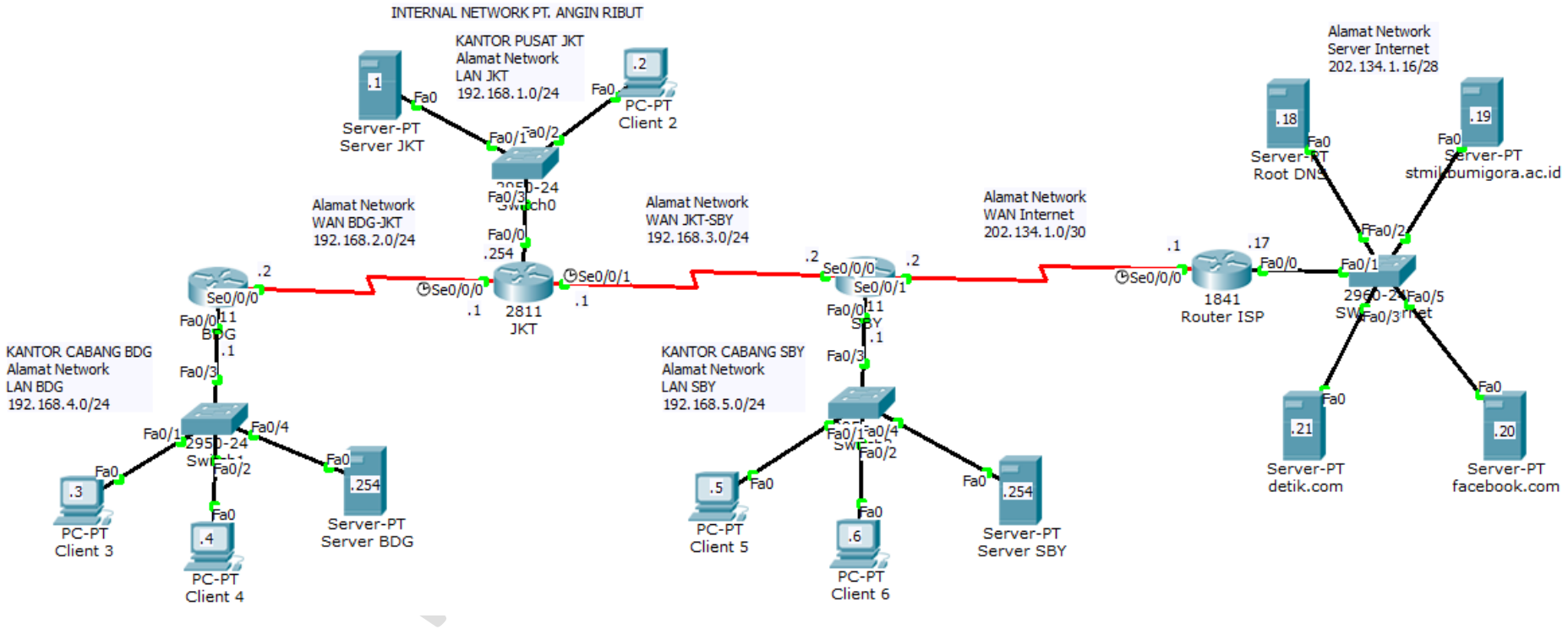
STUDI KASUS KONFIGURASI RIP DAN CISCO ACCESS CONTROL LIST (ACL)

Oleh I Putu Hariyadi (admin@iputuhariyadi.net)

SOAL:

Berdasarkan topologi jaringan seperti terlihat pada gambar dibawah ini, buat konfigurasi pada perangkat-perangkat terkait dengan ketentuan-ketentuan sebagai berikut:



1. Konfigurasi Routing Protokol RIP pada Router BDG, JKT, dan SBY agar antar jaringan internal kantor pusat dan cabang PT. Angin Ribut dapat saling berkomunikasi. Verifikasi komunikasi host antar jaringan menggunakan utilitas ping.
2. Konfigurasi NAT Overload/PAT pada Router SBY agar mengijinkan akses Internet hanya dari host-host pada LAN Kantor Cabang BDG. Verifikasi melalui browser dengan melakukan akses ke situs http://stmikbumigora.ac.id, http://facebook.com, http://detik.com. Akses Internet dari Client3, Client4, dan Server BDG di LAN Kantor Cabang BDG diijinkan, sebaliknya yang lainnya ditolak.
3. Konfigurasi ACL agar mengijinkan akses telnet pada masing-masing Router JKT, BDG, dan SBY dengan ketentuan sebagai berikut:
   a) Router JKT

      Hanya mengijinkan telnet dari host Client2.

   b) Router BDG

      Hanya mengijinkan telnet dari host Client2 dan Server BDG.

   c) Router SBY

      Hanya mengijinkan telnet dari host Client2 dan Server SBY.

   Verifikasi konfigurasi yang telah dilakukan dengan melakukan telnet dari masing-masing client yang diijinkan dan ditolak.
4. Konfigurasi ACL agar mengijinkan hanya host-host di LAN Kantor Cabang BDG dan LAN Kantor Cabang SBY yang dapat mengakses seluruh layanan HTTP, HTTPS, dan FTP pada Server BDG, sebaliknya menolak akses dari seluruh host di LAN Kantor Pusat JKT. Verifikasi konfigurasi yang telah dilakukan dengan melakukan akses HTTP, dan HTTPS melalui browser, serta FTP melalui command prompt baik dari host-host yang diijinkan maupun ditolak.
5. Konfigurasi ACL agar mengijinkan hanya host-host di LAN Kantor Cabang SBY dan LAN Kantor Cabang BDG yang dapat mengakses seluruh layanan HTTP, HTTPS, dan FTP pada Server SBY, sebaliknya menolak akses dari seluruh host di LAN Kantor Pusat JKT. Verifikasi konfigurasi yang telah dilakukan dengan melakukan akses HTTP, dan HTTPS melalui browser, serta FTP melalui command prompt baik dari host-host yang diijinkan maupun ditolak.

