COMPARISON OF PORT SECURITY SWITCH LAYER 2 MAC ADDRESS DYNAMIC WITH MAC ADDRESS STATIC STICKY

Firmansyah[1], Tommi Alfian Armawan Sandi[2], Sari Dewi[3], Eka Kusuma Pratama[4], Rachmawati Darma Astuti[5]
[1]Sistem Informasi, Universitas Nusa Mandiri, Jakarta
[2]Teknologi Komputer, Universitas Universitas Bina Sarana Informatika, Jakarta
[3]Sistem Informasi D3 PSDKU kota Pontianak, Universitas Bina Sarana Informatika, Jakarta
[4]Ilmu Komputer, Universitas Bina Sarana Informatika, Jakarta
[5]Teknologi Komputer, Universitas Universitas Bina Sarana Informatika, Jakarta
e-mail: [1] firmansyah.fmy@nusamandiri.ac.id, [2]tommi.taf@bsi.ac.id,
[3]sari.sre@bsi.ac.id,[4]eka.eem@bsi.ac.id,[5]rachmawati.rcd@bsi.ac.id

Received: 12, September, 2022 ***Revised: 18, September, 2022*** ***Accepted: 18, September, 2022***

ABSTRACT

Security and stability in a network service is a top priority for a network administrator. The slightest security vulnerability can make a very big threat in the stability of network services. The rise of cybercrime that intercepts access to a network service by performing ARP spoofing to imitate a client who has the right to access the network, with this happening it can be detrimental and disrupt network services. The application of MAC Address filtering to access network services is able to minimize the occurrence of cybercrime in the network. The filtering technique used is by registering the MAC address of each network service user who will connect to the network. This technique is able to recap the MAC Address on each device in the MAC Address table and is able to block access to clients whose MAC addresses are not registered. The test results obtained for the comparison of MAC Address filtering security using Dynamic with sticky MAC addresses are that the implementation of port security static sticky is considered better than the implementation of dynamic port security, where if there is a new client trying to access the network and the client's mac address is not registered then the client absolutely does not get access to network services.

Keywords: Cybercrime, Filtering, MAC Address, Port Security

1. INTRODUCTION

The development of information technology, especially in the world of computer networks, forces a network administrator to work more competently in their field. Ensuring stable and secure network services is a top priority in a network service (Firmansyah et al., 2019) . The choice of method in the application of computer network security is very vital (Firmansyah & Wahyudi, 2021) . Computer network security is vital for a network service, if there are weaknesses in network services, it can lead to instability of a service that is being used. In fact, the computer network security system in recent years has become a major focus in the world of computer networks, this is due to the rise of threats and attacks from the internet. Crime within a network is very difficult to detect, because cybercrime actors can remove traces of their location of attack (Anugrah & Rahmanto, 2018) .

Due to the exponential growth in network deployments, this field has become a prime target for attackers. Spoofing attacks are a very common type of attack on networks. This may sound simple, but it is a complex technique that involves impersonating and gaining access to restricted information. Some spoofing attacks complicate the scenario by launching other attackers using fake computers. Networks are usually unable to identify spoofing attacks because the attacking hackers can spoof the MAC addresses of their devices to impersonate other devices on the network resulting in advanced ARP spoofing thereby exposing network vulnerabilities (Anathi & Vijayakumar, 2020) .

The application of port security on layer 2 switches is expected to be able to ward off all cybercrime activities located at the location of computer network devices because crime in the world of computer networks is an interesting thing for a hacker by profession. For example, man-in-the-middle attacks intercept and corrupt data, which can lead to disruption of network communications and other serious consequences (Song & Ji, 2016) . By doing port security, the MAC address table will be activated on the switch port interface by synchronizing the ARP (Address Resolution Protocol), so the port cannot forward if the MAC address is not recognized (Sulaiman, 2016) . The application of port security aims to avoid intruders who will steal data on computer networks (Dwtias Sari et al., 2017) (Subekti & Subandri, 2020) . Because the MAC Address is an address from the hardware, each NIC (Network Interface Card) has a unique address from one another (Subekti & Subandri, 2020) (Hardi et al., 2020) . MAC Filtering allows access only for the desired device (Grabovica et al., 2016) (Riska et al., 2018) .

