**BÁO CÁO THỰC HÀNH HỆ PHÂN TÁN**

**CHƯƠNG 3: ĐỊNH DANH**

# Giao thức ARP

**Câu 1: Giải thích ý nghĩa các trường trong thông điệp ARP.**

Diagram

Description automatically generated

+ **Hardware Type**: xác định kiểu bộ giao tiếp phần cứng cần biết. Xác định với kiểu Ethernet giá trị là 1

+ **Protocol Type**: xác định kiểu giao thức cấp cao (layer 3) máy gửi sử dụng để giao tiếp. Giao thức dành cho IP có giá trị là 0x0800

+ **Hardware Address Length**: Xác định độ dài địa chỉ vật lý (tính theo đơn vị byte). Địa chỉ MAC nên giá trị của nó sẽ là 6.

+ **Protocol Address Length**: Xác định độ dài địa chỉ logic được sử dụng ở tầng trên (layer 3). Tùy thuộc vào IP sử dụng mà có giá trị khác nhau, hiện tại IPv4 được sử dụng rộng rãi nên trường này sẽ có giá trị là 4 (byte).

+ **OP Code (Operation code)**: Xác định loại bản tin ARP mà máy gửi gửi. Có một số giá trị phổ biến:

* 1: bản tin ARP request
* 2: bản tin ARP reply
* 3: bản tin RARP request
* 4: bản tin RARP reply

+ **Sender Hardware Address**: Xác định địa chỉ MAC máy gửi.

* Trong bản tin ARP request: trường này xác định địa chỉ MAC của host gửi request.
* Trong bản tin ARP reply: trường này xác định địa chỉ MAC của máy host mà máy gửi bên trên muốn tìm kiếm.

+ **Sender Protocol Address**: Xác định địa chỉ IP máy gửi.

+ **Target Hardware Address**: Xác định địa chỉ MAC máy nhận mà máy gửi cần tìm

* Trong bản tin ARP request: Trường này chưa được xác định (nên sẽ để giá trị là: 00:00:00:00:00:00)
* Trong bản tin ARP reply: Trường này sẽ điền địa chỉ của máy gửi bản tin ARP request.

+ **Target Protocol Address**: Xác định địa chỉ IP máy nhận

* Trong bài thực hành này em sử dụng 2 máy:
* Máy A: 192.168.1.141
* Máy B: 192.168.1.160
* Không có bản ghi nào trong ARP table của máy A:
* Ping từ máy B đến máy A:

Text

Description automatically generated

* Kết quả nhận được khi bắt gói tin ở máy A bằng wireshark

Graphical user interface, table

Description automatically generated

**Câu hỏi 2:**

* Phân tích gói tin nhận được

Graphical user interface, text, application

Description automatically generated

- Destination MAC address : Broadcast (ff:ff:ff:ff:ff:ff)

- Opcode: request (1)

- Target MAC address: 00:00:00:00:00:00

**Câu hỏi 3:**

Graphical user interface, text, application

Description automatically generated

- Opcode : reply(2)

- Sender MAC address: IntelCor\_56:83:d0 (e4:a4:71:56:83:d0)

- Sender IP address: 192.168.1.141

- Target MAC address: 74:27:ea:58:16:e9

- Target IP address: 192.168.1.160

**Câu hỏi 4:**

* ARP Table trên máy A:



# **Tự cài đặt máy chủ DNS**

1. Thông tin những máy trong bài thực hành:

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên máy** | **Vai trò** | **Private FQDN** | **Private IP Address** |
| ns1 | Primary DNS Server | ns1.ds.soict.hust.com | 192.168.1.151 |
| ns2 | Secondary DNS Server | ns2.ds.soict.hust.com | 192.168.1.126 |
| host1 | Generic Host 1 | host1.ds.soict.hust.com | 192.168.1.100 |
| host2 | Generic Host 2 | host2.ds.soict.hust.com | 192.168.1.101 |

**Câu hỏi 5: Vai trò của block *forwarders* trong block *options* là gì?**

Block forwarders chứa địa chỉ IP của các name server mà khi ns1 không thể phân giải tên miền sẽ chuyển tiếp yêu cầu phân giải tên miền cho các DNS được liệt kê trong block forwarders xử lý. Ở đây sử dụng DNS servers của Google

**Câu hỏi 6: Giải thích yêu cầu tìm kiếm *forward* và *reverse* trong DNS là gì?**

* Forward DNS: dùng để tìm kiếm địa chỉ IP từ một tên miền cho trước
* Reverse DNS: dùng để tìm kiếm tên miền từ một địa chỉ IP cho trước

**Câu hỏi 7: 2 tệp *db.ds.soict.hust.com* và *db.192.168.1* dùng để làm gì?**

Các tệp *db.ds.soict.hust.com* và *db.192.168.1* có thể coi là cơ sở dữ liệu của máy chủ DNS, ghi các thông tin về phân giải tên miền và các thông tin config cho các máy chủ DNS.

