CESS (Journal Of Computer Engineering, System And Science) **p-ISSN :2502-7131**
Vol 1, No 1, Januari 2016 **e-ISSN :2502-714x**

ANALISIS SISTEM KEAMANAN JARINGAN DENGAN MENGGUNAKAN SWITCH PORT SECURITY

Oris Krianto Sulaiman
Universitas Islam Sumatera Utara
Jalan Sisingamangaraja, Kelurahan Teladan, Medan Kota, Sumatera Utara
Fairystrawhat@gmail.com

Abstrak — Perkembangan teknologi dalam jaringan komputer lambat laun semakin pesat seiring dengan meningkatnya kebutuhan akan akses jaringan yang efisien , stabil dan cepat serta kemanan yang handal. Salah satu faktor yang mempengaruhi kualitas dalam jaringan adalah network security atau keamanan jaringan, banyak teknik yang dapat dilakukan dalam meningkatkan keamanan jaringan, baik dengan membangun sistem firewall, dengan menggunakan layer7 protocol maupun dengan port security, port security memanfaatkan port-port yang ada untuk mengizinkan akses ke jaringan, switch port security merupakan suatu kemampuan perangkat switch untuk mengamankan jaringan LAN (Local Area Network) terdapat beberapa jenis switch port security yang digunakan yaitu default/ static port security, port security dynamic learning dan sticky port security, penulis akan melakukan analisis terhadap masing-masing jenis switch port security untuk menentukan kehandalan, kegunaan dan pemanfaatannya dilapangan.

Keywords : **network security, port security, switch port security**

I. PENDAHULUAN

Kebutuhan akan jaringan komputer semakin bertambah penting , baik dalam pendidikan, pekerjaan maupun dalam sebuah permainan, salah satu hal penting dalam mengelola jaringan komputer yaitu kemanan dari jaringan itu sendiri, dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan tersebut, misalkan adanya pencurian data yang terjadi dijaringan tersebut ataupun adanya peretas yang mematikan sumber daya jaringan tersebut, dsb.

Banyak teknik yang dapat diupayakan dalam memperkecil tingkat kejahatan dalam jaringan ini, salah satu teknik yang banyak digunakan untuk pengamanan jaringan lokal adalah dengan menggunakan switch port security, switch port security merupakan teknik yang akan mengizinkan siapa saja yang berhak menggunakan akses jaringan melalui port yang tersedia di switch.

A. Switch Unmanageable

Switch merupakan perangkat yang berfungsi untuk menghubungkan beberapa komputer ataupun perangkat jaringan agar dapat berbagi sumber dayanya. Switch merupakan sebuah perangkat keras yang memungkinkan terjadinya distribusi packet data antar komputer dalam jaringan dan mampu untuk mengenali topologi jaringan dibanyak layer sehingga data dapat langsung sampai ketujuan, switch mempunyai memori yang disebut dengan CAM table (*Content Addressable Memory)* atau dikenal juga dengan sebutan MAC address table, setiap perangkat yang terhubung ke switch maka secara otomatis switch akan menyimpan seluruh MAC address setiap perangkat yang terhubung dengannya kedalam MAC address tabel, contoh switch

Gambar 1. Switch unmanageable

Pada gambar tersebut terlihat bahwa perangkat switch tersebut mempunyai 8 port , namun swich jenis ini tidak mendukung kemampuan untuk keamanan maupan kualitas layanan yang handal dijaringan.

B. *Switch Manageable*

Pada jenis switch ini tetap dengan fungsi yang sama namun banyak fitur fitur tambahan yang dapat meningkatkan kualitas dari jaringan tersebut, contoh fitur yang paling sering digunakan adalah kemampuan switch dalam membuat VLAN dan control traffic jaringan, switch ini juga dapat melakukan proses routing, berbeda hal nya dengan switch unmanageable yang hanya bekerja di layer 2 yaitu layer data link , namun pada switch manageable dapat dilakukan proses routingan ataupun menghubungkan alamat ip yang berbeda dalam hal ini switch bekerja di layer 3.

Selain dengan kemampuan untuk membuat VLAN dan control traffic jaringan , switch ini juga dapat meningkatkan kemanan dengan menggunakan kemampuan switch port security yang berfungsi untuk menangani hak akses kejaringan tersebut berdasarkan port – port yang dimiliki oleh switch tersebut.

Gambar 2. Switch manageable

II. SWITCH PORT SECURITY

Sebuah kemampuan switch manageable untuk meningkatkan keamanan jaringan dengan menggunakan port-port yang tersedia pada switch tersebut.