File template topologi Cisco Packet Tracer dapat diunduh pada alamat berikut: http://iputuhariyadi.net/wp-content/uploads/2016/07/Template-Studi-Kasus-Konfigurasi-RIP-dan-Cisco-ACL.zip. Sandi atau password login yang digunakan pada cisco router di file template tersebut adalah sebagai berikut:

a. Console: cisco
b. Privilege: sanfran
c. Telnet: sanjose

SOLUSI SOAL NO. 1:

A. Konfigurasi RIP di Router BDG

Berpindah ke mode privilege

```
BDG> enable
```

Berpindah ke mode global configuration

```
BDG# conf t
```

Mengaktifkan routing protocol RIP

```
BDG(config)# router rip
```

Mengatur alamat jaringan yang dimasukkan pada routing update yaitu yang terhubung langsung dengan router BDG

```
BDG(config-router)# network 192.168.4.0
BDG(config-router)# network 192.168.2.0
```

Berpindah ke mode privilege

```
BDG(config-router)# end
```

Menampilkan informasi routing protocol yang aktif

```
BDG#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 0 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       1     2 1
  Serial0/0/0           1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
         192.168.2.0
         192.168.4.0
Passive Interface(s):
Routing Information Sources:
         Gateway         Distance      Last Update
Distance: (default is 120)
```

B. Konfigurasi RIP di Router JKT

Berpindah ke mode privilege

```
JKT> enable
```

Berpindah ke mode global configuration

```
JKT# conf t
```

Mengaktifkan routing protocol RIP

```
JKT(config)# router rip
```

Mengatur alamat jaringan yang dimasukkan pada routing update yaitu yang terhubung langsung dengan router JKT

```
JKT(config-router)# network 192.168.1.0

JKT(config-router)# network 192.168.2.0

JKT(config-router)# network 192.168.3.0
```

Berpindah ke mode privilege

```
JKT(config-router)# end
```

Menampilkan informasi routing protocol yang aktif

```
JKT#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       1     2 1
  Serial0/0/0           1     2 1
  Serial0/0/1           1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
         192.168.1.0
         192.168.2.0
         192.168.3.0
Passive Interface(s):
Routing Information Sources:
         Gateway         Distance      Last Update
         192.168.2.2           120      00:00:21
Distance: (default is 120)
```

Menampilkan informasi routing tabel

```
JKT#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, Serial0/0/1
R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:12, Serial0/0/0
```

Perhatikan kode R pada output diatas yang menunjukkan informasi tentang jaringan tersebut diperoleh dari hasil routing update RIP.

C. Konfigurasi RIP di Router SBY

Berpindah ke mode privilege

```
SBY> enable
```

Berpindah ke mode global configuration

```
SBY# conf t
```

Mengaktifkan routing protocol RIP

```
SBY(config)# router rip
```

Mengatur alamat jaringan yang dimasukkan pada routing update yaitu yang terhubung langsung dengan router SBY

```
SBY(config-router)# network 192.168.3.0

SBY(config-router)# network 192.168.5.0
```

Berpindah ke mode privilege

```
SBY(config-router)# end
```

Menampilkan informasi routing protocol yang aktif

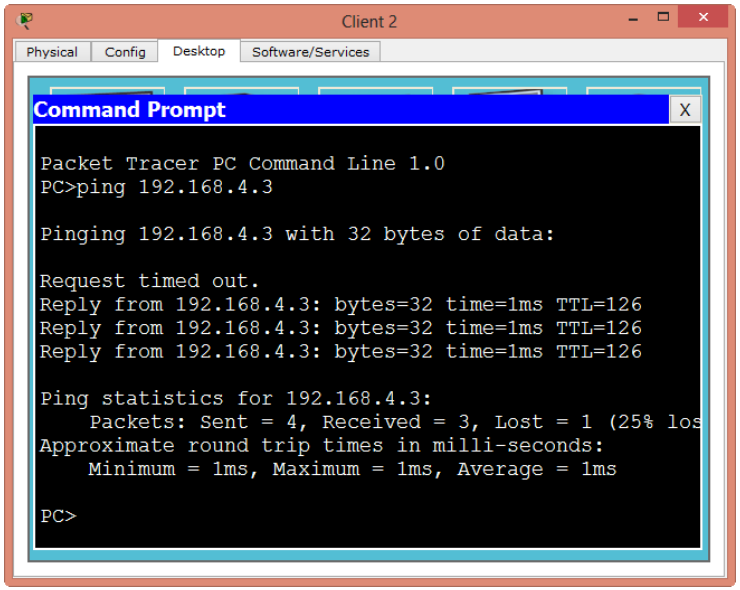
```
SBY#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 20 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           1     2 1
  FastEthernet0/0       1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
         192.168.3.0
         192.168.5.0
Passive Interface(s):
Routing Information Sources:
         Gateway         Distance      Last Update
         192.168.3.1           120      00:00:05
Distance: (default is 120)
```

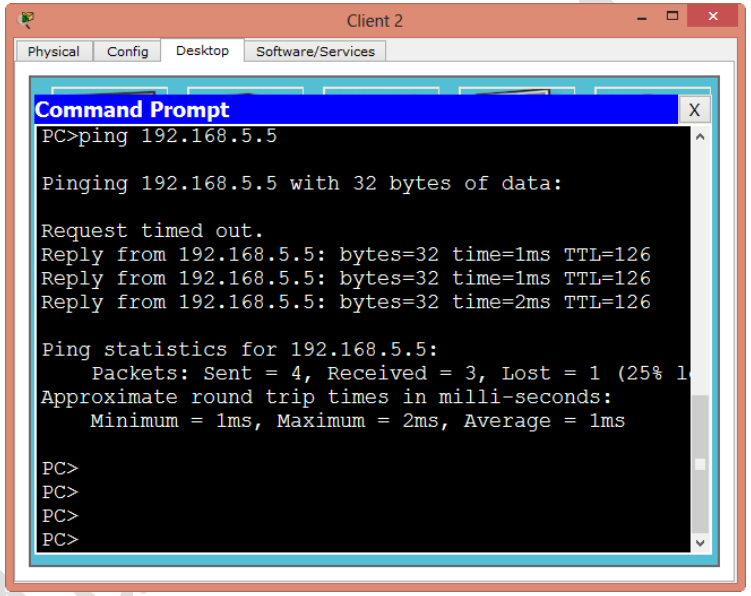
Menampilkan informasi routing table

```
SBY#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:10, Serial0/0/0
R    192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:10, Serial0/0/0
C    192.168.3.0/24 is directly connected, Serial0/0/0
R    192.168.4.0/24 [120/2] via 192.168.3.1, 00:00:10, Serial0/0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
     202.134.1.0/30 is subnetted, 1 subnets
C       202.134.1.0 is directly connected, Serial0/0/1
```

Perhatikan kode R pada output diatas yang menunjukkan informasi tentang jaringan tersebut diperoleh dari hasil routing update RIP.

