Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September

OPEN ACCESS

https://doi.org/10.35870/jimik.v5i3.993

Analisis Konfigurasi Tunnel IPv6, Auto Tunnel, dan ISATAP dalam Pembangunan Infrastruktur Jaringan

Yuma Akbar [1], Kiki Setiawan [2], Raisah Fajri Aula [3], Muqorrobin Aimar [4*]

[1,2,3,4*] Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Email: yuma.pjj@gmail.com [1], ki2djoaz@gmail.com [2], fajriaula@gmail.com [3], muqorrobina2002@gmail.com [4*]

Histori Artikel:
Dikirim 24 Juli 2024; *Diterima dalam bentuk revisi* 10 Agustus 2024; *Diterima* 20 Agustus 2024; *Diterbitkan* 20 September 2024. Semua hak dilindungi oleh Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) STMIK Indonesia Banda Aceh.

Abstrak

IP (Internet Protocol) dibutuhkan untuk menjadi Alamat sebuah perangkat yang ingin saling terhubung, baik terhubung secara local ataupun ke internet. Seiring berkembangnya teknologi, maka alokasi pengalamatan IP semakin diperlukan. Alamat IP yang sering di gunakan adalah IPv4, namun alokasi IPv4 semakin terbatas. Untuk itu dibuatlah versi IP terbarukan yaitu IPv6. IPv6 sendiri memiliki banyak keunggulan dari segi keamanan yang sudah di lengkapi dengan enkripsi, lalu dari segi efektifitas dalam konfigurasi yang bisa menggunakan Auto Config, serta jumlah alokasi yang lebih banyak di banding IPv4. Jika IPv4 hanya menggunakankan 32 bit, IPv6 menggunakan 128 bit, untuk itu jumlah alokasi yang diberikan IPv6 jauh lebih banyak. Jumlah itu seharusnya bisa menutup kekurang alokasi dari IPv4. Karenanya migrasi IPv4 ke IPv6 perlahan harus di lakukan, supaya dapat menanggulangi kekurangan alokasi pada IPv4. Untungnya pada IPv6 tunneling dapat berjalan paralel dengan IPv4 tanpa mengganggu infrastruktur yang sudah ada. Yang mana IPv4 dapat dijadikan sebagai Underlay Network (jaringan yang menjadi pondasi jaringan virtual di atasnya), dan IPv6 akan menjadi Overlay Network (jaringan virtual yang menghububungkan antar user seolah-olah terhubung secara langsung, jaringan virtual ini harus di bangun di atas Underlay Network, dalam kasus ini tunnel IPv6 yang akan di jadikan sebagai jaringan virtual).

Kata Kunci: IPv6 Tunnel; Underlay Network; Overlay Network; Konfigurasi.

Abstract

IP (Internet Protocol) is needed to be the address of a device that wants to connect to each other, whether connected locally or to the internet. As technology develops, IP addressing allocation becomes increasingly necessary. The IP address that is often used is IPv4, but IPv4 allocation is increasingly limited. For this reason, a renewable IP version was created, namely IPv6. IPv6 itself has many advantages in terms of security which is equipped with encryption, then in terms of effectiveness in configuration which can use Auto Config, as well as a larger number of allocations compared to IPv4. If IPv4 only uses 32 bits, IPv6 uses 128 bits, for this reason the number of allocations given by IPv6 is much greater. This amount should be able to cover the lack of allocation from IPv4. Therefore, IPv4 to IPv6 migration must be carried out slowly, in-order-to overcome the lack of allocation in IPv4. Fortunately, IPv6 tunneling can run in parallel with IPv4 without disrupting existing infrastructure. Where IPv4 can be used as an Underlay Network (a network that is the foundation of the virtual network above it), and IPv6 will be an Overlay Network (a virtual network that connects users as if they were connected directly, this virtual network must be built on top of the Underlay Network, in this case the IPv6 tunnel will be used as a virtual network).

Keyword: IPv6 Tunnel; Underlay Network; Overlay Network; Configuration.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

1. Pendahuluan

Dalam perkembangan teknologi jaringan, kebutuhan akan alokasi alamat *Internet Protocol* (IP) semakin meningkat seiring dengan pertumbuhan jumlah perangkat yang terhubung ke internet. Hal ini dipicu oleh peningkatan signifikan dalam penggunaan internet, baik oleh individu maupun lembaga, serta bertambahnya jumlah penyedia layanan internet. Fenomena ini mendorong permintaan yang lebih besar terhadap alamat IP publik. Namun, alokasi *IPv4* (*Internet Protocol Version* 4), yang merupakan protokol IP yang paling umum digunakan saat ini, telah mencapai batas maksimum, sehingga tidak mampu lagi memenuhi kebutuhan yang terus meningkat. Untuk mengatasi masalah ini, protokol IP terbaru, yaitu *IPv6* (*Internet Protocol Version* 6), dikembangkan dengan kapasitas alokasi alamat yang jauh lebih besar dan fitur-fitur tambahan yang lebih canggih. Menurut Lukman dan Wahyu Adi Pratomo dalam jurnal mereka yang berjudul "Implementasi Jaringan IPv6 Pada Infrastruktur Jaringan IPv4 Dengan Menggunakan *Tunnel* Broker," *IPv6* adalah solusi terbarukan yang dirancang untuk menggantikan keterbatasan dari *IPv4* dengan menyediakan ruang alamat yang lebih luas dan peningkatan keamanan. Penulis jurnal tersebut juga menekankan bahwa transisi dari *IPv4* ke *IPv6* menjadi sangat penting untuk dilakukan guna mendukung infrastruktur jaringan yang lebih modern dan fleksibel (Lukman & Wahyu Adi Pratomo, 2020).

Salah satu tantangan utama dalam penerapan *IPv6* adalah bagaimana memastikan protokol tersebut dapat berfungsi secara optimal tanpa harus menggantikan sepenuhnya infrastruktur *IPv4* yang sudah ada. Infrastruktur yang telah berjalan sebagian besar masih bergantung pada *IPv4*, sehingga membutuhkan solusi yang dapat mengintegrasikan kedua protokol tersebut. Michael Sitorus dan Neneng Rachmalia Feta dalam jurnal mereka yang berjudul "Analisis Interkoneksi Jaringan IPv6 Terhadap IPv4 Dengan *Tunnel* Broker Berbasis Web" menyoroti bahwa salah satu solusi potensial yang dapat diterapkan adalah penggunaan teknologi *tunnel broker*. Teknologi ini memungkinkan komunikasi antara *IPv6* dengan *IPv6* lainnya melalui jaringan yang hanya mendukung *IPv4*. Dengan demikian, proses transisi dari *IPv4* ke *IPv6* dapat dilakukan secara bertahap tanpa mengganggu kinerja infrastruktur yang sudah ada (Sitorus & Feta, 2020). Berdasarkan hal tersebut, perlu dilakukan analisis lebih mendalam mengenai bagaimana konfigurasi *tunnel* ini dapat dioptimalkan sehingga jaringan *IPv4* dan *IPv6* dapat bekerja secara fleksibel dan efisien.

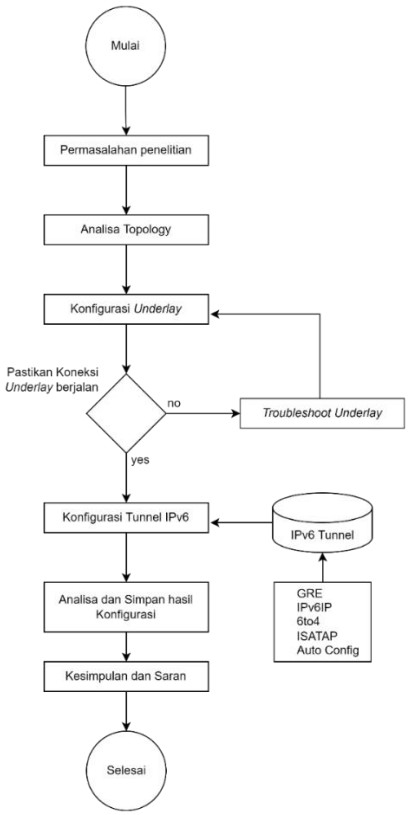
Selain teknologi *tunnel broker*, salah satu metode yang sering digunakan dalam proses migrasi *IPv4* ke *IPv6* adalah *dual stack tunneling*. Indra Warman dan Mohd Yudhistira Septian Nugraha dalam jurnal mereka yang berjudul "Analisa Implementasi Interkoneksi Antara IPv4 Dengan IPv6 Menggunakan Metode *Dual Stack* pada Mikrotik RouterOS" menyebutkan bahwa metode ini memungkinkan jaringan untuk mendukung kedua protokol, yaitu *IPv4* dan *IPv6*, secara bersamaan. Keunggulan dari metode *dual stack* ini adalah kemampuannya untuk memudahkan transisi tanpa mengganggu operasional jaringan yang sedang berjalan, sehingga kedua protokol dapat digunakan dalam satu infrastruktur yang sama (Warman & Nugraha, 2017). Hal ini penting terutama dalam masa-masa awal transisi, di mana jaringan harus tetap kompatibel dengan perangkat yang hanya mendukung *IPv4*, sambil secara bertahap mengadopsi *IPv6*.

