Prosiding Seminar Nasional Teknologi Informasi dan Kedirgantaraan : Transformasi Teknologi untuk Mendukung Ketahanan Nasional, Yogyakarta, 13 Desember 2018
SENATIK 2018, Vol. IV, ISBN 978-602-52742-0-6
DOI: http://dx.doi.org/10.28989/senatik.v4i0.239

IMPLEMENTATION PORT SECURITY FOR SECURITY SYSTEMS NETWORK AT THE COMPUTING LABORATORY OF ADISUTJIPTO TECHNOLOGY COLLEGE

Sudaryanto
Program Studi Informatika
Sekolah Tinggi Teknologi Adisutjipto
Jl. Janti, Blok-R, Lanud Adisucipto Yogyakarta
Email : sudaryanto@stta.ac.id

Abstract

At the Computing Laboratory Adisutjipto College of Technology (STTA) there are switch devices and several personal computers connected directly to the server, so that the equipment in the laboratory can be used by students, employees and lecturers freely to explore the world without borders (internet) by utilizing the STTA bandwidth. The absence of a security system in the laboratory, users can use bandwidth without administrator permission to carry out activities that are not in accordance with the provisions of bandwidth usage in the STTA environment, thus disrupting Practical activities in the Laboratory. Many techniques can be done in minimizing the crime rate or the use of irresponsible users in this network, one technique that will be used to secure local networks is to use security ports on the switch. With port security implemented in the Laboratory STTA computing theft or excessive bandwidth usage can be reduced 70,19% and the use of Unshielded twisted-pair (UTP) cables with unregistered computer devices can be prevented.

Keyword: Network Security, Manageable Switch, Port Security

Abstrak

Di Laboratorium Komputasi Sekolah Tinggi Teknologi Adisutjipto (STTA) ada perangkat *switch* dan beberapa personal komputer yang terhubung langsung ke *server*, sehingga peralatan di laboratorium dapat digunakan oleh mahasiswa, karyawan dan dosen secara bebas untuk menjelajahi dunia tanpa batas (internet) dengan memanfaatkan *bandwidth* STTA. Tidak adanya sistem keamanan di laboratorium, pengguna dapat menggunakan bandwidth tanpa izin administrator untuk melaksanakan kegiatan yang tidak sesuai dengan ketentuan penggunaan bandwidth di lingkungan STTA, sehingga mengganggu kegiatan Praktikum di Laboratorium. Banyak teknik yang dapat dilakukan dalam meminimalkan tingkat kejahatan atau penggunaan pengguna yang tidak bertanggung jawab dalam jaringan ini, salah satu teknik yang akan digunakan untuk mengamankan jaringan lokal adalah dengan menggunakan keamanan *port* pada *switch*. Dengan keamanan *port* yang diimplementasikan di Laboratorium Komputasi STTA pencurian atau penggunaan bandwidth yang berlebihan dapat dikurangi 70,19% dan penggunaan kabel *Unshielded twisted-pair* (UTP) dengan perangkat komputer yang tidak terdaftar dapat dicegah.

Kata kunci: Keamanan Jaringan, *Manageable Switch, Port Security*

1. Pendahuluan

Pada penelitian sebelumnya [1] sudah pernah dibahas tentang analasis jenis *switch port security* yaitu *Default / static port security*, *Port security dynamic learning*, *Sticky port*

security untuk menentukan kehandalan, kegunaan dan pemanfaatannya dilapangan tetapi belum di implementasikan dan belum diketahui *Port Security* yang tepat untuk digunakan di Laboratorium Komputasi STTA, sedangkan pada jurnal [2] sudah menganalisis dan mengimplementasikan jenis sistem keamanan menggunakan *port knocking* yang menggunakan *IPtables* sebagai *firewall*, tetapi bukan menggunakan sistem kemanan *port security* maka pada penelitian ini akan mencoba mengimplementasikan dan memanfaatkan *port security* sebagai sistem keamanan di Laboratorium Komputasi Sekolah Tinggi Teknologi Adisutjipto Yogyakarta.

