIK Bumigora*”, seperti terlihat pada gambar 14.



Gambar 14 Network Connection Windows

Setelah koneksi ke *hotspot* berhasil dilakukan maka pengguna dapat menggunakan *browser* untuk mengakses salah satu situs di *Internet* sebagai contoh koneksi dari *Client1* ke situs *STMIK Bumigora* dengan alamat “*stmikbumigora.ac.id*”. Pengguna akan diarahkan ke halaman *login hotspot* untuk melakukan otentikasi menggunakan *akun hotspot* yang telah dibuat, seperti terlihat pada gambar 15.



Gambar 15 Hotspot Login

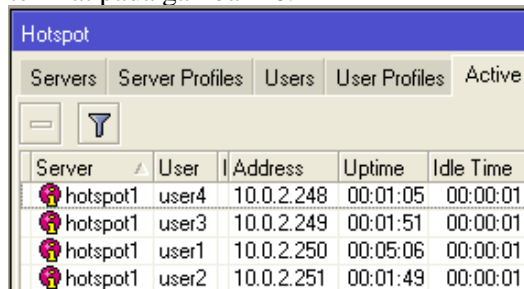
Apabila proses otentikasi berhasil maka pengguna akan diarahkan ke situs *STMIK Bumigora*.

Ketika keseluruhan *client* telah terkoneksi ke *Internet* melalui proses

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

otentikasi *login hotspot*, maka proses *monitoring user hotspot* dapat dilakukan melalui satu antarmuka *winbox* secara terpusat meskipun setiap client terhubung melalui perangkat *AP* berbeda, seperti terlihat pada gambar 16.



Server	User	Address	Uptime	Idle Time
hotspot1	user4	10.0.2.248	00:01:05	00:00:01
hotspot1	user3	10.0.2.249	00:01:51	00:00:01
hotspot1	user1	10.0.2.250	00:05:06	00:00:01
hotspot1	user2	10.0.2.251	00:01:49	00:00:01

Gambar 16 Monitoring User Hotspot

Terlihat terdapat 4 (empat) *user* yang sedang aktif menggunakan layanan *hotspot* dan keseluruhan *client hotspot* berada dalam satu alamat jaringan yaitu 10.0.2.0/24.

C. Analisa Hasil Ujicoba

Berdasarkan ujicoba yang telah dilakukan maka dapat diperoleh hasil analisa antara lain (a) *EoIP tunnel* dibangun diatas *SSTP tunnel* dengan referensi alamat IP yang digunakan oleh *interface SSTP Server* dan *Client*, (b) nilai *tunnel-id* pada *EoIP* harus unik untuk setiap *tunnel* karena digunakan sebagai metode untuk mengidentifikasi *tunnel*, *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, (c) 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, (d) koneksi Internet dapat dilakukan oleh *client* melalui setiap perangkat *AP* dengan *SSID* yang sama yaitu "STMIK Bumigora", (e) manajemen dan *monitoring user hotspot* dapat dilakukan secara terpusat meskipun setiap *user* terhubung ke perangkat *AP* berbeda.

IV. KESIMPULAN

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

- 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.

V. SARAN

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

- Menganalisa unjuk kerja jaringan atau *Quality of Service (QoS)* terkait penggunaan *transparent bridge tunnel EoIP over SSTP* pada hotspot.
- Menganalisa fitur keamanan terkait penerapan *transparent bridge tunnel EoIP over SSTP* pada hotspot.
- Menerapkan *Bridge Control Protocol (BCP)* pada *SSTP* sebagai pengganti *EoIP* untuk sentralisasi manajemen dan *monitoring hotspot*.
- Membandingkan QoS dan fitur keamanan terkait penerapan sentralisasi manajemen *hotspot* berbasis *transparent bridge tunnel EoIP over SSTP* dengan teknik lainnya seperti *transparent bridge tunnel EoIP over PPTP*, *BCP SSTP* dan *Multiprotocol Label Switching (MPLS) Virtual Private LAN Service (VPLS)*.
- Mengembangkan aplikasi manajemen dan *monitoring*

Sentralisasi Manajemen Hotspot Menggunakan Transparent Bridge Tunnel EoIP over SSTP

I Putu Hariyadi

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

DAFTAR PUSTAKA

- [1] Mikrotik. 2015. Manual:Interface/EoIP. <http://wiki.mikrotik.com/wiki/Manual:Interface/EoIP>. Diakses tanggal 4 Desember 2016
- [2] Microsoft. 2007. SSTP Remote Access Step-by-Step Guide: Deployment. [https://technet.microsoft.com/en-us/library/cc731352\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc731352(v=ws.10).aspx). Diakses tanggal 30 Nopember 2016
- [3] WikiBooks. 2016. Switches, Routers, Bridges and LANs/Bridges. https://en.wikibooks.org/wiki/Switches,_Routers,_Bridges_and_LANs/Bridges. Diakses tanggal 15 Desember 2016
- [4] 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
- [5] Deris Stiawan. 2009. Fundamental Internetworking Development & Life Cycle. http://unsri.ac.id/upload/arsip/network_development_cycles.pdf, Diakses tanggal 7 Desember 2016