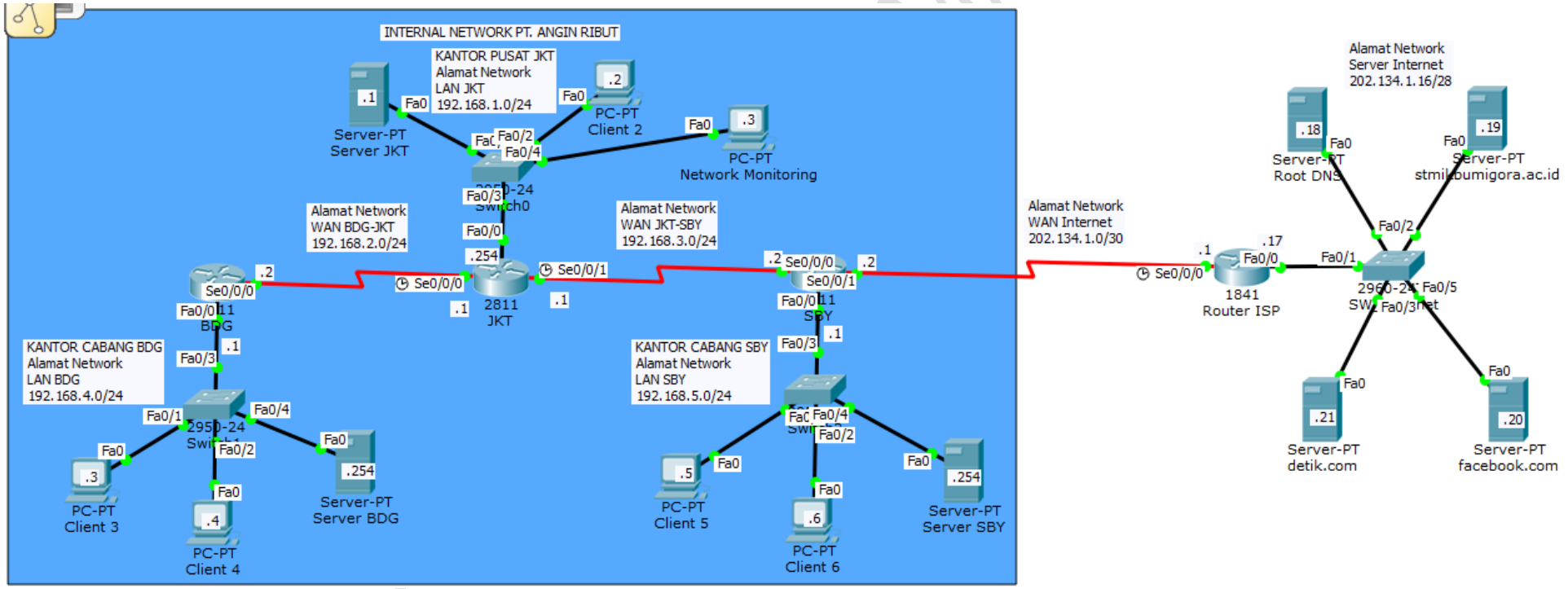
PEMBAHASAN SOLUSI SOAL UJIAN TENGAH SEMESTER (UTS) GENAP - TAHUN AKADEMIK 2016/2017
PRAKTIKUM SISTEM KEAMANAN JARINGAN TENTANG ROUTING STATIK DAN CISCO ACCESS CONTROL LIST (ACL)

Oleh I Putu Hariyadi (putu.hariyadi@stmikbumigora.ac.id)

SOAL:

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



1. Konfigurasi routing statik pada *router BDG, JKT* dan *SBY* agar antar jaringan internal kantor pusat dan cabang dari PT. Angin Ribut dapat saling berkomunikasi. Verifikasi komunikasi host antar jaringan menggunakan utilitas *ping* atau *Simple PDU* **(Point: 16)**.
   Catatan: Sintak penulisan parameter *gateway* pada konfigurasi *routing static* dan *default route* menggunakan referensi alamat IP.
2. Konfigurasi *NAT Overload* atau *Port Address Translation (PAT)* pada *router SBY* agar mengijinkan akses Internet hanya dari seluruh client yang terdapat di LAN JKT, LAN BDG dan LAN SBY. Verifikasi akses Internet melalui *browser* dari seluruh client **(Point: 36)**.
   Catatan:
   a) Sintak penulisan parameter *gateway* pada konfigurasi *routing static* dan *default route* menggunakan referensi alamat IP.
   b) Menggunakan *Numbered Access Control List (ACL)* untuk penyelesaian solusi dengan ketentuan sebagai berikut:
      - Apabila menggunakan *ACL Standard* maka gunakan nomor ACL **pertama** dari rentang yang diijinkan pada ACL tersebut.
      - Apabila menggunakan *ACL Extended* maka gunakan nomor ACL **terakhir** dari rentang yang diijinkan pada ACL tersebut.
3. Konfigurasi ACL di router JKT, BDG dan SBY agar hanya mengijinkan akses *telnet* dari *PC Network Monitoring* yang terdapat di LAN JKT. Verifikasi akses *telnet* ke seluruh router internal PT. Angin Ribut melalui *PC Network Monitoring* **(Point: 24)**.
   Catatan: Menggunakan *Numbered Access Control List (ACL)* untuk penyelesaian solusi dengan ketentuan yaitu menggunakan nomor ACL **terakhir** dari rentang yang diijinkan pada *ACL Standard* atau *ACL Extended*.
4. Konfigurasi ACL dengan ketentuan sebagai berikut **(Point: 24)**:
   a) Hanya mengijinkan host-host di LAN Kantor Pusat JKT dan LAN Kantor Cabang BDG yang dapat mengakses layanan HTTP dan HTTPS pada *Server JKT*. Verifikasi akses HTTP dan HTTPS menggunakan *browser* dari host-host di LAN JKT dan BDG ke Server JKT.
   b) Hanya mengijinkan host-host di LAN Kantor Pusat JKT dan LAN Kantor Cabang SBY yang dapat mengakses layanan FTP pada Server JKT. Verifikasi akses FTP melalui *Command Prompt* dari host-host di LAN JKT dan SBY ke Server JKT**.**
   Catatan: Menggunakan *Numbered Access Control List (ACL)* untuk penyelesaian solusi dengan ketentuan yaitu menggunakan nomor ACL **pertama** dari rentang yang diijinkan pada *ACL Standard* atau *ACL Extended*.