Salah satu faktor yang mempengaruhi kualitas dalam jaringan adalah sistem keamanan, banyak teknik yang dapat dilakukan dalam meningkatkan keamanan jaringan, baik dengan menggunakan layer7 *protocol*, dengan membangun sistem *firewall* maupun dengan *port security*. Dengan adanya *port security port-port* yang ada dapat dimanfaatkan untuk mengizinkan akses ke jaringan. *Switch port security* merupakan suatu kemampuan perangkat *switch* untuk mengamankan jaringan LAN (*Local Area Network*).

Implementasi *port security* ini bertujuan untuk mencari jenis keamanan jaringan yang sesuai dengan kondisi di Laboratorium Komputasi STTA kemudian mengimplementasikannya serta memanfaatkan *port security* pada sistem keamanan jaringan Laboratorium Komputasi untuk mengurangi pengguna yang memanfaatkan jaringan Laboratorium Komputasi untuk penggunaan *bandwidth* diluar perangkat komputer yang telah diijinkan/didaftarkan dan dengan sembarangan mengunakan jaringan yang ada di Laboratorium Komputasi STTA Yogyakarta.

2. Metodologi Penelitian

2.1 *Switch Manageable*

Pada *switch manageable* mempunyai fungsi yang sama dengan *switch unmanageable* namun banyak fitur-fitur tambahan yang dapat membedakan *switch unmanageable* dalam meningkatkan kualitas dari jaringan tersebut [8], contoh fitur yang paling sering digunakan adalah kemampuan *switch* dalam konfigurasi *Virtual LAN* (VLAN) dan *traffic* jaringan yang bisa dikontrol/diatur, switch ini juga dapat melakukan proses *routing*, *switch* ini juga dapat digunakan untuk meningkatkan kemanan dengan menggunakan kemampuan *switch port security* yang berfungsi untuk menangani hak akses kejaringan tersebut berdasarkan *port – port* yang dimiliki oleh *switch* tersebut, berbeda halnya dengan *switch unmanageable* yang hanya bekerja di layer *data link* atau layer 2 pada *switch* jenis ini tidak bisa melakukan konfigurasi.

Gambar 1. *Switch Manageable*

2.2 *Port Security*

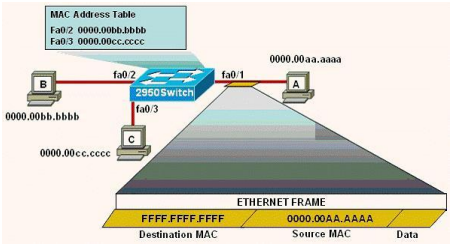
Dalam sebuah jaringan komputer keamanan sebuah jaringan dapat ditingkatkan salah satunya dengan menggunakan kemampuan sebuah *switch manageable* yaitu menggunakan *port-port* yang tersedia pada *switch* tersebut. Ada 2 jenis *switch port security* yaitu:

a. *Default / static port security*

Ketika *port security* ini di fungsikan maka *mac address port security* akan diaktifkan pada *port switch*, pengaturan *mac address* pada jenis *port security* ini untuk pengenalan *mac address* dilakukan secara manual dan alamat mac yang dimasukan atau dikonfigurasi yang di perbolehkan untuk terhubung ke port tersebut, sehingga jika *source address* bukanlah *address* yang telah kita defenisikan/tentukan sebelumnya *port* tidak akan mem-*forward packets*.

b. *Sticky port security*

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



Gambar 2. *Sticky Port Security*
(sumber: https://sites.google.com/site/ccnail2012/home/week/d7/d2c2-port-security)

Pada Gambar 2 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, contoh: jika didaftar hanya 3 (tiga) *mac* maka ketika ada perangkat yang ke 4 (empat) dengan otomatis *sticky port security* akan mencegah (blok) *mac* tersebut, sehinga perangkat yang terhubung tetap 3 yang pertama. Pada *port security* jenis ini untuk pengenalan *mac address* dilakukan secara otomatis, jika sebuah perangkat komputer yang terhubung dengan *swicth* dan melakukan *request* (ping) ke komputer lain maka komputer yang melakukan request akan mengirimkan *mac address* ke *switch* yang dilewati, oleh karena itu pendaftaran *mac address* tidak perlu dikonfigurasi satu-satu.

