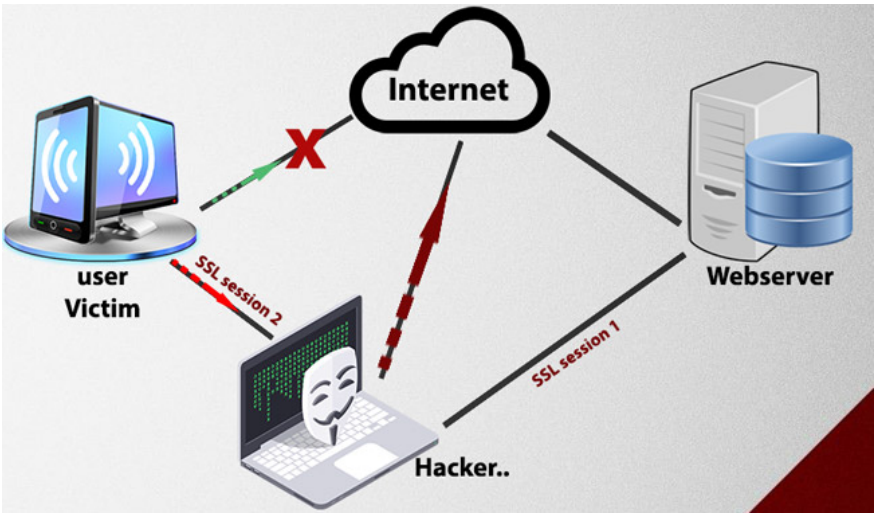
Learn about Man-in-the-Middle attacks - ARP Cache spoofing

In the first part of the series introducing some of the most commonly used MITM attacks, we will introduce you to ARP Cache spoofing, DNS Spoofing, hijacking (hijacking) attacks. session, ..

In the first part of the series introducing some of the most commonly used MITM attacks, we will introduce you to ARP Cache spoofing, DNS Spoofing, hijacking (hijacking) attacks. session, .

What is Man in the Middle?

Man in the Middle is one of the most common types of cyber attacks used against major individuals and organizations, often abbreviated as MITM. It can be understood that MITM is like an eavesdropper. MITM works by establishing connections to victim computers and relaying data between them. In the case of an attack, the victim believes that they are communicating directly with the other victim, but the truth is that the communication stream is again via the attacker's host. As a result, these hosts can not only interpret sensitive data, but they can also send in and change data streams to further control its victims.



In this series, we will explain some of the most commonly used MITM attacks, such as ARP Cache spoofing, DNS Spoofing attacks, hijacking HTTP sessions, and so on. What you see in the real world, most victim computers are Windows computers. For that reason, this series will focus exclusively on MITM exploits on computers running Windows operating systems. When possible, MITM attacks will be performed from Windows-based servers. In some cases, however, when there are no tools for the mentioned attacks, we will use Backtrack Linux 4, which can be downloaded as a live-CD or a virtual machine here.

ARP Cache (ARP Cache Poisoning)

In the first part of this series, we will talk about ARP cache poisoning. This is the oldest form of MITM attack originating (sometimes known as ARP Poison Routing), which allows hackers (located on the same subnet as its victims). can eavesdrop on all network traffic between victim computers. We chose this as the first attack to introduce because it is one of the simplest forms of attack but is the most effective form of action by an attacker.

Normal ARP communication

The ARP protocol is designed to serve the need to translate addresses between the second and third layers in the OSI model. The second layer (data-link layer) uses MAC addresses so that hardware devices can communicate with each other directly. The third layer (network layer) uses IP addresses to create scalable networks globally. The data-link layer handles directly with connected devices, while the network layer processes devices that are directly and not directly connected. Each class has its own address allocation mechanism, and they must work together to create a communication network. For that reason, ARP is created with RFC 826, ' *an Ethernet address resolution protocol* '.

