

Short View about the ARP Attack and Defense

Introduction:

This essay aims to evaluate a common flaw of ARP (Address Resolution Protocol) in the field of local network and the way by which hackers may possible attack. Also, this essay introduces the way to protect the PC from such attacks and how the ARP firewall works.

Brief Introduction of ARP (Address Resolution Protocol):

ARP is one kind of TCP/IP protocol that maps IP (Internet Protocol) address to MAC (Media Access Control) address. The IP address is allocated by the router every time our PCs are connected to the router. The IP address may change as our network environment changes. The MAC address is possessed by every network card. It is unique and unchangeable even if we change the router that our PC is connected.

Every time when other devices (including the router) want to send a data packet to a PC as the destination, they have to figure out the destination's MAC address (physics address) in advance, just like a postman need to get the destination address before he sends the letter. Suppose PC A as the source (IP: 192.168.0.2, MAC: 0x 11:11:11:11:11:11) wants to contact with PC B as the destination (IP: 192.168.0.3 MAC: 0x 22:22:22:22:22:22). When PC A is sending the packet to PC B, it only knows the IP address of PC B instead of its MAC address. Thus, PC A has to first figure out the MAC address of the destination by broadcasting an ARP request packet to every PC in the local network including PC B. At that point, every device in the network will receive the request packet which says "I am 192.168.0.2 with MAC address 0x 11:11:11:11:11:11, who is 192.168.0.3, please response with your own MAC address". The devices except PC B will not response to such request packet, because their IP addresses are not 192.168.0.3. Only PC B will response by sending an ARP reply packet which carries PC B's MAC address back to PC A. In that case, A can successfully contact with B.

Unfortunately, it is not applicable for PC A to broadcast the ARP request packet every time it wants to contact with PC B, as too many broadcast packets will result in a heavy burden in the local network. In order to solve this problem, an ARP cache table is created in each PC, which stores the mapping of an IP address to its corresponding MAC address. In the above example, when PC A has successfully obtained PC B's MAC address, the mapping of IP address 192.168.0.3 to the MAC address 0x 22:22:22:22:22:22 is stored in the ARP cache table of PC A. Such mapping will make it convenient for PC A to send the subsequent data packet directly to PC B based on such mapping without sending the request again. Meanwhile the cache table of PC B has also stored the mapping of PC A 's IP address to MAC address which is obtained from the request packet. In Windows operation system, the cache table will refresh in 20 seconds.

Introduction to the Process Hackers Attack through the Flaw of ARP:

As the introduction above, the ARP cache table will store the mapping of IP address and MAC address. This has generated an intrinsic flaw. If one computer intends to pretend to be other devices in the local network, it responds the request packet with its own MAC address to the source first before the real destination responses, the source computer will map the IP address to a wrong MAC address in the ARP cache table. This means the source computer will send the data packet to a wrong computer instead of the real destination.

In the above example, suppose there is a third PC C (IP address: 192.168.0.4; MAC address: 0x 44:44:44:44:44:44). PC C sends an ARP reply packet with the content "I am 192.168.0.3 and my MAC address is 0x 00:00:00:00:00:00" to PC A before PC B's reply arrives at PC A. PC A is not able to distinguish which reply is the real one or not. So, PC A has no choice but adding the mapping between 192.168.0.3 and 0x 00:00:00:00:00:00 to its ARP cache table based on the first arrived reply. Then if PC A wants to send a message to PC B, PC A will think that PC B's MAC is 0x 00:00:00:00:00:00 according to the mapping stored in the ARP cache table and sends the message to 0x 00:00:00:00:00:00 (no one) instead of PC B. In that case, PC C, the hacker, has successfully reach the purpose of cutting the conversation between PC A and PC B.

If PC B is the default gateway, usually the router (IP: 192.168.0.1; MAC address: 0x 50:2b:73:52:cd:f8) and PC C has performed such attack described above, the connection between PC A and the default gateway has been cut so that PC A will no longer get access to the internet.

Moreover, such attack is definitely applicable for the hackers to reach the purpose of eavesdropping by sending the reply with its own MAC address 0x 44:44:44:44:44:44 (PC C's MAC address) instead of 0x 00:00:00:00:00:00. All the packets supposed to send to PC B will be sent to PC C and therefore, PC C is able to eavesdrop the conversation between PC A and PC B.

Some of the Tools to Perform the ARP Attacking

There are many tools to perform the ARP attack. Apart from that, there are also a lot of other kind of local network attacking tools is based on ARP attack.

1. winarpattacker

The aim of Winarpattacker is to send the false reply ARP packet described above, which means it can allow a hacker to design an ARP packet and send it to machine he wants to attack.

