© 2017 IJSRST | Volume 3 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Review of IP and MAC Address Filtering in Wireless Network Security

Ressy Dwitias Sari[1], Supiyandi[2], Andysah Putera Utama Siahaan[3], Muhammad Muttaqin[4], Raheliya Br. Ginting[5]

[1,2,3,4]*Faculty of Computer Science, Universitas Pembanguan Panca Budi, Medan, Indonesia*
[5]*Department of Informatics, Politeknik Poliprofesi Medan, Medan, Indonesia*
[3]*Ph.D. Student of School of Computer and Communication Engineering, Universiti Malysia Perlis, Kangar, Malaysia*

ABSTRACT

Technological developments in computer networks increasingly demand security on systems built. Security also requires flexibility, efficiency, and effectiveness. The exchange of information through the internet connection is a common thing to do now. However, this way can be able to trigger data theft or cyber crime which resulted in losses for both parties. Data theft rate is getting higher by using a wireless network. The wireless system does not have any signal restrictions that can be intercepted Filtering is used to restrict incoming access through the internet. It aims to avoid intruders or people who want to steal data. This is fatal if not anticipated. IP and MAC filtering is a way to protect wireless networks from being used and misused by just anyone. This technique is very useful for securing data on the computer if it joins the public network. By registering IP and MAC on a router, this will keep the information unused and stolen. This system is only a few computers that can be connected to a wireless hotspot by IP and MAC Address listed.

Keywords : Wireless Security, IP, MAC Address, Filtering

I. INTRODUCTION

Currently, wireless networks are increasingly being used in homes, schools, universities, and offices. It is supported by the ease and convenience of its use since it does not need to use cable. Installing a network using a cable on a LAN will be very inconvenient. Wireless networks are vulnerable to attacks and interference from outside parties while on a network that uses cables, this can be overcome by checking the cable connection whether there is a violation of the rules or not. It is because wireless networks use radio signals as a medium of information delivery. Therefore, the main factor to be considered is the security issue so that the signal can not be taken over by the irresponsible person.

Wireless network is a network that uses electromagnetic waves as a transmitter. Because of strong waves, every client can connect with this router's emission. Wifi Access Point is a tool that can connect to it. The most common problem is to find out where the intruder is trying to connect to the wireless network. In the cable network, the connected computer can easily be known by checking the position of the LAN cable on the hub. Stealth cables can be easily found if there is any suspicion in the network. On a wireless network, the infiltrated intruders can be detected via a connected MAC Address, but the weakness of the person's existence can not be found as easily as imagined [4]. It is a reason why wireless network security is needed. Unlike wired networks, wireless signal coverage range can not be determined in absolute terms. The stronger the signal, the easier the computer can be connected. However, this is very dangerous. The more distance a router reaches, the more people can connect to it.

II. METHODS AND MATERIAL

2.1 Wireless Network

Wireless technology enables one or more equipment to communicate without using a cable. This connection requires only certain signals and frequencies to connect. Air mediates the transmission of information with the help of waves emitted from the router [3]. There are many types of data transmission wirelessly. For example, Infra Red, Bluetooth, WiFi, Radio are types of data transmission equipment. Wifi networks do not use cables as connected devices, but it still has a topology. It illustrates how wireless devices interact on the physical layer of the OSI model. At the Physical layer, the 802.11 wireless-based network uses spectrum communications spreading sequentially at 2.4 GHz, and the devices communicate with each other using two basic topologies: adhoc and infrastructure.

2.2 Wireless Threat

Wireless technology enables one or more equipment to communicate without any cable. There are several kinds of security threats that can be occurred when connected to the internet [3]. All of this represents potential threats in wireless networks as well. However, the main concern on wireless communication is the data, malicious software, malicious codes, theft and industrial and foreign espionage [5][6]. Theft can happen on wireless equipment because it has been taken. Eligible and unauthorized system users can commit embezzlement and theft. It is easier to steal since the interceptor knows the resources has a system security weakness. The people who do the interception is a cracker. They are who enter the system without rights, usually for personal retribution or for committing a crime. Crackers are from outside and inside the organization.

