

IMPLEMENTASI VIRTUAL PRIVATE NETWORK OVER GRE TUNNEL

Taufik Rahman

Manajemen Informatika

AMIK BSI Jakarta

<http://www.bsi.ac.id>

taufik.tkr@bsi.ac.id

Abstract— VPN network is very interesting to be discussed and widely so that many have done research then this research will do the implementation of vpn network using GRE Tunnel technology. This research will answer how this virtual interface can connect more than one router with another router by using GRE protocol to deliver packets, protocols and more so that user needs such as connecting layer 2 between sites can be fulfilled through VPN GRE Tunnel. Finally after the preparation for this research started install simulator GNS3, mikrotik routerOS, virtualbox, operating system. Network administration by writing ip address. Configuration on loopbaack adapter, MikroTik-HeadOffice, MikroTik-Branch and Pc-Branch. Once connected is formed a virtual interface and given ip address as ip binder of two public ip. Then proved by ping and tracert between Pc-Branch can be interconnected, so can also exchange data with sharing files so that can be done mapping drive. With Packet Sniffer and Torch tools on Mikrotik can see traffic passing through the virtual gre tunnel interface. After experimenting with the GNS3 simulator application in such a way with the console script and proven with the image that the vpn network with gre tunnel interface can connect more than 2 MikroTik-Branch routers through MikroTik-HeadOffice as network backbone. With its built vpn gre tunnel network, the data communication is safe because it is inside the tunnel even in the internet network. Further research, combining GRE Tunnel with others.

Intisari— Jaringan VPN sangat menarik untuk dibahas dan luas sehingga banyak yang sudah melakukan penelitian maka penelitian ini akan melakukan implementasi jaringan vpn menggunakan teknologi GRE Tunnel. Penelitian ini akan menjawab bagaimana interface virtual ini dapat menghubungkan lebih dari satu router dengan router lainnya dengan menggunakan protokol GRE mampu mengantarkan paket, protokol dan lainnya sehingga kebutuhan user seperti menghubungkan layer 2 antar site dapat dipenuhi melalui VPN GRE Tunnel. Akhirnya setelah dilakukan persiapan untuk penelitian ini dimulai instal simulator GNS3, mikrotik routerOS, virtualbox, sistem operasi. Administrasi jaringan dengan menuliskan ip address. Konfigurasi pada

loopbaack adapter, MikroTik-HeadOffice, MikroTik-Branch dan Pc-Branch. Setelah terkoneksi terbentuklah interface virtual dan diberikan ip address sebagai ip pengikat dari dua ip publik. Kemudian dibuktikan dengan ping dan tracert antar Pc-Branch dapat saling berhubungan, begitu juga dapat saling melakukan pertukaran data dengan berbagi file sehingga dapat dilakukan mapping drive. Dengan tool Packet Sniffer dan Torch pada Mikrotik dapat melihat trafik yang melewati interface virtual gre tunnel. Setelah melakukan eksperimen dengan aplikasi simulator GNS3 sedemikian rupa dengan script console dan dibuktikan dengan gambar bahwa jaringan vpn dengan interface gre tunnel dapat menghubungkan lebih dari 2 router MikroTik-Branch melalui MikroTik-HeadOffice sebagai backbone jaringan. Dengan dibangun nya jaringan vpn gre tunnel, maka komunikasi data aman karena berada di dalam tunnel meski di jaringan internet. Penelitian selanjutnya, mengkombinasikan GRE Tunnel dengan yang lainnya.

Kata Kunci: Network, Virtual, Tunnel, GRE.

PENDAHULUAN

Virtual Private Network meluas jaringan pribadi melalui jaringan publik, seperti internet. Hal ini memungkinkan pengguna untuk mengirim dan menerima data melalui jaringan publik bersama seakan perangkat komputasi mereka langsung terhubung ke jaringan pribadi. layanan VPN ini sepenuhnya didedikasikan untuk perusahaan ukuran kecil dan menengah (Krithikaa, Priyadharsini, & Subha, 2016).

Hari ini kantor organisasi secara luas tersebar di seluruh lokasi geografis yang berbeda. Ini jauh mencapai disebabkan peningkatan kegiatan usaha dan keinginan untuk memahami pangsa pasar yang lebih. Akibatnya, banyak kantor harus didirikan di lokasi yang berbeda. Dalam dunia bisnis global saat ini, kantor baru dapat terletak di dalam suatu negara atau dapat tersebar di benua berbeda juga. Karena lingkungan teknis ini, semua kantor jauh harus memiliki konektivitas jaringan yang efisien dengan kantor pusat mereka. Karena pentingnya, VPN telah menjadi solusi yang populer digunakan di banyak

lingkungan industri. Banyak variasi yang mungkin sementara menerapkan VPN. Hal ini dapat dikategorikan berdasarkan protokol tunneling (layer 2 atau layer 3), topologi dilaksanakan (full mesh, hub dan berbicara) dan infrastruktur (situs-situs, remote VPN) (Ahmed, Butt, & Siddiqui, 2016)

