Yogyakarta, Indonesia
October 09 - 10, 2015

MikroTik

Perencanaan dan Implementasi *Branch Office Network* Menggunakan RouterOS

Aliwarman Tarihoran

PT. Hendevane Indonesia

Objective

- Mempelajari tipe ***broadband connectivity***
- Mempelajari ***simple topology*** pada ***branch network***
- Mempelajari ***simple routing*** dan ***simple NAT*** pada ***branch network***
- Mempelajari ***simple VPN*** pada ***branch network***

Tentang Saya

RouterOS Broadband Connectivity

Skenario Branch Network

Konfigurasi Routing & NAT pada Branch Network

Konfigurasi VPN pada Branch Network

Profil Saya

Nama Lengkap

Aliwarman Tarihoran
id.linkedin.com/in/aliwarman

Pendidikan Formal

2006: Bachelor of Telecommunication Engineering @STT Telkom
2011: Magister Information of Technology @Universitas Indonesia

Pengalaman Kerja

2007 @ZTE, Indonesia
2007 @STMI, UAE (United Arab Emirates)
2008 @AXIS Telekom, Indonesia
2008 @Netsphere, Indonesia
2012 - Now (Consultant and Trainer) @ PT. Hendevane Indonesia

Profil Saya

Sertifikasi Profesional

MTCNA, license 1211NA149
MTCRE, license 1211RE033
MTCINE, license 1503INE021
MikroTik Certified Trainer, license TR0277
Juniper JNCIP-SEC, license F5SSSCQ5WB4Q1WDG
CCIE RS Written

Tentang Saya

RouterOS Broadband Connectivity

Skenario Branch Network

Konfigurasi Routing & NAT pada Branch Network

Konfigurasi VPN pada Branch Network

WAN pada Brach Network

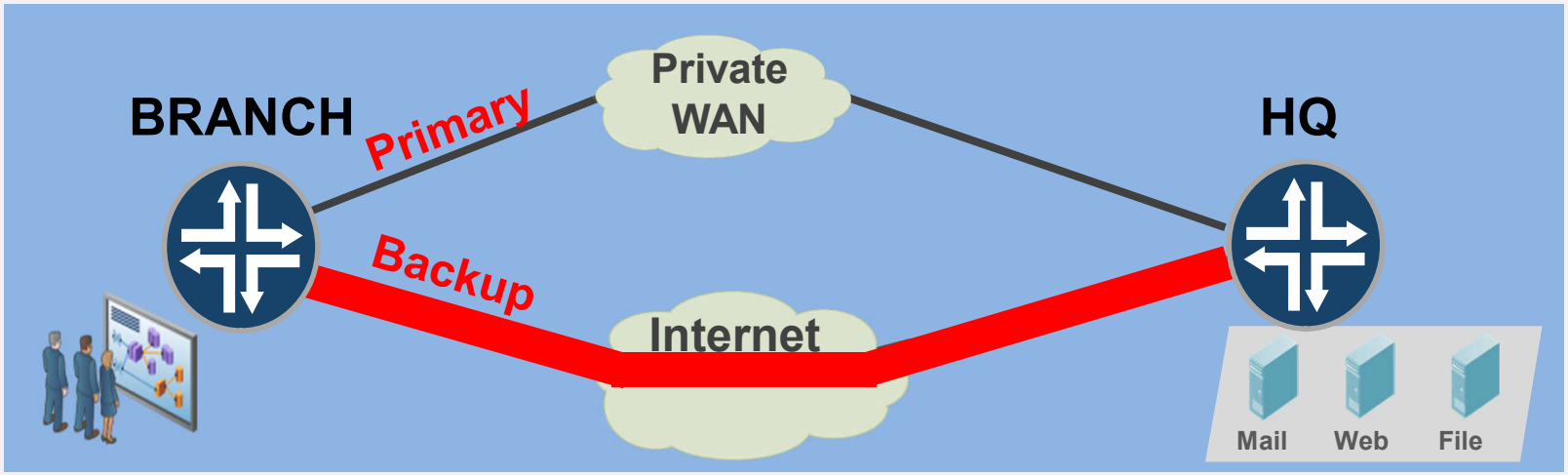
- Tipe dari **remote site** mempengaruhi ketika melakukan pemilihan **design WAN (Wide Area Network)**
  - Contoh:
    - **Regional Site** lebih mengutamakan link ***primary/backup*** dan ***routing protocol*** untuk memilih best path
    - **Branch Site** lebih mengutamakan ***link*** VPN dan static route

WAN pada Brach Network

- Pada **Branch Network** biasanya melewatkan tipe-tipe aplikasi yang berbeda, misalkan; ***voice, video, web-based application***, dsb
  - Oleh sebab itu pada sisi **Branch** membutuhkan bandwith yang besar

Backup Link pada Brach Network

- Dengan menggunakan ***backup link***, maka **Branch Network** menjadi lebih elastis
- ***Backup link*** tersebut dapat menggunakan koneksi ***broadband***.
  - Supaya koneksi lebih aman, maka dapat digunakan VPN



Pemilihan Teknologi Broadband

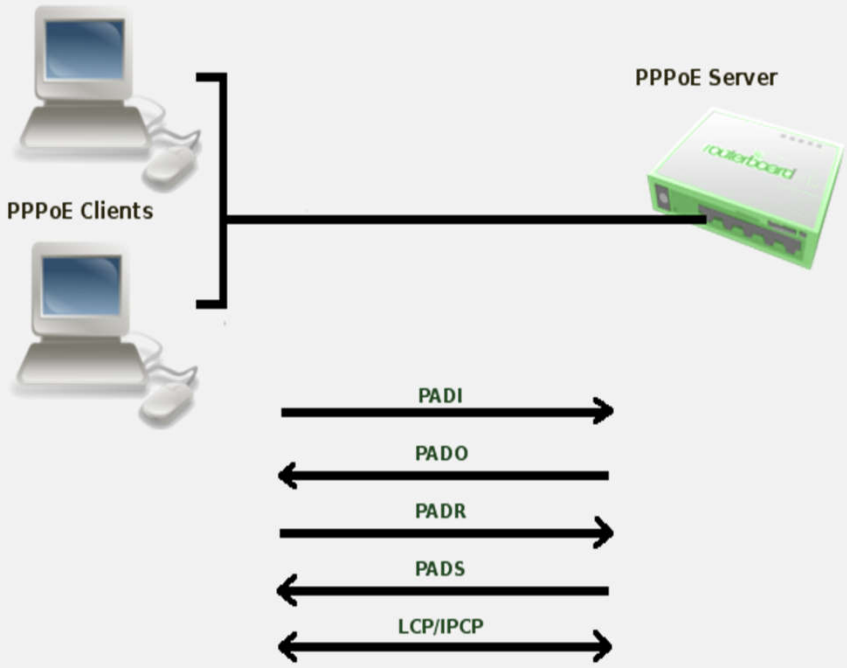
- Teknologi DSL
  - Saat ini, banyak ISP menggunakan protocol ***PPPoE (Point to Point Protocol over Ethernet)***
    - PPoE memiliki kemampuan user management dan accounting
  - PPoE Pada RouterOS
    - Menggunakan standarisasi **RFC 2516**
    - Dapat bertindak sebagai ***PPoE Client*** dan ***PPoE Server***
    - Packages yang dibutuhkan: **ppp**
    - ***Standard License***: Level1 (1 interface), Level3 (200 interface), level4 (200 interface), Level5 (500 interface), Level6 (unlimited)

PPoE Operation

Discovery stage

Sebuah client akan melakukan discover access concentrator (ppoe server) dan menciptakan ppoe session. Berikut adalah step-step yang terjadi:

- PPPoE Active Discovery **Initialization**
- PPPoE Active Discovery **Offer**
- PPPoE Active Discovery **Request**
- PPPoE Active Discovery **Session confirmation**



Session

Setelah discovery stage selesai, kedua peer akan mengetahui PPoE session ID satu sama lain