2.3 Perangkat yang Dipergunakan

Dalam implementasi sistem keamanan *port security* perlu sebuah hardware dan sebuah software yang dapat menunjang implementasi sistem keamanan di Laboratorium Komputasi STTA.

a. *Hardware* (perangkat keras) merupakan perangkat secara fisik ada, dapat dilihat dan dipegang. Sistem perangkat keras secara fungsional terdiri dari *input*, *process*, *output* dan *memory*. Adapun spesifikasi *hardware* yang digunakan dalam pengaplikasian sistem ini, yaitu:

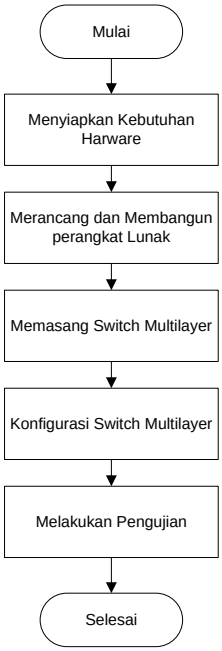
1) *Switch cisco catalyst* 2950T-24
2) Personal Komputer (Intel (R) Core(TM) i3-3217U CPU @ 1,80GHz (4CPUs), 2048 MB RAM)

b. *Software* (perangkat lunak) merupakan perangkat yang sifatnya abstrak yang berisi instruksi, program, prosedur, pengendali, pendukung dan aktivitas- aktivitas pengolahan perintah pada sistem komputer. Adapun spesifikasi minumum *software* yang dibutuhkan dalam pengaplikasian sistem ini, yaitu:

1) Ios Cisco

2) Sistem Operasi Windows 7 Enterprise
3) Bahasa Pemrograman PHP dan HTML

2.4 Metode Penelitian



Gambar 3. Metode Penlitian

3. Hasil dan Pembahasan

Pada penelitian ini untuk mengetahui efisiensi penggunaan *port security* di Lab. Komputasi ada dua pengujian yang pertama dilakukan pengujian penggunaan *bandwidth* sebelum dan sesudah implementasi keamanan dengan menggunakan *port security*, dan yang kedua dengan melihat keadaan Lab. Apakah masih ada kabel UTP yang berserakan atau dicabut dari pc aslinya.

