e-BUKU KERJA

NETWORK ADMINISTRATOR

FAZTRAIN

IT TRAINING & CONSULTING

Prakata e-Buku Kerja CNSA

Alhamdulillah, segala puji bagi ALLAH Ta'ala yang telah memberikan petunjuk-Nya, sehingga **e-Buku Kerja Network Administrator** ini dapat kami selesaikan. e-Buku Kerja ini Insya ALLAH akan menjadi solusi bagi rekan-rekan pembelajar, yang ingin mengetahui implementasi real ilmu pengelolaan jaringan komputer di lapangan.

e-Buku Kerja ini benar-benar kami susun berdasarkan kondisi di lapangan, oleh karena itu tahapan kerja yang disajikan pada e-Buku Kerja juga disesuaikan dengan urutan pengerjaan yang benar-benar runut, agar Anda dapat dipandu dengan mudah dan dapat menyelesaikan setiap tugas kerja dengan baik.

Skenario yang disajikan pada e-Buku Kerja ini didasarkan pada kebutuhan sebuah perusahaan bernama PT. **ABC**Net yang berkantor di **Jakarta** dan memiliki sebuah kantor cabang di **Palopo** (Sulawesi Selatan). Misi kerja yang harus diselesaikan antara lain menghubungkan semua komputer di area LAN/WLAN ke *internet*, baik yang ada di kantor pusat maupun kantor cabang, selanjutnya menyediakan akses dari kantor cabang ke mesin *server* aplikasi dan *server* VoIP yang ada di kantor pusat.

e-Buku Kerja **Network Administrator** ini harus digunakan bersama-sama dengan e-Buku Kerja **System Administrator** dan **VoIP Administrator**, hal ini karena ketiganya adalah satu kesatuan misi kerja yang harus diselesaikan untuk memenuhi kebutuhan dari PT. **ABC**Net. Hal ini dilakukan agar kemampuan yang dimiliki tidak hanya bekerja secara individu, namun juga mampu bekerja secara tim. Misi kerja pada PT. **ABC**Net harus diselesaikan oleh tiga komponen kompetensi sekaligus, yaitu NetAdmin, SysAdmin dan VoIP Admin.

Akhir kalam, Berkah adalah Kebaikan yang melahirkan Kebaikan...

e-Buku Kerja ini kami persembahkan dengan hati penuh cinta

FazTrain IT Training & Consulting

Tahap 1
Koneksi Jaringan LAN ke Internet

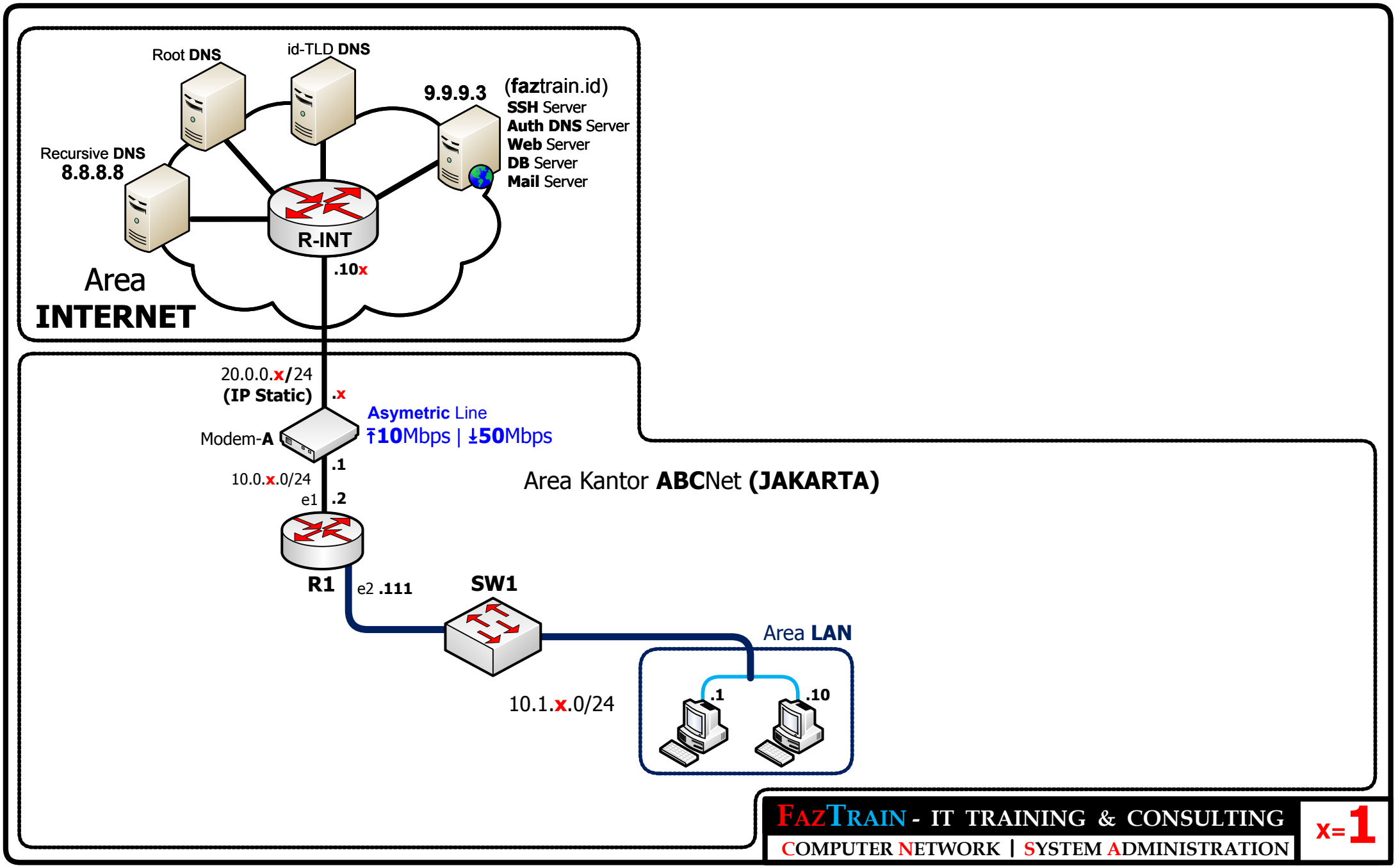
Sebuah perusahaan bernama PT. **ABC**Net yang berpusat di Jakarta membutuhkan sebuah jaringan LAN yang terhubung ke *internet* untuk membantu operasional perusahaan. PT. **ABC**Net akan berlangganan koneksi internet dari sebuah ISP dengan spesifikasi koneksi *upload* sebesar 10 Mbps dan *download* sebesar 50 Mbps, dan disediakan satu alamat IP publik statik yang dapat diakses dari *internet*.

Dari kebutuhan PT. **ABC**Net tersebut, maka dibuatlah rancangan topologi jaringan seperti pada gambar 1.1. Pengerjaan proyek tahap 1 ini akan mengikuti tahapan sebagai berikut.

A. Instalasi Perangkat Jaringan

Proses instalasi perangkat jaringan dimulai dari instalasi Modem-A yang dilakukan oleh pihak ISP. Koneksi *internet* Modem-A ke ISP menggunakan media transmisi kabel Fiber Optik (FO), sedang koneksi *port* (colokan) LAN Modem-A ke Router (R1) menggunakan media transmisi kabel *Twisted Pair* (UTP/STP).

Router (R1) adalah penghubung antara jaringan LAN dan jaringan *internet*, oleh karena itu maka Router (R1) akan dikoneksikan pula ke jaringan LAN. Spesifikasi dari Router (R1) bisa menggunakan merk dan model apa saja, namun pada proyek ini Router (R1) akan menggunakan RouterBoard MikroTik seri 900, minimal bisa menggunakan RB931 dengan jumlah koneksi Ethernet RJ45 sebanyak 3 port dan ada 1 koneksi Ethernet *Wireless*. Port LAN Modem-A dihubungkan ke Router (R1) pada port ether1 (e1), sedang port ether2 (e2) pada Router (R1) dihubungkan ke Switch 1 (SW1) agar jaringan LAN dapat terkoneksi ke *internet* lewat Router (R1).

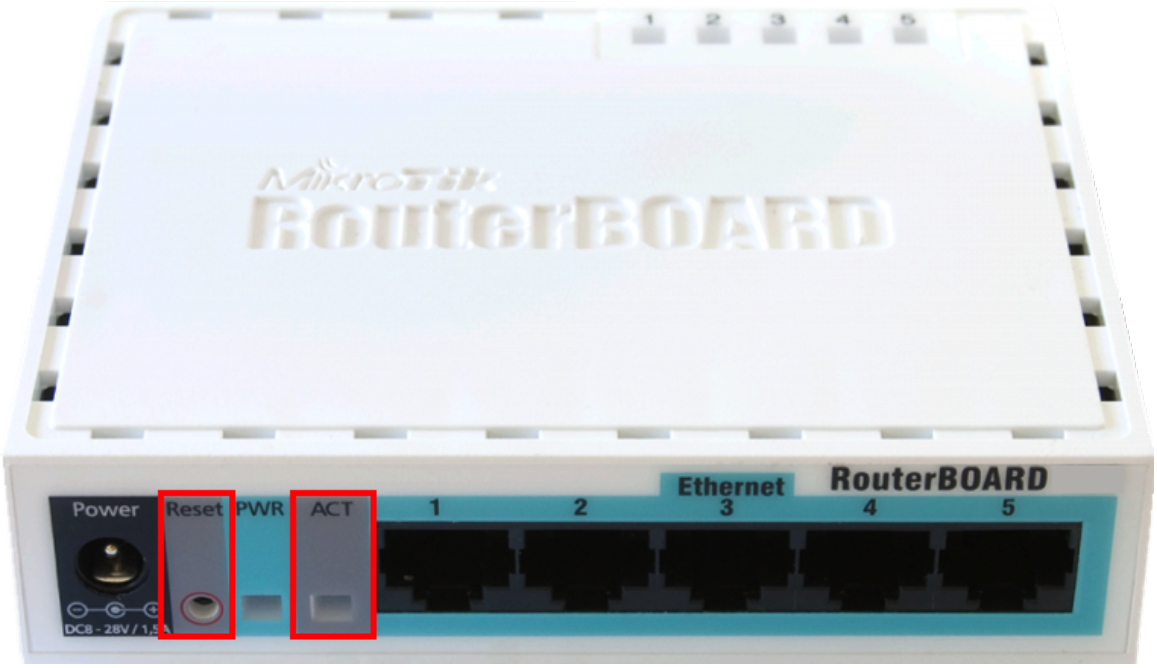

Root DNS
id-TLD DNS
9.9.9.3
(faztrain.id)
SSH Server
Auth DNS Server
Web Server
DB Server
Mail Server
Recursive DNS
8.8.8.8
R-INT
.10x
Area
INTERNET
20.0.0.x/24
(IP Static)
.x
Asymetric Line
↑10Mbps | ↓50Mbps
Modem-A
.1
10.0.x.0/24
e1
.2
Area Kantor ABCNet (JAKARTA)
R1
e2 .111
SW1
Area LAN
10.1.x.0/24
.1
.10
FAZTRAIN - IT TRAINING & CONSULTING
COMPUTER NETWORK | SYSTEM ADMINISTRATION
x=1

Semua komputer di jaringan LAN terhubung ke Switch (SW1), pada proyek ini Switch (SW1) masih menggunakan *Unmanageable Switch*, sehingga belum bisa dikonfigurasi untuk fungsi-fungsi tertentu, namun sudah cukup memenuhi kebutuhan koneksi di jaringan komputer sederhana.

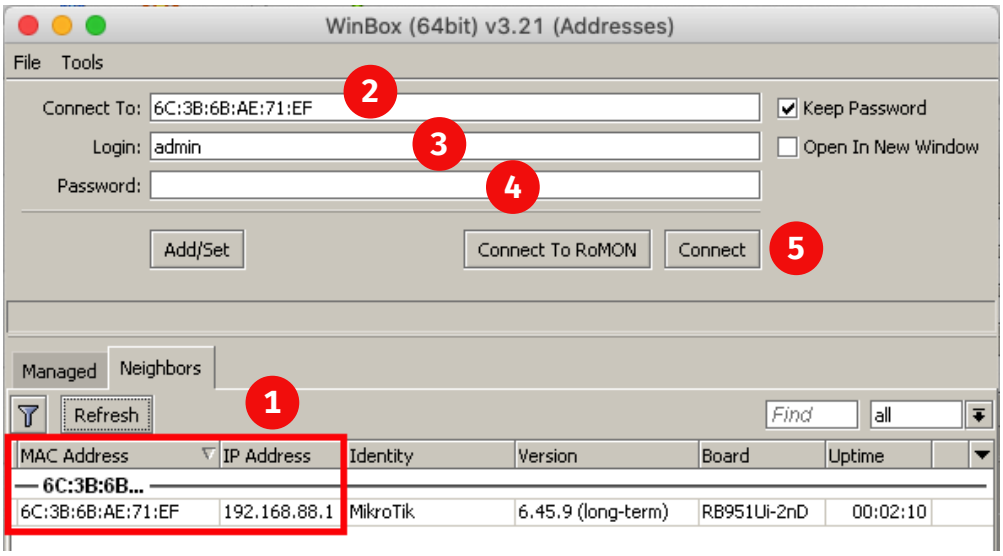
B. Konfigurasi Perangkat Jaringan

Topologi jaringan yang telah dibuat sebelumnya merupakan pemandu saat melakukan konfigurasi perangkat jaringan. Perangkat-perangkat jaringan yang akan dikonfigurasi antara lain, Router (R1) dan setiap komputer pada LAN yang akan dikoneksikan ke jaringan *internet*.

Umumnya RouterBoard Mikrotik (Router R1) sudah siap digunakan untuk mengkoneksikan jaringan LAN ke *internet*, namun kadang pada kondisi tertentu, konfigurasi bawaan tersebut belum sesuai dengan kondisi yang dibutuhkan, sehingga konfigurasi awal RouterBoard MikroTik perlu dihapus dengan melakukan *reset* agar dapat dikonfigurasi ulang sesuai kebutuhan. Berikut adalah cara melakukan *reset* pada RouterBoard, terlebih dahulu pastikan RouterBoard dalam kondisi mati, lalu tekan tombol "Reset" dan jangan dilepas, kemudian nyalakan RouterBoard dan tunggu hingga lampu indikator ACT/RES menyala kedap-kedip, lalu berhenti menekan tombol Reset, setelah itu matikan RouterBoard kemudian dihidupkan kembali, Gambar 1.2 menunjukkan posisi tombol RESET dan lampu indikator ACT/RES. Jalankan aplikasi Winbox untuk mengakses RouterOS, informasi terkait RouterBoard MikroTik akan tampil pada jendela deteksi Winbox seperti tampak pada Gambar 1.3, untuk mengakses RouterOS bisa menggunakan alamat MAC ataupun alamat IP, pastikan username terisi "***admin***" (tanpa tanda petik) sedang password dikosongkan saja, lalu klik tombol "***Connect***". Pada gambar 1.3 nampak bahwa RouterOS diakses menggunakan alamat MAC.

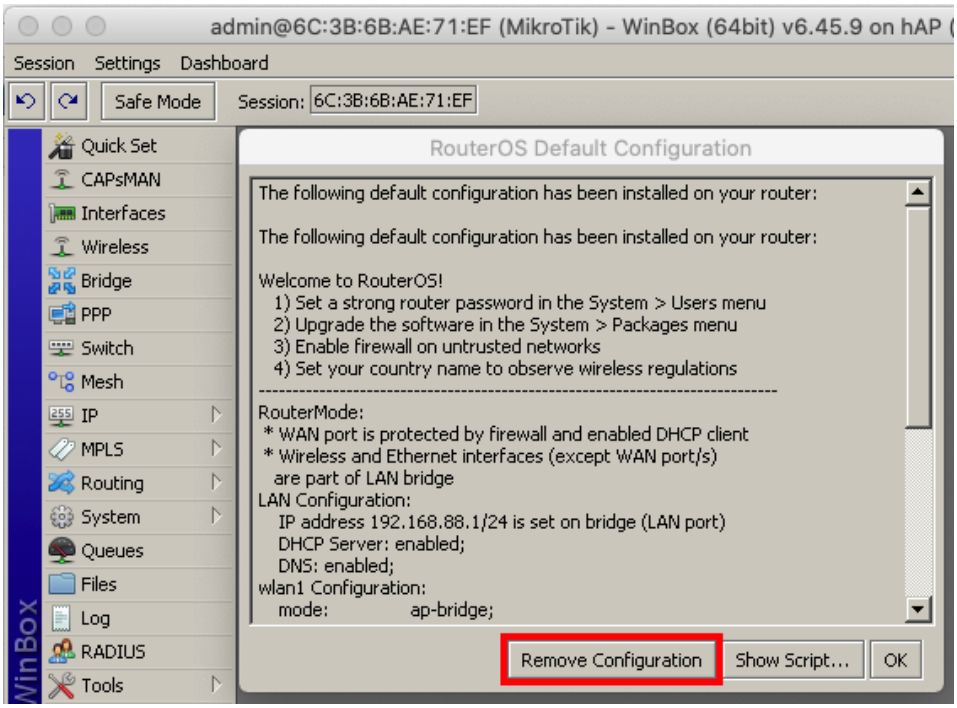


Gambar 1.2. Tombol RESET dan lampu indikator ACT/RES RouterBoard



Gambar 1.3. Mengakses RouterOS dengan Winbox

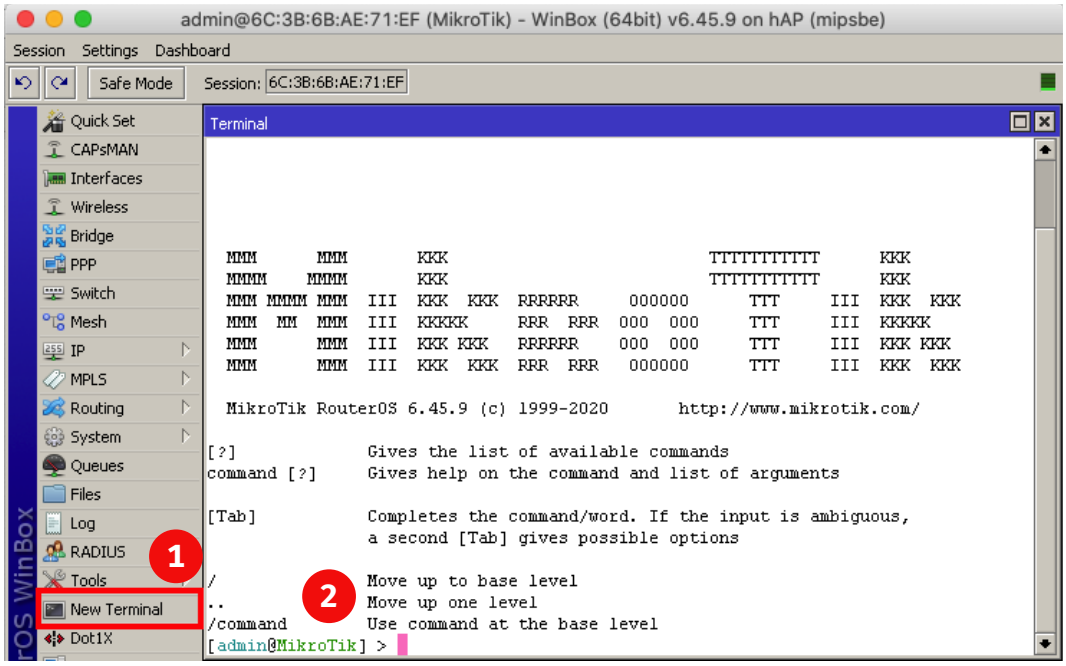
Jika berhasil mengakses RouterOS, maka pertama kali setelah di-*reset* akan tampil jendela konfirmasi seperti pada Gambar 1.4, klik tombol "***Remove Configuration***" untuk menghapus semua konfigurasi bawaan RouterBoard.



Gambar 1.4. Menghapus konfigurasi default RouterOS MikroTik

RouterBoard menggunakan sistem operasi bernama RouterOS, untuk melakukan konfigurasi pada RouterOS dibutuhkan aplikasi bawaan MikroTik bernama Winbox. Aplikasi Winbox ini bisa dijalankan dibeberapa jenis sistem operasi, seperti Microsoft Windows, Linux dan MacOS. Dalam proses konfigurasi RouterOS menggunakan Winbox, bisa dalam mode grafis (GUI) dan bisa pula dalam mode *console* (teks terminal). Dalam buku kerja ini, proses konfigurasi RouterOS akan menggunakan mode teks, hal ini dilakukan dengan pertimbangan kemudahan dan kecepatan proses konfigurasi serta kebutuhan koneksi yang jauh lebih rendah jika dibandingkan konfigurasi menggunakan mode grafis.

Setelah berhasil mengakses mode terminal pada Winbox seperti pada Gambar 1.5, maka tahap konfigurasi yang akan dilakukan pada RouterBoard MikroTik adalah memastikan RouterBoard MikroTik dapat terkoneksi ke *internet* serta beberapa konfigurasi tambahan lainnya, tahapannya sebagai berikut.



Gambar 1.5. Mengakses Terminal RouterOS pada Winbox

1. Secara *default* identitas RouterBoard akan bernama ”MikroTik”, hal ini akan menyulitkan proses identifikasi saat jumlah RouterBoard yang dikelola sudah banyak, olehnya itu maka konfigurasi identitas (*identity*) RouterBoard MikroTik perlu dilakukan. Perintah berikut untuk mengubah nama identitas RouterBoard MikroTik menjadi “R1” sesuai pada gambar topologi. Hal ini untuk memudahkan identifikasi RouterBoard MikroTik saat digunakan.

```
[admin@MikroTik] > system identity set name=R1
```

Lakukan verifikasi hasil konfigurasi dengan perintah berikut.

```
[admin@R1] > system identity print
   name : R1
```

2. Konfigurasi *interface* jaringan yang akan digunakan untuk terkoneksi ke jaringan *internet* dan ke jaringan LAN. Pada konfigurasi ini hanya dilakukan pengubahan nama *interface* `ether1` dan `ether2` agar mudah diidentifikasi.

