# Security Issues

# With

# Address Resolution Protocol

By

**Akash Shrivastava**

August 2008

Akash.InfoSec@gmail.com

## 1. Overview:

Any computer which is connected to the Network (LAN or WAN) has two addresses. One is the IP Address (*An IP Address is a 32-bit number included of a host number and a network prefix, both of which are used to uniquely identify each node within a network*), and the second is Physical or Ethernet Address called MAC Address (*An Ethernet address or MAC Address is a 48-bit six-part hexadecimal number in which a colon separates each part, for example, 8:0:20:1:2f:0. This number identifies the Ethernet board installed in a PC and is used to identify the PC as a member of the network*).

The foremost intention of present study is to understand and deal with the subject of ARP Spoofing. The issue that how ARP spoofing can be used for different kind of attacks to Network Structure and Operating Systems and how to provide countermeasures to protect them has been reviewed and discussed in this article.

## 2. ARP Mechanism:

ARP (Address Resolution Protocol) performs mapping of an IP addresses to Ethernet/ Physical Address. The protocol operates below the Network Layer as a part of the OSI Link Layer, and is used when IP is used over Ethernet.

A machine who wants to get a MAC Address sends an ARP request in the form of packets "Is your IP address X.X.X.X? If so, send your MAC back to me (Y.Y.Y.Y)." These packets are broadcast to all computers on the LAN, even on a switched network. Each computer examines the ARP request, checks if it is currently assigned the specified IP. Then the target system forms an ARP Response "Yes. I'm X.X.X.X, here is my MAC Address hh:hh:hh:hh:hh:hh", and sends an ARP reply containing its MAC address or Physical Hardware Address.

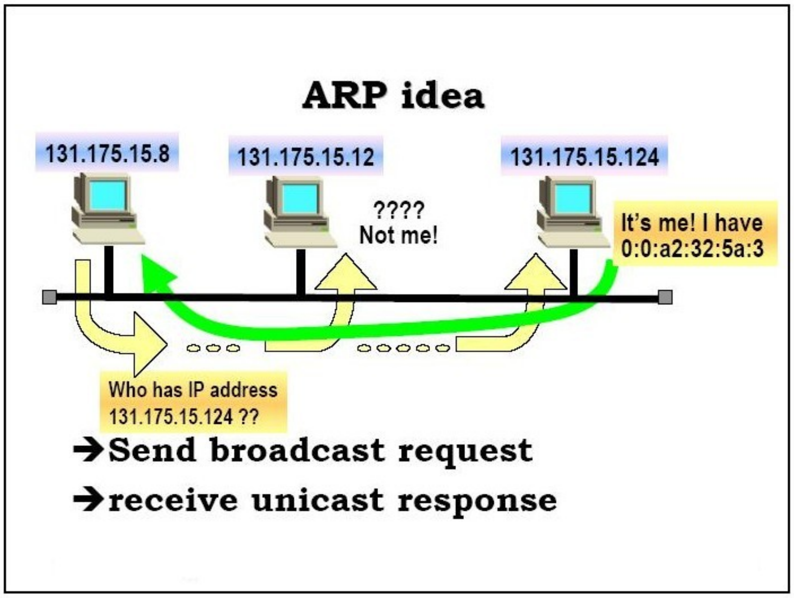

**DIAGRAM 1: ARP Mechanism**[23]

When performing mapping between an IP address and an Ethernet address, a table, usually called **ARP Cache**, is used to maintain a correlation between each MAC address and its corresponding IP address. An ARP Packet contains Sender's and Target's IP and Ethernet Addresses. It looks like this:

```
-----------------------------------------------
   |Sender IP Address     223.1.2.2        |
   |Sender Enet Address   08-00-28-00-38-A9|
   ----------------------------------------
   |Target IP Address     223.1.2.1        |
   |Target Enet Address   08-00-39-00-2F-C3|
-----------------------------------------------
```

**TABLE 1: Example ARP Request/ Response**

## 3. Major Constraints in Adoption of ARP:

ARP is a protocol in the TCP/IP suite that provides IP Address-to-MAC Address Resolution for IP packets. ARP is well known protocol and designed with so many securities which is limited to **Sniffing** and **Spoofing**, however there are so many points that ARP can be used for Sniffing and Spoofing.

