

Keamanan Jaringan Komputer Menggunakan Switch Port Security Pada Cisco Packet Tracer

Andy Satria ¹, Fanny Ramadhani ²

¹ Fakultas Teknik dan Ilmu Komputer, Teknologi Informasi, Universitas Dharmawangsa, Medan, Indonesia

² Fakultas Matematika dan Ilmu Pengetahuan Alam, Ilmu Komputer, Universitas Negeri Medan, Indonesia



INFORMASI ARTIKEL

Diterima Redaksi: 11 April 2023
Revisi Akhir: 18 Mei 2023
Diterbitkan Online: 21 Mei 2023

KATA KUNCI

Network Security; Protect; Restrict; Shutdown;
Switch Port Security; Violation

KORESPONDENSI

Phone: +62 81220820210

E-mail: andysatria@dharmawangsa.ac.id

A B S T R A K

Perkembangan teknologi yang semakin pesat dalam jaringan komputer membuat meningkatnya kebutuhan akses jaringan untuk memudahkan pekerjaan seperti kualitas jaringan yang stabil, cepat, dan efisien serta keamanan jaringan yang terkendali. Salah satu faktor yang dapat mempengaruhi kualitas jaringan adalah sistem keamanan jaringan atau network security. Metode yang digunakan pada penelitian ini adalah metode kualitatif dengan metode pendekatan deskriptif. Tujuan dari penelitian ini adalah dengan memanfaatkan Switch Port Security untuk pengamanan jaringan lokal (LAN) dalam membatasi hak akses host atau port demi kestabilan jaringan komputer sehingga pekerjaan tidak menjadi terhambat dan juga dapat mengurangi tingkat kejahatan di dalam jaringan. Switch Port Security bekerja di layer 2 dari bawah yaitu Data Link OSI Layer. Pada penelitian ini menggunakan tiga macam Violation yaitu Restrict, Protect, dan Shutdown.

PENDAHULUAN

Dalam kehidupan sehari-hari banyak manusia menggunakan jaringan komputer sebagai kebutuhan ataupun untuk memudahkan pekerjaannya karena sebuah sistem jaringan komputer mewujudkan suatu keterhubungan antara sekumpulan komputer yang dibangun oleh dua *station* atau lebih [1]. Maka, jaringan komputer menjadi hal penting sehingga dibutuhkan persiapan keamanan untuk jaringan komputer tersebut [2]. Dengan begitu hak akses untuk masuk ke jaringan tersebut dapat dibatasi sehingga tidak menjadi peluang kejahatan seperti pencurian data [3] [4].

Banyak cara yang dapat dimanfaatkan untuk mengurangi tingkat kejahatan di dalam jaringan seperti menggunakan Switch Port Security untuk pengamanan jaringan lokal (LAN) [5]. Switch Port Security adalah salah satu sistem untuk mengamankan jaringan dengan mengizinkan siapa saja yang dapat mengakses jaringan tersebut melalui Port yang tersedia di dalam Switch. Switch Port Security bekerja di layer 2 dari bawah yaitu Data Link OSI Layer [5] [6] [7].

TINJAUAN PUSTAKA

Port Security

Port Security adalah suatu keamanan jaringan yang dipakai pada Switch Cisco yang berfungsi untuk membatasi jumlah host dan menentukan *host* lain yang bisa terkoneksi pada setiap *port* yang ada di switch [8].

Adapun prinsip yang digunakan untuk mengkonfigurasi setiap *Port Security* yaitu harus mendaftarkan *MAC Address* terlebih dahulu agar dapat terhubung ke switch [9]. Cara kerja pada *Port Security* ini adalah dengan memblok *host* yang memiliki *MAC Address* tidak sesuai dengan konfigurasi pada *Port Security* [10].

Pada penelitian ini, Switch *Port Security* yang digunakan berbentuk topologi star karena memiliki tingkat keamanan yang tinggi dan cepat mendeteksi bila terjadi kerusakan pada jaringan [11]. Switch *Port Security* ini menggunakan tiga *Violation* yaitu *Restrict*, *Protect* dan *Shutdown*.

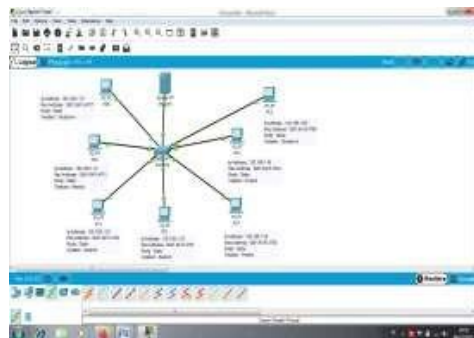
METODOLOGI

Metode yang digunakan pada penelitian ini adalah metode kualitatif dengan metode pendekatan deskriptif. Tujuan dalam penelitian ini adalah untuk memanfaatkan switch *port security* dalam membatasi hak akses *host* atau *port* demi kestabilan jaringan komputer. Pada penelitian ini, penulis memanfaatkan teknologi Cisco Packet Tracer untuk melakukan implementasi switch *port security* pada jaringan komputer.