Tabel 1.1. Daftar alamat IP versi 4 (*Classless*) dan prefiks untuk kebutuhan *subnetting* dan *summarization* (*supernetting*)

IP Loopback	IP Private	IP Link Local	IP Multicast	IP Broadcast	IP Public
127.0.0.0/8	10.0.0.0/8 172.16.0.0/12 192.168.0.0/24	169.254.0.0/16	224.0.0.0 - 239.255.255.255	255.255.255.255	https://www.iana.org/assignments/ipv4-address-space/

Prefix	/8	/9	/10	/11	/12	/13	/14	/15
Subnet Mask	255.0.0.0	255.128.0.0	255.192.0.0	255.224.0.0	255.240.0.0	255.248.0.0	255.252.0.0	255.254.0.0
Jumlah IP Host	16777214	8388606	4194302	2097150	1048574	524286	262142	131070
Range I IP Host	10.0.0.1 - 10.255.255.254	10.0.0.1 - 10.127.255.254	10.0.0.1 - 10.63.255.254	10.0.0.1 - 10.31.255.254	10.0.0.1 - 10.15.255.254	10.0.0.1 - 10.7.255.254	10.0.0.1 - 10.3.255.254	10.0.0.1 - 10.1.255.254

Prefix	/16	/17	/18	/19	/20	/21	/22	/23
Subnet Mask	255.255.0.0	255.255.128.0	255.255.192.0	255.255.224.0	255.255.240.0	255.255.248.0	255.255.252.0	255.255.254.0
Jumlah IP Host	65534	32766	16382	8190	4094	2046	1022	510
Range I IP Host	10.1.0.1 - 10.1.255.254	10.1.0.1 - 10.1.127.254	10.1.0.1 - 10.1.63.254	10.1.0.1 - 10.1.31.254	10.1.0.1 - 10.1.15.254	10.1.0.1 - 10.1.7.254	10.1.0.1 - 10.1.3.254	10.1.0.1 - 10.1.1.254

Prefix	/24	/25	/26	/27	/28	/29	/30
Subnet Mask	255.255.255.0	255.255.255.128	255.255.255.192	255.255.255.224	255.255.255.240	255.255.255.248	255.255.255.252
Jumlah IP Host	254	126	62	30	14	6	2
Range I IP Host	10.1.1.1 - 10.1.1.254	10.1.1.1 - 10.1.1.126	10.1.1.1 - 10.1.1.62	10.1.1.1 - 10.1.1.30	10.1.1.1 - 10.1.1.14	10.1.1.1 - 10.1.1.6	10.1.1.1 - 10.1.1.2

Lakukan pengecekan untuk mengetahui nomor urut interface `ether1` dan `ether2`

```
[admin@R1] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#     NAME                TYPE       ACTUAL-MTU   L2MTU    MAX-L2MTU
0 R   ether1              ether            1500    1598         2028
1 R   ether2              ether            1500    1598         2028
2     ether3              ether            1500    1598         2028
3     ether4              ether            1500    1598         2028
4     ether5              ether            1500    1598         2028
5 X   wlan1               wlan             1500    1600         2290
```

Lakukan konfigurasi pengubahan nama interface `ether1` menjadi `ether1-Internet` dan interface `ether2` menjadi `ether2-LAN`.

```
[admin@R1] > interface set 0 name=ether1-Internet
[admin@R1] > interface set 1 name=ether2-LAN
```

Lakukan verifikasi hasil konfigurasi dengan perintah berikut.

```
[admin@R1] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#     NAME                TYPE       ACTUAL-MTU   L2MTU    MAX-L2MTU
0 R   ether1-Internet     ether            1500    1598         2028
1 R   ether2-LAN          ether            1500    1598         2028
2     ether3              ether            1500    1598         2028
3     ether4              ether            1500    1598         2028
4     ether5              ether            1500    1598         2028
5 X   wlan1               wlan             1500    1600         2290
```

3. Konfigurasi alamat IP agar RouterBoard MikroTik dapat terkoneksi ke *gateway internet* dan ke jaringan LAN, sesuai alamat IP yang tertera pada topologi jaringan. Penentuan alamat IP dan prefiks didasarkan pada tabel 1.1. Alamat IP yang digunakan adalah alamat IP *Private* dan prefiks digunakan untuk menentukan jumlah alamat IP *host* pada setiap area jaringan.

```
[admin@R1] > ip address add address=10.0.1.2/24 interface=ether1-Internet
[admin@R1] > ip address add address=10.1.1.111/24 interface=ether2-LAN
```

Lakukan verifikasi hasil konfigurasi alamat IP dengan perintah berikut.

```
[admin@R1] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.1.2/24        10.0.1.0        ether1-Internet
 1   10.1.1.111/24      10.1.1.0        ether2-LAN
```

Lakukan pengujian koneksi ke alamat IP *gateway internet*.

```
[admin@R1] > ping 10.0.1.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.0.1.1                                   56  64 0ms
    1 10.0.1.1                                   56  64 0ms
    2 10.0.1.1                                   56  64 0ms
    3 10.0.1.1                                   56  64 0ms
```

4. Konfigurasi *routing* perlu dilakukan agar RouterBoard dapat terkoneksi ke *internet* lewat *gateway* (Modem), sekaligus lakukan verifikasi hasil konfigurasi.

```
[admin@R1] > ip route add dst-address=0.0.0.0/0 gateway=10.0.1.1
[admin@R1] > 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                          10.0.1.1               1
 1 ADC   10.0.1.0/24        10.0.1.2        ether1-Internet        0
 2 ADC   10.1.1.0/24        10.1.1.111      ether2-LAN             0
```

Lakukan pengujian koneksi ke alamat IP yang ada di *internet*.

```
[admin@R1] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56  52 45ms
    1 8.8.8.8                                    56  52 43ms
    2 8.8.8.8                                    56  52 46ms
    3 8.8.8.8                                    56  52 44ms
```

5. Konfigurasi *DNS Client* agar RouterBoard dapat terkoneksi ke *internet* menggunakan alamat nama domain (misal, google.com), dan sekaligus lakukan verifikasi hasil konfigurasi. Parameter "`allow-remote-requests=`**yes**" akan mengizinkan semua komputer dapat terkoneksi ke RouterBoard sebagai **DNS Cache**, jadi pada setiap komputer *client* di LAN cukup menjadikan alamat IP RouterBoard sebagai alamat **DNS Server**.

```
[admin@R1] > ip dns set servers=8.8.8.8 allow-remote-requests=yes
[admin@R1] > ip dns print
                    servers: 8.8.8.8
            dynamic-servers:
      allow-remote-requests: yes
        max-udp-packet-size: 4096
       query-server-timeout: 2s
        query-total-timeout: 10s
    max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
                 cache-size: 2048KiB
              cache-max-ttl: 1w
                 cache-used: 17KiB
```

Lakukan pengujian koneksi ke alamat nama domain yang ada di *internet*.

```
[admin@R1] > ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 74.125.24.100                              56  54  43ms
    1 74.125.24.100                              56  54  43ms
    2 74.125.24.100                              56  54  45ms
    3 74.125.24.100                              56  54  42ms
```

6. Konfigurasi *NTP Client* dan pengaturan waktu (*clock*) agar RouterBoard beroperasi menggunakan waktu (jam) yang sesuai standar. Setelah itu lakukan verifikasi untuk memastikan RouterBoard terkoneksi ke NTP Server. Pengatuan ini sangat berguna saat melakukan penjadwalan rutin kegiatan tertentu pada RouterBoard. NTP server yang digunakan adalah yang memiliki alamat `id.pool.ntp.org`.

```
[admin@R1] > system ntp client set enabled=yes server-dns-names=id.pool.ntp.org
[admin@R1] > system ntp client print
            enabled: yes
        primary-ntp: 0.0.0.0
      secondary-ntp: 0.0.0.0
  server-dns-names: id.pool.ntp.org
               mode: unicast
      poll-interval: 32s
      active-server: 162.159.200.1
   last-update-from: 162.159.200.1
 last-update-before: 14s610ms
    last-adjustment: 2682w4d21h1m37s714ms870us
```

Pengaturan waktu sesuai zona waktu (*time-zone*) dilakukan untuk wilayah **Asia/Jakarta**, selanjutnya dilakukan verifikasi hasil konfigurasi untuk mengetahui apakah RouterOS sudah menunjukkan waktu dan tanggal yang tepat.

```
[admin@R1] > system clock set time-zone-autodetect=no \
time-zone-name=Asia/Jakarta
```

```
[admin@R1] > system clock print
                  time: 08:52:01
                  date: jun/02/2021
  time-zone-autodetect: no
        time-zone-name: Asia/Jakarta
            gmt-offset: +07:00
            dst-active: no
```

7. Konfigurasi **SNAT** (*Source Network Address Translation*) harus dilakukan agar semua komputer di area LAN dapat terkoneksi ke *internet* lewat RouterBoard MikroTik.

```
[admin@R1] > ip firewall nat add chain=srcnat src-address=10.1.1.0/24 \
out-interface=ether1-Internet action=masquerade comment="Sharing \
Internet untuk Area LAN"
```

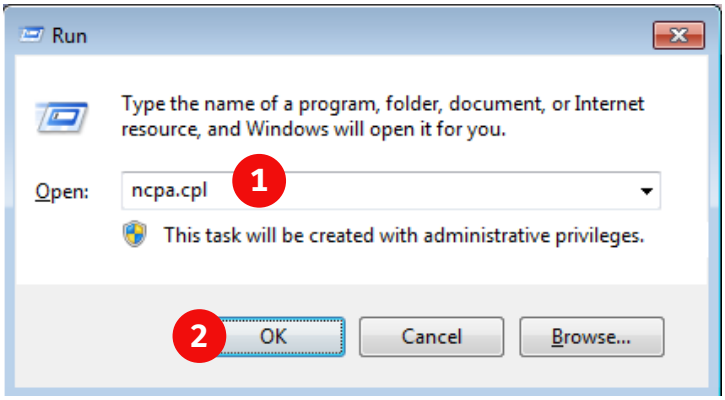
Verifikasi hasil konfigurasi SNAT.

```
[admin@R1] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Sharing Internet untuk Area LAN
      chain=srcnat action=masquerade src-address=10.1.1.0/24 out-
interface=ether1-Internet
```

C. Pengujian Koneksi Jaringan

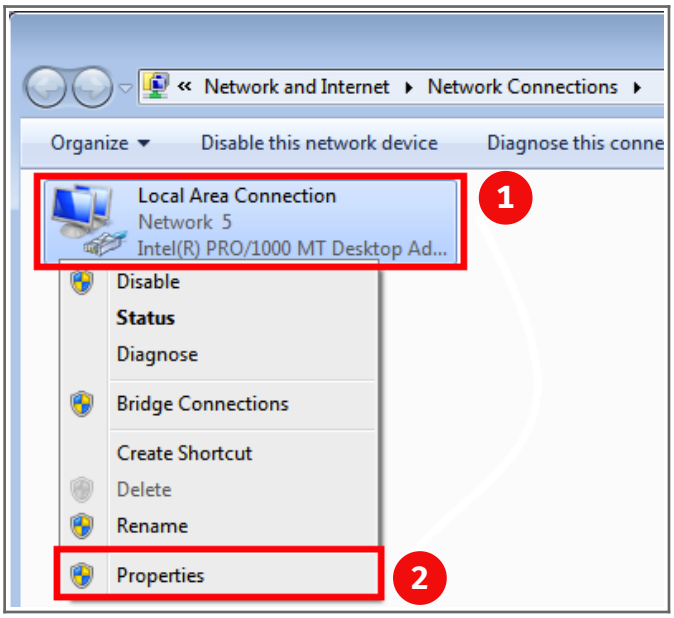
Proses pengujian koneksi jaringan terlebih dahulu diawali dengan konfigurasi alamat IP pada sisi komputer *client* di LAN, lalu dilakukan pengujian koneksi hingga ke jaringan *internet*. Pada skenario ini, komputer *client* menggunakan sistem operasi Microsoft Windows.

1. Buka jendela **RUN** dengan menekan tombol keyboard ⊞ + **R**, setelah itu ketik "**`ncpa.cpl`**" (tanpa tanda petik), lalu klik tombol OK, seperti pada gambar 1.6 untuk menampilkan jendela Network Connection.



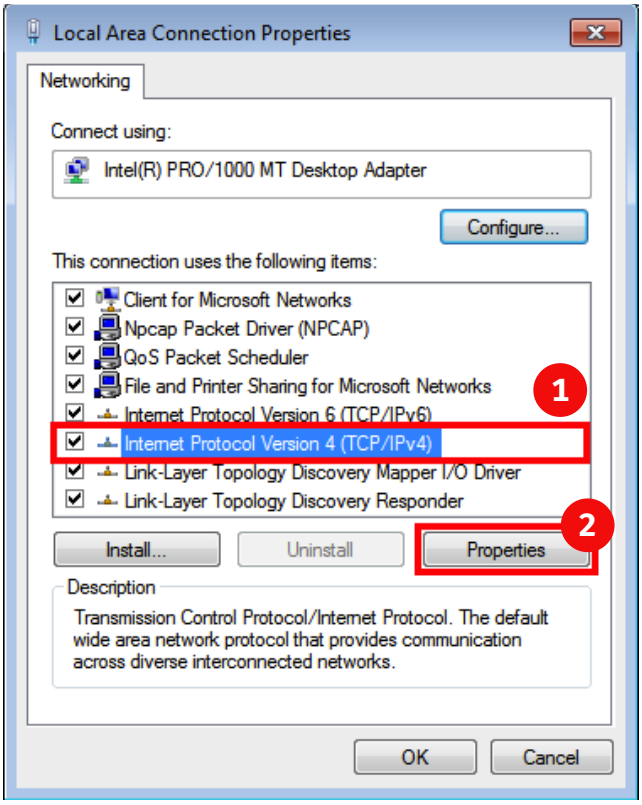
Gambar 1.6. Perintah menampilkan jendela *Network Connection*

2. Klik kanan pada icon LAN Connection (Gambar 1.7) kemudian pilih "*Properties*".



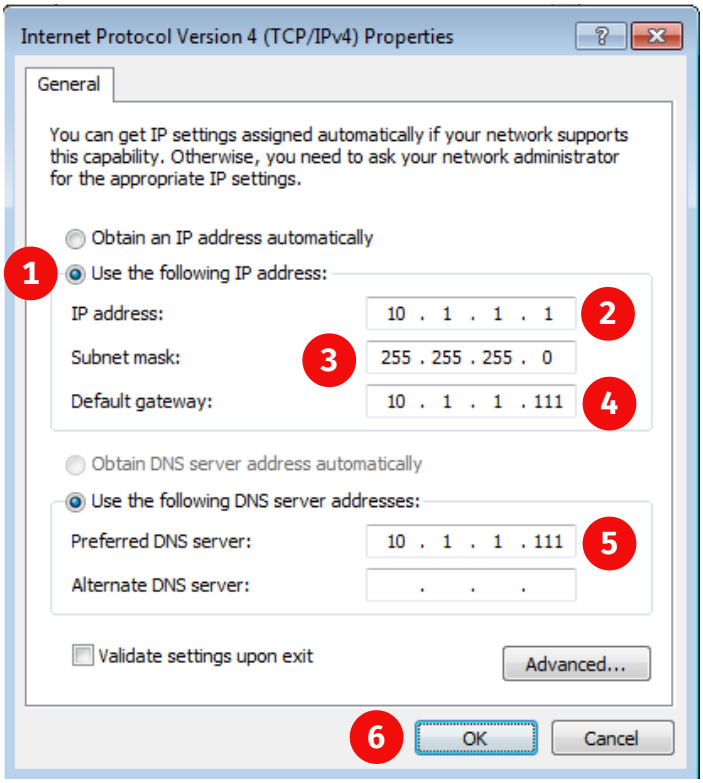
Gambar 1.7. Menampilkan jendela Properties LAN Connection

3. Pilih baris "Internet Protocol Version 4 (TCP/IPv4" kemudian klik tombol "Properties" (Gambar 1.8).



Gambar 1.8. Menampilkan Properties konfigurasi alamat IPv4

4. Isi semua kotak mulai dari "**IP Address**" untuk menentukan alamat IP komputer *client*, kemudian kotak "**Subnet Mask**" untuk menentukan rentang alamat IP yang searea dengan alamat IP yang telah ditentukan pada kotak IP Address, isi pula kotak "**Default Gateway**" agar komputer *client* dapat terkoneksi ke internet lewat *gateway* RouterBoard MikroTik, dan terakhir adalah mengisi kotak "**Preferred DNS Server**" agar komputer *client* dapat terkoneksi ke internet menggunakan alamat nama domain, kemudian klik OK, dan klik OK lagi pada jendela selanjutnya (Gambar 1.9). Alamat IP DNS pada kotak "*Preferred DNS Server*" menggunakan alamat IP lokal dari RouterOS MikroTik (**10.1.1.111**) karena kebutuhan akses *server* ABCNet menggunakan alamat nama domain "**abcnet-1.net**" pada tahap selanjutnya.



Gambar 1.9. Konfigurasi alamat IP

5. Lakukan pengujian koneksi dari komputer *client* ke *internet,* baik menggunakan alamat IP maupun alamat nama domain.

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=42ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 43ms

C:\>ping google.com

Pinging google.com [74.125.24.100] with 32 bytes of data:
Reply from 74.125.24.100: bytes=32 time=43ms TTL=52
Reply from 74.125.24.100: bytes=32 time=44ms TTL=52
Reply from 74.125.24.100: bytes=32 time=42ms TTL=52
Reply from 74.125.24.100: bytes=32 time=43ms TTL=52

Ping statistics for 74.125.24.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 43ms
```

Tahap 2
Koneksi Jaringan Wireless LAN ke Internet

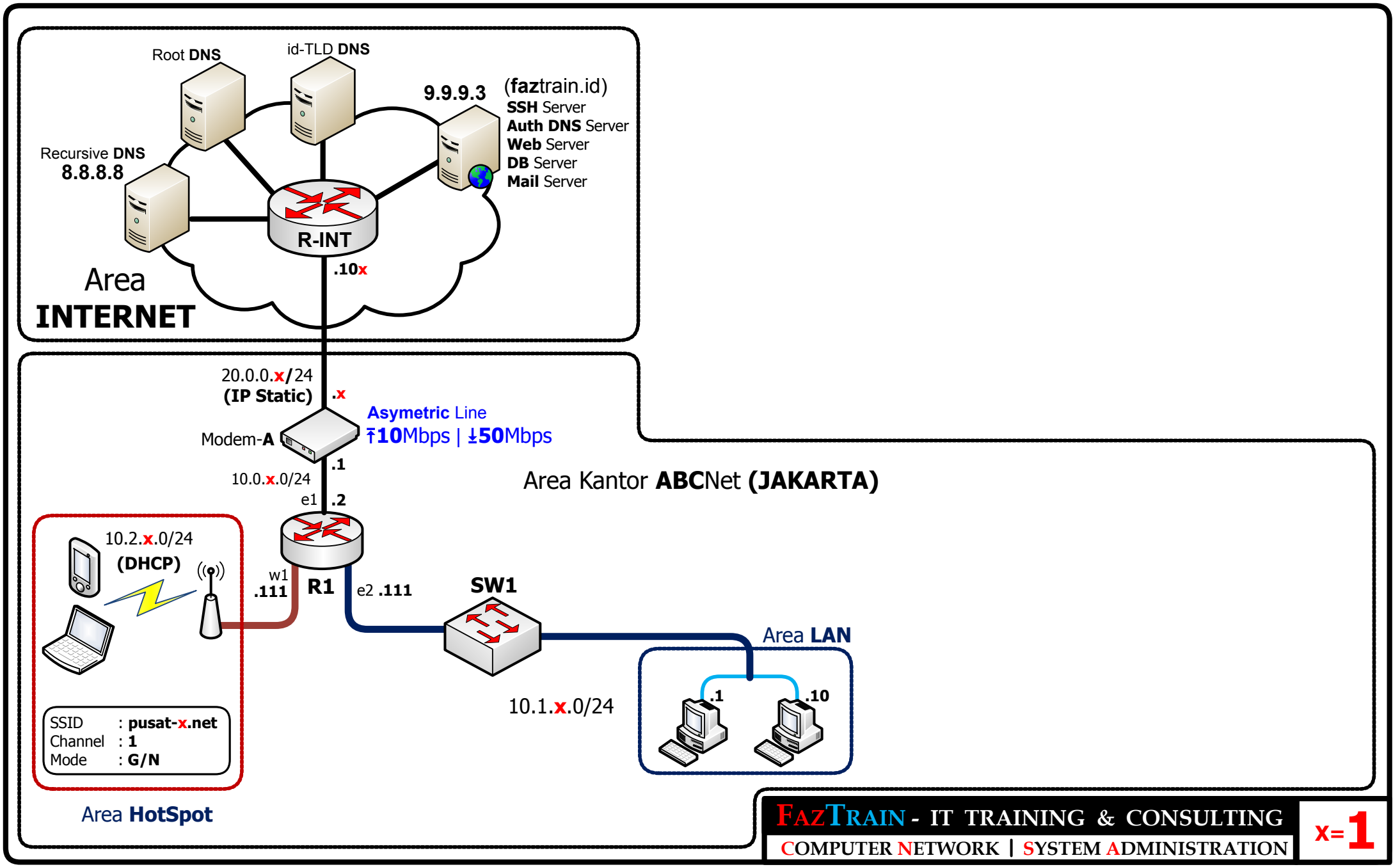
PT. **ABC**Net (Jakarta) meminta untuk melengkapi jaringan komputernya dengan fasilitas koneksi *wireless* atau umumnya dikenal dengan *Wireless* LAN (WLAN). Koneksi *wireless* juga akan dilengkapi dengan sistem ***hotspot captive portal*** yang akan mewajibkan setiap pengguna WLAN, melakukan *login* dengan akun yang telah terdaftar pada sistem *hotspot* untuk bisa terkoneksi ke *internet*.

Pada skenario ini, RouterBoard MikroTik yang digunakan telah dilengkapi dengan fitur koneki *wireless* dan sistem *hotspot captive portal*, sehingga tidak perlu melakukan penambahan baik perangkat fisik maupun perangkat lunak. Proses instalasi dan konfigurasi akan mengikuti topologi jaringan yang tertera pada gambar di halaman berikutnya.

A. Konfigurasi Perangkat Jaringan WLAN

Secara fisik RouterBoard MikroTik yang digunakan pada skenario ini sudah dilengkapi dengan koneksi *wireless* dan akan difungsikan sebagai ***Wireless Access Point*** (WAP). Beberapa hal yang harus ditentukan sebelum dilakukan konfigurasi pada tahap selanjutnya terkait koneksi *wireless* antara lain:

1. Mode operasi *wireless*, dalam hal ini mode operasi yang akan digunakan adalah sebagai ***Access Point*** (AP). Saat dalam mode **AP**, maka perangkat *wireless* akan beroperasi layaknya Switch pada jaringan LAN, yang akan menghubungkan setiap perangkat *wireless* di sisi *client* atau ***Wireless Station*** dengan perangkat *wireless* lainnya di jaringan WLAN, dan juga akan menjadi penghubung saat koneksi ke *internet*.


Root DNS
id-TLD DNS
9.9.9.3
(faztrain.id)
SSH Server
Auth DNS Server
Web Server
DB Server
Mail Server
Recursive DNS
8.8.8.8
R-INT
.10x
Area
INTERNET
20.0.0.x/24
(IP Static)
.x
Asymetric Line
↑10Mbps | ↓50Mbps
Modem-A
.1
10.0.x.0/24
e1
.2
Area Kantor ABCNet (JAKARTA)
10.2.x.0/24
(DHCP)
w1
.111
R1
e2 .111
SW1
Area LAN
10.1.x.0/24
.1
.10
SSID : pusat-x.net
Channel : 1
Mode : G/N
Area HotSpot
FAZTRAIN - IT TRAINING & CONSULTING
COMPUTER NETWORK | SYSTEM ADMINISTRATION
x=1

2. ***Service Set IDentifier*** (**SSID**), bagian ini untuk menentukan nama jaringan WLAN yang akan terdeteksi di sisi *wireless client* saat akan melakukan koneksi ke jaringan WLAN.

3. ***Wireless Band***, bagian ini akan menentukan apakah perangkat *wireless* akan dioperasikan menggunakan frekuensi berbasis **2GHz** ataukah **5GHz**, kedua jenis frekuensi tersebut merupakan frekuensi yang boleh digunakan secara bebas tanpa perlu izin dari pemerintah, namun tetap harus mematuhi aturan-aturan yang telah ditentukan oleh pemerintah, agar saat digunakan tidak merugikan pihak lain. Beberapa hal yang diatur adalah tentang **maksimal daya pancar** yang boleh digunakan oleh perangkat *wireless* ketika beroperasi. Hal selanjutnya yang harus ditentukan pada bagian ini adalah mode band yang digunakan, ada beberapa pilihan diantaranya mode **B**, **G** dan/atau **N**, perbedaan ketiganya ada pada besar data maksimal yang bisa ditransfer dalam waktu satu detik, **B** maksimal **11 Mbps**, **G** maksimal **54 Mbps** dan **N** maksimal **150 Mbps**.

4. ***Channel Width***, bagian ini menentukan lebar saluran (***channel***) yang akan membawa *bandwidth*, makin lebar saluran yang digunakan maka akan semakin besar *bandwidth* yang bisa dilewatkan pada saluran tersebut, yang artinya akan semakin besar data yang bisa ditransfer dalam tiap detiknya. Umumnya perangkat *wireless* di sisi *client* menggunakan lebar saluran 20MHz.

5. ***Wireless Frequency***, atau kadang juga menggunakan istilah "***Channel***" adalah bagian yang digunakan untuk menentukan frekuensi radio yang akan digunakan dalam proses komunikasi dengan *wireless client/station*. Berikut adalah daftar *channel* dan frekuensi yang boleh digunakan (khusus *band* 2,4GHz) seperti terlampir pada table 2.1. Sangat disarankan, untuk pemasangan wireless AP yang saling berdekatan untuk menggunakan kombinasi *channel* 1, 6 dan 11, agar tidak saling melemahkan sinyal satu sama lainnya, hal ini biasa juga dikenal dengan interferensi sinyal.

Tabel 2.1. Daftar Channel dan Frekuensi pada Band 2,4GHz

Channel	Frekuensi
1	**2412**
2	2417
3	2422
4	2427
5	2432
6	**2437**
7	2442
8	2447
9	2452
10	2457
11	**2462**

6. ***Security Profile***, bagian ini menentukan apakah dalam proses komunikasi antar perangkat akan menerapkan fitur keamanan akses atau tidak, secara default tidak menggunakan fitur keamanan, sehingga perangkat *wireless client* mana saja dapat terhubung ke *wireless* AP. Saat akan menerapkan sistem *hotspot captive portal*, maka bagian ini dibuat *default* saja, karena proses otentifikasi akan dilakukan oleh *captive portal*.

Berikut adalah tahapan konfigurasi WLAN sekaligus sistem *hotspot captive portal* yang merupakan fitur bawaan dari RouterOS MikroTik.

Konfigurasi diawali dengan mengaktifkan *interface wireless*.

