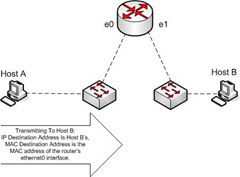
**1.ARP là gì?**

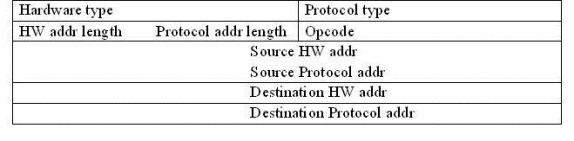
[[](http://hoangho.files.wordpress.com/2011/03/arp-with-router-3.jpg)](http://hoangho.files.wordpress.com/2011/03/arp-with-router-3.jpg)Mỗi thiết bị mạng đều có một địa chỉ MAC (Media Access Control address) và địa chỉ đó là duy nhất. Các thiết bị trong cùng một mạng thường dùng địa chỉ MAC để liên lạc với nhau tại tầng Data Link.

Trên thực tế, các card mạng (NIC) chỉ có thể kết nối với nhau theo địa chỉ MAC, địa chỉ cố định và duy nhất của phần cứng. Do vậy ta phải có một cơ chế để chuyển đổi các dạng địa chỉ này qua lại với nhau. Từ đó ta có giao thức phân giải địa chỉ: Address Resolution Protocol (ARP).

Đây là giao thức dùng để chuyển đổi giữa địa chỉ lớp 3 thành địa chỉ vật lí lớp 2. Sở dĩ cần phải có giao thức chuyển đổi như vậy là do có nhiều giao thức lớp 3 như IP; IPX,… mỗi giao thức lại có qui ước về địa chỉ logic riêng. Khi được đóng gói vào một frame tại lớp thì tất cả các địa chỉ này cần phải được qui đổi thành một kiểu địa chỉ thống nhất (địa chỉ MAC) nhằm giúp cho mọi thiết bị có thể trao đổi với các thiết bị khác khi chúng nằm trong cùng một môi trường truyền dẫn vật lí.

Mặc dù ARP là giao thức lớp 3, tuy nhiên nó lại được coi là giao thức IP cấp thấp bởi vì gói tin ARP không được đóng gói với header của các giao thức lớp 3 mà được đóng gói bởi frame lớp 2. ARP không chỉ được sử dụng trong mạng LAN ethernet mà còn có thể sử dụng cho các mạng LAN dạng token ring hoặc FDDI.

**Cấu trúc của 1 bản tin ARP bao gồm các trường:**

[](http://hoangho.files.wordpress.com/2011/03/arp_1.jpg)

Trong đó :

-Hardware type và protocol type qui định kiểu của phần cứng và của protocol được dùng ở lớp network

-Opcode: cho biết bản tin ARP là yêu cầu (=1) hoặc phúc đáp (=2)

-HW addr length: độ dài của địa chỉ vật lí.

-Protocol addr length: độ dài của địa chỉ logic.

-4 trường còn lại là địa chỉ vật lí và địa chỉ logic nguồn và đích.

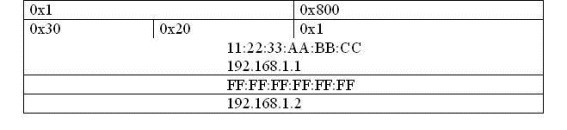
**2.Quá trình gửi 1 bản tin ARP:**

Khi một gói tin được gửi từ lớp mạng xuống, module Address Resolution ở lớp dưới cần phải chuyển đổi <kiểu protocol, kiểu địa chỉ logic đích> thành địa chỉ vật lí 48 bit.

Khi đó module này sẽ kiểm tra trong bảng ánh xạ của nó gọi là ARP cache để tìm xem có một cặp ánh xạ giữa địa chỉ logic đích với một địa chỉ vật lí nào đó hay không.

Nếu tìm được một ánh xạ như vậy, module sẽ trả về địa chỉ vật lí và địa chỉ này sẽ được dùng để chuyển đến đúng đích. Nếu không có ánh xạ như vậy, nó sẽ gửi đi bản tin ARP có địa chỉ vật lí đích là địa chỉ broadcast và Opcode=1. Bản tin này sẽ được gửi đến tất cả các thiết bị có trong mạng.

**Ví dụ:** một máy có địa chỉ IP là 192.168.1.1 muốn gửi đi bản tin ARP để tìm địa chỉ vật lí của máy có địa chỉ IP 192.168.1.2 thì bản tin ARP request sẽ có cấu trúc.

[](http://hoangho.files.wordpress.com/2011/03/arp_2.jpg)

**3.Quá trình nhận gói tin ARP:**

Khi một host trên mạng nhận được bản tin yêu cầu ARP, nó sẽ xử lí như sau:

-Kiểm tra xem có cùng HW type, Protocol type không. Nếu có, nó sẽ kiểm tra xem <protocol type, kiểu địa chỉ logic người gửi> có tồn tại trong bảng ARP cache của nó hay không. Nếu có thì cập nhật lại địa chỉ MAC tương ứng nếu thấy có thay đổi và đặt cờ Merge-flag = true.

