

BAB IV

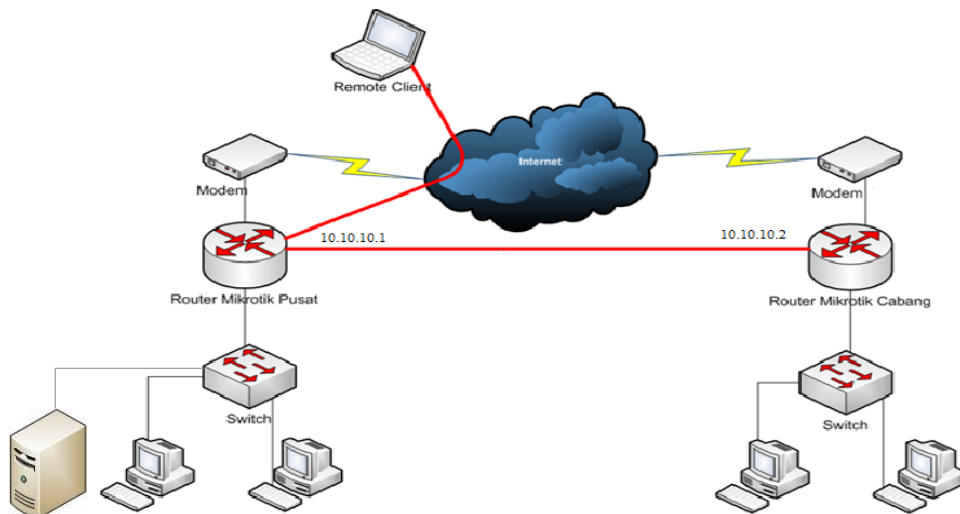
RANCANGAN JARINGAN USULAN

4.1. Jaringan Usulan

Pada bab ini penulis ingin mengajukan jaringan usulan dari apa yang penulis telah analisa sebelumnya setelah riset pada salah satu klien PT. Remala Abadi. Di dalam skripsi ini penulis ingin memberikan jaringan usulan agar kantor cabang dan pusat dapat saling berkomunikasi layaknya seperti dalam satu jaringan.

4.1.1. Topologi Jaringan

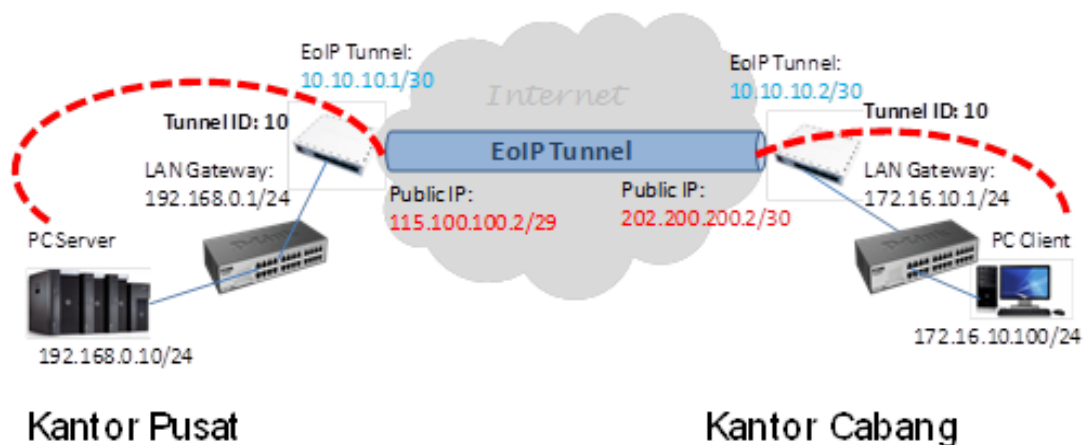
Dalam mengusulkan topologi jaringan yang akan diimplementasikan pada klien PT. Remala Abadi, penulis tidak akan merubah bentuk topologi yang sudah ada, hal ini karena bentuk topologi yang ada sekarang sudah sangat baik. Topologi jaringan kantor pusat dan cabang menggunakan topologi *star*. Penulis mengusulkan untuk menggunakan VPN (*Virtual Private Network*) untuk berkomunikasi atau pertukaran data antar kantor menjadi lebih aman.



Gambar IV.1. Topologi Jaringan Usulan

4.1.2. Skema Jaringan

Pada rancangan jaringan usulan ini, di sisi router kantor pusat yang sudah terkonfigurasi ip publik untuk akses internet 115.100.100.2 dan ip private 192.168.0.1 sebagai *gateway* LAN, maka ditambahkan sebuah konfigurasi baru dengan menambahkan IP *Tunnel* 10.10.10.1/30 pada router Mikrotik. Kemudian di sisi cabang yang sudah terkonfigurasi ip publik untuk internet 202.200.200.2 dan ip private 172.16.10.1 sebagai *gateway* LAN, maka ditambahkan sebuah *tunnel* dengan IP *Tunnel* 10.10.10.2/30. IP *Tunnel* ini nantinya yang akan menghubungkan komunikasi data dari kantor pusat dan kantor cabang melalui jaringan internet.



Gambar IV.2. Skema Jaringan Usulan

4.1.3. Keamanan Jaringan

Untuk keamanan jaringan yang digunakan pada implementasi kali ini kami menggunakan fitur keamanan dengan menggunakan tunneling, Metode tunneling membuat proses transfer data dari satu jaringan ke jaringan lain memanfaatkan jaringan internet secara terselubung (tunneling). Ketika paket berjalan menuju ke node tujuan, paket ini melalui suatu jalur yang disebut tunnel. Dan kami juga

menerapkan *filter rule* pada *firewall* di mikrotik untuk membatasi akses ke server hanya dari ip *address* tertentu.

Dalam juga penulis membedakan jaringan pada kantor pusat dan kantor cabang. Dari sisi kantor pusat, penulis menggunakan Net ID 192.168.0.0/24 dan pada kantor cabang menggunakan Net ID 172.16.10.0/24. Selain itu juga tidak memberlakukan *mode bridge* dikarenakan Net ID Pusat dan Cabang yang berbeda serta menjauhi adanya *broadcast* virus dari cabang ke kantor pusat ataupun sebaliknya. Untuk itu routing dibuat terpisah, yaitu routing ke arah internet dan routing ke arah jaringan LAN kantor.

