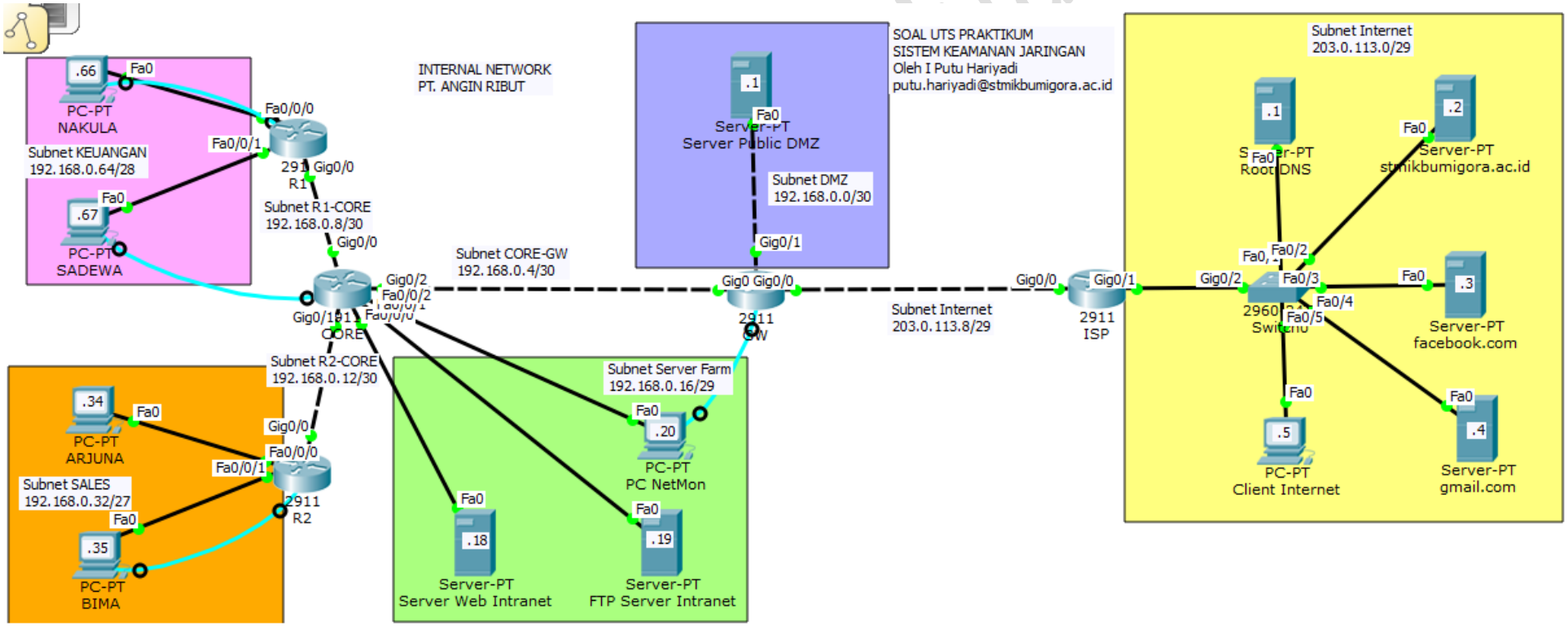
PEMBAHASAN SOLUSI SOAL UJIAN TENGAH SEMESTER (UTS) PRAKTIKUM SISTEM KEAMANAN JARINGAN (SKJ)

TENTANG ACCESS CONTROL LIST (ACL) PADA SEMESTER GENAP TAHUN AKADEMIK 2017/2018

STMIK BUMIGORA MATARAM

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

SOAL:



Sebuah perusahaan fiktif dengan nama **PT. Angin Ribut (AR)** memiliki jaringan internal untuk memfasilitasi komunikasi antara host-host yang terdapat di **bagian keuangan** dengan **bagian sales** serta akses ke layanan pada **Server Web** dan **FTP Intranet** yang terdapat pada **subnet Server Farm**. PT. AR juga memiliki koneksi Internet untuk menunjang kegiatan operasional perusahaan dan **Server Public** dengan nama domain**anginribut.com** yang terdapat di **area DMZ**. *Server Public* ini digunakan sebagai media distribusi informasi perusahaan agar dapat diakses oleh pengguna dari Internet. Selain itu PT. AR juga menggunakan layanan email dari **gmail.com** untuk korespondensi.

Terdapat 4 (empat) akun email yang telah dibuat di server **gmail.com** dan telah diatur pula **Email Client** atau **Mail User Agent** di PC pada jaringan internal PT. AR sehingga akun email tersebut dapat digunakan untuk mengirim dan menerima email yaitu:

No.	Nama Pengguna	Email Address	Password	Lokasi Email Client
1.	nakula	nakula@gmail.com	nakula	PC NAKULA di subnet KEUANGAN
2.	sadewa	sadewa@gmail.com	sadewa	PC SADEWA di subnet KEUANGAN
3.	arjuna	arjuna@gmail.com	arjuna	PC ARJUNA di subnet SALES
4.	bima	bima@gmail.com	bima	PC BIMA di subnet SALES
Nama PC dibuat sama dengan akun email yang telah diatur pada Email Client di PC tersebut untuk mempermudah ketika proses ujicoba.				

Konfigurasi pada perangkat router di jaringan internal PT. AR hanya dapat dilakukan melalui koneksi **console**. Sandi Login yang digunakan untuk mengakses CLI dari perangkat router di jaringan internal PT. AR adalah sebagai berikut:

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

Untuk mengamankan akses terhadap sumber daya di jaringan internal dan Internet maka PT. AR membuat kebijakan keamanan yang diimplementasikan menggunakan **Cisco Access Control List (ACL)**. Terdapat **5 (lima) tugas** yang harus diselesaikan agar komunikasi antar host di jaringan internal dapat dilakukan termasuk ke Internet dan untuk memenuhi kebijakan keamanan yang ditentukan oleh perusahaan. File template Cisco Packet Tracer Activities dari soal UTS ini dapat diunduh pada alamat berikut: http://iputuhariyadi.net/wp-content/uploads/2018/05/TEMPLATE-UTS-PSKJ-2018.zip. File dapat dibuka menggunakan Cisco Packet Tracer version 6.2. Limitasi waktu pengerjaan yang pada awalnya 80 menit telah dinonaktifkan agar rekan-rekan yang mencoba pembahasan ini tidak terkendala.

TUGAS 1

Konfigurasi routing protokol **RIPv2** pada **router R1, CORE, R2** dan **GW** agar antar jaringan internal PT. Angin Ribut (AR) termasuk **subnet DMZ** dapat saling berkomunikasi. Verifikasi komunikasi host antar jaringan menggunakan **Simple PDU**. Pastikan koneksi berhasil dilakukan.

CATATAN:

Command Line Interface (CLI) dari setiap router yang terdapat pada jaringan internal PT. AR hanya dapat diakses melalui **Terminal** dari PC yang terpasang kabel console menuju router tersebut.

- **CLI router R1** dapat diakses melalui **Terminal PC Nakula** yang terdapat di **subnet KEUANGAN**
- **CLI router CORE** dapat diakses melalui **Terminal PC Sadewa** yang terdapat di **subnet KEUANGAN**
- **CLI router R2** dapat diakses melalui **Terminal PC Bima** yang terdapat di **subnet SALES**
- **CLI router GW** dapat diakses melalui **Terminal PC NetMon** yang terdapat di **subnet Server Farm**

SOLUSI TUGAS 1:

A. Konfigurasi RIP di Router R1

Berpindah ke mode privilege

```
R1> enable
```

Berpindah ke mode global configuration

```
R1# conf t
```

Mengaktifkan **routing protocol RIP version 2**

```
R1(config)# router rip
```

```
R1(config-router)# version 2
```

Mengatur alamat jaringan yang dimasukkan pada routing update yaitu yang terhubung langsung dengan router R1

```
R1(config-router)# network 192.168.0.0
```

Berpindah ke mode privilege

```
R1(config-router)# end
```

Menampilkan informasi routing protocol yang aktif

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 13 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 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Vlan1                 2     2
  GigabitEthernet0/0    2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
          192.168.0.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
Distance: (default is 120)
```

B. Konfigurasi RIP di Router CORE

Berpindah ke mode privilege

```
CORE> enable
```

Berpindah ke mode global configuration

```
CORE# conf t
```

Mengaktifkan **routing protocol RIP version 2**

```
CORE(config)# router rip

CORE(config-router)# version 2
```

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

```
CORE(config-router)# network 192.168.0.0
```

Berpindah ke mode privilege

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

Menampilkan informasi routing protocol yang aktif

```
CORE#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 11 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 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Vlan1                 2     2
  GigabitEthernet0/0    2     2
  GigabitEthernet0/1    2     2
  GigabitEthernet0/2    2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
           192.168.0.0
Passive Interface(s):
Routing Information Sources:
           Gateway         Distance      Last Update
Distance: (default is 120)
```

Menampilkan informasi routing tabel