Sebelum melakukan pengujian penggunaan bandwidth peneliti membuat *script* pendek untuk memantau penggunaan bandwidth di Lab. Komputasi seperti terlihat pada penggalan script dibawah ini.

```
1.  $jumlah_target = 1;
2.  $target[1] = "10.10.10.4/32";
3.  $nama_target[1] = "PC 4";
4.  require('routeros_api.class.php');
5.  define('MIKROTIK_IP', '12.12.12.1');
6.  define('MIKROTIK_USERNAME', 'admin');
7.  define('MIKROTIK_PASSWORD', '12345');
8.  define('SERVER', 'all');
9.  define('PROFILE', 'default');
10. $API = new routeros_api();
11. //koneksi ke mysql
12. $koneksi = mysqli_connect('localhost','root','12345', 'api');
13.
14. for ($j=1;$j<=$jumlah_target;$j++) {
15.
16. if ($API->connect(MIKROTIK_IP, MIKROTIK_USERNAME, MIKROTIK_PASSWORD))
17. {
18.  //echo "target = $target[$j]<br>";
19.  $API->write('/tool/torch', false);
20.  $API->write($target[$j], false);
```

```
21.     $API->write('=ip-protocol=any', false);
22.     $API->write('=mac-protocol=any', false);
23.     $API->write('=src-address='.$target[$j], false);
24.     $API->write('=dst-address=0.0.0.0/0', false);
25.     $API->write('=duration=2', false);
26.     $API->write("=interface=ether2-Local");
27.
28.     $ARRAY[$j] = $API->read();
29.     //print_r($ARRAY[$j]);
30.
31.     $jumlah = sizeof($ARRAY[$j]);
32.     $waktu = date("Y-m-d H:i:s");
33.
34.     for ($i=0;$i<$jumlah;$i++)
35.     {
36.                     $destination = $ARRAY[$j][$i]['dst-address'];
37.                      //echo "destination = $destination<br>";
38.                     $mac_protocol = $ARRAY[$j][$i]['mac-protocol'];
39.                      //echo "mac = $mac_protocol<br>";
40.                     $ip_protocol = $ARRAY[$j][$i]['ip-protocol'];
41.                     $tx = $ARRAY[$j][$i]['tx'];
42.                     $rx = $ARRAY[$j][$i]['rx'];
43.                     $tx_packets = $ARRAY[$j][$i]['tx-packets'];
44.                     $rx_packets = $ARRAY[$j][$i]['rx-packets'];

45.     $sql = "insert into torch (target,destination,waktu,mac_protocol,ip_protocol,tx,rx,tx_packets,rx_packets,bagian) values
        ('$target[$j]', '$destination', '$waktu','$mac_protocol', '$ip_protocol', $tx , $rx , $tx_packets , $rx_packets, '$nama_target[$j]')";

46.                     $query = mysqli_query($koneksi, $sql);
47.     } }
48.     $API->disconnect();
49.     }
```

Script diatas digunakan untuk menampilkan seluruh *torch* yang ada pada *router* mikrotik yang nantinya akan digunakan untuk memantau penggunaan *bandwidth* Lab. Komputasi. Pada Tabel 1 menunjukan penggunaan *bandwidth* yang dipantau oleh *Router* Mikrotik sebelum implementasi *port security* di Lab. Komputasi.

Tabel 1. Tabel Penggunaan *Bandwidth* sebelum Implementasi *port Security*

Data Traffict Lab Komputasi

Target = Web Server & Data Server

source	destination	waktu	mac_protocol	ip_protocol	tx	rx	tx-packets	rx-packets
PC 4 / 10.10.10.4/32	50.7.196.154	2018-10-10 09:33:38	ip	tcp	780.2	35.2	68	53
PC 4 / 10.10.10.4/32	10.10.10.3	2018-10-10 09:33:38	ip	tcp	2776	1848	2	3
PC 4 / 10.10.10.4/32	10.10.10.3	2018-10-10 09:33:33	ip	tcp	1880	480	1	1
PC 4 / 10.10.10.4/32	50.7.196.154	2018-10-10 09:33:33	ip	tcp	753.7	20.9	69	34
PC 4 / 10.10.10.4/32	50.7.196.154	2018-10-10 09:33:02	ip	tcp	543.8	25.4	48	40
PC 4 / 10.10.10.4/32	50.7.196.154	2018-10-10 09:32:59	ip	tcp	679.2	25.3	61	43
PC 4 / 10.10.10.4/32	10.10.10.3	2018-10-10 09:32:59	ip	tcp	1880	480	1	1

Pada Tabel 1 kolom *source* menunjukan alamat ip komputer yang diamati, sedangkan *TX Rate* adalah penggunaan *bandwidth* komputer yang diamati, nilai *TX Rate* dengan *destination ip address* 50.7.196.154 bergerak dengan *range* 1.000-2.000 bit/second yang artinya *bandwidth* 2 *Mbps* tidak bisa digunakan secara maksimal dikarenakan belum ada sistem keamanan yang mengamankan jaringan Lab. Komputasi, sehingga bisa menyebabkan adanya kebocoran atau pencurian bandwidth. Bisa dilihat pada Gambar 4 menunjukan daftar mac-address yang terdaftar dan didaftarkan di Switch Lab. Komputasi, sedangkan Gambar 5 menunjukan pada tabel *mac address* ada *mac address* yang tidak dikenal menggunakan akses Lab. Komputasi melalui switch Lab Komputasi.

