Enhance the Security and Performance of IP over Ethernet Networks by Reduction the Naming System Design

Waleed Kh. Alzubaidi *waleed@ieee.org*
Information Technology Department
University Tun Abdul Razak
Selangor,46150, Malaysia

Dr. Longzheng Cai *charles_cai@unitar.my*
University Unitar International
Selangor,46150, Malaysia

Shaymaa A. Alyawer *sha_amh@yahoo.com*
Computer Science Department
Baghdad College
Baghdad, 645, Iraq

Abstract

In this research, we investigate the weak link between two protocols, IP protocol and Ethernet protocol. IP over Ethernet network has become the major network used by Internet. In this network, still the data link layer performance and security problems not adequately addressed yet. The findings of this research lead us to propose a modification, by making a reduction on current naming architecture to improve the network performance and security. The proposed architecture will be evaluated by a theoretical analysis.

Keywords: IP, MAC address, Ethernet, ARP, Security, Performance.

1. INTRODUCTION

Despite the Internet is widely adopted and success, still its architecture is far from ideal. The Open System Interconnect (OSI) model divides network functions into layers. Services are provided from lower layers to upper layers without the knowledge of each other. This model provides simplicity in working and flexibility in developing, and allows the changes been made in specific layers without the need of changes in other layers. For instance, when started to developing 802.11b wireless networks, changes were made only in data link layer and physical layer. On the other side, this model allows the performance problems and security flaws of lower layers affect upper layers. For example, the performance effect on resolving layer 2 addresses (MAC address) will delay or prevent connection setup in the network layer. The security weaknesses in data link layer may compromise the whole communication [14]. While there are several ways to enhance the performance and security in upper layers, still the problems in data link layer have not been addressed adequately yet. Although network devices like switches and bridges have provided some performance enhancements and security features, problems are still there. The design of the current naming architecture in IP over Ethernet networks that use to deliver the data within Local Area Network was not enhanced since it was founded. The current design is not ideal [1], and need be revised to make it more effective and secure. In this research, we will focus on improve performance and security in the data link layer of IP over Ethernet networks.

Data link layer is the last layer before the data is converted to physical signal. The network traffic at this layer considers a complete traffic. It contains data that want to be sent and the control information which include destination and source addresses (IP, MAC), protocol type and port

number, etc. That means any problem in data link layer may lead to more sophisticated problems in performance and security issues in the upper layer.

We found several performance and security problems in data link layer were generated due to using the current naming architecture in IP over Ethernet networks. This architecture used to accomplished data transfer inside the local area networks, and it consider one of the requirements for binding network layer address and data link layer address.

First, current naming architecture uses two different address forms, which introduces an overhead by constantly mapping between IP and MAC address.

Second, the mapping process is considering an extra process added to current data transmission procedure. This considers a delay issue when data been stored and not sent until the address resolving processes complete.

Third, Performance problems and security issues in data link layer may not be able to reduce or avoid it in the upper layers. The performance problem in data link layer has a direct effect on the whole communication, and upper layers cannot provide a solution. Therefore, it is better solve these problems from the base of the ISO model. However, a more efficient naming architecture may able to use one addressing type after initiation network stack, so no more constantly mapping needed. We can use only IP address to identify a host, and use it as a destination address in sending Ethernet frame to the target node. This new naming architecture may require a change in current naming architecture in Ethernet networks. Still network devices like bridges and switches need to maintain a table for IP and their ports.

In this study, we research on the weak link between Ethernet and IP protocol, and proposed a compatible-backward modification on current naming architecture to secure the data link layer in IP over Ethernet networks. Moreover, improve the performance by reducing on the address mapping in the data transmission process. This new proposed solution will be evaluated by theoretical analysis.

2. LITERATURE REVIEW AND BACKGROUND

2.1 ARP Overview

In the local area network, the Address Resolution Protocol (ARP) 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 a 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. Also ARP considers a layer 3 protocol. It does not design to have any security aspects to bind IP and MAC address.

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[9].As shown in Figure 1.a.

