

Pembatasan Jumlah *Client* Menggunakan *Security MAC-Address with Cisco*

Martias, Ramda Fadillah Djuanda

Jurusan Teknologi Komputer, Universitas Bina Sarana Informatika

Correspondence Author: martias.mts@bsi.ac.id

Abstrak

Seiring dengan perkembangan teknologi informasi dan komunikasi pada saat ini, suatu jaringan komputer sangat dibutuhkan agar dapat menghubungkan berbagai macam bidang diantaranya untuk berbagi informasi dan komunikasi jarak jauh, baik itu dibidang pemerintahan, pendidikan, bahkan dibidang bisnis moderen sekalipun, maka daripada itu internet sangat berpengaruh dalam kehidupan saat ini karena hampir semua kegiatan yang biasa manual dikerjakan seseorang sekarang ini dapat dilakukan dengan cara online. Pada PT. Pertamina Patra Niaga telah berjalan suatu jaringan LAN, oleh karena itu pengolahan data yang dilakukan pada PT. Pertamina Patra Niaga sangat mengandalkan sekali kinerja jaringan LAN, diantaranya untuk membantu mengolah data tentang perminyakan. Pada PT. Pertamina Patra Niaga juga menggunakan wireles acces point untuk membantu efisiensi pekerjaan pegawai dan karyawan dalam mengantisipasi apabila terjadi trouble pada salah satu perangkat. Pada penelitian ini penulis meneliti permasalahan pada jaringan berjalan dan melakukan pemecahan permasalahan dengan menggunakan security with mac address.

Keyword: Jaringan LAN, *Wireles Access Point*, Mac Address, *security*.

1. PENDAHULUAN

Jaringan *Local Area Network* (LAN) adalah jaringan lokal yang dibuat pada area terbatas, misalkan dalam satu gedung atau dalam satu ruangan [1]. Jaringan LAN bisa digunakan didalam rumah, perkantoran, perindustrian, universitas atau akademik, rumah sakit dan lain-lain. Pada PT. Pertamina Patra Niaga telah berjalan suatu jaringan LAN, oleh karena itu pengolahan data yang dilakukan pada PT. Pertamina Patra Niaga sangat mengandalkan sekali kinerja jaringan LAN, diantaranya untuk membantu mengolah data tentang perminyakan.

Keamanan jaringan yaitu proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah atau penggunaan secara ilegal dari komputer dan jaringan [2]. *Wifi Protected Access2* (WPA2) adalah protokol keamanan baru yang dirancang untuk memperbaiki beberapa kerentanan keamanan hadir dalam WPA asli [3]. Keamanan jaringan pada kantor PT. Pertamina Patra Niaga menggunakan keamanan yang masih kurang, dikarenakan masih menggunakan keamanan model *Wifi Protected Access2* (WPA2) pada jaringan *access point*, sedangkan yang dimaksud dengan *Wireless Access Point* adalah suatu piranti yang memungkinkan piranti nirkabel untuk terhubung ke dalam jaringan dengan menggunakan *WI-FI*, *Bluetooth* atau standar lain [4]. Dengan mengandalkan sistem keamanan seperti ini, maka 1 *password* dapat digunakan oleh banyak *user*. Hal ini pula dapat menyebabkan *user* yang tidak berhak akses kedalam jaringan PT. Pertamina Patra Niaga masih dapat melakukan akses jaringan. Untuk membatasi jumlah *user* yang dapat terkoneksi, penulis menyarankan untuk membuat jaringan usulan dengan menggunakan *Security MAC-address With Cisco* sebagai batasan jumlah *client* yang dapat melakukan akses. Jadi, hanya *client* yang telah didaftarkan MAC-addressnya saja yang dapat terkoneksi. *MAC (Mac Access Control) address* adalah alamat sebuah hardware atau alamat fisik yang secara unik mengidentifikasi setiap komputer atau alat yang terhubung dalam jaringan, *MAC address* juga sering disebut *physical/hardware address* [5].