Teknologi *tunnel* lainnya yang dapat diterapkan dalam proses transisi ini adalah *6to4 tunneling*. Gulam Fakih dan Angga Setiyadi dalam jurnal mereka yang berjudul "Implementasi IPv6 Dengan Metode Migrasi NAT64 dan VPLS Untuk Mendukung IPv6 Mobile di Sebuah Institusi Pendidikan" menjelaskan bahwa metode *6to4* memungkinkan pembuatan jalur *tunnel IPv6* di atas jaringan *IPv4* yang sudah ada. Teknologi ini menyediakan solusi efisien yang memungkinkan kedua protokol, *IPv4* dan *IPv6*, berjalan secara bersamaan tanpa memerlukan perubahan signifikan pada infrastruktur *IPv4* yang ada. Selain itu, metode ini juga memungkinkan pengangkutan paket *IPv6* melalui jaringan *IPv4*, menjadikannya alternatif yang lebih hemat biaya dalam proses migrasi (Fakih & Setiyadi, 2019). Pada penelitian ini, konfigurasi berbagai jenis *tunnel*, seperti *IPv6IP*, *auto-tunnel*, dan *ISATAP* (*Intra-Site Automatic Tunnel Addressing Protocol*), akan dianalisis secara mendalam untuk menilai bagaimana metode-metode tersebut dapat membantu menanggulangi keterbatasan alokasi *IPv4* dan mendukung proses migrasi ke *IPv6*.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

Desti Mualfah, Gope Mandala Putra, dan Rahmad Firdaus dalam jurnal mereka yang berjudul "Analisis Perbandingan IPv4 Dengan IPv6 Penggunaan CCTV Berbasis Area *Traffic* Control Security (ATCS)," performa layanan yang menggunakan *IPv6* terbukti lebih baik dibandingkan dengan *IPv4*, terutama dalam hal kualitas layanan (*Quality of Service* atau QoS) untuk aplikasi seperti pengawasan berbasis CCTV. Dari sini dapat diharapkan bahwa penerapan *tunneling IPv6* akan memberikan manfaat signifikan bagi layanan-layanan lainnya, seperti *FTP*, *IoT*, serta layanan telepon berbasis jaringan (Mualfah *et al.*, 2020). Oleh karena itu, penelitian ini bertujuan untuk menganalisis lebih lanjut penerapan berbagai metode *tunneling IPv6* pada perangkat *router*, serta mengevaluasi efektivitas metode-metode tersebut dalam mendukung migrasi *IPv6* yang lebih efisien tanpa mengganggu kinerja infrastruktur *IPv4* yang sudah berjalan.

2. Metode Penelitian



Gambar 1. Rancangan Pengujian

Berikut adalah metode penelitian yang akan di gunakan. Tahap pertama yaitu dengan merumuskan permasalahan penelitian melaui jurnal-jurnal pada bagian pendahuluan. Kasus-kasus dalam jurnal akan dijarikan fokus penelitian yaitu berkaitan dengan *tunnel* IPv6. Tahapan berikutnya adalah membuat Analisa topologi yang mudah untuk di pahami, supaya lebih mudah untuk di implementasikan pada jaringan yang lebih kompleks. Tahap berikutnya adalah konfigurasi, yang mana pada tahap ini di bagi menjadi 2 yaitu *Underlay* dan *Overlay*. *Underlay* adalah landasan dasar infrasutruktur yang di bangun menggunakan IPv4. *Overlay* adalah jaringan IPv6 yang berjalan di atas IPv4 underlay untuk mengirimkan *traffic* melalui t*unnel interface*. Terakhir adalah Analisa hasil dari konfigrasi *tunnel* yang mana akan menentukan Kesimpulan dan saran pada akhir penelitian.

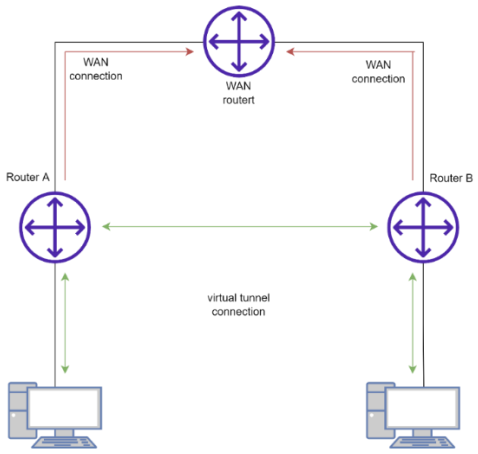
Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

3. Hasil dan Pembahasan

3.1 Hasil

3.1.1 Analisa *Topology*

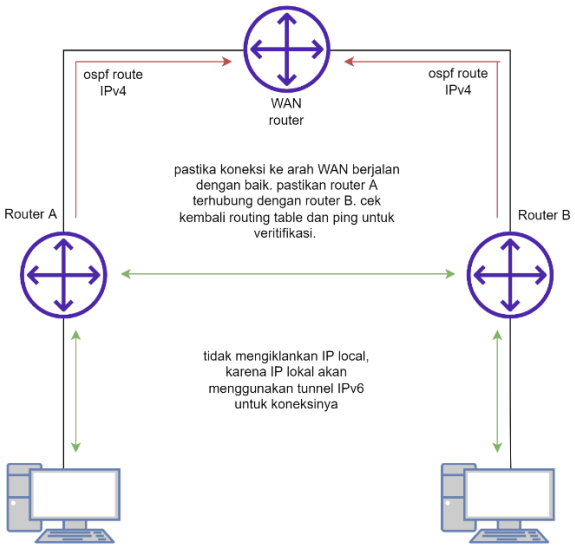
Dalam langkah ini, penulis menyiapkan emulator untuk menjalankan topology yang akan diteliti. Nantinya tiga router akan di aktifkan, dua router akan terhubung langusng dengan PC (jaringan lokal), dan satu router akan dijadikan sebagai WAN Router. Dengan demikian 2 jaringan local akan terpisah oleh WAN router. Ekspektasi dari lab ini adalah memastikan kedua jaringan lokal yang terpisah oleh WAN dapat terhubung dengan Interface Tunnel menggunakan IPv6.



Gambar 2. *Plan Topology*

3.1.2 Konfigurasi Underlay

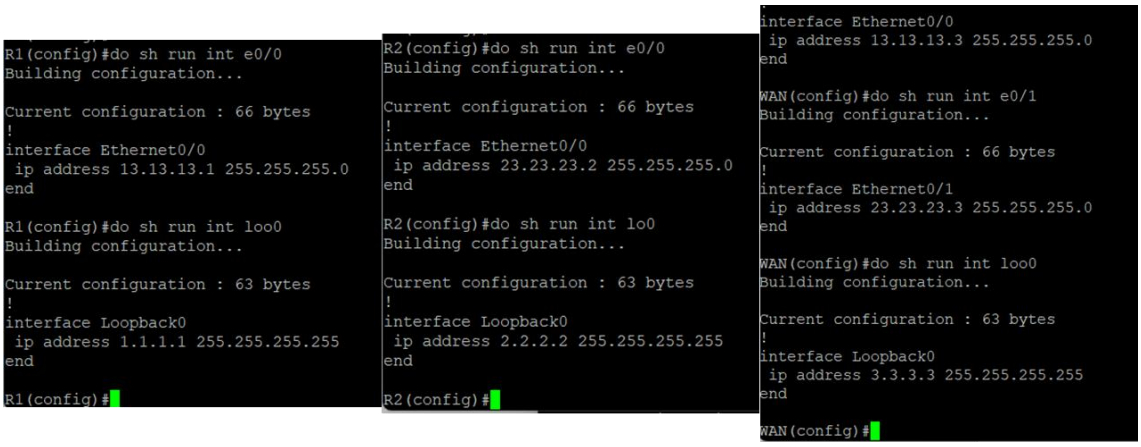
Pada tahapan ini, penulis melakukan Konfigurasi *Underlay*. Yang mana cukup memastikan masing-masing koneksi ke arah WAN *router* dapat di akses dari kedua lokal jaringan. Terkait dengan koneksi ke arah WAN *router* bisa menggunakan *static route* dan NAT, ataupun *dynamic route*. Untuk penelitian ini penulis memilih menggunakan *dynamic route* karena fokus uji hanya pada konfigurasi *tunnel* IPv6.