Surce: http://wiki.mikrotik.com/wiki/Manual:Interface/PPPoE

Tentang Saya

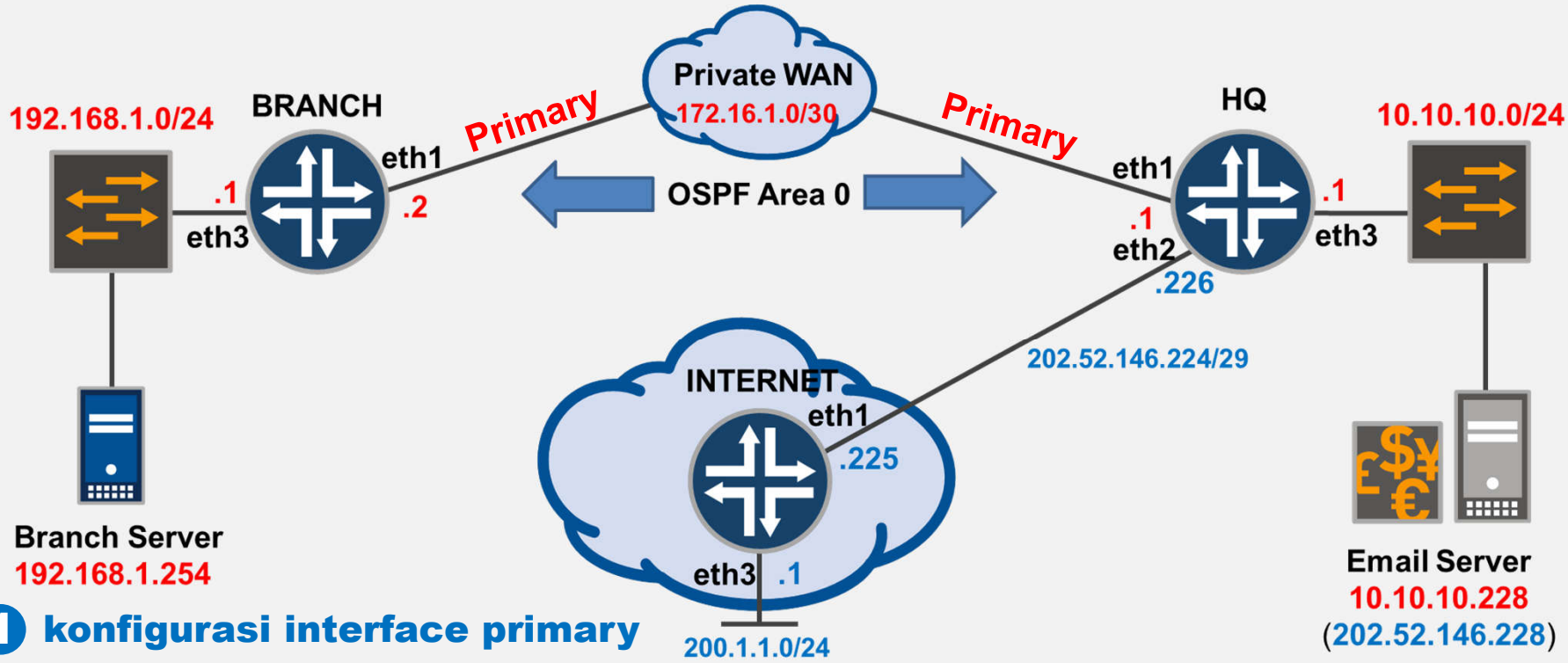
RouterOS Broadband Connectivity

Skenario Branch Network

Konfigurasi Routing & NAT pada Branch Network

Konfigurasi VPN pada Branch Network

Topologi Branch Network (Step 1)

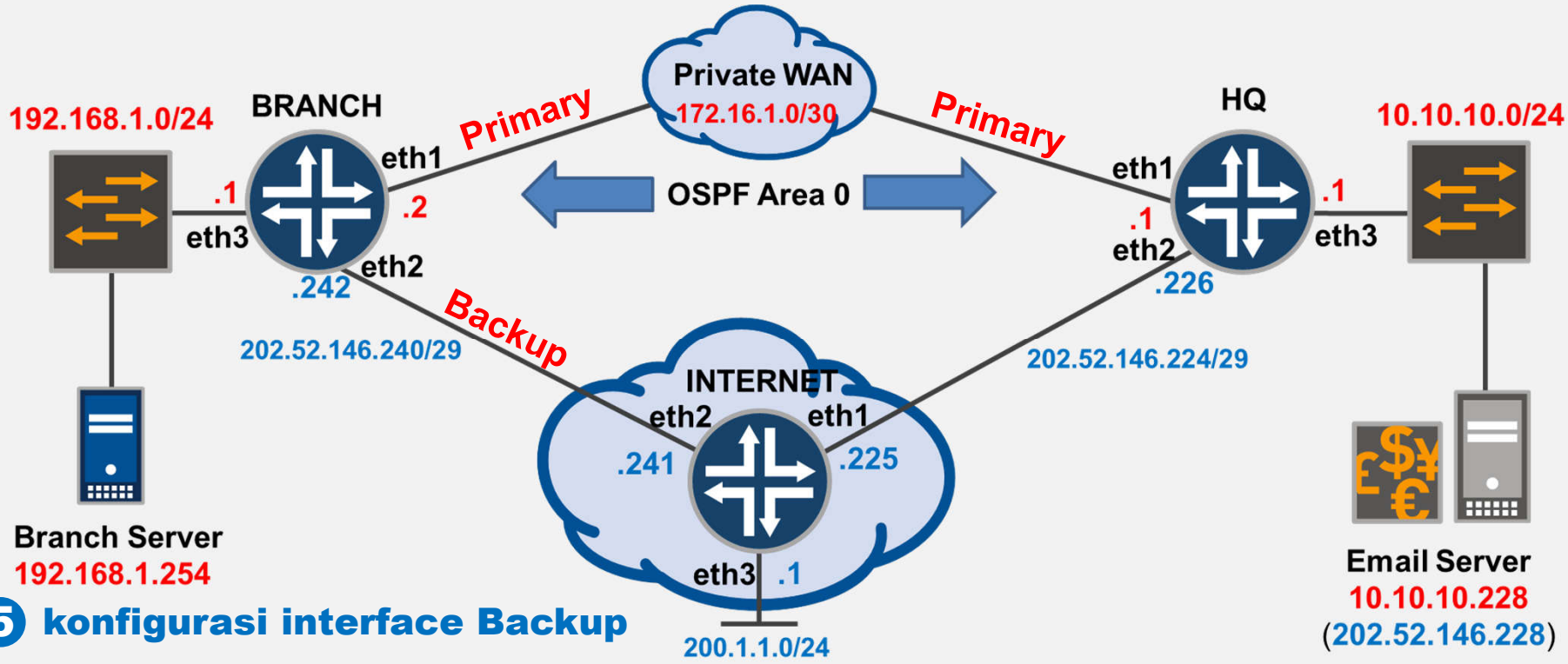


1. konfigurasi interface primary
2. konfigurasi OSPF pada HQ dan Branch
3. konfigurasi NAT pada HQ
4. konfigurasi Default Route dan Redistribusi pada HQ

Keterangan (Step 1)

- Informasi rute antara **Branch** dan **HQ (Head Quarter)** menggunakan OSPF area 0 melalui link Private WAN
- User LAN pada Branch melakukan akses internet menggunakan ***default route*** yang diberikan oleh **HQ Router**
- Semua trafik yang keluar dari interface **ether2** pada **HQ** akan ditranlasikan menggunakan NAT

Topologi Branch Network (Step 2)



5. konfigurasi interface Backup
6. konfigurasi PPoE pada Branch
7. konfigurasi NAT pada Branch
8. konfigurasi Default Route pada Branch

Keterangan (Step 2)

- Biasanya Perusahaan menyediakan ***fault tolerance*** pada **Branch Network**. Oleh sebab itu disediakan sebuah ***link*** alternatif menggunakan jaringan Internet.
  - Pada skenario, koneksi internet ***backup*** ditambahkan
    - Koneksi tersebut adalah ***backup route*** untuk ***link Private WAN (primary)***

Tentang Saya

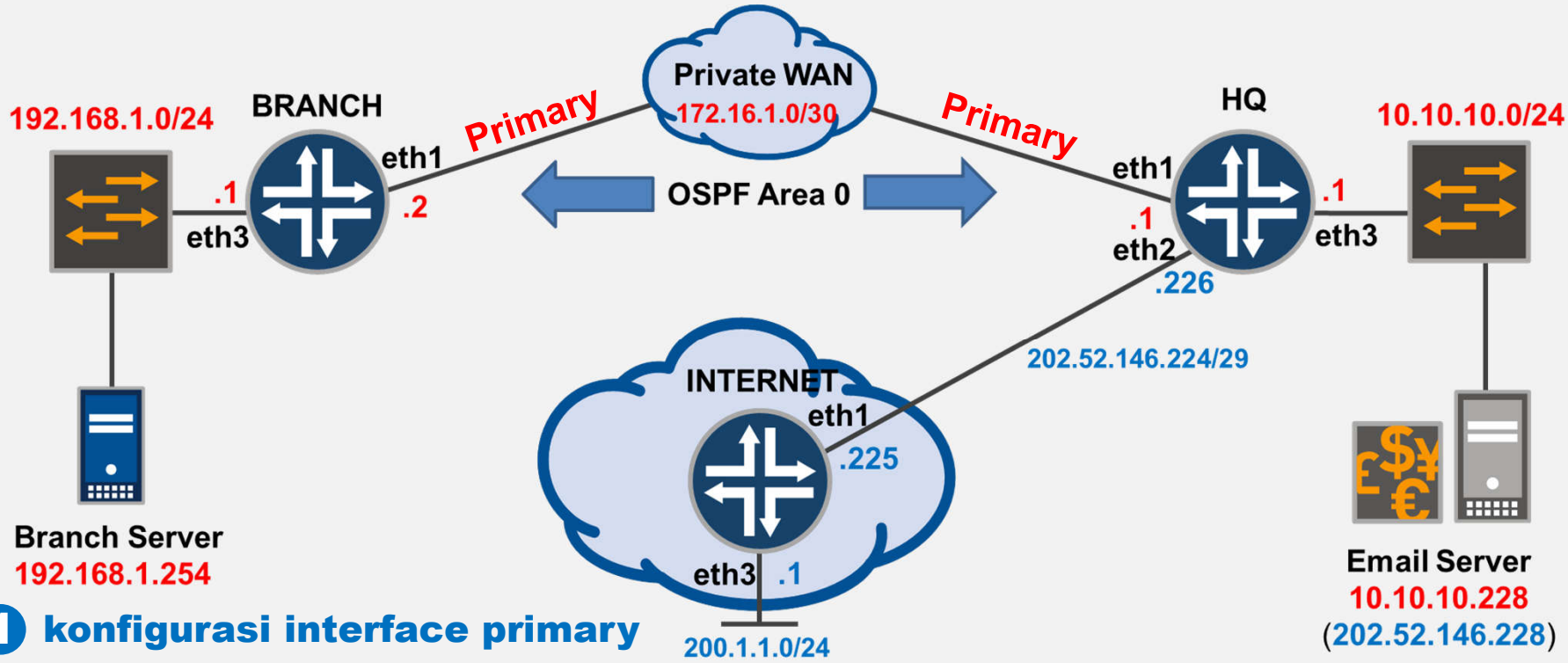
RouterOS Broadband Connectivity

Skenario Branch Network

Konfigurasi Routing & NAT pada Branch Network

Konfigurasi VPN pada Branch Network

Topologi Branch Network (Step 1)



