JUSTIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989
Vol. 7, No. 1, Januari 2019

Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen

Ridatu Ocanitra[#1], Muhamad Ryansyah[*2]

[#]*Fakultas Teknik,Universitas Bina Sarana Informatika*
[1]ridatu.rdo@bsi.ac.id

[*]*Sistem informasi, STMIK Nusamandiri Jakarta*
Jl. Damai No.8 Warung Jati Barat, Jakarta Selatan, Indonesia, 12740
[2]muhamad.mur@nusamandiri.ac.id

***Abstrak*—Perkembangan teknologi dalam jaringan komputer lambat laun semakin pesat seiring dengan meningkatnya kebutuhan akan akses jaringan yang efisien, stabil serta keamanan yang handal. Perusahaan membutuhkan keamanan jaringan untuk menjaga data perusahaan, serta untuk mengontrol dan mengintegrasikan semua penguna koneksi jaringan. Perusahaan ini dengan banyak karyawan dan divisi yang berbeda-beda sehingga sering dilakukan perpindahan tempat kerja atau adanya karyawan baru. Sehingga sangat diperlukan sistem keamanan jaringan yang terjamin untuk menentukan pengunaan hak akses pada jaringan. Untuk mengatasi masalah tersebut, maka perusahaan sangat membutuhkan adanya pengamanan jaringan pada setiap *port* lan (*local area network*) yaitu dengan menggunakan metode default atau *static port security*, *port security dynamic learning* dan *sticky port security* pada *port* yang berada diruang kerja tersebut. Hal ini berguna untuk memblok akses jaringan pada karyawan yang tidak melaporkan perpindahan tempat kerja dan dapat mencegah terjadinya pencurian data oleh orang asing atau bukan dari karyawan perusahaan tersebut.**

Kata kunci*— *Network Security, Port security, Network,* Hak akses,*Firewall

I. PENDAHULUAN

Di era saat ini kebutuhan akan jaringan komputer semakin bertambah penting baik dalam pendidikan maupun dalam sebuah pekerjaan dan salah satu hal penting dalam mengelola jaringan komputer yaitu keamanan 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. 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 *security port* dimana ini merupakan teknik yang akan mengizinkan siapa saja yang berhak menggunakan akses jaringan melalui *port* yang tersedia di *switch*[1].

Dalam kasus yang saat ini terjadi di PT Vitta Multi Oksigen adalah seringnya terjadi pencurian data disaat karyawan tersebut pindah ruangan atau keluar dari perusahaan sehingga membutuhkan pengamanan data menggunakan perangkat yang bisa mengontrol hak akses jaringan (*firewall security port*) yang sangat di butuhkan sekali terlebih saat ini di perusahaan tersebut belum menggunakan pengamanan seperti implementasi *firewall security port* atau sejenisnya.

Keterbatasan LAN melahirkan sebuah teknologi VLAN yang memungkinkan adanya konfigurasi dari suatu jaringan komputer secara virtual (virtualisasi).[2]

Masalah keamanan termasuk dalam salah satu aspek penting dari sebuah sistem informasi, seperti pada jaringan komputer.Terhubungnya LAN (*Local Area Network*) atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang membuka celah untuk merusak kinerja sistem.[3]

PT Vitta Multi Oksigen adalah perusahaan yang bergerak dalam bidang penjualan alat – alat kebutuhan medis. Pada kantor ini sering dilakukan perpindahan tempat kerja atau adanya karyawan baru. Dengan terjadinya perpindahan tersebut, perusahaan pasti perlu mendata kembali lokasi tempat kerja karyawannya, sehingga perusahaan ini sangat membutuhkan adanya pengamanan jaringan pada setiap *port* LAN (*Local Area Network*) yaitu dengan menggunakan metode default/ static *port security*, *port security dynamic* learning dan sticky *port security* pada *port* yang berada diruang kerja tersebut. Hal ini berguna untuk memblok akses jaringan pada karyawan yang tidak melaporkan perpindahan tempat kerja dan dapat mencegah terjadinya pencurian data oleh orang asing atau bukan dari karyawan perusahaan tersebut.

Saat ini pengembangan teknologi juga yang berhubungan proses penyebaran berita telah banyak dilaksanakan. terhadap teknologi penyebaran berita dilaksanakan dengan dua metode yakni melalui media *online* serta media *offline*, namun perkembangan banyak dilaksanakan terhadap media *online*. Media *offline* tidak banyak merasakan penyebaran disebabkan

Submitted 07-12-2018; Revised 18-12-2018; Accepted 16-01-2019

penggunaan media *offline* dinilai terbatas terhadap ruang lingkup tertentu Walaupun dinilai terbatas terhadap ruang lingkup terdefinisi jelas seperti perkantoran, media *offline* dinilai amat efisien buat media penyebaran berita dilingkungan tersebut. Namun penyampaian berita secara *offline* tak secepat media *online*, disebabkan media *online* didukung oleh teknologi yang paling efisien yakni jaringan komputer. terhadap ruang lingkup perkantoran lazimnya telah banyak menggunakan jaringan komputer sebagai teknologi pendukung pekerjaan dan sebagai media penyampaian informasi. Jaringan komputer terhadap saat ini amat berkembang dan menjadi kebutuhan.[4]