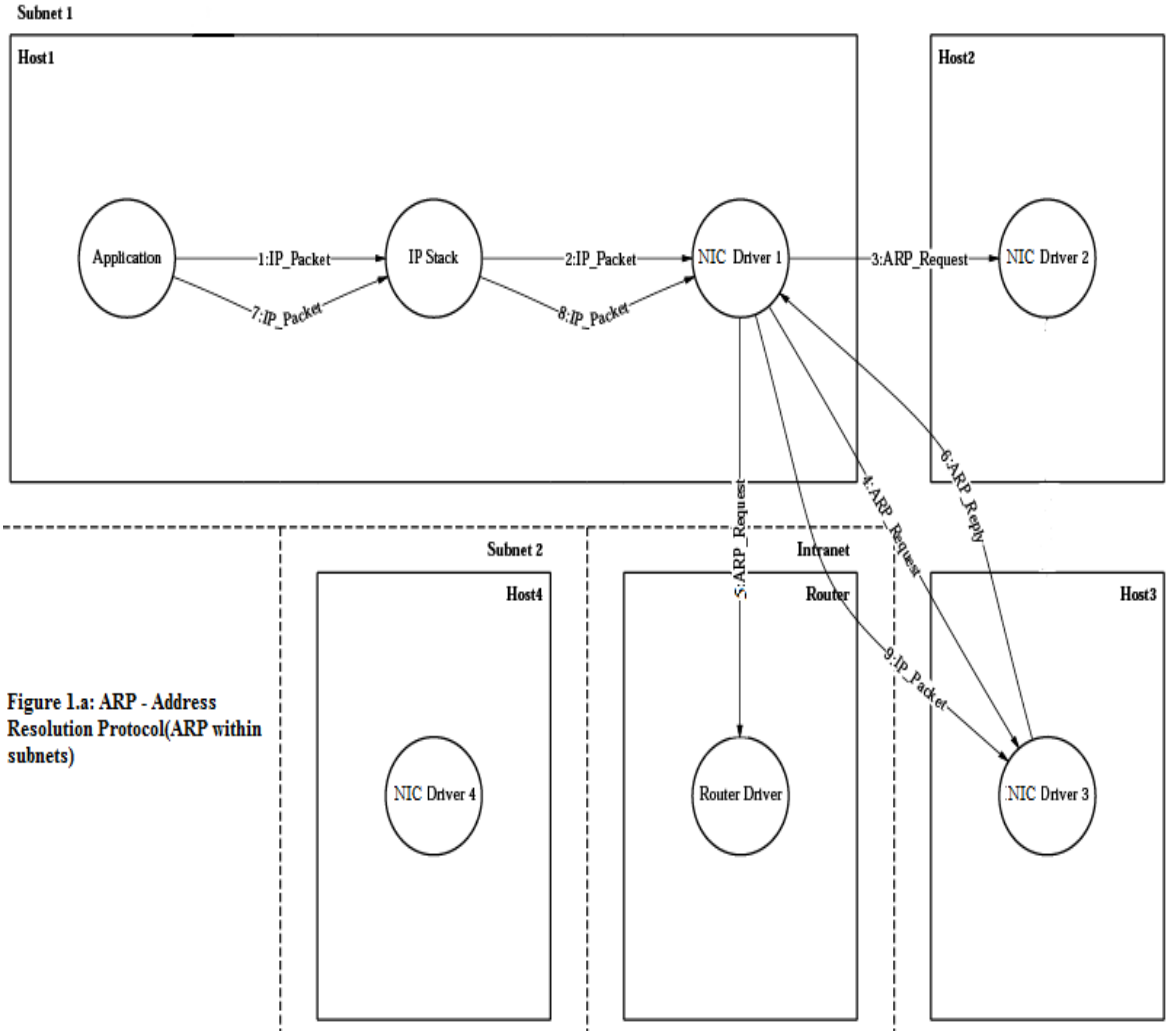

Figure 1.a: ARP - Address Resolution Protocol(ARP within subnets)

3. Analysis of Data Link Layer Performance

Current naming architecture in IP over Ethernet networks has many performance problems. To start Layer 2 communication, system will create IP packet at Layer 3 and it will be encapsulated at Layer 2 inside Ethernet frame. Before the system sends this frame it needs the destination hardware address (MAC address). System will do ARP request and queue the information until resolving the destination address. In the next step and if the remote host is reachable will return ARP reply message with its MAC address. Local system will be including this MAC address in the Ethernet frame header then send it. The remote host will receive and de-capsulate the frame and proceed the datagram to the upper layer. To explain the performance problems in data link layer and make it more clear, let suppose we have two computers. Local computer want to check remote computer is alive or not. Figure 2.1 show the procedure of checking remote host with ping program. Ping program is used for checking, and it will generate ICMP packet at layer 3 for send it to the remote computer. The system needs the destination hardware address to send this

frame. The system will do ARP request and at the same time queue the ICMP packet until can resolve remote hardware address. Remote computer will receive the request message and return ARP reply with its MAC address. After receiving ARP reply, local computer will encapsulate the ICMP packet inside Ethernet frame and include the destination MAC address in the header of the frame. Remote computer will receive the frame and return ICMP echo reply. Finally, Local computer after receive ICMP reply can determine the remote computer is alive. There are many problems in this mechanism due to use current naming architecture.

First, delay actual Data that want to be send while system queuing it until can be resolve the destination hardware address. The mapping messages susceptible to lose,

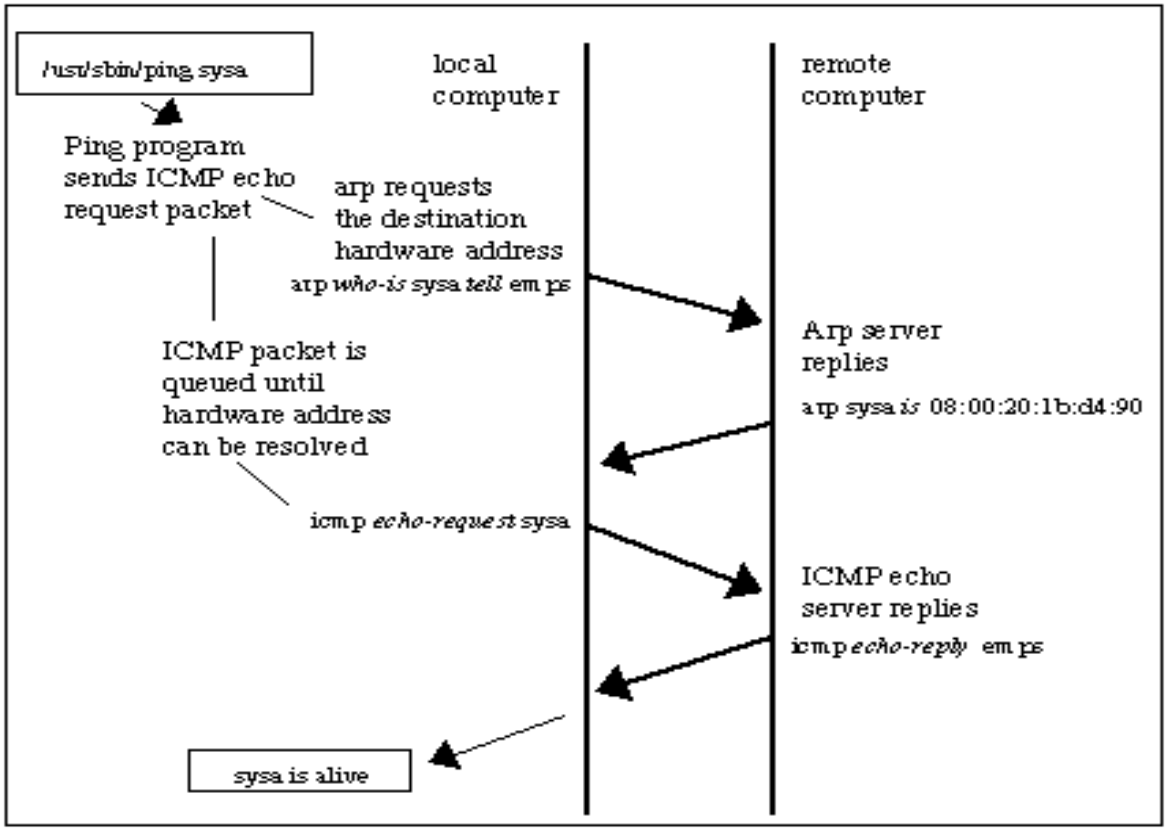

FIGURE 2: Ping program procedure

damage or delay due to media performance or attacks threads. The mapping process considers an extra process that is making data transmission process is heavier and more complex.

Second, in the mechanism of checking whether the remote computer is live or not, it is need four steps to determine. While already we understand the remote is live from the second step, because if the remote is not living so who reply ARP message. Our thesis focuses on these problems, to reduce queue time and to send data directly. Moreover, reduce the procedure to determine remote target is alive or not in two steps instead four. These problems emphasis our theory that the problem in the design of the naming architecture in IP over Ethernet networks.

4. Ethernet and IP protocol Link Security Problems

Data traffic in the data link layer considers a complete traffic. It is including the information that wants to be sent and the control information. The control information include destination and

source IP and MAC address, port number, protocol type, etc. Therefore, controlling data link layer traffic will compromise the whole communication.