In previous research, it was found that the application of port security was able to apply security to every client who wants to connect to the internet network must use a device that has registered the MAC address and is in accordance with user access rights and passwords (Firmansyah et al., 2021) . With the existence of port security, existing ports can be used to allow access to the network. Switch port security is a technique that will allow anyone who has the right to use network access through the available ports on the switch to secure the network (Zara et al., 2020) while in other studies, MAC Address Filtering results are a system that is able to prevent anonymous users from accessing the network. network, and allow users with registered MAC addresses to access the network (Bima Pramudya, 2021) .

2. THEORY

Based on previous research written by Oris Krianto Sulaiman with the title of network security system analysis using switch port security, sticky port security is very efficient to use because of its ability to dynamically analyze the mac-address to be registered (Sulaiman, 2016) . In research with the title wan network modeling with frame relay technology by utilizing switch port security as a network security system, it concludes that implementing a Switch Port on a device using Default / static port security settings is used for one port to be blocked, this security capability is quite minimal because static port security capability can only register one mac-address. Sticky port security is very efficient to use because of its ability to dynamically analyze the MAC address that will be registered (Zara et al., 2020) .

3. METHOD

In conducting research on Comparison of Port Security Switch Layer 2 MAC Address Dynamic with Static Sticky MAC Address, researchers used the help of Cisco packet tracer simulation software to create network simulations but did not change and reduce the original features (Trabelsi & Saleous, 2019) (Srikanth Reddy et al. , 2020) . In this study, researchers used 1 (one) device router which is used as a DHCP Server and gateway in the network and with 3 (three) computer devices used to test port security connectivity.

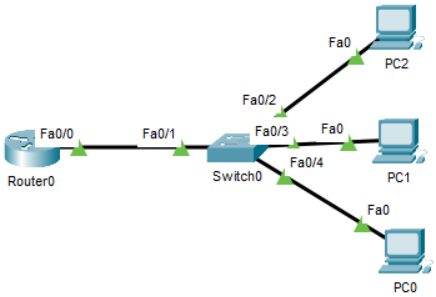

Figure 1. Network Schematic

Seen in Figure 1 is a network scheme that researchers use in the study of Comparison of Port Security Switch Layer 2 MAC Address Dynamic with MAC Address Static Sticky. The test is carried out to get the results of the comparison between the dynamic MAC Address port security and the static sticky MAC Address port security.

1. RESULTS AND DISCUSSION

1.1 Simulation Scenario

The test scenario for Comparison of Port Security Switch Layer 2 MAC Address Dynamic with Static Sticky MAC Address is done by adding one (1) new client to the running network but the client's mac address is not registered in the layer 2 switch mac-address table. get the results of the network security level both on the implementation of dynamic port security mac address and on the implementation of port security mac address with static sticky.

1.2 Dynamic Port Security Configuration

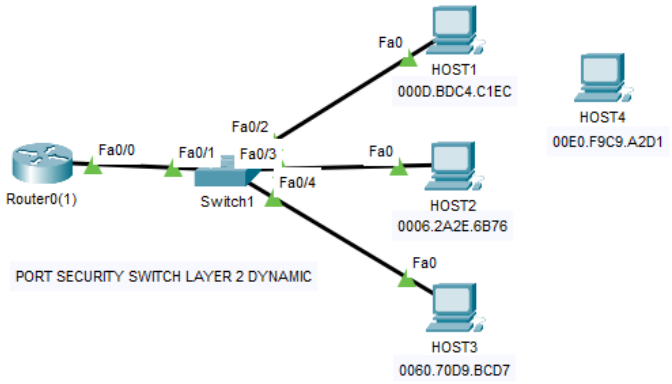

Figure 2. Network Schematic Port Security MAC Address Dynamic

To conduct research on Port Security Switch Layer 2 MAC Address Dynamic, there are several things that must be considered, such as the use of the interface in the switch that is connected to the client and the MAC Address used for each client. As shown in Figure 2 is the network scheme used in implementing the Port Security Switch. Layer 2 MAC Address Dynamic. There

are 3 (three) clients that are connected directly to the switch device HOST1 with MAC Address 000D.BDC4.C1EC, HOST2 with MAC Address 0006.2A2E.6B76 and HOST3 using 0060.70D9.BCD 7 while the MA Address 00E0.F9C9.A2D1 on HOST4 is not registered in the MAC-Address table which is used as a connectivity test.