1. konfigurasi interface primary
2. konfigurasi OSPF pada HQ dan Branch
3. konfigurasi NAT pada HQ
4. konfigurasi Default Route dan Redistribusi pada HQ

Interface pada HQ Router

- Konfigurasi Interface HQ Router

```
[admin@HQ] > /ip address add address=172.16.1.1/24 interface=ether1

[admin@HQ] > /ip address add address=202.52.146.226/29 interface=ether2

[admin@HQ] > /ip address add address=10.10.10.1/24 interface=ether3

[admin@HQ] > /interface bridge add name=Email-Server
[admin@HQ] > /ip address add address=10.10.10.228/24 interface=Email-
Server

[admin@HQ] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    10.10.10.1/24      10.10.10.0      ether3
 1    172.16.1.1/24      172.16.1.0      ether1
 2    202.52.146.226/29  202.52.146.224  ether2
 3    10.10.10.228/24    10.10.10.0      Email-Server
```

Interface pada Internet Router

- Konfigurasi Interface **Internet Router**

```
[admin@INTERNET] > /ip address add address=202.52.146.225/29
interface=ether1

[admin@INTERNET] > /ip address add address=200.1.1.1/24 interface=ether3

[admin@INTERNET] > /interface bridge add name=External-Server
[admin@INTERNET] > /ip address add address=200.1.1.254/24
interface=External-Server

[admin@INTERNET] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    200.1.1.1/24       200.1.1.0       ether3
 1    202.52.146.225/29  202.52.146.224  ether1
 2    200.1.1.254/24     200.1.1.0       External-Server
```

Interface pada Branch Router

- Konfigurasi Interface **Branch Router**

```
[admin@BRANCH] > /ip address add address=172.16.1.2/24 interface=ether1

[admin@BRANCH] > /ip address add address=192.168.1.1/24 interface=ether3

[admin@BRANCH] > /interface bridge add name=Branch-Server
[admin@BRANCH] > /ip address add address=192.168.1.254/24
interface=Branch-Server

[admin@BRANCH] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    192.168.1.1/24     192.168.1.0     ether3
 1    172.16.1.2/24      172.16.1.0      ether1
 2    192.168.1.254/24   192.168.1.0     Branch-Server
```

OSPF Overview pada RouterOS

- OSPF version 2 (**RFC 2328**)
- Merupakan protocol ***link state*** yang bertanggung jawab mengumpulkan rute pada jaringan dinamis
- Menentukan ***shortest path*** (jalur terpendek) menggunakan algoritma Dijkstra
- Sekumpulan router dapat digabung secara bersama (disebut juga Area)
  - Setiap area akan memiliki ***link-state database*** yang terpisah
  - ***Best Practice***: dalam satu area, maksimum 50 router

http://wiki.mikrotik.com/wiki/Manual:Routing/OSPF

Routing pada HQ Router

- Konfigurasi OSPF Area 0

```
[admin@HQ] > /routing ospf network add network=172.16.1.0/24 area=backbone
[admin@HQ] > /routing ospf network add network=10.10.10.0/24 area=backbone

[admin@HQ] > /routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
 #    INTERFACE                            COST PRIORITY NETWORK-TYPE
 0 D  ether1                                 10        1 broadcast      none
 1 D  ether3                                 10        1 broadcast      none
 2 D  Email-Server                           10        1 broadcast      none
```

Routing pada Branch Router

- Konfigurasi OSPF Area 0

```
[admin@BRANCH] > /routing ospf network add network=172.16.1.0/24
area=backbone
[admin@BRANCH] > /routing ospf network add network=192.168.1.0/24
area=backbone

[admin@BRANCH] > /routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
 #    INTERFACE                            COST PRIORITY NETWORK-TYPE
 0 D  ether1                                 10        1 broadcast      none
 1 D  ether3                                 10        1 broadcast      none
 2 D  Branch-Server                          10        1 broadcast      none
```

Verifikasi Routing Table OSPF

- Verifikasi routing table pada **HQ Router**

```
[admin@HQ] > /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 ADC  10.10.10.0/24      10.10.10.1      ether3                    0
                                           Email-Server
 1 ADC  172.16.1.0/24      172.16.1.1      ether1                    0
 2 ADo  192.168.1.0/24                     172.16.1.2              110
 3 ADC  202.52.146.224/29  202.52.146.226  ether2                    0
```

Verifikasi Routing Table OSPF

- Verifikasi routing table pada **Branch Router**

```
[admin@BRANCH] > 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 ADo  10.10.10.0/24                      172.16.1.1              110
 1 ADC  172.16.1.0/24      172.16.1.2      ether1                    0
 2 ADC  192.168.1.0/24     192.168.1.1     ether3                    0
                                           Branch-Server
```

Static Route Overview

- Administrator menambahkan rute secara manual ke dalam router
- Keuntungan menggunakan ***Static Route***
  - Tidak ada beban pada CPU
  - Tidak ada penggunaan bandwidth antar router
  - Menambah keamanan jaringan, karena administrator bisa memilih network tertentu yang ditambahkan kedalam table routing
- Kekurangan menggunakan ***Static Route***
  - Tidak cocok untuk jaringan besar
  - Administrator harus benar-benar memahami bagaimana koneksi router satu sama lain terhubung

http://wiki.mikrotik.com/wiki/Manual:Simple_Static_Routing

Static Route pada HQ Router

- Konfigurasi ***Static Route***

```
[admin@HQ] > /ip route add dst-address=0.0.0.0/0
gateway=202.52.146.225

[admin@HQ] > 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                          202.52.146.225             1
 1 ADC  10.10.10.0/24      10.10.10.1      ether3                     0
                                           Email-Server
 2 ADC  172.16.1.0/24      172.16.1.1      ether1                     0
 3 ADo  192.168.1.0/24                     172.16.1.2               110
 4 ADC  202.52.146.224/29  202.52.146.226  ether2                     0
```

Verifikasi Static Route pada HQ Router

- Menggunakan ***ping***

```
[admin@HQ] > ping 200.1.1.254 count=3
HOST                                     SIZE TTL TIME  STATUS
200.1.1.254                                56  64 1ms
200.1.1.254                                56  64 3ms
200.1.1.254                                56  64 2ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-
rtt=3ms
```

- Test Koneksi dari ***Email Server*** ke ***Internet***

```
[admin@HQ] > ping 200.1.1.254 src-address=10.10.10.228 count=3
HOST                                     SIZE TTL TIME  STATUS
200.1.1.254                                             timeout
200.1.1.254                                             timeout
200.1.1.254                                             timeout
    sent=3 received=0 packet-loss=100%
```

NAT Overview

- ***Network Address Translation (NAT)*** adalah standarisasi internet yang memungkinkan ***Local Area Network (LAN)*** dapat berkomunikasi dengan alamat publik
- Tipe NAT pada RouterOS:
  - source NAT atau ***srcnat***, melakukan translasi dari alamat private ke alamat publik
  - destionation NAT atau ***dstnat***, melakukan translasi dari alamat publik ke alamat ***private***

Source: http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT

Source NAT pada HQ Router

- Implementasi source NAT pada **HQ Router**, sehingga Internal ***Network*** dapat berkomunikasi dengan Internet (alamat publik)

```
[admin@HQ] > /ip firewall nat add chain=srcnat src-
address=10.10.10.0/24 action=masquerade
[admin@HQ] > /ip firewall nat add chain=srcnat src-
address=192.168.1.0/24 action=masquerade

[admin@HQ] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade src-
address=10.10.10.0/24 log=no log-prefix=""

 1    chain=srcnat action=masquerade src-
address=192.168.1.0/24 log=no log-prefix=""
```

Verifikasi Source NAT pada HQ Router

- Test Koneksi dari ***Email Server*** ke ***Internet***

```
[admin@HQ] > ping 200.1.1.254 src-address=10.10.10.228 count=3
HOST                                     SIZE TTL TIME  STATUS
200.1.1.254                                56  64 1ms
200.1.1.254                                56  64 1ms
200.1.1.254                                56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-
rtt=1ms
```

Redistribusi Static Route ke OSPF

- Supaya **Branch Router** dapat terkoneksi ke Internet, maka **HQ Router** harus melakukan redistribusi ***Static Route*** ke OSPF dengan perintah dibawah ini.

```
[admin@HQ] > /routing ospf instance set distribute-
default=always-as-type-2
numbers: 0
[admin@HQ] > /routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=0.0.0.0 distribute-
default=always-as-type-2 redistribute-connected=no
      redistribute-static=no redistribute-rip=no
redistribute-bgp=no redistribute-other-ospf=no
      metric-default=1 metric-connected=20 metric-static=20
metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-
filter=ospf-out
```

Verifikasi pada Branch Router

- Verifikasi ***Routing Table***

```
[admin@BRANCH] > 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 ADo  0.0.0.0/0                          172.16.1.1              110
 1 ADo  10.10.10.0/24                      172.16.1.1              110
 2 ADC  172.16.1.0/24      172.16.1.2      ether1                    0
 3 ADC  192.168.1.0/24     192.168.1.1     ether3                    0
                                           Branch-Server
```