```
[admin@R1] > interface wireless enable wlan1
```

Selanjutnya mengkonfigurasi interface wireless sesuai petunjuk pada topologi jaringan, SSID: "**pusat-1.net**" dengan frekuensi kerja **2,412GHz** (setara dengan *Channel* 1).

```
[admin@R1] > interface wireless set 0 master-interface=wlan1 \
mode=ap-bridge ssid=pusat-1.net band=2ghz-g/n frequency=2412 \
channel-width=20mhz security-profile=default
```

Selanjutnya melakukan konfigurasi alamat IP untuk *interface* wlan1, selain alamat IP berguna sebagai alamat IP *gateway* bagi semua perangkat *wireless client*, juga dibutuhkan dalam proses konfigurasi sistem *hotspot captive portal* RouterOS MikroTik. Alamat IP yang diberikan sesuai dengan yang terlampir pada topologi jaringan.

```
[admin@R1] > ip address add address=10.2.1.111/24 interface=wlan1
```

Konfigurasi *captive portal* RouterOS MikroTik akan dilakukan secara interaktif agar mempermudah proses konfigurasi.

```
[admin@R1] > ip hotspot setup
```

Penentuan *interface* yang akan digunakan sebagai jalur koneksi *wireless client* saat mengakses sistem *hotspot*, pilih atau ketik "**wlan1**".

```
Select interface to run HotSpot on

hotspot interface: wlan1
```

Penentuan alamat IP yang akan digunakan oleh sistem *hotspot*, ini otomatis akan muncul jika sebelumnya dilakukan konfigurasi alamat IP pada *interface* wlan1.

```
Set HotSpot address for interface

local address of network: 10.2.1.111/24
```

Menentukan apakah akan menerapkan fungsi **SNAT** pada jalur sistem *hotspot* terhadap semua *wireless client* agar bisa terkoneksi ke *internet*, pilih atau ketik "**yes**".

```
masquerade network: yes
```

Menentukan rentang alamat IP yang akan diberikan oleh layanan ***Dynamic Host Configuration Protocol*** (**DHCP**) kepada *wireless client* yang terkoneksi ke sistem *hotspot*, misalnya akan disediakan stok sebanyak 50 alamat IP.

```
Set pool for HotSpot addresses

address pool of network: 10.2.1.1-10.2.1.50
```

Menentukan apakah akan menggunakan sertifikat **SSL**, misalnya jika sistem *hotspot* akan dioperasikan menggunakan layanan **HTTPS** (HTTP *Secure*). Pilih atau ketik "**none**".

```
Select hotspot SSL certificate

select certificate: none
```

Menentukan apakah akan menggunakan layanan SMTP untuk keperluan pengiriman email. Pilih atau ketik "**0.0.0.0**".

```
Select SMTP server

ip address of smtp server: 0.0.0.0
```

Alamat IP DNS secara otomatis akan muncul jika sebelumnya telah dilakukan konfigurasi DNS.

```
Setup DNS configuration

dns servers: 8.8.8.8
```

Menentukan alamat nama yang akan digunakan untuk mengakses sistem *hotspot captive portal* RouterOS MikroTik, alamat ini diakses pada browser di sisi *client*. Misalnya menggunakan alamat nama "**hotspot.pusat-1.net**".

```
DNS name of local hotspot server

dns name: hotspot.pusat-1.net
```

Menentukan nama ***user*** dan ***password*** pertama yang akan digunakan untuk mengakses sistem *hotspot captive portal* agar nantinya dapat terkoneksi ke *internet*.

```
Create local hotspot user
name of local hotspot user: admin
password for the user: 123456
```

Untuk penambahan user akses *hotspot*, ada dua hal yang harus dilakukan.

1. Membuat profil *user hotspot* yang merupakan kategorisasi *user hotspot*, dan akan mengatur beberapa hal penting, misal nama profil, setiap user apakah hanya boleh digunakan untuk satu perangkat saja atau bisa beberapa perangkat sekaligus, hal lainnya adalah apakah koneksi *hotspot* akan dilewatkan pada jalur *web proxy* atau tidak.

   Berikut adalah konfigurasi profil *user hotspot* untuk para staf. Setiap *user hotspot* pada profil staf hanya boleh digunakan oleh satu perangkat saja, dan terhubung ke internet tidak melalui *web proxy*, hal ini dilakukan agar tidak membebani Router R1.

```
[admin@R1] > ip hotspot user profile add name=staf shared-users=1 \
transparent-proxy=no
```

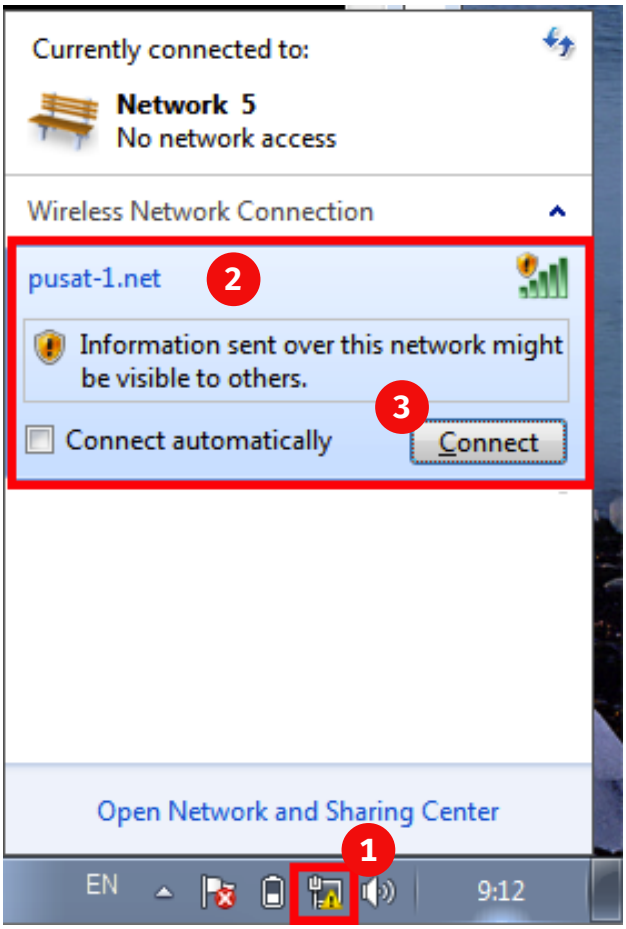
2. Membuat user *hotspot* baru untuk para staf sesuai. Berikut dicontohkan menambah user *hotspot* untuk staf yang bernama "**fulan**" dengan password "**123456**".

```
[admin@R1] > /ip hotspot> user add name=fulan password=123456 \
profile=staf
```

   Untuk user *hotspot* berikutnya tinggal menambahkan dengan perintah serupa sesuai dengan nama (*user*) dan *password* yang akan digunakan oleh para staf saat *login* ke *hotspot*.

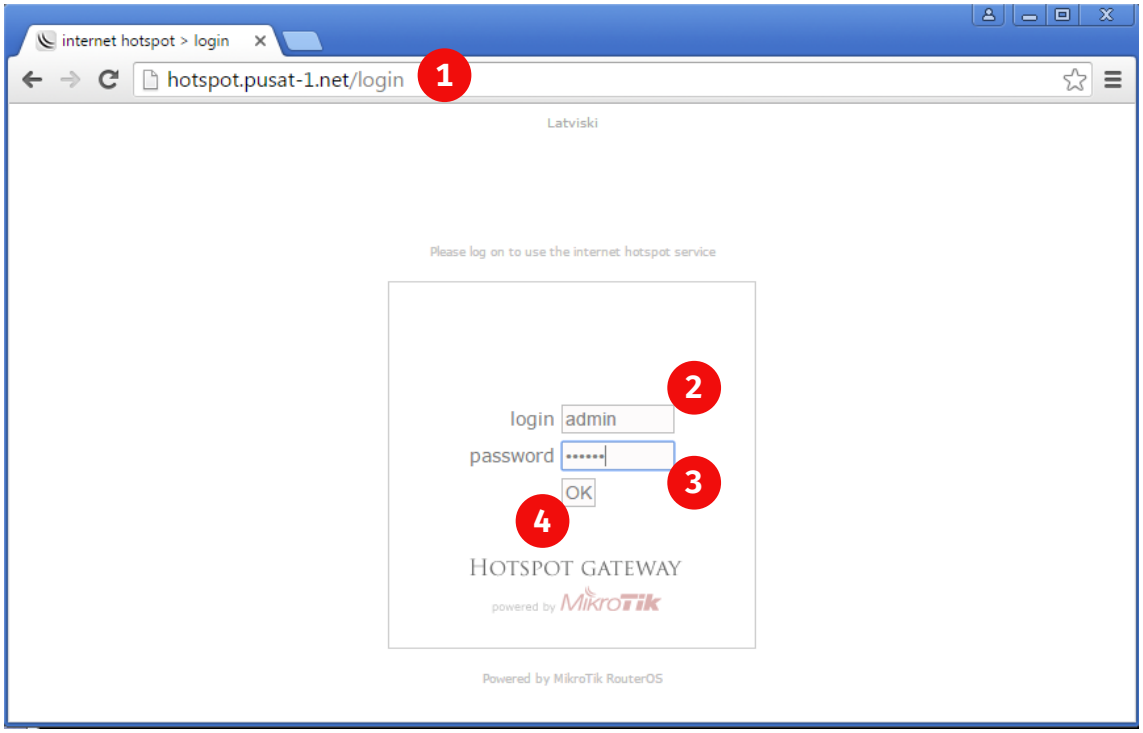
B. Pengujian Koneksi Perangkat Jaringan WLAN

Proses pengujian diawali dengan mengkoneksi *wireless client* ke *wireless* AP. Klik *icon network* di *taskbar client* Windows lalu pilih *wireless* dengan SSID "**pusat-1.net**", kemudian klik tombol "**Connect**" (Gambar 2.2).



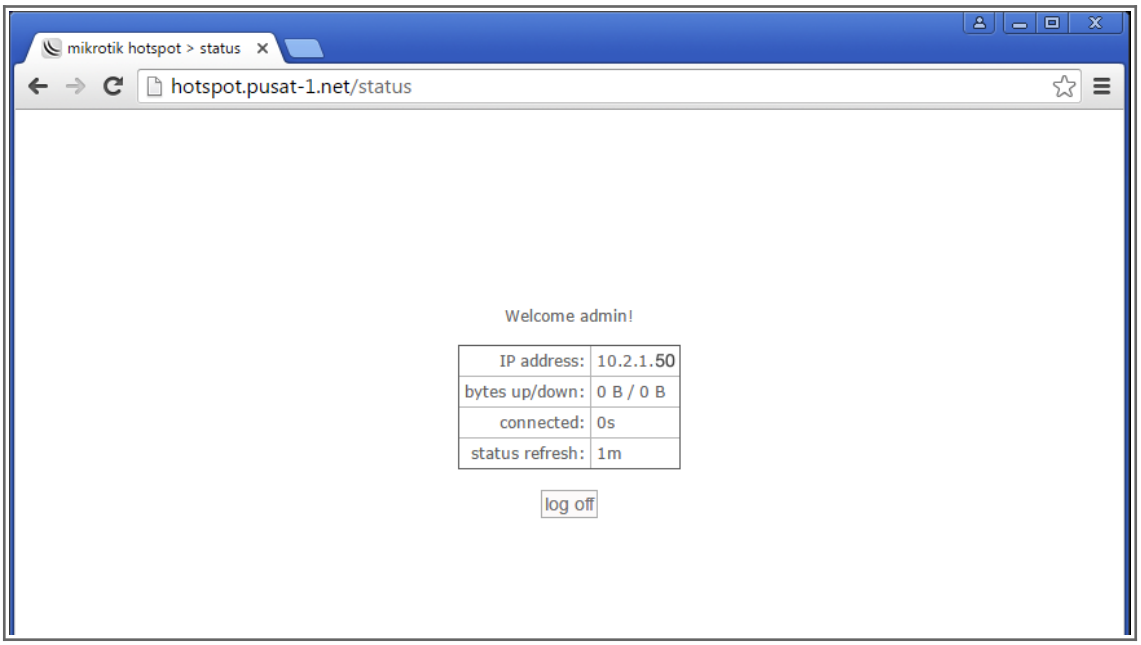
Gambar 2.2. Koneksi *wireless client* ke *wireless* AP

Selanjutnya melakukan login ke sistem *hotspot captive portal* menggunakan browser lalu ketikkan alamat **hotspot.pusat-1.net**, masukkan *user hotspot* yang telah dibuat sebelumnya (user: **admin**, password: **123456**), atau bisa juga menggunakan *user hotspot* lain yang telah didaftarkan sebelumnya.



Gambar 2.3. *Login* ke sistem *hotspot captive portal*

Jika proses *login* berhasil, maka akan tampil seperti gambar 2.4.



Gambar 2.4. Berhasil *login* ke sistem *hotspot captive portal*

Pengujian koneksi berikut dilakukan sebelum melakukan *login* ke sistem *hotspot captive portal*. Hasil pengujian mengindikasikan bahwa *wireless client* gagal terkoneksi ke *internet*, dengan munculnya pesan "**Destination net unreachable**".

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 10.2.1.111: Destination net unreachable.
Reply from 10.2.1.111: Destination net unreachable.
Reply from 10.2.1.111: Destination net unreachable.
Reply from 10.2.1.111: Destination net unreachable.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Berikut adalah hasil pengujian koneksi ke *internet* setelah berhasil melakukan *login* ke sistem *hotspot captive portal*.

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=42ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 43ms

C:\>ping google.com

Pinging google.com [74.125.24.100] with 32 bytes of data:
Reply from 74.125.24.100: bytes=32 time=43ms TTL=52
Reply from 74.125.24.100: bytes=32 time=44ms TTL=52
Reply from 74.125.24.100: bytes=32 time=42ms TTL=52
Reply from 74.125.24.100: bytes=32 time=43ms TTL=52

Ping statistics for 74.125.24.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 43ms
```

Tahap 3
Koneksi Komputer Client ke Server

PT. **ABC**Net (Jakarta) memiliki komputer *server* yang berisi *website* yang nantinya dapat diakses dari jaringan LAN dan WLAN (Gambar 3.1). Komputer *server* ini akan diletakkan di area **DMZ** (***De-Militerized Zone***), sehingga akses baik yang berasal dari jaringan lokal maupun jaringan *internet* akan dapat dikontrol oleh *firewall* yang ada di RouterBoard (R1) MikroTik. Pada tahap ini hanya fokus ada pada koneksi dari komputer *client* ke *server* saja, untuk masalah *firewall* akan dibahas pada tahap keamanan jaringan.

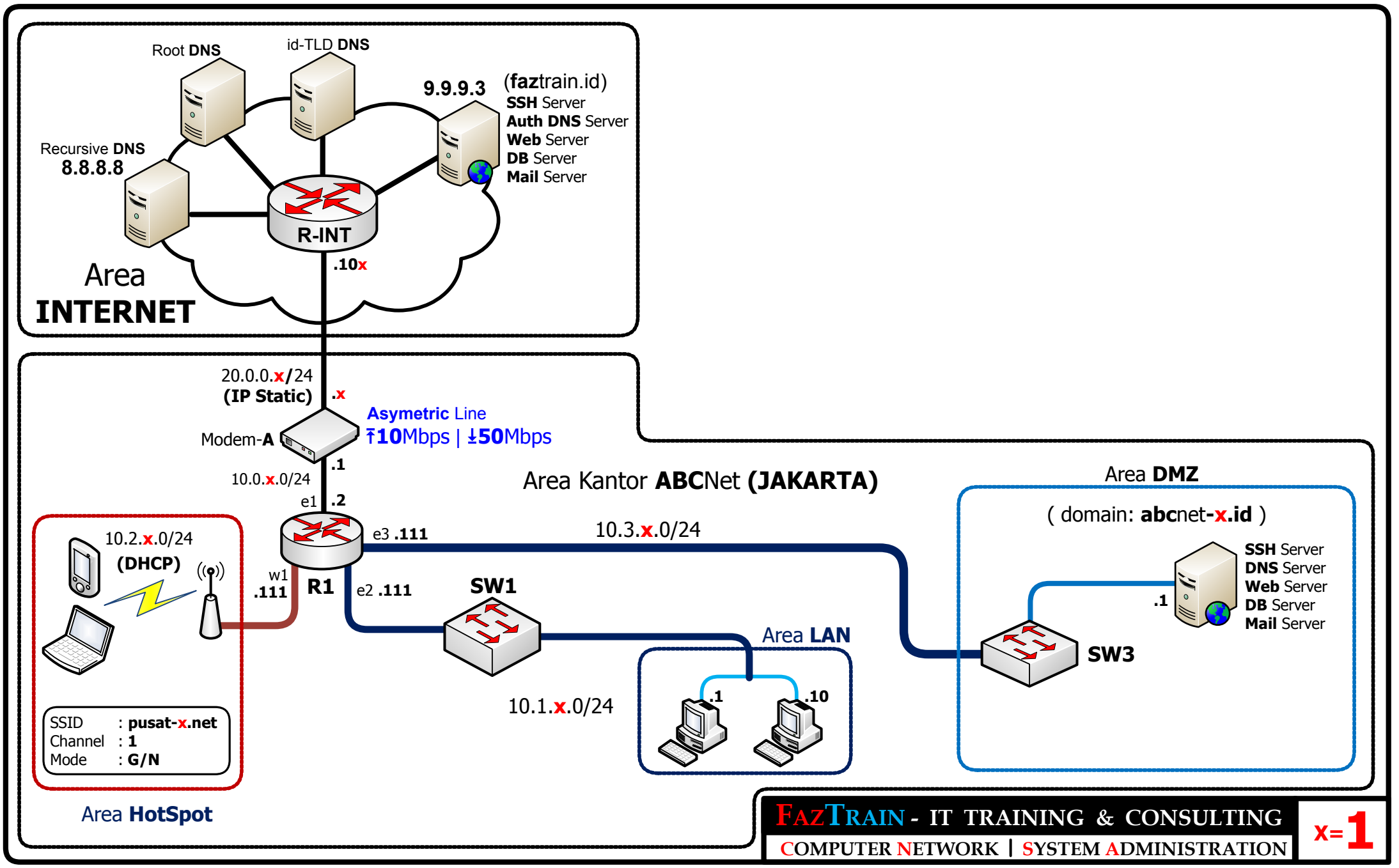
Karena buku kerja ini hanya fokus membahas area *Network Administrator*, maka tahapan konfigurasi di sisi komputer *server* tidak dibahas, karena pembahasan tersebut akan dilakukan pada buku kerja *System Administrator*. Selain dapat diakses dari komputer *client*, komputer *server* juga dapat terkoneksi ke *internet*. Berikut adalah tahapan konfigurasi dan pengujian yang akan dilakukan pada Router (R1).

A. Konfigurasi Router (R1)

Sesuai pada topologi jaringan yang ada di halaman berikutnya, maka komputer *server* akan dikoneksikan ke Router (R1) pada *interface* ether3 (e3). Hal-hal yang akan dikonfigurasi antara lain:

1. Mengganti nama *interface* "**ether3**" menjadi "**ether3-Server**" agar mudah diidentifikasi. Tampilkan terlebih dahulu daftar *interface* pada RouterOS untuk mengetahui urutan *interface* "ether3" dalam daftar.

```
[admin@R1] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#    NAME            TYPE   ACTUAL-MTU   L2MTU   MAX-L2MTU
0  R ether1-Internet ether         1500    1598        2028
1  R ether2-LAN      ether         1500    1598        2028
2    ether3          ether         1500    1598        2028
3    ether4          ether         1500    1598        2028
4    ether5          ether         1500    1598        2028
```


Root DNS
id-TLD DNS
9.9.9.3
(faztrain.id)
SSH Server
Auth DNS Server
Web Server
DB Server
Mail Server
Recursive DNS
8.8.8.8
R-INT
.10x
Area
INTERNET
20.0.0.x/24
(IP Static)
.x
Asymetric Line
↑10Mbps | ↓50Mbps
Modem-A
.1
10.0.x.0/24
e1
.2
Area Kantor ABCNet (JAKARTA)
Area DMZ
(domain: abcnet-x.id)
10.2.x.0/24
(DHCP)
w1
.111
R1
e3 .111
10.3.x.0/24
e2 .111
SW1
SSH Server
DNS Server
Web Server
DB Server
Mail Server
.1
SW3
Area LAN
.1
.10
10.1.x.0/24
SSID : pusat-x.net
Channel : 1
Mode : G/N
Area HotSpot
FAZTRAIN - IT TRAINING & CONSULTING
COMPUTER NETWORK | SYSTEM ADMINISTRATION
X=1

Setelah mengetahui urutan "ether3" dalam daftar, kemudian ubah nama interface "**ether3**" menjadi "**ether3-Server**".

```
[admin@R1] > interface set 2 name=ether3-Server
```

2. Menentukan alamat IP untuk *interface* ether3-Server agar nantinya dapat dijadikan sebagai alamat IP *gateway* bagi komputer *server* untuk terkoneksi ke jaringan *internet* dan terkoneksi ke jaringan LAN serta WLAN.

```
[admin@R1] > ip address add address=10.3.1.111/24 interface=ether3-Server
```

3. Mengaktifkan fungsi **SNAT** pada Router (R1) agar komputer *server* dapat terkoneksi ke *internet*.

```
[admin@R1] > ip firewall nat add chain=srcnat src-address=10.3.1.0/24 \
out-interface=ether1-Internet action=masquerade comment="Sharing \
Internet untuk Area Server"
```

4. Agar komputer *client* di LAN dan WLAN dapat mengakses *server* menggunakan alamat nama domain, maka pada Router (R1) dapat memanfaatkan fitur manipulasi **DNS Cache** lewat **DNS Static** untuk ditambahkan penerjemahan alamat nama domain **abcnet-1.id** ke alamat IP lokal **10.3.1.1** dari *web server* di kantor pusat.

```
[admin@R1] > ip dns static add name=abcnet-1.id address=10.3.1.1
[admin@R1] > ip dns static add name=www.abcnet-1.id address=10.3.1.1
```

B. Pengujian Koneksi dari Client ke Server

Pengujian koneksi dari komputer client LAN dan WLAN ke server bisa dilakukan dengan tiga cara, yaitu dengan PING, *Port Scanner* (NMAP) dan aplikasi *browser*.

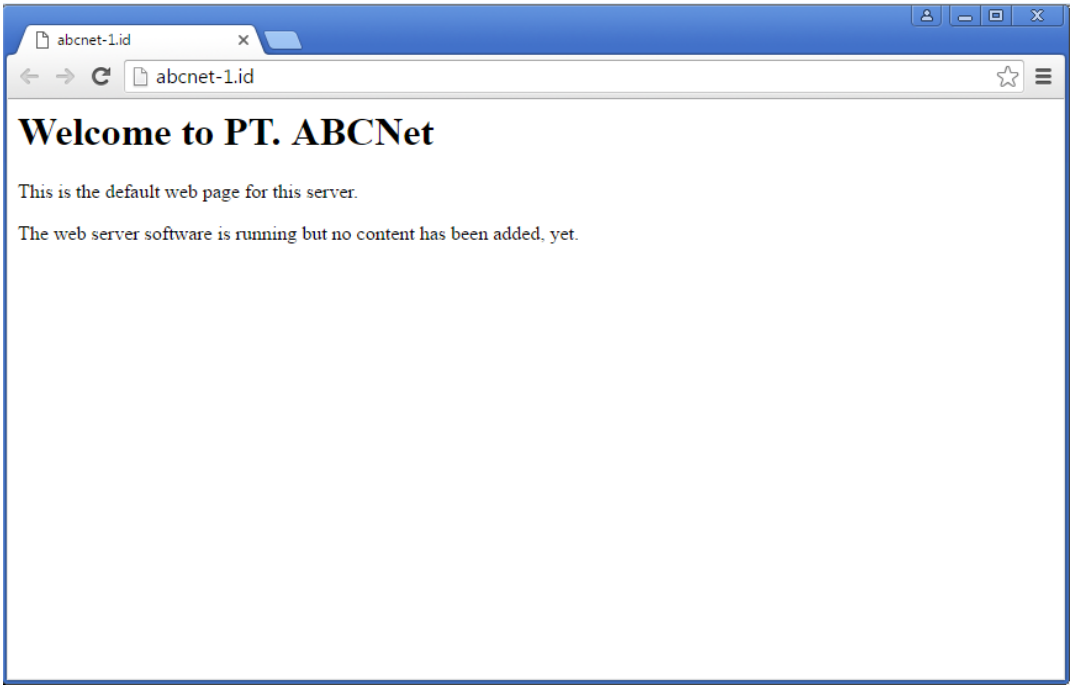
1. Pengujian koneksi menggunakan PING dari *client* ke *server*.

```
C:\>ping 10.3.1.1

Pinging 10.3.1.1 with 32 bytes of data:
Reply from 10.3.1.1: bytes=32 time=2ms TTL=63
Reply from 10.3.1.1: bytes=32 time=1ms TTL=63
Reply from 10.3.1.1: bytes=32 time=1ms TTL=63
Reply from 10.3.1.1: bytes=32 time=1ms TTL=63

Ping statistics for 10.3.1.1:

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

C:\>ping abcnet-1.id

Pinging abcnet-1.id [10.3.1.1] with 32 bytes of data:
Reply from 10.3.1.1: bytes=32 time=2ms TTL=63
Reply from 10.3.1.1: bytes=32 time=1ms TTL=63
Reply from 10.3.1.1: bytes=32 time=1ms TTL=63
Reply from 10.3.1.1: bytes=32 time=1ms TTL=63

Ping statistics for 10.3.1.1:

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

2. Pengujian koneksi terhadap ketersediaan layanan menggunakan aplikasi ***Port Scanner*** (misal, NMAP), pastikan telah menginstal aplikasi NMAP sebelumnya. Aplikasi NMAP akan menampilkan daftar alamat *port* yang mewakili jenis layanan tertentu, misal *port* 22 untuk layanan SSH, *port* 53 untuk layanan DNS, *port* 80 untuk layanan web.