2. METODE PENELITIAN

Untuk memperoleh data yang dibutuhkan, penulis menggunakan metode penelitian sebagai berikut:

1. Metode Observasi

Observasi adalah studi yang disengaja dan sistematis tentang fenomena sosial dan gejala-gejala psikis dengan jalan pengamatan dan pencatatan. Penulis melakukan pengamatan secara langsung terhadap

kegiatan yang berhubungan dengan masalah yang diambil pada kantor PT. Pertamina Patra Niaga secara nyata.

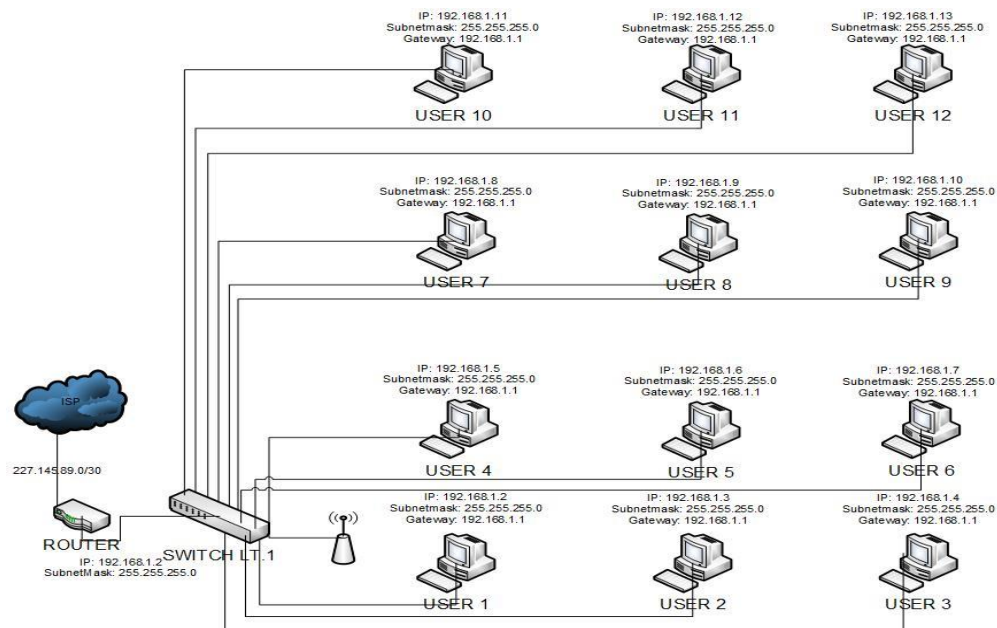
2. Metode Studi Pustaka

Studi Kepustakaan merupakan suatu teknik pengumpulan data dengan menghimpun dan menganalisis dokumen-dokumen, baik dokumen tertulis, gambar maupun elektronik. Studi pustaka merupakan metode yang dilakukan penulis setelah mendapatkan data dari observasi dan wawancara dengan cara mempelajari, mengkaji, dan membaca dari buku dan artikel mengenai jaringan komputer.

3. Wawancara

Wawancara adalah suatu percakapan yang diarahkan pada suatu masalah tertentu atau proses tanya jawab lisan dimana dua orang atau lebih berhadap-hadapan secara fisik. Teknik pengumpulan data yang dilakukan melalui wawancara secara langsung dengan bapak Mehnuari Wahyu Hidayat mengenai masalah yang ada pada jaringan komputer pada kantor PT. Pertamina Patra Niaga.

Skema jaringan yang digunakan pada PT. Pertamina Patra Niaga ialah sebagai berikut:



Gambar 1. Skema Jaringan PT. Pertamina Patra Niaga

PT. Pertamina Patra Niaga memiliki *desain* konfigurasi jaringan yang cukup kompleks. Konfigurasi tersebut dimulai dari *desain* secara fisik dalam artian *layout* perangkat jaringan dan kabel sebagai media penghubung hingga pada tahapan serta konfigurasi dari tiap perangkat tersebut. *Infrastruktur* jaringan LAN yang diterapkan pada PT. Pertamina Patra Niaga merupakan suatu bentuk jaringan LAN yang terintegrasi dan terkoneksi dengan jaringan internet melalui penyedia layanan internetspeedy.

