

BAB V

IMPLEMENTASI DAN PENGUJIAN

5.1.1 IMPLEMENTASI

Seperti dijelaskan pada bab sebelumnya, implementasi adalah tahapan dimana metode *Switch-Port Security* akan diterapkan dengan rancangan yang telah dibuat pada bab sebelumnya. Terdapat beberapa tahapan dalam implementasi metode *Switch-Port Security* pada jaringan CCTV Perimeter di Bandara Sultan Thaha.

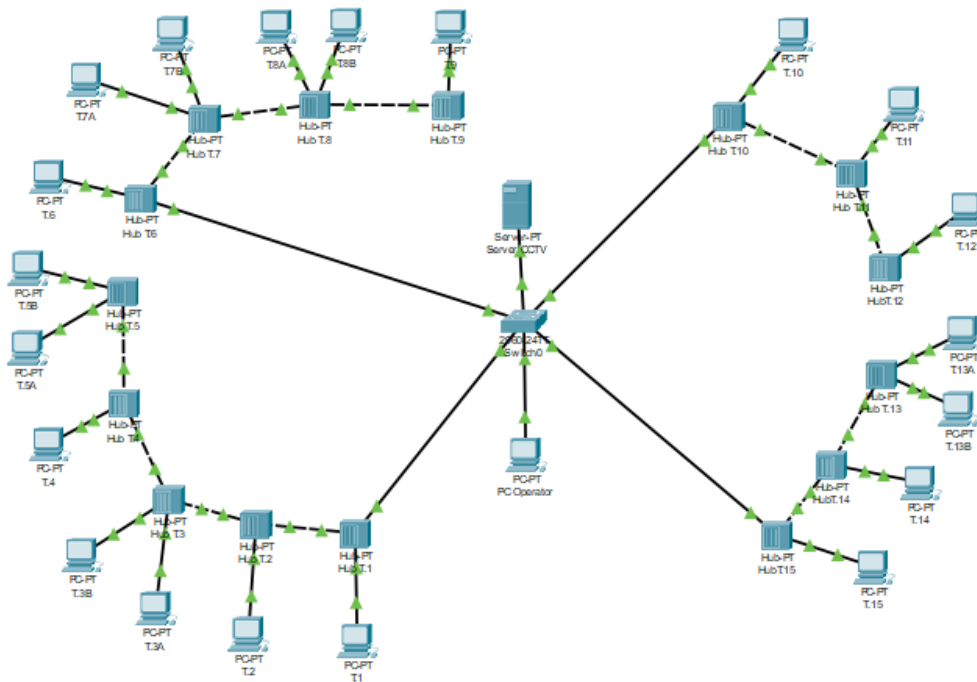
5.1.1 Pembuatan Arsitektur Jaringan di Cisco Packet Tracer

Langkah pertama yang dilakukan adalah membuat arsitektur jaringan CCTV di Bandara Sultan Thaha kedalam *software* jaringan cisco packet tracer, adapun tools yang dibutuhkan adalah sebagai berikut :

Tabel 5.1 Daftar Tools Pembuatan Arsitektur Jaringan CCTV

No	Nama Tools	Jumlah
1	Switch 24 Port	1
2	Server	1
3	Hub 5 Port	15
4	PC (Pengganti CCTV)	20
5	Laptop	1

Selanjutnya dengan *tools* yang sudah ada, kita implementasikan kedalam *cisco packet tracer* sesuai dengan perencanaan pada bab sebelumnya, dengan hasil sebagai berikut :



Gambar 5.1 Arsitektur Jaringan CCTV Perimeter dengan 4 backbone

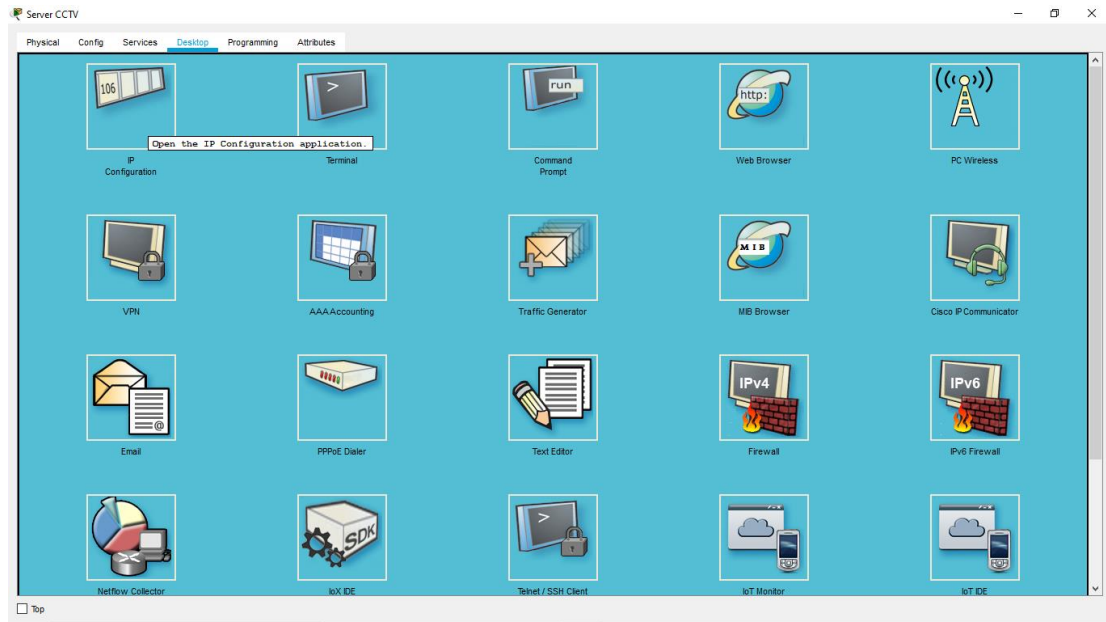
5.1.2 Input IP Address Pada Perangkat CCTV

Langkah selanjutnya yang kita lakukan pertama adalah menambahkan *ip address* ke dalam *server* dan PC yang dalam hal ini berperan sebagai pengganti CCTV karena karakteristik *mac-address* yang kita butuhkan.