Sandi login yang digunakan untuk mengakses *Command Line Interface (CLI)* dari *router BDG*, *JKT* dan *SBY* adalah sebagai berikut:

- Console: **cisco**
- Privilege: **sanfran**
- Telnet: **sanjose**

SOLUSI SOAL NO. 1:

A. Konfigurasi Routing Statik di Router BDG

Berpindah ke mode *privilege*

```
BDG> enable
```

Berpindah ke mode *global configuration*

```
BDG# conf t
```

Membuat *routing static* untuk menjangkau **LAN Kantor Pusat JKT** melalui **router JKT**

```
BDG(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

Membuat *routing static* untuk menjangkau **WAN JKT-SBY** melalui **router JKT**

```
BDG(config)# ip route 192.168.3.0 255.255.255.0 192.168.2.1
```

Membuat *routing static* untuk menjangkau **LAN Kantor Cabang SBY** melalui **router JKT**

```
BDG(config)# ip route 192.168.5.0 255.255.255.0 192.168.2.1
```

Berpindah ke mode *privilege*

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

Menampilkan informasi tabel *routing*

```
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 not set

S    192.168.1.0/24 [1/0] via 192.168.2.1
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.1
C    192.168.4.0/24 is directly connected, FastEthernet0/0
S    192.168.5.0/24 [1/0] via 192.168.2.1
```

Perhatikan kode **S** pada output diatas menunjukkan informasi tentang hasil dari konfigurasi *routing static*.

B. Konfigurasi Routing Statik di Router JKT

Berpindah ke mode privilege

```
JKT> enable
```

Berpindah ke mode global configuration

```
JKT# conf t
```

Membuat *routing static* untuk menjangkau **LAN Kantor Cabang BDG** melalui **router BDG**

```
JKT(config)# ip route 192.168.4.0 255.255.255.0 192.168.2.2
```

Membuat *routing static* untuk menjangkau **LAN Kantor Cabang SBY** melalui **router SBY**

```
JKT(config)# ip route 192.168.5.0 255.255.255.0 192.168.3.2
```

Berpindah ke mode *privilege*

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

Menampilkan informasi tabel *routing*

```
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
S    192.168.4.0/24 [1/0] via 192.168.2.2
S    192.168.5.0/24 [1/0] via 192.168.3.2
```

Perhatikan kode **S** pada output diatas menunjukkan informasi tentang hasil dari konfigurasi *routing static*.

C. Konfigurasi Routing Statik di Router SBY

Berpindah ke mode *privilege*

```
SBY> enable
```

Berpindah ke mode global configuration

```
SBY# conf t
```

Membuat *routing static* untuk menjangkau **LAN Kantor Pusat JKT** melalui **router JKT**

```
SBY(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
```

Membuat *routing static* untuk menjangkau **WAN BDG-JKT** melalui **router JKT**

```
SBY(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.1
```

Membuat *routing static* untuk menjangkau **LAN Kantor Cabang BDG** melalui **router JKT**

```
SBY(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.1
```

Berpindah ke mode privilege

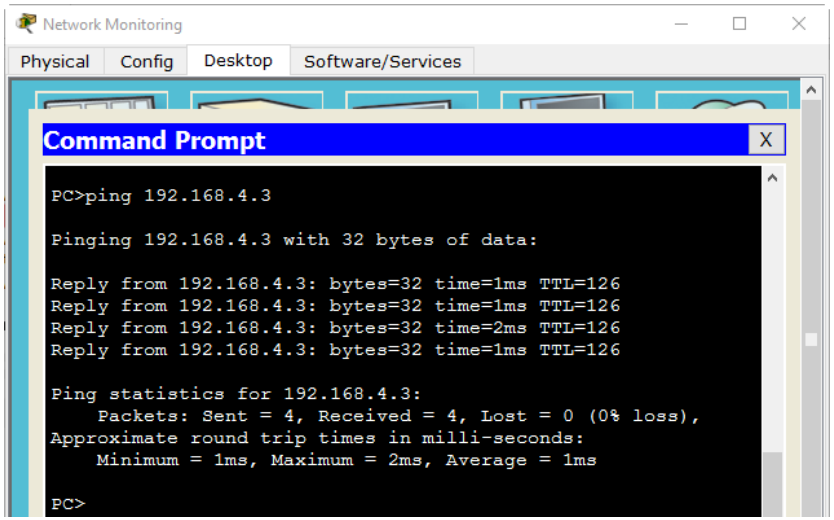
```
SBY(config)# end
```

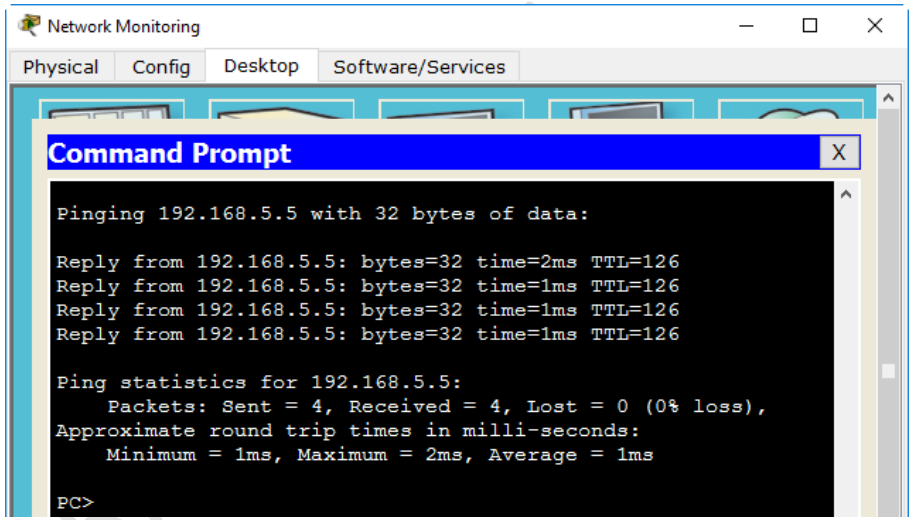
Menampilkan informasi tabel *routing*

```
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

S    192.168.1.0/24 [1/0] via 192.168.3.1
S    192.168.2.0/24 [1/0] via 192.168.3.1
C    192.168.3.0/24 is directly connected, Serial0/0/0
S    192.168.4.0/24 [1/0] via 192.168.3.1
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 **S** pada output diatas menunjukkan informasi tentang hasil dari konfigurasi *routing static*.