```
CORE#show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.0.0/24 is variably subnetted, 9 subnets, 3 masks
C       192.168.0.4/30 is directly connected, GigabitEthernet0/2
L       192.168.0.5/32 is directly connected, GigabitEthernet0/2
C       192.168.0.8/30 is directly connected, GigabitEthernet0/0
L       192.168.0.9/32 is directly connected, GigabitEthernet0/0
C       192.168.0.12/30 is directly connected, GigabitEthernet0/1
L       192.168.0.13/32 is directly connected, GigabitEthernet0/1
C       192.168.0.16/29 is directly connected, Vlan1
L       192.168.0.17/32 is directly connected, Vlan1
R       192.168.0.64/29 [120/1] via 192.168.0.10, 00:00:09, GigabitEthernet0/0
```

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

C. Konfigurasi RIP di Router R2

Berpindah ke mode privilege

```
R2> enable
```

Berpindah ke mode global configuration

```
R2# conf t
```

Mengaktifkan **routing protocol RIP version 2**

```
R2(config)# router rip
```

```
R2(config-router)# version 2
```

Mengatur alamat jaringan yang dimasukkan pada routing update yaitu yang terhubung langsung dengan router R2

```
R2(config-router)# network 192.168.0.0
```

Berpindah ke mode privilege

```
R2(config-router)# end
```

Menampilkan informasi routing protocol yang aktif

```
R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 19 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 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Vlan1                 2     2
  GigabitEthernet0/0    2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
           192.168.0.0
Passive Interface(s):
Routing Information Sources:
           Gateway         Distance      Last Update
Distance: (default is 120)
```

Menampilkan informasi routing table

```
R2#show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.0.0/24 is variably subnetted, 8 subnets, 4 masks
R       192.168.0.4/30 [120/1] via 192.168.0.13, 00:00:23, GigabitEthernet0/0
R       192.168.0.8/30 [120/1] via 192.168.0.13, 00:00:23, GigabitEthernet0/0
C       192.168.0.12/30 is directly connected, GigabitEthernet0/0
L       192.168.0.14/32 is directly connected, GigabitEthernet0/0
R       192.168.0.16/29 [120/1] via 192.168.0.13, 00:00:23, GigabitEthernet0/0
C       192.168.0.32/27 is directly connected, Vlan1
L       192.168.0.33/32 is directly connected, Vlan1
R       192.168.0.64/29 [120/2] via 192.168.0.13, 00:00:23, GigabitEthernet0/0
```

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

D. Konfigurasi RIP di Router GW

Berpindah ke mode privilege

```
GW> enable
```

Berpindah ke mode global configuration

```
GW# conf t
```

Mengaktifkan **routing protocol RIP version 2**

```
GW(config)# router rip
```

```
GW(config-router)# version 2
```

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

```
GW(config-router)# network 192.168.0.0
```

Berpindah ke mode privilege

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

Menampilkan informasi routing protocol yang aktif

```
GW#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 18 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 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  GigabitEthernet0/1    2     2
  GigabitEthernet0/2    2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
          192.168.0.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
Distance: (default is 120)
```

Menampilkan informasi routing table

```
GW#show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.0.0/24 is variably subnetted, 9 subnets, 4 masks
C       192.168.0.0/30 is directly connected, GigabitEthernet0/1
L       192.168.0.2/32 is directly connected, GigabitEthernet0/1
C       192.168.0.4/30 is directly connected, GigabitEthernet0/2
L       192.168.0.6/32 is directly connected, GigabitEthernet0/2
R       192.168.0.8/30 [120/1] via 192.168.0.5, 00:00:03, GigabitEthernet0/2
R       192.168.0.12/30 [120/1] via 192.168.0.5, 00:00:03, GigabitEthernet0/2
R       192.168.0.16/29 [120/1] via 192.168.0.5, 00:00:03, GigabitEthernet0/2
R       192.168.0.32/27 [120/2] via 192.168.0.5, 00:00:03, GigabitEthernet0/2
R       192.168.0.64/29 [120/2] via 192.168.0.5, 00:00:03, GigabitEthernet0/2
     203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C       203.0.113.8/29 is directly connected, GigabitEthernet0/0
L       203.0.113.9/32 is directly connected, GigabitEthernet0/0
```

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

Memverifikasi koneksi antar PC di beda subnet pada jaringan internal PT. Angin Ribut menggunakan **Simple PDU**, hasilnya seperti terlihat pada gambar berikut:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	NAKULA	ARJUNA	ICMP		0.000	N	0
	Successful	NAKULA	PC NetMon	ICMP		0.000	N	1
	Successful	NAKULA	Server Public DMZ	ICMP		0.000	N	2

Terlihat koneksi dari **PC NAKULA** ke **PC ARJUNA, PC NetMon**, dan **Server Public DMZ** berhasil dilakukan.

TUGAS 2

Konfigurasi **NAT Overload/Port Address Translation (PAT)** pada **Router GW** agar **mengijinkan akses Internet** dengan ketentuan:

1. Seluruh host pada **subnet KEUANGAN** hanya dapat mengakses layanan **Email** pada server **gmail.com** dengan alamat IP **203.0.113.4**.
2. Seluruh host di **subnet SALES** dapat mengakses layanan apapun di Internet.
3. Pada **subnet Server Farm hanya PC NetMon (Network Monitoring)** yang dapat mengakses keseluruhan layanan Internet.

Setelah konfigurasi selesai dilakukan, maka lakukan:

- Verifikasi pengiriman email melalui **Email Client** yang terdapat pada **PC NAKULA** ke **sadewa@gmail.com**. Subject atau topik pesan email bebas. Selanjutnya lakukan verifikasi pada **PC SADEWA** apakah email telah masuk.
- Verifikasi dengan mengakses layanan HTTP, HTTPS, Email dari **PC ARJUNA** dan **BIMA**
- Verifikasi pengiriman email melalui **Email Client** yang terdapat pada **PC ARJUNA** ke **bima@gmail.com**. Subject atau topik pesan email bebas. Selanjutnya lakukan verifikasi pada **PC BIMA** apakah email telah masuk.
- Verifikasi melalui browser **PC NetMon** dengan mengakses layanan **HTTP/HTTPS** dari server yang terdapat di **subnet Internet** seperti **http://stmikbumigora.ac.id, http://facebook.com,** dan **http://gmail.com**. Selain itu dapat pula dilakukan verifikasi akses ke layanan **FTP** pada *server Internet* melalui *command prompt*

PERHATIAN:

- Sintak penulisan parameter **gateway** pada konfigurasi **default route** menggunakan **referensi alamat IP**.
- ACL ditulis menggunakan *Numbered Access Control List (ACL)* dengan ketentuan yaitu menggunakan nomor ACL **terakhir** dari rentang yang diijinkan pada **ACL Standard** atau **ACL Extended**.

SOLUSI TUGAS 2

A. Mengatur default route agar router GW dapat merutekan paket data ke Internet

Berpindah ke mode global configuration

```
GW# conf t
```

Mengatur default route

```
GW(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.14
```

Berpindah ke mode privilege

```
GW(config)# end
```

Menampilkan informasi routing table

```
GW#show ip route
Codes: L - local, C - connected, S - static, 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 203.0.113.14 to network 0.0.0.0

     192.168.0.0/24 is variably subnetted, 9 subnets, 4 masks
C       192.168.0.0/30 is directly connected, GigabitEthernet0/1
L       192.168.0.2/32 is directly connected, GigabitEthernet0/1
C       192.168.0.4/30 is directly connected, GigabitEthernet0/2
L       192.168.0.6/32 is directly connected, GigabitEthernet0/2
R       192.168.0.8/30 [120/1] via 192.168.0.5, 00:00:22, GigabitEthernet0/2
R       192.168.0.12/30 [120/1] via 192.168.0.5, 00:00:22, GigabitEthernet0/2
R       192.168.0.16/29 [120/1] via 192.168.0.5, 00:00:22, GigabitEthernet0/2
R       192.168.0.32/27 [120/2] via 192.168.0.5, 00:00:22, GigabitEthernet0/2
R       192.168.0.64/29 [120/2] via 192.168.0.5, 00:00:22, GigabitEthernet0/2
     203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C       203.0.113.8/29 is directly connected, GigabitEthernet0/0
L       203.0.113.9/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 203.0.113.14
```

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

```
GW#ping 203.0.113.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Pastikan hasil eksekusi dengan ping adalah sukses.

