AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Visibility for Network Security Enhancement in Internet Protocol over Ethernet Networks

[1]Waleed Kh. Alzubaidi, [2]Dr. Longzheng Cai and [3]Shaymaa A. Alyawer, [1]Erika Siebert-Cole

[1]Information Technology Department, University of Tun Abdul Razak, Selangor, Malaysia
[2]International University, Selangor, Malaysia
3Computer Science Department, Baghdad College, Baghdad, 645, Iraq

ARTICLE INFO

Article history:
Received 25 April 2014
Received in revised form
8 May 2014
Accepted 20 May 2014
Available online 17 June 2014

Keywords:

ABSTRACT

This study addresses the naming architecture security problems arising in Internet protocol (IP) over Ethernet networks. These problems arise because of the compatibility issue between two different compositional protocols: the IP and Ethernet protocol. The findings of this study have given rise to proposals for modifications. A reduction in the current naming architecture design is advocated, which led to utilize Ethernet frame to provide a visibility for IP over Ethernet networks. The use of the IP address, as one flat address for the naming architecture, is proposed instead of using both the IP and Media Access Control (MAC) addresses. The proposed architecture has shown a promising in network security enhancement.

To Cite This Article: Waleed Kh. Alzubaidi, Dr. Longzheng Cai and Shaymaa A. Alyawer, Erika Siebert-Cole., Visibility for Network Security Enhancement in Internet Protocol over Ethernet Networks. ***Aust. J. Basic & Appl. Sci.,*** *8(21): 48-54, 2014*

INTRODUCTION

IP over Ethernet network has become the primary network used by the Internet. In this network, the data link layer (Layer 2) security problems, has not yet been adequately addressed. The motivation behind addressing the compatibility problem is to improve the security of networks by studying the link compatibility between the Ethernet and IP protocols. The Ethernet was not established to work with a specific network layer (Layer 3) protocol. Likewise, the IP protocol was not designed to work with a specific Layer 2 protocol (Postel, Jon, 1981). This scenario clearly indicates that the relationship between the IP and Ethernet protocols is not fully compatible because such networks are not dedicated to each other, which can give rise to numerous security problems. Resolving the IP to Media Access Control (MAC) address and the encapsulation of the IP packet into the Ethernet frame are some requirements to link the IP and Ethernet protocols. Therefore, flat IP address was proposed to represent the naming architecture (Alzubaidi, Waleed Kh, 2012). The use of the IP address, as one flat address for the naming architecture, is proposed instead of using both the IP and MAC addresses.

In this study, a new concept is introduced to reveal the origin of the private LAN addresses or of an undeclared Layer 2 address. Internet visibility is not possible with the current naming architecture in the IP over Ethernet networks (Wulf, Volker, 1993); thus, a new solution to current security problems is introduced in this study.

The visibility in the network provides new methods to handle the various network security threats. For instance, a client can connect to and request services from a Web server in the WAN without revealing private IP and MAC addresses (Forouzan, Behrouz A., 2002) (even with a public IP with a proxy case) in the current architecture. As a result, several types of network attacks can be accomplished without disclosing the source of the attack. The IP address from Layer 3 is not detected because of the existence of a NAT in the subsequent router that replaces the original private IP address with the router's public IP address. The Layer 2 MAC address cannot be revealed in any side point because the destination and the source MAC addresses are replaced with new addresses in each hop. Determining the source of the IP address, in case it is a public IP address, is possible in Layer 3; however, even this IP type, which has network proxies, cannot be revealed. This study introduces the main procedures for the visibility concept proposed for the networks and focuses on the factors that enable this concept. The dependency and the requirements of the visibility mechanism are also revealed, and the Visibility Merging Address (VMA) is also explained in the next sections.

Corresponding Author: Waleed Kh. Alzubaidi, Information Technology Department, University of Tun Abdul Razak, Selangor, Malaysia
E-mail: waleed@ieee.org.