Verifikasi koneksi antar *host* dengan mengeksekusi perintah **ping** dari **PC Network Monitoring** yang terdapat di **LAN Kantor Pusat JKT** ke **Client3 (192.168.4.3)** yang terdapat di **LAN Kantor Cabang BDG** dan **Client5 (192.168.5.5)** yang terdapat di **LAN Kantor Cabang SBY**, seperti terlihat pada gambar berikut:





Pastikan koneksi berhasil dilakukan.

SOLUSI SOAL NO. 2:

A. Mengatur default route di router SBY

Berpindah ke mode *privilege*

```
SBY> enable
```

Berpindah ke *mode global configuration*

```
SBY# conf t
```

Mengatur *default route*

```
SBY(config)# ip route 0.0.0.0 0.0.0.0 202.134.1.1
```

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 202.134.1.1 to network 0.0.0.0

S    192.168.1.0/24 [1/0] via 192.168.3.1
S    192.168.2.0/24 [1/0] via 192.168.3.1
C    192.168.3.0/24 is directly connected, Serial0/0/0
S    192.168.4.0/24 [1/0] via 192.168.3.1
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 [1/0] via 202.134.1.1
```

Perhatikan kode **S*** pada output diatas menunjukkan informasi tentang hasil dari konfigurasi *default route*.

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 100 percent (5/5), round-trip min/avg/max = 2/11/31 ms
```

Pastikan hasil koneksi berhasil dilakukan.

B. Mengaktifkan NAT pada interface s0/0/0 dan s0/0/1 serta f0/0

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 *f0/0*

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

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 satu mode sebelumnya

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

C. Membuat ACL agar dari seluruh client yang terdapat di LAN JKT, LAN BDG dan LAN SBY dapat mengakses Internet sehingga server di masing-masing LAN harus ditolak aksesnya.

Menolak akses *Internet* dari *Server JKT*

```
SBY(config)# access-list 1 deny host 192.168.1.1
```

Menolak akses *Internet* dari *Server BDG*

```
SBY(config)# access-list 1 deny host 192.168.4.254
```

Menolak akses *Internet* dari *Server SBY*

```
SBY(config)# access-list 1 deny host 192.168.5.254
```

Mengijinkan akses *Internet* dari *LAN JKT*

```
SBY(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Mengijinkan akses *Internet* dari *LAN BDG*

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

Mengijinkan akses *Internet* dari *LAN SBY*

```
SBY(config)# access-list 1 permit 192.168.5.0 0.0.0.255
```

D. Membuat NAT Overload

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

Berpindah ke *mode privilege*

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

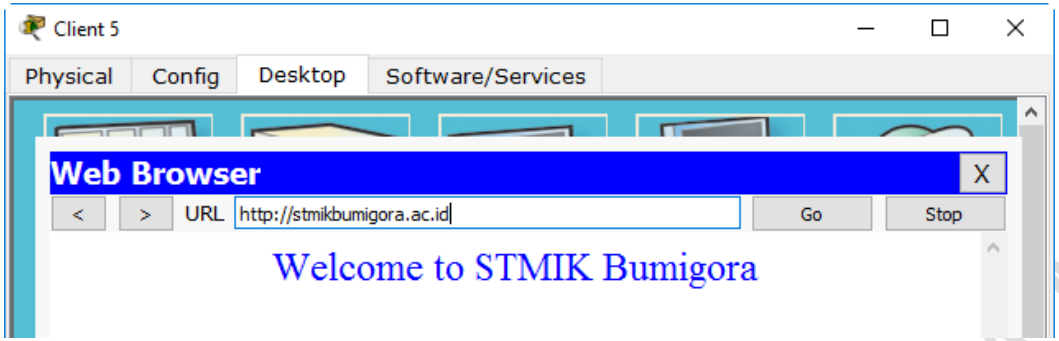
E. Memverifikasi ACL

```
SBY#show ip access-list
Standard IP access list 1
    10 deny host 192.168.1.1
    20 deny host 192.168.4.254
    30 deny host 192.168.5.254
    40 permit 192.168.1.0 0.0.0.255
    50 permit 192.168.4.0 0.0.0.255
    60 permit 192.168.5.0 0.0.0.255
```

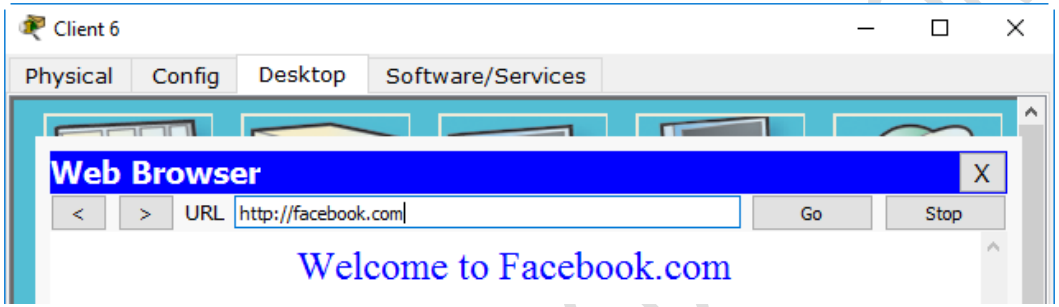
F. Memverifikasi pengaktifan NAT pada interface

```
SBY#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: FastEthernet0/0 , Serial0/0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

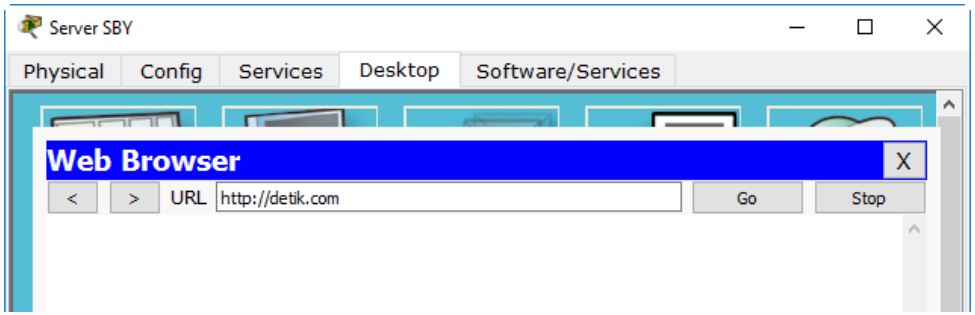
G. Memverifikasi koneksi Internet dari client5 yang terdapat di LAN Kantor Cabang SBY menggunakan web browser dengan mengakses salah satu situs di Internet sebagai contoh http://stmikbumigora.ac.id.