Solusi VPN dapat digunakan pada infrastruktur jaringan nirkabel untuk mengamankan transmisi antara klien nirkabel dan jaringan perusahaan kabel mereka. Ada banyak platform perangkat lunak yang dapat digunakan untuk mengimplementasikan VPN berbasis software solusi seperti windows, Linux, Solaris, Mac, dan BSD. Dalam tulisan ini, evaluasi kinerja beberapa solusi akses remote VPN, yaitu Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP / IPSec), dan Secure Socket Layer (SSL) akan diselidiki atas secara empiris jaringan nirkabel. Beberapa QoS metrik kinerja seperti throughput, latency, jitter, dan packet loss diukur untuk mengeksplorasi dampak VPN ini pada performa terbaik yang dirasakan oleh aplikasi pengguna akhir (Jaha, 2015).

Karena tunneling melibatkan pengemasan ulang data lalu lintas ke dalam bentuk yang berbeda, mungkin dengan enkripsi sebagai standar, penggunaan ketiga adalah untuk menyembunyikan sifat lalu lintas yang dijalankan melalui terowongan (Nigam & Gupta, 2016).

Metode tunneling dapat dilakukan secara manual maupun otomatis. Koneksi untuk manual menggunakan point to point mode dimana alamat sumber ditugaskan oleh operator dan alamat tujuan ditemukan secara otomatis. Metode ini diibaratkan membuat sebuah jembatan yang digunakan untuk mentransfer paket antar dua jaringan yang sama melalui jaringan yang tidak kompatibel. GRE (Generic Routing Encapsulation) adalah protokol tunneling yang pada awalnya dikembangkan oleh Cisco. GRE tunnel dapat meneruskan hanya IP dan IPv6 paket (ethernet tipe 800 dan 86dd). Jangan gunakan "Cek Gateway" pilihan "arp" ketika GRE tunnel digunakan sebagai rute gateway (MikroTik, Manual:Interface/Gre, 2015).

Generik Routing Encapsulation [GRE] protokol tunneling memberikan pendekatan generik sederhana untuk mengangkut paket satu protokol melalui protokol lain dengan cara enkapsulasi. GRE dapat digunakan sebagai protokol pembawa untuk berbagai protokol penumpang. GRE mengenkapsulasi muatan yang merupakan paket bagian dalam yang perlu disampaikan ke jaringan tujuan dalam sebuah paket IP luar. Setelah mencapai titik akhir terowongan, GRE enkapsulasi ini dihapus dan

payload diteruskan ke tujuan itu tepat (NIXON, DEVARAJ, & MOHAMMED, 2016).

GNS3 memungkinkan untuk memvisualisasikan, rencana, uji dan memecahkan masalah lingkungan jaringan di setiap vendor platform yang pada skala - tanpa perlu berinteraksi langsung dengan perangkat keras jaringan. Dengan antarmuka grafis intuitif, pengguna dengan lancar dapat menghubungkan semua jenis antarmuka virtual untuk menyusun representasi nyata dari jaringan. GNS3 berjalan pada hardware PC tradisional dan dapat digunakan pada beberapa sistem operasi, termasuk Windows, Linux, dan MacOS X. Membangun, desain dan uji jaringan dalam lingkungan virtual bebas risiko dan mengakses komunitas jaringan terbesar untuk membantu. GNS3 menawarkan cara mudah untuk merancang dan membangun jaringan dari berbagai ukuran tanpa perlu hardware. Dan bagian yang terbaik adalah gratis (GNS3, 2017).

Tujuan penelitian ini menghubungkan dua kantor atau lebih yang memiliki koneksi internet dengan membuat jaringan vpn menggunakan teknologi GRE Tunnel. Dalam melakukan penelitian ini mencoba menjawab bagaimana interface virtual menghubungkan lebih dari satu router dengan router lainnya dengan menggunakan protokol GRE mampu mengantarkan paket, protokol dan lainnya dengan mengencapsulasi sehingga kebutuhan user seperti menghubungkan layer 2 antar site memiliki platform router berbeda seperti cisco dan mikrotik.

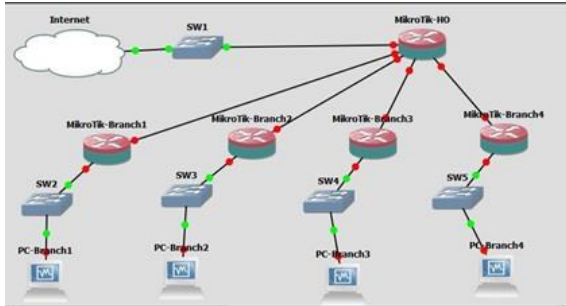
Penelitian ini menggunakan software GNS3 untuk simulasi nya yang didalam nya terdapat routerOS MikroTik untuk mengimplementasikan VPN GRE Tunnel agar dapat menjadi bahan pertimbangan dalam melakukan perancangan VPN.