HASIL DAN PEMBAHASAN

Percobaan Switch Port Security

Pada penelitian ini, percobaan Switch *Port Security* yang dilakukan yakni dengan menggunakan topologi *star* dimana terdapat 7 PC, 1 Switch, dan 1 Server.

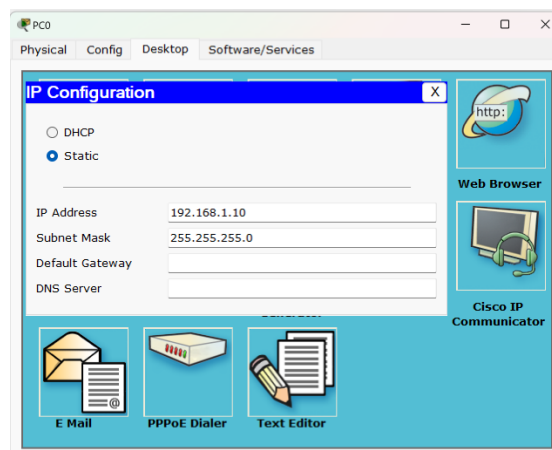


Gambar 1. Topologi Port Security Switch

Konfigurasi IP Address pada Client Port Security

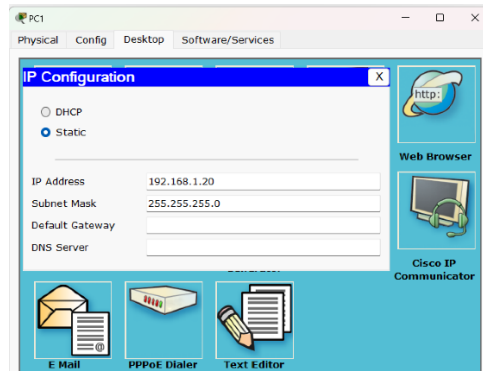
Tahapan pertama yang dilakukan yakni memberikan IP Address pada setiap PC yang sudah terhubung ke Switch.