```
C:\>nmap abcnet-1.id
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for abcnet-1.id (10.3.1.1)
Host is up (0.00026s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
```

3. Pengujian dengan akses langsung ke layanan *server* menggunakan aplikasi di sisi *client*, misal menggunakan *browser* (Gambar 3.2).



Gambar 3.2. Pengujian akses layanan web dari browser client

Tahap 4
Koneksi Jaringan Kantor Cabang ke Server Pusat

PT. **ABC**Net memiliki kantor cabang yang berlokasi di **Palopo**. Di kantor cabang Palopo akan dibangun jaringan LAN dan WLAN serta akan dikoneksikan ke *internet* dan ke jaringan kantor pusat PT. **ABC**Net (Jakarta). Topologi jaringan (Gambar 4.1) di kantor cabang Palopo pada dasarnya serupa dengan kantor pusat. Kantor cabang PT. **ABC**Net (Palopo) berlangganan koneksi *internet* dengan kecepatan *upload* sebesar **5Mbps** dan kecepatan *download* sebesar 20Mbps, dengan fasilitas alamat IP publik dinamis.

Tahapan instalasi dan konfigurasi jaringan di kantor cabang juga serupa dengan kantor pusat, hanya beberapa bagian yang perlu penyesuaian, terutama dari sisi penggunaan alamat IP. Berikut adalah tahapan konfigurasi dan pengujian yang akan dilakukan.

A. Koneksi Jaringan LAN Kantor Cabang (Palopo) ke Internet

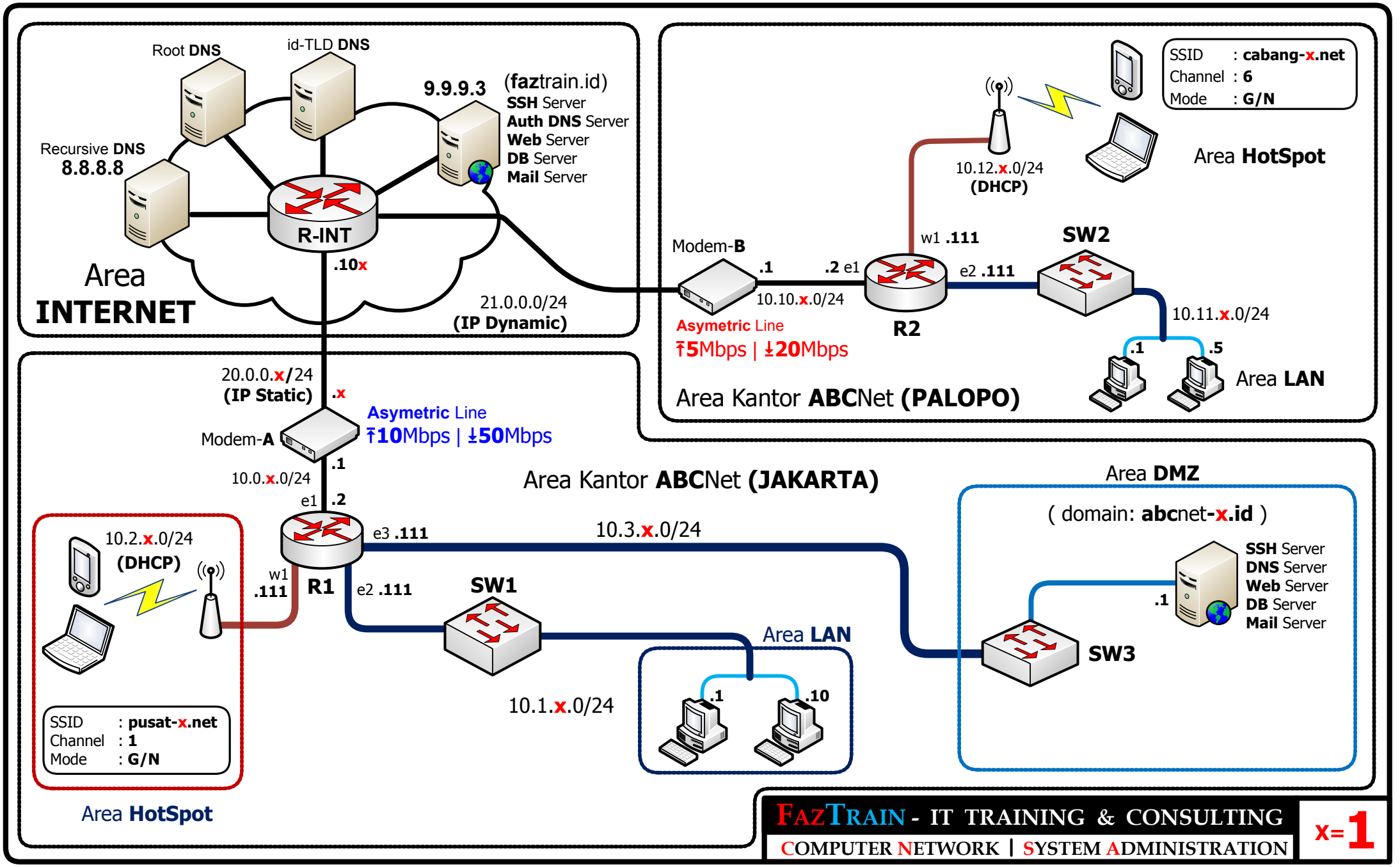
Sesuai pada topologi jaringan yang ada di halaman berikutnya, maka tahap awal proses konfigurasi dimulai dari mengkoneksikan Router (R2) agar dapat dikoneksikan ke *internet*. Pastikan Router (R2) juga telah di-*reset* agar semua konfigurasi bawaan RouterBoard ditiadakan untuk kemudahan dan kelancaran proses konfigurasi.

1. Konfigurasi identitas Router (R2)

```
[admin@MikroTik] > system identity set name=R2
```

2. Konfigurasi *interface* jaringan

```
[admin@R2] > interface set 0 name=ether1-Internet
[admin@R2] > interface set 1 name=ether2-LAN
```


Root DNS
id-TLD DNS
9.9.9.3
(faztrain.id)
SSH Server
Auth DNS Server
Web Server
DB Server
Mail Server
Recursive DNS
8.8.8.8
R-INT
.10x
Area
INTERNET
21.0.0.0/24
(IP Dynamic)
SSID : cabang-x.net
Channel : 6
Mode : G/N
10.12.x.0/24
(DHCP)
Area HotSpot
Modem-B
.1
.2 e1
10.10.x.0/24
Asymetric Line
↑5Mbps | ↓20Mbps
w1 .111
R2
SW2
e2 .111
10.11.x.0/24
.1
.5
Area LAN
Area Kantor ABCNet (PALOPO)
20.0.0.x/24
(IP Static)
.x
Modem-A
Asymetric Line
↑10Mbps | ↓50Mbps
.1
10.0.x.0/24
e1 .2
Area Kantor ABCNet (JAKARTA)
Area DMZ
(domain: abcnet-x.id)
10.2.x.0/24
(DHCP)
w1
.111
R1
e3 .111
10.3.x.0/24
e2 .111
SW1
SSH Server
DNS Server
Web Server
DB Server
Mail Server
.1
SW3
Area LAN
10.1.x.0/24
.1
.10
SSID : pusat-x.net
Channel : 1
Mode : G/N
Area HotSpot
FAZTRAIN - IT TRAINING & CONSULTING
COMPUTER NETWORK | SYSTEM ADMINISTRATION
x=1

3. Konfigurasi alamat IP

```
[admin@R2] > ip address add address=10.10.1.2/24 interface=ether1-Internet
[admin@R2] > ip address add address=10.11.1.111/24 interface=ether1-LAN
```

4. Konfigurasi *Routing*

```
[admin@R2] > ip route add dst-address=0.0.0.0/0 gateway=10.10.1.1
```

5. Konfigurasi DNS *Client*

```
[admin@R2] > ip dns set servers=8.8.8.8 allow-remote-requests=yes
```

6. Konfigurasi NTP *Client*

```
[admin@R2] > system ntp client set enabled=yes \
primary-ntp=id.pool.ntp.org
[admin@R2] > system clock set time-zone-autodetect=no \
time-zone-name=Asia/Makassar
```

7. Konfigurasi SNAT

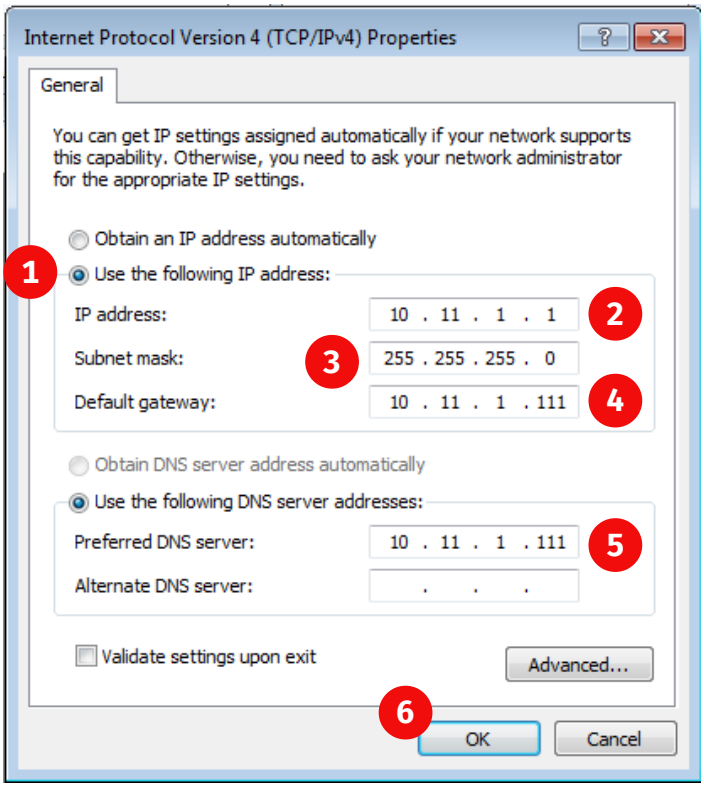
```
[admin@R2] > ip firewall nat add chain=srcnat src-address=10.11.1.0/24 \
out-interface=ether1-Internet action=masquerade comment="Sharing \
Internet untuk Area LAN"
```

8. Pengujian koneksi Router (R2) ke jaringan *internet*

```
[admin@R1] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56  52 44ms
    1 8.8.8.8                                    56  52 43ms
    2 8.8.8.8                                    56  52 45ms
    3 8.8.8.8                                    56  52 42ms

[admin@R1] > ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 74.125.24.100                              56  52 45ms
    1 74.125.24.100                              56  52 43ms
    2 74.125.24.100                              56  52 46ms
    3 74.125.24.100                              56  52 44ms
```

Selanjutnya adalah konfigurasi dan pengujian di sisi *client* LAN.

1. Konfigurasi alamat IP *client* LAN



Gambar 4.2. Konfigurasi alamat IP di *client* (Windows)

2. Pengujian koneksi dari *client* LAN ke *internet*

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=45ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53
Reply from 8.8.8.8: bytes=32 time=42ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

C:\>ping google.com

Pinging google.com [74.125.24.100] with 32 bytes of data:
Reply from 74.125.24.100: bytes=32 time=41ms TTL=52
Reply from 74.125.24.100: bytes=32 time=43ms TTL=52
Reply from 74.125.24.100: bytes=32 time=45ms TTL=52
Reply from 74.125.24.100: bytes=32 time=44ms TTL=52

Ping statistics for 74.125.24.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

B. Koneksi Jaringan WLAN Kantor Cabang (Palopo) ke Internet

Berikut adalah tahapan konfigurasi WLAN sekaligus sistem *hotspot captive portal*.

Konfigurasi diawali dengan mengaktifkan *interface wireless*.

```
[admin@R1] > interface wireless enable wlan1
```

Selanjutnya mengkonfigurasi interface wireless sesuai petunjuk pada topologi jaringan, SSID: "**cabang-1.net**" dengan frekuensi kerja **2,437GHz** (setara dengan *Channel* 6).

```
[admin@R1] > interface wireless set 0 master-interface=wlan1 \
mode=ap-bridge ssid=cabang-1.net band=2ghz-g/n frequency=2437 \
channel-width=20mhz security-profile=default
```

Selanjutnya melakukan konfigurasi alamat IP untuk *interface* wlan1, selain alamat IP berguna sebagai alamat IP *gateway* bagi semua perangkat *wireless client*, juga dibutuhkan dalam proses konfigurasi sistem *hotspot captive portal* RouterOS MikroTik. Alamat IP yang diberikan sesuai dengan yang terlampir pada topologi jaringan.

```
[admin@R1] > ip address add address=10.12.1.111/24 interface=wlan1
```

Konfigurasi *captive portal* RouterOS MikroTik akan dilakukan secara interaktif agar mempermudah proses konfigurasi.

```
[admin@R1] > ip hotspot setup
```

Penentuan *interface* yang akan digunakan sebagai jalur koneksi *wireless client* saat mengakses sistem *hotspot*, pilih atau ketik "**wlan1**".

```
Select interface to run HotSpot on

hotspot interface: wlan1
```

Penentuan alamat IP yang akan digunakan oleh sistem hotspot, ini otomatis akan muncul jika sebelumnya dilakukan konfigurasi alamat IP pada interface wlan1.

```
Set HotSpot address for interface
local address of network: 10.12.1.111/24
```

Menentukan apakah akan menerapkan fungsi **SNAT** pada jalur sistem *hotspot* terhadap semua *wireless client* agar bisa terkoneksi ke internet, pilih atau ketik "**yes**".

```
masquerade network: yes
```

Menentukan rentang alamat IP yang akan diberikan oleh layanan ***Dynamic Host Configuration Protocol*** (**DHCP**) kepada *wireless client* yang terkoneksi ke sistem *hotspot*, misalnya akan disediakan stok sebanyak 20 alamat IP.

```
Set pool for HotSpot addresses
address pool of network: 10.12.1.1-10.12.1.20
```

Menentukan apakah akan menggunakan sertifikat **SSL**, misalnya jika sistem *hotspot* akan dioperasikan menggunakan layanan **HTTPS** (HTTP *Secure*). Pilih atau ketik "**none**".

```
Select hotspot SSL certificate
select certificate: none
```

Menentukan apakah akan menggunakan layanan SMTP untuk keperluan pengiriman email. Pilih atau ketik "**0.0.0.0**".

```
Select SMTP server
ip address of smtp server: 0.0.0.0
```

Alamat IP DNS akan secara otomatis terisi jika sebelumnya telah dilakukan konfigurasi alamat IP DNS.

```
Setup DNS configuration
dns servers: 8.8.8.8
```

Menentukan alamat nama yang akan digunakan untuk mengakses sistem *hotspot captive portal* RouterOS MikroTik, alamat ini diakses pada browser di sisi *client*. Misalnya menggunakan alamat nama "**hotspot.cabang-1.net**".

```
DNS name of local hotspot server
dns name: hotspot.cabang-1.net
```

Menentukan nama ***user*** dan ***password*** pertama yang akan digunakan untuk mengakses sistem *hotspot captive portal* agar nantinya dapat terkoneksi ke *internet*.

```
Create local hotspot user
name of local hotspot user: admin
password for the user: 123456
```

Untuk penambahan user akses hotspot, juga ada dua hal yang harus dilakukan.

1. Membuat profil *user hotspot* pada Router R2

   Berikut adalah konfigurasi profil *user hotspot* untuk para staf. Setiap *user hotspot* pada profil staf hanya boleh digunakan oleh satu perangkat saja, dan terhubung ke internet tidak melalui *web proxy*, hal ini dilakukan agar tidak membebani Router R2.

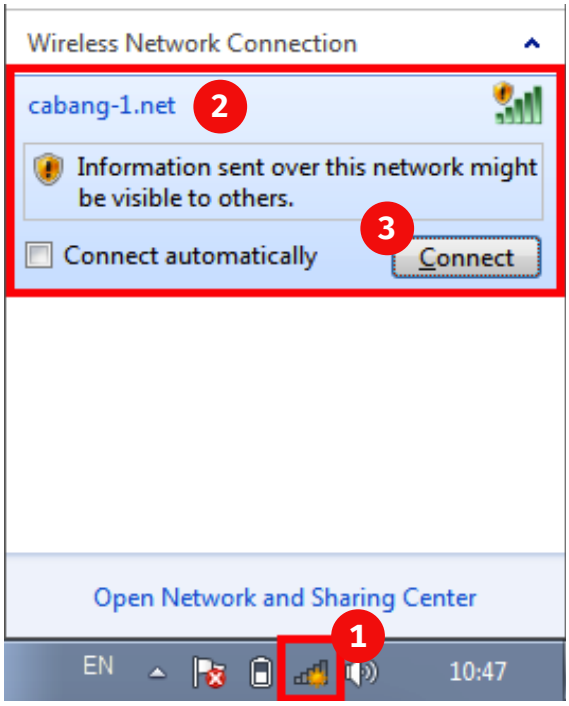
```
[admin@R2] > ip hotspot user profile add name=staf shared-users=1 \
transparent-proxy=no
```

2. Membuat *user hotspot* baru untuk para staf sesuai. Berikut dicontohkan menambah *user hotspot* untuk staf yang bernama "**fulanah**" dengan password "**123456**".

```
[admin@R2] > /ip hotspot> user add name=fulanah password=123456 \
profile=staf
```

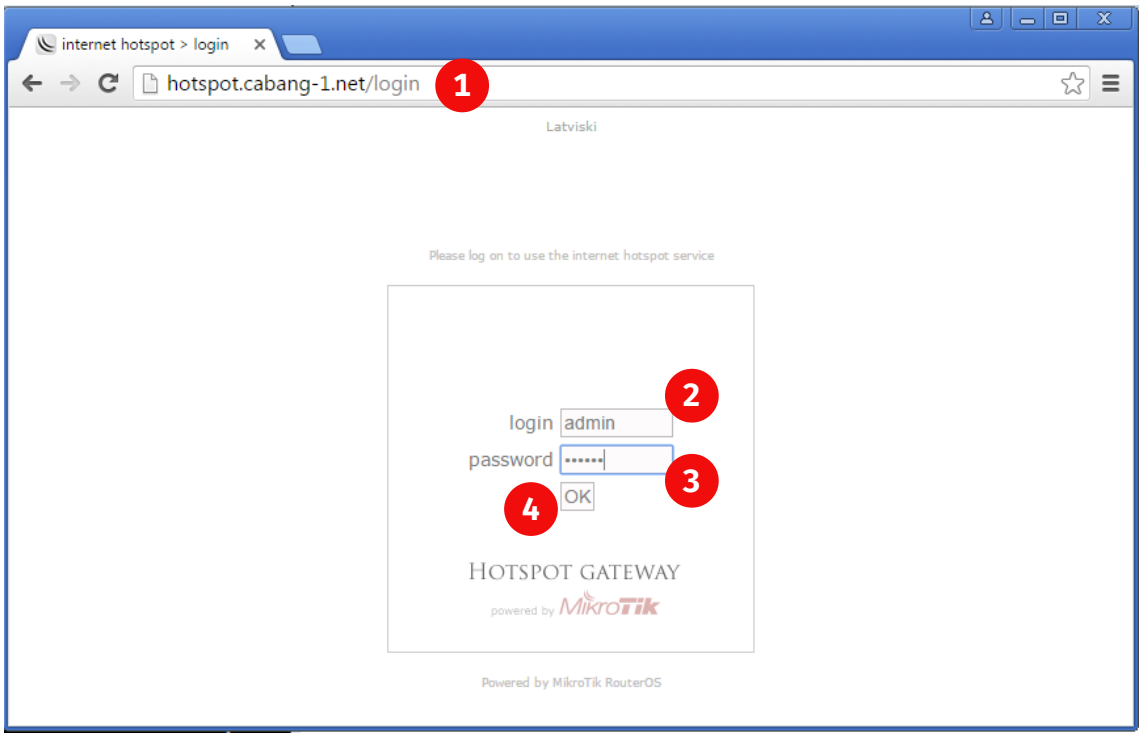
C. Pengujian Koneksi Perangkat Jaringan WLAN

Proses pengujian diawali dengan mengkoneksi *wireless client* ke *wireless* AP. Klik *icon network* di *taskbar* lalu pilih *wireless* dengan SSID "**cabang-1.net**", kemudian klik tombol "**Connect**" (Gambar 4.3).



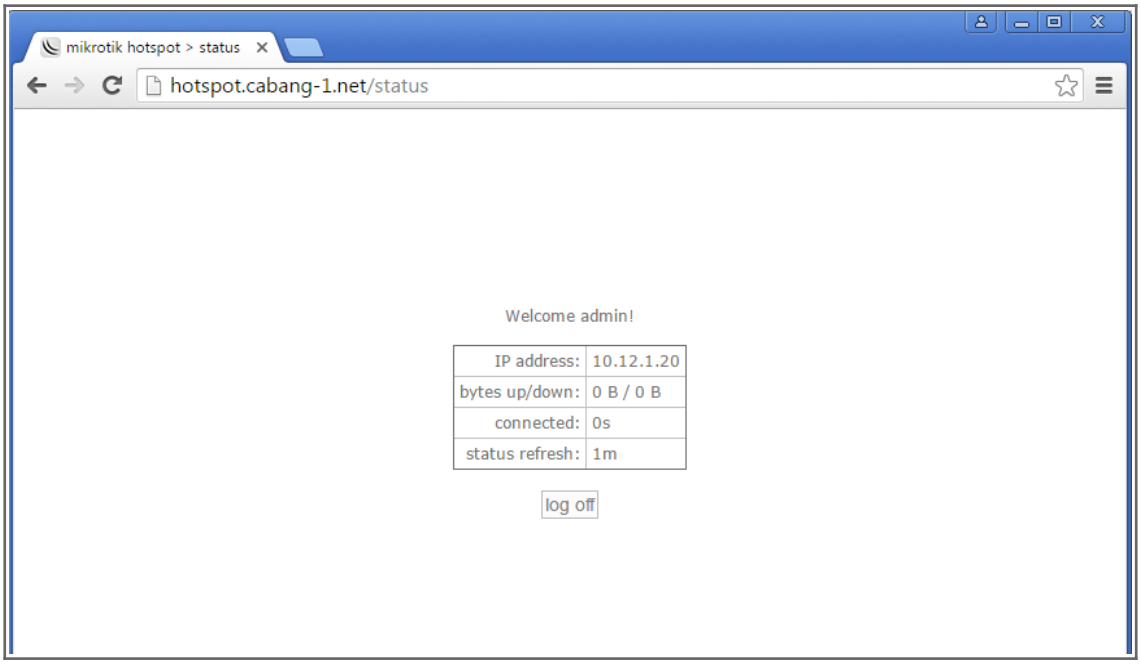
Gambar 4.3. Koneksi *wireless client* ke *wireless* AP

Selanjutnya melakukan login ke sistem *hotspot captive portal* menggunakan akun yang telah dibuat sebelumnya (user: **admin**, password: **123456**) seperti tampak pada gambar 4.4.



Gambar 4.4. *Login* ke sistem *hotspot captive portal*

Jika proses *login* berhasil, maka akan tampil seperti gambar 4.5.



Gambar 4.5. Berhasil *login* ke sistem *hotspot captive portal*

Berikut adalah hasil pengujian koneksi ke *internet* setelah berhasil melakukan *login* ke sistem *hotspot captive portal*.

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53
Reply from 8.8.8.8: bytes=32 time=44ms TTL=53
Reply from 8.8.8.8: bytes=32 time=42ms TTL=53
Reply from 8.8.8.8: bytes=32 time=43ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 43ms

C:\>ping google.com

Pinging google.com [74.125.24.100] with 32 bytes of data:
Reply from 74.125.24.100: bytes=32 time=43ms TTL=52
Reply from 74.125.24.100: bytes=32 time=44ms TTL=52
Reply from 74.125.24.100: bytes=32 time=42ms TTL=52
Reply from 74.125.24.100: bytes=32 time=43ms TTL=52

Ping statistics for 74.125.24.100:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 43ms
```

C. Koneksi Jaringan Kantor Cabang (Palopo) ke Server Kantor Pusat

Pada tahap ini, komputer-komputer *client* di jaringan kantor cabang (Palopo) harus dapat terhubung ke komputer *server* yang ada di kantor pusat (Jakarta). Dari proses konfigurasi sebelumnya di area kantor cabang yang telah terkoneksi *internet*, sebenarnya otomatis juga sudah dapat terkoneksi ke area kantor pusat, namun hanya sampai di perangkat Router (R1) saja, untuk masuk sampai ke jaringan lokal belum bisa dilakukan, hal ini karena di jaringan internet tidak ada satupun perangkat dengan alamat IP publik yang dirutekan (*routing*) ke area jaringan lokal dengan alamat IP *private*. Oleh karena itu perlu teknik tertentu yang memungkinkan agar koneksi dari jaringan internet dapat diteruskan ke area jaringan lokal, misal ditujukan ke *server* yang ada di kantor pusat.