This paper is organized as follows. Next, in Section 2, we describe utilizing source hardware address in Ethernet frame header. Section 3 presents the visibility merging address VMA. Section 4 describes the VMA construction mechanism. Section 5 describe the visibility architecture and Section 6 the conclusions.

1. Utilizing Source Hardware Address in Ethernet Frame Header:

In a LAN, the ARP is used to map the IP address to the MAC address. The destination of the MAC address should be obtained by a source machine using a destination IP address to construct and transmit the Ethernet frame in IP over Ethernet networks (Plummer, C. David, 1982). This task is performed by the ARP through a broadcast request for mapping the IP to the MAC address and through a stored reply in a memory space called an ARP cache table. ARP is work as follows: An application attempts to send data to an IP address of a machine. The IP packet is created by the network stack and then encapsulated into the Ethernet frame. The destination of the MAC address is required to transmit this frame (Alzubaidi, Waleed Kh, 2012). Therefore, the network stack verifies the IP in the ARP cache table to locate the destination of the MAC address. If such information is not there, the broadcast ARP request is sent in the network. Each machine in the network examines the ARP request and checks if the requested IP is owned. The machine that owns this IP will create an ARP reply containing the MAC address. A unicast reply would then be sent to the originator of this request. The originator uses this address in the destination MAC address field to complete and transmit the frame. This simple protocol does not have any type of security to bind the IP to the MAC and may result in serious breaches in security. For instance, the ARP poisoning attack uses unsolicited ARP reply messages. Network devices cannot verify the ARP sender and whether the message comes from the correct device. The ARP does not provide any security measures, but is based on broadcast messages on the LAN.

2. Network Visibility Concept:

Providing an address that represents the source of the IP and the MAC addresses on the Internet clearly informs the end point regarding the origin of the delivered information. Thus, the two ends of the connection to obtain precise information about each other. If the VMA concept is utilized, the server clearly identifies the location of a client in the client server architecture and vice versa. The role of the source hardware address field in the Ethernet frame in this approach is to provide this representative source address. Therefore, the transfer of the source MAC address and the source IP address is proposed to provide and enable visibility between the two ends of the connection. The two addresses are represented in the merged address form concept under the condition that 48 bits of the source hardware address field must be fitted (Spurgeon, Charles, E., 2009).

The VMA address is created by combining the least significant bits of each source IP address and MAC address. An original MAC address and an IP address are transferred to the outer side of the LAN, which provide precise source addresses for the data that are being transmitted. The transparency and visibility between the two points of the connection help to prevent unauthorized modifications of the source MAC and IP address pairs and prevents anonymous attacks. For instance, a DoS attack such example defines the source of the starting attack points by providing the original source MAC address and the private IP address (Mirkovic, Jelena, 2004). The link between the original MAC source and the private IP address source is critical in providing security and aids in the clear identification of the other party's connection. The DHCP server may assign a different Layer 3 IP address to a single network node each time it is attached to the network (Strebe, Matthew, 2006), even though the node and its MAC address remain the same. Visibility plays a main role in security, as even the dynamic IP address may change and may not be guided to the right attack node. Visibility can provide a Layer 2 source MAC address directed at the precise network machine that began the event. Thus, visibility can identify the source that is using the addresses of the two layers.

The proposed VMA address uses the existing size of the MAC address 48-bit to fit the source hardware address field and to avoid break the standard. The VMA address also provides advantages such as avoiding the creation of a non-standard Ethernet frame format. Avoiding the difficulties of adopting a new scheme entails fresh efforts and additional costs. Each router in the network path must follow the new procedure when re-encapsulating the arrived frame to resend it instead of following the current procedure included in a current router's MAC address. This procedure maintains the travel of the VMA through the networks until it arrives at the destination node.