The problem with ARP is that it is a **Stateless** protocol so it sends ARP reply packets to the target machine even if it (target) has not send any ARP requests yet. This makes it possible for the attacker to send forged ARP reply packets continuously to the victim where the MAC address is forged to correspond to the one of the attacker's machine.

Since it is a Stateless protocol hence, it is vulnerable for ARP Spoofing, which is a method of exploiting the interaction of IP and Ethernet protocols. It involves making fake ARP Request and Reply packets. It is only applicable to Ethernet networks running IP. When performing mapping, between IP Address and MAC Address, both the addresses stored in the **ARP Cache** for future packets. To minimize network traffic ARP Table updates their cache of IP-to-MAC mappings whenever an ARP request or reply is received. If the given IP has altered, then the new value will overwrite the old one in Cache.

Updating the host's ARP cache with false information via spoofed ARP Replies is known as "ARP Cache Poisoning".

If an intruder breaks into one of your machines on a subnet, he can use ARP Spoofing to compromise the rest of it.

Because of this vulnerability in ARP, attacker can Spoof into the ARP Request/ Reply procedure. ARP Spoofing can take place on the source, destination, or any network the traffic passes between. So, it is possible to redirect traffic from the attacked host to a different destination. Here is the example of the ARP Spoofing:

First you have to make sure that the attacking machine has ip-packet forwarding enabled. On RedHat Linux 8.0 this can be accomplished by executing the command:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

From the attacking machine run the following command:

```
arpspoof –t <ip-address of the victim> <ip-address of the gateway>
```

