A Framework for Optimizing IP over Ethernet Naming System

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

[1] Information Technology Department
University of Tun Abdul Razaq
Selangor, 46150, Malaysia

[2] University of Unitar International
Selangor, 46150, Malaysia

[3] Computer Science Department
Baghdad College
Baghdad, 645, Iraq

Abstract

Due to the rapid expansion of the technology field. Developing the Internet has become more urgent to meet the needs of the expansion. TCP/IP is the most protocol used in the Internet. It consists from layers, Each layer done its job separately. However these layers susceptible to different attacks and data link layer one of the most layers targeted by attacker, Attack at lower layer may lead to more sophisticated attacks to upper layers like Man in The Middle (MiTM), DNS spoofing and Denial of Service (DoS). Even with encrypted protocols such as HTTPS and SSL. In this paper we discuss security at the Data Link Layer and the attacks depend on the Address resolution protocol (ARP). Moreover proposed an approach to prevent address resolution protocol attacks, finally, we conclude at section 5.

Keywords: *IP protocol, Ethernet, ARP protocol, MAC address.*

1. Introduction

As OSI Model, Network stack consists of seven layers. Each layer do its job separately and pass the Datagram to next layer until reach to lower layer been the packet is complete at network layer and ready to encapsulate in the Ethernet frame at Data Link Layer. At Network Layer packet should be created and need to addressed with destination IP address after that Packet encapsulated inside Ethernet Frame to transmit physically to another host within Local area network. At this level of network stack we see there are two addressing system IP address with packet and MAC address at Data Link Layer to address Ethernet Frame. However IP address used to guide packet to the end point like a website and MAC address used in delivering Frame to the host inside local network. However, these two addressing system need a mechanism to binding between them. If the destination outside the network router, gateway MAC address will be used to direct the frame, and in each hop destination MAC address will change to next router address. Here the MAC address used as temporary address while IP address stay without change until reach to the right destination.

2. ARP Overview

In local area network, the Address Resolution Protocol (ARP) [1] is used to map IP address to MAC address. To construct and transmit Ethernet frame in IP over Ethernet networks, destination MAC address should be obtained by source machine by using a destination IP address. This task performed by ARP protocol by broadcast request for mapping IP to MAC address and store reply in a memory space called ARP cache table. ARP works as follows: an application attempts to send data to an IP address of a machine. IP packet will be created by the network stack, and then encapsulated inside Ethernet Frame. For transmission this frame, it needs the destination MAC address. Therefore, the network stack checks the IP in the ARP cache table to find the destination MAC address. If it is not there, then broadcast ARP request on the network. Each machine in the network will examine the ARP request and check if they own the requested IP. The machine that owns this IP will create ARP reply containing their MAC address. Then, send unicast reply to the originator of this request. The originator will use this address in destination MAC address field to complete the frame and transmit it. ARP is a simple statelessness protocol.

ARP is layer 3 protocol. It does not design to have any security aspects to bind IP and MAC address. ARP not designs to resolve IP address from outside the LAN.

Network device will determine whether the destination is inside or outside the network by comparing subnet with its target's IP address, if it is outside, then it need to construct a frame with corresponding default gateway router as a destination. Each network host makes maintenance for ARP cache to store IP with its corresponding MAC address. ARP cache may contain dynamic and static entries or one of them. Dynamic entries in the cache are added and remove automatically, depending on the time. ARP cache entry expires in two minutes under Windows 2K, and can be renewed up to a 10 minutes maximum while referenced in outgoing frames. Linux expire entries after one minute. These parameters are defaults and configurable per network device. While static entries remain in the cache table until the host reboot. Note this simple protocol does not have any type of security to bind IP to MAC, Leading to serious insecurity. For instance, the ARP poisoning attack uses unsolicited ARP reply message. Network devices can not verify the ARP sender and if it come from right device or not. ARP does not provide any security measures. However, it is based on broadcast messages on the LAN. ARP message is included inside Data field of Layer 2 Ethernet frame. The Ethernet type field set to 0x0806 indicating to ARP message inside. There are a couple of special cases of ARP requests replies that do not work as described above: proxy ARP and gratuitous ARP. Proxy ARP [2] was designed to allow seamless implementation of transparent subnet gateways. Using proxy ARP, a host can contact another host on the other side of a router, even if the original host does not have a default gateway configured. The basic idea is that the router is configured to reply to ARP requests on behalf of the hosts on the other side of the router. When the original host receives the reply, it is not aware that the MAC address it is receiving does not belong to the destination host, but to the interface of the router on the current network. Gratuitous ARP is unsolicited ARP messages sent by hosts, directed to their own IP addresses. Hosts commonly use this type of messages when joining a network with a dynamically assigned IP address. These hosts use gratuitous ARP to confirm that the newly assigned IP address is not currently in use by another host in the network.

