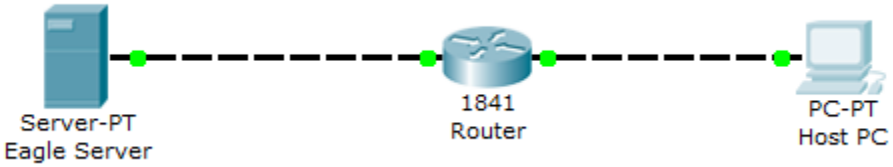
LAB 4.2: GIAO THỨC ARP

Mô hình mạng



Bảng địa chỉ IP

Device	IP Address	Subnet Mask
Eagle Server	192.168.10.5	255.255.255.0
Host PC	192.168.6.x	255.255.255.0

Mục tiêu

- Sử dụng lệnh arp.
- Phân tích hoạt động của giao thức ARP bằng Wireshark.

Kiến thức cần nắm

Giao thức ARP được sử dụng trong mô hình TCP/IP để ánh xạ một địa chỉ IP ở tầng 3 đến một địa chỉ vật lý (MAC address) của tầng 2. Khi một frame dữ liệu truyền thông trên mạng, nó cần có một địa chỉ vật lý đích. Để tự động thu thập được địa chỉ MAC của thiết bị đích, thiết bị nguồn sẽ quảng bá một ARP request ra toàn mạng LAN. Thiết bị có địa chỉ IP đích được tìm kiến sẽ trả lời và địa chỉ MAC sẽ được lưu trong bộ đệm ARP cache với mục đích truy vấn nhanh cho lần sau. Mỗi thiết bị trên mạng LAN có một ARP Cache của riêng chứa kết quả truy vấn ARP. Các kết quả truy vấn lưu trữ trong ARP cache chỉ tồn tại trong một thời gian nhất định và sẽ bị xóa đi nếu không được sử dung. Ví dụ, thời gian mặc định này trên hệ điều hành Windows là 120 giây.

Nội dung thực hiện

Tác vụ 1: Sử dụng lệnh arp

Bước1: Truy nhập vào màn hình chế độ dòng lệnh của Windows.

Click chọn **Start | Run**, gõ **cmd**, nhấn **Enter** để vào chế độ dòng lệnh của Windows. Tại máy của mình, sinh viên thực thi lệnh *arp* để tìm hiểu ý nghĩa cùng các tham số của lệnh.

```
C:\> arp
Displays and modifies the IP-to-Physical address translation tables used by address resolution
protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a              Displays current ARP entries by interrogating the current protocol data. If
                inet_addr is specified, the IP and Physical addresses for only the specified
                computer are displayed. If more than one network interface uses ARP, entries
                for each ARP table are displayed.
-g              Same as -a.
inet_addr       Specifies an internet address.
-N if_addr      Displays the ARP entries for the network interface specified by if_addr.
-d              Deletes the host specified by inet_addr. inet_addr may be wildcarded with *
                to delete all hosts.
-s              Adds the host and associates the Internet address inet_addr with the Physical
                address eth_addr.  The Physical address is given as 6 hexadecimal bytes
                separated by hyphens. The entry is permanent.
eth_addr        Specifies a physical address.
if_addr         If present, this specifies the Internet address of the interface whose address
                translation table should be modified. If not present, the first applicable
                interface will be used.
Example:
 > arp -s 157.55.85.212 00-aa-00-62-c6-09  .... Adds a static entry.
 > arp -a                                  .... Displays the arp table.
C:\>
```

Hình 4.2.1: Cú pháp lệnh arp

Thông qua việc tìm hiểu hướng dẫn của lệnh, trả lời các câu hỏi sau:

Lệnh nào được sử dụng để hiển thị tất cả các mục trong ARP cache?

_____

_____

Lệnh nào được sử dụng để xóa tất cả các mục trong ARP cache?

_____

Lệnh nào được sử dụng để xóa mục lưu cho địa chỉ 192.168.10.5 trong ARP cache?