Table 1. MAC Address Dynamic Port Security Specifications

Device	IP Address	Interface	MAC Address
Router	192.168.10.1	Fa0/0	000B.BE52.3987
HOST1	DHCP Client	Fa0/2	000D.BDC4.C1EC
HOST2	DHCP Client	Fa0/3	0006.2A2E.6B76
HOST3	DHCP Client	Fa0/4	0060.70D9.BCD7
HOST4			00E0.F9C9.A2D1

Described in Table 1, is a specification of IP Address, Interface and MAC address used in implementing Port Security Switch Layer 2 MAC Address Dynamic. The configuration used for implementation determines the interface used and activates access mode on the switch and provides port-security on all interfaces that will be used, such as:

```
!
FastEthernet0/1 . interfaces
switchport mode access
switchport port-security
!
FastEthernet0/2 . interfaces
switchport mode access
switchport port-security
!
FastEthernet0/3 . interfaces
switchport mode access
switchport port-security
!
FastEthernet0/4 . interfaces
switchport mode access
switchport port-security
!
```

After completing the configuration, use the "show port-security address" command to verify the MAC Address and interface used, shown in Figure 3. Figure 3 is the result of implementing the Port Security Switch Layer 2 MAC Address Dynamic, the results in the secure MAC address table will be filled with DynamicConfigured which contains the MAC Address and interface used.

```
Switch#sh port-security address
                              Secure Mac Address Table
------------------------------------------------------------------------
Vlan       Mac Address Type                          Ports

----       ----------- ----                          -----
1          000B.BE52.3987         DynamicConfigured      FastEthernet0/1
1          000D.BDC4.C1EC         DynamicConfigured      FastEthernet0/2
1          0006.2A2E.6B76         DynamicConfigured      FastEthernet0/3
1          0060.70D9.BCD7         DynamicConfigured      FastEthernet0/4
------------------------------------------------------------------------
```

Figure 3. Configuring Port Security MAC Address Dynamic

1.3 Configure Static Sticky Port Security

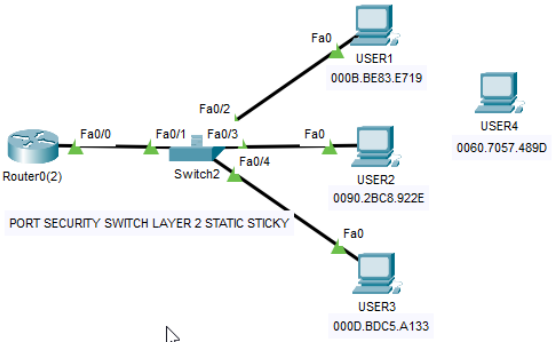

Figure 4. Network Schematic Port Security MAC Address Static Sticky

Meanwhile, to implement Port Security Switch Layer 2 MAC Address Static Sticky, the network scheme used is shown in Figure 4. Later, USER1 will be limited in access, that is, it can only access network services if it uses the fa0/2 interface on the switch port interface, USER2 can only use interfaces fa0/3 and USER3 can only use F0/4. It aims to restrict access to the port switch interface if there is a new client attempting access to network services. As well as the specifications for the IP Address, interface and MAC Address as shown in table 2.

Table 2. Specifications for Port Security MAC Address Static Sticky

Device	IP Address	Interface	MAC Address
Router	192.168.10.1	Fa0/0	000B.BE52.3987
USER1	DHCP Client	Fa0/2	000B.BE 83.E 719
USER2	DHCP Client	Fa0/3	0090.2BC8.922E
USER3	DHCP Client	Fa0/4	000D.BDC 5.A 133
USER4			0060.7057.489D

Referring to Figure 4 and table 3, the configuration used for implementing the Port Security Switch Layer 2 MAC Address Static Sticky is to determine the interface used, activate the access mode, activate the sticky mac-address, and activate the violation protect if a new client tries to access it. into the network so that it does not interfere with running network services and registers MAC addresses on all clients who will later have the right to access the running network, the configuration used is:

```
!
FastEthernet0/2 . interfaces
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address 000B.BE 83.E 719
!
FastEthernet0/3 . interfaces
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address 0090.2BC8.922E
```

```
!
FastEthernet0/4 . interfaces
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address 000D.BDC 5.A 133
!
```