4.1.4. Rancangan Aplikasi

Untuk menggunakan jaringan VPN dengan menggunakan protokol EoIP maka harus dilakukan konfigurasi pada router kantor pusat dan router cabang salah satu klien PT. Remala Abadi. Tahapannya adalah sebagai berikut :

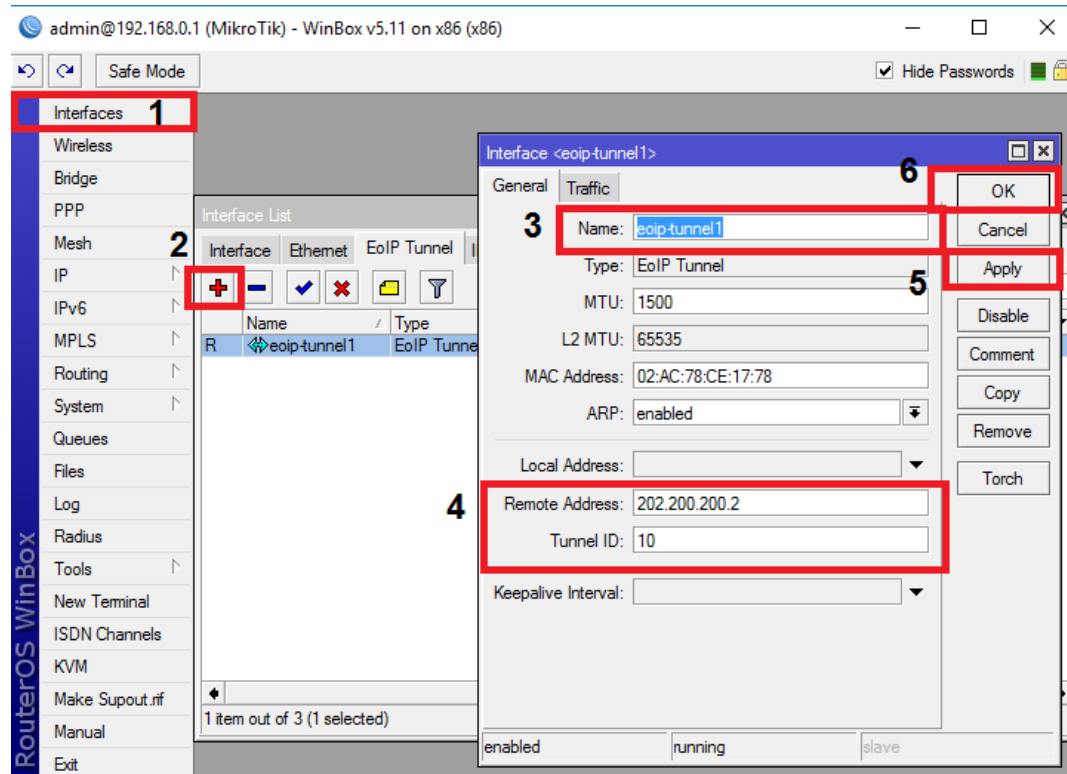
1. Konfigurasi Router Kantor Pusat

Pada sisi router kantor pusat membuat *eoip tunnel*, menambahkan ip *point-to-point* dan menambahkan *routing* ke kantor cabang.

a. Membuat EoIP Tunnel

Untuk membuat EoIP Tunnel langkah-langkahnya adalah sebagai berikut:

- 1) Pada Winbox klik pada menu **Interfaces**, kemudian pilih tab **Add (+)** seperti berikut:

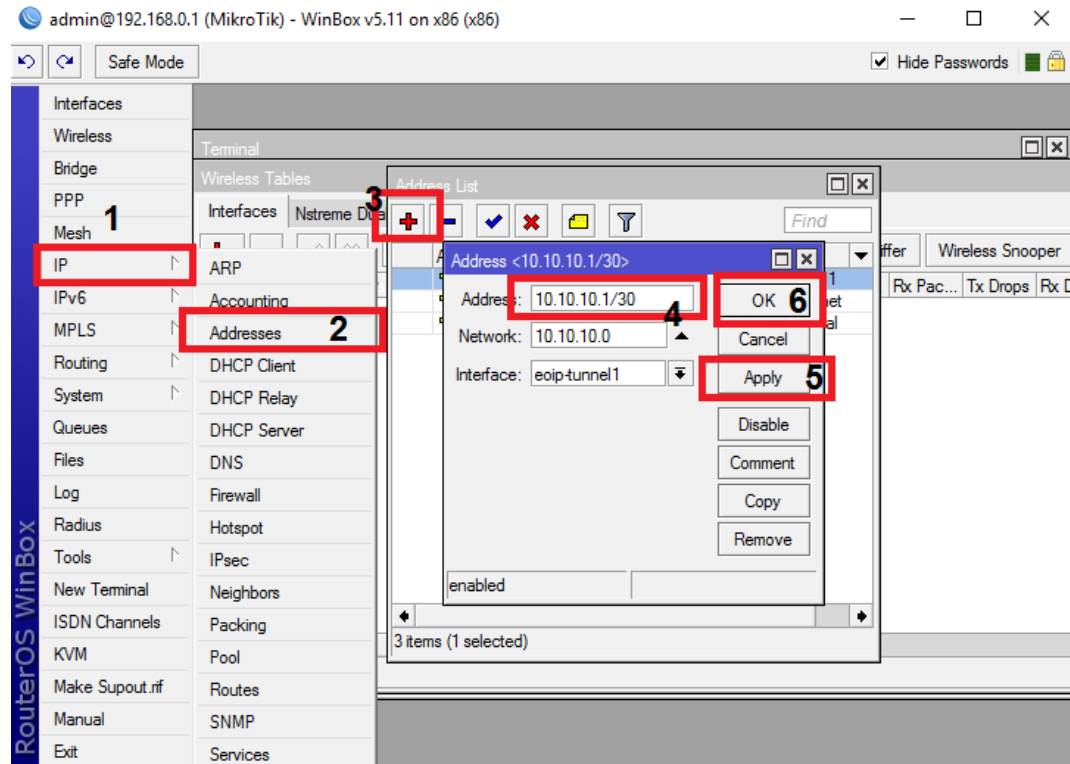


Gambar IV.3 Membuat EoIP Tunnel

- 2) Kemudian isi kolom **Name** dengan **eoiptunnel1**.
- 3) Pada **Remote Address** isikan IP *Public* lawan. Dalam hal ini adalah IP Publik kantor cabang.
- 4) Pada **Tunnel ID** isikan identitas *tunnel* yang akan dibuat. Yaitu 10. *Tunnel ID* ini harus sama dari kedua sisi router. Jika berbeda maka kedua kota tersebut tidak bisa saling berkomunikasi dalam satu jaringan.

