Krea-TIF: Jurnal Teknik Informatika
http://ejournal.uika-bogor.ac.id/index.php/krea-tif
p-ISSN: 2338-2910, e-ISSN: 2658-5836
Vol. 10, No. 1, Mei 2022, pp. 10 - 18
DOI: 10.32832/kreatif.v10i1.6678

Model Keamanan Jaringan Menggunakan *Firewall Port Blocking*

Sartomo, Wiwin Sulistyo
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Indonesia
*E-mail koresponden: 672017404@student.uksw.edu

Diserahkan *31 Januari 2022;* ***Direview*** *23 Februari 2022;* ***Dipublikasikan*** *30 April 2022*

Abstrak

Keamanan merupakan unsur yang sangat penting pada jaringan komputer. Hal ini dilakukan dalam upaya memberikan perlindungan pada jaringan komputer untuk mencegah ancaman-ancaman baik dari internal maupun eksternal dalam upaya mencegah pengambilan data secara paksa (tidak sah). Sistem keamanan jaringan perlu dibangun untuk mengontrol akses pada aset-aset yang penting, salah satunya data, sehingga hak akses setiap komputer maupun user perlu diatur. Metode port blocking menjadi salah satu teknik yang dapat digunakan dalam mengatur akses dari user maupun komputer. Port blocking dapat digunakan untuk mengatur hak akses jaringan pada setiap port LAN (Local Area Network). Secara spesifik pengaturan port yang berbeda dengan metode default atau static port security, port security dynamic learning dan sticky port security dapat dilakukan. Hal ini sangat berguna untuk menghalangi akses dari pihak satu ke pihak lain untuk mencegah terjadinya pencurian data dari orang tidak dikenal maupun yang dikenal. Dari pengujian yang dilakukan diketahui bahwa penerapan firewall security port dapat melakukan aksi block pada koneksi jaringan tersebut ketika terjadi perpindahan hak akses..

Kata kunci: *Network security, Hak akses, Port security, Firewall*

Abstract

Security is a very important element in computer networks. This is done in an effort which provide protection to the computer network preventing threats from both internal and external in an effort to prevent forced (illegal) data retrieval. A network security system needs to be built to control access to important assets, which is called data, so that access rights for each computer and user need to be regulated. The port blocking method is one of the techniques that can be used to regulate access from users and computers. Port blocking can be used to set network permissions on each LAN port (Local Area Network). Specifically, different port settings with the default method or static port security, dynamic learning port security and sticky port security can be done. This is very useful for blocking access from one party to another to prevent data theft from unknown and known people. From the tests carried out, sticky port security can run well according to the given performance.

Keywords: *Network security, Access rights, Port security, Firewall*

PENDAHULUAN

Perkembangan teknologi informasi khususnya teknologi jaringan komputer menyebabkan banyaknya layanan data yang dapat dilewatkan melalui teknologi tersebut. Peningkatan layanan tentu saja juga berdampak pada jumlah pengguna yang memanfaatkan teknologi tersebut, baik dalam bidang pemerintahan, bisnis, industri maupun pendidikan. Dampak selanjutnya adalah masalah ancaman dan keamanan yang perlu diperhatikan. Oleh sebab itu, sistem keamanan jaringan perlu dibangun untuk memberikan perlindungan terhadap ancaman yang dapat menyebabkan jaringan tidak dapat bekerja semestinya bahkan dapat mengakibatkan jaringan tidak mampu beroperasi. Disisi lain ancaman juga dapat menyebabkan adanya akses ke sumberdaya bahkan pencurian dari pihak yang tidak berwenang [1][2].

Potensi ancaman terhadap keamanan jaringan dapat terjadi baik dari pihak pengguna internal maupun eksternal. Hal tersebut terutama terjadi ketika jaringan lokal atau *Local Area Network* (LAN) terhubung ke jaringan publik. Ancaman bisa terjadi dengan target yang bermacam-macam, baik pada infrastruktur maupun aset lembaga serta pribadi. Oleh sebab itu, perlindungan terhadap jaringan komputer sangat dibutuhkan terutama ketika koneksi ke jaringan publik (*internet*), karena seluruh potensi kerentanan akan diekspos oleh pihak-pihak yang berniat melakukan serangan [3].