Tabel 2. Penggunaan *Bandwidth* sebelum implementasi *Port Security*

No	Waktu	*Max Bandwidth* (bps)	*Max Bandwidth* (Mbps)	Prosentase Penggunaan *Bandwidth*
1	10-10-2018	1.956.000	1,96	98%
2	11-10-2018	1.722.221	1,72	86%
3	12-10-2018	2.000	0,002	0.1%
4	13-10-2018	0	0	0%
5	14-10-2018	0	0	0%
6	15-10-2018	1.500	0,0015	0.075%
7	16-10-2018	2.350	0,0024	0.12%
8	17-10-2018	1.721	0,0017	0.085%
9	18-10-2018	2.113	0,0021	0.105%
10	19-10-2018	1.850.000	1,85	92.5%
11	20-10-2018	0	0	0%
12	21-10-2018	0	0	0%
13	22-10-2018	1.821	0,0018	0.09%
14	23-10-2018	2.052	0,0025	0.125%
15	24-10-2018	1.356	0,0014	0.07%

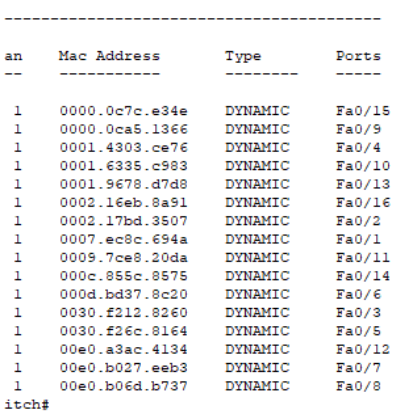
Perhitungan *Lost Bandwidth* yang digunakan pada Lab. Komputasi sebelum diimplementasikan sistem keamanan menggunakan *Port Security*.

$$\textit{Lost Bandwidth} = 100\% - \left[\frac{\text{Total \% penggunaan } \textit{Bandwidth}}{\text{Total Hari perhitungan}}\right]$$

$$\textit{Lost Bandwidth} = 100\% - \left[272{,}27\ \% \ /\ 11\right]$$

$$= 74{,}79\%$$

Dilihat pada Tabel 2 penggunaan bandwidth selama 15 hari dari tanggal 10 Oktober 2018 – 24 Oktober 2018 hampir setiap harinya access di Lab. Komputasi tidak bisa digunakan secara maksimal karena 74,79% bandwidth digunakan oleh pengguna yang tidak berkepentingan di Lab. Komputasi. Total hari perhitungan hanya 11 dari 15 kali percobaan dikarenakan 4 hari jatuh pada hari libur dan tidak ada pengguna yang menggunakan Lab. Komputasi.

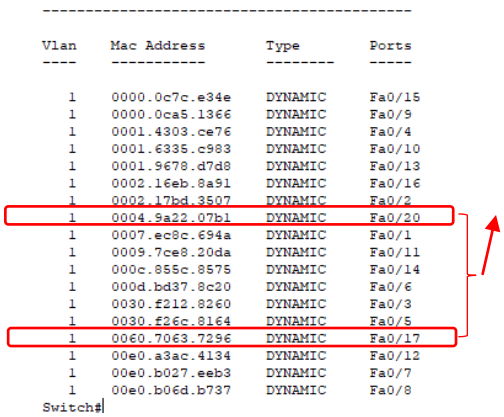


```
----------------------------------------

an    Mac Address       Type        Ports
--    -----------       --------    -----

 1    0000.0c7c.e34e    DYNAMIC     Fa0/15
 1    0000.0ca5.1366    DYNAMIC     Fa0/9
 1    0001.4303.ce76    DYNAMIC     Fa0/4
 1    0001.6335.c983    DYNAMIC     Fa0/10
 1    0001.9678.d7d8    DYNAMIC     Fa0/13
 1    0002.16eb.8a91    DYNAMIC     Fa0/16
 1    0002.17bd.3507    DYNAMIC     Fa0/2
 1    0007.ec8c.694a    DYNAMIC     Fa0/1
 1    0009.7ce8.20da    DYNAMIC     Fa0/11
 1    000c.855c.8575    DYNAMIC     Fa0/14
 1    000d.bd37.8c20    DYNAMIC     Fa0/6
 1    0030.f212.8260    DYNAMIC     Fa0/3
 1    0030.f26c.8164    DYNAMIC     Fa0/5
 1    00e0.a3ac.4134    DYNAMIC     Fa0/12
 1    00e0.b027.eeb3    DYNAMIC     Fa0/7
 1    00e0.b06d.b737    DYNAMIC     Fa0/8
itch#
```