Verifikasi koneksi antar host dengan melakukan perintah ping dari Client2 ke Client3, dan dari Client2 ke Client5, seperti terlihat pada gambar berikut:





Pastikan hasil verifikasi dengan ping adalah sukses.

Soal No. 2

A. Mengatur default route

Berpindah ke mode global configuration

```
SBY# conf t
```

Mengatur default route

```
SBY(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

Berpindah ke mode privilege

```
SBY(config)# end
```

Menampilkan informasi routing table

```
SBY#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

R    192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:16, Serial0/0/0
R    192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:16, Serial0/0/0
C    192.168.3.0/24 is directly connected, Serial0/0/0
R    192.168.4.0/24 [120/2] via 192.168.3.1, 00:00:16, Serial0/0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
     202.134.1.0/30 is subnetted, 1 subnets
C       202.134.1.0 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

Memverifikasi koneksi dari router SBY ke salah satu server yang terdapat di Internet sebagai contoh Server Root DNS menggunakan perintah ping.

```
SBY#ping 202.134.1.18

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.134.1.18, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Pastikan hasil eksekusi dengan ping adalah sukses.

B. Menyebarkan default route melalui RIP di Router SBY

```
SBY(config)# router rip

SBY(config-router)# default-information originate

SBY(config-router)# end
```

Memverifikasi hasil pengaturan penyebaran default route di router SBY pada tabel routing di router JKT

```
JKT#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.3.2 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, Serial0/0/1
R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:15, Serial0/0/0
R    192.168.5.0/24 [120/1] via 192.168.3.2, 00:00:06, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 192.168.3.2, 00:00:06, Serial0/0/1
```

Memverifikasi hasil pengaturan penyebaran default route di router SBY pada tabel routing di router BDG

```
BDG#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:17, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.1, 00:00:17, Serial0/0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/0
R    192.168.5.0/24 [120/2] via 192.168.2.1, 00:00:17, Serial0/0/0
R*   0.0.0.0/0 [120/2] via 192.168.2.1, 00:00:17, Serial0/0/0
```

C. Mengaktifkan NAT pada interface s0/0/0 dan s0/0/1

Berpindah ke mode global configuration

```
SBY# conf t
```

Berpindah ke interface configuration untuk s0/0/0

```
SBY(config)# int s0/0/0
```

Mengatur NAT inside

```
SBY(config-if)# ip nat inside
```

Berpindah ke interface configuration untuk s0/0/1

```
SBY(config-if)# int s0/0/1
```

Mengatur NAT outside

```
SBY(config-if)# ip nat outside
```

Berpindah ke mode ke satu mode sebelumnya

```
SBY(config-if)# exit
```

D. Membuat ACL agar mengijinkan LAN BDG dapat mengakses Internet

```
SBY(config)# access-list 1 permit 192.168.4.0 0.0.0.255
```

E. Membuat NAT Overload

```
SBY(config)# ip nat inside source list 1 interface s0/0/1 overload
```

Berpindah ke mode privilege

```
SBY(config)# end
```

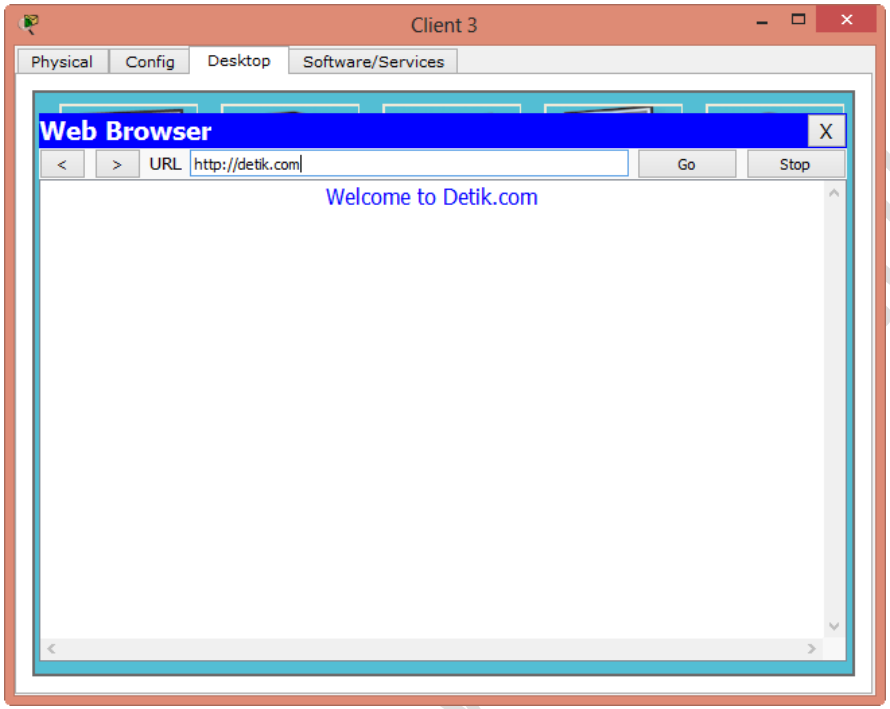
F. Memverifikasi ACL

```
SBY#show ip access-list
Standard IP access list 1
    permit 192.168.4.0 0.0.0.255
```

G. Memverifikasi pengaktifan NAT pada interface

```
SBY#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: Serial0/0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

H. Memverifikasi koneksi Internet dari client3 menggunakan web browser dengan mengakses salah satu situs di Internet sebagai contoh http://detik.com



Anda dapat memverifikasi koneksi Internet dari Client4 dan Server BDG serta pastikan hasilnya sukses. Sebaliknya dari client dan server yang lainnya ditolak aksesnya.