Ada 3 jenis switch port security yaitu:

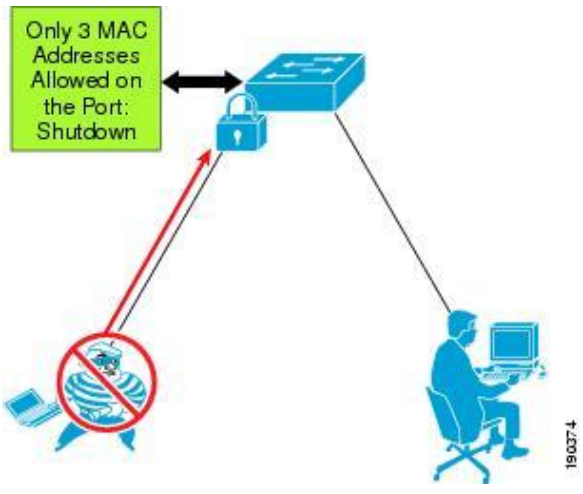
- *Default / static port security*
- *Port security dynamic learning*
- *Sticky port security*

A. Default / static port security

Ketika port security ini di fungsikan maka mac address port security akan diaktifkan pada port switch, sehingga port tidak akan mem-forward packets jika source address bukanlah address yang telah kita defenisikan/tentukan sebelumnya. menentukan alamat mac tertentu yang di perbolehkan untuk terhubung ke port tersebut secara manual

B. Port security dynamic learning

MAC address di pelajari secara dinamis ketika perangkat terhubung ke switch, mac address tersebut di simpan di mac address table

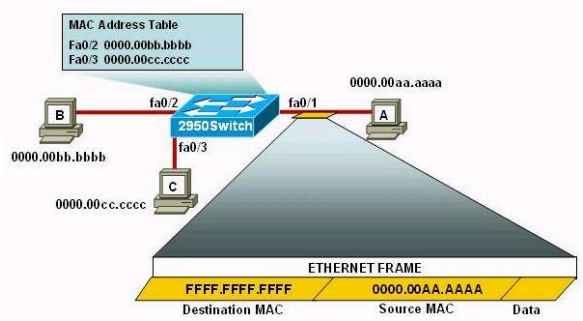


Gambar 3. Contoh switch port security

Pada gambar tersebut terlihat bahwa pengguna jaringan menggunakan media switch untuk berbagi sumber daya namun switch tersebut mempunyai kemampuan untuk mengamankan jaringannya, pada switch hanya di perbolehkan 3 MAC address yang terhubung di port tersebut selain itu jika MAC tidak terdaftar di MAC address table maka tidak diizinkan untuk masuk kejaringan tersebut.

C. Sticky port security

Sebuah kemampuan switch dalam mengenal mac address tiap tiap perangkat yang terhubung dan akan memblok setiap mac yang melebihi dari mac yang telah terdaftar.



Gambar 4. Sticky port security

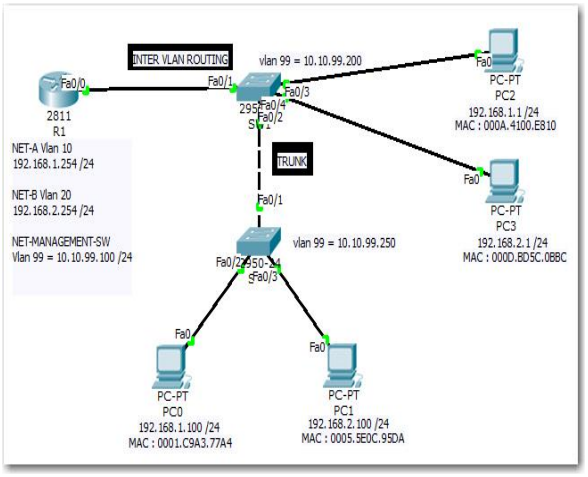
Pada gambar tersebut terlihat switch akan membaca mac addres dari tiap perangkat yang terhubung dengannya, dengan menggunakan sticky port security maka dapat didaftarkan jumlah pemakaian perangkat yang terhubung di switch tersebut, missal jika didaftar hanya 2 mac maka ketika ada perangkat yang ketiga dengan otomatis sticky port security akan mencegah (blok) mac tersebut , sehinga perangkat yang terhubung tetap 2 yang pertama.

