BAB IV

RANCANGAN SISTEM JARINGAN USULAN

4.1. Manajemen Jaringan Usulan

Manajemen jaringan yang akan diusulkan untuk menghadapi permasalahan yang dihadapi oleh kantor Vitta Multi Oksigen adalah diimplementasikannya keamanan jaringan *Firewall Security port* yang berfungsi untuk memberikan keamanan jaringan dan merupakan teknik yang akan mengizinkan hak akses melalui port yang tersedia diswitch cabang tersebut dengan monitoring dari pihak IT (*Information Technology*). Hal ini membuat semua karyawan yang berada di kantor tersebut dapat melaporkan jika terjadi perpindahan tempat kerja atau adanya karyawan baru yang akan mengunakan jaringan pada kantor ini, karena secara otomatis hak akses pada perangkat baru yang karyawan hubungkan keport switch akan di blok oleh port security. Dengan adanya laporan tidak dapat akses jaringan, maka pihak IT (*Information Technology*) akan membukakan hak akses dengan memastikan bahwa akses jaringan tersebut digunakan untuk kepentingan perusahaan.

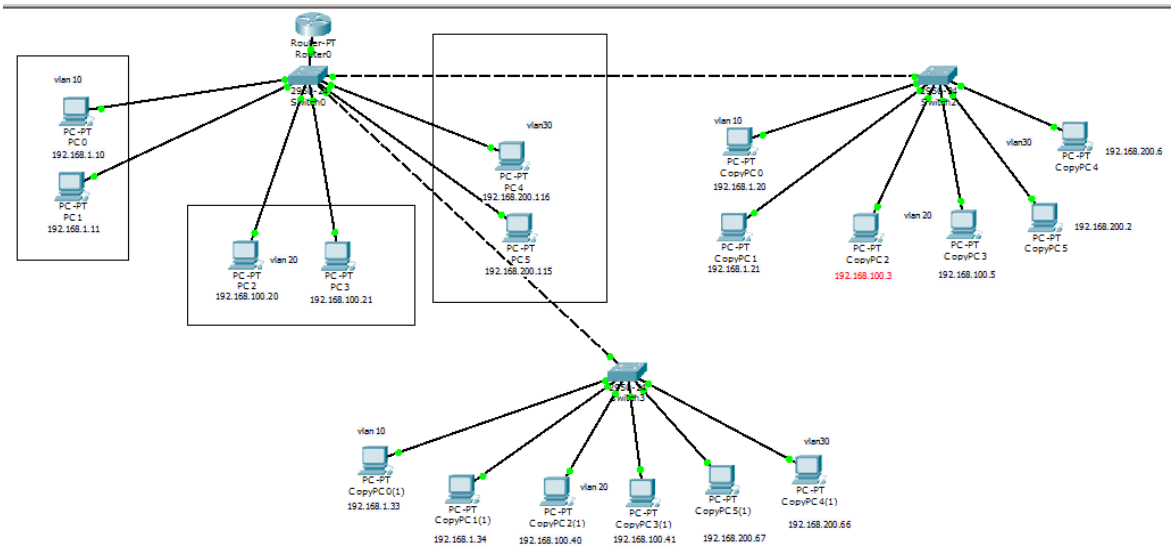
4.1.1. Topologi Jaringan

Penulis mengusulkan untuk tetap memafaatkan semua infrastruktur yang ada dengan menggunakan VLAN (*Virtual local area network*). VLAN dapat membagi jaringan ke dalam beberapa *subnetwork* dan ada beberapa keuntungan dari VLAN seperti keamanan data dari setiap divisi, penghematan dari penggunaan bandwidth dan VLAN memudahkan manajemen jaringan yang ada. Untuk pembagian bandwidth pada kantor Vitta Multi Oksigen adalah 4096Kbps.

