Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2025. Vol. 4. No. 2; e-ISSN: 2808-4519

Implementation of Bridge Filtering to Prevent DHCP Starvation Attack (Case Study: SD Inpres Papindung)

Yosua Nggaba Patimay[1]*, Fajar Hariadi[2], Raynesta Mikaela Indri Malo[3]

[1,2,3] Program Studi Teknik Informatika, Universitas Kristen Wira Wacana Sumba
Yosuaumbu83@gmail.com [1], fajar@unkriswina.ac.id [2], raynesta@unkriswina.ac.id [3]*

Abstract

The impact of internet cut off or disrupted at SD Inpres Papindung, the teachers will have difficulty finding teaching materials and may have to return to traditional methods that are less effective. Updating Dapodik data will also be disrupted, which could affect school administration and evaluation. The unavailability of an internet connection does occur due to technical reasons or due to intentional elements, one of which is the use of Yersinia software. Yersinia is a piece of software that is commonly used to attack available networks by sending fake MAC addresses continuously so that the IP address on the DHCP server runs out, so that the client does not get an IP address which causes the client unable to access the internet. This attack are called DHCP Starvation Attack. This can be prevented using Bridge Filtering method. Bridge Filtering can filter only recognized MAC addresses to transmit data or can request an IP address from the DHCP server, while MAC addresses that are not recognized or foreign devices will not be allowed to request from that port or will not receive an IP address from the DHCP server. The aim of implementing Bridge Filtering is to measure the creativity of the Bridge Filtering method in preventing DHCP Starvation Attack attacks so that clients who want to connect to the network can access the internet and improve network quality at SD Inpres Papindung.The results show that the Bridge Filtering method effective in preventing DHCP Starvation Attacks and improves network quality at SD Inpres Papindung which is shown by an increase of throughput, before implementation it was 794.66 Kbps and after implementation it was 1283.70 Kbps, there was a decrease of delay from 6.89 ms before implementation to 4.06 ms after implementation. There was also a decrease in jitter before implementation 10.56 ms and after implementation 6.05 ms, but caused an increase in packet loss which was 0.30% before implementation and after implementation increased to 0.79%. Of the four variables, all of them remain at the same level except for the throughput variable, where there is a change from the fair category to the good category, so that it has an impact on the quality of the internet network at SD Inpres Papindung after implementing Bridge Filtering which is stated to be better than before implementing Bridge Filtering on the internet network at SD Inpres Papindung.

Keywords: *MikroTik, DHCP, Yersinia, DHCP Starvation attack, Bridge Filtering.*

1. Introduction

With advances in technology, the need for computer networks and the internet will become increasingly important, both in education, work and other sectors. The use of internet networks in schools can make it easier for teachers to search for interesting and relevant open materials, such as educational videos, images and additional information that can enrich lesson material [1]. Apart from that, the internet network can support teachers to carry out other work, for example filling in performance, inputting Basic Education Data (Dapodik), monitoring the learning environment and accessing other educational information. Without reliable internet access, teachers face challenges in quickly finding open educational resources and may revert to traditional teaching methods, which tend to be less interactive and engaging. Filling in Dapodik data and learning environment surveys will also be disrupted, which could affect school administration and evaluation. Without internet access, getting the latest educational information and following developments in the world of education becomes more difficult, potentially hampering efforts to improve the quality of teaching and learning in schools [2].
Network security in educational environments is critical to protecting sensitive data, such as personal information of students, staff, and academic data, from growing cyber threats. Educational institutions are often targets of attacks due to the large amount of data they manage and their dependence on digital technology for the learning process. Without a strong security system, the risk of data leaks, hacking, and malware attacks can disrupt teaching and learning activities, damage the institution's reputation, and cause financial losses. In addition, good network security also creates a safe environment for students and teachers to access digital resources freely without worrying about online threats, while supporting the development of technology in education in a responsible way [3].

The Bridge Filtering method is used to solve the problem of filtering data or information flow in a network by connecting two different network segments, thereby enabling more efficient data traffic management. This concept is usually applied in systems that require separation between two types of networks or segments without breaking their connectivity. Bridge Filtering works by filtering data flowing between the two networks, blocking or allowing certain packets based on predetermined criteria, such as IP address, protocol, or data type. Its application in a network context can help reduce traffic loads, increase security, and optimize network performance [4].

Sometimes the unavailability of an internet network does not occur due to technical reasons, sometimes it occurs due to deliberate actions, one of which is the use of Yersinia software. Yersinia is a piece of software that is commonly used to attack available networks by sending fake MAC addresses continuously so that the IP address on the DHCP server runs out, so that the client does not get an IP address which causes the client to be unable to access the internet [5].

SD Inpres Papindung is one of the educational institutions located in Mauliru Village, Kec. Kambera District. East Sumba, which was founded on July 22 1980, has a total of 226 students, with 128 males and 98 females, with 17 teachers. The problem that occurs in schools is the lack of internet network security, one of which is the DHCP Starvation Attack, which will send IP addresses continuously so that the DHCP server will run out of IP addresses, so that clients who want to access the network will not get an IP address or will not have internet access.