III. METODOLOGI PENELITIAN

Metode yang digunakan pada analisis ini adalah dengan menggunakan perbandingan dan penggunaan tiap tiap fungsi dari :

- *Default / static port security*
- *port security dynamic learning*
- *sticky port security*

Uji coba akan dilakukan dengan menggunakan simulasi program Cisco Packet Tracer 6.2 (CPT).
Adapun topologi yang akan digunakan dalam melakukan perbandingan ini adalah sebagai berikut:



Gambar 5. Topologi jaringan

TABEL 1
ADDRESSING

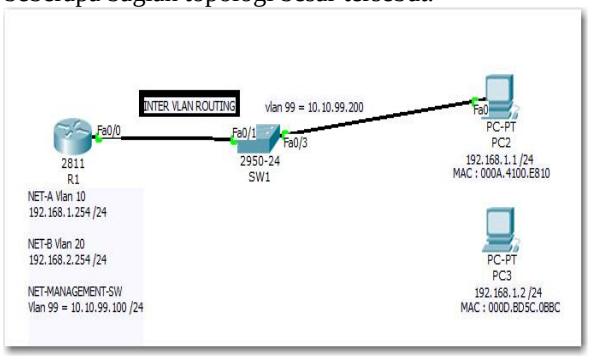
Device	Interface	IP address	Subnet Mask	Default Gateway
R1	NIC fa 0/0.10	192.168.1.254	255.255.255.0	N/A
	NIC fa 0/0.20	192.168.2.254	255.255.255.0	N/A
	NIC fa 0/0.99	10.10.99.100	255.255.255.0	N/A
SW1	VLAN 99	10.10.99.200	255.255.255.0	10.10.99.100
	VLAN 10	N/A	N/A	N/A
	VLAN 20	N/A	N/A	N/A
SW2	VLAN 99	192.168.99.250	255.255.255.0	10.10.99.100
	VLAN 10	N/A	N/A	N/A
	VLAN 20	N/A	N/A	N/A
PC0	NIC	192.168.1.1	255.255.255.0	192.168.100.254
PC1	NIC	192.168.2.1	255.255.255.0	192.168.200.254
PC2	NIC	192.168.1.100	255.255.255.0	192.168.100.254
PC3	NIC	192.168.2.100	255.255.255.0	192.168.200.254

IV. HASIL DAN PEMBAHASAN

A. *Default / static port security*

Ketika mac address port security diaktifkan pada port switch, maka port tidak akan mem-forward packets jika source address bukanlah address yang telah kita defenisikan/tentukan sebelumnya. Static dimaksud disini adalah menentukan alamat mac tertentu yang di perbolehkan untuk terhubung ke port tersebut secara manual.

Topologi berikut adalah hasil dari penghampusan beberapa bagian topologi besar tersebut.



Gambar 6. Topologi Static port security

SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address 000A.4100.E810

Ini artinya mac address 000A.4100.E810 yang dimiliki oleh PC2 yang hanya diizinkan oleh switch di interface fastehternet 0/3.

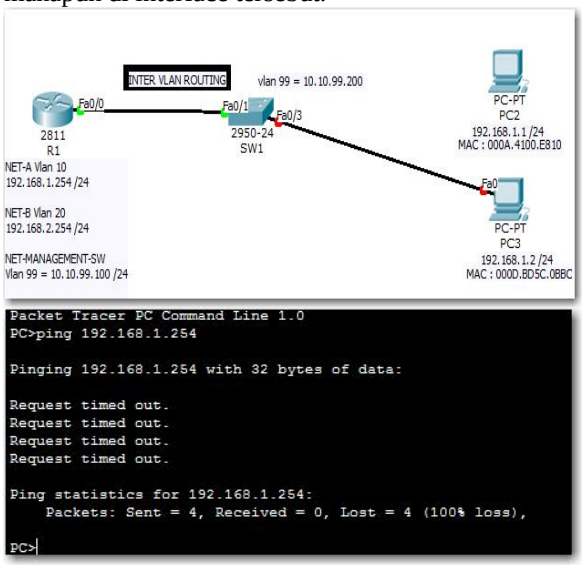
Mac-address table di SW1 maka Mac address dari PC2 telah didaftarkan

SW1#show mac address-table

Mac Address Table

Vlan	Mac Address	Type	Ports
10	**000a.4100.e810**	**STATIC**	**Fa0/3**
10	0060.5cda.d501	DYNAMIC	Fa0/1
20	0060.5cda.d501	DYNAMIC	Fa0/1
99	0060.5cda.d501	DYNAMIC	Fa0/1

Hal ini dibuktikan ketika port tersebut digunakan oleh PC3 maka tidak akan terkoneksi ke perangkat manapun di interface tersebut.