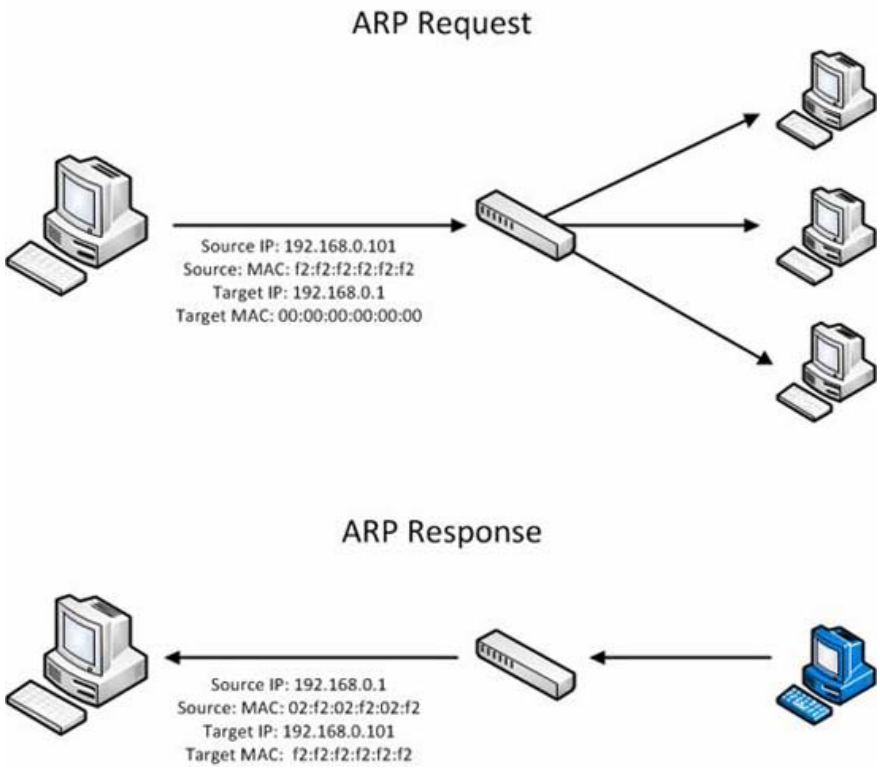


Figure 1: ARP communication process

The essence of ARP operation is focused on two packages, an ARP request package and an ARP reply packet. The purpose of the request and reply is to find the hardware MAC address associated with the given IP address so that the traffic can reach its destination in the network. The request packet is sent to the devices in the network segment, while sending it saying (this is just a personality to explain in the most understandable way) ' *Hey, my IP address is XX.XX.XX.XX , my MAC address is XX: XX: XX: XX: XX: XX. I need to send something to someone with the address XX.XX.XX.XX, but I don't know where this hardware address is in my network segment. If someone has this IP address, please respond with your MAC address!* 'Response will be sent in the ARP reply package and provide the answer,' *Hey the device plays. I am the person you are looking for with the*

IP address of XX.XX.XX.XX. My MAC address is XX: XX: XX: XX: XX: XX . ' When this process is complete, the transmitter will update its ARP cache table and these two devices can communicate with each other.

The fake Cache

The fake ARP table is to take advantage of the insecure nature of the ARP protocol. Unlike other protocols, such as DNS (which can be configured to accept only fairly secure dynamic updates), devices that use Address Resolution Protocol (ARP) will accept the upgrade. anytime. This means that any device can send an ARP reply packet to another computer and the computer will update its ARP cache table right away at this new value. Sending a ARP reply packet when no request is made is called sending an ARP 'aimlessly'. When these idle ARP replies reach the computers that have sent the request, this request computer will think that it is the object that I am seeking to communicate, but they are actually communicating with an attacker. .