Many software can damage the system by injecting it to a server. The crackers can get access to wireless network access points by eavesdropping on wireless equipment communications. Malicious code includes viruses, worms, Trojan Horses, logic bombs, or other unwanted software designed to damage files or weakens the system [7][8]. Theft of service occurs when users are not entitled to access to networks and use network resources. Many data are stolen when such virus has been inside the mainframe. It is, especially in government and military office. In wireless networks, the stealing is performed by eavesdropping in radio transmissions. Ensuring confidentiality, integrity, authenticity, and availability is the ultimate goal of the security policies of all governments.

2.3 IP Address

IP Address is the address or digital identity given to a computer device so that the computer can communicate with other computers. Of course, to get the IP Address, the computer must have a network card [2]. IP Address consists of 4 blocks of decimal numbers whose value has a range between 0 to 255. Distribution of IP Address consists of five classes, such as:

- IP Class A. The first 8 bits are the network ID, and the next 24 bits are the host ID, class A network has particularly Id from 0 to 127.
- IP Class B .The first 16 bits are network Id, and the next 16 bits are host Id, class B has network id from 128 to 191
- IP Class C. The first 24 bits are network Id, and the next 8 bits are host Id, class C has network id from 192 to 223
- IP Class D. It is used for multicasting, ie the use of applications together by multiple computers, and IP that can be used is 224.0.0.0 - 239.255.255.255
- IP Class E. It has a range of 240.0.0.0 - 254.255.255.255, this IP is used for experiments prepared for future IP address usage.

The IP Address function is like a home address. Each address has city, district, street, number and zip code. There can not be a house that has the same address combination. So is the IP Address. IP address has an important role in communicating on computer networks. The data packet delivery error will never occur if the IP Address is configured properly.

2.4 MAC Address

MAC Address is a special number on every computer network card, switch, router, access point, or all that can be connected with other devices in the network mechanism. It allows devices in the network to communicate with each other [1]. In an Ethernet-based network, each header in the Ethernet frame contains information about the MAC address of the source and MAC addresses of the destination computer. If a computer has more than one network card, then the computer must also have MAC Address respectively. Each laptop currently has two MAC Address, the wired network card (RJ-45), and wireless network card (802.11b).

III. RESULTS AND DISCUSSION

3.1 IP and MAC Address Filtering

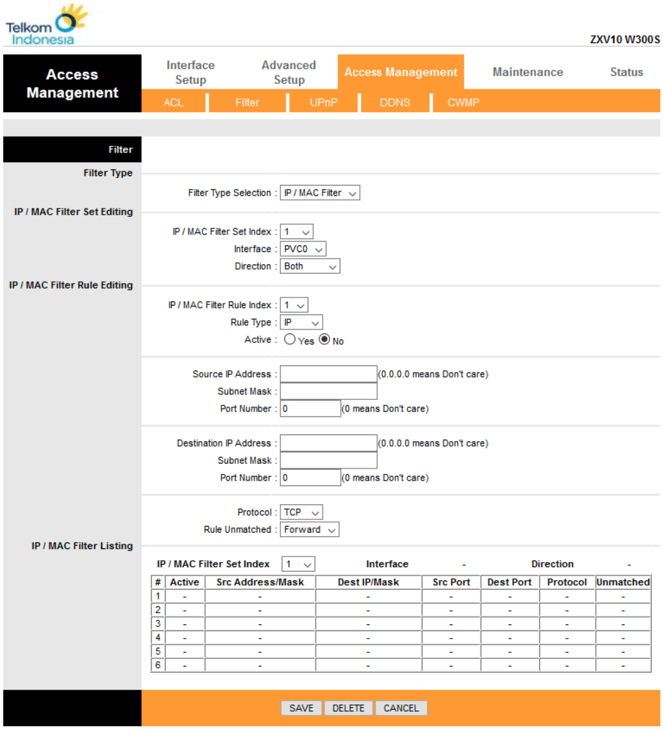
On a multiple-client network, an IP setting mechanism is necessary since it is used to prevent the monopoly of bandwidth usage so that all clients can get their respective bandwidth quota. Wireless networks have three standard security services to avoid any threats to the network.

- Authentication. It is to provide security services to ensure the identity of the client's communicating location. It provides network control by denying access to client stations that can not authenticate correctly.
- Confidentiality. It is to provide "the privacy gained on cable networks." The intention is to prevent leakage of information by eavesdropping.
- Integrity. It is to ensure that messages are not changed while sending between wireless clients and access points in active attacks.

