*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023*
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680*
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Website : jurnal.ummu.ac.id/index.php/J-TIFA

**J-TIFA**

( Jurnal Teknologi Informatika )

|Teknologi Informasi | Jaringan Komputer | Data Mining |

# Analisis Dan Implmentasi Keamanan Jaringan Menggunakan Metode DHCP Snooping dan Swirch Port Security

Nurul Qamar Buamona[a], *Mustamin Hamid[b], Erwin Gunawan[c]
[abcd] *Program Studi Teknik Informatika, Universitas Muhammadiyah Maluku Utara,,Indonesia*
*Email: nurqamar.buamona10@gmail.com, hamidmustamin@gmail.com[b], , ewyn@outlook.com[c],*

**Abstrak**

Akses jaringan Internet sangat dibutuhkan oleh setiap kalangan bahkan sudah menjadi kebutuhan pokok bagi penggunanya dalam memperoleh informasi. Semakin banyaknya pengguna internet menyebabkan keamanan jaringan sangat dibutuhkan terutama jaringan internet pada instansi besar. Dengan tersebarnya jaringan internet tersebut maka sangat berpotensi akan adanya DHCP server palsu, hal ini bisa jadi menyebabkan client mendapatkan IP address bukan dari DHCP yang sebenarnya melainkan dari DHCP Server palsu tersebut dan juga dengan penggunaan Switch yang tersebar menyebabkan switch bisa di akses oleh siapa saja yang memungkinkan penyalahgunaan port switch oleh orang – orang yang tidak berkepentingan. Karena metode untuk mencegah pelanggaran keamanan jaringan disebabkan adanya server lain yang tidak dipercaya dan untuk mencegah akses dari perangkat tidak dikenal yang ingin terhubung ke jaringan yang dapat mengakibatkan komputer client tidak terhubung pada sebuah jaringan yang semestinya jadi metode keamanan jaringan perlu ditingkatkan lagi yaitu dengan menggunakan metode DHCP Snooping client hanya akan mendapatkan Ip address dari DHCP server yang dipercaya dan metode Switch Port Security hanya mengijinkan perangkat yang Mac addressnya sudah terdaftar saja yang bisa terhubung ke Switch.

**Kata kunci :** Keamanan Jaringan, DHCP Snooping, Switch Port Security

**Abstract**

*Internet network access is needed by every group and has even become a basic requirement for its users in obtaining information. The increasing number of internet users causes network security to be needed, especially internet networks in large agencies. With the spread of the internet network, it is very likely that there will be a fake DHCP server, this could cause the client to get an IP address not from the real DHCP, but from the fake DHCP Server and also with the use of scattered switches, so that the switch can be accessed by anyone who allows it. misuse of switch ports by unauthorized persons. Therefore, network security techniques can be implemented to prevent the presence of other servers that are not trusted and to prevent access from unknown devices that are connected to the network which can result in client computers not being connected to a network. what should be a network security method needs to be improved again, namely by using the DHCP Snooping method the client will only get the ip address from a trusted DHCP server and the Switch Port Security method only allows devices with registered Mac addresses to be able to connect to the Switch.*

*Keywords: Network Security, DHCP Snooping, Switch Port Security*

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online ( 30 Maret 2023)

*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023* ISSN: 2654-2617 (Cetak)
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680* ISSN: 2654-2633(Online)

## 1. Pendahuluan

Akses jaringan Internet sangat dibutuhkan oleh setiap kalangan bahkan sudah menjadi kebutuhan pokok bagi penggunanya dalam memperoleh informasi kapanpun dan dimanapun selama terhubung dengan internet.

Semakin banyaknya pengguna internet menyebabkan keamanan jaringan sangat dibutuhkan terutama jaringan internet pada instansi besar seperti Universitas Muhammadiyah Maluku Utara yang selalu diakses oleh dosen maupun mahasiswa baik dalam pembelajaran online, akses system akademik dan lain sebagainya, topologi jaringan internet di Universitas Muhammadiyah Maluku Utara tidak hanya terpusat di Kampus A saja tetapi tersebar di Kampus B, Kampus C dan juga Gedung Rektorat, seperti pada Kampus A ruang ICT memiliki Switch dan router sendiri Ruang BAK, Prodi Fikes, Prodi Teknik informatika dan juga prodi – prodi yang ada di Kampus B maupun Kampus C juga memiliki perangkat router tersendiri.

Hal tersebut menyebabkan penyebaran internet menjadi terdistribusi tidak hanya di lokasi – lokasi tertentu tetapi juga menyisahkan masalah pada sistem kontrolnya salah satunya tidak terkontrolnya penggunaan switch dan router yang sangat rentan adanya server lain yang tidak dipercaya adanya akses dari perangkat tidak dikenal yang ingin terhubung ke jaringan internet dan juga terjadi pencurian data atau kejahatan apapun yang mungkin dilakukan oleh pihak yang tidak bertanggung jawab.