Penyedia layanan internetspeedy mengirimkan layanan internet-nya melalui transmisi kabel telepon yang kemudian diterima oleh PT. Pertamina Patra Niaga modem. Kemudian menuju *server router* lalu di-*sharing* ke seluruh komputer *client* yang terdapat di PT. Pertamina Patra Niaga dan menerima paket data tersebut menggunakan switch yang langsung terhubung kepada *server* dan *client* dengan menggunakan transmisi kabel UTP yang disambung dengan sistem *straight*. Sehingga seluruh PC yang terdapat di PT. Pertamina Patra Niaga menerima paket data internet yang berasal dari speedy.

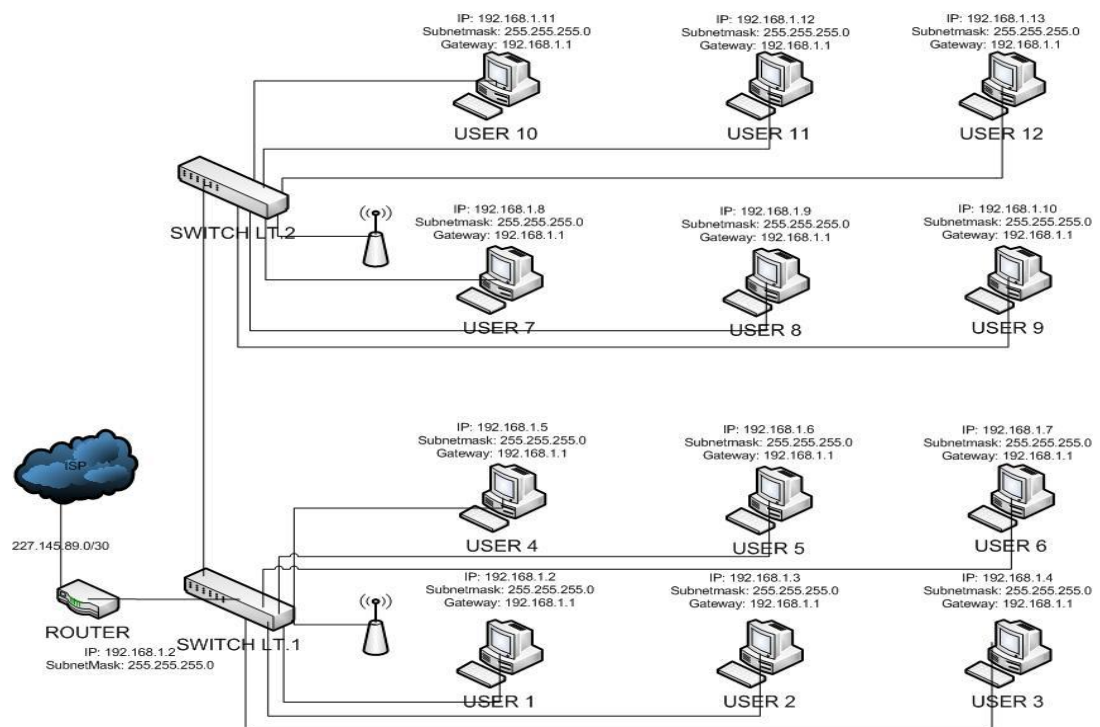
Tabel 1. Spesifikasi pembagian IP

Perangkat	Interface	Tujuan (Ether)	IP Address	Gateway
ISP	-	Router	227.145.89.0/30	-
Router	Ether 1	ISP	227.145.89.0/30	227.145.89.0
	Ether 2	Switch (1)	192.168.1.1/24	-
Switch	Ether 1	Router (2)	-	-
Lantai. 1				
User 1	NIC	Switch (2)	192.168.1.2	192.168.1.1
User 2	NIC	Switch (3)	192.168.1.3	