_____

Bước 2: Dùng lệnh *arp* để kiểm tra thông tin lưu trữ trong ARP cache.

Nếu trên máy hiện tại chưa truyền thông với thiết bị nào thì bộ đệm ARP cache sẽ rỗng, kết quả hiển thị tương tự như hình 4.2.2:

```
C:\> arp -a

No ARP Entries Found
```

Hình 4.2.2: ARP cache rỗng.

Sinh viên thực thi lệnh arp –a tại máy tính, kết quả có được là gì? Giải thích

_____

_____

Bước 3: Sử dụng lệnh *ping* để cập nhật tự động các địa chỉ MAC vào bộ đệm ARP cache. Thông qua việc truy cập thiết bị khác, ARP sẽ được thực thi đồng thời để thêm các địa chỉ MAC vào bộ đệm ARP cache.

- Trước hết suử dụng lệnh *ipconfig /all* để xác nhận các thông tin của máy tính ở tầng 3 và tầng 2.
- Thực thi lệnh *ping* đến một máy tính khác cùng mạng, tương tự như hình 4.2.3:

```
C:\> ping 192.168.6.110
Pinging 192.168.6.110 with 32 bytes of data:
Reply from 192.168.6.110: bytes=32 time<1ms TTL=128
Reply from 192.168.6.110: bytes=32 time<1ms TTL=128
Reply from 192.168.6.110: bytes=32 time<1ms TTL=128
Reply from 192.168.6.110: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.6.110:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Hình 4.2.3: Lệnh Ping đến một máy

- Thực thi lệnh arp –a, kết quả sẽ thấy địa chỉ MAC của máy tính vừa ping tới, như hình 4.2.4:

```
C:\> arp -a
Interface: 192.168.6.101 --- 0x60004
  Internet Address      Physical Address      Type
  192.168.6.110         00-10-a4-7b-01-5f     dynamic
C:\>
```

Hình 4.2.4: Kết quả của hiển thị ARP cache.

Các mục ARP chứa địa chỉ MAC được thêm vào ARP cache bằng cách nào? (Chú ý kết quả tại cột Type).

_____

Địa chỉ vật lý của máy tính đích là gì?

_____

Nếu có nhiều mục ARP, điền kết quả vào bảng sau:

Địa chỉ IP	Địa chỉ vật lý	Cách thức thêm vào ARP cache

- Ngừng việc truyền thông với máy tính vừa rồi, chờ khoảng 2 đến 3 phút và kiểm tra ARP cache một lần nữa.

Có phải địa chỉ MAC của máy tính đích bị xóa không? Giải thích?

_____

- Thực hiện lệnh *ping* đến Default Gateway (192.168.6.3). Kiểm tra các mục trong ARP cache.

Địa chỉ vật lý của Default Gateway là gì?

Địa chỉ IP	Địa chỉ vật lý	Cách thức thêm vào ARP cache

- Thực hiện lệnh *ping* đến www.dlu.edu.vn và xem kết quả hiển thị các mục của ARP

Cho biết Địa chỉ vật lý của www.dlu.edu.vn là gì?

_____

Tác vụ 2: Phân tích hoạt động giao thức ARP

Bước 1: Cấu hình Wireshark để bắt gói tin.

- Click **Capture** | **Options**.
- Chọn Interface tương ứng với mạng LAN.
- Chọn mục Update list of packet in real time.
- Click **Start**

Bước 2: Chuẩn bị để bắt các frame của giao thức ARP.

- Vào chế độ dòng lệnh, click **Start | Run,** gõ **cmd** và nhấn **Enter**.
- Sử dụng lệnh *arp –a* để kiểm tra trong ARP cache đã lưu địa MAC của Eagle Server chưa? Nếu đã có rồi, sinh viên không truyền thông với máy này trong khoảng 120 giây để xóa địa chỉ khỏi ARP cache.

Bước 3: Bắt và đánh giá quá trình trao đổi của ARP.

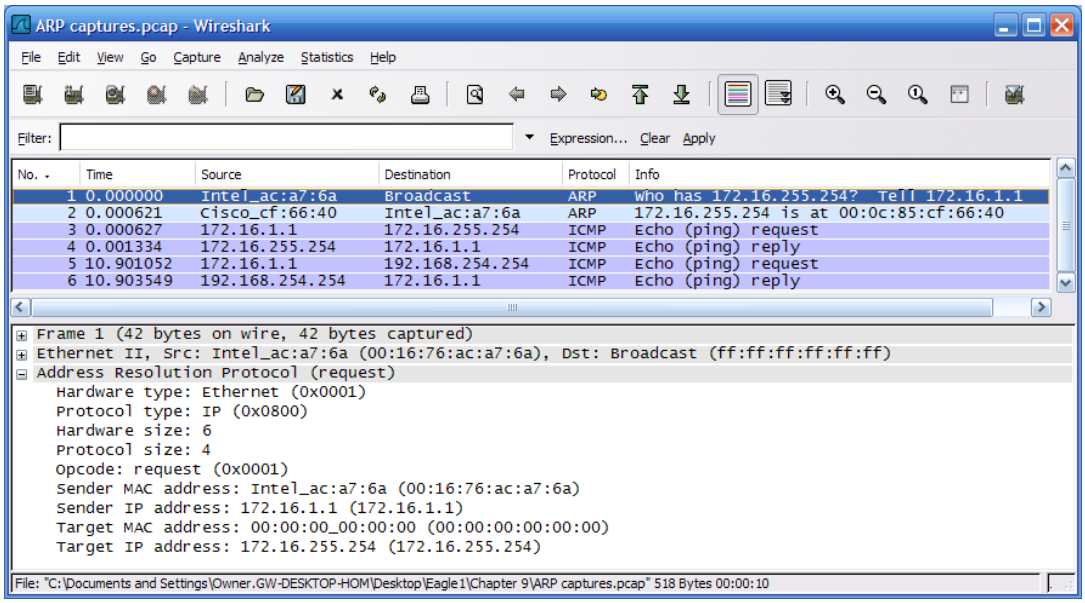
Trong bước này, các ICMP request sẽ được gửi tới Eagle Server, kết hợp dùng Wireshark để bắt và đánh giá quá trình hoạt động của giao thức ARP.

Chú ý: *Nếu không xóa được địa chỉ của Eagle trong ARP cache, sinh viên thực hiện ping đến một máy khác trong mạng để phân tích giao thức ARP.*

- Thực hiện lệnh ping đến Eagle Server, *ping eagle-server.example.com*.
- Dừng Wireshark và quan sát các gói tin bắt được. Kết quả tương tự như hình 4.2.6, trong danh sách các gói tin bắt được có giao thức ARP.
- Dựa trên kết quả thực tế, trả lời các câu hỏi sau:

  Gói tin ARP đầu tiên là gì? _____

  Gói tin ARP thứ hai là gì? _____



Hình 4.2.6: Quá trình truyền tin của ARP khi dùng Wireshark bắt được.

- Điền vào bảng các thông tin của gói ARP đầu tiên:

Field	**Value**
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

- Điền vào bảng các thông tin của gói ARP thứ hai:

Field	**Value**
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

Trong frame ARP request (được gửi broadcast ra mạng), tại sao trường Target MAC address có tất cả các bit mang giá trị 0?

_____

_____

Thực hiện lại lệnh *ping* tới Eagle Server đồng thời bắt gói. Kết quả có bắt được gói tin nào của ARP không ? Tại sao?

_____

_____

Thực hiện lệnh *ping* tới một máy ngoài internet (ví dụ *www.google.com.vn*) đồng thời bắt gói. Kết quả có bắt được gói tin nào của ARP không ? Giải thích kết quả?

_____

_____