BAB IV

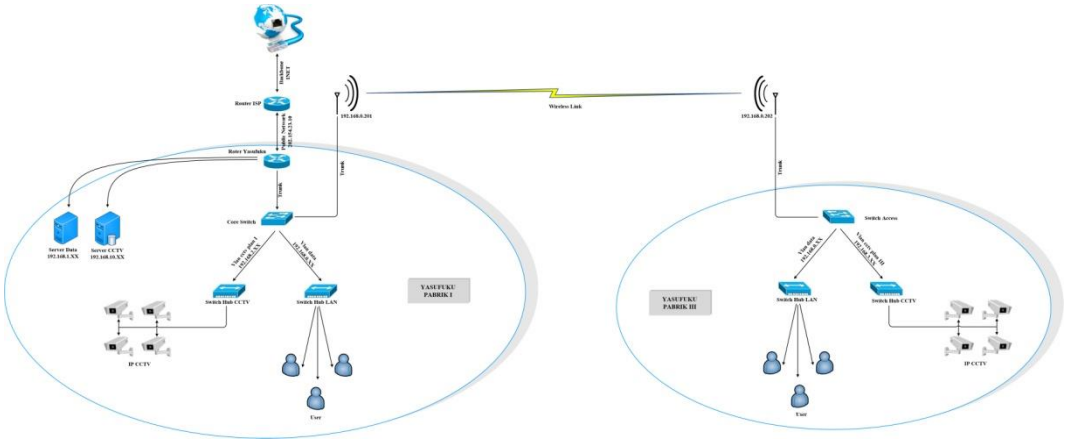
RANCANGAN SISTEM JARINGAN USULAN

4.1. Manajemen Jaringan Usulan

Pada bagian ini penulis membahas manajemen jaringan usulan sebagai penerapan sistem yang akan dibangun. Manajemen jaringan yang akan diusulkan mencakupi topologi jaringan usulan, skema jaringan usulan, perancangan sistem serta keamanan jaringan sebagai solusi dari permasalahan jaringan komputer yang ada pada objek penelitian.

4.1.1. Topologi Jaringan

Penulis mengusulkan untuk tetap menggunakan topologi jaringan *star* seperti jaringan yang sudah berjalan, akan tetapi untuk pengalamatan *IP address* dibagi menjadi beberapa pengalamatan (*network*) dimana *IP address* pada server, *ip camera*, serta jaringan LAN harus dibedakan guna untuk menghindari *collision* yang terjadi pada jaringan komputer yang akan diusulkan. Pada gambar 4.1 adalah topologi jaringan yang akan diusulkan. Dimana ada beberapa perangkat yang ditambahkan pada jaringan komputer usulan seperti penambahan *Mikrotik Router Board RB 1100AHx2* yang sebelumnya hanya menggunakan *Mikrotik Routerboard RB 450* milik ISP (*Internet Service Provider*) agar administrator dapat memegang penuh kendali atas jaringan PT Yasufuku Indonesia dan bukan oleh ISP. Penambahan *switch manageable* HP1810-24V2 yang berfungsi untuk membagi jaringan pada PT Yasufuku Indonesia menjadi beberapa pengalamatan dengan menggunakan VLAN. Berikut ini adalah gambar topologinya.

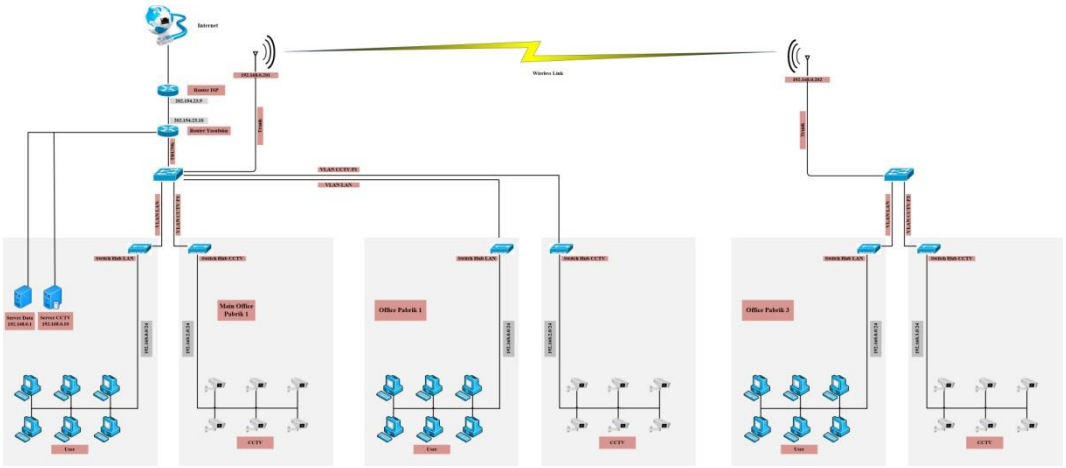


Gambar 4.1 Desain Jaringan Usulan

Terlihat pada gambar 4.1 *server data*, *ip camera* serta jaringan LAN sudah menggunakan pengalamatan yang berbeda, serta memanfaatkan *radio wireless* sebagai koneksi data antara pabrik 1 dengan pabrik 3.

4.1.2. Skema Jaringan

Konsep skema jaringan ini adalah membagi jaringan pada PT Ysufuku Indonesia menjadi beberapa *network* dengan memanfaatkan *Mikrotik Routerboard RB 1100AHx2* sebagai pusat jaringan serta *switch manageable* HP 1810-24V2 sebagai pembagi jaringan menjadi beberapa VLAN.



Gambar 4.2 Skema jaringan usulan

Berdasarkan skema jaringan baru yang telah dibuat pada gambar 4.2 berikut ini adalah sistem pengalamatan yang digunakan.

1. Router ISP

   Ip address : 202.154.23.9

   Subnet Mask : 255.255.255.252

2. Router Yasufuku

   Ip address : eth2 202.154.23.10 subnet 255.255.255.252

   eth3 vlan 30 192.168.0.1 subnet 255.255.255.0

   eth3 vlan 31 192.168.2.1 subnet 255.255.255.0

   eth3 vlan 32 192.168.3.1 subnet 255.255.255.0

   eth4 192.168.1.254 subnet 255.255.255.0

   eth5 192.168.10.1 subnet 255.255.255.0

3. Switch Pabrik 1

   Ip address : 192.168.0.253

   Subnet mask : 255.255.255.0

4. Switch pabrik 3

   Ip address : 192.168.0.254

   Subnet mask : 255.255.255.0

5. PC user pabrik 1 dan pabrik 3

   Ip address : 192.168.0.0 – 192.168.0.254

   Subnet mask : 255.255.255.0

6. CCTV Pabrik 1

   Ip address : 192.168.2.0 – 192.168.2.254

   Subnet mask : 255.255.255.0

7. CCTV Pabrik 3

   Ip address : 192.168.3.0 – 192.168.3.254

   Subnet mask : 255.255.255.0

8. Client VPN

   Alokasi Pengalamatan VPN 192.168.10.253

4.1.3. Keamanan Jaringan

Berdasarkan uraian diatas diperlukan sistem keamanan jaringan yang cukup, metode keamanan jaringan yang akan diusulkan adalah dengan menggunakan metode *blocking port* dimana fitur ini sudah tersedia pada *mikrotik router operating system*, dengan memanfaatkan fitur *blocking port* yang telah tersedia pada *mikrotik* tidak perlu melakukan penambahan perangkat sebagai sistem keamanan jaringannya sehingga lebih efisien. Adapun *port* yang akan diblokir adalah seperti pada table 4.1 berikut ini.