3. The VMA Construction Mechanism:

The VMA is entered into the 48-bit source hardware address field. The six-byte length of the MAC address is divided into two three-byte lengths. The first three least significant bytes from the source IP address replace the first three least significant bytes in the source hardware address field, whereas the first three least significant bytes from the source MAC address replace the last three most significant bytes in the source hardware address field. In other words, the 48-bit VMA is constructed when the first three least significant bytes from the source IP address replace the first three least significant bytes. The last three most significant bytes from the 48-bit VMA replace the first three least significant bytes in the source MAC address (as shown in Fig. 1).

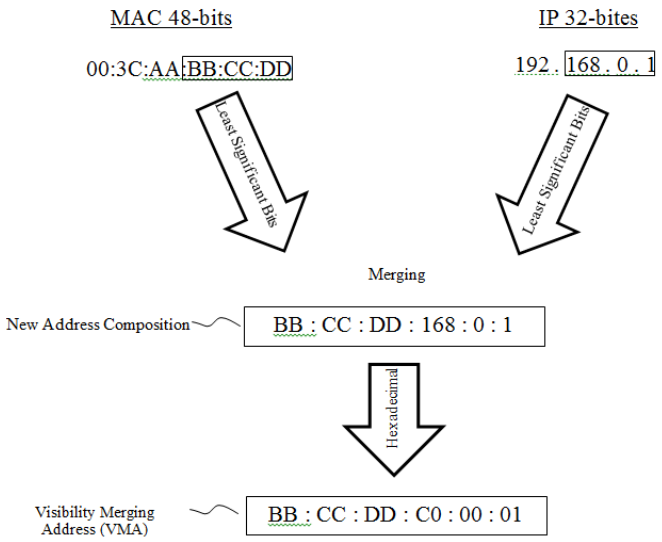


Fig. 1: Generation Mechanism for the Visibility Merging Address (VMA).

However, revealing the source's private IP address and MAC address may not be desirable in most cases. Thus, the sending process can proceed without enabling the VMA and providing the source hardware address containing a VMA in the frame header; the process may maintain the proposed scheme by providing the source IP address in the source hardware address field. In the destination MAC address, the most significant bits are occasionally used to indicate broadcast station. A broadcast station that checks or uses the source MAC address in the source hardware address field is available; in other words, a broadcast address is not used in the source hardware field of the Ethernet frame header. The VMA address in the proposed scheme uses the source hardware address field in the Ethernet frame as a carrier. To recognize whether the VMA address has been utilized or not, the last most significant byte included in the broadcast bits in the VMA address is examined. If this byte is used, the VMA address was utilized.

After converting the source IP address into the hexadecimal form, take the first three octets (the least significant bits) to be the first three octets from the VMA address. Taking the last three octets from the original MAC address (the most significant bits) to take the last three octets position from the VMA address that is want to be construct. The VMA address will carry in the destination hardware address field in Ethernet frame header.

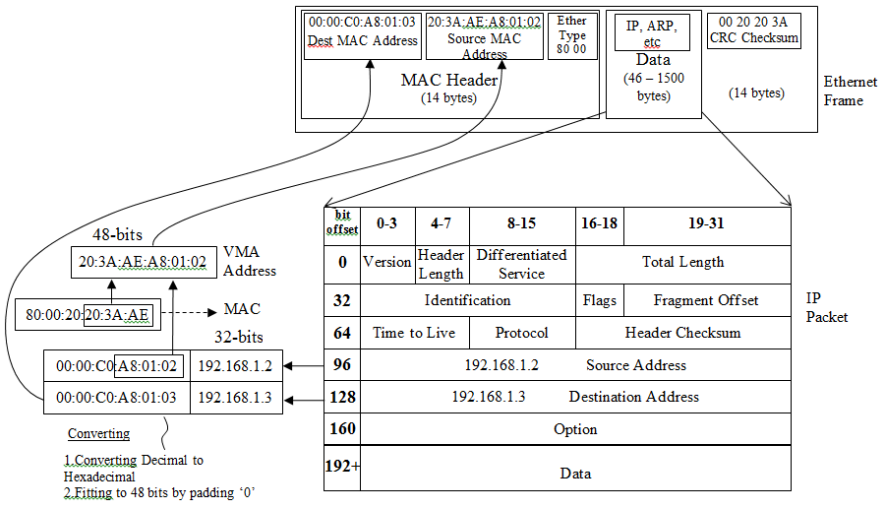


Fig. 2: Ethernet Frame with VMA for the Proposed Visibility Architecture.