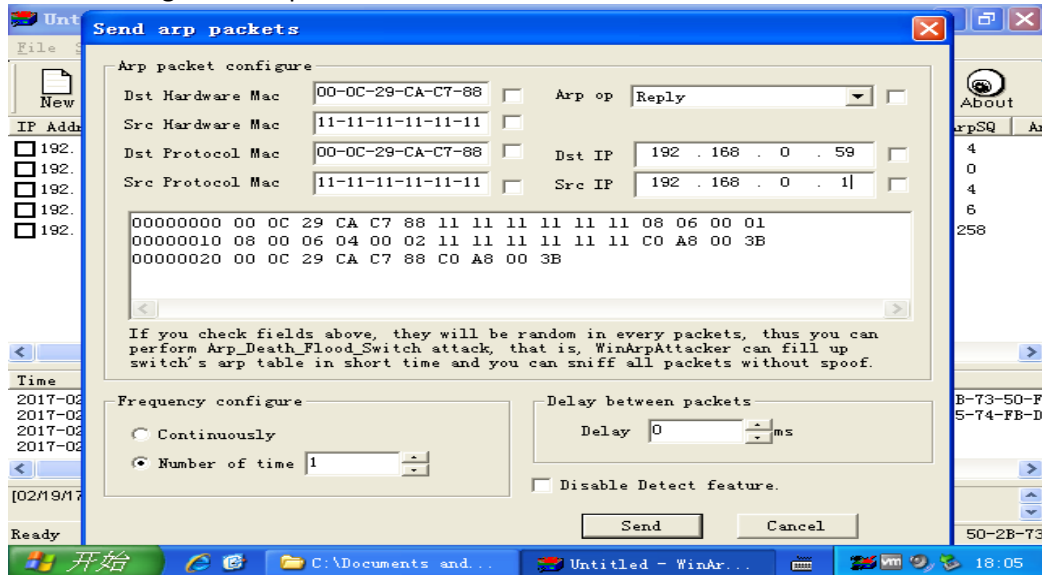
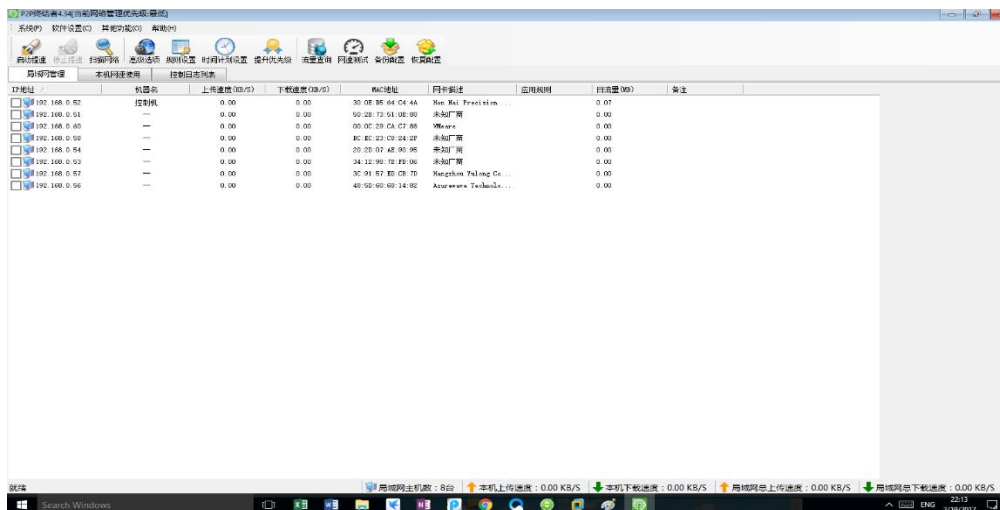


Diagram 1

As shown in diagram 1, the “Dst IP/MAC” refers to the target device we would like this ARP package send, while the Src IP/MAC indicate the content of this packet. In the above example, this packet is sent to 192.168.0.59 with the MAC 00-0C-29-CA-C7-88, which contains the content “I am 192.168.0.1, my MAC is 11-11-11-11-11-11”. In other words, such packet is to tell 192.168.0.59 that 192.168.0.1 should be mapped with 11-11-11-11-11-11.

Also, if we want all of the devices in the local network to be disconnected with the router, we just fill Dst IP 192.168.0.255 and the Dst MAC FF-FF-FF-FF-FF-FF, which is the broadcasting IP/MAC (which means you send a packet to every one)