There are different implementation methods between Dynamic MAC Address filtering and Static Sticky MAC Address filtering, if the Dynamic MAC Address does not register the MAC Address which will later have the right to access a network service while the implementation of Static Sticky MAC Address filtering must perform an order by registering the MAC The address that will have access rights to a network service using a predetermined interface.

```
Switch#sh port-security address
                                  Secure Mac Address Table
------------------------------------------------------------------------------
Vlan       Mac Address Type                                  Ports

----       ----------- ----                                  -----
1          000B.BE83.E719       SecureConfigured       FastEthernet0/2
1          0090.2BC8.922E       SecureConfigured       FastEthernet0/3
1          000D.BDC5.A133       SecureConfigured       FastEthernet0/4
------------------------------------------------------------------------------
```

Figure 5. Configuring Port Security MAC Address Static Sticky

Seen in Figure 5 is the result of the configuration of the Port Security Switch Layer 2 MAC Address Static Sticky. The results obtained are different between the implementation of Port Security Switch Layer 2 MAC Address Static Sticky with Port Security Switch Layer 2 MAC Address Dynamic. If in Port Security Dynamic the results obtained in the Secure MAC Address Table contain DynamicConfigured while in Port Security Static Sicky the results obtained are SecureConfigured between MAC Address and the interface used, which means that clients with MAC Address 000B.BE83.E719 can only access into network services if connected using the Fa0/2 interface and the client with MAC Address 0090.2BC8.922E will only be able to connect using the fa0/3 interface and the client with MAC Address 000D.BDC5.A133 can only use the fa0/4 interface on the switch device.

1.4 Port Security Dynamic Connectivity Test

To test the dynamic Port Security connectivity, we can refer to Figure 2, where there is one client with the name HOST4 that is not connected to the running network. The test is carried out by HOST4 experimenting access to the running network using the fa0/2 and fa0/10 interfaces on the switch.

Table 3. Port Security Dynamic Connectivity Test Results

Device	**MAC Address**	**Interface**	**Connectivity**	
			Before	**After**
HOST4	00E0.F9C9.A2D1	Fa0/2		OK
HOST4	00E0.F9C9.A2D1	Fa0/10		OK

Seen in Table 3 is the result of an experiment from the client side of HOST4 into the network. The first experiment HOST4 conducted a connectivity test using Interface Fa0/2 and the results

were able to connect to the network, the second experiment was carried out on HOST4 using the Fa0/10 interface and obtained the same result that HOST4 can still connect to running network services.

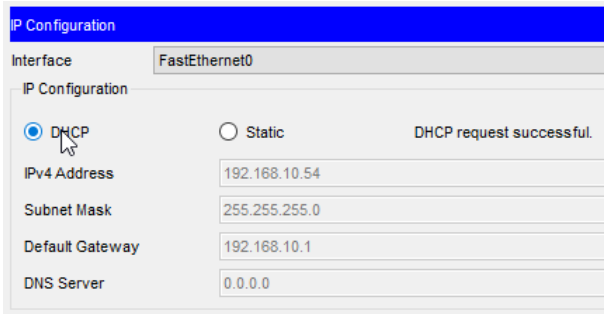

Figure 6. DHCP Client Results on HOST4

```
Switch#sh port-security address
                          Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address Type                          Ports

----    ----------- ----                          -----
1       000B.BE52.3987      DynamicConfigured     FastEthernet0/1
1       000D.BDC4.C1EC      DynamicConfigured     FastEthernet0/2
1       00E0.F9C9.A2D1      DynamicConfigured     FastEthernet0/2
1       0006.2A2E.6B76      DynamicConfigured     FastEthernet0/3
1       0060.70D9.BCD7      DynamicConfigured     FastEthernet0/4
------------------------------------------------------------------------------
```

Figure 7. HOST4 Connectivity Test Results

Described in Figure 6 is the result of testing from HOST4 into network services. The results obtained by HOST4 are able to get an IP Address allocation by DHCP which has been facilitated by the Router above it. And shown in Figure 7 is the result of verification from the layer 2 switch side which shows that there are 2 (two) MAC addresses connected to the FastEthernet0/2 interface, namely 000D.BDC4.C1EC and 00E0.F9C9.A2D1. the implementation of MAC Address Dynamic filtering is only able to record the user's MAC address into the MAC Address table without being able to restrict access such as denial of access if a new client tries to access it. This still forces a network administrator to monitor manually and periodically to ensure the quality of network services.