Oleh karena itu teknik keamanan jaringan yang dapat dilakukan untuk mencegah adanya server lain yang tidak dipercaya dan untuk mencegah akses dari perangkat tidak dikenal yang ingin terhubung ke jaringan yang dapat mengakibatkan komputer client tidak terhubung pada sebuah jaringan yang semestinya jadi metode keamanan jaringan perlu ditingkatkan lagi dengan menggunakan metode DHCP Snooping dan Switch Port Security, metode DHCP Snooping dan Switch Port Security diharapkan dapat membantu mengatasi masalah keamanan jaringan.

## 2. DCHP Snooping & Switch Port Security

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang berdiri sendiri (standalone). Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi. Namun network security biasanya bertentangan dengan network access semakin mudah, maka network security semakin rawan dan bila network security semakin baik, network access semakin tidak nyaman. Suatu network didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses kesistem komputer, sementara security didesain untuk mengontrol akses. Penyediaan network security adalah sebagai aksi penyeimbang antara open access dengan security (Diansyah, 2015:1).

DHCP Snooping adalah salah satu metode keamanan pada jaringan komputer dan internet yang dapat diterapkan pada perangkat router yang digunakan untuk mencegah atau mem-filter adanya server lain yang tidak dipercaya dalam memberikan akses jaringan kepada pengguna atau komputer client (Miftah, 2018)

Komputer yang terhubung dalam jaringan akan mendapatkan alamat ip yang diberikan dari server DHCP sehingga komputer dapat berkomunikasi. DHCP snooping adalah fitur keamanan yang berfungsi seperti firewall di mana komputer yang terhubung dengan server DHCP akan mendapatkan alamat IP dari sumber yang terpercaya sedangkan sumber atau server DHCP yang tidak tepercaya tidak mendapat ijin untuk memberikan alamat IP yang dimiliki. DHCP snooping merupakan solusi yang tepat untuk mengatasi masalah keamanan jaringan yang lebih baik (Ariyadi, 2017).

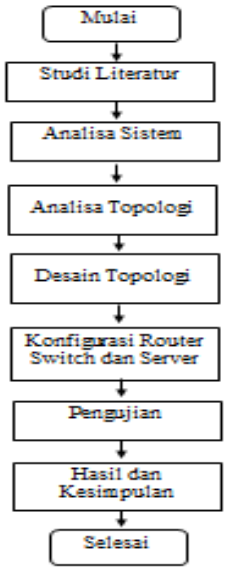
## 3. Metodologi Penelitian

Penelitian ini dilakukan secara teratur dan sistematis dari satu tahap ke tahap selanjutnya. Dalam alur proses penelitian ini yang pertama melakukan *Studi Literatur* Studi Literatur yaitu pengumpulan referensi – referensi sebagai bahan tinjauan Pustaka dan pembelajaran yang dapat di temukan didalam

Riwayat Artikel: Menerima(10 Januari 2023), Revisi (18 Februari 2023), Diterima (8 Maret 2023), Online ( 30 Maret 2023)

*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023*
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680*
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

jurnal – jurnal yang bersangkutan dengan Metode yang akan digunakan dalam penelitian