a. Input IP Address di *server* CCTV

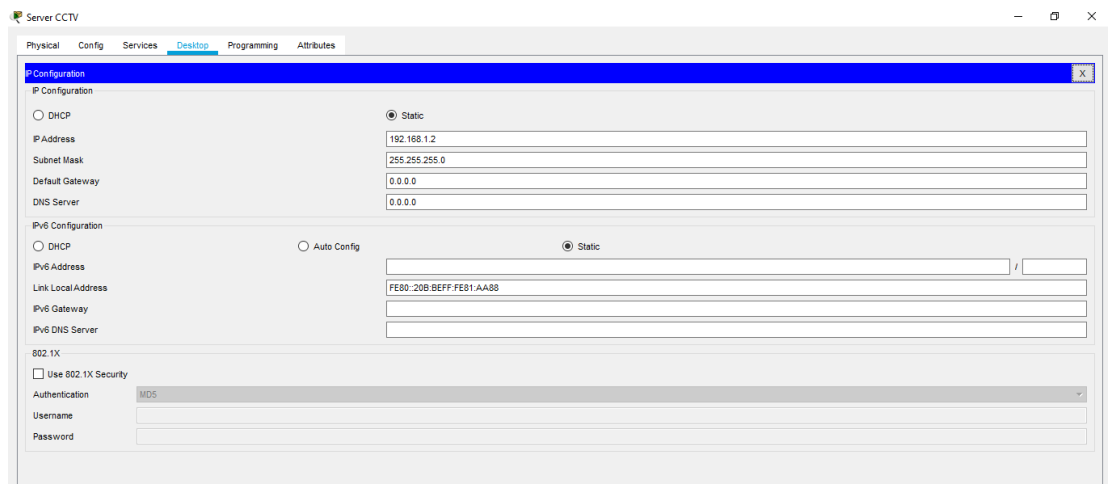
Langkah-langkah yang harus dilakukan adalah sebagai berikut :

1. Klik ikon PC dengan keterangan Server CCTV
2. Akan tampil kotak dialog informasi PC
3. Pilih tab menu desktop, lalu pilih *ip configuration*



Gambar 5.2 Tab Menu Desktop Pada PC Server di Simulasi Packet Tracer

5. Akan muncul kotak dialog *ip configuration*, lalu masukkan parameter *ip address*, *subnet mask*, sesuai dengan perencanaan pada bab sebelumnya, dengan *ip address* untuk server adalah 192.168.1.2



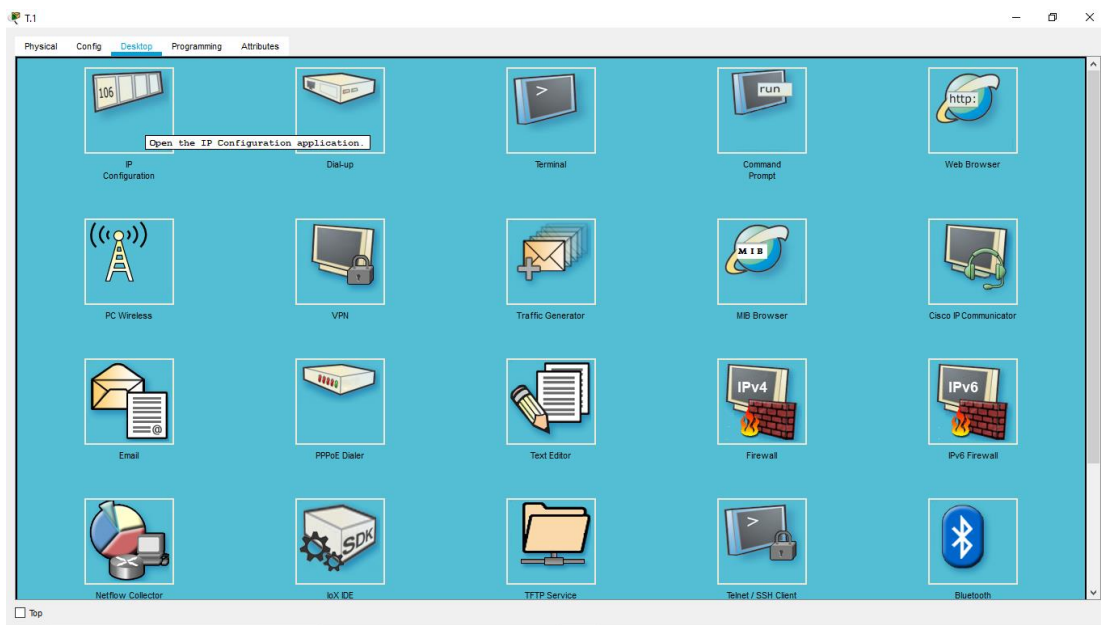
Gambar 5.3 Kotak Dialog IP Configuration Pada PC

Selanjutnya masukkan *ip address* CCTV sesuai dengan perencanaan pada bab sebelumnya yang dalam hal ini kita menggunakan PC sebagai pengganti CCTV, adapun langkah-langkahnya adalah :

b. Input IP Address di masing-masing PC (CCTV)

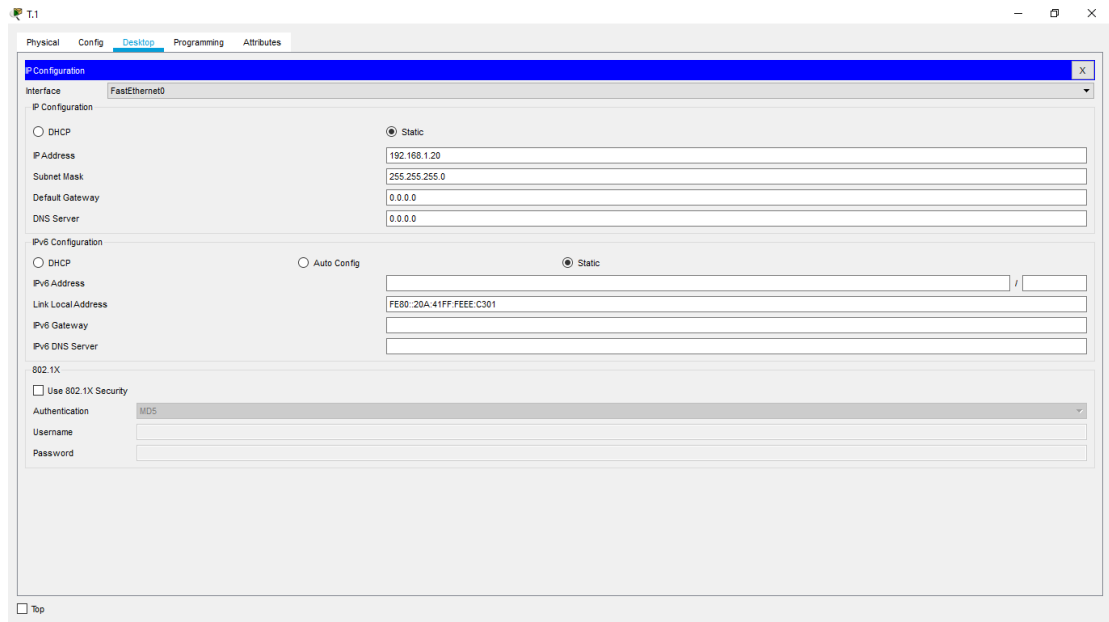
Langkah-langkah yang harus dilakukan adalah sebagai berikut :