Teknik yang akan digunakan agar koneksi dari jaringan internet dapat diteruskan ke komputer di area jaringan lokal adalah ***Destination* NAT** (**DNAT**). Pada topologi jaringan nampak bahwa Router (R1) terhubung ke *internet* melewati Modem-A, pada kondisi ini yang memperoleh alamat IP publik sebenarnya adalah Modem-A, artinya posisi Router (R1) berada di area lokal. Untuk itu pada Modem-A terlebih dahulu harus diaktifkan fungsi **DNAT**, umumnya fungsi DNAT pada modem dikenal dengan istilah **DMZ** (***De-Militerized Zone***) atau bisa juga menggunakan fitur ***Port Forwarding***, namun cara termudah meneruskan koneksi dari internet menuju area jaringan lokal pada *modem* adalah dengan menggunakan fitur DMZ.

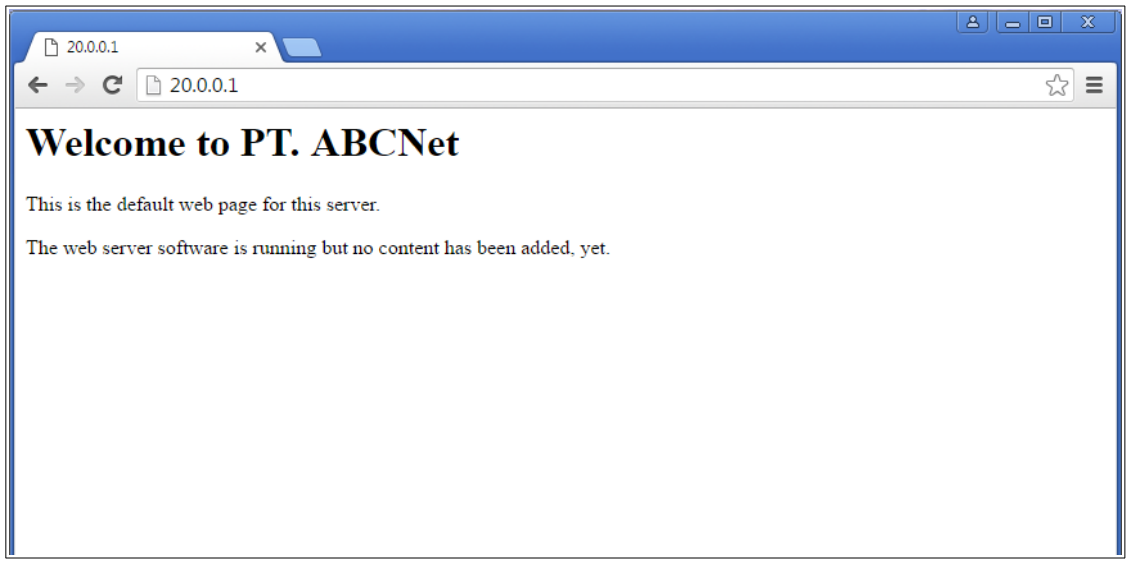
Pada skenario ini, *modem* telah diaktifkan fitur DMZ, sehingga semua koneksi dari *internet* akan diteruskan ke Router (R1). Maka pada tahap selanjutnya tinggal mengaktifkan fungsi DNAT pada Router (R1) agar dapat meneruskan koneksi ke *server* di kantor pusat. Layanan yang akan diakses pada *server* dari kantor cabang adalah layanan "**Web**", namun karena untuk mengakses layanan tersebut harus menggunakan alamat nama domain, maka dalam proses komunikasi juga harus melibatkan layanan **DNS**. Satu layanan lagi yang harus diteruskan oleh Router (R1) ke *server* adalah layanan *email* SMTP, ini dibutuhkan untuk komunikasi *server email* yang ada di *internet* ke *server email* milik PT. **ABC**Net. Ketika memasukkan baris

perintah DNAT pada RouterOS MikroTik, kedua layanan tersebut harus diwakili dengan nomor *port*, dalam hal ini untuk layanan *web* diwakili dengan nomor ***port* 80** pada protokol **TCP**, layanan *email* **SMTP** dengan nomor *port* **25** pada protokol TCP, sedang layanan DNS diwakili dengan nomor ***port* 53** pada protokol **UDP**. Berikut adalah konfigurasi untuk mengaktifkan fungsi DNAT untuk ketiga layanan tersebut. Untuk layanan lain tinggal membuat aturan serupa dengan alamat nomor port sesuai layanan, misal untuk layanan **SSH** dengan nomor port **22**, layanan *web* **HTTP** dengan nomor port **443**, keduanya ada pada protokol **TCP**.

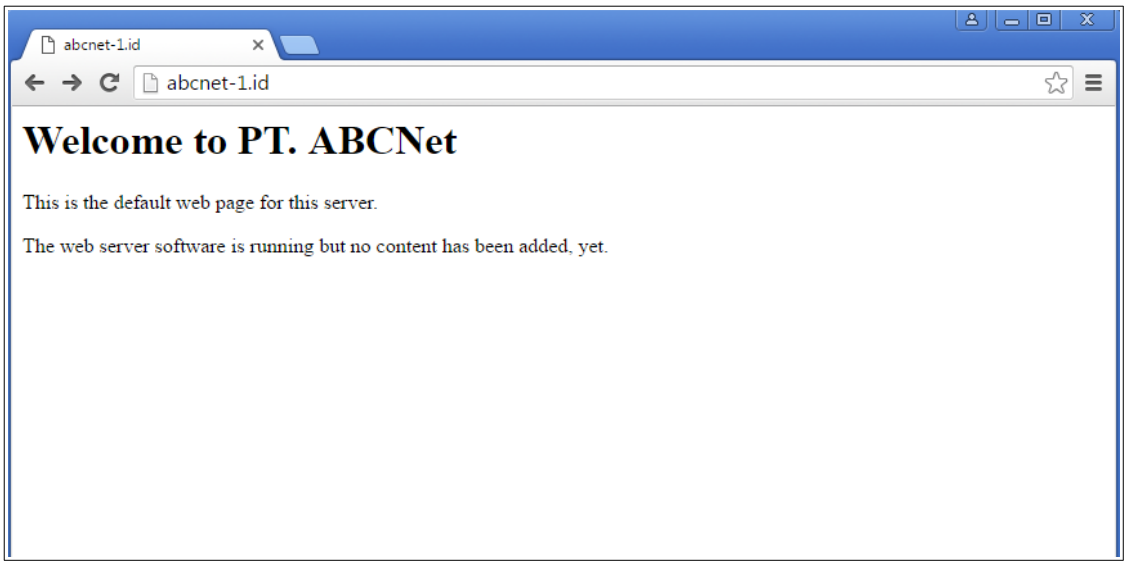
```
[admin@R1] > ip firewall nat add chain=dstnat protocol=tcp dst-port=25 \
in-interface=ether1-Internet action=dst-nat to-addresses=10.3.1.1 to-ports=25

[admin@R1] > ip firewall nat add chain=dstnat protocol=tcp dst-port=80 \
in-interface=ether1-Internet action=dst-nat to-addresses=10.3.1.1 to-ports=80

[admin@R1] > ip firewall nat add chain=dstnat protocol=udp dst-port=53 \
in-interface=ether1-Internet action=dst-nat to-addresses=10.3.1.1 to-ports=53
```

Untuk pengujian akses ke layanan DNS bisa dengan melakukan PING ke alamat nama domain dari PT. **ABC**Net (abcnet-1.id), sedang untuk menguji akses ke layanan web harus menggunakan browser pada komputer *client* yang ada di kantor cabang (Gambar 4.6 dan 4.7).

```
C:\>ping abcnet-1.id

Pinging abcnet-1.id [20.0.0.1] with 32 bytes of data:
Reply from 20.0.0.1: bytes=32 time=43ms TTL=52
Reply from 20.0.0.1: bytes=32 time=44ms TTL=52
Reply from 20.0.0.1: bytes=32 time=41ms TTL=52
Reply from 20.0.0.1: bytes=32 time=42ms TTL=52
```



Gambar 4.6. Menguji akses layanan web dengan alamat IP



Gambar 4.7. Menguji akses layanan web dengan alamat nama domain

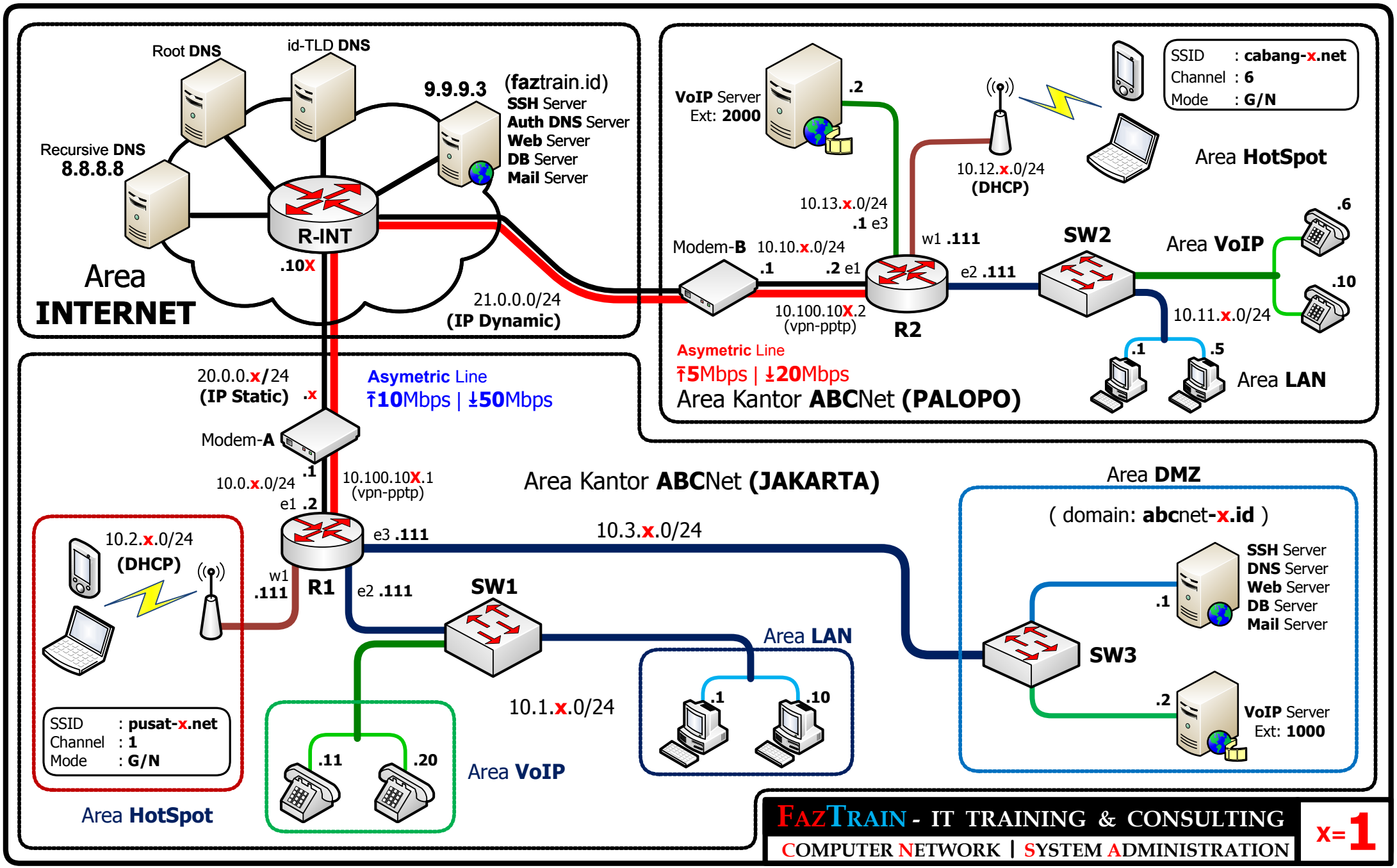
Tahap 5
Koneksi VoIP Kantor Cabang dan Pusat

PT. **ABC**Net membutuhkan layanan komunikasi telepon (suara) di internal perusahaan, terutama komunikasi antara kantor cabang dengan kantor pusat. Untuk kebutuhan ini maka ditentukanlah akan menggunakan layanan ***Voice over IP*** (VoIP). Untuk efisiensi penggunaan *bandwidth internet*, maka diputuskan bahwa baik kantor pusat dan kantor cabang akan memiliki *server* VoIP masing-masing. *Bandwidth internet* baru akan terpakai jika komunikasi VoIP terjadi antara kantor cabang dan kantor pusat, namun jika komunikasi yang terjadi hanya di internal kantor pusat atau kantor cabang, maka sama sekali tidak menggunakan koneksi *internet*.

Target di tahap ini adalah memastikan bahwa *client* VoIP baik di kantor pusat dan kantor cabang sudah dapat terkoneksi ke *server* VoIP masing-masing secara lokal maupun terkoneksi antar *server* VoIP. Pengujian bisa menggunakan PING atau aplikasi *client* VoIP seperti X-Lite, LinPhone atau Zoiper, baik di *notebook* maupun di *smartphone*. Diasumsikan bahwa semua perangkat VoIP (*server* dan *client*) telah dilakukan instalasi sesuai dengan topologi jaringan di halaman berikutnya, maka tahapan berikutnya adalah mengkonfigurasi Router (R1) di kantor pusat dan Router (R2) di kantor cabang.

A. Konfigurasi Router (R1) di Kantor Pusat

Pada tahap sebelumnya Router (R1) telah dikonfigurasi sesuai kebutuhan, sehingga untuk kebutuhan koneksi VoIP di internal kantor pusat cukup melakukan konfigurasi di sisi *server* dan *client* VoIP saja di kantor pusat, konfigurasi server dan client VoIP akan dilakukan oleh VoIP *Admin*, sehingga tidak dibahas di buku kerja Network Administrator, melainkan di buku kerja VoIP Administrator. Pada tahap ini, di area kantor pusat cukup melakukan konfigurasi VPN *server* untuk membuat koneksi privat antara *server* VoIP di kantor cabang dan kantor pusat.


Root DNS
id-TLD DNS
9.9.9.3
(faztrain.id)
SSH Server
Auth DNS Server
Web Server
DB Server
Mail Server
Recursive DNS
8.8.8.8
R-INT
.10X
Area
INTERNET
21.0.0.0/24
(IP Dynamic)
VoIP Server
Ext: 2000
.2
10.13.x.0/24
.1 e3
10.12.x.0/24
(DHCP)
SSID : cabang-x.net
Channel : 6
Mode : G/N
Area HotSpot
Modem-B
10.10.x.0/24
.1
.2 e1
10.100.10X.2
(vpn-pptp)
R2
w1 .111
e2 .111
SW2
Area VoIP
.6
.10
10.11.x.0/24
.1
.5
Area LAN
Asymetric Line
↑5Mbps | ↓20Mbps
Area Kantor ABCNet (PALOPO)
20.0.0.x/24
(IP Static)
.x
Asymetric Line
↑10Mbps | ↓50Mbps
Modem-A
.1
10.0.x.0/24
e1 .2
10.100.10X.1
(vpn-pptp)
Area Kantor ABCNet (JAKARTA)
Area DMZ
(domain: abcnet-x.id)
10.2.x.0/24
(DHCP)
w1
.111
R1
e3 .111
10.3.x.0/24
e2 .111
SW1
SW3
SSH Server
DNS Server
Web Server
DB Server
Mail Server
.1
.2
VoIP Server
Ext: 1000
Area LAN
.1
.10
10.1.x.0/24
.11
.20
Area VoIP
SSID : pusat-x.net
Channel : 1
Mode : G/N
Area HotSpot
FAZTRAIN - IT TRAINING & CONSULTING
COMPUTER NETWORK | SYSTEM ADMINISTRATION
X=1

Pada skenario ini, jenis layanan VPN yang digunakan adalah **PPTP** (***P****oint to* ***P****oint* ***T****unneling* ***P****rotocol*), berikut adalah tahapan konfigurasi VPN dengan PPTP di **Router (R1)**.

1. Mengaktifkan server PPTP di Router (R2) dan menerapkan proses enkripsi data, hal ini dilakukan untuk keamanan data komunikasi VoIP

```
[admin@R1] > interface pptp-server server set enabled=yes \
default-profile=default-encryption
```

2. Konfigurasi akun VPN dan *interface* PPTP yang nantinya akan digunakan oleh *client* VPN di Router (R2) kantor cabang untuk terhubung ke *server* VPN.

```
[admin@R1] >  interface pptp-server add name=pptp-voip user=voip
```

```
[admin@R1] >  ppp secret add name=voip password=123456 service=pptp \
local-address=10.100.101.1 remote-address=10.100.101.2
```

3. Konfigurasi *routing* harus ditambahkan di Router (R1) agar terbentuk rute komunikasi dari *server* VoIP di kantor pusat ke *server* VoIP di kantor cabang lewat jalur VPN PPTP.

```
[admin@R1] > ip route add dst-address=10.13.1.0/24 gateway=10.100.101.2
```

B. Konfigurasi **Router (R2)** di Kantor Cabang

1. Konfigurasi interface ether3 (e3) di Router (R2)

```
[admin@R2] > interface set 2 name=ether3-Server
```

2. Konfigurasi alamat IP ether3-Server (e3) di Router (R2)

```
[admin@R2] > ip address add address=10.13.1.1/24 interface=ether3-Server
```

3. Konfigurasi **SNAT** dibuat agar *server* VoIP dapat terkoneksi ke *internet*

```
[admin@R2] > ip firewall nat add chain=srcnat src-address=10.13.1.0/24 \
out-interface=ether1-Internet action=masquerade
```

4. Konfigurasi *client* VPN (PPTP) agar Router (R2) dapat terhubung ke *server* VPN (R1) di kantor pusat.

```
[admin@R2] > interface pptp-client add name=pptp-voip connect-to=20.0.0.1 \
user=voip password=123456 profile=default-encryption disabled=no
```

Melakukan verifikasi koneksi *client* VPN ke *server* VPN, huruf "**R**" yang muncul menandakan bahwa *client* VPN telah terkoneksi ke *server* VPN.

```
[admin@R2] > interface pptp-client print
Flags: X - disabled, R - running
 0  R name="pptp-voip" max-mtu=1450 max-mru=1450 mrru=disabled connect-
      to=20.0.0.1 user="voip" password="123456" profile=default-
      encryption keepalive-timeout=60 add-default-route=no dial-on-
      demand=no allow=pap,chap,mschap1,mschap2
```

5. Konfigurasi routing juga ditambahkan ke Router (R2) agar terbentuk rute yang akan mengkoneksikan *client* VoIP di kantor cabang ke *server* VoIP di kantor pusat.

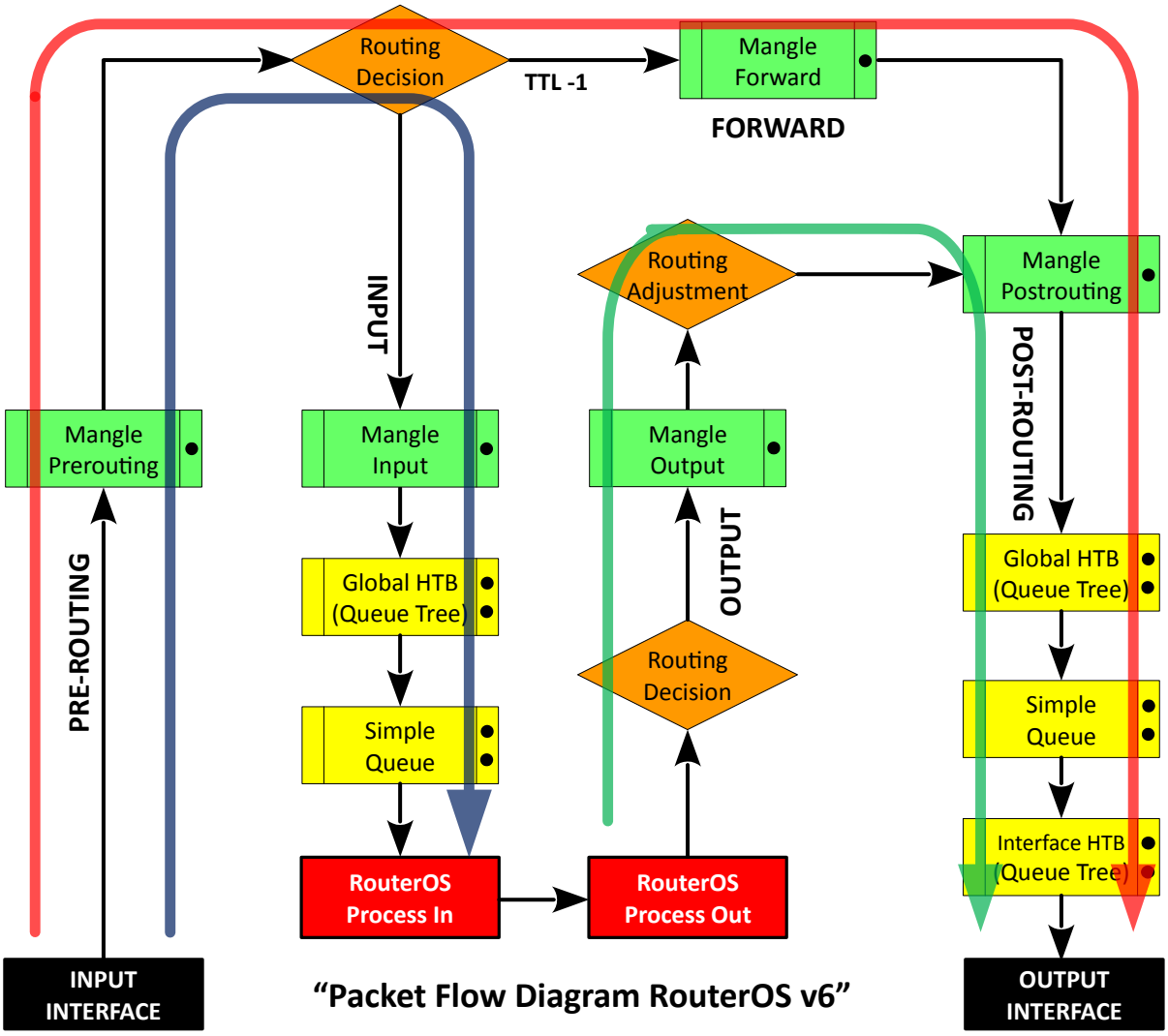
```
[admin@R2] > ip route add dst-address=10.3.1.0/24 gateway=10.100.101.1
```

Melakukan verifikasi koneksi Router (R2) ke Router (R1) lewat jalur VPN, serta verifikasi koneksi Router (R2) ke *server* VoIP di kantor pusat.