Ethernet protocol composes from Media Access Control operations and Ethernet frame structure. Ethernet was not design specifically to work with IP protocol and it is different. But the needed lead to made IP protocol work over Ethernet. The framework of IP protocol work over Ethernet is not fully compatible. This caused a weak link between Ethernet and IP protocol. This weak link appears clearly in data link layer where the joint between IP protocol and Ethernet, by mapping between IP and MAC addresses and encapsulate IP packet inside Ethernet frame. However, the weak link generates gaps that may use to exploit the communication in data link layer.

During these days TCP/IP has become the major protocol that used because the Internet depends on it widely. And Due to vary usage of Internet It is revealing shortcomings. TCP/IP protocol use IP address to identify the host, while Ethernet identify the host by MAC address. Data transfer need to use Ethernet address to deliver Ethernet frame from a network machine to another in the same subnet. The routing in the data link layer depends on upper protocol to deliver frame to the right node. Moreover, Ethernet protocol level needs a resolving mechanism to map the carry protocol address to Ethernet address. Therefore, one of the requirements to made IP work over Ethernet is founding a binding mechanism to bind between IP and MAC address. For instant in IP protocol, Ethernet protocol level need the destination IP address to resolve destination MAC address. Address Resolution Protocol (ARP) was founded to map the IP address to Ethernet address (MAC Address) in the local area network. When a host wants to know the MAC address of the destination IP address, it broadcasts an ARP request including the destination IP address of the target on the network. The nodes that match the IP address in the message return ARP reply with its MAC address. Each node in the network builds a table, called ARP cache, used to store the mapping IP addresses to MAC addresses.

In this section we will discuss attacks behavior and see there is some types depend on mapping process and other depend on MAC address and there is another with different criteria. It is beneficial to understand how layer 2 attacks works and what the dependency points that needs by attack to enable. So we can manipulate these points and can determine what types of attacks will affect by the proposed solution. These dependency points can be targeted in finding an appropriate solution. In our thesis we will focus on attacks that depend mainly on ARP protocol to redirect the traffic. Furthermore, the attacks that depend on the MAC address. The most known Layer 2 attacks are Denial of Service (DoS), Man In The Middle (MITM), MAC spoofing, ARP poisoning, MAC flooding, and port stealing. In Layer 2 based Denial of Service DoS attack, the attacker updates the ARP caches for the network hosts by sending nonexistent MAC addresses. The attacker uses a Layer 2 based DoS attacks to disable layer 2 network connection to the victim and then uses its pair IP and MAC addresses. Each network interface card in the network is supposed to have a globally unique MAC address[16]. It is well known physically burn and non-changeable. However, now it can be easily to change inside the operating system to enabling MAC cloning attack. The hijacking attack that is Layer 2-based, an attacker impersonate of the connection between two network hosts.

Man In The Middle (MITM) [2] is an attack that redirects the traffic between any two nodes in layer 2, like between host and a router. That possible, because ARP is a stateless protocol, and cannot verify the origin of the messages. Each time a host gets an ARP reply, and even it does not send an ARP request for this reply, it will updates its ARP cache table with this ARP reply [4]. The process of updating a target host's ARP cache table with a fake entry is referred to as poisoning. Attacker sends a fake ARP reply message with IP address of host B and the MAC address of the attacker to host A. Additionally, the attacker sends a fake ARP reply with IP address of host A and the MAC address of the attacker to host B. The traffic between the two hosts A and B pass through the attacker machine allowing sniffing.

Layer 2 has another attacks types, these attacks targeted switch forwarding table technic. Ethernet switch depends on CAM table to store the node’s MAC address and the corresponding

physical switch port. Normally this memory table has limited space. In the flooding attack, the attacker floods the network switch with MAC addresses using fake ARP frames to fill and overflow the CAM table. Then, the Ethernet switch starts broadcasting the traffic without switching to the right port similar to hub mode.

Port stealing is one of these attacks that depend on the switch technic to gain access to layer 2 traffic. The port stealing attack uses the mechanism of the switches in how binding MAC addresses to physical switch ports. When a switch receives Ethernet frame from a port, it binds the port number with a source MAC address. The attacker, first, floods the switch with fake ARP frames including the target host's MAC address as the source address and the attacker MAC address as the destination address in ARP reply frame. Since the target host also sends normal frames traffic, with consideration a race condition. The switch receive frames from two different ports with the same source MAC address and continuously amendment the binding of the MAC address to the physical port in CAM table. If the attacker is faster in sending frames, the frames that intend for the target host will send to the attacker's switch port instead to the target host. Attacker steals the target host's port so the traffic going through it first, and then to the target host. The attacker then will send an ARP request. The attacker request for the target hosts' MAC addresses in the ARP message.

The attacker wills stops sending fake ARP request frame during waiting for the ARP reply. The receiving an ARP reply means that the target hosts' port in the switch has been restored to the normal binding. After receiving the ARP reply, the attacker will forward the frame to the target host. Whole process will repeats by the attacker for each new frames [5] [6] [7].

There are many ways to mitigate these types of attacks. Some of the systems are monitor ARP cache table updates. And some reject unsolicited ARP reply message from updating its ARP table.

Some solutions depend on the switch to mitigate layer 2 attacks. Port security is one of the options in the switch that used to binds a physical port in the switch to MAC address. MAC flooding and cloning attacks are preventing by Port security option. Still ARP spoofing is possible and not prevent by port security [3]. Port security validate source MAC address in the frame header, whilst there is an additional source MAC field in the data payload inside ARP frames, and clients use this field to advertise their caches [10].

5. PROBLEM STATEMENT

This study have been reveals many weak points in current naming architecture in IP over Ethernet networks. Some of it related to ARP that is one of the most vulnerability points in Layer 2 and create an overhead, and some related to MAC address. The weak points hereinafter:

1. There are no security aspects for ARP protocol while mapping IP to MAC addresses as ARP RFC [10].
2. Delay actual Data in the Ethernet frame while waiting for ARP process to resolve destination MAC address. It will be more real-time if done without call sub-procedures. See Figures 5.1.a, b.
3. Using Address Resolution Protocol is susceptible network devices to various attacks in layer 2, which lead to sophisticated attacks to upper layers.
4. ARP introduces an overhead on operating system by continually sending and receiving ARP messages to map IP to MAC addresses and maintaining ARP cache table.
5. Employing ARP in current naming architecture will be generating extra noise in the network within the same collision domain. That exhausted the network resources.
6. IP protocol is not fully compatible work over Ethernet protocol, this cause a weak link that lead to many performance and security flaws, appear clearly in data link layer where IP joint with Ethernet, when encapsulate IP packet inside Ethernet frame, and resolving IP to its MAC address.