1. Memberikan *IP Address* pada PC0 yakni 192.168.1.10



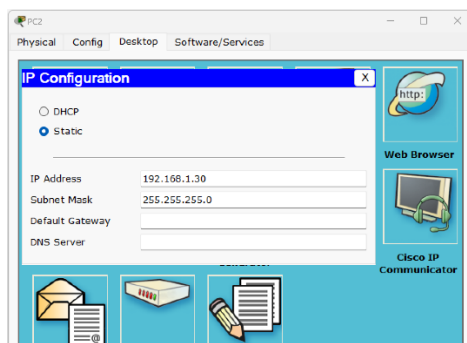
Gambar 2. *IP Address* Pada PC0

- Memberikan *IP Address* pada PC1 yakni 192.168.1.20



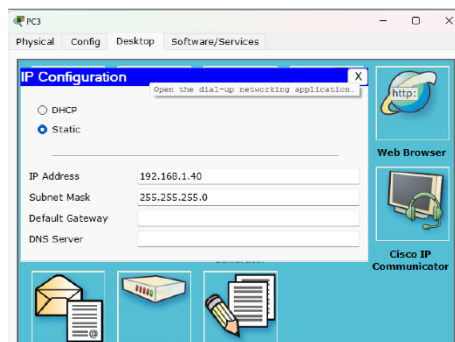
Gambar 3. *IP Address* Pada PC1

- Memberikan *IP Address* pada PC2 yakni 192.168.1.30



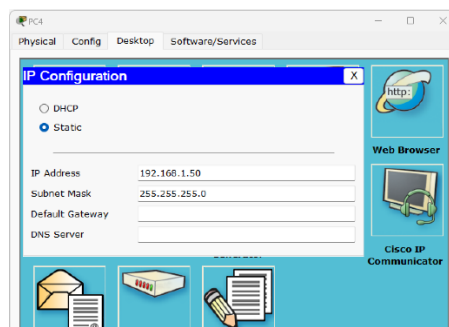
Gambar 4. *IP Address* Pada PC2

- Memberikan *IP Address* pada PC3 yakni 192.168.1.40



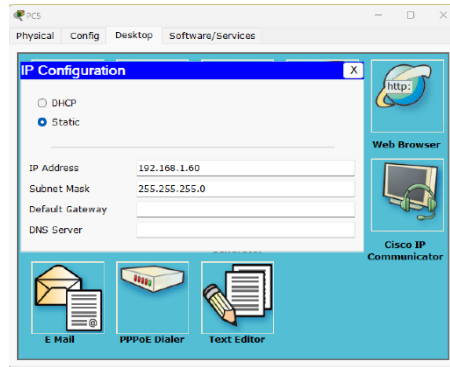
Gambar 5. *IP Address* Pada PC3

- Memberikan *IP Address* pada PC4 yakni 192.168.1.50



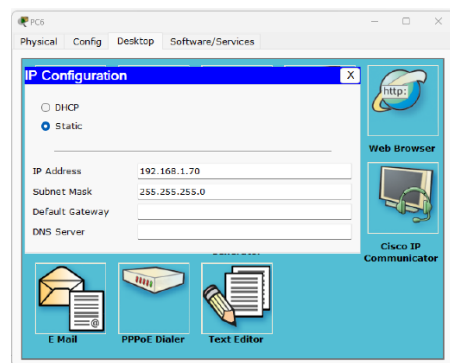
Gambar 6. *IP Address* Pada PC4

6. Memberikan *IP Address* pada PC5 yakni 192.168.1.60



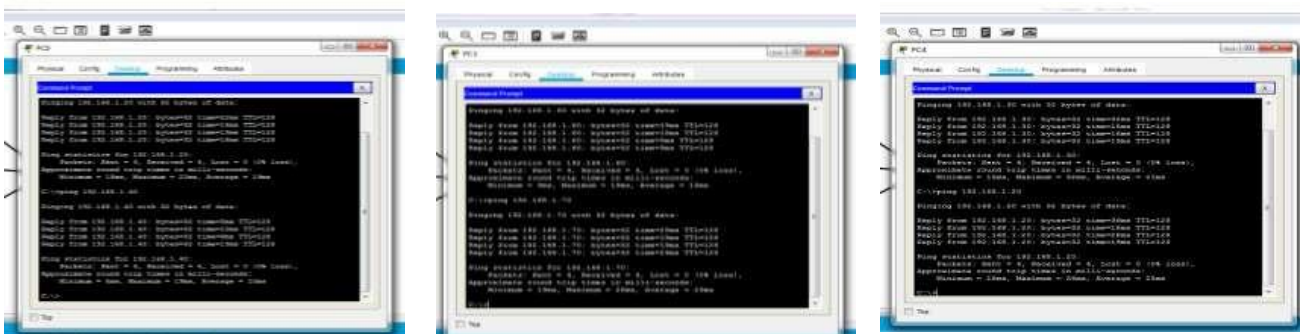
Gambar 7. *IP Address* Pada PC5

7. Memberikan *IP Address* pada PC6 yakni 192.168.1.70



Gambar 8. *IP Address* Pada PC6

Setelah memberikan *IP Address* pada setiap PC, maka selanjutnya akan melakukan perintah PING untuk membuktikan bahwa setiap PC dapat saling berkomunikasi.



Gambar 9. Uji Coba Jaringan

Konfigurasi Switch Port Security

Bila semua PC telah diberikan *IP Address*, selanjutnya yakni mengatur setiap *port* pada switch yang berfungsi untuk memberikan perintah yang berbeda pada setiap topologinya.

1. Port fa0/1 menggunakan Static mode SecurityRestrict.
2. Port fa0/2 menggunakan Static mode SecurityRestrict.
3. Port fa0/3 menggunakan Static mode SecurityRestrict.
4. Port fa0/4 menggunakan Static mode SecurityProtect.
5. Port fa0/5 menggunakan Static mode SecurityProtect.
6. Port fa0/6 menggunakan Static mode SecurityShutdown.