- Test Koneksi dari ***Branch Client*** ke ***Internet***

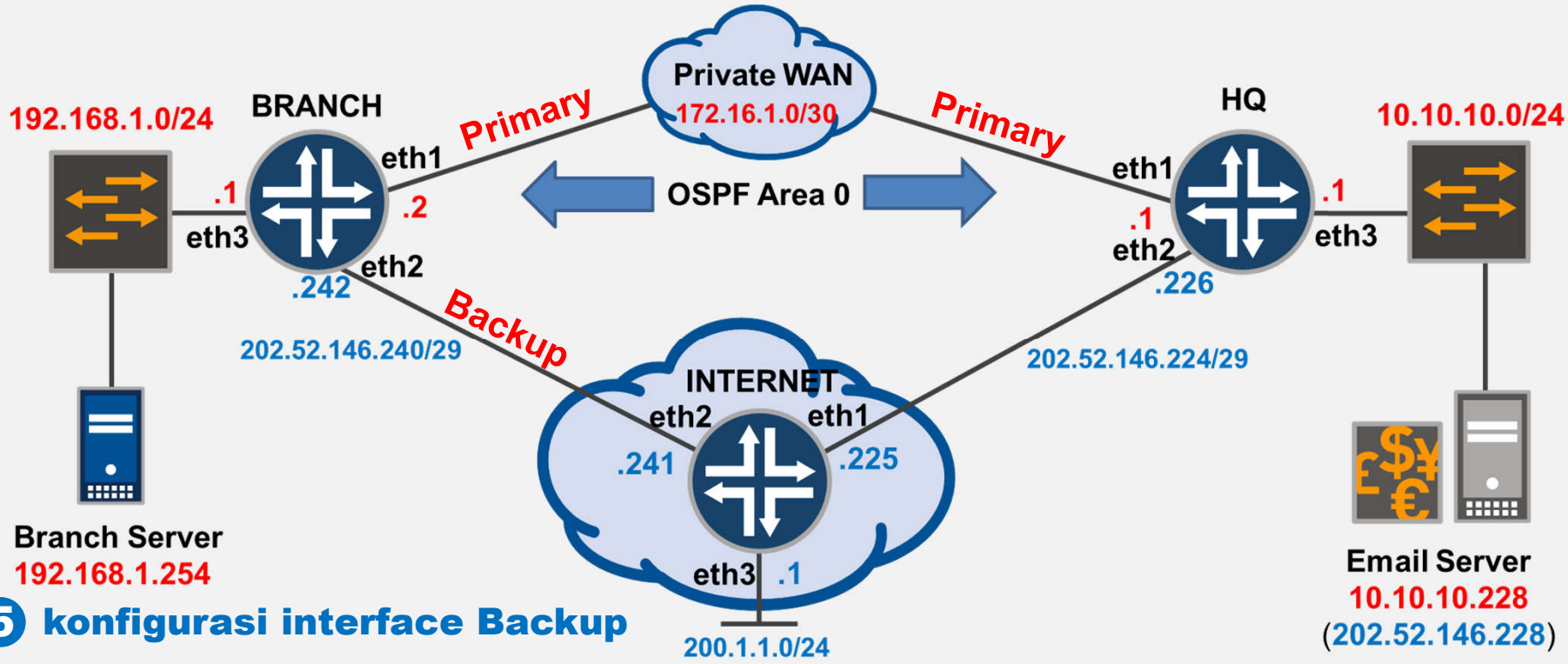
```
[admin@BRANCH] > ping 200.1.1.254 src-address=192.168.1.254 count=3
HOST                                     SIZE TTL TIME  STATUS
200.1.1.254                                56  63 3ms
200.1.1.254                                56  63 2ms
200.1.1.254                                56  63 2ms
    sent=3 received=3 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-
rtt=3ms
```

Destination NAT pada HQ Router

- Implementasi destination NAT pada **HQ Router**, sehingga ***Email server*** dapat di akses dari Internet

```
[admin@HQ] > /ip address add address=202.52.146.228/32
interface=ether2

[admin@HQ] > /ip firewall nat add chain=dstnat dst-
address=202.52.146.228 action=dst-nat to-
addresses=10.10.10.228
```

Topologi Branch Network (Step 2)



5. konfigurasi interface Backup
6. konfigurasi PPoE pada Branch
7. konfigurasi NAT pada Branch
8. konfigurasi Default Route pada Branch

Koneksi Backup Link

- Menggunakan protokol PPoE
- **Internet Router** sebagai PPoE Server
- **Branch Router** sebagai PPoE Client
- PPoE Server Profiles default
  - Local Address 202.52.146.241
- PPoE Server Secrets
  - Username: htp
  - Password: htp123

Konfigurasi Backup Link

- PPoE Server pada **Internet Router**

```
[admin@INTERNET] > /ip address add address=202.52.146.241/24
interface=ether2
[admin@INTERNET] > /ppp profile set name=default local-
address=202.52.146.241 remote-address=202.52.146.242
numbers: 0
[admin@INTERNET] > /ppp secret add name=htp password=htp123
service=pppoe profile=default
[admin@INTERNET] > /interface pppoe-server server add
service-name=htp interface=ether2 disabled=no
```

- PPoE Client pada **Branch Router**

```
[admin@BRANCH] > /interface pppoe-client add interface=ether2
user=htp password=htp123 disabled=no
```

Verfikasi Backup Link

- Interface ***Backup Link*** pada **Internet Router**

```
[admin@INTERNET] > /ppp active print
Flags: R - radius
 #   NAME         SERVICE CALLER-ID        ADDRESS         UPTIME   ENCODING
 0   htp            pppoe   00:00:AB:E1:87:01 202.52.146.242  4m8s

[admin@INTERNET] > ping 202.52.146.242 count=3
HOST                                     SIZE TTL TIME  STATUS
202.52.146.242                             56  64 1ms
202.52.146.242                             56  64 1ms
202.52.146.242                             56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-
rtt=1ms
```

Verfikasi Backup Link

- Interface ***Backup Link*** pada **Branch Router**

```
[admin@BRANCH] > /interface print from=6
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE        MTU L2MTU  MAX-L2MTU MAC-ADDRESS
 0  R  pppoe-out1                          pppoe-out   1480

[admin@BRANCH] > ip address print from=4
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 202.52.146.242/32  202.52.146.241  pppoe-out1

[admin@BRANCH] > ping 202.52.146.241 count=3
HOST                                     SIZE TTL TIME  STATUS
202.52.146.241                             56  64 1ms
202.52.146.241                             56  64 1ms
202.52.146.241                             56  64 1ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-
rtt=1ms
```

Konsep Best Route

- Router akan memilih ***route*** berdasarkan paramater dibawah ini:
  - ***Destination Address*** yang lebih spesifik
    - Contoh: ***Destination Address*** 172.16.1.0/24 lebih spesifik dibandingkan dengan 172.16.0.0/16
  - ***Distance***
    - Router akan memilih ***distance*** yang terkecil

Routing Protocol	Default Distance
connected routes	0
static routes	1
eBGP	20
OSPF	110
RIP	120
MME	130
iBGP	200

Source: http://wiki.mikrotik.com/wiki/Manual:IP/Route

Rekayasa Trafik (Basic)

- Melakukan rekayasa trafik dasar pada **Branch Router** dengan menambahkan ***default route*** melalui backup link (distance 111)

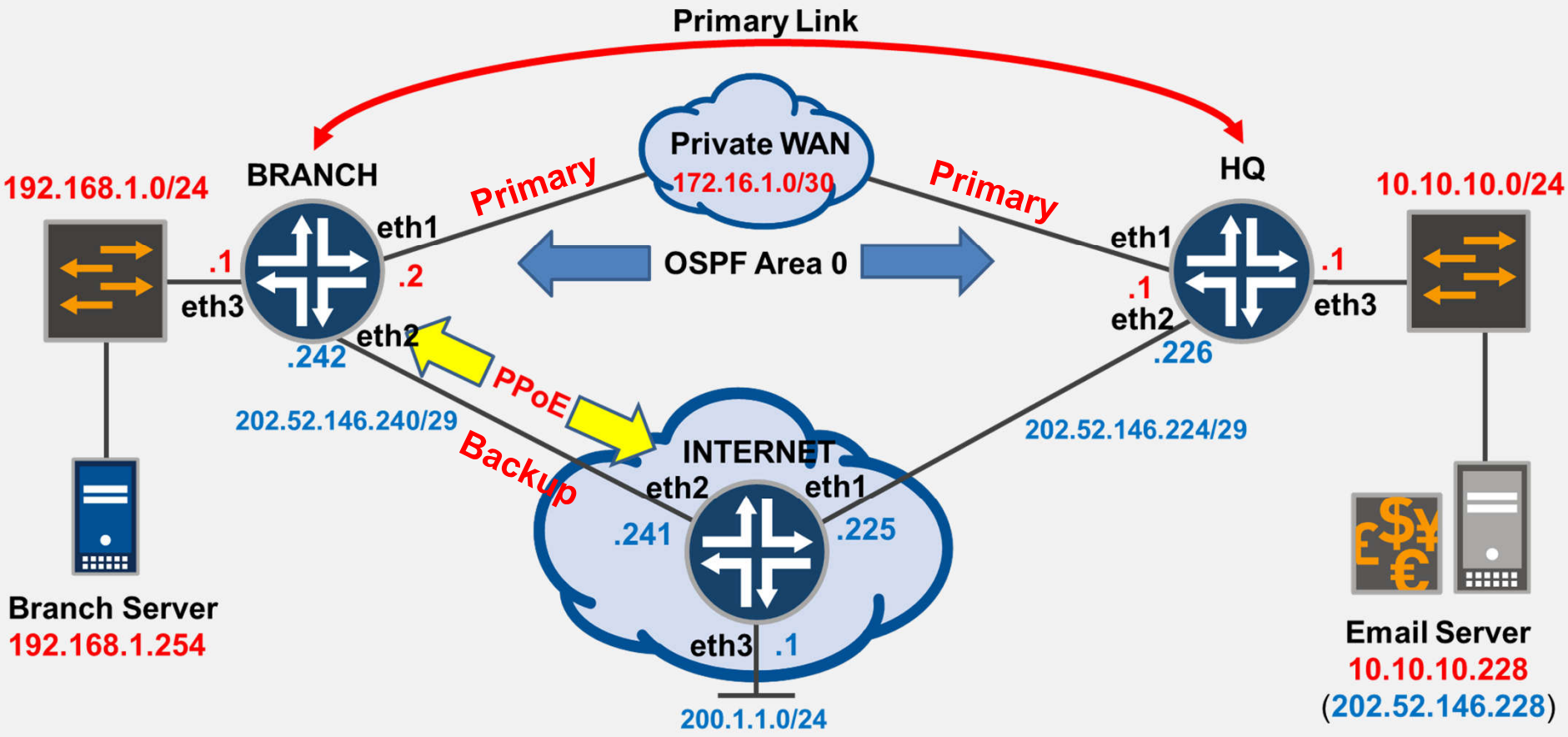
```
[admin@BRANCH] > /ip route add dst-address=0.0.0.0/0
gateway=202.52.146.241 distance=111

[admin@BRANCH] > 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 ADo  0.0.0.0/0                          172.16.1.1              110
 1   S  0.0.0.0/0                          202.52.146.241          111
 2 ADo  10.10.10.0/24                      172.16.1.1              110
 3 ADC  172.16.1.0/24      172.16.1.2      ether1                    0
 4 ADC  192.168.1.0/24     192.168.1.1     ether3                    0
                                           Branch-Server
 5 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                0
```