6. RELATED WORKS

In this section, we will provide an overview of secure ARP methods and new architecture that have been proposed to solve Layer 2 problem.

6.1 Cryptographic Architectures

S-ARP [19] Proposed to address the issues of ARP spoofing. It suggested messages encryptions as the basic strategic to tackle the issues of ARP spoofing. It is backward-compatible and extension to the Address Resolution Protocol, which depends on a public key cryptography to authenticate ARP replies message. To implement this solution in a LAN, every host to be secured should be modified to use S-ARP instead of ARP. Additionally, there must be a certification authority, which is called the AKD, that is contacted to obtain the public key of a host so that replies can be authenticated by The backwards-compatible design allows hosts without the middleware to function, but at the risk of being vulnerable to ARP attacks. Verifying the appended signature, The AKD also distributes its clock value so that the other hosts can synchronize to it. This is necessary to prevent replay attacks that could be performed to spoof a host that is down (or being DoSed).As a proof of concept, the system was implemented on Linux. To make the solution compatible with dynamic IP assignments, a modification of DHCP called S-DHCP is proposed. A drawback of this scheme is still employs ARP in broadcast, which will generates extra noise in the network within the same collision domain. Additionally, employ AKD server make a single point of failure in the network. If the AKD is down, a host cannot verify ARP packets that are sent by a previously unknown host (i.e., the sender's public key is not in the receiver's key ring). Even if the AKD is working properly, an attacker can impersonate a host that goes down by cloning the MAC address of the host (but only until the cache entry of the host being impersonated, in the host being attacked, expires). One of the most crucial problem with this approach is the processing time imposed to encrypt, decrypt and to send extra messages getting the public key or getting the host verified, all these extra time processing is burdening the current ARP protocol not including the current broadcast behavior.

TARP[13] 2005, Implements the security by distributing centrally issued secure IP,MAC address mapping attestations (called tickets) through existing ARP messages. These tickets are centrally generated and signed by a Local Ticket Agent (LTA), and contain an expiration time. Hosts attach these tickets to ARP replies so that the receiver can verify the validity of the address association. Versions for statically and dynamically address assigned networks also are described. TARP is backward-compatible with ARP protocol, but it is susceptible to replay attacks during a small period of time. Moreover, still have a single point of failure by relies on LTA server if it downs then the system down. The authors implemented TARP for Linux, as a combination of a kernel module and a user space daemon.

IEEE 802.1X [15] protocol is one of IEEE Standard for port-based Network Access Control (PNAC). This standard provides an authentication mechanism at layer 2 by use a modular topology to devices want to attach to network (LAN or WLAN). A user that want to accessing the network makes a request to a gateway that at the same time play the authenticator role that controls network accessing and redirect the requests to an authentication server. In addition, the authenticator and authentication server are in the same system, as is often with 802.11b wireless access points. The authentication servers may include RADIUS and LDAP.EAP allows methods of authentication like PEAP, MD5, TLS, TTLS and use optional keying material. Once this takes place, the authenticator forwards user credentials to the authentication server. The server send accept or reject message, along with user configuration data such as Virtual LAN number. Also EAPOL protocol was redrafted to use with IEEE 802.1AR and IEEE 802.1AE (MACSec) in 802.1X-2010.

The main drawback it is a non-Independent network that need additional device, and cause single point of failure. Moreover, Man-In-The-Middle and session hijacking attacks is possible. EAPOL send a Logoff frames by the 802.1X supplicant through the network in clear, and contain data for the credential exchange for initially authenticated the client. Therefore it easy to be

spoofed, and can be enable DoS attack on both wired and wireless LANs. In EAPOL-Logoff attack, constantly sends fake EAPOL-Logoff frames from the malicious third node that has access to the medium that the authenticator is attached to.

6.2 Middleware architectures

By using middleware architectures to detecting ARP attacks they will not change or extend ARP protocol. Watch the local ARP cache for changes. Analyze ARP packets. Actively validate mappings. Normally monitor a suspicious ARP behavior like was a request sent to a given reply, Invalid MAC addresses in reply and whether ARP packet breaks current mappings.

Dynamic ARP Inspection [18] some high-end Cisco switches has this feature. It is allows the switch to drop ARP packets with invalid *IP, MAC* address bindings.

To be able to detect which ARP packets have invalid bindings, the switch uses a local pairing table built using a feature called *DHCP snooping*. This scheme promises to be a very effective solution to the problem of ARP attacks, but thorough tests need to be performed to confirm if in fact it is able to prevent all types of ARP attacks. One main disadvantage of this solution is the high cost of switches that have this feature available. Additionally, depending on the setup of the DHCP server and the network, it might not be possible to validate some ARP packets on all switches in the VLAN [11].

Ebtables[12] is a Linux technique used to create programmable bridging and switching devices to perform Ethernet frame filtering, among other things. It has been suggested that Ebtables can be used to implement ARP attack prevention mechanisms, but the efficacy of such method has not been studied. The main drawback of this approach is that this solution would only filter malicious ARP messages that attempt to pass through the Linux box, while other areas of the network remain unprotected. Additionally, Ebtables rules to prevent ARP attacks are not widely available, and the task would have to be left to the administrator, who can easily make mistakes when programming the bridge or the switch.

Anticap [24] is a kernel patch for various UNIX-based operating systems that aims at preventing ARP poisoning attacks by rejecting ARP updates that contain a MAC address different from the current table entry for that IP address. This solution works in static environments, but does not work in dynamic (DHCP-enabled) networks, with no security if mapping not yet in cache, pure kernel mode processing, and is available for a limited number of operating systems (Linux 2.2/2.4, FreeBSD 4.6, NetBSD 1.5).

6.3 Operating System Architectures

Static ARP cache entries add a static entry to local ARP cache is simple and effective way to prevent ARP attacks because static entries cannot manipulate through ARP spoofing. It is good for individuals to secure ones gateway. This solution has two disadvantages: First, it does not work in dynamic environments to use DHCP (Dynamic Host Configuration Protocol).Second; it does not scale well, as it would be need more efforts for the network administrator to deploy and update these tables throughout the network because once new or changed hosts will affects all hosts.

Furthermore, some operating systems (such as Windows 2000/XP) may accept dynamic ARP replies and updates for static entries [21].

MAC spoofing attacks can be detected by sending an **Inverse ARP (InARP)** [22] request for a MAC address. The response can be used to determine if a computer is performing cloning [20] (if and only if the computer being cloned has not been DoSed or shutdown). This is a very limited solution as it only detects this type of ARP attacks.

