FR.IA.02. TUGAS PRAKTIK DEMONSTRASI

Skema Sertifikasi (KKNI/Okupasi/Klaster)	Judul	:	Network Administrator
	Nomor	:	FR.SKEMA-02
TUK		:	~~Sewaktu/Tempat Kerja/~~Mandiri*
Nama Asesor		:	Anop Sudiatmika
Nama Asesi		:	VINCENT ALFIAN ARTHA
Tanggal		:	5/17/2025

Lengkapi ketentuan berikut (siapkan jawaban: srenshoot jawaban praktek, penjelasan detail)

J.611000.003.02 Merancang Topologi Jaringan

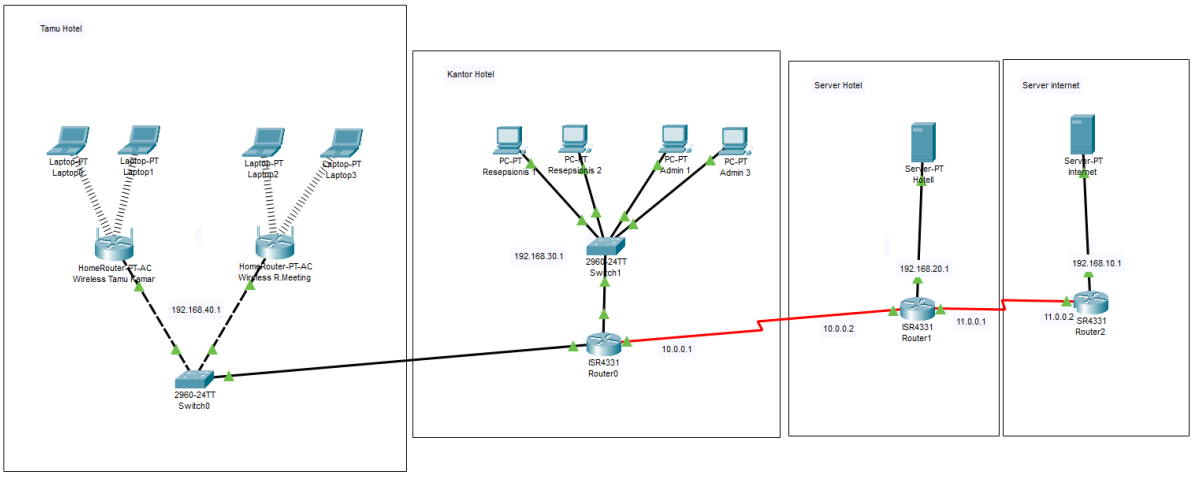
1. Tentukan spesifikasi perangkat dengan melihat Kebutuhan penggguna sesuai ruang lingkup diatas

Jawaban :

- Router: 3 unit (Router 0, Router 1, Router 2)
- Switch: 2 unit (Switch 0, Switch 1)
- Access Point: 2 unit (HomeRouter-PT-AC Wireless Tamu Kamar dan HomeRouter-PT-AC Wireless R.Meeting)
- PC: 4 unit (PC Resepsionis 1, PC Resepsionis 2,PC Admin 1, PC Admin 2)
- Laptop: 4 unit (Laptop 0, Laptop 1, Laptop 2, Laptop 3)
- Kabel: Copper Straight-Through, Copper Cross-Over, Serial DCE
- IP Address sesuai skenario jaringan hotel
- Bandwidth konfigurasi sesuai skenario

2. Gambarkan spesifikasi topologi jaringan sesuai kebutuhan diatas

Jawaban :



- Router 0 terhubung ke Switch 0 untuk jaringan kantor hotel dan tamu hotel (192.168.40.0/24)
- Router 2 terhubung ke Server Internet (192.168.10.0/24)
- Router 1 terhubung ke Server Hotell (192.168.20.0/24)
- Wireless Tamu Kamar dan R.Meeting terhubung ke Switch 0 melalui kabel Copper Cross-Over
- VLAN dan subnetting untuk memisahkan jaringan internal dan tamu

3. Berapakah estimasi biaya untuk kebutuhan diatas

Jawaban :

- Router Cisco ISR 4321: 3 x Rp. 10.000.000 = Rp. 30.000.000
- Pc Resepsionis 2 x Rp. 10.000.000 = Rp. 20.000.000
- Pc Admin 2 x Rp. 10.000.000 = Rp. 20.000.000
- Switch 2960-24TT: 2 x Rp. 5.000.000 = Rp. 10.000.000
- Access Point: 2 x Rp. 2.000.000 = Rp. 4.000.000
- Server 2x Rp.5.000.000 = Rp. 10.000.000
- Kabel, patch panel, dan konektor: Rp. 2.000.000
- Total estimasi biaya: Rp. 96.000.000

J.611000.006.01 Merancang Keamanan Jaringan

1. Identifikasi dan analisis risiko keamanan jaringan yang berjalan

Jawaban :

- Serangan dari pengguna tamu ke server internal
- Intercept dan sniffing data dari jaringan tamu
- Flooding dan DoS attack dari pengguna tidak terotorisasi
- Misconfiguration pada firewall dan ACL

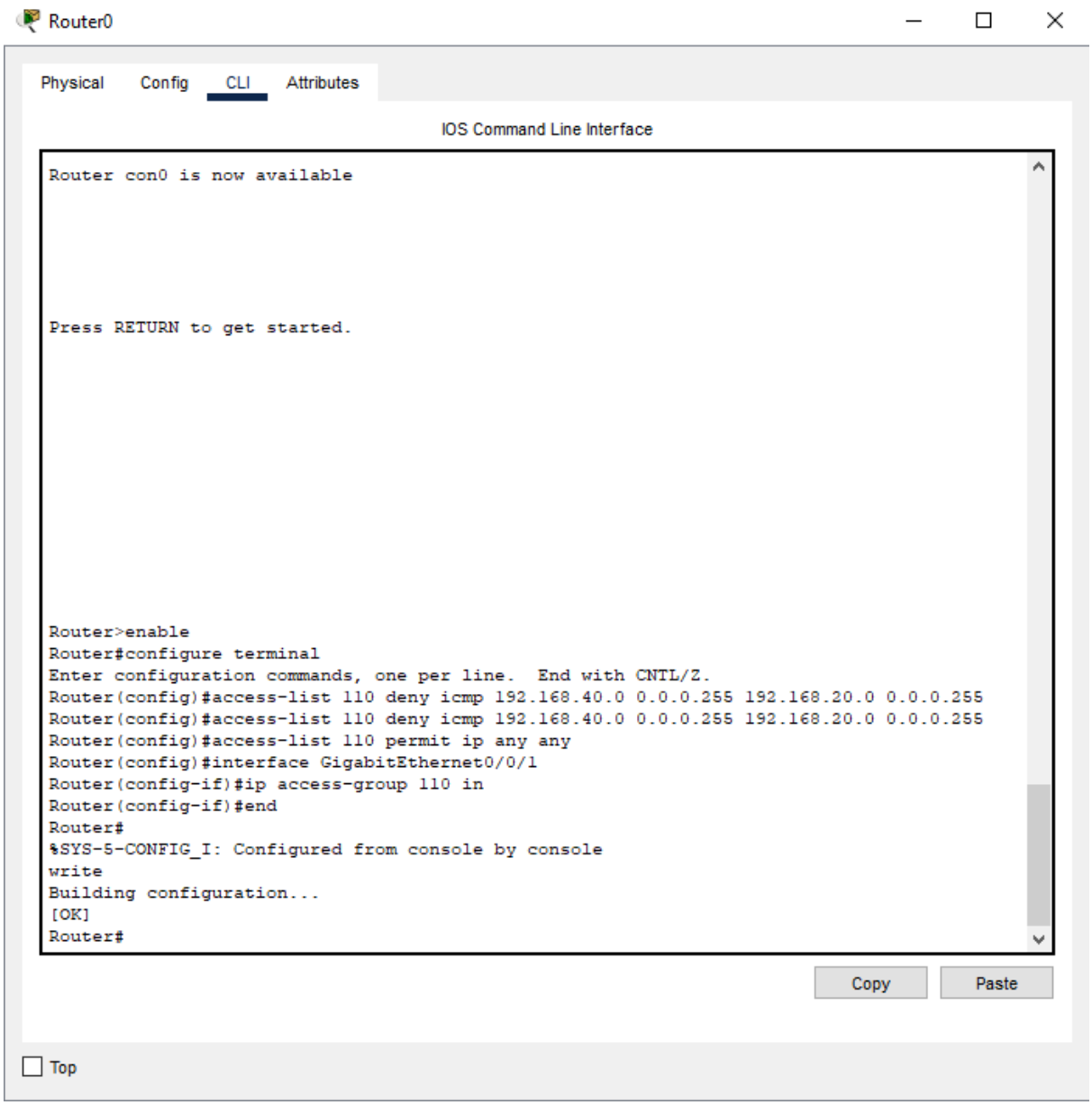
Berikut adalah Konfigirasi ACL (Access Control List) di Router 0

2. Buat rancangan keamanan jaringan berdasarkan skala prioritas

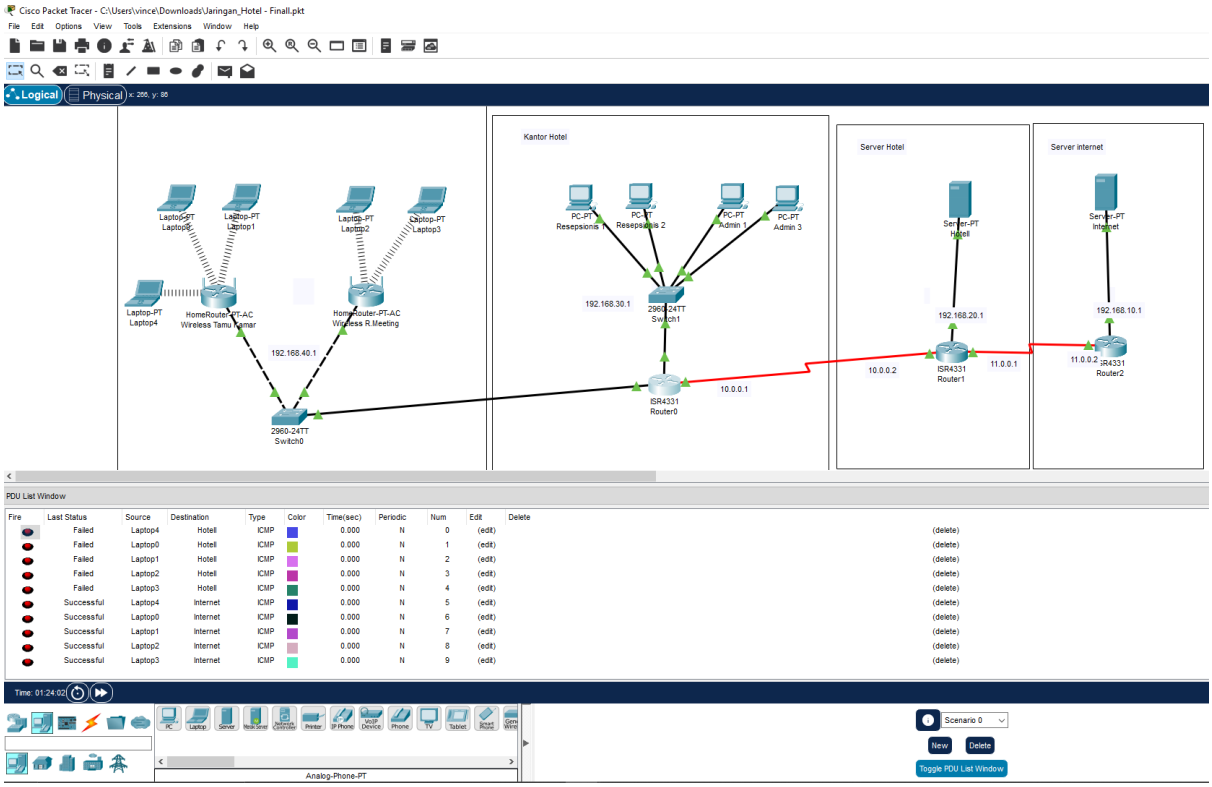
Jawaban :

- Menggunakan Access Control List (ACL) untuk memisahkan lalu lintas jaringan internal dan tamu

Berikut adalah Konfigirasi ACL (Access Control List) di Router 0



Berikut adalah hasil Mencoba melakukan ping Keserver Hotel dan Server Internet



1. Langkah-langkah Konfigurasi ACL
2. enable
3. configure terminal

   access-list 110 deny icmp 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
4. access-list 110 permit ip any any
5. interface GigabitEthernet0/0/1
6. ip access-group 110 in
7. end
8. write

- Menggunakan enkripsi WPA2-PSK untuk jaringan Wi-Fi

J.611000.014.02 Mengkonfigurasi routing pada perangkat jaringan antar autonomous system

1. Konfigurasi router, switch , PC sesuai skenario alamat IP nya

Jawaban :

- Router 0 (Gateway 192.168.40.1) untuk jaringan tamu hotel
- Router 0 (Gateway 192.168.30.1) untuk Pc Resepsionis dan Pc Admin

  Routing RIP pada Router 0:
  - 10.0.0.0

- 11.0.0.0
- 192.168.10.0 subnet (255.255.255.0)
- 192.168.20.0 subnet (255.255.255.0)
- 192.168.30.0 subnet (255.255.255.0)
- 192.168.40.0 subnet (255.255.255.0)

Serial 0/1/0

- 10.0.0.1 subnet (255.0.0.0)

- Router 1 (Gateway 192.168.20.1) untuk server hotel

  Routing RIP pada Router 1

  - 10.0.0.0
  - 11.0.0.0
  - 192.168.10.0 subnet (255.255.255.0)
  - 192.168.20.0 subnet (255.255.255.0)
  - 192.168.30.0 subnet (255.255.255.0)
  - 192.168.40.0 subnet (255.255.255.0)

  Serial 0/1/0

  - 11.0.0.1 subnet (255.0.0.0)