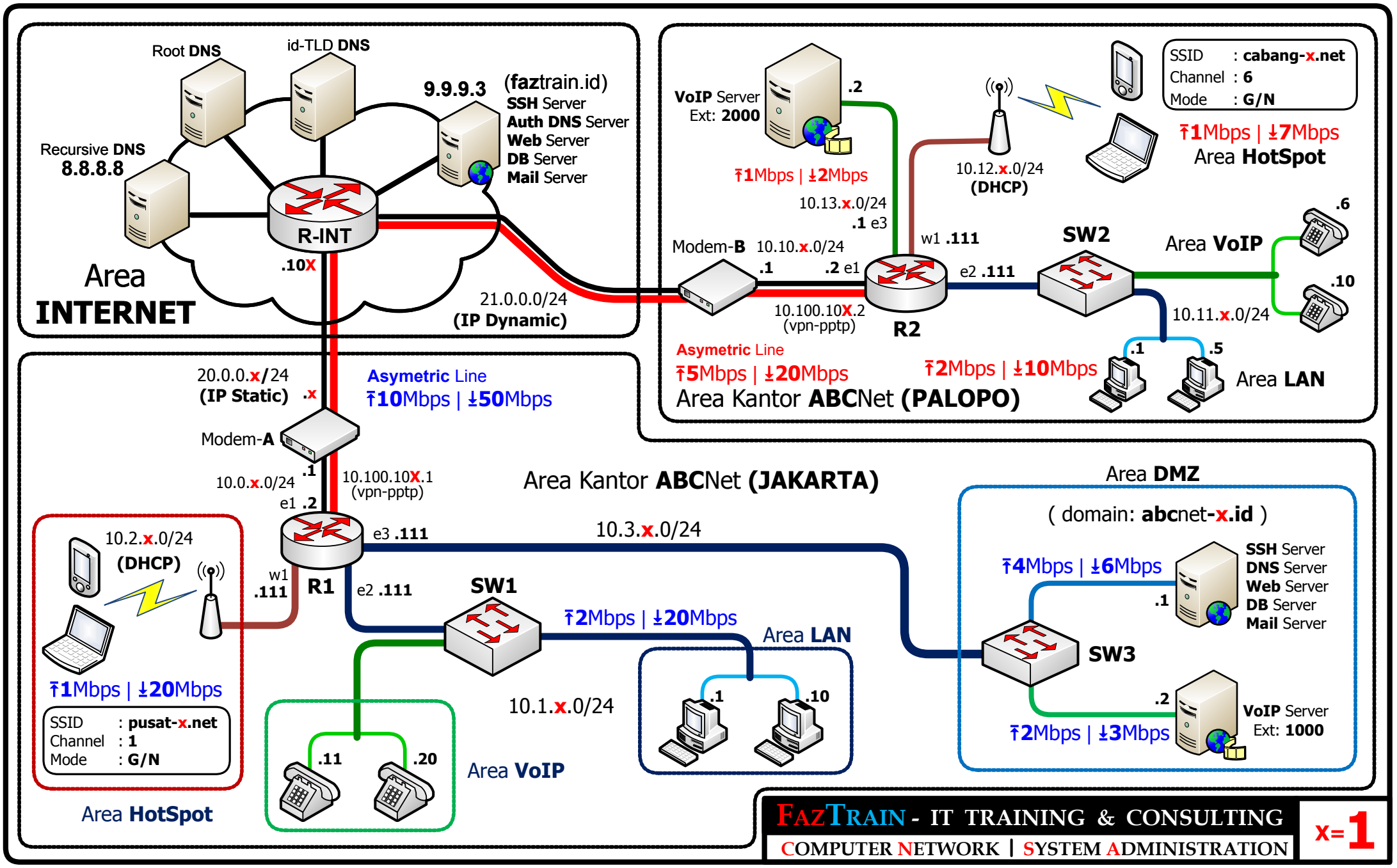
```
[admin@R2] > ping 10.100.101.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.100.101.1                               56  64 41ms
    1 10.100.101.1                               56  64 43ms
    2 10.100.101.1                               56  64 41ms
    3 10.100.101.1                               56  64 42ms


[admin@R2] > ping 10.3.1.2
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.3.1.2                                   56  63 42ms
    1 10.3.1.2                                   56  63 44ms
    2 10.3.1.2                                   56  63 44ms
    3 10.3.1.2                                   56  63 43ms
```

Tahap 6
Manajemen Bandwidth

Untuk efisiensi penggunaan *bandwidth internet*, maka PT. **ABC**Net meminta agar dilakukan manajemen *bandwidth*, baik di jaringan kantor pusat maupun di jaringan kantor cabang. Hal yang sangat penting untuk ditentukan terlebih sebelum melakukan manajemen *bandwidth* adalah besaran *bandwidth* yang akan diberikan ke area tertentu untuk menjamin ketersediaan *bandwidth* untuk kelancaran koneksi. Gambar *packet flow diagram* RouterOS (Gambar 6.1) berikut akan sangat membantu dalam proses konfigurasi.



Gambar 6.1. *Packet Flow Diagram* RouterOS untuk Fungsi Manajemen *Bandwidth*


Root DNS
id-TLD DNS
9.9.9.3
(faztrain.id)
SSH Server
Auth DNS Server
Web Server
DB Server
Mail Server
Recursive DNS
8.8.8.8
R-INT
.10X
Area
INTERNET
21.0.0.0/24
(IP Dynamic)
VoIP Server
Ext: 2000
.2
↑1Mbps | ↓2Mbps
10.13.x.0/24
.1 e3
Modem-B
10.10.x.0/24
.1
.2 e1
10.100.10X.2
(vpn-pptp)
R2
w1 .111
e2 .111
SW2
10.12.x.0/24
(DHCP)
SSID : cabang-x.net
Channel : 6
Mode : G/N
↑1Mbps | ↓7Mbps
Area HotSpot
Area VoIP
.6
.10
10.11.x.0/24
.1
.5
Area LAN
Asymetric Line
↑5Mbps | ↓20Mbps
↑2Mbps | ↓10Mbps
Area Kantor ABCNet (PALOPO)
20.0.0.x/24
(IP Static)
.x
Asymetric Line
↑10Mbps | ↓50Mbps
Modem-A
.1
10.0.x.0/24
e1 .2
10.100.10X.1
(vpn-pptp)
Area Kantor ABCNet (JAKARTA)
Area DMZ
(domain: abcnet-x.id)
10.2.x.0/24
(DHCP)
w1
.111
R1
e3 .111
10.3.x.0/24
e2 .111
SW1
↑2Mbps | ↓20Mbps
Area LAN
↑4Mbps | ↓6Mbps
SSH Server
DNS Server
Web Server
DB Server
Mail Server
.1
SW3
.2
VoIP Server
Ext: 1000
↑2Mbps | ↓3Mbps
↑1Mbps | ↓20Mbps
SSID : pusat-x.net
Channel : 1
Mode : G/N
Area HotSpot
10.1.x.0/24
.11
.20
Area VoIP
FAZTRAIN - IT TRAINING & CONSULTING
COMPUTER NETWORK | SYSTEM ADMINISTRATION
X=1

Berikut adalah penjelasan singkat terkait gambar 6.1 di halaman sebelumnya, dan sekaligus menjelaskan strategi yang akan digunakan dalam melakukan manajemen *bandwidth* untuk studi kasus seperti gambar topologi jaringan yang terlampir di halaman sebelumnya. Ada dua metode yang bisa digunakan untuk melakukan manajemen *bandwidth* pada RouterOS, yaitu: 1. *Simple Queue* dan 2. *Queue Tree*.

Sesuai namanya, metode *Simple Queue* sangat mudah dalam proses konfigurasi, karena tidak mengharuskan melakukan pengaturan penandaan (*marking*) paket untuk bisa digunakan. Namun hal ini tidak berarti metode *Simple Queue* tidak bisa melakukan manajemen *bandwidth* yang rumit, karena *Simple Queue* juga memiliki fitur pengaturan tingkat mahir "*Advance*" yang memungkinkan prosesnya seperti menggunakan metode *Queue Tree* yang rumit. Metode berikutnya yang bisa digunakan untuk manajemen *bandwidth* adalah *Queue Tree*, penggunaannya lebih rumit daripada *Simple Queue*, namun menggunakan *Queue Tree* adalah cara terbaik dalam melakukan manajemen *bandwidth*, oleh karena itu pada buku kerja ini, yang akan digunakan adalah *Queue Tree*.

Saat menggunakan metode *Queue Tree*, ada dua lokasi yang bisa digunakan dalam penerapan proses antrian paket di dalam RouterOS, yaitu "**Global HTB**" dan "**Interface HTB**". Pada buku kerja ini, yang akan digunakan adalah *Global* HTB, alasannya karena lebih mudah dan ringkas dalam proses konfigurasi. *Interface* HTB digunakan jika pada RouterBoard hanya digunakan dua *interface* saja (satu *interface* ke jaringan lokal dan satu lagi ke *internet*) dan tidak ada rencana akan melakukan pembatasan *bandwidth* untuk akses ke RouterBoard (INPUT).

Queue Tree membutuhkan fitur penandaan paket (*packet marking*) pada lokasi "**Mangle**" untuk klasifikasi paket yang akan dibatasi. Jika melihat gambar 6.1 secara seksama, maka akan diketahui bahwa untuk melakukan penandaan paket yang melewati RouterBoard dapat dilakukan di lokasi "**Mangle Pre-Routing**", "**Mangle Forward**" dan "**Mangle Post-Routing**". Untuk penandaan paket yang menuju ke RouterBoard dapat dilakukan di lokasi "**Mangle Pre-Routing**" dan "**Mangle Input**". Untuk penandaan paket yang keluar dari RouterBoard dapat dilakukan di lokasi

"**Mangle Output**" dan "**Mangle Post-Routing**". Karena yang akan diatur oleh *Queue Tree* nantinya adalah alokasi *bandwidth upload* dan *download* dari setiap area pada jaringan kantor pusat dan kantor cabang, maka lokasi paling ideal yang akan dipilih untuk melakukan penandaan paket adalah "**Mangle Forward**".

Untuk menghindari terjadi pembatasan saat akses ke jaringan lokal dan juga untuk kemudahan konfigurasi penandaan paket, maka terlebih dahulu dibuat daftar alamat-alamat IP yang akan dilibatkan dalam proses konfigurasi pembatasan *bandwidth*. Tabel 6.1 dan 6.2 merupakan daftar alamat IP yang akan dibuat pada ***Address-List*** RouterOS dan digunakan dalam proses konfigurasi penandaan paket. Penggunaan prefiks didasarkan pada tabel 1.1. Khusus penentuan alamat **AreaPusat** dan **AreaCabang** pada *Address-List* menggunakan teknik ***summarization*** (peringkasan) sesuai tabel 1.1, agar dapat mewakili keseluruhan alamat pada jaringan di area kantor pusat dan juga jaringan di area kantor cabang.

Tabel 6.1. Daftar alamat IP yang dibuat pada *Address-List* Router (R1)

Nama Address-List	Alamat IP
AreaPusat	10.0.0.0/13
AreaLAN	10.1.1.0/24
AreaWLAN	10.2.2.0/24
ServerWeb	10.3.1.1
ServerVoIP	10.3.1.2

Tabel 6.2. Daftar alamat IP yang dibuat pada *Address-List* Router (R2)

Nama Address-List	Alamat IP
AreaCabang	10.8.0.0/13
AreaLAN	10.11.1.0/24
AreaWLAN	10.12.2.0/24
ServerVoIP	10.13.1.2

Untuk alokasi *bandwidth* setiap area bisa dilihat pada gambar topologi jaringan yang telah dilampirkan pada halaman sebelumnya. Berikut adalah tahapan proses konfigurasi di masing-masing RouterBoard.

A. Konfigurasi Manajemen Bandwidth Router (R1)

1. Membuat daftar alamat IP di *address-list* sesuai tabel 6.1.

```
[admin@R1] > ip firewall address-list add address=10.0.0.0/13 list=AreaPusat
[admin@R1] > ip firewall address-list add address=10.1.1.0/24 list=AreaLAN
[admin@R1] > ip firewall address-list add address=10.2.1.0/24 list=AreaWLAN
[admin@R1] > ip firewall address-list add address=10.3.1.1 list=ServerWeb
[admin@R1] > ip firewall address-list add address=10.3.1.2 list=ServerVoIP
```

2. Membuat aturan penandaan koneksi dan penandaan paket untuk AreaLAN.

```
[admin@R1] > ip firewall mangle add chain=forward src-address-list=AreaLAN \
dst-address-list=!AreaPusat action=mark-connection new-connection-mark=Koneksi-AreaLAN \
passthrough=yes comment="Marking Koneksi AreaLAN"

[admin@R1] > ip firewall mangle add chain=forward in-interface=ether2-LAN \
connection-mark=Koneksi-AreaLAN action=mark-packet new-packet-mark=AreaLAN-Upload \
passthrough=no comment="Marking Upload AreaLAN"

[admin@R1] > ip firewall mangle add chain=forward in-interface=ether1-Internet \
connection-mark=Koneksi-AreaLAN action=mark-packet new-packet-mark=AreaLAN-Download \
passthrough=no comment="Marking Download AreaLAN"
```

3. Membuat aturan penandaan koneksi dan penandaan paket untuk AreaWLAN.

```
[admin@R1] > ip firewall mangle add chain=forward src-address-list=AreaWLAN \
dst-address-list=!AreaPusat action=mark-connection new-connection-mark=Koneksi-AreaWLAN \
passthrough=yes comment="Marking Koneksi AreaWLAN"

[admin@R1] > ip firewall mangle add chain=forward in-interface=wlan1 \
connection-mark=Koneksi-AreaWLAN action=mark-packet new-packet-mark=AreaWLAN-Upload \
passthrough=no comment="Marking Upload AreaWLAN"

[admin@R1] > ip firewall mangle add chain=forward in-interface=ether1-Internet \
connection-mark=Koneksi-AreaWLAN action=mark-packet new-packet-mark=AreaWLAN-Download \
passthrough=no comment="Marking Download AreaWLAN"
```

4. Membuat aturan penandaan koneksi dan penandaan paket untuk ServerWeb.

```
[admin@R1] > ip firewall mangle add chain=forward src-address-list=ServerWeb \
dst-address-list=!AreaPusat action=mark-connection new-connection-mark=Koneksi-ServerWeb \
passthrough=yes comment="Marking Koneksi ServerWeb"

[admin@R1] > ip firewall mangle add chain=forward in-interface=ether3-Server \
connection-mark=Koneksi-ServerWeb action=mark-packet new-packet-mark=ServerWeb-Upload \
passthrough=no comment="Marking Upload ServerWeb"

[admin@R1] > ip firewall mangle add chain=forward in-interface=ether1-Internet \
connection-mark=Koneksi-ServerWeb action=mark-packet new-packet-mark=ServerWeb-Download \
passthrough=no comment="Marking Download ServerWeb"
```

5. Membuat aturan penandaan koneksi dan penandaan paket untuk ServerVoIP.

```
[admin@R1] > ip firewall mangle add chain=forward src-address-list=ServerVoIP \
dst-address-list=!AreaPusat action=mark-connection new-connection-mark=Koneksi-ServerVoIP \
passthrough=yes comment="Marking Koneksi ServerVoIP"

[admin@R1] > ip firewall mangle add chain=forward in-interface=ether3-Server \
connection-mark=Koneksi-ServerVoIP action=mark-packet new-packet-mark=ServerVoIP-Upload \
passthrough=no comment="Marking Upload ServerVoIP"

[admin@R1] > ip firewall mangle add chain=forward in-interface=ether1-Internet \
connection-mark=Koneksi-ServerVoIP action=mark-packet new-packet-mark=ServerVoIP-Download \
passthrough=no comment="Marking Download ServerVoIP"
```

6. Membuat aturan *Queue Tree* untuk **akumulasi** penggunaan *bandwidth upload* dan *download*.

```
[admin@R1] > queue tree add name=Global-Traffic parent=global queue=default
```

7. Membuat aturan *Queue Tree* untuk **akumulasi** penggunaan *bandwidth upload* dengan total 10 Mbps.

```
[admin@R1] > queue tree add name=Total-Upload max-limit=10M queue=default \
parent=Global-Traffic comment="Total Bandwidth Upload"
```

8. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth upload* maksimal 2 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area LAN.

```
[admin@R1] > queue tree add name=AreaLAN-Upload packet-mark=AreaLAN-Upload \
limit-at=2M max-limit=2M parent=Total-Upload queue=pcq-upload-default
```

9. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth upload* maksimal 1 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area WLAN.

```
[admin@R1] > queue tree add name=AreaWLAN-Upload packet-mark=AreaWLAN-Upload \
limit-at=1M max-limit=1M parent=Total-Upload queue=pcq-upload-default
```

10. Membuat aturan *Queue Tree* untuk akumulasi penggunaan *bandwidth upload* di area *server* dengan total 6 Mbps.

```
[admin@R1] > queue tree add name=AreaServer-Upload max-limit=6M queue=default \
parent=Total-Upload
```

11. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth upload server web* maksimal 4 Mbps.

```
[admin@R1] > queue tree add name=ServerWeb-Upload packet-mark=ServerWeb-Upload \
limit-at=4M max-limit=4M parent=AreaServer-Upload queue=default
```

12. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth upload server* VoIP maksimal 2 Mbps.

```
[admin@R1] > queue tree add name=ServerVoIP-Upload packet-mark=ServerVoIP-Upload \
limit-at=2M max-limit=2M parent=AreaServer-Upload queue=default
```

13. Membuat aturan *Queue Tree* untuk **akumulasi** penggunaan *bandwidth download* dengan total 50 Mbps.

```
[admin@R1] > queue tree add name=Total-Download max-limit=50M queue=default \
parent=Global-Traffic comment="Total Bandwidth Download"
```

14. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth download* maksimal 20 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area LAN.

```
[admin@R1] > queue tree add name=AreaLAN-Download packet-mark=AreaLAN-Download \
limit-at=20M max-limit=20M parent=Total-Download queue=pcq-download-default
```

15. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth download* maksimal 20 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area WLAN.

```
[admin@R1] > queue tree add name=AreaWLAN-Download packet-mark=AreaWLAN-Download \
limit-at=20M max-limit=20M parent=Total-Download queue=pcq-download-default
```

16. Membuat aturan *Queue Tree* untuk akumulasi penggunaan *bandwidth upload* di area *server* dengan total 9 Mbps.

```
[admin@R1] > queue tree add name=AreaServer-Download max-limit=9M queue=default \
parent=Total-Download
```

17. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth download server web* maksimal 6 Mbps.

```
[admin@R1] > queue tree add name=ServerWeb-Download packet-mark=ServerWeb-Download \
limit-at=6M max-limit=6M parent=AreaServer-Download queue=default
```

18. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth download server* VoIP maksimal 3 Mbps.

```
[admin@R1] > queue tree add name=ServerVoIP-Download packet-mark=ServerVoIP-Download \
limit-at=3M max-limit=3M parent=AreaServer-Download queue=default
```

B. Konfigurasi Manajemen Bandwidth Router (R2)

1. Membuat daftar alamat IP di *address-list* sesuai tabel 6.2.

```
[admin@R2] > ip firewall address-list add address=10.8.0.0/13 list=AreaCabang
[admin@R2] > ip firewall address-list add address=10.11.1.0/24 list=AreaLAN
[admin@R2] > ip firewall address-list add address=10.12.1.0/24 list=AreaWLAN
[admin@R2] > ip firewall address-list add address=10.13.1.2 list=ServerVoIP
```

2. Membuat aturan penandaan koneksi dan penandaan paket untuk area LAN.

```
[admin@R2] > ip firewall mangle add chain=forward src-address-list=AreaLAN \
dst-address-list=!AreaCabang action=mark-connection new-connection-mark=Koneksi-AreaLAN \
passthrough=yes comment="Marking Koneksi AreaLAN"

[admin@R2] > ip firewall mangle add chain=forward in-interface=ether2-LAN \
connection-mark=Koneksi-AreaLAN action=mark-packet new-packet-mark=AreaLAN-Upload \
passthrough=no comment="Marking Upload AreaLAN"

[admin@R2] > ip firewall mangle add chain=forward in-interface=ether1-Internet \
connection-mark=Koneksi-AreaLAN action=mark-packet new-packet-mark=AreaLAN-Download \
passthrough=no comment="Marking Download AreaLAN"
```

3. Membuat aturan penandaan koneksi dan penandaan paket untuk area WLAN.

```
[admin@R2] > ip firewall mangle add chain=forward src-address-list=AreaWLAN \
dst-address-list=!AreaCabang action=mark-connection new-connection-mark=Koneksi-AreaWLAN \
passthrough=yes comment="Marking Koneksi AreaWLAN"

[admin@R2] > ip firewall mangle add chain=forward in-interface=wlan1 \
connection-mark=Koneksi-AreaWLAN action=mark-packet new-packet-mark=AreaWLAN-Upload \
passthrough=no comment="Marking Upload AreaWLAN"

[admin@R2] > ip firewall mangle add chain=forward in-interface=ether1-Internet \
connection-mark=Koneksi-AreaWLAN action=mark-packet new-packet-mark=AreaWLAN-Download \
passthrough=no comment="Marking Download AreaWLAN"
```

4. Membuat aturan penandaan koneksi dan penandaan paket untuk server VoIP.

```
[admin@R2] > ip firewall mangle add chain=forward src-address-list=ServerVoIP \
dst-address-list=!AreaCabang action=mark-connection new-connection-mark=Koneksi-ServerVoIP \
passthrough=yes comment="Marking Koneksi ServerVoIP"

[admin@R2] > ip firewall mangle add chain=forward in-interface=ether3-Server \
connection-mark=Koneksi-ServerVoIP action=mark-packet new-packet-mark=ServerVoIP-Upload \
passthrough=no comment="Marking Upload ServerVoIP"
```

```
[admin@R2] > ip firewall mangle add chain=forward in-interface=ether1-Internet \
connection-mark=Koneksi-ServerVoIP action=mark-packet new-packet-mark=ServerVoIP-Download \
passthrough=no comment="Marking Download ServerVoIP"
```

5. Membuat aturan *Queue Tree* untuk **akumulasi** penggunaan *bandwidth upload* dan *download*.

```
[admin@R2] > queue tree add name=Global-Traffic parent=global queue=default
```

6. Membuat aturan *Queue Tree* untuk **akumulasi** penggunaan *bandwidth upload* dengan total 5 Mbps.

```
[admin@R2] > queue tree add name=Total-Upload max-limit=5M queue=default \
parent=Global-Traffic comment="Total Bandwidth Upload"
```

7. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth upload* maksimal 2 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area LAN.

```
[admin@R2] > queue tree add name=AreaLAN-Upload packet-mark=AreaLAN-Upload \
limit-at=2M max-limit=2M parent=Total-Upload queue=pcq-upload-default
```

8. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth upload* maksimal 1 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area WLAN.

```
[admin@R2] > queue tree add name=AreaWLAN-Upload packet-mark=AreaWLAN-Upload \
limit-at=1M max-limit=1M parent=Total-Upload queue=pcq-upload-default
```

9. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth upload server* VoIP maksimal 1 Mbps.

```
[admin@R2] > queue tree add name=ServerVoIP-Upload packet-mark=ServerVoIP-Upload \
limit-at=1M max-limit=1M parent=Total-Upload queue=default
```

10. Membuat aturan *Queue Tree* untuk **akumulasi** penggunaan *bandwidth download* dengan total 20 Mbps.

```
[admin@R2] > queue tree add name=Total-Download max-limit=20M queue=default \
parent=Global-Traffic comment="Total Bandwidth Download"
```

11. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth download* maksimal 10 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area LAN.

```
[admin@R2] > queue tree add name=AreaLAN-Download packet-mark=AreaLAN-Download \
limit-at=10M max-limit=10M parent=Total-Download queue=pcq-download-default
```