2. P2P terminator



p2p terminator is a software which is designed to limit other devices' speed of the network through ARP attack. As it is said before, if a hacker told a PC the MAC of the default gateway is his own MAC, he can

```

C:\Users\dreamfly\cmd>arp -a

Interface: 192.168.229.1 --- 0xa
Internet Address      Physical Address      Type
192.168.229.255       ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-1c     static
239.0.0.123           01-00-5e-54-00-7b     static
239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.0.52 --- 0x10
Internet Address      Physical Address      Type
192.168.0.1           00-0c-29-a7-83        dynamic
192.168.0.51          50-20-73-51-0e-80     dynamic
192.168.0.52          24-12-86-7b-f3-06     dynamic
192.168.0.55          bc-75-74-fa-d1-ba     dynamic
192.168.0.56          48-5d-60-83-14-82     dynamic
192.168.0.57          3e-91-77-ed-d7-f9     dynamic
192.168.0.58          bc-e2-23-c3-24-2f     dynamic
192.168.0.60          00-0c-29-a7-83        dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff     static
192.168.1.1           a0-91-c8-27-0f-c3     dynamic
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-09     static
224.0.0.252           01-00-5e-00-00-1c     static
224.123.12.1          01-00-5e-7b-0c-01     static
239.0.0.123           01-00-5e-54-00-7b     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.92.1 --- 0x12
Internet Address      Physical Address      Type
192.168.92.255       ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-1c     static
239.0.0.123           01-00-5e-54-00-7b     static
239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.16.1 --- 0x1a
Internet Address      Physical Address      Type
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-1c     static
239.0.0.123           01-00-5e-54-00-7b     static
239.255.255.250       01-00-5e-7f-ff-fa     static

```

Diagram 3

eavesdrop others' packets. P2P terminator applies the same principle by cheating others' PC that the attacker is the router so that everyone needs to get through the attacker instead of visiting the router directly. In that case, the attacker is able to restrict others network speed and also issue other restrictions on the PC's access to the internet.

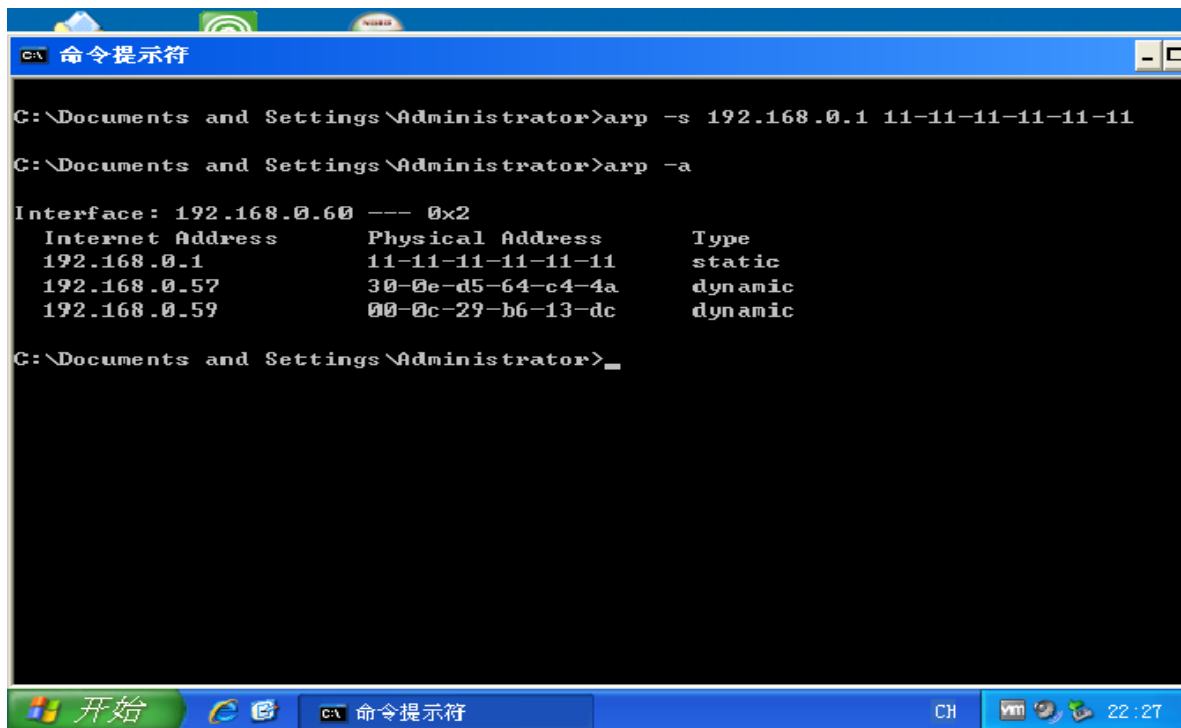
As shown in diagram 3, (192.168.0.60 is the attacker), after p2p terminator running on 192.168.0.60, the MAC of 192.168.0.1 (the router) has been changed into the attacker's MAC. At that point, the attacker is able to place some restrictions on the internet access of 192.168.0.52.

The Way to Defend against the ARP Attack

1.Stabilize the ARP Mapping

The main principle of ARP attacking is by cheating the PC so that the PC will have a wrong mapping between the IP and MAC. In that case, it would definitely practical for the PC to stabilize such mapping, which means such mapping cannot be changed by other reply packets.