1. Klik ikon PC dengan keterangan T.1 yang merupakan CCTV pada tiang 1
2. Akan tampil kotak dialog informasi PC
3. Pilih tab menu desktop, lalu pilih *ip configuration*



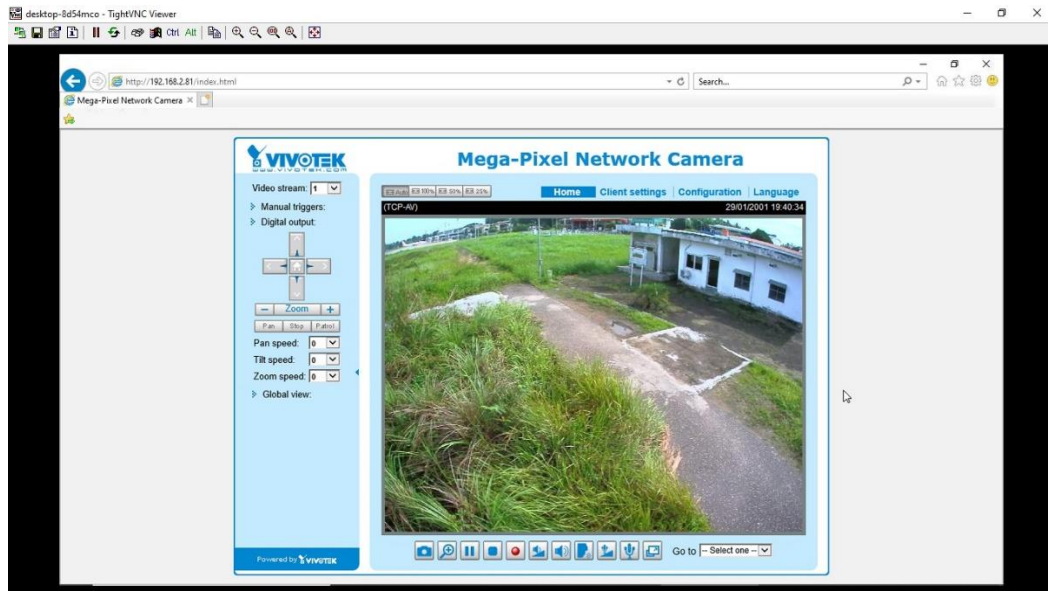
Gambar 5.4 Tab Menu Desktop Pada PC di Simulasi Packet Tracer

4. Akan muncul kotak dialog *ip configuration*, lalu masukkan parameter *ip address*, *subnet mask*, sesuai dengan perencanaan pada bab sebelumnya, dengan *ip address* untuk CCTV tiang 1 adalah 192.168.1.20

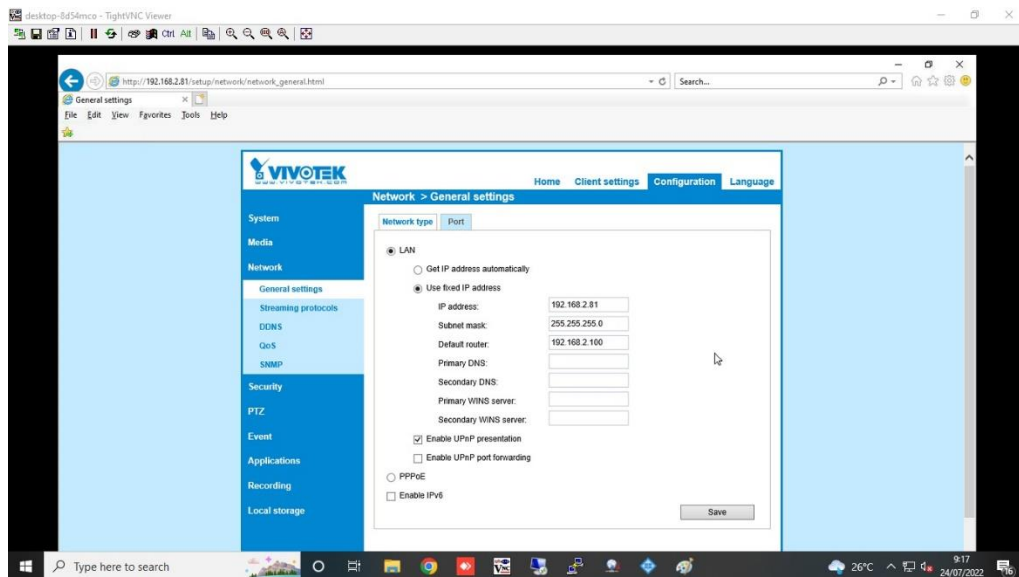


Gambar 5.5 Kotak Dialog IP Configuration Pada PC

Namun pada saat implementasi dilapangan, untuk mengubah atau menambahkan IP Address pada CCTV kita harus menginstall aplikasi *installation wizard* sebagai software dari CCTV vivotek untuk mengakses perangkat CCTV tersebut, setelah selesai selanjutnya lakukan *scanning* terhadap CCTV yang sudah terhubung dan akan ditambahkan IP address nya.



Gambar 5.6 Tampilan CCTV Saat Di Akses Melalui Aplikasi *Installation Wizard*



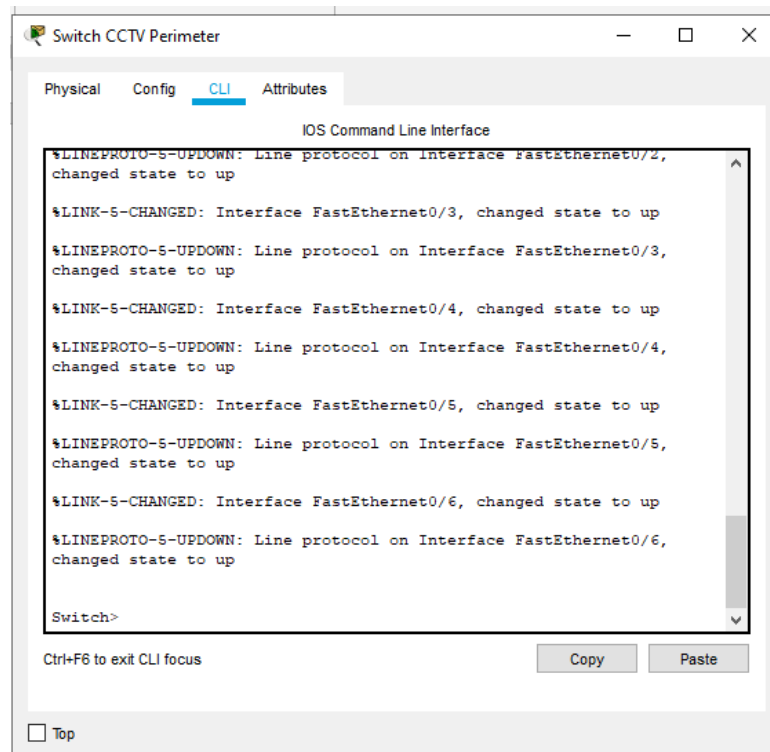
Gambar 5.7 Tampilan saat *Setting* IP Address CCTV

Kemudian dilanjutkan dengan menambahkan *ip address* ke perangkat CCTV lain dari T.2 sampai dengan T.15, lalu tambahkan juga *ip address* untuk PC Operator sesuai dengan tabel perencanaan 4.3.