Form of DHCP attack Starvation Attack is a form of attack where the attacker tries to exhaust all available IP addresses on the DHCP server, so that legitimate users cannot get an IP address and lose access to the network. Attackers typically use automated tools to send spoofed DHCP requests with a variety of random MAC addresses. As a result, the DHCP server runs out of IP addresses it can provide, blocking other devices from connecting to the network. After that, attackers can take advantage of this condition by building a fake DHCP server (rogue DHCP server) to control and traverse the data network.

The purpose of using Yersinia software is to carry out penetration testing and simulate attacks on data link layer protocols in the network, such as STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol), DTP (Dynamic Trunking Protocol), and other network protocols. Yersinia helps network administrators and security researchers identify weaknesses or vulnerabilities in the network infrastructure they manage, so that mitigation or repair steps can be taken before these weaknesses can be exploited by irresponsible parties.

By implementing the Bridge Filtering Method at SD Inpres Papindung, you can prevent DHCP Starvation Attacks. Bridge Filtering can filter only MAC addresses that are already recognized for sending data or can request an IP address from the DHCP server, while MAC addresses that are not recognized or foreign devices will not be allowed to request from that port or will not get an IP address from the DHCP server.

This research aims to prevent DHCP Starvation attacks by applying the Bridge Filtering Method on the network at SD Inpres Papindung. Then measure the effectiveness and influence of implementing Bridge Filtering on the network at SD Inpres Papindung by conducting analysis before and after implementing Bridge Filtering. It is hoped that the results of this research can improve network security at SD Inpres Papindung. The Bridge Filtering method was chosen to prevent DHCP Starvation Attacks at SD Inpres Papindung because the school only uses a MikroTik Router device without a switch. In these networks, a DHCP Starvation Attack attack can cause an exhaustion of IP addresses, making it impossible for legitimate devices to connect. Therefore, researchers used Bridge Filtering on existing MikroTik Routers to filter and limit Starvation Attack DHCP requests, thereby preventing the attack. Compared to the switch port security method, which is generally applied to switch devices to limit access based on MAC addresses, this method cannot be applied at SD Inpres Papindung because there is no switch in the network. Therefore, Bridge Filtering on the MikroTik Router side is an effective solution for protecting school internet networks from DHCP Starvation Attacks.

The effectiveness of the solution for using Bridge Filtering in dealing with DHCP Starvation Attack attacks, steps that can be taken include attack simulation testing before and after implementing Bridge Filtering. Network administrators can perform a controlled DHCP Starvation Attack attack in a test environment using tools such as Yersinia, then determine whether Bridge Filtering is capable of blocking or limiting incoming fraudulent DHCP packets. In addition, it is also important to pay attention to whether authorized users can still receive IP addresses from the DHCP server after Bridge Filtering is applied. Effectiveness can be measured by the reduction in spurious DHCP requests the server receives and the desire for network service to legitimate users without interruption.

2. Research Methodology

There are 5 stages of research that will be carried out by researchers in conducting this research, as shown in the following picture:

Fig. 1: Research Flow

The stages carried out are as follows:

1) Analysis: At this analysis stage the author carried out an analysis by experimenting with running the Yersinia software before applying the Bridge Filtering method. Data collection was carried out by direct observation and conducting interviews with school operators with questions related to the research carried out. Apart from interviews, observations and mapping of the network topology used at SD Inpres Papindung were also carried out.
2) Design: to implement Bridge Filtering by configuring the proxy router to filter invalid or suspicious DHCP packets. This includes checking the origin of packets and ensuring that only packets from legitimate clients are forwarded to the DHCP server at SD Inpres Papindung. Based on initial tests carried out on the Yersenia attack on the internet network at SD Inpres Papindung, it was found that the DHCP Starvation attack attacked the internet network at SD Inpres Papindung by continuously requesting IP addresses so that the DHCP server ran out of IP addresses so that new clients wanted to access the internet network at the elementary school. Inpres Papindung did not get another IP address because the DHCP starvation attack used up the IP provided by the DHCP server.
3) Implementation: Implementation is carried out on the MikroTik device at SD Inpres Papindung which is connected to the internet where the device will be implemented using the Bridge Filtering method according to the design that has been built.
4) Testing: Testing is carried out by comparing the IP Address obtained by the client when a DHCP Starvation Attack occurs using Yersinia before implementation and after implementation, and also testing network quality which is represented through QOS variables in the form of Throughput, Delay, Jitter and Packet Loss before and after application of Bridge Filtering between initial testing during the Yersinia attack on the internet network at SD Inpres Papindung and testing after implementing the Bridge Filtering method on the internet network at SD Inpres Papindung.
5) Final Results: In the analysis section of the final results a comparison will be made between the initial test and the test after applying the Bridge Filtering method. Where an analysis was carried out on the ability of Bridge Filtering to prevent DHCP Starvation Attack attacks, then an analysis was carried out by comparing four QOS variables, namely Trougphut, Delay, Jitter and Packet Loss.