3. Visibility Architecture:

The transmission of a Layer 2 MAC address to the outer side of the LAN to reach the second end of the connection on the WAN side is proposed. This proposal considers the necessary level of Internet visibility. The transfer of the MAC address outside the LAN has not been proposed previously because the MAC address is typically used to guide Ethernet frame travel within the LAN; thus, the MAC address does not exit its LAN. The

transfer of the original MAC address from one network to another using the source hardware address field in the Ethernet frame is proposed in this study. The source hardware address field no longer plays a main role given the previous description of the new Layer 2 transmission mechanism. Therefore, a new concept is introduced to utilize the source hardware address field to carry the information regarding the original MAC and IP address source. In the current scheme, the online destination IP address travels through the networks in a packet until it arrives at the target network node. The source IP address in the packet does not change if it is a public IP address type. If the source IP is a private IP address, it changes at the next router in the NAT process.

In this approach, the source hardware address in the Ethernet frame remains fixed until it reaches the end of the connection along with the destination IP address fields in the packet. As the destination MAC address in the Ethernet frame header changes, each hop obtains the value of the next destination. The destination IP address is used as a destination address for Layer 2 in the next hop instead of the destination MAC address in the current scheme, as previously described, on the condition that the content of the source hardware address is maintained without changing the visibility of the merging VMA with each intermediate node. This process has a significant effect on the private network, especially on the NAT function.

In terms of security, the visibility helps to identify attacks. Therefore, the visibility concept has a significant effect on the enhancement of network security, especially with elements, such as the MAC address and the original source private IP address, that are not revealed to the outside LAN. Visibility does not introduce any additional complexity to the naming system. The only amendments made are to the contents of the Ethernet frame header fields. This mechanism includes encapsulation with the new VMA concept. The size of the frame header field is also unaffected because the proposed VMA fits the 48-bit source hardware address.

In the proposed scheme, the source hardware address field in the Ethernet frame header is proposed as a carrier of information to the WAN side to provide the original source MAC and IP address. This information is viewed as a VMA that consists of a combination of part of the source MAC address and part of the IP address that conveys the 48-bit standard source hardware address field. All of the information for the original source MAC address is removed at the first router gateway and a new Layer 2 header is added because the Ethernet frame is used within the LAN. The IP and MAC addresses in the outgoing packet/frame from the router do not provide any information regarding the original source MAC address used in the frame. The Layer 2 encapsulation typically carries information only within the LAN. In the network node procedure, the Ethernet frame in each delivered node is de-capsulated and re-encapsulated with the new control information. In the current procedure, the routers do not allow the source MAC address to cross to another communication end point. The routers also do not allow the end points to know the original source of the private IP and MAC addresses. Each intermediate node removes the Layer 2 information and re-capsulate the information with its MAC address as a source address. As shown in Fig. 6, how a sending and receiving in the visibility was enabled with a Private IP Address and NATing in the proposed naming architecture. In private IP networks, the router has a NAT that removes the original source private IP address in the packet. Therefore, the maintenance of the source hardware address field in the Ethernet frame header, which contains an address generated by the merging of parts of the MAC and IP addresses in the source node, is proposed. In this approach, the intermediate routers do not change the parameters of the source hardware address field. In the intermediate router, the Ethernet frame is de-capsulated and then re-encapsulated on the condition that the VMA address remains unchanged and is resent to the next node.