Virtual Local Area Network (VLAN) diciptakan sebagai salah satu solusi yang dapat memberikan fleksibilitas terhadap keterbatasan LAN. Meskipun demikian ancaman keamanan pada jaringan VLAN tetap perlu dilakukan, salah satunya dengan *firewall port blocking*. Pencurian data merupakan hal yang patut dicegah oleh sebuah perusahaan sehingga perlunya keamanan dari jaringan tersebut dengan perangkat yang mampu mengontrol hak akses jaringan yaitu dengan *firewall port blocking*, terlebih banyak perusahaan masih belum menggunakan keamanan jaringan. *Port scanning* merupakan aktivitas untuk mengidentifikasi informasi serta status *port* yang terbuka ke komputer. *Port* memiliki penggunaan yang sah dalam mengelola jaringan [4].

Penelitian ini bertujuan mengembangkan keamanan jaringan komputer yaitu dengan metode *default atau static port security*, *port security dynamic learning* dan *sticky port security*, *static port security*, *port security dynamic*, *sticky port security*. *Sticky port security* adalah keamanan jaringan yang bekerja secara otomatis menggunakan MAC *Address* yang sudah terdaftar pada setiap komputer yang tidak dapat ditukar. Setiap perangkat jaringan memiliki MAC *Address* yang berbeda satu dengan lainnya [5]. *Static port security* merupakan metode pemberian IP secara manual pada tiap PC yang dapat dilakukan administrator, *port security dynamic learning* adalah salah satu metode pemberian IP secara otomatis pada tiap PC dan secara otomatis mendapatkan IP dari *router*. Selain itu penggunaan *port blocking* merupakan salah satu protokol keamanan jaringan komputer. Adapun topologi jaringan yang dibuat dalam penelitan ini yaitu topologi *star* sebuah jaringan yang didalamnya terdapat *router* dan beberapa klien [6]. Penelitian ini memberikan solusi keamanan jaringan menggunakan *port blocking* dalam mengontrol MAC *Address* yang terhubung secara tidak dikenal dan akan melakukan mode aksi *restrict, shutdown* dan *protect*.

METODE PENELITIAN

Metode penelitian ini merupakan tahapan yang disusun sistematis bertujuan dalam memperoleh hasil yang baik.

Gambar 1. Tahapan Penelitian

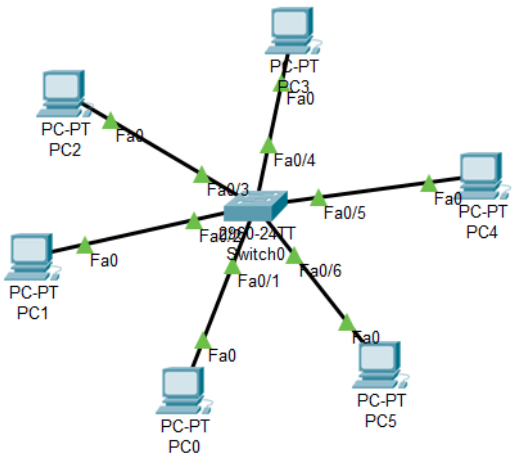
Pada Gambar 1 merupakan langkah-langkah dalam mengimplementasikan keamanan jaringan menggunakan *firewall port blocking*. Langkah-langkah yang harus dilakukan sebelum membangun model keamanan jaringan *firewall port blocking* yaitu pertama, topologi jaringan merupakan suatu koneksi untuk menghubungkan antara dua atau lebih komputer, yang didasarkan unsur-unsur penyusun jaringan. Kedua, implementasi topologi jaringan yaitu perancangan atau konsep untuk melakukan penelitian yang akan dilakukan. Ketiga, pengujian jaringan, merupakan tahapan yang dilakukan dalam pengujian koneksi jaringan yang berfungsi untuk mengontrol MAC *Address* yang tidak dikenal sehingga akan melakukan mode *restrict*, *shutdown* dan *protect*. Keamanan jaringan ini menggunakan metode *default* atau *static port security*, *port security dynamic learning* dan *sticky port security.*