4.1.2. Skema Jaringan

Pada penelitian ini penulis mencoba untuk menggambarkan dalam bentuk simulasi implementasi jaringan usulan tersebut menggunakan software simulator. Software yang penulis gunakan adalah *Cisco Packet Tracer*. Adapun konfigurasi jaringan usulan menggunakan software simulator dapat dilihat pada gambar IV.1 berikut

:



Gambar IV.1 Skema Usulan Jaringan

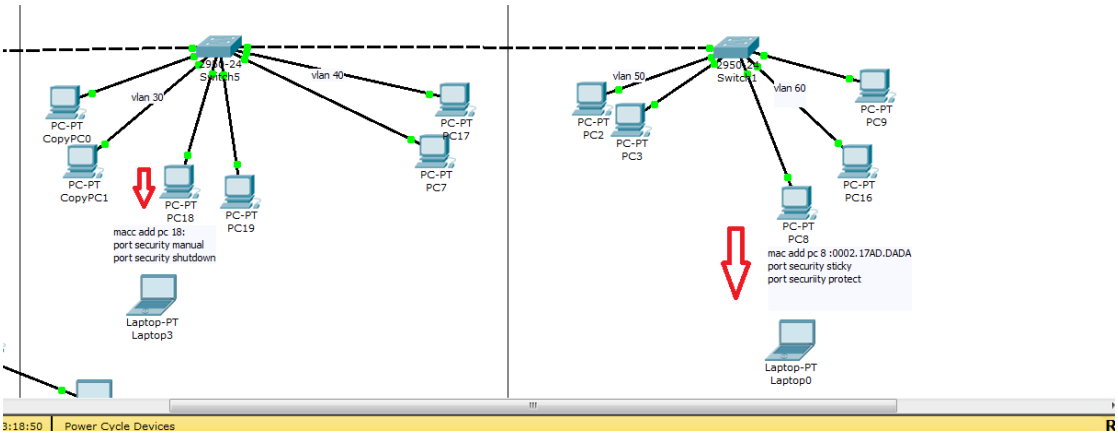
4.1.3. Keamanan Jaringan

Keamanan jaringan yang dapat penulis usulkan yaitu dengan menggunakan *Security port*. *Security Port* adalah sebuah trafik kontrol yang bekerja di layer 2 data link yang berfungsi untuk mendaftarkan dan membatasi perangkat *end devices* mana saja yang dapat terkoneksi jaringan pada suatu port di switch, untuk menjaga kerahasiaan data karyawan. *Seucrity port* yang digunakan untuk mengamankan akses jaringan data ini, menyediakan sebuah mekanisme

untuk mengamankan jaringan data dengan cara mendaftarkan mac-address dari end devices dan melakukan pemblokkan akses port apabila ada MAC address yang tidak terdaftar berusaha mengakses port. Maka dari itu penulis mengusulkan kemanan jaringan menggunakan *Security port*.

4.1.4. Rancangan Aplikasi

Dalam menetapkan keamanan jaringan yang akan diusulkan, akan dilakukan dalam sebuah simulasi. Dimana akan diberikan 3 jenis konfigurasi switch *security port* yaitu, *Default /static port security*, *Port security dynamic learning*, *Sticky port security*. Ketiga jenis konfigurasi ini yang akan diberikan pada setiap port yang ada diswitch. Dengan PC yang sudah mendaftarkan *mac address* akan terkoneksi pada jaringan, namun pada perangkat laptop tidak mendaftarkan *mac address* ,jika mengubungkan koneksi jaringan yang di pc maka akan otamatis jaringan akan di *shutdown* atau ter-*protect* (port akan tetap menyala tetapi tidak bisa digunakan). Simulasi keamanan jaringan komputer Port Security menggunakan software simulator *Cisco Packet Tracer*. Adapun gambar simulasi yang dilakukan adalah sebagai berikut :