  Serial 0/1/1

  - 10.0.0.2 subnet (255.0.0.0)
- Router 2 (Gateway 192.168.10.1) untuk server internet

  Routing RIP pada Router 2

  - 10.0.0.0
  - 11.0.0.0
  - 192.168.10.0 subnet (255.255.255.0)
  - 192.168.20.0 subnet (255.255.255.0)
  - 192.168.30.0 subnet (255.255.255.0)
  - 192.168.40.0 subnet (255.255.255.0)

  Serial 0/1/0

  - 11.0.0.2 subnet (255.0.0.0)
- Konfigurasi DHCP untuk wireless tamu kamar dan R.Meeting
- Menambahkan RIP route untuk memastikan koneksi ke server hotel dan server internet

- Ipv4 PC Resepsionis 1 (192.168.30.2) dan Resepsionis 2 (192.168.30.3)
- Ipv4 PC Admin 1 (192.168.30.4) dan Admin 2 (192.168.30.5)
- Mengatur Gateaway pada setiap PC dengan default gateaway 192.168.30.1

2. Pastikan terkoneksi dengan menguji koneksi tiap perangkat tersebut

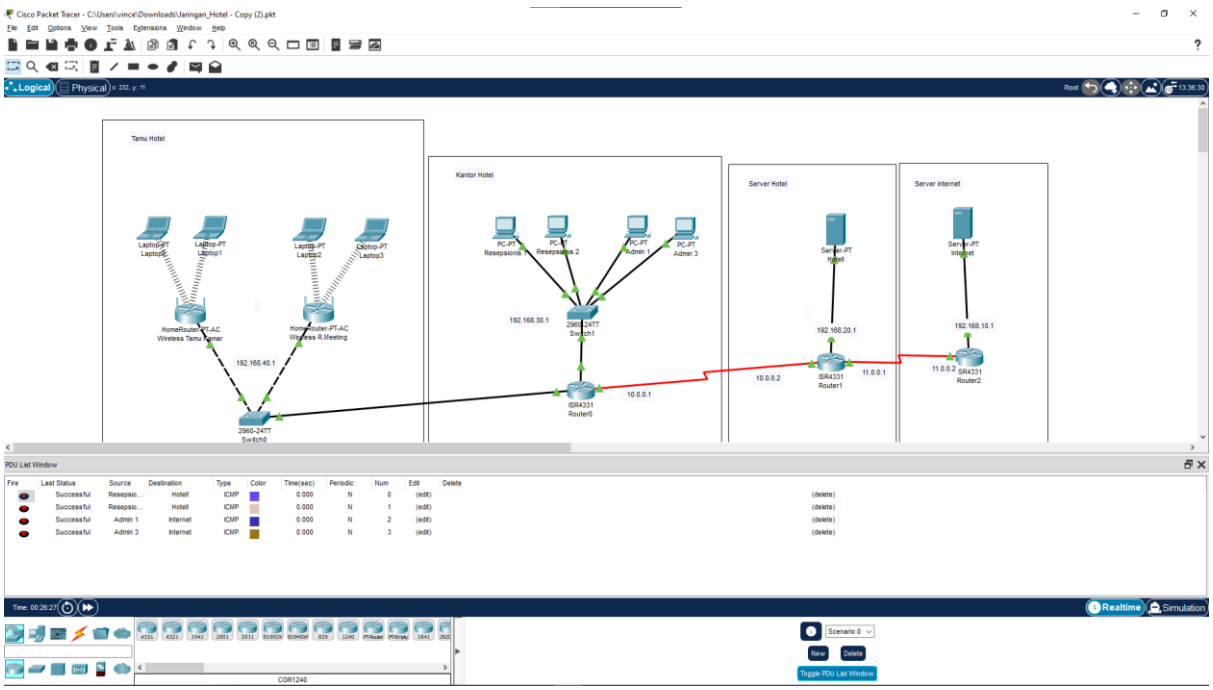
Jawaban :

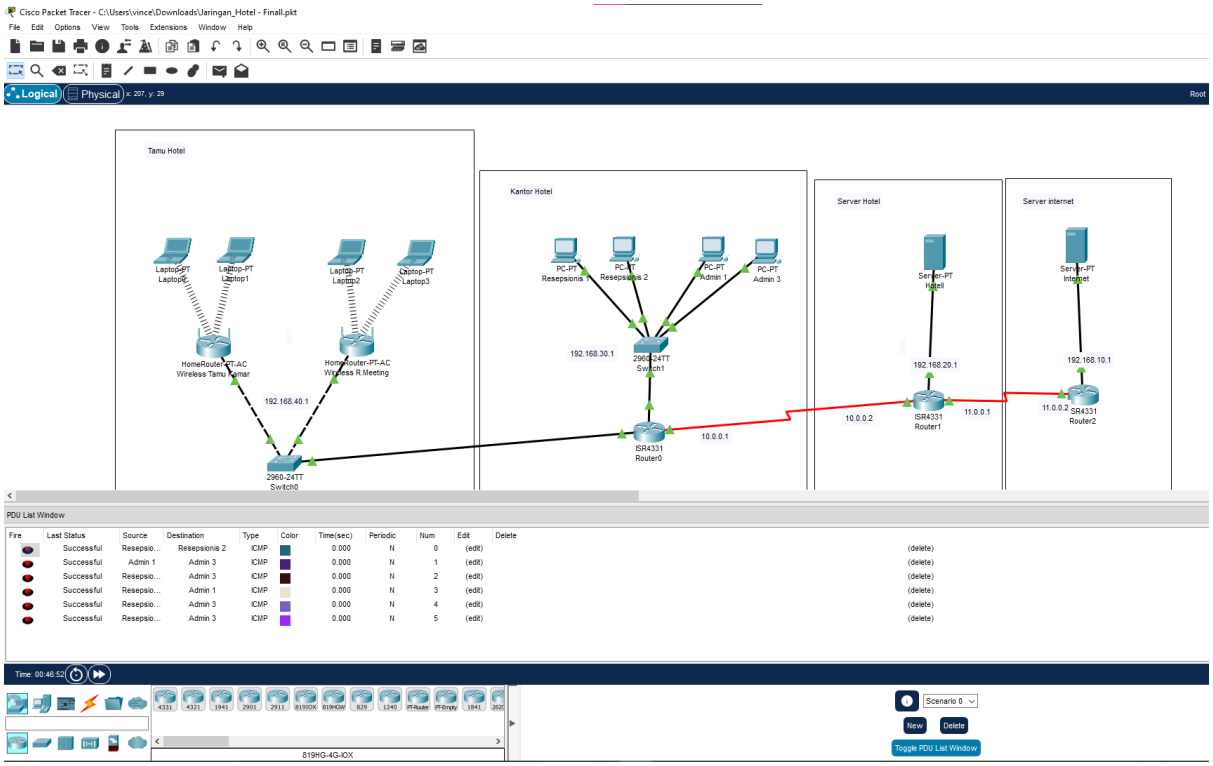
- Menggunakan perintah "ping" dari setiap perangkat untuk memastikan konektivitas

- Memeriksa tabel routing menggunakan "show ip route" pada setiap router

3. Dokumentasikan final gambar desain dan hasil uji koneksi , sampling 2 PC dari kelas yang berbeda

Jawaban :

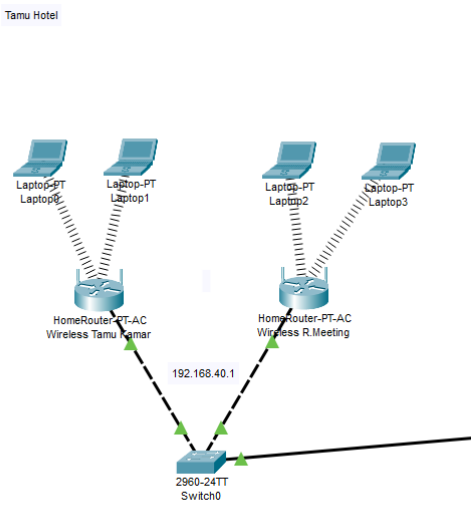




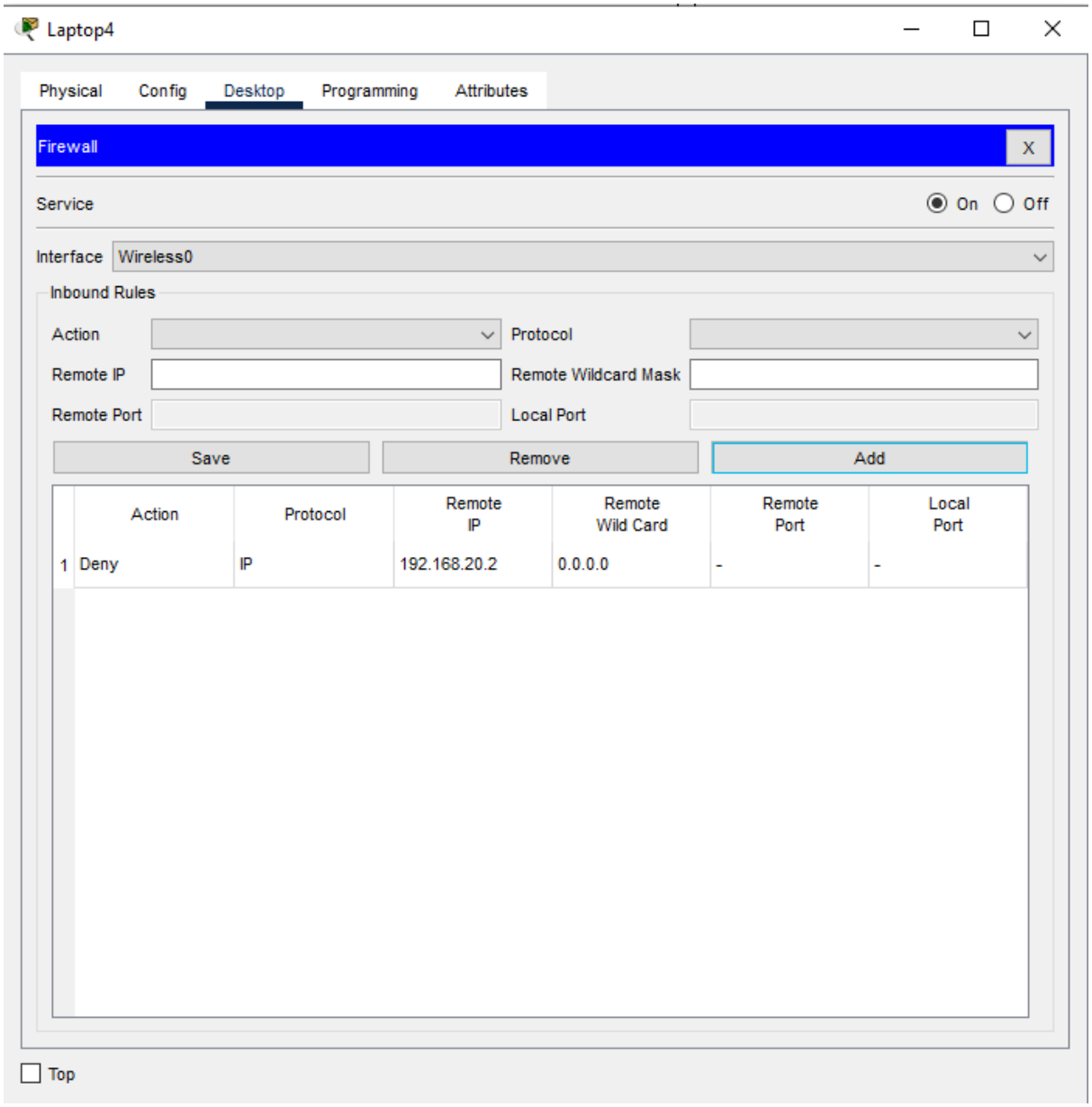
J.611000.015.02 Memonitor Keamanan dan Pengaturan Akun Pengguna dalam Jaringan Komputer

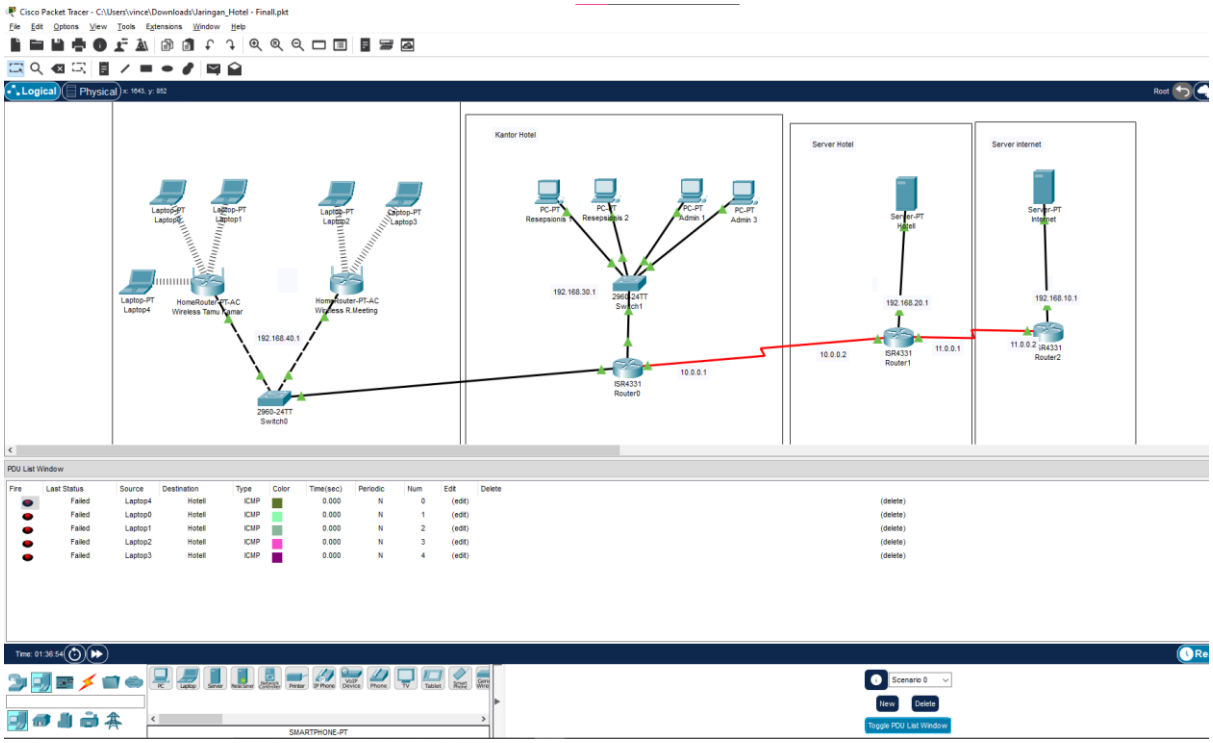
1. Konfigurasi switch, laptop sesuai skenario alamat IP nya

Jawaban :



Berikut adalah Konfigurasi Firewall pada Laptop memblokir koneksi ke Server Hotel.