Switch yang digunakan dalam pengujian tersebut akan dilakukan pengelompokan berdasarkan *port* yang ada pada jaringan komputer LAN. Kegunaan *port* sangat banyak menjadi penghubung dalam kegunaaan jaringan sehingga membentuk sebuah topologi jaringan LAN pada topologi *star*.

Pada *sticky port security* di dalamnya masih terdapat penerusnya yaitu *port security violation sticky* yang cara kerja *violation* ini memberikan pilihan mode yaitu *shutdown* (*port* akan otomatis mati), *restrict* ialah dimana *packet* tidak akan dihentikan namun dicatat dan tidak diberi ijin masuk dan *protect* akan melakukan *drop* pada *packet* agar tidak bisa terhubung.

Static port security melakukan pemberian alamat IP secara *static* yang membutuhkan waktu lama sehingga dapat berpengaruh negatif terhadap administrator.

Cara pengaturan IP *address* terdapat pada *Command Line Interface* (CLI). Persediaan otomatis pemberian IP dengan *Dynamic Host Configuration Protocol* (DHCP) ini dapat mempercepat waktu administrator dalam pemberian IP *address*. Perancangan ini memerlukan topologi jaringan yang baik seperti pada Gambar 2.



Gambar 2. Topologi jaringan

Bentuk topologi yang sering digunakan adalah *bus, token, ring*, dan *star*, dimana topologi ini sering diterapkan oleh perusahaan [7]. Topologi *star extended* [8] merupakan perancangan bentuk topologi yang akan digunakan pada penelitian ini. Rangkaian dalam pengembangan jaringan

komputer LAN sesuai dengan kebutuhan dari tiap komputer *client* terdapat pada tiap alur jaringan yang nantinya diterapkan.

Penerapan dalam pemberian alamat IP secara *static* akan berpengaruh negatif terhadap kinerja admin yang memerlukan waktu cukup lama apabila pemberian IP masih dilakukan satu persatu. Upaya mengatasi permasalahan ini dalam mengurangi waktu pengerjaannya ialah dengan menerapkan DHCP untuk pemberian alamat IP secara otomatis dari *router*. Admin jaringan cukup memilih DHCP atau obtain IP *address automatically* pada pemberian alamat IP [9].

HASIL DAN PEMBAHASAN

Manajemen keamanan usulan

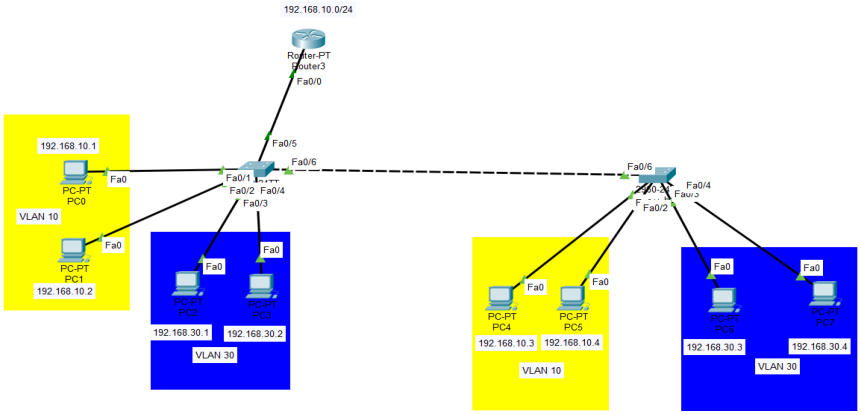
Pengembangan sebuah sistem keamanan jaringan dilakukan untuk menghadapi permasalahan yang terjadi pada suatu model jaringan. Keamanan jaringan *firewall security port* memiliki fungsi untuk memberikan keamanan pada jaringan dengan memonitor suatu jaringan melalui *switch*, dan memberikan hak akses melalui *port* yang terdapat pada *switch*.