Gambar IV.2
Tampilan jaringan port security di Cisco Packet Tracer

4.1.5. Manajemen Jaringan

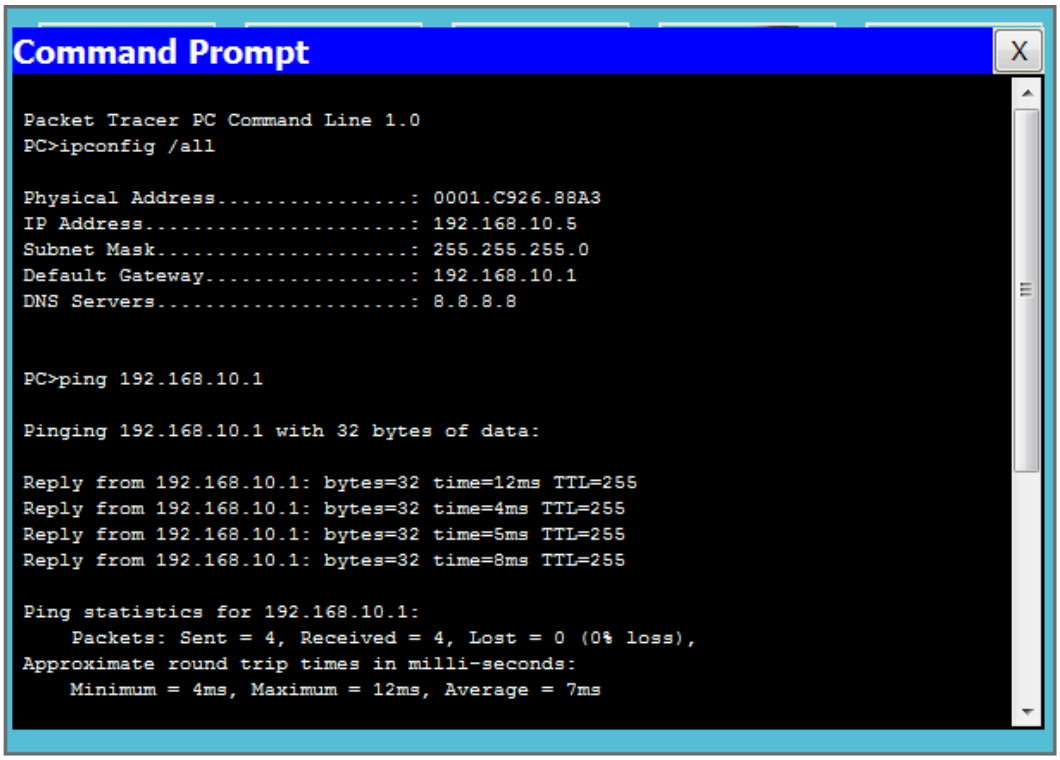
Untuk manajeman jaringan yang akan diusulkan, masih mengunakan VLAN (*Virtual local area network*) sebagai pembagi ip atau jaringan di beberapa subnetwork, yang terbagi dibeberapa segmen yaitu terdapat segmen untuk management switch dan segmen data.

4.2. Pengujian Jaringan

Pada pengujian system keamanan jaringan dengan *Security port* menggunakan software *cisco packet tracer* dengan melakukan ping dan *capture* aliran data, serta menjelaskan cara kerja port security dalam sytem jaringan komputer.