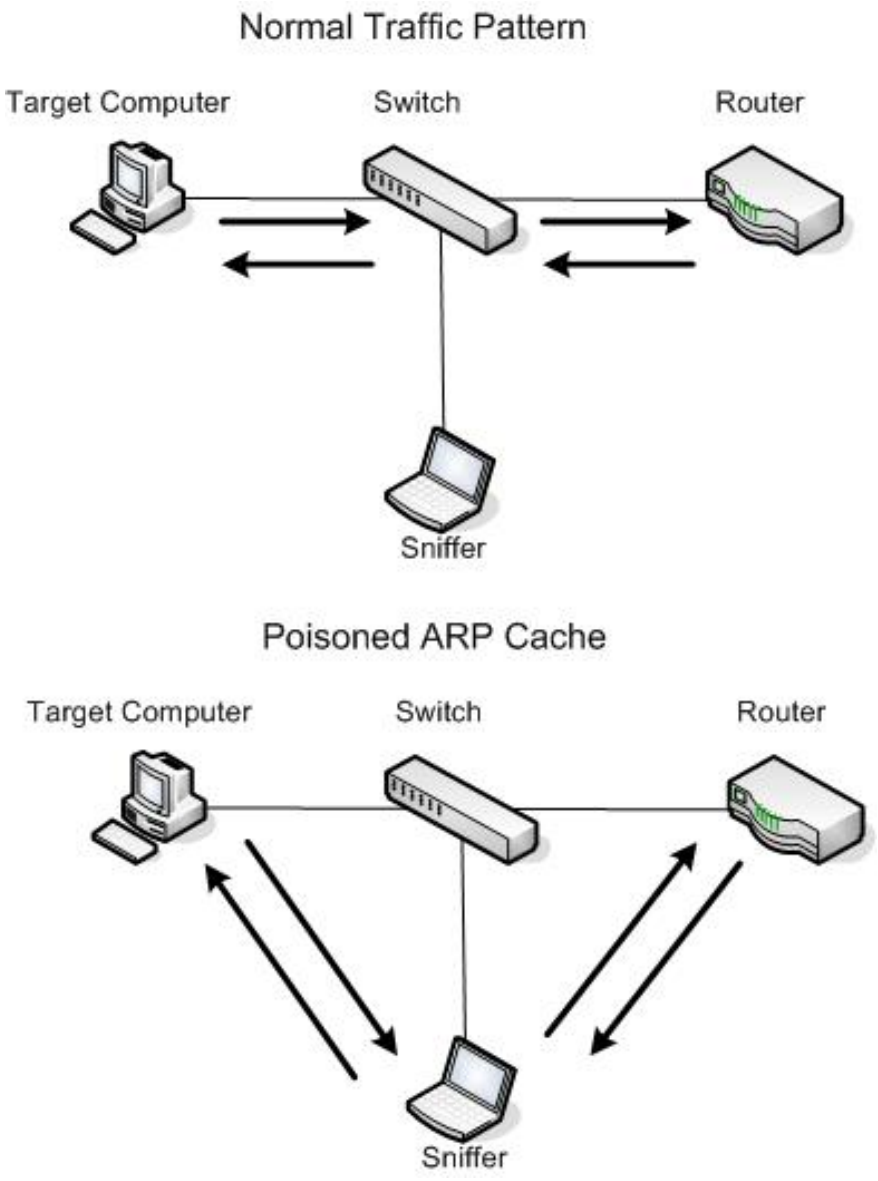


Figure 2: Block communication with ARP Cache spoofing

Use Cain & Abel

Let us give a scenario and consider it from a theoretical perspective to reality. There are several tools that can take the necessary steps to fake ARP cache of victim computers. We will use the popular security tool called Cain & Abel of Oxid.it. Cain & Abel does a lot of things besides ARP cache spoofing, which is a very useful tool to have in your arsenal. Installing this tool is quite simple.

Before you start, you need to select some additional information. Specifically, the network interface that you want to use for attack, two IP addresses of the victim computer.

When you first open Cain & Abel, you will see a series of tabs at the top of the window. For the purposes of the lesson, we will work in the Sniffer tab. When you click on this tab, you will see an empty table. To fill in this table you need to activate the program's built-in sniffer and scan the computers on your network.