5.1.3 Konfigurasi Switch

Setelah pengisian seluruh *ip address* selesai, akan dilanjutkan dengan konfigurasi *switch* menggunakan metode *switch-port security* dengan langkah-langkah sebagai berikut :

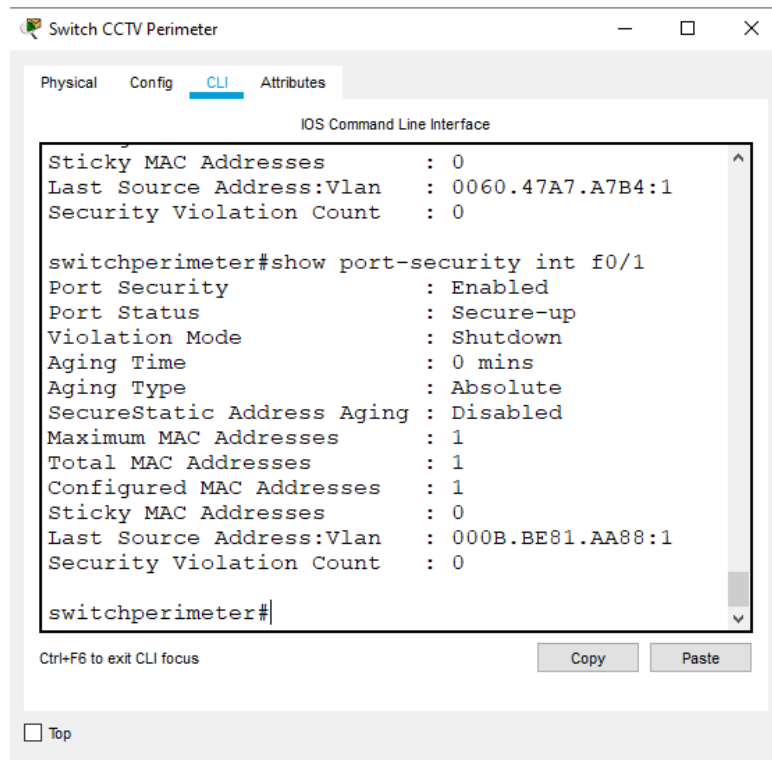
1. Klik ikon switch pada packet tracer, akan muncul kotak dialog informasi switch, pilih tab menu CLI.
2. Tunggu switch sampai selesai booting, lalu tekan enter.



Gambar 5.8 Tampilan Awal Konfigurasi Switch

3. Lalu selanjutnya lakukan konfigurasi, pertama ubah nama *switch* menjadi *switch* perimeter, lalu lakukan konfigurasi pada setiap *port* sesuai dengan perencanaan pada tabel 4.2, adapun langkah-langkahnya sebagai berikut :

```
switch>enable
switch#configure terminal
switch(config)#hostname switchperimeter
switchperimeter(config)#int f0/1
switchperimeter(config-if)#switchport
switchperimeter(config-if)#switchport mode ac
switchperimeter(config-if)#switchport mode access
switchperimeter(config-if)#switchport port-
switchperimeter(config-if)#switchport port-security
switchperimeter(config-if)#switchport port
switchperimeter(config-if)#switchport port-security mac-address
000B.BE81.AA88
switchperimeter(config-if)# switchport port-security maximum 1
switchperimeter(config-if)#switchport port-security violation shutdown
switchperimeter(config-if)#no shut
switchperimeter#show port-security int f0/1
```

Gambar 5.9 Hasil Konfigurasi Port f0/1

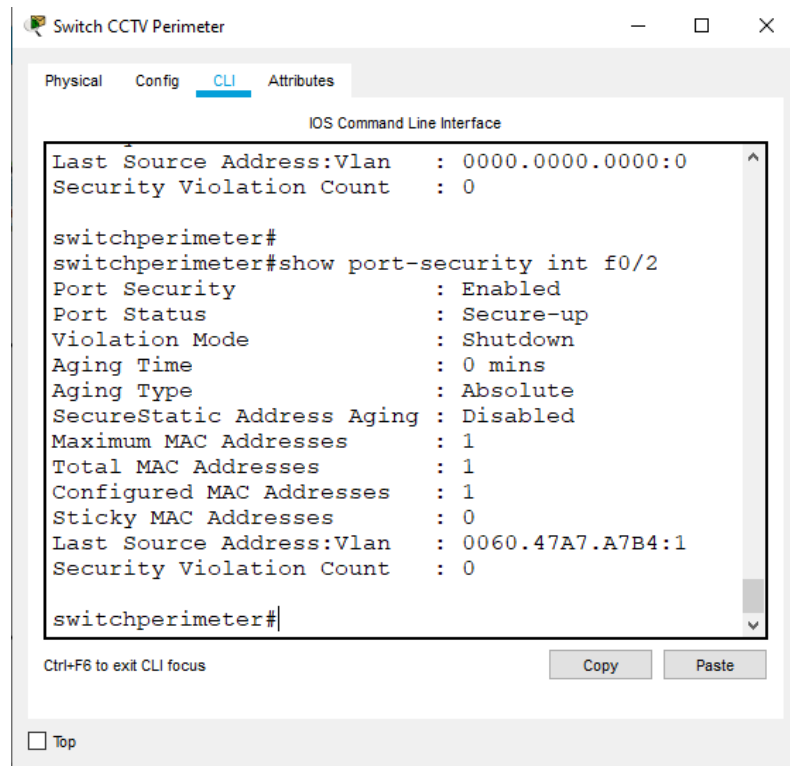
Konfigurasi pada *port fast ethernet* 0/1 khusus untuk jalur server telah selesai dilakukan, selanjutnya konfigurasi pada *port fast ethernet* 0/2 untuk koneksi PC Operator, dengan langkah-langkah :

```

switchperimeter(config)#int f0/2
switchperimeter(config-if)#switchport mode ac
switchperimeter(config-if)#switchport mode access
switchperimeter(config-if)#switchport port-secur
switchperimeter(config-if)#switchport port-security
switchperimeter(config-if)#switchport port-security mac-
switchperimeter(config-if)#switchport port-security mac-address
0060.47A7.A7B4
switchperimeter(config-if)#switchport port-security maximum 1