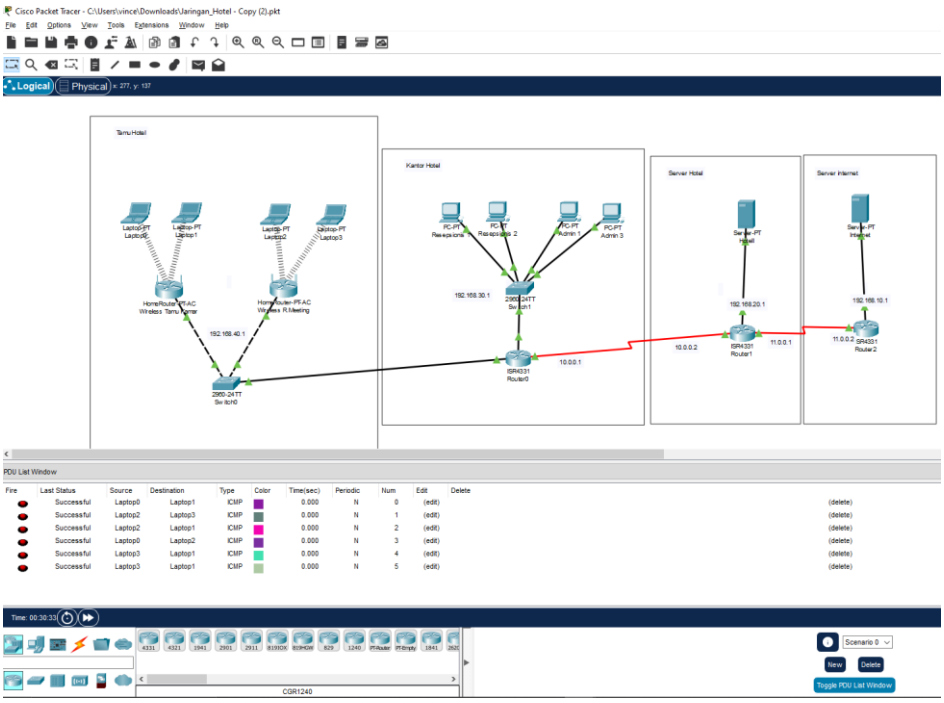


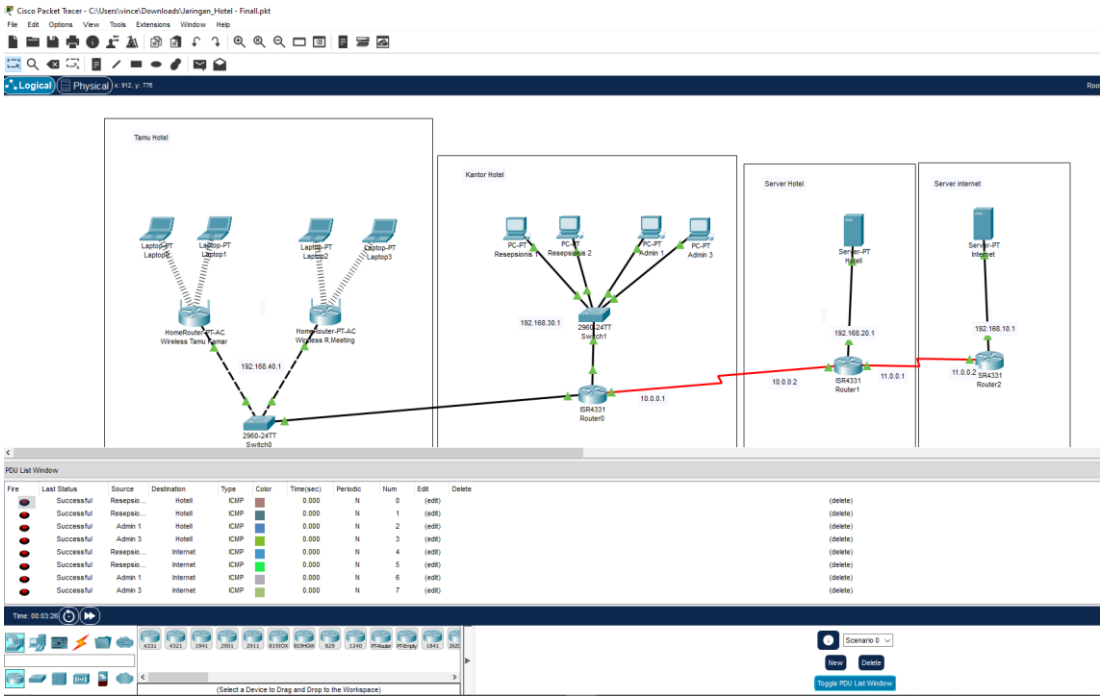
- Menggunakan kabel Copper Cross-Over untuk menghubungkan HomeRouter ke Switch 0
- Mengatur IP address dan DHCP pada setiap perangkat

2. Pastikan terkoneksi dengan menguji koneksi tiap perangkat tersebut

Jawaban :

Verifikasi koneksi menggunakan ping

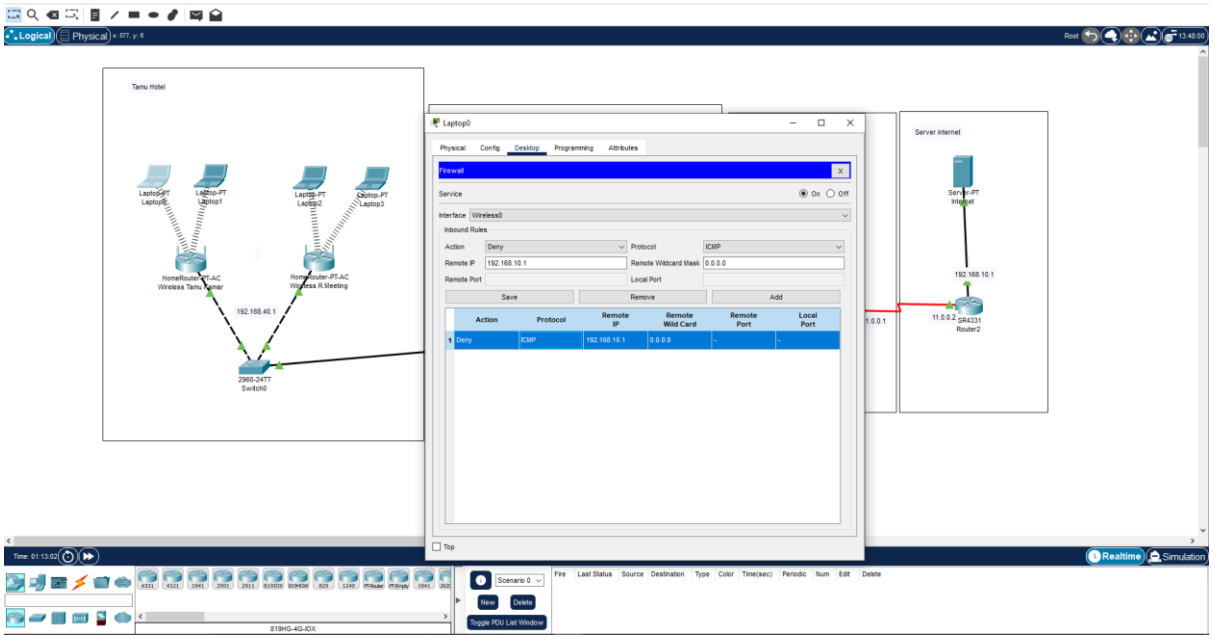




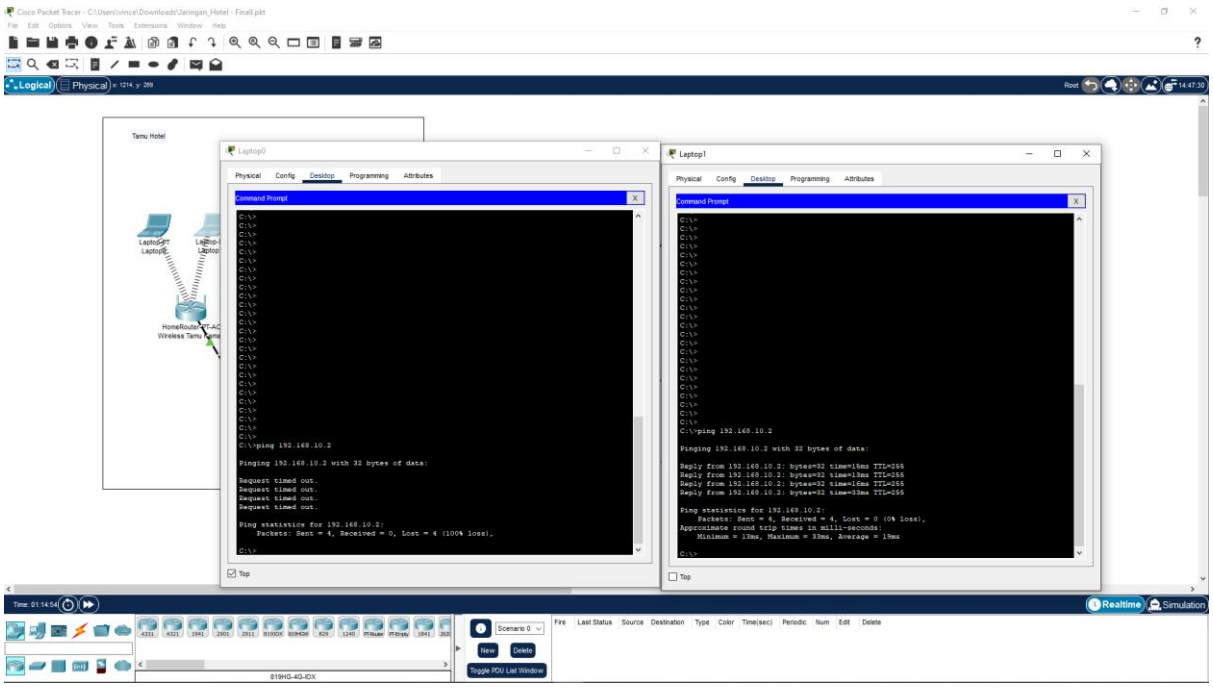
3. Jalankan software untuk melakukan monitor keamanan dan mengamankan baik server maupun 3 laptop tersebut

Jawaban :

Menambahkan IPv4 server internet pada firewall laptop 0



Berikut adlah hasil dari monitoring melakukan ping ke server Internet dari laptop 0 dan laptop 1 yang dimana laptop 0 saat melakukan ping server internet hasilnya request timeout sedangkan laptop 1 bisa melakukan ping ke server internet.



J.611000.016.02 Mengatasi Serangan pada Jaringan

1. Identifikasi jenis serangan dan dampak yang mungkin terjadi

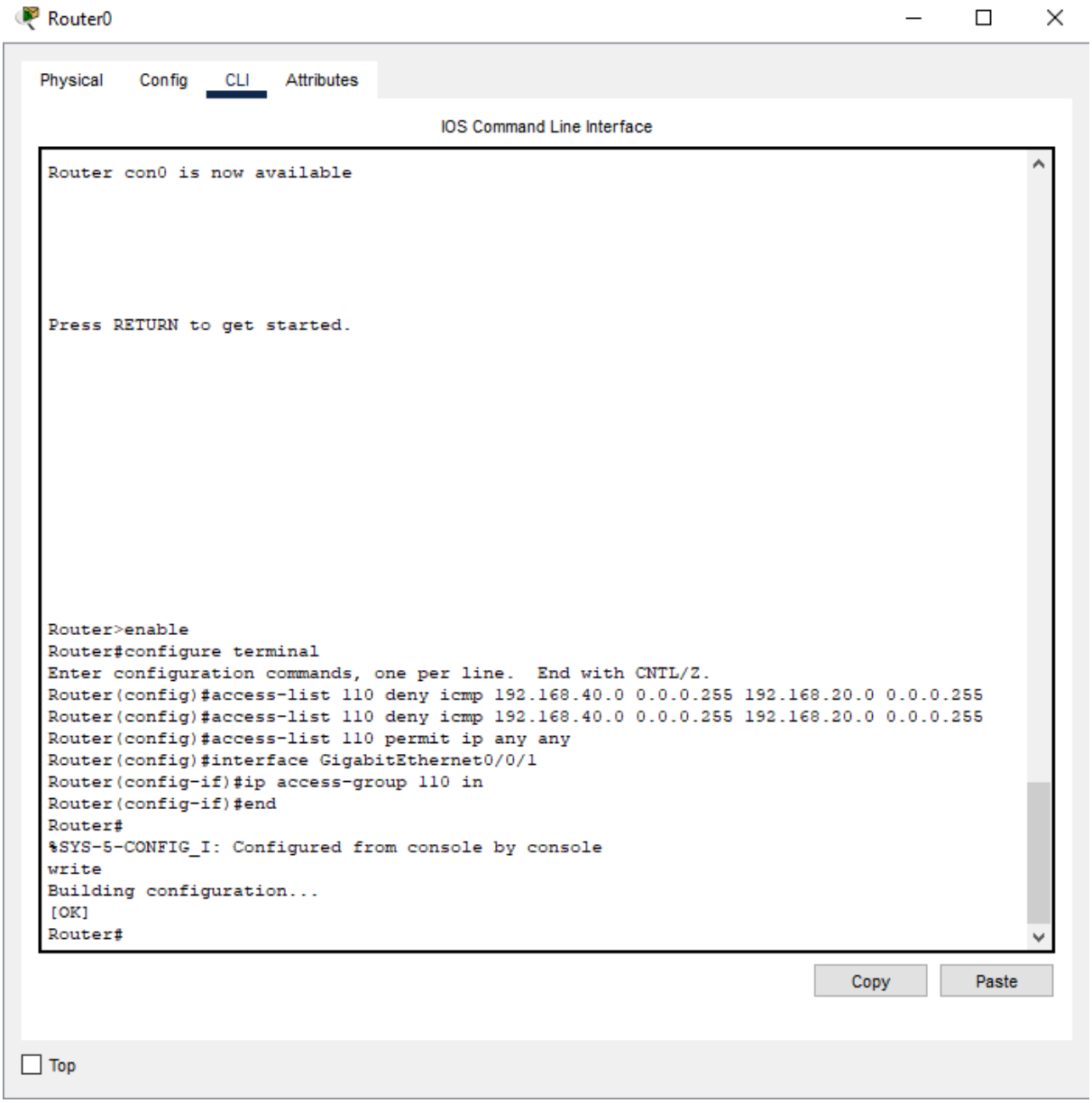
Jawaban :