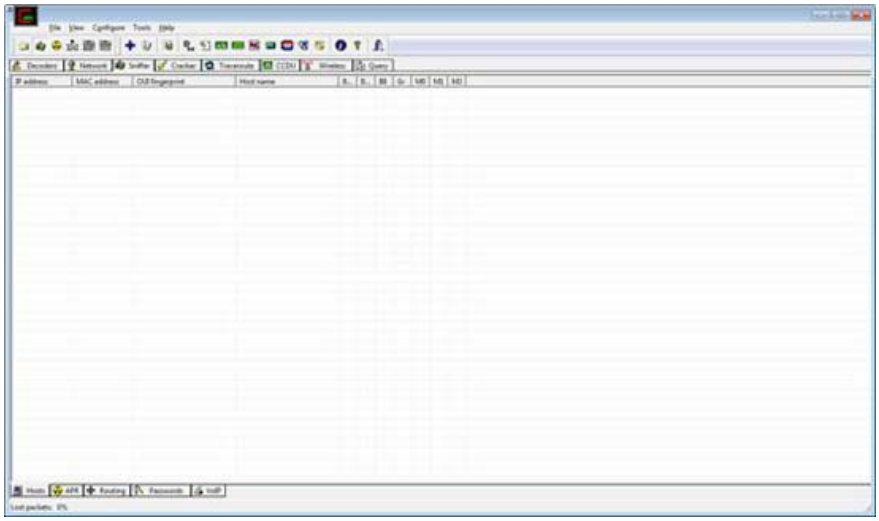


Figure 3: Cain & Abel's Sniffer Tab

Click on the second icon on the toolbar, like a network card. At first, you will be asked to choose the interface that you want to sniff. The interface needs to be connected to the network where you will perform your ARP cache spoofing on it. Once you've selected the interface, click **OK** to activate Cain & Abel's built-in sniffer. Here, the toolbar icon like the network card will be pressed down. If not, do it. To build a list of available computers in your network, click the icon like the (**+**) symbol on the main toolbar and click **OK** .

