1. Địa chỉ IP

Định nghĩa: Là một loại địa chỉ được quy định trong giao thức IP, nhằm mục đích “đánh số” cho các thiết bị tham gia vào kết nối liên mạng

Phân loại: Hiện nay có 2 loại địa chỉ: IPv4 và IPv6

* IPv4 (32bit)
* IPv6 (128bit)

Cấu trúc của địa chỉ IP gồm 2 phần:

* NetID: Định danh phân mạng
* HostID: Định danh cho thiết bị trong mạng

Về vấn đề đánh địa chỉ IP, có 2 mô hình là phân lớp và không phân lớp

* Mô hình phân lớp: Quy định sẵn độ dài phần netID thành các lớp A, B, C, D, E. Phần còn lại là hostID
* Mô hình không phân lớp: Không quy định sẵn mà phải thêm một subnet mask đi kèm để quy định độ dài của phần netID

Trong kết nối liên mạng, thường chia ra là mạng nội bộ và mạng internet, nên để kiểm soát lưu thông giữa các mạng, tránh việc gửi các gói tin trong mạng nội bộ rò rỉ ra bên ngoài, người ta đặt ra 2 loại địa chỉ là địa chỉ public và private. Dải địa chỉ private ở IPv4 gồm có

* 10.0.0.0/8
* 172.16.0.0/12
* 192.168.0.0/16
* 169.254.0.0/16

Một số IPv4 đặc biệt

* Địa chỉ Network: Toàn bộ hostID = 0
* Địa chỉ Broadcast trong mạng: toàn bộ hostID = 1
* Địa chỉ Broadcast nội bộ (dùng để broadcast trong nội bộ mạng hiện tại): 32 bit 1
* Địa chỉ nguồn rỗng (khi một máy chưa có địa chỉ IP cụ thể sẽ dùng tạm đ/c này): 32 bit 0

Bài tập Ví dụ:

ISP: 190.1.0.0 Cần phân địa chỉ cho các nhóm khách hàng

Group 1: 128 Customer \_ 64 Address/ 1 Customer

Group 2: 64C \_ 128A

Group 3: 256C \_ 64A

Xác định dải địa chỉ đã phân cho từng khách hàng trong nhóm

Tìm xem khách hàng nào có đ/c 190.1.30.65

Bài làm

\*Vì 64 đ/c = 2^6 -> sẽ mất 6 bit làm hostID -> số bit làm mask là 32-6 = 26

128 đ/c sẽ là 32 - 7 = 25 bit làm mask

--------------------Chia địa chỉ---------------------

G1: Customer 1 \_ 190.1.0.0/26 -> 190.1.0.63/26

G1: Customer 2 \_ 190.1.0.64/26 -> 190.1.0.127/26

....

G1: Customer 121 \_ 190.1.30.0/26 -> 190.1.30.63/26 ->**190.1.30.65 là khách hàng 122**

G1: Customer 125 \_ 190.1.31.0/26 -> 190.1.31.63/26

G1: Customer 128 \_ 190.1.31.192/26 -> 190.1.31.255/26

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

G2: Customer 1 \_ 190.1.32.0/25 -> 190.1.32.127/25

G2: Customer 2 \_ 190.1.32.128/25 -> 190.1.32.255/25

....

G2: Customer 64 \_ 190.1.63.128/25 -> 190.1.63.255/25

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

G3: Customer 1 \_ 190.1.64.0/26 -> 190.1.64.63/26

G3: Customer 2 \_ 190.1.64.64/26 -> 190.1.64.127/26

...

G3: Customer 256 \_ 190.1.127.192/26 -> 190.1.127.255/26

1. Giao thức ARP

\*Nhắc lại về địa chỉ MAC (dc vật lí) Là địa chỉ để định danh thiết bị (card mạng). Trong kết nối mạng vật lí nội bộ, các thiết bị, nếu sử dụng các công nghệ nhất định, có thể trao đổi với nhau thông qua địa chỉ MAC. VD: Trong 1 mạng LAN kết nối bởi 1 Switch, các thiết bị trao đổi thông tin thông qua gói tin ở tầng 2 Data Link và sử dụng địa chỉ MAC để trao đổi với nhau

Khi trao đổi liên mạng, các thiết bị sử dụng địa chỉ IP để trao đổi thông tin, mà theo mô hình phân tầng thì các gói tin vẫn phải được trao đổi qua tầng Data Link. Bởi vậy cần một **cơ chế để dịch từ địa chỉ IP sang địa chỉ MAC**