Gambar 3. Plan Konfigurasi *Underlay*

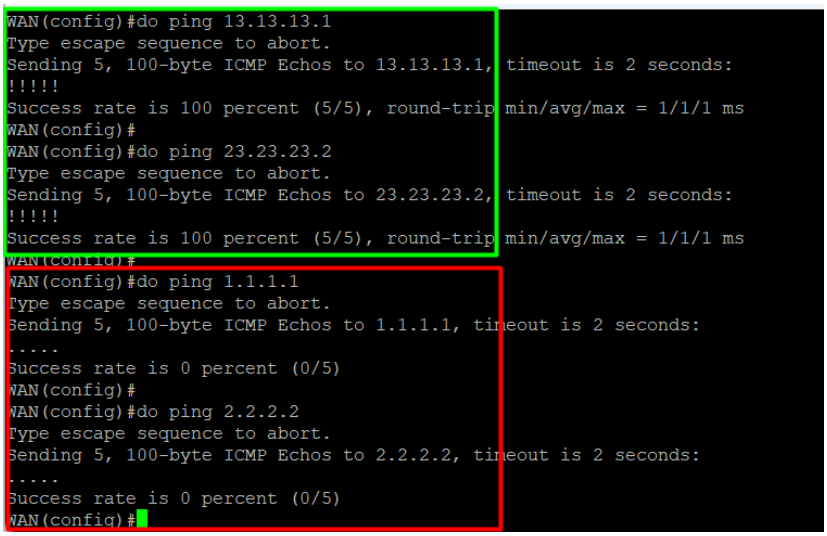
Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

Pada Konfigurasi underlay penulis akan menggunakan *dynamic route* OSPF yang umum dipakai dan bersifat *open source*. Konfigurasi OSPF akan di implementasikan pada setiap *router*. Untuk *router* A dan *router* B tidak merouting IPv6 lokal, karena koneksi lokal akan di bangun menggunakan IPv6. Yang mana IPv6 akan terhubung melalui *interface tunnel* yang berjalan di atas IPv4 *routing* OSPF sebagai *underlaynya*. Untuk itu sangat di perlukan pengecekan untuk memastikan underlay sudah berjalan dengan baik. Jika *underlay* tidak berjalan maka *tunnel interface* juga tidak akan aktif. Pengecekan bisa di lakukan dengan cara memastikan IP *router* A dan *router* B ke arah WAN sudah terdaftar pada table *routing*. Supaya lebih tervalidasi ping dan *trance route* juga bisa di lakukan untuk memastikan jaringan benar-benar berjalan dengan baik.



Gambar 4. Konfigurasi IP R1, R2, dan WAN

Berikut adalah gambar konfigurasi R1, R2, dan WAN yang mana *interface* eth0/0 pada R1 dikonfigurasikan IP 12.12.12.1 dan pada R2 dikonfigurasikan IP 23.23.23.2. Pada WAN konfigurasi IP menyesuaikan *segment* R1 dan R2 dimasing-masing *interfacenya*. Pada lab ini konfigurasi *interface loopback* juga di perlukan untuk melakukan verifikasi *routing* OSPF, serta *loopback* akan menjadi *router-id* dari OSPF yang akan di implementasikan.



Gambar 5. Tes Ping P2P dan Loopback

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

Sebelum melanjutkan ke tahap *routing*, penulis melakukan pengecekan *peer to peer connection* (P2P *Connection*) dengan ping. Memastikan WAN dapat terhubung ke R1 dan R2 lewat P2P. Terkait IP *interface Loopback* masih belum bisa terhubung karena *routing* belum di konfigurasikan.

```
R1(config)#do sh run | s ospf
router ospf 100
 network 1.1.1.1 0.0.0.0 area 0
 network 13.13.13.1 0.0.0.0 area 0
R1(config)#
R2(config)#do sh run | s ospf
router ospf 100
 network 2.2.2.2 0.0.0.0 area 0
 network 23.23.23.2 0.0.0.0 area 0
R2(config)#
WAN(config)#do sh run | s ospf
router ospf 100
 network 3.3.3.3 0.0.0.0 area 0
 network 13.13.13.3 0.0.0.0 area 0
 network 23.23.23.3 0.0.0.0 area 0
WAN(config)#
```

Gambar 6. Konfigurasi OSPF

IP pada setiap *interface* diiklankan menggunakan spesifik *wildcard prefix* 32 yaitu 0.0.0.0. dengen demikian *routing* OSPF sudah berjalan. Untuk verifikasi penulis melakukan *check neighbor* OSPF, *routing table*, dan ping ke arah IP *loopback* yang sebelumnya tidak bisa di jangkau.

```
WAN(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:36    23.23.23.2      Ethernet0/1
1.1.1.1           1   FULL/DR         00:00:37    13.13.13.1      Ethernet0/0
WAN(config)#
WAN(config)#do sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/11] via 13.13.13.1, 00:12:55, Ethernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/11] via 23.23.23.2, 00:11:43, Ethernet0/1
WAN(config)#
```

Gambar 7. Verifikasi OSPF

```
WAN(config)#do ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
WAN(config)#
WAN(config)#do ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
WAN(config)#
```

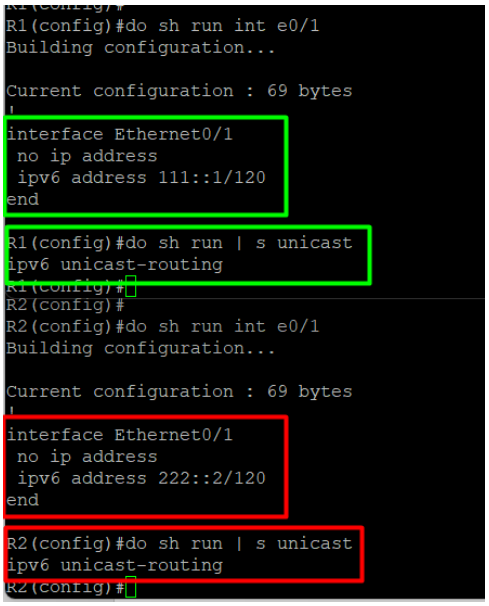
Gambar 8. Pengecekan Ping *Loopback*

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

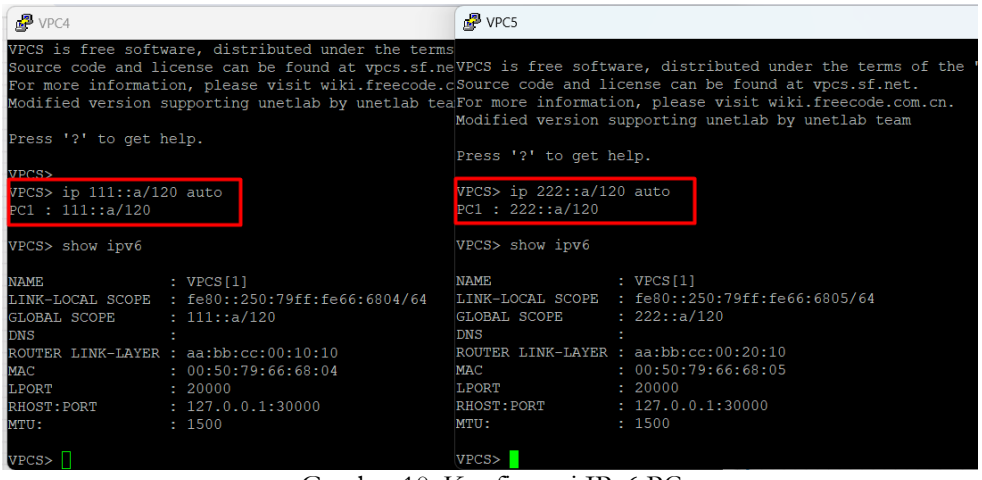
Pengecekan cukup di lakukan pada WAN router karena, WAN router ada diantara R1 dan R2. Dari hasil verifikasi ospf neighbor ke arah R1 dan R2 statusnya sudah FULL yang artinya OSPF sudah berjalan. Pada routing table juga sudah tersimpan IP loopback dari masing-masing router, dengan demikian ping ke arah loopback yang sebelumnya gagal sekarang sudah berhasil. Maka dari itu dapat disimpulkan bahwa underlay IPv4 pada infrastruktur sudah berjalan dengan baik.

3.1.3 Konfigurasi Tunnel GRE dan IPv6IP (Overlay)

Tahap berikutnya adalah konfigurasi *Tunnel* IPv6 menggunakan mode GRE. Sebelum itu konfigurasi IPv6 ke arah PC perlu dipasang. Berikut adalah detail pemasang IPv6 ke arah PC pada masing-masing *router*.