b. Menambahkan IP Address EoIP Tunnel

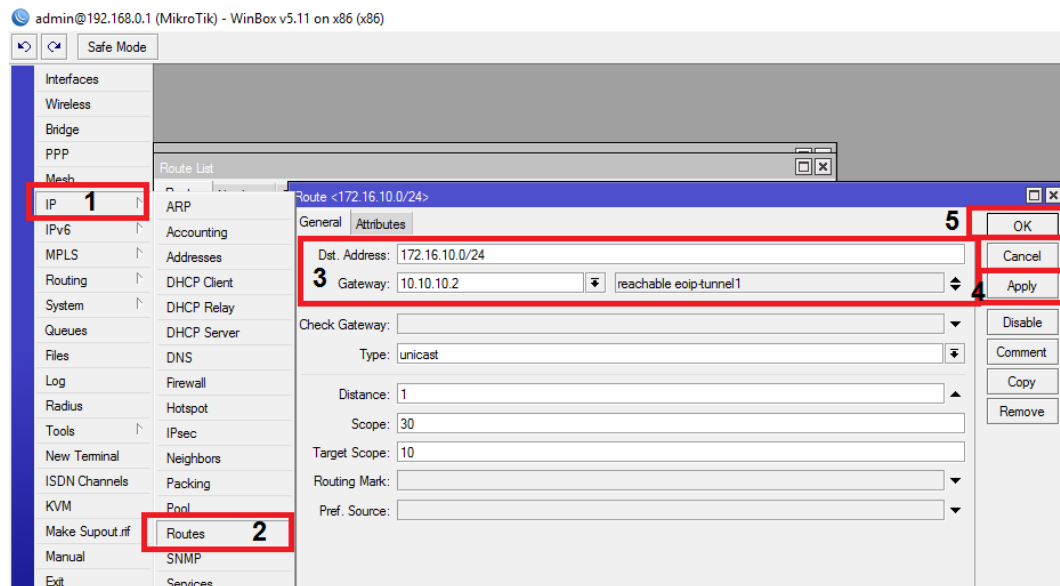
EoIP *tunnel Address* adalah alamat IP Address yang harus dikonfigurasi menjadi *Address tunnel*. Syarat IP Address *eoiptunnel* ini adalah IP harus satu *network* dengan *eoiptunnel Address* yang dikonfigurasi di sisi Cabang.



Gambar IV.4. Menambahkan EoIP Tunnel Address

Langkah-langkah untuk Menambahkan EoIP *Tunnel* Address yaitu:

- 1) Klik Tab **IP** lalu Pilih **Addresses**
 - 2) Isikan **Address** 10.10.10.1/30
 - 3) Pilih **Interface** eoip-tunnel1
 - 4) Lalu **Apply** dan **OK**.
- c. Membuat Routing ke Kantor Cabang
- Agar koneksi antar lokasi dapat terjadi, kita harus melakukan routing ke kantor cabang seperti berikut:
- 1) Pada Tab **IP** pilih **Routes**
 - 2) Pada Tab **General** kita isikan **dst-Address** 172.16.10.0/24
 - 3) Lalu pada **Gateway** eoip-tunnel cabang isikan 10.10.10.2
 - 4) Kemudian isikan klik **Apply** dan **OK**



Gambar IV.5. Membuat Routing ke arah kantor cabang

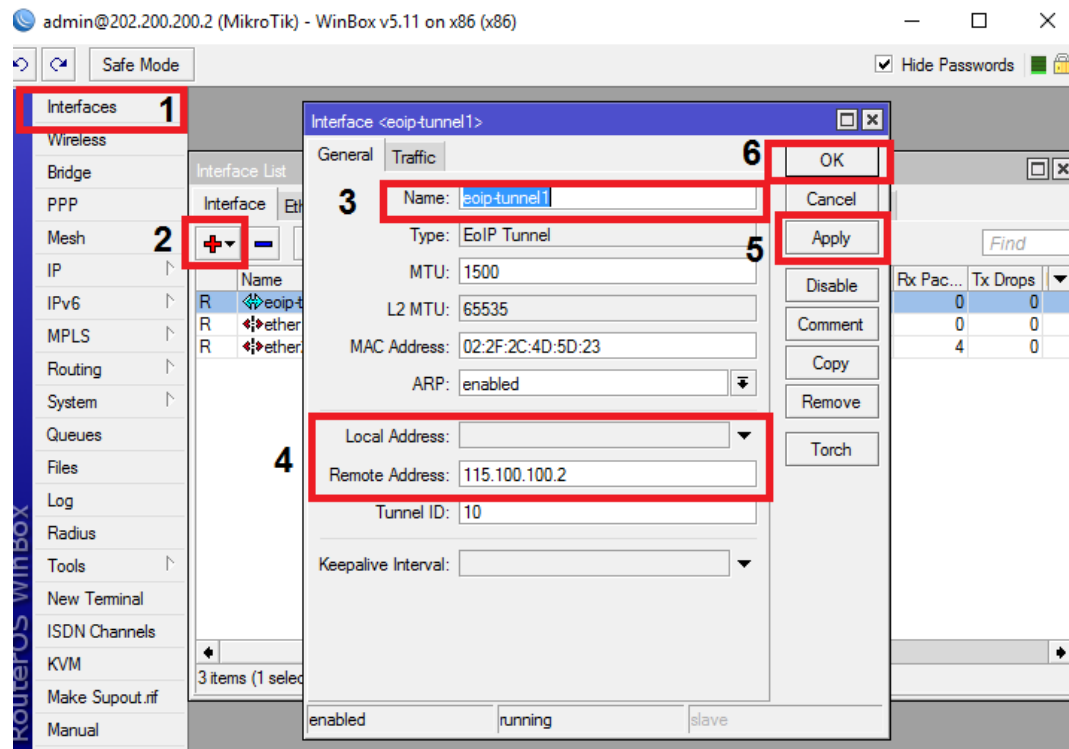
2. Konfigurasi Router Cabang

Untuk dapat memanfaatkan fitur *EoIP Tunnel*. Selain dari sisi kantor pusat, maka router Mikrotik yang berada di kantor cabang juga harus di konfigurasi sebagai berikut:

1) Konfigurasi Interface *EoIP Tunnel* cabang

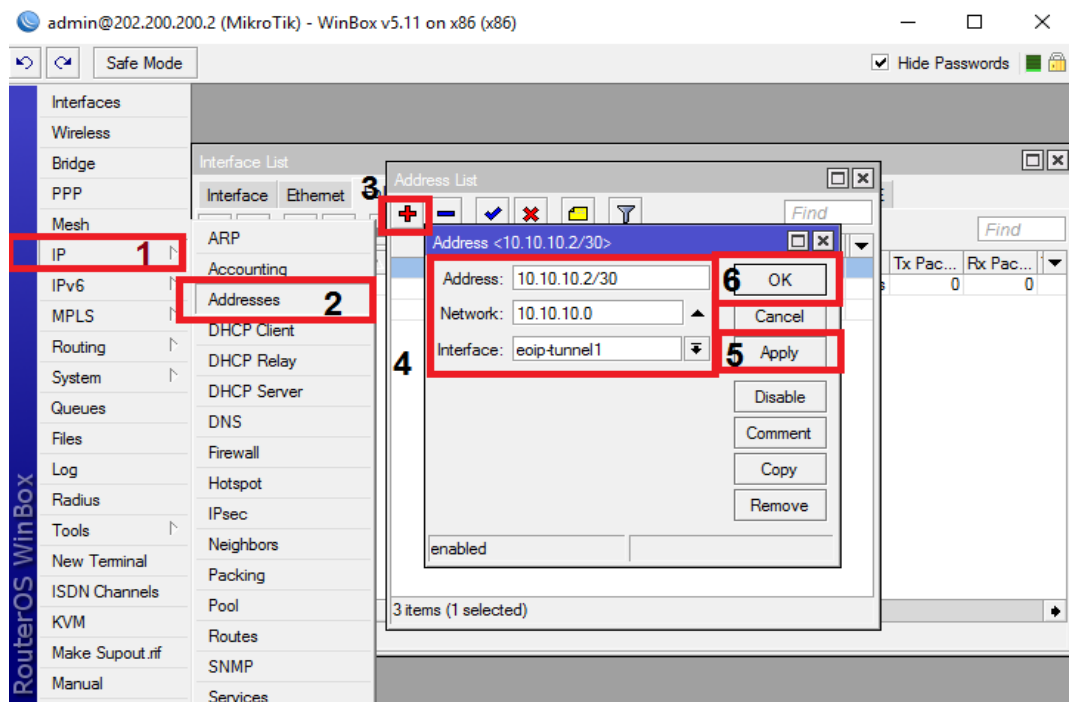
Untuk membuat *EoIP Tunnel* langkah-langkahnya adalah sebagai berikut:

- a. Pada Winbox klik pada menu **Interfaces**, kemudian pilih tab **Add (+)**
 - b. Kemudian centang isi kolom **Name** dengan eoip tunnel1
 - c. Pada **Remote Address** isikan IP *Public* lawan. Dalam hal ini adalah IP *Public* kantor pusat.
 - d. Pada **Tunnel ID** disini isikan identitas *tunnel* yang akan dibuat. Yaitu 10.
- Tunnel ID* ini harus sama dari kedua sisi router. Jika berbeda maka kedua kota tersebut tidak bisa saling berkomunikasi dalam satu jaringan.



Gambar IV.6. Membuat *interface* EoIP Tunnel pada Router Cabang

2) Menambahkan IP Address EoIP Tunnel

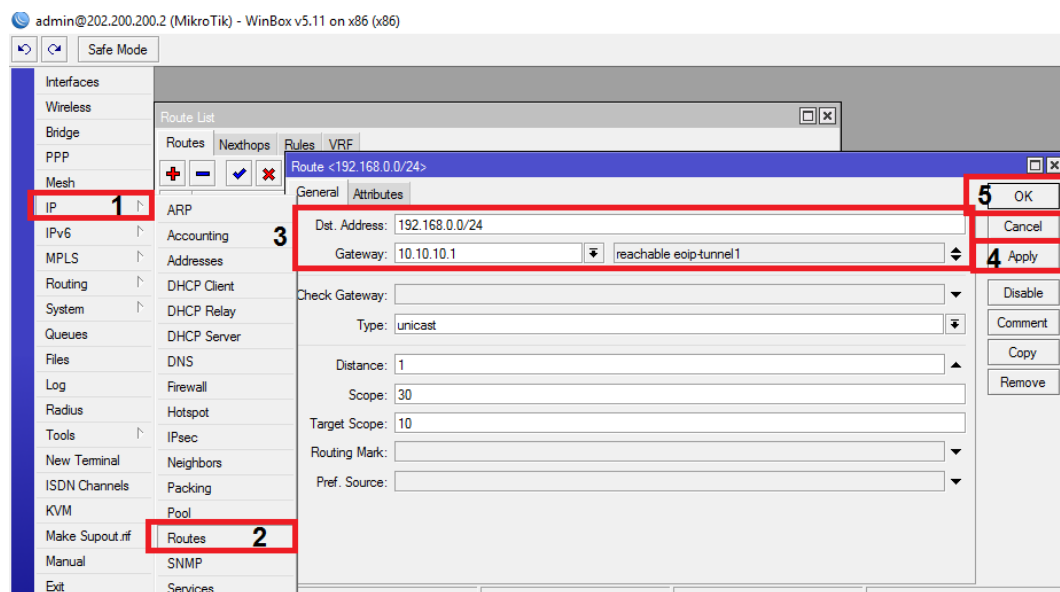


Gambar IV.7. Memberikan EoIP Tunnel Address kantor cabang

Langkah-langkah untuk Menambahkan EoIP *Tunnel* Address yaitu:

- a. Klik Tab **IP** lalu Pilih **Addresses**
- b. Isikan **Address** 10.10.10.2/30
- c. Pilih **Interface** eoip-tunnel1
- d. Lalu **Apply** dan **OK**.