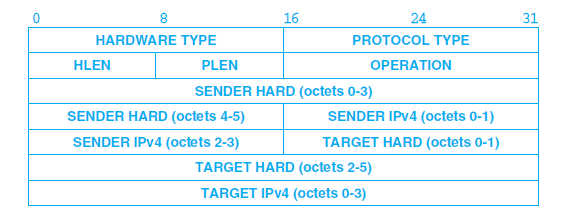
Cơ chế hoạt động: Có 2 trường hợp

* Dịch trực tiếp: Khi địa chỉ MAC có độ dài nhỏ hơn phần hostID trong IP thì ta sẽ gán địa chỉ MAC làm hostID cho thiết bị đó (Chủ yếu dùng trong IPv6 do hostID của IPv6 thường rất lớn)
* Dịch địa chỉ động: Trong trường hợp địa chỉ MAC có độ dài lớn hơn, ta sẽ sử dụng giao thức ARP
  + Bước 0: Giả sử thiết bị A có dc IP là IP-a và địa chỉ MAC là MAC-a. Thiết bị B đang muốn kết nối với thiết bị A khi đã biết IP-a
  + Bước 1: B sẽ Broadcast 1 gói tin ARP request với tham số là IP-a
  + Bước 2: Tất cả các thiết bị sẽ nhận được gói tin đó và so sánh tham số IP-a với dc IP của chính nó
  + Bước 3: Chỉ có thiết bị A thấy IP-a trùng với IP của mình, A sẽ trả lời lại cho B đ/c MAC-a của mình
  + Bước 4: 2 bên trao đổi thông qua đ/c MAC

Một số chú ý:

* Để giảm lưu lượng đường truyền, các host thiết lập và duy trì 1 bảng dịch IP – MAC gọi là ARP cache để lưu lại kết quả hỏi của lần trước
* Trong bước 1, khi B gửi request, có thể kèm theo đ/c MAC của chính B để đề phòng A chưa biết
* Khi A trả lời, có thể trả lời dưới dạng Broadcast để tất cả các thiết bị khác cùng biết đ/c MAC của A
* Khi thay đổi card mạng của mình, qua đó thay đổi địa chỉ MAC. Bởi vậy các host sẽ có thêm bước thông báo d/c MAC của mình trong quá trình khởi động hoặc/và DHCP.

Cấu trúc gói tin ARP



* HREDWARE TYPE (16bit): Xác định giao diện phần cứng trong đó giá trị 1 là địa chỉ MAC của Ethernet Address
* PROTOCOL TYPE (16bit): Để xác định loại địa chỉ sẽ được dịch bởi ARP, trong đó giá trị 0x0800 là đ/c IPv4
* HLEN (8 bit): Xác định độ dài của đ/c MAC
* PLEN (8 bit): Xác định độ dài đ/c IP
* OPERATION (16 bit): Xác định gói tin này đang ở bước nào.
* SENDER HARD (48 bit): Địa chỉ MAC bên gửi
* SENDER IPv4 (32 bit): Địa chỉ IP bên gửi
* TARGET HARD (48 bit): Địa chỉ MAC bên nhận
* TARGET IPv4 (32 bit): Địa chỉ IP bên nhận

RARP dùng trong một số trường hợp: các hệ thống boot, khi khởi động, thiết bị sẽ broadcast hỏi địa chỉ IP của mình

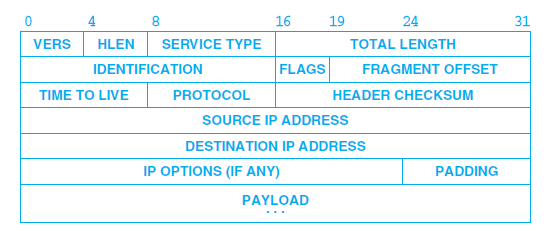
Ứng dụng: trong việc hệ thống điện toán đám mây (Cloud): dựa vào MAC ảo để chia IP, …

Thực tế hiện nay RARP không được sử dụng nhiều.

1. Giao thức IP

Định nghĩa: Là 1 giao thức truyền tin không kết nối (Là giao thức cố gắng gửi gói tin sang cho bên nhận mà không cần quan tâm đến kết nối bên nhận)

Cấu trúc gói tin IP:



-VERS (4 bit): Quy định version của IP (IPv4 hay IPv6)

-HLEN (4 bit): Quy định độ dài HEADER

-SERVICE TYPE (8 bit): Dùng để định danh loại dịch vụ truyền gói tin mong muốn

-TOTAL LENGTH (16 bit): Quy định độ dài của toàn bộ gói tin

-TIME TO LIVE (8 bit): giá trị này được đặt lúc bắt đầu gửi gói tin. Và nó sẽ giảm dần khi đi qua 1 router. gói tin sẽ bị hủy nếu giá trị này = 0 khi chưa đến đích. Việc làm này nhằm giải quyết vấn đề gói tin bị lặp vô hạn trên mạng.

-IDENTIFICATION (16 bit): Được dùng để nối các mảnh lại với nhau.