I. Memverifikasi hasil translasi NAT

```
SBY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 202.134.1.2:1025   192.168.4.3:1025   202.134.1.18:53    202.134.1.18:53
tcp 202.134.1.2:1025   192.168.4.3:1025   202.134.1.21:80    202.134.1.21:80
```

Soal No. 3

A. Konfigurasi ACL untuk mengijinkan telnet ke router JKT hanya dari host Client2

Berpindah ke mode global configuration

```
JKT# conf t
```

Membuat Standard ACL untuk mengijinkan Client2

```
JKT(config)# access-list 99 permit 192.168.1.2
```

Berpindah ke line configuration

```
JKT(config)# line vty 0 4
```

Menerapkan ACL yang telah dibuat

```
JKT(config)# access-class 99 in
```

Berpindah ke privilege mode

```
JKT(config)# end
```

Menampilkan informasi ACL yang terdapat pada router JKT

```
JKT#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.2
```

Memverifikasi hasil penerapan ACL pada line vty

```
JKT# show run

….

!
line vty 0 4
 access-class 99 in
 password sanjose
 login
!
!
!
end
```

B. Konfigurasi ACL untuk mengijinkan telnet ke router BDG hanya dari host Client2 dan Server BDG

Berpindah ke mode global configuration

```
BDG# conf t
```

Membuat Standard ACL untuk mengijinkan akses telnet dari host Client2

```
BDG(config)# access-list 99 permit 192.168.1.2
```

Membuat Standard ACL untuk mengijinkan akses telnet dari server BDG

```
BDG(config)# access-list 99 permit 192.168.4.254
```

Berpindah ke line configuration

```
BDG(config)# line vty 0 4
```

Menerapkan ACL yang telah dibuat

```
BDG(config)# access-class 99 in
```

Berpindah ke mode privilege

```
BDG(config)# end
```

Menampilkan informasi ACL yang terdapat di router BDG

```
BDG#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.2
    20 permit host 192.168.4.254
```

Memverifikasi hasil penerapan ACL pada line vty

```
BDG# show run
```

….

```
!
line aux 0
!
line vty 0 4
 access-class 99 in
 password sanjose
 login
!
!
!
end
```

C. Konfigurasi ACL untuk mengijinkan telnet ke router SBY hanya dari host Client2 dan Server SBY

Berpindah ke mode global configuration

```
SBY# conf t
```

Membuat Standard ACL untuk mengijinkan akses telnet dari host Client2

```
SBY(config)# access-list 99 permit 192.168.1.2
```

Membuat Standard ACL untuk mengijinkan akses telnet dari Server SBY

```
SBY(config)# access-list 99 permit 192.168.5.254
```

Berpindah ke line configuration

```
SBY(config)# line vty 0 4
```

Menerapkan ACL yang telah dibuat

```
SBY(config)# access-class 99 in
```

Berpindah ke mode privilege

```
SBY(config)# end
```

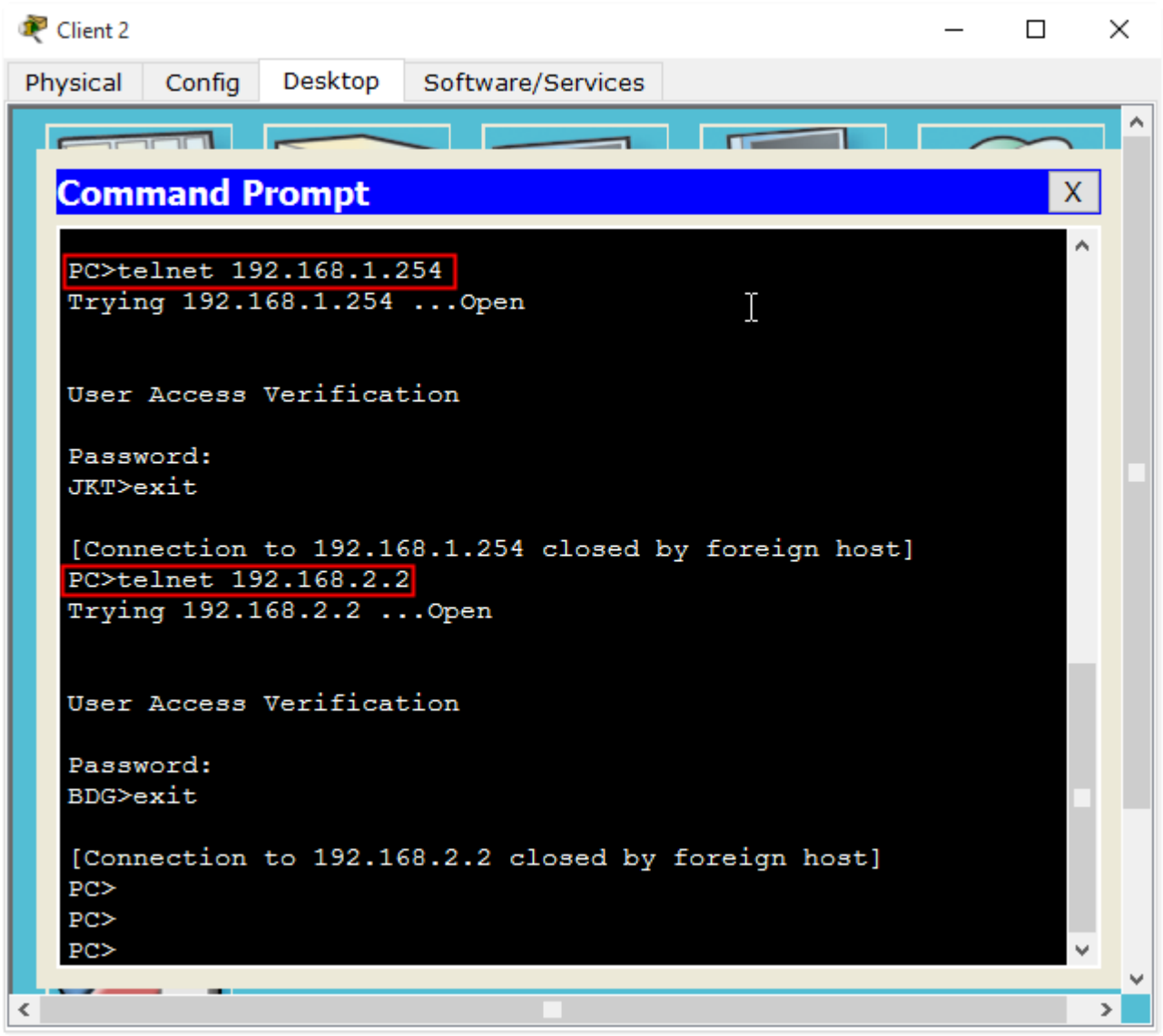
Menampilkan informasi ACL yang terdapat pada router SBY

```
SBY#show ip access-list
Standard IP access list 1
    10 permit 192.168.4.0 0.0.0.255 (4 match(es))
Standard IP access list 99
    10 permit host 192.168.1.2
    20 permit host 192.168.5.254
```