Gambar 4. Tabel *Mac-Address* 1



```
----------------------------------------

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

   1    0000.0c7c.e34e    DYNAMIC     Fa0/15
   1    0000.0ca5.1366    DYNAMIC     Fa0/9
   1    0001.4303.ce76    DYNAMIC     Fa0/4
   1    0001.6335.c983    DYNAMIC     Fa0/10
   1    0001.9678.d7d8    DYNAMIC     Fa0/13
   1    0002.16eb.8a91    DYNAMIC     Fa0/16
   1    0002.17bd.3507    DYNAMIC     Fa0/2
   1    0004.9a22.07b1    DYNAMIC     Fa0/20
   1    0007.ec8c.694a    DYNAMIC     Fa0/1
   1    0009.7ce8.20da    DYNAMIC     Fa0/11
   1    000c.855c.8575    DYNAMIC     Fa0/14
   1    000d.bd37.8c20    DYNAMIC     Fa0/6
   1    0030.f212.8260    DYNAMIC     Fa0/3
   1    0030.f26c.8164    DYNAMIC     Fa0/5
   1    0060.7063.729e    DYNAMIC     Fa0/17
   1    00e0.a3ac.4134    DYNAMIC     Fa0/12
   1    00e0.b027.eeb3    DYNAMIC     Fa0/7
   1    00e0.b06d.b737    DYNAMIC     Fa0/8
Switch#
```

Mac Address tak dikenal

Gambar 5. Tabel *Mac-Address* 2

Karena adanya kebocoran atau pencurian *bandwidth* maka Lab. Komputasi mencoba untuk mengimplementasikan keamanan dengan menggunakan *port Security*. Konfigurasi *Switch* Lab. Komputasi menggunakan *Port Security*:

Konfigurasi statik:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0030.F212.8260
Switch(config-if)#
```

Konfiggurasi dinamik:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

Perbedaan konfigurasi statik dan dinamik hanya pada konfigurasi terakhir dimana statik *mac address* langsung dikonfigurasi sedangkan pada dinamik untuk *mac address* ditulis *sticky* yang artinya *mac address* akan didapatkan pada waktu komputer dihubungkan dengan *switch* yang dikonfigurasi. Setelah dilakukan konfigurasi *port security* dengan *maximum* 1 maka tidak akan ada personal komputer yang bisa terhubung kecuali yang sudah didaftarkan *mac address*nya.

Pada Tabel 3 nilai *TX Rate* dengan *destination* 50.7.196.154 bergerak dengan *range* 1.800.000-2.000.000 bps yang artinya *bandwidth* 2 *Mbps* bisa digunakan secara maksimal. Pada Tabel 4 adalah data penggunaan bandwidth di Lab. Komputasi pada tanggal 26 Oktober 2018 s/d 10 Novenber 2018 setelah diimplementasikannya Port Security di switch Lab. Komputasi.

Tabel 3. Tabel Penggunaan *Bandwidth* sesudah Implementasi *port Security*

Data Traffict Lab Komputasi

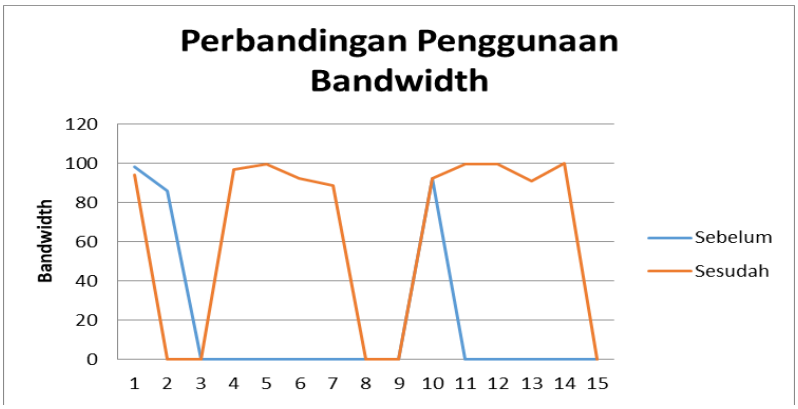
Target = Web Server & Data Server

source	destination	waktu	mac_protocol	ip_protocol	tx	rx	tx-packets	rx-packets
PC 4/ 10.10.10.4/32	50.7.196.154	2018-10-26 08:28:52	ip	tcp	1948176	99120	163	154
PC 4/ 10.10.10.4/32	50.7.196.154	2018-10-26 08:28:48	ip	tcp	1972080	117136	165	165
PC 4/ 10.10.10.4/32	10.10.10.3	2018-10-26 08:28:45	ip	tcp	3768	2752	3	4
PC 4/ 10.10.10.4/32	50.7.196.154	2018-10-26 08:28:45	ip	tcp	1852560	105200	155	155
PC 4/ 10.10.10.4/32	50.7.196.154	2018-10-26 08:28:40	ip	tcp	1960128	108976	164	158
PC 4/ 10.10.10.4/32	10.10.10.3	2018-10-26 08:28:40	ip	tcp	55208	2968	7	5
PC 4/ 10.10.10.4/32	50.7.196.154	2018-10-26 08:28:36	ip	tcp	1948176	54288	163	110

Pada Tabel 4 menunjukan bahwa *bandwidth* yang disediakan untuk Lab. Komputasi bisa digunakan secara maksimal. Dengan adanya Implementasi *port security* sangat berpengaruh pada penggunaan *bandwidth* di Lab. Komputasi dikarenakan hanya komputer yang terdaftar saja yang bisa mengakses *switch* Lab. Komputasi sehingga *bandwidth* untuk Lab. Komputasi sebesar 2 Mbps hanya digunakan untuk Lab. Komputasi saja dan kalau dilihat dilihat dari Tabel 4 *lost bandwidth* hanya= 4,6% sehingga dengan diimplementasikan port security kehingan bandwidth bisa berkurang sebesar= 74,79%-4,6%=70,19%.

Tabel 4. Penggunaan *Bandwidth* setelah implementasi *Port Security*

No	Waktu	*Max Bandwidth* (bps)	*Max Bandwidth* (Mbps)	Prosentase Penggunaan *Bandwidth*
1	26-10-2018	1.876.000	1,88	94%
2	27-10-2018	0	0	0%
3	28-10-2018	0	0	0%
4	29-10-2018	1.939.221	1,94	97%
5	30-10-2018	1.988.667	1,99	99,5%
6	01-11-2018	1.850.000	1,85	92,5%
7	02-11-2018	1.766.985	1,77	88,5%
8	03-11-2018	0	0	0%
9	04-11-2018	0	0	0%
10	05-11-2018	1.850.002	1,85	92.5%
11	06-11-2018	1.988.742	1,99	99,5%
12	07-11-2018	1.999.521	1,99	99,5%
13	08-11-2018	1.821.045	1,82	91%
14	09-11-2018	2.000.031	2,00	100%
15	10-11-2018	0	0	0%