As a result of this approach, visibility on the Internet is provided to the original Layer 2 device address and the Layer 3 private IP address. Therefore, the original MAC and IP address link is provided with protection to avoid unauthorized changes.

The destination hardware address field is examined to determine whether the delivered frame is for the right node or not because the IP address is used as a source and destination address instead of the MAC address in Layer 2, as described in the proposal. The flowcharts describing sending and receiving procedures are shown in Fig. 3, and Fig. 4.

In this approach, the reply of the network node to the source of the delivered frames is dependent on the source IP address field in the packet to construct the frame using the MAC address that was generated from the source IP address. This mechanism traditionally enters the source MAC address into the source hardware address field in the frame, and the reply uses the source hardware address as the destination address in the new frame. The algorithm used to generate the Layer 2 MAC address based on the source IP address in the header of the delivered packet shown as flowcharts as following.

The generated MAC address is used as a Layer 2 destination address and includes the constructed frame to be sent. As previously mentioned the procedure does not use the ARP cache table but depends only on the Layer 3 IP address as a flat address to guide the frame in Layer 2 transmission (Alzubaidi, Waleed Kh, 2012). The source hardware address field in the Ethernet frame header does not play a role at present because the source IP address is used as a reference in case the reply message requires knowledge regarding the source of the delivered frame.

Visibility also provides security advantages. In the event that a server is susceptible to any type of attack (such as Distributed Denial of Service or DDoS), the exact source of each delivered packet is easily determined. Thus, the identity of any anonymous attacker can be revealed as seen the description for the visibility architecture in Fig. 5.

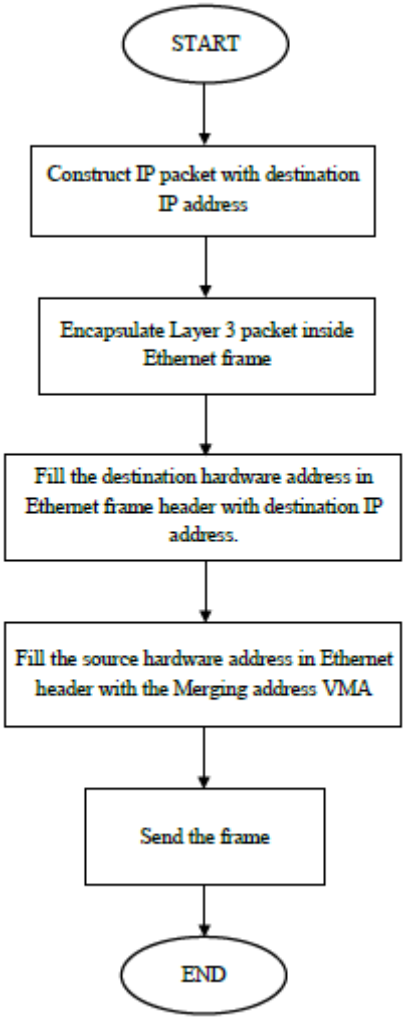


Fig. 3: Flowchart Sending data with Visibility enabled.