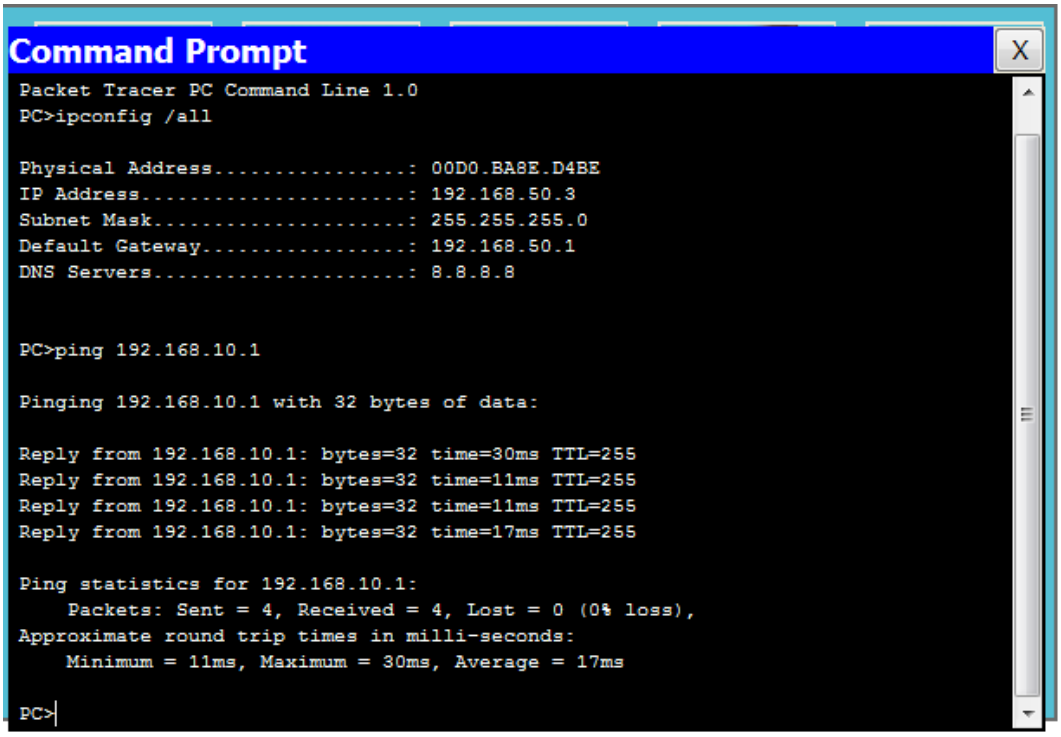
4.2.1. Pengujian Jaringan Awal

Pengujian jaringan awal keamanan jaringan dilakukan dengan melakukan percobaan koneksi jaringan antara *client* kantor dengan perangkat yang digunakan komputer yg berbeda vlan. Dalam pengujian awal ini, menggunakan *software* paket *Tracert* yang sudah di *routing* dan *switching.* Switch yang di konfigurasi tanpa mengunakan *Security port*. Pengujian dihubungkan pada jaringan dan test ping pada gateway ip 192.168.10.1 dengan vlan 10 ip 192.168.10.5 dan pada segmen lain ip 192.168.30.2 vlan 30 menggunakan software cisco packet Tracert yang sudah di *routing.*



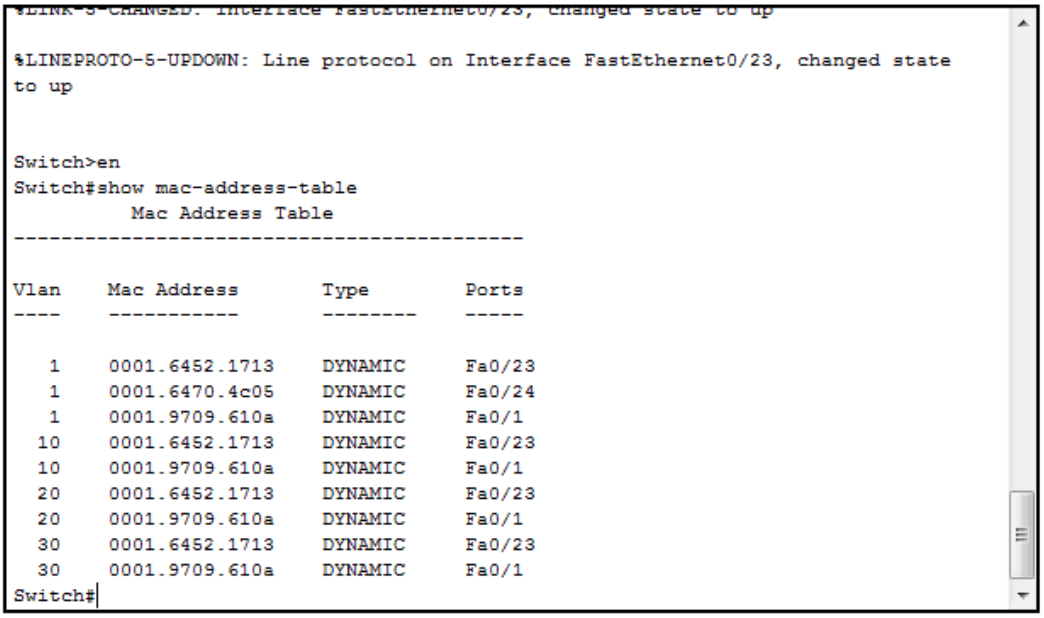
Gambar IV.3 Hasil Tes Ping vlan 10 lt 1 ke vlan 30 lt2