B. Menyebarkan default route melalui RIP di Router GW

```
GW(config)# router rip

GW(config-router)# default-information originate

GW(config-router)# end
```

Memverifikasi hasil pengaturan penyebaran default route di router GW pada tabel routing di router R1

```
R1#show ip route
Codes: L - local, C - connected, S - static, 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 192.168.0.9 to network 0.0.0.0

     192.168.0.0/24 is variably subnetted, 9 subnets, 4 masks
R       192.168.0.0/30 [120/2] via 192.168.0.9, 00:00:04, GigabitEthernet0/0
R       192.168.0.4/30 [120/1] via 192.168.0.9, 00:00:04, GigabitEthernet0/0
C       192.168.0.8/30 is directly connected, GigabitEthernet0/0
L       192.168.0.10/32 is directly connected, GigabitEthernet0/0
R       192.168.0.12/30 [120/1] via 192.168.0.9, 00:00:04, GigabitEthernet0/0
R       192.168.0.16/29 [120/1] via 192.168.0.9, 00:00:04, GigabitEthernet0/0
R       192.168.0.32/27 [120/2] via 192.168.0.9, 00:00:04, GigabitEthernet0/0
C       192.168.0.64/29 is directly connected, Vlan1
L       192.168.0.65/32 is directly connected, Vlan1
R*   0.0.0.0/0 [120/2] via 192.168.0.9, 00:00:04, GigabitEthernet0/0
```

Memverifikasi hasil pengaturan penyebaran default route di router GW pada tabel routing di router CORE

```
CORE#show ip route
Codes: L - local, C - connected, S - static, 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 192.168.0.6 to network 0.0.0.0

     192.168.0.0/24 is variably subnetted, 11 subnets, 4 masks
R       192.168.0.0/30 [120/1] via 192.168.0.6, 00:00:11, GigabitEthernet0/2
C       192.168.0.4/30 is directly connected, GigabitEthernet0/2
L       192.168.0.5/32 is directly connected, GigabitEthernet0/2
C       192.168.0.8/30 is directly connected, GigabitEthernet0/0
L       192.168.0.9/32 is directly connected, GigabitEthernet0/0
C       192.168.0.12/30 is directly connected, GigabitEthernet0/1
L       192.168.0.13/32 is directly connected, GigabitEthernet0/1
C       192.168.0.16/29 is directly connected, Vlan1
L       192.168.0.17/32 is directly connected, Vlan1
R       192.168.0.32/27 [120/1] via 192.168.0.14, 00:00:11, GigabitEthernet0/1
R       192.168.0.64/29 [120/1] via 192.168.0.10, 00:00:05, GigabitEthernet0/0
R*   0.0.0.0/0 [120/1] via 192.168.0.6, 00:00:11, GigabitEthernet0/2
```

Memverifikasi hasil pengaturan penyebaran default route di router GW pada tabel routing di router R2

```
R2#show ip route
Codes: L - local, C - connected, S - static, 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 192.168.0.13 to network 0.0.0.0
```

```
     192.168.0.0/24 is variably subnetted, 9 subnets, 4 masks
R       192.168.0.0/30 [120/2] via 192.168.0.13, 00:00:27, GigabitEthernet0/0
R       192.168.0.4/30 [120/1] via 192.168.0.13, 00:00:27, GigabitEthernet0/0
R       192.168.0.8/30 [120/1] via 192.168.0.13, 00:00:27, GigabitEthernet0/0
C       192.168.0.12/30 is directly connected, GigabitEthernet0/0
L       192.168.0.14/32 is directly connected, GigabitEthernet0/0
R       192.168.0.16/29 [120/1] via 192.168.0.13, 00:00:27, GigabitEthernet0/0
C       192.168.0.32/27 is directly connected, Vlan1
L       192.168.0.33/32 is directly connected, Vlan1
R       192.168.0.64/29 [120/2] via 192.168.0.13, 00:00:27, GigabitEthernet0/0
R*   0.0.0.0/0 [120/2] via 192.168.0.13, 00:00:27, GigabitEthernet0/0
```

C. Mengaktifkan NAT pada interface gi0/0 dan gi0/2

Berpindah ke mode global configuration

```
GW# conf t
```

Berpindah ke interface configuration untuk gi0/2

```
GW(config)# int gi0/2
```

Mengatur NAT inside

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

Berpindah ke interface configuration untuk gi0/0

```
GW(config-if)# int gi0/0
```

Mengatur NAT outside

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

Berpindah ke mode ke satu mode sebelumnya

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

D. Membuat ACL agar mengijinkan seluruh host pada **subnet KEUANGAN** hanya dapat mengakses layanan **Email** pada server **gmail.com** dengan alamat IP **203.0.113.4**.

```
GW(config)#access-list 199 permit tcp 192.168.0.64 0.0.0.15 203.0.113.4 0.0.0.0 eq 25
GW(config)#access-list 199 permit tcp 192.168.0.64 0.0.0.15 203.0.113.4 0.0.0.0 eq 110
```

E. Membuat ACL agar mengijinkan seluruh host di **subnet SALES** dapat mengakses layanan apapun di Internet.

```
GW(config)#access-list 199 permit ip 192.168.0.32 0.0.0.31 0.0.0.0 255.255.255.255
```

F. Membuat ACL agar mengijinkan hanya **PC NetMon (Network Monitoring)** yang terdapat pada **subnet Server Farm** dapat mengakses keseluruhan layanan Internet.

```
GW(config)#access-list 199 permit ip 192.168.0.20 0.0.0.0 0.0.0.0 255.255.255.255
```

G. Membuat NAT Overload

```
GW(config)#ip nat inside source list 199 interface gi0/0 overload
```

Berpindah ke mode privilege

```
GW(config)# end
```

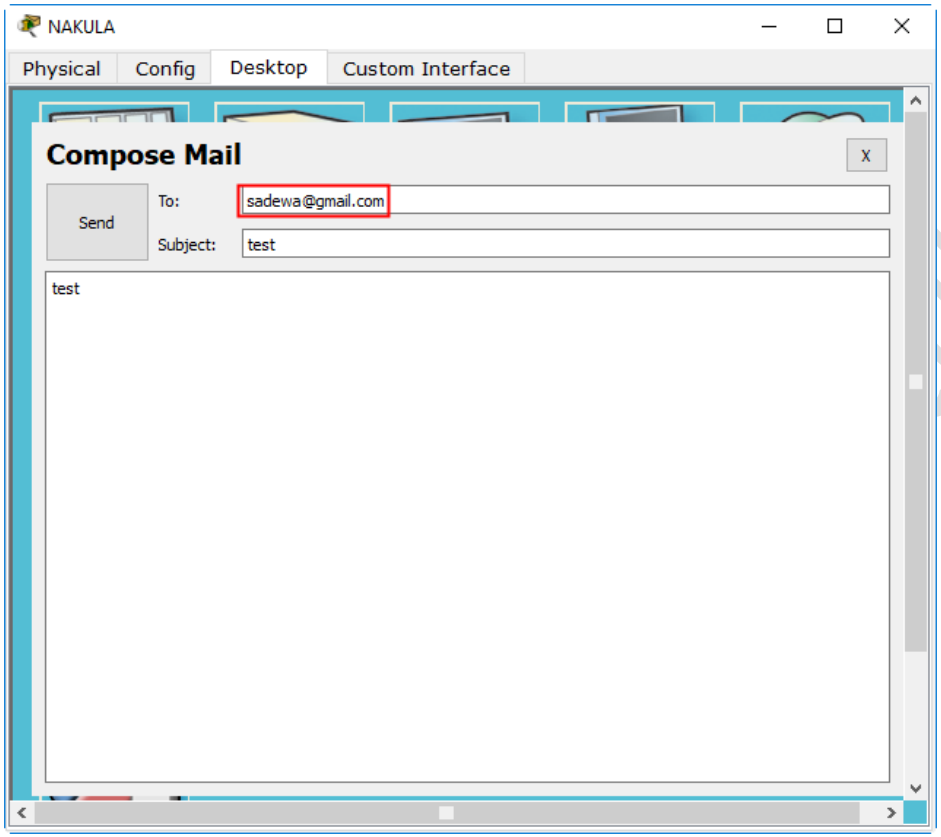
H. Memverifikasi ACL

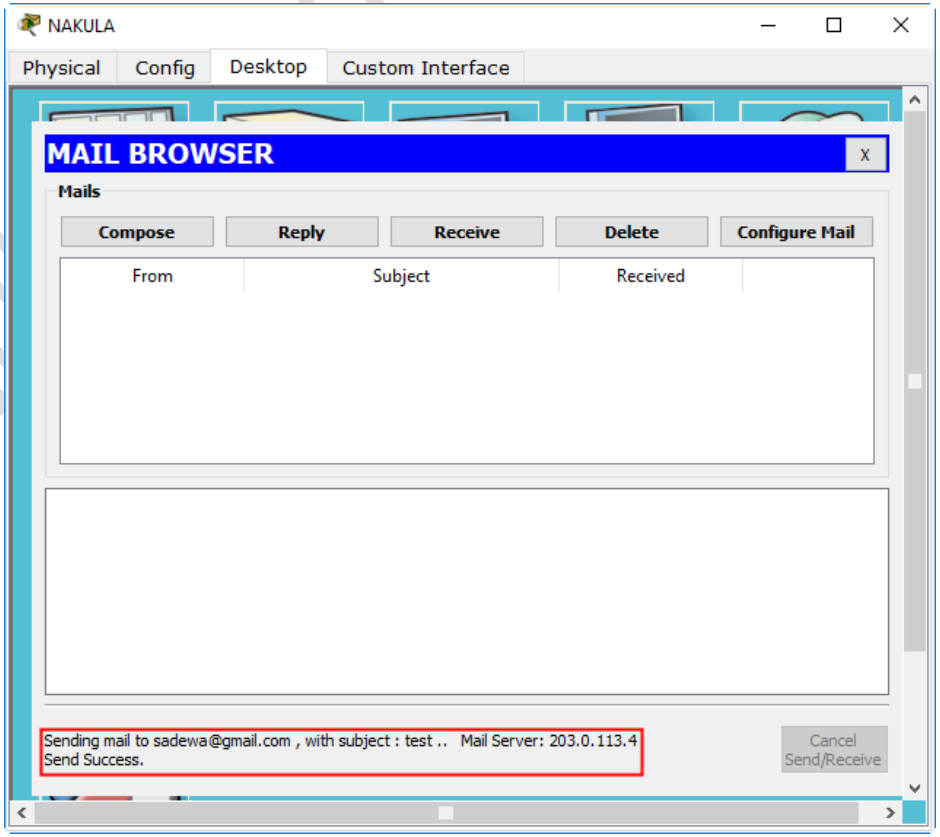
```
GW#show access-list
Extended IP access list 199
    10 permit tcp 192.168.0.64 0.0.0.15 host 203.0.113.4 eq smtp
    20 permit tcp 192.168.0.64 0.0.0.15 host 203.0.113.4 eq pop3
    30 permit ip 192.168.0.32 0.0.0.31 any
    40 permit ip host 192.168.0.20 any
```