In windows, such operation is realized by the command in the Command Prompt (cmd): arp -s (IP you want to stabilize) (MAC you want the IP to be mapped), just as what shown in diagram 4.



```
C:\Documents and Settings\Administrator>arp -s 192.168.0.1 11-11-11-11-11-11
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.0.60 --- 0x2
    Internet Address      Physical Address      Type
    192.168.0.1           11-11-11-11-11-11    static
    192.168.0.57          30-0e-d5-64-c4-4a    dynamic
    192.168.0.59          00-0c-29-b6-13-dc    dynamic

C:\Documents and Settings\Administrator>
```

Diagram 4

In this case, suppose I would like to map 192.168.1.1 with 11-11-11-11-11-11. After such command, the ARP mapping has been stabilized (the mapping 192.168.1.1 to 11-11-11-11-11 is static instead of dynamic).

However, in some of the cases, such command may not work, just as shown in the diagram 5.

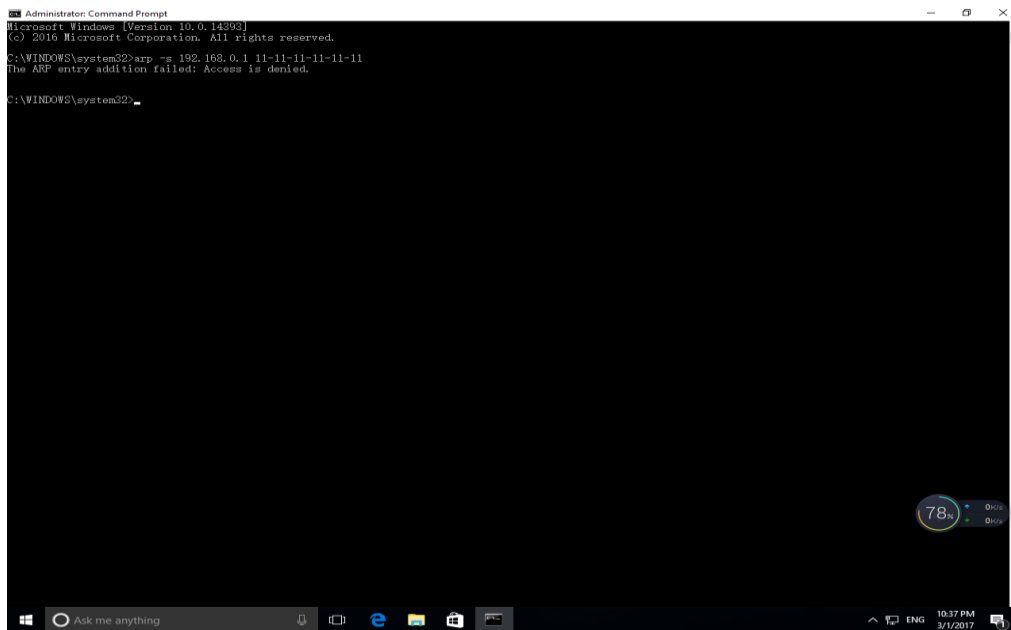


Diagram 5

In that case, we have to apply another command instead:

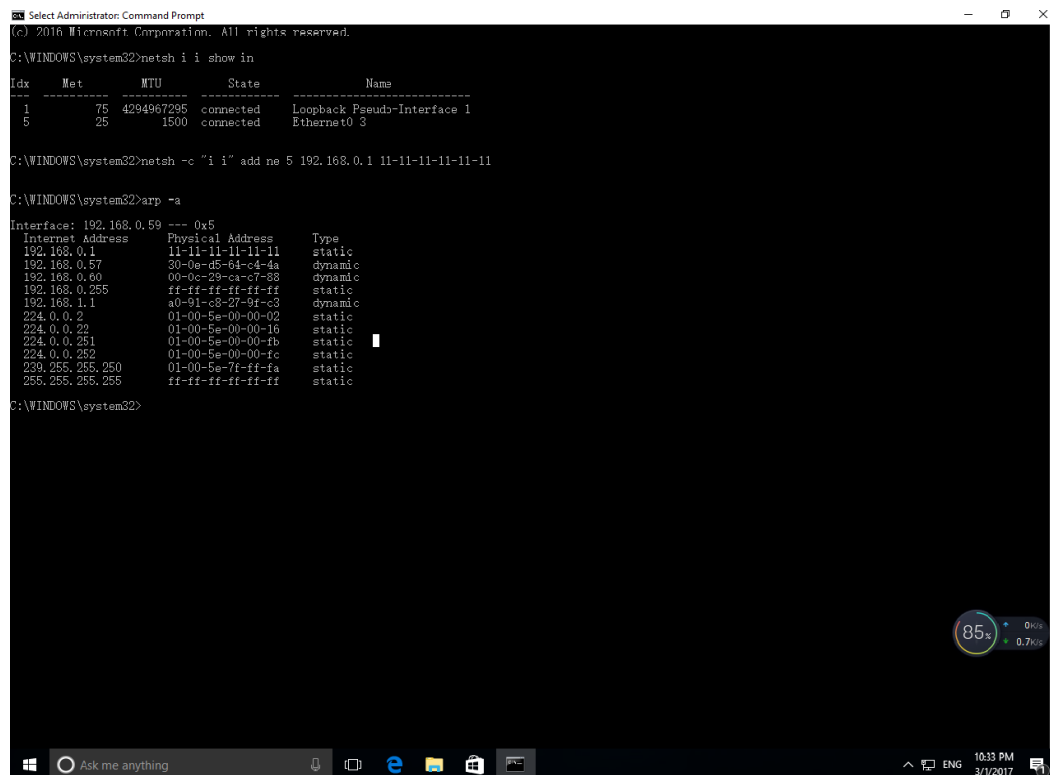


Diagram 6

First, use command “netsh i i show in”, as shown in the diagram. Find the Idx of your network name (Ethernet 0)

Then, apply the command “netsh -c "i" add ne [Idx] [IP] [MAC]”. As shown in the diagram 6, this case we would like to stabilize the map between 192.168.0.200 to 00-aa-00-62-c6-09.

Note: it is recommended that the devices (including the router) stabilize each other in double route. For example, A (the IP: 192.168.0.1; the MAC: 11-11-11-11-11-11) and B (the IP: 192.168.0.2; the MAC: 11-11-11-11-11-12) (it is possible that one of them is the router). It is suggested that A stabilize the mapping between 192.168.0.1 and 11-11-11-11-11-11, and B stabilize the mapping between 192.168.0.1 and 11-11-11-11-11-11. If they stabilize only the single route suppose only the mapping between 192.168.0.1 and 11-11-11-11-11-11 is stabilized by A but B does nothing, the hacker is still able to cut the connection between A and B by telling B that 192.168.0.2 is mapped with 22-22-22-22-22-22.

The disadvantage of this way:

Since it involved with stabilize the right mapping between IP and MAC, therefore, the PC has to make sure that they know the right mapping before stabilizing. If the hackers attacked the machine (send the wrong reply ARP packet) before the PC get the right mapping, such way will be ineffective.

2. Constantly Refresh the ARP Cache Table

As is introduced before, the hackers will constantly send the ARP attacking packet in order for the desired mapping to appear in the cache table of the PC being attacked. Therefore, it would be practical to constantly refresh the ARP cache table by broadcast the ARP request packet among the local network at the rate more frequent than the rate the hackers send the attacking packets. With such constant broadcast, the PC is able to make sure that it has got the right mapping. In that case, such way to protect against the ARP attack is most common among the ARP firewalls.

The disadvantage of this way:

Because such way involved with constantly broadcasting the ARP request packet in the local network, it will cause burden to the network so that the network speed will be lowered.

3. AP Isolation (PPP)

Any data packets including ARP packet transmit among the local network. Thus, in order for the attacker to successfully send the ARP packet, there must be connection between the attacker and the PC being attacked. If such connection has been cut down, there will be no problem of ARP attack. Such process can be realized by PPP (Point to Point Protocol), which can be configured by the router. Under such configuration, every device connected to such local network will be allocated with an account and there will be no connection between the devices so that ARP attack can be eliminated.

AP isolation can also be realized through a switcher. Since all of the local network connection should get through the switcher if it is a switcher network, the switcher can control or hold such communication.

The disadvantage of this way:

Any services involved in the local network such as print sharing and OA system will be not applicable.

Evaluation of some most common ARP firewalls:

1. Ruixin ARP Firewall:

Main principle of this protection:

stabilize and record the first ARP mapping between the router and the its MAC. Other ARP packet involved with the router (if the MAC does not match the recording MAC) will be intercepted.

Major Flaw of this firewall:

① hackers are able to attack the PC first hand.

If the hackers attack the PC first hand (the first ARP mapping the PC got is wrong), the firewall will stabilize the wrong mapping and intercepted the right mapping.