Dari gambar di atas dapat dilihat bahwa ping dapat berjalan dengan lancar tanpa terputus. Hal ini menunjukan bahwa jaringan sudah terkoneksi otomatis tanpa adanya keamanan jaringan yang mendeteksi detail perangkat yang terhubung. Kemudian pada komputer tersebut melakukan perpindahan lokasi kerja ke lantai berbeda tanpa adanya informasi perpindahan, untuk informasi koneksi jaringan akan dilakukan test ping pada komputer kantor vitta multi lantai 3 dengan segmen IP sumber 192.168.10.1 segmen ip reouter kantor vitta multi dengan PC ip 192.168.50.2 gateway 8.8.8.8 dengan menggunakan software *software cisco packet Tracert*.



Gambar IV.4 Test ping paket data kantor Vitta Multi

Pada gambar *IV.4* paket data dikirim dari lantai 2 vlan 30 kantor vitta multi ke lantai 1 vlan 10 mendapat tingkat kesuksesan 100 persen walau pun tanpa ada *lost*.



Gambar IV.5 Mac address table

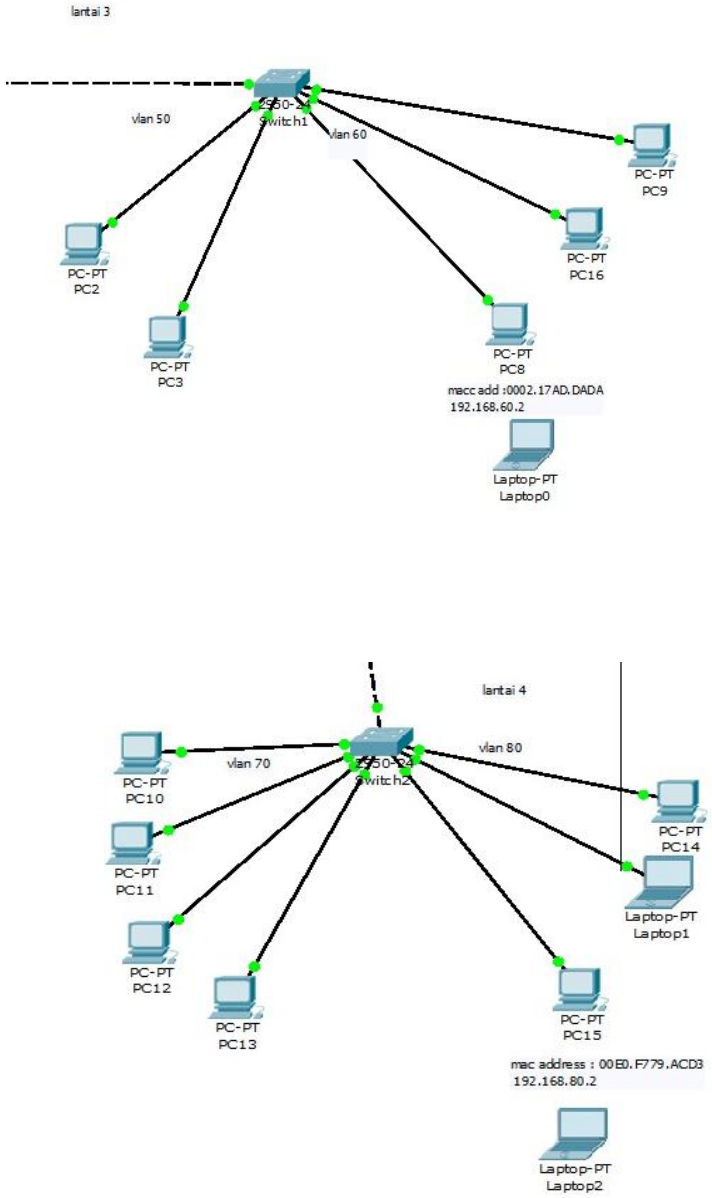
Pada gambar *IV.5* terlihat bahwa mac address dari perangkat yang terkoneksi, namun tidak terjadi manajemen dan system keamanan jaringan yang baik. Karena setiap perangkat yang dihubungkan pada jaringan tersebut bersifat dynamic dan dapat selalu terkoneksi karena tidak adanya security pada setiap port akses.