User 3	NIC	Switch (4)	192.168.1.4	
User 4	NIC	Switch (5)	192.168.1.5	
User 5	NIC	Switch (6)	192.168.1.6	
User 6	NIC	Switch (7)	192.168.1.7	
Access Point	NIC	Switch (24)	192.168.1.20- 192.168.1.50	
Lantai. 2				
User 7	NIC	Switch (8)	192.168.1.8	192.168.1.1
User 8	NIC	Switch (9)	192.168.1.9	
User 9	NIC	Switch (10)	192.168.1.9	
User 10	NIC	Switch (11)	192.168.1.10	
User 11	NIC	Switch (12)	192.168.1.11	
User 12	NIC	Switch (13)	192.168.1.12	

3. HASIL DAN ANALISA

3.1. Skema Usulan



Gambar 2. Skema Jaringan Usulan

Pada jaringan usulan penulis mengusulkan pada PT. Pertamina Patra Niaga melakukan penambahan 1 buah *switch* pada lantai 2, dengan tujuan supaya lebih mudah dalam melakukan *maintenance* jika terjadi permasalahan dan penambahan ataupun pengurangan jumlah *user*. Serta menggunakan 2 buah *Access Point* untuk *client* yang ingin melakukan akses kedalam jaringan pada Lantai 1 dan Lantai 2.

3.2. Konfigurasi Usulan

Tabel 2. Konfigurasi Usulan

Syntax	Pengertian
Switch>enable	Untuk mengaktifkan <i>device</i>
Switch#conf t	Untuk melakukan konfigurasi
Switch(config-if)#ip address 192.168.1.1 255.255.255.0	Untuk memberikan alamat IP pada sebuah <i>interface</i>
Switch port mode access	Untuk mengoperasikan pada konfigurasi <i>port</i>
Switch port security	Untuk mengamankan konfigurasi pada <i>port</i>
Switch port security max	Untuk menentukan batas maksimum
Switch port security mac address sticky	Untuk mencatat keamanan pada mac-address
Switch port security violation protect	Untuk memproteksi client yang masuk pada jaringan tersebut
Router>enable	Untuk mengaktifkan <i>device</i>
Router#conf t	Untuk melakukan konfigurasi
Router(config)#interface fa0/0	Untuk melakukan konfigurasi pada <i>interface</i> fa0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0	Untuk memberikan alamat IP pada sebuah <i>interface</i>
Router(config-if)#no shut down	Untuk mematikan konfigurasi
Router(config-if)#ip dhcp exclude- address	Untuk membatasi ip address pada konfigurasi ip address

1. Konfigurasi *Router*

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shut
```

Konfigurasi ini digunakan untuk memberikan alamat IP Address terhadap interface Fa0/0 pada router. Selanjutnya penulis menambahkan fitur *DHCP* Server terhadap interface fa0/0 yang nantinya akan digunakan sebagai gateway terhadap *user* Laptop. Berikut konfigurasi *DHCP* Server pada router cisco:

```
ip dhcp excluded-address 192.168.1.1 192.168.1.20
ip dhcp excluded-address 192.168.1.30 192.168.1.50
!
ip dhcp pool dhcp-ta
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
```

2. Konfigurasi *Security MAC* Address Lantai 1

```
interface FastEthernet0/2
switchport mode access
switchport port-security
switchport port-security maximum 4
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address 0001.C7C4.8D6C
switchport port-security mac-address 0001.C955.219C
switchport port-security mac-address 0050.0F27.EBB8
```

Konfigurasi ini digunakan untuk mendaftarkan Mac Address mana saja yang akan memiliki akses kedalam jaringan pada PT. PERTAMINA PATRA NIAGA.

3. Konfigurasi *Security MAC* Address Lantai 2

```
interface FastEthernet0/2
switchport mode access
switchport port-security
switchport port-security maximum 4
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address 0002.4A5B.E938
switchport port-security mac-address 0002.4AA5.560D
switchport port-security mac-address 0090.21CD.719C
```

4. Hasil konfigurasi *Security* MAC Address

```
Switch#sh mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0000.0c2a.ed01   DYNAMIC   Fa0/9
1       0001.c7c4.8d6c   STATIC    Fa0/2
1       0001.c955.219c   STATIC    Fa0/2
1       0007.ec46.5101   DYNAMIC   Fa0/1
1       0050.0f27.ebb8   STATIC    Fa0/2
Switch#
```