```

```
switchperimeter(config-if)#switchport port-security violation shutdown
switchperimeter(config-if)#no shut
```

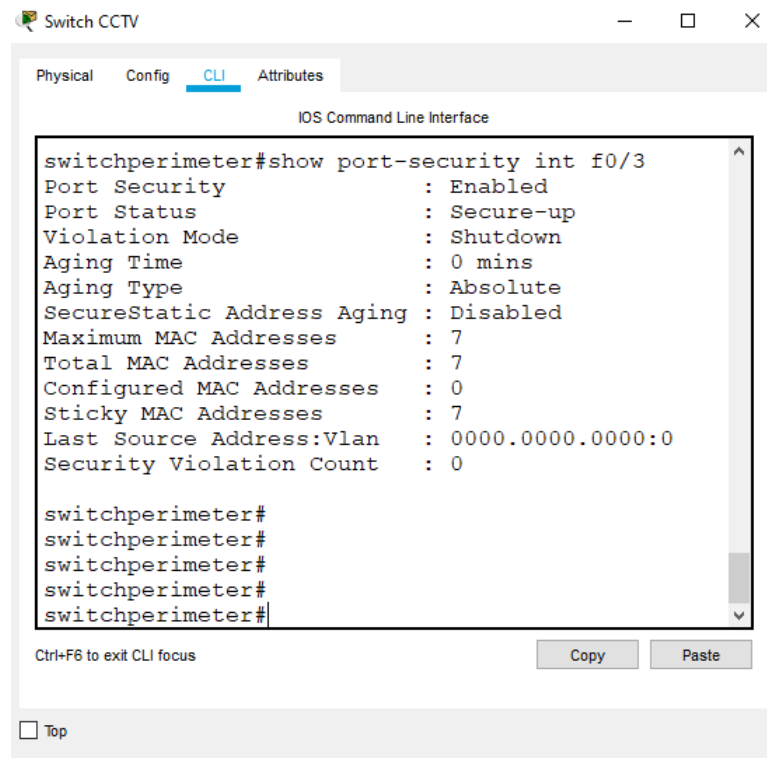


Gambar 5.10 Hasil Konfigurasi Port f0/2

Kemudian dilanjutkan konfigurasi pada *port fast ethernet f0/3* sebagai jalur untuk CCTV T.1 sampai dengan T.5, dengan langkah-langkah sebagai berikut :

```
switchperimeter#configure terminal
switchperimeter(config)#int f0/3
switchperimeter(config-if)#switchport mode access
switchperimeter(config-if)#switchport port-security
switchperimeter(config-if)#switchport port-security mac-address sticky
switchperimeter(config-if)#switchport port-security maximum 8
switchperimeter(config-if)#switchport port-security violation shutdown
```

```
switchperimeter(config-if)#no shut
```



Gambar 5.11 Hasil Konfigurasi Port f0/3

Selanjutnya konfigurasi *port fast ethernet f0/4*, dengan langkah-langkah :

```
switchperimeter(config)#int f0/4
```

```
switchperimeter(config-if)#switchport mode access
```

```
switchperimeter(config-if)#switchport port-security
```

```
switchperimeter(config-if)#switchport port-security mac-address sticky
```

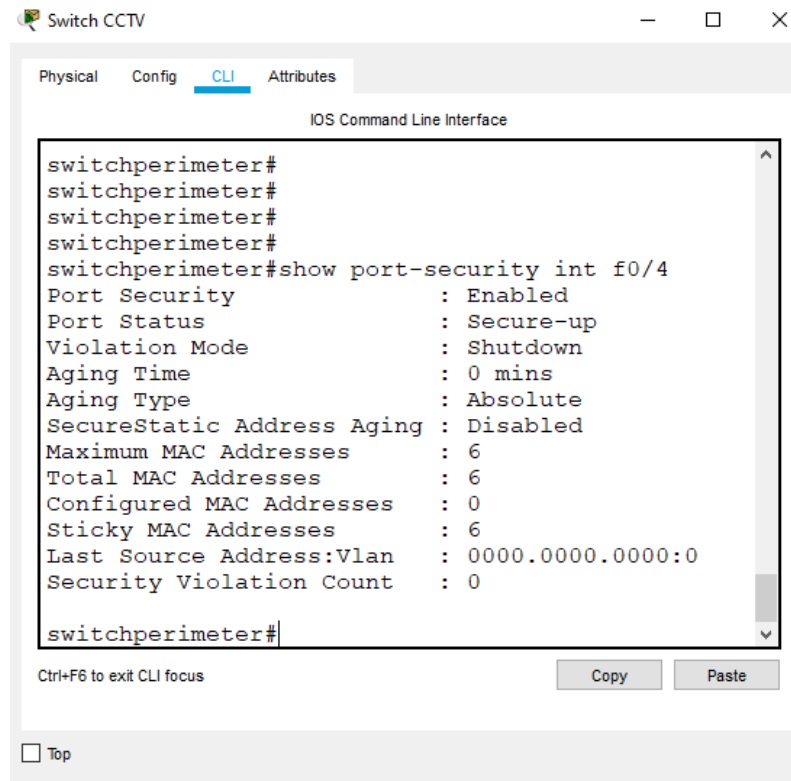
```
switchperimeter(config-if)#switchport port-security maximum 7
```

```
switchperimeter(config-if)#switchport port-security violation shutdown
```

```
switchperimeter(config-if)#no shut
```

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

```
switchperimeter#show port-security int f0/4
```



The screenshot shows a terminal window titled "Switch CCTV" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following configuration for interface f0/4:

```

switchperimeter#
switchperimeter#
switchperimeter#
switchperimeter#show port-security int f0/4
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 6
Total MAC Addresses     : 6
Configured MAC Addresses : 0
Sticky MAC Addresses    : 6
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

switchperimeter#

```

At the bottom of the terminal window, there are buttons for "Copy" and "Paste", and a "Top" button.