3) Membuat Routing ke kantor pusat



Gambar IV.8. Membuat Routing ke arah kantor pusat

- a. Pada Tab **IP** pilih **Routes**
- b. Pada Tab **General** kita isikan **dst-Address** 172.16.10.0/24
- c. Lalu pada **Gateway eoip-tunnel** cabang isikan 10.10.10.2
- d. Kemudian isikan klik **Apply** dan **OK**

Konfigurasi EoIP *Tunnel* di Mikrotik pada kedua kantor pusat dan kantor cabang telah kita buat. Sekarang kita akan masuk ke tahap pengujian jaringan.

4.1.5. Manajemen Jaringan

Setelah penulis menganalisa sistem jaringan berjalan pada salah satu klien PT. Remala Abadi, maka penulis mengusulkan sebuah jaringan menggunakan VPN (*Virtual Private Network*) dengan menggunakan protokol *Ethernet Over IP* (EoIP) untuk menghubungkan kantor pusat dengan cabang. Dan di fungsikan untuk menjembatani antara kantor pusat dan kantor cabang dengan memanfaatkan koneksi *internet* yang dimiliki tersebut.

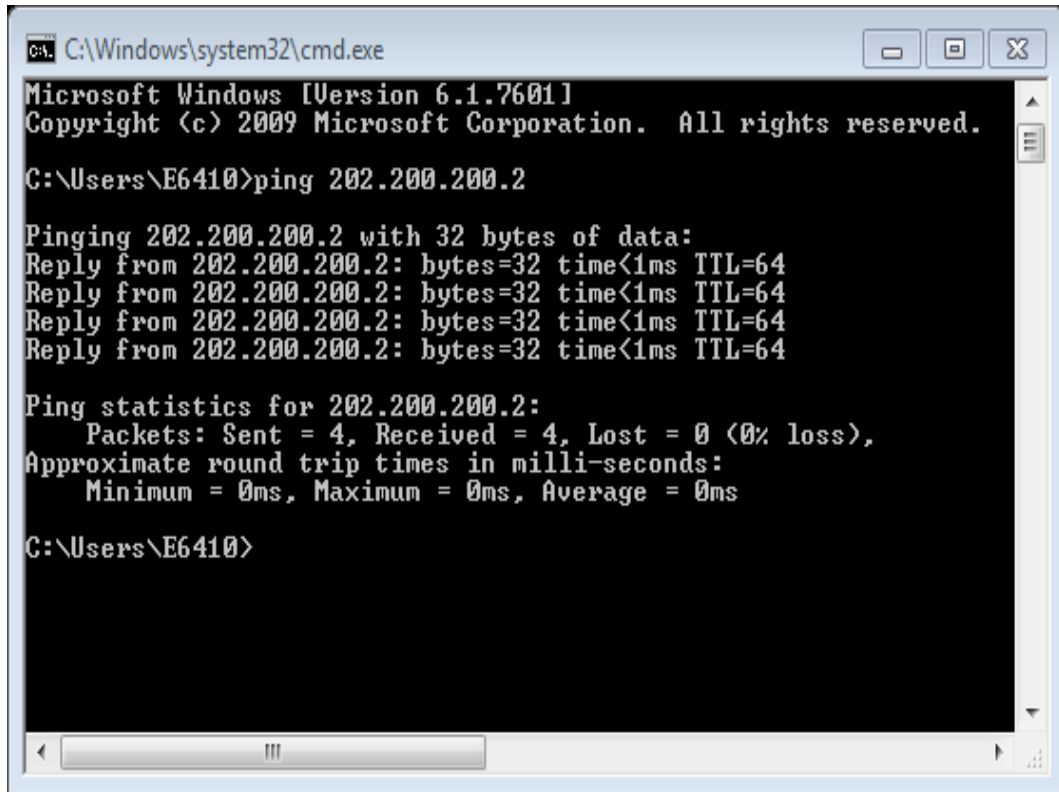
Dengan menggunakan *router* Mikrotik yang sudah ada, kemudian dikonfigurasi untuk menerapkan sistem jaringan VPN baik disisi kantor pusat maupun kantor cabang. Dengan ini antara kantor pusat, kantor cabang dan *remote client* akan lebih mudah untuk melakukan komunikasi, pengiriman data perusahaan serta memonitoring jaringan akan lebih aman.

4.2. Pengujian Jaringan

Pengujian jaringan dilakukan di awal sebelum EoIP Tunnel dibuat dan sesudah EoIP Tunnel dibuat pada konfigurasi diatas. Hasil akhir pengujian yang dilakukan adalah dengan melakukan *traceroute* atau lompatan dari *host* satu ke *host* lainnya. Pengujian dilakukan pada sisi user yang berada di kantor cabang dan kantor pusat.

4.2.1. Pengujian Jaringan Awal

Pada pengujian Awal. Mikrotik harus dapat Akses ke Internet. Pengujian ini dilakukan ketika fitur NAT dan DNS sudah diaktifkan pada Mikrotik. Pengujian dilakukan dengan tes ping ke IP Publik milik kantor cabang dan kantor pusat seperti gambar berikut