I. Memverifikasi pengaktifan NAT pada interface

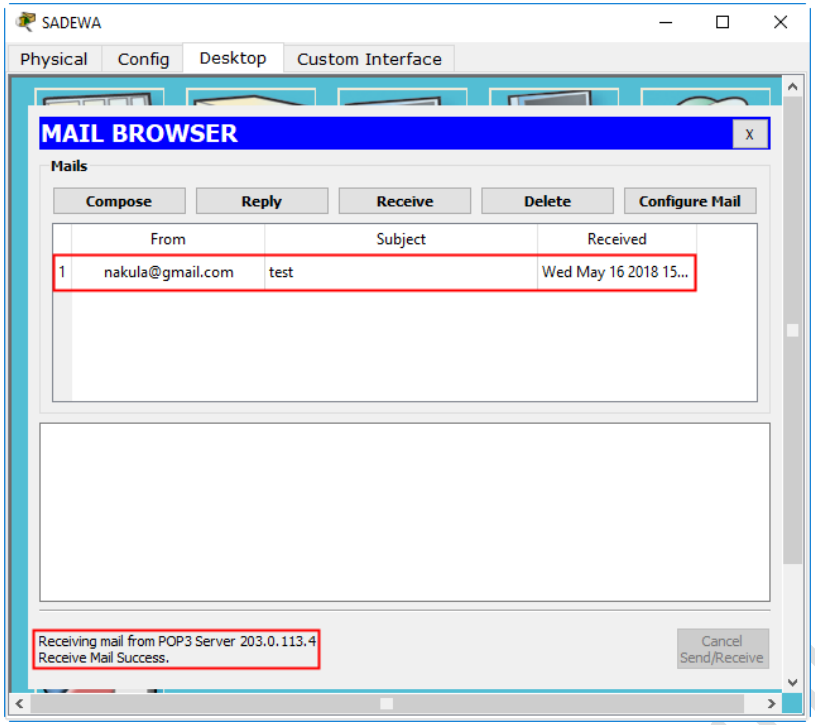
```
GW#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: GigabitEthernet0/2
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

J. Memverifikasi pengiriman email melalui **Email Client** yang terdapat pada **PC NAKULA** ke **sadewa@gmail.com**. Subject atau topik pesan email bebas.

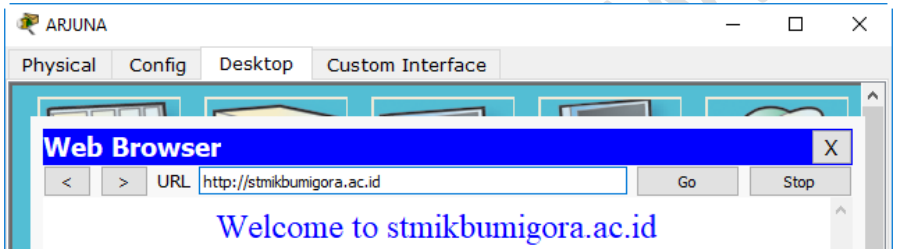


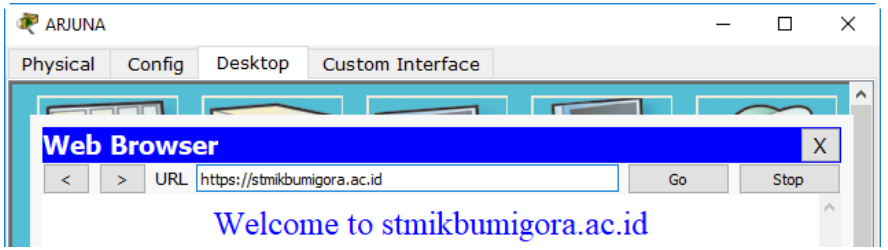


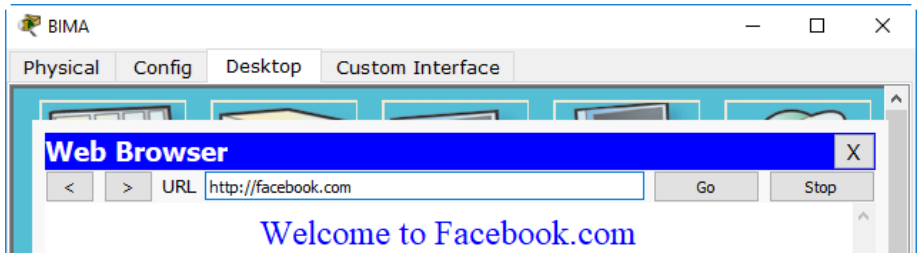
Terlihat email berhasil dikirim ke sadewa@gmail.com. Sedangkan pada **PC SADEWA** dilakukan pengunduhan email dari **POP3 Server**, seperti terlihat pada gambar berikut:

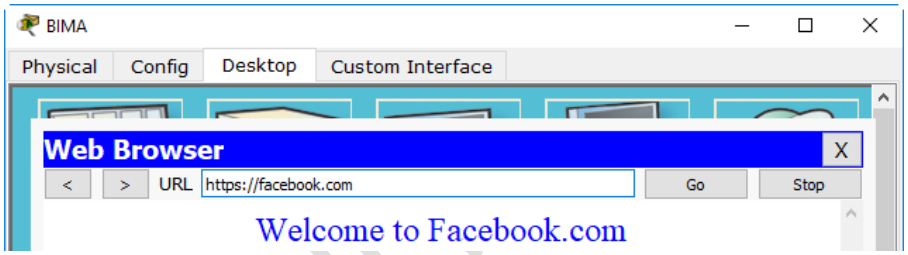


K. Memverifikasi dengan mengakses layanan HTTP, HTTPS dari **PC ARJUNA** dan **BIMA**. Hasil verifikasi terlihat seperti pada gambar berikut:

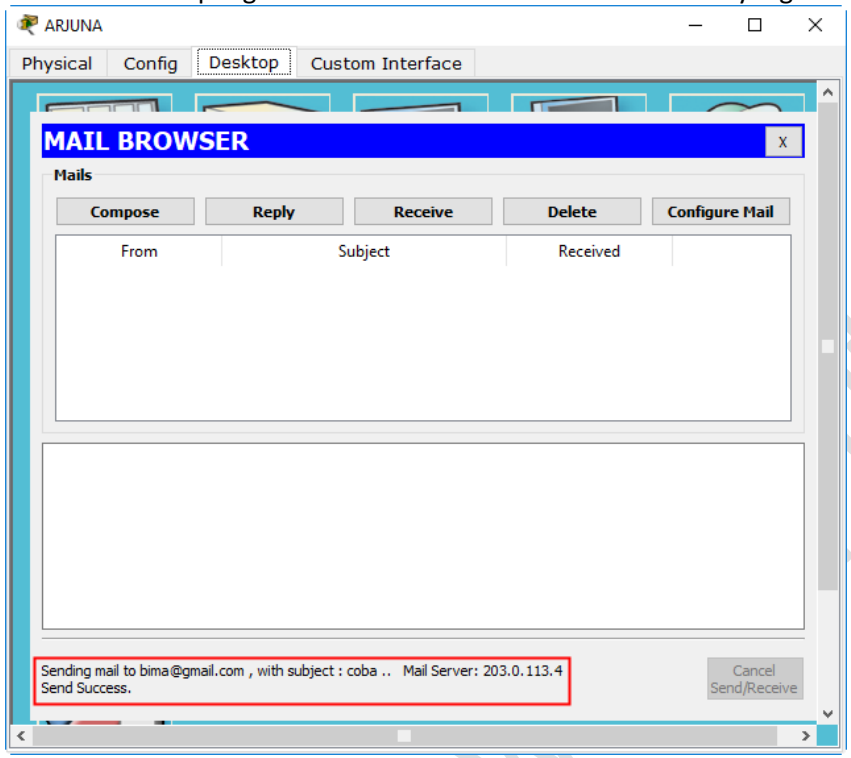




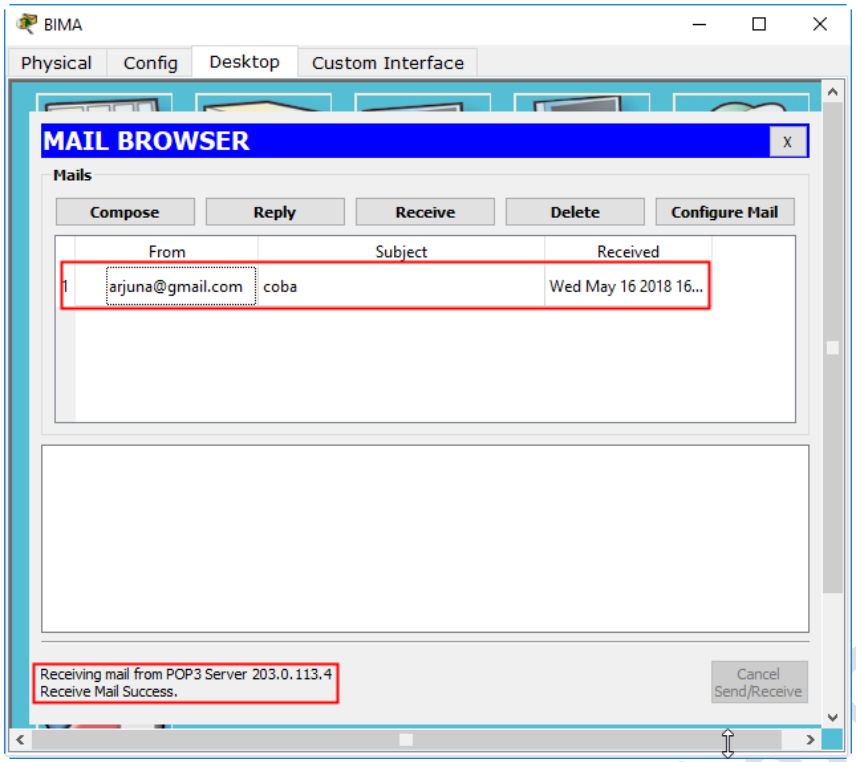




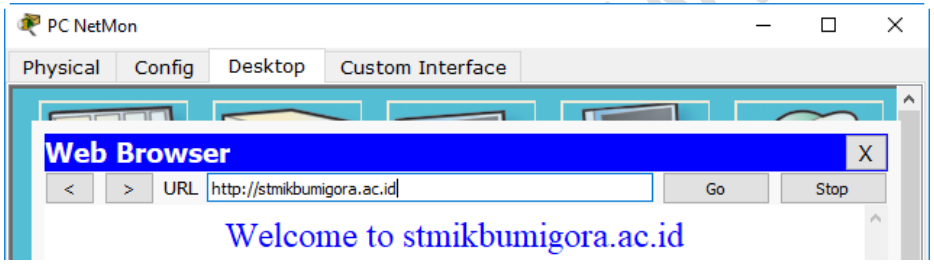
L. Memverifikasi pengiriman email melalui **Email Client** yang terdapat pada **PC ARJUNA** ke **bima@gmail.com**. Subject atau topik pesan email bebas.

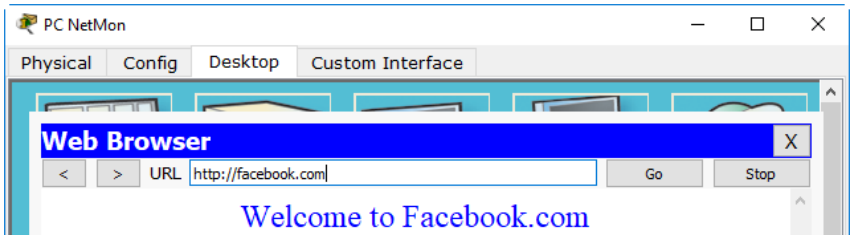


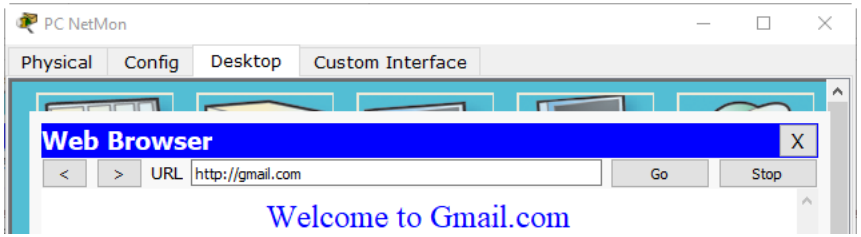
Terlihat email berhasil dikirim ke bima@gmail.com. Sedangkan **PC BIMA** dilakukan pengunduhan email dari **POP3 Server**, seperti terlihat pada gambar berikut:

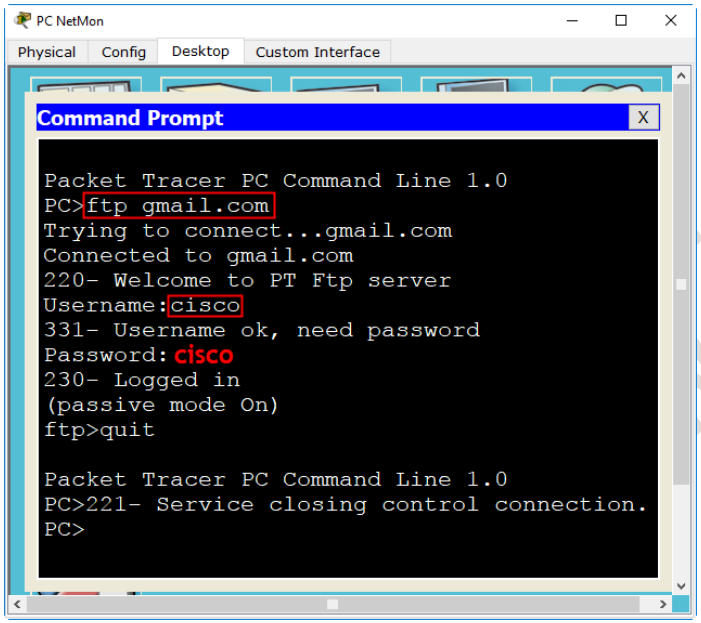


M. Memverifikasi melalui browser **PC NetMon** dengan mengakses layanan **HTTP/HTTPS** dari server yang terdapat di **subnet Internet** seperti **http://stmikbumigora.ac.id, http://facebook.com,** dan **http://gmail.com** serta memverifikasi akses ke layanan **FTP** pada *server Internet* melalui *command prompt.* Hasilnya terlihat seperti berikut:









N. Memverifikasi hasil translasi NAT