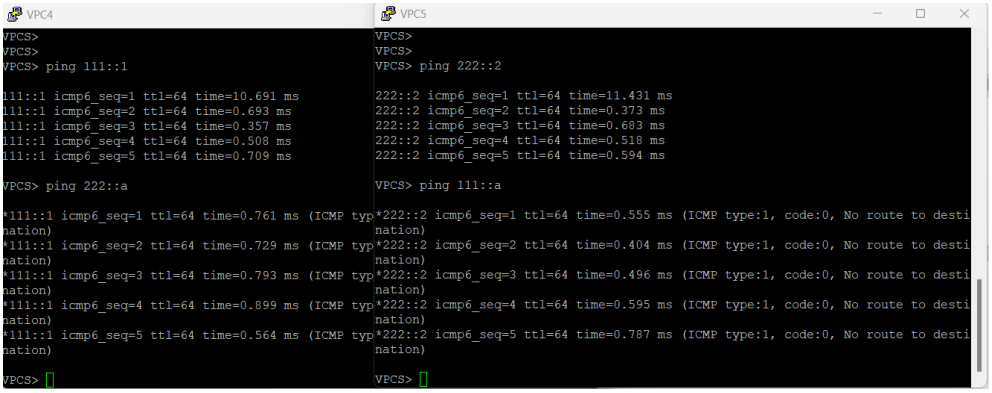
Gambar 9. Konfigurasi IPv6 router



Gambar 10. Konfigurasi IPv6 PC

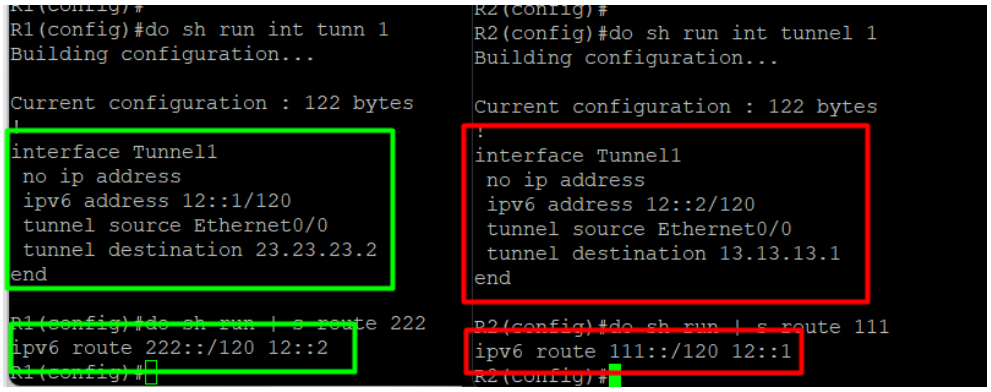
Alokasi dari R1 ke arah PC menggunakan *segment* 111::/120 sedangkan R2 menggunakan *segment* 222::/120. IPv6 *unicast routing* perlu di konfigurasikan untuk menjalankan *routing* pada IPv6. Terakhir dari sisi PC juga di konfigurasikan IPv6 ke arah *router*, pastikan ping P2P sudah berjalan.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993



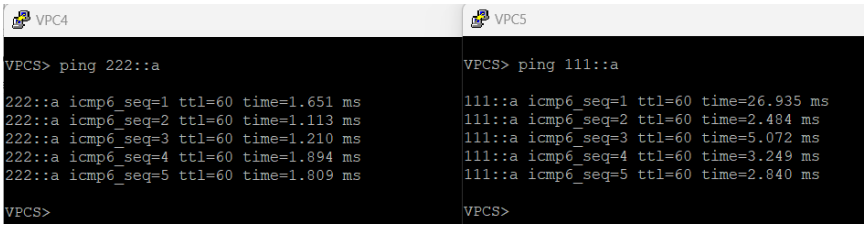
Gambar 11. Ping Gateway dan Ping Antar PC

Dari keterangan berikut ping ke arah *gateway/router* dari PC sudah berjalan dengan baik, namun PC masih belum terhubung satu sama lain. Untuk itu konfigurasi *tunnel* di perlukan supaya dapat menghubungkan koneksi antar kedua PC melalui jalur *private* di atas WAN.



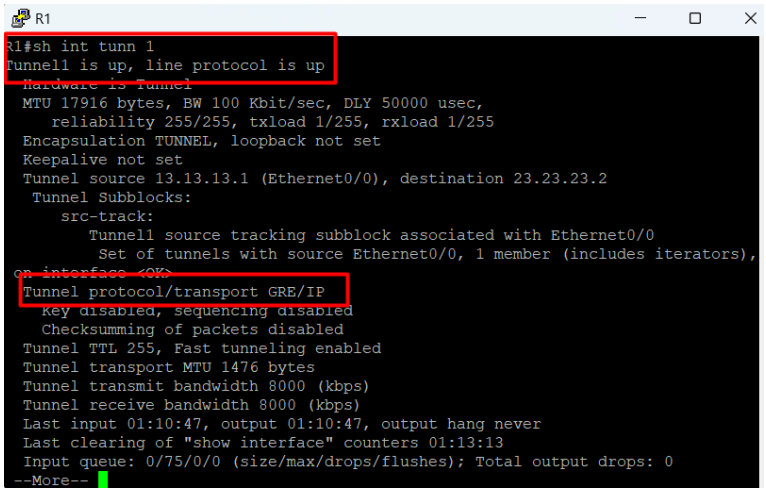
Gambar 12. Konfigurasi Tunnel GRE

Tahap pertama dalam konfigurasi *tunnel* adalah membuat *interface tunnel*, pada lab ini penulis menggunakan *tunnel number* 1. Setelah itu memberi IPv6 yang akan jadi *virtual private connection*, serta menentukan *tunnel source* dan *tunnel destination*. *Tunnel source* pada lab ini adalah *interface* e0/0, yaitu *interface* yang mengarah ke WAN *router*, sedangkan *tunnel destination* adalah IP *router* tetangga (*neighbor*) yang mengarah ke WAN *router*. Dalam hal ini dapat di simpulkan *tunnel source* dan *tunnel destination* adalah koneksi IPv4 publik yang sudah berjalan sebagai *underlay*.



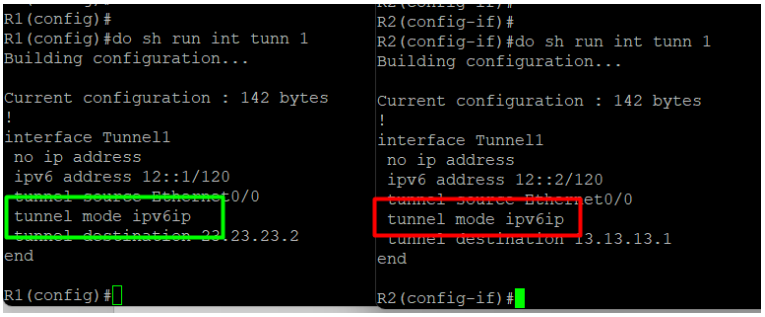
Gambar 13. Ping Antar PC

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

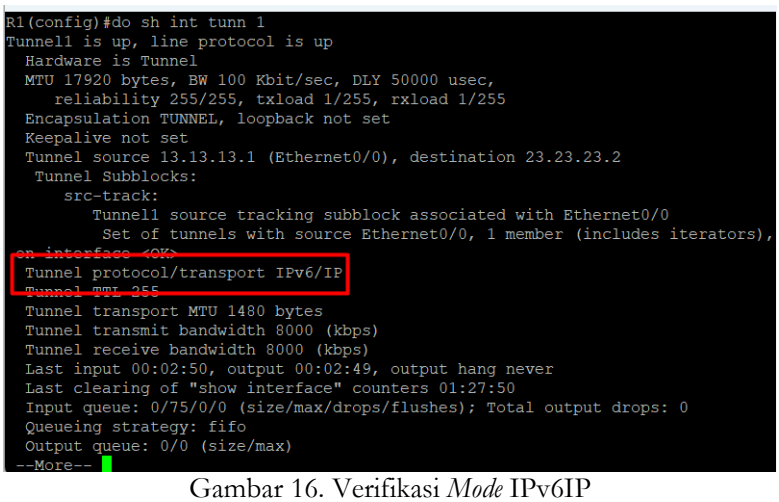


Gambar 14. *Show Interface Tunnel*

Untuk verifikasi apakah *interface tunnel* sudah berjalan, pengecekan dapat di lakukan dengan menggunakan ping antar PC. Ping yang sebelumnya gagal saat ini sudah sukses. Untuk memastikan apakah *interface tunnel* sudah berjalan bisa menggunakan *command show interface tunnel* 1 (*tunnel number*). Jika status UP maka *interface tunnel* sudah bekerja dengan baik. Terkait dengan *protocol tunnel* yang di gunakan, secara *default* cisco akan menjalakan *protocol* GRE. Untuk itu, jika ingin menggunakan mode IPv6IP maka, cukup rubah saja *tunnel* modenya ke IPv6IP.



Gambarv 15. Konfigurasi Mode IPv6IP



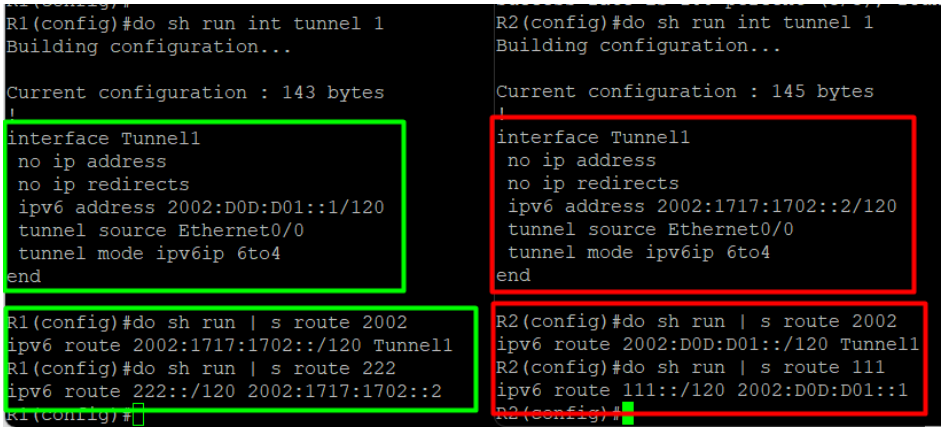
Gambar 16. Verifikasi *Mode* IPv6IP

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

Dengan ini *tunnel mode* sudah berubah, dengan status *interface* yang masih tetap UP dan berjalan dengan baik. Pada mode IPv6IP terdapat beberapa mode lanjutan seperti 6to4, ISATAP, dan Auto. Untuk konfigurasi *underlay* masih sama, namun perbedaan terletak pada konfigurasi *tunnel interfacenya*. Pada tahap berikutnya penulis masih menggunakan konfigurasi *underlay* yang sama. Perbedaan konfigurasi hanya terletak pada *tunnel*, oleh karena itu konfigurasi yang berubah hanya pada *interface tunnel*.