No	No Port	Jenis Port	Keterangan
1	135-139	TCP	Drob Blaster Worm
2	135-139	UDP	Drob Messenger Worm
3	445	TCP	Blaster Worm
4	445	UDP	Blaster Worm
5	593	TCP	Trojan
6	1024-1030	TCP	Worm
7	1080	TCP	Drob My Doom
8	1214	TCP	Worm
9	1363	TCP	Ndm requester
10	1364	TCP	Ndm server
11	1368	TCP	Screen cast
12	1373	TCP	Hromgrafx
13	1377	TCP	Cichlid
14	1433-1434	TCP	Worm
15	2745	TCP	Bagle Virus
16	2283	TCP	Drob Dumaru Y
17	2535	TCP	Drob Beagle
18	2745	TCP	Drob Beagle C-K

19	3127-3128	TCP	Drob My Doom
20	3410	TCP	Drob Backdoor OptixPro
21	4444	TCP	Worm
22	4444	UDP	Worm
23	5554	TCP	Drob Sasser
24	8866	TCP	Drob Beagle B
25	9898	TCP	Drob Dabber A-B
26	10000	TCP	Drob Dumaru Y
27	10080	TCP	Drob My Doom B
28	12345	TCP	Drob NetBus
29	17300	TCP	Drob Kuang2
30	27374	TCP	Drob Sub Severn
31	65506	TCP	Drob Phatboot

Tabel 4.1 Blocking Port

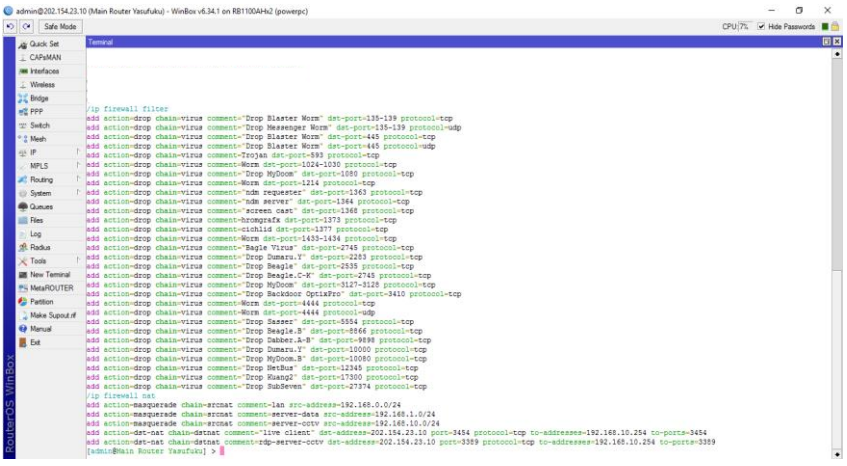
Adapun proses input *script* atau kodenya adalah sebagai berikut, masukkan *script* yang terdapat pada table 4.2 kedalam terminal *mikrotik*, *script* tersebut dapat kita peroleh dari *website* resmi *mikrotik* yang sengaja disediakan oleh *mikrotik* (http://wiki.mikrotik.com/wiki/Protecting_your_customers).berikut ini adalah script tersebut.

```
/ip firewall filter
add chain=virus protocol=tcp dst-port=135-139 action=drop comment="Drop Blaster Worm"
add chain=virus protocol=udp dst-port=135-139 action=drop comment="Drop Messenger Worm"
add chain=virus protocol=tcp dst-port=445 action=drop comment="Drop Blaster Worm"
add chain=virus protocol=udp dst-port=445 action=drop comment="Drop Blaster Worm"
add chain=virus protocol=tcp dst-port=593 action=drop comment="_________"
add chain=virus protocol=tcp dst-port=1024-1030 action=drop comment="_________"
add chain=virus protocol=tcp dst-port=1080 action=drop comment="Drop MyDoom"
add chain=virus protocol=tcp dst-port=1214 action=drop comment="_________"
add chain=virus protocol=tcp dst-port=1363 action=drop comment="ndm requester"
add chain=virus protocol=tcp dst-port=1364 action=drop comment="ndm server"
add chain=virus protocol=tcp dst-port=1368 action=drop comment="screen cast"
add chain=virus protocol=tcp dst-port=1373 action=drop comment="hromgrafx"
add chain=virus protocol=tcp dst-port=1377 action=drop comment="cichlid"
add chain=virus protocol=tcp dst-port=1433-1434 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Bagle Virus"
add chain=virus protocol=tcp dst-port=2283 action=drop comment="Drop Dumaru.Y"
```

```
add chain=virus protocol=tcp dst-port=2535 action=drop comment="Drop Beagle"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Drop Beagle.C-K"
add chain=virus protocol=tcp dst-port=3127-3128 action=drop comment="Drop MyDoom"
add chain=virus protocol=tcp dst-port=3410 action=drop comment="Drop Backdoor OptixPro"
add chain=virus protocol=tcp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=udp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=5554 action=drop comment="Drop Sasser"
add chain=virus protocol=tcp dst-port=8866 action=drop comment="Drop Beagle.B"
add chain=virus protocol=tcp dst-port=9898 action=drop comment="Drop Dabber.A-B"
add chain=virus protocol=tcp dst-port=10000 action=drop comment="Drop Dumaru.Y"
add chain=virus protocol=tcp dst-port=10080 action=drop comment="Drop MyDoom.B"
add chain=virus protocol=tcp dst-port=12345 action=drop comment="Drop NetBus"
add chain=virus protocol=tcp dst-port=17300 action=drop comment="Drop Kuang2"
add chain=virus protocol=tcp dst-port=27374 action=drop comment="Drop SubSeven"
add chain=virus protocol=tcp dst-port=65506 action=drop comment="Drop PhatBot, Agobot, Gaobot"
```

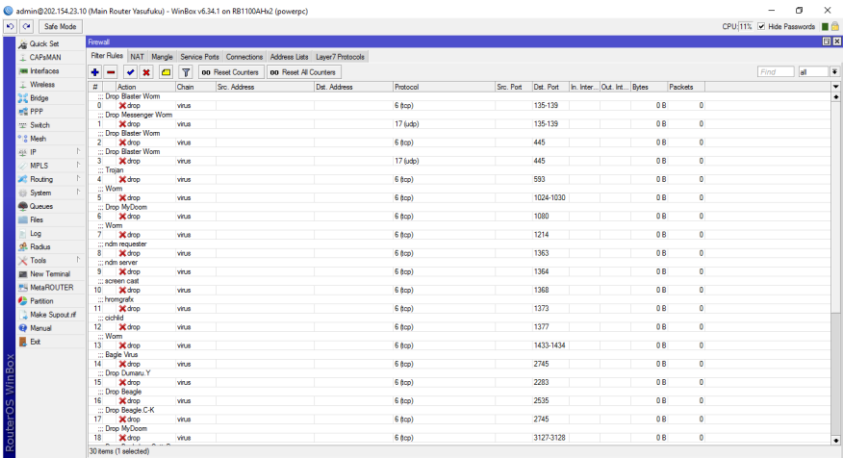
Tabel 4.2 Script Mikrotik Blocking Port

Proses input *scrip* diatas dapat dilakukan seperti pada gambar 4.3. Pertama yang harus dilakukan adalah *login* ke *mikrotik router board* yang akan diisi *script* diatas dengan menggunakan *Mikrotik WinBox Loader*, masuk pada menu *new terminal* kemudian *copy script* diatas kedalam terminal *mikrotik* seperti pada gambar 4.3 dibawah ini.



Gambar 4.3 Proses input script menggunakan terminal mikrotik

Pada gambar 4.4 merupakan hasil dari penambahan script yang telah dilakukan pada gambar 4.3.



Gambar 4.4 Tabel blocking port

Pada gambar 4.4 diatas dapat dilihat paket data melalui *port* apa saja yang sedang berjalan atau digunakan sehingga administrator pada PT Yasufuku Indonesia dapat dengan mudah mendeteksi virus atau malware yang menyerang pada jaringan komputer.