```
GW#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 203.0.113.9:1025   192.168.0.20:1025  203.0.113.1:53     203.0.113.1:53
udp 203.0.113.9:1026   192.168.0.20:1026  203.0.113.1:53     203.0.113.1:53
udp 203.0.113.9:1027   192.168.0.20:1027  203.0.113.1:53     203.0.113.1:53
udp 203.0.113.9:1028   192.168.0.20:1028  203.0.113.1:53     203.0.113.1:53
tcp 203.0.113.9:1024   192.168.0.67:1025  203.0.113.4:110    203.0.113.4:110
tcp 203.0.113.9:1025   192.168.0.66:1025  203.0.113.4:25     203.0.113.4:25
tcp 203.0.113.9:1026   192.168.0.34:1026  203.0.113.2:443    203.0.113.2:443
tcp 203.0.113.9:1026   192.168.0.34:1025  203.0.113.2:80     203.0.113.2:80
tcp 203.0.113.9:1027   192.168.0.34:1027  203.0.113.4:25     203.0.113.4:25
tcp 203.0.113.9:1028   192.168.0.35:1025  203.0.113.3:80     203.0.113.3:80
tcp 203.0.113.9:1029   192.168.0.35:1026  203.0.113.3:443    203.0.113.3:443
tcp 203.0.113.9:1030   192.168.0.35:1027  203.0.113.4:110    203.0.113.4:110
tcp 203.0.113.9:1031   192.168.0.20:1025  203.0.113.2:80     203.0.113.2:80
tcp 203.0.113.9:1032   192.168.0.20:1026  203.0.113.3:80     203.0.113.3:80
tcp 203.0.113.9:1033   192.168.0.20:1027  203.0.113.4:80     203.0.113.4:80
tcp 203.0.113.9:1034   192.168.0.20:1028  203.0.113.4:21     203.0.113.4:21
```

TUGAS 3

Konfigurasi **Static NAT** agar **mengijinkan Server Public DMZ dari PT. AR dengan alamat IP Private 192.168.0.1 ditranslasi ke alamat IP Publik 203.0.113.10** sehingga dapat diakses dari Internet.

Verifikasi hasil konfigurasi melalui *browser* **PC Client Internet** yang terdapat di **subnet Internet** dengan mengakses alamat **http://203.0.113.10** atau **http://anginribut.com**.

SOLUSI TUGAS 3

Berpindah ke mode global configuration

```
GW#conf t
```

Berpindah ke interface configuration untuk *GigabitEthernet0/1*