4.2.2. Pengujian Jaringan Akhir

Dengan keamanan jaringan mengunakan *Security port*, dalam hal ini penggunaan security port sangat perlu diterapkan karena setiap perangkat user akan menginformasikan mac address-nya dan terdeksripsi dalam port yang digunakan. Hal ini akan menjadi lebih aman dalam pemberian akses pada jaringan yang ada. Dalam pengujian ini terdapat 2 metode yang akan di impelemtasikan pada jaringan keamanan pada kantor vitta multi yaitu, dengan *security port dynamic learning dan sticky port security*.

Uji coba akan dilakukan dengan pemberian konfigurasi pada switch yang digunakan, pengujian ini akan dilakukan pada kantor vitta multi dengan

mengunakan 2 switch akses. Pada semua switch diberikan *port security dynamic learning dan sticky port security.*



Gambar IV.7 Tes koneksi pada perangkat di packet tracer

Pada switch 192.168.50.0 dan 192.168.70.0
Switch(config)#int ra fa0/1-2

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport port-security

Switch(config-if-range)#switchport port-security mac-address sticky

Switch(config-if-range)#switchport port-security violation restric

Switch(config-if-range)#ex

Switch(config)#int fa0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

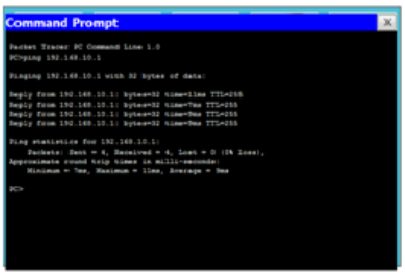
Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#ex

Switch(config)#ex

Pada konfigurasi yang digunakan switch port port-security untuk mac address perangkat pada setiap port switch hanya 1 perangkat. Dalam hal ini port security sticky dan dynamic learning sudah di buat.



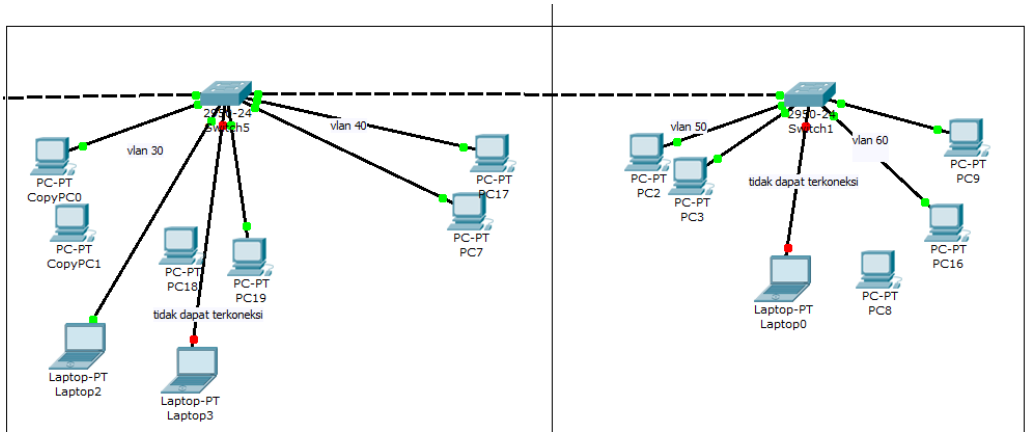
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int ra fa0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation restric
Switch(config-if-range)#ex
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#ex
Switch(config)#ex