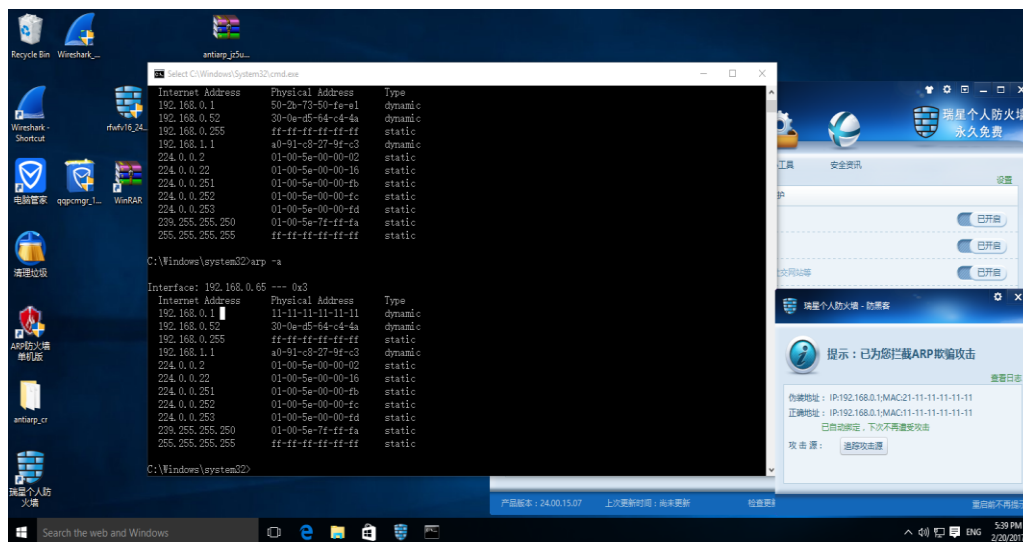


Diagram 7

As shown in the diagram 7, the firewall has wrongly match the 192.168.0.1 (the router's IP) and the MAC 11-11-11-11-11-11, because the attacker has initialed the attack before the PC get the right MAC from the router and it is shown that the firewall has already stabilize the wrong ARP mapping.

② it cannot intercept the packet that does not involved with the router.

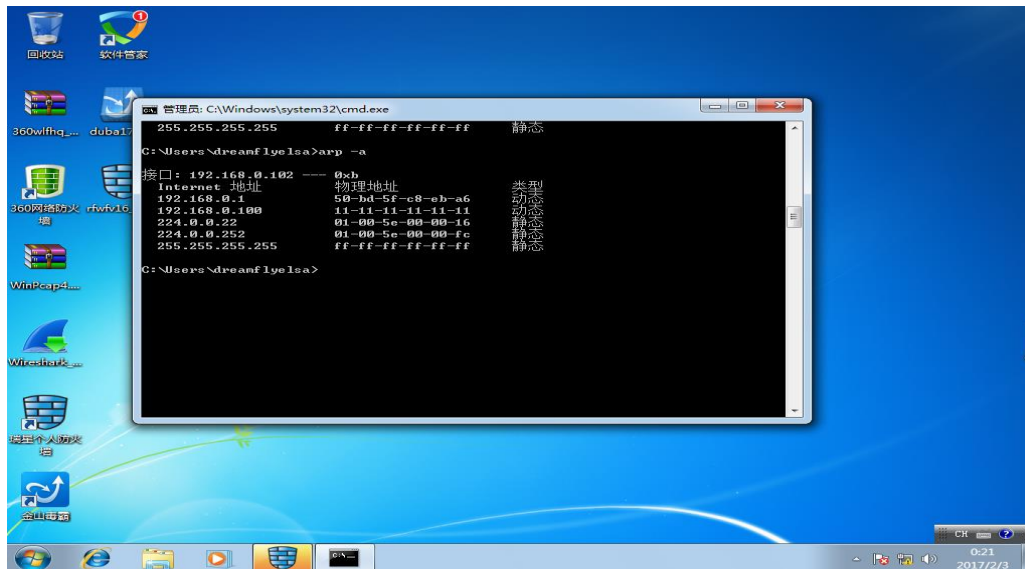


Diagram 8

If the hacker wants to cut the connection between the PCs in the local network other than the router, this firewall will pose no protection.

As shown in the diagram 8, the MAC of 192.168.0.100 has been changed into 11-11-11-11-11-11 and the firewall does not report it has intercepted any false packet, which means the connection between this PC (192.168.0.102) and the 192.168.0.100 has been cut.

2. 360 ARP firewall:

Main principle of this protection:

Ping the router actively, in case of finding out which is the correct MAC address if several contradictory ARP packets is received. If the right mapping has been found, it will stabilize such mapping.

Major flaw of this software:

the same as the second flaw of Ruixin ARP firewall

The IP 192.168.0.52 has been mapped to 22-22-22-22-22-22.