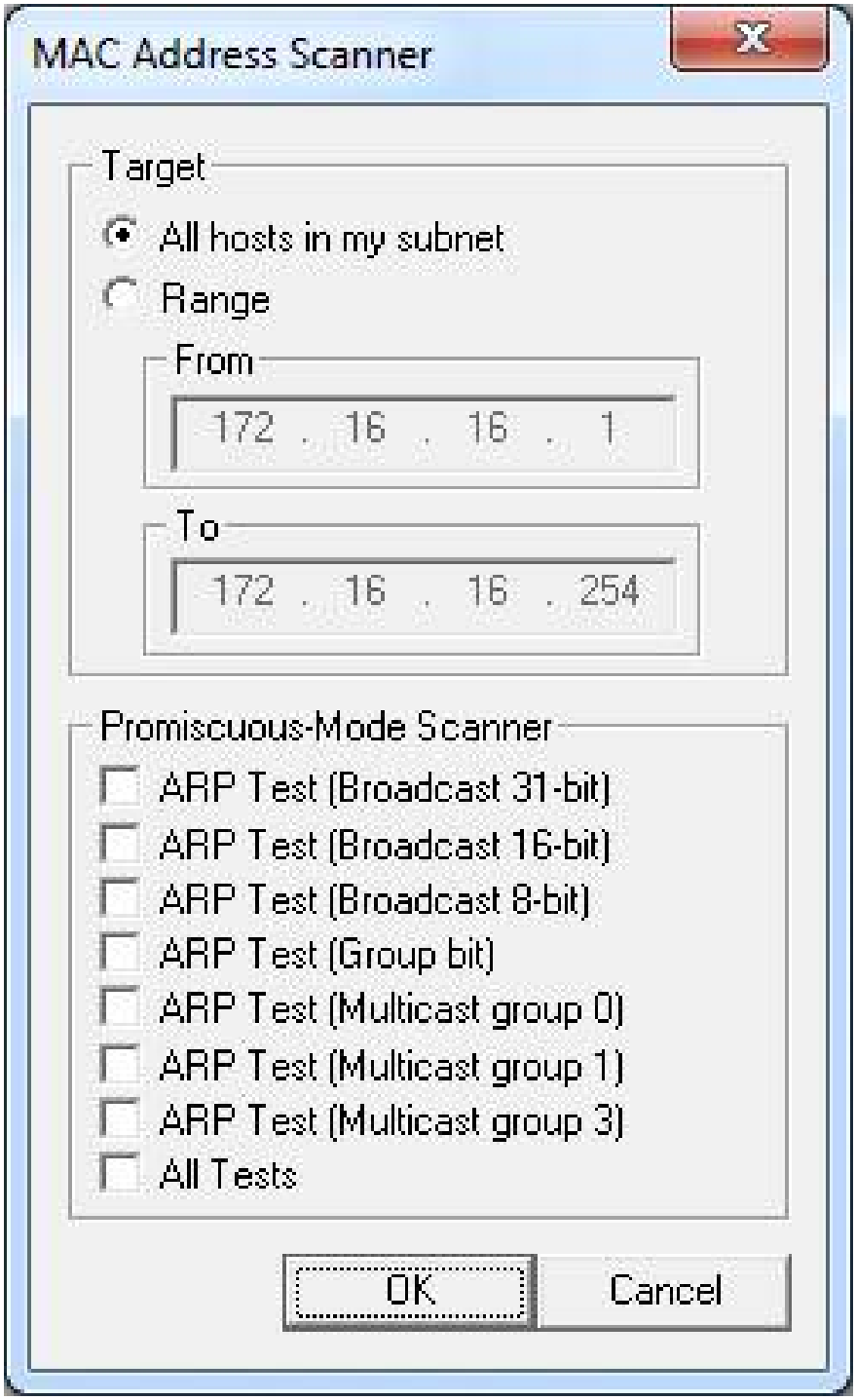


Figure 4: Scanning devices in the network

Empty grids will now be filled with a list of all the devices in your network, along with their MAC and IP addresses as well as their identity information. This is the list you will work with when setting up ARP cache spoofing.

At the bottom of the program window, you will see a series of tabs that take you to other windows below the Sniffer heading. Now that you have built your list of devices, your next task is to work with the APR tab. Switch

to the APR window by clicking the tab.

When in the APR window, you will see two empty tables: one above and one below. When setting them up, the table above will display the devices involved in ARP cache spoofing, and the table below will show all communications between spoofed computers.

Continue to set up ARP spoofing by clicking on the icon like the (+) mark on the program's standard toolbar. The window appears with two columns placed side by side. On the left, you will see a list of all available devices on the network. Click the IP address of one of the victims, you will see the results displayed in the right window is a list of all hosts in the network, ignoring the selected IP address. In the right window, click on the other victim's IP address and click **OK** .