Usulan topologi jaringan

Penerapan sistem agar berjalan dengan optimal melalui instalasi *software* [10]. Topologi yang akan dibangun ini mensimulasikan model keamanan jaringan menggunakan *software* simulator yaitu *Cisco Packet Tracer* menggunakan implementasi topologi *star*.

Gambar 3 adalah tahap perancangan topologi jaringan *port blocking* sebagai panduan dalam mempermudah alur keamanan jaringan yang dibangun. Topologi tersebut terdiri dari 1 router, 2 *switch* dan 8 komputer yang masing-masing *port* memiliki MAC *address*.

Pada tahap ini akan dibahas berbagai konfigurasi jaringan untuk membuat simulasi jaringan lokal komputer [11]. Tahap selanjutnya dilakukan perancangan protokol topologi jaringan yang terdiri dari 2 *switch* dan 8 komputer. Dari kedua *switch* ini akan dibagi menjadi 2 VLAN yaitu VLAN 10 yang berwarna kuning dan VLAN 30 yang berwarna biru. Dari kedua VLAN ini akan dilakukan konfigurasi IP *client* sesuai dengan DHCP *server* dengan *range* IP 172.20.0.0/24 – 172.47.255.254/24. *Default gateway* masing-masing *client* VLAN 10 menggunakan IP 192.168.10.1/24 dan VLAN 30 menggunakan IP 192.168.30.1/24.



Gambar 3. Topologi Jaringan

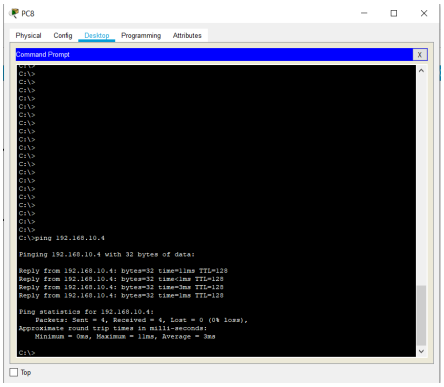
Pengujian jaringan tahap awal

Penelitian ini melakukan pengujian koneksi antara jaringan *client* dan perangkat yang digunakan komputer antar VLAN. Tahap ini menggunakan *Software Paket Tracer* yang

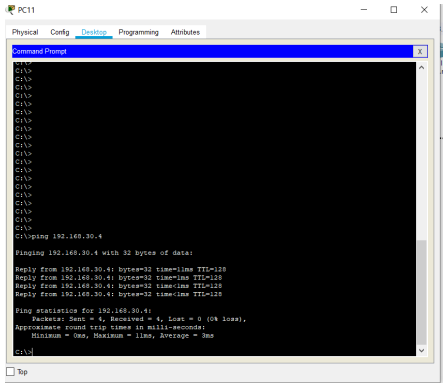
sebelumnya telah dilakukan *routing* dan *switching*. *Switch* yang terkonfigurasi dan belum menggunakan *security port* akan dihubungkan langsung pada jaringan kemudian dilakukan pengujian *ping* pada komputer ke *gateway* IP 192.168.10.2 dengan sesama VLAN 10 IP 192.168.10.4.

Gambar 4 merupakan hasil pengujian *ping* dimana jaringan dapat bekerja dengan lancar dan sukses walaupun tanpa keamanan jaringan. Pengujian dilakukan terhadap VLAN 30 dengan pengujian *ping* dari IP 192.168.30.2 kepada 192.168.30.5 dan pengujian *ping* ke VLAN 10 dengan IP 192.168.10.3 berjalan dengan sukses dan tanpa kendala. Pengujian *ping* ke segmen lain pada VLAN 30 IP 192.168.80.4 menggunakan *Cisco Packet Tracer* yang telah di routing.