Gambar IV.8 Tes ping ke router dan deskripsi mac address perangkat

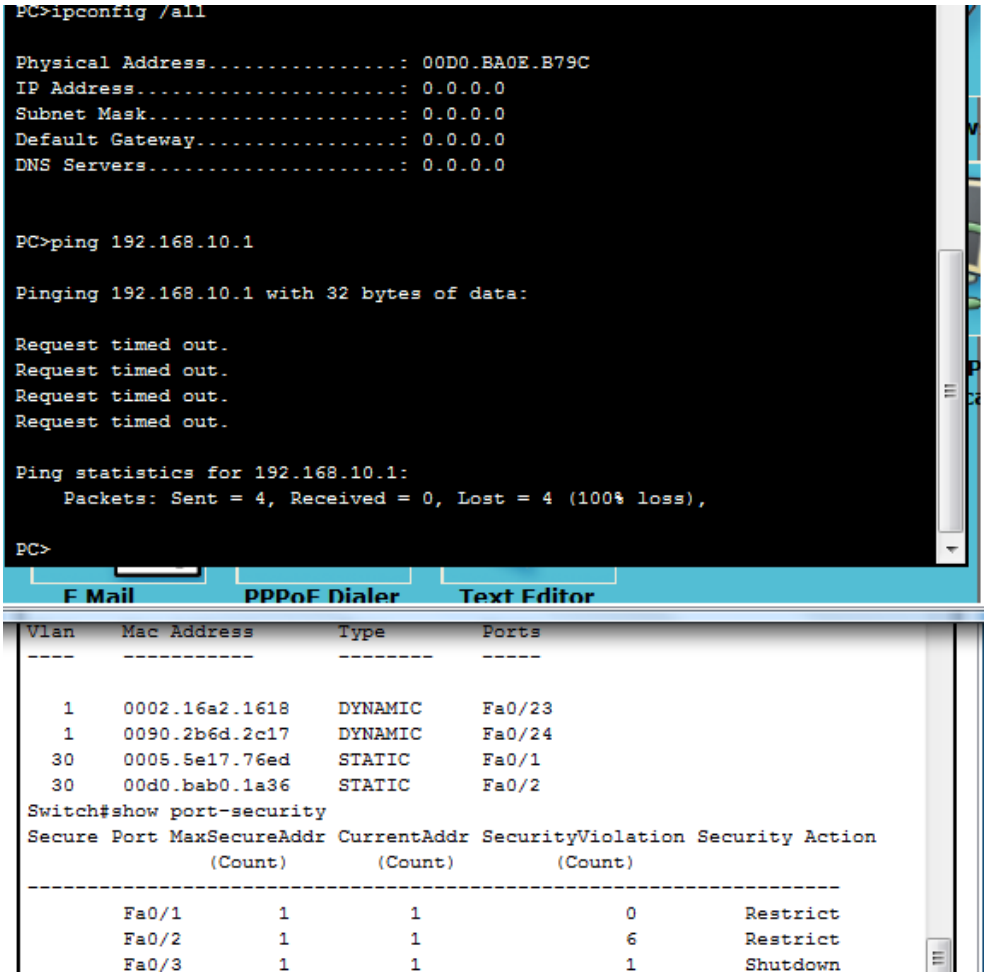
Pada gambar *IV.8* terlihat bahwa mac address dari perangkat yang terkoneksi akan menambahkan macc address secara otomatis, kemudian hasil ping masih dapat berjalan. Dalam hal ini perangkat yang didaftarkan pertama dan kedua akan terkoneksi pada jaringan yang ada, namun jika perangkat yang terkoneksi tidak sesuai dengan macc addressnya maka port pada switch akan otomatis shutdown atau protect.

```
Switch#show mac-address-table
        Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  1    0030.a332.2e5e    DYNAMIC     Fa0/24
 50    0005.5e52.9696    STATIC      Fa0/1
 50    0060.5c83.da4c    DYNAMIC     Fa0/24
 50    00d0.ba8e.d4be    STATIC      Fa0/2
 60    0002.168e.750c    STATIC      Fa0/5
 60    0010.1100.eaa3    STATIC      Fa0/6
 60    0060.3e24.0dc4    STATIC      Fa0/7
 60    0060.5c83.da4c    DYNAMIC     Fa0/24
```

Selanjutnya akan dilakukan pengujian dengan menghubungkan pc client dengan memindah koneksi pada laptop1 dan laptop2.