1.5 Static Sticky Security Port Connectivity Test

To test the connectivity of Static Sticky Port Security, the researcher refers to the network scheme provided in Figure 4, where there is one client with the name USER4 which was not initially connected to the running network. The test is carried out in the same way when testing on Port Security Dynamic, USER4 experimenting access to the running network using the fa0/2 and fa0/10 interfaces on the switch.

Table 4. Test Results for Static Sticky Port Security Connectivity

Device	MAC Address	Interface	Connectivity	
			Before	After
USER4	0060.7057.489D	Fa0/2		Failed
USER4	0060.7057.489D	Fa0/10		Failed

Seen in Table 4 is the result of the USER4 client experiment into the network. The first experiment USER4 conducted a connectivity test using Interface Fa0/2 and the results obtained were USER4 could not connect to the network, the second experiment USER4 used interface

Fa0/10 and got the same result that USER4 still cannot connect to the running network service. Different results between the implementation of Port Security Switch Layer 2 MAC Address Static Sticky with Port Security Switch Layer 2 MAC Address Dynamic. If the Port Security Dynamic new client trying to access network services can still connect, while the Port Security Static Sticky if there is a new client trying to access the network can't.

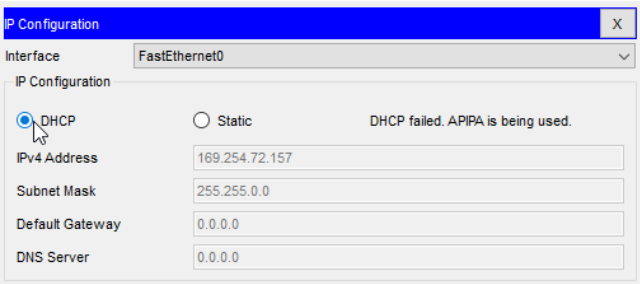

Figure 8. DHCP Client Results on USER4

```
Switch#sh port-security address
                              Secure Mac Address Table
------------------------------------------------------------------------------
Vlan       Mac Address Type                          Ports

----       ----------- ----                          -----
1          000B.BE83.E719        SecureConfigured      FastEthernet0/2
1          0090.2BC8.922E        SecureConfigured      FastEthernet0/3
1          000D.BDC5.A133        SecureConfigured      FastEthernet0/4
------------------------------------------------------------------------------
```

Figure 9. USER4 Connectivity Test Results

Described in Figure 8 is the test result of USER4, the results obtained are that USER4 does not get a DHCP IP Address allocation, different results on a dynamic security port where a new client is able to get an IP Address allocation. While Figure 7 explains the results of the verification of the switch device, it can be seen that there is no additional MAC Address in the MAC Address Table because there are no new clients who are considered successful or have the right to access network services. In order for HOST4 to be able to access network services, the MAC Address used on USER4 0060.7057.489D must be registered in the MAC address table by considering the interface port on the switch device.

4. CONCLUSIONS AND SUGGESTIONS

From the research that has been done, several conclusions can be drawn, as follows:

1) Implementing port security static sticky is considered better than implementing port security dynamically, where if there is a new client attempting access to the network and the client's mac address is not registered, the client absolutely does not get access to network services.
2) To implement port security mac address using either dynamic or static sticky methods, you must consider the MAC address of the client and the interface port on the switch device.
3) The implementation of dynamic port security still has a security gap, where new clients who try to access network services can still access network services. This still forces a network administrator to manually monitor the MAC address table to find out which clients are entitled and not.

Suggestions for further research by adding an interactive decision making tool for port security policy.