-FRAGMENT OFFSET (16 bit): Quy định vị trí của mảnh này so với gói tin đầy đủ ban đầu.

-FLAGS (4 bit): Đánh dấu đây là gói tin đầy đủ hay gói tin đã bị phân mảnh, đánh dấu đây có phải là mảnh cuối cùng hay không

-PROTOCOL (8 bit): Định danh giao thức của gói tin trong PAYLOAD

-HEADER CHECKSUM (16 bit): Checksum của header

-SOURCE IP ADDRESS (32 bit): địa chỉ IP nguồn

-DESTINA IP ADDRESS (32 bit): địa chỉ IP đích

- IP OFFTION: Lưu lại đường đi mà gói tin đi qua, định tuyến: quy định đường gói tin sẽ đi qua, lưu lại thời gian đến các router trên đường đi.

Truyền gói tin IP.

* Các thiết bị trong mạng sẽ duy trì 1 bảng thông tin gọi là bảng thông tin chuyển tiếp (FIB).
* ý tưởng cơ bản cho việc chuyển gói tin: với 1 gói tin nhất định thì giao thức IP phải tìm cách chuyển gói tin đó đến địa chỉ đích. Giao thức IP phải làm được điều này trong môi trường multi network.
* Việc chuyển gói tin trong môi trường liên mạng được thực hiện bởi các router. Các router sẽ truyền gói tin dựa theo phần netID trong địa chỉ đích đến mạng đích theo cơ chế chuyển tiếp next hop

1. Giao thức RIP (Dùng distance-vector)

Định nghĩa: Là một thuật toán định tuyến thuộc lớp distance-vector

Cơ chế hoạt động (theo cơ chế distance-vector):

* Mỗi nút mạng sẽ lưu 1 bảng FIB, trong đó chứa thông tin về đường đi ngắn nhất đến các đích đến có thể, next hop để đến các đích đó và trọng số
* Khi tại 1 nút có thay đổi, nút đó sẽ cập nhập bảng FIB của mình, sau đó gửi FIB của nó đến các nút xung quanh. Các nút đó sẽ cập nhập FIB của mình dựa theo FIB nhận được theo 3 quy tắc.

Trong RIP, trọng số được tính theo hop-count network. RIP định kì broadcast thông tin định tuyến 30s/1 lần. Thông tin định tuyến gồm:

* Đích đến
* Trọng số đến đích đó

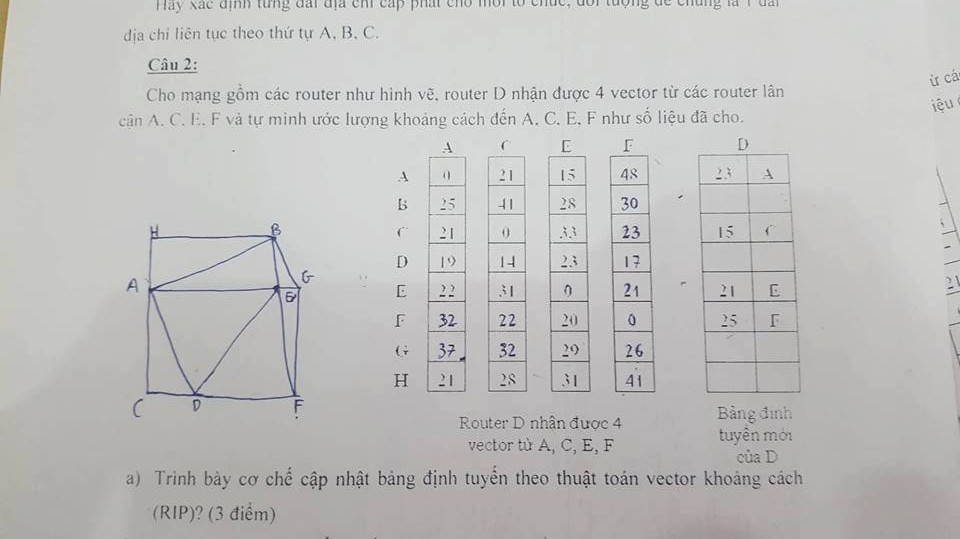
RIP chỉ cập nhập khi trọng số thực sự nhỏ hơn

RIP phát hiện 1 router lỗi bằng việc time-out

RIP phải xử lí 3 loại lỗi như sau:

* Phải có cơ chế để phát hiện vòng lặp
* RIP phải sử dụng một giá trị trọng số tối đa (<16)
* Độ hội tụ chậm (1 thông tin update phải sau 1 thời gian mới lan tỏa hết, dễ bị đụng độ nếu có 1 update xảy ra ngay sau đó).

VD bài tập



1. Giao thức TCP/IP