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\E6410>ping 202.200.200.2

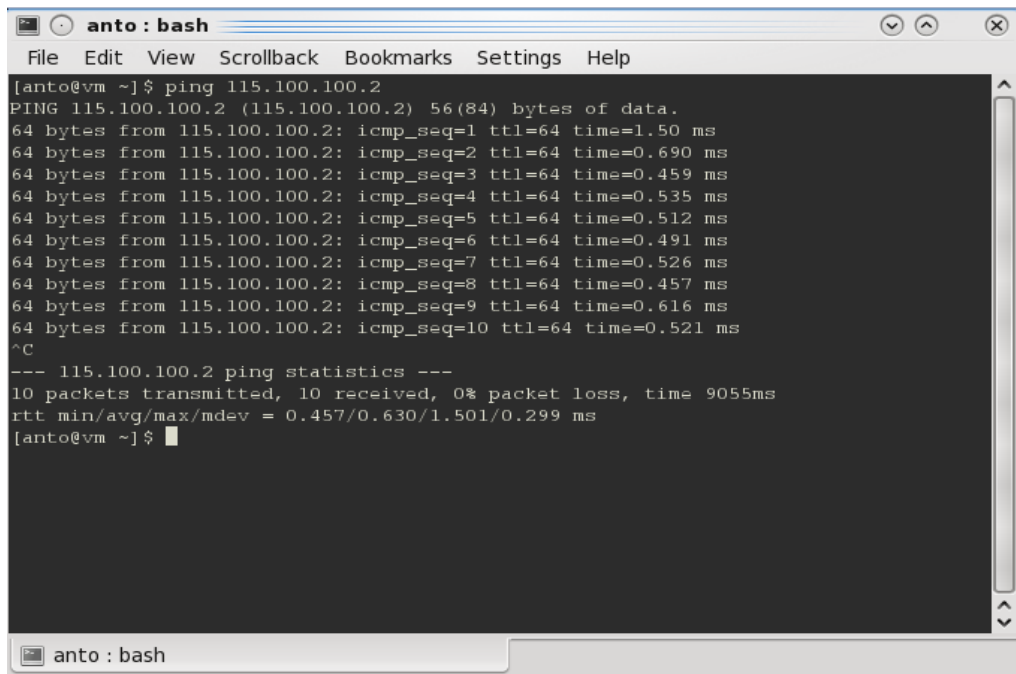
Pinging 202.200.200.2 with 32 bytes of data:
Reply from 202.200.200.2: bytes=32 time<1ms TTL=64
Reply from 202.200.200.2: bytes=32 time<1ms TTL=64
Reply from 202.200.200.2: bytes=32 time<1ms TTL=64
Reply from 202.200.200.2: bytes=32 time<1ms TTL=64

Ping statistics for 202.200.200.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\E6410>

```

Gambar IV.9. Tes ping ke arah IP publik kantor cabang



```

anto : bash
File Edit View Scrollback Bookmarks Settings Help
[anto@vm ~]$ ping 115.100.100.2
PING 115.100.100.2 (115.100.100.2) 56(84) bytes of data.
64 bytes from 115.100.100.2: icmp_seq=1 ttl=64 time=1.50 ms
64 bytes from 115.100.100.2: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 115.100.100.2: icmp_seq=3 ttl=64 time=0.459 ms
64 bytes from 115.100.100.2: icmp_seq=4 ttl=64 time=0.535 ms
64 bytes from 115.100.100.2: icmp_seq=5 ttl=64 time=0.512 ms
64 bytes from 115.100.100.2: icmp_seq=6 ttl=64 time=0.491 ms
64 bytes from 115.100.100.2: icmp_seq=7 ttl=64 time=0.526 ms
64 bytes from 115.100.100.2: icmp_seq=8 ttl=64 time=0.457 ms
64 bytes from 115.100.100.2: icmp_seq=9 ttl=64 time=0.616 ms
64 bytes from 115.100.100.2: icmp_seq=10 ttl=64 time=0.521 ms
^C
--- 115.100.100.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9055ms
rtt min/avg/max/mdev = 0.457/0.630/1.501/0.299 ms
[anto@vm ~]$

```

Gambar IV.10. Tes ping ke IP Publik kantor pusat

```

C:\Windows\system32\cmd.exe
C:\Users\E6410>
C:\Users\E6410>
C:\Users\E6410>ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:
Reply from 115.100.100.1: Destination net unreachable.
Reply from 115.100.100.1: Destination net unreachable.
Reply from 115.100.100.1: Destination net unreachable.
Reply from 115.100.100.1: Destination net unreachable.

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\E6410>tracert -d 172.16.10.1

Tracing route to 172.16.10.1 over a maximum of 30 hops

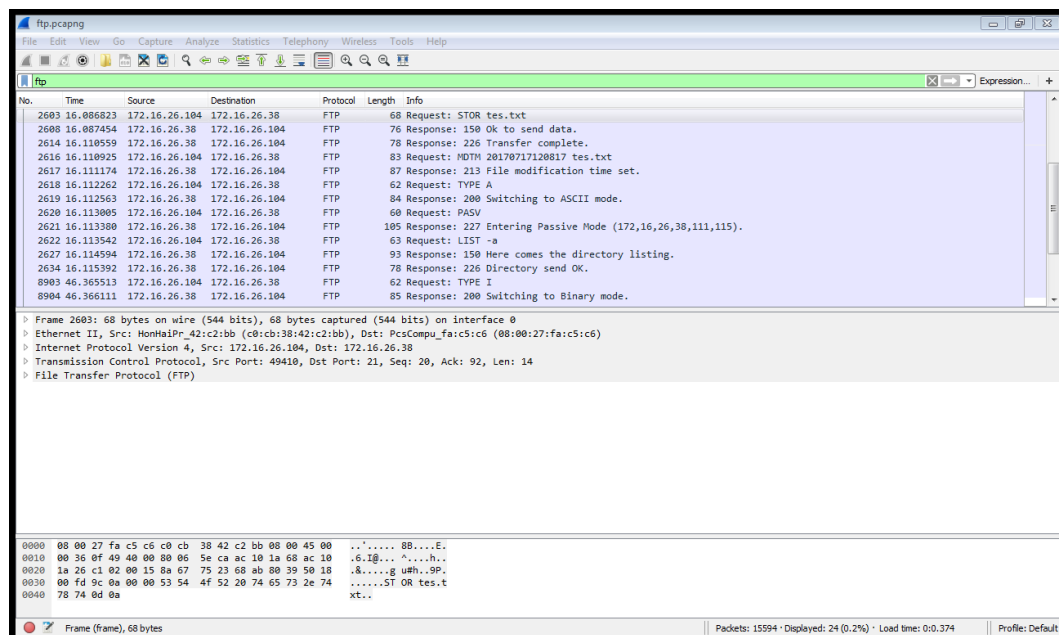
  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2  115.100.100.1  reports: Destination net unreachable.

