Mobile IP (Mobile IP)

Mobile IP (Mobile IP) is a standard proposed by the Internet Engineering Task Force (IETF) and presented in detail in RFC 3344 and RFC 5944 (RFC 5944 newly published in January). 11/2010).

***Mobile IP* (*Mobile IP*) is a standard proposed by the *Internet Engineering Task Force (IETF*) and presented in detail in RFC 3344 and RFC 5944 (RFC 5944 newly published in January). 11/2010).** Mobile IP is designed to allow users with their mobile devices to move from one network to another while maintaining ongoing information flows. Along with the development of 4G network technology, Mobile IP is still being researched and improved to ensure the mobility of devices in the future generation network. We hope that this article will help you understand the principles of operation and some basic issues of mobile IP.

In the design of IP protocol, each device when connecting to the network will be attached to a certain IP address. This is considered as the physical connection of the device to the internet. When exchanging data on the network the device is assumed to not change the IP address. If a contact node CN (Correspondent Node) sends the packet to the MN (*Mobile Node*) *mobile node* , the packet will first be routed to the HN (*Home Network*) resident *network* without depending on the current location. at MN's. Then, the mobile IP is responsible for forwarding this packet to the MN to maintain an uninterrupted flow of information between the two devices.

In order to understand the operational principles of IP Mobile, we need to become familiar with some key terms:

- Mobile MN button: is a device that installs Mobile IP client software. The MN is always assigned with a fixed IP called the Address of Resident HA (Home Address). In figure 1 below, the permanent address of the MN will be 12.1.2.3/24. When the MN is in the permanent network, the communication process is normal, the mobile button proceeds to send and receive packets as a normal device.

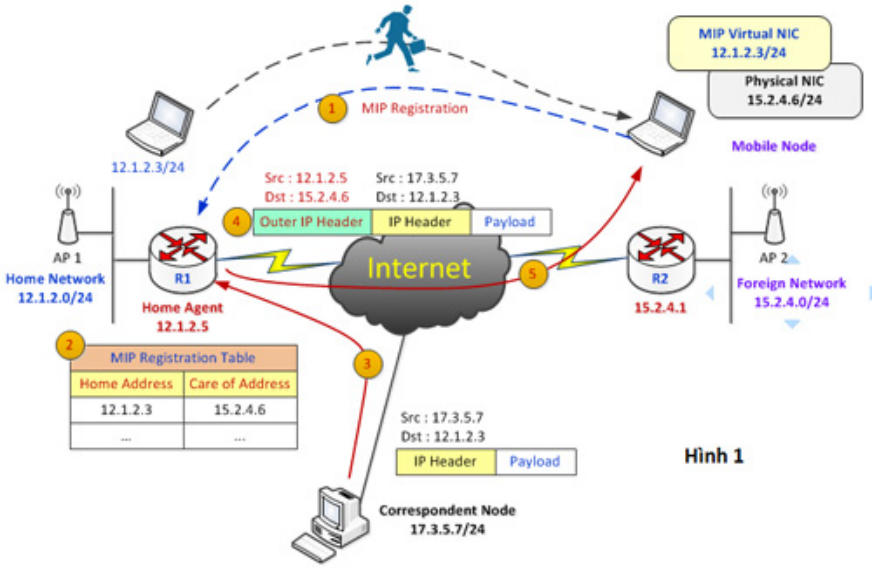
- If the MN moves out of the permanent network, the MN needs to have a HA Agent (Home Agent) on behalf of the device. The role of HA is to receive information sent to the MN and continue to forward to the new address of the MN.

- When the MN moves from the resident network to the FN (Foreign Network) temporary network, it will be provided with a temporary address called CoA (Care of Address). MN is responsible for registering with this new CoA address. The MN may receive this address from a DHCP server or use the IP of the FA (Foreign Agent) temporary agent.

You might be wondering how to make the MN determine whether it has moved away from the resident network or search for a new FA in the temporary network. This problem will be solved by the HA and FA by periodically sending broadcast messages on their local networks, the MN receives these packets and determines the necessary information. This process is known as Agent Discovery.

So how does Mobile IP work to maintain a constant stream of data when the device moves to a different network from the new IP address? To answer this question, we must see how to send packets to the MN when they are in

the temporary network in Figure 1 below:



Analysis:

1. In this illustration, the R1 router acts as a HA for the mobile node. When the MN moves to a temporary network, it will register the CoA address by sending a 'MIP registration' packet to the resident representative HA.

2. The HA uses the CoA address received in step 1 to update the registration table (MIP Registration Table). This registration table stores the mapping between permanent, temporary and some related information such as registration deadline.

3. When the packet is sent from the CN to the permanent address of the MN, the HA resident representative will act as an intermediary to receive this packet and then redirect them to the current position of the MN.