7. Port fa0/7 menggunakan Static mode SecurityShutdown.

Klik Switch, kemudian masuk ke Tab CLI:

1. Pengaturan Pada Port Ke-1 (fa0/1)

Mengatur fa0/1 menggunakan *Static mode Security Restrict* dan memberikan *MAC Address* yang dimasukkan melalui PC0, yaitu :0001.6415.4701

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0001.6415.4701
Switch(config-if)#switch port-security violation restrict
Switch(config-if)#ex
Switch(config)#ex
```

2. Pengaturan Pada Port Ke-2 (fa0/2)

Mengatur fa0/2 menggunakan *Static mode Security Restrict* dan memberikan *MAC Address* yang dimasukkan melalui PC1, yaitu :0001.6415.4702

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/2
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0001.6415.4702
Switch(config-if)#switch port-security violation restrict
Switch(config-if)#ex
Switch(config)#ex
```

3. Pengaturan Pada Port Ke-3 (fa0/3)

Mengatur fa0/3 menggunakan *Static mode Security Restrict* dan memberikan *MAC Address* yang dimasukkan melalui PC2, yaitu :0001.6415.4703

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0001.6415.4703
Switch(config-if)#switch port-security violation restrict
Switch(config-if)#ex
Switch(config)#ex
```

4. Pengaturan Pada Port Ke-4 (fa0/4)

Mengatur fa0/4 menggunakan *Static mode Security Protect* dan memberikan *MAC Address* yang dimasukkan melalui PC3, yaitu :0001.6415.4704

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/4
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0001.6415.4704
Switch(config-if)#switch port-security violation protect
Switch(config-if)#ex
Switch(config)#ex
```

5. Pengaturan Pada Port Ke-5 (fa0/5)

Mengatur fa0/5 menggunakan *Static mode Security Protect* dan memberikan *MAC Address* yang dimasukkan melalui PC4, yaitu :0001.6415.4705

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/5
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0001.6415.4705
Switch(config-if)#switch port-security violation protect
Switch(config-if)#ex
Switch(config)#ex
Switch#
```

6. Pengaturan Pada Port Ke-6 (fa0/6)

Mengatur fa0/6 menggunakan *Static mode Security Shutdown* dan memberikan *MAC Address* yang dimasukkan melalui PC5, yaitu :0001.6415.4706

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/6
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0001.6415.4706
Switch(config-if)#switch port-security violation shutdown
Switch(config-if)#ex
Switch(config)#ex
```

7. Pengaturan Pada Port Ke-7 (fa0/7)

Mengatur fa0/7 menggunakan *Static mode Security Shutdown* dan memberikan *MAC Address* yang dimasukkan melalui PC6, yaitu :0001.6415.4707