Verifikasi koneksi Internet juga dapat dilakukan dari *Client6* dan pastikan hasilnya sukses, seperti terlihat pada gambar berikut:



Sebaliknya pastikan pula *server SBY* tidak dapat mengakses *Internet*, seperti terlihat pada gambar berikut:



Percobaan koneksi dari *Server SBY* yang ditolak aksesnya dapat pula diverifikasi dengan melihat informasi *access list*, seperti terlihat pada gambar berikut:

```
SBY#show ip access-list
Standard IP access list 1
    10 deny host 192.168.1.1
    20 deny host 192.168.4.254
    30 deny host 192.168.5.254 (28 match(es))
    40 permit 192.168.1.0 0.0.0.255
    50 permit 192.168.4.0 0.0.0.255
    60 permit 192.168.5.0 0.0.0.255 (8 match(es))
```

H. Memverifikasi hasil translasi NAT di router SBY

```
SBY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 202.134.1.2:1025   192.168.5.6:1025   202.134.1.18:53    202.134.1.18:53
tcp 202.134.1.2:1024   192.168.5.6:1025   202.134.1.20:80    202.134.1.20:80
tcp 202.134.1.2:1025   192.168.5.5:1025   202.134.1.19:80    202.134.1.19:80
```

I. Mengatur default route di router JKT

Berpindah ke *mode privilege*

```
JKT> enable
```

Berpindah ke *mode global configuration*

```
JKT# conf t
```

Membuat *default route* agar dapat merutekan paket data ke Internet melalui *router SBY*

```
JKT(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.2
```

Berpindah ke *mode privilege*

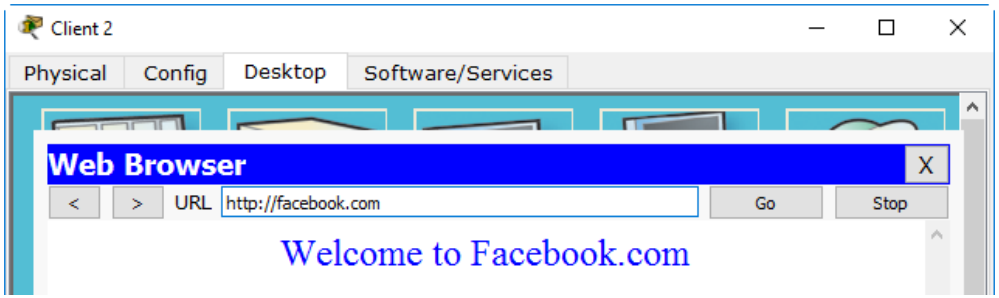
```
JKT(config)# end
```

Menampilkan informasi *table routing*

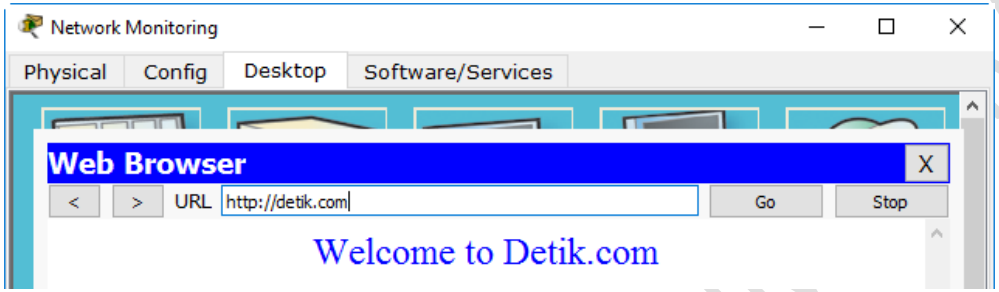
```
JKT#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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
S    192.168.4.0/24 [1/0] via 192.168.2.2
S    192.168.5.0/24 [1/0] via 192.168.3.2
S*   0.0.0.0/0 [1/0] via 192.168.3.2
```

Perhatikan kode **S*** pada output diatas menunjukkan informasi tentang hasil dari konfigurasi *default route*.

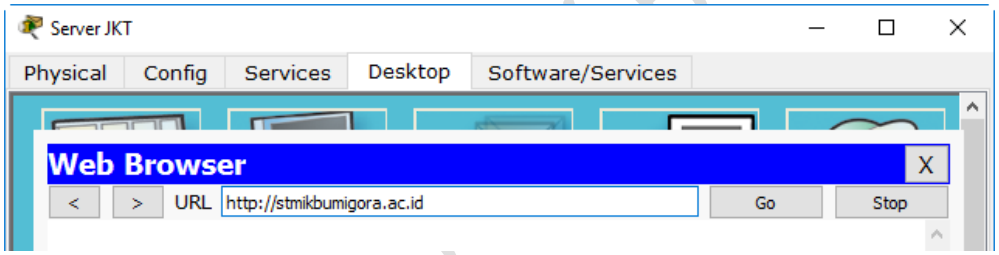
J. Memverifikasi koneksi Internet dari client2 yang terdapat di LAN Kantor Pusat JKT menggunakan web browser dengan mengakses salah satu situs di Internet sebagai contoh http://facebook.com.