Moreover, a host broadcast a gratuitous ARP when it is initializing its IP stack. The gratuitous ARP is an ARP request message to verify there is no conflict IP address. By gratuitous ARP, the host asks for Layer 2 address of its own IP address.

2.1 ARP Problem

ARP introduces a security risk to Data link layer, since ARP messages can easily be spoofed. Attacker can apply a serious attack like Man-In-The-Middle and MAC flooding. An attacker can send forged ARP message to host within local network to redirect traffic that going to gateway router or another peer host to rogue that network device. This is the Man in the Middle attack. Whereas in flooding attack, the attacker sends a spoof ARP replies to the switch to overflow the buffer of CAM table where store MAC addresses and corresponding switch port number and VLAN. Depending on switch setting and capacity some switches goes to Hub mode then broadcast the frames into all ports allowing sniffing. there is another possible attacks on the Data Link Layer, Like MAC cloning, Hijacking, Denial of service (DoS) and broadcasting[].In Denial of service, Attacker poisoning victim's ARP cache table, by sending a forged ARP message with IP of the gateway as an example and nonexistence MAC address. In this case victim cannot connect with the destination. attacker may be cheat switch CAM table to enable Denial of Service, by sending forged frame with source MAC address of the victim so any frame send to victim switch will forward it to port of attacker. One of the recommended actions against ARP attacks is applying static ARP entries in cache table. Apply it will be prevents most of the attacker. But it is impractical, because each new host machine administrator should update ARP table in all other machines or when new network interface card NIC is replaced, and does not allow utilizing from Dynamic Host configuration Protocol DHCP. In addition, most operating systems updates its ARP table when receive a gratuitous ARP even with static entries. Lastly, it does not solve the binding issue problem for IP and MAC address.

We observed a core problems related to link layer that causes vulnerabilities and creating an overhead.

First, there is no secure mapping between IP and MAC addresses. Due to that there are several possible ARP attacks on the Data Link Layer. In fact, the main cause for the problem is the naming architecture, and it is not fail from ARP. ARP is a protocol design to work with exist naming architecture used in the network stack. May be considering the naming architecture is the main reason for these issues. Ideally, a host should not have its identity tied to another address type. Instead there should be a naming architecture to identify host with one address type, without need to tie with MAC address. Another possible solution should be a mechanism to verify ARP sender and to confirm there is no conflict binding IP to MAC address.

Second, the constantly mapping IP to MAC address introduce an overhead. In IP over Ethernet networks, after the device initiated its network stack, it is identify its self with MAC as Layer 2 address, and establishes its IP address as layer 3 address. MAC address used to identify network device in local network. However, more efficient naming architecture may able to use one addressing type after initiation its network stack. So no more constantly mapping needed. Using only IP address to identify the host,

and use it as a destination address in sending Ethernet frame to the target node. Like this new naming architecture may requires a change in layer 2 architecture. However, more advantages gained by satisfying optimization in the process of the layer and enhance network resources. In this case there is no need for mapping processes. Still network devices like bridges and switches need to maintain table for IP and their ports.