```
GW(config)#int gi0/1
```

Mengatur NAT inside

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

Berpindah ke satu mode sebelumnya

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

Mengatur **static NAT** untuk mentranslasi alamat **IP Private** dari **Server Public DMZ** yaitu **192.168.0.1** menjadi **203.0.113.10**

```
GW(config)#ip nat inside source static 192.168.0.1 203.0.113.10
```

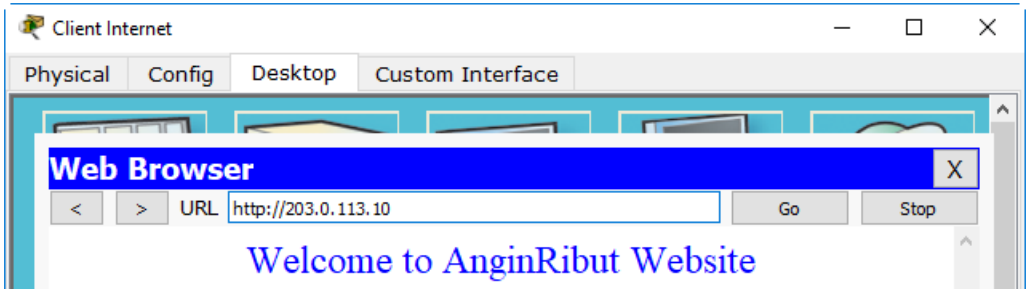
Berpindah ke mode privilege

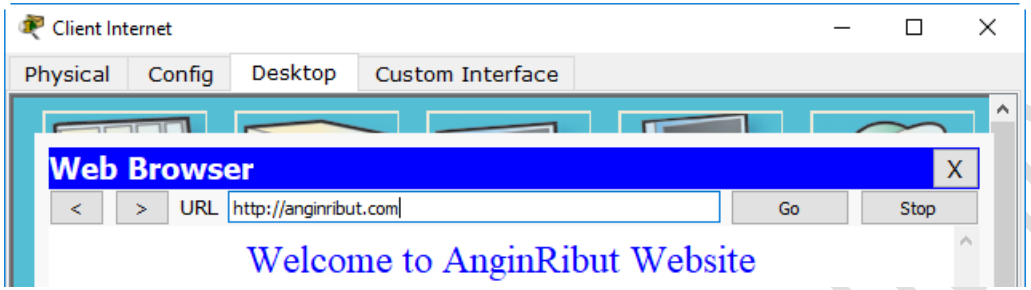
```
GW(config)#end
```

Memverifikasi hasil translasi NAT

```
GW#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  203.0.113.10      192.168.0.1        ---                ---
tcp 203.0.113.9:1024   192.168.0.67:1025  203.0.113.4:110    203.0.113.4:110
tcp 203.0.113.9:1025   192.168.0.66:1025  203.0.113.4:25     203.0.113.4:25
tcp 203.0.113.9:1026   192.168.0.34:1026  203.0.113.2:443    203.0.113.2:443
tcp 203.0.113.9:1026   192.168.0.34:1025  203.0.113.2:80     203.0.113.2:80
tcp 203.0.113.9:1027   192.168.0.34:1027  203.0.113.4:25     203.0.113.4:25
tcp 203.0.113.9:1028   192.168.0.35:1025  203.0.113.3:80     203.0.113.3:80
tcp 203.0.113.9:1029   192.168.0.35:1026  203.0.113.3:443    203.0.113.3:443
tcp 203.0.113.9:1030   192.168.0.35:1027  203.0.113.4:110    203.0.113.4:110
tcp 203.0.113.9:1031   192.168.0.20:1025  203.0.113.2:80     203.0.113.2:80
tcp 203.0.113.9:1032   192.168.0.20:1026  203.0.113.3:80     203.0.113.3:80
tcp 203.0.113.9:1033   192.168.0.20:1027  203.0.113.4:80     203.0.113.4:80
tcp 203.0.113.9:1034   192.168.0.20:1028  203.0.113.4:21     203.0.113.4:21
```

Memverifikasi hasil konfigurasi static NAT melalui browser PC Client Internet yang terdapat pada subnet Internet dengan mengakses alamat http://203.0.113.10 dan http://anginribut.com.





Terlihat layanan **HTTP** pada **Server Public DMZ** dapat diakses baik menggunakan alamat IP maupun nama domain **anginribut.com**.

TUGAS 4

Konfigurasi ACL pada seluruh router **(R1, CORE, R2** dan **GW)** di jaringan internal PT. AR agar **hanya mengijinkan akses telnet dari PC NetMon (Network Monitoring)** yang terdapat di **subnet Server Farm**.

ACL ditulis menggunakan *Numbered Access Control List (ACL)* dengan ketentuan yaitu menggunakan nomor ACL **pertama** dari rentang yang diijinkan pada **ACL Standard** atau **ACL Extended**.

SOLUSI TUGAS 4

A. Konfigurasi ACL untuk mengijinkan telnet ke **router R1** hanya dari **PC NetMon (Network Monitoring)** melalui **Terminal PC NAKULA**.

Berpindah ke mode global configuration

```
R1# conf t
```

Membuat Standard ACL untuk mengijinkan PC NetMon

```
R1(config)# access-list 1 permit 192.168.0.20
```

Berpindah ke line configuration

```
R1(config)# line vty 0 4
```

Menerapkan ACL yang telah dibuat

```
R1(config)# access-class 1 in
```

Berpindah ke privilege mode

```
R1(config)# end
```

Menampilkan informasi ACL yang terdapat pada router R1

```
R1#show access-list
Standard IP access list 1
    10 permit host 192.168.0.20
```

Memverifikasi hasil penerapan ACL pada line vty

```
R1# show run
```

….

```
line vty 0 4
 access-class 1 in
 password sanjose
 login
!
```

B. Konfigurasi ACL untuk mengijinkan telnet ke **router CORE** hanya dari **PC NetMon (Network Monitoring)** melalui **Terminal PC SADEWA**.

Berpindah ke mode global configuration

```
CORE# conf t
```

Membuat Standard ACL untuk mengijinkan PC NetMon

```
CORE (config)# access-list 1 permit 192.168.0.20
```

Berpindah ke line configuration

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

Menerapkan ACL yang telah dibuat

```
CORE(config)# access-class 1 in
```

Berpindah ke privilege mode

```
CORE(config)# end
```

Menampilkan informasi ACL yang terdapat pada router CORE

```
CORE#show access-list
Standard IP access list 1
    10 permit host 192.168.0.20
```

Memverifikasi hasil penerapan ACL pada line vty

```
CORE# show run
```

….

```
line vty 0 4
 access-class 1 in
 password sanjose
 login
!
```

C. Konfigurasi ACL untuk mengijinkan telnet ke **router R2** hanya dari **PC NetMon (Network Monitoring)** melalui **Terminal PC BIMA**.

Berpindah ke mode global configuration

```
R2# conf t
```

Membuat Standard ACL untuk mengijinkan PC NetMon

```
R2(config)# access-list 1 permit 192.168.0.20
```

Berpindah ke line configuration

```
R2(config)# line vty 0 4
```

Menerapkan ACL yang telah dibuat

```
R2(config)# access-class 1 in
```

Berpindah ke privilege mode

```
R2(config)# end
```

Menampilkan informasi ACL yang terdapat pada router R2

```
R2#show access-list
Standard IP access list 1
    10 permit host 192.168.0.20
```

Memverifikasi hasil penerapan ACL pada line vty

```
R2# show run
```

….

```
line vty 0 4
 access-class 1 in
 password sanjose
 login
!
```

D. Konfigurasi ACL untuk mengijinkan telnet ke **router GW** hanya dari **PC NetMon (Network Monitoring)** melalui **Terminal PC NetMon**.

Berpindah ke mode global configuration

```
GW# conf t
```

Membuat Standard ACL untuk mengijinkan PC NetMon

```
GW(config)# access-list 1 permit 192.168.0.20
```

Berpindah ke line configuration

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

Menerapkan ACL yang telah dibuat