BAHAN DAN METODE

Sebagai Bahan dalam penelitian ini yang dilakukan yaitu :

1. Perancangan topologi jaringan

Topologi yang digunakan untuk implementasi vpn gre tunnel adalah pengembangan dari topologi star, dimana terdapat koneksi internet dan router mikrotik yang menghubungkan.



Sumber: Rahman (2017)
Gambar 1. Rancangan Jaringan VPN GRE Tunnel

2. Aplikasi GNS3 untuk simulasi.
3. MikroTik RouterOS versi x86 untuk diinstall pada aplikasi GNS3
4. VirtualBox untuk install windows.
5. Image sistem operasi windows 7 untuk diinstal di virtualbox dan diintergrasikan dengan GNS3
6. Administrasi ip address yang berbeda segmen untuk di setting pada router. Untuk implementasi vpn GRE Tunnel real nya menggunakan ip publik statik untuk saling koneksi yang bisa didapat dari isp ketika berlangganan internet, dalam hal ini simulasi dengan GNS3 maka ip publik diganti dengan ip private. Pada penelitian ini ip address yang digunakan sebagai ip publik adalah :
10.1.1.0/24
10.1.2.0/24
10.1.3.0/24
10.1.4.0/24
Ip address yang digunakan pada interface gre tunnel adalah :
172.16.1.0/30
172.16.2.0/30
172.16.3.0/30
172.16.4.0/30
Ip address yang digunakan pada interface yang menuju ke host atau client adalah :
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
192.168.5.0/24
7. interface loopback pada laptop untuk memanggil interface pada hardware yang ada di GNS3 seperti MikroTik RouterOS, switch dan pc. Pada adapter interface loopback ini diberikan ip address 192.168.137.1/24.

Guna mendukung penelitian dilakukan tahapan pengumpulan data dengan cara :

1. Studi Pustaka dengan cara mempelajari jurnal terkait serta sumber buku yang berkaitan untuk dikutip sebagai acuan teori dalam mendukung penulisan penelitian ilmiah ini.

2. Ekperimental dengan mengadakan manipulasi terhadap objek penelitian, serta adanya kontrol yang disengaja terhadap objek penelitian tersebut (Perpusku, 2016).
Data diambil dari trafik koneksi Mikrotik-HO, MikroTik-Branch dan PC-Branch yang akan di analisa data berupa hasil dari ping dan tracert yang dapat dibuktikan untuk keberhasilan penelitian ini.

HASIL DAN PEMBAHASAN

Setelah menyiapkan administrasi jaringan yakni ip address maka langkah selanjutnya instalasi, konfigurasi dan pengujian.

1. Install GNS3 v1.2.3 untuk simulator graphical network nya
2. Install Mikrotik routerOS x86 v5.20, iso yang sudah didownload rename menjadi mikrotik.iso pindahkan ke folder D:\GNS3\qemu.0.13.0 , lalu buka cmd d:\GNS3\qemu-0.13.0>qemu-img create -f qcow2 mikrotik.img 256M. Selanjutnya ketik perintah d:\GNS3\qemu-0.13.0>qemu.exe mikrotik.img -boot d - cdrom "mikrotik.iso". Lalu ikuti langkah instalasi nya.
3. Install VirtualBox sebagai sarana partisi atau tempat yang terhubung dengan GNS3. Setelah instalasi selesai maka akan seperti pada gambar 2.
4. Install atau add adapter loopback, buka cmd ketikan hdwwiz.exe ikuti langkah nya.

Setelah proses instalasi, berikutnya proses konfigurasi. Pada GNS3, skenario nya adalah menggunakan 5 router mikrotik; satu mikrotik sebagai Head Office dan empat mikrotik sebagai Branch Office, juga menggunakan switch unmanage untuk penyebaran ip address ke komputer host atau client. Juga menggunakan adapter loopback agar dapat diakses dari luar GNS3.

1. Konfigurasi pada MikroTik-HO

Konfigurasi pada Mikrotik-HO, pemberian nama pada interface ethernet, berikut hasil print dari script console.

```
[admin@MikroTik] > interface pr
Flags: D - dynamic, X - disabled, R - running, S - slave
# NAME      TYPE      MTU      L2MTU    MAX-L2MTU
0 R         ether1    ether    1500
1 R         ether2-to-internet-Branch1 ether    1500
2 R         ether3-to-internet-Branch2 ether    1500
3 R         ether4-to-internet-Branch3 ether    1500
4 R         ether5-to-internet-Branch4 ether    1500
5 R         ether6    ether    1500
6 R         ether7    ether    1500
7 R         ether8    ether    1500
8 R         gre-tunnel1 1476    65535
9 R         gre-tunnel2 1476    65535
10 R        gre-tunnel3 1476    65535
11 R        gre-tunnel4 1476    65535
```