Gambar 5.12 Hasil Konfigurasi port f0/4

Selanjutnya dilanjutkan *port fast ethernet* f0/5, dengan langkah-langkah :

```
switchperimeter#configure terminal
```

```
switchperimeter(config)#int f0/5
```

```
switchperimeter(config-if)#switchport mode access
```

```
switchperimeter(config-if)#switchport port-security
```

```
switchperimeter(config-if)#switchport port-security mac-address sticky
```

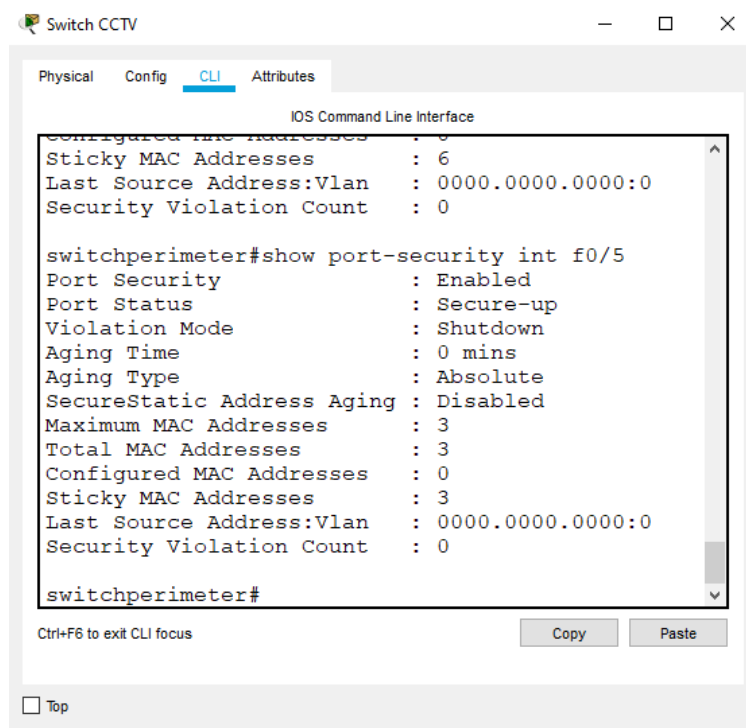
```
switchperimeter(config-if)#switchport port-security maximum 4
```

```
switchperimeter(config-if)#switchport port-security violation shutdown
```

```
switchperimeter(config-if)#no shut
```

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

```
switchperimeter#show port-security int f0/5
```



Gambar 5.13 Hasil Konfigurasi Port f0/5

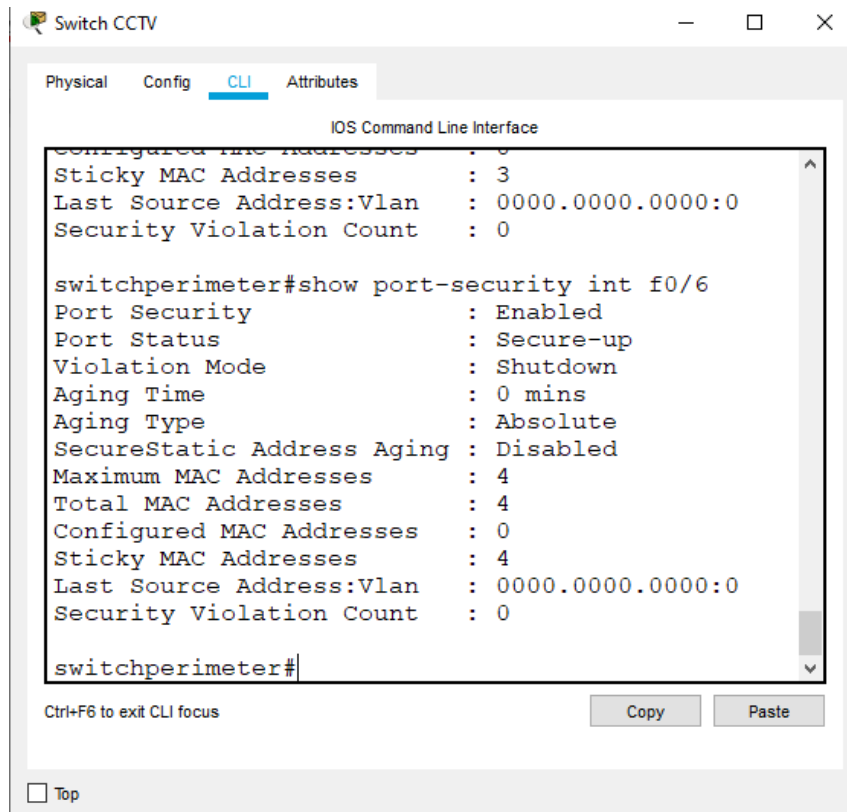
Kemudian yang terakhir lakukan konfigurasi pada *port fast ethernet f0/6* dan pada *port fast ethernet f0/7* sampai dengan *port fast ethernet f0/24* di *shutdown*.

```

switchperimeter#configure terminal
switchperimeter(config)#int f0/6
switchperimeter(config-if)#switchport mode access
switchperimeter(config-if)#switchport port-security
switchperimeter(config-if)#switchport port-security mac-address sticky
switchperimeter(config-if)#switchport port-security maximum 5
switchperimeter(config-if)#switchport port-security violation shutdown
switchperimeter(config-if)#no shut

```

```
switchperimeter(config-if)#end  
switchperimeter#configure terminal  
switchperimeter(config)#int range f0/7-24  
switchperimeter(config-if-range)#shutdown
```



Gambar 5.14 Hasil Konfigurasi Port f0/6

```

Switch CCTV Perimeter
Physical Config CLI Attributes
IOS Command Line Interface
vlan          VTP VLAN status
vtp           VTP information
switchperimeter#show interfaces status
Port          Name          Status      Vlan      Duplex  Speed Type
Fa0/1         Fa0/1         connected   1         auto    auto  10/100BaseTX
Fa0/2         Fa0/2         connected   1         auto    auto  10/100BaseTX
Fa0/3         Fa0/3         connected   1         auto    auto  10/100BaseTX
Fa0/4         Fa0/4         connected   1         auto    auto  10/100BaseTX
Fa0/5         Fa0/5         connected   1         auto    auto  10/100BaseTX
Fa0/6         Fa0/6         connected   1         auto    auto  10/100BaseTX
Fa0/7         Fa0/7         disabled 1         auto    auto  10/100BaseTX
Fa0/8         Fa0/8         disabled 1         auto    auto  10/100BaseTX
Fa0/9         Fa0/9         disabled 1         auto    auto  10/100BaseTX
Fa0/10        Fa0/10        disabled 1         auto    auto  10/100BaseTX
Fa0/11        Fa0/11        disabled 1         auto    auto  10/100BaseTX
Fa0/12        Fa0/12        disabled 1         auto    auto  10/100BaseTX
Fa0/13        Fa0/13        disabled 1         auto    auto  10/100BaseTX
Fa0/14        Fa0/14        disabled 1         auto    auto  10/100BaseTX
Fa0/15        Fa0/15        disabled 1         auto    auto  10/100BaseTX
Fa0/16        Fa0/16        disabled 1         auto    auto  10/100BaseTX
Fa0/17        Fa0/17        disabled 1         auto    auto  10/100BaseTX
Fa0/18        Fa0/18        disabled 1         auto    auto  10/100BaseTX
Fa0/19        Fa0/19        disabled 1         auto    auto  10/100BaseTX
Fa0/20        Fa0/20        disabled 1         auto    auto  10/100BaseTX
Fa0/21        Fa0/21        disabled 1         auto    auto  10/100BaseTX
Fa0/22        Fa0/22        disabled 1         auto    auto  10/100BaseTX
Fa0/23        Fa0/23        disabled 1         auto    auto  10/100BaseTX
Fa0/24        Fa0/24        disabled 1         auto    auto  10/100BaseTX
Gig0/1        Gig0/1        notconnect 1         auto    auto  10/100BaseTX
Gig0/2        Gig0/2        notconnect 1         auto    auto  10/100BaseTX
switchperimeter#
Ctrl+F6 to exit CLI focus
 Top