*db.ds.soict.hust.com:* cấu hình tên miền nào ứng với IP nào trong forward lookup

*db.192.168.1:* cấu IP nào ứng với tên miền nào trong reverse lookup

**Câu hỏi 8: Hãy giải thích 3 kiểu bản ghi của DNS: SOA, NS, và A**

**- SOA (Start of Authority)** : Trong mỗi tập tin cơ sở dữ liệu DNS phải có một và chỉ một record SOA (Start of Authority). Bao gồm các thông tin về domain trên DNS Server, thông tin về zone transfer.

* **Cú pháp :**

Ảnh có chứa văn bản

Mô tả được tạo tự động

* *Serial* : áp dụng cho mọi dữ liệu trong zone và là một số nguyên. Định dạng này theo kiểu YYYYMMDDNN, trong đó YYYY là năm, MM là tháng, DD là ngày, NN là số lần sửa đổi dữ liệu zone trong ngày. Bất kể là theo định dạng nào, luôn luôn phải tăng số này lên mỗi lần sửa đổi dữ liệu zone. Khi máy chủ Secondary liên lạc với máy chủ Primary, trước tiên nó sẽ hỏi số serial. Nếu số serial của máy Secondary nhỏ hơn số serial của máy Primary tức là dữ liệu zone trên Secondary đã cũ và sao đó máy Secondary sẽ sao chép dữ liệu mới từ máy Primary thay cho dữ liệu đang có.
* *Refresh* : chỉ ra khoảng thời gian máy chủ Secondary kiểm tra sữ liệu zone trên máy Primary để cập nhật nếu cần. Giá trị này thay đổi tùy theo tuần suất thay đổi dữ liệu trong zone.
* *Retry* : nếu máy chủ Secondary không kết nối được với máy chủ Primary theo thời hạn mô tả trong refresh (ví dụ máy chủ Primary bị shutdown vào lúc đó thì máy chủ Secondary phải tìm cách kết nối lại với máy chủ Primary theo một chu kỳ thời gian mô tả trong retry. Thông thường, giá trị này nhỏ hơn giá trị refresh).
* *Expire* : nếu sau khoảng thời gian này mà máy chủ Secondary không kết nối được với máy chủ Primary thì dữ liệu zone trên máy Secondary sẽ bị quá hạn. Một khi dữ liệu trên Secondary bị quá hạn thì máy chủ này sẽ không trả lời mỗi truy vấn về zone này nữa. Giá trị expire này phải lớn hơn giá trị refresh và giá trị retry.
* *TTL (time to live)* : giá trị này áp dụng cho mọi record trong zone và được đính kèm trong thông tin trả lời một truy vấn. Mục đích của nó là chỉ ra thời gian mà các máy chủ name server khác cache lại thông tin trả lời. Việc cache thông tin trả lời giúp giảm lưu lượng truy vấn DNS trên mạng.

**- NS (Name Server)** : Record tiếp theo cần có trong zone là NS (name server) record. Mỗi name server cho zone sẽ có một NS record. Chứa địa chỉ IP của DNS Server cùng với các thông tin về domain đó.

* **Cú pháp :** [domain\_name] IN NS [DNS-Server\_name]



**- A Record – Address Record** : dùng để phân giải Host ra một địa chỉ 32-bit IPv4. Dùng để trỏ tên website như www.domain.com đến một Server Hosting website đó.



**Câu hỏi 9:** Lệnh trên sẽ đưa ra kết quả gì? Giải thích.

Text

Description automatically generated

**Câu hỏi 10:** Bạn dùng lệnh nào để chắc chắn là *bind9* đang chạy?

Text

Description automatically generated

**Câu hỏi 11:** Bạn nhận được kết quả gì sau 2 lệnh ở trên? Hãy giải thích cơ chế hoạt động của nó.

Text

Description automatically generated

Text

Description automatically generated

* Khi gõ lệnh *nslookup host1* máy sẽ tìm trong file */etc/resolv.conf* các máy chủ phân giải tên miền. Trong file có nameserver 192.168.1.151 nên máy sẽ gửi yêu cầu phân giải tên miền cho 192.168.1.151 (ns1).

Ở máy ns1, ta đã cấu hình *host1.ds.soict.hust.com. IN A 192.168.1.100* trong file *db.ds.soict.hust.com* do vậy ns1 sẽ trả về kết quả như trên hình cho máy host.