Konfigurasi interface gre tunnel dengan memasukkan ip publik remote milik Mikrotik-Branch begitu sebaliknya, sehingga hasil print script consolnya berikut ini:

```
[admin@MikroTik] > interface gre pr
Flags: X - disabled, R - running
0 R name="gre-tunnel1" mtu=1476 l2mtu=65535 local-address=0.0.0.0 remote-address=10.1.1.2 dscp=0
1 R name="gre-tunnel2" mtu=1476 l2mtu=65535 local-address=0.0.0.0 remote-address=10.1.2.2 dscp=0
2 R name="gre-tunnel3" mtu=1476 l2mtu=65535 local-address=0.0.0.0 remote-address=10.1.3.2 dscp=0
3 R name="gre-tunnel4" mtu=1476 l2mtu=65535 local-address=0.0.0.0 remote-address=10.1.4.2 dscp=0
```

Memberikan ip address pada interface fisik (ether1-5), interface virtual (gre-tunnel1-4) berikut hasil print script consolnya;

```
[admin@MikroTik] > ip address pr
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 192.168.137.2/24 192.168.137.0 ether1
1 10.1.1.1/24 10.1.1.0 ether2-to-internet-Branch1
2 10.1.2.1/24 10.1.2.0 ether3-to-internet-Branch2
3 10.1.3.1/24 10.1.3.0 ether4-to-internet-Branch3
4 10.1.4.1/24 10.1.4.0 ether5-to-internet-Branch4
5 172.16.1.1/30 172.16.1.0 gre-tunnel1
6 172.16.2.1/30 172.16.2.0 gre-tunnel2
7 172.16.3.1/30 172.16.3.0 gre-tunnel3
8 172.16.4.1/30 172.16.4.0 gre-tunnel4
```

Setting ip route dengan script console hasilnya di print berikut;

```
[admin@MikroTik] > ip route pr
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static,
r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 A S 0.0.0.0/0 192.168.137.1 1
1 ADC 10.1.1.0/24 10.1.1.1 ether2-to-inter... 0
2 ADC 10.1.2.0/24 10.1.2.1 ether3-to-inter... 0
3 ADC 10.1.3.0/24 10.1.3.1 ether4-to-inter... 0
4 ADC 10.1.4.0/24 10.1.4.1 ether5-to-inter... 0
5 ADC 172.16.1.0/30 172.16.1.1 gre-tunnel1 0
6 ADC 172.16.2.0/30 172.16.2.1 gre-tunnel2 0
7 ADC 172.16.3.0/30 172.16.3.1 gre-tunnel3 0
8 ADC 172.16.4.0/30 172.16.4.1 gre-tunnel4 0
9 A S 192.168.2.0/24 172.16.1.2 1
10 A S 192.168.3.0/24 172.16.2.2 1
11 A S 192.168.4.0/24 172.16.3.2 1
12 A S 192.168.5.0/24 172.16.4.2 1
13 ADC 192.168.137.0/24 192.168.137.2 ether1 0
```

Setting nat dengan action masquerade dan dns untuk resolve domain, berikut hasil print script console nya;

```
[admin@MikroTik] > ip firewall nat pr
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade out-interface=ether1
[admin@MikroTik] > ip dns pr
servers: 192.168.137.1
dynamic-servers:
allow-remote-requests: yes
max-udp-packet-size: 4096
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 14KiB
```

2. Konfigurasi pada Mikrotik-Branch1

Pemberian nama pada interface ethernet dan gre tunnel, berikut hasil print dari script console;

```
[admin@MikroTik-Branch1] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
# NAME TYPE MTU L2MTU MAX-L2MTU
0 R ether1-Wan ether 1500
1 R ether2-Lokal ether 1500
2 R ether3 ether 1500
3 R ether4 ether 1500
4 R ether5 ether 1500
5 R ether6 ether 1500
6 R ether7 ether 1500
7 R ether8 ether 1500
8 R gre-to-HO gre-tunnel 1476 65535
```

Memberikan ip address pada interface fisik (ether1-2), interface virtual (gre-to-HO) berikut hasil print script consolnya;

```
[admin@MikroTik-Branch1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 10.1.1.2/24 10.1.1.0 ether1-Wan
1 172.16.1.2/30 172.16.1.0 gre-to-HO
2 192.168.2.1/24 192.168.2.0 ether2-Lokal
```

Setting ip route dengan script console hasilnya di print berikut;

```
[admin@MikroTik-Branch1] > 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 A S 0.0.0.0/0 10.1.1.1 1
1 ADC 10.1.1.0/24 10.1.1.2 ether1-Wan 0
2 ADC 172.16.1.0/30 172.16.1.2 gre-to-HO 0
3 ADC 192.168.2.0/24 192.168.2.1 ether2-Lokal 0
4 A S 192.168.3.0/24 172.16.1.1 1
5 A S 192.168.4.0/24 172.16.1.1 1
6 A S 192.168.5.0/24 172.16.1.1 1
```