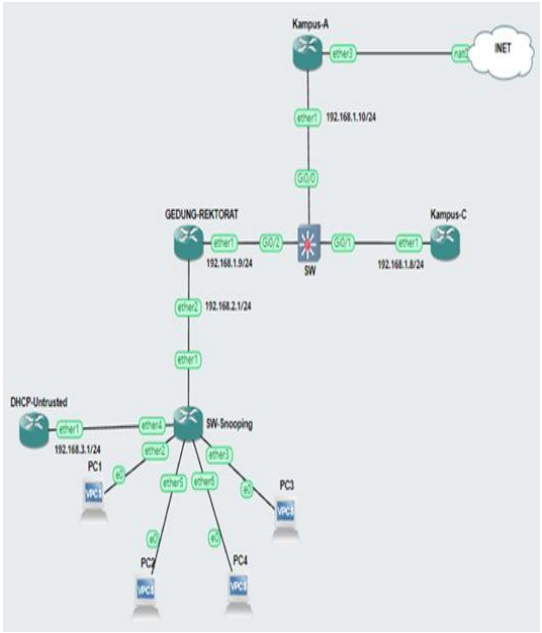

Gambar 1. Alur Penelitian

*Analisa Sistem* Sistem yang sedang berjalan di jaringan Internet Universitas Muhammadiyah Maluku Utara penyebaran internet menjadi terdistribusi tidak hanya di lokasi – lokasi tertentu tetapi juga menyisahkan masalah pada sistem kontrolnya salah satunya tidak terkontrolnya penggunaan switch dan router. *Analisa Topologi* Tidak terkontrolnya penggunaan switch dan router yang sangat rentan adanya server lain yang tidak dipercaya adanya akses dari perangkat tidak dikenal yang ingin terhubung ke jaringan internet. *Desain Topologi* Didalam topologi jaringan yang dibuat dengan simulasi menggunakan softwer GNS3 2.2.36 terdapat 2 buah Switch 4 buah Router dan 4 buah PC. Switch 1 menggunakan switch cisco yang akan di terapkan metode Switch Port Security dan switch 2 adalah switch biasa dihubungkan dengan Router 3 sebagai server DHCP trusted, router 4 sebagai server DHCP untrusted dan empat buah PC sebagai DHCP client. *Konfigurasi Router Switch dan Server* Yang dilakukan dalam konfigurasi yaitu memasang alamat IP pada masing – masing perangkat agar jaringan bisa saling terkoneksi dan bisa mengenal IP satu sama lain. *Pengujian* Pengujian dilakukan dengan pemasangan DHCP server palsu dan juga server lain yang tidak dipercaya yang ingin terhubung ke jaringan internet. *Hasil dan Kesimpulan* Dari alur penelitian di atas dapat di simpulkan Dengan menggunakan dua metode keamanan jaringan tersebut, penelitian ini diharapkan dapat meningkatkan keamanan jaringan internet kedepannya pada Universitas Muhammadiyah Maluku Utara dan mencegah penyalahgunaan jaringan tersebut oleh pihak yang tidak bertanggung jawab.

## 4. Analisis dan Perancangan Sistem

Objek penelitian secara umum merupakan permasalahan yang dijadikan topic penulisan dalam rangka menyusun suatu laporan penelitian. Menurut Sugiyono (2017:41), objek penelitian adalah : Menerapkan metode DHCP Snooping dan metode Switch Port Security pada jaringan internet di Universitas Muhammadiyah Maluku Utara.

Untuk melakukan pengujian dan pengambilan data penulis membuat topologi jaringan Universitas Muhammadiyah Maluku Utara.



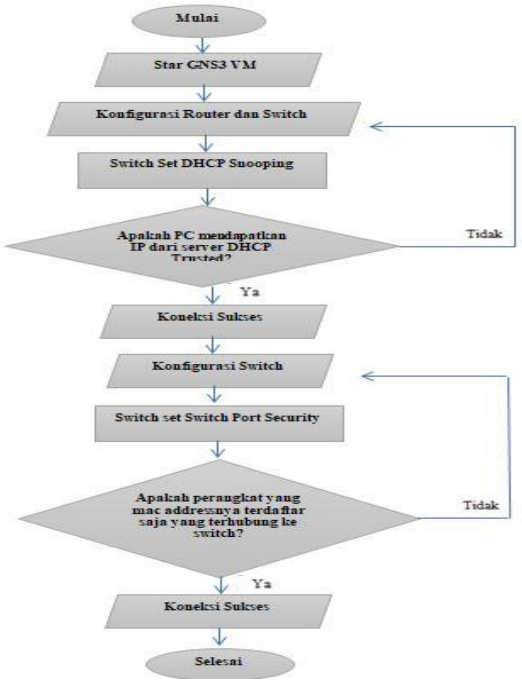

Gambar 2. Topologi Pengujian

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online ( 30 Maret 2023)

*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023*
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680*
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Topologi jaringan pada gambar 1 di atas akan disimulasikan menggunakan software GNS3 2.2.36 menggunakan dua metode yang pertama DHCP Snooping yang akan di terapkan pada Switch Snooping dengan memasang sebuah router sebagai Server DHCP Untrasted, metode yang kedua akan di terapkan pada Switch Cicko agar perangkan yang mac addressnya terdaftar saja yang bisa terhubung ke switch.

Selanjutnyan Skenario pengambilan data harus dilakukan untuk meminimalisasi adanya hambatan. Pengujian keamanan jaringan menggunakan metode DHCP Snooping dan metode Switch Port Security dapat menggunakan diagram alir flowchart sebagai berikut




Gambar 3. Skenario Pengambilan Data

Kemudian dilakukan pada skenario pengambilan data ini yaitu menghidupkan GNS3 VM kemudian melakukan konfigurasi pada router dan switch Lakukan set DHCP Snooping agar PC Client hanya mendapatkan IP dari DHCP Server Trusted. Melakukan pengecekan pada PC client apakah mendapatkan IP Address dari DHCP Server Trusted?, setelah menerapkan metode DHCP Snooping PC Client hanya mendapatkan IP dari server DHCP Trusted.

Selanjutnya lakukan konfigurasi pada switch Lakukan set Switch Port Security agar perangkat yang mac addressnya sudah terdaftar saja yang boleh terhubung ke switch dengan Melakukan Uji Coba apakah perangat yang mac addressnya belum terdaftar bisa terhubung ke switch?, ternyata hanya perangkat yang mac addressnya sudah terdaftar saja yang bisa terhubung ke switch.