-Kiểm tra xem địa chỉ logic của nó có trùng với địa chỉ logic đích mà gói tin gửi đến hay không. Nếu có và cờ Merge là false, nó sẽ cập nhật <protocol type, kiểu địa chỉ logic và vật lí của người gửi> vào bảng ARP cache của mình. Nếu không, gói tin ARP request sẽ bị hủy.

-Kiểm tra opcode: nếu opcode là request thì gửi lại bản tin ARP theo dạng unicast thông báo cho máy yêu cầu biết được địa chỉ MAC của mình.

-Thiết bị yêu cầu, sau khi nhận được bản tin ARP reply, sẽ cập nhật lại bảng ARP cache của mình và chuyển frame đến đích theo địa chỉ MAC nhận được. Trong trường hợp không có một bản tin reply nào đến có nghĩa là thiết bị mà nó muốn trao đổi không nằm cùng mạng LAN với nó, nếu trong mạng có cấu hình proxy ARP (thiết bị dùng để trả lời các ARP request) thì proxy ARP này sẽ có nhiệm vụ gửi bản tin ARP phúc đáp với địa chỉ MAC của nó như thể là phúc đáp của máy đích. Khi đó gói tin lớp 2 sẽ được đóng gói với địa chỉ MAC là địa chỉ MAC của proxy ARP và mọi thông tin sẽ được gửi đến proxy ARP này. Nếu không tồn tại proxy ARP trong mạng; gói tin sẽ bị huỷ và thông báo lỗi lên lớp trên.

**4.Các đặc điểm của giao thức ARP:**

Mỗi ánh xạ IP-MAC trong ARP cache đều chỉ tồn tại trong một khoảng thời gian cố định (trừ các ánh xạ đã được đặt tĩnh). Việc đề ra khoảng thời gian này là cần thiết khi một host nào đó:

1.Di dời khỏi mạng hoặc kết nối của host vào mạng bị hỏng

2. Địa chỉ logic của host được gán lại cho một địa chỉ vật lí mới.Khi đó bảng ARP cache của host có thể bị xoá trắng, tuy nhiên ánh xạ địa chỉ MAC-địa chỉ logic của nó vẫn còn tồn tại trong các bảng ARP cache của các máy khác. Điều này có thể dẫn đến trường hợp gói tin vẫn truyền đi được nhưng không đến được đích.

Biện pháp khắc phục trong trường hợp thứ nhất có thể là:

-Khi thiết lập kết nối bị hỏng, module Address Resolution cần phải được thông báo để loại bỏ ánh xạ ra khỏi bảng ARP cache của nó hoặc đặt một khoảng thời gian timeout cho mỗi kết nối giữa hai máy. Mỗi khi một máy nhận được bất kì một gói tin nào đó từ máy kia, nó sẽ gia hạn thời gian timeout cho ánh xạ và sau khoảng thời gian timeout mà nó vẫn không nhận được bản tin nào từ máy kia, ánh xạ giữa địa chỉ MAC-địa chỉ logic của máy kia sẽ bị loại bỏ khỏi bảng ARP cache của nó.

-Sử dụng một module xử lí thời gian timeout. Sau một khoảng thời gian nào đó, module này sẽ thực hiện việc loại bỏ ánh xạ ra khỏi bảng ARP cache. Tuy nhiên, trước khi tiến hành việc loại bỏ, module sẽ gửi đi một bản tin ARP request đến host cần phải loại bỏ. Nếu sau một khoảng thời gian rất ngắn mà nó không nhận được bản tin ARP reply từ host đó, nó sẽ tiến hành loại bỏ ánh xạ ra khỏi bảng.

Biện pháp khắc phục trong trường hợp thứ hai: khi nhận được một bản tin ARP, host sẽ kiểm tra xem địa chỉ vật lí nguồn đã tồn tại trong bảng ARP cache của nó chưa, nếu đã tồn tại rồi thì nó sẽ ghi đè địa chỉ mới này lên.

**\* Đặc điểm stateless của ARP:**

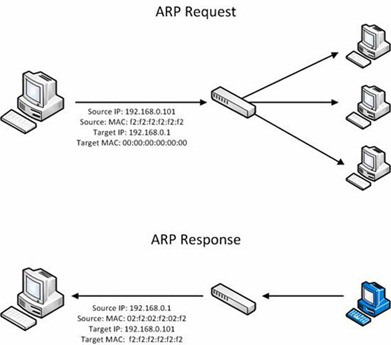
-Khi một host nhận được một bản tin ARP reply, nó sẽ cập nhật lại thông tin vào ARP cache mặc dù nó không gửi đi ARP request.

-Gratuitous ARP: đây là một bản tin được gửi đi bởi một host, yêu cầu địa chỉ MAC cho chính địa chỉ IP của nó. Trường hợp này xảy ra khi trong mạng LAN có một host khác cũng có cùng địa chỉ IP hoặc có một host tuyên bố rằng nó vừa thay đổi địa chỉ MAC.