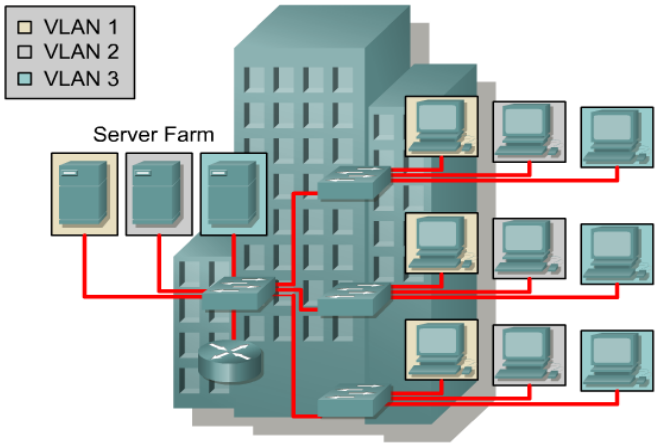
4.1.4. Rancangan Aplikasi

Pada bagian ini penulis akan membahas tentang cara kerja serta konfigurasi jaringan yang diusulkan diantaranya cara kerja dan konfigurasi VLAN, VPN dan *Port forwarding*.

1. Cara Kerja dan Konfigurasi VLAN

   Vlan digunakan untuk *mensegmentasi* berdasarkan *broadcast domain*, tujuan diterapkannya VLAN adalah untuk mengurangi terjadinya *collision* dan mempermudah manajemen jaringan dan security. Setiap VLAN adalah satu broadcast, pada gambar 4.5 Terdiri dari tiga broadcast domain. VLAN dikonfigurasi pada tiap port dari switch, bukan host. Untuk membuat host

menjadi sebuah anggota VLAN, host tersebut harus satu network dengan VLAN.

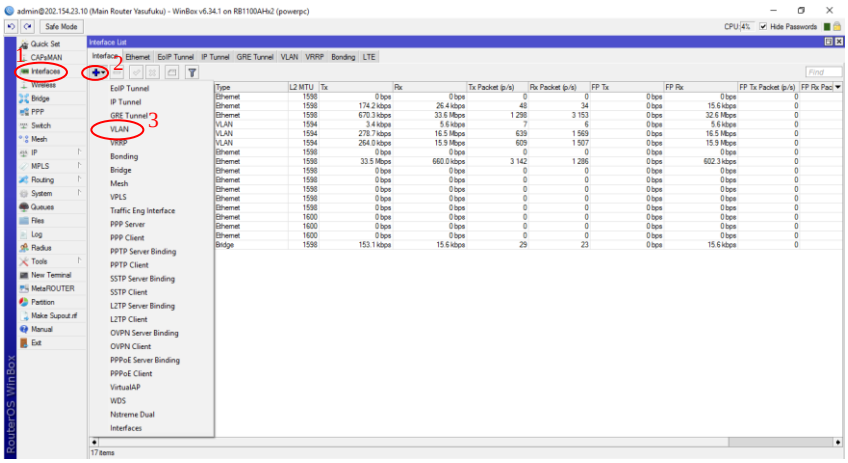


Gambar 4.5 VLAN

Berikuit ini tahap-tahap Instalasi VLAN pada *mikrotik router operating sistem* dan *switch* HP1810-24 V2. Langkah pertama yang harus dilakukan adalah membuka konfigurasi *mikrotik* dengan menggunakan *mikrotik winbox loader*.

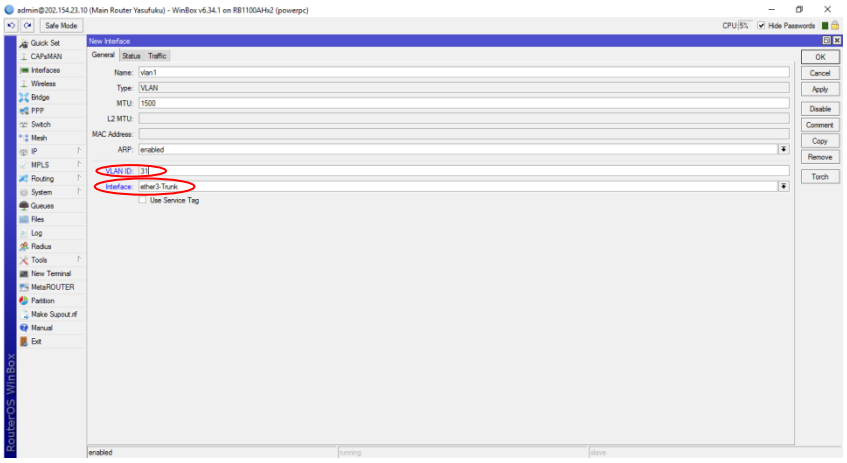
Gambar 4.6 Mikrotik

Pilih menu *interface* klik tanda " + " kemudian pilih VLAN.



Gambar 4.7 Mikrotik VLAN

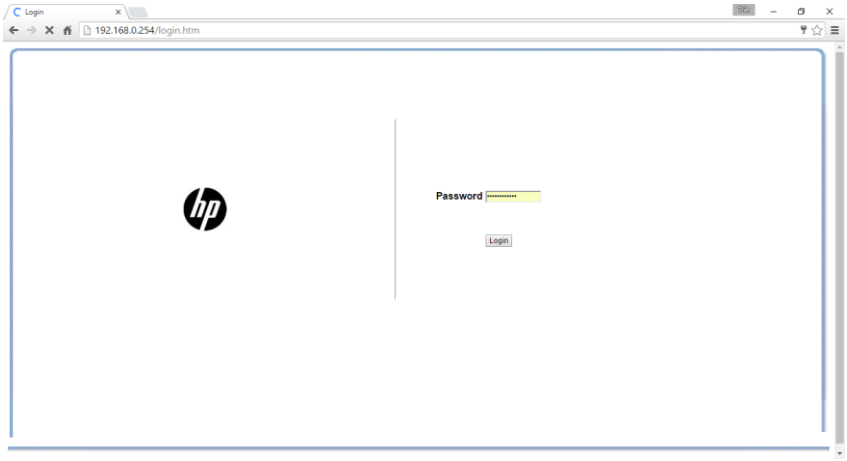
Isikan VLAN ID dan pilih interface yang akan diisi VLAN yang akan dibuat kemudian klik tombol OK.



Gambar 4.8 Konfigurasi VLAN

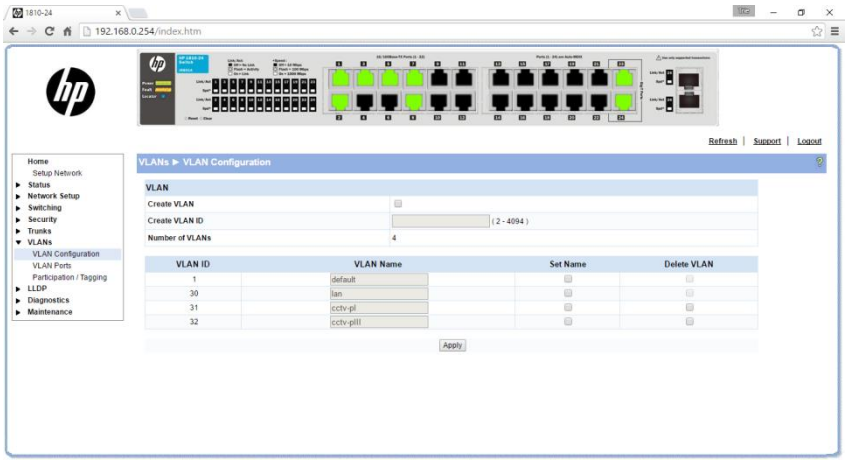
Konfigurasi VLAN pada mikrotik sudah selesai, selanjutnya konfigurasi VLAN pada switch HP1810-24 V2, berikut ini adalah konfigurasi pada switch HP1810-24 V2.

masuk pada menu konfigurasi *switch* dengan menggunakan browser, ketikkan alamat IP address switch kedalam browser tersebut seperti pada gambar 4.9.