## 5. Hasil dan Pembahasan

### *5.1 Konfigurasi pada Router*

Pada tahap ini akan dilakukan konfigurasi pada masing – masing perangkat router agar dapat terhubung atau bisa saling melakukan ping satu dengan yang lain.

a. Konfigurasi Router Gedung Rektorat sebagai Server DHCP Trusted

```
[admin@RouterOS] > system identity set
name=GEDUNG-REKTORAT
[admin@GEDUNG-REKTORAT] > ip
dhcp-client add interface= ether1
[admin@GEDUNG-REKTORAT] > ip
firewall nat add chain =srcnat out-interface=
ether1-Ke-SW action= masquerade
[admin@GEDUNG-REKTORAT] > ip
address  add address=192.168.2.1/24
interface=ether2-ke-SW-Snooping
[admin@GEDUNG-REKTORAT] > ip
dhcp-server setup
```

b. Konfigurasi Router sebagai Server DHCP Untrusted

```
[admin@RouterOS] > system identity
set name=DHCP-UNTRUSTED
[admin@DHCP-UNTRUSTED] > ip
address  add address=192.168.3.1/24
interface=ether1-ke-SW-Snooping
[admin@Kampus-A] > ip dhcp-server
setup
```

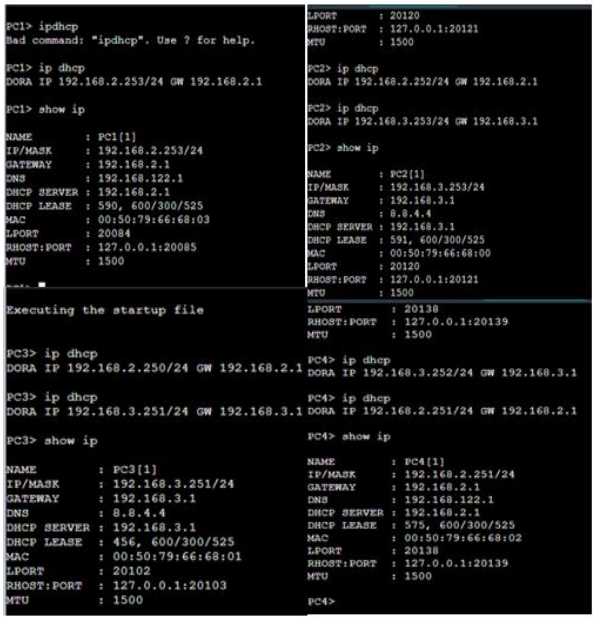
Riwayat Artikel: Menerima(10 Januari 2023), Revisi (18 Februari 2023), Diterima (8 Maret 2023), Online ( 30 Maret 2023)

*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023*
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680*
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Setelah melakukan setting pada seluruh perangkat router dan perangkat sudah bisa saling terhubung dengan tanpa DHCP Snooping maka

Tabel.1 IP Adrdress tanpa DHSCP Snooping

| Devic | IP Address | Subnet mask | Gateway | DNS |
|---|---|---|---|---|
| Trusted | 192.168.2.1 | 255.255.255.0 | | 192.168.122.1 |
| Untrsted | 192.168.3.1 | 255.255.255.0 | | 8.8.4.4 |
| PC1 | 192.168.2.253 | 255.255.255.0 | 192.168.2.1 | 192.168.122.1 |
| PC2 | 192.168.3.253 | 255.255.255.0 | 192.168.3.1 | 8.8.4.4 |
| PC3 | 192.168.3.251 | 255.255.255.0 | 192.168.3.1 | 8.8.4.4 |
| PC4 | 192.168.2.251 | 255.255.255.0 | 192.168.2.1 | 192.168.122.1 |




Gambar 4. Pengujuan PC dengan DHCP Server Untrudted

Hasil alamat IP pada PC1, PC2, PC3, dan PC4 yang terhubung pada jaringan memiliki IP Address yang berbeda, sehingga menyebabkan dua buah PC dapat terhubung dengan server, dan dua buah PC lainnya tidak dapat terhubung disebabkan adanya Server DHCP Untrusted atau tidak di percaya menyewakan alamat IP kepada client sehingga client tidak terhubung ke jarigan yang semestinya.

*5.1 Konfigurasi pada Switch*

Pada tahap ini akan di lakukan konfigurasi pada switch, switch yang pertama akan dilakukan konfigurasi menggunakan metode DHCP Snooping sedangkan switch cisco akan di terapkan metode Switch Port Security.

*a. Konfigurasi Switch Pertama dengan Metode DHCP Snooping*

- Yang pertama mengecek interface bridge port pada Switch
  [admin@SW-Snooping] > interface bridge port print

- Selanjutnya mensetting interface ether1 sebagai port yang di percaya.
  [admin@SW-Snooping] > interface bridge port set numbers=0 trusted=yes
  [admin@SW-Snooping] >

- Langkah terakhir yang dilakukan mensetting DHCP Snooping
  [admin@SW-Snooping] > interface bridge port set numbers=0 dhcp-snooping=yes add-dhcp-option82
  [admin@SW-Snooping] >