IP and MAC Filtering is always owned by the router to allow users to configure their network freely. This is done to keep everyone from entering indiscriminately to modify settings. The disadvantage of this is the MAC address is very easy dispoofing or even changed. Tools ifconfig on Linux / Unix OS or various tools such as network utilitis, regedit, smac, machange on Windows OS are some examples of applications that can modify MAC Address. For common protection, MAC Address is a great choice, but to keep big company data like government and military, MAC Address is not a good choice. In wireless networks, MAC address duplication does not result in conflict.

3.2 Filtering Advantages

Each router has been facilitated by IP and MAC Filtering menu. It aims to provide convenience in the distribution of internet bandwidth. Activities on the client can be controlled in full to ensure that the activities performed by the client do not violate the rules that have been set.



Filter Type Selection : IP / MAC Filter

IP / MAC Filter Set Index : 1
Interface : PVC0
Direction : Both

IP / MAC Filter Rule Index : 1
Rule Type : IP
Active : ○ Yes ● No

Source IP Address : (0.0.0.0 means Don't care)
Subnet Mask :
Port Number : 0 (0 means Don't care)

Destination IP Address : (0.0.0.0 means Don't care)
Subnet Mask :
Port Number : 0 (0 means Don't care)

Protocol : TCP
Rule Unmatched : Forward

IP / MAC Filter Set Index 1 Interface - Direction -

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

Figure 1. TP-LINK ZXV10 W300S IP/MAC Filtering

Figure 1 describes the menu contained on the TP-LINK ZXV10 W300S router. IP Address can be registered in detail in this section which can pass access to which router can not. The port number specifies the options when it wants to block access to certain ports. In addition to IP Address, MAC Address can also be blocked access. There are three parts to this menu, IP / MAC Set Editing, IP / MAC Rule Editing and IP / MAC Listing Filter.

IP and MAC Address filter serve to help administrators to prevent and control users who are entitled to enter their system, especially to the wireless router. Only wireless devices are trusted or have registered MAC addresses that may gain access to the wireless router.

IV. CONCLUSION

IP Address and MAC Filter are the essential security tool for avoiding the data theft. From the above discussion, it can be concluded that wireless technology has the advantage that the user does not have to bother with the affairs of wiring to make the network more efficient and effective. However, it also has a negative impact; This is to make it easier for data thieves to commit crimes without knowing where they are. IP and

MAC security can be done to minimize wireless crimes. Giving a password or access code to the router can help reduce data theft on the network system. Security on wireless networks can be anticipated from various things. However, it all depends on how a network administrator manages it. Things that need to be avoided is to provide additional access to the unauthorized person.

V. REFERENCES

[1]. Wikipedia, "MAC address," 6 July 2017. [Online]. Available: https://id.wikipedia.org/wiki/MAC_address. [Accessed 22 August 2017].

[2]. O. XL, "What is IP Address ? DNS And Subnetting?," [Online]. Available: http://www.open0xl.com/domain-ping. [Accessed 21 August 2017].

[3]. A. Lubis and A. P. U. S. , "Network Forensic Application in General Cases," IOSR Journal of Computer Engineering, vol. 18, no. 6, pp. 41-44, 2016.

[4]. A. K. Singh and B. Mishra, "WLAN Security: Active Attack of WLAN Secure Network (Identity theft)," International Journal of Computer Science Issues, vol. 3, no. 1, pp. 555-559, 2011.

[5]. S. Nixon and Y. Haile, "Analyzing Vulnerabilities on WLAN Security Protocols and Enhance its Security by using Pseudo Random MAC Address," International Journal of Emerging Trends & Technology in Computer Science, vol. 6, no. 3, pp. 293-300, 2017.

[6]. A. R. Vaidya and S. Jaiswal, "Secure and Flexible Communication Technique: Implementation Using MAC Filter in WLAN and MANET for IP Spoofing Detection," International Journal of Computer Networks and Wireless Communications, vol. 3, no. 4, pp. 519-525, 2016.

[7]. H. A. A., V. G. A. and H. A. P., "Media Access Control Spoofing Techniques and its Counter Measures," International Journal of Scientific & Engineering Research, vol. 2, no. 6, pp. 1-5, 2012.

[8]. M. Izhar and V. R. Singh, "Network Security Vulnerabilities: Malicious Nodes attack," International Journal of Scientific and Research Publications, vol. 4, no. 7, pp. 1-5, 2014.