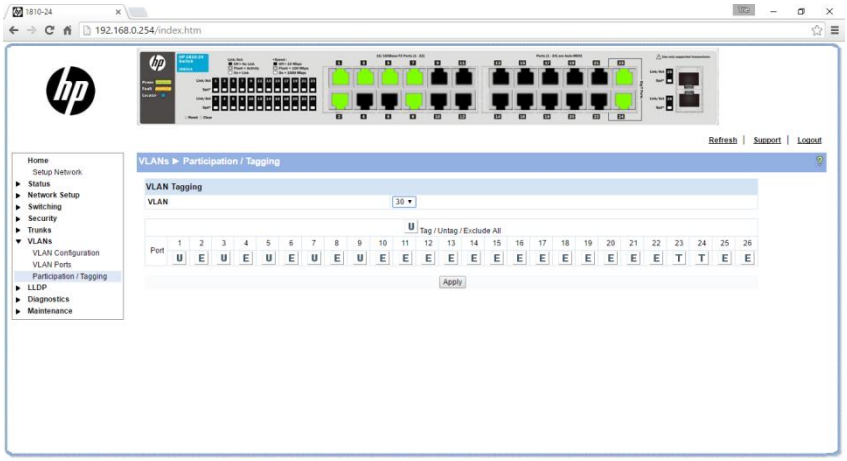
Gambar 4.9 Login page switch HP 1810-24V2

Buka menu *VLANs* dan pilih *VLAN Configuration*, beri tanda ceklist pada *create VLAN*, masukkan VLAN id yang akan dibuat pada pilihan *create VLAN ID*.



Gambar 4.10 Konfigurasi VLAN

Pindah pada menu *Participation / Tagging* pilih VLAN yang sudah dibuat, tentukan *port* mana saja yang akan diberi tanda *Tag*, *Untag*, atau *Exclude*. *Tag* artinya *port* yang dipilih sebagai anggota VLAN, *Untage* artinya *port* yang dipilih sebagai *trunk*, sedangkan *Exclude* artinya *port* yang dipilih tidak menjadi anggota dari VLAN maupun *trunk.*

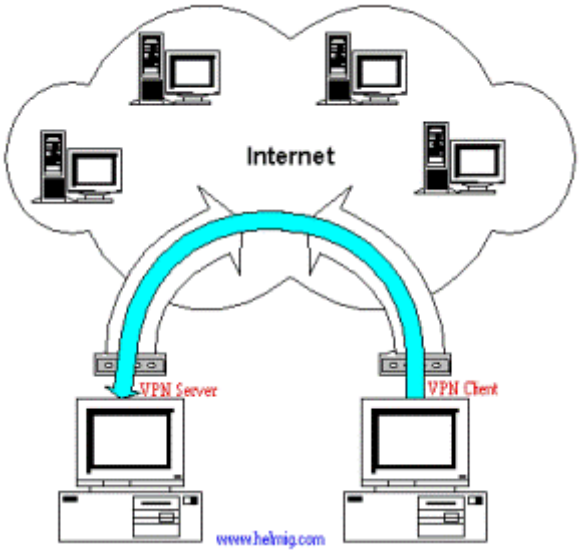


Gambar 4.11 Menu VLAN Participation/Tagging

Pada tahap ini proses konfigurasi VLAN baik pada *mikrotik* maupun pada *switch* sudah selesai dan Vlan sudah dapat digunakan.

2. Cara Kerja dan Konfigurasi VPN

VPN merupakan sebuah koneksi *private* yang melalui jaringan publik (dalam hal ini internet). Virtual berarti jaringan yang terjadi hanya bersifat virtual tidak ada koneksi jaringan secara rill antara dua titik yang akan berhubungan. Private jaringan yang terbentuk hanya bersifat private dimana tidak semua orang bisa mengaksesnya. Data yang dikirim terenkripsi sehingga tetap rahasia meskipun melalui jaringan publik. Dengan VPN kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut dengan *tunnel* (terowongan). Sedangkan *tunneling* adalah suatu cara membuat jalur *private* dengan menggunakan infrastruktur pihak ketiga yaitu PPTP, L2TP, serta IPSec (*internet Protocol Security*) dan protokol yang akan penulis gunakan adalah protokol PPTP.



Gambar 4.12 Cara kerja VPN

Dari gambar 4.12 Secara sederhana cara kerja VPN dengan protokol PPTP adalah sebagai berikut :

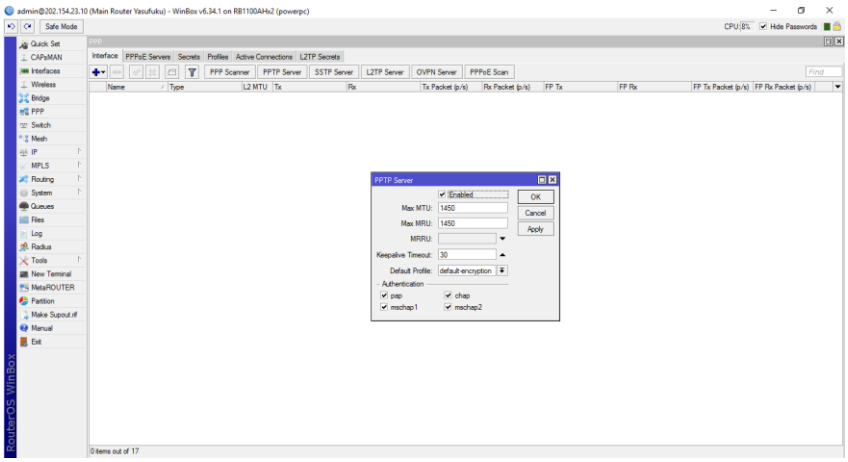
- VPN membutuhkan sebagai sebuah server (dapat berupa PC atau router dalam hal ini RB 1100AHx2) sebagai penghubungnya.
- Untuk memulai sebuah koneksi, komputer dengan aplikasi *VPN Client* mengontak *server* VPN kemudian server VPN memverifikasi username dan password dan apabila berhasil maka VPN server memberikan IP address baru pada komputer *client* dan selanjutnya sebuah koneksi / tunnel akan terbentuk.

Adapun konfigurasi VPN server pada mikrotik adalah sebagai berikut :

Buka konfigurasi *mikrotik* dengan menggunakan *mikrotik winbox loader*.

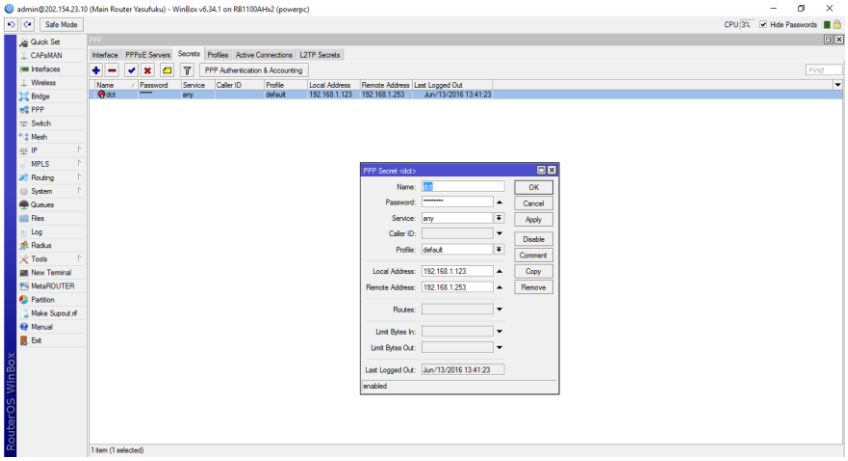
Gambar 4.13 Mikrotik

Pilih menu PPP lalu pilih menu PPTP Server beri tanda ceklist pada pilihan *enable.*



Gambar 4.14 Konfigurasi mikrotik VPN interface

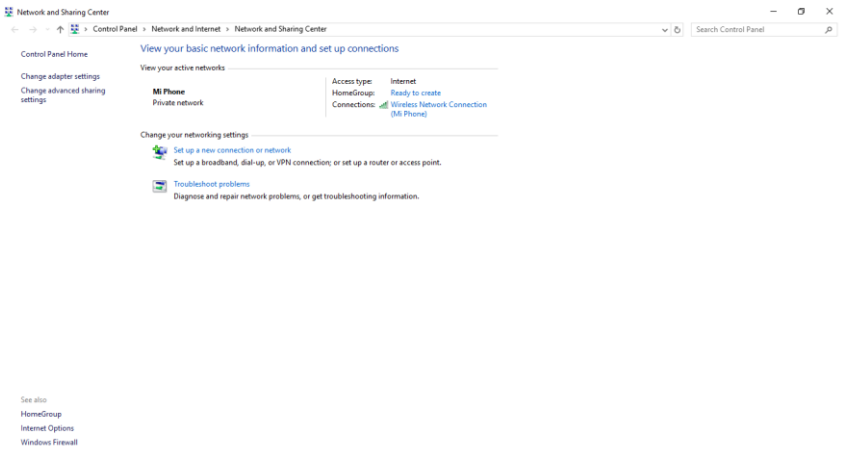
Klik pada tab *Secrets* klik symbol + isikan Name, *Password*, *Local Address*, dan *Remote Address*.