Operating System Security Behavior In general, every operating system has different network stack and behavior, each network interface card has different drivers with their own behavior,

even the same operating system may have different behavior depending on network stack version, driver, and firmware version. In Linux kernel 2.4 does not react to unsolicited replies but Inserts mappings from requests into cache.

Some operating systems like Solaris only accept ARP updates after timeout period [20]. This makes it harder for the attacker to poison the cache, but not impossible. When this type of mechanism is used, an attacker can poison the cache as long as the attacker's ARP reply arrives before the reply from the legitimate host, or by sending a forged ICMP echo request that appears to come from one of the two victims [20].In Windows no inbuilt ARP security and Registry settings affect ARP behavior [17].

7. OBJECTIVES OF THE STUDY

In this study, the goal is to improve the security and performance of the networks by studying the link compatibility between Ethernet and IP protocols. Ethernet was not founded to work with a specific Layer 3 protocol. Also, IP protocol was not designed to work with a specific Layer 2 protocol. This makes IP protocol and Ethernet protocol relation is not fully compatible, and results to many performance and security problems. Resolving IP to MAC address and encapsulation IP packet inside Ethernet frame are the requirements to link between IP and Ethernet protocol. This clearly appears in data link layer, which is the link between the two protocols.

Five main objectives have been identified that lead to a logical progression through the thesis:

1. Improve network security especially Layer 2 security: Most serious attacks in layer 2 depend on ARP protocol to redirect data traffic. By reducing the use of ARP protocol for resolving IP address in data transfer process, and cancelling the use of MAC address in delivery data process in layer 2, we will gain a better security state as well as more reliable communication.
2. Minimize operating system resources usage: ARP functions and cache table building and maintaining are responsibilities of the operating system. By stopping and removing ARP functions (request and reply) and stopping building and maintaining the cache table from operating system duties, we can reduce the computational time in operating system procedures to transmit network information, and reduce memory space consuming that used to store cache table.
3. Minimize network resources usage: ARP request message is based on broadcasting and its reply is based on unicast. By reducing this part of traffic, network will be more silent. Moreover, many other protocols will effects with this new proposal. For Instance, ICMP protocol will proceed without resolving process that leads to enhance in protocol mechanism. Another example, DHCP protocol will still work without the need to change and without enhancing on its performance. There are still many other protocols need to determine the level of effects. This will achieve by an empirical and monitor its procedures under the new circumstances and conclude its behavior. By applying that we save network resources by reduce part of traffic and enhance protocol mechanism.
4. Make a modification on the design of the Ethernet frame header which will use IP address instead MAC address: current naming architecture using MAC address which consists from 48-bits in the Ethernet header, while IP address is consisting from 32-bits. Therefore, utilize IP address instead MAC address makes no problem with the size of address field in the frame header. First, this will achieve by build a converting form procedure. Second monitoring what other cases will effects due these changes like the broadcast and multicast traffic.
5. Evaluate operating system and network functioning due to the architecture changes: We will use our knowledge gained in previous tasks to formally evaluate the new architecture against the current state.

8. THE METHODOLOGY

Our methodology will be focus on make a reduction on Data Link Layer to obtain a higher performance and security in IP over Ethernet Networks. Some literatures recommended our vision to solve Layer 2 problems but they consider it hard to implement [23].In this section we will explain our hypothesis and modification required to achieve our objectives. The hypothesis can be described as follow:

- After a device establish its IP and subnet addresses, it is satisfactory to have only IP address of the destination device to send the Ethernet frame for that device. In this case, there is no need to use MAC address, and there is no need for an ARP cache table.
- A more efficient protocol should be able to use only one of the addresses after an initial setup. A network device may identify itself when it is first connected to a subnet work to establish a network address and use that address without constant mappings. This type of protocol requires changes in Layer 2 architecture.

We follow two factors in methodology to achieve our objectives:

First, reduce the processes of the Address Resolution Protocol. To make these changes on current naming architecture in IP over Ethernet networks, it needs to cancel the use of Address Resolution Protocol ARP from data transmission procedure. This can be achieved by using one address form for both Layer 2 and Layer 3.Inthe current procedure when network device want to send Ethernet frame to another node in the LAN, the destination IP address is known, but destination MAC address is not. At this point the system will call ARP process to resolve destination MAC address, as shown in Figure 5.1.a. After canceling the use of ARP from unicast traffic the procedure will be optimized to be as shown in figure 5.1.b.