Gambar IV.9 Tes koneksi pada perangkat baru



Gambar IV.10 Tes ping ke router dan show port security

Pada gambar *IV.10* terlihat bahwa mac address dari perangkat baru yang terkoneksi tidak mendapatkan ip atau akses, dikarenakan mac address tidak sesuai dengan yang ditentukan, dengan begitu maka laptop1 dan laptop2 tidak dapat terkoneksi pada jaringan lain. Kegunaan port security mampu memberikan keamanan jaringan yang dapat berjalan dengan baik, sehingga bila perangkat tersebut ingin terkoneksi kembali harus dilakukan penghapusan mac address pada switch yang dilakukan oleh pihak IT. Hal ini dapat membantu dalam memanajemen lokasi kerja user setiap lantai dan mensegmentasikan ip sesuai lantai.

Berikut pengujian untuk menghapus *mac address* yang terblok oleh port security, agar dapat terkoneksi pada jaringan yang ada.

```
Switch>en
Switch#clear port-security all
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/1-8
Switch(config-if-range)#shutdown
Switch(config-if-range)#no shutdown
Switch>en
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)     (Count)       (Count)
---------------------------------------------------------------------
```

Fa0/1	1	0	0	Shutdown
Fa0/2	1	0	0	Shutdown
Fa0/3	1	0	0	Shutdown
Fa0/4	1	0	0	Shutdown
Fa0/5	1	1	0	Shutdown
Fa0/6	1	0	0	Shutdown
Fa0/7	1	0	0	Shutdown
Fa0/8	1	0	0	Shutdown

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#int range fa0/1-2

Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

Switch(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch(config-if-range)#int fa0/3

Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if)#ex

Switch(config)#ex

%SYS-5-CONFIG_I: Configured from console by console

Switch#

Switch#

Switch(config)#int fa0/3

Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

Switch>en

Switch#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

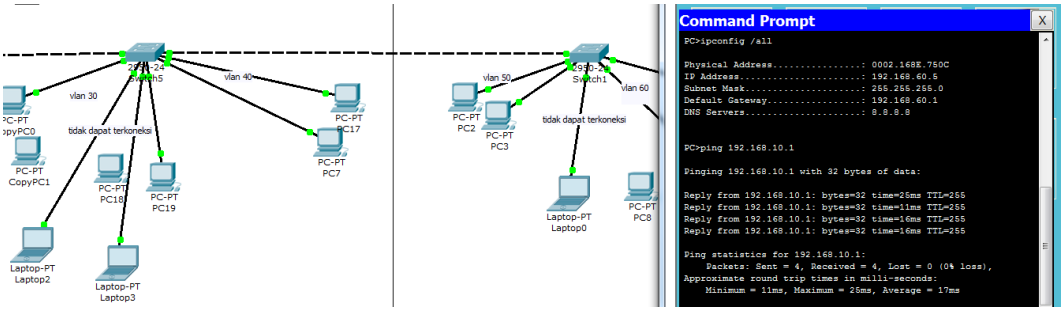
Fa0/1 1 0 0 restrict

Fa0/2 1 0 0 restrict

Fa0/3 1 0 0 restrict

Fa0/4 1 0 0 Shutdown

Fa0/5	1	1	0	Shutdown
Fa0/6	1	0	0	Shutdown
Fa0/7	1	0	0	Shutdown
Fa0/8	1	0	0	Shutdown



Gambar IV.11 Tes ping ke pc kantor lt 3 dan lt 4 ke router lt 1

Pada gambar *IV.10* terlihat bahwa laptop 1 mendapatkan ip dan dapat terkoneksi pada jaringan. Test ping ke pc kantor lantai 3 dan lantai 4 berhasil ke router lantai 1 tanpa ada *packet lost*.