3. Results and Discussiona

In this research the author has prepared a network topology design for the implementation of Bridge Filtering with the Bakti Kominfo ISP, modem, MikroTik router, and connected access points with the internet. The local network design in this research is as in Figure 2

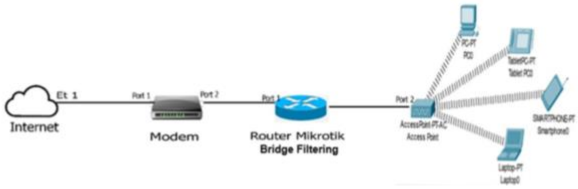


Fig. 2: Network Topology After Implementing The Bridge Filtering Method

a) Bridge

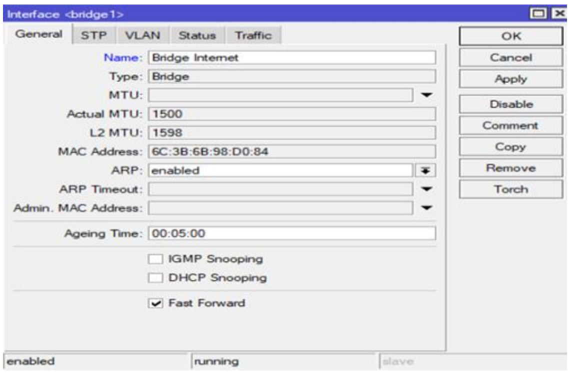


Fig. 3: Internet Bridge Menu

The image above shows the configuration interface for a network bridge in network management software. On the General tab, you can see that this bridge is named Internet Bridge with the bridge type then click apply and ok.

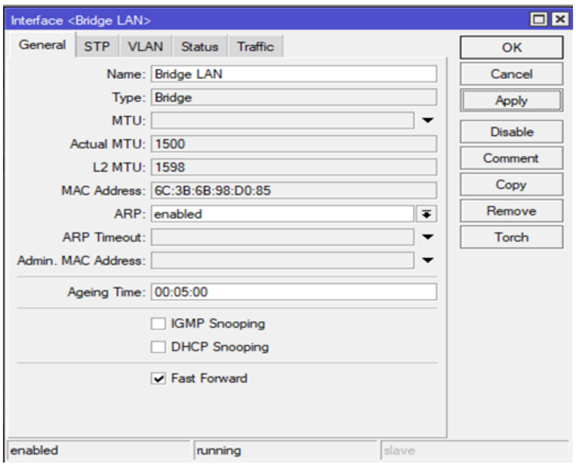


Fig. 4: LAN Bridge Menu

In the picture above is the Bridge 2 menu with the name bridge LAN with bridge type. Bridge LAN is used to connect several network segments so that it can function as one large network.

b) Bridge ports

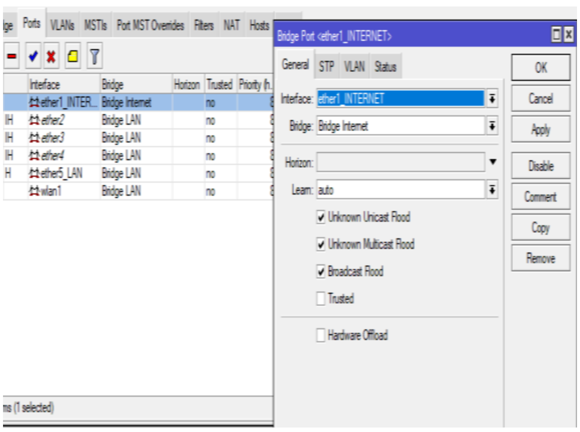


Fig. 5: Bridge Internet Ports

The figure above illustrates that port 1 is used for an internet bridge by entering the bridge then clicking the port menu, on the general tab in the interface menu selecting ether 2 or internet source then on the bridge menu selecting internet bridge then clicking apply and ok.

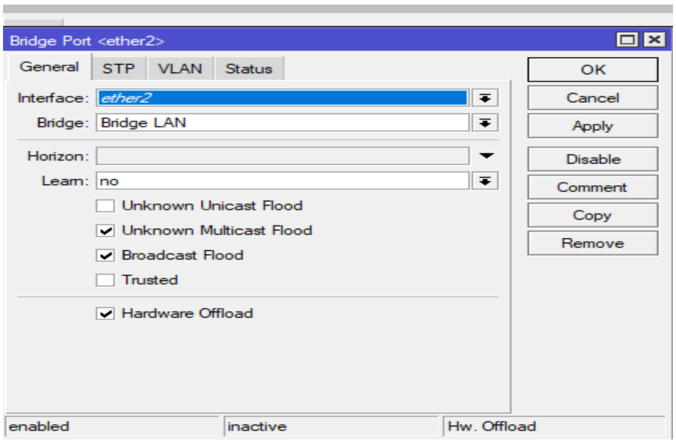


Fig. 6: Bridge LAN Ports

In the figure above illustrates that ports 2 – 5 are used for LAN bridges by entering the bridge then clicking the port menu, on the general tab in the interface menu select ether 2 then on the bridge menu select LAN bridge then uncheck unknown unicast flood then on learn select no click then apply and ok, do the same thing on ether 3,4 and 5.