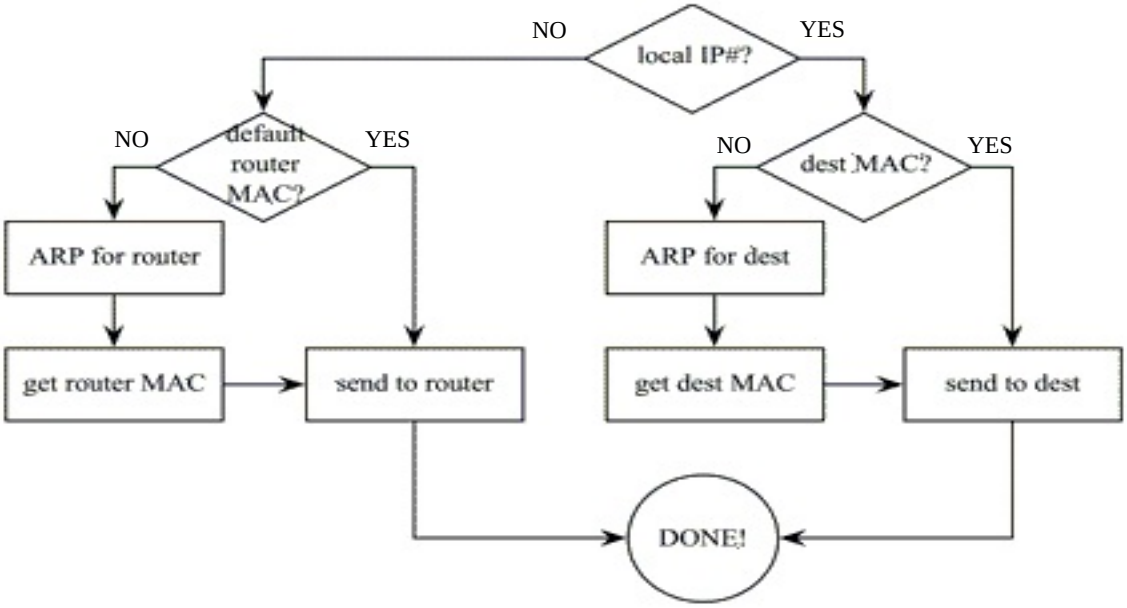

FIGURE5.1.a: Current Procedure for Transmission one Frame process

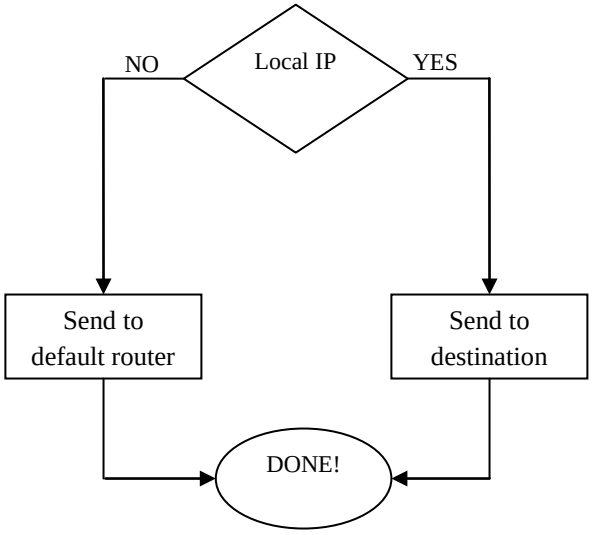

FIGURE5.1.b: Transmission process after apply the Hypothesis

Second, cancel the use of MAC address in the Ethernet frame header and use IP address from the packet (Layer 3 address). The packet in Layer 3 contains the source and destination IP address. While in Layer 2 the Ethernet frame header should fill with destination and source MAC address, see the Figure 5.2.a.

The proposed modification is to change the architecture to use IP address as a destination and source address in the Ethernet frame header instead using MAC address. See the Figure5.2.b.

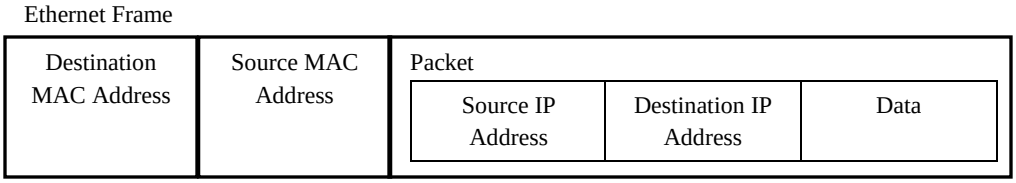

FIGURE5.2.a: Ethernet II frame

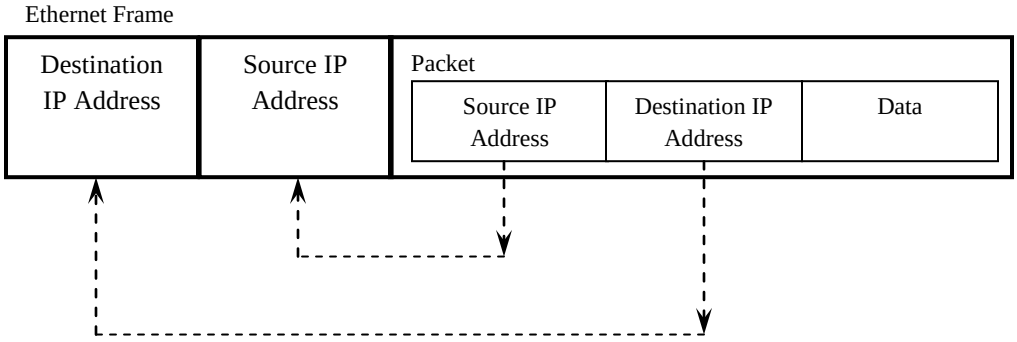

FIGURE 5.2.b: New Proposed Ethernet frame

The IP address will be used as a flat address for both Layer 2 and Layer3 and will represent in both Packet and Ethernet frame header. When received this frame by the destination node, the system will exam the address in the arrived frame header with Layer 3 address instead Layer 2 address, to check whether the frame is for this device or not. By following the above procedure in sending and receiving frame we could obtain:

- We will no need for use ARP request or reply.
- No more need for ARP cache table that take a time to process and memory space to maintain it.
- ARP processes (Request and Reply) will be optional after applying our hypothesis for use if need to inform about MAC address.
- Gratuitous ARP will still in use to detect conflict IP in Local Area Network.

From above descriptions there will be an influence significant on others protocols from all above layers. For example, ICMP protocol mechanism will optimize to be more efficient with two steps to achieve the goal instead current scheme with four steps. See Figure 5.3.

8.1 Study Phases

We can abbreviate our study passes three phases as follow:

1. **Phase 1**: Primarily analysis by collecting the result from different performance and security scenarios for the current scheme.
2. **Phase 2**: In this phase, after proposal evaluation we will start to explain the new circumstances for the proposed scheme there will be the explanation how the network components (devices and protocols) work under the proposed circumstances.

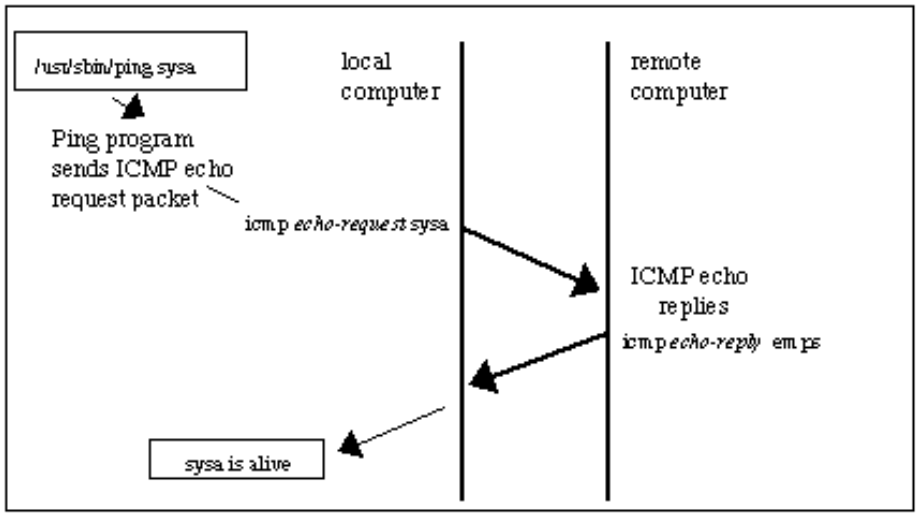

Figure 5.3: ICMP Enhancement

Main researching issues will be in:

- Router and Ethernet switch.
- Network Address Translation (NAT).
- Security issues, the attack that may still exist.
- Tunnel protocols.
- MAC unique.
- Internet Control Message protocol (ICMP).
- Traffic types: Broadcast and Multicast.
- Identity and authentication.
- Dynamic Host Configuration Protocol (DHCP).