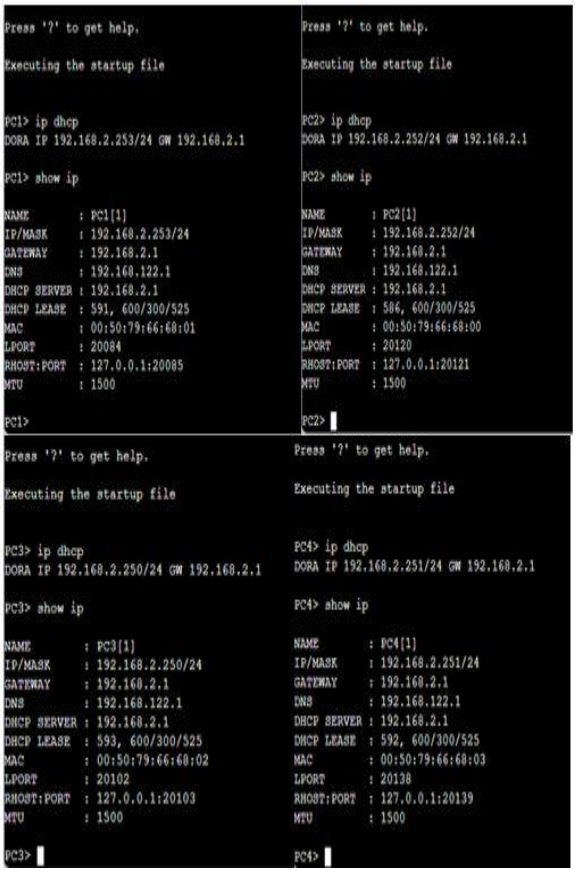
Dengan mensetting DHCP Snooping pada Switch maka PC1, PC2,PC3 dan PC4 telah mendapatkan alamat IP dari server trusted atau yang di percaya.

Tabel.2 IP Address tanpa DHSCP Snooping

| Devic | IP Address | Subnet mask | Gateway | DNS |
|---|---|---|---|---|
| Trusted | 192.168.2.1 | 255.255.255.0 | | 192.168.122.1 |
| Untrsted | 192.168.3.1 | 255.255.255.0 | | 8.8.4.4 |
| PC1 | 192.168.2.253 | 255.255.255.0 | 192.168.2.1 | 192.168.122.1 |
| PC2 | 192.168.2.252 | 255.255.255.0 | 192.168.2.1 | 192.168.122.1 |
| PC3 | 192.168.2.250 | 255.255.255.0 | 192.168.2.1 | 192.168.122.1 |
| PC4 | 192.168.2.251 | 255.255.255.0 | 192.168.2.1 | 192.168.122.1 |

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online ( 30 Maret 2023)

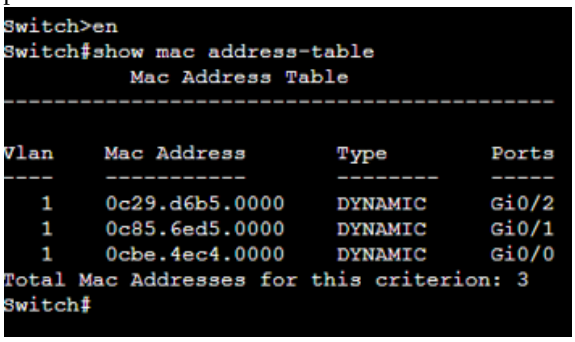
*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023* ISSN: 2654-2617 (Cetak)
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680* ISSN: 2654-2633(Online)



Gambar 5. Pengujuan PC dengan DHCP Snooping

b. Konfigurasi Switch Cisco dengan Metode Switch Port Security

Berikut adalah mac address yang telah terdaftar pada switch.



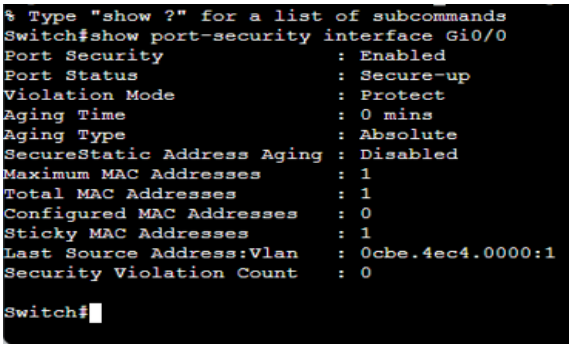
Gambar 6. Mac Address Table Print

Mac Address pada tabel di atas terdaftar secara otomatis pada switch yang disebut dengan port security sticky alias dinamik sehingga tidak perlu repot menginput mac address secara manual.