```
Switch#sh mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0002.1615.1309   DYNAMIC   Fa0/1
1       0002.4a5b.e938   STATIC    Fa0/2
1       0002.4aa5.560d   STATIC    Fa0/2
1       0090.21cd.719c   STATIC    Fa0/2
Switch#
```

Type mac address yang digunakan pada PT. Pertamina Patra Niaga yang penulis gunakan adalah *type Static* dan *Dynamic*. Mac address yang *type static* merupakan mac address yang dikonfigurasi, sedangkan mac address dynamic merupakan MAC yang secara pintar dipelajari oleh *switch*. Implementasi *port security* di *switch*, dapat mengkonfigurasi MAC mana saja yang dibolehkan terhubung ke *switch port* tertentu (ini disebut MAC Static), dan ketika sebuah *frame* memasuki *port* tertentu, *port* tersebut akan menyimpan MAC Address sumber fram maka ini merupakan dynamic MAC Address.

Penggunaan perangkat *switch* yang ada dilantai 1 dan lantai 2 pada PT. Pertamina Patra Niaga akan memberikan dampak terhadap peningkatan *performance* dan *network security* dari jaringan yang ada di PT. Pertamina Patra Niaga tersebut. Agar pengamanan jaringan lebih maksimal oleh perangkat *switch* maka dapat dilakukan dengan mengkonfigurasi *port* masing-masing *switch* dengan *port security* sehingga dapat diberikan batasan mac address dari komputer tertentu, dengan kata lain hanya yang terdaftar saja yang bisa terkoneksi pada *port* tersebut. Jika terjadi percobaan koneksi komputer yang tidak terdaftar pada *port* tersebut maka *port* dapat langsung disabled secara otomatis. Dengan adanya kemampuan *switch* yang maksimal ini merupakan salah satu peningkatan network security pada jaringan PT. Pertamina Patra Niaga.

4. KESIMPULAN

Pada jaringan wireless yang digunakan di PT. Pertamina Patra Niaga hanya menggunakan keamanan WPA2/WEP, sehingga masih banyak user yang tidak berhak akses dapat melakukan akses kedalam jaringan komputer. Untuk meminimalisir terjadinya kelemahan pada keamanan wireless, penulis mencoba menerapkan keamanan jaringan pada PT. Pertamina Patra Niaga menggunakan security with mac-address untuk meminimalisir user-user yang tidak diizinkan melakukan akses kedalam jaringan komputer.

ACKNOWLEDGEMENTS

Paper ini dihasilkan dari penelitian tugas akhir mahasiswa.

DAFTAR PUSTAKA

- [1] Sofana, Iwan, *Membangun Jaringan Komputer (Mudah membuat Jaringan Komputer Wire&Wireless untuk Pengguna Windows dan Linux) +DVD*. Bandung: Informatika, 2013.
- [2] Sukmaaji, Anjik dan Rianto, *Jaringan Komputer: Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan*. Yogyakarta: Andi, 2008.
- [3] Rajab, Muis, *Analisa Dan Perancangan Wireless LAN Security Menggunakan WPA2-Radius*, Jurnal Skripsi Fakultas Sains Dan Teknologi Universitas UIN Syarif Hidayatullah, 2010.
- [4] Waloeya Yohan Jati, *Computer Networking*. Yogyakarta: Andi Publisher, 2012.
- [5] Enterprise Jubilee, *100 Tip & Trik WiFi*. Jakarta: PT.Elex Media Komputindo, 2009.
- [6] Baihaqi, dkk. Implementasi Sistem Keamanan WPA 2-PSK Pada Jaringan Wafi. *Serambi Engineering*, Vol III : 248-254, Jan 2018.
- [7] Ariyadi, Tamsir. *Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN)*. Jusikom, Vol 2 : 28-36, Jun 2017.
- [8] Y, Peisong and Guangxue Yue. Security Research on WEP of WLAN. *Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10) Jingtangshan, P. R. China, 2-4, April. 2010, pp. 039-042*.
- [9] Park, S.Joon and Derrick Dicoi. *Wlan Security : Current and Future*. IEEE Internet Computing. 1089-7801/03/\$17.00©2003 IEEE. September-Oktober 2003.