```
GW(config)# access-class 1 in
```

Berpindah ke privilege mode

```
GW(config)# end
```

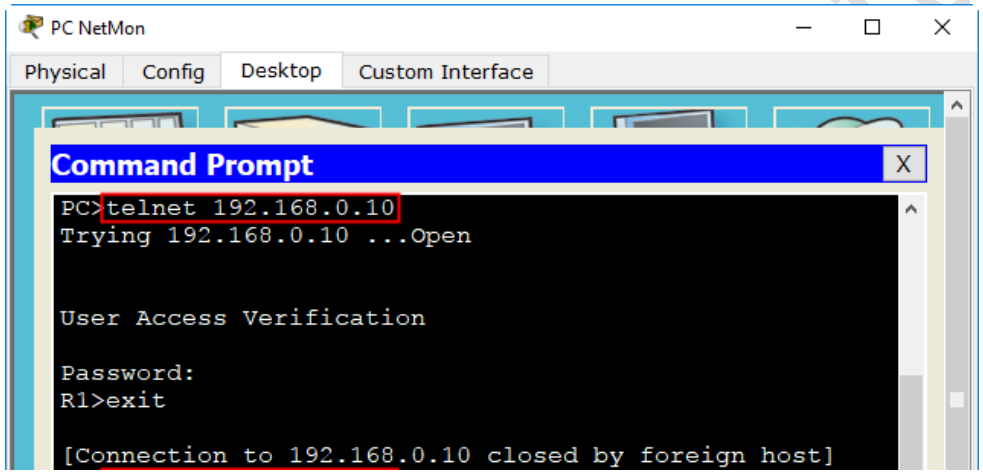
Menampilkan informasi ACL yang terdapat pada router GW

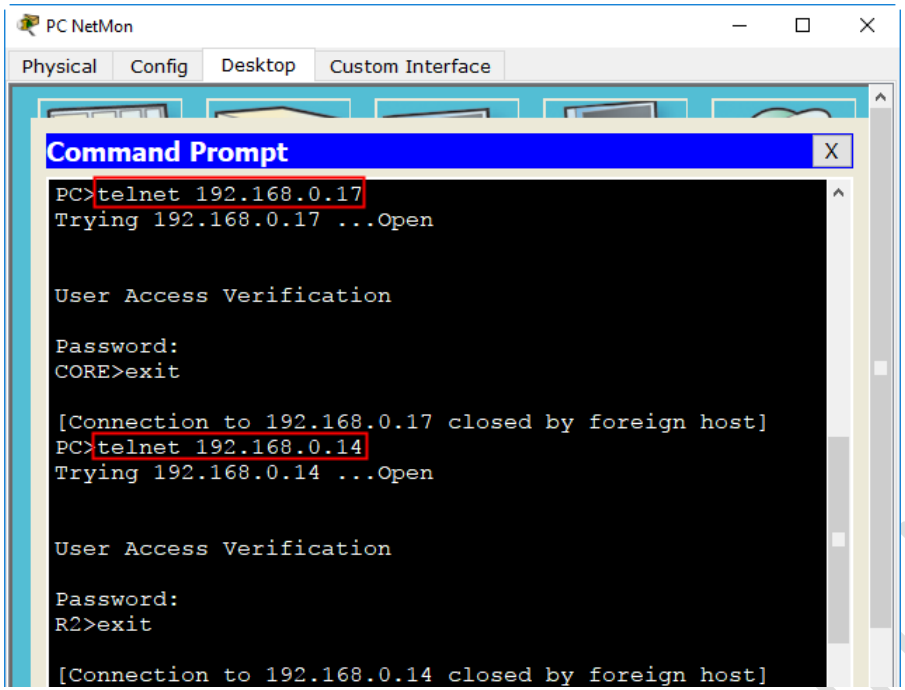
```
GW#show access-list
Extended IP access list 199
    10 permit tcp 192.168.0.64 0.0.0.15 host 203.0.113.4 eq smtp (2 match(es))
    20 permit tcp 192.168.0.64 0.0.0.15 host 203.0.113.4 eq pop3 (2 match(es))
    30 permit ip 192.168.0.32 0.0.0.31 any (20 match(es))
    40 permit ip host 192.168.0.20 any (16 match(es))
Standard IP access list 1
    10 permit host 192.168.0.20
```

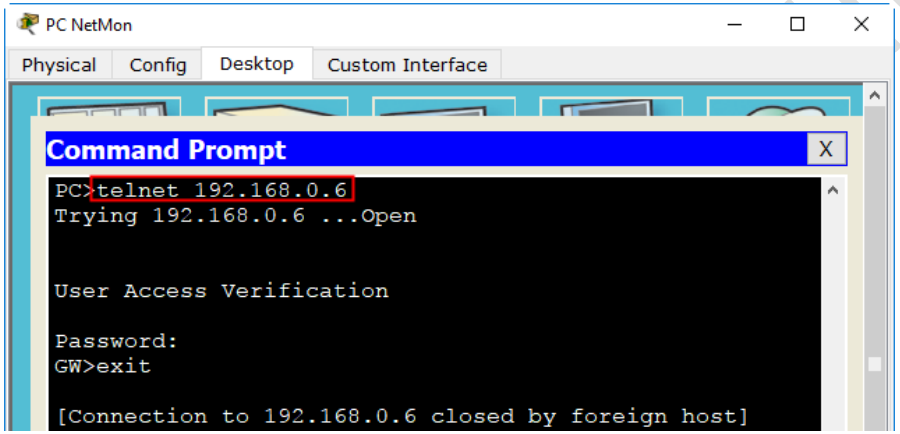
Memverifikasi hasil penerapan ACL pada line vty

```
GW# show run

….

line vty 0 4
 access-class 1 in
 password sanjose
 login
!
```

E. Verifikasi akses telnet dari **PC NetMon** yang terdapat di **subnet Server Farm** ke **router R1, CORE, R2** dan **router GW**







Pastikan akses telnet dari **PC NetMon** ke **router R1, CORE, R2** dan **GW** berhasil dilakukan. Sebaliknya selain dari **PC NetMon** tertolak aksesnya.

TUGAS 5

Konfigurasi ACL dengan ketentuan sebagai berikut (Point: 24):

a. Seluruh host baik di subnet **KEUANGAN** maupun **SALES** dapat mengakses layanan **HTTP** dan **HTTPS** pada **Server Web Intranet** yang berada di **subnet Server Farm**. Verifikasi akses **HTTP** dan **HTTPS** menggunakan *browser* dari host-host di subnet **KEUANGAN** dan **SALES**.
b. Hanya mengijinkan seluruh host di **subnet SALES** yang dapat mengakses layanan **FTP Server Intranet**. Verifikasi akses FTP melalui *command prompt* dari host-host yang terdapat di **subnet SALES**. *Username* dan *password* untuk login ke **FTP Server Intranet** adalah **cisco**.

ACL ditulis menggunakan *Numbered Access Control List (ACL)* dengan ketentuan:

- Apabila menggunakan **ACL Standard** maka gunakan nomor ACL **50**.
- Apabila menggunakan **ACL Extended** maka gunakan nomor ACL **150**.

PERHATIAN:

Verifikasi kembali hasil konfigurasi sebagai penyelesaian tugas 1-5 tetap bekerja atau berjalan dengan baik melalui host yang sesuai dengan kebijakan yang telah ditentukan.

SOLUSI TUGAS 5

A. Mengkonfigurasi **Extended ACL** pada **router CORE** melalui **Terminal** dari **PC SADEWA**.

Berpindah ke mode global configuration

```
CORE# conf t
```

Membuat *Extended ACL* untuk mengijinkan akses layanan **HTTP (tcp/80)** dan **HTTPS (tcp/443)** dari **subnet KEUANGAN 192.168.0.64/28** ke **Server Web Intranet** 192.168.0.18 yang terdapat di **subnet Server Farm**

```
CORE(config)# access-list 150 permit tcp 192.168.0.64 0.0.0.15 192.168.0.18 0.0.0.0 eq 80
CORE(config)# access-list 150 permit tcp 192.168.0.64 0.0.0.15 192.168.0.18 0.0.0.0 eq 443
```

Membuat *Extended ACL* untuk mengijinkan akses layanan **HTTP (tcp/80)** dan **HTTPS (tcp/443)** dari **subnet SALES 192.168.0.32/27** ke **Server Web Intranet 192.168.0.18** yang terdapat di **subnet Server Farm.**

```
CORE(config)# access-list 150 permit tcp 192.168.0.32 0.0.0.31 192.168.0.18 0.0.0.0 eq 80
CORE(config)# access-list 150 permit tcp 192.168.0.32 0.0.0.31 192.168.0.18 0.0.0.0 eq 443
```

Membuat *Extended ACL* untuk mengijinkan akses layanan **FTP** dari **subnet SALES 192.168.0.32/27** ke **FTP Server Intranet 192.168.0.19** yang terdapat di **subnet Server Farm.**

```
CORE(config)# access-list 150 permit tcp 192.168.0.32 0.0.0.31 192.168.0.19 0.0.0.0 range 20 21
```

Membuat *Extended ACL* untuk mengijinkan koneksi dari alamat IP sumber berapapun ke alamat **subnet Server Farm 192.168.0.16/29** dengan port lebih besar **(greater than - gt)** dari 1023.

```
CORE(config)# access-list 150 permit tcp 0.0.0.0 255.255.255.255 192.168.0.16 0.0.0.7 gt 1023
```

Membuat *Extended ACL* untuk mengijinkan balasan *DNS query* dari **Server DNS 203.0.113.1** port **53** dengan tujuan ke alamat IP dari **PC NetMon (Network Monitoring) 192.168.0.20.** Pada awalnya permintaan *DNS query* dikirimkan dari *PC NetMon* ke *Server DNS* sehingga akses Internet dengan nama domain dapat dilakukan.

```
CORE(config)# access-list 150 permit udp 203.0.113.1 0.0.0.0 eq 53 192.168.0.20 0.0.0.0
```

Membuat *Extended ACL* untuk mengijinkan protokol **ICMP** yang digunakan oleh **ping** ketika verifikasi koneksi antar host dari alamat IP sumber berapapun ke alamat subnet dari **subnet Server Farm** yaitu **192.168.0.16/29**.