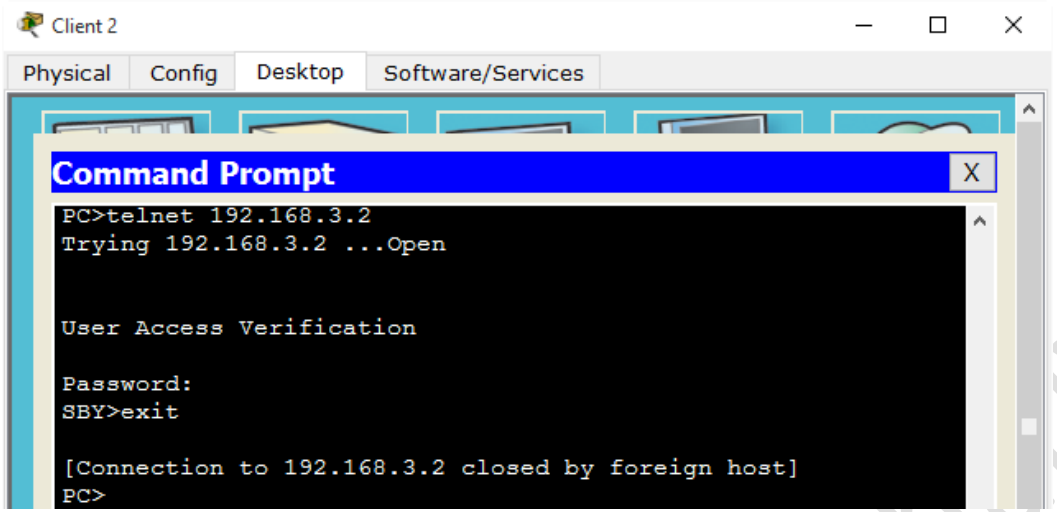
Memverifikasi hasil penerapan ACL pada line vty

```
SBY# show run

….

!
line vty 0 4
 access-class 99 in
 password sanjose
 login
!
!
!
end
```

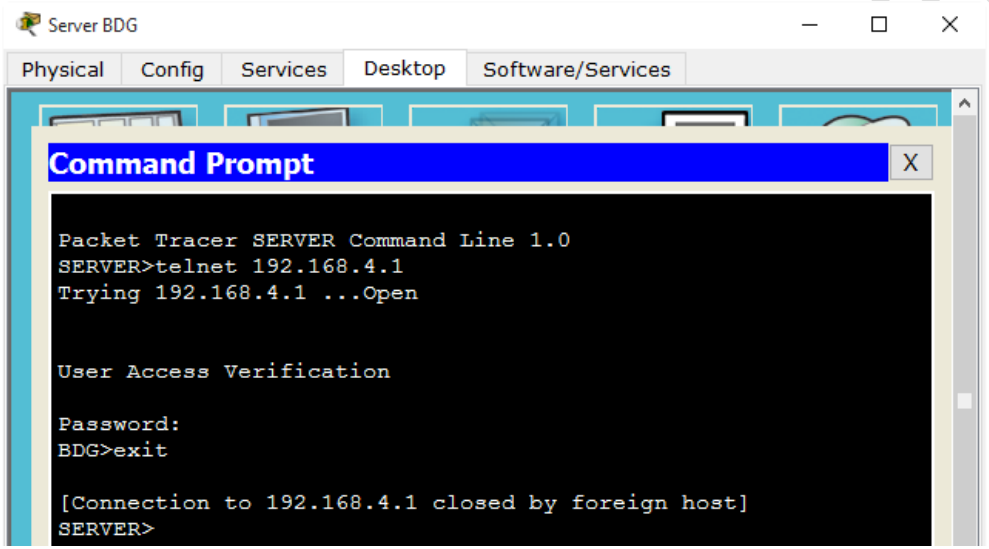
D. Verifikasi akses telnet dari client2 ke router JKT, dan router BDG


Client 2
Physical
Config
Desktop
Software/Services
Command Prompt
X
PC>telnet 192.168.1.254
Trying 192.168.1.254 ...Open
User Access Verification
Password:
JKT>exit
[Connection to 192.168.1.254 closed by foreign host]
PC>telnet 192.168.2.2
Trying 192.168.2.2 ...Open
User Access Verification
Password:
BDG>exit
[Connection to 192.168.2.2 closed by foreign host]
PC>
PC>
PC>

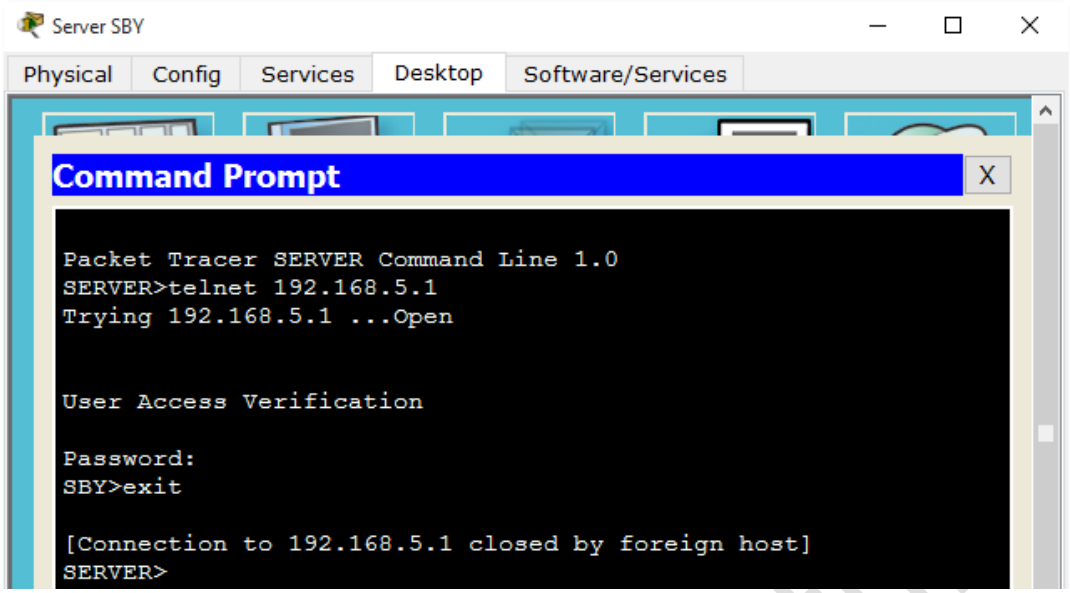
E. Verifikasi akses telnet dari client2 ke router SBY



F. Verifikasi akses telnet dari Server BDG ke router BDG



G. Verifikasi akses telnet dari Server SBY ke router SBY



Pastikan akses telnet dari host selain yang ditentukan untuk diijinkan agar tertolak aksesnya.