Gambar 4.15 Konfigurasi mikrotik VPN secrets

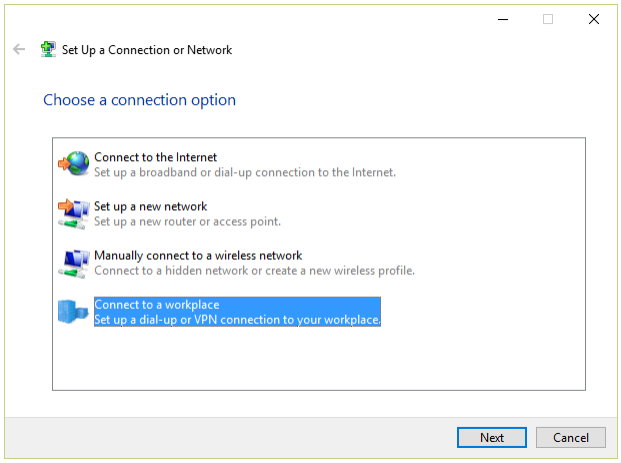
Pada tahap ini VPN sudah dapat kita gunakan, selanjutnya untuk memulai koneksi VPN pada client dapat dilakukan dengan cara sebagai berikut :

Penulis menggunakan sistem operasi Windows 10. Buka *Control Panel* > *Network and Internet* > *Network and Sharing Center* pilih menu *set up a new connection or network*.



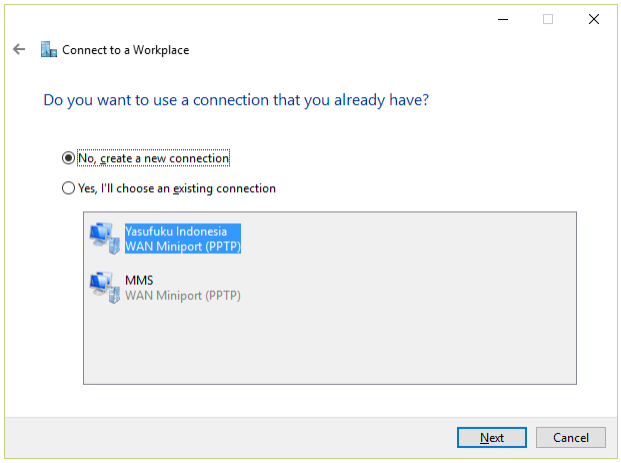
Gambar 4.16 Konfigurasi VPN client

Akan muncul jendela baru pilih *connect to a workplace* kemudian klik tombol *Next*.



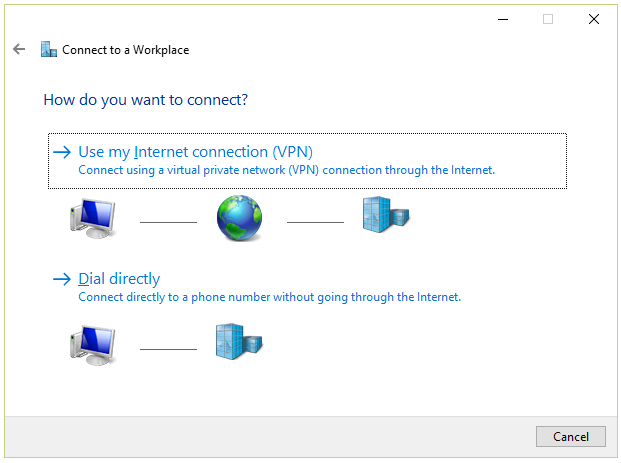
Gambar 4.17 konfigurasi VPN client

Pilih *No, create a new connections* dan klik tombol Next.



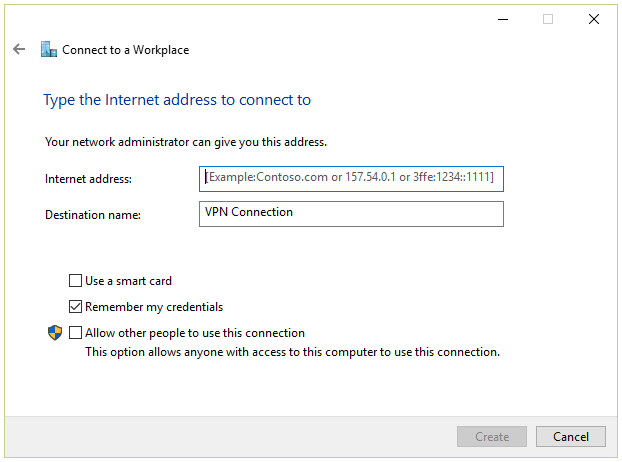
Gambar 4.18 konfigurasi VPN client

Pilih Use my Internet connections (VPN)



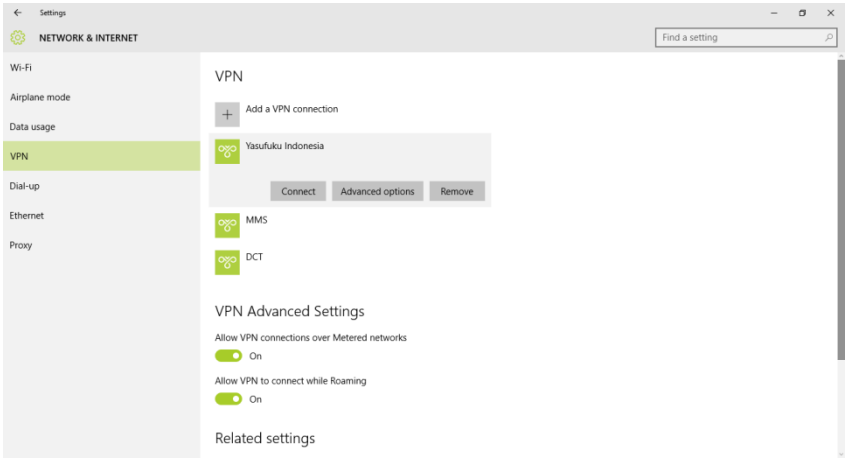
Gambar 4.19 konfigurasi VPN client

Isikan Internet address (IP address pada VPN server) dan Destination name kemudian klik tombol create.



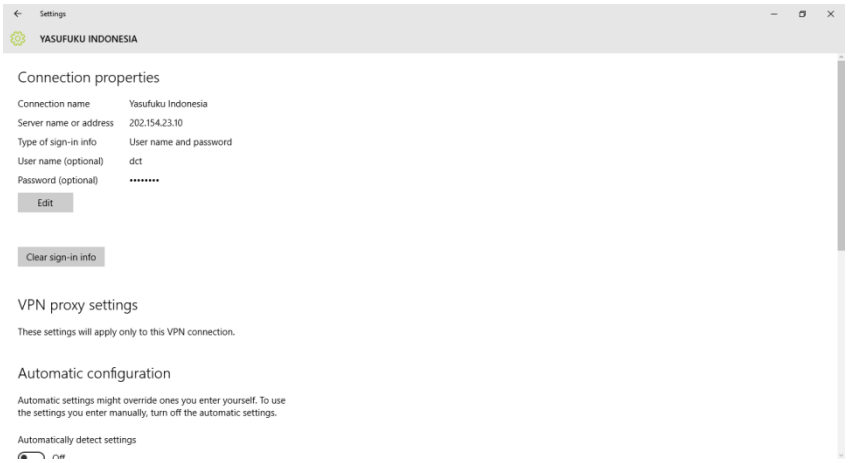
Gambar 4.20 konfigurasi VPN client

Buka menu windows pilih *Setting* > *Network & Internet* > VPN pilih VPN yang telah dibuat klik tombol *Advanced Options*.