Setting nat dengan action masquerade, berikut hasil print script console nya;

```
[admin@MikroTik-Branch1] > ip firewall nat print
```

```
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade to-addresses=0.0.0.0 out-interface=ether1-Wan
```

```
[admin@MikroTik-Branch1] > ip dns print
```

```
servers: 10.1.1.1
dynamic-servers:
allow-remote-requests: yes
max-udp-packet-size: 4096
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 11KiB
```

Konfigurasi server dhcp dan pool pada ether2-Lokal, berikut hasil print script consolnya;

```
[admin@MikroTik-Branch1] > ip dhcp-server print
Flags: X - disabled, I - invalid
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP
0 dhcp1 ether2-Lokal dhcp_pool1 1h
```

```
[admin@MikroTik-Branch1] > ip pool print
# NAME RANGES
0 dhcp_pool1 192.168.2.2-192.168.2.254
```

3. Konfigurasi pada Mikrotik-Branch2

Pemberian nama pada interface ethernet dan gre tunnel, berikut hasil print dari script console;

```
[admin@MikroTik-Branch2] > interface ethernet print
Flags: X - disabled, R - running, S - slave
# NAME MTU MAC-ADDRESS ARP
0 R ether1-Wan 1500 00:00:AB:A7:36:00 enabled
1 R ether2-Lokal 1500 00:00:AB:B1:7A:01 enabled
```

```
[admin@MikroTik-Branch2] > interface gre print
Flags: X - disabled, R - running
0 R name="gre-to-HO" mtu=1476 l2mtu=65535
local-address=0.0.0.0 remote-address=10.1.2.1
dscp=0
```

Memberikan ip address pada interface fisik (ether1-2), interface virtual (gre-to-HO) berikut hasil print script consolenya;

```
[admin@MikroTik-Branch2] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 10.1.2.2/24 10.1.2.0 ether1-Wan
1 172.16.2.2/30 172.16.2.0 gre-to-HO
2 192.168.3.1/24 192.168.3.0 ether2-Lokal
```

Setting ip route dengan script console hasilnya di print berikut;

```
[admin@MikroTik-Branch2] > 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 A S 0.0.0.0/0 10.1.2.1 1
1 ADC 10.1.2.0/24 10.1.2.2 ether1-Wan 0
2 ADC 172.16.2.0/30 172.16.2.2 gre-to-HO 0
3 A S 192.168.2.0/24 172.16.2.1 1
4 ADC 192.168.3.0/24 192.168.3.1 ether2-Lokal 0
5 A S 192.168.4.0/24 172.16.2.1 1
6 A S 192.168.5.0/24 172.16.2.1 1
```

Setting dns untuk resolve domain, berikut hasil print script console nya;

```
[admin@MikroTik-Branch2] > ip dns print
servers: 10.1.2.1
dynamic-servers:
allow-remote-requests: yes
max-udp-packet-size: 4096
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 11KiB
```

Konfigurasi server dhcp dan pool pada ether2-Lokal, berikut hasil print script consolenya;

```
[admin@MikroTik-Branch2] > ip dhcp-server print
```

```
[admin@MikroTik-Branch2] > ip dhcp-server print
Flags: X - disabled, I - invalid
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP
0 dhcp1 ether2-Lokal dhcp_pool1 1h
```

```
[admin@MikroTik-Branch2] > ip pool print
```

```
# NAME RANGES
0 dhcp_pool1 192.168.3.2-192.168.3.254
```

4. Konfigurasi pada Mikrotik-Branch3

Pemberian nama pada interface ethernet dan gre tunnel, berikut hasil print dari script console;

```
[admin@MikroTik-Branch3] > interface ethernet print
Flags: X - disabled, R - running, S - slave
# NAME MTU MAC-ADDRESS ARP
0 R ether1-Wan 1500 00:00:AB:18:A5:00 enabled
1 R ether2-Lokal 1500 00:00:AB:6F:B6:01 enabled
```

```
[admin@MikroTik-Branch3] > interface gre print
Flags: X - disabled, R - running
0 R name="gre-to-HO" mtu=1476 l2mtu=65535
local-address=0.0.0.0 remote-address=10.1.3.1
dscp=0
```

Memberikan ip address pada interface fisik (ether1-2), interface virtual (gre-to-HO) berikut hasil print script consolenya;

```
[admin@MikroTik-Branch3] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 10.1.3.2/24 10.1.3.0 ether1-Wan
1 192.168.4.1/24 192.168.4.0 ether2-Lokal
2 172.16.3.2/30 172.16.3.0 gre-to-HO
```

Setting nat dengan action masquerade, berikut hasil print script console nya;

```
[admin@MikroTik-Branch3] > ip firewall nat print
```

```
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade to-
addresses=0.0.0.0 out-interface=ether1-Wan
```