Soal No. 4

Konfigurasi ACL agar mengijinkan hanya host-host di LAN BDG dan SBY yg dpt mengakses layanan HTTP, HTTPS, dan FTP pada Server BDG

Berpindah ke mode global configuration

```
BDG# conf t
```

Membuat Extended ACL untuk mengijinkan akses layanan HTTP dari LAN SBY ke server BDG

```
BDG(config)# access-list 100 permit tcp 192.168.5.0 0.0.0.255 192.168.4.254 0.0.0.0 eq 80
```

Membuat Extended ACL untuk mengijinkan akses layanan HTTPS dari LAN SBY ke server BDG

```
BDG(config)# access-list 100 permit tcp 192.168.5.0 0.0.0.255 192.168.4.254 0.0.0.0 eq 443
```

Membuat Extended ACL untuk mengijinkan akses layanan FTP dari LAN SBY ke server BDG

```
BDG(config)# access-list 100 permit tcp 192.168.5.0 0.0.0.255 192.168.4.254 0.0.0.0 range 20 21
```

Membuat Extended ACL untuk mengijinkan penerimaan routing update RIP

```
BDG(config)# access-list 100 permit udp any any eq 520
```

Membuat Extended ACL untuk mengijinkan koneksi dari alamat IP sumber berapapun ke alamat IP tujuan berapapun dengan port lebih besar dari 1023 dan status koneksi telah berlangsung

```
BDG(config)#access-list 100 permit tcp any any gt 1023 established
```

Membuat Extended ACL untuk mengijinkan ping dari alamat IP sumber berapapun ke alamat IP tujuan berapapun

```
BDG(config)#access-list 100 permit icmp any any
```

Membuat Extended ACL untuk mengijinkan balasan DNS query dari Server DNS 202.134.1.18 port 53 dengan tujuan ke LAN BDG dimana pada awalnya permintaan DNS query dikirimkan dari host-host yang terdapat di LAN BDG ke Server DNS sehingga akses Internet dengan nama domain dapat dilakukan.

```
BDG(config)#access-list 100 permit udp 202.134.1.18 0.0.0.0 eq 53 192.168.4.0 0.0.0.255
```

Berpindah ke interface configuration

```
BDG(config)# int s0/0/0
```

Menerapkan ACL yang telah dibuat

```
BDG(config-if)# ip access-group 100 in
```

Berpindah ke mode privilege

```
BDG(config-if)# end
```

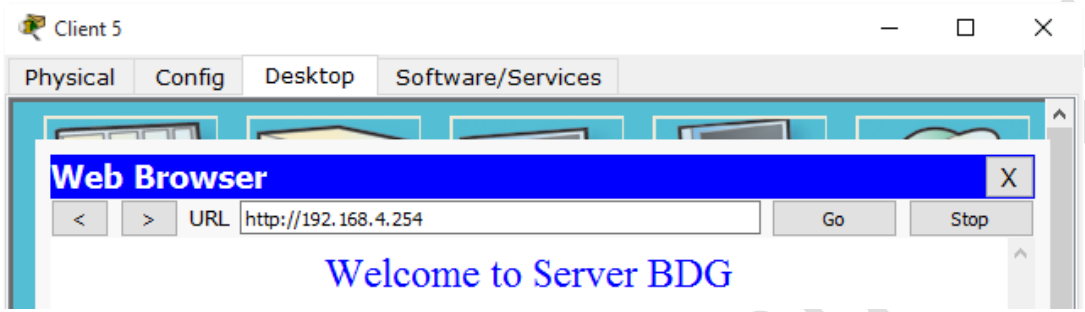
Menampilkan informasi ACL yang terdapat pada router BDG

```
BDG#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.2
    20 permit host 192.168.4.254
Extended IP access list 100
    10 permit tcp 192.168.5.0 0.0.0.255 host 192.168.4.254 eq www
    20 permit tcp 192.168.5.0 0.0.0.255 host 192.168.4.254 eq 443
    30 permit tcp 192.168.5.0 0.0.0.255 host 192.168.4.254 range 20 ftp
    40 permit udp any any eq 520
    50 permit tcp any any gt 1023 established
    60 permit icmp any any
    70 permit udp host 202.134.1.18 eq domain 192.168.4.0 0.0.0.255
```

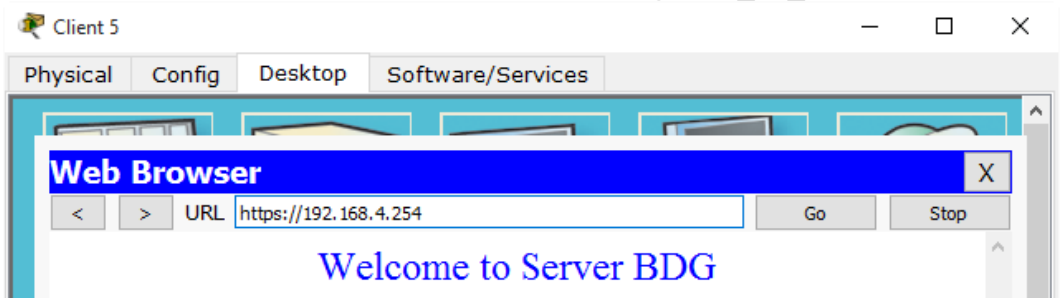
Memverifikasi penerapan ACL pada interface s0/0/0

```
BDG#show ip int s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.2.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 100
  Proxy ARP is enabled
```