1. Konfigurasi Switch Gi0/0 dengan mode Violation Mode Protect

```
Switch(config)#interface Gi0/0
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)#switchport port-security
violation protect
```

Cara melihat mode protect yang telah di konfigurasi pada switch



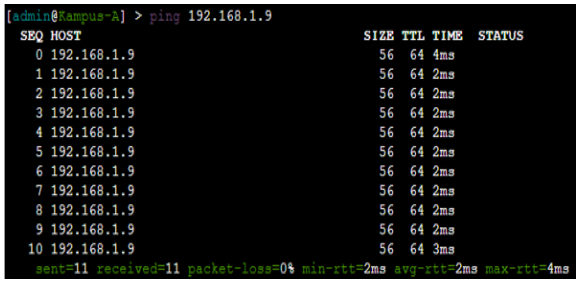
Gambar 7. Violation Mode Protect

Pengujian dengan ping dari router Kampus-A sebagai mac address yang telah terdaftar pada interface Gi0/0 ke GEDUNG-REKTORAT seperti pada gambar 8. Pengujian selanjutnya link Kampus-C dipindahkan ke interface Gi0/0 dengan violation mode protect seperti pada gambar 9.

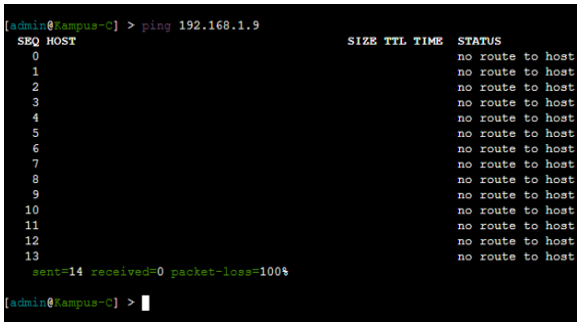
Hasil ping pada gambar di atas mode protect paket data yang dikirimkan oleh perangkat akan dibuang (dropped) oleh interface yang mac addressnya tidak terdaftar.

Riwayat Artikel: Menerima(10 Januari 2023), Revisi (18 Februari 2023), Diterima (8 Maret 2023), Online ( 30 Maret 2023)

*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023*
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680*
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)




Gambar 8. Ping Router Kampus A ke Gedung Rektorat



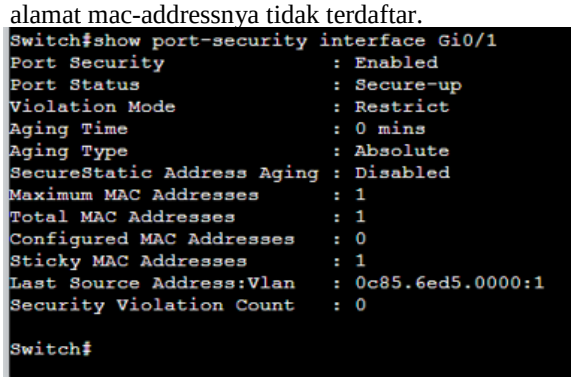

Gambar 9. Ping Setelah Link Kampus C dipidahkan ke Int Gi0/0

2. Konfigurasi Switch Gi0/1 dengan Violation Mode Restric

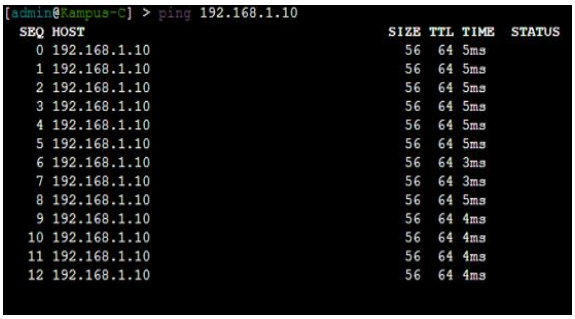
```
Switch(config)#interface Gi0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security
maximum 1
Switch(config-if)#switchport port-security mac
address sticky
Switch(config-if)#switchport port-security
violation restrict
```

Cara melihat mode restrict yang telah di konfigurasi pada switch (gambar 10). Kemudian Pengujian dengan ping dari router Kampus-C sebagai mac address yang telah terdaftar pada interface Gi0/1 ke Router Kampus-A telah sukses (gambar 11) Pengujian selanjutnya link GEDUNG-REKTORAT dipindahkan ke interface Gi0/1 dengan violation mode restrict (gambar 12).

Sehingga hasil ping pada gambar di atas mode restrict paket data yang dikirimkan oleh perangkat akan dibuang (dropped) sama seperti mode protect. Antarmuka, di sisi lain, akan melacak jumlah pelanggaran yang dilakukan oleh perangkat yang alamat mac-addressnya tidak terdaftar.




Gambar 10. Violation Mode Restrict




Gambar 11. Ping Router Kampus C ke Kampus A


*Gambar 12. Ping Setelah Link Gedung Rektorat dipidahkan ke Int Gi0/1*

3. Konfigurasi Switch Gi0/2 dengan Violation Mode shutdown

Cara melihat mode shutdown yang telah dikonfigurasi pada switch

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online ( 30 Maret 2023)

*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023*
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680*
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

```
Switch#show port-security interface Gi0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0c29.d6b5.0000:1
Security Violation Count   : 0

Switch#
```