Verifikasi koneksi Internet juga dapat dilakukan dari *PC Network Monitoring* dan pastikan hasilnya sukses, seperti terlihat pada gambar berikut:



Sebaliknya pastikan pula *server SBY* tidak dapat mengakses *Internet*, seperti terlihat pada gambar berikut:



K. Mengatur default route di router BDG

Berpindah ke *mode privilege*

```
BDG> enable
```

Berpindah ke *mode global configuration*

```
BDG# conf t
```

Membuat *default route* agar dapat merutekan paket data ke Internet melalui *router JKT*

```
BDG(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Berpindah ke *mode privilege*

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

Menampilkan informasi *table routing*

```
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

S    192.168.1.0/24 [1/0] via 192.168.2.1
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

```
S     192.168.3.0/24 [1/0] via 192.168.2.1
C     192.168.4.0/24 is directly connected, FastEthernet0/0
S     192.168.5.0/24 [1/0] via 192.168.2.1
S*    0.0.0.0/0 [1/0] via 192.168.2.1
```

Perhatikan kode **S*** pada output diatas menunjukkan informasi tentang hasil dari konfigurasi *default route*.

SOLUSI SOAL NO. 3:

A. Konfigurasi ACL untuk mengijinkan telnet ke router JKT hanya dari host PC Network Monitoring yang terdapat di LAN Kantor Pusat JKT

Berpindah ke *privilege mode*

```
JKT> enable
```

Berpindah ke mode *global configuration*

```
JKT# conf t
```

Membuat *Standard ACL* untuk mengijinkan akses *PC Network Monitoring* **(192.168.1.3)**

```
JKT(config)# access-list 99 permit 192.168.1.3
```

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 192.168.1.3
```

Memverifikasi hasil penerapan ACL pada *line vty*

```
JKT# show run
```

…….

…….

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

……..

…….

B. Konfigurasi ACL untuk mengijinkan telnet ke router BDG hanya dari host PC Network Monitoring yang terdapat di LAN Kantor Pusat JKT

Berpindah ke *privilege mode*

```
BDG> enable
```

Berpindah ke mode *global configuration*

```
BDG# conf t
```

Membuat *Standard ACL* untuk mengijinkan akses *PC Network Monitoring* **(192.168.1.3)**

```
BDG(config)# access-list 99 permit 192.168.1.3
```

Berpindah ke *line configuration*

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

Menerapkan ACL yang telah dibuat

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

Berpindah ke *privilege mode*

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

Menampilkan informasi ACL yang terdapat pada *router BDG*

```
BDG#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.3
```

Memverifikasi hasil penerapan ACL pada *line vty*

```
BDG# show run
```

…….

……..

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

……..

……..

C. Konfigurasi ACL untuk mengijinkan telnet ke router SBY hanya dari host PC Network Monitoring yang terdapat di LAN Kantor Pusat JKT

Berpindah ke *privilege mode*

```
SBY> enable
```

Berpindah ke mode *global configuration*

```
SBY# conf t
```

Membuat *Standard ACL* untuk mengijinkan akses *PC Network Monitoring* **(192.168.1.3)**

```
SBY(config)# access-list 99 permit 192.168.1.3
```

Berpindah ke *line configuration*

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

Menerapkan ACL yang telah dibuat

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

Berpindah ke *privilege mode*

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

Menampilkan informasi ACL yang terdapat pada *router SBY*