Trace complete.

C:\Users\E6410>

```

Gambar IV.11. Tes routing ke kantor cabang



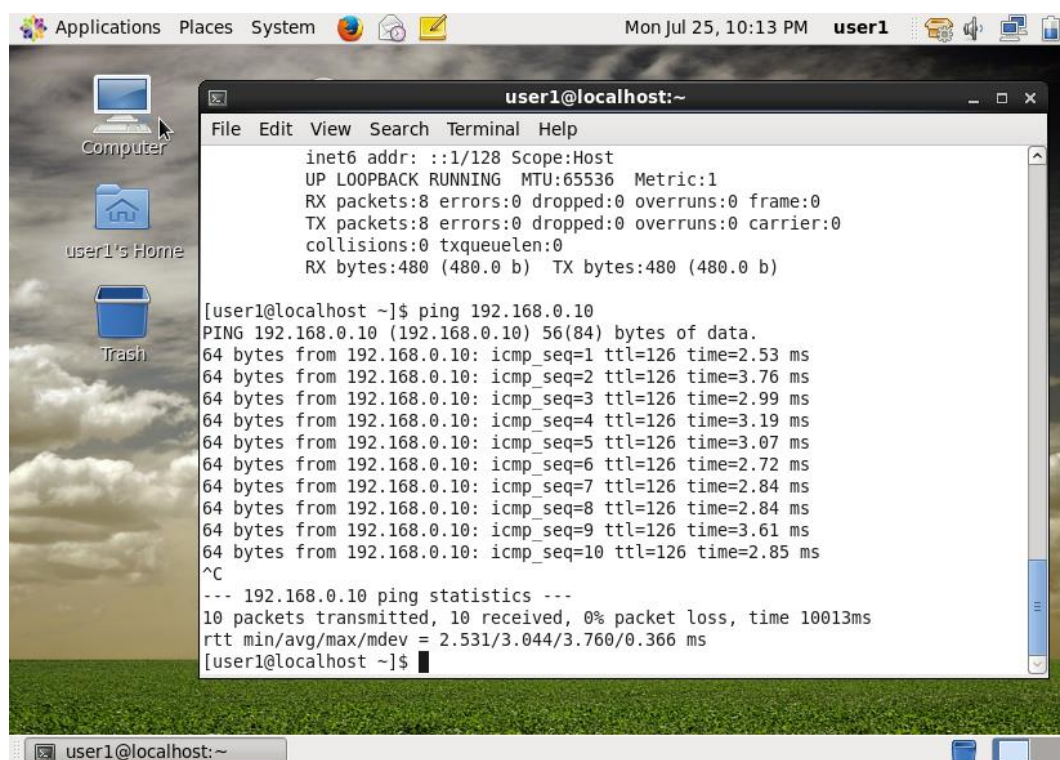
Gambar IV.12. Tes transfer data dengan Wireshark

Pada pengujian jaringan awal dari LAN dilakukan *traceroute* ke arah IP LAN kantor cabang. Hasil dari gambar di atas adalah terdapat pesan “*Destination host unreachable*” artinya *host* tujuan tidak dikenal. Kantor cabang dan kantor

pusat tidak dapat melakukan resource kearah kedua jaringan yang ada dikarenakan tidak adanya routing yang mengarah ke LAN kantor cabang, maka dari itu dibuat konfigurasi seperti di Sub bab 4.1.4. agar jaringan yang berada di belakang mikrotik dapat saling terhubung layaknya satu jaringan.

4.2.2. Pengujian Jaringan Akhir

Pada hasil akhir pengujian jaringan ini dilakukan berdasarkan tes ping dan *traceroute* ke arah kantor pusat dan cabang untuk mengetahui bahwa jalur data yang dikirim baik dari sisi pusat ke cabang atau sebaliknya adalah jalur melalui *gateway eoip tunnel* yang sudah dikonfigurasi sebelumnya.



```

Applications  Places  System  Mon Jul 25, 10:13 PM  user1
Computer
user1's Home
Trash

user1@localhost:~
File Edit View Search Terminal Help
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:8 errors:0 dropped:0 overruns:0 frame:0
TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:480 (480.0 b) TX bytes:480 (480.0 b)

[user1@localhost ~]$ ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=126 time=2.53 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=126 time=3.76 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=126 time=2.99 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=126 time=3.19 ms
64 bytes from 192.168.0.10: icmp_seq=5 ttl=126 time=3.07 ms
64 bytes from 192.168.0.10: icmp_seq=6 ttl=126 time=2.72 ms
64 bytes from 192.168.0.10: icmp_seq=7 ttl=126 time=2.84 ms
64 bytes from 192.168.0.10: icmp_seq=8 ttl=126 time=2.84 ms
64 bytes from 192.168.0.10: icmp_seq=9 ttl=126 time=3.61 ms
64 bytes from 192.168.0.10: icmp_seq=10 ttl=126 time=2.85 ms
^C
--- 192.168.0.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 10013ms
rtt min/avg/max/mdev = 2.531/3.044/3.760/0.366 ms
[user1@localhost ~]$
  
```

Gambar IV.13 Pengujian dengan Ping ke arah LAN kantor pusat

```

C:\Windows\system32\cmd.exe
C:\Users\E6410>ping 172.16.10.100

Pinging 172.16.10.100 with 32 bytes of data:
Reply from 172.16.10.100: bytes=32 time=1ms TTL=61
Reply from 172.16.10.100: bytes=32 time=2ms TTL=61
Reply from 172.16.10.100: bytes=32 time=2ms TTL=61
Reply from 172.16.10.100: bytes=32 time=2ms TTL=61

Ping statistics for 172.16.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\E6410>tracert -d 172.16.10.100