- Man-in-the-Middle (MITM) yang mencuri data pengguna
- Denial of Service (DoS) yang bisa menyebabkan downtime
- IP Spoofing yang menyamar sebagai perangkat tepercaya

2. Menghentikan serangan dan melakukan proses pemulihan

Jawaban :

- Menambahkan firewall dan IPS untuk memblokir serangan
- Memperbarui firmware dan memperkuat enkripsi
- Menggunakan ACL untuk membatasi akses jaringan



J.611000.017.01 Mengidentifikasi Sumber Kerusakan

1. Analisia problem dari sisi end point secara logical

Jawaban :

- Memeriksa konfigurasi IP address dan default gateway
- Menguji kabel dan koneksi fisik
- Verifikasi routing dan VLAN pada perangkat

2. Identifikasi problem secara physical

Jawaban :

- Memeriksa kabel yang digunakan (Straight-Through atau Cross-Over)

- Memastikan port pada switch aktif dan tidak error
- Mengganti perangkat yang rusak

J.611000.018.02 Memperbaiki Kerusakan Konfigurasi Jaringan

1. Identifikasikan potensi gangguan terhadap sistem yang berjalan

Jawaban :

- IP Conflict atau subnet overlap
- Kesalahan konfigurasi DHCP atau routing

2. Merumuskan strategi pemulihan dan pencegahan secara otomatis

Jawaban :

- Menggunakan backup konfigurasi secara berkala
- Menggunakan Network Management System (NMS) untuk monitoring

3. Mengembagkan perancanaan pecegahan kerusakan terhadap system

Jawaban :

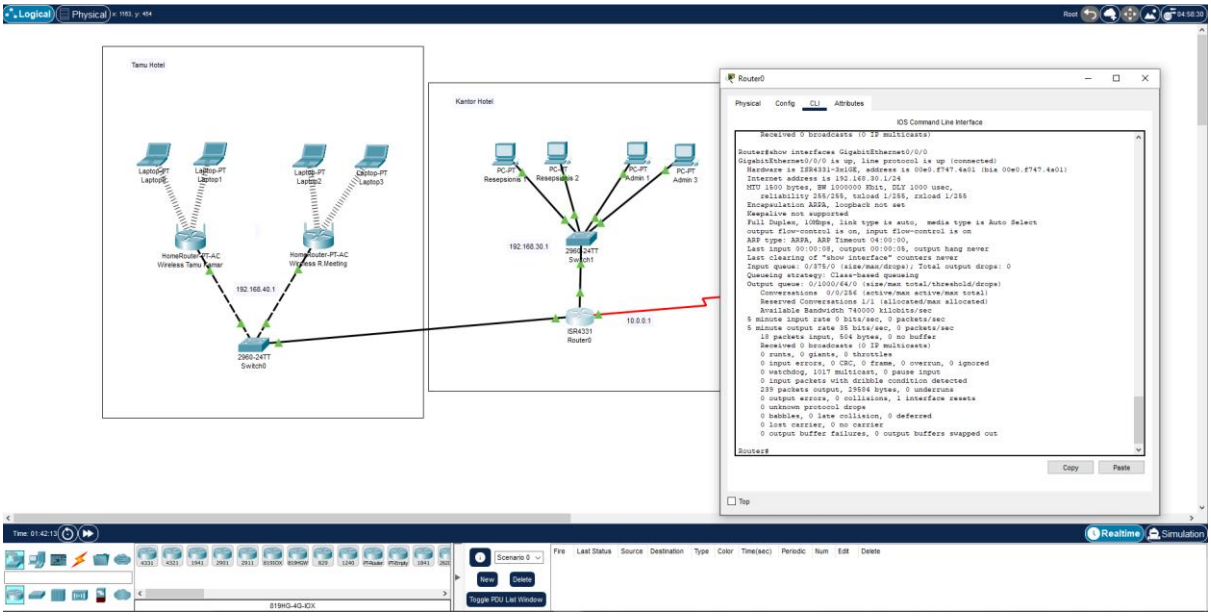
- Membuat rencana disaster recovery
- Menggunakan redundant link dan failover untuk mencegah downtime

J.611000.020.01 Mengoptimalkan Kinerja Sistem Jaringan

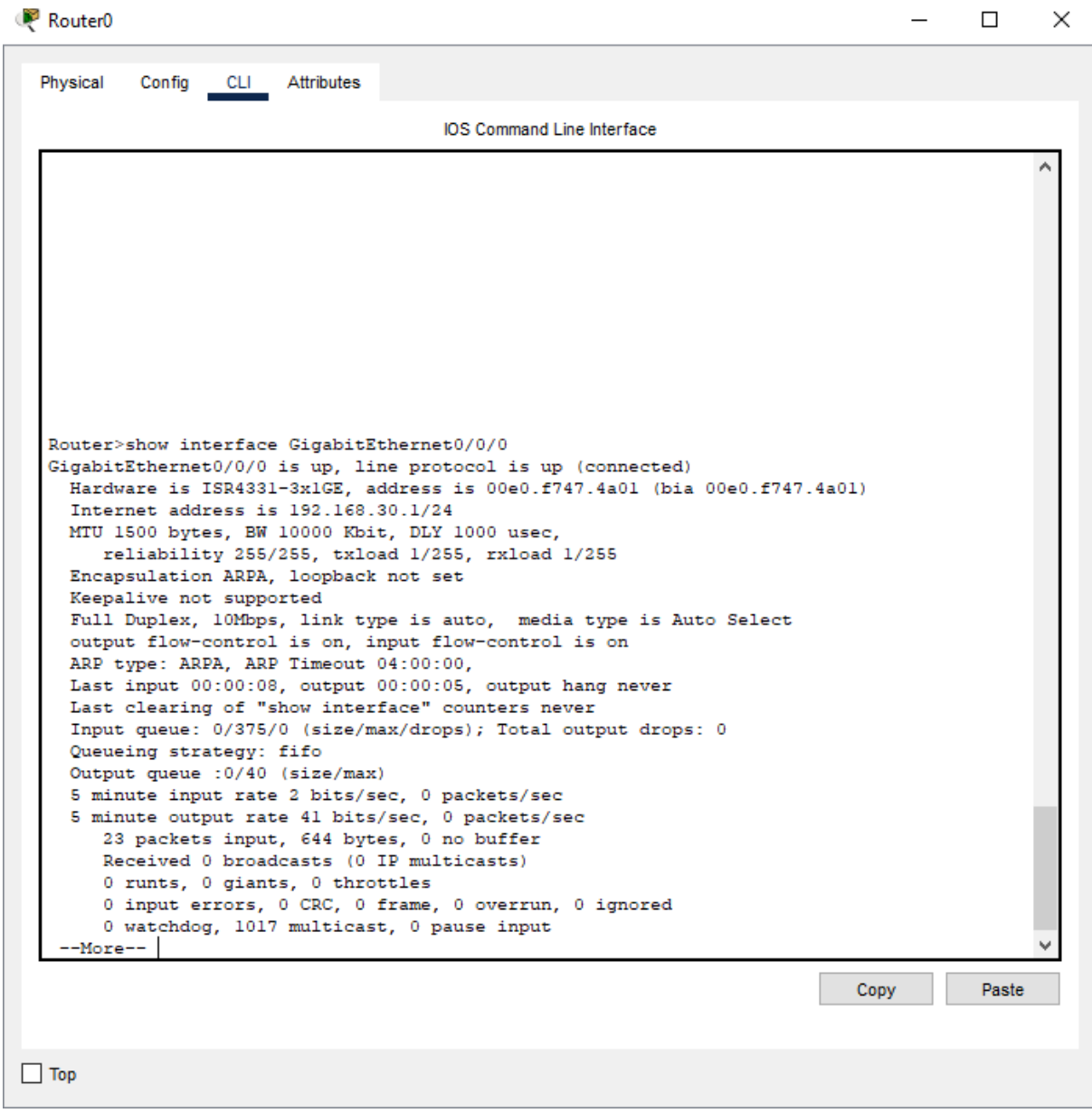
1. Identifikasi kinerja sistem berjalan sesuai kapasitas jaringan dan lakukan monitoring kinerja pada beban maksimal

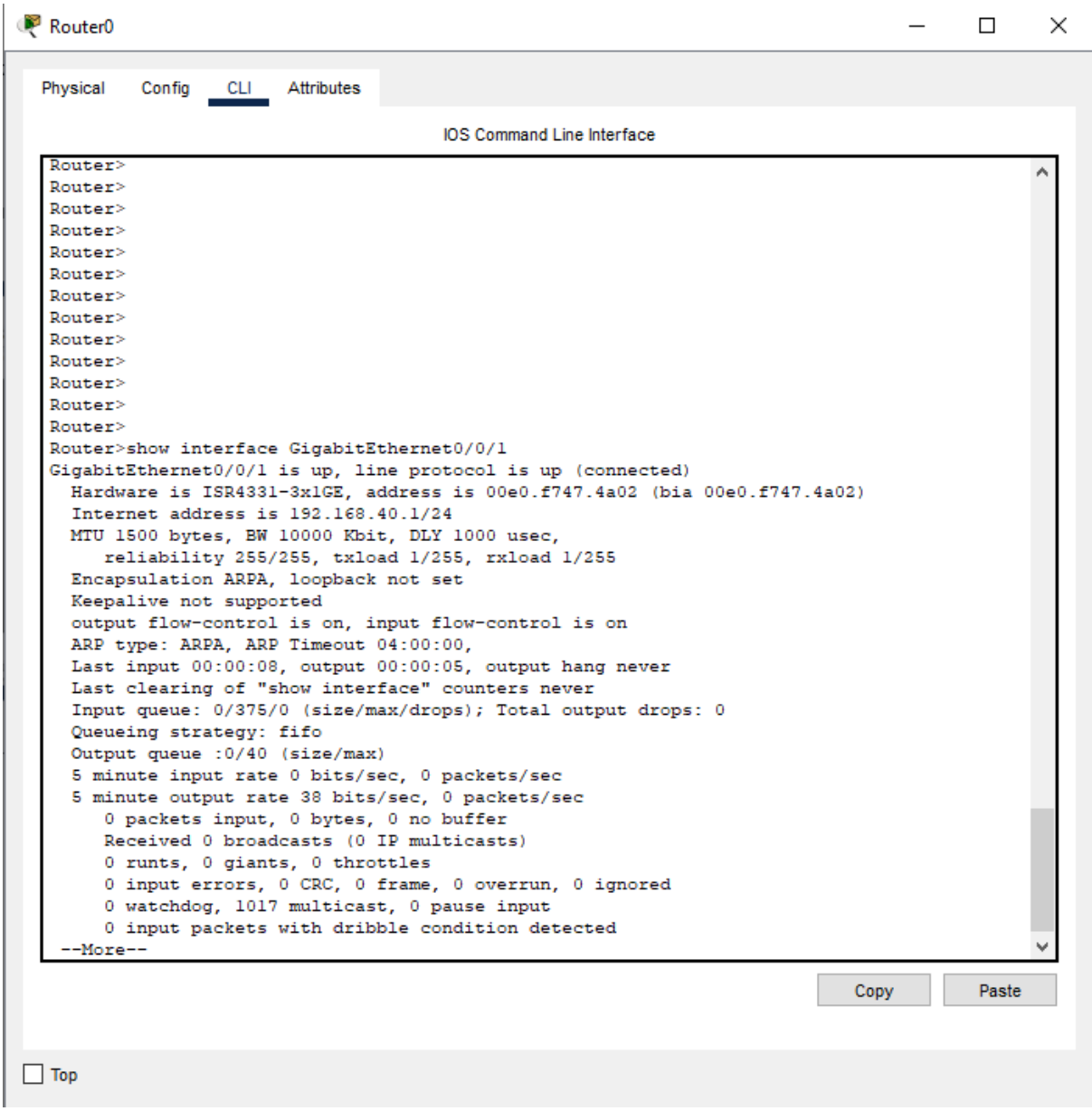
Jawaban :

- Memeriksa bandwidth setiap link jaringan menggunakan perintah "show interfaces" atau "show controllers"