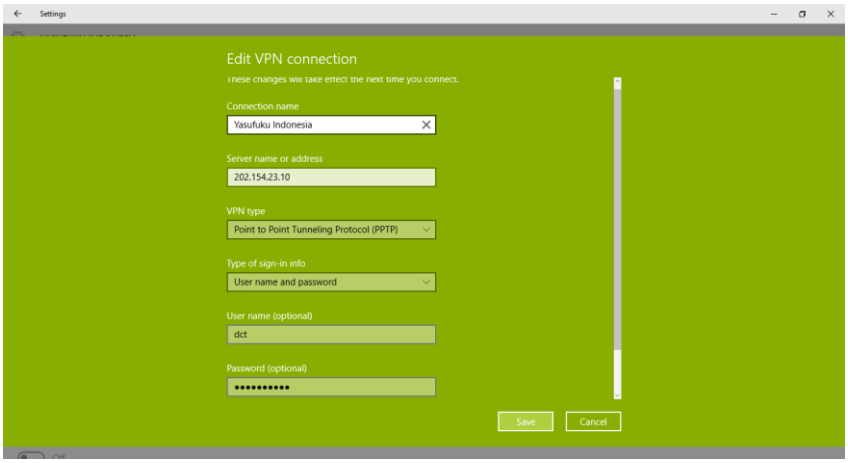
Gambar 4.21 VPN

Klik tombol *Edit* pada menu *Connections properties.*



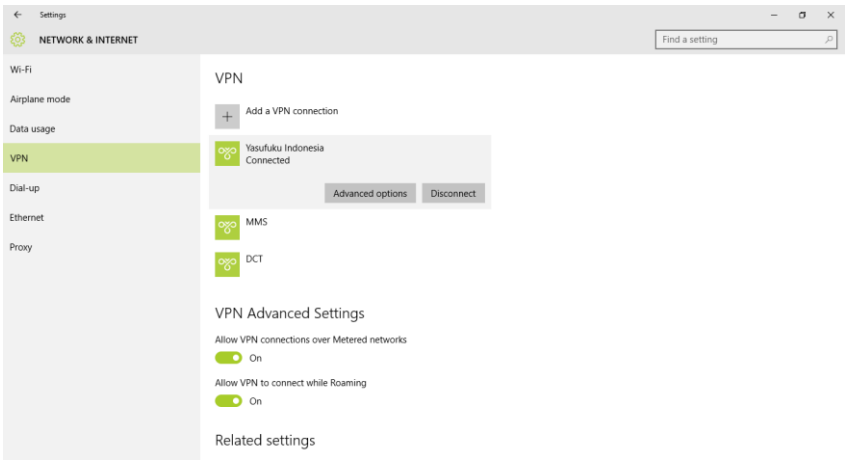
Gambar 4.22 VPN Connection properties

Isi *Connections name* dengan nama *VPN server*, *Server name or address* dengan alamat *IP address VPN server*, pilih *VPN type* dengan *Point to Point Tunneling Protocol (PPTP)*, pilih *Type of sign-in info user name and password*, isikan *username* dan *password* seperti yang sudah dibuat pada *VPN Server*.



Gambar 4.23 konfigurasi VPN client

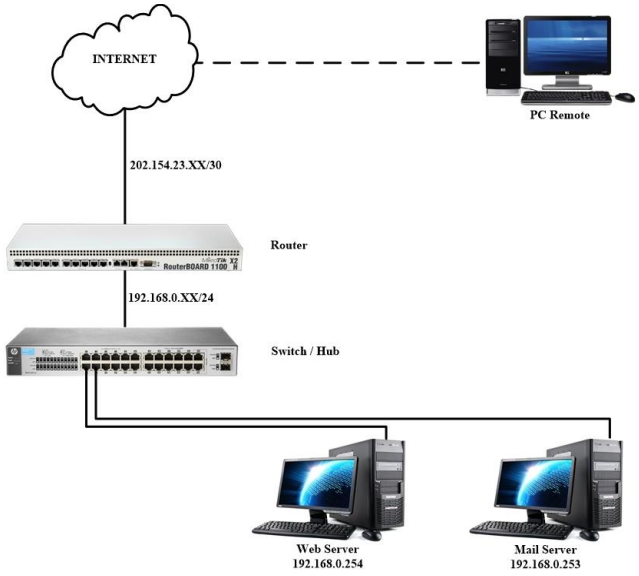
Jika koneksi VPN berhasil terbentuk akan terdapat tanda *connected* pada bagian bawah VPN yang telah dibuat, seperti terlihat pada gambar 4.24 dibawah ini, koneksi VPN sudah dapat dimanfaatkan seperti *file sharing*, *remote desktop*, *printer sharing* dan lain sebagainya.



Gambar 4.24 VPN Connected

3. Cara Kerja dan Konfigurasi *Port Forwarding*.

Secara prinsip *port* forwarding adalah pengalihan (redirect) koneksi dari suatu IP address dengan *port* tertentu ke IP address lain dengan *port* yang sama atau berbeda.



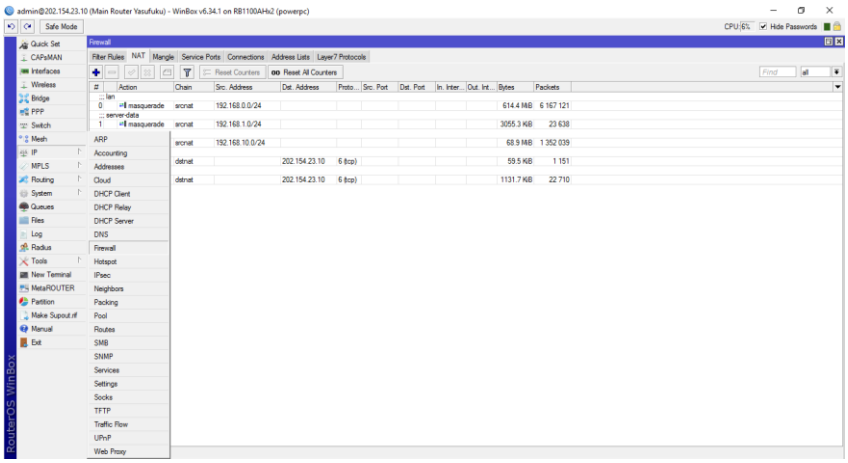
Gambar 4.25 Carakerja port forwarding

Misalkan pada topologi seperti gambar 4.25 diatas, router memiliki satu buah *IP public* dan *server* dengan *IP local* 192.168.0.254, misalkan *server* tersebut berfungsi sebagai *web server* sehingga *port* yang digunakan adalah *port* 80 maka dengan *port forwarding web server* yang berada pada IP local akan dapat diakses melalui *IP public*. Prinsip kerjanya ketika terdapat koneksi ke *IP public* 202.154.23.XX dengan *port* 80 maka akan dialihkan ke *IP local* 192.168.0.254 port 80, *port* ini dapat diubah sesuai dengan kebutuhan. Adapun konfigurasi *port forwarding* pada *mikrotik* sebagai berikut :