4. HA uses a "packet" method to transfer information to the MN by adding an external IP header (Outer IP header) to the original IP-in-IP tunneling and forwarding packet. CoA address that MN has registered. In the example illustrates the tunnel formed between HA and MN.

5. Physical Network Card (Physical NIC) removes the external IP header to restore the original packet and transfers it to the virtual network card (Virtual NIC). Executing applications on the MN which are only associated with the permanent address on the virtual network card, so the change of CoA of the device will not interrupt the information flow between the two devices.

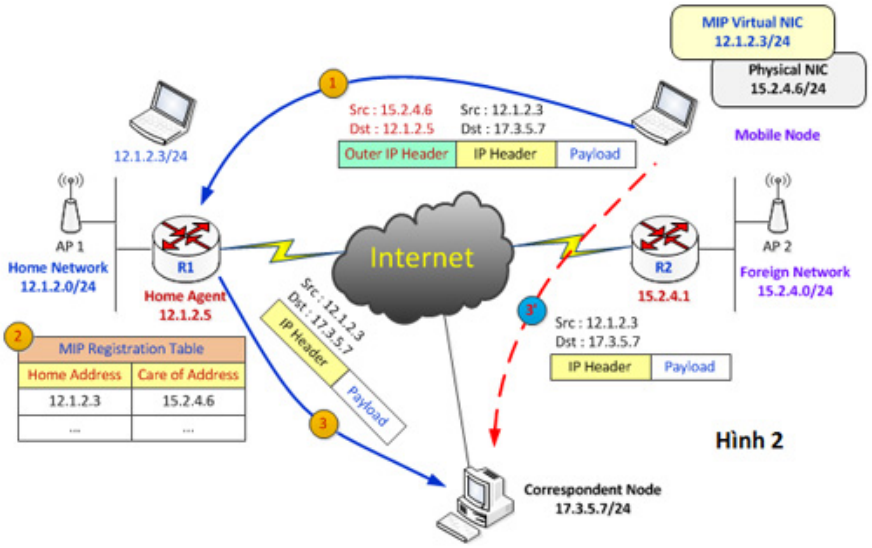
The process continues until the registration period expires (or MN moves to a new location). When this happens, MN will proceed to re-register with HA. When the MN returns to the permanent network, it no longer needs mobility, so the MN sends a request to cancel the mobile registration to the HA, stating that it is "at home" so that the HA does not perform the tunnel and clears. remove temporary addresses in the previous registration table.

As such, we have just explored the basic operational principles of Mobile IP. If we pay attention, we will see that this protocol has a disadvantage: a large delay (because the packet must first go to HA and then to MN) so it will affect time applications. real-time application. Therefore, many improvements have been made to Mobile IP to

increase efficiency and reduce delay.

The next section will explore some of the issues related to Mobile IP.

1. TR (Triangular Routing) triangular routing:



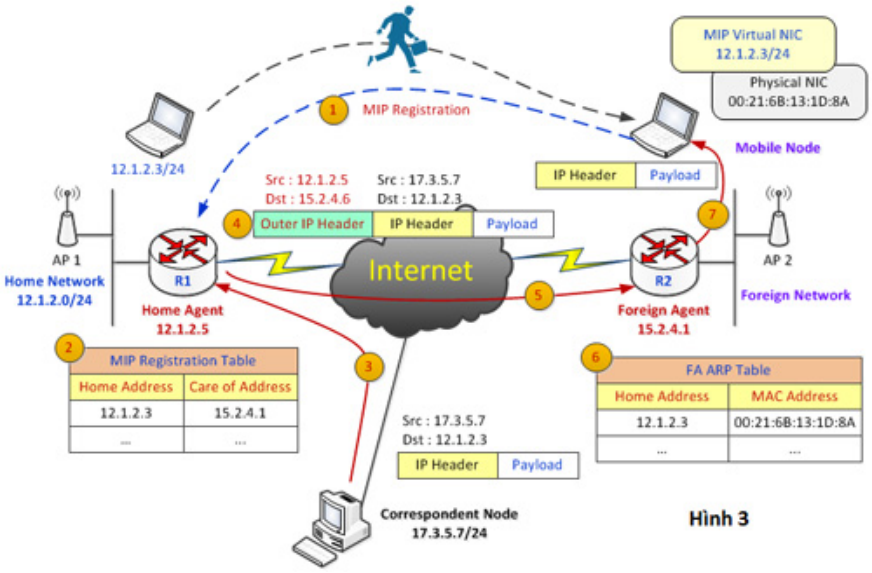
Hình 2

The MN after receiving the original packet will know the IP address of the CN correctly. Therefore, MN can send packets directly to the CN or via the tunnel to HA by transferring help. The direct sending of packets to CN will be the optimal solution to minimize the delay when sending / receiving information between MN and CN. This process is called triangular routing. However, in fact some routers and firewalls are usually configured with the "ingress filtering" function to prevent address spoofing attacks. This function will block packets with source IP addresses that are not on the local network subnet. In the figure 2, the packet sent from MN to CN will have IP source of 12.1.2.3, not belonging to the subnet of 15.2.4.0/24, so it will be removed. To solve this problem, mobile IP offers Reverse Tunneling solution. Accordingly MN will transfer the packet through the tunnel to HA before the transitional HA for CN (see steps 1, 2 and 3 in figure 2).