REFERENCES

Anathi, M., & Vijayakumar, K. (2020). An intelligent approach for dynamic network traffic restriction using MAC address verification. *Computer Communications* , *154* (July 2019), 559–564. https://doi.org/10.1016/j.com.2020.02.021

Anugrah, I., & Rahmanto, RH (2018). Local Area Network Network Security System Using De-Militarized Zone Technique. *Pixels: Embedded Systems and Logic Computer Science Research* , *5* (2), 91–106. https://doi.org/10.33558/piksel.v5i2.271

Bima Pramudya, P. (2021). Implementation of Mac Address Register To Overcome Anonymous Users On The Network. *Syntax: Journal of Informatics* , *10* (01), 21–32. https://journal.unsika.ac.id/index.php/syntax/article/download/4743/2747

Dwitias Sari, R., Putera Utama Siahaan, A., Muttaqin, M., & Br Ginting, R. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. *International Journal of Scientific Research in Science and Technology* , *3* (6), 470–473. www.ijsrst.com

Firmansyah, Dewi, S., & Adi Purnama, R. (2019). Quality of Service Gateway Load Balancing Protocol Message Digest Algorithm 5 Authentication for Network Quality Improvement. *Journal of International Stmic Informatics Engineering* , *5* (1), 45–50. http://section.iaesonline.com/index.php/JTI/article/view/709

Firmansyah, F., Purnama, RA, & Astuti, RD (2021). Wireless Security Optimization Using Mac Address Filtering. *Journal of Information Technology: Journal of Science and Applications in Informatics Engineering* , *15* (1), 25–33. https://doi.org/10.47111/jti.v15i1.1910

Firmansyah, F., & Wahyudi, M. (2021). Access Control List Performance Analysis Using Firewall Policy Base Method. *MATRIX: Journal of Management, Informatics Engineering and Computer Engineering* , *20* (2), 283–292. https://doi.org/10.30812/matrik.v20i2.1068

Grabovica, M., Pezer, D., Popić, S., & Knežević, V. (2016). Provided security measures of enabling technologies in Internet of Things (IoT): A survey. *2016 Zooming Innovation in Consumer Electronics International Conference, ZINC 2016* , 28–31. https://doi.org/10.1109/ZINC.2016.7513647

Hardi, R., Naim Che Pee, A., & Suryana Herman, N. (2020). Enhanced Security Framework On Chatbot Using Mac Address Authentication To Customer Service Quality. *International Journal of Scientific & Technology Research* , *9* (10). www.ijstr.org

Riska, P., Sugiartawan, P., & Wiratama, I. (2018). Computer Network Security System And Data Using The Port Knocking Method. *Indonesian Journal of Applied Information and Computer Systems (JSIKTI)* , *1* (2), 53–64. https://doi.org/10.33173/jsikti.12

Song, G., & Ji, Z. (2016). Anonymous-address-resolution model. *Frontiers of Information Technology & Electronic Engineering, Springer* , *17* (61472100), 1044–1055.

Srikanth Reddy, P., Saleem Akram, P., Ramana, TV, Aditya Sai Ram, P., Pruthvi Raj, R., & Adarsh Sharma, M. (2020). Configuration of firewalls in educational organization LAB setup by using cisco packet tracer. *Proceedings - 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security, ISSSC 2020* . https://doi.org/10.1109/iSSSC50941.2020.9358818

Subekti, ZM, & Subandri, S. (2020). Implementation of Method Per Connection Queue With Access User Direct Mac Filtering On Wireless Networks. *INOVTEK Polbeng - Informatics Series* , *5* (2), 240. https://doi.org/10.35314/isi.v5i2.1472

Sulaiman, OK (2016). ANALYSIS OF NETWORK SECURITY SYSTEM USING PORT

SECURITY SWITCH. *Computer Engineering, Systems And Science , 1* (1), 9–14.

Trabelsi, Z., & Saleous, H. (2019). Exploring the opportunities of cisco packet tracer for hands-on security courses on firewalls. *IEEE Global Engineering Education Conference, EDUCON , April - 2019* , 411–418. https://doi.org/10.1109/EDUCON.2019.8725112

Zara, SS, Elhanafi, AM, & ... (2020). WAN NETWORK MODELING WITH FRAME RELAY TECHNOLOGY USING PORT SECURITY SWITCH AS A NETWORK SECURITY SYSTEM. *SNASSTIKOM* . http://prosiding.snastikom.com/index.php/SNASTIKOM2020/article/view/66