3. **Phase 3**: Evaluating network functioning and operating system due to the architecture changes.

8.2Adoption

The literature was presented solutions that proposed extra devices like secure servers and protocols to attach to the current scheme. The complex, unforeseen problems, more administrator efforts and cost, all these factors prevent any propose solution from widely adoption. Processing the problem from the base will offer most advantages with mostly standardize. Here will illustrate how our proposal is promising to be widely adopted, and explain how network devices and protocols work under our proposal circumstances:

1. DHCP: DHCP is Layer 3 protocol, used to automatically assign IP address to LAN nodes. DHCP has no role with Data transmission. Since we are focusing on increase the performance and security for Data transmission in Layer 2 only, DHCP will still work without change. Host will still identify itself with its own MAC address to IP address.

2. Gateway Router: In the current scheme, when the network device desire to connect with external destination in WAN side, it will use gateway router MAC address in sending frame. In our proposed scheme, the destination address field in the Ethernet frame header will fill with gateway router IP address. Delivered frame will be test with router IP address, if it is equal then de-capsulate and proceed to the network layer to test the destination IP address in the packet header. The IP in the destination address field may equal to the gateway router IP address, which mean this deliver packet is send to the gateway itself, else the packet need to reroute.

3. Ethernet Switch: Ethernet switch build a table, called Content Addressable Memory (CAM) tables. It stores the binding MAC addresses to physical switch port numbers. Ethernet switch forward arrived frame to appropriate physical port depend on CAM table entries. At the same time switch look for the source address in the Ethernet frame header, and update the CAM table with this MAC address and the physical port that came from. With our propose modifications on the address in the frame header, switch will continue store this address, without recognize whether it change or it is MAC or other address. This means Ethernet switch will still work normally and no need for changes.

4. Point-to-Point connection within LAN: Network station needs IP address to attach to the network. To start a connection with another station within LAN, it needs the destination IP address of remote station, to fill the destination address field in the packet header with this address. ARP protocol is used to resolve the destination IP address to MAC address, and to fill the destination address field in Ethernet frame header with this destination MAC address. In this study we propose to use destination IP address as the address that fill with destination address field in the Ethernet frame header instead the destination MAC address. This will reduce the time and process required to send the frame, which means faster sending frame without need queue the frame until resolve hardware address No need for use ARP protocol, and no more need to build and maintain cache table.

9. COMPARATIVE EVALUATION

Most of the studies in the security and performance problems of IP over Ethernet naming architecture are focusing on ARP-based solutions architectures. While the problem is still there, that because the mapping process was founded due to the need for resolving mechanism between two different naming systems, IP and MAC address. So it is not the fault of ARP protocol. The main issues may introduce by the design of the architecture.

Whereas, our proposed modifications in the naming architecture depending on revising the origin naming architecture design, and make a reduction with replaceable parts.

ARP-based solutions depend on proposing and attach a new scheme to existence architecture. That will led to increasing the complexity degree and breaking the standards. Moreover, it may create an additional unforeseen performance problems and security vulnerabilities. Building a new architecture needs constructing everything from beginning and that will need more costs and efforts.

Whereas, in our proposed architecture we avoid to break the standard and increasing the complexity at the same time that will be achieved by avoiding propose a new architecture. Instead of that we revised the origin design and reduce the using of two addresses to using one flat address, which is the IP address from layer three. Same IP derived from layer 3 which is used in the packet that wants to send. This IP address will use in the Ethernet frame header instead the MAC address. In result, we are using same name space in IP over Ethernet naming architecture to guide the data travel through the network.

In our proposed architecture, we cancel the use of ARP protocol which will reduce the resources that need to accomplish the connection. Moreover, saving the network bandwidth by removing the heaviest bandwidth part, which it is the broadcast bandwidth that generated by ARP request messages and unicast ARP reply messages. This will provide a more reliability and increase the availability in the network connections.

Whereas, the ARP-based solution depend on existence of ARP protocol as essential to provide a protection. This will not provide any performance enhancement. On the contrary, this will increase the complexity. At the same time it may be provide a limited protection solution. Even that will break the standard and will not easy to adopt.

Still the solutions that ARP-based architecture is using MAC address as Ethernet address in layer 2. That was deployed in the destination and source hardware address in Ethernet frame header. Which need to use layer 3 IP address to resolve the destination layer 2 MAC address. Whereas, our proposed architecture no need any more for using MAC address in layer 2. Due to using IP address in the header of Ethernet frame, means the architecture will depend on the available destination IP address to accomplishing the frame transmission instead using the MAC address. That will save the efforts to bring and resolve the destination address. It is worth to mention here, that the current resolving mechanism faces many possibilities to attacks or drop or collision that will directly effects on the performance for the data queued and waiting for transmit.

In current naming architecture using ARP cache table is necessary to keep the resolved addresses for a specific period of time. This table is susceptible to attacks to poison its entries. leading to redirect the traffic toward third party point like ARP cache table overflow attack. Moreover, ARP cache table are requiring maintaining by the operating system and updating its contents. That will make the system always busy. Further, it is taking a memory space that is need also to reserve and maintain by the operating system.

Whereas, in our architecture, we proposed to cancel the use of ARP cache table due to no need for the resolution process with using one address in the naming system. That will return many advantages. For instance, avoiding the ARP cache table attacks, and save the operating system resources. Moreover, no need to update the ARP cache entries and remove the expire one. Further, canceling the resolution process will lead to cancel the reservation memory space and save the network node resources.

Most of the provided solutions are focusing on increasing the security features in IP over Ethernet naming architecture, which make the protocols heavy and more complex. Most of the data link layer protocols were not designed with or for security issues. In the literature, authentication servers, encryption algorithms and ticketing system are proposed to add to the current architecture, which make them not independent and need one more extra step to achieve the goal of the transferring process. Moreover, these solutions create a single point of failure.

On the contrary, our architecture was targeted the easy adoption goal. That was achieved by reduction the design making a significant optimization in the current naming architecture.