**5.Nguyên tắc làm việc của ARP trong một mạng LAN:**

Thực chất trong vấn đề hoạt động của ARP được tập trung vào hai gói, một gói ARP request và một gói ARP reply. Mục đích của request và reply là tìm ra địa chỉ MAC phần cứng có liên quan tới địa chỉ IP đã cho để lưu lượng có thể đến được đích của nó trong mạng.

Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ ở tầng network (IP, IPX…) nó sẽ gửi một ARP request bao gồm địa chỉ MAC address của nó và địa chỉ IP của thiết bị mà nó cần biết MAC address trên toàn bộ một miền broadcast. Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong request với địa chỉ tầng network của mình. Nếu trùng địa chỉ thì thiết bị đó phải gửi ngược lại cho thiết bị gửi ARP request một gói tin (trong đó có chứa địa chỉ MAC của mình). Trong một hệ thống mạng đơn giản, ví dụ như PC A muốn gửi gói tin đến PC B và nó chỉ biết được địa chỉ IP của PC B. Khi đó PC A sẽ phải gửi một ARP broadcast cho toàn mạng để hỏi xem “địa chỉ MAC của PC có địa chỉ IP này là gì ?” Khi PC B nhận được broadcast này, nó sẽ so sánh địa chỉ IP trong gói tin này với địa chỉ IP của nó. Nhận thấy địa chỉ đó là địa chỉ của mình, PC B sẽ gửi lại một gói tin cho PC A trong đó có chứa địa chỉ MAC của B. Sau đó PC A mới bắt đầu truyền gói tin cho B.

[](http://hoangho.files.wordpress.com/2011/03/arp1.jpg)

Quá trình hoạt động của ARP

**6**.**Nguyên tắc hoạt động của ARP trong môi trường hệ thống mạng:**

Hoạt động của ARP trong một môi trường phức tạp hơn đó là hai hệ thống mạng gắn với nhau thông qua một Router C. Máy A thuộc mạng A muốn gửi gói tin đến máy B thuộc mạng B. Do các broadcast không thể truyền qua Router nên khi đó máy A sẽ xem Router C như một cầu nối hay một trung gian (Agent) để truyền dữ liệu. Trước đó, máy A sẽ biết được địa chỉ IP của Router C (địa chỉ Gateway) và biết được rằng để truyền gói tin tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng định tuyến (routing table). Bảng định tuyến theo cơ chế này được lưu giữ trong mỗi máy. Bảng định tuyến chứa thông tin về các Gateway để truy cập vào một hệ thống mạng nào đó. Ví dụ trong trường hợp trên trong bảng sẽ chỉ ra rằng để đi tới LAN B phải qua port X của Router C. Bảng định tuyến sẽ có chứa địa chỉ IP của port X.

**Quá trình truyền dữ liệu theo từng bước sau :**

- Máy A gửi một ARP request (broadcast) để tìm địa chỉ MAC của port X.

- Router C trả lời, cung cấp cho máy A địa chỉ MAC của port X.

- Máy A truyền gói tin đến port X của Router.

- Router nhận được gói tin từ máy A, chuyển gói tin ra port Y của Router. Trong gói tin có chứa địa chỉ IP của máy B. Router sẽ gửi ARP request để tìm địa chỉ MAC của máy B.

- Máy B sẽ trả lời cho Router biết địa chỉ MAC của mình. Sau khi nhận được địa chỉ MAC của máy B, Router C gửi gói tin của A đến B.

Trên thực tế ngoài dạng bảng định tuyến này người ta còn dùng phương pháp proxyARP, trong đó có một thiết bị đảm nhận nhiệm vụ phân giải địa chỉ cho tất cả các thiết bị khác.Theo đó các máy trạm không cần giữ bảng định tuyến nữa Router C sẽ có nhiệm vụ thực hiện, trả lời tất cả các ARP request của tất cả các máy.

**7.ARP cache:**

ARP cache có thể coi như một bảng có chứa một tập tương ứng giữa các phần cứng và địa chỉ Internet Protocol (IP). Mỗi một thiết bị trên một mạng nào đó đều có cache riêng. Có hai cách lưu giữ các entry trong cache để phân giải địa chỉ diễn ra nhanh. Đó là:

- Các entry ARP Cache tĩnh. Ở đây, sự phân giải địa chỉ phải được add một cách thủ công vào bảng cache và được duy trì lâu dài.

- Các entry ARP Cache động. Ở đây, các địa chỉ IP và phần cứng được giữ trong cache bởi phần mềm sau khi nhận được kết quả của việc hoàn thành quá trình phân giải trước đó. Các địa chỉ được giữ tạm thời và sau đó được gỡ bỏ.

ARP Cache biến một quá trình có thể gây lãng phí về mặt thời gian thành một quá trình sử dụng thời gian một cách hiệu quả. Mặc dù vậy nó có thể bắt gặp một số vấn đề. Cần phải duy trì bảng cache. Thêm vào đó cũng có thể các entry cache bị “cũ” theo thời gian, vì vậy cần phải thực thi hết hiệu lực đối với các entry cache sau một quãng thời gian nào đó.