3. Addressing the Compatibility Problems between IP and Ethernet Protocols

Ethernet protocol and IP protocol each one has a special naming system. This naming system is jointing when IP protocol is working over Ethernet protocol. However, Make this jointing without any considerations to reduce the design and make one union naming system instead two will cause in result a many weak points.

To address the compatibility problems between network layer and data link layer in IP over Ethernet networks, one solution is to utilize a naming architecture that uses one addressing system type. In literature, there are many researches in trying to modify current naming architecture to use one addressing naming system. For instance, in [3] try to find alternative mechanism instead using layer 2 MAC address. While in [4] try to put a mechanism for Internet without using Internet protocol (layer 3) address. However, it is hard to implement such this proposed methods without creating services disruption. We found in practically it is difficult to use only one address with entire architecture that used two different protocols, IP and Ethernet protocols. Each one of these two protocols types has a different circumstances and each one work with different way and designed for different layers and purposes. But we found it is possible to apply one naming system partially in current IP over Ethernet architecture, by applying new concepts to satisfy a reduction. This reduction will be creating an enhancing in two direction performance and security. In the security side, one of the most important points in naming architecture is to prevent redirect network traffic that currently done anonymously without any sense if the attack was enabled.

Another possible approach to solve compatibility problem is to authenticate who should access to the network, that what proposed by IEEE 802.1X. Approach like IEEE 802.1X is authenticating to access network resources, by using EAPOL allowing only who authorized to attach to the network.

In the network, there are many data traffic types, unicast, multicast and broadcast. Unicast is the most important traffic type, that because it used with establishing the connection and start exchange data within two network nodes in the LAN or WAN. While multicast and broadcast used when node desired to spread data to more than one destination. Therefore, unicast traffic performance and security will effect directly on the performance and security of the network in overall. In our thesis, we are targeting a layer 2 unicast traffic mechanism to provide a significant enhancement to the network. Moreover, we will explain how can utilize IP address in layer 2 unicast as one flat address for layer 3 and layer 2 network stack.

One step toward the solution is making Layer 2 and Layer 3 is more close and compatible state. And that can be achieve by first, reducing mapping process between layer 3 IP address to layer 2 MAC address that performed by ARP protocol. Second, accomplish Layer 2 unicast data transfer using only Layer 3 IP address. That will be leading to reduce the performance and security problems without directly effect on current IP over Ethernet naming architecture. This approach also reduces the time and resources that spent to sending a piece of information through the network. In result, making a significant enhancement in the performance. For instant, reducing the use of ARP protocol from mapping from layer 2 unicast traffic, will offer more speed by direct sending the information without any prior process. Moreover, optimizing the transmission mechanism by reducing the parts that used by attacker in Layer 2, will provide an enhancements in the security. However, this method will not provide a comprehensive solution for Layer 2 performance and security problems.

Layer 2 was designed without providing security aspects; therefore, we consider revising and enhancing the design of the naming architecture is the recommended method to recover the shortcomings. Rather than proposed a new scheme and attach it to the traditional one, will produce a complexity and unforeseen problems plus break the standard. The traditional mechanism of ARP is not successfully work with the current transmission procedure. We consider it an extra step and overload on the performance, and used as vulnerability points exploit by the attacker. Then again, cancel the use of MAC address completely and depend on IP address only to accomplish data transmission in Layer 2 and Layer 3 is not practical. Instead, cancel the use of MAC address partially from Layer 2 data traffic is possible, and will create an optimization on the naming architecture.