c) Bridge DHCP clients

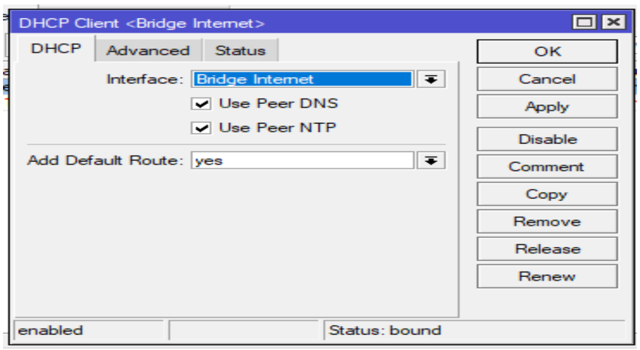


Fig. 7: DHCP Clients

The image above shows where the internet bridge is made into a DHCP client by entering the IP menu then entering DHCP client, on the interface tab select internet bridge then on the add default route menu select yes so that the internet bridge becomes a DHCP client, then click apply and ok wait until you get the IP.

d) LAN bridge IP

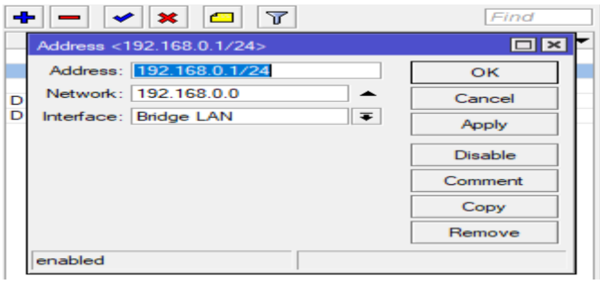


Fig. 8: LAN Bridge IP

The figure above illustrates shows the process of creating an IP address on a LAN bridge, by entering the IP menu section then selecting the address menu, then clicking add in the address column, we enter the IP as in the image above for the network 192.168.0.0 then select the interface. LAN bridge, then click apply and ok.

e) DHCP server

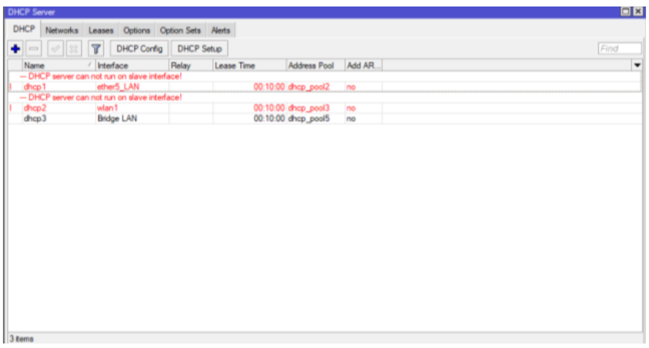


Fig. 9: DHCP Server

The figure above illustrates how to create a DHCP server on a LAN bridge by entering the IP menu then selecting the DHCP server tab then clicking DHCP setup then selecting LAN bridge then clicking next until successful and then a picture will appear like the picture above.

f) Bridge Filter

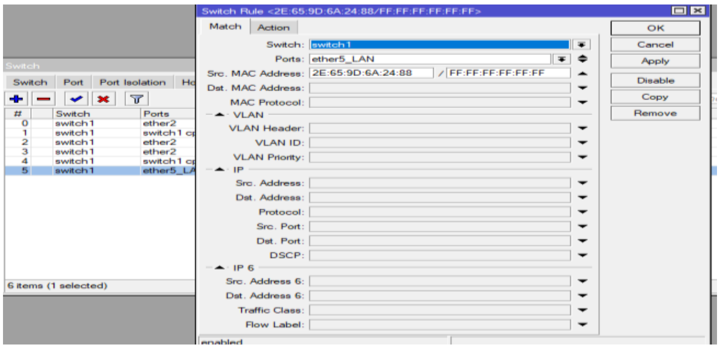


Fig. 10: Rules Menu

The figure above illustrates how to make switch 1 by selecting the switch menu then going to the rules tab, click add, then it will appear like the picture above on the switch, select switch 1 then fill in ports with ether5_LAN then Src. Mac Address: Fill in the MAC address of the laptop or PC that has been registered, then select the action menu as shown in the image below.

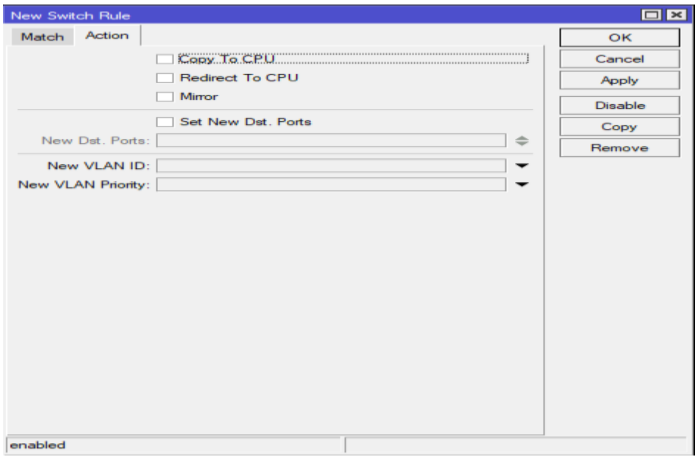


Fig. 11: Actions Tab

The figure above illustrates the devices that can pass through or can connect to the internet network by unchecking set new, etc. Ports.