Setting ip route dengan script console hasilnya di print berikut;

```
[admin@MikroTik-Branch3] > 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 A S 0.0.0.0/0 10.1.3.1 1
1 ADC 10.1.3.0/24 10.1.3.2 ether1-Wan 0
2 ADC 172.16.3.0/30 172.16.3.2 gre-to-HO 0
3 A S 192.168.2.0/24 172.16.3.1 1
4 A S 192.168.3.0/24 172.16.3.1 1
5 ADC 192.168.4.0/24 192.168.4.1 ether2-Lokal 0
6 A S 192.168.5.0/24 172.16.3.1 1
```

Setting dns untuk resolve domain, berikut hasil print script console nya;

```
[admin@MikroTik-Branch3] > ip dns print
```

```
servers: 10.1.3.1
dynamic-servers:
allow-remote-requests: yes
max-udp-packet-size: 4096
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 11KiB
```

Konfigurasi server dhcp dan pool pada ether2-Lokal, berikut hasil print script consolenya;

```
[admin@MikroTik-Branch3] > ip dhcp-server
print
Flags: X - disabled, I - invalid
# NAME          INTERFACE      RELAY
ADDRESS-POOL    LEASE-TIME ADD-ARP
0 dhcp1        ether2-Lokal   dhcp_pool1
1h
[admin@MikroTik-Branch3] > ip pool print
# NAME          RANGES
0 dhcp_pool1    192.168.4.2-192.168.4.254
```

5. Konfigurasi pada Mikrotik-Branch4

Pemberian nama pada interface ethernet dan gre tunnel, berikut hasil print dari script console;

```
[admin@MikroTik-Branch4] > interface ethernet
print
Flags: X - disabled, R - running, S - slave
# NAME          MTU MAC-ADDRESS  ARP
0 R ether1-Wan  1500 00:00:AB:4C:D6:00 enabled
1 R ether2-Lokal 1500 00:00:AB:34:9B:01 enabled
[admin@MikroTik-Branch4] > interface gre print
Flags: X - disabled, R - running
0 R name="gre-to-HO" mtu=1476 l2mtu=65535
local-address=0.0.0.0 remote-address=10.1.4.1
dscp=0
```

Memberikan ip address pada interface fisik (ether1-2), interface virtual (gre-to-HO) berikut hasil print script consolenya;

```
[admin@MikroTik-Branch4] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS      NETWORK  INTERFACE
0 10.1.4.2/24   10.1.4.0 ether1-Wan
1 192.168.5.1/24 192.168.5.0 ether2-Lokal
2 172.16.4.2/30 172.16.4.0 gre-to-HO
```

Setting nat dengan action masquerade, berikut hasil print script console nya;

```
[admin@MikroTik-Branch4] > ip firewall nat
print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade to-
addresses=0.0.0.0 out-interface=ether1-Wan
```

Setting ip route dengan script console hasilnya di print berikut;

```
[admin@MikroTik-Branch4] > 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 A S 0.0.0.0/0      10.1.4.1
1 ADC 10.1.4.0/24     10.1.4.2     ether1-Wan   0
2 ADC 172.16.4.0/30   172.16.4.2   gre-to-HO    0
3 A S 192.168.2.0/24   172.16.4.1
4 A S 192.168.3.0/24   172.16.4.1
5 A S 192.168.4.0/24   172.16.4.1
6 ADC 192.168.5.0/24   192.168.5.1 ether2-Lokal  0
```

Setting dns untuk resolve domain, berikut hasil print script console nya;

```
[admin@MikroTik-Branch4] > ip dns print
servers: 10.1.4.1
dynamic-servers:
allow-remote-requests: yes
max-udp-packet-size: 4096
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 13KiB
```

Konfigurasi server dhcp dan pool pada ether2-Lokal, berikut hasil print script consolenya;

```
[admin@MikroTik-Branch4] > ip dhcp-server
print
Flags: X - disabled, I - invalid
# NAME          INTERFACE      RELAY
ADDRESS-POOL    LEASE-TIME ADD-ARP
0 dhcp1        ether2-Lokal   dhcp_pool1
1h
```

```
[admin@MikroTik-Branch4] > ip pool print
# NAME          RANGES
0 dhcp_pool1    192.168.5.2-192.168.5.254
```

Pengujian dengan tool ping dan tracert antar mikrotik, dan antar PC-Branch untuk membuktikan bahwa interface virtual gre tunnel berfungsi dengan baik. Melihat routing pada setiap mikrotik, bergantung pada banyak nya network yang akan dilewati. Maka diperoleh dari pengujian adalah :

1. Ping dan dari loopback adapter ke Mikrotik-HO

Test ping ke ip address loopback adapter, hasil nya

```
c:\>ping 192.168.137.1
```

```
Pinging 192.168.137.1 with 32 bytes of data:
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128
Reply from 192.168.137.1: bytes=32 time<1ms TTL=128
```