Gambar 7. Interface fa 0/3 down

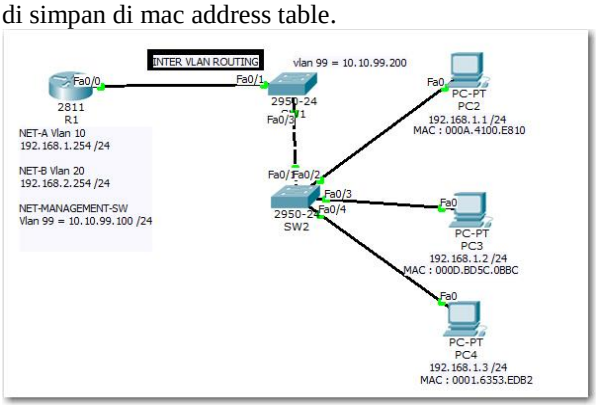
SW1#show interfaces fa0/3
FastEthernet0/3 is down, line protocol is down (err-disabled)
Interface fastethernet 0/3 down ini disebabkan karna mac address yang didaftarkan di interface ini tidak sama dengan perangkat yang terhubung diinterface ini.
Port tersebut tidak akan aktif (tetap dalam keadaan down) meskipun dipindahankan kembali ke PC2 yang mac-addressnya terdaftar.
Aktifkan kembali interface 0/3
SW1(config)#interface fastEthernet 0/3
SW1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
SW1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

Hal ini menyebabkan mac-address table akan kembali seperti semula.
SW1#show mac address-table
Mac Address Table

Vlan	Mac Address	Type	Ports
10	0060.5cda.d501	DYNAMIC	Fa0/1
20	0060.5cda.d501	DYNAMIC	Fa0/1
99	0060.5cda.d501	DYNAMIC	Fa0/1

B. Port security dynamic learning

MAC address di pelajari secara dinamis ketika perangkat terhubung ke switch, mac address tersebut di simpan di mac address table.

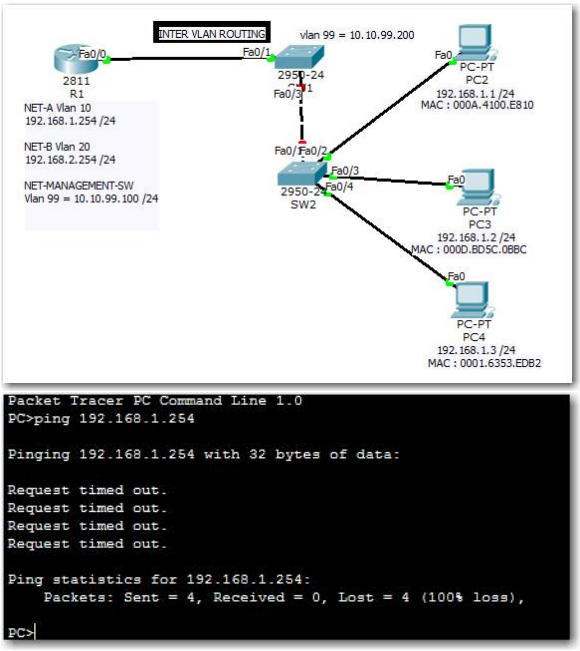


Gambar 8. Topologi Port security dynamic learning

Konfigurasi port fa0/3 di switch 1 agar hanya PC2 dan PC3 yang dapat terhubung sedangkan PC4 tidak dapat terhubung, yang artinya MAC address dari PC2 dan PC3 harus dipelajari atau di daftarkan ke fa0/3.
SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport port-security maximum ?
<1-132> Maximum addresses
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 3
SW1(config-if)#switchport port-security mac-address 000A.4100.E810
SW1(config-if)#switchport port-security mac-address 000D.BD5C.0BBC
Terlihat bahwah switchport port-security maximum hanya 132 Mac address
Maximum 3 untuk Mac-address dari PC2, PC3 dan SW2.
Dalam hal ini mac yang didaftarkan adalah manual yaitu mac address 000A.4100.E810 untuk PC2 dan mac address 000D.BD5C.0BBC untuk PC3
SW1#show mac address-table
Mac Address Table

Vlan	Mac Address	Type	Ports
10	0002.16aa.1601	STATIC	Fa0/3 *mac sw2*
10	000a.4100.e810	STATIC	Fa0/3 *mac pc2*
10	000d.bd5c.0bbc	STATIC	Fa0/3 *mac pc3*
10	0060.5cda.d501	DYNAMIC	Fa0/1
20	0060.5cda.d501	DYNAMIC	Fa0/1
99	0060.5cda.d501	DYNAMIC	Fa0/1

Pada saat PC4 ingin terhubung maka interface 0/3 diswitch akan memblokir mac dari PC4 tersebut.