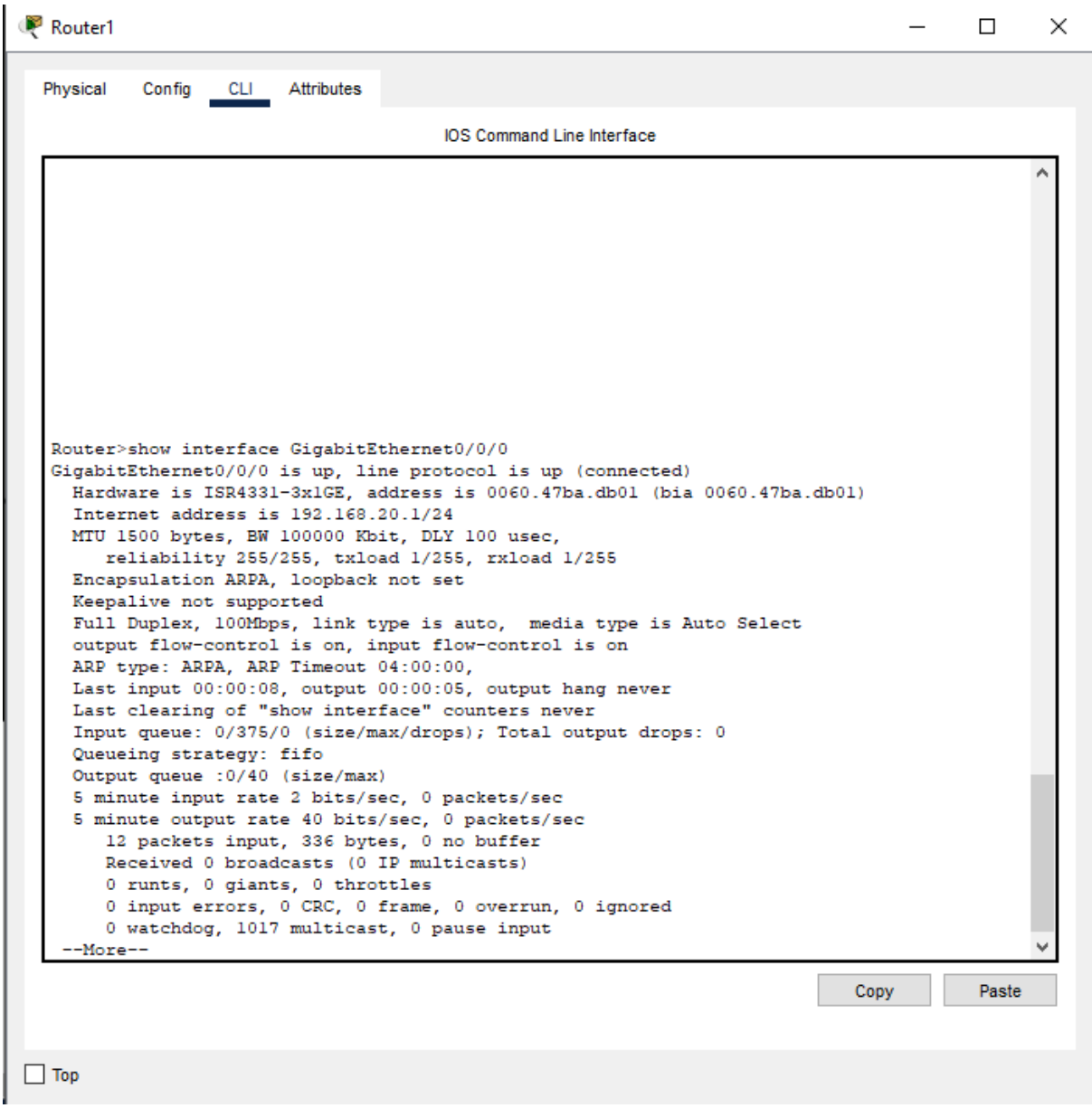

Logical
Physical
Tamu Hotel
Laptop-PT Laptop0
Laptop-PT Laptop1
Laptop-PT Laptop2
Laptop-PT Laptop3
HomeRouter-PT-AC Wireless Tamu Lantai
HomeRouter-PT-AC Wireless R.Meeting
192.168.40.1
2960-24TT Switch0
Kantor Hotel
PC-PT Resepsionis
PC-PT Resepsionis 2
PC-PT Admin 1
PC-PT Admin 3
192.168.30.1
2960-24TT Switch1
ISR4331 Router0
10.0.0.1
Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Received 0 broadcasts (0 IP multicasts)
Router#show interfaces GigabitEthernet0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
Hardware is ISR4331-3x1GE, address is 00e0.f747.4a01 (bia 00e0.f747.4a01)
Internet address is 192.168.30.1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
Full Duplex, 10Mbps, link type is auto, media type is Auto Select
output flow-control is on, input flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0 (size/max/drops); Total output drops: 0
Queueing strategy: Class-based queueing
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 1/1 (allocated/max allocated)
Available Bandwidth 740000 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 35 bits/sec, 0 packets/sec
18 packets input, 504 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 1017 multicast, 0 pause input
0 input packets with dribble condition detected
239 packets output, 25584 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Router#
Copy
Paste
Top
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
819HG-4G-IOX

- Cek kapasitas bandwidth setiap segmen:
  - Kantor & tamu hotel: 10 Mbps



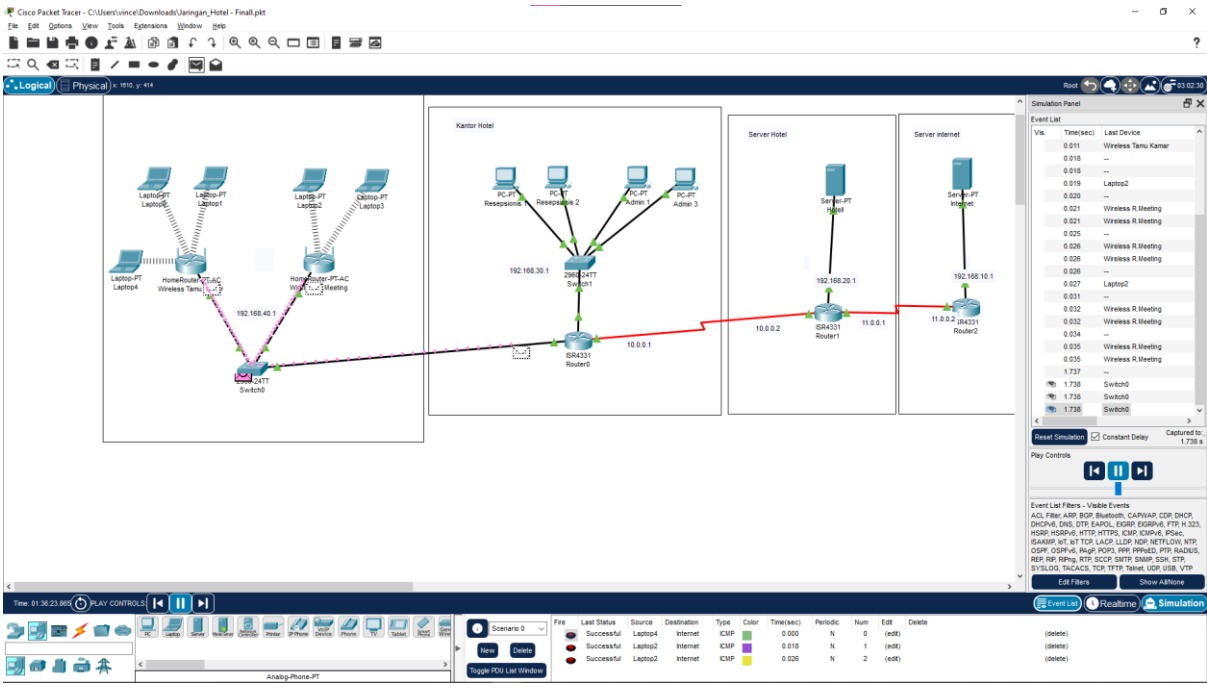

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>show interface GigabitEthernet0/0/1
GigabitEthernet0/0/1 is up, line protocol is up (connected)
Hardware is ISR4331-3x1GE, address is 00e0.f747.4a02 (bia 00e0.f747.4a02)
Internet address is 192.168.40.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
output flow-control is on, input flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 38 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 1017 multicast, 0 pause input
0 input packets with dribble condition detected
--More--
Copy
Paste
Top

➢ Jalur server Hotel: 100 Mbps



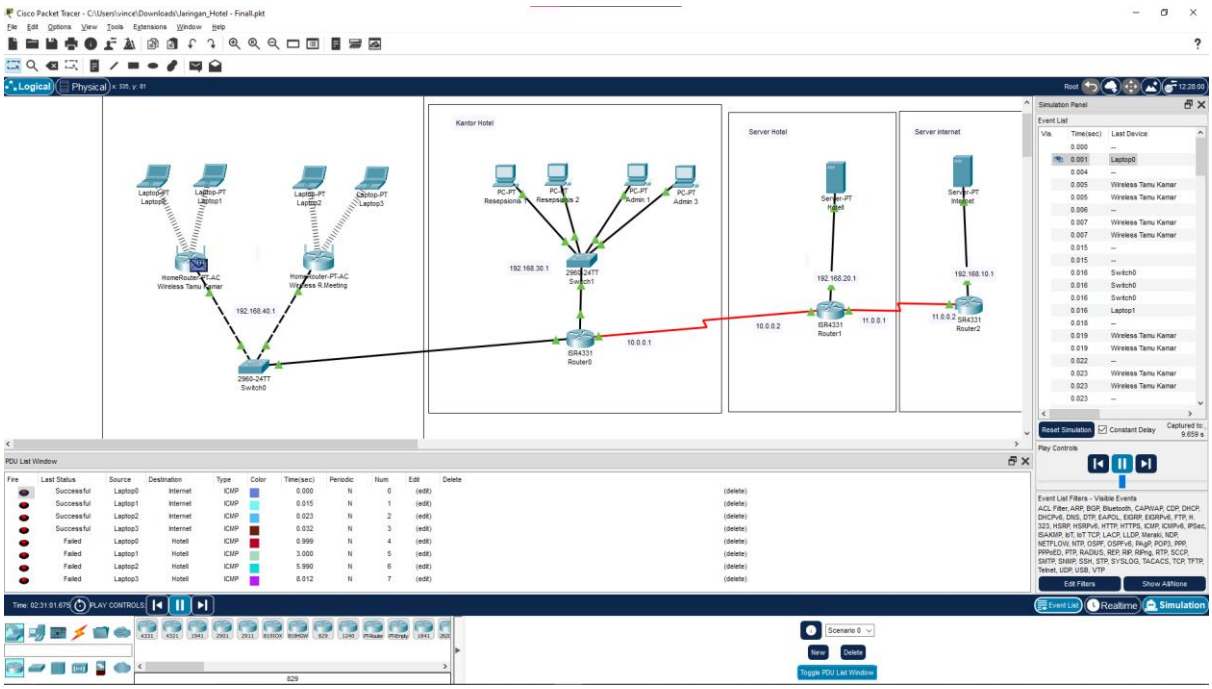
- Monitoring kinerja jaringan saat beban penuh:

- Gunakan ping berulang ke server saat banyak perangkat aktif untuk melihat delay/timeout



- Gunakan Simulation Mode di Packet Tracer untuk melihat aliran paket dan kemacetan

- Uji beban maksimal: Semua laptop ping + akses web ke server secara bersamaan untuk menguji delay



2. Merumuskan strategi pemulihan kinerja sistem terhadap kendala saat beban maksimal dan dokumentasikan

Jawaban :

Langkah-langkah untuk pemulihan dan optimasi sistem:

- Aktifkan QoS (Quality of Service) pada router:
  - Memberikan prioritas tinggi untuk perangkat penting seperti PC resepsionis dan server
- Pisahkan trafik tamu dan admin menggunakan VLAN
  - Agar broadcast tamu tidak mengganggu trafik kantor
- Upgrade bandwidth jalur padat, jika delay terus meningkat
- Gunakan Access Control List (ACL) untuk membatasi trafik tidak perlu
- Matikan service yang tidak digunakan di server atau switch untuk mengurangi beban
- Dokumentasi hasil monitoring dan tindakan perbaikan dibuat sebagai referensi untuk perencanaan pengembangan berikutnya

Contoh: Setelah menerapkan VLAN dan QoS, delay saat jam sibuk menurun drastis, dan koneksi server menjadi lebih stabil.