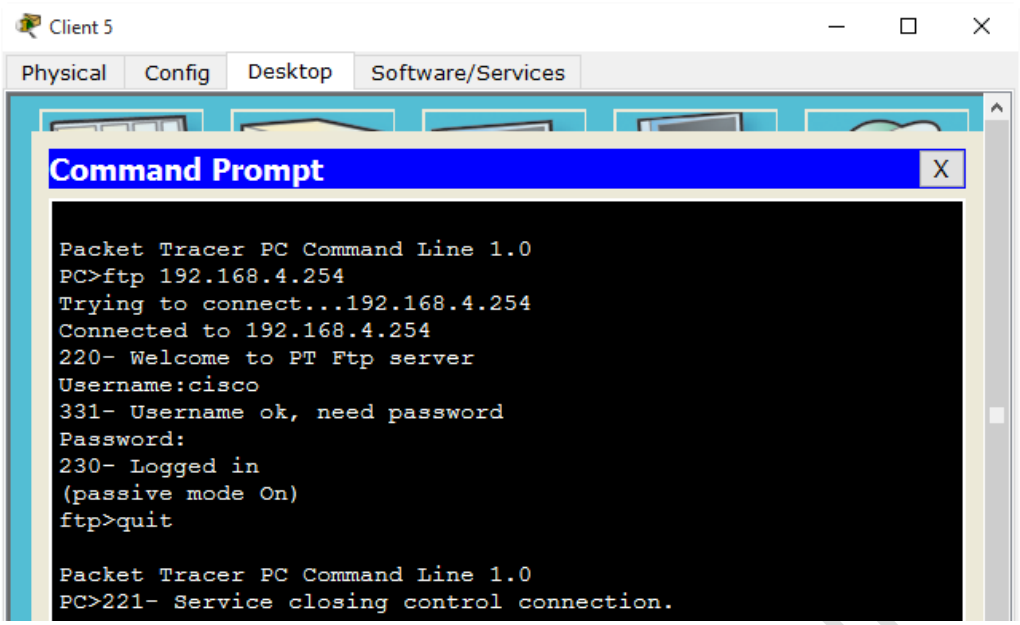
Memverifikasi akses HTTP dari client 5 yang terdapat di LAN SBY ke Server BDG



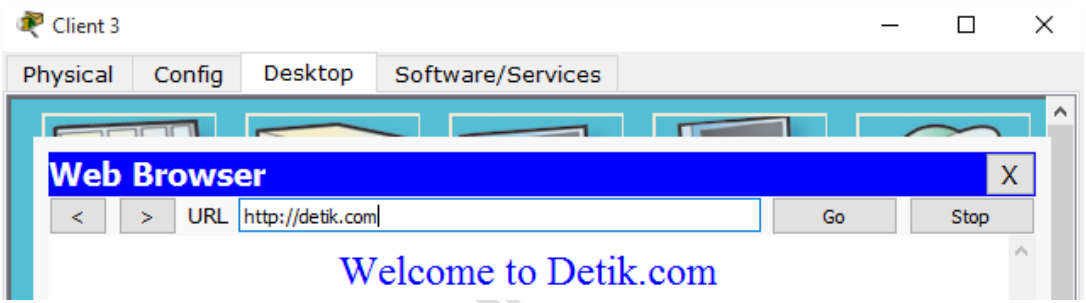
Memverifikasi akses HTTPS dari client 5 yang terdapat di LAN SBY ke Server BDG



Memverifikasi akses FTP dari client 5 yang terdapat di LAN SBY ke Server BDG. User dan Password untuk login ke Server FTP adalah "cisco".



Memverifikasi koneksi dari client 3 yang terdapat di LAN BDG ke Server Internet masih tetap dapat diakses



Soal No. 5

Konfigurasi ACL agar mengijinkan hanya host-host di LAN BDG dan SBY yg dpt mengakses layanan HTTP, HTTPS, dan FTP pada Server SBY

Berpindah ke mode global configuration

```
SBY# conf t
```

Membuat Extended ACL untuk mengijinkan akses layanan HTTP dari LAN BDG ke server SBY

```
SBY(config)# access-list 100 permit tcp 192.168.4.0 0.0.0.255 192.168.5.254 0.0.0.0 eq 80
```

Membuat Extended ACL untuk mengijinkan akses layanan HTTPS dari LAN BDG ke server SBY

```
SBY(config)# access-list 100 permit tcp 192.168.4.0 0.0.0.255 192.168.5.254 0.0.0.0 eq 443
```

Membuat Extended ACL untuk mengijinkan akses layanan FTP dari LAN BDG ke server SBY

```
SBY(config)# access-list 100 permit tcp 192.168.4.0 0.0.0.255 192.168.5.254 0.0.0.0 range 20 21
```

Membuat Extended ACL untuk mengijinkan koneksi dari alamat IP sumber berapapun ke alamat IP tujuan berapapun dengan port lebih besar dari 1023 dan status koneksi telah berlangsung

```
BDG(config)#access-list 100 permit tcp any any gt 1023 established
```

Membuat Extended ACL untuk mengijinkan ping dari alamat IP sumber berapapun ke alamat IP tujuan berapapun

```
BDG(config)#access-list 100 permit icmp any any
```

Berpindah ke interface configuration

```
SBY(config)# int f0/0
```

Menerapkan ACL yang telah dibuat

```
SBY(config-if)# ip access-group 100 out
```