```
SBY#show ip access-list
Standard IP access list 1
    10 deny host 192.168.1.1 (4 match(es))
    20 deny host 192.168.4.254
    30 deny host 192.168.5.254 (28 match(es))
    40 permit 192.168.1.0 0.0.0.255 (8 match(es))
    50 permit 192.168.4.0 0.0.0.255
    60 permit 192.168.5.0 0.0.0.255 (8 match(es))
Standard IP access list 99
    10 permit host 192.168.1.3
```

Memverifikasi hasil penerapan ACL pada *line vty*

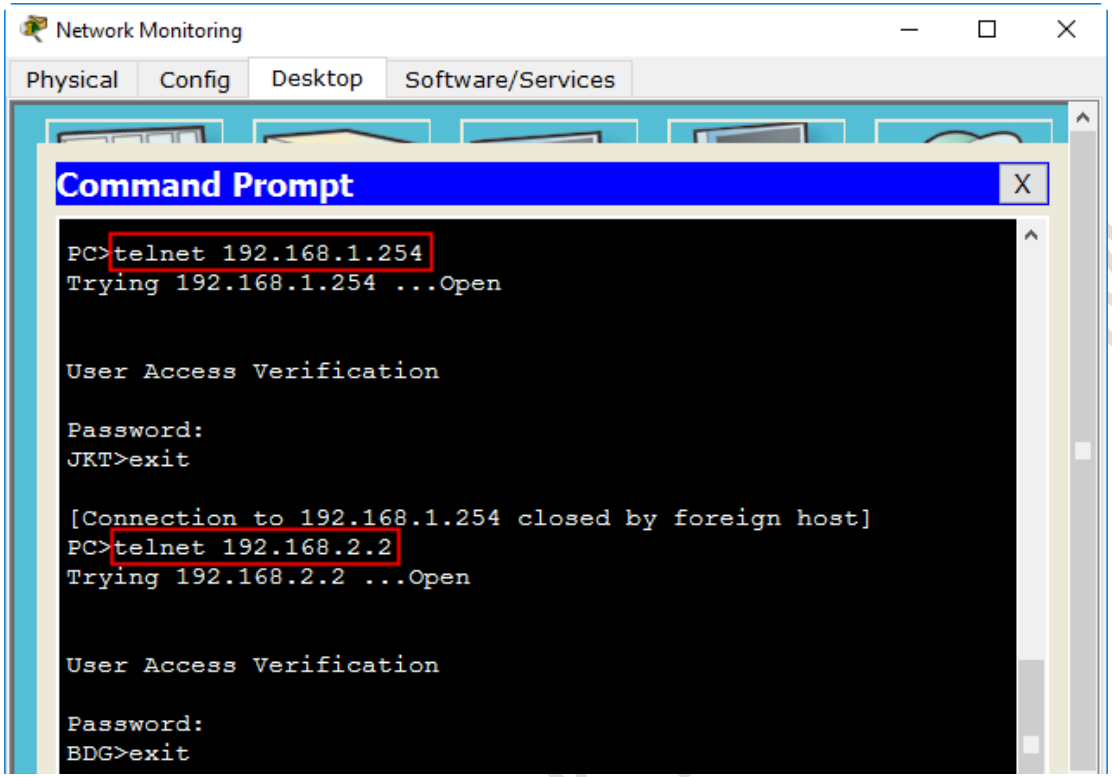
```
SBY# show run
```

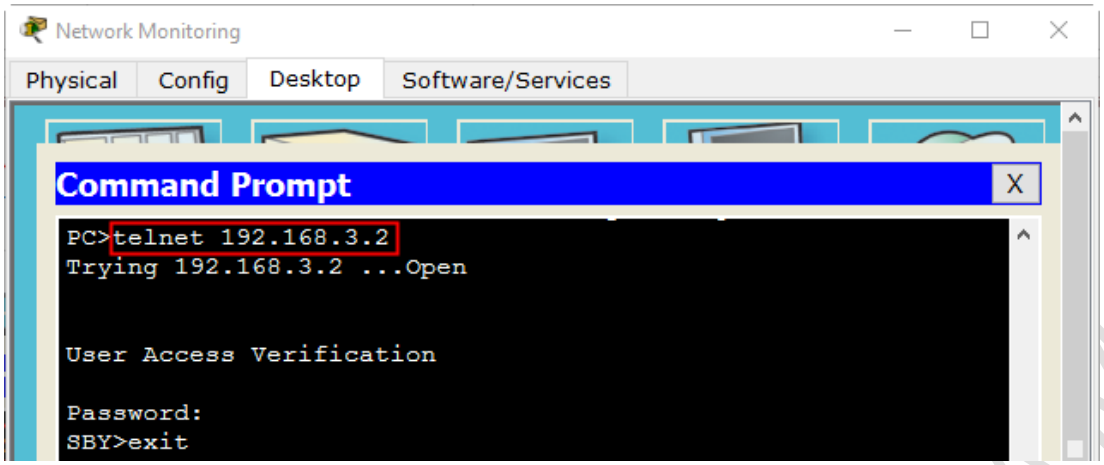
…….

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

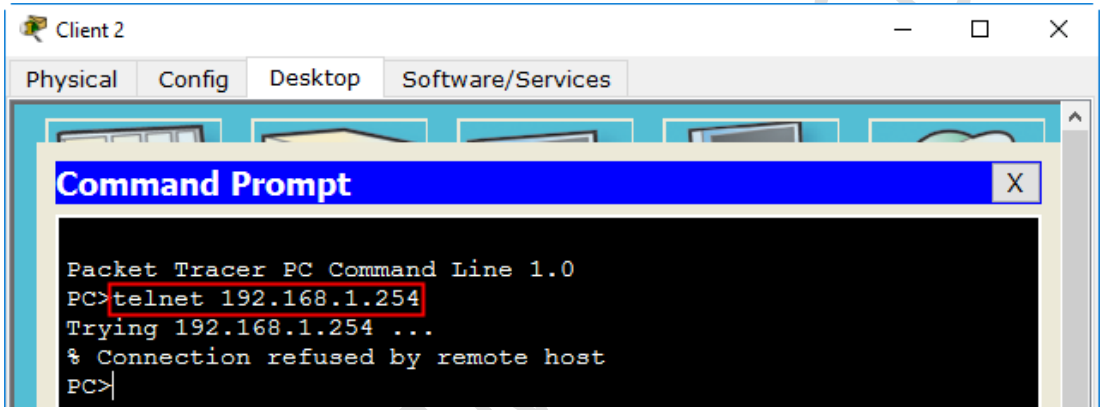
……..

D. Verifikasi akses telnet dari PC Network Monitoring yang terdapat di LAN Kantor Pusat JKT ke router JKT (192.168.1.254), BDG (192.168.2.2) dan SBY (192.168.3.2)





Pastikan akses *telnet* ke *router BDG, JKT* dan *SBY* dari *host* selain *PC Network Monitoring* ditolak aksesnya. Sebagai contoh percobaan akses *telnet* dari *PC Client2* ke *router JKT* yang ditolak, seperti terlihat pada gambar berikut:



SOLUSI SOAL No. 4:

A. Konfigurasi ACL agar hanya mengijinkan host-host di *LAN Kantor Pusat JKT* dan *LAN Kantor Cabang BDG* yang dapat mengakses layanan *HTTP* dan *HTTPS* pada *Server JKT*.

Berpindah ke *privilege mode*

```
JKT> enable
```

Berpindah ke mode *global configuration*

```
JKT# conf t
```

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

```
JKT(config)# access-list 100 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq www
```

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

```
JKT(config)# access-list 100 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq 443
```

Berpindah ke *interface configuration*

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

Menerapkan ACL yang telah dibuat

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

Berpindah ke *mode privilege*

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

Menampilkan informasi ACL yang terdapat pada *router JKT*

```
JKT#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.3 (4 match(es))
Extended IP access list 100
    10 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq www
    20 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq 443
```

Memverifikasi penerapan ACL pada *interface f0/0*

