# Bài tập thực hành Wireshark

MSSV: 18120254 Họ và tên: Nguyễn Huy Tú Lớp: 18\_2

**Lưu ý:**

* Bài tập cá nhân.
* Sinh viên làm bài trên đề bài sau.
* Cần chụp hình và ghi chú rõ ràng cho các câu trả lời.
* Nộp bài với file MSSV\_BTTH02.zip, bao gồm file báo cáo MSSV\_BTTH02.pdf và các files lưu thông tin các gói tin được bắt bởi Wireshark MSSV\_DHCP.pcap (câu 3), MSSV\_ICMP.pcap (câu 4).
* Các bài làm giống nhau sẽ nhận điểm 0.
* Chỉ nhận bài tập tại phần nộp bài của Website môn học, không nhận bài theo hình thức khác.

**Câu 1:** Cho tập tin **FTP\_01.cap**, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau:

1. *Username và password của người dùng là gì?*

Username: 07cm, password: 654321.





1. *Địa chỉ IP máy Client và máy Server là gì?*

IP Client: 10.0.0.1/8, IP Server: 10.0.0.123/8



1. *Client truy xuất lên Server theo mode nào: active hay passive?*

Client truy xuất trên Server theo mode active.

Vì client connect tới port command trên server là port 21. Sau đó Client sẽ lắng nghe và gửi command port tới server. FTP server sẽ connect tới Client bằng data port mặt định của nó là port 20.

1. *Port truyền dữ liệu của FTP Server và Client là bao nhiêu?*

Port dữ liệu:

* Port truyền dữ liệu của FTP Server: 20.
* Port truyền dữ liệu của Client: 49733.



Port lệnh:

* Port truyền lệnh của FTP Server: 21.
* Port truyền lệnh của Client: 49728.



**Câu 2:** Cho tập tin **FTP\_02.cap**, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau:

1. *FTP sử dụng giao thức nào UDP hay TCP?*

FTP sử dụng giao thức TCP.

1. *Port mặc định của FTP Server để nhận kết nối là bao nhiêu?*

Port mặc định của FTP Server để nhận kết nối nối là port 21. 

1. *Username và password của người dùng là gì?*

Usermame: cm07, password: 123654.





1. *Port truyền lệnh của Client là bao nhiêu?*

Port truyền lệnh của Client là port 49788.



1. *Client truy xuất lên Server theo mode nào: active hay passive?*

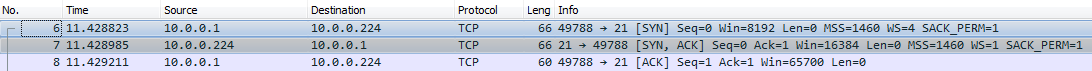
Client truy xuất trên Server theo mode passive.

Vì FTP Client khởi tạo 2 connections đến Server. Client mở 2 ports, port đầu tiên Client mở connect tới port 21 của Server. Sau đó, Client sẽ gửi câu lệnh PASV command. Lúc đó Server sẽ khởi tạo random unprivileged port. Lúc này Client khởi tạo connection giữa 2 port đó và transfer data.



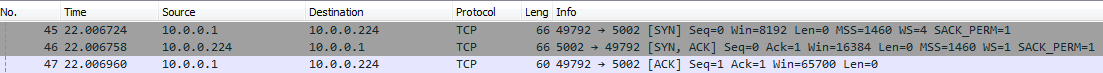
1. *Chỉ ra quá trình bắt tay 3 bước của Client và Server để tạo kết nối ban đầu khi thực hiện truyền username và password.*

Client gửi gói tin có SYN (seq=0), Server sẽ gửi lại SYN, ACK (seq=0, ACK=1). Sau đó, client gửi gói ACK (seq=1, ACK=1).



1. *Chỉ ra quá trình bắt tay 3 bước của Client và Server để tạo kết nối truyền dữ liệu.*

Client gửi gói tin có SYN (seq=0), Server sẽ gửi lại SYN, ACK (seq=0, ACK=1). Sau đó, client gửi gói ACK (seq=1, ACK=1).



1. *Port truyền dữ liệu của FTP Server và Client là bao nhiêu?*

Port dữ liệu:

* Port truyền dữ liệu của FTP Server: 5002.
* Port truyền dữ liệu của Client: 49792.



Port lệnh:

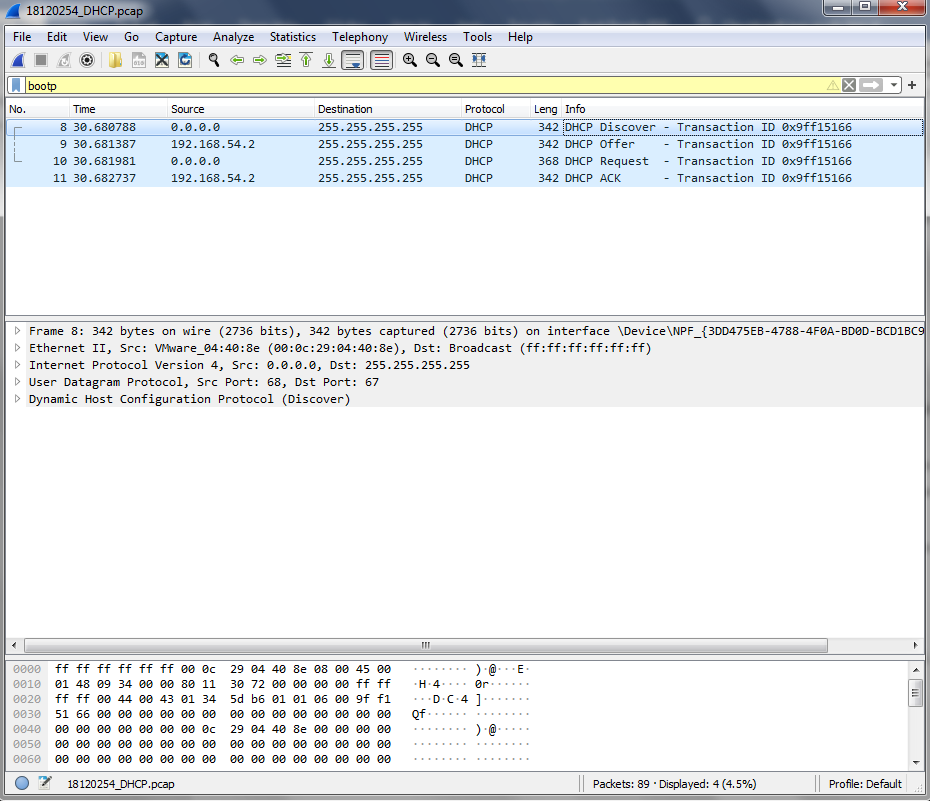
* Port truyền lệnh của FTP Server: 21.
* Port truyền lệnh của Client: 49788.



**Câu 3:** Cấu hình dịch vụ DHCP với các thông tin sau:

1. *Sử dụng máy ảo MS Windows Server 2003/2008/2012 để làm DHCP server. Thiết lập card mạng của máy ảo là Host-Only.*
2. *Cấu hình địa chỉ IP tĩnh cho máy làm DHCP server này là: 192.168.54.2/24.*
3. *Khoảng địa chỉ IP cấp cho các clients là: 192.168.54.20/24 – 192.168.54.200/24*
4. *Khoảng địa chỉ IP không được cấp tự động (exclusion): 192.168.54.50/24 – 192.168.54.70/24*
5. *Default gateway cung cấp cho các clients: 192.168.54.1*
6. *DNS server cung cấp cho các clients: 192.168.54.3*
7. *Cấu hình một máy ảo khác (ví dụ: Windows 7, Windows Server 2003…) làm DHCP client. Thiết lập card mạng của máy ảo này là Host-Only.*
8. *Tắt tính năng DHCP của phần mềm VMWare (Trên VMWare Player/Workstation > Chọn menu Edit > Virtual Network Editor > Chọn card mạng VMNet1 > Bỏ chọn “Use local DHCP service to distribute IP addresses to VMs).*
9. *Thực hiện xin cấp phát địa chỉ IP từ client đến DHCP server và dùng Wireshark để bắt gói tin của quá trình này.*
10. *Cho biết có bao nhiêu gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP?*

Có 4 gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP.

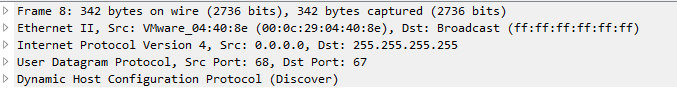


1. *Gồm những gói tin nào, giải thích mục đích của mỗi gói? Với mỗi gói cho biết: IP nguồn, IP đích, MAC nguồn, MAC đích, Port nguồn, Port đích?*

4 gói tin bao gồm: DHCP Discover, DHCP Offer, DHCP Request, DHCP ACK.

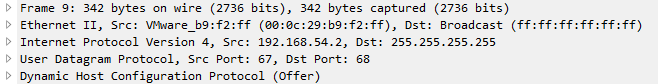
DHCP Discover: là một gói được gửi đến DHCP server từ một thiết bị Client khi muốn truy cập mạng để yêu cầu thông tin địa chỉ IP.

* + IP nguồn: 0.0.0.0
  + IP đích: 255.255.255.255
  + MAC nguồn: 00:0c:29:04:40:8e
  + MAC đích: ff:ff:ff:ff:ff:ff
  + Port nguồn: 68
  + Port đích: 67



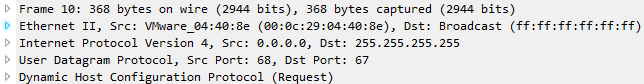
DHCP Offer: là gói tin chứa địa chỉ IP và thông tin cấu hình TCP/IP bổ sung. Nó được DHCP server gửi về cho Client sau khi nhận được DHCP Discover.