J.611000.022.01 Melakukan Backup dan Restore Konfigurasi Jaringan

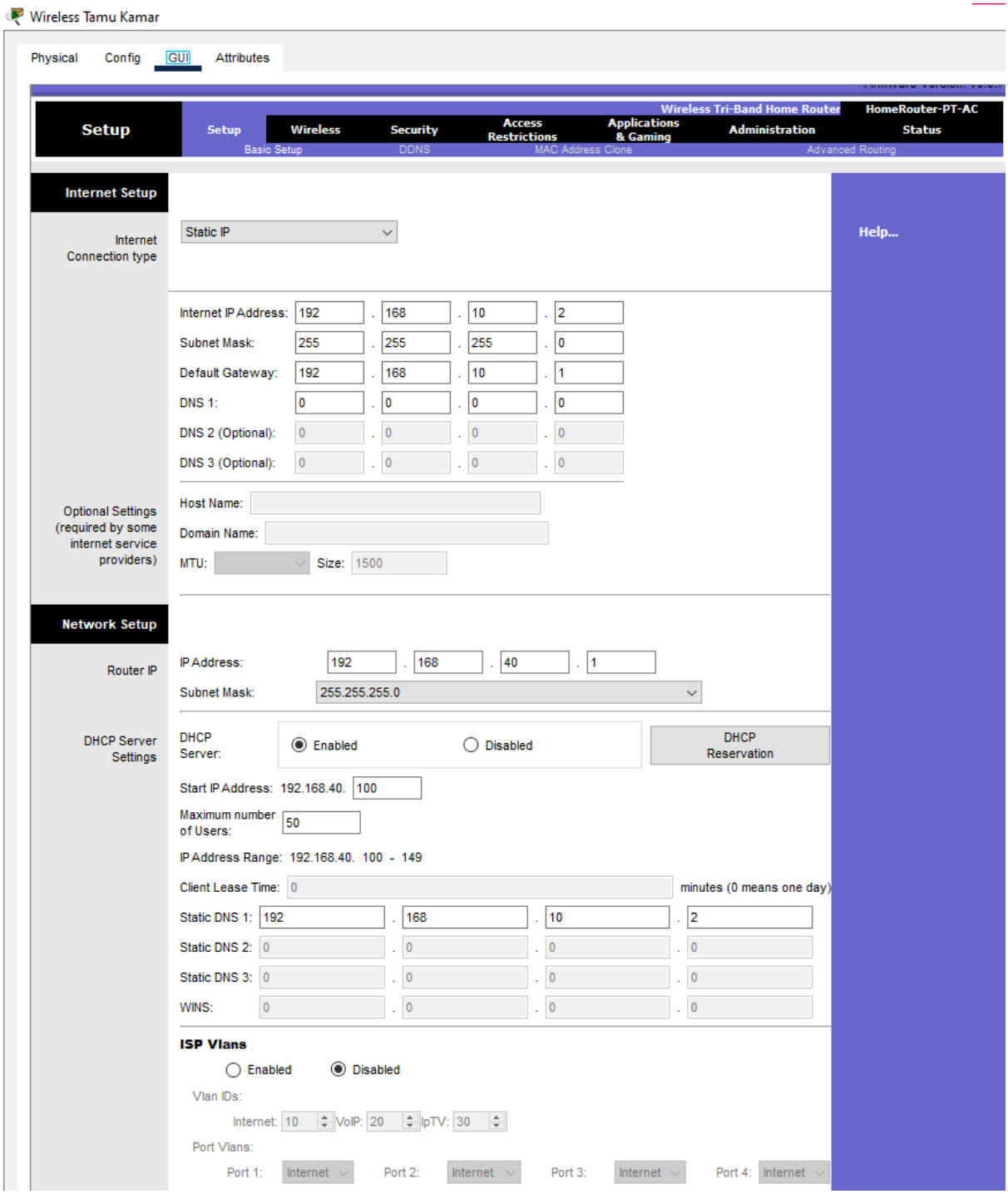
1. Identifikasi kebutuhan konfigurasi jaringan yang akan di back up

Jawaban :

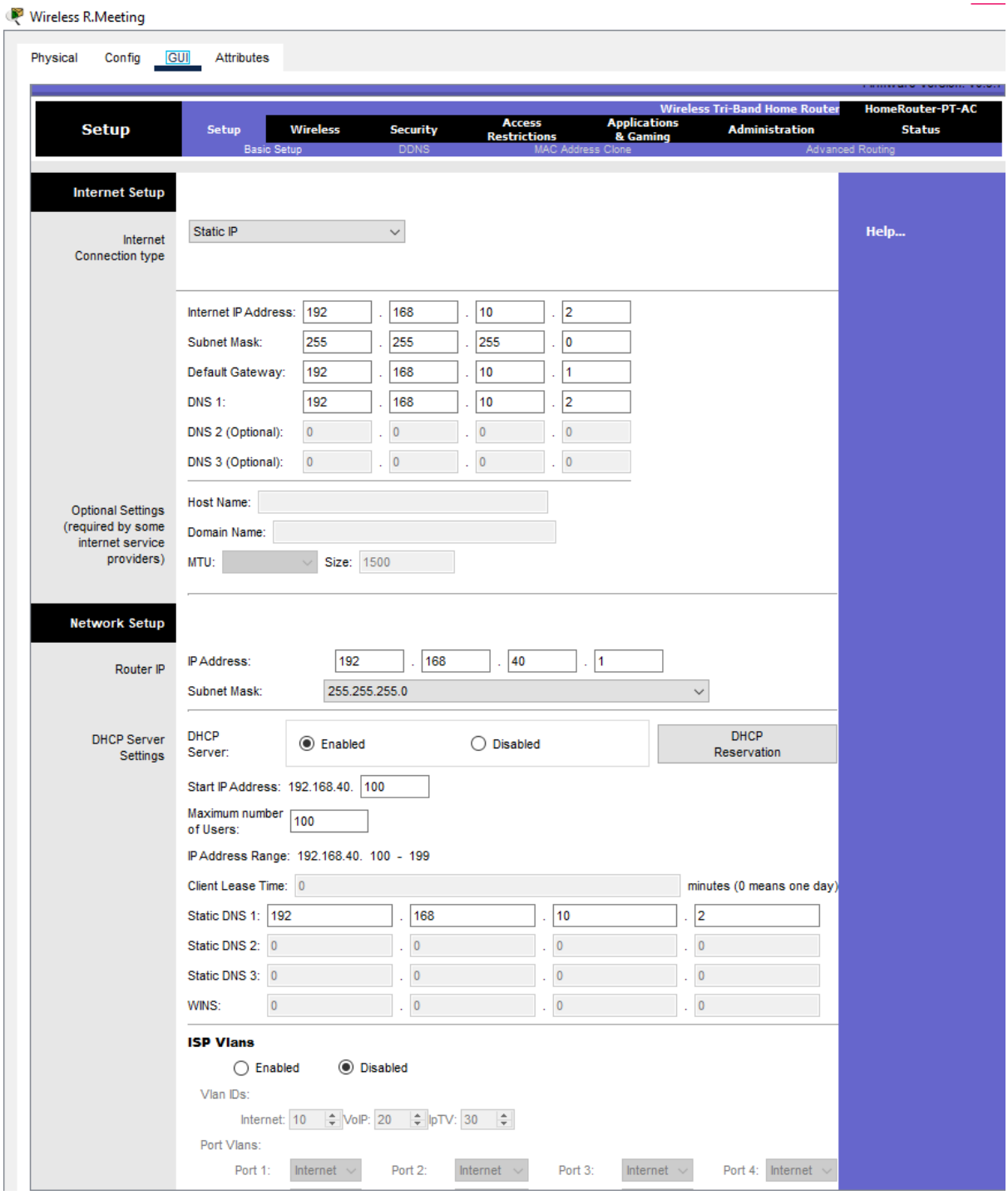
Konfigurasi jaringan yang perlu di-backup meliputi:

- Konfigurasi IP pada router dan server

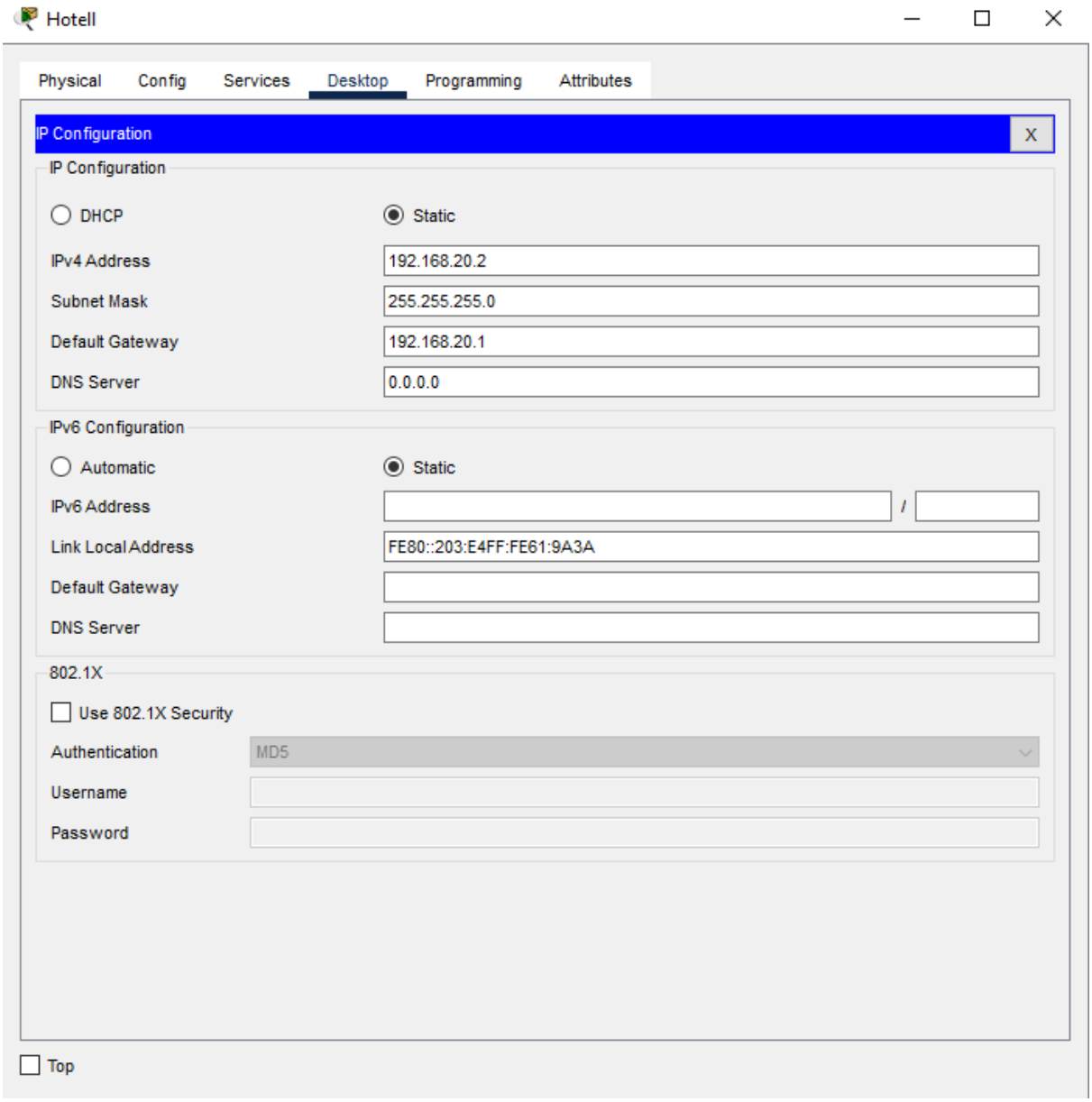
Berikut adalah konfigurasi pada Router Tamu Kamar.



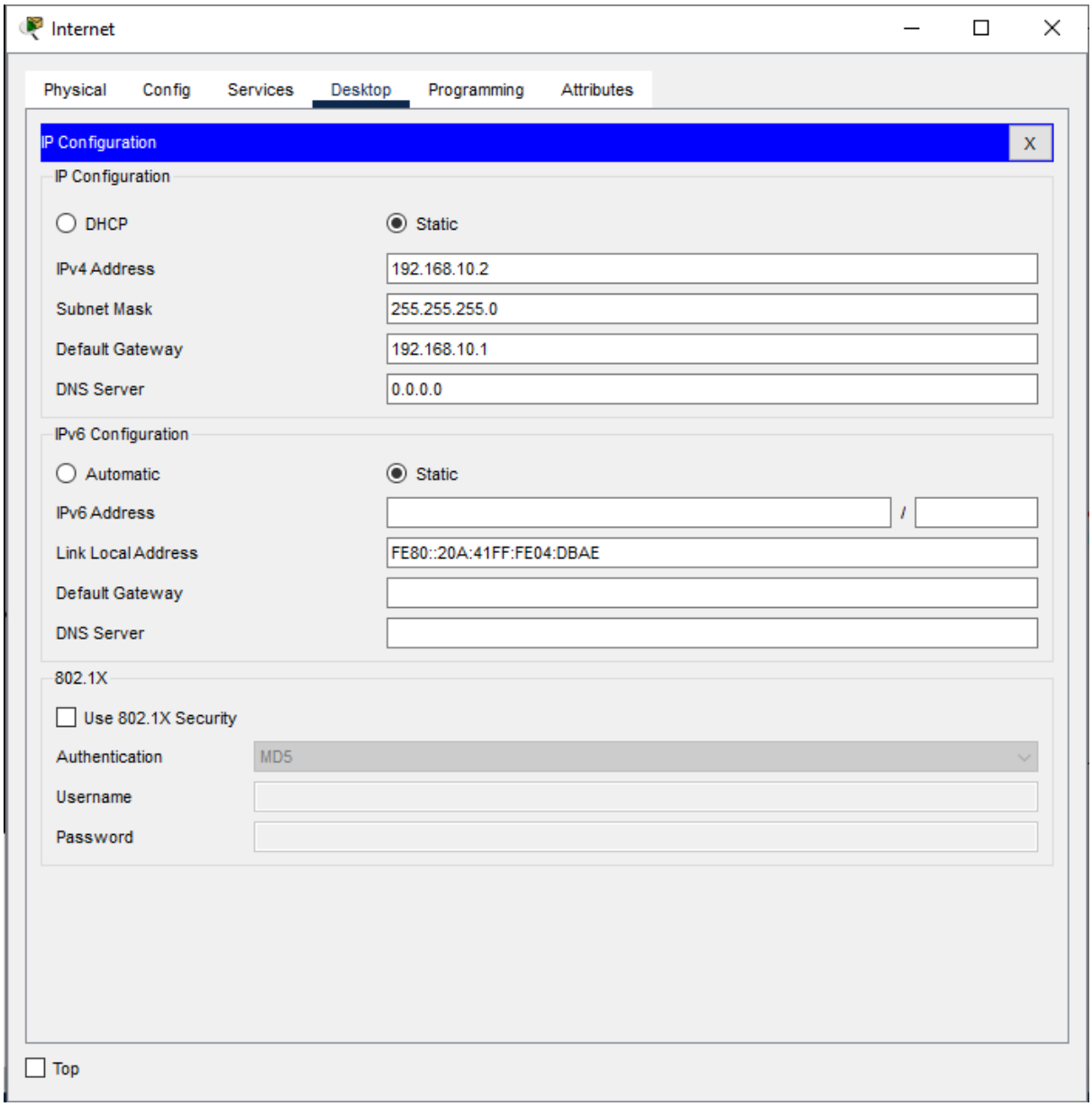
Berikut adalah Konfigurasi pada Router R.Meeting.



Berikut adalah Konfigurasi pada Server Hotell.