```
JKT#show ip int f0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.1.254/24
  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
  Proxy ARP is enabled
  Security level is default
```

B. Verifikasi akses HTTP dan HTTPS menggunakan browser dari host-host di LAN Kantor Pusat JKT ke Server JKT. Sebagai contoh dari PC Client2, seperti terlihat pada gambar berikut:

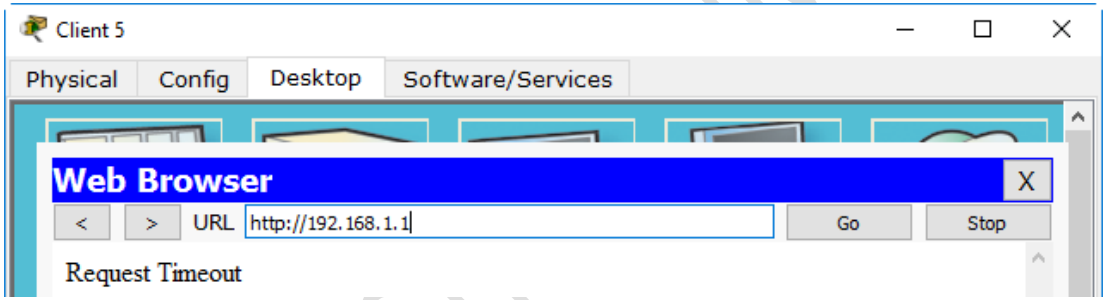
Terlihat akses *HTTP* dan *HTTPS* dari *client2* berhasil dilakukan. Akses *HTTP* dan *HTTPS* dari *host-host* di *LAN Kantor Pusat JKT* sebagai contoh dari *Client2* ke *Server JKT* tidak melalui *router JKT* karena keduanya berada dalam satu *network* sehingga tidak memerlukan pengaturan ACL di *router JKT*.

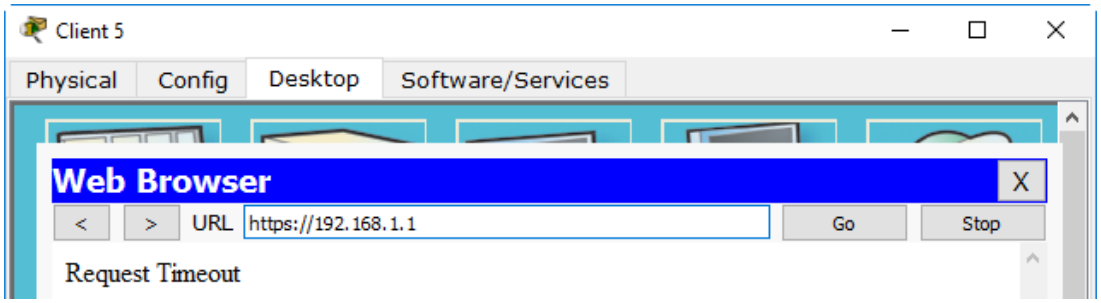
C. Verifikasi akses HTTP dan HTTPS menggunakan browser dari host-host di LAN BDG ke Server JKT, sebagai contoh dari PC Client3, seperti terlihat pada gambar berikut:

Terlihat akses *HTTP* dan *HTTPS* dari *client3* berhasil dilakukan. Percobaan akses *HTTP* dan *HTTPS* dari *host-host* di *LAN Kantor Cabang BDG* ke *Server JKT* sebagai contoh dari *Client3* dapat diverifikasi dengan melihat informasi *access-list* di *router JKT*, seperti terlihat pada gambar berikut:

```
JKT#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.3 (4 match(es))
Extended IP access list 100
    10 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq www (5 match(es))
    20 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq 443 (5 match(es))
```

D. Verifikasi akses HTTP dan HTTPS menggunakan browser dari host-host di LAN SBY ke Server JKT yang ditolak, sebagai contoh dari PC Client5, seperti terlihat pada gambar berikut:





Terlihat akses *HTTP* dan *HTTPS* dari *Client5* ke *Server JKT* tidak berhasil dilakukan.

SOLUSI SOAL No. 5:

A. Konfigurasi ACL agar mengijinkan hanya mengijinkan *host-host* di LAN Kantor Pusat JKT dan LAN Kantor Cabang SBY yang dapat mengakses layanan FTP pada Server JKT

Berpindah ke *privilege mode*

```
JKT> enable
```

Berpindah ke mode *global configuration*

```
JKT# conf t
```

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

```
JKT(config)# access-list 100 permit tcp 192.168.5.0 0.0.0.255 host 192.168.1.1 range 20 ftp
```

Membuat *Extended ACL* untuk mengijinkan balasan *DNS query* dari *Server DNS* dengan port 53 dimana pada awalnya permintaan *DNS query* dikirimkan dari *host-host* di *LAN Kantor Pusat JKT* ke *Server Root DNS* sehingga akses Internet menggunakan nama domain dapat dilakukan.

```
JKT(config)# access-list 100 permit udp any eq 53 any
```

Membuat *Extended ACL* untuk mengijinkan koneksi dari alamat IP sumber berapapun ke alamat IP tujuan berapapun dengan port lebih besar dari 1023.

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

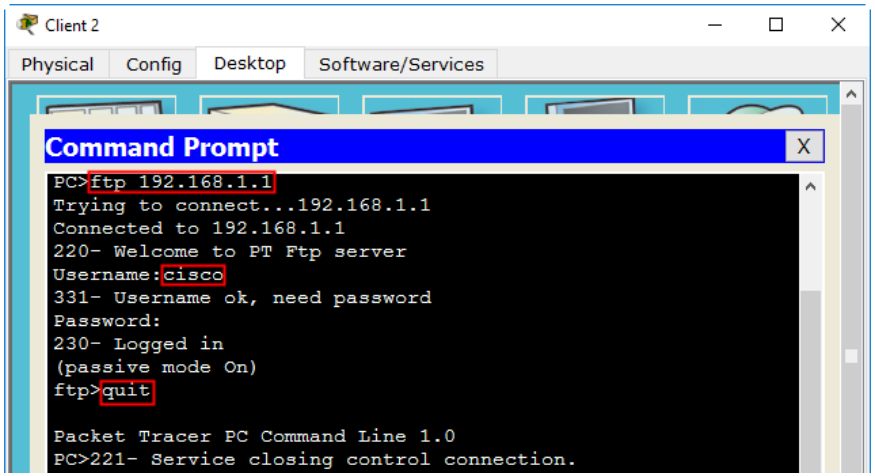
Berpindah ke *privilege mode*

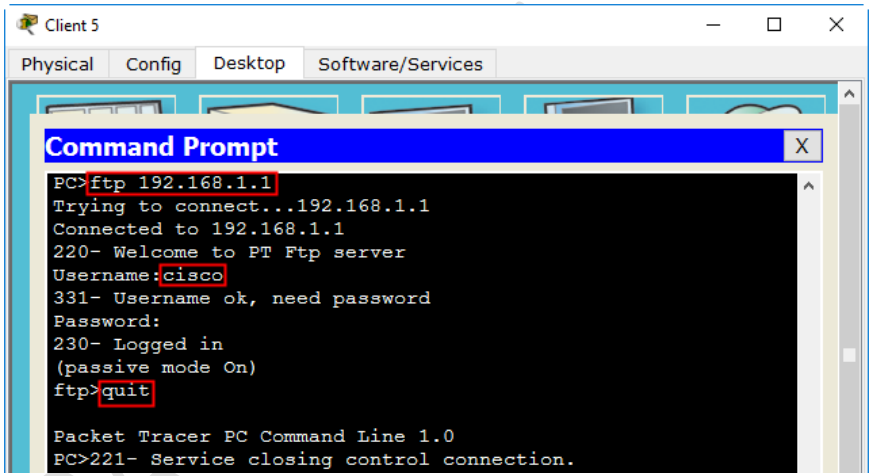
```
JKT(config)# enable
```

Menampilkan informasi *access-list*