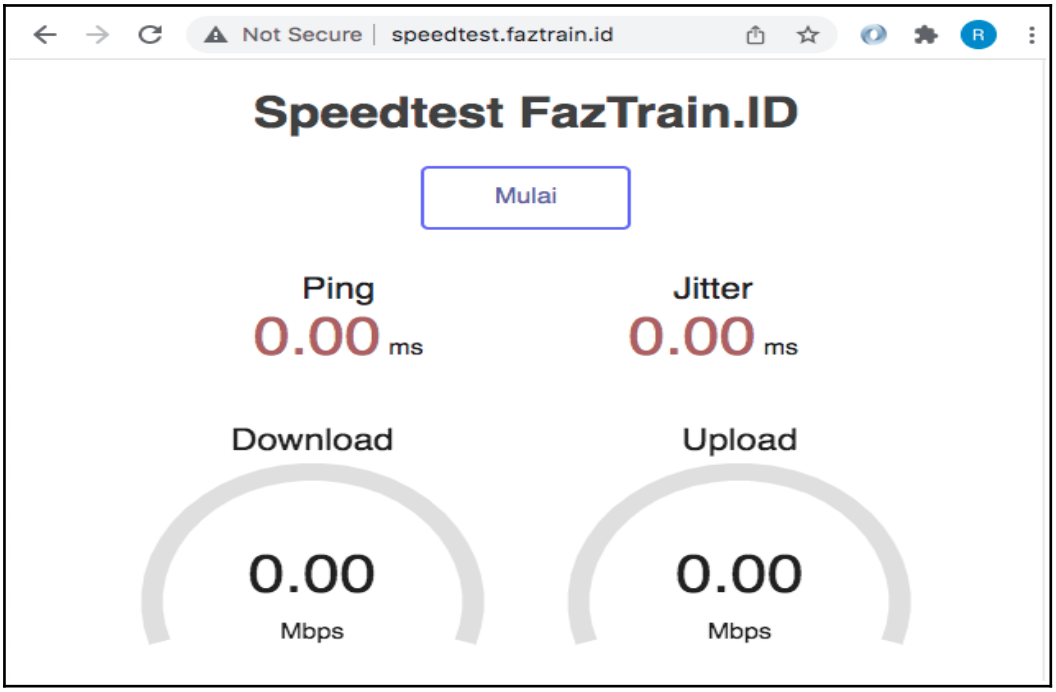
12. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth download* maksimal 7 Mbps dan akan dibagi secara merata (dengan metode PCQ) ke semua komputer di area WLAN.

```
[admin@R2] > queue tree add name=AreaWLAN-Download packet-mark=AreaWLAN-Download \
limit-at=7M max-limit=7M parent=Total-Download queue=pcq-download-default
```

13. Membuat aturan *Queue Tree* untuk membatasi penggunaan *bandwidth download server* VoIP maksimal 2 Mbps.

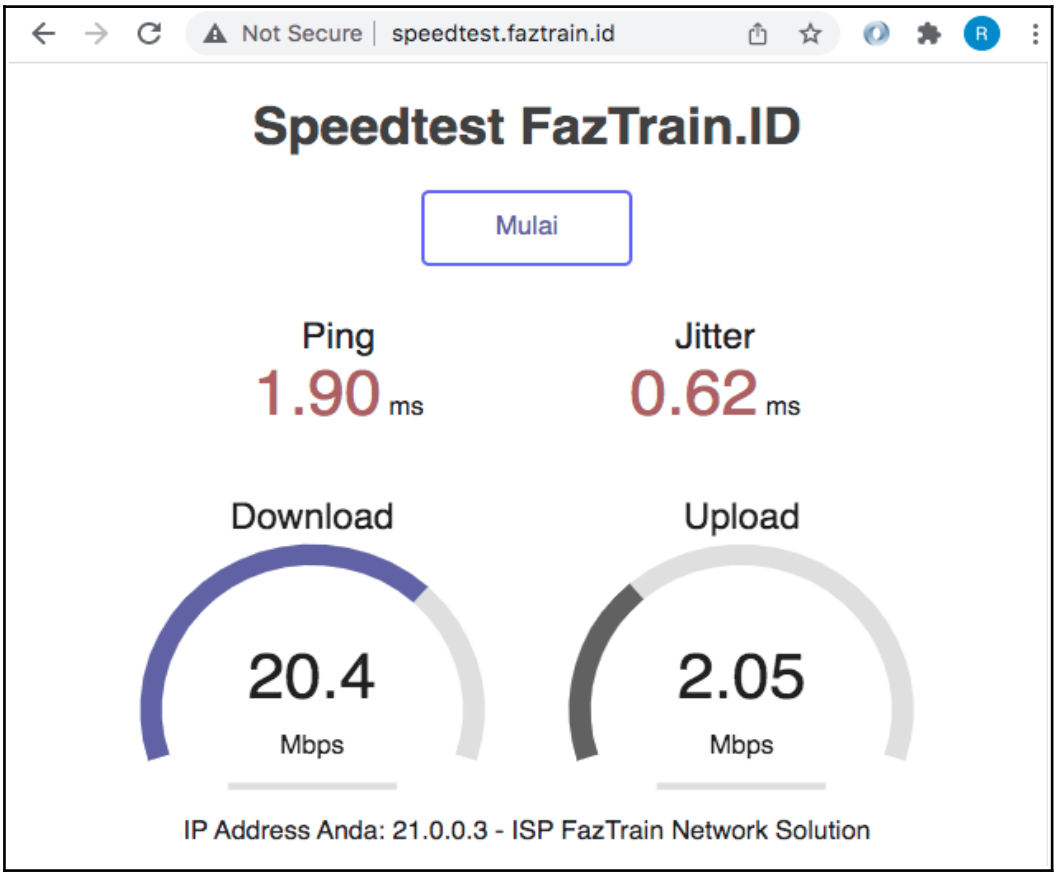
```
[admin@R2] > queue tree add name=ServerVoIP-Download packet-mark=ServerVoIP-Download \
limit-at=2M max-limit=2M parent=Total-Download queue=default
```

Tahap selanjutnya mengukur penggunaan *bandwidth* atau kecepatan *internet* menggunakan layanan **speedtest** pada alamat `speedtest.faztrain.id`. Pengukuran dilakukan pada *client* LAN Kantor Pusat (Gambar 6.3).



Gambar 6.3. Mengukur Bandwidth Internet dengan Layanan Speedtest

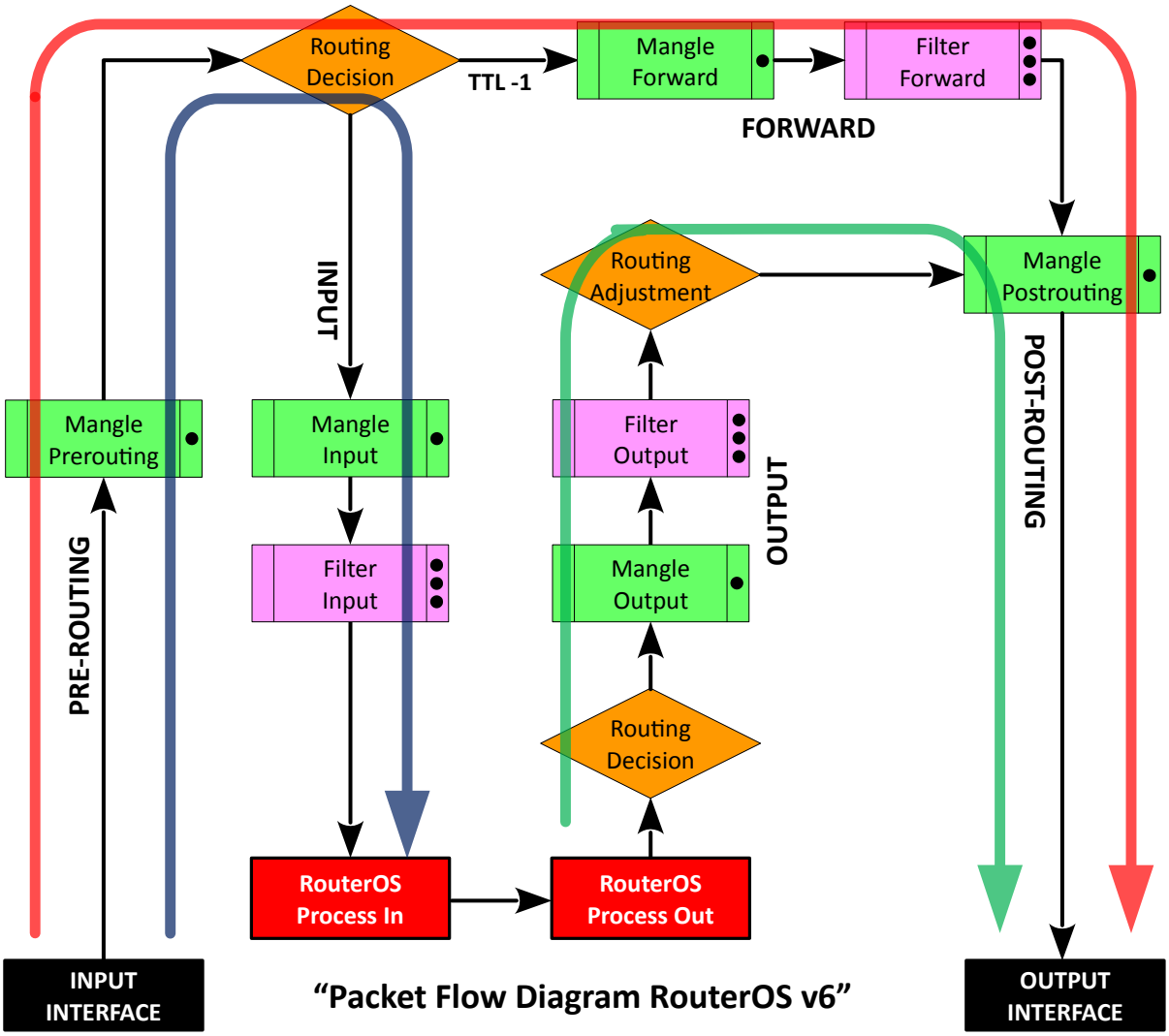
Hasil pengukuran penggunaan *bandwidth* atau kecepatan internet pada *client* ditunjukkan pada gambar 6.4. Hasil pengukuran menunjukkan bahwa kecepatan *download client* adalah **20 Mbps**, sedang kecepatan *upload client* adalah **2 Mbps**. Hal ini sesuai pengaturan *bandwidth* yang telah dilakukan pada RouterOS sebelumnya untuk *client* di area LAN Kantor Pusat PT. ABCNet.



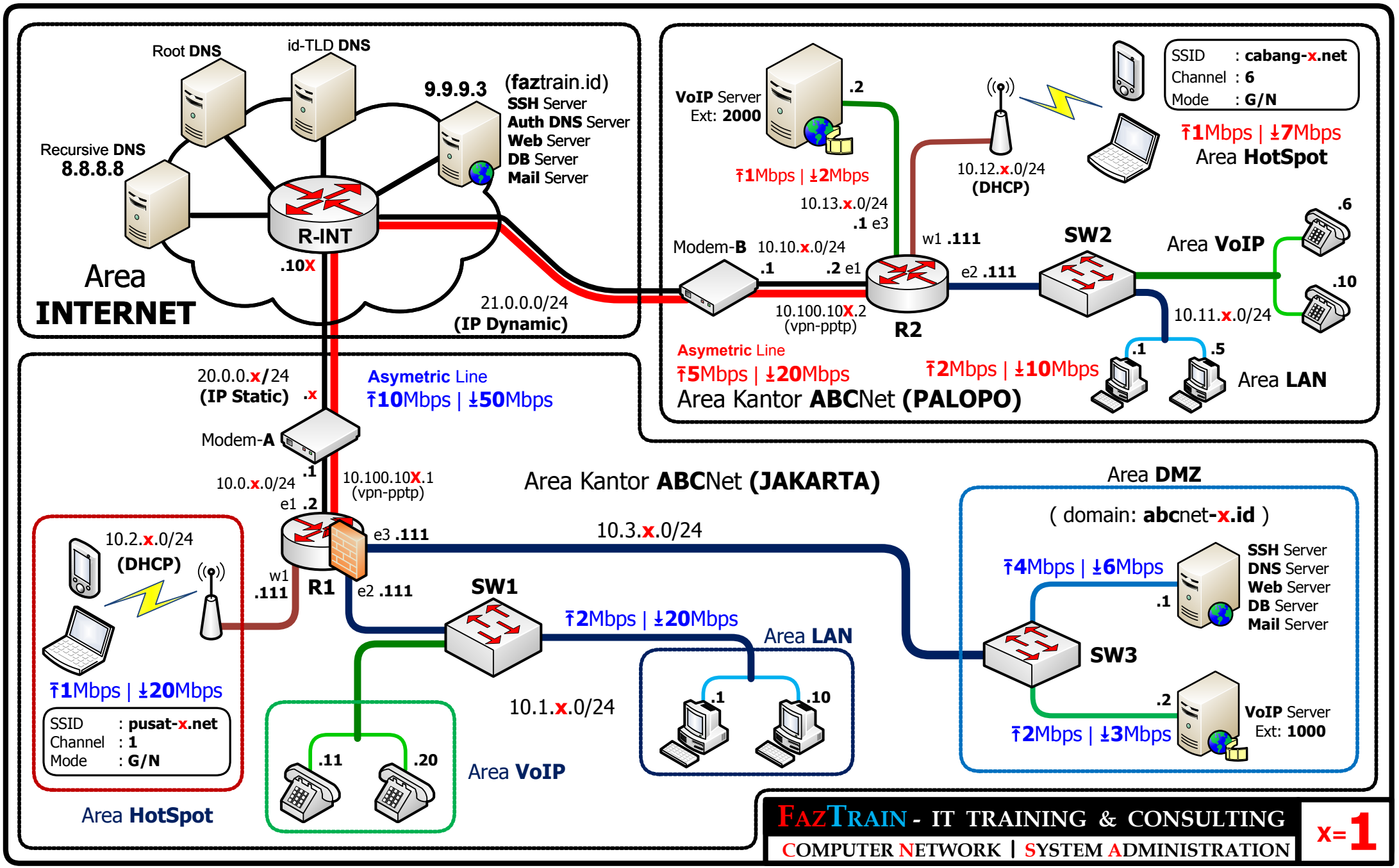
Gambar 6.4. Hasil Pengukuran Bandwidth dengan Layanan Speedtest

Tahap 7
Keamanan Sistem dan Jaringan

Salah satu peran penting seorang ***Network Administrator*** adalah menjaga jaringan yang dikelolanya agar tetap aman. Salah satu fitur pada RouterOS yang dapat digunakan untuk kebutuhan keamanan jaringan adalah "***Firewall***". Pada buku kerja ini akan dibahas beberapa teknik yang bisa digunakan untuk menangkal serangan baik dari luar maupun dari dalam. *Packet flow diagram* RouterOS (Gambar 7.1) akan digunakan sebagai pemandu untuk kemudahan proses konfigurasi *firewall*.

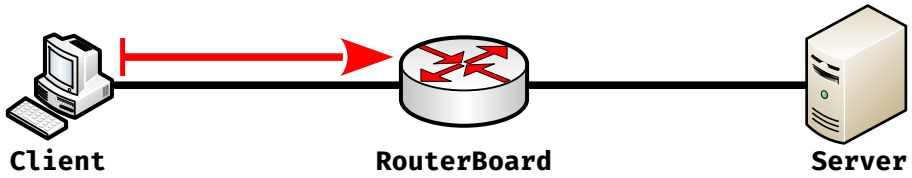


Gambar 7.1. *Packet Flow Diagram* RouterOS untuk Fungsi Keamanan Jaringan


Root DNS
id-TLD DNS
9.9.9.3
(faztrain.id)
SSH Server
Auth DNS Server
Web Server
DB Server
Mail Server
Recursive DNS
8.8.8.8
R-INT
.10X
Area
INTERNET
21.0.0.0/24
(IP Dynamic)
VoIP Server
Ext: 2000
.2
↑1Mbps | ↓2Mbps
10.13.x.0/24
.1 e3
Modem-B
10.10.x.0/24
.1
.2 e1
10.100.10X.2
(vpn-pptp)
R2
w1 .111
e2 .111
SW2
10.12.x.0/24
(DHCP)
SSID : cabang-x.net
Channel : 6
Mode : G/N
↑1Mbps | ↓7Mbps
Area HotSpot
Area VoIP
.6
.10
10.11.x.0/24
.1
.5
Area LAN
Asymetric Line
↑5Mbps | ↓20Mbps
↑2Mbps | ↓10Mbps
Area Kantor ABCNet (PALOPO)
20.0.0.x/24
(IP Static)
.x
Asymetric Line
↑10Mbps | ↓50Mbps
Modem-A
.1
10.0.x.0/24
e1 .2
10.100.10X.1
(vpn-pptp)
Area Kantor ABCNet (JAKARTA)
Area DMZ
(domain: abcnet-x.id)
10.2.x.0/24
(DHCP)
w1
.111
R1
e3 .111
10.3.x.0/24
e2 .111
SW1
↑4Mbps | ↓6Mbps
.1
SSH Server
DNS Server
Web Server
DB Server
Mail Server
SW3
↑2Mbps | ↓20Mbps
Area LAN
.1
.10
.2
VoIP Server
Ext: 1000
↑2Mbps | ↓3Mbps
↑1Mbps | ↓20Mbps
SSID : pusat-x.net
Channel : 1
Mode : G/N
10.1.x.0/24
.11
.20
Area VoIP
Area HotSpot
FAZTRAIN - IT TRAINING & CONSULTING
COMPUTER NETWORK | SYSTEM ADMINISTRATION
X=1

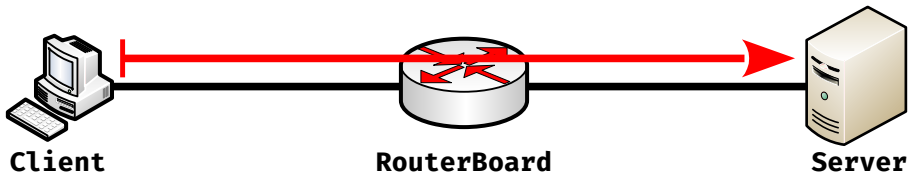
Seperti pada tahap manajemen *bandwidth* sebelumnya, pada pembahasan keamanan jaringan juga akan menggunakan diagram alir paket data (*packet flow diagram*) dari RouterOS untuk memudahkan dalam proses pembuatan aturan filter keamanan. Secara singkat dapat dijelaskan bahwa ada tiga kondisi dalam proses mengalirnya paket data pada RouterBoard, yaitu:

1. Paket data mengalir masuk menuju RouterBoard MikroTik (**INPUT**)



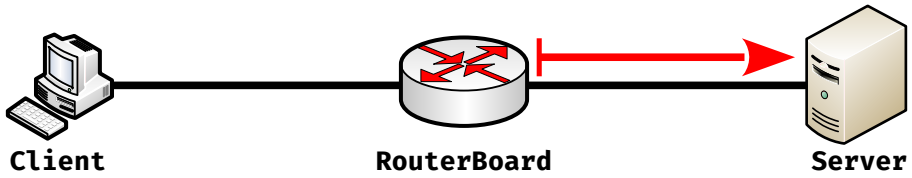
Gambar 7.3. Filter di lokasi INPUT

2. Paket data mengalir melewati RouterBoard MikroTik (**FORWARD**)



Gambar 7.4. Filter di lokasi FORWARD

3. Paket data mengalir keluar dari RouterBoard MikroTik (**OUTPUT**)



Gambar 7.5. Filter di lokasi OUTPUT

Proses filter oleh *firewall* akan dilakukan di tiga lokasi tersebut, lokasi mana yang akan digunakan sebagai tempat pemasangan filter tergantung dari asal dan tujuan dari aliran paket data. Jika paket data berasal dari luar menuju ke dalam RouterBoard, maka filter dipasang di lokasi FILTER INPUT (Gambar 7.3). Jika paket data hanya melewati RouterBoard menuju ke target perangkat atau mesin lain, maka filter dipasang di lokasi FILTER FORWARD (Gambar 7.4). Jika paket data berasal dari dalam RouterBoard menuju ke perangkat atau mesin lain, maka filter dipasang di lokasi FILTER OUTPUT (Gambar 7.5).

Jika melihat pada diagram alir paket (Gambar 7.1), terdapat "*mangle*" yang sebelumnya digunakan pada tahap manajemen *bandwidth.* Pada pembahasan keamanan jaringan, *mangle* akan digunakan untuk membuat proses filter menjadi lebih spesifik, hal ini untuk menghindari terjadinya salah memberikan kebijakan izin akses ataupun blokir.

Mangle digunakan untuk menandai paket-paket data yang dianggap ilegal ataupun sah, lalu diputuskan apakah diizinkan ataukah ditolak. Untuk penandaan paket yang akan difilter di lokasi INPUT, dapat dilakukan di "**Mangle Pre-Routing**" dan "**Mangle Input**". Untuk penandaan paket yang akan difilter dilokasi FORWARD, dapat dilakukan di "**Mangle Pre-Routing**" dan "**Mangle Forward**". Untuk penandaan paket yang akan difilter di lokasi OUTPUT, dapat dilakukan di "**Mangle Output**". Sedang "**Mangle Post-Routing**" bisa digunakan untuk melakukan pengubahan atau manipulasi (*Altering*) komponen *header* paket yang akan difilter pada perangkat filter berikutnya, walau hal ini mungkin jarang dilakukan.

Ada dua metode yang bisa digunakan dalam membuat aturan filter pada *firewall* :

1. Menerapkan filter dengan metode mengizinkan semua paket, kecuali sebagian paket saja yang akan diblokir (*Allow all, and Drop some*). *Firewall* pada RouterOS MikroTik secara *default* menggunakan metode ini. Artinya saat membuat aturan filter, cukup tentukan aturan yang akan digunakan untuk memblokir paket yang diinginkan.

2. Menerapkan filter dengan metode menolak semua paket, kecuali sebagian paket saja yang akan diizinkan (*Drop all, and Allow some*). Metode ini umumnya digunakan jika ingin menerapkan aturan yang ketat terhadap akses di jaringan. Jika kebijakan akses cenderung hanya mengizinkan sedikit akses terhadap pengguna, maka agar aturan yang dibuat tidak banyak, metode ini adalah pilihan yang sangat tepat. Hanya saja ketika membuat aturan *firewall* harus sangat berhati-hati, jangan sampai keliru sehingga membuat beberapa akses penting menjadi macet. Pastikan aturan blokir untuk semua paket

diletakkan di posisi paling bawah atau dibuat setelah semua aturan yang mengizinkan akses dibuat.

Saat dioperasikan, *firewall* filter RouterOS dapat berjalan dalam mode "***Stateless***" dan mode "***Stateful***", berikut penjelasan singkatnya.

1. ***Stateless Firewall***, adalah kondisi *firewall* ketika berjalan tidak melakukan pencatatan dari koneksi yang diterima, dilewatkan atau dikirimkannya. Sehingga ia tidak bisa mengetahui apakah koneksi yang terjadi adalah koneksi baru (*new*) atau koneksi yang sedang berlangsung (*established*). Hal ini karena semua status koneksi tidak tercatat oleh sistem *firewall filter* pada RouterOS.

2. ***Stateful Firewall***, berbeda dengan mode *stateless* sebelumnya, mode ini memberikan kemampuan kepada *firewall* untuk mengetahui status (*state*) dari koneksi yang diprosesnya, apakah statusnya baru (*new*), telah terjalin (*estatblished*), berkaitan dengan koneksi sebelumnya (*related*) atau malah koneksinya dianggap tidak sah (*invalid*). Mode ini sangat bermanfaat untuk meringkas aturan *firewall* yang akan dibuat, terutama saat menggunakan metode "*Blokir semua, izinkan sebagian saja*".

Pada buku kerja ini hanya fokus membahas penggunaan *firewall* pada Router (R1) dengan menerapkan metode "***Drop all, Allow some***", karena oleh manajemen kantor pusat PT. **ABC**Net meminta kebijakan akses yang sangat ketat dan pusat layanan memang berada pada kantor pusat. Berikut adalah kebijakan akses yang ditentukan oleh pihak PT. **ABC**Net yang akan menentukan aturan *firewall* pada RouterOS.

1. Semua staf kantor pusat PT. **ABC**Net, hanya diizinkan mengakses *internet* pada layanan ***web*** dan ***email*** **`faztrain.id`** saat jam kerja, sedang untuk akses penuh ke *internet* hanya diizinkan saat jam istirahat pada pukul **12.00 – 14.00**, kecuali hari Ahad (Minggu).

2. Hanya mengizinkan akses layanan *remote* **SSH** (tcp:22), *email* **SMTP** (tcp:25), **DNS** (udp:53), ***web*** (tcp:80) dan **PPTP** (tcp:1723) dari jaringan *internet* menuju ke Router (R1) yang sebagian akses diteruskan ke area *server* PT. **ABC**Net.