Packet redirection is done with iptables with the following commands:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp -s <victim ip> -d <server ip> --dport <dest_port> \ -j REDIRECT --to-port <dest_port_on_attacker_machine>
```

Now traffic to the port <*dest_port*> from the victim to the server is redirected to the attacker's IP address with destination port <*dest_port_on_attacker_machine*> [20]

Some Operating Systems vulnerable to ARP Spoofing are following:

1. Windows 95/98/2000/ NT/ 2000
2. HP 10.2
3. Linux RedHat 7.0

The OS that is protected against ARP Spoofing is:

6. Sun Solaris OS

## 4. Types of ARP Attacks:

There are many ways an attacker can gain access or exploit your system. It is not important how attacker gain access into the system. Once the intruder breaks into your system he can use it according to his way. Following are some types of attacks that can be resulted from ARP Spoofing:

- Man-in-the-Middle (MIM)
- Denial of Services (DoS)
- Session Hijacking
- Sniffing
    - *Passwords*
    - *Sensitive information*
    - *Information gathering*
- Broadcast Attacks

### *4.1. Man-In-the-Middle (MIM) Attack:*

Man-in-the-Middle (MIM) is a very common type of attack, in which an attacker inserts his computer between the communication paths of two target computers by Sniffs packets from Network, modified them and then insert them back into the Network. The malicious computer will forward frames between the two computers; so communications are not interrupted, but all traffic first goes to the attacking computer rather then targeting and victim computers. In this attack the attacker uses a program that appears to be the server to the client and appears to be the client to the server. Few programmes available for MIM Attacks are Juggernaut, T-Sight and Hunt. Following is an example of MIM Attack:

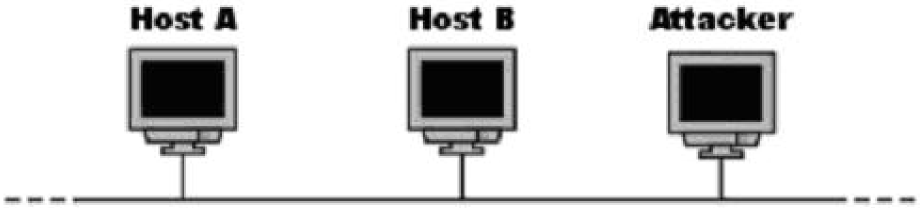

**DIAGRAM 2: Man-In-the-Middle Attack (MIM)** [19]

The attacker wishes to sniff all traffic that A sends to B and visa versa. This is currently not possible as the attacker is connected to the network via a switch. The correct IP addresses and MAC addresses for each host are as follows:

| Host | IP Address | MAC Address |
|---|---|---|
| Host A | 192.168.0.2 | 00:00:00:00:00:02 |
| Host B | 192.168.0.3 | 00:00:00:00:00:03 |
| Attacker | 192.168.0.4 | 00:00:00:00:00:04 |

**TABLE 2: ARP Cache Table**

We can also assume that the above is true for all the hosts ARP caches.

Firstly the Attacker will poison A's ARP cache with a spoofed ARP Reply. The ARP reply will tell A that the IP address of B now has a MAC address of 00:00:00:00:00:04. Once A has processed the ARP

Reply its ARP cache will look like this:

| Host | IP Address | MAC Address |
|---|---|---|
| Host A | 192.168.0.2 | 00:00:00:00:00:02 |
| Host B | 192.168.0.3 | 00:00:00:00:00:04 |
| Attacker | 192.168.0.4 | 00:00:00:00:00:04 |

**TABLE 3: Poisonous ARP Cache-1**

Secondly the Attacker will poison B's ARP cache with a spoofed ARP Reply. The ARP reply will tell B that the IP address of A now has a MAC address of 00:00:00:00:00:04. Once B has processed the ARP Reply its ARP cache will look like this:

| Host | IP Address | MAC Address |
|---|---|---|
| Host A | 192.168.0.2 | 00:00:00:00:00:04 |
| Host B | 192.168.0.3 | 00:00:00:00:00:03 |
| Attacker | 192.168.0.4 | 00:00:00:00:00:04 |