In order to improve routing efficiency, people give a solution to allow MN after identifying the IP address of CN, the MN will send the current CoA information directly to the branch. The CN will maintain the link mapping between the permanent address and the CoA of the MN (similar to HA) for a certain period of time. If this mapping is still valid, CN and MN will exchange data directly with each other without going through HA. If the mapping does not exist or is expired, the CN will proceed to send the packets to HA, then from HA will move to MN as normal, then MN can send CoA back to CN.

2. FA Resident Representative (Foreign Agents)

Using a real IP address (Public IP) to register as illustrated above will lead temporary networks to reserve a number of real IPs for mobile devices. If the number of MNs moving to the temporary network is too high, it will lead to a situation where there is not enough IP to provide for the new MN. To solve this problem, mobile IP has added the concept of a temporary agent FA (Foreign Agents). When the presence of FA is present, MNs will share FA IP to make their CoA. In figure 3 below CoA of MN will be IP router R2 15.2.4.1/24.



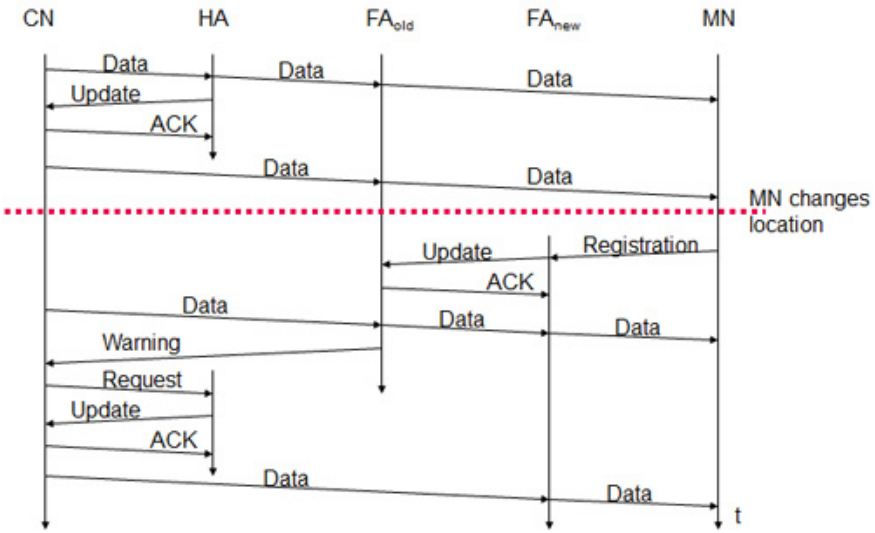
The steps from 1 to 4 are similar to the figure 1. However, the tunnel is formed between HA and FA and not between HA and MN. At FA, the original packet will be restored by removing the external IP header. After that, the FA based on MAC address information has its ARP table to send information to MN's current location correctly.

3. NAT and mobile IP

When the MN is behind a NAT device, the IP-in-IP tunnel between HA and MN cannot be performed, because the CoA address cannot be accessed directly from the external network. To solve this problem, the mobile IP executes the encapsulation of 'IP packet' in 'UDP segment' and uses the IP-in-UDP tunnel to send information (see details of IP-in-UDP tunneling in RFC). 3519).

4. Forwarding

If MN moves from this temporary network to another temporary network, it will transfer from the old FA (FAold) to a new FA (FAnew), then during the transition from FAold to FANew, the package information will continue to be moved to FAold. And to reduce the number of lost packets due to this problem, people have improved the forwarding feature to allow FAold to forward the information it received to FAnew.



Conclude

Here we have explored the basics of Mobile IP mobile management protocols that operate at the network layer (Network layer). Mobile IP was designed by IETF to solve mobile Internet problems. Since the advent of MIPv4 (Mobile IP version 4), there have been a lot of improvement studies to reduce the time from the time MN moves to the time the HA receives the CoA information of MN. And now, MIPv6 (Mobile IP version 6) is also being researched and completed.

The author is currently a lecturer of Saigon Technology Institute - SaigonCTT. For information on the article, please email **info@saigonctt.com.vn**