Rekayasa Trafik (Basic)

- Tambah source NAT pada **Branch Router**
  - Jika trafik yang berasal dari 192.168.1.0/24 menuju selain 10.10.10.0/24 akan dialirkan melalui NAT.

```
[admin@BRANCH] > /ip firewall nat

[admin@BRANCH] /ip firewall nat> add chain=srcnat src-
address=192.168.1.0/24 dst-address=!10.10.10.0/24 out-
interface=pppoe-out1 action=masquerade

[admin@BRANCH] > /ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade src-
address=192.168.1.0/24 dst-address=!10.10.10.0/24
      out-interface=pppoe-out1 log=no log-prefix=""
```

Flow Trafik Test 1

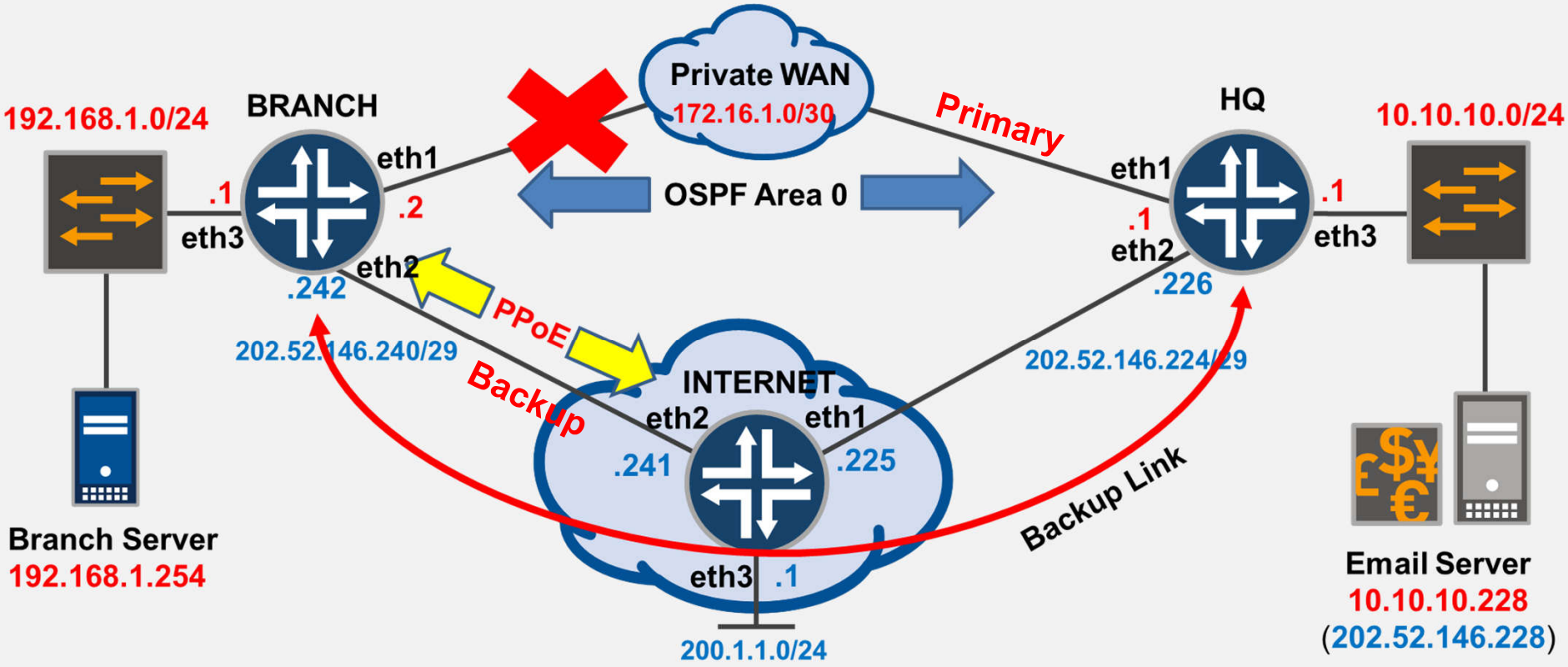


Flow Trafik Test 1

- Kondisi **Link Primary** dan **Link Backup** ***active***

```
[admin@BRANCH] > 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 ADo  0.0.0.0/0                          172.16.1.1               110
 1   S  0.0.0.0/0                          202.52.146.241           111
 2 ADo  10.10.10.0/24                      172.16.1.1               110
 3 ADC  172.16.1.0/24      172.16.1.2      ether1                     0
 4 ADC  192.168.1.0/24     192.168.1.1     ether3                     0
                                           Branch-Server
 5 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                 0

[admin@BRANCH] > /tool traceroute 200.1.1.254 src-
address=192.168.1.254
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 172.16.1.1                         0%    3   1.1ms     1.6     1.1     2.5     0.6
 2 200.1.1.254                        0%    3     2ms     2.3       2     2.8     0.4
```

Flow Trafik Test 2

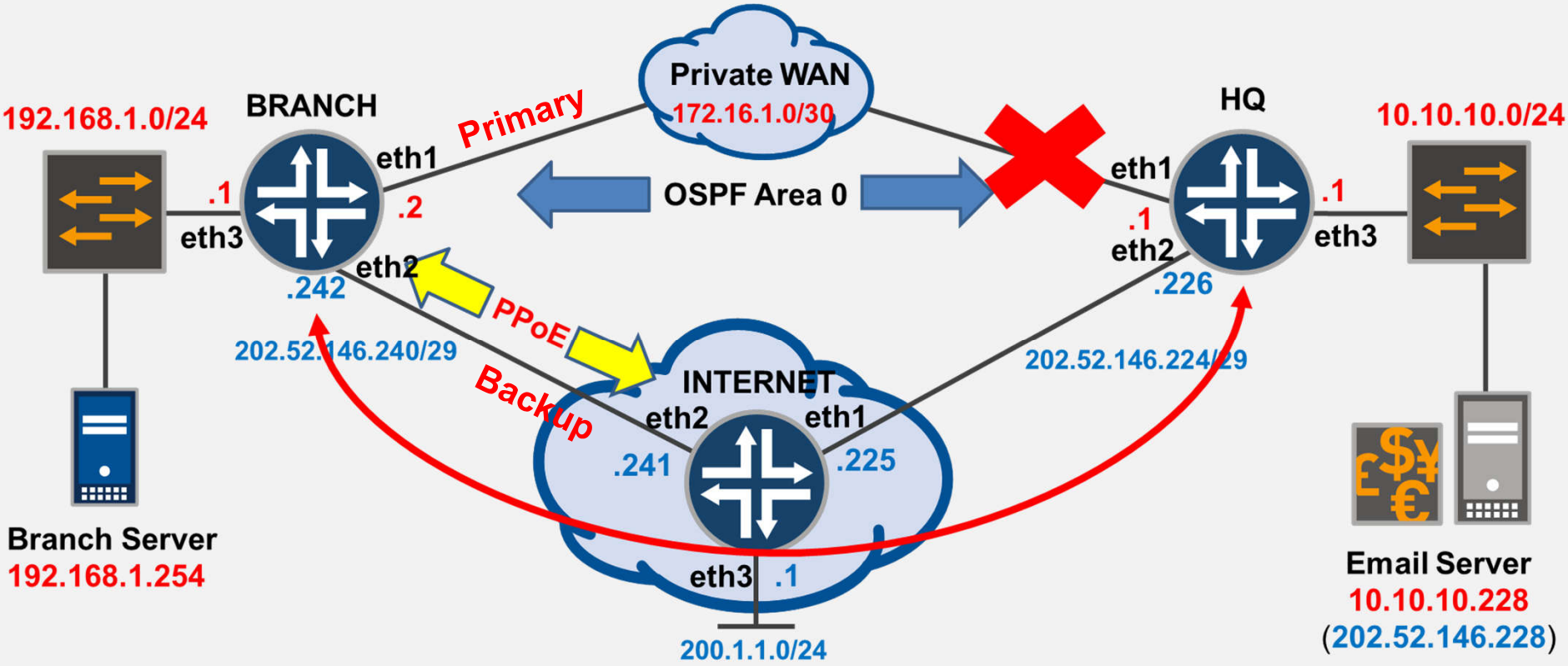


Flow Trafik Test 2

- Kondisi **Link Primary** down dan **Link**

```
[admin@BRANCH] > /interface disable
numbers: 0

[admin@BRANCH] > 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                          202.52.146.241           111
 1 ADC  192.168.1.0/24     192.168.1.1     ether3                     0
                                           Branch-Server
 2 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                 0

[admin@BRANCH] > /tool traceroute 200.1.1.254 src-
address=192.168.1.254
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 200.1.1.254                       0%    3   1.2ms     1.5     1.2     1.7     0.2
```