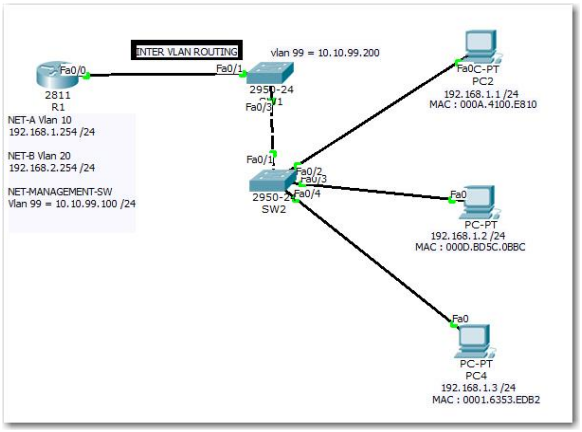
Gambar 9. Interface fa 0/3 down

Hal ini sama dengan static port security yang mana mac address table akan kembali ke semula dan fa0/3 akan down sehingga tidak dapat digunakan k, untuk menggunakan fa0/3 di switch 1 lakukan kembali hal yang sama dengan static port security.

C. Sticky port security

Spesifikasi MAC address:

- Dipelajari secara dinamis.
- Menambah MAC address ke dalam MAC address table.
- Disimpan di running configuration.



Gambar 10. Topologi sticky port security

Pada percobaan ini semua perangkat telah terhubung dan akan diuji coba sticky port security pada switch 1

SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 3
SW1(config-if)#switchport port-security mac-address ?
H.H.H 48 bit mac address
sticky Configure dynamic secure addresses as sticky
SW1(config-if)#switchport port-security mac-address sticky
Sticky akan membaca mac-address yang mana yang lebih dulu akan di masukkan ke dalam mac-address table dengan jumlah maksimum 3.
Konfigurasi saat ini adalah
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security maximum 3
switchport port-security mac-address sticky
Mac address table saat ini adalah
SW1#show mac address-table
Mac Address Table

Vlan	Mac Address	Type	Ports
10	0002.16aa.1601	STATIC	Fa0/3
10	0060.5cda.d501	DYNAMIC	Fa0/1
20	0060.5cda.d501	DYNAMIC	Fa0/1
99	0060.5cda.d501	DYNAMIC	Fa0/1

Untuk uji coba dengan mendaftarkan mac address PC3 dan PC4 , sementara untuk PC2 akan terputus karena jumlah maximum mac-address yang dapat di daftarkan hanya 3 mac address, dalam kasus ini mac address yang terdaftar adalah mac address SW2, PC3 dan PC4.

SW2 secara otomatis akan menambahkan mac addressnya , sementara untuk PC3 dan PC4 harus melakukan protokol ICMP (ping) agar mac address terdaftar di SW1.

Di port security sticky PC yang akan melakukan ICMP akan terdaftar di SW1 dengan jumlah maximum 3 mac address.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=1ms TTL=255
Reply from 192.168.1.254: bytes=32 time=1ms TTL=255
Reply from 192.168.1.254: bytes=32 time=0ms TTL=255
Reply from 192.168.1.254: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Gambar 11. Ping dari PC3 ke router

SW1#show mac address-table

10	0002.16aa.1601	STATIC	Fa0/3
	"Mac address SW2"		
10	000d.bd5c.0bbc	STATIC	Fa0/3
	"Mac address PC3"		
10	0060.5cda.d501	DYNAMIC	Fa0/1
20	0060.5cda.d501	DYNAMIC	Fa0/1
99	0060.5cda.d501	DYNAMIC	Fa0/1

Switch 2 akan menambahkan mac address secara otomatis , selanjutnya yang akan melakukan ICMP akan di tambahkan ke mac address table, PC3 telah ditambahkan ke mac address table,

```
PC>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=0ms TTL=255
Reply from 192.168.1.254: bytes=32 time=0ms TTL=255
Reply from 192.168.1.254: bytes=32 time=0ms TTL=255
Reply from 192.168.1.254: bytes=32 time=7ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms
```