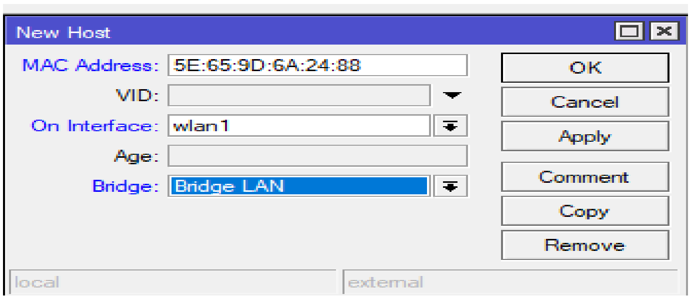


Fig. 12: Host Menu

he image above explains how to add a MAC address to the host menu by entering the bridge menu, then selecting the host menu, then clicking Add, an image like the one above will appear, then on the MAC Address tab, add the MAC address that has been registered or the interface where the plug is placed. connected then on the bridge menu select LAN bridge then click apply and ok.

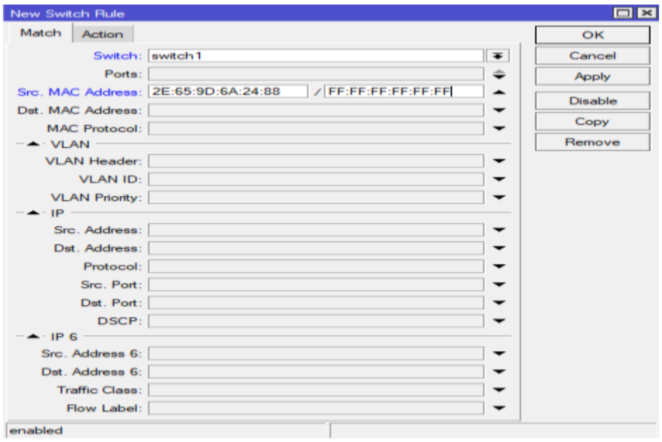


Fig. 13: Switch Rule Without Purpose

The image above explains the creation of switch 1 without a purpose by selecting the switch menu then entering the rules tab, clicking add, then it will appear like the image above on the switch. We use switch 1 in the port menu and leave it blank then on Src. Mac Address: Fill in the MAC address of the laptop or PC that has been registered. Then select the action menu as shown in the image below.

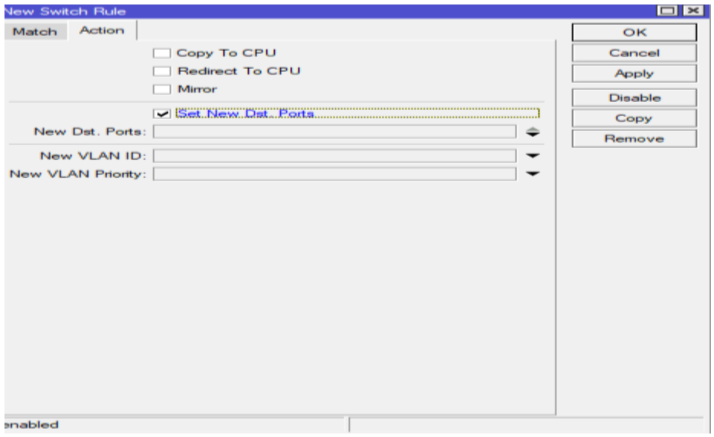
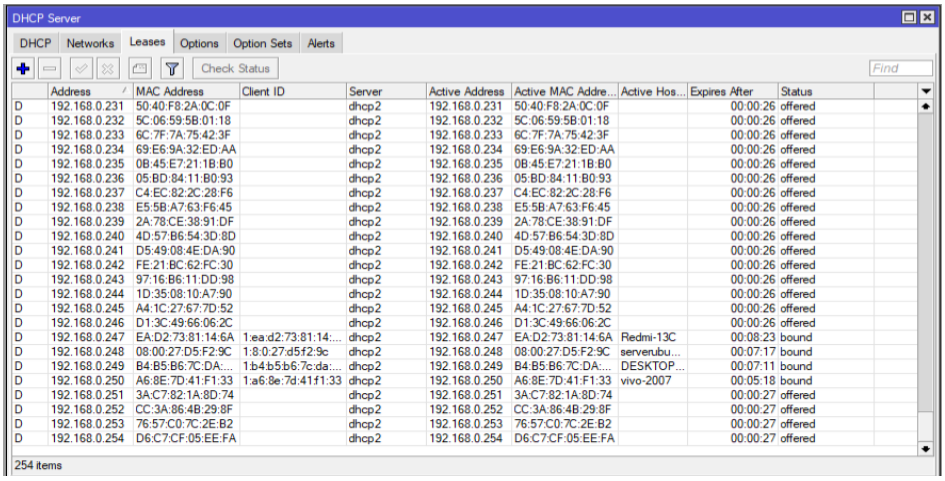