```

Gambar 5.15 Status Port f0/7-24 off

5.2 PENGUJIAN SISTEM

5.2.1 Pengetesan Koneksi dari Server ke Perangkat CCTV

Setelah selesai melakukan semua konfigurasi baik disisi CCTV maupun *Switch* lalu kita akan mencoba koneksi antara :

- a. Server ke CCTV

```

Server CCTV
Physical Config Services Desktop Programming Attributes
Command Prompt
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 2ms, Average = 1ms

Control-C
^C
C:\>ping 192.168.1.39

Pinging 192.168.1.39 with 32 bytes of data:

Reply from 192.168.1.39: bytes=32 time=1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
Reply from 192.168.1.39: bytes=32 time=1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.39:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>

```

Gambar 5.16 Pengujian Koneksi dari Server ke setiap Perangkat CCTV

b. Sever ke PC Operator

```

Server CCTV
Physical Config Services Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.1.39:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

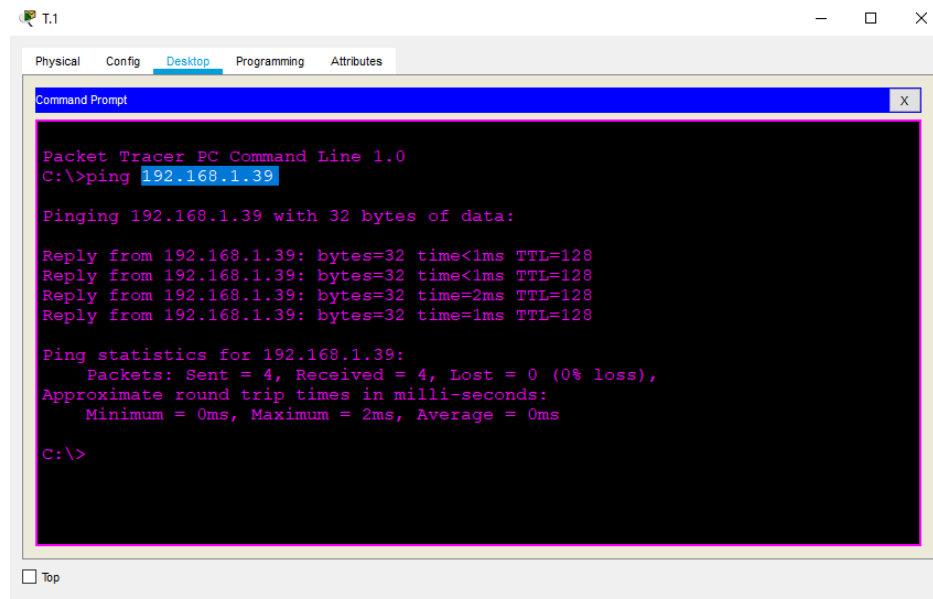
Ping statistics for 192.168.1.3:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>

```

Gambar 5.17 Pengujian Koneksi dari Server ke PC Operator

c. CCTV ke CCTV



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.39

Pinging 192.168.1.39 with 32 bytes of data:

Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
Reply from 192.168.1.39: bytes=32 time=2ms TTL=128
Reply from 192.168.1.39: bytes=32 time=1ms TTL=128

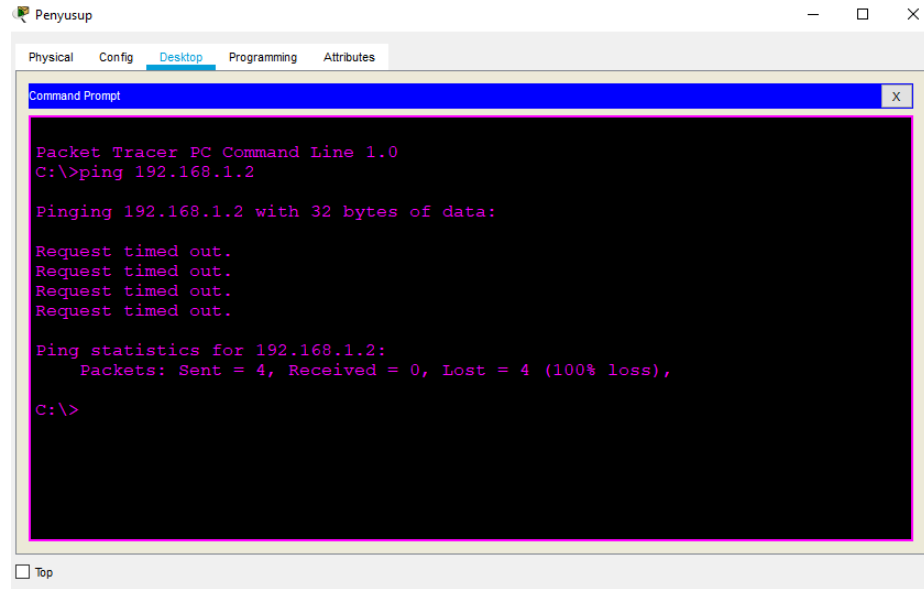
Ping statistics for 192.168.1.39:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