3.1 The Relation between making an Optimization by Reduction in Naming Architecture Design with Performance and Security Enhancement

Low level layers on OSI network model have the responsibilities of the transferring data. Therefore,

enhancing the performance in these levels will totally affect on upper layers by raising the connection speed and offer availability and reliability. The performance for layers depends on each other. For instance any fail in one layer will affect directly on the other layers in performance and security. That makes clearly the data link layer connection quality have a direct effect on the speed and the quality of the upper layer services. For instance, ICMP protocol from layer 3 will affect directly by cancel the use of ARP protocol from delivery mechanism in layer 2. In result, making an optimization in layer 2 will make ICMP protocol work better, faster reply and more reliable in result. Each layer offers its services with independent performance level from other layers, and performance in one layer may provide a sufficient level of integrity and speed to satisfying the connection circumstances. However, this scheme shows that the performance level in one layer will accumulate to other layers in result effect on the connection quality. That means the problem that start from lower layer increases linearly toward upper layer. That will enhance the services quality when optimization is happened in lower layers. In other hand, enhancing the performance in one layer will effect surly on the quality of service. While in the security side each layer provides the security individually, and the security that provided in one layer may provide a sufficient level. For instance, HTTPS protocol in application layer often provides a sufficient security for privacy of the data. Despite that, this is will not prevent to make a performance and security problems during datagram passing through data link layer. Moreover, many recent researches proof that even used HTTPS protocol in upper layers to protect the data still it is not safe and possible to attacks on low level layer by one of the MiTM techniques. For example, cutting the connection in layer 2 even using HTTPS protocol, that will protect the privacy of the sensitive information, but cannot avoid cutting the services in lower layers. And reduce the risk of redirect traffic that used mapping process between Layer 3 and Layer 2 addresses. We believe that unifying addressing in current naming architecture is necessary to improve network performance and security in the Internet.
We believe that a more optimization for the current design is needed to create a comprehensive and reliable solution. Moreover, the fast developments in Internet and various services provided by application layer it makes not recommended to add a more complexity by adding extra security mechanism. That can be achieved by revise and reduce the design of the naming architecture in IP over Ethernet networks. We proposed to reduce layer 2 transmit mechanism making data transfer without mapping process in unicast traffic. That to reduce the latency time for data transfers, and reduce the risk of enabling serious attacks by using mapping process.

4. Architecture Concepts

We found five main concepts to achieve an optimized naming architecture in IP over Ethernet networks. We will overview these concepts. These concepts are envisioned as a performance and security optimization in a reference diagram as shown in Figure 1.

4.1 One Flat Address for Layer 2 and Layer 3

We propose a new flat address concept where Layer 2 and Layer 3 depend on one address type form. Our approach is aimed to make one flat address between Layer 2 and Layer 3 in IP over Ethernet networks. We believe that unifying naming system in IP over Ethernet network and make it use one address form is necessary to enhance the network performance and security services in the Internet. We choose to utilize IP address as guided address represent in Ethernet frame header in Layer 2 instead of using MAC address. By making layer 3 IP address is available for layer 2 unicast traffic, and use IP address instead Layer 2 MAC address in the Ethernet frame header. Unifying naming system made IP address available in both Layer 3 packets and layer 2 frames at the same time. Our main motivation behind unifying naming system concept is to create an optimization stat in naming architecture in IP over Ethernet networks, in result, enhancing the performance and the security.
We argue that the naming system in IP over Ethernet networks should use a one naming address system with current scheme instead two, IP and MAC addresses. Avoiding by that the complexity in the naming architecture, and it is considered essential to satisfy a successful solution and offer easy adoption. Optimizing current naming architecture by make a reduction in data delivery mechanism is promising method comparing with other methodologies that added a new mechanism to the current used architecture. That will be preventing to produce any unforeseen fails or shortcomings in the performance and security in the new architecture.

4.2 Cancel the Use of MAC Address

We proposed to make IP Protocol can work over Ethernet without depending on layer 2 MAC address to accomplish delivery data, and using only layer 3 address to guide layer 2 Ethernet frame to reach to the destination. Cancelling the use of MAC address from all naming architecture in IP over Ethernet networks is not practically. We found that is

possible with layer 2 unicast traffic, but still there are many layer 2 services depend on using MAC address. For instance, getting the dynamic address is still need to introduce the MAC address.