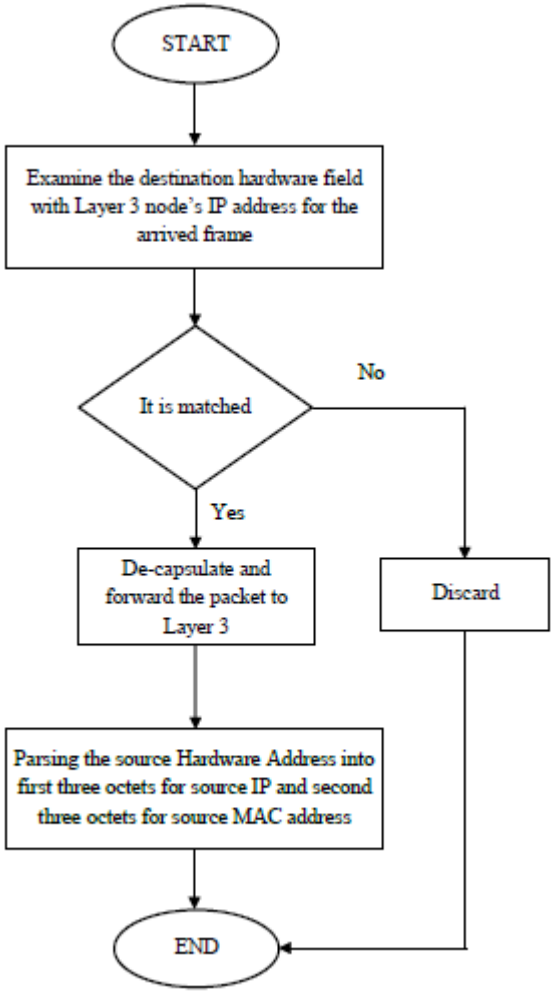


Fig. 4: Flowchart Receiving data with Visibility enabled.

4. Conclusions:

A new Internet visibility architecture is presented to enhance the security level by raising the Ethernet working level to match the WAN side. A visibility mechanism is proposed to provide the private IP and MAC addresses to the WAN side of the network. The private IP address is generally hidden behind the NAT in the router. In the proposed architecture, the private IP address is revealed to the second end node in the communication. This visibility causes the Internet to become more visible and to be easily tracked. The visibility also eliminates Internet attacks such as anonymous and DDoS attacks. The limitation is in the scope of this study, the current visibility concept is presented under the Ethernet protocol. This concept can also be applied to Layer 2 WAN protocols and provides visibility to for all of the architectures in the LAN and WAN networks. The application of the visibility concept to ATM and frame relay as WAN protocol examples may require further study. The influence of the proposed architecture and its effectiveness in terms of Internet visibility are theoretical evaluated.

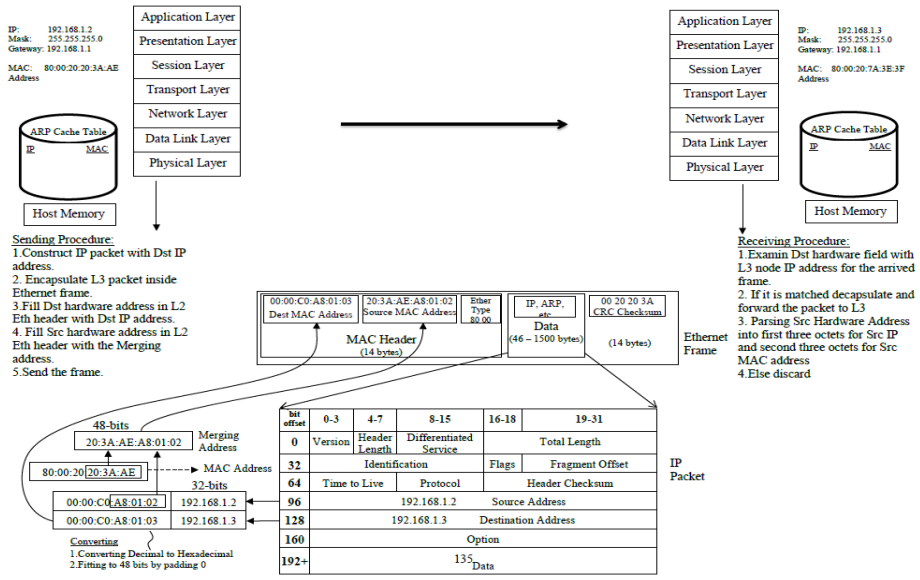
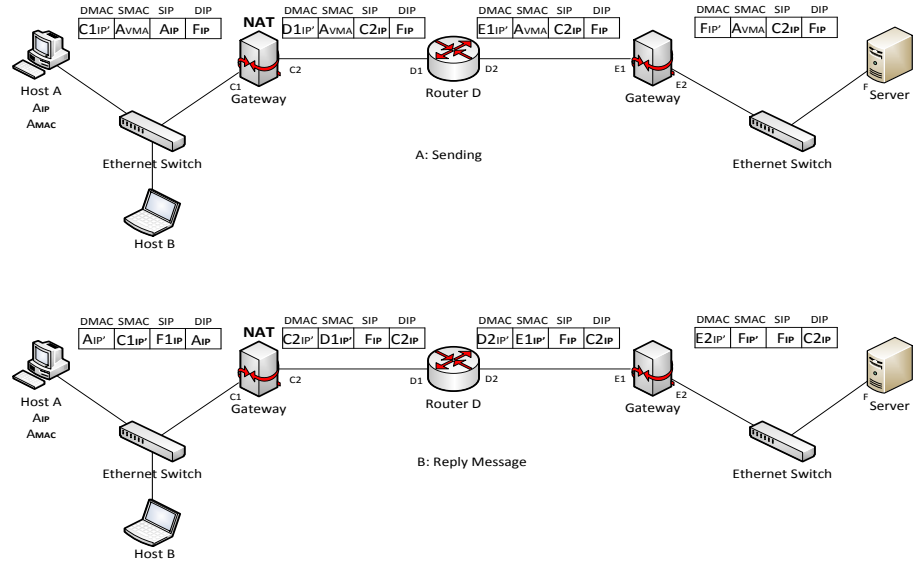