Gambar 5 menunjukan bahwa hasil pengujian *ping* antar VLAN 30 berjalan lancar dengan tingkat kesuksesan 100 persen tanpa adanya *lost*.



Gambar 4. Test Ping VLAN 30



Gambar 5. Test Ping VLAN 30

Pengujian tahap awal ini terdapat suatu MAC *Address* yang terhubung namun belum menggunakan manajemen keamanan jaringan, dikarenakan setiap penghubung jaringan di perangkat tersebut masih menggunakan sistem dinamis yang dapat terhubung serta belum menerapkan *security* pada *port*.

Pengujian Jaringan Tahap Akhir

Pada tahap ini akan melakukan implementasi model keamanan jaringan menggunakan *security port* atau *port blocking* yang sangat perlu diterapkan dalam perangkat *user*. Informasi akan diberikan oleh *user* apabila MAC *address* telah digunakan pada *port* yang ada. Tahapan pengujian ini diimplementasikan menggunakan metode *sticky port security* dan *security port dynamic learning*.

Percobaan ini menggunakan dua *switch* akses yang masing-masing akan dikonfigurasi dengan memberikan *sticky port security* dan *security dynamic learning.* Konfigurasi yang digunakan dapat dilihat pada Gambar 6, Gambar 7 dan Gambar 8.

```
Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0002.1651.0080:10
Security Violation Count   : 0
```

```
#int fa0/1
#switchport mode access
#switchport port-security
#switchport port-security
mac-address sticky
#switchport port-security
violation shutdown
#ex
```

Gambar 6. *Konfigurasi Violation Mode Shutdown*

```
Switch#show port-security int
Switch#show port-security interface fa0/3
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

```
#int fa0/3
#switchport mode access
#switchport port-security
#switchport port-security
mac-address sticky
#switchport port-security
violation restrict
#ex
```

Gambar 7. *Konfigurasi Violation Mode Restrict*

```
Switch#show port-security interface fa0/4
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

```
#int fa0/4
#switchport mode access
#switchport port-security
#switchport port-security
mac-address sticky
#switchport port-security
violation protect
#ex
```

Gambar 8. *Konfigurasi Violation Mode Protect*

Konfigurasi tersebut menggunakan *switch port security* yang mana MAC *address* pada perangkat setiap *switch* terdapat hanya satu perangkat, sehingga dapat dikatakan bahwa *port security sticky* dan *dynamic learning* telah dibuat. MAC *address* secara otomatis akan terkoneksi, jika MAC *address* perangkat yang terkoneksi tersebut tidak sesuai maka akan secara otomatis *port* di *switch* akan melakukan mode aksi *shutdown*, *protect* atau *restrict*.

Gambar 9 menunjukkan bahwa MAC *address* terbagi pada setiap *port* terdapat dua tipe yaitu *dynamic* dan *static*. *Dynamic* merupakan penentuan jalur *routing* secara otomatis oleh *router* itu sendiri sedangkan *static* pembagian jaringan secara manual.