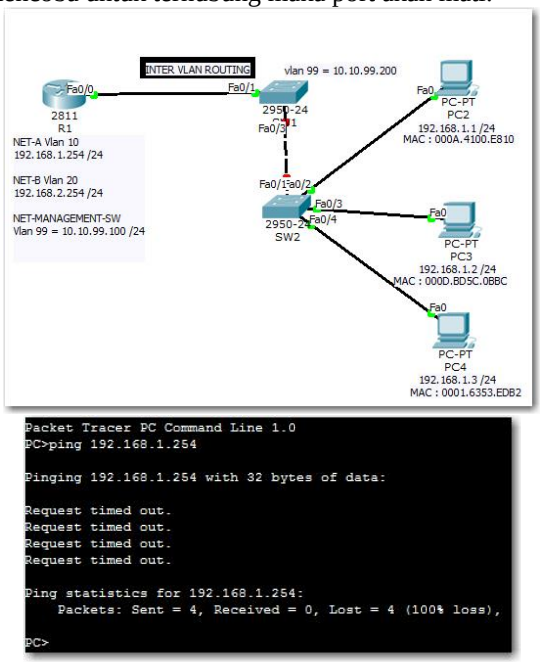
Gambar 12. Ping dari PC4 ke router

Periksa kembali mac address table di SW1
SW1#show mac address-table
Mac Address Table

Vlan	Mac Address	Type	Ports
10	0001.6353.edb2	STATIC	Fa0/3
	"MAC address PC4"		
10	0002.16aa.1601	STATIC	Fa0/3
	"MAC address SW2"		
10	000d.bd5c.0bbc	STATIC	Fa0/3
	"MAC address PC3"		
10	0060.5cda.d501	DYNAMIC	Fa0/1
20	0060.5cda.d501	DYNAMIC	Fa0/1
99	0060.5cda.d501	DYNAMIC	Fa0/1

Terlihat bahwa Mac address table telah penuh karna jumlah maksimum mac address table yang di

konfigurasikan adalah 3 , jadi jika ada perangkat yang mencoba untuk terhubung maka port akan mati.



Gambar 13. Ping dari PC2 ke router

Terlihat bahwa Interface FastEthernet0/3 link akan berubah menjadi warna merah, changed state to down dan PC2 tidak dapat terhubung serta mac address table akan kosong (kembali ke awal).Untuk mengaktifkannya sama seperti sebelumnya shutdown dan no shutdown.

V. KESIMPULAN & SARAN

A. Kesimpulan

Berdasarkan uji coba implementasi secara simulasi dengan menggunakan cisco packet tracer 6.2 maka dapat disimpulkan:

1. Default / static port security digunakan untuk satu port yang akan diblok, pada kemampuan pengamanan ini terbilang sangat minim dikarenakan kemampuan static port security hanya mampu mendaftarkan satu mac-address.
2. Port security dynamic learning kemampuan port security dynamic learning mampu mempelajari mac-address hingga 132 mac address namun memiliki kelemahan disisi admin jaringan yang kesulitan untuk mendaftarkan mac address yang akan diizinkan menggunakan jaringan tersebut.
3. Sticky port security sangat efisien digunakan karena kemampuannya yang dapat mempelajari secara dynamic mac-address yang akan didaftarkan.

B. Saran

Berikut adalah saran-saran untuk pengembangan lebih lanjut.

1. Port security merupakan teknik dasar pada jaringan, untuk pengembangan lebih lanjut dapat di analisis tentang keamanan yang lebih besar seperti DHCP snooping, Dynamic ARP inspection dan IP source guard

REFERENSI

[1] Jemi Y B, Kusrini, Sudarmawan, “Analisis aspek keamanan informasi jaringan komputer (studi kasus: stimik kupang)”, *Seminar Nasional Informatika 2013 (semnasIF 2013) ISSN: 1979-2328, UPN ”Veteran” Yogyakarta, 18 Mei 2013.*

[2] Salah Alabady,, “Design and Implementation of a Network Security Model for Cooperative Network”, *International Arab Journal of e-Technology, Vol. 1, No. 2,*pp.26-37 *, June 2009*.

[3] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005.

[4] Dr. Hussein Al-Bahadili, Dr. Ali H. Hadi, “Network Security Using Hybrid Port Knocking”, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, pp.8-12 ,August 2010.

[5] Sakshi S, Gurleen S, Prabhdeep S “Security enhancing of a LAN network using hardening technique” International Journal of Innovative