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/7
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0001.6415.4707
Switch(config-if)#switch port-security violation shutdown
Switch(config-if)#ex
Switch(config)#ex
```

Hasil Konfigurasi Switch Port Security

Menampilkan hasil konfigurasi pada port fa0/1 dengan memberikan perintah : show port- security interface fa0/1.



Gambar 12. Hasil Konfigurasi Pada PC0

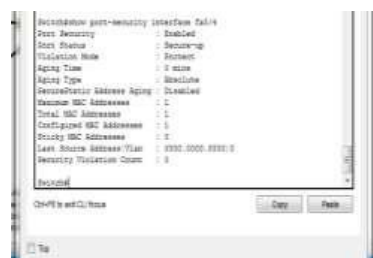
Menampilkan hasil konfigurasi pada port fa0/2 dengan memberikan perintah : show port- security interface fa0/2.



Gambar 13. Hasil Konfigurasi Pada PC1

Menampilkan hasil konfigurasi pada port fa0/3 dengan memberikan perintah : show port- security interface fa0/3.

Menampilkan hasil konfigurasi pada port fa0/4 dengan memberikan perintah : show port- security interface fa0/4.



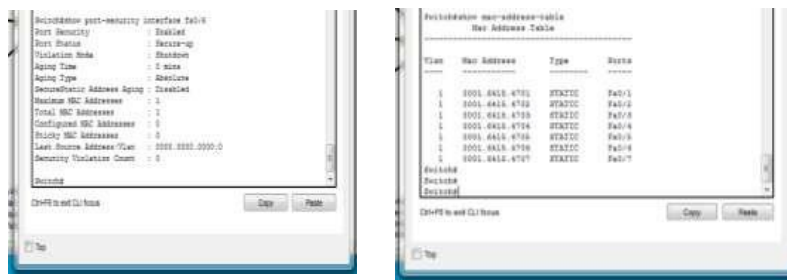
Gambar 14. Hasil Konfigurasi Pada PC3

Menampilkan hasil konfigurasi pada port fa0/5 dengan memberikan perintah : show port- security interface fa0/5.



Gambar 15. Hasil Konfigurasi Pada PC4

Menampilkan hasil konfigurasi pada port fa0/6 dengan memberikan perintah : show port- security interface fa0/6



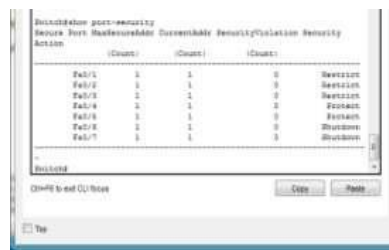
Gambar 16. Hasil Konfigurasi Pada PC5

Menampilkan hasil konfigurasi pada port fa0/7 dengan memberikan perintah : show port- security interface fa0/7.



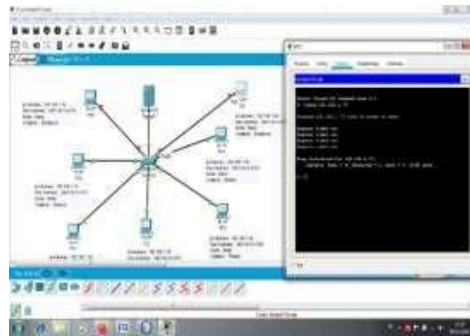
Gambar 18. Hasil Konfigurasi Pada PC6

Setelah melakukan pengecekan hasil konfigurasi pada setiap port. Selanjutnya, menampilkan seluruh konfigurasi masing-masing Port Security dengan memberikan perintah : show port-security.



Gambar 19. Hasil Seluruh konfigurasi

Hasil Konfigurasi Switch Port Security



Gambar 20. Hasil Pembuktian Switch Port Security

KESIMPULAN DAN SARAN

Switch port security terletak di layer ke 2 dari bawah yaitu pada Data Link OSI Layer. Dengan membuat konfigurasi port security static, akan membuat jaringan menjadi sangat aman. Hal itu dikarenakan jaringan memiliki switch yang tidak bisa diakses sembarangan oleh port lain kecuali dengan izin akses dari switch pada port yang tersedia. Dengan menggunakan tiga macam Violation yaitu Restrict, Protect, dan Shutdown.

DAFTAR PUSTAKA

- [1] A. P. Sujana, "Perangkat Pendukung Forensik Lalu Lintas Jaringan," *Jurnal Teknik Komputer Unikom*, vol. 3, pp. 31 - 37, 2014.
- [2] Z. Munawar and N. I. Putri, "Keamana Jaringan Komputer Pada Era Big Data," *Jurnal Sistem Informasi (J-SIKA)*, vol. 02, pp. 14 -20, 2020.
- [3] R. T. Prabowo and M. T. Kurniawan, "Analisis dan Desain Keamanan Jaringan Komputer Dengan Metode Network Development Life Cycle (Studi Kasus: Universitas Telkom)," *Jurnal Rekayasa Sistem & Industri*, vol. 2, pp. 1 - 7, 2015.
- [4] F. Ramadhani, U. Ramadhani and B. Lutfi, "Combination of Hybrid Cryptography In One Time Pad (OTP) Algorithm And Keyed-Hash Message Authentication Code (HMAC) In Securing The Whatsapp Communication Application," *Journal of Computer Science, Information Technology and Telecommunication Engineering*, vol. 1, no. 1, pp. 31 - 36, 2020.
- [5] K. A. Fikri and D. , "Keamanan Jaringan Menggunakan Switch Port Security," *InfoTekjar*, vol. 5, no. 2, pp. 302-307, 2021.
- [6] V. B. Djusmin, "Hotspot Berbasis Koneksi PPPoE (Point to Point Protocol Over Ethernet) Dengan Otentikasi User Manager Mikrotik Pada Warnet Starcom," *Jurnal Ilmiah d'ComPutarE*, vol. 5, pp. 47 -62, 2015.
- [7] F. Ramadhani, A. Satria and I. P. Sari, "Aplikasi Internet Berbasis Website sebagai E-Commerce Penjualan Komponen Sport Car," *Blend Sains Jurnal Teknik*, vol. 1, no. 2, pp. 69 - 75, 2022.
- [8] S. and A. Gunawan, "Firewall Port Security Switch Untuk Keamanan Jaringan Komputer Menggunakan Cisco Router 1600S Pada PT. Tirta Kencana Tata Warna Sukabumi," *Conten (Computer and Network Technology)*, vol. 1, pp. 13 - 22, 2021.
- [9] S. and A. Gunawan, "Firewall Port Security Switch Untuk Keamanan Jaringan Komputer Menggunakan Cisco Router 1600S Pada PT. Tirta Kencana Tata Warna Sukabumi," *Conten*, vol. 1, no. 1, pp. 13-22, 2021.
- [10] O. K. Sulaiman, "Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security," *CESS (Journal of Computer Engineering, System and Science)*, vol. 1, pp. 9 - 14, 2016.
- [11] S. N. Khasanah, "Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus: PT. Sukses Berkat Mandiri Jakarta)," *Jurnal Khatulistiwa Informatika*, vol. 4, pp. 182 - 191, 2016.