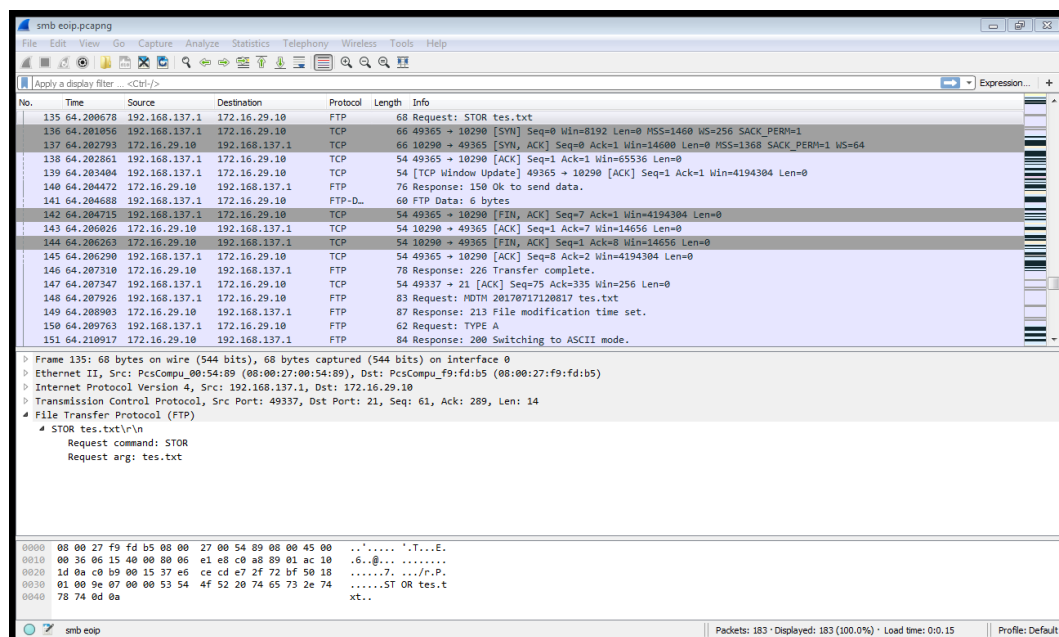
Tracing route to 172.16.10.100 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    192.168.0.1
  1  1 ms     1 ms     1 ms     202.200.200.2
  2  2 ms     2 ms     2 ms     172.16.10.100

Trace complete.

C:\Users\E6410>

```

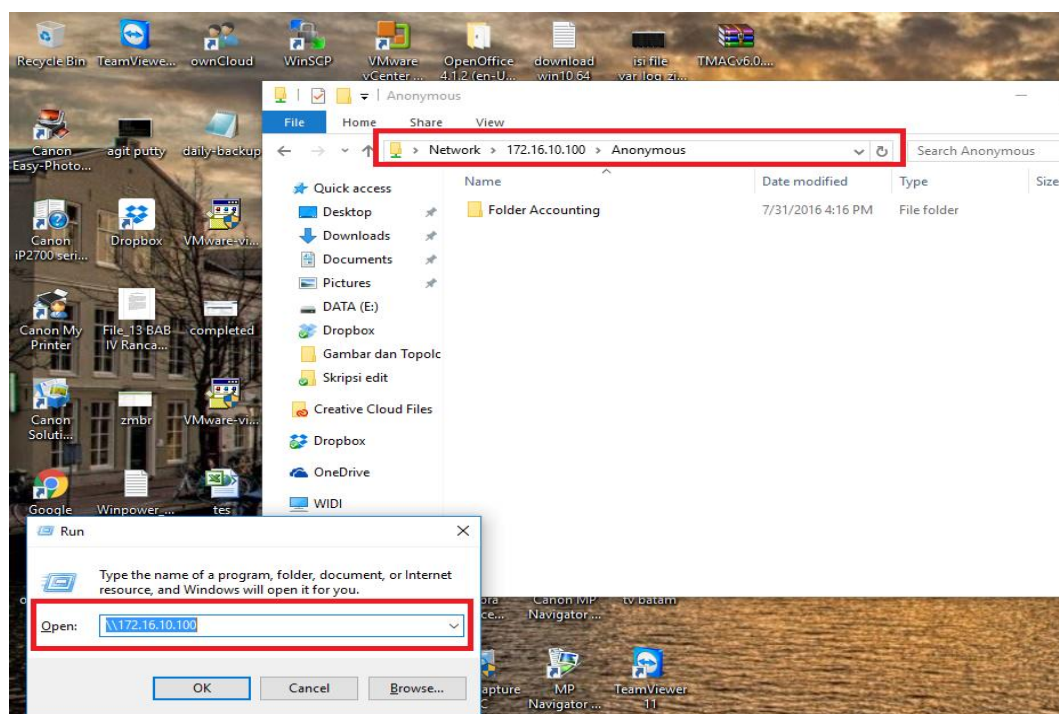
Gambar IV.14 Pengujian dengan *tracert*Gambar IV.15. Pengujian dengan *wireshark*

Dari gambar di atas dapat dijelaskan bahwa jalur yang dilewati untuk mencapai ke arah jaringan lokal (LAN) yang ada di cabang dengan IP Address 172.16.10.100 adalah melalui IP Address 192.168.0.1 yaitu IP Address Gateway

LAN di kantor pusat. Kemudian diteruskan melalui IP Gateway Tunnel kantor cabang yaitu 10.10.10.2 dan terakhir sampai di IP 172.16.10.100.

Ketika melakukan *tracerroute* ke *host* tujuan maka IP *Public* yang seharusnya menjadi *gateway* untuk berkomunikasi ke internet tidak akan terdeteksi sebab IP Address yang diminta dari user adalah bagian dari jaringan LAN kantor cabang dengan *gateway eoip-tunnel address* yang sudah di konfigurasi.

Sehingga data yang dilewati untuk mencapai host tertentu yang ada di cabang seakan-akan tidak melewati jalur internet.



Gambar IV.16 Tes folder *sharing* kearah kantor Cabang

Setelah terjadinya koneksi intranet yang ada di kantor pusat dan kantor cabang , maka kita dapat berbagi akses dan kemudahan untuk membentuk satu jaringan berskala *Wide Area Network* (WAN) sehingga seluruh staff dapat memanfaatkan *resource* seluruh jaringan yang ada untuk terhubung ke jaringan LAN yang ada di kantor pusat dan cabang tanpa harus membuat suatu autentifikasi

user terlebih dahulu. Untuk hak akses folder dapat diatur oleh sistem administrator sehingga tidak semua user dapat mengakses folder yang bukan pada divisi terkait.