10. DISCUSSION

The proposed architecture will eliminate the ARP spoofing attacks in the network. That will be by preventing update the ARP cache table with unverified entries. By using one flat address in the IP over Ethernet naming architecture, that will make the system without needing for mapping process by ARP protocol. Which it is the main point to enable layer 2 attacks by redirect the traffic to the third party. In this study we proposed a modification for the naming architecture without ARP cache table. That will eliminate the possibilities for the attackers to poison the cache table with fake information. Moreover, it will provide the ability to send the data in real time without queuing the layer 2 ready data. Depending on IP address in both layer 2 and layer 3 encapsulations. Another advantage it possible to eliminate the overflow attack of the cache table, duo to there is no more use for ARP cache table. Our new method avoids breaking the standard by bringing a novel mechanism and elements to attach to the current network architecture. In result, the complexity degree will not increase and keep the current scheme simple and clear. We made a modification on current scheme by using IP address as the only one flat address for naming system in IP over Ethernet networks. That will provide easy steps to adoption like such scheme in current network architecture. Like such scheme need only an update for operating system to add the proposed modifications to meet with the needs. The most stubborn attacks in IP over Ethernet networks are Man-In-The-Middle, and this attack are prevented by the new proposed scheme. This attack depends on poisoning to redirect layer 2 traffic toward third party. Another layer 2 attack is DoS attack, by poison the cache table of the victim with nonexistence IP/MAC pair for another machine in the network, which means it can't reach for this destination.

11. CONCLUSIONS

We made an investigation on the performance and security problems in Data Link Layer, and found the problem in the link between IP protocol and Ethernet protocol. These two protocols are not fully compatible and not designed to work specifically with each other. The current design of the naming architecture may take the main issue in the problem, while we found weak principles in using MAC address. This link needs to be enhanced to improve the performance and security in the data link layer. We proposed to make a reduction on the naming architecture design. In this architecture, we utilize Layer 3 address as a flat address for both Layer 2 and Layer 3 instead of using fixed media access control (MAC) addresses. Moreover, this architecture reduces the role of ARP in the unicast data traffic.

11.1 Future Research

The presented IP over Ethernet naming architecture with the new prosed concepts is a significant step toward enhancing the performance and security of the network naming architecture. During this study we observed many new field may further researches.

The impact of the proposed architecture on the others protocols in upper layers may study further. Especially the secure protocol such HTTPS, SSL and SSH.

The security in the data link layer may need to more explore. Various attacks with different techniques in layer 2, may research to investigate which is disabled and which is effects and who still not effected.

Our scope in this study includes IP protocol working with Ethernet technology environments. Further research may work on IP protocol with different layer 2 technologies. For instance, ATM protocol with fiber optic technologies. Further, frame relay and other layer 2 protocols.

12. REFERENCES

[1] Craig A. Shue, Minaxi Gupta, An Internet without the Internet protocol, Computer Networks 2010 54 (2010) 3232–3245, http://dx.doi.org/10.1016/j.comnet.2010.06.009.

[2] NathNayak, G., GhoshSamaddar, S., “Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions”, Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference.

[3] S.J. Prowell, R. Kraus, and M. Borkin, “Seven Deadliest Network Attacks”, Syngress, 2010.

[4] Bashir, M. S., “ARP Cache Poisoning with Ettercap" August 2003Available at http://www.giac.org/practical/GSEC/Mohammad Bashir GSEC.pdf.

[5] S.Vidya, R.Bhaskaran, “A Subnet Based Intrusion Detection Scheme for Tracking down the Origin of Man-In-The-Middle Attack”, IJCSI International Journal of Computer Science Issues, Vol.8, Issue 5, September 2011, ISSN(Online): 1694-0814, pp-173-179.

[6] S.Vidya, N.Gowri, R.Bhaskaran, “ARP traffic and Network Vulnerability”, in proceedings of INDIACOM-2011, conducted by BVICAM, New Delhi, India, page – 619 and in CD.

[7] Hayriye C. Altunbasak, “Layer 2 Security Inter-Layering In Networks,” Thesis dissertation, Georgia Institute of Technology, Dec. 2006.

[8] Xiangning HOU, Zhiping JIANG and Xinli TIAN. The detection and prevention for ARP Spoofing based on Snort. In 2010 International Conference on Computer Application and System Modeling (ICCASM 2010).

[9] Behrouz A. Forouzan, “TCP/IP Protocol Suite”, Fourth Edition, Tata McGraw Hill, pp. 220-223, 2010.

[10] 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.

[11] C. Schluting. Configure your Catalyst for a more secure layer 2, Jan. 2005. http://www.enterprisenetworkingplanet.com/netsecur/article.php/3462211.

[12] B.D.Schuymer.ebtables: Ethernet bridge tables,Mar.2006.http://ebtables.sourceforge.net.

[13] W. Lootah, W. Enck, and P. McDaniel. TARP: Ticket-based address resolution protocol. In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC ’05)*, Dec. 2005.

[14] TJ O’Connor, “Detecting and Responding to Data Link Layer Attacks”, SANS Institute InfoSec Reading Room, Oct 13, 2010, http://www.sans.org/reading_room/whitepapers/detection/detecting-responding-data-link-layer-attacks_33513, 2010.

[15] 802.1x-2004, http://www.ieee802.org/1/pages/802.1x-2004.html.

[16] Sanjeev Kumar, Orifiel Gomez, “Denial of Service due to direct and Indirect ARP storm attacks in LAN environment”, Journal of Information Security, 2010, 1, pp. 88-94, doi:10.4236/jis.2010.12010 Published online October 2010 (http://www.SciRP.org/journal/jis).

[17] Microsoft Windows 2008 TCP/IP Protocols and Services Technical Reference, Thomas Lee and Joseph Davies, Chapter 3: Adress Resolution Protocol (ARP).

[18] C. Schluting. Configure your Catalyst for a more secure layer 2, Jan. 2005. http://www.enterprisenetworkingplanet.com/netsecur/article.php/3462211.

[19] D. Bruschi, A. Ornaghi, and E. Rosti. S-ARP: A secure address resolution protocol. In *Proceedings of the 19th AnnualComputer Security Applications Conference (ACSAC ’03)*,Dec. 2003.

[20] S. Whalen. An introduction to ARP spoofing.2600: The Hacker Quarterly, 18(3), Fall 2001 http://www.node99.org/projects/arpspoof/arpspoof.pdf.

[21] Static ARP more dynamic than you might think on, http://www.chrismc.de, last access 15/8/2011.

[22] T. Bradley, C. Brown, and A. Malis. “Inverse address resolution protocol”, Sept. 1998. RFC 2390.

[23] Altunbasak, H., Krasser, S., Owen, H., Sokol, J., Grimminger, J.,andHuth, H.-P., “Addressing the weak link between Layer 2 and Layer 3 in the Internet architecture," in Proc. of the 29th Annual IEEE Conference on Local Computer Networks (LCN), (Tampa, Florida), November 2004.

[24] M. Barnaba. anticap. http://www.antifork.org/viewcvs/trunk/anticap, August/2011.

[25] Cisco Systems. *Configuring Dynamic ARP Inspection*, chapter 39, pages 39:1–39:22. 2010. Catalyst 6500 Series Switch Cisco IOS Sofware Configuration Guide, Release 12.2SX.