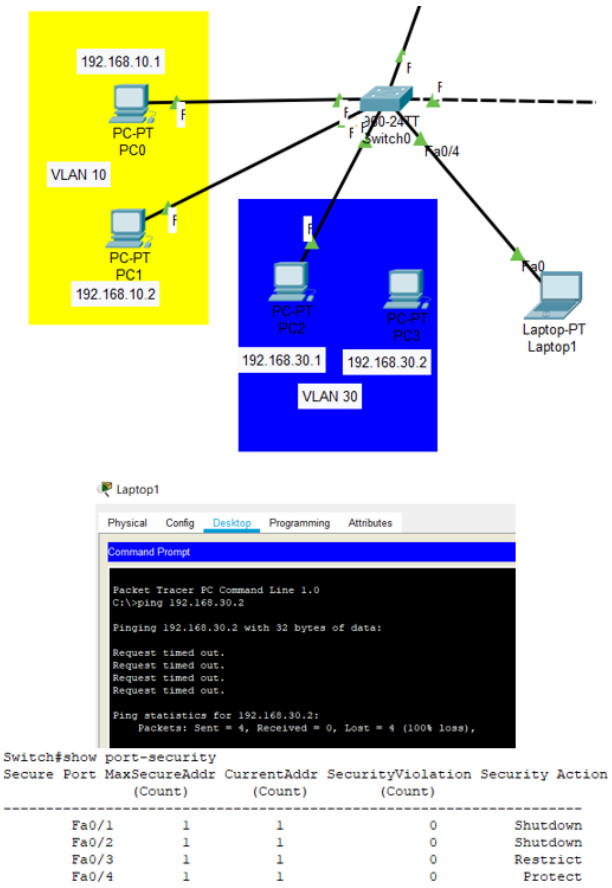
```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0002.4a3a.d306    DYNAMIC     Fa0/6
   1    00d0.d30a.5c5e    DYNAMIC     Fa0/7
   1    00e0.f719.de27    DYNAMIC     Fa0/5
  10    0002.1651.0080    STATIC      Fa0/1
  10    000c.857a.79bd    STATIC      Fa0/2
  10    00e0.f719.de27    DYNAMIC     Fa0/5
  30    00e0.f719.de27    DYNAMIC     Fa0/5
Switch#
```

Gambar 9. MAC *Address Table*

Selanjutnya akan dilakukan pengujian pada komputer yang mana dilakukan pemindahan koneksi kabel dari PC3 ke Laptop1.

Gambar 10 merupakan pengujian MAC *address* dari Laptop1 yang tidak dapat terkoneksi atau akses, karena MAC *address* dari perangkat Laptop1 tidak terkoneksi atau sesuai dengan yang ditentukan maka Laptop1 belum dapat terhubung pada jaringan lain. Hal tersebut akan terdeteksi pada *port security* sehingga akan muncul pada *interface* dengan status aksi *protect*. *Port security* merupakan mekanisme keamanan jaringan yang kegunaannya mampu memberikan keamanan yang baik dimana setiap *port* yang ada pada *switch* dapat di koneksi jaringan yang masuk tersebut. Apabila

ingin melakukan koneksi kembali maka harus dilakukan penghapusan MAC *address* pada *switch* yang dapat dilakukan oleh pihak IT sebagai administrator.



Gambar 10. Test Koneksi Perangkat Baru

Gambar 11 merupakan langkah–langkah dalam menghapus atau mengembalikan *MAC address* yang sebelumnya dilakukan *block* oleh *port security* sehingga dapat terhubung kembali pada jaringan tersebut.

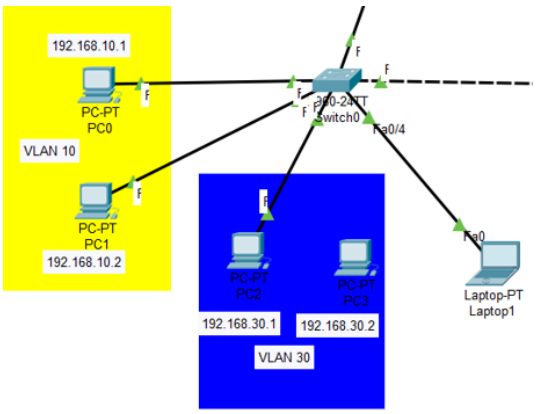
Di lihat dari Gambar 12 menunjukan bahwa Laptop1 sudah dapat terkoneksi ke PC2. PC2 sudah tidak dalam *block* oleh *port security* sehingga MAC *address* dari Laptop1 dapat terkoneksi ke PC2 tanpa adanya *packet lost*.