Maka dari itu penulis mengusulkan perusahaan menggunakan pengamanan jaringan komputer dengan pemberian default/ static *port security* (sebuah kemampuan switch untuk mendaftarkan dan membatasi perangkat yang dapat terkoneksi pada suatu *port*), *port security dynamic* learning (kemampuan switch untuk mengenali mac address secara dinamis ketika perangkat komputer terhubung ke switch dan akan menyimpan mac addres tersebut ke mac addres table), sticky *port security* (kemampuan switch dalam mengenal mac address pada tiap – tiap perangkat yang terhubung dan akan memblokir *mac address* yang telah terdaftar). Pada setiap *port* karena dapat mencegah terjadinya pencurian data. Selain itu dengan menggunakan *security port* merupakan salah satu solusi kemanan jaringan berupa protokol keamanan yang berada di setiap tempat kerja karyawan.

Keamanan jaringan merupakan suatu cara atau suatu system yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan dan pencurian data perusahaan[5].

Port adalah tempat di mana informasi masuk dan keluar dari komputer, *port* scanning mengidentifikasi pintu terbuka ke komputer. *Port* memiliki penggunaan yang sah dalam mengelola jaringan, tetapi scanning *port* juga bisa berbahaya jika seseorang sedang mencari titik akses yang lemah untuk masuk ke komputer anda.[6]

II. LANDASAN TEORI

A. Peralatan pendukung

Perangkat jaringan adalah semua komputer, *peripheral, interface card*, dan perangkat tambahan yang terhubung ke dalam suatu sistem jaringan komputer untuk melakukan komunikasi data.[7] Perangkat jaringan komputer terdiri dari :

1) Server merupakan pusat kontrol dari jaringan komputer. Server berfungsi untuk menyimpan informasi dan untuk mengelola suatu jaringan komputer. Server akan melayani seluruh client atau workstation yang terhubung ke jaringan. Sistem operasi yang digunakan pada server adalah sistem operasi yang khusus yang dapat memberikan layanan bagi workstation.

2) Network Interface Card (NIC) merupakan perangkat keras yang memungkinkan suatu komputer dan fasilitas komunikasi untuk bertukatar informasi dan mengontrol setiap informasi. Network Interface Card (NIC) juga diartikan sebagai expansion board yang digunakan supaya komputer dapat dihubungkan dengan jaringan. Sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu. NIC biasa disebut dengan LAN card.

3) Switch adalah perangkat yang juga berfungsi untuk menghubungkan multiple komputer. Switch secara fisik sama dengan hub tetapi logikalnya sama dengan barisan brigde. Peningkatan kecerdasan dibandingkan hub, yaitu memiliki pengertian terhadap alamat MAC (Medium Access Control) atau pada link layer model OSI sehingga hanya mengirimkan data pada port yang dituju (unicast). Proses kerjanya adalah apabila paket data datang, header dicek untuk menentukan di segment mana tujuan paket datanya. Kemudian data akan dikirim kembali (forwaded) ke segment tujuan tersebut.

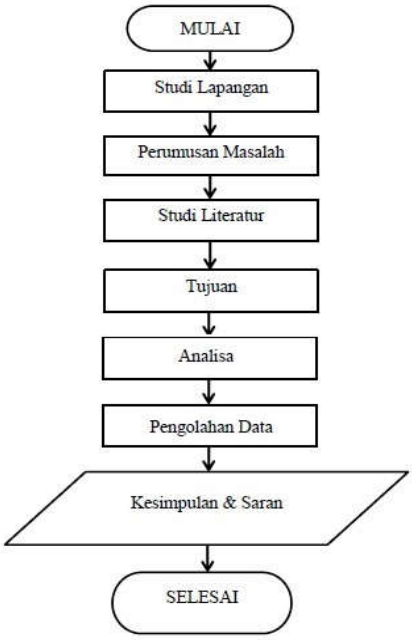
4) Open System Interconnection adalah layer yang diciptakan oleh International Standard Organization (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Standar ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien. Terdapat tujuh layer pada model OSI, setiap layer bertanggung jawab secara khusus pada proyek komunikasi data. Misal, satu layer bertanggung jawab untuk membentuk koneksi antar perangkat, sementara layer lainnya bertanggung jawab untuk mengoreksi terjadinya “error” selama proses transfer data berlangsung.

5) Internet Protocol (IP) adalah metode atau protocol untuk mengirimkan data ke internet. Setiap computer (biasanya disebut host) dalam internet setidaknya harus mempunyai sebuah alamat IP yang unik yang mengidentifikasikan komputer tersebut terhadap kamputer lainnya. Ketika anda mengirimkan atau menerima data (contoh: email atau website), pesan akan dibagi-bagi menjadi beberapa paket. Setiap berisikan IP pengirim dan IP penerima. Gateway yang menerimanya akan langsung mem-forward ke tujuan melalui jalur terbaik yang ditemukan sambil mengingat IP pengirim dan penerima. Karena pesan tersebut terbagi-bagi dalam paket dan bisa jadi diterima tidak secara berurutan ditujuan, IP tidak akan pernah memperhatikan, hanya megirimkan saja. TCP (Transmission Control Protocol) nantinya yang akan meletakkannya dalam urutan yang benar. Setiap komputer dalam suatu jaringan mempunyai identifikasi alamat yang unik. Ada dua yang digunakan untuk pengelamatan komputer dalam sebuah protocol TCP/IP Network.