3.1.4 Konfigurasi *Tunnel* 6to4

Tunnel 6to4 termasuk *automatic tunnel* turunan dari mode IPv6IP. Sebelumnya pada mode GRE dan IPv6IP ada beberapa poin penting dalam konfigurasi *interface tunnel*. Salah satunya adalah penentuan *source* dan *destination tunnel*. Pada *automatic tunnel* dapat menentukan *destination tunnel* secara *otomatis*. Dengan demikian *tunnel destination* tidak perlu didefinisikan dalam konfigurasi *interface tunnel*. Pada mode 6to4 *tunnel destination* tidak perlu di konfigurasi, cukup dengan melakukan konverisi IPv4 yang mengarah ke WAN menjadi IPv6. Setelah itu *routing static* melalui *interface tunnel*, berikut adalah detailnya:



Gambar 17. Konfigurasi 6to4

Saat menggunakan mode 6to4 maka pengalamatan harus menggunakan *segment* 2002:: di susul dengan konversi IPv4 yang mengarah ke WAN *router*. Setelah itu untuk mengenalkan hasil konversi ke router tetangga di perlukan *static route* yang mendefinisikan masing-masing IPv6 *tunnel* pada *interface tunnel*. Terakhir tambahkan spesifik route dengan *static* melalui IPv6 *interface tunnel*. Terkait dengan konversi IPv4 ke IPv6 bisa dilakukan melalui *tools* gratis yang tersedia di internet, atau secara manual. Untuk konversi manual cukup merubah bilangan *decimal* ke *hexa* pada setiap *oktet*. Agar lebih mudah bisa menggunakan table konversi berikut.

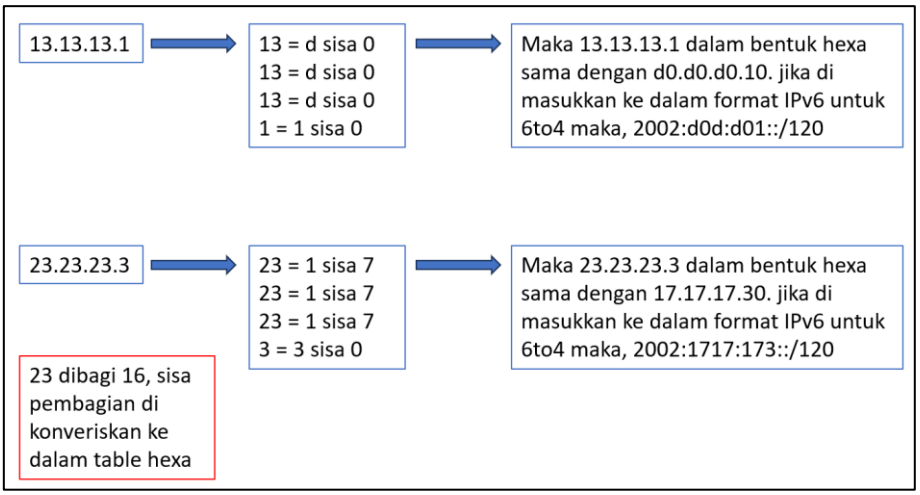
Tabel 1. Konversi *Decimal* ke *Hexa*

Decimal	Hexa
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

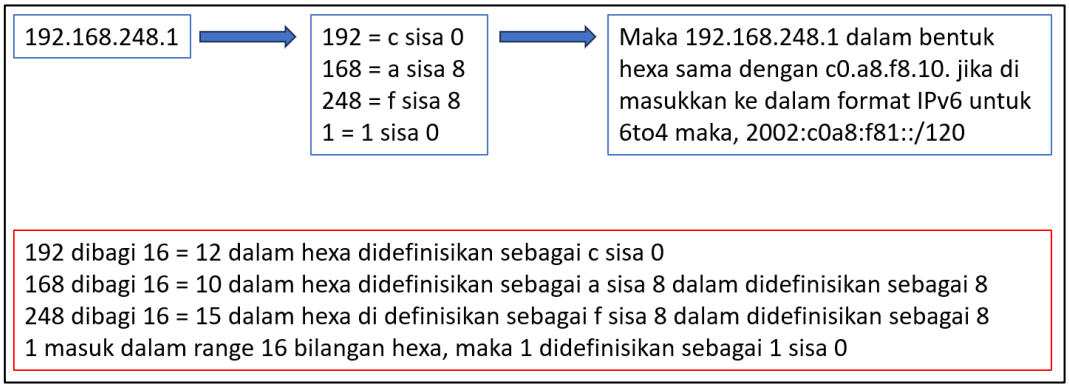
10	a
11	b
12	c
13	d
14	e
15	f

Bilangan *hexa* terdiri dari 0-9 dan huruf a-f, dengan demikian total dari bilangan *hexa* adalah 16. Untuk melakukan konversi pada IPv4 ke bilangan *hexa*, perlu dipecah setiap *oktetnya*. Contoh ip 13.13.13.1 pada R1 yang mengarah ke wan, akan di konversi ke bilangan *Hexa*.



Ganbar 18. Konversi Manual IPv4 ke IPv6

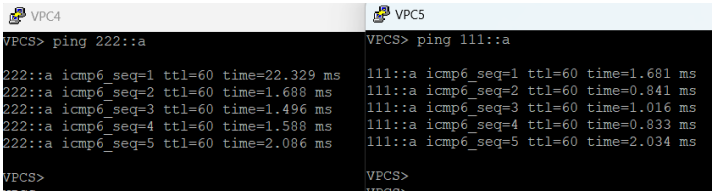
Jika bilangan tersebut masuk 16 range bilangan *hexa* maka cukup langsung di konversikan sesuai dengan table *hexa*. Tapi jika lebih besar maka perlu dibagi dengan 16 yang mana sisa pembagian juga di konversi ke dalam bilangan *hexa*. Misalkan ada IP 192.168.248.1 maka konversinya adalah 2002:c0a8:f81::/120.



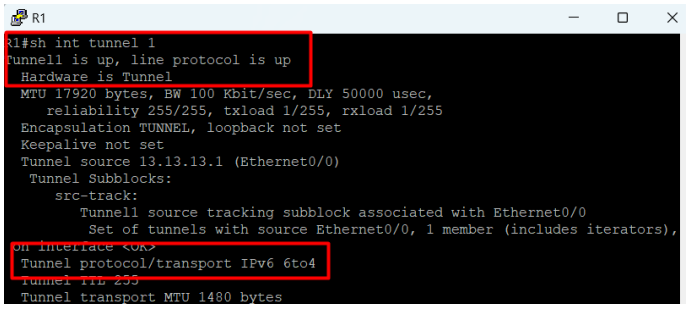
Gambar 19. Contoh Kompleks Konversi IPv4

Jika sudah di konversi maka implementasikan IPv6 tersebut ke dalam *interface tunnel* yang sudah dibuat. Terakhir routing IPv6 tersebut melalui *interface tunnel* dan tambhakna spesifik route untuk PC. Setelah itu *interface tunnel* sudah bisa melewatkan *traffic* antar PC. Berikut adalah hasil ping antar PC.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993



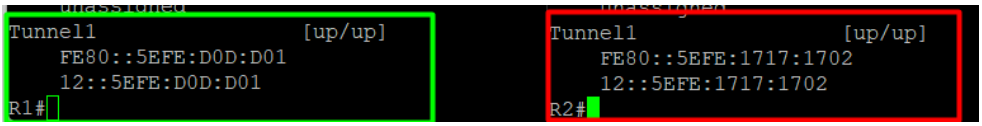
Gambar 20. Tes Ping Antar PC *Tunnel* 6to4



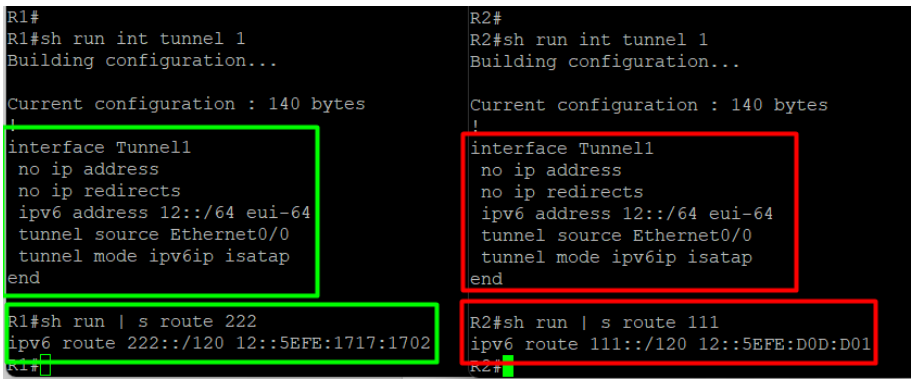
Gambar 21. Status dan *Protocol tunnel* 6to4