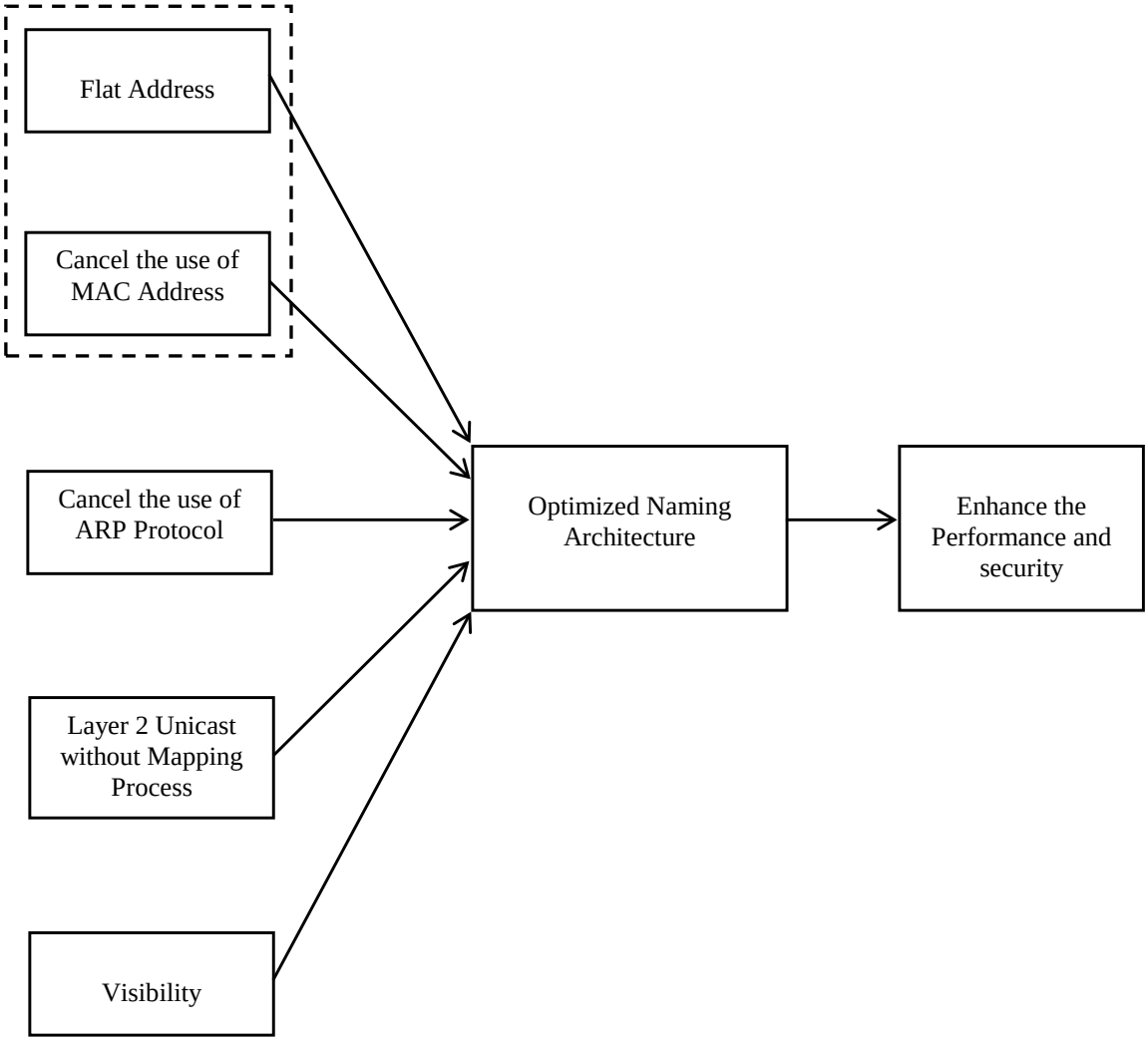

Figure 1: A simple flow diagram for the new concepts to generate an optimizing naming architecture