II. METODOLOGI PENELITIAN

Penulisan atau penelitian ini di susun secara sistematis hingga mendapatkan hasil yang optimal. Langkah untuk penelitian ini merupakan rangkaian prosedur tersturktur dan terarah agar tujuan dari penulisan ini dapat tercapai dengan baik. Berikut langkah-langkah *flowchart* yang digunakan untuk penelitian ini.

Korespondensi : Muhamad Ryansyah



Gambar 1. *Flowchart* penelitian

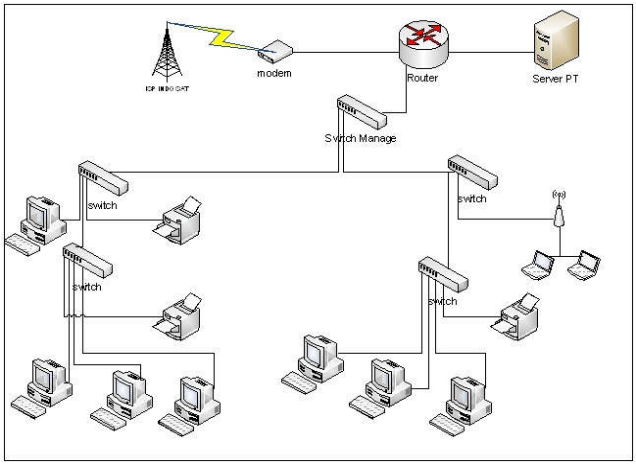
Untuk manajemen jaringan di kantor Vitta Multi Oksigen menggunakan active directory yang ada pada Windows Server 2008R2. *Active Directory Domain Services* (AD DS) menyediakan database terdistribusi yang menyimpan dan mengelola informasi tentang sumber daya jaringan. Administrator dapat menggunakan AD DS untuk mengatur elemen jaringan, seperti pengguna, komputer, group, printer, aplikasi, dan objek directory lain dari satu lokasi terpusat secara aman.

Menjelaskan kronologis penelitian, termasuk desain penelitian, prosedur penelitian (dalam bentuk algoritma, Pseudocode atau lainnya), bagaimana untuk menguji dan akuisisi data. Deskripsi dari program penelitian harus didukung referensi, sehingga penjelasan tersebut dapat diterima secara ilmiah.

Topologi jaringan komputer yang digunakan pada kantor Vitta Multi adalah topologi Star, yang mempunyai sistem jaringan komputer yang terdiri dari beberapa buah switch, jaringan yang terpasang pada gedung kantor menggunakan Router Board 1100 AHX2 dan D-link Switch DGS-1210-52, dan belum membentuk suatu jaringan komputer LAN (*local area network*).

Jaringan komputer adalah sekumpulan komputer yang dapat saling berhubungan antara satu dengan lainnya dengan menggunakan media komunikasi,sehingga dapat saling berbagi data, informasi, program, dan perangkat keras.[8]

D-link Switch DGS-1210-52 yang dipakai untuk mengelompokkan user berdasarkan departemen, atau mengelompokkan suatu group pekerja disetiap lantainya, jaringan komputer LAN merupakan komponen jaringan komputer yang memiliki banyak *port* yang akan menjadi penghubung bagi banyak titik jaringan atau node sehingga akan membentuk jaringan komputer LAN pada topologi star.



Gambar 2. Topologi Jaringan

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token ring dan star. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan kekurangan / kerugian dari masing - masing topologi berdasarkan karakteristiknya.[9]

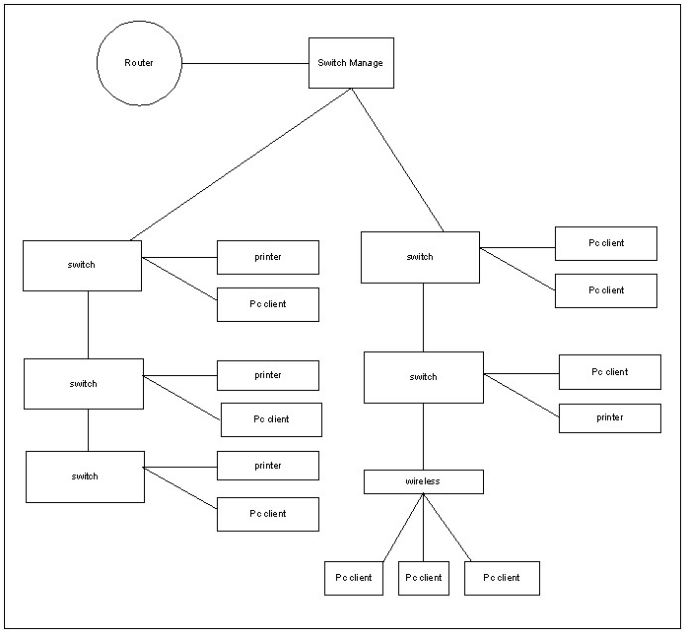
Setelah penulis melakukan penelitian di Vitta Multi penulis dapat menggambarkan rangkaian dari jaringan komputer *local area network* yang terdapat dilokasi tersebut, sesuai dengan kebutuhan jaringan komputer-komputer *Client* atau yang dinamakan dengan Workstation, alur dari jaringan yang di terapkan pada perusahaan meliputi workstation dari tiap-tiap divisi yang ada di Vitta Multi.