Flow Trafik Test 3

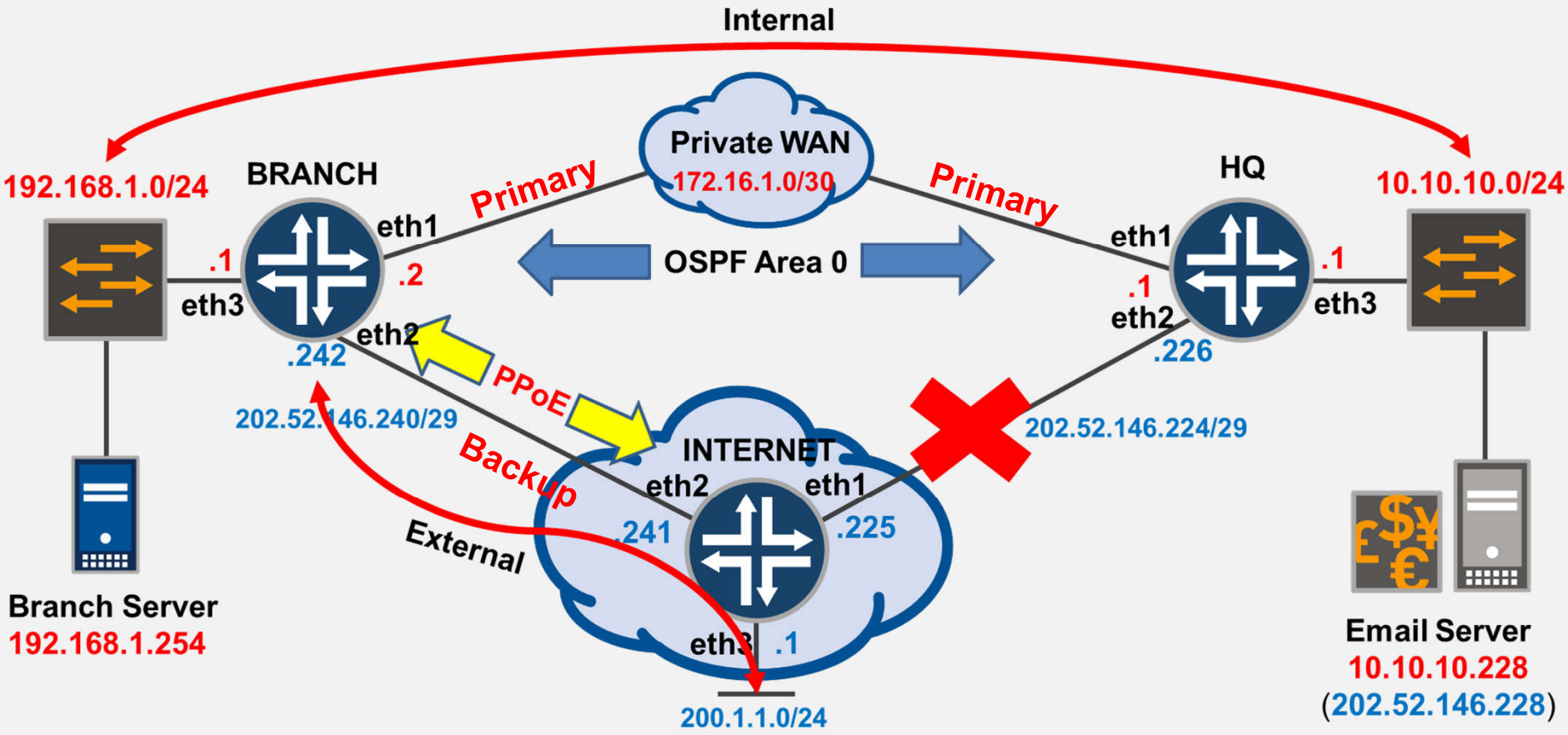


Flow Trafik Test 3

- Kondisi ***ether1*** pada **HQ Router** down

```
[admin@BRANCH] > 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                          202.52.146.241           111
 1 ADC  172.16.1.0/24      172.16.1.2      ether1                     0
 2 ADC  192.168.1.0/24     192.168.1.1     ether3                     0
                                           Branch-Server
 3 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                 0
[admin@BRANCH] > /tool traceroute 202.52.146.228 src-
address=192.168.1.254
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 202.52.146.241                    0%    2   1.2ms     1.5     1.2     1.8     0.3
 2 202.52.146.228                    0%    2   2.3ms     2.4     2.3     2.5     0.1

[admin@BRANCH] > /tool traceroute 200.1.1.254 src-
address=192.168.1.254
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 200.1.1.254                       0%    2   1.1ms     1.6     1.1       2     0.5
```

Flow Trafik Test 4



Flow Trafik Test 4

- Kondisi ***ether1*** pada **Internet Router** down

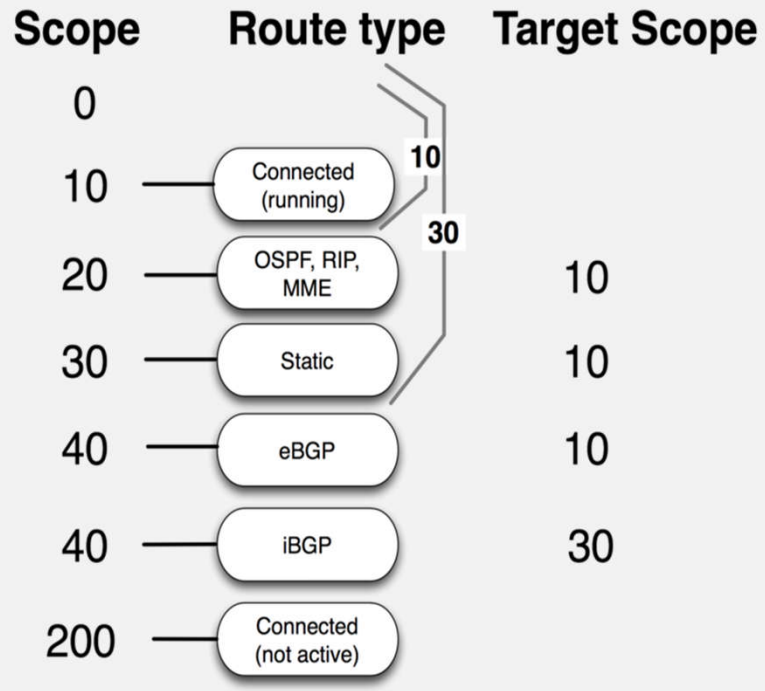
```
[admin@BRANCH] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static,
r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  0.0.0.0/0                          172.16.1.1              110
 1   S  0.0.0.0/0                          202.52.146.241          111
 2 ADo  10.10.10.0/24                      172.16.1.1              110
 3 ADC  172.16.1.0/24      172.16.1.2      ether1                    0
 4 ADC  192.168.1.0/24     192.168.1.1     ether3                    0
                                           Branch-Server
 5 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                0

[admin@BRANCH] > ping 200.1.1.254 src-address=192.168.1.254 count=3
HOST                                     SIZE TTL TIME  STATUS
200.1.1.254                                             timeout
200.1.1.254                                             timeout
200.1.1.254                                             timeout
    sent=3 received=0 packet-loss=100%
```

Rekayasa Trafik (Advanced)

- **Recursive Next-hop**
  - Memungkinkan untuk menetapkan sebuah ***gateway*** ke tujuan meskipun ***gateway*** tersebut tidak terhubung langsung (***undirectly reachable***)
    - **undirect next-hop** tersebut dapat dicapai dari rute yang telah ada (**existing route)**
  - Berfungsi untuk menyelesaikan masalah dimana antara router dan **gateway** tidak terhubung secara konstan (misalnya: iBGP)
  - Setiap rute harus berada di dalam **scope** dari rute yang lain supaya **recursive next-hop** bisa bekerja

Rekayasa Trafik (Advanced)

- **scope** dan **target-scope**
  - Sebuah route dikatakan **active**, jika rute tersebut dapat menentukan nexthop dan dapat dicapai (resolvable)
    - Route yang inactive tidak akan digunakan untuk memforward packet
  - **Scope** dari rute akan berisi semua rute yang nilai **scope** nya *lebih kecil* atau *sama dengan* **target-scope** nya



Source: http://wiki.mikrotik.com/wiki/Manual:Using_scope_and_target-scope_attributes

Solusi Flow Trafik Test 4

- Konfigurasi pada **Branch Router**
  - Ganti ***distance*** dari ***default route*** menuju internet dengan nilai 109
  - Tambahkan ***static route*** menuju **monitor ip address** (202.52.146.225) via gateway 172.16.1.1
  - Tambahkan ***default route*** via ***gateway*** 202.52.146.225 dengan target scope *lebih besar dari* atau *sama dengan* **scope** dari **static route** menuju **monitor ip address**
    - Monitoring gateway tersebut dengan menggunakan ping