4.3 Cancel the Use of ARP Protocol

We introduce a new concept to cancel the use of ARP protocol in Layer 2 unicast traffic to support enhancing the performance and security in Layer 2. In result, allowing for various upper layers protocols to work on reliable mechanism of layer 2 delivery frame mechanism. Canceling the use of ARP protocol completely from all naming architecture is not practical, because ARP protocol provide different services to the network. Moreover, there are many activities in the network depend on ARP mapping between layer 2 and layer 3 addresses. For instance, host still need to submit its MAC address to the Dynamic Host Configuration Protocol DHCP server to get a dynamic IP address. Therefore, using ARP is necessary to discover the neighbors and network services that offered, and then request it from network server. Moreover, detecting the conflict IP address in IP over Ethernet networks is one of the ARP responsibilities (by using Gratuitous ARP). The new circumstance for ARP cache table like cancellations of building and maintaining

cache table, and memory spaces that released and save due to the above are need a consideration also.

4.4 Layer 2 Unicast Traffic without Mapping Process

Layer 2 unicast traffic is used to transfer the data and exchange control information between two points in the network. Moreover, security protocol mostly uses a unicast connection. Thus, layer 2 unicast traffic is considering the most active connection type than Broadcast and Multicast. We found that cancelation mapping address from unicast is possible. Therefore, Layer 2 traffic under our new concepts will divide into two categories: First, unicast traffic without mapping process to enhance the performance and avoid fake mapping that uses to redirect data traffic. Second, all others traffic types like Broadcast and Multicast traffic will stay use current scheme with two addresses IP and MAC address to accomplish network activities. Layer 2 unicast sending and receiving procedures under the new scheme are need for modify. Cancelation mapping process from unicast connection may create a fast efficient layer 2 connection speed, and reduce layer 2 data loose due to weak connection. Moreover, the enhancing by unicast without mapping will inherent to the wireless connection. And enhance the delay time or latency time that was spent on mapping between layers addresses.

4.5 The Visibility Concept

We propose to transmit a layer 2 MAC address to outside of the LAN to reach the second end of the connection providing by that a necessary level of the visibility. Transferring MAC address outside LAN is not proposed before that because usually MAC address used to guide Ethernet frame travel within Local Area Network LAN, therefore, it is not going outside of its LAN. Here we are proposing to transfer original MAC address from network to another network using source hardware address field in Ethernet frame. After we described in previous the new mechanism to layer 2 transmissions, source hardware address field now have no main role. Therefore, we introduce a new concept to utilize source hardware address field to carry information about source original MAC and IP address. In our approach, the source hardware address in layer 2 Ethernet frame header and source and destination IP addresses fields in layer 3 packet header will stay fixed without change until reaching to the destination, while the destination MAC address will change with each hop. Instead destination MAC address in current scheme, there will be a destination IP address used as destination address for layer 2 next hop.

5. Conclusions

We analyzed Data Link Layer performance and security problems, and found it is not the fault of ARP protocol. The problem is in the design of the naming architecture in IP over Ethernet, not in the design and implementation of ARP protocol. We investigated the performance and security problems in the link between Ethernet and IP protocol, and found they are not fully compatible and not designed specifically for each other. We proposed a new naming architecture for IP over Ethernet networks to improve its performance and security. In this architecture, we utilized Layer 3 address as a flat address for both Layer 2 and Layer 3 instead of using fixed media access control (MAC) addresses. In addition, make a reduction on the ARP protocol role and in the design of current naming architecture.

References

[1] Plummer, D. C., “Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware." IETF RFC 826, November 1982.
[2] S. Carl-Mitchell and J. Quarterman. Using ARP to implement transparent subnet gateways, Oct. 1987. RFC 1027.
[3] Hayriye C. Altunbasak, “Layer 2 Security Inter-Layering In Networks,” Thesis dissertation, Georgia Institute of Technology, Dec. 2006.
[4] Craig A. Shue, "A BETTER INTERNET WITHOUT IP ADDRESSES", Thesis dissertation, Indiana University, May 2009.