Namun jika pemberian alamat IP dilakukan secara statik akan membuat hasil yang negatif terhadap admin jaringan, sebab menghasilkan waktu yang lama untuk pemberian alamat IP. Tetapi masalah ini dapat di tangani dengan memilih pemberian alamat IP menggunakan DHCP. *Dynamic Host Configuration Protocol* (DHCP) adalah salah satu metode pemberian alamat IP otomatis, PC akan meminta IP yang benar dari router. Setting DHCP dapat dilakukan pada router dengan menggunakan CLI (*Command Line Interface*).Dengan DHCP administrator jaringan tidak memerlukan waktu untuk memikirkan host IP yang akan digunakan karena sudah disediakan router secara otomatis. Admin jaringan hanya memilih DHCP atau obtain IP Address Automatically pada pemberian alamat IP.[10]

Untuk pengalamatan IP client menggunakan *Dynamic* Host Configuration Protocol (DHCP) server untuk pengaturannya dengan range IP 172.20.0.0/24 – 172.47.255.254/24. Dengan masing-masing client menggunakan IP 172.20.100.5 sebagai DNS server, IP 172.20.100.6 sebagai WINS server dan IP 172.20.100.1 sebagai default gateway. Pengaturan ini berlaku untuk semua *Client* yang berada disetiap lantai gedung tersebut.

Korespondensi : Muhamad Ryansyah

Adapun dari skema rangkaian jaringan computer yang terdapat di kantor Vitta Multi Oksigen, Jakarta Selatan yaitu terdapat pada gambar sebagai berikut:



Gambar 3. Skema Jaringan

Keamanan jaringan adalah salah satu aspek penting dalam dunia internet. Suatu jaringan internal perusahaan membutuhkan keamanan khusus yang dapat menjaga data-data penting dari serangan hacker karena itu sangat dibutuhkan *firewall*. *Firewall* adalah suatu sistem pertahanan terdepan pada suatu jaringan, sebagai peralatan yang memproteksi aliran data pada suatu jaringan. Vitta Multi menggunakan *firewall* Cisco Asa 5510 Series sebagai *firewall* dalam jaringannya. Dengan fitur yang dimiliki oleh Cisco Asa seperti, *remote access, Intrusion Prevention, content Security, unified communications, botnets*, dan karena beberapa hal lain, maka memilih Cisco Asa 5510 Series sebagai *firewall*-nya.

Untuk Proxy-nya juga menggunakan Cisco Asa untuk memberikan solusi yang paling efektif untuk manajemen lalu lintas P2P (Point to Point) , intranet pencegahan rahasia pengungkapan, akses internet catatan perilaku, keamanan on-line dan lain-lain. Untuk perlindungan *on-line* yang otomatis dapat menyaring halaman web bahwa virus , Trojan dan lain script berbahaya dan *plug-in* , sehingga untuk menghadapi potensi risiko di muka, perangkat ini dapat juga memblokir dan alarm intranet virus, Trojan dan lain-lain, sehingga dapat melindungi keamanan intranet dari berbagai aspek.

Penyebaran malware komputer pada jaman sekarang lebih cepat dan mudah dikarenakan juga oleh kemajuan-kemajuan teknologi komputer dan spesifikasi komputer tersebut. Salah satu kerja dari malware komputer ini adalah dengan menginfeksi salah satu file di komputer kemudian *malware* tersebut menyebar ke semua file yang ada di komputer, tidak hanya dalam komputer tersebut yang terkena *malware*. Jika dalam satu jaringan yang besar *malware* tersebut akan menyebar melalui jaringan internal atau yang terhubung internet dan akan dapat dicuri file yang ada dalam satu jaringan karena komputer saling terhubung satu sama lain sehingga pastinya setiap komputer akan saling berbagi file. Sebuah malware diciptakan untuk merusak atau membobol system operasi dengan melalui *script* yang dirahasiakan, artinya disisipkan oleh penyerang.[11]

Berikut akan ditampilkan tabel tentang spesifikasi hardware dan *software* jaringan yang sudah penulis dapatkan selama melakukan penelitian , untuk spesifikasi yang digunakan dapat dilihat pada table berikut.