Fig. 14: Action Block Tab

The image above explains how to block MAC addresses that are not registered by checking set new, etc. Ports then click apply and ok, so only the registered MAC addresses can be connected to the internet network.

g) The following are initial tests before implementing the Bridge Filtering Method:



DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

Check Status

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Hos...	Expires After	Status
D	192.168.0.231	50:40:F8:2A:0C:0F		dhcp2	192.168.0.231	50:40:F8:2A:0C:0F		00:00:26	offered
D	192.168.0.232	5C:06:59:5B:01:18		dhcp2	192.168.0.232	5C:06:59:5B:01:18		00:00:26	offered
D	192.168.0.233	6C:7F:7A:75:42:3F		dhcp2	192.168.0.233	6C:7F:7A:75:42:3F		00:00:26	offered
D	192.168.0.234	69:E6:9A:32:ED:AA		dhcp2	192.168.0.234	69:E6:9A:32:ED:AA		00:00:26	offered
D	192.168.0.235	0B:45:E7:21:1B:B0		dhcp2	192.168.0.235	0B:45:E7:21:1B:B0		00:00:26	offered
D	192.168.0.236	05:BD:84:11:B0:93		dhcp2	192.168.0.236	05:BD:84:11:B0:93		00:00:26	offered
D	192.168.0.237	C4:EC:82:2C:28:F6		dhcp2	192.168.0.237	C4:EC:82:2C:28:F6		00:00:26	offered
D	192.168.0.238	E5:5B:A7:63:F6:45		dhcp2	192.168.0.238	E5:5B:A7:63:F6:45		00:00:26	offered
D	192.168.0.239	2A:78:CE:38:91:DF		dhcp2	192.168.0.239	2A:78:CE:38:91:DF		00:00:26	offered
D	192.168.0.240	4D:57:B6:54:3D:8D		dhcp2	192.168.0.240	4D:57:B6:54:3D:8D		00:00:26	offered
D	192.168.0.241	D5:49:08:4E:DA:90		dhcp2	192.168.0.241	D5:49:08:4E:DA:90		00:00:26	offered
D	192.168.0.242	FE:21:BC:62:FC:30		dhcp2	192.168.0.242	FE:21:BC:62:FC:30		00:00:26	offered
D	192.168.0.243	97:16:B6:11:DD:98		dhcp2	192.168.0.243	97:16:B6:11:DD:98		00:00:26	offered
D	192.168.0.244	1D:35:08:10:A7:90		dhcp2	192.168.0.244	1D:35:08:10:A7:90		00:00:26	offered
D	192.168.0.245	A4:1C:27:67:7D:52		dhcp2	192.168.0.245	A4:1C:27:67:7D:52		00:00:26	offered
D	192.168.0.246	D1:3C:49:66:06:2C		dhcp2	192.168.0.246	D1:3C:49:66:06:2C		00:00:26	offered
D	192.168.0.247	EA:D2:73:81:14:6A	1:ea:d2:73:81:14:...	dhcp2	192.168.0.247	EA:D2:73:81:14:6A	Redmi-13C	00:08:23	bound
D	192.168.0.248	08:00:27:D5:F2:9C	1:8:0:27:d5:f2:9c	dhcp2	192.168.0.248	08:00:27:D5:F2:9C	serverubu...	00:07:17	bound
D	192.168.0.249	B4:B5:B6:7C:DA:...	1:b4:b5:b6:7c:da:...	dhcp2	192.168.0.249	B4:B5:B6:7C:DA:...	DESKTOP...	00:07:11	bound
D	192.168.0.250	A6:8E:7D:41:F1:33	1:a6:8e:7d:41:f1:33	dhcp2	192.168.0.250	A6:8E:7D:41:F1:33	vivo-2007	00:05:18	bound
D	192.168.0.251	3A:C7:82:1A:8D:74		dhcp2	192.168.0.251	3A:C7:82:1A:8D:74		00:00:27	offered
D	192.168.0.252	CC:3A:86:4B:29:8F		dhcp2	192.168.0.252	CC:3A:86:4B:29:8F		00:00:27	offered
D	192.168.0.253	76:57:C0:7C:2E:B2		dhcp2	192.168.0.253	76:57:C0:7C:2E:B2		00:00:27	offered
D	192.168.0.254	D6:C7:CF:05:EE:FA		dhcp2	192.168.0.254	D6:C7:CF:05:EE:FA		00:00:27	offered

254 items

Fig. 15: Testing Before Implementing Bridge Filtering

Based on initial tests carried out on the Yersenia attack on the internet network at SD Inpres Papindung, it was found that the DHCP Starvation attack attacked the internet network at SD Inpres Papindung by continuously requesting IP addresses so that the DHCP server ran out of IP addresses so that new clients wanted to access the internet network at the elementary school. Inpres Papindung did not get another IP address because the DHCP starvation attack used up the IP provided by the DHCP server.