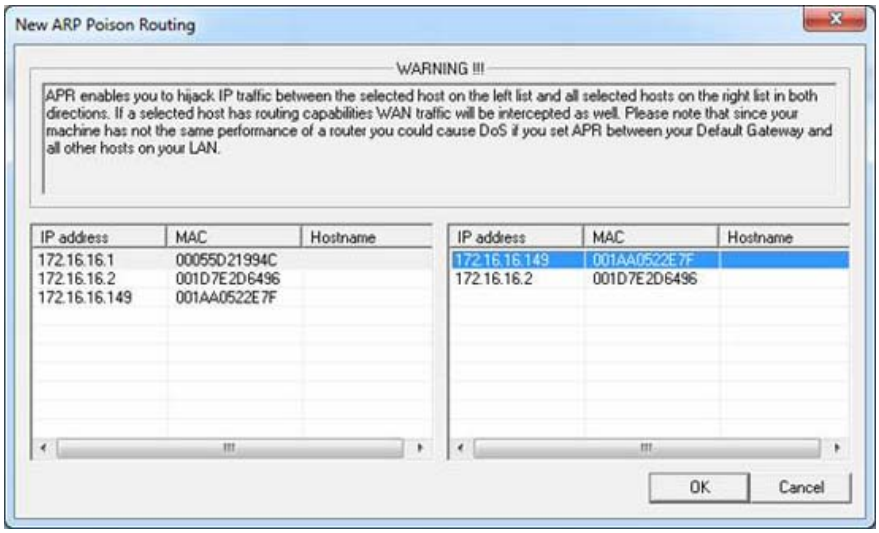


Figure 5: Select the victim device of tampering

The IP addresses of both devices will now be listed in the upper panel of the main application window. To complete the process, click on the radiation symbol (black gold) on the standard toolbar. That will enable Cain & Abel's ARP cache forgery features and allow your analytics system to become an eavesdropper for all communications between the two victims. If you want to see what's going on behind this font, install Wireshark and listen from the interface when you activate spoofing. You will see ARP traffic to the two devices and immediately see the communication between them.

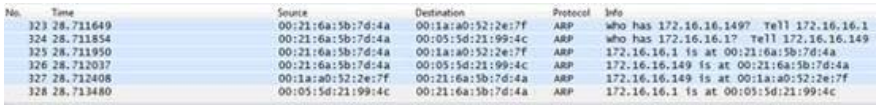


Figure 6: Insert ARP traffic

When finished, click on the radiation symbol (black gold) again to stop the ARP cache spoofing action.

Prevention measures

Studying the ARP cache spoofing process from the standpoint of the prevention, we have a little disadvantage. The ARP process occurs in the background mode, so there is little possibility that they can be controlled directly. There is no specific solution, but we still need pioneering and reactive stances if you are concerned about ARP cache spoofing in your network.

LAN security

ARP Cache spoofing is just an attack technique that only survives when trying to block traffic between two devices on the same LAN. The only reason you fear this problem is whether your internal device is compromised, whether a trusted user intends to be malicious or if someone can plug it in. Unreliable to the network. Although we often focus all of our security efforts on the network, preventing against threats from within and having a good internal security attitude can help you eliminate. Get scared in the attack mentioned here.

Encrypt ARP Cache

One way to protect against the inherent insecurity of ARP requests and reply ARPs is to perform a less dynamic process. This is an option because Windows computers allow you to add static entries to the ARP cache. You can view the ARP cache of your Windows computer by opening the command prompt and typing the **arp -a** command.

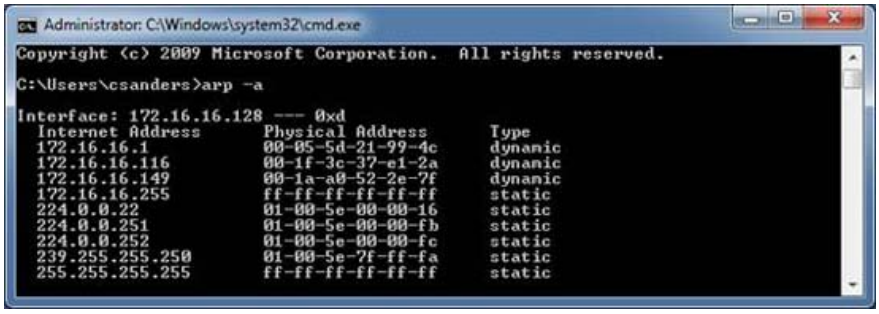


Figure 7: Viewing ARP Cache

You can add entries to this list using the **arp –s** command.

In cases where your network configuration doesn't change very often, it is possible to create a list of static ARP entries and use them for clients through an automated script. This will ensure that devices will always rely on their internal ARP cache instead of ARP requests and reply ARPs.

Check ARP traffic with a third-party program

The last option for preventing ARP cache spoofing is the response method that involves checking the network traffic of devices. You can do this with some intrusion detection systems (such as Snort) or through utilities designed specifically for this purpose (like xARP). This may be possible when you are only interested in a certain device, but it is still quite cumbersome and entangled in dealing with the entire network segment.