```
CORE(config)# access-list 150 permit icmp 0.0.0.0 255.255.255.255 192.168.0.16 0.0.0.7
```

Berpindah ke interface configuration

```
CORE(config)# int vlan 1
```

Menerapkan ACL yang telah dibuat

```
CORE(config-if)# ip access-group 150 in
```

Berpindah ke mode privilege

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

B. Menampilkan informasi ACL yang terdapat pada **router CORE**

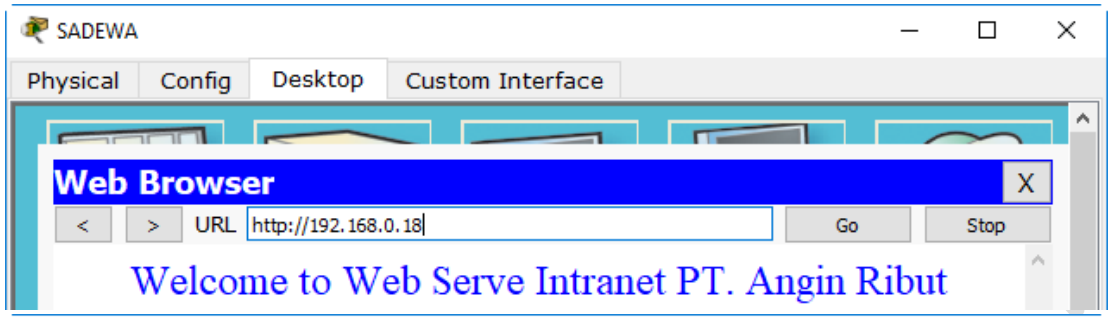
```
CORE#show access-list
Standard IP access list 1
    10 permit host 192.168.0.20
Extended IP access list 150
    10 permit tcp 192.168.0.64 0.0.0.15 host 192.168.0.18 eq www
    20 permit tcp 192.168.0.64 0.0.0.15 host 192.168.0.18 eq 443
    30 permit tcp 192.168.0.32 0.0.0.31 host 192.168.0.18 eq www
    40 permit tcp 192.168.0.32 0.0.0.31 host 192.168.0.18 eq 443
    50 permit tcp 192.168.0.32 0.0.0.31 host 192.168.0.19 range 20 ftp
    60 permit tcp any 192.168.0.16 0.0.0.7 gt 1023
    70 permit udp host 203.0.113.1 eq domain host 192.168.0.20
    80 permit icmp any 192.168.0.16 0.0.0.7
```

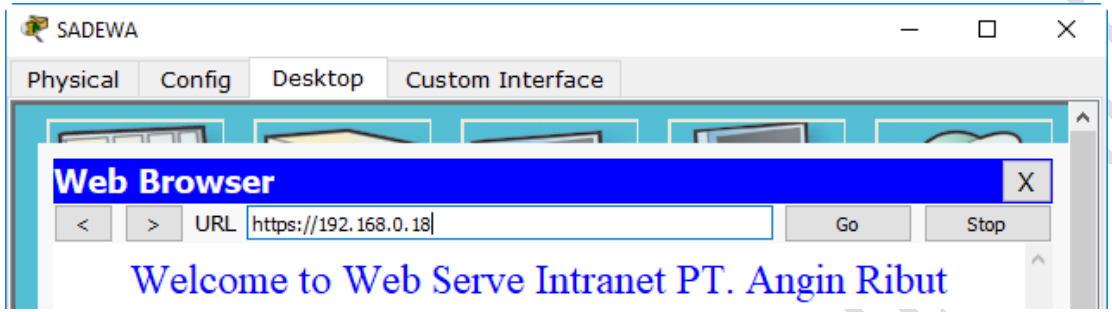
Terlihat ACL dengan nomor 150 telah terbuat

C. Memverifikasi penerapan ACL pada **interface vlan 1**

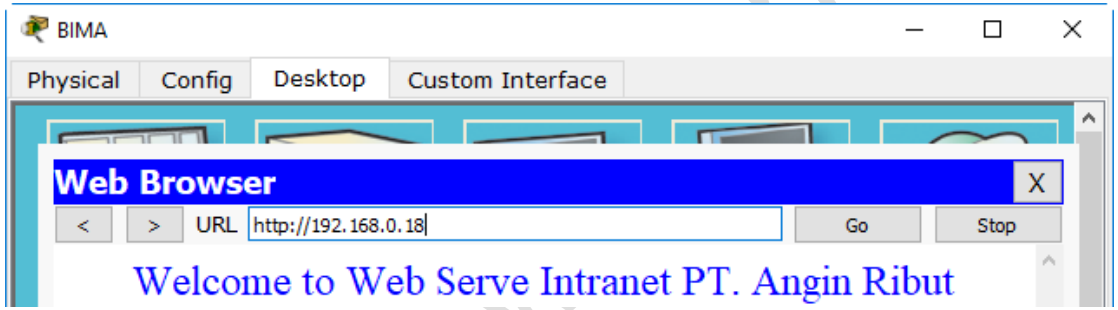
```
CORE# show run
!
interface Vlan1
 ip address 192.168.0.17 255.255.255.248
 ip access-group 150 out
!
```

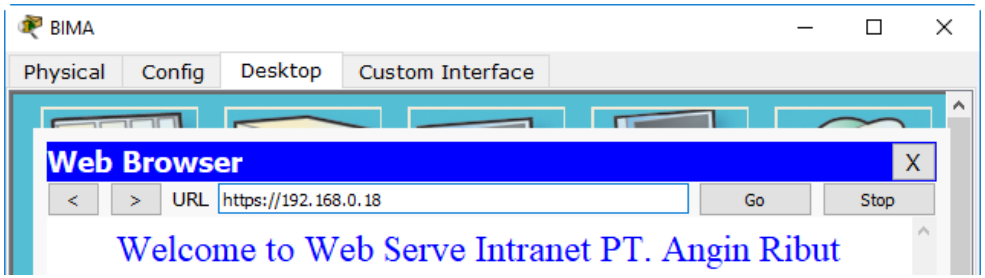
D. Memverifikasi akses **HTTP** dan **HTTPS** ke **Server Web Intranet 192.168.0.18** menggunakan *browser* dari salah satu PC yang terdapat di **subnet KEUANGAN** sebagai contoh **PC SADEWA**.



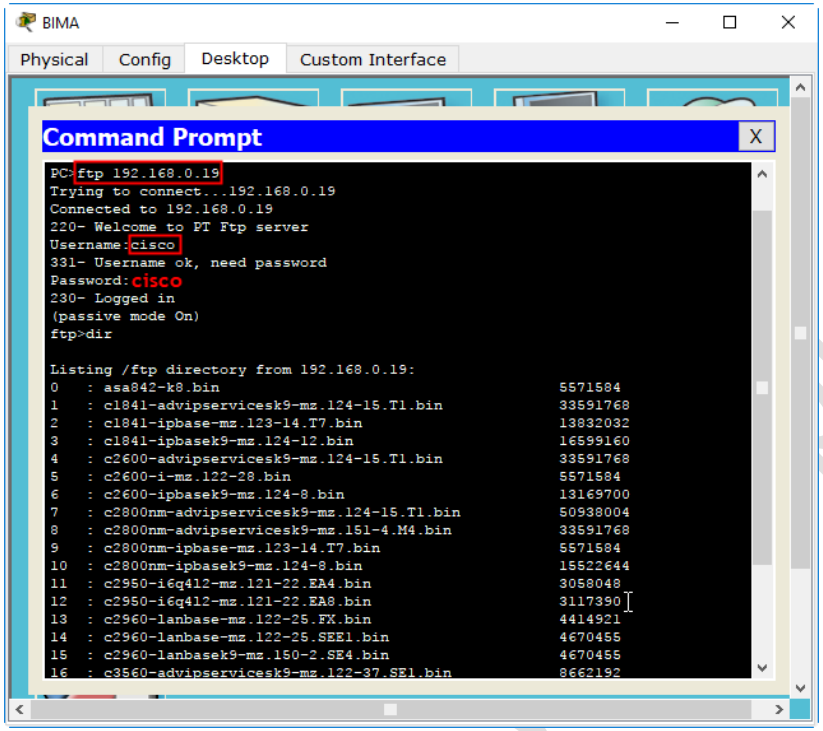


E. Memverifikasi akses **HTTP** dan **HTTPS** ke **Server Web Intranet 192.168.0.18** menggunakan browser dari salah satu PC yang terdapat di **subnet SALES** sebagai contoh **PC BIMA**.





F. Memverifikasi akses **FTP** ke **FTP Server Intranet 192.168.0.19** melalui command prompt dari salah satu PC yang terdapat di **subnet SALES** sebagai contoh **PC BIMA**. *Username* dan *password* untuk login ke **FTP Server Intranet** adalah **cisco**.



Selamat Anda telah berhasil menyelesaikan pembahasan solusi soal UTS Praktikum Sistem Keamanan Jaringan (SKJ) untuk semester genap tahun akademik 2017/2018. Apabila terdapat pertanyaan, jangan segan untuk bertanya dengan mengirimkan melalui email di **admin@iputuhariyadi.net**. Semoga bermanfaat. Terimakasih.