Untuk memudahkan proses pembuatan aturan *firewall* di RouterOS, maka sebaiknya tentukan terlebih dahulu beberapa hal seperti "**alamat IP asal dan/atau alamat IP tujuan**" atau "***interface* asal dan/atau *interface* tujuan**", dari alamat IP asal dan tujuan tersebut akan diketahui lokasi (*chain*) penerapan filter di *firewall*, apakah di lokasi INPUT, FORWARD ataukah di OUTPUT. Kemudian tentukan pula "**protokol dan/atau nomor *port***" yang akan diatur, serta aksi (*action*) apa yang akan diterapkan pada aturan tersebut, apakah diizinkan (*accept*) ataukah diblokir (*drop*).

Karena metode yang akan diterapkan adalah "*Blokir semua dan izinkan sebagian saja*", maka aturan *firewall* yang dibuat di awal adalah semua yang diizinkan terlebih dahulu, setelahnya baru membuat aturan blokir secara keseluruhan di bagian paling bawah. Berikut adalah aturan *firewall* yang akan diterapkan berdasarkan kebijakan akses yang telah ditentukan sebelumnya.

1. Cari tahu terlebih dahulu alamat IP dari **faztrain.id** yang nantinya akan dijadikan sebagai alamat IP tujuan, cara termudah mencari tahu adalah dengan melakukan PING ke alamat nama faztrain.id dari komputer area LAN/WLAN.

```
C:\>ping faztrain.id

Pinging faztrain.id [9.9.9.3] with 32 bytes of data:
Reply from 9.9.9.3: bytes=32 time=41ms TTL=52
Reply from 9.9.9.3: bytes=32 time=43ms TTL=52
Reply from 9.9.9.3: bytes=32 time=41ms TTL=52
Reply from 9.9.9.3: bytes=32 time=42ms TTL=52
```

Diketahui bahwa alamat IP dari alamat nama `faztrain.id` adalah **`9.9.9.3`**, yang akses diakses pada **`faztrain.id`** adalah layanan *web* HTTP (**tcp:80**) dan *email*, untuk layanan *email* menggunakan *web*, maka cukup membuka akses ke layanan *web* saja, karena akses DNS dari area LAN dan WLAN ditujukan ke Router (R1). Berikut adalah aturan yang dibuat pada *firewall*.

Aturan berikut untuk mengizinkan akses dari area LAN dan WLAN ke alamat `faztrain.id` yang ada di *internet*.

```
[admin@R1] > ip firewall filter add chain=forward src-address-list=AreaLAN \
dst-address=9.9.9.3 protocol=tcp dst-port=80 action=accept

[admin@R1] > ip firewall filter add chain=forward src-address-list=AreaWLAN \
dst-address=9.9.9.3 protocol=tcp dst-port=80 action=accept
```

Aturan berikut untuk memblokir semua akses dari area LAN dan WLAN ke *internet* kecuali pada jam istirahat (**12.00 – 14.00**) dan hari **Ahad** (Minggu).

```
[admin@R1] > ip firewall filter add chain=forward in-interface=ether2-LAN \
out-interface=ether1-Internet time=!12h-14h,mon,tue,wed,thu,fri,sat action=drop

[admin@R1] > ip firewall filter add chain=forward in-interface=wlan1 \
out-interface=ether1-Internet time=!12h-14h,mon,tue,wed,thu,fri,sat action=drop
```

2. Pada bagian ini ada dua kondisi yang harus dipisah. Pertama, akses dari *internet* pada *port* **tcp:25** (*email* SMTP), *port* **tcp:80** (*web* HTTP) dan *port* **udp:53** (DNS) yang akan diteruskan oleh Router (R1) ke *server* PT. **ABC**Net, akses ini harus difilter di lokasi FILTER FORWARD, karena paket hanya melewati RouterBoard. Kedua, akses PPTP (VPN) pada *port* **tcp:1723** dari Router (R2) di kantor cabang ke Router (R1) di kantor pusat harus difilter di lokasi FILTER INPUT, karena akses ini ditujukan ke Router (R1).

   Tahap pertama adalah membuat aturan filter untuk mengizinkan akses di lokasi FILTER FORWARD dan di lokasi FILTER INPUT pada alamat nomor *port* yang telah dilampirkan sebelumnya.

   Aturan filter ini untuk mengizinkan akses dari *internet* pada layanan *email* SMTP dan layanan *web* HTTP untuk diteruskan oleh Router (R1) ke *server* PT. **ABC**Net.

   ```
   [admin@R1] > ip firewall filter add chain=forward in-interface=ether1-Internet \
   protocol=tcp dst-port=25,80 action=accept
   ```

Aturan filter berikut untuk mengizinkan akses dari *internet* pada layanan DNS untuk diteruskan oleh Router (R1) ke *server* PT. **ABC**Net. Karena layanan DNS bekerja pada dua jenis protokol *transport* sekaligus, yaitu protokol TCP dan UDP, maka aturan *firewall* yang dibuat juga ada dua.

```
[admin@R1] > ip firewall filter add chain=forward in-interface=ether1-Internet \
protocol=tcp dst-port=53 action=accept

[admin@R1] > ip firewall filter add chain=forward in-interface=ether1-Internet \
protocol=udp dst-port=53 action=accept
```

Aturan filter berikut untuk mengizinkan akses dari *internet* pada layanan PPTP (VPN) yang ditujukan ke Router (R1).

```
[admin@R1] > ip firewall filter add chain=input in-interface=ether1-Internet \
protocol=tcp dst-port=1723 action=accept
```

Tahap kedua adalah membuat aturan blokir untuk semua jenis layanan selain yang telah diizinkan pada aturan filter sebelumnya. Aturan filter berikut untuk memblokir semua akses baik pada protokol TCP maupun UDP yang akan diteruskan oleh Router (R1) menuju ke *server* PT. **ABC**Net.

```
[admin@R1] > ip firewall filter add chain=forward in-interface=ether1-Internet \
protocol=tcp connection-state=!established,related action=drop

[admin@R1] > ip firewall filter add chain=forward in-interface=ether1-Internet \
protocol=udp connection-state=!established,related action=drop
```

Aturan filter berikut untuk memblokir semua akses baik pada protokol TCP maupun UDP yang menuju ke Router (R1), selain layanan yang telah diizinkan pada aturan sebelumnya dan koneksi-koneksi yang telah terjalin (*established*) atau yang berkaitan (*related*).

```
[admin@R1] > ip firewall filter add chain=input in-interface=ether1-Internet \
protocol=tcp connection-state=!established,related action=drop

[admin@R1] > ip firewall filter add chain=input in-interface=ether1-Internet \
protocol=udp connection-state=!established,related action=drop
```

Hal terakhir yang perlu dilakukan terkait masalah keamanan akses, adalah mengganti *user* dan *password* default dari RouterOS. Secara default, RouterOS menggunakan *username* "admin" dan tanpa password, hal ini akan sangat membahayakan jika tidak diganti. Berikut adalah cara mengganti *user* dan *password* RouterOS pada RouterBoard MikroTik kantor pusat PT. **ABC**Net.

Menampilkan daftar user pada RouterOS.

```
[admin@R1] > user print
Flags: X - disabled
 #   NAME                    GROUP       ADDRESS     LAST-LOGGED-IN
 0   ;;; system default user
     admin                   full                    jan/02/19
```

Menambahkan *user* "abcnet" dan *password* "123456", password hanya digunakan dalam belajar saja, tidak disarankan saat implementasi di kondisi real.

```
[admin@R1] > user add name=abcnet password=123456 group=full
```

Menonaktifkan *user default* "admin" pada RouterOS.

```
[admin@R1] > user disable 0
```

Melakukan verifikasi hasil akhir konfigurasi user RouterOS. Tanda "X" pada baris *user* admin, menandakan bahwa *user* admin dalam kondisi nonaktif.

```
[admin@R1] > user print
Flags: X - disabled
 #   NAME                    GROUP       ADDRESS     LAST-LOGGED-IN
 0 X ;;; system default user
     admin                   full                    jan/02/19
 1   abcnet                  full
```

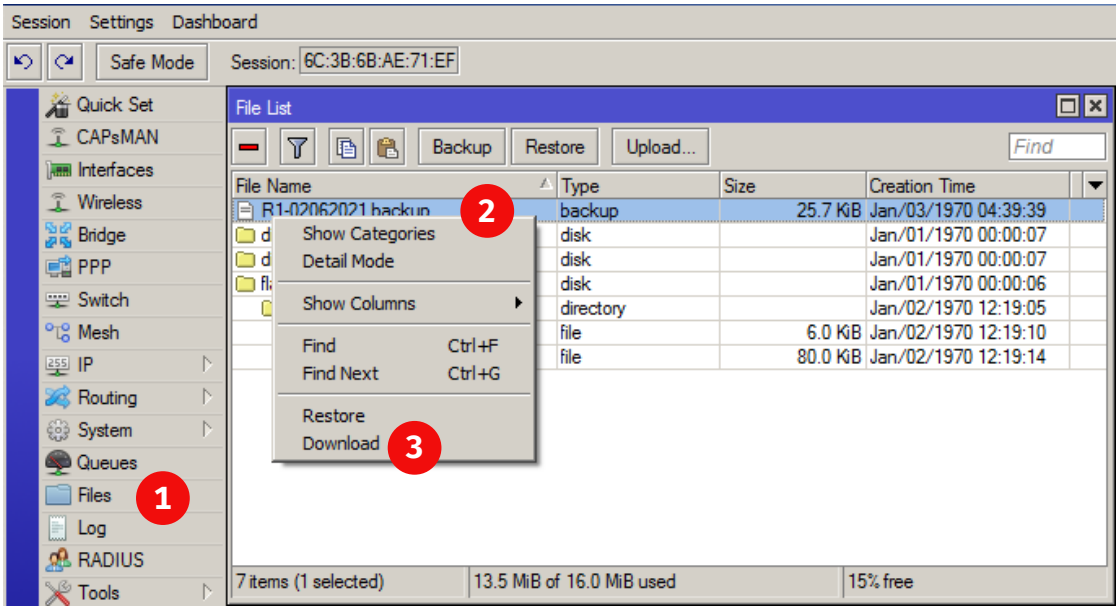
Lakukan tahapan yang sama pada RouterBoard MikroTik kantor cabang, untuk menambahkan *user* RouterOS yang baru, dan menonaktifkan *user default* RouterOS. Setelah keluar dari sistem RouterOS, maka berikutnya untuk masuk ke sistem harus menggunakan *user* dan *password* yang baru dibuat sebelumnya.

Sebaiknya secara berkala dilakukan *backup* pada sistem RouterOS, hal ini untuk mengantisipasi hal-hal yang tidak diinginkan, misalnya ada yang melakukan intrusi ke sistem RouterOS atau terjadi masalah pada sistem RouterOS sehingga tidak berfungsi baik. Keberadaan *backup* sangat membantu mengembalikan pada keadaan seperti semula. Berikut adalah tahapan konfigurasi sistem RouterOS.

File backup akan diberinama **`R1-02062021.backup`** disesuaikan dengan tanggal dilakukannya proses *backup*, hal ini agar mudah dilakukan identifikasi. *File backup* dalam kondisi tidak dienkripsi, hal ini utk mengantisipasi, jika NetAdmin lupa akan *password* masuk ke sistem RouterOS, maka file *backup* dapat diekstrak untuk menampilkan beberapa informasi penting, seperti *user* dan *password*, tentu saja hal ini dilakukan dengan bantuan aplikasi khusus. Perintah melakukan *backup* sebagai berikut.

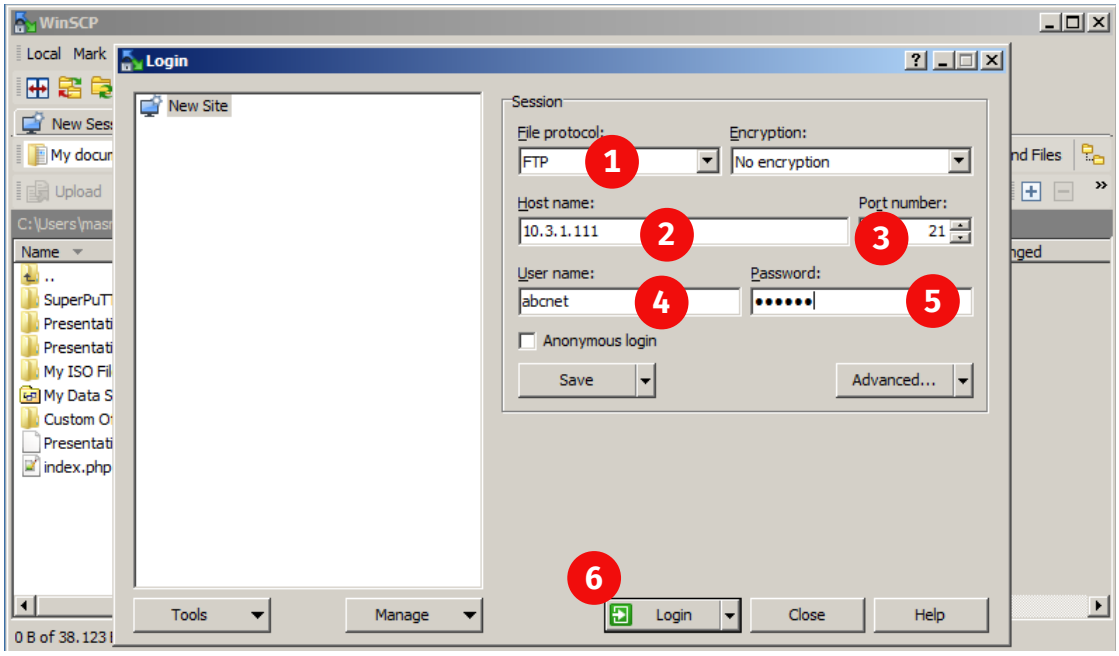
```
[abcnet@R1] > system backup save dont-encrypt=yes name=R1-02062021
```

File hasil *backup* dapat diunduh pada aplikasi Winbox, lewat (1) menu **Files** (2) lalu klik kanan pada *file backup* yang ingin diunduh, selanjutnya pilih (3)menu "Download" (Gambar 7.6).

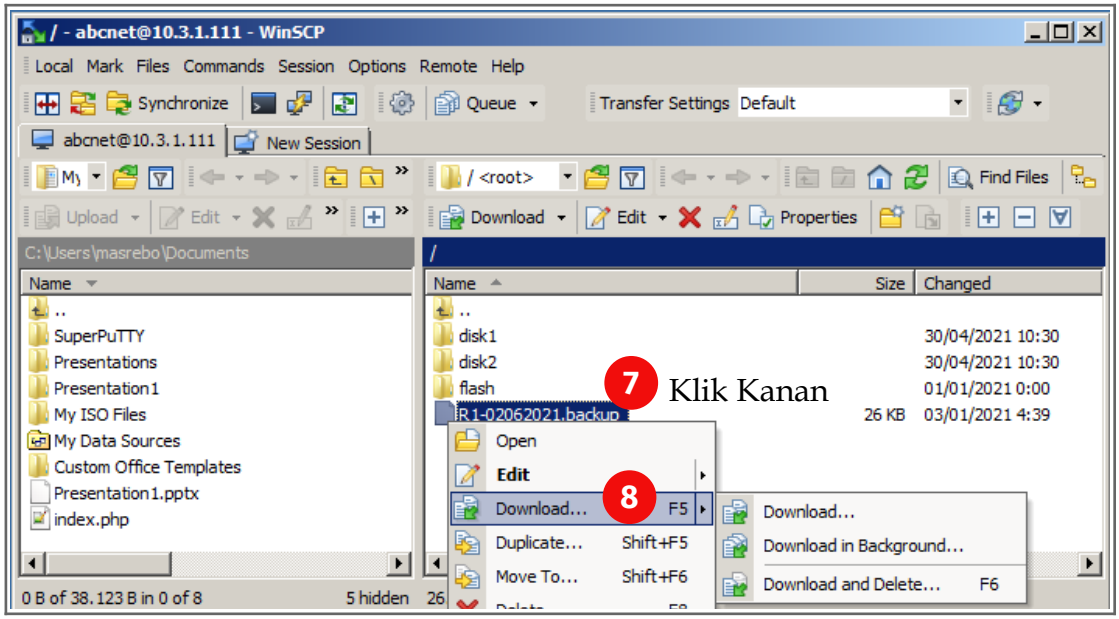


Gambar 7.6. Mengunduh File Backup RouterOS

Selain dapat diunduh lewat aplikasi WinBox, *file backup* RouterOS juga bisa diunduh lewat layanan *File Transfer Protocol* (FTP) menggunakan aplikasi WinSCP pada komputer *Client*. Buka aplikasi WinSCP, lalu *login* dengan *user* baru yang sebelumnya telah dibuat pada RouterOS (user: **abcnet**, password: **123456**) (Gambar 7.7). Setelah berhasil masuk, unduh *file backup* yang dibutuhkan (Gambar 7.8).



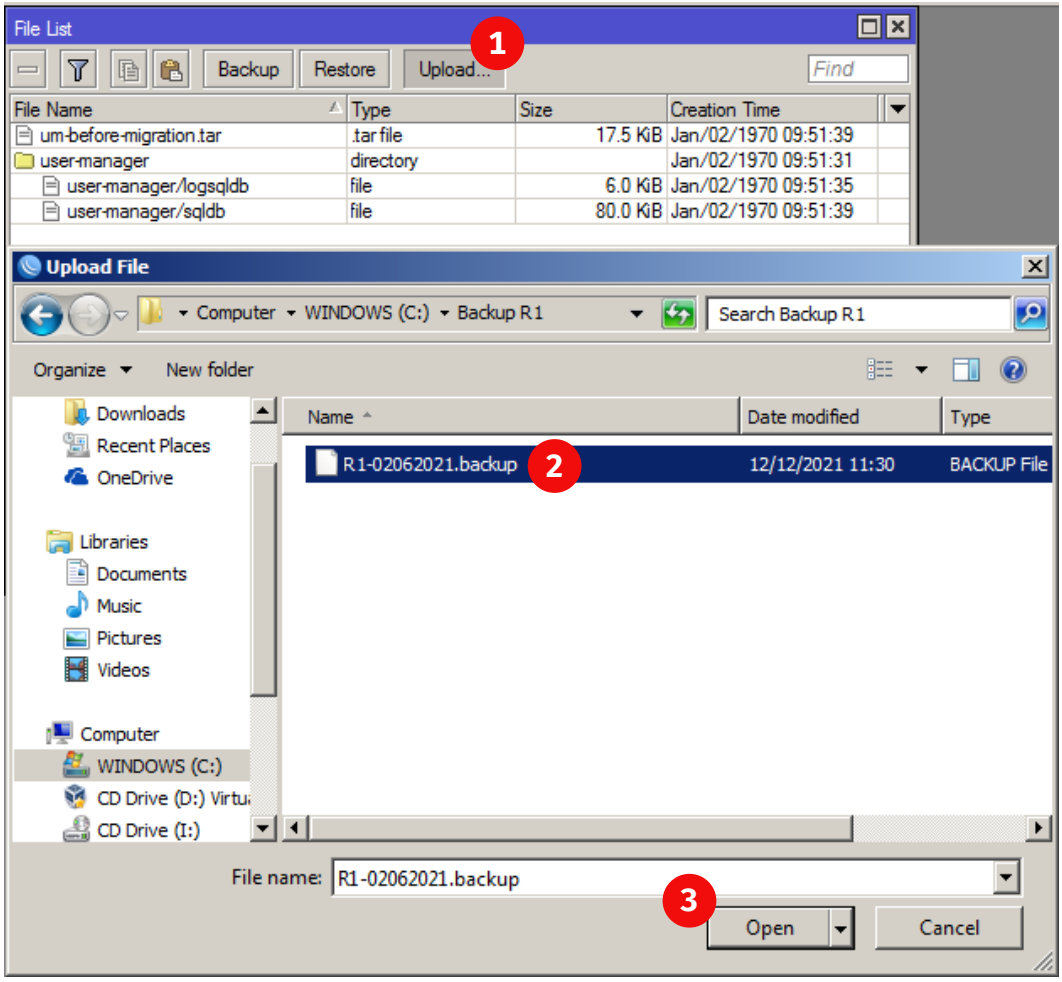
Gambar 7.7. Mengakses layanan FTP pada RouterOS



Gambar 7.8. Mengunduh file backup RouterOS

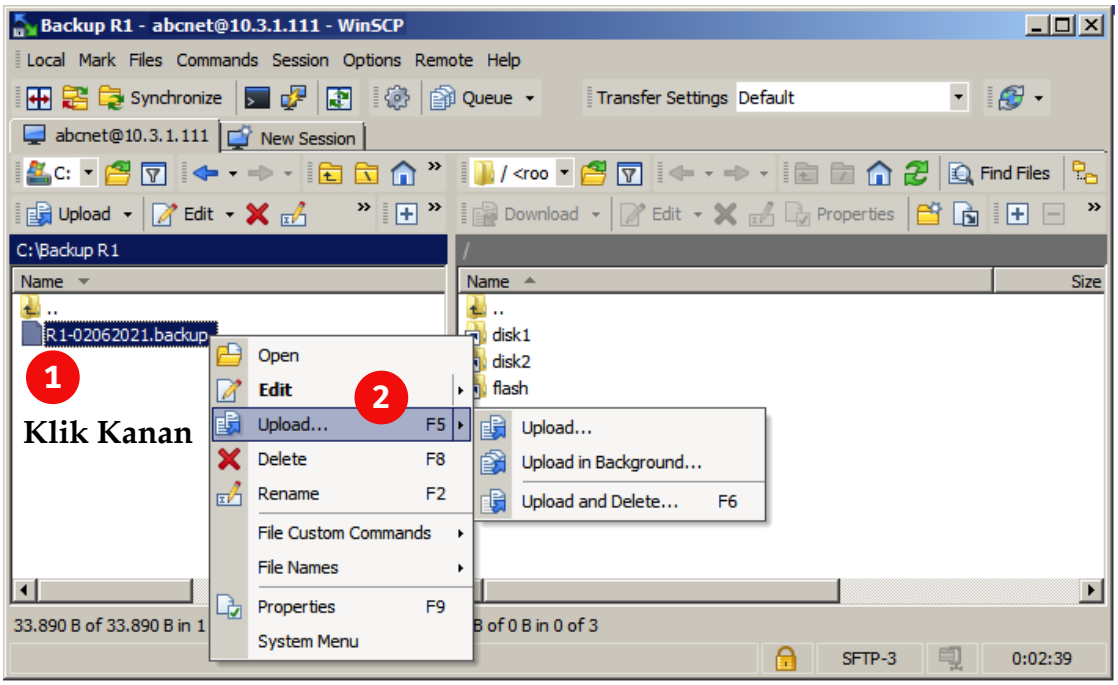
Setelah berhasil melakukan *backup* pada konfigurasi RouterOS R1 dan suatu saat *file backup* ini dibutuhkan, maka dilakukan proses *restore backup* kembali ke sistem RouterOS, langkahnya sebagai berikut.

Pada RouterOS pilih menu "**Files**" kemudian pilih tab "**Upload**" untuk mengunggah (*upload*) *file* hasil *backup*. Pada jendela **File Explorer**, cari lokasi penyimpanan dan pilih *file backup* tersebut, kemudian klik tombol "**Open**" (Gambar 7.9).



Gambar 7.9. Mengungah file backup lewat menu Files RouterOS

Selain menggunakan layanan *upload file backup* lewat RouterOS, bisa juga menggunakan layanan transfer *file* lewat SSH menggunakan aplikasi WinSCP, seperti tampak pada gambar 7.10.



Gambar 7.10. Mengunggah file backup lewat layanan SSH di aplikasi WinSCP

Setelah *file backup* berhasil diunggah (*upload*), selanjutnya melakukan *restore* pada sistem RouterOS. Setelah *file backup* di-*restore*, selanjutnya RouterBoard akan melakukan ***restart*** sistem dan selanjutnya memuat (*loading*) *file backup* tersebut ke sistem. Proses ini terjadi di belakang layar, dan tinggal menunggu hingga proses *restore* sistem selesai dilakukan. Berikut adalah perintah pada RouterOS untuk melakukan *restore file backup* ke sistem.

```
[abcnet@R1] > system backup load name=R1-02062021.backup
password: <langsung tekan tombol ENTER saja>
Restore and reboot? [y/N]: <tekan y>
```