Buka konfigurasi *mikrotik* dengan menggunakan *mikrotik winbox loader.*

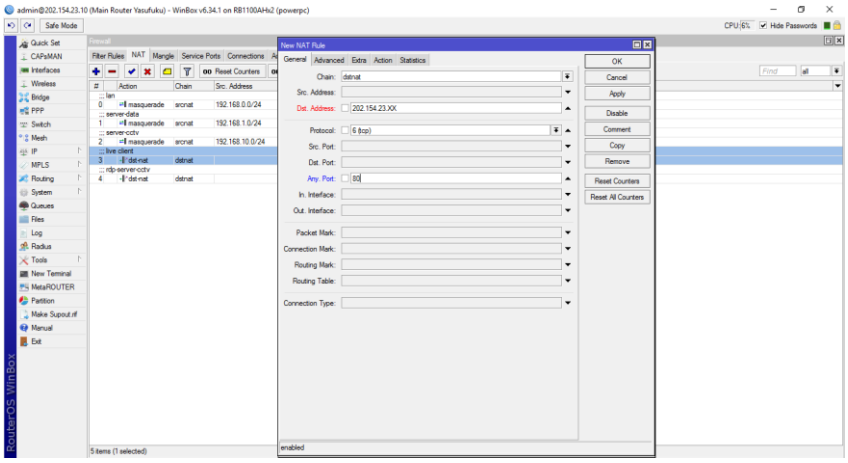
Gambar 4.26 Mikrotik

Pilih menu IP > *Firewall* dan klik pad tab NAT



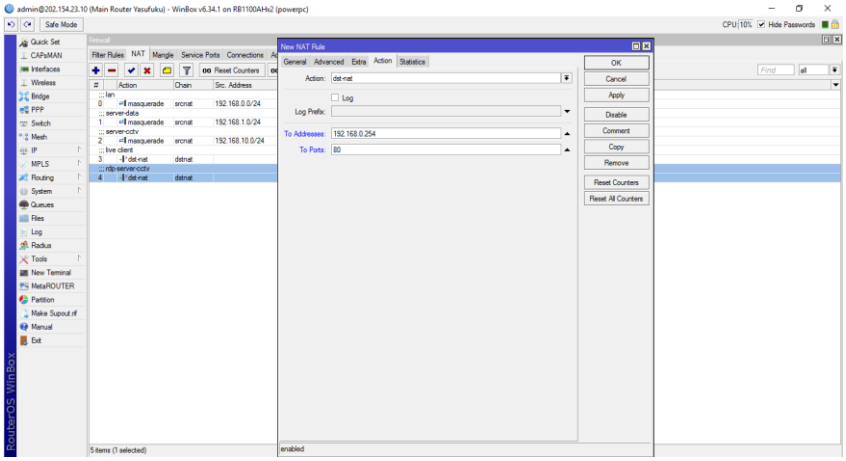
Gambar 4.27 Konfigurasi Firewall

Klik tanda + isikan Chain dstnat, Dst Address 202.154.23.XX (*IP public*), protocol TCP, dan Any *Port* 80.



Gambar 4.28 Firewall NAT

Kemudian masuk ke tab Action, pilih Action dst-nat, To Address 192.168.0.254 (*IP local*), To *Ports* 80. Untuk membuktikan konfigurasi *port forwarding* telah berhasil dapat kita lakukan pengetesan dengan mengakses alamat *IP address* 202.154.23.XX melalui *browser* dari jaringan *internet*. Jika berhasil maka halaman tersebut akan menampilkan halaman website yang telah ditempatkan pada webserver tersebut.



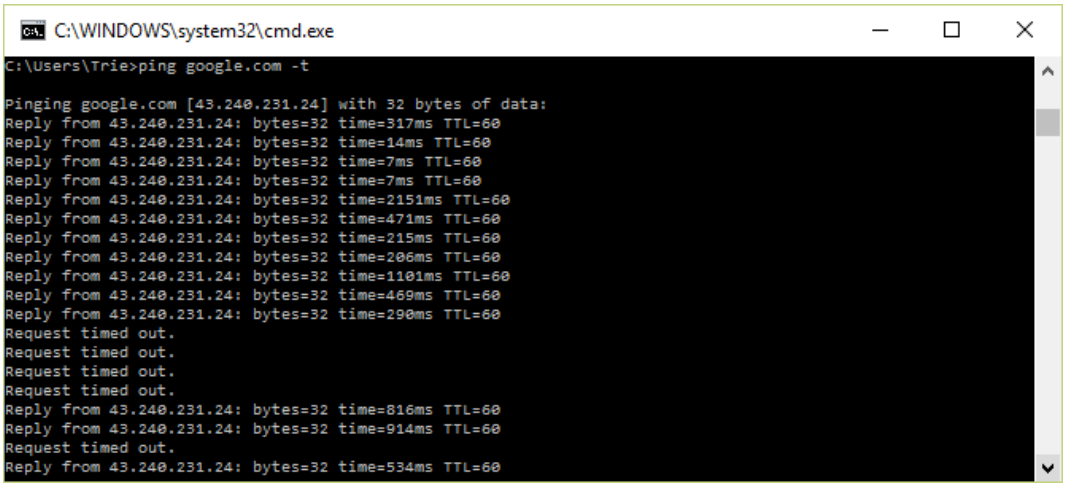
Gambar 4.29 Firewall Action

4.2. Pengujian Jaringan

Pada tahap ini penulis membahas mengenai proses pengujian pada jaringan yang sedang berjalan serta jaringan usulan yang telah diimplementasikan. Pengujian tersebut meliputi tes *ping* pada jaringan berjalan ke *internet* (*google.com*) sedangkan pengujian pada jaringan usulan meliputi tes *ping* ke internet (*google.com*) serta pengetesan *remote server cctv* melalui jaringan *internet*, akses VPN, *remote router mikrotik* melalui jaringan *internet*, serta *remote desktop* ke *server cctv* melalui jaringan *internet*.

4.2.1. Pengujian Jaringan Awal

Pengujian jaringan awal menggunakan *ping ke google.com* hasilnya sangat tidak stabil. Terlihat dalam beberapa kali *ping latency* (jumlah waktu yang dibutuhkan paket data) yang dihasilkan cukup besar, bahkan sampai beberapa kali terjadi *request time out* yang menandakan jaringan komputer sempat terputus beberapa saat.

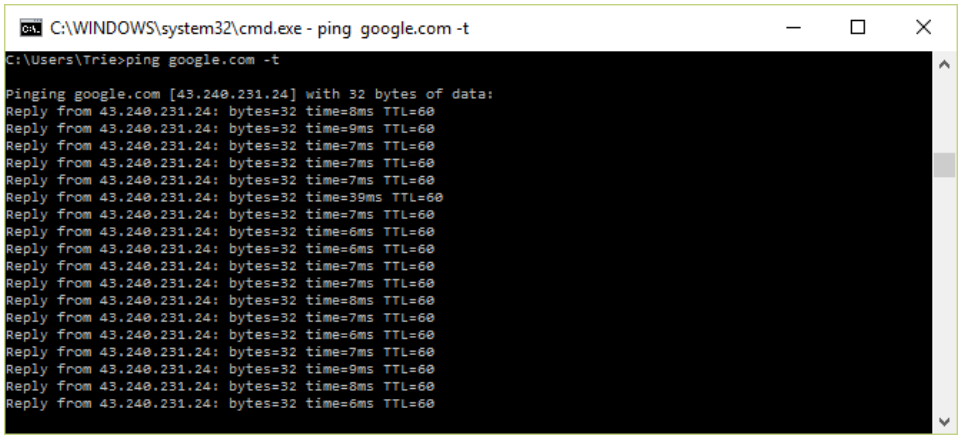


Gambar 4.30 Test ping google.com pada jaringan awal

4.2.2. Pengujian Jaringan Akhir

Pengujian jaringan akhir yang pertama dilakukan dengan cara yang sama pada pengujian jaringan awal yaitu dengan melakukan *ping google.com* agar dapat diketahui berapa besar perubahan yang terjadi. Kemudian dilanjutkan dengan pengujian *remote roueter*, *remote desktop*, dan *remote server* cctv dengan menggunakan sebuah *ip public*, serta dengan melakukan tes akses VPN dari *internet.*