```
JKT#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.3 (4 match(es))
Extended IP access list 100
    10 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq www (5 match(es))
    20 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq 443 (5 match(es))
    30 permit tcp 192.168.5.0 0.0.0.255 host 192.168.1.1 range 20 ftp
    40 permit udp any eq domain any
    50 permit tcp any any gt 1023
```

B. Verifikasi akses FTP melalui *Command Prompt* dari *host-host* di *LAN JKT* dan SBY ke *Server JKT*. Sebagai contoh dari Client2 yang terdapat di LAN Kantor Cabang JKT dan Client5 yang terdapat di LAN Kantor Cabang SBY, seperti terlihat pada gambar berikut:





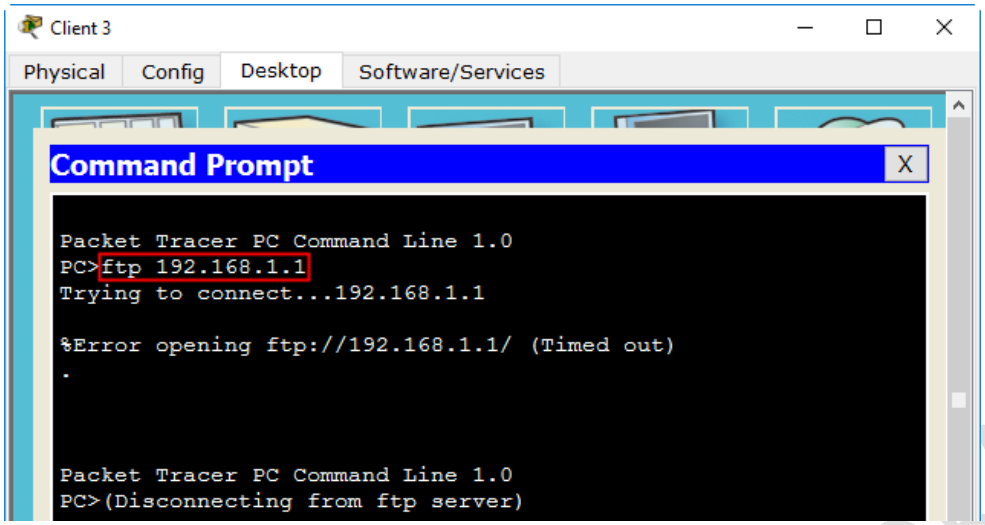
Username dan *password FTP* menggunakan "**cisco**". Terlihat akses FTP dari *Client2* dan *Client5* berhasil dilakukan.

Akses FTP dari *host-host* di *LAN Kantor Pusat JKT* sebagai contoh dari *Client2* ke *Server JKT* tidak melalui *router JKT* karena keduanya berada dalam satu *network* sehingga tidak memerlukan pengaturan ACL di *router JKT*. Sebaliknya akses ke layanan FTP di *Server JKT* dari *host-host* di *LAN Kantor Cabang SBY* akan melalui *router JKT* sehingga memerlukan pengaturan ACL agar akses tersebut diijinkan.

Verifikasi juga dapat dengan melihat informasi *access list* di *router JKT*, seperti terlihat pada gambar berikut:

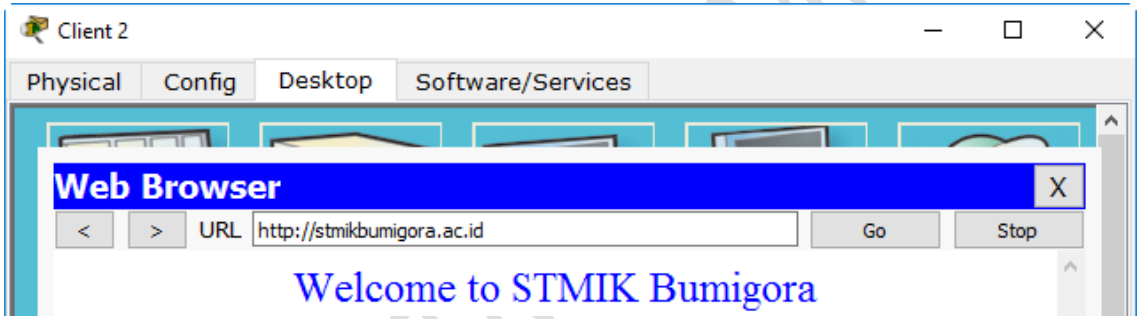
```
JKT#show ip access-list
Standard IP access list 99
    10 permit host 192.168.1.3 (4 match(es))
Extended IP access list 100
    10 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq www (5 match(es))
    20 permit tcp 192.168.4.0 0.0.0.255 host 192.168.1.1 eq 443 (5 match(es))
    30 permit tcp 192.168.5.0 0.0.0.255 host 192.168.1.1 range 20 ftp (36 match(es))
    40 permit udp any eq domain any (2 match(es))
    50 permit tcp any any gt 1023 (8 match(es))
```

C. Verifikasi akses FTP di *Server JKT* melalui *Command Prompt* dari *host-host* yang akan ditolak aksesnya yaitu dari luar *LAN JKT dan SBY*. Sebagai contoh dari Client3 yang terdapat di LAN Kantor Cabang BDG, seperti terlihat pada gambar berikut:



Terlihat akses FTP tidak dapat dilakukan.

D. Verifikasi akses Internet tetap dapat dilakukan dari *host-host* di *LAN JKT* menggunakan nama domain, sebagai contoh dari *Client2* ke situs *stmikbumigora.ac.id*, seperti terlihat pada gambar berikut:



Selamat Anda telah berhasil menyelesaikan pembahasan solusi soal UTS. Apabila terdapat pertanyaan, silakan mengirimkan melalui email ke alamat putu.hariyadi@stmikbumigora.ac.id. Terimakasih ☺