TABEL 1
SPESIFIKASI *HARDWARE* DAN *SOFTWARE* JARINGAN

Type	**Perangkat**			**Jml**
	Spesifikasi		**OS/Software**	
PC Client	CPU Type : CPU Merk : Processor : Memory : Harddisk :	HP PRO 3330MT HP CORE i3-2120 3.3GHZ DDR3 4GB Seagate 500 GB	Windows 7, 7zip, Adobe Reader, Ms. Office 2010, Mosaic 1P, Symantec	368
Notebook	CPU Type : CPU Merk : Processor : Memory : Harddisk :	HP Probook 430 G3 HP Core i7 2,5 GHz DDR3 4GB 1TB	Windows 7, 7zip, Adobe Reader, Ms. Office 2010, Mosaic 1P, Symantec	6
	CPU Type : CPU Merk : Processor : Memory : Harddisk :	HP Probook 4430S HP Core i3 2,3 GHz DDR3 2GB 500GB	Windows 7, 7zip, Adobe Reader, Ms. Office 2010, Mosaic 1P, Symantec	13
Router	Type :	RB-1100AHX2		1
Switch Manage	Type :	D-Link DES1210-52		1
Switching	Type :	TP-link SF1008		15
Firewall Router	Type :	Cisco Asa 5510 Series		1
Printer	Type :	HP GT 5820 All in one	Driver	6
Printer	Type :	HP LaserJet Pro P1560	Driver	2

III. HASIL DAN PEMBAHASAN

A. Manajeman jaringan usulan

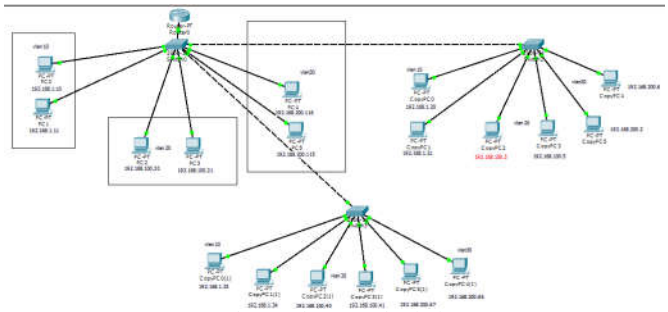
Manajemen jaringan yang akan diusulkan untuk menghadapi permasalahan yang dihadapi oleh kantor Vitta Multi Oksigen adalah diimplementasikannya keamanan jaringan *Firewall Security port* yang berfungsi untuk memberikan keamanan jaringan dan merupakan teknik yang akan mengizinkan hak akses melalui *port* 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 ke *port* 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.

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.

Korespondensi : Muhamad Ryansyah

B. Usulan topologi jaringan

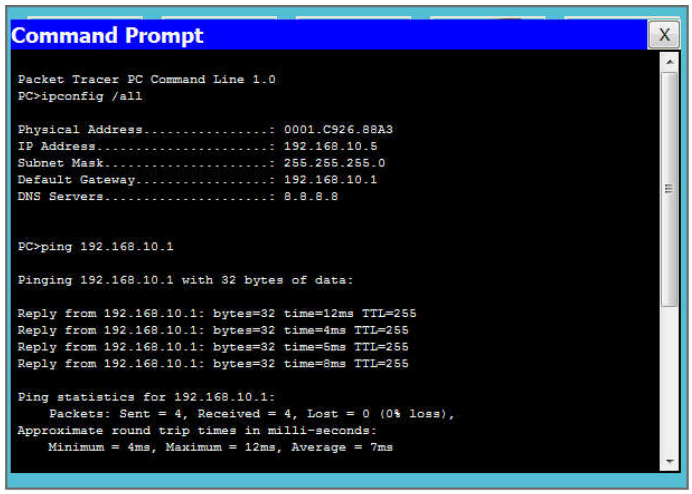
Pada penelitian ini penulis mencoba untuk menggambarkan dalam bentuk simulasi implementasi jaringan usulan tersebut menggunakan *software s*imulator. *Software* yang penulis gunakan adalah Cisco Packet Tracer.



Gambar 4. Skema usulan jaringan

C. Pengujuan jaringan awal

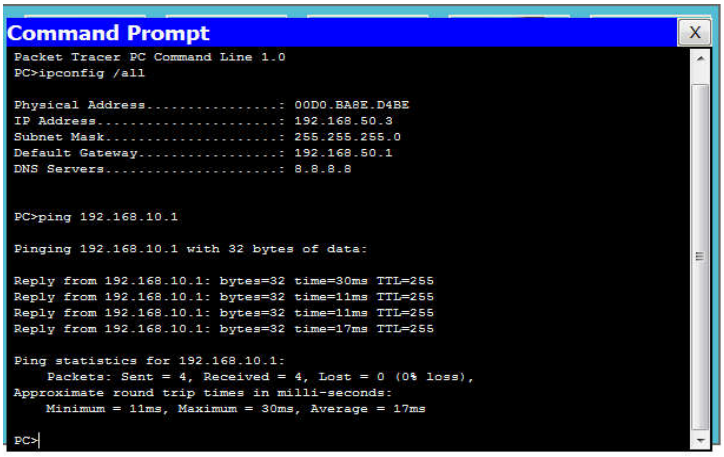
Pengujian jaringan awal keamanan jaringan dilakukan dengan melakukan percobaan koneksi jaringan antara *client* kantor dengan perangkat yang digunakan komputer yang berbeda vlan. Dalam pengujian awal ini, menggunakan *software paket Tracert* yang sudah di *routing* dan *switching*. Switch yang di konfigurasi 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.



```
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ipconfig /all

Physical Address.....: 0001.C926.88A3
IP Address.....: 192.168.10.5
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1
DNS Servers.....: 8.8.8.8


PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=12ms TTL=255
Reply from 192.168.10.1: bytes=32 time=4ms TTL=255
Reply from 192.168.10.1: bytes=32 time=5ms TTL=255
Reply from 192.168.10.1: bytes=32 time=8ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 12ms, Average = 7ms
```