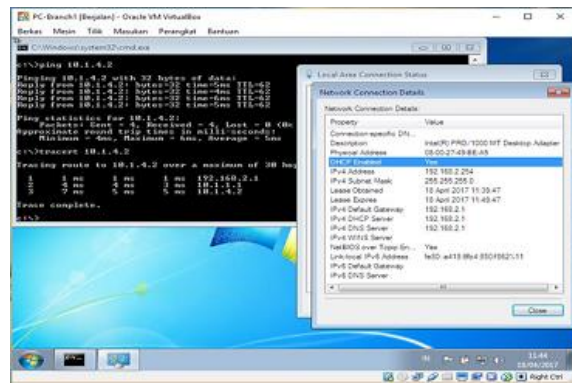
```
Ping statistics for 192.168.137.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Test koneksi dengan tool ping dari loopback adapter ke interface ether1 Mikrotik-Head Office, hasilnya:
c:\>ping 192.168.137.2

```
Pinging 192.168.137.2 with 32 bytes of data:
Reply from 192.168.137.2: bytes=32 time=2ms TTL=64
Reply from 192.168.137.2: bytes=32 time=1ms TTL=64
Reply from 192.168.137.2: bytes=32 time=2ms TTL=64
Reply from 192.168.137.2: bytes=32 time=2ms TTL=64
```

Ping statistics for 192.168.137.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms

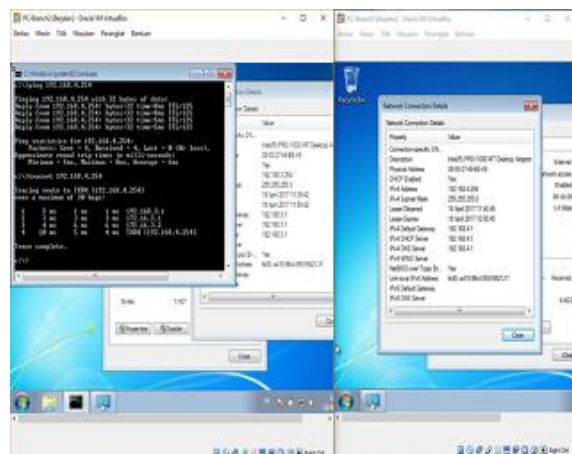
2. Ping dan tracet dari PC-Branch1 ke Mikrotik-Branch4



Sumber: Rahman (2017)
Gambar 2. Test koneksi dari PC-Branch1 ke Mikrotik-Branch4

Pada gambar 2, PC-Branch1 menerima ip address secara otomatis dari dhcp-server Mikrotik-Branch1, kemudian test koneksi berhasil dengan mendapatkan jawaban reply.

3. Ping dan tracet dari PC-Branch2 ke PC-Branch3

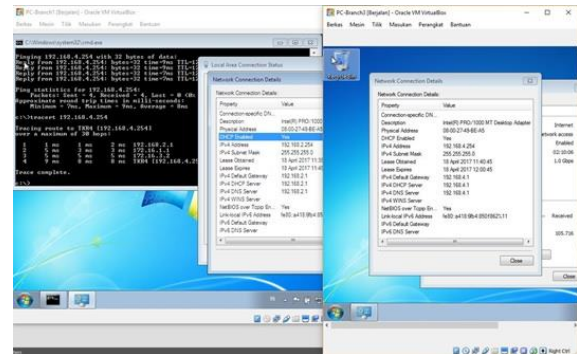


Sumber: Rahman (2017)

Gambar 3. Test koneksi dari PC-Branch2 ke PC-Branch3

Pada gambar 3, PC-Branch2 menerima ip address secara otomatis dari dhcp-server Mikrotik-Branch2 dan PC-Branch3 menerima ip otomatis dari dhcp-server Mikrotik-Branch3, kemudian test koneksi berhasil dengan mendapatkan jawaban reply.

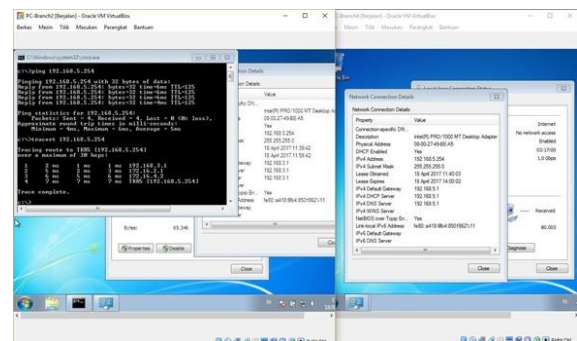
4. Ping dan tracet dari PC-Branch1 ke PC-Branch3



Sumber: Rahman (2017)
Gambar 4. Test koneksi dari PC-Branch1 ke PC-Branch3

Pada gambar 4, PC-Branch1 menerima ip address secara otomatis dari dhcp-server Mikrotik-Branch1 dan PC-Branch3 menerima ip otomatis dari dhcp-server Mikrotik-Branch3, kemudian test koneksi berhasil dengan mendapatkan jawaban reply.

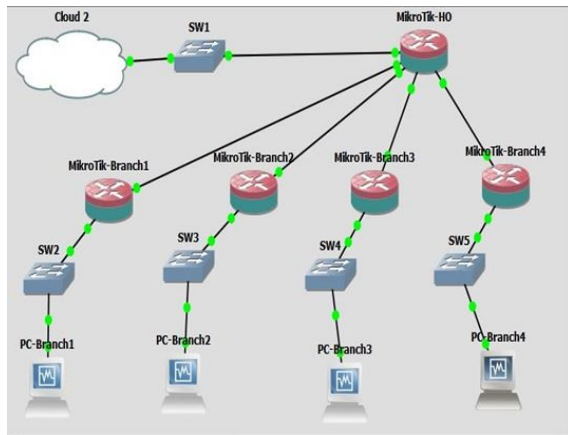
5. Ping dan tracet dari PC-Branch2 ke PC-Branch4



Sumber: Rahman (2017)
Gambar 5. Test koneksi dari PC-Branch2 ke PC-Branch4

Pada gambar 5, PC-Branch2 menerima ip address secara otomatis dari dhcp-server Mikrotik-Branch2 dan PC-Branch4 menerima ip otomatis dari dhcp-server Mikrotik-Branch4, kemudian test koneksi berhasil dengan mendapatkan jawaban reply.

Dengan demikian antar MikroTik-Branch dapat saling berkomunikasi melalui MikroTik-HeadOffice dengan menggunakan interface GRE Tunnel seperti pada gambar 21.



Sumber: Rahman (2017)

Gambar 21. Koneksi Up melalui interface GRE Tunnel

KESIMPULAN