Gambar 6. Gambar Perbandingan Penggunaan Bandwidth Sebelum dan Sesudah Implementasi Port Security

Pada Gambar 6 bisa dilihat bahwa grafik penggunaan sebelum dan sesudah implementasi sistem keamanan dengan menggunakan *port security* sangat bermanfaat, karena dengan implementasi ini pencurian dan penggunaan *bandwidth* yang tidak berkepentingan bisa dicegah.

Selain penggunaan *bandwidth* yang bisa dimaksimalkan penggunaan kabel UTP yang seharusnya digunakan pada personal Komputer Lab. Komputasi juga dapat digunakan sebagaimana mestinya.

4. Kesimpulan

Berdasarkan hasil dari penelitian dengan judul "*Implementation Port Security for Security Systems Network at the Computing Laboratory of Adisutjipto Technology College*" maka dapat diambil beberapa kesimpulkan sebagai berikut:

a. Implementasikan keamanan jaringan dengan menggunakan *port security* dapat memaksimalkan penggunaan *bandwidth* di Lab. Komputasi sebesar 95,4 %.
b. Implementasi *port security* dapat digunakan untuk mencegah penggunaan kabel UTP yang tidak bertanggungjawab.

Daftar Pustaka

[1] Sulaiman, K. (2016). Analisis Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security*. CESS (*Journal Of Computer Engineering, System And Science*) (Vol. 1, ISSN :2502-7131)
[2] Kusumaningrum, A. (2016, November). Pengujian Kinerja Jaringan Sistem Akses File Berbasis Client Server Menggunakan Samba Server. In Conference SENATIK STT Adisutjipto Yogyakarta (Vol. 2, pp. 129-134).
[3] Marin, G.A. (2015, November). *Network Security Basics, Security & Privacy*. IEEE. (Vol. 3, No 6 pp. 68-72).
[4] Saleh, I., Wintolo, H., & Nugraheni, D. (2014, November). Analisa Perbandingan Waktu Dan Kecepatan Transfer Pada Multi Protocol Label Switching (Mpls) Dengan Virtual Private Network (VPN) Untuk Perpindahan Dokumen Pada Jaringankomputer. In Compiler STT Adisutjipto Yogyakarta (Vol. 3, pp. 101-111).
[5] Pratama, A.W., Wintolo, H., & Astuti, Y. (2013). Konfigurasi Inter-Vlan Pada Cisco Berbasis Graphics User Interface (GUI) Sebagai Pembelajaran Peralatan Jaringan Komputer Cisco. In Compiler STT Adisutjipto Yogyakarta (Vol. 2, pp. 13-19).
[6] Suhendar, A. S. S., Sajati, H., & Astuti, Y. (2013). Perancangan Algoritma Anggi (Aa) Dengan Memanfaatkan Diffie-Hellman Dan Ronald Rivest (Rc4)Untuk Membangun Sistem Keamanan Berbasis Port Knacking. In Compiler STT Adisutjipto Yogyakarta (Vol. 2, pp. 59-66)
[7] Kusumaningrum, A., & Sianturi, R. (2015). Perancangan Pengamanan Server Secara Otomatis Menggunakan Metode Adam (Automatic Event Detection And Activity Monitoring). In Compiler STT Adisutjipto Yogyakarta (Vol. 4, pp. 29-35)
[8] Sudaryanto, S. (2018). *The Effect Of Multi Layer Switching For Data Transfer Speeds On Computer Network*. In Compiler STT Adisutjipto Yogyakarta (Vol. 7, No. 2)
[9] Sofana, I. (2010). Cisco CCNA & Jaringan Komputer. Bandung. Informatika Bandung.
[10] Sutanto, F. A., Yulianton, H., & Razaq, J. A. (2011). Rancang Bangun Vlan Untuk Segmentasi Jaringan Pada Cyber Campus Laboratory Universitas Stikubank. Dinamik, 16(2).