Gambar 5. Hasil Tes Ping vlan 10 lt 1 ke vlan 30 lt2

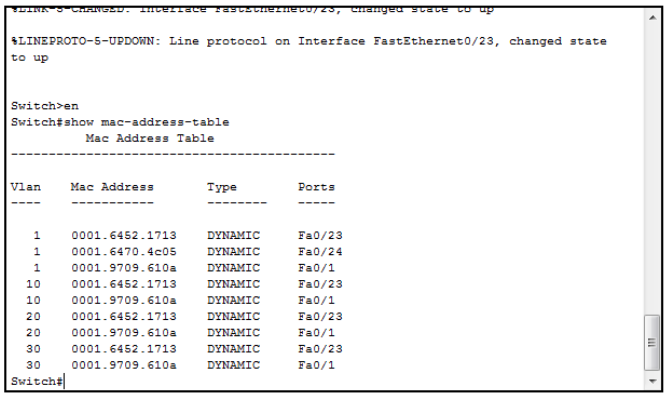
Dari gambar di atas dapat dilihat bahwa ping dapat berjalan dengan lancar tanpa terputus. Hal ini menunjukan bahwa jaringan sudah terkoneksi otomatis tanpa adanya keamanan jaringan yang mendeteksi detail perangkat yang terhubung. Kemudian pada komputer tersebut melakukan perpindahan lokasi kerja ke lantai 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 router kantor vitta multi dengan PC ip 192.168.50.2 gateway 8.8.8.8 dengan menggunakan *software cisco packet Tracert.*



```
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ipconfig /all

Physical Address.....: 00D0.BA8E.D4BE
IP Address.....: 192.168.50.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.50.1
DNS Servers.....: 8.8.8.8


PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=30ms TTL=255
Reply from 192.168.10.1: bytes=32 time=11ms TTL=255
Reply from 192.168.10.1: bytes=32 time=11ms TTL=255
Reply from 192.168.10.1: bytes=32 time=17ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 30ms, Average = 17ms

PC>
```

Gambar 6. *Test ping paket data kantor Vitta Multi*

Gambar diatas 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*.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state
to up