Solusi Flow Trafik Test 4

- Konfigurasi ***static route*** pada **Branch Router**

```
[admin@BRANCH] > ip route add dst-address=0.0.0.0/0
gateway=202.52.146.241 distance=109

[admin@BRANCH] > ip route add dst-
address=202.52.146.225 gateway=172.16.1.1

[admin@BRANCH] > ip route add dst-address=0.0.0.0/0
gateway=202.52.146.225 check-gateway=ping target-
scope=30
```

Flow Trafik Test 4

- Verifikasi ***table routing*** pada **Branch Router**

```
[admin@BRANCH] > 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                          202.52.146.225             1
 1   S  0.0.0.0/0                          202.52.146.241           109
 2  Do  0.0.0.0/0                          172.16.1.1               110
 3 ADo  10.10.10.0/24                      172.16.1.1               110
 4 ADC  172.16.1.0/24       172.16.1.2     ether1                     0
 5 ADC  192.168.1.0/24      192.168.1.1    ether3                     0
                                           Branch-Server
 6 A S  202.52.146.225/32                  172.16.1.1                 1
 7 ADC  202.52.146.241/32   202.52.146.242 pppoe-out1                 0
```

Flow Trafik Test 4

- Verifikasi ***table routing detail*** pada **Branch Router**

```
[admin@BRANCH] > ip route print detail
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
 0 A S  dst-address=0.0.0.0/0 gateway=202.52.146.225
        gateway-status=202.52.146.225 recursive via 172.16.1.1 ether1
check-gateway=ping distance=1
        scope=30 target-scope=30
 1   S  dst-address=0.0.0.0/0 gateway=202.52.146.241 gateway-
status=202.52.146.241 reachable via  pppoe-out1
        distance=109 scope=30 target-scope=10
 2  Do  dst-address=0.0.0.0/0 gateway=172.16.1.1 gateway-
status=172.16.1.1 reachable via  ether1 distance=11>
        scope=20 target-scope=10 ospf-metric=10 ospf-type=external-
type-2
  6 A S  dst-address=202.52.146.225/32 gateway=172.16.1.1 gateway-
status=172.16.1.1 reachable via  ether1
        distance=1 scope=30 target-scope=10
```

Flow Trafik Re-Test 4

- ***Disable*** interface ***ether1*** pada **Internet Router** Kemudian periksa ***routing table*** pada **Branch Router**

```
[admin@BRANCH] > 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   S  0.0.0.0/0                          202.52.146.225             1
 1 A S  0.0.0.0/0                          202.52.146.241           109
 2  Do  0.0.0.0/0                          172.16.1.1                 110
 3 ADo  10.10.10.0/24                      172.16.1.1                 110
 4 ADC  172.16.1.0/24      172.16.1.2      ether1                       0
 5 ADC  192.168.1.0/24     192.168.1.1     ether3                       0
                                           Branch-Server
 6 A S  202.52.146.225/32                  172.16.1.1                   1
 7 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                   0
```

Flow Trafik Re-Test 4

- Verifikasi Koneksi dari LAN **Branch Router**

```
[admin@BRANCH] /tool> traceroute 10.10.10.228 src-
address=192.168.1.254
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 10.10.10.228                      0%    4   1.2ms     2.2     1.2     4.8     1.5

[admin@BRANCH] /tool> traceroute 200.1.1.254 src-address=192.168.1.254
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 200.1.1.254                       0%   10   1.3ms     1.7     1.3     2.9     0.5
```

Tentang Saya

RouterOS Broadband Connectivity

Skenario Branch Network

Konfigurasi Routing & NAT pada Branch Network

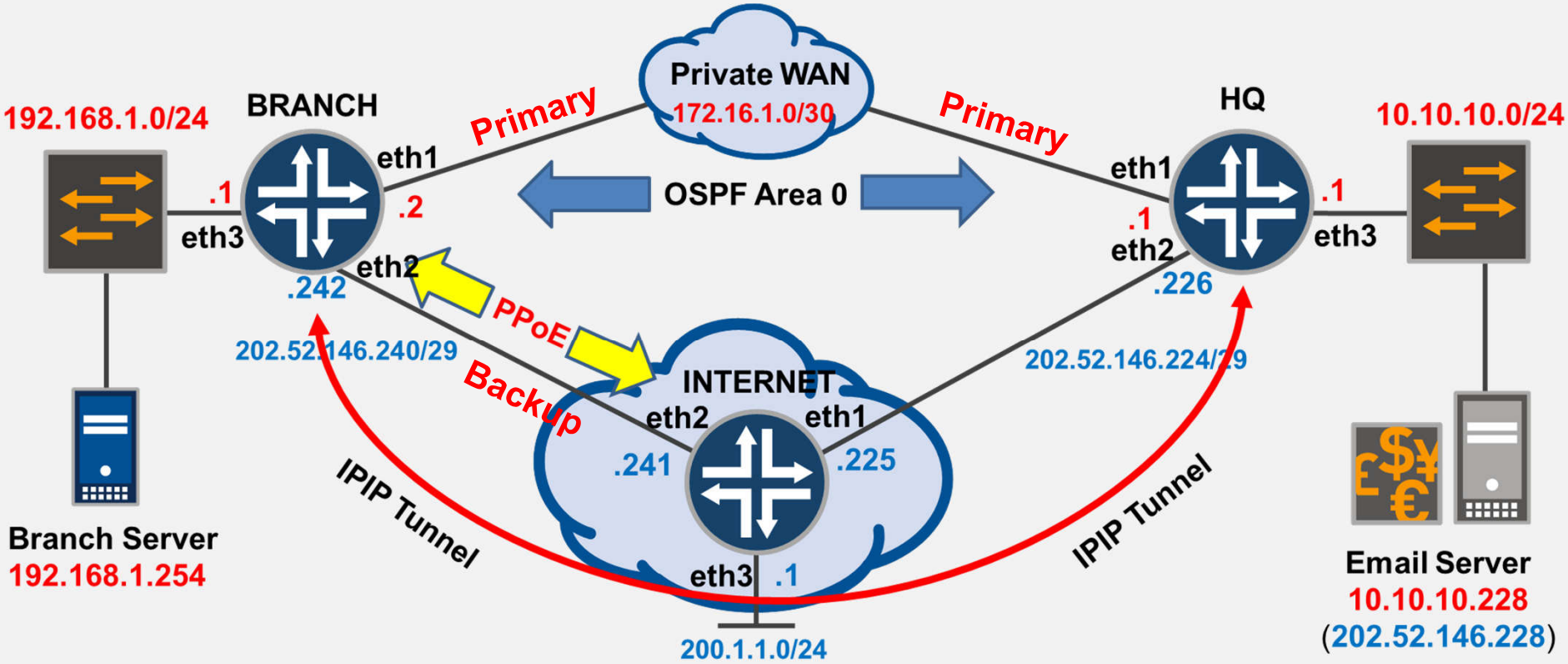
Konfigurasi VPN pada Branch Network

VPN Overview

- Menciptakan ***private network*** melalui sebuah public network
- Menciptakan ***point-to-point connection*** menggunakan ***tunneling protocol*** yang ter-enkripsi maupun tidak
- MikroTik mendukung berbagai jenis ***tunneling protocol*** dalam membangun VPN.
  - Namun untuk sesi ini kita akan membahas dan menggunakan **ipip tunnel**
- IPIP tunneling pada MikroTik mengacu pada standarisasi **RFC 2003**

Source: http://wiki.mikrotik.com/wiki/Manual:Interface/IPIP

Topologi Branch Network (Step 3)



9 konfigurasi IPIP Tunnel dan OSPF

Implementasi IPIP Tunnel

- ***IP Address Planning***

Properties	Router HQ	Router Branch
Local Address	202.52.146.226	202.52.146.242
Remote Address	202.52.146.242	202.52.146.226
IPIP Interface	1.1.1.1/24	1.1.1.2/24

Implementasi IPIP Tunnel

- Konfigurasi pada **HQ Router**

```
[admin@HQ] > interface ipip add
local-address: 202.52.146.226
remote-address: 202.52.146.242

[admin@HQ] > interface ipip
[admin@HQ] /interface ipip> enable 0
[admin@HQ] /interface ipip> /ip address add
address=1.1.1.1/24 interface=ipip1

[admin@HQ] /interface ipip> /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    10.10.10.1/24      10.10.10.0      ether3
 1    172.16.1.1/24      172.16.1.0      ether1
 2    202.52.146.226/29  202.52.146.224  ether2
 3    10.10.10.228/24    10.10.10.0      Email-Server
 4    202.52.146.228/32  202.52.146.228  ether2
 5    1.1.1.1/24         1.1.1.0         ipip1
```

Implementasi IPIP Tunnel

- Konfigurasi pada **Branch Router**

```
[admin@BRANCH] > interface ipip add
local-address: 202.52.146.242
remote-address: 202.52.146.226

[admin@BRANCH] > interface ipip
[admin@BRANCH] /interface ipip> enable 0
[admin@BRANCH] /interface ipip> /ip address add
address=1.1.1.2/24 interface=ipip1

[admin@BRANCH] /interface ipip> /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    192.168.1.1/24     192.168.1.0     ether3
 1    172.16.1.2/24      172.16.1.0      ether1
 2    192.168.1.254/24   192.168.1.0     Branch-Server
 3 D  202.52.146.242/32  202.52.146.241  pppoe-out1
 4    1.1.1.2/24         1.1.1.0         ipip1
```