The following is the final test after implementing the Bridge Filtering Method:

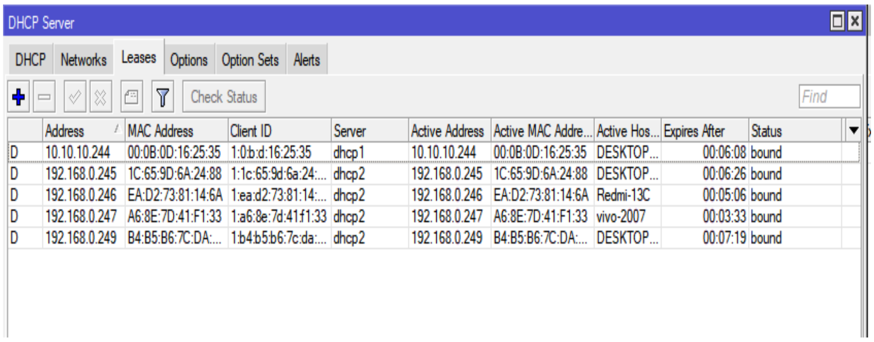


Fig. 16: Testing After Implementing Bridge Filtering

The picture above shows the final test carried out after implementing Bridge Filtering, where when the Yersenia software attacked the internet network, it was found that the DHCP Starvation attack could no longer attack the availability of internet network access at SD Inpres Papindung, in other words the Bridge Filtering method was able to block DHCP attacks Starvation Attack on the internet network of SD Inpres Papindung.

h) QoS (Quality of Service) Analysis

Quality of Service (QoS) is a method for measuring and managing performance and quality in a network. Various services have different requirements in terms of performance such as throughput, packet loss, delay, and jitter. Apart from testing the success of implementing Bridge Filtering, QOS testing was also carried out before and after implementing Bridge Filtering.

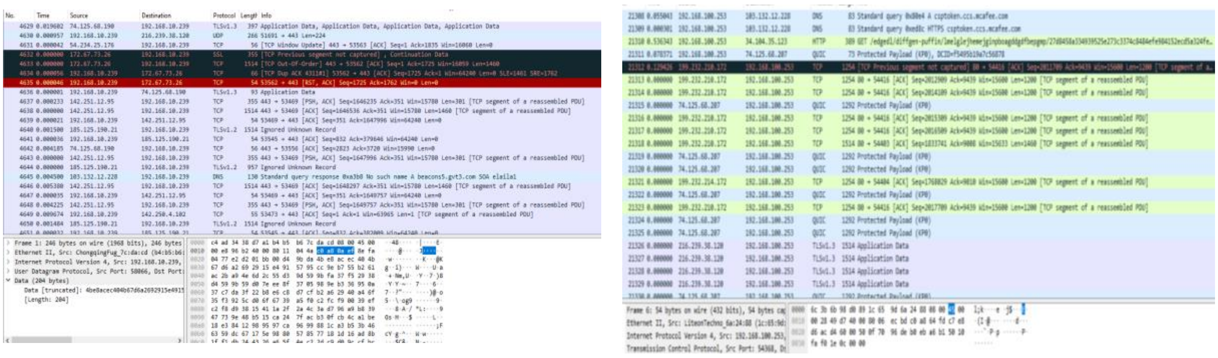


Fig. 17: 1) Capture Results Before Applying Bridge Filtering, 2) Capture Results After Applying Bridge Filtering

From the capture results, throughput, packet loss, delay and jitter are calculated beforehand application of Bridge Filtering and after application of Bridge Filtering.

1. Throughput Before Implementation

Throughput = (Data Packets Received)/(Observation Time)
Throughput = 65979923/664.232 bytes/second Bps
Throughput = 65979923/664.232
Throughput = 99332,647 byte per second (Bps)
Throughput = 99.33 kBps
Throughput = 99.33 x 8 kbps
Throughput = 794.66 kbps

1. Throughput After Implementation

Throughput=(Data Packets Received)/(Lama Pengamatan)
Throughput= 119520922/744.851 bytes/second Bps
Throughput=119520922/744.851
Throughput =160462,860 byte per second (Bps)
Throughput=160.462 kBps
Throughput=160.462 x 8 kbps
Throughput = 1283.70 kbps

2. Packet Loss Before Implementation

Packet Loss = (packet lost)/(Data Packet Sent) x 100%
Packet Loss = (292)/96410 x 100%
Packet Loss = (292)/96410 x 100%
Packet Loss = 0.30 %

2. Packet Loss After Implementation

Packet Loss = (packet lost)/(Data Packet Sent) x 100%
Packet Loss = (1456)/183287 x 100%
Packet Loss = 1456/183287 x 100%
Packet Loss = 0.79 %

Delay Before Implementation

Rata-rata Delay = Total Delay⁄Total Packages Received
Rata-rata Delay = 664.23⁄96410
Rata-rata Delay = 0.0069 s (seconds)
Rata-rata Delay = 0.0069 x 1000 ms (milliseconds)

Rata-rata Delay = 6.89 ms (milliseconds)

3. Jitter Before Implementation

Jitter = (Total Delay Variation)/(Total Packets Received-1)
Jitter = 1018.39/(96410-1)
Jitter = 1018.39/96409
Jitter = 0.01056 s
Jitter = 0.01056 x 1000 ms
Jitter = 10.56 ms