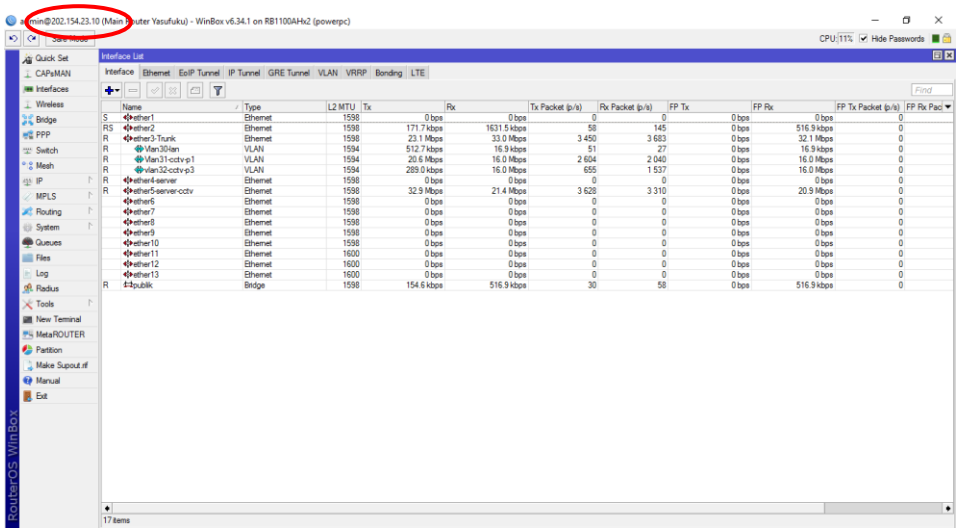
1. Ping google.com



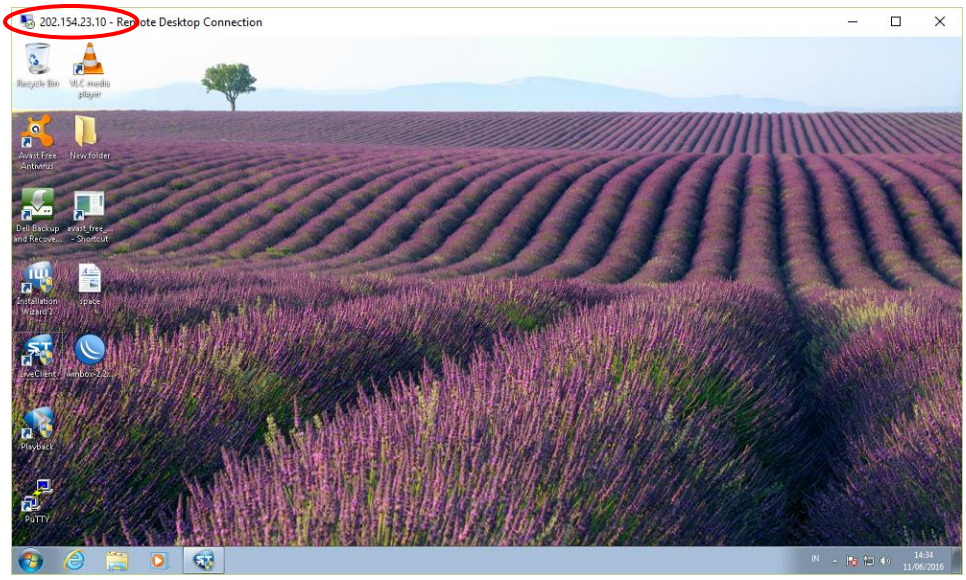
Gambar 4.31 Test ping google.com pada jaringan akhir

Terlihat pada gambar 4.31 hasil pengujian *ping google.com* terlihat lebih stabil daripada saat pengujian jaringan awal, sudah tidak ada lagi *request time out* bahkan *latency* yang dihasilkan jauh lebih baik dari pada saat pengujian jaringan awal.

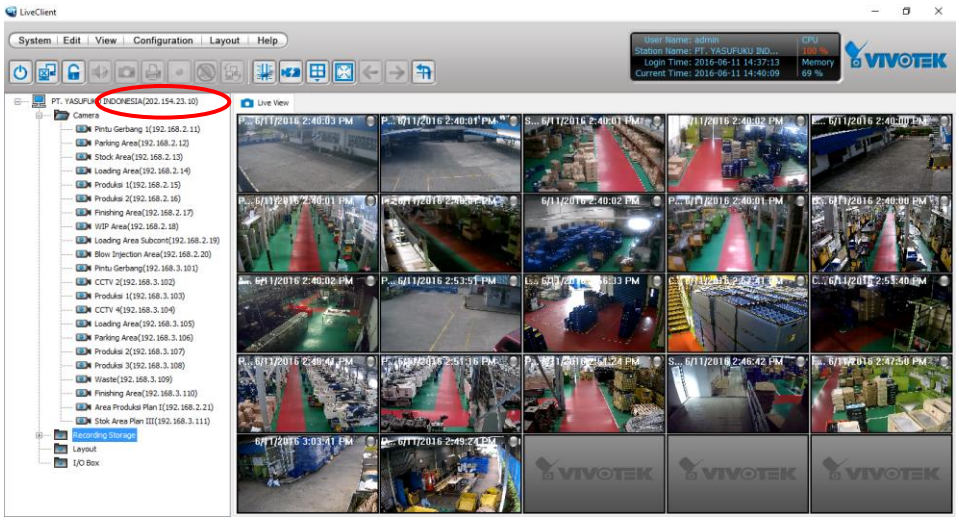
2. Pengujian *Remote Router Mikrotik, Remote Desktop*, serta *Remote Server CCTV* dengan sebuah *ip public.*



Gambar 4.32 Remote Akses Router



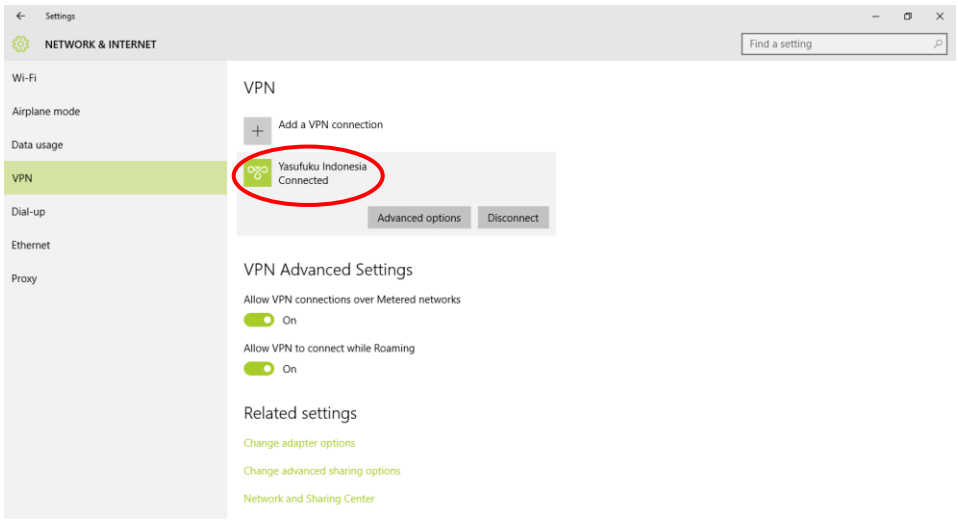
Gambar 4.33 Remote Desktop



Gambar 4.34 Remote Akses Server CCTV

Pada gambar 4.32, gambar 4.33 serta gambar 4.34 terlihat pada tanda lingkaran merah, dengan menggunakan sebuah *ip public* ketiga perangkat tersebut dapat diakses melalui jaringan internet. Hal ini menunjukkan bahwa implementasi *port forwarding* yang dilakukan pada jaringan PT Yasufuku Indonesia telah berhasil.

3. Pengujian Akses VPN



Gambar 4.35 Akses VPN

Pada gambar 4.35 merupakan pengujian akses VPN melalui jaringan internet, terlihat pada gambar yang diberi tanda lingkaran merah menunjukkan status *connected* yang berarti bahwa pengujian akses VPN melalui jaringan internet telah berhasil dilakukan.