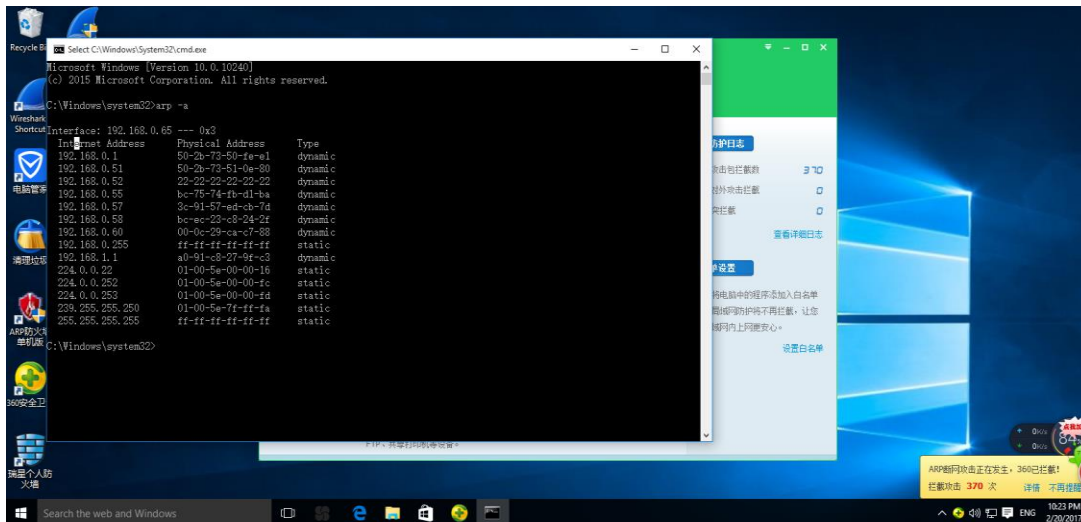


Diagram 9

3. AntiARP firewall:

Main principle of this protection:

Almost the same as that of the 360 ARP firewall.

Major flaw of this software:

1. the same as the second flaw of Ruixin ARP firewall

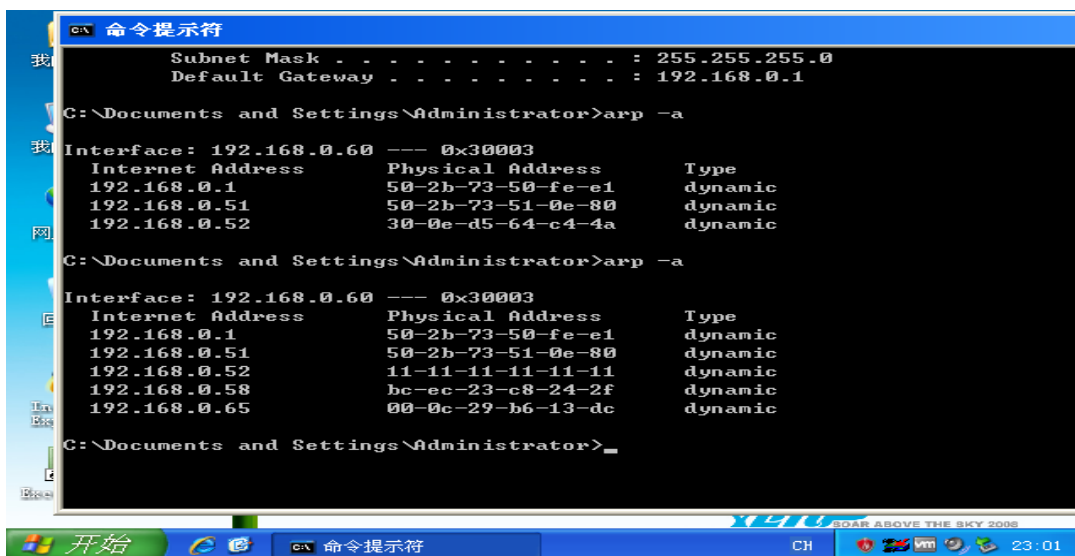


Diagram 10

Summary: except from the Ruixin firewall, all the other firewalls can effectively protect the connection between the PC and the router. However, in terms of the connection among devices in the local network, it can pose no protection. Perhaps, for most of the firewall programmer, they will only focus on the connection between the router and the PC but neglect the connection between the devices in the local network, which is absolutely one of the place needed to be fixed.

The Way to Find the Source of the Attack.