Conclude

ARP Spoofing is a fairly effective way in the world of man-in-the-middle passive attackers because it is very simple but effective. ARP Cache spoofing is still a very real threat on modern networks, both difficult to detect and hard to fight back. In the next part of this series, we'll focus on name resolution and DNS spoofing.

ARP and the working principle in LAN

As we know at the Network layer of the OSI model, we often use conventional types of addresses such as IP, IPX . These addresses are divided into two separate parts: the network address part (NetID). and machine address part (HostID). Such an addressing scheme makes it easier to find links from one network to another. These addresses can be changed according to user preferences.

In fact, network cards (NICs) can only connect to each other according to the MAC address, fixed and unique addresses of the hardware. So we must have a mechanism to convert these types of addresses back and forth. From there we have the address resolution protocol: Address Resolution Protocol (ARP).

Working principle of ARP in a LAN

When a network device wants to know the MAC address of a network device that already knows the address at the network layer (IP, IPX .) it sends an ARP request including its MAC address and IP address. of the device it needs to know the MAC address across an entire broadcast domain. Each device receiving this request compares the IP address in the request with its network layer address. If the address is the same, the device must send it back to the device to send a packet ARP request (which contains its MAC address). In a simple network, for example, PC A wants to send the packet to PC B and it only knows the IP address of PC B. Then PC A will have to send an ARP broadcast to the entire network to ask "where What is the PC's MAC with this IP address? " When the PC B receives this broadcast, it compares the IP address in this packet with its IP address. Realizing that the address is your address, PC B will return a packet to PC A which contains the MAC address of B. Then PC A will begin transmitting packets to B.

ARP operating principle in the network environment

The operation of ARP in a more complex environment is that two networks are tied together via a Router C. Machine A of network A wants to send packets to machine B of network B. Because the broadcast cannot be transmitted through the router. therefore, machine A will see Router C as a bridge or an intermediary (Agent) for data transmission. Previously, machine A will know the IP address of Router C (Gateway address) and know that to transmit packets to B must go through C. All such information will be contained in a table called a table routing (routing table). Routing table according to this mechanism is kept in each machine. The routing table contains information about the Gateway to access a certain network. The example in the above case in the table will indicate that to go to LAN B must go through port X of Router C. The routing table will contain the IP address of port X. The data transfer process follows these steps:

- Machine A sends an ARP request (broadcast) to find the MAC address of port X.

- Router C responds, providing machine A with MAC address of port X.

- Machine A transmits the packet to the X port of Router.

- Router receives packet from machine A, transfers packet to router's Y port. The packet contains the IP address of machine B. The router sends an ARP request to find the MAC address of machine B.

- Machine B will answer the router to know its MAC address. After receiving the MAC address of machine B, Router C sends the packet of A to B.

In fact, in addition to this routing table format, the proxyARP method is also used, including a device that performs address resolution for all other devices. Accordingly, the workstations do not need to hold the routing table. again Router C will perform the task, responding to all ARP requests of all machines.

ARP cache

ARP cache can be thought of as a table containing a corresponding set of hardware and Internet Protocol (IP) addresses. Each device on a particular network has its own cache. There are two ways to store entries in the cache to resolve the address quickly. That is:

* Static ARP Cache entries. Here, address resolution must be manually added to the cache table and maintained permanently.

* Dynamic ARP Cache entries. Here, the IP addresses and hardware are kept in the cache by the software after receiving the results of the previous resolution process. The addresses are temporarily kept and then removed.

ARP Cache turns a process that can waste time into an efficient use of time. However, it may encounter some problems. Need to maintain the cache table. In addition, it is also possible that cache entries are 'obsolete' over time, so it is necessary to expire the cache entries after a certain period of time.

See section 2: Understanding Man-in-the-Middle attacks - DNS spoofing