Fig 5: Ethernet Frame with VMA for the Proposed Visibility Architecture.



Visibility Merging Address (VMA) = First three leased significant bytes of MAC address + First three leased significant bytes from IP address
DMAC: Destination Hardware Address Field in the frame header SIP: Source IP address field in the Packet Header
SMAC: Source Hardware Address Field in the frame header DIP: Destination IP Address Field in the Packet Header
IP': The 48bits Address that derived from the Origen 32bit IP Address from Layer 3 and used Instead MAC address

Fig. 6: Visibility Enabled with a Private IP Address and NATing in the Proposed Naming Architecture.

REFERENCES

Alzubaidi, Waleed Kh, Cai, Longzheng, Alyawer, A. Shaymaa, 2012. Enhance the Security and Performance of IP over Ethernet Networks by Reduction the Naming System Design. International Journal of Computer Networks (IJCN), 4(5).

Alzubaidi, Waleed Kh, Cai, Longzheng, Alyawer, A. Shaymaa, 2012. A New Verification Method to Prevent Security Threads of Unsolicited Message in IP Over Ethernet Networks. International Journal, 4.

Alzubaidi, Waleed Kh, Cai, Longzheng, Alyawer, A. Shaymaa, 2012. A Framework for Optimizing IP over Ethernet Naming System. International Journal of Computer Science Issues(IJCSI), 9(6).

Forouzan, Behrouz A., 2002. TCP/IP protocol suite: McGraw-Hill, Inc.

Hayawi, Kadhim, Al Braiki, Arwa, Mathew, Sujith Samuel, 2012. Network Attacks and Defenses: A Hands-on Approach: CRC Press.

Kiravuo, Timo, Sarela, M., Manner, Jukka, A Survey of Ethernet LAN Security.

Mirkovic, Jelena, Dietrich, Sven, Dittrich, David, Reiher, Peter, 2004. Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security): Prentice Hall PTR.

Plummer, C. David, 1982. RFC 826: An ethernet address resolution protocol. InterNet Network Working Group.

Postel, Jon, 1981. Internet protocol.

Spurgeon, Charles, E., 2009. Ethernet: the definitive guide: O'Reilly.

Strebe, Matthew, 2006. Windows 2000 server 24seven: Wiley.

Wulf, Volker, Hartmann, Anja, 1993. The Ambivalence of Network Visibility in an Organizational Context. Paper presented at the NetWORKing.