1. Apply some tools (wiresharks or Sniffers) to grab ARP packets in the local network

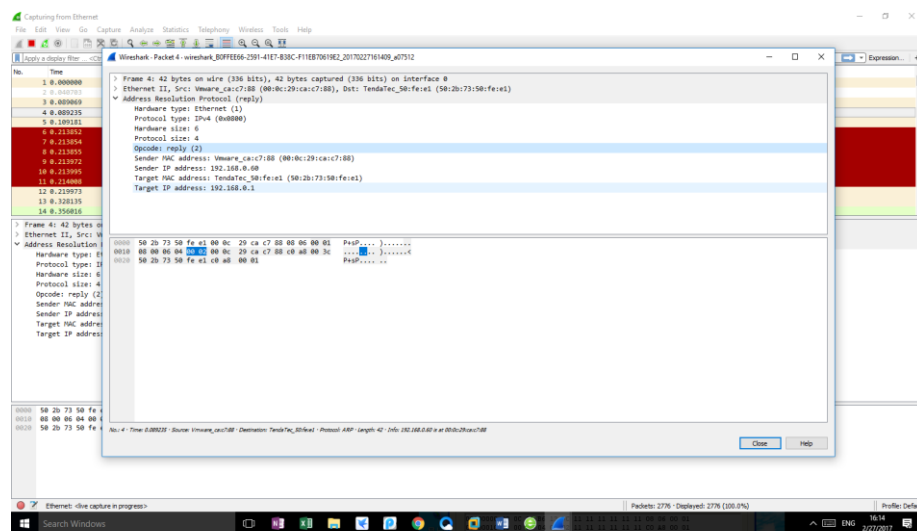


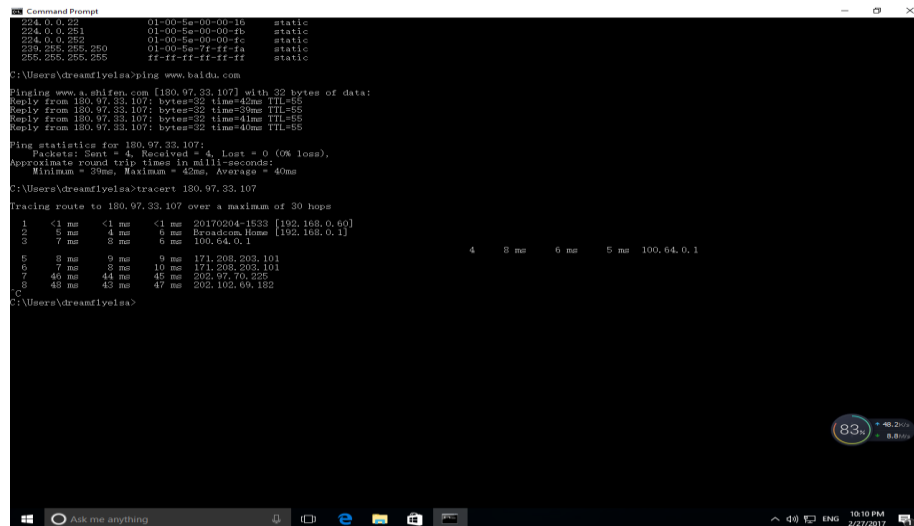
Diagram 11

When the attackers are deploying the ARP attack, there will be large number of ARP packet sent by the machine. In that case, by grabbing the data packet in the local network, we are able to find the IP address of the attacker.

As shown in the diagram 11, the third device has captured such ARP packet. Therefore, it is pinpoint that the attacker (the source of such ARP attack) is 192.168.0.60.

2. “tracert” command

“tracert” is the command that aimed to trace the route of the data packet. For example, as shown in the diagram 12, “tracert 180.97.33.107 (the IP of ‘www.baidu.com’)” is to trace the route of the data packet if the server of baidu sends a data packet to the PC.



```
224.0.0.22 01-00-5e-00-00-10 static
224.0.0.251 01-00-5e-00-00-4b static
224.0.0.252 01-00-5e-00-00-fc static
238.255.255.250 01-00-5e-ff-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\dreamfly\sa>ping www.baidu.com

Pinging www.a.chifen.com [180.97.33.107] with 32 bytes of data:
Reply from 180.97.33.107: bytes=32 time=42ms TTL=56
Reply from 180.97.33.107: bytes=32 time=51ms TTL=56
Reply from 180.97.33.107: bytes=32 time=41ms TTL=56
Reply from 180.97.33.107: bytes=32 time=40ms TTL=56

Ping statistics for 180.97.33.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 42ms, Average = 40ms

C:\Users\dreamfly\sa>tracert 180.97.33.107

Tracing route to 180.97.33.107 over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  20170204-1523 [192.168.0.60]
  1  <1 ms  <1 ms  <1 ms  Broadcom.Home [192.168.0.1]
  2  <1 ms  <1 ms  <1 ms  100.64.0.1
  3  <1 ms  <1 ms  <1 ms  171.208.203.101
  4  <1 ms  <1 ms  <1 ms  171.208.203.101
  5  <1 ms  <1 ms  <1 ms  202.97.70.225
  6  <1 ms  <1 ms  <1 ms  202.102.69.182
  7  <1 ms  <1 ms  <1 ms  180.97.33.107
  8  <1 ms  <1 ms  <1 ms  180.97.33.107

C:\Users\dreamfly\sa>
```

Diagram 12

In that case, if there is no ARP attack, the next station of the data packet from the PC must be the router. Otherwise, such local network is engaged in the ARP attack. As shown in the diagram,

As we are tracing the route of the packet from “180.97.33.107”, the “next station” of the data packet is not the router “192.168.0.1” but “192.168.0.60”. Therefore, we can infer that the 192.168.0.60 is attacking us.

Note: such way to find the source can only apply to the condition if the attacker wants to be eavesdrop the conversation between the PC and the router (the attacker will cheat the PC that he is the router) instead of just cutting the network.