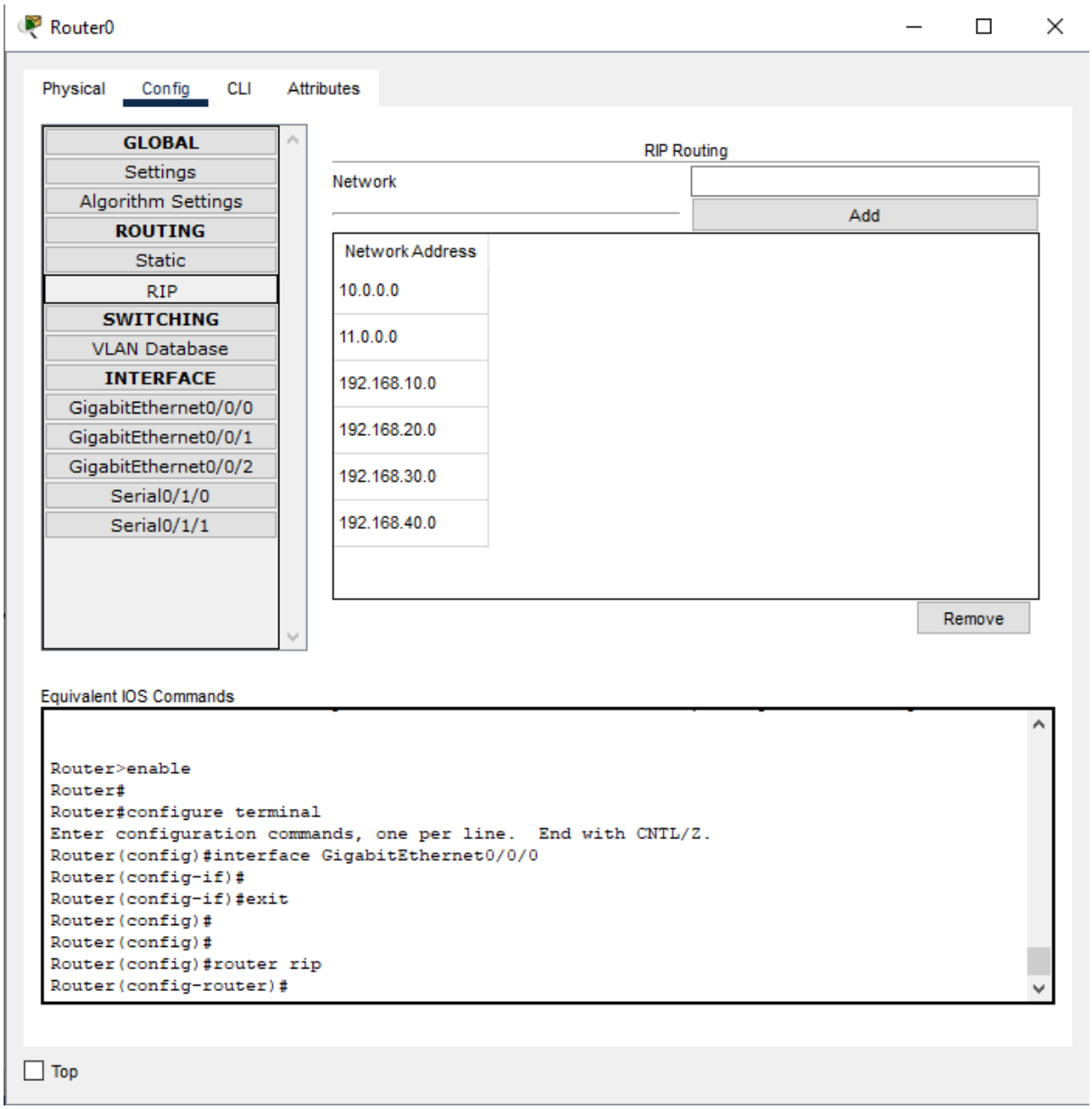


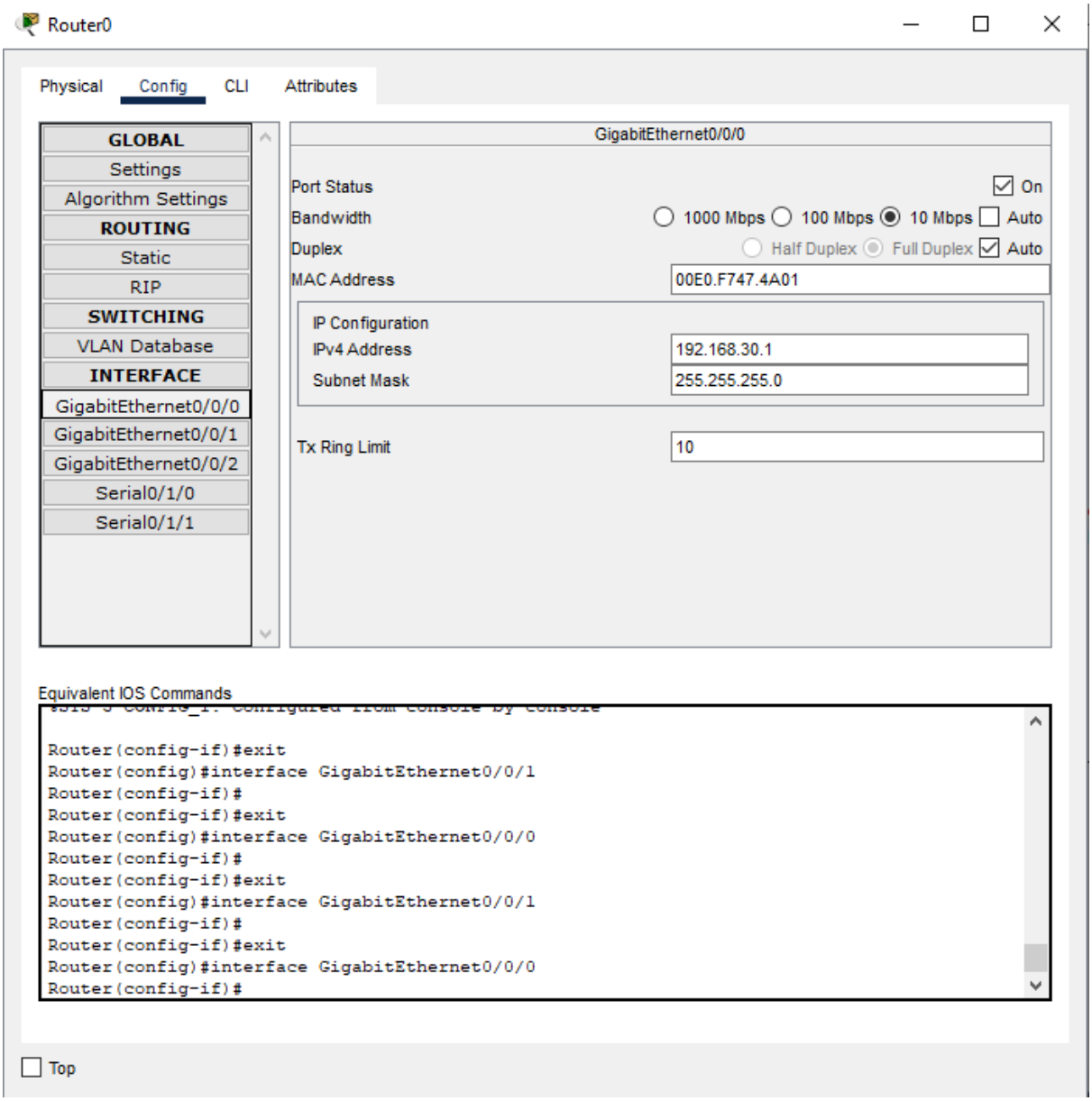
Berikut adalah konfigurasi dari Server Internet.

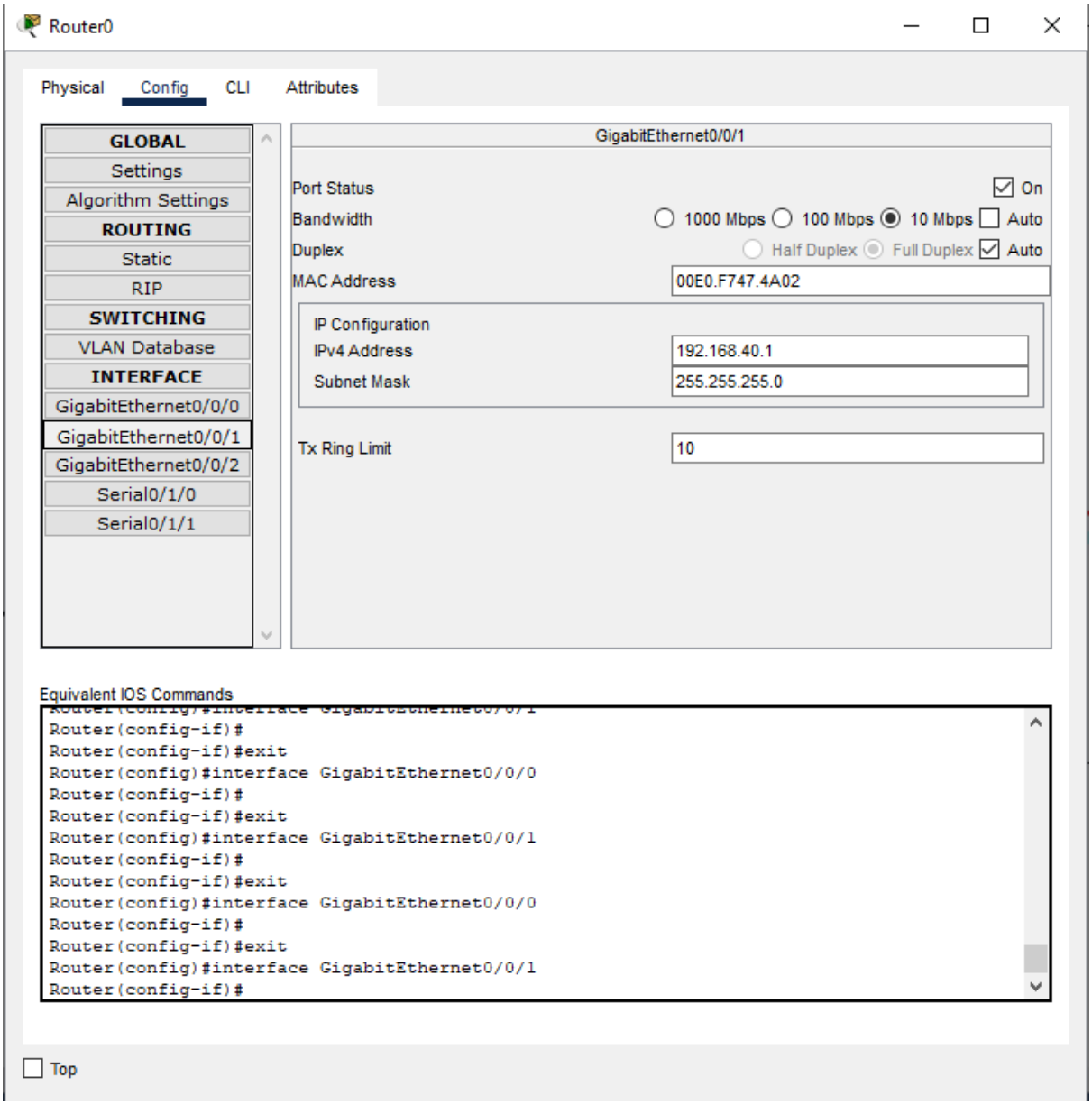


- Pengaturan routing (statik/dinamis)

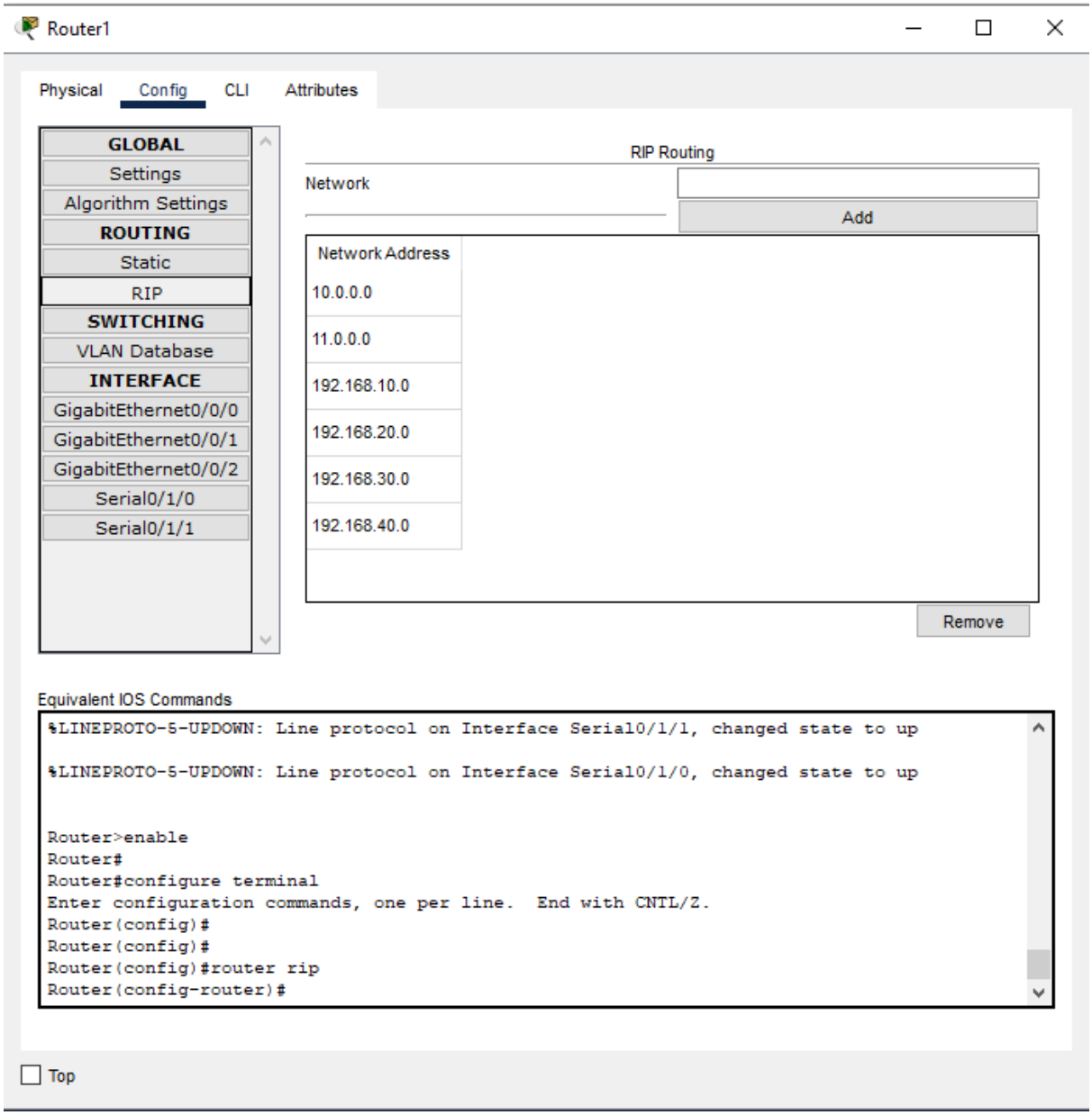
  Konfigurasi Routing pada Router 0.