KESIMPULAN

Setelah melakukan penelitian ini dapat disimpulkan bahwa keamanan jaringan sangat mudah merespon koneksi jaringan yang digunakan dengan DHCP pada IP *client* sehingga mempermudah *user* bekerja di seluruh port-port yang ada. Penerapan keamanan menggunakan *firewall port blocking* lebih aman digunakan untuk mencegah segala bentuk koneksi jaringan yang dapat diakses, hal tersebut untuk menjaga keamanan data yang menjadi hal utama untuk mencegah terjadinya pencurian. Penerapan *firewall security port* dapat melakukan aksi *block* pada koneksi jaringan tersebut ketika terjadi perpindahan hak akses.

```
Switch#clear port-security all
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int ran
Switch(config)#int range fa0/1-4
Switch(config-if-range)#sh
Switch(config-if-range)#shutdown



Switch(config-if-range)#
%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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

Switch(config-if-range)#no sh
Switch(config-if-range)#no shutdown



Switch(config-if-range)#
%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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch(config-if-range)#
```

Gambar 11. *Clear Port Security*




```
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time<1ms TTL=128
Reply from 192.168.30.2: bytes=32 time<1ms TTL=128
Reply from 192.168.30.2: bytes=32 time<1ms TTL=128
Reply from 192.168.30.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1           1                0         Shutdown
        Fa0/2        1           1                0         Shutdown
        Fa0/3        1           1                0         Restrict
        Fa0/4        1           1                0          Protect
```

Gambar 12. *Test* Ping Laptop1 ke PC2

DAFTAR PUSTAKA

1. S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," *Int. Arab J. e-Technology*, vol. 1, no. 2, pp. 26–36, 2009.
2. H. Gunawan, H. Simorangkir, M. Ghiffari, T. Informatika, F. I. Komputer, and U. E. Unggul, "Pengelolaan Jaringan Dengan Router Mikrotik untuk Meningkatkan Efektifitas Penggunaan Bandwith Internet (Studi Kasus SMK Ki Hajar Dewantoro Kota Tangerang)," vol. 3, pp. 54–70, 2018.
3. P. Soepomo, "Analisis Perancangan Firewall Paket Filtering dan Proxy Server Untuk Optimasi Bandwidth (Studi Kasus di Laboratorium Riset Universitas Ahmad Dahlan Kampus 3). Jurnal JSTIE. Vol. 3, no. 1, pp. 89–97, 2015, doi: 10.12928/jstie.v3i1.2926.
4. R. O. Nitra and M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," *J. Sist. dan Teknol. Inf.*, vol. 7, no. 1, p. 52, 2019, doi: 10.26418/justin.v7i1.29979.
5. Purnama, "Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address," *Indones. J. Netw. Secur.*, vol. 8, no. 4, pp. 43–47, 2019.
6. M. Ryansyah and M. S. Maulana, "Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx 2," vol. 6, no. 3, pp. 108–112, 2018.
7. A. Supriyadi and D. Gartina, "Memilih Topologi Jaringan dan Hardware dalam Desain Sebuah Jaringan Komputer," *Inform. Pertan.*, vol. 16, no. 2, pp. 1037–1053, 2007.
8. Rohman, "Analisis Dan Perancangan Jaringan Komputer Asrama Putri Boarding School Man 1 Surakarta," 2013.
9. J. Natali, F. Fajrillah, and T. M. Diansyah, "Implementasi Static Nat Terhadap Jaringan Vlan Menggunakan Ip Dynamic Host Configuration Protocol (Dhcp)," *J. Ilm. Inform.*, vol. 1, no. 1, pp. 51–58, 2016, doi: 10.35316/jimi.v1i1.444.
10. B. Adhi Prakosa, A. Hendri Hendrawan, and W. K. Apriana Unversitas Ibn Khaldun Bogor Jln Sholeh Iskandar Km, "Perancangan Sistem Remote Ip Table Dan Instrusion Detection System (Ids) Dengan Snort Pada Jaringan Lan," *J. Krea-TIF*, no. 02, p. 3, 2015.
11. A. H. Hendrawan, S. Kom, and M. Kom, "Analisis Serangan Flooding Data Pada Router Mikrotik," *Krea-TIF*, pp. 12–20, 2016.