Switch>en
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0001.6452.1713    DYNAMIC     Fa0/23
   1    0001.6470.4c05    DYNAMIC     Fa0/24
   1    0001.9709.610a    DYNAMIC     Fa0/1
  10    0001.6452.1713    DYNAMIC     Fa0/23
  10    0001.9709.610a    DYNAMIC     Fa0/1
  20    0001.6452.1713    DYNAMIC     Fa0/23
  20    0001.9709.610a    DYNAMIC     Fa0/1
  30    0001.6452.1713    DYNAMIC     Fa0/23
  30    0001.9709.610a    DYNAMIC     Fa0/1
Switch#
```

Gambar 7. Mac address table

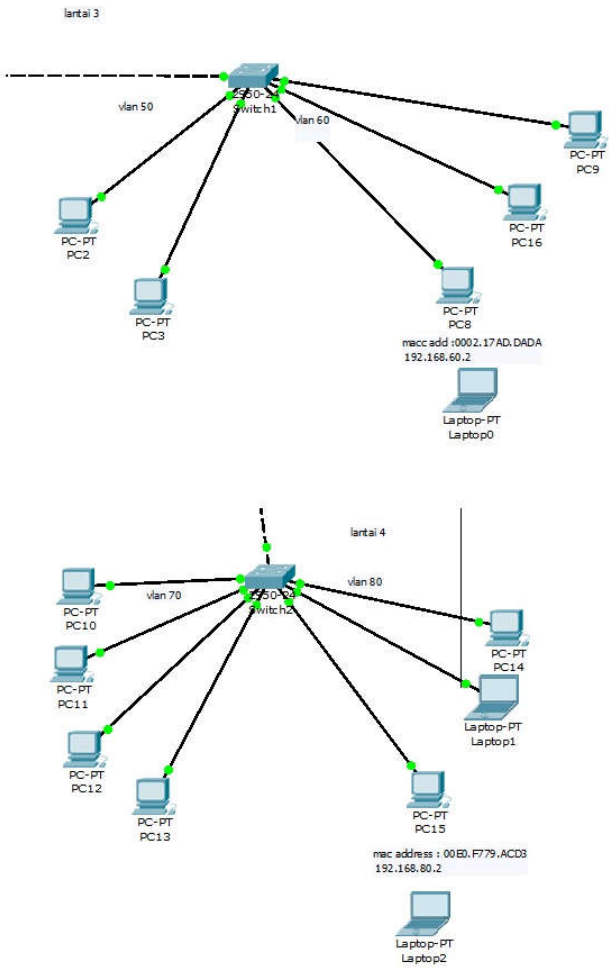
Terlihat pada gambar 7 bahwa mac address dari perangkat yang terkoneksi, namun tidak terjadi manajemen dan system keamanan jaringan yang baik. Karena setiap perangkat yang dihubungkan pada jaringan tersebut bersifat *dynamic* dan dapat selalu terkoneksi karena tidak adanya *security* pada setiap *port* akses.

D. Pengujian jaringan akhir

Dengan keamanan jaringan mengunakan *Security port*, dalam hal ini 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*.

Korespondensi : Muhamad Ryansyah



Gambar 8. Tes koneksi pada perangkat di packet tracer

Gambar 9. Tes ping ke router dan deskripsi mac address perangkat

Pada switch 192.168.50.0 dan 192.168.70.0
Switch(config)#int ra fa0/1-2
Switch(config-if-range)#switch*port* mode access
Switch(config-if-range)#switch*port port-security*
Switch(config-if-range)#switch*port port-security* mac-address sticky
Switch(config-if-range)#switch*port port-security* violation restric
Switch(config-if-range)#ex
Switch(config)#int fa0/3
Switch(config-if)#switch*port* mode access
Switch(config-if)#switch*port port-security*
Switch(config-if)#switch*port port-security* mac-address sticky
Switch(config-if)#switch*port 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.

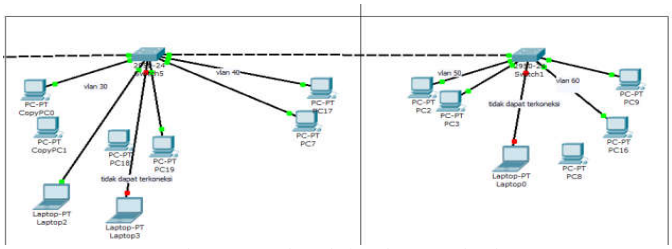
Terlihat bahwa mac address dari perangkat yang terkoneksi akan menambahkan macc address secara otomatis, kemudian hasil ping masih dapat berjalan. Dalam hal ini perangkat yang didaftarkan pertama dan kedua akan terkoneksi pada jaringan yang ada, namun jika perangkat yang terkoneksi tidak sesuai dengan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

Switch#show mac-address-table
Mac Address Table

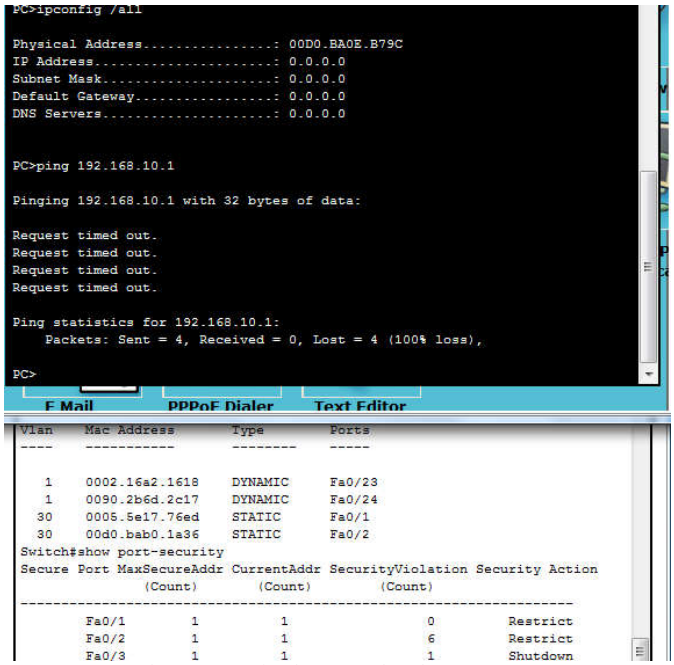
Vlan	Mac Address	Type	*Port*s
1	0030.a332.2e5e	*DYNAMIC*	Fa0/24
50	0005.5e52.9696	STATIC	Fa0/1
50	0060.5c83.da4c	*DYNAMIC*	Fa0/24
50	00d0.ba8e.d4be	STATIC	Fa0/2
60	0002.168e.750c	STATIC	Fa0/5
60	0010.1100.eaa3	STATIC	Fa0/6
60	0060.3e24.0dc4	STATIC	Fa0/7
60	0060.5c83.da4c	*DYNAMIC*	Fa0/24

Korespondensi : Muhamad Ryansyah

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



Gambar 10. Tes koneksi pada perangkat baru



Gambar 11. Tes ping ke router dan show *port security*

Diatas 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 (Count)	CurrentAddr (Count)	*Security*Violation (Count)	*Security* Action
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

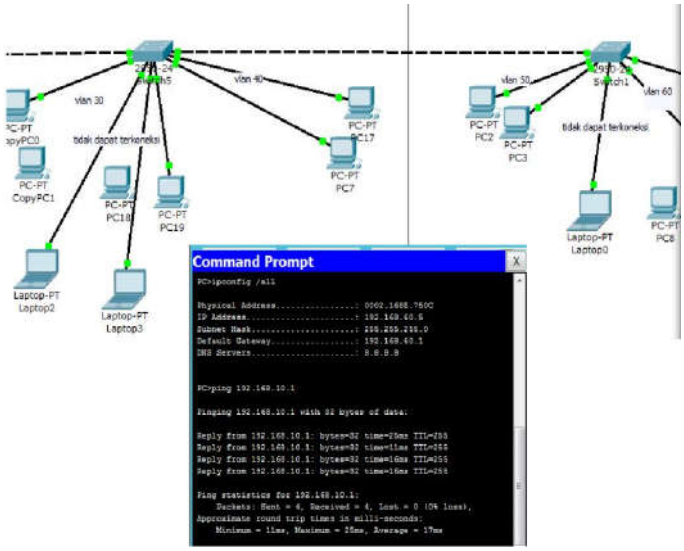
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
Switch(config-if)#no shutdown

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

Switch>en

Switch#show *port-security*