Optimize Protocol OSPF

- Masukkan interface **IPIP Tunnel** kedalam ***OSPF process*** pada **Branch Router** dan **HQ Router**

```
[admin@BRANCH] > /routing ospf network add
network=1.1.1.0/24 area=backbone
```

```
[admin@BRANCH] > /routing ospf network add
network=1.1.1.0/24 area=backbone
```

Verifikasi Protocol OSPF

- Verifikasi ***OSPF process*** pada HQ Router

```
[admin@HQ] > routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
 #    INTERFACE                                COST PRIORITY NETWORK-TYPE
AUTHENTICATION AUTHENTICATION-KEY
 0 D  ipip1                                     10        1 point-to-point none
 1 D  Email-Server                              10        1 broadcast      none
 2 D  ether1                                    10        1 broadcast      none
 3 D  ether3                                    10        1 broadcast      none

[admin@HQ] > routing ospf neighbor print
 0 instance=default router-id=172.16.1.2 address=1.1.1.2
interface=ipip1 priority=1 dr-address=0.0.0.0
   backup-dr-address=0.0.0.0 state="Full" state-changes=5 ls-
retransmits=0 ls-requests=0 db-summaries=0
   adjacency=1m10s
```

Verifikasi Protocol OSPF

- Verifikasi ***Routing Table*** pada **HQ Router**

```
[admin@BRANCH] > 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                          202.52.146.225             1
 1   S  0.0.0.0/0                          202.52.146.241           109
 2 ADC  1.1.1.0/24         1.1.1.2         ipip1                      0
 3 ADo  10.10.10.0/24                      172.16.1.1               110
                                           1.1.1.1
 4 ADC  172.16.1.0/24      172.16.1.2      ether1                     0
 5 ADC  192.168.1.0/24     192.168.1.1     ether3                     0
                                           Branch-Server
 6 A S  202.52.146.225/32                  172.16.1.1                 1
 7 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                 0
```

Verifikasi Protocol OSPF

- Verifikasi ***OSPF process*** pada **Branch Router**

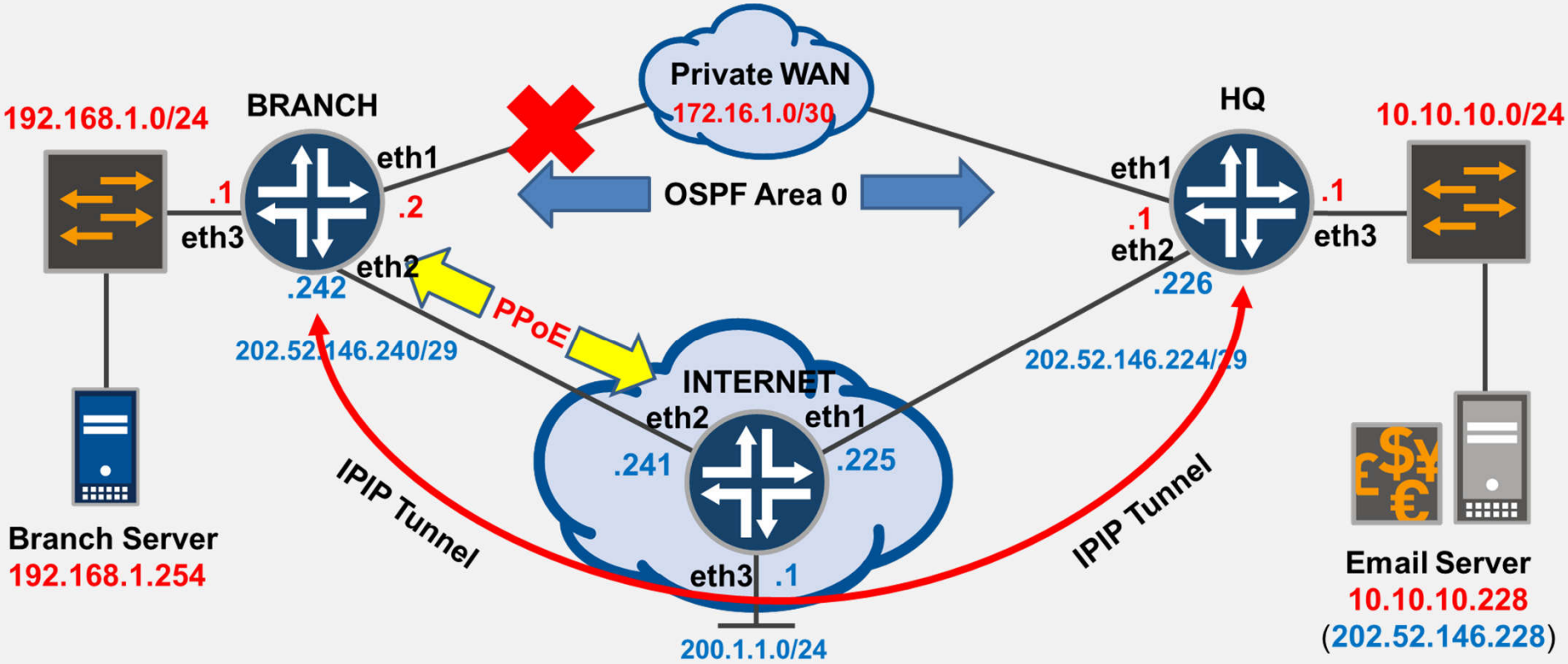
```
[admin@BRANCH] > /routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
 #    INTERFACE                                COST PRIORITY NETWORK-TYPE
AUTHENTICATION AUTHENTICATION-KEY
 0 D  ether1                                     10        1 broadcast      none
 1 D  ether3                                     10        1 broadcast      none
 2 D  Branch-Server                              10        1 broadcast      none
 3 D  ipip1                                      10        1 point-to-point none

[admin@BRANCH] > /routing ospf neighbor print
 0 instance=default router-id=1.1.1.1 address=1.1.1.1 interface=ipip1
priority=1 dr-address=0.0.0.0
   backup-dr-address=0.0.0.0 state="Full" state-changes=4 ls-
retransmits=0 ls-requests=0 db-summaries=0
   adjacency=3m56s
```

Verifikasi Protocol OSPF

- Verifikasi ***Routing Table*** pada **Branch Router**

```
[admin@HQ] > 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                          202.52.146.225              1
 1 ADC  1.1.1.0/24         1.1.1.1         ipip1                       0
 2 ADC  10.10.10.0/24      10.10.10.228    Email-Server                0
                                           ether3
 3 ADC  172.16.1.0/24      172.16.1.1      ether1                      0
 4 ADo  192.168.1.0/24                     1.1.1.2                   110
                                           172.16.1.2
 5 ADC  202.52.146.224/29  202.52.146.226  ether2                      0
 6 ADC  202.52.146.228/32  202.52.146.228  ether2                      0
```

Flow Trafik Test 5



Flow Trafik Test 5

- ***Disable*** interface ***ether1*** pada **Branch Router**
- Periksa ***table routing*** pada **Branch Router**

```
[admin@BRANCH] > 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   S  0.0.0.0/0                          202.52.146.225            1
 1 A S  0.0.0.0/0                          202.52.146.241          109
 2 ADC  1.1.1.0/24         1.1.1.2         ipip1                     0
 3 ADo  10.10.10.0/24                      1.1.1.1                 110
 4 ADC  192.168.1.0/24     192.168.1.1     ether3                    0
                                           Branch-Server
 5   S  202.52.146.225/32                  172.16.1.1                1
 6 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                0
```

Flow Trafik Test 5

- ***Test*** koneksi dari LAN **Branch Router**

```
[admin@BRANCH] > ping 200.1.1.254 src-address=192.168.1.254 count=3
HOST                                     SIZE TTL TIME  STATUS
200.1.1.254                                56  64 1ms
200.1.1.254                                56  64 2ms
200.1.1.254                                56  64 5ms
    sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-
rtt=5ms

[admin@BRANCH] > ping 10.10.10.228 src-address=192.168.1.254 count=3
HOST                                     SIZE TTL TIME  STATUS
10.10.10.228                               56  64 2ms
10.10.10.228                               56  64 5ms
10.10.10.228                               56  64 6ms
    sent=3 received=3 packet-loss=0% min-rtt=2ms avg-rtt=4ms max-
rtt=6ms
```

Flow Trafik Test 5

- ***Test Flow*** trafik dari LAN **Branch Router**

```
[admin@BRANCH] > /tool traceroute  200.1.1.254 src-
address=192.168.1.254 count=3
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 200.1.1.254                       0%    2     3ms     2.3     1.6       3     0.7

[admin@BRANCH] > /tool traceroute  10.10.10.228 src-
address=192.168.1.254 count=3
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 10.10.10.228                      0%    2   5.7ms     4.1     2.5     5.7     1.6
```

Flow Trafik Test 5

- ***Enable*** kembali interface ***ether1*** pada **Branch Router** dan periksa kembali ***table routing*** pada router tersebut.

```
[admin@BRANCH] > 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                          202.52.146.225             1
 1   S  0.0.0.0/0                          202.52.146.241           109
 2 ADC  1.1.1.0/24         1.1.1.2         ipip1                      0
 3 ADo  10.10.10.0/24                      172.16.1.1               110
                                           1.1.1.1
 4 ADC  172.16.1.0/24      172.16.1.2      ether1                     0
 5 ADC  192.168.1.0/24     192.168.1.254   Branch-Server              0
                                           ether3
 6 A S  202.52.146.225/32                  172.16.1.1                 1
 7 ADC  202.52.146.241/32  202.52.146.242  pppoe-out1                 0
```

“Pertanyaan?”

hendevane training partner htp
global knowledge in your hand

THANKS

www.htp.co.id