3.1.5 Konfigurasi ISATAP Tunnel

ISATAP *tunnel* mirip dengan 6to4, bedanya pada ISATAP konversi dilakukan secara otomatis dengan menggunakan *prefix* 64. Pada *tunnel* ISATAP pengalamatan *interface tunnel* menggunakan EUI-64. Berikut detail konfigurasinya:



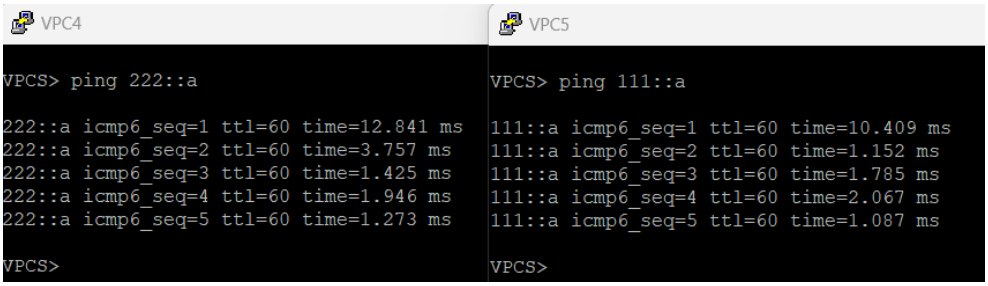
Gambar 22. Pengecekan IPv6 *Interface Tunnel* ISATAP



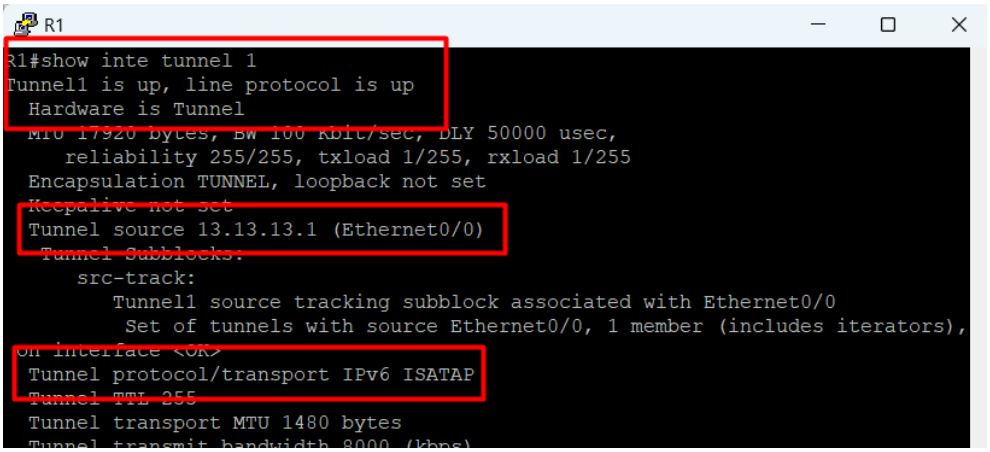
Gambar 23. Konfigurasi *Tunnel* ISATAP

Pada isatap tunnel pengalamatan menggunakan EUI-64. Disini penulis hanya menentukan network segment IPv6 yang akan di gunakan, maka secara otomatis IPv6 address terpasang menggunakan EUI-64. Pada kasus ini interface tunnel tidak menggunakan mac address, oleh karena itu EUI-64 melakukan konversi pada IPv4 yang mengarah ke WAN. Command *show IPv6 interface brief* dapat di gunakan untuk melihat IPv6 yang terpasang pada interface tunnel. Setelah memastikan IPv6 yang terpasang maka routing static bisa dikonfigurasikan untuk koneksi antar PC. Di sini konfigurasi static route ke arah IPv6 interface tunnel tidak di perlukan lagi, jadi cukup satu static route ke masing-masing PC yang dituju. Terakhir pengetesan ping antar PC dan memastikan interface tunnel sudah UP.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

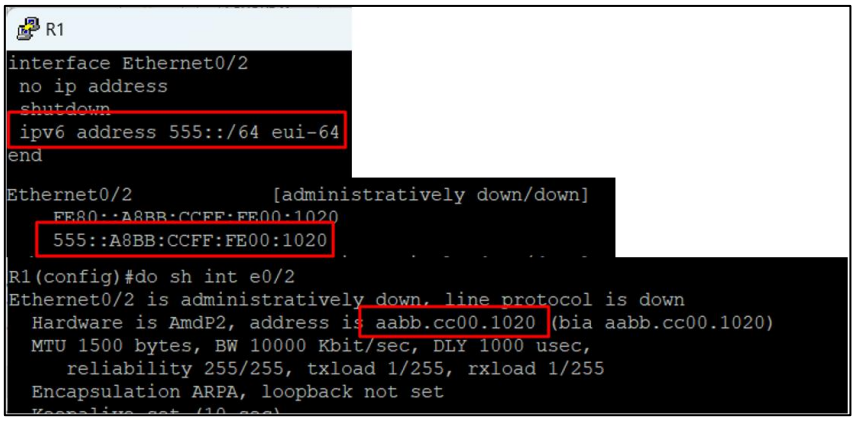


Gambar 24. Tes Ping Antar PC *Tunnel* ISATAP



Gambar 25. Cek *Interface Tunnel* ISATAP

Jika di perhatikan pada interface tunnel tidak memiliki alamat MAC, oleh karena itu EUI-64 melakukan konversi IPv6 menggunakan tunnel source IPv4. Lain hal pada interface fisik, alamat MAC akan di jadikan acuan EUI-64 saat melakukan konversi, berikut adalah contoh pada interface e0/2 sebagai interface testing EUI-64:

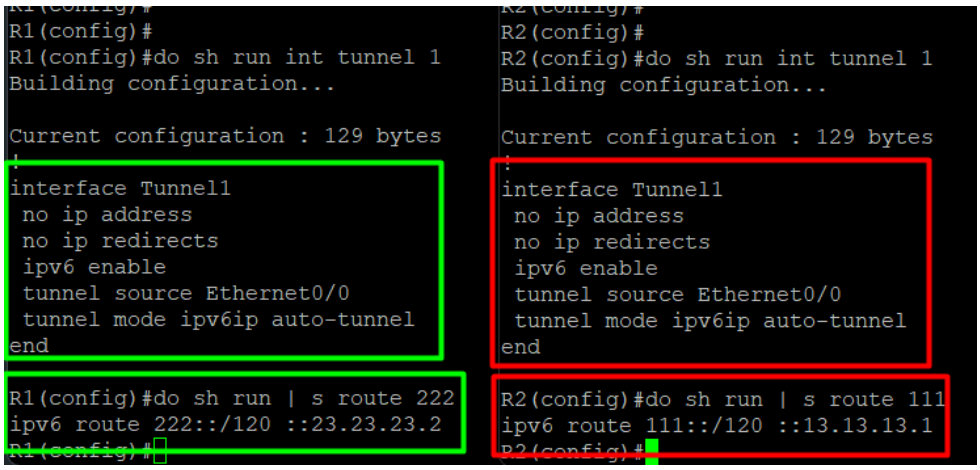


Gambar 26. Tes EUI-64 *Interface* Fisik

3.1.6 Konfigurasi *Tunnel Auto*

Auto tunnel adalah tunnel terakhir yang akan diteliti. Pada *auto tunnel* tidak diperlukan konfigurasi *tunnel destination* dan IPv6 untuk *interface tunnel*. Konfigurasi *auto tunnel* cukup dengan menentukan *source interface tunnel* dan aktifasi mode *auto*, berikut adalah detailnya:

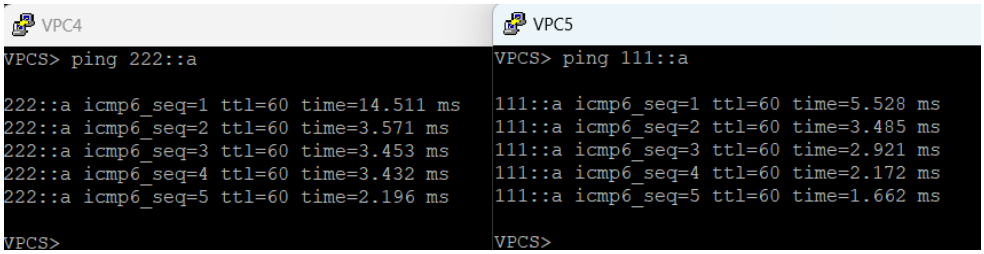
Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993



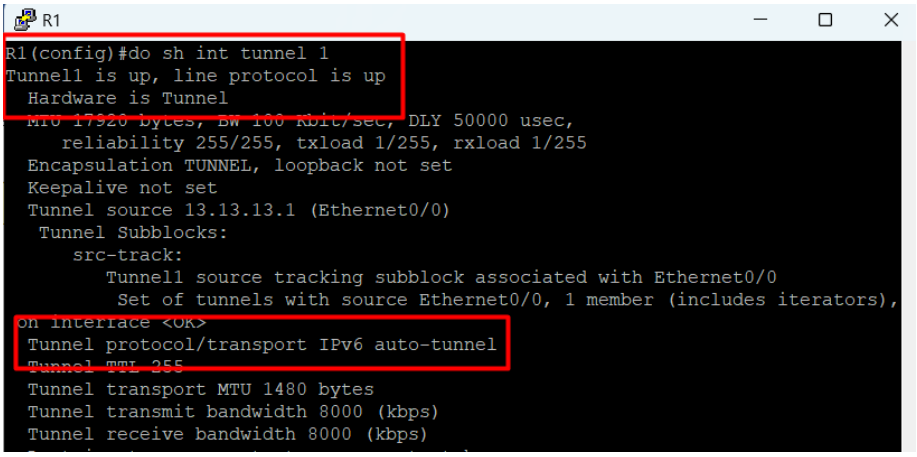
Gambar 27. Konfigurasi *Tunnel Auto*

Gambar 28. *Show* IPv6 *Tunnel Auto*

Pada konfigurasi *auto tunnel*, cukup menentukan *tunnel source* dan aktivasi *mode auto*. Nantinya IPv6 akan *otomatis terenable* pada *tunnel interface*. yang mana IPv6 akan di tulis dengan format *double colon* (::) di depan IPv4 *tunnel source*. Terakhir IP yang terpasang pada *tunnel interface* akan di jadikan *gateway* untuk *static route* antar PC.