* + IP nguồn: 192.168.54.2
  + IP đích: 255.255.255.255
  + MAC nguồn: 00:0c:29:b9:f2:ff
  + MAC đích: ff:ff:ff:ff:ff:ff
  + Port nguồn: 67
  + Port đích: 68



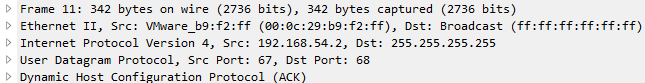
DHCP Request: là gói được DHCP client phản hồi với máy chủ sau khi nhận được DHCP Offer để thể hiện sự chấp nhận đối với địa chỉ IP.

* + IP nguồn: 0.0.0.0
  + IP đích: 255.255.255.255
  + MAC nguồn: 00:0c:29:04:40:8e
  + MAC đích: ff:ff:ff:ff:ff:ff
  + Port nguồn: 68
  + Port đích: 67



DHCP ACK: là một gói được DHCP server gửi đến cho Client để xác thực việc chấp nhận DHCP Request và định hướng các tham số tùy chọn cho phép Client tham gia mạng TCP/IP và hoàn thành hệ thống khởi động.

* + IP nguồn: 192.168.54.2
  + IP đích: 255.255.255.255
  + MAC nguồn: 00:0c:29:b9:f2:ff
  + MAC đích: ff:ff:ff:ff:ff:ff
  + Port nguồn: 67
  + Port đích: 68



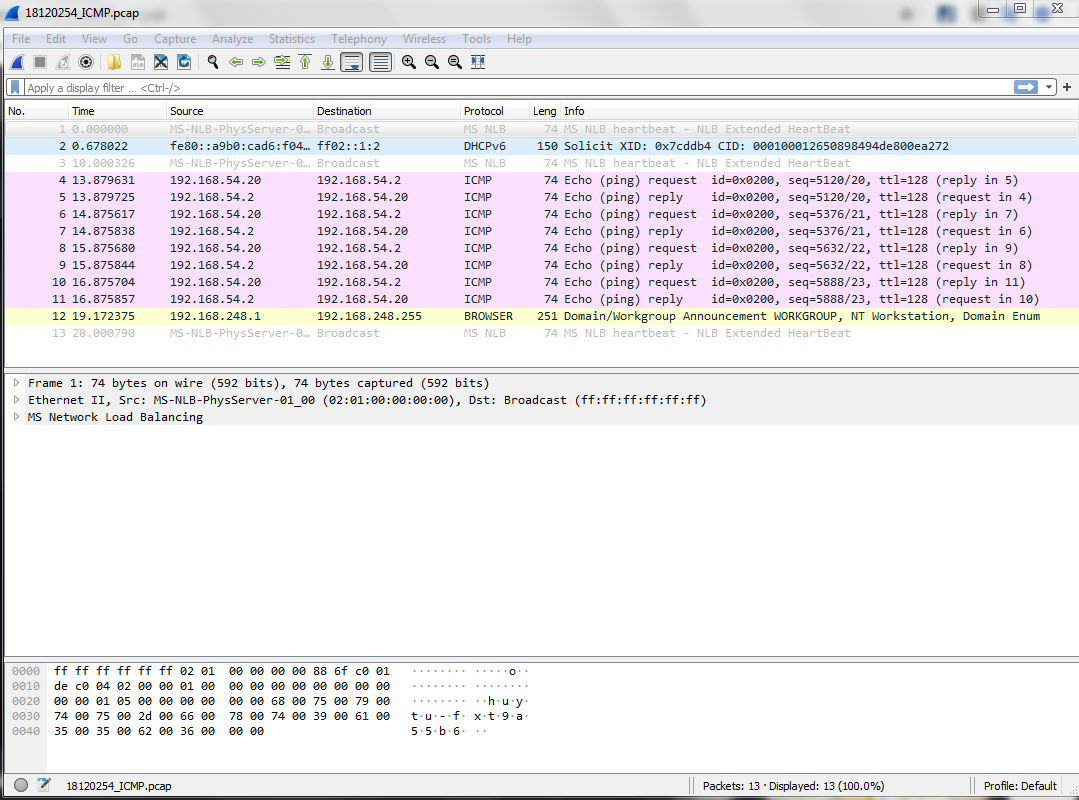
1. *Thông tin default gateway và DNS server nằm trong gói tin nào?*

Thông tin default gateway và DNS server nằm trong gói tin DHCP Offer.

**Câu 4:** Sử dụng 2 máy tính của bài tập 3, sau khi client đã có được thông tin TCP/IP được cấp phát với DHCP server, thực hiện các yêu cầu sau:

1. *Thực hiện lệnh ping từ client đến server và dùng Wireshark để bắt các gói tin tương ứng.*
2. *Cho biết có bao nhiêu gói tin của quá trình thực hiện lệnh ping?*

Có 8 gói tin của quá trình thực hiện lệnh ping.



1. *Địa chỉ MAC nguồn, MAC đích là gì?*

Địa chỉ MAC nguồn: 00:0c:29:04:40:8e

Địa chỉ MAC đích: 00:0c:29:b9:f2:ff



1. *Địa chỉ IP nguồn, IP đích là gì?*

Địa chỉ IP nguồn: 192.168.54.20

Địa chỉ IP đích: 192.168.54.2



1. *Nội dung phần data của gói tin ICMP là gì?*