Berpindah ke mode privilege

```
SBY(config-if)# end
```

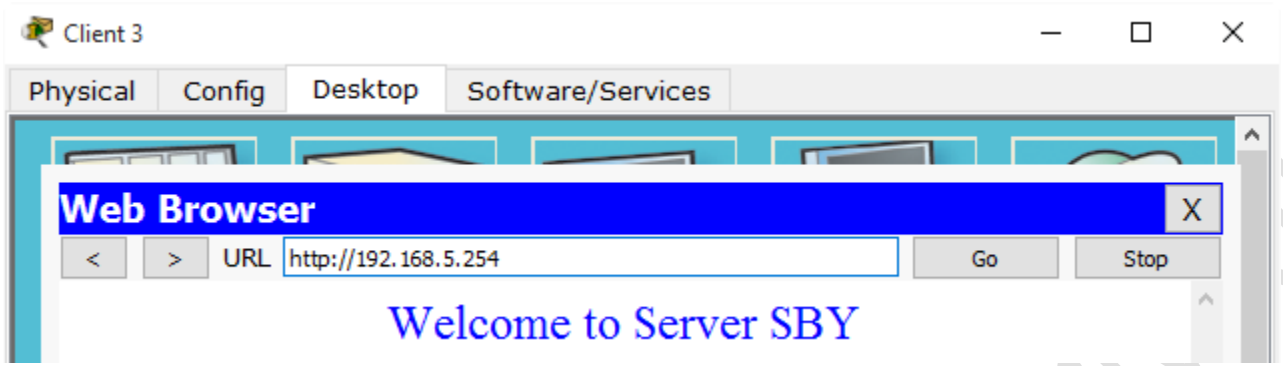
Menampilkan informasi ACL yang terdapat pada router SBY

```
SBY#show ip access-list
Standard IP access list 1
    10 permit 192.168.4.0 0.0.0.255
Standard IP access list 99
    10 permit host 192.168.1.2
    20 permit host 192.168.5.254
Extended IP access list 100
    10 permit tcp 192.168.4.0 0.0.0.255 host 192.168.5.254 eq www
    20 permit tcp 192.168.4.0 0.0.0.255 host 192.168.5.254 eq 443
    30 permit tcp 192.168.4.0 0.0.0.255 host 192.168.5.254 range 20 ftp
    40 permit tcp any any gt 1023 established
    50 permit icmp any any
```

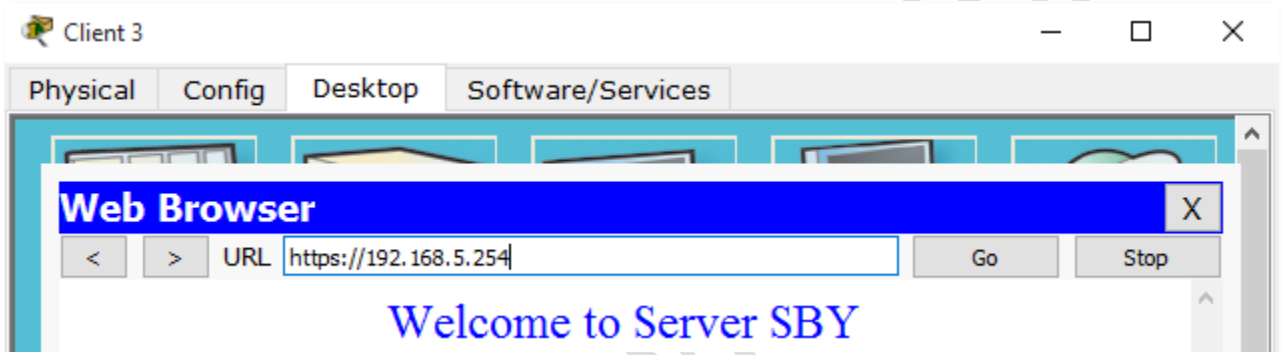
Memverifikasi penerapan ACL pada interface f0/0

```
SBY#show ip int f0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.5.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 100
  Inbound  access list is not set
```

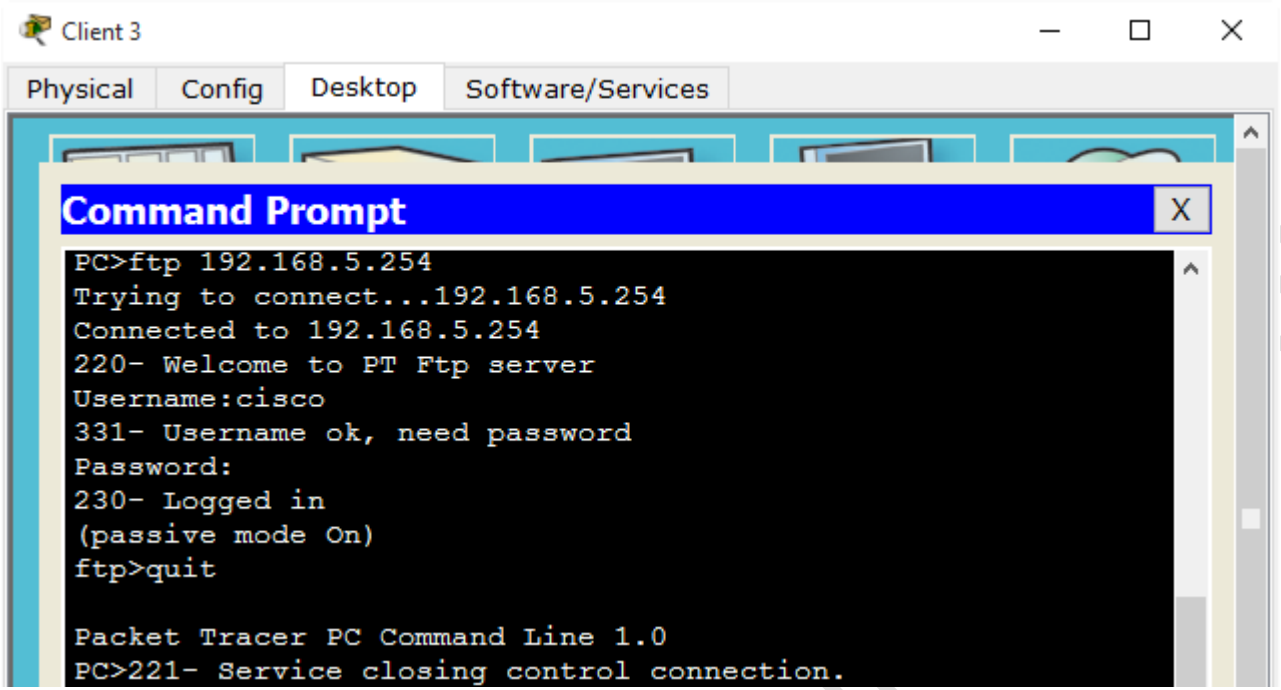
Memverifikasi akses HTTP dari client 3 yang terdapat di LAN BDG ke Server SBY



Memverifikasi akses HTTPS dari client 3 yang terdapat di LAN BDG ke Server SBY



Memverifikasi akses FTP dari client 3 yang terdapat di LAN BDG ke Server SBY. User dan Password untuk login ke Server FTP adalah "cisco".



Selamat Anda telah berhasil menyelesaikan solusi studi kasus ini. Apabila ada pertanyaan, jangan segan untuk mengirimkan melalui email ke admin@iputuhariyadi.net. Semoga bermanfaat. Terimakasih.