Secure *Port*	MaxSecureAddr	CurrentAddr	*Security*Violation	*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 12. *Tes ping ke pc kantor lt 3 dan lt 4 ke router lt 1*

Terlihat pada gambar 12 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.

IV. KESIMPULAN

Setelah mempelajari dan menganalisa sistem jaringan komputer pada kantor VITTA Multi Jakarta, dengan ini penulis dapat menyimpulkan bahwa jaringan komputer yang berada di gedung Vitta Multi Jakarta adalah sebagai berikut:

- Penerapan sistem kemananan yang digunakan dengan dhcp pada ip client sangat mudah merespon koneksi jaringan dan dapat memudahkan user bekerja diseluruh *port* tempat kerja yang ada.
- Dengan menggunakan *Security port*, maka system keamanan jaringan diterapkan lebih aman untuk menghidari koneksi jaringan dari akses yang tidak berkepentingan, serta menjaga data tersebut karena dapat dicuri oleh pihak yang tidak bertanggung jawab.
- Dengan menggunakan *Firewall Security port*, maka pihak IT dapat memanajemen setiap penguna jaringan, dan mendapatkan informasi jika terdapat perpindahan, karena perangkat yang tidak didaftarkan hak aksesnya akan diblok untuk terkoneksi ke jaringan tersebut.

REFERENSI

[1] O.K. Sulaiman. Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch *Port* Securiity. Jurnal Ilimiah "Computer Engineering" Universitas Islam Sumatera Utara. CESS (Journal Of Computer Engineering, System And Science) Vol 1, No 1, Januari 2016

[2] F. Muhamad, F. Andrew, and B. S. Hendra "SIMULASI JARINGAN VIRTUAL *LOCAL AREA NETWORK* (VLAN) MENGGUNAKAN POX CONTROLLER", JURNAL TEKNIK INFORMATIKA VOL. 10 NO. 1, 2017.

[3] W.J.D. Yanuar and R. Imam "ANALISIS PERANCANGAN *FIREWALL* PAKET FILTERING DAN PROXY SERVER UNTUK OPTIMASI BANDWIDTH", Jurnal Sarjana Teknik Informatika Volume 3 Nomor 1, Februari 2015.

[4] A. Haryadi, H. Priyanto, H. Anra ," RANCANG BANGUN APLIKASI PENYISIPAN BERITA DENGAN INTERNET CONTENT ADAPTATION PROTOCOL", Jurnal Sistem dan Teknologi Informasi (JUSTIN) Vol. 5, No. 3, 2017.

[5] S. Alabady. "Design and Implementation of a Network *Security* Model for Cooperative Network. International Arab Journal of e-Technology", (Vol. 1, No. 2). Iraq: University of Mosu.2009.

[6] T.A. Ahanger," *Port* Scan - A *Security* Concern," International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 10, April 2014.

[7] N. Kukuh, (2016), Jaringan Komputer Menggunakan Pendekatan Praktis Jakarta .Media tara.

[8] Rohman. "Analisis dan Perancangan Jaringan Komputer Asrama Putri Boarding School MAN 1". Surakarta (Vol. II). Surakarta: Indonesian Jurnal on Networking and *Security* (IJNS), 1, 2013.

[9] Supriyadi and Gartina, "Memilih Topologi Jaringan dan Hardware Dalam Desain Sebuah Jaringan Komputer ".Informatika Pertanian Volume 16 No. 2, 2007

[10] N. Juwanda, Fajrillah and T.M. Diansyah "IMPLEMENTASI STATIC NAT TERHADAP JARINGAN VLAN MENGGUNAKAN IP *DYNAMIC* HOST CONFIGURATION PROTOCOL (DHCP)", Jurnal Ilmiah Informatika Volume 1 No. 1 / Desember 2016.

[11] R. Adenansi and L.A. Novarina, "Malware *Dynamic*," Jurnal of Education and Information Communication Technology., Volume 1, Nomor 1, Tahun 2017: 37 – 43.

Korespondensi : Muhamad Ryansyah