Gambar 29. Tes Ping Antar PC *Tunnel Auto*



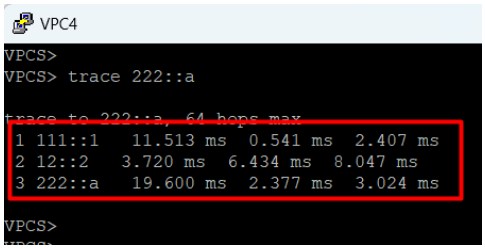
Gambar 30. Pengecekan *Interface Tunnel*

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

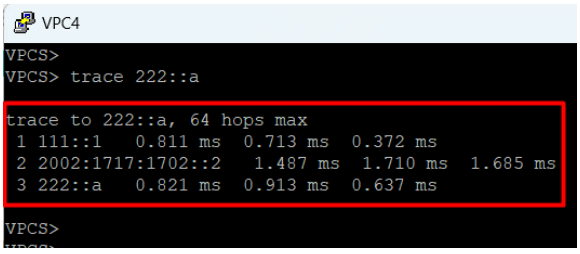
Dua PC sudah bisa saling terhubung, interface tunnel juga UP dengan protocol *auto-tunnel*. Untuk lebih mempermudah melakukan Analisa serta lebih memastikan hasil uji, penulis akan melakukan verifikasi menggunakan *trace route*. Yang mana jalur yang di lalui untuk koneksi antar PC harus melalui *interface tunnel* dan menggunakan IPv6.

3.1.7 Hasil Akhir Pengujian

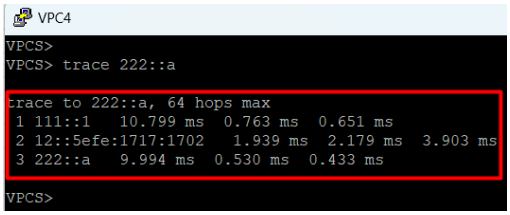
Pada tahap pengjian akhir, sesuai dengan gambar 1 maka penulis akan melakukan Analisa sekaligus verifikasi hasil konfigurasi. Yang mana penulis akan menggunakan *trace route* untuk memastikan koneksi antar PC terhubung melalui *interface tunnel* dan menggunakan IPv6. *Trace route* akan di eksekusi melaui PC, berikut adalah hasil *trace route* dari masing-masing *interface tunnel*:



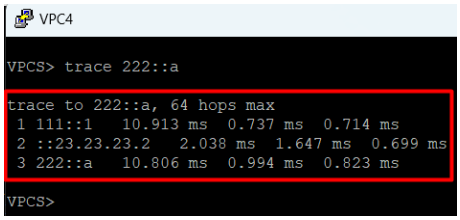
Gambar 31. *Trace Route* GRE dan IPv6IP



Gambar 32. *Trace Route* 6to4

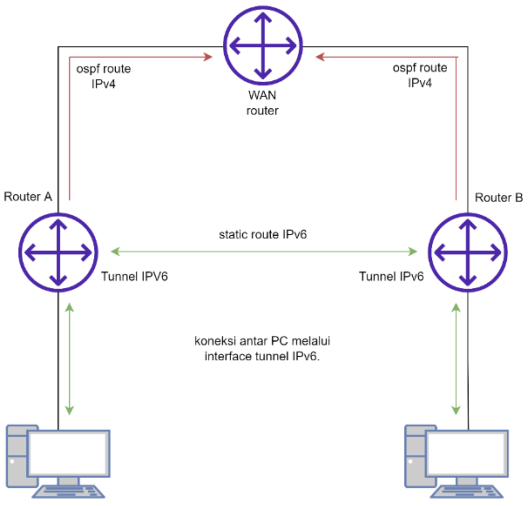


Gambar 33. *Trace Route* ISATAP



Gambar 34. *Trace Route Auto-Tunnel*

Dari hasil *trace route*, dapat dipastikan setiap koneksi melalui *interface tunnel* IPv6. Untuk *tunnel* GRE dan IPv6IP *traffic* melalui IPv6 12::2, *tunnel* 6to4 melaui IPv6 2002:1717:1702::2, *tunnel* ISATAP melalui IPv6 12::5efe:1717:1702, *tunnel auto* melaui IPv6 ::23.23.23.2. Dengan demikian dapat di simpulkan bahwa tunnel IPv6 dapat berjalan dengan baik di atas infrastruktur IPv4.



Ganbar 35. *Flow Traffic* Antar PC

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

3.2 Pembahasan

Migrasi dari *Internet Protocol Version 4* (*IPv4*) ke *Internet Protocol Version 6* (*IPv6*) merupakan salah satu tantangan utama dalam pengembangan jaringan modern. Keterbatasan alokasi alamat pada *IPv4* yang hanya memiliki ruang alamat 32-bit menjadi alasan mendesak untuk adopsi *IPv6*, yang menawarkan ruang alamat 128-bit dan mendukung lebih banyak perangkat. Untuk mendukung migrasi ini, teknologi *tunneling* menjadi solusi yang memungkinkan kedua protokol dapat berjalan bersamaan pada infrastruktur jaringan yang ada, tanpa memerlukan perubahan besar pada perangkat keras. Sebagaimana diungkapkan oleh Lukman (2020), teknologi *IPv6* dirancang untuk menggantikan *IPv4* dengan memperluas ruang alamat dan meningkatkan keamanan, serta mendukung konfigurasi otomatis yang memudahkan penggunaannya dalam jaringan yang semakin kompleks. Salah satu metode yang banyak dibahas dalam penelitian ini adalah *dual stack tunneling*, di mana jaringan diizinkan untuk mendukung kedua protokol, *IPv4* dan *IPv6*, secara bersamaan. Warman dan Nugraha (2017) dalam jurnal mereka menyebutkan bahwa penggunaan metode *dual stack* memungkinkan proses transisi berjalan lebih fleksibel. Hal ini penting karena dalam periode migrasi, masih banyak perangkat yang hanya mendukung *IPv4*. Dengan *dual stack*, perangkat yang mendukung *IPv6* dapat langsung berkomunikasi melalui jaringan *IPv6*, sementara perangkat lama yang masih menggunakan *IPv4* tetap bisa beroperasi dalam infrastruktur yang sama. Implementasi metode ini, meskipun memerlukan sumber daya jaringan yang lebih besar karena mendukung dua protokol sekaligus, memberikan transisi yang mulus dan tanpa gangguan terhadap operasional jaringan.

Selain *dual stack tunneling*, metode *6to4 tunneling* juga memberikan solusi yang efisien dalam mengintegrasikan *IPv6* ke dalam jaringan *IPv4* yang ada. Fakih dan Setiyadi (2019) menyebutkan bahwa *6to4* adalah salah satu metode migrasi yang memungkinkan pengiriman paket *IPv6* melalui jaringan *IPv4* tanpa perlu menentukan alamat tujuan *tunnel* secara manual. Metode ini menghasilkan alamat *IPv6* secara otomatis dari alamat *IPv4*, sehingga memudahkan administrator jaringan dalam mengelola transisi tanpa harus melakukan konfigurasi yang rumit. Fakih juga menunjukkan bahwa metode ini sangat efisien dalam memanfaatkan infrastruktur yang ada dan memberikan solusi yang hemat biaya untuk migrasi bertahap ke *IPv6*. Meskipun demikian, *6to4* memiliki keterbatasan dalam skala besar atau pada jaringan dengan kompleksitas tinggi, di mana konfigurasi manual mungkin tetap diperlukan untuk mengoptimalkan performa jaringan. Metode lain yang layak dipertimbangkan dalam penelitian ini adalah *ISATAP* (*Intra-Site Automatic Tunnel Addressing Protocol*), yang dirancang untuk memungkinkan jaringan *IPv6* berjalan di atas infrastruktur *IPv4* tanpa memerlukan perubahan signifikan pada perangkat keras. Warman dan Nugraha (2017) menyatakan bahwa *ISATAP* adalah metode yang konsisten dalam menghasilkan alamat *IPv6*, dengan memanfaatkan alamat *EUI-64* yang dihasilkan secara otomatis dari alamat *IPv4*. Hal ini mengurangi risiko duplikasi alamat dan meningkatkan efisiensi jaringan. Dalam implementasi *ISATAP*, perangkat yang mendukung *IPv6* dapat berkomunikasi melalui jaringan *IPv4* tanpa memerlukan perubahan besar pada infrastruktur, menjadikannya solusi yang ideal untuk jaringan internal atau *intra-site* yang belum siap sepenuhnya beralih ke *IPv6*.