**TABLE 4: Poisonous ARP Cache-2**

Now whenever A sends B an Ethernet frame the switch will route it to the Attackers port, this will also be the case whenever B sends A an Ethernet frame. The attacker may now **'Sniff'** the traffic whilst forwarding it on to its originally desired host.[19]

## *4.2 Denial of Services (DoS) Attack:*

A **"Denial of Service (DoS)"** attack is a flood of packets that consumes network resources and causes deadlock. Through **"Denial-of-Service** (DoS)" attack attackers make the system unusable and prevent services from using for legitimate user by overloading, damaging or destroying resources so that the services can not be used.

**DoS Attack** can be performed with an attacker **altering** the hosts **ARP Cache** (by ARP Poisoning) with non-existent entries (**MAC Addresses**). This cause frames to be dropped because of the limited size of ARP Cache.

In the Dos Attack, attacker attacks the server by **sending** an **abnormally high volume** of **requests** over a network, which essentially can **prevent valid network traffic**, **slows down** the performance of a **server**, **disrupt connection** between two or more machines, **disrupt services** and make machines and services unavailable for legitimate users.

Most of the operating systems, Routers, and Network Components that have to process packets at some level are vulnerable to DoS attacks.

### *4.3 Session Hijacking*:

Session Hijacking is a process by which an attacker sees/ listen an active TCP connection between two other hosts and then insert forged packets (in one or both directions) and takes control of the connection. This method is similar to the **MIM** attack.

In this technique attacker make the victim believe that he/she is connected to a trusted host system, but in reality the victim communicates with the attacker. The attacker uses a program (for example **Hunt**) that appears to be the server to the client and appears to be the client to the server.

For example, an attacker waits for users to make a remote connection to a server via Telnet. Then he use Spoofing technique and send fake information to the computer. By doing this he takes control over a connection that is already established. Following is an example of the Session-Hijacking:

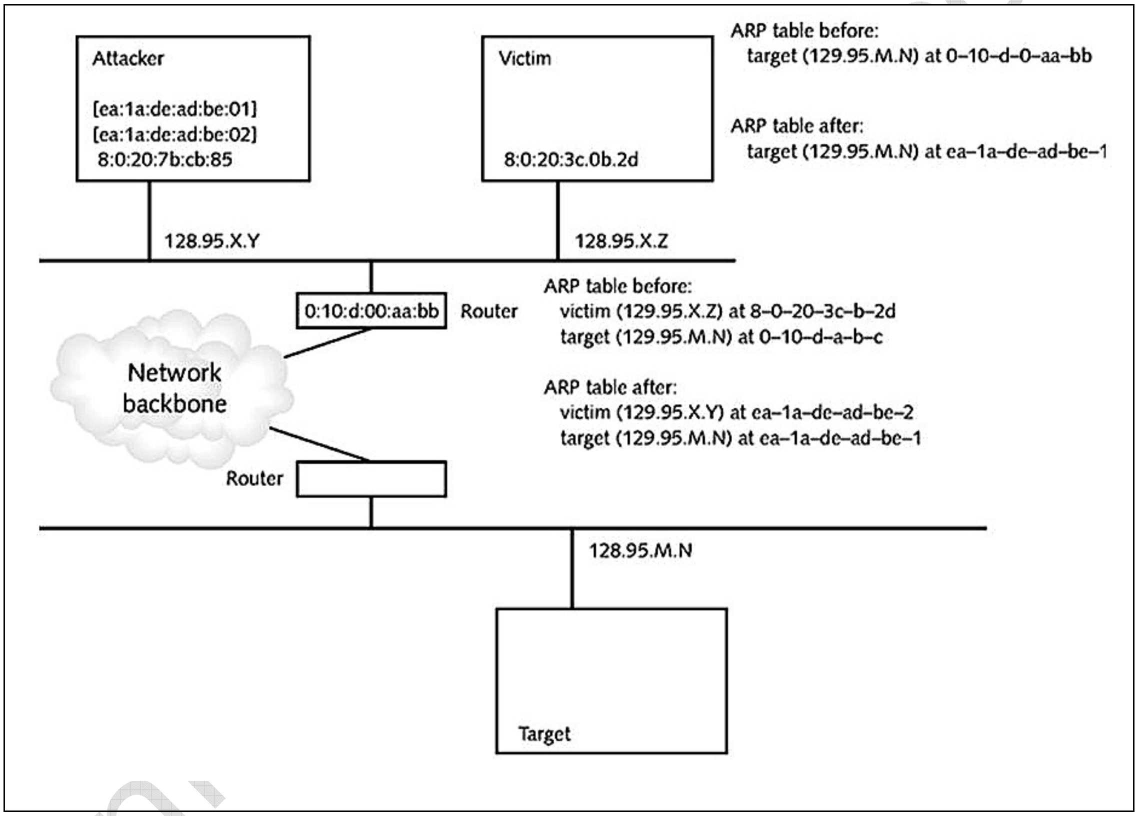

**DIAGRAM 3: Attacker using source Ethernet segment as a user** [22]

## *4.4 Sniffing (Passwords, Sensitive Information and Information Gathering)*:

Sniffing is a process of monitoring all information or reading the packets that are being transmitted on a network.

An attacker can sniff network traffic and can also passively intercept network traffic. Then, through packet analysis, he might be able to determine login IDs and passwords and collect other sensitive data. There are so many tools available for Sniffing like Hunt, Sniffit, Ettercap, Snort and Dsniff.

They work as follows:

a) Ethernet was built around a "shared" principle: all machines on a local network share the same wire.

b) This implies that all machines are able to "see" all the traffic on the same wire.

c) Thus, Ethernet hardware is built with a "filter" that ignores all traffic that doesn't belong to it. It does this by ignoring all frames whose MAC address doesn't match.

d) Through a Sniffer program turns off this filter, putting the Ethernet hardware into "promiscuous mode". Thus, an attacker can see all the traffic between Host A and Host B and pick up interesting information such as Usernames and Passwords, as long as they are on the same Ethernet wire.[21]

Following is the output of Sniffing by using Hunt:

```
192.168.0.103 [1069]  172.23.98.91 [109]
+OK QPOP (version 2.53) at testbox.example_web.net starting

192.168.0.103 [1069] --> 172.23.98.91 [109]
USER testuser

192.168.0.103 [1069] --> 172.23.98.91 [109]
PASS test1
```

In this small section of Hunt, we can see how Hunt can be used to capture usernames and passwords. In this case, the user (testuser) was accessing mail at a POP Server. The Password that was used test1.

### **4.5** *Broadcast Attacks***:**

This technique is used to send a large amount of ICMP echo request (Ping) traffic to all known IP broadcast addresses with the spoofed source address of the victim. In this attack, the malicious user generates packets with a source address of the Host he wishes to attack (Host A) and then sends a series of network packets to an organization with lots of computers, using an address that broadcasts the packets to every machine on the Network.

Now every machine on the Network will respond to the packets and send data to the organization (Host A) that was the target of the attack. The target will be flooded and then increases the Network Traffic.

## 5. Strategy to overcome the constraints:

"Officials found that 96% of the successful attacks could have been prevented if users had followed protocols." [Source: Government Computer News, 28 April 2001. www.gcn.com]

However stopping ARP attacks is quite impossible because of the intrinsic part it plays in data transfer, spoofed ARP requests are very easy to detect. A most useful defence if the use of "**Static** (Non-Changing)" ARP Entries. Since it can not be updated, spoofed ARP replies will be ignored. To prevent Spoofing, the ARP tables must have static entries for each machine on the Network. However if static ARP entries are used to prevent DoS attacks or Spoofing, they need to be protected from overwriting.

*Here are some countermeasures to protect the Network from Attackers.*

### *5.1 Network Analyzer Tools and Sniffers:*

Network Analyzer Tools and Sniffers are most useful tools available on Internet that can be used to debugging network problems.

They are used by network professionals to diagnose network abnormalities. It allows you to inspect network traffic at every level of the network stack in various degrees of detail. ARPWatch, Dsniff, Hunt, Parasite are some popular tools.

### *5.2 Encryption:*

Encryption is an effective way to defend against Sniffing and ARP Spoofing. Encryption prevents any non-authorized party from reading or changing data.

The level of protection provided by Encryption is determined by an **encryption algorithm**. In a powerful attack, the **strength** is measured by the number of possible **keys** and the **key size**.

If communication between hosts systems is **encrypted** at the **Network Layer** there is little chance for programs such as **Dsniff** to gather useful information from the Network, since the attacker will not know which packets contains authentication information and which do not.

### *5.3 Intrusion Detection Systems (IDS):*

IDS identify attacker's attempts to attack or break into the network and misuse it. IDSs may monitor packets passing over the network, monitor system files, monitor log files, or set up deception systems that attempt to trap hackers.

Port Scans and Denial-of-Service Attacks are an ongoing threat. An Intrusion Detection System is critical components of a defence-in-depth security solution that can identify potential threats and allow you to take immediate action to block a hacker or a particular IP address that's being used to launch an assault.