3. Delay After Implementation

Rata-rata Delay = Total Delay⁄Total Packages Received
Rata-rata Delay = 744.85⁄183287
Rata-rata Delay = 0.0040 s (seconds)
Rata-rata Delay = 0.0040 x 1000 ms (milliseconds)
Rata-rata Delay = 4.06 ms (milliseconds)

4. Jitter After Implementation

Jitter = (Total Delay Variation)/(Total Packets Received-1)
Jitter = 1109.53/(183286-1)
Jitter = 1109.53/183285
Jitter = 0.00605 s
Jitter = 0.00605 x 1000 ms
Jitter = 6.05 ms

QOS measurements have an impact on the quality of the internet network at SD Inpres Papindung where the network quality on the internet network at SD Inpres Papindung remains in good condition before and after the implementation of Bridge Filtering.

4. Conclusion

The implementation of Bridge Filtering at SD Inpres Papindung can be implemented and can successfully prevent attacks from DHCP Starvation Attack so that the internet network at SD Inpres Papindung can be used more safely. The implementation of Bridge Filtering also caused an increase in throughput, before implementation it was 794.66 Kbps and after implementation it was 1283.70 Kbps, there was a decrease in delay from before implementation 6.89 ms and after implementation 4.06 ms. There was also a decrease in jitter before implementation 10.56 ms and after implementation 6.05 ms, but caused an increase in packet loss which was 0.30% before implementation and after implementation increased to 0.79%. Of the four variables, all of them remain at the same level except for the throughput variable, where there is a change from the fair category to the good category. The implementation of Bridge Filtering at SD Inpres Papindung is effective in preventing DHCP Starvation Attack attacks and improving network quality, as proven by increasing throughput, reducing delay and jitter. However, despite the improvements, there has been an increase in packet loss that needs to be taken into account. As a recommendation, schools should continue to monitor network performance periodically to identify other potential problems, increase DHCP server capacity to reduce the possibility of network disruption, and consider strengthening network infrastructure to minimize packet loss. In addition, training for teachers in the use of network devices and security software is also important to maintain system stability.

For further research, it is recommended to explore various other network security methods that can complement the implementation of bridge filtering in preventing DHCP starvation attacks. Several areas that could be the focus of research include the implementation of intrusion detection systems (IDS) to detect and prevent attacks early, as well as the use of VLAN (Virtual Local Area Network) technology to limit network access and improve segmentation. Additionally, using security protocols such as IPsec to encrypt communications between devices can also provide an additional layer of protection. Further research could also include evaluating the effectiveness of such methods in more dynamic environments, such as in cloud-based networks or IoT systems, where security challenges are more complex. In this way, a more holistic solution can be found to protect the network from various growing threats.

References

[1] Amarudin, A. (2018). Desain Keamanan Jaringan Pada MikroTik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2), 72. https://doi.org/10.33365/jti.v12i2.121

[2] Ariyadi, T., Nur Riyansyah, A., Agung, M., & Ikrar, M. A. (2023). Analisis Serangan Dhcp Starvation Attack Pada Router Os MikroTik. *Jurnal Ilmiah Informatika*, *11*(01), 85–93. https://doi.org/10.33884/jif.v11i01.7162

[3] Dara, Y. C., Hariadi, F., Alfa, P., & Leo, R. (2022). Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode DHCP Snooping dan Switch Port Security. *Jurnal Inovatif Wira Wacana*, *01*(03), 187–196. https://ojs.unkriswina.ac.id/index.php/inovatif/article/view/337

[4] Fikri, K., & Djuniadi. (2021). Keamanan Jaringan Menggunakan Switch Port Security. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, *5*(2), 302–307. http://bit.ly/InfoTekJar

[5] Hanifia, R. (2019). Penerapan Quality of Service (QoS) Differentiated Service Pada Jaringan Multi-Protocol Label Switching (MPLS). *Jurnal Manajemen Informatika*, *9*(2), 1–7.

[6] Ishak, N., Hamza, S., & Hamid, M. (2023). Analisis Keamanan Jaringan Menggunakan Switch Port Security Padawarnet Gramit Kelurahan Sasa Ternate Selatan. *Jurnal PRODUKTIF*, *7*(1), 611–618.

[7] Rodiyah, A., Diana Mustafa, L., & Elfa M., P. (2018). Implementasi Management Bandwidth Pada Sistem Billing Kafe Menggunakan Autentikasi Qr Code. *Jartel*, *7*(2), 1–7.

[8] Sanjaya, T., & Setiyadi, D. (2019). 1-10 Teknik Informatika; STMIK Bina Insani. *Rawa Panjang Bekasi Timur*, *4*(1), 17114.

[9] Saputra, B. R. (2022). Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping Dan VLAN Mengggunakan CISCO. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *9*(4), 3481–3488. https://doi.org/10.35957/jatisi.v9i4.2730

[10] Sarip, N., & Setyanto, A. (2019). Packet Filtering Based On Differentiated Services Code Point For DHCP Starvation Attacks Prevention. *Journal Pekommas*, *4*(2), 137. https://doi.org/10.30818/jpkm.2019.2040204