Menurut Sitorus (2020), salah satu tantangan utama dalam transisi dari *IPv4* ke *IPv6* adalah memastikan komunikasi antar perangkat *IPv6* melalui jaringan *IPv4*. Dalam konteks ini, teknologi *tunnel broker* yang dibahas dalam jurnal tersebut menawarkan solusi yang memungkinkan komunikasi antar node *IPv6* tanpa perlu mengganti seluruh infrastruktur *IPv4*. Teknologi ini memanfaatkan jaringan *IPv4* sebagai medium transport untuk paket *IPv6*, memungkinkan perangkat *IPv6* saling berkomunikasi seolah-olah mereka berada di jaringan *IPv6* yang sama. Dengan menggunakan *tunnel broker*, administrator jaringan dapat mengurangi biaya dan kompleksitas dalam transisi ke *IPv6*, karena perangkat keras *IPv4* yang ada masih dapat digunakan untuk mendukung pengiriman paket *IPv6*. Dari perspektif keamanan dan kinerja, *IPv6* juga menawarkan keuntungan signifikan dibandingkan dengan *IPv4*. Seperti yang diungkapkan oleh Mualfah, Putra, dan Firdaus (2020) dalam studi mereka tentang penggunaan *IPv6* pada sistem pengawasan berbasis *CCTV*, hasil menunjukkan bahwa kualitas layanan (*Quality of Service* atau *QoS*) yang diberikan oleh *IPv6* lebih baik dibandingkan dengan *IPv4*. Hal ini terutama terlihat dalam hal latensi dan throughput, di mana *IPv6* lebih unggul dalam menangani trafik

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

data besar seperti video. Berdasarkan temuan ini, dapat diharapkan bahwa implementasi *IPv6 tunneling* tidak hanya membantu dalam proses transisi protokol, tetapi juga meningkatkan kinerja jaringan secara keseluruhan. Selain itu, Abdullah (2019) menyebutkan bahwa penggunaan teknologi transisi seperti *dual stack* dan *tunneling* tidak hanya membantu dalam hal interoperabilitas antar protokol, tetapi juga memberikan fleksibilitas dalam mengelola jaringan selama masa transisi. Penelitian Abdullah menyoroti pentingnya memilih metode yang sesuai dengan skenario jaringan spesifik, karena setiap metode memiliki kelebihan dan kekurangan masing-masing. Misalnya, sementara *dual stack* menawarkan fleksibilitas yang lebih tinggi, metode ini dapat memerlukan kapasitas jaringan yang lebih besar, sedangkan *6to4* dan *ISATAP* lebih cocok untuk skenario yang tidak memerlukan skala besar.

Penelitian ini juga menunjukkan bahwa teknologi *tunneling* memungkinkan transisi bertahap dari *IPv4* ke *IPv6* tanpa mengganggu infrastruktur yang ada. Sebagaimana diungkapkan oleh Nugroho (2019), teknologi seperti *SIIT* (*Stateless IP/ICMP Translation*) memungkinkan jaringan untuk secara dinamis menerjemahkan paket *IPv4* dan *IPv6*, sehingga kedua protokol dapat berfungsi secara bersamaan dalam satu jaringan. Hal ini semakin memperjelas bahwa berbagai metode transisi yang ada, termasuk *tunneling* dan teknologi terjemahan, memberikan fleksibilitas yang dibutuhkan untuk menghadapi tantangan migrasi ke *IPv6*.

4. Kesimpulan

Penerapan IPv6 dapat berjalan paralel bersamaan dengan infrastruktur IPv4. Dengan demikian migrasi dari IPv4 ke IPv6 dapat dieksekusi secara bertahap tanpa mengganggu infrastruktur IPv4. Metode penerapan bisa menggunakan beberapa opsi seperti *default* GRE atau IPv6IP, serta untuk mode *Automatic* bisa menggunakan 6to4, ISATAP, ataupun *Auto*. Penulis lebih menyarankan untuk menggunakan ISATAP tunnel yang lebih standar dibandingkan dengan mode lain. *Tunnel* ISATAP menggunakan konversi otomatis dengan EUI-64, membuat pengalamatan *interface tunnel* menjadi lebih konsisen dan mengurangi kemungkinan *duplicate*. Kekurangan dari tunnel 6to4 konversi masih di lakukan secara manual, sedangkan untuk auto tunnel beberapa router tidak bisa menjalankan mode ini. Oleh karena itu penulis menyarankan untuk menggunakan ISATAP *tunnel* yang lebih standar dan sudah bisa melakukan konversi secara otomatis. Dengan pemanfaatan *tunnel* IPv6 di harapkan mampu menghemat penggunaan IPv4 dalam infrastruktur jaringan. Oleh karena itu penulis menyarankan untuk membagi segmentasi penggunaan IPv6 untuk alokasi baru di beberapa titik infrasutriktur. Misalkan di perlukan penambahan perangkat IoT dalam infrastruktur, maka segmentasi IoT bisa di khususkan untuk menggunakan IPv6. Yang mana koneksi antar perangkat yang berkaitan dengan IoT di hubungkan dengan *tunnel* IPv6. Saran ini tidak hanya untuk perangkat IoT, bisa juga di terapkan untuk segmentasi lain, misal segmentasi untuk divisi A atau segmentasi *wireless,* telepon, DLL.

5. Daftar Pustaka

Abdullah, A. A., & Rizkillah, M. (2019). ANALISA PERBANDINGAN TEKNIK TRANSISI, DUAL-STACK DAN TUNNELING. *Jurnal Bumigora Information Technology (BITe)*, *1*(1), 10-21. DOI: https://doi.org/10.30812/bite.v1i1.417.

Duskarnaen, M. F., & Ajie, H. (2020). Desain Dan Implementasi Internet Protocol Version 6 (Ipv6) Di Kelas Unit Pelayanan Teknis Teknologi Informasi Dan Komunikasi (Upt Tik) Universitas Negeri Jakarta. *PINTER: Jurnal Pendidikan Teknik Informatika dan Komputer*, *4*(1), 30-34.

Fakih, G., & Setiyadi, A. (2019). IMPLEMENTASI IPv6 DENGAN METODE MIGRASI NAT64 DAN VPLS UNTUK MENDUKUNG IPv6 MOBILE DI SEBUAH INSTITUSI

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 5 No. 3 (2024) | September
OPEN ACCESS
https://doi.org/10.35870/jimik.v5i3.993

PENDIDIKAN. *Komputa: Jurnal Ilmiah Komputer dan Informatika*, *8*(2), 86-93. DOI 10.34010/KOMPUTA.V8I2.3054.

Haji, M. I., ESGS, S. P., & Arifin, S. P. (2018). Analysis Tunneling IPv4 and IPv6 on VoIP Network. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 337-344. DOI: https://doi.org/10.22219/kinetik.v3i4.708.

Lukman, L., & Pratomo, W. A. (2020). Implementasi Jaringan Ipv6 Pada Infrastruktur Jaringan Ipv4 Dengan Menggunakan Tunnel Broker. *Respati*, *15*(1), 1-11.

Marzuki, I. (2018). Mekanisme Transisi IPv4 dan IPv6 Menggunakan Metode Automatic Tunneling Pada Jaringan Client Server Berbasis Linux. *Jurnal Teknologi Informasi Indonesia (JTII)*, *3*(2), 68-73. DOI https://doi.org/10.30869/jtii.v3i2.311.

Mualfah, D., Putra, G. M., & Firdaus, R. (2022). ANALISIS PERBANDINGAN IPv4 DENGAN IPv6 PENGGUNAAN CCTV BERBASIS AREA TRAFFICT CONTROL SECURITY (ATCS). *Journal of Software Engineering and Information System (SEIS)*, 124-128. DOI: https://doi.org/10.37859/seis.v2i1.3339.

Nugroho, K., Wafiah, H., & Arifwidodo, B. (2019). Penggunaan Metode SIIT (Stateless IP/ICMP Translation) Dalam Migrasi IPv4 ke IPv6. *Journal of Telecommunication Electronics and Control Engineering (JTECE)*, *1*(01), 23-31. DOI https://doi.org/10.20895/jtece.v1i01.36.

Sitorus, M., & Feta, N. R. Analisis Interkoneksi Jaringan IPv6 Terhadap IPv4 Dengan Tunnel Broker Berbasis Web Analysis IPv6 in IPv4 Network Interconnection with Web Based Tunnel Broker. DOI: https://doi.org/10.35842/jtir.v15i1.324.

Warman, I., & Nugraha, M. Y. S. (2017). Analisa implementasi interkoneksi antara ipv4 dengan ipv6 menggunakan metode dual stack pada mikrotik routeros (studi kasus: pt. Linggo daya energi). *Jurnal Teknoif Teknik Informatika Institut Teknologi Padang*, *5*(2), 63-72.