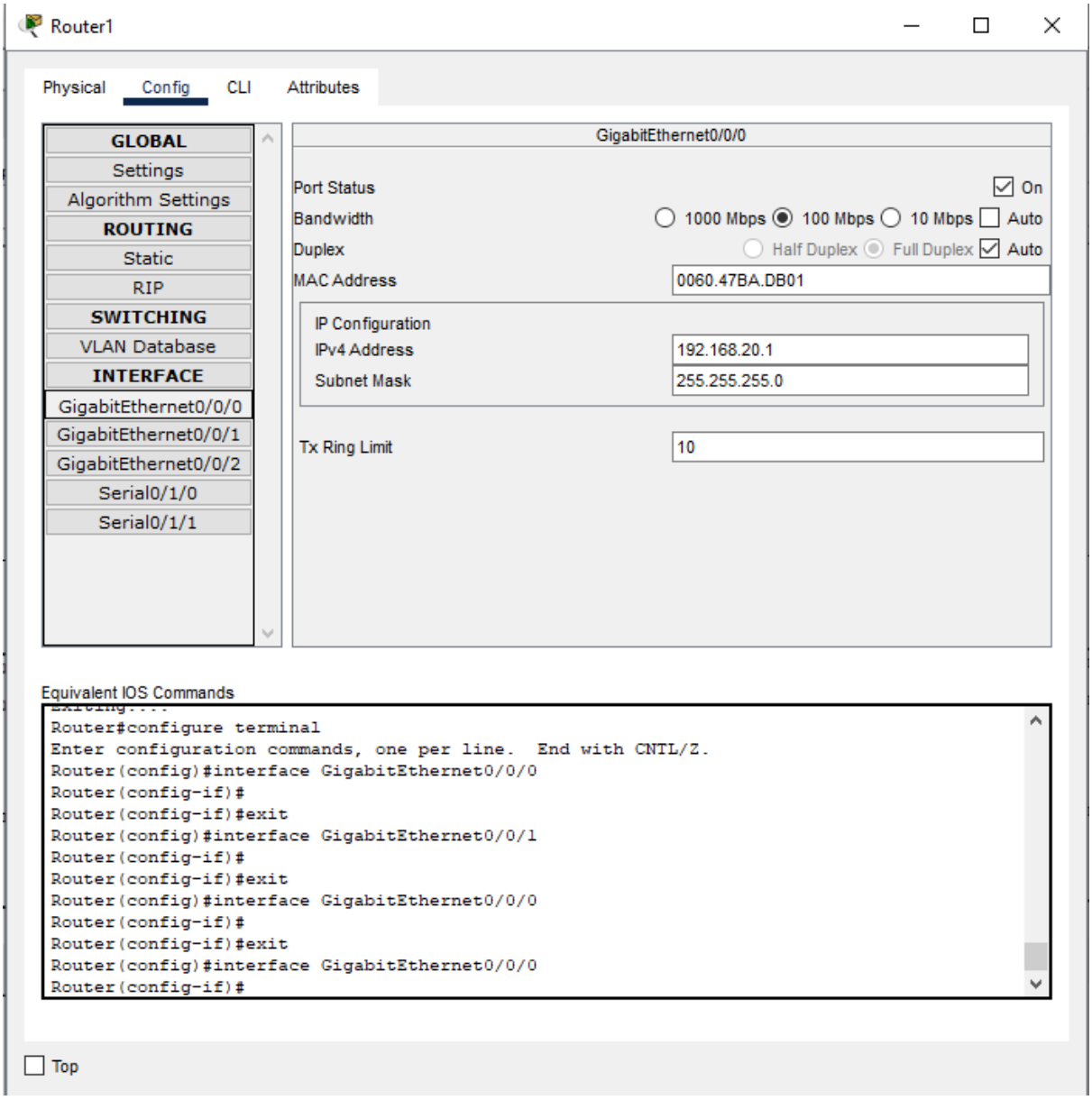



Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/2
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.F747.4A01
IP Configuration
IPv4 Address
192.168.30.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Top

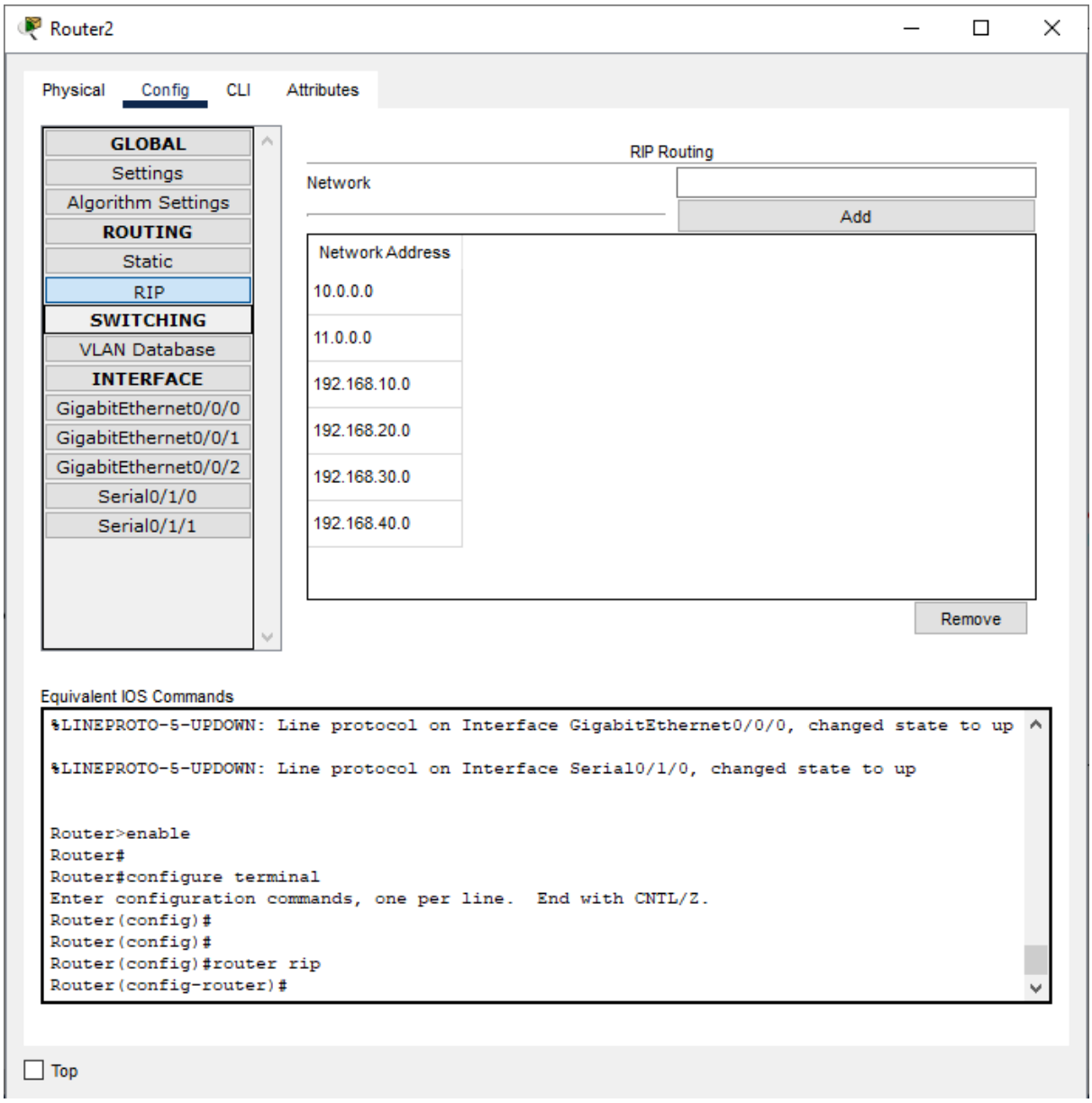

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/2
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.F747.4A02
IP Configuration
IPv4 Address
192.168.40.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Top

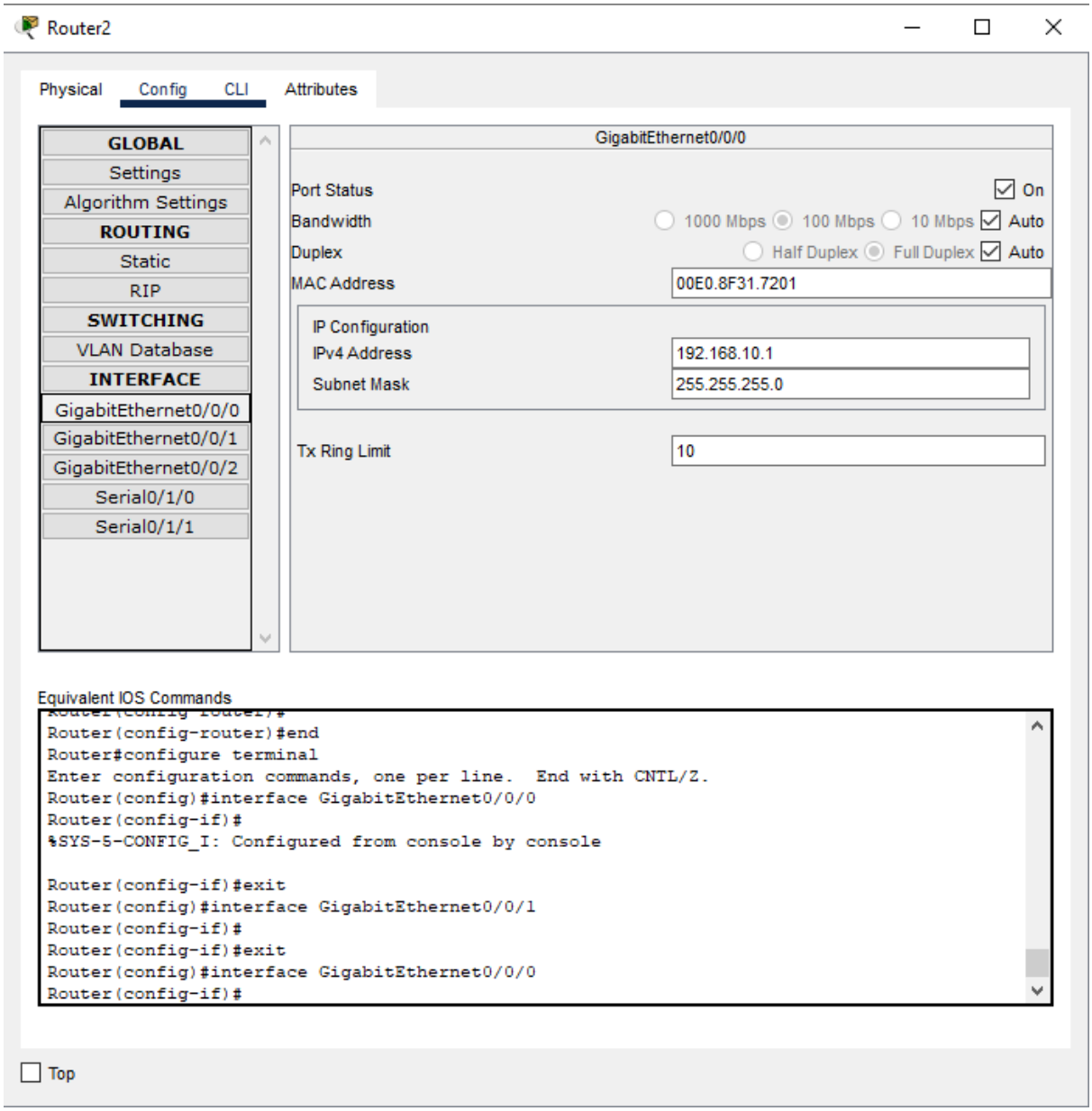
Konfigurasi Routing pada Router 1.




Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/2
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.47BA.DB01
IP Configuration
IPv4 Address
192.168.20.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Top

Konfigurasi Routing pada Router 2.





- Access Control List (ACL) yang digunakan untuk membatasi akses antar jaringan
- Firewall rules pada laptop dan server
- SSID dan password Wi-Fi access point
- Setting DHCP Server

Backup dibutuhkan untuk mencegah hilangnya konfigurasi akibat:

- Perangkat restart atau mati listrik
- Perubahan konfigurasi tidak disengaja
- Kerusakan fisik perangkat

Melakukan Backup konfigurasi router dan server termasuk konfigurasi IP, routing, dan ACL

2. Lakukan proses back up dan restore konfigurasi jaringan

Jawaban :

- Menggunakan perintah "copy running-config startup-config"
- Memindahkan file konfigurasi ke server backup atau storage eksternal