Akhirnya setelah dilakukan persiapan untuk penelitian ini dimulai instal simulator GNS3, mikrotik routerOS, virtualbox, sistem operasi. Administrasi jaringan dengan menuliskan ip address. Konfigurasi pada loopback adapter, MikroTik-HeadOffice, MikroTik-Branch dan Pc-Branch. Setelah terkoneksi terbentuklah interface virtual dan diberikan ip address sebagai ip pengikat dari dua ip publik. Kemudian dibuktikan dengan ping dan tracert antar Pc-Branch dapat saling berhubungan, begitu juga dapat saling melakukan pertukaran data dengan berbagi file sehingga dapat dilakukan mapping drive. Dengan tool Packet Sniffer dan Torch pada Mikrotik dapat melihat trafik yang melewati interface virtual gre tunnel. Setelah melakukan eksperimen dengan aplikasi simulator GNS3 sedemikian rupa dengan script console dan dibuktikan dengan gambar bahwa jaringan vpn dengan interface gre tunnel dapat menghubungkan lebih dari 2 router MikroTik-Branch melalui MikroTik-HeadOffice sebagai backbone jaringan. Dengan dibangun nya jaringan vpn gre tunnel, maka komunikasi data aman karena berada di dalam tunnel meski di jaringan internet. Penelitian selanjutnya, mengkombinasikan GRE Tunnel dengan yang lainnya.

REFERENSI

Ahmed, F., Butt, Z. U., & Siddiqui, U. A. (2016). MPLS based VPN Implementation in a Corporate Environment. *Journal of Information Technology & Software*

Engineering, 6(5), 1-7. doi: 10.4172/2165-7866.1000193

GNS3. (2017). Frequently Asked Questions. Retrieved February 2017, from GNS3: <https://www.gns3.com/software/faq>

Jaha, A. A. (2015, March). Performance Evaluation of Remote Access VPN Protocols on Wireless Networks. *International Journal of Computer and Information Technology*, 04, 201-206. Dipetik March 01, 2017

Krithikaa, M., Priyadharsini, M., & Subha, C. (2016). Virtual Private Network - A Survey. *International Journal of Trend in Research and Development*, 3(1), 78-81.

MikroTik. (2015, December 07). Manual:Interface/Gre. Retrieved March 12, 2017, from WIKI Mikrotik: <https://wiki.mikrotik.com>

Nigam, S., & Gupta, E. N. (2016). Implementation of New IPv6 Tunneling Transition Technique: II6T. *International Journal of Innovative Research in Computer and Communication Engineering*, 4(6), 12128-12132. doi:10.15680/IJIRCCE.2016.0406347

NIXON, D. J., DEVARAJ, D. A., & MOHAMMED, M. A. (2016, Agustus). CONFIGURING IPSEC TO ENCRYPT GRE TUNNELS TO PROVIDE NETWORK LAYER SECURITY FOR NON-IP TRAFFIC SUCH AS IPX USING GNS3. *International Journal of Engineering Science Invention Research & Development*, III(II), 112-119. Dipetik March 02, 2017

Perpusku, A. (2016, June). Metode Penelitian Eksperimental (Pengertian, Karakteristik, & Jenis-jenisnya). Retrieved March 01, 2017, from Perpusku: <http://www.perpusku.com/2016/06/pengertian-karakteristik-jenis-metode-penelitian-eksperimental.html>

Rahman, Taufik. (2017). Laporan Akhir Penelitian Mandiri. Jakarta: AMIK BSI Jakarta