Gambar 13. Violation Mode Shutdown

Pengujian dengan ping dari router GEDUNG-REKTORAT sebagai mac address yang telah terdaftar pada interface Gi0/2 ke Router Kampus-A telah sukses.

```
[admin@GEDUNG-REKTORAT] > ping 192.168.1.10
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.10                               56  64 6ms
    1 192.168.1.10                               56  64 5ms
    2 192.168.1.10                               56  64 5ms
    3 192.168.1.10                               56  64 5ms
    4 192.168.1.10                               56  64 3ms
    5 192.168.1.10                               56  64 5ms
    6 192.168.1.10                               56  64 3ms
    7 192.168.1.10                               56  64 3ms
    8 192.168.1.10                               56  64 4ms
    9 192.168.1.10                               56  64 4ms
   10 192.168.1.10                               56  64 4ms
   11 192.168.1.10                               56  64 4ms
   12 192.168.1.10                               56  64 5ms
    sent=13 received=13 packet-loss=0% min-rtt=3ms avg-rtt=4ms max-rtt=6ms

[admin@GEDUNG-REKTORAT] >
```

Gambar 14. Ping dari Gedung Rektorat ke Kampus A

Pengujian selanjutnya link Kampus-A dipindahkan ke interface Gi0/2 dengan violation mode shutdown.

```
[admin@Kampus-A] > ping 192.168.1.9
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.9                                               timeout
    1 192.168.1.9                                               timeout
    2 192.168.1.10                               84  64 968ms host unreachable
    3 192.168.1.9                                               timeout
    4 192.168.1.9                                               timeout
    5 192.168.1.10                               84  64 979ms host unreachable
    6 192.168.1.9                                               timeout
    7 192.168.1.9                                               timeout
    8 192.168.1.10                               84  64 978ms host unreachable
    9 192.168.1.9                                               timeout
   10 192.168.1.9                                               timeout
   11 192.168.1.10                               84  64 979ms host unreachable
    sent=12 received=0 packet-loss=100%

[admin@Kampus-A] >
```

Gambar 15. Ping Setelah Link Kampus A dipidahkan ke Int Gi0/2

Hasil ping pada gambar di atas adalah timeout mode shutdown port yang digunakan oleh perangkat yang tidak terdaftar dengan alamat mac-addressnya langsung dinonaktifkan oleh antarmuka yang menggunakan mode ini.

### *5.1 Analisis Perbandingan*

Pada tabel 3 adalah hasil analisis perbandingan sebelum dan sesudah menggunakan metode keamanan jaringan DHCP Snooping dan Switch Port Security. Pada tabel 3 metode DHCP Snooping di terapkan PC1 sampai dengan PC4 masih mendapatkan IP Address secara acak dari server DHCP trusted maupun untrusted dan sesudah metode DHCP Snooping diterapkan maka PC1 sampai dengan PC4 hanya mendapatkan IP Address dari server DHCP trusted atau server yang di percayai.

Tabel.3 Hasil Perbandingan DHCP Snoopong

| SEBELUM | | | | SESUDAH | | | |
|---|---|---|---|---|---|---|---|
| **Devic** | **IP Address** | **Gatway** | **DNS** | **Devic** | **IP Address** | **Gatway** | **DNS** |
| PC1 | 192.168.2.253 | 192.168.2.1 | 192.168.122.1 | PC2 | 192.168.2.253 | 192.168.2.1 | 192.168.122.1 |
| PC2 | 192.168.3.253 | 192.168.231 | 8,8.4.4 | PC2 | 192.168.2.252 | 192.168.2.1 | 192.168.122.1 |
| PC3 | 192.168.3.251 | 192.168.2.1 | 8.8.4.4 | PC3 | 192.168.2.250 | 192.168.2.1 | 192.168.122.1 |
| PC4 | 192.168.2.251 | 192.168.2.1 | 192.168.122.1 | PC4 | 192.168.2.251 | 192.168.2.1 | 192.168.122.1 |

Tabel.4 Hasil Perbandingan Switch Port Security

| SEBELUM | | | | SESUDAH | | | |
|---|---|---|---|---|---|---|---|
| **Perangkat** | **Interface** | **Ping** | **Status** | **Perangkat** | **Interface** | **Ping** | **Status** |
| Kampus A | Gi0/0 | 192.168.1.9 | Jalan | Kampus C | Gi0/0 | Protect | No Route Host |
| Kampus C | Gi0/1 | 192.168.1.10 | Jalan | Gedung Rektorat | Gi0/1 | Restrict | No Route Host |
| Gedung Rektorat | Gi0/2 | 192.168.1.10 | Jalan | Kampus A | Gi0/2 | Restrict | Time out |

Riwayat Artikel: Menerima(10 Januari 2023), Revisi (18 Februari 2023), Diterima (8 Maret 2023), Online ( 30 Maret 2023)

*Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023*
*DOI: https://doi.org/10.52046/j-tifa.v6i2.1680*
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Dari kedua uji coba pada tabel di atas hanya perangkat yang Mac addressnya sudah terdaftar saja yang bisa terhubung ke Switch seperti pada Router Kampus A mac addressnya telah terdaftar pada Switch interface Gi0/0, Kampus C pada interface Gi0/1 dan Gedung Rektorat pada interface Gi0/2 yaitu dengan hasil ping jalan