There are two types of IDSs available: **Network-Based IDSs (NIDS)** and **Host-Based IDs (HIDS)**.

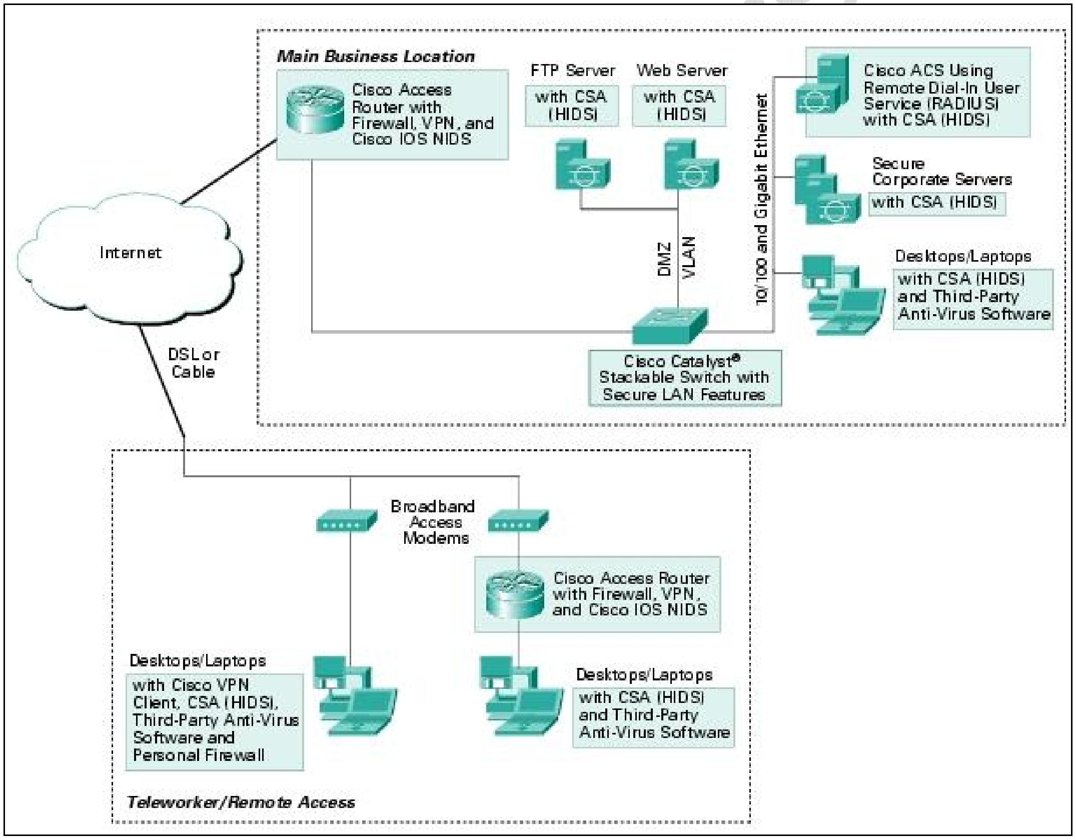
Main Business Location
Cisco Access Router with Firewall, VPN, and Cisco IOS NIDS
FTP Server
with CSA (HIDS)
Web Server
with CSA (HIDS)
Cisco ACS Using Remote Dial-In User Service (RADIUS) with CSA (HIDS)
Secure Corporate Servers
with CSA (HIDS)
10/100 and Gigabit Ethernet
DMZ
VLAN
Desktops/Laptops
with CSA (HIDS) and Third-Party Anti-Virus Software
Cisco Catalyst® Stackable Switch with Secure LAN Features
Internet
DSL or Cable
Broadband Access Modems
Cisco Access Router with Firewall, VPN, and Cisco IOS NIDS
Desktops/Laptops
with Cisco VPN Client, CSA (HIDS), Third-Party Anti-Virus Software and Personal Firewall
Desktops/Laptops
with CSA (HIDS) and Third-Party Anti-Virus Software
Teleworker/Remote Access

**DIAGRAM 4: An Example of Implementing IDS in the Network** [17]

## 6. Conclusion and Recommendation

Practice security is constantly changing process. ARP is not secure and easy to fool. We need stronger mechanism to enforce security. We must be aware of the fact that switches are not security tools.

Possibility of ARP Spoofing Attacks can be reduced by configuring the network to decline packets from the Internet that claim to originate from the local address. Second thing, proper router configuration in a router is also a good option for security. Most of the Attacks happen because of the **Improper Router Configuration**. Here one thing is important **if the network trusts foreign hosts**, routers will not protect against a spoofing attack that claims to originate from those hosts and if you allow internal addresses to access through the outside portion of the firewall, you are vulnerable to Attacks too.

All these problems are caused by the trust-relationship between one host and the other. With the current IP protocol technology, it is quite impossible to eradicate Spoofing. Better way to prevent Spoofing is by using IPv6 or IPSec instead of IPv4, which include two new characteristics authentication header and encapsulated security payload.

Finally, Network Control Mechanisms are dangerous, and must be carefully guarded.

## 7. References & Bibliography

1. FFIEC IT Examination Handbook (Information Security Dec' 2002)
2. www.hipaadvisory.com/tech/Manual99Pdf.pdf
3. www.insecure.org
4. www.packetstormsecurity.org/papers/protocols/intro_to_arp_spoofing.pdf
5. www.Howstuffworks.com
6. www.itpapers.zdnet.com
7. www.ks.uni-freiburg.de/inetwork/papers/ARP-spoofing-handout.pdf
8. www.informit.com
9. Maximum Windows 2000 Security (Morimoto, Amaris, Doyle, Locher, Burnett)
10. http://www.cert.org/tech_tips/denial_of_service.html
11. Eric Cole, Hackers Beware, SAMS Publication, ISBN: 0735710090
12. Government Computer News, 28 April 2001. www.gcn.com
13. Anonymous, Maximum Security, Fourth Edition, Que Publication, ISBN: 978-0-672-32459-8
14. www.security.ittoolbox.com
15. www.blackhat.com/presentations/bh-usa-01/MikeBeekey/bh-usa-01-Mike-Beekey.ppt
16. www.stallion.com/html/support/glossary.html
17. www.cisco.com
18. www.security.ece.orst.edu/koc/ece478/project/addr2.pdf
19. http://www.harmonysecurity.com/paper_arp.html
20. http://www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST_hijacking_attack.pdf
21. http://www.inforede.net/Technical/Layer_3_and_4/Network_Security/Network_Sniffing.pdf
22. Calvert Ben, Boswell Steven, Campbell Paul, Security+ in Depth, Thomson Course Technology Publication, ISBN 1-59200-064-9
23. http://www.tti.unipa.it/mat_bianchi/rete_internet/2001-2002/slides/09_arp.pdf