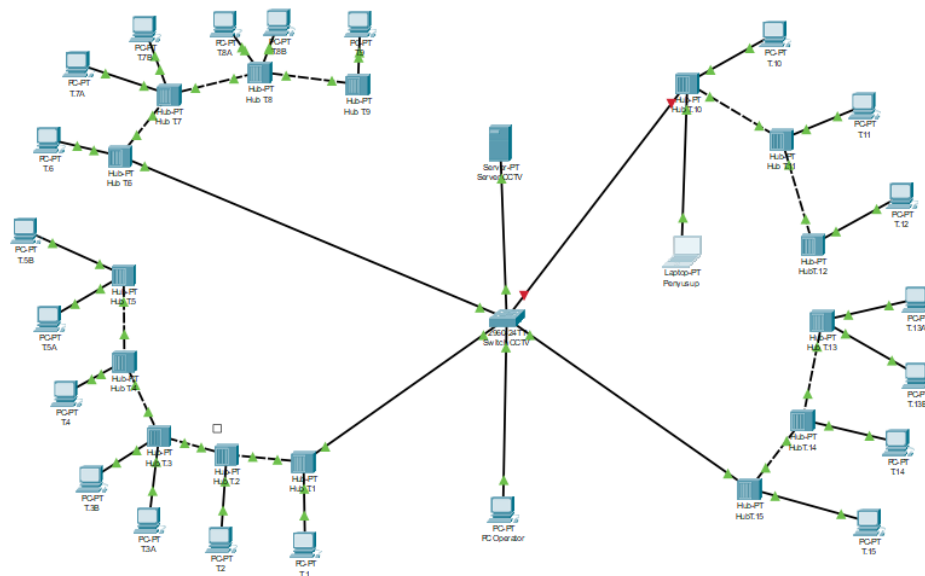
Gambar 5.18 Pengujian Koneksi dari CCTV ke CCTV

5.2.2 Simulasi Penyerangan

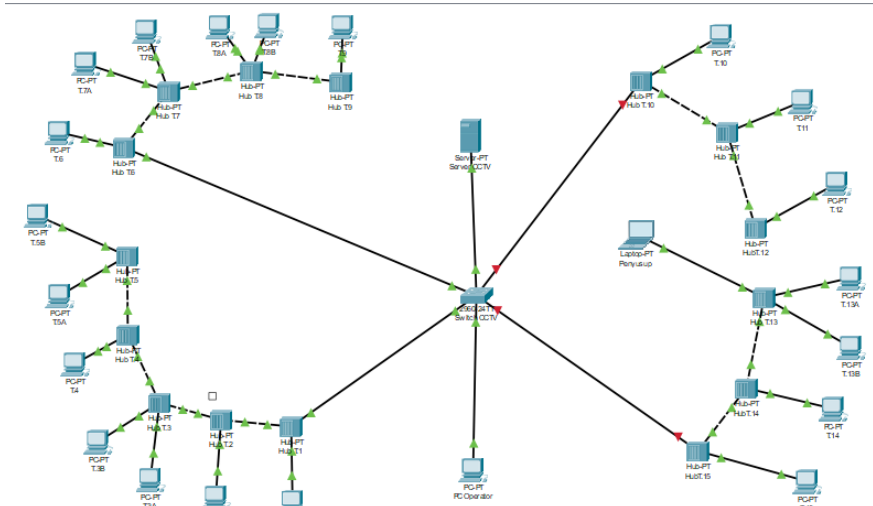
Selanjutnya siapkan 1 buah laptop sebagai *tools* untuk melakukan simulasi penyerangan, tambahkan *ip address* secara acak atau menyerupai dengan jaringan CCTV Perimeter lalu hubungkan ke setiap *port* kosong dimasing-masing *backbone* dan lihat apa yang akan terjadi pada *port* switch.



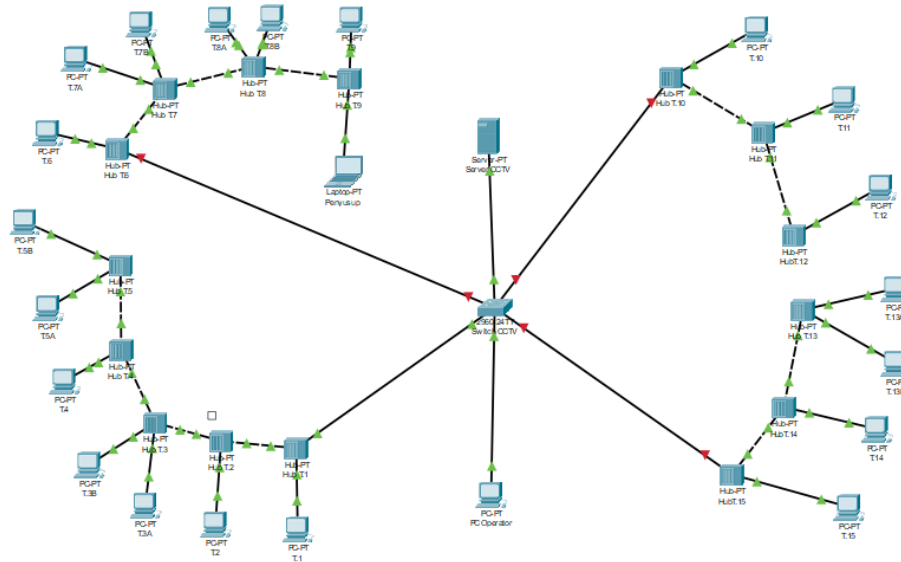
Gambar 5.19 Hasil Koneksi Laptop Penyusup ke Server



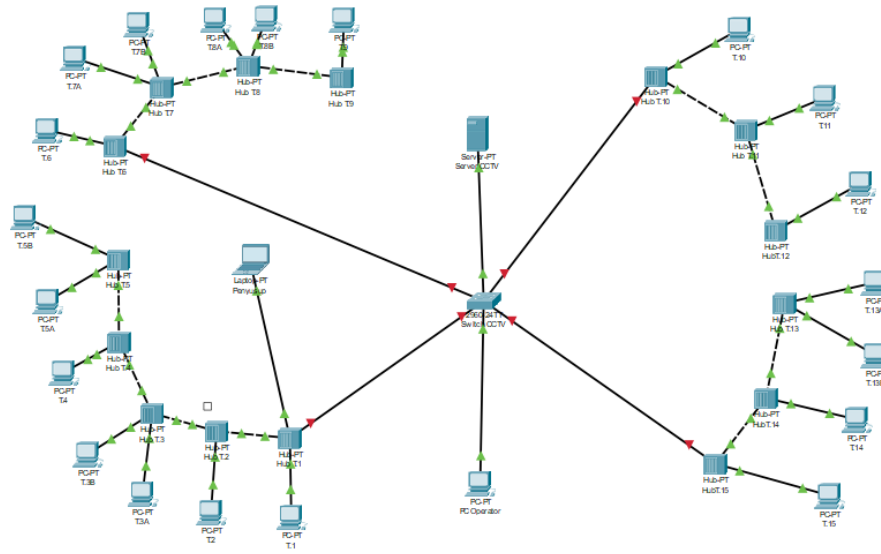
Gambar 5.20 Kondisi Port f0/5 Shutdown



Gambar 5.21 Kondisi Port f0/6 Shutdown



Gambar 5.22 Kondisi Port f0/4 Shutdown



Gambar 5.23 Kondisi Port f0/3 Shutdown