Selanjutnya dilakukan uji coba menggunakan Violation Mode yang sudah di konfigurasi pada setiap interface. Pertama memindahkan link kampus C ke interface Gi0/0 dengan violation mode protect hasil pingnya no route to host karena violation protect paket data yang dikirimkan oleh perangkat akan dibuang (dropped). Yang kedua memindahkan link Gedung Rektorat ke interface Gi0/1 dengan violation mode restrict hasil pingnya juga no route to host karena paket yang dikirim juga dibuang (drop) seperti pada mode protect. Yang ketiga link Kampus A dipindahkan ke interface Gi0/2 hasil ping time out dengan violation mode shutdown karena interface dengan mode ini seketika menonaktufkan port yang dipakai oleh perangkat yang mac addressnya tidak terdaftar pada Switch.

## 6. Kesimpulan dan Saran

Berdasarkan uji coba implementasi secara simulasi menggunakan software GNS3 maka dapat disimpulkan bahwa

1. Dengan menggunakan metode DHCP Snooping dapat mencegah adanya server lain atau DHCP sever palsu yang tidak di percaya yang menyebabkan client mendapatkan IP Address bukan dari DHCP server yang sebenarnya melainkan dari DHCP server palsu tersebut. Dengan adanya metode DHCP Snooping keamanan jaringan akan semakin meningkat dan client hanya akan mendapatkan alamat IP dari DHCP Server yang di percaya.
2. Meningkatkan keamanan jaringan menggunakan metode Switch Port Security sangat efektif karena semua perangkat jaringan yang ingin terhubung ke switch adalah perangkat yang mac addressnya sudah terdaftar, baik secara manual atau otomatis. Dengan menggunakan Violation mode protect, restrict, dan juga mode shutdown sehingga paket data yang dikirimkan dari perangkat yang belum terdaftar mac addressnya langsung di buang (drop) paket datanya, outputnya akan menghasilkan *no route to host* dan juga *time out.*

Penelitian Keamanan jaringan dengan metode DHCP Snooping dan Switch Port Security yang penulis buat diharapkan dapat di implementasikan secara nyata pada jaringan internet di Universitas Muhammadiyah Maluku Utara.

## Referensi

Artikel. (2020). [DHCP Security] – Pencegahan DHCP Rogue dengan DHCP Snooping (citraweb.com) (di akses pada tanggal 20 maret 2023).

Dantris sri, Junaidi Noh, Mustamin Hamid. (2020). Simulasi Protokol Autjentifikasi 802. 1x pada Jaringan Nirkabel di UMMU. JTIFA Vol 3 No 2 September 2020. Doi: https://doi.org/10.52046/j-tifa.v3i2.1044

Fikri, K. A dan Djuniadi. (2021). Keamanan Jaringan Menggunakan Switch Port Security. InfoTekJAr, Vol.5, No. 2, 303 – 307.

Guru Pendidikan. (2020). Topologi Jaringan. Topologi Jaringan : Pengertian, Macam, Kelebihan & Kekurangannya (seputarilmu.com) (diakses pada tanggal 12 Februari 2023).

Muttaqin., dkk. (2022). Teknologi Jaringan Kompuer. Yayasan Kita Menulis.

Miftah, Z. (2018). Simulasi Keamanan Jaringan Dengan Metode Dhcp Snooping Dan Vlan. Faktor Exacta, 11(2), 167.

Rahmani, M. A. C dan Swandhi Prabowo. (2020). Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping dan VLAN, JASIKA, Vol. 1, No. 1, April, 27 – 37.

Sutiman dan A. Gunawan. (2021). *Firewall Port Security Switch* untuk Keamanan Jaringan Komputer Menggunakan *Cisco Router* 1600s pada PT. Tirta Kencana Tata Warna Sukabumi, Computer and Network Tecnology, Vol. 1, No. 1, Juni, 13 – 22.

Sulicdio, Julias, Toibah Umi Kalsum dan Yode Arliando. (2022). Analisa Perbandingan Software Wireshark dan Windump dalam Monitoring Keamanan Jaringan. Media Computer Science, Vol. 1 No. 1, Januari, 1 – 6.

Sulaiman, O. K. (2016). Analisis Sistem Keamanan Jaringan dengan. Computer Engineering, System And Science, 1(1), 9–14.

Udrus Karina. Sahriar Hamza, Gamaria Mandar. (2021). Optimalisasi Bandwidth Menggunakan Traffic Shapping di Lab. Networking Universitas Muhammadiyah Maluku Utara. JTIFA Vol 4 No 1 Marer 2021. Doi; https://doi.org/10.52046/j-tifa.v4i1.1162

Yoga Ramadhan. (2017). Konfigurasi Port Security Cisco. (diaryconfig.com) (di akses pada tanggal 10 Januari 2023).

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online ( 30 Maret 2023)